Caractérisation sécuritaire des mémoires magnétiques MRAM

Thomas Sarno

NNT : 2015 EMSE 0796

THÈSE

présentée par

Thomas SARNO

pour obtenir le grade de
Docteur de l'École Nationale Supérieure des Mines de Saint-Étienne

Spécialité : Microélectronique

Caractérisation sécuritaire des mémoires magnétiques MRAM

Membres du jury

Président :	Jean-Michel PORTAL	Professeur, IN2MP, Marseille
Rapporteurs :	David NACCACHE	Professeur, ENS, Paris
	Lionel TORRES	Professeur, LIRMM, Montpellier
Examinateur(s) :	Anne-Lise RIBOTTA	Ingénieure de Recherche, EMSE, Gardanne
	Philippe COLLOT	Professeur, ENSAM
	Bruno MUSSARD	Ingénieur, Crocus Technology, Rousset
	Ali ALAOUI	Ingénieur, Crocus Technology, Rousset
Directeur(s) de thèse :	Assia TRIA	Ingénieure de Recherche, CEA-Tech, Gardanne

Spécialités doctorales	Responsables :	Spécialités doctorales	Responsables
SCIENCES ET GENIE DES MATERIAUX	K. Wolski Directeur de recherche	MATHEMATIQUES APPLIQUEES	O. Roustant, Maître-assistant
MECANIQUE ET INGENIERIE	S. Drapier, professeur	INFORMATIQUE	O. Boissier, Professeur
GENIE DES PROCEDES	F. Gruy, Maître de recherche	IMAGE, VISION, SIGNAL	JC. Pinoli, Professeur
SCIENCES DE LA TERRE	B. Guy, Directeur de recherche	GENIE INDUSTRIEL	A. Dolgui, Professeur
SCIENCES ET GENIE DE L'ENVIRONNEMENT	D. Graillot, Directeur de recherche	MICROELECTRONIQUE	S. Dauzere Peres, Professeur

EMSE : Enseignants-chercheurs et chercheurs autorisés à diriger des thèses de doctorat (titulaires d'un doctorat d'État ou d'une HDR)

ABSI	Nabil	CR	Génie industriel	CMP
AVRIL	Stéphane	PR2	Mécanique et ingénierie	CIS
BALBO	Flavien	PR2	Informatique	FAYOL
BASSEREAU	Jean-François	PR	Sciences et génie des matériaux	SMS
BATTAIA-GUSCHINSKAYA	Olga	CR		FAYOL
BATTON-HUBERT	Mireille	PR2	Sciences et génie de l'environnement	FAYOL
BERGER DOUCE	Sandrine	PR2	Sciences de gestion	FAYOL
BIGOT	Jean Pierre	MR(DR2)	Génie des Procédés	SPIN
BILAL	Essaid	DR	Sciences de la Terre	SPIN
BLAYAC	Sylvain	MA(MDC)	Microélectronique	CMP
BOISSIER	Olivier	PR1	Informatique	FAYOL
BONNEFOY	Olivier	MA(MDC)	Génie des Procédés	SPIN
BORBELY	Andras	MR(DR2)	Sciences et génie des matériaux	SMS
BOUCHER	Xavier	PR2	Génie Industriel	FAYOL
BRODHAG	Christian	DR	Sciences et génie de l'environnement	FAYOL
BRUCHON	Julien	MA(MDC)	Mécanique et ingénierie	SMS
BURLAT	Patrick	PR1	Génie Industriel	FAYOL
COURNIL	Michel	PR0	Génie des Procédés	DIR
DARRIEULAT	Michel	IGM	Sciences et génie des matériaux	SMS
DAUZERE-PERES	Stéphane	PR1	Génie Industriel	CMP
DEBAYLE	Johan	CR	Image Vision Signal	CIS
DELAFOSSE	David	PR0	Sciences et génie des matériaux	SMS
DELORME	Xavier	MA(MDC)		FAYOL
DESRAYAUD	Christophe	PR1	Mécanique et ingénierie	SMS
DOLGUI	Alexandre	PR0	Génie Industriel	FAYOL
DRAPIER	Sylvain	PR1	Mécanique et ingénierie	SMS
FAVERGEON	Loïc	CR	Génie des Procédés	SPIN
FEILLET	Dominique	PR1	Génie Industriel	CMP
FRACZKIEWICZ	Anna	DR	Sciences et génie des matériaux	SMS
GARCIA	Daniel	MR(DR2)	Génie des Procédés	SPIN
GAVET	Yann	MA(MDC)	Image Vision Signal	CIS
GERINGER	Jean	MA(MDC)	Sciences et génie des matériaux	CIS
GOEURIOT	Dominique	DR	Sciences et génie des matériaux	SMS
GRAILLOT	Didier	DR	Sciences et génie de l'environnement	SPIN
GROSSEAU	Philippe	DR	Génie des Procédés	SPIN
GRUY	Frédéric	PR1	Génie des Procédés	SPIN
GUY	Bernard	DR	Sciences de la Terre	SPIN
HAN	Woo-Suck	MR	Mécanique et ingénierie	SMS
HERRI	Jean Michel	PR1	Génie des Procédés	SPIN
KERMOUCHE	Guillaume	PR2	Mécanique et Ingénierie	SMS
KLOCKER	Helmut	DR	Sciences et génie des matériaux	SMS
LAFOREST	Valérie	MR(DR2)	Sciences et génie de l'environnement	FAYOL
LERICHE	Rodolphe	CR	Mécanique et ingénierie	FAYOL
LI	Jean-Michel		Microélectronique	CMP
MALLIARAS	Georges	PR1	Microélectronique	CMP
MAURINE	Philippe	Ingénieur de recherche		CMP
MOLIMARD	Jérôme	PR2	Mécanique et ingénierie	CIS
MONTHEILLET	Frank	DR	Sciences et génie des matériaux	SMS
MOUTTE	Jacques	CR	Génie des Procédés	SPIN
NEUBERT	Gilles	PR		FAYOL
NIKOLOVSKI	Jean-Pierre	Ingénieur de recherche		CMP
NORTIER	Patrice	PR1		SPIN
OWENS	Rosin	MA(MDC)		CMP
PICARD	Gauthier	MA(MDC)		FAYOL
PIJOLAT	Christophe	PR0	Génie des Procédés	SPIN
PIJOLAT	Michèle	PR1	Génie des Procédés	SPIN
PINOLI	Jean Charles	PR0	Image Vision Signal	CIS
POURCHEZ	Jérémy	MR	Génie des Procédés	CIS
ROBISSON	Bruno	Ingénieur de recherche		CMP
ROUSSY	Agnès	MA(MDC)	Génie industriel	CMP
ROUSTANT	Olivier	MA(MDC)	Mathématiques appliquées	FAYOL
ROUX	Christian	PR	Image Vision Signal	CIS
STOLARZ	Jacques	CR	Sciences et génie des matériaux	SMS
TRIA	Assia	Ingénieur de recherche	Microélectronique	CMP
VALDIVIESO	François	PR2	Sciences et génie des matériaux	SMS
VIRICELLE	Jean Paul	DR	Génie des Procédés	SPIN
WOLSKI	Krzystof	DR	Sciences et génie des matériaux	SMS
XIE	Xiaolan	PR1	Génie industriel	CIS
YUGMA	Gallian	CR	Génie industriel	CMP

ENISE : Enseignants-chercheurs et chercheurs autorisés à diriger des thèses de doctorat (titulaires d'un doctorat d'État ou d'une HDR)

BERGHEAU	Jean-Michel	PU	Mécanique et Ingénierie	ENISE
BERTRAND	Philippe	MCF	Génie des procédés	ENISE
DUBUJET	Philippe	PU	Mécanique et Ingénierie	ENISE
FEULVARCH	Eric	MCF	Mécanique et Ingénierie	ENISE
FORTUNIER	Roland	PR	Sciences et Génie des matériaux	ENISE
GUSSAROV	Andrey	Enseignant contractuel	Génie des procédés	ENISE
HAMDI	Hédi	MCF	Mécanique et Ingénierie	ENISE
LYONNET	Patrick	PU	Mécanique et Ingénierie	ENISE
RECH	Joël	PU	Mécanique et Ingénierie	ENISE
SMUROV	Igor	PU	Mécanique et Ingénierie	ENISE
TOSCANO	Rosario	PU	Mécanique et Ingénierie	ENISE
ZAHOUANI	Hassan	PU	Mécanique et Ingénierie	ENISE

Mise à jour : 11/05/2015

École Nationale Supérieure des Mines
de Saint-Étienne

NNT : *Communiqué le jour de la soutenance*

Thomas SARNO

Secure characterization of magnetic memories MRAM

Speciality: microelectronics

Keywords: MRAM, physical attacks, electromagnetic leakage, magnetic field, electromagnetic pulses, TAS-MRAM

Abstract:

MRAM (magnetoresistive RAM) is an emergent non-volatile memory technology; it has the particularity to store data in magnetic moments orientations. It has very interesting characteristics that overwhelm mature technologies on several points. Crocus Technology is developing a new MRAM technology called TAS-MRAM (for Thermally Assisted Switching). During write operations, this new MRAM technology uses a current to heat the memory cell. This reduces the power consumption and makes scalability easier. TAS-MRAM are developed for secure or critical applications but this technology relies on spintronic, a field of physics not much studied for electronics security.

This work aims to evaluate potential security weaknesses of this technology. More specifically the memory capacity to guarantee data confidentiality was studied. This work was divided in two parts; one part is dedicated to the analysis of MRAM resistance against physical perturbations, with a special focus on magnetic fields (both static and pulsed) effects on read and write operations as well as their effects on data retention. Various methods to reduce these effects were tested and compared. The effect of high temperature was also studied.

The second part focuses on the analysis of electromagnetic emissions of the MRAM components during its operations. Methods to retrieve the Hamming weight of data written in the memory are exposed and compared.

École Nationale Supérieure des Mines
de Saint-Étienne

NNT : *Communiqué le jour de la soutenance*

Thomas SARNO

Caractérisation sécuritaire des mémoires magnétiques MRAM

Spécialité: Microélectronique

Mots clefs : MRAM, attaques physiques, fuites électromagnétiques, champ magnétique, impulsions électromagnétiques, TAS-MRAM

Résumé :

La MRAM (magnetoresistive RAM) est une technologie de mémoire non-volatile émergente, elle a la particularité de stocker les données sous forme d'orientations de moments magnétiques. Ses performances sont intéressantes et surpassent les technologies actuellement utilisées sur plusieurs aspects. Crocus Technology développe une nouvelle génération de MRAM appelées TAS-MRAM (pour Thermally Assisted Switching MRAM). Ces MRAM ont la particularité d'effectuer les opérations d'écritures à hautes températures, améliorant ainsi la consommation électrique et facilitant sa réduction d'échelle. Les TAS-MRAM sont développées pour des applications sécuritaires ou critiques, cependant la technologie MRAM utilise des principes physiques notamment liés aux interactions magnétiques qui sont relativement peu étudiés en termes de sécurité du composant.
L'objet du travail de cette thèse est d'évaluer les potentielles faiblesses de sécurité pour cette technologie. En particulier la capacité de ce type de mémoire à garantir l'intégrité et la confidentialité des informations qui sont stockées a été étudiée. Ce travail est divisé en deux parties, une première partie est consacrée à l'analyse de la résistance des MRAM aux attaques physiques avec un focus tout particulier sur l'étude des effets des champs magnétiques sur l'écriture, la lecture et la rétention des données ainsi que les différentes solutions envisagées pour réduire ces effets. Une étude des effets de la température a également été réalisée. L'autre partie du travail porte sur l'étude des émissions électromagnétiques et l'analyse de plusieurs méthodes pour retrouver le poids de Hamming des données manipulées par la mémoire et de ce fait en extraire de potentiels secrets ou données sensibles.

Remerciements

Cette thèse CIFRE a été réalisée avec Crocus Technology et s'est déroulé à la fois au sein de ses locaux à Rousset et à Grenoble et dans le laboratoire systèmes et architectures sécurisées (SAS) du centre microélectronique de Provence (CMP) de Gardanne. Ce laboratoire regroupe un équipe mixte CEA-Tech et Mines de Saint Etienne et est dirigé par Bruno Robisson.

À l'issue de ces trois années, je me dois de remercier toutes celles et tous ceux qui ont permis à ce travail de thèse d'arriver à son terme dans les meilleures conditions.

En premier lieu, mes remerciements vont à Lionel Torres et à David Naccache pour avoir accepter d'être les rapporteurs de mon travail et pour l'intérêt qu'ils ont porté à mon travail. Je remercie également tout particulièrement Jean-Michel Portal, Anne-Lise Ribotta et Philippe Collot d'avoir acceptés d'être membre de mon jury de thèse.

Mes remerciements vont ensuite à Assia Tria qui a dirigé ces travaux, pour m'avoir donné l'opportunité d'effectuer ma thèse dans le laboratoire SAS et pour son aide pendant ces trois années, et plus spécialement pour la fin de thèse. Je suis également particulièrement reconnaissant pour sa relecture assidue et complète du manuscrit final qui m'a permis d'être plus serein lors de son envoie aux rapporteurs.

Je remercie aussi mes encadrants techniques de Crocus :

Bruno Mussard dont le soutien technique, organisationnel et matériel a été décisif. Je l'écris sans ironie, même si j'ai souvent râlé d'avoir à écrire des rapports hebdomadaires et des plannings, cela m'a permis de cadrer un peu mieux ce vaste projet de caractérisation des MRAM.

Et Ali Alaoui avec qui la plupart des bancs de tests ont été montés et utilisés, avec sa maitrise du VHDL et sa motivation, une partie non négligeable de cette thèse a pu être concrétisée.

Une pensée amicale également à tout ceux que j'ai côtoyé dans le laboratoire ou autour et qui ont participé à faire de ces trois ans une expérience enrichissante tant sur le plan professionnel que personnel, je pense notamment à Romain Wacquez, Jean-Baptiste Rigaud, Jean-Max Dutertre, Jacques Fournier, Driss Aboulkassimi, Amir-Pasha Mirbaha, Jean-Pierre Nikolovski, Philippe Maurine, Laurent Freund, Jérôme Quartana, Bruno Robisson, Michelle Gilet, Barbara Bruno et Bernard Dhalluin.

Mais aussi à tous mes collègues de Crocus, en particulier Christophe Gineste, Jérémie Clément, Julia Auffranc, Nathalie Vialle, Ken Macka, Lucien Lombard et Jeremy Herault.

Une mention spéciale à ceux qui m'ont supportés pendant mon travail, mes pauses café et autres apéros, David Cambon, Christian Cornesse, Alexis Krakovinski, Damien Jauvard, Maxime Lecomte, David Elbaze. Et aussi une mention super-spéciale à Jérémie Allais et Noémie Beringuier qui ont pris le temps de relire des versions alpha et pré-alpha de mon manuscrit, c'est long, ingrat et fatiguant

mais tellement utile.

Et enfin un grand merci à Marc, Ingrid, Nico, Loïc et bien sûr Zhao qui ont participé à faire de cette thèse un période inoubliable.

Table des matières

Liste des figures

Introduction générale

Les mémoires sont des dispositifs destinés à stocker de l'information et à la restituer à la demande. Les premiers objets remplissant ces fonctions datent de l'invention de l'écriture au IV^{ème} millénaire avant J.-C. [26]. Des murs d'une grotte aux livres papier en passant par les tablettes d'argile ou de cire de multiples supports ont été inventés. À l'ère de l'électronique, leurs fonctions ont évolué, l'information stockée n'est alors plus seulement destinée aux êtres humains, mais aussi à des systèmes automatisés. Les mémoires à semiconducteurs sont des dispositifs présents dans les circuits électroniques et microélectroniques depuis 1946 avec les tubes de Williams qui étaient les premières mémoires non mécaniques [49]. Elles sont aujourd'hui un élément incontournable de la plupart de ces systèmes.

Le marché des mémoires se divise actuellement entre deux technologies principales : les flash NAND et les DRAM qui représentaient à elles seules près de 90% de ce marché en 2010 [34]. Cependant, l'amélioration des performances de ces deux technologies demande de plus en plus d'efforts et d'investissements. Il existe néanmoins des technologies émergentes de mémoire aux performances très prometteuses.

C'est l'une d'elles, la Magnétorésistive Random Acccess Memory (MRAM), qui est étudiée dans de ce travail de thèse. Cette technologie est basée sur les variations de résistance d'empilements de matériaux magnétiques en fonction de leurs aimantations. Loin d'être un idée récente, le stockage sous forme magnétique était déjà utilisé dans les années 1950 avec les mémoires à tores magnétiques qui étaient la technologie dominante pendant plusieurs décennies. Ce type de mémoire était par exemple utilisé dans les supercalculateurs CDC6600 [19]. Ces mémoires ont cependant été remplacées dans les années 1970 par les DRAM qui, bien que volatiles, permettaient une densité de stockage plus importante puisqu'elles n'utilisaient qu'un transistor et un condensateur et pouvaient facilement être utilisées sur des circuits intégrés. Les mémoires magnétiques sont revenues sur le devant de la scène dans les années 1990, jusqu'à la première MRAM vendue en 2006 par Freescale. Aujourd'hui de nombreux fabricants et laboratoires de recherche travaillent au développement de cette technologie pour des applications dans de multiples domaines. On peut citer par exemple Toshiba qui développe un microprocesseur basé sur une mémoire cache en STT-MRAM [48], Buffalo qui utilise des STT-MRAM de Everspin comme RAM dans des disques SSD [47] ou encore des recherches dans le laboratoire LIRMM pour l'intégration de TAS-MRAM dans des architectures de FPGA [31].

Les MRAM étudiées sont des TAS-MRAM (pour Thermally Assisted Switching MRAM), il s'agit d'une évolution de celles développées par Freescale. Elles utilisent un processus d'écriture qui permet d'améliorer la robustesse et de réduire la taille des cellules en les chauffant lors de l'écriture. Ces mémoires sont développées par Crocus Technology, qui a initié et encadré ce travail de recherche.

Avec l'augmentation du nombre d'objets connectés utilisés quotidiennement, la

sécurité des composants électroniques est devenue une contrainte majeure, au même titre que la consommation ou la surface de ces circuits. Et cette nouvelle technologie de mémoire pourrait a priori limiter les effets de certaines attaques comme les attaques par impulsions laser. Le travail effectué durant cette thèse consiste à évaluer la robustesse de la technologie TAS-MRAM face aux attaques physiques connues, et face à d'éventuelles attaques qui pourraient tirer profit de faiblesses spécifiques aux MRAM et à imaginer le cas échéant des techniques pour limiter l'efficacité des attaques identifiées.

Aussi le *chapitre 1* présentera succinctement les technologies mémoires utilisées ainsi que les mémoires actuellement en développement. Puis la technologie MRAM sera présentée, depuis les bases du micromagnétisme jusqu'aux diverses architectures de mémoires. Un tour d'horizon des enjeux de la sécurité des composants électroniques sera effectué, et enfin les bancs de tests et les échantillons utilisés seront présentés.

Le *chapitre 2* présentera l'analyse des émissions électromagnétiques d'une mémoire MRAM de Crocus Technology, l'étude porte plus particulièrement sur plusieurs méthodes visant à retrouver les poids de Hamming des données écrites dans la mémoire. Deux types d'approches sont développées : une analyse supervisée, avec l'hypothèse d'un attaquant qui dispose d'un composant de référence complètement ouvert pour effectuer des analyses préliminaires et une analyse non supervisée qui suppose un attaquant qui ne connait pas le détail du fonctionnement la mémoire.

Le *chapitre 3* présentera une analyse d'un des points faibles identifiés de la technologie MRAM, à savoir les effets des champs magnétiques sur les opérations de la mémoire. L'étude du comportement de la mémoire dans un environnement soumis à de forts champs magnétiques statiques est un enjeu à la fois de sécurité matérielle et de fiabilité. En effet si le fonctionnement de la mémoire peut être garanti dans ce type d'environnement, de nouveaux champs d'applications s'ouvrent alors. Pour cette raison, différents moyens pour limiter les effets de ces perturbations seront étudiés et comparés.

Le *chapitre 4* portera sur les autres types d'attaques physiques qui ont été expérimentées sur les MRAM pendant cette thèse. En premier lieu les attaques par impulsions électromagnétiques seront étudiées. Contrairement aux champs magnétiques statiques du *chapitre 3*, ces impulsions permettent une meilleure précision temporelle et spatiale et donc des attaques beaucoup plus ciblées. Ces attaques ont cependant la particularité de ne pas seulement perturber les cellules MRAM, elles perturbent aussi les blocs logiques de contrôle de la mémoire. Elles nécessitent donc une analyse approfondie du composant pour obtenir des effets exploitables.
En second lieu, une analyse des effets combinés des hautes températures et de champs magnétiques sur les TAS-MRAM sera effectuée.

Une dernière partie conclura ce travail et présentera les perspectives ouvertes l'issue de ces recherches.

Chapitre 1

État de l'art et contexte

Sommaire

Cet état de l'art va permettre de mettre en place la plupart des éléments nécessaires à la compréhension de ce manuscrit. Dans un premier temps, la technologie des mémoires magnétiques (Magnetic Random Access Memory - MRAM) sera détaillée et positionnée au regard du marché actuel des mémoires à semiconducteur. Il existe plusieurs technologies mémoires avec des performances et des degrés de maturité divers. Elles seront comparées dans ce chapitre, leurs points forts et leurs points faibles seront mis en évidence ainsi que pour les moins matures, leur potentiel pour devenir d'ici à quelques années des acteurs importants du domaine. Ensuite l'accent sera mis sur la compréhension des MRAM et des interactions magnétiques nécessaires à leur fonctionnement. Une dernière partie sera consacrée à la présentation des différents bancs de caractérisation sécuritaire et des échantillons testés lors des expérimentations présentées dans ce travail.

1.1 État de l'art des technologies mémoires

Les mémoires représentent aujourd'hui une part importante du marché des semiconducteurs, en 2013 elles représentaient 21% des revenus de cette industrie [66,67]. Elles sont classées en deux grandes familles (figure 1.1) : les mémoires volatiles dont les données disparaissent en l'absence d'alimentation et les mémoires non volatiles qui les conservent. Les performances des mémoires sont comparées selon de multiples critères dont on peut citer :

- l'endurance : elle correspond au nombre de cycles de lecture/écriture maximum que peut supporter la mémoire avant que la fiabilité de la mémoire ne soit plus garantie
- la surface : elle est usuellement exprimée en F^2, qui est définie par le carré de la largeur de grille minimum de la technologie utilisée. Cette notation permet de s'affranchir du nœud technologique utilisé.
- le temps d'accès en lecture et en écriture.
- la consommation d'énergie, que ce soit, en lecture, écriture ou en veille.
- le prix en $/Gb.

Le tableau 1.1 résume ces caractéristiques principales pour chaque technologie de mémoire. Ces caractéristiques seront expliquées plus en détail dans la suite de ce chapitre.

	Mémoires Emergentes			Mémoires Matures		
	MRAM/STT MRAM	PCRAM	RRAM	FRAM	DRAM	Flash NAND
Non Volatile	OUI	OUI	OUI	OUI	NON	OUI
Endurance (Nb de cycles)	Haut (10^{15})	Moyen (10^{8})	Moyen (10^{8})	Haut (10^{12})	Haut (10^{15})	Bas (10^{5})
Dernier Nœud technologique (2013)	90 nm	45 nm	130 nm	130 nm	30 nm	20 nm
Surface de la cellule (F^2)	Importante/ Moyenne (6-40)	Moyenne (6-12)	Moyenne (6-12)	Importante (15-20)	Faible (6-10)	Très Faible (4)
Vitesse d'écriture (ns)	Rapide (10ns)	Moyenne (75ns)	Moyenne (75ns)	Moyenne (100ns)	Rapide (10ns)	Lente (10000 ns)
Consommation	Importante/Faible	Faible	Faible	Faible	Faible	Très Importante
Prix en $/GB (2013)	Important (1000 - 100$/GB)	Moyen (qq $/GB)	Important (10000$/GB)	Important (1 000$/GB)	Faible (1$/GB)	Très Faible (0,1$/GB)

TABLE 1.1 – Comparaison des performances des différents types de mémoires [17]

Mémoires Volatiles

Bien que les mémoires volatiles nécessitent une alimentation permanente afin de conserver leurs données, celles-ci offrent en contrepartie des avantages en terme des temps d'accès en écriture de 100 à 1000 fois plus faibles comparées à leurs équivalents non volatiles. Pour un système utilisant un microprocesseur, les premiers niveaux de hiérarchie mémoire sont constitués de mémoires volatiles. En particulier, les SRAM et les DRAM dont nous allons détailler le fonctionnement, sont utilisées respectivement dans les niveaux de cache 1 et 2 et dans la mémoire centrale.

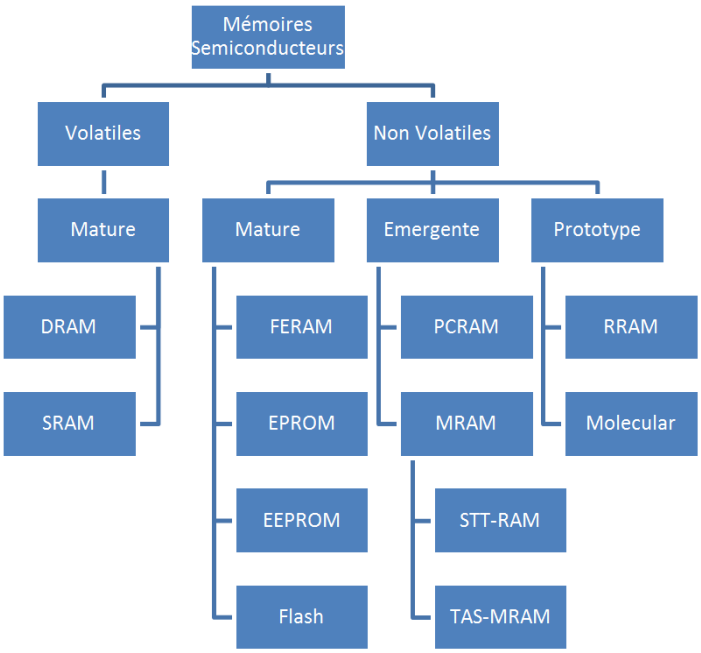

FIGURE 1.1 – Taxinomie des mémoires

SRAM

La SRAM ou Static Random Access Memory (figure 1.2) est une mémoire constituée uniquement de transistors. Dans sa forme la plus simple, une cellule mémoire SRAM élémentaire représentative d'un bit est constituée de deux inverseurs qui forment une bascule bistable et de deux transistors de sélection soit six transistors au total(SRAM 6T). Sa surface est relativement importante en raison du nombre de transistors qui la compose (minimum 6), elle est comprise entre 6 et 10 F^2, cet inconvénient est compensé par des temps d'accès en écriture et en lecture très faibles de l'ordre de la dizaine de nanosecondes. Elle est contrôlée par deux signaux, BL (Bit Line) et $\overline{\text{BL}}$ son complémentaire et par la *word line* (WL). La donnée est conservée dans la cellule tant que les inverseurs sont alimentés.

— Opération d'écriture : Les deux transistors de sélection sont ouverts et les lignes BL et $\overline{\text{BL}}$ envoient deux signaux complémentaires aux inverseurs forçant ainsi le système dans l'état stable désiré, '1' ou '0'.

— Opération de lecture : Les lignes BL et $\overline{\text{BL}}$ sont préchargées et les transistors de sélection sont ouverts propageant ainsi l'état de la bascule dans les deux lignes. Une chute de tension est alors mesurée sur une des deux lignes permettant de déterminer l'état de la cellule '1' ou '0'.

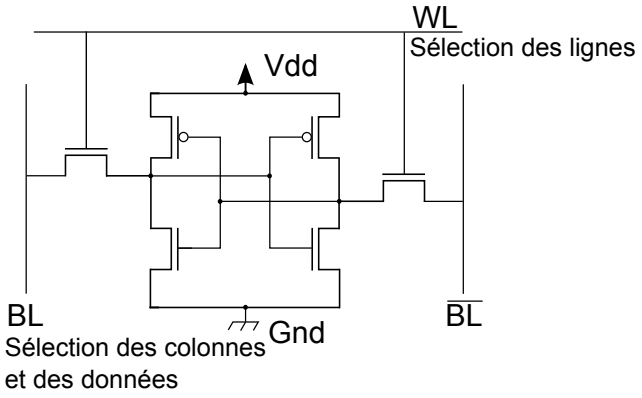

FIGURE 1.2 – Schéma d'une cellule SRAM

DRAM

La DRAM ou Dynamic Random Access Memory (figure 1.3) est à ce jour la mémoire la plus dense, en effet chaque bit d'une cellule mémoire de DRAM est constitué d'un transistor et d'un condensateur (DRAM 1T/1C).Le condensateur détermine la valeur du bit, le transistor quant à lui permet de sélectionner le bit. La cellule élémentaire ou point mémoire occupe une surface de l'ordre de $4F^2$. Ces mémoires sont utilisées comme mémoires vives des processeurs en raison de leur ratio vitesse/densité, leur principal inconvénient est une consommation élevée.

Le condensateur a une tendance naturelle à se décharger, pour que l'information perdure il est alors nécessaire de réaliser un rafraichissement via un cycle de lecture/écriture environ toutes les 50 ms suivant les types de DRAM. Les mémoires DRAM ont par conséquent une consommation d'énergie importante en particulier en mode veille (*stand by*) due à ce rafraichissement qui est de l'ordre de 2 mA pour 512Mbits [32].

— Opération d'écriture : l'écriture d'une donnée correspond à la charge ou décharge du condensateur. Pour cela le transistor de sélection est ouvert par le signal WL et la donnée est envoyée sur la BL qui est connectée soit à Vdd soit à la masse pour écrire respectivement un '1' ou un '0'.

— Opération de lecture : Le transistor de sélection est ouvert et la variation de tension aux bornes du condensateur est propagée dans la ligne BL. Cette opération décharge le condensateur et la cellule mémoire doit être réécrite pour une lecture ultérieure.

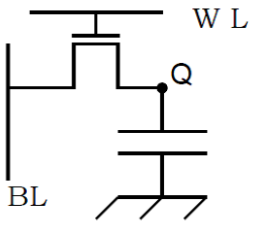

FIGURE 1.3 – Une cellule DRAM

Mémoires Non Volatiles

Les mémoires non volatiles, contrairement aux mémoires volatiles, conservent les données écrites même en l'absence d'alimentation. Leurs performances en termes de temps d'accès sont globalement plus faibles que les mémoires volatiles, mais comme elles ne nécessitent pas d'alimentation pour conserver les données, ces mémoires sont utilisées pour stockage de masse ou des programmes qui ont besoin d'être conservés même hors tension.

Mémoire Matures

Historiquement, les premières mémoires non volatiles à semiconducteurs ne pouvaient qu'être lues, les cellules étant programmées de manière définitive lors de la fabrication pour les ROM. À partir des années 60 les mémoires PROM, permettait un accès en écriture directement par l'utilisateur en effet les mémoires PROM sont équivalentes à des fusibles pouvant être claqués en appliquant une tension de l'ordre de 12 V sur les points mémoires sélectionnés. Si le fusible est grillé, le bit est à l'état '1', sinon il est à l'état '0'. En 1970 apparaissent les premières mémoires EPROM, ce sont des PROM effaçables en présence de rayons UV. Les fusibles sont reconstitués, mais cela nécessite un processus long d'insolation (3-4 minutes) et global (toute la mémoire est effacée) [20]. Les mémoires EEPROM quant à elles sont des mémoires PROM effaçables et programmables par un simple courant électrique, elles sont concurrencées depuis 1980 par les mémoires flash, qui sont plus rapides. La principale différence entre les deux technologies est la manière dont les données sont effacées.

EEPROM Les EEPROM ou Electrically Erasable Programmable ROM (figure 1.4) sont des mémoires non volatiles à base de transistors à grille flottante. Contrairement aux mémoires plus anciennes, elles sont reprogrammables dynamiquement. La donnée est stockée dans la grille flottante du transistor sous forme de charges. L'écriture et l'effacement des données dans les cellules EEPROM demandent des tensions importantes ce qui fragilise les jonctions après un nombre trop important d'opérations et limite l'endurance de ces mémoires.

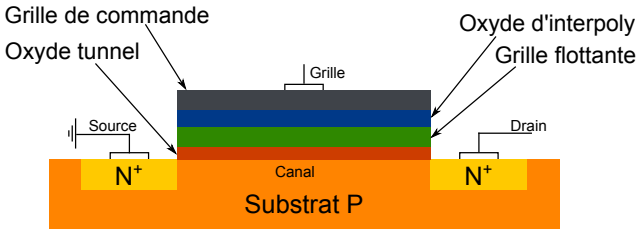

FIGURE 1.4 – Transistor à grille flottante

— Opération d'écriture : En appliquant une tension élevée sur la grille de la cellule (environ 12V [20]), les électrons transitent à travers l'oxyde mince dans la grille flottante (par effet tunnel depuis le drain) ce qui a pour effet d'augmenter la tension de seuil.
— Opération de lecture : Le transistor à grille flottante est bloqué si la grille flottante est chargée. Il est passant si la grille flottante est déchargée. Cela permet de différencier deux états, '0' et les '1'.
— Opération d'effacement : Pour effacer une donnée, il faut décharger la grille flottante des électrons précédemment piégés. Pour cela une tension élevée est appliquée sur le drain, la tension de seuil diminue alors pour atteindre son niveau précédent [39].

Les EEPROM sont aujourd'hui beaucoup moins utilisées, elles ont été remplacées par les flashs dans la plupart des applications. La mémoire flash utilise une cellule de base MOS possédant une grille flottante, deux mécanismes sont utilisées pour faire transiter les électrons à travers l'oxyde mince : l'effet tunnel, comme pour les EEPROM et l'injection d'électrons chauds pour l'effacement. L'effacement des mémoires flash n'est possible que pour la totalité de la mémoire ou par secteur.

Flash La mémoire flash est aujourd'hui la technologie mémoire la plus utilisée. Il en existe deux types, les flashs NOR et les flashs NAND (figures 1.5 et 1.6) qui sont en fait deux architectures différentes de la même cellule mémoire.
Les flashs NOR ont été inventées en 1980 par Toshiba puis ont été commercialisées par Intel en 1988. Il s'agit d'une architecture parallèle où chaque cellule est à l'intersection d'une ligne et d'une colonne ce qui permet de les adresser individuellement en lecture et en écriture. Cependant, cette architecture occupe une surface plus importante en comparaison d'une architecture NAND. Elle est principalement utilisée pour le stockage de programme en raison de ses accès rapides. Mais le surplus de surface et le coût des flashs NOR limitent leurs utilisations aux applications les plus critiques.

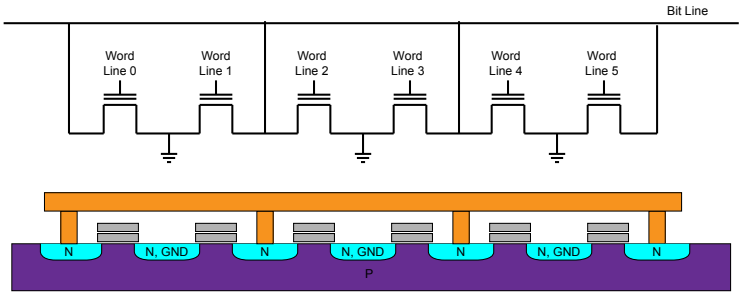

FIGURE 1.5 – Architecture Flash NOR

Les flashs NAND ont été développées quelques années après les flashs NOR, en 1989 par Toshiba. Contrairement à la NOR l'écriture ne se fait pas bit à bit,

mais par blocs. Les cellules sont adressées en série ce qui permet un gain de surface important en passant d'une cellule d'une surface occupée de 10 F^2 à 4 F^2, mais ne permet plus un accès aléatoire. Cette architecture est donc utilisée pour le stockage de données.

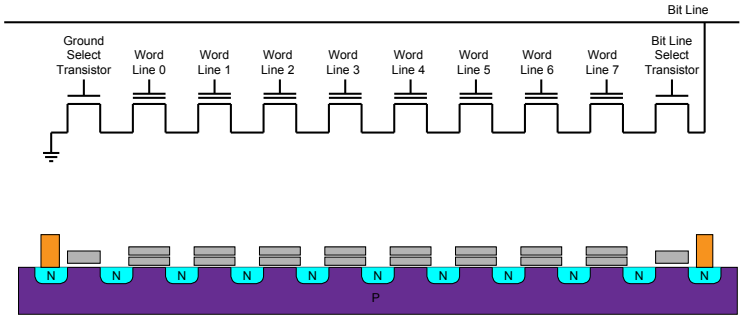

FIGURE 1.6 – Architecture Flash NAND

FeRAM La FeRAM ou ferroélectrique RAM est très similaire à la DRAM dans son fonctionnement. Son développement a débuté en 1984, mais des coûts de production encore très élevés et des problèmes de fiabilité l'empêchent d'être un acteur important du marché des mémoires non volatiles. La recherche sur cette technologie de mémoire a par ailleurs beaucoup diminué ces dernières années au profit d'autres types de mémoires non volatile émergentes [17].

Le point mémoire élémentaire d'une FeRAM est composée d'un transistor et d'un condensateur (1T-1C), mais la grande différence est que ce condensateur est ferroélectrique et ne nécessite pas d'être rafraichi pour conserver la donnée stockée.

Le condensateur ferroélectrique est un cristal à deux états stables (figure 1.7) qui sont définis par deux configurations cristallines. L'atome central peut se trouver dans deux positions différentes correspondant à deux états d'énergie haut ou bas. Pour passer d'une configuration à l'autre, un champ électrique est appliqué, modifiant ainsi la position de l'atome central. Cette transition produit de l'énergie sous forme d'une charge. Pour que la structure retrouve sa position initiale, un champ électrique opposé doit être appliqué.

