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　３ 年　 ４ 月　 ９ 日現在

機関番号：１１３０１
研究種目：基盤研究(A)（一般）
研究期間：2017～2020
課題番号：１７Ｈ００７２９

研究課題名（和文）冗長ガロア体算術に基づくセキュリティハードウェアの高水準設計技術の研究開発

研究課題名（英文）Development of high-level design methodology for security hardware based on redundant Galois-field arithmetic

研究代表者
本間　尚文（Homma, Naofumi）

東北大学・電気通信研究所・教授

研究者番号：００３４３０６２

交付決定額（研究期間全体）：（直接経費）　　32,700,000円

研究成果の概要（和文）：本研究では，暗号・誤り訂正用LSIの基幹となるガロア体算術演算データパスの設計技術を開発した．まず，(1)多項式環表現・冗長表現基底と呼ばれる冗長なガロア体表現に基づく高次算術演算データパスの形式的設計手法を開発し，(2)その回路表現に適用可能な計算機代数に基づく形式的検証手法を開発した．次に，(3)その応用として暗号プロセッサデータパスに同設計・検証手法を適用した．具体的には，ISO/IEC国際標準暗号を対象として，その高効率・耐タンパー性プロセッサデータパスの形式的設計に適用した．さらに，(4)高次ガロア体算術演算データパスを対象とした自動合成・検証システムを開発した．

研究成果の学術的意義や社会的意義
ガロア体上の算術演算回路は，これまで設計者により経験的に設計されており，その検証に膨大な時間を必要としてきた．特に，実用的な暗号や誤り訂正回路の設計では，項数が100を越える長大なAND-XOR論理式が必要となり，シミュレーション用のテストベンチ作成も非直観的で困難であった．これに対して本研究では，新たな形式的表現を発案するとともに，グレブナー基底などの計算機代数の技法を駆使した形式的検証手法を開発した．これにより，従来困難だった規模の回路の完全な検証に実用的な時間で成功した．

研究成果の概要（英文）：In this research project, we have developed a design technology for the Galois-field arithmetic data path, which is the basis of cryptographic and error correction LSIs. First, (1) a formal design method for high-order arithmetic data paths based on redundant Galois field representations, such as polynomial ring representation and redundant representation basis, was developed, and (2) a formal verification method based on computer algebra applicable to the circuit representation was developed. We have then applied the formal design and verification method to the cryptographic processor data path as its application. In particular, we have designed and verified efficient and/or tamper-resistant processor data paths for the ISO / IEC international standard ciphers. Furthermore, (4) we have developed an automatic synthesis / verification system for higher-order Galois-field arithmetic data paths.

研究分野：計算機科学

キーワード：計算機システム　ハードウェアセキュリティ　LSI設計技術

１．研究開始当初の背景

近年，個人情報の保護や高信頼な電子商取引への要求に伴い，暗号や誤り訂正処理を必要とする応用が急速に拡大しており，携帯電話や RFID など演算リソースの制限された組み込み機器ではそれらの処理のハードウェアによる実装が強く求められている．しかし，現在の回路設計技術は論理回路の設計を基本として発展しており，当該処理で多用されるガロア体（有限体）上の算術演算回路（ガロア体算術演算回路）に対しては十分な設計環境が整っていない．現在の回路設計で用いられるハードウェア記述言語 (HDL: Hardware Description Language) は，ガロア体上の変数を扱うための高水準なデータ構造を持たない．このため，ガロア体算術演算回路を設計する場合，AND-XOR の論理式による低水準な記述を強いられる．また，一般に多入力多出力の算術演算回路では，その機能を計算機シミュレーションで検証するために膨大な時間が必要となる．現代の暗号処理は，語長 128 ビット以上の演算を要するため，シミュレーションによる完全な検証は不可能である．さらに暗号実装の分野では，暗号処理を実行する回路に悪意ある回路を付帯させて秘密情報を奪うハードウェアトロイも報告されている．以上の背景から，ガロア体算術演算回路の機能を高速かつ完全に検証できる形式的手法は，設計・検証容易性の面だけでなく，セキュリティの面からも望まれている．　特に近年，冗長なガロア体表現に基づく高次回路の有効性が示されており，そうした大規模・複雑な回路にも適用可能な設計技術の開発が強く求められている．

