様　式　Ｃ－１９、Ｆ－１９、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　２８　年　　５　月　３１　日現在

機関番号：　１５３０１
研究種目：　若手研究(B)
研究期間：　2014～2015
課題番号：　２６８７０３９２

研究課題名（和文）漏洩ポテンシャルに基づく暗号機器へのサイドチャネル攻撃に対する安全予測法の研究

研究課題名（英文）A Study of Developing a Prediction Method of Security of Cryptographic Devices against Side-Channel Attacks Based on Information Leakage Potential

研究代表者

五百旗頭　健吾（Iokibe, Kengo）

岡山大学・自然科学研究科・助教

研究者番号：１０４２０４９９

交付決定額（研究期間全体）：（直接経費）　　3,000,000円

研究成果の概要（和文）：暗号技術への新しい攻撃手法であるサイドチャネル攻撃に対する安全性を予測する手法の開発を目的として、まず、暗号機能を実装したICの等価回路モデルに基づき情報漏洩の強さを精度良くシミュレーションできることを示した。次に、等価回路モデルからICがサイドチャネル情報を漏えいする性質を読み取れることを確認した。最後に、安全性予測で使用する情報漏洩ポテンシャルとして、サイドチャネル信号の信号対雑音比を実測により同定した。

研究成果の概要（英文）：Aiming for developing a method to predict security of cryptographic devices against side-channel attacks that is a new cryptanalytic method using physical behavior of the devices, we firstly confirmed that strength of side-channel information leakage can be simulated with an equivalent circuit model of an integrated circuit (IC) implementing a cryptographic circuit. Next, we indicated that the behavior of the cryptographic IC leaking the side-channel information can be seen in the equivalent circuit model. This can help develop a new and more efficient countermeasures to the attacks. Finally, we identified signal-to-noise ratios of side-channel traces as an information leakage potential to be used in prediction of side-channel attack security.

研究分野：　環境電磁工学，暗号回路のハードウェアセキュリティ

キーワード：　情報セキュリティ　暗号・セキュリティ　耐タンパー技術　AES暗号　等価回路モデル

１．研究開始当初の背景

あらゆる情報が電子化されインターネットを介して交換されるなか、個人情報や機密情報などの漏洩を防止するため様々な製品で高度な暗号技術が利用されている。そんな中、暗号回路の動作に伴って発生する電磁放射等の副次的・物理的な手段を利用して暗号を解読する攻撃法としてサイドチャネル攻撃が発見され、高度化が進んでいる。その結果、数学的には解読が困難な現代暗号を現実的な時間で解読される可能性が高まっている。そのため、サイドチャネル攻撃に対する安全設計法が必要となっている。

我々は、ディジタル IC 電源系回路の等価回路モデルを利用したサイドチャネル攻撃シミュレーション法を開発している。しかし、このシミュレーション法が暗号機器のサイドチャネル情報漏洩強度を予測可能かどうか、さらにその予測に基づく安全設計法の開発には至っていない。幅広い製品に実装される暗号回路の安全な実装を実現するためには、サイドチャネル情報漏洩強度の予測、および安全設計法の開発が必要である。

２．研究の目的

本課題では、漏洩ポテンシャルからサイドチャネル攻撃に対する安全性を予測する手法の提案、またその準備として、漏洩ポテンシャルを同定する元となる等価回路モデルに基づく予測法の実用性を検証する。まず、(1) 等価回路モデルをサイドチャネル攻撃のシミュレーションに適用し情報漏洩強度の予測精度を検証する。加えて、等価回路モデルより情報漏洩ポテンシャルを同定できることを確認するため、(2)等価回路モデルがサイドチャネル情報漏洩挙動を表現しているかどうか検証する。最後に、(3)漏洩ポテンシャルを同定し、サイドチャネル攻撃結果を予測する手法を提案する。

