Protection des données à caractère personnel pour les services énergétiques

Franklin Leukam Lako

INSTITUT POLYTECHNIQUE DE PARIS

NNT : 2021IPPAS004

Thèse de doctorat

Protection des données à caractère personnel pour les services énergétiques

Thèse de doctorat de l'Institut Polytechnique de Paris
préparée à Télécom SudParis – EDF R&D

École doctorale n°626 Institut Polytechnique de Paris (ED IP Paris)
Spécialité de doctorat : Informatique

Thèse présentée et soutenue à Palaiseau, le 03 mars 2021, par

FRANKLIN LEUKAM LAKO

Composition du Jury :

Houda Labiod Professeure, Télécom Paris	Présidente
Benjamin Nguyen Professeur, INSA Centre Val de Loire	Rapporteur
Josep Domingo Ferrer Professeur, Universitat Rovira i Virgili	Rapporteur
Houda Labiod Professeure, Télécom Paris	Examinatrice
Claude Castelluccia Directeur de recherche, INRIA Rhone-Alpes Innovalee	Examinateur
Nesrine Kaâniche Maîtresse de conférences, Télécom SudParis	Examinatrice
Yves Roudier Professeur, Université de la Côte d'Azur	Examinateur
Maryline Laurent Professeure, Télécom SudParis	Directrice de thèse
Paul Lajoie-Mazenc Ingénieur-chercheur, EDF R&D	Encadrant industriel
Georges Hebrail Chercheur senior, EDF R&D	Invité

Résumé

Les réseaux électriques intelligents sont des briques importantes dans la lutte contre le changement climatique. Ces réseaux intelligents permettent l'introduction massive des ENR (énergies renouvelables), qui sont intermittentes, tout en garantissant la stabilité du réseau, c'est-à-dire d'assurer en temps réel l'équilibre entre la demande et la production d'énergie en aval du réseau. Cette gestion de la stabilité du réseau est possible grâce aux compteurs communicants installés dans des foyers permettant au GRD (gestionnaire de réseau de distribution) de collecter les données de consommation et de production des consommateurs et des producteurs à un pas de temps allant jusqu'à 10 min en France. Ces données de consommations en temps réel permettent de fournir de nouveaux services énergétiques, comme la prévision de consommation des clients, ou encore la demande d'effacement à la pointe. Les services d'effacement permettent d'éviter les pics de consommation dans un quartier en s'assurant qu'à chaque instant, la consommation des utilisateurs ne dépasse pas la puissance maximale fournie au niveau du quartier.

Cependant, la collecte des données de consommation pose des problèmes de vie privée. En effet, les données de consommation d'un foyer permettent de révéler le comportement des habitants de ce foyer : présences, absences, heures de lever, heures de coucher, religion, etc.

Cette thèse vise à proposer de nouveaux services énergétiques, tout en protégeant la vie privée des consommateurs. Nous proposons cinq contributions qui se rapportent à deux thèmes : 1. La transformation d'un algorithme de demande d'effacement à la pointe en le rendant respectueux de la vie privée. Cette transformation utilise du SMC (*Secure Multi-party Computation*) ou calcul multipartite sécurisé, permettant de réaliser des calculs sur des données individuelles sans jamais les révéler. 2. La publication de sommes de consommation des foyers en préservant la vie privée et une bonne utilité. Cette publication utilise la DP (*Differential Privacy*) ou confidentialité différentielle garantissant que la publication ne permet pas de révéler indirectement les consommations individuelles des foyers. En combinant la DP avec des représentations de séries temporelles comme la TFD (transformée de Fourier discrète) et la TOD (transformée en ondelettes discrète), nous obtenons une meilleure utilité par rapport aux algorithmes de publication étudiés. Ces sommes de consommation permettent notamment de réaliser des prévisions de consommation.

Abstract

Smart grids are important bricks in the fight against climate change. Smart grids allow the massive introduction of renewable energies, which are intermittent, while guaranteeing grid stability, i.e., ensuring a real-time balance between demand and production in the power grid. The management of grid stability is possible thanks to smart meters installed in households, allowing the distribution system operator to collect consumption/production data from consumers/producers at a time step of up to 10 min in France. This real-time consumption data enables to provide new energy services, such as customer consumption forecasts or demand response. Demand response services help to avoid consumption peaks in a neighborhood by ensuring that, at all times, users' consumption does not exceed the maximum power of the local grid.

However, the collection of users' consumptions is a key privacy concern. Indeed, individual consumption data reflect the use of all electric appliances by inhabitants in a household over time, and enable to deduce the behaviors, activities, age or preferences of the inhabitants.

This thesis aims to propose new energy services, while protecting the privacy of consumers. We propose five contributions that relate to two themes : 1. The transformation of a demand response algorithm by making it privacy friendly. This transformation uses SMC (*Secure Multi-party Computation*), allowing to compute an aggregate, such as a sum of users' consumption, without disclosing any individual consumption. 2. The publication of sum of users' consumption while preserving privacy and good utility. This publication uses DP (*Differential Privacy*), ensuring that the publication of the sum does not indirectly reveal individual users' consumption. Among other energy services, these sums of consumption enable to perform consumption forecasts.

Remerciements

Cette thèse CIFRE de l'Institut Polytechnique de Paris (IPP) a été effectuée en partenariat avec EDF R&D et Télécom SudParis au sein du laboratoire commun SEIDO (Laboratoire cybersécurité et internet des objets).

Je remercie premièrement mes deux encadrants de thèse : ma directrice de thèse Maryline Laurent pour sa disponibilité, son écoute, son expérience de la recherche ; mon encadrant industriel, Paul Lajoie-Mazenc, pour sa disponibilité, sa rigueur scientifique. Cette thèse est le fruit de nos nombreux échanges.

J'ai passé 20% de mon temps dans l'équipe R3S (Réseaux, Systèmes, Services, Sécurité) du laboratoire SAMOVAR de Télécom SudParis. Je remercie tous les doctorants, postdoctorants, enseignants-chercheurs rencontrés qui m'ont accueillis, avec qui j'ai partagé des cafés, joué au futsal (avant que la Covid19 vienne tout supprimer).

La majeure partie de mon temps a été passé dans le groupe Innovation et Recherche en Cybersécurité (IRC) du département PERICLES de EDF R&D. Je remercie tous les membres de ce groupe pour la qualité de nos échanges, les parties de mini-pong, etc. Une pensée spéciale au chef de secteur FG, Frédéric Guyomard.

Le projet Privacy/Traces, riche en compétences (sociologie, datascience, cybersécurité, etc.) m'a beaucoup enrichi. Je remercie tous les membres de ce projet, en particulier Cécile Caron la pilote, Ghislain Agoua, Ivan Gazeau, Benoît Grossin, pour la contribution réalisée ensemble. Merci à Sawsan Al Zahr du laboratoire commun SEIDO pour nos échanges sur le GEEQ (Gestionnaire d'Énergie de l'Éco-Quartier).

Un spécial merci à ma famille, qui m'a soutenu durant tous ces travaux de thèse. Merci à mon père qui m'a encouragé à faire cette thèse. Merci à maman Brunette & papa Laurent, pour leur présence, et tout le soutien qu'ils me portent. Merci à Gaétane & Jonathan pour nos nombreux diners aromatisés de discussions/débats allant souvent jusqu'à l'aube. Votre présence m'a permis de me sentir moins seul pendant cette crise sanitaire. Merci à mes oncles et tantes, mes frères et sœurs, Saguy, Danielle Maxime, Karelle, pour votre présence. Enfin, merci à Carelle, pour tout et pour toujours.

Je remercie chaleureusement mes amis, qui ont été présents quand j'avais le plus besoin. Une pensée à Sophie, ma grande sœur de thèse, Marie-Calixte, Stephane & Sarah et mon filleul Maël, Jessica, Tony, Grâce, Adoline, Timal, et tous ceux que j'oublie, pour vos encouragements et votre présence.

Cette thèse est dédiée à ma mère, qui aurait bien voulu voir ces travaux de thèse. Repose en paix maman †

Cette thèse est dédiée à Rosalie Tientcheu épse Lako

Table des matières

Table des figures

Liste des tableaux

Chapitre 1

Introduction

Le changement climatique qui touche notre planète a poussé les pays de l'Europe et notamment la France à voter la LTECV (loi relative à la transition énergétique pour la croissance verte) publiée au Journal Officiel du 18 août 2015 [104]. Cette loi vise à permettre à la France de contribuer plus efficacement à la lutte contre le dérèglement climatique et à la préservation de l'environnement, ainsi que de renforcer son indépendance énergétique tout en offrant à ses entreprises et ses citoyens un accès à l'énergie à un coût compétitif [112]. Parmi les objectifs de cette loi, on peut citer la réduction des émissions de GES (gaz à effet de serre) de 40% entre 1990 et 2030 et la division par quatre des émissions de GES entre 1990 et 2050 (« facteur 4 » [1]) ; la réduction de la consommation énergétique finale de 50% en 2050 par rapport à la référence 2012 en visant un objectif intermédiaire de 20% en 2030. Le 12 décembre 2020, le secrétaire général des Nations unies, António Guterres, a déclaré au sommet pour le climat [29] que les gouvernements du monde entier devraient tous déclarer l'état d'urgence climatique jusqu'à ce que le monde ait atteint des émissions nettes de CO_2 nulles. Dans ce sens, le Royaume-Uni s'est fixé pour objectif de réduire les émissions de CO_2 de 68% entre 1990 et 2030. De même, l'UE (Union Européenne) a confirmé sa promesse de réduction des émissions de GES de 55% d'ici 2030 [63].

Les mesures phares permettant de réaliser ces objectifs sont entre autres le développement des transports propres, notamment avec l'expansion des véhicules électriques permettant de réduire l'impact carbone. En effet, la production d'électricité française est pour la plupart réalisée par les centrales nucléaires qui sont une source d'énergie bas carbone. Ainsi, comme le secteur des transports est le premier secteur en termes d'émissions de GES en France avec 29% en 2016 [126], l'électrification de ce secteur permettra de réduire les émissions de GES.

Le développement des ENR (énergies renouvelables) est aussi une mesure permettant de lutter contre le dérèglement climatique. L'UE a inscrit dans son nouveau paquet énergie-climat 2030, d'atteindre une part de 27% d'ENR dans la consommation finale brute. La France a quant à elle un objectif plus fort de 32% d'ENR en 2030 [110]. En 2018, la part des ENR était de 16% en France dans la consommation finale brute d'énergie. Ces nouvelles sources d'énergie peuvent être produites par des clients et doivent être intégrées dans le réseau existant, en

1. le facteur 4 est un terme qui désigne la division par 4 des émissions de GES à l'horizon 2050 [17].

assurant l'équilibre entre la demande et la production.

En effet, la production d'électricité grâce aux ENR dépend des conditions météorologiques, ce qui peut causer des pics de production pendant des heures creuses où il y a une faible demande de consommation. Par exemple, la nuit lors de forte intensité de vent, la production éolienne peut être supérieure à la demande. Cette production n'est pas disponible en permanence car dépendante des conditions météorologiques. De plus, sa disponibilité varie fortement, et est incontrôlable. Cette production d'électricité est donc de nature intermittente, ce qui crée de grandes variations de tension sur les réseaux et fait peser un risque de rupture (effondrement de la totalité du réseau électrique) [89].

La transformation du réseau électrique vers un réseau électrique intelligent ou *smart grid* en anglais permet la prise en charge en temps réel de la production d'ENR par différents acteurs (clients, producteurs, coopératives), tout en garantissant la stabilité du réseau. Cette gestion de la stabilité du réseau est possible grâce aux compteurs communicants installés dans chaque foyers, permettant au GRD (gestionnaire de réseau de distribution) de connaître en temps réel la demande et la production d'énergie en aval du réseau.

En France, le secteur du bâtiment constitue le plus gros poste de consommation d'énergie avec 43% de la production globale, et au total 120 millions de tonnes de dioxyde de carbone correspondant au quart des émissions nationales de GES [111]. Ainsi, la diminution de la consommation dans ce secteur contribuera à la réduction d'une part importante des émissions de GES. Les compteurs communicants permettent aux clients d'avoir des informations sur leur consommation en temps réel et donc de mieux la maitriser.

Les compteurs communicants permettent de collecter la consommation des clients à un pas de temps fin, allant jusqu'à 10 min en France [61]. Les fournisseurs d'électricité peuvent exploiter ces données de consommation électrique, également appelées courbes de charge, pour fournir des services additionnels à leurs clients. Par exemple, les fournisseurs peuvent proposer à leurs clients d'effectuer des prévisions de leur consommation, des conseils pour réaliser des économies d'énergie, ou encore de participer à des services de demande d'effacement à la pointe ou DR (*Demand Response*).

Les services d'effacement permettent d'éviter les pics de consommation dans un quartier en s'assurant qu'à chaque instant, la consommation des utilisateurs ne dépasse pas la puissance maximale fournie au niveau du quartier. Si la demande des utilisateurs est supérieure à la puissance disponible, le fournisseur demande aux utilisateurs flexibles de décaler l'usage de leurs appareils en échange d'une réduction de leur facture d'électricité. Ce type de service permet de résoudre un des problèmes lié à l'avènement des véhicules électriques : en effet, si plusieurs habitants du quartier chargent leur véhicule au même moment – par exemple le soir à 19h, lors d'un pic de consommation –, l'appel de puissance pourrait dépasser la puissance maximale fournie au niveau du quartier.

Comme le précise la CNIL (Commission Nationale de l'Informatique et des Libertés), ces données de consommation permettent de déduire de nombreuses informations relatives à la vie privée [61]. Des techniques comme le NALM (*Non-Intrusive Appliance Load Monitoring*) cherchent, à partir d'une courbe de charge, à déterminer les appareils utilisés dans un foyer [71, 129]. Pour être efficaces, ces techniques demandent toutefois des courbes de charge

très précises, avec un pas de temps inférieur à la seconde. Même sans utiliser de technique avancée, il est aisé d'estimer les heures de lever et de coucher, ou encore le nombre de personnes composant un foyer [14]. Les courbes de charge sont donc des DCP (donnée à caractère personnel) au sens du RGPD (Règlement Général sur la Protection des Données) [131], et tout traitement les exploitant doit respecter la règlementation en vigueur : consentement, licéité, transparence, etc.

Avec le RGPD, il est encore possible d'utiliser les courbes de charges afin de fournir des services énergétiques, par exemple en demandant le consentement explicite des clients. Cependant, le risque de fuite de données reste encore présent et pèse aussi bien sur les personnes concernées que sur les fournisseurs de service : les clients peuvent subir des vols d'identité, des cambriolages, car ces données permettent d'apprendre leurs habitudes, leurs heures de présence et d'absence, etc. En outre, une fuite de données peut avoir un impact conséquent sur l'image de marque, sur le cours de l'action [123], etc. Plusieurs approches permettent de réduire ce risque : mettre en place des mesures de sécurité visant à réduire la probabilité d'une fuite de donnée, ou réduire son impact, par exemple en minimisant les DCP stockées.

La littérature propose de nombreuses technologies préservant la vie privée [81], aussi appelées PETs (*Privacy-Enhancing Technologies*) : pseudonymisation [44, 52, 62, 134, 135], chiffrement partiellement et complètement homomorphe [68, 124], SMC (*Secure Multi-party Computation*) [15, 37, 67, 83, 84, 138], DP (*Differential Privacy*) [47, 48, 49, 114, 127], etc.

Malheureusement, l'intégration de ces techniques dans les services énergétiques est généralement difficile et entraîne souvent des pertes de performance (temps de calcul) et d'utilité. En effet, les techniques comme le chiffrement homomorphe sont lourdes en temps de calcul, ce qui peut rendre les services énergétiques les intégrant énergivores. De même, pour des services qui doivent se réaliser dans un temps court et qui nécessitent des calculs complexes, le chiffrement homomorphe ne peut pas être utilisé pour les mettre en œuvre.

De plus, les mécanismes comme la DP consistent à rajouter un bruit sur les courbes de charge. Cette perturbation sur les courbes de charge manipulées dans les services énergétiques peut réduire l'utilité de ces services. Par exemple, la perturbation d'une courbe de charge peut masquer un pic de consommation, ce qui diminue l'efficacité de la prévision de consommation des foyers.

Cette thèse vise à proposer des techniques préservant la vie privée, permettant à un fournisseur d'énergie de proposer un service tout en garantissant une bonne utilité.

1.1 Contributions

Cette thèse propose cinq contributions qui se rapportent à deux thèmes :

1. Transformation d'un algorithme de demande d'effacement à la pointe en le rendant respectueux de la vie privée.
2. Publication de courbes de charge en préservant la vie privée et une bonne utilité.

1.1.1 Transformer un algorithme de demande d'effacement à la pointe en le rendant respectueux de la vie privée

Dans ce thème, nous avons proposé une contribution. Après avoir étudié le GEEQ (Gestionnaire d'Énergie de l'Éco-Quartier), un algorithme de demande d'effacement à la pointe, permettant d'éviter les pics de consommation au sein d'un quartier, nous en proposons une version respectueuse de la vie privée, qui ne collecte aucune DCP. Cette version protégée du GEEQ intègre du SMC, permettant de faire des calculs distribués sur les données individuelles de clients sans jamais les révéler. Cet algorithme ne laisse fuiter aucune consommation individuelle de clients. Les résultats expérimentaux montrent que le GEEQ protégé a la même efficacité en termes de réduction de pics de consommation que la version non respectueuse de la vie privée. Cette première contribution est appelée GEEQ protégé.

1.1.2 Publication de courbes de charge en préservant la vie privée

Ce thème est consacré à la publication d'un agrégat de courbes de charge en garantissant que l'agrégat ne permet pas de révéler indirectement une courbe de charge individuelle, ce qui permet notamment d'éviter des attaques. Cette garantie est assurée par la DP. Quatre contributions sont consacrées à ce thème.

La deuxième contribution de cette thèse est l'analyse d'un algorithme de publication de courbes de charge de l'état de l'art, dans le but d'une part, de présenter une erreur entrainant une mauvaise protection de la vie privée des foyers, et d'autre part, de proposer des solutions pour éviter ce type d'erreur. La correction de cette erreur rend hélas, le résultat de l'agrégat publié inutile.

Les troisième et quatrième contributions sont deux algorithmes permettant d'optimiser la publication de courbes de charge en garantissant une bonne protection des données de consommations individuelles des foyers tout en préservant une bonne utilité de l'agrégat. Les résultats expérimentaux montrent que ces contributions obtiennent une meilleure utilité par rapport aux algorithmes de publication proposés dans la littérature. Une analyse des performances permet de comprendre pourquoi ces contributions obtiennent une meilleure utilité.

La dernière contribution montre de quelle façon les algorithmes proposés peuvent être décentralisés de telle sorte que les agrégats de courbes de charge puissent être publiés sans l'intervention d'un tiers de confiance. Cette contribution combine des technologies utilisées dans la première contribution (GEEQ protégé), notamment du SMC, avec la DP.

Les différentes contributions de cette thèse ont été implémentées et testées en utilisant un jeu de données réelles de consommations de la commission de régulation de l'énergie irlandaise : CER (*Commission for Energy Regulation*). Ce jeu de données est présenté dans la section 2.1.2. Les familles de méthodes d'évaluation utilisées sont les suivantes :

1. Simulations à l'aide de SCALE-MAMBA [8] et en utilisant des indicateurs statistiques (moyenne, médiane).
2. Analyses de complexité.

1.2 Organisation du manuscrit

Le chapitre 2 détaille le contexte général de cette thèse liée aux *smart grids*. Ensuite, il présente trois familles de service énergétique. Le premier consiste à réaliser des prévisions de consommation des utilisateurs, leur permettant d'être conseillés en vue de réduire leur facture d'électricité. Le deuxième service permet d'éviter les pics de consommation dans un quartier. Le dernier service consiste à mettre en œuvre de l'autoconsommation collective permettant de consommer tout ou une partie de l'énergie que l'on produit grâce aux énergies renouvelables. La troisième partie de ce chapitre est consacrée à la présentation des attaques permettant de réidentifier des utilisateurs à partir de leurs données de consommation, ou courbes de charge. Nous concluons ce chapitre en présentant la règlementation en vigueur notamment le RGPD.

L'état de l'art est présenté dans le chapitre 3, et passe en revue les technologies de protection de la vie privée, ainsi que les applications de ces technologies pour les services énergétiques. Nous présentons des techniques comme le SMC, le chiffrement homomorphe qui sont utilisées dans les protocoles d'agrégations sécurisées. Ensuite, nous étudions la DP qui permet de publier des sommes de courbes de charge en limitant le risque de ré-identification des courbes de charge individuelles qui ont permis de calculer cet agrégat. Nous présentons en dernière partie de ce chapitre, des algorithmes de DR respectueux de la vie privée.

Le chapitre 4 présente la première contribution de cette thèse (GEEQ protégé). Cette contribution utilise du SMC pour transformer un algorithme de DR qui collecte des DCP des clients, en le rendant respectueux de la vie privée (sans collecter les DCP des clients). En utilisant les méthodes 1 et 2, les résultats expérimentaux montrent qu'il est possible d'éviter les pics de consommation dans un quartier tout en protégeant la vie privée des clients.

Le chapitre 5 présente les quatre contributions se rapportant à la publication de courbes de charge : une mise en garde de la communauté scientifique sur l'utilisation de la DP pour les séries temporelles, en présentant une erreur commise dans l'état de l'art. Cette erreur est bénéfique en utilité mais protège moins que ce qui est annoncé, ce qui entraine un faux sentiment de protection. Ensuite, nous présentons une nouvelle technique basée sur la DP permettant de publier des séries de sommes de consommations des foyers sans que la publication ne divulgue d'informations sur les données de consommations individuelles, tout en garantissant une bonne utilité. Les résultats expérimentaux utilisent les méthodes 1 et 2.

La conclusion générale de ce manuscrit ainsi que les perspectives de cette thèse sont présentées dans le chapitre 6.

Chapitre 2

Smart grid : rôles dans la transition écologique, et risques liés à la vie privée des consommateurs

Comme le montre la figure 2.1, le réseau électrique traditionnel est composé de quatre briques principales :

- Les sources de production d'énergie (centrale nucléaire, hydraulique, thermique, etc.).
- Le transport très haute tension et haute tension géré en France par RTE (réseau de transport d'électricité).
- La distribution d'électricité moyenne tension pour les grosses et moyennes industries, et basse tension pour les résidences, commerces et petites industries. Le GRD (gestionnaire de réseau de distribution) en France est Enedis avec 95% du territoire métropolitain ; les 5% restant sont gérés par les quelque 150 ELD (entreprises locales de distribution) [113].
- Les fournisseurs d'énergie, qui ont pour rôle de commercialiser auprès des clients l'électricité qu'ils produisent ou achètent. Ces fournisseurs peuvent aussi proposer des services aux clients, par exemple d'optimisation de leur consommation.

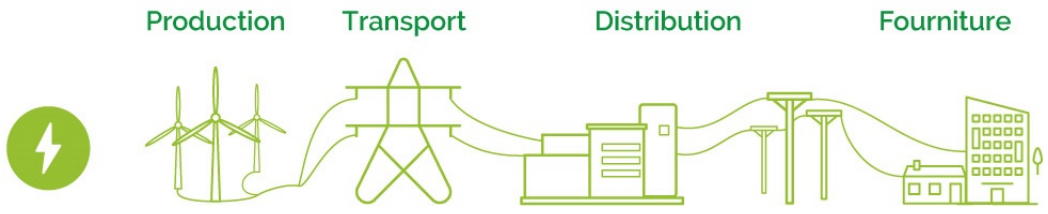


FIGURE 2.1 – Les acteurs du marché de l'énergie. Crédit : mega [109]

Dans le réseau électrique traditionnel, la production est localisée uniquement en amont du réseau. Le réseau de distribution est conçu pour servir les consommateurs.

Avec le développement des ENR (énergie renouvelable), permettant de réduire des émissions de GES (gaz à effet de serre), et ainsi d'atteindre les objectifs de la LTECV (loi relative à la transition énergétique pour la croissance verte), le réseau électrique doit être transformé afin de permettre les flux bidirectionnels, permettant l'intégration de ces nouvelles sources d'énergie. En effet, la production des ENR est décentralisée, ainsi l'électricité n'est plus produite uniquement en amont du réseau, mais aussi en aval. Par exemple, les consommateurs particuliers ou industriels peuvent être équipés de panneaux photovoltaïques, et ainsi consommer leur propre énergie et injecter le surplus sur le réseau de distribution d'énergie. En outre, l'intermittence de ces nouvelles sources d'énergie doit aussi être pris en compte afin de satisfaire l'équilibre entre l'offre et la demande.

Comme le précise le ministère de la Transition écologique [113], la modernisation du réseau électrique en un réseau intelligent ou *smart grid*, vise à « *optimiser les investissements dans les réseaux et à permettre l'insertion massive des productions intermittentes et des véhicules électriques, via l'utilisation de fonctions avancées de gestion, d'observabilité et de conduite des réseaux offrant plus de flexibilité, ainsi que le pilotage de la demande.* »

Dans ce sens, le développement des nouveaux services comme la demande d'effacement à la pointe ou DR (*Demand Response*) visent à optimiser la production et la consommation d'ENR en déplaçant par exemple l'usage des appareils flexibles (chauffe eau, chauffage) pendant les pics de production d'ENR. Pour qu'ils soient efficaces, ces services utilisent des données de consommation fines (à un pas de temps allant jusqu'à 10 min) des clients – aussi appelées courbes de charge – collectées grâce aux compteurs communicants installés dans chaque foyer.

Cependant, ces courbes de charge permettent d'identifier directement ou indirectement une personne physique. En effet des techniques comme le NALM (*Non-Intrusive Appliance Load Monitoring*) permettent d'identifier les appareils utilisées dans un foyer à partir des courbes de charge de ce foyer. Ainsi, le profil, en général unique du foyer peut être construit, en croisant l'usage de ces appareils avec d'autres données publiques, ce qui permet de l'identifier. L'utilisation de courbes de charge pose donc des problèmes de vie privée des consommateurs. Ainsi, tout traitement les exploitant doit respecter la règlementation en vigueur.

Après avoir présenté les *smart grids* dans la section 2.1, nous présentons dans la section 2.2 trois services énergétiques permettant à la fois de gérer le réseau et de permettre aux foyers de faire des économies d'énergie. La section 2.3 présente en détails les attaques NALM sur la courbe de charge. Après avoir présenté la règlementation en vigueur en section 2.4, le bilan de ce chapitre ainsi que les motivations de cette thèse sont présentés dans la section 2.5.

2.1 Smart Grids

Sauf précision contraire, les informations de cette section sont tirées de la délibération n° 2012-404 du 15 novembre 2012 portant recommandation relative aux traitements des données de consommation détaillées collectées par les compteurs communicants [61].

Les *smart grids* sont des réseaux électriques intelligents favorisant la circulation d'information entre les fournisseurs et les consommateurs. Dans ces réseaux, chaque foyer possède

un compteur intelligent, appelé Linky en France, permettant la collecte de ses données de consommation à un pas de temps régulier allant jusqu'à 10 min en France. En décembre 2019, 23 millions de ces compteurs Linky ont été installés en France avec un objectif de 35 millions prévus d'ici la fin de l'année 2021. Le compteur communicant est une des composantes des réseaux de distribution d'énergie intelligents. Ces réseaux utilisent des moyens informatiques évolués afin d'optimiser la production et l'acheminement de l'électricité, notamment grâce à la télétransmission d'informations relatives à la consommation des personnes. Cette télétransmission a notamment pour conséquence de supprimer la relève à pied des compteurs. En plus de l'optimisation de la production, ces compteurs permettent de faciliter et de fiabiliser la facturation des abonnés. Ils permettent également aux distributeurs (Enedis en France) de réaliser, de manière automatique, certaines opérations techniques à distance, comme la coupure ou le changement de puissance du compteur.

Les compteurs communicants permettent de collecter de très nombreuses informations, notamment :

— des données mesurant la qualité de l'alimentation électrique fournie à l'abonné ;
— les index de consommation : ces index permettent de calculer la consommation d'électricité et sont déjà utilisés par les fournisseurs d'énergie pour procéder à la facturation de leurs clients ;
— la courbe de charge qui est présentée dans la section 2.1.1

2.1.1 Courbe de charge

La courbe de charge est un ensemble de données de consommation collectées pendant une période de temps donnée. Sa collecte est une nouvelle fonctionnalité offerte par les compteurs communicants qui permet d'avoir une connaissance plus précise de la consommation des ménages afin de leur fournir de nouveaux services (bilan énergétique, par exemple). Cette courbe de charge est constituée d'un relevé, à intervalles réguliers (le pas de temps), de la consommation électrique de l'abonné. Plus le pas de temps est faible, plus les mesures sur une journée sont nombreuses et permettent d'avoir des informations précises sur les habitudes de vie des personnes concernées. Une courbe de charge au pas de temps 10 min permet notamment d'identifier les heures de lever et de coucher, les heures ou périodes d'absence, ou encore, sous certaines conditions, le volume d'eau chaude consommée par jour, le nombre de personnes présentes dans le logement, etc.

Enedis, en tant que GRD, est responsable de la collecte des données de consommations des clients et doit assurer la sécurité et la confidentialité de ces données par la mise en place de mesures adéquates afin notamment de garantir que ces informations ne sont pas rendues accessibles à des personnes non autorisées et ne sont utilisées que pour les finalités prévues : par exemple, en cas de détection de problèmes d'alimentation.

Le pas de temps de la courbe de charge collectée par Enedis est défini dans l'article 4 de l'arrêté du 4 janvier 2012 [9], qui prévoit que les dispositifs de comptage « doivent pouvoir mesurer et enregistrer la courbe de mesure, en puissance active, en soutirage selon trois pas de temps : horaire, demi-horaire, de dix minutes ainsi que la valeur maximale de la puissance

soutirée » (Article 4 de l'arrêté du 4 janvier 2012 [9]). La CNIL (Commission Nationale de l'Informatique et des Libertés) recommande que les paramètres de réglage des compteurs soient, par défaut, les plus protecteurs possibles pour les usagers et que toute modification du pas de mesure ainsi paramétré soit justifiée par la finalité poursuivie. Ainsi, les mesures techniques mises en œuvre dans les compteurs rendent strictement impossible la collecte, par l'intermédiaire de l'infrastructure des gestionnaires de réseau, de la courbe de charge à un pas de temps inférieur à dix minutes. Pour avoir accès aux courbes de charge à un pas de temps inférieur à dix minutes, un accès physique au compteur est nécessaire en se branchant sur la sortie de la TIC (passerelle Télé Information Client). Ainsi, en branchant un module ERL (Emetteur Radio Linky) capable de communiquer avec les objets connectés du foyer via les protocoles domotiques sans fil ZigBee et KNX sur la sortie de la TIC, un particulier ou un industriel (fournisseur, ou société de conseil en énergie) peut avoir accès aux données de consommations plus fines (à un pas de temps allant jusqu'à la seconde) leur permettant de fournir des nouveaux services plus précis en fonction des habitudes des clients. On peut penser à la flexibilité de la demande permettant par exemple de charger un véhicule électrique pendant les heures creuses de manière automatique, dans le but de consommer dans les plages où l'électricité est moins chère, et donc de réduire sa facture d'électricité.

Dans ce manuscrit, toutes les expérimentations de services énergétiques sont effectuées grâce au jeu de données de consommation présenté en section 2.1.2, publié par la CER (*Commission for Energy Regulation*) irlandaise, sur des foyers et entreprises irlandais.

2.1.2 Jeu de données de consommations irlandaise de la CER

La CER est l'organe de régulation de l'électricité et du gaz naturel en Irlande. En 2007, la CER a lancé le projet « Smart Metering » visant à évaluer la performance des compteurs communicants, leur impact sur la consommation d'énergie (électricité ou gaz) des consommateurs, et les arguments économiques en faveur d'un déploiement national plus large.

5 000 foyers et entreprises irlandaises (Dublin) ont accepté de participer à ce projet, permettant d'évaluer l'impact de leur consommation électrique [59]. Plus précisément, les données de consommation de ces foyers et entreprises ont été collectées toutes les 30 minutes du 30 décembre 2009 au 13 décembre 2010, correspondant à 348 jours. Chaque journée correspond donc à 48 pas de temps. Pour nos expérimentations, nous avons uniquement gardé les foyers, dont le nombre total est de 3 639.

La figure 2.2 donne un extrait de courbe de charge de 10 compteurs du 30 décembre 2009 de 00h à 09h30.

La figure 2.3 présente la courbe de charge de l'ensemble des 10 foyers de la figure 2.2, pendant la journée du 30 décembre 2009. Cette figure montre deux petits pics le matin à 8h et entre 11h et 14h, et un grand pic le soir à partir de 17h, ce qui pourrait correspondre aux préparatifs du nouvel an.

	row.names	Date	I1002	I1003	I1004	I1005	I1006	I1009	I1013	I1014	I1015	I1016
1	8114	2009-12-30 00:00:00	0.022	0.593	2.002	0.755	0.667	1.769	0.035	0.494	0.398	0.039
2	8115	2009-12-30 00:30:00	0.133	0.707	1.602	0.898	0.691	1.730	0.112	0.482	0.689	0.022
3	8116	2009-12-30 01:00:00	0.094	0.684	1.525	0.736	0.260	1.554	0.046	0.448	0.407	0.023
4	8117	2009-12-30 01:30:00	0.023	0.563	1.393	0.738	0.198	0.907	0.036	0.551	0.223	0.023
5	8118	2009-12-30 02:00:00	0.133	0.489	1.221	0.849	0.137	0.686	0.065	0.502	0.132	0.023
6	8119	2009-12-30 02:30:00	0.090	0.521	1.032	0.695	0.095	0.573	0.093	0.486	0.117	0.082
7	8120	2009-12-30 03:00:00	0.023	0.424	0.728	0.900	0.037	0.756	0.036	0.403	0.180	0.024
8	8121	2009-12-30 03:30:00	0.134	0.370	0.245	0.690	0.680	0.866	0.036	0.466	0.160	0.023
9	8122	2009-12-30 04:00:00	0.084	0.620	0.220	0.843	0.601	0.658	0.112	0.397	0.174	0.023
10	8123	2009-12-30 04:30:00	0.023	0.625	0.217	0.752	0.036	0.531	0.048	0.499	0.103	0.022
11	8124	2009-12-30 05:00:00	0.137	0.541	0.310	0.785	0.075	0.521	0.036	0.523	0.079	0.032
12	8125	2009-12-30 05:30:00	0.090	0.594	0.234	0.761	0.036	0.665	0.063	0.554	0.113	0.071
13	8126	2009-12-30 06:00:00	0.023	0.666	0.207	0.852	0.068	0.598	0.097	0.516	0.167	0.022
14	8127	2009-12-30 06:30:00	0.125	0.726	0.215	0.671	0.049	0.517	0.086	0.453	0.137	0.022
15	8128	2009-12-30 07:00:00	0.111	0.781	0.238	1.038	0.036	0.376	0.173	0.532	0.126	0.023
16	8129	2009-12-30 07:30:00	0.022	1.097	0.290	0.739	0.075	0.480	0.105	2.014	0.182	0.022
17	8130	2009-12-30 08:00:00	0.093	0.987	0.222	1.760	0.041	0.397	0.051	3.583	0.164	0.058
18	8131	2009-12-30 08:30:00	0.129	0.888	0.227	1.087	0.042	0.335	0.035	1.222	0.263	0.047
19	8132	2009-12-30 09:00:00	0.167	1.381	0.184	1.048	0.504	0.273	0.071	0.194	0.249	0.024
20	8133	2009-12-30 09:30:00	0.256	0.825	0.242	0.953	0.102	0.398	0.084	0.138	0.498	0.022

FIGURE 2.2 – Courbe de charge de 10 compteurs de la CER du 30 décembre 2009 de 00h à 09h30

2.2 Vers de nouveaux services énergétiques

Les courbes de charge collectées par les compteurs communicants permettent de fournir de nouveaux services. Cette section présente trois principaux services permis par la collecte de courbes de charge fines : la demande d'effacement à la pointe, la prévision de consommation et l'autoconsommation collective.

2.2.1 Demande d'effacement à la pointe

La demande d'effacement à la pointe ou DR (*Demand Response*) permet d'éviter les pics de consommation au sein d'un quartier, en vérifiant à chaque instant que la demande d'énergie est inférieure à la puissance disponible du réseau local de distribution. Si ce n'est pas le cas, alors le distributeur ou le fournisseur peut solliciter des clients, sur la base du volontariat, de décaler l'usage de leurs appareils domestiques vers les périodes de forte production renouvelable.

Parmi les solutions de DR, on peut distinguer principalement deux types de programmes : les effacements tarifaires et les effacements dissociables de l'offre de fourniture [113].

Les effacements tarifaires consistent à moduler le prix de l'électricité en fonctions des jours afin d'inciter les clients à réduire leur consommation pendant certaines périodes. On peut citer notamment des tarifs réglementés dits EJP (Effacements Jour de Pointe) qui a été

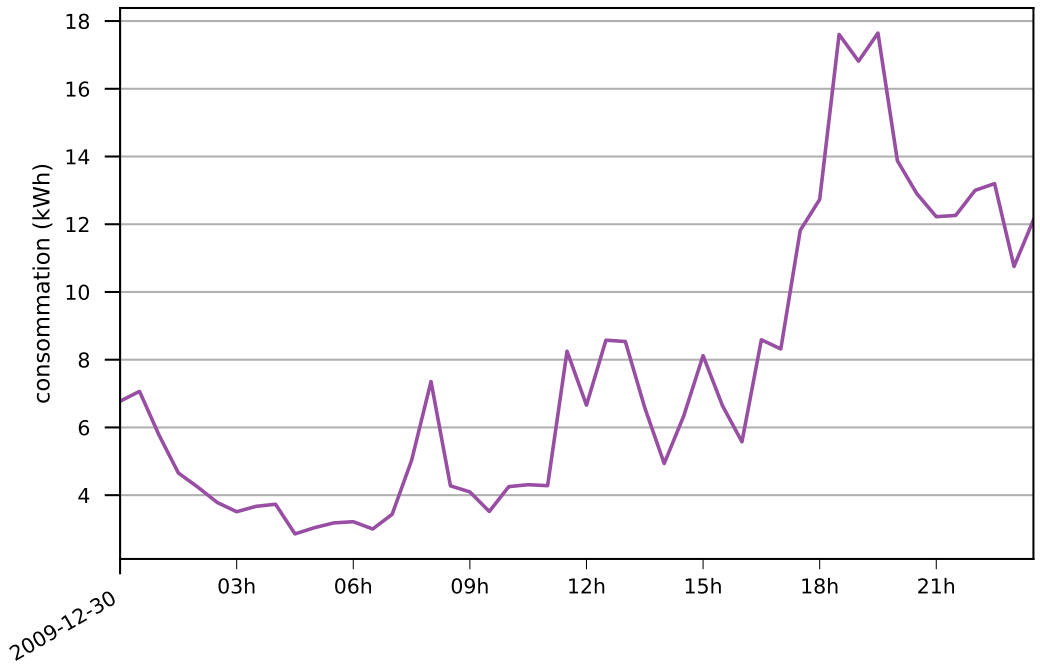


FIGURE 2.3 – Courbe de charge d'un quartier de 10 foyers pour la journée du 30 décembre 2009 de la CER

créé par EDF (Electricité de France) dans les années 80 permettant aux clients de bénéficier d'un prix du kWh 17% moins cher durant 343 jours par an tandis que 22 jours (de pointe) dans l'année ont un prix 300% plus cher. Cependant, ce tarif a été suspendu en 1990 et seuls les clients ayant souscrit à cette offre avant cette année peuvent encore en bénéficier [10]. Un autre tarif réglementé nommé Tempo et similaire aux EJP permet d'avoir un prix d'électricité très attractif 300 jours par an, un peu moins attractif 43 jours par an et exorbitant 22 jours par an.

En utilisant un tarif variable dans le temps du kWh, Al Zahr et coll. [6] montrent que le déplacement de certaines charges électriques permet de réduire la facture énergétique d'environ 8%.

Les effacements dissociables de l'offre de fourniture peuvent être classifiés en deux catégories [140]. D'une part, des programmes basés sur l'incitation qui consistent à rémunérer des clients en échange de leur flexibilité pendant des pics de consommation sur le réseau local ou régional [116]. Ce type de programme se traduit soit par le contrôle direct de la charge (les consommateurs donnent le contrôle de certains appareils électriques en échange d'une rémunération), soit par une réponse d'urgence à la demande (les clients reçoivent des paiements incitatifs pour les réductions de charge lorsqu'elles sont nécessaires pour

assurer la fiabilité du réseau), un marché de capacité (les clients sont sollicités pour réduire leur charge comme substitut pour des mécanismes de capacité [1]), ou encore un marché de services auxiliaires (les clients reçoivent des paiements d'un gestionnaire de réseau pour s'engager à réduire leur charge lorsque cela est nécessaire pour soutenir l'exploitation du réseau électrique) [118, 140].

D'autre part, les clients peuvent participer aux programmes d'appel d'offres d'effacement qui consistent à faire des offres pour réduire la charge lorsque les prix du marché de gros sont élevés [118]. Avec l'émergence d'opérateurs d'effacement indépendants, les effacements dissociables de l'offre de fourniture se sont développés de manière significative « *sous l'impulsion de nouveaux dispositifs mis en place par le Gouvernement, et devraient compenser l'érosion des effacements tarifaires observée à la fin des tarifs réglementés de vente d'électricité pour les moyens et grands consommateurs au 31 décembre 2015.* » [113]

Bien que les consommateurs individuels soient encouragés à participer à des programmes de DR, il a été démontré qu'une participation non coordonnée ne permet pas d'obtenir les avantages escomptés par les gestionnaires des réseaux électriques [101] et peut entraîner des problèmes indésirables tels que des pics de rebond. Des mécanismes de coordination sont donc nécessaires pour que les foyers puissent ajuster leurs stratégies d'optimisation sans avoir d'impact négatif sur le réseau. Dans le chapitre 4, nous présentons le GEEQ (Gestionnaire d'Énergie de l'Éco-Quartier), un algorithme de DR collaboratif.

2.2.2 Prévision de consommation

Comme son nom l'indique, la prévision de consommation permet au fournisseur ou distributeur d'énergie de prédire les consommations futures d'un foyer, d'un quartier, d'une ville, d'un département ou d'une région, etc. à partir des consommations précédentes et d'autres paramètres externes comme les données météorologiques. La prévision de consommation joue un rôle important dans la gestion du réseau notamment pour maintenir l'équilibre entre la production et la consommation d'électricité.

Une bonne prévision de consommation permet à un fournisseur de répondre au mieux à la demande de ses clients, et peut lui permettre d'éviter des achats d'énergie sur les marchés de capacité (où l'électricité est chère) pendant les périodes de pic de consommation de ses clients.

En outre, une bonne maîtrise des consommations des clients permet de rendre plus efficaces les algorithmes de DR, en définissant en avance les stratégies lors des pics ou des faibles consommations de clients. Par exemple, pendant les faibles consommations des clients, l'électricité produite par les ENR peut être stockée pour être réutilisée pendant les pics, ou revendue dans les marchés de l'énergie.

Dans l'état de l'art, plusieurs technologies sont utilisées pour réaliser des prévisions

1. Le mécanisme de capacité consiste à valoriser et à rémunérer des unités de production électrique sur la base de leur puissance disponible. Il vise in fine à pouvoir garantir à tout instant l'équilibre entre production et consommation sur un réseau électrique et ainsi à assurer la sécurité de l'approvisionnement, en particulier lors des pics de demande [25].

de consommation. On peut citer par exemple des techniques basées sur l'IA (intelligence artificielle) comme la logique floue, utilisée dans [28]. Shayeghi et coll. [139] font des prévisions en utilisant des réseaux de neurones artificiels. Les SVM (*Support Vector Machines*) et les réseaux de neurones en ondelettes sont respectivement utilisés par Chen et coll. [27], et Hossen et coll. [75]. Hossen et coll. [74] utilisent des techniques de *deep learning* pour faire de la prévision de courbes de charge des foyers.

2.2.3 Autoconsommation collective

L'autoconsommation est un nouvel usage croissant qui consiste à consommer tout ou une partie de l'énergie que l'on produit grâce aux énergies renouvelables. Elle est collective si les parties prenantes sont liées entre elles au sein d'une personne morale (association, coopérative, copropriété, etc.) [55]. La consommation de cette énergie peut être totale ou partielle. L'électricité non consommée est injectée sur le réseau et peut alors être revendue. Enedis estime que la part d'autoconsommation [2] se situe aux environs de 20% pour un logement équipé, sans système de stockage. Le reste de l'énergie dont le foyer a besoin est fourni par le fournisseur d'électricité [57].

En France, la loi n° 2017-227 du 24 février 2017 [105] suivie du décret n° 2017-676 du 28 avril 2017 [40] permet d'encadrer l'autoconsommation. Fin 2017, environ 20 000 foyers consommaient leur propre électricité [57]. Depuis avril 2018, la commune de Malaunay en Normandie a implémenté l'autoconsommation collective avec 10 bâtiments publics qui produisent localement une électricité grâce à 8 centrales photovoltaïques installées sur les toits en 2019 [56].

L'autoconsommation collective ne s'adresse pas uniquement aux collectivités. Des bailleurs sociaux, copropriétés, établissements scolaires, ou entreprises peuvent se lancer dans un projet d'autoconsommation collective à conditions de se regrouper au sein d'une personne morale [40] et d'être proches géographiquement.

Fin 2019, EDF et le promoteur OGIC se sont associés pour mettre en œuvre une opération d'autoconsommation collective solaire au sein de l'éco quartier Ydéal Confluence dans la ville de Lyon [50, 51]. Cette copropriété composée de 5 bâtiments, une centaine de logements, une résidence étudiante, des bureaux, des commerces et une crèche sur une superficie de 12 000m² produit et consomme sa propre électricité grâce à 532 panneaux photovoltaïques, un système de stockage et un pilotage intelligent de l'énergie. Le système de stockage est composé d'une batterie au lithium de 200 kWh permettant de restituer le surplus de production au moment des pics de consommation notamment le soir.
Dans cette installation, toute l'énergie produite est consommée, et permet de couvrir 50% des besoins en énergie des habitants. Ce taux est supérieur au taux d'autoproduction [3] ou de couverture moyen qui est de 20%. En outre, cette autoconsommation collective permet aux *consomm'acteur*s (consommateurs et acteurs) de faire des économies d'au moins 8% sur leur

2. La part d'autoconsommation ou taux d'autoconsommation, est égale à la production consommée sur place divisée par la production totale en utilisant des sources d'ENR.

3. Le taux d'autoproduction est égal à la production des ENR consommée sur la consommation totale.

facture d'électricité.

Concrètement, l'autoconsommation est possible grâce aux compteurs communicants Linky, notamment grâce aux Emetteur Radio Linky. En effet, le compteur Linky permet de mesurer en temps réel l'énergie produite et consommée par un foyer, ou par un bâtiment. À chaque instant, il est possible de savoir la part consommée de cette énergie et ainsi de stocker le surplus à l'aide des batteries pour les réutiliser pendant les pics de consommation.

