様式Ｃ－１９

科学研究費助成事業（科学研究費補助金）研究成果報告書

平成 25 年 5 月 30 日現在

機関番号：１２６１２
研究種目：基盤研究（C）
研究期間：２０１０～２０１２年度
課題番号：２２５００００８

研究課題名（和文）サイドチャネル攻撃の限界追及と情報漏洩メカニズムの解明

研究課題名（英文）Research on Attack Limits of Side-Channel Analysis and Clarification of Information Leakage Mechanism

研究代表者
崎山　一男（SAKIYAMA KAZUO）
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：８０５０８８３８

研究成果の概要（和文）：サイドチャネル攻撃は暗号ハードウェアの電力消費や電磁波放出といった物理現象を利用し，ハードウェア内部の秘密情報を取得する攻撃である．本研究では，暗号実装におけるサイドチャネル攻撃限界を詳しく調査し，サイドチャネルからの情報漏洩のメカニズム解明を行った．これにより，漏洩情報量の理論値導出に成功し，暗号理論で取り扱われる秘密情報と乱数情報との関連性を一層明確にすることができた．

研究成果の概要（英文）：Side-channel attacks are methods, where attackers retrieve secret information by using physical phenomena leaked from cryptographic hardware such as power consumption and electromagnetic radiation. Exploring the attack limits of side-channel analysis, this research focused on the clarification of information leakage. We succeeded in deriving the theoretical bound for the amount of information leakage, and extended the understanding of the relationship between secret and random information handled in cryptology.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
２０１０年度	1,300,000	390,000	1,690,000
２０１１年度	1,300,000	390,000	1,690,000
２０１２年度	700,000	210,000	910,000
年度			
年度			
総　計	3,300,000	990,000	4,290,000

研究分野：総合領域
科研費の分科・細目：情報学・情報学基礎
キーワード：暗号・認証等，情報システム，セキュア・コンピューティング，証明可能安全性，サイドチャネル解析，情報理論的安全性，PUF (Physical Unclonable Function)

１．研究開始当初の背景

サイドチャネル攻撃は，暗号システムへの新たな脅威として活発に研究が進められている．現代の暗号理論では考慮されていなかった暗号システムからの物理情報の漏洩を巧みに利用したサイドチャネル攻撃が 1996 年に提案された．暗号処理中のタイミングの違いやデバイスの消費電力を用いた初期の攻撃に加え，電磁波，音などといった思いもよらぬサイドチャネルを情報経路とする攻撃が次々と提案されている．また，サイドチャネル情報を受動的に収集することにとどまらない．異常クロックや供給電圧を降下させるといった攻撃者の能動的サイドチャネルの利用により，暗号システムに故意にエラ

ーを誘発し，秘密情報を取得するフォールト攻撃が提案されている．さらに DRAM などの揮発性メモリを低温保存することにより，暗号処理の途中データを読み出すコールドブート攻撃が提案されるなど，今なお新たなサイドチャネルが発見され，より強力な攻撃手法が提案されている．

攻撃者が得ることができるサイドチャネル情報と暗号システムの入出力情報から，秘密情報を取り出す機械を，サイドチャネル識別機とよぶ．一般に攻撃者が得られる物理的予備知識（暗号システムの設計データなど）が多いほど，サイドチャネル識別機は高効率となり攻撃に成功する確率は高くなる．これは攻撃者が構築するシステムモデルと実際のシステムとの相関が高くなるためである．近年では，サイドチャネル識別機の性能向上に関する研究も活発であり，攻撃者能力は向上の一途をたどっている．

攻撃を防ぐ対抗策として，暗号処理を行うアルゴリズムレベルでの対策が 90 年後半より提案され始めた．乱数を用いてソフトウェア実装への攻撃を防ぐ対策が多く提案されている．しかし，攻撃研究が進むにつれて，一部のアルゴリズムレベルでの対策は，実際の暗号システムでは安全でないことが示され， 2000 年からハードウェアのロジックレベルでの対策が提案されるようになった．この対策法は，ハードウェアの構成単位であるロジックゲートを最小単位とするため，どのような暗号アルゴリズムに対しても適用可能であるが，全てのロジックに正しく対策を施すと，ハードウェアのコスト高を引き起こす．一方で，安全性を妥協し，低コスト化を狙ったハードウェアも提案されているが，これらはサイドチャネル攻撃に脆弱であることが指摘されている．

物理的特性の違いを利用して，ハードウェアデバイス毎に特有の情報を与えることができる PUF 回路が提案されている．この個体に特有な情報は，物理的複製が困難とされ，2005 年以降，その困難さを安全性の根拠とする権利保護方式や暗号プロトコルの提案が多くなされている．しかしながら， PUF 回路に対するサイドチャネル攻撃は，未だよく研究されていないため，今後 PUF 回路の安全性を，実デバイスを用いて評価する技術が求められるものと考える．

