SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

確率モデルと実験による増分故障解析の安全性評価
Security Evaluation of IFA(Incremental Fault Analysis) Using Probability Model and Experiments

加藤 光 * 菅原 健 * 崎山 一男 * 李 陽 *
Hikaru Kato Takeshi Sugawara Kazuo Sakiyama Yang Li

キーワード AES, 物理攻撃, フォールト解析，差分故障解析

あらまし

差分故障解析は AES のようなブロック暗号に対する代表的なフォールト解析である．2019 年，これを発展させた増分故障解析 [1] が提案された．差分故障解析では暗号文と故障暗号文を利用する (図 1).

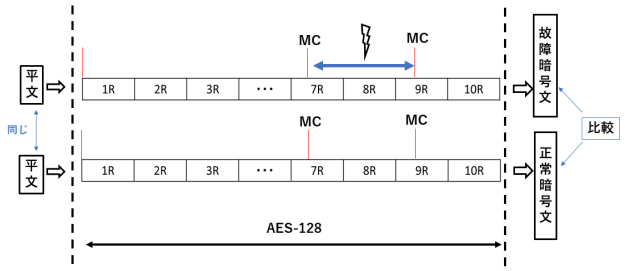

図 1: DFA の概略図

増分故障解析では故障中間値も利用する (図 2).

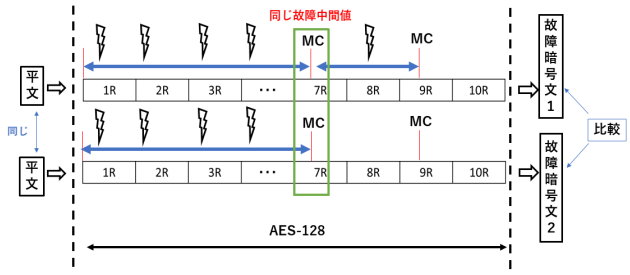

図 2: IFA の概略図

これにより，攻撃条件が緩くなり，暗号化の最中に複数回故障を入れても攻撃が成功する可能性がある．

本研究では，増分故障解析の暗号に対しての脅威を先行研究よりも詳しく考察する．まず，増分故障解析の前提条件である同じ故障中間値の確率モデルを提案する．

$$P_{same} = \prod_{k=1}^{n} \frac{a_{k,0}^2 + a_{k,1}^2 + \cdots + a_{k,m_k}^2}{S^2} \qquad (1)$$

さらに，先行研究とは違った SW 実験環境で同じ故障中間値の確率モデルを用いて増分故障解析の脅威を評価した (図 3).

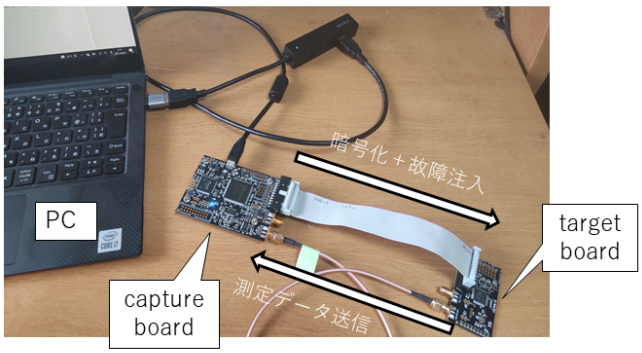

図 3: 実験環境の様子

参考文献

[1] Trevor E. Pogue , Nicola Nicolici, *"Incremental Fault Analysis: Relaxing the Fault Model of Differential Fault Attacks"*, IEEE Transactions on Very Large Scale Integration(VLSI) Systems, Vol.28, NO.3, MARCH 2020 pp750-763

* 電気通信大学, 東京都調布市調布ヶ丘 1-5-1, Faculty of Informatics and Engineering, The University of Electro-Communications, 1-5-1 Chofu-shi, Tokyo 182-8585, Japan, h.kato@uec.ac.jp