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

平成　３０　年　　６　月　　４　日現在

機関番号：　１２６１２
研究種目：　挑戦的萌芽研究
研究期間：　2015～2017
課題番号：　１５Ｋ１２０３５

研究課題名（和文）サイドチャネル情報を用いた認証システムの構築と安全性評価

研究課題名（英文）Security Evaluation of Authentication Systems Using Side-Channel Information

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・教授

研究者番号：８０５０８８３８

交付決定額（研究期間全体）：（直接経費）　　2,700,000円

研究成果の概要（和文）：暗号システムから漏洩する電力や電磁波といった物理情報（サイドチャネル情報）を用いた既存研究は，サイドチャネル情報の一部を解析し，秘密鍵を取得する攻撃のケーススタディが主であった．これに対して本研究課題では，サイドチャネル情報に対する考え方を転換し，サイドチャネル情報の全てを有効に利用する研究フレームワークを設定した．アプリケーションとして，サイドチャネル情報を用いた認証システム，測距装置，および侵入検出装置といった新たな暗号システムを提案・構築し，安全性の向上を実証した．本研究課題に対する一連の取り組みにより，サイドチャネル解析研究の発展に寄与することができた．

研究成果の概要（英文）：Previous work on side-channel information, physical information such as power leakage and electromagnetic waves leaked from a cryptographic system, focused on a case study of attacks that analyzed a part of side channel information and acquired a secret key. On the other hand, in this research project, we changed the way of thinking about side-channel information and set up a research framework that effectively utilizes all of the side-channel information. As an application, we proposed and constructed a new cryptosystem such as an authentication system, a ranging device, and an intrusion detection device using side-channel information, and demonstrated the enhancement of security. A series of efforts and understandings on this research topic has contributed to the development of side-channel analysis research.

研究分野：　情報学

キーワード：　暗号・認証等　情報システム　サイドチャネル

１．研究開始当初の背景

暗号システムの消費電力や放射電磁波を用いて、暗号の秘密鍵を取得する攻撃は、サイドチャネル攻撃と呼ばれ、国内外で活発に研究されている。特に、欧州の大学での研究活動が盛んである。1996 年に、国際暗号学会(IACR)主催の国際会議で発表された論文を魁とし、最近では、ACM、IEEE、及び USENIX 協会主催の国際会議へと広がりを見せている。例えば、車のキーレスエントリー装置のサイドチャネル攻撃といった実システムの脆弱性が指摘されている。暗号システムに対する脅威の把握と対策技術の開発には、サイドチャネル攻撃の研究が、不可欠となっている。

サイドチャネル攻撃の際、暗号の秘密鍵は未知のパラメータとして扱われる。そのため、解析に使われるサイドチャネル情報は、極めて限定的であった。例えば、現在最も広く使われている 128 ビットの AES 暗号を攻撃対象とする場合、攻撃者は、サイドチャネル情報全体の 1/160 程度で１バイトの鍵を導出することができる。サイドチャネル情報の理解を深めるためには、攻撃に使われない情報を含め、全てのサイドチャネル情報を解析に利用する研究フレームワークが必要である。

２．研究の目的

サイドチャネル情報の理解を深化する研究フレームワークを構築するために、これまでの発想を転換し、サイドチャネル情報を認証に利用するサイドチャネル認証システムを仮設する。具体的には、暗号実装から漏洩するサイドチャネル情報をレスポンスとするチャレンジレスポンス認証システムを開発する。さらに、サイドチャネル認証システムの高性能化を狙い、それに伴って生まれる新たな研究課題に取り組み、サイドチャネル解析研究の学術的発展を目指す。

３．研究の方法

研究目的を達成するために、サイドチャネルの位置づけを整理し、研究計画をたてる。図１は、従来の解析研究と本研究課題のサイドチャネル研究の概要を示す。図中の①から⑤に対応する項目として､以下５つを設定し、研究に取り組む。

(1) 攻撃者への情報漏えい評価
(2) 既知鍵の設定における解析技術構築
(3) サイドチャネル解析技術の高精度化
(4) 既存の認証プロトコルとの性能比較
(5) 認証システム全体の計算量の評価

