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　５ 年　 ６ 月 １２ 日現在

機関番号：３３９１９
研究種目：基盤研究(C)（一般）
研究期間：2019～2022
課題番号：１９Ｋ１１９７６

研究課題名（和文）Society5.0でのプライバシー指向セキュアインテリジェントエッジモジュール

研究課題名（英文）Privacy oriented secure intelligent module in Society 5.0

研究代表者
吉川　雅弥（Yoshikawa, Masaya）

名城大学・情報工学部・教授

研究者番号：５０３７３０９８

交付決定額（研究期間全体）：（直接経費）　　3,300,000円

研究成果の概要（和文）：申請研究では，Society 5.0を支えるエッジを実現するプライバシーを考慮したセキュアなデバイスを開発する。このセキュアなデバイスでは，プライバシーを保護するだけでなく，情報を秘匿するための暗号化やセキュアな認証システムを実現する。本研究の成果により，エッジからクラウドへのデータを転送する，また，クラウドでのデータの解析・加工後に，クラウドからエッジへのその加工したデータを転送するというSociety 5.0でのスキーム全体をセキュアに実行することが可能になる。このように申請研究で開発するプライバシーを考慮したセキュアなデバイスは，Society 5.0を支える基盤技術の1つを確立する。

研究成果の学術的意義や社会的意義
Society5.0では，あらゆるものがネットワーク接続されるため，サイバー・フィジカル・セキュリティ（CPS）の問題を解決することが必須課題である。この問題では，従来の不正アクセスに代表される攻撃だけでなく，個人情報保護の観点からプライバシーを考慮する必要がある。プライバシー問題について，国内では個人情報保護法が，厳罰化だけでなく，適用対象が拡大した。改正前は5001人以上の事業者のみが対象であったが，改正後は小規模事業者でなく，非営利団体や大学の研究室も含む全ての事業者が対象となった。申請研究では，このCPSの問題を解決して，社会の安定と安心・安全に貢献できる。

研究成果の概要（英文）：Due to huge number of devices are connected to the internet in Society 5.0 which are promoted by Japanese government, cyber-physical security is an essential issue. This study proposed a privacy oriented secure intelligent module in Society 5.0 to solve the cyber-physical security issue. The proposed module achieved not only privacy protection, but also tamper resistant encryption which includes a countermeasure against side-channel attacks and a secure authentication system. The proposed method consists of two components: (1) edge aware secure intelligent module which reduces power consumption and circuit-size overhead, and (2) privacy oriented authentication system.
The proposed method enables secure operation of the entire scheme in Society 5.0 which is based on data flow between an edge device and a cloud server. Thus, this study established one of the fundamental technologies in Society 5.0.

研究分野：セキュリティ

キーワード：セキュリティ　サイバーフィジカル

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

内閣府の総合科学技術・イノベーション会議での第 5 期科学技術基本計画において，情報社会（Society 4.0）に続く，Society 5.0 が提唱された。Society 5.0 とは，サイバー空間（仮想空間）とフィジカル空間（現実空間）を融合させることで，国内外の経済発展と社会的課題の解決を両立し，人間中心の社会（Society）を実現するとされている。この Society5.0 では，あらゆるものがつながる Internet of Things（IoT）において，データの利活用を推進することで付加価値の創出を目指している。具体的なスキームの 1 つとしては，エッジ（端末）からデータをクラウド（データベース）にあげ，クラウドでデータを解析・加工し，またエッジに情報（解析結果）を提供する事を繰り返すことで，高度なサービスを実現する。このエッジ・クラウドによるサービスを持続可能なものにするための課題の 1 つにエッジの電源問題があり，電源配線や電池交換にかかるコストが指摘されている。そのため，エッジの電源の課題を解決する技術として，光や電波，振動，熱を電気エネルギーに変換する環境発電技術が注目されている。

