

チャレンジヒステリシス特性を有する PUF の設計とシミュレーションに基づく性能評価

粟野 皓光^{1,a)} 佐藤 高史²

概要: チャレンジヒステリシス特性を有する PUF の設計コンセプトを提案する。提案 PUF は格子状に配置された小型の Arbiter-PUF と、各 Arbiter-PUF のレスポンスを記憶する 1-bit の記憶素子から構成される。Arbiter-PUF は自身に隣接する Arbiter-PUF のレスポンスをチャレンジとして受け取り、新たなレスポンスを生成する。得られたレスポンスは、隣接する Arbiter-PUF に再帰的に入力され、カオティックな状態遷移を実現する。また、提案 PUF は再帰結合によって過去のチャレンジ入力系列を記憶できるため、同一のチャレンジを与えても、その入力順序によって異なる応答を示す。シミュレーション実験の結果、理想に近い 50.1% のチップ間、チャレンジ間ハミング距離を達成できることを示した。

A Design of Challenge-Hysteresis PUF and its Simulation-based Evaluation

HIROMITSU AWANO^{1,a)} TAKASHI SATO²

Abstract: A concept of novel PUF structure that features a challenge hysteresis is proposed. The proposed PUF consists of a lattice like arrangement of cells, each of which is composed of a small Arbiter-PUF and a 1-bit register that stores the response of the Arbiter-PUF. The Arbiter-PUF reads the registers of the neighbor cells and outputs a response, which again serves as a challenge of its neighbors. Utilizing the state-memorizing property of the spin registers, the proposed PUF attains a challenge hysteresis, allowing a sequence of challenge inputs continuously stimulate its chaotic behaviour. Our simulation experiments reveal that the proposed PUF has nearly ideal metrics of inter-chip Hamming distance (HD) of 50.1% and inter-sequence HD of 49.9%.

1. はじめに

モノ同士が人間を介さずに情報をやり取りする、Internet-of-Things (IoT) 時代が到来し、ネットワークに接続される情報機器の数は爆発的に増加している。IoT の普及に伴い、社会の利便性や効率の大幅な向上が期待されている一方で、情報のやり取りに人が介在しなくなることに起因するセキュリティリスクが問題視されている。様々なセキュリティ技術が提案される中で、機器認証は依然として最も基本的かつ重要な技術である。従来は、個々のデバイスに搭載した不揮発メモリに機器固有の ID を書き込んで機器認証を実現する方式が一般的であった。しかしながら、不揮発メモリの製造には特殊なプロセスが必要であり、デバ

イスコストが高くなることや、書き込んだ固有 ID そのものが盗まれることに伴う、“なりすまし攻撃”に脆弱であることが問題視されていた。

これら不揮発メモリを活用したデバイス認証に代わる方式として、近年、Physically unclonable function (PUF) が着目されている。PUF はチャレンジと称する入力を与えると、レスポンスと称する応答を返す回路である。PUF は、デバイスが本来持っている個体差を利用してレスポンスを生成する。このため、全く同じチャレンジを与えたとしても、デバイス毎に異なるレスポンスを返すことができる。近年のトランジスタは微細化が進んでおり、その電気的特性（しきい値電圧 V_{TH} や移動度等）が大きくばらつくことが知られている。そこで、信号バス対の信号伝播遅延差やインバータペアの駆動力比、カレントミラーの電流コピーばらつき等を活用した PUF が提案されている。

PUF を個体識別に応用するにあたって、“一意性”及び“安定性”と呼ばれる 2 つの性質が重要となる。まず、個々のデバイスを一意に識別するために、同一のチャレンジに対し、デバイス毎に異なる応答を返すことが求められる。これを一意性と呼ぶ。一方、PUF が置かれている環境（温

¹ 東京大学大規模集積システム設計教育研究センター
School of Engineering 3rd Bldg., The University of Tokyo,
Hongo 7-3-1, Bunkyo-ku, Tokyo, 113-8656, Japan

² 京都大学情報学研究科通信情報システム専攻
Kyoto University, Yoshida-hon-machi, Sakyo, Kyoto, 606-
8501, Japan

