Hindawi
Active and Passive Electronic Components
Volume 2017, Article ID 4070589, 8 pages
https://doi.org/10.1155/2017/4070589

Research Article

Design Impedance Mismatch Physical Unclonable Functions for IoT Security

Xiaomin Zheng, Yuejun Zhang, Jiaweng Zhang, and Wenqi Hu

Institute of Circuits and Systems, Ningbo University, No. 818 Fenghua Road, Ningbo 315211, China

Correspondence should be addressed to Yuejun Zhang; zhangyuejun@nbu.edu.cn

Received 21 July 2016; Revised 14 November 2016; Accepted 27 December 2016; Published 24 January 2017

Academic Editor: Sourabh Khandelwal

We propose a new design, Physical Unclonable Function (PUF) scheme, for the Internet of Things (IoT), which has been suffering from multiple-level security threats. As more and more objects interconnect on IoT networks, the identity of each thing is very important. To authenticate each object, we design an impedance mismatch PUF, which exploits random physical factors of the transmission line to generate a security unique private key. The characteristic impedance of the transmission line and signal transmission theory of the printed circuit board (PCB) are also analyzed in detail. To improve the reliability, current feedback amplifier (CFA) method is applied on the PUF. Finally, the proposed scheme is implemented and tested. The measure results show that impedance mismatch PUF provides better unpredictability and randomness.

1. Introduction

The Internet of Things is a dynamic living entity, which enables things to exchange information and communication through the networking of physical terminal devices, humans, intelligent buildings, and others [1, 2]. The IoT improves efficiency, accuracy, and economic benefit but is also potentially a huge security risk. Some reports predict that it will spend $547 million on IoT security in 2018 and will involve more than 25% of identified attacks on enterprises by 2020 [3]. Some possible IoT threats are outlined in Figure 1.

According to [4], IoT weakness is so ubiquitous that industrial espionages find it easy to get a good target for attacking. And also, privacy is the other important area of concern. The cybercriminals may recover the personal information, which is potentially residing on IoT networks. In addition, as more and more objects interconnect to today's IoT networks, the physical security of each device is greatly reduced. Attackers could add all kinds of risk scenarios to control systems or change functionality, such as reading, intercepting, or changing the data [5]. To address these problems, there are some methods to increase security for IoT network with the help of security tools, such as identification (ID) authentication, data encryption/decryption, and code obfuscation.

To build a secure and safe IoT, it is very important that the identity of each thing is authenticated. That is a massive challenge, but fortunately there is a way to take full advantage of each thing's unique identifier through Physically Unclonable Function (PUF) technology [6, 7]. PUF generates a unique identifier by exploiting random physical factors introduced in the semiconductor manufacturing process. PUF circuit has the properties of uniqueness, randomness, and unclonability [8–12]. The above features make the PUF circuit an effective defense against intrusion attacks, including a variety of attack patterns. Printed circuit board (PCB) is one of the important hardware carriers of IoT. In the supply chain of PCB, malicious users may make counterfeit PCB come from a variety of sources, such as direct cloning, overproduction, and recycling. In fact, the quality of imitation PCB is poor, such as reliability and performance problems. With the proliferation of fake PCBs and the increase in accidental reports, the problems of the board-level feature recognition technique are becoming more and more important. In this work, we propose an impedance mismatch PUF, which has been exploited to generate a security unique private key to authenticate each thing in an IoT network. According to the characteristic of transmission line and signal transmission theory, the impedance mismatch will cause the transmission signal to