2.3 NALM

Les nouveaux services énergétiques sont des briques permettant de lutter contre le changement climatique. Les services présentés dans la section 2.2 prennent tous en entrée les courbes de charge des foyers. Plus la courbe de charge est fine (c'est-à-dire que le pas de mesure est faible), plus le service est efficace. Cependant, plus le pas de mesure est faible, plus les mesures sur une journée sont nombreuses et permettent de déduire des informations précises sur les habitudes de vie des personnes concernées. Par exemple une courbe de charge avec un pas de temps de dix minutes permet d'identifier les heures de lever et de coucher, les heures ou périodes d'absence, ou encore, sous certaines conditions, le volume d'eau chaude consommée par jour, le nombre de personnes présentes dans le logement, etc. [61]. La courbe de charge peut ainsi permettre de déduire de nombreuses informations relatives à la vie privée des personnes concernées.

Les techniques comme le NALM permettent d'identifier les appareils utilisés dans un foyer à partir de la courbe de charge de ce foyer. Cette technique consiste à désagréger la courbe de charge afin d'identifier la charge de chaque appareil. Les recherches sur le NALM ont commencé à partir des années 1980, principalement avec des publications de Hart [70] entre 1983 et 1995. Prudenzi [129] donne également un bon aperçu de ce domaine.

Hart [73] présente une approche en deux phases permettant de résoudre le problème de désagrégation de courbes de charge afin de retrouver les appareils électriques utilisés. La première phase encore appelée phase d'entrainement permet d'apprendre le profil électrique ou signature de différents appareils, manuellement ou automatiquement en les allumant et en les éteignant. Cette phase peut être complétée ou remplacée par une base de connaissances des signatures des appareils électriques. Après la phase d'entrainement, les profils sont utilisés pour identifier les appareils électriques utilisés à partir de la courbe de charge.

Molina-Markham et coll. [117] utilisent les agendas des habitants comme information auxiliaire permettant de corréler l'usage des appareils électriques et la courbe de charge. En considérant que l'activité électrique pendant les heures creuses correspond à la consommation des appareils automatiques comme le chauffe eau, la forme de la consommation de ces appareils automatiques peut être filtrée sur la courbe de charge totale. Ainsi l'agenda des habitants du foyer, peut aider à identifier l'usage des autres appareils.

Dans [13], Batra et coll. présentent un outil open source appelé NILMTK permettant d'évaluer plusieurs algorithmes de NALM sur un ensemble de jeux de données. Cet outil contient un ensemble de fonctions statistiques et de *préprocessing* permettant par exemple

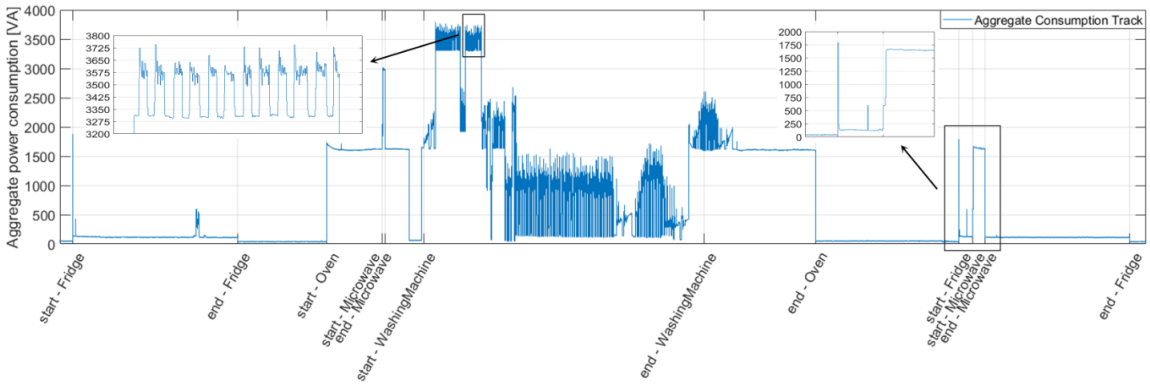


FIGURE 2.4 – Usage des appareils électriques détecté par un algorithme de NALM à partir d'une courbe de charge [121]

de nettoyer les données, une liste de quelques algorithmes de désagrégation, et un ensemble de métriques d'évaluation de ces algorithmes.

La majorité des algorithmes de NALM sont supervisés c'est-à-dire qu'ils utilisent une étape d'apprentissage qui permet de déterminer les signatures des différents appareils du foyer. Bonfigli et coll. [19] font un état de l'art des algorithmes de NALM non supervisés (qui n'ont pas besoin d'une base de connaissances de signatures d'appareils électriques) et les évaluent sur un ensemble de jeux de données en utilisant plusieurs métriques d'évaluation. Les résultats expérimentaux montrent un taux de réussite allant jusqu'à 92% en utilisant des jeux de données au pas de temps de la seconde.

La Figure 2.4 tirée de [121] montre les appareils utilisés dans un foyer à partir de sa courbe de charge en utilisant un algorithme de NALM.

Les violations de la vie privée des foyers causées par la NALM ont été dénoncées premièrement en 1989 par Hart [72]. Il identifie le NALM comme une technologie potentielle de surveillance et suggère un cadre juridique permettant de limiter la collecte des données en utilisant le NALM. Il montre par exemple que le NALM peut être utilisé par des cambrioleurs pour planifier leurs infractions lorsque les habitants ne sont pas chez eux. De plus, cette technologie peut être utilisée pour envoyer des publicités ciblées ou faire du marketing direct aux consommateurs.

2.4 Règlementations

Comme évoqué dans la section 2.3, le NALM cause des problèmes de vie privée pour les consommateurs si les courbes de charge sont divulguées. Un cadre légal est donc indispensable afin de limiter la collecte abusive des courbes de charge des foyers. La collecte des DCP (donnée à caractère personnel) comme la courbe de charge est encadrée par le RGPD (Règlement Général sur la Protection des Données) présenté dans la section 2.4.2. En France, la CNIL est en charge de l'application de ce règlement.

Depuis la loi sur l'ouverture à la concurrence du 7 décembre 2006 [103], la production et la fourniture d'énergie sont ouvertes à la concurrence en France. Les réseaux de transport et de distribution gérés respectivement par RTE et Enedis (sur 95% du territoire métropolitain) sont encore publics. Ainsi, pour éviter la concurrence déloyale, les données de clients (comme la courbe de charge) envoyées à Enedis pour gérer le réseau de distribution ne doivent pas être divulguées à un fournisseur ou à un producteur. Ces données sont appelées ICS (Information Commercialement Sensible) et définies dans le Code de l'énergie.

2.4.1 Information commercialement sensible (ICS)

Une ICS est une information dont la communication pourrait porter atteinte aux règles de concurrence libre et loyale et de non-discrimination, conformément aux articles L111-73 et -81 du Code de l'énergie [32] et au décret n° 2001-630 du 16 juillet 2001 [41], auquel il est fait référence par le décret n° 2011-1554 du 16 novembre 2011 [58]. La liste des ICS est donnée par Enedis dans le document [58] :

- les informations relatives aux puissances enregistrées, aux volumes d'énergie consommée ou produite, ainsi qu'à la qualité de l'électricité issues des comptages ou de toute autre mesure physiques effectuées par le distributeur sur les ouvrages de raccordement et les installations de l'utilisateur,
- les caractéristiques de la production, de la fourniture ou de la consommation,
- les conditions de vente de chaque fournisseur,
- l'identité des parties contractantes,
- les dispositions contractuelles,
- les conditions de paiement,
- la durée des contrats et protocoles d'accès ou de fourniture,
- les informations échangées en vue de la préparation et de l'application des contrats, des protocoles,
- les dispositions des protocoles d'accès aux réseaux publics de transport et de distribution.

Comme le précise l'article 20 de la loi n° 2000-108 du 10 février 2000 relative à la modernisation et au développement du service public de l'électricité [102] :

> « Chaque gestionnaire de réseau public de distribution préserve la confidentialité des informations d'ordre économique, commercial, industriel, financier ou technique dont la communication serait de nature à porter atteinte aux règles de concurrence libre et loyale et de non-discrimination imposées par la loi. La liste des informations concernées est déterminée par décret en Conseil d'Etat. Est punie de 15000 euros d'amende la révélation à toute personne étrangère aux services du gestionnaire d'un réseau de distribution d'une des informations visées au présent article par une personne qui en est dépositaire soit par état ou par profession, soit en raison d'une fonction ou d'une mission temporaire. »

Ainsi, toute ICS, comme la courbe de charge, doit être stockée de manière protégée par le distributeur (Enedis).

Cependant, il existe des dispositifs légaux permettant de transmettre la courbe de charge des clients au fournisseur. Par exemple pour réaliser des services de prévisions de consommation des foyers, la courbe de charge des clients peut être transmise au fournisseur après que les clients ont donné leur consentement explicite.

2.4.2 Règlement général sur la protection des données (RGPD)

En plus d'être une ICS, une courbe de charge est aussi une DCP. Ainsi, tout traitement l'exploitant doit respecter la règlementation en vigueur : le RGPD. Ce nouveau règlement est entré en vigueur le 25 mai 2018 et apporte douze grandes nouveautés par rapport à la DPD (Data Protection Directive) [80]. Ces changements visent à redonner le contrôle aux clients sur ses DCP et à l'informer du traitement qui est effectué sur ses données.

Le traitement des DCP des clients doit respecter le principe de PBD (privacy-by-design) qui consiste à appliquer des techniques de protection des données dès la conception des traitements. Le RGPD parle aussi de privacy-by-default qui consiste à appliquer la protection des données par défaut dès la conception d'un traitement.

Le RGPD met l'accent sur la notion du consentement qui doit être explicite et clair. Ce consentement a pour but d'informer le client lors d'un traitement sur ses DCP.

Le droit à l'oubli et le droit à la portabilité des données permettent de donner le contrôle au client sur ses DCP. En effet, le droit à l'oubli permet à un client de demander l'effacement de ses DCP notamment lorsque leur conservation n'est plus nécessaire. Il faut noter que le RGPD a prévu une durée de conservation des données même après la résiliation d'un contrat, ou d'un service. Par exemple, dans une entreprise, les données d'un candidat non retenu peuvent être conservées pendant 2 ans maximum (sauf s'il en demande l'effacement) par le service des ressources humaines.

Quant à la portabilité des données, elle permet au client de changer par exemple de fournisseur de service.

Concernant le transfert de données dans des pays hors de l'UE (Union Européenne), le RGPD met l'accent sur les conditions de protection des DCP pour les traitements envisagés qui doivent être conformes avec les principes de protection de UE. Dans ce sens, le transfert de données des citoyens européens vers les États-Unis était encadré par le « Privacy shield » adopté en 2016 par la Commission européenne [78]. Cependant, cet accord (« Privacy shield » ou décision 2016/1250 [78]) a été invalidé par la CJUE (Cour de justice de l'Union européenne) le 16 juillet 2020 suite à l'affaire dite « Schrems II » [30, 33].

En effet, Maximilian Schrems, juriste et ressortissant autrichien, utilisateur de Facebook depuis 2008, avait déposé une plainte auprès de l'autorité irlandaise de contrôle visant à suspendre ou à faire interdire les transferts de ses DCP par Facebook Irlande vers des serveurs de Facebook Inc. situés aux États-Unis. Dans sa plainte il évoque l'incohérence entre la protection des DCP en Europe et le droit américain sur la surveillance qui permet aux services

de renseignement et aux autorités d'accéder aux DCP traités par les opérateurs américains. Cette plainte a d'abord été rejetée puis examinée plus tard par la CJUE qui donnera raison à Schrems en invalidant un premier accord de transfert entre l'UE et les États-Unis (« Safe Harbor » [79]). Par la suite la Commission européenne avait proposé de nouvelles règles de transfert remplaçant le « Safe Harbor » via la décision 2016/1250 ou « Privacy shield » [78]. Suite aux insuffisances en matière de protection des DCP du « Privacy Shield », Schrems a déposé une nouvelle plainte visant à invalider la décision 2016/1250, ce qui a été effectué par la CJUE le 16 juillet dernier. Pour plus d'information sur cette affaire, les lecteurs sont invités à se reporter à [33]. Cette affaire montre l'importance accordée à la la protection des DCP des citoyens européens par la Commission européenne, et plus largement par l'UE.

En cas de non respect du RGPD, des sanctions lourdes pouvant aller jusqu'à 20 M€ ou 4% du chiffre d'affaires annuel mondial peuvent être appliquées. En France c'est la CNIL qui est chargée d'appliquer cette règlementation. Ainsi, depuis 2018, date d'entrée en vigueur du RGPD, plusieurs sanctions ont été prononcées par la CNIL, notamment celle de Google LLC le 21 janvier 2019 de 50M€ pour manque de transparence, information insatisfaisante et absence de consentement valable pour la personnalisation de la publicité [31].

2.5 Conclusion

Ce chapitre a présenté les rôles des *smart grids* dans la transition écologique, ainsi que les risques sur la vie privée des consommateurs dans les services énergétiques. Après avoir introduit les *smart grids*, la courbe de charge et les services les exploitant, ce chapitre a présenté les problèmes de vie privée relatifs à la collecte de la courbe de charge des foyers. Ce chapitre a montré que la courbe de charge est une DCP et doit donc être protégée. La règlementation en vigueur (ICS, RGPD) qui encadre le traitement des courbes de charge est aussi présentée dans ce chapitre.

Étant donné que la courbe de charge utilisée dans les services énergétiques permet d'identifier directement ou indirectement les habitants d'un foyer, cette thèse cherche à fournir des services énergétiques mais sans collecter les DCP des clients notamment la courbe de charge.

Chapitre 3

État de l'art

Dans le chapitre précédent, nous avons vu l'importance de l'utilisation des courbes de charge des clients nécessaire dans l'implémentation des nouveaux services énergétiques. Cependant ces courbes de charge révèlent des informations sur la vie privée des clients et doivent donc être protégées.

La littérature utilise de nombreuses techniques de protection de la vie privée pour proposer des services préservant la vie privée : cryptographie homomorphe, calcul multipartite sécurisé ou SMC (*Secure Multi-party Computation*), confidentialité différentielle ou DP (*Differential Privacy*).

La section 3.1 décrit ces technologies de protection de la vie privée utilisées dans le domaine de l'énergie. La section 3.2 décrit ensuite l'application de ces technologies pour les services énergétiques.

3.1 Technologies de protection de la vie privée

Les technologies de protection de la vie privée encore appelées PETs (*Privacy-Enhancing Technologies*) permettent d'effectuer des traitements sur de données sécrètes sans jamais les révéler. Cette section présente trois principales PETs utilisées pour les services énergétiques : le chiffrement homomorphe, le SMC et la DP.

3.1.1 Cryptographie homomorphe

La cryptographie homomorphe permet d'effectuer des traitements sur des données chiffrées, sans que la personne effectuant le traitement ne prenne connaissance des données [68, 124]. Il existe principalement trois types de chiffrement homomorphe :

1. Le chiffrement partiellement homomorphe, PHE (*Partially Homomorphic Encryption*), qui permet d'effectuer un seul type d'opérations (addition ou multiplication) sur les chiffrés. Par exemple RSA [132] et El Gamal [54] supportent la multiplication de chiffrés, tandis que Paillier [124] supporte l'addition de chiffrés.

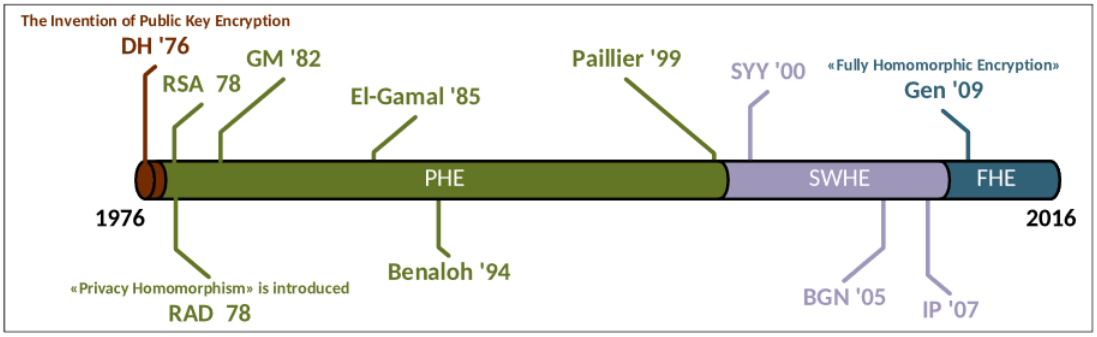


FIGURE 3.1 – Historique de schémas de chiffrement homomorphe, tiré de [1]

2. Le chiffrement totalement homomorphe, FHE (*Fully Homomorphic Encryption*), qui permet d'effectuer plusieurs types d'opérations (addition et multiplication) et donc d'évaluer des circuits booléens sur des données chiffrées sans jamais les déchiffrer. On peut par exemple citer le chiffrement de Gentry [68]. Cependant, ce chiffrement est coûteux en temps de calcul.
3. Le chiffrement quelque peu homomorphe, SWHE (*Somewhat Homomorphic Encryption*), permettant d'effectuer l'addition et la multiplication sur les chiffrés mais en limitant le nombre d'opérations. Par exemple Boneh et al. [18] présentent un cryptosystème supportant l'addition et au plus une multiplication sur les données chiffrées. Le SWHE est un compromis entre le PHE qui supporte un seul type d'opération et le FHE qui est très coûteux en temps de calcul.

Acar et coll. [1] présentent l'évolution des algorithmes de chiffrement homomorphe (PHE, SWHE, FHE), ainsi que leur implémentation. La figure 3.1 présente l'historique de schémas de chiffrement homomorphe, tiré de [1].

Dans les schémas de FHE, le chiffrement est associé à un bruit, et l'évaluation d'une porte AND ajoute ce bruit. Cependant si pendant le déchiffrement du résultat final, le bruit dépasse un certain seuil, alors le résultat sera erroné. Pour résoudre ce problème, Gentry a introduit le *bootstrapping* permettant de réduire le bruit dans les chiffrés et donc de déchiffrer le résultat final de la fonction calculée. Cependant cette opération de *bootstrapping* est couteuse dans la pratique [46, 69], et doit donc être effectuée le moins possible.

Benhamouda et coll. [16] présentent un algorithme permettant de réduire le nombre d'opérations de *bootstrapping* dans un circuit, en fonction du seuil du bruit.

Brakerski et coll. [21] proposent le *leveled*-FHE permettant d'évaluer des circuits (dont la profondeur est connue à l'avance) sans utiliser le processus de *bootstrapping*. Ce schéma obtient de meilleure performance comme le montrent Acar et coll. [1]. D'autres mécanismes de FHE sont présentés en [1].

Le FHE est utilisé dans la pratique, par exemple par Chen et al. [26] pour entrainer des modèles de régressions logistique sur des données génomiques chiffrées. Les données sont chiffrées homomorphiquement côté client puis envoyées dans le cloud. Le gestionnaire

du cloud applique un algorithme d'entrainement sur ces données chiffrées et obtient un modèle logistique chiffré. Le résultat est déchiffré par le client sans que ni ses données, ni le modèle obtenu ne soient divulgués. Les auteurs montrent la faisabilité de ce cas d'usage mais avec une complexité calculatoire très élevée. En effet, en utilisant un PC haut de gamme [1], l'entrainement de leur algorithme sur les données chiffrées prend 115,33 h en utilisant un seul *thread*, tandis que ce calcul s'éxécute en moins d'une seconde en utilisant Matlab.

Bien que les technologies aient évolué depuis, la cryptographie totalement homomorphe ne semble toujours pas être utilisable sur des cas d'usages complexes et réalistes. La cryptographie partiellement homomorphe (PHE), moins couteuse, est souvent privilégiée quand elle peut être utilisée, c'est-à-dire quand les calculs effectués ne nécessitent pas de la somme et de la multiplication sur les chiffrés. Par exemple, la section 3.2.3 montre comment calculer de manière sécurisé, une agrégation de consommation des clients sans révéler les consommations individuelles des foyers, en utilisant du PHE. L'algorithme de PHE principalement utilisé dans l'état de l'art, pour calculer des agrégations de consommations est celui de Paillier [124].

En outre, le modèle de fonctionnement de la cryptographie homomorphe, où un client chiffre ses données, les envoie à un fournisseur qui exécute son traitement et renvoie le résultat chiffré au client, n'est pas adapté à tous les traitements. Par exemple, les algorithmes d'effacement demandent de combiner les consommations de tous les clients. La cryptographie homomorphe ne permet pas de combiner ces données en les chiffrant avec des clés différentes. Cette technologie n'est donc pas adaptée à la protection du GEEQ (Gestionnaire d'Énergie de l'Éco-Quartier), présenté en section 4.1.2.

3.1.2 Partage de secret et calcul multipartite sécurisé (SMC)

Le SMC permet à plusieurs parties de calculer conjointement une fonction sans révéler les entrées individuelles. Cette technique requiert des échanges de données entre les différentes parties. Contrairement à la cryptographie homomorphe, la complexité calculatoire du SMC est négligeable, la complexité du SMC est comptée en nombre de communications entre les parties. Le SMC repose généralement sur du partage de secret, qui permet à une partie de « partager » une valeur secrète auprès de plusieurs autres parties. Le secret ne peut ensuite être reconstitué que si un certain nombre de parties collaborent. Le principe du SMC est le suivant : chaque partie partage sa valeur secrète avec d'autres parties et, à partir des valeurs partagées, les parties calculent conjointement la fonction prédéterminée. La figure 3.2 présente le principe du SMC : les parties partagent leurs valeurs secrètes a, b, et ainsi de suite. Elles peuvent ensuite évaluer des fonctions, à partir des parts, avant de finalement révéler le résultat final.

Le SMC comporte deux phases : une phase hors ligne ou *preprocessing*, et une phase en ligne ou *online*. La phase hors ligne consiste à générer des valeurs partagées entre les parties. Ces valeurs partagées sont utilisées dans la phase en ligne pour calculer des fonctions prédéfinies. La méthode de SMC présentée ici a été proposée par Damgård et coll. [37].

1. Plus précisément, processeur Intel(R) Xeon(R) CPU E3-1280 v5 ©3,70 GHz avec 16 GB de RAM

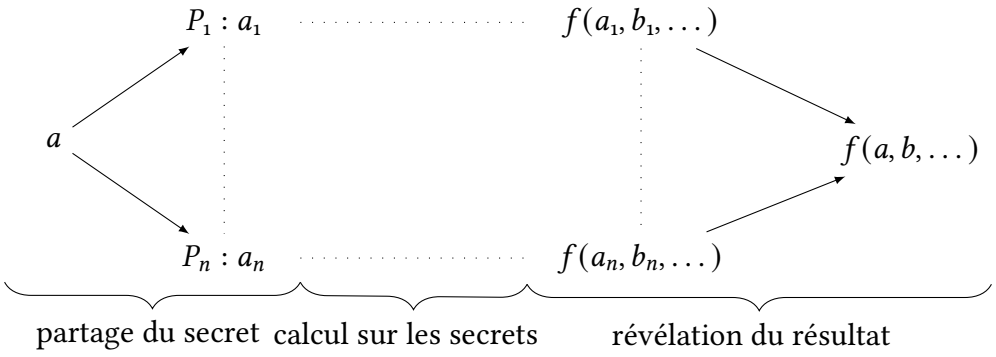


FIGURE 3.2 – Principes du SMC reposant sur le partage de secret. Les valeurs secrètes sont partagées auprès des n parties $P_1, \dots, P_n$, ce qui permet de calculer $f(a, b, \dots)$ sans révéler directement les valeurs $a, b, \dots$

Phase hors-ligne ou de *preprocessing*

Dans [37], la phase hors-ligne utilise une adaptation du SWHE proposé par Brakerski et coll. [22]. Cette adaptation supporte un grand nombre d'addition sur les chiffrés et une seule multiplication sur les chiffrés. La première étape de la phase hors-ligne est une phase d'initialisation qui consiste à générer un couple clé publique, clé privée noté (pk, sk). La clé publique (pk) est envoyée à toutes les parties. La clé privée sk est partagée entre toutes les parties de telle sorte que chaque partie possède une part sk_i de cette clé pour tout $i = 1, \dots, n$ et n le nombre de parties. On note $\text{Enc}_{\text{pk}}(m)$ la fonction de chiffrement, qui prend en entrée un message m, la clé publique pk et renvoie un chiffré. Ce chiffrement est homomorphique de telle sorte que $\text{Enc}_{\text{pk}}(m_1) + \cdots + \text{Enc}_{\text{pk}}(m_n) = \text{Enc}_{\text{pk}}(m_1 + \cdots + m_n)$ et $\text{Enc}_{\text{pk}}(m_1) \times \text{Enc}_{\text{pk}}(m_2) = \text{Enc}_{\text{pk}}(m_1 \times m_n)$. La fonction de déchiffrement notée $\text{Dec}_{\text{sk}}(c)$ prend en entrée un chiffré c et la clé privée sk et renvoie le clair de c. On a $\text{Dec}_{\text{sk}}(\text{Enc}_{\text{pk}}(m)) = m$. Le déchiffrement s'effectue de manière collaborative et utilise chaque part sk_i détenue par chaque partie. Cette fonction est détaillée dans [37].

Dans la suite, on note $e_m = \text{Enc}_{\text{pk}}(m)$ le chiffré de m en utilisant la clé publique pk. Tous les nombres utilisés ci-dessous appartiennent au corps $\mathbb{F}_{p^k}$ avec p premier et k entier

La phase hors-ligne utilise trois principaux protocoles : *Reshare*, *PBracket* et *PAngle* définis respectivement dans les algorithmes 1, 2 et 3.

L'algorithme 1 permet de partager un secret m, avec des parties, à partir du chiffré e_m avec la clé pk de ce secret. À la fin de cet algorithme, chaque partie P_i possède une part m_i du secret m, pour $i = 1, \dots, n$.

La représentation $[\![v]\!]$ en utilisant l'algorithme 2 garantit que pour tout $i = 1, \dots, n$,

$$v\beta_i = \sum_{j=1}^{n} \gamma_i^j \tag{3.1}$$

avec $v = v_1 + \cdots, v_n$

Algorithme 1 Reshare : permet de partager $m \in \mathbb{F}_{p^k}$, à partir du chiffré $e_m = \mathrm{Enc}_{\mathrm{pk}}(m)$

Utilisation : prend en entrée un chiffré e_m obtenu, avec la clé pk, d'un message m. Cette fonction retourne la part m_i de m à chaque partie, pour tout $i = 1, \ldots, n$ tel que $\sum_{i=1}^{n} m_i = m$.

protocole :

1. Chaque partie P_i ($i = 1, \ldots, n$) génère un nombre f_i et envoie le chiffré e_{f_i} (en utilisant la clé pk) aux autres parties.
2. Chaque partie calcule $e_f = e_{f_1} + \cdots + e_{f_n}$ et $e_{f+m} = e_f + e_m$
3. Les parties demandent le déchiffrement de e_{f+m} en utilisant la fonction de déchiffrement collaborative.
4. La partie P_1 calcule $m_1 = m + f - f_1$, et les autres parties P_i ($i \neq 1$) définissent $m_i = -f_i$

Algorithme 2 PBracket : génération de $[\![v]\!]$

Utilisation : Prend en entrées les parts $v_1, \ldots, v_n$ détenues par les parties (la partie P_i détient la part v_i, pour tout $i = 1, \ldots, n$), et le chiffré e_v, et génère $[\![v]\!]$. On suppose que $\sum_{i=1}^{n} v_i$ est le clair du chiffré e_v. Ce protocole utilise e_{β_i} le chiffré de β_i qui est généré pendant la processus d'initialisation, et connu de toutes les parties (Algorithme 4).

Protocole :

1. pour tout $i = 1, \ldots, n$
   (a) Chaque partie P_i calcule $e_{\gamma_i} = e_{\beta_i} \times e_v$.
   (b) Les parties génèrent $(\gamma_i^1, \ldots, \gamma_i^n) = \mathrm{Reshare}(e_{\gamma_i})$, ainsi chaque partie P_j ($j = 1, \ldots, n$) obtient la part γ_i^j de $v \cdot \beta_i$.
2. le protocole renvoie la représentation $[\![v]\!] = (v_1, \ldots, v_n, (\beta_i, \gamma_1^i, \ldots, \gamma_n^i)_{i=1,\ldots,n})$. Cette représentation signifie que chaque partie P_i possède $v_i, \beta_i, \gamma_1^i, \ldots, \gamma_n^i$ pour $i = 1, \ldots, n$

Pour $i = 1, \ldots, n$, la somme $\sum_{j=1}^{n} \gamma_i^j$ est le MAC (*Message Authentication Code*) permettant d'authentifier v via la clé secrète β_i de la partie P_i générée pendant la phase hors-ligne (Algorithme 4)

On note δ la première composante de $\langle v \rangle$ initialisée à 0. La représentation $\langle v \rangle$ garantit l'égalité suivante :

$$\alpha(v + \delta) = \sum_{i=1}^{n} \gamma_i \tag{3.2}$$

$\gamma_1 + \cdots + \gamma_n$ est le MAC permettant d'authentifier v et α une clé partagée générée pendant la phase hors-ligne (Algorithme 4). Pour plus de précision, on note $\gamma(v) = \gamma(v)_1 + \cdots + \gamma(v)_n$ le MAC permettant d'authentifier v. La valeur δ permet de garantir l'égalité de l'équation (3.2) pendant la phase en ligne (section 3.1.2), en additionnant une valeur partagée et un nombre publique.

Algorithme 3 PAngle : génération de $\langle v \rangle$

Utilisation : Prend en entrées les parts $v_1, \ldots, v_n$ détenues par les parties (la partie P_i détient la part v_i, pour tout $i = 1, \ldots, n$), et le chiffré e_v, et génère $\langle v \rangle$. On suppose que $\sum_{i=1}^{n} v_i$ est le clair du chiffré e_v. Ce protocole utilise e_α le chiffré de α avec la clé pk, généré pendant la processus d'initialisation, et connu de toutes les parties (Algorithme 4).
Protocole :

1. Toutes les parties calculent $e_{v \cdot \alpha} = e_v \times e_\alpha$.
2. Les parties génèrent $(\gamma_1, \ldots, \gamma_n) = \text{Reshare}(e_{v \cdot \alpha})$,ainsi chaque partie P_i obtient la part γ_i de $\alpha \cdot v$.
3. Le protocole renvoie la représentation $\langle v \rangle = (0, (v_1, \ldots, v_n), (\gamma_1, \ldots, \gamma_n))$. Cette représentation signifie que chaque partie P_i possède v_i, γ_i pour $i = 1, \ldots, n$.

Les protocoles Reshare, PBracket et PAngle sont des briques de base de la phase hors-ligne. Ces protocoles permettent notamment de générer des nombres aléatoires, ou des triplets $\langle a \rangle, \langle b \rangle, \langle c \rangle$ tels que $c = ab$. Ces derniers sont utilisés dans la phase en ligne permettant de réaliser la multiplication de secrets partagés. L'algorithme 4 détaille la phase hors-ligne.

L'étape d'initialisation de l'algorithme 4 consiste à générer la clé partagée α entre toutes les parties, et les clés individuelles β_i de chaque partie P_i pour $i = 1, \ldots, n$. La représentation $[\![\alpha]\!]$ permet d'authentifier la clé partagée α via les clés individuelles β_i pour $i = 1, \ldots, n$, comme le montre l'équation 3.1.

Phase en ligne

La phase en ligne permet d'effectuer des calculs sur les valeurs partagées et est divisée en trois sous-étapes, comme l'indique la figure 3.2 : partage du secret, calcul sur les secrets partagés, et révélation du résultat final. Cette phase utilise la clé globale partagée $[\![\alpha]\!]$, les paires $[\![r]\!], \langle r \rangle$, et les triplets $\langle a \rangle, \langle b \rangle, \langle c \rangle$ générés dans la phase hors-ligne.

Partage du secret Pour partager un secret x_i de la partie P_i, la partie P_i demande une paire $[\![r]\!], \langle r \rangle$ générée pendant la phase hors ligne puis exécute les étapes suivantes :

1. P_i demande le déchiffrement de $[\![r]\!]$ de telle sorte que r soit connu uniquement de P_i.
2. P_i calcule $e = x_i - r$ et envoie le résultat à toutes les autres parties.
3. Les parties calculent $\langle x_i \rangle = \langle r \rangle + e = (\delta - e, (r_1 + e, r_2, \ldots, r_n), (\gamma(r)_1, \ldots, \gamma(r)_n))$

Ainsi il est facile de remarquer que $r_1 + e + r_2 + \cdots + r_n = r + e = r + x_i - r = x_i$.
De plus, $\alpha(x_i + \delta - e) = \alpha(x_i + \delta - x_i + r) = \alpha(\delta + r) = \gamma(r)_1 + \cdots + \gamma(r)_n$ d'après le partage de r (équation (3.2)). Ainsi, la consommation x_i est bien authentifiée par le MAC $\gamma(r) = \gamma(r)_1 + \cdots + \gamma(r)_n$.

Calcul sur les secrets partagés À partir du partage de plusieurs secrets représentés, il est possible de calculer des combinaisons linéaires. Soient $\langle x \rangle = (\delta_x, (x_1, \ldots, x_n), (\gamma(x)_1, \ldots, \gamma(x)_n))$

et $\langle y \rangle = (\delta_y, (y_1, \ldots, y_n), (\gamma(y)_1, \cdots, \gamma(y)_n))$ deux secrets partagés et λ une constante publique. D'après l'équation (3.2), on a respectivement $\alpha(x + \delta_x) = \gamma(x)_1 + \cdots, \gamma(x)_n$ et $\alpha(y + \delta_y) = \gamma(y)_1 + \cdots, \gamma(y)_n$, avec $x = \sum_{i=1}^{n} x_i$ et $y = \sum_{i=1}^{n} y_i$. La somme $\langle x \rangle + \langle y \rangle$ est égale au partage de la somme :

$$\begin{aligned}\langle x \rangle + \langle y \rangle &= (\delta_x + \delta_y, (x_1 + y_1, \ldots, x_n + y_n), (\gamma(x)_1 + \gamma(y)_1, \cdots, \gamma(x)_n + \gamma(y)_n)) \\ &= \langle x + y \rangle.\end{aligned}$$

Avec,

$$\begin{aligned}\alpha(\delta_x + \delta_y + x + y) &= \alpha(\delta_x + x) + \alpha(\delta_y + y) \\ &= \gamma(x)_1 + \cdots, \gamma(x)_n + \gamma(y)_1 + \cdots, \gamma(y)_n\end{aligned}$$

l'égalite du MAC est donc vérifiée.

Par conséquent, pour calculer $\langle x + y \rangle$, chaque partie P_i ($1 \leq i \leq n$) additionne localement ses parts.

Pour calculer $\langle \lambda + x \rangle = (\delta_x - \lambda, (x_1 + \lambda, x_2, \ldots, x_n), (\gamma(x)_1, \cdots, \gamma(x)_n))$, toutes les parties retranchent λ à δ, la partie P_1 (ou une autre partie préalablement déterminée) ajoute λ à sa part x_1 tel que $x + \lambda = x_1 + \lambda + x_2 + \cdots + x_n$.

De même, le produit d'un secret partagé $\langle x \rangle$ avec une constante publique λ est égal au partage du produit :

$$\begin{aligned}\lambda \cdot \langle x \rangle &= (\lambda \cdot \delta, (\lambda \cdot x_1, \ldots, \lambda \cdot x_n), (\lambda \cdot \gamma(x)_1, \cdots, \lambda \cdot \gamma(x)_n)) \\ &= \langle \lambda \cdot x \rangle\end{aligned}$$

On remarque que l'égalité du MAC est préservée (équation 3.2). Par exemple, pour le partage de la multiplication $\langle \lambda \cdot x \rangle$, on a : $\alpha(\lambda \cdot x + \lambda \cdot \delta) = \lambda \cdot \alpha(x + \delta) = \lambda(\gamma(x)_1 + \cdots + \gamma(x)_n)$.

Calculer une combinaison linéaire de secrets partagés se fait donc localement, c'est-à-dire sans communication avec d'autres parties (sans compter la communication initiale liée au partage de secret ou celle liée à la révélation finale). Cependant pour la multiplication de secrets, il est nécessaire de communiquer avec les autres parties.

La multiplication de deux secrets partagés $\langle x \rangle$ et $\langle y \rangle$ nécessite la génération d'un triplet partagé $\langle a \rangle$, $\langle b \rangle$, $\langle c \rangle$, avec $c = a \cdot b$. Ce triplet partagé est généré pendant la phase hors-ligne présentée dans la section 3.1.2.

Pour calculer la multiplication $\langle x \cdot y \rangle$, il faut premièrement calculer et « ouvrir » $\langle x \rangle - \langle a \rangle$ afin d'obtenir e, et $\langle y \rangle - \langle b \rangle$ afin d'obtenir g. On peut donc calculer

$$\begin{aligned}\langle x \rangle \cdot \langle y \rangle &= \langle c \rangle + e \cdot \langle b \rangle + g \cdot \langle a \rangle + e \cdot g \\ &= \langle c \rangle + (x - a) \cdot \langle b \rangle + (y - a) \cdot \langle a \rangle + (x - a) \cdot (y - a) \\ &= \langle x \cdot y \rangle.\end{aligned}$$

Grâce à la multiplication de secrets partagés, il est possible d'évaluer des circuits booléens : en utilisant un protocole de décomposition binaire [122], un entier partagé peut être converti en binaire. L'addition et la multiplication de booléens permettent respectivement d'obtenir les portes XOR et AND. Comme ces deux portes permettent d'obtenir n'importe quelle autre porte logique, cela permet d'évaluer n'importe quel circuit booléen.

Révélation du résultat Après les calculs précédents, chaque partie possède une part du résultat $\langle a \rangle$. Pour révéler le résultat du calcul, chaque partie P_i envoie sa part a_i et $\gamma(a)_i$ au foyer P_1 (ou à une autre partie choisie), qui calcule $a = a_1 + \cdots + a_n$. Pour vérifier que le calcul s'est bien effectué, chaque partie P_i envoie sa part α_i au foyer P_1 permettant de calculer la clé globale $\alpha = \alpha_1 + \cdots + \alpha_n$. Les parties peuvent donc vérifier si $\gamma(a)_1 + \cdots + \gamma(a)_n = \alpha(a + \delta)$. La vérification du MAC s'effectue une seule fois à la fin de tous les calculs [37]. Ce MAC permet de résister aux attaquants byzantins.

Opérations complexes en utilisant le SMC

Avec l'addition et la multiplication, il est possible de calculer des fonctions plus complexes sur des secrets partagés. Par exemple il est possible de calculer des tests d'égalité comme suit :

$$\text{equal}(\langle a \rangle, \langle b \rangle) = 1 - (\langle a \rangle - \langle b \rangle)^{p-1} \tag{3.3}$$

La sortie de equal est $\langle 1 \rangle$ en cas d'égalité et $\langle 0 \rangle$ sinon. En effet, en utilisant le petit théorème de Fermat, pour tout $c \in \mathbb{Z}_p$ avec p premier, $c^{p-1} = 0$ si $c = 0$, et $c^{p-1} = 1$ si $c \neq 0$. Burkhart et coll. [24] ont implémenté equal en $\ell + 1$ multiplications en ℓ tours de communication, avec ℓ la taille binaire de p ($\ell = \lceil \log_2(p) \rceil$). De plus, il est possible de calculer la comparaison *less-than* lessThan($\langle a \rangle, \langle b \rangle$) qui renvoie $\langle 1 \rangle$ si $a \leq b$ et $\langle 0 \rangle$ sinon, en $24\ell + 5$ multiplications en $2\ell + 10$ tours [24].

Pour des questions de simplicité, dans la suite, nous notons un secret partagé de a par $\langle a \rangle = (a_1, \ldots, a_n)$, en ignorant le MAC.

Évolutions du SMC

Le SMC a beaucoup évolué pendant ces dernières années. Après avoir présenté les dernières améliorations dans ce domaine, cette section décrit le fonctionnement du SMC.

Le partage de secret de Shamir permet de calculer des combinaisons linéaires (additions, multiplications par des scalaires, etc.) sur des entrées secrètes sans les révéler [138]. Gennaro et coll. [67] proposent une méthode pour multiplier des valeurs secrètes en utilisant le partage de Shamir. Cette méthode permet de faire des calculs linéaires et non linéaires. Cependant, multiplier des secrets nécessite aux parties de communiquer entre elles.

Bendlin et coll. [15] améliorent la complexité et la sécurité du SMC en utilisant du SWHE et en authentifiant les secrets partagés. Leur protocole utilise une phase de *preprocessing*, qui se fait hors-ligne, et une phase en ligne. La phase en ligne permet d'additionner et de

multiplier des secrets sans communication, et utilise un MAC pour permettre aux parties de vérifier que le calcul s'est effectué correctement. Les multiplications de secrets requièrent des triplets particuliers comme expliqué plus loin, et la phase de *preprocessing* permet entre autres de générer ces triplets.

Damgård et coll. [35] présentent un protocole de décomposition binaire permettant de convertir un secret partagé appartenant à un corps fini $\mathbb{F}_p$ (avec p un nombre premier) en binaire. Cette technique permet d'effectuer des opérations comme des tests d'égalités ou des comparaisons en utilisant du SMC. La comparaison est importante pour la réponse active à la demande : en effet, elle permet de comparer la demande globale de consommation avec la puissance maximale du quartier. Si la demande est supérieure à la puissance maximale du quartier, les foyers sont sollicités pour diminuer leur consommation prévisionnelle.

Nishide et coll. [122] proposent une optimisation du protocole de décomposition binaire de Damgård et coll. [35] ainsi que des nouveaux protocoles pour effectuer des tests d'égalité, des tests d'intervalle (vérifier qu'un nombre appartient à un intervalle) et des comparaisons sans utiliser le protocole de décomposition binaire. Burkhart et coll. [24] optimisent le protocole de comparaison en diminuant le nombre de communications.

Damgård et coll. [37] proposent un protocole de SMC, nommé SPDZ (prononcé « Speedz ») résistant aux attaquants dits « byzantins », c'est-à-dire aux attaquants qui peuvent se comporter arbitrairement. Ce protocole, utilise du SWHE pendant la phase hors ligne et a évolué au cours du temps. Damgård et coll. [36] proposent des améliorations théorique et pratique du SPDZ en améliorant la sécurité de la phase hors-ligne. Keller et coll. [83] présentent une optimisation de SPDZ, appelée MASCOT, en remplaçant le SWHE de la phase hors-ligne par du transfert inconscient (*oblivious transfer* en anglais). Keller et coll. [84] présentent une nouvelle version de SPDZ utilisant SWHE. Leur implémentation est six fois plus rapide que MASCOT sur un LAN (*Local Area Network*) et vingt fois plus rapide sur un WAN (*Wide Area Network*).

Complexité du SMC

Un calcul sur des secrets, en utilisant le SMC, nécessite des communications entre les parties et est donc moins efficace que ce même calcul sur des données connues par un tiers de confiance. Cette perte de performances doit être prise en compte pendant l'élaboration d'algorithmes intégrant du SMC. Le partage d'un secret avec n parties nécessite $(n-1)$ communications. En effet, la partie partageant le secret, génère n parts, envoie $n-1$ parts aux autres parties et garde la dernière part. D'où une complexité en $O(n)$ pour un partage de secret.

Pour révéler un secret partagé, il faut que chaque partie envoie sa part à une partie définie préalablement qui effectuera la somme des parts, ce qui correspond aussi à $n-1$ communications : $O(n)$.

Les opérations telles que l'addition de secrets partagés ou la multiplication d'un secret partagé avec un nombre public se font en local, donc sans communication.

Cependant, la multiplication de deux secrets partagés, nécessite la génération pendant

la phase hors ligne d'un triplet partagé, entre les parties, et la révélation de deux valeurs intermédiaires (les e et g présentées dans la section 3.1.2). La génération d'un triplet se fait en $O(n^2)$ communications. Comme les deux valeurs à révéler sont indépendantes, cette révélation peut se faire en parallèle ou en un tour en n communications, d'où un total de $n + O(n^2)$ communications correspondant à $O(n^2)$.

En utilisant MASCOT [83], dans un réseau local (LAN) où chaque partie possède un PC haut de gamme [2], les parties peuvent générer 4 800 triplets par seconde avec 2 parties, et 1 000 triplets par seconde avec 5 parties.

3.1.3 Confidentialité différentielle

Le SMC présenté dans la section 3.1.2 permet de calculer une fonction en protégeant les entrées. Cependant, la sortie de la fonction reste vulnérable aux attaques de ré-identifications indirectes des entrées. Par exemple, l'attaque de différence [39] consiste à retrouver une entrée en calculant la différence de deux agrégats différents en cette entrée. La DP apporte des garanties formelles, permettant de limiter ce risque de ré-identification indirecte des entrées.

La DP est un *framework* introduit par Dwork en 2006 [48] qui permet de quantifier la garantie de vie privée apportée par une requête sur une base de donnée. Cette requête peut être la publication d'une base de donnée entière, ou une requête plus précise, comme par exemple « quelle est la consommation énergétique moyenne des usagers dans cette base de donnée ? »

La DP a beaucoup évolué au cours du temps [127] et a été adopté par plusieurs organisations comme le bureau du recensement des États-Unis [66], Google [60], Apple [42], ou encore Microsoft [45]. La définition formelle de la DP repose sur la notion de *distance* entre deux bases de données.

Définition 3.1.1 *(Distance entre deux bases de données)*
Soit $\mathcal{D}$ un format de bases de données, c'est-à-dire les attributs de ces bases de données. Alors, soit

$$\begin{array}{rccc} d & : & \mathcal{D} \times \mathcal{D} & \to & \mathbb{N} \\ & & (D_1, D_2) & \mapsto & d(D_1, D_2) \end{array}$$

le nombre minimal d'opérations qui permettent de passer de D_2 à D_1, où les opérations peuvent être la modification d'un enregistrement, la suppression d'un enregistrement, ou l'insertion d'un enregistrement.

La fonction d est une distance. Cette fonction mesure le nombre d'enregistrements qui diffèrent entre les bases de données D_1 et D_2.

Une requête sur des bases de données est dite différentiellement confidentielle si cette requête rend des bases de données proches presque indistinguables en regardant uniquement la sortie de la requête. La DP repose sur un paramètre, noté ϵ, qui est appelé le *budget de*

2. Plus précisément un processeur Intel i7 à 8 cœurs à 3,1 GHz et 32 Go de RAM.

privacy. La définition formelle d'une requête différentiellement confidentielle est alors donnée de la manière suivante.

Définition 3.1.2 *Une requête $f : \mathcal{D} \to \mathfrak{S}$ est* $\epsilon-$différentiellement confidentielle, *avec $\mathfrak{S}$ l'image de f si et seulement si pour toutes bases de données D_1 et D_2 telles que $d(D_1, D_2) \leq 1$, et pour tous les sous-ensembles $S \subset \mathfrak{S}$,*

$$\Pr\big(f(D_1) \in S\big) \leq \exp(\epsilon) \Pr\big(f(D_2) \in S\big).$$

Cette définition peut s'appliquer non seulement à des requêtes sur des bases de données, mais à n'importe quelle fonction, en considérant le domaine de la fonction comme un format de base de données.

