PAPER

Architecture and Physical Implementation of Reconfigurable Multi-Port Physical Unclonable Functions in 65 nm CMOS

Pengjun WANG[†a)], **Yuejun ZHANG**[†b)], **Jun HAN**[††], *Nonmembers*, **Zhiyi YU**[††], **Yibo FAN**[††], *Members*, *and* **Zhang ZHANG**[†††], *Nonmember*

SUMMARY In modern cryptographic systems, physical unclonable functions (PUFs) are efficient mechanisms for many security applications, which extract intrinsic random physical variations to generate secret keys. The classical PUFs mainly exhibit static challenge-response behaviors and generate static keys, while many practical cryptographic systems need reconfigurable PUFs which allow dynamic keys derived from the same circuit. In this paper, the concept of reconfigurable multi-port PUFs (RM-PUFs) is proposed. RM-PUFs not only allow updating the keys without physically replacement, but also generate multiple keys from different ports in one clock cycle. A practical RM-PUFs construction is designed based on asynchronous clock and fabricated in TSMC low-power 65 nm CMOS process. The area of test chip is 1.1 mm^2, and the maximum clock frequency is 0.8 GHz at 1.2 V. The average power consumption is 27.6 mW at 27°C. Finally, test results show that the RM-PUFs generate four reconfigurable 128-bit secret keys, and the keys are secure and reliable over a range of environmental variations such as supply voltage and temperature.

key words: *RM-PUFs, reconfigurable, Multi-port, asynchronous clock, 65 nm*

1. Introduction

Physical unclonable functions (PUFs) provide a basis for many securities and digital rights management protocols, e.g., smart cards, credit cards, radio frequency identification (RFID) tags, value papers, chips, security cameras, etc. PUF-based security approaches have numerous comparative strengths with respect to traditional cryptography-based techniques, including resilience against physical and side channel attacks and suitability for lightweight protocols [1]. Research works have been carried out for developing PUFs circuit. Arbiter-based physical unclonable functions exploit the statistical delay variation of wires and transistors across integrated circuits (ICs) in manufacturing processes to build unclonable secret keys [2]. Truly unclonable tokens PUFs are introduced by Pappu et al. [3]. These tokens are so complex that it is infeasible to fully read out the data contained in a token. This makes PUFs suitable for online protocols as well as verification involving physical probing by untrusted devices. Skoric B analyses capacitive physical unclonable functions by information theoretic [4]. Holcomb presents a system of fingerprint extraction and random numbers in SRAM (FERNS) that harvests static identity and randomness from existing volatile CMOS memory without requiring any dedicated circuitry [5]. Ying Su designs a 128-bit, 1.6 pJ/bit, 96% stable chip identification generation circuit utilizing process variations in a 0.13 μm CMOS process [6]. Ulrich Ruhrmair proposes the new concept a "SHIC PUF", where SHIC stands for super high information content [7].

However, the classical PUFs exhibit static challenge-response behaviors and generate static keys. The private key generation by PUFs is vulnerable against replay attacks. For example, the encrypted data stored in a memory can be replaced by other data with the same private key. In order to resistant the replay attacks, the encrypted data can be encrypted with dynamic keys. Instead of using static key generation, reconfigurable PUFs generate dynamic public-private key pairs for cryptographic systems. In this paper, the concept of reconfigurable multi-port PUFs (RM-PUFs) is proposed. RM-PUFs allow updating the key without physically replace and generating multiple keys from different ports. A practical RM-PUFs construction is designed and fabricated in Taiwan Semiconductor Manufacturing Company (TSMC) low-power 65 nm CMOS process. The RM-PUFs eliminate the stated PUFs limitations and generate four 128-bit secret keys in one chip. The test chip has an area of 1.1 mm^2, and has a peak clock frequency of 0.8 GHz at 1.2 V. The average power consumption is 27.6 mW. Finally, measured results show that the keys generated from RM-PUFs are secure and reliable over a practical range of environmental variations such as supply voltage and temperature.

This paper is organized as following: The related works of PUFs have been introduced in Sect. 2. The model of RM-PUFs is discussed in Sect. 3. The circuit architecture of RM-PUFs is discussed in Sect. 4. The chip fabrication and measurement results are proposed in Sect. 5. Security analysis and evaluation are discussed in Sect. 6. Finally, the conclusion is given in Sect. 7.

2. Related Works

Physical unclonable functions map input challenges to output responses using a function determined by the inherent variations of intrinsic random physical variations. In 2002, the primary notion of PUFs was achieved by Pappu et al.

Manuscript received August 20, 2012.
Manuscript revised January 9, 2013.

[†]The authors are with Institute of Circuits and Systems, Ningbo University, Ningbo Zhejiang, China.
[††]The authors are with State Key Laboratory of ASIC & System, Fudan University, Shanghai, China.
[†††]The author is with Electronics and Apply Physical School, Hefei University of Technology, Hefei Anhui, China.
a) E-mail: wangpengjun@nbu.edu.cn
b) E-mail: zyj99.com@163.com

DOI: 10.1587/transfun.E96.A.963

and reported in journal *SCIENCE* [3]. Their initial targeted PUFs platform was an optical coherence system. Integrated circuit identifiers (ICIDs) are completely static features that provide excellent accounting mechanisms, while basically have no security features. A significant practical step to enable instantaneous and widespread application of PUFs concept was proposal of Gassend et al. who leverage silicon manufacturing variability and had implemented experiments that reliable authentication of individual FPGA can be performed even in the presence of significant environmental variations [8], [9]. These works motivated several silicon PUFs that use various mechanisms to extract a secret. The most prominent examples of electrical PUFs include arbiter PUFs [2], ring oscillator PUFs [10], memory-based PUFs [5], [11], glitch PUFs [12] and coating PUFs [13]. Besides, the application domain of PUFs is much larger. PUFs can be powerful candidates for creation of the new generation of security and cryptographically protocols that are intrinsically more resilient against physical and side channel attacks [13]. This wide range of PUFs applications has one ramification: significantly more stringent operation and security requirements [14]. There are also conceptually sharply different mechanisms for PUFs [15]–[17].