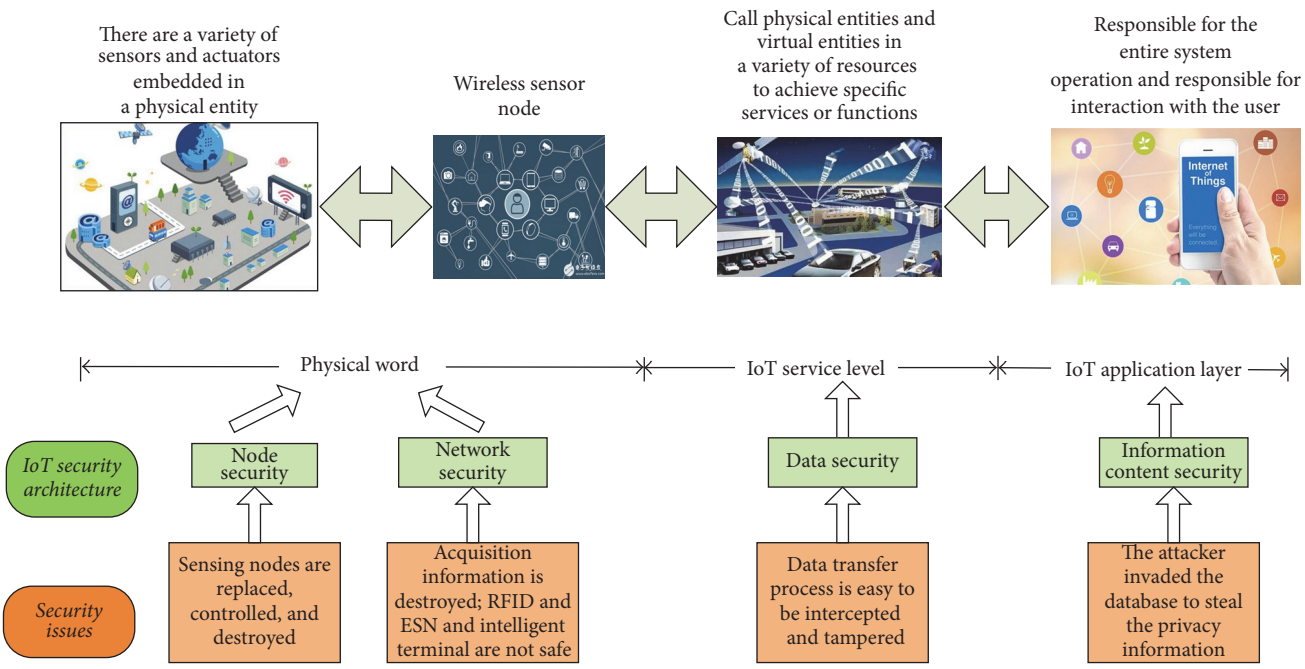

Figure 1: The IoT threats model.

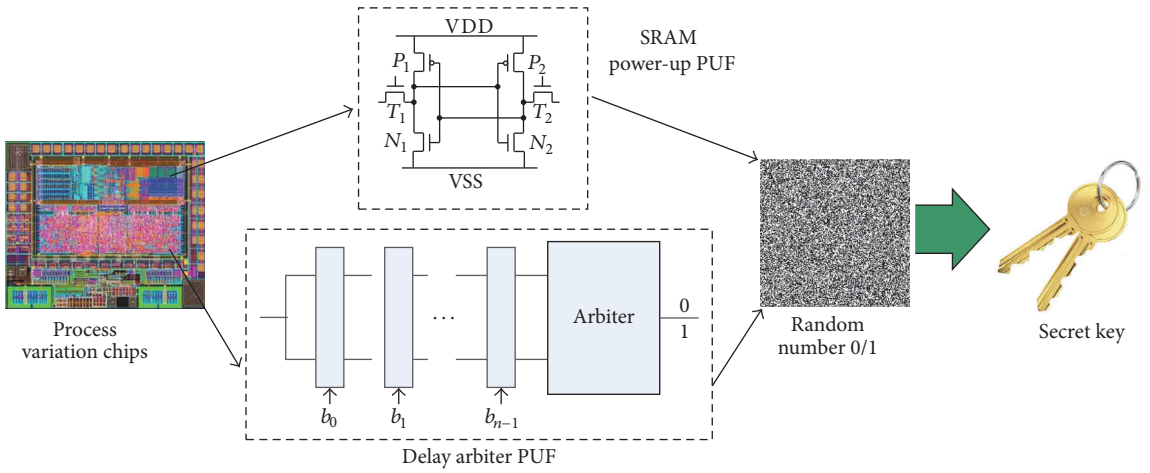

Figure 2: Physical Unclonable Functions circuit.

reflect, especially in high-frequency scenarios. The proposed PUF circuit will improve the board-level security of IoT.

This paper is organized as follows: The existing Physically Unclonable Functions circuits are summarized in Section 2. The impedance mismatch effect of transmission line is detailed in Section 3. The designed method of PUF for IoT security is proposed in Section 4. Some experimental results are analyzed in Section 5. This work is concluded in Section 6.

2. Physically Unclonable Functions

SRAM PUF [8, 9] and Arbiter PUF [11–13, 15, 16] are two kinds of typical PUF circuit. SRAM-PUF circuits are produced through the manufacturing process, which introduces a biased digital signal in an integrated circuit. As shown in Figure 2, the SRAM-PUF cell consists of cross coupled inverters and T1 and T2 transmission transistors. SRAM-PUF circuit cells generate a logic level, which is determined by random process deviation threshold V_{th} of the cross coupled inverters. The function relation of SRAM-PUF circuit is easy to affect through the power supply voltage, temperature, aging, and other factors [10]. The output value has stability problems.

The arbiter PUF circuit [11–13, 15, 16] is composed of a delay unit and an arbiter circuit, as shown in Figure 2. The delay unit is composed of two delay paths and switch components. When the left input of the circuit experiences a low level to high level signal rise, the input signal will be conveyed along two paths, each after a data selector signal making two kinds of path selection, as dictated by the control signal b_i.

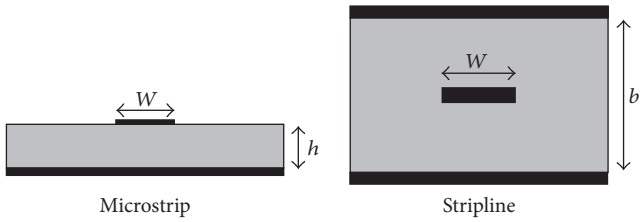

Figure 3: Microstrip and Stripline.