a) awano@vdec.u-tokyo.ac.jp

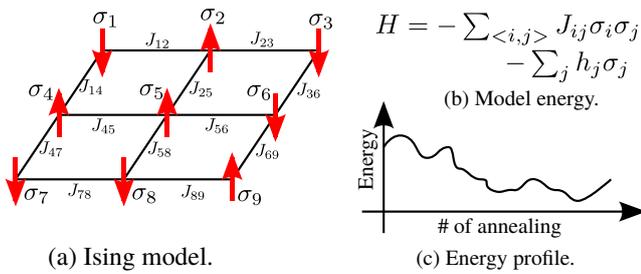


図 1 Ising-model

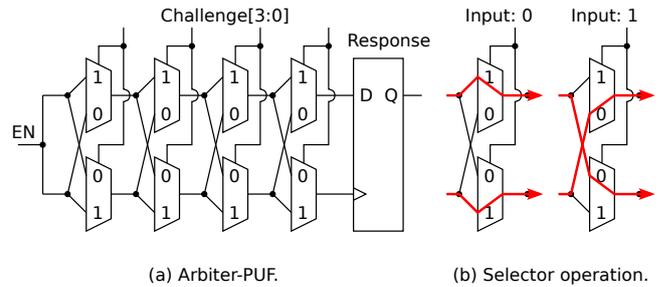


図 2 Example schematic of Arbiter-PUF.

度や電源電圧)等が変化しても、チャレンジ・レスポンス関係は不変であることが求められる。これを安定性と呼ぶ。

よく知られた PUF として, Arbiter-PUF と Ring-Oscillator PUF (RO-PUF) が挙げられる。Arbiter-PUF は論理ゲートの信号伝播遅延差を利用して, デバイス固有のレスポンスを生成する。Arbiter-PUF のチャレンジ・レスポンスペア (CRP) 数は回路規模に対して指数オーダで増加するため, 非常に面積効率が高い実装方式と言える。しかし, 信号伝播遅延は線形モデルで精度良く近似できることから, Support vector machine (SVM) 等を使った機械学習攻撃に対して非常に脆弱であることが知られている。そこで, Ring-Oscillator (RO) ペアの発振周波数差に基づきレスポンスを決定する RO-PUF と呼ばれる方式が提案された。RO-PUF は, Arbiter-PUF の弱点であった機械学習攻撃への脆弱性を克服した一方で, CRP 数が回路規模の 2 乗でしか増加しないため, 面積効率が悪いという問題がある。近年では, RO-PUF や Arbiter-PUF 双方の弱点を克服した bi-stable ring PUF (BR-PUF) と呼ばれる方式も提案され [1], 安全性の検証が行われている [2]。

PUF は, 製造ばらつきを利用している関係から, 回路方式と合わせてその実装方式についても十分検討する必要がある。例えば, RO-PUF や Arbiter-PUF の実装では, レスポンスが製造ばらつきのみで感度を持つよう, RO や遅延パスを完全に対称にレイアウトする必要がある。この設計制約は, 大規模な PUF を設計する上で大きな障害となる。また, FPGA への実装も強く制約される。そこで, 大規模な PUF を小規模 PUF の組み合わせに分割し, 階層的な設計を可能とする Composite-PUF と呼ばれる設計パラダイムが提案されている [3]。

本論文では, イジングモデルに着想を得た PUF の回路方式を提案する。イジングモデルは, 統計物理分野において, 磁性体のスピンを表現するために考案されたモデルであるが, 組み合わせ最適化問題との親和性から, D-Wave [4] を始めとした新概念コンピューティング等にも応用が広がっている。イジングモデルは +1 及び -1 の 2 値を取る, スピンと呼ばれる 1 bit の変数, スピン間の相互作用, 及び外部磁場で規定される。通常, スピンは格子状に配置され, 各スピンは隣接するスピンとの相互作用にもとづいて自身のスピンを更新する。図 1 に 9 個のスピンから構成される単純なイジングモデルを示す。ここで矢印はスピンの向きに対応している。イジングモデルには Hamiltonian 関数で表現されるエネルギーが定義されており, 個々のスピンはエネルギーを最小化するように変化する特性がある。この特性を組み合わせ最適化問題のソルバーに応用した例が D-Wave や CMOS アニーリングマシン [5], [6] である。

これらのソルバーマシンでは, イジングモデルのエネルギー

を最小化するスピン状態が, 組み合わせ最適化問題の解と対応するようにスピン間の相互作用を調整する。一方, 本論文では, スピン間の相互作用をトランジスタの特性ばらつきで決定することで, イジングモデルを PUF として利用する。イジングモデルでは, 現在のスピン状態が分かれば次時刻のスピン状態は簡単に計算できるが, 逆に, 過去のスピン状態を推定することは困難である。つまり, イジングモデルを PUF に応用することで, 攻撃者による PUF の内部状態推定を困難とし, より強固な個体識別を実現できると考えられる。

提案 PUF は, スピンを記憶する 1 bit のレジスタと, デバイス固有の相互作用を実現するための小規模 Arbiter-PUF から構成される。Arbiter-PUF のレスポンスはレジスタに取り込まれた後に, 再び隣接する Arbiter-PUF にチャレンジとして再帰的に入力される。提案 PUF は, この再帰結合によって過去の状態を記憶するため, レスポンスはチャレンジ入力のみならず, その入力順序にも依存する。

