Wireless Pers Commun (2011) 59:85–94
DOI 10.1007/s11277-010-0191-5

Ultra-Low Power Truly Random Number Generator for RFID Tag

Wei Chen · Wenyi Che · Na Yan · Xi Tan · Hao Min

Published online: 1 December 2010

Abstract This paper proposes low power, low voltage Truly Random Number Generators (TRNG) for Electrical Product Code (EPC Generation 2 Radio Frequency Identification (RFID) tag. Design considerations and trade-offs among randomicity, chip area and power consumption are analyzed according to the special requirements of Gen2 RFID tag. The proposed TRNG circuits consist of an analog random seed generator which uses the oscillator sampling mechanism, and Linear Feedback Shift Registers for post digital processing. These TRNG are implemented in SMIC 0.18 μm CMOS process. And their randomicity performances are verified by the FIPS 140-2 standard for security. One of the TRNG circuits outputs a random bit series at a speed of 40 kHz. Its power consumption is 1.04 μW and chip area is 0.05 mm^2. The other one has a bit rate at 48 kHz. It has a power consumption of 2.6 μW and chip area of 0.018 mm^2. The features of low power and small chip area in these TRNG circuits provide a good choice to solve the security and privacy problems in RFID systems.

Keywords Random number generator · Low power · RFID

1 Introduction

Radio Frequency Identification network has been widely used for various applications in recent years. However, the security and privacy concerns of RFID networks have slowed RFID adoption and its further development. In order to enhance the security and privacy performance of RFID systems, especially to defend the attacks upon communications between tags and readers, cryptographic circuits and algorithms have been employed in RFID tags. These algorithms need good random numbers as seeds to encode and decode the information.

W. Chen · W. Che · N. Yan (✉) · X. Tan · H. Min
State Key Laboratory of ASIC and System, Auto-ID Laboratory,
Fudan University, 201203 Shanghai, China
e-mail: yanna@fudan.edu.cn

In addition, a 16-bit random number is needed for anti-collision purpose according to the EPC Generation 2 protocol for UHF RFID tags [1].

For these purposes, pseudo random number generator (PRNG) including pure digital circuits used to be widely used in tag design. But they are vulnerable to attacks because of their fixed structure. As a result, the PRNG needs truly random seeds that are realized by physical random sources in TRNG circuit to insure randomicity. Many TRNG designs have been reported in recent years. But considering the requirements in Gen2 tags, some of them have low randomicity performances [2], some consume large power [3], some have large chip area or slow bit rate [4]. So far, no thorough analysis on the requirements of Gen2 tags of TRNG has been done, and no TRNG circuit is designed for it.

The common methods used in TRNG can be classified into three main categories. (1) Direct amplification of noise using a wideband high gain amplifier, (2) Discrete time chaos systems using analog signal processing technique, (3) Sampling of a high frequency oscillator with a jittered low frequency oscillator [2], [5]. The first two methods are not suitable for Gen2 RFID system because of their features of large power consumption and complicated circuitry, while the oscillator-based method is more adaptable with the RFID system. By adapting the oscillator-based random number generation technology to the requirements and limitations of Gen2 tags, two TRNG circuits are proposed for security and anti-collision purpose in Gen2 RFID system. The proposed TRNG circuits realized both the merits of low power consumption and small chip area. These two features also make them possible to be used in other security system that requires low power and low cost.

The system architecture of the TRNG is presented in Sect. 2. Based on the requirements of Gen2 tags, design considerations and tradeoffs among power consumption, chip area, and output speed are shown in Sect. 3. Section 4 gives the measurement results, analyses and comparisons with other works. And finally, a conclusion is drawn in Sect. 5.

