情報処理学会論文誌 Vol.63 No.3 840–848 (Mar. 2022)

秘密分散法を利用したPUFのセキュア認証方式とその評価

野崎 佑典[1,a)] 吉川 雅弥[1]

受付日 2021年5月10日, 採録日 2021年12月3日

概要：本研究では，新たに秘密分散法を利用した Physically Unclonable Function（PUF）のセキュア認証方式を提案する．提案手法では，PUF レスポンスから生成した分散情報を通信に用いることで，機械学習攻撃への耐性を向上させる．評価実験では，機械学習攻撃による安全性評価を行い，提案手法が攻撃に対して耐性を持つことを明らかにした．また，回路規模の比較結果から従来の対策 PUF を用いた認証方式と比較して回路規模を削減し，提案手法は小回路規模で利用可能であることを示した．

キーワード：ハードウェアセキュリティ，PUF，機械学習攻撃，秘密分散法

PUF Secure Authentication Method Using Secret Sharing Schemes and its Evaluation

Yusuke Nozaki[1,a)] Masaya Yoshikawa[1]

Received: May 10, 2021, Accepted: December 3, 2021

Abstract: This paper proposes a new physically unclonable function (PUF) secure authentication method utilizing secret sharing schemes. The proposed method enhances the resistance against machine learning attacks by using distributed values generated from PUF responses for communication. Experimental results of security evaluation showed the proposed method had the resistance to machine learning attacks. In addition, the comparison results showed that the proposed method could reduce the circuit area.

Keywords: hardware security, PUF, machine learning attack, secret sharing scheme

1. はじめに

Internet of Things（IoT）によって，様々な機器がネットワークと接続されるようになっており，これらのデバイスのセキュリティを確保することは重要な課題である．セキュリティの確保に関して，Physically Unclonable Function（PUF）が機器の認証技術として注目されている [1], [2], [3], [4], [5], [6], [7]．PUF は，IoT 機器で用いられる Large Scale Integration（LSI）の製造ばらつきから，機器固有の ID を生成する技術である．この ID を用いることで，各機器の認証を行うことができる．また，製造ばらつきは人工的に制御することが難しく，PUF で生成する ID は物理的に複製困難とされている．

PUF を使用した機器の簡易認証方式として，チャレンジ・レスポンス認証が知られている [3]．この認証方式では，まず PUF のチャレンジとレスポンスの組（Challenge and Response Pairs：CRPs）を事前にデータベースに登録する．認証を行う際には，対象機器にチャレンジを入力し，このときに得られるレスポンスとデータベースに登録されているレスポンスを照合することで認証する．一方で，チャレンジ・レスポンス認証でやりとりされる CRPs を複数個利用した機械学習を行うことで，PUF の認証機能を複製する機械学習攻撃の脅威が指摘されている [8], [9], [10], [11], [12], [13]．そのため，機械学習攻撃に対する耐性を向上させた対策 PUF [2], [5], [6], [7] がいくつ

[1] 名城大学
Meijo University, Nagoya, Aichi 468–8502, Japan
[a)] 143430019@ccalumni.meijo-u.ac.jp

本論文の内容は，著者らがこれまでに発表した内容 [25] に，詳細な実装方式とその評価結果を加えて発展させたものである．

か提案されている．しかし，対策 PUF は無対策の PUF と比べ，その構造を拡張する必要があるため，回路規模が増加する．ここで，IoT で用いる組み込み機器は回路規模に制約があるため，回路規模の増加を抑えた方式が必要とされている．

そこで本研究では，従来の対策 PUF とは異なり，回路の実装オーバヘッドを抑えた機械学習攻撃に耐性を持つ PUF の認証方式を提案する．提案手法は，新たに秘密分散法を導入することで，攻撃耐性を持つ機器の認証を実現する．提案手法では，PUF のレスポンスを秘密情報と見なして分散情報を生成する．そして，生成した分散情報をレスポンスの代わりに認証に利用する．提案手法は，PUF のレスポンスを直接やりとりしないことで，機械学習攻撃への耐性を向上させる．そして，機械学習攻撃による安全性評価やハードウェア実装評価によって，提案手法の有効性を検証する．

2. 準備

まず，2.1 節では PUF の概要について，2.2 節ではチャレンジ・レスポンス認証と PUF の機械学習攻撃について説明する．そして，2.3 節では本研究で使用する秘密分散法について，2.4 節では関連する研究について述べる．

2.1 PUF

PUF は，LSI の製造ばらつきから機器固有の ID を生成する技術である．具体的には，入力であるチャレンジに対して，レスポンスと呼ばれる値を出力する．これまでに多くの PUF が提案されているが，本研究では代表的な PUF の 1 つであるアービタ PUF [2] を例に説明する．

アービタ PUF の概要を**図 1** に示す．図 1 に示すように，アービタ PUF は 2 本の等長な配線上の N 個のセレクタユニット（マルチプレクサのペア）とアービタ回路で構成する．アービタ PUF のチャレンジは N bit であり，それぞれ各セレクタユニットへと入力される．このチャレンジによって，各信号の伝搬経路（チャレンジが 0 のときは直進経路，1 のときは交差経路）が決定し，最終的にアービタ回路へ入力される．アービタ回路では，2 つの信号の到着順を判定し，この判定結果を 1 bit のレスポンスとして出力する．

2.2 チャレンジ・レスポンス認証と機械学習攻撃

チャレンジ・レスポンス認証方式 [3] の概要を**図 2** に示す．チャレンジ・レスポンス認証方式では，事前に CRPs をデータベースに登録する．認証時には，任意のチャレンジを対象の PUF に入力し，このときのレスポンスを取得する．そして，取得したレスポンスとデータベース上のレスポンスを照合することで，対象機器を認証する．

しかし，チャレンジ・レスポンス認証方式は機械学習攻撃に対して脆弱であることが知られている [8], [9]．機械学習攻撃では，**図 3** に示すようにチャレンジ・レスポンス認証方式でやりとりする CRPs を複数個窃取する．そして，この CRPs を利用した機械学習を行うことで，対象の PUF のレスポンスを予測するモデルを生成する．