Pour mesurer l'état d'une cellule FeRAM un champ électrique est appliqué, s'il provoque un changement de configuration cristalline une charge est libérée et peut être détectée. À l'instar de la DRAM, la lecture efface la donnée écrite. Cependant, contrairement aux condensateurs à semiconducteur, les condensateurs ferroélectriques ont l'avantage de ne pas avoir de fuite de courant. La charge reste donc constante et n'a pas besoin d'être rafraichie, ce qui limite considérablement la consommation et permet aux données d'être conservées même hors tension [68].

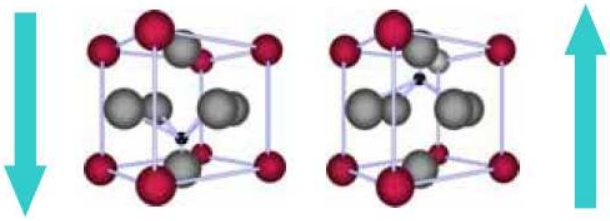

FIGURE 1.7 – Les deux configurations cristallines du condensateur ferroélectrique d'une FeRAM

Mémoires émergentes

Aujourd'hui tous les types de mémoires sont conçus et optimisés pour un certain type d'application, cependant pour la plupart des applications plusieurs technologies de mémoires complémentaires sont combinées. De ce fait, de nouvelles technologies de mémoire sont en cours de développement pour obtenir à terme une mémoire universelle.
Parmi ces technologies certaines telles que les MRAM sont déjà commercialisées dans des volumes relativement faibles [29], tandis que d'autres existent seulement à l'état de prototype [18]. Toutes ont pour point commun de promettre des performances très intéressantes comparées aux mémoires dites matures, mais elles ne sont pas encore suffisamment fiables ou économiquement rentables pour les concurrencer véritablement, comme illustré dans le tableau 1.1.

PCRAM La PCRAM ou Phase Change RAM est un type de mémoire basé sur la propriété de certains matériaux à passer d'une structure cristalline à une structure amorphe, sous l'effet de la chaleur (figure 1.8). Cette propriété est connue et utilisée en optique depuis 1968 [53], aujourd'hui elle est utilisée pour les disques réinscriptibles. Entre l'état cristallin et l'état amorphe la réflexion est différente ce qui permet de stocker et lire les données. Dans le cas de la PCRAM, c'est la différence de résistivité entre les états amorphe et cristallin qui permet de distinguer un '1' stocké d'un '0'. Les principaux fournisseurs de PCRAM ont opté pour un alliage de verre à chalcogénure, le GST ($Ge_2Sb_2Te_5$) [15].

Comme le montre la figure 1.8, il y a deux températures critiques pour les PCRAM, la température de fusion d'environ 600°C au-delà de laquelle le GST passe en phase amorphe, et la température de cristallisation d'environ 300°C à laquelle le GST devient cristallin après une dizaine de nanosecondes. Lors des opérations d'écriture, le GST est chauffé à l'une de ces deux températures [59].

La résistivité de l'état amorphe est de l'ordre de 10 Ω.cm tandis que celle de l'état cristallin est de 10 mΩ.cm, cette différence apporte une importante stabilité aux données. De plus, dans la mesure où il n'y a pas de charge électrique impliquée dans la rétention des données, ce type de mémoire est intrinsèquement immunisé aux

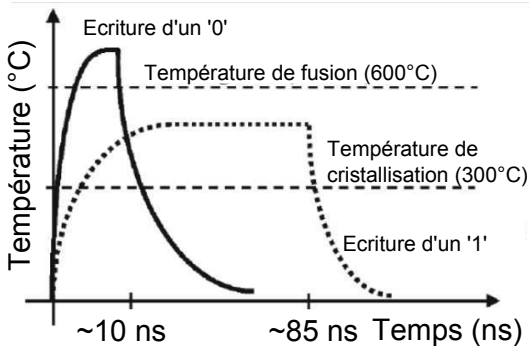

FIGURE 1.8 – Changement de phase dans une PCRAM

radiations ce qui facilite les applications notamment pour l'industrie aéronautique et spatiale. En revanche l'opération de *reset*, nécessite d'atteindre une température de l'ordre de 600°C ce qui induit un courant important et qui augmente le bruit thermique entre les cellules : ce sont deux facteurs encore limitants pour les PCRAM.

RRAM Les mémoires RRAM (ou ReRAM) pour Resistive RAM sont basées sur le changement de résistance par la création ou dissolution de filament conducteur au travers d'une couche isolante (figure 1.9). Un empilement RRAM est composé de deux électrodes séparées par un isolant diélectrique, dans la plupart des cas un TMO (transition metal oxyde). Il existe trois types principaux de RRAM :

— Les CBRAM (Conductive-Bridge RAM) dont le principe est basé sur une réaction d'oxydoréduction. Sous l'influence d'un courant d'électrons depuis la cathode, un dépôt d'ions métalliques se forme dans la couche isolante (un verre de chalcogénure) entre l'anode et la cathode créant un pont conducteur. La quantité d'ions déposés et donc la conductivité de l'empilement dépend de l'intensité du courant. En appliquant un courant de la cathode vers l'anode, le pont est dissout [70].
— Les VCM (Valence Change Memory) pour lesquelles le courant dans les électrodes va créer des lacunes en oxygène dans le réseau cristallin de la couche entre les deux électrodes (typiquement $SrTiO_3$), cela a pour effet de changer la conductivité de cette couche. [72]
— Les TCM (Thermo Chemical Memory) où l'effet joule provoqué par le courant dans les électrodes provoque une réaction d'oxydoréduction qui crée un filament conducteur ; pour l'opération de *reset* de la cellule le même courant est utilisé. Le filament étant plus conducteur que l'isolant, le courant est concentré à l'intérieur de celui-ci qui se dissout par effet thermique. Contrairement aux autres RRAM, la TCM est dite unipolaire, c'est-à-dire que l'écriture et la lecture sont faites en appliquant un courant de même signe.

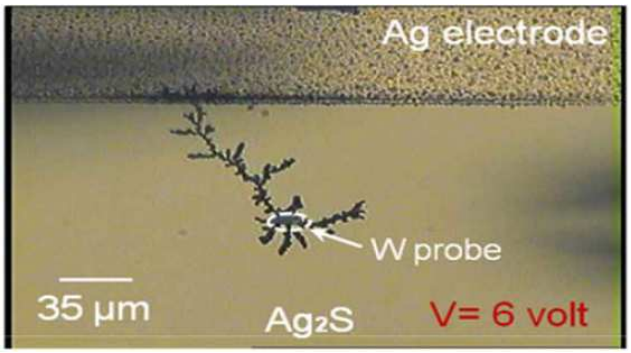

FIGURE 1.9 – Pont conducteur dans une CBRAM

Pour chacune de ces trois technologies le principe est le même, une opération de formation du pont conducteur est effectuée avant la première écriture, l'opération de *reset* ou dissolution du pont n'est jamais complet. Les écritures suivantes nécessitent alors un courant plus faible pour combler l'isolant entre les deux parties du pont précédemment formé. Ces mémoires sont très denses, elles utilisent une architecture 1T/1R voire 1R dans certains cas (avec simplement une matrice de sélection).

1.2 Du Spin à la MRAM

Dans ce travail de thèse, l'accent est porté sur les composants autonomes/autosuffisants de mémoires MRAM et des attaques physiques auxquels ils sont sensibles. Cependant pour pouvoir comprendre, prédire et prévenir les effets de ces attaques il est nécessaire de plonger au cœur de la matière et d'appréhender les interactions entre les différents éléments composant une MRAM. C'est l'objet de la section suivante.

Notions de micromagnétisme

Les bases du magnétisme

Le caractère magnétique d'un matériau est défini par le moment magnétique des électrons gravitant autour de ses atomes. Les électrons apportent deux contributions à l'aimantation, le moment magnétique angulaire et le moment magnétique intrinsèque ou spin. Le moment magnétique angulaire est nul si l'atome n'est pas en mouvement et sera négligé par la suite (tous les éléments dans les systèmes étudiés étant immobiles les uns par rapport aux autres). Les électrons remplissent les couches énergétiques du nuage électronique selon les règles de Pauli et de Hund [54], si une couche est pleine les spins s'équilibrent et leurs contributions sont nulles. La seule contribution vient des couches et sous-couches non pleines. Le moment magnétique d'un atome est égal à la somme des contributions de ses électrons.

Le moment magnétique d'un solide dépend de l'interaction entre les moments magnétiques des atomes qui le compose, on peut définir l'énergie d'échange entre deux atomes voisins comme :

$$E_{ij} = -J\vec{m}_i.\vec{m}_j \tag{1.1}$$

Avec $\vec{m}_i$ et $\vec{m}_j$ moments magnétiques de deux atomes voisins directs et J la constante d'échange dont le signe définit la nature magnétique du matériau.

Si J est positive, le matériau est dit ferromagnétique (figure 1.10), l'énergie d'échange est minimale avec tous les moments magnétiques parallèles. Leur contribution globale est donc non nulle et le matériau a une aimantation.

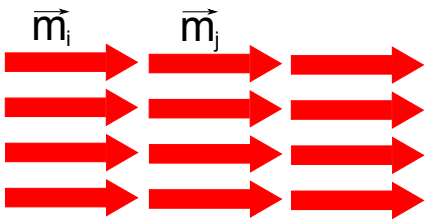

FIGURE 1.10 – Moment magnétique d'un matériau ferromagnétique

Si J est négative et si les moments magnétiques sont tous égaux, le matériau est dit antiferromagnétique (figure 1.11), l'énergie d'échange est minimale avec le moment magnétique des atomes voisins dans des directions opposées. Leur contribution globale est donc nulle et le matériau n'a pas d'aimantation.

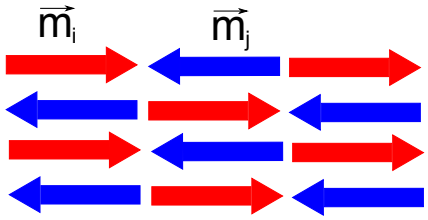

FIGURE 1.11 – Moment magnétique d'un matériau antiferromagnétique

Si J est négative avec des moments magnétiques différents entre les atomes, le matériau est dit ferrimagnétique (figure 1.12), l'énergie d'échange est minimale avec le moment magnétique des atomes voisins dans des directions opposées, mais la contribution globale est non nulle car due aux différences entre les moments magnétiques.

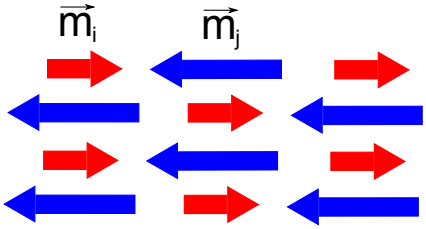

FIGURE 1.12 – Moment magnétique d'un matériau ferrimagnétique

L'aimantation d'un matériau est définie comme la contribution globale des moments magnétiques des atomes qui le composent :

$$\vec{M} = \frac{d\vec{m}}{dV}$$

Avec $\vec{m}$ le moment magnétique d'un électron et V le volume considéré.

Les énergies d'aimantation

Si on peut parler d'un vecteur d'aimantation d'un point de vue macroscopique, au niveau local de nombreuses interactions sont mises en jeu dans un système magnétique. Celles-ci produisent des changements au niveau des orientations locales du champ magnétique. En considérant l'énergie totale d'un système magnétique, on

peux compter quatre contributions énergétiques : l'énergie d'échange E_{ex}, l'énergie d'anisotropie magnétocristalline E_u, l'énergie dipolaire E_{dip} et l'énergie de Zeeman E_z.
L'énergie totale du système est alors :

$$E = E_{ex} + E_u + E_{dip} + E_z \tag{1.2}$$

D'où le champ effectif de ces quatre contributions :

$$\vec{H}_{eff} = -\vec{\nabla}_{\vec{M}} E = \vec{H}_{ex} + \vec{H}_{dip} + \vec{H}_u + \vec{H}_{Zeeman} \tag{1.3}$$

— Énergie d'échange
L'énergie d'échange d'un système à n spins est définie par :

$$E_{ex} = -\frac{1}{2}.\sum_{i=1}^{n}\sum_{j=1}^{n} J_{ij}.(\vec{m}_i.\vec{m}_j) \tag{1.4}$$

Avec J_{ij} la constante d'échange (positive dans un système ferromagnétique) qui représente l'intégrale de l'échange correspondant aux interactions entre les moments magnétiques i et j. Cette interaction est plus importante pour les moments adjacents. Elle favorise les alignements parallèles des spins dans les matériaux ferromagnétiques.

— Énergie d'anisotropie magnétocristalline

À cause des interactions entre le moment magnétique et le réseau cristallin à travers les interactions spin-orbitales, l'orientation du moment magnétique a des directions préférentielles en fonction des symétries du réseau. Le décalage entre le moment magnétique et ces directions préférentielles augmente l'énergie du système, c'est l'énergie magnétocristalline d'anisotropie :

$$E_u = K_u.|1 - \left(\vec{u}.\frac{\vec{M}}{M_s}\right)^2| \tag{1.5}$$

Avec $\vec{u}$ vecteur unitaire dans la direction de l'axe de l'anisotropie (axe dit "facile"), K_u la constante anisotropique d'énergie et $\vec{M}/M_s$ le vecteur d'aimantation uniformisé. On peut en déduire le champ magnétique d'anisotropie en fonction de la direction du vecteur d'aimantation :

$$\vec{H_u} = \frac{2K_u}{\mu_0.M_s}.(\vec{u}.\frac{\vec{M}}{M_s}).\vec{u} \tag{1.6}$$

— Énergie dipolaire

Pour un échantillon uniformément magnétisé, des pôles magnétiques apparaissent à la surface, donnant naissance à un champ démagnétisant $\vec{H_d}$, l'énergie correspondante s'exprime par :

$$E_{dip} = -\frac{1}{2}.\int_V \vec{M}(\vec{r}).\vec{H_d}(\vec{r}).d\vec{r} \tag{1.7}$$

Cette énergie est faible comparée à l'énergie d'échange entre les moments voisins : elle n'intervient donc pas directement dans l'alignement parallèle des spins voisins. En revanche, sa portée plus grande va influencer la géométrie des lignes de champ. De façon similaire on peut en déduire le champ démagnétisant correspondant :

$$\vec{H_d} = -\overline{\overline{N}}.\vec{M} \tag{1.8}$$

Avec $\overline{\overline{N}}$, le tenseur de démagnétisation qui est généralement fonction de la position $\overline{\overline{N}}(\vec{r})$. Dans un échantillon magnétisé de manière homogène, le champ de démagnétisation est opposé au vecteur $\vec{M}$ et le tenseur $\overline{\overline{N}}$ est alors :

$$\overline{\overline{N}} = \begin{vmatrix} N_x & 0 & 0 \\ 0 & N_y & 0 \\ 0 & 0 & N_z \end{vmatrix} \text{ avec } N_x + N_y + N_z = 1 \tag{1.9}$$

L'énergie de démagnétisation provoque une distribution non uniforme de l'aimantation et la création de domaines magnétiques [37] ce qui a pour effet de limiter les charges volumiques et surfaciques.

— Énergie de Zeeman

L'énergie créée par l'interaction entre l'aimantation et le champ magnétique externe est appelée énergie de Zeeman :

$$E_{Zeeman} = -\mu_0 \vec{M}.\vec{H_{ex}} \tag{1.10}$$

Pour minimiser cette énergie, l'aimantation du système a tendance à s'aligner avec le champ extérieur. Si le champ extérieur est assez important pour que cette énergie surpasse toutes les autres, tous les moments magnétiques vont s'aligner avec celui-ci, l'aimantation du matériau est alors maximale. Cette aimantation est appelée aimantation de saturation, notée M_s. Cependant, la valeur de cette aimantation de saturation n'est valable que pour des températures relativement faibles. Au-delà d'une certaine température T_c, ou température de Curie, la valeur de l'aimantation de saturation décroit, l'agitation thermique rend les moments magnétiques désordonnés et le matériau change alors de phase (figure 1.13). Il devient alors paramagnétique, c'est-à-dire que l'alignement désordonné des moments magnétiques ne permet plus d'avoir une aimantation globale non nulle.

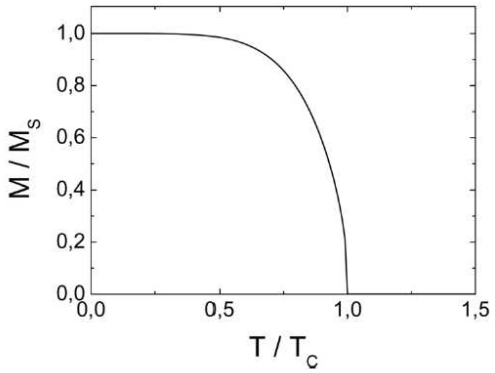

FIGURE 1.13 – Effet de la température sur l'aimantation de saturation

La connaissance de toutes les énergies magnétiques qui régissent l'aimantation des couches magnétiques permet de déterminer le champ effectif associé qui correspond au champ créé par la somme de leurs influences. De ce champ effectif Landau et Lifshitz ont proposé une équation de l'évolution de l'aimantation dans le temps et l'espace, cette équation a été améliorée par Gilbert en 1955 [3] pour donner l'équation de Landau-Lifshitz-Gilbert (LLG) :

$$\frac{\partial \vec{M}}{\partial t} = -\gamma \left(\vec{M}.\mu_0 \vec{H}_{eff} \right) + \frac{\alpha}{M_s} \left(\vec{M} \frac{\partial \vec{M}}{\partial t} \right) \tag{1.11}$$

Avec $\gamma = g\frac{e}{2m_e}$ et α la constante d'amortissement, strictement positive. Cette équation permet de calculer la dynamique de retournement des moments magnétiques.

Magnetorésistance tunnel et magnetorésistance géante

La spintronique est une branche de l'électronique qui utilise les propriétés du spin des électrons. Elle est issue de la découverte par Michel Julliere en 1975 de la magnétorésistance tunnel (TMR) [35], mais la discipline a réellement pris de l'importance suite au travaux d'Albert Fert sur la magnétorésistance géante (GMR) en 1988 [5].
Un électron est caractérisé par sa masse, sa charge et son spin. Là où l'électronique agit sur la charge de l'électron, la spintronique agit sur le spin. Les électrons sont alors contrôlés par l'action de champs magnétiques ou de courants polarisés en spin. Dans le cas des MRAM, les propriétés des spins sont utilisées dans les jonctions tunnel magnétiques qui constituent l'élément de stockage. Une jonction tunnel magnétique est composée d'un empilement de matériaux dont la résistance globale varie en fonction de l'orientation relative des spins des électrons de ses couches. Les matériaux utilisés, le nombre et l'épaisseur des couches déterminent ses performances.

Lorsque des électrons traversent un matériau ferromagnétique, ils sont filtrés. Ceux dont le spin est parallèle avec le spin des électrons du matériau le traversent, mais ceux qui ont un spin opposé sont réfléchis : c'est le principe de base de la GMR. Ce phénomène a été mis en évidence par deux équipes en parallèle, celles d'Albert Fert et de Peter Grünberg en 1986, qui leur a valu à tous deux le prix Nobel de physique en 2007.

Deux couches de matériau ferromagnétique sont séparées par une fine couche de matériau non magnétique (par exemple Fe/Cr/Fe). Les deux couches ont une aimantation plane (dans le plan de la couche). Ainsi, la première couche filtre le courant en ne gardant que les électrons de moments magnétiques parallèles à ceux de la couche ferromagnétique. Ces électrons passent dans la couche non magnétique, qui polarise le courant. En effet, le courant qui circule dans la couche non magnétique sera composé d'électrons dont le spin est identique à ceux des électrons de la première couche ferromagnétique. Le courant est à nouveau filtré au passage dans la seconde couche ferromagnétique. Si les moments magnétiques dans les couches sont alignés, la conductance de l'empilement est élevée, si elles sont anti-alignées, la conductance est plus faible comme montré dans la figure 1.14, ce phénomène est appelé magnétorésistance. Albert Fert and al [5] ont conduit des expérimentations et ont réussi à obtenir un écart de résistance d'environ 20% entre l'état parallèle et antiparallèle, les résultats de la publication originale sont illustrés dans la figure 1.15.

La TMR, magnetorésistance tunnel, a été mise en évidence par Michel Jullière en 1975. Il a observé une variation de la conductance électrique en fonction de l'orientation relative des couches magnétiques dans un empilement de $Fe/Gr/Fe$, cette variation est due à l'existence d'un courant tunnel à travers la barrière de germanium. Le changement relatif de résistance est de l'ordre de 2.7% pour une jonction à une température de 4.2K.

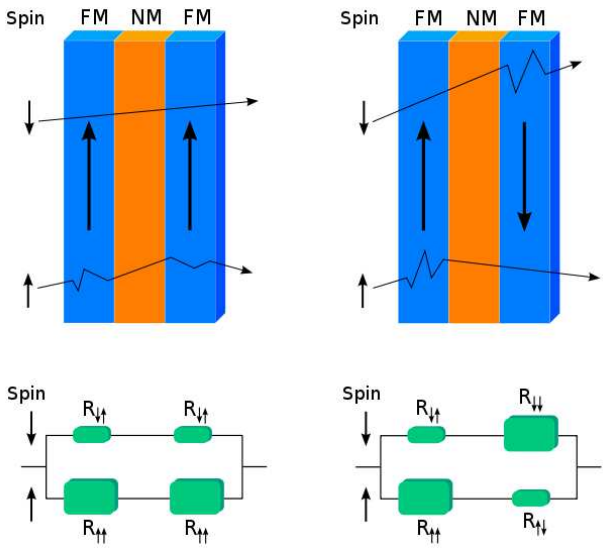

FIGURE 1.14 – Variation de la résistance en fonction de l'orientation relative du spin des électron des couches de l'empilement

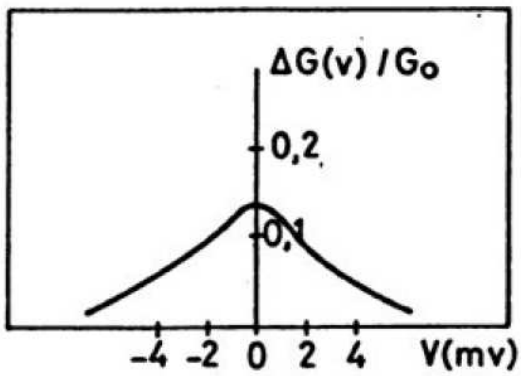

FIGURE 1.15 – Conductance relative d'un empilement Fe/Cr/Fe en fonction de la tension appliquée [35]

À la différence de la magnétorésistance géante pour laquelle un métal sépare deux électrodes ferromagnétiques, la couche de séparation est dans le cas de la magnetorésistance tunnel un isolant.
La publication de Jullière n'attira pas beaucoup l'attention à sa parution, cependant en 1995 la TMR a connu un regain d'intérêt avec la mise en évidence du même phénomène à température ambiante avec un empilement $Co/Al_2O_3/NiFe$ [43] puis avec l'utilisation de cristaux d'oxyde de magnésium (MgO) comme couche isolante

qui permet d'observer des écarts de résistance beaucoup plus importants, de l'ordre de 200% [12].

D'après la physique classique, si la tension appliquée aux bornes d'une jonction est inférieure à la hauteur de barrière, qui correspond à l'énergie nécessaire pour traverser la couche d'isolant, alors aucun courant ne la traverse. D'un point de vue quantique, les électrons possèdent la propriété d'être à la fois corpuscule et onde, une partie de l'onde est réfléchie tandis qu'une autre franchit la barrière, ce qui induit la création d'un courant. On peut alors exprimer la densité de courant :

$$J = J_0 \left[\bar{\varphi} \exp\left(-A\bar{\varphi}^{1/2}\right) - (\bar{\varphi} + eV) \exp\left(-A(\bar{\varphi} + eV)^{1/2}\right) \right] \tag{1.12}$$

Avec

$$J_0 = \frac{e}{2\pi\bar{h}(\beta\Delta_s)^2} \tag{1.13}$$

Et

$$A = \frac{4\pi\beta\Delta_s}{\bar{h}}(2m_e)^{1/2} \tag{1.14}$$

Avec $\bar{\varphi}$ la hauteur moyenne de la barrière, e et m_e la charge et la masse de l'électron, Δ_s l'épaisseur de la barrière, $\bar{h}$ la constante de Planck et $\beta \approx 1$ un coefficient correctif.

Pour des tensions faibles la densité de courant peut être approximée à une relation linéaire avec la tension qui peut-être alors assimilée à une loi d'ohm :

$$J \approx \left(\frac{\sqrt{2m_e}}{\Delta_s} \left(\frac{e}{\bar{h}}^2 \right) exp\left(-\sqrt{A\bar{\varphi}}\right) \right) V \tag{1.15}$$

Dans la suite du manuscrit on considérera que les tensions utilisées dans les mémoires MRAM se situent dans la gamme qui permet d'utiliser cette approximation. D'autre part il est important de préciser que dans les empilements utilisés pour les cellules MRAM, les résistances des autres couches sont négligeables par rapport à la TMR [1].

Les MRAM

Les MRAM (Magnetoresistive RAM) sont des mémoires pour lesquelles les données sont stockées sous forme d'orientations relatives de moments magnétiques. L'idée de stocker les données sous forme magnétique n'est pas nouvelle puisque dès 1898 l'inventeur polonais Valdemar Poulsen a développé et breveté le "Telegraphone", capable d'enregistrer des sons sur des fils magnétiques [46]. Il est l'ancêtre des cassettes audio avec lesquelles il était en concurrence jusque dans les années 1960.
Plus récemment, en 1953 les mémoires à tores magnétiques ont été conçues. Ce sont les premières mémoires magnétiques à accès aléatoire où chaque bit est stocké dans un tore magnétique qui est sélectionné par deux lignes de courant perpendiculaires, le tout formant une matrice. L'addition du champ magnétique généré par ces deux lignes de courant permet d'inverser le moment magnétique du tore. La lecture se fait en écrivant un '0' dans le tore : si le moment magnétique s'inverse, un courant est induit dans une ligne de lecture indiquant qu'un '1' est stocké dans la cellule mémoire. L'absence de courant induit indique un '0' dans la cellule [27].
Aujourd'hui le stockage magnétique est principalement utilisé dans les disques durs. Jusque dans les années 1990, les disques sont constitués de plateaux magnétiques sur lesquels les données sont écrites sur des secteurs par une bobine et lues en détectant ou non une variation de courant lors d'une réécriture à travers la même bobine. En 2000 les têtes de lecture et d'écriture sont séparées, la tête d'écriture est toujours une bobine mais la tête de lecture est maintenant un élément GMR ou TMR qui capte le flux magnétique émis par les bits de données. Ces têtes de lectures sont plus sensibles aux émissions magnétiques ce qui permet de réduire la surface des secteurs et augmente la densité de données stockées [8].
Les MRAM sont les successeurs des mémoires à tores magnétiques quant aux fonctionnalités : ce sont des mémoires à accès aléatoire non volatiles. Elles utilisent le principe de la TMR pour stocker et lire des données. Les premiers composants MRAM ont été commercialisés en 2006 par Freescale [2] en technologie Toggle. Depuis plusieurs laboratoires et entreprises ont lancé des développements sur d'autres technologies de MRAM, en particulier les MRAM STT par Everspin (anciennement Freescale), Samsung et Micron principalement et la technologie TAS-MRAM par Crocus Technology.

Field Induced Magnetic switching - FIMS, Toggle

Le changement d'orientation relatif des couches ferromagnétiques d'une jonction tunnel magnétique (MTJ) constitue l'opération de base pour l'écriture d'une donnée dans une cellule MRAM. Les premières générations de MRAM utilisent un champ magnétique généré par des lignes de courant pour effectuer ce changement d'orientation. Une des couches ferromagnétiques est construite pour être moins sensible à ce champ (la couche dite de référence) de sorte que seule l'autre couche (dite couche de stockage) change d'orientation magnétique. Une mesure de la résistance

permet de différencier l'état de la cellule : une résistance élevée (Rmax) pour un '0' et une résistance faible (Rmin) pour un '1'.

La couche de référence La couche de référence est conçue pour être fixe pendant les opérations d'écriture. Le champ magnétique généré par les lignes de champ ne doit pas modifier l'orientation de ses moments magnétiques. La principale caractéristique que doit avoir cette couche, c'est d'être très stable. Cependant, il ne faut pas qu'elle ait d'influence sur la couche de stockage. En effet, le moment magnétique de chaque couche ferromagnétique génère un champ magnétique qui va avoir tendance à modifier la direction des moments magnétiques des couches proches, cet effet vient de l'énergie dipolaire qui crée un champ démagnétisant 1.7. Dans le cas de la couche de stockage, ce champ va privilégier l'alignement parallèle ou antiparallèle. Pour répondre à ces deux contraintes, on utilise un empilement de couches comme illustré dans la figure 1.16.

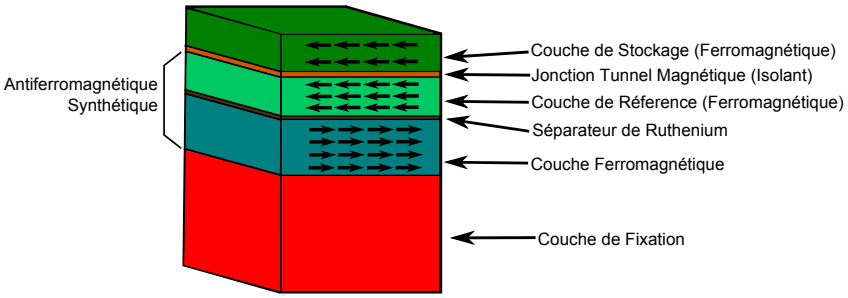

FIGURE 1.16 – Empilement magnétique de la couche de référence

En premier lieu, une couche de fixation épaisse avec un moment magnétique important et capable de garder son orientation magnétique face à des champs magnétiques élevés (voir équation 1.10). Cette couche ne peut exister de manière isolée du fait de son influence sur la couche de stockage. Pour pallier à celle-ci une couche antiferromagnétique synthétique est insérée entre la couche de fixation et la MTJ.

Un antiferromagnétique synthétique (SAF) est un empilement de deux couches ferromagnétiques séparées par une couche métallique non magnétique (généralement du Ruthénium). De la même façon que pour un matériau antiferromagnétique naturel, l'orientation des moments magnétiques de ces deux couches ferromagnétiques est opposée. Ces orientations opposées sont assurées par un couplage fort qui force l'orientation des deux couches ferromagnétiques en fonction de l'épaisseur de matériau non magnétique les séparant. Ce couplage est appelé RKKY (du nom de ses découvreurs Ruderman, Kittel, Kasuya et Yosida) [63].

Ce SAF est lui-même fortement couplé avec la couche de fixation par les interactions d'échanges entre atomes voisins (équation 1.4). Chacune de ces couches crée son propre champ magnétique qui va influencer les couches proches, mais la

direction de ces champs étant alternée, l'influence globale de l'empilement est négligeable sur la couche de stockage. La figure 1.17 montre la variation de l'intensité du couplage en fonction de l'épaisseur de la couche de séparation, le couplage privilégie les alignements parallèles ou antiparallèles en fonction de l'épaisseur de la couche de séparation.

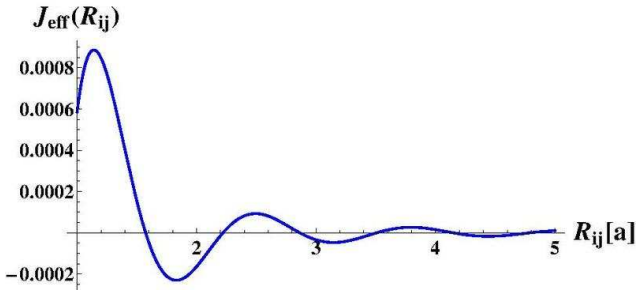

FIGURE 1.17 – Intensité du couplage RKKY en fonction de l'épaisseur de la couche de séparation

MRAM de Première Génération La première génération de MRAM est basée une architecture matricielle (voir figure 1.18) où chaque MTJ est positionnée sous le croisement de deux lignes de courants. Seule l'addition du champ magnétique généré par ces deux lignes est suffisante pour permettre la rotation de la couche de stockage de la cellule, de cette façon il est possible de n'en sélectionner qu'une seule. Cette méthode d'écriture est appelée Stoner-Wohlfarth, du nom de ses inventeurs.

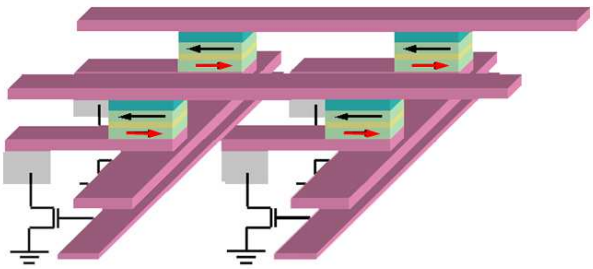

FIGURE 1.18 – Architecture en matrice des premières générations de mémoires

Pour garantir une meilleure stabilité, les empilements magnétiques ont une forme elliptique, cette géométrie permet d'augmenter l'anisotropie de la jonction. Les moments magnétiques ont alors tendances à s'aligner suivant des directions préférentielles dues à l'énergie d'anisotropie magnétocristalline (équation 1.5). Concrètement, les moments magnétiques s'alignent parallèlement à la direction la plus longue qui est appelée l'axe facile.

Cette approche a néanmoins des inconvénients au niveau de la réduction d'échelle. En effet avec des jonctions tunnel magnétiques de surfaces plus réduites, il apparait d'une part un problème de sélectivité : il arrive que certaines jonctions changent d'orientation alors qu'elles ne sont soumises qu'au champ d'une seule ligne. D'autre part, un champ magnétique plus élevé est nécessaire pour écrire sur des jonctions de taille plus réduite.
Ceci s'explique par le fait qu'avec des dimensions plus réduites il est plus difficile de produire des formes elliptiques optimales ce qui engendre des effets de bord d'autant plus importants que la jonction est petite. En effet, la géométrie elliptique et donc l'axe facile sont moins marqués [57]. Ceci impose une taille minimale aux cellules Stoner-Wohlfarth et a motivé la recherche de méthodes d'écriture alternatives pour les MRAM.

Toggle MRAM

Pour résoudre le problème de sélectivité, une des solutions proposées a été le développement de la Toggle MRAM par Freescale. L'écriture dépend toujours de l'addition des champs magnétiques de deux lignes de champs, mais elle utilise la méthode "Svatchenko switching". Plutôt que d'utiliser simultanément les deux champs magnétiques, chaque ligne est activée selon une séquence qui permet d'éviter les MTJ à moitié sélectionnées. La figure 1.19 montre la différence de sélectivité entre les méthodes d'écriture Stoner-Wohlfarth et Toggle. Avec la première méthode, des bits peuvent être retournés même avec une seule des deux lignes de champ activée ($i_{bit} = 0$ ou $i_{digit} = 0$) tandis que pour la méthode Toggle, le retournement n'a lieu que lorsque les deux lignes sont activées.

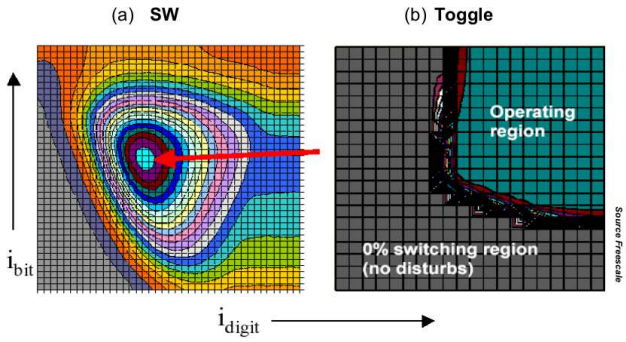

FIGURE 1.19 – Sélectivité de l'écriture Toggle comparée à la méthode Stoner-Wohlfarth

La couche de stockage des Toggle MRAM est en fait une triple couche qui compose un SAF (voir 1.2). Les deux couches ferromagnétiques du SAF ont des moments magnétiques orientés de manière opposée avec un fort couplage RKKY garantissant cette opposition. C'est cette caractéristique qui est utilisée pour l'écriture. Le champ magnétique modifie simultanément les deux couches, la position la

plus stable se trouve alors être celle où les moments magnétiques des deux couches sont orientés perpendiculairement au champ magnétique. Comme illustré dans la figure 1.20, la rotation de 180 ° des moments magnétiques est effectuée en trois étapes qui correspondent respectivement à l'activation d'une ligne de champ, l'activation des deux simultanément puis l'activation uniquement de la seconde.

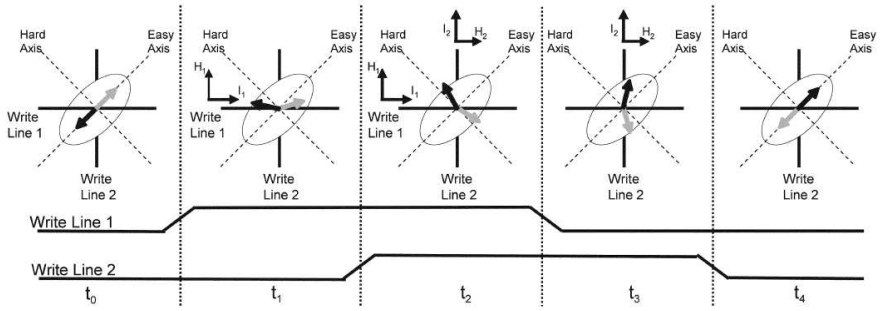

FIGURE 1.20 – Mécanisme d'écriture "Svatchenko switching" d'une MRAM Toggle [23]

Cette méthode a la particularité de retourner le moment magnétique de la couche de stockage, c'est-à-dire qu'il n'y a qu'un mécanisme d'écriture : cette opération inverse la donnée stockée. Il faut donc connaitre l'état initial de la MTJ afin de savoir si l'opération est requise ou non.
Cette méthode améliore beaucoup la stabilité et la fiabilité des MRAM et les premières MRAM commercialisée en 2006, fonctionnaient selon ce principe. Cependant, les problèmes de réduction d'échelle existaient toujours et rendaient la technologie MRAM incapable de concurrencer d'autres types de mémoires en l'état malgré des performances inégalées en termes de durabilité (environ 10^{15} opérations pour une MRAM contre 10^5 pour une mémoire flash NAND [17]) et de temps d'accès pour une mémoire non volatile (de l'ordre de 30 ns [17]).

