BoardPUF: Physical Unclonable Functions for Printed Circuit Board Authentication

Lingxiao Wei[†‡], Chaosheng Song[†], Yannan Liu[†], Jie Zhang[†‡], Feng Yuan[†‡] and Qiang Xu[†‡]

[†]CUhk REliable Computing Laboratory (CURE)
Department of Computer Science & Engineering
The Chinese University of Hong Kong, Shatin, N.T., Hong Kong
[‡]Shenzhen Research Institute, The Chinese University of Hong Kong
Email: {lxwei, cssong, ynliu, jzhang, fyuan, qxu}@cse.cuhk.edu.hk

ABSTRACT

Physical Unclonable Functions (PUFs) are cryptographic primitives that can be used to generate volatile secret keys for cryptographic operations and enable low-cost authentication of integrated circuits. Existing PUF designs mainly exploit variation effects on silicon and hence are not readily applicable for the authentication of printed circuit boards (PCBs). To tackle the above problem, in this paper, we propose a novel PUF device that is able to generate unique and stable IDs for individual PCB, namely BoardPUF. To be specific, we embed a number of capacitors in the internal layer of PCBs and utilize their variations for key generation. Then, by integrating a cryptographic primitive (e.g. hash function) into BoardPUF, we can effectively perform PCB authentication in a challenge-response manner. Our experimental results on fabricated boards demonstrate the efficacy of BoardPUF.

1. INTRODUCTION

Counterfeit products not only result in revenue loss and reputation damage to victim companies, but also cause severe reliability and security vulnerabilities for customers. As reported by US Department of Commerce [1], counterfeiting accounts for more than 8% of global merchandise trade, which is in the trillion dollars range. In particular, counterfeit electronics are increasingly being distributed throughout the market and legitimate electronic companies miss out on about $100 billion of global revenue every year because of counterfeiting, thereby posing a severe threat to the global electronic supply chain [2]. Printed Circuit Board (PCB), as a basic component of electronic systems, can be easily counterfeited by reverse engineering the legitimate copies. From another perspective, critical systems that employ counterfeit PCBs may suffer from performance degradation and security threat. The result of investigation done by Ghosh [3] showed that counterfeit PCBs with malicious modification or Trojan inserted can cause system failure and sensitive information loss. Therefore anti-counterfeit solutions for PCBs are in an urgent need for electronic systems' security.

From security engineering standpoint, anti-counterfeiting can be formulated as an authentication problem. Consequently, we could rely on a unique ID to differentiate between counterfeits and legitimate products. Various techniques have been presented in the literature to generate unique IDs for IC products [4]. In particular, physical unclonable function (PUF), first introduced by Gassend *et al.* [5] based on inevitable manufacturing variations, can be used to generate unpredictable and unclonable IDs. However, there are very few effective authentication solutions for PCBs. Commercial solutions such as [6] and [7] rely on a dedicated secure chip integrated into the system. However, since the secure chip itself (recycled or from overproduction) can be assembled onto a counterfeit PCB, even if the ID itself is unpredictable and unclonable, we cannot guarantee the board is authentic. A counterfeit PCB detection method is proposed recently [8] based on the measurement of trace impedance using dedicated testing equipment. Their method mainly focused on the potential attacks on the supply chain from PCB designers to system designers. Though they've showed effective PCB authentication, the method is hard to automate and is not applicable for attacks after deployment.

Motivated by the above, in this work, we propose to construct a physical unclonable function for PCB in a fully automatic way, leveraging the manufacturing variations of the board itself. The proposed solution, namely *BoardPUF*, consists of a number of capacitive copper patterns fabricated within the PCB to reflect manufacturing variation and a dedicated secure chip that connects to these units for ID generation. In order to ensure high-quality PUF design in terms of uniqueness and robustness, on the one hand, we try to design PCB capacitive patterns in such manner that PCB fabrication variation effects can be maximized; on the other hand, the ID generation strategy in BoardPUF is tailored for the characteristics of PCB variations. We fabricate one hundred boards to validate the proposed solution and results show that both the uniqueness and robustness of BoardPUF are quite high.

The rest of the paper is organized as follows. Section 2 introduces the preliminary of PUF designs. Section 3 presents our proposed solution. Potential attacks and defense methods on BoardPUF are then discussed in Section 4. Experimental results in Section 5 validate the effectiveness of BoardPUF and finally Section 6 concludes the paper.

2. PRELIMINARIES

There exist a number of different PUF designs for integrated circuits, such as arbiter PUF [5], ring oscillator (RO) PUF [9], SRAM PUF [10], and butterfly PUF [11]. Arbiter PUF outputs are based on a digital race condition which is determined by process variation in two paths on chip. RO PUF captures the difference of delay from a pair of ROs. The above two PUFs utilize the delay characters on silicon. SRAM PUF is based on the fact that a SRAM cell logically constructed as two cross-coupled inverters would initialize to a random value due to the mismatch of cell when powering up. Butterfly PUF imitates the SRAM cell by using two cross-coupled transparent latches on FPGA to generate unique bits on every clear/preset actions.