If there are m data selectors, this is a signal with 2^m different transmission modes. If the differences in signal transmission to the arbiter through the two delay paths have a time difference, the upper end of the output signal end of a data selector first will output a signal arbiter "1." Otherwise, the output signal of the arbiter is "0." Therefore, the output signal of the arbitrator is determined by the priority arrived signal. The arbiter PUF circuit recognizes model attacks [17, 18].

3. Impedance Mismatch Effect

The definition of characteristic impedance is the ratio of voltage amplitudes and current value on the transmission line. The most important physical factors of characteristic impedance are geometry and materials of the transmission line. It is not dependent on length of transmission line. Under the condition of matching with the load impedance, the signal on transmission line transmits long distant without reflection [19]. If the impedance of transmission line mismatches with the load impedance, it will transmit loss and produce reflection. Impedance mismatch phenomenon means that the impedance of transmission line is different from the characteristic impedance, and transmission signal will be reflected to the opposite direction [20]. If the impedance of transmission line matches with the load impedance, the voltage signal generates positive reflection, and current signal generates negative reflection [21]. On the other hand, when the load impedance is smaller than the characteristic impedance, the voltage signal generates negative reflection, and the current signal generates positive reflection.

There are two types of transmission lines on the PCB board, Microstrip and Stripline (as shown in Figure 3). The impedance calculation formula of Microstrip is shown as follows [22]:

$$Z = \frac{87.0}{\sqrt{\varepsilon_r + 1.41}} \ln\left(\frac{5.98h}{0.8w + t}\right). \quad (1)$$

Among them, Z is the characteristic impedance, ε_r is the relative permittivity, h is the medium wire thickness (mil), w is the wire width (mil), and t is the thickness of the wire (1 oz = 1.5 mil). In (1), relative permittivity ε_r is between 1 and 15; ratio of w/h is between 1 and 15; the width of the ground wire is more than 7 times the width of the signal line. The impedance calculation formula of Stripline is shown as follows [23]:

$$Z_0 = \frac{87}{\sqrt{\varepsilon_r}} \ln \frac{4h}{067\pi\,(0.8w + t)}. \quad (2)$$

In (2), $w \approx h < 0.35$; relative permittivity ε_r is between 1 and 15; the width of the ground wire is more than 7 times the width of the signal line. From formulas (1) and (2), it is known that the width, thickness, and dielectric constant determine the impedance. Reference [24] shows that the length of the wire, the thickness of the pad, the path of the ground wire, and other nearby wires will also affect the characteristic impedance of the transmission line, especially in high-speed data transmission.

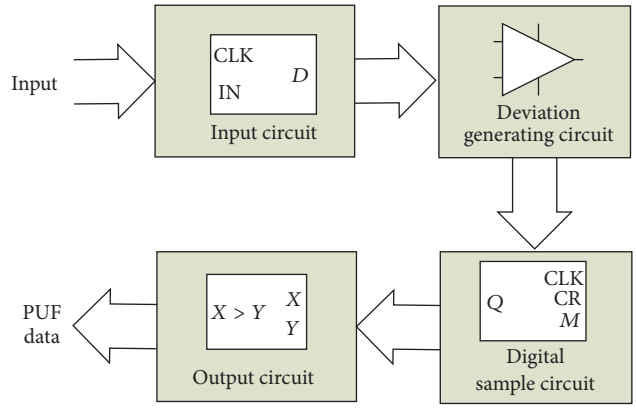

Figure 4: IM-PUF circuit model.

The cut-off frequency calculation formula is shown as follows [25]:

$$f_{\text{cut-off}} = \frac{1}{2\pi RC}, \quad (3)$$

where R and C represent the PCB's equivalent resistance and capacitance, respectively. According to (3), the cut-off frequency does not relate to input signal and power supply. On transmission line of PCB, reflection caused by impedance mismatch may happen. The more the transmission signal reflects, the weaker the output signal is [26]. In experimental testing, the cut-off frequency is described as specific operational frequency that causes the output signal amplitude to reduce 0.707-fold [25]. So, the characteristic impedance Z and Z_0 influence the cut-off frequency of PCB.

4. Proposed Impedance Mismatch PUF Circuit

Comparing the deviation signals present in the same structure, a PUF circuit generates random output response. In PCB circuit, there are random physical factors that affect output signal amplitude, frequency, and bandwidth [27]. The random physical factors can be divided into two categories. The first category is in the integrated circuit, which is produced by the chip fabrication process, such as the ratio of channel width to length, and the threshold voltage. The second is the PCB layout of the processing device, such as the length and the width of wires, capacitors, resistors, and other factors [28]. Thus, the intrinsic characteristics of the PCB may establish a unique and robust fingerprint in these scenarios.

