暗号ハードウェアの形式的設計に関する研究

博士学位論文要約（平成30年３月）

Formal Design of Cryptogprahic Hardware

Rei Ueno
Supervisor: Takafumi Aoki

暗号ハードウェアの形式的設計に関する研究

上野　嶺
指導教官：青木　孝文

This thesis presents a formal design methodology of cryptographic hardware based on Galois Fields (GFs) arithmetic. In the proposed methodology, the entire datapath structure of a cryptographic hardware is described in the form of a hierarchical graph called *Galois-Field Arithmetic Circuit Graph* (*GF-ACG*). The proposed GF-ACG has the following features: (i) able to describe any kind of GF arithmetic circuits including ones based on redundant GF representations and (ii) able to handle pipelined circuits. The correctness of circuit functions is then verified by a combination of an algebraic method, a natural deduction method for the first order predicate logic, and an equivalance checking method based on positive-polarity Reed-Muller expansion of logic formulae. In addition, we develop an automatic generation system for GF multiplers on the basis of the proposed methodology. The proposed system generates Hardware Description Language (HDL) description from circuit specifications. The proposed system can generate more than 10,000 multiplers including one with (256×77)-bit input. Moreover, we show designs of highly efficient cryptographic hardware based on redundant GF arithmetic, higher-degree functions, and logic optimization. The Advanced Encryption Standard (AES) hardware designed in this thesis achieved approximately 25–72% higher efficiency than any other conventional ones. The proposed methodology is applicable to such practical and state-of-the-art cryptographic hardware.

1. 諸言

秘匿通信や認証，電子署名に基づく情報セキュリティを実現するためにガロア体算術に基づく暗号ハードウェアが広く用いられている．そこで，多様な機能・実装法が存在する暗号ハードウェアを効率的に設計するために，その大部分を占めるガロア体算術演算回路の高速かつ正確な設計が強く求められている．一方で，現在のハードウェア設計の電子設計自動化 (EDA) ツールはガロア体算術演算回路の高水準設計に対応しておらず，その記述と検証に大きなコストがかかっている．本論文は，多様な暗号ハードウェアを高速かつ正確に設計可能な形式的設計手法のための理論的基礎の確立を目的とする．まず，多様なガロア体算術演算回路に適用可能な形式的設計手法を提案し，いくつかのガロア体算術演算回路への適用を通してその有効性を示す．さらに，提案手法に基づくガロア体算術演算回路の自動合成システムの開発を通して，既存の EDA 技術と提案手法を融合する．その上で，提案設計手法の有用性を実証するために，提案設計手法を応用した高効率暗号ハードウェア設計を示す．

2. 暗号ハードウェアの設計に関する基礎的考察

暗号アルゴリズムは暗号技術における最も重要なビルディングブロックの一つであり，システムの秘匿性や完全性を実現するために必要不可欠である．現代暗号アルゴリズムのほとんどはガロア体算術によって規定されている．したがって，暗号ハードウェア設計時には，その性能の大部分を決定するガロア体算術演算回路を適切に設計する必要がある．

しかしながら，現在回路設計の現場で一般的に用いられる EDA ツールはガロア体算術を扱うための高水準なデータ構造を持たない．暗号ハードウェア設計時には低水準な論理式による膨大な記述が必要となってしまうことから，その設計を困難とする大きな要因となっている．さらに，その機能検証においても問題がある．暗号ハードウェアのバグはセキュリティ上の致命的な脆弱性になり得るため，完全な機能検証が強く求められているが，暗号ハードウェアの長大なビット長や論理的特異性，さらにリファレンス回路やテストデータを用意することの制約などを原因として完全な機能検証は事実上不可能とされていた．

