Sur quelques questions de cryptographie : Anonymat révocable et Une généralisation du schéma de Goldwasser-Micali

Davide Alessio

Technicolor & Université de Rennes 1

Rennes, 13 décembre 2011

Plan de l'exposé

Introduction
- Définitions

Anonymat révocable
- Présentation du problème
- Contribution 1 : transformation générique
- Contribution 2 : schéma à double trappe

Une généralisation du schéma de Goldwasser-Micali
- Définitions
- Chiffrement de Goldwasser-Micali
- Contribution

Conclusion

Plan de l'exposé

Introduction
- Définitions

Anonymat révocable
- Présentation du problème
- Contribution 1 : transformation générique
- Contribution 2 : schéma à double trappe

Une généralisation du schéma de Goldwasser-Micali
- Définitions
- Chiffrement de Goldwasser-Micali
- Contribution

Conclusion

Plan de l'exposé

Introduction
- Définitions

Anonymat révocable
- Présentation du problème
- Contribution 1 : transformation générique
- Contribution 2 : schéma à double trappe

Une généralisation du schéma de Goldwasser-Micali
- Définitions
- Chiffrement de Goldwasser-Micali
- Contribution

Conclusion

Plan de l'exposé

Introduction
- Définitions

Anonymat révocable
- Présentation du problème
- Contribution 1 : transformation générique
- Contribution 2 : schéma à double trappe

Une généralisation du schéma de Goldwasser-Micali
- Définitions
- Chiffrement de Goldwasser-Micali
- Contribution

Conclusion

Plan de l'exposé

Introduction
- Définitions

Anonymat révocable
- Présentation du problème
- Contribution 1 : transformation générique
- Contribution 2 : schéma à double trappe

Une généralisation du schéma de Goldwasser-Micali
- Définitions
- Chiffrement de Goldwasser-Micali
- Contribution

Conclusion

Chiffrement à clé publique

Définition

Setup : Paramètres publics : $I \xleftarrow{R} \text{Setup}(\kappa)$

Génération des clés : Exécuté une fois par utilisateur.
$(\text{pk}, \text{sk}) \xleftarrow{R} \text{KeyGen}(I)$

Chiffrement : $c \leftarrow \text{Encrypt}(m, \text{pk})$

Déchiffrement : $m \leftarrow \text{Decrypt}(c, \text{sk})$

Propriétés

Complétude : le message peut être déchiffré

Sécurité : seul qui possède la bonne clé peut déchiffrer

Définition d'adversaire

Adversaire défini par le couple (but, moyens)

Définition d'adversaire

Adversaire défini par le couple (but, moyens)

but :
- la clé secrète
- le message en clair
- la sécurité sémantique
- la non-malléabilité

moyens :
- oracle de chiffrement (adaptatif)
- oracle de déchiffrement (adaptatif)

Définition d'adversaire

Adversaire défini par le couple (but, moyens)

but :
- la clé secrète
- le message en clair
- la sécurité sémantique
- la non-malléabilité

moyens :
- oracle de chiffrement (adaptatif)
- oracle de déchiffrement (adaptatif)

Définition d'adversaire

Adversaire défini par le couple (but, moyens)

but :
- la clé secrète
- le message en clair
- la sécurité sémantique
- la non-malléabilité

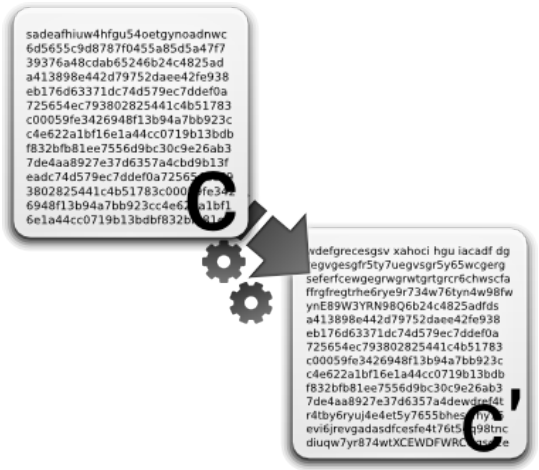
moyens :
- oracle de chiffrement (adaptatif)
- oracle de déchiffrement (adaptatif)

Définition d'adversaire

Adversaire défini par le couple (but, moyens)

but :
- la clé secrète
- le message en clair
- la sécurité sémantique
- la non-malléabilité

moyens :
- oracle de chiffrement (adaptatif)
- oracle de déchiffrement (adaptatif)



Définition d'adversaire

Adversaire défini par le couple (but, moyens)

but :
- la clé secrète
- le message en clair
- la sécurité sémantique
- la non-malléabilité

moyens :
- oracle de chiffrement (adaptatif)
- oracle de déchiffrement (adaptatif)

Définition d'adversaire

Adversaire défini par le couple (but, moyens)

but :
- la clé secrète
- le message en clair
- la sécurité sémantique
- la non-malléabilité

moyens :
- oracle de chiffrement (adaptatif)
- oracle de déchiffrement (adaptatif)

Définition d'adversaire

Adversaire défini par le couple (but, moyens)

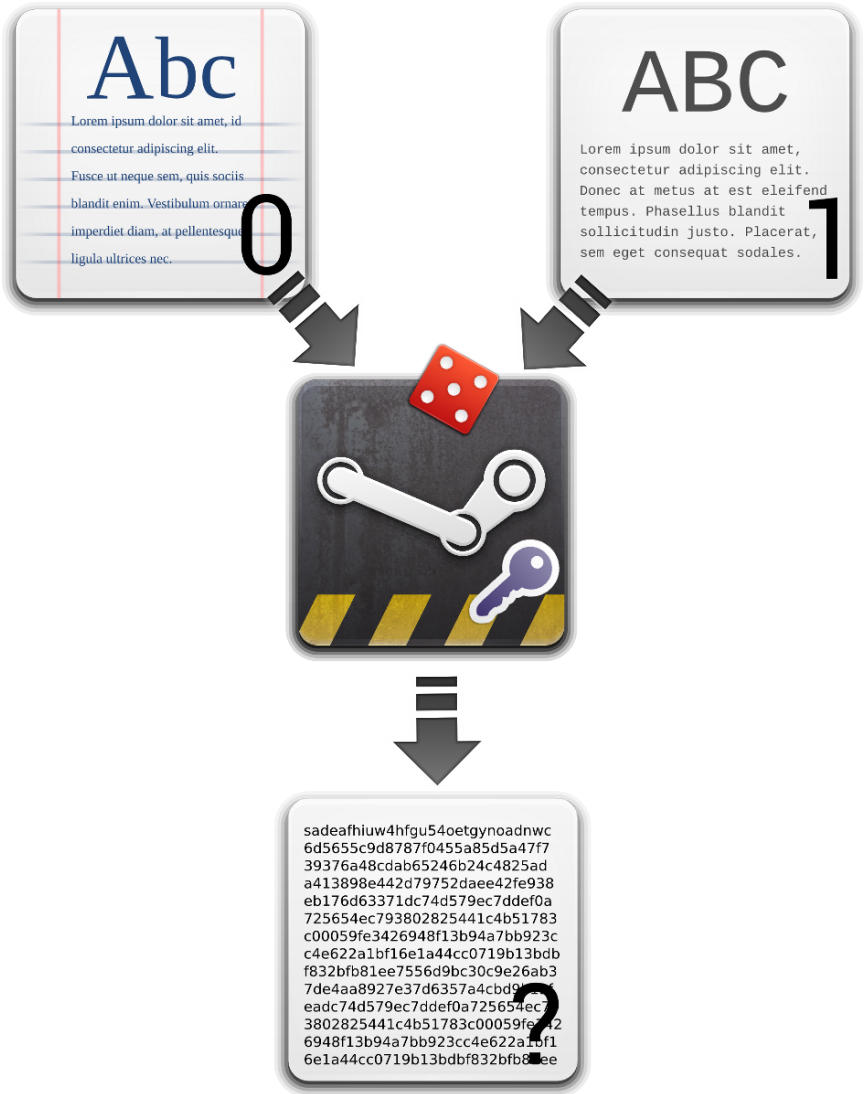
la clé secrète

Scénario usuel

Sécurité sémantique et oracle de chiffrement (IND-CPA)

m

Sécurité sémantique (ou *indistinguabilité*)



