様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　　元 年　　５ 月 ２５ 日現在

機関番号：１５３０１
研究種目：基盤研究(C)（一般）
研究期間：2016～2018
課題番号：１６Ｋ００１８６

研究課題名（和文）IC設計情報に基づく暗号回路のサイドチャネル攻撃予測に関する研究

研究課題名（英文）Vulnerability simulation of cryptographic circuit to side-channel attacks based on IC design information

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）　　3,500,000円

研究成果の概要（和文）：暗号回路のサイドチャネル攻撃(SCA)耐性をICの設計情報から予測する手法を開発した。FPGA実装されたAES回路のSCA耐性予測結果は実測と精度よく一致した。次に、SCA耐性設計手法の確立に向けて、サイドチャネル情報漏洩(SCIL)強度を漏洩波形のSNRを変数として表す理論式を実験により検証し、その有効性を確認した。さらにAES回路のSCIL帯域を導出し、実験結果との一致を確認した。これにより漏洩波形のSNRとFPGA電源系回路の等価回路に基づくSCA耐性設計手法開発の見通しを得た。最後に、SCA手法を応用した電磁妨害波源推定法を開発し、各妨害波源に起因する妨害波強度を精度よく推定した。

研究成果の学術的意義や社会的意義
暗号技術はIoT機器の情報セキュリティにおいて重要な役割を期待されるが、十分なセキュリティを実現するためにはハードウェアレベルでの安全性が不可欠である。本成果は、暗号ハードウェアのサイドチャネル攻撃耐性設計を製品開発の初期段階で実現することを可能にする。それにより暗号ハードウェア設計の低コスト化を実現でき、その結果、IoT機器の情報セキュリティ向上が期待できる。

研究成果の概要（英文）：A method to estimate side channel attack (SCA) vulnerability of cryptographic circuit from design information of IC was developed. The SCA vulnerability was simulated for an FPGA-implemented AES circuit and agreed with the measurement results accurately. Next, for establishing an SCA vulnerability design method, a theoretical formula that expresses the side channel information leakage (SCIL) intensity with the SNR of the leakage trace is verified by experiments, and its effectiveness is confirmed. Furthermore, the SCIL band of the AES circuit was derived and confirmed to be consistent with the experimental results, suggesting that the SCA vulnerability design method can be established based on the formula and the equivalent circuit model of FPGA power distribution circuit. Finally, we developed an electromagnetic interference source estimation method applying the SCA method and accurately estimated the interference intensities caused by individual interference sources.

研究分野：通信・ネットワーク 工学

キーワード：情報セキュリティ　暗号　セキュリティ評価　耐タンパー性　等価回路モデル　漏洩源推定　相関解析

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９、ＣＫ－１９（共通）

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。最新の暗号技術は、スーパコンピュータを使用しても現実的な期間で解読は困難と言われており、そのような暗号技術によって情報漏洩防止が図られている。一方、暗号回路の動作に伴って発生する電磁妨害波等の副次的・物理的な手段を利用して暗号を解読する攻撃法(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。

サイドチャネル攻撃に対する安全設計は、アルゴリズム、回路、プリント基板、製品の各設計段階において要求される。これまでに、アルゴリズムおよび回路レベルで幾つかの対策設計法が提案され、それらの手法に基づく安全設計が為されている。また、申請者らはプリント基板レベルでのサイドチャネル攻撃予測法を提案し、過去に例を見ない予測精度を実現した[IoK15][IoK13]。その予測精度は同様の予測法を検討している他研究グループからも良い評価を得ている([KaD14])。しかし、予測法の基礎となる暗号 IC 電源系の等価回路モデルは実測により同定している。そのため設計段階でのサイドチャネル攻撃予測は実現できない。暗号 IC の設計情報に基づきサイドチャネル攻撃予測する手法も提案されているが、予測精度は不十分である。そこで本応募課題では、設計情報に基づき高精度にサイドチャネル攻撃予測を実現する手法を開発する。

２．研究の目的

暗号回路のサイドチャネル攻撃耐性を設計段階で予測する手法を開発する。開発する手法は、研究代表者らが提案した IC 電源系回路の等価回路モデルを利用した安全性予測手法[IoK15][IoK13]に基づいており、その既存手法では実測により同定していた等価回路モデルを、本研究では IC 設計情報より同定することで、設計段階でのサイドチャネル攻撃予測を実現する。この IC 設計情報からの等価回路モデル同定は挑戦的な課題であるとともに、サイドチャネル攻撃予測だけでなく、IC の電源品質予測や電磁妨害波(EMI)予測など、他領域への応用も期待できる。