2 Circuit Architecture

The mechanism of oscillator-based TRNG is shown in Fig. 1. It mainly contains two parts: an analog random seed generator and a cascade stage of post digital processor. The analog random seed generator consumes the largest power and area in the system. It includes two independent clocks: a fast free running clock (CLK_f) and a slow jittery clock (CLK_s). Since the system clock of the RFID system, which is 1.28/1.92/2.56 MHz [6], can be used as CLK_f, the focus of the design is located on the slow jittery clock. As the random source of the whole system, the duty cycle of CLK_s is designed to be uncertain. So, the rising and falling edge of this clock cannot be predicted. The value of the fast clock that is sampled by CLK_s is uncertain. As a result, the output bit cannot be predicted. Considering the utility in low power RFID system, CLK_s should be realized as simple as possible.

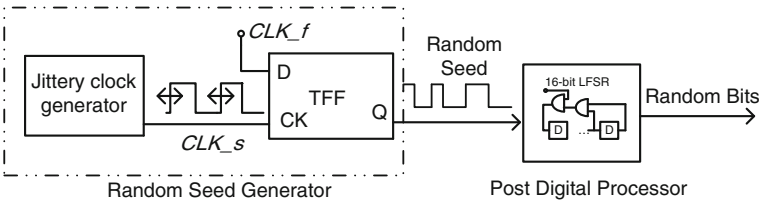


Fig. 1 System architecture of proposed TRNG

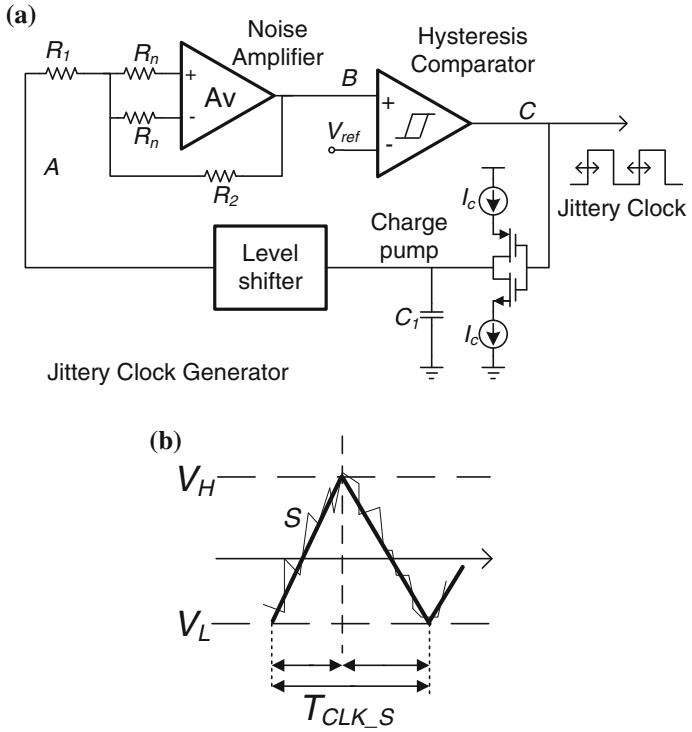


Fig. 2 **a** Circuit detail of Jittery Clock Generator. R_n is the noise resistor. R_1 and R_2 are feed back resistors. I_c is the charge and dis-charge current of the charge pump. **b** The noise-added triangular wave [3,7] at the output of the noise amplifier(*node B*). V_H and V_L are respectively up and low threshold of the hysteresis comparator. S is the average slope of the triangular wave and T_{CLK_S} is the period of the wave

In this TRNG, a T flip-flop (TFF) is used instead of a commonly used D flip-flop (DFF) to make the output more robust. This is because the duty cycle of CLK_f can also affect the output randomicity. The time of high level and low level of CLK_f cannot be precisely equal even if excellently designed, and this will affect the probabilities of '1' and '0' sampled by a DFF. But when a large number of output bits are sampled by TFF, they tend to be equal [3]. For the consideration of low power consumption and chip area, the digital processor is realized by a 16-bit linear feedback shift register (LFSR).

