北京大学学报(自然科学版), 第 50 卷, 第 4 期, 2014 年 7 月
Acta Scientiarum Naturalium Universitatis Pekinensis, Vol. 50, No. 4 (July 2014)
doi: 10.13209/j.0479-8023.2014.039

Design and Implementation of Baseband Transmitter for UHF RFID Reader

YONG Shanshan, WANG Xin'an†, ZHANG Fangni, SHI Xiaolong, LIU Bin, GUO Zhaoyang, LÜ Wei, CAO Ying, SU Jiting

The Key Laboratory of Integrated Micro-systems Science and Engineering Applications, Peking University Shenzhen Graduate School, Shenzhen 518055; † Corresponding author, E-mail: wangxa@pkusz.edu.cn

Abstract A baseband transmitter for UHF (ultra high frequency) RFID (radio frequency identification) reader is proposed, which supports ISO 18000-6B&6C protocol and works at 840 – 960 MHz. Taking security and compatibility into consideration, 2-bits PIE-kind encoder and PIE encoder are both implemented, the former is 6 times higher security than the later. In SSB modulation, when there is amplitude mismatch of two quadrature signals, it will generate two frequency bands and result in performance lost. For this problem, an amplitude matching module is integrated. A power adjustment module in baseband is also proposed to enhance the signal and get larger input signal for PA to generate larger PA output power. The whole reader chip is implemented in a 0.18 μm CMOS process and consumes 209461 gates and 102.609 mW. The baseband transmitter takes up 22% of the total area. This novel architecture doesn't bring much lost in area and power consumption compared with other existing designs.

Key words UHF RFID reader; baseband transmitter; encoder; power adjustment

一种超高频 RFID 读写器基带发射机的设计与实现

雍珊珊 王新安† 张芳妮 史小龙 刘彬 郭朝阳 吕伟 曹颖 苏吉婷

北京大学深圳研究生院集成微系统科学工程与应用重点实验室, 深圳 518055; † 通信作者, E-mail: wangxa@pkusz.edu.cn

摘要 设计了一个超高频射频识别读写器的基带发射机, 该读写器基带芯片工作在 840~960 MHz 频段, 支持 ISO 18000-6B&6C 协议。为了增强安全性同时保证与协议的兼容, 采用 2-bits 类 PIE 编码和 PIE 编码方式, 前者相对后者安全性提高了 6 倍。针对单边带调制中由于两路正交信号幅度不相等而产生的双频带对标签接收信号产生干扰的问题, 在基带发射机中增加了幅度匹配模块, 尽量消除幅度差异。还在基带部分增加了功率放大模块, 使得到达 PA 的输入信号幅度增强, 从而得到更高的输出功率。整个读写器芯片在 0.18 μm CMOS 工艺下, 电路规模为 209461 个门, 功耗为 102.609 mW, 其中发射机部分占面积的 22%。与当前的一些设计相比, 该设计并没有带来较大的面积和功耗损失。

关键词 超高频 RFID 读写器; 基带发射机; 编码器; 功率调节
中图分类号 TN492

Radio frequency identification (RFID) technology, which can provide both identification and definition localization of objects, has been widely applied in more and more areas, such as logistics, military, NFC (near field communication) payment, health care, security, etc[1]. UHF (ultra high frequency) RFID, the range frequency of which is from 840 to 960 MHz, has the advantage in long distance identification, high

深圳市重点实验室提升计划(CXB201104210007A)资助
收稿日期: 2013–03–27; 修回日期: 2013–06–07; 网络出版日期: 2014–02–14

efficiency, high robustness and high throughput[2]. However, with RFID applied in a wide range of applications, which bring us new challenges, such as the security and privacy concerns[3–4], management of various tags, lower power, small size and low cost[5]. In this paper, a baseband transmitter for UHF RFID reader is presented. We focus on the security and signal processing issues.

To solve the security and privacy problem, one most cost-effective method is secure authentication protocol, which is based on hash lock algorithm[6], or encryption algorithm[7–8]. However, the requirements of low area and low power limit the application of these algorithms in RFID. We realize that the encode algorithm can also be a security enhancement point. So, a new encode algorithm, 2-bits PIE-kind encoding, which is developed from PIE (pulse interval encoding), is proposed. In consideration of compatibility, PIE is also supported. The degree of security of the former is 6 times higher than the later. Compared with the authentication algorithms, the implementtation of new encoder is simpler with less cost. What's more, two encoders in reader make system more secure through switching encoder randomly controlled by termination.

