Ising-PUF: A Machine Learning Attack Resistant PUF Featuring Lattice Like Arrangement of Arbiter-PUFs

Hiromitsu Awano
VLSI Design and Education Center, The University of Tokyo
Hongo 7-3-1, Bunkyo-ku, Tokyo, Japan, 113–8656
Email: awano@vdec.u-tokyo.ac.jp

Takashi Sato
Graduate School of Informatics, Kyoto University
Yoshida-honmachi, Sakyo-ku, Kyoto, Japan 606–8501
Email: paper@easter.kuee.kyoto-u.ac.jp

***Abstract*—A concept of Ising-PUF, a novel PUF structure that utilizes chaotic behavior of mutually interacting small PUFs, is proposed. Ising-PUF consists of a lattice like arrangement of small PUFs, each of which contains a spin register that stores the response of the small PUF, which also serves as a challenge of its neighbors. The spin patterns that develop along time determine the 1-bit response of the Ising-PUF. Utilizing state-memorizing nature of the spin registers, Ising-PUF attains a challenge hysteresis, i.e., allowing sequence of challenge inputs that continuously stimulate its chaotic behavior, which provides the drastically large challenge-to-response space. Experimental results demonstrate nearly ideal metrics; inter-chip Hamming distance (HD) of 50.1% and inter-environment HD of 2.26%. Further, Ising-PUF is remarkably tolerant to machine learning attacks, demonstrating that, even with a deep neural network using a 50k training CRPs, the prediction accuracy remains 50%, which is comparable to a random guess.**

I. Introduction

Zillions of connected devices are beginning to penetrate into various areas of our daily living. A representative example is the Amazon Dash Button [1], a small internet-connected device, which allows us to order daily necessities, such as coffee, washing powder, etc., by simply "pressing" a button on it. This kind of convenience may be threatened by various security risks. Among the security measures taken, device and/or user authentication is considered the most important since identity validation is required almost wherever the communications are involved. Until recently, the best practice for enabling the authentication is to store a secret key in a non-volatile memory (NVM). However, fabrication of a CMOS logic with dedicated NVMs requires additional processes, which increases the device cost. Moreover, the stored secret key is vulnerable to physical attacks and hence the device should also be designed with an active tamper protection/detection circuit, which further increases the device cost.

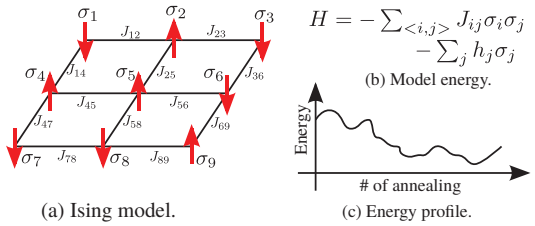
Physically unclonable functions (PUFs) [2] attract increasing attention as a promising alternative for the secret-key-based device authentication. Instead of storing a secret key in NVM, PUFs utilize a manufacturing variability of transistors as a security key. Due to miniaturization of transistors, variations of a number of doping ions and/or atomic level bumps on a gate electrode result in significant threshold voltage (V_{TH}) variations. The V_{TH} variability is an inherent characteristic to the transistor and cannot be replicated even by the manufacturer of the PUF, making it a unique and unclonable "fingerprint" of each chip.

In order to serve as an alternative to the secret-key-based authentication, PUF should achieve high level of *uniqueness* and *robustness.* The uniqueness measures how widely the response of an individual PUF varies among chips, while the robustness measures the stability of PUF response upon the changes of operational voltage or temperature. On top of the uniqueness and robustness, it is also required for PUFs to provide a large variety of CRPs so that the attacker is unable to read out all CRPs within a practical time period.

Arbiter-PUF (APUF) [3] is a firstly proposed silicon PUF, which exploits gate delay variations to generate chip specific keys. APUF can provide exponentially large CRPs with respect to hardware resource. However, since signal propagation delay can be well represented by an additive linear delay model with a limited number of unknown parameters, it is quite easy for attackers to retrieve these unknown parameters by collecting challenges and the corresponding responses [4]. Another popular PUF architecture is a ring-oscillator PUF (RO-PUF) [5] which exploits frequency variations of ROs. Although RO-PUFs tend to achieve a good uniqueness, it can supply only quadratic number of CRPs with respect to the number of embedded ROs, which makes the comprehensive read-out of CRPs feasible in a reasonable time. To alleviate these shortcomings, bi-stable ring PUF (BR-PUF) [6], [7] or double APUF (DAPUF) [8] have been proposed. Although BR-PUF utilizes stable state of an inverter ring consisting of an odd number of stages to achieve a complex challenge-response behavior, Xu et al. showed that the responses of BR-PUF can be predicted with 95% accuracy [9]. Yashiro et al. employed an advanced deep neural network (DNN) to predict the responses of DAPUF with the accuracy of 68%, demonstrating that DAPUF is resistant to machine learning (ML) attacks [10]. However, as we show later, a DNN-based classifier implemented on a modern DNN framework successfully achieves a significantly better prediction accuracy of 88%, which indicates that DAPUF no longer offers resistance to the ML attacks. Hence, a novel PUF circuit, which is truly resistant to DNN-based ML attacks, is definitely required.