Dwork propose également le mécanisme de Laplace, qui permet de faire en sorte que n'importe quelle fonction à valeur réelle garantisse la ϵ-DP [47]. Ce mécanisme repose sur la notion de *sensibilité* d'une fonction, qui représente l'influence qu'un enregistrement de la base de donnée (ou qu'une entrée de la fonction) a sur le résultat de la requête (ou de la fonction).

Définition 3.1.3 *(Sensibilité)*
Soit $f : \mathcal{D} \to \mathbb{R}^d$ une fonction, alors la sensibilité de f est donnée par

$$\Delta_1(f) = \max_{D_1, D_2 \in \mathcal{D} \text{ t.q. } d(D_1, D_2) \leq 1} \|f(D_1) - f(D_2)\|_1.$$

Par exemple, si la fonction f calcule la somme des consommations des utilisateurs dans la base de données D pendant T pas de temps, alors la sensibilité de f est la plus grande consommation de la base de données D multiplié par T. Cette sensibilité est aussi appelée L_1-sensibilité due à la norme 1. Similairement, la L_2-sensibilité noté Δ_2 est calculée de la même manière en remplaçant la norme 1 par la norme 2. Cette sensibilité sera utilisée plus tard dans le chapitre 5.

Définition 3.1.4 *(L_2-sensibilité)*
Soit $f : \mathcal{D} \to \mathbb{R}^d$ une fonction, alors la L_2-sensibilité de f est donnée par

$$\Delta_2(f) = \max_{D_1, D_2 \in \mathcal{D} \text{ t.q. } d(D_1, D_2) \leq 1} \|f(D_1) - f(D_2)\|_2.$$

La norme 1 et la norme 2 d'une série $S = (s_1, \ldots, s_T)$ sont égales respectivement à $\|S\|_1 = \sum_{i=1}^{T} |s_i|$ et $\|S\|_1 = \sum_{i=1}^{T} s_i^2$.

Le mécanisme de Laplace consiste à ajouter une valeur aléatoire suivant la distribution de Laplace, paramétrée par la sensibilité de la fonction et le budget de *privacy* ϵ désiré.

Théorème 3.1.1 *Pour toute fonction $f : \mathcal{D} \to \mathbb{R}^d$, la fonction*

$$\hat{f}(D) = f(D) + (\mathcal{L}_1(\Delta_1(f)/\epsilon), \ldots, \mathcal{L}_d(\Delta_1(f)/\epsilon))$$

*est $\epsilon-$*différentiellement confidentielle, *où $\mathcal{L}(\cdot)$ est la distribution de Laplace et $\Delta_1(f)$ est la sensibilité de f.*

C'est-à-dire que toute fonction à valeur réelle $f(x_1, \ldots, x_n)$ peut être rendue $\epsilon-$différentiellement confidentielle en y ajoutant un bruit aléatoire suivant la distribution $\mathcal{L}(\Delta_1(f)/\epsilon)$.

En outre, il est intéressant de noter que la distribution de Laplace $\mathcal{L}(\cdot)$ est divisible : à partir de plusieurs valeurs aléatoires suivant la distribution de Gamma, il est possible d'obtenir une valeur aléatoire suivant la distribution de Laplace, comme l'explique le Lemme 3.1.1. Cette propriété est utile pour combiner la DP et le SMC. Cette technique est notamment utilisée par Ács et Castelluccia [3], comme expliqué en section 3.2.

Lemme 3.1.1 *(Divisibilité de la distribution de Laplace [86])*
Soit $\mathcal{L}(\lambda)$ une variable aléatoire ayant une distribution de Laplace, c'est-à-dire une fonction de densité de probabilité

$$f(x, \lambda) = \frac{1}{2\lambda} e^{\frac{|x|}{\lambda}}.$$

Alors, pour tout entier $n \geq 1$, $\mathcal{L}(\lambda) = \sum_{i=1}^{n} [\mathcal{G}_1(n, \lambda) - \mathcal{G}_2(n, \lambda)]$,[3] où $\mathcal{G}_1(n, \lambda)$ et $\mathcal{G}_2(n, \lambda)$ sont des variables aléatoires indépendantes et identiquement distribuées, suivant la distribution de Gamma de paramètres $\frac{1}{n}$ et $\frac{1}{\lambda}$, c'est-à-dire avec une fonction de densité de probabilité

$$g(y, \frac{1}{n}, \frac{1}{\lambda}) = \frac{(1/\lambda)^{1/n}}{\Gamma(1/n)} y^{\frac{1}{n}-1} e^{-y/\lambda} \text{ pour } y \geq 0.$$

La DP introduit du bruit afin de protéger la vie privée. Ce bruit peut diminuer l'efficacité de la fonction. Cette perte d'efficacité peut être mesurée en utilisant l'erreur relative, définie comme suit.

Définition 3.1.5 *(Erreur relative)*
L'erreur relative entre a et b, avec $a \neq 0$, est définie par

$$\frac{|a - b|}{a}.$$

Soit $D = (x_1, \cdots, x_n)$, et $\hat{f}(D) = f(D) + \mathcal{L}(\Delta(f)/\epsilon)$ la fonction perturbée de $f(D)$. L'utilité de $\hat{f}(D)$ peut être quantifiée, si $f(D) \neq 0$, par l'erreur relative entre $f(D)$ et $\hat{f}(D)$:

$$\delta = \frac{|f(D) - \hat{f}(D)|}{f(D)} = \frac{|\mathcal{L}(\Delta(f)/\epsilon)|}{f(D)}. \tag{3.4}$$

L'erreur relative δ dépend de la sensibilité de f et du budget de *privacy* ϵ. C'est pourquoi, lorsqu'on applique le mécanisme de Laplace à une fonction, il est nécessaire de considérer le compromis entre l'utilité nécessaire pour pouvoir exploiter la fonction, et entre le niveau de protection qui doit être garanti. Plus ϵ est petit, meilleure est la protection mais l'utilité est plus dégradée.

En outre, le calcul de plusieurs mécanismes qui garantissent la confidentialité différentielle, garantit aussi la confidentialité différentielle. Cependant, si les données utilisées sont corrélées, le budget ϵ total de l'ensemble des résultats est égal à la somme des budgets de tous les mécanismes, comme le montre le théorème 3.1.2.

3. Cette notation abusive indique l'égalité des distributions.

Théorème 3.1.2 *(Mécanisme de composition)*
Soit $f_i : \mathcal{D} \to \mathfrak{S}$, ϵ_i-différentiellement confidentielle, pour tout $i = 1, \ldots, k$. Alors la fonction $f : \mathcal{D} \to \prod_{i=1}^{k} \mathfrak{S}$ définie par $f(x) = (f_1(x), \ldots, f_k(x))$ est $\sum_{i=1}^{k} \epsilon_i-$différentiellement confidentielle

Ainsi, il faut faire attention dans le choix de la valeur ϵ lors de plusieurs publications de jeu de données garantissant la confidentialité différentielle.

Le choix du budget de privacy ϵ

Choisir le bon ϵ est complexe. Dans la littérature, des chercheurs pensent que le choix de ϵ devrait être relatif, parce que pour une même valeur ϵ, la probabilité de ré-identification d'un participant est dépendante du contexte. Lee et Clifton [88] proposent une technique permettant de choisir ϵ en fonction du cas d'usage. Ils proposent de calculer ϵ en utilisant la formule suivante :

$$\epsilon = \frac{\Delta_1(f)}{\Delta v} \ln \frac{(n-1)p}{1-p} \tag{3.5}$$

avec $\Delta_1(f)$ la sensibilité de la fonction, Δv la distance maximale entre les réponses possibles de la fonction à protéger, p la probabilité d'identification de la présence d'un individu, et n le nombre de participants dans le jeu de données. Par exemple, pour publier le nombre de personne atteinte du diabète dans une base de données de 50 personnes, en considérant une probabilité d'identification d'une personne de 1/10, il est suggéré d'avoir :

$$\epsilon \leq \frac{1}{1} \ln \frac{49 \times 10}{9 \times 10} = 1{,}69$$

Dans cet exemple, en utilisant un budget de 1,69 un attaquant à une probabilité de $\frac{1}{10}$ de retrouver si une personne dans la base de données est atteinte du diabète. En utilisant un probabilité d'identification de 3%, on obtient $\epsilon = 0{,}41$.

Lee et Clifton [88] montrent que le choix du budget de privacy ϵ dépend du domaine de la fonction à protéger, mais aussi de la fonction elle même. En effet, la sensibilité de la fonction dépend du domaine, et la distance maximale entre les réponses possibles Δv dépend de la fonction à protéger. Dans [88], les auteurs montrent par exemple que pour une même probabilité de ré-identification, le budget ϵ utilisé pour publier une moyenne est différent de celui utilisé pour la publication d'une médiane.

3.1.4 Bilan des technologies de protection présentées

Dans la section 3.1, nous avons présenté trois technologies de protection de la vie privée : le chiffrement homomorphe, le SMC (*Secure Multi-party Computation*) et la DP (*Differential Privacy*).

Le chiffrement homomorphe permet d'effectuer des opérations sur des entrées chiffrées (par une même clé de chiffrement) sans l'intervention du détenteur de la clé privée. Le résultat

des opérations est connu uniquement de celui qui possède la clé privée de déchiffrement. Cette technologie peut être utilisée pour calculer un agrégat de données d'un utilisateur. Par exemple, il peut être utilisé par un fournisseur pour calculer la facture d'électricité de ses clients pendant une tranche horaire sans connaitre leur consommation individuelle. Pour ce faire, pour chaque pas de temps, un client chiffre sa consommation avec sa clé publique et l'envoie au fournisseur, celui-ci peut donc multiplier la consommation chiffrée par le prix du kWh correspondant au pas de temps choisi, et envoyer le résultat au client. En déchiffrant le résultat, le client obtient le montant consommé pendant le pas de temps considéré.

Cependant le chiffrement homomorphe ne peut pas être utilisé pour manipuler les données chiffrées avec des clés de chiffrement différentes. De plus, effectuer des opérations complexes (multiplications et additions) sur des chiffrés prend encore beaucoup de temps.

Le SMC permet de calculer une fonction sans révéler les données d'entrée. Cette technologie est basée sur le partage de secret. Chaque partie partage son secret avec les autres parties, ce qui permet de calculer conjointement, de manière distribuée, le résultat de la fonction prédéfinie, sans rien apprendre des secrets partagés. Par exemple, le SMC peut être utilisé pour calculer la somme de consommation des habitants d'un quartier sans révéler les consommations individuelles des foyers. Cependant cette technologie requiert de communiquer avec les parties prenant part au calcul.

Un agrégat peut faire fuiter indirectement les données individuelles ayant permis de le calculer. La DP apporte des garanties formelles limitant ces fuites de données, en ajoutant un bruit sur l'agrégat. Cette technique peut être utilisée par exemple pour publier un histogramme, publier un agrégat de courbes de charge en garantissant que l'agrégat ne révèle pas indirectement des informations sur les courbes de charge individuelles. Cependant, cette technologie peut rendre l'agrégat publié inutilisable, si la perturbation introduite entraine une grande différence entre l'agrégat initial et celui bruité.

3.2 Application des PET à l'énergie

Les technologies de protection de la vie privée, ou PET, présentées dans la section 3.1 permettent de mettre en œuvre des services énergétiques tout en préservant la vie privée des foyers. Cette section présente plusieurs applications pour le domaine de l'énergie.

La première application présentée cherche à éviter des attaques NALM (*Non-Intrusive Appliance Load Monitoring*), en utilisant des batteries, ou en implémentant la DP. Ensuite, nous présentons des techniques de pseudonymisation, permettant d'envoyer uniquement les courbes de charge des foyers au fournisseur, sans envoyer des éléments identifiant un foyer. La troisième application consiste à calculer des agrégations sécurisées de courbes de charge, en utilisant du PHE ou du SMC. Ces agrégations permettent de calculer par exemple la consommation moyenne dans un quartier sans avoir accès aux courbes de charge individuelles des foyers. La section 3.2.4 présente des techniques de publication de séries temporelles en utilisant la DP. Finalement, la section 3.2.5 étudie des services de DR (*Demand Response*) respectueuses de la vie privée.

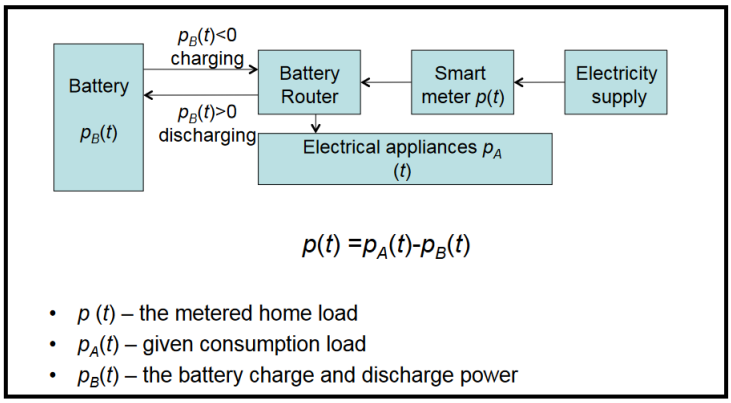


FIGURE 3.3 – Modèle d'utilisation de la batterie dans la consommation d'un foyer, tiré de [82]

3.2.1 Protection contre le NALM : utilisation des batteries

Kalogridis et coll. [82] proposent d'utiliser des batteries afin d'éviter de connaitre les appareils qui sont utilisés dans un foyer à partir de la courbe de charge, en utilisant le NALM. Trois scénarios sont étudiés : le premier consiste à utiliser la puissance disponible de la batterie pour faire fonctionner les appareils de la maison, et ensuite recharger la batterie en utilisant de l'énergie produite par le fournisseur. Ce scénario permet de masquer les signatures des appareils utilisés. Le deuxième scénario permet d'utiliser à la fois la puissance des batteries et l'énergie produite par le fournisseur, pour faire fonctionner les appareils du foyer. Ce scénario permet d'obtenir une courbe de charge globale plus lisse que celle des appareils utilisés, et masque donc l'usage des appareils. La dernière stratégie consiste à offusquer la signature de l'appareil utilisée en restituant l'énergie consommée par la batterie par une série de recharges. Ainsi, à partir de la courbe de charge on ne peut pas déterminer le pic correspondant à l'utilisation de l'appareil.

Cependant, l'utilisation de batteries peut causer une augmentation de la consommation, et donc de la facture d'électricité. En effet, les auteurs proposent un algorithme permettant d'avoir une consommation constante dans le foyer. Pour cela, ils proposent d'une part de charger des batteries quand la consommation des appareils est faible, afin d'atteindre le seuil de consommation fixé. D'autre part, les batteries seront déchargées (ou utilisées), lorsque la demande d'énergie des appareils du foyer sera supérieure au seuil fixé.

Formellement, soit $p_A(t)$ la consommation des appareils du foyer à l'instant t et $p_B(t)$ la puissance produite par la batterie à l'instant t. La courbe de charge mesurée par le compteur à l'instant t est $p(t) = p_A(t) - p_B(t)$ comme le montre la figure 3.3.

La protection de l'algorithme de Kalogridis et coll. [82] consiste à faire varier la puissance $P_B(t)$ fournie par la batterie de telle sorte qu'à partir de la courbe de charge $p(t)$ on ne peut pas tirer des informations sur la consommation $p_A(t)$ des appareils du foyer.

Pour quantifier le niveau de protection de leur algorithme, les auteurs utilisent trois métriques : l'entropie relative ou la distance de Kullback-Leibler [34], la classification, et

l'analyse de la régression.

L'entropie relative permet de comparer deux sources d'information ($p(t)$ et $p_A(t)$), et donc de déterminer si la courbe de charge globale du foyer peut permettre de révéler la signature d'un appareil précis. La classification quant à elle permet de déterminer à quel point la courbe de charge d'un appareil est proche de celle du foyer, et ainsi permet de déterminer si la courbe de charge du foyer peut révéler la signature des appareils utilisés. La dernière métrique utilisée est la régression linéaire permettant de calculer le degré de prédiction de la courbe de charge $p(t)$ à partir de la consommation des appareils du foyer $p_A(t)$. L'idée générale est de tracer la courbe de charge du foyer $p(t)$ et celle de la consommation des appareils $p_A(t)$ en fonction du temps (t), puis de comparer leur alignement en calculant une régression linéaire. Les auteurs concluent qu'ils peuvent masquer l'usage des appareils du foyer en utilisant une batterie [4].

Varodayan et coll. [144] proposent une extension de l'algorithme proposé par Kalogridis et coll. [82]. À la place de vouloir obtenir une consommation constante dans le foyer, les auteurs randomisent les choix de l'algorithme en utilisant des politiques stochastiques d'usage des batteries : la charge ou la décharge de la batterie se produit avec une probabilité définie. Les auteurs montrent une amélioration de la protection de la vie privée en utilisant comme métrique le taux d'information mutuelle entre la consommation des appareils du foyer et la courbe de charge mesurée par le compteur, permettant de mesurer la dépendance mutuelle entre la consommation des appareils et la courbe de charge mesurée par le compteur.

Un autre algorithme proche de celui de Kalogridis et coll. [82] a été proposé par McLaughlin et coll. [107]. Cet algorithme est appelé NILL (Non-Intrusive Load Leveling), et consiste à uniformiser le profil de consommation d'un foyer à une courbe de charge constante, supprimant ainsi les caractéristiques des appareils utilisés dans le foyer. Pour réaliser cet objectif, le NILL utilise des batteries pour compenser l'énergie consommée par les appareils du foyer : les batteries sont déchargées pour supporter partiellement l'usage des appareils afin que la consommation du foyer (relevée par le compteur communicant) ne dépasse pas le seuil fixé. De même, pendant une demande faible de consommation dans le foyer, les batteries sont rechargées afin d'atteindre le seuil fixé de consommation. Les auteurs ont implémenté le NILL, en utilisant quatre types de foyers : deux maisons, un appartement et une *townhouse* ou « maison de ville ». Les courbes de charge de ces foyers ont été collectées pendant le printemps 2010 dans le Nord-Est des États-Unis. Les résultats expérimentaux montrent qu'en utilisant 10 batteries [5], les *features* ou caractéristiques permettant d'identifier les appareils utilisés dans un foyer à partir de la courbe de charge de ce foyer diminuent jusqu'à 91% à 94% en fonction du type de foyers (maison, appartement, *townhouse*). Ainsi, les attaques de type NALM ne sont plus réalisables.

Cependant, ces algorithmes utilisant les batteries ne sont pas formellement prouvés

4. Les auteurs testent leur algorithme en utilisant quatres batteries de capacité différente ; B1 :250 W/500 Wh ; B2 :500 W/1 kWh ; B3 :1 kW/2 kWh et B4 :2 kW/4 kWh. En utilisant la batterie B4, ils obtiennent la meilleure protection

5. Chaque batterie à une capacité de 50 Ah, et une tension de 12 V. Avec les 10 batteries en série, la tension totale est de 120 V. L'intensité maximale du courant est de 60 A pendant la décharge des batteries

comme protégeant la vie privée. Dans la littérature, les batteries sont utilisées pour garantir la DP afin d'apporter des garanties formelles réduisant le risque d'identification des appareils utilisés dans un foyer à partir de la courbe de charge de ce foyer.

Àcs et coll. [2] montrent comment garantir la DP en utilisant des batteries : un bruit qui suit la distribution de Laplace est simulé par des batteries et rajouté à la consommation des appareils du foyer. Ainsi la courbe de charge globale du foyer garantit la DP, c'est-à-dire, le risque d'identification des appareils utilisés dans le foyer est réduit. Cependant, cette technique nécessite une batterie avec une grande capacité. Pour garantir la DP avec un budget $\epsilon < 0,1$ sur 10 pas de temps, le mécanisme de Laplace proposé nécessite une batterie d'une capacité qui est 500 fois supérieure à la consommation maximale du foyer. Par exemple, si la consommation maximale du foyer à un pas de temps est de 6000 W, en considérant la tension du circuit égale à 240 V, la batterie à utiliser doit avoir une capacité de $500 \times 6000/240 = 12500$ Ah. Ce qui est énorme, c'est pourquoi les auteurs concluent en disant que ces travaux sont préliminaires.

Backes et coll. [11] utilisent la même idée, en ajoutant la consommation des batteries (pendant la recharge) à la courbe de charge globale du foyer. Ce qui permet de charger des batteries tout en garantissant (par la DP) que la courbe de charge du foyer ne permet pas d'identifier les appareils utilisés dans le foyer. Dans cet article, il faut une batterie d'une capacité qui est 250 fois supérieure à la consommation maximale du foyer, pour garantir la DP avec un budget de $\epsilon = 0,5$ sur 10 pas de temps. Par exemple, pour cacher l'utilisation d'un écran plasma de 42 pouces d'une puissance de 335 W sur une durée de 5 h, avec un budget $\epsilon = 0,33$, les auteurs montrent qu'il faut utiliser une batterie d'une capacité de stockage supérieure à 11 kWh.

3.2.2 Pseudonymisation et anonymisation

La pseudonymisation [44, 52, 62, 134, 135] consiste à séparer les données d'identification des compteurs (ou des clients), des données de consommation qui seront envoyées au fournisseur. Cependant, des techniques de ré-identification [12, 77, 120, 143] permettent souvent de retrouver l'identité des utilisateurs.

Jawurek et coll. [77] utilisent des techniques comme le NALM pour identifier l'ensemble des appareils utilisés dans un foyer à partir de la courbe de charge pseudonymisée. À partir des appareils utilisés dans un foyer, il est possible de déduire les habitudes des personnes habitants dans ce foyer : les heures de lever, de coucher (lumières allumées ou éteintes), si des travaux sont effectués dans ce foyer (pics de consommation dans la courbe de charge), les heures de retour des enfants de l'école, le retour des parents du travail. À partir de ces informations, déduites de la courbe de charge, il est possible de construire un profil en général unique et donc de ré-identifier les foyers. La pseudonymisation n'est donc pas suffisante pour préserver la vie privée des utilisateurs.

L'anonymisation consiste à transformer un jeu de données de telle sorte qu'il n'y ait plus de lien entre le jeu de données transformé, ou « anonymisé » et l'identité des utilisateurs appartenant à ce jeu de données. En d'autres termes, un jeu de données anonymisé ne permet

pas de retrouver l'identité des personnes qui le constitue.

Le RGPD (Règlement Général sur la Protection des Données) indique clairement que

> « Il n'y a dès lors pas lieu d'appliquer les principes relatifs à la protection des données aux informations anonymes, à savoir les informations ne concernant pas une personne physique identifiée ou identifiable, ni aux données à caractère personnel rendues anonymes de telle manière que la personne concernée ne soit pas ou plus identifiable » (RGPD, considérant 26 [131]).

Un ensemble courbes de charge anonymisé permet de réaliser de nombreux services énergétiques, par exemple, des prévisions de consommation dans un quartier.

Cependant, il n'existe pas de techniques d'anonymisation dans l'absolu, c'est-à-dire ayant un risque zéro d'identification des personnes appartenant à un jeu de données anonymisé. Mais il existe des algorithmes permettant de réduire la probabilité de ré-identification. Par exemple, la DP est une technique d'anonymisation, permettant de quantifier formellement, la probabilité de ré-identification des utilisateurs appartenant à une base de données.

En outre, avec des données anonymisées, il ne serait pas possible de fournir tous types de services. En effet, les algorithmes d'effacement nécessitent l'envoi de consignes par le fournisseur aux clients, ce qui serait impossible avec des données anonymes étant donné que les personnes concernées ne sont plus identifiables.

3.2.3 Agrégation sécurisée de courbes de charge

Les protocoles d'agrégation sécurisée cherchent à calculer un agrégat, en général une somme de consommation sans révéler les consommations individuelles des clients [38, 43, 65, 87, 119]. Cela permet par exemple de calculer la consommation globale d'un quartier, ce qui peut ensuite être utilisé pour prévoir la consommation d'énergie d'un quartier [76, 125].

Garcia et coll. [65] utilisent du PHE de Paillier [124] permettant aux utilisateurs d'envoyer leurs consommations chiffrées au fournisseur en garantissant que seule la somme totale de consommations peut être déchiffrée.

Description du protocole de Garcia et coll. [65]

Soit x_i la consommation du foyer P_i à agréger pour tout $i = 1, \dots N$ avec N le nombre de foyers. Un serveur central qui peut jouer le rôle d'un distributeur ou fournisseur est connecté aux compteurs des foyers $P_1, \dots, P_N$. Soit $\mathrm{Enc}_{\mathrm{pk}}(\cdot)$ la fonction de chiffrement partiellement homomorphe additif de Paillier et pk la clé publique du destinataire (le serveur central). On a :

$$\mathrm{Enc}_{\mathrm{pk}}(x_1) \times \mathrm{Enc}_{\mathrm{pk}}(x_2) = \mathrm{Enc}_{\mathrm{pk}}(x_1 + x_2)$$

Dans ce protocole, chaque compteur appartenant à un foyer P_i possède une clé publique pk_i pour tout $i = 1, \dots, N$. Ces clés publiques sont connues du serveur central. Le protocole proposé est décrit dans l'algorithme 5. Cet algorithme est exécuté T fois, avec T la granularité de la courbe de charge considérée. Par exemple, si on veut calculer la somme de courbes de charge sur une journée à un pas de temps 30 min, l'algorithme 5 sera exécuté 48 fois.

Ce protocole résiste aux attaquants qui sont dits HBC (*Honest-but-Curious* ou honnête mais curieux). Cependant, ce protocole ne résiste pas aux attaquants byzantins. Dans le cas où au moins un participant a un comportement byzantin, le résultat final calculé peut ne pas être correct, ce qui entraîne des erreurs de prévision de consommation.

Danezis et coll. [38] montrent comment calculer une agrégation sécurisée en utilisant du partage de secret. Leur solution permet de facturer les consommations et de faire quelques analyses statistiques. Cependant ce protocole nécessite des TTP (*trusted third parties*).

Pour résoudre ce problème, Dimitriou et coll. [43] proposent deux protocoles d'agrégation sécurisée qui n'utilisent pas de TTP. Le premier protocole utilise du PHE et résiste aux attaquants honnêtes mais curieux. Le second protocole utilise des ZK-PEQ (*Zero-Knowledge proof of Plaintext EQuality*) ce qui permet de résister contre des attaquants byzantins, mais réduit les performances.

En utilisant du SMC, Mustafa et coll. [119] décrivent un algorithme d'agrégation sécurisée appliqué à un cas réel de marché d'électricité. Les auteurs considèrent que l'électricité n'est pas produite par un seul fournisseur, et que les foyers peuvent aussi produire de l'électricité, par exemple grâce à des panneaux solaires. Leur protocole permet de calculer la consommation et la production d'électricité en considérant les différentes entités suivantes.

1. *Utilisateurs* – qui consomment uniquement et sont facturés pour cette consommation d'électricité
2. *Ressources énergétiques distribuées* – qui sont des petits générateurs d'électricité (par exemple des panneaux solaires), ces utilisateurs qui produisent de l'énergie, la consomment et injectent le surplus de production dans le réseau.
3. *Fournisseurs* – qui fournissent de l'électricité aux utilisateurs.

Les algorithmes d'agrégations présentés dans cette section permettent de calculer des sommes de courbes de charge de plusieurs foyers, sans révéler les consommations individuelles des foyers. Ces agrégats sont utilisés pour calculé des prévisions de consommation de la région considérée.

Cependant, ces techniques ne permettent pas de calculer des fonctions plus élaborées comme la comparaison. Cette opération est utilisée pour des services de DR, par exemple pour vérifier à chaque instant que la consommation des foyers d'un quartier ne dépasse pas la puissance maximale du poste local.

En outre, l'agrégation sécurisée de courbes de charge, ne garantit pas que l'agrégat ne révèle pas indirectement les courbes de charge individuelles qui ont permis de le calculer.

3.2.4 Publication de courbes de charge

En combinant SMC et DP, Ács et coll. [3] montrent comment calculer un agrégat de manière sécurisé tout en limitant la ré-identification des données individuelles à partir de l'agrégat. Leur solution permet de calculer une somme de consommations sans révéler les entrées, en divisant un bruit qui suit la distribution de Laplace $\mathcal{L}(\cdot)$ en n bruits qui suivent la distribution de Gamma (lemme 3.1.1). Pour chaque consommation x_i ($i = 1, \ldots, n$), le compteur ajoute

un bruit aléatoire σ_i qui suit la distribution de Gamma, et envoie le résultat au fournisseur. La somme des consommations bruitées reçues est $\sum_{i=1}^{n}(x_i + \sigma_i) = x_1 + \cdots + x_n + \mathcal{L}(\cdot)$, avec $\sum_{i=1}^{n} \sigma_i = \mathcal{L}(\cdot)$. Le bruit de Laplace permettant de garantir la DP, le calcul de la somme garantit donc bien la DP. Ce protocole permet d'éviter l'attaque de différence [39]. Cependant, cette proposition résiste uniquement aux attaquants honnêtes mais curieux.

En outre, l'utilisation de la DP entraine une perte d'utilité due au bruit de Laplace introduit dans l'agrégat. Eibl et coll. [53] ont montré que pour le comptage, le nombre de données agrégées (ou le nombre de compteurs communicants) doit être de l'ordre du millier pour avoir une utilité raisonnable. Pour un groupe de taille 14 052, ils obtiennent une erreur inférieure à 13%. Dans le chapitre 5, nous montrons comment obtenir une bonne utilité, inférieur à 10% pour un agrégat d'une centaine de foyers.

La DP est généralement appliquée en considérant les données de manière indépendante. C'est-à-dire, faire plusieurs publications de données avec un budget ϵ pour chaque publication. Bien que les données publiées sont souvent différentes, dans la plus part des cas ces données sont corrélées. Par exemple, une courbe de charge sur une journée à un pas de temps de 30 min est corrélée, en effet le cycle de consommation d'un appareil comme la machine à laver s'étend sur plusieurs pas de temps, sa consommation au pas de temps $t + 1$, dépend de celle du pas de temps t. Wang et coll. [147] montrent qu'en appliquant la DP sur des données corrélées, en les considérant indépendantes, un attaquant qui connait la fonction de corrélation des données, peut construire un filtre (comme le filtre de Wiener) permettant de retrouver une estimation des données initiales à partir de celles bruitées.

Le théorème 3.1.2 de composition de la DP dit qu'en publiant plusieurs agrégations, en utilisant des données corrélées, le budget total de privacy ϵ est égal à la somme de tous les budgets utilisés pour chaque agrégation. Par exemple, en utilisant un budget $\epsilon = 0.5$ pour publier chaque point d'une somme de courbes de charge à un pas de temps 30 min sur une journée, le budget total utilisé est $\epsilon = 0.5 \times 48 = 24$. Pour garantir un budget global ϵ, une idée est d'utiliser un budget ϵ/T pour chaque publication. Cependant, plus de bruit est ajouté sur l'agrégat des courbes de charge, ce qui conduit à une perte d'utilité.

Rastogi et Nath [130] proposent l'APF (algorithme de perturbation de Fourier) qui combine la TFD (transformée de Fourier discrète) et la DP pour publier des séries temporelles de requêtes de comptage, en garantissant une bonne protection et une bonne utilité. Cette méthode consiste à compresser la série temporelle, ainsi d'introduire moins de bruit (comme la taille de la série a diminué), ce qui conduit à une erreur plus faible que lorsqu'on bruite directement la série temporelle. Cependant, l'APF possède quelques erreurs présentées dans le chapitre 5. La sensibilité d'une requête de comptage est de 1, et la sensibilité globale est de T pour une séries temporelles de taille T. Ács et coll. [4] proposent une optimisation de l'APF permettant de publier des histogrammes, avec une sensibilité globale de 1. Leurs résultats expérimentaux montrent une amélioration d'un facteur 10 de l'utilité de l'algorithme proposé par rapport à l'APF.

Lyu et coll. [106] appliquent l'APF pour la publication de courbes de charge, et proposent l'APO (algorithme de perturbation en ondelettes) en remplaçant la TFD par la TOD (transformée en ondelettes discrète). Les auteurs montrent à travers des résultats expérimentaux que l'APO

à une meilleure utilité que l'APF.

Dans le chapitre 5, nous présentons plus en détail l'APF et l'APO, et proposons une optimisation de ces deux algorithmes en réduisant la sensibilité des transformées utilisées, afin de garantir une meilleure utilité par rapport à ces algorithmes.

3.2.5 Demande d'effacement à la pointe préservant la vie privée

Les algorithmes d'effacement à la pointe ou DR en anglais, présentés en section 2.2.1, ont pour objectif de réduire les pics de consommation dans un quartier. Ces algorithmes collectent les DCP (donnée à caractère personnel) des foyers (courbes de charge individuelles, niveau de flexibilité), permettant au GRD (gestionnaire de réseau de distribution) ou au fournisseur, de solliciter les foyers pour réduire leur consommation lors d'un pic sur le réseau. En contrepartie les foyers peuvent recevoir des récompenses pouvant se traduire par la réduction de leur facture d'électricité. Une autre technique d'incitation à décaler l'usage de ces appareils pendant les pics de consommation est de proposer des tarifs d'électricité variables comme l'option Heures Pleines/Heures Creuses (HP/HC).

Les algorithmes de demande d'effacement à la pointe préservant la vie privée cherchent à éviter les pics de consommation au sein d'un quartier sans avoir accès aux DCP des foyers concernés.

Thoma et coll. [142] ont proposé un algorithme de gestion de la demande d'énergie respectueuse de la vie privée en utilisant du SMC et du chiffrement partiellement homomorphe : PHE (*Partially Homomorphic Encryption*) [124]. Chaque groupe d'utilisateurs calcule sa somme de consommation sans révéler les consommations individuelles en utilisant du chiffrement partiellement homomorphe. Si la somme de consommation d'un groupe est supérieure à un seuil fixé, alors un statut *pointe* est attribué à ce groupe, sinon le statut *creux* est attribué. Pour chaque groupe ayant le statut *pointe*, un seuil de groupe est calculé. Ce seuil peut correspondre à la consommation moyenne des utilisateurs de ce groupe. Les utilisateurs ayant une consommation supérieure à ce seuil de groupe sont considérés comme ayant une demande d'énergie élevée et le calcul de la facturation d'électricité dépendra du statut de chaque client. Cependant, comme la somme de consommation de chaque groupe est révélée, cette somme reste vulnérable aux attaques indirectes de ré-identification.

Rottondi et coll. [136] ont proposé un protocole d'ordonnancement de la demande d'énergie respectant la vie privée, en utilisant le partage de secret de Shamir [138], et le chiffrement partiellement homomorphe. Chaque utilisateur partage sa demande d'énergie générée par ses appareils électriques avec un ensemble d'ordonnanceurs, qui calculent conjointement le délai de démarrage de chaque appareil, de telle sorte que la charge totale des appareils ne dépasse pas la puissance maximale du réseau local. Ce protocole résiste aux attaquants honnêtes mais curieux.

Rottondi et coll. [133] ont proposé un protocole d'ordonnancement de la demande d'énergie respectant la vie privée, en utilisant de l'agrégation, et des techniques de perturbation de données. Chaque utilisateur envoie sa consommation prévisionnelle perturbée par un bruit additif Gaussien aux autres utilisateurs. Ainsi chaque utilisateur a la possibilité de calculer

la demande de consommation totale perturbée du réseau local à chaque instant. Comme le prix de l'électricité à chaque instant dépend de la demande d'énergie des utilisateurs à cet instant, chaque utilisateur peut décider de décaler sa consommation d'énergie permettant de minimiser sa facture d'électricité journalière. L'inconvénient de cette technique est le manque de précision dans le calcul de la somme de consommation (dû à la perturbation), ce qui peut entrainer une augmentation inattendue de la facture d'électricité.

Rottondi et coll. [133] montrent que leur protocole résiste à un attaquant HBC, c'est-à-dire un utilisateur qui suit le protocole mais veut déduire la plage horaire de l'usage des appareils d'un foyer à partir des données agrégées de demande d'énergie reçues. Comme les consommations prévisionnelles des foyers sont bruitées par un bruit Gaussien aléatoire, les auteurs modélisent les consommations prévisionnelles des foyers sous forme d'une variable aléatoire multivariée notée V. En notant Ψ une variable aléatoire multivariée décrivant la probabilité de chaque combinaison possible des préférences d'utilisation des appareils des utilisateurs, les auteurs définissent le niveau de protection par $\gamma = H(V) - H(V|\Psi)$ avec $H(\cdot)$ la fonction calculant l'entropie. Quand γ est petit, alors la probabilité qu'un attaquant déduit les préférences d'utilisation des appareils d'un foyer est faible. Quand γ est élevé, cette probabilité est forte. Les résultats expérimentaux montrent que plus le bruit ajouté est grand, plus γ diminue (meilleure protection), en contrepartie, la facture d'électricité augmente. Par exemple, pour une protection de $\gamma = 2$, il faut introduire un bruit Gaussien dont l'écart-type correspond à environ 210 W, avec en contrepartie une augmentation de la facture d'électricité de 2% en considérant 50 foyers.

3.2.6 Bilan des applications des PET à l'énergie

Dans la section 3.2, nous avons présenté des applications des PET dans le domaine de l'énergie. Ces applications se sont beaucoup développées pendant cette dernière décennie, d'une part, grâce à l'avènement des *smart grids*, nécessaire à la réduction des émissions de GES (gaz à effet de serre), et d'autre part, grâce à la population française, qui se soucie du respect de sa vie privée.

Nous avons premièrement présenté des techniques permettant de protéger une courbe de charge contre l'identification des appareils utilisés dans le foyer. Ensuite, nous avons présenté des techniques d'agrégations sécurisées de courbes de charge. Ces techniques utilisent principalement du PHE et du SMC, et calcule des sommes de consommation sans révéler des consommations individuelles. Ces agrégats sont généralement pour réaliser des prévisions de consommation.

Cependant, un agrégat ne garantit pas qu'un attaquant ne peut pas identifier une courbe de charge individuelle qui compose cet agrégat. Pour empêcher toutes fuites indirectes de données, la DP est appliquée aux courbes de charge, ce qui entraine souvent une dégradation de l'agrégat obtenu, et peut rendre inutilisable le résultat des prévisions de consommation qui prend en entrées ces agrégats perturbés.

Finalement, nous avons présenté des services de DR respectueuses de la vie privée. Cependant, ces services ne sont pas encore assez matures.

3.3 Conclusion

Dans ce chapitre, nous avons présenté d'une part, les technologies de protection de la vie privée, abrégées PET en anglais. D'autre part, nous avons présenté les applications de ces technologies dans le domaine de l'énergie. Cependant, ces applications sont encore peu matures, par exemple, la publication de courbes de charge rend souvent l'agrégat trop perturbé en considérant une centaine de foyers. Ainsi, réaliser des prévisions de consommation pour une centaine de foyers, tout en protégeant la vie privée de ces foyers est impossible. Le chapitre 5 présente de nouveaux algorithmes permettant de publier de courbes de charge d'une centaine de foyers, en garantissant à la fois une bonne utilité et une bonne protection de la vie privée des foyers.

En outre, les algorithmes de DR respectueuses de la vie privée, qui sont proposés dans la littérature, peuvent être soit vulnérables aux attaques indirectes de ré-identification, soit entrainer une perte de précision, ce qui peut se traduire par une augmentation inattendue de la facture d'électricité [133]. Dans le chapitre 4, nous montrons comment transformer un algorithme de DR réel en protégeant les DCP qu'il manipule, tout en préservant son efficacité.

Algorithme 4 Phase hors-ligne ou de preprocessing, permettant de générer la clé globale $[\![\alpha]\!]$, les paires $[\![r]\!], \langle r \rangle$ et les triplets $\langle a \rangle, \langle b \rangle, \langle c \rangle$ tels que $c = ab$.

Utilisation : permet de générer des nombres aléatoires partagés, des triplets partagés
Initialisation : Cette partie permet de générer la clé globale α et les clés individuelles β_i de chaque partie P_i $(i = 1, \ldots, n)$

1. Les parties font appel à la fonction d'initialisation (présentée en [37]) qui renvoie la clé publique pk
2. Chaque partie P_i génère de manière aléatoire les clés β_i, et α_i appartenant à $\mathbb{F}_{p^k}$. On note $\alpha = \sum_{i=1}^{n} \alpha_i$.
3. Chaque partie P_i calcule les chiffrés e_{α_i} et e_{β_i} en utilisant la clé pk, et envoie le résultat à tous les autres parties.
4. Toutes les parties calculent $e_\alpha = e_{\alpha_1} + \cdots + e_{\alpha_n}$ et génèrent $[\![\alpha]\!] = \text{PBracket}(\alpha_1, \ldots, \alpha_n, e_\alpha)$.

Génération de paires partagées : cette étape génère une paire $[\![r]\!], \langle r \rangle$, et peut être utilisée pour générer une seule valeur partagée $[\![r]\!]$ (il suffit de ne pas faire appel à PAngle.)

1. Chaque partie P_i génère r_i ; on note $r = \sum_{i=1}^{n} r_i$.
2. Chaque partie calcule e_{r_i} et envoie le résultat aux autres parties.
3. Les parties calculent $e_r = e_{r_1} + \cdots + e_{r_n}$ et génèrent $[\![r]\!] = \text{PBracket}(r_1, \ldots, r_n, e_r)$ et $\langle r \rangle = \text{PAngle}(r_1, \ldots, r_n, e_r)$

Génération de triplets partagés : cette étape génère un triplet $\langle a \rangle, \langle b \rangle, \langle c \rangle$ qui est utilisé pour réaliser des multiplications de secrets partagés.

1. Chaque partie génère a_i et b_i. Soit $a = \sum_{i=1}^{n} a_i$, et $b = \sum_{i=1}^{n} b_i$.
2. Chaque partie calcule e_{a_i} et e_{b_i}, et envoie le résultat aux autres parties.
3. Les parties calculent $e_a = e_{a_1} + \cdots + e_{a_n}$ et $e_b = e_{b_1} + \cdots + e_{b_n}$, et génèrent $\langle a \rangle = \text{PAngle}(a_1, \ldots, a_n, e_a)$ et $\langle b \rangle = \text{PAngle}(b_1, \ldots, b_n, e_b)$.
4. Les parties calculent $e_c = e_a \times e_b$ et fixent $(c_1, \ldots, c_n, e_c^{'}) = \text{Reshare}(e_c)$.
5. Les parties génèrent $\langle c \rangle = \text{PAngle}(c_1, \ldots, c_n, e_c^{'})$.

Algorithme 5 Agrégation de sommes de consommation de Garcia et coll. [65]

1. Le serveur central envoie les clés publiques $pk_1, \cdots, pk_N$ à tous les compteurs des foyers participants.
2. Chaque compteur S_i choisit aléatoirement les parts $a_{i,1}, \cdots, a_{i,N}$ tels que $x_i = \sum_j a_{i,j} \mod n$ avec n un grand nombre. Puis envoie au serveur central les parts $y_{i,1}, \cdots, y_{i,i-1}, y_{i,i+1}, \cdots, y_{i,N}$ tel que $y_{i,j} = \mathrm{Enc}_{\mathrm{pk}_j}(a_{i,j})$ avec $j = 1, \cdots, i-1, i+1, \cdots, N$. Si N n'est pas assez grand alors le foyer P_i arrête l'algorithme. En effet il faut un nombre minimal de participants pour éviter des coalitions et apprendre des consommations des autres participants.
3. Le serveur central envoie au compteur du foyer P_i le produit de tous les chiffrés qui lui sont destinés : $\prod_{j \neq i} y_{j,i} = \mathrm{Enc}_{\mathrm{pk}_i}(\sum_{j \neq i} a_{j,i})$ (propriété d'addition homomorphique)
4. Le compteur déchiffre le chiffré reçu puis ajoute son secret $a_{i,i}$:
   $\sum_{j \neq i} a_{j,i} + a_{i,i} = \sum_j a_{j,i} \mod n$ et envoie le résultat au serveur
5. En sommant les données reçues, le serveur obtient : $x = \sum_{i=1}^{N} \sum_{j=1}^{N} a_{j,i} \mod n = \sum_{i=1}^{N} x_i$

Chapitre 4

Algorithme d'effacement à la pointe respectueux de la vie privée

Les algorithmes d'effacement à la pointe ou DR (*Demand Response*) permettent d'éviter les pics de consommation dans un quartier en s'assurant qu'à chaque instant, la consommation des utilisateurs ne dépasse pas la puissance maximale fournie au niveau du quartier. Si la demande des utilisateurs est supérieure à la puissance disponible, le fournisseur demande aux utilisateurs flexibles de décaler l'usage de leurs appareils en échange d'une réduction de leur facture d'électricité. Ce type de service permet de résoudre un des problèmes liés à l'avènement des véhicules électriques : en effet, si plusieurs habitants du quartier chargent leur véhicule au même moment – par exemple le soir à 19h, lors d'un pic de consommation –, l'appel de puissance pourrait dépasser la puissance maximale fournie au niveau du quartier.

Comme expliqué en section 2.2.1, pour être plus efficaces, les algorithmes de DR doivent être collaboratifs afin d'éviter les rebonds de pics de consommation. Le GEEQ (Gestionnaire d'Énergie de l'Éco-Quartier) [64] est un algorithme de DR collaboratif développé par le laboratoire SEIDO (Laboratoire cybersécurité et internet des objets), un laboratoire commun entre EDF R&D, Télécom Paris, Télécom SudParis et LAAS–CNRS.

Cependant, cet algorithme a l'inconvénient de collecter les DCP (donnée à caractère personnel) des clients : courbes de charge, coefficients de flexibilité, etc.

Ce chapitre montre qu'il est possible d'adapter un algorithme de DR collaboratif, ici le GEEQ, pour le rendre respectueux de la vie privée. Il présente le GEEQ protégé, une transformation du GEEQ, permettant de fournir un service d'effacement à la pointe sans avoir accès aux DCP des foyers concernés. Le GEEQ protégé utilise du SMC (*Secure Multi-party Computation*) présenté dans la section 3.1.2 du chapitre 3. Une comparaison entre le GEEQ protégé et le GEEQ dans la section 4.1.6 montre qu'il est possible de concilier vie privée et utilité.

La section 4.1 présente le GEEQ, puis décrit le GEEQ protégé – une manière de protéger les DCP utilisées par cet algorithme. Ensuite, la section 4.2 analyse les résultats expérimentaux de la version protégée du GEEQ suivant deux critères : les performances et l'utilité comparativement au GEEQ. Enfin, la section 4.4 conclut ce chapitre.

4.1 Protection des DCP pour l'effacement à la pointe

Cette section présente tout d'abord l'algorithme du GEEQ, puis une adaptation du GEEQ qui s'appuie sur le SMC et qui empêche la collecte des DCP tout en garantissant son utilité (l'efficacité concernant la diminution des pics de consommation). Le tableau 4.1 liste les symboles utilisés dans cette section.

