様　式　Ｆ－１９－２

科学研究費助成事業　　研究成果報告書

平成 ３０ 年　 ５ 月 ２５ 日現在

機関番号：１１３０１
研究種目：国際共同研究加速基金（国際共同研究強化）
研究期間：2016～2017
課題番号：１５ＫＫ０００１

研究課題名（和文）ガロア体算術演算に基づくVLSIデータパスの形式的設計技術の開拓（国際共同研究強化）

研究課題名（英文）Development of formal design methodology for VLSI datapaths based on Galois-field arithmetic operations(Fostering Joint International Research)

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）　　11,100,000円
渡航期間：　　６ヶ月

研究成果の概要（和文）：本研究では，ガロア体上の算術演算として記述される攻撃対策を施した耐タンパー性暗号プロセッサの形式的設計技術の確立を目指し，その形式的記述・検証手法を開発した．また，その応用として高効率な耐タンパー性暗号プロセッサの設計・開発を行った．特に，近年暗号プロセッサに物理的に直接アクセスして秘密情報を奪うサイドチャネル攻撃の脅威が急速に高まっていることから，サイドチャネル攻撃対策に着目し，同対策を施した暗号プロセッサの形式的設計・検証手法の開発および同対策を施した暗号プロセッサの試作・評価を推進した．

研究成果の概要（英文）：This research has developed a formal description and verification method of tamper resistant cryptographic processors with attack countermeasures described as arithmetic operations on the Galois field in order to establish a formal design methodology of tamper resistant cryptographic processors. In addition, we have designed and developed highly efficient tamper resistant cryptographic processors as its application. In particular, since the threat of side-channel attack which directly accesses cryptographic processors to retrieve secret information is rapidly increasing, we focused on countermeasures against side-channel attacks and formally designed cryptographic processors resistant to that kind of attacks, and also performed the prototyping and evaluation of designed cryptographic processors.

研究分野：計算機科学

キーワード：計算機システム

１．研究開始当初の背景

平成 25 年度から 28 年度にかけて採択された科研費では，暗号や誤り訂正処理 LSI において近年重要性が急速に高まっているガロア体上の算術演算回路の形式的設計技術の確立を目指し，その形式的記述・検証手法の開発およびそれを応用した自動生成システムの構築に取り組んだ．当初計画通りの研究成果が得られており，特にガロア体上の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)」の理論を構築するとともに，多項式・正規基底表現されたガロア体上の並列乗算器を GF-ACG により網羅的に設計・検証することに成功している．上記の研究成果は，世界最高峰の学術論文誌および国際会議に採録されるなど，当該分野において世界的に高く評価されている．これまでの研究により，開発した代数的な手法を用いることで，語長が 100 ビットを越える実用的な暗号プロセッサの完全な検証を実現可能との見通しが得られた．そこで，その成果を発展させ，仏国 Telecom ParisTech で開発が進められる最先端のセキュリティ検証と組み合わせた耐タンパー性暗号プロセッサの形式的設計・検証手法を開発し，機能およびセキュリティプロパティが完全に保証された耐タンパー性暗号プロセッサを設計・試作するという本研究の着想を得た．

２．研究の目的

本研究では，ガロア体上の算術演算として記述される攻撃対策を施した耐タンパー性暗号プロセッサの形式的設計技術の確立を目指し，その形式的記述・検証手法の開発を目的とした．特に，近年暗号プロセッサに物理的に直接アクセスして秘密情報を奪うサイドチャネル攻撃の脅威が急速に高まっている一方で，サイドチャネル攻撃耐性を有する暗号プロセッサの設計は高度に専門的な知識が必要とされ，またその機能検証も困難な状況であった．そこで，本研究では，そうしたサイドチャネル攻撃対策を対象として，下記の 2 項目の研究を推進した．

(I)　サイドチャネル攻撃対策を施した暗号プロセッサの形式的設計・検証手法の開発
(II)　サイドチャネル攻撃対策を施した暗号プロセッサの試作・評価

３．研究の方法

本研究では，上記で挙げた，ガロア体上の算術演算として記述されるサイドチャネル攻撃対策を施した暗号プロセッサの形式的記述・検証手法の開発とその応用としての高効率・耐タンパー性 AES 暗号プロセッサの試作・評価を以下の通り推進した．