Unfortunately, the proposed silicon PUFs often is subject to significant security vulnerabilities. For example, the states of PUFs are limited by the hardware and the PUFs generate only one bit data per clock cycle. In this work, the concept of reconfigurable multi-port PUFs is proposed. RM-PUFs not only allow updating the keys without physically replace, but also generate multiple keys from different ports in one clock cycle. Instead of using static key generation, RM-PUFs generate dynamic public-private key pairs for cryptographic systems.

3. The Model and Architecture of RM-PUFs

The notion of RM-PUFs can be defined as a set of physical systems presented by the elements $(S, F, N, C, R_0R_1 \ldots R_n)$ with state space S, function space F, number ports space N, challenge space C, response space $R_0R_1 \ldots R_n$. The secret keys of RM-PUFs depend on both the physical properties of the circuit and the state space S maintained in a non-volatile memory. And the secret keys can be dynamically changed after it has been deployed by updating its state S. An instantiation model of RM-PUFs $F(N, R(S, C))$ has been discussed as the following function.

$$R(c) \leftarrow F(N, R(S, C)), \quad R(c) \in R_0R_1 \ldots R_n \tag{1}$$

Note that $R(c) \in R_0R_1 \ldots R_n$ implies that a completely new unclonable physical system (challenge-response pairs) is generated. The space keys are judged by state space S and challenge space C. And the cryptographic systems can select the number of output ports by reconfiguration control circuit. RM-PUFs combine a reconfigurable physical unclonable function and a multiple ports network circuit. The architecture of RM-PUFs is shown in Fig. 1. The reconfiguration control circuit provides the challenge signal

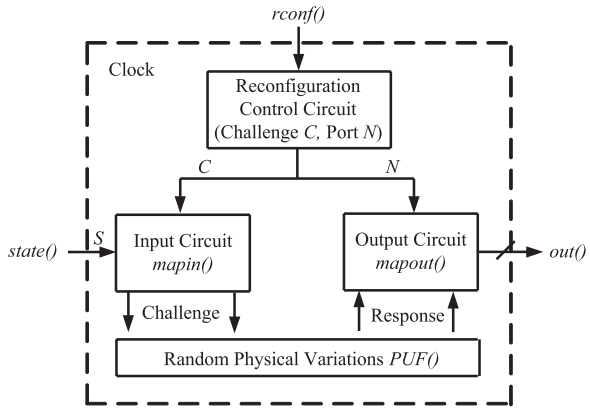


Fig. 1 The architecture of RM-PUFs.

C and number ports N. The input circuit maintains a state S, which is stored in non-volatile memory. The process consists of an input transformation function *mapin()* and an output transformation function *mapout()*. Input circuit computes *x mapin(C, S)*, random physical variations circuit evaluates *y PUF(x)*, and output circuit returns *R mapout(y, N)*. The implementing reconfigure feature of RM-PUFs by changing the current state S to a new state S^*, and the implementing multiple ports feature of RM-PUFs by N ports component and suitable network circuit *out()*.

Setup: The cryptographic systems sets up RM-PUFs by choosing state space S, challenge space C, and number ports space N.

Phase I: Challenge space C is allowed to *rconf()* of the RM-PUFs at the first step. At the end of *rconf()*, challenge C maintains in a non-volatile memory that is used as input to *mapin()*. The output of *mapin()* is set as the challenge of random physical variations *PUF()* during phase I.

Reconfiguration: S reconfigures the RM-PUFs by input circuit *state()*, which updates the internal RM-PUFs from state S to state S^*.

Phase II: Number ports space N is allowed to *rconf()* of the RM-PUFs at the second step. Number ports N is used as input to *mapout()*. The input of *mapout()* is the response of random physical variations *PUF()* during phase II.

Output: Finally, the output network circuit *out()* outputs N pairs challenge/response (c^*, r^*) of the RM-PUFs.

4. The Circuit Design of RM-PUFs

According to the model and architecture of RM-PUFs, we propose a scheme of implemental construction. The block diagram is shown in Fig. 2. RM-PUFs consist of the four fundamental building blocks: (i) input logic network, (ii) random physical variation PUFs, (iii) output logic network, and (iv) wire interconnect network. In the RM-PUFs, the random physical variations are implemented by the asynchronous clocks, and the multiple ports component is implemented by register file.

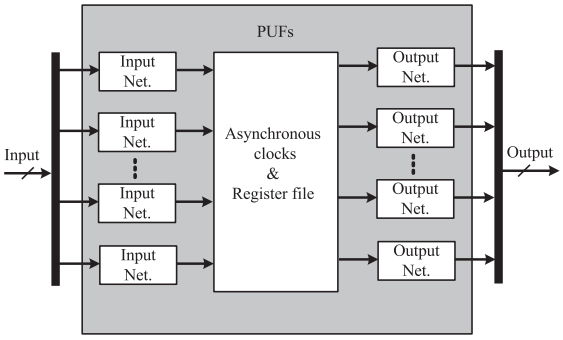


Fig. 2 The block diagram of RM-PUFs.

