平成 22 年度　実績報告

# 「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22年度実施報告書

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

## 1. 研究実施の概要

本研究プロジェクトでは，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を実施する．具体的には，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，安全性評価のためのサイドチャネル情報のシミュレーション技術および暗号モジュールの標準評価プラットフォームの開発を目的とする．

初年度となる平成22年度は，主に日仏の連携方法を確認・整備するとともに， 全体研究計画書に記載する①サイドチャネル情報漏洩メカニズムの解明，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，③サイドチャネル情報解析ツールの開発と実装評価，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の 4 項目について理論的検討および実験環境の立ち上げを行った．各項目は主担当グループを中心に関係するグループと連携して進めた．また，フランス側研究者との合同打ち合わせを実施するとともに，研究上の必要に応じて適宜国内外の学会において研究発表や資料収集を行った．各項目で当初計画通りの研究成果が得られ，一部では計画を上回る成果が得られた．具体的には，初年度のマイルストーンとしていた標準評価プラットフォーム（SASEBO-W）を開発し， 暗号モジュールの IC カード実装および FPGA 実装に対応した実験・評価環境を構築した．また，新たなサイドチャネル解析技術として故障感度解析を開発するとともに，サイドチャネル情報漏洩メカニズムの解明に向けて電磁波漏洩の計測システムを構築した．さらに，仏国グループとの共著論文等により，それらの成果の一部を主要な国際会議において公表した．これは初年度の計画を上回る成果である．今後は，本年度の成果をさらに発展させるとともに，日仏の共同研究グループ間での連携をさらに深めていく予定である．

## 2. 研究実施体制

| グループ名 | 研究代表者又は 主たる共同研究者氏名 | 所属機関・部署・役職名 | 研究題目 |
|---|---|---|---|
| 東北大グループ | 本間　尚文 | 東北大学・大学院情報科学研究科・准教授 | サイドチャネル情報漏洩メカニズムの解明 |
| 産総研グループ | 佐藤　証 | 産業技術総合研究所・情報セキュリティ研究センター・チーム長 | 電力・電磁波解析攻撃向け評価プラットフォームの開発 |
| 電通大グループ | 﨑山　一男 | 電気通信大学大学院・情報理工学研究科総合情報学専攻・准教授 | サイドチャネル情報解析ツールの開発と実装評価 |
| 神戸大グループ | 永田　真 | 神戸大学大学院・システム情報学研究科・教授 | 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 |

## 3. 研究実施内容

東北大グループ

研究項目：「サイドチャネル情報漏洩メカニズムの解明」

本研究項目では，暗号モジュール近傍および遠方におけるサイドチャネル情報の漏洩現象を電磁環境両立性（EMC）の観点から解明することを目的とする．暗号モジュール近傍および遠方における電磁界を計測し，その可視化を行うとともに，電磁波解析（EMA）実験により計測された磁場と情報漏洩との関係を評価する．また，それに関連する解析・対策技術を開発する．

平成22年度は，暗号モジュールから漏洩・放射する電磁波を計測するための実験システムを開発した．特に，産総研グループと協力し，実証評価ボードおよびサイドチャネル情報取得用にチューニングした磁界プローブを開発し，開発した磁界プローブを用いたモジュール近傍での電磁波計測システムを構築した（図1）．また，RF カレントプローブを利用した暗号モジュール遠方での電磁波計測のための実験環境を整備した（図 2）．

