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

平成　２９　年　　４　月　２７　日現在

機関番号：　１１３０１
研究種目：　基盤研究(A)（一般）
研究期間：　2013～2016
課題番号：　２５２４０００６

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

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

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）　　24,800,000円

研究成果の概要（和文）：本研究では，ガロア体上の算術演算によって構成されるVLSIデータパスの形式的設計技術を開発した．まず，(1)暗号や誤り訂正に多用される多項式基底・正規基底に基づくガロア体上の算術演算回路の形式的表現を考案し，(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の形式的設計・検証を実現した．具体的には，ISO/IEC国際標準ブロック暗号の一つであるAESを対象として，そのプロセッサデータパスの形式的設計を実現した．さらに，(4)多様な設計仕様に応じてガロア体算術演算回路を自動合成するジェネレータを開発した．

研究成果の概要（英文）：This research project developed a formal design methodology for VLSI datapaths consisting of arithmetic operations on Galois fields. First, we provided (1) a formal description for Galois-field arithmetic circuits based on polynomial basis and normal basis which are frequently used for cryptography and error-correction code, and then developed (2) a formal verification method, which is applicable to the circuit description, using computer algebra. In addition, (3) we applied the design and verification methods to a cryptographic processor. More precisely, we designed a processor datapath for AES, which is one of the ISO/IEC international standard block ciphers, by the developed method. Furthermore, we developed an automatic generator for generating a variety of Galois-field arithmetic circuits depending on various design specification.

研究分野：　計算機科学

キーワード：　計算機システム　LSI設計技術　ハードウェアセキュリティ

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 ビット以上の演算のため，シミュレーションによる完全な検証は不可能である．さらに暗号理論の分野では，暗号処理を実行する回路のバグを利用して秘密情報を奪う攻撃も報告されている．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強く望まれている．

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．一方で，本研究代表者は，暗号研究の第一人者である Adi Shamir 教授らとの共同研究を通して，暗号プロセッサの設計および安全性検証法を体系化してきた実績を有する．

本研究では，これまでに培ってきた上記技術を深化・拡張し，ガロア体算術演算回路の形式的設計技術を開拓することを目指した．

２．研究の目的

本研究では，ガロア体上の算術演算に基づく VLSI プロセッサデータパスの形式的設計技術の確立を目指し，形式的記述・検証手法から自動生成システムの開発までの下記 4 項目を目的とする．

(1) ガロア体上の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整数演算向けの形式的表現手法をもとに，ガロア体算術演算回路の形式的表現手法を開発する．具体的には，整数環とガロア体の代数的な類似性に着目し，ガロア体を基底集合，係数ベクトル集合，既約多項式により形式的に表現できることを明らかにする．また，基底集合の階層的な表現により拡大体・合成体を含む任意のガロア体を記述できることを示す．

(2) ガロア体上の算術演算回路の形式的検証手法の開発
これまでに開発した整数演算向けの形式的検証手法[2]をもとに，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，検証の中心となる連立代数方程式の解法において，ガロア体の既約多項式による簡約を用いて計算時間の爆発的増加を抑制する機構を開発する．また，開発した手法により，語長が 128 ビット以上のガロア体算術演算回路も形式的に検証可能なことを実証する．

(3) 暗号プロセッサの形式的設計・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・検証が可能となることを実証する．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 128 ビット AES（Advanced Encryption Standard）プロセッサの形式的設計・検証を実現する．主要演算である逆元演算に Table 実装や合成体を用いた高速・低消費電力プロセッサに加えて，サイドチャネル攻撃への対策を施したプロセッサも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
形式的手法で設計・検証された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する．本ジェネレータは，仕様としてアーキテクチャ，基数，既約多項式を入力すると，それに応じて形式的に機能を完全が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，上述の研究目的を 4 年間で達成した．平成 25 年度は，多項式基底表現されたガロア体算術演算回路の形式的表現手法および同表現に対する形式的検証手法を開発した．平成 26 年度は，前年度に開発した多項式基底の形式的表現・検証手法を拡張し，正規基底表現されたガロア体算術演算回路の設計・検証手法を開発した．平成 27 年度は，前年度までに開発・拡張したガロア体算術演算回路の設計・検証手法を応用し，暗号プロセッサデータパスの形式的設計および設計したデータパスの安全性解析を行った．平成 28 年度は，前年度までに開発・拡張したガロア体算術演算回路の形式的設計・検証

手法を応用し，設計仕様（アーキテクチャ，基数および算術アルゴリズム）に応じてガロア体算術演算回路の HDL 記述を自動生成するジェネレータを開発した.

