International Journal of Electronics
Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/tetn20

Model and physical implementation of multi-port PUF in 65nm CMOS

Yuejun Zhang [a], Pengjun Wang [a], Yi Li [b], Xingxing Zhang [b], Zhiyi Yu [b] & Yibo Fan [b]

[a] Institute of Circuits and Systems, Ningbo University, Ningbo, China

[b] State Key Laboratory of ASIC & System, Fudan University, Shanghai, China

Version of record first published: 25 Jul 2012

To cite this article: Yuejun Zhang, Pengjun Wang, Yi Li, Xingxing Zhang, Zhiyi Yu & Yibo Fan (2012): Model and physical implementation of multi-port PUF in 65nm CMOS, International Journal of Electronics, DOI:10.1080/00207217.2012.687189

To link to this article: http://dx.doi.org/10.1080/00207217.2012.687189

International Journal of Electronics
2012, 1–14, iFirst

Model and physical implementation of multi-port PUF in 65 nm CMOS

Yuejun Zhang[a], Pengjun Wang[a]*, Yi Li[b], Xingxing Zhang[b], Zhiyi Yu[b] and Yibo Fan[b]

[a]*Institute of Circuits and Systems, Ningbo University, Ningbo, China;* [b]*State Key Laboratory of ASIC & System, Fudan University, Shanghai, China*

(*Received 24 September 2011; final version received 28 March 2012*)

In modern cryptographic systems, multi-port physically unclonable function (MPUF) is an efficient mechanism for many security applications, which extracts secret information inherently embedded in the unclonable physical variations and generates multiple secret keys. In this article, we propose an explicit analytic MPUF model, which is useful in predicting the effect of parameter changes on the state as well as in optimizing the design of PUF. Then, a novel MPUF based on register file is designed and fabricated in TSMC low-power 65 nm CMOS technology. There are four ports in the MPUF, and each port produces a 256-bit key. The chip has an area of 0.045 mm^2, and has a peak clock frequency of 1.25 GHz at 1.2 V. The average power consumption is 13.8 mW at 27°C. Being multi-ports technology and high operation frequency, the throughput of MPUF improves about 50 times compared to the other works. We carry out a robust test by varying the operational conditions such as supply voltage, temperature and noise. The measured results show that the reliability achieves 98.1% at worse case and has a certain improvement compared with the proposed works. The reliability operates at an acceptable range in integrated circuit identification (ICID).

Keywords: MPUF; multi-port; process variation; register file; 65 nm

1. Introduction

Modern cryptographic protocols are based on the premise that only authorised participants can obtain secret keys and access to information system. System security is based on the protection of the secret keys. However, various kinds of tampering methods have been devised to extract secret keys, such as power analysis (Mangard, Oswald, and Popp 2007), electromagnetic attacks (Pankaj 2009) and glitch attacks (Alam, Ghosh, Mohan, and Mukhopadhyay 2009). To prevent these attacks, researchers have started investigating protection mechanisms in multiple levels securing processors (Ambrose, Parameswaran, and gnjatovic 2008; Mathew, Sheikh, Kounavis, Gueron, and Agarwal 2011), software protection (Preda and Vizireanu 2010, 2011) and IC authentication (Majzoobi and Koushanfar 2011). Understanding them requires know how from different disciplines such as cryptology, statistics, measurement technology and electronics. They have attracted the attention of researchers from all these fields. As a result, a large number of relevant research articles have been published over the previous years from model

*Corresponding author. Email: wangpengjun@nbu.edu.cn

ISSN 0020–7217 print/ISSN 1362–3060 online

http://dx.doi.org/10.1080/00207217.2012.687189
http://www.tandfonline.com

estimation method (Vizireanu 2011, 2012; Vizireanu and Halunga 2011) or analytical technique (Vizireanu and Halunga 2012) to field-programmable gate arrays (FPGAs) (Pable and Mohd 2012) and application-specific integrated circuits (ASICs) (Geng and Li 2012) implementations. Physical unclonable function (PUF) is one of the efficient mechanisms for many security applications (Pappu, Recht, Taylor, and Gershenfeld 2002; Skoric, Maubach, Kevenaar, and Tuyls 2006), which exploit secret information embedded in the intrinsic random process variation in the manufacturing of ICs to produce secret keys. We all know that the process variation is beyond manufacturers' control. For measurements, the internal signals are quantised to the digital keys (Udrea and Vizireanu 2008; Vizireanu 2009; Preda and Vizireanu 2011a,b). After this the secret keys of PUF is unique and unclonable.

In 2002, the journal *Science* initially reported that PUF can be used as an underlying security mechanism (Pappu et al. 2002). Subsequently, a group of researchers observed that the manufacturing process variability in modern silicon technology can be utilised for building a PUF, and a number of methods for realising PUF have been proposed. Lim proposed the arbiter-based PUF architecture based on the variations in CMOS logic delays (Lim et al. 2005). Later it was observed that the linear arbiter-based PUF is vulnerable to modelling attacks, and the nonlinear feed-forward arbiters and hashing were proposed to protect against this attack (Gassend, Clarke, Dijk, and Devadas 2002). To implement PUF on FPGA, a ring oscillator PUF was also proposed in Suh and Devadas (2007). However, the major drawback of the RO PUF is that they have only a quadratic number of challenges with respect to the number of ring oscillators. Furthermore, the ring oscillators consume significant dynamic power due to frequent transitions during oscillations (Skoric et al. 2006). Holcomb presented a system of fingerprint extraction and random numbers in SRAM that harvests static identity and randomness from existing volatile CMOS memory without requiring any dedicated circuitry (Holcomb, Burleson, and Fu 2009). Ying Su designed a 128-bit, 1.6 pJ/bit, 96% stable chip ID generation circuit utilising process variations in a 0.13 μm CMOS process (Ying, Holleman, and Otis 2008). Even though a number of methods for realising PUF have been proposed, they have been limited by either the number of challenge-response pairs, or the power consumption, or the noise and other vulnerabilities to the system.