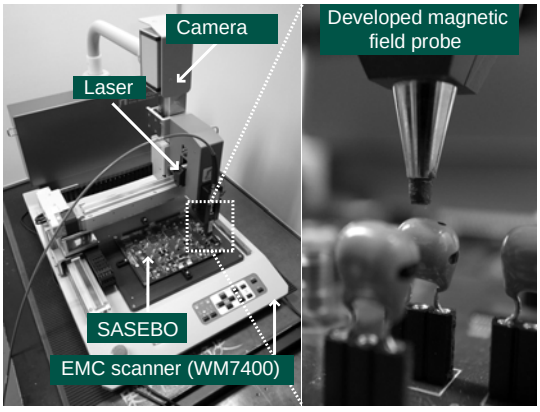


図 1：モジュール近傍の電磁波計測システムの概観

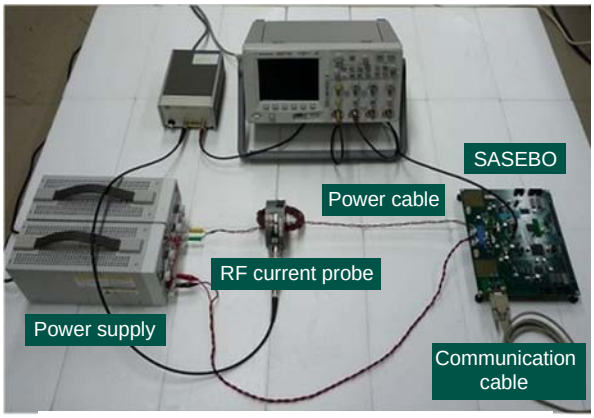


図 2：モジュール遠方の電磁波計測システムの概観

また，モジュール近傍および遠方での電磁波の漏洩・放射モデルを構築するため，予備的な電磁波解析（EMA）実験を実施した．まず，モジュール近傍での EMA では，モジュール表面数十マイクロメートルにおいて電磁波計測を行うことで，内部電流の向きと回路ブロックの配置に関する情報が得られ，結果としてより高度なサイドチャネル攻撃が可能であることを実証した[3]．モジュールを搭載した基板の近傍では，仏側の研究パートナーである Telecom ParisTech との共同研究の効果により，変調技術を利用することで公開鍵暗号モジュールに対するより高精度な EMA が可能となることを明らかにした[10]．これは当初の計画を上回る成果である．一方，モジュール遠方での EMA では，モジュール基板に接続されたケーブルなどを通してモジュールから離れた箇所にもサイドチャネル情報が伝搬することを実証した[4]． なお，上記の研究内容は，IEEE の EMC Society において電磁情報漏洩（EM Information Leakage）という新たな研究領域として認識され，新たな小技術委員会（委員長は本研究参画者）が発足するに至った．

上記の実験に関連して，EMA を高精度化するための技術の開発も行った．まず，公開鍵暗号モジュールに対する単純電磁波解析(SEMA)の精度を向上させる平文選択手法を開発した[1]．これは，特定の平文ペアを入力することにより，標準的なべき乗剰余演算（公開鍵暗号の主要な演算）アルゴリズム全てに対応可能となる．また，重回帰分析による計測波形の事前処理および周波数領域上での解析により，少ない波形数で安全性評価が可能となることを確認した[6]．その際，関連する対策・評価手法を検討した．[5,9]

今後は，当初の計画通り，上記で開発した電磁波計測システムを用いた EMA 実験を推進し，情報漏洩メカニズムの理解を深めるとともに，その可視化を行う．また，仏側パートナーと連携し，今年度得られた公開鍵暗号モジュールに対する EMA を発展させる．

産総研グループ

研究項目：「電力・電磁波解析攻撃向け評価プラットフォームの開発」

評価プラットフォームの開発として，(A) FPGA および IC カードによる電磁波解析実験を可能とする評価ボード SASEBO-W の設計と試作を主に実施した．また，(B) 専用暗号 LSI 開発に向けて電気通信大学とハッシュ関数 SHA-3 候補 14 アルゴリズムの設計・性能評価を行い，(C) 神戸大学とは AES 暗号回路の電力シミュレーションを実施した．

A. 評価プラットフォームの開発：

暗号回路を実装する FPGA に最新デバイス Spartan-6 LX150 を実装し，回路容量を従来の評価ボード SASEBO-GII の 3～5 倍とした評価ボード SASEBO-W の試作を行った．また IC カード用ソケットを付加し，FPGA から電圧制御可能な電源と入出力信号，電力・電磁波測定用のポイントを備えることで，既存の IC カードリーダでは困難なナノ秒オーダーでの波形解析実験が可能とした．さらに，解析対象として Atmel ATMega 163 プロセッサ搭載の IC カードに，カード OS と暗号ソフトウェアを実装し，SASEBO-W をカードリーダとして機能させるための回路，ドライバ，ソフトウェアの開発も行った．これらを統合し，図 1 に示す評価プラットフォームを構築した[24].