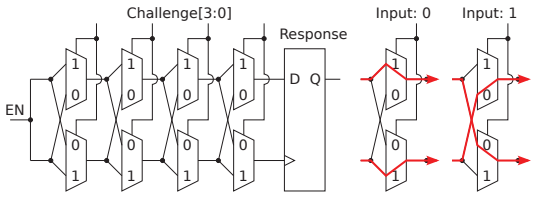
Not only the circuit structures but also their implementations severely affect the performance of PUFs. In order to reflect only the mismatches introduced during device manufacturing process, unit structure that comprises the PUF must be structurally identical and symmetric. Otherwise, the mismatch biases the response-bit toward either "0" or "1," which severely deteriorates the randomness of the response. Although the symmetric layout may be easily achieved in small PUF designs, it becomes increasingly challenging as the size of the PUF becomes larger. The symmetry requirement also becomes a barrier for implementing PUFs on FPGAs. To solve this problem, a new design paradigm called *PUF composition* has been proposed [11], in which multiple small PUFs are used as building blocks for a large PUF.

978-3-9819263-0-9/DATE18/©2018 EDAA



(a) Ising model. (b) Model energy. (c) Energy profile.

Fig. 1. Ising-model



(a) Arbiter-PUF. (b) Selector operation.

Fig. 2. Example schematic of APUF.

In this paper, we propose a novel PUF circuit structure named *Ising-PUF*, which is inspired from the Ising model [12] originally developed in physics community. The Ising model consists of 1-bit variable called *spin*, which takes one of two states ($+1$ or -1). The spins are connected to form a graph structure, usually a lattice, which allows each spin to interact with its neighbors. Fig. 1(a) illustrates a simplified example of the Ising model with 9 spins, where the red arrows and the edges represent the spin values (σ_i) and the mutual interactions between spins (J_{ij}), respectively. The energy of the Ising model is defined by the Hamiltonian function shown in Fig. 1(b), where h_j corresponds to an external magnetic field. By iteratively updating spin values according to their local interactions, they gradually converge to an equilibrium state at which the energy function takes a local minimum as shown in Fig. 1(c). D-wave [13] or CMOS Ising machine [14], [15] exploit this intrinsic convergence property of Ising model for solving combinatorial optimization problems, i.e., the interactions between spins are adjusted so that the minimum energy configuration also optimizes the original optimization problem.

Contrary to those Ising model emulators that utilize convergence of spin values to solve combinatorial optimization problem, Ising-PUF utilizes transient change of spin values to extract device-intrinsic fingerprint. Specifically, in Ising-PUF, the spin in the Ising model is replaced with a circuit called *cell*. The cell consists of a small PUF, hereafter an *elemental PUF*, and a spin register that memorizes the response of the elemental PUF. At the same time, the value of each spin register is distributed to adjacent elemental PUFs as the challenge signal, enabling elemental PUFs to interact mutually. According to the different responses of the elemental PUFs, the transient changes of spin values become unique to each IC chip, with which the chip authentication can be realized.

While Ising-PUF may somewhat look like the composite PUF, the most important advancement is that the elemental PUFs are mutually connected to form many closed loops. This construction drastically increases the variation of challenge-to-response mapping. The complex behavior of Ising-PUF may be analogously compared with the difficulty of test pattern generation for large sequential circuits.

From the mathematical perspective, Ising-PUF can be viewed as a "chaotic" system. Chaos is a dynamical system whose time development is highly sensitive to the initial condition (also known as *butterfly effect*) [16]. Small difference in initial conditions yields large difference of the output, making the prediction of system outputs almost impossible. Here, the "chaotic" unpredictability can be achieved through a deterministic system; by using the randomness of V_{TH} in transistors, hence the *robustness* and the *uniqueness* properties are simultaneously and naturally achieved.

The advantages of Ising-PUF are summarized as follows:

uniqueness and robustness: Ising-PUF achieves a uniqueness of 50.1%, which is close to an ideal value of 50%. Further, with the help of the dedicated dark-cell elimination scheme (DCE), robustness of 2.26%, which is again close to an ideal 0%, is achieved.

Machine learning (ML) attack resistance: Even with a deep neural network (DNN), which is considered to be one of the most powerful ML models available today, the prediction accuracy remains 49.7%, which is close to that of a random guess (50%).