提案 PUF の利点は以下のように整理できる。

レスポンスの予測が困難であること: チャレンジ・ヒステリシス特性を有するため, レスポンスはある時点で与えられたチャレンジのみならず, その入力順序によっても変化する。このため, チャレンジからレスポンスへの変換関数は非常に複雑かつ予測が困難となる。

レスポンス再現度が高いこと: 不安定な Arbiter-PUF をマスクすることで, レスポンスの再現度を大幅に高めることができる。

秘密モデルを構築できること: 提案 PUF は格子状に配置された Arbiter-PUF から構成されており, Arbiter-PUF の CRP から, スピン状態の時間発展を決定的に再現できる。つまり, 提案 PUF の全 CRP を記録する代わりに, 小規模 Arbiter-PUF の CRP をデータベースに保存しておくだけで, 任意のチャレンジに対するレスポンスを予測することができ, 認証に必要なデータベース容量を大幅に削減することができる。

2. 事前準備

2.1 Physically Unclonable Function

PUF は Strong-PUF 及び Weak-PUF に大別される。Strong-PUF とはチャレンジを受け取り, デバイス毎の特性を付加した応答を返す回路のことであり, Arbiter-PUF や RO-PUF が代表的な例である。一方, Weak-PUF は CRP が 1 組である特殊な Strong-PUF であり, 例えば SRAM の初期状態を活用した SRAM-PUF [7], [8] が知られている。以下, 本論文では, Strong-PUF を対象とする。

Arbiter-PUF の基本構成を図 2 に示す。マルチプレクサ

を多段接続したセクタチェーン回路は、チャレンジ信号に応じて入力端子からアービター回路までの2つの経路を選択する。各セクタは信号伝播遅延が等価となるように設計されているが、製造ばらつきにより選択された経路毎に信号伝播遅延が異なるため、これをレスポンスとして用いることが出来る。セクタ段数を N とすると、 2^N 通りの経路選択が可能である。アービター回路は、2つの経路のうち、どちらの信号が先に到着したか判定し、0/1の信号を出力する。

2.2 PUF の性能指標

PUF の性能指標として一意性と安定性が挙げられる。一意性は2つのPUFに同じチャレンジを与えた時のレスポンスの差異であり、通常はレスポンス間のハミング距離で表現される。理想的なPUFではレスポンスは一様にランダムであり、一意性は50%となる。

また、機器認証にPUFを応用するためには、周囲の温度や電源電圧が変動しても、同じチャレンジ C_A に対し、常に同じレスポンス R_A を返すことが求められる。これは安定性と呼ばれる性質であり、同一PUFに繰り返し同じチャレンジを与えて得られるレスポンス間のハミング距離で表現される。理想的には温度や電圧変動がレスポンスに影響を与えないことであり、その時の安定性は0%となる。

2.3 PUF を活用したデバイス認証プロトコル

一般に、PUFを用いたデバイス認証は以下のような手順により実現される。

PUF 製造フェーズ

(1) PUF インスタンス製造後にCRPを読み取り、認証サーバのデータベースに格納する。

(2) PUF インスタンスを顧客に提供し、顧客がこれを製品に組み込む。

認証フェーズ

(3) 認証を受けたいクライアントが、認証サーバに対してリクエストを送信する。

(4) リクエストに対する応答として、サーバは(1)で得られたCRPデータベースからランダムに1つペアを選択し、チャレンジのみをクライアントに送信する。

(5) チャレンジを受け取ったクライアントは、搭載されたPUFでレスポンスを計算し、結果をサーバに返送する。

(6) サーバはクライアントのレスポンスを、データベースの記録と照合する。また、認証フェーズで使用したCRPは、再使用されないようにデータベースから削除しておく。

PUFのレスポンスが攻撃者に盗聴される可能性を考えると、一度認証で使用したCRPは再度使用しないことが望ましい。認証回数が膨大になると、サーバ側に膨大なCRPを保持する必要があり、データベースの記憶容量増大が課題となっている。

3. 提案回路

3.1 提案 PUF のコンセプト

本論文では、イジングモデルを活用した新概念コンピューティングに着想を得て、スピンの複雑な時間発展を応用したPUFを提案する。提案PUFは、イジングモデルのスピンの対応するレジスタと、レジスタ間の相互作用を制御するArbiter-PUFから構成する。各Arbiter-PUFの

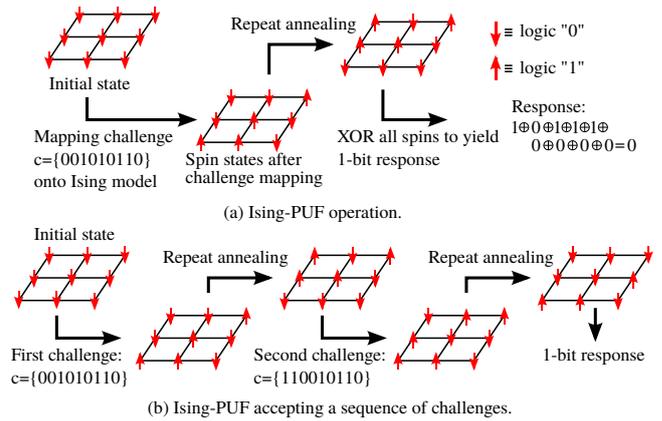


図3 Example operation of Ising-PUF.

