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　２ 年　 ６ 月　 ５ 日現在

機関番号：１２６１２
研究種目：研究活動スタート支援
研究期間：2018～2019
課題番号：１８Ｈ０６４６０・１９Ｋ２１５２９

研究課題名（和文）General and Efficient Masking Strategy for Fixed Secret Value Against Side-Channel Attacks

研究課題名（英文）General and Efficient Masking Strategy for Fixed Secret Value Against Side-Channel Attacks

研究代表者

李　陽（LI, Yang）

電気通信大学・大学院情報理工学研究科・准教授

研究者番号：２０８２１８１２

交付決定額（研究期間全体）：（直接経費）　　2,300,000円

研究成果の概要（和文）：本研究は、単純電力解析に対する、AES鍵スケジュールのより正確で安全性評価できる鍵復元アルゴリズムを確立した．マスクされた鍵に対した鍵復元効率を大幅に改善し、既存研究と比較して、鍵復元速度は最大95%向上した.特定のシナリオでは、鍵復元の成功率が47%から96%に向上した．そして、漏洩モデルとノイズモデルのバリエーションが増えることを対応して、鍵復元アルゴリズムの汎用性を拡張した．最後に、制限されたランダム量を使用した場合、鍵復元の計算量を最大化できるマスキングスキームを設計した．これに基づいて、マスキングのランダム量と電力攻撃に対する安全性の間に正確な比例関係を確立した．

研究成果の学術的意義や社会的意義
電力攻撃の対策として、AES鍵スケジュールのマスキング技術の研究成果は、非侵入型物理攻撃の基本的な問題に属する．研究成果は、ハミング重みリークモデルに基づく他の安全性解析問題にも影響を与える． 関連する研究結果は、電力攻撃に対する冗長に保存した固定値の汎用的なマスキング方法にも拡張できる．そして、鍵復元の計算量を正確に評価することにより、さまざまなマスキングスキームの実際の安全性を合理的に評価し、AESを載せった暗号チップの設計者に、コストと安全性のバランスを取った鍵スケジュール部分のマスキングスキームを提供することができる．

研究成果の概要（英文）：This research has established a key recovery algorithm that can evaluate the security of AES key scheduling against simple power analysis more accurately and more efficiently. The key recovery speed has been improved up by 95%. In certain scenarios, the success rate of key recovery increased from 47% to 96%. Then, the versatility of the key recovery algorithm was expanded in response to the variations of the leakage model and the noise model. Finally, we designed a masking scheme that maximizes the computational complexity of the key recovery when the amount of randomness is limited. Based on this masking scheme, we established a proportional relationship between the random amount of masking and security against simple power analysis.

研究分野：情報セキュリティー

キーワード：AES　マスキング　サイドチャネル攻撃

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

スマートカードに代表される電子スマートデバイスは、金融、交通、アクセス制御などのさまざまな情報システムで広く利用されている．スマートデバイスには通常、暗号アルゴリズムが組み込まれており、通信セキュリティやデータセキュリティなどのセキュリティ要件を保証している．暗号システムの安全性は、鍵の安全性に基づいている．攻撃者は、暗号デバイスの暗号アルゴリズムの実行時間、消費電力、電磁波、故障出力などの情報を取得し、鍵復元の攻撃に使う．これらの非侵襲的物理攻撃は、暗号デバイスの動作状態を変更せず、実装コストが低く、攻撃の検出が困難であり、強力な鍵復元能力を備えているという特徴がある.したがって、このような攻撃は、暗号デバイスのセキュリティに深刻な脅威をなってしまう．

電力攻撃に代表されるパッシブ攻撃の主流の対策が、情報隠蔽技術（Hiding）とマスキング技術（Masking）に大きく分類されている．その中、マスキング技術は、計算に乱数を導入することにより、処理されたデータと秘密情報の間の相関を排除し、電力攻撃に対する安全性を実現する．既存のマスキング技術について、ほとんどの研究はラウンド関数に向けられているが、鍵スケジュール部分の研究は比較的少ないである．鍵スケジュールの場合、鍵を交換しない限り、計算プロセスと計算結果は固定される.したがって、鍵スケジュールに対する攻撃は、大量のデータを処理して統計情報を取得することはできない．

ブロック暗号 AES の鍵スケジュールに対する電力消費攻撃は、Biham と Shamir によって最初に提案された．8 ビットマイクロプロセッサに実装されている AES の場合、攻撃者は鍵スケジュールに、一部のオペランド（各ラウンド鍵の各バイト）のハミング重みを観察できることを仮定する．攻撃者は、これらのハミング重みと、鍵スケジュールアルゴリズムの鍵バイト間の計算関係を使用して、AES の鍵スペースを削減する．

