修士学位論文要約（令和４年３月）

軽量暗号ソフトウェアのサイドチャネル解析に関する研究

伊藤　圭吾
指導教員：本間 尚文

A Study on Side-Channel Analysis for Lightweight Cryptography Software

Keigo ITO
Supervisor: Naofumi HOMMA

With the development of technology, Society5.0 is getting closer to reality and the use of next-generation information and communication network systems such as the Internet of Things (IoT) is expected to expand. On the other hand, the risk of physical attacks on cryptographic implementations is increasing. A realistic threat is a side-channel analysis (SCA), a method to analyze secret information using side-channel information leaked from a cryptographic device. Gimli-Substitution is a cryptographic substitution function designed to perform well in a variety of environments and can be used to construct the hash function Gimli-HASH and the authentication cipher Gimli-AEAD. The purpose of this study is to evaluate the implementation security of Gimli-AEAD and to examine the possibility of key information leakage by its side-channel analysis. In addition, since the characteristics of the intermediate values of Gimli-AEAD make it difficult to identify the intermediate values using conventional side-channel analysis methods, i applied DL-SCA to the Gimli-AEAD and studied the key recovery.

1. はじめに

テクノロジーの発展によりSociety5.0の実現が近づき，IoT (Internet of Things)に代表される次世代情報通信ネットワークシステム利用の拡大が考えられる．一方で暗号実装に対する物理攻撃の危険性が高まっている．現実的な脅威としてサイドチャネル解析（SCA: Side-Channel Analysis）がある．SCA は暗号デバイスから漏洩するサイドチャネル情報を用いて，秘密情報を解析する手法である．IoT デバイスの安全性を担保する軽量暗号の候補として Gimli[1]がある．Gimli 置換は様々な環境で高い性能を発揮するよう設計された暗号学的置換関数である．Gimli 置換を使用することで，ハッシュ関数 Gimli-HASH や認証暗号 Gimli-AEAD を構成可能である．本研究では，Gimli-AEAD の実装安全性評価を目的として，そのサイドチャネル解析による鍵情報漏えいの可能性を検討する． また，Gimli-AEAD の中間値の特徴から，従来サイドチャネル解析手法による中間値の特定が困難であるため，深層学習に基づくサイドチャネル解析 (DL-SCA: Deep-Leaning based Side-Channel Analysis）を適用し，鍵復元について検討する．

2. 軽量認証暗号 Gimli-AEAD と DL-SCA

Gimli は384ビットの暗号学的疑似ランダム置換関数であり，スポンジ構造の置換に Gimli を用いることでハッシュ関数 Gimli-HASH や認証暗号 Gimli-AEAD を構成する．Gimli-AEAD は初期化，認証，暗号化の 3 つのセクションから成り，図 1 にその構造を示す．初期化では，128 ビットナンスと 256 ビット鍵を入力として

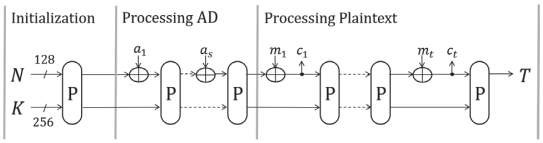

図 1　軽量認証暗号 Gimli-AEAD の構造

Gimli 置換を適用する．Gimli 置換は24ラウンドの関数であり，一ラウンドは主に非線形変換 SP-box で構成される．また，4 の倍数および 4 の倍数+2 のラウンドでは中間値ステートのワード単位のスワップと定数加算が適用される．SP-box は，循環シフトと非線形関数 T-function，行方向スワップで構成される．SP-box は 32 ビット単位の処理であるが，出力の各ビットは入力の高々4 ビット程度にしか影響されず，その代数次数も高々2 である．4 ビット S-box を用いた既存の軽量ブロック暗号と比較しても一ラウンドの SP-box は同等あるいはそれ以上に軽量な処理である．一方で，Gimli には S-box の出力といった，SCA での利用に適した明示的な中間値が存在しない．したがって，既存の SCA を用いた Gimli への鍵回復攻撃の適用可能性は非常に低いと言える．

DL-SCA は，強力なプロファイリング型 SCA の一つとして近年注目されている．DL-SCA はプロファイリングフェーズと攻撃フェーズから構成される．プロファイリングフェーズでは，攻撃者は，攻撃対象と同型のプロファイリングデバイスからサイドチャネル波形を取得し，ニューラルネットワークを用いて漏洩情報の学習を行う．

