国際科学技術共同研究推進事業
（戦略的国際共同研究プログラム）

（研究領域「情報通信技術」）

研究課題名

「組込みシステムにおける暗号プロセッサの物理攻撃に対する安全性評価」

平成24年度実施報告書

代表者氏名　本間尚文
（所属・役職）（東北大学大学院情報科学研究科・准教授）

1. 研究実施内容

1－1. 研究実施の概要　公開

本研究では，日仏双方の知識と経験を相互補完的に組み合わせることで，暗号モジュールの安全性評価技術に関する包括的な研究開発を実施する．具体的には，暗号モジュールへのサイドチャネル攻撃に対する潜在的なリスクの評価を暗号モジュールの製造前に行うことを目指し，サイドチャネル情報の漏洩メカニズムの解明，安全性評価のためのサイドチャネル情報シミュレーション技術および暗号モジュールのプロトタイプに対する解析・評価用プラットフォーム技術の開発を目的とする．

平成 24 年度は，当初の研究計画に基づき①サイドチャネル情報漏洩メカニズムの解明（主担当：東北大学），②電力・電磁波解析攻撃向け評価プラットフォームの開発（主担当：産業技術総合研究所），③サイドチャネル情報解析ツールの開発と実装評価（主担当：電気通信大学），および④物理デバイスレベルのサイドチャネル情報シミュレーションモデルの開発（主担当：神戸大学）の 4 項目について研究を推進した．各項目は主担当グループを中心として関係する研究グループが連携して進めた．特に，日仏共同によるノイズモニタ機能を搭載した暗号 LSI（日仏暗号 LSI．平成 23 年度開発）および標準評価基板（SASEBO-W．平成 22 年度開発）を用いた共通の評価プラットフォームを開発することで，これまで以上に高い精度での共同開発・評価・各種フィードバックを実施した．また，当初計画を一部変更して開発してきた故障感度解析手法および意図的な電磁波注入による故障解析手法を発展させるための共同研究にも取り組んだ．

その結果，各研究項目において当初想定した成果が得られた．また一部は想定を上回る成果が得られた．各研究項目（上記①～④）の主な成果の概要を以下に示す．

① 電磁波を介したサイドチャネル情報漏洩の推定・可視化手法の開発

暗号モジュールを実装したデバイス（基板）近傍において電磁波を介して漏洩するサイドチャネル情報の効率的な推定・可視化手法を開発した．これまでに開発した日仏暗号 LSI および SASEBO-W を用いた実験を通して，提案手法による推定値と実測値がよく一致することを確認した．また，モジュール遠方からの意図的な電磁波注入による情報漏洩の可能性について，日仏双方で検証実験を実施し，その故障注入メカニズムを検証した．

② SASEBO-W 向け制御・測定ソフトウェアの改良・高機能化

前年度までに構築した IC カードインタフェースを持つ SASEBO-W において，制御・測定ソフトウェアのリファクタリングを進め，コード複雑化により困難となってきた機能拡張性を高めた．また，暗号モジュールの制御回路，ならびに，FPGA 向けの AES 暗号プロセッサの改良により，測定容易性が大幅に向上した．それらを日仏のチームで共有するとともに，Web 上でも公開した．

③ 故障感度解析の高精度化およびデバイスレベルの対策技術の開発

故障利用解析を基本とするサイドチャネル識別器のさらなる高精度化を行い，AES 暗号モジュールを用いて有効性を実証した．本研究により，(ア)クロック間衝突を考慮した，高精度に解析可能なサイドチャネル識別器が実現できた．また(イ)故障利用解析の本質的な理解が得られた．特に上記イ）については，日仏暗号 LSI を用いることで，回路レイアウトレベルまで考慮した詳細な解析により，高いレベルで達成ができた．さらに，故障感度解析の対策技術を世界に先駆けて開発・公表した．

④ 日仏暗号 LSI を用いた網羅的なサイドチャネル情報の収集および解析

日仏暗号 LSI と SASEBO-W を電力・電磁波解析攻撃向け評価プラットフォームとして初期統合し、サイ

ドチャネル情報取得の物理過程の詳細な理解につながる実験データの収集に成功した. とりわけ, オンチップ電源ノイズモニタによる暗号回路内部の電源ノイズ波形の直接観測を実現し, 暗号回路の動作に起因した電源ノイズの変動を明瞭に評価できること, およびサイドチャネル情報シミュレーションによる解析性能の向上につながること, を明らかにした.