アービタ PUF に対する機械学習攻撃では，アービタ PUF 内部の信号伝搬遅延とチャレンジ，レスポンスの関係を線形式で表現する．具体的には，文献 [8], [9] のモデリングに基づき，チャレンジを特徴ベクトルへと変換し，この特徴ベクトルとレスポンスを入力とした機械学習によって，PUF 内部の信号伝搬遅延を重みベクトルとして学習する．そして，この学習結果を PUF のレスポンス予測モデルとして使用する．

そのため，機械学習攻撃に対して耐性を持つ PUF が提案されている．代表的な対策 PUF には，XOR アービタ PUF [2] や Lightweight PUF [6]，Double アービタ PUF [7] などがある．これらの対策 PUF は複数のアービタ PUF で構成し，各アービタ PUF の出力を XOR 演算したものをレ

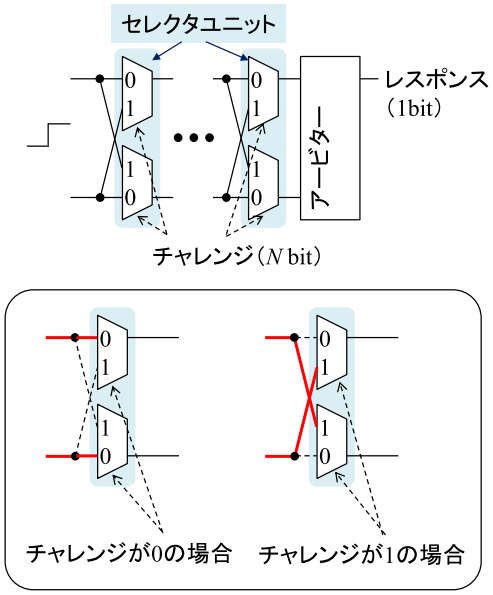


図 1 PUF の概要
Fig. 1 Outline of PUF.

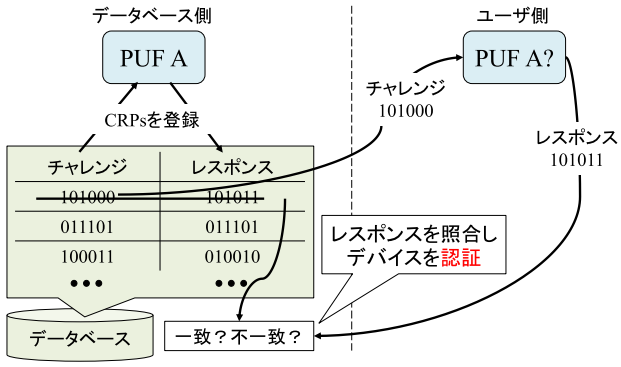


図 2 チャレンジ・レスポンス認証
Fig. 2 Challenge and response authentication.

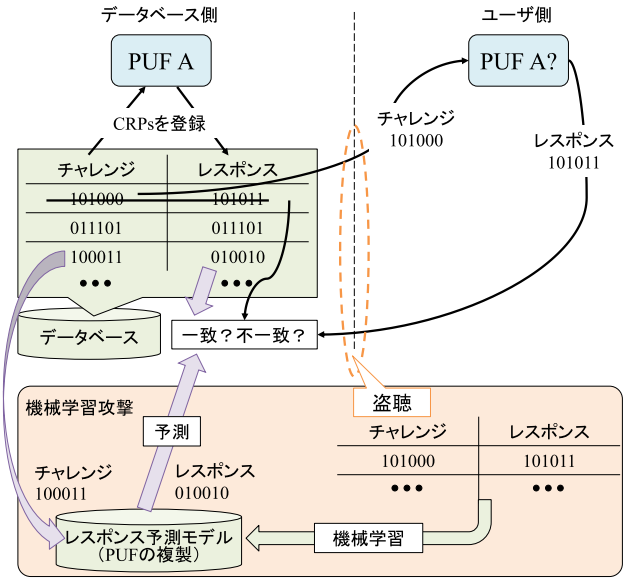


図 3 機械学習攻撃
Fig. 3 Machine learning attack.

スポンスとして利用する．XOR 演算を行うことで，チャレンジとレスポンスの関係を線形式で表現することを困難にし，機械学習攻撃への耐性を向上させている．一方で，対策 PUF は複数のアービタ PUF で構成するため，通常の PUF と比較して，回路規模が倍以上に増加する．

2.3 秘密分散法

秘密分散法は，秘密情報を複数の分散情報へと分割し，分散情報をいくつか集めることで，秘密情報を復元する手法である [14], [15]．このとき，一部の分散情報が漏えいしたとしても，あらかじめ決められた分散情報を集めなければ，秘密情報は復元できない．そのため，秘密分散法は暗号化に必要な秘密鍵などの重要な情報の管理に利用されている．秘密分散法は，主に分散情報を生成する分散処理と，秘密情報を復元する復元処理で構成する．(k,n) 閾値秘密分散法（(k,n) Threshold Secret Sharing Scheme：TSSS [14], [15]）では，n 個の分散情報を生成し，このうち k 個の分散情報を利用することで，秘密情報を復元することができる（$k<n$）．一方で，集めた分散情報が k よりも少ない場合，秘密情報を復元することができない．

(k,n)-TSSS に関して，$k=2$，$n=3$ の場合（$(2,3)$-TSSS）を例に説明する．$(2,3)$-TSSS ではある 1 次関数 y（$y=ax+S$）を利用する．まず分散処理では，秘密情報 S を 1 次関数の y 切片と見なし，傾き a は乱数で決定する．そして，1 次関数上の任意の 3 点を分散情報 W_0，W_1，W_2 として生成する．次に復元処理では，3 点の分散情報のうち任意の 2 点の分散情報を利用した連立方程式を解くことで，秘密情報 S を復元する．このとき，分散情報を 1 点しか得ることができない場合，1 次関数を一意に決定することができないため，秘密情報を復元することはできない．

