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　　６ 月 ２４ 日現在

機関番号：２１６０２
研究種目：基盤研究(C)（一般）
研究期間：2015～2018
課題番号：１５Ｋ００００８０

研究課題名（和文）プログラマブル遅延素子を用いた束データ方式による非同期式回路の耐タンパ性評価

研究課題名（英文）Evaluation of Tamper Resistance for Asynchronous Circuits with Bundled-data Implementation Using Programmable Delay Element

研究代表者

齋藤　寛（Saito, Hiroshi）

会津大学・コンピュータ理工学部・上級准教授

研究者番号：５０３６１６７１

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）：本研究では、非同期式回路の耐タンパ性を評価するために、プログラム遅延素子を用いた束データ方式による非同期式回路の設計を行った。プログラマブル遅延素子によって、暗号化における処理時間を変えることで、秘密鍵取得のための電力解析を困難にすることを想定している。成果として、プログラマブル遅延素子による非同期式回路モデル、および非同期式回路をXilinx FPGAに実装するための設計支援環境を実現した。

研究成果の学術的意義や社会的意義
電力消費の少ない非同期式回路に対して、さらにプログラマブル遅延素子を用いることで秘密鍵取得のための電力解析を困難にすることができれば、デジタル集積回路のセキュリティ向上に寄与することが期待できる。また、開発したXilinx FPGAを対象とした設計支援環境を用いることで、Xilinx FPGA上に非同期式回路を容易に実現することができる。近年、FPGAは、組み込みや機械学習の用途で広く用いられるため、こうしたアプリケーションの回路設計にも貢献することができる。

研究成果の概要（英文）：In this work, to evaluate the tamper resistance, we designed asynchronous circuit with bundled-data implementation using programmable delay element. By changing the execution time for encryption using programmable delay element, we expect to make difficult acquiring secret key. As the results of this project, we modeled asynchronous circuit with bundled-data implementation using programmable delay element and developed a design support environment to implement asynchronous circuits on Xilinx FPGA.

研究分野：非同期式回路，設計自動化

キーワード：非同期式回路　FPGA　サイドチャネルアタック

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９、ＣＫ－１９（共通）

１．研究開始当初の背景

一般的に、高い性能と安全性を実現するために、電子機器に組み込まれる暗号アルゴリズムは暗号モジュール（専用回路、FPGA、CPU など）上に実装される。暗号モジュールへの物理攻撃は、暗号モジュールに直接アクセスする方法や通信路にアクセスする方法があるが、暗号モジュールの物理情報から暗号解読を防止するのは暗号モジュール設計者の責任である。物理情報は主に、処理時間、電力、電磁波などが挙げられるが、これらを利用したサイドチャネル攻撃は、割と容易に行うことができるため深刻な脅威である。

我々はこれまでにクロック信号を用いずに、ローカルな要求・応答信号からなるハンドシェーク信号によって回路を制御する非同期式回路の研究を行ってきた。非同期式回路はクロック信号を用いた同期式回路と比べ、潜在的に低消費電力、低電磁放射といった利点がある。非同期式回路は、データ a を二線で表し（a.t と a.f)、有効データ（a = 0 は a.t = 0 と a.f = 1, a = 1 は a.t = 1 と a.f = 0）の間にスペーサ（a.t = a.f = 0）を入れ、有効データの完了を検出することによって次の処理に対する要求を行う二線方式による非同期式回路と、同期式回路と同じデータパス回路を用いて、要求信号線上に付加されたデータパスの最大遅延より大きい遅延素子によってタイミングを保証する束データ方式による非同期式回路に分類することができる。前者に関しては、二線論理の電力消費をバランスよくすることで Differential Power Analysis (DPA)を難しくするといった研究が存在する。しかし、回路面積が倍以上に増大するといった問題がある。後者に関しては、回路面積の増大は遅延素子を含んだ制御回路分のみであるが、データパス回路は同期式回路と同じなので、DPA に関しては本質的に同期式回路と同じであると考えることができるかもしれないが、仮に遅延素子にプログラマブルな物を用いれば、処理時間をランダムにすることができるので、同じ処理でも電力トレース毎に異なる波形が得られることが期待でき、DPA が困難になるのではないかと考えられる。