上記の研究成果は, 15 編を越える国際会議論文および国際学術誌論文として発表・採録された. そのうち 7 編が日仏双方の研究者が共著となった論文である. 一例として, 電磁波を介した情報漏えいの効率的な推定・可視化手法を提案した日仏共著論文(Efficient mapping of EM radiation associated with information leakage for cryptographic devices)は EMC(電磁両立性)分野の最も主要な国際会議である 2012 EMC Symposium に採択された. 同論文は 100 を越える採択論文の中から最優秀論文賞 Finalist に選出されている. また, 当初計画を一部変更して実施している故障感度解析に関する日仏共著論文がサイドチャネル解析に関する主要な国際会議(Constructive Side-Channel Analysis and Secure Design)に採択された.

本研究を推進するにあたり, 日本側研究チームで定期的に研究打ち合わせを実施するとともに, フランス側研究チームとも活発な研究打ち合わせ・研究交流を実施した. それらの会議では取り扱いきれない個々の研究項目や実験の詳細については適宜 TV 会議を実施することで補った. また, 8 月に開催された 2012 SICE Conference で研究成果のデモンストレーションを実施するとともに, 9 月に「第一回暗号実装に関するワークショップ」を東北大学で主催するなど, 本研究の成果を広く公開し, 国内外の大学・企業・研究機関の研究者らと活発な研究討論・交流を行った.