レスポンスは、レジスタに記憶された後に、再び隣接するArbiter-PUFにチャレンジとして再帰的に入力される。このループを繰り返すことで、僅かな初期状態の差異を増幅させ、高い一意性を獲得することが可能となる。

提案PUFがチャレンジをレスポンスに変換する過程を図3(a)に示す。まず全てのスピンを“0”に初期化する。ここで、イジングモデルを標準的な論理回路として実装するために、2値のスピン状態(+1・-1)を、それぞれ、“1”・“0”に読み替えていることに注意されたい。次に、チャレンジ $c = c_0c_1 \dots c_N$ をイジングモデルにマッピングする。具体的には、チャレンジの対応するビットが“1”の時 ($c_i = 1$) に、スピン σ_i の論理を反転させる。図3(b)に9bitのチャレンジ {001010110} が入力される様子を示す。チャレンジに従って初期スピンを設定した後に、アニーリングと呼ぶ操作を行う。アニーリングにおいて、各セルは上下左右に隣接するセルのスピンを読み取って4bitのチャレンジを作り、Arbiter-PUFに入力し、得られた1bitのレスポンスに従って自身のスピンを更新する。スピンの値は、再び隣接するセルにチャレンジとして再帰的に入力され、カオティックな状態遷移を実現する。アニーリングを繰り返した後に、全スピンを読み出し、その排他的論理和をレスポンスとして返す。

提案PUFは再帰結合によって過去のチャレンジに対する記憶を有する。図3(b)に同一チャレンジを異なる順番で入力した時のレスポンスを示す。図に示すように、チャレンジ入力に対するヒステリシス特性によって非常に複雑なチャレンジ・レスポンス変換を実現できる。

3.2 提案 PUF の基本操作

ここでは N 個のスピンを持つ提案PUFにおける基本操作について述べる。以下では、 N bitのチャレンジを $c = \{c_1, c_2, \dots, c_N\}$ 、 i 番目のスピンを σ_i で表す。

Step 1:初期化 全てのスピンを“0”に初期化する。つまり、 $i = 1, 2, \dots, N$ について σ_i を“0”に設定する。

Step 2:チャレンジ入力 チャレンジ c に従ってスピン状態を初期化する。前述の通り、 $c_i = 1$ の時に、 σ_i の論理を反転させる。

Step 3:アニーリング 次に各スピンの状態を、隣接スピンの相互作用によって繰り返し更新する。各セルは上下左右に隣接するセルのスピンを読み取り、各セルに搭載されたArbiter-PUFによって1bitのレスポンスに変換して自身のスピンを更新する。スピンとして

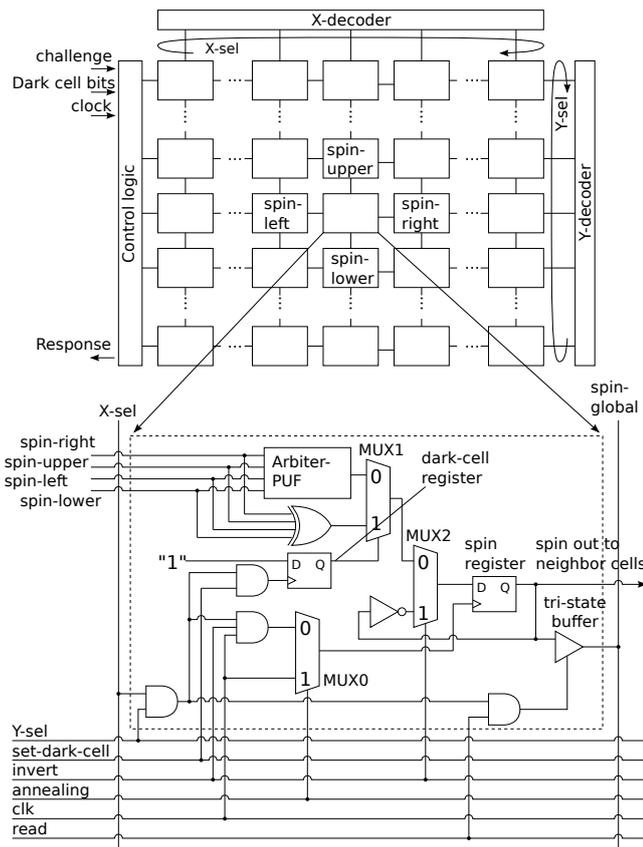


図 4 Circuit structure.