また，高速に計算可能な TSSS として XOR 演算を利用した手法（(k,n)-XOR-TSSS）も提案されている [16]．ここでは，$(2,3)$-XOR-TSSS について説明する．まず分散処理では，秘密情報 S を 2 つの秘密情報 S_1，S_2 に分割する（$S=S_1 \parallel S_2$）．次に，2 つの乱数 R_0，R_1 との XOR 演算によって，3 つの分散情報 W_0，W_1，W_2 を生成する．この分散情報の計算式を式 (1) から (3) に示す．ここで，S_0 はすべて 0 のビット列を，$\oplus$ は XOR 演算を，$\parallel$ はビットの連結を表している．

$$W_0 = S_0 \oplus R_0 \parallel S_2 \oplus R_1 \tag{1}$$
$$W_1 = S_1 \oplus R_0 \parallel S_0 \oplus R_1 \tag{2}$$
$$W_2 = S_2 \oplus R_0 \parallel S_1 \oplus R_1 \tag{3}$$

復元処理では，3 つの分散情報のうち 2 つの分散情報を用いた XOR 演算を計算することで，秘密情報を復元することができる．具体的には，分散情報 W_1 と W_2 を用いる場合，式 (4) に示すように，XOR 演算によって乱数によるマスクを打ち消すことができる．

$$W_1 \oplus W_2 = S_1 \oplus S_2 \parallel S_0 \oplus S_1 \tag{4}$$

2.4 関連する研究

PUF を用いた認証方式について，チャレンジ・レスポンス認証以外の手法もいくつか提案されている [17], [18]．しかしこれらの手法では，対策 PUF の利用や，ハッシュ関数や暗号回路の追加実装が必要とされるため，通常のチャレンジ・レスポンス認証と比べ，回路規模が大きくなる．

秘密分散法に関連する研究としては，PUF を用いた秘密分散法の構成方法に関するもの [19] や，視覚復号型秘密分散法（Visual SSS：VSSS）を利用した PUF の認証手法 [20] が提案されている．文献 [19] の研究では，Controlled PUF を使用した情報比を改善した秘密分散法の構成方法を提案している．この手法は，秘密分散法の構成方法の研究であるため，PUF の認証方法は示されていない．また文献 [20] の研究では，VSSS と PUF を用いた認証手法が提案されているが，その構成方法の詳細について不明瞭な部分がある．さらに，機械学習攻撃耐性に関する安全性評価は行われおらず，有効性は不明瞭である．

本研究で提案する認証手法は，ハッシュ関数や暗号回路を必要としないため，回路規模の増加を抑えることができる．また，回路規模増加の抑制に加えて，機械学習攻撃への耐性を向上させた機器の認証を実現する．

3. 提案手法

本研究では，PUF のセキュア認証方式として，秘密分散法を利用した手法を提案する．まず，3.1 節では提案手法の概要について説明する．そして，提案手法を実現するための方法として，3.2 節では $(2,3)$-TSSS を使用する手法

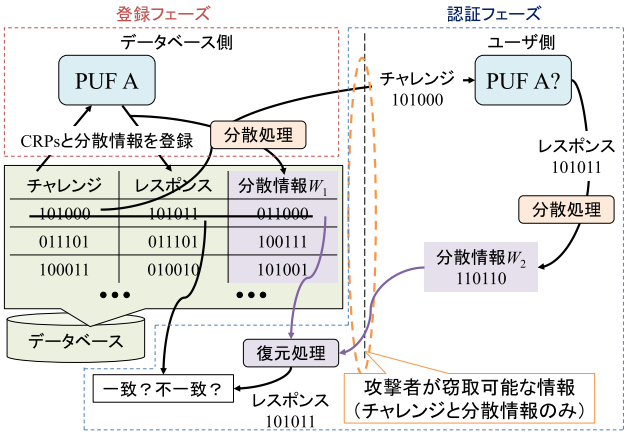


図 4 提案手法の概要

Fig. 4 Outline of the proposed method.

を，3.3 節では $(2,3)$-XOR-TSSS を使用する手法について，それぞれ説明する．

3.1 提案手法の概要

提案手法の概要を**図 4** に示す．提案手法では，従来のチャレンジ・レスポンス認証とは異なり，データベース側とユーザ側で PUF レスポンスを直接やりとりしない．提案手法では，PUF レスポンスを秘密分散法における秘密情報と見なして，分散情報を生成する．そして，図 4 に示すように，生成した分散情報を認証に利用する．ここで，通常の秘密分散法の乱数の代わりに PUF レスポンスを用いることに関して，文献 [21] では NIST SP800-22 の検定を通して PUF レスポンスのエントロピーが十分であることが評価されている．また提案手法は，登録フェーズと認証フェーズの 2 つの処理で構成する．

まず，登録フェーズでは，PUF レスポンスから秘密分散法の分散処理を利用して分散情報を生成する．そして，データベース上には，PUF のチャレンジとレスポンスに加えて，生成した分散情報をそれぞれ登録する．次に，認証フェーズでは，対象の PUF にチャレンジを与えてレスポンスを取得する．そして，取得したレスポンスから秘密分散法の分散処理によって，分散情報を生成し，この分散情報をデータベース側へ送信する．データベース側では，受信した分散情報とデータベース上の分散情報の 2 つの情報を利用して，秘密分散法の復元処理を実施する．この復元処理で，秘密情報である PUF レスポンスを復元し，データベース上の PUF レスポンスと照合し，認証を行う．以上のように，提案手法はチャレンジと分散情報のみを通信に用いるため，PUF レスポンスを直接やりとりしない．また，1 つの分散情報のみでは，秘密分散法によってレスポンスを復元することができない．そのため，提案手法を用いることで，機械学習攻撃への耐性を向上させることができる．

提案手法の具体的な実現方法に関して，$(2,3)$-TSSS を用いる手法は 3.2 節で，$(2,3)$-XOR-TSSS を用いる手法は 3.3 節でそれぞれ説明する．