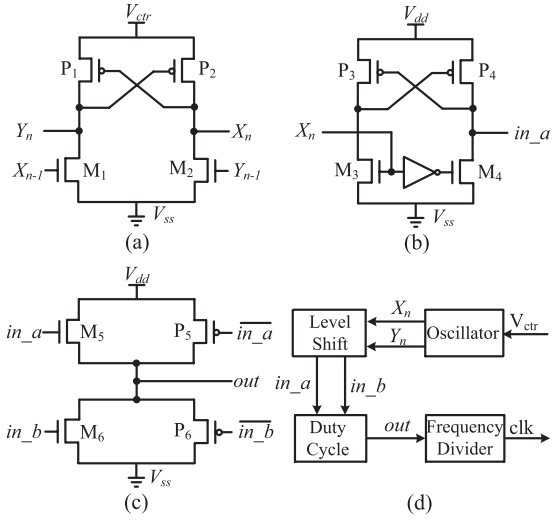


Fig. 3 The circuit of VCO: (a) Differential delay cell, (b) Level Shift, (c) Duty Cycle, (d) Blocks of the VCO.

4.1 Asynchronous Clocks

Asynchronous clocks are consisted of a high frequency clock *clock_f* and a low frequency clock *clock_s*. The *clock_f* is provided by a Voltage Controlled Oscillator (VCO). The *clock_s* is provided by a global clock. We develop VCO through full-custom design under standard 65 nm CMOS process. The schematic of VCO is shown in Fig. 3. There are four blocks: Oscillator, Level Shift, Duty Cycle and Frequency Divider.

Oscillator: Oscillator is implemented by the ring of differential delay cell. The frequency of the Oscillator f_{osc} is [18]:

$$f_{osc} = 1/(2M \cdot T_D) \tag{2}$$

Where T_D is the delay time of one Differential delay cell, M is the number of differential delay cells in the ring Oscillator (M= 9 in this design). The schematic of Differential delay cell is shown in Fig. 3(a). The voltage V_{ctr} control the delay time T_D. Due to the manufacturing variability, the different test chips may have different frequencies under the same V_{ctr}.

Level Shift: The high voltage of Oscillator is V_{ctr}, while V_{dd} is required in the system. There are two Lever Shifts in the VCO. And the schematic of Lever Shift is shown in Fig. 3(b). When $X_n = V_{ss}$, M_4 is open, and $in\_a = V_{ss}$; When $X_n = V_{ctr}$, M_3 is open, and $in\_a = V_{dd}$.

Duty Cycle: Duty Cycle is also an important specification in the applications of VCO. The schematic of Duty Cycle is shown in Fig. 3(c). The principle can be described as: When in_a is V_{dd}, M_5 and P_5 are both open, and $out = V_{dd}$. When in_a changes to V_{ss}, out will keep on the high voltage until in_b turns to V_{dd}. When in_b is V_{dd}, M_6 and P_6 are both open, and $out = V_{ss}$, When in_b changes to V_{ss}, out will keep on the low voltage until in_a turns to V_{dd}. Because in_a and in_b are differential signal, the duty cycle will be 50%.

Frequency Divider: Frequency Divider is composed by 64 inverters chain, and is used to divide the frequency of VCO.

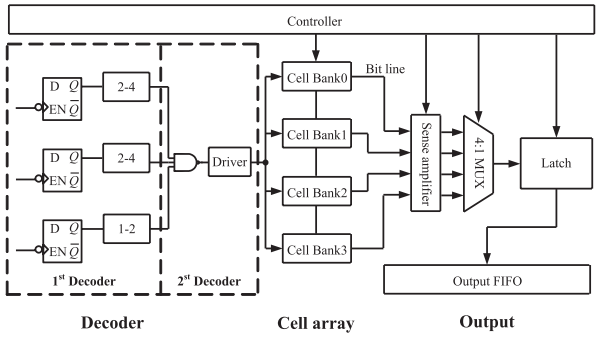


Fig. 4 Block diagram of register file.

4.2 Register File

RM-PUFs employ a register file to implement multiple ports characteristic. And the 4R2W register file is developed through full-custom design in standard 65 nm CMOS process. The 4R2W register file includes Decoder, Cell array and Output circuit. The block diagram is shown in Fig. 4 [19].

Two-stage static decoder technique is adopted for high performance and low power, as shown in Fig. 4. Each word line driver consists of a single large device capable to drive one port of Cell Bank. An active sense amplifier is used to convert the voltage difference on a pair of read bit lines into an output differential voltage. After that, each read port contains a set of output latches to capture the output data.

4.3 Circuit Design of RM-PUFs

In this subsection, we describe the system that efficiently extracts intrinsic frequency deviation between asynchronous clocks as a function of PUFs caused by silicon manufacturing variability. The RM-PUFs unit is shown in Fig. 5. The input signals are *Enable*, *Data*, *Address*, *clock_f* and *clock_s*. The output signals are $Output_0$, $Output_1 \ldots Output_{n-1}$, $Output_n$. Where, *clock_f* is provided by VCO and *clock_s* is provided by Global clock.

