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　 ６ 月 １２ 日現在

機関番号：１２６１２
研究種目：若手研究
研究期間：2020～2023
課題番号：２０Ｋ１９７９８

研究課題名（和文）Security Evaluation of IoT Devices against Medium and Long-Range Side-Channel Attacks

研究課題名（英文）Security Evaluation of IoT Devices against Medium and Long-Range 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）　　3,300,000円

研究成果の概要（和文）：本研究では，遠距離でIoTデバイスの秘密鍵を復元できるscreaming channels攻撃と呼ばれる電磁波攻撃の漏洩特性に着目した．実験環境を構築した後，プロファイリング技術を使用して分析した結果，漏洩特性について新たな知見を得た．さらに，プロファイリングを必要としない新しい攻撃手法を開発した．従来の攻撃方法と比較して，鍵復元に必要のデータ量を削減できることが実証された．また，新しい攻撃手法として，異なる漏洩チャンネルを組み合わせることで，組み合わせ攻撃を提案した．最後に，本研究では暗号実装のアセンブリコードを部分的に変更し，これが漏洩特性にどのような影響を与えるかを検証した．

研究成果の学術的意義や社会的意義
本研究は，物理的アクセスの制約を克服したscreaming channels攻撃の漏洩特性を研究した．遠距離からでもIoTデバイスのセキュリティを脅かすscreaming channels攻撃の実際の安全性脅威をより正確に評価し，防御策の開発を促進する．また，安全なデバイス設計のための基準を提供し，社会全体のデジタルセキュリティ意識の向上に寄与する．学術的には，新しい漏洩モデルと攻撃手法の提案が暗号解析分野に新たな視点をもたらす．

研究成果の概要（英文）：In this study, we established an environment to investigate the leakage characteristics of electromagnetic side-channel attacks known as screaming channels, which can recover secret key of IoT device from a long distance . Using profiling techniques for analysis, we gained new general insights into the leakage characteristics. Furthermore, we developed a new attack method that does not require profiling unlike previous works. Compared to traditional attack methods, this new approach has been proven to reduce the amount of measurements needed for key recovery. As part of the attack methodology, we proposed a combined attack by integrating different leakage channels. Finally, in this study, we partially modified the assembly code of the cryptographic implementation to investigate how these changes affect leakage characteristics for screaming channels.

研究分野：情報安全

キーワード：side-channel attack　screaming channel　AES

１．研究開始当初の背景

モバイル・インターネット技術の急速な進展と無線通信機能を搭載するデバイスの普及に伴い，日常生活で欠かせないものとなっているのが現状である．そのため，端末やデバイスがあちこちで無線通信を行うことで，様々な攻撃の潜在的なリスクを講じることが重要である．特に，攻撃者はモバイル機器に物理的に容易に接近できるため，物理攻撃に対するセキュリティの向上が不可欠である．物理攻撃の一つであるサイドチャネル攻撃は，Kocher らによる提案以来，暗号実装に対する脅威として盛んに研究されている．その中，電磁波サイドチャネル攻撃に関して，様々な攻撃手法の提案や様々な実装に対する攻撃が報告されている．

電磁波サイドチャネル攻撃において，漏洩電磁波は信号強度が弱く，測定距離が制限される．そのため，非接触で計測可能であっても，数 mm の距離での測定が必要である．近年，Camurati らは，攻撃者が特定のミックスドシグナルチップから離れた場所から秘密情報を取得できる，screaming channels（SC,スクリーミングチャネル）を提案した．Screaming channel 攻撃は，対策が組み込まれていないソフトウェア実装である tinyAES に対して，10m の距離から鍵復元を達成した．このアプローチは，ターゲットデバイスへの物理的なアクセスという攻撃者の持つ制約を緩和するものである．また，Camurati らの研究により，screaming channels の漏洩特性が電磁波サイドチャネルの漏洩特性とは異なることが実証された．また，プロファイリング相関攻撃は，より現実に近い環境下で，最大 15m の距離から鍵復元に成功した．さらに，ディープラーニングを使用した攻撃を導入し，鍵復元に必要なターゲットデバイスへのアクセス数を削減された．

