暗号機器のサイドチャネル攻撃に対する安全設計に関する研究開発（122308001）

Development for Secure Design of Cryptographic Modules against Side-Channel Attacks

研究代表者

五百旗頭 健吾　岡山大学

Kengo Iokibe　Okayama University

研究分担者

野上 保之†　籠谷 裕人†　豊田 啓孝†　渡邉 哲史††

Yasuyuki Nogami†　Hiroto Kagotani†　Yoshitaka Toyota†　Tetsushi Watanabe††

†岡山大学　††岡山県工業技術センター

†Okayama University　††Industrial Technology Center of Okayama Prefecture

研究期間　平成 24 年度～平成 25 年度

概要

安全・安心な ICT 製品を普及させる基盤技術として、暗号 IC のサイドチャネル攻撃に対する安全性シミュレーション技術を開発した。シンプルだが情報漏洩源とその振舞いに特化した等価回路モデルにより、攻撃者が収集するサイドチャネル波形、そして攻撃に対する最終的な安全性の高精度予測を実現した。また、より強力な攻撃法であるフォルト攻撃についても、実験的検討により安全性予測実現に向けた課題を明らかにした。さらに、これらの研究開発成果を展示会や講習会等で地元企業に向けて発信し、その中から高度情報セキュリティ機能を有する新たな ICT 製品開発に向けた動きも生まれ始めている。

１．まえがき

ICT 技術の進化に伴い多くの情報が電子化されるなか、個人情報や企業、国家の機密データが漏洩する可能性も高まっている。そんな中、暗号化された情報を数学的に解読するだけでなく、暗号機器から副次的に漏洩する電磁波等の物理現象を利用して解読する攻撃(サイドチャネル攻撃)の存在が知られるようになっている。その結果、ICT 製品はサイドチャネル攻撃に対して安全であることが要求されるようになっている。そこで、本研究課題ではサイドチャネル攻撃への対策技術を組込んだ安全･安心な ICT 製品を普及させる基盤技術の開発を目的とした。

２．研究開発内容及び成果

サイドチャネル攻撃について、暗号機器の安全性を予測する手法を開発した。加えて、より強力な攻撃法と言われるフォルト攻撃に対しても安全性予測法開発の基礎検討を行った。さらに、地域企業技術者を対象として、これらの物理攻撃に関する安全設計講習会を実施した。

2.1. サイドチャネル攻撃に対する安全性予測

暗号機器のサイドチャネル攻撃に対する安全設計を実現する基盤技術として、機器設計の段階で安全性をシミュレーションする手法を開発した。

まず、評価対象の暗号機器としてサイドチャネル標準評価プリント基板の一つである SASEBO-G を使用し、等価回路モデルを構築した。SASEBO-G 上の FPGA には、暗号回路として鍵長が 128 ビット(16 バイト)の AES 回路を実装した。プリント基板上には種々の回路、部品、配線パターンが存在するが、そのうち、サイドチャネル情報の伝搬に支配的に寄与する要素のみを抽出し等価回路を構成した。構成要素は、暗号回路が実装された FPGA コア回路、およびコア回路に直流バイアスを供給する電源供給回路(Power Distribution Network: PDN)である。コア回路部は電流源と受動回路で構成される等価電流源で表す。電流源は暗号回路動作時にコア回路で発生する過渡電流を、受動回路は FPGA チップ上の V_{DD}-V_{SS} ポートから見たコア回路のインピーダンスを表す。PDN 部は FPGA パッケージおよびプリント基板部から成り、パッケージ部はボンディングワイアやインタポーザ配線のインダクタンスで構成される。プリント基板部は、基板上に実装されたデカップリングキャパシタや電圧レギュレータ IC 等の部品および配線のインピーダンスを RLC 素子で表している。

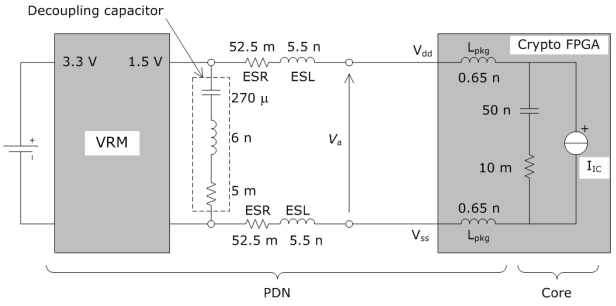
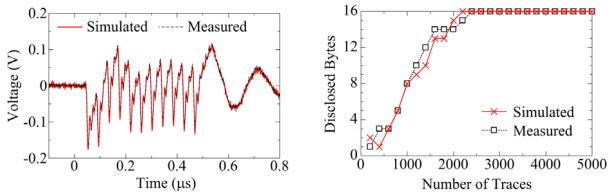


図 1 構築した等価回路モデル



(a)サイドチャネル波形　(b)鍵解読コスト

図 2　シミュレーション結果

サイドチャネル攻撃に対する安全性予測は、まず等価回路モデルに基づく回路シミュレーションにより攻撃者が取得するサイドチャネル波形を予測し、次に予測波形をサイドチャネル解析することで実現した。サイドチャネル攻撃では暗号化する平文の値に依存するサイドチャネル波形の変化を利用して秘密鍵を特定する。そこで、本研究開発では 5,000 通りの平文に対するサイドチャネル波形をシミュレートした。その一例を図 2(a)に示す。シミュレー