本研究代表者は，これまで重み数系で表される算術演算回路の高水準な記述・検証・合成技術とその応用に関する研究を推進してきた．特に，任意の重み数系を統一的に記述可能な新しい算術演算回路の形式的表現手法を発案し，2 進数系と非 2 進数系を最適に融合した算術演算回路の自動合成・検証システムを開発した．同検証システムは，グレブナー基底や多項式簡約といった計算機代数の技法を回路検証に適用することで初めて実現されたものであり，それまで完全な検証が困難だった規模の回路検証に成功している．近年では，同技術を非冗長・低次なガロア体表現に適用できることを見出している．一方で，本研究代表者は，フランスの研究機関との国際共同研究を通して，暗号プロセッサのセキュリティ設計・検証法を開発してきた実績を有する．本研究では，これまで培ってきた上記技術を深化・拡張し，冗長表現を含む高次ガロア体算術演算回路の高水準設計技術を開発する．特に，現在注目を集める認証暗号の多くが高次のガロア体演算で表現されることに着目し，同プロセッサデータパスの形式的設計・検証を実現する．

２．研究の目的

本研究では，非冗長・冗長表現混載の高次ガロア体算術演算 VLSI データパスの設計技術の確立を目指し，その形式的記述・検証手法から自動合成システムの開発までの下記 4 項目を目的とする．

(1)冗長ガロア体表現に基づくガロア体算術演算回路の形式的表現手法の開発

これまでに開発した形式的表現手法をもとに，冗長ガロア体表現に基づく算術演算回路の形式的表現手法を開発する．具体的には，従来表現（基底集合，係数ベクトル集合，既約多項式）を冗長表現に拡張するため，基底集合部分に任意の冗長性を許す剰余多項式環の基底表現を導入するとともに，既約多項式部分を既約･生成多項式の積の形で表現することにより定式化を行う．

(2)ガロア体上の算術演算回路の形式的検証手法の開発

上記(1)で開発したガロア体表現により記述される高次なガロア体算術演算回路の形式的検証手法を開発する．特に，高次のガロア体算術演算を検証するため，これまでの計算機代数に基づく形式的検証に自然演繹に基づく形式的検証を組み合わせる手法を開発する．また，開発手法の有効性を示すため，語長 256 ビットを越える実用的な誤り訂正回路が検証可能なことを実証する．

(3)暗号プロセッサデータパスの形式的設計・検証への応用

上記で開発した手法を用いて実用的な暗号プロセッサの形式的設計・検証が可能なことを実証する．具体的には，ISO/IEC 国際標準ブロック暗号の一つであり，現在世界で最もよく利用されている AES（Advanced Encryption Standard）プロセッサ等の形式的設計･検証を実現する．冗長ガロア体表現を用いた世界最高水準の高速・低消費電力データパスに加えて，各種物理攻撃への耐性を有するセキュアデータパスを開発手法により設計・検証できることを示す．

(4)ガロア体算術演算回路ジェネレータの開発と公開

上記手法で設計・検証された多様なガロア体算術演算回路を自動生成するジェネレータを開発し，Web 上で公開する．本ジェネレータは，仕様として機能（アーキテクチャ），基数，ガロア体を入力すると，それに応じて機能が完全に保証されたガロア体算術演算回路の HDL 記述を生成する．

３．研究の方法

本研究では，上述の目的に対して 4 年間研究開発を行った．平成 29 年度は，冗長ガロア体表現で与えられる算術演算回路の形式的表現および検証手法を開発した．平成 30 年度は，前年度開発した非冗長表現に基づくガロア体算術演算回路の形式的表現が表す回路機能の形式的検証