Sécurité sémantique (ou *indistinguabilité*)

Définition

Un chiffrement à clé publique est *indistinguable* (ou *sémantiquement sûr*) si

$$\left| \Pr \left[\begin{array}{l} I \xleftarrow{R} \mathsf{Setup}(\kappa), (\mathsf{pk}, \mathsf{sk}) \xleftarrow{R} \mathsf{KeyGen}(I), \\ (m_0, m_1, s) \leftarrow \mathcal{A}_1(\mathsf{pk}), b \xleftarrow{R} \{0,1\}, c \leftarrow \mathsf{Encrypt}(m_b, \mathsf{pk}) \end{array} : \mathcal{A}_2(s, c) = b \right] - \frac{1}{2} \right|$$

est négligeable

Anonymat et *key-privacy*

Anonymat et *key-privacy*

Définition

Un chiffrement à clé publique est *anonyme* (ou *key-private*) si

$$\left| \Pr \left[\begin{array}{l} I \xleftarrow{R} \mathsf{Setup}(\kappa), \{(\mathsf{pk}_0, \mathsf{sk}_0), (\mathsf{pk}_1, \mathsf{sk}_1)\} \xleftarrow{R} \mathsf{KeyGen}(I), \\ (m, s) \leftarrow \mathcal{A}_1(\mathsf{pk}_0, \mathsf{pk}_1), b \xleftarrow{R} \{0,1\}, c \leftarrow \mathsf{Encrypt}(m, \mathsf{pk}_b) \end{array} : \mathcal{A}_2(s, c) = b \right] - \frac{1}{2} \right|$$

est négligeable

Plan de l'exposé

Introduction
- Définitions

Anonymat révocable
- Présentation du problème
- Contribution 1 : transformation générique
- Contribution 2 : schéma à double trappe

Une généralisation du schéma de Goldwasser-Micali
- Définitions
- Chiffrement de Goldwasser-Micali
- Contribution

Conclusion

Anonymat révocable

- Contexte :
  - commerce électronique,
  - fournisseurs de contenu numérique,
  - communication hiérarchique
  - ...
- But
  - garder l'anonymat du destinataire
  - permettre à l'envoyeur de connaître l'identité de son interlocuteur

Solution

Un compromis entre les besoins du vendeur et les souhaits de l'acheteur

Anonymat révocable

- Contexte :
  - commerce électronique,
  - fournisseurs de contenu numérique,
  - communication hiérarchique
  - ...
- But
  - garder l'anonymat du destinataire
  - permettre à l'envoyeur de connaître l'identité de son interlocuteur

Solution

Un compromis entre les besoins du vendeur et les souhaits de l'acheteur

Contribution 1 : transformation générique

Anonymat révocable : de quoi s'agit il ?

Un schéma à clé publique anonyme enrichi de la propriété que l'anonymat peut être révoqué par un autorité de confiance

Contexte :

- Environnement homogène
- Envoyeur honnête

Contribution 1 : transformation générique

Anonymat révocable : de quoi s'agit il ?

Un schéma à clé publique anonyme enrichi de la propriété que l'anonymat peut être révoqué par un autorité de confiance

Contexte :

- Environnement homogène
- Envoyeur honnête

Notre formalisation

Définition

Un *schéma de chiffrement à clé publique avec l'anonymat révocable* est la donnée de 5 algorithmes :
(Setup, KeyGen, Encrypt, Decrypt, Trace)

Setup prenant κ en entrée, donne comme sortie

- $I \xleftarrow{R} \text{Setup}(\kappa)$
- (tsk, tpk) : clés de l'autorité de Traçage

Génération des clés $(\text{upk}, \text{usk}) \xleftarrow{R} \text{KeyGen}(I)$

Chiffrement $c \leftarrow \text{Encrypt}(\text{upk}, m)$

Déchiffrement $m \leftarrow \text{Decrypt}(\text{usk}, c)$

Traçage $\text{upk} \leftarrow \text{Trace}(\text{tsk}, c)$.

Notre formalisation

Définition

Un *schéma de chiffrement à clé publique avec l'anonymat révocable* est la donnée de 5 algorithmes :
(Setup, KeyGen, Encrypt, Decrypt, Trace)

Setup prenant κ en entrée, donne comme sortie
- $I \xleftarrow{R} \text{Setup}(\kappa)$
- (tsk, tpk) : clés de l'autorité de Traçage

Génération des clés $(\text{upk}, \text{usk}) \xleftarrow{R} \text{KeyGen}(I)$

Chiffrement $c \leftarrow \text{Encrypt}(\text{upk}, m)$

Déchiffrement $m \leftarrow \text{Decrypt}(\text{usk}, c)$

Traçage $\text{upk} \leftarrow \text{Trace}(\text{tsk}, c)$.

Anonymat révocable : une approche

Solution simple

Concaténer au message chiffré c_1 l'identité chiffrée du destinataire c_2.

$$c = (\underbrace{\text{Encrypt}(m, \text{upk})}_{c_1}, \underbrace{\text{Encrypt}(\text{upk}, \text{tpk})}_{c_2})$$

Solution non optimale : **Malléable**

c_2 peut être corrompu $\rightarrow$ perte de traçabilité

Anonymat révocable : une approche

Solution simple

Concaténer au message chiffré c_1 l'identité chiffrée du destinataire c_2.

$$c = (\underbrace{\text{Encrypt}(m, \text{upk})}_{c_1}, \underbrace{\text{Encrypt}(\text{upk}, \text{tpk})}_{c_2})$$

Solution non optimale : **Malléable**

c_2 peut être corrompu $\rightarrow$ perte de traçabilité

Anonymat révocable : une approche

Solution simple

Concaténer au message chiffré c_1 l'identité chiffrée du destinataire c_2.

$$c = (\underbrace{\text{Encrypt}(m, \text{upk})}_{c_1}, \underbrace{\text{Encrypt}(\text{upk}, \text{tpk})}_{c_2})$$

Notre solution : « lier » c_1 et c_2

Notre transformation : description

ENTRÉE $\mathcal{S}_{Msg}$, schéma de chiffrement à clé publique anonyme

$+$ Autorité de Traçage, $\mathcal{S}_{Id}$

SORTIE $\mathcal{S}'$, schéma de chiffrement à clé publique avec anonymat révocable

Transformation : Description

ENTRÉE $\mathcal{S}_{\mathsf{Msg}} = (\,\mathsf{Setup}, \mathsf{KeyGen}, \mathsf{MsgEnc}, \mathsf{MsgDec})$

Setup $I \xleftarrow{R} \mathsf{RevSetup}(\kappa) = \mathsf{Setup}(\kappa)$
$\mathcal{E}$ et $\mathcal{KDF}$ sont choisis pendant cette phase

Génération de clés $(\mathsf{upk}, \mathsf{usk}) \xleftarrow{R} \mathsf{RevKeyGen}(I) = \mathsf{KeyGen}(I)$.
La clé publique upk est enregistrée

