SICORP France ICT final summary

Project title : Security evaluation of physically attacked cryptoprocessors in embedded system(SPACES)

Coordinator of the French part of the project : Jean-Luc Danger (Telecom ParisTech)

Coordinator of the Japanese part of the project : Naofumi Homma (Tohoku University)

Project period : 1 December 2010 - 31 March 2014

CONSOLIDATED PUBLIC SUMMARY IN ENGLISH

Development of unified security evaluation platform for embedded cryptographic systems

General Objectives:

Development of security evaluation methodologies on cryptographic modules against physical attacks before fabricating actual chips

Physical attacks based on side-channel observation (side-channel attacks), are now of major concern for design and evaluation of cryptographic devices. From an industrial point of view, if the product is not robust enough, it has to be redesigned. Such redesign is very costly and sometimes impossible. However, there is no dedicated method or technology to design and evaluate the robustness before the fabrication phase. Conventional simulators are not suitable due to the computation time or inaccuracy. Even worse, the attacks based on Electromagnetic (EM) radiation are more and more powerful, which requires a new security boundary that cannot be simulated by conventional methods. In addition, the robustness is heavily dependent on the type of implementation. Addressing the above issues, this project did a comprehensive study of security evaluation methodologies for cryptographic devices against physical attacks. In particular, we have developed a novel evaluation platform based on high-accuracy security simulation and in-situ evaluations. The main results give the future prospects about the product robustness over physical attacks without fabricating actual chips. This project has also led to a new research area “EM Information Security” in the research field of electric circuit design.

Methods or technologies :

Security evaluation of cryptographic devices by a dedicated simulator and rapid prototyping platform applicable to various implementation methods

A specific simulation engine was developed for a novel simulation technology to evaluate the robustness of cryptographic devices against side-channel attacks. The associated simulation models were also developed at two levels of abstraction: (i) high-level model where the circuit is like a black box, and (ii) low-level model based on post-layout circuit data. An effective extraction of physical parameters was proposed as a key technology to simulate a cryptographic device in the low-level model. The simulation is efficiently calculated to obtain the accurate information of the device robustness without fabricating actual chips. On the other hand, a rapid prototyping platform was constructed based on a newly developed evaluation board and custom ASICs plugged via daughter boards. The target implementations that can be handled on the platform are FPGA, ASIC and IC card ones. A novel analysis technique was also studied in order to enhance the accuracy and efficiency of the security evaluation. Moreover new evaluation methods for attacks based on electromagnetic (EM) information leakage and EM fault injection from/to cryptographic devices were studied with a developed EM probing system.

Project main results :

This project has successfully developed a novel simulation technology to evaluate the robustness of cryptographic devices against physical attacks, a prototyping platform consisting of a new evaluation board and custom ASICs developed by all partners. The project has also achieved some novel analysis techniques for the security evaluation which have not been foreseen from the beginning. Moreover, this project brought strong links between the Japanese and French partners, which resulted in exchanges of young researchers, promising research fields and further collaboration possibilities.

Added Value from International collaborative work :

The French partners have been mainly focusing on both a “top-down” approach and analysis algorithms to understand the issues of physical attacks such as a high-level simulator and an analysis technique for evaluating cryptographic modules. The Japanese partners have much knowledge and experiences of implementing actual evaluation boards and cryptographic circuits and of measuring real power/EM signals, which is so-called a “bottom-up” approach. The partners ideally combined efficiently these two complementary approaches.