In this work, we propose and implement a novel scheme for MPUF. Firstly, we propose an explicit analytic expression of MPUF model, and the model is useful in predicting the effect of parameter changes on the state as well as in optimising the design of PUF. Then, a novel MPUF scheme based on register file is designed and fabricated in TSMC low-power 65 nm CMOS technology. There are four ports in the MPUF, and each port produces a 256-bit key. The chip has an area of 0.045 mm^2, and has a peak clock frequency of 1.25 GHz at 1.2 V. The average power consumption is 13.8 mW at 27°C. In addition, we ensure that the responses are robust to fluctuations in operational conditions such as supply voltage, temperature and static noise margin (SNM). It is concluded that the proposed MPUF can reach to 98.1% stable, and is highly reliable since the ID collision probability is vanishingly small.

This article is organised as follows: the ID cell design and the model of MPUF are discussed in Section 2. The circuit and layout of MPUF based on register file are proposed in Section 3. The chip fabrication and measurement results are introduced in Section 4. Robustness to environmental factors is discussed in Section 5. Finally, the conclusion is given in Section 6.

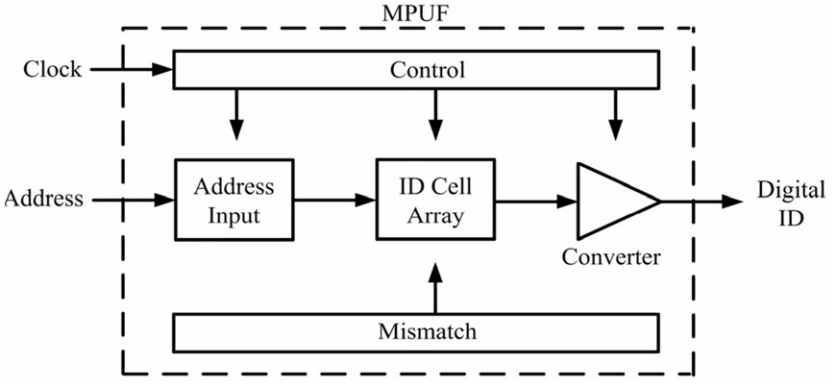

Figure 1. Block diagram of identification digital generator.

2. ID cell design and the model of MPUF

Random process variation in the manufacture, such as ion implantation, oxide growth and lithography, causes random mismatch even in transistors with identical layout. The mismatch will cause small deviations from the device electrical parameters, resulting in unique identification digital (ID) on each chip. We extract the unique ID as the secret key. The block diagram of identification digital generator is shown in Figure 1. Addresses for this experiment are provided externally, and the random analogy voltage sequence is converted to a digital identification sequence with a converter.

2.1. *The mismatch of MOSFET*

MOS transistor mismatch can be defined as the variation in drain current for identically designed devices under similar bias conditions (Yuan, Shimizu, Mahalingam, Brown, and Habib 2011). The parameter variance is dependent on device area WL and separation distance D_x. A mismatch model is described as (Noije, Liu, and Navarro 1995):

$$\sigma^2(\Delta P) = \frac{A_P^2}{WL} + S_P^2 D_x^2 \tag{1}$$

where A_p and S_p are process-dependent constants relating the parameter variance to the device area and separation distance, respectively. The mismatch of metal oxide semiconductor field effect transistor (MOSFET) is shown in Figure 2.

2.2. *ID cell design*

In this work, we design MPUF based on a register file. The structure of the register file cell is shown in Figure 3, consisting of cross-coupled inverters, isolated inverters and access transistors. During power up time, the cross-coupled inverters cause unique random ID because of transistor mismatch. Each of the inverters drives one of the two state nodes, labelled P and $\bar{P}$. When the circuit is un-powered, both state nodes are low ($P\bar{P} = 00$). Once power is applied, this unstable state is immediately transformed to one of the two stable states, either '0' ($P\bar{P} = 01$) or '1' ($P\bar{P} = 10$). The choice between the two stable states

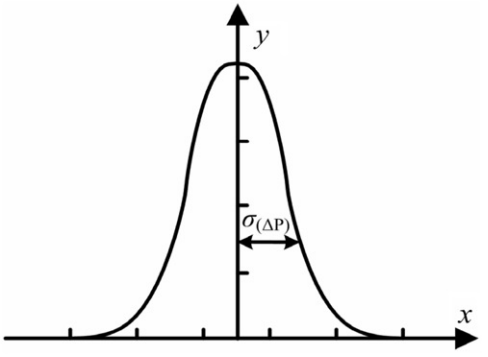

Figure 2. The mismatch of MOSFET.