２．研究の目的

本研究の主な目的は，screaming channel の漏洩特性を解析し，その攻撃手法について検証することである．具体的には，低電力デバイスを対象とした場合の漏洩電磁波の特徴を詳細に観察し，より厳密な漏洩モデルを定義することにより，効果的な攻撃手法を開発し，より厳密な安全性評価を目指している．

3． 研究方法

本研究の研究方法では，四つのステップに分けられる．

１)Camurati らが作成したトレース収集および解析環境を参考に実験環境を構築する．
２)プロファイリング技術から screaming channels の漏洩特性を推定する．分析した結果，新たに提案される MSB4 モデルを定義する．MSB4 モデルは，漏洩物理量の中間値の上位 4 ビットに依存する特性を着目する．
３)Screaming channel 攻撃には従来の電磁波サイドチャネルとは異なる漏洩特性があることを見出し，それに基づく新しい攻撃手法を開発した．そして，MSB4 モデルの有効性を実証し，MSB4 モデルを用いて tinyAES に対する 2 ラウンド目と 10 ラウンド目を攻撃し，鍵復元能力を検証する．本研究の攻撃は，専門のプロファイリング

を実施する必要がなく，事前に MSB4 モデルが有効であるという知識のみを使用した攻撃である．

4)最後に，MSB4 モデルがプロファイリング結果から観察できる条件を考察するため，暗号実装のアセンブリを一部変更して比較実験を行い,実装差による漏洩特性の変化を調査した．

4．研究成果

1) Screaming channels の漏洩特性の探索

Camurati らが以前に作成したトレース収集および解析環境を参照し，tinyAES の screaming channels の漏洩のプロファイリング結果を示し，プロファイリング技術から screaming channels の漏洩の特性を推定するものである．図 1 は S-box の入力値の変化とそれに伴う漏洩信号の変動が示されており，これらの値に対する漏洩信号のパターンが識別される．このデータから，特定の S-box の入力値に基づいて，暗号アルゴリズムの内部状態が外部に漏洩していることが確認される．

観察結果から，わかったことは S-box 入力の上位 4 ビットに基づき，漏洩がグループ分けされる.グループの大きさと順序は，実験セットアップによって異なる結果となった.1 ラウンド目と2ラウンド目を比較したとき，漏洩の特徴が非常に類似する結果となった．これは，漏洩信号が暗号アルゴリズムの実行中にどのように変化するかを示しており，特定の漏洩点での情報漏洩のパターンを明らかにしている．

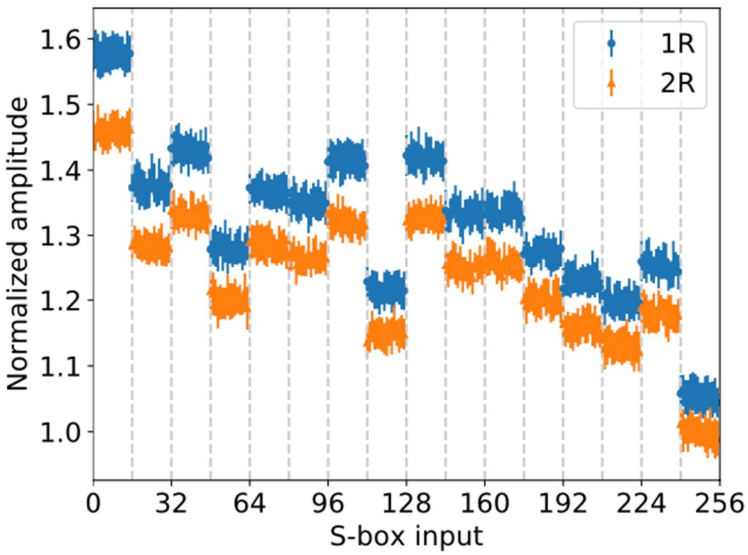

図 1　S-box 入力に対する漏洩プロファイル

2) 電磁波サイドチャネルとスクリーミングチャネルの同時収集攻撃の提案

構築した screaming channels の実験環境を使って，電磁波サイドチャネルとスクリーミングチャネルで収集した情報漏洩の漏洩モデルの違いに気づき，二つの情報漏洩を組み合わせる新しい鍵回復方法を提案した．同時収集でも鍵復元が困難になるような歪みは生じず，相関同時攻撃により擬似波形と実際に収集した波形，共にターゲットへのアクセス回数を削減できた．この新しい方法は攻撃対象へのアクセス回数を減少させることができる．この関連結果は SCIS 2022 で発表された．

