様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　６ 年　 ６ 月 １０ 日現在

機関番号：１１３０１
研究種目：若手研究
研究期間：2020～2023
課題番号：２０Ｋ１９７６５

研究課題名（和文）物理複製困難ハードウェアIDに基づく高安全・高信頼な認証システムの開発

研究課題名（英文）Development of highly secure and reliable authentication system based on physically unclonable hardware identifier

研究代表者

上野　嶺（Ueno, Rei）

東北大学・電気通信研究所・助教

研究者番号：８０８２６１６５

交付決定額（研究期間全体）：（直接経費）　　3,200,000円

研究成果の概要（和文）：本研究では，まず，物理複製困難関数（PUF）からハードウェアIDを，確率的手法に基づいて，極めて効率的かつ高信頼に抽出する手法を複数開発した．その中でも最も新しい提案手法では，標準的なほぼ全ての状況下でハードウェアIDを既存手法に比べて高効率に抽出でき，同等の安全性を担保しつつPUFのハードウェア実装コストを最大で55%削減できることを確認した．さらに，PUFに基づく認証モジュールは各種サイドチャネル攻撃の対象となりうるが，PUFによって生成された秘密鍵・認証鍵の抽出を目的としたサイドチャネル攻撃の評価を行うとともに，対策としてマスキングや暗号鍵変換の有効性を確認した．

研究成果の学術的意義や社会的意義
本研究成果は，確率的アルゴリズムの有効性をPUFに基づく認証システムの構築に応用することで，現実的コストで実装可能な手法の中で到達可能な効率性の解明に大きく貢献した．また，PUFは暗号アルゴリズム・プロトコルにおける「信頼の起点（root-of-trust）」として扱うことで暗号アルゴリズム・プロトコルの信頼をハードウェアから保証するという重要な役割がある．本成果によりPUFを信頼の起点として扱うコストが大幅に削減したことで，ハードウェアroot-of-trustの普及，そしてより安全・高信頼な情報社会に貢献する．

研究成果の概要（英文）：Wwe developed multiple methods to extract hardware IDs from Physical Unclonable Functions (PUFs) with extremely high efficiency and reliability based on probabilistic techniques. Among these methods, the most recent proposal demonstrated significantly higher efficiency in extracting hardware IDs compared to existing methods in most standard scenarios, allowing for up to a 55% reduction in hardware implementation costs of PUFs while ensuring equivalent security. Furthermore, as cryptographic authentication modules based on PUFs can be vulnerable to various side-channel attacks, we evaluated side-channel attacks to extract secret and authentication keys generated by PUFs. Subsequently, we confirmed the effectiveness of countermeasures such as masking and cryptographic key transformation.

研究分野：ハードウェアセキュリティ

キーワード：物理複製困難関数（PUF）　hardware root-of-trust　暗号　情報セキュリティ

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

LSI の認証技術は物流の効率化やトレーサビリティの確保，商品の真贋判定のために広く普及している．LSI の解析・製造技術の発展に伴い LSI の模造品や偽造品，非正規品による被害が急増しており，無視できない社会問題となっている．現在では半導体製品の 5%以上が模造品・非正規品と言われており今後も被害は拡大する恐れがある．そこで，LSI の模造品や偽造品，非正規品に対する対策として，LSI 上に実装可能な物理複製困難関数 (PUF: Physically Unclonable Function) に基づくハードウェア認証技術が期待されている[1]．PUF は LSI 製造時の制御不可能な物理的ばらつき（半導体素子のドライブ能力や配線遅延など）を利用することで各個体に固有かつ第三者に予測不可能な値，すなわちハードウェア ID を生成する．ハードウェア ID は LSI の指紋のようなものであり，PUF に基づくハードウェア認証では PUF の出力値（レスポンス）を暗号鍵の生成や格納に用いることでリバースエンジニアリングなどの LSI 解析が可能な攻撃者に対しても安全な認証を行うことが可能となる．

