

メモリスタを用いた等価な応答を返す PUF 対の検討

田中 悠貴^{1,a)} 辺 松¹ 廣本 正之¹ 佐藤 高史¹

概要: 近年, 半導体の製造ばらつきを用いてチップの個体識別を行う Physically Unclonable Function (PUF) の研究が活発に行なわれている. 既存の PUF 認証方式には認証側で Challenge Response Pair (CRP) を記録しなければならない課題があった. 本研究では, 等価な応答を返す PUF 対を提案することで, CRP を記録する必要のない認証を実現する. 提案 PUF 対は製造時に同時に二つ製造され, それぞれ等価な CRP を持つ PUF である. 解析により PUF の評価指標とともに CRP の一致率が 1.0 となり, 提案 PUF 対で CRP を記録する必要のない認証を実現可能であることを確認する.

A Study on Memristor-based PUFs with Paired Responses

YUKI TANAKA^{1,a)} SONG BIAN¹ MASAYUKI HIROMOTO¹ TAKASHI SATO¹

Abstract: While numerous physically unclonable functions (PUFs) were proposed in recent years, the basic PUF usage model remained the same. In the general PUF setting, a server pre-records a certain set of challenge-response pairs (CPRs), and sends out some of the challenges in the set for chip authorization. In contrast, in this work, we propose a paired memristor-based PUFs architecture where the server needs not to pre-record CRPs. Instead, the proposed architecture consists of a pair of PUFs manufactured to return identical responses upon receiving the same challenges. Therefore, the server can just keep one of the paired PUFs for future authorization, instead of pre-recording a large database, or peer-to-peer authorizations become possible. In the experiment, SPICE simulation shows that the matching rate of CRPs between the proposed paired PUFs is 1.0, promising the possibility of a new PUF-based authentication paradigm.

1. はじめに

近年, ハードウェアセキュリティの分野では PUF (Physically Unclonable Function) [1, 2] の研究が盛んである. PUF はあるチャレンジ (入力値, c) を与えると, 対応するレスポンス (出力値, r) を返す関数 $r = f_\alpha(c)$ として機能する回路である. ただし, チャレンジとレスポンスの対応 (CRP: challenge response pair) は物理的なばらつき α に依存して決まるため, 同じチャレンジに対するレスポンスはチップごとに異なり, 人工的な複製が困難となる. そのため PUF は個体認証や暗号プロトコルにおける使用 [3–6], 更には小規模な回路で実現可能である特徴から IoT デバイスのセキュリティ等 [7], 様々なセキュリティシステムでの応用が期待されている.

また, PUF には回路方式によって様々な種類があり, 代表的なものには SRAM PUF [8], Arbiter PUF [1], Ring

Oscillator PUF [2], BR-PUF (Bistable Ring PUF) [9] 等が存在する. これらの PUF を評価する主な指標として, 再現性と一意性がある. 再現性は同じ PUF に対して同じチャレンジを与えた場合に, 常に同じレスポンスを返す性質である. 一意性は異なる PUF に同じチャレンジを与えた場合に, それぞれ異なるレスポンスを返す性質である. これらの指標が優れるほど, 優れた PUF と言える.

また, PUF には大きく分けて Weak PUF と Strong PUF の二種類が存在する [10, 11]. Weak PUF は CRP が回路規模に対して線形にしか増えないため CRP 空間が小さいのに対し, Strong PUF は攻撃者が全ての CRP を取得できないほどの大きな CRP 空間を有する. そのため, セキュリティシステムで用いる場合に Weak PUF と Strong PUF で使用の仕方が異なる. 以下で, チップ認証を例にそれぞれの PUF の使用手法について説明する.

まず, Weak PUF を用いてチップ認証を行う際には, CRP を秘密鍵として使い, 一般的な暗号アルゴリズムと組み合わせる [10, 12]. 一般的な暗号アルゴリズムでは, ま