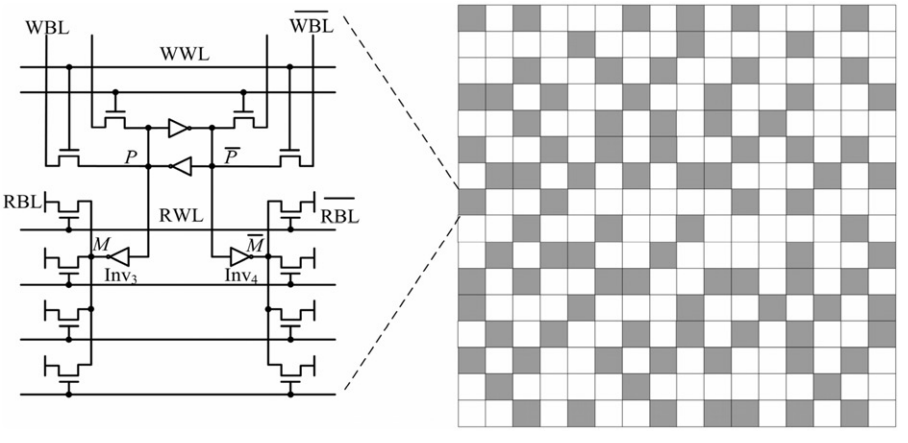

Figure 3. The MPUF cell.

depends mainly on mismatch between local devices. The impacts of common mode process variations such as lithography, and common mode noise such as substrate temperature and supply voltage fluctuations, are minimised.

2.3. *Analytic expression of MPUF model*

As the transistor mismatch is usually small, a small-signal model is used in this article. Figure 4 shows that the small-signal model for the cross-coupled inverters (Xu, Kim, and Chung 2010), where g_m is the equivalent transconductance ($M_{\mathrm{Pl}}/M_{\mathrm{nl}}$ and $M_{\mathrm{p2}}/M_{\mathrm{n2}}$, respectively); g_d is the equivalent conductance; C_m is the coupling capacitance between the gate and drain of the MOSFET and C_n is the total node capacitance.

The cell storage nodes Q and $\bar{Q}$ can be derived by Kirchhoff current equations (Xu et al. 2011), respectively.

$$g_m \cdot v_2 + g_d \cdot v_1 + C_n \frac{\mathrm{d}v_1}{\mathrm{d}t} + C_m \frac{\mathrm{d}(v_1 - v_2)}{\mathrm{d}t} = 0 \tag{2}$$

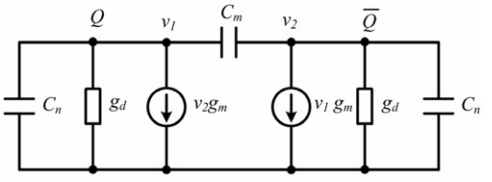

Figure 4. Small-signal model for cross-coupled inverters.

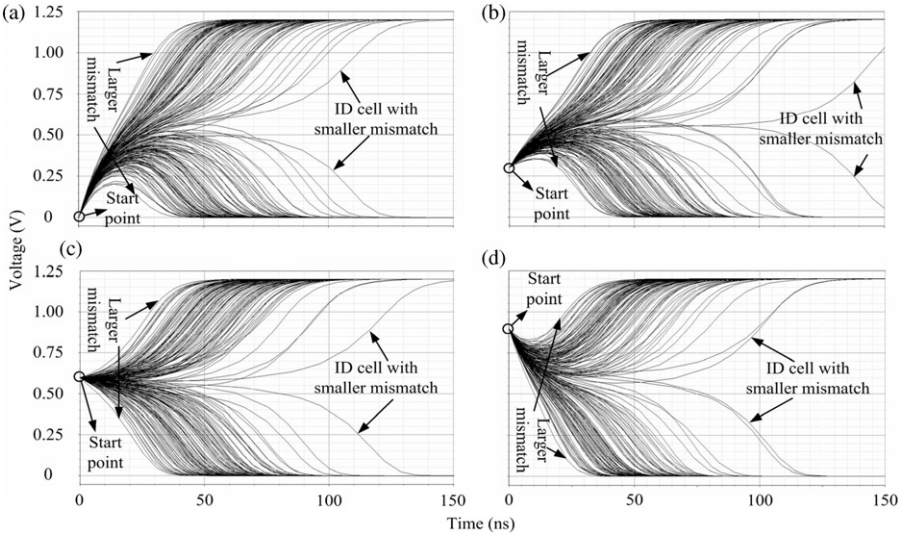

Figure 5. Monte Carlo simulation of ID cells.

$$g_m \cdot v_1 + g_d \cdot v_2 + C_n \frac{\mathrm{d}v_2}{\mathrm{d}t} + C_m \frac{\mathrm{d}(v_2 - v_1)}{\mathrm{d}t} = 0 \tag{3}$$

Solving Equations (2) and (3), we obtain

$$v_d(t) = v_d(t_0)\ \exp\left(\frac{t - t_0}{\tau_r}\right) \tag{4}$$

Here, $v_d(t)$ is the instantaneous voltage of the output node; $v_d(t_0)$ is the initial voltage at the start point and τ_r is a constant. From Equation (4), it is concluded that unstable states will exponentially change to the stable states during power up.