一方で，あらゆるものがネットワーク接続されるため，サイバー・フィジカル・セキュリティの問題を解決することも必須課題である。このサイバー･フィジカル･セキュリティの問題では，従来の不正アクセスに代表される攻撃だけでなく，個人情報保護の観点からプライバシーを考慮する必要がある。プライバシー問題について，国内では平成 17 年に全面施行された個人情報保護法が，平成 29 年に改正され，厳罰化だけでなく，適用対象が拡大した。改正前は 5001 人以上の事業者のみが対象であったが，改正後は全ての事業者が対象となった。このことは，小規模事業者でなく，非営利団体や大学の研究室も法律の対象に含まれることを意味する。

２．研究の目的

申請研究では，Society 5.0 を支えるエッジを実現するプライバシーを考慮したセキュアなデバイスを開発する。このセキュアなデバイスでは，プライバシーを保護するだけでなく，情報を秘匿するため暗号化やセキュアな認証を実現する。本研究の成果により，エッジからクラウドへのデータ転送，また，クラウドでのデータの解析・加工後のクラウドからエッジへのデータ転送のスキーム全体をセキュアに実行することが可能になる。このように申請研究で開発するプライバシーを考慮したセキュアなデバイスは，Society 5.0 を支える基盤技術の 1 つで，社会の安定と安心・安全に貢献できる。

３．研究の方法

プライバシーを考慮したセキュアなデバイスを開発するために，申請研究では(1)エッジ向けセキュアインテリジェントモジュールと(2)プライバシーを考慮した認証方式をそれぞれ開発する。

まず(1)では，セキュリティの要である暗号モジュールでは，代表的な不正攻撃であるサイドチャネル攻撃に対してはハイディング（隠蔽）とマスキング（遮蔽）の多重化対策により，高いタンパ性確保する。さらに，エッジでは消費電力削減も大きな課題であるため，低消費電力も同時に実現する。ここでは，これまで研究を進めてきた軽量暗号の対策技術を応用すると共に，実装方式についても高いタンパ性と低レイテンシを確保できるアンロールドアーキテクチャを用いる。一般的に高いタンパ性を確保するための対策は，面積と消費電力のオーバーヘッドが大きくなる傾向がある。申請研究では，アンロールドアーキテクチャでの攻撃・解析対象になる部分は，耐タンパ実装を優先して，攻撃・解析対象外の部分では，面積と消費電力の削減を優先する適応的な実装を実現する。

次に(2)では，プライバシーを考慮した認証方式では，これまで進めてきた認証暗号，検索可能暗号，秘密分散法の研究を応用する。これらの技術を組み合せる事で，セキュアに認証技術を確立する。

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。申請研究での研究成果の１つとして，アンロールドアーキテクチャ実装の PRINCE を利用したグリッチ PUF（P-PUF）を開発した。アンロールドアーキテクチャでは，暗号コアが全て組み合わせ回路で実現されるため，生じるグリッチは大きくなる。P-PUF では，このグリッチ波形を利用することで，機器の認証に必要な ID を生成する。PRINCE への入力を PUF のチャレンジとし，PRINCE による計算結果をレスポンス生

成器へ入力して PUF のレスポンスを生成する。ここで，P-PUF は PRINCE の暗号コア全体ではなく，任意のタイミングの計算結果をグリッチ生成器として利用できる。任意のタイミングを利用することで，PUF の使用目的に合わせて安定性やユニーク性を調整することができる。レスポンス生成では，対象の出力をレスポンス生成器の TFF へと入力する．このとき，出力は 64bit であるため，64bit 分の TFF へ接続し，64bit のレスポンスを生成する。また，P-PUF の安全性を評価するための深層学習（Deep Neural Network: DNN）を利用したモデリング攻撃手法についても開発した。開発したモデルでは 4 層の中間層を用いた全結合による DNN であり，入力層は P-PUF の 64bit チャレンジに合わせて，64 個のニューロンで構成した。中間層は 4,000 個，8,000 個，4,000 個，32 個のニューロンで構成しており，出力層は各レスポンスをビットごとに予測するために，2 個のニューロンで構成した．中間層の活性化関数には ReLU 関数を，出力層の活性化関数には softmax 関数をそれぞれ使用した。また，勾配消失を防ぐためのバッチ正則化に加え，過学習を抑えて汎化性能を向上させるためのドロップアウト処理を適用した。損失関数には，categorical cross entropy を，学習時における最適化アルゴリズムには，広く利用されている Adam を利用した。