For the issue of signal processing, we try to solve two problems existing in reader. The first one is associated with SSB (single sideband) modulation. If the amplitude of two quadrature signals, in-phase (I) and quadrature (Q), are not equal, it will generate two frequency bands which decreases the antijamming capability of tag receiver. So, an amplitude adjustable module designed to eliminate amplitude mismatch. The second problem is about the signal power of transmitter. In this paper, we design a power adjustable module enlarge signal in baseband to enlarge input signal of PA, and then make PA generate higher power output.

1 Chip Architecture

Fig. 1 shows the block diagram of the proposed UHF RFID reader, which includes an analog front-end, baseband receiver, baseband transmitter, MPS (message passing station) and serial interface. The analog receiver captures signals from antenna and transform them into digital signals, then baseband receiver implements decimation filtering, channel filtering, phase recovery, demodulation, decoding and CRC (cyclic redundancy check). MPS plays the role of system control like setting state registers and anti-collision processing. Through the serial interface, the termination visits MPS to get the response data from tag and sends instructions to MPS. When MPS gets an instruction from termination, it will open baseband transmitter to start encoding and CRC. After encoding, the next step is to narrow the frequency

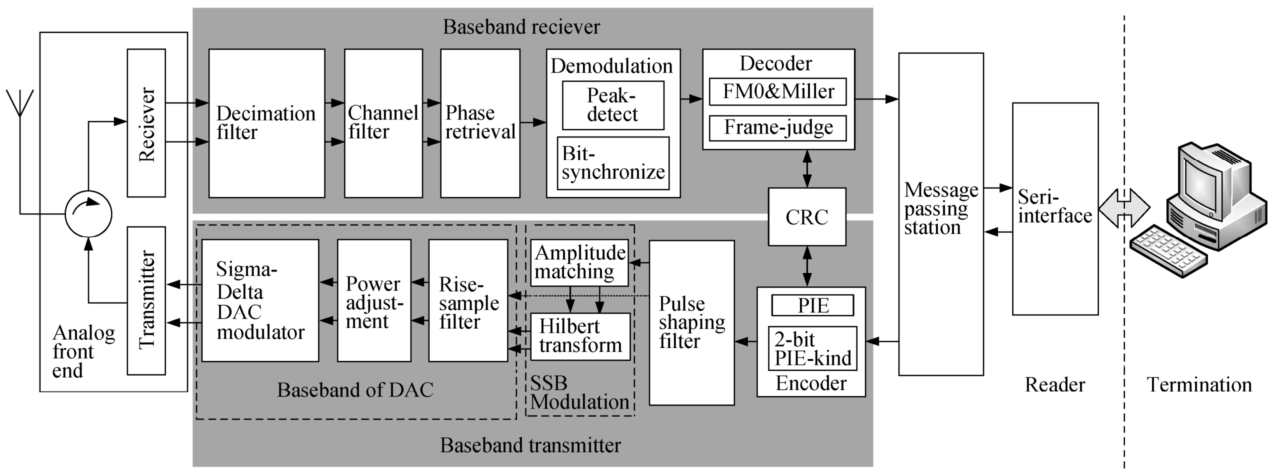


Fig. 1 Block diagram of the proposed UHF RFID reader

bandwidth of pulse signals through shape filtering. Then in SSB modulation, it will generate two amplitude matching and quadrature signals, *I* and *Q*, through amplitude matching and Hilbert transforming. The last step before signals enter into analog front end is to convert digital signal to analog signal. In the proposed reader, a rise-sample filter and power adjustment module are used for preparing high sampling rate and high power signals before the sigma-delta DAC (digital analog convert) digital modulator. The transmitter in analog front-end will process the signals from baseband and transmit to tag through antenna.

The proposed reader supports both ISO 18000-6B&6C with higher security and better quantity of signals. In this paper, we mainly discuss the baseband transmitter's design consideration and implementation.

2 Reader Baseband Transmitter

2.1 2-bit PIE-kind encoder

In the forward link (reader to transmitter), PIE and Manchester are the most popular encode algorithms. In this paper, we do not only choose PIE as forward link encoder, but also choose a 2-bit PIE-kind encode algorithm to enhance the security of reader.