しかしながら，PUF レスポンスの乱数性が不足している場合は求められる安全性を達成できないという問題があった．特に，PUF レスポンスが制御不可能であるために必要な性質として一様性が挙げられる．一様性はレスポンスの 0 と 1 の出現確率が等しい（バイアスが無い）という性質であり，PUF レスポンスに無視できないバイアスがある場合，攻撃者は容易にハードウェア ID を特定可能であることが知られている．しかしながら，PUF は上述のとおり制御不可能な微小な物理的ばらつきに基づいて性能されるため，用いるテクノロジによっては完全に安定かつ一様な PUF を製造することはしばしば困難となる．したがって，レスポンスの安定性と一様性が低い PUF を用いても高い安全性と信頼性を有するハードウェア ID 生成・認証システムの実現に高い需要があり，非安定かつ非一様な PUF レスポンスから効率的に安定かつ一様なレスポンスを抽出する技術が強く求められていた．

２．研究の目的

本研究は，PUF に基づく高安全・高信頼なハードウェア認証システムの構築法の確立を目的として，PUF から安定かつ安全なハードウェア ID を高効率に抽出する手法の理論的基礎の構築を行う

３．研究の方法

本研究では，PUF から安定かつ安全なハードウェア ID を高効率に抽出する手法の理論的基礎の構築を目指して，(i) PUF レスポンスの抽出に求められる符号化手法・サンプリング手法の要件の解明，および (ii) PUF レスポンスの分布とエラーパターンが与えられたときに最適となるハードウェア ID 生成・認証システムの構成法の定式化を行う．

(i) においては，どのような符号化手法およびサンプリング手法が PUF レスポンスおよびハードウェア ID 生成・認証システムに適しているのかを理論面および実装面の両

方から解明する．例えば，ハッシュ関数は PUF レスポンスから一様なレスポンスを抽出することは可能であるが, 同手法は誤りをレスポンス全体に拡散してしまうため PUF レスポンスの抽出には利用できない．すなわち，誤りの拡散や復元可能性，安全性（一様性），そして実装時における性能（回路面積やレイテンシ，消費電力など）のトレードオフを考慮したレスポンス符号化手法・サンプリング手法に求められる要件を解明する．その上で，要件を満たすレスポンス抽出手法を開発し，シミュレーションや FPGA 実装を用いてその正当性と効率を評価する．

次に (ii) について述べる．テクノロジや PUF 回路の構成法によって PUF レスポンスの誤りパターンや分布は大きく異なることが知られている．そこで，PUF レスポンスの誤りパターンや分布が与えられたときに，上述のトレードオフを考慮して最適となるハードウェア ID 生成・認証システムの構成法を明らかにする．すなわち，与えられた PUF レスポンスの情報に対して，最も実装コストを小さくできる ECC の構成，符号化手法，サンプリング手法の組み合わせを構成する方法を定式化する．これにより，多くのテクノロジや PUF 回路に対して容易に PUF に基づく高安全・高信頼のハードウェア ID 生成・認証システムが利用可能となる．

４．研究成果

本研究では，まず，物理複製困難関数（PUF）からハードウェア ID を，確率的手法に基づいて，極めて効率的かつ高信頼に抽出する手法を複数開発した．その中でも最も新しい提案手法では，標準的なほぼ全ての状況下でハードウェア ID を既存手法に比べて高効率に抽出でき，同等の安全性を担保しつつ PUF のハードウェア実装コストをシミュレーションにより最大で 55%削減できることを確認した．また，同手法は多値符号化された PUF にも拡張されており，シミュレーションおよび FPGA による実機評価によりその有効性を確認している．

さらに，PUF に基づく認証システムの包括的な物理的安全性評価を実施することで，認証モジュールの実利用における妥当性評価も行った．PUF に基づく認証モジュールは各種サイドチャネル攻撃の対象となりうるが，PUF によって生成された秘密鍵・認証鍵の抽出を目的としたサイドチャネル攻撃の評価を行うとともに，対策としてマスキングや暗号鍵変換の有効性を確認した．

