東北大学 電気通信研究所

研究室外部評価 参考資料

(2016 年度-2018 年度)

Research Laboratory Reference Data 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

1. 研究成果 / Research Achievements

(1) 査読付学術論文 / Refereed journal papers

1. Yu-ichi Hayashi, Naofumi Homma, Yohei Toriumi, Kazuhiro Takaya, and Takafumi Aoki, "Remote Visualization of Screen Images Using a Pseudo-Antenna that Blends into the Mobile Environment," IEEE Transactions on Electromagnetic Compatibility, Vol. 59, Issue 1, pp. 24-33, DOI: 10.1109/TEMC.2016.2594237, August 2016.
2. Ville Yli-Mäyry, Naofumi Homma, and Takafumi Aoki, "Power Analysis on Unrolled Architecture with Points-of-Interest Search and Its Application to PRINCE Block Cipher," IEICE Transactions 100-A(1), pp. 149-157, DOI: 10.1587/transfun.E100.A.149, January 2017.
3. Makoto Nagata, Daisuke Fujimoto, Noriyuki Miura, Naofumi Homma, Yu-ichi Hayashi, and Kazuo Sakiyama, "Protecting cryptographic integrated circuits with side-channel information," IEICE Electronics Express, Vol. 14, No. 2, pp. 1-13, DOI: 10.1587/elex.14.20162005, January 2017
4. 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.
5. Shoei Nashimoto, Naofumi Homma, Yu-ichi Hayashi, Junko Takahashi, Hitoshi Fuji, and Takafumi Aoki, "Buffer overflow attack with multiple fault injection and a proven countermeasure," Journal of Cryptographic Engineering, Vol. 7, Issue 1, pp. 35-46, DOI: 10.1007/s13389-016-0136-3, April 2017.
6. Naofumi Homma, Yu-ichi Hayashi, Naoriyuki 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, DOI: 10.1007/s00145-015-9223-3, April 2017.
7. Rei Ueno, Naofumi Homma, Takafumi Aoki, and Sumio Morioka, "Hierarchical Formal Verification Combining Algebraic Transformation with PPRM Expansion and Its Application to Masked Cryptographic Processors," IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol. E100-A, No. 7, pp. 1396-1408, DOI: 10.1587/transfun.E100.A.1396, July 2017.
8. Rei Ueno, Naofumi Homma, and T. Aoki, "Automatic Generation System for Multiple-Valued Galois-Field Parallel Multipliers," IEICE Transactions on Information and Systems, Vol. E100-D, No. 8, pp. 1603-1610, DOI: 10.1587/transinf.2016LOP0010, August 2017.
9. 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. (Preprint).
10. Saki Osuka, Daisuke Fujimoto, Yu-ichi Hayashi, Naofumi Homma, Arthur Beckers, Josep Balasch, Benedikt Gierlichs, and Ingrid Verbauwhede, "EM Information Security Threats Against RO-Based TRNGs: The Frequency Injection Attack Based on IEMI and EM Information Leakage," IEEE Transactions on Electromagnetic Compatibility, DOI: 10.1109/TEMC.2018.2844027, June 2018. (Preprint)
11. Yu-Ichi Hayashi and Naofumi Homma, "Introduction to Electromagnetic Information Security," IEICE Transactions on Communications, Vol. E102-B, No. 1, pp. 40-50, DOI: 10.1587/transcom.2018EBI0001, August 2018. (Invited)
12. Manami Suzuki, Rei Ueno, Naofumi Homma, and Takafumi Aoki, "Efficient Fuzzy Extractors Based on Ternary Debiasing Method for Biased Physically Unclonable Functions," IEEE Transactions on Circuits and Systems I: Regular Papers, Vol. 66,

Issue 2, pp. 616-629, DOI: 10.1109/TCSI.2018.2869086, September 2018.

13. Akira Ito, Rei Ueno, Naofumi Homma, Takafumi Aoki, “Characterizing Parallel Multipliers for Detecting Hardware Trojans,” Journal of Applied Logics, Vol. 5, No. 9, pp. 1815-1832, DOI: None, December 2018.
14. Rei Ueno, Manami Suzuki, and Naofumi Homma, “Tackling Biased PUFs through Biased Masking: A Debiasing Method for Efficient Fuzzy Extractor,” IEEE Transactions on Computers, DOI: 10.1109/TC.2019.2897996, February 2019. (Preprint)

(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

1. Rei Ueno, Sumio Morioka, Naofumi Homma, and Takafumi Aoki, “A High Throughput/Gate AES Hardware Architecture by Compressing Encryption and Decryption Datapaths - Toward Efficient CBC-Mode Implementation,” International Conference on Cryptographic Hardware and Embedded Systems (CHES 2016), Lecture Notes in Computer Science 9813, pp. 538-558, Springer-Verlag, DOI: 10.1007/978-3-662-53140-2_26, August 2016.
2. Rei Ueno, Naofumi Homma, Sumio Morioka, and Takafumi Aoki, “Automatic Generation of Formally-Proven Tamper-Resistant Galois-Field Multipliers Based on Generalized Masking Scheme,” IEEE Design, Automation and Test in Europe Conference and Exhibition 2017 (DATE 2017), pp. 978-983, DOI: 10.23919/DATE.2017.7927133, March 2017.
3. Noriyuki Miura, Kohei Matsuda, Makoto Nagata, Shivam Bhasin, Ville Yli-Mayry, Naofumi Homma, Yves Mathieu, Tarik Graba, and Jean-Luc Danger, “A 2.5ns-Latency 0.39pJ/b 289μm2/Gb/s Ultra-Light-Weight PRINCE Cryptographic Processor,” 2017 Symposium on VLSI Circuits, Digest of Technical Papers, pp. C266-C267, DOI: 10.23919/VLSIC.2017.8008502, June 2017.
4. Daisuke Ishihata, Naofumi Homma, Yu-ichi Hayashi, Noriyuki Miura, Daisuke Fujimoto, Makoto Nagata, and Takafumi Aoki, “Enhancing Reactive Countermeasure against EM Attacks with Low Overhead,” 2017 IEEE International Symposium on Electromagnetic Compatibility, pp. 399-404, DOI: 10.1109/ISEMC.2017.8077903, June 2017.
5. Ville Yli-Mäyry, Daisuke Miyata, Naofumi Homma, Hayashi Yuichi, and Takafumi Aoki, “On the Evaluation of Electromagnetic Information Leakage from Mobile Device Screens,” Joint IEEE EMC & APEMC, pp. 1050-1052, DOI: 10.1109/ISEMC.2018.8393945, May 2018.