P-PUF の有効性を検証するために FPGA を用いた評価実験を行った。P-PUF は PRINCE の任意の範囲をグリッチ生成器として利用することができる．そこで実験では，(a)1R 目の S 層の出力，(b)1R 目の出力，(c)2R 目の M 層の出力の 3 種類の P-PUF を実装し，評価した。PUF の性能評価の実験では，それぞれ，L，K，N，T が 128，128，3，100 となるようにレスポンスを取得した。具体的には，256 種類の 64bit チャレンジを乱数で生成し，これらのチャレンジから 256 種類の 64bit レスポンス，すなわち 128 種類の 128bit の ID を取得した。ID の評価項目はいくつかあるが，ここでは最も重要な安定性とユニーク性について示す。

まず，安定性は，同一チャレンジに対する ID 間のハミング距離（Same Challenge Intra-HD：SC Intra-HD）で評価する。安定性の実験結果を図 1 に示す。

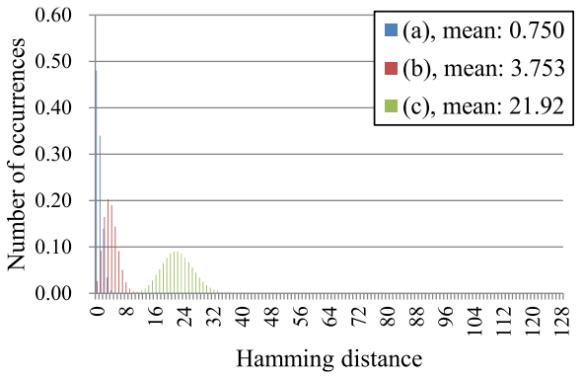

図 1 安定性の評価結果

図 1 から SC Intra-HD の平均は，各実装で 0.750，3.753，21.92 であることが分かる。このとき，(a)(b)の実装では SC Intra-HD は 0 に近く，これはそれぞれ PG PUF で生成される ID の 99%，97%以上が同一の値であることを示しており，ID の安定性が高いことが分かる。一方で，(c)の実装では SC Intra-HD は 21.92 であり，他の実装と比較して安定性が低下していることが確認できる。これはグリッチ生成器の段数が深くなることで，生成されるグリッチ波形が複雑になることが原因だと考えられる。

次に，ユニーク性の評価では，機器間での ID 間のハミング距離（Same Challenge Inter-HD: SC Inter-HD）の平均だけでなく，分布の情報を用いた。そのため，SC Inter-HD の平均値に加えて，分布の標準偏差（Standard Deviation：SD）を算出した。ここで，SC Inter-HD の分布について，SD が小さく（分布の広がりが狭く），安定性の基準である SC Intra-HD の分布と重ならなければ，良好なユニーク性をもつと評価できる。ユニーク性の実験結果を図 2 に示す。

