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　５ 年　 ６ 月 １６ 日現在

機関番号：１２６１２
研究種目：基盤研究(S)
研究期間：2018～2022
課題番号：１８Ｈ０５２８９

研究課題名（和文）暗号技術によるIoTエコシステムのレジリエンス向上

研究課題名（英文）Resilience Enhancement of IoT Ecosystem by Cryptographic Technologies

研究代表者
崎山　一男（Sakiyama, Kazuo）

電気通信大学・大学院情報理工学研究科・教授

研究者番号：８０５０８８３８

交付決定額（研究期間全体）：（直接経費）　 152,500,000円

研究成果の概要（和文）：レーザー照射や直接プロービングでIoTデバイス内部の信号を読み取る物理攻撃に対して、安全性状態の循環をIoTエコシステムの機能とみなし、漏洩耐性暗号(暗号理論分野)、漏洩鍵の蒸留(情報理論分野)及び漏洩検知技術(ハードウェアセキュリティ分野)の3課題に取り組み、トップレベルの国際会議や学術論文誌で研究成果を発表した。従来の研究の枠組みを超え分野横断的に研究を推進し、攻撃を検知するリーケージセンサ回路、安全に鍵を修復するアルゴリズムとそれらを安全に運用するプロトコルを開発することができ、信頼の基点となる暗号ハードウェアによるレジリエントなIoTシステムの構築に資する成果をあげることができた。

研究成果の学術的意義や社会的意義
情報基盤が高度に整備され、多くの人がデジタル化の利便性を享受できるようになった。しかし、社会に新しい技術が普及することでセキュリティを脅かす新たな脅威が出現している。セキュリティの根幹を担う暗号技術の脆弱性をつく攻撃者の手の内を明かし、効率的な対策を社会実装し、攻撃による被害を未然に防ぐ、あるいは最小限に留めるにはどうすれば良いか？
本研究課題で得られた成果は、こういった社会からのセキュリティ上のニーズに柔軟に応えた。学術の観点からは、複数の学術分野で培った知識を融合することで、セキュリティやプライバシーに関する暗号技術のさらなる深化と新たな学術的知識創生の場の形成に寄与した。

研究成果の概要（英文）：Against physical attacks that read signals inside IoT devices by laser irradiation or direct probing, by regarding the circulation of security states as a function of the IoT ecosystem, we worked on leakage-resilient cryptography (cryptography field), information distillation (information theory field), and leakage detection technology (hardware security field.) We have presented the research results at top-tier international conferences and academic journals. Furthermore, by promoting cross-disciplinary research beyond conventional research, we have developed leakage sensor circuits that detect attacks, algorithms that securely restore keys, and protocols that operate them securely. As a result, we have achieved significant results that contribute to constructing a resilient IoT system using cryptographic hardware.

研究分野：応用暗号学

キーワード：情報セキュリティ　暗号理論　情報理論　ハードウェアセキュリティ　集積回路工学

１．研究開始当初の背景

暗号回路に対する物理攻撃は、IoT セキュリティにおけるルートオブトラスト（信頼の基点）であるハードウェア上の暗号機能を無力化し、IoT システム全体の掌握に繋がる最も現実的で強力な攻撃のひとつである。物理攻撃の中でも、レーザー光を用いたレーザーフォールト攻撃は、極めて高い時空間分解能で暗号回路に故障を誘発することを可能にする。例えば、暗号処理中のあるタイミングにおいて、特定の中間値に１ビットのフォールトを高い確率で発生させることができる。攻撃者にとって極めて有利なフォールトモデルを仮定できるため、僅か数回のフォールト注入で AES 暗号の秘密鍵情報が全て漏洩することが知られている。実際の暗号回路を搭載した IC チップに対する攻撃実験でも実証されており、レーザーフォールト攻撃が情報セキュリティに対する最も深刻な攻撃であることは、学術界だけでなく産業界でも広く認識されている。攻撃における情報漏洩メカニズムの解明と低コストでの検知及び対策技術の確立は急務である。

攻撃者の能力が格段に高くなった場合には、レーザーフォールト攻撃を凌駕するプロービング攻撃を想定しなければならない。従来のプロービング攻撃では、IC チップを開封し、暗号回路上の配線にプローブ針を物理的に接触させ、暗号処理中の電圧変化を直接観測するか、近傍電磁界の変化を観測し中間値を読み出すことを想定していた。前者の方法では、IC チップの物理構造の影響を多大に受け、プローブを所望の配線に電気的に接触させるためには、膨大な攻撃コストを要する。後者の近傍電磁界を用いる方法では、測定ノイズの影響から、信頼性の高いデータを一回の測定で得ることは困難である。こういった理由から、プロービング攻撃は現実の脅威として考えられることはほとんどなかった。特に、複数のプローブを用いて複数ビットを同時に入手できる攻撃者の存在は、暗号理論研究では想定されていたものの、実システムでの安全性評価指標の条件として扱われることはなかった。しかしながら、例えば、IC チップの欠陥解析技術として利用されているレーザーを用いた LVP（レーザーボルテージプロービング）や電子線を用いた EBP（電子線プロービング）といったプロービング技術は、非接触で内部信号をモニタできるため、プロービング攻撃に転用されうる。また、最新の攻撃研究では、レーザー照射時のフォールト発生確率を暗号解析技術と融合することで、非接触でのレーザープロービングの精度と効率を高めることに成功している。プロービング攻撃は目の前にある脅威となっている。

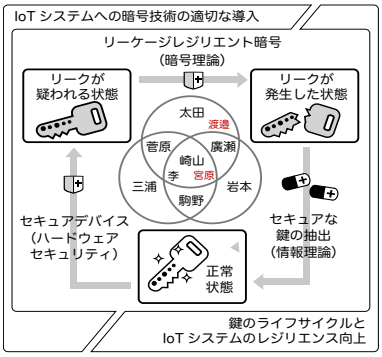
２．研究の目的

IoT システムにおいて高いレジリエンスを実現するには、IoT デバイスに暗号機能を適切に搭載し、膨大な数の IoT デバイスの安全性をリアルタイムに監視・評価できる機構が不可欠である。本研究では、IoT デバイスにおける暗号鍵の危殆化の変化に着目し、攻撃者との攻防によるデバイスの安全性の状態遷移をエコシステムと見なす。そして、プロービング攻撃の理解と対策技術の確立における理論的・実験的な考察を発展させ、IoT エコシステムにおける新たな暗号方式やより厳格な安全性評価の実現に寄与することを目的とする。そのために、暗号回路及び暗号処理を行うソフトウェアを含む IoT デバイスに対するプロービング攻撃の脅威と現状の安全性評価項目を整理した上で、最新のテクノロジーを考慮した攻撃者能力を想定し、新たな安全性評価のためのシナリオ及び対策プロトコルを構築する。具体的な取り組みとして、次の二つの課題を設定し、ハードウェアセキュリティ、暗号理論及び情報理論といった学術分野から生まれた最先端の研究成果を有機的に繋げ、本研究課題の解決の突破口とする。

【課題１：IoT システムへの暗号技術の適切な導入】　産業制御システムの IoT 化では、システムが大規模であるほど IoT デバイスの数は膨大になり、情報を分散的に集約処理するエッジ端末の担う役割が、システム性能とセキュリティの両面で重要となる。この階層的なシステム構成では、IoT デバイスの計算能力は低く、一方で、エッジ端末の計算能力は高いことを想定している。エッジ端末が、外部攻撃者の踏み台となった場合、その計算能力の高さから IoT システムに与える被害は深刻となる。しかし、エッジ端末のセキュリティレベルを高くすると、計算能力の低い IoT デバイスは、セキュリティレベルを整合させるための一定のコスト増を許容しなければならない。そこで本課題では、この種の議論を定量的かつ高精度に進められる設計指標を定義し、IoT デバイスのプロービング攻撃耐性の強化を図るとともに、デバイスの安全性の状態をリアルタイムにセンシングし、エッジ端末及び IoT システムにその状態を通知するセキュアデバイス技術の設計手法を確立する。

【課題２：鍵のライフサイクルと IoT システムのレジリエンス向上】　暗号回路を搭載したデバイスが常時ネットワークに接続されている IoT システムを仮設し、攻撃対象と攻撃者の物理的制約を強く意識しつつ、理論及び実践研究を進める。主に、攻撃モデルの想定から算出される漏洩情報量と社会が被る経済的損失が研究でのパラメータであるが、さらにレジリエンスを追加で考慮する。例えば、攻撃の検知後に、個々のデバイスが自動的に鍵を消去するような攻撃対策も考えられるが、レジリエント IoT システムでは端末の自律的な判断は必ずしも良い選択とはならない。本課題では、システム全体のレジリエンスを優先し、漏洩情報量が基準値を超えたことが明らかとなった場合でも、危殆化した IoT デバイスの機能を無効化せず、被害がシステム全体に広がらないよう攻撃者が得た情報を無効化できるようなシステムレベルでの対策を考える。

３．研究の方法



右図は研究体制である。３チームの役割は以下の通りである。**渡邉**及び**宮原**は、本研究課題との適格性が高く、研究を加速するべく、それぞれ R2.4 及び R4.3 に研究分担者に加えた。

（**チーム三浦**：**駒野**、**菅原**、**李**、**崎山**）　レジリエント IoT システムから求められる要求仕様を、リーケージセンサに反映させるための実装方法論を検討し、センサの設計配置自動化の実現性を明らかにする。また、計算資源の乏しい IoT デバイスにおいても、高いリーケージレジリエンスに繋がるプロービング攻撃対策が実現できるかについて明らかにする。現実的な条件下での実装と評価を通じて、IoT デバイスの攻撃耐性とコストのトレードオフを定量的に議論し、リーケージセンサ導入のメリット（デメリット）を解明する。最終的には、複数の物理攻撃対策を備えた網羅的なライブラリの構築や、暗号回路の耐タンパー性評価手法を確立し、これらを安全性評価手法と一体化することで、現実世界で担保できる安全性の限界を明らかにする。

（**チーム太田**：**菅原**、**渡邉**、**廣瀬**、**崎山**）　システムのレジリエンスを高める上では、たとえある程度の情報漏洩があったとしても安全に運用できる方式が必要である。実現に向けて、まずは暗号実装を構成する論理回路やメモリなどの部品から生じる情報漏洩を定性的・定量的に評価するとともに、安全性証明において利用できる形式的モデルとして抽象化する。次に、形式的モデルに基づき、情報漏洩を発生させる暗号実装を部品として用い、証明可能安全性を有する認証暗号や暗号利用モードの方式を考案し、モデル化と証明可能安全性における攻撃耐性とコストのトレードオフを明らかにし、対策技術の設計手法を構築する。

（**チーム岩本**：**廣瀬**、**駒野**、**宮原**、**崎山**）　漏洩情報をもとに、セキュアな鍵を抽出する技術は情報蒸留として知られている。本研究では、暗号化アルゴリズムや実際のプロービング攻撃を想定した情報漏洩のモデル化とともに、漏洩した情報を排除して新しい鍵を共有するための、より現実的な情報蒸留の理論や技術の現状と IoT システムでの実現性を明らかにする。研究代表者／分担者の具体的な役割は次の通りである。

崎山一男（**研究代表者**）は、本研究全体の統括を行い、レーザーフォールト攻撃及びプロービング攻撃の対策技術の構築に、物理レイヤーから暗号処理アルゴリズムに至るまで、総合的な視点を持って取り組み、情報漏洩の物理的・数理的理解を深める。【**課題１**：IoT **システムへの暗号技術の適切な導入**】における対策技術の実現性については**チーム三浦**が、情報漏洩対策の理論限界についてはチーム太田が議論を進め、**崎山**は研究分野間の橋渡し役を担う。【**課題２**：**鍵のライフサイクルと** IoT **システムのレジリエンス**】では、**チーム太田**と**チーム岩本**が進める IoT システムのレジリエンスに繋がる理論的対策技術に対して、実際の IoT システムに対応する物理パラメータを導入する。いずれの課題においても、新たな知見を体系化し、暗号工学、集積回路工学及び IoT セキュリティにわたる新研究課題の創出と各分野の発展を目指す。

