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　 ７ 日現在

機関番号：３４３１５
研究種目：基盤研究(A)（一般）
研究期間：2020～2023
課題番号：２０Ｈ００５９０

研究課題名（和文）スケーラブルな物理セキュリティを可能にする近似計算の設計基盤と理論の構築

研究課題名（英文）Design Framework and Theory for Scalable Hardware Security Enabled by Approximate Computing

研究代表者

冨山　宏之（Tomiyama, Hiroyuki）

立命館大学・理工学部・教授

研究者番号：８０３６２２９２

交付決定額（研究期間全体）：（直接経費）　　34,500,000円

研究成果の概要（和文）：サイドチャネル攻撃に強いIoTデバイスを設計するための技術と理論を開発した。IoTデバイスはコスト制約が厳しいことを念頭に、攻撃対策に要するコストとその対策によって得られるセキュリティとのトレードオフ最適化や、セキュリティのスケーラビリティに焦点を当てた。スケーラブルな物理セキュリティを実現するための手段として近似計算に着目し、本研究を通じて、近似演算回路、近似演算回路を活用する高位合成、高位合成における設計空間探索、乱数生成の近似、低コストな攻撃対策などについて、新たな設計手法および理論を開発した。開発した手法の有効性を、シミュレーション、FPGA、カスタム設計により評価した。

研究成果の学術的意義や社会的意義
IoT（Internet of Things）とは、さまざまなモノ（デバイス）をインターネットに接続することで高度なサービスを実現する技術であり、世界中で普及が進んでいる。一方で、IoTデバイスは現場に設置される性質上、サイドチャネル攻撃などの物理攻撃にさらされやすい。しかし、多くのIoTデバイスは小型で安価であるため、セキュリティ対策に許容されるコストは厳しく制限されている。本研究では、安全なIoTデバイスを設計するための技術と理論を開発した。本研究により、物理攻撃に対して堅牢なIoTデバイスを低コストで実現することが可能となる。

研究成果の概要（英文）：We developed techniques and theories for designing IoT devices resistant to side-channel attacks. Considering the severe cost constraints of IoT devices, we focused on optimizing the trade-off between the cost of countermeasures and the security they provide, as well as the scalability of these security measures. To achieve scalable hardware security, we leveraged approximate computing. Through this research, we developed numerous new design methods and theories related to approximate arithmetic circuits, high-level synthesis utilizing approximate arithmetic circuits, design space exploration in high-level synthesis, approximate random number generation, and low-cost attack countermeasures. The effectiveness of these methods was evaluated through simulations, FPGA implementations, and custom designs.

研究分野：計算機システム

キーワード：Approximate Computing　物理セキュリティ　IoT

様　式　Ｃ－１９、Ｆ－１９－１（共通）

１．研究開始当初の背景

Society 5.0 はサイバー空間とフィジカル空間を高度に融合させたシステムにより実現さる。そこでは Internet of Things（IoT、モノのインターネット）により人とモノが繋がることで従来の情報社会では不十分だった情報の共有が可能になり、高度なサービスが提供される。センサやアクチュエータを制御する IoT デバイスはサイバー空間とフィジカル空間のインタフェースであり、家庭、オフィス、工場、農場など、ユーザの現場（フィールド）に設置される。その性質上、IoT デバイスはサイドチャネル攻撃などの物理的なセキュリティ攻撃を受ける危険性が高い。ここでサイドチャネル攻撃とは、入力に対する応答時間、デバイスが消費する電力、デバイスが発生する電磁波などの物理情報（サイドチャネル情報）を観測し、統計処理を施すことにより、デバイス内部の秘密情報（例えば、暗号鍵）を取得する攻撃手法の総称である。安心安全な Society 5.0 を実現するためには、IoT デバイスの物理セキュリティへの対策が不可欠である。一方、IoT デバイスは多種多様であり、セキュリティ対策に許容されるコストや、要求されるセキュリティレベルが大きく異なる。

２．研究の目的

上述のように、IoT デバイスは、フィールドに設置される性質上、サイドチャネル攻撃などの物理攻撃にさらされやすい。一方、IoT デバイスは多種多様であり、セキュリティ対策に許容されるコストもさまざまである。そこで本研究では、IoT デバイスを対象として、スケーラブルな物理セキュリティを実現する設計基盤と理論の構築を目的とする。この目的を達成するため、近似計算（Approximate Computing）技術を物理セキュリティに応用する。近似計算とは、計算の精度を犠牲にすることにより、高性能化や低消費電力化を実現する技術である。従来、1 ビットの計算誤差も許されない暗号アルゴリズムなどのセキュリティ対策には、近似計算は適していないと考えられてきた。本研究は、従来の発想を大きく転換し、サイドチャネル攻撃への対策に近似計算を応用する。これにより、セキュリティの実装コストと安全性をトレードオフでき、多種多様な IoT デバイスを、それぞれ許容されるコストで保護することを可能にする。

３．研究の方法

上述の目的を達成するため、専門分野の異なる 7 名の研究者が協力して本研究に取り組んだ。安全な IoT デバイス／システムを実現するためには、暗号分野で培われた理論と計算機システム分野で体系化された設計技術が、一方でも欠かすことのできない両輪である。なぜなら、理論的な完全性を追求すると設計が非現実的になり、逆に理論的な裏付けを欠く設計は安全でないためである。そこで、応用暗号学の専門家と IoT 設計技術の専門家の両者が参画した。ここで、単に設計技術と言っても、ソフトウェア設計、回路の高位設計、論理設計、物理設計など、多くのレイヤから構成される。安全な IoT デバイス／システムを実現するためには、すべてのレイヤを包括することが非常に重要である。そこで、IoT 設計技術の各レイヤの専門家が本研究に参画した。

7 名の研究者が、スケーラブルな物理セキュリティを可能にする近似演算回路、物理セキュリティ強度要求に応じた回路の自動合成技術、スケーラブルな物理セキュリティに関する安全性指標の理論をサブテーマとする 3 つのグループに分かれて研究を実施することを基本としつつ、臨機応変にグループの境界を越えて連携することによりサブテーマ間の境界領域に取り組んだ。

４．研究成果

研究期間を通じ、IoT 回路の高位設計、論理設計、物理設計、ならびに、理論について、多くの成果を挙げることができた。以下、主要な成果を記載する。なお、以下の成果のいくつかは、スケーラブルな物理セキュリティを実現する手段として近似計算を用いているわけではないが、いずれもスケーラブルな物理セキュリティの実現という目標を達成する重要な成果である。