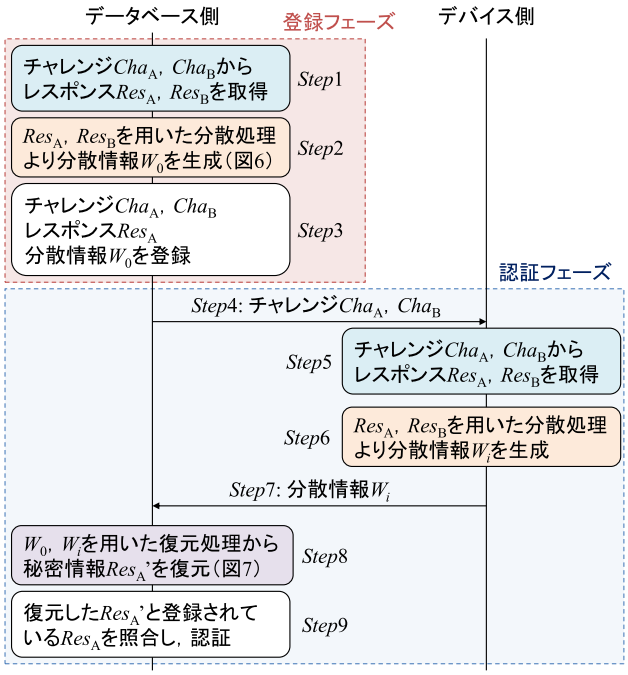


図 5 提案手法（$(2,3)$-TSSS）の認証の流れ

Fig. 5 Authentication flow of the proposed method using $(2,3)$-TSSS.

3.2 $(2,3)$-TSSS を使用する場合

まず，認証の流れを**図 5** に示す．図 5 に示すように，9 個の Step で構成する．登録フェーズでは，2 種類のチャレンジ（Cha_A と Cha_B）から 2 種類の PUF レスポンス（Res_A と Res_B）を取得する（図 5 の *Step1*）．次に，取得した 2 種類のレスポンスを使用した分散処理によって分散情報を生成する．この登録フェーズにおける分散処理を**図 6** に示す．図 6 に示すように，レスポンス Res_A は $(2,3)$-TSSS の秘密情報である y 切片と見なし，レスポンス Res_B は 1 次関数の傾きとして利用する．すなわち，1 次関数は $y = Res_B x + Res_A$ となる．そして，1 次関数 y 上の任意の x（$x = x_0$）に対する値 y（$y = y_0$）を計算し，これを分散情報（$W_0 = (x_0, y_0)$）とする（図 5 の *Step2*）．最後に，2 つのチャレンジ（Cha_A と Cha_B）とレスポンス Res_A，分散情報 W_0 をデータベース上に登録する（図 5 の *Step3*）．

認証フェーズでは，データベース側から対象機器に対して 2 種類のチャレンジ（Cha_A と Cha_B）を送信する（図 5 の *Step4*）．ユーザ側では，受信したチャレンジから 2 種類の PUF レスポンス（Res_A と Res_B）を取得する（図 5 の *Step5*）．そして，登録フェーズの分散処理と同様に，1 次関数 $y = Res_B x + Res_A$ から分散情報を生成する．このとき，登録フェーズとは別の任意の x（$x = x_i$）から y_i を計算して，これを分散情報（$W_i = (x_i, y_i)$）とする（図 5 の

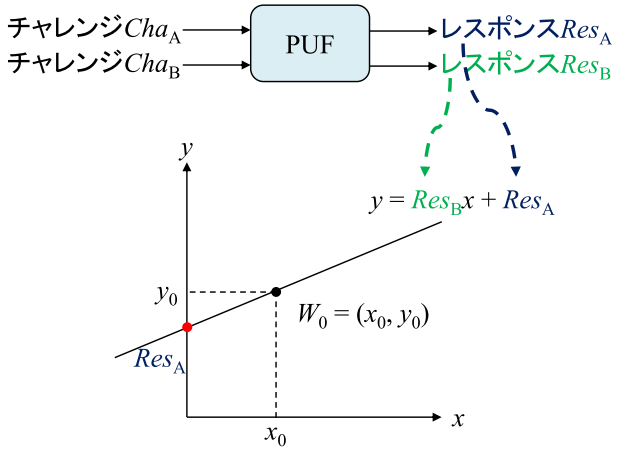


図 6 提案手法（(2, 3)-TSSS）の分散処理

Fig. 6 Distribution processing of the proposed method using (2, 3)-TSSS.

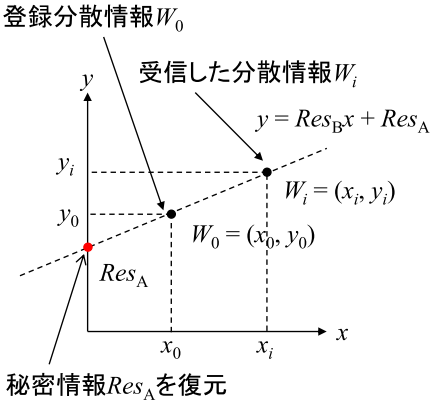


図 7 提案手法（(2, 3)-TSSS）の復元処理

Fig. 7 Restoration processing of the proposed method using (2, 3)-TSSS.

Step6）．次に，生成した分散情報 W_i をデータベース側へ送信する（図 5 の *Step7*）．

データベース側では，**図 7** に示すように，受信した分散情報 W_i とデータベース上に登録してある分散情報 W_0 を用いて，秘密情報 Res_A' を復元する（図 5 の *Step8*）．そして，復元した秘密情報 Res_A' とデータベース上に登録してある秘密情報 Res_A を照合し，認証を行う（図 5 の *Step9*）．

以上のように，提案手法は (2, 3)-TSSS をベースとしているが，実際に生成する分散情報は 2 種類である．そのため，秘密分散法に関するパラメータは $k = 2$，$n = 2$ ととらえることができる．

3.3 (2, 3)-XOR-TSSS を使用する場合

(2, 3)-XOR-TSSS を使用する場合も，3.2 節の (2, 3)-TSSS を使用する場合と同様の流れで認証を行う．異なる点は，認証フェーズにおいて，(2, 3)-TSSS は任意の分散情報 W_i をデータベース側へ送信していたが，(2, 3)-XOR-TSSS は分散情報 W_2 を送信する．