保存されたレスポンスは、再び、隣接セルにチャレンジとして再帰的に入力され、チップ固有のスピン更新パターンを実現する。

Step 4:レスポンス生成 アニーリングが終わると全セルのスピンを読み出し、排他的論理和を取って 1 bit のレスポンスを得る。

3.3 回路構造

提案 PUF は、図 4 に示すように、スピンレジスタ・ダークビットレジスタ及び 4 入力 Arbiter-PUF を含むセルと、アドレスデコーダ及び制御回路から構成されている。

回路動作は以下のとおりである。初めに、チャレンジをマッピングするために、“invert” 信号を制御してアドレスで指定されたセルのスピンを反転させる。次にアニーリングを実行し、スピンの相互作用を考慮して逐次的にスピンを更新する。“annealing” 信号を “H” として Arbiter-PUF の出力とスピンレジスタを接続し、この状態でクロックを立ち上げると隣接セルのスピンが Arbiter-PUF によって 1 bit のレスポンスに変換され、スピンレジスタに保存される。上記の全セル並列のアニーリング操作を十分繰り返した後に、各セルのスピン状態を読み出す。ここでは、“read” 信号を “H” として選択セルのスピンレジスタを読み出し線に接続し、スピン状態を順次読み取る。最後に排他的論理和を計算して 1 bit のレスポンスを返す。

次に、提案 PUF の安定性について考える。理想的な PUF では、温度や電源電圧が変動したとしても、同じチャレンジに対して、常に同じレスポンスを返すことが求められる。しかし、一般には、温度・電圧に対する感度はトランジスタ毎に異なるため、常に完全に同じレスポンスを得る

ことは困難である。また提案 PUF では、Arbiter-PUF を再帰的に接続しているため、Arbiter-PUF の僅かな特性変動が、アニーリングを繰り返すことで増幅されてしまう懸念がある。そこで、提案 PUF ではレスポンスが不安定な Arbiter-PUF をマスクするための Dark-Cell Elimination (DCE) という枠組みを採用している [9]。図 4 中のダークビットレジスタに “H” を設定すると、隣接スピンの排他的論理和がスピンレジスタに入力される。レスポンスが不安定な Arbiter-PUF を迂回させ、決定的な論理をスピンとして設定することで、誤差がイジングモデル全体に拡散することを防ぐ狙いがある。

DCE では、PUF 製造後のテスト工程にて、各セルに搭載された Arbiter-PUF の CRP をキャラクタライズすることを想定している。Naive な Arbiter-PUF は CRP 数がチャレンジのビット幅に対して指数的に増大するため、全ての CRP をキャラクタライズすることは非現実的である。一方、提案 PUF では Arbiter-PUF のチャレンジビット幅は高々 4 bit であることから、縦に M 、横に N 個のセルを並べた場合、キャラクタライズすべき CRP の数は $2^4 \times N \times M$ となるため、現実的な時間で全ての CRP を読み取ることが可能である。その後、応答が不安定な Arbiter-PUF を含むセルの座標を不揮発メモリなどに保存しておく。

3.4 認証プロトコル

理想的な PUF では、チャレンジに対するレスポンスを予測することが出来ない。そのため、PUF を用いた個体識別では、PUF を出荷する前に CRP を読み出し、認証サーバに保存しておくことが求められる。前述のように、Arbiter-PUF 等は回路規模に対して CRP 数が指数的に増大するため、認証サーバに膨大な記憶領域が必要となる。そこで、PUF の CRP を保存する代わりに、PUF のレスポンスを予測する“秘密モデル”を構築し、サーバの記憶負荷を低減する手法が提案されている [10], [11]。例えば、Arbiter-PUF では、CRP を記憶する代わりに各マルチプレクサの遅延を保存しておくことで、任意のチャレンジに対するレスポンスを計算により求めることが出来る。

図 5 に提案 PUF を用いた個体識別プロトコルを示す。

機器登録フェーズ: 提案 PUF はレジスタを介して Arbiter-PUF を相互接続した構造であり、各 Arbiter-PUF の CRP が分かれば、提案 PUF への任意のチャレンジ入力に対してレスポンスを計算することが出来る。そこで、機器登録にあたっては、事前に全ての Arbiter-PUF の CRP を読み出し、これを秘密のデータベースに格納する。先に述べたように、提案 PUF で使用されている Arbiter-PUF は高々 4 入力であるため、現実的な時間で全ての CRP を読み出すことが出来る。また、不安定な Arbiter-PUF を同定するために、異なる温度・電圧条件下で CRP を繰り返し読み出す。図 5 の例では、PUF#1 の “1110” に対するレスポンスが異なっているため、当該 Arbiter-PUF を含むセルのダークビットレジスタに “1” を設定する。

機器認証フェーズ: 認証サーバはランダムに選んだチャレンジをクライアントに送信する。チャレンジを受け取ったクライアントは、提案 PUF を用いて対応するレスポンスを求め、サーバに送り返す。サーバはクライアントからのレスポンスと、自身の秘密モデルから計算されるレスポンスとを比較して、一致すれば、クライアントを認証する。

Instance registration

Exhaustively read CRPs of all primitive PUFs and securely transfer them to the authentication server.