(1) 可変精度近似演算器と高位合成

可変精度近似加算器を開発した。開発した加算器は、被加数と加数に加え、演算精度を制御するための入力を有している。この入力値により、精度と消費電力のトレードオフが可能となる。すなわち、より正確な加算を行うためには大きな消費電力が必要であり、消費電力を抑えるためには誤差が大きくなる。既存の可変精度近似加算器は、符号なし加算については期待通りの振る舞いを行っていたが、負の数に対しては精度と消費電力のトレードオフが乱れることを発見した。そこで、可変精度近似加算器に符号の誤り訂正を導入することにより、上記の問題点を解決した。

FPGA を対象として、32 ビットの可変精度近似乗算器を開発した。多くの FPGA は内部に DSP ブロックを有しており、その DSP ブロックで乗算を行うことができる。しかし、1 個の DSP ブロックで計算可能な乗算のビット数は限られており、現在広く普及している FPGA の場合、32 ビットの乗算を行うためには 4 個の DSP ブロックを用いて 4 個の部分積を求め、その

後、部分積を加算する。この加算の際に可変精度近似加算器を用いることで、32 ビットの可変精度近似乗算器を構成した。これにより、FPGA における乗算についても、精度と消費電力・性能のトレードオフが可能となった。

さらに、可変精度近似演算器を活用する高位合成技術を開発した。高位合成とは、C 言語などのプログラミング言語により記述されたソフトウェアからハードウェア回路を自動的に合成する技術であり、近年では産業界の実設計でも広く利用されている。開発した高位合成技術は、時間制約と資源制約の下で、出力の計算誤差が最小となる回路を自動合成する（図 1 参照）。プログラム中の各乗算について、近似して良いか、あるいは正確に計算すべきかを自動的に決定する。

上記の可変精度近似演算器、ならびに可変精度近似演算器を活用する高位合成技術は物理セキュリティ応用に限定されない汎用的な技術であるが、IoT デバイスの物理攻撃対策回路の設計に応用することにより、物理セキュリティにスケーラビリティを与えることが可能である。

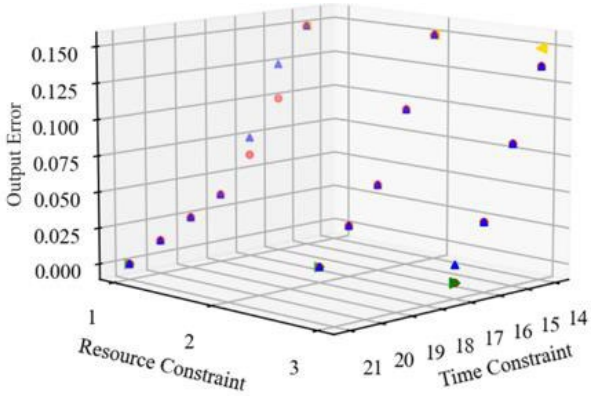


図 1. 計算誤差・時間・性能のトレードオフ

(2) 高位合成の設計空間探索によるスケーラブルな物理セキュリティの実現

一般的に、高位合成を利用して専用回路を設計する際、クロック周波数やさまざまな最適化（ループパイプライニング、ループ展開など）の適用の有無を指定することができる。これらの指定を変更しながら高位合成を繰り返し実行することにより、性能、面積、消費電力の異なる回路を複数生成し、その中から最適な回路を選択することができる。この作業は設計空間探索と呼ばれる。本研究では、高位合成の設計空間探索により、性能、面積、消費電力だけでなく、物理セキュリティの強度も最適化できることを実証した。具体的には、AES や軽量暗号アルゴリズム Chaskey の専用回路を設計する際に、クロック周波数制約と最適化オプションを変更し、性能、面積、消費電力、物理セキュリティ強度を評価した。物理セキュリティ強度の評価はウェルチの t 検定により行った。図 2 は、AES 暗号回路の設計空間探索を行い、回路の面積（FPGA 資源数）と物理セキュリティ強度とのトレードオフを示したものである。このような設計空間探索を通じて、コスト制約の下で物理セキュリティ強度を最大化したり、あるいは、物理セキュリティ強度の制約下でコストを最小化したりすることが可能となる。

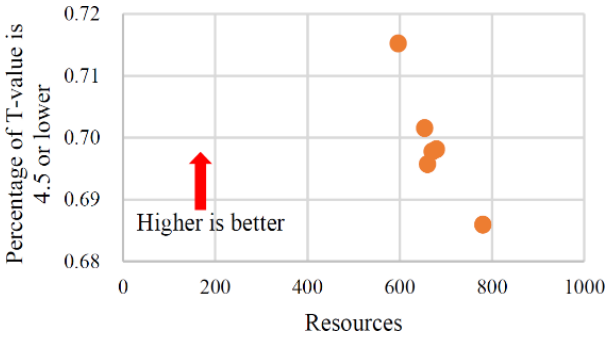
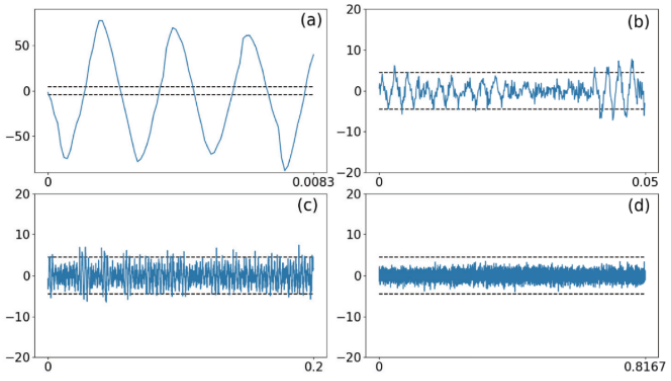


図 2. セキュリティと資源のトレードオフ

(3) 物理セキュリティ強度の高い ARX 暗号回路の高位合成

電力サイドチャネル攻撃に強い ARX 暗号回路を設計する高位合成手法を提案した。提案手法は、C コード内の演算に 3-share Threshold Implementation を適用し、さらに、高位合成のスケジューリング時に演算チェイニングを無効化することで、電力サイドチャネル漏洩を軽減する。Chaskey、Speck、Simon の 3 種類の ARX 暗号を FPGA に実装し、サイドチャネル攻撃耐性と回路面積、遅延を評価した。評価の結果、提案手法は、3 種類の暗号回路すべてにおいて物理セキュリティを向上させることに成功した。図 3 は Chaskey 暗号回路に対する評価結果である。また、物理セキュリティを高めつつ回路面積と遅延のトレードオフを改善する高位合成に関する知見を得た。