Availability of a compact secret model: Since Ising-PUF is a collection of multiple elemental PUFs, a compact "secret model" can be constructed by reading CRPs of all elemental PUFs, which facilitates to regenerate any CRPs.

The rest of this paper is constructed as follows. In Section II, basics of PUFs are briefly reviewed. Then, Section III details Ising-PUF architecture. The authentication protocol assumed in this paper is also described. Numerical experiments and their results are summarized in Section IV. Finally, in Section V, concluding remarks are provided.

II. Preliminaries

A. Physically Unclonable Function

PUFs can be classified into two subtypes: strong-PUFs and weak PUFs. Strong-PUFs are those that accept challenges and output the corresponding responses which are unique to each IC chip. Further, they are required to provide exponentially large CRPs to prevent their challenge-to-response mappings from being modeled accurately. APUF [3] and RO-PUF [5] are the well-known examples of strong PUF. Weak PUFs are the special case of the Strong-PUF that takes no challenge. An example of the weak-PUF is SRAM-PUF [17], [18] which utilizes the instability of power-on state of an SRAM cell. Although an SRAM bit cell is designed symmetric for storing logic 0 and 1, due to the manufacturing variability, each cell has a tendency to take either one of those, which can be used as the chip intrinsic fingerprint. Since the application of Weak-PUF is limited, such as secret key generation, we specifically focus on Strong-PUFs in this paper.

A typical construction of APUF is shown in Fig. 2. The multiplexers (MUXes) in the APUF pass through two input signals without changing the lanes when its challenge bit is "1." Otherwise, the signal lanes are swapped; inputs at the top and bottom signal lanes are lead to the bottom and top lanes, respectively. Even though the MUXes are identically designed, signal propagation delays of the straight and crossed paths are slightly different due to manufacturing variation. While signals pass through the MUXes, delay difference of the two signals is accumulated and finally converted into a binary output using the arbiter equipped at the end of the MUXes array.

B. Quality Metrics of PUF

Uniqueness and robustness are the two major metrics that define the quality of the PUFs. Uniqueness measures how different are the responses of two PUF instances. Specifically,

the uniqueness can be calculated as the average hamming distance (HD) between the responses of PUF-instance pair when the same challenge is applied. For an ideal PUF which produces uniformly distributed independent random bits, the uniqueness becomes 50%.

In addition to the uniqueness, PUF is required to reproduce the same response for the same challenge regardless of the operating condition. This characteristic is called robustness, which is calculated as the average HD of the responses of the same PUF instance when an identical challenge is repeatedly given. The ideal robustness is 0%, i.e., environmental change for a PUF has no impact on the CRPs.

In addition to attaining good uniqueness and robustness, PUFs are also required to be robust against ML or modeling attacks [19]. A general ML attack assumes the following situation: a malicious third party has an access to a subset of all CRPs and then they tries to derive a mathematical model that best predicts the responses for remaining challenges. Let us then take an APUF as an example target for ML attacks. According to the additive delay model [20], the delay difference between the upper and lower paths can be represented as $\Delta = \boldsymbol{w} \cdot \boldsymbol{x}$, where $\boldsymbol{w}$ are determined by the process variations and $\boldsymbol{x}$ is the function of the challenge input. Hence, the one-bit response (r) can be represented as $r = sign(\boldsymbol{w} \cdot \boldsymbol{x})$, where $sign(x)$ returns "0" when $x < 0$ and "1" otherwise. Due to this linearity, APUF is known to be vulnerable to ML attacks, i.e., only a few thousands of CRPs are sufficient to derive an accurate model for a target APUF [4].

C. Device Authentication Protocol

As a desirable property, responses of PUFs should not disclose any information inherent to the instance so that prediction of the remaining CRPs difficult or impossible even when the past CRPs are collected by a malicious third party. Considering these unique characteristics of PUFs, device authentication protocol based on PUFs are entirely different than that based on private key cryptographic systems. The following briefly summarizes the authentication protocol based on PUF [2].

During the manufacturing phase

(1) A manufacturer collects CRPs and securely stores them in the database on an authentication server.

(2) PUF instances are shipped to clients.

When device authentication is required

(3) A client sends an authentication request to the authentication server.

(4) In response to the request, the server picks N challenges $\{\boldsymbol{c}_1, \boldsymbol{c}_2, \cdots, \boldsymbol{c}_N\}$ and sends them to the client.

(5) The client obtains N responses $\{r_1, r_2, \cdots, r_N\}$, where r_i is the response of the PUF instance to the challenge $\boldsymbol{c}_i$, and submits them to the server.

(6) The server evaluates the difference between the received responses and that stored in the database (Hamming distance is typically chosen), and reports the result to the client. Finally, the CRP used for the authentication is discarded to prevent it from being reused in the future authentication.