Fig. 2 shows the symbol of these two encoding algorithms. For PIE, there are only two symbols to represent data 0 and data 1. Despite the change of Tari, the capture time to crack the encode principle is $A_2^2=4$. For 2-bit PIE-kind, there are four symbols to represent data 00, 01, 10 and 11. One symbol carries two bits data. We can infer that the capture time of it is $A_4^4=24$ which is 6 times larger than PIE, which means that 2-bit PIE-kind encoder is more secure.

Meanwhile, the new encode algorithm does not bring performance lost. The power of signals is associated with the duty cycles of data and higher duty cycle can bring better performance[9]. To make a comparison of duty cycles shown in Table 1, there is no lost of duty cycle in 2-bits PIE-kind encoder. Table 2 shows that there is no encode efficiency lost. The data preamble of PIE and 2-bit PIE-kind is different shown in Fig. 3.

Table 1 Duty cycles of data in two encoders

Encoder	Duty cycle/%			
	00	01	10	11
PIE	50	66.7	66.7	75
2-bit PIE-kind	50	66.7	80	75

Table 2 Encode efficiency of data in two encoders

Encoder	Encode efficiency/Tari			
	00	01	10	11
PIE	4	4	4	4
2-bit PIE-kind	2	3	5	4

The architecture of encoder is based on a 6 state FSM (finite state machine). State one is "IDLE" which keep all registers unchangeable with initialization value. When MPS fires the encoder, state jumps to second state. In second state, the function is to choose preamble according to the value of encode flag register. After finishing preamble transmits, state goes on jumping to next state, "Adjustment" implements generation of calibration or frame synchronous data.

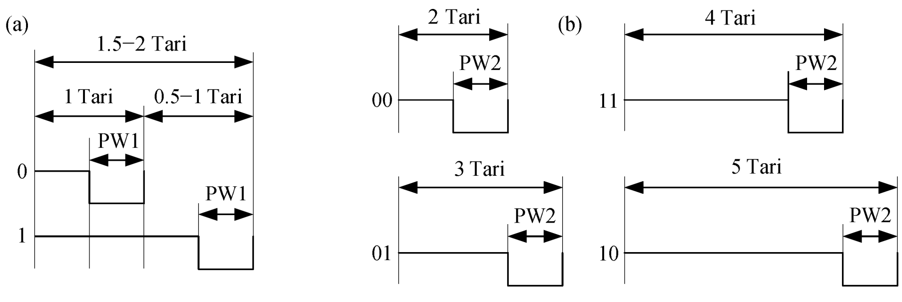


Fig. 2 PIE symbol (a) and 2-bits PIE-kind encode symbol (b)