システムを開発した．また，前年度に規定した冗長表現を含めて定式化したガロア体表現による高次なガロア体算術演算回路の形式的検証手法を開発した．令和元年度は，前年度までに開発した非冗長表現に基づくガロア体算術演算回路の形式的検証手法の応用として，暗号プロセッサデータパスの形式的設計・検証に取り組んだ．令和 2 年度は，冗長ガロア体表現に基づくガロア体算術演算回路の自動生成ジェネレータを開発した．

４．研究成果

平成 29 年度は，多項式環表現および冗長表現基底と呼ばれる冗長なガロア体表現を対象として，その拡大体および合成体上の算術演算回路の形式的表現・検証手法を開発した．具体的には，これまでに開発したガロア体算術演算回路を形式的に表すグラフ表現「ガロア体算術回路グラフ(GF-ACG: Galois-Field Arithmetic Circuit Graph)」の理論を拡張した．ガロア体は，整数環との代数的な類似性に着目すると，整数における各桁の“重み”がガロア体では“基底”に，各桁の“取り得る値”がガロア体では“多項式係数の取り得る値”に対応する．これに加えて，整数では暗黙的に演算（加算や乗算）の規則が定義されていたが，ガロア体では既約多項式として演算規則を明示的に定義する．結果として，基底集合，多項式係数の取り得る値の集合，既約多項式によってガロア体は形式的に定義される．本研究では，これを冗長表現にも拡張するため，基底集合部分に任意の冗長性を許す剰余多項式環の基底表現を導入するとともに，既約多項式部分を多項式の積で表現する形に GF-ACG を拡張した．その基本構造としては，これまでに開発した GF-ACG と同様に，機能の“算術化(Arithmetization)”と“階層化（Hierarchization)”を用いた．算術化とは，回路の機能を論理関数部分も含めて全てガロア体上の変数による算術演算として与えることである．これに加えて，回路構造を効率的に記述するため階層的な記述を導入した．この階層化は，算術演算回路がしばしばそれ自身も算術演算機能を有する部分回路の組み合わせにより表現されることを利用している．開発した表現手法の評価では，多項式環表現されたガロア体上の並列乗算器を網羅的に設計し，当該グラフ表現から変換したハードウェア記述言語（HDL: Hardware Description Language）記述の論理シミュレーションを通して，表現された機能の完全性を評価した．

平成 30 年度は，前年度に開発した非冗長・冗長表現が混載したガロア体算術演算回路の形式的表現が表す回路機能の形式的検証システムを開発した．開発するシステムでは，まず，検証対象となる機能との等価性判定に用いる内部回路記述を多項式集合と見なしてグレブナー基底に変換する．ここで，冗長表現を非冗長表現と同様に扱うため，線形再帰関係 LRR と呼ばれる関係式を多項式集合に追加して変換を行う．変換には任意の多項式集合をグレブナー基底へと変換するブッフバーガーアルゴリズムの高速演算ライブラリを用いる．次に，得られたグレブナー基底を用いて多項式簡約を実行することにより，検証対象の機能が多項式集合により導出できるかどうかを判定する．本年度は，以上の形式的検証システムのプロトタイプソフトウェアを開発した．なお，開発では各種数値計算ライブラリを利用した．

さらに，前年度に規定した冗長表現を含めて定式化したガロア体表現による高次なガロア体算術演算回路の形式的検証手法を開発した．これまでの手法でも 128 ビット程度までの次数であれば検証可能であったが，実用的な暗号や誤り訂正プロセッサの機能表現では高次の算術演算（べき乗算や逆元演算など）がしばしば出現し，グレブナー基底の算出を困難としていた．そこで，高次の算術演算を検証するため，これまでの計算機代数に基づく形式的検証に自然演繹に基づく形式的検証を組み合わせる新たな検証手法を開発した．これは，高次の算術演算の機能表明が一般に高階層の記述に出現し，入力を単純に内部構造に代入した形で与えられることに着目している．代入操作により得られる機能検証は，等号付き一階述語論理の自然演繹に基づく検証により容易に検証可能とした．この拡張により，暗号プロセッサ設計に開発手法を応用する際に，高速および低消費電力暗号プロセッサに加えて，暗号実装の脅威となっている各種物理攻撃への対策を施した（対策により高次となった）プロセッサの検証も可能とした．なお，開発手法の評価は，語長が 256 ビットを越える実用的な誤り訂正符号の復号回路を網羅的に検証することで実施した．