５．主な発表論文等

〔雑誌論文〕　計23件（うち査読付論文　21件／うち国際共著　0件／うちオープンアクセス　17件）

１．著者名 Ueno Rei、Homma Naofumi	４．巻 4
２．論文標題 How Secure is Exponent-blinded RSA?CRT with Sliding Window Exponentiation?	５．発行年 2023年
３．雑誌名 IACR Transactions on Cryptographic Hardware and Embedded Systems	６．最初と最後の頁 241～269
掲載論文のDOI（デジタルオブジェクト識別子） 10.46586/tches.v2023.i2.241-269	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 Ito Akira、Ueno Rei、Homma Naofumi	４．巻 -
２．論文標題 On the Success Rate of Side-Channel Attacks on Masked Implementations	５．発行年 2022年
３．雑誌名 Proceedings on ACM SIGSAC Conference on Computer and Communications Security	６．最初と最後の頁 1521～1535
掲載論文のDOI（デジタルオブジェクト識別子） 10.1145/3548606.3560579	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 Saito Kotaro、Ito Akira、Ueno Rei、Homma Naofumi	４．巻 4
２．論文標題 One Truth Prevails: A Deep-learning Based Single-Trace Power Analysis on RSA?CRT with Windowed Exponentiation	５．発行年 2022年
３．雑誌名 IACR Transactions on Cryptographic Hardware and Embedded Systems	６．最初と最後の頁 490～526
掲載論文のDOI（デジタルオブジェクト識別子） 10.46586/tches.v2022.i4.490-526	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 Ito Akira、Ueno Rei、Homma Naofumi	４．巻 4
２．論文標題 Perceived Information Revisited	５．発行年 2022年
３．雑誌名 IACR Transactions on Cryptographic Hardware and Embedded Systems	６．最初と最後の頁 228～254
掲載論文のDOI（デジタルオブジェクト識別子） 10.46586/tches.v2022.i4.228-254	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 Inoue Akiko、Minematsu Kazuhiko、Oda Maya、Ueno Rei、Homma Naofumi	４．巻 17
２．論文標題 ELM: A Low-Latency and Scalable Memory Encryption Scheme	５．発行年 2022年
３．雑誌名 IEEE Transactions on Information Forensics and Security	６．最初と最後の頁 2628～2643
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/tifs.2022.3188146	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 Nakashima Ayano、Ueno Rei、Homma Naofumi	４．巻 69
２．論文標題 AES S-Box Hardware With Efficiency Improvement Based on Linear Mapping Optimization	５．発行年 2022年
３．雑誌名 IEEE Transactions on Circuits and Systems II: Express Briefs	６．最初と最後の頁 3978～3982
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/tcsii.2022.3185632	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 Koseki Ryusuke、Ito Akira、Ueno Rei、Tibouchi Mehdi、Homma Naofumi	４．巻 -
２．論文標題 Homomorphic encryption for stochastic computing	５．発行年 2022年
３．雑誌名 Journal of Cryptographic Engineering	６．最初と最後の頁 -
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/s13389-022-00299-6	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 Itabashi Yuma、Ueno Rei、Homma Naofumi	４．巻 -
２．論文標題 Efficient Modular Polynomial Multiplier for NTT Accelerator of Crystals-Kyber	５．発行年 2022年
３．雑誌名 Proceedings on Euromicro Conference on Digital System Design	６．最初と最後の頁 528～533
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/dsd57027.2022.00076	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 Ueno Rei、Homma Naofumi	4．巻 -
2．論文標題 High-Speed Hardware Architecture for Post-Quantum Diffie?Hellman Key Exchange Based on Residue Number System	5．発行年 2022年
3．雑誌名 Proceedings on IEEE International Symposium on Circuits and Systems	6．最初と最後の頁 -
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/ISCAS48785.2022.9937804	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Ito Akira、Ueno Rei、Homma Naofumi	4．巻 41
2．論文標題 Efficient Formal Verification of Galois-Field Arithmetic Circuits Using ZDD Representation of Boolean Polynomials	5．発行年 2022年
3．雑誌名 IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems	6．最初と最後の頁 794～798
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TCAD.2021.3059924	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 Rei Ueno, Naofumi Homma, Sumio Morioka, and Takafumi Aoki	4．巻 38
2．論文標題 A Systematic Design Methodology of Formally-Proven Side-Channel-Resistant Cryptographic Hardware	5．発行年 2021年
3．雑誌名 IEEE Design & Test Magazine	6．最初と最後の頁 84～92
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/MDAT.2021.306333.	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 ITO Akira、UENO Rei、HOMMA Naofumi	4．巻 E104.D
2．論文標題 An Algebraic Approach to Verifying Galois-Field Arithmetic Circuits with Multiple-Valued Characteristics	5．発行年 2021年