太田和夫（**研究分担者**）は、IoT システムの文脈に即した公開鍵と秘密鍵の管理に着目し、情報漏洩を考慮した暗号プロトコルの提案とその証明可能安全性について研究する。また、理論研究の統括者として、**廣瀬**、**駒野**、**岩本**及び**渡邉**の進める研究成果をまとめ、リーケージレジリエント暗号を拡張し、IoT 時代の新たな研究分野として体系化を図る。

廣瀬勝一（**研究分担者**）は、暗号実装から生じる情報漏洩の形式的モデルを構築し、それらのモデル上で安全な認証暗号などの暗号利用モードの設計と安全性証明を研究する。モデルの構築においては、情報漏洩の物理的メカニズムを証明可能安全性のために抽象化する。鍵情報の漏洩が致命的となる前に、新たな鍵に交換するリキー方式に基づき、ハッシュ関数、認証暗号などの暗号利用モードの設計を行う。物理的な観測による情報漏洩への対策は、処理効率の観点から非常にコストが高いため、有望と考えられる実装方式を仮定し、設計改善に繋げる。

岩本貢（**研究分担者**）は、情報理論的な観点から漏洩情報量を理論的に推定し、定量化する。鍵情報が漏洩した場合の対策として、セキュアな鍵の抽出という高速かつ精度の高い定量化技術の確立が求められる研究に挑み、リキー方式とは異なる発想でシステムのレジリエンス向上にアプローチする。得られた知見は、リーケージレジリエント暗号をはじめとした暗号プロトコルの理論設計にフィードバックするとともに、**チーム三浦**のメンバーとして、理論・実装研究それぞれ単体では達成できない精度を有するリーケージセンサの実現を狙う。

駒野雄一（**研究分担者**）は、リキーを行うことで暗号通信時の情報漏洩を最小限に抑える通信方式に関して、計算リソースが限られた IoT デバイスに搭載する上での課題を定義して解決することで、システムレベルでの漏洩耐性向上に繋げる。さらに、秘密鍵を動的に生成する PUF（物理的複製困難関数）技術を利用して、IoT デバイスを保護する上での暗号応用システムの課題を定義し解決する。

三浦典之（**研究分担者**）は、情報漏洩を最小限に抑えることができる IC チップの設計と攻撃評価環境の構築を担う。安全性評価における実測データをこれまでのアナログ回路研究で培った知識と融合し、本研究課題の目的に即した対策技術の最適設計手法を構築する。**チーム三浦**では、暗号アルゴリズムと回路技術の間にある抽象度のギャップを過不足なく埋め、セキュアで効率の良い IoT デバイスの構築を目指す。

菅原健（**研究分担者**）は、トランジスタ、演算器、マイクロアーキテクチャ及びソフトウェアの

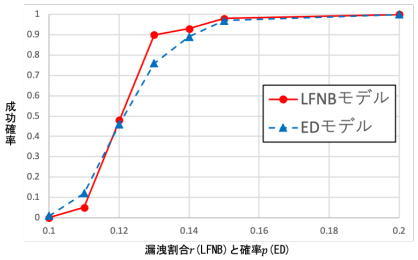
各レイヤーで発生する情報漏洩とその物理的メカニズムを解明する。さらに、それらを形式的モデルとして抽象化することで、**チーム太田**が進める暗号プリミティブレベルでの対策に繋げる。また、実装の側面から攻撃のシナリオを構築し、現実の IoT システムと照らし合わせ、レジリエンス評価技術に資する本質的な課題を定義し解決する。また、トランジスタ及び論理ゲートレベルの情報漏洩が、演算器及びマイクロアーキテクチャに与える影響を明らかにする。
李陽（**研究分担者**）は、IoT デバイスに対する新しい安全性評価技術の確立に取り組む。具体的には、深層学習を用いたサイドチャネル情報の解析能力の向上と、デバイスの並列計算における情報漏洩特性を考慮したデータ解析アルゴリズムの開発に注力する。また、ベルギーKU Leuven との国際共同研究では、M&M 技術で対策された AES 暗号ハードウェアに対して物理攻撃による安全性評価を行い、理論的安全性に基づくデバイスの開発を推進する。
渡邉洋平（R2.4 **から研究分担者**）は、高機能暗号の観点からのリーケージレジリエント暗号の検討及び情報理論的観点からの情報漏洩とリキー方式の検討を行う。特に、任意の文字列を公開鍵として利用可能な公開鍵暗号である ID ベース暗号を重点的に研究し、マスター秘密鍵が漏洩した場合でも一定の安全性を保証可能な方式を提案し、鍵更新機能を実現する効率的な構成及び量子計算機に耐性のある構成を提案する。
宮原大輝（R4.3 **から研究分担者**）は、**チーム岩本**における**崎山**と**岩本**の境界研究である物理的暗号におけるプロトコルの開発を行う。特に、本研究課題でも重要視してきた物理仮定の定式化について道具を使った暗号の観点から定義し、新たな研究分野の開拓に繋げる。

４．研究成果
研究計画調書において提案した研究計画については、全て予定通りの研究成果が得られた。評価 IC チップは、予定していたリーケージセンサ回路（レーザープロービングセンサとダイレクトプロービングセンサ）に加え、当初計画にはなかった理論的安全性に基づく M&M 技術を用いた AES 暗号回路を試作した（KU Leuven との国際共同研究）。以下、リーケージレジリエント暗号（リーク耐性暗号）、セキュアな鍵の抽出（リーク鍵の蒸留）及びセキュアデバイス（リーク検知技術）の三つの研究テーマについて得られた研究成果を説明する。

(1) **リーケージレジリエント暗号（リーク耐性暗号）の研究成果**　証明可能安全で効率の良い技術の検討を行い、レジリエント IoT システムを実現する暗号プロトコルの構築を通じて、本研究の目指すリーケージレジリエント暗号の社会実装に向けた理解を深めた。また、IoT システムにも適用可能な効率性とリーケージレジリエンスを両立するため、鍵を更新することで定期的にリーケージレジリエンスを初期化できるようにする ID ベース暗号について重点的に研究を行った。代表的な鍵更新可能な IBE である鍵隔離 IBE について、既存方式とほぼ同等な効率性と高い安全性を達成する鍵隔離 IBE 方式を新たに提案し、学術論文誌 Designs, Codes and Cryptography に採択された。次に、鍵更新に加えて効率的な鍵失効が可能な鍵失効可能 IBE について研究を行い、高い効率性と安全性を両立する方式の提案が、学術論文誌 Theoretical Computer Science に採択された。また、効率性を重視した鍵更新可能暗号である鍵更新可能公開鍵暗号について、既存方式の安全性解析を行い、その構成が不十分であることを指摘し、新たな構成の提案を行った。成果は国内会議 SCIS2023 で発表した。これらの知見を基に、リーケージレジリエンスと鍵更新機能を両立するリーク耐性暗号として、漏洩耐性鍵隔離暗号を新たに定式化し、効率的な構成法を体系化することができた。また、機密性と改竄検知を同時に提供する認証暗号について、誤用と物理的な情報漏洩を防ぐ方式を設計することができた。特に、サイドチャネル攻撃による情報漏洩に対する耐性を有する暗号利用モードを構成し国内研究会で発表した。また、ISO/IEC 国際標準軽量ハッシュ関数の一つである Lesamnta-LW に基づき、入力メッセージの暗号化に用いる秘密鍵を頻繁に更新することにより情報漏洩への耐性を実現し、国際会議 ICISC2019 で発表した。また、Lesamnta-LW に基づく MAC（メッセージ認証コード）関数を構成する暗号利用モードでは、従来の２倍の効率を達成でき、国際会議 ACNS2020 や学術論文誌 IEICE Trans. Fundamentals の掲載に繋がった。物理的情報漏洩メカニズムの解明に資する実験・評価環境を構築することができ、その結果、暗号ハードウェア分野における最高水準の学術論文誌 IACR Trans. CHES に採択された。情報漏洩の評価実験の結果は、理論研究にフィードバックした。プロービング攻撃における物理的情報漏洩メカニズムを解明し、CPU で生じるビット非独立なサイドチャネルリークの原因を究明し、国際会議 PROOFS2021 で発表した。

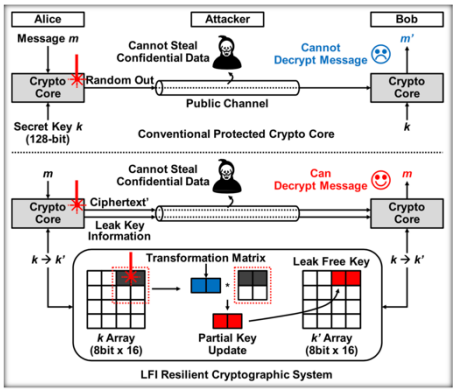
(2) **セキュアな鍵の抽出（リーク鍵の蒸留）の研究成果**　情報漏洩に関する理論的研究のうち、マルチーパーティ計算の実現例として、トランプのカードを用いた暗号（カードベース暗号）やキャンディーのペッツを用いた研究に取り組み、成果を多く得ることができた。特に、暗号理論分野のトップ会議である TCC2019 にペッツ研究の成果が採択されたことは特筆に値する。この成果は、国際会議 IWSEC2019 の Best Poster Award と情報セキュリティ研究奨励賞受賞に繋がった。カードベース暗号では、ハイパースペクトルカメラでカード組の物理的仮定を検証する実証実験を行い、プロトコルによって情報漏洩に差が生じることを国際会議 SecITC2022 で発表した。他にも、フランス Clermont Auvergne 大との国際共同研究を進め、国際会議論文 TAMC などで発表した。漏洩情報量の測定に関する研究では、AES 暗号アルゴリズムの鍵スケジューリングがプロービング攻撃を受けた場合について、正確に見積もることができた。鍵の各ビットが確率

$1-p$で消失する ED モデル（右図の青プロット）では、$p=0.15$で鍵がほぼ完全に復元できることが分かった。また、鍵の漏洩割合を仮定する LFNB モデル（右図の赤プロット）の場合、$r \geq 0.13$でほぼ確率 1 で鍵が復元できる一方で、$r \leq 0.11$で成功確率がほぼ 0 となることを解明した。成果は国内会議 SCIS2020、SCIS2021 及び国際会議 ISITA2020 で発表した。暗号利用モードの安全性証明に関しては、模倣可能性と呼ばれる物理的な情報漏洩の形式的モデルについて、その簡略化を検討し、評価を進めた。また、リークした暗号鍵の更新に必要となるリキー方式を新規に設計し、学術論文誌 Applied Science に採択された。リキー方式の実装面での安全性に関して、方式によって高次サイドチャネル攻撃への耐性が異なること（リキーしたとしても耐性が無い場合があること）を理論的に確認できた。