4.1. Impedance Mismatch PUF Model. According to the impedance mismatch theory and the PUF design method, we presented an impedance mismatch PUF (IM-PUF) model, as shown in Figure 4. The model is composed of input

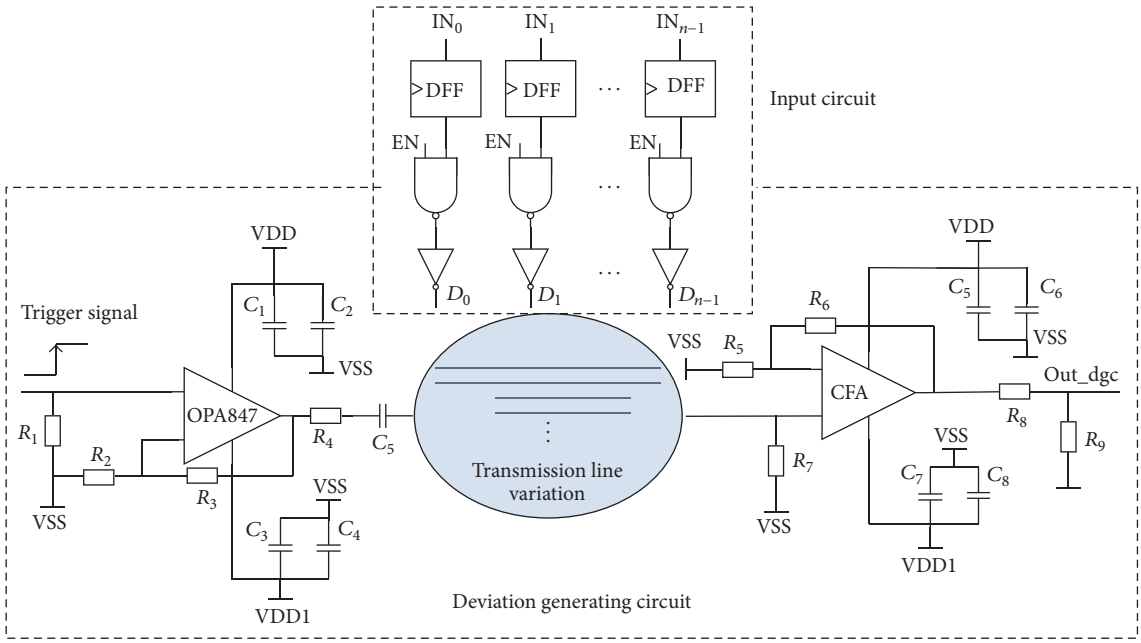

Figure 5: Input circuit and deviation generating circuit.

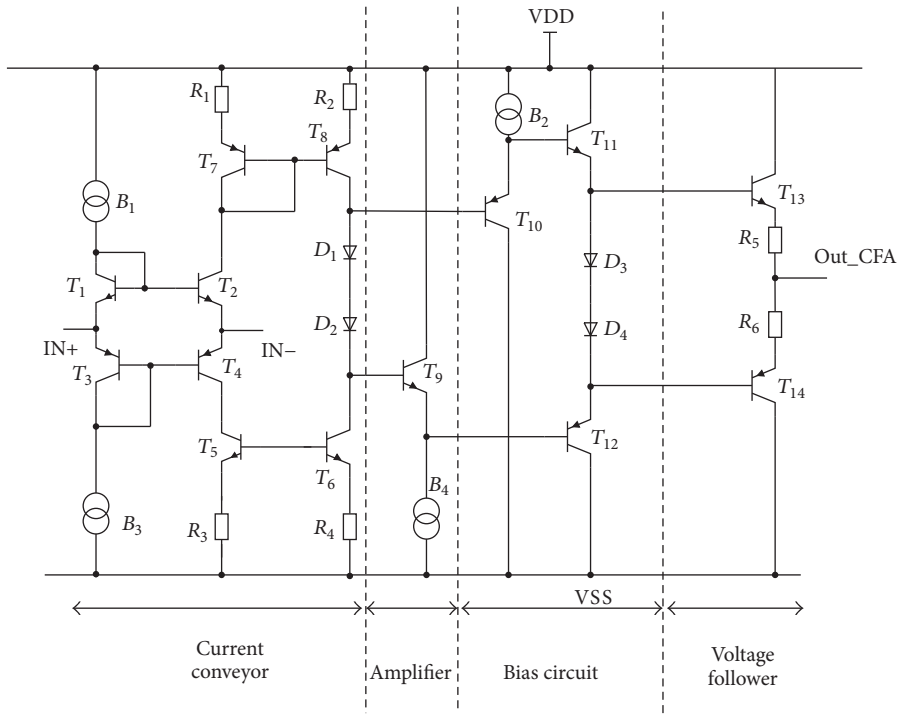

Figure 6: CFA circuit structure.

circuit, deviation generating circuit, digital sample circuit, and output circuit. The deviation generating circuit is the core of the PUF circuit, which generates the upper cut-off frequency with the deviation. The upper cut-off frequency is the clock frequency of the digital sample circuit. During the T time, the circuit compares the two signals and generates a "0" or "1" as the response of PUF circuit.