Using the parameters of TSMC 65 nm CMOS device, the MPUF is designed and simulated to verify this model. The W/L ratio of PMOS transistor equals to 150 nm/60 nm, and the W/L ratio of NMOS transistor equals to 300 nm/60 nm. Unlike previous implementations, no offset-nulled comparator or low offset amplifier is needed to detect very small mismatch voltage variations, allowing a reduction in the circuit complexity and power dissipation. Our approach relies on the positive feedback inherent in the cross-coupled inverters. Under the conditions at 1.2 V and 27°C, Figure 5 shows a Monte Carlo simulation of the MPUF cells array, yielding a random logic value with an even

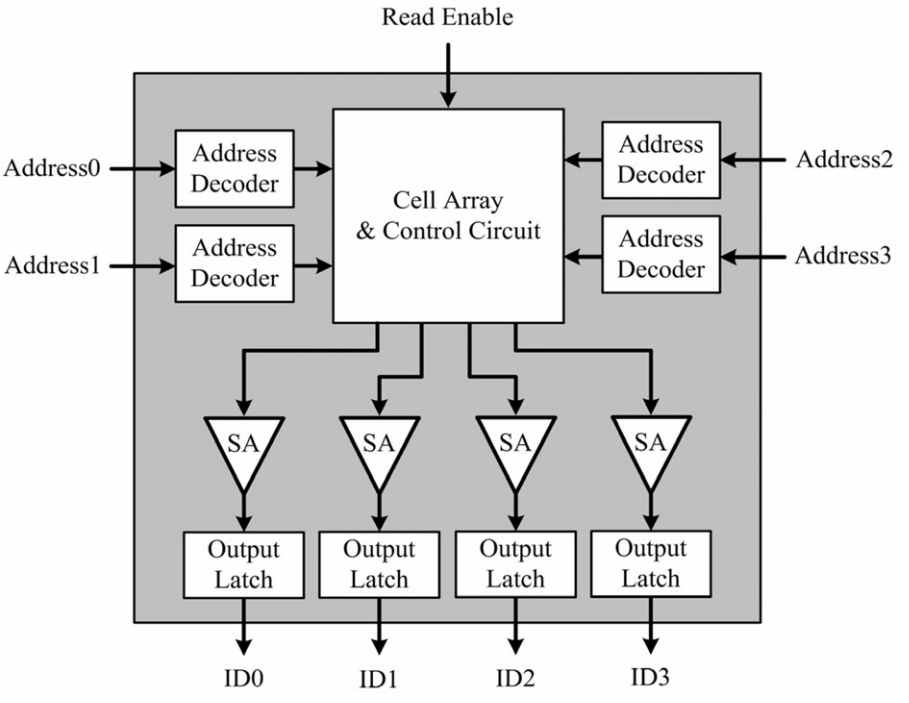

Figure 6. MPUF block diagram.

distribution of logic '0' and '1'. The start point are set at 0, 0.3 V, 0.6 V and 0.9 V, respectively. Once power is applied, this unstable state will exponentially change to one of the two stable states, either '0' ($P\bar{P}=01$) or '1' ($P\bar{P}=10$). During larger mismatch, the transition time is about 50 ns, while during smaller mismatch, the transition time is about 100 ns. The curve of the transition is better agreement with the MPUF model.

3. Circuit design and layout techniques

The MPUF has a size of four banks of 256 bits that can be accessed simultaneously by four read ports. A block diagram for the MPUF, shown in Figure 6, illustrates that the MPUF contains five distinct types of functional blocks. These are the cell array, the control circuit, the read address decoders, the sense amplifiers and the output latches. The cell array is responsible for generating unique random ID. It is arranged in four banks 16 rows by 16 columns of cells. Read address decoder is responsible for decoding a 5-bit address to determine which of the 32 rows is selected for each read operation. The output latches are responsible for storing the ID from the sense amplifiers.

3.1. *Circuit design of MPUF*

The read address decoder is composed of two stages, as shown in Figure 7. In the first stage, wired-OR techniques are used to separately decode the lower one bits, middle two bits and the upper two bits of the address. The 1-2 decoder drive has two wired-OR lines,

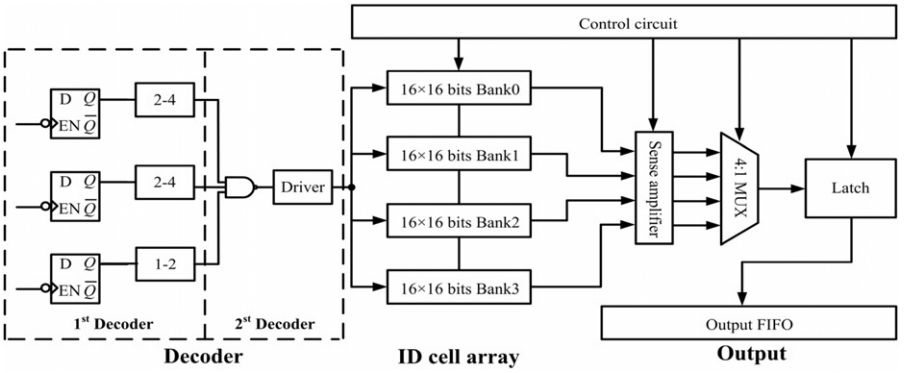

Figure 7. Block diagram about one read path of MPUF.