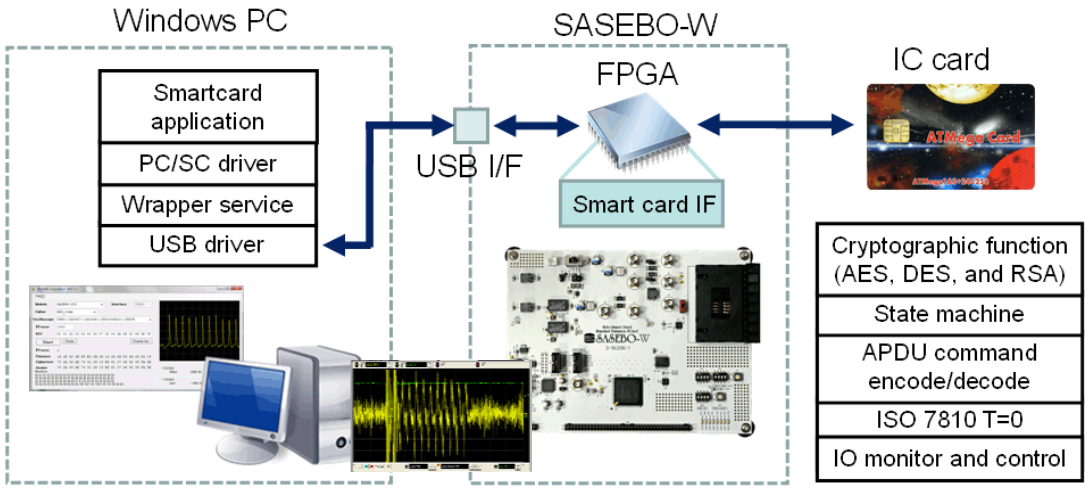


図 1. SASEBO-W と IC カードを利用した評価プラットフォームの構成

B. 解析対象物の開発：

標準化作業が進んでいる次世代ハッシュ関数 SHA-3 の 14 の候補アルゴリズムの回路の設計と，FPGA および ASIC 実装評価を行った．特に，日本から提案された Lufffa については，小型～高速までアプリケーションに応じて柔軟な実装を行うことのできる各種回路アーキテクチャを開発した[2,22,23].

C. 解析環境・モデルの評価：

65 nm CMOS スタンダードセルライブラリの LSI から取得した AES 回路の電力波形と，そのレイアウトデータを用いて神戸大開発のシミュレーションモデルから得られた電力波形の双方に対して CPA 攻撃評価を行った結果，両者に高い類似性が見られ，シミュレーションによる評価システムの構築が大きく前進した．

電通大グループ

研究項目：「サイドチャネル情報解析ツールの開発と実装評価」

平成 22 年度の電通大グループの研究目的は，以下の二項目に関するものである．

1）新たなサイドチャネル情報解析手順の発掘

2）評価プラットフォームにおけるサイドチャネル情報解析ツールのインタフェース策定

1）については， SASEBO に搭載されている秘密鍵暗号アルゴリズム AES に対して，故障感度解析（FSA：Fault Sensitivity Analysis）と呼ばれる新たなサイドチャネル識別器を提案した[7,14]． FSA とは，暗号デバイスの故障感度を解析し，暗号デバイスに格納されている秘密情報（鍵）を取得するサイドチャネル解析手法である．

図1はFSAの概念図である．暗号デバイスは通常の環境下において正しい出力Cを出力するが，暗号デバイスの動作環境を徐々に悪化させると，ある動作環境条件を境界とし誤った出力 C’を出力するようになる．この動作環境の限界条件を故障感度と呼ぶ．この故障感度は暗号回路内部で処理されるデータおよび演算に依存す