(I) サイドチャネル攻撃対策を施した暗号プロセッサの形式的設計・検証手法の開発

元となった科研費にて開発したガロア体上の算術演算回路の形式的設計・検証手法を拡張して，サイドチャネル攻撃対策も含めた形式的設計・検証手法の開発を行った．ここでは，特に代表的なマスキングもしくはハイディングを実現するアルゴリズムレベルおよび論理回路レベルでの対策を対象とした．これは，AES 等の暗号化・復号処理全体がガロア体上の演算として代数的に記述されるのと同様に，同対策も代数的な表現が可能であり，GF-ACG によるデータパス全体の記述・検証が可能との着想を得たためである．まず，対策手法の代数的な表現に向けた GF-ACG の拡張を施すとともに，サイドチャネル攻撃対策を施したデータパス全体の機能検証に取り組んだ．その際重要となるのは，単なる機能検証だけでなく，演算の過程でマスクのはがれた危険な状態が生じないというセキュリティプロパティの検証も合わせて行うことであった．セキュリティプロパティの検証手法については，仏国 Telecom ParisTech の Sylvain Guilley 教授，Jean-Luc Danger 教授らと連携して開発を進めた．

(II) サイドチャネル攻撃対策を施した暗号プロセッサの試作・評価

上記形式的手法で設計・検証された暗号プロセッサを試作・評価した．元となった科研費で開発してきたガロア体算術演算回路ジェネレータの応用として，多様な AES 暗号プロセッサを試作した．仕様としては，実用的な高速・低消費電力プロセッサに加えて，上記で開発したサイドチャネル攻撃対策を施したプロセッサも試作した．具体的には，代表的なループアーキテクチャにおいて乱数マスクによるマスキング対策を施した AES プロセッサを試作し，その安全性を評価した．

４．研究成果

上記で挙げた 2 項目に対して，それぞれ以下の研究成果が得られた．

これまでに開発したガロア体上の算術演算回路の形式的設計・検証手法を拡張して，サイドチャネル攻撃に耐性を有する暗号プロセッサの形式的設計・検証手法を開発した．特に，代表的な共通鍵暗号方式である AES を対象として，ガロア体上の算術演算として記述されるマスキング対策も含めた完全な検証を実現するとともに，同マスキング対策で求められるセキュリティプロパティの形式的検証に世界で初めて成功した．

また，上記で開発した形式的手法で設計・検証された暗号プロセッサを試作するとともに，その安全性を実験的に実証した．まず，低遅延の軽量暗号として知られる PRINCE を対象として世界最低遅延 PRINCE 暗号プロセッサを試作・評価した（図 1）．同成果は回路設計における主要な国際会議の一つである VLSI に採択された．さらに，国際標準暗号 AES を対象として，耐タンパー性と効率を両立する AES 暗号プロセッサを試作し，本研究者らが開発・公開するサイドチャネル攻撃標準評

価ボード（SASEBO）上に同暗号プロセッサを実装し，ディジタルオシロスコープを用いてサイドチャネル情報を計測・解析する実験システムを構築し，100 万程度の計測を行っても秘密情報が１ビットも漏えいしないことを確認した．さらに，演算効率も世界最高水準であることを同ボード上で確認した．