As shown in Fig. 2a, the random seed generator is composed of a noise amplifier, a hysteresis comparator, a constant current charge pump, an analog level shifter. The noise sources of this circuit are two large noise resistors R_n at the input of the amplifier, whose noise is collected and amplified. To make use of this noise voltage, a triangular carrier wave is formed by the generator. Shown in Fig. 2a, the charge-pump charges or discharges the load capacitor C_1 with constant current I_c at first. The level shifter shifts this wave to the common mode input voltage of the amplifier at node "A" in Fig. 2a. Demonstrated in Fig. 2b, the voltage gets nearly unit gain by the noise amplifier, through which the noise is added to the wave as random source. When the noise-added triangular wave crosses the threshold of the hysteresis comparator, the voltage at node "C" is inverted and the charge pump discharges (or recharges) the capacitor C_1 with constant current I_c. Since the level shifter isolates the capacitor C_1 and the amplifier, the carrier wave will stabilize automatically according to the reference voltage.

3 Design Considerations and Tradeoffs

In RFID tags, a good RNG means low power, small chip area and high randomicity level. However, these requirements usually conflict with each other. Therefore, tradeoffs among these factors need to be taken with care. In the tradeoffs, the power and area limitations of Gen2 RFID tag should be taken into consideration. Power budget of a typical Gen2 tag today is less than 10 μW [10]. Therefore, the power of an RNG should be one order lower, so as not to greatly deteriorate the performance of the tag. The area of a typical Gen2 tag is about 0.5 mm^2 [11], and the area occupied by the RNG should be one order smaller as well.

The noise amplifier is the core of the whole circuit. It consumes the largest part of the power and need to be considered carefully. The noise voltage at the output of the amplifier can be get according to Eq. (1) [3]. $\delta(V_n)$ is the noise voltage, A_v and B_W are respectively gain and bandwidth of the amplifier, R_n is the noise resistance.

$$\delta(V_n) = \sqrt{8KT \cdot GBW \cdot R_n A_V} = \sqrt{8KTB_W R_n A_V^2} \tag{1}$$

Equation (2) shows the relationship between delta of clock jitter $\delta(T_{CLK\_S})$ and noise voltage $\delta(V_n)$ [3,7]. S is the slope of the triangular wave, as shown in Fig. 2b.

$$\delta(T_{CLK\_S}) = \frac{\sqrt{2}}{S}\delta(V_n) \tag{2}$$

Since the TRNG has a low sample frequency, the $1/f$ noise could result in some co-relations among the output bits. In order to minimize this effect, PMOS transistors, instead of NMOS transistors, and large area MOSFETs are used. Digital post processor is also employed to de-relate the output bits to reduce this effect [8,12].

The upper limit of sample rate f_s, which is the frequency of *CLK_s*, is determined by the equation below [7].

$$r_x(T_s) = \exp(-2\pi B_W/f_s) = E\{R_X(1)\} < 0.367(N)^{-\frac{1}{2}} \tag{3}$$

where $r_x(T_s)$ is the continuous-time auto-correlation function, $E\{\mathrm{R}_x(1)\}$ is the estimation of the Gaussian variable and N is the number of the output bits. From the equation, It can be drawn that with certain B_W, larger the output bit number is required, smaller the sample rate is limited. When $N = 16$, which is the number of random bits in RFID system, the relationship between bit rate and bandwidth of the noise amplifier can be drawn as Eq. (4). B_W should be larger than the sample rate f_s, so that the output of the amplified thermal noise is still Gaussian distributed in the spectrum.

$$f_s \leq 1.66B_W \tag{4}$$

The lower limit of the bit rate is determined by the communication cycle of tag to reader in RFID system. Since the 16-bit random number needs to be prepared during the power-on phase of the tag, total time for random number generation must be less than 1 ms according to the Gen2 protocol. In order to get plentiful time for post processing, the analog part should prepare a 16-bit random seed in less than 500 μs. Therefore, the smallest f_s should be no less than 32 kHz.