(3) 査読付国際会議 / Papers in refereed conference proceedings

1. Wataru Kawai, Rei Ueno, Naofumi Homma, Takafumi Aoki, Kazuhide Fukushima, and Shinsaku Kiyomoto, “Side channel Security Evaluation for KCipher-2 Software on Smart Cards,” 25th International Workshop on Post-Binary ULSI Systems, pp. 9-12, DOI: None, May 2016.
2. Ville Yli-Maeyry, Naofumi Homma, and Takafumi Aoki, “Power Analysis on Unrolled PRINCE Processor and its Countermeasure,” 25th International Workshop on Post-Binary ULSI Systems, pp. 22-25, DOI: None, May 2016.
3. Daisuke Ishihata, Naofumi Homma, Yu-ichi Hayashi, Noriyuki Miura, Daisuke Fujimoto, Makoto Nagata, and Takafumi Aoki, “Enhancement of Reactive Countermeasure against Side-Channel Attacks with Microprobing,” 25th International Workshop on Post-Binary ULSI Systems, pp. 28-32, DOI: None, May2016.
4. Rei Ueno, Yukihiro Sugawara, Naofumi Homma, and Takafumi Aoki, “Formal Design of Pipelined GF Arithmetic Circuits and Its Application to Cryptographic Processors,”

2016 IEEE 46th International Symposium on Multiple-Valued Logic (ISMVL), pp. 217-222, DOI: 10.1109/ISMVL.2016.25, 2016.

5. Ville Yli-Mäyry, Naofumi Homma, and Takafumi Aoki, "Chosen-Input Side-Channel Analysis on Unrolled Light-Weight Cryptographic Hardware," The 18th International Symposium on Quality Electronic Design, pp. 301-306, DOI: 10.1109/ISQED.2017.7918332, March 2017.
6. Rei Ueno, Naofumi Homma, and Takafumi Aoki, "Toward More Efficient Tamper-Resistant AES Hardware Architecture Based on Threshold Implementation," International Workshop on Constructive Side-Channel Analysis and Secure Design (COSADE 2017), pp. 50-64, DOI: 10.1007/978-3-319-64647-3_4, April 2017.
7. Manami Suzuki, Rei Ueno, Naofumi Homma, and Takafumi Aoki, "Multiple-Valued Debiasing for Physically Unclonable Functions and Its Application to Fuzzy Extractors," International Workshop on Constructive Side-Channel Analysis and Secure Design (COSADE 2017), pp. 248-263, DOI: 10.1007/978-3-319-64647-3_15, April 2017.
8. Wataru Kawai, Rei Ueno, Naofumi Homma, Takafumi Aoki, Kazuhide Fukushima, and Shinsaku Kiyomoto, "Practical Power Analysis on KCipher-2 Software on Low-End Microcontrollers," IEEE EuroS&P Workshops on Security for Embedded and Mobile Systems (SEMS), pp. 113-121, DOI: 10.1109/EuroSPW.2017.60, April 2017.
9. Rei Ueno, Naofumi Homma, and Takafumi Aoki, "A Systematic Design of Tamper-Resistant Galois-Field Arithmetic Circuits Based on Threshold Implementation with (d+1) Input Shares," IEEE 47th International Symposium on Multiple-Valued Logic (ISMVL), pp. 136-141, May 2017.
10. Kazuhide Fukushima, Rui Xu, Shinsaku Kiyomoto, and Naofumi Homma, "Fault Injection Attack on Salsa20 and ChaCha and a Lightweight Countermeasure," 2017 IEEE International Conference on Trust, Security and Privacy in Computing and Communications, pp. 1032-1037, 10.1109/Trustcom/BigDataSE/ICESS.2017.348, August 2017.
11. Kazuhiro Oshida, Rei Ueno, Naofumi Homma, and and Takafumi Aoki, "On Masked Galois-Field Multiplication for Authenticated Encryption Resistant to Side Channel Analysis," International Workshop on Constructive Side-Channel Analysis and Secure Design (COSADE) 2018, pp. 44-60, DOI: 10.1007/978-3-319-89641-0_3, April 2018.
12. Kosuke Koiwa, Daisuke Fujimoto, Yuichi Hayashi, Makoto Nagata, Makoto Ikeda, Tsutomu Matsumoto, and Naofumi Homma, "EM Security Analysis of Compact ECDSA Hardware," Joint IEEE EMC & APEMC Reviewed Abstract, p. 12, DOI: 10.1109/ISEMC.2018.8394012, May 2018.
13. Saki Osuka, Daisuke Fujimoto, Yu-ichi Hayashi, Naofumi Homma, Arthur Beckers, Josep Balasch, Benedikt Gierlich, and Ingrid Verbauwhede, "Fundamental Study on Non-invasive Frequency Injection Attack against RO-Based TRNG," Joint IEEE EMC & APEMC Reviewed Abstract, p. 8, DOI: 10.1109/ISEMC.2018.8394008, May 2018.
14. Akira Ito, Rei Ueno, Naofumi Homma, and Takafumi Aoki, "On the Detectability of Hardware Trojans Embedded in Parallel Multipliers," IEEE 48th International Symposium on Multiple-Valued Logic, pp. 62-67, DOI: 10.1109/ISMVL.2018.00019, May 2018.
15. Manami Suzuki, Rei Ueno, Naofumi Homma, and Takafumi Aoki, "Quaternary Debiasing for Physically Unclonable Functions," IEEE 48th International Symposium on Multiple-Valued Logic, pp. 7-12, DOI: 10.1109/ISMVL.2018.00010, May 2018.
16. Akira Ito, Rei Ueno, Naofumi Homma, and Takafumi Aoki, "A Non-Reversible Insertion Method for Hardware Trojans Based on Path Delay Faults," International Workshop

on Security Proofs for Embedded Systems (PROOFS) 2018, pp. 50-67, DOI: doi.org/10.29007/fxvv, September 2018.

(4) 査読なし国際会議・シンポジウム等 / Papers in conference proceedings

特になし/None

(5) 総説・解説 / Review articles

1. 本間尚文, 林優一, “電磁情報セキュリティの最新動向～電磁的盗視とその対策～,” 映像情報メディア学会誌, Vol. 72, No. 6, pp. 862-866, November 2018.