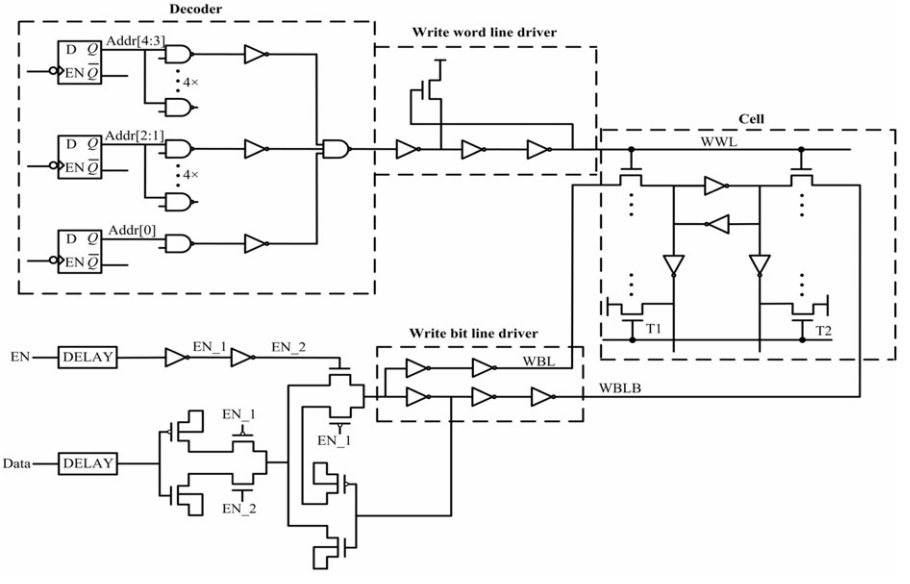

Figure 8. The circuit about one read path of MPUF.

and only one of the two wired-OR lines produces a high output voltage. The 2-4 decoder drive has four wired-OR lines, and only one of the four wired-OR lines produces a high output voltage. In the second stage, since only one of lines in each set is low for any given address, only one NAND gate will receive three high signals as input. This NAND gate produces a high output signal, indicating that the corresponding row is selected, while all the other NAND gates produce low output signals. Each read word line driver consists of a single large device capable of driving a read port in every memory cell for a single row. 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 ID.

Figure 8 is the circuit of one read path. Before reading, signals are latched to avoid the unpredictable change by input module. The bit lines RWL/RWLB will be pre-charged

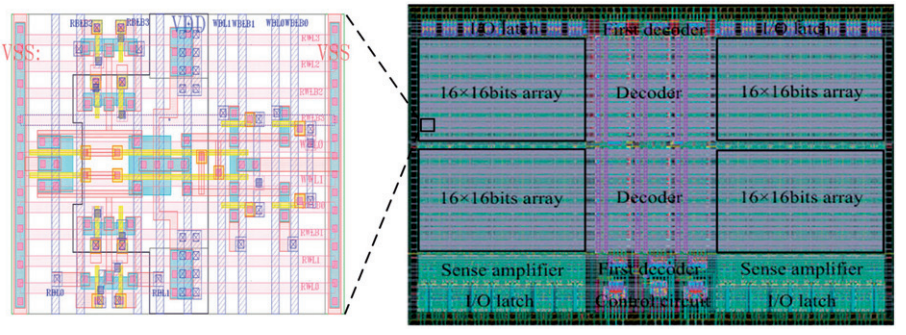

Figure 9. Layout of ID cell and four banks 256-bit MPUF.

to VDD. To achieve a short read path, the I/O block is placed between the top and bottom halves of each sub array. The decoder is used to generate and buffer the word line (WL) including read word line (RWL) and read word line bar (RWLB). When read operation is performed, the RWL/RWLB selects the corresponding cells, and the selected cells drive the read local bit line (RLBL). If the cell's word line is chosen, one bit line will be discharged, and then a voltage difference between two bit lines will be generated. Finally, the output value is '1' or '0'.

3.2. *The layout of PUF circuit*

Generally, the PUF circuit requires a symmetric layout to produce 'ideal' performance. The layout of the proposed ID cell and four banks 256-bit ID is shown in Figure 9. The cell array is divided into two parts (right and left parts). Each part consists of 4 data output ports, which have 16 bits. One part of cell area has 16 rows by 16 columns of cells. Decoder circuits and control units, located in the center of layout, are divided into two segments (up and down segments). The cell area of MPUF is about 44%. The bit density of MPUF is 1.84 Mb/mm^2.

4. Chip fabrication and measurement results

We fabricated multi-port PUF test chips using TSMC 65 nm low-power CMOS technology. Figure 10 shows the die photograph of the test chip for the multi-port PUF, along with the test circuit and the phase locked loop (PLL). The physical layout size of the test chip is 0.045 mm^2.

The feature of fabricated multi-port PUF is summarised in Table 1. The 0.045 mm^2 fully customised design contains 30,287 transistors. There are 34 I/O pads along the die periphery, of which 20 pads are signal pads and the others are power pads. The frequency and power dissipation characteristics are shown in Figure 11(a) and (b) respectively, and simulation results show that it can run at 1.25 GHz and dissipate 13.8 mW at 1.2 V and 27°C.

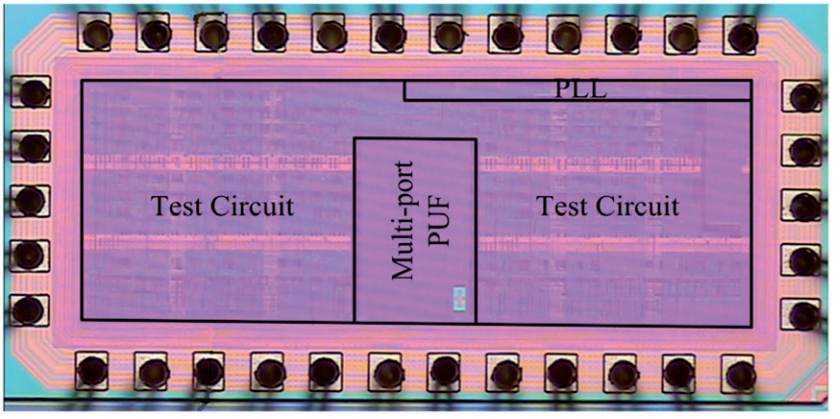

Figure 10. Die photograph of a test chip.