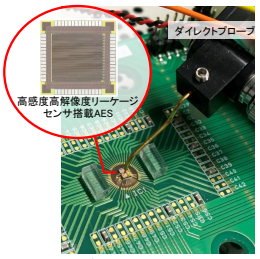


各モデルにおける漏洩割合及び確率に対する攻撃成功確率

(3) セキュアデバイス（リーク検知技術）の研究成果
リーケージセンサを搭載した AES 暗号プロセッサを実現し、物理攻撃が IC チップ基板に及ぼす影響を詳細に解析することができ、固体素子分野の世界最高峰の学術論文誌に採択された。また、物理的なプロービング攻撃を検知するリーケージセンサを新たに開発し、ダイレクトプローブを正しく検知できることを実機実証した。さらに、このダイレクトプロービングセンサと前身の基課題にて開発したレーザープロービングセンサを統合し、AES 暗号ハードウェアに実装した。これにより、IC チップの表面・裏面の両面からの攻撃を検知できる対策版 AES 暗号ハードウェアを実現して、安全性評価を行った。また、物理攻撃の検知後に能動的に暗号ハードウェアの動作モードを切り替えることで、セキュリティ耐性を向上するセンスアンドリアクト技術を開発し、電源遮断、自己破壊、鍵更新方式を含むリアクト機能をそれぞれ集積した AES 暗号ハードウェアを開発して、セキュリティ耐性を評価した。特に、鍵更新方式の技術の発展形として、リーケージセンサの空間解像度を利用した軽量な部分鍵更新方式を考案し、その実現可能性を評価した。この部分鍵更新方式は、研究チーム全体の技術的な議論の中で高度化されたもので、事前共有乱数を利用することで、サーバと情報通信する IoT 端末側のハードウェアオーバーヘッドを軽量化できる実用的技術に発展させた。PUF ベース暗号応用については、物理解析が困難な秘密鍵を効率よく生成する PUF を用いた新たな手法を学術論文誌 Security and Communication Networks で発表した。本研究は、ベルギーKU Leuven の Verbauwhede 教授との国際共同研究によるものである。さらに、PUF を用いて物理的解析に困難な秘密鍵を効率よく生成する技術と、PUF を用いた小型端末向けの機器認証技術を研究し、国際会議 SecITC2022 で発表した。模擬 IoT システムの構築については、Amazon の商用 IoT プラットフォーム（AWS IoT）を利用し、機器へのサイドチャネル攻撃がシステムのセキュリティに与える影響の安全性評価を行うことができ、国内研究会で発表した。さらに、IoT デバイスに対する新しい安全性評価技術の確立においては、深層学習を利用したサイドチャネル解析環境を構築し、学術論文誌に採択された。また、並列計算の情報漏洩特性を利用してノイズ軽減する解析手法を AsianHOST2021 で提案し、学術論文誌 IEICE Trans. Fundamentals に採択された。

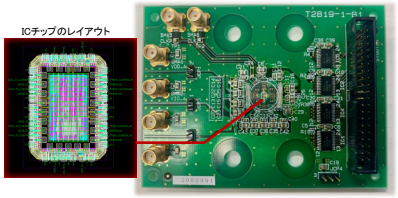


チーム岩本／三浦によるリーケージレジリエント暗号システム



プロービング攻撃の実証実験

(4) 当初に予見していなかった新たな展開等によって得られた研究成果　KU Leuven の Rijmen 教授（AES 暗号アルゴリズムの開発者の一人）と Nikova 教授（物理攻撃対策 TI 技術の開発者）の研究チームは、M&M とよばれる理論的な安全性に基づく物理攻撃対策を 2019 年に提案した。**崎山**と**三浦**は、M&M 技術が本研究課題のリーケージセンサと相補的な関係にあると判断し、AES 暗号を評価する IC チップを追加で実装することにした。修士学生一名が KU Leuven に R4.9 から一ヶ月間短期留学し、安全性評価を完了した。他にも、新しい PUF 研究として、多くの IoT 機器に搭載されている LED に注目し、その発光スペクトルから非侵襲で個体識別する手法を提案した。リーク耐性暗号研究については、漏洩耐性の程度と効率性の間のトレードオフに関する知見を検索可能暗号に応用することで、新たな研究成果が得られた。国際会議 CODASPY2022 や国内会議で発表し、CSS2019 と CSS2020 で**渡邉**が奨励賞を受賞している。公開鍵型の方式についても既存方式より優れた安全性や効率性を達成し、国際会議 ProvSec2022 で発表し Best Paper Award を受賞した。ハッシュ関数の安全性評価についても、SHA-256 への代数的故障利用解析で、先行研究と比較して少ない故障注入で入力を復元できた。IoT デバイスの安全性評価においては、オシロスコープを使わずに電力サイドチャネル情報を収集する技術を開発し、IEICE 全国大会で学生奨励賞を受賞した。



M&M技術を用いたAES暗号ハードウェアの評価用基板

５．主な発表論文等

〔雑誌論文〕　計73件（うち査読付論文　69件／うち国際共著　8件／うちオープンアクセス　27件）

１．著者名 Samuel Hand, Alexander Koch, Pascal Lafourcade, Daiki Miyahara and Leo Robert	４．巻 LNCS
２．論文標題 Check Alternating Patterns: A Physical Zero-Knowledge Proof for Moon-or-Sun	５．発行年 2023年
３．雑誌名 Proc. IWSEC 2023 (Lecture Notes in Computer Science)	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） なし	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 該当する

１．著者名 ABE Yoshiki、NAKAI Takeshi、WATANABE Yohei、IWAMOTO Mitsugu、OHTA Kazuo	４．巻 E106.A
２．論文標題 A Computationally Efficient Card-Based Majority Voting Protocol with Fewer Cards in the Private Model	５．発行年 2023年
３．雑誌名 IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	６．最初と最後の頁 315-324
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transfun.2022CIP0021	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 WATANABE Yohei、NAKAI Takeshi、OHARA Kazuma、NOJIMA Takuya、LIU Yexuan、IWAMOTO Mitsugu、OHTA Kazuo	４．巻 E105.A
２．論文標題 How to Make a Secure Index for Searchable Symmetric Encryption, Revisited	５．発行年 2022年
３．雑誌名 IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	６．最初と最後の頁 1559-1577
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transfun.2021EAP1163	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 Nakai Takeshi、Shirouchi Satoshi、Tokushige Yuuki、Iwamoto Mitsugu、Ohta Kazuo	４．巻 40
２．論文標題 Secure Computation for Threshold Functions with Physical Cards: Power of Private Permutations	５．発行年 2022年
３．雑誌名 New Generation Computing	６．最初と最後の頁 95-113
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/s00354-022-00153-7	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 Abe Yoshiki、Nakai Takeshi、Kuroki Yoshihisa、Suzuki Shinnosuke、Koga Yuta、Watanabe Yohei、Iwamoto Mitsugu、Ohta Kazuo	4．巻 40
2．論文標題 Efficient Card-Based Majority Voting Protocols	5．発行年 2022年
3．雑誌名 New Generation Computing	6．最初と最後の頁 173-198
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/s00354-022-00161-7	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 Yohei Watanabe, Kazuma Ohara, Mitsugu Iwamoto, and Kazuo Ohta	4．巻 -
2．論文標題 Efficient Dynamic Searchable Encryption with Forward Privacy under the Decent Leakage	5．発行年 2022年
3．雑誌名 Proc. ACM CODASPY 2022	6．最初と最後の頁 312-323
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 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 Kyoichi Asano, Keita Emura, Atsushi Takayasu, and Yohei Watanabe	4．巻 LNCS13600
2．論文標題 A Generic Construction of CCA-secure Attribute-based Encryption with Equality Test	5．発行年 2022年
3．雑誌名 Proc. ProvSec 2022 (Lecture Notes in Computer Science)	6．最初と最後の頁 3-19
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-031-20917-8_1	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 Anastasiia Doi, Toimoki Ono, Takeshi Nakai, Kazumasa Shinagawa, Yohei Watanabe, Koji Nuida, and Mitsugu Iwamoto	4．巻 -
2．論文標題 Card-based Cryptographic Protocols for Private Set Intersection	5．発行年 2023年
3．雑誌名 Proc. ISITA 2022	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） なし	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 Seiya Shimizu, Takeshi Nakai, Yohei Watanabe, and Mitsugu Iwamoto	4．巻 -
2．論文標題 An Improvement of Multi-Party Private Set Intersection Based on Oblivious Programmable PRFs	5．発行年 2023年
3．雑誌名 Proc. ISITA 2022	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） なし	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 Keita Emura, Ryoma Ito, Sachiko Kanamori, Ryo Nojima, and Yohei Watanabe	4．巻 -
2．論文標題 State-free End-to-End Encrypted Storage and Chat Systems based on Searchable Encryption	5．発行年 2022年
3．雑誌名 Proc. ICEIS 2022	6．最初と最後の頁 312-323
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/0011045200003179	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 Yuichi Komano and Takaaki Mizuki	4．巻 LNCS 13809
2．論文標題 Card-Based Zero-Knowledge Proof Protocol for Pancake Sorting	5．発行年 2023年
3．雑誌名 Proc. SecITC 2022 (Lecture Notes in Computer Science)	6．最初と最後の頁 222-239
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-031-32636-3_13	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 Yuichi Komano, Mitsugu Iwamoto, Kazuo Ohta, and Kazuo Sakiyama	4．巻 LNCS13809
2．論文標題 Lightweight Authentication Using Noisy Key Derived from Physically Unclonable Function	5．発行年 2023年
3．雑誌名 Proc. SecITC 2022 (Lecture Notes in Computer Science)	6．最初と最後の頁 203-221
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-031-32636-3_12	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 Yuichi Komano and Takaaki Mizuki	4．巻 LNCS13620
2．論文標題 Physical Zero-knowledge Proof Protocol for Topswops	5．発行年 2022年
3．雑誌名 Proc. ISPEC 2022 (Lecture Notes in Computer Science)	6．最初と最後の頁 537_553
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-031-21280-2_30	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 三浦 典之	4．巻 16(3)
2．論文標題 情報空間と物理空間をつなぐ集積システムのカタチ	5．発行年 2023年
3．雑誌名 電子情報通信学会 Fundamentals Review	6．最初と最後の頁 147-155
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/essfr.16.3_147	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 Leo Robert, Daiki Miyahara, Pascal Lafourcade, and Takaaki Mizuki	4．巻 LNCS13571
2．論文標題 Hide a_Liar: Card-Based ZKP Protocol for_Usowan	5．発行年 2023年
3．雑誌名 Proc. TAMC 2022 (Lecture Notes in Computer Science)	6．最初と最後の頁 201-217
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-031-20350-3_17	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 該当する

1．著者名 Daiki Miyahara andTakaaki Mizuki	4．巻 LNCS13461
2．論文標題 Secure Computations Through Checking Suits of_Playing Cards	5．発行年 2023年
3．雑誌名 Proc. IJTCS-FAW 2022 (Lecture Notes in Computer Science)	6．最初と最後の頁 110-128
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-031-20796-9_9	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 L_o Robert, Daiki Miyahara, Pascal Lafourcade, and Takaaki Mizuki	4．巻 LNCS13751
2．論文標題 Card-Based ZKP Protocol for_Nurimisaki	5．発行年 2022年
3．雑誌名 Proc. SSS 2022 (Lecture Notes in Computer Science)	6．最初と最後の頁 285-298
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-031-21017-4_19	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 該当する

