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 １１ 日現在

機関番号：３３９１９
研究種目：基盤研究(C)（特設分野研究）
研究期間：2016～2019
課題番号：１６ＫＴ０１８８

研究課題名（和文）IoTハードウェアを指向した安全性を強化するハイブリッド認証システムに関する研究

研究課題名（英文）IoT Hardware oriented Secure Hybrid Authentication System

研究代表者
吉川　雅弥（Yoshikawa, Masaya）

名城大学・理工学部・教授

研究者番号：５０３７３０９８

交付決定額（研究期間全体）：（直接経費）　　3,700,000円

研究成果の概要（和文）：Internet of Things（IoT）では，ネットワークで安全性を確保するためには，適切な認証を行うことが重要である。しかし，実装面積の観点から従来のパソコンを中心とするIT技術での認証システムを適用することは出来ない。さらに，従来の認証で使用される標準暗号は，計算量的安全性は保障されているが，サイドチャネル攻撃に対しては脆弱であることが明らかになってきた。そこで，申請研究では，IoTハードウェアを指向した認証システムを新たに開発した。この認証システムでは，複数の手法を組み合わせて，様々なサイドチャネル攻撃耐性を向上させることで，安全性を強化した。

研究成果の学術的意義や社会的意義
研究成果の学術的意義は，Internet of Things時代におけるネットワークでの安全性を確保できることである。様々なデバイスが接続されているネットワークでは，各デバイスの認証が安全性を確保する上で最も重要な方法であるが，従来のパソコンを中心とするIT技術での認証システムは，実装制約があるIoTデバイスに適用することが難しい。そのため，本研究でのIoTハードウェアを指向した認証システムは，安全なネットワークを実現する上で社会的意義が大きい。

研究成果の概要（英文）：n IoT era, authentication of each device is the most important to ensure security. However, IT based authentication can’t be applied to IoT devices from a view point of implementation constraints. Moreover, standard cipher which is used in the internet is pointed out its vulnerability against side channel attacks. This study developed IoT Hardware oriented Secure Hybrid Authentication System. The proposed method achieved the secure authentication against illegal attacks by adopting some tamper resistance techniques.

研究分野：計算機工学

キーワード：認証　セキュリティ

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

Internet of Things (IoT) では，あらゆるハードウェアがインターネットに接続して，分散的・階層的なネットワークを構築する。このようなネットワークで安全性を確保するためには，適切な認証を行うことが重要である。しかし，IoT の基盤技術の１つであるウェアラブルなハードウェアに対しては，実装面積の観点から従来のパソコンを中心とする IT 技術での認証システムを適用することは出来ない。さらに，従来の認証で使用される標準暗号は，計算量的に解読が不可能であることが十分検証されているが，暗号回路の動作時の消費電力や漏洩電磁波などのサイドチャネル情報を利用して，秘密鍵を解析するサイドチャネル攻撃に対しては脆弱であることが明らかになってきた。特に，暗号回路中の秘密鍵に関連する情報と消費電力に相関があることを利用する電力解析攻撃は，サイドチャネル攻撃の中で最も脅威である攻撃の１つである。

また，関連する研究動向について，サイドチャネル攻撃に対して暗号回路中の秘密情報が消費電力情報にリークしてしまうことを防ぐような対策がいくつか発表されて，米国の Cryptography Research 社やオランダの Riscure 社を中心に，実用化されている。また，ハードウェアの複製防止技術には，微小な製造ばらつきを利用した電子指紋の働きをする PUF と呼ばれる技術が発表され，米国の Verayo 社やオランダの Intrinsic-ID 社で開発されている。

２．研究の目的

申請研究では，IoT ハードウェアを指向した認証システムを新たに開発する。この認証システムでは，物理的・数学的手法を組み合わせて，様々なサイドチャネル攻撃耐性を向上させることで，安全性を強化する。本研究の成果により，ネットワークの信頼性だけでなく，Root of trust であるハードウェアの安全性も強化する。このように申請研究で開発する IoT でのハードウェアの安全性に関する基盤技術の確保は，情報漏洩だけでなく，ハッカーなど不正な攻撃にも対応することができ，社会の安定に貢献できる。

３．研究の方法

IoT ハードウェアを指向した認証システムを実現するために，申請研究では，セキュアコードシステムと認証 ID システムで構成するハードウェア認証システムを開発する。

まず，セキュアコードシステムでは，物理的なアプローチとしては，多重構造を用いた PUF を開発する。また,数学的なアプローチとしては，生物の進化過程を工学的にモデル化した遺伝的アルゴリズムや遺伝的プログラミングを用いた進化的手法をベースとするプロファイリングシステムを開発する。