¹ 京都大学 大学院情報学専攻 通信情報システム専攻
〒 606-8501 京都府京都市左京区吉田本町

^{a)} paper@easter.kuee.kyoto-u.ac.jp

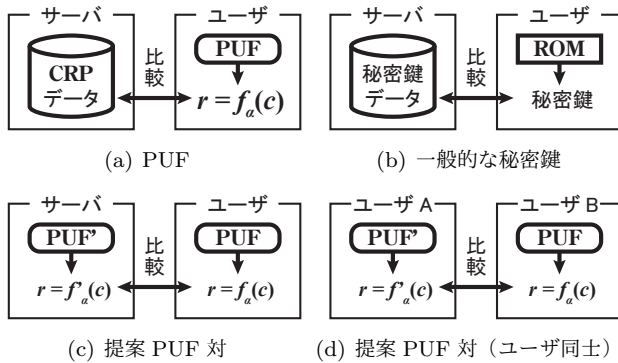


図 1 認証方式の概要

チップ製造者が製造したチップの ROM に秘密鍵を書き込むが、Weak PUF を用いる場合には製造したチップに搭載されている PUF について、CRP を調べ秘密鍵として記録する。次にチップ購入者がチップの認証を行うとき、製造者に認証の要求を行う。製造者は乱数を生成しチャレンジとしてチップに送信する。チップはチャレンジに対し、PUF のレスポンスを用いて署名演算を行い署名データを製造者にレスポンスとして返す。最後に製造者は署名データを分析し、チップの PUF が記録していた秘密鍵を保持していることが確認出来れば正規品と判定する。

次に、Strong PUF を用いてチップ認証を行う際には、Weak PUF と同様にまずチップ製造者は製造したチップに搭載されている PUF について、認証を行う回数と等しいかそれよりも十分大きい回数分の CRP を調べ記録し、CRP データベースを作成する。次にチップ購入者がチップの認証を行う時、製造者に認証の要求を行う。製造者は作成したデータベースからあるチャレンジ c を PUF に送信する。PUF は受け取ったチャレンジ c から、製造者にレスポンス r を返す。最後に製造者は受け取ったレスポンス r とデータベース内の r' を照合し、一致すれば正規品と判定する。

いずれの認証方式も基本は図 1(a) のようにサーバの CRP データとユーザの PUF のレスポンスを比較することで認証を行う。この認証方式ではユーザが PUF を所有し、サーバが PUF の CRP をデータとして保存する必要がある。しかし、サーバにおける CRP データの保存には、CRP を読み出す面でも、保持する面でもコストがかかる問題がある。さらに Strong PUF を用いる場合には認証回数分の CRP を保存する必要がある、図 1(b) のような ROM から読み出される秘密鍵とサーバの秘密鍵を比較する一般的な認証方法に比べ、サーバに保存すべきデータ量が大きい問題も生じる。加えて、サーバに完全に悪意がないことを保証する必要もある。

本稿における研究の目的は、等価な応答を返す PUF 対を用いた、CRP データを保存する必要のない PUF 対認証方式を提案することである。提案する PUF 対認証方式の概要を図 1(c) と図 1(d) に示す。PUF 対認証方式では図 1(c) のように、サーバがユーザの PUF と対になる PUF' を所有し PUF と PUF' のレスポンスを比較する。または図 1(d) のように、サーバを介することなく PUF 対を持つユーザ

間で直接の認証を可能とする。等価な応答を返す PUF 対は、製造時に二つ同時に対として製造されそれぞれの PUF が等価な CRP を持つ。本稿ではメモリスタを用いた PUF 対を提案する。提案 PUF 対は、1 対のメモリスタ回路にストレス電圧を与えることで、対を成すメモリスタ間にある既知の関係を持たせる。例えば、対を成すメモリスタ間に正または負の極めて強い相関をもたせる。個々のメモリスタの抵抗状態は、メモリスタ回路またはその周辺回路の物理的なばらつきで異なるため、PUF のレスポンスとして用いることができる。対を成すメモリスタ回路を切り離すことにより、二つの PUF を等価な応答（同一応答か、または互いに反転する応答）を返す PUF 対として用いることができる。本稿では、回路シミュレーションにより提案 PUF 対におけるレスポンスの一致率と一意性、再現性を評価する。

以下に本稿の構成を示す。まず、第 2 章で PUF 対を用いた認証方式を提案する。次に第 3 章でメモリスタを用いた PUF 対を提案し、第 4 章で提案 PUF 対におけるレスポンスの一致率と一意性、再現性の評価を回路シミュレーションを用いて行う。最後に第 5 章で本稿をまとめる。

2. 提案認証方式

まず CRP データを保存する必要のない PUF 対認証方式を提案する。次に等価な応答を返す PUF 対を用いた PUF 対認証方式について検討する。

2.1 PUF 対認証方式

関数 $r = f_\alpha(c)$ として機能する PUF と、 $r = f'_\alpha(c)$ として機能し PUF と対をなす PUF' があり、またすべてのチャレンジ c に対し、 $g(f_\alpha(c), f'_\alpha(c)) = \text{const.}$ が成立する関数 g があるとする。このとき図 1(c) や図 1(d) のように PUF と PUF' の比較により認証が可能となるため、図 2 のような PUF 対認証方式が考えられる。以下で PUF 対認証方式の詳しい認証手法を述べる。