そこで近年，暗号ハードウェアの形式的設計手法が提案されている [1]．同手法では，ガロア体算術回路グ

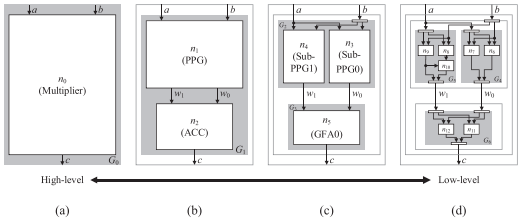

図 1　$GF(2^2)$ 並列乗算器を表す GF-ACG：(a)–(d) 第 1–4 階層

ラフ (GF-ACG: Galois-Field Arithmetic Circuit Graph) と呼ばれる数系と数式に基づく階層的グラフを用いて回路を内部構造を持つ部分回路の組み合わせとして階層的に記述する．これにより，ガロア体算術演算回路を数式を用いて構造的に記述できるだけでなく，階層間の等価性判定に基づく形式的検証が適用可能となる．ここで，回路機能は数式を用いて記述されるため，この等価性判定は数式処理によって解決できる．これまで，この数式処理にグレブナー基底に基づく多項式簡約アルゴリズムが用いられており，同手法により 128 ビットガロア体乗算器や国際標準暗号 AES 暗号ハードウェアの完全検証が可能となることが示されている．以上より，同手法は上述の暗号ハードウェアの設計問題を解決する手法として注目されている．

一方で，既存の GF-ACG に基づく形式的設計手法においても，実用的な暗号ハードウェア設計においては課題がある．まず，既存の GF-ACG は冗長表現されたガロア体算術演算回路やパイプライン化された回路を扱うことができず，多様な実装法が存在する暗号ハードウェアに対して限定的なものしか設計できないという問題がある．近年，冗長表現に基づく高性能ガロア体算術アルゴリズムが多数提案されており，今後暗号ハードウェア設計において冗長表現を扱う必要性はますます増加するものと考えられる．また，パイプライン化は暗号ハードウェア設計においてはスループットや実装効率のみならず，実装攻撃（タンパー手段を用いて暗号ハードウェアから秘密情報を取得する攻撃）に対する対策として現在広く用いられており，暗号ハードウェア設計においてパイプライン化された回路を扱うことは必須と言える．

さらに，グレブナー基底に基づく多項式簡約アルゴリズムの計算時間（すなわち検証時間）が回路機能の次数や項数，変数の数に依存するという問題もあり，これも GF-ACG に基づく形式的設計手法の限定的な設計空間の原因となっている．例えば，AES 暗号においても復号ハードウェアの機能は暗号化に対して高次な関数で表現されるため，AES 復号ハードウェアの完全検証は依然として困難であった．他にも，グレブナー基底の計算時間の制約により，最適化された AES 暗号ハードウェアや耐タンパー性 AES 暗号ハードウェアなど実用上重要な暗号ハードウェアの設計は事実上不可能とされていた．

以上より，多様な暗号ハードウェアを高速に設計可能な手法が強く求められている．

表 1　図 1 中のノード，ガロア体，ガロア体変数

Node
[Multiplier]
$n_0 = (\{c = a \times b\}, G_1)$
[PPG]
$n_1 = (\{\sum_{i=0}^{1} w_i = a \times b\}, G_2)$,
[SubPPG0]
$n_3 = (\{w_0 = a \times b_0\}, G_4)$
[GF(2) Multiplier]
$n_6 = (\{w_{0,0} = a_0 \times b_0\}, nil)$,
$n_7 = (\{w_{0,1} = a_1 \times b_0\}, nil)$,
[SubPPG1]
$n_4 = (\{w_1 = a \times b_1\}, G_5)$
[GF(2) Multiplier]
$n_8 = (\{w'_{1,0} = a_0 \times b_1\}, nil)$,
$n_9 = (\{w_{1,1} = a_1 \times b_1\}, nil)$,
[GF(2) Adder]
$n_{10} = (\{w_{1,0} = w_{1,1} + w'_{1,0}\}, nil)$,
[Accumulator]
$n_2 = (\{c = \sum_{i=0}^{2} w_i\}, G_3)$
[GFA0]
$n_5 = (\{w_0 = w_0 + w_1\}, G_6)$
[GF(2) Adder]
$n_{11} = (\{c_0 = w_{0,1} + w_{0,0}\}, nil)$
$n_{12} = (\{c_1 = w_{1,1} + g_{1,0}\}, nil)$
GFs
$GF_{(2^2)} = (\langle x^2, x^1, x^0 \rangle, (\{0,1\}, \{0,1\}, \{0,1\}), (x^2 + x + 1, x + 1))$
$GF_{(2)} = ((1), (\{0,1\}), nil)$
GF variables
$a, b, c = (GF_{(2^2)}, (1, 0))$
$w_0, w_1 = (GF_{(2^2)}, (1, 0))$
$a_0, a_1, b_0, b_1, c_0, c_1 = (GF_{(2)}, (0, 0))$
$w_{0,0}, w_{0,1}, w_{1,0}, w_{1,1}, w'_{1,0} = (GF_{(2)}, (0, 0))$