Notation	Description
n	nombre de compteurs communicants ou de foyers
$\langle x \rangle$	partage du secret x
$\mathcal{T}$	ensemble des pas de temps auxquels l'algorithme d'effacement à la pointe est exécuté
p_i^t	consommation prévisionnelle du foyer i ($1 \leq i \leq n$) à l'instant t
$\mathcal{P}_{\max}$	puissance maximale du réseau local
$p_i^{\max,t}$	puissance souscrite du foyer i à l'instant t
p'^t_i	consommation prévisionnelle recommandée du foyer i à l'instant t calculée par le GEEQ
α	facteur de sûreté du réseau local
ϵ^t	surplus de consommation à l'instant t – différence entre la somme des consommations prévisionnelles des foyers et la puissance maximale du réseau local à l'instant t : $\epsilon^t = \sum_i p_i^t - (1-\alpha)\mathcal{P}_{\max}$ avec α le facteur de sûreté
a^t	détermine l'absence ou la présence d'un pic de consommation : a^t est égal à 1 si à l'instant t la somme des consommations prévisionnelles des foyers est inférieure à la puissance maximale du réseau local, et 0 sinon
k	nombre de clients sollicités pour réduire leur consommation prévisionnelle à chaque tour de réduction
b_i	nombre de points gagnés par le foyer i pendant la phase de réduction
c_t	facteur de récompense à l'instant t
$f_i^t (0 \leq f_i^t \leq 1)$	flexibilité du foyer i à l'instant t par rapport à sa puissance souscrite $p_i^{\max,t}$ choisie par chaque client
I	ensemble des foyers ayant déjà été sollicités pour réduire leur consommation prévisionnelle (initialement, $I = \emptyset$)

TABLEAU 4.1 – Liste des symboles utilisés dans l'algorithme du GEEQ

4.1.1 Modèle du système

Les parties prenantes du GEEQ sont :

— Le GESH (Gestionnaire d'Énergie de la Smart Home) – chaque foyer dispose d'un appareil appelé GESH permettant de gérer l'utilisation des appareils flexibles des utilisateurs dans le foyer. Chaque utilisateur communique les heures préférentielles d'utilisation de ses appareils au GESH, qui se charge d'ordonnancer le démarrage des appareils électriques du foyer en privilégiant la consommation aux heures creuses où l'électricité est la moins chère possible. Le GESH calcule ensuite la consommation prévisionnelle

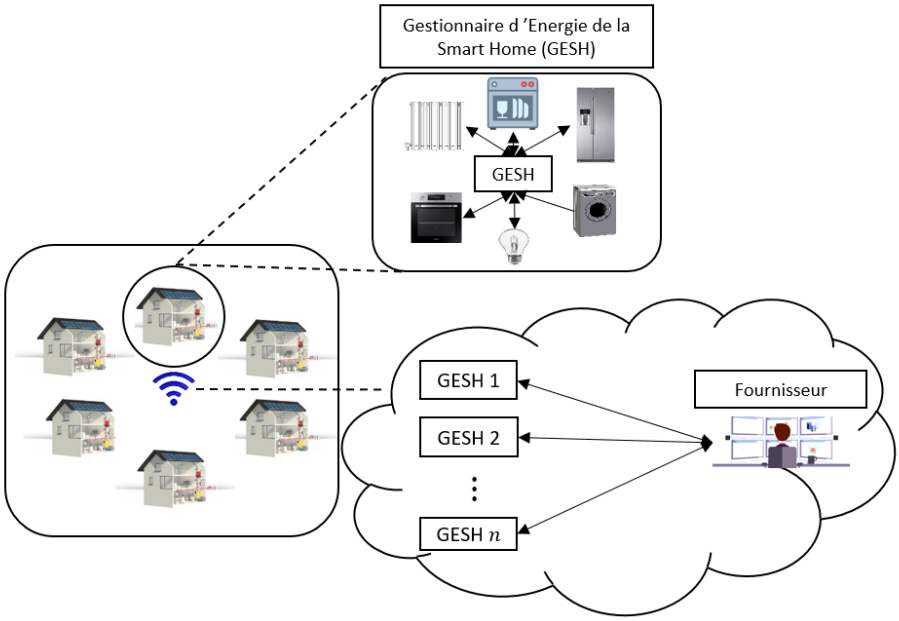


FIGURE 4.1 – Modèle du système pour le GEEQ

des appareils du foyer à chaque pas de temps et peut communiquer le résultat au fournisseur. Le GESH peut retarder ou déplacer l'usage des appareils dans le foyer. Rousselle et coll. proposent un tel appareil [137].

— Le fournisseur, qui veut satisfaire les demandes en énergie des utilisateurs tout en évitant les pics de consommation dans le réseau.

Nous supposons que les communications entre les GESH et le fournisseur sont chiffrées et authentifiées. Dans la suite le mot foyer peut être utilisé pour désigner les actions de son GESH. La figure 4.1 représente le modèle du système pour le GEEQ.

4.1.2 GEEQ (Gestionnaire d'Énergie de l'Éco-Quartier)

Forestier et coll. [64] proposent le GEEQ, un algorithme de demande d'effacement à la pointe permettant de coordonner les GESH afin d'éviter les pics de consommation dans le foyer tout en optimisant la consommation individuelle de chaque foyer. Le GEEQ prend en entrée les consommations prévisionnelles des foyers d'un quartier à chaque pas de temps (grâce au GESH), et vérifie si la somme des consommations prévisionnelles ne dépasse pas la puissance maximale du réseau local. Si cette somme dépasse la puissance maximale du réseau local, le GEEQ sollicite les foyers (les GESH) en leur demandant de réduire (ou de décaler) leur consommation.

Plus précisément, comme le montre l'algorithme 6, chaque GESH envoie sa consommation prévisionnelle au fournisseur (étape 1). Après avoir reçu toutes les consommations prévisionnelles des GESH du quartier, le fournisseur vérifie si la somme des consommations

prévisionnelles est inférieure à la puissance maximale du réseau local (étape 2), en prenant en compte un facteur de sûreté α. Si ce n'est pas le cas ($a^t = 0$), le fournisseur calcule le surplus de consommation des habitants du quartier, la consommation maximale recommandée p'^t_i de chaque foyer i au pas t en fonction de sa flexibilité et du surplus de consommation : $p'^t_i = p^t_i - \min(e^t, f^t_i \times p^{\max,t}_i)$. Le fournisseur calcule aussi le nombre de points que gagne chaque foyer s'il réduit sa consommation.

Notons que les foyers sélectionnés sont libres d'accepter ou de refuser de diminuer leur consommation prévisionnelle. La flexibilité des clients est récompensée par des points, qui permettent ultérieurement de réduire la facture d'électricité.

Comme le montre l'algorithme du GEEQ, le fournisseur sélectionne en priorité les GESHs qui ont le moins de points afin de ne pas toujours solliciter les mêmes GESHs (étape 3b). Finalement, le fournisseur envoie aux foyers leur consommation recommandée et le nombre de points gagnés correspondant (étape 3d).

L'algorithme 6 se termine en renvoyant la somme des consommations prévisionnelles des foyers du quartier.

Algorithme 6 GEEQ

Pour tout $t \in \mathcal{T}$:

1. Chaque GESH $i : 1 \leq i \leq n$ envoie sa consommation prévisionnelle p^t_i au fournisseur
2. Le fournisseur calcule $a^t = \sum_{i=1}^{n} p^t_i \leq (1-\alpha)\mathcal{P}_{\max}$
3. Si $a^t = 0$,
   (a) le fournisseur calcule $\epsilon^t = \epsilon^t_0 = \sum_{i=1}^{n} p^t_i - (1-\alpha)\mathcal{P}_{\max}$
   (b) le fournisseur sélectionne les GESHs en fonction de leur nombre de points : $\forall i \in \{1, \cdots, n\}$ s.t. $b_i \leq b_{i+1} \leq \cdots$.
   Ensuite le fournisseur calcule
      — la consommation recommandée des GESHs : $p'^t_i = p^t_i - \min(e^t, f^t_i \times p^{\max,t}_i)$
      — le nombre de points gagnés : $b_i = b_i + \frac{p^t_i - p'^t_i}{\epsilon^t_0} \times c^t$
      — la mise à jour du surplus de consommation prévisionnelle : $\epsilon^t = \epsilon^t - \min(\epsilon^t, f^t_i \times p^{\max,t}_i)$
   (c) Si $\epsilon^t < 0$, alors $a^t = 1$
   (d) le fournisseur envoie aux GESHs leur consommation recommandée p'^t_i, et le nombre de points gagnés correspondant b_i.
   (e) le fournisseur calcule et révèle la somme des consommations prévisionnelles des habitants du quartier.

L'algorithme du GEEQ permet d'éviter les pics de consommation dans un quartier mais

au prix de la collecte de DCP : les données de consommations individuelles des foyers, ainsi que leurs flexibilités.

Avant de présenter le GEEQ protégé – une transformation du GEEQ respectueuse de la vie privée des habitants des foyers –, la section suivante présente le modèle de l'attaquant considéré.

4.1.3 Hypothèses

Nous supposons que les GESH sont honnêtes mais curieux, c'est-à-dire qu'ils suivent le protocole, mais tentent d'apprendre des informations privées à partir de leurs observations. Notons que grâce au MAC (*Message Authentication Code*) mentionné dans la section 3.1.2, le framework SCALE-MAMBA [8] permet de détecter toute modification malveillante sur les secrets partagés, mais ne garantit pas que le partage est correct.

Les fournisseurs peuvent essayer d'apprendre les consommations individuelles des clients. Le modèle du système pour le GEEQ protégé est donné par la figure 4.2.

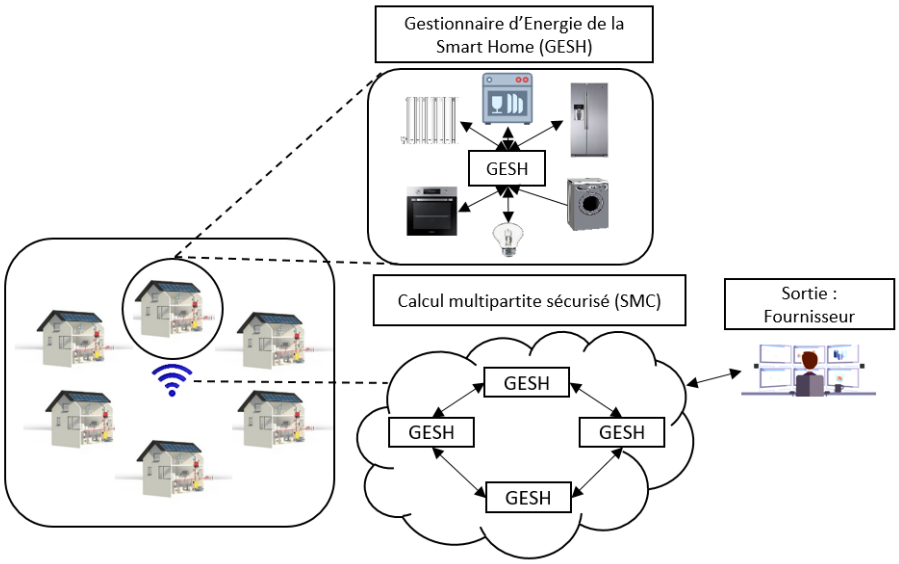


FIGURE 4.2 – Modèle du système pour le GEEQ protégé

4.1.4 Motivations

Le GEEQ est un algorithme centralisé : chaque foyer via son GESH envoie sa prévision de consommation au fournisseur qui réalise toutes les opérations. Cependant, cette configuration (centralisée) pose de nombreux problèmes de vie privée en cas de fuite de données. En effet si le fournisseur est compromis, toutes les données des foyers (identifiants, prévisions de consommation, flexibilités, etc.) sont compromises, ce qui pose des problèmes à la fois au

fournisseur (amendes pour non-respect de la protection des données des clients, dégradation de l'image de marque, etc.) et aux clients (vol d'identité, hameçonnage, etc.). Plus le nombre de données collectées sur un serveur centralisé est important, plus ce serveur est la cible privilégiée des attaquants.

Au contraire, le GEEQ protégé est distribué : les opérations sont effectuées conjointement par tous les foyers (GESH) et il n'existe pas de système physique exécutant, de manière centralisée, l'algorithme du GEEQ protégé. Cela nécessite des communications entre foyers sans avoir recours à un système administratif centralisé, il faut par exemple que les foyers soient en réseau pair à pair. Cette décentralisation permet de redonner le contrôle aux foyers de leurs données de consommation. De plus, la compromission d'un foyer, en cas de succès d'une attaque, ne permet pas de faire fuiter les consommations individuelles des autres foyers. Les systèmes décentralisés sont donc moins ciblés par des attaquants.

4.1.5 Protection des DCP dans le GEEQ

Cette section montre comment produire le même service que le GEEQ sans collecter les données personnelles des clients en utilisant le SMC. Ce nouvel algorithme obtenu, appelé « GEEQ protégé », est présenté dans l'algorithme 7.

À l'étape 1, à chaque pas de temps $t \in \mathcal{T}$, chaque GESH partage sa consommation prévisionnelle avec les autres GESH afin de calculer conjointement si la somme des consommations prévisionnelles des habitants du quartier est inférieure à la puissance maximale du réseau local (étape 2).

Le fournisseur a uniquement accès au résultat binaire de la comparaison et non plus aux données individuelles des consommations prévisionnelles des clients : 1 si la somme des consommations prévisionnelles des clients est inférieure à la puissance maximale du réseau local, 0 si ce n'est pas le cas. Ni le fournisseur, ni les foyers n'apprennent la valeur de cette somme.

Si le résultat de la comparaison est 1, l'algorithme se termine en renvoyant le résultat de cette comparaison ($a^t = 1$) au fournisseur (étape 4). Ainsi, le fournisseur sait qu'il n'y a pas de pics de consommation dans le réseau à l'instant t.

Si le résultat de la comparaison est 0 et que le nombre maximal de GESH sélectionné n'est pas encore atteint, les GESH sélectionnent k GESHs qui doivent réduire leur consommation prévisionnelle de manière aléatoire. Ce choix aléatoire se fait avec un algorithme de *coin-tossing*, comme présenté en section 4.1.5.

L'utilisateur qui accepte de réduire sa consommation reçoit une récompense (étape 3a). Après avoir réduit leur consommation prévisionnelle, les GESH partagent leur nouvelle consommation prévisionnelle avec les autres GESH (étape 3c). Si après la réduction de consommation ($\{1, \ldots, n\} \backslash I = \emptyset$), la somme des consommations prévisionnelles est supérieure à la puissance maximale du réseau ($a^t = 0$), alors les GESH n'ont pas pu réduire suffisamment leur consommation prévisionnelle. Dans ce cas, le fournisseur sait qu'il pourrait y avoir un pic de consommation dans le réseau à cet instant.

Pour être rémunéré, à la fin de la période de temps $\mathcal{T}$, chaque GESH i envoie au fournisseur

Algorithme 7 GEEQ protégé

Initialisation : $I = \emptyset$
Pour tout $t \in \mathcal{T}$:

1. Chaque GESH $i : 1 \leq i \leq n$ partage sa consommation prévisionnelle p_i^t avec les autres GESH
2. Les n GESH calculent
   $\left\langle a^t \right\rangle = \left\langle \sum_{i=1}^{n} \langle p_i^t \rangle \leq (1 - \alpha)\mathcal{P}_{\max} \right\rangle$ et ouvrent le résultat a^t
3. Si $a^t = 0$ and $\{1, \ldots, n\} \backslash I \neq \emptyset$, alors
   (a) Choisir aléatoirement k GESH $\in \{1, \ldots, n\} \backslash I$, en utilisant un protocole de *coin-tossing*. Chaque GESH i choisi calcule en parallèle,
   — sa consommation prévisionnelle maximale recommandée : $p'^t_i = p_i^t - f_i^t \times p_i^{\max,t}$
   — son nombre de points : $b_i = b_i + (p_i^t - p'^t_i) \times c^t$
   — met à jour sa consommation prévisionnelle maximale : $p_i^t = p'^t_i$
   (b) Mise à jour de l'ensemble des GESH qui ont déjà participé : $I = I \cup \{i\}$
   (c) Aller à l'étape 1
4. Sinon, le GESH 1 (ou un autre GESH) envoie a^t au fournisseur. Ce résultat est la sortie du GEEQ protégé.

À la fin de la période de temps $\mathcal{T}$, chaque GESH révèle son nombre de points gagnés b_i au fournisseur

son nombre de points gagnés b_i durant le GEEQ protégé. Le nombre de points est alors transformé en réduction de la facture d'électricité. Cependant, le processus de récompense peut permettre de révéler la flexibilité des utilisateurs. En effet, si après chaque pas de temps t, un utilisateur révèle son nombre de points b_i ($|\mathcal{T}| = 1$), le fournisseur peut déduire son facteur de flexibilité à l'instant t par $f_i^t = \frac{b_i}{p_i^{\max,t} \times c^t}$. Pour éviter cette fuite, le nombre de points doit être révélé seulement après une longue période de temps (par exemple à la fin de chaque mois).

Sélection de k clients parmi n

La phase hors-ligne de SCALE-MAMBA permet de générer des nombres aléatoires. Soit w un nombre aléatoire révélé à chaque GESH. Il est alors possible d'utiliser w comme graine permettant de sélectionner les k premiers clients distincts comme suit :

$$\left\{ \left\lfloor \frac{H(1\|w)}{\lfloor \frac{2^h}{n} \rfloor} \right\rfloor, \left\lfloor \frac{H(2\|w)}{\lfloor \frac{2^h}{n} \rfloor} \right\rfloor, \ldots \right\},$$

où H est une fonction de hachage cryptographique, comme SHA-256, avec h la taille binaire de sa sortie et $\|$ est l'opération de concaténation [1].

Nous faisons le choix de sélectionner les utilisateurs dans le GEEQ protégé aléatoirement au lieu de nous baser sur le nombre de points gagnés comme dans le GEEQ. En effet la connaissance à chaque instant du nombre de points gagnés des clients donne une information sur la flexibilité des utilisateurs, qui est une DCP.

4.1.6 Différences entre le GEEQ et le GEEQ protégé

Le GEEQ est un algorithme centralisé : chaque foyer envoie sa consommation au fournisseur qui réalise toutes les opérations. En revanche, le GEEQ protégé est distribué : les opérations sont effectuées conjointement par tous les GESHs. Ce qui nécessite des communications entre clients sans avoir recours à un système centralisé, par exemple en réseau P2P (Pair-à-Pair). Pour que le GEEQ protégé ne collecte pas les DCP des clients, tout en fournissant le même service que le GEEQ, les modifications suivantes ont été apportées :

1. Les GESH partagent leur consommation prévisionnelle entre eux de telle sorte qu'aucune partie n'a accès à la consommation prévisionnelle individuelle d'un foyer ; contrairement au GEEQ où le fournisseur a accès aux données de consommation individuelles de chaque foyer.
2. La vérification que la somme des consommations prévisionnelles des foyers est inférieure à la puissance maximale du réseau local est faite par le fournisseur dans le GEEQ. Dans le GEEQ protégé, elle est réalisée conjointement par tous les GESH. C'est uniquement le résultat de ce calcul qui est connu de tous (0 ou 1) dans le GEEQ protégé, à chaque fois où l'étape 2 est exécutée. Cela permet de savoir si la réduction effectuée par k clients permet de passer sous le seuil de puissance maximale du réseau local.
3. La sélection des foyers qui participent à la réduction de consommation ne se fait plus selon le nombre de points gagnés précédemment, mais aléatoirement. En effet le nombre de points gagnés peut révéler indirectement des informations sur la flexibilité des clients.
4. Dans le GEEQ, le calcul de la consommation à réduire se fait en fonction du surplus de consommation et de la flexibilité des foyers : $\min(\epsilon^t, f_i^t \times p_i^{\max,t})$; dans le GEEQ protégé, la consommation à réduire est uniquement fonction de la flexibilité : $f_i^t \times p_i^{\max,t}$. Cela peut entrainer une sur-sollicitation des foyers.
5. Le calcul de la consommation recommandée et du nombre de points gagnés correspondant se fait par le fournisseur dans le GEEQ et par chaque foyer dans le GEEQ protégé. Ici on suppose que les foyers sont honnêtes mais curieux c'est à dire qu'ils exécutent exactement le protocole.

1. Plus précisément, pour avoir un choix non biaisé, les valeurs de $H(i\|w)$ dans l'intervalle $[n \cdot \lfloor 2^h/n \rfloor, 2^h - 1]$ doivent être éliminées.

Analyse de sécurité

Toutes ces modifications apportées dans le GEEQ protégé permettent de garder secrets la consommation prévisionnelle, la consommation recommandée, la flexibilité et le nombre de points gagnés de chaque foyer. Ce qui est révélé dans le GEEQ protégé est uniquement le résultat de la comparaison (0 ou 1 étape 2) et les GESH sollicités à réduire leur consommation. En outre, en utilisant le MAC du SMC, toutes les données partagées sont authentifiées. Ainsi les parties ont une garantie sur l'authenticité des calculs effectués dans le GEEQ protégé, notamment le résultat de la comparaison a^t, tant que les GESHs sont honnêtes (les GESH ne doivent pas mentir sur leur consommation prévisionnelle). L'algorithme 7 résiste aux attaquants honnêtes mais curieux.

4.2 Résultats expérimentaux

Cette partie montre que le GEEQ protégé est presque aussi efficace que le GEEQ pour réduire les pics de consommation. La section 4.2.2 étudie la complexité du GEEQ protégé.

4.2.1 Évaluation de l'efficacité du GEEQ protégé comparativement au GEEQ

Nous avons implémenté l'algorithme 7 en utilisant le *framework* SCALE-MAMBA [8]. Le jeu de données qui a permis d'obtenir ces résultats expérimentaux provient du CER (*Commission for Energy Regulation*) présenté dans la section 2.1.2 du chapitre 3

Cette section montre que la réduction des consommations prévisionnelles des utilisateurs dans le GEEQ protégé est presque identique à celle du GEEQ.

Ce résultat est important sur le plan économique. Le fournisseur souhaite éviter les pics de consommation en évitant que les utilisateurs ne réduisent plus que nécessaire leur consommation prévisionnelle. En effet, la réduction de consommation des utilisateurs a un coût pour le fournisseur (réduction de la facture d'électricité des utilisateurs).

Afin de comparer l'efficacité du GEEQ protégé à celle du GEEQ, nous exécutons les deux algorithmes sur un même jeu de données et procédons comme dans la figure 4.3 :

- révéler la somme des consommations prévisionnelles des clients en utilisant le GEEQ : $f_G^{'} = \sum_{i=1}^{n} p_i^{'t}$;
- calculer la somme des consommations prévisionnelles des clients après avoir exécuté le GEEQ protégé (algorithme 7) : $f_{Gp}^{'} = \sum_{i=1}^{n} p_i^{'t}$;
- calculer l'erreur relative entre les deux sorties comme dans la figure 4.3 : ER = $|\frac{f_G^{'} - f_{Gp}^{'}}{f_G^{'}}|$;
- calculer le nombre de clients qui ont été sollicités pour réduire leur consommation dans le GEEQ protégé en fonction de la valeur de k.

Notons que nous calculons l'erreur relative entre la sortie du GEEQ et la somme des consommations prévisionnelles des clients après avoir exécuté le GEEQ protégé (il faut noter

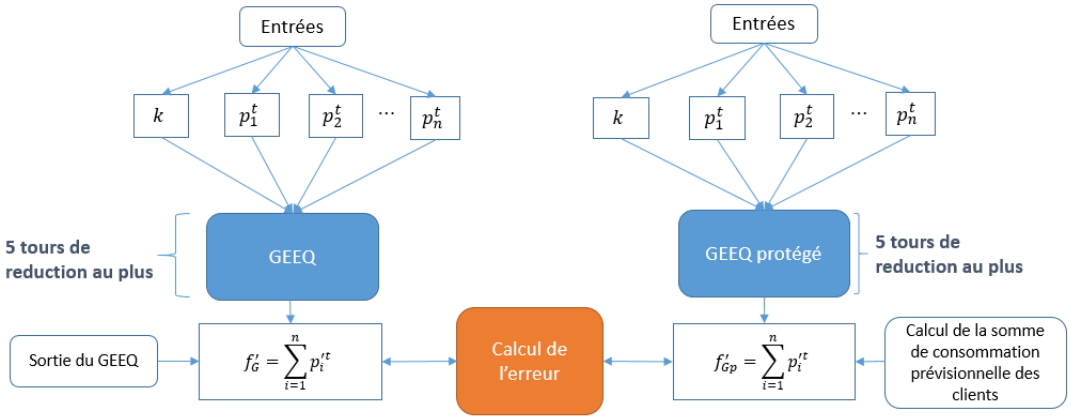


FIGURE 4.3 – Calcul de l'erreur relative – GEEQ vs GEEQ protégé

que la sortie du GEEQ protégé est a^t qui renvoie 1 si la somme des consommations des clients est inférieure à la puissance maximale du réseau local et 0 si ce n'est pas le cas). En effet, nous voulons comparer la réduction effective des consommations entre le GEEQ et le GEEQ protégé. Il faut donc comparer la somme des consommations prévisionnelles des clients après l'exécution des deux algorithmes.

Pour que le résultat de cette comparaison soit déterminant, nous utilisons la même graine pour sélectionner les foyers dans les deux algorithmes, les foyers sélectionnés seront identiques dans les deux algorithmes. Il faut noter que dans le GEEQ, la sélection des clients qui vont réduire leur consommation se fait en fonction de leur nombre de points afin de sélectionner en priorité les clients qui ont le moins de points. Ce critère de sélection permet de faire participer tous les clients. Dans le GEEQ protégé, la sélection des clients se fait de manière aléatoire, en empêchant un client de participer plusieurs fois à la réduction de consommation, ce qui permet aussi de faire participer tous les clients. Ainsi, la différence entre les deux critères de sélection réside uniquement dans l'ordre de participation à la réduction de consommation des parties.

Pendant les expériences, nous supposons que l'étape 3 de réduction de consommation dans le GEEQ et le GEEQ protégé se produit au plus cinq fois. Ce qui correspond à au plus $5 \cdot k$ foyers sollicités pour réduire leurs consommations prévisionnelles. Enfin, nous avons choisi $n = 50$ foyers, ce qui correspond à la taille moyenne d'un quartier.

Nous remarquons que lorsque la somme des consommations prévisionnelles est inférieure à la puissance maximale du réseau local ($a^t = 1$), alors les foyers n'ont pas à réduire leur consommation prévisionnelle dans le GEEQ et le GEEQ protégé. Ainsi, les deux algorithmes ont la même efficacité.

De même, en cas de surconsommation ($a^t = 0$), si la réduction totale de consommation (par $5 \cdot k$ foyers) n'est pas suffisante pour passer en dessous du seuil de puissance maximale du réseau local ($a^t = 0$ après les réductions de consommation), alors l'erreur relative entre les deux algorithmes est nulle. En effet, pour les tests, la sélection des clients dans le GEEQ se fait ici de manière aléatoire et non par rapport au nombre de points des foyers comme décrit

dans l'algorithme 6. Dans l'algorithme 6 la consommation à réduire $\min(\epsilon^t, f_i^t \times p_i^{\max,t})$ par un foyer sélectionné i est égale à $f_i^t \times p_i^{\max,t}$ car le surplus ne peut pas être réduit comme supposé en hypothèse. De même, dans l'algorithme 7, la consommation à réduire par un foyer sélectionné i est de $f_i^t \times p_i^{\max,t}$. D'où l'obtention d'une erreur relative nulle.

Cependant, si après quelques réductions de consommation prévisionnelle, la somme des consommations prévisionnelles des foyers est inférieure à la puissance maximale du réseau local ($a^t = 1$), l'erreur relative entre les deux algorithmes dépend du nombre k de foyers sélectionnés à chaque tour pour réduire leur consommation dans l'algorithme 7.

Plus k est grand, plus l'erreur relative augmente, comme le montre la figure 4.4a. Cette erreur relative dépend du nombre de foyers qui doivent être sollicités pour éviter une surconsommation. La figure 4.4b donne le nombre de réductions de consommation dans le GEEQ protégé en fonction du nombre k de foyers sollicités à chaque tour.

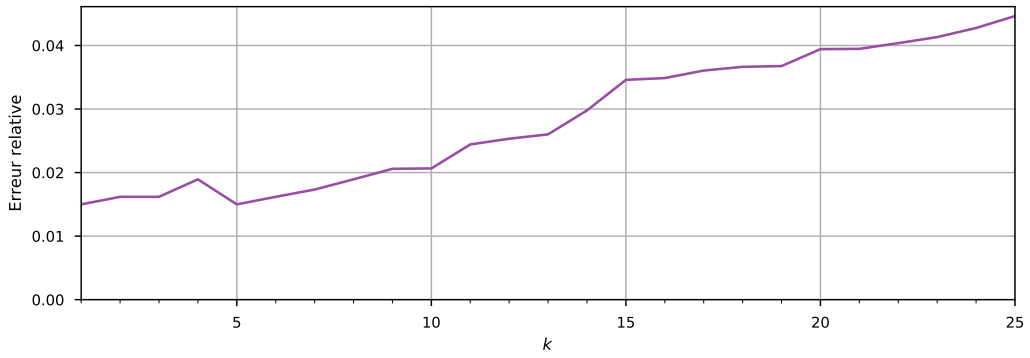
Dans cette expérience, les figures 4.4a et 4.4b montrent que le nombre de foyers nécessaires pour éviter une surconsommation est de 5. En effet quand $k = 1$ et quand $k = 5$, le nombre de foyers total sollicités pour réduire leur consommation est de 5. On peut donc déduire qu'après la réduction de consommation par 5 foyers, la somme des consommations des foyers est inférieure à la puissance maximale du réseau local. Si ce n'était pas le cas alors quand $k = 5$, le nombre de foyers qui aurait été sollicités pour réduire leur consommation devrait être d'au moins 10 (2 tours de réduction) dans le GEEQ protégé.

La figure 4.4a montre que quand k est bien choisi pour que la réduction de consommation ne dépasse pas celle nécessaire ($k = 1$ ou $k = 5$) alors l'erreur relative est entre 1% et 2%.

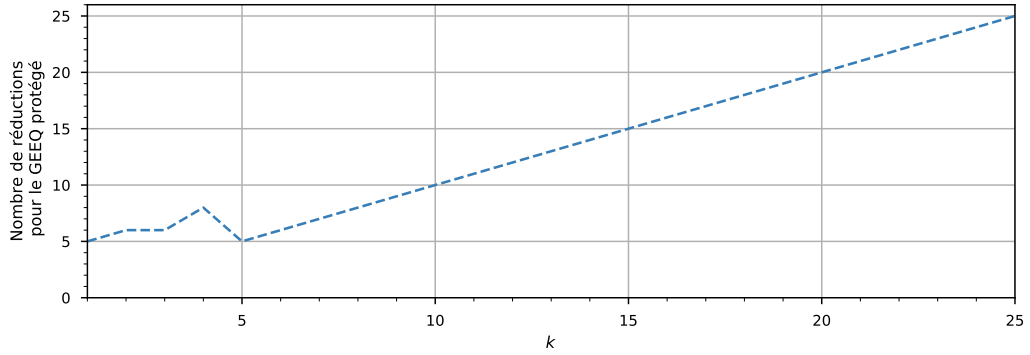
Cette erreur relative est due à l'absence du surplus de consommation dans le calcul de la réduction de consommation dans le GEEQ protégé (algorithme 7). En effet, dans l'algorithme 6 lorsque le surplus e^t de consommation est inférieur à la flexibilité du foyer sélectionné, alors la réduction de consommation $\min(\epsilon^t, f_i^t \times p_i^{\max,t})$ est égale au surplus e^t. Alors que dans l'algorithme 7, la réduction de consommation est toujours fonction de la flexibilité du foyer : $f_i^t \times p_i^{\max,t}$.

Par exemple, dans la figure 4.4a, si $k = 15$, en utilisant le GEEQ protégé, 15 foyers réduisent leur consommation de $f_i^t \times p_i^{\max,t}$. Par contre, dans le GEEQ, après la réduction de consommation par 5 foyers, le surplus devient nul. Ainsi, les 10 autres foyers réduisent leur consommation de $\min(\epsilon^t, f_i^t \times p_i^{\max,t})$. Comme $\epsilon^t = 0$, ce minimum vaut également 0. Dans cette expérience, chaque foyer a une flexibilité f_i^t égale à 15%.

De plus lorsque k n'est pas un diviseur du nombre de foyers nécessaires pour réduire le surplus de consommation, alors cette erreur relative augmente. Par exemple si $k = 4$, dans le GEEQ protégé pendant le premier tour de réduction 4 foyers sont sollicités pour réduire leur consommation. Ensuite, comme le nombre de foyers nécessaires pour éviter le surplus de consommation est de 5 il y a un deuxième tour de réduction de la consommation où 4 autres foyers sont sollicités pour réduire leur consommation ; ce qui fait un total de 8 foyers sollicités pour réduire leur consommation de $f_i^t \times p_i^{\max,t}$ dans le GEEQ protégé. Par contre, pour le GEEQ, après la réduction de consommation par 5 foyers, le surplus ϵ^t est égale à 0 car la réduction de consommation par 5 foyers suffit pour éviter le surplus de consommation. Ainsi donc, les 3 autres foyers réduisent leur consommation de $\min(\epsilon^t, f_i^t \times p_i^{\max,t}) = \epsilon^t = 0$.



(a) Erreur relative – GEEQ vs GEEQ protégé – en fonction de k : évaluation de l'efficacité du GEEQ protégé comparativement au GEEQ.



(b) Nombre de foyers sollicités en fonction du nombre k de foyers sollicités à chaque tour. Dans cet exemple, la réduction nécessite que 5 foyers réduisent leur consommation, c'est pourquoi la courbe est linéaire pour $k \geq 5$.

FIGURE 4.4 – Erreur relative – GEEQ vs GEEQ protégé – en fonction de k, le nombre de foyers sollicités à chaque tour. Nombre de foyers sollicités dans le GEEQ protégé en fonction de k. Dans cet exemple, la réduction nécessite que 5 foyers réduisent leur consommation.

Dans cet exemple, le GEEQ protégé sur-sollicite les foyers, ce qui fait augmenter l'erreur relative.

En conclusion, le choix du nombre k de foyers à solliciter à chaque tour de réduction dans l'algorithme 7 est important.

Plus k est petit, plus le temps de convergence (le temps pour passer en dessous du seuil de puissance maximale) est grand et plus il y a des risques de fuite d'information sur la flexibilité. En effet quand $k = 1$, si après la réduction de la consommation d'un foyer, la somme de consommation devient inférieure à la puissance maximale du réseau local, alors on peut déduire que ce foyer est flexible, sans toutefois connaitre exactement la valeur de sa flexibilité. Plus k est grand, plus l'erreur relative peut être grande, le GEEQ protégé est donc moins efficace.

La figure 4.4a montre que l'erreur relative entre le GEEQ et le GEEQ protégé est tolérable et donc qu'il est possible de réduire les pics de consommation tout en préservant la vie privée.

4.2.2 Analyse de la complexité du GEEQ protégé

Cette section analyse la complexité de l'algorithme 7. Ici, nous nous intéressons aux nombres de multiplications et d'échanges (communications) réalisés par chaque partie. En effet ces opérations sont les plus coûteuses : comme expliqué en section 3.1.2, les additions de secrets et les multiplications par un scalaire peuvent s'effectuer sans communication, c'est-à-dire en un seul « tour », tandis que les multiplications nécessitent de révéler des valeurs, ce qui nécessite des communications. Nous mesurons donc, à chaque étape du GEEQ protégé, le nombre de communications, de multiplications effectuées par chaque foyer, et le nombre de tours nécessaires. Soit ℓ la taille binaire de la consommation prévisionnelle maximale d'un foyer ($\ell = \max_{p_i^t} \log_2(p_i^t)$).

— L'étape 1 nécessite n partages de secrets (n^2 communications).

— L'étape 2 nécessite 1 comparaison et 1 révélation de secret (n communications). La complexité de la comparaison est de $24\ell + 5$ multiplications en $2\ell + 10$ tours de communications comme le montre Burkhart et coll. [24] : les données de consommations sont décomposées en binaire pour effectuer la comparaison.

— À l'étape 3 le choix de k GESH en utilisant le protocole de *coin tossing* requiert 1 révélation d'une valeur aléatoire qui sera utilisée comme graine (n communications). Les autres opérations de l'étape 3a sont calculées localement.

— L'étape 4 requiert 1 communication avec le fournisseur.

Le tableau 4.2 récapitule la complexité de chaque étape.

étape	multiplications	tours	communications
étape 1	0	1	n^2
étape 2	$24\ell + 5$	$2\ell + 10$	$(2\ell + 11)n$
étape 3	0	1	n
étape 4	0	1	1

TABLEAU 4.2 – Complexité de chaque étape de l'algorithme 7

Soit C le nombre de fois où l'étape 3 est calculée (c'est-à-dire le nombre de sollicitations de foyers à réduire leur consommation), la complexité de l'algorithme 7 est alors

$$(C+1)(\text{step}_1) + (C+1)(\text{step}_2) + C(\text{step}_3) + \text{step}_4$$

où step_i pour $i = 1, 2, 3, 4$ est la complexité de l'étape i. La complexité du GEEQ protégé est donc de $O(n^2)$ communications.

Il faut noter que C, le nombre de fois où l'étape 3 est calculée dépend aussi de k, le nombre de GESH sélectionnés pour réduire leur consommation. Plus k est grand, plus C diminue. En considérant les résultats expérimentaux présentés dans la section 4.2, quand $k = 1$ on effectue 5 fois l'étape 3, c'est-à-dire $C = 5$. Par contre, quand $k = 5$, on effectue une seule fois l'étape 3, c'est-à-dire $C = 1$. Dans cet exemple, il est donc plus avantageux de fixer k à 5, afin d'avoir une complexité moindre, tout en réduisant efficacement les pics de consommation (erreur relative entre 1% et 2%).

En outre, il est possible de réduire la complexité en faisant participer moins de foyers (par exemple 5 choisis aléatoirement). Dans ce cas, n ne vaudra plus le nombre de foyers composant le quartier, mais le nombre de foyers participant à l'exécution du SMC. Mais alors, la garantie de sécurité est réduite : si les n foyers participant au SMC collaborent, ils peuvent déduire les valeurs secrètes des autres foyers et donc mettre à mal tous les efforts de protection des DCP des foyers.

4.3 GEEQ protégé résistant à la fraude

Dans cette section, nous proposons une extension du GEEQ protégé résistant à la fraude. En effet dans le GEEQ protégé (algorithme 7), les GESH malveillants peuvent mentir sur le nombre de points gagnés puisque ce nombre est calculé localement. Dans le GEEQ, le nombre de points gagnés par chaque GESH est calculé par le fournisseur, ce qui est possible puisque le fournisseur connaît la prévision de consommation initiale du GESH ainsi que sa prévision de consommation après la réduction. Cette solution n'est pas envisageable pour le GEEQ protégé.

L'algorithme 8 permet de résoudre ce problème. Après avoir calculé leur nombre de points $b'_i = b_i + (p_i^t - p'^t_i) \times c^t$, les clients sélectionnés partagent cette nouvelle valeur $\langle b_i^{'} \rangle$. Ainsi, les GESH disposent de partages $\langle b_i \rangle$, $\langle b'_i \rangle$, $\langle p_i^t \rangle$ et $\langle p'^t_i \rangle$. Ils peuvent donc calculer $\Big\langle (\langle p_i^t \rangle - \langle p'^t_i \rangle) \times c^t == (\langle b'_i \rangle - \langle b_i \rangle) \Big\rangle$ en utilisant l'équation (3.3) et révéler cette valeur, qui vaut 0 si les points ont été calculés correctement et 1 sinon. Si la révélation de cette valeur donne 1, alors le GESH a essayé de tricher, et le fournisseur pourra donc prendre des mesures pour le pénaliser (réduction du nombre de points, etc.).

Cependant, l'algorithme 8 nécessite plus de communication par rapport au GEEQ protégé initial (algorithme 7). En effet, chaque GESH doit partager son nombre de points, sa puissance maximale recommandée et doit effectuer un test d'égalité.

Malgré cette contre-mesure, une autre attaque est encore possible : les GESH malveillants peuvent mentir sur leur consommation prévisionnelle afin de gagner plus de points. Par exemple, si un GESH envoie une prévision de consommation élevée de telle sorte que la consommation prévisionnelle totale soit supérieure à la puissance maximale du réseau, alors ce GESH pourra réduire sa consommation prévisionnelle pour gagner plus de points. Ce genre d'attaque n'est pas spécifique au GEEQ protégé, mais pourrait aussi se produire avec le GEEQ.

Pour empêcher ces attaques, les foyers pourraient révéler les prévisions de consommation effectuées sur de longues périodes (par exemple sur un trimestre) et, si ces prévisions sont trop

Algorithme 8 GEEQ protégé résistant à la fraude

Initialisation : $I = \emptyset$, $\langle b_i \rangle = \langle 0 \rangle$, pour tout $1 \leq i \leq n$
Pour tout $t \in \mathcal{T}$:

1. Chaque GESH $i : 1 \leq i \leq n$ partage sa consommation prévisionnelle p_i^t avec les autres GESH
2. Les n GESH calculent conjointement $\left\langle a^t \right\rangle = \left\langle \sum_{i=1}^{n} \langle p_i^t \rangle \leq (1 - \alpha)\mathcal{P}_{\max} \right\rangle$ et révèlent le résultat a^t
3. Si $a^t = 0$ et $\{1, \ldots, n\} \backslash I \neq \emptyset$, alors
   (a) choisir aléatoirement k GESH $\in \{1, \ldots, n\} \backslash I$, en utilisant un protocole de *coin-tossing*. Le GESH i choisi calcule en parallèle,
      — sa consommation prévisionnelle maximale recommandée : $p'^t_i = p_i^t - f_i^t \times p_i^{\max,t}$
      — son nombre de points : $b'_i = b_i + (p_i^t - p'^t_i) \times c^t$
      — Chaque GESH i partage sa consommation prévisionnelle maximale recommandée p'^t_i et son nouveau nombre de points b'_i avec les autres GESH
   (b) Mise à jour de l'ensemble des GESH qui ont déjà participé : $I = I \cup \{i\}$
   (c) Pour tout GESH i choisi, les n GESH calculent conjointement $\langle \text{verif} \rangle = \left\langle (\langle p_i^t \rangle - \langle p'^t_i \rangle) \times c^t == (\langle b'_i \rangle - \langle b_i \rangle) \right\rangle$ et révèlent le résultat verif
      i. Si verif = 1, mettre à jour la consommation prévisionnelle et le nombre de points du foyer i : $\langle p_i^t \rangle = \langle p'^t_i \rangle$ et $\langle b_i \rangle = \langle b'_i \rangle$ et aller à l'étape 2
      ii. Si verif = 0, alors le GESH i a triché et est considéré comme malveillant
4. Sinon, le GESH 1 (ou un autre GESH) envoie a^t au fournisseur. Ce résultat est la sortie du GEEQ protégé.

À la fin de la période de temps $\mathcal{T}$, chaque GESH révèle son nombre de points b_i au fournisseur

importantes par rapport à la consommation réelle relevée par le compteur sur ce trimestre, les foyers concernés pourraient également être pénalisés.

Cependant, une autre attaque plus approfondie et non spécifique au GEEQ protégé peut être réalisée : les GESH peuvent consommer indépendamment de la prévision effectuée. Ce qui pourrait causer des pics de consommation sur le réseau, et rendre inutile le GEEQ comme le GEEQ protégé.

Pour empêcher cette attaque, les foyers ou GESHs peuvent utiliser des méthodes cryptographiques appelées preuves à divulgation nulle de connaissances (ou *zero-knowledge proofs* en anglais) [150] pour prouver que leurs consommations correspondent bien aux prévisions effectuées, sans que leurs consommations soient révélées.

4.4 Conclusion

Ce chapitre montre la transformation du GEEQ (Gestionnaire d'Énergie de l'Éco-Quartier), algorithme de demande d'effacement à la pointe permettant d'éviter les pics de consommation dans un quartier mais qui collecte les données à caractère personnel des clients, en un algorithme respectueux de la vie privée c'est à dire ne collectant aucune donnée individuelle des clients. Cet algorithme appelé GEEQ protégé utilise le SMC qui donne des garanties élevées de protection de la vie privée. La complexité du GEEQ protégé est de $O(n^2)$ communications.

Les résultats expérimentaux montrent que l'utilité du GEEQ protégé est proche de celle du GEEQ, avec une erreur relative entre 1% et 2% si le paramètre k est bien choisi et entre 4 et 5 dans le pire des cas. Ce qui montre qu'il est possible de concilier la vie privée et l'utilité. Le paramètre k correspond au nombre de foyers sollicités pour réduire/déplacer leur consommation en cas de pic dans le réseau doit être choisi avec délicatesse. Plus k est petit, plus le GEEQ protégé a une efficacité proche du GEEQ, mais plus le temps de convergence (le temps pour passer en dessous du seuil de puissance maximale) est grand, causé par la complexité de la comparaison, et plus il peut avoir des risques de fuite d'information sur la flexibilité. Plus k est grand, plus le temps de convergence diminue, mais plus l'erreur relative peut être grande, des foyers pourront réduire plus ce que ce qui est nécessaire. Il y a donc un compromis à faire entre l'efficacité de la réduction, le temps de calcul et le risque de fuite d'information sur la flexibilité.

Il faut noter que notre approche peut être généralisée à d'autres algorithmes, en effet, le SMC permet d'effectuer des opérations linéaires et non linéaires.

Une des limites du GEEQ protégé est que cet algorithme ne publie pas le résultat de la somme des consommations des foyers afin de protéger les utilisateurs contre les fuites indirectes dont le but est d'obtenir les courbes de charge individuelles des foyers à partir de la somme de courbes de charge. Or, comme présenté dans la section 2.2 du chapitre 2, cette somme est une donnée intéressante. Elle peut permettre de prédire la consommation du quartier et donc d'adapter la production en conséquence.

Pour pallier cette limite, le chapitre suivant utilise la DP (*Differential Privacy*) permettant de publier les sommes de courbes de charge des foyers d'un quartier tout en garantissant que la publication ne donne pas d'informations indirectes sur les courbes de charge individuelles des foyers.

Chapitre 5

Publication de la courbe de charge d'un quartier en protégeant la vie privée des clients

Les agrégats de courbes de charge peuvent être utilisés pour réaliser des prévisions de consommation d'un quartier, une ville ou une région [76, 125]. Ces prévisions de consommation pourront ensuite être utilisées par des élus municipaux afin d'implémenter des algorithmes d'optimisation de la consommation visant à réduire la consommation des communes et donc des émissions de CO_2.