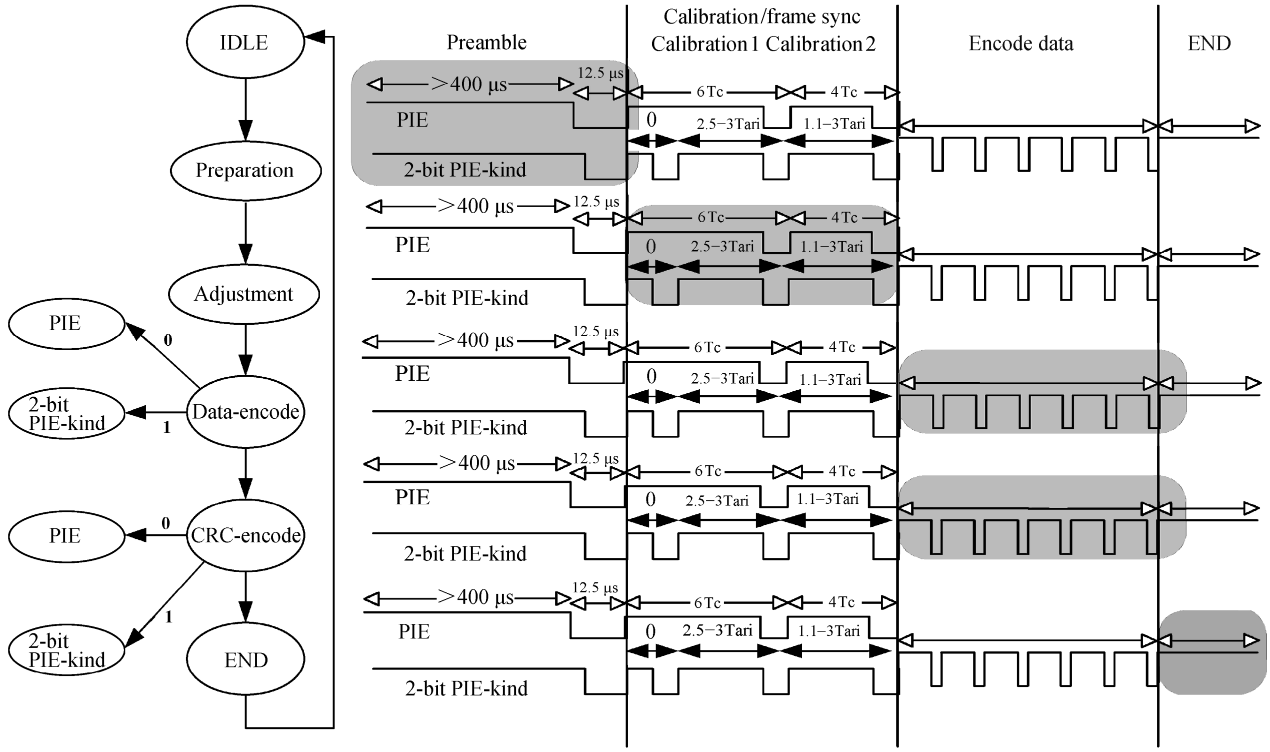


Fig. 3　FSM based encoder

Then, state moves to “Data-encode” to encode data according to the symbols of data shown in Fig. 2. After data encoding, state goes to “CRC-encode” to encode CRC data. In the last state, sending 8 cycles high level signal to imply encode completion.

2.2　SSB modulation with amplitude matching

In the proposed reader transmitter, DSB and SSB modulation are both supported. Hilbert filter is used to generate signal Q which is a 21-orders FIR filter and the AF diagram of it is shown in Fig. 4. There are a lot of multipliers existing in filter which will bring too much area and power cost. To reduce cost, all multipliers are designed based on shifting and addition logic. Each data, A (n bits), can be split like Eq. (1). So, the multiply of two operands, A and B, can be expressed as the sum-shift format shown in Eq. (2).

$$A[n:0]=2^{n}+2^{n-1}+\cdots+2^{0}, \quad (1)$$

$$A*B=B \ll n+B \ll n-1+\cdots B \ll 1+B. \quad (2)$$

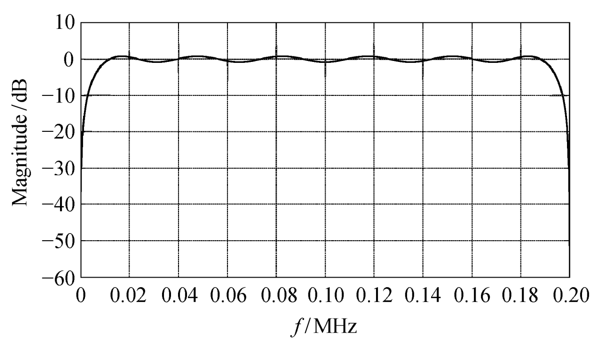
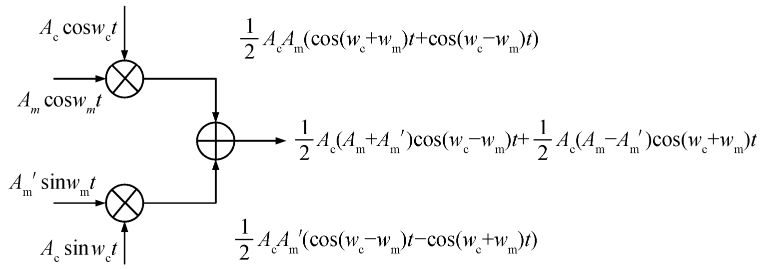


Fig. 4　AF diagram of the proposed Hilbert filter

For SSB, there is only one frequency band exist. Compared with DSB, the bandwidth efficiency of SSB is doubled. Fig. 5 shows the SSB modulation principle. $A_m \cos w_m t$ is signal I, $A_m \sin w_m t$ is signal Q. $A_c \cos w_c t$ and $A_c \sin w_c t$ are two quadrature carrier signals. After modulation, the SSB signal is $A_c A_m \cos(w_c - w_m)t$ which only has one frequency band. However, if the amplitude of signal I and Q is not equal, there will be two frequency bands exist in SSB shown in Eq. (3) in Fig. 5 which brings performance lost. So, an amplitude matching module is taken into consideration to reduce the amplitude difference between signal I and Q.



