Physically Unclonable Function Based on Disordered Photonic Structure

Qian Li*, Feiliang Chen, Mo Li*, Heng Long, Peng Sun, Jian Zhang
Microsystem & Terahertz Research Center of China Academy of Engineering Physics, 596 Yin He Road, Chengdu, China 610200

Abstract

We build the numerical simulation modeling of the physically unclonable function based on disordered photonic structure. The demonstration of uniqueness and tamper evidence properties of disordered photonic PUF is presented by numerical simulation in this paper. The relevant results provide theoretical supports for optimal designing and generating disordered photonic PUF.

I. Introduction

Physically unclonable functions (PUF) are physical security object consisting of disordered structure that cannot be feasibly cloned because of its fabrication process inherently contains a large number of random and uncontrollable factors [1]. This means that once a PUF is manufactured, it is unique, just like a fingerprint, but much more complex. As result, it's nearly impossible to clone or concoct a sufficiently accurate PUF [2]. Therefore, PUF is a very promising and trustworthy solution for the fields of hardware security, such as secure authentication, identification, cryptographic key generation.

Based on the intrinsic random physical features, a PUF can output an unpredictable response when being challenged, which can be regarded as a one-way functional operation. Usually, a challenge–response pair (CRP) behavior is used to describe the PUF physically. The relation enforced between challenges and responses by one particular PUF is referred to as its CRP behavior [3]. The CRP behavior can reflect the inner microstructure properties of PUF in great extent.

The concept of PUF was first proposed as physical one-way functions in 2001 by R.S. Pappu [4,5]. Since thenvarious types of PUFs were proposed , including optical-based PUFs, RF-based PUFs, electronics-based PUFs, magnetic-based PUFs, acoustical-based PUFs and etc. Among those, disordered photonic structure (DPS) based PUFs are regard as one of the most promising PUFs, because it can be stimulated by quantum light and combined with quantum key distribution (QKD). DPS-based PUF has been studied experimentally in recent years. However, simulation and theoretical study is relatively rare, especially for PUF properties and mechanism study. For example, although widely believed to be one of the main advantages of PUF technology, tamper evidence was only experimentally verified for the (non-intrinsic) optical and coating PUFs.

In this paper, we present the demonstration of uniqueness and tamper evidence properties of DPS-based PUF by numerical simulation, The relevant results provide theoretical supports for optimal designing and generating disordered photonic PUF.

II. Simulation Models and Device Structure

In our simulation, the process is mainly divided into two steps. The first step is the construction of DPS-based PUF as numerical simulation modeling. Due to the complexity and disorder of optical PUF with microstructure characteristics, it is unable to apply directly to the existing commercial software modeling. Thus we build disordered microstructure model by Matlab software with optimization algorithm. The schematic view of DPS-based PUF generated randomly using Matlab software is shown in figure 1. The second step, two-dimension finite-difference time-domain (FDTD) method is employed. And the input electric field intensity in the incident optical beam as the unity is taken as the challenge. The calculated distribution of the square of relative electromagnetic field components is taken as the response of the PUF. The perfect matched layers are imposed at the front and back surfaces. To ensure the accuracy the grid size is carefully chosen. As we know, this is the first numerical simulation of the DPS-based PUF.

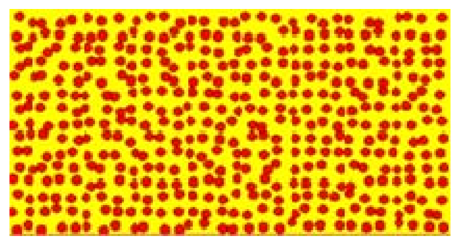

Figure 1. (Color online) The schematic view of DPS-based PUF generated randomly by Matlab software.

III. Result And Discussion

An effective PUF should possess a seriesof attractive properties including unclonable, unique, reproducible, unpredictable, one-way, tamper evident. Uniqueness is the core property of a PUF. When the same challenge is injected on differentPUFs, they output different responses, or we call CRP behavior. From the information theoretic sense, one possible measure of uniqueness which is provided in most experimental results is the Hamming inter-distance histogram, summarized by its average value μ_{inter}. For an ideal PUF, the average value μ_{inter} should be 0.5.

* Corresponding author: limo@mtrc.ac.cn, liqian@mtrc.ac.cn.

The uniqueness of optical PUF is demonstrated by simulating different PUFs with randomly distributed nanoparticles. Different disordered photonic structures output completely different scattered distribution of the electromagnetic field, showing that two random optical PUFs can be identified through the speckle figure in figure 2. The Hamming distance between two random disordered structure is close to 0.5, as shown in table 1. The results prove the optical PUF is unique and can be used for authentication.