3.1 Trade-off Between Bit Rate, Noise Voltage $\delta(V)_n$ and Power Consumption

According to Eqs. (1) and (2), a large bandwidth is needed if a fast bit rate is chosen. A large noise voltage $\delta(V_n)$ also requires a large gain of the noise amplifier. But either the increase of the bandwidth or the gain requires more power consumption.

$$GBW = A_V B_W \tag{5}$$

According to Eqs. (1), (2), (5), $\delta(V_n) = 3\,\text{mV}$ and $f_s = 40\,\text{kHz}$ is chosen to cut down the power consumption. Accordingly, the 3 dB bandwidth of the noise amplifier is chosen to be larger than 50 kHz in order to guarantee the quality of the random seeds, while its gain should be 34 dB at least.

3.2 Trade-off Between Power Consumption and Chip Area

According to Eq. (2), the larger the noise resistor is, the smaller the gain and bandwidth of the amplifier is needed to achieve a certain noise voltage, which leads to lower power consumption. However, a large resistor consumes a large chip area. Therefore, careful consideration should be taken to balance the area of resistors and the power consumption. Since the TRNG should be one order smaller than the total area of a tag, the TRNG should be no more than 0.05 mm^2. In SMIC 0.18 μm standard process, one 2 MΩ high resistance poly resistor, which has the largest sheet resistance of about 989.6 Ω/□, accounts for about 0.01 mm^2 chip area. Considering other parts of the circuit, one noise resistor R_n should be no larger than 2–3 MΩ.

3.3 Trade-off Between Power Consumption of Fast Oscillator and Noise Amplifier

It has been demonstrated that the clock jitter should be several times of the fast oscillator to guarantee randomicity [3,5,9]. The relationship between noise voltage $\delta(V_n)$ and the clock jitter $\delta(T_{TCK\_S})$ is determined by Eq. (5).

$$S = \frac{\sqrt{2}\delta\,(V_n)}{\delta\left(T_{CLK\_S}\right)} \tag{6}$$

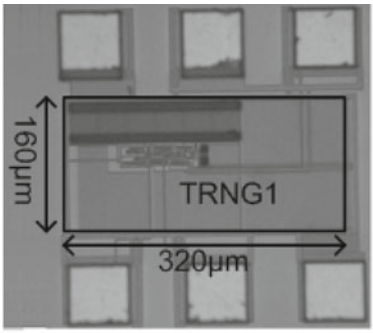
The clock jitter should be at least 6 times of the fast oscillator [3]. The system clock of UHF tag is normally 1.28, 1.92 or 2.56 MHz [6]. As in Eqs. (1), (2), (5), $\delta(V_n)$ can be smaller if CLK_f runs faster. In order to insure that the TRNG can be utilized in all UHF tags, we choose the slowest clock frequency (1.28 MHz) as the fast oscillator.

4 Implementation and Measurement Results

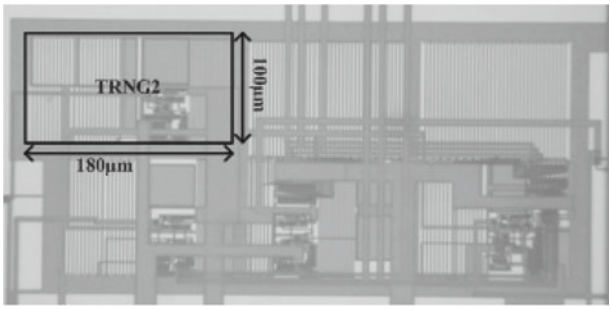
Based on the above trade-offs and limitations in Gen2 RFID tag system, two TRNG circuits are designed at the speed of 40 kb/s. With the same randomicity level, different power consumption and noise resistors are chosen, in order to verify the trade-off between the power and chip area. The specifications of the two TRNG circuits are listed in Table 1. In TRNG1, the noise resistors are chosen to 2 MΩ each. And the bandwidth of the noise amplifier is 50 kHz in order to cut down the power consumption to 1 μW. On the other hand, the power consumption of TRNG2 is released to 2.6 μW while its noise resistors are chosen to be 700 KΩ, in order to minimize the chip area.

