東北大学 電気通信研究所

研究室外部評価資料

(2016 年度-2018 年度)

Activity Report of Research Laboratory for External Review

June 2016 - March 2019
(FY.2016-2018)

Research Institute of Electrical Communication

Tohoku University

環境調和型セキュア情報システム研究室

Environmentally Conscious Secure Information System

A. 研究室名 / Research Laboratory

環境調和型セキュア情報システム研究室
Environmentally Conscious Secure Information System

B. 構成員 / Faculty and Research Staff (as of May 1, 2019)

※ 欄を適宜追加削除等調整して下さい．期間内に異動等があった場合には，在籍期間を記載して下さい．

教授 / Professor	
氏名 Name	本間 尚文 Naofumi Homma (June 2016 -)
分野名 Research Field	環境調和型セキュア情報システム研究分野 Environmentally Conscious Secure Information System
准教授 / Associate Professor	
氏名 Name	
分野名 Research Field	
助教 / Assistant Professor	
氏名 / Name	上野 嶺 Rei Ueno (April 2018 -)
他 / Others	

C. 研究目的 / Research Purpose

本研究室では，暗号技術を中心とした次世代の情報セキュリティ技術に関する研究に取り組んでいる．特に，Internet of Things (IoT) や Cyber Physical System (CPS) といった新しいネットワークの形態において安心・安全の基盤となるハードウェアセキュリティ技術を軸に，サイバー・フィジカルセキュリティ技術を縦断的に探求している．

Our research group is pursuing research and development on novel and emerging information security technologies based on cryptography. We are specifically studying cyber-physical security technologies, centering on the hardware security technology that serves as the foundation for next-generation information networks such as the internet of things (IoT) and the cyber-physical system (CPS).

D. 主な研究テーマ / Research Topics

1. サイバー・フィジカルシステムのセキュリティ設計・評価・検証の研究
2. IoT セキュリティのためのコンピューティング理論の研究
3. 組込み AI システムに対する攻撃とその防御
4. 電磁情報セキュリティの理論と応用の研究
5. 環境に調和した情報処理技術の研究
6. 次世代デバイスのセキュリティ技術の研究

1. Hardware algorithms for high-performance and lightweight cryptography
2. Secure implementation of embedded systems (attack and defense)
3. Security design and evaluation technology of cyber physical systems
4. Security-oriented information processing (signal and statistical processing)
5. Theory of EM information security and its application
6. Creation of security functions using next-generation devices

E. 学術論文等の編数 / The Number of Research Papers							
	2013	2014	2015	2016	2017	2018	Total
(1) 査読付学術論文 Refereed journal papers	-	-	-	4	5	5	14
(2) 原著論文と同等に扱う 査読付国際会議発表論文 Full papers in refereed conference proceedings equivalent to journal papers	-	-	-	2	2	1	5
(3) 査読付国際会議 Papers in refereed conference proceedings	-	-	-	5	5	6	16
(4) 査読なし国際会議・シンポジウム等 Papers in conference proceedings	-	-	-	0	0	0	0
(5) 総説・解説 Review articles	-	-	-	0	0	1	1
(6) 査読付国内会議 Refereed proceedings in domestic conferences	-	-	-	0	0	0	0
(7) 査読なし国内研究会・講演会 Proceedings in domestic conferences	-	-	-	10	13	19	42
(8) 著書 Books	-	-	-	1	2	1	4
(9) 特許 Patents	-	-	-	2	3	2	7
(10) 招待講演 Invited Talks	-	-	-	4	2	7	13

F. 特筆すべき研究成果 / Significant Research Achievements (FY.2013-2018)

See Ref. 1. "#" mark indicates research carried out at a former organization.