まず，登録フェーズでは，あるチャレンジ（Cha_A と Cha_B）に対する PUF レスポンス（Res_A と Res_B）をそれぞれ取得する．ここで，レスポンス Res_A を秘密情報と見なし，2 つの秘密情報 S_1，S_2 に分割する（$Res_A = S_1 \parallel S_2$）．また，レスポンス Res_B も 2 つの情報 R_0，R_1 に分割して（$Res_B = R_0 \parallel R_1$），それぞれ (2, 3)-XOR-TSSS の乱数として使用する．そして，**図 8** に示すように，式 (1) から式 (3) を利用して，分散情報を生成する．最後に，チャレンジ（Cha_A と Cha_B）とレスポンス Res_A，分散情報（W_0 または W_1）をデータベース上に登録する．

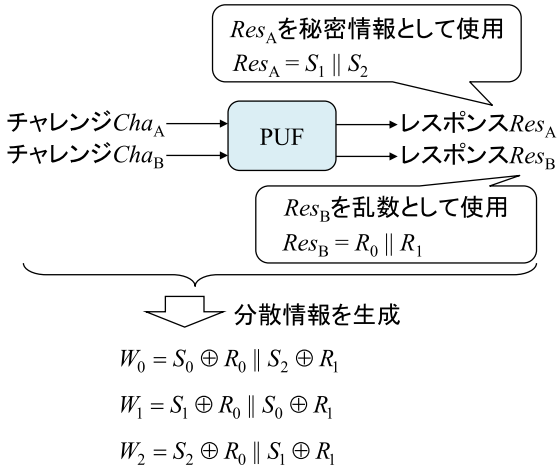


図 8 提案手法（(2, 3)-XOR-TSSS）の分散処理

Fig. 8 Distribution processing in the proposed method using (2, 3)-XOR-TSSS.

認証フェーズでは，対象機器に対してチャレンジ（Cha_A と Cha_B）を与えて，PUF レスポンス（Res_A と Res_B）を取得する．そして，登録フェーズの分散処理と同様にして分散情報を生成し（図 8 を参照），生成した分散情報 W_2 をデータベース側へ送信する．このとき，(2, 3)-TSSS を使用する場合とは異なり，分散情報として W_2 を送信する．なぜなら，分散情報 W_0 と W_1 で使用する S_0 はすべて 0 のビット列であるため，W_0 または W_1 が盗聴された場合，攻撃者に PUF レスポンスを直接観測されるからである（式 (1)，(2) を参照），一方で，分散情報 W_2 は XOR 演算によってレスポンス情報を秘匿することができる．そして，データベース側では，**図 9** に示すように，受信した分散情報 W_2 とデータベース上に登録してある分散情報（W_0 または W_1）を利用して，レスポンスを復元する．最後に，復元したレスポンス Res_A' とデータベース上に登録してあるレスポンス Res_A を照合することで，認証を行う．

以上のように，提案手法（(2, 3)-XOR-TSSS）は PUF レスポンスに対して XOR 演算を用いた計算によって実現できる．ここで，XOR 演算を用いる PUF には XOR アービタ PUF [2] などがあるが，XOR アービタ PUF は複数のアービタ PUF を必要とするのに対して，提案手法では複数の PUF を必要としないため，小回路規模で実現することができる．

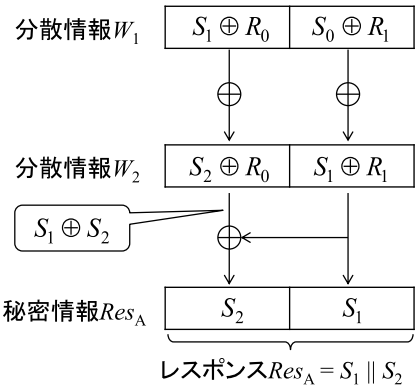


図 9 提案手法（(2, 3)-XOR-TSSS）の復元処理

Fig. 9 Restoration processing in the proposed method using (2, 3)-XOR-TSSS.

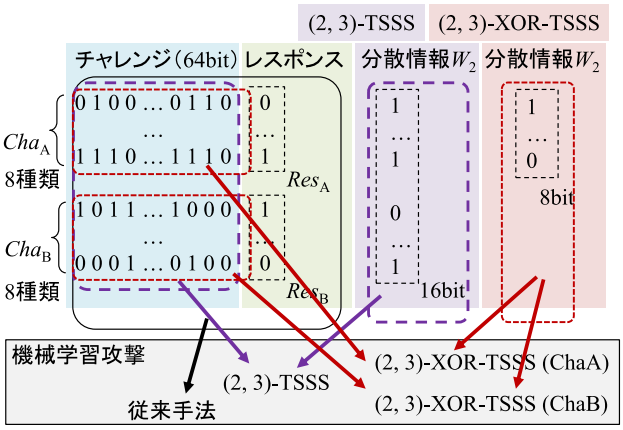


図 10 実験方法

Fig. 10 Experimental method.

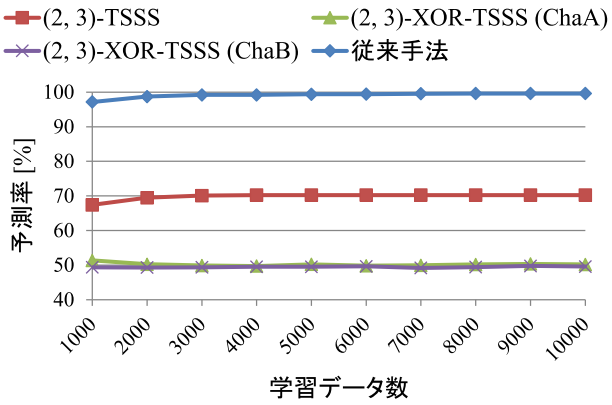


図 11 機械学習攻撃の結果

Fig. 11 Results against machine learning attack.