(6) 査読付国内会議 / Refereed proceedings in domestic conferences

特になし/None

(7) 査読なし国内研究会・講演会 / Proceedings in domestic conferences

1. 忍田大和, 上野嶺, 本間尚文, 青木孝文, “認証付き暗号のための耐タンパー性ガロア体乗算に関する検討,” 第 39 回多値論理フォーラム, Vol. 39, No. 3, pp. 1-7, September 2016.
2. 鈴木麻奈美, 上野嶺, 本間尚文, 青木孝文, “物理複製困難関数の多値化とその応用に関する検討,” 第 39 回多値論理フォーラム, Vol. 39, No. 4, pp. 1-8, September 2016. **（多値論理フォーラム奨励賞受賞）**
3. 上野嶺, 本間尚文, 青木孝文, “冗長表現に基づく耐タンパー性ガロア体算術演算回路の設計に関する検討,” 第 30 回多値論理とその応用研究会, No. 8, pp. 38-43, January 2017.
4. 福島和英, 許 瑞, 清本晋作, 本間尚文, “Salsa20/ChaCha に対する故障利用攻撃とその対策,” 2017 年暗号と情報セキュリティシンポジウム (SCIS2017), Vol. 2A3-1, pp. 1-5, January 2017.
5. 忍田大和, 上野嶺, 本間尚文, 青木孝文, “認証付き暗号の耐タンパー性ガロア体乗算に対するサイドチャネル攻撃,” 2017 年暗号と情報セキュリティシンポジウム (SCIS2017), Vol. 3C1-4, pp. 1-7, January 2017.
6. ヴィッレウリマウル, 本間尚文, 青木孝文, “アンロールド軽量暗号ハードウェアに対する選択平文型高効率 サイドチャネル解析,” 2017 年暗号と情報セキュリティシンポジウム (SCIS2017), Vol. 3C1-5, pp. 1-6, January 2017.
7. 上野嶺, 本間尚文, 青木孝文, “1 階 TI に基づく耐タンパー性を有する高効率 AES 暗号ハードウェアの実装,” 2017 年暗号と情報セキュリティシンポジウム (SCIS2017), Vol. 3C1-2, pp. 1-7, January 2017. **(SCIS 論文賞受賞)**
8. 鈴木麻奈美, 上野嶺, 本間尚文, 青木孝文, “多値化 PUF に基づく効率的なファジー抽出器の設計,” 2017 年暗号と情報セキュリティシンポジウム (SCIS2017), Vol. 3C1-5, pp. 1-8, January 2017.
9. ヴィッレウリマウル, 本間尚文, 林優一, 鳥海陽平, 伊丹 豪, 鈴木康直, 中村雅之, 高谷和宏, 青木孝文, “t 検定による電磁的画面情報漏えいの安全性評価手法,” 電子情報通信学会総合大会, AS-3-11, March 2017.
10. 林優一, 本間尚文, “サイバー空間における攻撃モデルはハードウェアへの物理攻撃にも適用可能か？,” 電子情報通信学会総合大会, AS-3-9, March 2017.
11. 遠藤空, ヴィッレウリマウル, 本間尚文, 青木孝文, “数論変換に基づく秘匿計算向け暗号の高効率実装,” 平成 29 年度電気関係学会東北支部連合大会, 1F15, August 2017. **（情報処理学会東北支部奨励賞）**

12. 伊東燦, 上野嶺, 本間尚文, 青木孝文, “乗算アルゴリズムに対するハードウェアトロイ挿入可能性の評価,” 平成 29 年度電気関係学会東北支部連合大会, 1E05, August 2017.
13. 伊東燦, 上野嶺, 本間尚文, 青木孝文, “算術演算ハードウェアアルゴリズムの改変検知に関する検討,” 第 40 回多値論理フォーラム, Vol. 40, No. 16, September 2017.
14. 遠藤空, ヴィッレウリマウル, 本間尚文, 青木孝文, “剰余演算に基づく秘匿計算向け暗号の高効率実装,” 第 40 回多値論理フォーラム, Vol. 40, No. 17, September 2017.
15. 宮田大輔, ヴィッレウリマウル, 本間尚文, 林優一, 青木孝文, “スマートデバイスからの電磁的情報漏えいの評価に関する検討,” ハードウェアセキュリティフォーラム 2017, ポスターNo. 11, December 2017.
16. 伊東燦, 上野嶺, 本間尚文, 青木孝文, “ハードウェアトロイ挿入が困難な公開鍵暗号データパスに関する検討,” ハードウェアセキュリティフォーラム 2017, ポスターNo. 9, December 2017.
17. 大須賀彩希, 藤本大介, 林優一, 本間尚文, Arthur Beckers, Josep Balasch, Benedikt Gierlichs, Ingrid Verbauwhede, “サイドチャネル情報を用いた乱数生成器への非侵襲な周波数注入攻撃,” 2018 年暗号と情報セキュリティシンポジウム (SCIS 2018), No. 1D2-4, January 2018.
18. Ville Yli-Mäyry, 宮田大輔, 林優一, 本間尚文, 青木孝文, “スマートデバイスからの電磁的情報漏えいに対する安全性評価手法,” 2018 年暗号と情報セキュリティシンポジウム (SCIS 2018), No. 1D1-3, January 2018.
19. 忍田大和, 上野嶺, 本間尚文, 青木孝文, 仲野有登, 福島和英, 清本晋作, “ガロア体乗算に基づく認証タグ生成に対する代数的サイドチャネル攻撃,” 2018 年暗号と情報セキュリティシンポジウム (SCIS 2018), No. 1D1-6, January 2018.
20. 鈴木麻奈美, 上野嶺, 本間尚文, 青木孝文, “バイアスを含む PUF に対する高効率な 4 値デバイアシング,” 2018 年暗号と情報セキュリティシンポジウム (SCIS2018), No. 2D2-2, January 2018.
21. 上野嶺, 鈴木麻奈美, 本間尚文, 青木孝文, “偏位マスキングに基づくファジー抽出器の構成,” 2018 年暗号と情報セキュリティシンポジウム (SCIS 2018), No. 2D2-3, January 2018.
22. 上野嶺, 本間尚文, 森岡澄夫, 青木孝文, “乱数オーバーヘッドを抑制した耐タンパー性 AES 暗号ハードウェア,” 2018 年暗号と情報セキュリティシンポジウム (SCIS 2018), No. 3D2-4, January 2018.
23. 小岩航介, 藤本大介, 林優一, 永田真, 池田誠, 松本勉, 本間尚文, “楕円曲線署名の小規模実装に対する耐タンパー性評価,” 2018 年電子情報通信学会総会, AS-2-1, pp. s-21, March 2018.
24. 上野嶺, 本間尚文, 飯田伴則, 峯松一彦, “AES-OTR ハードウェアアーキテクチャとその評価,” ハードウェアセキュリティ研究会, pp. 17-22, April 2018.
25. 船越秀隼, 本間尚文, “耐量子計算機鍵共有方式の組込み機器向け実装に関する検討,” LSI とシステムのワークショップ 2018, ポスターNo. 52, May 2018.
26. 宮田大輔, ヴィッレウリマウル, 林優一, 本間尚文, “スマートデバイスの電磁的画面情報漏えいに対する統計的安全性評価手法,” LSI とシステムのワークショップ 2018, ポスターNo. 50, May 2018.
27. 伊東燦, 上野嶺, 本間尚文, 青木孝文, “パス遅延故障に基づくハードウェアトロイの系統的挿入法とその評価,” 夏のセキュリティワークショップ 2018, pp. 349-356, July 2018.
28. 澤田石尚太郎, 上野嶺, 本間尚文, “ガロア体演算の共有に基づく統合認証暗号ハードウェアの設計,” 平成 30 年度電気関係学会東北支部連合大会, 2G19, September 2018.
29. 数森康平, 上野嶺, 本間尚文, “PUF による軽量かつ安全なハードウェア ID 生成システムの設計と評価,” 平成 30 年度電気関係学会東北支部連合大会, 2G17, September 2018.