CRPs are read under different temperature conditions to determine "dark-cell-bits."

Instance authentication

1. Authentication server randomly select challenge.
2. Transfer the challenge to the target instance.
3. Emulate the behaviour of target instance and pre-compute the expected response.
4. The response from the target instance is compared with the expected one and return the authentication result.

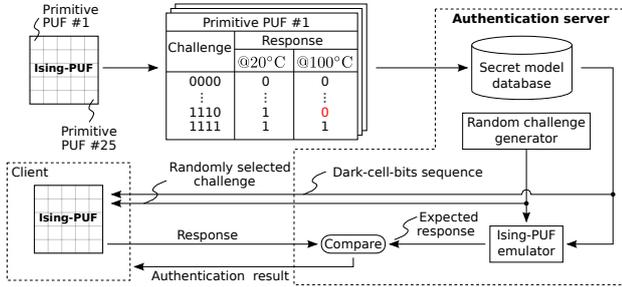


図 5 Chip authentication protocol based on Ising PUF.

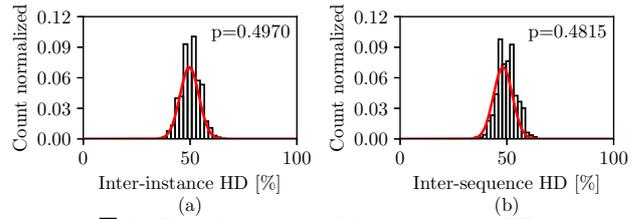


図 7 Inter-instance and inter-sequence HD.

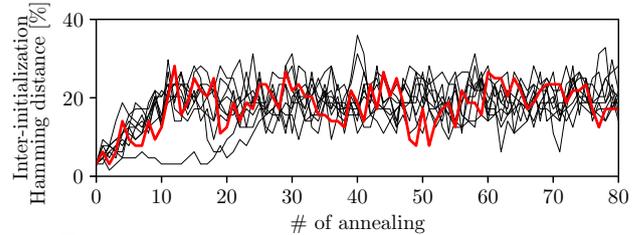


図 8 Sensitivity of spin states to initial spin states.

4. 数値実験

4.1 実験設定

数値実験により提案 PUF の性能を評価する．ここでは，シミュレーション時間を削減するために，Arbiter-PUF 部分のみをトランジスタレベルでシミュレーションし，その他の回路動作は Python スクリプトによって模擬した．図 6 に実験フローを示す．まず，65nm プロセスを想定して Arbiter-PUF を仮想的に 6400 個作り，各々の CRP を SPICE でシミュレーションする．次に，得られた CRP をもとに 8 × 8 個のセルを持つ提案 PUF を仮想的に 100 個作り，一意性と安定性を評価する．図 6 の右側に，提案 PUF を用いて 1 bit のレスポンスを得る手順を示す．本数値実験では，提案 PUF に対するチャレンジは 3 つの 64 bit 長のサブチャレンジから構成されているとし，このチャレンジを 128 回与えて，128 bit 長のレスポンスを得ている．提案 PUF はサブチャレンジ 1 つに対して，スピン反転及びアニーリングを 1 セット実行している．従って，本実験で，提案 PUF はチャレンジを 1 つ受け取る度に，スピン反転・アニーリングを 3 セット実行し，最終的に得られたスピン状態の排他的論理和をレスポンスとして返す．前述のように，本実験では 100 個のインスタンスをシミュレーションしており，各インスタンスに 128 回チャレンジを与えているため，全体としては 128 bit 長のレスポンス系列が 100 インスタンス分得られる．得られたビット系列を使って以下を検証する．

- 提案 PUF の一意性及び安定性
- サブチャレンジを与える順番に対するレスポンスの感度
- 初期スピン状態に対する時間発展の変化

また，レスポンスが不安定な Arbiter-PUF を同定するために，20°C 及び 100°C でトランジスタレベルシミュレーションを実行した．その後，2 つの温度条件で CRP を比較し，一致しない Arbiter-PUF を“不安定”であると見なして当該 Arbiter-PUF を含むセルのダークビットレジスタに“1”を設定している．本実験では，およそ 10% から 40% の Arbiter-PUF で温度変化に伴うレスポンス変動が見られた．