Chiffrement $c \leftarrow \mathsf{RevEnc}_{\mathsf{tpk}}(\mathsf{upk}, m) =$
$= (\mathsf{IDEnc}_{\mathsf{tpk}}(\mathsf{upk}), \mathsf{MsgEnc}_{\mathsf{upk}}(\mathcal{E}_k(m))$
où $k = \mathcal{KDF}(\mathsf{IDEnc}_{\mathsf{tpk}}(\mathsf{upk}))$

Déchiffrement
1. $k' = \mathcal{KDF}(c_1)$
2. $m \leftarrow \mathcal{E}_{k'}^{-1}(\mathsf{MsgDec}_{\mathsf{usk}}(c_2))$

Traçage $\mathsf{upk} \leftarrow \mathsf{Trace}_{\mathsf{tsk}}(c_1) = \mathsf{IDDec}_{\mathsf{tsk}}(c_1)$

SORTIE $\mathcal{S}' = (\,\mathsf{RevSetup}, \mathsf{RevKeyGen}, \mathsf{RevEnc}, \mathsf{RevDec}, \mathsf{Trace})$

Transformation : Description

ENTRÉE $\mathcal{S}_{\text{Msg}} = (\text{Setup}, \text{KeyGen}, \text{MsgEnc}, \text{MsgDec})$

Setup $I \xleftarrow{R} \text{RevSetup}(\kappa) = \text{Setup}(\kappa)$
$\mathcal{E}$ et $\mathcal{KDF}$ sont choisis pendant cette phase

Génération de clés $(\text{upk}, \text{usk}) \xleftarrow{R} \text{RevKeyGen}(I) = \text{KeyGen}(I)$.
La clé publique upk est enregistrée

Chiffrement $c \leftarrow \text{RevEnc}_{\text{tpk}}(\text{upk}, m) =$
$= (\text{IDEnc}_{\text{tpk}}(\text{upk}), \text{MsgEnc}_{\text{upk}}(\mathcal{E}_k(m))$
où $k = \mathcal{KDF}(\text{IDEnc}_{\text{tpk}}(\text{upk}))$

Déchiffrement
1. $k' = \mathcal{KDF}(c_1)$
2. $m \leftarrow \mathcal{E}_{k'}^{-1}(\text{MsgDec}_{\text{usk}}(c_2))$

Traçage $\text{upk} \leftarrow \text{Trace}_{\text{tsk}}(c_1) = \text{IDDec}_{\text{tsk}}(c_1)$

SORTIE $\mathcal{S}' = (\text{RevSetup}, \text{RevKeyGen}, \text{RevEnc}, \text{RevDec}, \text{Trace})$

Transformation : Description

ENTRÉE $\mathcal{S}_{\mathsf{Msg}} = (\,\mathsf{Setup}, \mathsf{KeyGen}, \mathsf{MsgEnc}, \mathsf{MsgDec})$

Setup $I \xleftarrow{R} \mathsf{RevSetup}(\kappa) = \mathsf{Setup}(\kappa)$
$\mathcal{E}$ et $\mathcal{KDF}$ sont choisis pendant cette phase

Génération de clés $(\mathsf{upk}, \mathsf{usk}) \xleftarrow{R} \mathsf{RevKeyGen}(I) = \mathsf{KeyGen}(I)$.
La clé publique upk est enregistrée

Chiffrement $c \leftarrow \mathsf{RevEnc}_{\mathsf{tpk}}(\mathsf{upk}, m) =$
$= (\mathsf{IDEnc}_{\mathsf{tpk}}(\mathsf{upk}), \mathsf{MsgEnc}_{\mathsf{upk}}(\mathcal{E}_k(m))$
où $k = \mathcal{KDF}(\mathsf{IDEnc}_{\mathsf{tpk}}(\mathsf{upk}))$

Déchiffrement
1. $k' = \mathcal{KDF}(c_1)$
2. $m \leftarrow \mathcal{E}_{k'}^{-1}(\mathsf{MsgDec}_{\mathsf{usk}}(c_2))$

Traçage $\mathsf{upk} \leftarrow \mathsf{Trace}_{\mathsf{tsk}}(c_1) = \mathsf{IDDec}_{\mathsf{tsk}}(c_1)$

SORTIE $\mathcal{S}' = (\,\mathsf{RevSetup}, \mathsf{RevKeyGen}, \mathsf{RevEnc}, \mathsf{RevDec}, \mathsf{Trace})$

Transformation : Description

ENTRÉE $\mathcal{S}_{\mathsf{Msg}} = (\mathsf{Setup}, \mathsf{KeyGen}, \mathsf{MsgEnc}, \mathsf{MsgDec})$

Setup $I \xleftarrow{R} \mathsf{RevSetup}(\kappa) = \mathsf{Setup}(\kappa)$
$\mathcal{E}$ et $\mathcal{KDF}$ sont choisis pendant cette phase

Génération de clés $(\mathsf{upk}, \mathsf{usk}) \xleftarrow{R} \mathsf{RevKeyGen}(I) = \mathsf{KeyGen}(I)$.
La clé publique upk est enregistrée

Chiffrement $c \leftarrow \mathsf{RevEnc}_{\mathsf{tpk}}(\mathsf{upk}, m) =$
$= (\mathsf{IDEnc}_{\mathsf{tpk}}(\mathsf{upk}), \mathsf{MsgEnc}_{\mathsf{upk}}(\mathcal{E}_k(m))$
où $k = \mathcal{KDF}(\mathsf{IDEnc}_{\mathsf{tpk}}(\mathsf{upk}))$

Déchiffrement
1. $k' = \mathcal{KDF}(c_1)$
2. $m \leftarrow \mathcal{E}_{k'}^{-1}(\mathsf{MsgDec}_{\mathsf{usk}}(c_2))$

Traçage $\mathsf{upk} \leftarrow \mathsf{Trace}_{\mathsf{tsk}}(c_1) = \mathsf{IDDec}_{\mathsf{tsk}}(c_1)$

SORTIE $\mathcal{S}' = (\mathsf{RevSetup}, \mathsf{RevKeyGen}, \mathsf{RevEnc}, \mathsf{RevDec}, \mathsf{Trace})$

Transformation : Description

ENTRÉE $\mathcal{S}_{\mathsf{Msg}} = (\mathsf{Setup}, \mathsf{KeyGen}, \mathsf{MsgEnc}, \mathsf{MsgDec})$

Setup $I \xleftarrow{R} \mathsf{RevSetup}(\kappa) = \mathsf{Setup}(\kappa)$
$\mathcal{E}$ et $\mathcal{KDF}$ sont choisis pendant cette phase

Génération de clés $(\mathsf{upk}, \mathsf{usk}) \xleftarrow{R} \mathsf{RevKeyGen}(I) = \mathsf{KeyGen}(I)$.
La clé publique upk est enregistrée

Chiffrement $c \leftarrow \mathsf{RevEnc}_{\mathsf{tpk}}(\mathsf{upk}, m) =$
$= (\mathsf{IDEnc}_{\mathsf{tpk}}(\mathsf{upk}), \mathsf{MsgEnc}_{\mathsf{upk}}(\mathcal{E}_k(m))$
où $k = \mathcal{KDF}(\mathsf{IDEnc}_{\mathsf{tpk}}(\mathsf{upk}))$

Déchiffrement
1. $k' = \mathcal{KDF}(c_1)$
2. $m \leftarrow \mathcal{E}_{k'}^{-1}(\mathsf{MsgDec}_{\mathsf{usk}}(c_2))$