Generally speaking, PUFs should have unpredictable, robust and unclonable [12] characteristics. The unpredictable characteristic means that each PUF instance should have an unique response. The robust characteristic means that PUF

978-1-4673-8388-2/15/$31.00 ©2015 IEEE

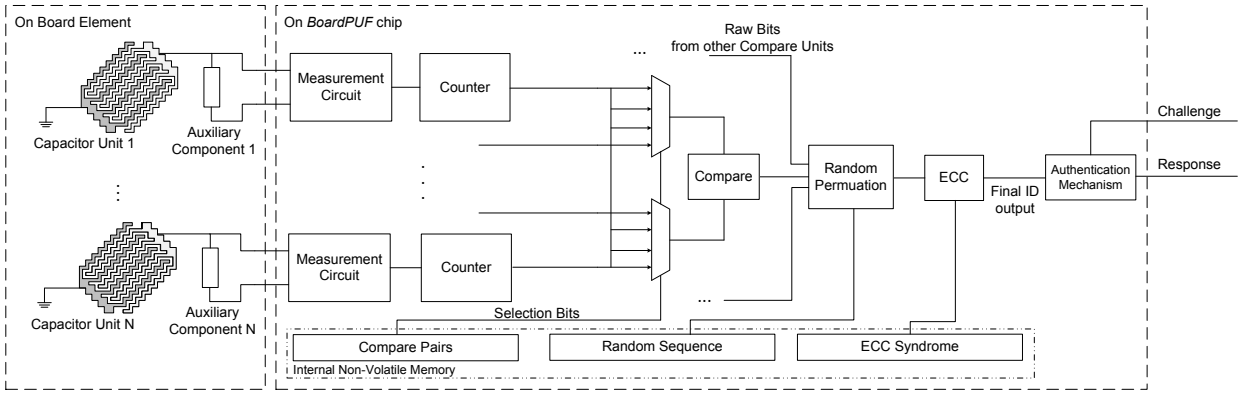


Figure 1: BoardPUF Architecture

instance should generate the same response in different environments. The unclonable characteristic means an adversary cannot replicate a PUF that emulates the original one, and it is generally guaranteed by uncontrollability of process variations in manufacturing process.

PUFs are widely used for authentication. Among all authentication methods, the concept of challenge-response pairs is the most prominent one. A challenger can authenticate an entity (PUF instance) by sending a challenge or a query to it and verify the response returned by the entity in a database maintained by a trusted third-party. In reality, the PUF designer keeps a database storing the challenge-response pair for every legitimate PUF instances. The customers or users can verify the product by challenging the PUF instances on it. In order to prevent from replay attacks, every challenge-response pair can only be used once and then shall be deleted from the database.

Existing PUF designs are mainly used for the IC authentication, and they are not readily applicable for PCB authentication, simply because such designs do not contain any variation source from the PCB. The above has motivated the proposed solution for PCB authentication.

3. METHODOLOGY

The purpose of BoardPUF is to generate an ID for Printed Circuit Board and to resolve the challenges arising from limited on-board variations. The ID then can be used for a reliable authentication of PCB. In this section, we present the detail design of BoardPUF. The overall architecture is shown in Figure 1.

3.1 Overview

The architecture of BoardPUF mainly contains two parts, the variation sources fabricated on board and a *BoardPUF* chip performing measurement and authentication. The intuition behind why BoardPUF works is based on the intrinsic variation during the PCB manufacturing.

The variation sources are capacitor units which are composed of a set of well-designed copper patterns and placed between layers of PCB, to reflect the variation of PCB during the manufacturing process, to be detailed in Section 3.2. Each capacitive unit, together with auxiliary components (e.g, resistors), is connected to I/O pins of the dedicated chip, like in Figure 2.

Due to the variations of manufacturing, every capacitor unit on board would generate different frequencies by capacitive sensing circuits in the PUF chip, which to be detailed in Section 3.4. A counter is used to record the signal generated

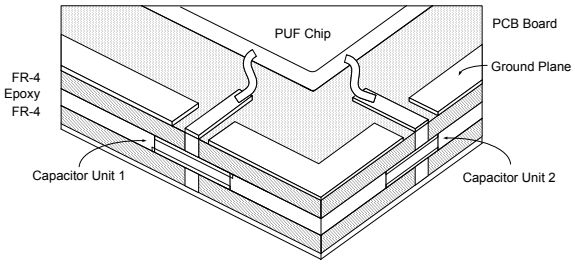


Figure 2: The connection between capacitor units and dedicated IC

by each sensing circuit in a definite time. Then BoardPUF loads the list of compare pair list form internal non-volatile memory (NVM) and generates a set of response bit by compare the counts between two capacitor units which is specified by compare pairs. The final ID is generated by permuting the bits from compare unit using a random sequence which is also pre-stored in the NVM. Compare pairs and random sequence are generated at "calibration" stage, to be detailed in Section 3.5, before BoardPUF is shipped to customers. Error Correction Code (ECC) is used to correct burst bit errors in the final ID. This ID shall be invisible from a challenger who wants to authenticate PCB, but it is archived by PUF designers. By integrating a cryptographic primitive, the PCB can be authenticated in a challenge-response way.