2. 研究実施体制 公開

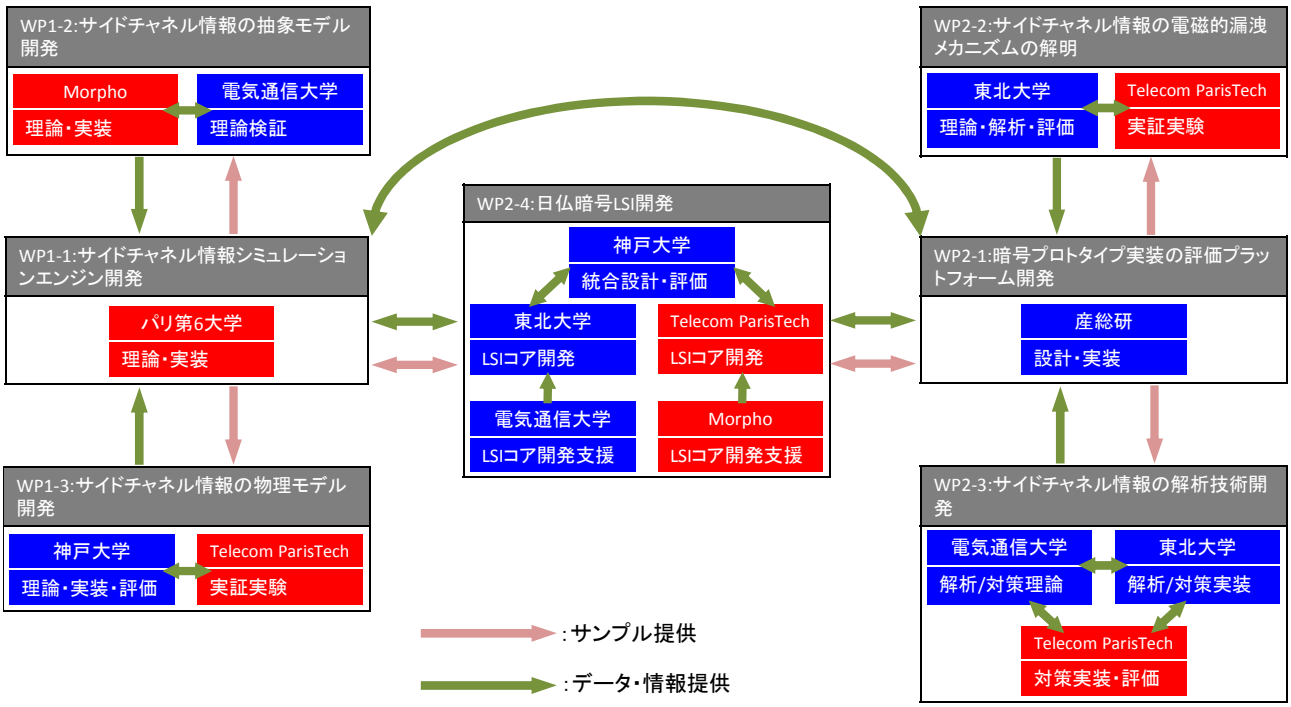
2－1. 日本側の研究実施体制

研究代表者/主な共同研究者	氏名	所属	所属部署	役職
研究代表者	本間　尚文	東北大学	大学院情報科学研究科	准教授
主な共同研究者	川村　信一	産業技術総合研究所	セキュアシステム研究部門	招聘研究員
主な共同研究者	崎山　一男	電気通信大学	大学院情報理工学研究科	准教授
主な共同研究者	永田　　真	神戸大学	システム情報学研究科	教授

2－2. 相手側の研究実施体制

研究代表者/主な共同研究者	氏名	所属	所属部署	役職
研究代表者	Jean-Luc Danger	テレコム・パリテック	通信電子学部	教授
主な共同研究者	Pirouz Bazargan-Sabet	パリ第 6 大学	コンピュータ科学研究室	教授
主な共同研究者	Thanh-Ha Le	モルフォ(株)	ハードウェアセキュリティ部	主任研究員

2－3. 両国の研究実施体制



3. 原著論文発表　公開

3－1. 原著論文発表

① 発行済論文数

	うち、相手側チームとの共著（※）
国内誌　0 件	（　0 件）
国際誌　11 件	（　4 件）
計　11 件	（　4 件）

※本共同研究の相手側チーム研究者との共著に限る

1. Yuichi Hayashi, Naofumi Homma, Takaaki Mizuki, Takeshi Sugawara, Yoshiki Kayano, Takafumi Aoki, Shigeki Minegishi, Akashi Satoh, Hideaki Sone, and Hiroshi Inoue, "Evaluation of Information Leakage from Cryptographic Hardware via Common-Mode Current," IEICE Transactions on Electronics, Vol.E95-C, No.6, pp.1089--1097, June 2012.

＊2 Haruki Shimada, Yu-ichi Hayashi, Naofumi Homma, Takaaki Mizuki, Takafumi Aoki, Hideaki Sone, Laurent Sauvage, and Jean-Luc Danger, "Efficient mapping of EM radiation associated with information leakage for cryptographic devices," IEEE International Symposium on Electromagnetic Compatibility, pp. 794--799, August 2012. (**Best Paper Finalist**)(**日仏共著論文**)

電磁波を介した情報漏えいの効率的な推定・可視化手法を提案した日仏共著の論文. EMC(電磁両立性)分野の最も主要な国際会議である 2012 EMC Symposium に採択された. 同論文は 100 を越える採択論文の中から最優秀論文賞 Finalist に選出された.

3. Yu-ichi Hayashi, Naofumi Homma, Taishi Ikematsu, Takaaki Mizuki, Takafumi Aoki, Hideaki Sone, and Jean-Luc Danger, "An efficient method for estimating the area of information propagation through electromagnetic radiation," IEEE International Symposium on Electromagnetic Compatibility, pp. 800--805, August 2012. (**日仏共著論文**)
4. Junko Takahashi, Yu-ichi Hayashi, Naofumi Homma, Hitoshi Fuji, and Takafumi Aoki, "Feasibility of Fault Analysis Based on Intentional Electromagnetic Interference," IEEE International Symposium on Electromagnetic Compatibility, pp. 782--787, August 2012.
5. Laurent Sauvage, Sylvain Guilley, Jean-Luc Danger, Naofumi Homma and Yu-ichi Hayashi, "A Fault Model for Conducted Intentional ElectroMagnetic Interferences," IEEE International Symposium on Electromagnetic Compatibility, pp. 788--793, August 2012. (**日仏共著論文**)
6. Haruki Shimada, Yuichi Hayashi, Naofumi Homma, Takaaki Mizuki, Takafumi Aoki, and Hideaki Sone, "Using Selected-Plaintext Sets for Efficient Evaluation of EM Information Leakage from Cryptographic Devices," SICE Annual Conference 2012, pp. 64-67, August, 2012.
7. Sho Endo, Yuichi Hayashi, Naofumi Homma, Takafumi Aoki, Toshihiro Katashita, Yohei Hori, Kazuo Sakiyama, Makoto Nagata, Jean-Luc Danger, Thanh-Ha Le and Pirouz Bazargan