1．著者名 Masahisa Shimano, Kazuo Sakiyama, and Daiki Miyahara	4．巻 LNCS13809
2．論文標題 Towards Verifying Physical Assumption in Card-Based Cryptography	5．発行年 2023年
3．雑誌名 Proc. SecITC 2022 (Lecture Notes in Computer Science)	6．最初と最後の頁 289-305
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-031-32636-3_17	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 Ryota Hira, Tomoaki Kitahara, Daiki Miyahara, Yuko Hara-Azumi, Yang Li, and Kazuo Sakiyama	4．巻 31
2．論文標題 Software Evaluation for Second Round Candidates in NIST Lightweight Cryptography	5．発行年 2023年
3．雑誌名 Journal of Information Processing	6．最初と最後の頁 205-219
掲載論文のDOI（デジタルオブジェクト識別子） 10.2197/ipsjjip.31.205	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 Tomoaki Kitahara, Ryota Hira, Yuko Hara-Azumi, Daiki Miyahara, Yang Li, and Kazuo Sakiyama	4．巻 -
2．論文標題 Optimized Software Implementations of Ascon, Grain-128AEAD, and TinyJambu on ARM Cortex-M	5．発行年 2022年
3．雑誌名 Proc. CANDARW 2022	6．最初と最後の頁 316-322
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/CANDARW57323.2022.00030	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 Tamon Asano and Takeshi Sugawara	4．巻 -
2．論文標題 Simulation Based Evaluation of Bit-Interaction Side-Channel	5．発行年 2023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） なし	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 花岡悟一郎，岩本貢，渡邉洋平，水木敬明，安部芳紀，品川和雅，新井美音，矢内直人	4．巻 J106-A
2．論文標題 高機能暗号の社会展開を促進する物理・視覚暗号	5．発行年 2023年
3．雑誌名 電子情報通信学会和文論文誌A	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） なし	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 藤聡子，土屋彩夏，李陽，崎山一男，菅原健	4．巻 62
2．論文標題 分光スペクトルを用いた調光機能のある白色LEDの個体識別	5．発行年 2021年
3．雑誌名 情報処理学会論文誌	6．最初と最後の頁 1549-1559
掲載論文のDOI（デジタルオブジェクト識別子） 10.20729/00212760	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 Daiki Miyahara, Yuichi Komano, Takaaki Mizuki, and Hideaki Sone	4．巻 -
2．論文標題 Cooking Cryptographers: Secure Multiparty Computation Based on Balls and Bags	5．発行年 2021年
3．雑誌名 Proc. of CSF 2021	6．最初と最後の頁 1-16
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/CSF51468.2021.00034	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 羽田野凌太，平田 遼，松田航平，三浦典之，李陽，崎山一男	4．巻 104-A(5)
2．論文標題 LFI検知回路に対するサイドチャネル攻撃耐性評価	5．発行年 2021年
3．雑誌名 電子情報通信学会論文誌(A)	6．最初と最後の頁 118-126
掲載論文のDOI（デジタルオブジェクト識別子） 10.14923/transfunj.2020JAP1023	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 Shoichi Hirose	4．巻 -
2．論文標題 Another Algebraic Decomposition Method for Masked Implementation	5．発行年 2021年
3．雑誌名 Proc. of AC3 2021	6．最初と最後の頁 105-114
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-80851-8_8	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 Shoichi Hirose, Yu Sasaki, and Hirotaka Yoshida	4．巻 E104-A(9)
2．論文標題 Update on Analysis of Lesamnta-LW and New PRF Mode LRF	5．発行年 2021年
3．雑誌名 IEICE Transactions on Fundamentals	6．最初と最後の頁 1304-1320
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transfun.2020EAP1109	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 Kazuki Nakamura, Koji Hori, and Shoichi Hirose	4．巻 12
2．論文標題 Algebraic Fault Analysis of SHA-256 Compression Function and Its Application	5．発行年 2021年
3．雑誌名 Information	6．最初と最後の頁 1-9
掲載論文のDOI（デジタルオブジェクト識別子） 10.3390/info12100433	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 Shoichi Hirose, Hidenori Kuwakado, and Hirotaka Yoshida	4．巻 E104-D(11)
2．論文標題 Provable-Security Analysis of Authenticated Encryption Based on Lesamnta-LW in the Ideal Cipher Model	5．発行年 2021年
3．雑誌名 IEICE Transactions on Information and Systems	6．最初と最後の頁 1894-1901
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transinf.2021NGP0008	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 Go TAKAMI, Takeshi SUGAWARA, Kazuo SAKIYAMA, and Yang LI	4．巻 E105-A(3)
2．論文標題 Mixture-Based 5-Round Physical Attack against AES: Attack Proposal and Noise Evaluation	5．発行年 2022年
3．雑誌名 IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	6．最初と最後の頁 289-299
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transfun.2021CIP0016	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 Yuichi Komano and Takaaki Mizuki	4．巻 -
2．論文標題 Coin-based Secure Computations	5．発行年 2022年
3．雑誌名 International Journal of Information Security	6．最初と最後の頁 1-14
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/s10207-022-00585-8	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 Takaaki Mizuki and Yuichi Komano	4．巻 -
2．論文標題 Information Leakage Due to Operative Errors in Card-based Protocols	5．発行年 2022年
3．雑誌名 Information and Computation	6．最初と最後の頁 1-15
掲載論文のDOI（デジタルオブジェクト識別子） 10.1016/j.ic.2022.104910	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 Kaoru Takemure, Yusuke Sakai, Bagus Santoso, Goichiro Hanaoka, and Kazuo Ohta	4．巻 E104-A(9)
2．論文標題 Achieving Pairing-Free Aggregate Signatures using Pre-Communication between Signers	5．発行年 2021年
3．雑誌名 IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	6．最初と最後の頁 1188-1205
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transfun.2020DMP0023	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 Keita Emura, Shuichi Katsumata, and Yohei Watanabe	4．巻 900
2．論文標題 Identity-Based Encryption with Security against the KGC: A Formal Model and Its Instantiations	5．発行年 2022年
3．雑誌名 Theoretical Computer Science	6．最初と最後の頁 97-119
掲載論文のDOI（デジタルオブジェクト識別子） 10.1016/j.tcs.2021.11.021	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 Keita Emura, Atsushi Takayasu, and Yohei Watanabe	4．巻 89(10)
2．論文標題 Efficient Identity-Based Encryption with Hierarchical Key-Insulation from HIBE	5．発行年 2021年
3．雑誌名 Designs, Codes and Cryptography	6．最初と最後の頁 2397-2431
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/s10623-021-00926-z	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 Keita Emura, Atsushi Takayasu, and Yohei Watanabe	4．巻 89(7)
2．論文標題 Adaptively Secure Revocable Hierarchical IBE from k-linear Assumption	5．発行年 2021年
3．雑誌名 Designs, Codes and Cryptography	6．最初と最後の頁 1535-1574
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/s10623-021-00880-w	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 Masahiro Ebina, Jumpei Mita, Junji Shikata, and Yohei Watanabe	4．巻 -
2．論文標題 Efficient Threshold Public Key Encryption from the Computational Bilinear Diffie-Hellman Assumption	5．発行年 2021年
3．雑誌名 Proc. of APKC 2021	6．最初と最後の頁 23-32
掲載論文のDOI（デジタルオブジェクト識別子） 10.1145/3457338.3458296	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 Sho Tada, Yuki Yamashita, Kohei Matsuda, Makoto Nagata, Kazuo Sakiyama, and Noriyuki Miura	4．巻 60
2．論文標題 Design and Concept Proof of an Inductive Impulse Self-Destructor in Sense-and-React Countermeasure Against Physical Attacks	5．発行年 2021年
3．雑誌名 Japanese Journal of Applied Physics (JJAP)	6．最初と最後の頁 SSBL01_1-8
掲載論文のDOI（デジタルオブジェクト識別子） 10.35848/1347-4065/abdf1f	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 八代理紗，堀洋平，片下敏宏，崎山一男	4．巻 61
2．論文標題 意図的なエラーを付与することによる深層学習を用いたArbiter PUFへのクローニング攻撃の対策	5．発行年 2020年
3．雑誌名 情報処理学会論文誌	6．最初と最後の頁 1871-1880
掲載論文のDOI（デジタルオブジェクト識別子） 10.20729/00208749	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 Atsushi Takayasu and Yohei Watanabe	4．巻 849
2．論文標題 Revocable Identity-based Encryption with Bounded Decryption Key Exposure Resistance: Lattice-based Construction and More	5．発行年 2021年
3．雑誌名 Theoretical Computer Science	6．最初と最後の頁 64-98
掲載論文のDOI（デジタルオブジェクト識別子） 10.1016/j.tcs.2020.10.010	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 Kaoru Takemure, Yusuke Sakai, Bagus Santoso, Goichiro Hanaoka, and Kazuo Ohta	4．巻 LNCS12505
2．論文標題 Achieving Pairing-Free Aggregate Signatures using Pre-Communication between Signers	5．発行年 2020年
3．雑誌名 Proc. of ProvSec 2020 (Lecture Notes in Computer Science)	6．最初と最後の頁 65-84
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-62576-4_4	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 該当する