The schematic of one port path for RM-PUFs is shown

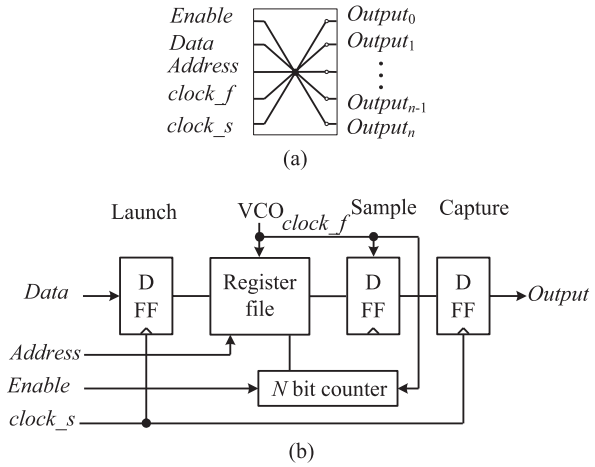


Fig. 5 The RM-PUFs unit: (a) The symbol of RM-PUFs, (b) Schematic of one port path for RM-PUFs.

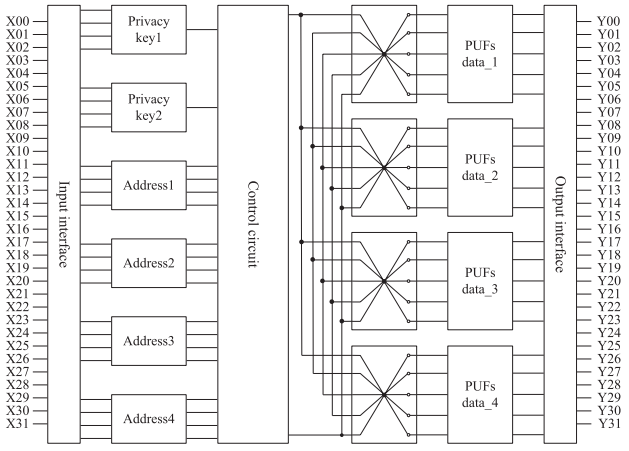


Fig. 6 The circuit of four ports 128 bits RM-PUFs.

in Fig. 5(b), including three flip-flops: launch, sample, and capture. A transition is invoked by the launch flip-flop at the combinatorial register file input. The output of the register file is sampled by VCO clock later and stored by the sample flip-flop. The sampled value is captured by Global clock and the result is recorded by the capture flip-flop. The output logic value is determined by input data and frequency deviation between asynchronous clocks. Because of the manufacturing variability, the different test chips may have different frequencies under the same control voltage. The final output reflects the intrinsic manufacturing variability of silicon.

In this work, we design RM-PUFs with asynchronous clocks and register file. The circuit architecture of four ports 128-bit RM-PUFs are shown in Fig. 6. X_{00}, X_{01}, X_{02}, $X_{03} \ldots X_{28}$, X_{29}, X_{30}, X_{31} are the input data of system including privacy keys and address information. These data initially are stored in internal memory through input interface. The internal memory can be divided as: Privacy key 1, Privacy key 2, Address 1, Address 2, Address 3, Address 4. Then, the privacy keys are written into register file by control circuit and launch flip flop under global clock. If the *Enable* is high, register file read out the privacy keys to sample flip flop in serial from the different port under *clock_f*. Also, a counter is controlled by *Enable* signal and works under *clock_f*. When counter reaches N, the data stored in sample flip flop is record in capture flip-flop. The output of RM-PUFs is stored in stored in memory, which is PUFs data_1, PUFs data_2, PUFs data_3, PUFs data_4. Finally, Y_{00}, Y_{01}, Y_{02}, $Y_{03} \ldots Y_{28}$, Y_{29}, Y_{30}, Y_{31} keys are output through output interface.

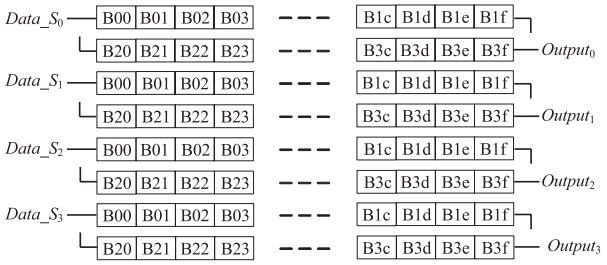


Fig. 7 The data path of four ports 128 bits RM-PUFs.

Sample flip-flops receive the privacy keys from the four output ports of the register file, such as *data_S*$_0$, *data_S*$_1$, *data_S*$_2$, and *data_S*$_3$. The data B_{00}, B_{01}, B_{02}, $B_{03} \ldots B_{3c}$, B_{3d}, B_{3e}, B_{3f} are sampled by Sample flip-flops and transmitted one by one with *clock_f*. In this circuit, we have realized four data paths, as shown in Fig. 7. Also, the privacy keys of each port can be set different. At the some time, the data *Output*$_0$, *Output*$_1$, *Output*$_2$, and *Output*$_3$ are recorded Capture flip-flops with *clock_s*. The output data of Capture flip-flops are defined as the keys of RM-PUFs.

5. Chip Fabrication and Measurement Results

We fabricated RM-PUFs test chips with TSMC 65 nm low-power CMOS technology. Figure 8 shows the die photograph of the test chip, along with Register file, VCO, Core and others [19]. The die area is 1400 μm $\times$ 784 μm. The feature of the fabricated coprocessor is summarized in Fig. 8. The chip is fully synthesized from Verilog, except the VCO and Register file which are implemented by full custom design. There are 34 I/O pads along the die periphery, of which 20 pads are signal pads and the others are power pads.