４．研究成果

(1)平成 25 年度は，下記の 2 項目について研究成果を得た.

①多項式基底表現されたガロア体算術演算回路の形式的表現手法の開発

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)」の理論を構築した．多項式基底表現されたガロア体は，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”が多項式表現されたガロア体では“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必要がある．以上の観点から，基底の集合，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を形式的に定義する手法を考案した．定義されるガロア体はプログラム言語におけるいわゆる変数の型に相当する．その変数を用いて GF-ACG を定式化した.

②多項式基底表現されたガロア体算術演算回路の形式的検証手法の開発

上記で開発する GF-ACG が表す回路機能の形式的検証手法の理論を構築した．その基本アイデアは，検証対象となる（ガロア体上の算術演算で表現される）回路機能の正当性を判定する問題を多項式イデアル所属問題に帰着させることである．開発手法では，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．この変換にはブッフバーガーアルゴリズムを用いた．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．本研究では，以上の形式的検証手法を定式化するとともに，そのプロトタイプソフトウェアを開発した.

(2)平成 26 年度は，下記の 2 項目について研究成果を得た.

①正規基底表現されたガロア体算術演算回路の形式的表現手法の開発

前年度に規定した多項式基底表現されたガロア体の定義を正規基底表現に拡張するため，グラフノードの定義と有向辺（信号データのフローを表す）の分割・結合方法を拡張した．正規基底表現は，逆元演算器などをコンパクトに設計する際に有利であるが，多項式基底表現と比べて次数が指数関数的に増大するため，計算機代数による検証時間が大幅に増大することが予想された．そこで，検証過程で適宜次数を削減する機構を新たに導入することで多項式基底表現されたガロア体と同程度まで検証時間を抑制した．多項式基底表現に加えて正規基底表現にも対応することにより，暗号プロセッサ設計に開発手法を応用する際に，従来の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サイドチャネル攻撃への対策を施したプロセッサの形式的設計も可能とした.

②多項式基底表現されたガロア体算術演算回路の形式的検証手法の開発

上記の拡張に合わせて検証システムも拡張した．前年度開発した検証手法に，検証過程で適宜次数を削減する機構を搭載し，その有効性を評価した．開発手法の評価は，前年度と同様に正規基底表現されたガロア体上の並列乗算器を網羅的に設計・検証することで行った.

(3)平成 27 年度は，前年度までに開発・拡張したガロア体上の算術演算回路の設計・検証手法を応用し，暗号プロセッサデータパスの形式的設計に取り組んだ．設計対象としては，現在世界で最も利用されている ISO/IEC 国際標準ブロック暗号である AES を選定した．AES はその暗号化・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ため，提案手法によるデータパス全体の記述・検証が可能である．現在のブロック暗号は AES と同様に処理全体が代数的に表現されることが多いため，AES に適用できれば他の暗号への応用も期待できる．ここでは，まず，高速性や低消費電力性に優れたデータパス，サイドチャネル攻撃への耐性を有するデータパスを用いて形式的に設計し，主要な構成要素の検証時間を評価した．次に，上記で設計した暗号プロセッサを ASIC セミカスタム設計し，その性能評価を実施した．特に，回路面積や消費電力，演算速度を従来回路と比較し，同等の性能を有する回路を設計可能であることを確認した．さらに，設計した回路のサイドチャネル攻撃に対する耐性を実験的に検討した．本実験では，本研究代表者らが開発したサイドチャネル攻撃標準評価ボード SASEBO-R に ASIC を搭載し，マイクロ磁界プローブ等を用いて消費電力・放射電磁波を測定した．測定した波形の評価には，現在最も強力な攻撃の一つである選択平文型の電力・電磁波解析を用いた．また，Xilinx FPGA のディジタルクロック制御機能を利用して意図的に発生させたグリッチを用いた故障利用攻撃実験も実施した.