(a)対策なし、(b)チェイニング無効、(c)TI、(d)TI＋チェイニング無効

図 3. Chaskey 暗号回路の物理セキュリティ向上

(4) 乱数生成の近似と物理セキュリティのスケーラビリティの解析

Threshold Implementation 技術を AES 暗号回路に適用し、Test Vector Leakage Assessment（TVLA）評価を実施した。Threshold Implementation の安全性を保証する上で重要な要素の一つに乱数の更新処理がある。更新処理では中間値を多くの乱数を使って再マスキングすることで情報漏洩を防ぐが、本研究ではたとえ暗号理論的に安全な乱数生成器（PRNG）を用いていたとしても、十分な更新が行われない乱数では情報漏洩が起きてしまうことを明らかにした。具体的には、PRNG に供給するシード値を暗号化毎に更新しない場合や、乱数ビットの更新を暗号処理中に停止した場合に、情報漏洩を観測した。図 4 は、乱数ビットの更新を停止した場合に情報漏洩が観測されたことを示している。

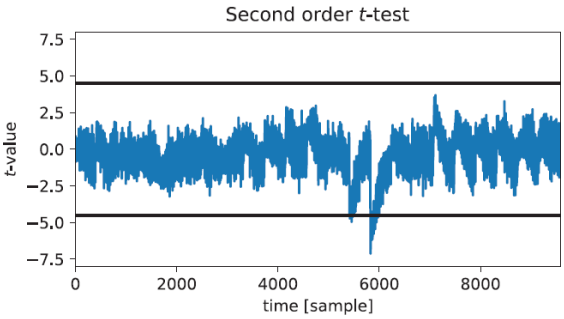


図 4. 乱数ビット更新停止による情報漏洩

また、加算器単体を対象として、マスキングの近似が物理セキュリティに与える影響について調査した。マスクすべき値に対して乱数のビット数が短い場合の加算器の構成法を提案し、t 検定により情報漏洩の大きさを評価した。

(5) 低オーバーヘッドな電力サイドチャネル攻撃対策

FPGA 実装された暗号回路を対象として、オーバーヘッドの小さな電力サイドチャネル攻撃対策法を開発した。提案手法は、使用されていない組込みハードマクロ DCM (Digital Clock Manager) を活用することで、低オーバーヘッドを実現する（図 5 参照）。DCM により、動作クロックに依存しない周期のノイズを FPGA 内部で生成することを実現した。

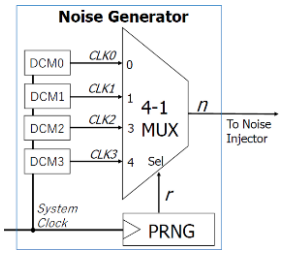


図 5. FPGA 向け
ノイズ生成回路

(6) AES 暗号回路のカスタム設計

AES 暗号回路において情報漏洩の危険性が大きい S-box について、電源および電磁波サイドチャネル漏洩を低減するためのカスタム設計を行った。対象回路を搭載した実証チップを製造し、物理攻撃に対するセキュリティ耐性とそのコストのトレードオフを実機評価した。128 ビット AES 回路用の S-box の実装において、速度と消費電力面で約 2 倍、面積で 30%程度のハードウェアオーバーヘッドが発生するが、t 検定では 100 倍以上のセキュリティ耐性の向上があることを明らかにした。また、実際に電源解析攻撃を行い、未対策版ではおよそ 1 万波形で鍵が漏洩するのに対し、100 万波形に対して攻撃を行っても鍵を奪取できないことを確認した。

(7) ニューラルネットワークに対するサイドチャネル攻撃

従来、サイドチャネル攻撃の主な対象は暗号回路であったが、近年、AI が広く普及し、その重要性が高まるにつれ、AI に対するサイドチャネル攻撃の脅威が高まっている。そこで、ニューラルネットワークの乗算に対するサイドチャネル攻撃を想定した研究を行った。攻撃シミュレーションの結果を比較し、最適なアルゴリズムを検討した。その結果、バイトごとの漏洩情報の利用とアルゴリズムの繰り返し適用により、復元率が向上する手法を提案した。また、量子化された値の乗算に対する攻撃も可能であることが検証された。

