博士学位論文要約（令和４年３月）

暗号モジュールの安全性評価手法に関する研究

伊東　燦
指導教員：本間 尚文

Security Evaluation Methods of Cryptographic Modules

Akira ITO
Supervisor: Naofumi HOMMA

This thesis proposes methods for evaluating the logical and physical security of cryptographic modules. In this paper, logical security is defined as the correct implementation of a cryptographic module according to the expected specification, and physical security is defined as the ability to resist side-channel attacks. This paper proposes a fast equivalence verification method between the netlist of cryptographic hardware and its specification as a logical security evaluation. By using the proposed equivalence checking method, it is possible to guarantee that the logical functions of a given cryptographic module are implemented correctly. We also propose an accurate vulnerability detection method based on side-channel attacks using deep learning as a physical security evaluation method. By using the proposed security evaluation methods, the security of cryptographic modules can be further enhanced.

1. はじめに

情報化社会の深化に伴い，秘匿通信や認証，電子署名などの情報セキュリティ機能実現のための，暗号技術の利用が拡大している．この傾向は，モノのインターネット（IoT: Internet of Things）に代表される次世代情報通信システムにおいて益々強まると予想される．IoT システムでは，ノード間の通信を盗聴・改ざんすることでシステム全体へ攻撃が可能なことから，暗号技術を用いて通信の保護を行う必要がある．また，サーバやパーソナルコンピュータ（PC）に加えて，モバイル端末や車載システムなどのリソース制約の厳しいデバイスも構成要素となり得る．したがって，効率的な暗号処理に向けて，暗号計算のための専用モジュール（暗号モジュール）による実装が必要不可欠である．

暗号モジュールには，暗号アルゴリズムが仕様どおりに正しく動作するという論理的な安全性に加えて，その実装が物理攻撃に対して耐性を有するという物理的な安全性が求められる．特に，暗号演算において副次的に発生する物理的変量（消費電力，漏洩電磁波，処理時間など）に，暗号演算に関する情報が漏洩することを利用するサイドチャネル攻撃は，最も強力な物理攻撃の一つであり，同攻撃に対する暗号モジュールの耐性評価は必須となっている．

本論文では，暗号モジュールの安全性評価手法の確立を目的とし，暗号モジュールの論理的な安全性評価手法として，計算機代数に基づく形式的検証手法を提案する．また，暗号モジュールの物理的な安全性評価手法として，深層学習に基づく高精度なサイドチャネル攻撃耐性評価手法を提案する．

2. 暗号モジュールの安全性評価に関する基礎的考察

本節では，暗号モジュールの安全性評価の，論理的な側面と，物理的な側面のそれぞれについて現状とその課題について述べる．

暗号モジュールの論理的な安全性評価では，あらゆる入力に対して，その出力が正しいことを保証することが必要となる．これは，暗号モジュールに，故障を引き起こす入力が一つでも存在すれば，秘密鍵の漏洩に直結する可能性があるためである．そのため，暗号モジュールの機能設計では，バグなどの脆弱性となり得る要素を完全に取り除く必要がある．一方，現在広く用いられている暗号アルゴリズムである ISO/IEC 標準暗号 AES（Advanced Encryption Standard）や，楕円曲線暗号（ECC: Elliptic Curve Cryptography）は，ガロア体上の算術を用いて構築されている．しかし，ガロア体算術は，主に暗号や符号理論でのみ使用される特殊な数体系であり，通常の設計・製造環境ではサポートされていない．一例として，暗号ハードウェアの実装に着目すると，現在の LSI の設計自動化（EDA: Electronic Design Automation）技術で，標準的に用いられるハードウェア記述言語（HDL: Hardware Description Language）には，ガロア体の演算を行うための高位合成や設計支援

のための機能は用意されていない．そのため，これらの暗号アルゴリズムを回路として実装するには，ガロア体で表現される算術アルゴリズムを人手で論理式に変換する必要があるため，多大な労力がかかる．これは，暗号モジュールの設計および最適化を困難にしている．したがって，設計した暗号モジュールの論理的な正しさを検証するための手法が必要とされている．