Since CRPs that have been already used in authentication should be discarded, server must store sufficiently large CRPs so that they will not run out. In order to store all CRPs of a PUF that accepts N-bit challenges, a quite large storage of $\mathcal{O}(2^N)$ is required, which should be alleviated.

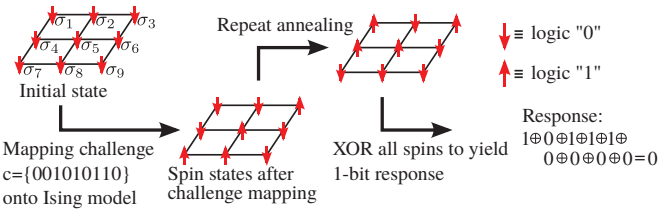


Fig. 3. Example operation of Ising-PUF.

III. Proposed Method

A. Concept

Inspired by the interaction of spins in Ising computing machines, this paper proposes *Ising-PUF*, a novel PUF architecture. Similar to the Ising model, Ising-PUF consists of a lattice like arrangement of cells, each of which contains an elemental PUF and a spin register that stores the response of the elemental PUF. Each spin register serves as a challenge to its neighbor cells, realizing mutual interactions among small PUFs.

Fig. 3 illustrates the procedure for Ising-PUF to convert a challenge into a response bit. First, all spin values are initialized to "0." Here, the two spin values, $+1$ and -1, are respectively represented by logic "1" and logic "0" in order to implement Ising model in a standard digital circuit. Then, a challenge $\boldsymbol{c} = c_0 c_1 \cdots c_N$ is mapped onto Ising model; spin value σ_i is inverted when c_i="1." In the example of Fig. 3, a 9-bit challenge of $\{001010110\}$ is given, so that the values of corresponding spins ($\sigma_3 \sigma_5 \sigma_7 \sigma_8$) are inverted. After the challenge mapping, "annealing" is invoked; a 1-bit response of the elemental PUF is generated being the spin values of its four neighbor cells as its challenge. The response is stored into the spin register, which again serves as a challenge to its neighbors. As each elemental PUF mutually interacts with its neighbors, chip-intrinsic spin patterns are formed, which is utilized as the fingerprint. After the annealing is sufficiently repeated, all the spin values are XOR-ed to yield a 1-bit response.

B. Basic Operation

Let us then briefly explain the basic operation of Ising-PUF having N spins. In the following, let $\boldsymbol{c} = \{c_1, c_2, \cdots, c_N\}$ be the N-bit challenge and σ_i be the binary value of i-th spin.

Step 1: Initialization All spin values are reset to "0," i.e., σ_i is set to "0" for $i = 1, 2, \cdots, N$.

Step 2: Challenge mapping Spin values are inverted according to challenge $\boldsymbol{c}$. Specifically, σ_i is inverted when c_i=1.

Step 3: Annealing Spin values are updated according to the interaction between neighbor spins. Each cell reads spin values of its neighbors and using them as a challenge, the elemental PUF yields the corresponding response bit, which is stored into the spin register. In an example of Fig. 1, spins of the four cells (up, down, left, and right) become the 4-bit challenge for the center cell. For example, the new spin value of fifth spin (σ_5^{t+1}) in Fig. 1, is calculated as $\sigma_5^{t+1} = f_5(\sigma_2^t, \sigma_4^t, \sigma_6^t, \sigma_8^t)$, where $f_5(\cdot, \cdot, \cdot, \cdot)$ is the 4-bit challenge-to-response mapping function of the elemental PUF embedded in the fifth spin and σ_i^t is the binary value representing the i-th spin state at time t. Again, each spin register serves as the challenge for its neighbor cells in the next annealing step, making the time development of spin values as chip intrinsic. The spin update is repeated for N_A times, to develop a chip-specific spin pattern. The update can be conducted very efficiently with hardware, in which all