In order to achieve a robust PUF design on PCB variation, Section 3.3 presents how to increase the relative difference of capacitance of on-board units by organizing them in different rotational angles. Two techniques, embedding random sequence and compare pair generation, are introduced in Section 3.5, which are used to enhance the randomness of the final ID, considering the characteristics of PCB variations.

3.2 PCB Capacitor Unit

In this subsection, we introduce a two-layer comb-shaped pattern fabricated on PCB as in Figure 4, which can be modeled as a capacitor, and analyze how it can reflect the manufacturing variation.

3.2.1 Capacitor Structure

For capacitors on board, the basic requirement is that they should manifest enough variations of manufacturing for measurement while maintaining a relative large capacitance, compared to on-board parasitics, for noise immunity at the same time.

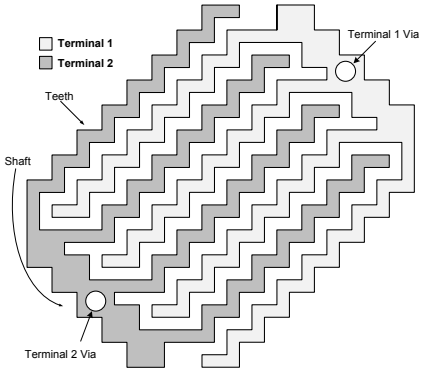


Figure 3: Comb-shaped capacitor structure in one layer

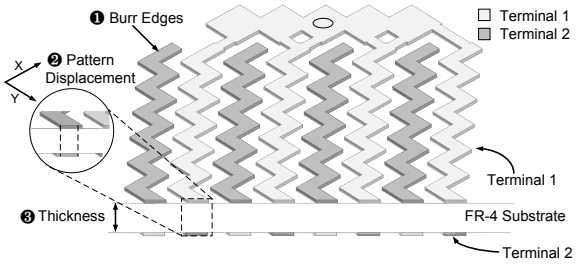


Figure 4: 3-D structure and Variation Source

The capacitor is designed in two layers of PCB with two terminals. Each terminal is composed of several zig-zag copper traces connecting together as in Figure 3 within one layer, forming a comb shape. The same pattern is also fabricated on the other layer and connected by vias on the "shaft". Two terminals are interdigitated together. Thus every "teeth" is surrounded by "teeth" of another terminal, generating lateral and vertical electrical field when charged. Total capacitance is contributed by both vertical and lateral electrical field component. In order to reduce the noise, the capacitor structure is "buried" into the internal layers of PCB and protected with uninterrupted ground planes, as that in Figure 2.

The lateral capacitance formed by interdigitated "teeth" helps to achieve higher capacitance density on PCB because the distance between "teeth" can be very small in today's manufacturing capability.

3.2.2 *Variation Source*

First, in order to magnify the effect of variation, the parameters of PCB capacitor units are chosen to be very close to the capability of PCB manufacturers. Then the manufacturing errors would cause relative large variations of PCB capacitance.

Before analyzing the variation of proposed capacitor, we first review the manufacturing process of PCBs: 1) desired copper patterns are produced by methods of etching away unwanted copper on board substrate for every layer of PCB. 2) All patterned layers are stacked over together and laminated under high temperature and pressure. 3) Vias are drilled by either mechanical drills or laser. 4) Solder mask is applied on a rinsed PCB and exposed copper is coated with solder or other anti-corrosion coatings.

The imprecise manufacturing process would cause following effects, listed in Table 1 and Figure 4, affecting the capacitance of our proposed structure.

Burr edge results from imperfect chemical etching stage.

Table 1: Categories of Variations in PCB manufacturing

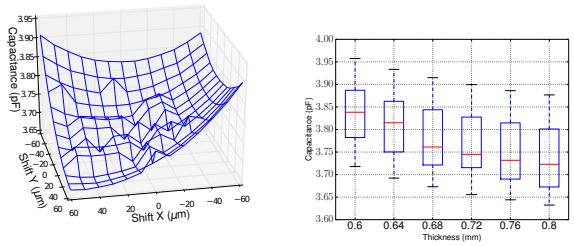
PCB Variation	Global	Local
❶ Burr edges		✓
❷ Pattern displacement	✓	✓
❸ Thickness	✓	

The shape of copper pattern may varies little from units to units due to displacement of traces when fabricate the pattern mask. The misalignment of layers during lamination also contributes to pattern displacement. Finally, the thickness of the each board cannot be guaranteed identical when produced and laminated.

Chemical etching and trace displacement affects every units on board independently, thus they are local variations. Global variations arise from the change of thickness and layer shift in lamination process which are the same for all capacitors on the same board. All three effects would vary internal electrical field of capacitor and change its capacitance.