(3)

Fig. 5　SSB modulation principle

There are two 12 bits × 12 bits multipliers in amplitude matching module to generate two 12 bits data. The architecture of multiplier in Hilbert filter and amplitude matching module is both based on shifting-addition logic.

2.3　Baseband Sigma-Delta DAC modulator with power adjustment

Sigma-Delta DAC consists of digital modulator and analog-shaping filter. The first module of digital modulator is an interpolator for oversampling the encode data to generate oversampled data which is implemented by a 21-orders FIR filter.

Nowadays, most popular tag is passive that acquires energy from reader. The energy of tag can be expressed as Eq. (4)[10]:

$$P_{\text{tag}} = P_{\text{tx}} G_{\text{tx}} G_{\text{tag}} \left(\frac{\lambda}{4\pi R} \right)^2 , \tag{4}$$

P_{tag} is the receive power of tag, P_{tx} is the transmit power of reader, G_{tx} is the transmit gain of reader antenna, G_{tag} is the receive gain of tag antenna, λ is the wavelength of carrier signal, R is the length between reader and tag. When G_{tx}, G_{tag}, λ and P_{tag} are all unchanged, R is depended on P_{tx} which means that P_{tx} is larger will make R larger too. To achieve longer transfer length, the higher power of signals from reader the better. In general, power amplifying is performed in analog front-end. However, the design of PA is one of the most difficult tasks in analog front-end design. In this paper, we introduce a digital power amplifier into reader to extend the ability of power control which can amplify signal from 1 to 15 times before sigma-delta DAC digital modulator. The circuit is composed of two 12 bits × 4 bits multipliers which is based on shiting-addition architecture and generate two 16 bits data. Fig. 6 shows the two groups input signal of PA with different adjusting coefficients, the maximum amplitude of signal is *I*_max which is up to 600 mV, and the minimum one is *Q*_min which is 100 mV.

At last, the mainly module is a digital modulator which is based on 3-level CIFF[11] architecture shown in Fig. 7. Function simulation and performance evaluation by Simulink, we get the power spectrum density shown in Fig. 8. The SNDR (signal to noise and distortion ratio) of modulator is 89.2 dB, real accuracy (ENOB) is 14.52 bits.

3　Results and Discussion

In this paper, we introduce the design and implementation of UHF RFID reader transmitter which passes fully function verification and tapes out. The simulation result is shown in Fig. 9. Data which comes from encoder is one bit stream of 0/1, then data will be shaped by pulse shaping filter and the width extended to 12 bits. The next step is SSB modulation which includes amplitude matching and Hilbert transform filter. For DSB modulation, data will be passed through these two modules straightly. The wave of data after oversampling becomes much smoother prepared for DAC. According to Fig. 9, we can also see that the amplitude of signal *I* and *Q* become larger, the width of which is 16 bits. Finally, 16 bits data is transformed into one bit stream of 0/1 again.

Compared with current designs, we make much effort on enhancing security and signal processing for UHF RFID reader transmitter design. A new encoder,