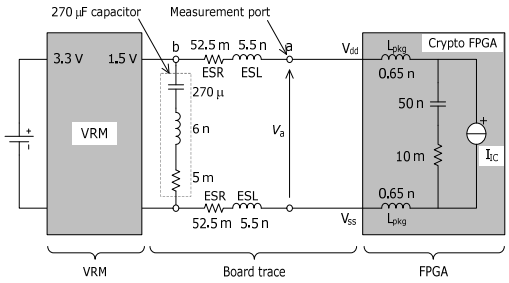

図 1 暗号 IC の電源系等価回路モデル

３．研究の方法

本プロジェクトではサイドチャネル攻撃シナリオとして次の環境を使用した。まず、攻撃対象の評価暗号モジュールには、サイドチャネル攻撃標準評価プリント基板の一つである SASEBO-G を使用した。次に、攻撃対象の暗号アルゴリズムとして、国際標準暗号の一つである AES-128 をした。最後に、サイドチャネル攻撃法として、AES への最も強力なサイドチャネル攻撃法の一つである相関電力解析(CPA)を想定した。CPA において使用されるパワーモデルにはハミング距離モデルを採用した。

本研究はディジタル IC の等価回路モデルがベースとなっている。SASEBO-G に実装した AES-128 回路の等価回路モデルを実測により図１のように同定し、その等価回路モデルを利用して検討を行った。等価回路モデルの構成要素の一つである電流源は、IC 内部で発生するスイッチング電流を表わしている。この電流源には暗号回路で発生するスイッチング電流を含んでいる。つまり、そこには暗号回路の情報漏洩挙動が現れる。そして、IC 外部からは直接測定できない。このように、等価回路モデルを利用することで、直接測定が困難な IC 内部の情報漏洩挙動を詳細に観察できる利点がある。

４．研究成果

(1)等価電流源モデルによる情報漏洩強度シミュレーション（学会発表③）

暗号回路が実装された IC の等価電流源モデルにより、暗号回路からのサイドチャネル

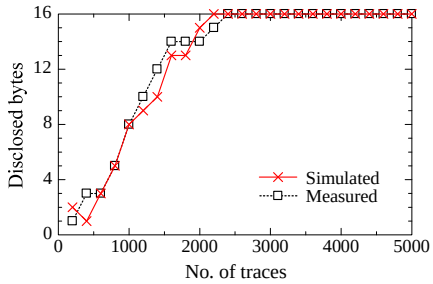

図 2 情報漏洩強度シミュレーション

情報漏洩強度を高精度に予測できることを示した。図 2 に示すように、サイドチャネル攻撃を受けた暗号機器の情報漏洩強度に相当する波形数をシミュレーションした。波形数とは、AES 暗号の秘密鍵を CPA により解読するのに必要な波形数である。波形数が少ないほど解読が容易であり情報漏洩強度は高い。反対に、波形数が多いと情報漏洩強度は低い。図 2 に示した結果では、シミュレーションでは 2200 波形で秘密鍵の 16 バイト全てを解読できた。一方、実測では 2400 波形で解読された。ここで実測は評価用暗号モジュール SASEBO-G へのサイドチャネル攻撃に相当する。したがって、シミュレーション結果は実攻撃を精度良く再現している。

(2)サイドチャネル情報漏洩挙動分析への適用可能性（雑誌論文①、学会発表①②④）

等価回路モデルが、サイドチャネル情報漏洩強度予測だけでなく、暗号回路のサイドチャネル情報漏洩挙動の分析に適用できることを示した。暗号回路においてサイドチャネル情報漏洩に寄与することが知られている 3 つの性質について、情報漏洩強度の変化を等価回路モデルが表現していることを調べた。ここで評価した 3 つの性質とは、「SNR 向上による情報漏洩強度の増加」、「レジスタのハミング距離一定化による情報漏洩強度の低減」、そして「レジスタ負荷のアンバランスに起因する情報漏洩」である。これらの性質を変化させた AES-128 回路を FPGA 実装し、実測により同定したそれらの回路の等価回路モデルを分析した。その結果、等価回路モデルが上記 3 つの性質を表現していることを確認した。