次に，暗号モジュールへの物理的な安全性について述べる．まず，暗号モジュールへの物理攻撃は，対象の暗号モジュールの変形を伴うか否かによって，侵入型と非侵入型の２つに大別される[1]．侵入型攻撃は，暗号モジュールへ狭義のタンパー手段（切る，削る，孔を開ける，溶かす，分解するなど）により，モジュールの変形を伴う直接的な手段を通して，モジュール内の秘密情報を窃取する攻撃のことである．代表的な侵入型攻撃として，回路内のバスやレコード，メモリの値の，マイクロプロービングによる読み出しが挙げられる．暗号アルゴリズムを実装した回路に直接アクセスするため高い攻撃能力を有するが，チップの開封には専門知識や高価な機器が必要となる．また，侵入型攻撃に対する対策・検知は，古くから研究されており，暗号モジュールのワンチップ化や，プローブの接近を検知するための金属メッシュセンサなどを用いるなど，様々な対策手法が存在する．したがって，物理攻撃を意識した製品へ，侵入型攻撃を検知されずに行うことは容易ではない．

一方，非侵入型攻撃は，暗号モジュールの変形を伴うことなく，正規もしくは非正規の入出力を利用して行う攻撃のことである．非侵入型攻撃は，侵入型攻撃と比べて痕跡が残らず検知が困難であり，攻撃方法によっては安価な機器で実行可能なため，現実的な脅威として注目されている．

非侵入型攻撃は，サイドチャネル攻撃と故障注入（フォルト）攻撃に大別できる．フォルト攻撃は，暗号処理の実行中に正規ではない入力を印加し，誤作動による計算誤りを誘発させ，その誤りパターンから秘密鍵を解析する攻撃である．正規ではない入力として，不正なクロック信号や入力電圧の印加，チップへのレーザー照射などが挙げられる．一方で，サイドチャネル攻撃は，暗号演算において副次的に発生する物理的変量（消費電力，漏洩電磁波，処理時間など）を計測し，統計処理を行うことで秘密情報の抽出を行う攻撃である．フォルト攻撃と比較して，サイドチャネル攻撃は実装による検知が困難であり，PC とオシロスコープのような比較的安価な機器のみで実行可能なため，高い注目を集めている．特に近年では，深層学習技術を利用した，新たなタイプのサイドチャネル攻撃（Deep-Learning based Side-Channel-Attack）が報告されるなど，攻撃自体の高度化・最適化のための研究が盛んに行われている．特に，DL-SCA は，サイドチャネル攻撃対策が施された暗号モジュールに対しても，効率的な秘密鍵の推定が可能なことが知られている．したがって，今後は，現状最も強力な攻撃である DL-SCA を対象とした，安全性評価が必要とされると考えられる．

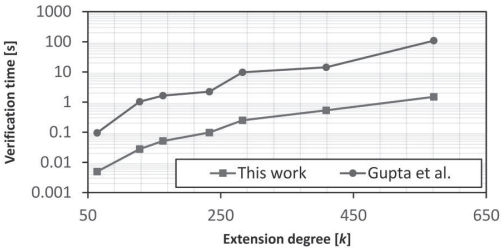

図 1 ガロア体乗算器の検証時間

以上を踏まえ，次章以降では，暗号モジュールの論理的および物理的な安全性を評価するための手法を提案する．

3. 暗号ハードウェアの等価性検証手法

本章では，暗号モジュールの論理的な安全性（正しさ）を検証するための手法として，計算機代数に基づく等価性検証手法を提案する．提案手法は，入力として暗号ハードウェアのゲートレベルネットリストと，その設計仕様を受け取り，出力として両者が等しいかどうかを返す．提案手法を用いることで，与えられた任意の暗号ハードウェアに対して，仕様どおりに設計されているかどうかを調べることができ，バグなどの脆弱性となりえる原因をすべて検出できる．

ECC（Elliptic Curve Cryptography）の一部や，AES（Advanced Encryption Standard）では，その入出力関係がガロア体の方程式として与えられる．そのため，これらの暗号ハードウェアの大部分は，ガロア体算術を計算するための演算回路（ガロア体算術演算回路）によって構成される．そこで，提案する検証手法は，ガロア体に基づく暗号回路と親和性の高い計算機代数に基づく等価性検証手法[2]をベースとする．