令和元年度は，前年度までに開発した非冗長・冗長表現が混載したガロア体算術演算回路の形式的検証手法の応用として，暗号プロセッサデータパスの形式的設計・検証を実現した．設計対象は，まず，現在世界で最も利用されているブロック暗号 AES (Advanced Encryption Standard) を元に構成される認証暗号 AES-GCM とした．AES-GCM は ISO/IEC 国際標準の認証暗号方式であり，その暗号化・認証タグ生成処理全体がガロア体上の演算として記述されるため，開発した手法によるデータパス全体の設計・検証が可能である．ここでは，高速性や低消費電力性に優れたデータパス，物理攻撃への耐性を有するデータパスを有する AES ハードウェアを形式的に設計し，主要な構成要素の検証時間を評価することで，開発手法の有効性を実証した．また，現在，CAESAR プロジェクトと呼ばれる国際コンペティションにおいて，AES を基本とする認証暗号方式が国際的にいくつも提案されており，今後の活用が期待されている．そこで，AES を基本とする次世代方式への適用も合わせて検討した．具体的には，AES-OCB，AES-COLM，AES-OTR といった次世代方式への適用可能性を示した．その上で，上記で設計した暗号プロセッサのプロトタイプを ASIC で実装した場合の性能評価を実施するとともに，その物理攻撃に対する耐性実験を実施した．同実験では，本研究代表者らが開発してきた最新の物理攻撃評価ボードを用いて，物理攻撃の中でも特に強力とされるマイクロ磁界プローブによるサイドチャネル攻撃（局所電磁波解

析攻撃）に対する耐性を評価した．

令和 2 年度は，それまでに開発した冗長表現により記述されるガロア体算術演算回路の形式的設計・検証手法に基づくガロア体算術演算回路の自動生成ジェネレータを開発した．同ジェネレータは，設計仕様としてアーキテクチャ，基数，および算術アルゴリズムを入力すると，形式的に完全性を検証済みのガロア体算術演算回路の HDL 記述を自動生成するシステムである．まず，入力された仕様に応じて，本研究で開発した拡張ガロア体算術演算グラフを生成する．次に，これまでに開発したグレブナー基底に基づく検証および自然演繹に基づく検証を併用する検証システムを用いて当該グラフ表現で与えられる回路コードから回路機能を検証する．その後，検証された当該グラフを HDL の形式に変換して出力する．ここで，同変換は一対一対応で行えるため直接変換できることに注意されたい．本研究で生成する対象は，代表的なガロア体算術演算である Mastrovito 乗算と Massey-Omura 乗算とした．入力にはには同乗算の並列アーキテクチャ，基数（2〜256 の範囲）および使用するガロア体表現を与える仕様とした．開発方法としては，まず本研究者がこれまでに開発済みの他回路のジェネレータを拡張した．特に，本研究において拡張したグラフ表現の生成システムおよびグラフから HDL への変換システムを新たに開発し，それらをこれまでの検証システムに接続した．その上で，典型的な乗算器を現実的な時間（数秒程度）で生成・検証可能であることを実証した．さらに，将来的な応用を見据え，車載向けセキュリティハードウェア設計への当該システムの適用可能性を評価した．