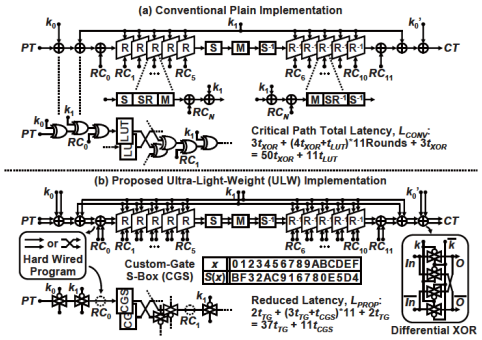

図１：設計・試作した超軽量 PRINCE 暗号プロセッサの概観

５．主な発表論文等

〔雑誌論文〕（計　4　件）

1. Daisuke Ishihata, Naofumi Homma, Yu-ichi Hayashi, Noriyuki Miura, Daisuke Fujimoto, Makoto Nagata, and Takafumi Aoki, “Enhancing Reactive Countermeasure against EM Attacks with Low Overhead,” 2017 IEEE International Symposium on Electromagnetic Compatibility, pp. 399–404, August 9, 2017.査読有
2. Noriyuki Miura, Kohei Matsuda, Makoto Nagata, Shivam Bhasin, Ville Yli-Mayry, Naofumi Homma, Yves Mathieu, Tarik Graba, and Jean-Luc Danger, “A 2.5ns-Latency 0.39pJ/b 289μm^2/Gb/s Ultra-Light-Weight PRINCE Cryptographic Processor,” 2017 Symposium on VLSI Circuits, Digest of Technical Papers, pp. C266-C267, June 2017. 査読有
3. Rei Ueno, Naofumi Homma, Sumio Morioka and Takafumi Aoki “Automatic Generation of Formally-Proven Tamper-Resistant Galois-Field Multipliers Based on Generalized Masking Scheme,” Design, Automation and Test in Europe Conference and Exhibition 2017 (DATE 2017), pp. 978-983, March 29, 2017. 査読有
4. Ville Yli-Mäyry, Naofumi Homma, and Takafumi Aoki, “Chosen-Input Side-Channel Analysis on Unrolled Light-Weight Cryptographic Hardware,” The 18th International Symposium on Quality Electronic Design, pp. 301-306, March 15, 2017. 査読有

〔学会発表〕（計　9　件）

1. 大須賀彩希，藤本大介，林優一，本間尚文，Arthur Beckers，Josep Balasch，Benedikt Gierlichs，Ingrid Verbauwhede，“サイドチャネル情報を用いた乱数生成器への非侵襲な周波数注入攻撃，”2018 年暗号と情報セキュリティシンポジウム（SCIS 2018），No. 2D2-2，新潟，January 2018.
2. 忍田大和，上野嶺，本間尚文，青木孝文，仲野有登，福島和英，清本晋作，“ガロア体乗算に基づく認証タグ生成に対する代数的サイドチャネル攻撃，”2018 年暗号と情報セキュリティシンポジウム（SCIS 2018），No. 1D1-6，新潟，January 2018.
3. ヴィッレウリマウル，宮田大輔，林優一，本間尚文，青木孝文，“スマートデバイスからの電磁的情報漏えいに対する安全性評価手法，”2018 年暗号と情報セキュリティシンポジウム（SCIS 2018），No. 1D1-3，新潟，January 2018.
4. 宮田大輔，ヴィッレウリマウル，本間尚文，林優一，青木孝文 “スマートデバイスからの電磁的情報漏えいの評価に関する検討，”ハードウェアセキュリティフォーラム 2017，ポスターNo.11，東京，December 2017.
5. 鈴木麻奈美，上野嶺，本間尚文，青木孝文，“多値化 PUF に基づく効率的なファジー抽出器の設計，” 2017 年暗号と情報セキュリティシンポジウム，那覇，Vol. 3C1-5，pp.1--8，January 27，2017.
6. ヴィッレウリマウル，本間尚文，青木孝文，“アンロールド軽量暗号ハードウェアに対する選択平文型高効率サイドチャネル解析，” 2017 年暗号と情報セキュリティシンポジウム，那覇,Vol. 3C1-5，pp.1--6，January 26，2017.
7. 忍田大和，上野嶺，本間尚文，青木孝文 “認証付き暗号の耐タンパー性ガロア体乗算に対するサイドチャネル攻撃，”2017 年暗号と情報セキュリティシンポジウム，那覇,Vol. 3C1-4，pp.1--7，January 26，2017.
8. 上野嶺，本間尚文，青木孝文 “1 階 TI に基づく耐タンパー性を有する高効率 AES 暗号ハードウェアの実装，”2017 年暗号と情報セキュリティシンポジウム，那覇,Vol. 3C1-2，pp.1--7，January 26，2017.
9. 上野嶺，本間尚文，青木孝文，"冗長表現に基づく耐タンパー性ガロア体算術演算回路の設計に関する検討," 第 30 回多値論理とその応用研究会，No. 8，pp.

38--43, 金沢, January 8, 2017.

〔その他〕
ホームページ等
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
(1)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

(2)研究協力者
〔主たる渡航先の主たる海外共同研究者〕
Jean-Luc Danger
COMELEC・Professor・Telecom ParisTech, France