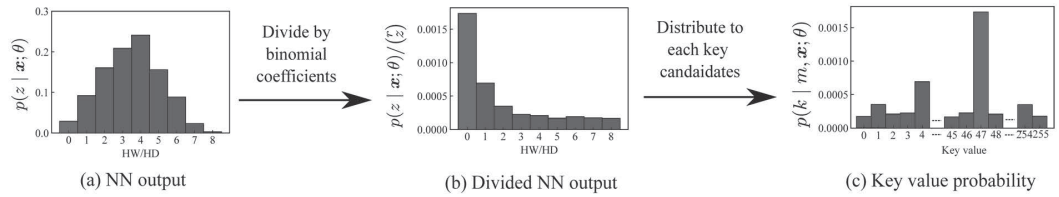

図 2 提案手法による不均衡データ問題解消の例

従来の計算機代数に基づくガロア体算術演算回路の検証手法[2]では，（1）検証時の多項式簡約において計算量が爆発する恐れがあること，（2）標数が 2 よりも大きいガロア体算術演算回路への適用可能性が不明であることという 2 つの問題が存在した．本章では，これら 2 つの問題の解消を行うことで，実用的な規模の暗号ハードウェアの等価性検証を実現する．

（1）について説明する．従来の等価性検証では，まず設計仕様から，暗号ハードウェアが満たすべき入出力関係をブール多項式として抽出する．次に，ゲートレベルネットリストを構成するすべてのゲートから，ゲート機能を表現するブール多項式を抽出し，グレブナー基底と呼ばれる多項式集合を生成する．最後に，回路のプライマリ出力変数に対して，グレブナー基底を用いて簡約と呼ばれる処理を行い，先程得た仕様と簡約結果のブール多項式が一致するかを調べることで，等価性を判定する．従来手法では，この検証過程における多項式の表現として，ゼロサプレス型二分決定グラフ（ZDD: Zero-suppressed Binary Decision Diagram）を用いる．ZDD は，多項式を因数分解した形で保持するグラフ表現のことであり，因数分解が容易な多項式であれば，非常に小さく表現できるため，検証時間を短縮できる．一方で，従来の等価性検証における多項式簡約アルゴリズムでは，中間処理で出現する多項式が，必ずしも因数分解が容易ではないために, ZDD による表現効率が下がってしまうという問題が存在した．そこで, 提案手法では, ZDD を効率的に活用可能な，新たな多項式簡約アルゴリズムを考案し，検証時間を短縮した．

提案する簡約アルゴリズムの有効性を確認するために, ECC 向けのガロア体乗算器の検証実験を行った．図 1 にその結果を示す．図の横軸はガロア体の拡大次数, 縦軸は検証時間を表す．また，比較のために最も高速な従来手法[2]を用いた場合の結果も示した．提案手法を用いることで，平均して約 70 倍の高速化を果たした．また，サイドチャネル攻撃の対策が施された AES ハードウェアの検証実験も行い，約 11 秒で検証可能なことを実験的に示した．

次に（2）について説明する．ガロア体算術演算回路の従来の等価性検証手法では，ガロア体の標数が 2 であることを前提としていた．一方で，ペアリング暗号や超特異楕円曲線暗号などの次世代暗号では，標数が 2 以上のガロア体（多標数ガロア体）を用いたほうが，より効率的となることが知られている．そこで，（2）では，多標数ガロア体算術を含む，幅広い暗号ハードウェアの論理的な安全性評価の実現を目指して，従来の等価性検証手法の拡張を行った．具体的には，従来のガロア体算術演算回路の等価性検証における多項式簡約アルゴリズムを改良し，多標数の場合に適用可能にした．さらに，ZDD を，標数が 2 以上のガロア体多項式の表現が可能なように拡張した GFBMD（Galois-field Binary Moment Diagram）を提案した．提案手法を用いることで，拡大次数が 256 のような巨大な多標数ガロア体乗算器であっても，約 2 分で検証可能なことを示した．

4. 共通鍵暗号モジュールの物理攻撃に対する安全性評価手法

本章では，共通鍵暗号モジュールのサイドチャネル攻撃耐性評価手法を提案する．これは，深層学習に基づくサイドチャネル攻撃（DL-SCA: Deep-Learning based Side-Channel Attack）を用いることで，共通鍵暗号モジュールの安全性を従来と比べてより高精度に評価できる．DL-SCA は，プロファイリング型サイドチャネル攻撃の一種であり，暗号モジュールに対する事前のプロファイリング（モデルの学習）により，強力な攻撃が可能である．

典型的な DL-SCA では, プロファイリングフェーズにおいて，入力が漏洩サイドチャネル情報（消費電力や漏洩電磁波），出力が暗号計算の中間値（例えば 1 ラウンド目の S-box の出力）の出現確率となるニューラルネットワーク(NN)を学習させる．そして，攻撃フェーズでは学習された NN の出力の対数尤度を用いて秘密情報を推定する．このとき，しばしば，学習時の複雑度を軽減