認証を行う際には、まず認証側がユーザの PUF と対をなす PUF' を所有する。次にユーザがチップの認証を行うとき、認証側に認証の要求を行う。認証側は乱数生成器等を用いてチャレンジ c を生成し、ユーザに送信する。ユーザは受け取ったチャレンジ c から、PUF を用いてレスポンス r を生成し認証側に返す。最後に製造者は受け取ったレスポンス r と PUF' にチャレンジ c を与えたときの r' を用いて $g(r, r')$ を算出し、期待値に等しければ認証通過となる。PUF 対認証方式であれば、CRP データを保持することなく $r = f'_\alpha(c)$ として機能する PUF' と関数 g を保持することで認証可能となる。

PUF 対認証方式における PUF と対をなす PUF' を製造する手法として、大きく二つ考えられる。一つ目が、図 3(a) のように乱数生成器のエントロピーから f_α と f'_α を生成し、それぞれの関数を PUF と PUF' の物理的なばらつきに変換する手法である。二つ目が、図 3(b) のようにチップの物理的なばらつきから f_α と f'_α を生成し、それぞれの関

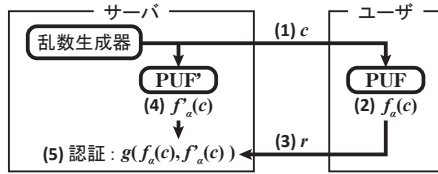
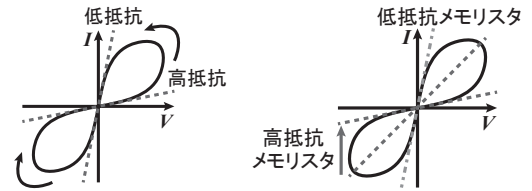
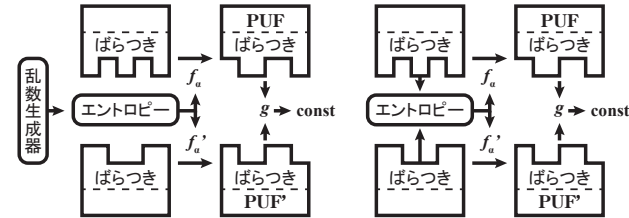


図2 CRPデータの不要なPUF対認証方式



(a) 一般的な特性 (b) 提案PUF対における特性

図4 メモリスタの特性



(a) 乱数生成器のエントロピーを使用 (b) チップのばらつきを使用

図3 提案認証方式を実現するPUFの製造手法

数をPUFとPUF'の物理的ばらつきに変換する手法である。乱数生成器を用いた場合、攻撃者が生成した乱数を取り得しPUF認証を破られる可能性があるため、チップのばらつきを用いてPUFを生成する手法の方が安全であると考えられる。次節では等価な応答を返すPUF対を用いたCRPデータの不要なPUF対認証方式を提案する。

2.2 等価な応答を返すPUF対を用いた認証方式

ここでは、等価な応答を返すPUF対を用いて実現するPUF対認証方式を提案する。等価な応答を返すPUF対とは同じチャレンジに対して等価なレスポンスを返すPUFとPUF'の対である。そのため、PUF'を表す関数 $f'_a(c)$ は $f'_a(c) = f_a(c)$ で表され、認証の際にはPUFとPUF'のそれぞれのレスポンス r と r' が一致しているか確認し、一致すれば正規品と判定する。次章では、図3(b)のようにチップの製造ばらつきから f_a と f'_a を生成する、メモリスタを用いた等価な応答を返すPUF対を提案する。

3. メモリスタを用いたPUF対

3.1 メモリスタ

メモリスタは通過した電荷を抵抗値として記憶する素子として1970年代にChuaによってその存在が理論的に予想され、2008年にStrukovらによって発見された[13, 14]。このデバイスは二種類の金属によって酸化金属を挟み込んだ構造をしている。メモリスタの特徴的な点として図4(a)に示すバタフライ状のI-V特性のヒステリシスが挙げられる。メモリスタに正方向のストレスをかけると低抵抗状態に、逆方向のストレスをかけると高抵抗状態になる。メモリスタがこのような特性を示す理由は完全には解明されていないが、デバイス内部の酸素イオン欠損がデバイス内で高抵抗と低抵抗の二種類の領域を生み出し、内部電流によってその境界が移動するためであると考えられている[13]。

