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

マスキング対策実装に対するサイドチャネル攻撃成功確率の情報理論的解析
Information Theoretical Analysis of Success Rate in Side Channel Attacks on Masking Countermeasures

伊東 燦 * 上野 嶺 * 本間 尚文 *
Akira Ito Rei Ueno Naofumi Homma

キーワード サイドチャネル攻撃，情報理論，マスキング対策

あらまし

本稿では，情報理論的な観点から，マスキング対策された暗号実装に対してサイドチャネル攻撃が成功する確率の上界を導出する．本稿の結果により，マスキング対策実装に対する攻撃の成功に少なくとも必要となる波形数を（先行研究と比較して）正確に推定できる．

マスキング対策実装に対するサイドチャネル攻撃では，サイドチャネル攻撃に使用する秘密中間値が d 個のシェア $S_1, S_2, \ldots, S_d$ に分解（マスキング）されており，攻撃者は各シェア S_i に関する情報を，対応するサイドチャネル漏洩 $\boldsymbol{L}_i$（S_i 処理時のサイドチャネル情報）から得る．このとき，マスキングの次数は高々 $d-1$ である．本稿では，この攻撃者が S_i に関して $\boldsymbol{L}_i$ から得る情報を相互情報量として $I(S_i;\boldsymbol{L}_i)$ と表し，攻撃成功確率と波形数に関する次の定理を証明する．

定理 2. 部分鍵と中間値のビット数を $n \in \mathbb{N}$ とする．シェアの数を d とし，i 番目のシェア S_i とその漏洩 $\boldsymbol{L}_i$ との間の相互情報量を $I(\boldsymbol{L}_i;S_i)$ とする．このとき，攻撃に使用可能な波形数 m と攻撃成功確率 SR_d には次の関係

$$n-(1-\mathrm{SR}_d)\log(2^n-1)-H_2(\mathrm{SR}_d) \le m\log_2\left((2^n-1)(2\ln(2))^d\prod_{i=1}^{d}I(S_i;\boldsymbol{L}_i)+1\right)$$

が成り立つ．ここで，H_2 は二値エントロピー関数を表す．

定理 2 より得られる結果として，図 1 に，全てのシェアの漏洩の強度が同一（$\forall i,j, I(S_i;\boldsymbol{L}_i)=I(S_j;\boldsymbol{L}_j)$）と仮定したときの，$\mathrm{SR}=0.99$ を達成するために必要な波形数の漏洩強度（相互情報量 $I(S_i;\boldsymbol{L}_i)$）に対する下界を示す．比較のために，Duc らの結果 [1] による下界も示す．図 1 は $\mathrm{SR}=0.99$ の達成に少なくとも必要となる波形数を表すため，より値が大きいほど正確に必要波形数を評価できていることになる．例えば，$d=3$ で相互情報量が 10^{-6} ビットのとき，$\mathrm{SR}=0.99$ のために Duc らの結果は少なくとも約 10^3 波形は必要なことを示すのに対し，本稿の解析結果はさらに少なくとも約 10^{15} 波形は必要ということを新たに示した．

さらに本稿では，定理 2 を用いて，$|\mathrm{SR}-1/2^n| = O(\epsilon^{d/2})$ $(d\to\infty)$ を証明する．ここで，ϵ は $\max_i I(S_i;\boldsymbol{L}_i) < \epsilon/(2\ln(2))$ を満たす 1 未満の正実数である．これは，マスキングの次数 d の増加に対して，攻撃難易度（攻撃時に必要な波形数）が指数的に増加することを表している．

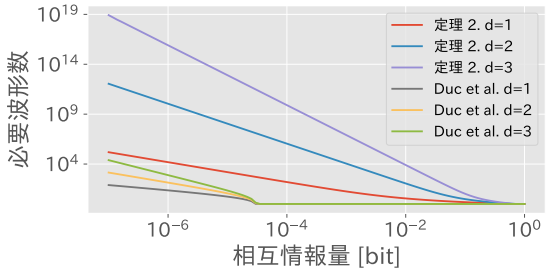

図 1: $\mathrm{SR}=0.99$ の達成に必要となる波形数の下界

参考文献

[1] A. Duc, et al., “Making masking security proofs concrete,” EUROCRYPT, pp. 401–429 (2015).

* 東北大学電気通信研究所，宮城県仙台市青葉区片平 2-1-1, Research Institute of Electrical Communication, Tohoku University, Katahira 2-1-1, Sendai 980-8577, Japan, Email: akira.ito.s1@dc.tohoku.ac.jp, {rei.ueno.a8, naofumi.homma.c8}@tohoku.ac.jp