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　２ 年　 ６ 月　 １ 日現在

機関番号：１１３０１
研究種目：研究活動スタート支援
研究期間：2018～2019
課題番号：１８Ｈ０６４５６・１９Ｋ２１５２６

研究課題名（和文）演算中に生じた誤りを訂正する機構を備えた暗号ハードウェアの設計手法の開発

研究課題名（英文）Development of cryptographic hardware with concurrent error-correcting scheme

研究代表者
上野　嶺（Ueno, Rei）

東北大学・電気通信研究所・助教

研究者番号：８０８２６１６５

交付決定額（研究期間全体）：（直接経費）　　2,300,000円

研究成果の概要（和文）：本研究では，高効率かつ高信頼な暗号ハードウェアの設計法の開発を行った．まず，数系変換などのデータパス最適化手法を組み合わせることで世界最高効率のAES暗号データパスを設計した．同データパスはパイプライン化と組み合わせた検算が容易に実装できるようになっており，高効率に演算誤りを検知または修正できるよう拡張が可能である．次に，タンパー手段を用いた攻撃などに対しても高安全かつ高信頼な暗号鍵ストレージを開発した．本成果では，物理複製困難関数と呼ばれる回路に安全かつ高効率に適用可能な誤り訂正スキームを開発し，その暗号鍵ストレージへの応用を示した．

研究成果の学術的意義や社会的意義
本成果は主に暗号ハードウェアおよび物理複製困難関数に基づく耐タンパー性暗号鍵ストレージの高効率化・高安全化・高信頼化に貢献している．暗号ハードウェアと暗号鍵ストレージの設計・実装コストを大幅に削減することで多くの情報システム，特にリソースの厳しいIoTシステムにおけるセキュリティ機能の導入が容易になり，本成果は安全な情報社会の実現に貢献するものと期待している．本成果は学術的にも高く評価されており，当該分野における世界最高峰の学術論文誌に複数論文が採択された他，本成果に関して招待講演も行っている．

研究成果の概要（英文）：I have developed a design methodology for highly efficient and reliable cryptographic hardware. Firstly, I have designed the world most efficient AES hardware based on a combination of optimization techniques such as transformation of Galois field. The designed hardware is suitable to and efficiently adoptable of concurrent error-detecting/correcting schemes with pipelining due to the structural feature of the designed hardware. Secondly, I have developed a highly reliable cryptographic key storage on the basis of physically unclonable function (PUF), which is resistant to tampering attacks. For securely storing cryptographic key and reliably reconstructing (i.e., reading) it, we developed novel error-correcting schemes based on multiple-valued encoding of PUF response, ternary von Neumann corrector, and rejection sampling. The error-correcting scheme achieves 128-bit cryptographic key storage with less hardware cost than any other conventional PUF-based one.

研究分野：ハードウェアセキュリティ

キーワード：ハードウェアセキュリティ　暗号実装　情報セキュリティ　算術演算回路　VLSI

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

個人情報の保護や安全な電子商取引への要求に伴い，ガロア体算術に基づく暗号ハードウェアの応用が急速に拡大している．これまで想定もされなかった環境下においても暗号ハードウェアが利用されており，さらなる高信頼・耐タンパー性暗号ハードウェアが求められている．一例として，暗号ハードウェア地上とは比較ならない強度の中性子線が飛び交う宇宙空間での利用のためにロケットや衛星にも搭載されつつある．このような頻発にソフトエラーが発生しうる極限的な環境下においては，演算誤りを検知するだけでは情報セキュリティの三大要件である可用性を維持することができない．また，レーザー照射や電磁波印加，不正な電源電圧操作などにより意図的に暗号ハードウェアの演算誤りを誘発し，その誤り方を解析することで秘密鍵を抽出する故障解析攻撃手法も年々高度化している．これらの環境からの負荷や故障解析攻撃に対しても正常かつ情報を漏洩せず暗号処理が可能な暗号ハードウェアが強く求められていることから，演算中の誤りを効率的に訂正可能なガロア体算術演算データパスの設計技術の開発という本研究の着想に至った．

２．研究の目的

本研究では，上記のような極限的な環境下においても可用性および耐タンパー性を有する暗号ハードウェアの設計手法の開発を目的とする．具体的には，極限的な環境とは非意図的なソフトエラーが頻繁に起きる宇宙空間などの物理的に過酷な環境や，レーザー照射などによる故障解析攻撃が可能な環境を指す．