2003 年に Mangard は、対策なしの AES 鍵スケジュールの鍵復元方法を最初に提案した．2005 年に、VanLaven らは、同じ問題に対してより効果的な鍵復元アルゴリズムを提案した．2014 年、Christophe らは 3 つ対策済みの AES 鍵スケジュールの安全性を分析し、その結果を国際会議 CHES2014 で公開された．分析したマスキング対策スキームに対して、Christophe らはそれぞれに対して鍵復元攻撃実験を行ったが、いずれも効果的な対策ではないことが確認された．

２．研究の目的

Christophe らはいくつのマスキング方法の安全性を分析したが、AES の鍵スケジュールに効果的なマスキングスキームを実現するにはまだ大きなギャップが存在する.そして、CHES2014 で公開された安全性分析は、攻撃者の鍵復元能力を過小評価し、ランダムな量の割り当てスキームが変更された場合の汎用的な安全性解析の能力を欠きしているし、効果的なマスキングスキームを提供できていない．

AES の鍵スケジュールに対する鍵復元攻撃は、暗号化製品に対する真の脅威になる.本研究は、既存研究よりも効率的かつ汎用的な鍵復元アルゴリズムを設計し、AES 鍵スケジュールの安全性評価を最適化したい．そして、固定値である AES 鍵スケジュールの低リソース実装のコストとセキュリティ強度のバランスを取れる実用的かつ明確なマスキングスキームを提供したい．最後に、固定値に対する電力攻撃の安全性評価の理論的基礎を提供することを目的にしている．

３．研究の方法

研究目標を達成するために、3 つのステップに分かれている.

(1) まず、AES 鍵スケジュールに対する単純電力攻撃に効率的な鍵復元アルゴリズムを確立する. 既存のアルゴリズムと比較して、新しいアルゴリズムは、鍵復元の計算量とデータ量を軽減し、マスキングスキームの安全性評価の精度を向上させる.
(2) ノイズを導入した鍵復元問題に対して、鍵復元アルゴリズムの汎用性を拡張する. 改善された鍵復元アルゴリズムは、ノイズモデルによって鍵復元でき、ノイズリークモデルでのマスクされた AES 鍵スケジュールの安全性評価のために使用できる.
(3) 汎用的な鍵復元アルゴリズムに基づいて、AES 鍵スケジュールの新たなマスキングスキームを確立する.汎用的な鍵復元アルゴリズムの計算量を分析することにより、ランダムビットの総量を制限するときに、鍵復元の計算量を最大化するランダムビット割り当て方式を見つける.

４．研究成果

(1) AES 鍵スケジュールの効率的かつ汎用的な鍵復元アルゴリズムとマスキング技術の確立

本研究では、単純電力攻撃の下での鍵スケジュールのためより正確で安全性評価できる鍵復元アルゴリズムを確立した. マスクされた鍵に対した鍵復元効率を大幅に改善し、既存研究と比較して、鍵復元速度は最大 95%向上した。特定のシナリオでは、鍵復元の成功率が 47%から 96%に向上した。これらの改善は、(1) 鍵復元の新しいデータ構造、(2) ハミングウェイトからの情報抽出の改善、(3) すべての情報漏えいの完全な使用、(4) 鍵復元の最適化された復元シーケンスなど、いくつかの手法から由来する。そして、漏洩モデルとノイズモデルのバリエーションが増えることを考慮して、改善された鍵復元アルゴリズムをさらに拡張した。最後に、制限されたランダム性を使用して鍵復元の複雑さを最大化できるマスキングスキームを設計した。確立された鍵復元アーキテクチャに基づいて、セキュリティ評価結果とマスキングスキームの関係を要約し、マスキングスキームのいくつかの設計原則に従って形式化された。これらの成果はまだ投稿中である.

本研究は、AES 鍵スケジュール部分のマスキング技術を研究して、電力攻撃に対抗し、マスクのランダムな量と電力攻撃に対する安全性の間に正確な比例関係を確立した.これに基づいて、ランダムビットの総数が制限されている場合に、最適なマスキングスキームと鍵復元の計算量の対応が得られた.実際の暗号アルゴリズムの実装者が合理的なマスキングスキームを選択する理論知識を提供した.

(2) 認証暗号に対する差分故障攻撃の安全性評価の改善

データ複雑度最適化のアイデアを使用して、AES 構造を使った認証暗号 PAEQ に対する差分故障攻撃の安全性解析を改善した. PAEQ は、2014 年に Biryukov と Khovratovich によって提案された AES ベースの認証暗号である. CHES 2016 で、Dhiman Saha と Dipanwita Roy Chowdhury は、差分故障解析を PAEQ への適用した. 本研究では、既存研究が PAEQ-128 の差分故障解析が完全に最適化されていないことを明らかにした. AES の情報理論分析と差分故障解析技術を PAEQ に採用して、PAEQ-128 で実用的な差分故障解析が実現できることを示した. 具体的には、既存研究の攻撃仮定を変更せずに、PAEQ-128 の鍵復元の計算量を 2^{50} から 2^{24}