Table 1 System specification of proposed TRNG circuits

Items	TRNG1	TRNG2
Output speed (kb/s)	40	40
Gain of noise amplifier (dB)	34	34
Bandwidth of noise amplifier (KHz)	50	150
Output noise voltage $\delta(V_n)$ (mV)	3	3
Noise resistor	2 MΩ	700 KΩ
Threshold voltage of comparator (mV)	30	30
Power (μW)	1	2.6



(a) Layout of TRNG1



(b) Layout of TRNG2

Fig. 3 Micrograph of proposed TRNG Circuits.

Both of the circuits are fabricated in SMIC 0.18 μm standard process. As demonstrated in Fig. 3, the proposed TRNG1 accounts for a chip area of about 0.05 mm^2 and TRNG2 occupies a chip area of 0.018 mm^2.

The measurement platform is set up as Fig. 4. Both the random seeds and jittery clock are put into a logic analyzer to collect the random bits. The jittery clock is used as the sample clock that triggers the sampling, and the random bits are collected as data. In order to minimize the noise from power supply, a battery is used as power supply.

A modified 16-bit LFSR is used as the digital post processor. It utilizes a XOR gate to introduce random seeds, (shown in Fig. 5). This post process is done by MATLAB simulation in the design. In practical application, the clock of the LFSR is supposed to be connected

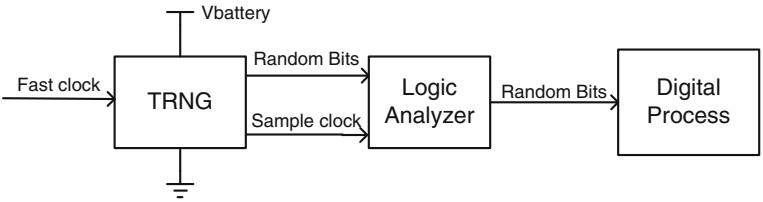


Fig. 4 TRNG measure platform

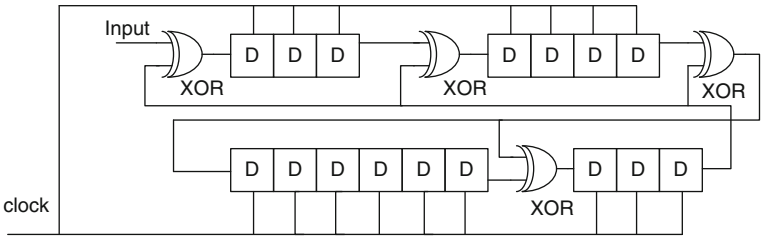


Fig. 5 Post digital process scheme of TRNG [7]. It is comprised by 16 LFSR, 16 bit DFF and 4 XOR gate

Table 2 Pass rate performance in FIPS 140-2 standard

Test item	Criteria/20,000 bits	Pass rate of TRNG1 (%)	Pass rate of TRNG2 (%)
Monobit	9750–10250	93.8	98.0
Poker test	2.16–46.17	86.1	94.1
Runs test	Runs of length 1–6	96.9	95.2
Long run test	1–26	95.3	100

to the sample clock of the analog part during the seed getting period. It is reconnected to system clock for fast de-correlation processing when 16-bit analog output is produced and the analog seed generator is shut down to save power [7–9].