３．研究の方法

サイドチャネル攻撃耐性予測法は、FPGA 実装された AES 暗号回路を対象として、その設計情報である HDL ファイル情報に基づく RTL レベルシミュレーションにより予測する。FPGA の電源品質(PI)性能や電磁妨害波(EMI)の予測に RTL シミュレーションを適用した報告があり[ReL14]、本研究ではそれらの手法を FPGA のサイドチャネル攻撃耐性予測に適用する。RLT レベルシミュレーションにより AES 暗号アルゴリズムの攻撃ターゲット処理に伴い発生する消費電流を予測する。予測結果の検証のため、暗号回路内部で発生する消費電流を測定により同定する。この内部電流は FPGA 電源系回路の等価回路モデリング手法[IoK15]に基づき同定する。

サイドチャネル攻撃耐性の設計手法の開発は、サイドチャネル解析によって得られる相関係数をサイドチャネル漏洩波形の SNR の関数として表した式の検証から始める。この式は解析的に導出された既知の式であり[MaS07]、実測される漏洩波形の相関係数がこの式に従って SNR の関数として表されることを実験により検証する。サイドチャネル情報漏洩の周波数特性を調べ、サイドチャネル波形の SNR を評価指標としてサイドチャネル攻撃耐性を設計する方法論を検討する。

EMI のノイズ源推定法開発では、漏洩波形の変動がノイズ源であるディジタル IC で発生するスイッチング電流の変動と相関することを利用する。既知の 2 値データ系列を変調信号としてスイッチング電流を振幅変調し、その時に観測される EMI とデータ系列の相関係数を指標として IC 毎の EMI 強度を推定する手法を開発する。

参考文献

[IoK15] K. Iokibe, K. Maeshima, T. Watanabe, Y. 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, Aug. 2015.

[IoK13] K. Iokibe, T. Amano, K. Okamoto and Y. Toyota, “Equivalent Circuit Modeling of Cryptographic Integrated Circuit for Information Security Design,” IEEE Transactions on Electromagnetic Compatibility, Vol. 55, No. 3, pp.581-588, 2013.

[KaD14] D. Kamel, M. Renauld, D. Flandre, F.-X. Standaert, “Understanding the limitations and improving the relevance of SPICE simulations in side-channel security evaluations,” Journal of Cryptographic Engineering, Vol. 4, No. 3, pp 187-195, September 2014.

[ReL14] L. Ren, T. Li, S. Chandra, X. Chen, H. Bishnoi, S. Sun, P. Boyle, I. Zamek, J. Fan, D. G. Beetner, J. L. Drewniak, “Prediction of Power Supply Noise From Switching Activity in an FPGA,” IEEE Trans. Electromagn. Compat. Vol. 56, pp. 699-706, 2014.

[MaS07] S. Mangard, et al. “Power Analysis Attacks: Revealing the Secrets of Smart Cards,” Chap. 6, Springer, 2007.

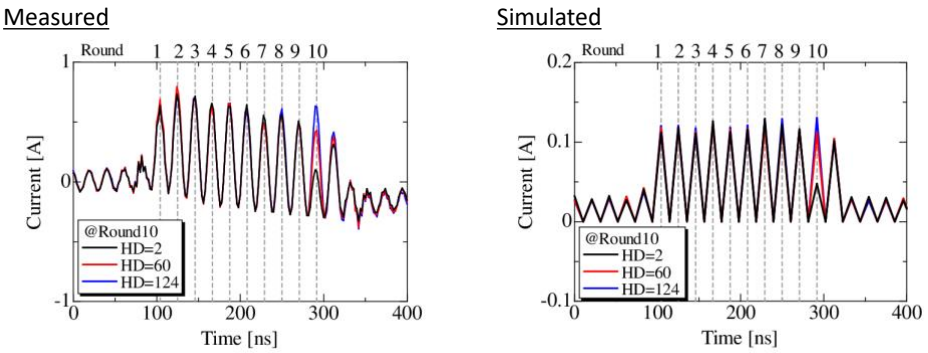


図 1　消費電流波形シミュレーション(左)、および実測波形(右)