(4)平成 28 年度は，前年度までに開発・拡張してきた形式的設計・検証手法を応用し，設計仕様（アーキテクチャ，基数および算術アルゴリズム）に応じてガロア体算術演算回路の HDL 記述を自動生成するジェネレータを開発した．同ジェネレータは，まず，入力され

た仕様に応じて開発した回路表現（GF-ACG）を生成する．次に，そのコードからグレブナー基底を導出し，多項式簡約によりイデアル所属問題を解いて回路機能を検証する．その後，検証された GF-ACG を HDL の形式に変換して出力する．生成対象は，代表的なガロア体並列乗算器である Mastrovito 乗算器と Massey-Omura 乗算器とした．設計仕様には基数（2～128 の範囲）と既約多項式を与える．開発方法としては，まず既存の整数乗算器ジェネレータを拡張して GF-ACG の生成システムと GF-ACG から HDL への変換システムを開発し，それらを前年度までに開発した検証システムに接続した．さらに同ジェネレータの応用として，前年度に設計・評価した AES 暗号プロセッサの一部自動生成を実施した．一般的なラウンド型アーキテクチャにおいてデータパス部分の自動生成・検証を実施し，意図通りのデータパスを生成・検証可能なことを確認した．

５．主な発表論文等

（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計２０件）

1. Rei Ueno, Naofumi Homma, Yukihiro Sugawara, and Takafumi Aoki “Formal Approach for Verifying Galois Field Arithmetic Circuits of Higher Degrees,” IEEE Transactions on Computers, Vol. 66, No. 3, pp. 431-442, March 2017. 査読有
2. Ville Yli-Maeyry, Naofumi Homma, and Takafumi Aoki, “Power Analysis on Unrolled Architecture with Points-of-Interest Search and Its Application to PRINCE Block Cipher,” IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol.E100-A, No.1, pp.149-157, January 2017. 査読有
3. Rei Ueno, Sumio Morioka, Naofumi Homma, and Takafumi Aoki, “A High Throughput/Gate AES Hardware Architecture by Compressing Encryption and Decryption Datapaths - Toward Efficient CBC-Mode Implementation,” Conference on Cryptographic Hardware and Embedded Systems, Lecture Notes in Computer Science 9813, pp. 538-558, Springer-Verlag, August, 2016. 査読有
4. Rei Ueno, Yukihiro Sugawara, Naofumi Homma, and Takafumi Aoki, “Formal Design of Pipelined GF Arithmetic Circuits and Its Application to Cryptographic Processors,” 2016 IEEE 46th International Symposium on Multiple-Valued Logic, pp. 217-222, Sapporo, May, 2016. 査読有
5. Ville Yli‐Mayry, Naofumi Homma, and Takafumi Aoki, “Power Analysis on Unrolled PRINCE Processor and its Countermeasure,” 25th International Workshop on Post-Binary ULSI Systems, pp.22--25, May, 2016. 査読有
6. 林優一, 本間尚文, 青木孝文, 曽根秀昭, “電磁情報セキュリティ研究最前線,” 電子情報通信学会学会誌, Vol. 99, No.1, pp. 60-65, January 2016.（解説）
7. Rei Ueno, Naofumi Homma, Yukihiro Sugawara, Yasuyuki Nogami, and Takafumi Aoki, “Highly Efficient GF(28) Inversion Circuit Based on Redundant GF Arithmetic and Its Application to AES Design,” Workshop on Cryptographic Hardware and Embedded Systems, Lecture Notes in Computer Science 9293, pp. 63--80, Springer-Verlag, September, 2015. 査読有
8. Ville Yli-Mäyry, Naofumi Homma, and Takafumi Aoki, “Improved Power Analysis on Unrolled Architecture and Its Application to PRINCE Block Cipher,” Fourth International Workshop on Lightweight Cryptography for Security & Privacy‐LightSec 2015, Lecture Notes in Computer Science 9542, pp. 148–163, Springer-Verlag, September, 2015. 査読有
9. Sho Endo, Yang Li, Naofumi Homma, Kazuo Sakiyama, Kazuo Ohta, Daisuke Fujimoto, Makoto Nagata, Toshihiro Katashita, Jean-Luc Danger, and Takafumi Aoki, “A Silicon-level Countermeasure against Fault Sensitivity Analysis and Its Evaluation,” IEEE Transactions on Very Large Scale Integration Systems, Vol.23, No.8, pp.1429--1438 August, 2015. 査読有
10. Hajime Uno, Sho Endo Naofumi Homma, Yu-ichi Hayashi, and Takafumi Aoki, “Electromagnetic Analysis against Public-Key Cryptographic Software on Embedded OS,” IEICE Transactions on Communications, Vol.E98-B, No. 7, pp.1242-1249, July 2015. 査読有
11. Yukihisa Sugawara, Rei Ueno, Naofumi Homma, and Takafumi Aoki, “System for Automatic Generation of Parallel Multipliers over Galois Field,” 2015 IEEE 45th International Symposium on Multiple-Valued Logic, pp. 54--59, Waterloo, May, 2015.（Student Travel Award 受賞）査読有
12. Rei Ueno, Naofumi Homma, Yukihisa