Traçage $\mathsf{upk} \leftarrow \mathsf{Trace}_{\mathsf{tsk}}(c_1) = \mathsf{IDDec}_{\mathsf{tsk}}(c_1)$

SORTIE $\mathcal{S}' = (\mathsf{RevSetup}, \mathsf{RevKeyGen}, \mathsf{RevEnc}, \mathsf{RevDec}, \mathsf{Trace})$

Discussion sur la sécurité

Pour garantir la traçabilité

- $\mathcal{S}_{Msg}$ exigé anonyme
- $\mathcal{S}_{Id}$ exigé indistinguable
- $\mathcal{KDF}$ exigé résistant à 2ième pré-image
- $\mathcal{E}$ exigé non malléable

Anonymat révocable

Contributions :

- formalisation de la primitive de l'anonymat révocable
- définition d'une transformation générique
- (application aux contextes PKI et IBE)
- solution dans le contexte du chiffrement diffusion

Anonymat révocable

Contributions :

- formalisation de la primitive de l'anonymat révocable
- définition d'une transformation générique
- (application aux contextes PKI et IBE)
- solution dans le contexte du chiffrement diffusion

Anonymat révocable dans le contexte du chiffrement diffusion

Idée : Fonction à double trappe

- deux fonctions à trappe *différentes* : logarithme discret et factorisation
- deux secrets *indépendants*

L'idée vient du schéma de Paillier revisité par Bresson *et al.* :

> *« . . . dans un sous ensemble de $\mathbb{Z}/N^2\mathbb{Z}$ la connaissance de la factorisation de N permet de calculer le logarithme discret aisément ».*

Anonymat révocable dans le contexte du chiffrement diffusion

Idée : Fonction à double trappe

- deux fonctions à trappe *différentes* : logarithme discret et factorisation
- deux secrets *indépendants*

L'idée vient du schéma de Paillier revisité par Bresson *et al.* :

> *« . . . dans un sous ensemble de* $\mathbb{Z}/N^2\mathbb{Z}$ *la connaissance de la factorisation de N permet de calculer le logarithme discret aisément ».*

Description détaillée (1/4)

Setup $(p, q) \leftarrow \mathsf{Setup}(\kappa)$ et $N = pq$. Setup choisit un $g \in \mathbb{Z}^*_{N^2}$ d'ordre $\lambda(N)/2$.
Paramètres communs pp : $\{(N, g)\}$.
La clé de Traçage tsk : $\{\lambda(N)\}$.

Génération des clés $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KeyGen}(\mathsf{pp})$ où

$$\begin{cases} \mathsf{sk} & : & a \in \mathbb{Z}^*_N \\ \mathsf{pk} & : & h \equiv g^a \pmod{N^2}. \end{cases}$$

La clé est enregistrée dans une base de données.

Description détaillée (2/4)

Chiffrement Soit $m \in \mathbb{Z}_N$ le message pour $\mathcal{S} = \{\mathsf{pk}_i\}$, Encrypt :

1. tire $r \in_R \mathbb{Z}_N$ aléatoire
2. $\forall \mathsf{pk}_i \in \mathcal{S}$ calcule : $c_i \equiv h_i^r(1 + mN) \pmod{N^2}$
3. enchaîne le $\{c_i\}_{\mathsf{pk}_i \in \mathcal{S}}$ en ordre aléatoire
4. le chiffré est $C = (C_1, C_2) = (g^r, c_1||c_2|| \ldots ||c_n)$

Description détaillée (3/4)

Déchiffrement Decrypt prend C et une clé secrète $\mathsf{sk} = \{a_{\mathsf{id}}\}$:

1. décompose C comme C_1 et le chaînage des c_i
2. déchiffre les c_i jusqu'à ce que le bon soit trouvé :
   calcule $\tilde{m} \equiv \frac{c_i}{C_1^{a_{\mathsf{id}}}} - 1 \equiv \frac{h_i^r(1+mN)}{(g^r)^{a_{\mathsf{id}}}} - 1 \mod N^2$
   et $m = \frac{\tilde{m}}{N}$ dans $\mathbb{Z}$

Description détaillée (4/4)

Traçage Pour *déchiffrer* l'Autorité de Traçage prend un c_i aléatoirement et calcule $m \equiv \frac{L_N(c_i^{\lambda(N)})}{\lambda(N)} \mod N$ ($L_N(\cdot)$ est le logarithme discret partiel).
Pour tracer, l'Autorité de Traçage :

1. calcule $\tilde{c}_i \equiv c_i \mod N$ ($\equiv h_i^r \equiv g^{a_{\mathrm{id}} r} \mod N$)
2. calcule $\frac{L_N(\tilde{c}_i)}{L_N(C_1)} = \frac{a_{\mathrm{id}} r}{r} = a_{\mathrm{id}} \mod N$

Et interroge une base de données pour le lien clé-propriétaire.

Remarques sur le schéma (1/2)

Déchiffrement Decrypt prend C et une clé secrète $\mathsf{sk} = \{a_{\mathsf{id}}\}$:

1. ...
2. déchiffre les c_i jusqu'à ce que le bon soit trouvé : ...

Remarque :

Amélioration possible du temps de déchiffrement

Un seul déchiffrement nécessaire

Technique due à **[Bart *et al.* 2006]**

Remarques sur le schéma (2/2)

Traçage ...

Pour tracer, l'Autorité de Traçage :

1. ...
2. ...

Et interroge une base de données pour le lien clé-propriétaire.

Remarque :

Techniques pour base de données sans fuites (exemple : conserver une copie *hash*ée)

Sécurité et Anonymat

Indistinguabilité des chiffrements

$c_i \equiv h_i^r(1 + mN) \pmod{N^2}$
Montré indistinguable sous l'hypothèse du problème Diffie-Hellman décisionnel.

Indistinguabilité des clés

$c_i \equiv h_i^r(1 + mN) \pmod{N^2}$, où $1 + mN$ est une constante.
Montré anonyme sous l'hypothèse du problème Diffie-Hellman décisionnel.

Sécurité et Anonymat

Indistinguabilité des chiffrements

$c_i \equiv h_i^r(1 + mN) \pmod{N^2}$
Montré indistinguable sous l'hypothèse du problème Diffie-Hellman décisionnel.

Indistinguabilité des clés

$c_i \equiv h_i^r(1 + mN) \pmod{N^2}$, où $1 + mN$ est une constante.
Montré anonyme sous l'hypothèse du problème Diffie-Hellman décisionnel.