Power consumption, output bit rate, and randomicity performance of the TRNG are measured. The widely used FIPS 140-2 standard was employed to verify randomicity performance of the output bits [13]. Over 100 million bits were sampled and analyzed among ten chips. Their total pass rate is shown in Table 2. It can be seen though the pass rate of Poker test is a little lower than the pass rate of other tests because of the $1/f$ noise and limited amplifier bandwidth, both circuits have high pass rate over 90% through the tests in FIPS 140-2. The measured circuit properties and comparison with other high quality TRNG designs are summarized in Table 3. The proposed TRNG circuits make a balance between power consumption, chip area, bit rate at a small cost of randomicity. TRNG1 successfully makes a 40 kb/s random number output with a power consumption of 1.04 μW and a chip area of 0.05 mm^2. TRNG2 realizes in a small chip area of 0.018 mm^2 by a power of 2.6 μW. The measured speed of TRNG2 is 48 kb/s.

Table 3 Comparison of TRNG circuits

TRNG Design	Power	Bit rate	Chip area (mm^2)
Trans. circuits and systems, 2003 [3]	2.3 mW	10 Mb/s	0.0016
ESSCC, (DC), 2006 [4]	180 μW	50 kb/s	1.49
ESSCC, (FIR), 2006 [4]	2.92 μW	0.5 kb/s	0.031
Proposed TRNG1	1.04 μW	40 kb/s	0.05
Proposed TRNG2	2.6 μW	48 kb/s	0.018

5 Conclusion

Low power oscillator-based TRNG mechanism suitable to cope with the security and privacy concerns in RFID tags was analyzed. The TRNG can also be used as a means for anti-collision purpose. And two ultra-low power TRNG circuits were implemented in SMIC 0.18 μm CMOS process according to the analysis. Both of them have features of low power and small chip area. Measurement results of the TRNG show high pass rate through the tests. The proposed TRNG circuits are not restricted to the applications of Gen2 RFID system. The theoretical analysis and tradeoffs deduced in this paper make them also feasible in other low power applications of cryptography, like ISO-15693 ID cards, WSN, VSAT, and etc.

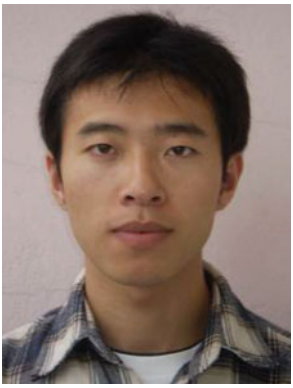
Acknowledgments This Project was supported by National Key Technology R&D Program (2008BAH 22B04) and General project of State Key Lab of ASIC and System, Fudan University, China (No.09MS009).

References

1. EPC^{TM} Radio-frequency identity protocols class-1 generation-2 UHF RFID protocol for communications at 860 MHz–960 MHz Version 1.1.0 (pp. 40). http://www.epcglobalinc.org/standards/uhfc1g2/uhfc1g2_1_1_0-standard-20071017.pdf.
2. Balachandran, G., & Barnett, R. (2008). A 440-nA true random number generator for passive RFID tags. *IEEE Transactions on Circuits and Systems I: Regular Papers, 55*(11), 3723–3732.
3. Bucci, M., Germani, L., Luzzi, R., et al. (2003). A high-speed oscillator-based truly random number source for cryptographic applications on a smart card IC. *IEEE Transactions on Computers, 52*(4).
4. Holleman, J., & Otis, B. (2006). A 2.92 μW hardware random number generator. In *Proceedings of the 32nd European solid-state circuits conference* (pp. 134–137).
5. Dichtl, M. (2003). How to predict the output of a hardware random number generator. In *Workshop on cryptographic hardware and embedded systems*, LNCS (Vol. 2779, pp.181–188), 2003.
6. Luo, Q., Guo, L., Li, Q., et al. (2009). A low-power dual-clock strategy for digital circuits of EPC Gen2 RFID tag. *International RFID conference* (pp. 7–14).
7. Che, W., Deng, H., Tan, X., et al. (2007). Scheme of truly random number generator application in RFID Tag. http://www.autoidlabs.org/single-view/dir/article/6/231/page.html.
8. Xin, Q., Zeng, X., et al. (2005). Modeling and system simulation of truly random number generator. *Journal of System Simulation,* 17(1).
9. Golic, J. (2006). New methods for digital generation and post processing of random data. *Transactions on Computers,* 55(10).
10. Pillai, V., & Heinrich, H. (2007). An ultra-low-power long range battery/passive RFID tag for UHF and microwave bands with a current consumption of 700 nA at 1.5 V. *IEEE Transactions on Circuits and Systems I Regular Papers, 54*(7), 1500–1512.
11. Barnett, R., Balachandran, G., Lazar, S., et al. (2007). A passive UHF RFID transponder for EPC Gen 2 with −14 dBm sensitivity in 0.13μm CMOS. *IEEE ISSCC Dig Tech Papers.*
12. Petrie, C., & Connelly, J. (1996). Modeling and simulation of oscillator-based random nunmber generators. *IEEE International Symposium on Circuits and Systems, 4*, 324–327.

