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

M&M により対策された AES 暗号ハードウェアの乱数依存性について
On the Dependency of Randomness in AES Hardware with M&M Countermeasure

塚原 麻輝 * 平田 遼 * 宮原 大輝 * 李 陽 * 崎山 一男 *
Maki Tsukahara Haruka Hirata Daiki Miyahara Yang Li Kazuo Sakiyama

キーワード AES, Masks and Macs, サイドチャネル解析, 電力解析, t 検定

あらまし

消費電力や暗号化計算時間などを利用して鍵復元を行うサイドチャネル解析や, 暗号システムに故障を発生させ誤りを含む暗号文を用いて鍵復元を行う故障利用解析が存在する．これらの物理攻撃の対策として M&M（Masks and Macs）が CHES2019 で Mayer らによって提案された [1]．M&M は，サイドチャネル解析対策の Masking と，故障利用解析対策の Infective Countermeasure に情報理論的 Mac タグを利用した手法である．

本研究の目的は，M&M における乱数が暗号ハードウェアの安全性にどのくらい寄与するのかを検証することであり，サイドチャネル解析に対する対策手法の本質を理解することである．本稿では，M&M により対策された AES を実装した暗号ハードウェア [2] に対して，乱数生成を無効にした場合と有効にした場合において，乱数生成回路の動作周波数を調整しながら暗号化処理中の消費電力を測定して文献 [3] を参考に t 検定を行い，安全性を検証する．

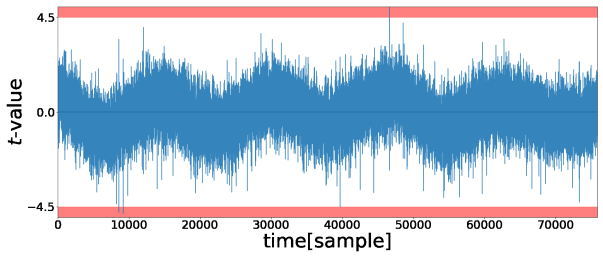

図 1: 乱数生成を無効にしたときの t 検定の結果

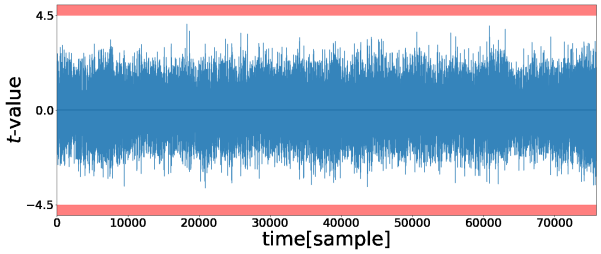

図 2: 乱数生成を有効にしたときの t 検定の結果

参考文献

[1] Lauren De Meyer, Victor Arribas Abril, Svetla Nikova, Ventzislav Nikov, and Vincent Rijmen. M&M: Masks and Macs against Physical Attacks. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, Vol. 2019, No. 1, pp. 25–50, 2018.

[2] 平田遼, 羽田野凌太, 李陽, 三浦典之, Svetla Nikova, 崎山一男. M&M により対策された AES ハードウェアの安全性評価について．IEICE2020 年 ソサイエティ大会, 2020.

[3] Jeremy Cooper, Elke DeMulder, Gilbert Goodwill, Joshua Jaffe, Gary Kenworthy, Pankaj Rohatgi, et al. Test Vector Leakage Assessment (TVLA) methodology in practice. In *International Cryptographic Module Conference*, Vol. 20, 2013.

* 電気通信大学, 東京都調布市調布ヶ丘 1-5-1, The University of Electro-Communications, 1-5-1, Chofugaoka, Chofu, Tokyo 182-8585, Japan