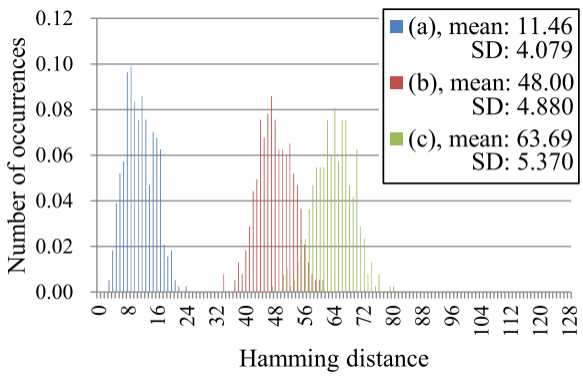

図 2 ユニーク性の評価結果

図 2 から(c)の実装では，SC Inter-HD の平均は 63.69 であり，平均は ID 長の半分である 64 に近い。また，SD は 5.370 程度でありユニーク性が高いことが分かる。また，(b)の実装では SC Inter-HD の平均は 48.00 であるが，従来研究の AES の Sbox を利用したグリッチ PUF では，SC Inter-HD を正規化した値は 39.8%であり，(b)の結果を同様に正規化すると 37.5% であることから，ほぼ同等の結果である。また，SD も 4.880 程度であり，良好なユニーク性をもっていると考えられる。一方で，(a)の実装では SC Inter-HD の平均は 11.46 である。また，SD は 4.079 でありユニーク性が低下していることが確認できる。これは，グリッチ生成器の段数が浅いことで複雑なグリッチ波形が生成できず，機器ごとのばらつきを抽出できなかったためだと考えられる。

最後に，モデリング攻撃について，最も耐性が高かった実装(c)の実験結果を図 3 に示す。

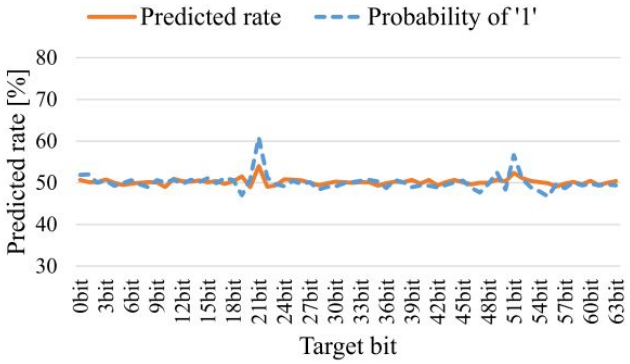

図 3 実装(c)の実験結果

図 3 より，(c)の実装ではほとんどのビット位置で予測率が 50%程度であることが確認でき，モデリング攻撃に対して耐性をもつことが分かる。これはグリッチ生成器の段数が深くなることで，複雑なグリッチ波形が生成され，攻撃に必要なモデル生成が困難になったためだと考えられる。

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　4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 竹本 修、池崎 良哉、野崎 佑典、吉川 雅弥	４．巻 63
２．論文標題 Midori128に対する電力解析攻撃手法と低エネルギーなセキュア実装	５．発行年 2022年
３．雑誌名 情報処理学会論文誌	６．最初と最後の頁 831～839
掲載論文のDOI（デジタルオブジェクト識別子） 10.20729/00217479	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 西田奏太，野崎佑典，吉川雅弥	４．巻 vol. 140, no. 7
２．論文標題 車載向け認証方式でのメッセージ長を削減するカウンタ同期手法とその評価	５．発行年 2020年
３．雑誌名 電気学会論文誌C	６．最初と最後の頁 826-834
掲載論文のDOI（デジタルオブジェクト識別子） 10.1541/ieejeiss.140.826	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 竹本修，西田奏太，野崎佑典，本田晋也，倉地亮，吉川雅弥	４．巻 vol. 140, no. 8
２．論文標題 SROS2における認証付き暗号の組込みシステムを指向したセキュア実装とその評価	５．発行年 2020年
３．雑誌名 電気学会論文誌C	６．最初と最後の頁 939-948
掲載論文のDOI（デジタルオブジェクト識別子） 10.1541/ieejeiss.140.939	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 竹本修，野崎佑典，吉川雅弥	４．巻 vol.139, no.12
２．論文標題 アンロールドアーキテクチャ実装したPRINCEの電力解析に対する多重対策手法とその評価	５．発行年 2019年
３．雑誌名 電気学会論文誌C	６．最初と最後の頁 1380-1388
掲載論文のDOI（デジタルオブジェクト識別子） 10.1541/ieejeiss.139.1380	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16件（うち招待講演　0件／うち国際学会　7件）

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

２．発表標題
AI Hardware Oriented Trojan Detection Architecture

３．学会等名
5th International Conference on Electronics, Communications and Control Engineering（国際学会）

