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

平成　３０　年　　５　月　２５　日現在

機関番号：　１１１０１
研究種目：　基盤研究(C)（一般）
研究期間：　2015～2017
課題番号：　１５Ｋ００１７９

研究課題名（和文）動的解析による情報漏洩を防ぐための耐タンパ非同期式プロセッサの開発

研究課題名（英文）Development of Tamper-resistant Asynchronous Processors for Avoiding Information Leakage using Dynamic Analysis Methods

研究代表者

今井　雅（Imai, Masashi）

弘前大学・理工学研究科・教授

研究者番号：７０３２３６６５

交付決定額（研究期間全体）：（直接経費）　　3,600,000円

研究成果の概要（和文）：サイドチャネル攻撃は、現代のVLSIシステムの深刻な問題の1つとなっている。クロック信号が不要な非同期式回路では、要求・応答信号をランダムに遅らせるランダム遅延素子を用いることで、同じ論理動作でも異なる電流・電磁波特性を示す回路を実現できる。本研究では、高性能な回路を実現するため、立ち上がりエッジと立ち下がりエッジを区別しない2phaseハンドシェイクプロトコルに基づいた非同期式回路を対象とし、ランダム遅延素子の構成要素として、6段のインバータ構成で2段目と5段目に遅延要素となる負荷容量を付加する回路構成を提案し、非同期式AES暗号化回路に適用してその有効性を明らかにした。

研究成果の概要（英文）：Side-channel attacks have become one of serious issues in the modern VLSI systems. In asynchronous systems which do not require any clock signals, it is possible to change current/electromagnetic wave characteristics when performing the same logical operations by using random delay elements that can change the magnitude of their delay values at random. In this research, two-phase handshaking asynchronous circuits which do not distinguish between rising edges and falling edges are assumed in order to achieve high-performance circuits. The proposed random delay cells contain six inverter gates in which load capacitances are inserted into the second and the fifth inverter gates. The effectiveness of the proposed scheme is shown using asynchronous AES encryption circuits.

研究分野：　ディペンダブルコンピューティング、ハードウェアセキュリティ

キーワード：　サイドチャネル攻撃　耐タンパ　非同期式回路　2phaseハンドシェイクプロトコル　束データ方式データ転送　ランダム遅延素子　線形帰還シフトレジスタ

１．研究開始当初の背景

計算機システム内の秘匿情報は、データの処理・移動が行われていない時は暗号化などのソフトウェア的方式、物理的な接触が生じた時に記憶値を破壊するハードウェア的方式など、様々な手段により保護されている。一方、プロセッサ内でデータを処理する時には、暗号化されていない生の情報を扱うことになり、何も対策をしないと演算内容や処理データに応じた電流・電磁波が生じてしまう。そのため、それらシステム外部から観測可能な情報を利用して秘匿情報を窃取するサイドチャネル攻撃が情報セキュリティ分野における脅威となっており、データの処理・移動時における耐タンパ性（内部構造・情報の解析の困難さ）に優れた VLSI システムの実現が情報セキュリティ分野の重要な課題である。

電磁波を抑える方式として、クロック信号にわずかな変動を与えてピーク電流を分散させる周波数変調方式や、パッケージ材料を改良する方式などが提案されている。しかしながら、いずれもクロック信号の高周波数化には対応できていない。また、耐タンパ性に優れたプロセッサの開発としては、どのような演算を行っても電力特性や電磁波特性が同じになるように均一化する方式などが提案されている。しかしながら、論理ゲートにクロック信号により制御されたダイナミック論理回路を用いるためクロック信号の負荷が大きくなる。また、電流を均一に揃えるために余分な電力を消費するなどの問題がある。

２．研究の目的

コンピュータの要となるプロセッサにおいて、現在ほぼ全てで採用されている同期式回路では、記憶素子における情報の更新がクロック信号に合わせて一斉に行われるため、一定周期でピーク電流が流れ、大きな電磁波が発生する。一方、クロック信号を用いず、要求-応答方式により必要な箇所が必要な時にのみ動作する非同期式回路は、電流が分散・平坦化されるため電磁波の発生が大幅に抑制され、外部からの観測自体を困難にすることができる。

本研究では、非同期式回路は遅延変動に高耐性であるという利点を積極的に利用し、ランダムにタイミングをずらすことで、全く同じ処理でも異なる電流特性・電磁波特性を示す、耐タンパ性に優れたプロセッサを開発することを目的とする。クロック信号を一切使用しない非同期式回路設計方式を用いることにより、クロック信号に縛られた従来アプローチとは全く異なる、耐タンパ性に優れたプロセッサを開発する。また、これまでの研究では、同一製造プロセス、同一性能における同期式回路と非同期式回路のフェアな比較が十分に行われていない。そこで、本研究では、同期式回路と非同期式回路の定量的な評価を行い、セキュリティ分野における非同期式回路の有効性を明らかにする。