Scientific production and patents :

The major scientific productions of this project are as follows

- **Specific circuit simulator "SPACES simulator"** to simulate transient signals effectively related to side-channel information such as signal glitches,
- **Rapid prototyping/evaluation platform** to implement and evaluate a variety of cryptographic modules on FPGA, ASIC and Smart cards.
- **VLSI chip "SPACES explorer"** for extremely deep analysis of physics behind attacks
- **Establishment of new research area "EM Information Security"** in the research field of Electromagnetic Compatibility

Illustrations

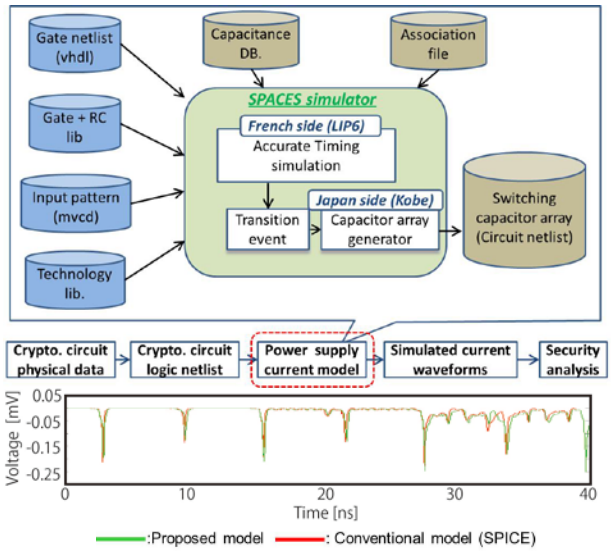

Fig. 1 : Framework of developed simulator and example of wareforms

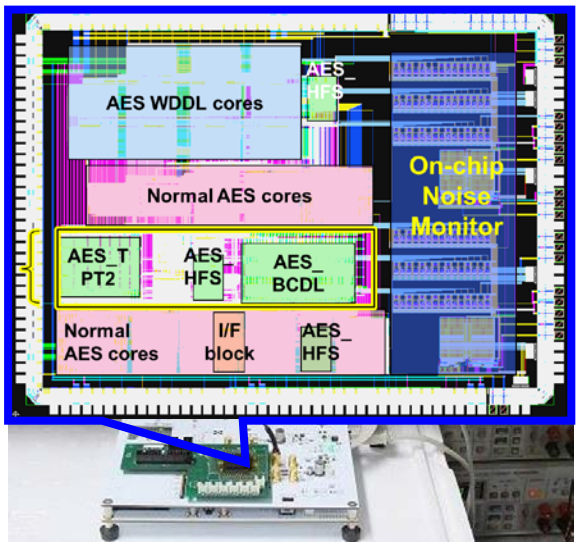

Fig. 2 : SPACES Explorer (VLSI chip) and evaluation platform

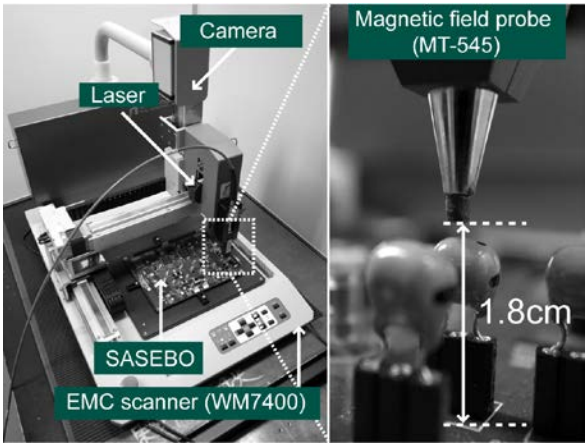

Fig. 3 : Development of estimation and visualization system for information leakage risk

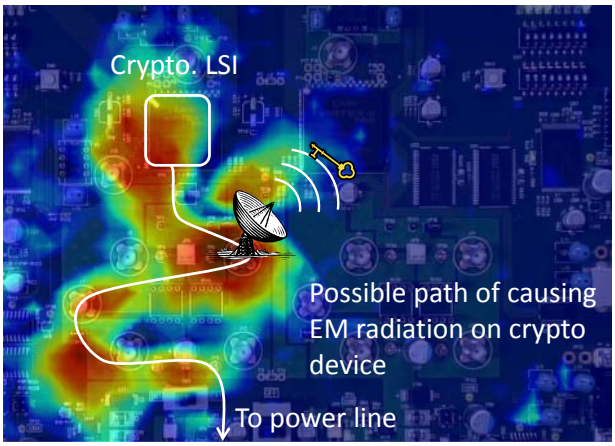

Fig. 4 : Estimation result of Electromagnetic information leakage risk

Factual information:

The SPACES project is an industrial research coordinated by Jean-Luc Danger in France and by Naofumi Homma in Japan. It associate Telecom ParisTech (e.g., Jean-Luc Danger), LIP6 (e.g., Pirouz Bazargan-Sabet), Morpho (e.g., Thanh Ha Le), as well as Tohoku Univ (e.g., Naofumi Homma), AIST (e.g., Shinichi Kawamura), UEC (e.g., Kazuo Sakiyama), Kobe Univ (e.g., Makoto Nagata). The project started on December 1, 2010 and lasted 40 months. ANR grant amounted to 738,105 € and JST grant amounted to ¥149,500,000 .

SICORP 仏 情報通信技術（ICT） 終了報告書（概要）

課題名：Security evaluation of physically attacked cryptoprocessors in embedded system(SPACES)

フランス側代表者名・所属：代表：Jean-Luc Danger（テレコムパリテック）

日本側代表者名・所属：代表：本間 尚文（東北大学）

期間：2010 年 12 月 1 日 ～ 2014 年 3 月 31 日

CONSOLIDATED PUBLIC SUMMARY IN JAPANESE

組込み暗号処理システムの統合安全性評価プラットフォームの開発

要約：物理攻撃の対象となる組込み系暗号システムの新たな安全性評価手法の開発

正規の入出力チャネル以外から漏洩する情報を用いた物理攻撃（サイドチャネル攻撃）は，暗号処理デバイスの設計や安全性評価において大きな懸案となっている．産業上の観点では，製品認証の段階でその安全性に問題が指摘された場合，その不具合の修正に再設計を余儀なくされてしまう．この再設計は製品の市場流通を大きく遅らせ，コストを増加させ，結果として製品の競争力を大幅に減退させてしまう．しかしながら，そのような事前評価のための理論や技術は今日に至るまで確立していない．従来のシミュレーション技術は，計算量や精度の観点から適用が難しい．また，観測されるサイドチャネル情報が実装の詳細（回路アーキテクチャ，デバイスの種類，計測器や計測環境）に大きく依存することも問題となる．それに加えて，サイドチャネル攻撃（特に漏洩電磁波を用いた攻撃）は年々発展しており，デバイス近傍のみを取り扱う従来の評価手法を適用することは極めて困難となっている．本プロジェクトでは，これらの問題を解決するため，新たな安全性評価理論および技術の包括的な研究を実施した．特に，高精度なシミュレーションとプロトタイプによる実地的な評価を組み合わせた統一的な安全性評価プラットフォームを構築した．本成果により，製造に先立ち，物理攻撃に対する暗号機器の情報漏洩リスクを高精度に評価可能となることが期待される．また，本プロジェクトの成果が契機となり，環境電磁工学分野において，「電磁情報セキュリティ」という新たな研究領域が創始された．

手法：暗号機器の安全性評価専用シミュレータおよび多様な実装に適用可能な高速試作・評価プラットフォームの開発

本プロジェクトでは，暗号機器のサイドチャネル攻撃に対する安全性評価に特化した新たなシミュレーション技術を開発した．同シミュレータは，回路詳細を抽象化した高位モデル，回路レイアウトの物理データを用いた低位モデルと，それらのモデルを用いて効率的な動作解析を行うシミュレーションエンジンから構成される．低位モデルで暗号機器をシミュレートするためのキーテクノロジは物理データの効率的な抽出である．同シミュレーションでは，これを用いて，製品を実際に製造することなく安全性評価に関する正確な情報を得ることができる．また，本プロジェクトでは，これと並行して，高速試作/評価プラットフォームを開発した．同プラットフォームは，新たに開発した評価ボードとその解析・評価ソフトウェア群から構成される．本プラットフォームの開発により，暗号デバイスおよびそのソフトウェア・ハードウェア対策の設計を製造前に評価することが可能となる．特に，開発したプラットフォームでは，FPGA（再構成可能な LSI），ASIC（専用 LSI）からスマートカードまでの多様な実装を評価することができる．そこで，様々なアーキテクチャによる暗号回路を搭載した専用 LSI コアを開発し，サイドチャネル情報の収集・詳細評価を実施した．それに加えて，評価の精度と効率をさらに高めるため，新たな解析技術も合わせて開発した．電磁的な情報漏洩や故障注入を利用した攻撃については，新たに電磁波計測システムを開発することで，その物理メカニズムの解明を行った．