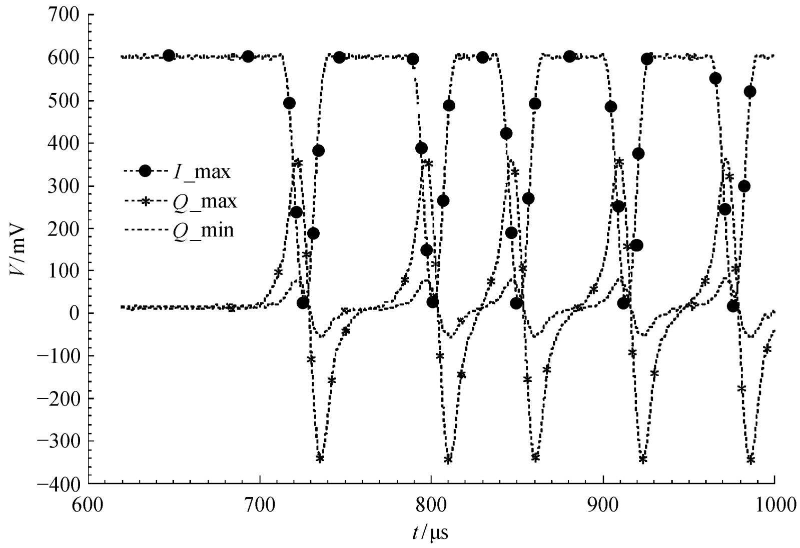


Fig. 6　Input signal of PA with different adjusting coefficients

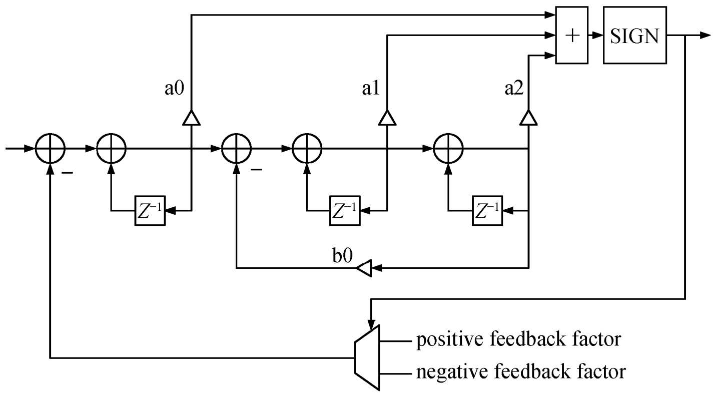


Fig. 7　3-level CIFF digital modulator[11]