５．主な発表論文等

〔雑誌論文〕　計13件（うち査読付論文　13件／うち国際共著　0件／うちオープンアクセス　11件）

１．著者名 Saya Inagaki, Mingyu Yang, Yang Li, Kazuo Sakiyama, Yuko Hara-Azumi	４．巻 22
２．論文標題 Power Side-channel Attack Resistant Circuit Designs of ARX Ciphers Using High-level Synthesis	５．発行年 2023年
３．雑誌名 ACM Transactions on Embedded Computing 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） 10.1145/3609507	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 Takumi Mizuno, Hiroki Nishikawa, Xiangbo Kong, Hiroyuki Tomiyama	４．巻 12
２．論文標題 Empirical Analysis of Power Side-Channel Leakage of High-Level Synthesis Designed AES Circuits	５．発行年 2023年
３．雑誌名 International Journal of Reconfigurable and Embedded Systems	６．最初と最後の頁 305-319
掲載論文のDOI（デジタルオブジェクト識別子） 10.11591/ijres.v12.i3.pp305-319	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 Mingyu Yang, Tanvir Ahmed, Saya Inagaki, Kazuo Sakiyama, Yang Li, Yuko Hara-Azumi	４．巻 11
２．論文標題 Hardware/Software Cooperative Design against Power Side-channel Attacks on IoT Devices	５．発行年 2024年
３．雑誌名 IEEE Internet of Things Journal	６．最初と最後の頁 16758-16768
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/JIOT.2024.3355417	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 Yuto Miura, Hiroki Nishikawa, Xiangbo Kong, Hiroyuki Tomiyama	４．巻 -
２．論文標題 Timing Issues on Power Side-Channel Leakage of AES Circuits Designed by High-Level Synthesis	５．発行年 2024年
３．雑誌名 International Journal of Reconfigurable and Embedded 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） なし	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 Go Takatoi, Takeshi Sugawara, Kazuo Sakiyama, Yuko Hara-Azumi, Yang Li	4．巻 12 (9)
2．論文標題 The Limits of Timing Analysis and SEMA on Distinguishing Similar Activation Functions of Embedded Deep Neural Networks	5．発行年 2022年
3．雑誌名 Applied Sciences	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） 10.3390/app12094135	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 Hiroki Nishikawa, Kana Shimada, Ittetsu Taniguchi, Hiroyuki Tomiyama	4．巻 15 (1)
2．論文標題 Mouldable Fork-Join Task Scheduling Techniques with Inter and Intra-Task Communications	5．発行年 2022年
3．雑誌名 International Journal of Embedded Systems	6．最初と最後の頁 69-81
掲載論文のDOI（デジタルオブジェクト識別子） 10.1504/IJES.2022.122074	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 Koyu Ohata, Hiroki Nishikawa, Xiangbo Kong, Hiroyuki Tomiyama	4．巻 11 (10)
2．論文標題 ILP-based and Heuristic Scheduling Techniques for Variable-Cycle Approximate Functional Units in High-Level Synthesis	5．発行年 2022年
3．雑誌名 Computers	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） 10.3390/computers11100146	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 Yilin Zhao, Hiroki Nishikawa, Xiangbo Kong, Hiroyuki Tomiyama	4．巻 12 (1)
2．論文標題 Side Channel Power Analysis Resistance Evaluation of Masked Adders on FPGA	5．発行年 2023年
3．雑誌名 International Journal of Reconfigurable and Embedded 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） 10.11591/ijres.v12.i1.pp97-112	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 Ryota Hira, Tomoaki Kitahara, Daiki Miyahara, Yuko Hara-Azumi, Yang Li, 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 Takuma Hikida, Hiroki Nishikawa, Hiroyuki Tomiyama	4．巻 10
2．論文標題 Heuristic Algorithms for Dynamic Scheduling of Moldable Tasks in Multicore Embedded Systems	5．発行年 2021年
3．雑誌名 International Journal of Reconfigurable and Embedded Systems (IJRES)	6．最初と最後の頁 157-167
掲載論文のDOI（デジタルオブジェクト識別子） 10.11591/ijres.v10.i3.pp157-167	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 Hiroki Nishikawa, Kana Shimada, Ittetsu Taniguchi, Hiroyuki Tomiyama	4．巻 E105-A
2．論文標題 Simultaneous Scheduling and Core-Type Optimization for Moldable Fork-Join Tasks on Heterogeneous Multicores	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 540-548
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transfun.2021VLP0003	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 Hiroki Nishikawa, Kenta Shirane, Ryohei Nozaki, Ittetsu Taniguchi, Hiroyuki Tomiyama	4．巻 42
2．論文標題 Function-Level Module Sharing Techniques in High-Level Synthesis	5．発行年 2020年
3．雑誌名 ETRI Journal	6．最初と最後の頁 527-533
掲載論文のDOI（デジタルオブジェクト識別子） 10.4218/etrij.2020-0107	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 Kenta Shirane, Takahiro Yamamoto, Hiroyuki Tomiyama	4．巻 10
2．論文標題 A Design Methodology for Approximate Multipliers in Convolutional Neural Networks: A Case of MNIST	5．発行年 2021年
3．雑誌名 International Journal of Reconfigurable and Embedded Systems (IJRES)	6．最初と最後の頁 1-10
掲載論文のDOI（デジタルオブジェクト識別子） 10.11591/ijres.v10.i1.pp1-10	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 －

〔学会発表〕　計104件（うち招待講演　5件／うち国際学会　56件）

1．発表者名 Hiro Minamiguchi, Nagisa Ishiura, Hiroyuki Tomiyama, Hiroyuki Kanbara
2．発表標題 Automatic Generation of Management Module for Full Hardware Implementation of RTOS-Based Systems
3．学会等名 International Technical Conference on Circuits/Systems, Computers, and Communications（国際学会）
4．発表年 2023年

1．発表者名 Taosong Zhao, Hiroki Nishikawa, Xiangbo Kong, Hiroyuki Tomiyama
2．発表標題 Design and Evaluation of AES Encryption Circuits with Various S-Box Implementations
3．学会等名 International Symposium on Advanced Technologies and Applications in the Internet of Things（国際学会）
4．発表年 2023年

1．発表者名 Yuto Miura, Hiroki Nishikawa, Xiangbo Kong, Hiroyuki Tomiyama
2．発表標題 Simulation-based Analysis of Power Side-Channel Leakage at Different Sampling Intervals
3．学会等名 International Workshop on Advances in Networking and Computing（国際学会）
4．発表年 2023年

１．発表者名
Maki Tsukahara, Haruka Hirata, Mingyu Yang, Daiki Miyahara, Yang Li, Yuko Hara-Azumi, Kazuo Sakiyama

２．発表標題
On the Practical Dependency of Fresh Randomness in AES S-box with Second-Order TI

３．学会等名
International Workshop on Information and Communication Security（国際学会）

４．発表年
2023年

１．発表者名
Tomoaki Ukezono, Yui Koyanagi

２．発表標題
A Countermeasure to Power Analysis Attack by Arbitrarily Injecting Multiple Types of Noise

３．学会等名
IEEE Region 10 Symposium（国際学会）

４．発表年
2023年

１．発表者名
Tomoaki Ukezono, Yui Koyanagi

２．発表標題
Disturbing Bit-transition Using History-based Mechanism against Power Analysis Attacks

３．学会等名
International Seminar on Application for Technology of Information and Communication（国際学会）

４．発表年
2023年

１．発表者名
Yui Koyanagi, Tomoaki Ukezono

２．発表標題
Improving Tamper-Resistance Exploiting Clock Phase Shifter Embedded in FPGAs

３．学会等名
International Conference on Electrical Engineering, Computer Science and Informatics（国際学会）

４．発表年
2023年

１．発表者名
Tomoaki Ukezono, Yui Koyanagi

２．発表標題
Effect of High Frequency Noise Using DCMs in FPGA on Power Analysis Attack

３．学会等名
International Symposium on Communications and Information Technologies（国際学会）

４．発表年
2023年

１．発表者名
Ryoma Katsube, Tomoaki Ukezono

２．発表標題
Investigation for Impact of Environmental Noise on Power Analysis Attacks

３．学会等名
International SoC Design Conference（国際学会）

４．発表年
2023年

１．発表者名
Yui Koyanagi, Tomoaki Ukezono

２．発表標題
A Cost-sensitive and Simple Masking Design for Side-channels

３．学会等名
IEEE Region 10 Technical Conference（国際学会）

４．発表年
2023年

１．発表者名
Tomoaki Ukezono, Yui Koyanagi

２．発表標題
Reusing Outputs from S-boxes for Tamper Resistant Design

３．学会等名
International Conference on Electrical, Computer and Energy Technologies（国際学会）