Cependant, ces sommes de consommation ne doivent pas être publiées telles quelles. En effet la publication d'un agrégat (ici la somme) de courbes de charge est vulnérable aux fuites indirectes de données. Buescher et coll. [23] montrent qu'il est possible d'identifier les appareils utilisés dans des foyers à partir d'un agrégat de courbes de charge allant jusqu'à 10 foyers à un pas de temps de 15 min. Plus la taille de l'agrégat augmente, plus le risque d'identification diminue, à cause de la dilution des courbes de charge individuelles dans l'agrégat. Cependant, cette dilution ne garantit pas formellement que les courbes de charge individuelles ne peuvent pas être ré-identifiées à partir de l'agrégat.

Une courbe de charge individuelle est une DCP (donnée à caractère personnel) car elle permet d'identifier directement ou indirectement le foyer associé à cette courbe de charge, en utilisant par exemple des techniques de NALM (*Non-Intrusive Appliance Load Monitoring*) présentées en section 2.3. Ainsi, la publication d'une somme de courbes de charge pose des problèmes de vie privée.

Ce chapitre s'intéresse à la publication des sommes de courbes de charge en garantissant la DP (*Differential Privacy*), présentée en section 3.1.3. La DP donne des garanties formelles permettant de réduire le risque de divulgation indirecte des données individuelles (ici les courbes de charge individuelles) à partir d'un agrégat composé de ces données (par exemple une somme de courbes de charge). Le degré de protection est calibré par un budget de privacy ϵ : plus ce budget est petit, plus les garanties de protection sont élevées. Cependant, cette protection se caractérise par un ajout de bruit sur l'agrégat calculé, ce qui rend souvent cet

agrégat bruité peu utile. En effet, l'agrégat bruité peut souvent être trop différent de l'agrégat non bruité.

Les contributions présentées ici permettent de publier une somme de courbes de charge par un agrégateur (par exemple Enedis) en garantissant la DP, et une bonne utilité. Ces contributions se résument comme suit :

- Nous revisitons l'APF (algorithme de perturbation de Fourier) [130] afin de corriger quelques erreurs entrainant une garantie faible de protection des données de consommation individuelle des foyers. Pour corriger ces erreurs, un facteur $\sqrt{2T}$ doit être rajouté au bruit permettant de garantir la DP, avec T le nombre de points de la courbe de charge publiée. Cependant, cette correction réduit l'utilité annoncée de cet algorithme.
- Nous proposons l'APFB (algorithme de perturbation de Fourier borné), une amélioration de l'APF qui utilise la TFD (transformée de Fourier discrète) et le mécanisme de bornage, ou *clamping*, proposé par McSherry et Mironov [108], permettant de réduire la sensibilité de la somme de courbes de charge à publier. Les résultats expérimentaux montrent une amélioration de l'utilité d'un facteur 6 par rapport à l'APF.
- Nous proposons aussi l'APOB (algorithme de perturbation en ondelettes borné), qui est une adaptation de l'APO (algorithme de perturbation en ondelettes) présenté par Lyu et coll. [106], avec une amélioration de l'utilité d'un facteur 2 par rapport à l'APO.
- Nous comparons ensuite l'APF, l'APO, l'APFB et l'APOB. Puis nous analysons les performances de ces différents algorithmes, notamment leurs erreurs relatives afin d'expliquer pourquoi l'APFB obtient la meilleure utilité.
- Nous montrons comment décentraliser les algorithmes proposés afin de publier un agrégat sans s'appuyer sur un agrégateur centralisé de confiance.

Ce chapitre est structuré comme suit : la section 5.1 présente les préliminaires, notamment l'APF et l'APO. La section 5.2 corrige les erreurs présentes dans l'APF, notamment en calculant correctement une estimation de la sensibilité de la TFD. La section 5.3 donne des détails sur notre technique de publication de séries temporelles respectueuse de la vie privée basée sur le mécanisme de bornage : l'APFB et l'APOB. Ensuite, nous présentons les résultats expérimentaux dans la section 5.4. Finalement, la section 5.5 présente une extension permettant de publier des courbes de charge sans tiers de confiance. La conclusion de ce chapitre est présentée dans la section 5.6.

5.1 Préliminaires

5.1.1 Hypothèses

Dans ce chapitre (sauf indication contraire et explicite), on considère que chaque client possède un compteur communicant capable de collecter sa courbe de charge journalière. Cette courbe de charge est envoyée à un agrégateur, ou un tiers de confiance (par exemple Enedis), qui veut publier la somme de courbe de charge des habitants d'un quartier, d'une

ville ou d'une région, etc. en garantissant que la publication ne divulgue pas indirectement les courbes de charge individuelles des clients.

Soit N le nombre de compteurs communicants, notés SM (*smart meter*) dans la maille considérée (quartier, ville, région, etc.). Soit $X^i = (x_1^i, x_2^i, \ldots, x_T^i)$ la courbe de charge collectée par le SM du client i ($i = 1, \ldots, N$), avec x_t^i sa consommation au pas de temps t ($t = 1, \ldots, T$), où T est l'ensemble des pas de temps considérés. Chaque courbe de charge X^i est envoyée à l'agrégateur qui calcule l'agrégation suivante :

$$\begin{aligned} f &: (\mathbb{R}^T)^N \to \mathbb{R}^T \\ (X^1, \ldots, X^N) &\mapsto S = (S_1, \ldots, S_T) = (\sum_{i=1}^{N} x_1^i, \ldots, \sum_{i=1}^{N} x_T^i). \end{aligned} \tag{5.1}$$

Soient $(X^1, X^2, \ldots, X^N)$ et $(X'^1, X^2, \ldots, X^N)$ deux jeux de données différents en une seule entrée (ici on suppose que X^1 est différent de X'^1). En supposant que la consommation maximale d'un foyer à un pas de temps est M, la L_1-sensibilité de la fonction f est :

$$\begin{aligned} \Delta_1(f) &= \max_{X^1, X^2, \ldots, X^N, X'^1} \left\| f(X^1, X^2, \ldots, X^N) - f(X'^1, X^2, \ldots, X^N) \right\|_1 \\ &= \max \left\| (x_1^1 - x'^1_1, \ldots, x_T^1 - x'^1_T) \right\|_1 \\ &= \max \sum_{j=1}^{T} |x_j^1 - x'^1_j| \\ &= \sum_{j=1}^{T} M \\ &= M \cdot T \end{aligned}$$

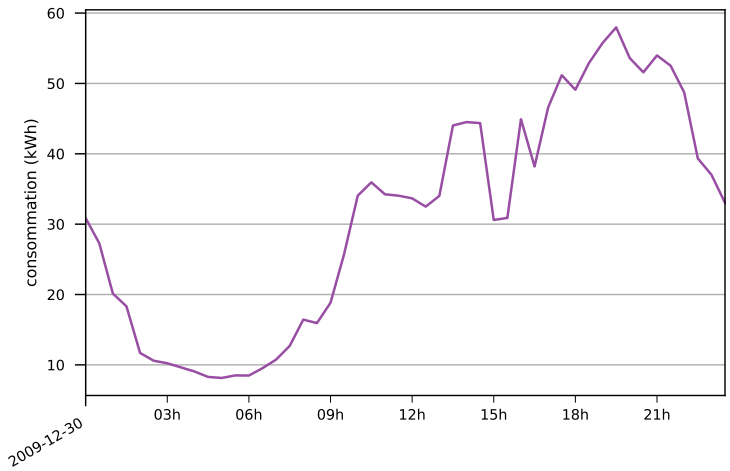
5.1.2 Publication naïve de séries temporelles

Pour publier cette somme S sans divulguer indirectement les consommations individuelles X^i ($i = 1, \ldots, N$), l'agrégateur peut utiliser la DP. Plus précisément, une solution naïve est d'utiliser le mécanisme de Laplace (théorème 3.1.1) en ajoutant un bruit indépendant de Laplace sur chaque composant de S et de publier le résultat :

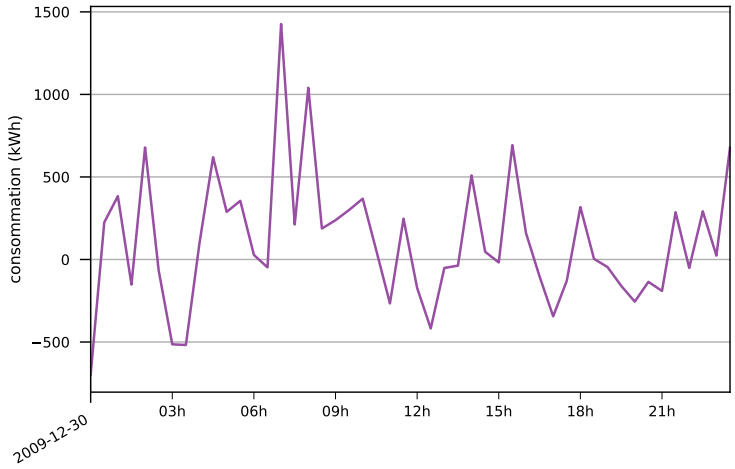
$$\hat{S} = \left(S_1 + \mathcal{L}(\frac{M \cdot T}{\epsilon}), \ldots, S_T + \mathcal{L}(\frac{M \cdot T}{\epsilon}) \right),$$

avec M la consommation maximale du domaine, et $M \cdot T$ la L_1-sensibilité de la somme de la série de consommation. D'après le théorème 3.1.1, cette solution naïve garantit la ϵ-DP.

Cependant, cette approche simple entraine un ajout excessif de bruit et rend l'agrégat inexploitable [53]. Par exemple, les figures 5.1a et 5.1b représentent respectivement la somme de courbes de charge de 50 foyers le 30 décembre 2009 du jeu de données de la CER irlandaise et sa version bruitée en utilisant le mécanisme de Laplace appliqué naïvement. On remarque



(a) somme de courbes de charge



(b) somme de courbes de charge bruitée

FIGURE 5.1 – Somme de courbes de charge de 50 foyers le 30 décembre 2009 du jeu de données de la CER (*Commission for Energy Regulation*) irlandaise et sa version bruitée en utilisant le mécanisme de Laplace appliqué naïvement. Il faut noter que les échelles sont différentes.

dans la figure 5.1b que la courbe de charge bruitée est complètement différente de celle non bruitée de la figure 5.1a : les consommations instantanées bruitées ont des valeurs incohérentes (valeurs négatives), et peuvent avoir des valeurs élevées allant jusqu'à 1 000 kWh, alors que les consommations initiales sont comprises entre 5 et 60 kWh. Pour quantifier l'utilité de

la publication d'une somme de courbes de charge, on peut utiliser l'ERM (erreur relative moyenne) définie ci-dessous.

Définition 5.1.1 *ERM (erreur relative moyenne)*
L'ERM entre deux vecteurs $A = (a_0, \ldots, a_{n-1})$ *et* $B = (b_0, \ldots, b_{n-1})$ *est donnée par :*

$$ERM = \frac{1}{n} \sum_{i=0}^{n-1} \frac{|a_i - b_i|}{a_i + 1} \text{ [1]}$$

L'ERM de la publication de la somme de courbes de charge de l'exemple ci-dessus est de 2 850%. Une erreur acceptable dépend du cas d'usage défini, ainsi il est difficile de fixer le seuil d'erreur à ne pas dépasser. Pour la publication de courbes de charge, nous fixons le seuil acceptable de l'erreur à 10%. Ainsi, l'agrégat bruité obtenu en utilisant cette solution naïve n'est pas utile.

5.1.3 Publication plus adaptée de séries temporelles

D'après la section précédente, rajouter du bruit sur chaque point de la courbe de charge entraine une grande perturbation de celle-ci. Pour réduire ce bruit, une solution est de compresser la courbe de charge en utilisant une autre représentation. Comme le nombre de points conservés diminue (compression), le bruit de Laplace rajouté sera inférieur par rapport au bruit rajouté avec la méthode naïve.

Rastogi et Nath [130] présentent l'APF permettant de réduire le bruit introduit dans le mécanisme de Laplace pour les séries temporelles. Lyu et coll. [106] appliquent l'APF aux séries de courbes de charge et présentent l'APO qui obtient une meilleure utilité par rapport à l'APF.
Ces deux algorithmes consistent à :

1. Transformer la série à publier dans une autre représentation des séries temporelles : la TFD pour l'APF, et la TOD (transformée en ondelettes discrète) pour l'APO.
2. Appliquer le mécanisme de Laplace pour bruiter les premiers coefficients (correspondant aux basses fréquences) de la transformée considérée, et remplacer les autres coefficients par des zéros.
3. Calculer la transformée inverse et renvoyer le résultat.

L'intérêt de cette démarche est d'une part, de conserver la structure temporelle de la courbe de charge. Et de limiter le bruit ajouté en bruitant un nombre réduit de coefficients d'autre part.

Il faut noter que la sensibilité de la transformée considérée doit être évaluée afin d'appliquer le mécanisme de Laplace. Le calcul de la sensibilité est détaillée dans les sections 5.1.5 et 5.2.

En outre, le budget de privacy est optimisé en bruitant uniquement les coefficients représentant les basses fréquences et en remplaçant les autres coefficients par des zéros.

1. le dénominateur est égal à $a_i + 1$ à la place de a_i pour éviter des divisions par 0

Cette démarche permet de diminuer l'erreur due au bruit introduit par le mécanisme de Laplace, mais introduit une erreur de reconstruction causée par le remplacement de certains coefficients de la transformée par des zéros.

Avant de présenter l'APF et l'APO, la section 5.1.4 présente des représentations alternatives de séries temporelles : la transformée de Fourier discrète et la transformée en ondelettes discrète.

5.1.4 Représentations alternatives de séries temporelles

TFD (transformée de Fourier discrète)

La transformée de Fourier discrète permet de transformer un signal du domaine temporel vers le domaine fréquentiel. Soit $X = (x_0, \ldots, x_{n-1})$ un signal de taille n ; la TFD [2] du signal X est le vecteur $C = (c_0, \ldots, c_{n-1})$ de taille n appartenant à $\mathbb{C}$ tel que :

$$c_j = \frac{1}{\sqrt{n}} \sum_{i=0}^{n-1} x_i \exp(\frac{-2\pi i j \sqrt{-1}}{n}) \text{ pour } j = 0, \ldots, n-1 \tag{5.2}$$

La transformée inverse est donnée par l'équation :

$$x_j = \frac{1}{\sqrt{n}} \sum_{i=0}^{n-1} c_i \exp(\frac{2\pi i j \sqrt{-1}}{n}) \text{ pour } j = 0, \ldots, n-1 \tag{5.3}$$

Cette version de la TFD est orthonormale, c'est-à-dire que la transformée a la même norme 2 que le signal initial. En pratique, le calcul de la première moitié des coefficients de la TFD suffit pour représenter un signal à valeurs réelles. En effet on a :

$$c_j = c^*_{n-j} \text{ pour } j = \begin{cases} 1, \ldots, (n-1)/2 & \text{si } n \text{ est impair} \\ 1, \ldots, n/2 - 1 & \text{si } n \text{ est pair} \end{cases}$$

où c^*_{n-j} désigne le complexe conjugué de c_{n-j}.

La figure 5.2 représente la somme de courbes de charge de 50 foyers du jeu de données de la CER irlandaise le 30 décembre 2009, ainsi que les quatre premiers coefficients de sa transformée de Fourier.

TOD (transformée en ondelettes discrète)

Chaque fréquence d'un signal obtenue en utilisant la TFD dépend de tout le signal, ainsi, la TFD ne permet pas de savoir à quelle période de temps correspond une fréquence du signal. Pour résoudre ce problème, une idée est de diviser le signal en plusieurs fenêtres glissantes, et de calculer la TFD correspondant à chaque petite période de temps.

2. Ici nous utilisons la version normalisée de la transformée de Fourier discrète, pour éviter l'erreur de l'article [130], expliquée dans la section 5.2

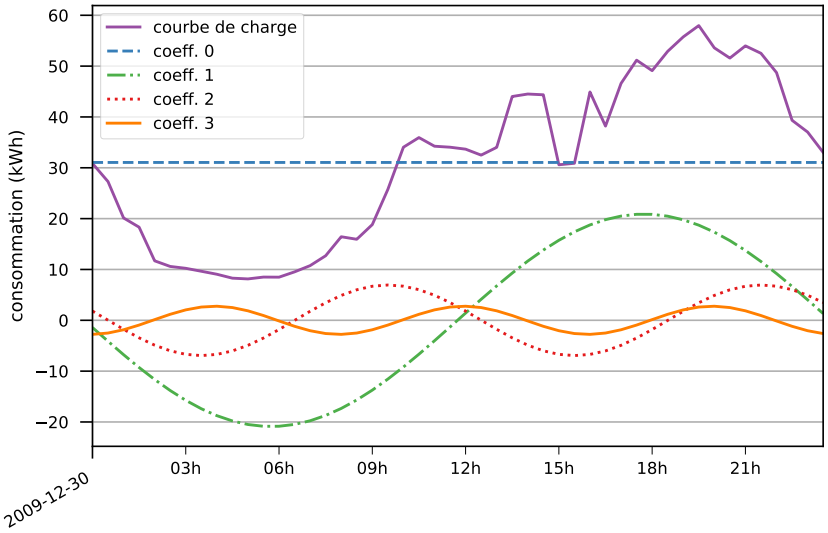


FIGURE 5.2 – représentation de la somme de courbes de charge de 50 foyers le 30 décembre 2009, et des coefficients de sa transformée de Fourier discrète

La TOD (transformée en ondelettes discrète) est une méthode permettant de représenter un signal à la fois dans le domaine fréquentiel et temporel. Les ondelettes ont été introduites pour permettre une bonne représentation temporelle et une mauvaise représentation fréquentielle pour les hautes fréquences, et une bonne représentation fréquentielle et une mauvaise représentation temporelle pour les faibles fréquences [128].

La figure 5.3 détaille la structure temporelle-fréquentielle d'une transformée en ondelettes. On remarque dans la figure 5.3 que la largeur et la hauteur de chaque case varient, mais la surface est la même : chaque case représente une partie égale du plan temps-fréquence, mais avec une résolution temporelle et fréquentielle différente. Les faibles fréquences, correspondent aux cases avec une petite hauteur (ce qui correspond à une bonne résolution fréquentielle, car il y a moins d'ambigüité sur la valeur de la fréquence exacte) mais une grande largeur (ce qui correspond à une mauvaise résolution temporelle, car il y a une grande ambiguïté concernant la valeur exacte du temps). Les hautes fréquences quant à elles sont représentées par les cases avec une grande hauteur et une petite largeur, ce qui correspond respectivement à une mauvaise résolution fréquentielle et une bonne résolution temporelle.

Ainsi, il est possible de savoir à quelle période de temps apparaît une fréquence donnée du signal. Cette transformation est orthonormale, et est généralement utilisée pour analyser les courbes de charge [115].

La figure 5.4 représente la courbe de charge présentée dans la section précédente, ainsi que les quatre premiers coefficients de sa représentation en ondelettes de Daubechies 2. On remarque que le coefficient 3 représente le pic entre 10 h et 18 h.

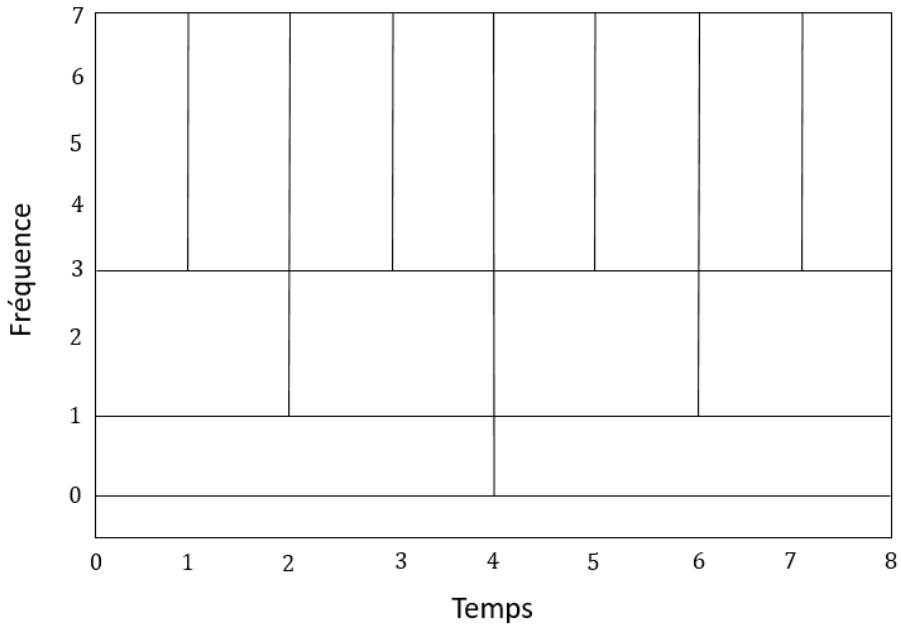


FIGURE 5.3 – Représentation temporelle et fréquentielle d'une transformée en ondelettes

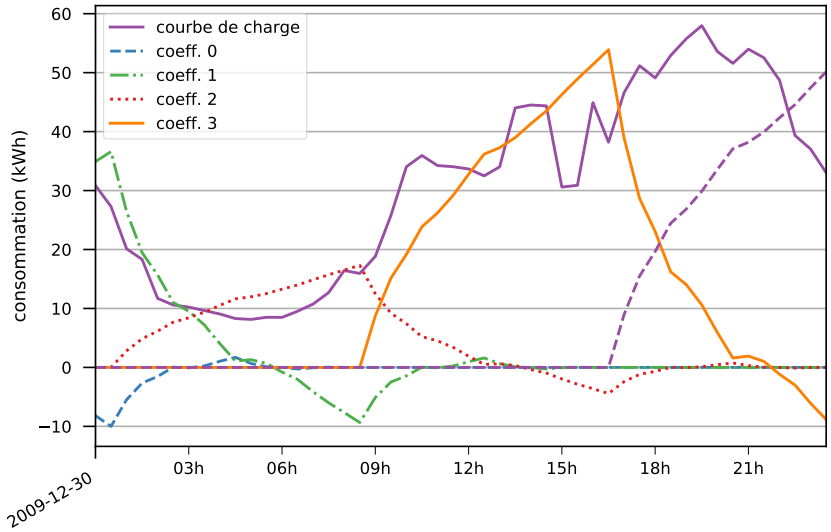


FIGURE 5.4 – représentation de la somme de courbes de charge de 50 foyers le 30 décembre 2009 et des coefficients de sa transformée en ondelettes discrète.

Il existe plusieurs types d'ondelettes. Dans ce chapitre, nous utilisons les ondelettes de Haar et de Daubechies, qui sont généralement utilisées pour décomposer les courbes de charge[115]. Nous montrons dans la section 5.4 que les ondelettes de Haar et de Daubechies permettent de mieux compresser l'information contenue dans une courbe de charge par rapport à d'autres types d'ondelettes. C'est-à-dire, qu'en conservant un nombre restreint de coefficients de la transformée, la transformée inverse de la série compressée reste proche de la courbe de charge initiale. Cette erreur liée à cette compression est appelée erreur de reconstruction, et est formalisée dans la section 5.4.1.

La transformée en ondelettes prend en entrée un signal, et renvoie des coefficients d'ondelettes. Ces coefficients sont de deux types : coefficients d'approximation qui correspondent aux basses fréquences, et les coefficients de détails qui correspondent aux hautes fréquences. Le nombre de coefficients d'approximation et de détail dépend du niveau de la transformation. Le premier niveau consiste à calculer la transformée en ondelettes en prenant en entrée le signal initial. Dans ce premier niveau, il y a autant de coefficients d'approximation que de coefficients de détail. Le niveau suivant s'obtient en appliquant à nouveau la transformée en ondelettes sur les coefficients d'approximation et en conservant les coefficients de détail obtenus lors du premier niveau. Plus le niveau augmente, plus le nombre de coefficients de détail augmente, et le nombre de coefficients d'approximation diminue. Le dernier niveau correspond à celui qui a un seul coefficient d'approximation. Par exemple, les différents niveaux de la transformée de Haar de la série $(10; 12; 16; 20; 8; 14; 3; 7)$ sont donnés par la figure 5.5

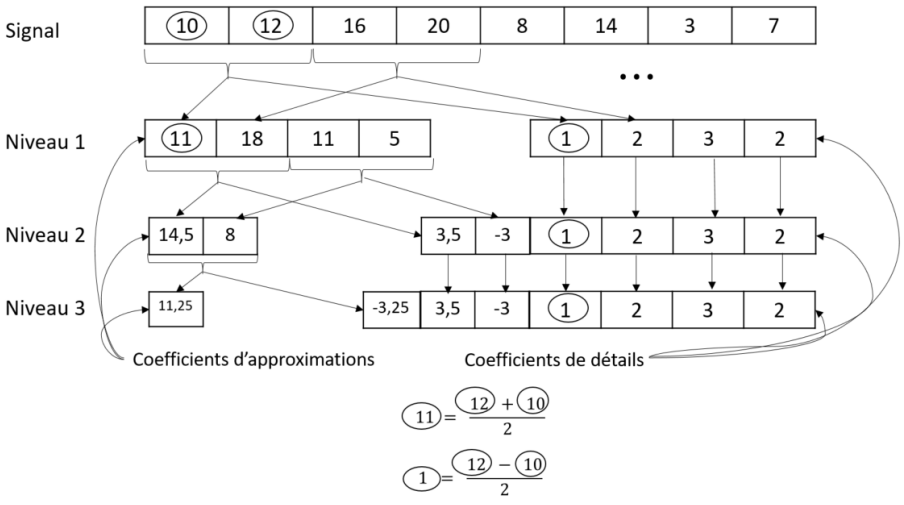


FIGURE 5.5 – Transformée en ondelettes de Haar.

La transformée de Haar est obtenue en calculant successivement des moyennes et des différences des coefficients précédents. Par exemple, pour le niveau 1, le premier coefficient d'approximation est $\frac{12+10}{2} = 11$ et le premier coefficient de détail est $\frac{12-10}{2} = 1$. La transformée de Haar de niveau 1 de la série $(10; 12; 16; 20; 8; 14; 3; 7)$ est $(11; 18; 11; 5; 1; 2; 3; 2)$ comprenant 4

coefficients d'approximations (les 4 premiers) et 4 coefficients de détails (les 4 derniers).

Pour passer au niveau suivant, la transformée est appliquée sur les coefficients d'approximations, et les coefficients de détails restent inchangés. La transformée de Haar finale ou de niveau 3 est $(11, 25; -3, 25; 3, 5; -3; 1; 2; 3; 2)$ qui possède 1 seul coefficient d'approximation $(11, 25)$ et 7 coefficients de détails. Il faut noter que ce coefficient d'approximation est égal à la moyenne de la série initiale.

La transformée inverse consiste à calculer des différences et des sommes entre les coefficients d'approximations et de détails. Par exemple on a : $11, 25 - (-3, 25) = 14, 5$ et $11, 25 + (-3, 25) = 8$. La transformée inverse de Haar des coefficients $(11; 18; 11; 5; 1; 2; 3; 2)$ est donnée par la figure 5.6. Pour plus d'information sur les ondelettes, les lecteurs peuvent consulter [146].

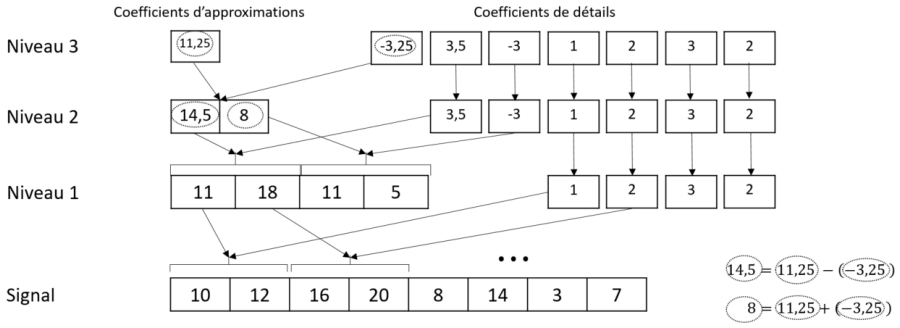


FIGURE 5.6 – Transformée en ondelettes inverse de Haar.

Maintenant que nous avons présenté la TFD et la TOD, nous pouvons détailler les algorithmes de perturbation des séries temporelles : l'algorithme de perturbation de Fourier et l'algorithme de perturbation en ondelettes.

5.1.5 Algorithmes de perturbation de séries temporelles

En utilisant la DP et des représentations alternatives de courbes de charge, cette section présente l'idée générale permettant de publier une somme de courbes de charge $S = (s_1, \ldots, s_T)$ de plusieurs foyers pendant un ensemble de pas de temps T (par exemple $T = 48$ pour une journée en considérant un pas de temps de 30 min). Cette approche a été premièrement utilisée par Rastogi et Nath [130].

La première étape consiste à transformer la courbe de charge S dans une autre représentation en utilisant une transformée orthonormale, c'est-à-dire que la transformée a la même norme 2 que la série initiale. Par exemple en utilisant la TFD, on obtient comme résultat $C = (c_1, \ldots, c_T) = \text{TFD}(S)$. On note que la TFD peut être remplacée par d'autres transformées orthonormales (comme la transformée en ondelettes).

La deuxième étape permet de gagner en budget de privacy. Seuls les k premiers coefficients de la transformée sont conservés. Les autres coefficients sont remplacés par des zéros. On

note :

$$C_k = (c_1, \ldots, c_k, 0, \ldots, 0).$$

L'ignorance des $T-k$ derniers coefficients de la transformée dans cette étape est une première source d'erreur pour la courbe de charge publiée, et est appelée erreur de reconstruction.

La troisième étape consiste alors à bruiter les k coefficients conservés en utilisant le mécanisme de Laplace, afin de garantir la DP. Pour appliquer le mécanisme de Laplace, une méthode consiste à calculer la sensibilité de la transformée (ou un majorant de la sensibilité). Cela donne :

$$\widehat{C}_k = C_k + \left(\mathcal{L}\left(\frac{\Delta \text{TFD}}{\epsilon}\right), \ldots, \mathcal{L}\left(\frac{\Delta \text{TFD}}{\epsilon}\right), 0, \ldots, 0 \right).$$

Cette perturbation est une d'autre source d'erreur pour la courbe de charge publiée, appelée erreur de perturbation.

Enfin, en calculant la TFDI (transformée de Fourier discrète) de $\widehat{C}_k$, on obtient la courbe de charge bruitée de S :

$$\widehat{S} = (\hat{s}_1, \ldots, \hat{s}_T) = \text{TFDI}(\widehat{C}_k).$$

Les sections suivantes détaillent cette technique pour les transformées présentées ci-dessus : la TFD et la TOD.

APF (algorithme de perturbation de Fourier)

L'APF (algorithme de perturbation de Fourier) présentée premièrement dans [4, 106, 130] prend en entrées la courbe de charge à publier $S = (s_1, \ldots, s_T)$, $k \ll T$ le nombre de coefficients de la TFD à conserver, M la consommation maximale du domaine, le budget de privacy ϵ, et renvoie la courbe de charge bruitée $\widehat{S} = (\hat{s}_1, \ldots, \hat{s}_T)$ comme le montre l'algorithme 9. Rastogi et Nath [130] montrent que l'APF (Algorithme 9) garantit la DP grâce au théorème suivant :

Théorème 5.1.1 *L'APF (algorithme de perturbation de Fourier) garantit la ϵ-confidentialité différentielle [130].*

Démonstration 5.1.1 *Soit f la fonction définie en (5.1), qui prend en entrée N courbes de charges et qui renvoie leur somme notée S. Comme la TFD est orthonormale, S et sa transformée $C = \text{TFD}(S)$ ont la même norme 2. De plus, on a $\|C_k\|_2 \leq \|C\|_2 = \|S\|_2$ car C_k contient les k premiers coefficients de C et $T-k$ zéros. D'après l'inégalité des normes de Cauchy-Schwarz, on a $\|C_k\|_1 \leq \sqrt{k}\,\|C_k\|_2 \leq \sqrt{k}\,\|S\|_2$. Ainsi, la L_1-sensibilité de la fonction qui renvoie les premiers coefficients de la TFD est inférieure ou égale à $\sqrt{k}$ multipliée par la L_2-sensibilité de la courbe de charge S : $\Delta_1 \text{TFD}^k \leq \Delta_2(f)$, où TFD^k désigne la fonction qui renvoie les k premiers coefficients de la TFD de S. En notant M la consommation maximale du domaine, alors $\Delta_2(f) = \sqrt{\sum_{i=1}^{T} M^2} = M\sqrt{T}$. On obtient alors : $\Delta_1(\text{TFD}^k) = M\sqrt{Tk}$. Ainsi, d'après le mécanisme de Laplace, le calcul de $\widehat{C}_k$ garantit la ϵ-confidentialité différentielle. Comme le post-traitement d'un mécanisme qui garantit la ϵ-confidentialité différentielle garantit aussi la ϵ-confidentialité différentielle, alors $\widehat{S} = \text{TFDI}(\widehat{C}_k)$ garantit aussi la ϵ-confidentialité différentielle.*

Algorithme 9 APF (algorithme de perturbation de Fourier)

Entrées :

- $S = (s_1, \ldots, s_T)$: courbe de charge à publier
- k : nombre de coefficients de la TFD à conserver
- M : consommation maximale du domaine
- ϵ : budget de privacy

Algorithme :

1. Calculer la TFD de S :
$$C = (c_1, \ldots, c_T) = \text{TFD}(S).$$
2. Garder uniquement les k premiers coefficients de C et remplacer les autres coefficients par des zéros :
$$C_k = (c_1, \ldots, c_k, 0, \ldots, 0).$$
3. Calculer la version bruitée de C_k, notée $\widehat{C}_k$ en bruitant les k premiers coefficients de C_k par un bruit de Laplace $\mathcal{L}(\frac{\Delta_2(S)\sqrt{k}}{\epsilon})$, avec $\Delta_2(S) = M\sqrt{T}$ la sensibilité liée à la norme 2 de S :
$$\widehat{C}_k = C_k + \left(\mathcal{L}(\frac{M\sqrt{Tk}}{\epsilon}), \ldots, \mathcal{L}(\frac{M\sqrt{Tk}}{\epsilon}), 0, \ldots, 0 \right)$$
4. Calculer la transformée de Fourier inverse de $\widehat{C}_k$ et renvoyer le résultat :
$$\widehat{S} = (\hat{s}_1, \ldots, \hat{s}_T) = \text{TFDI}(\widehat{C}_k).$$

Sortie : Courbe de charge bruitée $\widehat{S} = (\hat{s}_1, \ldots, \hat{s}_T)$

La figure 5.7 donne un exemple d'une courbe de charge bruitée de 50 foyers sur une semaine, du 30 décembre 2009 au 6 janvier 2010, du jeu de données de la CER irlandaise en utilisant l'algorithme de perturbation de Fourier avec un budget de privacy de $\epsilon = 1$, et $k = 5$ pour chaque journée. Dans cette figure on remarque que la forme de la courbe de charge est globalement préservée, malgré une erreur relative moyenne encore élevée de 45%.

Cependant, il y a quelques erreurs dans la démonstration du théorème 5.1.1, ce qui ne permet pas d'affirmer que l'algorithme 9 garantit la ϵ-confidentialité différentielle. Dans [130], la TFD utilisée n'était pas normalisée, c'est-à-dire que $\|C\|_2 = \sqrt{T}\,\|S\|_2$. En outre, la démonstration du théorème 5.1.1 applique le mécanisme de Laplace aux coefficients de la transformée qui sont des nombres complexes et non pas des nombres réels. Ces erreurs sont détaillées et corrigées dans la section 5.2.

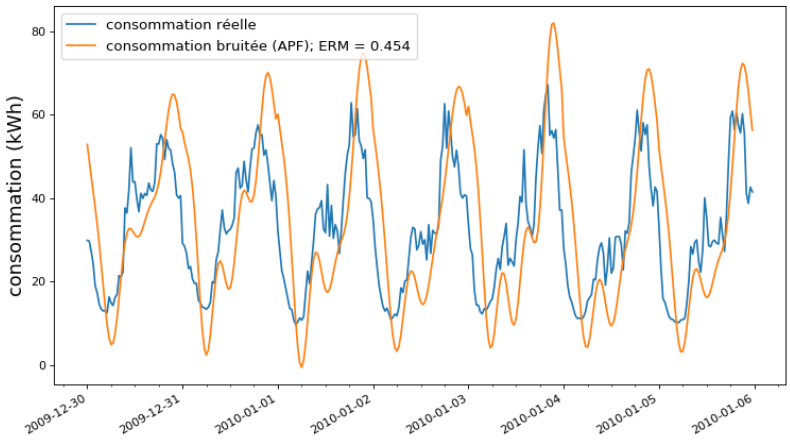


FIGURE 5.7 – somme de courbes de charge bruitée de 50 foyers, du 30 décembre 2009 au 6 janvier 2010 du jeu de données de la CER irlandaise en utilisant l'algorithme de perturbation de Fourier [130] avec un budget de privacy de $\epsilon = 1$, et $k = 5$ pour chaque journée.

APO (algorithme de perturbation en ondelettes)

En remplaçant la TFD par la TOD dans l'algorithme 9, Lyu et coll. [106] proposent l'APO (algorithme de perturbation en ondelettes), et montre que l'APO obtient une meilleure utilité que l'APF. L'APO est présenté dans l'algorithme 10

Le Théorème 5.1.2 montre que l'APO garantit la ϵ-confidentialité différentielle.

Théorème 5.1.2 *L'APO (algorithme de perturbation en ondelettes) garantit la ϵ-confidentialité différentielle.*

Démonstration 5.1.2 *Soit f la fonction définie en* (5.1)*, qui prend en entrée N courbes de charges et qui renvoie leur somme notée S. On note TOD^k la fonction qui renvoie uniquement les k premiers coefficients de la transformée en ondelettes considérée. Comme la TOD est orthonormale [146], $C = \mathrm{TOD}(S)$ et S ont la même norme 2, et $\Delta_2(\mathrm{TOD}) = \Delta_2(f)$, ainsi $\Delta_2(\mathrm{TOD}^k) \leq \Delta_2(f)$ (parce que $T - k$ coefficients de la TOD sont remplacés par des zéros). De plus, avec l'inégalité des normes, $\Delta_1(\mathrm{TOD}^k) \leq \sqrt{k}\Delta_2(\mathrm{TOD}^k)$. Ainsi, $\Delta_1(\mathrm{TOD}^k) \leq \sqrt{k}\Delta_2(f) = M\sqrt{kT}$. Le bruit introduit à l'étape 3 de l'algorithme 10 est donc justifié et l'APO garantit la ϵ-confidentialité différentielle.*

La figure 5.8 donne un exemple d'une courbe de charge bruitée de 50 foyers sur une semaine, du 30 décembre 2009 au 6 janvier 2010 du jeu de données de la CER irlandaise en utilisant l'algorithme de perturbation en ondelettes de Haar de niveau 5, avec un budget de privacy de $\epsilon = 1$, et $k = 5$ pour chaque journée. De même, comme dans la figure 5.7, la

Algorithme 10 APO (algorithme de perturbation en ondelettes)

Entrées :

- $S = (s_1, \ldots, s_T)$: courbe de charge à publier
- k : nombre de coefficients de la TOD à conserver
- M : consommation maximale du domaine
- ϵ : budget de privacy

Algorithme :

1. Calculer la TOD de S :
$$C = (c_1, \ldots, c_T) = \text{TOD}(S).$$
2. Garder uniquement les k premiers coefficients de C et remplacer les autres coefficients par des zéros :
$$C_k = (c_1, \ldots, c_k, 0, \ldots, 0).$$
3. Calculer la version bruitée de C_k, notée $\widehat{C}_k$ en bruitant les k premiers coefficients de C_k par un bruit de Laplace $\mathcal{L}(\frac{\Delta_2(S)\sqrt{k}}{\epsilon})$, avec $\Delta_2(S) = M\sqrt{T}$ la sensibilité liée à la norme 2 de S :
$$\widehat{C}_k = C_k + \left(\mathcal{L}\left(\frac{M\sqrt{Tk}}{\epsilon}\right), \ldots, \mathcal{L}\left(\frac{M\sqrt{Tk}}{\epsilon}\right), 0, \ldots, 0\right)$$
4. Calculer la transformée en ondelettes inverse de $\widehat{C}_k$ et renvoyer le résultat :
$$\widehat{S} = (\hat{s}_1, \ldots, \hat{s}_T) = \text{TODI}(\widehat{C}_k).$$

Sortie : courbe de charge bruitée $\widehat{S} = (\hat{s}_1, \ldots, \hat{s}_T)$

forme de la courbe de charge bruitée est globalement préservée, mais avec une erreur relative moyenne encore élevée de 30%.

5.2 Erreur dans l'APF (algorithme de perturbation de Fourier) [130]

Rastogi et Nath [130] montrent que l'APF (Algorithme 9) garantit la ϵ-confidentialité différentielle (Théorème 5.1.1). Cependant, il y a quelques erreurs dans la preuve de ce théorème, plus précisément dans l'approximation de la sensibilité de la TFD. Les auteurs montrent que la L_1-sensibilité de la TFD est de $M\sqrt{Tk}$, alors qu'elle devrait être de $MT\sqrt{2k}$. Cette section détaille ces erreurs ainsi que comment y remédier.

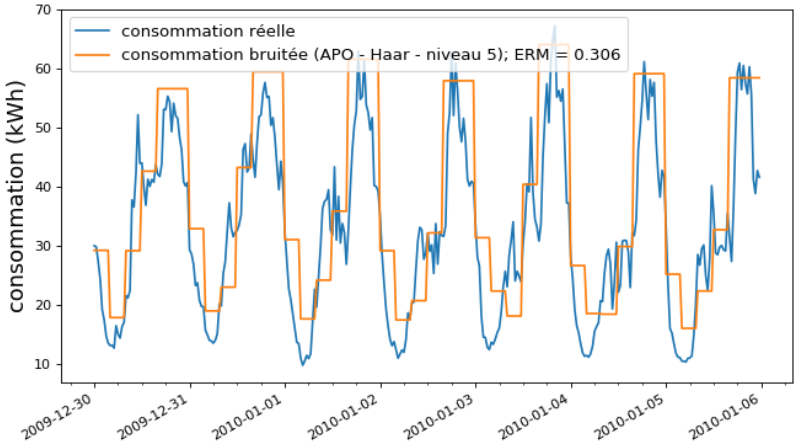


FIGURE 5.8 – somme de courbes de charge bruitée de 50 foyers du 30 décembre 2009 au 6 janvier 2010, du jeu de données de la CER irlandaise en utilisant l'algorithme de perturbation en ondelettes de Haar de niveau 5, avec un budget de privacy de $\epsilon = 1$, et $k = 5$ pour chaque journée.

5.2.1 Première erreur : choix de la TFD (transformée de Fourier discrète)

La version de la TFD (équations 5.2 et 5.3) présentée dans la section 5.1.4 est normalisée, c'est à dire que $\|\text{TFD}(S)\|_2 = \|S\|_2$. Une autre version, non normalisée, existe en remplaçant $1/\sqrt{T}$ par 1 dans la TFD (équation 5.2) et $1/\sqrt{T}$ par $1/T$ dans l'inverse de la TFD (équation 5.3). Cette version non normalisée de la TFD est utilisée dans [4, 106, 130]. Dans cette version à la place d'avoir l'égalité des normes 2 entre S et sa TFD, on a : $\|\text{TFD}(S)\|_2 = \sqrt{T}\,\|S\|_2$ (Théorème de Parseval). Ainsi, en utilisant cette version, la L_1-sensibilité de la TFD serait $MT\sqrt{k}$ à la place de $M\sqrt{Tk}$. Ceci est la première erreur faite dans [4, 106, 130].

5.2.2 Deuxième erreur : mauvaise approximation de la sensibilité de la TFD (transformée de Fourier discrète)

Dans [4, 106, 130], le mécanisme de Laplace est appliqué uniquement sur la partie réelle des coefficients de la TFD, qui sont à valeurs complexes. Or, la partie imaginaire de ces coefficients doit aussi être prise en compte dans le mécanisme de Laplace. Ainsi $2k$ valeurs, à la place de k, doivent être bruitées. En outre, le mécanisme de Laplace s'applique uniquement à des fonctions à valeurs réelles, les coefficients de la TFD doivent être vus comme des éléments de $\mathbb{R}^2$.

Soit TFD^k la fonction qui prend en entrée une courbe de charge S et renvoie les k premiers coefficients de la TFD de S. Cette fonction peut être vue comme $\text{TFD}^k : \mathbb{R}^T \longrightarrow \mathbb{R}^{2k}$

une fonction qui renvoie les parties réelles et imaginaires des k premiers coefficients de la TFD de S. Cette fonction est à valeurs réelles, ainsi, nous pouvons appliquer le mécanisme de Laplace afin de la rendre ϵ-différentiellement confidentielle. Mais avant, nous devons calculer la sensibilité de cette fonction.

Lemme 5.2.1 *Soit* TFD^k *la fonction définie comme suit :*

$$\begin{aligned}\mathrm{TFD}^k : \mathbb{R}^T &\longrightarrow \mathbb{R}^{2k} \\ S &\longmapsto ((a_1, b_1), \ldots, (a_k, b_k))\end{aligned}$$

On note $c_j = a_j + b_j\sqrt{-1}$ *le* j^e *coefficients de la* TFD *de* S*, avec* $i^2 = -1$ *et* $j = 1, \ldots, k$*.* a_j *et* b_j *représentent respectivement la partie réelle et imaginaire de* c_j*.*

La L_1*-sensibilité de* TFD^k *est égale à* $M\sqrt{2Tk}$ *avec* M *la consommation maximale du domaine.*

Démonstration 5.2.1 *Soit la fonction* TFD^k *définie comme dans le lemme 5.2.1.*

$$\begin{aligned}\left\|\mathrm{DFT}^k(S)\right\|_1 &= \|(a_1, b_1, \ldots, a_k, b_k)\|_1 \\ &= |a_1| + |b_1| + \cdots + |a_k| + |b_k| \\ &= \sum_{j=1}^{k} \left\|(a_j, b_j)\right\|_1 \\ &\leq \sqrt{2} \sum_{j=1}^{k} \left\|(a_j, b_j)\right\|_2 \ \textit{inégalité des normes de Minkowski} \\ &= \sqrt{2} \sum_{j=1}^{k} \sqrt{a_j^2 + b_j^2} \\ &= \sqrt{2} \sum_{j=1}^{k} |c_j| \\ &= \sqrt{2}\, \|(c_1, \ldots, c_k)\|_1 \\ &\leq \sqrt{2}\sqrt{k}\, \|(c_1, \ldots, c_k)\|_2 \ \textit{inégalité des normes de Minkowski} \\ &\leq \sqrt{2k}\, \|S\|_2 \ \textit{égalité de la norme 2 entre } S \textit{ et } \mathrm{DFT}(S) \ [3]\end{aligned}$$

Ainsi :

$$\Delta_1(\mathrm{DFT}^k) \leq \sqrt{2k}\Delta_2(S) \ [4]$$

3. Ce résultat est vrai quand la version normalisée de la TFD est utilisée (5.2) comme dans notre cas. Dans [4, 106, 130], la norme 2 des coefficients de la TFD est égale à $\sqrt{T}$ fois la norme 2 de S (Théorème de Parseval).