The viability of the RM-PUFs is related to the environments where the circuit will be used. This section explores the potential influence of supply voltage on the output of RM-PUFs. The reliability of the challenge-response behaviors of RM-PUFs against supply voltage variations is an important measure of quality for PUFs that may be applied in a voltage-varying environment. To evaluate the reliability of the RM-PUFs against supply voltage variations, we measured four 128-bit on a test chip under VCO 680 MHz and 780 MHz at 27°C. The result is shown in Fig. 9. We have not found the data is changed under different supply voltage conditions, and the reliability achieves about 100%. So, it shows great robust feature against supply voltage variations.

To evaluate the reliability of the MPUF against temperature variations, we measured 128-bit on a test chip under

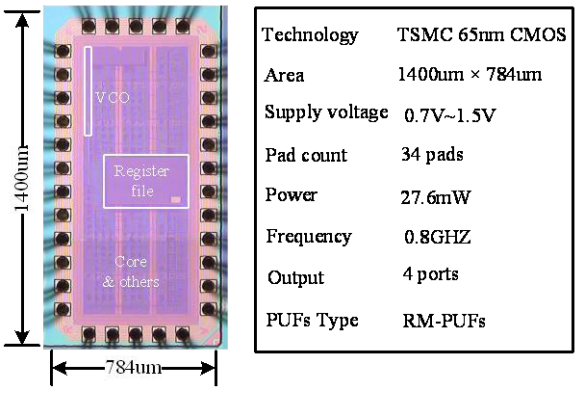


Fig. 8 Micrograph of the RM-PUFs.

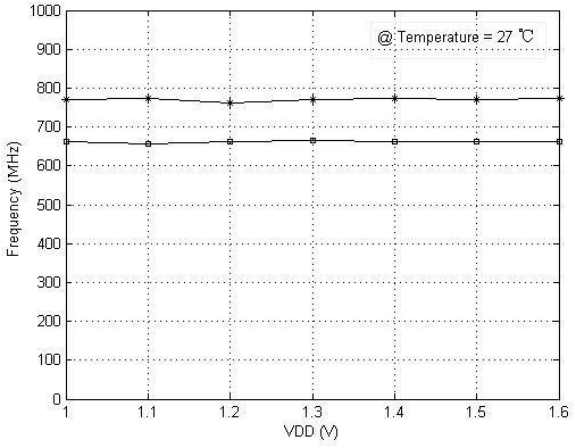


Fig. 9 Frequency versus VDD.

temperatures from 0 to 100°C at 1.2 V. The results are shown in Table 1. We have not found the data is changed under different temperature conditions, and the reliability achieves about 100%. So, it shows great robust feature against temperature variations.

Table 1 shows the output keys codes in hexadecimal format form RM-PUFs for all 4 test chips. Tables 2 and 3 are the calculated Hamming distance result from the output keys of RM-PUFs. Table 2 shows the measured numerical Hamming distance between 16 keys under privacy keys 1. Table 3 shows the measured numerical Hamming distance between 16 keys under privacy keys 2. Figure 10 shows the measured histogram of the measured numerical Hamming distance between 16 keys under privacy keys 1. Figure 11 shows the measured histogram of the measured numerical Hamming distance between 16 keys under privacy keys 2. In addition, the theoretical ideal Hamming distance distribution is plotted for comparison.

6. Security Analysis and Evaluation of RM-PUFs

The characteristics of RM-PUFs is not only classical PUFs robust, physically unclonable, unpredictable, but also reconfigurable and multiple ports. RM-PUFs improve security by amending PUFs with privacy keys that changes the challenge/response pairs. An adversary might be able to obtain the encrypted state with invasive means and even try to overwrite internal state with this encrypted state. However, he will not be successful as the RM-PUFs derived authentication keys will have been updated. It should be noted that appropriate countermeasures must be taken to protect the privacy keys. Power analysis attacks exploit the data dependency of the power consumption of cryptographic de-

Table 1 The keys codes in hexadecimal format for RM-PUFs.

Test Chips	Output Ports	Key Number	The Privacy Keys 1	The Privacy Keys 2
1	1	1	3EE4B99DCE278A63C47167C68C1C1C07	6B2DA495AD95A92F3A4EE4AB5ACD2A69
	2	2	C13CC027F88113FE648059C8FFCF0001	532DD6AACD5AAAB928D6B34A996EB556
	3	3	7E6067CC09FC01FE404BC809FE81FC90	6AD5557233375555552D296EAA909157
	4	4	13FE0067F202F7803E84F62F80FC1FCB	6EAA91D76E912AD52AD555AD52AB5554
2	1	5	D07EC4E42D9B46E0E97074BC3B3E973F	FF803034731C70867BA1B9B9A3232323
	2	6	3D2F3F3C7860C183887C735198E311EA	39CC3A3E1DF000000E7D1F03471DEEE4
	3	7	196798218F1CABEF9E54E3469D1A1C30	CB74979DEA9D55555D4352B293660806
	4	8	39EE18578EF9863BCC3BD863484AEDD5	7310E61A78585C17A13F58074E80017D
3	1	9	6C9A24C3A649999A2464C99213131326	1BD0682161D19E215CEE4CDC93A2FDA6
	2	10	24C9999932E7CCD1B766DB366CD16ECD	802F09FC3694293857A856A82ADD24CA
	3	11	93266666CCCCCC91909191272F270C4C	AB6554B5AA9B9325555555509332416B4
	4	12	0C4C4859998C9999B261D22C936BB4D2	8D9B12D68933245AD2365555212AAEDD
4	1	13	000000001FFFFFFFE0000000127997BA	600000001C002070FFFFFFFC0000000
	2	14	1FFFFFFF797B1E7A00000000FFFFFFF	FFFFFFFFF000000007FFFFFFD36CC68
	3	15	000000001FFFFFFFE00000001FFFFFF	FFFFFFFFE5F33FF7FFFFFFFC0000000
	4	16	1FFFFFFFE0000000000000003FFFFFF	C00000000000000213EE1B5E48012F0F

Table 2 Measured numerical Hamming distance under privacy keys 1.

