様　式　Ｃ－１９、Ｆ－１９、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　２８　年　　６　月　２２　日現在

機関番号：　３１３０２
研究種目：　基盤研究(C)（一般）
研究期間：　2013～2015
課題番号：　２５３３０１５７

研究課題名（和文）DFA脆弱性総合評価システムの開発と検証

研究課題名（英文）Development of DFA vulnerability evaluation system

研究代表者
神永　正博（Kaminaga, Masahiro）

東北学院大学・工学部・教授

研究者番号：６０２６６８７２

交付決定額（研究期間全体）：（直接経費）　　3,800,000円

研究成果の概要（和文）：ICカード、ICタグなどに実装された暗号処理に対し、主にDFA(Differential Fault Analysis：差分故障攻撃)手法の研究ならびにその対策技術についての研究を行った。主として軽量ブロック暗号、RSA暗号、ラビン暗号に対し、命令スキップ現象を利用した攻撃技術を開発し、実装上の危険性を明らかにした。最も大きな仕事は、RSA電子署名の実装で多用される2t-ary法の事前計算処理部に命令スキップを行い、1528ビット標準RSAの最速パラメータt=6の場合に、これまでで最少の63回のフォールト注入で秘密指数を再構成するアルゴリズムDCAを開発したことである。

研究成果の概要（英文）：In our work, we developed several attack technologies against block ciphers, RSA and Rabin cryptosystem implemented on smartcard or RFID tag. Our attack techniques are based on instruction skip differential fault analysis. We reveal its vulnerabilities, and propose effective countermeasures in some cases. Highlight of our study is development of a new fault attack, double counting attack (DCA), on the precomputation of 2t-ary modular exponentiation for a classical RSA digital signature. DCA can reconstruct an entire secret exponent using the position checker with 63 faulted signatures in a short time for a 1536-bit RSA implementation using the 26-ary method.

研究分野：　暗号理論

キーワード：　差分故障解析

１．研究開始当初の背景

本研究の研究成果は主に次の二つにまとめられる。
(1) ブロック暗号に対する差分故障解析（Differential Fault Analysis. 以下 DFA と略）に関する結果
(2) RSA, Rabin 暗号に対する DFA に関する結果

1996 年に Bellcore の 3 名の研究者（当時）Boneh, Demillo, Lipton が IC カードなどの暗号処理デバイスに実装された公開鍵暗号（電子署名）に対する DFA の理論的可能性を示して以来、各種の DFA と対策技術が活発に研究されている。

ブロック暗号に対する DFA に関しては、1996 年に Biham-Shamir が DES に対する DFA を発表して以来、主としてレジスタにフォールトを発生させる DFA 技術が研究されてきた。Biham-Shamir の結果が既にそうであるが、レジスタの変化はランダムでよく、アタッカーが操作できなくても攻撃ができる点が優れている。一方、レジスタフォールトを前提とした DFA を実現するためには、IC チップのパッケージを開封して暗号処理で用いられているレジスタに YAG レーザなどを照射してフォールトを発生させる必要があるため、攻撃コストが高い点が問題であった。

一方、電源の瞬時降圧（瞬断）はローコストで実現できるフォールト印可手段である。ただし、パッケージを開封しているわけではないので、特定のレジスタ値を直接コントロールすることは困難である。

(1)は、この点を克服する技術として、命令スキップ（命令バイパス）DFA に注目して軽量ブロック暗号を中心として研究したものである。

命令スキップとは、アセンブラレベルで見た命令が実行されずにプログラムカウンタだけがインクリメントされ、次のプログラムアドレスの命令に進んでしまう現象である。その際、レジスタの値や、IC チップの他の処理には影響を与えず命令の読み飛ばしだけが生ずる現象をいう。この現象を利用した DFA を命令スキップ DFA と称する。本研究代表者は Atmel 社の IC チップに対してこの現象が生ずることを繰り返し確認している。この現象は、Choukri, Tunstall によって PIC チップでも確認されており、一定の普遍性を持つ攻撃手法であると考えられるが、これまではほとんど注目されていなかった。対象とするブロック暗号も限られていた。例えば、Choukri,Tunstall によって AES に対する命令スキップ DFA が発表されているが、軽量ブロック暗号に対して適用する研究はなかった。

そこで、本研究代表者は、吉川英機、志子田有光と共同で CLEFIA などの軽量ブロック暗号に対する命令スキップ DFA 手法を発表し、研究の基礎が築かれつつあった。

