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　６ 年　 ５ 月 １４ 日現在

機関番号：１４４０１
研究種目：研究活動スタート支援
研究期間：2022～2023
課題番号：２２Ｋ２１２７６

研究課題名（和文）サイドチャネル攻撃に高い耐性を持つマルチコアIoTデバイスのソフトウェア基盤

研究課題名（英文）Side-Channel Attack Resistant Software Platforms for Multicore IoT Devices

研究代表者
西川　広記（Nishikawa, Hiroki）

大阪大学・大学院情報科学研究科・助教

研究者番号：９０９６３５３８

交付決定額（研究期間全体）：（直接経費）　　2,200,000円

研究成果の概要（和文）：本研究では、インターネットに接続される小型デバイス（IoTデバイス）のセキュリティ強化を目的として、情報を安全に保護するための対策に関する成果を出した。具体的には、CやC++といったプログラミング言語からデジタル回路に自動で変換する高位合成技術を用いて設計されたAES暗号回路の安全性を多角的に評価した。さらに、CPU上で動作するAESにおいて、暗号化の際にラウンド関数内の各関数をランダムな順序で実行するシャッフリング技術を応用し、拡張した。この手法は情報を予測不可能な順序で処理し、攻撃者による暗号鍵の解読をより困難にすることを目指している。

研究成果の学術的意義や社会的意義
Society 5.0の実現に向け、Internet of Things (IoT) デバイスは様々なフィールドで普及しつつある。一方で、サイドチャネル攻撃などの物理セキュリティ攻撃の危険に晒されている。この脅威に対し、これまでに多数のセキュリティに特化した専用のハードウェアやソフトウェアが開発されてきたが、専用ハードウェアを刷新したり、セキュリティ対策 ソフトウェアを特別に開発したりするにはコストの増大が課題となる。本研究の意義は、オペレーティングシステムの基盤技術のみを活用することでサイドチャネル攻撃に強いソフトウェア基盤を提供できないか？」という問いに答えることにある。

研究成果の概要（英文）：In this study, we aimed to enhance the security of small devices connected to the Internet (IoT devices) and produced results concerning measures to protect information safely. Specifically, we evaluated the safety of AES encryption circuits designed using high-level synthesis technology, which automatically converts programming languages such as C and C++ into digital circuits. Furthermore, we extended and applied shuffling technology, which randomizes the order of functions within the round function during encryption, on AES operations performed on CPUs. This method processes information in an unpredictable order, making it more difficult for attackers to decrypt the encryption keys.

研究分野：計算機システム

キーワード：ハードウェア・セキュリティ　サイドチャネル攻撃

１．研究開始当初の背景

Society 5.0 の実現に向けて、Internet of Things（IoT）デバイスは、家庭、オフィス、工場、農地など多岐にわたるフィールドで広く普及している。これらのデバイスは、様々な分野で注目を集めているが、物理的に多様なフィールド上に配置されるため、サイドチャネル攻撃を含む物理セキュリティ攻撃のリスクに常に晒されている。サイドチャネル攻撃とは、デバイスの応答時間や消費電力、発生する電磁波などの物理情報を観測し、統計的に解析することにより、デバイス内部の秘密情報を不正に取得する手法である。これに対抗するため、多くのセキュリティ専用ハードウェアやソフトウェアが開発されてきたが、これらの対策は設計・開発コストの増大という課題を抱えている。したがって、本研究は、オペレーティングシステムの基盤技術のみを活用し、サイドチャネル攻撃に強いマルチコア IoT デバイスのソフトウェア基盤を提供できるかという問いに答えるものである。

２．研究の目的

本研究の目的は、マルチコア IoT デバイスにおけるサイドチャネル攻撃に対して高い耐性を持つソフトウェア基盤技術を開発することであり、是を以て前項(1)で提起した問いに答える。特に本研究で注目する基盤技術は、Large-Scale Integration (LSI) の設計技術としても知られるタスクスケジューリングである。本研究では、このタスクスケジューリング技術と並列処理とを組み合わせたソフトウェア基盤を開発し、サイドチャネル攻撃に強い IoT デバイスを実現する。