最後に，提案手法では認証のために，データベースにCRPs に加えて分散情報も保持する必要があり，分散情報の保持が追加のコストとなる．これに関して，デバイス側であらかじめどの分散情報を生成するかを決めておくことで，データベース側での分散情報の保持コストを削減できると考えられる．具体的には，認証時にデータベース側のレスポンスから，デバイス側とは異なる分散情報を生成することで，復元処理を適用し，認証を行うことができる．

4. 機械学習攻撃耐性評価

提案手法の有効性を検証するために，機械学習攻撃による安全性評価を行った．4.1 節では実験環境と実験方法について述べる．そして，4.2 節では実験結果について述べる．

4.1 実験環境

この実験では，提案手法と従来のチャレンジ・レスポンス認証に対してそれぞれ機械学習攻撃を実施した．実験はシミュレーションで行い，PUF にはアービタ PUF を使用した．アービタ PUF のセレクタ段数は 64（$N = 64$）とし，文献 [10] と同様に各セレクタ間の信号遅延は平均 300，標準偏差 40 のガウス分布に従う乱数で決定した．

実験方法を**図 10** に示す．提案手法における Res_A と Res_B のビット長はそれぞれ 8 bit とした．アービタ PUF は，1 種類のチャレンジに対して，1 bit のレスポンスを出力するため，1 つの分散情報（(2, 3)-TSSS は 16 bit，(2, 3)-XOR-TSSS は 8 bit）の生成には 16 種類のチャレンジを利用した．また，(2, 3)-TSSS の分散処理の任意の x_i の値は 2 で固定した．

機械学習攻撃にはロジスティック回帰を使用し，従来手法を対象とした実験では，アービタ PUF のチャレンジから生成した特徴ベクトルとレスポンスを学習に使用した．また，提案手法を対象とした実験では，特徴ベクトルと分散情報を学習に使用した．このとき，(2, 3)-XOR-TSSS では，16 種類のチャレンジ（8 種類の Cha_A と Cha_B）から 8 bit の分散情報が生成される．そのため，チャレンジと分散情報が 1 対 1 で対応しないため，図 10 に示すように，実験では Cha_A を使用した攻撃と，Cha_B を使用した攻撃をそれぞれ実施した．

4.2 実験結果

機械学習攻撃の実験結果を**図 11** に示す．図 11 の横軸は学習データ数を，縦軸は機械学習攻撃によって予測に成功したレスポンスや分散情報の割合を示している．図 11 に示すように，従来手法では 99%以上のレスポンスの予測に成功しており，チャレンジ・レスポンス認証は機械学習攻撃に対して脆弱であることが分かる．一方で提案手法は，(2, 3)-TSSS と (2, 3)-XOR-TSSS のどちらを用いた場合でも予測率が低下しており，機械学習攻撃への耐性が向上していることが確認できる．このとき，(2, 3)-TSSS の予測率が 70%であるのは，生成される分散情報の 0/1 の出現確率が 70%に偏っていたためである．すなわち，攻撃による予測結果がすべて同じ値（すべて 0 またはすべて 1）でも予測率は 70%となる．

ここで，PUF レスポンスは温度変化や電源電圧の変化な

どの環境変動によって最大でも 10%程度不安定なレスポンスが存在することが知られている [22]．そのため，認証システムではこの誤りを考慮した閾値の設定や，誤り訂正アルゴリズムによる修正が行われ，認証が実施される．したがって，攻撃者の観点からは 90%以上の予測率を達成できれば，認証システムを通過できると考えられる．提案手法の予測率は最大でも 70%であるため，上記の観点から機械学習攻撃に対して十分な攻撃耐性を持っており，有用性があると考えられる．

5. ハードウェア実装評価

ここでは，提案手法を Field Programmable Gate Array（FPGA）に実装し，そのハードウェア量について評価する．まず，5.1 節では実験環境について説明する．そして，5.2 節では提案手法の実装方法について述べる．最後に，5.3 節では実験結果について述べる．

5.1 実験環境

実験では，FPGA 評価ボードとして SASEBO-GII を使用し，Xilinx Virtex-5 XC5VLX30 に提案手法を実装した．また，比較対象として，対策 PUF である 2-XOR アービタ PUF も実装した．実験環境を**表 1** にまとめる．設計では Verilog HDL を用いて記述し，実装ツールには Xilinx ISE Design Suite 14.7 を使用した．

5.2 実装方法

提案手法の実装に関して，デバイス側での処理に必要な PUF 回路と分散処理を実装する．まず，(2, 3)-TSSS の実装について説明する．(2, 3)-TSSS の分散処理では，任意の x に対する y（$y = Res_{\mathrm{B}}x + Res_{\mathrm{A}}$）を計算する．このとき，$x$ を 2 に固定した場合，y はレスポンスのシフト演算と加算処理で計算できる．本研究で実装した加算回路を**図 12** に示す．図 12 の全加算器は a，b，c の 3 つの入力を持ち，a と b は加算する信号であり，PUF のレスポンス Res_{A} と Res_{B} に対応する．また，c は入力される桁上がり信号である．そして，各全加算器は加算した計算結果 S と桁上がり信号 co を出力する．

次に，(2, 3)-XOR-TSSS の実装では，分散情報 W_2 を生成する処理を実装した．本研究で実装した回路を**図 13** に示す．図 13 に示すように，XOR ゲートで実現することができ，2 種類の PUF レスポンスから分散情報 W_2 を生成する．

5.3 実験結果

回路規模の比較結果を**表 2** に示す．ここで実環境において，PUF には環境変動による不安定なレスポンスが生じる．このようなレスポンスの変動が生じる場合，提案手法で生成する分散情報は大きく変化する．そのため，提案手法での認証を行うためには，データベース側（サーバ側）とデバイス側（クライアント側）でレスポンスを完全に一致させる必要がある．PUF のレスポンスの誤り訂正では Fuzzy Extractor [23], [24] がよく用いられており，その有効性は実証されている [24]．そこで，本研究では文献 [24]

表 1 実験環境
Table 1 Experimental condition.