４．研究成果

①暗号回路設計情報に基づくサイドチャネル攻撃耐性予測法

暗号回路の設計情報に基づき RTL レベルシミュレーションによりサイドチャネル攻撃耐性を予測する方法を開発した[2][8]。FPGA 実装した AES 回路を対象として HDL データに基づく RTL シミュレーションを実行し、得られた消費電流に対して代表的なサイドチャネル攻撃法の一つである電力解析攻撃を実行して攻撃耐性予測を得た。併せて、実測した消費電流に対する攻撃も実行し予測結果と比較した。その結果、RTL シミュレーションにより予測した攻撃耐性は実測に対する結果とよく一致した。サイドチャネル攻撃において攻撃者が取得する 1 次データとなる消費電流波形についても実測波形と形状および振幅ともによく一致した。図 1 はシミュレーションにより予測した消費電流波形、および実測波形であり、両者はよく一致している。シミュレーション波形をサイドチャネル解析した結果が図 2 である。こちらも実測波形を解析した結果とよく一致している。これらの結果より、暗号回路の設計情報に基づく RTL レベルシミュレーションによりサイドチャネル攻撃耐性を精度よく予測可能であることを示し、設計データからシミュレーションモデルを同定する方法を開発できた。

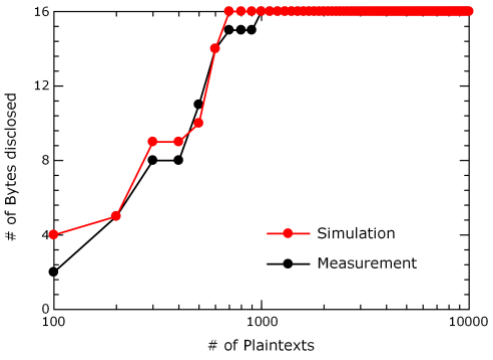


図 2　サイドチャネル攻撃シミュレーション

②暗号回路のサイドチャネル攻撃耐性設計手法

②-1 信号対雑音比に基づく設計方法論の検討

設計情報に基づく耐性予測に基づく暗号回路のサイドチャネル攻撃耐性の設計方法論の開発を目的として、サイドチャネル情報漏洩波形の信号対雑音比(SNR)による耐性予測の可能性を検証した[3][5][6][7]。実測した漏洩波形に基づく検討より、解析的に導出されたサイドチャネル情報漏洩強度を SNR の関数として表した関係式が実際に漏洩波形に対して成立することを示した。図 3 に示すように、実測されたサイドチャネル波形の SNR とその

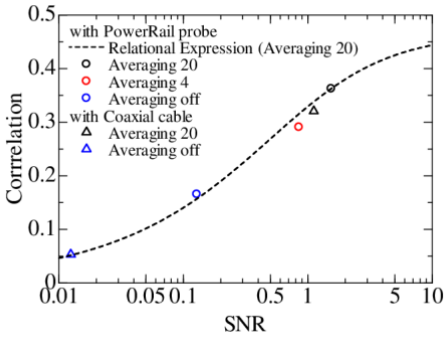


図 3　SNR と相関係数の関係式の検証

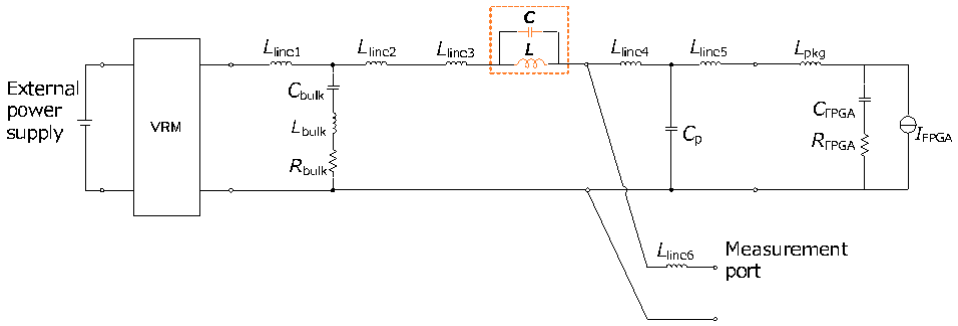


図 4　LC 共振器を付加した FPGA 電源系回路の等価回路

波形をサイドチャネル解析して得られて相関係数の分布が、SNR と相関係数の関係式とよく一致している。この結果は、サイドチャネル情報漏洩強度を漏洩波形の SNR より予測可能であることを示している。