30. 船越秀隼, 本間尚文, “楕円点の差分表現に基づく耐量子計算機暗号の高効率実装,” 平成 30 年度電気関係学会東北支部連合大会, 2H17, September 2018.
31. 小岩航介, 上野嶺, 藤本大介, 林優一, 永田真, 池田誠, 松本勉, 本間尚文, “楕円曲線署名ハードウェアに対するサイドチャネル攻撃とその対策,” 第 41 回多値論理フォーラム, Vol. 41, No. 08, September 2018.
32. 宮田大輔, ヴィッレ・ウリマウル, 林優一, 本間尚文, “スマートデバイスの電磁的な安全性評価に関する検討,” 第 41 回多値論理フォーラム, Vol. 41, No. 07, September 2018. **（多値論理フォーラム奨励賞受賞）**
33. 数森康平, 上野嶺, 本間尚文, “3 値 PUF を用いた暗号鍵生成に関する検討,” 第 41 回多値論理フォーラム, Vol. 41, No. 09, September 2018.
34. 森隼人, 上野嶺, 高橋順子, 林優一, 本間尚文, “OSS-RSA からのキャッシュリークの取得容易性評価,” ハードウェアセキュリティ研究会, vol. 118, no. 272, HWS2018-53, pp. 35-40, October 2018.
35. 遠藤空, 上野嶺, 青木孝文, 本間尚文, “数論変換に基づく Ring-LWE 暗号ハードウェアの高効率実装に関する検討,” ハードウェアセキュリティ研究会, vol. 118, no. 272, HWS2018-52, pp. 31-34, October 2018.
36. 上野嶺, 本間尚文, “Weak PUF を用いた耐タンパー性暗号鍵ストレージの構成法,” 2018 年ハードウェアセキュリティフォーラム, December 2019.
37. 上野嶺, 本間尚文, “偏位マスキングの多値化 PUF への拡張とその暗号鍵生成への応用,” 第 32 回多値論理とその応用研究会, No. 7, pp. 49-57, January 2019.
38. 伊東燦, 上野嶺, 本間尚文, 青木孝文, “ガロア体ハードウェアアルゴリズムの形式的トロイフリー性検証手法,” 2019 年暗号と情報セキュリティシンポジウム (SCIS 2019), No. 2D1-4, January 2019.
39. 大須賀彩希, 藤本大介, 本間尚文, Arthur Beckers, Josep Balasch, Benedikt Gierlichs, Ingrid Verbauwhede, 林優一, “TRNG on-the-fly テストを実装したリングオシレータベースの乱数生成器への周波数注入攻撃,” 2019 年暗号と情報セキュリティシンポジウム (SCIS 2019), No. 2D4-3, January 2019.
40. 上野嶺, 福島和英, 仲野有登, 清本晋作, 本間尚文, “Poly1305 への単一波形を用いたサイドチャネル攻撃とその実現可能性の評価,” 2019 年暗号と情報セキュリティシンポジウム (SCIS 2019), No. 2D3-3, January 2019.
41. Ville Yli-Mäyry, 上野嶺, 本間尚文, 青木孝文, 三浦典之, 松田航平, 永田真, Shivam Bhasin, Yves Mathieu, Tarik Graba, Jean-Luc Danger, “低遅延暗号における中間ラウンドからのサイドチャネル漏えいとその RSM に基づく効率的な対策,” 2019 年暗号と情報セキュリティシンポジウム (SCIS 2019), No. 3D3-1, January 2019.
42. 上野嶺, 森岡澄夫, 本間尚文, “情報理論的安全性を有する鍵長可変 MAC ハードウェアアーキテクチャの設計,” 2019 年暗号と情報セキュリティシンポジウム (SCIS 2019), No. 1D1-3, January 2019.

(8) 著書 / Books

1. Naofumi Homma and Marcel Medwed, “Smart Card Research and Advanced Applications - 14th International Conference, CARDIS 2015, Bochum, Germany, November 4-6, 2015. Revised Selected Papers,” Lecture Notes in Computer Science 9514, Springer, ISBN 978-3-319-31270-5, 2016.
2. Wieland Fischer and Naofumi Homma “Cryptographic Hardware and Embedded Systems - CHES 2017 - 19th International Conference, Taipei, Taiwan, September 25-28, 2017, Proceedings.” Lecture Notes in Computer Science 10529, Springer, ISBN 978-3-319-66786-7, 2017.

3. Naofumi Homma, “Special Section of PROOFS 2016,” Journal of Cryptographic Engineering, 2017.
4. Wieland Fischer and Naofumi Homma, “Special issuie of CHES 2017,” Journal of Cryptogprahic Engineering, Vol. 8, Issue 2, 2018.