評価ボード	SASEBO-GII
FPGA	Xilinx Virtex-5 XC5VLX30
ハードウェア記述言語	Verilog HDL
実装ツール	Xilinx ISE Design Suite 14.7
フロアプラン	Xilinx PlanAhead v14.7
PUF のセレクタ段数	64

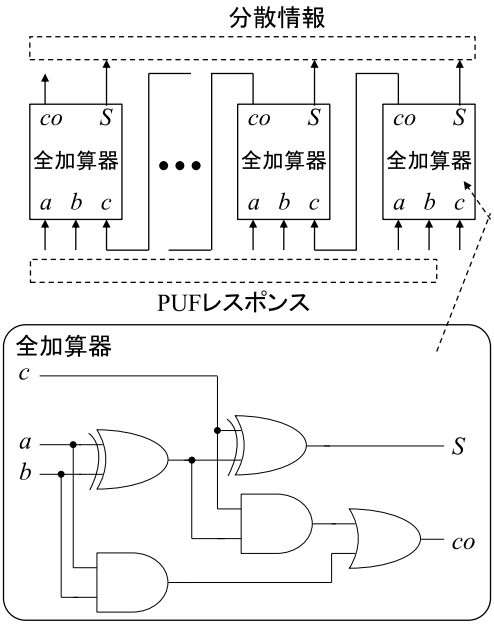


図 12 提案手法（(2, 3)-TSSS）の実装方法
Fig. 12 Implementation method of the proposed method using (2, 3)-TSSS.

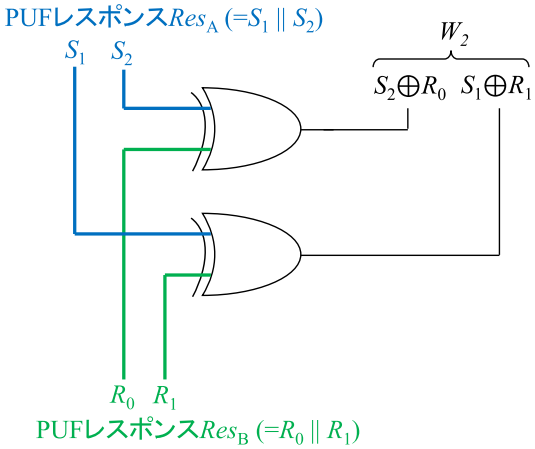


図 13 提案手法（(2, 3)-XOR-TSSS）の実装方法
Fig. 13 Implementation method of the proposed method using (2, 3)-XOR-TSSS.

表 3 各方式との比較結果
Table 3 Comparison result with conventional methods.

	提案手法	通常のチャレンジ・レスポンス認証	対策 PUF を用いたチャレンジ・レスポンス認証
機械学習攻撃耐性	○	×	○
回路規模	○	○	×

表 2 回路規模の比較結果
Table 2 Comparison result of circuit area.

		SLICE 数	レジスタ数
提案手法 ((2, 3)-TSSS)	PUF 回路	130	3
	加算回路	12	0
	周辺回路	33	97
	誤り訂正 [24]	112	—
	合計	287	100
提案手法 ((2, 3)-XOR-TSSS)	PUF	130	3
	周辺回路	37	97
	誤り訂正 [24]	112	—
	合計	279	100
従来手法 (対策 PUF によるチャレンジ・レスポンス認証)	PUF 回路	262	5
	周辺回路	32	97
	合計	294	102

の実装方式を用いることとする．具体的には，文献 [24] では BCH 符号を用いており，提案手法のデバイス側で必要な BCH 符号の復号処理の回路規模を参照した．回路規模には，FPGA のハードウェア量である SLICE 数で比較した．表 2 から，提案手法の SLICE 数は，(2, 3)-TSSS と (2, 3)-XOR-TSSS でそれぞれ，287，279 であることが分かる．一方で，対策 PUF（2-XOR アービタ PUF）の SLICE 数は 294 であり，提案手法は回路規模を削減できていることが確認できる．したがって，提案手法は対策 PUF を用いた方式よりも小回路規模での実装が可能である．

また，各実験結果について定性的にまとめた結果を**表 3** に示す．表 3 に示すように，提案手法は機械学習攻撃耐性と回路規模の両方において有効性があることが確認できる．

6. まとめ

本研究では，秘密分散法を利用した新たなセキュア PUF 認証方式を提案した．提案手法では，PUF のレスポンスを秘密分散法における秘密情報と見なして，分散情報を生成し，これを認証に利用する．提案手法では，レスポンスを直接やりとりする必要がなく，やりとりされる 1 つの分散情報だけでは，秘密分散法の性質によって秘密情報であるレスポンスを復元することができない．したがって，機械学習攻撃への耐性を向上させることができる．実際の機械学習攻撃による評価では，提案手法によって攻撃耐性を向上させることに成功した．また，ハードウェア実装評価では，FPGA に提案手法を実装して，従来の対策 PUF を用いたチャレンジ・レスポンス認証と比較した．実験結果から，提案手法は従来手法と比較して回路規模を削減し，小回路規模で実現できることを明らかにした．