1．著者名 Tomoki Uemura, Yohei Watanabe, Yang Li, Noriyuki Miura, Mitsugu Iwamoto, Kazuo Sakiyama, and Kazuo Ohta	4．巻 -
2．論文標題 A Key Recovery Algorithm Using Random Key Leakage from AES Key Schedule	5．発行年 2020年
3．雑誌名 Proc. of ISITA 2020	6．最初と最後の頁 382-386
掲載論文のDOI（デジタルオブジェクト識別子） 10.34385/proc.65.C01-10	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 Yoshiki Abe, Mitsugu Iwamoto, and Kazuo Ohta	4．巻 -
2．論文標題 How to Detect Malicious Behaviors in a Card-Based Majority Voting Protocol with Three Inputs	5．発行年 2020年
3．雑誌名 Proc. of ISITA 2020	6．最初と最後の頁 377-381
掲載論文のDOI（デジタルオブジェクト識別子） 10.34385/proc.65.C01-9	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 Shoichi Hirose, Yu Sasaki, and Hirotaka Yoshida	4．巻 LNCS12146
2．論文標題 Lesamnta-LW Revisited: Improved Security Analysis of Primitive and New PRF Mode	5．発行年 2020年
3．雑誌名 Proc. of ACNS 2020 (Lecture Notes in Computer Science)	6．最初と最後の頁 89-109
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-57808-4_5	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 Shoichi Hirose	4．巻 LNCS12570
2．論文標題 Compactly Committing Authenticated Encryption Using Tweakable Block Cipher	5．発行年 2020年
3．雑誌名 Proc. of NSS 2020 (Lecture Notes in Computer Science)	6．最初と最後の頁 187-206
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-65745-1_11	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 渡邉 洋平	4．巻 65(9)
2．論文標題 検索可能暗号:データベースシステムの安全な運用に向けて	5．発行年 2020年
3．雑誌名 ケミカルエンジニヤリング	6．最初と最後の頁 552-560
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 Takeshi Nakai, Yuto Misawa, Yuuki Tokushige, Mitsugu Iwamoto, and Kazuo Ohta	4．巻 39(1)
2．論文標題 How to Solve Millionaires' Problem with Two Kinds of Cards	5．発行年 2021年
3．雑誌名 New Gener. Comput.	6．最初と最後の頁 73-96
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/s00354-020-00118-8	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 Kazuo Sakiyama, Tatsuya, Fujii, Kohei Matsuda, and Noriyuki Miura	4．巻 -
2．論文標題 Flush Code Eraser: Fast Attack Response Invalidating Cryptographic Sensitive Data	5．発行年 2020年
3．雑誌名 IEEE Embedded Systems Letters	6．最初と最後の頁 4pages
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/LES.2019.2949788	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 Akiko Toh, Yang Li, Kazuo Sakiyama, and Takeshi Sugawara	4．巻 Volume 55, Issue 24
2．論文標題 Fingerprinting Light Emitting Diodes Using Spectrometer	5．発行年 2019年
3．雑誌名 IET Electronics Letters	6．最初と最後の頁 1295-1297
掲載論文のDOI（デジタルオブジェクト識別子） 10.1049/el.2019.1908	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 Takeshi Sugawara, Natsu Shoji, Kazuo Sakiyama, Kohei Matsuda, Noriyuki Miura, and Makoto Nagata	4．巻 Volume 90
2．論文標題 Side-Channel Leakage from Sensor-Based Countermeasures against Fault Injection Attack	5．発行年 2019年
3．雑誌名 Microelectronics Journal	6．最初と最後の頁 63-71
掲載論文のDOI（デジタルオブジェクト識別子） 10.1016/j.mejo.2019.05.017	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 Yuichi Komano, Hideo Shimizu, and Hideyuki Miyake	4．巻 Vol.27
2．論文標題 Integrative Acceleration of First-order Boolean Masking for Embedded IoT Devices	5．発行年 2019年
3．雑誌名 Journal of Information Processing	6．最初と最後の頁 585-592
掲載論文のDOI（デジタルオブジェクト識別子） 10.2197/ipsjjip.27.585	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 Kohei Matsuda, Sho Tada, Makoto Nagata, Yuichi Komano, Yang Li, Takeshi Sugawara, Mitsugu Iwamoto, Kazuo Ohta, Kazuo Sakiyama, Noriyuki Miura	4．巻 Vol.59
2．論文標題 An IC-Level Countermeasure Against Laser Fault Injection Attack By Information Leakage Sensing Based on Laser-Induced Opto-Electric Bulk Current Density	5．発行年 2020年
3．雑誌名 Japanese Journal of Applied Physics (JJAP)	6．最初と最後の頁 12pages
掲載論文のDOI（デジタルオブジェクト識別子） 10.7567/1347-4065/ab65d3	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 Kazuma Ohara, Yohei Watanabe, Mitsugu Iwamoto, and Kazuo Ohta	4．巻 102-A
2．論文標題 Multi-Party Computation for Modular Exponentiation based on Replicated Secret Sharing	5．発行年 2019年
3．雑誌名 IEICE Trans. on Fundamentals	6．最初と最後の頁 1079-1090
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transfun.E102.A.1079	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 Kazuma Ohara, Keita Emura, Goichiro Hanaoka, Ai Ishida, Kazuo Ohta, and Yusuke Sakai	4．巻 102-A
2．論文標題 Shortening the Libert-Peters-Yung Revocable Group Signature Scheme by Using the Random Oracle Methodology	5．発行年 2019年
3．雑誌名 IEICE Trans. on Fundamentals	6．最初と最後の頁 1101-1117
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transfun.E102.A.1101	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 菅原健	4．巻 103巻1号
2．論文標題 サイドチャネル攻撃と対策	5．発行年 2020年
3．雑誌名 電子情報通信学会誌	6．最初と最後の頁 45-50
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 菅原健，崎山一男	4．巻 47巻7号
2．論文標題 組込機器のセキュリティを脅かすレーザーフォールト攻撃	5．発行年 2019年
3．雑誌名 レーザー研究	6．最初と最後の頁 305-309
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 Reo Eriguchi, Noboru Kunihiro, and Mitsugu Iwamoto	4．巻 -
2．論文標題 Optimal Multiple Assignment Schemes Using Ideal Multipartite Secret Sharing Schemes	5．発行年 2019年
3．雑誌名 Proc. IEEE International Symposium on Information Theory (ISIT2019)	6．最初と最後の頁 3047-3051
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/ISIT.2019.8849591	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 Kohei Matsuda, Sho Tada, Makoto Nagata, Yang Li, Takeshi Sugawara, Mitsugu Iwamoto, Kazuo Ohta, Kazuo Sakiyama, Noriyuki Miura	4．巻 -
2．論文標題 An Information Leakage Sensor Based on Measurement of Laser-Induced Opto-Electric Bulk Current Density	5．発行年 2019年
3．雑誌名 Extended Abstracts of International Conference on Solid State Devices and Materials (SSDM)	6．最初と最後の頁 501-502
掲載論文のDOI（デジタルオブジェクト識別子） 10.7567/1347-4065/ab65d3	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 Hakuei Sugimoto, Ryota Hatano, Natsu Shoji, and Kazuo Sakiyama	4．巻 LNCS12056
2．論文標題 Validating the DFA Attack Resistance of AES (Short Paper)	5．発行年 2020年
3．雑誌名 Proc. International Symposium on Foundations & Practice of Security (FPS2019) (Lecture Notes in Computer Science)	6．最初と最後の頁 371-378
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-45371-8_25	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 Yang Li, Ryota Hatano, Sho Tada, Kohei Matsuda, Noriyuki Miura, Takeshi Sugawara, and Kazuo Sakiyama,	4．巻 LNCS12020
2．論文標題 Side-Channel Leakage of Alarm Signal for a Bulk-Current-Based Laser Sensor	5．発行年 2020年
3．雑誌名 Proc. International Conference on Information Security and Cryptology (Inscrypt2019) (Lecture Notes in Computer Science)	6．最初と最後の頁 346-361
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-42921-8_20	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 Shoichi Hirose, Hidenori Kuwakado and Hirotaka Yoshida	4．巻 LNCS11975
2．論文標題 Authenticated Encryption Based on Lesamnta-LW Hashing Mode	5．発行年 2020年
3．雑誌名 Proc. International Conference on Information Security and Cryptology (ICISC 2019) (Lecture Notes in Computer Science)	6．最初と最後の頁 52-69
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-40921-0_3	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 Yoshiki Abe, Mitsugu Iwamoto, and Kazuo Ohta	4．巻 LNCS11891
2．論文標題 Efficient Private PEZ Protocols for Symmetric Functions	5．発行年 2019年
3．雑誌名 Proc. Theory of Cryptography Conference (TCC2019) (Lecture Notes in Computer Science)	6．最初と最後の頁 372-392
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-36030-6_15	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 Ryuga Matsumura, Takeshi Sugawara, and Kazuo Sakiyama	4．巻 -
2．論文標題 A Secure LiDAR with Side-channel Fingerprinting	5．発行年 2018年
3．雑誌名 Proc. International Symposium on Computing and Networking, CANDAR Workshops (CANDARW2018)	6．最初と最後の頁 479-482
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/CANDARW.2018.00092	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 Natsu Shoji, Takeshi Sugawara, Mitsugu Iwamoto, and Kazuo Sakiyama	4．巻 -
2．論文標題 An Abstraction Model for 1-bit Probing Attack on Block Ciphers	5．発行年 2019年
3．雑誌名 Proc. International Conference on Computer and Communication Systems (ICCCS2019)	6．最初と最後の頁 5 pages
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/CCOMS.2019.8821754	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 Yuichi Komano and Shoichi Hirose	４．巻 9(5), 1002
２．論文標題 Re-Keying Scheme Revisited: Security Model and Instantiations	５．発行年 2019年
３．雑誌名 Applied Sciences	６．最初と最後の頁 1-15
掲載論文のDOI（デジタルオブジェクト識別子） 10.3390/app9051002	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 Yuichi Komano, Kazuo Ohta, Kazuo Sakiyama, Mitsugu Iwamoto, and Ingrid Verbauwhede	４．巻 -
２．論文標題 Single-Round Pattern Matching Key Generation Using Physically Unclonable Function	５．発行年 2019年
３．雑誌名 Security and Communication Networks	６．最初と最後の頁 13 pages
掲載論文のDOI（デジタルオブジェクト識別子） 10.1155/2019/1719585	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 該当する

１．著者名 Kohei Matsuda, Tatsuya Fujii, Natsu Shoji, Takeshi Sugawara, Kazuo Sakiyama, Yu-ichi Hayashi, Makoto Nagata, and Noriyuki Miura	４．巻 Vol.53, No.11
２．論文標題 A 286 F2/Cell Distributed Bulk-Current Sensor and Secure Flush Code Eraser Against Laser Fault Injection Attack on Cryptographic Processor	５．発行年 2018年
３．雑誌名 IEEE Journal of Solid-State Circuits	６．最初と最後の頁 3174-3182
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/JSSC.2018.2869142	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 Takeshi Sugawara	４．巻 Volume 2019, Issue 1
２．論文標題 3-Share Threshold Implementation of AES S-box without Fresh Randomness	５．発行年 2019年
３．雑誌名 IACR Transactions on Cryptographic Hardware and Embedded Systems	６．最初と最後の頁 123-145
掲載論文のDOI（デジタルオブジェクト識別子） 10.13154/tches.v2019.i1.123-145	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 Takeshi Sugawara, Yang Li, and Kazuo Sakiyama	4．巻 -
2．論文標題 Probing Attack of Share-Serial Threshold Implementation of Advanced Encryption Standard	5．発行年 2019年
3．雑誌名 IET Electronics Letters	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） 10.1049/el.2018.7518	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 Zhiwei Yuan, Yang Li, Kazuo Sakiyama, Takeshi Sugawara, and Jian Wang	4．巻 LNCS11125
2．論文標題 Recovering Memory Access Sequence with Differential Flush+Reload Attack	5．発行年 2018年
3．雑誌名 Proc. International Conference on Information Security Practice and Experience (ISPEC2018) (Lecture Notes in Computer Science)	6．最初と最後の頁 424-439
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-319-99807-7_26	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 該当する

1．著者名 Yohei Watanabe, Yoshihisa Kuroki, Shinnosuke Suzuki, Yuta Koga, Mitsugu Iwamoto, and Kazuo Ohta	4．巻 -
2．論文標題 Card-Based Majority Voting Protocols with Three Inputs Using Three Cards	5．発行年 2018年
3．雑誌名 Proc. International Symposium on Information Theory and Its Applications (ISITA2018)	6．最初と最後の頁 218-222
掲載論文のDOI（デジタルオブジェクト識別子） 10.23919/ISITA.2018.8664324	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 Anjelina Espejel-Trujillo, Mitsugu Iwamoto, and Mariko Nakano-Miyatake	4．巻 77
2．論文標題 A Proactive Secret Image Sharing Scheme with Resistance to Machine Learning Based Steganalysis	5．発行年 2018年
3．雑誌名 Multimedia Tools And Applications	6．最初と最後の頁 15161-15179
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/s11042-017-5097-8	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 該当する

1．著者名 Jean-Luc Danger, Risa Yashiro, Tarik Graba, Yves Mathieu, Abdelmalek Si-Merabet, Kazuo Sakiyama, Noriyuki Miura, and Makoto Nagata	4．巻 -
2．論文標題 Analysis of Mixed PUF-TRNG Circuit Based on SR-Latches in FD-SOI Technology	5．発行年 2018年
3．雑誌名 Proc. 21st Euromicro Conference on Digital System Design (DSD2018)	6．最初と最後の頁 508-515
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/DSD.2018.00090	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 該当する

〔学会発表〕　計131件（うち招待講演　18件／うち国際学会　16件）

1．発表者名 安部 芳紀，岩本 貢，太田 和夫
2．発表標題 m値n入力関数を計算するprivate PEZプロトコルの初期文字列長の漸近評価
3．学会等名 暗号と情報セキュリティシンポジウム（SCIS）
4．発表年 2023年

1．発表者名 淺野 京一，渡邉 洋平
2．発表標題 CCA安全な鍵更新可能公開鍵暗号の安全性解析と効率的な一般的構成法
3．学会等名 暗号と情報セキュリティシンポジウム（SCIS）
4．発表年 2023年

1．発表者名 甘田 拓海，岩本 貢，渡邉 洋平
2．発表標題 効率的かつ安全な更新処理を備えた結果秘匿可能な検索可能暗号
3．学会等名 暗号と情報セキュリティシンポジウム（SCIS）
4．発表年 2023年

１．発表者名
岩成 慶太，小野 知樹，安倍 芳紀，中井 雄士，渡邉 洋平，岩本 貢

２．発表標題
秘匿置換を用いた効率的なトランプベース秘密計算プロトコル

３．学会等名
暗号と情報セキュリティシンポジウム（SCIS）

４．発表年
2023年

１．発表者名
内薗 駿，中井 雄士，渡邉 洋平，岩本 貢

２．発表標題
保証金が一定なビットコインベース宝くじプロトコルの拡張

３．学会等名
暗号と情報セキュリティシンポジウム（SCIS）

４．発表年
2023年

１．発表者名
小野 知樹，品川 和雅，中井 雄士，渡邉 洋平，岩本 貢

２．発表標題
任意の論理回路に対する1ゲートあたり6枚のカードベースプロトコル

３．学会等名
暗号と情報セキュリティシンポジウム（SCIS）

４．発表年
2023年

１．発表者名
杉本 航太，渡邉 洋平，岩本 貢

２．発表標題
Two Sheriffs Problemの一般化と鍵共有プロトコルへの応用

３．学会等名
暗号と情報セキュリティシンポジウム（SCIS）

４．発表年
2023年

１．発表者名
初貝 恭祐，渡邉 洋平，岩本 貢

２．発表標題
天体ショーに対する物理的ゼロ知識証明

３．学会等名
暗号と情報セキュリティシンポジウム（SCIS）

４．発表年
2023年

１．発表者名
土井 アナスタシヤ，小野 知樹，安部 芳紀，渡邉 洋平，岩本 貢

２．発表標題
カードを用いた秘匿和集合プロトコル

３．学会等名
コンピュータセキュリティシンポジウム(CSS)