５．主な発表論文等

〔雑誌論文〕　計24件（うち査読付論文　24件／うち国際共著　1件／うちオープンアクセス　7件）

１．著者名 Ueno Rei、Morioka Sumio、Miura Noriyuki、Matsuda Kohei、Nagata Makoto、Bhasin Shivam、Mathieu Yves、Graba Tarik、Danger Jean-Luc、Homma Naofumi	４．巻 69
２．論文標題 High Throughput/Gate AES Hardware Architectures Based on Datapath Compression	５．発行年 2020年
３．雑誌名 IEEE Transactions on Computers	６．最初と最後の頁 534～548
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TC.2019.2957355	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 Ueno Rei、Takahashi Junko、Hayashi Yu-ichi、Homma Naofumi	４．巻 1
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 1～10
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 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 Ueno Rei、 Kazumori Kohei、 Homma Naofumi	４．巻 2020
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 Ueno Rei、Fukushima Kazuhide、Nakano Yuto、Kiyomoto Shinsaku、Homma Naofumi	4．巻 12244
2．論文標題 Single-Trace Side-Channel Analysis on Polynomial-Based MAC Schemes	5．発行年 2021年
3．雑誌名 Constructive Side-Channel Analysis and Secure Design	6．最初と最後の頁 43～67
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-68773-1_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 Ito Akira、Ueno Rei、Homma Naofumi	4．巻 1
2．論文標題 Effective Formal Verification for Galois-field Arithmetic Circuits with Multiple-Valued Characteristics	5．発行年 2020年
3．雑誌名 IEEE 50th International Symposium on Multiple-Valued Logic	6．最初と最後の頁 46～51
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/ISMVL49045.2020.00-31	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 Kazumori Kohei、Ueno Rei、Homma Naofumi	4．巻 1
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 IEEE 50th International Symposium on Multiple-Valued 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 Rei Ueno, Junko Takahashi, Yu-ichi Hayashi, Naofumi Homma	4．巻 11
2．論文標題 Constructing Sliding Windows Leak from Noisy Cache Timing Information of OSS-RSA	5．発行年 2019年
3．雑誌名 Proceedings of 8th International Workshop on Security Proofs for Embedded Systems	6．最初と最後の頁 64～77
掲載論文のDOI（デジタルオブジェクト識別子） 10.29007/ws8z	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 Ville Yli-Maeyry, Daisuke Miyata, Naofumi Homma, Yuichi Hayashi, Takafumi Aoki,	4．巻 61
2．論文標題 Statistical Test Methodology for Evaluating Electromagmetic Information Leakage from Mobile Touchscreen Devices	5．発行年 2019年
3．雑誌名 IEEE Transactions on Electromagnetic Compatibility	6．最初と最後の頁 1107～1114
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TEMC.2018.2866553	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 Rei Ueno, Manami Suzuki, Naofumi Homma	4．巻 68
2．論文標題 Tackling Biased PUFs Through Biased Masking: A Debiasing Method for Efficient Fuzzy Extractor	5．発行年 2019年
3．雑誌名 IEEE Transactions on Computers	6．最初と最後の頁 1091～1104
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TC.2019.2897996	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, Yasuyuki Nogami, Takafumi Aoki	4．巻 9
2．論文標題 Highly Efficient GF(2^8) Inversion Circuit Based on Hybrid GF Representations	5．発行年 2019年
3．雑誌名 Journal of Cryptographic Engineering	6．最初と最後の頁 101～113
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/s13389-018-0187-8	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 Rei Ueno, Naofumi Homma, Tomonori Iida, Kazuhiko Minematsu	4．巻 1
2．論文標題 High Throughput/Gate FN-Based Hardware Architectures for AES-OTR	5．発行年 2019年
3．雑誌名 IEEE International Symposium on Circuits and Systems	6．最初と最後の頁 1～4
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/ISCAS.2019.8702231	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 Kazumori, Rei Ueno, Naofumi Homma	4．巻 1
2．論文標題 A Ternary Fuzzy Extractor for Efficient Cryptographic Key Generation	5．発行年 2019年
3．雑誌名 IEEE 49th International Symposium on Multiple-Valued Logic	6．最初と最後の頁 49～54