4.2. Input Circuit and Deviation Generating Circuit. The input circuit and deviation generating circuit are shown in Figure 5. The input circuit is composed of D flip-flops (DFF), NAND gates, and inverters, while the deviation generation circuit is composed of an operational amplifier (OPA847), transmission lines, and current feedback amplifier (CFA). The diagram of a current feedback amplifier is shown in Figure 6

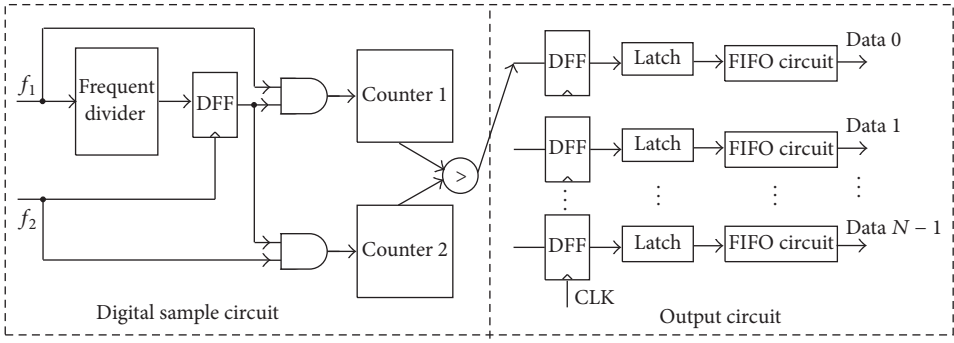

Figure 7: Digital sample circuit and output circuit.

[29]. In Figure 6, the class current conveyors are $T_1 \sim T_8$, the amplifier is T_9, the bias circuit is T_{11} and T_{12}, and the voltage follower is T_{13} and T_{14}. In Figure 6, R_3 is a 750-ohm OPA847 feedback resistor, C_1, C_2, C_3, and C_4 are the decoupling capacitors of OPA847. R6 is a 560-ohm CFA feedback resistance; C_5, C_6, C_7, and C_8 are the decoupling capacitors of CFA. R_3 and R_6 are used to set the amplification of the output signal. R_1, R_4, R_7, and R_8 are used in the impedance matching. The amplitude and frequency of the output signal are determined by the process parameters. In this experiment, the deviation of the characteristic impedance of the transmission line makes the upper cut-off frequency of the output signal changed. The amplifier works as follows equation $\beta = \lambda \times (S + \Delta S)$. It means that the deviation signal ΔS is amplified λ times.

4.3. Digital Sample Circuit and Output Circuit. As shown in Figure 7, the digital sample circuit consists of a frequency divider, a D flip-flop, two AND gates, two counters, and a comparator. Two input signal frequencies f_1 and f_2 serve as the upper cut-off of the output of two transmission lines, respectively. The frequency f_1, though frequency divider, generates a gate control signal TC. During the clock pulse width (named T), f_1 and f_2 behave as two counter clock frequencies. Counter 1 counts the number of N_1, and Counter 2 counts the number of N_2. Comparing N_1 and N_2, if $N_1 > N_2$, the output is "0"; otherwise the output is "1." The output circuit comprises M output units. Each output unit comprises a latch and First Input First Output (FIFO) circuit, as shown in Figure 7.

5. Experimental Results and Analysis

We used many pieces of IM-PUF PCB as designed to measure the upper cut-off frequency in different situations. Figure 8 shows the experiment setup for the IM-PUF measurements. The test platform mainly includes tested PCB board, two MOTECH LPS-305 DC Power Supplies (5 V), SP1461 Type II 300 M Signal Generator, Tektronix MDO3022 200 MHz Oscilloscope, and some wires.

The flow of the experimental measurement is summarized as follows. Four steps are needed in total.

Step 1. Under the peak-to-peak value of 20 mV of the sine wave, measure the voltage amplification values on the original PCB with different frequencies.

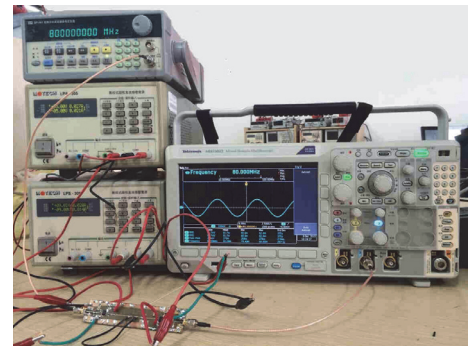

Figure 8: The experiment setup for measuring IM-PUF.

Step 2. If the frequency is less than 60 MHz, the output of RMS voltage is about 130 mV.

Step 3. As input frequency increases, voltage values begin to decay.

Step 4. Determine the upper cut-off frequency voltage value as 0.707 times the middle frequency, namely, 91.91 mV; the upper cut-off frequency is 85.6 MHz.