メモリスタに対しパルス波形を印加し、その振幅の大小

で読み出しと書き込みを切り替える。読み出し電圧を V_r 、書き込み電圧を V_w とするとメモリスタの回路方程式は、メモリスタの抵抗値 R 、電圧印加時間 T 、適当な定数 α を用いると以下のように近似できる[15]。

$$\text{読み出し: } I = RV_r \quad (1)$$

$$\text{書き込み: } \Delta R \propto RT \exp(\alpha V_w) \quad (2)$$

読み出し時は線形性が成り立つとみなすことができる。一方で、書き込み時は抵抗変化が電圧に対し指数的に増大し、抵抗値の増加量はその時の抵抗値に相関がある。

メモリスタの抵抗値を書き込むことができる特性を利用し、次節ではメモリスタを用いたPUF対を提案する。

3.2 提案PUF対のメモリスタ対の基本構成

メモリスタが通過した電荷を抵抗値として記憶可能である点を利用し、メモリスタに抵抗値を書き込むことでPUF対を実現する。提案PUF対は製造時、対を成す二つのメモリスタをもつ回路である。ここでは、回路全体にストレスをかけることで、一方のメモリスタにのみ逆方向のストレスがかかり高抵抗状態となる回路を例に説明する。以下でNMOSを用いたPUF対とPMOSを用いたPUF対の二種類のPUF対を提案し、製造時のストレス状態について詳しく説明する。

まず、NMOSトランジスタを用いた提案PUF対の製造時の回路構造を図5(a)に示す。左右のメモリスタの初期抵抗値をそれぞれ R_l と R_r とする。 $R_l > R_r$ のとき、 V_{dd} を低電圧から高電圧に上げることでストレスをかければ図5(b)のように R_l が接続されているトランジスタのみがオン状態となり、 R_l にのみストレスがかかる。 $R_r > R_l$ のときも同様に高抵抗のメモリスタ R_r にのみストレスがかかる。

次にPMOSトランジスタを用いた提案PUF対の製造時の回路構造を図6(a)に示す。NMOSトランジスタを用いたPUF対と同様に、 $R_l > R_r$ のとき、 V_{ss} を高電圧から低電圧に下げることでストレスをかければ図6(b)のように R_l が接続されているトランジスタのみがオン状態となり、 R_l にのみストレスがかかる。 $R_r > R_l$ のときも同様である。

以上、いずれの回路においても、対となるメモリスタのうち抵抗値の高いメモリスタにのみストレスがかかり、図4(b)のようにそのメモリスタのみ抵抗値が上昇する。ストレスをかけた後、図7のように二つのメモリスタを切り離し、それぞれのメモリスタをPUFとそれに対応するPUF'

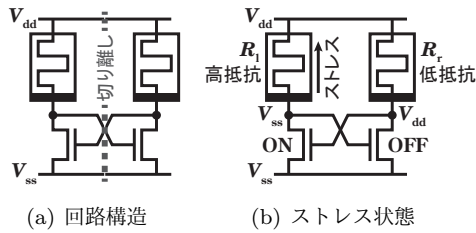


図 5 NMOS を用いた提案 PUF 対

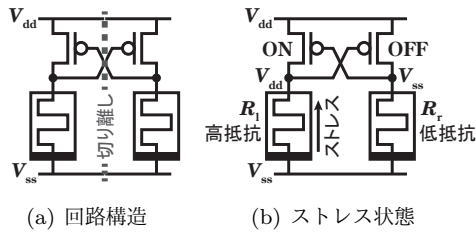


図 6 PMOS を用いた提案 PUF 対

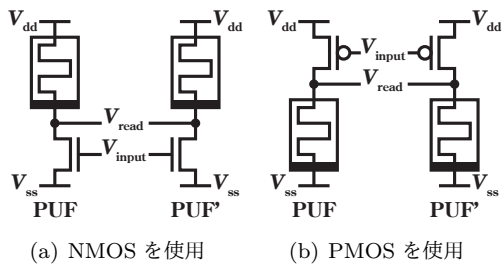


図 7 提案 PUF 対の読み出し回路構造

とする。PUF と PUF' のレスポンスはメモリスタの抵抗値から生成し、高抵抗状態であれば 1、初期状態のままであれば 0 とする。上の書き込み動作から、PUF と PUF' のレスポンスは常に反転関係にある。よって PUF と PUF' は等価な応答を返す PUF 対となる。