2013-2018 年度の研究成果（論文・特許など）のうち，前半（2013-2015 年度）と後半（2016-2018 年度）それぞれで代表的な数件（2-3 件程度ずつ）について，参考資料を引用して，その特徴と学術的意義などを簡単に紹介する．英文のみ，もしくは和文と英文で記載．
要約は 300 字程度．論文誌の要約/Abstract のコピー可．学術面での国際的インパクトならびに社会的影響を 100 字程度で記載．
必ずしも当該期間内に発表・出版したものに限るのではなく，例えば過去に発表したものでもこの期間内に成果が得られたり，評価されるようになったりしたものも含むものとする．
インパクトファクターや被引用件数など，できる限り第三者が定量的に評価できる指標を用いてアピールすること．それらの指標にはそぐわない場合には，その事情とそれに変わる適当な評価指標・尺度を示すこと．

[2013-2015]

該当なし/None

[2016-2018]

1. **Rei Ueno, Naofumi Homma, Yukihiro Sugawara, and Takafumi Aoki, "Formal Approach for Verifying Galois Field Arithmetic Circuits of Higher Degrees," IEEE Transactions on Computers, Vol. 66, No. 3, pp. 431—442, DOI: 10.1109/TC.2016.2603979, March 2017.**

Abstract: This paper presents an efficient approach to verifying higher-degree Galois-field (GF) arithmetic circuits. The proposed method describes GF arithmetic circuits using a mathematical graph-based representation and verifies them by a combination of algebraic transformations and a new verification method based on natural deduction for first-order predicate logic with equal sign. The natural deduction method can verify one type of higher-degree GF arithmetic circuit efficiently while the existing methods require an enormous amount of time, if they can verify them at all. In this paper, we first apply the proposed method to the design and verification of various Reed-Solomon (RS) code decoders. We confirm that the proposed method can verify RS decoders with higher-degree functions while the existing method needs a lot of time or fail. In particular, we show that the proposed method can be applied to practical decoders with 8-bit symbols, which are performed with up to 2,040-bit operands. We then demonstrate the design and verification of the Advanced Encryption Standard (AES) encryption and decryption processors. As a result, the proposed method successfully verifies the AES decryption datapath while an existing method fails.

International impact on both academic and social aspects: This work is published in one of the most prestigious journals in the field of computer design research named IEEE Transactions on Computers (TC). IEEE TC is ranked second in the circuit hardware design category of Google Scholar (h5-index: 61). This work achieved the world's first formal verification of AES encryption/decryption processors, and led to the development and release of Galois-Field Arithmetic Module Generator that can perform the automatic generation/verification of practical Galois-Field multipliers used in many modern cryptographic processors.

2. **Naofumi Homma, Yu-ichi Hayashi, Noriyuki Miura, Daisuke Fujimoto, Makoto Nagata, and Takafumi Aoki, "Design Methodology and Validity Verification for a Reactive Countermeasure against EM Attacks," Journal of Cryptology, Vol. 30, Issue 2, pp. 373-391, April 2017.**

Abstract: This paper presents a standard-cell-based semi-automatic design methodology for a new conceptual countermeasure against electromagnetic (EM) analysis and fault-injection attacks. The countermeasure, called the EM attack sensor, utilizes LC oscillators that react to variations in the EM field around a cryptographic LSI caused by a microprobe brought near the LSI. A dual-coil sensor architecture with digital calibration based on lookup table programming can prevent various microprobe-based EM attacks that cannot be thwarted by conventional

countermeasures. All components of the sensor core are semi-automatically designed by standard electronic design automation tools with a fully digital standard cell library and hence minimum design cost. This sensor can therefore be scaled together with the cryptographic LSI to be protected. The sensor prototype is designed based on the proposed methodology together with a 128-bit-key composite AES processor in 0.18-μm CMOS with overheads of only 2 % in area, 9 % in power, and 0.2 % in performance, respectively. The countermeasure has been validated against a variety of EM attack scenarios. In particular, some further experimental results are shown for a detailed discussion.

International impact on both academic and social aspects: This work is an extended version of a flagship international conference paper presented at 2014 IACR Conference on Cryptographic Hardware and Embedded Systems (CHES 2014). CHES is ranked as one of the best conferences in the field of hardware security research, and only the conference ranked in the both security and circuit design categories of Google Scholar. The acceptance rate and h5-index are ~25% and 36. In addition, the conference paper received the Best Paper Award. While the conventional countermeasures usually require a large overhead in terms of power and performance, the attack sensor can achieve the equivalent (and more) tamper-resistibility with a negligible overhead.