２．研究の目的

本研究の目的は、プログラマブル遅延素子を用いた束データ方式による非同期式暗号回路の電力・電磁波解析に対する耐タンパ性評価である。

３．研究の方法

本研究では耐タンパ性評価のために、産総研が開発したサイドチャネル攻撃の標準評価ボード SASEBO の互換ボードを用いる。SASEBO 互換ボードは、Xilinx 社の Field Programmable Gate Array (FPGA)に暗号アルゴリズム Advanced Encryption Algorithm (AES)を実装し、オシロスコープを用いて耐タンパ性の評価を行う。そのため、まず、耐タンパ性の評価を行う環境を構築する必要がある。次に、Xilinx FPGA にプログラマブル遅延素子を用いた束データ方式による非同期式暗号回路を実装するための、設計支援ツールセットの開発が必要である。一般的に、商用 FPGA は、クロック信号にて動作する同期式回路を想定しているため、FPGA の設計支援環境は非同期式回路の設計を想定していない。そのため、非同期式回路に特有な、設計制約の生成、タイミング検証、および遅延調整を自動化するツールセットを開発することで、非同期式回路の設計を容易にする。次に、提案するプログラマブル遅延素子を用いた束データ方式による非同期式回路にて AES アルゴリズムを SASEBO 互換ボード上に実装し、プログラマブル遅延素子の個数やバッファ数を変え、DPA および DEMA を行った上で耐タンパ性を評価すると共に、可能な限り電力消費が平坦となるようにプログラマブル遅延素子を制御した上で耐タンパ性を評価する。

４．研究成果

まず、SASOBO 互換ボード上から電力波形を取得する環境の構築を行った。次に、耐タンパ性の評価で利用する AES の回路モデルを取得し、制御ステートマシンの解析を行った。この制御ステートマシンを非同期式制御回路としてモデリングし、シミュレーションにて動作確認を行った。また、プログラマブル遅延素子のモデリングと動作確認を行った。ここでは、回路面積や遅延のパターンを念頭に、複数のプログラマブル遅延素子の構成を検討し、モデリング、および論理シミュレーションを行った。

一方、非同期式回路を Xilinx FPGA に実装するための設計支援ツールセットは、我々がこれまでに開発してきた Intel FPGA を対象とした設計支援ツールを拡張することで対応した。このツールセットは、Python 言語で実装されており、非同期式回路に特有な制約生成、タイミング検証、遅延調整を自動で行う。制約やレポートファイルの解析を Xilinx FPGA 向けに修正することで制約生成、タイミング検証、および遅延調整の全てを自動化するプログラムを完成させた。その後、2 つのベンチマーク回路を対象に、生成したプログラムの支援の下、非同期式回路を設計し、動作検証および評価を行った。また、評価の段階で、期待する性能が得られなかったため、配置制約を用いた性能最適化を検討し、配置制約を自動生成するプログラムを実装した。

当初計画に含めてなかった、SASEBO 互換ボード上から電力波形を取得する環境の構築、および、Xilinx FPGA に実装するための設計支援ツールセットに大半の時間を費やしたため、耐タンパ性の評価ができなかった。そのため、今後耐タンパ性の評価を行いたい。

５．主な発表論文等

〔雑誌論文〕（計 2 件）

- S. Semba and H. Saito, “Conversion from Synchronous RTL Models to Asynchronous RTL Models”, IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences, E102-A, No. 7, 2019. (印刷中)
- J. Furushima, M. Nakajima, and H. Saito, “Design of an Asynchronous Processor with Bundled-data Implementation on a Commercial Field Programmable Gate Array”, Informatica, Informatica, An International Journal of Computing and Informatics, vol.40, pp.399-408, 2016.

〔学会発表〕（計 6 件）

- S. Semba and H. Saito, “Comparison of RTL Conversion and GL Conversion from Synchronous Circuits to Asynchronous Circuits”, Proc. ISCAS, 2019.
- J. Furushima, T. Otake, and H. Saito, “Performance Optimization by Placement Constraints for FPGA-based Asynchronous Processors”, Proc. SASIMI, 2018.
- J. Furushima and H. Saito, “FPGA based Design of a Low Power Asynchronous MIPS Processor”, Proc. ICAIT, 2016.
- T. Urakawa and H. Saito, “Design of an Asynchronous Inverse Discrete Cosine Transform Circuit on an FPGA”, Proc. ICAIT, 2016.
- K. Yoshimi and H. Saito, “A Delay Adjustment Method for Asynchronous Circuits with Bundled-data Implementation Considering a Latency Constraint, Proc. SASIMI, 2016.
- S. Hosaka and H. Saito, “Constraining Operation Delay for Dynamic Power Optimization of Asynchronous Circuits”, Proc. IWAIT-2015, 2015.

〔図書〕（計 0 件）

〔産業財産権〕
○出願状況（計 0 件）

名称：
発明者：
権利者：
種類：
番号：
出願年：
国内外の別：

○取得状況（計 0 件）

名称：
発明者：
権利者：
種類：
番号：
取得年：
国内外の別：

〔その他〕
ホームページ等

６．研究組織

(1)研究分担者
研究分担者氏名：

ローマ字氏名：

所属研究機関名：

部局名：

職名：
研究者番号（8 桁）：

(2)研究協力者
研究協力者氏名：
ローマ字氏名：

※科研費による研究は、研究者の自覚と責任において実施するものです。そのため、研究の実施や研究成果の公表等については、国の要請等に基づくものではなく、その研究成果に関する見解や責任は、研究者個人に帰属されます。