3.2.3 *Simulation*

We simulate the proposed capacitive structure using ANSYS Maxwell [13], a electromagnetic field emulation software based on finite element method (FEM). According to typical PCB manufacturer's ability [14], we set the width of copper traces to 0.2mm, the space between two adjacent traces to be 0.2mm also and the thickness of one board is 0.7mm. The total size of one capacitor unit is 4mm × 6mm. The capacitance is calculated by sweeping displacement from -0.06mm to 0.06mm in both X and Y direction between layers and thickness from 0.6mm to 0.8mm. The result is shown in Figure 5. Figure 5(a) illustrates the relation between capacitance and the displacement in 2 direction when the thickness of board is set to 0.7mm. Figure 5(b) is a box diagram showing the capacitance distribution when we change the thickness. The red line in each box is the average value of capacitance simulated in this thickness. The capacitance ranges from 3.6pF to 4.0pF and the maximum variations is around 10%.



(a) Displacement (b) Thickness

Figure 5: Simulation of Capacitance

3.3 Organization of capacitor units

Robustness, or stability, is the basic requirement of a PUF design. Sufficient difference among variation sources is the key factor to ensure robustness. Otherwise, small environmental change or measurement error would have a great impact on the stability of ID generation. Although simulation in Section 3.2 has shown there are enough variations among fabricated capacitor units in total, only local variations would contribute to the differences when we consider all capacitor units on one board. Typically the local variation is smaller than the global variation [14].

In this section, we propose to organize the capacitor units in a simple yet effective way to magnify the differences between two units by rotating each one with a different angle. Rotation can be viewed as a function that maps global layer shift into the pattern displacement(❷ in Figure 4) of every capacitor unit, using angle as a parameter.

We use Δx_i and Δy_i to represent the total displacement of capacitor unit i in X and Y dimension respectively. Δx_g and Δy_g are global layer shift, Δx_{il} and Δy_{il} are the local displacements of unit i. θ_i is the rotational angle.

The displacement without rotation is shown in Equation 1.

$$\begin{pmatrix}\Delta x_i \\ \Delta y_i\end{pmatrix} = \begin{pmatrix}\Delta x_g \\ \Delta y_g\end{pmatrix} + \begin{pmatrix}\Delta x_{il} \\ \Delta y_{il}\end{pmatrix} \quad (1)$$

The total pattern displacement of capacitor unit i can be represented by Equation 2.

$$\begin{aligned}\begin{pmatrix}\Delta x_i \\ \Delta y_i\end{pmatrix} &= \begin{pmatrix}\cos\theta_i & -\sin\theta_i \\ \sin\theta_i & \cos\theta_i\end{pmatrix}\begin{pmatrix}\Delta x_g \\ \Delta y_g\end{pmatrix} + \begin{pmatrix}\Delta x_{il} \\ \Delta y_{il}\end{pmatrix} \\ &= \begin{pmatrix}\Delta x_{ig} \\ \Delta y_{ig}\end{pmatrix} + \begin{pmatrix}\Delta x_{il} \\ \Delta y_{il}\end{pmatrix}\end{aligned} \quad (2)$$

If we represent the capacitance C of on-board unit as a function f_t (determined by thickness, as we only consider the effect of layer displacement) in terms of the displacement in X and Y direction:

$$C = f_t(\Delta X, \Delta Y)$$

We consider the difference between two capacitor unit i and j without and with rotation by Taylor Expansion:

Without rotation:

$$\begin{aligned}|C_i - C_j| = |&\frac{\partial}{\partial x} f_t(\Delta x_g, \Delta y_g)(\Delta x_{il} - \Delta x_{jl}) + \\ &\frac{\partial}{\partial y} f_t(\Delta x_g, \Delta y_g)(\Delta y_{il} - \Delta y_{jl})| + \\ &o(\Delta x_{il}, \Delta y_{il})\end{aligned} \quad (3)$$

With rotation:

$$\begin{aligned}|C_i - C_j| = |&f_t(\Delta x_{ig}, \Delta y_{ig}) - f_t(\Delta x_{jg}, \Delta y_{jg}) + \\ &\frac{\partial}{\partial x} f_t(\Delta x_{ig}, \Delta y_{ig})\Delta x_{il} - \frac{\partial}{\partial x} f_t(\Delta x_{jg}, \Delta y_{jg})\Delta x_{jl} + \\ &\frac{\partial}{\partial y} f_t(\Delta x_{ig}, \Delta y_{ig})\Delta y_{il} - \frac{\partial}{\partial y} f_t(\Delta x_{jg}, \Delta y_{ig})\Delta y_{jl}| + \\ &o(\Delta x_{il}, \Delta y_{il})\end{aligned} \quad (4)$$

Assuming the local variations are relative small than global variation and are similar among different units, the sum of four products with local variation item in Equation 4 is of same magnitude with total difference in Equation 3. The left part $f_t(\Delta x_{ig}, \Delta y_{ig}) - f_t(\Delta x_{jg}, \Delta y_{jg})$ is the additional discrepancy we want to get from rotating capacitor units. As the global shift varies from one board to another, the difference between two units also varies across boards.

Based on the Maxwell simulation data, we build a model to predict the capacitance of capacitor unit in terms of three variation sources. We estimate the effects of rotation using parameters in [14]. 1000 boards with 48 capacitor units on each board are simulated and rotation angles are assigned with angles distributed in range $[0, 2\pi)$. The result is that average standard deviation of all capacitances increases from 0.009pF to 0.022pF after rotation.