3．雑誌名 IEICE Transactions on Information and Systems	6．最初と最後の頁 1083～1091
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transinf.2020LOP0004	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Ito Akira、Saito Kotaro、Ueno Rei、Homma Naofumi	4．巻 16
2．論文標題 Imbalanced Data Problems in Deep Learning-Based Side-Channel Attacks: Analysis and Solution	5．発行年 2021年
3．雑誌名 IEEE Transactions on Information Forensics and Security	6．最初と最後の頁 3790～3802
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TIFS.2021.3092050	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 Nashimoto Shoei、Suzuki Daisuke、Ueno Rei、Homma Naofumi	4．巻 1
2．論文標題 Bypassing Isolated Execution on RISC-V using Side-Channel-Assisted Fault-Injection and Its Countermeasure	5．発行年 2021年
3．雑誌名 IACR Transactions on Cryptographic Hardware and Embedded Systems	6．最初と最後の頁 28～68
掲載論文のDOI（デジタルオブジェクト識別子） 10.46586/tches.v2022.i1.28-68	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 Ueno Rei、Xagawa Keita、Tanaka Yutaro、Ito Akira、Takahashi Junko、Homma Naofumi	4．巻 1
2．論文標題 Curse of Re-encryption: A Generic Power/EM Analysis on Post-Quantum KEMs	5．発行年 2021年
3．雑誌名 IACR Transactions on Cryptographic Hardware and Embedded Systems	6．最初と最後の頁 296～322
掲載論文のDOI（デジタルオブジェクト識別子） 10.46586/tches.v2022.i1.296-322	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 Xagawa Keita、Ito Akira、Ueno Rei、Takahashi Junko、Homma Naofumi	4．巻 1
2．論文標題 Fault-Injection Attacks Against NIST’s Post-Quantum Cryptography Round 3 KEM Candidates	5．発行年 2021年
3．雑誌名 nternational Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT2021)	6．最初と最後の頁 33～61
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-92075-3_2	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Ueno Rei、Takahashi Junko、Hayashi Yu-ichi、Homma Naofumi	4．巻 －
2．論文標題 A method for constructing sliding windows leak from noisy cache timing information	5．発行年 2020年
3．雑誌名 Journal of Cryptographic Engineering	6．最初と最後の頁 －
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/s13389-020-00230-x	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 Sawataishi Shotaro、Ueno Rei、Homma Naofumi	4．巻 67
2．論文標題 Unified Hardware for High-Throughput AES-Based Authenticated Encryptions	5．発行年 2020年
3．雑誌名 IEEE Transactions on Circuits and Systems II: Express Briefs	6．最初と最後の頁 1604～1608
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TCSII.2020.3013415	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 Rei Ueno、Kohei Kazumori、Naofumi Homma	4．巻 4
2．論文標題 Rejection Sampling Schemes for Extracting Uniform Distribution from Biased PUFs	5．発行年 2020年
3．雑誌名 IACR Transactions on Cryptographic Hardware and Embedded Systems	6．最初と最後の頁 86～128
掲載論文のDOI（デジタルオブジェクト識別子） 10.13154/tches.v2020.i4.86-128	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 Kazumori Kohei、Ueno Rei、Homma Naofumi	4．巻 －
2．論文標題 Debiasing Method for Efficient Ternary Fuzzy Extractors and Ternary Physically Unclonable Functions	5．発行年 2020年
3．雑誌名 Proceedings of International Symposium on Multiple-Value Logic	6．最初と最後の頁 52～57
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/ISMVL49045.2020.00-30	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 Ueno Rei、Homma Naofumi、Morioka Sumio、Aoki Takafumi	4．巻 －
2．論文標題 A Systematic Design Methodology of Formally-Proven Side-Channel-Resistant Cryptographic Hardware	5．発行年 2021年
3．雑誌名 IEEE Design & Test	6．最初と最後の頁 1～1
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/MDAT.2021.3063337	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 上野嶺、本間尚文	4．巻 34
2．論文標題 物理複製困難関数を用いたハードウェア認証技術	5．発行年 2021年
3．雑誌名 月刊自動認識	6．最初と最後の頁 36～43
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Ueno Rei、Homma Naofumi、Inoue Akiko、Minematsu Kazuhiko	4．巻 2024
2．論文標題 Fallen Sanctuary: A Higher-Order and Leakage-Resilient Rekeying Scheme	5．発行年 2023年
3．雑誌名 IACR Transactions on Cryptographic Hardware and Embedded Systems	6．最初と最後の頁 264～308
掲載論文のDOI（デジタルオブジェクト識別子） 10.46586/tches.v2024.i1.264-308	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