(2)の RSA 暗号に関しては、Boneh, Demillo, Lipton の研究以来、多くの DFA 手法とその対策手法が研究されてきた。RSA 電子署名に対する攻撃としては、CRT（Chinese Remainder Theorem）を用いた高速実装に対し、Lenstra が現実的な攻撃手法を発表し、その後も膨大な研究が積み重ねられてきた。CRT を用いた RSA 電子署名は、通常実装（CRT を用いない実装）の RSA 電子署名と比べて処理時間が 1/3~1/4 程度まで減少することが知られているが、この攻撃の存在により実装を避けられることもしばしばであった。一方、通常実装の RSA 電子署名に関しては多くのフォールテッドデータが必要となるため、相対的に安全性が高いと考えられていた。

(2)の Rabin 暗号に関しては、電子署名に利用する場合には、CRT を用いる必要があり、CRT-RSA 電子署名と同様の DFA ができると考えられていた。また Rabin 暗号は IC カードでほとんど利用されておらず、DFA の対象としてはほとんど注目されていなかった。

２．研究の目的

(1)に関しては、AES 等に適用されてきた命令スキップ DFA 技術を他のブロック暗号、特に種々の軽量ブロック暗号に拡張することである。

(2)に関しては、通常実装の RSA 電子署名に対し、現実的なフォールテッドデータ数で秘密鍵を再構成する命令スキップ DFA 技術を開発すること、ならびに Rabin 暗号化処理に対する DFA 技術を開発し、有効な対策技術を提案することである。

３．研究の方法

(1)に関しては主に２つの方法がある。一つは、ラウンド処理が終了しているかどうかをラウンドカウンタの値の正負を判定している条件分岐命令をスキップさせるものと、カウンタのインクリメントまたはデクリメントを行っている inc または dec 命令をスキップする方法である。それぞれにおいて最終的に実行されるラウンド処理の回数が変わる。減るか増えるかに応じ、前者は、ラウンド減少攻撃、後者はラウンド加算攻撃と呼ばれる。ここでは、後者の手法を採用し、ブロック暗号の構造を詳細に調べることによって、できるだけ少ないフォールテッドデータから秘密鍵を復元する具体的な手続きを与えることと、それが実際に可能であることを Atmel 社の IC チップを用いて実証することである。

(2)の通常実装 RSA 電子署名に関しては、こ

れまで注目されていなかった 2^t-ary 法の事前計算部の処理で命令スキップが起きた場合の処理結果を検討し、できるだけ少ないフォールテッドデータに対して秘密指数と取り出す技術を開発し、計算機シミュレーションによって結果を確認することである。
(2)の Rabin 暗号に関しては、電子署名に関しては、CRT-RSA 電子署名と同様であるので、IC カードではなく、IC タグ（RFID タグ）に注目し、Rabin 暗号化処理に注目し、特に公開鍵にフォールトを入れることで、IC タグ内の UID（ユニーク ID）を取り出す手法を検討し、結果を計算機シミュレーションで確認する。

４．研究成果

(1)に関して本研究代表者は、吉川英機、志子田有光、鈴木利則との共著論文[雑誌論文④IEICE Transactions D E96-D(9) 2031-2035 2013 年 9 月]において次の結果を得た：軽量ブロック暗号として知られる Piccolo(80bit), TWINE に対し、ラウンド加算攻撃が可能であることを示し、１つの正しい暗号文と２つの誤った暗号文から秘密鍵が復元できることを示した。これらは本研究代表者らが既に発表している 128bit-CLEFIA に対するラウンド加算攻撃 [IEICE Transactions E96.D(1) 146-150）]よりも容易であることが判明した。この他、Triple-DES へのラウンド加算 DFA 攻撃[学会発表④ Proc. The 2nd IEEE Global Conference on Consumer Electronics (GCCE2013) 538-539 2013], SPN 型の計量ブロック暗号へのラウンド加算 DFA 攻撃[雑誌論文② IEICE Trans. Vol.E97-A(12) 2671-2674 2014 年], LBlock へのラウンド加算攻撃[学会発表③Proc. of iSITA 2014 2014 年], オンザフライ（ラウンド鍵をあらかじめ用意しておくのではなく、ラウンド処理と同時に計算する実装のこと）の軽量ブロック暗号に対するラウンド加算攻撃[学会発表②Proc. ICACPS2015, Dubai, UAE, World Academy of Science, Engineering and Technology 17(9)(Part X) 1743-1746 2015]、[学会発表①情報理論とその応用シンポジウム（SITA2015）予稿集 pp.715-719, 2015 年]を得た。

これらの研究を通じて、ラウンド加算攻撃においては、攻撃の成否を分けるのは、ブロック暗号の暗号処理部の構造というより、鍵スケジュールの構造が重要であることがわかった。元の秘密鍵全体を復元するためには、鍵スケジュールを逆に辿る必要があるためである。この観点で見た場合、暗号処理部と比較して鍵スケジュールに関しては理論的検討が十分なされているとは言い難い状況である。この点を検討することは今後の課題である。

