POSTER: Attack on Non-Linear Physical Unclonable Function

Jing Ye
State Key Laboratory of
Computer Architecture,
Institute of Computing Technology,
Chinese Academy of Sciences
yejing@ict.ac.cn

Yu Hu
State Key Laboratory of
Computer Architecture,
Institute of Computing Technology,
Chinese Academy of Sciences
huyu@ict.ac.cn

Xiaowei Li
State Key Laboratory of
Computer Architecture,
Institute of Computing Technology,
Chinese Academy of Sciences
lxw@ict.ac.cn

ABSTRACT

Physical Unclonable Function (*PUF*) is a promising hardware security primitive with broad application prospect. However, the strong PUF with numerous *Challenge and Response Pair*s (*CRP*s), e.g. the arbiter PUF, is vulnerable to modeling attacks. There are two major kinds of countermeasures. One is restricting CRP access interface, such as controlled PUF and XOR arbiter PUF, which unfortunately has been broken with the help of side-channels. The other is using non-linear electronic characteristics to produce CRPs, such as the current mirror PUF and the voltage transfer PUF. They are only proved to be resistant to SVM based attack, while no more analysis is further explored so far. In this paper, we propose an attack method based on compound heuristic algorithms of evolution strategy, simulated annealing, and ant colony to efficiently attack these two non-linear PUFs. This paper reveals that current mirror and voltage transfer are still not able to help strong PUF resist attacks. Our experimental results show that the average CRP prediction accuracy is as high as 99%.

Keywords

Physical Unclonable Function; Attack; Non-Linear; Compound Heuristic Algorithms.

1. INTRODUCTION

The *Physical Unclonable Function* (*PUF*) is a promising hardware security primitive [1]. It exploits the random physical disorder and the process variation to output particular responses for input challenges, which are called the *Challenge-Response Pairs* (*CRPs*). The PUF has broad application prospects in the field of hardware security, such as authentication, key-exchange, IP protection, and hardware obfuscation.

PUF can be divided into two major categories: (1) the weak PUF with a few number of CRPs, such as the coating PUF [2] and the SRAM PUF [3]; (2) the strong PUF with a large number of CRPs. The arbiter PUF [4][5] is a typical strong PUF. It compares the delays of two paths to produce a response. Each path is consisted of path segments which are selected by a challenge. As the delays of path segments are affected by process variation, the CRPs cannot be predicted before manufacturing. However, to break the arbiter PUF, attackers model the delay of each path as the sum delay of path segments [6]. When attackers collect certain number of CRPs, they can use machine learning algorithms to speculate the delays of path segments, so that all the unknown CRPs can be predicted. It takes only several minutes to achieve 99.9% CRP prediction accuracy.

To resist modeling attacks, there are two major kinds of countermeasures. One is restricting CRP access interface by using hash function [7] or XOR gates [8]. In this way, attackers cannot directly access the original responses. Unfortunately, the work in [9] adopts the unreliability side-channel to build a new model for attack. The power [10] and the photon [11] are also successfully used to imply or expose the original responses.

The other countermeasure is using other electronic characteristics than delay to produce CRPs. Two recent typical PUFs are the current mirror PUF [12] and the voltage transfer PUF [13]. It is claimed that both of them can resist SVM based attack. However, seldom analysis of their security is further explored so far [16]. Can these electronic characteristics really resist attacks?

To answer this question, we propose an attack method toward the current mirror PUF and the voltage transfer PUF. Our contributions include:

(1) An attack method based on compound heuristic algorithms of evolution strategy, simulated annealing, and ant colony is proposed;

(2) This paper reveals that current mirror and voltage transfer non-linear PUFs are still not able to resist attacks.

The rest of this paper is organized as follows. Section 2 reviews the two non-linear PUFs. Section 3 proposes the attack method. Section 4 presents experimental results. Final is the conclusion.

2. NON-LINEAR PUF

The current mirror PUF and the voltage transfer PUF are shown in Fig.1 [12][13]. The current mirror (voltage transfer) PUF propagates currents (voltages) through two paths to the arbiter, and the arbiter compares the two currents (voltages) to produce a response. The challenge determines whether the currents (voltages) pass or switch along the paths as shown in Fig.1.

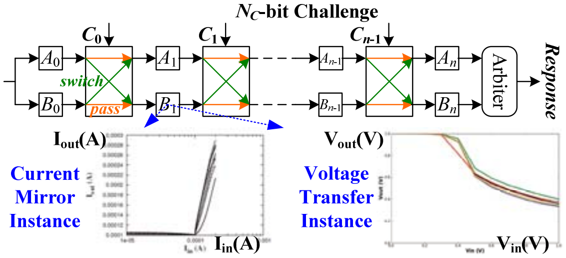

Figure 1. Current Mirror PUF and Voltage Transfer PUF

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the Owner/Author. Copyright is held by the owner/author(s).