4.2 実験結果

提案 PUF の一意性を評価するために，得られた 100 個のレスポンス間でハミング距離を計算した．結果を図 7(a) に示す．ここで赤の線は二項分布の確率密度関数を示している．平均ハミング距離は 50.1% であり，これは理想的な平均ハミング距離である 50% に非常に近い．

次に，サブチャレンジを与える順番を変更した時のレスポンス変化を調べるために，同一のチャレンジで，サブチャレンジの順番のみ入れ替えたものを提案 PUF に与え，レスポンスをシミュレーションした．このとき前述の一意性に関する検証と全く同じようにレスポンス間のハミング距離を計算した結果が図 7(b) である．平均的なハミング距離は 49.9% であり，チャレンジの順番を入れ替えただけでもレスポンスが大幅に変化することが確かめられた．

さらに，スピンの初期状態がレスポンスに与える影響を調べるために，初期状態が 2 bit だけ異なる 2 つの提案 PUF を用意し，同一のチャレンジを与えて，スピン状態の時間発展をシミュレーションした(図 8)．ここで，縦軸は 2 つのスピン状態のハミング距離，横軸はアニーリング回数である．実験には，仮想的に作成した 100 インスタンスからランダムに選択された 10 インスタンスを用いた．図 8 の黒線は各 PUF のハミング距離の時間発展，赤線は 10 インスタンスの平均を示している．この結果から，アニーリングを繰り返すことで，スピン状態の僅かな差異が大きく増幅されることが分かる．つまり，PUF 外部に新しいエントロピー源を導入しなくても，提案 PUF が内包するエントロピー源を再帰的に活用することで，よりランダムなレスポンスを返すことが可能になっている．

最後に，提案 PUF の安定性を評価する．今回は，同一のチャレンジを同じ PUF に繰り返し与え，温度変化に対するレスポンスの変化をシミュレーションによって求めた．図 9 にランダムに選択された 10 インスタンスについて，20°C 及び 50°C の条件で得られたレスポンス間のハミング距離を示す．ここで，青，黒，及び赤の線は，それぞれ，不安定な Arbiter-PUF をマスクした場合，マスクしなかった場合及び平均的なハミング距離を示す．この結果から，不安定な Arbiter-PUF があると，安定性が大幅に損なわれることが分かる．一方，マスク機構を用いることでハミング距離が“0”になっており，温度変化がレスポンス変化に

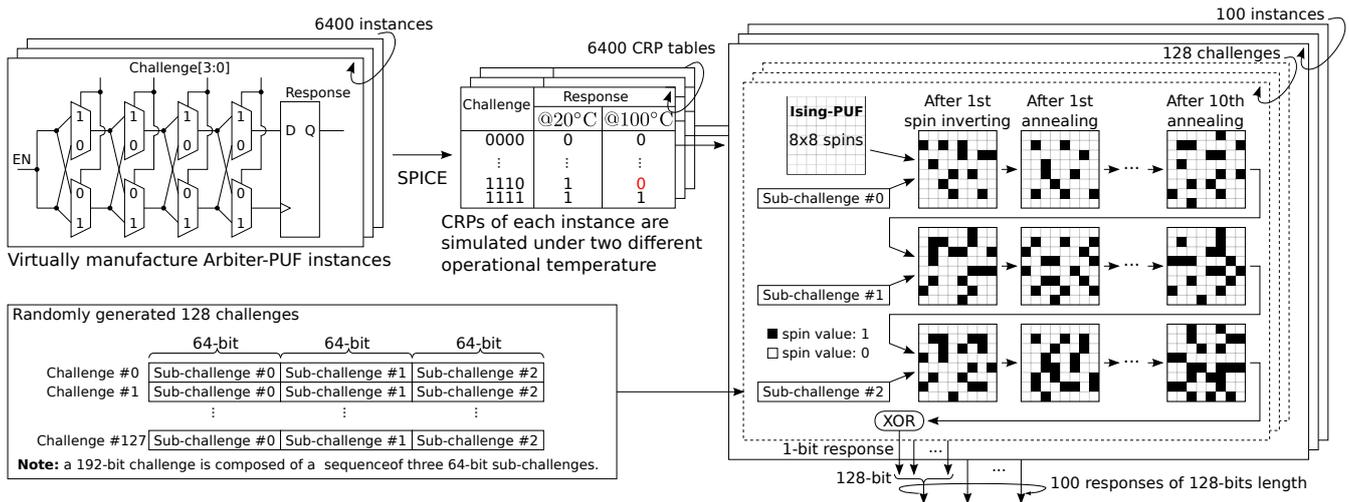


図 6 Simulation flow.