上記目的を実現するために，暗号ハードウェアの大部分はガロア体算術演算データパスが占めることから，演算中に生じた誤りを訂正する機能を有する冗長ガロア体算術演算データパスの設計手法の理論的基礎の確立を目指す．冗長ガロア体算術演算回路により，ソフトエラーが頻繁に発生する環境下において正常に暗号化を実現できるだけでなく，上記のセーフエラー攻撃に対する対策としも有効であると考えられる．これまで誤り検出が可能なガロア体算術演算回路に関しては回路設計分野や暗号実装の分野では報告があったものの，本研究で扱う，冗長ガロア体算術に基づく誤り訂正が可能なガロア体算術演算データパスはこれまで例が無く，本研究はこれまでの暗号ハードウェア設計手法では達成しえなかった信頼性と耐タンパー性を有する情報システムの創造に貢献すると期待される．

３．研究の方法

本研究では，高信頼・高効率暗号データパスの開発に主に着目する．暗号データパスの開発では，これまで本研究者が行ってきたガロア体の数系変換や冗長表現に基づくガロア体算術演算回路の最適化技術に加え，暗号演算を効率的に実装するための最適な命令順序を検討することで，低遅延・少消費電力かつ誤り検出・訂正スキームを効率的に適用可能な暗号データパス構成を目指す．その上で，冗長ガロア体算術やパイプライン化を用いたオンザフライ検算スキームなど様々な誤り検出・訂正スキームの適用を検討し，高効率かつ高信頼な暗号データパスの開発を目指す．

さらに本研究では，実用的な暗号ハードウェアの開発を目的として，暗号データパスのみならず暗号鍵を安全に格納するための耐タンパー性暗号鍵ストレージの開発も並行して行う．ここで，半導体の微小な製造ばらつきを利用してハードウェア固有の値を生成する物理複製困難関数（PUF: Physically Unclonable Function）に着目する．PUF は物理複製困難性や外部から PUF の値の読み取りに係る困難性から耐タンパー性暗号鍵ストレージの実現に期待されているが，PUF は制御不可能な物理的ばらつきを用いるため値を制御することが困難であるという問題や PUF の出力はノイズを含み安定しないという問題がある．そこで，ファジー抽出器（FE: Fuzzy Extractor）と呼ばれる誤り訂正機構が用いられている．本研究では，この FE を効率や安全性の観点から改良することで，ノイズやタンパー手段を用いた攻撃に対して頑強かつ効率的な暗号鍵ストレージを開発する．

４．研究成果

本研究で得られた主たる成果として，故障注入攻撃や環境不可によるソフトエラーを考慮しても高信頼に処理を実現可能な暗号ハードウェアの開発を行った．具体的には，まず，世界で最も広く用いられている国際標準の共通鍵暗号 Advanced Encryption Standard (AES)に着目し，現実的なシナリオにおいて高効率に暗号化と復号を実現できるハードウェアを開発した．開発したハードウェアは数系変換などの数学的な技法とレジスタリタイミングや命令順序交換などの回路設計における技法を最適に組み合わせることで小さい回路面積で低遅延を達成した．さらに，開発したハードウェアを既存のハードウェアと同条件下で合成およびシミュレーションすることで性能評価を行った．その結果から，提案手法は従来の AES 暗号ハードウェアに対し約半分のエネルギーで暗号化および復号が可能なことを確認した（図 1）．また，設計したハードウェアはデータパスの冗長化や検算などの故障に対する対策を効率的に適用可能な回路構成をと

っており高信頼化を比較的少ないオーバーヘッドで実現可能である．

さらに，高信頼・高安全な耐タンパー性暗号鍵ストレージの構成法を開発した．同手法はハードウェアの各個体に固有の乱数を生成する回路である PUF に基づいており，FE による誤り訂正と，本研究で開発した乱数抽出手法を組み合わせることで安全かつ高効率な鍵ストレージを実現する（図 2）．シミュレーションの結果，提案手法は従来手法と比べ最大約 60%小さいハードウェアコストで安全性が保証された 128 ビット暗号鍵ストレージを実現できることを確認した．

これらの成果は計算機学に関する世界最高峰の学術論文誌である IEEE Transactions on Computers や IEEE Transactions on Circuits and Systems などに採択されている．