プロジェクトの主な成果：

本プロジェクトでは，当初計画の通り，上記のシミュレーション技術および高速な試作・評価プラットフォームの開発に成功した．特に，評価用 ASIC は日仏共同研究者の 6 か月以上の緊密な協働によって開発された．また，新たな解析・評価技術の開発に成功するなど，一部では計画を上回る成果が得られた．そのような成果は，本プロジェクトに参画した多様な研究者の相乗効果によって初めて実現されたものである．上記の学術的・技術的成果により，環境電磁工学の分野では，電磁情報セキュリティと呼ばれる新たな研究領域が創始された．それに加えて，若手研究者の相互交流などを通して，参画研究者間の強固なパートナーシップが形成された．日仏双方の参画者は，本プロジェクトの内容を発展させ，将来的にも連携していく予定である．

国際共同研究によって得られた付加的な価値：

フランス側のメンバーは，暗号モジュールのサイドチャネル攻撃への安全性評価を，主にトップダウンアプローチによるハイレベルなシミュレータと解析アルゴリズムの側面から実施してきた．一方，日本側のメンバーは，いわゆるボトムアップアプローチにより，評価ボードや暗号回路の実装，電力・電磁波信号の計測を豊富な知識と経験をもとに実施してきた．本プロジェクトのコンソーシアムは，上記のトップダウンとボトムアップのアプローチを理想的に組み合わせた構成となっており，学際的な研究領域である物理攻撃に対する暗号機器の安全性評価研究を相互補完的に推進することができた．

プロジェクト開始以降の学術的な成果物：

本プロジェクトの主な成果を以下に示す.

- **サイドチャネル情報評価用回路シミュレータ“SPACES シミュレータ”** ：信号の急峻な変化などサイドチャネル情報に関する時間信号変化を効率的に計算可能なシミュレータ.
- **高速な試作・評価プラットフォーム：**FPGA や ASIC，スマートカード上での 多様な実装を評価可能とする統合プラットフォーム.
- **評価用暗号 LSI“SPACES Explorer”：** 様々なアーキテクチャの暗号回路を搭載した評価用 LSI. 内部のサイドチャネル情報を詳細評価するためのオンチップモニタも搭載.
- **新研究領域“電磁情報セキュリティ”：**本プロジェクトの成果が契機となり，米国電気電子学会(IEEE)環境電磁工学ソサイエティにおいて新たな承認された技術小委員会．初代委員長に本プロジェクト参画研究者が選出された.

説明図

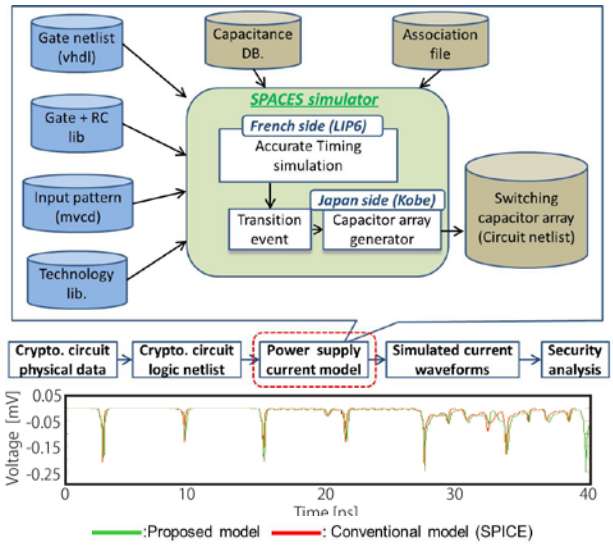

図 1： 開発したシミュレータの構成と波形例 .