However, one thing should be noted that rotation does not increase the security level of BoardPUF. It is because rotation is set for all manufactured board, thus does not provide an additional variation sources. Potential adversaries can feasibly obtain the rotation angle for each capacitor by reverse engineering.

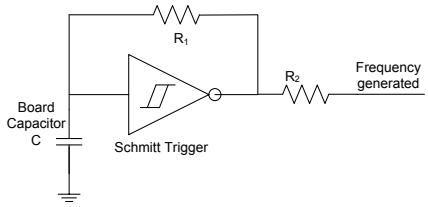


Figure 6: Measurement Circuit for capacitor

3.4 Capacitor Sensing

Capacitor Sensing Circuits are used to convert capacitor value to measurable physical quantity, such as voltage, frequency, etc. We built a relaxation oscillator based on Schmitt trigger, whose frequency is dependent on the capacitance under measure. We adopted it for better noise immunity and sensitivity of capacitance change. The measurement schematic is shown in Figure. 6. The oscillation frequency is determined by:

$$f = \frac{1}{K} \times \frac{1}{R_1 \times C}. \quad (5)$$

K is a value determined by the supply voltage. R_2 is a resistor to isolate the measurement circuit from noises in latter phases.

3.5 Calibration

PUF Designers are always reminded with two core requirements, uniqueness and robustness. In order to improve these two properties, many schemes have been proposed to generate response bit from measurement of variations (e.g., 1-of-k coding [5]). Randomness can by ensured by leveraging regression-based distiller [15] to remove systematic variations. In this subsection, we employ two techniques tailored for bits generations considering the characteristics of on-board capacitor units. An additional random sequence is produced to add on the randomness of generated bits and a sequence pairing algorithm is adopted to generate compare pairs on the runtime. Both stages are finished in a so-called "calibration" procedure when the BoardPUF is produced in a safe environment. The results are stored into a on-chip non-volatile memory.

3.5.1 Random Sequence

It is known that bits generated by PUF suffer from reduced randomness because of systematic variation on the chip die [15]. The systematic variations also occur on the capacitor units we fabricated on PCB, because the global shifts of different board are sometimes correlated, especially after rotating on-board units to enhance the stability. The correlated global shift may result from the situation that some boards are cut from a PCB array which is an large panel containing repeated individual boards. Simulation has done, in Figure. 7, to show the correlation between capacitor units on different boards. The reason why existing entropy enhancement technique like [15] does not fit into the authentication of PCB is that the local variation is not as large as that on chip die.

We resort to employ a random sequence to break the correlation between each board, which is used to permute final bits in the runtime evaluation. The sequence is generated by PCB manufacturer when the on-board capacitor units are ready and stored into the NVM of BoardPUF chip in a safe environment. For the sake of security, these random sequences shall be kept confidential.

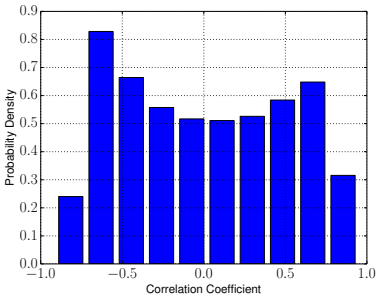


Figure 7: Correlation Coefficient Distribution between different boards

3.5.2 *Compare Pair Selection*

The PUF designers are supposed to test and record the frequency of each capacitor sensing circuit at two extreme environment conditions (usually in different temperatures) after the board and BoardPUF chip are ready. First we filtered out those capacitor units that generates unstable frequency. We then adopted Sequential Pairing Algorithm (SPA) [16] with modification to generate compare pairs. The original SPA sorts the frequency and selects pairs whose ranking difference is larger than $\lfloor N/2 \rfloor$ among total N frequencies. The frequency discrepancy of every pair exceeds a preset threshold Δf. Our selection scheme choose those pairs that ranking difference larger than ΔR to improve uniqueness. We present the modified selection algorithm in Algorithm 1.

Algorithm 1: SEQUENTIAL PAIRING (MODIFIED)

Input: List of tuple containing maximum and minimum frequency of every capacitor, Frequency Discrepancy Δf, Ranking Difference ΔR
Output: List of Compare Pairs{i, j}

```
Sort the tuple in the descending order by its f_min and
stored them in list L;
i ← 0;
for j ← ΔR to N − 1 do
    if L[j].f_min − L[i].f_min ≥ Δf and
    L[j].f_max − L[i].f_max ≥ Δf then
        Create Pair (i, j);
        i ← i + 1;
    end if
end for
```

4. ATTACKS AND DEFENSES

Various attacks on Silicon PUFs have been reported in the literature, e.g., machine learning algorithms [17] on challenge-response pairs, gate-level characterization [18] on side channel information leakage, and key recovery attack [19] on public helper data. All these attacks are based on the assumption that attackers are able to run their algorithms effectively and/or retrieve enough information for internal structure modeling. Our BoardPUF is ID-based and challenge response pair only interacts with embedded cryptographic primitive, not altering the internal structure of PUF, thus adversaries are unable to obtain enough information-rich data, which unveiled the internal parameters, from the operations of BoardPUF. Also, the helper data containing compare pairs, random sequence and ECC syndromes are securely stored inside PUF chip, and it is very difficult, if not impossible, for attackers to manipulate them for key-recovery.