Thermally Assisted Switching MRAM - TAS-MRAM

Une autre technologie de MRAM, la MRAM à retournement assisté thermiquement (Thermally Assisted switching MRAM ou TAS-MRAM), est développée en parallèle des MRAM Toggle, par Crocus Technology. Cette technologie repose sur une autre propriété des matériaux magnétiques, à savoir la dépendance en température du couplage d'échange. Les MTJ sont construites pour être extrêmement stables à température ambiante de sorte que même un champ d'écriture ne soit pas en mesure de modifier leur état. Un échauffement localisé au-delà d'une température dite de blocage permet de les déverrouiller. Une opération d'écriture s'effectue avec une seule ligne de courant, la sélection de la MTJ est effectuée par l'échauffement de cette dernière.

Le Couplage d'Échange - Exchange Bias Le couplage d'échange ou *exchange bias* est un couplage à l'interface entre une couche antiferromagnétique et une couche ferromagnétique. Comme le montre l'équation 1.4, les moments magnétiques de chaque atome influencent les moments magnétiques des atomes voisins et vont tendre à les aligner dans la même direction (ou la direction opposée suivant le signe de la constante d'échange). Dans la couche de matériau antiferromagnétique (naturel) la structure cristalline impose à chaque atome d'avoir ses plus proches voisins avec des moments magnétiques opposés. Cette configuration est donc très stable puisque chaque moment magnétique est compensé par ses voisins. Cependant en bordure du matériau, les moments magnétiques ne sont pas complètement compensés. Lorsque cette bordure se retrouve en contact avec un matériau ferromagnétique, ce déséquilibre contraint l'état des atomes de la couche ferromagnétique à l'interface avec cette couche [9].

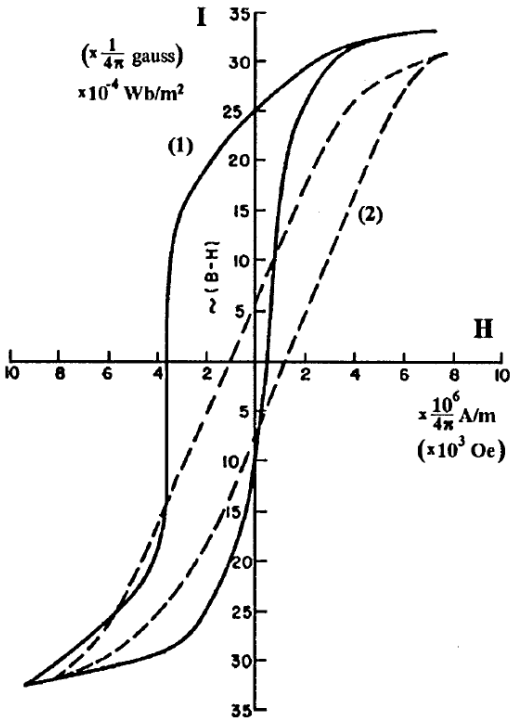

FIGURE 1.21 – Courbe d'hysteresis avec (trait plein) et sans (pointillé) couplage d'échange [9]

Grâce à sa structure, la couche antiferromagnétique est très stable et insensible aux influences des moments magnétiques extérieurs. La couche ferromagnétique quant à elle, est plus sensible et ses moments magnétiques peuvent être retournés plus facilement. Elle a donc un *offset* magnétique orienté dans la direction de la couche à l'interface de la couche antiferromagnétique (figure 1.21). C'est-à-dire qu'il faudra un champ externe plus élevé pour retourner son aimantation globale dans la direction inverse de celle du couplage. Un champ plus faible est nécessaire pour retourner son aimantation globale dans la direction du couplage.

Ce couplage disparait cependant au-delà d'une température dite de blocage. Avant d'atteindre la température de Néel, la température à partir de laquelle la nature antiferromagnétique du matériau disparait, l'agitation thermique dans la couche magnétique devient trop importante pour maintenir le couplage. La couche de stockage est alors libre et le champ magnétique des lignes de courant peut changer l'orientation de ses moments magnétiques (voir figure 1.22).

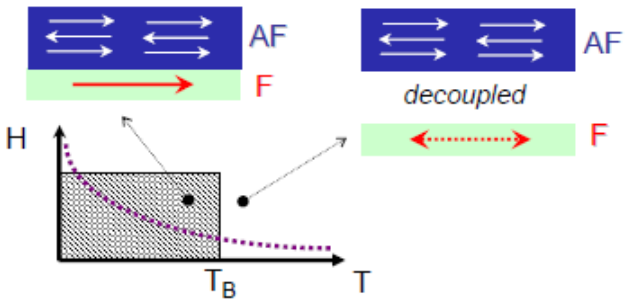

FIGURE 1.22 – Effet de la température sur le couplage d'échange entre une couche ferromagnétique et une couche antiferromagnétique [57]

Opération d'écriture Le couplage d'échange est utilisé pour verrouiller la couche de stockage de l'empilement. Comme illustré sur la figure 1.23, l'écriture se déroule en trois étapes :

1 - Chauffage de l'empilement - L'empilement est chauffé au-delà de la température de blocage de la couche antiferromagnétique, soit environ 180°C, le couplage d'échange disparait et l'aimantation de la couche ferromagnétique devient sensible aux perturbations extérieures.

2 - Application du champ magnétique - Une seule ligne de champ génère un champ électromagnétique sur toute une ligne de MTJ, mais seule la couche de stockage dont l'empilement est préalablement chauffé change d'orientation magnétique.

3 - Refroidissement sous champ - La couche antiferromagnétique retrouve sa structure anti-alignée mais les moments magnétiques de la couche ferromagnétique ont été retournés et sont maintenus dans cet état par le champ électromagnétique de la ligne de champ : ils exercent une force sur les moments magnétiques de l'antiferromagnétique à l'interface. Ces derniers s'alignent donc comme ceux de la couche ferromagnétique appliquant un couplage d'échange dans la direction opposée.

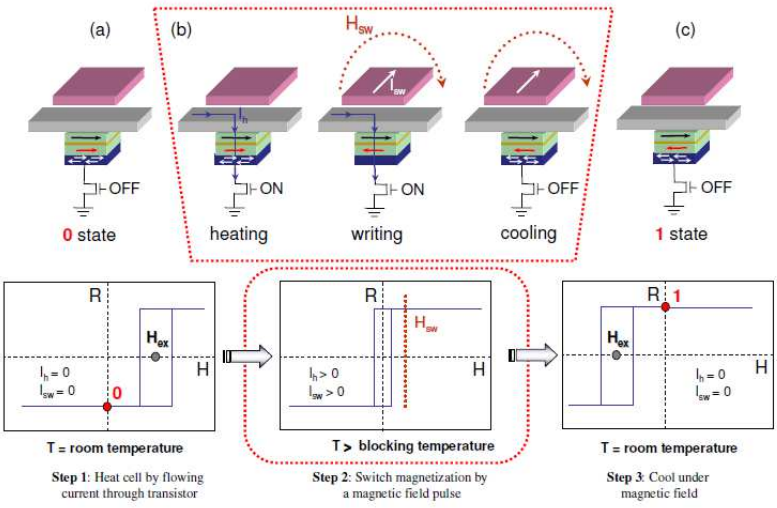

FIGURE 1.23 – Processus d'écriture d'une TAS-MRAM

Le chauffage des MTJ est fait par effet Joule en faisant circuler du courant au travers de la jonction, cela permet de sélectionner uniquement la cellule mémoire sur laquelle la donnée doit être écrite et élimine les erreurs d'adressage et de sélectivité rencontrées pour les premières générations de MRAM.

Considération énergétique Le fait de n'utiliser qu'une seule ligne de champ (au lieu de l'intersection de deux dans une MRAM conventionnelle) permet un gain important en termes de consommation d'énergie, et ce malgré le préchauffage né-

cessaire. En effet, le courant de chauffage est de l'ordre de la centaine de μA tandis que le courant pour générer le champ magnétique dans une ligne de champ est de l'ordre de la dizaine de mA. Mais ce n'est pas le seul facteur qui permet de réduire la consommation lors d'une écriture. Contrairement aux mémoires Toggle ou Stoner-Wolfarth qui utilisent un point mémoire de forme elliptique pour améliorer l'anisotropie et donc la stabilité de la donnée stockée, le point mémoire est circulaire ce qui réduit le champ nécessaire pour retourner son moment magnétique (l'énergie dipolaire est quasi nulle, voir equation 1.7). Cette amélioration est possible, car la stabilité est déjà garantie par le couplage d'échange avec la couche d'antiferromagnétique.
L'énergie totale pour retourner un bit peut s'écrire sous la forme :

$$E \approx K + (AR - 1).\left(\frac{e}{L}\right).M_s^2 + \frac{J_{eb}.M_s^2}{t}.\left(1 - \frac{T}{T_b}\right) \tag{1.16}$$

Avec K l'anisotropie cristalline, e et L respectivement l'épaisseur et la longueur du point mémoire, M_s^2 l'aimantation de saturation de la couche et AR le facteur de forme ou *Aspect Ratio* qui est égal à 1 dans le cas d'un point mémoire circulaire, rendant le second terme de l'équation nul. J_{eb} est l'énergie d'échange avec la couche ferromagnétique, T et T_b sont la température à laquelle est soumise l'échantillon et la température de blocage [57].
Avec cette expression on constate également qu'en réduisant la surface du point mémoire, on augmente l'énergie nécessaire pour le retournement du moment magnétique dans le cas d'un point mémoire non circulaire. De ce fait, la technologie TAS-MRAM permet de résoudre en théorie le problème de la réduction d'échelle des MRAM tout en réduisant leurs consommations (figure 1.24).

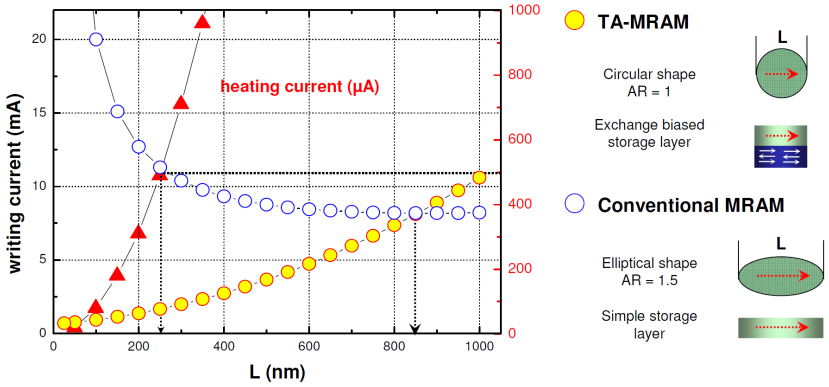

FIGURE 1.24 – Comparaison de la consommation d'une MRAM conventionnelle et d'une TAS-MRAM en fonction de la surface du point mémoire [57]

Spin Torque Transfer MRAM - STT-MRAM

Les MRAM à retournement assisté thermiquement sont le sujet principal du travail effectué durant cette thèse, cependant d'autres technologies de MRAM existent. La plus prometteuse d'entre elles est la MRAM à couple de transfert de spin (Spin Torque Transfer ou STT-MRAM) pour laquelle l'écriture est effectuée à l'aide d'un courant polarisé en spin. À l'origine de ce type d'écriture, le phénomène de couple de transfert de spin était une source de bruit pour les disques durs. En effet, le courant utilisé pour la mesure de la GMR par les têtes de lecture créait un couplage entre la couche de référence et la couche de stockage [1, 36].

Lorsque des électrons franchissent une couche aimantée, ils ont tendance à se polariser, c'est-à-dire que leurs moments magnétiques vont s'aligner avec les moments magnétiques locaux. Réciproquement il existe un effet qui a tendance à aligner les moments magnétiques des électrons de la couche magnétique avec ceux des électrons entrants.
Dans le cas où les deux couches ont des moments magnétiques antiparallèles, les électrons vont se polariser dans la couche de référence qui est stable et venir retourner les moments magnétiques de la couche de stockage. Dans le cas parallèle, les électrons transitent par la couche de stockage. Ainsi, les électrons polarisés avec le bon moment magnétique vont franchir sans difficulté la jonction tunnel tandis que les autres vont s'accumuler dans la couche de stockage jusqu'à exercer une pression suffisante pour retourner son moment magnétique.
Cet effet se traduit par un couple qui agit sur les moments magnétiques : le couple de transfert de spin (Spin Torque Transfer ou STT) [65] :

$$\vec{\Gamma_s} = a_J \vec{M}.\left(\vec{P}.\vec{M}\right) \tag{1.17}$$

Avec $\vec{P}$ la polarisation des électrons circulant dans la couche de stockage et a_J un terme proportionnel au courant J traversant la couche. Ce couple ajoute un terme à l'équation 1.11 qui devient :

$$\frac{\partial \vec{M}}{\partial t} = -\gamma\left(\vec{M}.\mu_0\vec{H}_{eff}\right) + \frac{\alpha}{M_s}\left(\vec{M}\frac{\partial \vec{M}}{\partial t}\right) + a_J\vec{M}.\left(\vec{P}.\vec{M}\right) \tag{1.18}$$

L'intensité du courant utilisé pour l'écriture (présent dans l'équation 1.18 via le paramètre a_J) va déterminer le temps minimum pour retourner le moment magnétique de la couche de stockage. Un courant plus important réduit le temps de retournement, mais réduit la durabilité de la jonction magnétique tunnel ; il y a un compromis à trouver entre ces deux facteurs (figure 1.25).

Sur la figure 1.25, on constate que la densité de courant minimal nécessaire pour retourner un bit est un paramètre clé de la réduction de la consommation. Et c'est sur ce point que les STT-MRAM permettent de réduire significativement la consommation.
Ce principe permet d'écrire et de lire des cellules MRAM sans utiliser de lignes de courant pour générer de champ magnétique. La consommation de courant est alors réduite d'un facteur 100 [17].

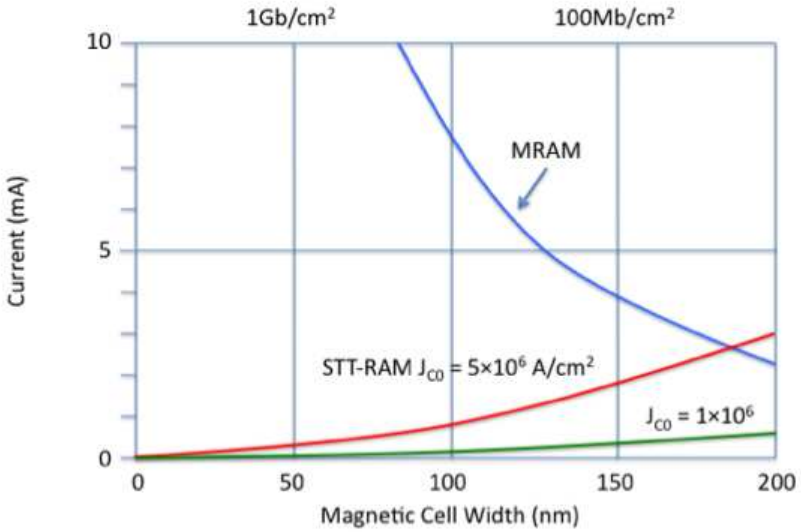

FIGURE 1.25 – Comparaison de la consommation d'une MRAM conventionnelle et d'une STT-MRAM en fonction de la surface du point mémoire.

1.3 La sécurité des mémoires

Les problématiques liées à la sécurité des composants mémoires peuvent être abordées de deux points de vues différents.

— D'une part en considérant la mémoire comme un composant non critique d'un point de vue sécurité, typiquement pour le stockage de données publiques ou non sensibles. Dans ce cas, la priorité sera l'intégrité des données stockées en fonctionnement normal, mais aussi face à des perturbations extérieures qui ne sont pas nécessairement malicieuses, mais qui peuvent pour autant perturber ou endommager le composant, on parle dans ce cas de fiabilité.

— D'autre part, il est également possible de considérer les mémoires comme partie intégrante d'un système sécurisé pour stocker des clés secrètes ou des variables temporaires d'un algorithme sécurisé. Dans ce cas-là, l'intégrité et la confidentialité des données doivent être garanties.

La sécurité des systèmes électroniques

Les systèmes électroniques communicants ainsi que les systèmes d'identifications utilisent dans leur grande majorité des algorithmes de cryptographie embarquée. Ils permettent entre autres d'assurer la confidentialité et l'intégrité des données et des fonctionnalités de ces applications. Ces algorithmes embarqués sont réputés fiables d'un point de vue mathématique. Avec les puissances de calculs accessibles à l'heure

actuelle la cryptanalyse des données chiffrées n'est pas réalisable dans un temps jugé raisonnable.
Cependant l'implantation de ces algorithmes dans des circuits électroniques qui peuvent être attaqués pour réduire la robustesse intrinsèque des algorithmes. Les attaques sur l'implantation électronique des circuits sont classiquement regroupées en trois catégories :

— La rétro-conception : Cette technique consiste à obtenir des informations sur le détail de l'implantation physique d'un circuit sécurisé, pour en extraire le *layout*

— Les attaques en fautes : Cette technique consiste à perturber le circuit pour le dérouter de son fonctionnement normal dans le but d'obtenir des erreurs exploitables [6].

— Les attaques par canaux auxiliaires : Cette technique consiste à observer les paramètres physiques du circuit tels que sa consommation de courant, ses émissions électromagnétiques, ses temps de réponse pour en déduire des informations sur les données manipulées.

Dans le cas de l'implantation matérielle d'un algorithme, ces trois catégories d'attaque conduisent à un même objectif, réduire le nombre de possibilités à tester pour retrouver la clé de chiffrement de l'algorithme en un temps raisonnable.

Notre étude porte sur la mise en œuvre de ces attaques afin de déterminer celles qui seraient les plus pertinentes pour la sécurité des MRAM. En effet l'objectif ciblé est de définir le potentiel de sécurité de la technologie MRAM en elle-même d'où la nécessité permanente de se focaliser sur des erreurs directement liées aux empilements magnétiques et aux opérations les plus basiques sur la mémoire. Dans cette étude des attaques seront menés sur des circuits de technologie hybride MTJ/CMOS avec un focus particulier sur la partie magnétique. En effet, contrairement à la partie CMOS qui a été largement étudiée en terme d'attaque, peu de travaux ont été menés sur la partie magnétique. D'où l'originalité de ce travail.

Attaques en fautes

A l'origine la perturbation des circuits est une problématique de fiabilité avant d'être une problématique de sécurité. Les premières perturbations à avoir été étudiées portaient sur les effets des particules radioactives sur les circuits [42]. En effet, les circuits destinés à des applications aéronautiques et spatiales étaient soumis à des concentrations en particules ionisantes très élevées du fait de la présence de rayonnements cosmiques. Depuis plusieurs méthodes pour perturber les circuits ont été décrites, les principales portent sur les variations de tension [75], de fréquence d'horloge [74], les variations de température [14], les injections de fautes lasers [56] et les injections des fautes électromagnétiques [7].

Par exemple dans le cas d'algorithme cryptographique implanté, L'attaque DFA (Differential Fault Analysis) repose sur la génération de perturbations contrôlées dans le circuit pour pouvoir analyser la différence entre le résultat attendu correct et le résultat fauté [10, 11]. L'analyse des différences entre un résultat volontairement fauté et un résultat non fauté permet d'extraire des informations sur les secrets cryptographiques à condition d'avoir une bonne maitrise de la perturbation pour avoir un modèle de comparaison précis.

Cependant dans le cas des mémoires, les attaques se résument à corrompre l'écriture ou la lecture d'une donnée par des moyens autres que le protocole normal. Sergei Skorogobatov et al montrent que des variations en température appliquées à une mémoire flash modifie les données stockées dans cette mémoire [64], Roscian et al utilisent l'effet photoélectrique pour modifier les données de cellules SRAM [62]. Les attaques physiques qui vont être présentées dans ce manuscrit sont largement inspirées de ces techniques, mais adaptées aux spécificités technologiques des MRAM, en particulier l'utilisation de champs magnétiques (statique ou par impulsions).

Attaques par canaux auxiliaires

L'attaque par canal auxiliaire est une autre méthode pour avoir accès à des données secrètes dans un circuit électronique. L'attaque est basée sur les fuites inhérentes au circuit que ce soit en consommation, en émissions électromagnétiques, thermiques ou en onde acoustique [28]. Ces fuites dépendent des données manipulées dans le circuit.
En particulier, dans un circuit CMOS une porte logique va avoir une signature de fuite repérable en fonction des transitions d'états. L'analyse de ces fuites peut permettre de retrouver quelles données ont été manipulées et d'en déduire des informations qui ne sont pas accessibles par les entrées du circuit [30].

L'attaque de référence par canaux auxiliaires Differential Power Analysis (DPA) a été proposée par Kocher et al. dès 1999 [38], elle basée sur la différence de moyenne entre une hypothèse de consommation de courant théorique et des mesures réelles extraites du circuit. Cette attaque a ensuite été améliorée en remplaçant la différence de moyenne par un autre distingueur, la corrélation. Elle porte le nom de CPA (Correlation Power Analysis) [13].
L'attaque par dictionnaire ou *template attack* est un autre type d'attaque qui permet également de relier les mesures de fuites à des valeurs du circuit sans connaissances approfondies de son fonctionnement interne. En constituant un dictionnaire de mesures qu'il comparera au système qu'il veut attaquer, l'attaquant peut analyser les fuites d'un circuit avec un nombre relativement faible de courbes. Cependant, cette méthode nécessite l'accès à un circuit de référence complètement ouvert pour la constitution de la bibliothèque.

1.4 Bancs de test et échantillons

Durant les travaux de cette thèse, une partie importante du travail a été expérimentale. Les différentes faiblesses identifiées lors de l'analyse théorique des mémoires et la compréhension des architectures des composants utilisés ont dû être testées. La première partie de cette section va être consacrée à la description des outils expérimentaux mis à ma disposition ou mis en place pour valider mes hypothèses, la première partie sera complétée par la description du circuit de test et enfin elle inclura une présentation des circuits mémoires testés.

Bancs de caractérisations

Les bancs de caractérisations sécuritaires disponibles au laboratoire SAS permettent de définir les niveaux de résistances des circuits aux différents types d'attaques proposées. Lors de ce travail, ils peuvent être utilisées tels que ou nécessiter des adaptations en fonctions de besoins spécifiques (nouvelles mémoires, circuits non standards, ..). Trois bancs principaux ont été utilisés :

— Banc champ magnétique permanent
— Banc injection d'impulsions électromagnétiques
— Bancs de caractérisation température

Banc champ magnétique permanent

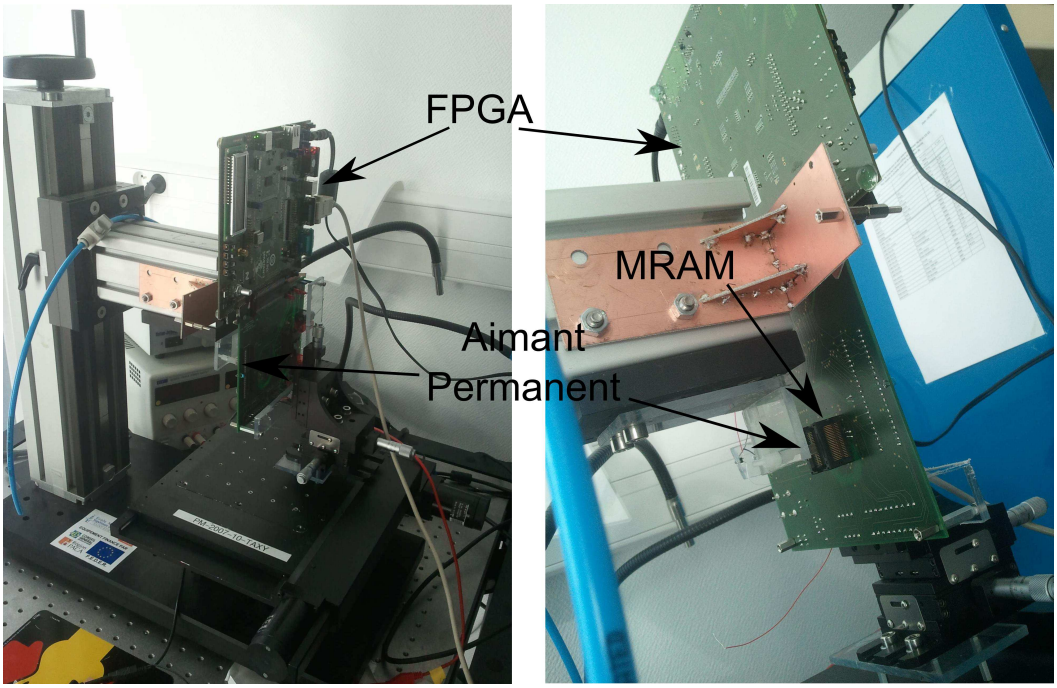

FIGURE 1.26 – Photos du banc de champ magnétique permanent

Il a pour but de tester les limites de fonctionnement d'une MRAM sous l'effet d'un champ magnétique statique. Ce banc ne fait pas partie des outils standards de caractérisation sécuritaire, il a donc été conçu spécifiquement pour le cas des MRAM.

Il est composé d'une table XY et d'un aimant permanent monté sur un support fixe. L'aimant se présente sous la forme d'un cube de 5 mm de côté en néodyme-fer-bore avec un champ magnétique au contact de l'ordre de 500 Oe. La table XY permet de contrôler la distance entre le composant et l'aimant (figure 1.26). Pour cela la carte sur laquelle est placé le composant est positionnée verticalement, cela permet d'utiliser l'axe X à la façon d'un axe vertical.

Pour des champs magnétiques importants (>100 Oe), un écart de quelques centaines de micromètres peut engendrer des erreurs de mesures non négligeables. Pour cette raison, avant chaque campagne de mesure une table de correspondance de référence entre la distance et le champ magnétique au niveau du composant est construite à partir de mesures du champ magnétique à l'aide d'un capteur à effet Hall. Malgré cette précaution, pour garder une précision suffisante le champ utilisé ne doit pas dépasser les 200 Oe, au-delà les imprécisions de la position relative de l'aimant et du circuit deviennent trop importantes.

D'autre part, l'effet du champ est maximum sur les MRAM lorsque les lignes de champ sont parallèles aux couches magnétiques et au champ généré par les lignes de champ.L'aimant doit donc être positionné de manière à ce que les lignes du champ magnétique qu'il génère soient orientées dans la bonne direction.

Banc d'injection d'impulsions électromagnétiques

Ce banc est complémentaire du banc champ magnétique permanent dans la mesure ou il permet de tester les effets d'un champ magnétique transitoire. L'intérêt d'un tel banc est qu'il permet d'avoir une précision spatio-temporelle propice à des attaques ciblées Le banc d'injection d'impulsions électromagnétiques est composé d'un générateur d'impulsions relié à une bobine qui va convertir les impulsions de tension en impulsions électromagnétiques. D'autre part, à l'inverse du banc champ permanent statique, le circuit est fixé sur une table XYZ qui permet de positionner la bobine avec précision pour permettre de modifier la position de l'injection.

Le impulsions générées d'une largeur de 10 à 200 ns pour une tension de -200V à +200V.

Les impulsions électromagnétiques ont des effets à la fois sur les signaux électriques dans le circuit et sur les moments magnétiques des cellules mémoires, les tests demandent donc une précision temporelle importante pour bien différencier les types d'erreurs obtenus. Ce point sera développé plus en détail dans le chapitre 4.2.

Bancs température

Ces bancs permettent de tester l'effet de la température sur des TAS-MRAM lors des opérations d'écriture et lecture. Des tests ont également été effectués sur

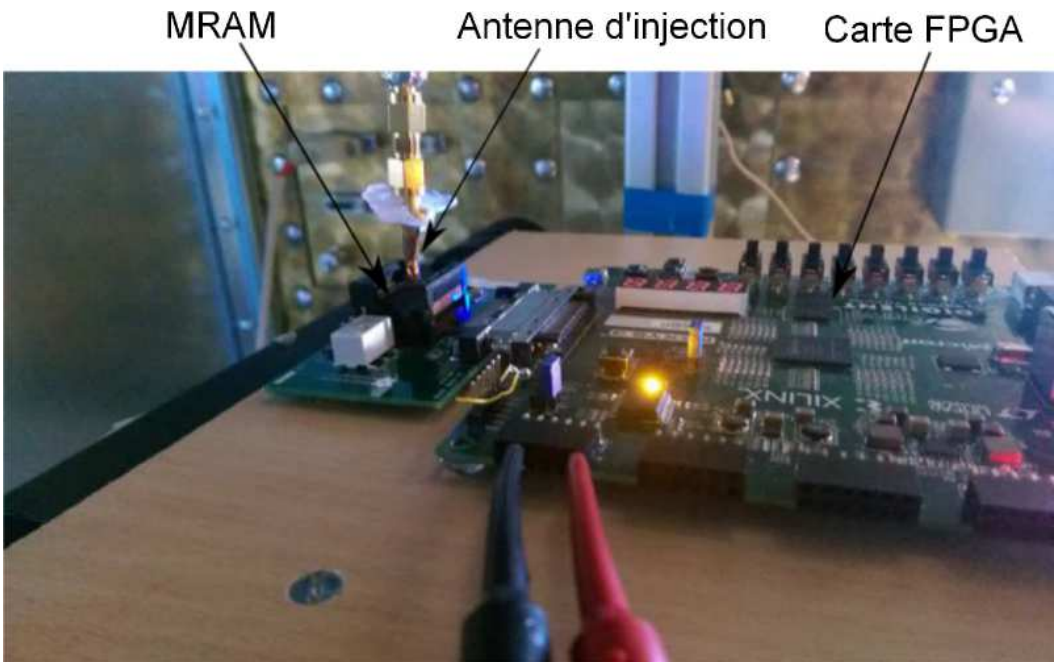

FIGURE 1.27 – Photo du banc d'injection d'impulsions électromagnétiques

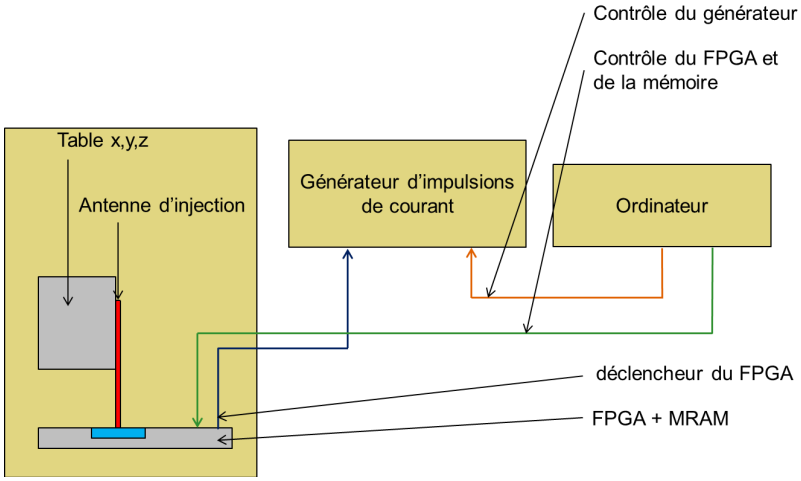

FIGURE 1.28 – Schéma de fonctionnement du banc d'injections d'impulsions électromagnétiques

des MRAM toggle. Deux bancs ont été utilisés. Le premier est une étuve qui permet de programmer différents types de gabarit en modulant les temps de montée et de descente ainsi que les températures à atteindre.

L'enceinte peut atteindre une température de +180°C ce qui permet des tests allant au-delà des spécifications des composants TAS-MRAM à ma disposition (leur

spécification autorise un fonctionnement jusqu'à 90°C). D'autre part, une petite ouverture sur le coté de l'étuve permet de déporter le circuit de commande (le FPGA) permettant ainsi de ne stresser que la mémoire en température.

FIGURE 1.29 – Enceinte climatique

Le second banc est une station de dessoudage de composants BGA à air chaud, qui permet des apports de chaleur maitrisé en température et très localisé. Les tests ont été effectués par palier de 10 à 20 °C jusqu'à 300°C permettant de perturber les composants sans les endommager. De plus contrairement à l'étuve qui a un effet global sur le composant, ce banc permet de concentrer le flux sur une partie du composant, en effet des buses de différentes tailles et géométries sont disponibles. Celle utilisée dans notre cas dispose d'une ouverture carrée de 6mm de côté. Cependant, la température est mesurée sur le package et la température atteinte par le composant n'est qu'évaluée à l'intérieur du boitier. Cette évaluation part de l'hypothèse que le flux de chaleur ainsi que la fonction de transfert du boitier sont constants.

Carte d'interfaçage

Pour les besoins des différents tests, un carte d'adaptation a été spécifiquement conçue. Cette carte dispose d'un support pour accueillir les mémoires et est connectée à un FPGA de contrôle qui envoie les différents signaux au composant testé. Du fait du caractère programmable du FPGA et de la modularité de la carte, l'ajout de nouvelles expérimentations est possible sans changer le montage.

L'utilisation du FPGA rend également possible un contrôle temporel précis des signaux de contrôle, ainsi que la génération de déclencheurs permettant la synchronisation des perturbations avec les opérations de la mémoire.

Pour certains tests il est nécessaire d'accéder aux *fuse bits*, il s'agit de zones mémoires dédiées accessibles uniquement en mode de test, ils permettent de modifier certaines caractéristiques de la mémoire ainsi que d'activer ou désactiver certaines fonctionnalités telles que la correction automatique d'erreurs. Pour y accéder, une alimentation de 6.9V est nécessaire, contre 3.3V pour une opération standard de la mémoire. La carte d'interfaçage doit donc pouvoir permettre de changer l'alimentation, c'est le rôle de l'alimentation 2 illustrée dans la figure 1.30. En outre, la carte prévoit également la possibilité de choisir d'alimenter le composant testé par une alimentation externe ou par le FPGA.

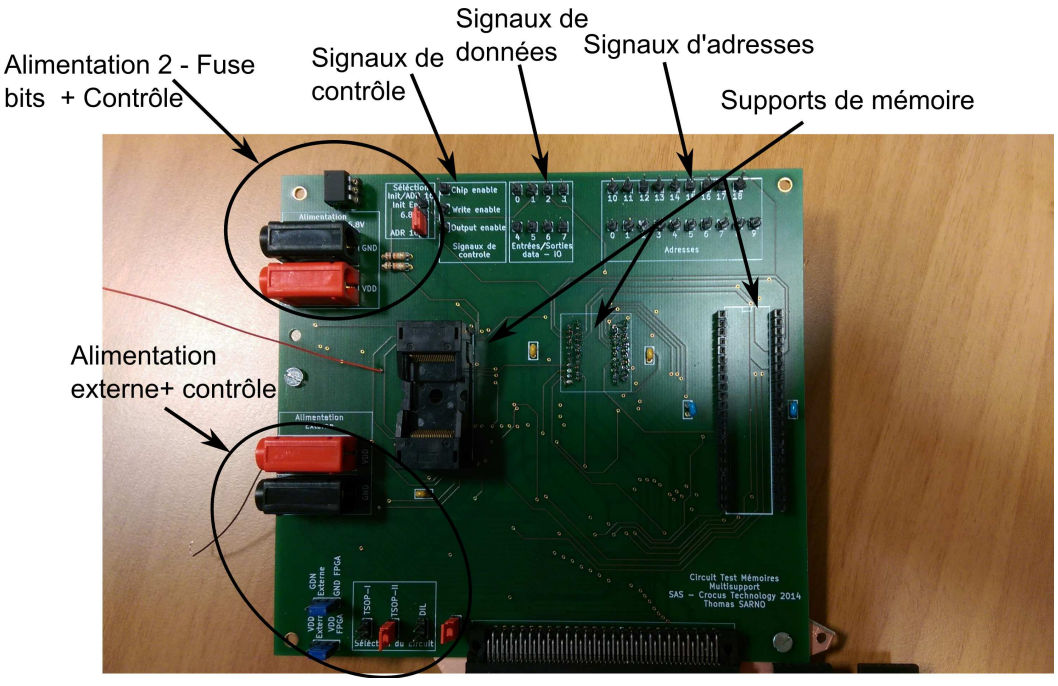

FIGURE 1.30 – Carte pour MRAM développée pour les tests

Description des échantillons

Everspin Toggle MRAM 4Mbit

Everspin est à ce jour le seul fabricant à commercialiser des mémoires de technologie MRAM, une partie des tests effectués au cours de ma thèse l'ont été sur des mémoires de type Toggle (voir paragraphe 1.2). Ces mémoires ont l'avantage d'avoir le même brochage ainsi que le même protocole d'écriture et de lecture que les mémoires de Crocus Technology auxquelles j'ai eu accès ce qui facilite la transposition des tests d'un composant à l'autre [25].