4. Ce résultat est vrai quand la version normalisée de la TFD est utilisée (5.2). Quand la version non normalisée de la TFD est utilisée, comme dans [4, 106, 130], la L_1 sensibilité des k premiers coefficients de la TFD est $\Delta_1(\mathrm{TFD}^k) = \sqrt{T} \times M\sqrt{2Tk} = MT\sqrt{2k}$ à la place de $M\sqrt{Tk}$.

Ainsi, la sensibilité de la fonction qui renvoie les k premiers coefficients de la TFD est égale à $M\sqrt{2Tk}$ à la place de $M\sqrt{Tk}$. D'après le mécanisme de Laplace (Théorème 3.1.1), la fonction :

$$\begin{array}{rccc} \tilde{\mathrm{TFD}}^k : & \mathbb{R}^T & \to & \mathbb{R}^{2k} \\ & S & \mapsto & \tilde{\mathrm{TFD}}(\mathrm{S}) = ((a_1, b_1), \ldots, (a_k, b_k)) + ((y_{1,1}, y_{1,2}), \ldots, (y_{k,1}, y_{k,2})) \end{array}$$

garantit la ϵ-confidentialité différentielle, avec $y_{j,\ell} = \mathcal{L}(\frac{M\sqrt{2Tk}}{\epsilon})$ pour $j = 1, \ldots, k$ et $\ell = 1, 2$. Pour des raisons de simplicité, dans la suite nous écrirons $c_j + \mathcal{L}(\frac{M\sqrt{2Tk}}{\epsilon})$ à la place de $(a_j, b_j) + (\mathcal{L}(\frac{M\sqrt{2Tk}}{\epsilon}), \mathcal{L}(\frac{M\sqrt{2Tk}}{\epsilon}))$, signifiant que deux bruits indépendants de Laplace $\mathcal{L}(\frac{M\sqrt{2Tk}}{\epsilon})$ sont ajoutés respectivement aux parties réelle et imaginaire de c_j. L'algorithme 11 décrit l'APF modifié. Dans cet algorithme, la TFD utilisée est normalisée.

Algorithme 11 APF (algorithme de perturbation de Fourier) modifié

Entrées :

- $S = (s_1, \ldots, s_T)$: courbe de charge à publier
- k : nombre de coefficients de la TFD à conserver
- M : consommation maximale du domaine
- ϵ : budget de privacy

Algorithme :

1. Calculer la TFD de S :
$$C = (c_1, \ldots, c_T) = \mathrm{TFD}(S).$$
2. Garder uniquement les k premiers coefficients de C et remplacer les autres coefficients par des zéros :
$$C_k = (c_1, \ldots, c_k, 0, \ldots, 0).$$
3. Calculer la version bruitée de C_k, notée $\widehat{C}_k$ en bruitant les k premiers coefficients de C_k par un bruit de Laplace $\mathcal{L}(\frac{\Delta_2(S)\sqrt{k}}{\epsilon})$, avec $\Delta_2(S) = M\sqrt{T}$ la sensibilité liée à la norme 2 de S :
$$\widehat{C}_k = C_k + \left(\mathcal{L}\left(\frac{M\sqrt{2Tk}}{\epsilon}\right), \ldots, \mathcal{L}\left(\frac{M\sqrt{2Tk}}{\epsilon}\right), 0, \ldots, 0\right)$$
4. Calculer la transformée de Fourier inverse de $\widehat{C}_k$ et renvoyer le résultat :
$$\widehat{S} = (\hat{s}_1, \ldots, \hat{s}_T) = \mathrm{TFDI}(\widehat{C}_k).$$

Sortie : Courbe de charge bruitée $\widehat{S} = (\hat{s}_1, \ldots, \hat{s}_T)$

Par la suite, APF désigne la version modifiée, qui garantit effectivement la ϵ-confidentialité différentielle. La figure 5.9 donne un exemple d'une courbe de charge bruitée de 50 foyers sur

une semaine, du 30 décembre 2009 au 6 janvier 2010 du jeu de données de la CER irlandaise en utilisant l'Algorithme 11, avec un budget de privacy de $\epsilon = 1$, et $k = 5$ pour chaque journée. On remarque une perte d'utilité significative par rapport à la figure 5.7, avec une erreur relative moyenne passant de 45% à 361%, d'où une perte d'un facteur 8.

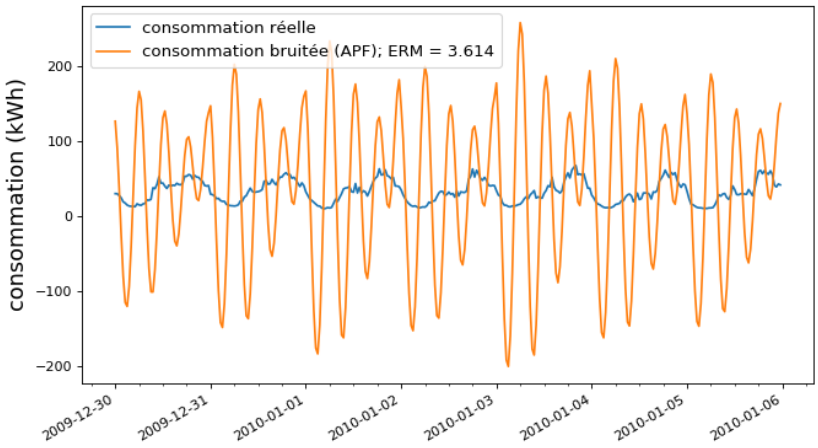


FIGURE 5.9 – somme de courbes de charge bruitée de 50 foyers du 30 décembre 2009 au 6 janvier 2010, du jeu de données de la CER irlandaise en utilisant l'algorithme de perturbation en ondelettes de Haar de niveau 5, avec un budget de privacy de $\epsilon = 1$, et $k = 5$ pour chaque journée.

L'APF n'est donc pas utile pour ce cas d'usage (publication de courbes de charge de 50 foyers avec un budget global de $\epsilon = 1$.

5.3 Algorithmes de perturbation bornés

Le bruit de Laplace introduit dans les coefficients des transformées permet de garantir la confidentialité différentielle au prix d'une perte d'utilité. En remarquant que ce bruit dépend de la sensibilité de la fonction calculée (transformée de Fourier ou d'ondelettes), cette section propose des algorithmes de perturbation bornés visant à réduire l'amplitude du bruit de Laplace en bornant les coefficients de la transformée considérée à un seuil fixé par apprentissage. La figure 5.10 décrit ces algorithmes de perturbation bornés.

Pour trouver le seuil des coefficients de la transformée (TFD, ou TOD) à ne pas dépasser, nous avons divisé notre jeu de données en deux parties égales : D_1 comprenant les consommations des $N/2$ premiers consommateurs, et D_2 la base de données des $N/2$ derniers consommateurs, où N est le nombre de clients de la base de données. Ensuite, nous calculons la distribution des modules des coefficients de la transformée des courbes de charge

FIGURE 5.10 – Descriptif des algorithmes de perturbation bornés

de la base D_1. En enlevant les valeurs extrêmes, nous pouvons définir le seuil de chaque coefficient de la transformée à ne pas franchir.

Par exemple, en utilisant le jeu de données de la CER, la distribution des coefficients de la TFD des consommations des $N/2$ premiers consommateurs est donnée par la figure 5.11, où les cercles représentent les valeurs extrêmes. D'après la figure 5.11, une approximation des

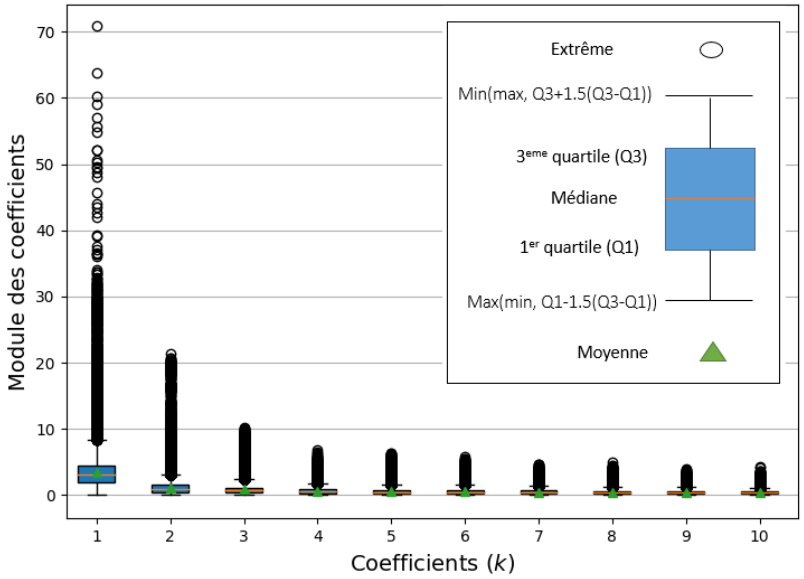


FIGURE 5.11 – Distribution des coefficients de la TFD (transformée de Fourier discrète) de la courbe de charge des $N/2$ premiers consommateurs du jeu de données de la CER.

valeurs maximales des modules des 5 premiers coefficients est $M = (M_1, M_2, M_3, M_4, M_5) = (9, 4, 3, 2, 2)$.

Ainsi, avant d'appliquer les algorithmes de perturbation (APF, APO), on vérifie que les coefficients des transformées des courbes de charge sont inférieurs au seuil calculé M. Si ce n'est pas le cas, les coefficients sont alors remplacés et bornés par ce seuil. Dans les algorithmes de perturbation présentés précédemment (APF, APO), la sensibilité des transformées était bornée par la valeur maximale des modules des coefficients des transformées. Par exemple,

la valeur maximale est supérieure à 70 pour le premier coefficient de la TFD d'après la figure 5.11. Dans cette nouvelle technique, le bornage des valeurs extrêmes permet de réduire la sensibilité (de 70 à 9 pour le premier coefficient de la TFD), et ainsi de réduire le bruit introduit par le mécanisme de Laplace.

5.3.1 APFB (algorithme de perturbation de Fourier borné)

Soit $X^i = (x_1^i, x_2^i, \ldots, x_T^i)$ la courbe de charge d'un foyer i ($i = 1, \ldots, N$). La somme de courbes de charge de N foyers est donnée par : $S = (S_1, \ldots, S_T) = (\sum_{i=1}^N x_1^i, \sum_{i=1}^N x_2^i, \ldots, \sum_{i=1}^N x_T^i)$. L'algorithme de perturbation de Fourier borné, détaillé dans l'algorithme 12, prend en entrée les courbes de charge individuelles des foyers, le seuil maximal M des coefficients de la TFD à ne pas dépasser, le budget de privacy, et renvoie une version bruitée de la somme de courbes de charge S.

Algorithme 12 APFB (algorithme de perturbation de Fourier borné)

entrées :

- courbes de charge individuelles : $(X^1, \ldots, X^N)$, avec $X^i = (x_1^i, x_2^i, \ldots, x_T^i)$ pour tout $i = 1, \ldots N$.
- Nombre de coefficients de la TFD à conserver : k.
- Valeur maximale des modules des k premiers coefficients de la TFD : $M = (M_1, \ldots, M_k) \in \mathbb{R}_+^k$.
- Budget de privacy : ϵ.

Algorithme :

1. **Bornage** : pour chaque consommation individuelle X^i :
   - Calculer les k premiers coefficients de la TFD de X^i : $C_k^i = (c_1^i, \ldots, c_k^i) = \text{TFD}(X^i)$
   - Pour tout $j = 1, \ldots, k$; si $|c_j^i| > M_j$ alors remplacer c_j^i par $c_j^i \times \frac{M_j}{|c_j^i|}$
2. **Mécanisme de Laplace** : calculer la somme bruitée de chaque coefficient : $\hat{c_j} = \sum_{i=1}^N c_j^i + \mathcal{L}(\frac{M_j\sqrt{2}}{\epsilon/k})$ pour tout $j = 1, \ldots, k$. On note $\widehat{C_k} = (\hat{c_1}, \ldots, \hat{c_k})$
3. Compléter $\widehat{C_k}$ par $T - k$ zéros :
$$\widehat{C_k} = (\hat{c}_1, \ldots, \hat{c}_k, 0, \ldots, 0).$$
4. Calculer la TFD inverse de $\widehat{C}_k$ et renvoyer le résultat :
$$\widehat{S} = (\hat{s}_1, \ldots, \hat{s}_T) = \text{TFDI}(\widehat{C}_k).$$

Sortie : Somme de courbes de charge bruitée $\widehat{S} = (\hat{s}_1, \ldots, \hat{s}_T)$

L'étape 1, appelée bornage, calcule les k premiers coefficients de la TFD de chaque courbe de charge individuelle X^i pour tout $i = 1, \ldots, N$. Si le module d'un coefficient noté c^i_j est supérieur à la valeur maximale M_j, alors ce coefficient est borné et remplacé par $\frac{c^i_j \times M_j}{|c^i_j|}$ qui est de module M_j.

Après avoir calculé les k coefficients de la TFD, notés $C^i_k = (c^i_1, \ldots, c^i_k)$, de chaque courbe de charge individuelle, l'étape 2 consiste à calculer la somme $(c_1, \ldots, c_k) = (\sum_{i=1}^n c^i_1, \ldots, \sum_{i=1}^n c^i_k)$ de ces coefficients pour les N foyers considérés en utilisant le mécanisme de Laplace. Il faut noter que le bruit de Laplace est rajouté aux parties réelle et imaginaire des coefficients. Le résultat complété de $T - k$ zéro est noté $\widehat{C}_k = (\hat{c}_1, \ldots, \hat{c}_k, 0, \ldots, 0)$.

Enfin, la somme de consommation bruitée des N foyers est égale à l'inverse de la TFD des coefficients bruités $\widehat{C}_k$.

Le lemme 5.3.1 justifie les paramètres du bruit de Laplace de l'étape 2.

Lemme 5.3.1 *Soit $C^i_k = (c^i_1, \ldots, c^i_k) = TFD(X^i)$ les k premiers coefficients la TFD de la consommation individuelle du foyer i ($i = 1, \ldots, N$), obtenus après le processus de bornage (1). Alors la sensibilité de la somme $\sum_{i=1}^N c^i_j$ est égale à $M_j\sqrt{2}$, pour $j = 1 \ldots, k$, en considérant c^i_j comme un élément de $\mathbb{R}^2$.*

Démonstration 5.3.1 *Soit $C^i_k = (c^i_1, \ldots, c^i_k) = TFD(X^i)$. Après le bornage, le module de chaque coefficient c^i_j est inférieur ou égale à M_j pour tout $j = 1, \ldots, k$. On note a^i_j et b^i_j les parties réelle et imaginaire de c^i_j respectivement. Soit $\mathbb{R}^T$ l'ensemble des courbes de charge individuelles. Pour $j = 1, \ldots, k$, la L_1-sensibilité de la fonction $F_j : \mathbb{R}^{TN} \longrightarrow \mathbb{R}^2$ définie par $F_j : (X^1, \ldots, X^N) \mapsto (\sum_{i=1}^N a^i_j, \sum_{i=1}^N b^i_j)$, est égale à :*

$$
\begin{aligned}
\Delta_1(F_j) &= \max_{a^i_j, b^i_j} \left\| (\sum_{i=1}^N a^i_j, \sum_{i=1}^N b^i_j) - (\sum_{i=2}^N a^i_j, \sum_{i=2}^n b^i_j) \right\|_1 \\
&= \max \left\| a^1_j, b^1_j \right\|_1 \\
&\leq \max \sqrt{2} \left\| a^1_j, b^1_j \right\|_2 \ \textit{inégalité des normes de Minkowski} \\
&= \max \sqrt{2} |c^1_j| \\
&= M_j\sqrt{2}
\end{aligned}
$$

Le lemme 5.3.1 justifie le bruit de Laplace introduit à l'étape 2, et permet de montrer que l'APFB garantit la ϵ-confidentialité différentielle.

Théorème 5.3.1 *L'algorithme 12 est ϵ-DP*

Démonstration 5.3.1 *D'après le lemme 5.3.1, pour $j = 1, \ldots, k$, la sensibilité de la somme $\sum_{i=1}^N c^i_j$ du j^e coefficient de la TFD des consommations individuelles des foyers est égale à $M_j\sqrt{2}$. Ainsi, le mécanisme de Laplace de l'étape 2 rend le calcul de chaque composant $\hat{c}_j$ ϵ/k-différentiellement confidentiel pour $j = 1, \ldots, k$. De plus, comme on calcule k sommes*

bruitées, d'après le théorème de composition de la DP (théorème 3.1.2), le résultat global $\widehat{C_k}$ est ϵ-différentiellement confidentiel. Comme le post-traitement d'un mécanisme qui garantit la DP, garantit aussi la DP, alors le calcul de l'inverse de la TFD de $\widehat{C_k}$ garantit aussi la DP.

La figure 5.12 donne un exemple d'application de l'APFB sur la courbe de charge utilisée dans l'illustration des algorithmes présentés précédemment (par exemple Figure 5.9), avec un budget de privacy de $\epsilon = 1$, et $k = 5$ pour chaque journée.

Cet exemple montre une amélioration de l'utilité par rapport à l'APF (Figure 5.9), avec une erreur relative moyenne passée de 361% à 34%, d'où une diminution de l'erreur d'un facteur 10,6. Cependant, l'utilité recherchée n'est pas encore atteinte. La section 5.4 montre qu'en augmentant le nombre de foyers, on arrive à avoir une erreur relative moyenne inférieure à 10%.

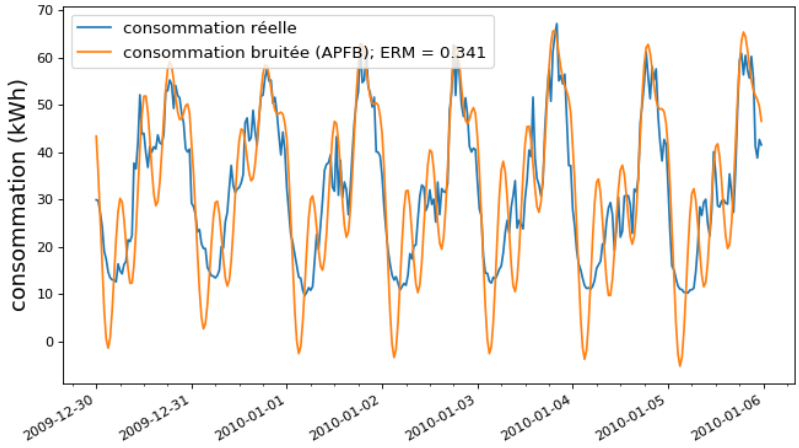


FIGURE 5.12 – somme de courbes de charge bruitée de 50 foyers du 30 décembre 2009 au 6 janvier 2010, du jeu de données de la CER irlandaise en utilisant l'algorithme de perturbation de Fourier borné, avec un budget de privacy de $\epsilon = 1$, et $k = 5$ pour chaque journée.

5.3.2 APOB (algorithme de perturbation en ondelettes borné)

L'APOB (algorithme de perturbation en ondelettes borné) est obtenu en remplaçant la TFD par la TOD dans l'algorithme 12. Comme pour l'APFB, l'APOB requiert de calculer en amont le seuil de la sensibilité des coefficients de la transformée en ondelettes à ne pas dépasser. Pour trouver ce seuil, il faut calculer la distribution des valeurs absolues des coefficients de la TOD choisie (Haar, Daubechies, etc., ainsi que leur niveau de décomposition) des courbes de charge individuelles de la base de données D_1. Ensuite, le seuil est défini pour chaque coefficient de la transformée en enlevant les valeurs extrêmes comme expliqué dans la section 5.3.

Par exemple, la distribution des valeurs absolus des coefficients de la TOD en utilisant Haar est donnée par la figure 5.13.

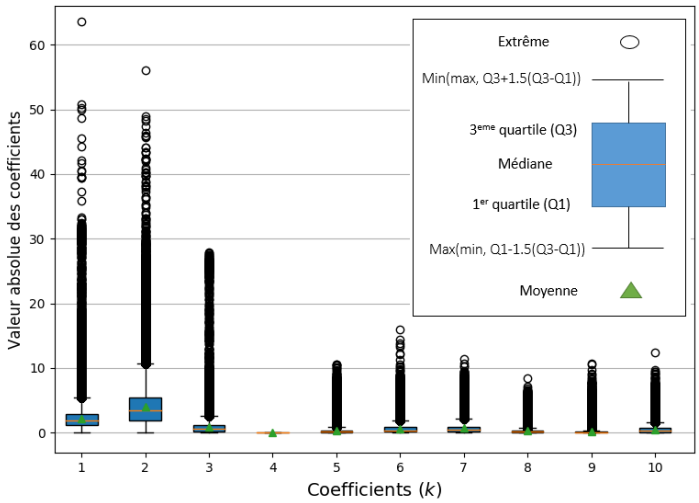


FIGURE 5.13 – Distribution des coefficients de la TOD (transformée en ondelettes discrète) en utilisant Haar, de la courbe de charge des $N/2$ premiers consommateurs du jeu de données de la CER

L'APOB est détaillé dans l'algorithme 13, qui prend en entrée les courbes de charge individuelles des foyers, le seuil maximal M des coefficients de la TOD à ne pas dépasser, le budget de privacy, et renvoie une version bruitée de la somme de courbes de charge S (équation (5.1))

Le bruit ajouté à l'étape 2 est justifié par le lemme 5.3.2.

Lemme 5.3.2 *Soit $C_k^i = (c_1^i, \ldots, c_k^i) = TOD(X^i)$ les k premiers coefficients la TOD de la consommation individuelle du foyer i ($i = 1, \ldots, N$), obtenus après le processus de bornage (1). Alors pour $j = 1 \ldots, k$, la sensibilité de la somme $\sum_{i=1}^{N} c_j^i$ est égale à M_j.*

Démonstration 5.3.2 *Soit $C_k^i = (c_1^i, \ldots, c_k^i) = TOD(X^i)$. Après le bornage, la valeur absolue de chaque coefficient c_j^i est inférieur ou égale à M_j pour $j = 1, \ldots, k$. Soit $\mathbb{R}^T$ l'ensemble des courbes de charge individuelles. Pour $j = 1, \ldots, k$, la sensibilité de la fonction $W_j : \mathbb{R}^{TN} \longrightarrow \mathbb{R}$ définie par $W_j : (X^1, \ldots, X^N) \mapsto \sum_{i=1}^{N} c_j^i$ est :*

$$\begin{aligned}
\Delta_1(W_j) &= \max_{|c_j^i|} |\sum_{i=1}^{N} c_j^i - \sum_{i=2}^{N} c_j^i| \\
&= \max |c_j^1| \\
&= M_j
\end{aligned}$$

Algorithme 13 APOB (algorithme de perturbation en ondelettes borné)

entrées :

- courbes de charge individuelles : $(X^1, \dots, X^N)$, avec $X^i = (x_1^i, x_2^i, \dots, x_T^i)$ pour $i = 1, \dots N$.
- Nombre de coefficients de la TOD à conserver : k.
- Valeur maximale des modules des k premiers coefficients de la TOD : $M = (M_1, \dots, M_k) \in \mathbb{R}_+^k$.
- Budget de privacy : ϵ.

Algorithme :

1. **Bornage** : pour chaque consommation individuelle X^i :
   - Calculer les k premiers coefficients de la TOD de X^i : $C_k^i = (c_1^i, \dots, c_k^i) = \text{TOD}(X^i)$.
   - Pour tout $j = 1, \dots, k$, si $|c_j^i| > M_j$, alors remplacer c_j^i par $c_j^i \times \frac{M_j}{|c_j^i|}$.
2. **Mécanisme de Laplace** : calculer la somme bruitée de chaque coefficient : $\hat{c_j} = \sum_{i=1}^N c_j^i + \mathcal{L}(\frac{M_j}{\epsilon/k})$ pour tout $j = 1, \dots, k$. On note $\widehat{C_k} = (\hat{c}_1, \dots, \hat{c}_k)$.
3. Compléter $\widehat{C_k}$ par $T - k$ zéros :
$$\widehat{C_k} = (\hat{c}_1, \dots, \hat{c}_k, 0, \dots, 0).$$
4. Calculer la TOD inverse de $\widehat{C_k}$ et renvoyer le résultat :
$$\widehat{S} = (\hat{s}_1, \dots, \hat{s}_T) = \text{TODI}(\widehat{C_k}).$$

Sortie : Somme de courbe de charge bruitée $\widehat{S} = (\hat{s}_1, \dots, \hat{s}_T)$

Comme l'APFB, l'APOB garantit la ϵ-confidentialité différentielle.

Théorème 5.3.2 *L'algorithme 13 garantit la ϵ-confidentialité différentielle.*

Démonstration 5.3.3 *La démonstration du théorème 5.3.2 est similaire à celle du théorème 5.3.1. D'après le lemme 5.3.2, le mécanisme de Laplace de l'étape 2 rend le calcul de chaque composant $\hat{c}_j$ ϵ/k-différentiellement confidentiel pour $j = 1, \dots, k$. De plus, comme on calcule k sommes bruitées, d'après le théorème de composition de la DP (théorème 3.1.2), le résultat global $\widehat{C_k}$ est ϵ-différentiellement confidentiel. Comme le post-traitement d'un mécanisme qui garantit la ϵ-DP garantit aussi la ϵ-DP, alors le calcul de l'inverse de la TOD de $\widehat{C_k}$ garantit aussi la DP.*

On remarque que le paramètre du bruit de Laplace dans l'APOB est inférieur à celui de l'APFB. En effet, pour $j = 1, \dots, k$, le paramètre du bruit de Laplace dans l'APFB est de $\mathcal{L}(\frac{M_j\sqrt{2}}{\epsilon/k})$, contre $\mathcal{L}(\frac{M_j}{\epsilon/k})$ pour l'APOB, c'est-à-dire une différence d'un facteur $\sqrt{2}$. En outre, le

nombre de coefficients bruités dans l'APFB est deux fois supérieur à celui dans l'APOB. Plus précisément, dans l'APFB, la perturbation est introduite sur les parties réelles et imaginaires des k coefficients de la TFD, d'où un total de $2k$ perturbations. Alors que dans l'APOB, les k premiers coefficients de la TOD sont à valeurs réelles, la perturbation est donc introduite sur ces k coefficients.

La figure 5.14 donne un exemple d'application de l'APOB en utilisant la TOD de Haar avec une décomposition de niveau 5, sur la courbe de charge utilisée pour l'application de l'APO. Dans cet exemple, on obtient une augmentation de l'utilité par rapport à l'APO (figure 5.8),

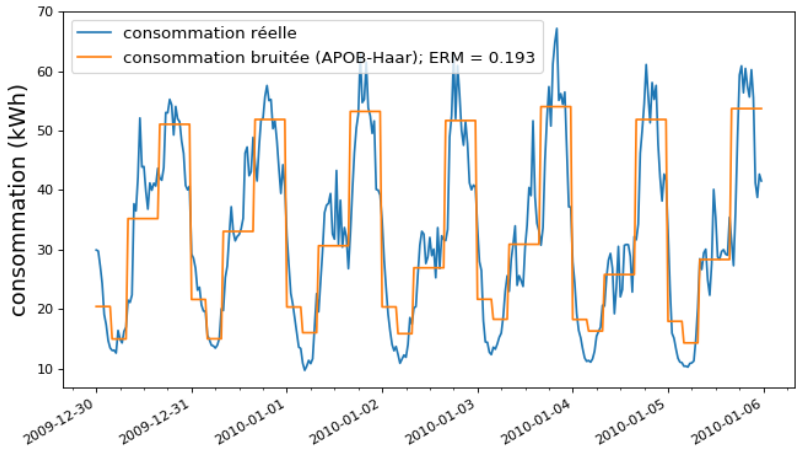


FIGURE 5.14 – somme de courbes de charge bruitée de 50 foyers du 30 décembre 2009 au 6 janvier 2010, du jeu de données de la CER irlandaise en utilisant l'algorithme de perturbation en ondelettes borné, avec Haar de niveau 5, un budget de privacy de $\epsilon = 1$, et $k = 5$ pour chaque journée.

avec une Une analyse plus poussée de l'utilité des différents algorithmes présentés ci-dessus (APF, APO, APFB et APOB) est faite dans la section 5.4, en comparant et en analysant leur erreur relative moyenne respective.

5.4 Analyse des performances

Cette section présente les résultats expérimentaux des algorithmes présentés ci-dessus. La base de données de la CER utilisée ici est divisée en deux parties égales, comme expliqué dans la section 5.3 : D_1, permettant de calculer une approximation des valeurs maximales des modules des coefficients des transformées utilisées pour les algorithmes de perturbations bornés (APFB et APOB), et D_2, utilisée pour le test des différents algorithmes de perturbation (APF, APO, APFB et APOB).

En outre, cette section analyse les deux sources d'erreurs présentes dans les algorithmes de perturbation : l'erreur de perturbation et l'erreur de reconstruction. L'erreur de perturbation dépend de l'amplitude du bruit de Laplace introduit sur les k premiers coefficients de la transformée considérée. Elle est analysée dans la section 5.4.2. L'erreur de reconstruction est causée par l'ignorance des $T - k$ coefficients de la transformée considérée. Elle varie en fonction du nombre k de coefficients conservés mais aussi du type de transformée considérée. La section 5.4.1 montre que la transformée en ondelettes de Haar avec 2 coefficients d'approximations (2cA), notée haar, Daubechies 2 avec 5cA, notée db-2, et Daubechies 3 avec 10cA, notée db-3, sont les TOD qui obtiennent la plus faible erreur de reconstruction parmi les autres types d'ondelettes. Ces transformées sont donc choisies pour le tester les algorithmes APO et APOB.

Soit N le nombre de foyers considérés. Pour les tests, nous avons exécuté chaque algorithme de perturbation sur 100 groupes différents de N foyers, choisis aléatoirement. Ensuite, nous avons calculé la distribution de l'ERM (erreur relative moyenne) entre les courbes de charge bruitées et non bruitées. Dans ces résultats expérimentaux, un budget de privacy ϵ est alloué pour chaque journée.

La figure 5.15 (respectivement la figure 5.16) correspond la distribution de l'ERM de l'APF, l'APFB, l'APO,et l'APOB en fonction du nombre de foyers N et de $k = 5, 8, 10$ pour $\epsilon = 1$ (respectivement pour $\epsilon = 3$). Dans ces deux figures, la première colonne correspond à la comparaison entre l'APF et l'APFB, les colonnes suivantes correspondent à la comparaison entre l'APO et l'APOB en utilisant respectivement la transformée de Haar avec 2cA, de Daubechies 2 avec 5cA (db2), et de Daubechies 3 avec 10cA (db3).

Les figures 5.15 et 5.16 montrent que l'APFB obtient une meilleure utilité que l'APF. Par exemple pour un budget $\epsilon = 1$ (Figure 5.15), quand $k = 5$ et $N = 350$, la médiane de l'ERM de l'APFB est de 12%, contre 75% pour l'APF. C'est-à-dire un gain d'utilité d'un facteur 6,25.

Similairement, l'APOB obtient une meilleure utilité que l'APO. Par exemple, pour un budget $\epsilon = 1$ (Figure 5.15), quand $k = 5$ et $N = 350$, la médiane de l'ERM de l'APOB en utilisant Haar est de 15%, contre 30% pour l'APO en utilisant la même décomposition en ondelettes (Haar). d'où un gain d'utilité d'un facteur 2.

De manière générale, plus le nombre de foyers N augmente, plus l'ERM diminue. De même, plus le budget de privacy ϵ augmente, plus l'utilité augmente au détriment de la garantie de protection.

Quand k augmente, l'ERM de l'APO et de l'APOB en utilisant db3 diminuent. En outre, pour un budget $\epsilon = 3$ (Figure 5.16), quand le nombre de foyers N est supérieur à 250, la médiane de l'ERM de l'APOB est inférieure à 11%. L'APOB en utilisant Haar obtient la deuxième meilleure utilité : la médiane de son ERM est inférieure à 10% quand N est supérieur de 250. La meilleure utilité est obtenue par l'APFB : la médiane de son ERM atteint 5% quand N est égal à 550 et $k = 8$.

Cependant, plus k est grand, plus l'ERM de l'APF et des APO (sauf pour db3) augmente. Ce phénomène est dû à l'erreur de perturbation présentée dans la section 5.4.2. Comme il faut garantir un budget global ϵ sur l'ensemble des coefficients des transformées, plus k est grand, plus le budget alloué à chaque coefficient diminue (ϵ est divisé par k), ainsi, le bruit

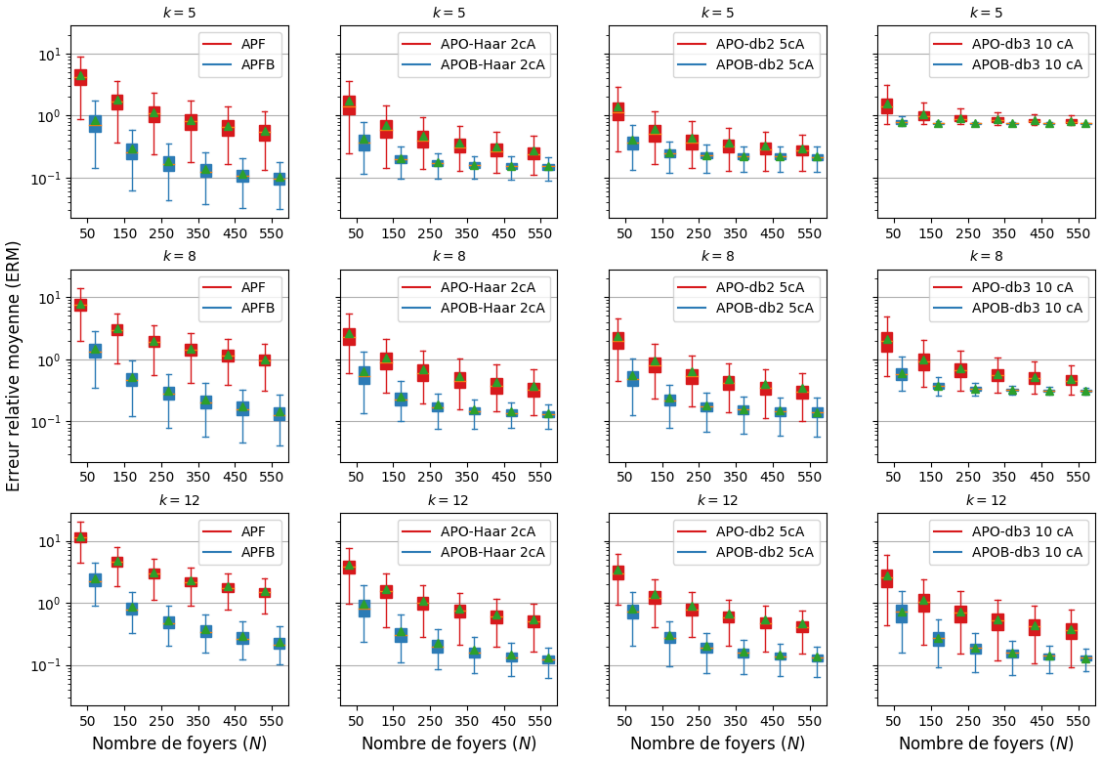


FIGURE 5.15 – Distribution de l'ERM (erreur relative moyenne) des algorithmes de perturbation de Fourier, d'ondelettes, avec les versions bornées associées en fonction du nombre de foyers (N) et de k, pour un budget de privacy $\epsilon = 1$

de Laplace introduit dans chaque coefficient augmente malgré la diminution de l'erreur de reconstruction.

Ce bruit peut être atténué par le mécanisme de bornage, qui diminue la sensibilité. Comme le bruit de Laplace ajouté sur chaque coefficient des transformées a pour paramètre la sensibilité et le budget de privacy, alors, pour un même budget ϵ, le bruit sera moins important dans les algorithmes bornés que dans les algorithmes non bornés.

Par exemple, pour $\epsilon = 3$ (Figure 5.16), quand k augmente de 5 à 8, l'erreur de reconstruction diminue, et le bornage diminue aussi l'erreur de perturbation, entrainant une diminution de l'erreur totale. Cependant, quand k augmente de 8 à 12, Bien que l'erreur de reconstruction diminue, le bornage ne permet pas de diminuer suffisamment l'erreur de perturbation. Cela explique une légère augmentation de l'ERM quand $k = 12$ par rapport à $k = 8$.

Il faut aussi noter que, dans les figures 5.15 et 5.16, la médiane de l'ERM de l'APO et l'APOB converge vers un seuil qui n'est jamais dépassé. Par exemple quand $k = 5$, la médiane de l'ERM de l'APO et de l'APOB en utilisant db2 converge vers 20%. Ceci est dû à l'erreur de reconstruction décrite en section 5.4.1.

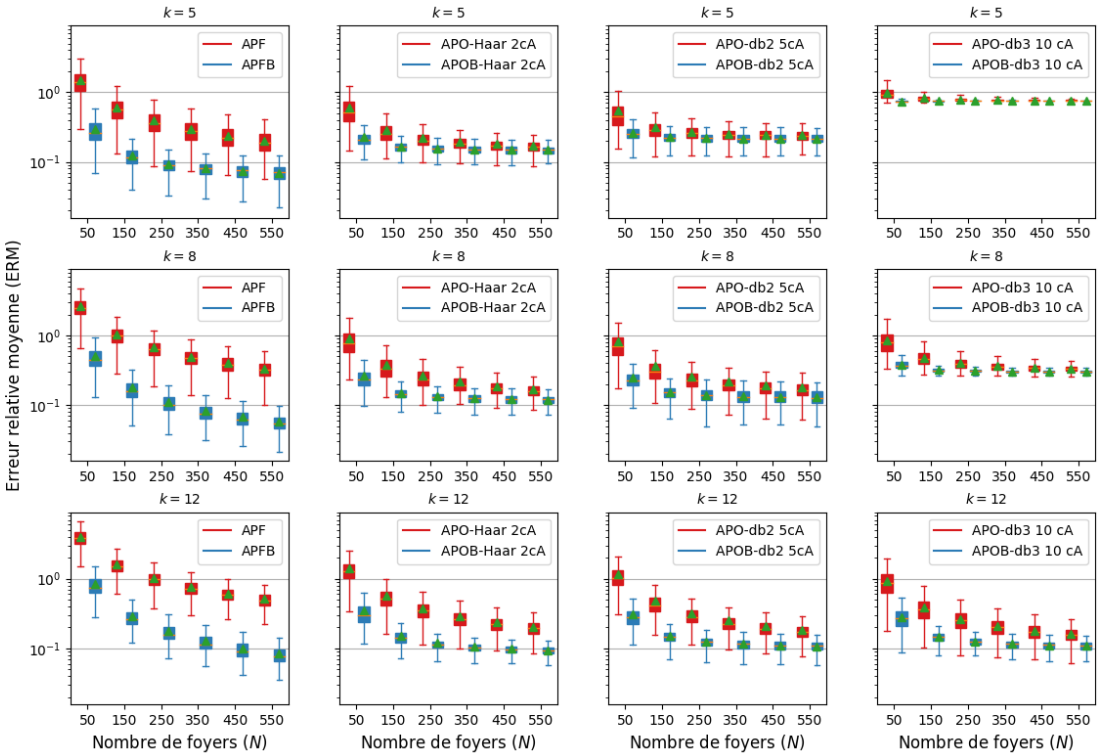


FIGURE 5.16 – Distribution de l'ERM (erreur relative moyenne) des algorithmes de perturbation de Fourier, d'ondelettes, avec les versions bornées associées en fonction du nombre de foyers (N) et de k, pour un budget de privacy $\epsilon = 3$

5.4.1 Erreur de reconstruction

Cette section présente l'erreur de reconstruction des transformées considérées dans ce chapitre, ce qui permet d'expliquer l'obtention de l'ERM des différents algorithmes de perturbation.

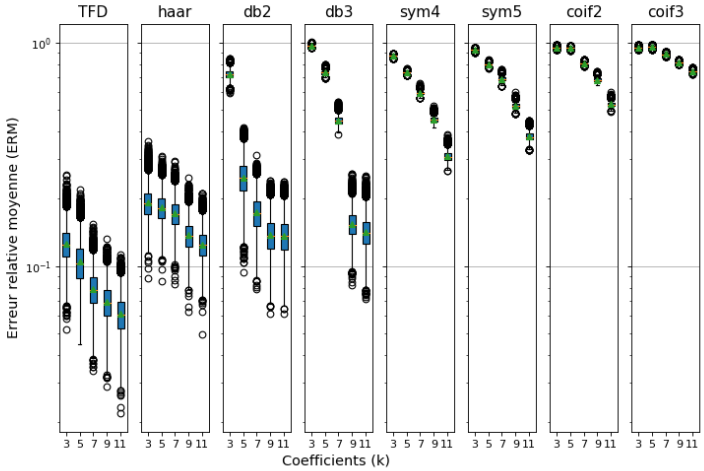
L'erreur de reconstruction est due à l'ignorance des $T - k$ derniers coefficients, et est définie comme suit :

Définition 5.4.1 *Erreur de reconstruction*
Soit $S = (s_1, \ldots, s_T)$ la somme de courbes de charge de N foyers, $C = (c_1, \ldots, c_T)$ les coefficients de sa transformée en utilisant la TFD ou la TOD. Soit $C_k = (c_1, \ldots, c_k, 0, \ldots, 0)$ les coefficients obtenus en remplaçant les $T - k$ derniers coefficients par des zéros, et $\tilde{S} = (\tilde{s}_1, \ldots, \tilde{s}_T)$ le résultat de la transformée inverse de C_k. L'erreur de reconstruction (ER) de C_k est définie comme l'erreur relative moyenne entre S et $\tilde{S}$, donnée par :[5]

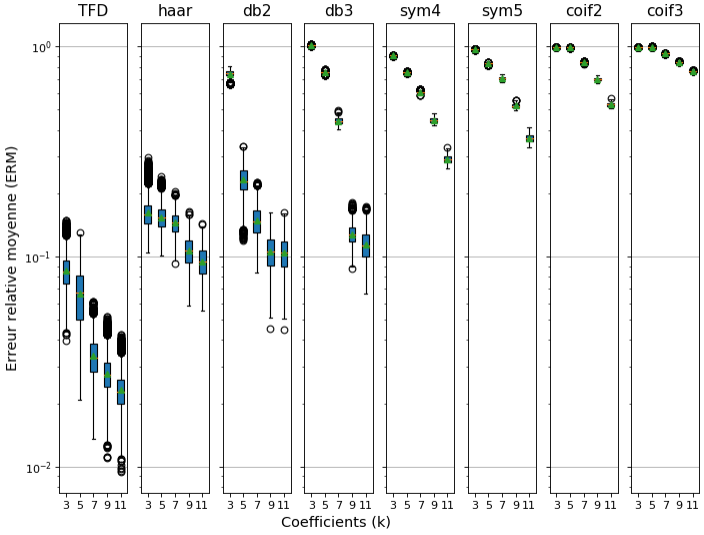
$$\mathrm{ER}(C_k) = \frac{1}{T} \sum_{i=1}^{T} \frac{|s_i - \tilde{s}_i|}{s_i + 1}$$

5. Ici, nous rajoutons 1 au dénominateur pour éviter les divisions par zéro.

Les figures 5.17a et 5.17b représentent la distribution de erreur de reconstruction de la TFD et de la TOD en fonction du nombre de coefficients conservés (k) respectivement pour $N = 50$ foyers et $N = 450$ foyers.



(a) 50 foyers.



(b) 450 foyers.

FIGURE 5.17 – Distribution de l'erreur de reconstruction de la transformée de Fourier discrète et de la transformée en ondelettes discrète en fonction du nombre de coefficients conservés (k) pour 50 et 450 foyers.

Les figures 5.17a et 5.17b montrent que la TFD obtient la plus faible erreur de reconstruction, précédée de la TOD en utilisant Haar et db2. Plus k augmente, plus l'erreur de reconstruction

diminue. En effet, plus on conserve de coefficients, moins on perd de l'information dans la transformée considérée.

Quand k est inférieur ou égal à 7, la TOD en utilisant Daubechies 3 (db3) a une erreur de reconstruction supérieure à 40%. Ceci, explique pourquoi, quand $k = 5$ par exemple, l'ERM de l'APO et l'APOB en utilisant db3 est supérieure à 70%.

En outre, les figures 5.17a et 5.17b montrent que l'erreur de reconstruction de la TOD en utilisant les ondelettes Symlets 4 et 5 et Coiflets 2 et 3 est supérieure à 30% pour tout k allant de 3 à 11. C'est la raison pour laquelle nous n'utilisons pas ces ondelettes dans les algorithmes APO et APOB.

5.4.2 Erreur de perturbation

L'erreur de perturbation dépend directement du bruit de Laplace ajouté sur les k premiers coefficient de la transformée considérée. Pour l'APFB et l'APOB, le bornage des k premiers coefficients s'ajoute à l'erreur de perturbation.

Dans la section 5.4.1, nous avons vu que plus on conserve de coefficients (c'est-à-dire plus k est grand), plus l'erreur de reconstruction diminue (on perd moins d'information dans la transformée considérée). Cependant, plus k est grand, plus le budget des premiers coefficients de la transformée considérée diminue (le budget ϵ est divisé par k). Ce qui entraine un ajout plus important du bruit, et ainsi une augmentation de l'erreur de perturbation. Il faut donc trouver un k qui minimise simultanément l'erreur de reconstruction et l'erreur de perturbation.

Nous notons que l'amplitude du bruit de Laplace inséré sur chaque coefficient pour les algorithmes de perturbation de Fourier (APF, respectivement APFB) est $\sqrt{2}$ fois supérieure à celle pour les algorithmes de perturbation en ondelette (APO, respectivement APOB) : la distribution du bruit de Laplace de l'APF est $\mathcal{L}(\frac{M\sqrt{2Tk}}{\epsilon})$, contre $\mathcal{L}(\frac{M\sqrt{Tk}}{\epsilon})$ pour l'APO. De plus, il y a deux fois plus de valeurs à bruiter dans les algorithmes de perturbation qui utilisent la TFD (parties réelle et imaginaire) que ceux qui utilisent la TOD.

En outre, si les coefficients de la transformée sont petits alors que le paramètre du bruit de Laplace est important, alors l'erreur relative sera grande. La figure 5.18 montre une comparaison de la médiane des coefficients de la TFD et de TOD pour toutes les courbes de charge du jeu de données, en utilisant Haar, Daubechies 2 et Daubechies 3 et en considérant les derniers niveaux de décomposition pour les TOD. C'est-à-dire, le niveau de décomposition avec le moins de coefficients d'approximation.

La figure 5.18 montre que la médiane des coefficients varie en fonction de k et du type de la transformée. En comparant les modules des 5 premiers coefficients de la TFD et de la TOD en utilisant db2, on remarque que le module du premier coefficient de la TFD est supérieur à celui de db2, mais les modules du deuxième au cinquième coefficient de la TFD sont inférieurs à ceux de db2.

