修士学位論文要約（令和４年３月）

合成体算術に基づく暗号ハードウェアに関する研究

中嶋　彩乃
指導教員：本間　尚文

Cryptographic Hardware Based on Composite Field Arithmetic

Ayano NAKASHIMA
Supervisor: Naofumi HOMMA

In recent years, high throughput cryptographic hardware is likely to be installed in various devices due to the increase in traffic data volume associated with CPS/IoT. Therefore, a high-throughput, high-efficiency, side-channel attack-resistant cipher is required, which is especially important for the hardware implementation of AES, a major cipher. In this paper, to achieve high efficiency, the we improved the efficiency of the S-Box, which is the most resource-intensive part of the AES process. Specifically, we aimed for a more efficient implementation of the S-Box based on the previously proposed composite field arithmetic by improving the efficiency of the linear arithmetic part of the S-Box. As a result, the proposed S-Box achieved a 23.1% efficiency improvement. In addition, to ensure SCA resistance, we investigated information leakage specific to unrolled implementations of AES. We proposed an SCA for the second round and a power model for the SCA, and evaluated the information leakage by performing the SCA. The results show that unique information leakage occurs and can be used for attacks.

1. はじめに

近年，CPS (Cyber Physical System) 化が進み，IoT (Internet of Things) に関連するデバイスを利用したデータ化とその活用が著しい．これに伴い，通信トラフィック量が増加しており，暗号技術においても高スループット性能が要求される．特に，デバイスに搭載される暗号技術については，リソース使用における高効率性や，デバイスの物理的特性を利用した攻撃であるサイドチャネル攻撃 (Side-Channel Attack) に対する耐性も求められている．そこで本研究では，Wi-Fi やウェブ通信の暗号化などに広く利用されている AES (Advanced Encryption Standard) のハードウェア実装について，高スループットかつ高効率性とSCA 耐性を実現するために次の 2 点に注目した．まず，高効率性については，AES の処理の中で最もリソース使用が大きい S-Box について，現状で最もリソース使用を抑制できる構成を調べた．次に，SCA 耐性については，高スループットな AES ハードウェアにおいて特有な情報漏洩の有無を調べ，これを利用した攻撃の可能性を明らかにした．

2. AES ハードウェア

AES は，ラウンド処理と呼ばれる処理を繰り返す暗号方式である． AES のハードウェア実装法は，ラウンド処理結果をレジスタに保存してループさせるループ実装と，ラウンド処理をすべて展開してパイプライン化するアンロールド実装に大別される．ループ実装は，リソース使用量が少なく，ループ処理を必要とするためスループットが低い．一方，アンロールド実装は，処理を展開しているためリソースの使用量が多く，パイプライン化しているため高スループットである．

本稿では高スループット性に着目するため，アンロールド実装の AES を対象とする．アンロールド実装の AES には次の二点の課題が存在する．まず一つ目は，リソース使用量，すなわち高効率性における課題である．特に，ラウンド処理に含まれる換字処理の S-Box のリソース使用量が多く，効率化が必須である．S-Box は，ガロア体上で逆元演算とアフィン変換を行う処理であり，合成体算術を用いることで演算効率の良い実装が可能となる．合成体算術に基づく S-Box は，用いる合成体などの構成によって演算効率が異なる．近年では，合成体上の逆元演算を高効率化する手法[1]と，アフィン変換をはじめとする線形演算を効率化する手法[2]が提案されているが，その両方を取り入れた S-Box の効率はまだ検討されていない．二つ目に，SCA 耐性における課題である．近年の研究で，アンロールド実装された暗号において特有のサイドチャネル情報漏洩の存在が指摘されている．これは，処理を展開するために，第 1 ラウンドの処理内容が後続ラウンドに影響することで，後続ラウンドから発生する第 1 ラウンドに関連した情報漏洩である．同漏洩は，暗号のアルゴリズムに依存するためそれぞれの暗号について調査する必要があるが，広く利用されている AES における特有な SC 情報の漏洩は未だ調査されていない．

3. 高効率な S−Box の実装

合成体算術に基づく S-Box は，ガロア体から合成体への変換と，合成体上の逆元演算，合成体からガロア体への逆変換，アフィン変換で構成される．

本稿では，合成体上の逆元演算を高効率化した

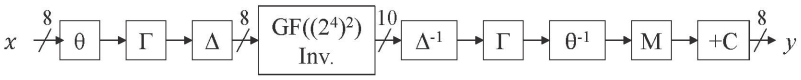

図 1 提案する S-Box の構成

上野らの S-Box[1]について，Maximov らの手法[2]を用いて，合成体変換・逆変換およびアフィン変換といった線形演算を最適化した．このとき提案する S-Box の構成 (図 1) は，ガロア体上の定数γ倍および2^{θ}乗を行う演算Γおよびθと，合成体変換Δ，上野らの逆元演算 $(\mathrm{GF}((2^4)^2)$ Inv.)，合成体逆変換Δ^{-1}，2^{θ}乗および定数γ倍を行う演算Θ^{-1}およびΓ，アフィン変換$(\mathrm{M}(x)+\mathrm{C})$ となる．[2]に基づいて逆元演算の前後に挿入されたγおよびθを伴う演算を，それぞれ乗法的オフセットと指数的オフセットと呼び，上野らの S-Box に最適なパラメータの探索を行った．