３．研究の方法

本研究では、はじめに図 1 に示す線形帰還シフトレジスタを用いたランダム遅延素子の開発を行う。その際、耐タンパ性を保証するために必要な遅延のランダム性や種類を検討し、それに応じた遅延素子を設計する。

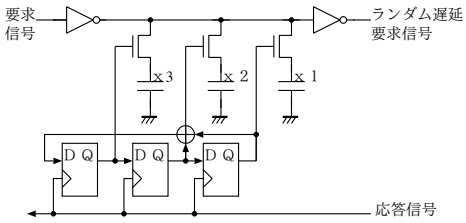

図 1:　ランダム遅延素子の構成

次に設計したランダム遅延素子を用いて、束データ方式に基づく非同期式暗号化回路を設計する。束データ方式は、組合せ回路は同期式と同じ 1 線式回路を用いることができるため、同一プロセスでありほぼ同一な性能を持った同期式回路を同時に設計することができる。また、ランダム遅延素子を用いない非同期式暗号化回路も設計し、それらを用いることで定量的な評価を行う。さらに、設計した回路は東京大学大規模集積システム設計教育研究センター（VDEC）が提供するチップ試作サービスを用いて実際にチップを試作し、実チップにより電磁波の評価などを行う。

４．研究成果

(1) ランダム遅延素子の設計

束データ方式非同期式回路を設計する際、ハンドシェイクプロトコルを決める必要がある。主なものとして 4phase ハンドシェイクプロトコルと 2phase ハンドシェイクプロトコルがある。4phase ハンドシェイクプロトコルはレベル論理であり、制御回路の設計が容易であるが、return-to-0 の動作のため速度性能に対するオーバーヘッドが大きい。一方、2phase ハンドシェイクプロトコルは遷移論理のため、回路が複雑になりやすいが、理論的には前者より 2 倍高速となる。そのため、本研究では、高速動作が可能な 2phase ハンドシェイクプロトコルを対象とした。

2phase ハンドシェイクプロトコルにおいて、遅延素子を要求-応答ハンドシェイク回路に用いる場合、立ち上がり遅延と立ち下がり遅延を等しくしなければならない。そのため、ランダム遅延素子として図 2 に示すように 6 段のインバータ構成とし、2 段目と 5 段目に遅延を調整するための容量を付加する構成を提案した。これにより、2 段目の負荷容量が立ち上がり遅延に影響する時には、同時に 5 段目が立ち下がり遅延に同じ影響を与えるよう

にする事ができる。また、接続される負荷容量のサイズを調整する機構として、N 段の線形帰還シフトレジスタを用いる方式を提案した。

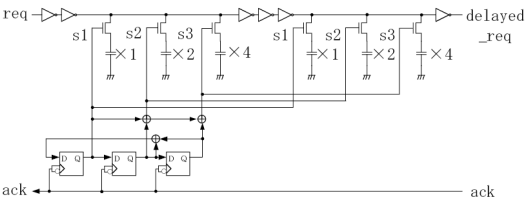

図 2: 2phase ハンドシェイク用ランダム遅延素子の構成

設計したランダム遅延素子は、VDEC を通してチップ試作を行うため、0.18μm プロセスを用いてレイアウトし、セルの特性を Synopsys 社 SiliconSmart により評価し、セルライブラリとして整備した。また、同時に D ラッチセル及びスキャン D ラッチセルなど、非同期式回路設計に必要となるセルも設計し、設計環境を構築した。これら非同期式回路設計用セルは VDEC のチップ試作サービスで NDA が結ばれた研究者に提供することができるよう、非同期式セルライブラリとして整備を行っている。

耐タンパ性を向上させる方式に関して検討した結果、以下のことが明らかになった。図 2 では 3 ビットの制御信号に対して 3 個のシフトレジスタを用いる手法を示しているが、この方式では 2^3-1=7 種類の遅延値しか生成できないため、耐タンパ性を向上させるためには、必要なビット数と等しい線形帰還シフトレジスタは用いず、ビット数の多い構成とした方がよい。また、複数のパイプラインステージにランダム遅延素子を適用する場合、各ステージで使用している線形帰還シフトレジスタで生成されるランダム値の個数の最小公倍数がシステム全体のランダム値の生成に関する周期を決定する。例えば、7 ビットと 8 ビットの線形帰還シフトレジスタの組合せを用いると、2^7-1=127 と 2^8-1=255 の最小公倍数は 32385 となる。これは 7 ビットと 8 ビットのうち 3 ビットしか用いない場合でも全体の周期としては 32385 サイクルとなることを表している。そのため、提案する方式を用いないプロセッサよりも 32385 倍、サイドチャネル解析に必要なデータ量を増加させることができる。