Dans les algorithmes de perturbations bornés (APFB et APOB), le bornage permet d'ajouter un bruit proportionnelle au module des coefficients de la transformée considérée. Ce qui diminue l'impact du bruit par rapport aux algorithmes de perturbation non bornés (APF,

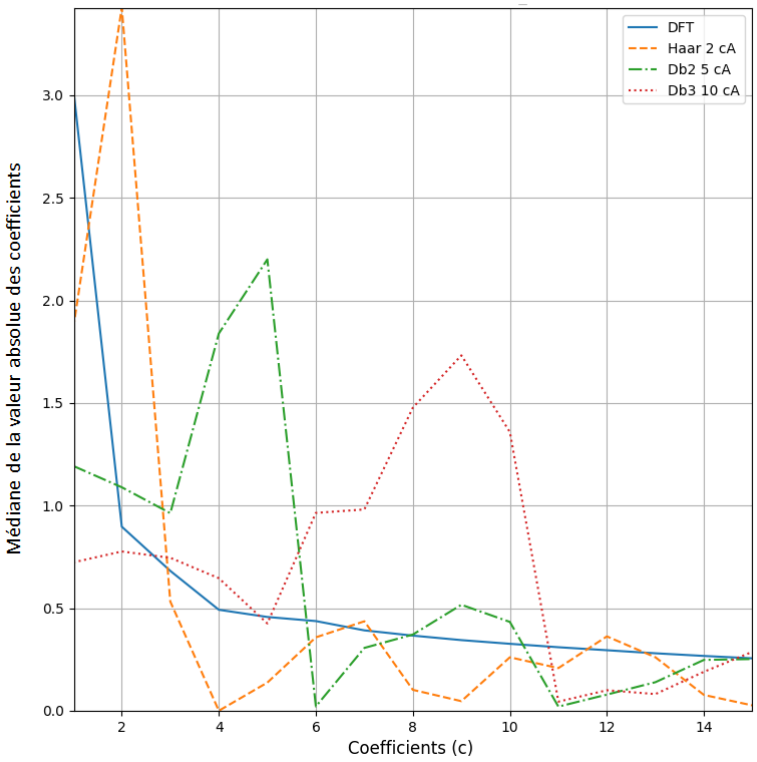


FIGURE 5.18 – Médiane des coefficients de la transformée de Fourier discrète et de la transformée en ondelettes discrète en utilisant Haar, Daubechies 2 et Daubechies 3 pour toutes les courbes de charge du jeu de données.

APO). Mais ajoute une erreur liée au bornage des coefficients. Formellement, l'erreur de perturbation des algorithmes de perturbation bornés (APFB et APOB) est définit comme suit :

Définition 5.4.2 *Erreur de perturbation pour les algorithmes de perturbation bornés (APFB et APOB)*
Soit $X^1, \ldots, X^N$ les courbes de charges individuelles de N foyers, avec $X^i = (x_1^i, \ldots, x_T^i)$ pour $i = 1, \ldots, N$. La somme des courbes de charge est notée $S = (s_1, \ldots, s_T) = (\sum_{i=1}^N x_1^i, \ldots, \sum_{i=1}^N x_T^i)$. Pour $i = 1, \ldots N$, on note $\overline{C}^i = (\bar{c}_1^i, \ldots, \bar{c}_k^i, c_{k+1}^i, \ldots, c_T^i)$ le résultat de la transformée considérée de la courbe de charge X^i dont les k premiers coefficients $(\bar{c}_1^i, \ldots, \bar{c}_k^i)$ ont été bornés. On note $M = (M_1, \ldots, M_k)$ la valeur maximale des modules des k premiers coefficients de la transformée considérée. Soit $\overline{C} = (\sum_{i=1}^N \bar{c}_1^i + \mathcal{L}(\frac{\delta_1}{\epsilon/k}), \ldots, \sum_{i=1}^N \bar{c}_k^i + \mathcal{L}(\frac{\delta_k}{\epsilon/k}), \sum_{i=1}^N c_{k+1}^i, \ldots, \sum_{i=1}^N c_T^i)$ la somme des coefficients de la transformée considérée en bruitant uniquement les k premiers coefficients. Avec $\delta_j = M_j\sqrt{2}$ pour l'APFB et $\delta_j = M_j$ pour l'APOB, pour $j = 1, \ldots, k$.

Soit $\overline{S} = (\bar{s_1}, \ldots, \bar{s_T})$ la transformée inverse de $\overline{C}$. L'erreur de perturbation de $\overline{C}$ est égale à l'erreur relative moyenne entre la somme des courbes de charge S et $\bar{S}$, donnée par :[6]

$$\mathrm{EP}(\overline{C}) = \frac{1}{T}\sum_{\ell=1}^{T}\frac{|s_\ell - \bar{s}_\ell|}{s_\ell + 1}$$

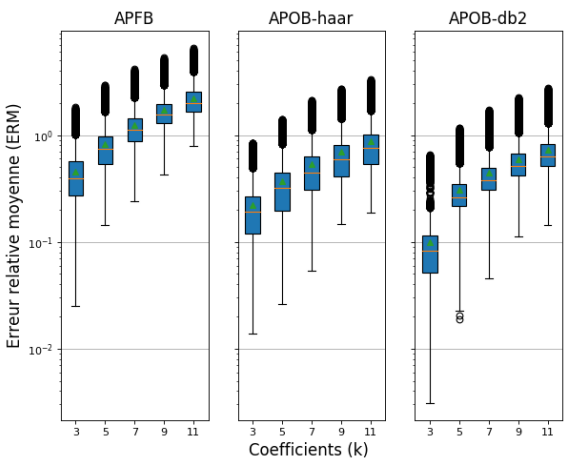
L'erreur de perturbation dépend de quatre paramètres : k, M_j, ϵ, et N pour $j = 1, \ldots, k$. k, M_j $(j = 1, \ldots, k)$ et ϵ sont des paramètres de la distribution de Laplace, ils impactent donc directement l'amplitude du bruit ajouté. Soit ϵ et M_j fixes, plus k est grand, plus le paramètre de la distribution de Laplace $\frac{\delta_k}{\epsilon/k}$ diminue, ainsi le bruit ajouté sur les k premiers coefficients augmente. Ce qui rend l'erreur de perturbation importante. le choix de M_j est important à la fois pour définir le seuil du bornage et impacte aussi directement la perturbation dans le mécanisme de Laplace. Dans ces résultats expérimentaux nous n'avons pas fait varier cette valeur, son impact sur l'erreur de perturbation devrait être analysé. Le nombre de foyers N joue indirectement un rôle dans l'erreur de perturbation, plus il est grand, plus le bruit ajouté sera dilué. Et ainsi, l'erreur de perturbation sera moins importante.

La figure 5.19 (respectivement, la figure 5.20) donne la distribution de l'erreur de perturbation des algorithmes de perturbation bornés (APFB et APOB) en fonction de k, N, avec $\epsilon = 1$ (respectivement, $\epsilon = 3$).

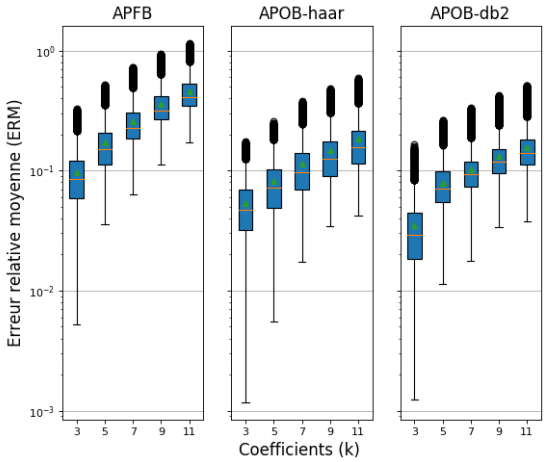
Les figures 5.19 et 5.20 montrent que l'erreur de perturbation de l'APFB est supérieure à celle de l'APOB. Ce résultat s'explique par :

1. le nombre de coefficients à bruiter dans l'APFB qui est 2 fois supérieur au nombre de coefficients à bruiter dans l'APOB. En effet, dans l'APFB, les coefficients de la TFD sont des complexes, il faut donc bruiter à la fois les parties réelles et imaginaires.
2. La valeur absolue du bruit ajouté dans l'APFB qui est $\sqrt{2}$ fois supérieure à celle dans l'APOB.

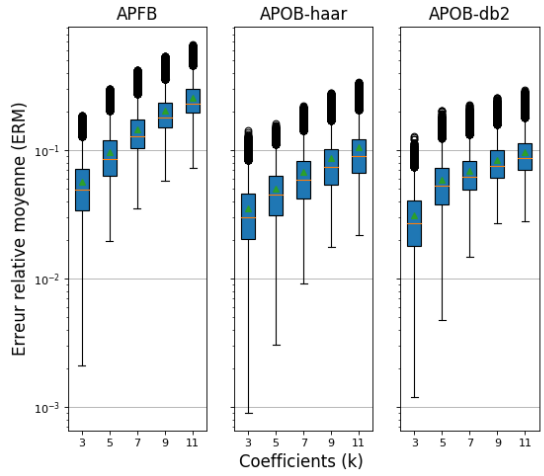
6. Ici, nous rajoutons 1 au dénominateur pour éviter les divisions par zéro.



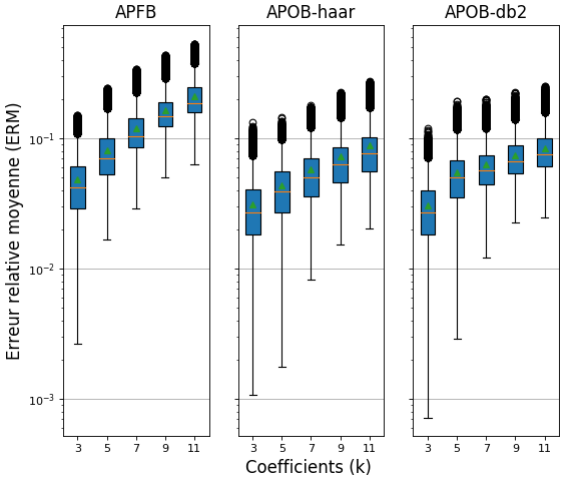
(a) $N = 50$



(b) $N = 250$

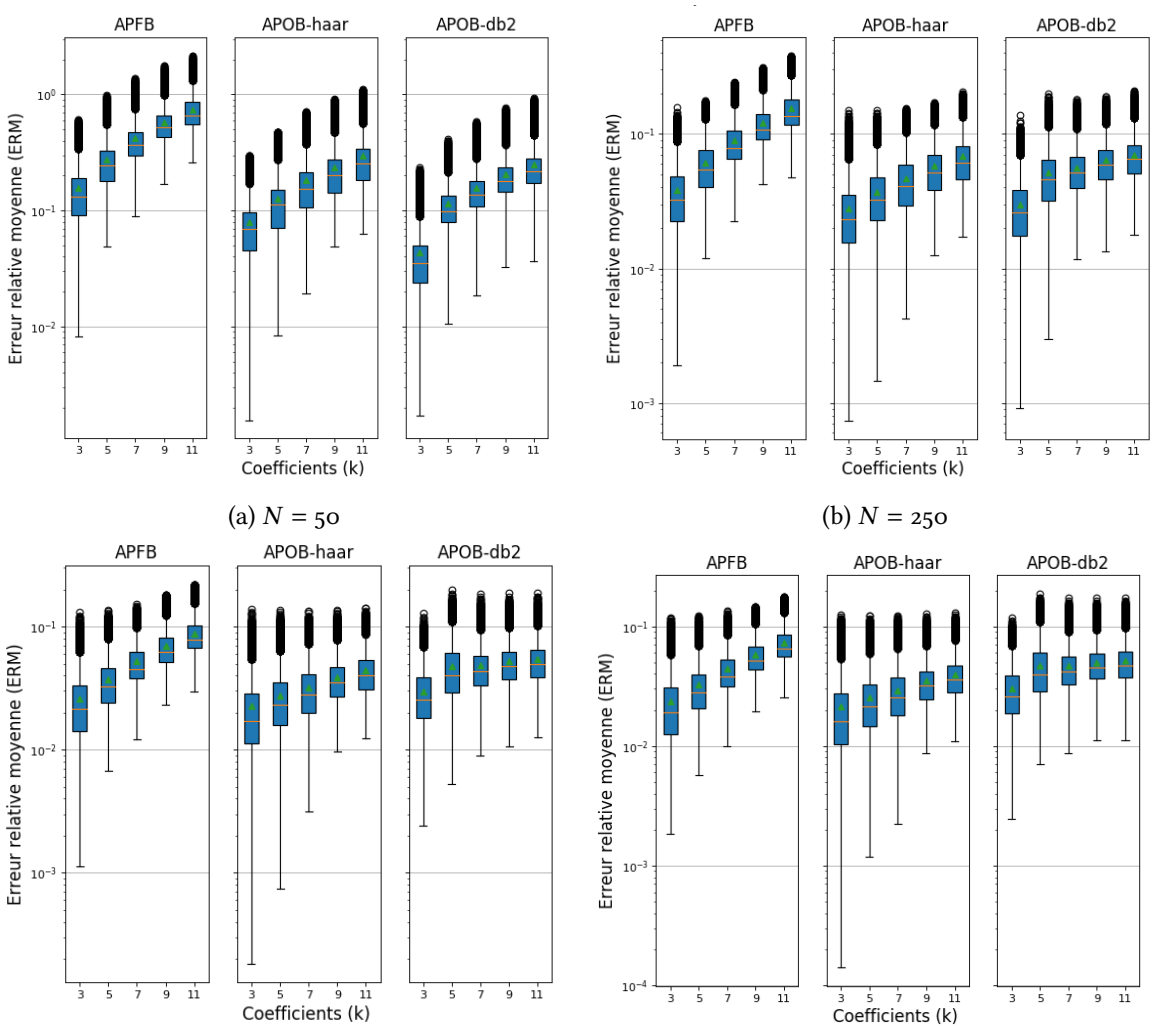


(c) $N = 450$



(d) $N = 550$

FIGURE 5.19 – Distribution de l'erreur de perturbation en fonction des algorithmes de perturbation bornés APFB et APOB, avec Haar, Daubechies 2 et Daubechies 3. Et en fonction de k et du nombre de foyers N, pour un budget de privacy fixe $\epsilon = 1$. Il faut noter que les échelles des figures 5.19a, 5.19b, 5.19c et 5.19d sont différentes.



(a) $N = 50$

(b) $N = 250$

(c) $N = 450$

(d) $N = 550$

FIGURE 5.20 – Distribution de l'erreur de perturbation en fonction des algorithmes de perturbation bornés APFB et APOB, avec Haar, Daubechies 2 et Daubechies 3. Et en fonction de k et du nombre de foyers N, pour un budget de privacy fixe $\epsilon = 3$. Il faut noter que les échelles des figures 5.20a, 5.20b, 5.20c et 5.20d sont différentes.

En outre, plus N est grand, plus le bruit ajouté est dilué dans l'agrégat, ce qui plus entraine la diminution de l'erreur de perturbation. Par exemple, pour $\epsilon = 1$ (figure 5.19), quand $k = 5$, En utilisant l'APFB (respectivement, l'APOB avec Haar), la médiane de l'erreur de perturbation passe de 70% (respectivement, 32%) pour $N = 50$ à 7% (respectivement, 4%) pour $N = 550$. De même, pour $\epsilon = 3$ (figure 5.20), quand $k = 5$, en utilisant l'APFB (respectivement, l'APOB avec Haar), la médiane de l'erreur de perturbation passe de 25% (respectivement, 11%) pour $N = 50$ à 2.7% (respectivement, 2.1%) pour $N = 550$. On remarque que, plus N est grand, plus la différence de l'erreur de perturbation entre l'APFB et l'APOB se fait moins ressentir. Ce résultat est aussi vrai quand ϵ augmente. Ce qui s'explique par la diminution du bruit introduit sur les coefficients des transformées.

Les figures 5.19 et 5.20 confirment que l'erreur de perturbation augmente quand k augmente, comme expliqué précédemment : le bruit ajouté a le même paramètre pour chaque coefficient des transformées. De plus, plus k est grand, plus le budget ϵ/k alloué à chaque coefficient diminue, ce qui entraine une augmentation du bruit sur chaque coefficient et donc de l'erreur de perturbation.

5.4.3 Bilan

La combinaison de l'erreur de reconstruction (figures 5.17a et 5.17b) et de l'erreur de perturbation (figures 5.19 et 5.20) permet de déterminer la transformée appropriée en fonction de k afin d'obtenir une ERM la plus faible possible.

Lemme 5.4.1 *L'ERM (erreur relative moyenne) de l'APFB (respectivement de l'APOB) est inférieure ou égale à la somme de l'erreur de reconstruction et de l'erreur de perturbation de l'APFB (respectivement de l'APOB).*

Démonstration 5.4.1 *Soit $S = (s_1, \ldots, s_T)$ la somme de courbes de charge à publier en utilisant l'APFB ou l'APOB. Soit $C = (c_1, \ldots, c_T)$ les coefficients de la transformée considérée de S. Pour plus de simplicité on considère qu'on utilise l'APFB, on a : $S = \text{TFDI}(c_1, \ldots, c_T)$. On note $\bar{c}_j$ le coefficient borné de c_j pour $j = 1, \ldots, k$ Soit $\widehat{S} = \text{TFDI}(\bar{c}_1 + \mathcal{L}(\frac{M_1\sqrt{2}}{\epsilon/k}), \ldots, \bar{c}_k + \mathcal{L}(\frac{M_k\sqrt{2}}{\epsilon/k}), 0, \ldots, 0)$ le résultat de la somme de courbes de charge bruitée, avec $M = (M_1, \ldots, M_k)$ la valeur maximale des modules des k premiers coefficients de la TFD. En posant $d_j = \bar{c}_j - c_j$ pour $j = 1, \ldots, k$, on a :*

$$
\begin{aligned}
\widehat{S} &= \text{TFDI}(\bar{c}_1 + \mathcal{L}(\frac{M_1\sqrt{2}}{\epsilon/k}), \ldots, \bar{c}_k + \mathcal{L}(\frac{M_k\sqrt{2}}{\epsilon/k}), 0, \ldots, 0) \\
&= \text{TFDI}(d_1 + c_1 + \mathcal{L}(\frac{M_1\sqrt{2}}{\epsilon/k}), \ldots, d_k + c_k + \mathcal{L}(\frac{M_k\sqrt{2}}{\epsilon/k}), 0, \ldots, 0) \\
&= \text{TFDI}(c_1, \ldots, c_T) + \text{TFDI}(d_1 + \mathcal{L}(\frac{M_1\sqrt{2}}{\epsilon/k}), \ldots, d_k + \mathcal{L}(\frac{M_k\sqrt{2}}{\epsilon/k}), 0, \ldots, 0) - \text{TFDI}(0, \ldots, 0, c_{k+1}, \ldots, c_T)
\end{aligned}
$$

Soit $\widetilde{S} = (\tilde{s}_1, \ldots, \tilde{s}_T) = \text{TFDI}(c_1, \ldots, c_k, 0, \ldots, 0) - \text{TFDI}(c_1, \ldots, c_T) = -\text{TFDI}(0, \ldots, 0, c_{k+1}, \ldots, c_T)$ correspondant à la différence entre la courbe de charge dont les $T - k$ coefficients de la TFD sont remplacés par des zéros et la courbe de charge initiale (erreur de reconstruction).

Soit $\overline{S} = (\bar{s}_1, \ldots, \bar{s}_T) = \text{TFDI}(\bar{c}_1 + \mathcal{L}(\frac{M_1\sqrt{2}}{\epsilon/k}), \ldots, \bar{c}_k + \mathcal{L}(\frac{M_k\sqrt{2}}{\epsilon/k}), c_{k+1}, \ldots, c_T) - \text{TFDI}(c_1, \ldots, c_T) = \text{TFDI}(d_1 + \mathcal{L}(\frac{M_1\sqrt{2}}{\epsilon/k}), \ldots, d_k + \mathcal{L}(\frac{M_k\sqrt{2}}{\epsilon/k}), 0, \ldots, 0)$ *correspondant à la différence entre la courbe de charge dont les* k *premiers coefficients de la* TFD *sont bornés et bruités et la courbe de charge initiale (erreur de perturbation).*

Ainsi on obtient :

$$\widehat{S} = S + \overline{S} + \widetilde{S}$$

Soit $S + 1 = (s_1 + 1, \ldots, s_T + 1)$*, on a :*

$$\frac{\widehat{S} - S}{S + 1} = \frac{\overline{S}}{S + 1} + \frac{\widetilde{S}}{S + 1}$$

Donc

$$\begin{aligned}\left\|\frac{\widehat{S} - S}{S + 1}\right\|_1 &= \left\|\frac{\overline{S}}{S + 1} + \frac{\widetilde{S}}{S + 1}\right\|_1 \\ &\leq \left\|\frac{\overline{S}}{S + 1}\right\|_1 + \left\|\frac{\widetilde{S}}{S + 1}\right\|_1\end{aligned}$$

*Ainsi, l'*ERM *de l'*APFB *(respectivement de l'*APOB*) est inférieure ou égale à la somme de l'erreur de perturbation et de l'erreur de reconstruction de l'*APFB *(respectivement de l'*APOB*).*

Dans la section 5.4.1, nous avons vu que la TFD a une erreur de reconstruction inférieure à celle des TOD considérées. Par exemple quand $N = 450$ et $k = 5$ la médiane de l'erreur de reconstruction est de 6% pour la TFD contre 13% pour la transformée de Haar et celle de Daubechies 2.

Cependant, la section 5.4.2 montre que les algorithmes basés sur la TFD ont une erreur de perturbation plus importante que ceux basés sur la TOD. Les algorithmes basés sur la TFD ont deux fois plus de valeurs à bruiter (parties réelle et imaginaire des coefficients complexe) que ceux utilisant la TOD. De plus, le paramètre du bruit Laplace est plus grand d'un facteur $\sqrt{2}$ dans les algorithmes utilisant la TFD par rapport à ceux utilisant la TOD.

D'après le lemme 5.4.1, l'erreur totale appelée ici ERM est inférieure ou égale à la somme de l'erreur de reconstruction et de l'erreur de perturbation. Comme la TOD a une erreur de reconstruction (la médiane) supérieure à 9%, alors l'erreur totale de l'APOB n'ira pas en dessous de ce seuil même si le bruit de Laplace diminue, c'est-à-dire, quand le nombre de foyers N ou le budget de privacy ϵ augmente. Cependant, comme la TFD a une erreur de reconstruction faible (médiane entre 2% et 3% quand $k = 7, 8, 9$), alors l'erreur totale de l'APFB pourra être en-dessous de celle de l'APOB quand l'impact du bruit de Laplace diminue. Par exemple la médiane de l'erreur de perturbation de l'APFB est comprise entre 3% et 5% quand $k = 7, 8, 9$, $N = 550$ et $\epsilon = 3$.

Cette analyse explique pourquoi, pour $\epsilon = 1$, l'APOB obtient une meilleure utilité que l'APFB quand le nombre de foyers N est inférieur à 250. Par exemple, quand $N = 50$ et $k = 5$, la médiane de l'erreur de perturbation (respectivement de l'erreur de reconstruction) de l'APFB est de 70% (respectivement de 10%) contre 32% (respectivement 18%) pour l'APOB en utilisant Haar. Ainsi la médiane de l'ERM est comprise entre 70% et 80% pour l'APFB contre 32% et 50% pour l'APOB. Quand N est supérieur à 250, l'APFB obtient une meilleure utilité que l'APOB. Par exemple, quand $N = 450$ et $k = 5$, la médiane de l'erreur de perturbation (respectivement de l'erreur de reconstruction) de l'APFB est de 8.5% (respectivement de 6.5%) contre 4.5% (respectivement 16%) pour l'APOB en utilisant Haar. Ainsi la médiane de l'ERM est comprise entre 8.5% et 15% pour l'APFB contre 16% et 20.5% pour l'APOB.

De même, quand le budget de privacy augmente à $\epsilon = 3$ (le bruit diminue), la tendance s'inverse quand $N = 150$. C'est-à-dire, l'APOB obtient la meilleure utilité par rapport à l'APFB quand le nombre de foyers N est strictement inférieur à 150. Et l'APFB obtient la meilleure utilité quand N est supérieur ou égal à 150.

En comparant les différentes techniques de publication de courbes de charge, il en ressort que les algorithmes de perturbation bornés obtiennent une meilleure utilité que les algorithmes non bornés. En outre, quand le nombre de foyers est supérieur à 250, l'APFB (algorithme de perturbation de Fourier borné) obtient la meilleure utilité, avec une erreur relative moyenne inférieure à 10% pour $\epsilon = 3$. Quand le budget de privacy $\epsilon = 1$, l'erreur relative moyenne de l'APFB est inférieure à 10% à partir de $N = 450$ foyers. En utilisant l'APFB, il est donc possible d'obtenir une bonne utilité en publiant des courbes de charge des habitants d'un quartier, tout en protégeant la vie privée des consommateurs. Il est donc possible de faire des analyses, comme le calcul des prévisions de consommation au niveau d'un quartier d'une taille supérieure à 250 (respectivement, 450) foyers pour un budget de privacy $\epsilon = 3$ (respectivement, $\epsilon = 1$).

Par ailleurs, il faut noter que dans ces travaux, nous avons considéré que la courbe de charge est corrélée sur toute une journée. Si cette condition de corrélation est relaxée, par exemple à 2h, alors le bruit ajouté diminuera, ce qui conduira à une meilleure utilité. Mais si, au contraire, on souhaite publier des courbes de charge sur une longue durée par exemple un trimestre, en considérant que chaque journée est corrélée, le bruit rajouté sera plus important et l'utilité sera moindre.

Le tableau 5.1 donne l'algorithme de publication qui a la plus petite ERM (erreur relative moyenne) en fonction du budget de privacy ϵ et du nombre de foyers dans le quartier (N).

5.5 Extension : publication de courbes de charge sans tiers de confiance

Dans les sections précédentes, nous avons montré comment publier une somme de courbes de charge en utilisant un tiers de confiance qui connait des courbes de charge individuelles de clients. Par exemple, on peut penser à Enedis qui publie des courbes de charge des habitants d'une commune pour les collectivités.

Taille du quartier (N)	Budget ϵ	Algorithme optimal	Coefficients k	Médiane de l'ERM
50	1	APOB – Haar, db2	5	35%
	3	APOB – Haar		21%
150	1	APOB – Haar	5	19%
	3	APFB		11%
250	1	APFB, APOB – Haar	5, 8 resp.	16%
	3	APFB	5	8%
350	1	APFB	5	12%
	3		8	7%
450	1	APFB	5	10%
	3		8	6%
550	1	APFB	5	9%
	3		8	5%

TABLEAU 5.1 – Algorithme de publication qui a la plus petite ERM en fonction du budget de privacy ϵ et du nombre de personnes dans le quartier (N)

Cependant, si l'agrégateur ou le tiers de confiance est malveillant, alors la vie privée des consommateurs est compromise. Cet agrégateur qui connait les courbes de charge individuelles des clients peut les vendre auprès d'autre organisation, par exemple pour des finalités d'espionnage, de publicité, etc.

Comme dans le cas d'usage du GEEQ (Gestionnaire d'Énergie de l'Éco-Quartier) (chapitre 4) où un fournisseur ou un gestionnaire de réseau cherche à réduire les pics de consommation dans un quartier sans révéler les consommations individuelles des foyers, cette section montre comment publier des sommes de courbes de charge en utilisant les algorithmes de perturbation bornés présentés plus haut (APFB et APOB) sans avoir un tiers de confiance. Ces agrégats de courbes de charge sont à destination d'un fournisseur ou d'un gestionnaire du réseau, et permettent de réaliser des services énergétiques comme la prévision de consommation présentée dans le chapitre 2.

Nous proposons deux variantes dont chacune utilise l'un des deux mécanismes suivants : le SMC (*Secure Multi-party Computation*) et la PHE (*Partially Homomorphic Encryption*). Avant de présenter la transformation des algorithmes de perturbations en une version décentralisée, nous présentons les hypothèses faites dans cette section.

5.5.1 Hypothèses

Dans cette section, nous supposons que :

— Chaque foyer i a une courbe de charge individuelle $X^i = (x_1^i, \ldots, x_T^i)$, avec $i = 1, \ldots, N$.

— La sensibilité maximale $M = (M_1, \ldots, M_k)$ est connue de tous les foyers.

— Chaque foyer i peut calculer la TFD ou la TOD de sa courbe de charge X^i.

— Tous les foyers peuvent communiquer entre eux de manière sécurisée (canaux authentifiés et chiffrés).

— Les foyers peuvent communiquer avec le destinataire de l'agrégat à calculer et à publier (fournisseur, GRD (gestionnaire de réseau de distribution), etc.) de manière sécurisée.

5.5.2 Algorithmes de perturbation bornés décentralisés en utilisant le SMC

En remarquant que le bruit de Laplace peut être divisé en plusieurs parts (lemme 3.1.1), chaque foyer peut ajouter une part de ce bruit à sa courbe de charge individuelle de telle sorte que la somme de courbe de charge garantisse la confidentialité différentielle, comme dans [3].

Le SMC présenté en section 3.1.2 permet de calculer une fonction sans révéler les entrées. Il est utilisé dans le chapitre 4, pour fournir un service de DR (*Demand Response*) sans apprendre de courbes de charge individuelles des foyers.

En combinant le SMC et la divisibilité de la distribution de Laplace, l'algorithme 14 permet de calculer les algorithmes de perturbation bornés (APFB et APOB) de manière décentralisée.

Il faut noter que l'algorithme 14 résiste aux attaquants (foyers) HBC (*Honest-but-Curious* ou honnête mais curieux).

Le fournisseur obtient uniquement un résultat lui permettant de calculer la somme de courbes de charge bruitée, sans avoir accès aux courbes de charge individuelles des foyers. En effet, l'algorithme renvoie les coefficients bruités de la transformée considérée et de la somme bruitée. Il suffit de calculer l'inverse de la transformée pour obtenir la somme bruitée. Comme les calculs distribués sont couteux en communication, ce choix permet de gagner en performances.

5.5.3 Algorithmes de perturbation bornés décentralisés en utilisant le PHE

Cette section utilise du PHE pour calculer les algorithmes de perturbation bornés de manière décentralisée. Dans la section 3.2.3, nous avons présenté des applications permettant de calculer un agrégat de manière sécurisée en utilisant le chiffrement de Paillier [124]. Par exemple, l'algorithme d'agrégation de Borges et coll. [20] ou celui de Garcia et coll. [65] permettent de calculer un agrégat sans révéler les entrées.

Ainsi, comme le bruit de Laplace peut être divisé en plusieurs parts, chaque foyer peut ajouter une part à sa courbe de charge de telle sorte que le calcul de la somme de courbes de charge via un algorithme d'agrégation sécurisée garantit la DP.

L'algorithme 15 permet de calculer une agrégation sécurisée sans révéler les consommations individuelles en utilisant Paillier.

7. La distribution du bruit de Laplace est $\mathcal{L}(\frac{M_j}{\epsilon/k})$ en utilisant la TOD, et $\mathcal{L}(\frac{M_j\sqrt{2}}{\epsilon/k})$ en utilisant la TFD.

Algorithme 14 Algorithme de perturbation borné décentralisé utilisant du SMC

Entrées :

- Courbes de charge : $X = (X^1, \ldots, X^n)$ avec $X^i = (x_1^i, \ldots, x_T^i)$ pour $i = 1, \ldots, n$
- Nombre de coefficients de la transformée considérée à conserver : k
- Sensibilité maximale pour les k premiers coefficients de la transformée considérée (TFD ou TOD) : $M = (M_1, \ldots, M_k) \in \mathbb{R}_+^k$
- Budget de privacy : ϵ

Algorithme :

1. **Bornage :**
   - Chaque foyer calcule les k premiers coefficients de la transformée (TFD ou TOD) de X^i :
     $C_k^i = \text{transformee}(X^i) = (c_1^i, \ldots, c_k^i)$, avec transformee égal à TFD ou TOD
   - Si $|c_j^i| > M_j$, alors remplacer c_j^i par $\frac{c_j^i \times M_j}{|c_j^i|}$ pour tout $j = 1, \ldots, k$
2. **Mécanisme de Laplace** : Chaque foyer ajoute un bruit de Gamma aux coefficients calculés :
   $\hat{c}_j^i = c_j^i + \gamma_i$ pour tout $j = 1, \ldots, k$ tel que $\sum_{i=1}^n \gamma_i = \mathcal{L}(\frac{M_j}{\epsilon/k})$ [7]en utilisant la divisibilité de la distribution de Laplace (lemme 3.1.1).
3. En utilisant le SMC, tous les foyers calculent conjointement la somme $\hat{c}_j = \sum_{i=1}^n \hat{c}_j^i$ et révèlent le résultat pour tout $j = 1, \ldots, k$. On note $\widehat{C}_k = (\hat{c}_1, \ldots, \hat{c}_k)$
4. Une partie ajoute $T - k$ zéros à $\hat{C}_k$:
   $$\widehat{C}_k = (\hat{c}_1, \ldots, \hat{c}_k, 0, \ldots, 0)$$
5. renvoyer le résultat $\widehat{C}_k$ au fournisseur qui calcule la transformer inverse (TFDI ou TODI (transformée en ondelettes discrète inverse)) pour obtenir la version bruitée de S notée :
   $$\widehat{S} = \text{transformeeInverse}(\widehat{C}_k) = (\hat{s}_1, \ldots, \hat{s}_T),$$
   où transformeeInverse désigne la TFDI ou la TODI

Sortie : somme de courbes de charge bruitée

En combinant l'algorithme 15 et la divisibilité de la distribution de Laplace, l'algorithme 16 permet de calculer les algorithmes de perturbation bornés (APFB et APOB) de manière décentralisée.

8. La distribution du bruit de Laplace est $\mathcal{L}(\frac{M_j}{\epsilon/k})$ en utilisant la TOD, et $\mathcal{L}(\frac{M_j\sqrt{2}}{\epsilon/k})$ en utilisant la TFD.

Algorithme 15 Algorithme d'agrégation sécurité, par exemple [20, 65] (section 3.2.3)

Entrées : $x_1, \ldots, x_n$ avec x_i valeur secrète du foyer i, avec $i = 1, \ldots, N$
En utilisant un algorithme d'agrégation sécurisée, présenté dans la section 3.2.3, les foyers peuvent calculer une somme de leurs données individuelles sans jamais les révéler (c'est uniquement le résultat de la somme qui est révélé). Ici x_i correspond par exemple à un bruit de Gamma, additionné à une composante des coefficients de la transformée considérée (TFD ou TOD) du foyer i, pour $i = 1, \ldots, N$.
Sortie : $X = \sum_{i=1}^{N} x_i$

Algorithme 16 Algorithme de perturbation borné décentralisé en utilisant l'agrégation sécurisée (algorithme 15)

Entrées :

- Courbes de charge : $X = (X^1, \ldots, X^n)$ avec $X^i = (x_1^i, \ldots, x_T^i)$ pour tout $i = 1, \ldots, n$
- Nombre de coefficients de la transformée considérée à conserver : k
- Sensibilité maximale pour les k premiers coefficients de la transformée considérée (TFD ou TOD) : $M = (M_1, \ldots, M_k) \in \mathbb{R}_+^k$
- Budget de privacy : ϵ

Algorithme :

1. **Bornage :**
   - Chaque foyer calcule les k premiers coefficients de la transformée (TFD ou TOD) de X^i :
     $C_k^i = \text{transformee}(X^i) = (c_1^i, \ldots, c_k^i)$, avec transformee égal à TFD ou TOD
   - Si $|c_j^i| > M_j$, alors remplacer c_j^i par $\frac{c_j^i \times M_j}{|c_j^i|}$ pour tout $j = 1, \ldots, k$
2. **Mécanisme de Laplace** : Chaque foyer ajoute un bruit de Gamma aux coefficients calculés :
   $\hat{c}_j^i = c_j^i + \gamma_i$ pour tout $j = 1, \ldots, k$ tel que $\sum_{i=1}^n \gamma_i = \mathcal{L}(\frac{M_j}{\epsilon/k})$ [8]en utilisant la divisibilité de la distribution de Laplace (lemme 3.1.1).
3. En utilisant l'algorithme 15, tous les foyers calculent conjointement la somme $\hat{c}_j = \sum_{i=1}^n \hat{c}_j^i$ et révèlent le résultat pour tout $j = 1, \ldots, k$. On note $\widehat{C}_k = (\hat{c}_1, \ldots, \hat{c}_k)$
4. Une partie ajoute $T - k$ zéros à $\hat{C}_k$:
   $$\widehat{C}_k = (\hat{c}_1, \ldots, \hat{c}_k, 0, \ldots, 0)$$
5. renvoyer le résultat $\widehat{C}_k$ au fournisseur qui calculer la transformer inverse (TFDI ou TODI) pour obtenir la version bruitée de S notée :
   $$\widehat{S} = \text{transformeeInverse}(\widehat{C}_k) = (\hat{s}_1, \ldots, \hat{s}_T),$$
   avec transformeeInverse égal à TFDI ou TODI

Sortie : somme de courbes de charge bruitée

5.6 Conclusion

Ce chapitre propose principalement deux contributions : Premièrement, il analyse l'APF (algorithme de perturbation de Fourier) proposé par Rastogi et Nath [130], et réutilisé plusieurs fois, notamment dans [4, 106]. Cette analyse montre que l'APF initialement proposé ne garantit pas le niveau de protection annoncé. Une correction de cette erreur est faite, notamment en calculant correctement la sensibilité de la TFD (transformée de Fourier discrète) utilisée dans cet algorithme. Cependant, cette correction rend l'APF peu utile pour notre cas d'usage : l'ERM de l'APF est de 61% pour la publication de la courbe de charge de N foyers, alors que l'ERM souhaitée devrait être moins de 10%.

D'autre part, nous avons proposé deux algorithmes de perturbation (APFB (algorithme de perturbation de Fourier borné) et APOB (algorithme de perturbation en ondelettes borné)) permettant de publier des sommes de courbes de charge en garantissant la DP, tout en préservant l'utilité de l'agrégat. Ces algorithmes minimisent le bruit de Laplace introduit sur les coefficients des transformées, en utilisant un mécanisme de bornage qui réduit la sensibilité globale des transformées. L'APFB obtient un gain d'utilité d'un facteur supérieur à 6 par rapport à l'APF, tandis que l'APOB obtient un gain d'utilité d'un facteur 2 par rapport à l'APO.

Avec un budget de privacy $\epsilon = 1$, l'APFB obtient une ERM (erreur relative moyenne) de moins de 10% pour la publication de la somme de courbes de charge à partir de 450 foyers. Plus le nombre de foyers (N) augmente, plus l'ERM diminue comme le montre la table 5.1.

Le choix des k coefficients conservés dans les algorithmes de perturbation joue un rôle important dans l'obtention d'une bonne utilité. Au lieu de choisir uniquement les k premiers coefficients de la transformée considérée, conserver les k coefficients ayant une plus grande amplitude pourrait permettre de réduire l'erreur de reconstruction et donc l'ERM. Cependant, le choix de ces k coefficients doit se faire de manière confidentielle. Le mécanisme exponentiel [49] permettant de garantir la DP peut être utilisé dans ce contexte.

Chapitre 6

Conclusion et perspectives

6.1 Conclusion

Les *smart grids* ou réseaux électriques intelligents permettent de fournir de nouveaux services énergétiques à l'échelle d'un quartier, ville, région etc. Ces smart grids sont un outil important pour lutter contre le changement climatique, via des services permettant d'optimiser la consommation des foyers et donc de réduire la production, et par conséquent des émissions de GES (gaz à effet de serre).

Cependant, pour être efficaces, ces services collectent des données fines de consommations des foyers, encore appelées courbes de charge. Ces courbes de charge révèlent les habitudes des habitants du foyer, qui sont associés à ces données. Ce qui pose des problèmes de vie privée.

Dans cette thèse, nous avons proposé cinq contributions qui peuvent être classées en deux thèmes. Nous nous sommes intéressés en premier lieu à la mise en œuvre d'un service de DR (*Demand Response*), permettant d'éviter les pics de consommation dans un quartier sans collecter les courbes de charge des foyers. Ce service appelé GEEQ (Gestionnaire d'Énergie de l'Éco-Quartier) protégé est une transformation d'un algorithme réel de DR en le rendant respectueuse de la vie privée, tout en préservant son efficacité de réduction des pics de consommations. Le GEEQ protégé utilise du SMC (*Secure Multi-party Computation*) permettant d'effectuer des opérations de manière décentralisée. L'une des différences importante qui diffère le GEEQ protégé du GEEQ est qu'il est distribué. En cas d'attaque réussie dans un système centralisé comme le GEEQ, toutes les données des foyers (identifiants, prévisions de consommation, flexibilités, etc.) seront compromises, ce qui pose des problèmes à la fois au fournisseur (amendes pour non-respect de la protection des données des clients, dégradation de l'image de marque, etc.) et aux clients (vol d'identité, hameçonnage, etc.). Dans le GEEQ protégé, la compromission d'un foyer, en cas de succès d'une attaque, ne permet pas de faire fuiter les consommations individuelles des autres foyers.

Le deuxième thème est la publication de courbes de charge des foyers en protégeant les clients du risque de ré-identification de leurs courbes de charge. Dans cette partie, nous présentons premièrement l'APF (algorithme de perturbation de Fourier) proposé initialement

par Rastogi et Nath [130], qui consiste à publier des séries temporelles en combinant la DP (*Differential Privacy*) avec la TFD (transformée de Fourier discrète). L'idée consiste dans un premier temps à compresser la série temporelle à publier, en la transformant dans le domaine fréquentiel à l'aide de la TFD, et en conservant uniquement les basses fréquences de la transformée obtenue (les premiers coefficients). L'étape suivante consiste à perturber les coefficients de la transformée obtenue en garantissant la DP. La série temporelle bruitée à publier est obtenue en calculant la transformée inverse du résultat. Cette méthode permet d'obtenir une meilleure utilité par rapport à la méthode naïve, qui consiste à perturber directement la série temporelle initiale. Cependant, l'APF présente une erreur dans l'estimation de la sensibilité permettant de perturber les coefficients de la TFD. En corrigeant cette erreur, l'APF devient inefficace.

Pour résoudre ce problème nous avons ensuite développé deux optimisations de cet algorithme, en bornant les coefficients des transformées considérées (TFD et TOD (transformée en ondelettes discrète)), ce qui permet de réduire la sensibilité et donc la perturbation introduite. Les algorithmes obtenus garantissent une bonne protection ainsi qu'une bonne utilité, avec une erreur relative inférieure à 10% pour une taille d'agrégat de 450 foyers et un budget de privacy $\epsilon = 1$.

La dernière contribution est une décentralisation des deux algorithmes proposés permettant de résister aux agrégateurs malveillants. Cette méthode combine des technologies de calculs d'agrégations sécurisés et la DP. Par exemple, nous combinons le SMC avec la DP.

Toutes ces contributions ont été implémentées et testées afin d'évaluer leurs performances. Nous avons utilisé le *framework* SCALE-MAMBA, pour comparer le GEEQ et sa version protégée. Les résultats de simulation montrent une erreur relative entre 1% et 2%, c'est-à-dire, le nombre de réductions en utilisant la version protégée est supérieur à celui pour la version non protégée. Ce résultat s'explique par le fait que le GEEQ protégé sollicite un nombre fixe de foyers pour réduire leur consommation lors d'un pic, alors que dans le GEEQ initial les foyers sont sollicités l'un après l'autre jusqu'à la réduction du pic. Par exemple si le nombre de clients sollicités en cas d'un pic de consommation est de 5 dans le GEEQ protégé, et que la réduction de consommation par 2 foyers suffit pour réduire ce pic, alors, dans le GEEQ uniquement 2 foyers seront sollicités contre 5 dans la version protégée. D'où une sur-sollicitation dans la version protégé.

Les algorithmes de publication de courbes de charge proposés ont été implémentés en Python 3, et testés sur un jeu de données de consommation de la commission de régulation irlandaise de l'énergie CER. En calculant la distribution de l'erreur relative entre la somme bruitée et celle non protégée des courbes de charge, la médiane de l'erreur relative moyenne est inférieure à 10% à partir d'une taille d'agrégat de 450 foyers, en utilisant un budget de privacy $\epsilon = 1$.

6.2 Perspectives

Plusieurs travaux peuvent être envisagés à la suite de cette thèse.

1. La première contribution de cette thèse vise à transformer un service de DR en le rendant respectueux de la vie privée. Cet algorithme a été simulé sur un LAN (*Local Area Network*) en utilisant le *framework* SCALE-MAMBA. Ce qui montre la faisabilité de cette solution. Cependant, en utilisant du SMC, les foyers doivent communiquer entre eux, par exemple en P2P (Pair-à-Pair). Une amélioration de cette contribution pourrait être d'implémenter cette solution sur un réseau MAN (*Metropolitan Area Network*) en utilisant par exemple des Raspberry Pi, ce qui rapprocherait l'expérimentation des conditions d'une architecture réelle permettant aux foyers de communiquer entre eux.
2. Dans le chapitre 5, nous avons présenté des algorithmes de publication de courbes de charge en garantissant la DP, avec un budget ϵ sur une journée. Les algorithmes proposés préservent l'utilité de la publication, c'est-à-dire avec une ERM (erreur relative moyenne) faible entre l'agrégat perturbé et celui d'origine. Par exemple, pour un agrégat de 450 foyers, l'APFB (algorithme de perturbation de Fourier borné) obtient une ERM de 10% pour un budget de privacy de $\epsilon = 1$ sur la journée.
   Cependant, en publiant plusieurs courbes de charge pendant plusieurs jours, si les courbes de charge journalières sont corrélées, alors le budget de privacy s'additionne comme le montre le théorème 3.1.2. Par exemple, en publiant une courbe de charge chaque jour pendant 30 jours avec un budget journalier $\epsilon = 1$, le budget total au bout des 30 jours est de $\epsilon = 30$, en considérant que les courbes de charge sont corrélées. Or, un budget $\epsilon = 30$ est élevé, et ne permet donc pas de protéger la publication des données contre des attaques de ré-identification des courbes de charge individuelles des consommateurs. Pour résoudre ce problème, Wang et coll. [147] présentent une nouvelle technique de publication de séries temporelles corrélées en utilisant la DP. Les auteurs proposent un nouveau mécanisme appelé mécanisme de Laplace corrélé qui permet de garantir que les données corrélées bruitées et celles d'origine sont indistinguables. Ces techniques de publications de données corrélées doivent être étudiées.
3. Le *framework* de privacy appelé *Pufferfish* [85] permet de créer de nouvelles définitions de privacy, et peut être utilisé pour définir une protection adaptée pour les séries temporelles corrélées. Des applications utilisant Pufferfish [141, 149] proposent des algorithmes de publications de séries temporelles corrélées garantissant la DP. Ce *framework* ainsi que d'autres méthodes permettant de publier des séries temporelles en temps réel en garantissant la DP doivent être investiguées [145, 148]. Ce qui permettrait de publier de plus nombreuses courbes de charge (par exemple sur plusieurs années) en garantissant que l'ensemble des publications ne fait pas fuiter les données individuelles. Avec les techniques actuelles, plus on publie des données, plus le budget de privacy augmente ainsi que le risque de ré-identification des données individuelles.