〔学会発表〕　計46件（うち招待講演　5件／うち国際学会　14件）

1．発表者名 Rei Ueno
2．発表標題 High-Speed Hardware Architecture for Post-Quantum Diffe-Hellman Key Exchange Based on Residue Number Systems
3．学会等名 IEEE International Symposium on Circuits and Systems（国際学会）
4．発表年 2022年

１．発表者名
Rei Ueno

２．発表標題
AES S-Box Hardware with Efficiency Improvement Based on Linear Mapping Optimization

３．学会等名
IEEE International Symposium on Integrated Circuits and Systems（国際学会）

４．発表年
2022年

１．発表者名
Akira Ito

２．発表標題
Perceived Information Revisited: New Metrics to Evaluate Success Rate of Side-Channel Attacks

３．学会等名
International Conference on Cryptographic Hardware and Embedded Systems（国際学会）

４．発表年
2022年

１．発表者名
Rei Ueno

２．発表標題
ne Truth Prevails: A Deep-learning Based Single-Trance Power Analysis on RSA--CRT with Windowed Exponentiation

３．学会等名
International Conference on Cryptographic Hardware and Embedded Systems（国際学会）

４．発表年
2022年

１．発表者名
Rei Ueno

２．発表標題
Curse of Re-encryption: A Generic Power/EM Analysis on Post-Quantum KEMs

３．学会等名
International Conference on Cryptographic Hardware and Embedded Systems（国際学会）

４．発表年
2022年

１．発表者名
Shoe Nashimoto

２．発表標題
Bypassing Isolated Execution on RISC-V using Side-Channel-Assisted Fault-Injection and Its Countermeasure

３．学会等名
International Conference on Cryptographic Hardware and Embedded Systems（国際学会）

４．発表年
2022年

１．発表者名
Shoe Nashimoto

２．発表標題
PoC TEE: Proof-of-Concept Implementation of RISC-V Trusted Execution Environment for Embedded Devices

３．学会等名
Topics in hArdware SEcurity and RISC-V（国際学会）

４．発表年
2022年

１．発表者名
Akira Ito

２．発表標題
On the Success Rate of Side-Channel Attacks on Masked Implementations: Information-Theoretical Bounds and Their Practical Usage