3. 暗号ハードウェアの形式的設計手法

本章では，冗長表現された回路やパイプライン化された回路を表現可能な新たな GF-ACG と，高次かつ最適化された回路であっても検証が可能な新たな形式的検証手法からなる暗号ハードウェアの形式的設計手法を提案する．

GF-ACG G は有向グラフであり，演算ノードの集合 $\boldsymbol{N}$ と有向辺の集合 $\boldsymbol{E}$ を用いて

$$G = (\boldsymbol{N}, \boldsymbol{E}) \tag{1}$$

と定義される．各演算ノード $n \in \boldsymbol{N}$ は算術演算機能を持つ部分回路を表現しており，回路機能を表すガロア体方程式の集合 $\boldsymbol{F}$ と，内部構造を表す GF-ACG G_{in} を用いて $n = (\boldsymbol{F}, G_{in})$ と定義される．一方，有向辺 $e \in E$ はノード間のデータフローを表現しており，始点ノード n_s，終点ノードの集合 $\boldsymbol{n}_e$ および回路の信号

とガロア体の変数の対応を表すガロア体変数 ν を用いて $e = (n_s, \boldsymbol{n}_e, \nu)$ と定義される．ガロア体変数は，形式的に表現されたガロア体 GF に属するものとして与えられる．GF は，$(\boldsymbol{X}, \boldsymbol{C}, (F, G))$ で与えられる．ここで，$\boldsymbol{X}, \boldsymbol{C}$ はそれぞれ基底と係数ベクトルを表し，(F, G) は演算ルールを決定する剰余多項式と，生成多項式と呼ばれる回路への禁止入力を表す多項式である．G から線形再帰関係 (LRR: Linear Reccurance Relation) と呼ばれる禁止入力を表す線形制約式が直ちに導出できるため，提案手法は禁止入力を有する冗長ガロア体算であっても扱うことができる．このように，既存の GF-ACG は基底に冗長性を許さないため冗長表現されたガロア体を扱うことができないのに対し，提案 GF-ACG では基底に任意の冗長性を許すことで任意の冗長表現されたガロア体を扱うことが可能である．さらに，提案 GF-ACG では，機能表明 $\boldsymbol{F}$ に時相論理と呼ばれる非古典論理に基づく表現を用いることで時間の概念を有する回路，すなわち順序回路型のガロア体算術演算回路を表現することが可能である．ここで，時相論理に基づく表現は一般的な数式処理ソフトウェアや等価性判定アルゴリズムでは扱うことができないが，可能世界意味論と呼ばれる解釈を用いることにより等価かつ一般的な数式処理ソフトウェアや等価性判定アルゴリズムで扱うことができる形に変形可能である．例として，図 1 に四階層で表現した $GF(2^2)$ 並列乗算器の GF-ACG を示す．また，表 1 に図 1 中のノード，ガロア体，そしてガロア体変数を示す．

次に，形式的検証手法について述べる．アルゴリズム 1 に提案検証アルゴリズムを示す．アルゴリズム 1 では入力された全てのノードの機能表明と内部構造の等価性判定を行うために，GF-ACG の各ノードの内部構造を表す GF-ACG に再帰的にアルゴリズム 1 を適用する．等価性判定においては，ノードの内部構造もしくは機能表明の形によって三つの検証手法を使い分ける．“GB-BasedEvaluation” は既存のグレブナー基底に基づく多項式簡約アルゴリズムを用いた等価性判定であり，あらゆるノードに適用可能である一方，論理レベルで最適化された回路や高次な機能を持つ回路の検証に膨大な時間を消費する．そこで，“PPRM-BasedEvaluation” は正極性リードマラー (PPRM: Positive-Polarity Reed-Muller) と呼ばれる論理式のカノニカル形を用いた等価性判定手法であり，論理レベルで表現されたノードにしか適用できない一方，論理レベルで最適化された回路を高速で検証可能である．さらに，“ND-BasedEvaluation” は一回述語論理の自然演繹 (ND: Natural Deduction) に基づく手法であり，回路機能が内部構造から演繹的に導かれるノードにしか適用できない一方，そのようなノードは回路機能の次数に依らず高速な検証が可能となる．一般に，ガロア体算術演算回路では，高次な回路機能は内部構造の演算器を単純に接続するだけで実現されるため，ND-BasedEvaluation によりほとんどの高次な回路を検証できる．このように，三種類の手法を使い分けることにより，実用的なものを含む多様な暗号ハードウェアを高速に検証可能となる．

