修士学位論文要約（平成29年３月）

暗号ハードウェアへの物理攻撃に対する反応型対策の高精度化に関する研究

石幡 大輔
指導教員：青木 孝文

Enhancement of Reactive Countermeasure against Physical Attacks on Cryptographic Hardware

Daisuke ISHIHATA
Supervisor: Takafumi AOKI

This paper proposes a method of increasing EM attack sensor precision for countering a wider range of EM attacks on cryptographic modules (cryptographic LSIs). During an attack, an EM attack sensor finds the proximity of a probe to an LSI by detecting a change in the mutual inductance between the probe and LSI from the resulting oscillation frequency shift in the sensor's LC oscillator. The subsequent would-be attack is thwarted by instantaneous detection of the probe's proximity. This paper shows that smaller oscillation frequency shifts can be detected by extending the detection operation time. This paper also demonstrates that this extension enables attacks to be detected even when they come from the LSI's back surface (which was previously difficult to achieve).

1. はじめに

近年，IoT (Internet of Things) や M2M (Machine to Machine) に代表されるような新たなネットワーク形態に注目が集まっている．このようなネットワーク形態では，攻撃者が末端の機器になりすまし，ネットワークを介してサーバやシステム全体へ攻撃を行うことを防ぐため，末端の機器への暗号の実装によって安全な通信を行う必要がある．一方で，近年，暗号処理を実装したハードウェアに対する物理的な攻撃の危険性が指摘されている．特に，機器の動作中の消費電力や漏洩電磁波などを利用し，内部の秘密情報を奪うサイドチャネル攻撃は，PC やオシロスコープなどの市販の機器のみで実行可能であることや，攻撃の痕跡が残らないことから，暗号ハードウェアに対する現実的な脅威とされている．サイドチャネル攻撃への対策としては，ハイディングやマスキングなど，漏洩情報と内部情報を無関係にする手法がこれまでに研究されている．一方で，計測精度の向上により，設計者の想定を超えた精度の漏洩情報を攻撃者が得ることができた場合，こうした対策は無効化される可能性がある．文献 [1] では，マイクロプロービングにより回路中の特定箇所からの漏洩電磁波を観測することで，従来の対策手法のほとんどを無効化する局所電磁波攻撃が報告されており，このような攻撃への対策技術の研究開発は急務となっている．

こうした状況に対し，著者の所属する研究グループでは，電磁波攻撃センサという新たな対策技術を提案している [2]．これは，マイクロ磁界プローブの LSI への接近を検知することにより，攻撃を防ぐ対策技術である．本センサは従来対策と異なり，攻撃者のサイドチャネル情報の取得そのものを防ぐ反応型対策であるため，これまで有効な対策手法のなかった攻撃に対しても根本的な対策となることが期待されている．一方で，本センサによって検知可能なプローブ距離はチップ近傍約 0.1mm 以内と短く，より多様なシナリオにおける電磁波解析を本センサで対策するためにはセンサの最大検知距離の延伸が課題となる．

本論文では，電磁波攻撃センサの高精度化手法の提案を行う．具体的には，より多様なシナリオにおける電磁波解析攻撃を電磁波攻撃センサによって検知可能にするため，本センサのプローブ検知距離の延伸手法を提案する．また，センサ-プローブ間の距離とセンサの反応性の関係についての評価実験を行い，提案手法の有効性を確認する．

2. 電磁波攻撃センサの高精度化

図１に，電磁波攻撃センサによるプローブの検知の原理を示す．暗号ハードウェアにプローブが接近すると，LSI とプローブの間に電気的結合が発生し，プローブの接近に従って増加する値である相互インダクタンスおよび相互キャパシタンスが生じる．電磁波

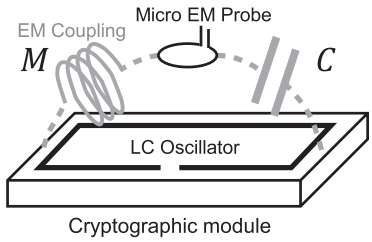

図 1　電磁波攻撃センサの原理

表 1　シフト量とカウンタの値の変化の関係

検知動作時間	値の変化に必要なシフト量 [%]	
$[\mu s]$	LC0(4 turns)	LC1(3 turns)
0.15	0.392	0.740
15	0.016	0.010