メモリスタの抵抗値は、 V_{read} の電圧を読み取ることで読み出す。ソースドレイン間の抵抗値を r_d 、読み込み状態のメモリスタの抵抗値を R 、電源電圧を V_{dd} とする。このとき V_{read} は

$$\text{NMOS を使用: } V_{read} = \frac{r_d}{r_d + R} V_{dd} = \frac{1}{1 + R/r_d} V_{dd} \quad (3)$$

$$\text{PMOS を使用: } V_{read} = \frac{R}{r_d + R} V_{dd} = \frac{1}{1 + r_d/R} V_{dd} \quad (4)$$

で表される。メモリスタが高抵抗状態のときの V_{read} と初期状態のときの V_{read} に十分な差が検出できるように V_{input} を入力すれば、レスポンスが生成可能となる。

3.3 提案 PUF 対のアレイ回路の構成

NMOS を用いた提案 PUF 対において、複数のレスポンスを生成するためのアレイ回路とアレイ回路として構成する際のセル (1 ビット分) の回路構造を、それぞれ図 8 と図 9(a) に示す。アレイ回路では図 7 の読み出し回路をアレイ状に配置する。同じ行で V_{dd} を V_{rn} として共有し、同じ列では V_{read} と V_{input} をそれぞれ V_{xm} と V_{ym} として共有する。ただし、 V_{read} と V_{xm} 、 V_{input} と V_{ym} は NMOS トランジスタによるスイッチを接続し、セルを選択しているときのみ接続する。NMOS トランジスタのゲートは同じ行で V_{sn} として共有する。 V_{RESET} は書き込み前に V_{xm} と

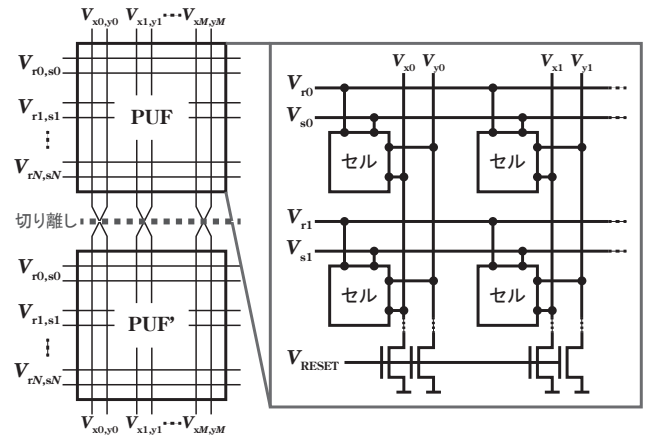


図 8 NMOS トランジスタを用いた提案 PUF 対のアレイ回路

V_{ym} を V_{ss} とする信号である。

値の書き込みは次のように行う。まず、PUF の V_{xm} と PUF' の V_{ym} 、PUF の V_{ym} と PUF' の V_{xm} をそれぞれ接続した状態で製造する。次に、行ごとにストレスをかけメモリスタの抵抗値を書き込む。ストレスをかける際、 V_{RESET} を一度 V_{dd} に引き上げ、 V_{xm} と V_{ym} を V_{ss} に落とす。その後 V_{RESET} を再度 V_{ss} に落とし、書き込みたい行の PUF と PUF' の V_{xm} と V_{ym} にストレスを一定時間かける。以上の書き込みをすべての行に対して行い、最後に PUF と PUF' を V_{ym} と V_{xm} とで切り離す。

PUF と PUF' を読み出す際も、行単位でレスポンスを生成する。読み出したい行の V_{rn} と V_{sn} を V_{dd} に引き上げ、すべての列の V_{ym} に適切な電圧を与え、 V_{xm} の電圧値を読み取る。一定の電圧より高ければレスポンスを 1、低ければ 0 とする。

また PMOS を用いた提案 PUF 対のアレイ回路は、ストレス時に V_{ss} を高電圧から低電圧に引き下げるため、図 9(b) のようにセル回路における V_{ss} を V_{rn} として同じ行で共有し、行ごとに書き込みを行う。 V_{read} と V_{xm} 、 V_{input} と V_{ym} のスイッチには PMOS トランジスタを用いる。また、 V_{xm} と V_{ym} を V_{dd} に引き上げ RESET を行うため、図 8 の V_{RESET} における NMOS トランジスタには PMOS トランジスタを用いる。