次に，認証 ID システムでは，サイドチャネル耐性を備えた耐タンパ併用アーキテクチャと秘密分散拡散処理手法を開発する。耐タンパアーキテクチャでは，セキュアコードシステムで生成したコートを，これまで研究を進めてきた耐タンパ暗号回路の鍵として用いる。このように，PUF の出力を秘密鍵として用いることで，電源が入っているときのみ鍵が存在して，鍵が入っていない時には鍵が存在しないようになる。このことにより，リバースエンジニアリングを用いた秘密鍵の解析や複製を防ぐことが可能になる。また,暗号処理では,軽量暗号を用いることで，安全性と実装制約のトレードオフを解決する。秘密分散拡散処理では，秘密分散法により，暗号化の結果と鍵との相関を隠ぺいすることで，数学的に安全なコードを生成し，これを各ハードウェアの認証 ID とする。

４．研究成果

全体として，当初の目標をおおむね達成することができた。まず，セキュアコードシステムを構成する多重構造を用いた PUF に関しては，リングオシレータ PUF だけでなく，複数の PUF について，FPGA に実装して，その性能を評価した。その評価において，従来の評価項目だけでなく，環境変動の違いによる PUF の機械学習攻撃に対する耐性評価も行った。具体的には，アービタ PUF を対象に，環境変動の違いによる PUF の機械学習攻撃耐性を評価するために，PUF のレスポンスを一定確率で変化させる。このレスポンスの反転に関して，アービターPUF のレスポンスは DFF に入力される信号の伝搬時間の差が小さいほど，反転しやすい。これは環境変動により，信号の伝搬時間の差が小さいほど，DFF でセットアップタイム制約違反が引き起こされやすいためである。そこで，レスポンスを反転させるために，図１に示す関数を使用した。このレスポンス反転関数は，信号の伝搬時間の差Δを入力とし，レスポンスの反転確率を返す。すなわち，信号の伝搬時間の差Δが小さいほど，レスポンスの反転確率は高くなり，最大で 50%の確率でレスポンスが反転する。実験結果ず図２に示す。実験結果より，レスポンスの正答率がわずかに低下していることが分かる。すなわち，環境変動によりわずかに機械学習攻撃の攻撃能力が低下していることが分かる。

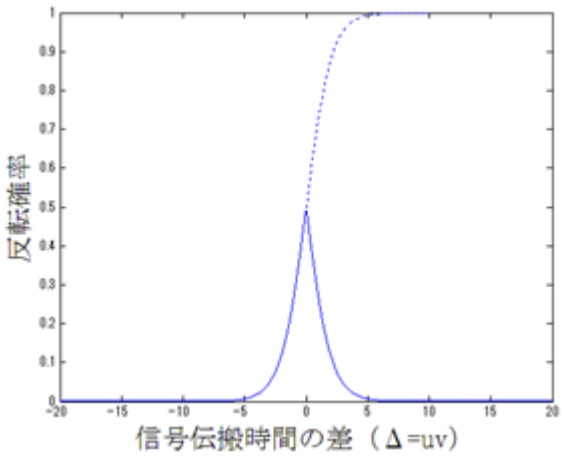

図 1 レスポンス反転関数

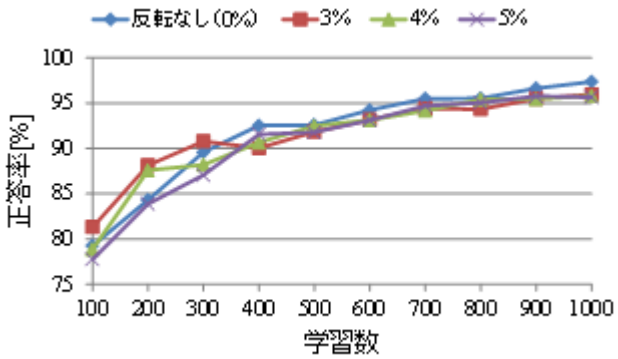

図 2 環境変動による耐性評価

また，セキュアコードシステムにおける進化的を用いた補正処理についても，これらを検討するために，遺伝的アルゴリズムと遺伝的プログラミングをベースとした解析手法を開発し，評価を行った。

次に，認証 ID システムを構成する耐タンパ併用アーキテクチャに関して，いくつかの認証暗号・軽量暗号について，FPGA に実装して様々な耐タンパの評価を行った。図 3 に，その中の 1 つである認証暗号 SIMON-JAMBU を対象に小面積を指向した対策に対する電力解析の耐タンパ評価を示す。図 3 に示すように，無対策では，5,000 波形で部分鍵が全て推定されていることが分かる。一方で，提案対策手法では，50,000 波形を用いても解析に成功した部分鍵は 30bit である。ここで，全部分鍵は 48bit であるため，この結果は 1bit ずつランダムに予測した結果である 24bit（48 / 2 = 24）に近い値である。したがって，提案対策手法により電力解析に対する耐性が向上していることが確認できる。最後に，認証 ID システムを構成する秘密分散拡散処理についても，機械学習攻撃に耐性のある ID 生成手法を検討した。