CCS'16, October 24-28, 2016, Vienna, Austria
ACM ISBN 978-1-4503-4139-4/16/10.
DOI: http://dx.doi.org/10.1145/2976749.2989039

As shown in Fig.1, since the input-output characteristic I_{in}-I_{out} of current mirror and V_{in}-V_{out} of voltage transfer are both non-linear, they are claimed in [12][13] with higher resistance to SVM based attack. Due to process variation, different instances of current mirror and voltage transfer have different input-output characteristics to guarantee the PUF uniformity and uniqueness.

3. ATTACK ON NON-LINEAR PUF

3.1 Problem Formulation

According to Fig.1, to attack a non-linear PUF with N_C-bit challenge, the key is to speculate the input-output characteristic of each current mirror instance or voltage transfer instance. There are totally $2\times N_C+2$ instances in one PUF. Instead of directly formulating the input-output characteristic, which needs high computation complexity, we simulate $N_I=10^5$ current mirror instances and N_I voltage transfer instances with random process variations. For the sake of simplicity, in the following, "instance" means the current mirror instance or the voltage transfer instance. Then, to attack a target PUF, the problem is formulated as:

Given: Training set S_T: N_T known CRPs of the target PUF;

Simulated instance set S_I: N_I instances;

Task: Select $2\times N_C+2$ instances from the S_I, and put them at appropriate positions (A_0~A_n, B_0~B_n in Fig.1) to form a *Fitting PUF* (*FPUF*);

Object: Among the S_T, make the target PUF and the *FPUF* have the same CRPs as many as possible.

3.2 Compound Heuristic Algorithm

Many algorithms such as SVM, logistic regression, evolution strategy have been adopted to attack PUFs [6]. Evolution strategy is a common algorithm for handling linear or non-linear problems. We find that the evolution strategy can attack current mirror PUF and voltage transfer PUF, but with a low efficiency. Therefore, we introduce the simulated annealing process and the pheromone of ant colony algorithm into the evolution strategy, and propose a compound heuristic algorithm to attack the two non-linear PUFs. The pseudo code is given in Alg.1. The fitness of a *FPUF* means the percentage of same CRPs between the target PUF and the *FPUF* among S_T.

At Line 1~5 of Alg.1, F_T, N_E, N_S, N_F, and N_O are five user-defined parameters. At Line 6, $(2\times N_C+2)$ instances are randomly selected from S_I to form a *FPUF*. Totally, N_F *FPUFs* are initialized. The evolution of *FPUFs* happens through Line 8~32. During the evolution, for each *FPUF*, the simulated annealing algorithm combined with the pheromone of ant colony algorithm is used to mutant the *FPUF* at Line 9-27. After N_S iterations of simulated annealing, at Line 29, only N_F-N_O *FPUFs* with higher fitness than others are kept, and rest *FPUFs* are deleted. Then at Line 30, the kept *FPUFs* are crossed to generate N_O new *FPUFs*. In the crossing process, two FPUFs ($A_{1,0}$~$A_{1,n}$, $B_{1,0}$~$B_{1,n}$) and ($A_{2,0}$~$A_{2,n}$, $B_{2,0}$~$B_{2,n}$) are randomly selected from the kept *FPUFs*. One position $o\in[0, n]$ is also randomly selected, and then the new *FPUF* is ($A_{1,0}$~$A_{1,o}$, $A_{2,o+1}$~$A_{2,n}$, $B_{1,0}$~$B_{1,o}$, $B_{2,o+1}$~$B_{2,n}$). The whole procedure ends if the highest fitness of the *FPUFs* achieves F_T at Line 31.

Pheromone plays an important role in the ant colony algorithm. The previous iterations guide the operations of latter iterations through the pheromone. The pheromone is introduced in our simulated annealing algorithm at Line 10-27. In each iteration of simulated annealing, the instance at P is replaced by a randomly selected instance from S_I. The P is selected from A_0~A_n, B_0~B_n according to its pheromone. A position with higher pheromone has higher probability to be selected. If the replacement makes *FPUF* obtain higher fitness, this replacement is accepted, and the pheromone of P is increased. If not, this replacement is only accepted with certain probability, and the pheromone of P is decreased. Please notice that, in one iteration, more than one instance can also be replaced simultaneously.