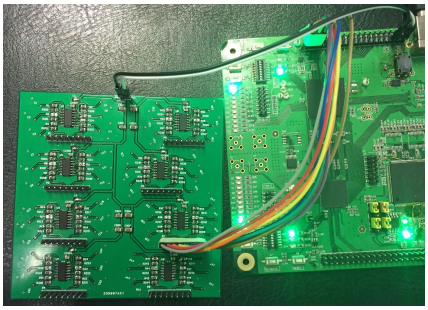


Figure 8: Experimental Setup

Another possible threat comes from physical inspection. As we utilize off-the-chip elements for secret generation, the signals on board, e.g. the wires which directly connected to capacitor units, can be measured by an oscilloscope. Attackers may expect to reverse the internal secret from their measurements. However, measurement itself (e.g., using an oscilloscope), incurs innegligible parasitic capacitance on its probe, and usually the capacitance is of the same magnitude with capacitor units, around 10pF [20]. When the probe is put on the measured signal, the equivalent capacitance would be dramatically affected by the probe, thus the attackers would fail to retrieve the genuine frequency on board.

Finally, let us consider an extreme attack scenario wherein attackers are able to produce a number of counterfeit printed circuit board with the proposed capacitor units. They desoldered a BoardPUF chip from genuine board and resoldered it onto the counterfeit boards, and hoped to generate the exact same ID to replicate challenge-response pair. We would measure this security property in Section 5 via experiment. Based on this concept, we defined a new metric called Inter-Board-Intra-Chip (IBIC) distance. Though the bits generated in this situation fails to achieve high entropy as that in normal case, the result is still acceptable considering the cost that the attacker has to pay for fabricating large numbers of counterfeit PCBs.

5. EXPERIMENTAL RESULTS

5.1 Experimental Setup

We designed a 4-layer PCB with the proposed capacitor units and sensing circuits. And we fabricated 100 boards to validate our proposed BoardPUF solution. Each capacitor is designed as in Section 3.2 with 0.2mm wire width and 0.2mm spacing. Each board contains 48 capacitor units, connected with auxiliary resistors of 1MΩ to 8 Hex-inverting-Schmitt-trigger chips (74HCT14) and each unit is rotated with an angle in $[0, 2\pi)$. The size of the entire board is within 10cm × 10cm. For the sake of simplicity, we adopted a Xilinx Spartan-6 FPGA to perform response bit generation instead of fabricating a dedicated IC. The output of Schmitt triggers are connected to the FPGA for bits generation. Every Schmitt trigger is connected to a counter inside FPGA and the counter's value is recorded every 0.67s. According to our strategy to generate bits, the frequency discrepancy in modified SPA is 100Hz while the ranking discrepancy is set to 4. We choose to generate a 24-bit ID in total. Figure 8 is a picture showing our experiment setup. The left board is the PCB to be tested with capacitor units "buried" into the internal layers while the right board is the FPGA board performing PUF functions.

The test was run both at room temperature around 25°C and at an incubator, shown in Figure 9 controlled at 35°C,

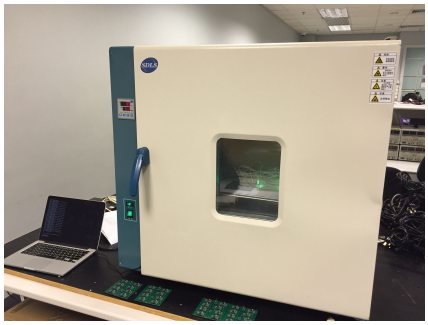


Figure 9: Incubator for Stability Test

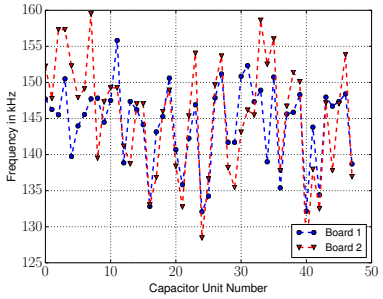


Figure 10: Frequency on two different boards

45°C, 55°C and 65°C, respectively. We also tested the performance of BoardPUF in 3 different voltages, 4.5V, 5.0V and 5.5V.

Generally speaking, there are two metrics, inter-distance and intra-distance, used to evaluate the uniqueness and robustness of PUF design. Inter-distance measures the Hamming Distance (HD) of ID generated by two distinct BoardPUF chip on distinct PCB, while intra-distance is the HD between IDs generated by the same BoardPUF and PCB in different environmental conditions. For a good PUF design, the average inter-distance shall be around 50% of total bit length, the average intra-distance is close to 0%. Besides the above two metric, the BoardPUF shall also be able to produce different IDs for different PCBs even if the BoardPUF chip remain the same. We adopt another metric called inter-board-intra-chip (IBIC) distance, evaluating the ability to differentiate two boards soldered with the same authentication chip. IBIC distance is the Hamming Distance between two IDs generated from the same PUF chip connecting to two different PCBs. The ideal value of IBIC distance is 50% in expectation.