３．研究の方法

過去に得られた科学研究補助金による研究を通じ、タスクを複数スレッドへ並列化し、それらを適切にスケジューリングすることでマルチコアの性能向上や低消費エネルギー化を図る技術を開発してきた。これらの研究成果に基づくタスケジューリング技術をさらに活用し、各タスクの並列度や動作周波数、各スレッドの開始時刻をランダムに決定することで得られるスケジュールのランダム性を高め、消費電力と暗号処理との相関を大幅に減少させる。これにより、暗号処理の情報を隠蔽することが可能となる。これが本研究で提案するサイドチャネル攻撃に強いマルチコア IoT デバイスにおけるセキュリティ対策ソフトウェア基盤技術である。この技術の実現に向けて、これまでの研究を一層発展させる。まず、並列度および各スレッドの開始時刻だけでなく動作周波数を決定する手法を開発する。開発した手法に基づいて得られたスケジュール結果が電力解析と暗号処理との間の相関を減少させることを、 シミュレーションを通して実証する(研究Ⅰ:理論研究)。後に、マルチコア IoT デバイス上に本手法を適用する。その上で、本研究で開発された技術がサイドチャネル攻撃に対してどれだけの耐性を持つかを実際の IoT デバイス上で評価し、その優位性を明らかにする (研究Ⅱ:実装と評価)。このように研究計画は 研究Ⅰおよび研究Ⅱに分割して遂行される予定である。つまり、これらの研究を遂行することが本研究の達成を意味する。

４．研究成果

本研究では、インターネットに接続される小型デバイス（IoT デバイス）のセキュリティ強化を目的として、情報を安全に保護するための新しい対策を検討した。当初想定していたマルチコアにおけるハードウェアセキュリティを想定していたが、当該研究費では要求されるオシロスコープの発注が困難であることが判明し、方向転換を余儀なくされた。そこで、FPGA 上に設計された AES 暗号回路に対するサイドチャネル情報の漏えい量を評価することと Chipwhisperer と呼ばれるサイドチャネル攻撃評価用ボードを利用し、サイドチャネル情報の漏えい量を評価した。

まず、C や C++といったプログラミング言語からデジタル回路に自動で変換する高位合成技術を用いて FPGA 上に設計された AES 回路の安全性を評価した。当該研究では、異なるクロック周期を持つ 7 つの AES 回路を設計し、そのサイドチャネル漏洩量を評価した。この研究では AES の回路クロック周期と電力サンプリング間隔の関係に着目し、これらがサイドチャネル情報の漏えいに対してどのような影響を及ぼすかを実験的に明らかにした。図 1 にその概念図を示す。まず、C 言語を用いて CHStone と呼ばれる高位合成用ベンチマークライブラリで提供される AES を Vivado HLS と呼ばれる高位合成ツールを利用し、FPGA における暗号回路を合成する。この回路に対して任意の平文を大量に入力し、その都度電力波形をサンプリングすることで電力トレースを得る。取得された電力トレースに対する T 値を評価することにより、電力攻撃への耐性評価を行う。

RTL コード設計された HLS を用いて、ロジック合成およびロジックシミュレーションが実行される。ロジック合成は、Verilog HDL や VHDL で記述された RTL コードからロジック回路を実装するものである。本研究では、ロジック合成とロジックシミュレーションに

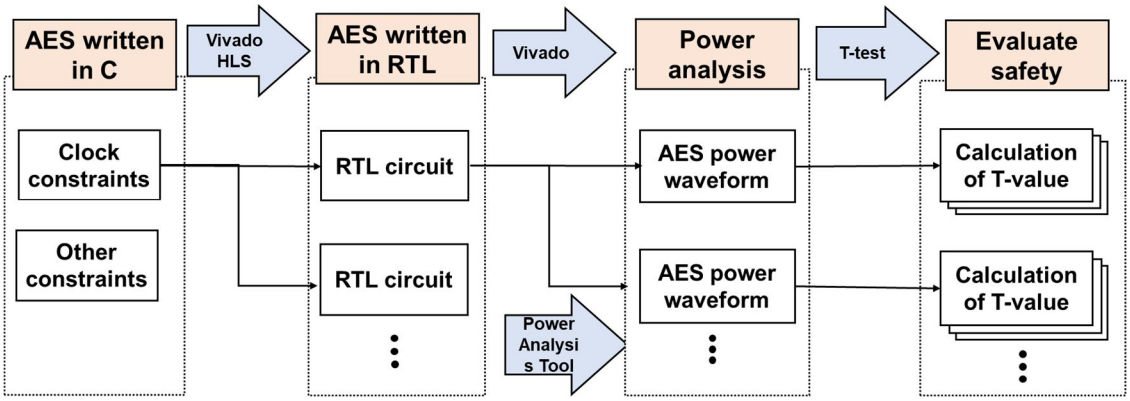


図 1. FPGA 上に設計された AES 回路に対するサイドチャネル攻撃の流れ

表 1. AES 回路の合成およびシミュレーション結果 t

Clock constraint [ns]	7.0	7.5	8.0	8.5	9.0	9.5	10.0
Clock cycles	5,889	5,825	5,359	5,223	4,559	4,559	4,544
Execution time [ns]	41,223	43,688	42,872	44,396	41,031	43,311	45,440
Slices	655	651	632	656	648	643	651
Average power [uW]	12,213	11,182	10,837	10,389	10,535	9,981	9,635
Energy consumption [nJ]	503	488	464	461	432	432	437