るため，攻撃者は暗号デバイスの内部情報を得ることができ，結果として秘密鍵の導出が可能であることを新たに解明した．

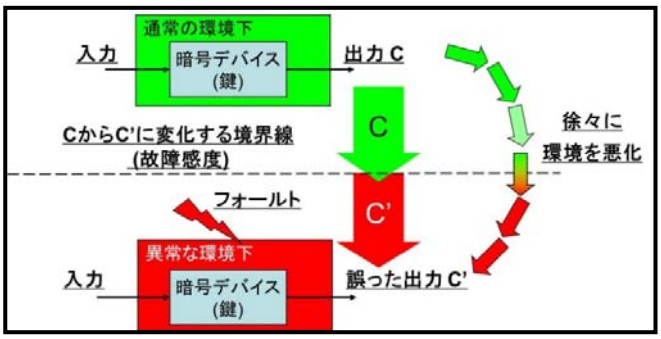


図1　故障感度解析の概念図

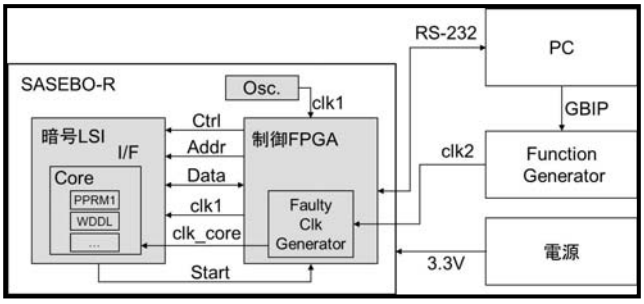


図2　実験環境およびインタフェース仕様

2）FSA の実証実験を行うために，2)について取り組んだ．図2は FSA の実験環境を示し，図中の矢印は各種インタフェースにおける必要な制御信号およびデータの流れを示す．GPIB および RS-232C を経由して，プラットフォームおよび制御機器は全て PC 上の MATLAB ソフトウェアから制御できるよう仕様策定し[8]，効率よく FSA の実験ができる環境を構築した．

今回の FSA 実験では，暗号デバイスに供給するクロック信号を用いて，暗号 LSI の動作環境を悪化させる方法を採用した．具体的には，Function Generator から供給されるクロック信号（clk2）を，制御 FPGA に実装された異常クロック生成モジュール（Faulty Clock Generator）により，グリッチノイズを有する異常クロック(clk_core)に変換し，暗号 LSI のコア部分に供給する．clk_core のグリッチ幅は，ここで，clk2 の周期に比例するように設計しているため，clk2 の周波数を上げていくことで暗号 LSI の動作環境は悪化していく．暗号LSIに供給されるもう一つのクロック信号 clk1 は，24MHz の正常なクロック信号であり，暗号 LSI内のインタフェース部の動作を保証する．

1）で考案した FSA は clk2 の周波数とそのときの暗号 LSI からの出力を観測することで実現可能となる．これを実現する制御および FSA 処理プログラムを MATLAB ソフトウェアで開発し，図 2 に示す実験環境に組み込んだ．その結果，PPRM1 型や WDDL 型といった AES 暗号 LSI に対して秘密鍵を取得することができた．

本研究成果において特筆すべきは，WDDL 型 AES の解析に成功した点である．従来，WDDL 型の AES は電力，電磁波および故障を利用した解析が難しいとされていたが，今回我々が提案した故障感度解析 FSA を用いる事で解析可能であることが実証された．しかしながら，従来の電力解析と比べ FSA が定量的にどの程度効率が良いかについてはまだ解明できていない．今後は FSA を用いた安全性解析を，公開鍵暗号アルゴリズムに適用し，電力解析との効率比較という点を重視し，AES 暗号の解析ツールのさらなる拡充と RSA および ECC ハードウェアの安全性解析を進めていく[26]．さらに FSA と電磁波解析を組み合わせ，より高い精度で暗号実装解析が行えるよう，各種ツール群の整備と併せて取り組んでいく．また暗号理論的観点から本研究の位置づけを明確にすることも検討していく[28]．

神戸大グループ

研究項目：「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」

本研究では，セキュリティモジュールにおけるサイドチャネル攻撃の解析手法の確立に向けて，物理デバイスレベルの低抽象度なサイドチャネル情報シミュレーションモデルを開発する．また，セキュリティモジュールを搭載

した LSI チップを実対象として解析性能を評価し，サイドチャネル攻撃の標準評価プラットフォームへの統合に向けた基礎的な取り組みを行う．

平成 22 年度は，CMOS デジタル技術により実装したセキュリティモジュールを対象として，セキュリティ処理の実行時における動的な電源電流に着目したサイドチャネル情報のシミュレーション手法の開発を進めた．具体的には，代表的なセキュリティモジュールである Advanced Encryption Standard (AES)暗号モジュールを対象として，65 nm CMOS デバイス技術によるトランジスタレベルの物理実装を行い(図 1)，またこの設計データを用いて AES 暗号処理の実行時における動的な電源電流波形についてシミュレーションデータを取得した(図 2)．