Table 1. Multi-port PUF features.

Technology	TSMC 65 nm CMOS
Area	180 μm × 250 μm
Supply voltage	1.2 V
Pad count	34 pads
Transistor count	30,287
Topology	4 ports
Power consumption	13.8 mW
Frequency	1.25 GHz
Memory cell arrays	32 × 32

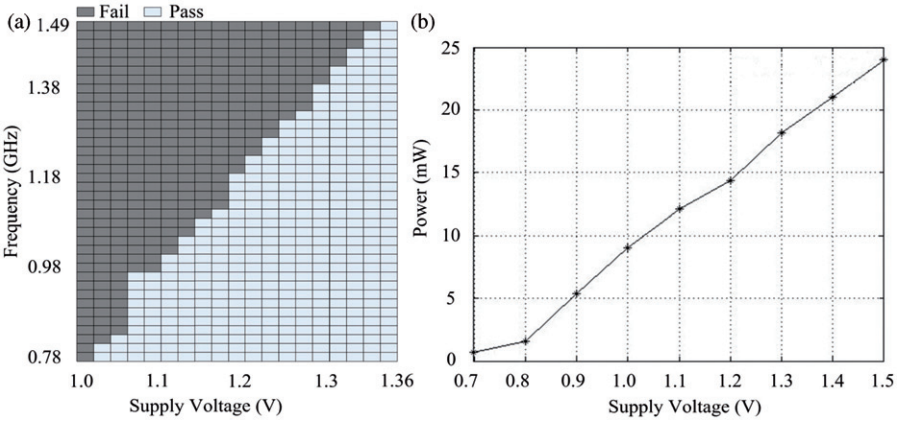

Figure 11. (a) Frequency characteristics of MPUF; (b) power characteristics of MPUF.

5. Robustness to environmental factors

The viability of the MPUF is related to the environments where the circuit is used. This section explores the potential influence of supply voltage and temperature on the output of MPUF.

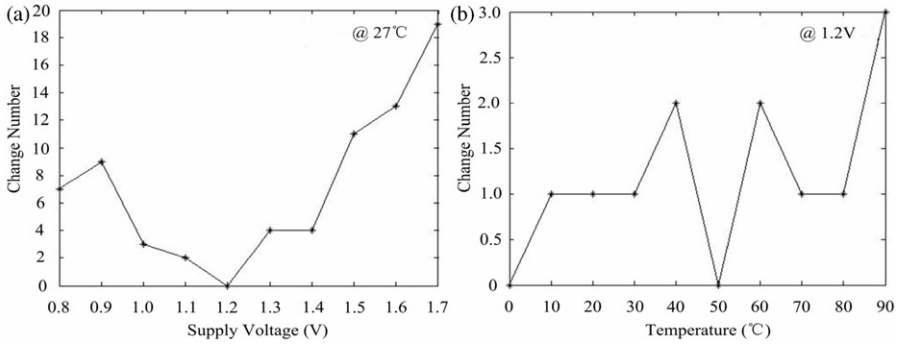

Figure 12. (a) Change number of MPUF versus supply voltage; (b) change number of MPUF versus temperature.

The reliability of the challenge-response behaviours of PUF against supply voltage variations is an important measure of quality for PUF that may be applied in a voltage-varying environment. To evaluate the reliability of the multi-port PUF against VDD variations, we measured 1024-bit on a test chip under different temperatures at 27°C. The result is shown in Figure 12(a). From the curves obtained from 0.8 V to 1.7 V, it can be seen that the maximum of 1.85% can be caused by the change in supply voltage.

The reliability of the challenge-response behaviours of PUF against temperature variations is an important measure of quality for PUF that may be applied in a temperature-varying environment. To evaluate the reliability of the MPUF against temperature variations, we measured 256-bit on a test chip under different temperatures at 1.2 V. The result is shown in Figure 12(b). From the curves obtained from 0 to 90°C, it can be seen that the maximum 0.3% can be caused by the change in environmental temperature.

MOS transistor threshold voltage of the main pipe is channel doping concentration and gate oxide thickness is determined. The transistor mismatch will cause small deviations from the device electrical parameters, resulting in changing of SNM. To determine the influence due to transistor mismatch, we performed Monte Carlo simulations for read mode SNM at a supply voltage of 1.2 V and a temperature of 20°C. As can be seen from Figure 13(a), the values of SNM follow a standard normalised distribution. The SNM value is about 385 mV in the worst case; the SNM value is about 525 mV in the best case, and the SNM value is about 450 mV at the typical case.