67	65	65	60	65	45	55	64	62	63	66	70	60	70	63
0	62	62	59	70	64	68	59	77	62	63	63	65	61	64
0	0	88	71	66	68	60	67	71	64	57	59	65	59	62
0	0	0	61	62	62	66	67	65	60	61	67	59	69	58
0	0	0	0	71	65	69	64	78	61	66	56	60	56	59
0	0	0	0	0	60	64	63	65	62	61	69	61	73	54
0	0	0	0	0	0	58	63	71	62	55	57	63	59	72
0	0	0	0	0	0	0	67	61	60	61	65	65	61	66
0	0	0	0	0	0	0	0	64	67	58	56	66	62	63
0	0	0	0	0	0	0	0	0	71	60	68	66	62	69
0	0	0	0	0	0	0	0	0	0	59	67	65	63	58
0	0	0	0	0	0	0	0	0	0	0	50	62	54	63
0	0	0	0	0	0	0	0	0	0	0	0	56	12	77
0	0	0	0	0	0	0	0	0	0	0	0	0	44	23
0	0	0	0	0	0	0	0	0	0	0	0	0	0	65

Table 3 Measured numerical Hamming distance under privacy keys 2

61	75	55	65	64	60	63	69	54	57	70	62	68	61	64
0	74	60	74	67	65	66	64	73	62	67	67	63	64	67
0	0	68	58	71	59	54	62	65	58	67	63	69	60	63
0	0	0	62	65	61	64	66	63	56	61	59	63	56	71
0	0	0	0	65	59	62	62	67	62	67	55	67	64	55
0	0	0	0	0	74	61	61	62	61	58	60	52	69	58
0	0	0	0	0	0	63	61	64	45	70	66	62	57	70
0	0	0	0	0	0	0	66	79	68	69	57	67	64	55
0	0	0	0	0	0	0	0	73	56	69	65	65	64	59
0	0	0	0	0	0	0	0	0	63	66	60	68	71	58
0	0	0	0	0	0	0	0	0	0	61	69	65	64	71
0	0	0	0	0	0	0	0	0	0	0	64	62	65	56
0	0	0	0	0	0	0	0	0	0	0	0	60	51	36
0	0	0	0	0	0	0	0	0	0	0	0	0	43	64
0	0	0	0	0	0	0	0	0	0	0	0	0	0	79

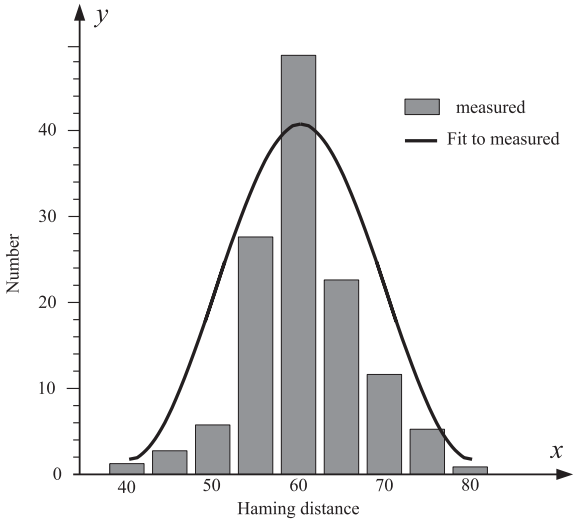


Fig. 10 Measured numerical Hamming distance under privacy keys 1.

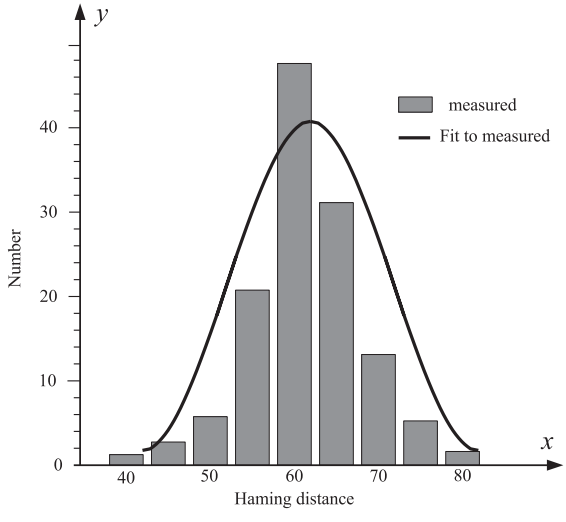


Fig. 11 Measured numerical Hamming distance under privacy keys 2.

Table 4 The comparison with others' implementations.