4. 評価

提案 PUF 対について、PUF と PUF' のレスポンスの一致率と、PUF の一般的な指標である一意性と再現性を回路シミュレーションによって評価する。

メモリスタのモデルには Verilog-A によるビヘイビアモデルを用いる [16]。このモデルでは I-V 特性を決める状態量としてギャップ g を用いており、これはメモリスタ内部の高抵抗領域の長さを示すものと定義されている。メモリスタのギャップ初期値 g_{ini} には正規分布のばらつきを与えた。また、MOSFET には商用 65 nm プロセスのモデルを用い、正規分布のしきい値電圧ばらつきを与えた。

まず、3.2 節の NMOS を用いた PUF 対と PMOS を用いた PUF 対について、それぞれ 10,000 個の PUF と PUF'

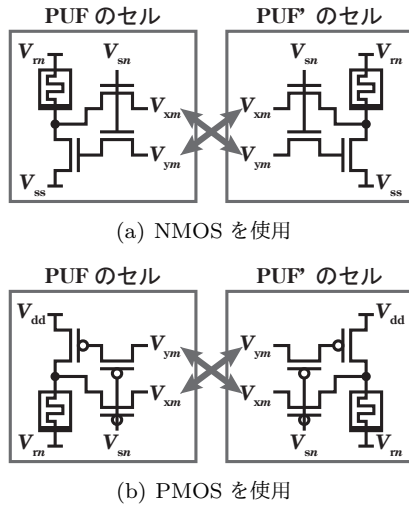


図 9 提案 PUF 対アレイ回路におけるセルの回路構造

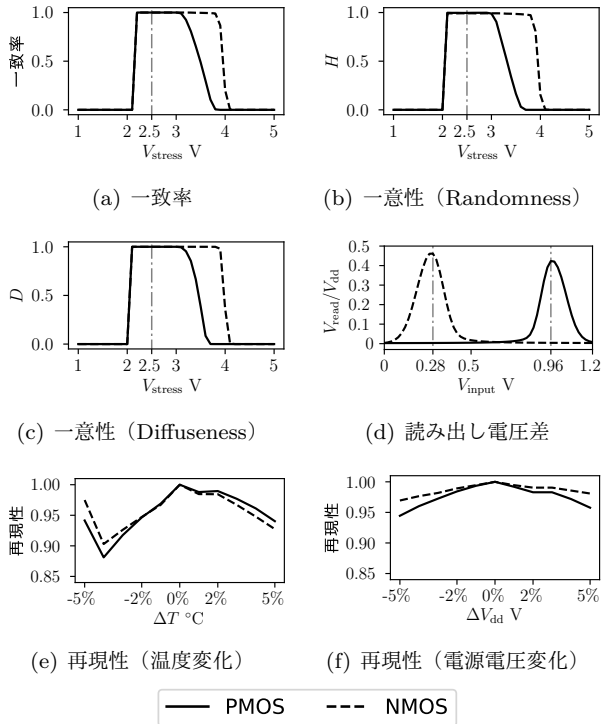


図 10 提案 PUF 対の評価

の対をランダムに生成し、レスポンスの一致率、一意性、再現性の指標を評価する。次に、3.3 節のアレイ回路についても、NMOS, PMOS を用いた PUF 対について、それぞれ $N = 8, M = 8$ の 16 個のアレイ回路をランダムに生成し、レスポンスの一致率、一意性の指標を評価する。

4.1 レスポンスの一致率

PUF' のレスポンスを反転させたときに PUF のレスポンスと一致する割合を一致率として評価する。図 5 の NMOS を用いた PUF 対と図 6 の PMOS を用いた PUF 対について、それぞれストレスをかけ、メモリスタの抵抗値 R が $R > 3.35 \times 10^6 \Omega$ となった PUF と PUF' のレスポンスを 1, $R \leq 3.35 \times 10^6 \Omega$ となった PUF と PUF' のレスポンス

を 0 とし評価を行った。ストレス電圧 V_{stress} を変化させたときの一致率の結果を図 10(a) に示す。いずれの回路構造であっても、 $V_{\text{tress}} = 2.5 \text{ V}$ 前後の適切なストレス電圧を与えることで一致率を 1.0 にできることが分かる。