４．発表年
2023年

１．発表者名
Yui Koyanagi, Tomoaki Ukezono

２．発表標題
A Cost-aware Generation Method of Disposable Random Value Exploiting Parallel S-box Implementation for Tamper-resistant AES Design

３．学会等名
International Workshop on Advances in Networking and Computing（国際学会）

４．発表年
2023年

１．発表者名
Hiroyuki Hama, Tomoaki Ukezono, Toshinori Sato

２．発表標題
Leveraging Approximate Computing for IoT Image Transmission

３．学会等名
International SoC Design Conference（国際学会）

４．発表年
2023年

１．発表者名
Toshinori Sato, Hiroyuki Hama, Tomoaki Ukezono

２．発表標題
Comparative Evaluation between Carry Prediction and Sign Error Correction in Approximate Addition

３．学会等名
International SoC Design Conference（国際学会）

４．発表年
2023年

１．発表者名
Taiki Nagatomo, Toshinori Sato

２．発表標題
Improving Energy Efficiency in Medical Edge Devices for ECG Feature Detection via Approximate Computing

３．学会等名
Eurasia Conference on IoT, Communication and Engineering（国際学会）

４．発表年
2023年

１．発表者名
Hiroyuki Hama, Toshinori Sato

２．発表標題
Towards At-The-Edge ECG Signal Processing With Accuracy-Tunable Approximate Adders

３．学会等名
Global Conference on Consumer Electronics（国際学会）

４．発表年
2023年

１．発表者名
Toshinori Sato, Hiroyuki Hama

２．発表標題
Evaluating Sign Error Correction for Approximate Adders Employing ECG Signal Processing

３．学会等名
International Conference on Electrical Engineering, Computer Science and Informatics（国際学会）

４．発表年
2023年

１．発表者名
Hiroyuki Hama, Tomoaki Ukezono, Toshinori Sato

２．発表標題
Negative Impact of Approximated Signed Addition on Power Reduction

３．学会等名
International Symposium on Devices, Circuits and Systems（国際学会）

４．発表年
2023年

１．発表者名
Yuto Miura, Hiroki Nishikawa, Xiangbo Kong, Hiroyuki Tomiyama

２．発表標題
Impacts of Clock Frequency and Sampling Intervals on Power Side-Channel Leakage of AES Circuits

３．学会等名
International Conference on Electronics, Information, and Communication（国際学会）

４．発表年
2024年

１．発表者名
Tomoki Shimizu, Hiroki Nishikawa, Xiangbo Kong, Hiroyuki Tomiyama

２．発表標題
A Non-Work Conserving Algorithm for Dynamic Scheduling of Moldable Gang Tasks on Multicore Systems

３．学会等名
International Conference on Electronics, Information, and Communication（国際学会）

４．発表年
2024年

１．発表者名
Wakana Ohashi, Aoi Yamaguchi, Hiroki Nishikawa, Hiroyuki Tomiyama

２．発表標題
Fast 32-bit and 48-bit Multipliers for FPGA

３．学会等名
International Conference on Electronics, Information, and Communication（国際学会）

４．発表年
2024年

１．発表者名
Yui Koyanagi, Tomoaki Ukezono

２．発表標題
Masking Regularity of Noise for Tamper-resistant Design on FPGAs

３．学会等名
Workshop on Synthesis And System Integration of Mixed Information technologies（国際学会）

４．発表年
2024年

１．発表者名
Yui Koyanagi, Tomoaki Ukezono, Toshinori Sato

２．発表標題
A Light-Weight and Tamper-Resistant AES Implementation by FPGAs

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

４．発表年
2024年

１．発表者名
Yuhui Liu, Taosong Zhao, Hiroki Nishikawa, Xiangbo Kong, Hiroyuki Tomiyama