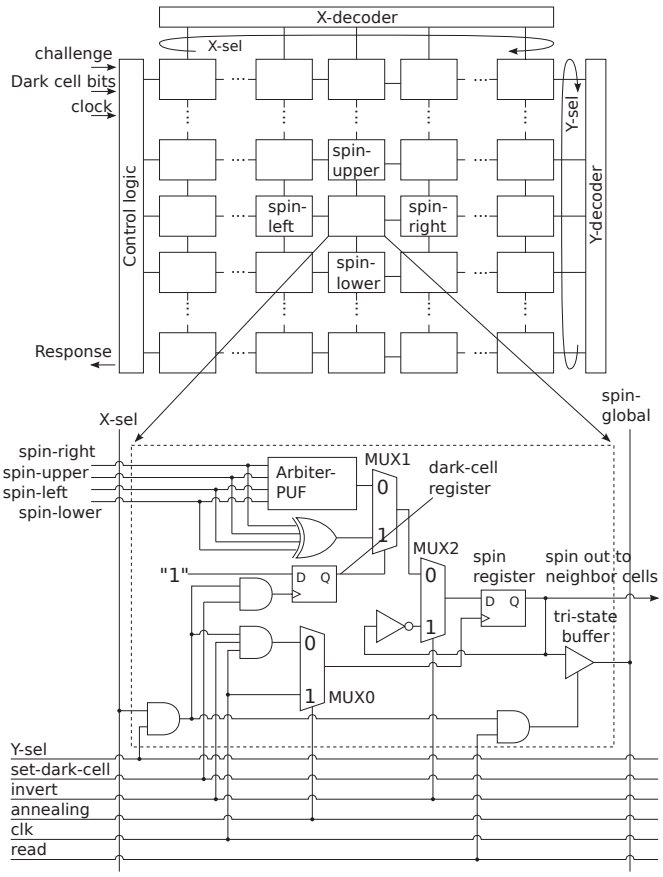


Fig. 4. Circuit structure.

spin values in a chip can be updated simultaneously within one clock cycle.

Step 4: Response generation After the annealing, all spin values are XORed and the resulting 1-bit response is transmitted as the response of the given challenge.

C. Circuit Structure

Ising-PUF is composed of an array of unit cells, X- and Y-address decoders, and a control circuit, as shown in Fig. 4. Within each cell exists an elemental PUF with 4-bit input, a 1-bit spin register, a 1-bit dark cell register, and a control circuit. In this study, an APUF is adopted as the elemental PUF, but any strong PUFs, such as BR-PUF or RO-PUF, can be used.

The circuit operation is summarized as follows. First, a challenge is mapped for the cells. By asserting "invert" in Fig. 4, the inversion of the spin register output is fed back to the spin register input through MUX2, which is captured at the next rising edge of "clk." In order to reduce circuit complexity, only a single spin selected by "X-sel" and "Y-sel" is inverted. The annealing is then invoked by asserting "annealing" signal, which causes the APUF output to be directed to the spin register through MUX1 and MUX2. The APUF converts the spin values of its four neighbor cells (up, down, left, and right) into a 1-bit response, which is stored into the spin register at the next clock cycle. After the annealing is sufficiently repeated, the "read" signal is asserted to invoke the read mode, in which the selected spin register is connected to the global wire. Again, single global wire is shared among all cells to simplify circuit structure. The spin registers are read in a serial manner by incrementing the X- and Y-address.

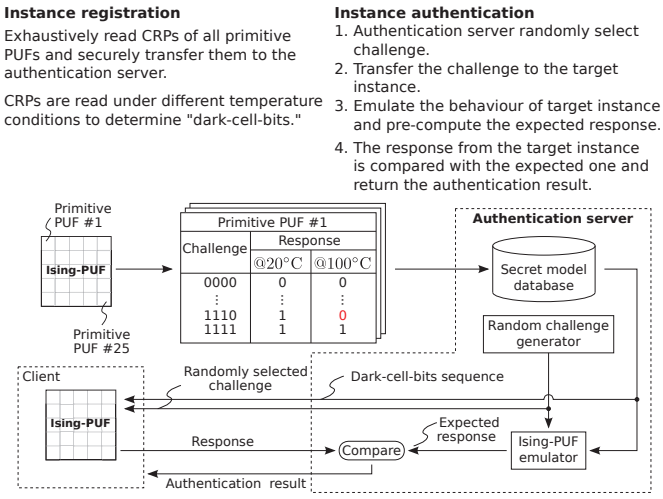


Fig. 5. Chip authentication protocol based on Ising PUF.

When transistor mismatch in the elemental PUF is insufficient, its output (APUF in this example) becomes uncertain. Depending on the temperature and/or supply voltage variation, the output of APUF changes even if an identical challenge is given. Such PUF is called a dark-bit [21]. An uncertain output of a dark-bit spreads gradually in the Ising-PUF, and finally corrupts the spin values of entire array. Hence, a new dark-cell elimination (DCE) scheme suitable for Ising-PUF is devised. Our DCE scheme does not just ignore the dark cell, but takes XOR of the challenge bits for the elemental PUF. Due to the nonlinearlity of XOR and as the dark-cell appears randomly in an array, the chaotic behavior of the Ising-PUF is maintained and uniqueness of entire PUF is not deteriorated.

In DCE scheme, the manufacture evaluates the robustness of all APUFs before shipping the PUF instance. The dark-cells are extracted and their locations on a chip are stored in the authentication server similarly with the CRPs. The cell circuit can be simplified by storing dark-cell bit written in on-chip NVM or one time programmable ROM, etc.