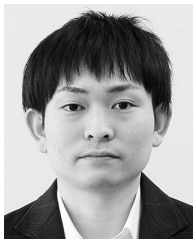
今後は，より詳細な性能評価を行っていく予定である．

謝辞 本研究の一部は，JSPS 科研費 19K24357 の助成を受けたものです．

参考文献

[1] Dey, K., Kule, M. and Rahaman, H.: PUF Based Hardware Security: A Review, *Proc. 4th International Symposium on Devices, Circuits and Systems* (*ISDCS*), pp.153–158, IEEE (2021).
[2] Lee, J.-W., Lim, D., Gassend, B., Suh, G.E., Dijk, M.V. and Debadas, S.: A Technique to Build a Secret Key in Integrated Circuits for Identification and Authentication Applications, *Proc. IEEE VLSI Circuits Symposium*, pp.176–179, IEEE (2004).
[3] Suh, G.E. and Devadas, S.: Physical Unclonable Functions for Device Authentication and Secret Key Generation, *Proc. 44th ACM/IEEE Design Automation Conference* (*DAC'07*), pp.9–14, IEEE (2007).
[4] Guajardo, J., Kumar, S.S., Schrijen, G.J. and Tuyls, P.: FPGA Intrinsic PUFs and Their Use for IP Protection, *Proc. 9th International Workshop on Cryptographic Hardware and Embedded Systems* (*CHES 2007*), LNCS 4272, pp.63–80, Spinger-Verlag (2007).
[5] Majzoobi, M., Koushanfar, F. and Potkonjak, M.: Testing Techniques for Hardware Security, *Proc. IEEE International Test Conference* (*ITC 2008*), pp.1–10, IEEE (2008).
[6] Majzoobi, M., Koushanfar, F. and Potkonjak, M.: Lightweight Secure PUFs, *Proc. IEEE/ACM International Conference on Computer Aided Design* (*ICCAD*), pp.670–673, IEEE (2008).
[7] Machida, T., Yamamoto, D., Iwamoto, M. and Sakiyama, K.: A New Mode of Operation for Arbiter PUF to Improve Uniqueness on FPGA, *Proc. 2014 Federated Conference on Computer Science and Information Systems* (*FedCSIS*), Vol.2, pp.871–878, IEEE (2014).
[8] Lim, D.: Extracting Secret Keys from Integrated Circuits, M.S. Thesis, MIT (2004).
[9] Rührmair, U., Sölter, J., Sehnke, F., Xu, X., Mahmoud, A., Stoyanova, V., Dror, G., Schmidhuber, J., Burleson, W. and Devadas, S.: PUF Modeling Attacks on Simulated and Silicon Data, *IEEE Trans. Information Forensics and Security*, Vol.8, No.11, pp.1876–1891 (2013).
[10] Alkatheiri, M.S. and Zhuang, Y.: Towards Fast and Accurate Machine Learning Attacks of Feed-Forward Arbiter PUFs, *Proc. IEEE Conference on Dependable and Secure Computing*, pp.181–187, IEEE (2017)
[11] Ikezaki, Y., Nozaki, Y. and Yoshikawa, M.: Deep learning attack for physical unclonable function, *Proc. IEEE 5th Global Conference on Consumer Electronics* (*GCCE 2016*), pp.457–458, IEEE (2016).

[12] Yashiro, R., Machida, T., Iwamoto, M. and Sakiyama, K.: Deep-Learning-Based Security Evaluation on Authentication Systems Using Arbiter PUF and Its Variants, *Proc. 11th International Workshop on Security* (*IWSEC 2016*), LNCS 9836, pp.267–285, Springer (2016).
[13] 飯塚知希，粟野皓光，池田 誠：深層ニューラルネットワークを用いた Double-Arbiter PUF に対するモデリング攻撃，電子情報通信学会技術研究報告，IEICE-VLD, Vol.117, No.455, pp.231–236 (2018).
[14] Shamir, A.: How to share a secret, *Comm. ACM*, Vol.22, No.11, pp.612–613 (1979).
[15] 保坂範和，多田美奈子，加藤岳久：秘密分散法とその応用，東芝レビュー，Vol.62，No.7，pp.23–26 (2007).
[16] 須賀祐治：XOR 演算ベースの閾値秘密分散法から秘密計算法を構成する試み，情報処理学会研究報告，IPSJ-IOT, Vol.29, No.11, pp.1–7 (2015).
[17] Aman, M.N., Chua, K.C. and Sikdar, B.: Mutual Authentication in IoT Systems using Physical Unclonable Functions, *IEEE Internet of Things Journal*, Vol.4, No.5, pp.1327–1340 (2017).
[18] Braeken, A.: PUF Based Authentication Protocol for IoT, *Symmetry 2018*, Vol.10, No.8, pp.1–15 (2018).
[19] Khoshroo, S.: Design and Evaluation of FPGA-based Hybrid Physically Unclonable, M.S. thesis, The University of Western Ontaio (2013).
[20] Naveen, D. and Praveen, K.: PUF Authentication using Visual Secret Sharing Scheme, *Proc. 5th International Conference on Advanced Computing & Communication Systems* (*ICACCS*), pp.472–475, IEEE (2019).
[21] Ebrahimabadi, M., Younis, M. and Karimi, N.: A PUF-Based Modeling-Attack Resilient Authentication Protocol for IoT Devices, *IEEE Internet of Things Journal*, pp.1–19, IEEE (2021).
[22] 福島照理，汐崎 充，古橋康太，村山貴彦，藤野 毅：アービター PUF で生成した固有 ID の環境安定性の実チップ評価，2011 年暗号と情報セキュリティシンポジウム講演論文集，2D2-2, pp.1–7 (2011).
[23] Dodis, Y., Reyzin, L. and Smith, A.: Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data, *Proc. EUROCRYPT 2004*, LNCS 3027, pp.523–540, Springer-Verlag (2004).
[24] Maes, R., Herrewege, A.V. and Verbauwhede, I.: PUFKY: A Fully Functional PUF-Based Cryptographic Key Generator, *Proc. 14th International Workshop on Cryptographic Hardware and Embedded Systems* (*CHES 2012*), LNCS 7428, pp.302–319, Springer-Verlag (2012).
[25] Nozaki, Y. and Yoshikawa, M.: Secret Sharing Schemes Based Secure Authentication for Physical Unclonable Function, *Proc. IEEE 4th International Conference on Computer and Communication Systems* (*ICCCS 2019*), pp.445–449, IEEE (2019).



野崎 佑典 （正会員）

2019 年 3 月名城大学大学院理工学研究科電気電子・情報・材料工学専攻博士後期課程修了．博士（工学）．2019 年 4 月より同大学理工学部特任助手，2020 年 4 月より同大学理工学部情報工学科助教．2017 年 4 月～2019 年 3 月まで日本学術振興会特別研究員（DC2）．暗号 LSI のセキュリティに関する研究に従事．IEEE CEDA AJJC Academic Research Award 2018 など受賞．電子情報通信学会，日本知能情報ファジィ学会，IEEE 各会員．

吉川 雅弥 （正会員）

2001 年 3 月立命館大学大学院理工学研究科博士課程修了．博士（工学）．同大学理工学部第 1 号助手・講師を経て，2007 年 4 月より名城大学理工学部准教授，2012 年 4 月より教授．2009 年～2015 年 CREST 研究員．LSI 設計・設計自動化技術の研究に従事．第 3 回 LSI IP デザインアワード開発奨励賞，第 10 回 LSI IP デザインアワード研究助成賞，FIT2003 ベストペーパー賞，2007 年度システム制御情報学会産業技術賞，CAINE2010 Best Paper Award，WCECS2011 Best Paper Award 等受賞．電気学会，電子情報通信学会，システム制御情報学会，日本知能情報ファジィ学会，IEEE 各会員．