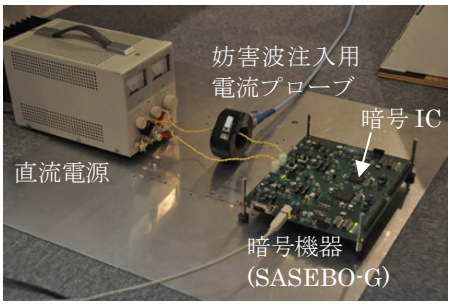


図 3 電源ケーブルへ妨害波注入によるフォルト発生実験

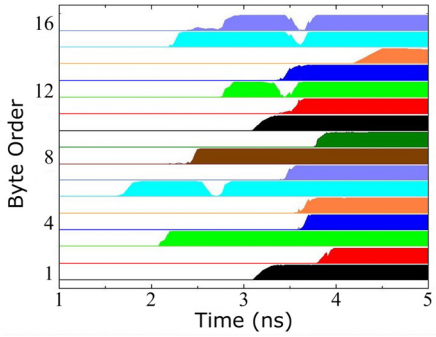


図 4　グリッチタイミングによるフォルト発生の変化

ション結果(赤)は実測波形(黒)とよく一致している。さらに、5,000 波形をサイドチャネル解析した結果を図 2(b)に示す。横軸は被解析波形数を、縦軸は秘密鍵の全 16 バイトのうち解読できたバイト数を表している。シミュレーション波形を解析すると、3000 波形で全 16 バイトを解読できており(赤)、実測波形の解析結果(黒)と一致している。

以上のとおり、サイドチャネル攻撃に対する安全性を高精度に予測する等価回路モデルを開発した。

2.2. フォルト攻撃予測に向けた検討

暗号機器のフォルト攻撃に対する安全性を決定づける支配的な要素を特定するため、2 種類の実験を行った。一つは、攻撃者が暗号機器に注入する妨害波の機器外部から暗号 IC への伝達しグリッチを発生させることを確認する実験であり、もう一つは、発生したグリッチが引き起こす誤り暗号文(フォルト)が、グリッチ形状にどのように依存するかを検証する実験である。

前者の結果、電源ケーブルから妨害波を注入することにより暗号 IC のクロック端子およびコア電源端子にグリッチを発生させられることを確認した(図 3)。そして発生するグリッチの大きさは注入位置からクロック端子や電源端子までの妨害波の伝達係数に依存することを推定した。

後者では、クロックグリッチの振幅およびタイミングを変化させた時の発生フォルトを観測し、グリッチ振幅が論理値判定の閾値を超え、かつ AES のラウンド処理が完了しないバイトが 1 バイト以上存在するタイミングでグリッチが入力した時にフォルト発生することを確認した。さらに、図 4 に示すように、グリッチタイミングのサブ ns の変化によって発生フォルトが変化することを確認した。

以上より、フォルト攻撃に対する安全性予測には、妨害波の伝達係数、そしてグリッチタイミングに対する発生フォルトの挙動評価が必要と明らかにした。

2.3. 地域における安全設計講習会等

岡山県内のエレクトロニクス企業との連携、および本研究開発で得られた知識の共有による地域企業の振興を目的として、サイドチャネル攻撃に対する安全設計技術に関


図 5　情報セキュリティセミナーの様子

する講習会「情報セキュリティセミナー」を開催し、26 名の参加を得た(図 5)。さらに岡山県内のエレクトロニクス企業技術者が参加するイミュニティ講習会において、本研究課題の成果を発表した。加えて、地域内外の展示会や研究会において計 7 回の出展・発表をし、本研究開発成果の地域企業への展開を図った。

3．今後の研究開発成果の展開及び波及効果創出への取り組み

現在までに、2.3 節で述べた情報セキュリティセミナーに参加した地元企業が、暗号技術を利用した無線通信機器の開発を開始している。この例のように、最終製品レベルにおいて、サイドチャネル攻撃に対する安全性を付加価値とする ICT 機器への展開が期待できる。さらに、暗号機器のコア部品の一つである暗号 IC レベルにおいても、開発した等価回路モデルに基づいた新たな対策回路の研究開発へと繋がる。

4．むすび

暗号機器へのサイドチャネル攻撃に対する安全設計の基盤技術として、等価回路モデルに基づく高精度な安全性予測法を開発した。また、フォルト攻撃に対する安全設計に向けても実験による予備検討を行い、安全性予測に向けた評価項目を明らかにした。さらに、地元企業の技術者を対象とした講習会の開催等を通じて、研究開発成果を地域へ還元し、その中からサイドチャネル攻撃に対する耐性を付加価値とする新たな製品開発の動きも出ている。

【誌上発表リスト】

[1]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 年 6 月)

[2]K. Nekado, Y. Nogami, and K. Iokibe, “Very Short Critical Path Implementation of AES with Direct Logic Gates,” The 7th International Workshop on Security (IWSEC2012), LNCS, Vol. 7631, pp.51-68 (2012 年 11 月 7 日)

[3]K. Iokibe, K. Maeshima, T. Watanabe, H. Kagotani, Y. Toyota, “Non Invasive Pulse Injection through Power Cable to Cryptographic FPGA for Fault Analysis,” 2014 IEEE International Symposium on Electromagnetic Compatibility, pp.743-747 (2014 年 8 月 7 日)

【本研究開発課題を掲載したホームページ】

http://www.oew.ec.okayama-u.ac.jp/project/scope2012