D. Authentication Protocol

Studying the chip authentication protocol explained in Section II, it is clear that one of the drawbacks of PUF-based authentication is the secure CRP collection. Prior to the instance authentication, CRPs of target PUF instance must be collected in a secure way, and should be transferred and stored in the authentication server. Further, once a CRP is used, it must be discarded and never used again to avoid an impersonation attack. Hence, the server requires a large storage for CRPs, deteriorating the cost advantage of PUF-based authentication.

A novel authentication protocol for Ising-PUF is also proposed to reduce the amount of secure CRP storage. Our proposal is based on the idea of "secret model" scheme [22], [2], in which an authenticator collects an associated secret model, with which full emulation of PUF behavior becomes possible. Instead of storing the raw CRPs, the authenticator calculates a response for any challenge whenever necessary. With the secret model, the capacity requirement of the secure CRP storage can be greatly reduced.

Fig. 5 illustrates the proposed authentication protocol based on Ising-PUF.

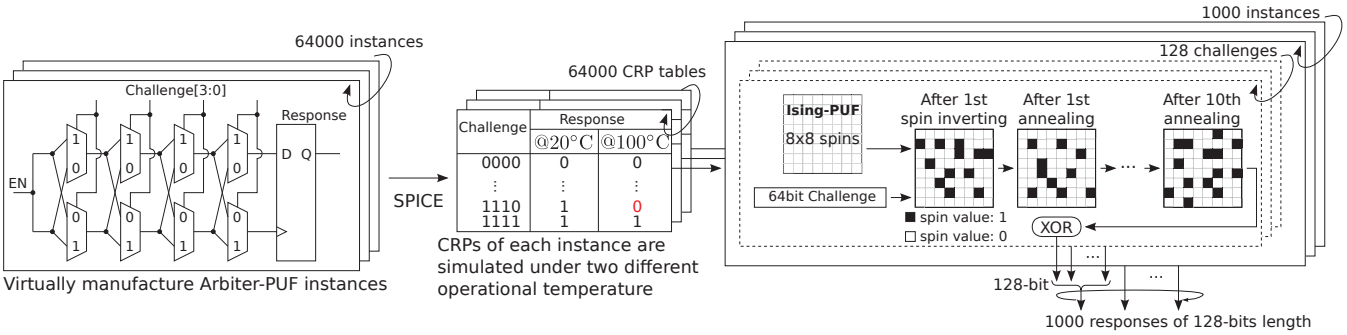


Fig. 6. Simulation flow.

Instance registration: Since Ising-PUF is a collection of multiple elemental PUFs, CRPs of each elemental PUF and the location of dark-bits are the sufficient information to fully emulate the temporal development of spin values. Hence, in the instance registration step, the manufacturer exhaustively reads CRPs for all elemental PUFs, and securely transfers them to the authentication server. In order to identify dark bits, the CRPs are read under different operational conditions. In the example of Fig. 5, the CRPs are read at two temperatures: 20°C and 100°C. The example in Fig. 4 shows difference for the challenge "1110," indicating that the elemental PUF#1 is a dark-bit, and hence its dark-cell-register is set. Each elemental PUF has only a small number of neighbors (which is equal to the challenge bits), such as four as in the example, the exhaustive reading is feasible in a short time. Note here that the secure storage space required in the authentication server increases linearly to the number of cells N_{cell}, which is drastic improvement from the conventional approach that requires an exponentially large secure storage space. For example, in order to store the all CRPs of a 64 bit APUF, a table with 2^{64} entries is required. On the other hand, an Ising-PUF having 8×8 cells requires a table of $2^4 \times 8 \times 8$ entries for storing CRPs of APUFs and an additional 8×8 bits for dark-bits storage, which corresponds to a 1.7×10^{16} times improvement.

Instance authentication: The authentication server randomly selects a challenge sequence and sends it to the Ising-PUF instance. Then, the server computes the expected response to the selected challenge using the stored secret model. Finally, the expected response is compared with the actual response from the instance and reports the comparison result to the client.

IV. Numerical Experiment

A. Experimental Setup

Thorough numerical experiments have been conducted to study the performance of the proposed Ising-PUF. In order to reduce the computational cost, an in-house mixed-signal simulator has been developed, in which arbiters and selector chains are accurately simulated by using a SPICE simulator and the behavior of the other digital circuit components are emulated by using a Python scripting language. Fig. 6 shows our experimental flow. First, 64,000 Arbiter-PUF instances are virtually manufactured using a commercial 65-nm CMOS PDK and their CRPs are simulated exhaustively by using a SPICE simulator. Then, based on the simulated CRPs, the behavior of 1,000 Ising-PUF instances consisting of 64(=8×8) cells is emulated. In the right part of Fig. 6 shows the simulation flow to obtain a single bit response. Since we simulated 1,000 Ising-PUF instances each of which takes 128 challenges, we finally obtain 1,000 response-bit streams each of which is 128 bits in length. On the obtained bit-streams, the followings are evaluated:

- Uniqueness and robustness of the Ising PUF.
- Vulnerability against machine learning attacks.