Paper	PUFs type	Process (nm)	Power (W)	Frequency (Hz)	Number Ports	Reliability	Reconfigure
Lim's[2]	Arbiter-based PUFs	180	137u	100M	1	95%	No
Holcomb's [5]	SRAM	350	250u	25M	1	-	No
Rührmair's [7]	SHIC PUFs	32	72m	100	1	95%	No
Majzoob's [9]	Time-bounded	Xilinx Virtex 5	-	20M	1	90%	No
Ying's [10]	Cross-coupled logic	130	1.6u	1M	1	96%	No
Suzuki's[12]	Glitch PUFs	Xilinx Spartan-3A	-	50M	1	93.4%	No
Majzoob's [15]	Reconfigurable PUFs	Xilinx Virtex 5	-	15M	1	90%	Yes
In this work	RM-PUFs	65	27.6m	0.8G	4	100%	Yes

vices. RM-PUFs improve security by processing multiple keys in one clock cycle to reduce dependency between keys and power.

The keys of RM-PUFs are assigned randomly. Thus, there is a possibility of key code collision within a given number of chips, even if all bits in the key code are stable. Modeling the key collision probability is important for investigating the security of RM-PUFs. The probability of key collision across chips can be represented as [20]:

$$P_{collision} = 1 - \prod_{n=1}^{Y}\left(1 - \frac{n-1}{2^x}\right) \tag{3}$$

This probability model assumes the number of chips (Y) is smaller than the total number of available key codes 2^x — a reasonable assumption with a 128-bit key length. The key collision probability for a 128-bit key code versus different number of chips is highly reliable since the key collision probability is vanishingly small.

Key characteristics of implemented RM-PUFs are summarized in Table 4. Frequency and reliability of our design are best in class. Our design is the first reported in reconfigurable and multi-port PUFs that allows updating the keys without physically replace, and generates multiple keys from different ports in one clock cycle.

7. Conclusion

From characteristics of register file and principles of process variation, a new design scheme for reconfigurable multi-port PUFs is proposed in this paper. The RM-PUFs circuit which utilizing asynchronous clock and register file is designed and fabricated in a TSMC low-power 65 nm CMOS process. The RM-PUFs eliminate the stated PUF limitations and generate multiple secret keys in one chip. RM-PUFs not only allow updating the keys without physically replacement, but also generate multiple keys from different ports in one clock cycle. A practical RM-PUFs construction is designed based on asynchronous clock and fabricated in TSMC low-power 65 nm CMOS process. The test chip has an area of 1.1 mm^2, and has a peak clock frequency of 0.8 GHz at 1.2 V. The average power consumption is 27.6 mW at 27°C. Finally, measured results show the RM-PUFs generate four reconfigurable 128-bit secret keys, and the keys are secure and reliable over a range of environmental variations such as temperature and power supply voltage.

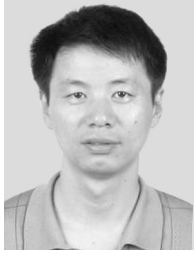
Acknowledgments

This project is supported by the National Natural Science Foundation of China (61274132, 61076032); Research Fund for the Doctoral Program of Higher Education of China (20113305110005); the Key Project of Zhejiang Provincial Natural Science Foundation of China (Z1111219); the K. C. Wong Magna Fund in Ningbo University, China; the Excellent Doctoral Dissertation Foundation of China (PY20100003); National Significant Science and Technology Projects – 01 Special 2010ZX01030-001-001 -03.

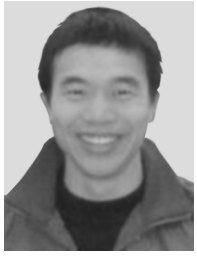
References

[1] D. Lim, "Extracting secret keys from integrated circuit," Massachusetts Institute of Technology, pp.1–119, 2004.
[2] D. Lim, J.W. Lee, B. Gassend, G.E. Suh, M. Dijk, and S. Devadas, "Extracting secret keys from integrated circuits," IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol.13, no.10, pp.1200–1205, 2005.
[3] R. Pappu, B. Recht, J. Taylor, and N. Gershenfeld, "Physical one-way functions," Science, vol.297, no.5589, pp.2026–2030, 2002.
[4] B. Skoric, S. Maubach, T. Kevenaar, and P. Tuyls, "Information-theoretic analysis of capacitive physical unclonable functions," J. Appl. Phys., vol.100, no.2, pp.024902-1–024902-11, 2006.
[5] D.E. Holcomb, W.P. Burleson, and K. Fu, "Power-up SRAM state as an identifying fingerprint and source of true random numbers," IEEE Trans. Comput., vol.58, no.9, pp.1198–1210, 2009.
[6] S. Ying, J. Holleman, and B.P. Otis, "A digital 1.6 pJ/bit chip identification circuit using process variations," IEEE J. Solid-State Circuits, vol.43, no.1, pp.69–77, 2008.
[7] U. Rührmair, C. Jaeger, M. Bator, M. Stutzmann, P. Lugli, and G. Csaba, "Applications of high-capacity crossbar memories in cryptography," IEEE Trans. Nanotechnol., vol.10, no.3, pp.489–498, 2011.
[8] B. Gassend, D. Clarke, M. Dijk, and S. Devadas, "Silicon physical random functions," Computer and Communications Security (CCS), pp.148–160, 2002.
[9] M. Majzoobi and F. Koushanfar, "Time-bounded authentication of FPGAs," IEEE Trans. Information Forensics and Security, vol.6, no.3, pp.1123–1135, 2011.
[10] S. Stanzione, D. Puntin, and G. Iannaccone, "CMOS silicon physical unclonable functions based on intrinsic process variability," IEEE J. Solid-State Circuits, vol.46, no.6, pp.1456–1463, 2011.
[11] D.Y. Meng, M.R. David, S. Richard, and S. Devadas, "Light weight and secure PUF key storage using limits of machine learn-