4. EXPERIMENTAL RESULTS

In our experiments, we use the proposed method to attack current mirror PUFs and voltage transfer PUFs. The proposed method is implemented in C++, and is run in desktop computers with Intel i7 3.6GHz CPU. As [12], the PUFs are simulated in a 32nm PTM model [14], assuming threshold voltage variations obey Gaussian distribution with 3σ deviation 90mV [15]. 100 current mirror PUFs and 100 voltage transfer PUFs are simulated and attacked. Certain number of CRPs is randomly selected. Some of them are used as the training set S_T for attack, while other 20000 CRPs are used as the testing set for evaluating the CRP prediction accuracy (fitness of *FPUF* under testing set). On the other hand, due to variations of working circumstances, the CRPs may be unreliable. According to [12][13], the reliability of both current mirror PUF and voltage transfer PUF is around 98%. The experimental results are shown in Table 1, where maximum number of iterations is 10^6.

Algorithm 1. Compound Heuristic Algorithm

```
1   $F_T$ = target fitness
2   $N_E$ = maximum number of evolution iterations
3   $N_S$ = maximum number of simulated annealing iterations
4   $N_F$ = number of FPUFs
5   $N_O$ = number of FPUFs generated by crossing
6   Initialize $N_F$ FPUFs by randomly selecting
    $N_F\times(2\times N_C+2)$ instances from $S_I$
7   Iteration = 0
8   For ( $e = 0$ ; $e < N_E$ ; $e$++ ) {
9     For ( $f = 0$ ; $f < N_F$ ; $f$++ ) {
10      Pheromone of $A_0$~$A_n$, $B_0$~$B_n$ = 100%
11      For ( $s$ = Iteration ; $s < N_S$ + Iteration ; $s$++ ) {
12        $FPUF_0$ = $f^{th}$ FPUF
13        $F_0$ = fitness of $FPUF_0$
14        $I$ = randomly select an instance from $S_I$
15        $P$ = select from $A_0$~$A_n$, $B_0$~$B_n$ based on Pheromone
16        $FPUF_1$ = Put $I$ at $P$ in $FPUF_0$
17        $F_1$ = fitness of $FPUF_1$
18        If ( $F_0 > F_1$) {
19          With probability $e^{\frac{1}{(F_1-F_0)\times s}}$ : $f^{th}$ FPUF = $FPUF_0$
20          Else: $f^{th}$ FPUF = $FPUF_1$
21          Decrease Pheromone of $P$
22        } Else {
23          $f^{th}$ FPUF = $FPUF_1$
24          Increase Pheromone of $P$
25        }
26      }
27    }
28    Iteration += $N_S$
29    Keep $N_F$-$N_O$ FPUFs with higher fitness
30    Cross kept $N_F$-$N_O$ FPUFs to generate $N_O$ FPUFs
31    If ( Highest fitness of $N_F$ FPUFs ≥ $F_T$ ) break;
32  }//
```

When the training set is fully reliable, and current mirror PUFs and voltage transfer PUFs have 32-bit challenge, the average prediction accuracy achieves 99.9%. Even when N_C is 128, the average prediction accuracy is still beyond 98%. The unreliability of training set causes a slight decrease of prediction accuracy. This can be handled by obtaining the training set in a more stable working circumstance. The time of attack is from several minutes to several hours. In comparison with SVM based attack used in [12][13], this data reveals that the current mirror PUF and the voltage transfer PUF are not as secure as claimed in [12][13].

To explore the relation among time, N_P, and prediction accuracy, we illustrate the attack process of a voltage transfer PUF in Fig.2 and Fig.3 when reliability is 100%. Fig.2 shows the prediction accuracy at different *Iteration* of Alg.1, while N_P is set as Table 1. With more iterations, longer time is spent to achieve higher prediction accuracy. For PUFs with more challenge bits, more iterations are needed to achieve higher prediction accuracy. Please notice that, with the increasing of *Iteration* in Alg.1, the highest fitness of *FPUFs* to training set will never decrease, but the fitness of *FPUFs* to testing set, i.e. the prediction accuracy shown in Fig.2, may decrease. Fig.3 shows the prediction accuracy when different sizes of training set are used, while maximum number of iterations is 10^6. With larger training set, higher prediction accuracy can be obtained.

Table 1. Prediction Accuracy

Current Mirror (CM) Voltage Transfer (VT)		N_C	N_T	Prediction Accuracy Reliability =100%	 Reliability =98%	Time (min)
Proposed Attack Method	CM PUF	32	1×10^3	99.92%	98.55%	9
		64	1×10^4	99.26%	98.97%	112
		128	2×10^4	98.03%	97.89%	548
	VT PUF	32	1×10^3	99.90%	98.70%	11
		64	1×10^4	99.31%	99.18%	83
		128	2×10^4	98.16%	98.11%	374
SVM Attack [12][13]	CM PUF	80	2×10^6	70.0%	64.0%	21
	VT PUF	64	5×10^4	79.2%	N/A	N/A