これらの成果は、ビット数を増加させることにより回路面積の増加を招くが、耐タンパ性を向上させることができることを示している。耐タンパ性と面積オーバーヘッドのトレードオフを考慮した設計が可能であることを明らかにしたものであり、今後の耐タンパ回路設計において、要求仕様に応じた設計方式の一つの指針となる。

(2) 耐タンパ非同期式暗号化回路の設計

2phase ハンドシェイクプロトコルに基づく高速な非同期式パイプラインテンプレートとして、D ラッチと XNOR ゲート、および遅延素子のみから構成される MOUSETRAP と呼ばれる構成が提案されている。記憶素子にフリップフロップではなく D ラッチを用いているため、D ラッチが書き込み可能になっている場合、それぞれのラッチでデータが到着したところから書き込みが行われる。そのため、タイミング信号に同期して一斉に書き込みが行われるフリップフロップを用いた構成と比べて、より電流を平坦化することができる。

図 3 に、AES (Advanced Encryption Standard) 暗号化回路の概略図を示す。expand_key モジュール、one_round モジュールおよび final_round モジュールはそれぞれ 2 つのパイプラインステージを持ち、合計 23 パイプラインステージの構成となっている。この回路構成はループ構造を持っていないため、非同期式化を行うに当たって、MOUSETRAP パイプラインテンプレートを容易に適用することができる。0.18μm プロセスを用いた場合、この回路の最小サイクルタイムは 1.4[ns] となった。そのため、ランダム遅延素子は 0.4～1.0[ns]の遅延を持つものとして設計した。

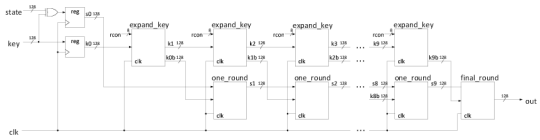

図 3: 同期式 AES 回路

図 4 に提案したランダム遅延素子を用いた耐タンパ非同期式 AES 暗号化回路の概略を示す。各パイプラインステージは MOUSETRAP パイプラインテンプレートを用いている。

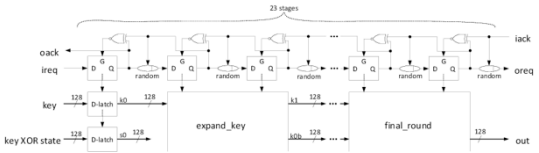

図 4: 耐タンパ非同期式 AES 回路

設計した AES 暗号化回路に関して、デジタルシミュレーションによりゲート出力の信号遷移の数を評価した例を図 5 に示す。横軸は時間であり、縦軸は信号遷移数である。両図は異なるシードを与えたときの、同一の一定時間での遷移数を比較したものである。シードにより信号遷移数が明らかに異なることが確認できる。すなわち、ランダム遅延素子を用いることで、回路の電流特性を変化させることが可能であると言える。

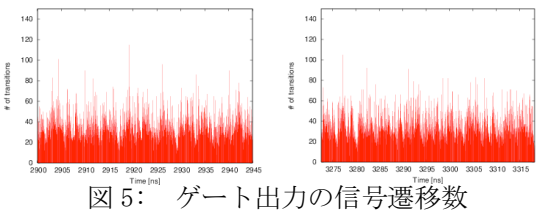

図 5: ゲート出力の信号遷移数

(3) 非同期式回路設計の有効性の評価

同期式回路と非同期式回路の定量的な評価を行うため、オンチップネットワークルータを両回路でそれぞれ設計し、評価を行った。その結果として、データ転送が疎に行われる状況では、非同期式回路の方がレイテンシを小さくできること、データ転送が密に行われる状況では、同期式回路の方が高いデータ入力周期にも対応できることが明らかになった。

一方、消費電力を比較すると図 6 となった。横軸はフリットの挿入周期、縦軸が消費電力である。図 6 に示すように、非同期式回路は使用しないときは一切電力を消費しないのに対し、同期式回路はゲーテッドクロック手法を適用したとしても電力が消費されるため、非同期式回路の方が低消費電力となることが明らかになった。このことは今後の VLSI 設計において、低消費電力が求められるときは非同期式回路の利用が有効であることを示している。