２．発表標題
FPGA Design of a Masked AES Circuit with PPRM-based S-Box

３．学会等名
International SoC Design Conference（国際学会）

４．発表年
2024年

１．発表者名
Xiangyu Li, Hiroki Nishikawa, Xiangbo Kong, Hiroyuki Tomiyama

２．発表標題
An Approximate Multiplier Design Based on Mitchell's Algorithm

３．学会等名
International SoC Design Conference（国際学会）

４．発表年
2024年

１．発表者名
大橋和奏，山口葵生，西川広記，冨山宏之

２．発表標題
FPGAを対象とした高速な32ビットおよび48ビットの乗算器

３．学会等名
情報処理学会組込みシステム研究会

４．発表年
2023年

１．発表者名
三浦佑斗，西川広記，孔祥博，冨山宏之

２．発表標題
電力のサンプリング間隔がAES回路のサイドチャネルリーク量に与える影響の評価

３．学会等名
情報処理学会組込みシステム研究会

４．発表年
2023年

１．発表者名
清水智貴，西川広記，孔祥博，冨山宏之

２．発表標題
Moldable Gangタスクに対するNon-work Conserving型の動的スケジューリングアルゴリズム

３．学会等名
情報処理学会組込みシステム研究会

４．発表年
2023年

１．発表者名
原田優咲，塚原麻輝，宮原大輝，李陽，原祐子，崎山一男

２．発表標題
乱数性に対するTI-AESの一様性に関する基礎評価

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
2023年

１．発表者名
長友泰樹，請園智玲

２．発表標題
電力解析攻撃におけるS-Boxのハミング距離と消費電力の関係の調査

３．学会等名
情報科学技術フォーラム

４．発表年
2023年

１．発表者名
勝部諒真，請園智玲，佐藤寿倫

２．発表標題
暗号チップへの電力解析攻撃における環境ノイズの影響調査

３．学会等名
Student Workshop of IEEE IM Japan Chapter

４．発表年
2023年

１．発表者名
三上啓，石浦菜岐佐，冨山宏之，神原弘之

２．発表標題
RTOS利用システムのフルハードウェア化における状態レジスタの最適化による回路規模削減

３．学会等名
電子情報通信学会VLD/RECONF研究会

４．発表年
2024年

１．発表者名
原田優咲，塚原麻輝，宮原大輝，李陽，原祐子，崎山一男

２．発表標題
TI-AES に使用する擬似乱数生成器の物理安全性への影響

３．学会等名
暗号と情報セキュリティシンポジウム

４．発表年
2024年

１．発表者名
古野亨紀，佐藤泰雅，平田遼，宮原大輝，李陽，崎山一男

２．発表標題
故障感度情報を用いたt検定によるAESハードウェアの安全性評価

３．学会等名
暗号と情報セキュリティシンポジウム

４．発表年
2024年

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

２．発表標題
Implementation of Multiplicative Masked AES S-Box for M&M Scheme

３．学会等名
暗号と情報セキュリティシンポジウム

４．発表年
2024年

１．発表者名
胡宇暘，宮原大輝，崎山一男，李陽

２．発表標題
高シェア数状況下でのt検定による安全性評価の有効性について

３．学会等名
暗号と情報セキュリティシンポジウム

４．発表年
2024年

１．発表者名
天野龍乃如，崎山一男，宮原大輝，李陽

２．発表標題
MLPのハミング距離モデルに基づくサイドチャネル攻撃に対する 加算マスキング対策の提案

３．学会等名
電子情報通信学会総合大会

４．発表年
2024年

１．発表者名
楊明宇，比留間紘斗，崎山一男，李陽，原祐子

２．発表標題
コンポーザブルセキュリティによる暗号回路の高位合成

３．学会等名
電子情報通信学会HWS研究会

４．発表年
2024年

１．発表者名
角颯太，楊明宇，原祐子

２．発表標題
故障注入攻撃耐性を強化した擬似乱数生成器の設計

３．学会等名
電子情報通信学会HWS研究会

４．発表年
2024年

１．発表者名
Yui Koyanagi, Tomoaki Ukezono

２．発表標題
Lightweight Countermeasures to Power Analysis Attacks by Injecting Noise to Cryptographic Circuits

３．学会等名
IEICE GlobalNet Workshop 2024

４．発表年
2024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
IEEE International Solid-State Circuits Conference（招待講演）（国際学会）

４．発表年
2022年

１．発表者名
Saya Inagaki, Mingyu Yang, Yang Li, Kazuo Sakiyama, Yuko Hara-Azumi

２．発表標題
Examining Vulnerability of HLS-designed Chaskey-12 Circuits to Power Side-Channel Attacks

３．学会等名
International Symposium on Quality Electronic Design（国際学会）

４．発表年
2022年

１．発表者名
Tongxin Yang, Tomoaki Ukezono, Toshinori Sato

２．発表標題
Reducing Power Consumption using Approximate Encoding for CNN Accelerators at the Edge

３．学会等名
Great Lakes Symposium on VLSI（国際学会）

４．発表年
2022年

１．発表者名
Tomoki Shimizu, Hiroki Nishikawa, Xiangbo Kong, Hiroyuki Tomiyama

２．発表標題
A Fair-Policy Dynamic Scheduling Algorithm for Moldable Gang Tasks on Multicores

３．学会等名
Mediterranean Conference on Embedded Computing（国際学会）

４．発表年
2022年

１．発表者名
Yuho Toku, Hiroki Nishikawa, Xiangbo Kong, Hiroyuki Tomiyama

２．発表標題
Container-based Throughput Balancing for Multiple Streaming Applications: A Case Study

３．学会等名
Mediterranean Conference on Embedded Computing（国際学会）

４．発表年
2022年

１．発表者名
Koyu Ohata, Hiroki Nishikawa, Xiangbo Kong, Hiroyuki Tomiyama

２．発表標題
A Heuristic Scheduling Algorithm with Variable Cycle Approximate Functional Units in High Level Synthesis

３．学会等名
International Symposium on Advanced Technologies and Applications in the Internet of Things（国際学会）

４．発表年
2022年

１．発表者名
Masaki Sano, Hiroki Nishikawa, Xiangbo Kong, Hiroyuki Tomiyama, Tongxin Yang, Tomoaki Ukezono, Toshinori Sato

２．発表標題
An Accuracy Controllable Approximate Adder for FPGAs

３．学会等名
International Symposium on Advanced Technologies and Applications in the Internet of Things（国際学会）

４．発表年
2022年

１．発表者名
Yilin Zhao, Qidi Zhang, Hiroki Nishikawa, Xiangbo Kong, Hiroyuki Tomiyama

２．発表標題
Evaluation of Power Analysis Attack Resistance of Masked Adders on FPGA

３．学会等名
International Symposium on Advanced Technologies and Applications in the Internet of Things（国際学会）

４．発表年
2022年

１．発表者名
Yui Koyanagi, Tomoaki Ukezono

２．発表標題
An Extremely Light-Weight Countermeasure to Power Analysis Attack in Dedicated Circuit for AES

３．学会等名
International SoC Design Conference（国際学会）

４．発表年
2022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 AP/CAS/ED/MTT/SSCS Webinar Seminar（招待講演）（国際学会）

４．発表年
2022年

１．発表者名
Tomoaki Kitahara, Ryota Hira, Yuko Hara-Azumi, Daiki Miyahara, Yang Li, Kazuo Sakiyama

２．発表標題
Optimized Software Implementations of Ascon, Grain-128AEAD, and TinyJambu on ARM Cortex-M

３．学会等名
International Workshop on Information and Communication Security（国際学会）

４．発表年
2022年

１．発表者名
Eiji Sugahara, Hiroki Nishikawa, Xiangbo Kong, Hiroyuki Tomiyama

２．発表標題
Energy Consumption Reduction through Resource Allocation Using Docker

３．学会等名
International Workshop on Advances in Networking and Computing（国際学会）

４．発表年
2022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/ED DL Technical Seminar（招待講演）（国際学会）

４．発表年
2022年

１．発表者名
Tomoaki Ukezono

２．発表標題
A Countermeasure to Power Analysis Attack in Flip Flops

３．学会等名
Asia and South Pacific Design Automation Conference（国際学会）

４．発表年
2023年

１．発表者名
Takumi Mizuno, Hiroki Nishikawa, Xiangbo Kong, Hiroyuki Tomiyama

２．発表標題
Empirical Analysis of Side-Channel Attack Resistance of HLS-Designed AES Circuits

３．学会等名
International Conference on Electronics, Information, and Communication（国際学会）

４．発表年
2023年

１．発表者名
Yuto Miura, Takumi Mizuno, Hiroki Nishikawa, Xiangbo Kong, Hiroyuki Tomiyama

２．発表標題
Impacts of Clock Constraints on Side-Channel Leakage of HLS-Designed AES Circuits

３．学会等名
International Conference on Electronics, Information, and Communication（国際学会）