(9) 特許 / Patents

1. 林優一, 本間尚文, 青木孝文, 長尾篤, 奥川雄一郎, 高谷和宏, ”タッチスクリーン用シールド,“ NTT, 特開 2016-91203
2. 林優一, 本間尚文, 青木孝文, 高谷和宏, 奥川雄一郎 “電磁的情報漏洩評価システムおよびその方法,” NTT, 特開 2016-91204
3. 三浦典之, 本間尚文, 林優一, 青木孝文, 永田真,“サイドチャネル攻撃の検知装置, サイドチャネル攻撃の検知装置によるサイドチャネル攻撃の検知方法,”東北大学・神戸大学, 特開 2017-79336
4. 鳥海陽平, 高谷和宏, 林優一, 本間尚文, 青木孝文,“電磁的情報漏洩評価装置, 電磁的情報漏洩評価方法および電磁的情報漏洩評価処理プログラム,”NTT, 特開 2017-122685
5. 鳥海陽平, 伊丹豪, 高谷和宏, 林優一, 本間尚文, 青木孝文,“電磁的情報漏洩評価装置, 電磁的情報漏洩評価方法および電磁的情報漏洩評価処理プログラム,”NTT, 特開 2017-146272
6. 伊丹豪, 鳥海陽平, 中村雅之, 鈴木康直, 高谷和宏, 林優一, 本間尚文, 青木孝文,“電磁的情報復元評価装置、電磁的情報復元評価方法および電磁的情報復元、評価処理プログラム,”NTT, 特開 2018-36552
7. 中村雅之, 伊丹豪, 鳥海陽平, 鈴木康直, 高谷和宏, 林優一, 本間尚文, 青木孝文,“漏洩電磁波評価パラメタ推定方法,”NTT, 特開 2018-91645

(10) 招待講演 / Invited Talks

1. Naofumi Homma, “Education for Practical Hardware Security Technology, 2016 IEEE International Symposium on Electromagnetic Compatibility,” Tutorial session, July 2016.
2. Naofumi Homma, “Detection and Prevention of Side-Channel Attacks,” 2016 Dagstuhl Seminar on Foundations of Secure Scaling, August 2016.
3. Naofumi Homma, “Environmentally Conscious AES Hardware Design,” STMicroelectronics workshop on hardware security, September 2016.
4. 上野嶺, 森岡澄夫, 本間尚文, 青木孝文, “CHES の紹介と日本からの発表,” 第一回ハードウェアセキュリティフォーラム, December 2016.
5. 本間尚文, “IoT セキュリティを支える暗号技術の最新動向,” IEEE SSCS Kansai Chapter 技術セミナー, October 2017.
6. 本間尚文, “IoT 時代の情報セキュリティ技術,” みやぎ高度電子機械産業振興協議会・エレクトロニクス実装学会セミナー, January 2018.
7. Naofumi Homma, “Recent Topics on Cryptographic Hardware Design,” National Tsing Hua University Seminar, April 2018.
8. Naofumi Homma, “Side-Channel-Aware LSI Design” 2018 International Symposium on VLSI-Design, Automation and Test (VLSI-DAT), April 2018. (Invited talk)
9. Naofumi Homma, “Hardware Security: Emerging Research Field in IoT Era,” International Workshop on Security (IWSEC), September 2018. (Keynote)

10. Naofumi Homma, “Hardware Security: Research Field Expanding in IoT Era,” IIH-MSP, November 2018. (Invited talk)
11. 本間尚文, “耐タンパー性暗号 LSI の設計技術,” LSI とシステムのワークショップ, 電子情報通信学会集積回路研究専門委員会 (ICD), May 2018.
12. 本間尚文, “ハードウェアセキュリティ技術とその展望,” 東北大学　電気・情報　仙台フォーラム, 東北大学電気情報系, November 2018.
13. 本間尚文, “情報セキュリティを支える暗号技術,” 寺子屋せんだい, 公益財団法人仙台市産業振興技術団, December 2018.

2. 学会活動 / Activities in academic societies

(1) 学会役員等の活動 / Activities on committees of academic societies

International

1. IEEE Sendai Section, Student Activity Committee Chair, January 2018 – present

Domestic

2. 電子情報通信学会, スマートインフォメディア研究専門委員, May 2010 – May 2016
3. 電子情報通信学会, VLSI 設計技術研究専門委員, May 2013 – May 2017
4. 電子情報通信学会, ハードウェアセキュリティ時限研究専門委員, August, 2016 – March 2018
5. 多値論理研究会, 会計監事, September, 2016 – September, 2018
6. 電子情報通信学会, ハードウェアセキュリティ研究専門委員, April, 2018 – present
7. 多値論理研究会　委員長, September 2018 -- present

(2) 学術的国際会議の企画・運営
Planning and organizing academic international conferences.

1. 2016 International Workshop on Constructive Side-Channel Analysis and Secure Design, Program Committee Member (November, 2015 – April, 2016)
2. 2016 IEEE International Symposium on Multiple-Valued Logic, Publication Chair (May, 2015 – May, 2016)
3. 2016 IEEE International Symposium on Multiple-Valued Logic, Program Committee Member (September, 2015 – May, 2016)
4. 2016 International Technical Conference on Circuits/Systems, Computers and Communications, Program Committee Member (December, 2015 – July, 2016)
5. 15th Smart Card Research and Advanced Application Conference (CARDIS 2016) Program Committee Member (December, 2015 – November, 2016)
6. 13th Workshop on Fault Diagnosis and Tolerance in Cryptography Program Committee Member (January, 2016 – August, 2016)
7. Workshop on Synthesis And System Integration of Mixed Information technologies 2016, Program Committee Member (December, 2015 – October, 2016)
8. International Workshop on Cryptographic Hardware and Embedded Systems 2016, Program Committee Member (December, 2015 – August, 2016)
9. Workshop on Security Proofs for Embedded Systems 2016, Program Committee Chair

(May, 2016 – August, 2016)

10. 2017 IEEE International Symposium on Multiple-Valued Logic, Program Committee Member (September, 2016 – May, 2017)
11. 2017 International Workshop on Constructive Side-Channel Analysis and Secure Design, Program Committee Member (November, 2016 – April, 2017)
12. 2017 Workshop on Security for Embedded and Mobile Systems, Program Committee Member (November, 2016 – April, 2017)
13. International Workshop on Cryptographic Hardware and Embedded Systems 2017, Program Committee Co-Chair (August, 2016 – September, 2017)
14. Workshop on Security Proofs for Embedded Systems 2017, Program Committee Member (January, 2017 – September, 2017)
15. International Conference on Cryptographic Hardware and Embedded Systems 2018, Program Committee Member (June, 2017 – September, 2018)
16. 2018 International Workshop on Constructive Side-Channel Analysis and Secure Design, Program Committee Member (August, 2017 – April, 2018)
17. 2018 IEEE International Symposium on Multiple-Valued Logic, Program Committee Member (September, 2017 – May, 2018)
18. Workshop on Security Proofs for Embedded Systems 2018, Program Committee Member (January, 2018 – September, 2018)
19. 8th International Conference on Security, Privacy, and Applied Cryptography Engineering, Program Committee Member (August 2018 – December 2018)
20. 2019 International Workshop on Constructive Side-Channel Analysis and Secure Design, Program Committee Member (July, 2018 – April, 2019)
21. International Conference on Cryptographic Hardware and Embedded Systems 2019, Program Committee Member (July, 2018 – August, 2019)
22. 2019 IEEE International Symposium on Multiple-Valued Logic, Program Committee Co-Chair (September, 2018 – May, 2019)

(3) 学術論文誌の編集・査読 / Editor and reviewer for academic journals.