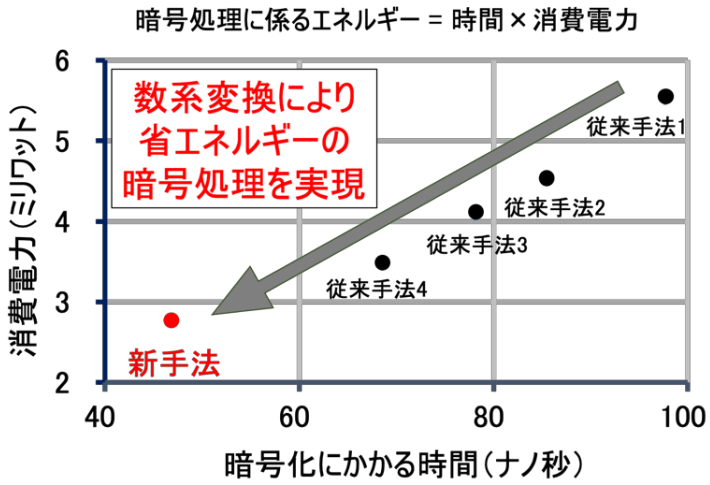

図 1: 設計した AES 暗復号ハードウェアと既存手法の遅延と消費電力の比較．設計したハードウェアは遅延・消費電力両方の観点から従来手法よりも大きく優れており，結果として約半分の消費エネルギーで暗号処理が可能なことを確認した．

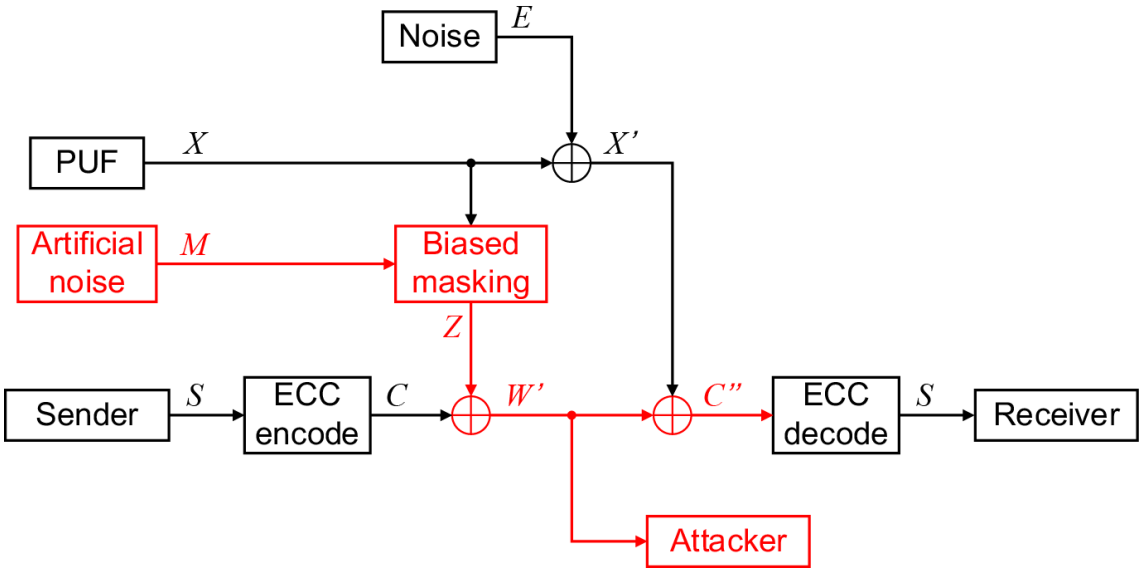

図 2: 開発した耐タンパー性暗号鍵ストレージのブロック図．赤で示した箇所は人工的なノイズにより秘密情報が適切にマスクされた箇所であり，これによりタンパー手段を用いた秘密情報の抽出を困難とする．さらに，通常の FE と同様誤り訂正符号を用いて PUF のノイズと上述のノイズを除去することで安全性と信頼性を両立する．

５．主な発表論文等

〔雑誌論文〕　計6件（うち査読付論文　6件／うち国際共著　1件／うちオープンアクセス　2件）

１．著者名 Ueno Rei、Suzuki Manami、Homma Naofumi	４．巻 0
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 1～1
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 9
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 1815～1832
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 Ueno Rei、Homma Naofumi、Nogami Yasuyuki、Aoki Takafumi	４．巻 9
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 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 オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Ueno Rei、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 Suzuki Manami、Ueno Rei、Homma Naofumi、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 2018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.2018.286908	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Ueno Rei、Takahash Junkoi、Hayashi Yu-ichii、Naofumi Homma	４．巻 N/A
２．論文標題 A method for constructing sliding windows leak with noise in cache timing information	５．発行年 2020年
３．雑誌名 Journal of Cryptographic Engineering	６．最初と最後の頁 ～
掲載論文のDOI（デジタルオブジェクト識別子） 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 －

〔学会発表〕　計32件（うち招待講演　1件／うち国際学会　8件）

１．発表者名 遠藤空
２．発表標題 数論変換に基づくRing-LWE暗号ハードウェアの高効率実装に関する検討
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 森隼人
２．発表標題 OSS-RSAからのキャッシュリークの取得容易性評価
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
上野嶺