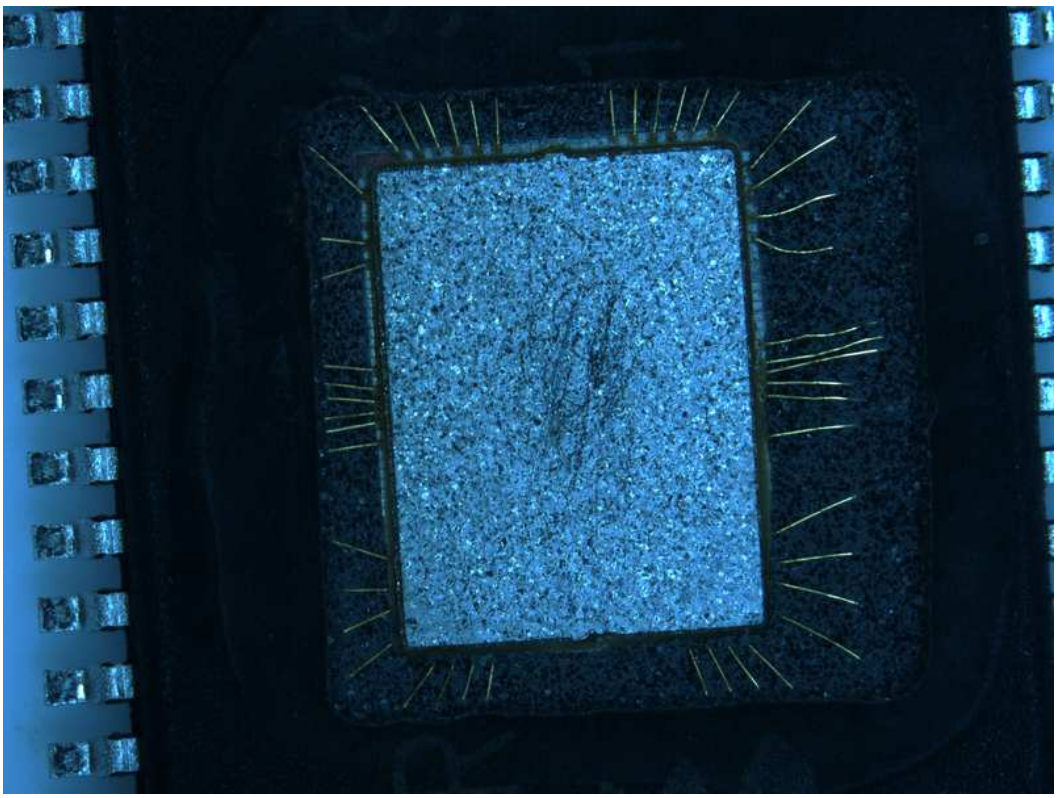

FIGURE 1.31 – MRAM Everspin décapsulée avec un bouclier magnétique en nickel-fer-molybdène

En plus du mode d'écriture qui diffère des TAS-MRAM, les mémoires Everspin ont la particularité d'être protégées par deux boucliers magnétiques, un sur la face avant du composant (voir figure 1.31) et un sur la face arrière. Ces boucliers sont des couches d'un alliage de nickel-fer-molybdène (Ni-Fe-Mo) de quelques dizaines de micromètres qui sont déposé sur la couche de passivation du composant. Ils ont la propriété de concentrer le champ magnétique ce qui protège le circuit des champs magnétiques externes (le fonctionnement des boucliers magnétiques sera détaillé dans le paragraphe 3.3).

Crocus TAS-MRAM 4Mbit - Revisions E-G-I

Plusieurs versions des TAS-MRAM de Crocus Technology ont été étudiées dans cette thèse au fur et à mesure de leurs disponibilités, elles correspondent à trois révisions de mémoire de 4 Mbits (soit 256 kilooctets). Chaque révision correspond à des améliorations de l'architecture ou de l'empilement mémoire.

Historique :

Révision E : C'est une des premières (avec la révision D) à avoir été encapsulée et à avoir un rendement utilisable pour des tests de caractérisation et de sécurité. Cependant, le nombre d'empilements en court-circuit ou en circuit ouvert était encore relativement important (de l'ordre de 10 à 20% d'erreurs)

Révision G : Dans cette révision une couche de tantale (Ta) a été ajoutée dans l'empilement ce qui améliore considérablement la stabilité des données stockées. Pour les meilleurs échantillons, 99.8% des bits étaient corrects. La majorité des tests ont été effectués sur ces échantillons.

Révision I : La stabilité de la révision G a mis en lumière une asymétrie de l'écriture et du stockage entre les '1' et les '0', une optimisation des épaisseurs des couches des empilements des cellules mémoires a permis d'encore réduire les erreurs et d'augmenter la fiabilité dans cette révision.

Implantation : Pour tous les échantillons auxquels j'ai eu accès, la matrice mémoire se décompose en deux parties, les bits de données et les bits de corrections d'erreur. Pour chaque octet de donnée stocké, il y a 8 bits de corrections d'erreur, la correction est basée sur le décodage par syndrome. Le circuit est capable de corriger deux erreurs (voire trois si elles sont sur des bits adjacents). La mémoire est divisée en huit banques, chacune est divisée en deux, une partie pour les données, une partie pour la correction d'erreurs.

1.5 Conclusion

Ce chapitre permet au lecteur de posséder les éléments nécessaires à la compréhension de la suite de ce manuscrit. Il s'agit également de donner les bases théoriques à la suite du document. La sécurité des composants fait en effet appel à tout un éventail de domaines allant de la physique et du micromagnétisme à l'implantation technologique des mémoires. La suite du document présente une étude de la robustesse des MRAM face à l'analyse des fuites pendant leur fonctionnement puis l'étude de leur sécurité et de leur fiabilité face à des perturbations externes.

Chapitre 2

Attaques par canaux auxiliaires

Sommaire

2.1 Analyses des courbes d'émissions électromagnétiques

En termes de sécurité, les composants électroniques doivent répondre à 4 propriétés : la confidentialité, l'authentification, l'intégrité et la non-répudiation. Deux de ces propriétés nous intéressent dans les mémoires : la confidentialité et l'intégrité, en effet le rôle d'une mémoire étant de stocker des données, les propriétés d'authentification et de non-répudiation sont assurées par d'autres composants. Dans ce chapitre c'est la propriété de confidentialité qui va être étudiée. Pour rappel il existe plusieurs sources de fuites dans les composants électroniques qui permettent de récupérer des informations sur son fonctionnement interne (voir 1.3). Dans le cas des mémoires deux sources principales peuvent être retenues : la consommation de courant et les émissions électromagnétiques. La première permet une analyse globale du circuit, car tous les appels de courant vont être détectés tandis que la seconde permet de se concentrer sur certaines zones en particulier, et ainsi de cibler les fuites les plus riches en informations. Dans ce chapitre ce sont les émissions électromagnétiques et leur analyse qui vont être étudiées.

Mesure des rayonnements électromagnétiques émanant des circuits MRAM

Comme expliqué dans le paragraphe 1.3, pour les composant CMOS il y a une corrélation entre les données manipulées et des signatures en courants, dans le cas des MRAM il s'agit principalement d'analyser les opérations de lecture et d'écriture. Les rayonnements électromagnétiques sont issus de plusieurs sources :

- les entrées/sorties qui sont une source particulièrement importante d'émissions en raison de la présence de fils de connexions, ou *bondings*, qui agissent comme des antennes et qui sont parcourus par des courants importants.
- les blocs analogiques tels que les pompes de charges ou les amplificateurs, car ils sont constitués de circuits capacitifs dont la charge et la décharge sont des sources importantes de rayonnement.
- les rails d'alimentation qui distribuent le courant dans le circuit et qui au même titre que les fils de connexions agissent comme des antennes [52].

D'une manière générale les blocs logiques synchrones sont une source importante d'émissions électromagnétiques, cependant les circuits MRAM étant asynchrones, il ne devrait donc pas y avoir d'émissions inhérente à ces blocs logiques. Cependant, certains blocs sont synchronisés sur les signaux de contrôles de la mémoire, tels que Chip Enable ($\overline{CE}$), Write Enable ($\overline{WE}$) ou Output Enable ($\overline{OE}$) : ils auront donc une activité identifiables sur les courbes des signatures.

Afin de pouvoir capter et étudier ces émissions, il est nécessaire d'utiliser des sondes d'analyse avec des caractéristiques spécifiques (qui seront détaillées plus loin dans cette section), ces sondes peuvent être soit achetées dans le commerce, soit fabriquées sur place . Ce type de sonde est constitué d'une bobine métallique comportant une ou plusieurs spires qui mesurent le flux électromagnétique (voir la

photo de la figure 2.1).

D'après le théorème d'Ampère-Maxwell, le flux électromagnétique traversant une boucle de surface S est égal à :

$$\Phi_B(t) = \int_S \vec{B}(t).d\vec{(}s) \tag{2.1}$$

D'après la loi de Lenz, la force électromotrice (fem) est alors définie par :

$$\text{fem}(t) = -\frac{\mathrm{d}\Phi(t)}{\mathrm{d}t} \tag{2.2}$$

La force électromotrice est mesurée aux extrémités de la bobine de la sonde. Les signatures correspondent à ses variations.

Les sondes utilisées sont des sondes à champs proches fournies par Langer (kit de sonde Langer RF2), ces sondes sont passives, c'est-à-dire qu'elles n'utilisent pas d'amplificateurs. Deux de ces sondes ont été utilisées :

— La sonde RF-R 50-1 : Cette sonde, sonde A dans les figures suivantes, est de forme circulaire d'un diamètre de 10 mm et capte les émissions perpendiculaires à son plan. Elle a une bande passante d'un peu moins de 3 GHz (de 30 MHz à 3GHz)
— La sonde RF-U 5-2 : Cette sonde, sonde B dans les figures suivantes, d'une taille de 5 mm permet de mesurer des champs parallèles aux circuits. Elle a une bande passante d'un peu moins de 2GHz (de 30 MHz à 2 GHz).

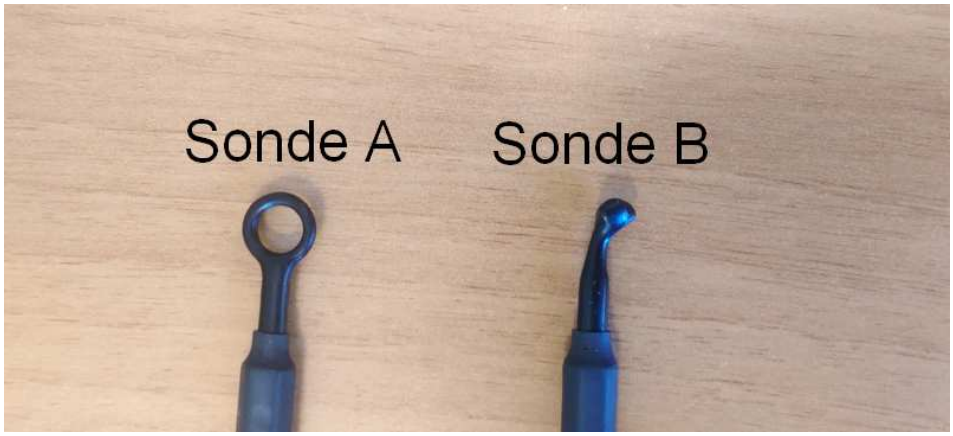

FIGURE 2.1 – Sondes électromagnétiques utilisées

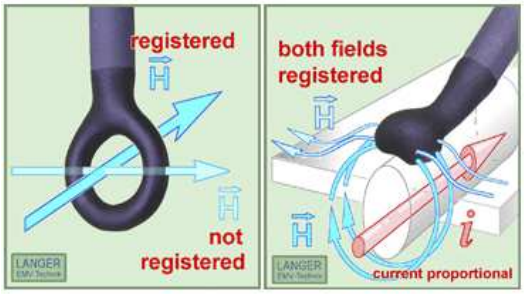

FIGURE 2.2 – Sondes électromagnétiques utilisées - Schéma des émissions mesurées

Les rayonnements mesurés par ces deux sondes sont différents en raison de leur sélectivité en terme d'orientation de lignes de champs et de précision spatiale comme illustré dans les figures 2.3 et 2.4. La sonde A (sonde circulaire) a une surface trop importante au regard de la taille du composant et récupère donc les émissions provenant à la fois des opérations de la mémoire, mais aussi des signaux transitant par les fils de connexion (*bondings*) qui peuvent être bien plus importantes et donc noyer la partie utilisable de la signature (voir figure 2.3).

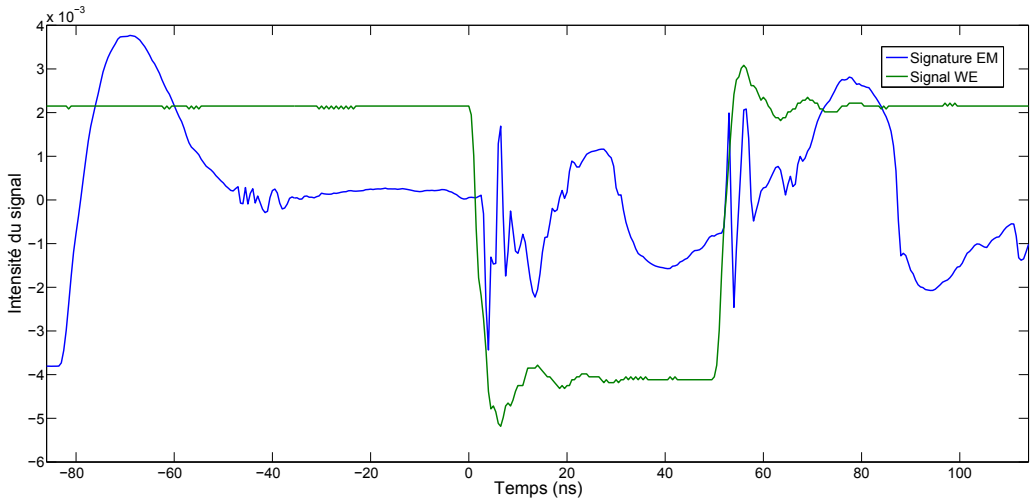

FIGURE 2.3 – Émissions électromagnétiques d'une opération d'écriture dans une TAS-MRAM et signal $\overline{WE}$ captées par la sonde circulaire

La seconde sonde (sonde B) dont la surface est moins importante et la géométrie permet de capter les ondes électromagnétiques parallèles au plan de la mémoire et de manière plus localisée. En faisant varier la position spatiale de la sonde, il est possible de repérer des zones dans lesquelles les signatures des opérations de la mémoire sont suffisamment importantes pour permettre l'analyse des données

écrites ou lues et des adresses mises en jeu lors de l'opération. La figure 2.4 montre la signature d'une écriture mesurée par cette sonde.

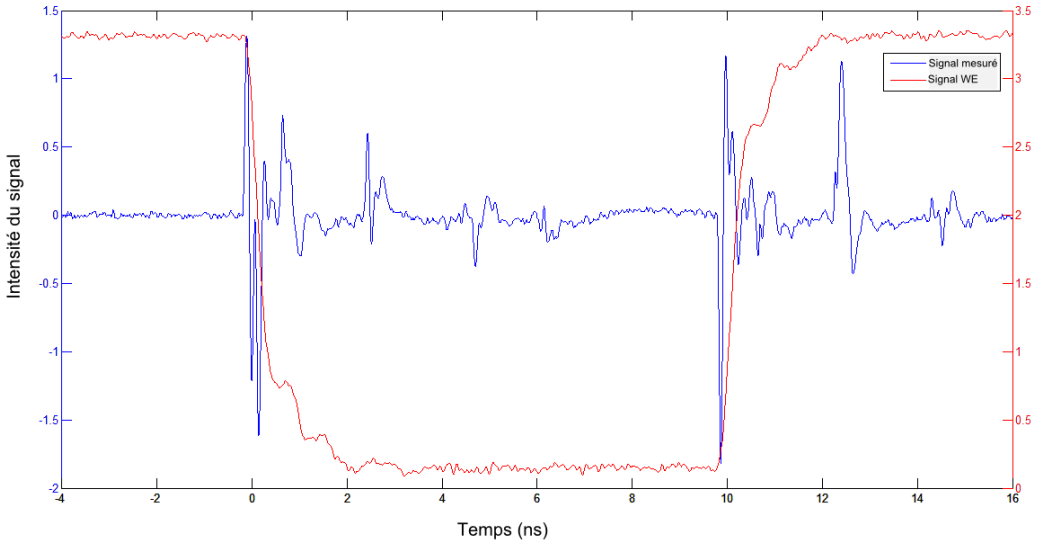

FIGURE 2.4 – Émissions électromagnétiques d'une opération d'écriture dans une TAS-MRAM et signal $\overline{WE}$

Identification des signatures de la TAS-MRAM

En observant les signatures d'une opération d'écriture récupérée par la sonde A sur la figure 2.5, on peut observer 4 phases :

Une opération d'écriture d'un bit sur une TAS-MRAM se déroule en trois étapes (voir paragraphe 1.2), la montée en température du point mémoire, la création du champ magnétique et le refroidissement sous champ.
L'écriture d'un octet, 8 bits, se fait en une seule opération durant laquelle les 8 bits sont adressés en même temps. La mémoire est conçue pour que tous les bits d'un même octet soient sous la même ligne de courant. Une seule impulsion de la ligne champ permet donc d'écrire les 8 bits.

Cependant, l'écriture de '1' (résistance basse - Rmin du point mémoire) et de '0' (résistance haute - Rmax du point mémoire) impose l'écriture avec des champs sens opposés, ce qui se traduit par des courants dans les lignes de signes opposés. Pour écrire une donnée contenant des '1' et des '0', il faut donc effectuer deux cycles d'écriture :

— Une première écriture pour mettre tous les bits de l'octet à '0' qui nécessite une synchronisation sur le front descendant du signal $\overline{WE}$
— Une seconde écriture pour mettre les bits sélectionnés à '1' qui est elle synchronisée sur le front montant du signal $\overline{WE}$

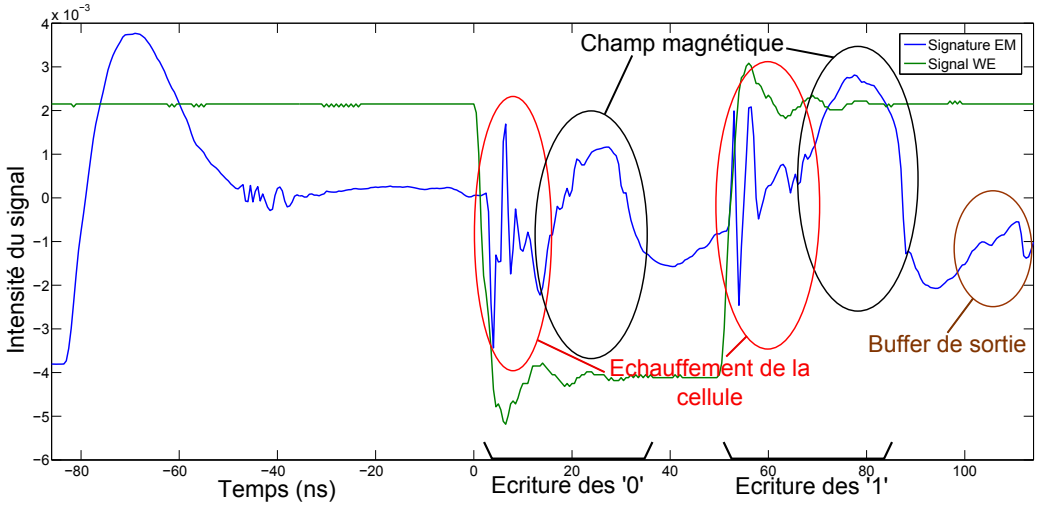

FIGURE 2.5 – Analyses des émissions électromagnétiques des différentes phases d'un opération d'écriture dans une TAS-MRAM

Il y a donc quatre phases pour une opération d'écriture d'un octet : deux échauffements de la cellule et deux impulsions de courant dans les lignes de champ. Ces quatre phases peuvent être identifiées dans la signature lors de l'utilisation du premier type de sonde (circulaire). Sur la figure 2.5, on voit les pics d'émissions EM correspondants au chauffage et à la création du champ magnétique.

Pour pouvoir retrouver des informations à partir de ces signatures, il n'est pas indispensable de mesurer tous ces pics. En effet, le champ magnétique est généré une seule fois quel que soit la donnée écrite, son amplitude reste donc toujours la même et n'est donc pas porteuse d'information. Un troisième pic peut être observé il correspond à l'écriture des données dans les buffers de sorties. En effet dès qu'un octet est écrit les données sont copiées.

La figure 2.5, acquise avec la sonde A, permet d'identifier distinctement les phases de l'opération d'écriture de manière globale. Pour rentrer dans le détail et pouvoir étudier plus finement les émissions électromagnétiques, il est cependant nécessaire d'utiliser la sonde B qui est plus petite et permet une meilleure sélectivité.

Si on analyse la figure 2.4, acquise avec la sonde B, on remarque que le pic correspondant au chauffage des cellules mémoires ainsi que celui du chargement des buffers de sorties sont bien visibles alors que les pics des lignes de champs magnétiques ne signent pas. Cette sonde mesure les lignes de champs parallèles au plan mémoire, ce qui permet de ne sélectionner qu'une partie du signal.

2.2 Recherche des signatures des poids de Hamming

Les émissions électromagnétiques du circuit peuvent potentiellement donner des informations sur le type d'opération effectué, les données manipulées et sur les adresses utilisées. Dans cette section, l'étude se concentre sur les opérations d'écriture, le but étant dans un premier temps de retrouver la donnée écrite à partir des signatures électromagnétiques. L'hypothèse émise est que l'intensité des émissions électromagnétiques lors de la phase de chauffage de l'écriture des '1' est dépendante du poids de Hamming des données écrites.

Définition : On appelle poids de Hamming d'un mot binaire le nombre de bit à '1' et distance de Hamming le nombre de bits différents entre deux mots.

Analyse préliminaire

Avant de pouvoir retrouver les poids de Hamming des données à partir des signatures électromagnétiques, il convient de vérifier la validité de l'hypothèse. Pour cela une analyse préliminaire d'un jeu de signatures a été effectuée. Ce jeu de signatures est composé 25600 signatures soit 100 mesures obtenues par l'écriture de chaque donnée (de 0x00 à 0xFF). Pour ces signatures, les mesures ont été effectuées dans les mêmes conditions, même sonde, même adresse, même position spatiale de la sonde le but étant de mettre en évidence l'effet du changement de donnée écrite sur la signature. Pour chaque donnée écrite, les 100 signatures sont moyennées pour éliminer le bruit. Il y a en définitive 256 courbes, une pour chaque donnée de 0x00 à 0xFF.

Ces 256 courbes ont ensuite été groupées et moyennées pour chaque poids de Hamming. La figure 2.6 montre la superposition des 9 moyennes des signatures, pour chaque poids de Hamming. On constate qu'en moyenne les courbes sont superposées excepté pendant la phase d'échauffement et l'écriture des buffers de sortie

L'hypothèse selon laquelle les signatures électromagnétiques sont dépendantes du poids de Hamming des données écrites semble donc se vérifier, en particulier dans les zones identifiées dans le paragraphe précédent, à savoir l'échauffement pendant la phase d'écriture des '1' et l'envoi des données dans les buffers de sortie. Sur la figure2.7 est représenté l'écart-type entre ces 9 courbes, on constate que les zones correspondent à l'échauffement et aux buffers. Une zone supplémentaire apparait cependant, la zone correspondant l'échauffement des cellules mémoires pour l'écriture des '0'.

Cette analyse préliminaire simple appelée *simple power analysis* (SPA) montre qu'il existe bien des différences observables en terme d'intensité de la signature électromagnétique et le poids de Hamming de la donnée manipulée, cependant cette simple analyse ne permet pas de retrouver de manière fiable le poids de Hamming. Pour pouvoir le déterminer, il est nécessaire d'utiliser d'autres outils.

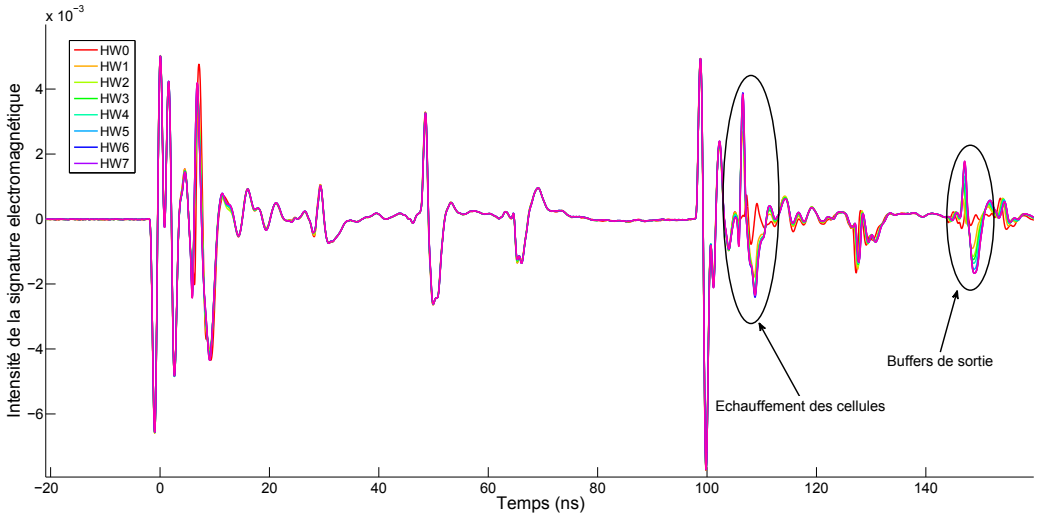

FIGURE 2.6 – Moyenne des signatures électromagnétiques en fonction du poids de Hamming

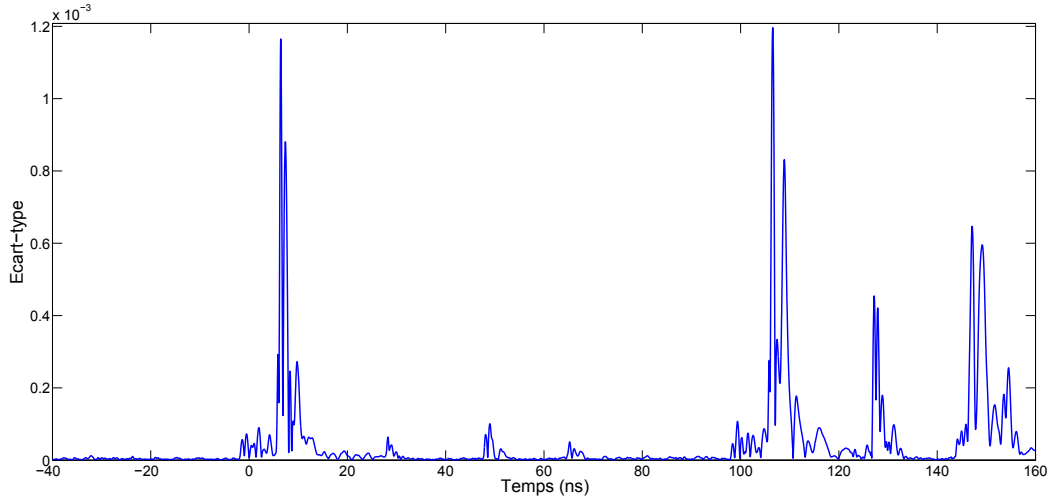

FIGURE 2.7 – Écart-type des moyennes des signatures électromagnétiques en fonction du poids de Hamming

Analyse en "boîte grise"

L'analyse dite en "boîte grise" suppose que l'attaquant dispose d'un composant à partir duquel il est capable de générer des courbes de références à comparer au composant qu'il attaque. Il peut ainsi avoir par exemple accès à l'amplitude moyenne des signatures électromagnétiques pour chaque donnée. La même méthodologie que

l'analyse préliminaire effectuée en 2.2 est mises en place : un jeu de 25600 courbes est organisé par poids de Hamming et moyenné par groupe. Nous utiliserons deux types d'analyse qui reposent sur deux distingueurs.

Définition : Un distingueur est un outil statistique qui permet de faire ressortir une hypothèse en utilisant des observables (ici les émissions électromagnétiques) et des prédictions (ici les poids de Hamming des données pour chaque signature).

Recherche des poids de Hamming par analyse des moyennes

La différence de moyenne est le distingueur le plus simple à mettre en place, si des écarts sont visibles sur les courbes alors une étude de la moyenne des courbes peut permettre de retrouver le poids de Hamming en les comparant.

La figure 2.8 représente les moyennes des signatures A_x pour chaque courbe (représentant chacune l'écriture d'une donnée x), classées par poids de Hamming h. La moyenne de l'amplitude en émission électromagnétique A_x de l'écriture de chaque donnée x est représentée par une barre verticale. Chacun des carrés noirs représente la moyenne de l'amplitude des émissions pour l'ensemble des courbes associées à un poids de Hamming ApH_h. On constate que s'il y a une tendance croissante à l'intensité des émissions électromagnétiques, il y a tout de même deux éléments qui compliquent l'analyse.

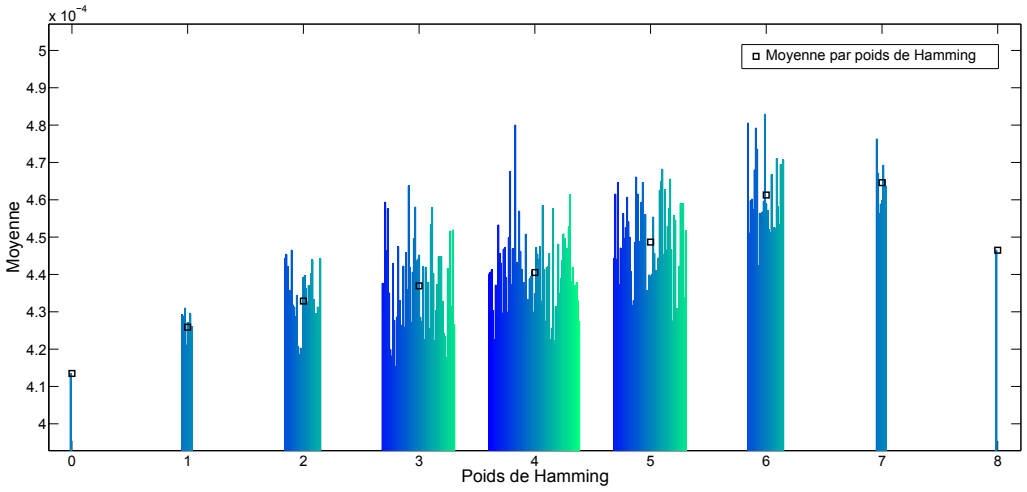

FIGURE 2.8 – Émissions électromagnétiques moyennes mesurées pendant l'écriture classées par poids de Hamming

On constate d'une part que l'intensité moyenne de la signature du poids de Hamming $h = 8$, qui correspond à la donnée 0xFF, est plus faible que celle de poids de Hamming inférieurs. Plus précisément, elle se situe entre les intensités moyennes des signatures des données de poids de Hamming $h = 4$ et $h = 5$. Ce résultat

n'est pas en accord avec l'hypothèse, en effet ce poids de Hamming correspond au nombre maximum de '1' dans une donnée et donc au maximum de points mémoires à monter en température.

De plus, les extremums d'amplitude dans la même catégorie de poids de Hamming sont plus importants que les écarts entre les moyennes de chacun. Un classement en fonction de la moyenne ne serait donc pas significatif et ne permettrait a priori pas de retrouver le poids de Hamming d'une signature quelconque.

Méthodologie : L'ensemble des courbes représentées dans la figure 2.8 sera la référence. Sur la signature d'une donnée x (inconnue) quelconque mesurée expérimentalement, l'amplitude moyenne A_x est calculée et est comparée aux amplitudes moyennes des émissions pour l'ensemble des courbes associé aux poids de Hamming ApH_h. On recherche alors ApH_{h*} tel que $ApH_{h*} = \min_h |A_x - ApH_h|$. h^* est alors identifié comme le poids de Hamming associé à la courbe de la donnée x.

Résultats : En utilisant cette méthodologie, le poids de Hamming est retrouvé pour 22% des données. Elle ne permet donc pas de retrouver les poids de Hamming avec un taux de réussite suffisant et il est nécessaire d'utiliser d'autres méthodes. Il est cependant possible d'améliorer ce résultat en ne sélectionnant que les zones avec un fort écart-type mises en évidence dans le paragraphe 2.2, le taux de bonnes hypothèses de poids de Hamming ne dépasse cependant pas 48% ce qui reste encore insuffisant.

Analyse à l'aide du coefficient de corrélation de Pearson

Un autre distingueur possible est le calcul du coefficient de corrélation de Pearson, ce coefficient constitue une mesure de l'intensité de liaison linéaire entre deux variables.

Définition : Le corrélation de Pearson entre deux variables aléatoires X et Y, Cor(X,Y) se définit comme :

$$\mathrm{Cor(X, Y)} = \frac{\mathrm{Cov}(X, Y)}{\sqrt{\mathrm{Var}(X).\mathrm{Var}(Y)}} \tag{2.3}$$

Avec Cov(X,Y), la covariance des variables X et Y et Var(X), Var(Y) les variances de respectivement X et Y. Deux variables pour lesquelles il existe une relation affine ont une corrélation égale à 1.

En se basant sur la même méthodologie que pour la moyenne, c'est-à-dire en calculant le coefficient de corrélation entre une signature et la moyenne des signatures dans chaque catégorie Hamming. On obtient alors un taux de bonnes hypothèses de l'ordre de 42%.
Ce résultat n'est pas suffisant pour être utilisé en l'état et il faut pouvoir affiner

la méthode pour obtenir un taux de bons résultats suffisamment important pour permettre une utilisation expérimentale.

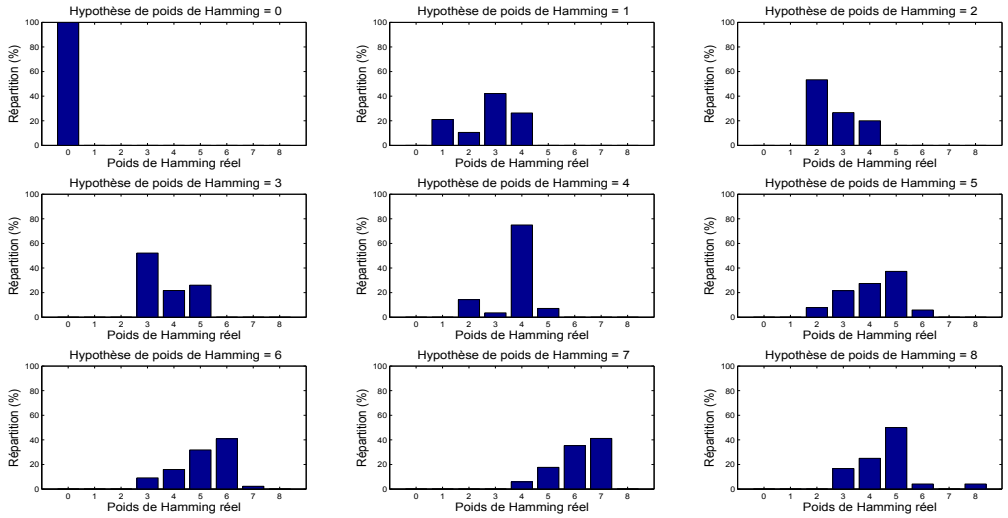

FIGURE 2.9 – Répartition des hypothèses de poids de Hamming par corrélation

La figure 2.9 représente la répartition des hypothèses de poids de Hamming en fonction de poids de Hamming réel. Chaque case est une hypothèse de poids de Hamming, les abscisses représentent les poids de Hamming réels et les ordonnées la répartition de ces poids de Hamming. On remarque que pour chaque poids de Hamming, la bonne hypothèse est majoritaire dans sept cas sur neuf, dans le cas $h = 1$ et $h = 8$ elle est même largement minoritaire. Cependant, seuls les poids de Hamming $h = 0$ et $h = 4$ donnent un résultat exploitable, toutes les signatures associées à un poids de Hamming $h = 0$ et 75% des 28 associées à $h = 4$ sont correctes.

Conclusion

L'analyse en "boite grise" des courbes avec pour objectif de retrouver les poids de Hamming des données manipulées ne donne pas de résultats avec un taux de réussite suffisant en utilisant les distingueurs présentés dans cette section pour une donnée quelconque. Cependant dans le cas de la corrélation de Pearson, les courbes ayant été associées à un poids de Hamming $h = 0$ et $h = 4$ ont un poids de Hamming effectivement égale à 0 et 4. Une partie des résultats obtenue par ce distingueur est donc utilisable expérimentalement.

Analyse "boite noire" - Recherche par partitionnement K-means

Les résultats précédents nécessitent d'utiliser des courbes de références pour générer les moyennes des signatures pour chaque poids de Hamming, cependant un attaquant n'a pas forcement accès à ce type d'information. Ce type d'analyse est possible avec seulement l'accès à des traces d'émission.

Détail de l'algorithme

Une des méthodes d'analyse proposée est le partitionnement par k-means. Il permet de diviser un groupe d'éléments en k partitions, le critère de sélection des partitions est la minimisation des distances entre le centre de chaque partition (centroïde) et les éléments qu'elle contient. Dans notre cas, le groupe d'éléments correspond au jeu de courbes à notre disposition que l'on va diviser en 9 partitions correspondant quand à elles aux poids de Hamming possibles.

Pour cela ,chaque courbe sera projetée dans un espace de dimension égale au nombre de points de la courbe pour n'être plus représentée que par un seul point. Dans cette représentation, la distance entre les courbes est vue comme la distance euclidienne entre ces points. L'algorithme du k-means se compose des quatre étapes suivantes qui se répètent jusqu'à ce qu'une configuration stable soit atteinte :

Choix aléatoire de k centroïdes;
tant que *les positions des centroïdes évoluent* **faire**
- Calcul de la distance entre chaque élément et chaque centroïde;
- Création des partitions : chaque élément est placé dans la partition du centroïde dont il est le plus proche;
- Définition des nouveaux centroïdes (les barycentres des partitions);

fin

Algorithme 1 : Algorithme du k-means

Cet algorithme est très dépendant des conditions initiales choisies, en effet des configurations stables (avec des centroïdes qui n'évoluent plus) locales peuvent être rencontrées ce qui a pour conséquence de générer des partitions différentes à partir du même ensemble de départ [40]. Pour pallier cette instabilité, l'algorithme est itéré plusieurs fois (de 20 à 15000 fois dans les tests effectués) et à chaque itération trois critères sont évalués pour choisir la meilleure configuration de départ. Ces critères sont :

— La distance moyenne des signatures au centre des partitions
— La distance moyenne des partitions entre elles
— Le nombre d'éléments dans chaque partition

Ce troisième critère est basé sur la distribution connue du nombre d'éléments théoriques pour chaque poids de Hamming. En effet pour des données de 8 bits, on retrouve la distribution du tableau 2.1 :

Poids de Hamming	0	1	2	3	4	5	6	7	8
Nombre d'éléments	1	8	28	56	70	56	28	8	1

TABLE 2.1 – Distribution des données par poids de Hamming

En calculant la différence entre les distributions obtenues en sortie de l'algorithme et cette distribution théorique on obtient un critère pour évaluer la qualité des conditions initiales sélectionnées et ainsi pouvoir choisir la plus à même se rapprocher des véritables poids de Hamming.