Editor

1. Journal of Cryptographic Engineering, Associate Editor (January, 2016 – present)
2. IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES), Editorial Board Member (June, 2017 – present)
3. IEICE Transactions on Information and Systems, Guest Associate Editor, (June 2016 – August 2017)

Reviewer

4. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Reviewer, April 2016
5. IEICE Electronics Express, Reviewer, April 2016

6. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Reviewer, May 2016
7. IEEE Transactions on Computers, July 2016
8. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Reviewer, August 2016
9. IEICE Transactions on Information and Systems, Reviewer, December 2016
10. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Reviewer, February 2017
11. IEICE Electronics Express, Reviewer, February 2017
12. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Reviewer, March 2017
13. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Reviewer, April 2017
14. IEEJ Transactions on Electrical and Electronic Engineering, Reviewer, April 2017
15. IEEE Transactions on VLSI Systems, Reviewer, April 2017
16. IEICE Transactions on Electronics, Reviewer, May 2017
17. IEICE Transactions on Communications, Reviewer, June 2017
18. Journal of Cryptographic Engineering, Reviewer, September 2017
19. IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES), Reviewer, October 2017 (4 papers)
20. IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES), Reviewer, January 2018 (4 papers)
21. Journal of Cryptographic Engineering, Reviewer, February 2018
22. IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES), Reviewer, April 2018 (6 papers)
23. IEEE Transactions on Computers, Reviewer, May 2018
24. IEEE Transactions on Computers, Reviewer, June 2018
25. IEICE Electronics Express, Reviewer, June 2018
26. IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES), Reviewer, July 2018 (4 papers)
27. Journal of Cryptographic Engineering, Reviewer, August 2018
28. IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES), Reviewer, October 2018 (4 papers)
29. IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES), Reviewer, January 2019 (4 papers)
30. IEEE Transactions on Information Forensics and Security, Reviewer, January 2019
31. IEEE Transactions on Electromagnetic Compatibility, Reviewer, February 2019
32. IEEE Transactions on Circuits and Systems I: Regular Papers, Reviewer, March 2019
33. Journal of Cryptographic Engineering, Reviewer, March 2019

3. 社会貢献 / Contributions to society

(1) 教育活動 / Educational activities outside university

1. 文部科学省「分野・地域を越えた実践的情報教育協働ネットワーク」(通称 enPiT) において，ハードウェアが関連する情報セキュリティの諸問題と解決法を教授する国内初の取り組みとして，ハードウェアセキュリティ演習を開講．奈良先端科学技術大学院大学においても開講，2016-present
2. IEEE SSCS Kansai Chapter 技術セミナー，大阪，Octrober 2017
3. 科学技術振興機構日本・アジア青少年サイエンス交流事業さくらサイエンスプログラム（台湾の高校生（台北市立大同高級中学と国立南投高級中学）に対して情報セキュリティの講義を開講），October 2018
4. 宮城県仙台第一高等学校からの依頼により模擬授業を実施，November 2018

(2) 産業界における指導・啓蒙 / Instruction and education for industry

1. 組込みシステムセキュリティ技術の研究開発（KDDI 総合研究所）
2. ハードウェアの形式的検証の研究（NEC 中央研究所）
3. モバイル端末の電磁的画面盗視リスク予防方法に関する研究（NTT ネットワーク基盤技術研究所）
4. CHES の紹介と日本からの発表（2016 ハードウェアセキュリティフォーラム）
5. 暗号の White-Box 実装に対する実装安全性評価（NTT セキュアプラットフォーム研究所）
6. 認証暗号ハードウェアの研究（NEC セキュリティ研究所）
7. マイクロアーキテクチャに対するサイドチャネル解析の研究（NTT セキュアプラットフォーム研究所）
8. 車載向けハードウェアセキュリティ技術の研究（トヨタ IT 開発センター）
9. ハードウェアセキュリティ技術の研究（日立製作所）
10. 形式的検証技術の研究開発（アイシンコムクルーズ）
11. IoT 機器セキュリティ技術の研究開発（アクトラス）
12. 組込みシステムのセキュリティハードウェアの研究（インターステラテクノロジズ）
13. IoT ハードウェアセキュリティ技術の研究（三菱電機）
14. 情報セキュリティを支える暗号技術（寺子屋せんだい）
15. IoT 時代の情報セキュリティ技術（みやぎ高度電子機械産業振興協議会・エレクトロニクス実装学会）
16. 電子情報技術産業協会（JEITA）ハードウェアセキュリティ技術分科会，委員長，April 2017 - March 2019

(3) 国・地方自治体・公共団体における活動 Activities for national and local governments, and public organizations

1. CRYPTREC 暗号技術検討会，構成員，August 2009 - present
2. CRYPTREC 暗号技術評価委員会，委員，August 2009 - present
3. CRYPTREC 軽量暗号 WG，主査，July 2013 - March 2017
4. 日本学術振興会（JSPS）科学研究費委員会，専門委員，December 2017 - November 2018

5. 情報通信研究機構（NICT），専門委員，April 2014 - March 2017
6. 産業技術総合研究所（AIST）産業サイバーセキュリティ検討委員会，委員，March 2018
7. 情報処理推進機構（IPA）IT セキュリティ評価及び認証制度におけるハードウェア認証審議委員会，委員，June 2018 - March 2020
8. 日本学術振興会（JSPS）科学研究費委員会，専門委員，December 2018 - November 2019

(4) アウトリーチ活動 / Outreach activities

1. Press Release “Successful development of the world’s most efficient cryptographic processing technology for IoT devices with less than half the energy consumption needed for AES cryptographic processing,”, August 2016
2. Phy.org
3. Science Daily
4. RBB-Today
5. マイナビニュース

4. 競争的資金の獲得状況 / Research funds/grants received

(1) 科学研究費補助金 / Grant-in-Aid for Scientific Research (KAKENHI)