Contributions

Un schéma de chiffrement diffusion à clé publique avec la proprieté de l'anonymat révocable basé sur une fonction à double trappe

Plan de l'exposé

Introduction
- Définitions

Anonymat révocable
- Présentation du problème
- Contribution 1 : transformation générique
- Contribution 2 : schéma à double trappe

Une généralisation du schéma de Goldwasser-Micali
- Définitions
- Chiffrement de Goldwasser-Micali
- Contribution

Conclusion

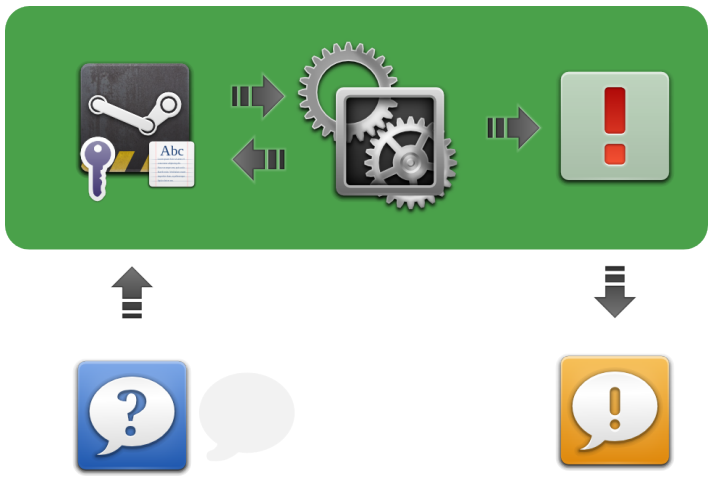
Sécurité prouvée

Modèle : hypothèse calculatoire

Adversaire : (but, moyens)

Réduction : Schéma réduit à l'hypothèse calculatoire

$\rightarrow$ adversaire $\mathcal{A}$ vu comme boîte noire



Symbole de Legendre

Définition (Symbole de Legendre)

Soit p un entier premier, soit $a \in (\mathbb{Z}/p\mathbb{Z})^*$. Le *symbole de Legendre de* $a \mod p$, noté $\left(\frac{a}{p}\right)$, vaut :

$$\left(\frac{a}{p}\right) = \begin{cases} +1 & \text{si } a \text{ est un résidu quadratique } \textit{modulo } p \\ -1 & \text{si } a \text{ n'en est pas un résidu quadratique } \textit{modulo } p \end{cases}$$

Comme le calculer ?

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p, \quad \forall a \in (\mathbb{Z}/p\mathbb{Z})^*.$$

Résiduosité quadratique *modulo* un entier *composite*

Résiduosité quadratique modulo un entier composite

Soit $N = pq$, avec p, q premiers impairs. Étant donné $a \in (\mathbb{Z}/N\mathbb{Z})^*$, on définit le *symbole de Jacobi modulo N* comme le produit de symboles de Legendre correspondants aux facteurs de N : $\left(\frac{a}{N}\right) = \left(\frac{a}{p}\right)\left(\frac{a}{q}\right)$

Résiduosité quadratique *modulo* un entier *composite*

Éléments *pseudo-quadratiques modulo N*

$$\mathbb{J}(N) = \left\{ a \in (\mathbb{Z}/N\mathbb{Z})^* \middle| \left(\frac{a}{N}\right) = 1 \right\}$$

Éléments *résidus quadratiques modulo N*

$$\mathbb{QR}(N) = \left\{ a \in (\mathbb{Z}/N\mathbb{Z})^* \middle| \left(\frac{a}{p}\right) = 1 = \left(\frac{a}{q}\right) \right\}$$

Hypothèse de la Résiduosité quadratique (QRA)

Définition

Soient p, q premiers et $N = pq$ leur produit. Alors, $\forall \mathcal{B}$ ppt, prenant en entrée un composite et un *pseudo-carré* z, qui donne en sortie « $z \in \mathbb{QR}(N)$ » ou « $z \notin \mathbb{QR}(N)$ » :

$$\left| \Pr\left[\mathcal{B}\left(\begin{array}{l} N \leftarrow \mathsf{KeyGen}(\kappa), \\ z \in_R \mathbb{J}(N) \end{array} \right) = \text{« } z \in \mathbb{QR}(N) \text{ »} \,\middle|\, z \in \mathbb{QR}(N) \right] - \Pr\left[\mathcal{B}\left(\begin{array}{l} N \leftarrow \mathsf{KeyGen}(\kappa), \\ z \in_R \mathbb{J}(N) \end{array} \right) = \text{« } z \in \mathbb{QR}(N) \text{ »} \,\middle|\, z \notin \mathbb{QR}(N) \right] \right|$$

est négligeable.

Schéma de chiffrement à clé publique Goldwasser-Micali

KeyGen(1^κ) $(p, q) \leftarrow$ KeyGen(1^κ). KeyGen définit $y \in (\mathbb{Z}/N\mathbb{Z})^*$ t.q. $y \in \mathbb{J}(N) \setminus \mathbb{QR}(N)$.
La clé publique est $\mathsf{pk} = (N, y)$ et la clé privée correspondante est $\mathsf{sk} = p$.

Encrypt(pk, m) Soit $\mathcal{M} = \{0, 1\}$. Encrypt :

- prend un $x \in_R (\mathbb{Z}/N\mathbb{Z})^*$ aléatoirement et
- calcule $c \equiv y^m x^2 \mod N$.

Le chiffré en sortie est c.

Decrypt(sk, c) Decrypt :

- calcule $z = \left(\frac{c}{p}\right)$
- retrouve le message m tel que $(-1)^m = z$.

Le message déchiffré en sortie est m.

Sécurité sémantique

Soit $\mathcal{A}$ un adversaire avec une probabilité de réussite :

$$\Pr\left[b = b' \mid \dots\right] = \frac{1}{2} + \delta_{\mathcal{A}}$$

Supposons que $\mathcal{A}$ soit un adversaire efficace : $\delta_{\mathcal{A}}$ non négligeable.

Réduction

Soit $\mathcal{B}$ l'algorithme qui suit :

Input: Un couple (N, z) où $N = pq$ avec p, q premiers impairs et $z \in \mathbb{J}(N)$
Output: Un bit guess $\in \{\square, \boxslash\}$

1: Pose la clé publique égale à $\mathsf{pk} = (N, y) = (N, z)$
2: Envoie la clé publique à l'adversaire $\mathcal{A}$
3: Tire un bit aléatoire $b \in \{0, 1\}$, un élément $x \in_R (\mathbb{Z}/N\mathbb{Z})^*$ et calcule le chiffré challenge :

$$c = y^b x^2 \pmod{N}$$

4: Soit b' le bit en réponse de $\mathcal{A}$
5: guess $\leftarrow \begin{cases} \boxslash & \text{si } b = b' \\ \square & \text{si } b \neq b' \end{cases}$

Avantage de $\mathcal{B}$

Stratégie de réponse : guess $\leftarrow \begin{cases} \boxslash & \text{si } b = b' \\ \square & \text{si } b \neq b' \end{cases}$

Probabilité que $\mathcal{B}$ donne la réponse correcte :

si $z \notin \mathbb{QR}(N)$:

$$\Pr[\text{« } z \notin \mathbb{QR}(N) \text{ »}] = \Pr[b = b' \,|\, b' \leftarrow \mathcal{A}(\dots)] = \tfrac{1}{2} + \delta_{\mathcal{A}}$$

si $z \in \mathbb{QR}(N)$:

$$c = y^b x^2 = z^b x^2 = t^{2b} x^2 = (t^b x)^2 \pmod N$$

$$\Pr[\text{« } z \notin \mathbb{QR}(N) \text{ »}] = \Pr[b = b' \,|\, b' \leftarrow \mathcal{A}(\dots)] = \tfrac{1}{2}$$

$$\mathrm{Adv}_{\mathrm{QRA}}(\mathcal{B}) = \left| \frac{1}{2} - \frac{1}{2} - \delta_{\mathcal{A}} \right|.$$

$\mathrm{Adv}_{\mathrm{QRA}}$ non négligeable si $\mathcal{A}$ efficace $\Rightarrow \delta_{\mathcal{A}}$ négligeable.