Les données sont classées selon les trois critères et la mieux classée est conservée. Une fois les partitions définies, il faut identifier quel poids de Hamming correspond à quelle partition.
Pour cela les partitions sont classées par nombre d'éléments : les deux ayant le plus petit nombre d'éléments sont identifiées comme étant les poids de Hamming 0 et 8, les deux suivantes comme étant les poids de Hamming 1 et 7 et ainsi de suite jusqu'au poids de Hamming 4 qui correspond à la partition ayant le plus d'éléments. On obtient donc 4 paires de partitions et la partition du poids de Hamming 4. L'étude de la moyenne du paragraphe 2.2 a montré la tendance croissante des moyennes globales en fonction du poids de Hamming, en se servant de ce résultat on compare la moyenne dans chaque paire de partitions, la plus faible correspond au poids de Hamming le plus faible.

En appliquant cet algorithme, le taux de bons résultats est cependant assez proche des tests décrits dans les paragraphes 2.2 et 2.2, entre 10 et 40 % avec les meilleurs résultats sur les pics à fort écart type, en particulier le pic de chargement des *buffers*. Ces résultats ne permettent cependant pas de retrouver des informations de manière fiable.

Amélioration de la méthode du k-means

Une amélioration de ce procédé a donc été conçue. Elle consiste à étudier successivement des petites portions de ces intervalles (d'une longueur de 1 à 5 ns) plutôt que d'étudier des intervalles importants de courbes. Ainsi pour chaque donnée l'hypothèse de poids de Hamming majoritaire est utilisée.

Pour chaque portion k de l'intervalle et pour chaque donnée D, un poids de Hamming H_{kD} est estimé à partir de l'algorithme du k-means (*algorithme 1*) et de l'identification des partitions. On obtient alors un tableau de k lignes et D colonnes contenant les résultats trouvés par l'algorithme. Par ligne, on compte alors le nombre d'occurrences de chaque poids de Hamming. On en déduit le pourcentage $T(H_D)$ de chaque poids de Hamming H pour chacune des données D. Le poids de Hamming fournit par ce nouvel algorithme pour la donnée D est alors appelé H^*_D tel que $T(H^*_D) = \max(T(H_D))$. $T(H^*_D)$ représentera notre indice de confiance du résultat.

Cette amélioration de l'algorithme permet d'augmenter de manière peu significative le taux de réussite de l'estimation des poids de Hamming variant entre 40 et 45 % sur le pic le plus sensible identifié plus haut. La figure 2.10 montre la répartition des résultats de l'algorithme en fonction des poids de Hamming réels.

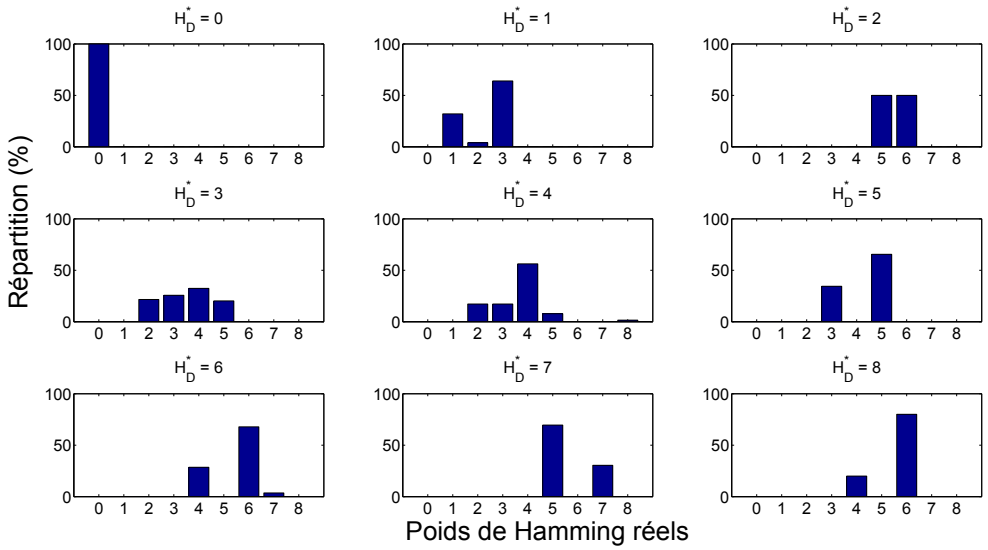

FIGURE 2.10 – Répartition des hypothèses de poids de Hamming en utilisant l'algorithme du K-Means

Seul le poids de Hamming 0 donne un résultat exploitable, les autres poids de Hamming sont au mieux exacts dans 70% des cas pour H_D^*6 et H_D^*5.

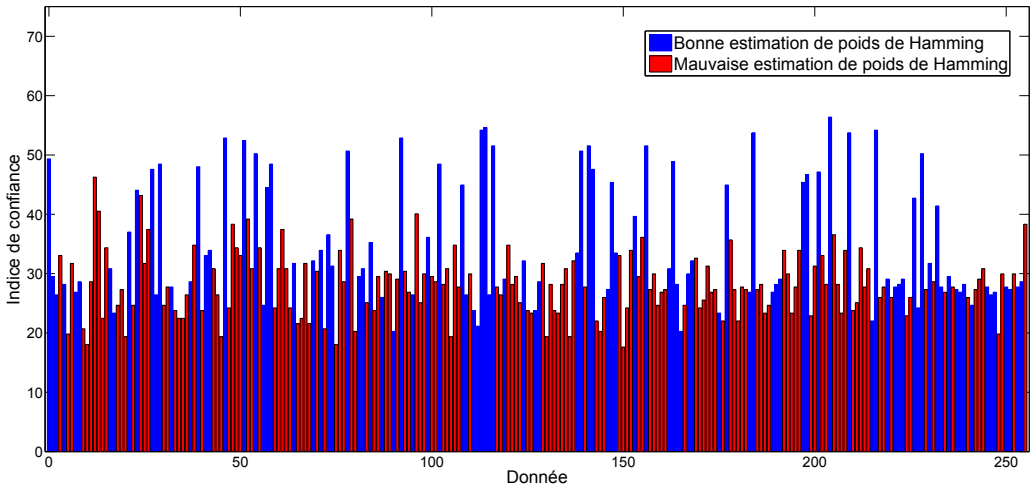

FIGURE 2.11 – Résultats de l'algorithme du K-means amélioré en fonction de l'indice de confiance des résultats

Cependant l'analyse de l'indice de confiance T_{hDi} de chacun de ces résultats apporte de nouvelles informations comme le montre la figure 2.11. Dans ce graphe, les lignes bleues représentent les données ayant bénéficié d'une bonne estimation de poids de Hamming tandis que les lignes rouges représentent les données avec une mauvaise estimation. On constate que les données avec le plus haut indice de confiance sont en moyenne mieux estimées par l'algorithme amélioré.

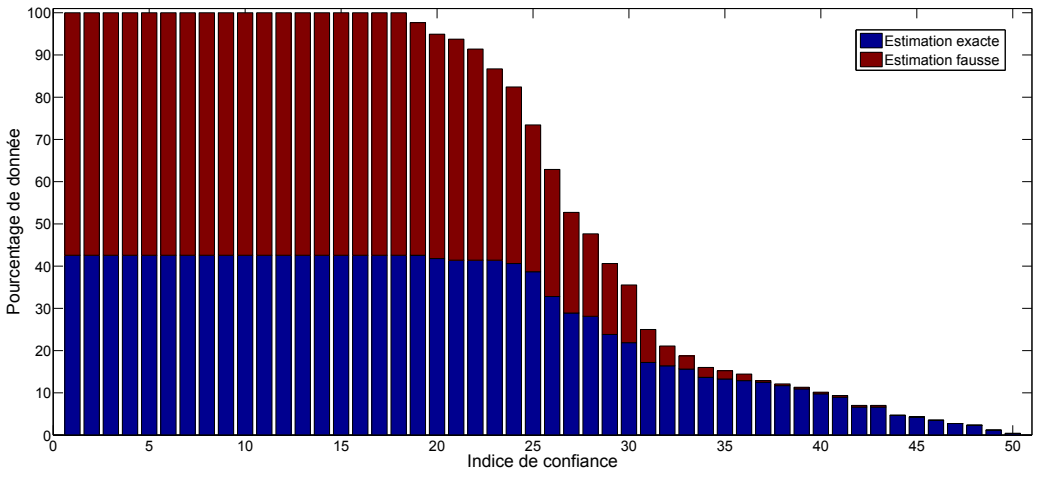

FIGURE 2.12 – Pourcentage de bonnes estimations en fonction du poids de Hamming

La figure 2.12 montre un peu plus en détail l'évolution des bonnes estimations en fonction de l'indice de confiance. On constate qu'à partir d'un indice de confiance de 25, les bonnes estimations deviennent majoritaires. Le taux de bonnes réponses croit ensuite linéairement jusqu'à ce que l'indice de confiance atteigne 36 à 40. Au-delà d'un indice de confiance de 45 le pourcentage de bonnes réponses varie entre 96% et 100%.

En choisissant un seuil d'indice de confiance adéquat, il est donc possible de sélectionner les estimations avec le taux d'erreurs adapté Cependant les variations dues aux conditions initiales de l'algorithme du k-means peuvent faire varier les indices de confiances de 5% à 10 %.

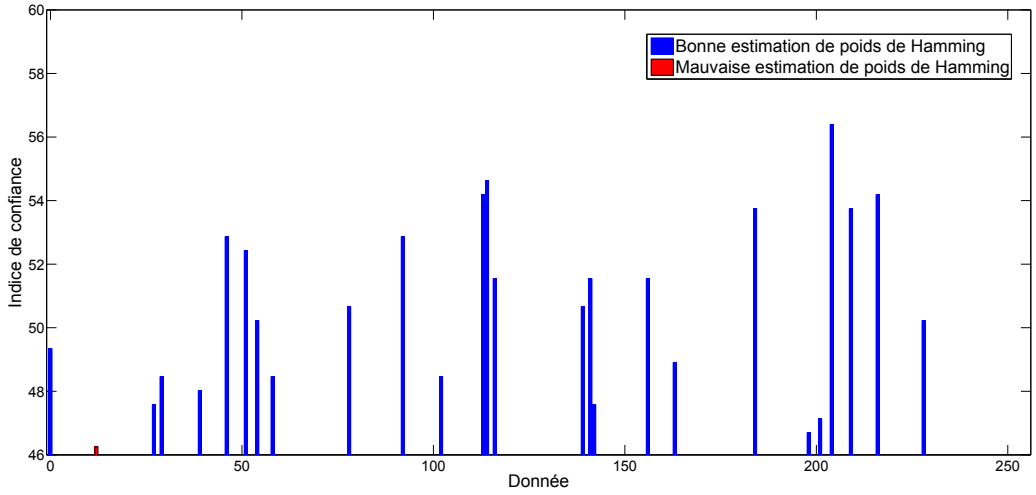

FIGURE 2.13 – Résultat de l'amélioration de l'algorithme du K-means pour les plus hauts indices de confiance

Comme le montre la figure 2.13, en ne sélectionnant que les données ayant un indice de confiance dans les 10 % supérieur le taux d'erreurs ne dépasse pas 4%. Dans le cas présenté, sur les 27 données sélectionnées 26 ont reçu une bonne estimation du poids de Hamming.

En relançant plusieurs fois l'algorithme avec des paramètres différents (taille et nombre des portions d'intervalle) et en agrégeant les résultats il est possible de retrouver les poids de Hamming de 40 données avec une certitude 95%.

2.3 Conclusion

Les composants MRAM au même titre que les autres composants électroniques émettent des ondes électromagnétiques lorsqu'ils effectuent des opérations (lecture et écriture). L'analyse de ces émissions permet de décomposer les différentes opérations effectuées (chauffage, champs magnétiques, etc.) et de déterminer les paramètres des opérations (données écrite ou lu et adresses). Ce chapitre s'est intéressé à l'analyse des ondes rayonnées pendant les opérations d'accès à la mémoire MRAM et plus particulièrement aux données écrites. Il a été montré que conformément à l'hypothèse de départ, le poids de Hamming est corrélé aux émissions électromagnétiques. Cependant, l'extraction des poids de Hamming à partir d'une signature quelconque nécessite des connaissances sur le composant et une méthodologie adaptée.

En ayant une connaissance basique du fonctionnement de la mémoire, à savoir la succession des phases de l'opération d'écriture et plus particulièrement l'instant de la copie des données dans le buffer de sortie, il est possible de retrouver les poids de Hamming de 40 données avec un taux de réussite de plus de 95%.
Ce type de résultat est particulièrement intéressant dans l'hypothèse où ce nouveau type de mémoire MRAM est embarquée pour des applications cryptographiques pour stocker ou transférer des clés. En effet la connaissance des poids de Hamming des clés utilisées dans un algorithme de chiffrement tel que l'AES est une faille de sécurité importante.
Cependant, les tests ont été effectués sur des circuits MRAM indépendants et sans protections particulières vis-à-vis d'analyses d'émissions électromagnétiques. Une mémoire MRAM embarquée sur un composant sécurisé, avec des contre-mesures adaptées, n'aurait pas nécessairement le même niveau de faiblesse.

Chapitre 3

Attaques physiques sur les mémoires magnétiques : champ magnétique statique

Sommaire

3.1 Introduction

Comme indiqué dans la partie 1.2 les matériaux ferromagnétiques réagissent en présence d'un champ magnétique, c'est ce principe qui est à la base des mémoires à retournement induit par un champ magnétique (FIMS), mais c'est aussi un des inconvénients inhérents aux MRAM : placées dans un environnement soumis à un champ magnétique trop important, leur fonctionnement est perturbé. L'étude de ces perturbations ainsi que les différents moyens de les limiter sont l'objet principal dans ce chapitre.

La donnée stockée dans une MRAM est dépendante des orientations relatives des moments magnétiques de ses couches de stockage et de référence. La couche de référence est par définition beaucoup moins sensible au champ magnétique, car elle doit rester stable même lors des opérations d'écriture (voir paragraphe 1.2), c'est donc d'abord au niveau de la couche de stockage que le champ magnétique externe perturbe une MRAM.

Forme du champ magnétique et géométrie de la mémoire

L'orientation des lignes de champs générées est un paramètre capital quant aux effets que peut avoir l'aimant permanent sur les MRAM. En effet, comme le montre l'équation 1.10, l'effet du champ sur l'aimantation est maximal lorsqu'il est aligné ou anti-aligné avec les moments magnétiques. D'autre part, toutes les orientations de moments magnétiques ne sont pas stables pour les couches de stockage et de référence dans la mémoire, les moments magnétiques s'alignant préférentiellement sur l'axe facile de la couche magnétique. L'étude des effets d'un champ externe sur une MRAM a été faite dans deux cas distincts : avec les lignes de champs dans le sens des moments magnétiques des couches d'aimantation, et perpendiculairement à ces moments (figure 3.1).

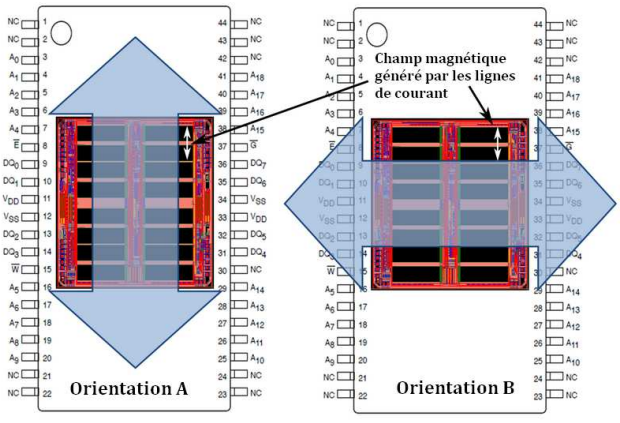

FIGURE 3.1 – Orientation A : champ magnétique suivant les moments magnétiques ; Orientation B : champ magnétique perpendiculaire aux moments magnétiques

Le champ généré par les lignes de courant du circuit est également parallèle à ces moments magnétiques, le champ magnétique externe est donc additionné ou soustrait aux champs internes dans le cas parallèle.

Le champ magnétique utilisé pour perturber le circuit de la MRAM est généré à l'aide d'un aimant permanent en néodyme-fer-bore (voir description du banc en 1.4). L'utilisation d'un aimant permanent permet d'obtenir des champs magnétiques dont l'intensité dépend uniquement de la distance à l'aimant. La caractérisation en champ magnétique permanent a été faite en deux étapes, dans un premier temps le champ magnétique généré par l'aimant est mesuré à l'aide d'une sonde à effet Hall, puis dans un second temps la forme et de l'intensité du champ magnétique sont simulées pour confirmer la précision des mesures. Les champs mesurés expérimentalement au voisinage de l'aimant permanent atteignent un maximum de 320 Oe. La simulation de ce champ s'appuie sur une expression analytique du champ magnétique généré par un aimant parallélépipédique [60]. Cette vérification est nécessaire, car pour des champs élevés, une variation de distance de quelques dizaines de micromètres engendre une variation de champ magnétique de plus d'une dizaine d'Oersted. Pour conserver un maximum de précision, seules les mesures correspondantes à un champ inférieur à 200 Oe sont exploitées, ce qui est suffisant pour la majorité des environnements. En comparaison, l'ICNIRP (International Commission on Non-Ionizing Radiation Protection) recommande une limite équivalente à 10 Oe [51] pour l'utilisation de pacemakers.

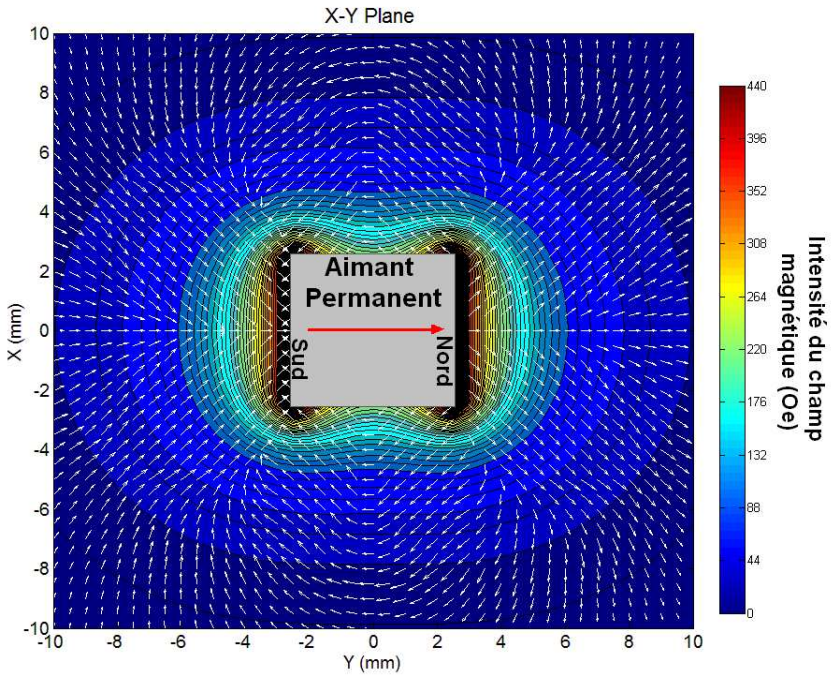

FIGURE 3.2 – Simulation de lignes de champ générées par l'aimant permanent en fonction de la distance et intensité du champ magnétique associée

L'aimant permanent utilisé est un dipôle magnétique, c'est-à-dire que ses lignes de champ partent du pôle nord magnétique pour aller au pôle sud. En plaçant le circuit entre ces pôles, le champ est, avec une bonne approximation, dans le plan de la mémoire et son intensité est fonction de la distance entre l'aimant et le circuit. Cette approximation est d'autant plus vraie que la distance est grande, en effet comme le montre la figure 3.2 en s'éloignant de l'aimant la zone dans laquelle les lignes de champ sont parallèles à l'aimant est plus importante.

Empilement magnétique d'un point mémoire

L'empilement de la révision G décrit en figure 3.3 est composé de :

- Platine-manganèse (PtMn) : un matériau antiferromagnétique utilisé dans la couche de référence et qui a une température de blocage de 350°C.
- Cobalt-fer (CoFe) : un matériau ferromagnétique avec une forte aimantation.
- Cobalt-fer-bore (CoFeB) : un matériau magnétique amorphe. Il est utilisé pour améliorer la cristallisation du MgO (ce qui augmente sa résistance tunnel magnétique - TMR).
- Ruthénium (Ru) : un matériau non magnétique qui sert à séparer les deux couches ferromagnétiques qui composent le SAF.
- Fer-manganèse (FeMn) : un matériau antiferromagnétique qui est utilisé pour verrouiller l'orientation de la couche de référence.
- Nickel-fer (NiFe) : matériau qui sert à faire la liaison entre le CoFe de la couche de référence et le FeMn de verrouillage.
- Tantale (Ta) : un matériau non magnétique utilisé pour améliorer la stabilité de l'empilement

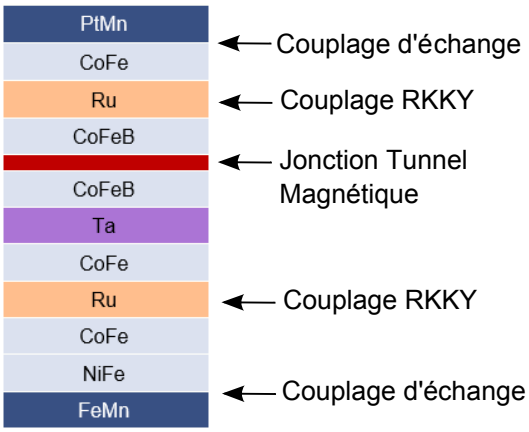

FIGURE 3.3 – Empilement magnétique d'une TAS-MRAM de révision G avec les différents couplages impliqués

La couche de stockage est composée d'une couche de CoFeB à l'interface avec la barrière en MgO, cela permet de maximiser la TMR. En effet, le CoFeB est structure amorphe ce qui n'interfère pas avec la structure cristalline cubique centrée de la couche de MgO. La triple couche CoFe/Ru/CoFe est un antiferromagnétique synthétique, l'utilisation de CoFe cristallin plutôt que du CoFeB amorphe permet un meilleur couplage RKKY et donc une couche de stockage plus stable lorsque l'empilement n'est pas chauffé. La couche tantale (Ta) est utilisée pour la construction de l'empilement. En effet lors de la phase de recuit de la fabrication de l'empilement, elle attire les atomes de bore. En outre, elle permet d'améliorer l'interface entre le CoFe et le CoFeB qui ont des textures très différentes.

Les orientations des moments magnétiques de chaque couche sont garanties par deux types de couplage, le couplage RKKY (voir paragraphe 1.2) et le couplage d'échange (voir paragraphe 1.2). Le couplage d'échange se fait à l'interface d'une couche ferromagnétique et d'une couche antiferromagnétique or les couches antiferromagnétiques sont très peu sensibles aux champs externes, car leur aimantation globale est nulle. C'est-à-dire que même en présence d'un champ magnétique externe intense en mesure de retourner l'aimantation de la couche ferromagnétique, et donc de surpasser le couplage d'échange, dès que ce champ disparait, les couches retrouvent leurs aimantations initiales.

3.2 Effet des champs magnétiques statiques sur les MRAM

Mémoire au repos

On considère comme étant au repos une mémoire sous tension lorsqu'aucune opération n'est en cours. Dans ce cas, le couplage d'échange entre la couche de stockage et la couche antiferromagnétique est maximum et des champs magnétiques directement opposés au moment magnétique de la donnée stockée de l'ordre 200 Oe ne perturbent pas la mémoire. Le matériel disponible pour les caractérisations ne permet pas de mesurer avec précision des champs magnétiques d'intensités supérieures, cependant les estimations faites grâce aux simulations (voir section 3.1) montrent qu'un champ de l'ordre de 500 Oe ne perturbe pas non plus les données stockées.

Opérations de lecture

Lorsqu'une opération de lecture est en cours sur un empilement magnétique, un courant le traverse pour permettre de mesurer sa résistance. Ce courant provoque un échauffement de l'ordre de 2,5°C (non significatif au regard des 180°C de l'échauffement lors de l'écriture)ce qui ne modifie pas la sensibilité du champ magnétique du point mémoire. Pourtant, des modifications non permanentes des données stockées apparaissent. En effet, on observe sur la figure 3.4 des erreurs sur la MRAM soumise à des champs magnétiques à partir de 100 Oe, mais les données redeviennent correctes lorsque la mémoire n'est plus soumise au champ.

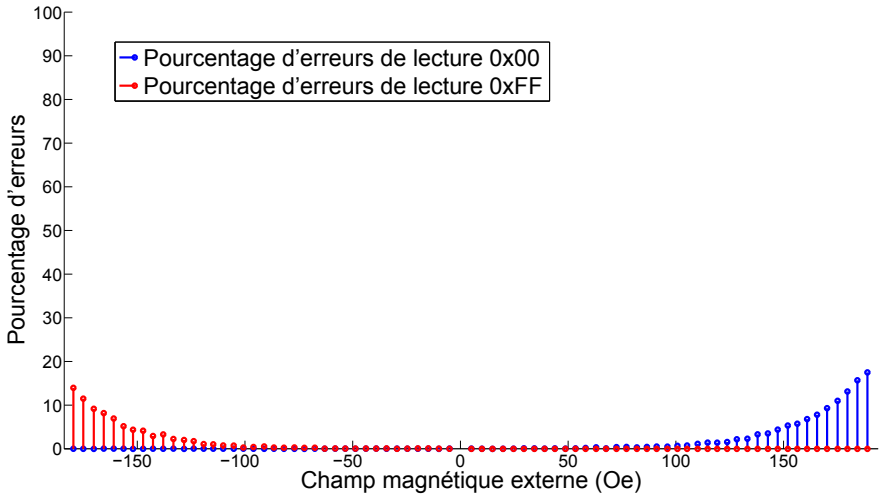

FIGURE 3.4 – Pourcentage d'erreurs pendant des opérations de lecture sous l'effet d'un champ magnétique permanent pour une TAS-MRAM de révision G

Pour rappel, la couche de stockage est un empilement antiferromagnétique syn-

thétique (SAF) dont une couche ferromagnétique est couplée à une couche d'antiferromagnétique de FeMn. Pour qu'une donnée soit perturbée, il faut que les moments magnétiques de la couche de ferromagnétique au contact avec la barrière tunnel soient inversés (voir paragraphe 1.2). Pour que ces moments magnétiques s'inversent il faut que l'intensité du champ soit assez importante pour retourner l'orientation des moments magnétiques des couches ferromagnétiques et donc de surpasser le couplage RKKY. Cependant, la couche antiferromagnétique (FeMn) reste stable même sous l'effet d'un champ magnétique intense, donc dès que le champ magnétique externe disparait, le couplage reprend le dessus et les moments magnétiques de la couche de stockage retournent dans leur état initial.

Opérations d'écriture

Lorsqu'une opération d'écriture est en cours, l'empilement magnétique est chauffé jusqu'à la température de Néel (voir paragraphe 1.2) ce qui rend le couplage d'échange inopérant. La couche de stockage est alors libre et ses moments magnétiques peuvent facilement être retournés par un champ magnétique. En fonctionnement normal il s'agit du champ magnétique généré par les lignes de courant, mais si le champ externe est assez important, en particulier s'il est supérieur à celui des lignes de courant, alors c'est ce dernier qui influencera le plus les moments magnétiques de la couche de stockage. Lorsqu'un moment magnétique est retourné, c'est l'état du point mémoire qui est modifié. Ainsi, en augmentant l'intensité du champ magnétique externe, on observe donc une proportion de plus en plus importante de points mémoires modifiée par le champ externe.

Et lorsque l'opération d'écriture se termine, les orientations sont conservées. Le refroidissement se produisant dans les mêmes conditions de champ, la couche antiferromagnétique qui assure la stabilité de la donnée se couple avec la couche de stockage en conservant la même orientation. Pour isoler au maximum les effets du champ externe, ces tests sont effectués en désactivant les codes correcteurs d'erreurs : leur effet sera expliqué dans le paragraphe 3.3.

Deux orientations de champs magnétiques ont été testées, la première avec le champ magnétique parallèle au champ magnétique généré par les lignes de courant et la seconde avec le champ magnétique externe perpendiculaire. Conformément aux résultats attendus, le premier cas perturbe beaucoup plus le fonctionnement de la MRAM. En effet, un champ externe parallèle à celui des lignes de courants de 150 Oe perturbe 99% des bits écrits quand le même champ perpendiculaire n'en perturbe que 0.3%.

Pour bien mesurer les effets des champs magnétiques externes, les tests suivants ont été effectués dans les conditions les moins favorables c'est-à-dire avec un champ parallèle aux champs des lignes de courants.

La figure 3.5 montre l'influence du champ magnétique externe sur l'opération d'écriture avec l'aimant orienté dans deux directions opposées. Dans un cas le champ magnétique perturbe les '1' et dans l'autre les '0'. Les codes correcteurs d'erreurs étant désactivés, des erreurs peuvent apparaitre même sans présence de champ ex-

terne (ou à champ très faible). On constate également que le champ magnétique perturbant les '0' réduit le nombre d'erreurs sur les '1' et vice-versa.

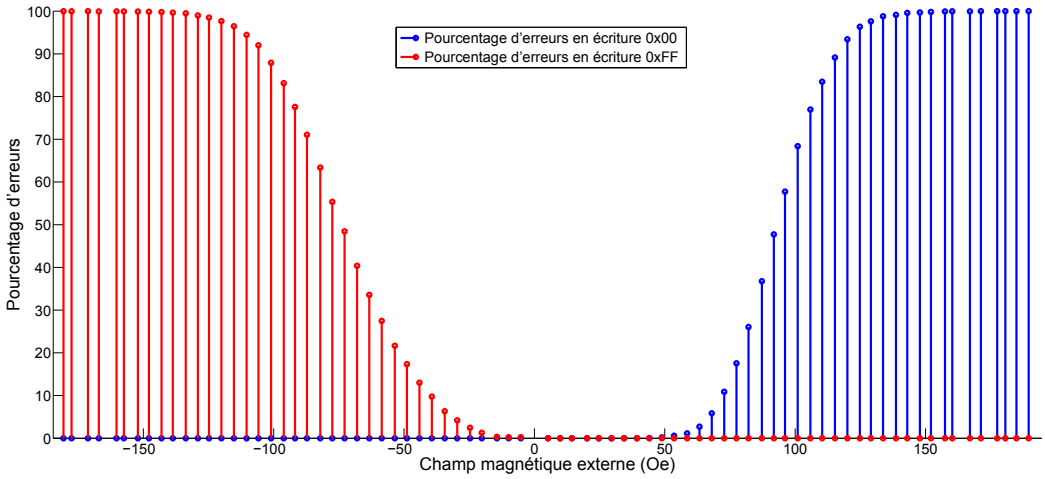

FIGURE 3.5 – Pourcentage d'erreur pendant des opérations d'écriture sous un champ magnétique externe en fonction des données pour la révision G

Cependant, il y a une importante asymétrie entre les comportements dans les champs positifs, qui correspondent ici aux champs qui perturbent les '0', et les champs négatifs. A champ magnétique externe identique, il y a un écart de l'ordre de 200 fautes qui apparait entre les deux orientations. A nombre de fautes identiques correspond un écart de l'ordre de 30 Oe entre les deux orientations. Ce comportement asymétrique relatif au mode d'écriture existe également lorsque la mémoire n'est soumise à aucun champ magnétique externe, en effet il s'agit d'un défaut inhérent à l'empilement magnétique de cette révision de la mémoire TAS-MRAM.

L'asymétrie de comportement pour l'écriture est liée à un couplage dipolaire parasite entre la couche de référence et la couche de stockage : l'aimantation de la couche de référence crée un champ qui dévie les moments magnétiques de la couche de stockage dans la direction opposée pendant les opérations d'écriture. Lorsqu'un champ magnétique externe est appliqué, cette aimantation induite par la couche de référence est amplifiée ce qui augmente la vulnérabilité de la cellule mémoire (et plus particulièrement de la couche de stockage) aux champs magnétiques externes. Ces erreurs disparaissent cependant lorsque les codes correcteurs sont activés.

Dans toutes les configurations étudiées dans ce chapitre, seules les erreurs sur les '0' pour les champs positifs et les erreurs sur les '1' pour les champs négatifs seront affichées pour améliorer la lisibilité, le nombre d'erreurs sur les '1' en champs positifs et sur les '0' en champs négatifs étant nuls.

3.3 Limitation des effets d'un champ magnétique externe sur les MRAM

Même si les champs magnétiques auxquels sont sensibles les MRAM de génération G sont suffisamment élevés pour la majorité des applications, en comparaison avec d'autres types de mémoires matures ou émergentes, cette limitation peut être un handicap notamment pour les applications dans le domaine automobile ou aérospatials dans lesquelles les circuits peuvent être soumis à des champs magnétique beaucoup plus intenses. C'est pourquoi un certain nombre d'améliorations ont été étudiées pour réduire cette sensibilité au maximum.

Amélioration de l'empilement magnétique

L'empilement des premiers échantillons (révision E) a pour défaut d'avoir un effet d'asymétrie en écriture. Cette anomalie diminue non seulement la résistance de la mémoire aux champs magnétiques externes, mais augmente également le taux d'erreurs en fonctionnement normal. Comme expliqué dans le paragraphe 3.2, cet effet est dû à l'aimantation de la couche de référence sur la couche de stockage. Pour rappel la couche de référence est un SAF, c'est-à-dire qu'elle est composée d'un empilement de deux couches ferromagnétiques séparées par une fine couche de ruthénium. Ces deux couches ont des orientations magnétiques opposées, et donc une aimantation globale nulle.

Cependant la couche de référence n'étant séparée de la première couche ferromagnétique que par la barrière tunnel de quelques nanomètres d'épaisseur, un couplage dipolaire apparait entre les deux. En ajustant l'épaisseur des couches composant la couche de référence, le champ magnétique au niveau de la couche de stockage est réduit, ce qui réduit également le couplage dipolaire parasite qu'il engendrait lors d'une écriture. Ces améliorations ont été prises en compte à partir de la révision I de la mémoire. Le résultat est un empilement mieux équilibré qui a pour effet de diminuer le taux d'erreurs.

Des tests identiques à ceux de la révision G ont été effectués pour cette nouvelle révision et l'on constate une résistance accrue aux champs magnétiques externes comme le montre la figure 3.6

Contrairement à ce à quoi l'on aurait pu s'attendre, l'asymétrie n'a pas disparu. Elle est très proche de l'asymétrie de la révision G de la MRAM avec un écart maximum entre les deux orientations de l'ordre de 45 Oe. En fait si l'empilement est optimisé pour être équilibré sans perturbation magnétique, l'ajout d'un champ externe perturbe cet équilibre. On note par ailleurs que l'asymétrie est maximale pour un champ proche de celui généré par les lignes de courant : le champ résultant au niveau de l'empilement magnétique est donc très faible et l'orientation antiparallèle est favorisée.

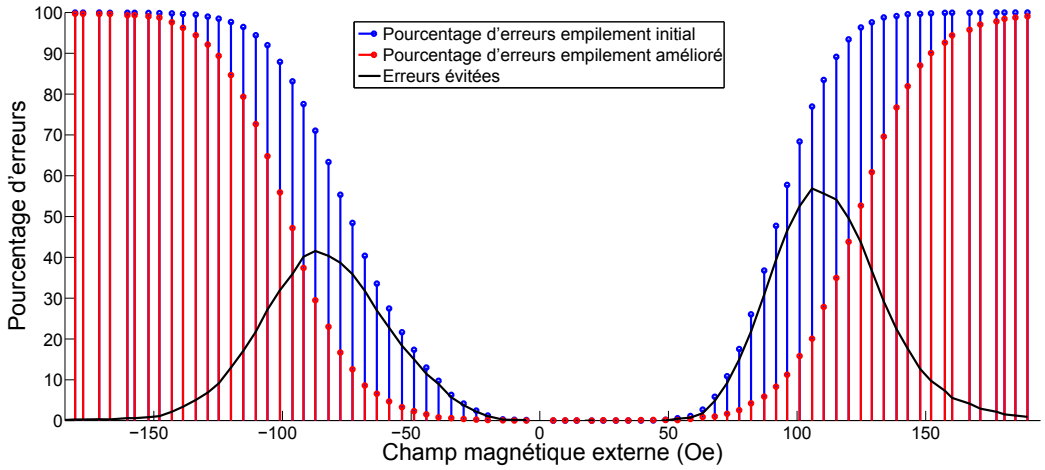

FIGURE 3.6 – Apport de la révision I (empilement amélioré) sur le taux d'erreurs lors d'opérations d'écriture sous l'effet d'un champ externe

L'augmentation de la résistance au champ magnétique externe est en revanche la même suivant les deux orientations avec un gain de 25 Oe en moyenne (voir le détail dans le tableau 3.1).