Algorithm 1 提案検証手法

Require: GF-ACG $G = (\boldsymbol{N}, \boldsymbol{E})$
Ensure: Verification result $res \in \{\text{true}, \text{false}\}$
1: **function** NewVerify(G)
2: **Bool** $res \leftarrow$ true;
3: **for all** $(\boldsymbol{F}, G_{in}) \in \boldsymbol{N}$ **do**
4: **if** $G' \neq nil$ **then**
5: $res \leftarrow res$ & NewVerify(G_{in});
6: **if** G_{in} is $GF(2)$-level **then**
7: $res \leftarrow res$ & PPRM-BasedEvaluation($\boldsymbol{F}, G_{in}$);
8: **else if** LayerOf($\boldsymbol{F}$) ≤ 2 **then**
9: $res \leftarrow res$ & ND-BasedEvaluation($\boldsymbol{F}, G_{in}$);
10: **else**
11: $res \leftarrow res$ & GB-BasedEvaluation($\boldsymbol{F}, G_{in}$);
12: **end if**
13: **end if**
14: **end for**
15: **return** res;
16: **end function**

表 2 に代表的なガロア体算術演算回路および暗号ハードウェアの提案手法に加えて代表的な検証手法 [2] による検証時間を示す．ここで，“PB-based $GF(2^{16})$ mult.,” “PRR-based $GF(2^{16})$ mult.,” “AES enc. hardware,” “AES dec. hardware,” “Masked AES hardware,” そして “TI-based LED hardware” はそれぞれ非冗長 $GF(2^{16})$ 乗算器，冗長 $GF(2^{16})$ 乗算器，AES 暗号ハードウェア，AES 復号ハードウェア，マスクド AES 暗号ハードウェア（論理レベルの最適化により実装攻撃対策を施した AES 暗号ハードウェア），そしてパイプライン化に基づく実装攻撃対策を施した軽量暗号 LED 暗号ハードウェアを示す．また，“TO” は一日以内に検証が完了しなかったことを表し，“N/A” は適用が困難であることを表す．表 2 では入力オペランド長が 16 ビットの乗算器の検証時間したか記載していないが，入力オペランド長が 256 ビットという長大な場合においても数分以内に検証を完了することができた．表 2 より，提案手法は実用的なものを含む多様な AES 暗号ハードウェアに適用可能であり，提案手法の優位性・有効性が確認できる．

4. 暗号ハードウェア向けガロア体算術演算回路の自動合成システム

図 2 に提案システムであるガロア体算術モジュール生成器 (GF-AMG: Galois-Field Arithmetic Module

表 2　代表的なガロア体算術演算回路および暗号ハードウェアの提案手法と既存手法による検証時間 (秒)

	PB-based $GF(2^{16})$ mult.	PRR-based $GF(2^{16})$ mult.	AES enc. hardware	AES dec. hardware	Masked AES hardware	TI-based LED hardware
Logic simulation	9,330.00	TO	TO	TO	TO	TO
BDD	1,899.69	N/A	TO	TO	TO	N/A
SAT solver	TO	N/A	TO	TO	TO	N/A
Existing GF-ACG	5.52	N/A	6.12	TO	TO	N/A
This study	5.50	4.84	5.07	6.99	2.77	3,163.88