2016-2019: 49,938,000 Yen

代表	本間尚文 (Naofumi Homma) • 基盤研究 (A)「ガロア体算術演算に基づく VLSI データパスの形式的設計技術の開拓」 • 挑戦的萌芽研究「組込みシステムへのサイバー・フィジカル協調型攻撃を防ぐ命令シーケンス構成法の開拓」 • 国際共同研究加速基金（国際共同研究強化)「ガロア体算術演算に基づく VLSI データパスの形式的設計技術の開拓」 • 基盤研究 (A)「冗長ガロア体算術に基づくセキュリティハードウェアの高水準設計技術の研究開発」 上野嶺 (Rei Ueno) • 研究活動スタート支援「演算中に生じた誤りを訂正する機構を備えた暗号ハードウェアの設計手法の開発」	2013-2017 2016-2018 2016-2018 2017-2021 2018-2020	7,280,000 Yen (2016-2017) 3,380,000 Yen (2016-2018) 14,430,000 Yen (2016-2018) 20,020,000 Yen (2017-2019) 1,560,000 Yen (2018-2019)
分担	本間尚文 (Naofumi Homma) • 基盤研究 (A) 「暗号 VLSI の電磁波セキュリティを確保するサイドチャネル攻撃センサの構成法と実証」（代表：永田真） • 基盤研究 (B) 「公共空間におけるスマートデバイスに対する物理攻撃への対策」（代表：林優一） • 基盤研究 (B) 「局所位相配列を特徴記述子として用いた高精度画像マッチング技術の体系化」（代表：青木孝文）	2014-2017 2016-2019 2015-2018	1,638,000 Yen (2016-2017) 1,430,000 Yen (2016-2019) 200,000 Yen (2016-2018)

(2) 受託研究費 / Other grants and subsidies

2016-2019: 82,532,000 Yen

代表	本間尚文 (Naofumi Homma) • 共同研究（NTT セキュアプラットフォーム研究所）「暗号の White-Box 実装に対する実装安全性評価」 • 共同研究（NEC セキュリティ研究所）「認証暗号ハードウェアの研究」 • セコム科学技術振興財団・一般研究助成「高安全・高信頼な情報通信のためのトロイフリーLSI システム設計・検証技術の開発」 • 共同研究（NTT セキュアプラットフォーム研究所）「マイクロアーキテクチャに対するサイドチャネル解析の研究」 • 共同研究（トヨタ IT 開発センター）「車載向けハードウェアセキュリティ技術の研究」 上野嶺 (Rei Ueno) • JST さきがけ「バッテリレス無線センサネットワークのためのポスト量子暗号計算技術」	2017-2018 2017-2019 2018-2022 2018-2019 2018-2019 2018-2022	1,000,000 Yen (2017-2018) 2,000,000 Yen (2017-2019) 2,000,000 Yen (2018-2019) 500,000 Yen (2018-2019) 2,500,000 Yen (2018-2019) 10,000,000 Yen (2018-2019)
分担	本間尚文 (Naofumi Homma) • ECSEC・戦略的イノベーション創造プログラム「IoT 向けのセキュリティ確認技術の研究開発」（代表：植村泰佳） • セコム科学技術振興財団・一般研究助成「次世代 IT 社会に求められる新機能暗号とそのハードウェア実装技術の開発」（代表：松本勉） • NEDO・IoT 推進のための横断技術開発プロジェクト「Sensor-to-Cloud Security ～ビッグデータを守る革新的 IoT セキュリティ基盤技術の研究開発」（代表：松本勉） • NEDO・戦略的イノベーション創造プログラム（SIP）第 2 期・IoT 社会に対応したサイバー・フィジカル・セキュリティ「IoT サプライチェーンの信頼の創出技術基盤の研究開発」（代表：植村泰佳）	2015-2020 2015-2019 2016-2021 2018-2021	17,500,000 Yen (2016-2019) 10,000,000 Yen (2016-2019) 35,147,000 Yen (2016-2019) 1,885,000 Yen (2018-2019)

5. 国際共同研究・連携研究・連携教育活動の実績
International joint research, collaborative research, and collaborative education

(1) 国際共同研究/International joint research

1. International joint/collaborative research on hardware security with Telecom ParisTech, France, Kobe University and NAIST (2016-2019)

   ① Dispatch of researchers

(a) Naofumi Homma, September 2016 - March 2017, August 2017, November 2017, February 2018, October 2018

② Visiting researchers

(a) Jean-Luc Danger, October 2017

(b) Ulrich Kuhne, March 2019

2. International joint/collaborative research on EM information security with NAIST and KU Leuven, Belgium (2017-2019)

① Dispatch of researchers

(a) Naofumi Homma, May 2017, November 2017, January 2019

② Visiting researchers

(a) Ingrid Verbauwhede, February 2018, November 2018, March 2019

(b) Josep Balasch, February 2018, November 2018, March 2019

(c) Arthur Beckers, February 2018

(2) 連携研究/Collaborative research

1. 「暗号 VLSI の電磁波セキュリティを確保するサイドチャネル攻撃センサの構成法と実証」（神戸大学, NAIST との連携研究）2014-2017
2. 「公共空間におけるスマートデバイスに対する物理攻撃への対策」（NAIST との連携研究）2016-2019
3. 「IoT 向けのセキュリティ確認技術の研究開発」（横浜国立大学, 東京大学, 神戸大学, 電気通信大学, NAIST, 産総研との連携研究）2015-2020
4. 「次世代 IT 社会に求められる新機能暗号とそのハードウェア実装技術の開発」（横浜国立大学, 東京大学, 神戸大学, 電気通信大学, NAIST, 産総研との連携研究）2015-2019
5. 「Sensor-to-Cloud Security ～ビッグデータを守る革新的 IoT セキュリティ基盤技術の研究開発」（横浜国立大学, 三菱電機, 東京大学, 神戸大学, 産総研, ECSEC との連携研究）2016-2021
6. 「高安全・高信頼な情報通信のためのトロイフリーLSI システム設計・検証技術の開発」（神戸大学, NAIST との連携研究）2018-2022
7. 「IoT サプライチェーンの信頼の創出技術基盤の研究開発」（横浜国立大学, 神戸大学, 東京大学, NAIST, 三菱電機, 産総研との連携研究）2018-2021
8. 「暗号の White-Box 実装に対する実装安全性評価」(NTT セキュアプラットフォーム研究所, NAIST との連携研究）2017-2018
9. 「認証暗号ハードウェアの研究」（NEC セキュリティ研究所との連携研究）2017-2019
10. 「マイクロアーキテクチャに対するサイドチャネル解析の研究」（NTT セキュアプラットフォーム研究所, NAIST との連携研究）2018-2019
11. 「車載向けハードウェアセキュリティ技術の研究」(トヨタ IT 開発センターとの連携研究）2018-2019