研究の初期段階では、項目 1)から 3)に注力する。まずは、AES 暗号実装から漏洩するサイドチャネル情報に対して、攻撃者への情報漏洩対策技術とサイドチャネル解析技術の定量的評価が可能となる実験環境を構築する。具体的には、AES 暗号を実装した FPGA（Field Programmable Gate Array）を被認証装置とし、攻撃者と認証者の双方の立場から、被認証装置から漏えいするサイドチャネル情報の解析を行う。攻撃者は、秘密鍵の復元に必要なサイドチャネル情報量 La を、認証者は、認証に必要となるサイドチャネル情報量 Ln を実験により導出にする。安全なサイドチャネル認証に必要となるサイドチャネル情報量 L は、Ln ＜ L ＜ La となるように選べばよい。ここでは、処理した AES 暗号のラウンド数を基準として、サイドチャネル情報量を算出する。

サイドチャネル解析技術の高精度化については、既知鍵であることを最大限に活かし、新たな解析を提案する。例えば、鍵長が 128 ビットの AES 暗号では、16 個のバイト演算からなるラウンド演算を 10 回繰り返す。つまり、AES 暗号全体では、合計で 160 回のバイト演算を行う。この演算に相当する全てのサイドチャネル情報を有効に解析するために、これまでの解析技術を基に、複数バイト演算に適したサイドチャネル情報モデルを構築する。攻撃とは異なり、モデルが汎用である必要はないため、被認証装置における暗号の設計情報や測定環境といったこともモデルに取り込むようにする。

一連の研究が進めば、秘密鍵が異なればサイドチャネル情報は異なること（被認証装置の固有性）が確認できる。また、秘密鍵の埋め込まれた被認証装置からは、サイドチャネル情報を容易に取得することができるが、鍵を持たない攻撃者には困難であること（サイドチャネル情報の一方向性）の確認もできる。固有性と一方向性を確認する実験結果の考察から、解析手法やサイドチャネル情報モデルの改善を目指す。最終的には、構築したモデルの最適性に対して理論的な説明を付ける。

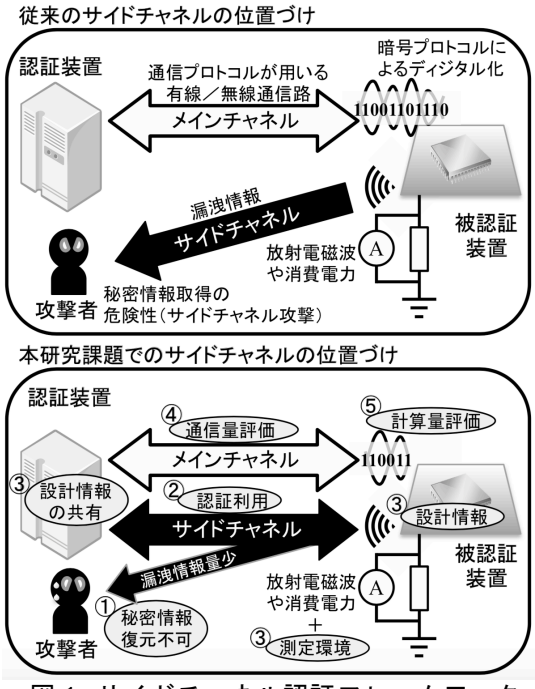

図１ サイドチャネル認証フレームワーク

次の段階では、4)5)の項目を研究に追加する。従来の認証プロトコルと比べて、サイドチャネル情報を追加で利用することによる機能性と安全性の向上を定量的に評価する。評価指標は大きく２つある。メインチャネルとサイドチャネルのそれぞれにおける通信量と、それぞれのチャネルから得られた情報の解析に必要となる計算量である。