After that, change the length and width of the PUF circuit transmission line, with 7 cm thin wire, 14 cm thin wire, 7 cm thick wire, and 14 cm thick wire in the original circuit on a transmission line. The deviation of 5% more or less than the component's performance shall be allowed, and the fluctuation range of 1 V more or less than power supply shall be allowed. Measure the upper cut-off frequency at 85.5 MHz, 80.4 MHz, 86.5 MHz, and 80.9 MHz. Experimental measurement data is shown in Figure 9. The frequency curve of PUF obviously changed after changing its transmission line. After changing length and width of the transmission line, its frequency changed accordingly. Given the 6 V and 5 V power supply, the cut-off frequencies have nearly equal values with values lower than 100 MHz, as shown in Figure 10. The frequency of the output signal serves as a trigger for a counter. Then, comparing the outputs of counters, the IM-PUF produces a value of 0 or 1.

In statistics, autocorrelation is defined as the correlation among values of random process [30]. In this work, the hypothesis behind calculation of the autocorrelation is that

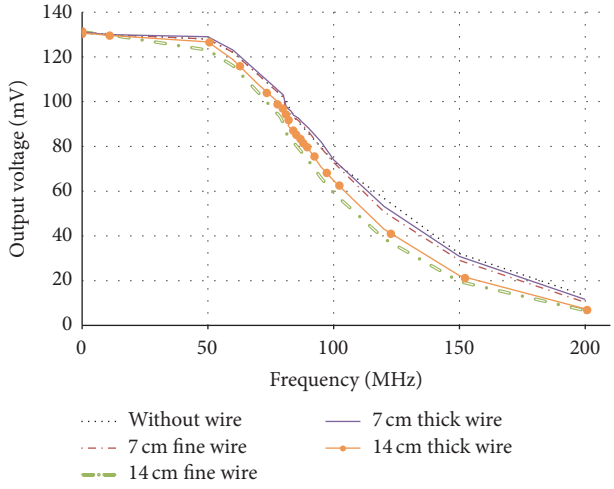

Figure 9: Frequency curve of PUF circuit.

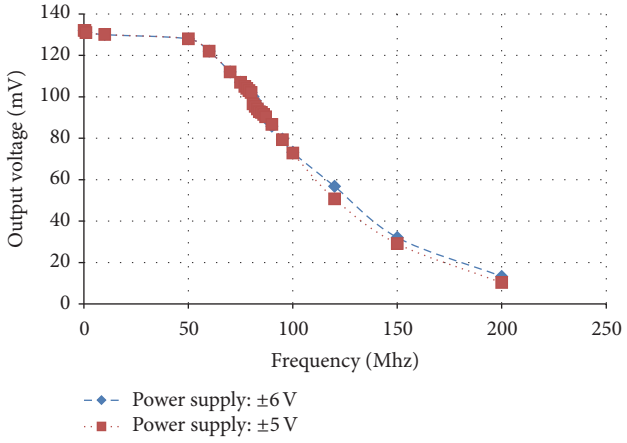

Figure 10: IM-PUF with different power supply.

IM-PUF is a random process. Because IM-PUF is designed according to random variation during PCB manufacturing process, the proposed hypothesis is ok. In other words, the autocorrelation can be used to characterize the performance of antianalysis attack. In the experiment, the sample data of 1# PCB is set as a reference. Figure 11 shows the autocorrelation rates of the IM-PUF circuit. As can be seen, the autocorrelation of the proposed PUF circuit fluctuates between −0.3 and 0.3. The low autocorrelation rates mean that the PUF is resistant to correlation analysis.

The output data of IM-PUF is measured with 60 samples PCB. Recording this data, we use a hamming distance of the IM-PUF output to demonstrate the randomness characteristic. Figure 12 shows the hamming distance of the IM-PUF circuit. As can be seen, the distribution of hamming distance is consistent with standard normal distribution. The Normalized Standard Deviation (σ) of IM-PUF is 0.0611, while the Normalized Standard Deviation of [31, 32] is 0.0818 and 0.0627, respectively. This means the proposed PUF circuit has better randomness characteristic.

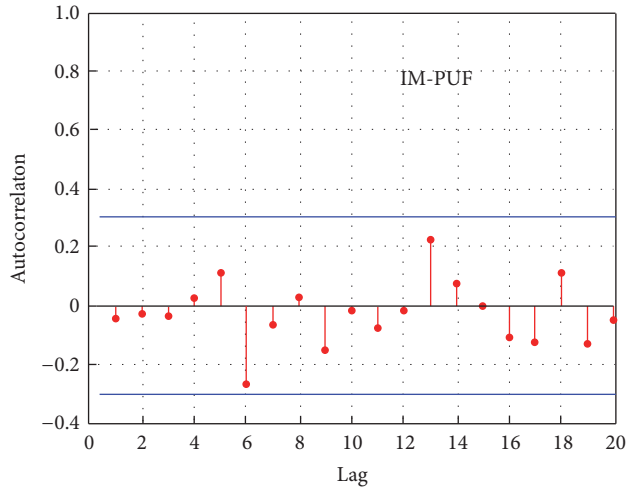

Figure 11: Autocorrelation of the IM-PUF output.