3. Rei Ueno, Naofumi Homma, Yasuyuki Nogami, and Takafumi Aoki, "Highly Efficient GF(2^8) Inversion Circuit Based on Hybrid GF Representations," Journal of Cryptographic Engineering, DOI: 10.1007/s13389-018-0187-8, March 2018.

Abstract: This paper proposes a compact and highly efficient GF(2^8) inversion circuit design based on a combination of non-redundant and redundant Galois field (GF) (or finite field) arithmetic. The proposed design utilizes an optimal normal basis and redundant GF representations, called polynomial ring representation and redundantly represented basis, to implement GF(2^8) inversion using a tower field GF((2^4)^2). The flexibility of the redundant representations provides efficient mappings from/to the GF(2^8). This paper evaluates the efficacy of the proposed circuit by gate counts and logic synthesis with a 65-nm CMOS standard cell library in comparison with conventional circuits. Consequently, we show that the proposed circuit achieves approximately 25% higher area–time efficiency than the conventional best inversion circuit in our environment. We also demonstrate that AES S-Box with the proposed circuit achieves the best area–time efficiency.

International impact on both academic and social aspects: This work is an extended version of a flagship international conference paper presented at 2015 IACR Conference on Cryptographic Hardware and Embedded Systems (CHES 2015). As mentioned in the above Achievement 1, CHES is ranked as one of the best conferences in the field of hardware security research. The most efficient AES inversion circuit in this work led to the world's highest throughput/gate AES hardware architecture design that also presented in CHES 2016. AES is now commonly used for numerous secure communications including WiFi and SSL/TLS on the internet. If all the AES communications are performed by our AES hardware newly developed in this research, the total energy consumption for AES secure communication would be reduced at least by half.

G. 特筆すべき活動 / Significant Activities (FY.2013-2018)

See Ref. 2-9. "#" mark indicates research carried out at a former organization.

研究室外部評価参考資料の 2 以降を参照しながら，2013-2018 年度のなどの活動の中から特筆すべきものを取り出し，前半（2013-2015 年度）と後半（2016-2018 年度）に分けて簡単に紹介する．英文のみ，もしくは和文と英文で記載．

[2013-2015]

該当なし/None

[2016-2018]

- **セキュリティシステムの設計と検証に関する研究**

  Research on Security System Design and Verification:

概要/Overview

秘匿通信や認証といった情報セキュリティ機能を有する情報通信システムを，世界最高水準の性能および安全性で設計するための技術を開発した．特に，各種セキュリティ機能の基幹となる高次・多入出力ガロア体演算ハードウェアの形式的設計・検証技術に関する研究を推進し，そのプロトタイプソフトウェアを世界に先駆けて開発し，その有効性を実証した．また，ハードウェア認証の基幹技術として期待される物理複製困難関数の研究を推進し，同関数回路を世界最高効率で実装する技術を開発した．

We have conducted research and development to design high-performance/secure information communication systems with information security functions such as confidential communication and authentication. In particular, we have studied formal design and verification technologies for high-order and multi-input / output Galois field arithmetic hardware, which is a major component for various security functions, and developed its prototype software for the first time. In addition, we have promoted research on hardware authentication technology, and developed the implementation technology of physically unclonable functions system with the highest efficiency.