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/ISMVL.2019.00017	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 Manami Suzuki, Rei Ueno, Naofumi Homma, Takafumi Aoki	4．巻 66
2．論文標題 Efficient Fuzzy Extractors Based on Ternary Debiasing Method for Biased Physically Unclonable Functions	5．発行年 2019年
3．雑誌名 IEEE Transactions on Circuits and Systems I: Regular Papers	6．最初と最後の頁 616-629
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TCSI.2018.2869086	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 Akira Ito, Rei Ueno, Naofumi Homma, Takafumi Aoki	4．巻 5
2．論文標題 Characterizing Parallel Multipliers for Detecting Hardware Trojans	5．発行年 2018年
3．雑誌名 Journal of Applied Logics	6．最初と最後の頁 1815-1831
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 Akira Ito, Rei Ueno, Naofumi Homma, Takafumi Aoki	4．巻 1
2．論文標題 On the Detectability of Hardware Trojans Embedded in Parallel Multipliers	5．発行年 2018年
3．雑誌名 IEEE 48th International Symposium on Multiple-Valued Logic	6．最初と最後の頁 62-67
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/ISMVL.2018.00019	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 Manami Suzuki, Rei Ueno, Naofumi Homma, Takafumi Aoki	4．巻 1
2．論文標題 Quaternary Debiasing for Physically Unclonable Functions	5．発行年 2018年
3．雑誌名 IEEE 48th International Symposium on Multiple-Valued Logic	6．最初と最後の頁 7-12
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/ISMVL.2018.00010	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 Kazuhiro Oshida, Rei Ueno, Naofumi Homma, Takafumi Aoki	4．巻 1
2．論文標題 On Masked Galois-Field Multiplication for Authenticated Encryption Resistant to Side Channel Analysis	5．発行年 2018年
3．雑誌名 International Workshop on Constructive Side-Channel Analysis and Secure Design 2018	6．最初と最後の頁 44-60
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-319-89641-0_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 Rei Ueno, Naofumi Homma, Takafumi Aoki	4．巻 E100-D
2．論文標題 Automatic Generation System for Multiple-Valued Galois-Field Parallel Multipliers	5．発行年 2017年
3．雑誌名 IEICE Transactions on Information and Systems	6．最初と最後の頁 1603-1610
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transinf.2016LOP0010	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 Rei Ueno, Naofumi Homma, Takafumi Aoki, Sumio Morioka	4．巻 E100-A
2．論文標題 Hierarchical Formal Verification Combining Algebraic Transformation with PPRM Expansion and Its Application to Masked Cryptographic Processors	5．発行年 2017年
3．雑誌名 IEICE Transactions on Fundamentals of Electronics, Communications and Computer Science	6．最初と最後の頁 1396-1408
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transfun.E100.A.1396	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 Rei Ueno, Naofumi Homma, Yasuyuki Nogami, Takafumi Aoki	4．巻 1
2．論文標題 Highly Efficient GF(2^8) Inversion CIrcuit Based on Hybrid GF Representations	5．発行年 2018年
3．雑誌名 Journal of Cryptographic Engineering	6．最初と最後の頁 1-13
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/s13389-018-187-8	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 Rei Ueno, Naofumi Homma, Takafumi Aoki	4．巻 1
2．論文標題 A Systematic Design of Tamper-Resistant Galois-Field Arithmetic Circuits Based on Threshold Implementation with (d+1) Input Share	5．発行年 2017年
3．雑誌名 IEEE 47th International Symposium on Multiple-Valued Logic (ISMVL)	6．最初と最後の頁 136-141
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/ISMVL.2017.35	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 Rei Ueno, Naofumi Homma, Takafumi Aoki	4．巻 10348
2．論文標題 Toward More Efficient Tamper-Resistant AES Hardware Architecture Based on Threshold Implementation	5．発行年 2017年
3．雑誌名 International Workshop on Constructive Side-Channel Analysis and Secure Design (COSADE 2017)	6．最初と最後の頁 50-64
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-319-64647-3_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 －