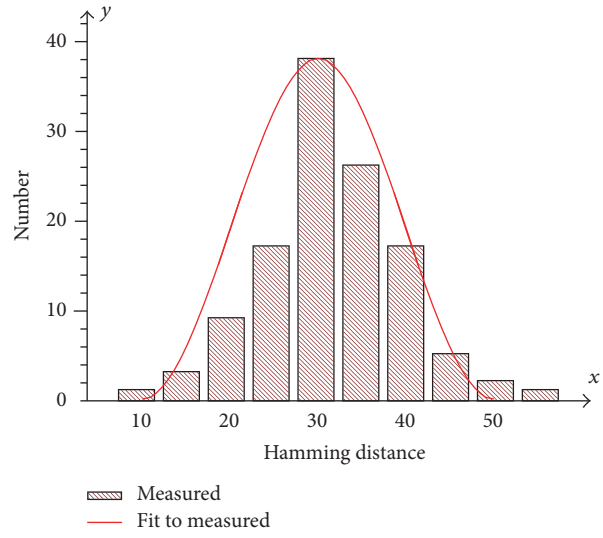

Figure 12: Measured hamming distance for IM-PUF.

Table 1: The comparison with other works.

Paper	PUFs type	Frequency (Hz)	Variation source
TNANO, 2015 [8]	MRAM-PUF	—	Material-level
VLSI, 2005 [11]	Arbiter-based PUFs	100 M	Circuit-level
CHES, 2010 [12]	Glitch PUFs	50 M	Circuit-level
IFS, 2011 [13]	Time Bounded	20 M	Circuit-level
Scientific reports, 2015 [14]	mrS-PUFs	25 M	Material-level
This work	IM-PUFs	100 M	Board-level

Key characteristics of implemented PUFs are summarized in Table 1. Our design is the first reported in board-level

PUFs that can read out an ID at each PCB. Because the variation of transmission line will lead to impedance mismatch and signal reflection, the high-frequency signal processing is very hard in board-level. The 100 M frequency of IM-PUF is closed to the best circuit about arbiter-based PUFs. The total number of possible IM-PUF data depends on the number of the transmission lines (2^N). There are so much possible transmission lines in PCB that it is feasible for an adversary to guess the output. And also, under a fixed input, the output data varies across different PCBs, because the IM-PUF responses are designed to be sensitive to circuit delays which are determined by process variation in wires. Since process variation is beyond the manufacturers' control, no one can physically clone the IM-PUF. So the impedance mismatch Physical Unclonable Functions eliminate the problems of a board-level physical feature recognition technique.

6. Conclusion

We proposed a new kind of PUF circuit design based on PCB. Imposing the impedance matching characteristic of high-frequency PCB circuit, changing length and width of the transmission line, causes the output of the upper cut-off frequency to be different. With this frequency as a counter clock frequency, the output produced by the deviation frequency circuit is different, and with the same time T, the count value is also different. Due to the difference in count value, the comparison circuit would output a binary response signal. The function of this PUF on a PCB is unpredictable, so the security of the IoT will be improved.

Competing Interests

The authors declare that they have no competing interests.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (nos. 61404076, 61474068, and 61274132); the Zhejiang Provincial Natural Science Foundation of China (no. LQ14F040001); The S&T Plan of Zhejiang Provincial Science and Technology Department (no. 2015C31010); China Spark Program (no. 2015GA701053); and Programs Supported by Ningbo Natural Science Foundation (nos. 2014A610148 and 2015A610107).

References

[1] F. Ganz, D. Puschmann, P. Barnaghi, and F. Carrez, "A practical evaluation of information processing and abstraction techniques for the internet of things," *IEEE Internet of Things Journal*, vol. 2, no. 4, pp. 340–354, 2015.

[2] M. Görges, G. A. Dumont, C. L. Petersen, and J. M. Ansermino, "Using machine-to-machine/'Internet of Things' communication to simplify medical device information exchange," in *Proceedings of the International Conference on the Internet of Things (IoT '14)*, pp. 49–54, Cambridge, Mass, USA, October 2014.

[3] http://www.gartner.com/newsroom/id/3291817.

[4] R. Roman, P. Najera, and J. Lopez, "Securing the Internet of things," *Computer*, vol. 44, no. 9, pp. 51–58, 2011.

[5] http://ahmedbanafa.blogspot.com/2015/03/internet-of-things-iot-security-privacy.html.

[6] A. P. Johnson, R. S. Chakraborty, and D. Mukhopadhyay, "A PUF-enabled secure architecture for FPGA-based IoT applications," *IEEE Transactions on Multi-Scale Computing Systems*, vol. 1, no. 2, pp. 110–122, 2015.

[7] D. Mukhopadhyay, "PUFs as promising tools for security in Internet of things," *IEEE Design & Test*, vol. 33, no. 3, pp. 103–115, 2016.

[8] J. Das, K. Scott, S. Rajaram, D. Burgett, and S. Bhanja, "MRAM PUF: a novel geometry based magnetic PUF with integrated CMOS," *IEEE Transactions on Nanotechnology*, vol. 14, no. 3, pp. 436–443, 2015.