させる目的で，NN の出力は中間値そのものではなく，そのハミングウェイト(HW)やハミングディスタンス(HD)をクラスラベルとして利用する．一方で，共通鍵暗号モジュールに対する従来の DL-SCA では，HW や HD が二項分布に従うために発生する不均衡データ問題により，適切な安全性評価が難しくなっていることが指摘されていた[3]．不均衡データ問題とは，教師あり学習におけるクラスラベルに偏りが存在することで，学習時および推論時に悪影響が発生する問題である．二項分布のように，クラスラベルの出現確率に極端な差が存在する場合，出現確率の低いラベルを軽視するように学習が行われるため，推論時に深刻な問題が発生する．これは，DL-SCA の性能の大幅な低下に直結し，適切な攻撃耐性評価に支障をきたしていた．

そこで本章では，DL-SCA の不均衡データ問題の発生原理を明らかにし，その解消により暗号モジュールの安全性評価の高精度化手法を提案した．具体的には，DL-SCA において，HW/HD を用いて学習を行った NN を用いた推論（攻撃）時に，その出力を二項係数で割ることで，クラスラベルの出現頻度の不均衡による影響を除去する手法である．これにより，NN の出力が表す確率分布が，鍵値に関する確率となり，HW/HD 由来のクラスラベルの不均衡による問題を軽減することが可能となる．図 2 に提案手法の様子を示す．複数の AES の暗号モジュールに対する DL-SCA の評価実験において，従来のデータ拡張の適用や，損失関数の変更による解決方法と比べて，提案手法がより優れていることを示した．

5. 公開鍵暗号モジュールの物理攻撃に対する安全性評価手法

本章では，公開鍵暗号モジュールのサイドチャネル攻撃耐性評価手法を提案する．特に，今後利用が拡大していくと見込まれる耐量子計算機暗号（PQC: Post-Quantum Cryptography）モジュールを対象として，深層学習によるサイドチャネル攻撃耐性評価手法を考案した．PQC とは，量子計算機でも解読が困難な暗号方式のことである．従来の代表的な公開鍵暗号（RSA や ECC）は，量子計算機による効率的な解読方法が知られていることから，次世代の暗号方式として，PQC に高い注目が集まっている．一方で，PQC が注目されたのは最近のことであり，サイドチャネル攻撃に対する耐性評価が十分であるとは言えない．そこで，本章では PQC に対する DL-SCA の脅威を指摘し，その対策方法を明らかにする．

本章で対象とするのは，PQC に基づく鍵カプセル化メカニズム（KEM: Key Encapsulation Mechanism）である．KEM とは，公開鍵暗号を用いた鍵交換プロトコルの一つである．PQC に基づく KEM スキームの多くでは，IND-CCA（Indistinguishability under Chosen Ciphertext Attack）安全を実現するために，藤崎岡本（FO: Fujisaki Okamoto）変換が用いられている．FO 変換は，簡単に言えば暗号文のチェック機構のことであり，再暗号化を用いて，受信した暗号文の正当性を判定する．FO 変換が適切に実施しなければ，IND-CCA 安全が保証されないため，暗号モジュールへの攻撃が可能となる．提案攻撃では，深層学習を用いることで，FO 変換に対するサイドチャネル攻撃を行い，選択暗号文攻撃の実現方法を明らかにする．

本章では，米国標準技術研究所（NIST: National Institute of Standards and Technology）によって行われている PQC コンペティションにおける９つの候補の内，８つについては提案攻撃が有効であることを実験的に示した．また，提案手法に対する対策として，ハードウェアマスキング対策が有効であることを明らかにした．

6. まとめ

本論文では，暗号モジュールの安全性評価手法として，論理的及び物理的脆弱性検知手法を提案し，その有効性を様々な実験を通して示した．今後の展望としては，ハードウェアだけでなくソフトウェア実装の暗号モジュールの論理的な安全性評価手法の検討や，DL-SCA などの特定の攻撃によらない，サイドチャネル攻撃耐性評価手法の確立が挙げられる．

謝辞

研究室配属以来親身にご指導くださった本間尚文教授に深く感謝いたします．

文献

1) 情報処理推進機構．耐タンパー性調査研究委員会報告書．https://www.ipa.go.jp/security/enc/CRYPTREC/fy15/documents/INSTAC_rep.pdf, 2003.
2) U. Gupta, P. Kalla, and V. Rao, IEEE Trans. Comput. Aided Des. Integr. Circuits Syst, 2019.
3) S. Picek, et al., IACR Trans. Cryptogr Hardw. Embed. Circuits, 2019.