４．発表年
2023年

１．発表者名
原 祐子

２．発表標題
組込みマイクロプロセッサにおけるハードウェアセキュリティ

３．学会等名
電子情報通信学会Webinarテクノロジートレンドシリーズ（招待講演）

４．発表年
2022年

１．発表者名
清水智貴，西川広記，孔祥博，冨山宏之

２．発表標題
Fair方式に基づくMoldable Gangタスクの動的スケジューリングアルゴリズム

３．学会等名
回路とシステムワークショップ

４．発表年
2022年

１．発表者名
南口比呂，石浦菜岐佐，冨山宏之，神原弘之

２．発表標題
RTOS利用システムのフルハードウェア化における管理ハードウェアの自動生成

３．学会等名
DAシンポジウム

４．発表年
2022年

１．発表者名
志摩和毅，西川広記，孔祥博，冨山宏之

２．発表標題
RISC-Vプロセッサへの乱数生成命令の追加

３．学会等名
組込みシステム技術に関するサマーワークショップ

４．発表年
2022年

１．発表者名
菅原英治，西川広記，孔祥博，冨山宏之

２．発表標題
Dockerを用いたリソース割り当てによる低電力化と高速化

３．学会等名
組込みシステム研究会

４．発表年
2022年

１．発表者名
三浦佑斗，水野拓己，西川広記，孔祥博，冨山宏之

２．発表標題
クロック制約がAES回路の電力解析攻撃耐性に与える影響の評価

３．学会等名
組込みシステム研究会

４．発表年
2022年

１．発表者名
水野拓己，西川広記，孔祥博，冨山宏之

２．発表標題
高位合成で設計されたAES回路のサイドチャネル攻撃耐性の評価

３．学会等名
組込みシステム研究会

４．発表年
2022年

１．発表者名
趙意琳，西川広記，孔祥博，冨山宏之

２．発表標題
FPGAにおけるマスキングを施した加算器の電力解析攻撃耐性の評価

３．学会等名
組込みシステム研究会

４．発表年
2022年

１．発表者名
小柳結依，請園智玲

２．発表標題
FPGA組込みPLLを用いたサイドチャネル攻撃対策のためのノイズ生成手法の検討

３．学会等名
Young CAS Researchers Workshop

４．発表年
2022年

１．発表者名
小柳結依，請園智玲

２．発表標題
乱数を用いた軽量な電力解析攻撃対策実装の検討

３．学会等名
システムとLSIの設計技術研究会

４．発表年
2022年

１．発表者名
長友泰樹，請園智玲

２．発表標題
ARX型暗号への近似加算適用による電力解析攻撃対策の検討

３．学会等名
システムとLSIの設計技術研究会

４．発表年
2022年

１．発表者名
濵寛之，請園智玲，佐藤寿倫

２．発表標題
DCTへの近似加算適用によるJPEG圧縮の低消費電力化の検討

３．学会等名
システムとLSIの設計技術研究会

４．発表年
2022年

１．発表者名
稲垣沙耶，楊明宇，李陽，崎山一男，原祐子

２．発表標題
電力サイドチャネル攻撃に対して堅牢なARX型暗号回路の高位合成

３．学会等名
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
Qidi Zhang, Xiangbo Kong, Hiroyuki Tomiyama

２．発表標題
A Toolkit for Power Behavior Analysis of HLS-Designed FPGA Circuits

３．学会等名
Symposium on Low-Power and High-Speed Chips and Systems（国際学会）

４．発表年
2021年

１．発表者名
Tomoaki Ukezono

２．発表標題
Resistance for Side-Channel Attack by Virtual Dual-Rail Effect

３．学会等名
International Conference on Electrical, Communication, and Computer Engineering（国際学会）

４．発表年
2021年

１．発表者名
Takumi Mizuno, Qidi Zhang, Hiroki Nishikawa, Xiangbo Kong, Hiroyuki Tomiyama

２．発表標題
Impacts of HLS Optimizations on Side-Channel Leakage for AES Circuits

３．学会等名
International SoC Design Conference（国際学会）

４．発表年
2021年

１．発表者名
Masaki Sano, Kenta Shirane, Hiroki Nishikawa, Xiangbo Kong, Hiroyuki Tomiyama, Tongxin Yang, Tomoaki Ukezono

２．発表標題
Design of a 32-bit Accuracy-Controllable Approximate Multiplier for FPGAs

３．学会等名
International SoC Design Conference（国際学会）

４．発表年
2021年

１．発表者名
Koyu Ohata, Kenta Shirane, Hiroki Nishikawa, Xiangbo Kong, Hiroyuki Tomiyama

２．発表標題
Scheduling with Variable-Cycle Approximate Functional Units in High-Level Synthesis

３．学会等名
International SoC Design Conference（国際学会）

４．発表年
2021年

１．発表者名
Yilin Zhao, Qidi Zhang, Hiroki Nishikawa, Xiangbo Kong, Hiroyuki Tomiyama

２．発表標題
Power Side-Channel Analysis for Different Adders on FPGA

３．学会等名
International SoC Design Conference（国際学会）

４．発表年
2021年

１．発表者名
Kenta Shirane, Hiroki Nishikawa, Xiangbo Kong, Hiroyuki Tomiyama

２．発表標題
High-Level Synthesis of Approximate Computing Circuits with Dual Accuracy Modes

３．学会等名
International SoC Design Conference（国際学会）

４．発表年
2021年

１．発表者名
Chiharu Shiro, Hiroki Nishikawa, Xiangbo Kong, Hiroyuki Tomiyama, Shigeru Yamashita

２．発表標題
Minimization of Routing Area in MEDA Biochips

３．学会等名
Biomedical Circuits and Systems Conference（国際学会）

４．発表年
2021年

１．発表者名
Mao Nishira, Satoshi Ito, Hiroki Nishikawa, Xiangbo Kong, Hiroyuki Tomiyama

２．発表標題
An ILP-based Approach to Delivery Drone Routing under Load-dependent Flight Speed

３．学会等名
International Conference on Electronics, Information, and Communication（国際学会）

４．発表年
2022年

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

２．発表標題
Simple Electromagnetic Analysis Against Activation Functions of Deep Neural Networks (from AIHWS 2020)

３．学会等名
電子情報通信学会ISEC研究会（招待講演）

４．発表年
2021年

１．発表者名
菅原英治，江頭拓也，西川広記，孔祥博，冨山宏之

２．発表標題
セキュリティカメラシステムの低電力化と高速化

３．学会等名
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
大幡孝融，白根健太，西川広記，孔祥博，冨山宏之

２．発表標題
高位合成における可変サイクル近似演算のスケジューリング

３．学会等名
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
佐野正樹，白根健太，西川広記，孔祥博，冨山宏之，ヨウドンキン，請園智玲

２．発表標題
FPGA向け32ビット可変精度近似乗算器の設計と解析

３．学会等名
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
城千春，西川広記，孔祥博，冨山宏之，山下茂