結果として，従来の上野らの S-Box に対して面積遅延積を 23.2%削減できた．さらに，2020 年最高効率であった Maximov の S-Box に対しても，面積遅延積が約 3%減少した．以上のことから，本稿で提案した S-Box の構成とパラメータ探索による効率化の有効性を確認し，最高効率を達成した．

4. 高スループットな AES に対する SCA 耐性の評価

アンロールド実装された AES の第 2 ラウンド以降 (中間ラウンド) で発生する特有な漏洩を評価するために，中間ラウンドから発生する消費電力を用いた SCA を行う．本稿では，従来研究[3]で提案された方法で SCA を行う．これは，第 1 ラウンドにおいて，16 バイト中 1 バイトのみがスイッチングするような平文を入力して暗号化させ，その時の中間ラウンドにおける消費電力を測して解析するものである．解析では，鍵候補を用いて計算される第 1 ラウンドで処理される可能性のあるデータ (中間値) と電力モデルに基づいて中間ラウンドにおける消費電力を予測し，実際の消費電力との相関係数を算出することで，正解鍵を推定する．本稿では新たにアンロールド実装された AES のための電力モデルを提案し，それを用いて SC 情報漏洩を評価したため報告する．

まず，従来研究より電力モデルが暗号アルゴリズムの特性 (拡散特性) に基づくことが明らかになっているため，AES の拡散特性を調査した．まず，従来研究で対象としていた暗号 PRINCE では，入力値の HD (Hamming Distance) 値と出力の HD 値が比例関係であったことを踏まえて，AES についても同様の相関を調べたが比例関係にはなかった．そのため，入力値の HD 値ではなく XOR 値に基づいて細分化したところ，比例関係ではないが差異が生じることが判明した．すなわち，HD 値に基づく 8 分類では利用できなかった差異が，XOR 値に基づく 255 分類により利用可能となる．

このような拡散特性をもとに，AES のための電力モデルとして，スイッチングビット系列依存な拡散特性に基づく HD モデルを提案した．本モデルは，第 1 ラウンド中間値の XOR 値に基づいて，事前計算された中間ラウンドにおける予測消費電力量を利用するものである．そのため，事前計算によって中間ラウンドにおける消費電力予測をする必要があり，これは第 1 ラウンド中間値の XOR 値ごとに，各中間ラウンドにおける HD 値を複数回計算して平均化したものである．事前計算は，ソフトウェア上のシミュレーションを一回行うだけで攻撃時に何度でも利用できるため，攻撃における実質的なオーバーヘッドはない．

本モデルを用いた SCA の結果を図 2 に示す．これは，横軸を使用波形数，縦軸を相関係数として，第 2 ラウンドについて，各鍵候補に対応する予測消費電力と実消費電力の相関係数をプロットしたグラフである．正解鍵(赤)の相関係数が上昇しており，正解鍵を特定可能であることがわかる．これにより，第 2 ラウンドに対して特有の漏洩を利用した攻撃が可能であることが判明した．

5. まとめ

高スループットで高効率かつ SCA 耐性を有する AES 実現のために，S-Box の効率化を行って最高効率を達成し，また特有な情報漏洩を評価した．

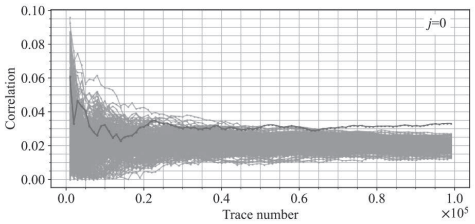

図2 第2ラウンドを攻撃対象とした場合の MTD

文献

1) R. Ueno et al., “Highly efficient GF(28) inversion circuit based on hybrid GF representations,” JCEN, 2019.
2) A. Maximov, P. Ekdahl, “New Circuit Minimization Techniques for Smaller and Faster AES SBoxes,”, CHES, 2019.
3) V. Yli-M¨ayry et al., “Diffusional Side-Channel Leakage From Unrolled Lightweight Block Ciphers: A Case Study of Power Analysis on PRINCE,” TIFS, 2020.