攻撃フェーズでは，プロファイリングフェーズで得られる学習済みモデルを用いて，攻撃対象デバイスから秘密情報の抽出を行う．

3. 提案手法

深層学習を利用した Gimli-AEAD の中間値の推定について，その手順を述べる．

～プロファイリングフェーズ～

(1) 攻撃対象と同型のデバイスに任意の入力を与え，攻撃対象演算からの漏洩電力波形及びその際の中間値を測定する．この漏洩電力は，対象演算の結果として得られる中間値のハミング重みに比例する．ここで，入力として与えるナンスは，選択ナンス攻撃では全体が既知の乱数，既知ナンス攻撃ではある初期値から1ずつインクリメントされた既知の値である．また，秘密鍵は暗号化処理ごとに乱数を設定する．(2) (1)で測定した中間値をラベルとして，漏洩電力波形をニューラルネットに与えて学習させ，モデルを生成する．

～攻撃フェーズ～

(1) 攻撃対象デバイスが暗号処理を実行中の漏洩電力を測定する．(2) プロファイリングフェーズで得られた学習済みモデルに測定した波形を入力し，その波形に関するハミング重みの確率分布を得る．(3) 攻撃者は，鍵候補ごとに攻撃対象演算を再現し，仮定的な中間値のハミング重みを求める．(4) (2)で得られた確率分布から，(3)で計算したハミング重みが取る確率の負の対数尤度（NLL）を計算する．(5) 波形ごとに(1)～(4)を繰り返し，NLL が最小となる鍵候補を正解鍵と仮定する．特定した正解鍵を用いて，次ラウンドの入力中間値を求める．(6) (1)～(5)を Gimli-AEAD の中間値ステート全体が既知になるまで繰り返し行い，攻撃を完了させる．

4. 評価実験

本研究では，攻撃者がナンスを選択できる場合とナンスを選択できず観測のみできる場合を想定して実験を行う．選択ナンス攻撃の場合は，学習に用いるデータとしてナンスと鍵の両方を乱数として Gimli-AEAD を実行したときに得られる電力波形を1,000,000 回取得した．学習用データのうち 10%を検証用，残りの 90%を実際の訓練用データとした．推論時に用いるデータ（攻撃成功確率の評価に用いるデータ）は，100 パターンの秘密鍵に対して，ナンスを乱数としてそれぞれ 1,000 波形取得した．本実験では，第一ラウンドの SP-box における演算結果を対象とした．部分鍵 4 バイトを一つのモデルで推定するのは計算量的に困難なため，1 バイトごとに部分鍵の推論を行った．攻撃成功確率の評価には，400 回の攻撃結果を用いた．また，既知ナンス攻撃の場合は，Gimli-AEAD のナンスが一般にアップカウンタで実装されることを考慮して学習と推論用の波形を取得した．すなわち，学習に用いるデータは，波形ごとに 1 ずつインクリメントしたナンスと乱数で設定した鍵を入力として 65,536 波形取得した．学習用データのうち 10%を検証用，残りの 90%を実際の訓練用データとした．推論に用いるデータは，10 パターンの秘密鍵に対し，アップカウンタで生成した値をナンスとしてそれぞれ 65,536 波形取得した．選択ナンス攻撃と同様に，第一ラウンドの SP-box の演算結果を対象とした．攻撃成功確率の評価には，40 回の攻撃結果を用いた．図 2 に選択ナンス攻撃と既知ナンス攻撃における攻撃結果を示す．ここで，横軸は各秘密鍵で 0～255 の鍵候補が取る確率を比べた際の正解鍵の順位，縦軸はその順位の出現確率を表す．これらの結果より，選択ナンス攻撃と既知ナンス攻撃の場合でそれぞれ約 25%と約 18%の確率で秘密鍵を推定可能であると確認できる．従来のサイドチャネル解析では困難とされる非線形性の弱い演算においても，提案 DL-SCA により鍵推定が成功することが示された．

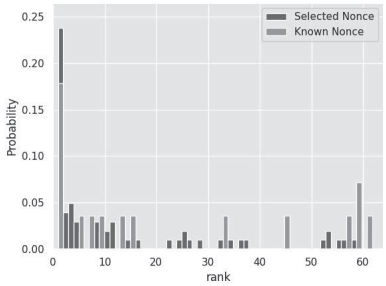

図 2 選択ナンス攻撃・既知ナンス攻撃における攻撃成功確率

5. まとめ

軽量認証暗号 Gimli-AEAD に対するサイドチャネル解析手法を提案し，実験による評価を行った．Gimli の中間値ステート全体での全単射性に着目し，中間値ステートを段階的に推定していくことで，鍵復元を行う手法を提案した．また，Gimli の中間値の分布の特徴に着目し，従来 SCA ではなく DL-SCA による解析が Gimli-AEAD に適していることを示した．従来は困難と考えられていた Gimli 置換のような非線形性が弱い演算に対して DL-SCA を適用することで，鍵復元の可能性があることを示した．今後の課題として，中間値推定の正答率の向上および後段ラウンドに対するサイドチャネル解析の攻撃可能性の実証による全鍵復元を検討している．

文献

1) Daniel J. Bernstein and et al., “Gimli: A cross-platform permutation,” in CHES 2017, pp. 299–320