Sabet, "Measurement of Side-Channel Information from Cryptographic Devices on Security Evaluation Platform: Demonstration of SPACES Project," SICE Annual Conference 2012, pp.313--316, August, 2012. (**日仏共著論文**)

8. Sho Endo, Yang Li, Naofumi Homma, Kazuo Sakiyama, Kazuo Ohta and Takafumi Aoki, "An Efficient Countermeasure against Fault Sensitivity Analysis using Configurable Delay Block," 2012 Workshop on Fault Diagnosis and Tolerance in Cryptography, pp.95--102, September 2012.
9. Yongdae Kim, Naofumi Homma, Takafumi Aoki, and Heebong Choi, "Security Evaluation of Cryptographic Modules against Profiling Attacks," Proceedings of the 15th International Conference on Information Security and Cryptology, pp. 383--394, November 2012.
10. Yang Li, Kazuo Ohta, and Kazuo Sakiyama, "A New Type of Fault-Based Attack: Faulty Behavior Analysis," IEICE Trans. Fundam. Electron. Commun. Comput. Sci., Vol.A96-A, No.1, pp.177-184, 2013 (DOI: 10.1587/transfun.E96.A.177).
11. Yuichi Hayashi, Naofumi Homma, Takaaki Mizuki, Takafumi Aoki, and Hideaki Sone, "Transient IEMI Threats for Cryptographic Devices," IEEE Transactions on Electromagnetic Compatibility, Vol. 55, No. 1, pp. 140--148, February 2013.

② 未発行論文数

	うち、相手側チームとの共著（※）
国内誌　1 件	（　0 件）
国際誌　5 件	（　3 件）
計　6 件	（　3 件）

※本共同研究の相手国チーム研究者との共著に限る

12. Yang Li, Sho Endo, Nicolas Debande, Naofumi Homma, Takafumi Aoki, Thanh-Ha Le, Jean-Luc Danger, Kazuo Ohta, Kazuo Sakiyama, "Exploring the Relations Between Fault Sensitivity and Power Consumption," In Proc. Constructive Side-Channel Analysis and Secure Design (COSADE'13), LNCS, Springer-Verlag, March 2013. (in press) (**日仏共著論文**)
13. Takafumi Hibiki, Naofumi Homma, Takafumi Aoki, Yuto Nakano, Kazuhide Fukushima, Shinsaku Kiyomoto and Yutaka Miyake, "Chosen-IV Correlation Power Analysis on KCipher-2 and a Countermeasure," International Workshop on Constructive Side-Channel Analysis and Secure Design (COSADE '13), LNCS, Springer-Verlag, March 2013. (in press)
14. Yang Li, Kazuo Ohta, and Kazuo Sakiyama, "An Extension of Fault Sensitivity Analysis Based on Clockwise Collision," In Proc. International Conferences on Information Security and Cryptology 2012 (Inscript'12), LNCS 7763, Springer-Verlag, 2012. (in press)
15. 嶋田晴貴, 林優一, 本間尚文, 水木敬明, 青木孝文, 曽根秀昭, "選択したデータセットを用いた暗号デバイスの電磁情報漏えいの効率的な安全性評価," 電子情報通信学会論文誌 B, April 2013 (in press).

16. Yuichi Hayashi, Naofumi Homma, Takaaki Mizuki, Haruki Shimada, Takafumi Aoki, Hideaki Sone, Laurent Sauvage, and Jean-Luc Danger, "Efficient Evaluation of EM Radiation Associated with Information Leakage from Cryptographic Devices," IEEE Transactions on Electromagnetic Compatibility, (DOI: 10.1109/TEMC.2012.2222890) (in press) (**日仏共著論文**)
17. Yuichi Hayashi, Naofumi Homma, Takaaki Mizuki, Takafumi Aoki, Hideaki Sone, Laurent Sauvage, and Jean-Luc Danger, "Analysis of Electromagnetic Information Leakage from Cryptographic Devices with Different Physical Structures," IEEE Transactions on Electromagnetic Compatibility, (DOI: 10.1109/TEMC.2012.2227486) (in press) (**日仏共著論文**)