5.2 Results and Discussion

First we report the average frequency generated by our capacitor sensing circuit. The frequency ranges from 130kHz to 158kHz under 5V at room temperature, with an average of 146.2KHz. According to the Equation 5 in Section 3.4, while K is approximately to be 1 at 5V [21], the equivalent capacitance is 6.84pF. This capacitance is around 3pF larger than the simulation result in Section 3.2. This is because connecting on board elements would inevitably bring in the capacitive parasitics of chip package. Routing wires on PCB also contribute to equivalent capacitance as an additional sources. [22] has provided typical capacitance value of different packages, and all are within the range from 0.3pF to 2.6pF. In fact, the final oscillation frequency is determined by a mixed variation source, but the on-board capacitor unit is the dominant one as its value contributes a large portion of the total capacitance.

We measured the frequency of every capacitor units of two randomly-selected boards and display them in Figure 10. We can see that although there are some frequency changing randomly at unit number 10 to 15, the curves are quite similar at number from 20 to 30. This phenomenon is caused by systematic variation, and such correlated global shift effect is mitigated using techniques shown in Section 3.5.1.

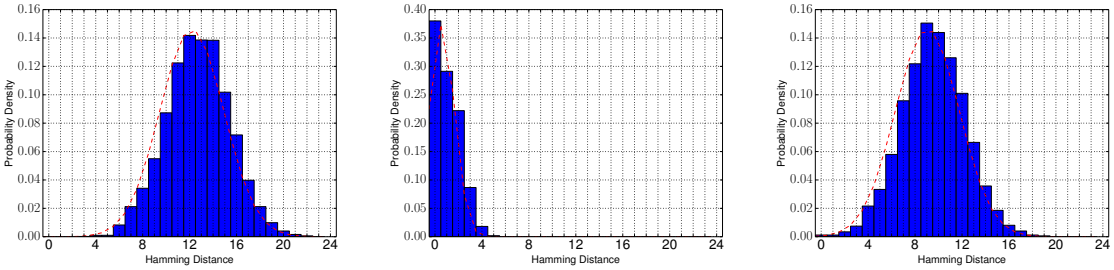
Next, we evaluate the performance of BoardPUF. Figure 11 illustrates the result of BoardPUF in the measure of inter-distance, intra-distance and IBIC-distance. The x axis represents the Hamming distance between two BoardPUF's output while the y axis represents the probability. The red dash line models the experimental result with a normal distribution. Both inter-distance and the IBIC distance conforms to a normal distribution with mean value of 12.67 and 9.53 respectively. The mean value of intra-distance is 0.87, meaning that BoardPUF can also achieve good stability. As can be observed, BoardPUF achieves 47.21% inter-distance and 3.63% intra-distance, both are very close to its ideal value. The maximum number of bit flips occurred of one BoardPUF instance in different testing environments is 4. Although BoardPUF behaves slightly worse in the presence of the new threat model, as the IBIC distance is around 39.7%, it still remains costly for attackers to manufacture a board that produce the exact ID with their target.

False rejection ratio and false acceptance ratio are analyzed as follows. False rejection ratio means the probability that a legitimate board fails to generate the same ID with that in database and do not pass the authentication process. False acceptance ratio means one PUF is mis-identified as another. Based on the results we get, in normal use case, the false rejection ration is 5.89×10^{-6} and the false acceptance ratio is 3.01×10^{-11}. If we consider the scenario that an attacker deliberately counterfeit a number of PCBs, desoldered the BoardPUF chip and put it onto counterfeit PCBs, false acceptance ratio in this case is 1.60×10^{-4}. This means the attacker can found one PCB that produces the exact ID with he desired in more than 6 thousand counterfeit PCBs in the average case, which is a quite great cost.

Finally we give the result of intra-distance in various environment in Table. 2. We count the total number of bit flips among all tested boards compared to original state (25°C, 5V) and calculate the percentage. Both voltage fluctuation and temperature change would contribute to the instability of bit generation. From the table, we can conclude, higher voltage supply would deteriorate more than lower voltage supply, as the percentage of bit flips is 3-fold increase in 5.5V. Higher temperature causes more flips than lower temperature. If we compare the temperature and voltage, voltage fluctuations would cause more flips, which gives us an indication that it is more important to keep voltage stable for higher robustness.

Table 2: Robustness Metric in Different Environment conditions Compared to 25°C, 5V

Environmental Condition	% of bit flipped
25°C, 4.5V	2.5%
25°C, 5.5V	8.3%
35°C, 5V	2.5%
45°C, 5V	3.1%
55°C, 5V	3.9%
65°C, 5V	4.2%



(a) Inter-Distance (b) Intra-Distance (c) IBIC-Distance

Figure 11: Results of BoardPUF

6. CONCLUSION

Counterfeit detection is an urgent need for securing the revenue of legitimate company. PUF is a promising technique to mitigate this threat and has attracted significant attentions from both academia and industry. In this paper, we developed a novel PUF device for PCB authentication, namely BoardPUF. BoardPUF generates unique and robust IDs for each PCB by utilizing the variations of the capacitors carefully embedded in the internal layers of PCB. We adopt various method tailored for variations on board, such as capacitor unit rotation, random permutation to improve the uniqueness and robustness. Experimental results prove that BoardPUF is a high-quality PUF design in terms of uniqueness and stability.