４．発表年
2022年

１．発表者名
小野 知樹，中井 雄士，渡邉 洋平，岩本 貢

２．発表標題
任意のブール回路に対する秘匿操作を用いたカードベースプロトコル

３．学会等名
コンピュータセキュリティシンポジウム(CSS)

４．発表年
2022年

１．発表者名
甘田 拓海，岩本 貢，渡邉 洋平

２．発表標題
効率的かつ検索結果秘匿可能な動的検索可能暗号

３．学会等名
コンピュータセキュリティシンポジウム(CSS)

４．発表年
2022年

１．発表者名
淺野 京一，江村 恵太，高安 敦，渡邉 洋平

２．発表標題
CCA安全な平文一致確認可能属性ベース暗号の一般的構成

３．学会等名
コンピュータセキュリティシンポジウム(CSS)

４．発表年
2022年

１．発表者名
杉本 航太，中井 雄士，渡邉 洋平，岩本 貢

２．発表標題
攻撃成功確率からみたTwo Sheriffs Problem

３．学会等名
コンピュータセキュリティシンポジウム(CSS)

４．発表年
2022年

１．発表者名
渡邉 洋平

２．発表標題
Recent Progress in Searchable Encryption

３．学会等名
IMI共同利用研究集会 高度化する暗号技術と数学的技法の進展（招待講演）

４．発表年
2022年

１．発表者名
中村一貴，飯沼浩仁，廣瀬勝一

２．発表標題
ハッシュ関数SHA-1，SHA-256に基づくMAC関数への偽造攻撃を目的とした代数的故障利用解析

３．学会等名
暗号と情報セキュリティシンポジウム（SCIS）

４．発表年
2023年

１．発表者名
Shoichi Hirose and Kazuhiko Minematsu

２．発表標題
Compactly Committing Authenticated Encryption Using Encryptment and Tweakable Block Cipher

３．学会等名
IACR Cryptology ePrint Archive: Report 2022/1670（国際学会）

４．発表年
2022年

１．発表者名
駒野 雄一，水木 敬明

２．発表標題
Pancakeソーティングに対する物理的ゼロ知識証明

３．学会等名
コンピュータセキュリティシンポジウム(CSS)

４．発表年
2022年

１．発表者名
駒野 雄一，水木 敬明

２．発表標題
Topswopsの物理的ゼロ知識証明プロトコル

３．学会等名
マルチメディア、分散、協調とモバイル（DICOMO 2022 ）シンポジウム

４．発表年
2022年

１．発表者名
西澤慧悟 ，崎山一男，原祐子，李陽

２．発表標題
相互補助相関電力解析の正解鍵順位と鍵復元率の調査

３．学会等名
暗号と情報セキュリティシンポジウム（SCIS)

４．発表年
2023年

１．発表者名
Enhao Xu, Takeshi Sugawara, Kazuo Sakiyama, Yuko Hara-Azumi, and Yang Li

２．発表標題
Attention-Based Non-Profiled SCA on ASCAD Database

３．学会等名
暗号と情報セキュリティシンポジウム（SCIS）

４．発表年
2023年

１．発表者名
内山 一秀，李 陽

２．発表標題
SAKURA-GにおけるVITIセンサーの実装

３．学会等名
情報処理学会　全国大会

４．発表年
2023年

１．発表者名
吉田 深月，宮原 大輝，崎山 一男

２．発表標題
サイドチャネル攻撃と偽コイン問題の関連性

３．学会等名
電子情報通信学会ソサイエティ大会

４．発表年
2022年

１．発表者名
荻原 実那，李 陽，宮原 大輝，崎山 一男

２．発表標題
AES暗号に対する非プロファイリング深層学習攻撃の再現実験

３．学会等名
電子情報通信学会ソサイエティ大会

４．発表年
2022年

１．発表者名
佐藤 泰雅，古野 亨紀，平田 遼，宮原 大輝，崎山 一男

２．発表標題
TI技術を用いたAES S-boxの故障感度の評価

３．学会等名
電子情報通信学会ソサイエティ大会

４．発表年
2022年

１．発表者名
工藤 紗織，嶌野 雅久，宮原 大輝，崎山 一男

２．発表標題
ハイパースペクトルカメラを用いた指紋の付着時期推定

３．学会等名
電子情報通信学会ソサイエティ大会

４．発表年
2022年

１．発表者名
嶌野 雅久，崎山 一男，宮原 大輝

２．発表標題
カードベース暗号における物理仮定に対する脅威とその対策に関する検討

３．学会等名
コンピュータセキュリティシンポジウム(CSS)

４．発表年
2022年

１．発表者名
Haruka Hirata, Daiki Miyahara, Yang Li, and Kazuo Sakiyama

２．発表標題
Glitch-Based Key Recovery with Shannon Entropy on the Last AES Round

３．学会等名
Poster Session, CARDIS 2022（国際学会）

４．発表年
2022年

１．発表者名
佐藤 泰雅，古野 亨紀，平田 遼，宮原 大輝，李 陽，崎山 一男

２．発表標題
TI技術によりシェア化されたAES S-boxの故障感度解析手法

３．学会等名
暗号と情報セキュリティシンポジウム（SCIS）

４．発表年
2023年

１．発表者名
吉田 深月，金子 尚平，李 陽，崎山 一男，宮原 大輝

２．発表標題
天秤とコインを使った秘密計算

３．学会等名
暗号と情報セキュリティシンポジウム（SCIS）

４．発表年
2023年

１．発表者名
宮原大輝

２．発表標題
安全に証明する方法～ペンシルパズルを例に～

３．学会等名
IPSJ-ONE（招待講演）

４．発表年
2023年

１．発表者名
平賀幸仁，菅原健

２．発表標題
乱数の消費が少なく PINI を満たす 4 次マスキング

３．学会等名
暗号と情報セキュリティシンポジウム（SCIS）

４．発表年
2023年

１．発表者名
浅野多聞，菅原健

２．発表標題
誤り訂正符号によって生じるビット非独立なサイドチャネルリーク

３．学会等名
暗号と情報セキュリティシンポジウム（SCIS）

４．発表年
2023年

１．発表者名
根本昌也，浅野多聞，菅原健

２．発表標題
Romulus の TI 付きハードウェア実装と電力リークのシミュレーション評価

３．学会等名
ハードウェアセキュリティ研究会（HWS）

４．発表年
2023年

１．発表者名
Yuiko Matsubara, Daiki Miyahara, Yohei Watanabe, Mitsugu Iwamoto, and Kazuo Sakiyama

２．発表標題
Abstraction Model of Probing and DFA Attacks on Block Ciphers

３．学会等名
IACR Cryptology ePrint Archive: Report 2023/443（国際学会）

４．発表年
2023年

１．発表者名
T. Asano and T. Sugawara

２．発表標題
Simulation Based Evaluation of Bit-Interaction Side-Channel Leakage on RISC-V Processor

３．学会等名
PROOFS 2021（国際学会）

４．発表年
2021年

１．発表者名
浅野多聞，菅原健

２．発表標題
バレルシフタと加算器によるビット非独立なサイドチャネルリークの発生機序とその対策

３．学会等名
暗号と情報セキュリティシンポジウム（SCIS）

４．発表年
2022年

１．発表者名
平田遼，宮原大輝，李陽，三浦典之，崎山一男

２．発表標題
パイプライン化されたAES S-boxへのフォールト攻撃に対する安全性評価

３．学会等名
暗号と情報セキュリティシンポジウム（SCIS）

４．発表年
2022年

１．発表者名
塚原麻輝，平田遼，宮原大輝，李陽，崎山一男

２．発表標題
M&Mにより対策されたAES暗号ハードウェアの乱数依存性について

３．学会等名
暗号と情報セキュリティシンポジウム（SCIS）

４．発表年
2022年

１．発表者名
嶌野雅久，崎山一男，宮原大輝

２．発表標題
ハイパースペクトルカメラによるカードベース暗号の安全性評価に向けた基礎的検討

３．学会等名
暗号と情報セキュリティシンポジウム（SCIS）

４．発表年
2022年

１．発表者名
星野翔，嶋野裕一郎，崎山一男

２．発表標題
ローリングシャッター効果を用いた音声情報復元とその評価

３．学会等名
コンピュータセキュリティシンポジウム(CSS)

４．発表年
2021年

１．発表者名
嶋野裕一郎，星野翔，崎山一男

２．発表標題
ローリングシャッター方式のカメラを用いた音声情報の復元実験

３．学会等名
電子情報通信学会ソサイエティ大会

４．発表年
2021年

１．発表者名
塚原麻輝，平田遼，李陽，崎山一男

２．発表標題
M&Mにより対策されたAES暗号ハードウェアに対するt検定

３．学会等名
電子情報通信学会ソサイエティ大会

４．発表年
2021年

１．発表者名
古野亨紀，平田遼，李陽，崎山一男

２．発表標題
M&Mにより対策されたAES暗号ハードウェアへの故障利用解析に向けた基礎実験

３．学会等名
電子情報通信学会ソサイエティ大会

４．発表年
2021年

１．発表者名
高見豪，菅原健，崎山一男，李陽

２．発表標題
ミクスチャ差分を用いた暗号解析の LED64 への適用

３．学会等名
電子情報通信学会ソサイエティ大会

４．発表年
2021年

１．発表者名
加藤光，菅原健，崎山一男，李陽

２．発表標題
確率モデルと実験による増分故障解析の安全性評価

３．学会等名
暗号と情報セキュリティシンポジウム（SCIS）

４．発表年
2022年

１．発表者名
岩成 慶太，中井 雄士，渡邉 洋平，栃窪 孝也，岩本 貢

２．発表標題
一様で閉じたシャッフルの効率的な実装

３．学会等名
暗号と情報セキュリティシンポジウム（SCIS）

４．発表年
2022年

１．発表者名
淺野 京一，岩本 貢，渡邉 洋平

２．発表標題
効率的な漏洩耐性鍵隔離暗号

３．学会等名
暗号と情報セキュリティシンポジウム（SCIS）

４．発表年
2022年

１．発表者名
清水 聖也，中井 雄士，渡邉 洋平，岩本 貢

２．発表標題
出力埋め込み可能な紛失擬似ランダム関数に基づく多者間秘匿積集合プロトコルの効率化

３．学会等名
暗号と情報セキュリティシンポジウム（SCIS）

４．発表年
2022年

１．発表者名
植村 友紀，渡邉 洋平，李 陽，三浦 典之，岩本 貢，崎山 一男，太田 和夫

２．発表標題
プロービング攻撃による漏洩情報を用いたAES鍵復元アルゴリズムの改良

３．学会等名
暗号と情報セキュリティシンポジウム（SCIS）

４．発表年
2022年

１．発表者名
土井 アナスタシヤ，中井 雄士，品川 和雅，渡邉 洋平，岩本 貢

２．発表標題
カードを用いた秘匿共通集合プロトコル

３．学会等名
コンピュータセキュリティシンポジウム(CSS)

４．発表年
2021年

１．発表者名
淺野 京一，岩本 貢，渡邉 洋平

２．発表標題
秘密鍵の漏洩耐性を有する鍵隔離暗号

３．学会等名
コンピュータセキュリティシンポジウム(CSS)

４．発表年
2021年

１．発表者名
三浦典之

２．発表標題
[基調講演]サイバー空間とフィジカル空間の接点：集積システムのあるべきカタチ

３．学会等名
システムとLSIの設計技術研究発表会(デザインガイア2021)（招待講演）

４．発表年
2021年

１．発表者名
Noriyuki Miura

２．発表標題
Integrated Security Interface Against Cyber-Physical Attacks

３．学会等名
IEEE SSCS Japan Chapter/Seoul Chapter DL Technical Seminar（招待講演）（国際学会）

４．発表年
2021年

１．発表者名
Noriyuki Miura

２．発表標題
Integrated Sense-and-React Countermeasures Against Physical Attacks

３．学会等名
International Solid-State Circuits Conferecne (ISSCC)（招待講演）（国際学会）

４．発表年
2022年

１．発表者名
Sho Tada, Yuki Yamashita, Kohei Matsuda, Makoto Nagata, Kazuo Sakiyama, and Noriyuki Miura