4.2 一意性

一意性は、異なる PUF に同じチャレンジを与えた時にそれぞれが異なるレスポンスを返す性質であり、Hori ら [17] による 3 つの評価指標 Randomness (H), Diffuseness (D) により評価を行った。それぞれの指標は以下の式で算出でき、いずれも 1 に近いほど良い。

$$H = -\log_2 \left(\frac{1}{2} + \left| \frac{1}{C} \sum_{c=1}^C r_c - \frac{1}{2} \right| \right) \quad (5)$$

$$D = \frac{4}{C^2} \sum_{c=1}^{C-1} \sum_{c'=c+1}^C (r_c \oplus r_{c'}) \quad (6)$$

ただし、 r_c は PUF にチャレンジ c を与えた時に得られたレスポンスであり、 C は c の最大数である。

提案回路については、どのメモリスタを選択するかをチャレンジとし評価を行った。それぞれの結果を図 10(b) と図 10(c) に示す。レスポンスの一致率と同様に $V_{\text{stress}} = 2.5 \text{ V}$ 前後の適切なストレス電圧を与えることで、 H, D ともに 1.0 にできることが分かる。

4.3 読み出し時の入力電圧

メモリスタに抵抗値を書き込み PUF と PUF' を生成した後、レスポンスを生成する際に図 7 の読み出し回路において V_{input} に入力する適切な電圧を評価する。書き込み時のストレス電圧を $V_{\text{stress}} = 2.5 \text{ V}$ として書き込みを行った後、 V_{input} の電圧を変化させて V_{read} を読み出した時の、高抵抗状態の $V_{\text{read,high}}$ と低抵抗状態の $V_{\text{read,low}}$ の差の平均値について評価を行った。なお、読み出し時には $V_{\text{dd}} = 1.2 \text{ V}$ とした。結果を図 10(d) に示す。NMOS を用いた場合には $V_{\text{input}} = 0.28 \text{ V}$ 、PMOS を用いた場合には $V_{\text{input}} = 0.96 \text{ V}$ であれば大きな電圧差が読み取れ、レスポンスが生成できることが分かる。

4.4 再現性

再現性は、同じ PUF に同じチャレンジを与えると常に同じレスポンスを返すという性質であり、Steadiness と Correctness という 2 つの指標で評価される [17]。これらは一般に実際に製造した PUF に対し、同じチャレンジに対するレスポンスを繰り返し生成することで評価する。本稿ではシミュレーションにより評価を行うため、これら 2 つについては扱わず、環境温度と電源電圧を変化させたときのレスポンスについて再現性を評価した。

$V_{\text{stress}} = 2.5 \text{ V}$ としてメモリスタに書き込みを行った後、4.3 節から得られた入力電圧を V_{input} に入力しレスポンスを生成する。測定温度が 25°C 、電源電圧 $V_{\text{dd}} = 1.2 \text{ V}$ のときのレスポンスの一致率が 0.92% であったため、レスポンスが一致した PUF と PUF' についてのみ測定温度を -5%

表 1 アレイ回路の一致率と一意性

アレイ回路	一致率	R	D
NMOS を使用	0.84	0.93	1.00
PMOS を使用	0.88	1.00	1.00

から +5% まで、電源電圧を -5% から +5% まで変化させ、レスポンスが変化しない割合を評価した。それぞれの結果を図 10(e) と図 10(f) に示す。電源電圧変化に比べ、温度変化に対する再現性が悪いものの、0.9 程度の再現性が得られた。

4.5 提案 PUF 対のアレイ回路の一致率と一意性

提案 PUF 対のアレイ回路のレスポンスについても、一致率と一意性を評価した。書き込み時のストレス電圧は $V_{\text{stress}} = 2.5 \text{ V}$ とした。また読み出し時には、電源電圧に $V_{\text{dd}} = 1.2 \text{ V}$ を、読み出し電圧 V_{ym} には 4.3 節で得られた入力電圧を入力した。レスポンスの一致率と、一致したレスポンスについて一意性を評価した結果を表 1 に示す。一意性については 1.00 に近い十分な値がとれていることが分かる。単体回路に比べて一致率は低下したが、これはアレイ回路にしたために出力電圧が低下したことが原因と考えられる。