４．発表年
2022年

１．発表者名
竹本修，池崎良哉，野崎佑典，吉川雅弥

２．発表標題
SROS2における最終ラウンド候補軽量暗号の評価

３．学会等名
電子情報通信学会技術研究報告

４．発表年
2022年

１．発表者名
濵口晃輔，竹本修，野崎佑典，吉川雅弥

２．発表標題
低遅延暗号MANTISを利用したグリッチPUFの実装評価

３．学会等名
電子情報通信学会技術研究報告

４．発表年
2022年

１．発表者名
竹本修，池崎良哉，野崎佑典，吉川雅弥

２．発表標題
AIハードウェアに対するトロイ検出器の評価

３．学会等名
電子情報通信学会技術研究報告

４．発表年
2022年

１．発表者名
三輪峻右，竹本修，野崎佑典，吉川雅弥

２．発表標題
低消費電力暗号Midori128へのアンロールドアーキテクチャ実装を指向した対策回路の実装と評価

３．学会等名
電子情報通信学会技術研究報告

４．発表年
2022年

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

２．発表標題
High-Level Synthesis against Authenticated Lightweight Cryptography Finalists

３．学会等名
RISP International Workshop on Nonlinear Circuits, Communications and Signal Processing（国際学会）

４．発表年
2022年

１．発表者名
竹本修，池崎良哉，野崎佑典，吉川雅弥

２．発表標題
最終ラウンド候補の認証機能付き軽量暗号に対する高位合成の評価

３．学会等名
暗号と情報セキュリティシンポジウム

４．発表年
2022年

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

２．発表標題
Hardware Trojan for Lightweight Cryptoraphy Elephant

３．学会等名
EEE 10th Global Conference on Consumer Electronics（国際学会）

４．発表年
2021年

１．発表者名
竹本修，池崎良哉，野崎佑典，吉川雅弥

２．発表標題
軽量暗号に対する高位合成の評価

３．学会等名
電気・情報関係学会北陸支部連合大会

４．発表年
2021年

１．発表者名
竹本　修，池崎良哉，野崎佑典，吉川雅弥

２．発表標題
セキュア実装の軽量暗号をターゲットとしたハードウェアトロイの検討

３．学会等名
2020年度電気・情報関連学会北陸支部連合大会

４．発表年
2020年

１．発表者名
竹本　修，池崎良哉，野崎佑典，吉川雅弥

２．発表標題
低遅延実装の対策回路を指向したハードウェアトロイ挿入とその評価

３．学会等名
電子情報通信学会技術研究報告

４．発表年
2020年

１．発表者名
F. Mizutani, Y. Nozaki, and M. Yoshikawa

２．発表標題
Security evaluation of timing attacks based on CNN complexity

３．学会等名
the 6th IEEE International Conference on Applied System Innovation（国際学会）

４．発表年
2020年

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

２．発表標題
Hardware Trojan Focusing on Plaintext in Power Analysis Attacks

３．学会等名
the 6th IEEE International Conference on Applied System Innovation（国際学会）

４．発表年
2020年

１．発表者名
F. Mizutani, S. Takemoto, Y. Nozaki, and M. Yoshikawa

２．発表標題
Adapting Generating Method for Imperceptibility Adversarial Examples

３．学会等名
2021 RISP International Workshop on Nonlinear Circuits, Communications and Signal Processing（国際学会）

４．発表年
2021年

１．発表者名
S. Takemoto, F. Mizutani, Y. Ikezaki, Y. Nozaki, and M. Yoshikawa

２．発表標題
Detection Evaluation for Netlist of Secure Cryptographic Module with Malicious Circuit

３．学会等名
2021 RISP International Workshop on Nonlinear Circuits, Communications and Signal Processing（国際学会）

４．発表年
2021年

１．発表者名
竹本修，野崎佑典，吉川雅弥

２．発表標題
相互情報量解析に対する電力解析攻撃用の多重化対策手法の安全性実装評価

３．学会等名
令和2年電気学会全国大会予稿集

４．発表年
2020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