[9] Y. Zhang, P. Wang, Y. Li, X. Zhang, Z. Yu, and Y. Fan, "Model and physical implementation of multi-port PUF in 65 nm CMOS," *International Journal of Electronics*, vol. 100, no. 1, pp. 112–125, 2013.

[10] M. T. Rahman, F. Rahman, D. Forte, and M. Tehranipoor, "An aging-resistant RO-PUF for reliable key generation," *IEEE Transactions on Emerging Topics in Computing*, vol. 4, no. 3, pp. 335–348, 2016.

[11] D. Lim, J. W. Lee, B. Gassend, G. E. Suh, M. Van Dijk, and S. Devadas, "Extracting secret keys from integrated circuits," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 13, no. 10, pp. 1200–1205, 2005.

[12] D. Suzuki and K. Shimizu, "The glitch PUF: a new delay-PUF architecture exploiting glitch shapes," in *Proceedings of the 12th International Conference on Cryptographic Hardware and Embedded Systems (CHES '10)*, pp. 366–382, San Diego, Calif, USA, 2010.

[13] M. Majzoobi and F. Koushanfar, "Time-bounded authentication of FPGAs," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 1123–1135, 2011.

[14] Y. Gao, D. C. Ranasinghe, S. F. Al-Sarawi, O. Kavehei, and D. Abbott, "Memristive crypto primitive for building highly secure physical unclonable functions," *Scientific Reports*, vol. 5, Article ID 12785, 2015.

[15] T. Machida, D. Yamamoto, M. Iwamoto, and K. Sakiyama, "A new arbiter PUF for enhancing unpredictability on FPGA," *The Scientific World Journal*, vol. 2015, Article ID 864812, 13 pages, 2015.

[16] M. Wan, Z. He, S. Han, K. Dai, and X. Zou, "An invasive-attack-resistant PUF based on switched-capacitor circuit," *IEEE Transactions on Circuits and Systems. I. Regular Papers*, vol. 62, no. 8, pp. 2024–2034, 2015.

[17] D. P. Sahoo, P. H. Nguyen, D. Mukhopadhyay, and R. S. Chakraborty, "A case of lightweight PUF constructions: cryptanalysis and machine learning attacks," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 34, no. 8, pp. 1334–1343, 2015.

[18] G. T. Becker, A. Wild, and T. Güneysu, "Security analysis of index-based syndrome coding for PUF-based key generation," in *Proceedings of the IEEE International Symposium on Hardware-Oriented Security and Trust (HOST '15)*, pp. 20–25, IEEE, Washington, DC, USA, May 2015.

[19] Y. J. Peng, Y. G. He, J. R. Guo, S. H. Wang, and B. F. Cao, "Study for signal reflections in transmission lines," *Modern Electronic Technology*, vol. 30, no. 21, pp. 179–184, 2007.

[20] C. D. Wu, *A Study On Signal Integrity of High-Speed Digital Design*, Xi'an Electronic and Science University, Xi'an, China, 2005.

[21] L. Chen, "Analysis of reflection of signal integrity of transmission line," *Industry and Minc Automation*, vol. 40, no. 3, pp. 49–52, 2014.

[22] G. Z. Wen and J. D. Tan, "Impedance matching on transmission line," *Modern Electronics Technique*, vol. 29, no. 10, pp. 140–142, 2006.

[23] X. Y. Chen, K. Li, T. Dan, and M. D. Chen, "Model and calculation of microstrip multi capacitor load impedance matching," *Information and Electronic Engineering*, vol. 2, no. 2, pp. 106–108, 2004.

[24] THS3001 Datasheet, http://www.ti.com/lit/ds/symlink/ths3001-die.pdf.

[25] S. B. Tong and C. Y. Hua, *Analog Electronic Technology Foundation*, Higher Education Press, Beijing, China, 2006.

[26] X. Su, "Analysis and simulation of impedance matching in transmission line of high speed circuits," *Coal Technology*, vol. 30, no. 10, pp. 38–40, 2011.

[27] P. Jiang, *The Research of Board-Level Signal Integrity, Power Integrity and Electromagnetic Interference*, Inner Mongolia University, Hohhot, China, 2015.

[28] C. B. Zheng, *Analysis and Design of PCB Signal Integrity*, 2008.

[29] OPA847 Datasheet, http://www.ti.com/lit/ds/symlink/opa847.pdf.

[30] https://en.wikipedia.org/wiki/Autocorrelation.

[31] K. Yang, Q. Dong, D. Blaauw, and D. Sylvester, "14.2 A physically unclonable function with BER $< 10^{-8}$ for robust chip authentication using oscillator collapse in 40 nm CMOS," in *Proceedings of the 2015 IEEE International Solid-State Circuits Conference (ISSCC '15)*, pp. 1–3, San Francisco, Calif, USA, 2015.

[32] Y. Su, J. Holleman, and B. P. Otis, "A digital 1.6 pJ/bit chip identification circuit using process variations," *IEEE Journal of Solid-State Circuits*, vol. 43, no. 1, pp. 69–77, 2008.