3) 2 ラウンド目選択平文攻撃の提案

選択平文攻撃を用いた 2 ラウンド目の攻撃手法を提案し，攻撃の実行がよりシンプルで効率的になるように設計した．MSB4 モデルを使用した 2 ラウンド目の攻撃では，データが少なくても効率的な復号が可能であることが示された．デバイスへの直接的な攻撃では，S-box 入力値の上位 4 ビットのみが重要であることが示され，これにより，プロファイリングのプロセスが単純化される．この攻撃方法では，特定のバイトを変更することにより鍵候補の数を大幅に削減し，計算負荷を低減した．また，この手法は分散に基づく新しい鍵判別手法を用いることで，正しい鍵と誤った鍵候補をより確実に区別することが可能である．この攻撃の成功は，従来の手法と比較して著しく攻撃時間を短縮し，また鍵の復元精度を向上させることが証明された．

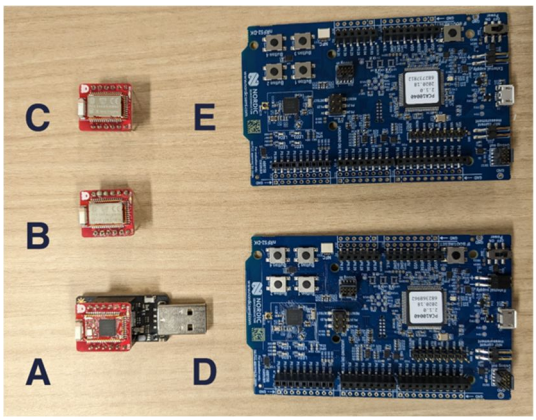

図 2　ターゲットデバイス

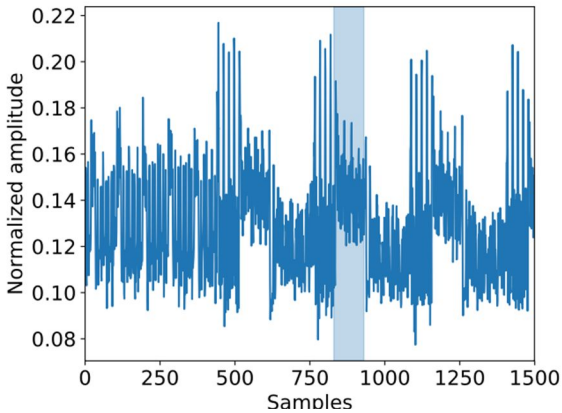

図 3　収集したトレース

2 ラウンド目選択平文攻撃を検証するため, 図 2 に示した 2 種類のターゲットデバイスから 10 cm の距離にソフトウェア無線機とアンテナを設置して, 図 3 に示したトレースを収集した．表 1 に示した攻撃実験の結果の通り，2 ラウンド目への攻撃は全てのデバイスで鍵復元に成功した.先行研究に比べると，50000 トレースでも鍵取得きなかったものを本研究の 2 ラウンド目への攻撃は, 中間値全ての漏洩の特徴を十分にプロファイリングすることなく鍵を復元した.さらに，アンテナやボードが変化しても鍵復元に成功した.これらの結果は, screaming channels を利用した tinyAES への攻撃において, プロファイリングによる十分な漏洩の解析を実施せずとも MSB4 モデルが使用できると仮定するだけで鍵復元可能であることを示した．この関連結果は SCIS2023 と国際会議 MobiSec2023 で発表された.