２．発表標題
An Inductive Impulse Self-Destructor in Sense-and-React Countermeasure Against Physical Attacks

３．学会等名
International Conference on Solid State Devices and Materials (SSDM)（国際学会）

４．発表年
2020年

１．発表者名
Noriyuki Miura

２．発表標題
Tutorial: Integrated Security Interface Against Cyber-Physica Attacks

３．学会等名
Asian Solid-State Circuits Conference (A-SSCC)（招待講演）（国際学会）

４．発表年
2020年

１．発表者名
植村 友紀，渡邉 洋平，李 陽，三浦 典之，岩本 貢，崎山 一男，太田 和夫

２．発表標題
AES鍵スケジュールからの固定ビット数漏洩を用いた鍵復元アルゴリズムの性能評価

３．学会等名
暗号と情報セキュリティシンポジウム（SCIS）

４．発表年
2021年

１．発表者名
渡邉 洋平，大原 一真，岩本 貢，太田 和夫

２．発表標題
より少ない漏洩の下で安全な動的検索可能暗号への変換手法

３．学会等名
コンピュータセキュリティシンポジウム（CSS）

４．発表年
2020年

１．発表者名
根岸 奎人，渡邉 洋平，岩本 貢

２．発表標題
視覚復号型秘密分散法における任意の改ざんを検知する手法

３．学会等名
暗号と情報セキュリティシンポジウム（SCIS）

４．発表年
2021年

１．発表者名
初貝 恭祐，安部 芳紀，中井 雄士，品川 和雅，渡邉 洋平，岩本 貢

２．発表標題
時間ドロボー問題に対する健全性誤りのない物理的ゼロ知識証明

３．学会等名
暗号と情報セキュリティシンポジウム（SCIS）

４．発表年
2021年

１．発表者名
中井 雄士，徳重 佑樹，岩本 貢，太田 和夫

２．発表標題
秘匿置換を用いたカードベースしきい値関数プロトコル

３．学会等名
暗号と情報セキュリティシンポジウム（SCIS）

４．発表年
2021年

１．発表者名
安部 芳紀，岩本 貢，太田 和夫

２．発表標題
対称関数を効率的に計算するPrivate PEZ プロトコル（from TCC 2019）

３．学会等名
電子情報通信学会情報セキュリティ研究会（ISEC）（招待講演）

４．発表年
2020年

１．発表者名
石田真，菅原健

２．発表標題
IoT クラウドサービスに対するローカル攻撃の安全性評価に関する研究

３．学会等名
ハードウェアセキュリティ研究会（HWS）

４．発表年
2021年

１．発表者名
須藤嵩，菅原健

２．発表標題
樹脂へのホログラム転写によるチップ移植攻撃への対策

３．学会等名
電子情報通信学会ハードウェアセキュリティ研究会（HWS）

４．発表年
2021年

１．発表者名
浅野多聞，菅原健

２．発表標題
ALU内部のビット非独立なリーケージのシミュレーション評価

３．学会等名
暗号と情報セキュリティシンポジウム（SCIS）

４．発表年
2021年

１．発表者名
菅原健，李陽，﨑山一男

２．発表標題
シェアシリアル型 Threshold Implementation へのプロービング攻撃

３．学会等名
電子情報通信学会ハードウェアセキュリティ研究会（HWS）

４．発表年
2020年

１．発表者名
Koji Hori and Shoichi Hirose

２．発表標題
Evaluation of an Algebraic Fault Attack on the SHA-256 Compression Function

３．学会等名
The 15th International Workshop on Security (IWSEC)

４．発表年
2020年

１．発表者名
廣瀬勝一

２．発表標題
マスキングを行う実装のための代数的分解法について

３．学会等名
暗号と情報セキュリティシンポジウム（SCIS）

４．発表年
2021年

１．発表者名
堀弘二，廣瀬勝一

２．発表標題
SHA-256圧縮関数に対する代数的故障利用解析とその応用について

３．学会等名
暗号と情報セキュリティシンポジウム（SCIS）

４．発表年
2021年

１．発表者名
工藤黎，菅原健，崎山一男，原祐子，李陽

２．発表標題
サイドチャネル攻撃の並列実装におけるシステムノイズの評価：遺伝的アルゴリズムとの比較

３．学会等名
暗号と情報セキュリティシンポジウム（SCIS）

４．発表年
2021年

１．発表者名
Go Takatoi, Takeshi Sugawara, Kazuo Sakiyama, Yuko Hara-Azumi, and Yang Li

２．発表標題
Pushing the Limits of Simple Electromagnetic Analysis Against Similar Activation Functions

３．学会等名
暗号と情報セキュリティシンポジウム（SCIS）

４．発表年
2021年

１．発表者名
星野翔，崎山一男

２．発表標題
ローリングシャッター効果を用いたLEDデバイスの物理指紋抽出に関する基礎的実験

３．学会等名
暗号と情報セキュリティシンポジウム（SCIS）

４．発表年
2021年

１．発表者名
畑碧，崎山一男

２．発表標題
塗布剤による個人情報の秘匿性評価

３．学会等名
暗号と情報セキュリティシンポジウム（SCIS）

４．発表年
2021年

１．発表者名
平田遼，羽田野凌太，李陽，三浦典之，崎山一男

２．発表標題
M&Mにより対策されたAES暗号ハードウェアに対するサイドチャネル攻撃

３．学会等名
暗号と情報セキュリティシンポジウム（SCIS）

４．発表年
2021年

１．発表者名
平田遼，羽田野凌太，李陽，三浦典之，Svetla Nikova，崎山一男

２．発表標題
M&Mにより対策されたAESハードウェアの安全性評価について

３．学会等名
電子情報通信学会ソサイエティ大会

４．発表年
2020年

１．発表者名
駒野 雄一，水木 敬明

２．発表標題
コインベースプロトコルの初期配置誤りに関する考察

３．学会等名
コンピュータセキュリティシンポジウム（CSS）

４．発表年
2020年

１．発表者名
土屋彩夏，藤聡子，李陽，崎山一男，菅原健

２．発表標題
LED の個体識別における温度変化の影響

３．学会等名
IEICE 情報通信 システムセキュリティ研究専門委員会・第 50 回合同研究会

４．発表年
2020年

１．発表者名
山下憂記，松田航平，永田真，三浦典之

２．発表標題
暗号回路における基板電流検出型レーザー故障注入攻撃対策の軽量設計法

３．学会等名
電子情報通信学会ハードウェアセキュリティ研究会

４．発表年
2020年

１．発表者名
多田捷，松田航平，永田真，_山一男，三浦典之

２．発表標題
誘導インパルス型の瞬時自己破壊回路を利用した検知後対処に基づく物理攻撃対策

３．学会等名
電子情報通信学会ハードウェアセキュリティ研究会

４．発表年
2020年

１．発表者名
植村友紀，李陽，三浦典之，岩本貢，崎山一男，太田和夫

２．発表標題
鍵のランダムな漏洩に対するAES鍵スケジュール復元アルゴリズム

３．学会等名
暗号と情報セキュリティシンポジウム（SCIS）2020

４．発表年
2020年

１．発表者名
竹牟禮薫，坂井祐介，Bagus Santoso，花岡悟一郎，太田和夫

２．発表標題
事前通信モデルにおけるペアリングを用いない集約署名

３．学会等名
暗号と情報セキュリティシンポジウム（SCIS）2020

４．発表年
2020年

１．発表者名
品川和雅，三浦典之，岩本貢，崎山一男，太田和夫

２．発表標題
気泡検出器を用いたゼロ知識非破壊検査

３．学会等名
暗号と情報セキュリティシンポジウム（SCIS）2020

４．発表年
2020年

１．発表者名
安部芳紀，岩本貢，太田和夫

２．発表標題
任意の始集合を持つ関数を計算するprivate PEZプロトコル

３．学会等名
暗号と情報セキュリティシンポジウム（SCIS）2020

４．発表年
2020年

１．発表者名
高見豪，菅原健，崎山一男，李陽

２．発表標題
AESへの5ラウンドの物理攻撃の可能性の考察

３．学会等名
暗号と情報セキュリティシンポジウム（SCIS）2020

４．発表年
2020年

１．発表者名
杉本悠馬，菅原健，崎山一男，李陽

２．発表標題
無線通信から収集した電磁波を用いたテンプレート攻撃研究

３．学会等名
暗号と情報セキュリティシンポジウム（SCIS）2020

４．発表年
2020年

１．発表者名
駒野雄一，廣瀬勝一

２．発表標題
Re-keying方式の高次サイドチャネル攻撃への耐性に関する検討

３．学会等名
暗号と情報セキュリティシンポジウム（SCIS）2020

４．発表年
2020年

１．発表者名
藤聡子，土屋彩夏，李陽，崎山一男，菅原健

２．発表標題
調光機能のあるLEDの個体識別

３．学会等名
暗号と情報セキュリティシンポジウム（SCIS）2020

４．発表年
2020年

１．発表者名
羽田野凌太，平田遼，松田航平，三浦典之，李陽，崎山一男

２．発表標題
レーザー検知回路から漏洩するサイドチャ ネル情報の考察

３．学会等名
暗号と情報セキュリティシンポジウム（SCIS）2020

４．発表年
2020年

１．発表者名
安部芳紀，岩本貢，太田和夫

２．発表標題
任意の関数を計算するprivate PEZプロトコルの改善

３．学会等名
コンピューターセキュリティシンポジウム 2019（CSS 2019）

４．発表年
2019年

１．発表者名
渡邉洋平，大原一真，岩本貢，太田和夫_

２．発表標題
(強)フォワード安全な動的検索可能暗号の効率的な構成

３．学会等名
コンピューターセキュリティシンポジウム 2019（CSS 2019）

４．発表年
2019年

１．発表者名
Yoshiki Abe, Mitsugu Iwamoto, and Kazuo Ohta

２．発表標題
How to improve the private PEZ protocol for general functions

３．学会等名
International Workshop on Security（IWSEC2019）（国際学会）

４．発表年
2019年

１．発表者名
松田航平

２．発表標題
小型・低電力セキュアモジュールのための暗号回路と物理攻撃対策の軽量実装に関する研究

３．学会等名
電子情報通信学会集積回路研究会（招待講演）

４．発表年
2020年

１．発表者名
土屋彩夏，藤聡子，李陽，崎山一男，菅原健

２．発表標題
積分球による光量の均一化に基づくLEDの個体識別

３．学会等名
IEICE2019年ソサイエティ大会

４．発表年
2019年

１．発表者名
高見豪，菅原健，崎山一男，李陽

２．発表標題
AESに対する5ラウンド攻撃の物理攻撃への応用検討

３．学会等名
IEICE2019年ソサイエティ大会

４．発表年
2019年

１．発表者名
羽田野凌太，李陽，多田捷，松田航平，三浦典之，菅原健，崎山一男

２．発表標題
レーザーフォールト注入攻撃への対 策が施された AES 暗号チップの脆弱性評価

３．学会等名
IEICE2019年ソサイエティ大会

４．発表年
2019年

１．発表者名
椎名瞭，菅原健，松村竜我，崎山一男

２．発表標題
LED 光源を用いた光サイドチャネル認証装置

３．学会等名
IEICE2019年ソサイエティ大会

４．発表年
2019年

１．発表者名
杉本博英，羽田野凌太，庄司奈津，崎山一男

２．発表標題
AES 暗号への 9 ラウンド差分故障解析の攻撃耐性の評価

３．学会等名
IEICE2019年ソサイエティ大会

４．発表年
2019年

１．発表者名
星野翔，椎名瞭，松村竜我，崎山一男

２．発表標題
レーザー光を使った音情報の漏洩に対する安全性評価

３．学会等名
IEICE2019年ソサイエティ大会

４．発表年
2019年

１．発表者名
Kazuo Ohta

２．発表標題
Card-based Majority Voting Protocols with Three Inputs Using Three Cards

３．学会等名
nternational Secure Multi-party Computation Forum (SMPS2019)（招待講演）（国際学会）

４．発表年
2019年

１．発表者名
Kazuo Sakiyama

２．発表標題
Invited Talk: Deep Learning for Security Evaluation of Physically Unclonable Function