一般的に、認証システムにおいて、認証側の ID 検索には多くの計算を要する。サイドチャネル認証では、解析処理するデータ量が膨大になるため、ID 検索時間はさらに長くなる。したがって、認証システム全体の通信量や計算量を削減する最適化に取り組む。また、こういった最適化による認証性能への影響を調べ、ユースケースにおけるバランスを考える。最終的には、サイドチャネル認証フレームワークで、通信量、計算量、認証性能、攻撃の危険などのトレードオフをシミュレーションできるようにする。そして、サイドチャネル情報の体系的理解に繋げる。
また、サイドチャネル認証の拡張について検討を進める。サイドチャネル認証の基礎となる技術を計測システム等に応用・展開し、機能性と安全性の向上を目指す。

４．研究成果

本研究課題で設定した５つの研究項目に対して、研究成果の概要を以下にまとめる。

1) 攻撃者への情報漏洩の対策技術構築

AES 暗号を実装した FPGA を被認証装置として準備し、装置から漏洩する電磁波をサイドチャネル情報とする実験環境を構築した。そして、秘密鍵を知る認証者と秘密鍵を知らない攻撃者の双方の立場で、サイドチャネル解析を行った。その結果、安全にサイドチャネル認証が行える情報量 L に関する条件を導出することができた。また、攻撃が困難になる AES 暗号の入出力データの処理法を提案した。これは、次の 2)の研究項目における識別可能な被認証装置数の増加に関する成果にもつながった。

2) 既知鍵の設定における解析技術構築

AES 暗号から漏洩する全サイドチャネル情報を利用する解析技術を開発した。また、被認証装置の固有性を調べるために、複数の被認証装置に異なる秘密鍵を設定し、識別可能な被認証装置数を実験により明らかにした。また、サイドチャネル情報量を増やすために、AES のラウンド関数を数千回程度まで繰り返し実行できるようにした。その結果、識別可能な装置数を大幅に増やすことができた。

3) サイドチャネル解析技術の高精度化

サイドチャネル情報のモデルとして、HW（Hamming Weight）モデルと HD（Hamming Distance）モデルを用いて解析を行い、HD モデルを用いた解析の優位性を確認した。また、サイドチャネル情報の実測値から構築したモデル（XOR プロファイリングモデル）による解析を行い、HD モデルを用いた解析よりも精度が高いことが分かった。さらに、実装形態の異なるデバイスを被認証装置として用いる実験を行い、被認証装置の設計情報がサイドチャネル認証に大きな影響を与えることが分かった。この結果からも、サイドチャネル解析に使用するモデルとして、プロファイリングモデルが最適であることが明らかとなった。

4)5) 既存の認証プロトコルとの性能比較、及び認証システム全体の計算量の評価

メインチャネル情報を有効に利用したサイドチャネル認証システムを構築し、認証装置の計算量の削減を実現した。具体的には、ユースケースで求められる安全性と照らし合わせ、誤認証率が十分低くなるような認証試行回数をシステム要件として、必要となるサイドチャネル情報の通信量と認証装置における計算量を評価した。その結果、認証成功率やメインチャネル/サイドチャネルの通信量と計算量を指標とするサイドチャネル認証システムを提案することかができた。

また、サイドチャネル情報のキャリアとして、電磁波に加えて光にも挑戦した。被認証装置に接続した LED の発光を用いた場合、従来の漏えい電磁波を用いた認証と比べて、認証の通信距離を伸ばせるといったメリットが確認できた。レーザー光を用いることで、さらに通信距離を伸ばすこともが可能であることも分かった。

さらに、サイドチャネル認証の応用研究として、認証機能付きの測距システムを構築した。サイドチャネル情報を重畳したレーザー光を物体に照射し、その反射光を解析することで、受信光の真正性の確認と物体の位置情報の取得を同時に行うことができる測距装置を開発した。真正性を確認することで、距離を偽装する攻撃を検知することができる。自動車などに用いられる LiDAR（Light Detection And Ranging）の安全性・信頼性向上につながる技術と考える。

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３件）

① Momoka Kasuya and Kazuo Sakiyama, “Improved EM Side-Channel Authentication Using Profile-Based XOR Model,” Proc. International Workshop on Information Security Applications (WISA’17), Aug., 2017, to be published（査読有）.