学術的・社会的インパクト/Academic/Social Impacts

関連する(1)-4 の論文は，本研究分野における最も主要な国際学術雑誌 IEEE Transactions on Computers（TC）に掲載された．TC は 2019 年 7 月時点で Google Scholar における h5-指標 61 で Computer Hardware Design 部門学術論文誌の第 2 位に入っている．また，関連する(2)-2 の論文は，LSI システム設計技術に関するトップカンファレンスの一つ DATE（採択率は 25%未満）に採択されている．同カンファレンスは，Google Scholar における h5-指標 41 で Computer Hardware Design 部門国際会議で第 7 位に入っている．同業績は従来困難であった高次・多入出力のガロア体演算ハードウェアの形式的設計・検証を初めて可能としただけでなく，内部乱数の"一様性"と呼ばれるセキュリティプロパティを同時に形式的に検証できることを世界で初めて示している．2018 年には，これまでの研究内容を主要業績として，第 14 回日本学術振興会賞（2018.2.7)および第 50 回市村学術賞(2018.3.14)が授与された．

また，関連する(2)-12 と(2)-14 の論文では，世界最高水準の効率性を有する物理複製困難関数の実装方法を明らかにしている．(2)-12 の論文は，回路とシステムに関する最も主要な国際論文誌である IEEE Transactions on Circuits and Systems1（h5-index: 56，Google Scholar Computer Hardware Design 部門第 4 位)に掲載されている．また(2)-14 の論文は，計算機に関する最も主要な国際論文誌 IEEE Transactions on Computers（h5-index: 61，Google Scholar Computer Hardware Design 部門 2 位)に掲載されている．また，当該業績に関連して，国際会議 2018International Workshop on Security および 2018 International Conference on Intelligent Information Hiding and Multimedia Signal Processing において，それぞれ基調講演を行った．

また，当該業績が評価された結果，当該分野の主要な国際学術誌 Journal of Cryptographic Engineering の特集号のゲストエディタを務めた．

本業績によって開発された技術を応用して，多様なガロア体乗算器の自動生成・検証を可能とする算術演算モジュールジェネレータのプロトタイプソフトウェアを開発するとともに 2019 年 3 月に Web 上で公開した（https://www.ecsis.riec.tohoku.ac.jp/topics/amg）．同ジェネレータは，従来では合成困難だった無数にあるガロア体乗算器の自動合成・検証が可能であり，すでに数百件を超える利用がある．

The related paper of (1)-4 was published in IEEE Transactions on Computers (TC), the leading international journal of this research field. At July 2019, TC has been ranked No. 2 in the Computer Hardware Design category with the h5-index 61 in Google Scholar. Also, the related paper of (2)-2 was accepted at the top conference on LSI system design technology (DATE). where the acceptance rate is less than 25%. The conference is ranked No. 7 in the Computer Hardware Design category with the h5-index 41 in Google Scholar. This research made it possible for the first time to formally design and verify Galois field arithmetic hardware of high order and multiple input while the conventional methods failed. In addition, the developed method first verified a security property, called “uniformity,” of internal gate outputs in a formal manner. In 2018, the series of this research were highly evaluated, and the 14th Japan Society for the Promotion of Science (JSPS) Prize and the 50th Ichimura Academic Award were awarded.

Also, in the related papers of (2) -12 and (2) -14, the implementation methods (i.e., fuzzy extractors) for physical unclonable functions with the world's highest level of efficiency were developed. The paper of (2)-12 was published in IEEE Transactions on Circuits and Systems1 (h5-index: 56), which is the most important international journal in the research field of circuits and systems. The paper of (2)-14 was published in IEEE Transactions on Computers (h5-index). In addition, in relation to the achievements, Prof. Homma was invited as a keynote speaker at the 2018 International Workshop on Security and the 2018 International Conference on Intelligent Information Hiding and Multimedia Signal Processing. In addition, as a result of the high reputation of the work, he also served as a guest editor for the special issue of the major international journal named Journal of Cryptographic Engineering.

With the technology developed by this work, we have developed and released an arithmetic module generator that enables automatic generation and verification of various Galois field multipliers on the Web in March 2019 (https://www.ecsis.riec.tohoku.ac.jp/topics/amg). The generator is capable of automatic synthesis and verification of numerous Galois field multipliers, and has already been used in over hundreds.