Lexique

APF algorithme de perturbation de Fourier. 5, 7, 42, 59, 60, 63, 67–70, 73–75, 78, 80–82, 84, 86, 94

APFB algorithme de perturbation de Fourier borné. 8, 60, 75, 77–82, 84–94, 97

APO algorithme de perturbation en ondelettes. 7, 8, 42, 60, 63, 67, 69–72, 74, 75, 80–84, 86, 94

APOB algorithme de perturbation en ondelettes borné. 5, 8, 60, 78–94

byzantins attaquants qui peuvent se comporter arbitrairement, qui peuvent modifier des données de consommation. 31, 40

CER *Commission for Energy Regulation*, ou commission de la régulation énergétique. 7, 8, 13, 16–18, 52, 61, 62, 64, 68, 70, 72–76, 78–81, 97

CJUE Cour de justice de l'Union européenne. 23, 24

CNIL Commission Nationale de l'Informatique et des Libertés. 11, 16, 22, 24

consomm'acteur consommateur qui produit de l'électricité grâces aux sources d'énergie renouvelables. 20

DCP donnée permettant d'identifier directement ou indirectement une personne physique. 11–13, 21, 23, 24, 42, 44, 45, 48, 49, 51, 56, 59

deep learning ou apprentissage en profondeur, est un ensemble de méthodes d'apprentissage automatique tentant de modéliser avec un haut niveau d'abstraction des données grâce à des architectures articulées de différentes transformations non linéaires. 20

DP *Differential Privacy*, ou confidentialité différentielle, une définition formelle de la garantie de vie privée apportée par un algorithme. 1, 2, 11–13, 25, 33–37, 39, 41–43, 58–61, 67, 68, 77, 79, 94–97

DPD Data Protection Directive. 23

DR *Demand Response*, algorithme effacement à la pointe permettant d'éviter les pics de consommation. 11, 13, 15, 18, 19, 37, 41–45, 92, 96, 97

EDF Electricité de France. 18, 20

EJP Effacements Jour de Pointe. 18

ELD entreprises locales de distribution. 14

Enedis distributeur d'énergie en France. 14–16, 20, 22, 23, 59, 60, 91, 99

ENR énergie renouvelable. 1, 10, 11, 14, 15, 19, 20

ERL Emetteur Radio Linky. 16, 20

ERM erreur relative moyenne. 8, 61, 78, 80–84, 87, 90–92, 94, 95, 97

erreur de perturbation erreur de perturbation due à au bruit introduit par le mécanisme de Laplace. 68, 81–84, 86, 87, 90, 91

erreur de reconstruction erreur de reconstruction due à l'ignorance des $T - k$ coefficients de la transformée (TFD ou TOD). 8, 63, 68, 81–85, 87, 90, 91, 94

FHE *Fully Homomorphic Encryption*, ou chiffrement totalement homomorphe, du chiffrement qui permet d'effectuer toutes fonctions calculables sur des données chiffrées. 25, 26

GEEQ Gestionnaire d'Énergie Éco-Quartier, un dispositif permettant d'éviter les surconsommations au niveau d'un quartier. 7, 12, 13, 19, 27, 45–58, 91, 96, 97

GES gaz à effet de serre. 10, 11, 14, 43, 96

GESH Gestionnaire d'Énergie de Smart Home, un dispositif permettant de gérer l'utilisation des appareils flexibles des utilisateurs dans le foyer. 46–51, 55–57

GRD gestionnaire de réseau de distribution. 1, 11, 14, 16, 42, 92

HBC *Honest-but-Curious* ou honnête mais curieux, attaquants qui suivent le protocole mais essayent d'obtenir des informations confidentielles sur les autres participants. 40, 93

IA intelligence artificielle. 19

ICS Information Commercialement Sensible. 22–24

LAN *Local Area Network*, ou réseau local, peu étendu. 32, 97

l'attaque de différence [39] attaque permettant de retrouver indirectement une donnée individuelle d'un utilisateur à partir de deux agrégats différents en cette donnée. 33

Linky Compteur communicant, appartenant à Enedis. 15, 20

LTECV loi relative à la transition énergétique pour la croissance verte, publiée au Journal Officiel du 18 août 2015. 10, 14

MAC *Message Authentication Code*, ou code d'authentification de message, un code permettant d'authentifier une valeur. 29–32, 48, 51

MAN *Metropolitan Area Network*, ou réseau métropolitain. 97

MASCOT Protocole permettant d'effectuer du calcul multipartite sécurisé développé par Keller, Orsini et Scholl [83]. 32, 33

NALM *Non-Intrusive Appliance Load Monitoring*, une technique qui permet d'identifier les usages à partir d'une courbe de charge. 7, 11, 15, 21, 22, 37–39, 59

NILL Union Européenne. 38

P2P Pair-à-Pair, modèle d'échange où chaque entité du réseau est à la fois client et serveur. 51, 97

PBD Privacy-by-Design. 23

PET *Privacy-Enhancing Technology*, se dit d'une technologie visant à protéger la vie privée. 4, 11, 25, 37, 43

PHE *Partially Homomorphic Encryption*, ou chiffrement partiellement homomorphe, du chiffrement qui permet d'effectuer certains calculs sur des données chiffrées. 25, 26, 37, 40–43, 92, 94

RGPD Règlement Général sur la Protection des Données [131]. 11, 13, 22–24, 39

RTE réseau de transport d'électricité. 14, 22

SEIDO Laboratoire commun entre EDF R&D, Télécom Paris, Télécom SudParis et LAAS–CNRS. 45

SM *smart meter*, ou compteur communicant. 60

smart grid Réseau électrique intelligent. 4, 11, 13–15, 24, 96

SMC *Secure Multi-party Computation*, ou calcul multipartite sécurisé, une technique qui permet de calculer une fonction à partir de plusieurs entrées fournies par plusieurs parties sans révéler directement les entrées. 1, 2, 11–13, 25, 27, 32–34, 36, 37, 41–43, 45, 49, 51, 56–58, 92, 93, 96, 97

SPDZ Protocole permettant d'effectuer du calcul multipartite sécurisé développé par Damgård, Pastro, Smart, et Zakarias [37]. 32

SVM *Support Vector Machines*, ou machines à vecteurs de support ou séparateurs à vaste marge, sont un ensemble de techniques d'apprentissage supervisé destinées à résoudre des problèmes de discriminationnote 1 et de régression. Les SVM sont une généralisation des classifieurs linéaires. . 19

SWHE *Somewhat Homomorphic Encryption*, ou chiffrement quelque peu homomorphe, permettant de calculer certaines fonctions limitées sur des chiffrés. 25–27, 32

TFD transformée de Fourier discrète. 5, 8, 42, 60, 63, 64, 67–78, 80, 84–88, 90–95, 99

TFDI transformée de Fourier discrète inverse. 68, 69, 74, 77, 88–90, 93, 95

TIC télé information client. 16

TOD transformée en ondelettes discrète. 8, 42, 63, 64, 67–71, 75, 78–81, 84–86, 90, 92–95, 99

TODI transformée en ondelettes discrète inverse. 71, 80, 93, 95

TTP *Trusted third parties*, ou tierces parties de confiance, des parties qui doivent se comporter honnêtement pour assurer la sécurité d'un protocole. 41

UE Union Européenne. 10, 23, 24

WAN *Wide Area Network*, ou réseau étendu. 32

ZK-PEQ *Zero-Knowledge proof of Plaintext EQuality*, ou preuve à divulgation nulle de connaissance d'égalité de texte clair, des preuves qui permettent d'assurer que les textes clairs derrière deux chiffrés distincts sont égaux. 41

Publications

Conférences et Journaux

[5] Ghislain Agoua, Ivan Gazeau, Benoît Grossin, Paul Lajoie-Mazenc et Franklin Leukam Lako. « Publication de données de consommation électrique et risque de réidentification ». Dans : *Lavoisier Collection EDF R&D* (2021, (en cours)).

[7] Sawsan Al Zahr, Paul Lajoie-Mazenc et Franklin Leukam Lako. « Protection des données à caractère personnel dans les services énergétiques à l'échelle d'un quartier ». Dans : *Lavoisier Collection EDF R&D* (2021, (en cours)). Lavoisier.

[97] Franklin Leukam Lako, Paul Lajoie-Mazenc et Maryline Laurent. « Personal Data Protection in Energy Services – Survey ». Dans : *Cryptacus*. 2018.

[98] Franklin Leukam Lako, Paul Lajoie-Mazenc et Maryline Laurent. « Privacy-preserving Publication of Time-series Data in Smart Grid ». Dans : *Security and Communication Networks* (2021).

[100] Franklin Leukam Lako, Paul Lajoie-Mazenc et Maryline Laurent. « Reconciling Privacy and Utility for Energy Services–an Application to Demand Response Protocols ». Dans : *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE. 2020, pages 348-355.

Brevets

[99] Franklin Leukam Lako, Paul Lajoie-Mazenc et Maryline Laurent. « Procédé de gestion de consommation dans un réseau de distribution ». FR3097087. 2019.

Présentations

[90] Franklin Leukam Lako. *Algorithme d'effacement à la pointe respectueux de la vie privée*. Séminaire R3S des doctorants, 2020.

[91] Franklin Leukam Lako. *Comment sécuriser et partager des données de consommation à l'échelle du quartier ?* Séminaire Privacy et espaces publics : l'enjeu territorial – EDF R&D, 2018.

[92] Franklin Leukam Lako. *Personal Data Protection in Energy Services.* Séminaire EDF R&D des doctorants, 2019.

[93] Franklin Leukam Lako. *Personal Data Protection in Energy Services.* Séminaire SAMOVAR des doctorants, 2018.

[94] Franklin Leukam Lako. *Protection des données à caractère personnel pour les services énergétiques.* Workshop SEIDO Lab, 2019.

[95] Franklin Leukam Lako. *Protection des données à caractère personnel pour les services énergétiques.* Workshop SEIDO Lab, 2020.

[96] Franklin Leukam Lako. *Reconciling Privacy and Utility for Energy Services – an Application to Demand Response Protocols.* 2020 International Workshop on Privacy Engineering – IWPE'20.

Références

[1] Abbas Acar, Hidayet Aksu, A Selcuk Uluagac et Mauro Conti. « A survey on homomorphic encryption schemes : Theory and implementation ». Dans : *ACM Computing Surveys (CSUR)* 51.4 (2018), pages 1-35.

[2] Gergely Acs, Claude Castelluccia et William Lecat. « Protecting against physical resource monitoring ». Dans : *Proceedings of the 10th annual ACM workshop on Privacy in the electronic society*. 2011, pages 23-32.

[3] Gergely Ács et Claude Castelluccia. « I have a DREAM ! (DiffeRentially privatE smArt Metering) ». Dans : *International Workshop on Information Hiding*. 2011.

[4] Gergely Ács, Claude Castelluccia et Rui Chen. « Differentially private histogram publishing through lossy compression ». Dans : *2012 IEEE 12th International Conference on Data Mining*. IEEE. 2012, pages 1-10.

[5] Ghislain Agoua, Ivan Gazeau, Benoît Grossin, Paul Lajoie-Mazenc et Franklin Leukam Lako. « Publication de données de consommation électrique et risque de réidentification ». Dans : *Lavoisier Collection EDF R&D* (2021, (en cours)).

[6] Sawsan Al Zahr, Elias A Doumith et Philippe Forestier. « Advanced demand response considering modular and deferrable loads under time-variable rates ». Dans : *GLOBECOM 2017-2017 IEEE Global Communications Conference*. IEEE. 2017, pages 1-6.

[7] Sawsan Al Zahr, Paul Lajoie-Mazenc et Franklin Leukam Lako. « Protection des données à caractère personnel dans les services énergétiques à l'échelle d'un quartier ». Dans : *Lavoisier Collection EDF R&D* (2021, (en cours)). Lavoisier.

[8] Abdelrahaman Aly, Daniele Cozzo, Marcel Keller, Emmanuela Orsini, Dragos Rotaru, Peter Scholl, Nigel P. Smart et Tim Wood. « SCALE–MAMBA v1.6 : Documentation ». Dans : (2019).

[9] *Arrêté du 4 janvier 2012 pris en application de l'article 4 du décret n° 2010-1022 du 31 août 2010 relatif aux dispositifs de comptage sur les réseaux publics d'électricité*. https://www.legifrance.gouv.fr/loda/id/JORFTEXT000025126353/2016-11-09/. Janvier 2012.

[10] Aurélien Pennec. *EDF EJP, jours et tarifs : doit-on rester chez EJP en 2020 ?* https://www.lesfurets.com/energie/guide/electricite-quest-loption-effacement-jour-de-pointe-ejp. Septembre 2020.

[11] Michael Backes et Sebastian Meiser. « Differentially private smart metering with battery recharging ». Dans : *Data Privacy Management and Autonomous Spontaneous Security*. Springer, 2013, pages 194-212.

[12] Michael Barbaro et Zeller Jr. Tom. *A Face Is Exposed for AOL Searcher No. 4417749*. 2006.

[13] Nipun Batra, Jack Kelly, Oliver Parson, Haimonti Dutta, William Knottenbelt, Alex Rogers, Amarjeet Singh et Mani Srivastava. « NILMTK : an open source toolkit for non-intrusive load monitoring ». Dans : *Proceedings of the 5th international conference on Future energy systems*. 2014, pages 265-276.

[14] Gerald Bauer, Karl Stockinger et Paul Lukowicz. « Recognizing the use-mode of kitchen appliances from their current consumption. » Dans : *EuroSSC* 9 (2009), pages 163-176.

[15] Rikke Bendlin, Ivan Damgård, Claudio Orlandi et Sarah Zakarias. « Semi-homomorphic encryption and multiparty computation ». Dans : *EUROCRYPT*. 2011.

[16] Fabrice Benhamouda, Tancrède Lepoint, Claire Mathieu et Hang Zhou. « Optimization of bootstrapping in circuits ». Dans : *Proceedings of the Twenty-Eighth Annual ACM-SIAM Symposium on Discrete Algorithms*. SIAM. 2017, pages 2423-2433.

[17] Antoine Bonduelle, Mathilde Szuba et Bertrand Zuindeau. *Facteur 4 : le chantier social et politique*. http://journals.openedition.org/developpementdurable/8905. Mars 2011.

[18] Dan Boneh, Eu-Jin Goh et Kobbi Nissim. « Evaluating 2-DNF formulas on ciphertexts ». Dans : *Theory of cryptography conference*. Springer. 2005, pages 325-341.

[19] Roberto Bonfigli, Stefano Squartini, Marco Fagiani et Francesco Piazza. « Unsupervised algorithms for non-intrusive load monitoring : An up-to-date overview ». Dans : *2015 IEEE 15th International Conference on Environment and Electrical Engineering (EEEIC)*. IEEE. 2015, pages 1175-1180.

[20] Fábio Borges, Denise Demirel, Leon Böck, Johannes Buchmann et Max Mühlhäuser. « A privacy-enhancing protocol that provides in-network data aggregation and verifiable smart meter billing ». Dans : *2014 IEEE Symposium on Computers and Communications (ISCC)*. IEEE. 2014, pages 1-6.

[21] Zvika Brakerski, Craig Gentry et Vinod Vaikuntanathan. « (Leveled) Fully Homomorphic Encryption without Bootstrapping ». Dans : *ACM Trans. Comput. Theory* 6.3 (juillet 2014). issn : 1942-3454. doi : 10.1145/2633600. url : https://doi.org/10.1145/2633600.

[22] Zvika Brakerski et Vinod Vaikuntanathan. « Fully homomorphic encryption from ring-LWE and security for key dependent messages ». Dans : *Annual cryptology conference*. Springer. 2011, pages 505-524.

[23] Niklas Buescher, Spyros Boukoros, Stefan Bauregger et Stefan Katzenbeisser. « Two is not enough : Privacy assessment of aggregation schemes in smart metering ». Dans : *Proceedings on Privacy Enhancing Technologies* 2017.4 (2017), pages 198-214.

[24] Martin Burkhart, Mario Strasser, Dilip Many et Xenofontas Dimitropoulos. « SEPIA : Privacy-preserving aggregation of multi-domain network events and statistics ». Dans : 2010.

[25] CDE (connaissance des energies). *Électricité : en quoi consiste le mécanisme de capacité ?* https://www.connaissancedesenergies.org/electricite-en-quoi-consiste-le-mecanisme-de-capacite-140220. Décembre 2016.

[26] Hao Chen, Ran Gilad-Bachrach, Kyoohyung Han, Zhicong Huang, Amir Jalali, Kim Laine et Kristin Lauter. « Logistic regression over encrypted data from fully homomorphic encryption ». Dans : *BMC medical genomics* 11.4 (2018), page 81.

[27] S-T Chen, David C Yu et Alireza R Moghaddamjo. « Weather sensitive short-term load forecasting using nonfully connected artificial neural network ». Dans : *IEEE Transactions on Power Systems* 7.3 (1992), pages 1098-1105.

[28] Mo-yuen Chow et Hahn Tram. « Application of fuzzy logic technology for spatial load forecasting ». Dans : *Proceedings of 1996 Transmission and Distribution Conference and Exposition.* IEEE. 1996, pages 608-614.

[29] *Climate Ambition Summit 2020 – Co-convened by the United Nations, the United Kingdom and France In partnership with Chine and Italy.* https ://www.climateambitionsummit2020.org/index Décembre 2020.

[30] CNIL. *Invalidation du « Privacy shield » : la CNIL et ses homologues analysent actuellement ses conséquences.* https://www.cnil.fr/fr/invalidation-du-privacy-shield-la-cnil-et-ses-homologues-analysent-actuellement-ses-consequences. Juillet 2020.

[31] CNIL. *La formation restreinte de la CNIL prononce une sanction de 50 millions d'euros à l'encontre de la société GOOGLE LLC.* https://www.cnil.fr/fr/la-formation-restreinte-de-la-cnil-prononce-une-sanction-de-50-millions-deuros-lencontre-de-la. Janvier 2019.

[32] *Code de l'énergie.* https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000023983208/2012-04-06/. Avril 2012.

[33] Cour de justice de l'Union européenne COMMUNIQUE DE PRESSE n° 91/20. *La Cour invalide la décision 2016/1250 relative à l'adéquation de la protection assurée par le bouclier de protection des données UE-États-Unis.* https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091fr.pdf. Juillet 2020.

[34] Thomas M Cover. *Elements of information theory.* John Wiley & Sons, 1999.

[35] Ivan Damgård, Matthias Fitzi, Eike Kiltz, Jesper Buus Nielsen et Tomas Toft. « Unconditionally secure constant-rounds multi-party computation for equality, comparison, bits and exponentiation ». Dans : *Theory of Cryptography Conference.* 2006.

[36] Ivan Damgård, Marcel Keller, Enrique Larraia, Valerio Pastro, Peter Scholl et Nigel P. Smart. « Practical covertly secure MPC for dishonest majority–or : breaking the SPDZ limits ». Dans : *ESORICS*. 2013.

[37] Ivan Damgård, Valerio Pastro, Nigel P. Smart et Sarah Zakarias. « Multiparty computation from somewhat homomorphic encryption ». Dans : *CRYPTO*. 2012.

[38] George Danezis, Cédric Fournet, Markulf Kohlweiss et Santiago Zanella-Béguelin. « Smart meter aggregation via secret-sharing ». Dans : *Workshop on Smart energy grid security*. 2013.

[39] Tulio De Souza, Joss Wright, Piers O'Hanlon et Ian Brown. « Set difference attacks in wireless sensor networks ». Dans : *International Conference on Security and Privacy in Communication Systems*. 2012.

[40] *Décret n° 2017-676 du 28 avril 2017 relatif à l'autoconsommation d'électricité et modifiant les articles D. 314-15 et D. 314-23 à D. 314-25 du code de l'énergie*. `https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000034517272?r=Rb1zAISW09`. Avril 2017.

[41] *Décret No. 2001-630 du 16 juillet 2001 relatif à la confidentialité des informations détenues par les gestionnaires de réseaux publics de transport ou de distribution d'électricité, pris pour l'application des articles 16 et 20 de la loi No. 2000-108 du 10 février 2000 relative à la modernisation et au développement du service public de l'électricité*. `https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000000578863/`. Juillet 2001.

[42] Differential Privacy Team. « Learning with Privacy at Scale ». Dans : (2017).

[43] Tassos Dimitriou et Mohamad Khattar Awad. « Secure and scalable aggregation in the smart grid resilient against malicious entities ». Dans : *Ad Hoc Networks* 50 (2016), pages 58-67.

[44] Tassos Dimitriou et Ghassan O. Karame. « Enabling Anonymous Authorization and Rewarding in the Smart Grid ». Dans : *IEEE Transactions on Dependable and Secure Computing* 14.5 (2017), pages 565-572.

[45] Bolin Ding, Janardhan Kulkarni et Sergey Yekhanin. « Collecting telemetry data privately ». Dans : *Advances in Neural Information Processing Systems*. 2017, pages 3571-3580.

[46] Léo Ducas et Daniele Micciancio. « FHEW : bootstrapping homomorphic encryption in less than a second ». Dans : *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer. 2015, pages 617-640.

[47] Cynthia Dwork. « Differential privacy : A survey of results ». Dans : *International Conference on Theory and Applications of Models of Computation*. 2008.

[48] Cynthia Dwork, Frank McSherry, Kobbi Nissim et Adam Smith. « Calibrating noise to sensitivity in private data analysis ». Dans : *Theory of cryptography conference*. Springer. 2006, pages 265-284.

[49] Cynthia Dwork, Aaron Roth et coll. « The algorithmic foundations of differential privacy. » Dans : *Foundations and Trends in Theoretical Computer Science* 9.3-4 (2014), pages 211-407.

[50] EDF. *A Lyon, Ydeal Confluence ouvre la voie de l'autoconsommation collective à grande échelle*. https://www.edf.fr/collectivites/transition-energetique/references-et-realisations/ydeal-confluence-ouvre-la-voie-de-l-autoconsommation-collective-a-grande-echelle-a-lyon. 2020.

[51] EDF. *Autoconsommation collective : produisez et consommez votre électricité... à plusieurs !* https://www.edf.fr/autoconsommation-collective. 2020.

[52] Costas Efthymiou et Georgios Kalogridis. « Smart grid privacy via anonymization of smart metering data ». Dans : *International Conference on Smart Grid Communications*. 2010.

[53] Günther Eibl et Dominik Engel. « Differential privacy for real smart metering data ». Dans : *Computer Science-Research and Development* 32.1-2 (2017), pages 173-182.

[54] Taher ElGamal. « A public key cryptosystem and a signature scheme based on discrete logarithms ». Dans : *IEEE transactions on information theory* 31.4 (1985), pages 469-472.

[55] Enedis. *Autoconsommation collective*. https://www.enedis.fr/autoconsommation-collective.

[56] Enedis. *Autoconsommation collective : au cœur de la transition énergétique des territoires*. https://www.enedis.fr/actualites/autoconsommation-collective-au-coeur-de-la-transition-energetique-des-territoires. Décembre 2019.

[57] Enedis. *L'autoconsommation*. https://www.enedis.fr/lautoconsommation.

[58] Enedis. *La confidentialité des données gérées par Enedis*. https://www.enedis.fr/professionnel-confidentialite-des-donnees.

[59] Commission for Energy Regulation (CER). *CER Smart Metering Project - Electricity Customer Behaviour Trial, 2009-2010 [dataset]*. http://www.ucd.ie/issda/data/commissionforenergyregulationcer/. 2012.

[60] Úlfar Erlingsson, Vasyl Pihur et Aleksandra Korolova. « Rappor : Randomized aggregatable privacy-preserving ordinal response ». Dans : *Proceedings of the 2014 ACM SIGSAC conference on computer and communications security*. 2014, pages 1054-1067.

[61] Isabelle Falque-Pierrotin. *Délibération No. 2012-404 du 15 novembre 2012 portant recommandation relative aux traitements des données de consommation détaillées collectées par les compteurs communicants*. Janvier 2013.

[62] Sören Finster et Ingmar Baumgart. « Pseudonymous smart metering without a trusted third party ». Dans : *International Conference on Trust, Security and Privacy in Computing and Communications*. 2013.

[63] Fiona Harvey. *UN secretary general urges all countries to declare climate emergencies.* https://www.theguardian.com/environment/2020/dec/12/un-secretary-general-all-countries-declare-climate-emergencies-antonio-guterres-climate-ambition-summit. Décembre 2020.

[64] Philippe Forestier, Sawsan Al Zahr et Melaine Rousselle. « Coordination de la gestion de consommation d'énergie électrique ». Patent FR 3060819 (FR). Juin 2018.

[65] Flavio D. Garcia et Bart Jacobs. « Privacy-friendly energy-metering via homomorphic encryption ». Dans : *International Workshop on Security and Trust Management*. 2010.

[66] Simson L Garfinkel, John M Abowd et Sarah Powazek. « Issues encountered deploying differential privacy ». Dans : *Proceedings of the 2018 Workshop on Privacy in the Electronic Society*. 2018, pages 133-137.

[67] Rosario Gennaro, Michael O Rabin et Tal Rabin. « Simplified VSS and fast-track multiparty computations with applications to threshold cryptography ». Dans : *Symposium on principles of distributed computing*. 1998.

[68] Craig Gentry. *A fully homomorphic encryption scheme*. 2009.

[69] Craig Gentry et Shai Halevi. « Fully homomorphic encryption without squashing using depth-3 arithmetic circuits ». Dans : *2011 IEEE 52nd Annual Symposium on Foundations of Computer Science*. IEEE. 2011, pages 107-109.

[70] George W. Hart. *Nonintrusive Appliance Load Monitor Published References*. http://www.georgehart.com/research/nalmrefs.html.

[71] George W. Hart. « Nonintrusive appliance load data acquisition ». Dans : *Proceedings : International Load Management Conference*. 1985.

[72] George W. Hart. « Residential energy monitoring and computerized surveillance via utility power flows ». Dans : *IEEE Technology and Society Magazine* (1989).

[73] George William Hart. « Nonintrusive appliance load monitoring ». Dans : *Proceedings of the IEEE* 80.12 (1992), pages 1870-1891.

[74] Tareq Hossen, Arun Sukumaran Nair, Radhakrishnan Angamuthu Chinnathambi et Prakash Ranganathan. « Residential load forecasting using deep neural networks (DNN) ». Dans : *2018 North American Power Symposium (NAPS)*. IEEE. 2018, pages 1-5.

[75] Tareq Hossen, Siby Jose Plathottam, Radha Krishnan Angamuthu, Prakash Ranganathan et Hossein Salehfar. « Short-term load forecasting using deep neural networks (DNN) ». Dans : *2017 North American Power Symposium (NAPS)*. IEEE. 2017, pages 1-6.

[76] Samuel Humeau, Tri Kurniawan Wijaya, Matteo Vasirani et Karl Aberer. « Electricity load forecasting for residential customers : Exploiting aggregation and correlation between households ». Dans : *2013 Sustainable Internet and ICT for Sustainability (SustainIT)*. IEEE. 2013, pages 1-6.

[77] Marek Jawurek, Martin Johns et Konrad Rieck. « Smart metering de-pseudonymization ». Dans : *Annual Computer Security Applications Conference*. 2011.

[78] Journal officiel de l'Union européenne. *DÉCISION D'EXÉCUTION (UE) 2016/1250 DE LA COMMISSION*. https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32016D1250. Juillet 2016.

[79] Journal officiel de l'Union européenne. *DÉCISION DE LA COMMISSION du 5 février 2010 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des sous-traitants établis dans des pays tiers en vertu de la directive 95/46/CE du Parlement européen et du Conseil*. https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32010D0087. Février 2010.

[80] Journal officiel des Communautés européennes. *Directive 95/46/EC du Parlement européen et du Conseil du 24 octobre1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données*. https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:31995L0046&from=FR. Octobre 1995.

[81] Nesrine Kaâniche et Maryline Laurent. *Personnalisation de services : quelles technologies pour la préservation de la vie privée ?* Avril 2019. isbn : 978-2-9557308-7-4. url : https://cvpip.wp.imt.fr/2019/04/29/livre-electronique-avril-2019-personnalisation-de-services-quelles-technologies-pour-la-preservation-de-la-vie-privee/ (visité le 16/10/2019).

[82] Georgios Kalogridis, Costas Efthymiou, Stojan Z Denic, Tim A Lewis et Rafael Cepeda. « Privacy for smart meters : Towards undetectable appliance load signatures ». Dans : *2010 First IEEE International Conference on Smart Grid Communications*. IEEE. 2010, pages 232-237.

[83] Marcel Keller, Emmanuela Orsini et Peter Scholl. « MASCOT : faster malicious arithmetic secure computation with oblivious transfer ». Dans : *Computer and Communications Security*. 2016.

[84] Marcel Keller, Valerio Pastro et Dragos Rotaru. « Overdrive : making SPDZ great again ». Dans : *EUROCRYPT*. 2018.

[85] Daniel Kifer et Ashwin Machanavajjhala. « Pufferfish : A Framework for Mathematical Privacy Definitions ». Dans : *ACM Trans. Database Syst.* 39.1 (janvier 2014). issn : 0362-5915. doi : 10.1145/2514689. url : https://doi.org/10.1145/2514689.

[86] Samuel Kotz, Tomasz Kozubowski et Krzystof Podgorski. *The Laplace distribution and generalizations : a revisit with applications to communications, economics, engineering, and finance*. 2012.

[87] Klaus Kursawe, George Danezis et Markulf Kohlweiss. « Privacy-friendly aggregation for the smart-grid ». Dans : *Privacy Enhancing Technologies*. 2011.

[88] Jaewoo Lee et Chris Clifton. « How much is enough ? choosing ε for differential privacy ». Dans : *International Conference on Information Security*. Springer. 2011, pages 325-340.

[89] *Les réseaux électriques intelligents (smart grids) au cœur de la réponse des territoires au changement climatique*. https://reseaudurable.com/reseaux-intelligentssmart-grids-changement-climatique/. Octobre 2015.

[90] Franklin Leukam Lako. *Algorithme d'effacement à la pointe respectueux de la vie privée*. Séminaire R3S des doctorants, 2020.

[91] Franklin Leukam Lako. *Comment sécuriser et partager des données de consommation à l'échelle du quartier ?* Séminaire Privacy et espaces publics : l'enjeu territorial – EDF R&D, 2018.

[92] Franklin Leukam Lako. *Personal Data Protection in Energy Services*. Séminaire EDF R&D des doctorants, 2019.

[93] Franklin Leukam Lako. *Personal Data Protection in Energy Services*. Séminaire SAMOVAR des doctorants, 2018.

[94] Franklin Leukam Lako. *Protection des données à caractère personnel pour les services énergétiques*. Workshop SEIDO Lab, 2019.

[95] Franklin Leukam Lako. *Protection des données à caractère personnel pour les services énergétiques*. Workshop SEIDO Lab, 2020.

[96] Franklin Leukam Lako. *Reconciling Privacy and Utility for Energy Services – an Application to Demand Response Protocols*. 2020 International Workshop on Privacy Engineering – IWPE'20.

[97] Franklin Leukam Lako, Paul Lajoie-Mazenc et Maryline Laurent. « Personal Data Protection in Energy Services – Survey ». Dans : *Cryptacus*. 2018.

[98] Franklin Leukam Lako, Paul Lajoie-Mazenc et Maryline Laurent. « Privacy-preserving Publication of Time-series Data in Smart Grid ». Dans : *Security and Communication Networks* (2021).

[99] Franklin Leukam Lako, Paul Lajoie-Mazenc et Maryline Laurent. « Procédé de gestion de consommation dans un réseau de distribution ». FR3097087. 2019.

[100] Franklin Leukam Lako, Paul Lajoie-Mazenc et Maryline Laurent. « Reconciling Privacy and Utility for Energy Services–an Application to Demand Response Protocols ». Dans : *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE. 2020, pages 348-355.

[101] Na Li, Lijun Chen et Steven H Low. « Optimal demand response based on utility maximization in power networks ». Dans : *2011 IEEE power and energy society general meeting*. IEEE. 2011, pages 1-8.

[102] *Loi No. 2000-108 du 10 février 2000 relative à la modernisation et au développement du service public de l'électricité.* https://www.legifrance.gouv.fr/loda/id/LEGITEXT000005629085/2010-06-04/. Février 2000.

[103] *Loi No. 2006-1537 du 7 décembre 2006 relative au secteur de l'énergie (1).* https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000000462914/. Décembre 2006.

[104] *Loi No. 2015-992 du 17 août 2015 relative à la transition énergétique pour la croissance verte (1).* https://www.legifrance.gouv.fr/eli/loi/2015/8/17/DEVX1413992L/jo/texte. Août 2015.

[105] *Loi No. 2017-227 du 24 février 2017 ratifiant les ordonnances n° 2016-1019 du 27 juillet 2016 relative à l'autoconsommation d'électricité et n° 2016-1059 du 3 août 2016 relative à la production d'électricité à partir d'énergies renouvelables et visant à adapter certaines dispositions relatives aux réseaux d'électricité et de gaz et aux énergies renouvelables (1).* https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000034080223/. Février 2017.

[106] Lingjuan Lyu, Yee Wei Law, Jiong Jin et Marimuthu Palaniswami. « Privacy-preserving aggregation of smart metering via transformation and encryption ». Dans : *2017 IEEE Trustcom/BigDataSE/ICESS*. IEEE. 2017, pages 472-479.

[107] Stephen McLaughlin, Patrick McDaniel et William Aiello. « Protecting consumer privacy from electric load monitoring ». Dans : *Proceedings of the 18th ACM conference on Computer and communications security*. 2011, pages 87-98.

[108] Frank McSherry et Ilya Mironov. « Differentially private recommender systems : Building privacy into the netflix prize contenders ». Dans : *Proceedings of the 15th ACM SIGKDD international conference on Knowledge discovery and data mining*. 2009, pages 627-636.

[109] mega. *Comprendre le marché énergétique en Belgique ? Notre expert vous éclaire !* https://blog.mega.be/comprendre-le-marche-energetique-en-belgique-notre-expert-vous-eclaire/. Octobre 2018.

[110] Ministère de la Transition écologique. *Les énergies renouvelables en France : les chiffres clés 2018.* https://www.ecologie.gouv.fr/energies-renouvelables-en-france-chiffres-cles-2018. Mai 2018.

[111] Ministère de la transition écologique. *Énergie dans les bâtiments.* https://www.ecologie.gouv.fr/energie-dans-batiments. Juin 2017.

[112] Ministère de la transition écologique. *Loi de transition énergétique pour la croissance verte.* https://www.ecologie.gouv.fr/loi-transition-energetique-croissance-verte. Mai 2017.

[113] Ministère de la transition écologique. *Vers un système électrique plus flexible.* https://www.ecologie.gouv.fr/vers-systeme-electrique-plus-flexible.

[114] Ilya Mironov, Omkant Pandey, Omer Reingold et Salil Vadhan. « Computational differential privacy ». Dans : *Annual International Cryptology Conference*. 2009, pages 126-142.

[115] M. Misiti, Y. Misiti, G. Oppenheim et Jean-Michel Poggi. « Décomposition par ondelettes et méthodes comparatives : étude d'une courbe de charge électrique ». fr. Dans : *Revue de Statistique Appliquée* 42.2 (1994), pages 57-77. url : http://www.numdam.org/item/RSA_1994__42_2_57_0.

[116] Salman Mohagheghi, James Stoupis, Zhenyuan Wang, Zhao Li et Hormoz Kazemzadeh. « Demand response architecture : Integration into the distribution management system ». Dans : *2010 First IEEE International Conference on Smart Grid Communications*. IEEE. 2010, pages 501-506.

[117] Andrés Molina-Markham, Prashant Shenoy, Kevin Fu, Emmanuel Cecchet et David Irwin. « Private memoirs of a smart meter ». Dans : *Proceedings of the 2nd ACM workshop on embedded sensing systems for energy-efficiency in building*. 2010, pages 61-66.

[118] Naoya Motegi, Mary Ann Piette, David S Watson, Sila Kiliccote et Peng Xu. *Introduction to Commercial Building Control Strategies and Techniques for Demand Response–Appendices*. Rapport technique. Lawrence Berkeley National Lab.(LBNL), Berkeley, CA (United States), 2007.

[119] Mustafa A Mustafa, Sara Cleemput, Abdelrahaman Aly et Aysajan Abidin. « A Secure and Privacy-preserving Protocol for Smart Metering Operational Data Collection ». Dans : *IEEE Transactions on Smart Grid* (2019).

[120] Arvind Narayanan et Vitaly Shmatikov. « Robust de-anonymization of large sparse datasets ». Dans : *Security and Privacy, 2008. SP 2008. IEEE Symposium on*. 2008, pages 111-125.

[121] Matteo Nardello, Maurizio Rossi et Davide Brunelli. « A low-cost smart sensor for non intrusive load monitoring applications ». Dans : *2017 IEEE 26th International Symposium on Industrial Electronics (ISIE)*. IEEE. 2017, pages 1362-1368.

[122] Takashi Nishide et Kazuo Ohta. « Multiparty computation for interval, equality, and comparison without bit-decomposition protocol ». Dans : *International Workshop on Public Key Cryptography*. 2007.

[123] Jeremy C. Owens. *Equifax earnings hit by data breach stock declines*. 9 novembre 2017. url : https://www.marketwatch.com/story/equifax-earnings-hit-by-data-breach-stock-declines-2017-11-09 (visité le 15/10/2019).

[124] Pascal Paillier. « Public-key cryptosystems based on composite degree residuosity classes ». Dans : *EUROCRYPT*. 1999.

[125] Yue Pang, Bo Yao, Xiangdong Zhou, Yong Zhang, Yiming Xu et Zijing Tan. « Hierarchical Electricity Time Series Forecasting for Integrating Consumption Patterns Analysis and Aggregation Consistency. » Dans : *IJCAI*. 2018, pages 3506-3512.

[126] *Panorama des émissions françaises de gaz à effet de serre.* https://ree.developpement-durable.gouv.fr/themes/defis-environnementaux/changement-climatique/emissions-de-gaz-a-effet-de-serre/article/panorama-des-emissions-francaises-de-gaz-a-effet-de-serre. 2018.

[127] Balázs Pejó et Damien Desfontaines. « SoK : Differential Privacies ». Dans : (2020).

[128] Robi Polikar. *The wavelet tutorial.* https://cseweb.ucsd.edu/~baden/Doc/wavelets/polikar_wavelets.pdf. 1996.

[129] Alberto Prudenzi. « A neuron nets based procedure for identifying domestic appliances pattern-of-use from energy recordings at meter panel ». Dans : *Power Engineering Society Winter Meeting.* Tome 2. 2002.

[130] Vibhor Rastogi et Suman Nath. « Differentially private aggregation of distributed time-series with transformation and encryption ». Dans : *Proceedings of the 2010 ACM SIGMOD International Conference on Management of data.* 2010, pages 735-746.

[131] « Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) ». Dans : *Official Journal of the European Union* (2016).

[132] Ronald L Rivest, Adi Shamir et Leonard Adleman. « A method for obtaining digital signatures and public-key cryptosystems ». Dans : *Communications of the ACM* 21.2 (1978), pages 120-126.

[133] Cristina Rottondi, Antimo Barbato, Lin Chen et Giacomo Verticale. « Enabling Privacy in a Distributed Game-Theoretical Scheduling System for Domestic Appliances. » Dans : *IEEE Transactions on Smart Grid* 8.3 (2016), pages 1220-1230.

[134] Cristina Rottondi, Giulia Mauri et Giacomo Verticale. « A data pseudonymization protocol for smart grids ». Dans : *Online Conference on Green Communications.* 2012.

[135] Cristina Rottondi, Giulia Mauri et Giacomo Verticale. « A protocol for metering data pseudonymization in smart grids ». Dans : *Transactions on Emerging Telecommunications Technologies* 26.5 (2015), pages 876-892.

[136] Cristina Rottondi et Giacomo Verticale. « Privacy-friendly appliance load scheduling in smart grids ». Dans : *International Conference on Smart Grid Communications (SmartGridComm).* 2013.

[137] Melaine Rousselle, Philippe Forestier et Sawsan Al Zahr. « Method for managing a group of electrical energy consuming devices, and electrical energy management module ». Patent US20180375328A1. 6 décembre 2016.

[138] Adi Shamir. « How to share a secret ». Dans : *Communications of the ACM* 22.11 (1979), pages 612-613.

[139] H Shayeghi, HA Shayanfar et G Azimi. « Intelligent neural network based STLF ». Dans : *International Journal of Computer Systems Science and Engineering* 4.1 (2009).

[140] Pierluigi Siano. « Demand response and smart grids—A survey ». Dans : *Renewable and sustainable energy reviews* 30 (2014), pages 461-478.

[141] Shuang Song, Yizhen Wang et Kamalika Chaudhuri. « Pufferfish Privacy Mechanisms for Correlated Data ». Dans : *Proceedings of the 2017 ACM International Conference on Management of Data*. SIGMOD '17. Chicago, Illinois, USA : Association for Computing Machinery, 2017, pages 1291-1306. isbn : 9781450341974. doi : 10.1145/3035918.3064025. url : https://doi.org/10.1145/3035918.3064025.

[142] Cory Thoma, Tao Cui et Franz Franchetti. « Secure multiparty computation based privacy preserving smart metering system ». Dans : *2012 North American power symposium (NAPS)*. IEEE. 2012, pages 1-6.

[143] Valentin Tudor, Magnus Almgren et Marina Papatriantafilou. « A study on data de-pseudonymization in the smart grid ». Dans : *European Workshop on System Security*. 2015.

[144] David Varodayan et Ashish Khisti. « Smart meter privacy using a rechargeable battery : Minimizing the rate of information leakage ». Dans : *2011 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. IEEE. 2011, pages 1932-1935.

[145] Qian Wang, Yan Zhang, Xiao Lu, Zhibo Wang, Zhan Qin et Kui Ren. « Real-time and spatio-temporal crowd-sourced social network data publishing with differential privacy ». Dans : *IEEE Transactions on Dependable and Secure Computing* 15.4 (2016), pages 591-606.

[146] Ruye Wang. « Continuous- and discrete-time wavelet transforms ». Dans : *Introduction to Orthogonal Transforms : With Applications in Data Processing and Analysis*. Cambridge University Press, 2012, pages 461-491. doi : 10.1017/CBO9781139015158.012.

[147] Tianhao Wang, Jeremiah Blocki, Ninghui Li et Somesh Jha. « Locally differentially private protocols for frequency estimation ». Dans : *26th {USENIX} Security Symposium ({USENIX} Security 17)*. 2017, pages 729-745.

[148] Xingxing Xiong, Shubo Liu, Dan Li, Zhaohui Cai et Xiaoguang Niu. « Real-time and private spatio-temporal data aggregation with local differential privacy ». Dans : *Journal of Information Security and Applications* 55 (2020), page 102633.

[149] Bin Yang, Issei Sato et Hiroshi Nakagawa. « Bayesian Differential Privacy on Correlated Data ». Dans : *Proceedings of the 2015 ACM SIGMOD International Conference on Management of Data*. SIGMOD '15. Melbourne, Victoria, Australia : Association for Computing Machinery, 2015, pages 747-762. isbn : 9781450327589. doi : 10.1145/2723372.2747643. url : https://doi.org/10.1145/2723372.2747643.

[150] ZKProof. *ZKProof Community Reference. Version 0.2*. Décembre 2019. Updated versions at https ://zkproof.org.

Titre : Protection des données à caractère personnel pour les services énergétiques

Mots clés : Vie privée, réseaux électriques intelligents, services énergétiques, calcul multipartite sécurisé, confidentialité différentielle, techniques de protection de la vie privée

Résumé : Les réseaux électriques intelligents sont des briques importantes dans la lutte contre le changement climatique. Ces réseaux intelligents permettent l'introduction massive des énergies renouvelables, qui sont intermittentes, tout en garantissant la stabilité du réseau, c'est-à-dire d'assurer en temps réel l'équilibre entre la demande et la production d'énergie en aval du réseau. Cette gestion de la stabilité du réseau est possible grâce aux compteurs communicants installés dans des foyers permettant au gestionnaire de réseau de distribution de collecter les données de consommation et de production des consommateurs et des producteurs à un pas de temps allant jusqu'à 10 min en France. Ces données de consommations en temps réel permettent de fournir de nouveaux services énergétiques, comme la prévision de consommation des clients, ou encore la demande d'effacement à la pointe. Les services d'effacement permettent d'éviter les pics de consommation dans un quartier en s'assurant qu'à chaque instant, la consommation des utilisateurs ne dépasse pas la puissance maximale fournie au niveau du quartier.

Cependant, la collecte des données de consommation pose des problèmes de vie privée. En effet, les données de consommation d'un foyer permettent de révéler le comportement des habitants de ce foyer : présences, absences, heures de lever, heures de coucher, religion, etc.

Cette thèse vise à proposer de nouveaux services énergétiques, tout en protégeant la vie privée des consommateurs. Nous proposons cinq contributions qui se rapportent à deux thèmes : 1. La transformation d'un algorithme de demande d'effacement à la pointe en le rendant respectueux de la vie privée. Cette transformation utilise du calcul multipartite sécurisé, permettant de réaliser des calculs sur des données individuelles sans jamais les révéler. 2. La publication de sommes de consommation des foyers en préservant la vie privée et une bonne utilité. Cette publication utilise la confidentialité différentielle, garantissant que la publication ne permet pas de révéler indirectement les consommations individuelles des foyers. Ces sommes de consommation permettent notamment de réaliser des prévisions de consommation.

Title : Personal Data Protection in Energy Services

Keywords : Privacy, smart grids, energy services, secure multiparty computation, differential privacy, privacy enhancing technologies

Abstract : Smart grids are important bricks in the fight against climate change. Smart grids allow the massive introduction of renewable energies, which are intermittent, while guaranteeing grid stability, i.e., ensuring a real-time balance between demand and production in the power grid. The management of grid stability is possible thanks to smart meters installed in households, allowing the distribution system operator to collect consumption/production data from consumers/producers at a time step of up to 10 min in France. This real-time consumption data enables to provide new energy services, such as customer consumption forecasts or demand response. Demand response services help to avoid consumption peaks in a neighborhood by ensuring that, at all times, users' consumption does not exceed the maximum power of the local grid.

However, the collection of users' consumptions is a key privacy concern. Indeed, individual consumption data reflect the use of all electric appliances by inhabitants in a household over time, and enable to deduce the behaviors, activities, age or preferences of the inhabitants.

This thesis aims to propose new energy services, while protecting the privacy of consumers. We propose five contributions that relate to two themes: 1. The transformation of a demand response algorithm by making it privacy friendly. This transformation uses secure multiparty computation, allowing to compute an aggregate, such as a sum of users' consumption, without disclosing any individual consumption. 2. The publication of sum of users' consumption while preserving privacy and good utility. This publication uses differential privacy, ensuring that the publication of the sum does not indirectly reveal individual users' consumption. Among other energy services, these sums of consumption enable to perform consumption forecasts.

Institut Polytechnique de Paris
91120 Palaiseau, France