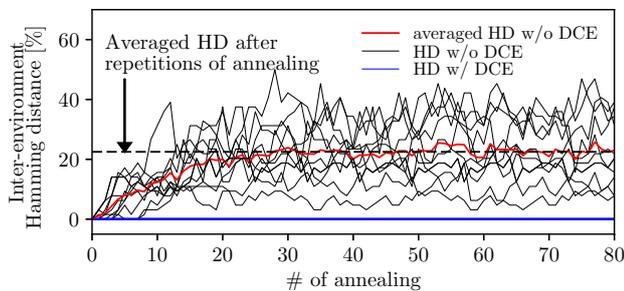


図 9 Effectiveness of dark-cell scheme.

与える影響を完全に排除できていることが確認できる。

5. 結論

本論文ではイジングモデルにおけるスピン状態の時間発展に着目した PUF を提案した。提案 PUF はチャレンジ入力に対するヒステリシス特性を有し、同じチャレンジであっても入力する順番によって全く異なるレスポンスを返す。この特性により、機械学習攻撃への高い耐性が期待できる。実験結果から提案 PUF は高い一意性及び安定性を有していることが確認された。また、提案 PUF には、対応する秘密モデルによって任意のチャレンジに対するレスポンスを計算することが出来るため、認証サーバに要求されるデータベース容量を大幅に圧縮することが可能となる。提案 PUF を用いることで、高いセキュリティと低い認証コストを両立することが出来ると期待される。

謝辞

本研究の一部は、科研費 17H01713 の助成を受けた。

参考文献

[1] Q. Chen, G. Csaba, P. Lugli, U. Schlichtmann, and U. Rührmair, "The Bistable Ring PUF: A new architecture for strong Physical Unclonable Functions," in *Int. Symp. on Hardware-Oriented Security and Trust*, June 2011, pp. 134–141.

[2] Q. Chen, G. Csaba, P. Lugli, U. Schlichtmann, and U. Rührmair, "Characterization of the bistable ring PUF," in *Design, Automation and Test in Europe*,

March 2012, pp. 1459–1462.

[3] D. P. Sahoo, S. Saha, D. Mukhopadhyay, R. S. Chakraborty, and H. Kapoor, "Composite PUF: A new design paradigm for Physically Unclonable Functions on FPGA," in *Int. Symp. on Hardware-Oriented Security and Trust*, May 2014, pp. 50–55.

[4] M. W. Johnson, M. H. S. Amin, S. Gildert, T. Lanting, F. Hamze, N. Dickson, R. Harris, A. J. Berkley, J. Johansson, P. Bunyk, E. M. Chapple, C. Enderud, J. P. Hilton, K. Karimi, E. Ladizinsky, N. Ladizinsky, T. Oh, I. Perminov, C. Rich, M. C. Thom, E. Tolkacheva, C. J. S. Truncik, S. Uchaikin, J. Wang, B. Wilson, and G. Rose, "Quantum annealing with manufactured spins," *Nature*, vol. 473, pp. 194–198, May 2012.

[5] M. Yamaoka, C. Yoshimura, M. Hayashi, T. Okuyama, H. Aoki, and H. Mizuno, "20k-spin Ising chip for combinatorial optimization problem with CMOS annealing," in *Int. Solid-State Circuits Conf.*, Feb 2015, pp. 1–3.

[6] M. Yamaoka, C. Yoshimura, M. Hayashi, T. Okuyama, H. Aoki, and H. Mizuno, "A 20k-Spin Ising Chip to Solve Combinatorial Optimization Problems With CMOS Annealing," *IEEE J. Solid-State Circuits*, vol. 51, no. 1, pp. 303–309, Jan 2016.

[7] J. Guajardo, S. S. Kumar, G.-J. Schrijen, and P. Tuyls, "FPGA Intrinsic PUFs and Their Use for IP Protection," in *Conf. on Cryptographic Hardware and Embedded Systems*, P. Paillier and I. Verbauwhede, Eds., 2007, pp. 63–80.

[8] D. E. Holcomb, W. P. Bursleson, and K. Fu, "Initial SRAM State as a Fingerprint and Source of True Random Numbers for RFID Tags," in *Conf. on RFID Security*, 2007.

[9] J. Guajardo, S. S. Kumar, G.-J. Schrijen, and P. Tuyls, "FPGA Intrinsic PUFs and Their Use for IP Protection," in *Conf. on Cryptographic Hardware and Embedded Systems*, 2007, pp. 63–80.

[10] M. Majzoobi and F. Koushanfar, "Time-Bounded Authentication of FPGAs," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 1123–1135, Sept 2011.

[11] C. Herder, M. D. Yu, F. Koushanfar, and S. Devadas, "Physical Unclonable Functions and Applications: A Tutorial," *Proc. of the IEEE*, vol. 102, no. 8, pp. 1126–1141, Aug 2014.