# «SÉCURITÉ DES SYSTÈMES CRYPTOGRAPHIQUES EMBARQUÉS VIS À VIS DES ATTAQUES PHYSIQUES» PAR ALBERTO BATTISTELLO

**Présentée par : Alberto Battistello Discipline : informatique Laboratoire : LMV**

Résumé :
Le sujet de cette thèse est l'analyse de sécurité des implantations cryptographiques embarquées.
La sécurité a toujours été un besoin primaire pour les communications stratégiques et diplomatiques dans l'histoire. Le rôle de la cryptologie a donc été de fournir les réponses aux problèmes de sécurité, et le recours à la cryptanalyse a souvent permis de récupérer le contenu des communications des adversaires.
L'arrivée des ordinateurs a causé un profond changement des paradigmes de communication et aujourd'hui le besoin de sécuriser les communications ne s'étend qu' aux échanges commerciaux et économiques.
La cryptologie moderne offre donc les solutions pour atteindre ces nouveaux objectifs de sécurité, mais ouvre la voie à des nouvelles attaques : c'est par exemple le cas des attaques par fautes et par canaux auxiliaires, qui représentent aujourd'hui les dangers plus importants pour les implantations embarquées.

Cette thèse résume le travail de recherche réalisé ces trois dernières années dans le rôle d'ingénieur en sécurité au sein d'Oberthur Technologies. La plupart des résultats a été publiée sous forme d'articles de recherche ou de brevets.
Les objectifs de recherche en sécurité pour les entreprises du milieu de la sécurité embarqué sont doubles. L'ingénieur en sécurité doit montrer la capacité d'évaluer correctement la sécurité des algorithmes et de mettre en avant les possibles dangers futurs. Par ailleurs il est désirable de découvrir des nouvelles techniques de défense qui permettent d'obtenir un avantage sur les concurrents. C'est dans ce contexte que ce travail est présenté.
Ce manuscrit est divisé en quatre chapitres principaux.
Le premier chapitre présente une introduction aux outils mathématiques et formels nécessaires pour comprendre la suite. Des résultats et notions fondamentaux de la théorie de l'information, de la complexité, et des probabilités sont présentés, ainsi qu'une introduction à l'architecture des micro-ordinateurs.
Le chapitre suivant présente la notion d'attaque par faute et des stratégies connues pour contrecarrer ce type d'attaques. Le corps du deuxième chapitre est ensuite dédié à notre travail sur le code infectif pour les algorithmes symétriques et asymétriques ainsi que à notre travail sur les attaques par faute sur courbes elliptiques.
Le troisième chapitre est dédié aux attaques par canaux auxiliaires, et présente une introduction aux résultats et à certaines attaques et contremesures classiques du domaine. Ensuite nos deux nouvelles attaques ciblant des contremesures considérées sécurisées sont présentées. Dans ce troisième chapitre est enfin présentée notre nouvelle attaque combinée qui permet de casser des implémentations sécurisées à l'état de l'art.
A la fin de ce manuscrit, le quatrième chapitre présente les conclusions de notre travail, ainsi que des perspectives pour des nouveaux sujets de recherche.
Pendant nos investigations nous avons trouvé différentes contremesures qui permettent de contrecarrer certaines attaques.
Ces contremesures ont été publiées sous la forme de brevets. Dans certains cas les contremesures sont présentées avec l'attaque qu'elles contrecarrent.

Abstract :
The subject of this thesis is the security analysis of cryptographic implementations. The need for secure communications has always been a primary need for diplomatic and strategic communications. Cryptography has always been used to answer this need and cryptanalysis have often been solicited to reveal the content of adversaries secret communications. The advent of the computer era caused a shift in the communication paradigms and nowadays the need for secure communications extends to most of

commercial and economical exchanges. Modern cryptography provides solutions to achieve such new security goals but also open the way to a number of new threats. It is the case of fault and side-channel-attacks, which today represents the most dangerous threats for embedded cryptographic implementations. This thesis resumes the work of research done during the last years as a security engineer at Oberthur Technologies. Most of the results obtained have been published as research papers or patents. The security research goals of companies around the world working in the embedded domain are twofold. The security engineer has to demonstrate the ability to correctly evaluate the security of algorithms and to highlight possible threats that the product may incur during its lifetime. Furthermore it is desirable to discover new techniques that may provide advantages against competitors. It is in this context that we present our work.
This manuscript is divided into four main chapters.
The first chapter presents an introduction to various mathematical and computational aspects of cryptography and information theory. We also provide an introduction to the main aspects of the architecture of secure micro-controllers.
Afterwards the second chapter introduces the notion of fault attacks and presents some known attack and countermeasure. We then detail our work on asymmetric and symmetric infective fault countermeasures as long as on elliptic curves fault attacks.
The third chapter discusses about side-channels, providing a brief introduction to the subject and to well-known side-channel attacks and countermeasures. We then present two new attacks on implementations that have been considered secure against side channels. Afterwards we discuss our combined attack which breaks a state-of-the-art secure implementation.
Finally, the fourth chapter concludes this works and presents some perspectives for further research.
During our investigations we have also found many countermeasures that can be used to thwart attacks. These countermeasures have been mainly published in the form of patents. Where possible some of them are presented along with the attack they are conceived to thwart.

## INFORMATIONS COMPLÉMENTAIRES

**Jean-Sébastien CORON**, Maître de Conférences, Habilité à Diriger des Recherches, à l' Université du Luxembourg/Département Informatique - Luxembourg (Luxembourg) - Rapporteur
**Emmanuel PROUFF**, Ingénieur, à Safran Morpho - Issy-les-Moulineaux - Rapporteur
**Louis GOUBIN**, Professeur des Universités, à l'Université Versailles Saint-Quentin-en-Yvelines/Laboratoire Mathématiques de Versailles (LMV) - Versailles - Directeur de

thèse
**Christophe GIRAUD**, Ingénieur, à Oberthur Technologies - Pessac - Co-Encadrant de thèse
**Benedikt GIERLICHS**, Chercheur, à l'Université Catholique de Louvain/Département d' Ingénierie Electrique - Heverlee (Belgique) - Examinateur
**Sylvain GUILLEY**, Professeur, à Télécom ParisTech - Laboratoire Traitement et Communication de l'Information (LTCI) - UMR 5141 - Paris - Examinateur
**David POINTCHEVAL**, Directeur de Recherche CNRS, à ENS Paris/Département d' Informatique - Paris - Examinateur
**Gilles ZEMOR**, Professeur des Universités, à l'Université de Bordeaux/Institut de Mathématiques de Bordeaux - Talence - Examinateur
**Christophe CLAVIER**, Professeur des Universités, à l'Université de Limoges/Institut de recherche Xlim - UMR CNRS 7252 - Limoges - Invité

**Contact :** dredval - service FED : theses@uvsq.fr