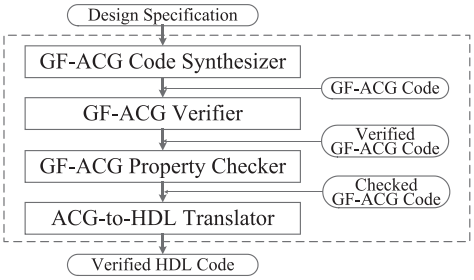

図 2　GF-AMG のブロック図

Generator) のブロック図を示す．GF-AMG は回路仕様（標数 p (= 2, 3, 5, 7, 11)，拡大次数 m，ガロア体表現，算術アルゴリズム，タンパー攻撃対策の有無）から機能と耐タンパー性が形式的に検証された HDL 記述を出力する．GF-AMG では，まず回路仕様から対応する乗算器の GF-ACG 記述を合成する．そして合成した GF-ACG の機能検証を行い，さらに必要に応じて GF-ACG の代数的記述を利用した耐タンパー性の形式的検証を行う．そしてその GF-ACG を変換することで，機能と耐タンパー性が保証された HDL を生成する．GF-AMG の処理のうち最も時間を消費するのは基本的に機能検証であり，GF-ACG に基づく手法を用いることで生成時間を大きく短縮している．同システムにより，入力ビット長が 256×77 といった巨大な乗算器であっても数分で生成できることを確認した．

5. 高効率 AES 暗号ハードウェアの設計

暗号ハードウェア設計において冗長表現や論理レベルで最適化された回路，高次な回路の重要性を実証するために，これらを用いた高効率 AES 暗復号ハードウェア設計を行った．表 3 に設計した AES 暗号ハードウェアの論理合成結果を示す．ここで，論理合成には Synopsys 社の Design Compiler を用いており，三種類の標準セルライブラリを用いて評価を行った．比較のために，既存の代表的な AES 暗復号ハードウェアを同様の条件に合成した結果も示す．表 3 より，冗長表現や論理レベル最適化を適用し，そしてレジスタリタイミングにより高次な回路機能を持つ本論文で設計したアーキテクチャが最高効率を達成した．このような実用的かつ最新の暗号ハードウェアであっても提案手法により設計・検証が可能である．

表 3　AES 暗復号ハードウェアの性能評価

	Area (GE)	Throughput (Gbps)	Efficiency (Kbps/GE)
TSMC 65-nm			
Satoh et al. [3]	14,516.50	2.25	155.05
Lutz et al. [4]	22,883.25	3.78	165.00
Liu et al. [5]	13,970.50	2.13	152.27
Mathew et al. [6]	23,298.49	1.96	83.94
This study	15,807.00	3.75	237.47
NanGate 45-nm			
Satoh et al. [3]	13,386.67	5.24	391.55
Lutz et al. [4]	22,417.01	8.89	396.52
Liu et al. [5]	12,443.66	4.53	363.86
Mathew et al. [6]	19,243.67	4.01	208.51
This study	14,582.99	9.46	648.73
NanGate 15-nm			
Satoh et al. [3]	16,924.74	38.66	2,284.17
Lutz et al. [4]	25,692.49	61.44	2,391.28
Liu et al. [5]	15,768.43	35.07	2,224.29
Mathew et al. [6]	23,789.48	31.76	1,334.95
This study	17,232.00	71.19	4,131.14

6. まとめ

本論文では，多様な暗号ハードウェアの形式的設計の理論的基礎の確立を目的として，新たな形式的設計手法の提案（第三章），実装（第四章），そして応用（第五章）を行った．今後の課題としては，提案設計手法の様々な暗号ハードウェアへの適用を通した理論的限界の究明などが挙げられる．

謝辞

研究室配属以来親身にご指導下さった青木孝文教授と本間尚文教授に深く感謝いたします．

文献

1) N. Homma et al., *IEEE Trans. Comput.*, Vol. 63, Issue 10, pp. 2604–2613, 2014.
2) R. Drechsler, “Advanced Formal Verification,” 2004.
3) A. Satoh et al., *ASIACRYPT*, pp.239–254, 2001.
4) A.K. Lutz et al., *CHES*, pp. 144–158, 2002.
5) P.-C. Liu et al., *ESSCIRC*, pp. 404–407, 2009.
6) S.K. Mathew, *IEEE J. SSC*, pp. 767–776, 2011.