Orientation	Révision G	Révision I	Différence
A	72 Oe	94 Oe	22 Oe
B	39 Oe	68 Oe	29 Oe

TABLE 3.1 – Champs magnétiques externes pour 10% d'erreurs

Le nouvel empilement influe aussi sur la résistance aux champs externes des opérations de lecture. Le couplage dipolaire parasite qui créait l'asymétrie dans la révision G de l'empilement ayant disparu, le champ au niveau de la couche de stockage lors d'une écriture est plus important ce qui rend l'alignement de ses moments magnétiques meilleur. Une des causes possibles a cette amélioration vient du fait que tous les atomes de la couche de stockage ne s'alignent pas parfaitement avec le champ magnétique, on observe l'apparition de domaines magnétiques plus ou moins alignés : les domaines de Weiss [37]. Leurs présences réduisent la force du couplage avec la couche antiferromagnétique ce qui facilite leur retournement par un champ externe. A l'inverse, si un champ plus important est utilisé lors de l'écriture, il y a moins de domaines magnétiques et ils sont mieux alignés avec le champ des lignes de courant ce qui renforce d'autant le couplage et la résistance aux champs externes comme on peut l'observer dans la figure 3.7.

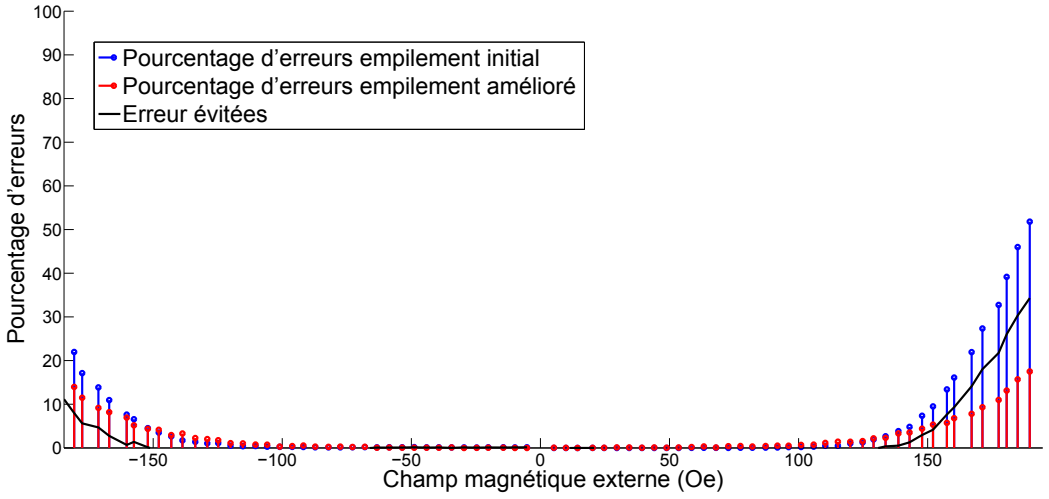

FIGURE 3.7 – Effets d'un champ magnétique externe sur l'empilement amélioré lors d'une opération de lecture

L'étude étant faite sur un nombre d'échantillons réduit, il est difficile d'isoler les causes précises de ces améliorations. Elles sont en partie dues à l'amélioration de l'empilement magnétique, mais il faut cependant prendre en compte les variations de procédé sur un même *wafer* et les différences au cours des étapes de la fabrication. On ne peut donc conclure sur la part de chacun de ces paramètres dans l'amélioration des résultats. Néanmoins dans la suite de cette étude, le nouvel empilement sera pris comme référence, étant plus stable, l'étude d'autres solutions pour réduire l'effet du champ magnétique est donc plus simple à isoler.

Code de correction d'erreurs

Les codes de correction d'erreurs ont à l'origine été développés pour améliorer la fiabilité dans la transmission d'informations, mais sont aujourd'hui également utilisés dans le stockage de données. Il s'agit de techniques qui permettent grâce à des mécanismes de redondance de détecter et de corriger un certain nombre erreurs. Dans le cadre des mémoires à semiconducteur, le choix du type de la correction d'erreurs varie beaucoup en fonction des applications envisagées de la mémoire, par exemple si un bit erroné provoque un changement de caractère dans un fichier de texte, l'effet de cette erreur sera minime, en revanche, si le même bit utilisé dans un code informatique, l'impact de cette erreur peut être critique.

Rendre la mémoire technologiquement fiable est un prérequis indispensable, mais un code de correction d'erreurs efficace permet de s'assurer que dans le cas d'un événement local qui perturberait quelques bits de la mémoire, l'intégrité des données puisse encore être garantie.

Généralités sur les codes correcteurs

Il existe plusieurs types de construction de codes correcteurs dépendant des cas d'usage, dans certain cas le but est simplement de détecter l'apparition d'erreurs : c'est le cas par exemple du protocole TCP, le destinataire calcule une somme de contrôle qu'il compare à celle du message. Si les deux sommes de contrôles sont différentes, la correction est réalisée par une nouvelle demande de transmission du message [58]. Dans d'autres cas, le but est de détecter et de corriger les erreurs sans renvoyer les données. Les codes correcteurs Reed-Solomon comme le CIRC (Cross-Interleaved Reed-Solomon Coding) qui est implanté par exemple sur les supports cd, est capable de corriger les erreurs dues à une rayure (un maximum de 4096 bits consécutifs) [33].

Sommes de contrôle Pour détecter l'apparition d'erreurs, les sommes de contrôle sont les outils les plus communément utilisés. Dans sa version la plus simple, il s'agit d'ajouter un bit de parité à la donnée. Ce bit de parité est alors défini comme étant égal à '1' si la somme des autres bits est paire et à '0' dans le cas contraire. Ainsi, la modification d'un bit de la donnée initiale modifie la valeur du bit de parité et permet de détecter une altération. Cependant si deux erreurs apparaissent alors un seul bit de parité ne permet pas de les détecter.

Codes linéaires Les sommes de contrôle sont un cas particulier d'un ensemble de codes correcteurs d'erreurs appelé codes linéaires. Le codage c d'un mot m par un code linéaire est une transformation linéaire. Cette transformation est caractérisée par une matrice génératrice G tel que :

$$c = m.G \tag{3.1}$$

Ces codes sont caractérisés par trois paramètres : n, k et σ, qui sont respectivement la taille du code, le nombre de bits de correction et la distance de Hamming minimale

entre deux mots du code. Ce dernier paramètre permet de caractériser la capacité de détection et de correction d'un code. En effet, le nombre minimal d'erreurs que le code peut détecter est égale à :

$$D_{\min} = \sigma - 1 \tag{3.2}$$

Le nombre minimal d'erreurs que le code peut corriger est égal à :

$$T_{\min} = \frac{\sigma - 1}{2} \tag{3.3}$$

Dans le cas de la somme de contrôle à 1 bit de parité, si on prend l'exemple d'un mot de 3 bits, on a alors G, sa matrice génératrice :

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix} \tag{3.4}$$

Ce code correcteur est caractérisé par n=4, k=3 et $\sigma = 2$. Il est donc en mesure de détecter [16] :

$$D_{\min} = \sigma - 1 = 1 \text{ erreur} \tag{3.5}$$

et de corriger :

$$T_{\min} = \frac{\sigma - 1}{2} = \frac{1}{2} \text{ soit } 0 \text{ erreur} \tag{3.6}$$

Ce code correcteur simple est cependant très limité puisqu'il ne permet pas la correction d'erreurs. Pour permettre de corriger des erreurs, il faut une distance de Hamming minimale du code $\sigma \geq 3$. Le code le plus simple et le plus commun ayant cette propriété est appelé code de Hamming(7,4).

Codes de Hamming Ce sont les codes linéaires dont la distance de Hamming est supérieure ou égale à 3 et qui ont la propriété d'être des codes parfaits. Cette propriété traduit le fait qu'il n'y a pas de redondances inutiles dans le code. Pour évaluer cette propriété, il faut définir la région de décodage. Elle correspond pour un code c_i à tous les mots de n bits tels que c_i est le code le plus proche (au sens de Hamming). Dans un code linéaire, la région de décodage possède 2^{n-k} éléments. D'autre part, pour un poids de Hamming h, le nombre de vecteurs de taille n vaut $\binom{n}{h}$. Le nombre total de vecteurs de taille n avec un poids de Hamming de 0 à T_{min} (le nombre minimal d'erreurs que le code peut corriger) est donc :

$$\sum_{h=0}^{T_{\min}} \binom{n}{h} \tag{3.7}$$

Ce qui correspond au nombre de vecteurs que le code peut corriger.

On peut donc définir la borne de Hamming qui est le nombre maximum de vecteurs pouvant être corrigés par le code de correction :

$$\sum_{h=0}^{T_{\min}} \binom{n}{h} \leq 2^{n-k} \tag{3.8}$$

Un code est parfait lorsque cette borne est atteinte [44]. Il s'agit donc de tous les codes avec pour caractéristiques :

$$n = 2^{n-k}; k; \sigma \geq 3 \tag{3.9}$$

Le plus utilisé est le code de Hamming[n=7,k=3,σ=3], il est capable de détecter 2 erreurs et d'en corriger 1 pour des mots de 4 bits.

Cas des TAS-MRAM Dans les composants TAS-MRAM des mémoires Crocus, le code correcteur utilisé est un code linéaire de caractéristique n = 16, k = 8, σ = 5. C'est-à-dire que pour 8 bits de donnée, il y a 8 bits de redondance. Ce n'est pas un code de Hamming dans la mesure où il ne possède pas la propriété d'être un code parfait. En effet si l'on revient à l'équation 3.9, avec une taille de code $n = 16$, un code est parfait pour un nombre de bit de correction $k = 12$. Ainsi $n = 2^{n-k} = 2^{16-12} = 16$.
Ce code correcteur est capable de détecter :

$$D_{\min} = \sigma - 1 = 5 - 1 = 4 \text{ erreurs} \tag{3.10}$$

et de corriger :

$$T_{\min} = \frac{\sigma - 1}{2} = \frac{4}{2} = 2 \text{ erreurs} \tag{3.11}$$

La matrice génératrice G de ce code est de dimension (8,16). Elle peut être interprétée comme la concaténation de 2 matrices (8,8) :

$$G = [I_8|A] \tag{3.12}$$

Avec I_8 la matrice identité de dimension 8, et une matrice A qui va contenir la redondance. Cette concaténation permet d'une part de diviser les bits du code en deux parties, les 8 premiers bits correspondant aux données écrites et les 8 suivants à la redondance. D'autre part, cela facilite le décodage comme expliqué dans le paragraphe suivant.

Décodage par syndrome Les mémoires TAS-MRAM de Crocus utilisent la méthode du décodage par syndrome pour corriger les éventuelles erreurs. Le décodage par syndrome est une méthode de décodage qui utilise une table stockée en mémoire. Cela limite les calculs à effectuer, mais ne fonctionne que pour des données de taille réduite, en effet la taille de la table varie exponentiellement avec le nombre de bits de donnée [41]. Pour un code de caractéristique [n,k,σ], à partir de la matrice génératrice $G = [I_m|A]$, on définit H la matrice de vérification de parité telle que $H = [A^t|I_{n-k}]$.
Soit C l'ensemble des codes générés par la matrice G, alors :

$$\text{Pour } x \in \mathbb{Z}_2^n \text{ , } x \in C \text{ si et seulement si } H.x^t = \mathbf{0} \tag{3.13}$$

On note **0** les vecteurs de 0 de toute taille.
On a alors pour tout mot de n bits $r \in \mathbb{Z}_2^n$, $r = c + e$ avec $c \in C$ le code correct et $e \in \mathbb{Z}_2^n$ l'erreur. On en déduit donc :

$$H.r^t = H.e^t \tag{3.14}$$

$H.r^t$ est appelé le syndrome de r. L'ensemble des mots de n bits ayant le même syndrome est appelé *coset* de C. Les éléments du *coset* correspondent au vecteur de l'erreur e, et en appliquant le principe du maximum de vraisemblance, l'élément du *coset* ayant le poids de Hamming le plus faible est choisi comme le vecteur de correction du mot r. Cet élément est appelé chef du *coset*.

On construit ensuite un tableau avec deux colonnes, la première correspondant aux 2^{n-m} syndromes et la seconde aux chefs des *cosets*. La donnée non-fautée, égale à $c = r - e$, avec e vecteur d'erreur retrouvé dans le tableau en calculant le syndrome de r.

L'implantation de ce type de correction permet dans les révisions I de la mémoire de corriger toutes les erreurs en condition d'utilisation normale de la mémoire. Dans les paragraphes suivants vont être étudiés les effets de ce mécanisme de correction d'erreurs en présence d'un champ magnétique statique.

Code correcteur et perturbations magnétiques des MRAM

Lorsqu'aucun champ externe n'est présent, le code de correction est suffisant pour corriger la plupart des erreurs sur la révision G et toutes les erreurs sur la révisions I.

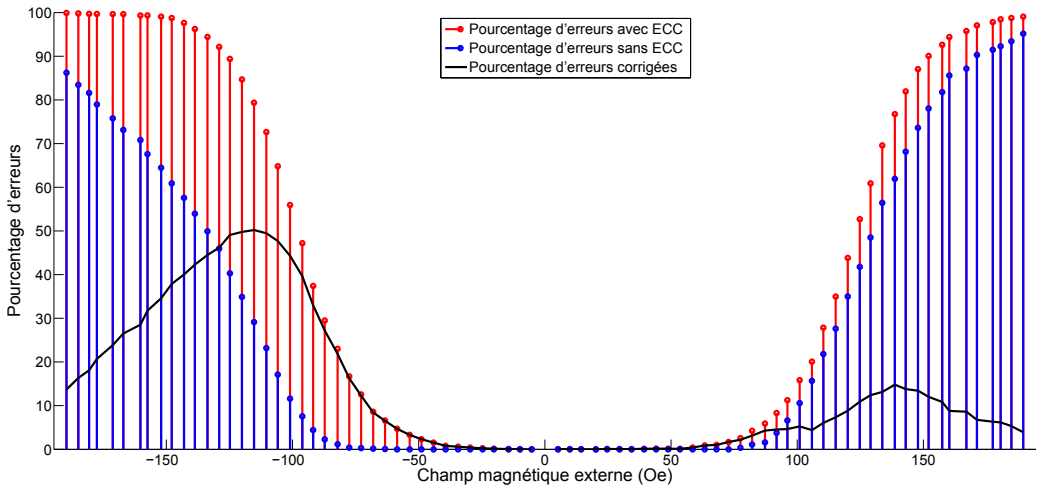

FIGURE 3.8 – Effets d'un champ magnétique externe avec l'utilisation de code correcteurs d'erreurs (ECC)

Lorsque la mémoire est soumise à un champ magnétique externe, tous les bits de la mémoire sont susceptibles d'être modifiés, aussi bien les bits de donnée que les bits de redondance. Ce point rend le mécanisme de correction très dépendant des données stockées, car la correction est globale pour les 16 bits du mot. Dans la figure 3.8, deux exemples extrêmes sont illustrés. Pour les champs positifs, les données fautées sont très majoritairement des '0'. Les erreurs correspondent à l'écriture de 0x00 dans la mémoire, dans ce cas-là les bits de corrections sont aussi huit '0' voir tableau 3.2. Les bits de redondances ont la même probabilité d'être fautés que les bits de données d'où la faible différence observée avec ou sans corrections.

Bits de donnée (hexadécimal)	Bits de donnée (binaire)	Bits de redondance (calculé depuis la matrice de génération)
0x00	0000 0000	0000 0000
0xFF	1111 1111	0000 0000

Table 3.2 – Bits de donnée et bits de redondance pour 0x00 et 0xFF

En revanche pour les champs négatifs, les données fautées sont les '1' et les erreurs correspondent à l'écriture de 0xFF dont les huit bits de correction sont aussi huit '0'. Parce que ce sont des '0', les bits de redondance vont donc être très largement insensible au champ magnétique externe.

Pourcentage d'erreurs	Orientation	Sans ECC	avec ECC	Différence
10%	A	68 Oe	101 Oe	33 Oe
10%	B	96 Oe	101 Oe	5 Oe
50%	A	96 Oe	133 Oe	37 Oe
50%	B	124 Oe	128 Oe	5 Oe

Table 3.3 – Récapitulatif des erreurs avec la correction d'erreur

Quelles que soient les conditions d'application du champ, la correction d'erreurs permet de limiter les effets du champ externe, en particulier pour les champs de faible intensité qui n'engendrent des fautes que sur quelques bits dans chaque octet. En particulier, ils permettent de repousser le champ d'apparition des premières erreurs sur la mémoire de 10 à 35 Oe suivant les données stockées. Cependant pour des champs plus intenses, la correction d'erreurs devient contre-productive. En effet, le nombre de bits fautés parmi les bits de redondance est trop important induisant des erreurs dues à la méthode de correction. Les tests ont montré que dans les cas les plus défavorables (champs magnétiques externes opposés à l'orientation des bits de redondance) jusqu'à 25% d'erreurs supplémentaires peuvent apparaitre.

Bouclier Magnétique

Un autre moyen de réduire les effets d'un champ magnétique externe est de placer un bouclier magnétique au-dessus et/ou au-dessous du composant. Un bouclier magnétique est une couche de matériau ferromagnétique, généralement de la taille de la puce avec une haute permittivité magnétique et une faible coercitivité. Une permittivité élevée permet au matériau de se magnétiser fortement sous l'effet d'un champ magnétique, et la faible coercitivité rend le matériau magnétisable sous l'effet d'un champ faible. Les principaux matériaux de boucliers magnétiques sont des alliages de nickel-fer associé à d'autres matériaux, en particulier du molybdène. Les plus utilisés étant le permalloy composé de 80% de nickel et 20% de fer avec une perméabilité de 80000 [4] et le μ – métal dont les proportions peuvent varier, mais sont généralement proches de 80% nickel, 15% fer et 5% molybdène dont la perméabilité est de l'ordre de 400000 [24].

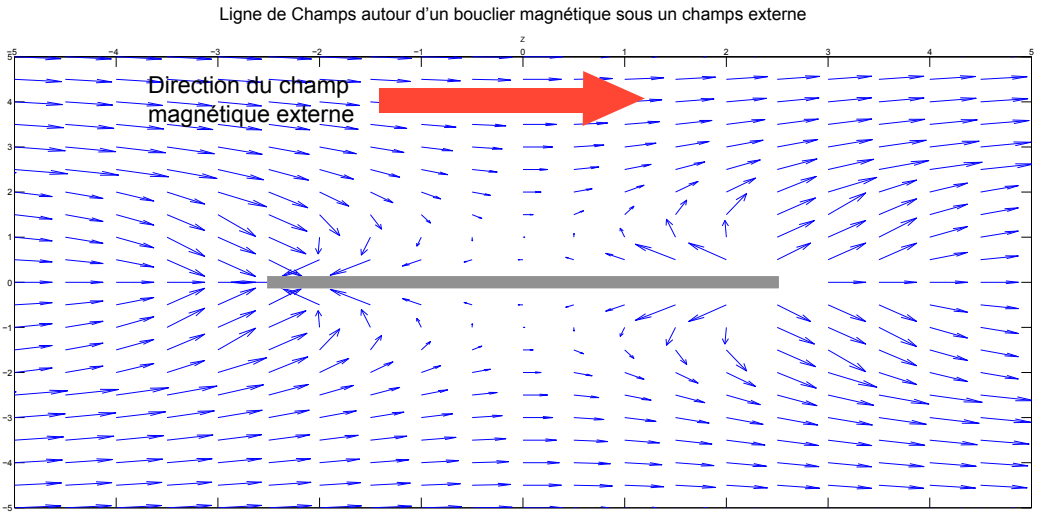

FIGURE 3.9 – Ligne de champ proche d'un bouclier magnétique, le champ est concentré dans le bouclier laissant le champ magnétique dans son voisinage proche très réduit

Lorsque le bouclier magnétique est soumis à un champ magnétique externe il se magnétise. D'après l'équation de Maxwell-Thomson, $div\vec{B} = 0$, c'est-à-dire que le flux traversant une surface fermée est nul ou autrement dit que les lignes de courant bouclent du pôle nord vers le pôle sud du bouclier, créant un champ magnétique opposé. Une zone dans laquelle l'intensité du champ est réduite apparait comme le montre la figure 3.9.

Pour ces tests un bouclier magnétique constitué de $\mu-$métal a été placé sur une mémoire de révision I. En utilisant le même montage que pour les tests précédents, l'évolution des erreurs dues aux champs magnétiques statiques est étudiée et illustrée dans la figure 3.10.

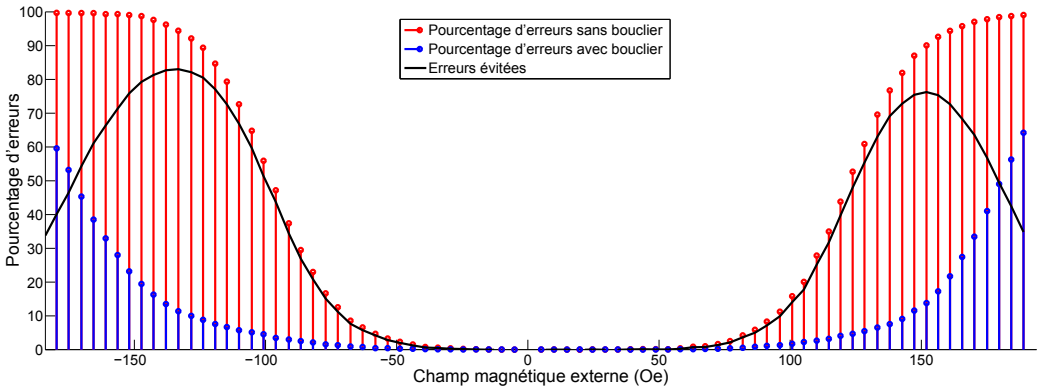

FIGURE 3.10 – Effets d'un champ magnétique externe avec l'utilisation d'un bouclier magnétique

On observe que la résistance au champ magnétique externe est significativement amélioré, comme détaillée dans le tableau 3.4, l'asymétrie est également réduite mais reste présente. De fait, cet effet est proportionnel au champ magnétique au niveau des empilements magnétiques. Pour une perturbation plus faible sur le point mémoire, l'effet d'asymétrie est également plus faible.

Pourcentage d'erreurs	Orientation	Sans bouclier	avec bouclier	Différence
10%	A	68 Oe	128 Oe	60 Oe
10%	B	96 Oe	143 Oe	47 Oe
50%	A	96 Oe	175 Oe	79 Oe
50%	B	124 Oe	>180 Oe	>56 Oe

TABLE 3.4 – Récapitulatif des erreurs avec et sans bouclier magnétique

Un bouclier magnétique est donc une protection très efficace contre les champs magnétiques externes, il permet d'éviter jusqu'à 80% d'erreurs dans la mémoire. Ce résultat est d'autant plus intéressant que comme illustré dans la figure 3.9, la position du bouclier influence de manière significative son efficacité. Or pour ces tests, une seule position a été testée ce qui permet de supposer qu'une optimisation est possible pour encore améliorer la résistance de la mémoire aux champs externes.

Champ magnétique généré par les lignes de courant

Lorsque la mémoire est soumise à un champ externe, c'est la composante du champ qui est parallèle au champ généré par les lignes de courant qui perturbe la mémoire. Lors d'une opération d'écriture, cette composante s'additionne ou se soustrait aux champs magnétiques des lignes de courant et c'est l'effet de cette somme de champ magnétique qui est observé. Une façon simple de réduire l'effet d'un champ externe sur les cellules MRAM est donc d'amplifier l'intensité du champ généré par les lignes de courant.

Le champ magnétique généré par les lignes de courant est proportionnel au courant qui les traverse et dans le cas des échantillons de MRAM de Crocus Technology, ce courant est proportionnel à la tension d'alimentation du circuit. L'alimentation normale des échantillons est de 3.3V, ce qui correspond à un champ d'environ 103 Oe au niveau de l'empilement magnétique. En appliquant l'alimentation à 3.6V, on obtient un champ de 114 Oe. Un test effectué suivant le même protocole que les tests précédents a été effectué (voir figure 3.11). Dans ce test les codes correcteurs sont désactivés.

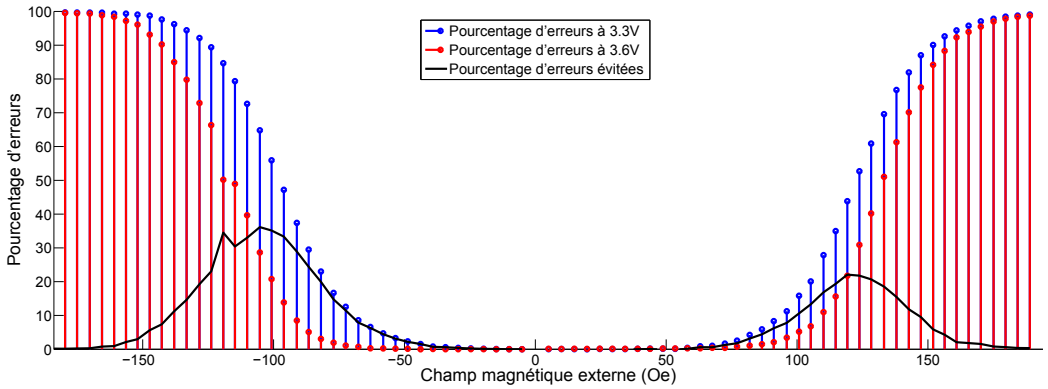

FIGURE 3.11 – Effet d'une augmentation du champ magnétique généré par les lignes de courant lors d'une opération d'écriture

On observe que l'effet du champ externe est réduit d'environ 15 Oe dans une des orientations du champ magnétique, ce qui correspond à l'écart entre le champ magnétique généré avec une alimentation de 3,3V et une alimentation de 3,6V. En revanche dans l'autre orientation l'écart est d'environ 35 Oe. L'asymétrie observée avec un champ magnétique généré par les lignes de courant de 103 Oe est ainsi considérablement réduite. Cet effet s'explique par le fait que le champ magnétique généré par les lignes de courant est directement appliqué sur les couches de stockage tandis que le champ asymétrique est lui proportionnel à l'aimantation des couches ferromagnétiques.

Augmenter le champ généré par les lignes de courant permet de réduire les effets indésirables d'un champ magnétique externe, mais cela a un coût en termes de

consommation d'énergie. En effet, lors d'une écriture à 3,3V la mémoire consomme entre 40 et 50 mA dont 34 mA pour le courant dans les lignes de champ. Alimenté en avec 3,6V, le courant des lignes de champ passe à 38 mA pour une consommation de la mémoire de 45 à 55 mA.

Le *cladding* est une autre méthode pour augmenter le champ magnétique sans modifier la consommation de courant. Il permet de concentrer le champ en recouvrant les lignes de courant d'une couche de matériau magnétique sur trois des quatre faces, comme illustré dans la figure 3.12. Ces couches ferromagnétiques agissent de la même façon que les boucliers magnétiques décrits dans la section 3.3 : elles concentrent le champ magnétique ainsi plutôt que de se disperser équitablement tout autour de la ligne de courant, le champ est plus intense sur la face non recouverte [61]. Les lignes de courant sont recouvertes d'une couche de matériau magnétique sur trois de leurs quatre faces ce qui permet de concentrer le champ et d'augmenter de 50% le champ généré pour un courant égal [71].

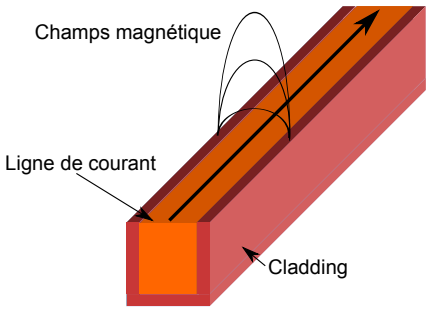

FIGURE 3.12 – Ligne de courant avec *cladding* pour concentrer le champ magnétique

3.4 Comparaison des méthodes de réduction des effets des champs magnétiques statiques

La figure 3.13 résume les différents moyens pour atténuer les champs magnétiques externes pendant les opérations d'écriture.

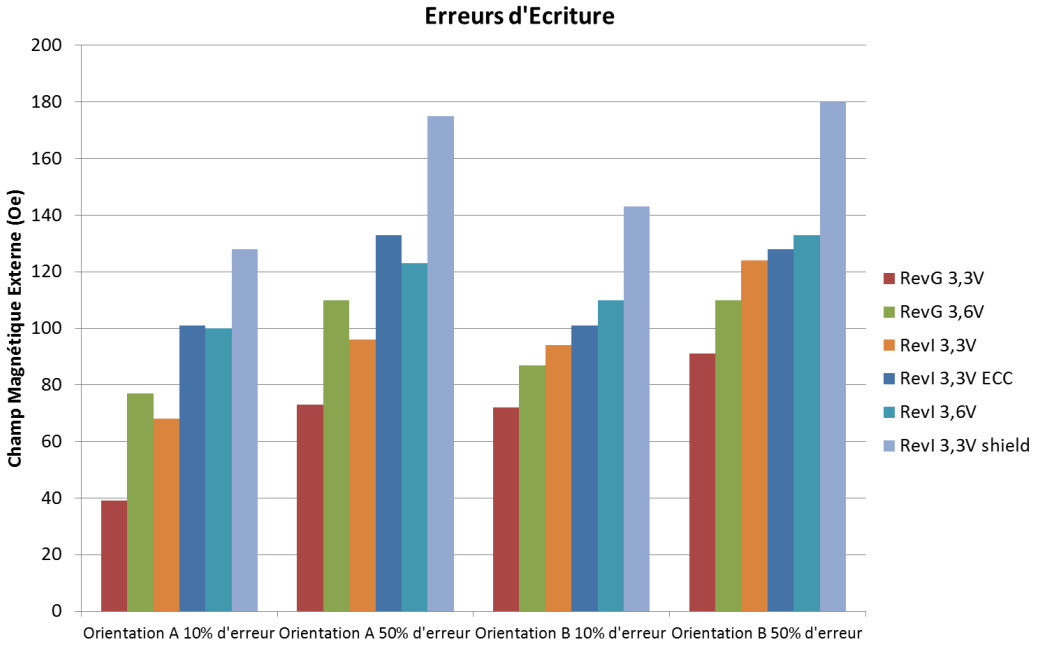

FIGURE 3.13 – Efficacité des différentes méthodes pour atténuer les perturbations d'un champ magnétique statique externe

Les champs magnétiques nécessaires pour provoquer 10% et 50% d'erreurs dans la mémoire pour les orientations de champs A et B sont affichés en ordonnée, tandis les couleurs indiquent quelle révision est testée et suivant quelles conditions : avec ou sans code correcteurs d'erreurs, avec ou sans bouclier et avec une alimentation de 3,3V ou de 3,6V.
On constate une amélioration de près de 300% entre les tests sur les premières révisions et les tests sur la révision I protégée par un bouclier. Le but de cette section est de démontrer l'efficacité de ces différentes méthodes, ainsi l'addition de ces protections n'a pas été testée. Cependant, tout laisse à penser que leurs effets se cumuleraient.

3.5 Conclusion

Les MRAM stockent les données sous forme magnétique, contrairement aux mémoires dominant le marché actuellement (DRAM et flash) qui stockent les données sous forme électrique. Cette particularité des MRAM peut être un avantage pour des applications en environnements extrêmes, en particulier pour l'aéronautique où les composants sont exposés aux radiations cosmiques. En effet les MRAM sont insensibles à ces radiations [69]. Cependant, elles ont d'autres faiblesses, notamment les effets des champs magnétiques importants. De fait les interactions magnétiques sont l'élément central de cette technologie et ce genre de perturbations est critique pour le bon fonctionnement de la mémoire. S'il est très difficile de supprimer complètement cette faiblesse, il existe cependant des moyens d'en réduire les effets.

Les méthodes pour réduire les effets d'un champ externe sont nombreuses, mais elles ont un coût soit en consommation d'énergie pour l'augmentation du champ magnétique des lignes de courant, soit en surface pour les codes de correction d'erreurs, soit en coût de fabrication pour les boucliers magnétiques. Cependant l'intégrité des données est une propriété indispensable des mémoires et ce surcoût peut s'avérer déterminant pour les applications fonctionnant dans des environnements soumis à des champs magnétiques .

Chapitre 4

Attaques physiques sur les mémoires magnétiques : hautes températures et impulsions EM

Sommaire

4.1 Effet des hautes températures sur le comportement d'une MRAM

La température modifie les propriétés des matériaux magnétiques, et peut perturber le fonctionnement des mémoires MRAM. Dans le cas des TAS-MRAM, l'opération d'écriture inclut un échauffement de l'empilement magnétique pour découpler la couche de stockage et la couche antiferromagnétique ce qui permet de faciliter le retournement du moment magnétique (voir section 1.2). Une augmentation de la température peut alors affaiblir la mémoire et la rendre plus sensible à d'autres perturbations. Dans le cas d'autres types de MRAM, comme les MRAM Toggle, l'augmentation de la température a aussi un effet important. L'équilibre des interactions magnétiques dans l'empilement des points mémoires est sensible et la température en modifiant les propriétés magnétiques perturbe cet équilibre ce qui peut engendrer des perturbations.

Effet sur les MRAM Toggle

Protocole expérimental

Pour les tests sur les MRAM toggle, le banc à air chaud décrit dans la section 1.4 a été utilisé. Les effets d'une élévation de la température de 100 °C à 300 °C ont été étudiés pour les opérations de lecture et d'écriture. Les échantillons sont des MRAM 4 Mbits produits par Everspin. Pour les tests sur l'opération de lecture, l'écriture d'une donnée est faite à température ambiante puis la lecture est faite sous le souffle d'air chaud par paliers de 5 °C de la température. L'opération d'écriture a été testée avec la lecture dans des conditions à température ambiante dans un premier temps. Aucune faute de lecture n'apparaissant pour des températures inférieures 285 °C, l'opération de lecture a également été effectuée à chaud. Les mémoires sont alternativement programmées à 0x55 et 0xAA (valeurs hexadécimales comportant des '0' et des '1' alternés) puis testées dans les conditions décrites précédemment.

La température indiquée sur les figures de cette section correspond à la consigne envoyée à l'appareil de chauffe. En prenant en compte la dissipation de chaleur par le boitier et les pertes de chaleur dans la buse, la température précise au niveau de la puce ne peut être déterminée de manière précise. Néanmoins, pour s'assurer que la température estimée au niveau de la puce reste constante, le flux d'air chaud est maintenu pendant une minute au-dessus de la mémoire.

Résultats des mesures

Au-delà de 285°C le nombre et le type des erreurs en écriture comme en lecture met en évidence que s'il y a perturbations, celles-ci affectent entre autres les blocs logiques de la mémoire. Les erreurs issues des perturbations sur les points mémoire ajoutées à celles issues des blocs logiques rendent l'analyse plus complexe du fait de l'addition de ces comportements. Pour cette raison, l'analyse des données sera restreinte à des températures inférieures à 285°C.

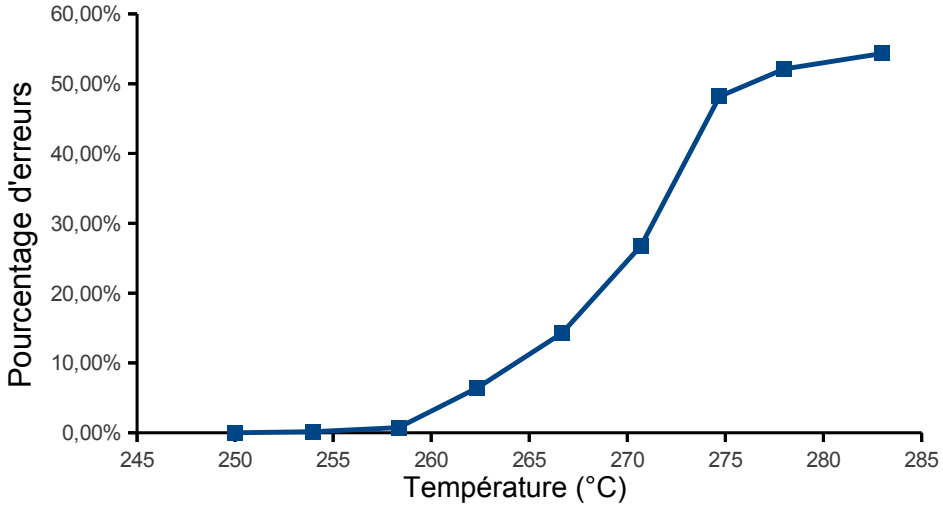

FIGURE 4.1 – Erreurs en écriture sur MRAM Toggle en fonction de la température

Comme précisé dans la partie protocole expérimentale, les opérations de lecture ne sont pas perturbées pour des températures inférieures à 285 °C, il en résulte que les erreurs obtenues dans cette gamme de température sont donc uniquement liées aux opérations d'écriture. La figure 4.1 montre que les premières erreurs apparaissent aux alentours de entre 257°C et 260 °C. On peux observer trois zones phases distinctes :

— 100°C à 260°C : Aucune erreur n'est observée
— 260°C à 275°C : Le pourcentage d'erreurs croît rapidement jusqu'à atteindre environ 50% des bits écrits
— 275°C à 275°C : La croissance est bien moins prononcée pour atteindre un taux d'erreur de à 60% à 285°C

Afin de comprendre l'origine de cette inflexion à 275 °C, les résultats sont agrégés. Sur la figure 4.2 est représentée la proportion des bits collés à '0'. Un bit est considéré collé à '0' si lors d'une opération d'écriture d'un '1', ce bit reste à la valeur '0'.

On constate que la grande majorité des erreurs observées sont des bits écrits à '1' alors que l'ordre envoyé était une écriture à '0', en effet jusqu'à 275 °C, moins de 1% des erreurs est un collage à '0'. La forte croissance des erreurs observées dans la figure 4.1 correspondrait donc à des collages à '1' jusqu'à atteindre près de 50% du total des bits écrits vers 275°C. Cependant en examinant la répartition des erreurs représentées sur la figure 4.2 on constate que la grande majorité (99%) des données fautées sont des bits collés à '1'. Or les tests comportant autant d'écritures à '1' qu'à '0', les 50% observés correspondent en fait à la totalité des bits écrit à '0' qui

sont collés à '1'.