②-2 サイドチャネル情報漏洩帯域の同定

サイドチャネル攻撃耐性の設計ため、情報漏洩周波数帯域を導出しそれを実験により検証した[4]。導出式に基づき FPGA 実装した AES 回路の漏洩帯域を求め、その帯域における消費電流の伝達係数を増加すると漏洩強度が増加することを確認した。FPGA 実装された AES 回路の情報漏洩帯域がクロック周波数の側波帯に存在することを確認し、側波帯に共振周波数を持つ LC 共振器を FPGA の電源系回路に付加することで側波帯の情報漏洩強度が増加することを確認した。図 4 は FPGA 電源系回路の等価回路であり、電源配線上に LC 共振器を追加している。この時、FPGA で発生するスイッチング電流 I_{FPGA} からサイドチャネル波形を観測する測定ポートへの伝達インピーダンスには図 5 に示すようにピークが発生する。本検討ではこのピークをクロック周波数の下側側波帯に合わせた。図 6 はクロック周波数の側波帯の一つである 37 MHz 付近の相関係数のピークが、側波帯に共振周波数を持つ LC 共振器を付加したことにより 0.17 から 0.23 へと増加した結果を示している。この結果は、サイドチャネル攻撃耐性評価において、クロック周波数の側波帯に共振器を付加するなどして情報漏洩強度を増大させ、評価コストを低減できる可能性を示唆している。

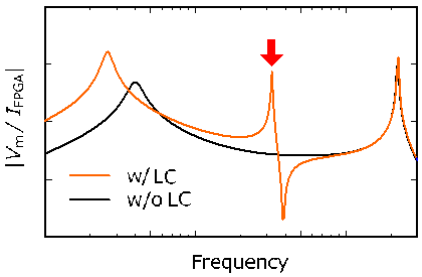
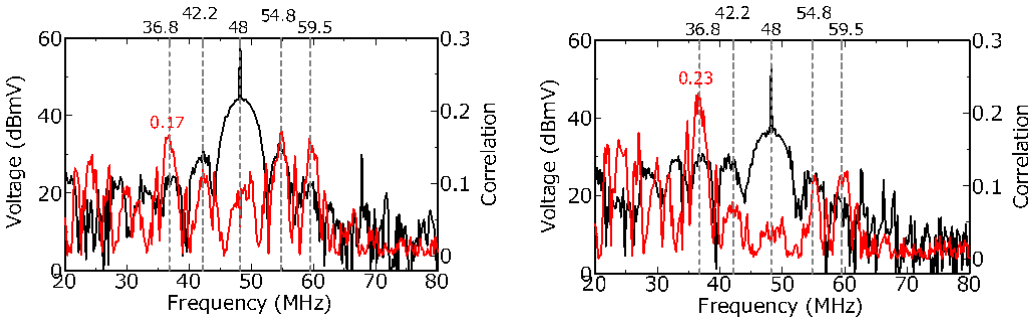


図 5　LC 共振器による伝達インピーダンスの変化



(a)LC 共振器なし　　(b)LC 共振器あり

図 6　LC 共振器による情報漏洩帯域の相関係数の増加

③サイドチャネル解析手法の応用による電磁妨害波源推定法

サイドチャネル攻撃法を応用し、EMI のノイズ源を推定する手法を開発した[1]。ノイズ源となるディジタル IC のスイッチング電流を IC で処理されるデータを変更することにより振幅変調し、その結果時間変動する EMI 強度と処理データの相関係数に基づき各 IC が発生する EMI 強度を定量的に推定する手法を開発した。この手法をノイズ源となりうるディジタル IC を 3 個搭載したプリント基板に対して適用し、その有効性を検証した。その結果、各 IC に起因する EMI 強度を 1 GHz 以下において数 dB 以下の誤差で推定できることを示した。

図 7 に開発したノイズ源振幅変調と相関解析(NSM-CA)手法の概略を示す。ノイズ源となる

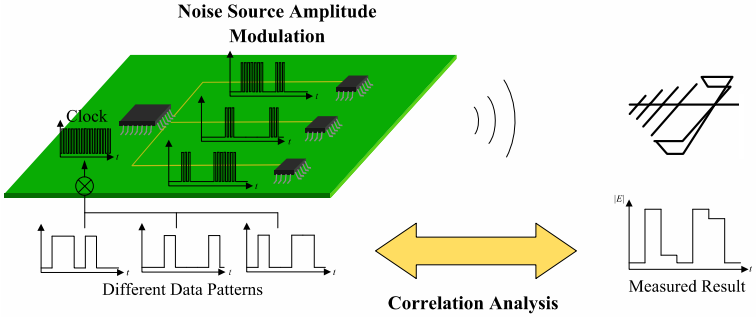


図 7　ノイズ源振幅変調と相関解析(NSM-CA)によるノイズ源強度推定法

IC のスイッチング電流を互いに異なる 2 値データ系列で振幅変調し、その時に観測される EMI の時間変動と変調信号である 2 値データ系列との相関係数より各 IC により発生する EMI の強度を推定する。この手法によりプリント基板上に実装された 1 つのラインドライバ IC のスイッチング動作に起因して発生する EMI の強度を推定した結果を図 8 に示す。クロック周波数の 50 MHz とその高調波でスペクトルが立っているが、その多くで推定結果は実測（黒実線）と一致しており精度よく推定できている。