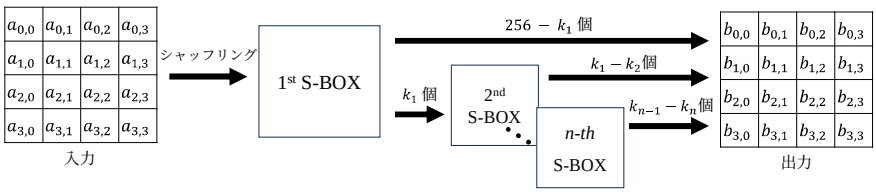
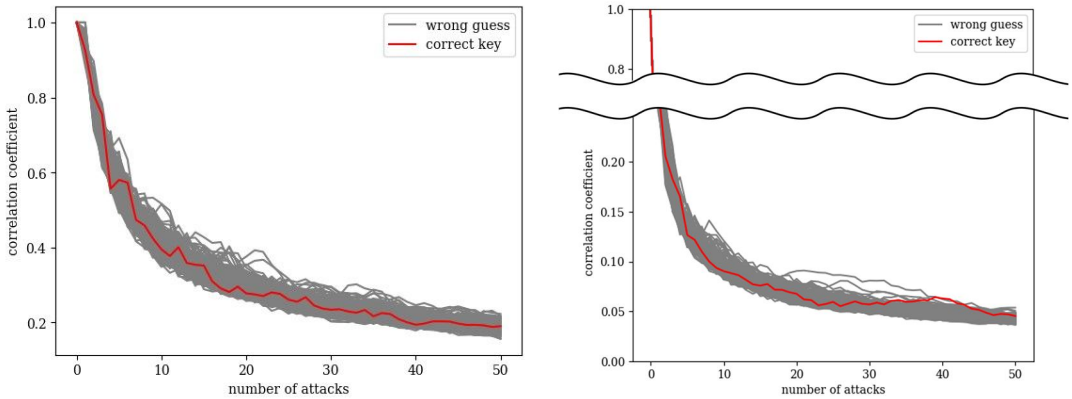


図 2.　*N* 個の S-BOX を用いたオペレーション・シャッフリング

Vivado 2019.2 を用い、ターゲットデバイスとして Zynq XC7Z020 を指定している。合成された 7 つの AES 回路のロジックシミュレーションは Vivado で行われ、回路のクロック周期は設定されたクロック制約に応じて速く動作することが求められる。ロジックシミュレーションを採用する理由は、ノイズや環境による誤差がないため、より正確な電力分析が可能であるからである。この研究においては、128 ビットのランダム平文に対して 20 回、固定平文に対して 10 回の暗号化が実施される。これらの条件下で Vivado によるロジックシミュレーションが行われ、回路に関する情報を含む VCD ファイルが出力される。ロジックシミュレーションから得られたクロックサイクル数、実行時間、スライス数、平均電力、エネルギー消費量は表 1 に示されており、クロック制約が大きくなるにつれて、電力およびエネルギー消費量は減少傾向にあることが確認される。クロック制約が 9.0 ナノ秒より大きい場合には変化が見られない。これは、クロック制約が 9.0 ナノ秒を超えるとクロックサイクル数が変わらないためである。本研究で設計された AES 回路は、スライス数に関して相関関係を示さなかった。実験結果から、クロック周期とサンプリング間隔は、サイドチャネル情報の漏えい量において相互干渉しないことが明らかとなった。この研究成果は、5 件の国際会議で発表し、3 編の国際学術論文誌にまとめて投稿した。それらの論文はいずれも出版済みである。