In order to identify dark-bits, the CRPs of Arbiter-PUFs are simulated comprehensively at two different temperatures: 20°C and 100°C. We regard the Arbiter-PUF being stable, if and only if all CRPs at the two temperatures match completely. Otherwise, Arbiter-PUFs are considered unusable and the corresponding dark-cell bits are set. In this experiment, approximately 10% to 40% Arbiter-PUF per a single Ising-PUF instance is identified as unstable.

The area required to implement Ising-PUF having 8×8 cells is estimated approximately 4.1 k gate equivalent (GE), while 64 bit DAPUF requires approximately 0.91 kGE.

B. Experimental Results

To evaluate the uniqueness of Ising-PUF, pair-wise HD between the 1,000 responses are computed. Fig. 7(a) shows the histogram of the calculated HD. The average inter-instance HD is 50.1%, which is very close to the ideal value of 50%.

We then evaluate the robustness of Ising-PUF. Fig. 7(b) summarizes the HD between a pair of responses across the temperatures of 20°C and 50°C. The averaged inter-temperature HD is 2.26%, which is again very close to the ideal value of 0%.

Finally, we evaluate the vulnerability of Ising-PUF against ML attacks. Three conventional PUFs (64 bit APUF [3], 64 bit BR-PUF [6], and 64 bit 3-1-DAPUF [8]) and Ising-PUF are virtually manufactured assuming the same 65 nm CMOS process and their challenge-response behaviors are simulated by using a SPICE, yielding 60,000 CRPs for each. The ML classifier is trained by using 50,000 CRPs and remaining 10,000 CRPs are used to evaluate the ML resilience.

Figs. 8(a) summarizes the results in which an SVM with a linear kernel is used to predict the challenge-response behaviors of three conventional PUFs and Ising-PUF. The X- and Y-axes correspond to the number of CRPs used to train the SVM-based binary classifiers and the prediction accuracies, respectively. The prediction accuracies of the conventional PUFs are shown in black lines while that of Ising-PUF is shown in red. CRPs of APUF and BR-PUF were successfully predicted by the simple linear classifier, indicating their vulnerability to ML attacks. Due to the nonlinear challenge-response relationships, the linear SVM failed to predict the response of the 3-1-DAPUF and Ising-PUF.

The ML attack tolerance has been further investigated by using more advanced binary classifier based on a deep neural

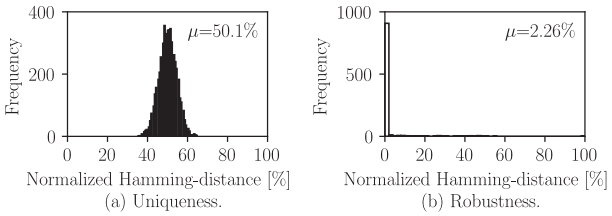


Fig. 7. (a) Uniqueness and (b) robustness of Ising-PUF.

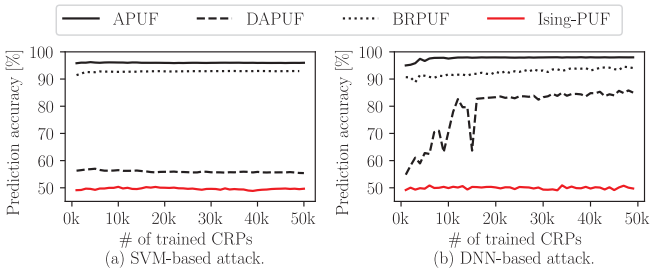


Fig. 8. ML-attack tolerance. (a) SVM and (b) DNN are used as binary classifier.

network (DNN), whose results are summarized in Fig. 8(b). In this experiment, a multilayer neural network (NN) having four fully connected layers is utilized. Contrary to [10], in which an NN is utilized only to extract feature vectors from challenge inputs, our DNN-classifier is trained in an end-to-end manner, i.e., the feature extraction and the succeeding classification stages are jointly trained. In Fig. 8(b), the black and the red lines again shows the prediction accuracies of the conventional PUFs and Ising-PUF, respectively. By employing the DNN to build a prediction model, the prediction accuracy of the CRPs for 3-1-DAPUF increased to 88% while that of Ising-PUF still maintains 50%, demonstrating the excellent tolerance of Ising-PUF to ML attacks. We also notice that, as the number of training samples increases, the prediction accuracy of 3-1-DAPUF increases gradually, while that of Ising-PUF remains 50% up to 50,000 training samples, which also demonstrates an excellent ML attack tolerance of Ising-PUF.