5. まとめ

本稿では、PUF を用いた認証において、サーバが CRP データを保存する必要のない PUF 対認証方式を新たに提案した。また、抵抗値を記録可能な素子であるメモリストアを用いた PUF 対の実現方法とそのアレイ回路を提案した。提案 PUF 対は二つのメモリストアの対であり、ストレス電圧を印加することにより一方のメモリストアが他方に対し高抵抗の状態となる。従ってメモリストアの抵抗値状態をレスポンスとして用いれば、等価な応答を返す PUF 対となる。

回路シミュレーションにより提案 PUF 対の性能を評価した結果、適切なストレス電圧をかけることで PUF 対のレスポンスの一致率は 1.0 となり、十分な一意性と再現性も得られた。また、適切な入力電圧を与えることで、メモリストアの抵抗状態も読み取れることが分かった。さらに、提案 PUF 対のアレイ回路についても同様に評価を行い、十分な一致率と一意性が得られることを確認した。

謝辞 本研究は一部、JSPS 科研費 17H01713 の助成を受けた。また、本研究は東京大学大規模集積システム設計教育研究センターを通し、日本シノプシス合同会社の協力で行われたものである。

参考文献

- [1] B. Gassend, D. Clarke, M. van Dijk, and S. Devadas, "Silicon physical random functions," in *Proc. Computer and Communication Security Conf.*, 2002, pp. 148–160.
- [2] G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in *Proc. DAC*, 2007, pp. 9–14.
- [3] A. Stanciu, M. N. Cirstea, and F. D. Moldoveanu, "Analysis and evaluation of PUF-based SoC designs

- for security applications," *IEEE Trans. Ind. Electron.*, vol. 63, no. 9, pp. 5699–5708, Sept 2016.
- [4] C. Brzuska, M. Fischlin, H. Schröder, and S. Katzenbeisser, "Physically uncloneable functions in the universal composition framework," in *Proc. CRYPTO*, 2011, pp. 51–70.
- [5] R. Ostrovsky, A. Scafuro, I. Visconti, and A. Wadia, "Universally composable secure computation with (malicious) physically uncloneable functions," in *Proc. EUROCRYPT*, 2013, pp. 702–718.
- [6] U. U. Rührmair and M. van Dijk, "PUFs in security protocols: Attack models and security evaluations," in *Proc. IEEE Symp. Security and Privacy*, 2013, pp. 286–300.
- [7] A. P. Johnson, R. S. Chakraborty, and D. Mukhopadhyay, "A PUF-enabled secure architecture for FPGA-based IoT applications," *IEEE Trans. Multi-Scale Comput. Syst.*, vol. 1, no. 2, pp. 110–122, 2015.
- [8] G. S. J. Guajardo, S. Kumar and P. Tuyls, "FPGA intrinsic PUFs and their use for IP protection," in *Proc. Cryptographic Hardware and Embedded Systems*, pp. 63–80, 2007.
- [9] Q. Chen, G. Csaba, P. Lugli, U. Schlichtmann, and U. Rührmair, "The bistable ring PUF: A new architecture for strong physical unclonable functions," in *Proc. Int'l Symp. Hardware-Oriented Security and Trust*, 2011, pp. 134–141.
- [10] U. Rührmair, S. Devadas, and F. Koushanfar, *Security Based on Physical Unclonability and Disorder*. Springer New York, 2011, ch. 4, pp. 65–102.
- [11] C. Herder, M. D. Yu, F. Koushanfar, and S. Devadas, "Physical unclonable functions and applications: A tutorial," *Proc. IEEE*, vol. 102, no. 8, pp. 1126–1141, 2014.
- [12] B. Gassend, "Physical random functions," *Master's Thesis*, 2003.
- [13] D. B. Strukov, G. S. Snider, D. R. Stewart, and R. S. Williams, "The missing memristor found," *Nature*, vol. 453, no. 7191, pp. 80–83, 2008.
- [14] L. O. Chua, "Memristor—the missing circuit element," vol. 18, no. 5, pp. 507–519, 1971.
- [15] F. M. Bayat, B. Hoskins, and D. B. Strukov, "Phenomenological modeling of memristive devices," *Applied Physics A*, vol. 118, pp. 779–786, 2015.
- [16] P. Y. Chen and S. Yu, "Compact modeling of RRAM devices and its applications in 1T1R and 1S1R array design," vol. 62, no. 12, pp. 4022–4028, 2015.
- [17] Y. Hori, T. Yoshida, T. Katashita, and A. Satoh, "Quantitative and statistical performance evaluation of arbiter physical unclonable functions on FPGAs," in *Proc. Int'l Conf. Reconfigurable Computing*, 2010, pp. 298–303.