

修士学位論文要約（平成29年3月）

# ストリーム暗号ソフトウェアへのサイドチャネル攻撃に対する安全性評価に関する研究

河井 航

指導教員：青木 孝文

Security evaluation of stream cipher software against Side-Channel attacks

Wataru KAWAI

Supervisor: Takafumi AOKI

This paper presents the security evaluation of a stream cipher software against side-channel attacks. In particular, this paper focuses on practical power-analysis-based attacks on KCipher-2 software implemented on microcontrollers and its countermeasure. The key idea of the proposed attack is to exploit a specific Hamming weight (HW) leakage from low-end microcontrollers or to skip a specific part of the software sequence by a fault injection on low-end microcontrollers in addition to a conventional power analysis available for KCipher-2 hardware. The efficiency and validity of the proposed method are demonstrated through experiment on KCipher-2 software implemented on 8-bit AVR and 32-bit ARM microcontrollers. The proposed attack can reveal the entire 128-bit key of KCipher-2 within a realistic computation cost, while the conventional attack does not. In this paper, we also present a compact countermeasure against the proposed attack on the basis of random masking techniques, which can be implemented on a resource-constrained microcontroller.

## 1. はじめに

現在、携帯電話やスマートカードなどの組み込み機器へ暗号モジュールが用いられているが、暗号モジュールが動作中に発する電磁波や消費電力、処理時間の違いなどを物理的な手法で観測し、内部の秘密情報を取得するサイドチャネル攻撃の脅威が指摘されている。こうした暗号処理中の内部情報を取得する攻撃は、実装形態に依存するため、暗号アルゴリズムの設計段階では考慮できないことが多く、理論上は安全と評価されている暗号アルゴリズムに対しても有効である可能性がある。サイドチャネル攻撃は、オシロスコープやPCなどの比較的安価な機器で実行可能であり、また、攻撃の痕跡が残りにくいことから、暗号を実装した機器に対する従来の攻撃と比べて危険度が高い。サイドチャネル攻撃は、能動型と受動型の攻撃に分類できる。代表的な能動型攻撃として故障注入攻撃が知られている。故障注入攻撃では、まず、暗号処理を行っている暗号モジュールに物理的な手段を用いて故障を注入する。こうして注入した故障により、命令スキップやビット反転といった現象を発生させ、得られた処理結果を用いて秘密情報を取得する。代表的な受動型攻撃としては電力（電磁波）解析攻撃が挙げられる。同攻撃では、暗号処理中の暗

号モジュールからの消費電力（漏えい電磁波）を観測し、内部の秘密情報を取得する。近年のIoTの応用の拡大によって、攻撃者の手元に存在するIoT機器の数が増加し、また監視などが少ないIoT機器も増えることが予想されることから、サイドチャネル攻撃への対策は急務となっている。

本論文では、ローエンドマイコン上に実装されたストリーム暗号KCipher-2<sup>1)</sup>ソフトウェアに対する、能動型及び受動型のサイドチャネル攻撃をそれぞれ提案する。具体的には、文献<sup>2)</sup>で報告されている手法に能動型または受動型のサイドチャネル攻撃を組み合わせることにより、秘密鍵の推定に必要な計算量を削減する。さらに、本論文では、文献<sup>2)</sup>で提案されている対策手法を拡張し、提案攻撃に対しても耐性を持つKCipher-2ソフトウェアを提案する。

## 2. KCipher-2に対するサイドチャネル攻撃

本節では、ローエンドマイコン上にソフトウェア実装されたKCipher-2に対する、2つのサイドチャネル攻撃を提案する。提案攻撃と文献<sup>2)</sup>で提案されている手法を組み合わせることで、秘密鍵の復元が可能となる。

1つ目の提案攻撃では、代表的な電力解析攻撃である、相関電力解析（Correlation Power Analysis:

CPA) を用いる。文献<sup>2)</sup>を含む既存の CPA では、一般的に、非線形関数によって処理された後の値を部分鍵推定から予測して相関値を求める。これに対し提案手法では、複雑な並列処理が行われないローエンドマイコンでは、多倍長を並列に処理するハードウェア実装と比べて、観測波形中のアルゴリズムノイズが小さいことに着目し、非線形関数による処理が行われていない中間値を予測して相関電力解析を行う。文献<sup>2)</sup>で報告されている手法により取得できる秘密鍵に本手法を組み合わせることで、全秘密鍵の復元に必要な計算量を、 $2^{96}$  から多くとも  $2^{38}$  に削減することが可能となる。