② Momoka Kasuya, Takanori Machida, and Kazuo Sakiyama, “New Metric for Side-Channel Information Leakage: Case

Study on EM Radiation from AES Hardware," In Proc. URSI Asia-Pacific Radio Science Conference (URSI AP-RASC'16), Aug., 2016, (査読有).
DOI: 10.1109/URSIAP-RASC.2016.7601332

③ Kazuo Sakiyama, Momoka Kasuya, Takanori Machida, Arisa Matsubara, Yunfeng Kuai, Yu-Ichi Hayashi, Takaaki Mizuki, Noriyuki Miura, and Makoto Nagata, "Physical Authentication Using Side-Channel Information," Proc. International Conference on Information and Communication Technology (ICoICT'16), May, 2016, (査読有, Best Presenter 賞).
DOI: 10.1109/ICoICT.2016.7571953

〔学会発表〕(計１１件（うち招待１件))

① Momoka Kasuya and Kazuo Sakiyama, "Side-Channel Authentication Using XOR Model," SCIS & CSS Award Session, International Workshop on Security 2017 (IWSEC'17), Aug., 2017 (招待講演).
② 松村竜我, 菅原健, 崎山一男, "光に重畳したサイドチャネル情報に関する基礎的な解析," 2018 年暗号と情報セキュリティシンポジウム (SCIS2018), 3D2-3, 6 pages, Jan., 2018.
③ 松村竜我, 庄司奈津, 菅原健, 崎山一男, "光を用いたサイドチャネル認証," コンピュータセキュリティシンポジウム 2017(CSS2017)デモンストレーション (ポスター) セッション, Oct., 2017.
④ 松村竜我, 庄司奈津, 菅原健, 崎山一男, "ダイオードレーザーを用いた光によるサイドチャネル認証," ハードウェアセキュリティ研究会(HWS), Jun., 2017.
⑤ 粕谷桃伽, 町田卓謙, 崎山一男, "XOR モデルを用いたサイドチャネル認証," 2017 年暗号と情報セキュリティシンポジウム (SCIS2017), 3C2-3, 6 pages, Jan., 2017, (SCIS 論文賞).
⑥ Momoka Kasuya and Kazuo Sakiyama, "Authentication Using Physical Information," Poster Session, Asian Hardware Oriented Security and Trust Symposium (AsianHOST'16), Dec., 2016.
⑦ 粕谷桃伽, 崎山一男, "認証の枠組みを用いたサイドチャネル攻撃に必要な波形数の導出," IEICE2016 年ソサイエティ大会, Sep., 2016.
⑧ 粕谷桃伽, 町田卓謙, 崎山一男, "サイドチャネル情報における固有性解析," IEICE2016 年総合大会, 学生ポスターセッション, Mar., 2016.
⑨ 粕谷桃伽, 町田卓謙, 崎山一男, "AES 暗号を用いたサイドチャネル認証における識別可能なデバイス数," 2016 年暗号と情報セキュリティシンポジウム (SCIS2016), 1F2-3, 4 pages, Jan., 2016.
⑩ 藤井達哉, 粕谷桃伽, 町田卓謙, 崎山一男, "DE0-nano を用いたサイドチャネル認証," コンピュータセキュリティシンポジウム 2015(CSS2015)デモンストレーション(ポスター)セッション, Oct., 2015, (最優秀デモンストレーション賞).
⑪ 粕谷桃伽, 町田卓謙, 崎山一男, "漏洩電磁波を用いたサイドチャネル認証の基礎実験," IEICE2015 年ソサイエティ大会, Sep., 2015.

〔図書〕
なし

〔産業財産権〕

○出願状況（計１件）

名称：測距装置及び侵入検出装置
発明者：崎山 一男, 粕谷 桃伽
権利者：同上
種類：特許
番号：特許願 2017-95232 号
出願年月日：平成２９年５月１２日
国内外の別：国内

○取得状況（計０件）

〔その他〕
なし

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・教授
研究者番号：８０５０８８３８

(2)研究分担者
なし

(3)連携研究者
なし

(4)研究協力者
なし