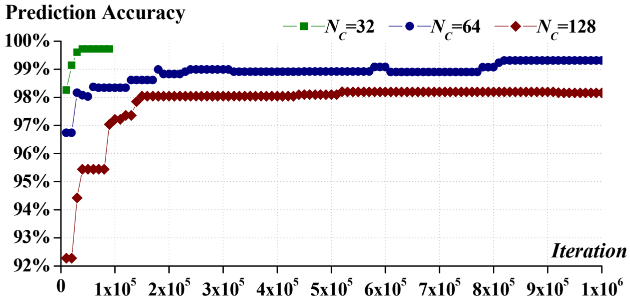

Figure 2. *Iteration* vs. Prediction Accuracy

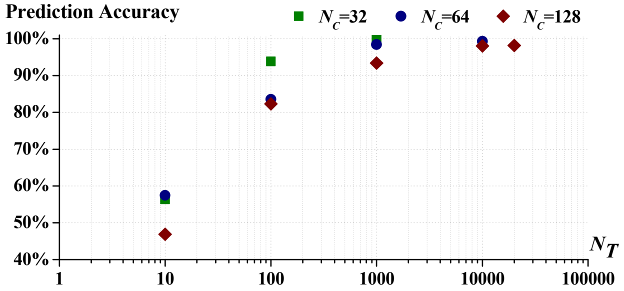

Figure 3. N_P vs. Prediction Accuracy

5. CONCLUSION

This paper proposes compound heuristic algorithms of evolution strategy, simulated annealing, and ant colony to attack non-linear PUFs: the current mirror PUF and the voltage transfer PUF. The average prediction accuracy achieves 99%, so it reveals that the current mirror PUF and the voltage transfer PUF are not as secure as being claimed. More efficient designs for resisting attacks are still highly needed.

6. ACKNOWLEDGE

This paper is supported by the *National Natural Science Foundation* (*NSFC*) of China: 61532017, 61274030, 61376043.

7. REFERENCE

[1] Ruhrmair, U., Holcomb, D. E., 2014. PUFs at a Glance. Design, Automation and Test in Europe (DATE).

[2] Tuyls, P., Schrijen, G. J., et. al., 2006. Read-Proof Hardware from Protective Coatings. Cryptographic Hardware and Embedded Systems (CHES), 369-383.

[3] Guajardo, J., Kumar, S. S., et. al., 2007. FPGA Intrinsic PUFs and Their Use for IP Protection. Cryptographic Hardware and Embedded Systems (CHES), 63-80.

[4] Lim D., 2004. Extracting Secret Keys from Integrated Circuits. MIT MSc Thesis.

[5] Ye, J., Hu, Y., Li, X., 2015. OPUF: Obfuscation Logic Based Physical Unclonable Function. International On-Line Testing Symposium (IOLTS), 156-161.

[6] Ruhrmair, U., Solter, J., et. al., 2013. PUF Modeling Attacks on Simulated and Silicon Data. IEEE Transactions on Information Forensics and Security (TIFS), 8, 11, 1876-1891.

[7] Gassend, B., Clarke, D., et. al., 2002. Controlled Physical Random Functions. Computer Security Applications Conference (CSAC), 149-160.

[8] Majzoobi, M., Koushanfar, F., Potkonjak, M., 2008. Lightweight Secure PUFs. International Conference on Computer-Aided Design (ICCAD), 670-673.

[9] Becker, G. T., 2015. The Gap Between Promise and Reality: On the Insecurity of XOR Arbiter PUFs. Cryptographic Hardware and Embedded Systems (CHES), 535-555.

[10] Becker, G. T., Kumar, R., 2014. Active and Passive Side-Channel Attacks on Delay Based PUF Designs. IACR Cryptology.

[11] Ganji, F., Kramer, J., et. al., 2015. Lattice Basis Reduction Attack against Physically Unclonable Functions. Conference on Computer and Communications Security (CCS), 1070-1080.

[12] Kumar, R., Burleson, W., 2014. On Design of a Highly Secure PUF Based on Non-Linear Current Mirrors. Hardware-Oriented Security and Trust (HOST), 38-43.

[13] Vijayakumar, A., Kundu, S., 2015. A Novel Modeling Attack Resistant PUF Design based on Non-Linear Voltage Transfer Characteristics. Design, Automation and Test in Europe Conference and Exhibition (DATE), 653-658.

[14] ITRS. International Technology Roadmap for Semiconductors. http://public.itrs.net

[15] Maiti, A., Gunreddy, V., Schaumont, P., 2013. A Systematic Method to Evaluate and Compare the Performance of Physical Unclonable Functions. IACR Cryptology, 245-267

[16] Guo, Q., Ye, J., Hu, Y., Li X., 2016. Efficient Attack on Non-Linear Current Mirror PUF with Genetic Algorithm. to be published in Proc. IEEE Asian Test Symposium (ATS).