３．学会等名
ECTI UEC Workshop on AI and Application (ECTI-UEC2019)（招待講演）（国際学会）

４．発表年
2019年

１．発表者名
駒野雄一

２．発表標題
PUF出力からのID／暗号鍵の再現法

３．学会等名
第2回PUF技術シンポジウム（招待講演）

４．発表年
2019年

１．発表者名
羽田野凌太，庄司奈津，李陽，菅原健，崎山一男

２．発表標題
AES暗号への故障差分攻撃のモデル化と攻撃回数の評価

３．学会等名
IEICE2018年ソサイエティ大会

４．発表年
2018年

１．発表者名
Kazuo Sakiyama

２．発表標題
Keynote: Hardware Security and IoT Ecosystem

３．学会等名
International Conference on Advanced Computing and Applications (ACOMP2018)（招待講演）（国際学会）

４．発表年
2018年

１．発表者名
Kazuo Sakiyama

２．発表標題
Anti-tamper cryptographic hardware with analog electronics

３．学会等名
Mini Symposium: Crypto for long-term security and privacy（招待講演）

４．発表年
2019年

１．発表者名
Kazuo Sakiyama

２．発表標題
Keynote: Towards Resilient IoT System - How to Evaluate Information Leakage

３．学会等名
The First International Workshop on Hardware Oriented Cybersecurity (HwSec2018)（招待講演）（国際学会）

４．発表年
2018年

１．発表者名
Ryota Hatano and Kazuo Sakiyama

２．発表標題
An Abstraction Model for Differential Fault Analysis on AES

３．学会等名
The First International Workshop on Hardware Oriented Cybersecurity (HwSec2019)（国際学会）

４．発表年
2018年

１．発表者名
Shoji Natsu and Kazuo Sakiyama

２．発表標題
Modeling 1-bit Probing Attack on Block Ciphers

３．学会等名
The First International Workshop on Hardware Oriented Cybersecurity (HwSec2020)（国際学会）

４．発表年
2018年

１．発表者名
堀越健太郎，崎山一男

２．発表標題
ハイパースペクトルカメラを用いた液晶ディスプレイの個体差に関する基礎的研究

３．学会等名
暗号と情報セキュリティシンポジウム（SCIS2019）

４．発表年
2018年

１．発表者名
八代理紗，藤聡子，菅原健，崎山一男

２．発表標題
Arbiter PUFへのサイドチャネルモデリング攻撃の実装と応用

３．学会等名
IEICE2018年ソサイエティ大会

４．発表年
2018年

１．発表者名
八代理紗，菅原健，崎山一男

２．発表標題
Arbiter PUFに対する攻撃手法に関する一考察

３．学会等名
情報処理学会 DAシンポジウム2018（特別セッション）（招待講演）

４．発表年
2018年

１．発表者名
駒野雄一、清水秀夫、三宅秀享

２．発表標題
IoT端末へのサイドチャネル攻撃の脅威評価～攻撃環境の変遷と対策技術の展望～

３．学会等名
暗号と情報セキュリティシンポジウム（SCIS2019）

４．発表年
2019年

１．発表者名
松田航平，藤井達哉，庄司奈津，菅原健，崎山一男，林優一，永田真，三浦典之

２．発表標題
基板電流センサと電源瞬断回路を利用した小面積レーザーフォールト注入攻撃対策

３．学会等名
電子情報通信学会 ハードウェアセキュリティ研究会

４．発表年
2018年

１．発表者名
松田航平，藤井達哉，庄司奈津，菅原健，崎山一男，林優一，永田真，三浦典之

２．発表標題
レーザー故障注入攻撃対策を備えた暗号ICの設計手法

３．学会等名
情報処理学会 DAシンポジウム2018（特別セッション）

４．発表年
2018年

１．発表者名
松田航平，永田真，三浦典之

２．発表標題
PRINCEファミリ暗号プロセッサの超軽量実装

３．学会等名
電子情報通信学会 ハードウェアセキュリティ研究会

４．発表年
2019年

１．発表者名
藤聡子，李陽，崎山一男，菅原健

２．発表標題
分光スペクトルを用いたLEDの個体識別における電流変化の影響

３．学会等名
暗号と情報セキュリティシンポジウム（SCIS2019）

４．発表年
2019年

１．発表者名
藤聡子，李陽，崎山一男，菅原健

２．発表標題
分光スペクトルを用いたLEDの個体識別における電流変化の影響

３．学会等名
サイバーセキュリティシンポジウム道後2019（ＳＥＣ道後2019学生研究賞受賞研究発表会）（招待講演）

４．発表年
2019年

１．発表者名
菅原健

２．発表標題
Changing of the Guards の一般化

３．学会等名
暗号と情報セキュリティシンポジウム (SCIS2019)

４．発表年
2019年

１．発表者名
藤聡子，李陽，崎山一男，菅原健

２．発表標題
分光器を用いたLEDの個体識別に向けた基礎的研究

３．学会等名
IEICE2018年ソサイエティ大会

４．発表年
2018年

１．発表者名
Erina Tatsumi, Kazuo Sakiyama, and Takeshi Sugawara

２．発表標題
A Case Study of Row Hammer under Different Refresh Rates

３．学会等名
The 13th International Workshop on Security (IWSEC2018)（国際学会）

４．発表年
2018年

１．発表者名
Yang Li, Natsu Shoji, Takeshi Sugawara, Kazuo Sakiyama

２．発表標題
Investigation of Information Leakage from A Laser Fault Injection Sensor

３．学会等名
IEICE2019年総合大会

４．発表年
2019年

１．発表者名
伊藤駿輔，菅原健，崎山一男，李陽

２．発表標題
AESの指定したラウンド間差分の平文探索アルゴリズムの改良

３．学会等名
IEICE2018年ソサイエティ大会

４．発表年
2018年

１．発表者名
廣瀬勝一，菅原健，駒野雄一

２．発表標題
サイドチャネル攻撃への耐性を有する認証暗号方式について

３．学会等名
電子情報通信学会 情報セキュリティ研究会

４．発表年
2019年

１．発表者名
岩本貢

２．発表標題
秘密計算の安全性～プライバシーを保ちつつどこまで計算できるか

３．学会等名
第8回バイオメトリクスと認識・認証シンポジウム(SBRA)（招待講演）

４．発表年
2018年

１．発表者名
太田和夫

２．発表標題
現代暗号研究の事始め ～ 1つのケーススタディ ～

３．学会等名
情報理論・情報セキュリティ・ワイドバンドシステム合同研究会（招待講演）

４．発表年
2019年

１．発表者名
安部 芳紀，山本 翔太，岩本 貢，太田 和夫

２．発表標題
初期文字列が29 文字の4 入力多数決Private PEZプロトコル

３．学会等名
情報理論・情報セキュリティ・ワイドバンドシステム合同研究会

４．発表年
2019年

１．発表者名
渡邉洋平，岩本貢，太田 和夫

２．発表標題
効率的でフォワード安全な動的検索可能暗号

３．学会等名
暗号と情報セキュリティシンポジウム（SCIS2019）

４．発表年
2019年

１．発表者名
安部 芳紀，山本 翔太，岩本 貢，太田 和夫

２．発表標題
不正検知可能な3入力多数決カードプロトコル

３．学会等名
暗号と情報セキュリティシンポジウム（SCIS2019）

４．発表年
2019年

１．発表者名
山本 翔太，安部 芳紀，岩本 貢，太田 和夫

２．発表標題
4入力多数決を計算する効率的なPrivate PEZプロトコル

３．学会等名
暗号と情報セキュリティシンポジウム（SCIS2019）

４．発表年
2019年

１．発表者名
Wenjia Wang, Yoshiki Abe, Mitsugu Iwamoto, and Kazuo Ohta,

２．発表標題
Three-Party Private Set Operation Protocols Using Polynomials and OPPRF

３．学会等名
暗号と情報セキュリティシンポジウム（SCIS2019）

４．発表年
2019年

１．発表者名
江利口礼央，國廣昇，岩本貢

２．発表標題
いくつかの理想的な秘密分散法を用いた最適な複数割り当て法

３．学会等名
情報理論とその応用シンポジウム（SITA2018）

４．発表年
2018年

１．発表者名
Bagus Santoso and Kazuo Ohta

２．発表標題
Another Look at One-More Discrete Logarithm Problem in Generic Model

３．学会等名
暗号と情報セキュリティシンポジウム（SCIS2019）

４．発表年
2019年

〔図書〕　計6件

1．著者名 Kazuo Sakiyama and Yang Li	4．発行年 2024年
2．出版社 Springer	5．総ページ数 -
3．書名 “Fault Sensitivity Analysis,” Chapter in Sushil Jajodia, Pierangela Samarati, and Moti Yung editors, Encyclopedia of Cryptography, Security and Privacy, Third Edition	

1．著者名 太田 和夫，岩本 貢，渡邉 洋平（取材協力）	4．発行年 2021年
2．出版社 Newton Press	5．総ページ数 28
3．書名 ニュートン別冊　数学の世界 現代編 増補第2版，暗号 個人情報を守る数学	

1．著者名 Takeshi Nakai	4．発行年 2021年
2．出版社 The University of Electro-Communications	5．総ページ数 96
3．書名 PRIVATE PERMUTATIONS IN CARD-BASED CRYPTOGRAPHY	

1．著者名 崎山一男	4．発行年 2019年
2．出版社 電子情報通信学会	5．総ページ数 9
3．書名 電子情報通信学会 知識ベース 1群（信号・システム）- 3編（暗号理論）-14章（サイドチャネル攻撃と耐タンパー技術）	

１．著者名 松田航平	４．発行年 2020年
２．出版社 神戸大学学位論文	５．総ページ数 89
３．書名 小型・低電力セキュアモジュールのための暗号回路と物理攻撃対策の軽量実装に関する研究	

１．著者名 崎山一男，菅原健，李陽	４．発行年 2019年
２．出版社 コロナ社	５．総ページ数 174
３．書名 暗号ハードウェアのセキュリティ	

〔産業財産権〕

〔その他〕

研究業績一覧
https://sakiyama-lab.jp/study/

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
研究分担者	廣瀬　勝一 (Hirose Shoichi) (20228836)	福井大学・学術研究院工学系部門・教授 (13401)	

6．研究組織（つづき）

	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
研究分担者	李　陽 (Li Yang) (20821812)	電気通信大学・大学院情報理工学研究科・准教授 (12612)	
研究分担者	宮原　大輝 (Miyahara Daiki) (20928288)	電気通信大学・大学院情報理工学研究科・助教 (12612)	
研究分担者	渡邉　洋平 (Watanabe Yohei) (40792263)	電気通信大学・大学院情報理工学研究科・助教 (12612)	
研究分担者	岩本　貢 (Iwamoto Mitsugu) (50377016)	電気通信大学・大学院情報理工学研究科・教授 (12612)	
研究分担者	駒野　雄一 (Komano Yuichi) (50393856)	株式会社東芝研究開発センター・その他部局等・主任研究員 (92705)	
研究分担者	菅原　健 (Sugawara Takeshi) (60785236)	電気通信大学・大学院情報理工学研究科・准教授 (12612)	
研究分担者	三浦　典之 (Miura Noriyuki) (70650555)	大阪大学・情報科学研究科・教授 (14401)	
研究分担者	太田　和夫 (Ohta Kazuo) (80333491)	電気通信大学・大学院情報理工学研究科・特命教授 (12612)	

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			
フランス	Clermont Auvergne大			
ベルギー	KU Leuven			
オランダ	Radboud University			
フランス	Telecom ParisTech			
ベトナム	Le Quy Don Technical University			