ISS-P-17

サイドチャネル情報への相関解析を用いた暗号処理時刻推定

中村　紘†　　林　優一††　　水木　敬明†　　曽根　秀昭†
† 東北大学大学院情報科学研究科　　†† 東北学院大学工学部

1. はじめに

漏えい電磁波の観測に基づく故障発生時刻推定手法[1]では，暗号回路の動作に関連した漏えい電磁波の変動を観測する．しかし，トリガが取得できない条件下において，暗号処理が実行されている期間のみ観測を行うことは困難である．本稿では，トリガが取得できない状況下において，テンプレート波形とのマッチングにより暗号処理の実行時刻を特定する手法を検討する．

2. 時間領域における暗号処理実行時刻の特定

本手法は，暗号処理が実行されると推測される（十分長い）期間において観測を行った時間領域の波形の使用を前提とする．暗号処理実行時刻の推定には，実行時刻が既知の条件下で事前に観測を行った場合の波形をテンプレートとして使用する．図 1 にマッチングによる暗号処理時刻特定の概念を示す．観測時間が長い波形に対して，時刻をずらしながらテンプレート波形とのマッチングを行う．波形のマッチングでは，ピアソンの積率相関係数を計算し，相関係数の絶対値が最も大きい時刻において，暗号処理が実行されていると判断する．

3. 暗号処理時刻特定の実証

図 2 のセットアップにより，クランプ型電流プローブを用いてサイドチャネル攻撃用標準評価基板 SASEBO-G の電源線から漏えいする電磁波を観測した．波形の一例を図 3 に示す．AES 暗号化処理を 2,000 回実行し，各回について波形の観測を行った．SASEBO-G では AES 暗号化処理を実行しており，処理は 25 μs 付近において実行されている．図 3 の波形におけるマッチングのため計算した相関係数（絶対値）を図 4 に示す．また，マッチングに使用したテンプレート波形を図 5 に示す．得られた全ての波形に対してマッチングを行った結果，774 個（38.7 %）の波形おいて暗号処理時刻を正しく特定した．図 3 の波形よりマッチングにより検出された時刻における波形を図 6 に示す．11 個の変動ピークが見られ，暗号回路の動作に関連した漏えい電磁波の変動が観測された．

4. まとめと今後の課題

相関係数を利用した波形マッチングにより，暗号処理に同期すること無く，暗号処理が実行された時間における漏えい電磁波の変動を観測可能な場合があることを示した．

今後は，故障注入により一時的な故障が発生した場合の波形を用いて処理時刻および故障発生時刻を特定可能であるかを実験により検証を行っていく．また，波形解析手法を改善し暗号処理時刻の検出精度向上を目指す．

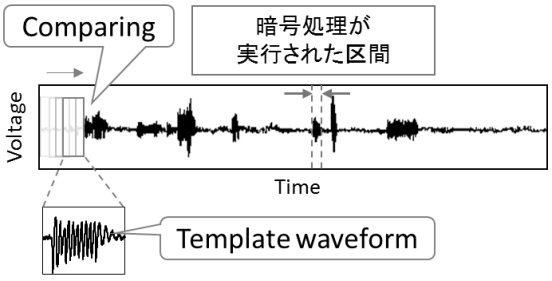

図 1 観測時間が長い波形に対するマッチング

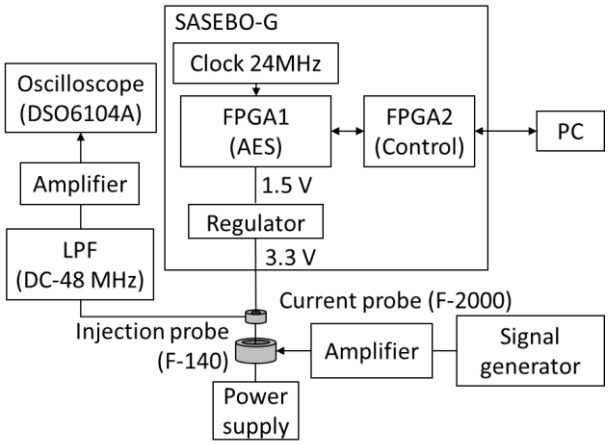

図 2 漏えい電磁波の観測セットアップ

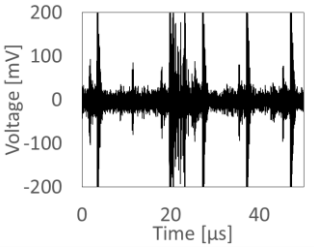

図 3 解析対象波形

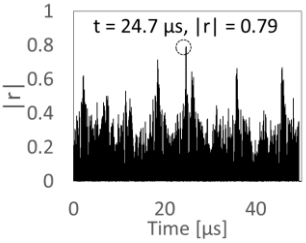

図 4 相関係数（絶対値）

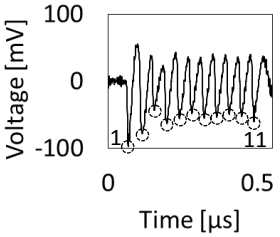

図 5 テンプレート波形
（V_{DD}-GND 間電圧）

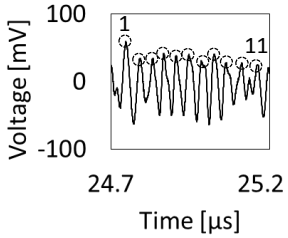

図 6 マッチングにより
検出された波形

参考文献

[1] 中村紘 ほか，信学技報，vol.115, no.131, pp.73-78, 2015.