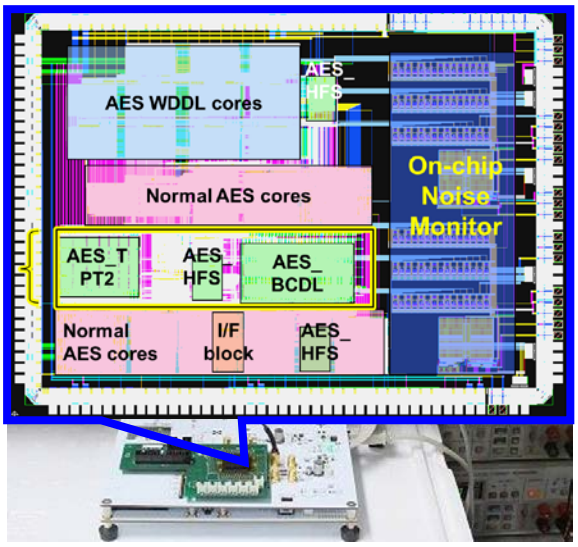

図 2： 開発した評価用暗号 LSI と評価プラットフォーム.

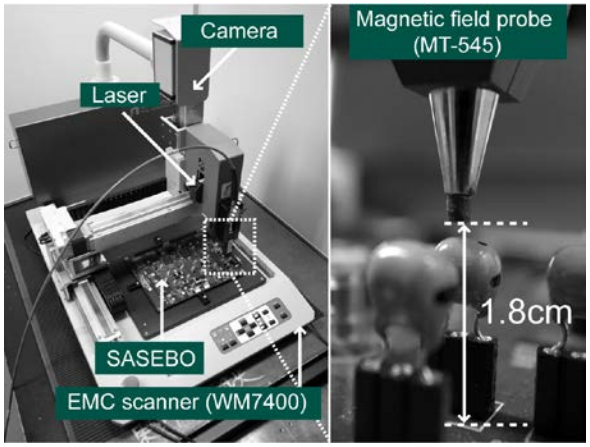

図 3：開発した情報漏えいリスクの推定・可視化システム.

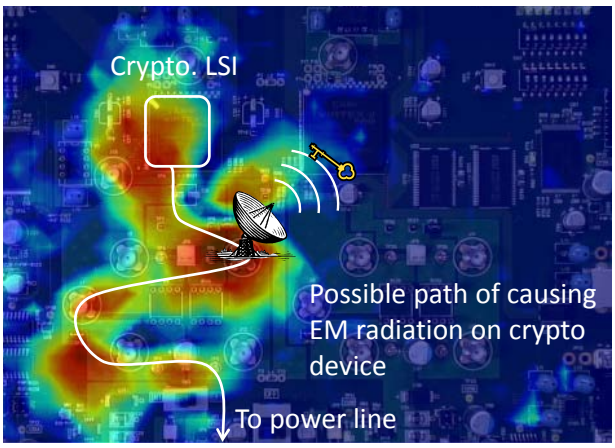

図 4：電磁情報漏えいリスクの推定結果例.

事実情報：

本プロジェクトは，フランス側の研究分類では「Industrial research」に分類される．フランス側はジャンリュック ダンジェ，日本側は本間尚文が研究代表者を務める．参画研究機関は，テレコムパリテック（代表：ジャンリュック ダンジェ），パリ第 6 大学（代表：ピロウズ バザルガン サベット），モルフォ（代表：タン ハ リ），東北大学（代表：本間 尚文），産業技術総合研究所（代表：川村 信一），電気通信大学（代表：崎山 一男），神戸大学（永田　真）である．本プロジェクトは，2010 年 12 月 1 日に開始され，2014 年 3 月 31 日まで実施された．フランス側への ANR の支援研究経費は，738,105 ユーロであった． 日本側への JST の支援研究経費は 149,500,000 円であった.