- **暗号コンピューティングに関する研究**

  Research on Cryptographic Computing

概要/Overview

現代暗号および今後の利用増大が予想される次世代暗号（高機能暗号・軽量暗号）をハードウェアやソフトウェアで高性能・高効率・低コストかつ安全に実現するための研究開発を行った．特に，現在世界で最も広く利用されている AES（Advanced Encryption Standard）の世界最高効率のハードウェア・アーキテクチャを開発した．また，軽量暗号 PRINCE の超低遅延セキュアハードウェアの設計と評価に関する国際共同研究を推進した．さらに，悪意のあるハードウェアが暗号ハードウェアに混入していた場合にそれらを完全かつ高速に検出する手法を開発した．

We have conducted research and development to realize modern and prospective encryption (e.g., high-performance encryption and light-weight encryption) in hardware and/or software that are expected to increase in the future. In

particular, we have developed the world's most efficient hardware architecture for the Advanced Encryption Standard (AES) encryption and decryption, which is the most widely used in the world. We have also promoted an international joint research on the design and evaluation of ultra-low latency secure hardware of the light-weight cipher PRINCE. Furthermore, we have studied a fast and complete detection method available for to malicious hardware built in cryptographic hardware.

学術的・社会的インパクト/Academic/Social Impacts

関連する(2)-1 の論文は，暗号技術を搭載したハードウェア・組込みシステムに関するトップカンファレンス（採択率 25%未満）であり，上述の通り一流の国際学術誌論文に匹敵するレベルにある．同論文では，現在世界で最も広く利用される AES 暗号の暗号化・復号処理の効率を 50%以上向上させる新規のハードウェア・アーキテクチャを開発したことが高く評価された．本業績は，Phy.org，Science Daily，RBB Today 等の各種メディアでも取り上げられた．また，(2)-3 の関連論文は，PRINCE と呼ばれる軽量暗号の世界最速実装を達成した国際共同研究の成果であり，回路設計有数の国際会議（VL）に採択されている（h5-index: 25）.

本研究の成果に関連して，国際会議 2018 International Symposium on VLSI -Design, Automation and Test において招待講演（(10)-5）を行ったほか，国内においても LSI とシステムのワークショップなど計 2 件の招待講演を行った（(10)-8, (10)-9）． 同技術は国内学会でもその実用性が高く評価されており，国内最大の情報セキュリティに関するシンポジウム「2017 年暗号と情報セキュリティシンポジウム」（2017 年 1 月 26 日）において関連する発表に対して論文賞の受賞した．またこうした一連の業績が評価され，CHES2017 において本間教授がプログラム委員長を務めるに至った．さらに，2018 年には，本間教授が German Innovation Award: Gottfried Wagener Prize 2018 を受賞した．同賞は，技術革新を重視するドイツ企業と在日ドイツ商工会議所により 2008 年に創設された賞である．本間教授は，デジタル化とモビリティ分野において，「軽量・耐タンパー性暗号ハードウェア設計技術」の業績により受賞した（2018.6.26）.

The related paper of (2) -1 was presented at the top conference on hardware/embedded systems equipped with cryptographic technology, which was comparable to the top international journal articles as mentioned above. It was highly evaluated that we have developed a new hardware architecture that improves the efficiency of the AES encryption/decryption, which is currently widely used in the world, by more than 50%. This achievement has been featured in various media such as Phy.org, Science Daily, RBB Today and so on. Also, the related paper of (2) -3 was given as the result of an international joint research, where we have achieved the world's fastest implementation of lightweight encryption called PRINCE. As a result, it was accepted by VLSI circuit symposium, one of the leading international conferences on circuit design (h5-index: 25).

In conjunction with the results of this research, Prof. Homma delivered an invited talk at 2018 International Symposium on VLSI-Design, Automation and Test (i.e., (10) -5) in addition to two invited talks in Japan (i.e., (10) -8, (10) -9). The developed technology has been highly evaluated for its practicality, and awarded at the Symposium on Cryptography and Information Security in 2017 (January 26, 2017), the largest information security symposium in Japan. Also, with a series of these achievements, Prof. Homma served as a program co-chair of CHES 2017. Furthermore, in 2018, he received the German Innovation Award: Gottfried Wagener Prize 2018. The award was created in 2008 by German companies and the German Chamber of Commerce in Japan. Prof. Homma was awarded for his achievements in “Lightweight and tamper-resistant cryptographic hardware design technology” in the field of digitization and mobility (2018.6.26).