までに減らし、鍵復元シミュレーションによって検証された．この成果は情報セキュリティと暗号学に関する国際会議の Inscrypt2018 において発表した．

(3) レーザーセンサーによって生成されたアラーム信号の情報漏洩

レーザーベースのフォールトインジェクション（LFI）攻撃は、暗号化実装に対する深刻な脅威である．LFI 攻撃に対する効果的な対策の 1 つは、レーザーショットを検出し、漏洩が発生する前に機密情報を削除することである．この研究では、レーザーセンサーによって保護された ASIC AES 実装に焦点を当てた．レーザーセンサーによって生成されたアラーム信号が、AES 計算の機密情報を漏洩するサイドチャネルリークの発生源であることを実験的に示した．具体的には、不安定なアラーム信号が鍵復元に最も有効的な情報源であることを示した．よって、オンチップセンサーの感度が暗号計算の機密情報を漏らす可能性があることを示唆した．この成果は情報セキュリティと暗号学に関する国際会議の Inscrypt2019 において発表した．

(4) AES への 5 ラウンドの物理攻撃の可能性の考察

AES への 5 ラウンドの物理攻撃の可能性を検討した．具体的は、複雑度が大幅に改善された 5 ラウンドの理論攻撃を用いた物理攻撃の可能性や攻撃者に必要な能力を検討し，ノイズが与える攻撃への影響を定量的に評価した．また，深層学習を用いた中間値のクラス分類を差分判定確率モデルに応用した場合，データ量を $2^{22.5}$ に増やすことでシミュレーション上 3 バイトの鍵復元が可能であることを示した．5 ラウンドの物理攻撃の可能性を示したことのより、AES が攻撃に利用される情報漏洩の脆弱性を明らかにした．この成果は国内のセキュリティシンポジウムのソサイエティ大会と SCIS2020 において発表した．

(5) 無線通信から収集した電磁波を用いたテンプレート攻撃の改良

ASM CCS 2018 において，離れた場所から攻撃対象の機器が送信している無線通信を利用したサイドチャネル攻撃が提案された．本研究では，遠距離サイドチャネル攻撃により効果的鍵復元方法を提案することを目標とした．無線通信信号から収集した波形を用いた鍵復元の精度を上げ，鍵復元に必要な波形数を減らすために，波形のサンプルポイントを限定することと POI の選択方法の調整を行った．プロファイリングに用いる波形のサンプルポイントを限定することによって鍵復元効率が向上すること分かった．また，鍵復元の使うサンプルポイントの前後を削除しないことにも鍵復元効率が向上することが分かった．２つの改良方法の組み合わせはより効率的な鍵復元ができることを示した．この成果は国内のセキュリティシンポジウムの SCIS2020 において発表した．

５．主な発表論文等

〔雑誌論文〕　計2件（うち査読付論文　1件／うち国際共著　1件／うちオープンアクセス　1件）

１．著者名 Wang Ruyan、Meng Xiaohan、Li Yang、Wang Jian	４．巻 Inscrypt 2018
２．論文標題 Improved Differential Fault Analysis on Authenticated Encryption of PAEQ-128	５．発行年 2019年
３．雑誌名 Proc. International Conference on Information Security and Cryptology	６．最初と最後の頁 183～199
掲載論文のDOI（デジタルオブジェクト識別子） https://doi.org/10.1007/978-3-030-14234-6_10	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 該当する

１．著者名 Li Yang、Hatano Ryota、Tada Sho、Matsuda Kohei、Miura Noriyuki、Sugawara Takeshi、Sakiyama Kazuo	４．巻 LNCS, volume 12020
２．論文標題 Side-Channel Leakage of Alarm Signal for a Bulk-Current-Based Laser Sensor	５．発行年 2020年
３．雑誌名 Proceeding of International Conferences on Information Security and Cryptology	６．最初と最後の頁 346～361
掲載論文のDOI（デジタルオブジェクト識別子） https://doi.org/10.1007/978-3-030-42921-8_20	査読の有無 無
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　0件）

１．発表者名 高見豪，菅原健，崎山一男，李陽
２．発表標題 AESに対する5ラウンド攻撃の物理攻撃への応用検討
３．学会等名 IEICE2019年ソサイエティ大会
４．発表年 2019年

１．発表者名 高見豪，菅原健，崎山一男，李陽
２．発表標題 AESへの5ラウンドの物理攻撃の可能性の考察
３．学会等名 2020年暗号と情報セキュリティシンポジウム
４．発表年 2020年

１．発表者名 杉本悠馬，菅原健，崎山一男，李陽
２．発表標題 無線通信から収集した電磁波を用いたテンプレート攻撃研究
３．学会等名 2020年暗号と情報セキュリティシンポジウム
４．発表年 2020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