2009 年に入り，暗号実装からの情報漏洩を前提とした暗号プロトコルが提案されるようになった．これはサイドチャネルからの情報漏洩に，ある一定の制限が与え，改良した既存の暗号プロトコルに対して耐タンパー性を含めた安全性証明を与えたものである．その代表例として，コールドブート攻撃による情報報漏洩を前提とした，安全性証明がある．暗号プロトコルの安全性を保証するために，コールドブート攻撃における情報漏洩モデルを関数化し，どの程度までの情報漏洩が証明可能安全にとって許容できるかを検討するものである．しかしながら，コールドブート攻撃以外のサイドチャネル攻撃に対しては，漏洩のメカニズムに不明点が多く，適切な漏洩関数が存在していない．

２．研究の目的

攻撃と対策が次々と提案されていく中，あらゆるサイドチャネル攻撃に対して耐性のある暗号システムを構築するためには，秘密情報の漏洩を完全に防ぐような暗号実装の構成を目指すと同時に，攻撃者の能力向上に伴う秘密情報の漏洩を認識することが重要と考える．この認識の下では，秘密鍵のライフタイムの導出が不可欠となる．そこで，本研究では，最強の攻撃者が有する能力の理解と情報漏洩のメカニズムの解明（情報漏洩モデル化）を目的とした．

３．研究の方法

本研究の初期では，多面的な手段を用いて最強のサイドチャネル攻撃について研究する．まず FPGA（Field Programmable Gate Array）を用いて，種々のサイドチャネルからの情報の収集を行う．次に，得られたサイドチャネル情報を効率よく解析するために新たなサイドチャネル識別機の開発を行う．そして，暗号方式の観点からサイドチャネル攻撃のシナリオと攻撃者の能力との整合性を検討し，設定した攻撃者能力の妥当性について検討を行う．

次に，情報漏洩メカニズムの解明とパラメータ設定可能な情報漏洩モデルの構築を行い，パラメータ変更による情報理論的意味を考察する．最終的には，暗号アプリケーションに対して，安全性・コスト・パフォーマンスのトレードオフを評価する．本研究課題では，暗号理論，暗号実装，情報理論の三本柱で研究目標を達成する．

４．研究成果

2010 年度では，耐タンパー性を有する暗号ハードウェアに対して，サイドチャネル解析を行い，攻撃者の能力と秘密情報漏洩との相

関を明確にすることを目的とし研究を進めた．外乱等によりハードウェアに一過性の故障を誘発させ，暗号アルゴリズム処理中の中間値を操作できる非常に強力な攻撃者を想定し，異常動作時に出力される誤った暗号文から何ビット分の秘密情報の取得が可能かを実験により明確にした．これは，故障利用攻撃に基づく実験である．

より具体的には，AES，Trivium および MUGI といった暗号回路に対して，異常なクロック信号を混入し，情報漏洩のメカニズムと故障注入毎の漏洩情報量を算出した（文献③，④，⑩）．攻撃者の異常クロック混入能力には，実装形態に起因する制限が存在するものの，取得したサイドチャネル情報は，無制限の計算能力で解析できるものとした．これにより，FPGA に実装された暗号回路に対して攻撃を行った場合の情報漏洩を定量的に評価することができた．

2011 年度では，故障利用攻撃において，暗号アルゴリズム処理中の任意の中間値をビット単位で操作できる最強のサイドチャネル攻撃能力を有する攻撃者を想定した．これにより，実装形態に起因する攻撃者の能力の制限はなくなる．つまり，異常クロック混入時の制御能力，解析に必要な計算能力に関して，攻撃者能力を最大限高めた攻撃設定である．これにより，情報理論的観点を研究に取り入れることが可能となり，漏洩情報量の理論値導出に成功した．導出した理論値は，AES 暗号回路を用いた実証実験の結果とよく一致している（文献②）．本成果は，「サイドチャネル識別機の開発」，「情報漏洩モデルの構築」および「暗号プロトコルとの整合性の検証」が融合した結果生まれた成果である．

情報漏洩メカニズムの解明をさらに進めるため，サイドチャネル情報に測定環境に依存したノイズが混入するような攻撃を想定した．具体的には，暗号アルゴリズム処理中に攻撃者が行う中間値操作が確率的であると仮定し，最強の攻撃者がサイドチャネル解析において，どの程度のノイズまで許容できるかを定量的に評価するフレーム・ワークを構築した．現実には，全てのサイドチャネル情報が，攻撃者にとって有益であるとは限らず，攻撃者はノイズデータの除去等が可能なサイドチャネル識別機を構築する必要があるため，ノイズ耐性を有するサイドチャネル識別機の構築および識別機の利用方法を検討した．これにより，暗号理論からのアプローチで取り扱われる秘密乱数情報との関連性を一層明確にする環境を整備した．

2012 年度では，情報漏洩メカニズムの解明をさらに進めるべく，サイドチャネル情報に測定環境ノイズが混入する具体的な攻撃シナリオを設定し，どの程度のノイズを許容できるかについて，情報漏洩の定量評価が可能となる以下２種類の新たなサイドチャネル識別機を構築した．