- **電磁情報セキュリティに関する研究**

  Research on Electromagnetic Information Security

概要/Overview

タブレットやスマートフォン等の携帯情報通信端末から放射する電磁波による情報漏えいについて、そのメカニズム解明と安全性評価・対策技術に関する研究を行った．特に，携帯情報通信端末の画面情報が同端末から漏えいする電磁波によって遠隔で復元される電磁的盗視の問題に取り組み，ノートパソコンに接続された電源ケーブル付近から漏えいする電磁波に含まれる画面情報について実験的に明らかにし，その対策技術を考案した．また，端末等に搭載される乱数生成器の意図的な電磁放射による乱数性の消失メカニズムの解明に国際共同研究により取り組み，その実現可能性を明らかにした．

We have clarified the mechanism of information leakage via electromagnetic (EM) waves emitted from mobile information communication terminals such as tablets and smartphones, and developed on security evaluation and countermeasure technologies. In particular, we have tackled the problem of EM eavesdropping remotely restored by EM waves from mobile information communication terminals, and studied about screen information included in EM waves leaked from a power cable connected to a notebook computer. We have clarified it experimentally and devised the countermeasure technology. In addition, we worked on the mechanism of randomness loss in the random number generator by intentional EM interference through an international joint research.

学術的・社会的インパクト/Academic/Social Impacts

関連する(1)-1, (1)-10 の論文は本研究分野の最も主要な国際学術雑誌 IEEE Transactions on Electromagnetic Compatibility に掲載された（h5-指標：30）．(1)-1 の論文では，ノートパソコンに接続された電源ケーブルがアンテナとなって放射される電磁波による情報漏えい現象の発見とその効果的な対策技術を提案した．同内容に関して，NTT ネットワーク基盤技術研究所と共同研究を実施し，計 7 件の共同特許を出願した．(1)-10 の論文では，乱数生成器の乱数性を電磁波により巧みに操作可能であることを初めて示した．また，関連する(1)-6 の論文は，放射電磁波を利用した電磁波攻撃に対する世界初の反応型対策を提案するものであり，国際暗号学会の旗艦論文誌に掲載された（h5-index: 29）．同論文は，CHES と呼ばれるハードウェアセキュリティトップカンファレンスで最優秀論文賞を受賞した内容を拡張したものである．さらに，国内においても，本研究内容に関連して 2 件の招待講演（(10)-5, (10)-6）を行うとともに，電子情報通信学会に招待論文（(1)-11），映像情報メディア学会の学会誌に解説記事を掲載した（(5)-1）．また，関連する(7) -32 の発表で，多値論理フォーラム奨励賞を受賞した．

The related papers of (1)-1 and (1)-10 were published in the IEEE Transactions on Electromagnetic Compatibility in this research field (h5-index: 30). The paper of (1) -1 describes the discovery of an information leak phenomenon due to EM waves emitted by a power cable connected to a laptop computer as an antenna and its effective countermeasure technology. With the same contents, we have conducted a joint research with NTT Network Technology Laboratories and applied for seven related joint patents in total. In the paper of (1) -10, we have shown for the first time that the randomness of a random number generator can be manipulated with EM waves. In addition, the related paper of (1)-6 proposed the world's first reactive countermeasure against EM attacks using electrical coupling, and was published in the IACR flagship journal named Journal of Cryptology (h5-index: 29). This paper was an extended version of a conference paper received the Best Paper Award at the top conference called CHES. Furthermore, in Japan, we gave two invited talks ((10) -5, (10) -6) about this research, and also provided an invited paper to the IEICE journal ((1) -1), and a commentary article in the journal of the Institute of Image Information

and Television Engineers ((5) -1). Furthermore, we received the Encouragement Prize at the Multi-Valued Logic Forum ((7)-10).