V. Conclusion

In this paper, we proposed Ising-PUF, a novel PUF circuit that utilizes chaotic behavior of mutually connected small PUFs in an Ising-model like array to generate chip's "fingerprint." Experimental results show that Ising-PUF with 8×8 spins exhibits the average inter-instance HD of 50.1% and the inter-environment HD of 2.26%, both of which are very close to the ideal values of 50% and 0%. An outstanding tolerance of Ising-PUF to the ML attacks is also demonstrated; even if the advanced DNN is employed, the prediction accuracy remains ideal 50% after using 50,000 training samples. Further, Ising-PUF is suitable for secret-model based authentication and hence a large secure CRP database can be alleviated, which reduce the authentication cost.

Acknowledgment

This work was partially supported by MEXT/JSPS KAKENHI Grant No. 17H01713. The authors also acknowledge support from VDEC with the collaboration with Synopsys Corporation.

References

[1] "Amazon Dush Button," https://www.amazon.com/Dash-Buttons/b?ie=UTF8&node=10667898011.
[2] 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.
[3] S. Devadas, E. Suh, S. Paral, R. Sowell, T. Ziola, and V. Khandelwal, "Design and Implementation of PUF-Based "Unclonable" RFID ICs for Anti-Counterfeiting and Security Applications," in *IEEE Int. Conf. on RFID*, April 2008, pp. 58–64.
[4] G. Hospodar, R. Maes, and I. Verbauwhede, "Machine learning attacks on 65nm Arbiter PUFs: Accurate modeling poses strict bounds on usability," in *Int. Workshop on Information Forensics and Security*, Dec 2012, pp. 37–42.
[5] G. E. Suh and S. Devadas, "Physical Unclonable Functions for Device Authentication and Secret Key Generation," in *Design Automation Conf.*, June 2007, pp. 9–14.
[6] 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.
[7] 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.
[8] T. Machida, D. Yamamoto, M. Iwamoto, and K. Sakiyama, "Implementation of double arbiter PUF and its performance evaluation on FPGA," in *Asia and South Pacific Design Automation Conf.*, Jan 2015, pp. 6–7.
[9] X. Xu, U. Rührmair, D. E. Holcomb, and W. Burleson, "Security Evaluation and Enhancement of Bistable Ring PUFs," pp. 3–16, 2015. [Online]. Available: https://doi.org/10.1007/978-3-319-24837-0_1
[10] R. Yashiro, T. Machida, M. Iwamoto, and K. Sakiyama, "Deep-Learning-Based Security Evaluation on Authentication Systems Using Arbiter PUF and Its Variants," in *Advances in Information and Comput. Security*. Springer International Publishing, 2016, pp. 267–285.
[11] 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.
[12] E. Ising, "Beitrag zur Theorie des Ferromagnetismus," *Zeitschrift für Physik*, vol. 31, no. 1, pp. 253–258, 1925.
[13] 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.
[14] M. Yamaoka, C. Yoshimura, M. Hayashi, T. Okuyama, H. Aoki, and H. Mizuno, "20k-spin ising chip for combinational optimization problem with CMOS annealing," in *Int. Solid-State Circuits Conf.*, Feb 2015, pp. 1–3.
[15] 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.
[16] G. Boeing, "Visual Analysis of Nonlinear Dynamical Systems: Chaos, Fractals, Self-Similarity and the Limits of Prediction," *Syst.*, vol. 4, no. 4, 2016.
[17] J. Guajardo, S. S. Kumar, G.-J. Schrijen, and P. Tuyls, "FPGA Intrinsic PUFs and Their Use for IP Protection," in *Int. Workshop on Cryptographic Hardware and Embedded Syst.*, 2007, pp. 63–80.
[18] D. E. Holcomb, W. P. Burleson, and K. Fu, "Power-Up SRAM State as an Identifying Fingerprint and Source of True Random Numbers," *IEEE Trans. Comput.*, vol. 58, no. 9, pp. 1198–1210, Sept 2009.
[19] U. Rührmair, J. Sölter, F. Sehnke, X. Xu, A. Mahmoud, V. Stoyanova, G. Dror, J. Schmidhuber, W. Burleson, and S. Devadas, "PUF Modeling Attacks on Simulated and Silicon Data," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 11, pp. 1876–1891, Nov 2013.
[20] M. Majzoobi, F. Koushanfar, and M. Potkonjak, "Testing Techniques for Hardware Security," in *Int. Test Conf.*, Oct 2008, pp. 1–10.
[21] 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.
[22] M. Majzoobi and F. Koushanfar, "Time-Bounded Authentication of FPGAs," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 1123–1135, Sept 2011.