(3) 連携教育活動/Collaborative education

1. 文部科学省「分野・地域を越えた実践的情報教育協働ネットワーク」（通称 enPiT）の教育プログラムを全国の大学と連携して実施. 特に, 開講するハードウェアセキュリティ演習では NAIST と実施, 2016-present

6. 共同利用・共同研究拠点活動の実績
Achievements of work done under the framework of Joint Usage/Research Center

1. セキュリティハードウェアの電磁波解析に関する研究（永田真, 神戸大学）2017-2019
   (a) 研究会開催 2 件（February 2018, October 2018）
   (b) 大型研究プロジェクト（セコム科学技術振興財団・一般研究助成「高安全・高信頼な情報通信のためのトロイフリーLSI システム設計・検証技術の開発」）に発展
2. 電磁情報セキュリティに関する研究（林優一, NAIST）2017-2019
   (a) 研究会開催 2 件（February 2018, September 2018）
   (b) 大型研究プロジェクト（セコム科学技術振興財団・一般研究助成「高安全・高信頼な情報通信のためのトロイフリーLSI システム設計・検証技術の開発」）に発展
3. 先端的ハードウェアセキュリティ技術に関する研究（Jean-Luc Danger, Telecom ParisTech）2017-2019
   (a) 研究会開催 2 件（October 2017, March 2019）
4. IoT 用ハードウェアセキュリティの研究（小熊博, 富山高等専門学校）2018-2019
   (a) 学生受入・共同研究の実施 3 件（August 2018, November 2018, February 2019）

7. 研究教育指導 / Research supervision
(1) 担当講義リスト / List of lectures
1. 学部教育科目/List of lectures for under graduate students
① ディジタル信号処理/Digital Signal Processing 2 単位/Credit (2009-2018)
② ディジタルコンピューティング/Digital Computing 2 単位/Credit (2010-present)
③ 創造工学研修/Creative Engineering Training 1 単位/Credit (2016-present)
④ 基礎ゼミ/Basic seminar 2 単位/Credit (2010-present)
⑤ 電気･通信･電子･情報工学セミナー/Engineering Seminar 3 単位/Credit (2016-present)
⑥ 電気情報物理工学卒業研修/Graduation Thesis 6 単位/Credit (2016-present)
⑦ 学生実験 A/Laboratory A (2018-present)

2. 大学院教育科目/List of lectures for under graduate students
① セキュア情報通信システム論/Secure Information Communication System 2 単位/Credit (2018-present)
② 工学セミナー/Engineering Seminar 3 単位/Credit (2016-present)
③ 通信工学修士研修/Master Course Seminar on Communication Engineering 6 単位/Credit (2016-present)
④ 通信工学特別研修/Advanced Seminar on Communication Engineering 2 単位/Credit (2016-present)
⑤ 通信工学博士研修/Doctor Course Seminar on Communication Engineering 2 単位/Credit (2016-present)

(2) 学位取得者リスト
List of bachelor’s, master’s and doctoral degree students supervised

	2016	2017	2018
博士課程修了者 /Doctoral degree	0	1	1
修士課程修了者 /Master’s degree	2	2	5
学部卒業者 /Bachelor’s degree	2	3	3

1. 学部卒業者/List of Bachelor’s degree students supervised

   2016: 伊東燦/Akira Ito, 遠藤空/Sora Endo

   2017: 数森康平/Kohei Kazumori, 澤田石尚太郎/Shotaro Sawataishi, 船越秀隼/Shuto Funakoshi

   2018: 永戸謙成/Kensei Nagato, 小田麻矢/Maya Oda, 大澤創紀/Souki Ohsawa

2. 修士卒業者/List of Master’s degree students supervised

   2016: 石幡大輔/Daisuke Ishihata, 河井航/Wataru Kawai

   2017: 忍田大和/Hirokazu Oshida, 鈴木麻奈美/Manami Suzuki

   2018: 伊東燦/Akira Ito, 宮田大輔/Daisuke Miyata, 小岩航介/Kosuke Koiwa, 森隼人/Hayato Mori, 遠藤空/Sora Endo

3. 博士卒業者/List of Doctoral degree students supervised

   2017: 上野嶺/Rei Ueno

   2018: ヴィッレウリマウル/Ville Yli-Mäyry

8. 叙勲・受賞・表彰 / Honors, awards, and prizes

1. 多値論理フォーラム奨励賞, 鈴木麻奈美, 上野嶺, 本間尚文, 青木孝文, “物理複製困難関数の多値化とその応用に関する検討,” January 7, 2017
2. Kenneth C. Smith Early Career Award in Microelectronics, Rei Ueno, “Formal Design of Pipelined GF Arithmetic Circuits and Its Application to Cryptographic Processors,” May 23, 2017.
3. RIEC Award 学生賞, 上野嶺, “ガロア体算術演算回路の形式的設計技術とその暗号ハードウェアへの応用に関する研究,” October 31, 2017.
4. SCIS 論文賞, 上野嶺, “1 階 TI に基づく耐タンパー性を有する高効率 AES 暗号プロセッサの実装,” 2017 年暗号と情報セキュリティシンポジウム (SCIS 2017), January 24, 2018.
5. 第 14 回日本学術振興会賞, 本間尚文, “算術演算ハードウェアアルゴリズムの理論構築と暗号ハードウェア設計への応用,” February 7, 2018.
6. 東北大学工学部長賞, 船越秀隼, March 26, 2018.
7. 東北大学情報科学研究科長賞, 上野嶺, March 27, 2018.

8. 東北大学総長賞，上野嶺，March 27，2018.
9. 第 50 回市村学術賞貢献賞， 本間尚文， “ハードウェアアルゴリズムの高水準設計手法の開発とその応用，” April 16，2018.
10. 情報処理学会東北支部奨励賞，遠藤空， “数論変換に基づく秘匿計算向け暗号の高効率実装，” June 20，2018.
11. German Innovation Award Gottfried Wagener Prize 2018， Naofumi Homma， “Design Methodology for Lightweight Tamper-Resistant Cryptographic Hardware，” June 26，2018.
12. ハードウェアセキュリティ夏のワークショップ 最優秀ポスター賞，伊東燦， “ハードウェアトロイに耐性を有する算術演算回路の構成とその評価，” September 28，2018.
13. 第 41 回多値論理フォーラム奨励賞，宮田大輔，ヴィッレウリマウル，林優一，本間尚文， “スマートデバイスの電磁的な安全性評価に関する検討，” January 12，2019.

9. その他 / Others

1. 算術演算モジュールジェネレータの開発・公開/Development and release of Arithmetic Module Generator，https://www.ecsis.riec.tohoku.ac.jp/topics/amg，March 2019