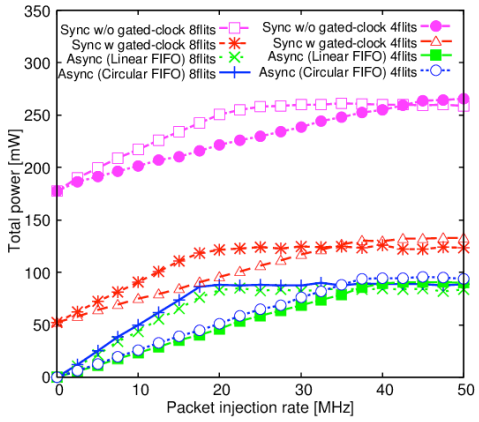

図 6:　オンチップネットワークの消費電力比較

また、ハードウェアセキュリティ面での同期式回路と非同期式回路の比較の例として、両者のネットワークオンチップルータに内部情報を摂取するハードウェアトロイを挿入し、その影響を評価した。その結果、非同期式回路は遅延非依存特性があるため、ハードウェアトロイ挿入に伴う遅延変動に対しても耐性があり、非同期式回路の設計方式に熟知している攻撃者に対してはトロイ挿入が容易になってしまう可能性があることを明らかにした。

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 寺山恭平, 今井雅, “ラッチベース非同期式回路のスキャンテスト,” 電子情報通信学会論文誌 A, 査読有, Vol. J99-A, No. 8, pp. 298-308, Aug., 2016, Online ISSN: 1881-0195

〔学会発表〕（計 28 件）

① 豊嶋太樹, 金本俊幾, 黒川敦, 今井雅, “ランダム遅延素子を用いた耐タンパ非同期式回路の設計,” 情報処理学会東北支部 (2.19, 弘前大学), Feb., 2018

② 豊嶋太樹, 金本俊幾, 黒川敦, 今井雅, “ランダム遅延素子を用いた非同期式回路の耐タンパ性向上に関する一考察,” 平成 29 年度電気関係学会東北支部連合大会, Aug., 2017

③ Shinichiro Akasaka, Toshiki Kanamoto, Atsushi Kurokawa, Masashi Imai, “A Study on Replica Delay Circuit of Bundled-Data Transfer Asynchronous Circuits,” Tohoku-Section Joint Convention of Institutes of Electrical and Information Engineers (IEEE Student Session), Aug., 2017

④ Koutaro Inaba, Tomohiro Yoneda, Masashi Imai, “A Study on Hardware Trojan Insertion into Asynchronous NoC Router,” ASYNC2017, May, 2017

⑤ 稲葉光太郎, 金本俊幾, 黒川敦, 今井雅, “非同期式 NoC ルータへのハードウェアトロイ挿入に関する研究,” 電子情報通信学会総合大会, Mar., 2017

⑥ Masashi Imai, Tomohiro Yoneda, “Hardware Trojan Insertion Difficulties into Synchronous and Asynchronous Circuits,” SASIMI2016, Oct., 2016

⑦ Daiki Toyoshima, Tatsuya Ishikawa, Atsushi Kurokawa, Masashi Imai, “Random Delay Elements for Tamper Resistant Asynchronous Circuits based on 2-phase Handshaking Protocol,” SASIMI2016, Oct., 2016

⑧ Masashi Imai, Theim Van Chu, Kenji Kise, Tomohiro Yoneda, “The Synchronous vs. Asynchronous NoC Routers: An Apple-to-Apple Comparison between Synchronous and Transition Signaling Asynchronous Designs,” NOCS2016, Sep., 2016

⑨ 今井雅, 米田友洋 “多数決イネーブルラッチを用いた非同期式回路の耐故障性に関する一検討,” 電子情報通信学会 VLSI 設計技術研究会 (6.16-17, 弘前市立観光館), VLD2016-39, Jun., 2016

⑩ 豊嶋太樹, 黒川敦, 今井雅,“ランダム遅延素子を用いた耐タンパ非同期式パイプライン回路,”電子情報通信学会 VLSI 設計技術研究会 (6.16-17, 弘前市立観光館), VLD2016-40, Jun., 2016

⑪ Masashi Imai, Tomohiro Yoneda,“Can Asynchronous Circuits Tolerate Hardware Trojan Threat?,” ASYNC2016, May, 2016

⑫ 石川達也, 黒川敦, 今井雅,“非同期式回路を用いたピーク電流抑制型バンドパスフィルタの実装と評価,”電子情報通信学会 デザインガイア 2015 (12.1-3, 長崎県勤労福祉会館), Dec., 2015

⑬ Masashi Imai, Tomohiro Yoneda,“Comparing Permanent and Transient Fault Tolerance of Multiple-core based Dependable ECUs,” CARS2015, Sep., 2015

⑭ 豊嶋太樹, 寺山恭平, 黒川敦, 今井雅,“ラッチを用いた非同期式パイプライン回路の機能テストに関する一検討,”電子情報通信学会 ディペンダブルコンピューティング研究会 (6.16 機械振興会館), DC2015-19, Jun., 2015

６．研究組織

(1)研究代表者

今井　雅 (IMAI, Masashi)

弘前大学・理工学研究科・教授

研究者番号：７０３２３６６５