次に、CPU 上で動作する AES において、暗号化の際にデータをランダムに配置するシャッフリング技術を応用し、拡張した。図 2 は，S-BOX を n 個利用する場合の提案手法の概略を示す．左端の 4×4 の行列は，入力である．これらの値を，予め設計された複数の S-BOX を通じて非線形変換する．まず，16×16 の計 256 個の要素からなる S-BOX から，ランダムに k (k≤256) 個の要素を選択する．i (i≤n)番目の S-BOX で選ばれた k_i 個の要素は，さらに i+1 から n までのいずれかの個数の S-BOX を用いて非線形変換される．これらの操作をシャッフリングしながら行う． 例えば， S-BOX の 2 つだけ用いて変換する場合，256 個の要



(a). 500 トレース攻撃時の相関係数　　(b). 10,000 トレース実行時の相関係数

図 3. 電力解析攻撃実行時の相関係数: 灰色: 鍵候補に対する相関係数、赤色: 正解鍵の相関係数

表 2. 10,000 回実行時の実行時間 (sec)

一般的な AES	提案手法
430.85 (1.00)	481.15 (1.12)

素のうちランダムに選択された k 個は 2 つ目の S-BOX を通過し．その他 256-k 個はそのまま 1 つ目の S-BOX で非線形変換されて出力される．このように，入力がアクセスすべき S-BOX の個数をランダム化することで，中間値を空間的に値が Masking し，かつ，メモリアクセス数の増大により時間方向に中間値が Hiding されることで，消費電力と中間値との相関が低減される．従来のシャッフリング技術は、AES における S-Box 関数の実行順序を単にランダム化するのみで、組合せが非常に少なく、容易に暗号鍵の特定が為されていた。しかし本研究で提案するシャッフリング技術は、S-Box 関数を実行する際に実行順序をランダム化するだけでなく、マスキングを複数回冗長的に行うことで組合せ爆発を起こし、暗号鍵の解析を困難にしている。図 3 は、電力解析攻撃をそれぞれ 500 トレースと 10,000 トレース実行したときの相関係数の変化を表している。横軸は、500 トレースと 10,000 トレースを表しており、それぞれ 10 トレースと 200 トレースずつで相関値を平均したものがプロットされている。プロット図 3(b)は、最初の秘密鍵予測でのすべての鍵候補の相関係数を示している。これらグラフから、正しい秘密鍵の相関係数は他の鍵候補のいくつかよりも小さいことがわかる。したがって、秘密鍵は特定されていない。これらの結果から、提案された方法は 500 トレースおよび 10,000 トレースの相関電力分析に対して攻撃耐性があることが示された。表 2 では、AES と提案手法を 10,000 回実行したときの実行時間を表している。図前述した処理を追加したことにより約 1.12 倍の実行時間増大となったが、従来のシャッフリングに比べて暗号鍵の解読が困難になることを確認した。この研究成果は、国内学会において 1 件の口頭発表を行い、現在は国際会議に向けて執筆中である。

５．主な発表論文等

〔雑誌論文〕　計1件（うち査読付論文　1件／うち国際共著　0件／うちオープンアクセス　0件）

１．著者名 Zhao Yilin、Nishikawa Hiroki、Kong Xiangbo、Tomiyama Hiroyuki	４．巻 12
２．論文標題 Side channel power analysis resistance evaluation of masked adders on FPGA	５．発行年 2023年
３．雑誌名 International Journal of Reconfigurable and Embedded Systems (IJRES)	６．最初と最後の頁 97～97
掲載論文のDOI（デジタルオブジェクト識別子） 10.11591/ijres.v12.i1.pp97-112	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

〔学会発表〕　計3件（うち招待講演　0件／うち国際学会　3件）

１．発表者名 Yuto Miura, Takumi Mizuno, Hiroki Nishikawa, Xiangbo Kong, Hiroyuki Tomiyama
２．発表標題 Impacts of Clock Constraints on Side-Channel Leakage of HLS-Designed AES Circuits
３．学会等名 International Conference on Electronics, Information, and Communication (ICEIC)（国際学会）
４．発表年 2022年

１．発表者名 Takumi Mizuno, Hiroki Nishikawa, Xiangbo Kong, Hiroyuki Tomiyama,
２．発表標題 Empirical Analysis of Side-Channel Attack Resistance of HLS-Designed AES Circuits,
３．学会等名 International Conference on Electronics, Information, and Communication (ICEIC)（国際学会）
４．発表年 2022年

１．発表者名 Eiji Sugahara, Hiroki Nishikawa, Xiangbo Kong, Hiroyuki Tomiyama
２．発表標題 Energy Consumption Reduction through Resource Allocation Using Docker
３．学会等名 International Workshop on Advances in Networking and Computing (WANC)（国際学会）
４．発表年 2022年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関