1．著者名 Manami Suzuki, Rei Ueno, Naofumi Homma, Takafumi Aoki	4．巻 10348
2．論文標題 Multiple-Valued Debiasing for Physically Unclonable Functions and Its Application to Fuzzy Extractors	5．発行年 2017年
3．雑誌名 International Workshop on Constructive Side-Channel Analysis and Secure Design (COSADE 2017)	6．最初と最後の頁 248-263
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-319-64647-3_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 －

〔学会発表〕　計27件（うち招待講演　9件／うち国際学会　6件）

1．発表者名
伊東 燦

2．発表標題
決定グラフ表現に基づくハードウェアトロイ検知手法

3．学会等名
第43回多値論理フォーラム

4．発表年
2020年

1．発表者名
中嶋彩乃

2．発表標題
線形写像の最適化による高効率AES S-Boxハードウェアの設計と評価

3．学会等名
ハードウェアセキュリティ研究会

4．発表年
2021年

1．発表者名
Naofumi Homma

2．発表標題
Designing Secure Cryptographic Circuits

3．学会等名
2019 IEEE International Electron Devices Meeting（招待講演）（国際学会）

4．発表年
2019年

1．発表者名
本間尚文

2．発表標題
ハードウェアセキュリティ技術とその展望

3．学会等名
第110回ニューパラダイムコンピューティング研究会（招待講演）

4．発表年
2019年

１．発表者名
Naofumi Homma

２．発表標題
Circuit Design Resistant to Side Channel Attacks

３．学会等名
2019 Symposium on VLSI Circuits（招待講演）（国際学会）

４．発表年
2019年

１．発表者名
澤田石尚太郎，上野嶺，本間尚文

２．発表標題
ガロア体演算に基づく認証暗号の統合ハードウェアの設計，

３．学会等名
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
伊東燦，上野嶺，本間尚文

２．発表標題
ガロア体演算に基づく暗号ハードウェアにおけるHT検知技術

３．学会等名
LSIとシステムのワークショップ

４．発表年
2019年

１．発表者名
上野嶺，森岡澄夫，三浦典之，松田航平，永田真，Shivam Bhasin，Yves Mathieu，Tarik Graba，Jean-Luc Danger，本間尚文