2つ目の提案攻撃では、能動型のサイドチャネル攻撃である故障注入攻撃により、秘密情報を取得する。本論文では、故障注入により命令スキップを発生させることで攻撃を行う。具体的には、暗号処理を行っている KCipher-2 ソフトウェアに対して故障を注入して命令スキップを発生させ、その初期化処理の一部をスキップする。文献<sup>2)</sup>で報告されている手法に本攻撃を組み合わせることで、全秘密鍵の復元に必要な計算量を、 $2^{96}$  から  $2^{32}$  に削減することが可能となる。

### 3. 攻撃実験と対策

8 ビット AVR マイコン (ATmega163) 上に実装した KCipher-2 ソフトウェアに対して提案する相関電力解析を適用し、その有効性を確認した。

図 1 に内部鍵の推定結果を示す。図 1 においては、正しい候補鍵以外にも、高い相関値を示す候補鍵が存在している。これは、電流と候補鍵のハミング重みの間に線形の関係が成り立つため、候補鍵の示す相関値が、その候補鍵が持つ正しい鍵と同じビットの数に比例するためである。加えて、正しい鍵以外にも、赤線で示されている候補鍵が 1 に近い相関値を示していた。図 2 に、推定に使用した波形数と相関値の関係を示す。図 2 より、50 波形程度で、1 バイト当たりの鍵候補を 2 つに絞り込むことができ、内部鍵の候補数を  $2^{32}$  から  $2^4$  にまで絞り込むことができた。これにより、既存の攻撃に提案攻撃を組み合わせることで、合計  $2^{36}$  の計算量の総当りで、全初期鍵を復元することが可能である。

また、同様に 32 ビット ARM マイコン (STM32L053; Cortex-M0+) に関しても、攻撃を実行し、その有効性を確認した。

さらに、8 ビット AVR マイコン (ATmega163) 上に実装した KCipher-2 ソフトウェアに対して、提案する故障注入攻撃を適用した。故障注入を行った際に得られた鍵系列と、文献<sup>2)</sup>で報告されている手法

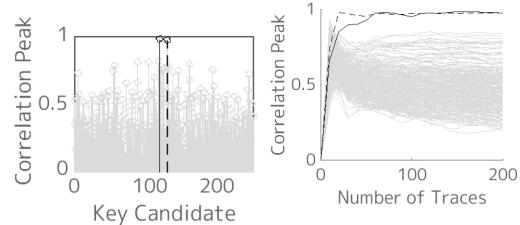


図 1 推定結果

図 2 使用波形数と相関値の関係

により推定できる内部鍵から、初期鍵  $IK$  の全 128 ビットを最大  $2^{32}$  の試行で特定可能となることを確認できた。

次に、提案攻撃への対策手法について述べる。文献<sup>3)</sup>で提案されている対策手法では、非線形演算部のレジスタ  $L_1$  及び  $L_2$  とその周辺のレジスタや演算にのみマスキングによる対策を施していた。しかし、提案攻撃を考慮すると、レジスタ  $R_1$  及び  $R_2$  とその周辺のレジスタや演算に対しても、マスキングによる対策を施す必要がある。本論文で提案する対策手法では、文献<sup>3)</sup>で提案されている対策を拡張し、乱数マスキングに基づく対策を  $R_1$  を含むデータパスにも適用する。本論文で提案しているサイドチャネル攻撃は、 $R_1$  や  $L_1$  に注目して電力解析攻撃や電磁波解析攻撃を行い、内部鍵の取得が可能であるという前提で攻撃を行っている。このため、レジスタ  $R_1$  及び  $R_2$  とその周辺のレジスタや演算にも対策を施すことで、提案攻撃への耐性を持たせることができるものである。

さらに、8 ビット AVR マイコン (ATmega163) を用いた実験を通して、提案対策の有効性を確認した。

### 4. まとめ

本論文では、ローエンドマイコン上に実装された KCipher-2 ソフトウェアに対するサイドチャネル攻撃を提案した。また、実験を通して、提案攻撃の有効性を確認した。さらに、提案攻撃への対策手法を提案し、その有効性を実験を通して示した。

### 文献

- 1) Shinsaku Kiyomoto, Toshiaki Tanaka, and Kouichi Sakurai, "K2: A stream cipher algorithm using dynamic feedback control," in *SECRYPT*, pp. 204–213, 2007.
- 2) 宇野甫, 遠藤翔, 本間尚文, 青木孝文, 仲野有登, 清本晋作, 三宅優, "Zigbee 評価用マイコン上に実装された kcipher-2 に対する相関電磁波解析の検討," 電子情報通信学会技術研究報告. ISEC, 情報セキュリティ, Vol. 113, No. 484, pp. 35–40, 2014.
- 3) 宇野甫, 遠藤翔, 本間尚文, 青木孝文, 仲野有登, 清本晋作, 三宅優, "Kcipher-2 ソフトウェアの ic カード実装とその評価," コンピュータセキュリティシンポジウム 2014 論文集, Vol. 2014, No. 2, pp. 64–71, 2014.