The ID codes in this work are assigned randomly. Thus, there will be a finite possibility of ID code collision within a given number of chips, even if all bits in the ID code are stable. Modelling the ID collision probability is important for investigating the robustness of this technique in a production environment. Consider x as the number of bits in an ID code, resulting in a total number of available ID codes of 2^x. The probability of ID collision across chips can be represented as (Ying et al. 2008):

$$P_{\text{collision}} = 1 - \prod_{n=1}^{Y} \left(1 - \frac{n-1}{2^x}\right) \tag{5}$$

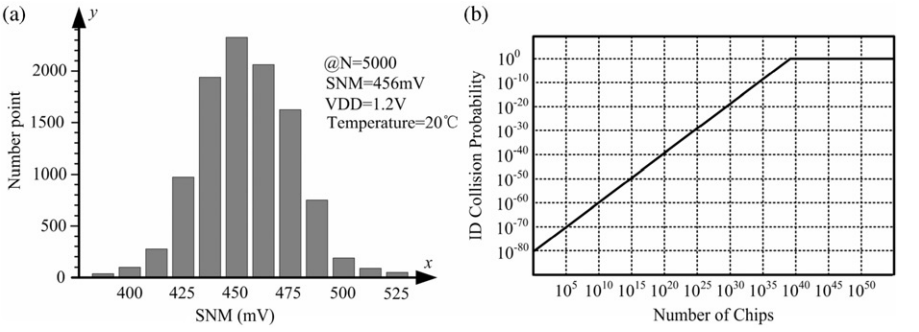

Figure 13. (a) Monte Carlo simulation results of SNM; (b) ID collision probability.

Table 2. Characteristics and comparison to other works.

Paper	Process	Port	Power (W)	Frequency (Hz)	Supply (V)	Reliability
Lofstrom, Daasch, and Taylor (2000)	350 nm	1	250 u	25 M	2.5	95%
Lim et al. (2005)	180 nm	1	137 u	100 M	1.8	95%
Ying, Holleman and Otis (2008)	130 nm	1	1.6 u	1 M	1	96%
Majzoobi, Koushanfar and Potkonjak (2009)	Xilinx Virtex 5	1	–	15 M	1	90%
Suzuki and Shimizu (2010)	Xilinx Spartan-3A	1	–	50 M	1.2	93.4%
Majzoobi and Koushanfar (2011)	Xilinx Virtex 5	1	–	20 M	0.9/1	90%
Rührmair et al. (2011)	32 nm	1	72 m	100	1.0	–
In this work	65 nm	4	13.8 m	1.25 G	1.2	98.1%

This probability model assumes that the number of chips (Y) is smaller than the total number of available ID codes 2^x – a reasonable assumption with a 256-bit ID length. The ID collision probability for a 256-bit ID code versus different number of chips is shown in Figure 13(b). This demonstrates that the use of randomly assigned ID codes is highly reliable since the ID collision probability is vanishingly small.

Table 2 compares the key characteristics of the PUF with other published implantations. 4-ports MPUF designed in TSMC 65 nm low-power CMOS achieves a measured maximum frequency of 1.25 GHz, which translates to a maximum throughput of 1.25×4 bit/s. Compared to the other works, the throughput of MPUF improves more than 50 × times. During the peak throughput of MPUF, the power consumption measured is 13.8 mW, which shows that the MPUF is low power circuit. MPUF has been measured in a wide range of power supplies, clock frequencies and temperatures. In the worst case, the reliability achieves 98.1% and shows a certain improvement compared with the proposed works. Also, the reliability of MPUF operates at an acceptable range in integrated circuit identification (ICID) (Lofstrom et al. 2000).

6. Conclusions

In this article, we have presented a novel scheme of MPUF for using process variation to generate unique digital keys and identify circuits. The MPUF is designed and implemented in TSMC 65 nm low-power CMOS technology. This MPUF offers three advantages. First, being multi-ports technology, it can improve $4\times$ throughput by increasing the access ports. Compared to the other studies, the throughput of MPUF has improved more than $50\times$. Secondly, the MPUF has low power characteristic. The measured result is 13.8 mW at the worst case. Finally, the MPUF has better performance in cell stability. The measured result shows that the reliability achieves 98.1% and has a certain improvement compared with the proposed studies. Also, the reliability of MPUF operates at an acceptable range in integrated circuit identification (ICID). We believe that MPUF can be widely used in integrated circuit applications, ranging from low power radio frequency identification devices (RFID) tags and Smart Cards to embedded caches on high-end devices and next generation of wireless sensor networks. These aspects will be explored in our future work.

Acknowledgements

This project is supported by the National Natural Science Foundation of China (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

Alam, M., Ghosh, S., Mohan, M.J., and Mukhopadhyay, D. (2009), 'Effect of Glitches against Masked AES S-box Implementation and Countermeasure', *Information Security, IET*, 3, 34–44.

Ambrose, J.A., Parameswaran, S., and Ignjatovic, A. (2008), 'MUTE-AES: A Multiprocessor Architecture to Prevent Power Analysis based Side Channel Attack of the AES Algorithm', In *ICCAD 2008*, pp. 678–684.

Gassend, B., Clarke, D., Dijk, M., and Devadas, S. (2002), 'Silicon Physical Random Functions', In *The 9th ACM Conference on Computer and Communications Security*, pp. 148–160.

Geng, M.C., and Li, J.C. (2012), 'A Secure Test Wrapper Design Against Internal and Boundary Scan Attacks for Embedded Cores', *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 20, 126–134.

Holcomb, D.E., Burleson, W.P., and Fu, K. (2009), 'Power-Up SRAM State as an Identifying Fingerprint and Source of True Random Numbers', *IEEE Transactions on Computers*, 58, 1198–1210.

Lim, D., Lee, J.W., Gassend, B., Suh, G.E., Dijk, M., and Devadas, S. (2005), 'Extracting Secret Keys from Integrated Circuits', *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 13, 1200–1205.

Lofstrom, K., Daasch, W.R., and Taylor, D. (2000), 'IC Identification Circuit Using Device Mismatch', in *IEEE International Solid-State Circuits Conference (ISSCC)*, pp. 372–373.