Pas d'adversaire efficace $\Rightarrow$ schéma sûr

Avantage de $\mathcal{B}$

Stratégie de réponse : guess $\leftarrow \begin{cases} \boxslash & \text{si } b = b' \\ \square & \text{si } b \neq b' \end{cases}$

Probabilité que $\mathcal{B}$ donne la réponse correcte :

si $z \notin \mathbb{QR}(N)$:

$$\Pr[\text{« } z \notin \mathbb{QR}(N) \text{ »}] = \Pr[b = b' \,|\, b' \leftarrow \mathcal{A}(\dots)] = \tfrac{1}{2} + \delta_{\mathcal{A}}$$

si $z \in \mathbb{QR}(N)$:

$$c = y^b x^2 = z^b x^2 = t^{2b} x^2 = (t^b x)^2 \pmod{N}$$

$$\Pr[\text{« } z \notin \mathbb{QR}(N) \text{ »}] = \Pr[b = b' \,|\, b' \leftarrow \mathcal{A}(\dots)] = \tfrac{1}{2}$$

$$\mathrm{Adv}_{\mathrm{QRA}}(\mathcal{B}) = \left| \frac{1}{2} - \frac{1}{2} - \delta_{\mathcal{A}} \right|.$$

$\mathrm{Adv}_{\mathrm{QRA}}$ non négligeable si $\mathcal{A}$ efficace $\Rightarrow \delta_{\mathcal{A}}$ négligeable.

Pas d'adversaire efficace $\Rightarrow$ schéma sûr

Avantage de $\mathcal{B}$

Stratégie de réponse : guess $\leftarrow \begin{cases} \boxslash & \text{si } b = b' \\ \square & \text{si } b \neq b' \end{cases}$

Probabilité que $\mathcal{B}$ donne la réponse correcte :

si $z \notin \mathbb{QR}(N)$:

$$\Pr[\text{« } z \notin \mathbb{QR}(N) \text{ »}] = \Pr[b = b' \,|\, b' \leftarrow \mathcal{A}(\dots)] = \tfrac{1}{2} + \delta_{\mathcal{A}}$$

si $z \in \mathbb{QR}(N)$:

$$c = y^b x^2 = z^b x^2 = t^{2b} x^2 = (t^b x)^2 \pmod N$$

$$\Pr[\text{« } z \notin \mathbb{QR}(N) \text{ »}] = \Pr[b = b' \,|\, b' \leftarrow \mathcal{A}(\dots)] = \tfrac{1}{2}$$

$$\mathrm{Adv}_{\mathrm{QRA}}(\mathcal{B}) = \left| \frac{1}{2} - \frac{1}{2} - \delta_{\mathcal{A}} \right|.$$

$\mathrm{Adv}_{\mathrm{QRA}}$ non négligeable si $\mathcal{A}$ efficace $\Rightarrow \delta_{\mathcal{A}}$ négligeable.

Pas d'adversaire efficace $\Rightarrow$ schéma sûr

Avantage de $\mathcal{B}$

Stratégie de réponse : guess $\leftarrow \begin{cases} \boxslash & \text{si } b = b' \\ \square & \text{si } b \neq b' \end{cases}$

Probabilité que $\mathcal{B}$ donne la réponse correcte :

si $z \notin \mathbb{QR}(N)$:

$$\Pr[\text{« } z \notin \mathbb{QR}(N) \text{ »}] = \Pr[b = b' \,|\, b' \leftarrow \mathcal{A}(\dots)] = \tfrac{1}{2} + \delta_{\mathcal{A}}$$

si $z \in \mathbb{QR}(N)$:

$$c = y^b x^2 = z^b x^2 = t^{2b} x^2 = (t^b x)^2 \pmod N$$
$$\Pr[\text{« } z \notin \mathbb{QR}(N) \text{ »}] = \Pr[b = b' \,|\, b' \leftarrow \mathcal{A}(\dots)] = \tfrac{1}{2}$$

$$\mathrm{Adv}_{\mathrm{QRA}}(\mathcal{B}) = \left| \frac{1}{2} - \frac{1}{2} - \delta_{\mathcal{A}} \right|.$$

$\mathrm{Adv}_{\mathrm{QRA}}$ non négligeable si $\mathcal{A}$ efficace $\Rightarrow \delta_{\mathcal{A}}$ négligeable.

Pas d'adversaire efficace $\Rightarrow$ schéma sûr

Avantage de $\mathcal{B}$

Stratégie de réponse : guess $\leftarrow \begin{cases} \boxslash & \text{si } b = b' \\ \square & \text{si } b \neq b' \end{cases}$

Probabilité que $\mathcal{B}$ donne la réponse correcte :

si $z \notin \mathbb{QR}(N)$:

$$\Pr[\text{« } z \notin \mathbb{QR}(N) \text{ »}] = \Pr[b = b' \,|\, b' \leftarrow \mathcal{A}(\dots)] = \tfrac{1}{2} + \delta_{\mathcal{A}}$$

si $z \in \mathbb{QR}(N)$:

$$c = y^b x^2 = z^b x^2 = t^{2b} x^2 = (t^b x)^2 \pmod N$$
$$\Pr[\text{« } z \notin \mathbb{QR}(N) \text{ »}] = \Pr[b = b' \,|\, b' \leftarrow \mathcal{A}(\dots)] = \tfrac{1}{2}$$

$$\mathrm{Adv}_{\mathrm{QRA}}(\mathcal{B}) = \left| \frac{1}{2} - \frac{1}{2} - \delta_{\mathcal{A}} \right|.$$

$\mathrm{Adv}_{\mathrm{QRA}}$ non négligeable si $\mathcal{A}$ efficace $\Rightarrow$ $\delta_{\mathcal{A}}$ négligeable.

Pas d'adversaire efficace $\Rightarrow$ schéma sûr

Généralisations et améliorations

- Benalot et Fischer (**Ben87, CF85**)
- Naccache et Stern (**NS98**)

Utilisent des résidus de puissances r-ièmes ($r > 2$). Le déchiffrement est un calcul de logarithme discret. . . et le problème est plus « artificiel ».

Contribution

- utilise des résidus d'ordre 2^k-ièmes
- basée sur la résiduosité quadratique
- bonne expansion du chiffré
- déchiffrement rapide
- pour $k = 1$ coïncide avec le schéma originel

Notre schéma généralisé

KeyGen(1^κ) $(p, q, y) \leftarrow \mathsf{KeyGen}(1^\kappa)$

$$\begin{cases} p, q \equiv 1 \pmod{2^k}, \\ y \in \mathbb{J}(N) \setminus \mathbb{QR}(N) \end{cases}$$

La clé publique est $\mathsf{pk} = (N, y, k)$ et la clé privée correspondante est $\mathsf{sk} = p$

Encrypt(pk, m) Soit $\mathcal{M} = \{0, \cdots, 2^k - 1\}$. Encrypt :

- prend un $x \in_R (\mathbb{Z}/N\mathbb{Z})^*$ aléatoirement et
- calcule $c \equiv y^m x^{2^k} \mod N$

Le chiffré : c

Decrypt(sk, c) Decrypt :

- il calcule $z = \left(\frac{c}{p}\right)_{2^k}$
- il trouve $m \in \{0, \cdots, 2^k - 1\}$ tel que la relation $\left[\left(\frac{y}{p}\right)_{2^k}\right]^m = z \mod p$ soit vérifiée

  Le déchiffré : m

Performances

TABLE: Expansion du chiffré lors d'une utilisation typique

Schéma de chiffrement	**Hypothèse**	**Taille du chiffré**
Goldwasser-Micali	QR	$k \cdot \log_2 N$
Benaloh-Fisher	PR	$\left\lceil \frac{k}{\log_2 r} \right\rceil \cdot \log_2 N$
Naccache-Stern	PR	$\log_2 N$
Notre schéma	QR	$\log_2 N$

Sécurité sémantique

Soit $\mathcal{A}$ un adversaire avec une probabilité de réussite :

$$\Pr\left[b = b' \mid \dots\right] = \frac{1}{2} + \delta_{\mathcal{A}}$$

Supposons que $\mathcal{A}$ soit un adversaire efficace : $\delta_{\mathcal{A}}$ non négligeable.