３．学会等名
ACM SIGSAC Conference on Computer and Communications Security（国際学会）

４．発表年
2022年

１．発表者名
上野嶺

２．発表標題
層学習サイドチャネル攻撃における交差エントロピー損失関数と攻撃性能の関係に関する考察

３．学会等名
ハードウェアセキュリティ研究会

４．発表年
2022年

１．発表者名
羽田大倫

２．発表標題
Gem5を用いたメモリ暗号化認証スキームELMのシステムレベル性能評価

３．学会等名
LSIとシステムのワークショップ

４．発表年
2022年

１．発表者名
田中祐太郎

２．発表標題
耐量子鍵カプセル化メカニズムに対する多クラスニューラルネットワークを用いたサイドチャネル攻撃の検討

３．学会等名
ハードウェアセキュリティ研究会

４．発表年
2022年

１．発表者名
羽田大倫

２．発表標題
更新並列化可能認証木に基づく高速なセキュア不揮発性メモリの実現

３．学会等名
ARC研究会

４．発表年
2022年

１．発表者名
蛯名克海

２．発表標題
AES-CTRに対するプロファイリングサイドチャネル解析の検討

３．学会等名
ハードウェアセキュリティ研究会

４．発表年
2022年

１．発表者名
田村佑樹

２．発表標題
AES-CTRに対するプロファイリングサイドチャネル解析の検討

３．学会等名
ハードウェアセキュリティ研究会

４．発表年
2022年

１．発表者名
上野嶺

２．発表標題
耐ソフトエラー性浮動小数点数値表現の提案とその実機評価

３．学会等名
第66回宇宙科学技術連合講演会

４．発表年
2022年

１．発表者名
上野嶺

２．発表標題
ハードウェアセキュリティに関する主要な国際学術会議の動向

３．学会等名
ハードウェアセキュリティフォーラム（招待講演）

４．発表年
2022年

１．発表者名
田中祐太郎

２．発表標題
耐量子計算機暗号に対する多値ニューラルネットワークを用いたサイドチャネル解析

３．学会等名
第36回多値論理とその応用研究会

４．発表年
2023年

１．発表者名
田村佑樹

２．発表標題
確率的暗号化状態処理ハードウェアの設計と評価

３．学会等名
第36回多値論理とその応用研究会

４．発表年
2023年

１．発表者名
梨本翔永

２．発表標題
TEEバイパス攻撃対策のRISC-V Keystone実装評価

３．学会等名
2023年暗号と情報セキュリティシンポジウム

４．発表年
2023年

１．発表者名
上野嶺

２．発表標題
部分鍵差分推測を用いたノンプロファイリング型深層学習サイドチャネル攻撃に関する検討

３．学会等名
2023年暗号と情報セキュリティシンポジウム

４．発表年
2023年

１．発表者名
上野嶺

２．発表標題
分離カウンタを用いたセキュアNVMの効率的な復旧保証

３．学会等名
ETNET2023

４．発表年
2023年

１．発表者名
Akira Ito

２．発表標題
A Formal Approach to Identifying Hardware Trojans in Cryptographic Hardware

３．学会等名
IEEE 51th International Symposium on Multiple-Valued Logic (ISMVL)（国際学会）

４．発表年
2021年

１．発表者名
Shoei Nashimoto

２．発表標題
Bypassing Isolated Execution on RISC-V using Side-Channel-Assisted Fault-Injection and Its Countermeasure

３．学会等名
International Conference on Cryptographic Hardware and Embedded Systems（国際学会）

４．発表年
2022年

１．発表者名
Rei Ueno

２．発表標題
Curse of Re-encryption: A Generic Power/EM Analysis on Post-Quantum KEMs

３．学会等名
International Conference on Cryptographic Hardware and Embedded Systems（国際学会）

４．発表年
2022年

１．発表者名
Keita Xagawa

２．発表標題
Fault-Injection Attacks against NIST’s Post-Quantum Cryptography Round 3 KEM Candidates

３．学会等名
International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT2021)（国際学会）