さらに、[雑誌論文③電子情報通信学会学生論文特集（和文論文誌 A）Vol. J97-A(No.2) 124-126 2014]において、暗号処理を直接対策するのではなく、一般的に多重化可能な命令列を利用したラウンド加算攻撃対策も開発した。

現在、Feistel 構造を持つ種々のブロック暗号に対するラウンド加算 DFA を理論的に検討した論文を準備中である。

（２）に関しては、[雑誌論文① IEEE Transactions on Information Forensics and Security 10(7) 1394-1401 2015 年]において、通常実装 RSA 電子署名において 2^t-ary 法を用いた場合の事前計算部において命令スキップを起こすことで、RSA 電子署名において、少ないフォールト数で秘密指数が復元できることを示した。例えば、1536bit の場合の 2^6-ary 法の場合、63 回のフォールトで秘密鍵が再構成できる。これはそれまで 100 回以上必要だったフォールト数を大幅に削減した初めての結果である。再構成の際に、position-checker という新技術を用いることで、効率よく秘密指数を計算することができる。公開指数 e が小さい場合（例えばよく利用されている e=65537 の場合）は秘密指数の再構成が高速になることも示した。
もう一つ（2）に関する成果は、現在投稿中なため詳細は割愛するが（preprint が arXiv:1603.00100 にある）、このプレプリントにおいて IC タグに実装された Rabin 暗号に対して公開鍵を命令スキップまたは１バイト破壊することで UID を再構成する攻撃が可能であることを示した。

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４件）

① Masahiro KAMINAGA, Hideki YOSHIKAWA, and Toshinori SUZUKI, Double Counting in 2^t-ary RSA Precomputation Reveals the Secret Exponent, IEEE Transactions on Information Forensics and Security 10(7) 1394-1401 2015 年 7 月、査読有
② Hideki YOSHIKAWA, Masahiro KAMINAGA, Arimitsu SHIKODA, and Toshinori SUZUKI, Round addition DFA on SPN block ciphers, IEICE Trans. Vol.E97-A(12) 2671-2674 2014 年 12 月、査読有
③ 高橋遼、神永正博、志子田有光、吉川英機「多重化可能な命令によるラウンド加算攻撃対策」電子情報通信学会学生論文特集（和文論文誌 A）Vol. J97-A(No.2) 124-126 2014 年 2 月、査読有
④ Hideki YOSHIKAWA, Masahiro KAMINAGA, Arimitsu SHIKODA, and Toshinori SUZUKI,

Round addition DFA on 80-bit Piccolo and TWINE, IEICE Transactions D E96-D(9) 2031-2035 2013 年 9 月、査読有

〔学会発表〕（計４件）

① 吉川英機、神永正博、志子田有光、鈴木利則"ラウンド加算 DFA による軽量暗号における鍵導出に関する検討," 第 36 回情報理論とその応用シンポジウム（SITA2015）予稿集 pp.715-719, 2015 年 11 月、査読有
② Hideki Yoshikawa, Masahiro Kaminaga, Arimitsu Shikoda, Toshinori Suzuki, Round Addition DFA on Lightweight Block Ciphers with On-The-Fly Key Schedule, 査読有, Proc. ICACPS2015, Dubai, UAE, World Academy of Science, Engineering and Technology 17(9)(Part X) 1743-1746 2015 年 9 月、査読有
③ Hideki YOSHIKAWA, Masahiro KAMINAGA, Arimitsu SHIKODA, and Toshinori SUZUKI, Secret Key Reconstruction Method using Round Addition DFA on Lightweight Block Cipher LBlock, Proc. of iSITA 2014 2014 年 10 月、査読有
④ Hideki YOSHIKAWA, Masahiro KAMINAGA, Arimitsu SHIKODA, and Toshinori SUZUKI, Round addition DFA for microcontroller implemented the triple DES, Proc. The 2nd IEEE Global Conference on Consumer Electronics (GCCE2013) 538-539 2013 年 10 月、査読有

〔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：
出願年月日：
国内外の別：

○取得状況（計０件）

名称：
発明者：
権利者：
種類：
番号：
取得年月日：
国内外の別：

〔その他〕
ホームページ等

６．研究組織
(1)研究代表者
神永　正博（KAMINAGA, Masahiro）
東北学院大学・工学部・電気情報工学科・教授
研究者番号：60266872

(2)研究分担者
志子田　有光（SHIKODA, Arimitsu）
東北学院大学・工学部・電子工学科・教授
研究者番号：00215972
吉川　英機（YOSHIKAWA, Hideki）
東北学院大学・工学部・電気情報工学科・准教授
研究者番号：60259885

(3)連携研究者
なし