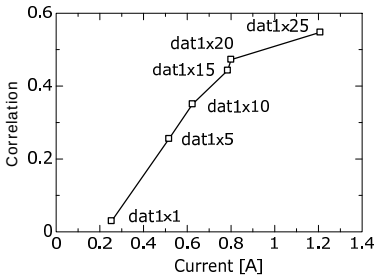

図 3 攻撃者が注目する電流の大きさと情報漏洩強度の関係

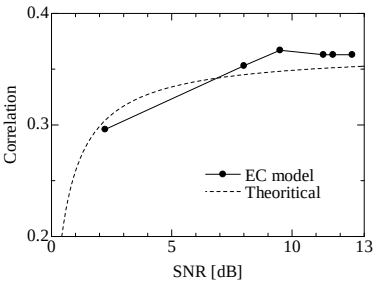

図 4 SNR と情報漏洩強度の関係

この結果より、等価回路モデルが暗号 IC のサイドチャネル情報漏洩挙動分析に利用できることが確認された。

(3)情報漏洩ポテンシャルの同定（学会発表④）

FPGA 実装したサイドチャネル攻撃耐性の異なる暗号回路について、情報漏洩ポテンシャルを同定した。標準暗号である AES を評価対象とし、AES 回路のうちサイドチャネル情報を含むスイッチング電流を発生するレジスタ部の回路サイズが 1～20 倍異なる複数の AES 回路を使用した。それぞれの AES 回路について、我々が提案する等価回路モデルに基づき等価電流源を同定し、スイッチング電流と情報漏洩強度を表す相関係数との関係を分析した。その結果、図 3 に示すように、攻撃者が狙いを定めたスイッチング電流のみを増加させた時、サイドチャネル波形に含まれる信号成分の増分に比例して相関係数が増大することを実証した。この結果より、情

報漏洩ポテンシャルとして、当初想定していた線形な漏洩関数と相関係数を包含する信号対雑音比(SNR)が適していることを示した。さらに、図 4 に示すように、SNR と相関係数の関係が理論式と一致することを実測結果により示した。

５．主な発表論文等
（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計　1 件）

① 五百旗頭健吾，田井伸拓，籠谷裕人，大西紘之，豊田啓孝，渡辺哲史，"暗号回路におけるサイドチャネル情報漏洩挙動の内部電流源による分析," 電気学会論文誌 A，Vol．131，No．6，2016(採録決定)．

〔学会発表〕（計　4 件）

① 田井伸拓，五百旗頭健吾，籠谷裕人，大西紘之，豊田啓孝，渡辺哲史，“内部等価電流源に基づく相関電力解析における AES 暗号回路の情報漏洩源分析，” 第 16 回 IEEE 広島支部学生シンポジウム，A-14，広島市，2014．

② 五百旗頭健吾，田井伸拓，籠谷裕人，大西紘之，前島一仁，豊田啓孝，渡辺哲史，“内部電流波形に基づく AES 回路のサイドチャネル情報漏洩特性の考察，” 2015 年 暗号と情報セキュリティシンポジウム (SCIS2015)，2F3-1，北九州市，2015．

③ Kengo Iokibe，Kazuhiro Maeshima，Tetushi Watanabe，Yoshitaka Toyota，"Security Simulation against Side-Channel Attack on Advanced Encryption Standard Circuit based on Equivalent Circuit Model," IEEE International Symposium on Electromagnetic Compatibility and EMC Europe，SS-1-2，pp.224-229，Dresden，Germany，2015．

④ 五百旗頭健吾，田井伸拓，大西紘之，籠谷裕人，豊田啓孝，渡辺哲史，"サイドチャネル情報漏洩に寄与が大きい AES 回路部の内部電流源に基づく検討," 第 38 回情報理論とその応用シンポジウム (SITA2015)予稿集，pp．720-724，倉敷市，2015．

〔図書〕（計　0 件）

〔産業財産権〕
○出願状況（計　0 件）

○取得状況（計　0 件）

〔その他〕
ホームページ等
http://www.ec.okayama-u.ac.jp/~oew/research.html

６．研究組織
(1)研究代表者
五百旗頭　健吾（IOKIBE，Kengo）
岡山大学・大学院自然科学研究科・助教
研究者番号：10420499

(2)研究分担者
なし

(3)連携研究者
なし