ing," Workshop on Cryptographic Hardware and Embedded Systems (CHES 2011), LNCS 6917, pp.358–373, 2011.
[12] D. Suzuki and K. Shimizu, "The glitch PUF: A new delay-PUF architecture exploiting glitch shapes," Workshop on Cryptographic Hardware and Embedded Systems (CHES 2010), LNCS 6225, pp.366–382, 2010.
[13] G. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," Design Automation Conference (DAC), pp.9–14, 2007.
[14] S. Stanzione and G. Iannaccone, "Silicon physical unclonable function resistant to a 1025-trial brute force attack in 90 nm CMOS," Symposium on VLSI Circuits (VLSI), pp.116–117, 2009.
[15] M. Majzoobi, F. Koushanfar, and M. Potkonjak, "Techniques for design and implementation of secure reconfigurable PUFs," ACM Trans. Reconfigurable Technology and Systems, vol.2, no.1, pp.1–33, 2009.
[16] X. Xin, J. Kaps, and K. Gaj, "A configurable ring-oscillator-based PUF for xilinx FPGAs," 2011 14th Euromicro Conference on Digital System Design (DSD), pp.651–657, 2011.
[17] K. Stefan, K. Ünal, V.L. Vincent, A. Sadeghi, G. Schrijen, H. Schröder, and C. Wachsmann, "Recyclable PUFs: Logically reconfigurable PUFs," Workshop on Cryptographic Hardware and Embedded Systems (CHES 2011), LNCS 6917, pp.374–389, 2011.
[18] Z. Zhang, Z.Y. Yu, X. Cheng, and X.Y. Zeng, "A low power 1.0 GHz VCO in 65 nm-CMOS LP-process," 2011 IEEE 9th International Conference on ASIC (ASICON), pp.1006–1009, 2011.
[19] X.X. Zhang, Y. Li, B.Y. Xiong, J. Han, Y.J. Zhang, F.Y. Dong, Z. Zhang, Z.Y. Yu, J. Han, X. Chen, and X.Y. Zeng, "Robust and low power register file in 65 nm technology," J. Semiconductors, vol.33, no.3, 035010-5, 2012.
[20] Y.J. Zhang, P.J. Wang, Y. Li, X.X. Zhang, Z.Y. Yu, and Y.B. Fan, "Model and physical implementation of multi-port PUF in 65 nm CMOS," Int. J. Electron., vol.100, no.1, pp.112–125, 2013.



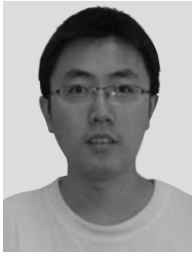
Pengjun Wang is doctor of engineering, professor, and Ph.D. candidate supervisor. He is a senior member of Chinese institute of electronics, senior member of Chinese Computer Federation, member of Electronic Circuits and Systems Professional Committee of Chinese institute of electronics, member of Multi-valued logic and fuzzy logic Professional Committee of Chinese Computer Federation. He is currently engaged in multi-valued logic circuits and low power integrated circuit design theory and research.



Yuejun Zhang received the B.S. degree in Circuits and Systems from Ningbo University in 2008. He is currently working toward the Ph.D. degree in Communication and Information System in the Institute of Circuits and Systems, Ningbo University, Ningbo, China. His research interests include register file and information security chip design, and their VLSI implementations.

Jun Han received the B.S. degree from Zhejiang University, Zhejing, China, in 2009 and the M.S. in integrated circuits engineering from Fudan University, Shanghai China in 2011. He is now a student in the State Key Laboratory of Application-Specific IC (AS IC) and System. His research interests include mixed signal circuits design and digital VLSI design.

Zhiyi Yu received the B.S. and M.S. degrees in electrical engineering from Fudan University, Shanghai, China, in 2000 and 2003, respectively, and the Ph.D degree in electrical and computer engineering from the University of California, Davis, in 2007. Dr. Yu is a Hardware Engineer with IntellaSys Corporation, headquartered in Cupertino, CA. And he is an Associate Professor in the State Key Laboratory of ASIC & System in Fudan University. His research interests include high-performance and energy- efficient digital VLSI design, architectures, and processor interconnects, with an emphasis on many-core processors. He was a key designer of the 36-core Asynchronous Array of simple Processors (AsAP) chip, and one of the designers of the 150+ core second generation computational array chip.



Yibo Fan received the B.E. degree in electronics and engineering from Zhejiang University, China in 2003, M.S. degree in Micro electronics from Fudan University, China in 2006, and Ph.D. degree in engineering from Waseda University, Japan in 2009. From 2009 to 2010, he worked as an Assistant Professor in Shanghai Jiaotong University. And currently, he is the Assistant Professor in Department of Microelectronics of Fudan University. His research interesting includes information security, video coding and associated VLSI architecture.

Zhang Zhang received the B.S. degree in electronic science and technology from Hefei University of Technology, Hefei, China, in 2004, and the Ph.D. degree in microelectronics from Fudan University, Shanghai, China, in 2010. He is currently an Associate Professor of electronic science and technology with the Hefei University of Technology, and his work focuses on mixed signal circuits such as ADC and PLL and ultra-low power biomedical circuits.