Sugawara, and Takafumi Aoki, “Formal Design of Galois-Field Arithmetic Circuits Based on Polynomial Ring Representation,” 2015 IEEE 45th International Symposium on Multiple-Valued Logic, pp. 48--53, Waterloo, May, 2015. （Student Travel Award 受賞）査読有

13. Kazuya Saito, Naofumi Homma, and Takafumi Aoki, “A Formal Approach to Designing Multiple-Valued Arithmetic Circuits,” Journal of Multiple-Valued Logic and Soft Computing, Vol. 24, No. 1-4, pp. 21--34, February, 2015. 査読有
14. Naofumi Homma, Kazuya Saito, and Takafumi Aoki, “Toward Formal Design of Practical Cryptographic Hardware Based on Galois Field Arithmetic,” IEEE Transactions on Computers, Vol. 63, No. 10, pp. 2604--2613, October, 2014. 査読有
15. Kotaro Okamoto, Naofumi Homma, and Takafumi Aoki, “Formal design of arithmetic circuits over Galois fields based on normal basis representations,” IEICE Transactions on Information and Systems, Vol.E97-D, No.9, pp.2270--2277, September, 2014. 査読有
16. Rei Ueno, Kotaro Okamoto, Naofumi Homma, and Takafumi Aoki, "An Efficient Approach to Verifying Galois-Field Arithmetic Circuits of Higher Degrees and Its Application to ECC Decoders," 2014 IEEE 44th International Symposium on Multiple-Valued Logic, pp. 144--149, Bremen, May, 2014. 査読有
17. Hajime Uno, Sho Endo, Yu-ichi Hayashi, Naofumi Homma, and Takafumi Aoki, “Chosen-message Electromagnetic Analysis against Cryptographic Software on Embedded OS,” 2014 International Symposium on Electromagnetic Compatibility, Tokyo, pp. 313--316, May, 2014. 査読有
18. Kotaro Okamoto, Naofumi Homma, Takafumi Aoki and Sumio Morioka, "A Hierarchical Formal Approach to Verifying Side-channel Resistant Cryptographic Processors," 2014 IEEE International Symposium on Hardware-Oriented Security and Trust, pp. 76--79, May, 2014. 査読有
19. Sho Endo, Naofumi Homma, Yu-ichi Hayashi, Junko Takahashi, Hitoshi Fuji and Takafumi Aoki, “A Multiple-fault Injection Attack by Adaptive Timing Control under Black-box Conditions and a Countermeasure,” International Workshop on Constructive Side-Channel Analysis and Secure Design, Lecture Notes in Computer Science 8622, pp. 214--228, April, 2014. 査読有
20. Kotaro Okamoto, Naofumi Homma, and Takafumi Aoki, “A hierarchical graph-based approach to generating formally-proofed Galois-field multipliers,” Proceedings of 2013 PROOFS (Security Proofs for Embedded Systems) Workshop, pp. 98--109, August, 2013. 査読有

〔学会発表〕（計２１件）

1. 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, Vol. 3C1-4, pp.1--7, January 26, 2017（那覇）
2. 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, Vol. 3C1-2, pp.1--7, January 26, 2017（那覇）
3. 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, January 2017（金沢）
4. 鈴木麻奈美, 上野嶺, 本間尚文, 青木孝文, "物理複製困難関数の多値化とその応用に関する検討," 第 39 回多値論理フォーラム, Vol. 39, No. 4, pp. 1--8, September 11, 2016（盛岡）（多値論理フォーラム奨励賞受賞）
5. 忍田大和, 上野嶺, 本間尚文, 青木孝文, "認証付き暗号のための耐タンパー性ガロア体乗算に関する検討," 第 39 回多値論理フォーラム, Vol. 39, No. 3, pp. 1--7, September 10, 2016（盛岡）
6. 上野嶺, 菅原幸弘, 本間尚文, 青木孝文, 森岡澄夫, “一般化マスキングスキームに基づく耐タンパー性暗号ハードウェアの自動合成,” 2016 年暗号と情報セキュリティシンポジウム, Vol. 2F3-4, pp.1--8, January 20, 2016 （熊本）
7. 上野嶺, 本間尚文, 菅原幸弘, 野上保之, 青木孝文, “冗長表現に基づく高効率ガロア体算術演算回路の設計,” 第 29 回多値論理とその応用研究会, No. 4, pp. 22--30, January 9 2016（仙台）
8. 菅原幸弘, 上野嶺, 本間尚文, 青木孝文, “マルチパーティ計算に基づく暗号ハードウェアの形式的設計に関する検