13. National Institute of Standards and Technology USA, FIPS PUB 140-2 Federal Information Processing Standards. Publication. http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf.

Author Biographies



Wei Chen received the B.S. degree in science of microelectronics and solid-state electronics from Fudan University, Shanghai, China, in 2008. He is working toward the M.S. degree in science of microelectronics and solid-state electronics at state key laboratory of application specific integrated circuits in Fudan University. His research interests include RF and analog circuit design. In his M.S. degree study, his has worked on analog front end for passive and semi-passive RFID tags and analog random number generator for RFID.

Wenyi Che received the B.S. degree in science of microelectronics and solid-state electronics from Fudan University, Shanghai, China, in 2005. He is currently working toward the Ph.D. degree in science of microelectronics and solid-state electronics at state key laboratory of application specific integrated circuits in Fudan University. His research interests include RF and analog circuit design. During his Ph.D. program, he has been in charge of developing various kinds of RFID tags, such as passive, semi-passive UHF tag, and sensor enabled tag.

Na Yan received the Ph.D. degree in Microelectronics from Fudan University, China, in 2007. Then she joined the Faculty of Fudan University, where she is an assistant professor of State Key Laboratory of ASIC & System and Auto ID Laboratory in Fudan. Her research interests are RF ad mixed signal integrated circuit design, including ultra low power circuit design, memory, RFID tag chip, and transceiver circuits, etc.

Xi Tan received the B.S. degree in physics from Nanjing University, China, in 2000, the M.S. degree in micro-electronics from Delft University of Technology, Netherland, in 2005, and the Ph.D. degree in micro-electronics from Fudan University, China, in 2008. From 2000 to 2002, he has been with Silan micro-electronics Corporation, working on MCU design. Since 2008, he has been assistant researcher in the department of micro-electronics of Fudan University, working on radio frequency circuits and wireless transceiver chip design.

Hao Min received the B.S. and M.S. degrees in electrical engineering and Ph.D. degree in material science from Fudan University, Shanghai, China, in 1985, 1988, and 1991, respectively. From 1991 to 1998, he was an Associate Professor with the Application Specific Integrated Circuit (ASIC) and Systems State Key Laboratory, Fudan University. From 1995 to 1998, he was a Visiting Associate Professor with the Department of Electrical Engineering, Stanford University, Stanford, CA, where he was involved in low-power mixed-signal very large scale integration (VLSI) design, especially in the design and characterizing of CMOS image sensors. Since 1998, he has been a Professor and Director of the ASIC and System State Key Laboratory, Fudan University. In 2002, he began the Auto-ID Center of China and is currently the Research Director of Auto-ID Laboratory, Fudan University. He has authored or coauthored over 50 papers in journals and conferences. He has ten patents pending. His current research interests include VLSI architecture, RF and mixed-signal integrated circuit (IC) design, digital signal processing, and image processing.