４．発表年
2021年

１．発表者名
上野嶺

２．発表標題
招待講演］バイアスを有するPUFからの棄却サンプリングを用いた一様乱数の抽出法（CHES2020より）

３．学会等名
ハードウェアセキュリティ研究会（招待講演）

４．発表年
2021年

１．発表者名
伊東燦

２．発表標題
深層学習を用いたサイドチャネル攻撃の性能評価手法に関する検討

３．学会等名
ハードウェアセキュリティ研究会

４．発表年
2021年

１．発表者名
上野嶺

２．発表標題
剰余数系を用いた同種写像暗号の高速ハードウェア実装

３．学会等名
ハードウェアセキュリティ研究会

４．発表年
2021年

１．発表者名
上野嶺

２．発表標題
並列化Quotient Pipeliningモンゴメリ乗算に基づくFp2乗算器データパスの設計とその同種写像暗号への応用に関する検討

３．学会等名
ハードウェアセキュリティ研究会

４．発表年
2021年

１．発表者名
伊東燦

２．発表標題
マスキング対策された暗号ハードウェアへの深層学習を用いたサイドチャネル解析

３．学会等名
ハードウェアセキュリティ研究会

４．発表年
2021年

１．発表者名
伊藤圭吾

２．発表標題
軽量暗号GIMLIに対するサイドチャネル解析の検討

３．学会等名
34回回路とシステムワークショップ

４．発表年
2021年

１．発表者名
板橋由磨

２．発表標題
格子暗号向け数論変換ハードウェアの設計

３．学会等名
第44回多値論理フォーラム

４．発表年
2021年

１．発表者名
齋藤宏太郎

２．発表標題
耐タンパー性を有するCRT-RSAソフトウェアに対する深層学習に基づく単一波形サイドチャネル攻撃

３．学会等名
ハードウェアセキュリティ研究会

４．発表年
2021年

１．発表者名
板橋由磨

２．発表標題
格子暗号向けKリダクションに基づく数論変換ハードウェアの検討

３．学会等名
ハードウェアセキュリティ研究会

４．発表年
2021年

１．発表者名
伊藤圭吾

２．発表標題
軽量暗号GIMLI-AEADに対する深層学習を用いたサイドチャネル解析の検討

３．学会等名
情報セキュリティ研究会

４．発表年
2021年

１．発表者名
中嶋彩乃

２．発表標題
アンロールドアーキテクチャに基づく AESハードウェア特有のサイドチャネル情報漏洩の評価

３．学会等名
ハードウェアセキュリティフォーラム

４．発表年
2021年

１．発表者名
上野嶺

２．発表標題
耐量子鍵カプセル化メカニズムに対する一般化サイドチャネル攻撃

３．学会等名
2022年暗号と情報セキュリティシンポジウム

４．発表年
2022年

１．発表者名
草川恵太

２．発表標題
NIST PQC Round3候補の鍵カプセル化方式への故障注入攻撃

３．学会等名
2022年暗号と情報セキュリティシンポジウム

４．発表年
2022年

１．発表者名
伊東燦

２．発表標題
マスキング対策実装に対するサイドチャネル攻撃成功確率の情報理論的解析,

３．学会等名
2022年暗号と情報セキュリティシンポジウム

４．発表年
2022年

１．発表者名
小関隆介

２．発表標題
確率的準同型暗号の高効率化とその性能評価

３．学会等名
ハードウェアセキュリティ研究会

４．発表年
2022年

１．発表者名
中嶋彩乃

２．発表標題
アンロールド実装されたAESハードウェア特有のサイドチャネル情報漏洩の評価

３．学会等名
ハードウェアセキュリティ研究会

４．発表年
2022年

１．発表者名
梨本翔永

２．発表標題
RISC-V Keystoneへの故障注入に基づく隔離実行バイパス攻撃

３．学会等名
ハードウェアセキュリティ研究会

４．発表年
2022年

１．発表者名
Rei Ueno

２．発表標題
Rejection Sampling Schemes for Extracting Uniform Distribution from Biased PUFs

３．学会等名
International Conference on Cryptographic Hardware and Embedded Systems（国際学会）

４．発表年
2020年

１．発表者名
上野嶺

２．発表標題
物理複製困難関数が実現する情報セキュリティとその方法

３．学会等名
第12回暗号及び情報セキュリティと数学の相関ワークショップ（CRISMATH 2020）（招待講演）

４．発表年
2020年

１．発表者名
上野嶺

２．発表標題
バイアスを有するPUFからの棄却サンプリングを用いた一様乱数の抽出法（CHES2020より）

３．学会等名
ハードウェアセキュリティ研究会（招待講演）

４．発表年
2021年

１．発表者名 Rei Ueno
２．発表標題 Secure Implementation of Post-Quantum Cryptography: Challenges and Opportunities
３．学会等名 International Conference on Information Security and Cryptology（招待講演）（国際学会）
４．発表年 2023年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関