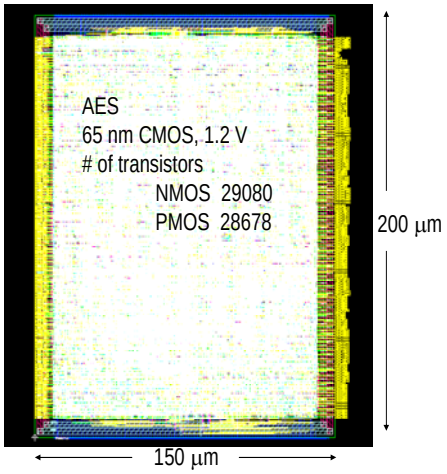


図 1: AES 暗号コアの CMOS 実装

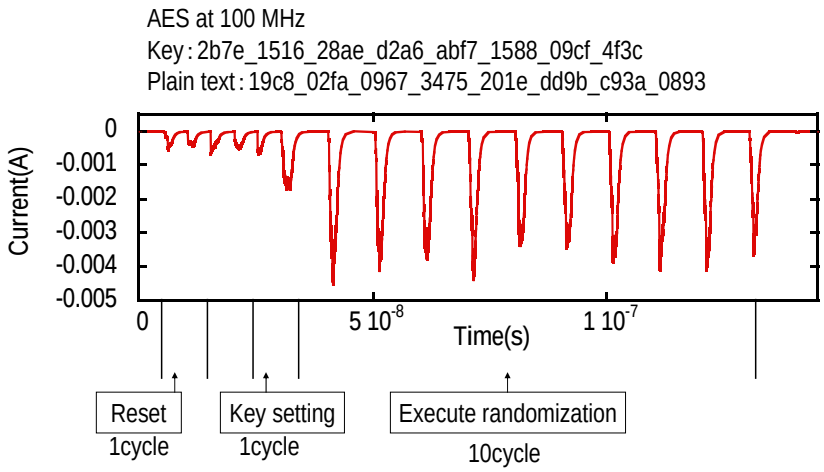


図 2: AES 暗号コアの暗号処理における電源電流シミュレーション波形

ここで，独自の容量充電モデルによる電源電流モデル化手法を適用することにより，AES 暗号処理時の電源電流シミュレーションの計算コストを大幅に削減し，平文 10,000 個以上に対する電源電流波形を実用的な時間で取得する事に成功した．AES 暗号コアは数万個のトランジスタを含むため，従来のトランジスタレベル回路シミュレーションによる電源電流解析では計算コストが大きすぎ，このように多数の平文に対する電源電流波形を取得する事は現実的でない．

さらに，代表的なサイドチャネル攻撃手法である電力相関解析(Correlation Power Analysis，CPA)に着目し，前述のシミュレーションによる電源電流波形を用いて AES 暗号モジュールに対する CPA 攻撃能力を評価できることを示した．これらのことから，容量充電モデルによる電源電流モデル化法が，セキュリティモジュールにおける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の基本原理として有効であることを確認した．

また，産総研グループによる AES 暗号モジュールの電源電流波形の実測データと，神戸大グループによる前述のシミュレーションデータを用いて，それぞれのサイドチャネル情報による CPA 攻撃能力を比較した．AES 暗号処理の最終ラウンドで AES 秘密鍵をバイト単位で特定する CPA 攻撃過程において，電源電流波形と鍵候補値との相関性が電源電流波形数に対して増加する傾向が観測され，また実測とシミュレーションで定量的に一致することを確認した．

今後は，本サイドチャネル情報の漏洩プロセスについて物理デバイスレベルの理解を深め，シミュレーションモデルの精度を引き上げるとともに，標準評価プラットフォームへの統合に向けた取り組みを進める．

## 4. 原著論文発表

① 国際誌

[1] Naofumi Homma, Atsushi Miyamoto, Takafumi Aoki, Akashi Satoh, and Adi Shamir, “Comparative Power Analysis of Modular Exponentiation Algorithms,” IEEE Transactions on Computers, Vol. 59, No. 6, pp. 795—807, June 2010.

[2] Akashi Satoh, Toshihiro Katashita, Takeshi Sugawara, Takafumi Aoki and Naofumi Homma, “Hardware Implementations of Hash Function Luffa,” IEEE International Symposium on Hardware-Oriented Security and Trust, pp. 102--106, June 2010.

[3] Masahiro Yamaguchi, Hideki Toriduka, Shoichi Kobayashi, Takeshi Sugawara, Naofumi Homma, Akashi Satoh, and Takafumi Aoki, “Development of an on-chip micro shielded-loop probe to evaluate performance of magnetic film to protect a cryptographic LSI from electromagnetic analysis,” IEEE International Symposium on Electromagnetic Compatibility, pp. 103--108, July 2010.

[4] Yu-ichi Hayashi, Takeshi Sugawara, Yoshiki Kayano, Naofumi Homma, Takaaki Mizuki, Akashi Satoh, Takafumi Aoki, Shigeki Minegishi, Hideaki Sone, Hiroshi Inoue, “Information Leakage from Cryptographic Hardware via Common-Mode Current,” IEEE International Symposium on Electromagnetic Compatibility, pp. 109--114, July 2010.