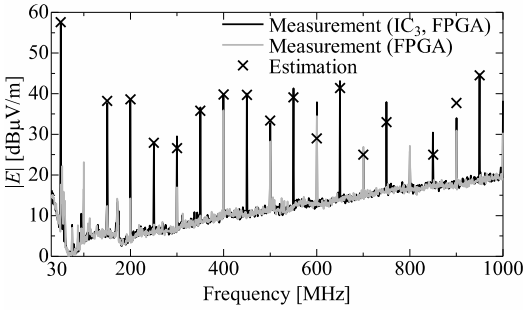


図 8　NSM-CA 手法により推定した個別 IC に起因する EMI 強度

５．主な発表論文等

〔雑誌論文〕（計　1 件）

[1] 吉野慎平, 五百旗頭健吾, 矢野佑典, 豊田啓孝, "ノイズ源振幅変調と相関解析に基づくノイズ源 IC 毎の電磁妨害波強度推定," エレクトロニクス実装学会誌, Vol. 22, No. 3, pp. 218-225, May 2019. https://doi.org/10.5104/jiep.22.218 (査読有り)

〔学会発表〕（計　7 件）

[2] 手嶋俊彰, 五百旗頭健吾, 豊田啓孝, 矢野佑典, “差分電力解析におけるサイドチャネル波形の SNR と相関係数の関係式パラメータの実験による同定,” 暗号と情報セキュリティシンポジウム (SCIS2019), 2D3-4, 滋賀県大津市, 2019.1.22-25.

[3] Kengo Iokibe, Toshiaki Teshima, Yusuke Yano, and Yoshitaka Toyota, “Extension of signal-to-noise ratio measurement method to byte-by-byte side-channel attack,” 2018 IEEE International Symposium on Electromagnetic Compatibility and 2018 Asia-Pacific Symposium on Electromagnetic Compatibility (EMC/APEMC), WE-PM-SS-09-3, pp. 745-748, Singapore, 2018.5.14-17.

[4] 河田直樹, 矢野佑典, 五百旗頭健吾, 豊田啓孝, "サイドチャネル攻撃耐性評価コスト削減を目的とした暗号機器への LC 共振器付加," 電子情報通信学会環境電磁工学研究会, EMCJ2018-101, pp. 77-81, Jan. 2018.

[5] 手嶋俊彰, 五百旗頭健吾, 豊田啓孝, 矢野佑典, "AES 回路から漏洩するサイドチャネル波形の SNR 測定法~バイト毎のラウンド鍵解読への適用~," 2018 年暗号と情報セキュリティシンポジウム (SCIS2018), 1D2-2, Jan. 2018.

[6] Yusuke Yano, Toshiaki Teshima, Kengo Iokibe, Yoshitaka Toyota, "Signal-to-Noise Ratio Measurements of Side-Channel Traces for Establishing Low-Cost Countermeasure Design," 2017 Asia-Pacific International EMC Symposium (APEMC 2017), WE-PM-7-02, pp. 93-95. 2017.

[7] 矢野佑典, 手嶋俊彰, 五百旗頭健吾, 豊田啓孝, "低コストな安全設計法実現のためのサイドチャネル波形の信号対雑音比測定法," 2017 年 暗号と情報セキュリティシンポジウム (SCIS 2017), 3C3-1, Naha, Japan, Jan. 2017.

[8] 五百旗頭健吾, 河田直樹, 矢野佑典, 籠谷裕人, 豊田啓孝, "内部電流源による暗号回路のサイドチャンネル情報漏洩部特定の試み ~AES 回路を実装し た FPGA に対する検討~," 電子情報通信学会環境電磁工学研究会, EMCJ2016-74, pp. 79-84, Sendai, Japan, Oct. 2016.

〔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/project.html

６．研究組織

(1)研究分担者

(2)研究協力者