7. ACKNOWLEDGEMENT

This work was supported in part by the Hong Kong S.A.R. General Research Fund (GRF) under Grant No. N_CUHK444/12 and in part by National Natural Science Foundation of China under Grant No. 61432017.

8. REFERENCES

[1] US department of commerce. Defense Industrial Base Assessment: Counterfeit Electronics. `http://www.bis.doc.gov/defenseindustrialbaseprograms/osies/defmarketresearchrpts/final_counterfeit_electronics_report.pdf`, 2010.

[2] U. Guin, K. Huang, D. DiMase, J. M. Carulli, M. Tehranipoor, and Yiorgos Makris. Counterfeit Integrated Circuits: A Rising Threat in the Global Semiconductor Supply Chain. *Proceedings of the IEEE*, 102(8), 2014.

[3] S. Ghosh, A. Basak, and S. Bhunia. How Secure Are Printed Circuit Boards Against Trojan Attacks? *IEEE Design & Test*, 32(2):7–16, 2015.

[4] B. Gassend. *Physical random functions*. PhD thesis, Massachusetts Institute of Technology, 2003.

[5] B. Gassend, D. Clarke, M. van Dijk, and S. Devadas. Silicon Physical Random Functions. In *ACM conference on Computer and Communications Security (CCS)*, pages 148–160, 2002.

[6] Renesas. Board ID. `http://am.renesas.com/products/security/boardid/`, 2014.

[7] Maxim. PCB ID and Authentication. `http://www.maximintegrated.com/en/products/comms/one-wire/pcb-id-and-authentication.html`, 2014.

[8] F. Zhang, A. Hennessy, and S. Bhunia. Robust Counterfeit PCB Detection Exploiting Intrinsic Trace Impedance Variations. In *IEEE VLSI Test Symposium (VTS)*, pages 1–6, Apr. 2015.

[9] G. E. Suh and S. Devadas. Physical Unclonable Functions for Device Authentication and Secret Key Generation. In *ACM/IEEE Design Automation Conference (DAC)*, pages 9–14, 2007.

[10] J. Guajardo, S. S. Kumar, G.-J. Schrijen, and P. Tuyls. FPGA Intrinsic PUFs and Their Use for IP Protection. In *Workshop on Cryptographic Hardware and Embedded Systems (CHES)*, pages 63–80, 2007.

[11] S. S. Kumar, J. Guajardo, R. Maes, G.-J. Schrijen, and P. Tuyls. Extended abstract: The butterfly PUF protecting IP on every FPGA. In *IEEE International Workshop on Hardware-Oriented Security and Trust (HOST)*, pages 67–70, 2008.

[12] R. Maes and I. Verbauwhede. Physically Unclonable Functions: A Study on the State of the Art and Future Research Directions. In *Towards Hardware-Intrinsic Security - Foundations and Practice*, pages 3–37, 2010.

[13] ANSYS. ANSYS Maxwell. `http://www.ansys.com/Products/Simulation+Technology/Electronics/Electromechanical/ANSYS+Maxwell`, 2015.

[14] Sunstone Circuits. PCB manufactruing Capabilities. `http://www.sunstone.com/pcb-capabilities/pcb-manufacturing-capabilities`, 2014.

[15] C.-E. Yin and G. Qu. Improving PUF Security with Regression-based Distiller. In *ACM/IEEE Design Automation Conference (DAC)*, pages 1–6, 2013.

[16] C.-E. Yin and G. Qu. LISA: Maximizing RO PUF's Secret Extraction. In *IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*, 2010,

[17] U. Rührmair, F. Sehnke, J. Sölter, G. Dror, S. Devadas, and J. Schmidhuber. Modeling Attacks on Physical Unclonable Functions. In *ACM Conference on Computer and Communications Security (CCS)*, pages 237–249, 2010.

[18] S. Wei, J. B. Wendt, A. Nahapetian, and M. Potkonjak. Reverse Engineering and Prevention Techniques for Physical Unclonable Functions Using Side Channels. In *ACM/IEEE Design Automation Conference (DAC)*, pages 90:1–90:6, 2014.

[19] J. Delvaux and I. Verbauwhede. Key-recovery Attacks on Various RO PUF Constructions via Helper Data Manipulation. In *Design, Automation & Test in Europe Conference & Exhibition (DATE)*, 2014.

[20] Tektronix. How Oscilloscope Probes Affect Your Measurement. `http://www.tek.com/dl/51W_30013_0_MR_Letter_0.pdf`, 2013.

[21] NXP Semiconductors. 74HC14;74HCT14 Product data sheet. `http://www.nxp.com/documents/data_sheet/74HC_HCT14.pdf`, 2012.

[22] Intel, editor. *Intel Packaging Databook – Performance Characterisitics of IC Packages*. 2000.