Majzoobi, M., and Koushanfar, F. (2011), 'Time-Bounded Authentication of FPGAs', *IEEE Transactions on Information Forensics and Security*, 6, 1123–1135.

Majzoobi, M., Koushanfar, F., and Potkonjak, M. (2009), 'Techniques for Design and Implementation of Secure Reconfigurable PUFS', *ACM Transactions on Reconfigurable Technology and Systems*, 2, 1–33.

Mangard, S., Oswald, E., and Popp, T. (2007), *Power Analysis Attacks: Revealing the Secrets of Smart Cards*, Austria: Springer.

Mathew, S.K., Sheikh, F., Kounavis, M., Gueron, S., and Agarwal, A. (2011), '53 Gbps Native Composite-Field AES-Encrypt/Decrypt Accelerator for Content-Protection in 45 nm High-Performance Microprocessors', *IEEE Journal of Solid State Circuits*, 46, 767–776.

Noije, W.A.M., Liu, W.T., and Navarro, S.J. (1995), 'Precise Final State Determination of Mismatched CMOS Latches', *IEEE Journal of Solid-State Circuits*, 30, 607–611.

Pable, S.D., and Mohd, H. (2012), 'A Novel Robust FPGA Routing Switch Box Design for Ultra Low Power Applications', *International Journal of Electronics*, 99, 15–27.

Pankaj, R. (2009), 'Electromagnetic Attacks and Countermeasures', in *Cryptographic Engineering*, 10.1007/978-0-387-71817-0_15, 407–430.

Pappu, R., Recht, B., Taylor, J., and Gershenfeld, N. (2002), 'Physical One-Way Functions', *Science*, 297, 2026–2030.

Preda, R.O., and Vizireanu, D.N. (2010), 'A Robust Digital Watermarking Scheme for Video Copyright Protection in the Wavelet Domain', *Measurement*, 43, 1720–1726.

Preda, R.O., and Vizireanu, D.N. (2011a), 'Quantization Based Video Watermarking in the Wavelet Domain with Spatial and Temporal Redundancy', *International Journal of Electronics*, 98, 393–405.

Preda, R.O., and Vizireanu, D.N. (2011b), 'Robust Wavelet-based Video Watermarking Scheme for Copyright Protection Using the Human Visual System', *Journal of Electronic Imaging*, 20, 013022-1–013022-7.

Rührmair, U., Jaeger, C., Bator, M., Stutzmann, M., Lugli, P., and Csaba, G. (2011), 'Applications of High-Capacity Crossbar Memories in Cryptography', *IEEE Transactions on Nanotechnology*, 10, 489–498.

Skoric, B., Maubach, S., Kevenaar, T., and Tuyls, P. (2006), 'Information-theoretic Analysis of Capacitive Physical Unclonable Functions', *Journal of Applied Physics*, 100, 024902-1–024902-11.

Suh, G., and Devadas, S. (2007), 'Physical Unclonable Functions for Device Authentication and Secret Key Generation', in *Design Automation Conference*, pp. 9–14.

Suzuki, D., and Shimizu, K. (2010), 'The Glitch PUF: A New Delay-PUF Architecture Exploiting Glitch Shapes', in *Workshop on Cryptographic Hardware and Embedded Systems (CHES)*, pp. 366–382.

Udrea, R.M., and Vizireanu, D.N. (2008), 'Quantized Multiple Sinusoids Signal Estimation Algorithm', *Journal of Instrumentation*, 3, 1–7.

Vizireanu, D.N. (2009), 'Quantized Sine Signals Estimation Algorithm for Portable DSP Based Instrumentation', *International Journal of Electronics*, 96, 1175–1181.

Vizireanu, D.N. (2011), 'A Simple and Precise Real-time four Point Single Sinusoid Signals Instantaneous Frequency Estimation Method for Portable DSP based Instrumentation', *Measurement*, 44, 500–502.

Vizireanu, D.N. (2012), 'A Fast, Simple and Accurate Time-varying Frequency Estimation Method for Single-phase Electric power Systems', *Measurement,* 45, 1331–1333.

Vizireanu, D.N., and Halunga, S.V. (2011), 'Single Sine Wave Parameters Estimation Method Based on Four Equally Spaced Samples', *International Journal of Electronics*, 98, 941–948.

Vizireanu, D.N., and Halunga, S.V. (2012), 'Analytical Formula for Three Points Sinusoidal Signals Amplitude Estimation Errors', *International Journal of Electronics*, 99, 149–151.

Xu, H., Kim, H.J., and Chung, W.S. (2010), 'Experimental Identification Method for Small-Signal Analysis of Smart Power ICs', *IEEE Transactions on Industrial Electronics*, 57, 2142–2150.

Xu, J.Z., Luo, L.F., Li, Y., Rehtanz, C., Zhang, Z.W., and Liu, F.S. (2011), 'Operating Characteristics of a New Filter-commutated Converter Based on Equivalent Graetz Bridge Circuit Model', *Power Electronics, IET*, 4, 959–967.

Ying, S., Holleman, J., and Otis, B.P. (2008), 'A Digital 1.6 pJ/bit Chip Identification Circuit Using Process Variations', *IEEE Journal of Solid-State Circuits*, 43, 69–77.

Yuan, X.B., Shimizu, T., Mahalingam, U., Brown, J.S., and Habib, K.Z. (2011), 'Transistor Mismatch Properties in Deep-Submicrometer CMOS Technologies', *IEEE Transactions on Electron Devices*, 58, 335–342.