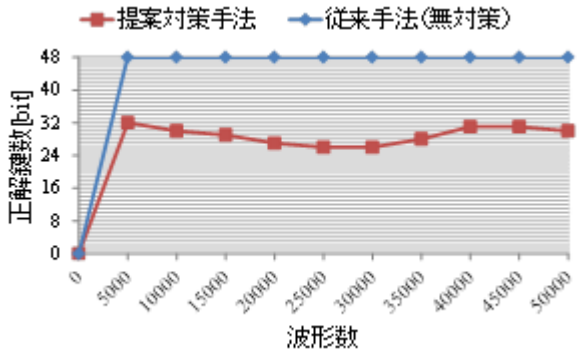

図 3 耐タンパ評価結果

以上，これらの研究の成果ついては，関連する国内研究会や国際会議で発表するだけでなく，専門の学術論文誌に投稿して採択されて公開した。

５．主な発表論文等

〔雑誌論文〕　計4件（うち査読付論文　3件／うち国際共著　0件／うちオープンアクセス　0件）

１．著者名 野崎佑典，池崎良哉，吉川雅弥	４．巻 vol.138, no.12
２．論文標題 低消費電力軽量暗号Midoriに対する階層的電力解析とその評価	５．発行年 2018年
３．雑誌名 電気学会論文誌C	６．最初と最後の頁 1455-1463
掲載論文のDOI（デジタルオブジェクト識別子） 10.1541/ieejeiss.138.1455	査読の有無 有
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 －

１．著者名 Y.Nozaki, Y.Ikezaki, and M.Yoshikawa	４．巻 vol.101, no.5
２．論文標題 Two Stages Statistical Fault Analysis Method for Midori and its Evaluation	５．発行年 2018年
３．雑誌名 Electronics and Communications in Japan	６．最初と最後の頁 3-11
掲載論文のDOI（デジタルオブジェクト識別子） 10.1002/ecj.12057	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 －

１．著者名 野崎 佑典、池崎 良哉、吉川 雅弥	４．巻 137
２．論文標題 Midoriに対する2段階の統計的故障利用解析手法とその評価	５．発行年 2017年
３．雑誌名 電気学会論文誌.　C	６．最初と最後の頁 1554～1561
掲載論文のDOI（デジタルオブジェクト識別子） 10.1541/ieejeiss.137.1554	査読の有無 有
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 －

１．著者名 野崎佑典，吉川雅弥	４．巻 vol.7, no.2
２．論文標題 改ざん検知暗号Minalpherに対する階層的電力解析手法とその評価	５．発行年 2017年
３．雑誌名 情報処理学会論文誌コンシューマ・デバイス&システム	６．最初と最後の頁 125-134
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 有
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10件（うち招待講演　0件／うち国際学会　5件）

1．発表者名
M.Yoshikawa and Y.Nozaki

2．発表標題
"Lightweight Cipher Aware Countermeasure Using Random Number Masks and Its Evaluation

3．学会等名
International Conference on Vision, Image and Signal Processing（国際学会）

4．発表年
2018年

1．発表者名
M.Yoshikawa, Y.Ikezaki, and Y.Nozaki

2．発表標題
Implementation of Searchable Encryption System with Dedicated Hardware and its Evaluation

3．学会等名
IEEE Annual Ubiquitous Computing, Electronics and Mobile Communication Conference（国際学会）

4．発表年
2018年

1．発表者名
M. Yoshikawa and Y. Nozaki

2．発表標題
Electromagnetic Analysis Method for Ultra Low Power Cipher Midori

3．学会等名
8th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference（国際学会）

4．発表年
2017年

1．発表者名
Y. Ikezaki, Y. Nozaki, H. Nagata, and M. Yoshikawa

2．発表標題
FPGA Implementation Technique for Power Consumption Aware Tamper Resistance Accelerator of Lightweight PUF

3．学会等名
IEEE 6th Global Conference on Consumer Electronics（国際学会）

4．発表年
2017年

１．発表者名
野崎佑典，吉川雅弥

２．発表標題
小面積実装を指向した耐タンパ認証暗号とその評価

３．学会等名
第43回東海ファジィ研究会

４．発表年
2017年

１．発表者名
野崎佑典，吉川雅弥

２．発表標題
環境変動の違いによるPUFの機械学習攻撃耐性評価

３．学会等名
東海ファジィ研究会

４．発表年
2016年

１．発表者名
野崎佑典，吉川雅弥

２．発表標題
改ざん検知暗号Minalpherに対する電力解析

３．学会等名
情報処理学会 CDS研究会

４．発表年
2016年

１．発表者名
Y.Ikezaki, Y.Nozaki, M.Yoshikawa

２．発表標題
Deep Learning Attack for Physical Unclonable Function

３．学会等名
IEEE 5th Global Conference on Consumer Electronics（国際学会）

４．発表年
2016年

１．発表者名 池崎良哉，吉川雅弥
２．発表標題 PUFに対する消費電力を利用した深層学習攻撃の基本検討
３．学会等名 東海ファジィ研究会
４．発表年 2017年

１．発表者名 野崎佑典，吉川雅弥
２．発表標題 実装方式の違いによるアービターPUFの機械学習攻撃耐性評価
３．学会等名 電子情報通信学会総合大会
４．発表年 2017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