Preuve *réduite* :

- $k = 2$;
- $\mathcal{A}$ choisit toujours $m_0 = 0$.

Trace de la preuve

Lemme ↘

Sous la QRA les distributions du chiffré du message $m_i = 2^i$ est indiscernable du chiffrement du message $m_0 = 0$.
(Dans notre cas : $m_i \in \{1, 2\}$)

Lemme ↗

Si le chiffrement du message $m_0 = 0$ est indistinguable respectivement du chiffrement des messages $m = 1, \ldots, j$ alors il est indistinguable du chiffrement du message $m = j + 1$.

Trace de la preuve

Lemme ↘

Sous la QRA les distributions du chiffré du message $m_i = 2^i$ est indiscernable du chiffrement du message $m_0 = 0$.
(Dans notre cas : $m_i \in \{1, 2\}$)

Lemme ↗

Si le chiffrement du message $m_0 = 0$ est indistinguable respectivement du chiffrement des messages $m = 1, \ldots, j$ alors il est indistinguable du chiffrement du message $m = j + 1$.

Cas $(m_0, m_1) = (0, 2)$

Dans ce cas :

$$c = y^{2b}x^4 = (y^b x^2)^2 \pmod{N}$$

Il s'agit du carré du chiffré du schéma pour $k = 1$ (GM).

$$\Downarrow$$

Indistinguables sous la QRA.

Les chiffrements de $m_0 = 0$ et $m_1 = 2$ sont indistinguables

Cas $(m_0, m_1) = (0, 2)$

Dans ce cas :

$$c = y^{2b}x^4 = (y^b x^2)^2 \pmod{N}$$

Il s'agit du carré du chiffré du schéma pour $k = 1$ (GM).

$$\Downarrow$$

Indistinguables sous la QRA.

Les chiffrements de $m_0 = 0$ et $m_1 = 2$ sont indistinguables

Cas $(m_0, m_1) = (0, 2)$

Dans ce cas :

$$c = y^{2b}x^4 = (y^b x^2)^2 \pmod{N}$$

Il s'agit du carré du chiffré du schéma pour $k = 1$ (GM)

$\mathsf{Adv}_{\mathsf{IND}}(\mathcal{A}) = \delta_2$ est négligeable

Les chiffrements de $m_0 = 0$ et $m_1 = 2$ sont indistinguables

Cas $(m_0, m_1) = (0, 1)$

Démonstration par l'absurde.
Soit $\mathcal{A}$ un adversaire efficace avec probabilité de réussite :

$$\Pr\left[b = b' \mid \dots\right] = \frac{1}{2} + \delta_1 \gg \frac{1}{2}$$

(c.-à-d. δ_1 non négligeable)

Cas $(m_0, m_1) = (0, 1)$

Soit $\mathcal{B}$ l'algorithme qui suit :

Input: Un couple (N, z) où $N = pq$ avec p, q premiers impairs et $z \in \mathbb{J}(N)$

Output: Un bit guess $\in \{\square, \boxslash\}$

1: Pose la clé publique égale à $\mathsf{pk} = (N, y, 2) = (N, z, 2)$

2: Envoie la clé publique à l'adversaire $\mathcal{A}$

3: Tire un bit aléatoire $b \in \{0, 1\}$, un élément $x \in_R (\mathbb{Z}/\mathbb{Z})^*$ et calcule le chiffré challenge :

$$c = y^{m_b} x^4 \pmod{N}$$

4: Soit b' le bit en réponse de $\mathcal{A}$

5: guess $\leftarrow \begin{cases} \boxslash & \text{si } b = b' \\ \square & \text{si } b \neq b' \end{cases}$

Avantage de $\mathcal{B}$

Stratégie de réponse : guess $\leftarrow \begin{cases} \boxslash & \text{si } b = b' \\ \square & \text{si } b \neq b' \end{cases}$

Probabilité que $\mathcal{B}$ donne la réponse correcte :

si $z \notin \mathbb{QR}(N)$:

$$\Pr[\text{« } z \notin \mathbb{QR}(N) \text{ »}] = \Pr[b = b' \,|\, b' \leftarrow \mathcal{A}(\dots)] = \tfrac{1}{2} + \delta_1$$

si $z \in \mathbb{QR}(N)$:

$$c = y^b x^4 = z^b x^4 = t^{2b} x^4 \pmod{N}$$

$$\Pr[\text{« } z \notin \mathbb{QR}(N) \text{ »}] = \Pr[b = b' \,|\, b' \leftarrow \mathcal{A}(\dots)] = \tfrac{1}{2} + \delta_2$$

$$\mathrm{Adv}_{\mathrm{QRA}}(\mathcal{B}) = \left| \frac{1}{2} + \delta_1 - \frac{1}{2} - \delta_2 \right| = |\delta_1 - \delta_2| .$$

Avantage de $\mathcal{B}$

Stratégie de réponse : guess $\leftarrow \begin{cases} \boxslash & \text{si } b = b' \\ \square & \text{si } b \neq b' \end{cases}$

Probabilité que $\mathcal{B}$ donne la réponse correcte :

si $z \notin \mathbb{QR}(N)$:

$$\Pr[\text{« } z \notin \mathbb{QR}(N) \text{ »}] = \Pr[b = b' \,|\, b' \leftarrow \mathcal{A}(\dots)] = \tfrac{1}{2} + \delta_1$$

si $z \in \mathbb{QR}(N)$:

$$c = y^b x^4 = z^b x^4 = t^{2b} x^4 \pmod{N}$$

$$\Pr[\text{« } z \notin \mathbb{QR}(N) \text{ »}] = \Pr[b = b' \,|\, b' \leftarrow \mathcal{A}(\dots)] = \tfrac{1}{2} + \delta_2$$

$$\mathrm{Adv}_{\mathrm{QRA}}(\mathcal{B}) = \left| \frac{1}{2} + \delta_1 - \frac{1}{2} - \delta_2 \right| = |\delta_1 - \delta_2| .$$

Avantage de $\mathcal{B}$

Stratégie de réponse : guess $\leftarrow \begin{cases} \boxslash & \text{si } b = b' \\ \square & \text{si } b \neq b' \end{cases}$

Probabilité que $\mathcal{B}$ donne la réponse correcte :

si $z \notin \mathbb{QR}(N)$:

$$\Pr[\text{« } z \notin \mathbb{QR}(N) \text{ »}] = \Pr[b = b' \,|\, b' \leftarrow \mathcal{A}(\dots)] = \tfrac{1}{2} + \delta_1$$

si $z \in \mathbb{QR}(N)$:

$$c = y^b x^4 = z^b x^4 = t^{2b} x^4 \pmod{N}$$

$$\Pr[\text{« } z \notin \mathbb{QR}(N) \text{ »}] = \Pr[b = b' \,|\, b' \leftarrow \mathcal{A}(\dots)] = \tfrac{1}{2} + \delta_2$$

$$\mathrm{Adv}_{\mathrm{QRA}}(\mathcal{B}) = \left| \frac{1}{2} + \delta_1 - \frac{1}{2} - \delta_2 \right| = |\delta_1 - \delta_2| .$$

Avantage de $\mathcal{B}$

Si $\mathcal{A}_1$ est efficace : $\mathrm{Adv}_{\mathrm{QRA}}$ est non négligeable . Absurde.