表 1 鍵回復の必要トレース数

攻撃手法	デバイス（名前）	攻撃トレース (プロファイリング)
先行研究 [17]	BLE Nano V2	1273 (5000)
CRA	BLE Nano V2 (A)	> 50000
2 ラウンド目への攻撃	BLE Nano V2 (A)	2896
2 ラウンド目への攻撃	BLE Nano V2 (B)	1680
2 ラウンド目への攻撃	BLE Nano V2 (C)	1520
2 ラウンド目への攻撃	PCA10040 (D)	3616
2 ラウンド目への攻撃	PCA10040 (E)	1776
10 ラウンド目への攻撃	BLE Nano V2 (A)	175
10 ラウンド目への攻撃	BLE Nano V2 (B)	34
10 ラウンド目への攻撃	BLE Nano V2 (C)	69
10 ラウンド目への攻撃	PCA10040 (D)	> 5000
10 ラウンド目への攻撃	PCA10040 (E)	900

4)　10 ラウンド目への攻撃手法の提案

本研究で生成されたプロファイルは, S-box 入力値の上位 4 ビットを分類するだけでなく，これらの上位 4 ビットのハミング重みも近似できる．この特徴は，第 10 ラウンドの攻撃を実行するために使用された．ランダムな暗号文を使用する相関解析であり，各鍵候補に対する相関が最も高いスコアを持つ鍵推測が正しい鍵であると判断する. 表１に示した通り，第 10 ラウンドの攻撃結果として，デバイス D を除くすべてのデバイスから鍵を成功に取得した. 攻撃に必要なトレースの数は，BLE Nano V2 と PCA10040 の間で大きく異なり，S-box 入力値の上位 4 ビットのみに依存し，そのハミング重みと相関しない適切な漏洩モデルが欠如していたためである．この成果は SCIS2023 と国際会議 MobiSec 2023 で発表された.

5)　実装差による漏洩特性の調査

異なるデバイスと実装方法による漏洩特性の違いを調査した. tinyAES と mbedTLS の実装において，焦点は，tinyAES と mbedTLS での非線形テーブルのメモリ配置の違いにある．tinyAES では S-box がフラッシュ領域に，mbedTLS では T-table がデータ RAM 領域に配置されている．テーブルの配置によって漏洩モデルが異なるという仮説の下，tinyAES での S-box をフラッシュ領域からデータ RAM 領域に移動し，漏洩モデルの変化の可能性を観察することを試みた. 標準的な tinyAES では 50000 トレースでも回復できなかったが，S-box の配置を変更した tinyAES バージョンでは同じトレース数で全ての鍵の回復が可能であった.

また，SubBytes プロセスのアセンブリにおける不必要な操作の影響も調査した．これには，中間値を保持するレジスタ値の過剰な複製や，中間値の不要なメモリ読み書きを削除され，「nop」命令に置き換えられた．もしこれらの不要なプロセスが MSB4 モデルが現れる条件を包含している場合, 変更された AES 漏洩のプロファイルにおいて MSB4 モデルの特徴は消えると予想される．MSB4 モデルと一致すると思われるいくつかのグルーピングを示している．これらの結果から，MSB4 モデルの出現条件はメモリの種類とアドレスによって影響を受けることが確認された．この成果は国際会議の MobiSec 2023 において発表された.

５．主な発表論文等

〔雑誌論文〕　計0件

〔学会発表〕　計3件（うち招待講演　0件／うち国際学会　1件）

１．発表者名 Yuki Matsukawa, Daiki Miyahara, Takeshi Sugawara, Kazuo Sakiyama and Yang Li
２．発表標題 Exploring Leakage Characteristics and Attacks through Profiles of Screaming Channels
３．学会等名 The 7th International Conference on Mobile Internet Security（国際学会）
４．発表年 2023年

１．発表者名 松川侑生，崎山一男，菅原健，李陽
２．発表標題 Screaming channelsの漏洩モデルの実験的検証
３．学会等名 2023年暗号と情報セキュリティシンポジウム（SCIS’23）
４．発表年 2023年

１．発表者名 松川侑生
２．発表標題 電磁波サイドチャネルとスクリーミングチャネルの同時収集攻撃の検証
３．学会等名 2022年暗号と情報セキュリティシンポジウム（SCIS’22）
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