２．発表標題
MEDAバイオチップにおける使用面積の最小化

３．学会等名
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
北原知明，日良僚太，原祐子，李陽，崎山一男

２．発表標題
NIST軽量暗号最終候補におけるAD長と平文長に対するレイテンシの測定

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
請園智玲

２．発表標題
Wave-FFによるAESへの電力解析攻撃の耐タンパ性評価

３．学会等名
電子情報通信学会HWS/ICD研究会

４．発表年
2021年

１．発表者名
西羅真央，伊藤哲，西川広記，孔祥博，冨山宏之

２．発表標題
荷重により速度変化する荷物配送ドローンの経路計画に対する近似解法

３．学会等名
情報処理学会組込みシステム研究会

４．発表年
2021年

１．発表者名
趙意琳，張啓迪，西川広記，孔祥博，冨山宏之

２．発表標題
FPGAにおける加算器の電力解析攻撃耐性の評価

３．学会等名
情報処理学会組込みシステム研究会

４．発表年
2021年

１．発表者名
水野拓己，張啓迪，西川広記，孔祥博，冨山宏之

２．発表標題
高位合成における最適化のサイドチャネル攻撃耐性への影響

３．学会等名
情報処理学会組込みシステム研究会

４．発表年
2021年

１．発表者名
北原知明，日良僚太，原祐子，宮原大輝，李陽，崎山一男

２．発表標題
NIST軽量暗号最終候補におけるソフトウェア実装性能の評価

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
安堂拓也，石井雄吾，石浦菜岐佐，冨山宏之，神原弘之

２．発表標題
RTOS利用システムの汎用高位合成系を用いたフルハードウェア化

３．学会等名
電子情報通信学会VLD/CPSY/RECONF/情報処理学会SLDM/ARC研究会

４．発表年
2022年

１．発表者名
大幡孝融，西川広記，孔祥博，冨山宏之

２．発表標題
高位合成における可変サイクル近似演算のヒューリスティックスケジューリングアルゴリズム

３．学会等名
電子情報通信学会VLD/HWS研究会

４．発表年
2022年

１．発表者名
Hiroki Nishikawa, Kana Shimada, Ittetsu Taniguchi, Hiroyuki Tomiyama

２．発表標題
Scheduling of Moldable Fork-Join Tasks with Inter- and Intra-Task Communications

３．学会等名
International Workshop on Software and Compilers for Embedded Systems（国際学会）

４．発表年
2020年

１．発表者名
Takuma Hikida, Hiroki Nishikawa, Hiroyuki Tomiyma

２．発表標題
Heuristic Algorithms for Dynamic Scheduling of Moldable Tasks

３．学会等名
International SoC Design Conference（国際学会）

４．発表年
2020年

１．発表者名
Jo Yoshimoto, Ittetsu Taniguchi, Hiroyuki Tomiyma, Takao Onoye

２．発表標題
An Evaluation of Edge Computing Platform for Reliable Automated Drones

３．学会等名
International SoC Design Conference（国際学会）

４．発表年
2020年

１．発表者名
Takaya Watanabe, Hiroki Nishikawa, Hiroyuki Tomiyma

２．発表標題
Scheduling of Rigid Tasks on Heterogeneous Multicores

３．学会等名
International SoC Design Conference（国際学会）

４．発表年
2020年

１．発表者名
Takuya Egashira, Hiroki Nishikawa, Xiangbo Kong, Hiroyuki Tomiyama

２．発表標題
A Home Security Camera System with Container-based Resource Allocation on Raspberry Pi

３．学会等名
International Conference on Electronics, Information, and Communication（国際学会）

４．発表年
2021年

１．発表者名
Eiji Sugahara, Hiroki Nishikawa, Takuya Egashira, Xiangbo Kong, Hiroyuki Tomiyama

２．発表標題
A Low-power Security Camera System Using OpenCV and YOLO

３．学会等名
International Workshop on Nonlinear Circuits, Communications and Signal Processing（国際学会）

４．発表年
2021年

１．発表者名
日良僚太，李陽，原祐子，崎山一男

２．発表標題
NIST軽量暗号の第2ラウンド候補の軽量実装に向けた分類と比較

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
Go Takatoi, Takeshi Sugawara, Kazuo Sakiyama, Yuko Hara-Azumi, 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
日良僚太，李陽，原祐子，崎山一男

２．発表標題
NIST軽量暗号第2ラウンド候補のソフトウェア実装に向けた調査

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
2021年

１．発表者名
六車伊織，石浦菜岐佐，安堂拓也，冨山宏之，神原弘之

２．発表標題
RTOS利用システムのフルハードウェア化におけるサービス処理機能の集約

３．学会等名
電子情報通信学会VLD/HWS研究会

４．発表年
2021年

１．発表者名
疋田拓万，西川広記，冨山宏之

２．発表標題
可変並列度タスクの動的スケジューリングアルゴリズム

３．学会等名
電子情報通信学会VLD/HWS研究会

４．発表年
2021年

１．発表者名
白根健太，西川広記，孔祥博，冨山宏之

２．発表標題
精度可変な近似計算回路の高位合成

３．学会等名
電子情報通信学会VLD/HWS研究会

４．発表年
2021年

１．発表者名 稲垣沙耶，楊明宇，李陽，崎山一男，原祐子
２．発表標題 高位合成による軽量暗号ChaskeyのFPGA実装およびサイドチャネル攻撃耐性の評価
３．学会等名 電子情報通信学会VLD/HWS研究会
４．発表年 2021年

〔図書〕　計0件

〔出願〕　計1件

産業財産権の名称	発明者	権利者
漏洩情報抑制回路	三浦 典之	同左
産業財産権の種類、番号	**出願年**	**国内・外国の別**
特許、2024-003538	2024年	国内

〔取得〕　計0件

〔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
研究分担者	佐藤　寿倫 (Sato Toshinori) (00322298)	福岡大学・工学部・教授 (37111)	
研究分担者	原　祐子 (Hara-Azumi Yuko) (20640999)	東京工業大学・工学院・准教授 (12608)	
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	請園　智玲 (Ukezono Tomoaki) (50610060)	福岡大学・工学部・助教 (37111)	

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	三浦　典之 (Miura Noriyuki) (70650555)	大阪大学・大学院情報科学研究科・教授 (14401)	
研究分担者	崎山　一男 (Sakiyama Kazuo) (80508838)	電気通信大学・大学院情報理工学研究科・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			
ドイツ	RWTH Aachen University			