２．発表標題
乗法的オフセットに基づく高効率AESハードウェアアーキテクチャの設計

３．学会等名
セキュリティサマーサミット2019

４．発表年
2019年

１．発表者名
伊東燦，上野嶺，本間尚文

２．発表標題
ガロア体算術に基づく暗号ハードウェアの形式的トロイフリー検証

３．学会等名
セキュリティサマーサミット2019

４．発表年
2019年

１．発表者名
伊東燦，上野嶺，本間尚文

２．発表標題
ブール多項式のZDD表現を用いたガロア体算術演算回路の形式的検証手法

３．学会等名
第42回多値論理フォーラム

４．発表年
2019年

１．発表者名
数森康平，上野嶺，本間尚文

２．発表標題
3値PUFに対する効率的なエントロピー抽出手法とその評価

３．学会等名
第42回多値論理フォーラム

４．発表年
2019年

１．発表者名
伊東燦，上野嶺，本間尚文

２．発表標題
多標数ガロア体算術演算回路の形式的検証手法

３．学会等名
第33回多値論理とその応用研究会

４．発表年
2020年

１．発表者名
伊東燦，上野嶺，本間尚文

２．発表標題
暗号ハードウェアに対する形式的ハードウェアトロイ検出手法

３．学会等名
2020年暗号と情報セキュリティシンポジウム

４．発表年
2020年

１．発表者名
小田麻矢，上野嶺，井上明子，峯松一彦，本間尚文

２．発表標題
BBB安全なインクリメンタルMACスキームとそのハードウェア実装

３．学会等名
2020年暗号と情報セキュリティシンポジウム

４．発表年
2020年

１．発表者名
数森康平，上野嶺，本間尚文

２．発表標題
PUFからの棄却サンプリングを用いた効率的な暗号鍵生成

３．学会等名
2020年暗号と情報セキュリティシンポジウム

４．発表年
2020年

１．発表者名
Naofumi Homma

２．発表標題
Recent Topics on Cryptographic Hardware Design

３．学会等名
National Tsing Hua University Seminar（招待講演）（国際学会）

４．発表年
2018年

１．発表者名
Naofumi Homma

２．発表標題
Side-Channel-Aware LSI Design

３．学会等名
2018 International Symposium on VLSI -Design, Automation and Test（招待講演）（国際学会）

４．発表年
2018年

１．発表者名
本間尚文

２．発表標題
耐タンパー性暗号LSIの設計技術

３．学会等名
LSIとシステムのワークショップ（招待講演）

４．発表年
2018年

１．発表者名
Naofumi Homma

２．発表標題
Hardware Security: Emerging Research Field in IoT Era

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

４．発表年
2018年

１．発表者名
Naofumi Homma

２．発表標題
Hardware Security: Research Field Expanding in IoT Era

３．学会等名
14th International Conference on Intelligent Information Hiding and Multimedia Signal Processing（招待講演）（国際学会）

４．発表年
2018年

１．発表者名
Ville Yli-Maeyry，上野嶺，本間尚文，青木孝文，三浦典之，松田航平，永田真，Shivam Bhasin，Yves Mathieu，Tarik Graba，Jean-Luc Danger

２．発表標題
低遅延暗号における中間ラウンドからのサイドチャネル漏えいとそのRSMに基づく効率的な対策

３．学会等名
2019年暗号と情報セキュリティシンポジウム

４．発表年
2019年

１．発表者名
伊東燦，上野嶺，本間尚文，青木孝文

２．発表標題
ガロア体ハードウェアアルゴリズムの形式的トロイフリー性検証手法

３．学会等名
2019年暗号と情報セキュリティシンポジウム

４．発表年
2019年

１．発表者名
上野嶺，本間尚文，飯田伴則，峯松一彦

２．発表標題
AES-OTRハードウェアアーキテクチャとその評価

３．学会等名
ハードウェアセキュリティ研究会

４．発表年
2018年

１．発表者名
鈴木　麻奈美

２．発表標題
バイアスを含むPUFに対する高効率な4値デバイアシング

３．学会等名
2018年暗号と情報セキュリティシンポジウム

４．発表年
2018年

１．発表者名
上野　嶺

２．発表標題
偏位マスキングに基づくファジー抽出器の構成

３．学会等名
2018年暗号と情報セキュリティシンポジウム

４．発表年
2018年

１．発表者名
上野　嶺

２．発表標題
乱数オーバーヘッドを抑制した耐タンパー性AES暗号ハードウェア

３．学会等名
2018年暗号と情報セキュリティシンポジウム

４．発表年
2018年

１．発表者名
本間　尚文

２．発表標題
IoT時代の情報セキュリティ技術

３．学会等名
みやぎ高度電子機械産業振興協議会・エレクトロニクス実装学会セミナー（招待講演）

４．発表年
2018年

〔図書〕　計1件

１．著者名	４．発行年
Wieland Fischer, Naofumi Homma	2017年
２．出版社	５．総ページ数
Springer International Publishing	XIV, 710
３．書名	
Cryptographic Hardware and Embedded Systems - CHES 2017	

〔産業財産権〕

〔その他〕

東北大学電気通信研究所環境調和型セキュア情報システム研究分野
http://www.ecsis.riec.tohoku.ac.jp/

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
連携研究者	青木　孝文 (Aoki Takafumi) (80241529)	東北大学・情報科学研究科・教授 (11301)	
連携研究者	上野　嶺 (Ueno Rei) (80826165)	東北大学・電気通信研究所・助教 (11301)	

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			
シンガポール	Nanyang Technological University			
フランス	Telecom Paris			