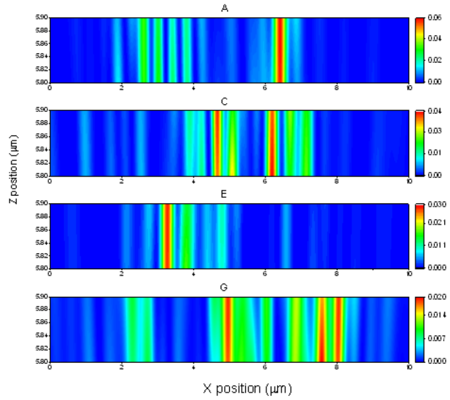

Figure 2. (Color online) the simulated distribution of the square of relative electromagnetic field components of four different PUFs.

Table 1. The Hamming inter-distance of eight disordered photonic PUFs (labelled as a - h) with the same particle size and thickness.

	a	b	c	d	e	f	g	h
a	0	0.49	0.43	0.51	0.54	0.53	0.54	0.51
b	0.49	0	0.42	0.52	0.41	0.47	0.50	0.54
c	0.43	0.42	0	0.45	0.45	0.50	0.47	0.50
d	0.51	0.52	0.45	0	0.46	0.50	0.46	0.53
e	0.54	0.41	0.45	0.46	0	0.49	0.46	0.48
f	0.53	0.47	0.50	0.50	0.49	0	0.37	0.55
g	0.54	0.50	0.47	0.46	0.46	0.37	0	0.49
h	0.51	0.54	0.50	0.53	0.48	0.55	0.49	0

Tamper evident property is also a very significant feature of PUF. It means CRP behaviors of PUF will change if it is eampered. Here, a PUF with 600 disordered nanoparticles is simulated, and 1 or 2 of these nanoparticles is removed for comparison, as shown in figure 3. However, the simulation results show thatthe scattering distributions of electromagnetic field are completely different (see Fig 4). This phenomenon is caused by the light localization and the change of scattering paths. The Hamming distance between the three disordered structure is 0.31, 0.40 and 0.45. The numerical results commendably validate the tamper evident property of disordered photonic PUF.

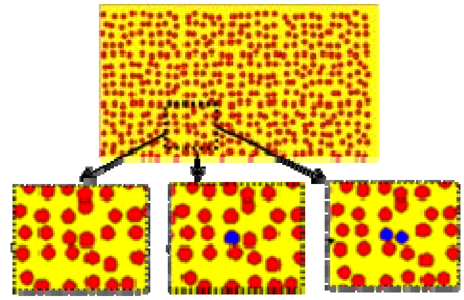

Figure 3. (Color online) The schematic view of DPS-based PUF tamper evident modeling (left); PUF with one nanoparticle removed (middle); PUF with two nanoparticles removed (right).

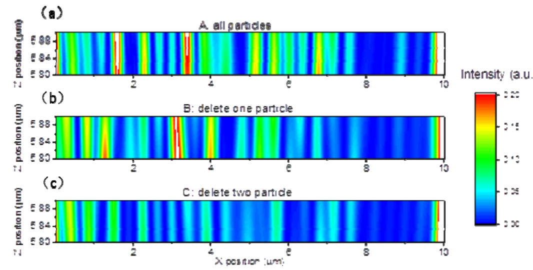

Figure 4 (Color online) the simulated distribution of the squared electromagnetic field components of three PUFs with tiny differences.

IV. Conclusion

In this paper, we reported a simulation of disordered photonic PUFs, through building the numerical simulation modeling of the PUF and calculating the scattered distribution of the electromagnetic field. The results commendably validate the unique and tamper evident property of disordered photonic PUF which are important to be used for authentication. The relevant results provide the theoretical guidance for the optimal design and generate disordered photonic PUF.

References

[1] S.A. Goorden, M. Horstmann, A.P. Mosk, B. Škorić, and P.W.H. Pinkse, Optica 1, 42-424 (2014).

[2] J. D. R. Buchanan, R. P. Cowburn, A. Jausovec, D. Petit, P. Seem, G. Xiong, D. Atkinson, K. Fenton, D. A. Allwood, and M. T. Bryan, Nature 436, 475 (2005).

[3] 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, ser. Information Security and Cryptography, D. Basin, U. Maurer, A.-R. Sadeghi, and D. Naccache, Eds. Springer Berlin Heidelberg, pp. 3–37, (2010).

[4] R.S. Pappu, Physical One-Way Functions, Ph.D. thesis, Massachusetts Institute of Technology, (2001).

[5] R.S. Pappu, B. Recht, J. Taylor, N. Gershenfeld, Science 297, 2026-2030 (2002).