Adversaire a avantage négligeable : le schéma est sûr

si $z \in \mathbb{QR}(N)$:

$$c = y^b x^4 = z^b x^4 = t^{2b} x^4 \pmod{N}$$

$$\Pr[\text{« } z \notin \mathbb{QR}(N) \text{ »}] = \Pr[b = b' \,|\, b' \leftarrow \mathcal{A}(\dots)] = \tfrac{1}{2} + \delta_2$$

$$\mathrm{Adv}_{\mathrm{QRA}}(\mathcal{B}) = \left| \frac{1}{2} + \delta_1 - \frac{1}{2} - \delta_2 \right| = |\delta_1 - \delta_2| .$$

Plan de l'exposé

Introduction
- Définitions

Anonymat révocable
- Présentation du problème
- Contribution 1 : transformation générique
- Contribution 2 : schéma à double trappe

Une généralisation du schéma de Goldwasser-Micali
- Définitions
- Chiffrement de Goldwasser-Micali
- Contribution

Conclusion

Conclusion

Anonymat révocable :

- formalisation de la primitive
- définition d'une transformation générique
- (application aux contextes PKI et IBE)
- solution dans le contexte du chiffrement diffusion

Conclusion

Chiffrement de Goldwasser-Micali :

- généralisation du schéma aux résidus 2^k-ièmes
- amélioration de l'expansion du chiffré
- hypothèse algorithmique standard
- déchiffrement rapide

Perspectives

- rendre anonyme (révocable) le schéma de Goldwasser-Micali
- généraliser le schéma de Cocks avec les résidus 2^k-ièmes

Merci !

Sur quelques questions de cryptographie :
Anonymat révocable et
Une généralisation du schéma de
Goldwasser-Micali

Davide Alessio

Technicolor & Université de Rennes 1
Rennes, 13 décembre 2011

Plan de l'exposé

Slides optionnels

Déchiffrement rapide

Decrypt(sk, c) L'algorithme de déchiffrement Decrypt pour récupérer le message en clair m à partir du chiffré c procède comme suit :

- il pose $m = 0$,
- pour $i \in \{1, \ldots, k\}$
  1. il calcule $z = \left(\frac{c}{p}\right)_{2^i} \pmod p$ et $t = \left(\frac{c}{p}\right)_{2^i}^{m} \pmod p$
  2. si $z \neq t$ alors $m \leftarrow m + 2^{i-1}$
- il donne en sortie m.

Déchiffrement rapide

Soit $m \in \mathcal{M}$ un message en clair. Considérons son expansion binaire : $m = \sum_{i=0}^{k-1} m_i 2^i$ où $m_i \in \{0, 1\}$. Soit maintenant $c = y^m x^{2^k} \mod N$ son chiffré, avec x un entier non nul, alors

$$\begin{aligned}
\left(\frac{c}{p}\right)_{2^i} &= \left(\frac{y^m x^{2^k}}{p}\right)_{2^i} = \left(\frac{y^{\sum_{j=0}^{k-1} m_j 2^j}}{p}\right)_{2^i} = \left(\frac{y^{\sum_{j=0}^{i-1} m_j 2^j}}{p}\right)_{2^i} \cdot \left(\frac{y^{\sum_{j=i}^{k-1} m_j 2^j}}{p}\right)_{2^i} = \\
&= \left(\frac{y^{\sum_{j=0}^{i-1} m_j 2^j}}{p}\right)_{2^i} \cdot \left(\frac{y^{\sum_{j=0}^{k-i-1} m_{j+i} 2^j}}{p}\right)_{2^i}^{2^i} = \left(\frac{y^{\sum_{j=0}^{i-1} m_j 2^j}}{p}\right)_{2^i} \cdot 1 = \\
&= \left(\frac{y^{\sum_{j=0}^{i-1} m_j 2^j}}{p}\right)_{2^i} = \\
&= \left(\frac{y}{p}\right)_{2^i}^{\sum_{j=0}^{i-1} m_j 2^j} \pmod{p}.
\end{aligned}$$

Anonymat révocable : basé sur la PKI

Setup $g \in \mathbb{G}$, $|\mathbb{G}| = p$.
Paramètres communs : $\{I = \{p, g\}, \mathcal{E}, \mathcal{KDF}, \mathcal{H}\}$.
Clé de traçage : $(\text{tpk}, \text{tsk}) = (h = g^s, s) \in \mathbb{G}^2$

Génération des clés $\mathcal{U}_i$ choisit $x_i \in \mathbb{Z}_p$, calcule $y_i = g^{x_i}$
Clé de $\mathcal{U}_i$: $(\text{upk}_i, \text{usk}_i) = (y_i, x_i)$

Chiffrement Pour chiffrer $m \in \mathcal{M}$:

1. $r_1 \xleftarrow{R} \mathbb{Z}_p$; $c_1 = (g^{r_1}, y_i \cdot h^{r_1})$;
2. $k = \mathcal{KDF}(c_1)$, $r_2 \xleftarrow{R} \mathbb{Z}_p$, $c_2 = (g^{r_2}, \mathcal{H}({y_i}^{r_2}) \oplus \mathcal{E}_k(m))$

Le chiffré est $c = (c_1, c_2)$

Déchiffrement En entrée $c = (c_1, c_2)$, pour déchiffrer m :

1. donné $c_2 = (\varphi_1, \varphi_2)$, calcule $t = H({\varphi_1}^{x_i})$ avec l'élément secret x_i
2. calcule $k' = \mathcal{KDF}(c_1)$ et ensuite $m = \mathcal{E}_{k'}^{-1}(t \oplus \varphi_2)$

Tracing The recipient can be traced as follow :

1. letting $c_1 = (\vartheta_1, \vartheta_2)$, compute $y' = \vartheta_2 \cdot {\vartheta_1}^{-s}$;
2. find $y_j = y'$

Anonymat révocable : basé sur l'identité

Setup $\hat{e} : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ un couplage non-degenere Paramètres communs : $\{\mathcal{M}, p, g, \hat{e}, h, \mu, \mathcal{E}, \mathcal{KDF}, \mathcal{H}\}$ Clé de traçage : $(\text{tpk}, \text{tsk}) = (h = g^s, s)$

Génération des clés $\mathcal{U}_i$ obtient $\text{usk}_i = g_i$, où $g_i = \mu(\mathcal{U}_i)^s$.

Chiffrement Pour chiffrer $m \in \mathcal{M}$:

1. $r_1 \xleftarrow{R} \mathbb{Z}_p$; $c_1 = (g^{r_1}, \mu(\mathcal{U}_i) \cdot h^{r_1})$;
2. $k = \mathcal{KDF}(c_1)$, $r_2 \xleftarrow{R} \mathbb{Z}_p$, $c_2 = (g^{r_2}, \mathcal{H}(z_i{}^{r_2}) \oplus \mathcal{E}_k(m))$ où $z_i = \hat{e}(\mu(\mathcal{U}_i), h)$

Le chiffré est $c = (c_1, c_2)$

Déchiffrement En entrée $c = (c_1, c_2)$, pour déchiffrer m :

1. $c_2 = (\varphi_1, \varphi_2)$, $t = \mathcal{H}(\hat{e}(g_i, \varphi_1))$, g_i
2. $k' = \mathcal{KDF}(c_1)$, $m = \mathcal{E}_{k'}^{-1}(t \oplus \varphi_2)$

Traçage Le destinataire est tracé comme suit :

1. soit $c_1 = (\vartheta_1, \vartheta_2)$, on calcule $g' = \vartheta_2 \cdot \vartheta_1{}^{-s}$
2. trouver $\mu(\mathcal{U}_j) = g'$ dans la base de données