討，” 第 38 回多値論理フォーラム，No. 11，pp. 11-1--11-6，September 13，2015 （札幌）
9. Naofumi Homma，“Hardware security - A New Challenge of Micro-electronics，”2015 International Workshop on Emerging Technologies of Microelectronics and Their Application to IoT Paradigm，December 11，2015，ホノルル（米国）（招待講演）
10. Naofumi Homma，“Recent topics on hardware security，” International Workshop on Information and Communication Security，December 9，2015（札幌）（招待講演）．
11. 本間尚文，“CRYPTREC における最新の共通鍵暗号性能評価，”IoT セキュリティフォーラム，September 30，2015 （東京）（招待講演）．
12. 本間尚文，“暗号システムへのサイドチャネル攻撃とその対策，”スマートインフォメディアシステム研究会，September 3，2015（吹田）（招待講演）
13. 梨本翔永，遠藤翔，本間尚文，林優一，青木孝文，“マイクロコントローラ上のプログラム制御フローへの故障注入攻撃，” 2015 年暗号と情報セキュリティシンポジウム，Vol. 2F4-2，pp.1--8，January 21，2015 （北九州）
14. 上野嶺，本間尚文，菅原幸弘，青木孝文，“多項式環表現を用いた GF(2^8)合成体逆元演算器の設計，” 2015 年暗号と情報セキュリティシンポジウム，Vol. 2B1-1，pp.1--6，January 21，2015 （北九州）
15. Naofumi Homma，“Formally-proofed Cryptographic Processor Design，” 2014 NII Shonan Workshop，September 16，2014（横須賀）
16. 上野嶺，本間尚文，菅原幸弘，青木孝文，“多項式環表現されたガロア体上の算術演算回路の形式的設計に関する検討，”第 37 回多値論理フォーラム，No. 14，pp. 15-1--15-8，September 14，2014 （吹田）
17. 菅原幸弘，上野嶺，本間尚文，青木孝文，“ガロア体上の並列乗算器自動生成システムの構築とその評価，”第 37 回多値論理フォーラム，No. 14，pp. 14-1--14-7，September 14，2014（吹田）
18. 菅原幸弘，上野嶺，本間尚文，青木孝文，“共通鍵暗号プロセッサの効率的な検証システムの構築，” 平成 26 年度 電気関係学会東北支部連合大会，No. 2G06，p. 1，August 22，2014 （米沢）
19. 上野嶺，本間尚文，青木孝文，“LED 暗号への単一の故障注入を用いた差分故障解析とその評価，” 2014 年暗号と情報セキュリティシンポジウム，Vol. 3A1-5，pp.1--8，January 23，2014 （鹿児島）
20. 岡本広太郎，本間尚文，青木孝文，“多様なガロア体上の算術演算に基づく暗号プロセッサの形式的設計手法，” 2014 年暗号と情報セキュリティシンポジウム，Vol. 1A3-4，pp.1--8，January 21，2014 （鹿児島）
21. 上野嶺，岡本広太郎，本間尚文，青木孝文，“ガロア体算術回路グラフに基づく誤り訂正回路の形式的検証に関する検討，” 第 36 回多値論理フォーラム，No. 10，pp. 10-1--10-7，September 14，2013 （姫路）

〔図書〕（計３件）
1. Vincent Gaudet，Jon T. Butler，Robert Wille，and Naofumi Homma (Eds.)，“Special Issue on Emerging Topics in Multiple-Valued Logic and Applications，” IEEE Journal on Emerging and Selected Topics in Circuits and Systems，” IEEE Circuit and Systems Society，Vol. 6，No. 1，March 1，2016.1-100 ページ
2. Naofumi Homma，and Marcel Medwed (Eds.)，“14th Smart Card Research and Advanced Application Conference - CARDIS 2015，” LNCS 9514，Springer，February，2016. 1-287 ページ
3. Naofumi Homma and Victor Lomné (Eds.)，“2015 Workshop on Fault Diagnosis and Tolerance in Cryptography，FDTC 2015，” IEEE Computer Society，September 13，2015.1-109 ページ

〔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)研究分担者
青木　孝文（AOKI，Takafumi）
東北大学・大学院情報科学研究科・教授
研究者番号：80241529