Ce changement de type de faute permet d'expliquer l'existence de l'inflexion au de la figure 4.1, en effet à partir de 275°C, un nouveau type de faute est observé : le collage de bits à '1'.

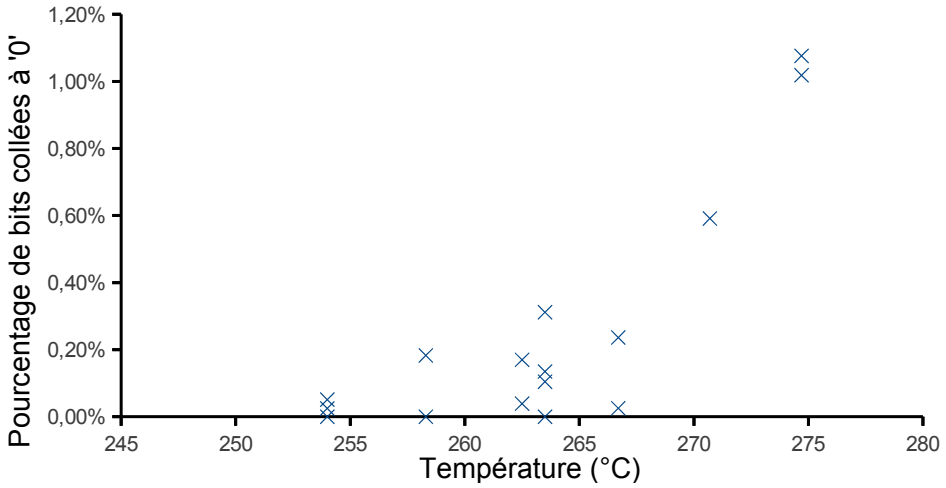

FIGURE 4.2 – Bit collés à '0' sur MRAM Toggle sous l'effet de la température

Les spécifications précises du fonctionnement des mémoires Everspin n'étant pas publiques, nous ne disposons pas de tous les éléments pour analyser en détail les mécanismes en jeu. Cependant, le fonctionnement d'une écriture par la méthode Toggle est connu et permet d'interpréter les résultats observés.

Effet de la température sur le couplage RKKY

Les opérations d'écriture dans les MRAM toggle utilisent la méthode dite de *Svatchenko* pour retourner les moments magnétiques des points mémoires, cette méthode est décrite dans le paragraphe 1.2. La couche de stockage est un empilement SAF composé de deux couches ferromagnétiques séparées par une couche de ruthénium. Les deux couches ferromagnétiques sont couplées entre elles avec des orientations de leurs moments magnétiques opposés, c'est le couplage RKKY, dont le fonctionnement est également détaillé dans le paragraphe 1.2.

En simplifiant l'empilement global à ses couches principales, il peut être résumé à l'empilement de la figure 4.3. Un empilement SAF pour la couche de référence et un second de l'autre côté de la barrière tunnel pour la couche de stockage.

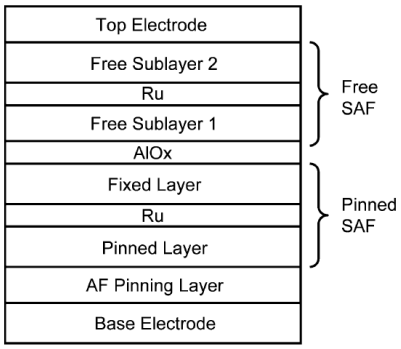

FIGURE 4.3 – Empilement simplifié d'une MRAM toggle [22]

Drchal et al. ont montré en 1999 dans [21] que la température a un effet important sur la force du couplage dans un empilement SAF. En effet, la force du couplage RKKY décroit de manière linéaire en fonction de la température (voir figure 4.4).

Zhang et al. décrivent dans [73] une relation entre que le champ magnétique d'échange dans un couplage RKKY et la température ou H_{ex}^{0}, T_0 et H_{ex}^{∞} sont des constantes en température et en champ qui dépendent de l'épaisseur des couches :

$$H_{ex} = \frac{H_{ex}^{0}.(\frac{T}{T_0})}{sinh(\frac{T}{T_0})} + H_{ex}^{\infty} \tag{4.1}$$

L'équation 4.1 montre que l'augmentation de la température T a donc tendance à réduire le couplage H_{ex} de manière significative. Dans le cas des MRAM toggle l'écriture repose sur le couplage RKKY ce qui dans des conditions de température élevées peut avoir des conséquences importantes sur le bon fonctionnement de la mémoire.

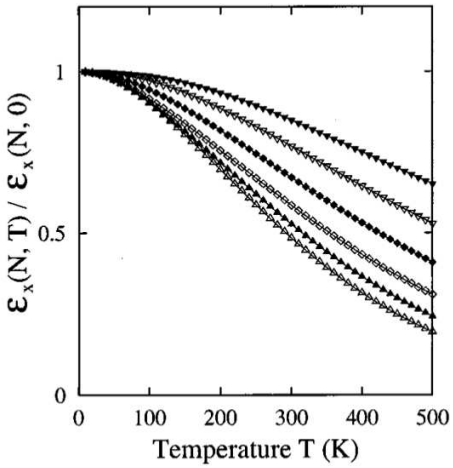

FIGURE 4.4 – Effet de la température sur le couplage RKKY avec différentes épaisseurs pour la couche de séparation (de haut en bas 9, 14 19, 24, 29 et 34 nm) [21]

Modèle de fautes

Pour rappel la composition de l'empilement magnétique et l'architecture des MRAM Everspin ne sont pas connues de manière précise. Bien que n'ayant pas accès à ces informations non publiques, la connaissance de ces éléments n'est pas un point bloquant pour formuler des hypothèses probables sur les effets internes de la température sur ces circuits.

Lors d'une écriture utilisant la méthode de Svatchenko, les interactions entre les couches du SAF de stockage et les interactions avec le champ magnétique généré par les lignes de courants alignent les moments magnétiques des deux couches ferromagnétiques de stockage perpendiculairement aux champs magnétiques, comme illustré dans la figure 1.20 du paragraphe 1.2. Or comme expliqué dans le paragraphe précédent, les interactions entre les couches magnétiques dans un SAF sont dépendantes de la température. Le couplage étant de plus en plus faible lorsque la température augmente, il en résulte donc un fonctionnement perturbé de la mémoire qui est illustré dans la figure 4.5.

Le couplage RKKY de la couche de stockage est moins intense, les aimantations des deux couches de l'empilement antiferromagnétique sont alignées sur le champ d'écriture.

Le couplage étant réduit, les moments magnétiques des deux couches du SAF s'alignent sur le champ des lignes de courant. Lorsque ce champ disparait, le couplage bien que réduit impose à nouveau aux moments magnétiques des deux couches d'être anti-alignés, tandis que la forme ovale du point mémoire impose un axe facile sur lequel vont s'aligner les deux moments magnétiques. La distribution devrait à ce point être aléatoire avec autant de '1' que de '0' pour une lecture de bits chauffés. Cependant, la figure 4.2 montre que plus de 98% des erreurs sont des bits collés à '1'.

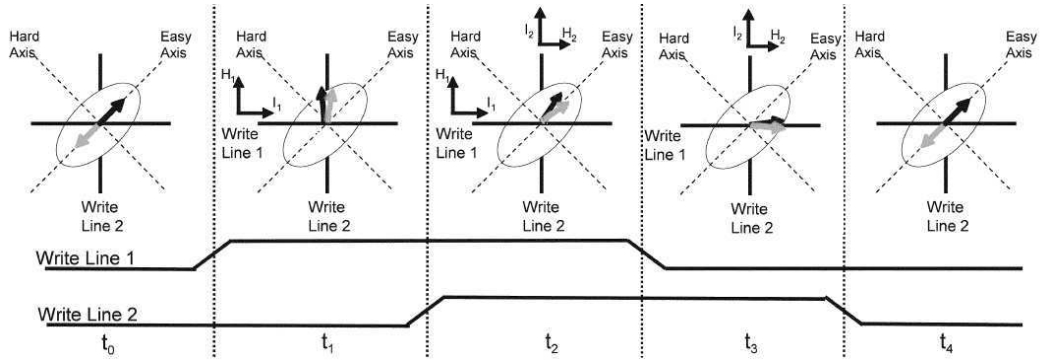

FIGURE 4.5 – Modification du fonctionnement des opérations d'écriture toggle à température élevée

Cet écart s'explique par le couplage dipolaire (voir paragraphe 1.2), c'est-à-dire le couplage dû au champ magnétique généré par une couche ferromagnétique proche, en particulier de la couche de référence qui n'est séparée de la couche de stockage que par la barrière tunnel de quelques nanomètres. Ce champ va aligner la couche la plus proche de la barrière dans la direction opposée de celle de la couche de référence or les autres contributions magnétiques étant minimales lorsque les lignes de courant sont inactives. Il est suffisant pour imposer dans une grande majorité des cas une orientation préférentielle à la couche de stockage, c'est ce qui apparait dans la figure 4.2.

Ces tests montrent qu'en dépit du fait que la température n'est pas utilisée de manière directe dans les opérations des toggle MRAM, son effet sur l'équilibre des interactions dans l'empilement magnétique des points mémoires est loin d'être négligeable. Les températures mises en jeux sont cependant bien au-delà des températures limites du fonctionnement du composant, et ce, malgré l'incertitude sur la température sur le puce. Mais en utilisant les résultats des tests sous champ magnétique statique et les effets des hautes températures, il est possible de perturber la mémoire dans des conditions beaucoup moins extrêmes.

Effet de la température sur les TAS-MRAM

Les MRAM utilisant la technologie TAS ont un processus d'écriture différent. Le point mémoire est porté à haute température pour débloquer ses moments magnétiques et permettre leur renversement par champ magnétique. Une augmentation importante de la température (explication détaillée dans le paragraphe 1.2) est appliquée pendant l'opération d'écriture. Les points mémoires atteignent une température de 180 °C, et l'on a montré que dans le cas de MRAM toggle, à des températures de l'ordre de 285 °C les opérations d'écriture sont perturbées. Dans les deux cas, on observe un changement des propriétés magnétiques des empilements en fonction de la température. De plus, les perturbations liées à des champs

magnétiques ont été étudiées dans le chapitre 3, et sans protections appropriées, leurs effets peuvent être néfastes pour la mémoire.

Que ce soit par des modifications de température ou de champ magnétique externe, les empilements magnétiques sont perturbés. L'analyse des effets combinés de la température et des champs magnétiques externes permet de montrer que l'intensité des perturbations évolue en fonction de ces deux paramètres. Pour ce test, l'enceinte thermique a été utilisée, cela facilite l'intégration du montage et autorise l'utilisation de deux sources de perturbation, mais en contrepartie, elle limite l'utilisation à des températures moins élevées. L'expérience montre cependant que les températures accessibles sont largement suffisantes pour mettre en évidence les effets de ces perturbations combinées (voir figure 4.6).

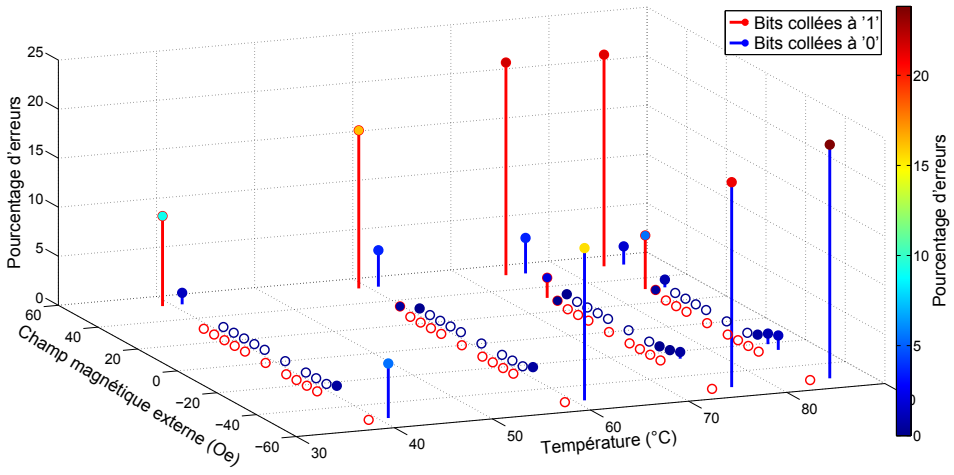

FIGURE 4.6 – Effet de la température sur la sensibilité aux champs externes

La figure 4.6 montre l'évolution du nombre d'erreurs en fonction de la température, du champ magnétique externe et des données écrites. Pour une température de 40 °C on observe un taux d'erreurs comparable au taux d'erreurs à température ambiante : les premières erreurs apparaissent sous l'effet d'un champ magnétique d'une intensité d'environ 50 Oe. Lorsque la température augmente les premières erreurs se manifestent sous l'effet de champs magnétiques plus faibles, entre 15 et 20 Oe pour une température de 75 °C et entre 10 et 15 Oe pour 85 °C. De la même façon le taux d'erreurs passe de 10% à 25% à 50 Oe lorsque la température croit de 40 °C à 85 °C.

Ces résultats illustrent le même type de phénomène que celui observé dans le cas de la toggle MRAM : une diminution de l'intensité des couplages entre les différentes couches magnétiques qui augmente la sensibilité des empilements par rapport au champ magnétique externe.

Proposition de brevet : fusibles thermiques

Suite à ces résultats, une proposition de brevet en vue de la détection d'attaque par haute température a été proposée. Elle consiste à la création de fusibles thermiques utilisant la réduction du couplage d'échange à haute température.

En effet comme expliqué dans la partie 1.2, le couplage d'échange entre une couche antiferromagnétique et une couche ferromagnétique disparait au delà d'une température dite de blocage. C'est sur ce principe que sont faites les écritures dans une mémoire TAS MRAM. Dans une cellule mémoire normale, l'empilement est construit de telle sorte que la couche découplée ne soit influencée par aucun champ magnétique ou aucun couplage à l'exception du champ généré par les lignes de courant.

L'idée proposée dans le brevet consiste à créer un biais important par un couplage dipolaire avec une couche de référence de grande épaisseur afin de modifier l'état de la cellule au-delà de la température de blocage. C'est le principe du fusible thermique illustré dans la figure 4.7.

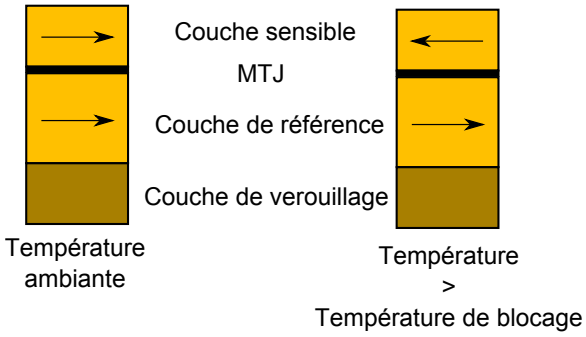

FIGURE 4.7 – Fusibles thermiques : principe de la cellule

Cependant, la température de blocage n'est pas exactement la même pour toutes les cellules, c'est pour cette raison qu'il est proposé d'utiliser un réseau de cellules. En effet dans ce réseau dès qu'un certain nombre de cellules change d'état cela indique le franchissement de la température de déblocage et de ce fait définit le seuil de détection.

Cette solution a l'avantage d'être facilement intégrable à des composants MRAM et permet de détecter les attaques par haute température et de prendre une décision appropriée en termes de gestion de sécurité : effacement de la mémoire, arrêt des opérations d'écriture, etc.

4.2 Comportement d'une MRAM soumise à des impulsions électromagnétiques

Protocole expérimental

Les champs magnétiques statiques étudiés dans le chapitre 3 ne sont qu'une partie des perturbations électromagnétiques qui peuvent avoir un effet sur les composants MRAM. Les impulsions électromagnétiques sont déjà utilisées pour attaquer des composants électroniques, et plus particulièrement les implémentations d'algorithmes cryptographiques. Les effets du couplage entre la pointe d'une antenne et un circuit intégré sont démontrés expérimentalement dans [55], dans [7] les sorties d'un générateur de nombres aléatoires sont verrouillées par des impulsions électromagnétiques et dans [45] ce sont des instructions de microcontrôleurs qui sont ignorés lorsque des impulsions interviennent aux bons moments pour n'en citer que quelques-uns. Dans le cas particulier des composants MRAM, en plus des problèmes liés au CMOS s'ajoute le comportement des empilements mémoires sous l'effet d'une impulsion électromagnétique. C'est ce point qui est étudié dans cette section.

Préparation d'échantillons

Pour réaliser ces tests, le banc expérimental décrit en section 1.4 et dans la figure 1.28 a été utilisé. De nombreux paramètres vont être étudiés en comparaison avec les tests de champs magnétiques externes statiques, en particulier la position de l'antenne d'injection va être un paramètre qui nécessite une précision importante. Les composants n'ayant pas besoin d'être décapsulés pour permettre l'attaque, il est cependant nécessaire de connaitre la position exacte du circuit dans son boitier. Pour cela une cartographie aux rayons X a été effectuée (figure 4.8), si elle ne permet pas d'identifier les différents blocs de la mémoire, elle permet en revanche de les délimiter avec précision.

À partir des images obtenues, les limites des positions d'antennes ont pu être identifiées pour d'une part avoir des résultats qui ne varient pas d'un test à l'autre et d'autre part faciliter l'identification des éléments perturbés par les impulsions électromagnétiques.

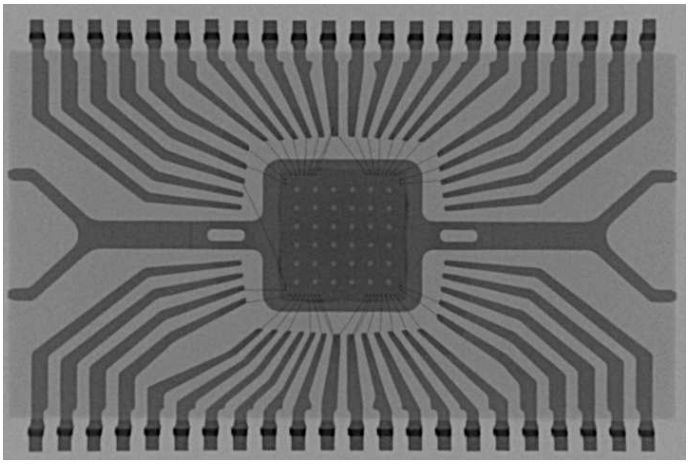

FIGURE 4.8 – Cartographie au rayon X d'un composant MRAM

Forme des impulsions électromagnétiques

L'antenne d'injection est une bobine avec un cœur ferromagnétique, elle a été fabriquée dans le laboratoire. La forme et les matériaux utilisés pour construire l'antenne influencent beaucoup les performances, c'est-à-dire le transfert de l'énergie du générateur d'impulsions en ondes électromagnétiques [50]. D'autre part, l'impulsion électrique envoyée par le générateur n'est pas convertie directement en une impulsion électromagnétique de la même forme, en réalité ce sont les fronts montants et descendants de l'impulsion électrique qui déterminent les caractéristiques de l'onde électromagnétique envoyée. Pour les besoins des tests, il est nécessaire d'avoir une position temporelle précise pour cibler les opérations de la mémoire. Il faut donc pouvoir limiter au maximum les réflexions qui génèrent des trains d'impulsions. L'intensité des répliques est suffisamment importante pour perturber également le circuit compliquant l'analyse des effets en multipliant les moments impactés par l'impulsion. Pour mesurer ces oscillations, un antenne d'analyse est placée sous l'antenne d'injection ce qui permet d'observer la forme de l'impulsion sur un oscilloscope, comme illustré dans la figure 4.9.

Ces réflexions sont principalement dues aux connexions du câble, les expériences ont montré qu'en augmentant la longueur du câble, la fréquence des oscillations diminue. Ces oscillations ont une fréquence de 35 MHz pour le montage utilisé dans les tests. En faisant une analyse fréquentielle de ce signal, on remarque aussi la présence d'une oscillation d'intensité plus faible d'une fréquence aux environs de 100 MHz . L'origine de cette seconde oscillation n'est pas formellement identifiée même si elle vient très probablement des connecteurs entre l'antenne et le câble. En effet, des tests ont montré que sa forme variait en fonction du type de connecteurs.

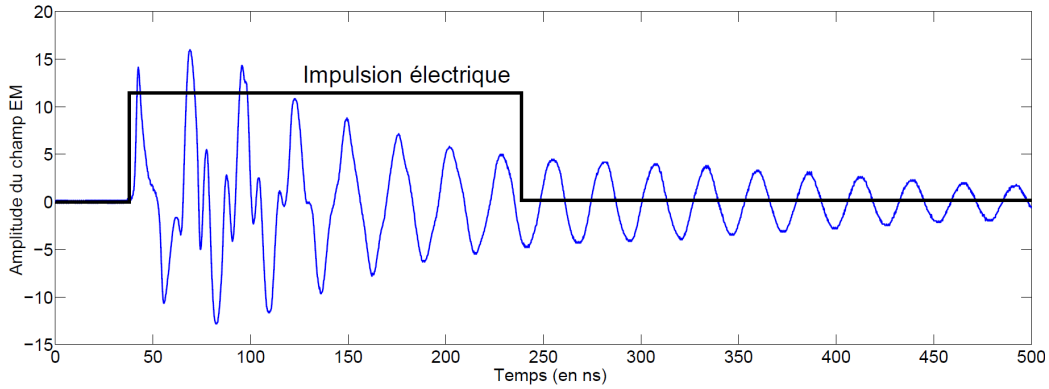

FIGURE 4.9 – Mesure à l'oscilloscope de l'onde électromagnétique, les oscillations sont dues à sa réflexion dans le câble et l'antenne

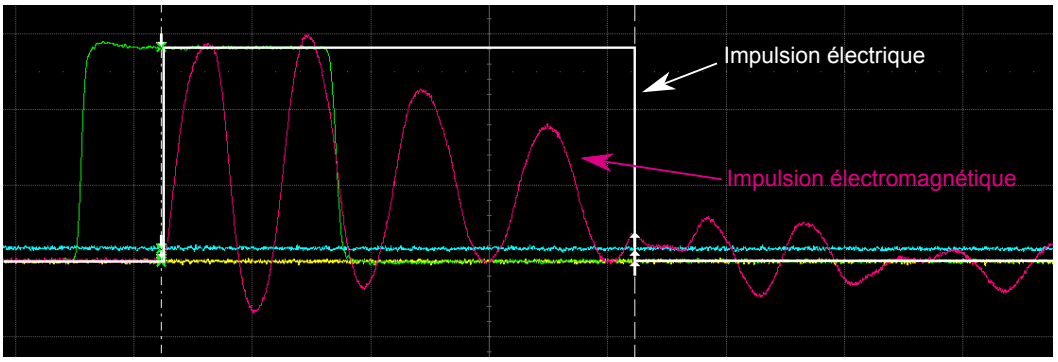

FIGURE 4.10 – Les oscillations générées lors du front montant de l'impulsion électrique sont atténuées par celles générées lors du front descendant

Pour pouvoir limiter ces réflexions, l'idée initiale a été d'adapter l'impédance de l'antenne avec le générateur, mais cette solution atténue trop fortement l'impulsion électromagnétique. La seconde solution testée fut de choisir une longueur d'impulsion électrique qui permet de réduire les signaux parasites des réflexions. En effet, les impulsions électromagnétiques sont générées par les fronts montants et descendants de l'impulsion électrique. Le front montant génère un train d'ondes dont la première oscillation est positive, et le front descendant génère un train d'onde de même fréquence dont la première oscillation est négative. La figure 4.10 montre bien le cinquième pic écrasé par le champ crée lors du front descendant du signal électrique. Cependant, les oscillations ne sont pas strictement superposables d'où la présence oscillations après le front descendant.

En synchronisant avec soin les deux fronts, il est possible d'atténuer les oscillations suivant la première. La solution optimale est trouvée en synchronisant le front descendant de l'impulsion électrique quelques nanosecondes avant le premier

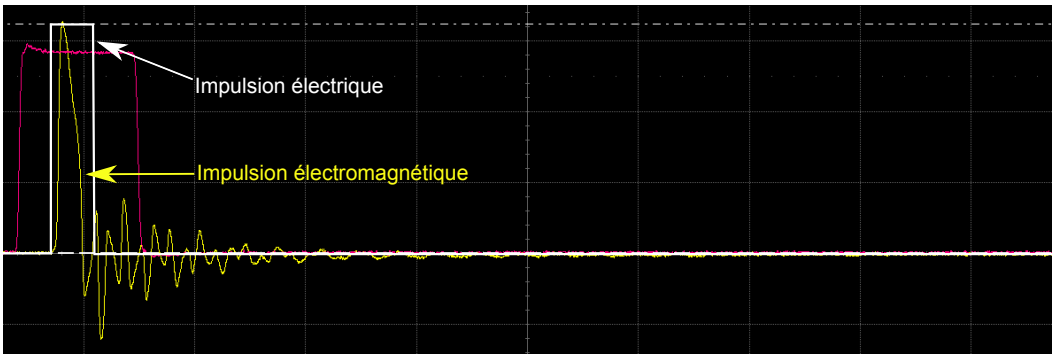

FIGURE 4.11 – Largeur d'impulsion et longueur de câble optimisées pour générer une unique impulsion électromagnétique

pic négatif généré par le front montant. Il est également important de choisir un câble suffisamment long pour que la demi-période des oscillations soit d'une durée minimum de 10 ns, car il s'agit de la largeur minimale de l'impulsion électrique. Avec une impulsion d'une durée de 29.8 ns, il est possible de réduire les oscillations secondaires à moins de 40% de l'amplitude du premier pic comme illustré dans la figure 4.11. Ce travail préliminaire permet d'avoir un contrôle précis du moment d'injection sur le circuit et donc de perturber spécifiquement les phases d'écriture ou de lecture de la mémoire.

Paramètres étudiés

Les impulsions électromagnétiques peuvent avoir pour effet de générer des erreurs permanentes ou nécessitant une coupure de l'alimentation et une réinitialisation de la mémoire pour permettre à celle-ci de retrouver un fonctionnement normal. C'est pourquoi chaque impulsion est précédée d'opérations d'écritures et de lectures pour avoir des informations sur la durée et le type de fautes provoquées.

Lors de ces tests six paramètres ont été pris en compte :

— L'amplitude de l'impulsion
— Le moment de l'injection
— La position physique de l'adresse dans la puce
— La position de l'antenne
— Le nombre d'itérations
— La donnée écrite en mémoire

Le moment de l'injection est défini par rapport au signal WE (*Write Enable*) qui déclenche l'écriture d'une donnée dans la mémoire. Comme expliqué dans le paragraphe 2.1, le front descendant déclenche l'écriture de '0' sur tous les bits de l'adresse ciblée tandis que le front montant déclenche l'écriture des '1' sur les bits en fonction de la donnée à écrire. Comme illustré dans la figure 4.12, les tests sont donc concentrés sur ces deux zones temporelles.

L'effet de l'impulsion est limité dans l'espace ce qui impose de prendre en compte

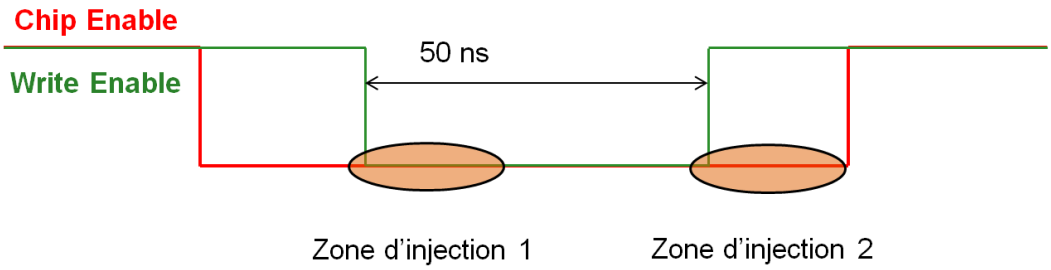

FIGURE 4.12 – Zones d'injection d'impulsions EM

la position des bits testés dans le composant ainsi que la position de l'antenne d'injection. Cependant, l'antenne d'injection a un diamètre d'environ 4-5 mm, ce qui est proche de la taille de la puce, limitant les effets liés à sa position et à celle des bits écrits.

Le nombre d'itérations reste relativement restreint pour la plupart des tests pour limiter leurs durées. Ce paramètre permet néanmoins de distinguer les erreurs ponctuelles et moins reproductibles (voire non reproductibles) des erreurs ayant des causes identifiables.

Effet global des impulsions électromagnétiques

Ce type de test comporte beaucoup de paramètres et certains effets sont difficilement prévisibles, la première étape consiste donc à utiliser un jeu de paramètres large pour délimiter les contours des zones d'intérêt des tests et les zones limites de fonctionnement du circuit.
En particulier sont recherchées les zones dans lesquelles les impulsions électromagnétiques n'ont pas d'effet, et celles dans lesquelles elles ont trop d'effet (mémoire temporairement ou définitivement inutilisable).

Chaque itération de ce test se déroule en trois étapes :
— initialisation de toute la mémoire à la même valeur, '1' ou '0'
— impulsion électromagnétique pendant l'écriture sur une seule adresse
— relecture de toute la mémoire

Deux types d'erreurs en particulier imposent des précautions quant aux paramètres des injections.

Le premier est un collage à '1' qui bloque l'intégralité des bits de la mémoire comme illustré en figure 4.13. Chaque point représente une position de l'antenne d'injection, lorsqu'elle est positionnée au centre du circuit, une impulsion d'une amplitude de 180 V ou supérieure provoque ce type d'erreur. Les écritures ultérieures sont inefficaces, l'alimentation de la mémoire doit être réinitialisée pour retrouver un comportement normal de la mémoire. Il y a trois points importants qui caractérisent ce type d'erreur, la position de l'antenne qui peut être reliée à la position

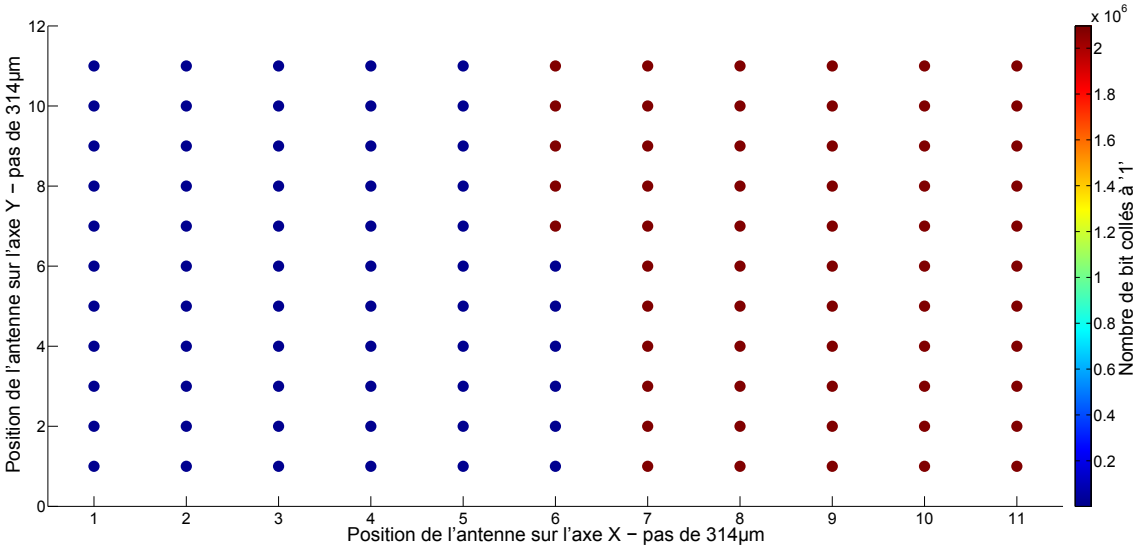

FIGURE 4.13 – Erreurs globales - Collage à '1'

de blocs précis de la mémoire, la durée de l'erreur qui disparait lorsque l'alimentation est coupée et le caractère systématique de ces erreurs qui touchent 100% des bits de la mémoire. Ce dernier point permet d'exclure une perturbation des points mémoires et indique plutôt un problème lié aux opérations de lecture.
Tous ces éléments permettent de formuler deux hypothèses générales sur les causes possibles de ces erreurs :

- Une perturbation d'un élément initialisé à la mise sous tension de la mémoire telle qu'une tension de référence.
- Une perturbation liée aux *sense amplifiers* qui est le bloc de circuit permettant de convertir la résistance mesurée dans une cellule mémoire en bit numérique.
- Une perturbation liée au circuit gérant les entrées/sorties des données, qui sont les blocs positionnés sous l'antenne lorsque cette faute apparait.

Ces hypothèses n'ont pas été testées de manière approfondie, la priorité ayant été donnée à la recherche des conditions de leurs apparitions (amplitude de l'impulsion et position de l'antenne) pour éviter qu'elles ne perturbent les tests suivants. Une étude plus approfondie de ces fautes pourrait être intéressante : si ces dernières sont généralisables à l'ensemble de la mémoire. En effet elles peuvent constituer une contre-mesure aux attaques malicieuses par impulsions EM. En effet un déni de service contrôlé et non-destructif de la mémoire dû à une impulsion électromagnétique permet de considérablement réduire les conséquences sur la sécurité de la mémoire et de son contenu face à ces attaques.

Le second type d'erreurs globales est un collage à '0', très proche des erreurs précédemment décrites, l'ensemble des adresses de la mémoire est lu à 0x00 cepen-

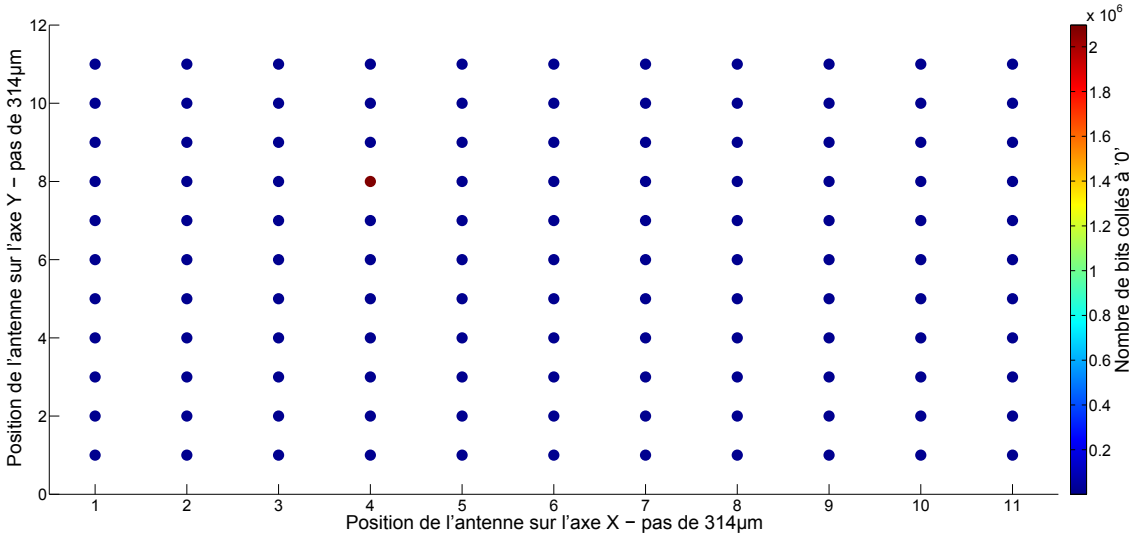

FIGURE 4.14 – Erreurs globales - Collage à '0'

dant après une nouvelle écriture la mémoire retrouve son fonctionnement (voir la figure 4.14). Les positions auxquelles apparaissent les erreurs diffèrent d'un test à l'autre, mais elles apparaissent toujours pour des impulsions d'amplitude supérieure à 180 V.

Contrôle des écritures par impulsion électromagnétique

En jouant sur l'amplitude et le moment des impulsions, il est possible de perturber l'écriture d'une donnée sur la MRAM. Il est possible non seulement de bloquer la mémoire comme expliqué dans le paragraphe 4.2, mais aussi de produire des perturbations plus fines qui peuvent aller jusqu'à forcer l'écriture d'un octet à 0x00 ou 0xFF indépendamment des données écrites prévues.

Les figures 4.15 et 4.16 montrent les erreurs causées par des impulsions lors d'opérations d'écritures. La donnée écrite est 0xAA soit en binaire 0b10101010 ce qui permet de tester à la fois les collages à '0' et les collages à '1', chaque point de la courbe représente les écritures de 16 adresses, réparties spatialement dans le circuit, synchronisées avec des impulsions électromagnétiques. Le moment exact des impulsions ainsi que leurs amplitudes sont représentés sur les axes x et y respectivement.

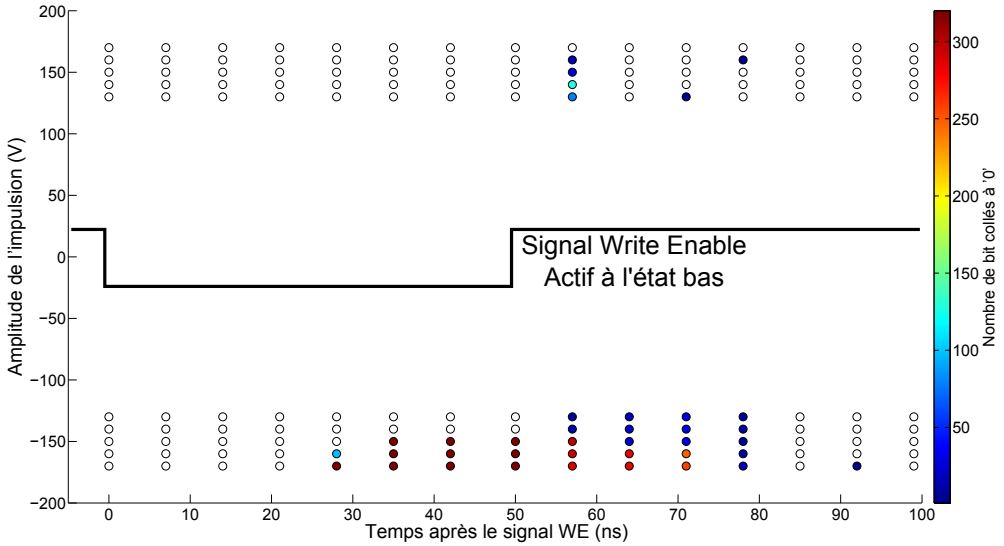

FIGURE 4.15 – Répartition des bits collés à '0' en fonction du moment d'injection et de l'amplitude de l'impulsion électromagnétique

Les erreurs observées dans ces figures sont des collages à '0' et '1' en effet, comme expliqué dans le paragraphe 4.2, entre deux impulsions, les données complémentaires sont écrites. Ce qui signifie que les erreurs observées ne sont pas des bits retournés, mais des écritures empêchées. De plus, ces fautes sont non permanentes, ni le point mémoire, ni les blocs CMOS du composant ne sont endommagés. C'est un point important en termes de sécurité, car la perturbation reste très localisée dans le temps ce qui complique sa détection par d'éventuelles contre-mesures.