２．発表標題
Weak PUFを用いた耐タンパー性暗号鍵ストレージの構成法

３．学会等名
ハードウェアセキュリティフォーラム2018

４．発表年
2018年

１．発表者名
上野嶺

２．発表標題
偏位マスキングの多値化PUFへの拡張とその暗号鍵生成への応用

３．学会等名
第32回多値論理とその応用研究会

４．発表年
2019年

１．発表者名
上野嶺

２．発表標題
情報理論的安全性を有する鍵長可変MACハードウェアアーキテクチャの設計

３．学会等名
2019年暗号と情報セキュリティシンポジウム（SCIS 2019）

４．発表年
2019年

１．発表者名
上野嶺

２．発表標題
Poly1305への単一波形を用いたサイドチャネル攻撃とその実現可能性の評価

３．学会等名
2019年暗号と情報セキュリティシンポジウム（SCIS 2019）

４．発表年
2019年

１．発表者名
上野嶺

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（SCIS 2019）

４．発表年
2019年

１．発表者名
Ville Yli-Maeyry

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（SCIS 2019）

４．発表年
2019年

１．発表者名
澤田石尚太郎

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

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

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
サーマーセキュリティサミット2019

４．発表年
2019年

１．発表者名
伊東燦

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
サーマーセキュリティサミット2019

４．発表年
2019年

１．発表者名
大澤創紀

２．発表標題
暗号ソフトウェアの高精度なキャッシュタイミング解析とその評価

３．学会等名
2019年度電気関係学会東北支部連合大会

４．発表年
2019年

１．発表者名
小田麻矢

２．発表標題
メモリ完全性検証のための軽量かつ高速なMACハードウェアの設計

３．学会等名
2019年度電気関係学会東北支部連合大会

４．発表年
2019年

１．発表者名
伊東燦

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

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
門脇悠真

２．発表標題
ペアリング暗号ハードウェアの相関電磁波解析に関する検討

３．学会等名
ハードウェアセキュリティ研究会

４．発表年
2019年

１．発表者名
船越秀隼

２．発表標題
剰余数系を用いた同種写像暗号ハードウェアアーキテクチャの設計に関する検討

３．学会等名
ハードウェアセキュリティ研究会

４．発表年
2019年

１．発表者名
伊東燦

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
上野嶺

２．発表標題
確率的計算手法を用いた秘密計算に関する検討

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
上野嶺

２．発表標題
ストカスティック計算に基づく確率的準同型暗号の構成に関する検討

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
伊東燦

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

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

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
Kohei Kazumori

２．発表標題
A Ternary Fuzzy Extractor for Efficient Cryptographic Key Generation

３．学会等名
IEEE 49th International Symposium on Multiple-Valued Logic (ISMVL)（国際学会）

４．発表年
2019年

１．発表者名
Rei Ueno

２．発表標題
High Throughput/Gate FN-Based Hardware Architectures for AES-OTR

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

４．発表年
2019年

１．発表者名
Rei Ueno

２．発表標題
Collision-Based EM Analysis on ECDSA Hardware and a Countermeasure

３．学会等名
Joint International Symposium on Electromagnetic Compatibility and Asia-Pacific International Symposium on Electromagnetic Compatibility (Joint IEEE EMC & APEMC 2019) (国際学会)

４．発表年
2019年

１．発表者名
Rei Ueno

２．発表標題
onstructing Sliding Windows Leak from Noisy Cache Timing Information of OSS-RSA

３．学会等名
8th International Workshop on Security Proofs for Embedded Systems (PROOFS 2019) (国際学会)

４．発表年
2019年

１．発表者名
Rei Ueno

２．発表標題
Automatic Generation of Formally-Proven Tamper-Resistant Galois-Field Multipliers Based on Generalized Masking Scheme

３．学会等名
Workshop on Top Picks in Hardware and Embedded Security (国際学会)

４．発表年
2019年

１．発表者名
Rei Ueno

２．発表標題
Hardware Implementation of Block Cipher: Case Study Using AES

３．学会等名
The 9-th Asian-workshop on Symmetric Key Cryptography (ASK2019) (招待講演) (国際学会)

４．発表年
2019年

１．発表者名
Rei Ueno

２．発表標題
Single-Trace Side-Channel Analysis on Polynomial-based MAC Schemes

３．学会等名
International Workshop on Constructive Side-Channel Analysis and Secure Design (COSADE 2020)（国際学会）

４．発表年
2020年

１．発表者名
Maya Oda

２．発表標題
PMAC++: Incremental MAC Scheme Adaptable to Lightweight Block Ciphers

３．学会等名
IEEE International Symposium on Circuits and Systems (ISCAS 2020)（国際学会）

４．発表年
2020年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

Arithmetic Module Generator
www.ecsis.riec.tohoku.ac.jp/topics/amg

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