[5] Naofumi Homma, Yuichi Baba, Atsushi Miyamoto, and Takafumi Aoki, “Multiple-Valued Constant-Power Adder and Its Application to Cryptographic Processor,” IEICE Transactions on Information and Systems, Vol.E93-D, No.8, pp.2117-2125, August 2010.

[6] Takeshi Sugawara, Naofumi Homma, Takafumi Aoki, and Akashi Satoh, “Profiling attack using multivariate regression analysis,” IEICE Electronics Express, Vol. 7, No. 15, pp. 1139--1144, August 2010.

*[7] Yang Li, Kazuo Sakiyama, Shigeto Gomisawa, Toshinori Fukunaga, Junko Takahashi, and Kazuo Ohta, ″Fault Sensitive Analysis,″ In Proc. Cryptographic Hardware and Embedded Systems (CHES ’10), LNCS 6225, Springer-Verlag, pp. 320-334, August 2010.

故障感度解析(FSA : Fault Sensitivity Analysis)と呼ばれる新たなサイドチャネル解析技術を提案した. 採択されたのは暗号実装における主要な国際会議論文誌である.

[8] Daisuke Nakatsu, Yang Li, Kazuo Sakiyama, and Kazuo Ohta, ″Combination of SW Countermeasure and CPU Modification on FPGA against Power Analysis,″ In Proc. The 11th International Workshop on Information Security Applications (WISA2010), LNCS 6513, Springer-Verlag, pp. 258—272, August 2010.

[9] Sho Endo, Naofumi Homma, Takeshi Sugawara, Takafumi Aoki, and Akashi Satoh, “An On-Chip Glitchy-Clock Generator and its Application to Safe-Error Attack,” International Workshop on Constructive Side-Channel Analysis and Secure Design (COSADE 2011), pp. 175—182, February 2011.

[10] Olivier Meynard, Denis Real, Sylvain Guilley, Jean-Luc Danger, and Naofumi Homma, “Enhancement of Simple Electro-Magnetic Attacks by Pre-characterization in Frequency Domain and Demodulation Techniques,” Design, Automation, and Test in Europe (DATE2011), pp. 1004—1009, March 2011.(仏国グループとの共著論文)

[11] Miroslav Knez(evic’, Kazuyuki Kobayashi, Jun Ikegami, Shin’ichiro Matsuo, Akashi Satoh, U″nal Kocabas,, Junfeng Fan, Toshihiro Katashita, Takeshi Sugawara, Kazuo Sakiyama, Ingrid Verbauwhede, Kazuo Ohta, Naofumi Homma, and Takafumi Aoki, “Fair and Consistent Hardware Evaluation of Fourteen Round Two

SHA-3 Candidates," to appear in IEEE Transactions on VLSI, 13 pages, 2011.

② 国内誌

[12] 馬場祐一, 宮本篤志, 本間尚文, 青木孝文, 佐藤証, "RSA 暗号プロセッサ自動生成システムの設計と評価," 情報処理学会論文誌, Vol. 51, No. 9, pp. 1847−1858, September 2010.(情報科学技術フォーラム推薦論文)

## 5. 主催したワークショップ等

| 年月日 | 名称 | 場所 | 参加人数 | 概要 |
|---|---|---|---|---|
| 2010 年 5 月 18 日 | 日本側グループ<br>第 1 回ミーティング | 東京 | 4 | 日本側の研究代表者と主たる共同研究者による打ち合わせ |
| 2010 年 9 月 24 日 | 日仏合同<br>第 1 回ミーティング | パリ | 17 | 日仏全ての参画研究者による打ち合わせ |
| 2010 年 12 月 7 日 | 研究代表者<br>第 1 回ミーティング | TV 電話 | 4 | 日仏の研究代表者による打ち合わせ |
| 2010 年 12 月 29 日 | 日本側グループ<br>第 2 回ミーティング | TV 電話 | 4 | 日本側の研究代表者と主たる共同研究者による打ち合わせ |
| 2011 年 2 月 22 日 | 研究代表者<br>第 2 回ミーティング | パリ | 6 | 日仏の研究代表者による打ち合わせ |
| 2011 年 3 月 7-8 日 | 日本側グループ<br>第 3 回ミーティング | 仙台 | 5 | 日本側の研究代表者と主たる共同研究者による打ち合わせ |

その他, 連携する研究者間での小規模なミーティング(TV 電話)を複数回実施した.

以上