L'instant d'injection est un paramètre important, il définit le type de faute qui va être générée. Pour une injection synchronisée sur front descendant du signal *WE*

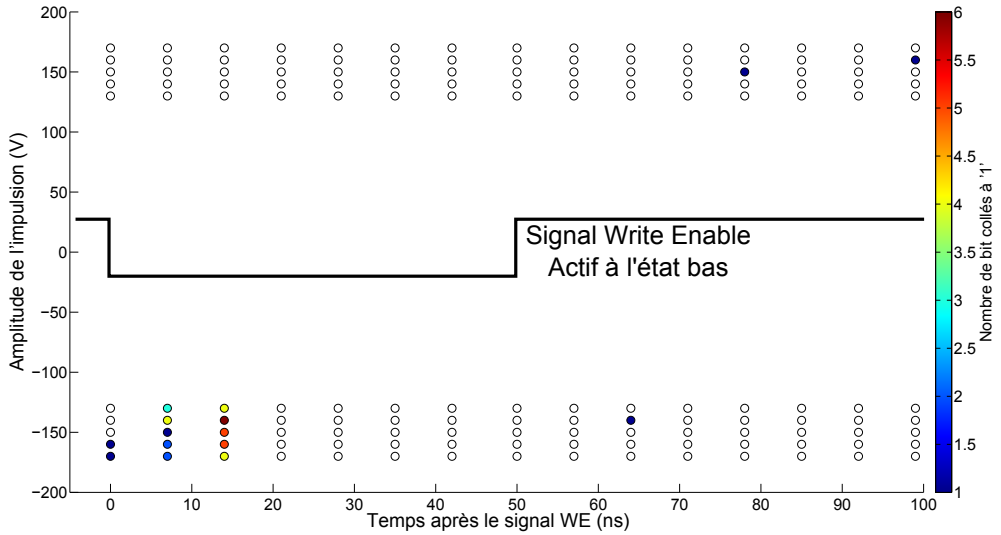

FIGURE 4.16 – Répartition des bits collés à '1' en fonction du moment d'injection et de l'amplitude de l'impulsion électromagnétique

et jusqu'à 20 ns après, les fautes provoquées vont être des collages à '1'. Tandis que pour des injections synchronisées sur front montant de ce signal les erreurs sont des collages à '0'.

Effets de l'instant d'injection

L'analyse préalable des opérations dans la mémoire pendant une écriture montre bien que l'écriture des '0' et des '1' sont séparées temporellement, ce qui laisse une opportunité pour atteindre spécifiquement une de ces deux phases. Comme le montre la figure 4.17, la répartition des erreurs peut-être conditionnée par l'instant de l'injection indépendamment des autres paramètres. Pour une impulsion électromagnétique injectée entre 5 et 15 nanosecondes après le front descendant du signal *WE*, plus de 85 % des erreurs sont des bits collés à '1' tandis que pour une impulsion injectée dans les 20 nanosecondes après le front montant de ce signal, plus de 95 % des erreurs causées sont des collages à '1'.

En reprenant l'enchainement des phases d'une opération d'écriture (voir section 2.1), on peut identifier lesquelles sont perturbées par les impulsions électromagnétiques :

— le chargement des lignes de courant, durant les 20 nanosecondes avant le front montant du signal *Write Enable*
— le chauffage des cellules mémoires, à partir de 5 nanosecondes après le front montant du signal *Write Enable*

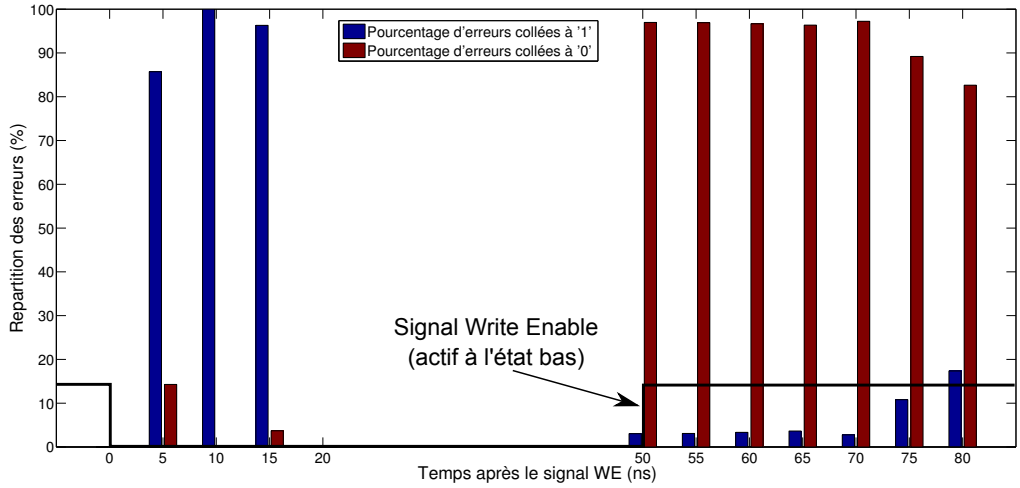

FIGURE 4.17 – Répartition des erreurs en fonction de l'instant d'injection lors d'une écriture

Cependant, le taux de succès des perturbations causées par les impulsions est très inégal. Les figures 4.18 et 4.19 montrent que pour les perturbations après le front descendant du signal *Write Enable* entre 2% et 2.5% des bits écrits sont perturbés tandis que les perturbations synchronisées sur le front montant atteignent 50% des bits écrits.

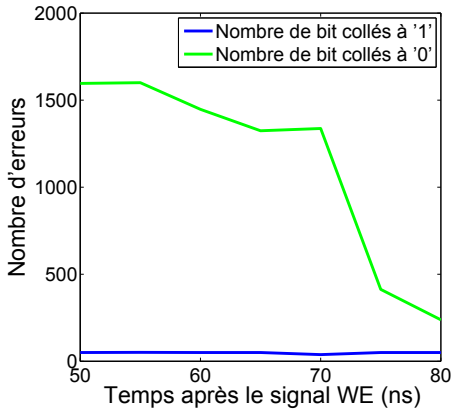

FIGURE 4.18 – Nombre d'erreurs au front descendant du signal WE

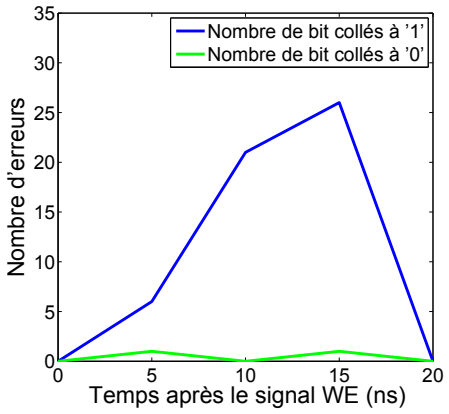

FIGURE 4.19 – Nombre d'erreurs au front montant du signal WE

Effets de l'amplitude de l'impulsion

Il apparait également en analysant les figures 4.15, 4.16 que les erreurs apparaissent dans la grande majorité (>97%) pour des impulsions de signe négatif, et ce aussi bien pour les erreurs sur les '1' que sur les '0'. Si on observe le nombre d'erreurs en fonction de la tension de l'impulsion électromagnétique, comme illustré dans la figure 4.20, on remarque que les erreurs apparaissent principalement à partir d'une impulsion d'une tension supérieure à 150 V et uniquement pour des impulsions négatives.

Les champs magnétiques pour écrire les '0' et celui pour écrire les '1' sont de directions opposées, or les impulsions causant des erreurs étant négatives, on peux en déduire que les impulsions ne perturbent pas directement les points mémoires comme c'est le cas pour les champs magnétiques statiques. Ce résultat indique donc une perturbation des blocs logiques CMOS.

En observant la figure 4.16, on constate une exception notable une dizaine de secondes après le front montant du signal *Write Enable*, où quelques bits sont collés à '0'. Cet instant correspond à l'impulsion dans les lignes de courant. Les lignes de courant ayant une surface suffisamment importante pour générer le champ magnétique d'écriture, une cause probable de ces erreurs est un couplage entre le champ magnétique et ces lignes. Un courant opposé à celui généré par la mémoire apparait dû à ce couplage et réduit l'intensité du champ effectif par les lignes de courant. Cette hypothèse est cependant compliquée à vérifier en raison du nombre important de paramètres et de la fenêtre très limitée en temps (l'impulsion dure moins de 10 ns ce qui est proche du pas des impulsions). Ces erreurs sont peu nombreuses au regard de celles causées par une impulsion négative, il s'agit de moins de 250 erreurs contre environ 5 fois plus pour les erreurs sous une impulsion négative.

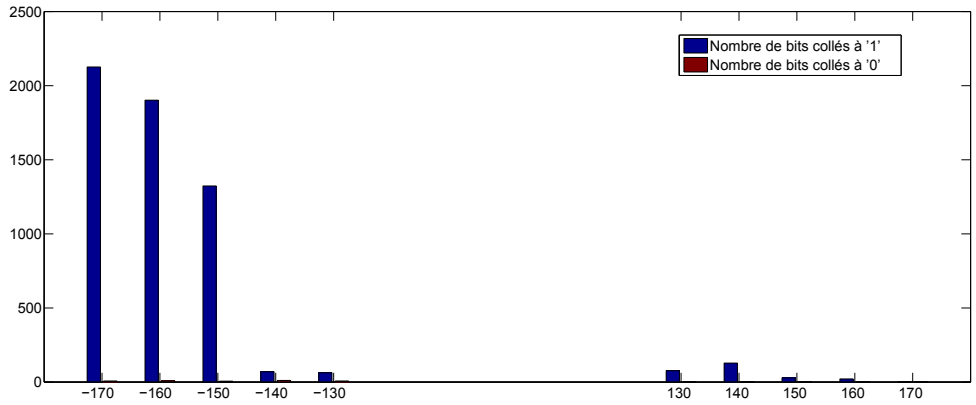

FIGURE 4.20 – Répartition des erreurs en fonction de la tension de l'impulsion

Conclusion

En comparaison avec des attaques à l'aide d'un champ magnétique statique, perturber une MRAM à l'aide d'impulsions électromagnétiques demande plus de ressources et de connaissances sur le fonctionnement interne de la mémoire. Cependant, le fait de pouvoir cibler précisément certaines phases des opérations de la mémoire limite considérablement les risques de détection de l'attaque tout en assurant un taux de succès qui peut être important. L'analyse des résultats de ces attaques montre que les impulsions ont des effets principalement sur la logique de contrôle de la mémoire, plus que sur les cellules elles-mêmes. Les erreurs liées à ces attaques ne sont donc pas directement inhérentes à la technologie MRAM mais plutôt à son implantation. Un effort de développement vers la sécurité de l'implantation des circuits MRAM pourrait donc réduire l'efficacité de ces attaques.

Conclusions et perspectives

Ce travail de thèse avait pour objectif d'explorer le domaine encore peu étudié de la sécurité des mémoires magnétiques face aux attaques physiques. Les schémas d'attaques et de cryptanalyse sur les composants électroniques sont multiples et tous ne sont pas applicables à la technologie MRAM. Cependant, de nouvelles techniques d'attaques ciblant spécifiquement cette technologie peuvent apparaitre. Ce sont ces deux aspects qui ont donc été étudiés.

Le premier chapitre de ce manuscrit a présenté l'écosystème dans lequel se situent les mémoires magnétiques, à savoir les technologies mémoires volatiles et non volatiles, matures et émergentes. La MRAM étant une technologie à fort potentiel qui commence à trouver sa place dans cet écosystème. Le fonctionnement interne de la mémoire a également été détaillé, depuis les interactions microscopiques entre atomes jusqu'aux différentes architectures de mémoires magnétiques. Ces éléments permettent de mieux appréhender les divers effets observés lors des perturbations physiques auxquels ont été soumis les échantillons mis à notre disposition.
Ce chapitre décrit ensuite les différentes techniques d'attaque et de cryptanalyse auxquels les composants électroniques doivent pouvoir faire face. Les applications sécuritaires font parties des domaines dans lesquels Crocus Technology souhaite s'implanter, ainsi il est important de pouvoir se positionner face à ces menaces.
Enfin, les dispositifs expérimentaux développés et utilisés sont décrits. Ils doivent répondre aux deux aspects présentés en introduction : éprouver les mémoires magnétiques face aux attaques connues et étudier les menaces spécifiques à la technologie magnétique.

L'analyse de la sécurité des MRAM porte pour commencer sur l'étude des fuites intrinsèques de la mémoire. En particulier ce sont les émissions électromagnétiques qui ont été observées. Il y a deux raisons à cela, d'une part cela permet de pouvoir étudier précisément la succession des opérations internes de la mémoire lors des opérations de lecture et d'écriture. Ces informations sont primordiales pour la suite du travail, en particulier pour améliorer l'efficacité des perturbations physiques étudiées par la suite. D'autre part, ces analyses permettent de mettre en évidence d'éventuelles failles de sécurité si ces fuites permettent de remonter aux données ou aux adresses transitant dans le composant mémoire.
L'étude a montré que pour l'opération d'écriture, en utilisant une sonde adaptée, il est possible de retrouver les poids de Hamming de certaines données écrites dans la mémoire à partir de l'analyse des émissions électromagnétiques du composant. Pour arriver à ce résultat, une adaptation de l'algorithme du k-means a été utilisée et testée. Elle permet sans connaissance a priori du fonctionnement interne de la mémoire ou de son architecture de pouvoir retrouver plus de 17% des poids de Hamming avec une précision supérieure à 98%.

L'étude des perturbations et des attaques des composants MRAM constitue

l'étape suivante dans l'analyse sécuritaire. La principale menace identifiée provient des champs magnétiques : non seulement le fonctionnement des MRAM très dépendant des interactions magnétiques les rend a priori sensibles à ces perturbations, de plus elles sont très peu étudiées dans le cadre de la sécurité. L'impact d'un champ magnétique sur les mémoires magnétiques a donc été étudié. Plusieurs méthodes pour limiter l'impact des champs magnétiques statiques sont étudiés : l'augmentation de l'intensité du champ d'écriture, l'ajout de code de corrections d'erreurs, l'amélioration de l'empilement magnétique et l'addition d'un bouclier magnétique. Chacune de ces méthodes permet de réduire le nombre d'erreurs causées par le champ magnétique mais au détriment des performances, de la densité, du prix ou de la consommation. Ces inconvénients cantonnent l'utilisation de ces protections à des applications dans des environnements magnétiques extrêmes ou critiques.

Les résultats de ces tests ainsi que l'étude de l'efficacité des contre-mesures ouvrent de nouvelles perspectives en termes d'architecture. En particulier les expériences ont montré que les empilements magnétiques sont sensibles à une direction particulière de champ magnétique et beaucoup plus résistant dans la direction perpendiculaire (identifiées par les axes dits faciles et difficiles). À l'heure actuelle dans les MRAM étudiées, tous les points étaient orientés dans la même direction. Une architecture dans laquelle chaque point mémoire serait composé de deux empilements, dans deux directions perpendiculaires permettrait en théorie de réduire significativement l'impact d'un champ magnétique statique. Des tests préliminaires ont été effectués et ce type d'architecture pourrait permettre de doubler le champ magnétique nécessaire pour fauter la mémoire.
Une autre voie à explorer porte sur l'étude des codes correcteur d'erreurs. En effet les tests effectués dans le chapitre 3 ont montré que les bits de redondance peuvent à partir de certaines intensités de champs magnétiques ajouter trop d'erreurs et devenir contre-productifs. Cependant si l'on tient compte du fait que le type d'erreurs est très dépendant du champ magnétique externe, il est alors possible d'adapter la correction à ce champ en corrigeant préférentiellement les '1' ou les '0'.

La perturbation de circuits par impulsions électromagnétiques est un type d'attaque très efficace sur les circuits logiques ou cryptographiques, mais les mémoires magnétiques, de part leur nature y sont a priori également sensibles. C'est la raison pour laquelle ce type d'attaque a été étudiée : au vu de l'impact important des champs magnétiques statiques, un champ localisé spatialement et temporellement est une faille potentielle importante de sécurité.
Cependant l'expérience a montré que ces impulsions perturbent en premier les blocs logiques de la mémoire, de la même façon qu'ils perturberaient n'importe quel autre type de circuit. Si les points mémoires magnétiques ne sont pas directement sensibles à ces attaques, les perturbations sur le composant mémoire sont cependant importantes. Il a été démontré qu'avec des impulsions synchronisées avec une opération d'écriture il était possible de perturber l'écriture soit des '1' , soit des '0' suivant l'instant d'injection.

Un autre type de perturbation a été testé : les attaques par haute température. En effet, les interactions magnétiques sont très dépendantes des conditions de températures et ceci est d'autant plus vrai sur les technologies de MRAM étudiées qui utilisent un mécanisme d'écriture basé sur l'addition d'une montée en température et d'un champ magnétique. Les tests ont été effectués sur deux types de MRAM : des MRAM Toggle de Everspin et des MRAM TAS de Crocus Technology. L'une comme l'autre ont vu leurs opérations perturbées par la montée en température. Ceci a mené au lancement d'une procédure de dépôt de brevet pour détecter toute perturbation trop importante de la température afin de pouvoir prendre les mesures adaptées.

Le travail présenté porte principalement sur les TAS-MRAM, cependant comme expliqué dans le premier chapitre (section 1.2), il existe d'autres technologies de MRAM. En particulier, la génération suivante de MRAM, les MRAM à couple de transfert de spin ont un fonctionnement différent. En effet elles n'utilisent pas de champs magnétiques pour les opérations d'écriture mais uniquement des courants qui se polarisent en traversant les empilements magnétiques. Les analyses et les attaques étudiées dans ce travail de recherche ouvrent la voie à des adaptations spécifiques à cette nouvelle technologie MRAM. Par exemple, les émissions électromagnétiques et la consommation vont avoir une signature très différente de celle observée dans les échantillons étudiés dans ces recherches. Cependant, rien n'indique a priori que les fuites vont être moins importantes. Ce travail d'analyse est donc un élément important de la caractérisation sécuritaire de cette nouvelle génération de MRAM.

Bibliographie

[1] Jeremy Alvarez Hérault. *Mémoire magnétique à écriture par courant polarisé en spin assistée thermiquement.* Theses, Université de Grenoble, October 2000. (Cité en pages 19 et 29.)

[2] Thomas W Andre, Joseph J Nahas, Chitra K Subramanian, Bradley J Garni, Halbert S Lin, Asim Omair, and William L Martino Jr. A 4-mb 0.18-μm 1t1mtj toggle mram with balanced three input sensing scheme and locally mirrored unidirectional write drivers. *Solid-State Circuits, IEEE Journal of*, 40(1) :301–309, 2005. (Cité en page 20.)

[3] Anonymous. Abstracts of papers to be presented at the 1955 thanksgiving meeting at the university of chicago, chicago, illinois, november 25 and 26, 1955. *Phys. Rev.*, 100 :1235–1235, Nov 1955. (Cité en page 16.)

[4] HD Arnold and GW Elmen. Permalloy, a new magnetic material of very high permeability. *Bell System Technical Journal*, 2(3) :101–111, 1923. (Cité en page 75.)

[5] Mario Norberto Baibich, JM Broto, Albert Fert, F Nguyen Van Dau, F Petroff, P Etienne, G Creuzet, A Friederich, and J Chazelas. Giant magnetoresistance of (001) fe/(001) cr magnetic superlattices. *Physical Review Letters*, 61(21) :2472, 1988. (Cité en page 17.)

[6] Hagai Bar-El, Hamid Choukri, David Naccache, Michael Tunstall, and Claire Whelan. The sorcerer's apprentice guide to fault attacks. *Proceedings of the IEEE*, 94(2) :370–382, 2006. (Cité en page 31.)

[7] Pierre Bayon, Lilian Bossuet, Alain Aubert, Viktor Fischer, François Poucheret, Bruno Robisson, and Philippe Maurine. Contactless electromagnetic active attack on ring oscillator based true random number generator. In *Constructive Side-Channel Analysis and Secure Design*, pages 151–166. Springer, 2012. (Cité en pages 31 et 90.)

[8] Jim Belleson and Ed Grochowski. The era of giant magnetoresistive heads. *Hitachi Global Storage Technologies*, 1998. (Cité en page 20.)

[9] AE Berkowitz and Kentaro Takano. Exchange anisotropy ?a review. *Journal of Magnetism and Magnetic Materials*, 200(1) :552–570, 1999. (Cité en page 25.)

[10] Eli Biham and Adi Shamir. Differential fault analysis of secret key cryptosystems. In *Advances in Cryptology ?CRYPTO'97*, pages 513–525. Springer, 1997. (Cité en page 32.)

[11] Dan Boneh, Richard A DeMillo, and Richard J Lipton. On the importance of checking cryptographic protocols for faults. In *Advances in Cryptology ?EUROCRYPT ?97*, pages 37–51. Springer, 1997. (Cité en page 32.)

[12] M. Bowen, V. Cros, F. Petroff, A. Fert, C. Martinez Boubeta, J.L. Costa-Kramer, J.V. Anguita, A. Cebollada, F. Briones, J.M. de Teresa, L. Morellon,

M.R. Ibarra, F. Guell, F. Peiro, and A. Cornet. Large magnetoresistance in fe/mgo/feco(001) epitaxial tunnel junctions on gaas(001). *Applied Physics Letters*, 79(11) :1655–1657, Sep 2001. (Cité en page 19.)

[13] Eric Brier, Christophe Clavier, and Francis Olivier. Correlation power analysis with a leakage model. In *Cryptographic Hardware and Embedded Systems-CHES 2004*, pages 16–29. Springer, 2004. (Cité en page 32.)

[14] J. Brouchier, T. Kean, C. Marsh, and D. Naccache. Temperature attacks. *Security Privacy, IEEE*, 7(2) :79–82, March 2009. (Cité en page 31.)

[15] Bruno Bureau, Xiang Hua Zhang, Frederic Smektala, Jean-Luc Adam, Johann Troles, Hong-li Ma, Catherine Boussard-Plèdel, Jacques Lucas, Pierre Lucas, David Le Coq, et al. Recent advances in chalcogenide glasses. *Journal of non-crystalline solids*, 345 :276–283, 2004. (Cité en page 9.)

[16] Jean-Cédric Chappelier. (Cité en page 71.)

[17] De Charentenay. Emerging nvm market : Mram positionning vs pcm and reram. InMRAM, 2014. (Cité en pages 3, 8, 24 et 29.)

[18] Yong Chen, Gun-Young Jung, Douglas AA Ohlberg, Xuema Li, Duncan R Stewart, Jan O Jeppesen, Kent A Nielsen, J Fraser Stoddart, and R Stanley Williams. Nanoscale molecular-switch crossbar circuits. *Nanotechnology*, 14(4) :462, 2003. (Cité en page 9.)

[19] Control Data Corporation. Reference manual. `http://ygdes.com/CDC/60100000D_6600refMan_Feb67.pdf`. Accessed : 2015-08-03. (Cité en page vii.)

[20] Gregory Di Pendina. *ASIC Innovative design and Process Design Kit development for Hybride CMOS / Magnetic Technology.* Theses, Université de Grenoble, October 2012. (Cité en pages 6 et 7.)

[21] V. Drchal, J. Kudrnovský, P. Bruno, I. Turek, P. H. Dederichs, and P. Weinberger. Temperature dependence of the interlayer exchange coupling in magnetic multilayers : An *ab initio* approach. *Phys. Rev. B*, 60 :9588–9595, Oct 1999. (Cité en pages 85 et 86.)

[22] M Durlam, D Addie, J Akerman, B Butcher, P Brown, J Chan, M DeHerrera, BN Engel, B Feil, G Grynkewich, et al. A 0.18/spl mu/m 4mb toggling mram. In *Electron Devices Meeting, 2003. IEDM'03 Technical Digest. IEEE International*, pages 34–6. IEEE, 2003. (Cité en page 85.)

[23] B. N. Engel, J. Akerman, B. Butcher, R.W. Dave, M. DeHerrera, M. Durlam, G. Grynkewich, J. Janesky, S.V. Pietambaram, N.D. Rizzo, J.M. Slaughter, K. Smith, J. J. Sun, and S. Tehrani. A 4-mb toggle mram based on a novel bit and switching method. *Magnetics, IEEE Transactions on*, 41(1) :132–136, 2005. (Cité en page 24.)

[24] Magnetic Shield Electromagnetic Engineering. Wmu metal sheet. `http://mumetalsheet.co.uk/mu-metal`. Accessed : 2015-03-30. (Cité en page 75.)

[25] Everspin. Everspin mr2a08a. `http://www.everspin.com/PDF/EST_MR2A08A_prod.pdf`. Accessed : 2015-03-05. (Cité en page 38.)

[26] Steven Roger Fischer. *History of Writing*. Reaktion Books, 2004. (Cité en page vii.)

[27] Jay W Forrester. Digital information storage in three dimensions using magnetic cores. *Journal of Applied Physics*, 22(1) :44–48, 1951. (Cité en page 20.)

[28] Daniel Genkin, Adi Shamir, and Eran Tromer. Rsa key extraction via low-bandwidth acoustic cryptanalysis. In *Advances in Cryptology–CRYPTO 2014*, pages 444–461. Springer, 2014. (Cité en page 32.)

[29] Yole Geveloppement. Yole developpement sees the pcm and mram markets reaching 1,6 billion dollars in 2018. . Accessed : 2015-01-04. (Cité en page 9.)

[30] Kamil Gomina, J Rigaud, Philippe Gendrier, Philippe Candelier, and Assia Tria. Power analysis methodology for secure circuits. In *Design and Diagnostics of Electronic Circuits & Systems (DDECS), 2013 IEEE 16th International Symposium on*, pages 102–107. IEEE, 2013. (Cité en page 32.)

[31] Yoann Guillemenet, Lionel Torres, Gilles Sassatelli, Nicolas Bruchon, and Ilham Hassoune. A non-volatile run-time fpga using thermally assisted switching mrams. In *Field Programmable Logic and Applications, 2008. FPL 2008. International Conference on*, pages 421–426. IEEE, 2008. (Cité en page vii.)

[32] Hynix. Hynix sram 512mb. http://fr.farnell.com/hynix-semiconductor/h55s5122efr-60m/sdram-mobile-512mb-166mhz-90fbga/dp/2314396. Accessed : 2015-02-12. (Cité en page 5.)

[33] Kees A Schouhamer Immink. Reed-solomon codes and the compact disc. *Reed-Solomon codes and their applications*, pages 41–59, 1994. (Cité en page 70.)

[34] Scott Jacobson. How flash and dram growth trends are reshaping the memory industry. http://www.chipestimate.com/tech-talks/2012/08/07/Cadence-How-Flash-and-DRAM-Growth-Trends-are-Reshaping-the-Memory-Industry. Accessed : 2015-08-03. (Cité en page vii.)

[35] Michel Julliere. Tunneling between ferromagnetic films. *Physics Letters A*, 54(3) :225–226, 1975. (Cité en pages 17 et 18.)

[36] JA Katine and Eric E Fullerton. Device implications of spin-transfer torques. *Journal of Magnetism and Magnetic Materials*, 320(7) :1217–1226, 2008. (Cité en page 29.)

[37] Charles Kittel, Paul McEuen, and Paul McEuen. *Introduction to solid state physics*, volume 8. Wiley New York, 1976. (Cité en pages 15 et 68.)

[38] Paul Kocher, Joshua Jaffe, and Benjamin Jun. Differential power analysis. In *Advances in Cryptology ?CRYPTO ?99*, pages 388–397. Springer, 1999. (Cité en page 32.)

[39] A. Kolodny, S.T.K. Nieh, B. Eitan, and J. Shappir. Analysis and modeling of floating-gate eeprom cells. *Electron Devices, IEEE Transactions on*, 33(6) :835–844, Jun 1986. (Cité en page 7.)

[40] Stuart P Lloyd. Least squares quantization in pcm. *Information Theory, IEEE Transactions on*, 28(2) :129–137, 1982. (Cité en page 52.)

[41] Florence Jessie MacWilliams and Neil James Alexander Sloane. *The theory of error correcting codes*, volume 16. Elsevier, 1977. (Cité en page 72.)

[42] Timothy C May and Murray H Woods. A new physical mechanism for soft errors in dynamic memories. In *Reliability Physics Symposium, 1978. 16th Annual*, pages 33–40. IEEE, 1978. (Cité en page 31.)

[43] JS Moodera, L Kinder, P Leclair, R Meservey, and J Nowak. Origin of magnetoresistance in ferromagnetic tunnel junctions and ways to optimize the effect. In *APS March Meeting Abstracts*, volume 1, page 2205, 1996. (Cité en page 18.)

[44] Robert H Morelos-Zaragoza. *The art of error correcting coding*. John Wiley & Sons, 2006. (Cité en page 72.)

[45] Nicolas Moro, Amine Dehbaoui, Karine Heydemann, Bruno Robisson, and Emmanuelle Encrenaz. Electromagnetic fault injection : towards a fault model on a 32-bit microcontroller. In *Fault Diagnosis and Tolerance in Cryptography (FDTC), 2013 Workshop on*, pages 77–88. IEEE, 2013. (Cité en page 90.)

[46] David Morton. Inventing the wire recorder. http://www.recording-history.org/HTML/wire2.php. Accessed : 2015-01-21. (Cité en page 20.)

[47] MRAM-Info. Buffalo memory launched the first product with stt-mram - a new industrial sata iii ssd. http://www.mram-info.com/buffalo-memory-launched-first-product-stt-mram-new-industrial-sata-iii-ssd. Accessed : 2015-08-04. (Cité en page vii.)

[48] MRAM-Info. Toshiba developed stt-mram based microprocessor cache memory. http://www.mram-info.com/toshiba-developed-stt-mram-based-microprocessor-cache-memory. Accessed : 2015-08-05. (Cité en page vii.)

[49] Computer History Museum. Williams-kilburn tubes. http://www.computerhistory.org/revolution/memory-storage/8/308. Accessed : 2015-02-02. (Cité en page vii.)

[50] R Omarouayache, J Raoult, S Jarrix, L Chusseau, and P Maurine. Magnetic microprobe design for em fault attack. In *Electromagnetic Compatibility (EMC EUROPE), 2013 International Symposium on*, pages 949–954. IEEE, 2013. (Cité en page 91.)

[51] International Commission on Non-Ionizing Radiation Protection et al. Guidelines on limits of exposure to static magnetic fields. *Health Physics*, 96(4) :504–514, 2009. (Cité en page 61.)

[52] Thomas Ordas, Mathieu Lisart, Etienne Sicard, Philippe Maurine, and Lionel Torres. Near-field mapping system to scan in time domain the magnetic emissions of integrated circuits. In *Integrated Circuit and System Design. Power and Timing Modeling, Optimization and Simulation*, pages 229–236. Springer, 2009. (Cité en page 42.)

[53] Stanford R Ovshinsky. Reversible electrical switching phenomena in disordered structures. *Physical Review Letters*, 21(20) :1450, 1968. (Cité en page 9.)

[54] Wolfgang Pauli. Exclusion principle and quantum mechanics. http://www.nobelprize.org/nobel_prizes/physics/laureates/1945/pauli-lecture.pdf. Accessed : 2015-06-04. (Cité en page 12.)

[55] François Poucheret, Karim Tobich, M Lisarty, Laurent Chusseau, Bruno Robisson, and Philippe Maurine. Local and direct em injection of power into cmos integrated circuits. In *Fault Diagnosis and Tolerance in Cryptography (FDTC), 2011 Workshop on*, pages 100–104. IEEE, 2011. (Cité en page 90.)

[56] V. Pouget, A. Douin, G. Foucard, P. Peronnard, D. Lewis, P. Fouillat, and R. Velazco. Dynamic testing of an sram-based fpga by time-resolved laser fault injection. In *On-Line Testing Symposium, 2008. IOLTS '08. 14th IEEE International*, pages 295–301, July 2008. (Cité en page 31.)

[57] I L Prejbeanu, M Kerekes, R C Sousa, H Sibuet, O Redon, B Dieny, and J P Nozières. Thermally assisted MRAM. *Journal of Physics : Condensed Matter*, 19(16) :165218, April 2007. (Cité en pages 23, 26 et 28.)

[58] User Datagram Protocol. Rfc 768 j. postel isi 28 august 1980. *Isi*, 1980. (Cité en page 70.)

[59] S. Raoux, G.W. Burr, M.J. Breitwisch, C.T. Rettner, Y.C. Chen, R.M. Shelby, M. Salinga, D. Krebs, S.-H. Chen, H. L Lung, and C.H. Lam. Phase-change random access memory : A scalable technology. *IBM Journal of Research and Development*, 52(4.5) :465–479, July 2008. (Cité en page 9.)

[60] Romain Ravaud and Guy Lemarquand. Magnetic field produced by a parallelepipedic magnet of various and uniform polarization. *Progress In Electromagnetics Research*, 98 :207–219, 2009. (Cité en page 61.)

[61] Nicholas D Rizzo, Mark F Deherrera, and Bradley N Engel. Magnetic random access memory having digit lines and bit lines with a ferromagnetic cladding layer, August 6 2002. US Patent 6,430,084. (Cité en page 78.)

[62] Cyril Roscian, Alexandre Sarafianos, J-M Dutertre, and Assia Tria. Fault model analysis of laser-induced faults in sram memory cells. In *Fault Diagnosis and Tolerance in Cryptography (FDTC), 2013 Workshop on*, pages 89–98. IEEE, 2013. (Cité en page 32.)

[63] Melvin A Ruderman and Charles Kittel. Indirect exchange coupling of nuclear magnetic moments by conduction electrons. *Physical Review*, 96(1) :99, 1954. (Cité en page 21.)

[64] Sergei Skorobogatov. Local heating attacks on flash memory devices. In *Hardware-Oriented Security and Trust, 2009. HOST'09. IEEE International Workshop on*, pages 1–6. IEEE, 2009. (Cité en page 32.)

[65] John C Slonczewski. Current-driven excitation of magnetic multilayers. *Journal of Magnetism and Magnetic Materials*, 159(1) :L1–L7, 1996. (Cité en page 29.)

[66] Statista. Forecast for global semiconductor revenue from 2012 to 2017 (in billion u.s. dollars). http://www.statista.com/statistics/272872/

global-semiconductor-industry-revenue-forecast/. Accessed : 2015-03-04. (Cité en page 2.)

[67] Statista. Global semiconductor industry revenue from memory components from 2006 to 2016. http://www.statista.com/statistics/266987/forecast-of-worldwide-semiconductor-sales-from-memory-components. Accessed : 2015-03-04. (Cité en page 2.)

[68] D. Takashima. Overview of ferams : Trends and perspectives. In *Non-Volatile Memory Technology Symposium (NVMTS), 2011 11th Annual*, pages 1–6, Nov 2011. (Cité en page 8.)

[69] Georgios Tsiligiannis, Luigi Dilillo, Alberto Bosio, Patrick Girard, Aida Todri, Arnaud Virazel, SS McClure, AD Touboul, Frédéric Wrobel, and Frédéric Saigne. Testing a commercial mram under neutron and alpha radiation in dynamic mode. *Nuclear Science, IEEE Transactions on*, 60(4) :2617–2622, 2013. (Cité en page 80.)

[70] M. Van Buskirk. Conductive bridging ram (cbramt : A scalable, low power and high performance resistive memory technology platform. In *Interconnect Technology Conference (IITC), 2012 IEEE International*, pages 1–3, June 2012. (Cité en page 10.)

[71] Shih-Hui Wang, Ke-Chin Lin, Cheng-Tyng Yen, Dun-Ying Shu, MJ Kao, and Ming-Jinn Tsai. Application of cmp to the cladding layer of mram. In *Planarization/CMP Technology (ICPT), 2007 International Conference on*, pages 1–4. VDE, 2007. (Cité en page 78.)

[72] Rainer Waser, Regina Dittmann, Georgi Staibayon2012contactlessv, and Kristof Szot. Redox-based resistive switching memories–nanoionic mechanisms, prospects, and challenges. *Advanced Materials*, 21(25-26) :2632–2663, 2009. (Cité en page 10.)

[73] Z. Zhang, L. Zhou, P.E. Wigen, and K. Ounadjela. Temperature dependence of interlayer exchange coupling in co/ru/co trilayer structures. *Journal of Applied Physics*, 75(10) :6434–6436, 1994. (Cité en page 85.)

[74] Loic Zussa, J-m Dutertre, Jessy Clédiere, Bruno Robisson, and Assia Tria. Investigation of timing constraints violation as a fault injection means. In *27th Conference on Design of Circuits and Integrated Systems (DCIS), Avignon, France*, 2012. (Cité en page 31.)

[75] Loic Zussa, J-M Dutertre, Jessy Clediere, and Assia Tria. Power supply glitch induced faults on fpga : An in-depth analysis of the injection mechanism. In *On-Line Testing Symposium (IOLTS), 2013 IEEE 19th International*, pages 110–115. IEEE, 2013. (Cité en page 31.)