１）クーポンコレクタ問題に基づく識別機：有名な数学の問題である「クーポンコレクタ問題」と従来の暗号解析で用いられていた「スクエア攻撃」を融合し，本課題に応用した．ある確率で定まる中間値差分をクーポンと捉え，鍵復元で必要となるクーポン収集の際に許容可能なノイズ（所望でないクーポン）をサイドチャネル識別機の入力として評価し，AES 暗号回路からの情報漏洩量を明らかにした（文献⑤）．

２）誤り暗号文の頻度分布に基づく識別機：攻撃者が行う確率的な中間値操作により得られた誤り暗号文の出現頻度分布は，多くの暗号回路構成で非一様となり，一過性の故障が誘発された場合，暗号回路は偏った誤り暗号文を出力する．この偏りに関する情報をサイドチャネル識別機の入力として，秘密鍵情報の漏洩メカニズムを解明した（文献⑥）．

これにより，情報漏洩メカニズムの解明が一層深まり，暗号理論からのアプローチで取り扱われる秘密乱数情報との関連性を一層明確にすることができた．

本研究課題での取り組みにより，現実の攻撃者能力と秘密鍵導出に必要な暗号処理回数の下限値の相関を正確に評価することができた．応用として，秘密鍵のライフタイムや RFID タグの使用回数の上限値の特定および回路レベルでの情報漏洩メカニズムの解明につなげることができるものである（文献①，⑦，⑧，⑨）．

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５件）

① 小池彩歌，李陽，中津大介，太田和夫，崎山一男，複数の要因に対する新たな故障感度解析(研究速報)，電子情報通信学会論文誌(A)，査読有，Vol.J95-A，No.10，2012，751-755，http://search.ieice.org/bin/summary.php?id=j95-a_10_751&category=A&year=2012&lang=J&abst=j

② Kazuo Sakiyama, Yang Li, Mitsugu Iwamoto, and Kazuo Ohta, Information-Theoretic Approach to Optimal Differential Fault Analysis, IEEE Trans. Inf. Forensic Secur., 査読有, Vol.7, No.1, 2012, 109-120, DOI: 10.1109/TIFS.2011.2174984

③ Junko Takahashi, Toshinori Fukunaga, and Kazuo Sakiyama, Differential Fault Analysis on Stream Cipher MUGI, IEICE Trans. Fundam. Electron. Commun. Comput. Sci., 査読有, E94-A, No.1, 2011, 242-251, DOI: 10.1587/transfun.E95.A.242

④ Yang Li, Kazuo Sakiyama, Shinichi Kawamura, and Kazuo Ohta, Power Analysis against a DPA-resistant S-box Implementation Based on the Fourier Transform, IEICE Trans. Fundam. Electron. Commun. Comput. Sci., 査読有, E94-A, No.1, 2011, 191-199, DOI:10.1587/transfun.E94.A.191

〔学会発表〕（計２０件）

⑤ 佐々木悠, 李陽, 阪本光, 崎山一男, クーポンコレクタ問題を利用したノイズに強い飽和フォールト攻撃, 電子情報通信学会総合大会, 2013 年 3 月 21 日, 岐阜大学（岐阜市）

⑥ 松原有沙, 李 陽, 太田和夫, 崎山一男, 故障混入時の AES 暗号ハードウェアの脆弱性について, 電子情報通信学会総合大会（学生ポスターセッション）, 2013 年 03 月 20 日, 岐阜大学（岐阜市）

⑦ 李陽, 太田和夫, 崎山一男, マスク対策 AES に対する誤り暗号文を用いた故障感度解析～CHES2011 での発表のレビュー～, 情報セキュリティ研究会（ISEC2011-49), 2011 年 12 月 14 日, 機会振興会館（東京都港区）

⑧ Yoshikazu Hanatani, Miyako Ohkubo, Shin'ichiro Matsuo, Kazuo Sakiyama, and Kazuo Ohta, A Study on Computational Formal Verification for Practical Cryptographic Protocol: The Case of Synchronous RFID Authentication, RLCPS'11, 2011 年 3 月 4 日, Bay Gardens Beach Resort (Saint Lucia)

⑨ 岩井祐樹, 太田和夫, 崎山一男, 故障感度解析を利用した PUF の実現について, 2011 年 暗号と情報セキュリティシンポジウム (SCIS2011), 2011 年 1 月 26 日, リーガロイヤルホテル小倉（北九州市）

⑩ Qi Li, Shigeto Gomisawa, Mitsugu Iwamoto, Kazuo Ohta, and Kazuo Sakiyama, New Differential Fault Analysis on Trivium Based on Setup-Time Violations, 情報通信基礎サブソサイエティ合同研究会, 2011 年 3 月 4 日, 大阪大学 （吹田市）

〔図書〕（計０件）

〔産業財産権〕

○出願状況（計０件）

○取得状況（計０件）

〔その他〕
ホームページ等
http://sakiyama-lab.jp

６．研究組織

(1)研究代表者
崎山　一男（SAKIYAMA KAZUO）
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：80508838

(2)研究分担者
太田　和夫（OHTA KAZUO）
電気通信大学・大学院情報理工学研究科・教授
研究者番号：80333491

(3)連携研究者
岩本　貢（IWAMOTO MITSUGU）
電気通信大学・先端領域教育研究センター ・特任准教授
研究者番号：50377016