攻撃センサでは，相互インダクタンスの増加を検知するため，暗号 LSI の上部配線層にコイルを配置し，LC 発振回路を構成する．このとき，コイルを流れる電流の発振周波数は，プローブの接近による相互インダクタンス M の増加に伴って変化する．この発振周波数の変化を計測することで，センサは攻撃の兆候を検知する．本論文では，より多様な攻撃を検知するためのセンサの改良手法として，プローブ検知距離の延伸手法を提案する．本センサでは，二つの発振回路の発振回数を一定時間カウンタにより計数し，その値の差分を取ることによって周波数シフトの有無を検出する．提案手法のアイデアは，検知動作時間を延長することにより，発振周波数のシフト量をより長時間積算することである．これにより，面積オーバーヘッドをほぼ増加させることなく検知感度の向上を図る．表 1 に，本手法による効果を示す．提案手法により，0.02%程度の小さな周波数シフトも検出可能となる．

3.　評価実験

提案手法により誤検知を起こすことなく高精度な検知が可能になることを確認するため，プローブ距離 0.00mm（接地）から 0.5mm までの場合について，各距離にプローブを接近させた場合の発振周波数を 100 回ずつ計測し，プローブが存在しない場合と比較したシフト量の分布を求めた．図 2,3 に，上記実験の結果を示す．横軸を発振周波数のシフト量，縦軸を計測される確率とする．図 2 では，1 回の計測（シグナルアナライザによる単一の計測）におけるシフト量を示す．測定ごとの結果のばらつきを評価するため，各プローブ距離において 100 回の計測を行い，100 回分の結果の分布を示した．一方，図 3 では，観測時間を 100 倍とすることを想定し，100 回の計測における平均のシフト量を示す．

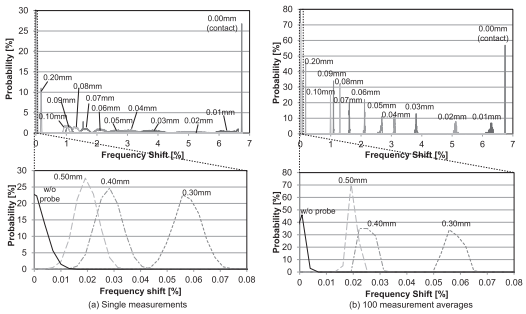

図 2　各プローブ距離による発振周波数の分布 (単一計測)

図 3　各プローブ距離による発振周波数の分布 (100 回平均)

図 2 より，単一の計測では，プローブ距離 0.5mm（シフト量が 0.01 %程度）の場合とプローブがない場合の発振周波数の分布に重複している部分が存在するため，この部分の発振周波数においてはプローブの有無の判別ができない可能性があることがわかる．これに対して，図 3 のように平均をとった場合，プローブがない場合の観測誤差を 0.01%未満に抑えることができ，プローブ距離 0.5mm 程度のシフト量でもプローブの有無を検知可能となることが確認できる．これは，検知時間を 100 倍とすれば (時間平均と同様の効果が得られるため)，0.5mm 程度の距離まで検知可能となることを示唆している．

4.　まとめ

本論文では，暗号ハードウェアへの物理攻撃と，それに対する反応型対策である電磁波攻撃センサ，ならびにその高精度化手法について述べた．特に，検知動作時間を延長し，発振出力をより長時間積算することによってプローブ検知距離を延伸する手法を提案するとともに，攻撃距離とセンサ発振周波数のシフト量についての評価実験の結果を示し，提案手法によって従来は検知困難な距離からの攻撃を対策可能となることを示した．

文献

1) Takeshi Sugawara, Daisuke Suzuki, Minoru Saeki, Mitsuru Shiozaki, and Takeshi Fujino, “On measurable side-channel leaks inside ASIC design primitives,” *CHES 2013*, pp. 159–178, 2013.
2) Naofumi Homma, Yu-ichi Hayashi, Noriyuki Miura, Daisuke Fujimoto, Daichi Tanaka, Makoto Nagata, and Takafumi Aoki, “EM attack is non-invasive? - design methodology and validity verification of EM attack sensor,” *CHES 2014*, pp. 1–16, 2014.