ランダム故障混入時の AES 暗号回路への故障利用解析攻撃

松原　有沙†　　町田　卓謙†　　崎山　一男†
† 電気通信大学　大学院情報理工学研究科　総合情報学専攻

1.　はじめに

近年，暗号回路内の秘密鍵を特定するための手法として，攻撃者が暗号回路に異常を誘発させるような外乱を与え，その異常挙動から秘密鍵を復元する故障利用攻撃と呼ばれる強力な攻撃手法が存在する．

中でも，故障混入暗号文の非一様な分布を利用して秘密鍵を特定する攻撃(NU-FVA)[1]は，攻撃者が精確に故障注入できる機材などを持つ必要がなく，攻撃者に有利な環境で攻撃可能となるため，現実的な脅威となっている．本研究では，対策手法考案のために，NU-FVA に対して，パラメータ毎に，どの程度鍵情報が漏洩するのか，定量的な調査を行う．

2.　研究手法

本実験の手法はシミュレーションを用いて実装機の結果を再現することで検証を行う．故障の混入方法は供給しているクロック周期を短くすることで計算誤りを発生させる．シミュレーションソフトは，Mentor Graphics 社の ModelSim を使用する．128 ビット AES 暗号回路にセットアップタイム違反を起こすことで故障を誘発し，その際の故障強度(クロック周波数の高さ)と入手した故障環境下での暗号文の数毎に，全 16 バイトの鍵のうち，何バイト特定できるのかを評価する．

3.　NU-FVA とは

NU-FVA(Non-Uniform Faulty Value Analysis)とは，2013 年に提案された攻撃手法であり，故障入り暗号文の頻度分布に偏りが生じることを利用して鍵復元を行う．このような鍵復元が可能となる理由として，AES 暗号実装の一種である AES-comp[2]の回路規模を縮小するために使用された合成体 S-box 内部の信号の遅延差が大きい事が挙げられる．

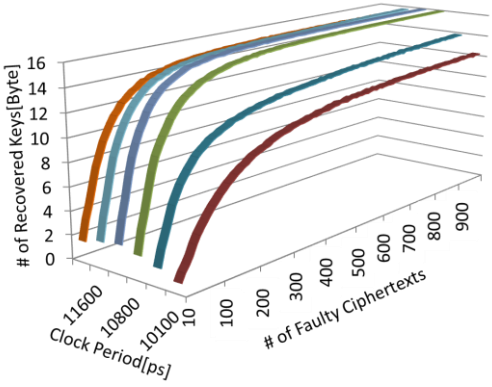

図1. クロック周波数，暗号文の数毎の秘密鍵復元できたバイト

3.　実験結果

図 1 にクロック周波数を 10000～12000[ps]の間で変更させた際の取得暗号文毎の秘密鍵を復元できたバイト数を示す．図 1 から分かるように，ほぼすべてのクロック周波数の場合において，取得する故障入り暗号文を増やしていくと 12 バイト以上の秘密鍵を復元可能である．また，図 1 を真横から見た時を図 2 に示す．

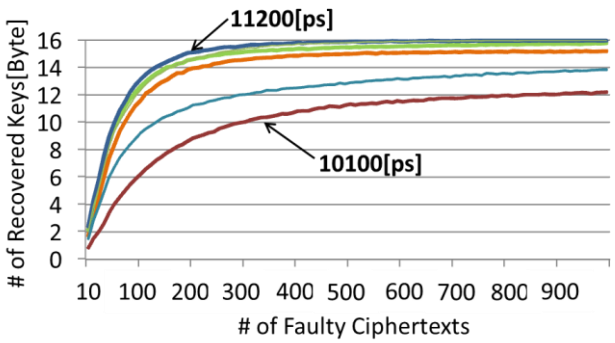

図 2. 暗号文数毎の秘密鍵復元バイト数

図 2 より，暗号文を 900 以上入手した場合，全てのクロック周波数において，12 バイト以上の秘密鍵が復元されることが分かる．また，もっとも効果的な故障強度の時(クロック周波数=11200[ps])に着目すると 400 程度暗号文を入手すれば 16 バイト全ての秘密鍵がほぼ復元可能ということが分かる．

4.　まとめ

最も適切なクロック周波数を選択した場合，約 400 程度の暗号文を入手できれば，128 ビット AES 暗号実装において秘密鍵を全バイト復元させることが可能ということがわかった．

また，NU-FVA を用いた攻撃は，ランダムにクロック周波数を任意に変更させ，ランダムな故障混入暗号文を幾つか入手するという攻撃者にとって非常に有利な環境で鍵復元が可能であることがわかった．

参考文献

[1] Y. Li, Y. Hayashi, A. Matsubara, N. Homma, T. Aoki, K. Ohta, and K. Sakiyama, “Yet Another Fault-Based Leakage in Non-Uniform Faulty Ciphertexts.” In FPS’2013, (2013).

[2] A. Satoh, S. Morioka, K. Takano, and S. Munetoh, “A Compact Rijndael Hardware Architecture with S-Box Optimization” In ASIACRYPT’2001, (2001).