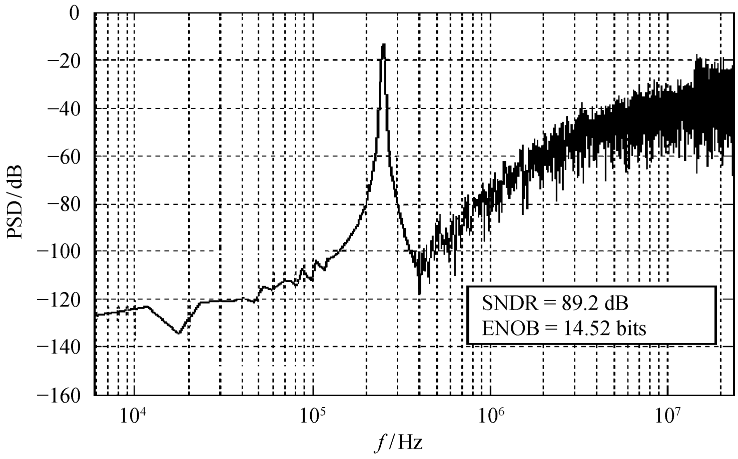


Fig. 8　Power spectral density of digital modulator

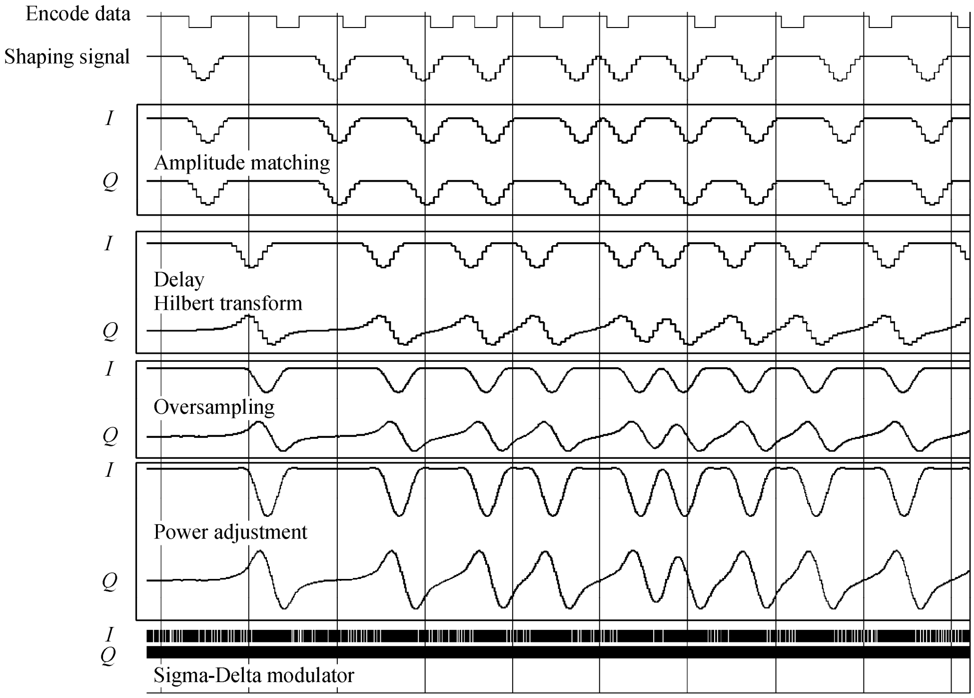


Fig. 9　Simulation wave of each part

which is developed from PIE algorithm, enhances the security of system. The other two novel modules in the system, which are amplitude matching and power adjustment module, enhance the quantity of transmit signals from reader. The whole chip is implemented in 0.18 μm CMOS process, the layout of which is presented in Fig. 10. Core size of reader is 989.5 μm × 1587.6 μm, and the chip size is 1299.52 μm × 1897.60 μm. The power of whole chip is 102.609 mW. Compared with Ref. [12], the performance of this work is comparable in area (Table 3).

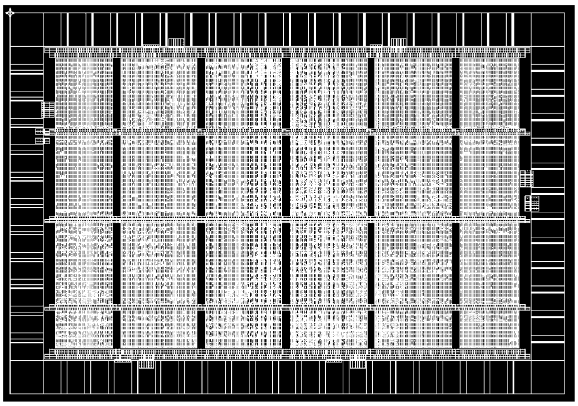


Fig. 10　Layout of UHF RFID reader chip

Table 3　Performance comparison

Items	This work	Ref. [12]
Standard Spec	ISO 18000 6B & 6C	EPC C1G2
Process	0.18 μm CMOS	IBM 0.13 μm RF CMOS
Chip area/μm^2	2465969	9000000
Gates	209461	270000
Power cost/mW	102.609	298.5456

4　Conclusion

In this paper, we have introduced a novel architecture of UHF RFID reader baseband transmitter. In consideration of security and signal quantity, we have integrated three new modules in transmitter. One is a 2-bit PIE-kind encoder, the security of which is 6 times higher than PIE. The second one is amplitude matching used to generate two quadrature phase signals with other largest approximate amplitude to avoid performance lost brought by two frequency bands in SSB modulation.

The last one is a power amplifier which plays the role of auxiliary digital PA for analog PA to enhance the power of signals from reader. Under 0.18 μm CMOS process, the whole reader chip consumes 209461 gates and 102.609 mW which are acceptable. The baseband transmitter takes up 22% area. Compared with some designs, this novel architecture does not bring up much area and power cost.

References

[1] Zuo Yanjun. Survivable RFID systems: issues, challenges, and techniques. IEEE Transactions on Systems, Man, and Cybernetics: Applications and Reviews, 2010, 40(4): 406–418

[2] Wang Wenting, Lou S, Chui K. A single-chip UHF RFID reader in 0.18 μm CMOS process. IEEE Journal of Solid-State Circuits, 2008, 43(8): 1741–1754

[3] Liu A, Bailey L. PAP: a privacy and authentication protocol for passive RFID tags. Computer Communications, 2009, 32: 1194–1199

[4] Langheinrich M. A survey of RFID privacy approaches. Pervasive Ubiquitous Computing, 2009, 13: 413–421

[5] Dardari D, D'Errico R, Roblin C, et al. Ultrawide bandwidth RFID: the next generation. Proceedings of the IEEE, 2010, 98(9): 1570–1582

[6] Weis S A, Sarma S E, Rivest R L. Security and privacy aspects of low-cost radio frequency identification system // Proc of the 1st International Conference on Security in Pervasive Computing. Berlin: Spring-Verlag, 2004: 201–212

[7] Abdelhalim M B, El-Mahallawy M, Ayyad M, et al. Implementation of a modified lightweight cryptographic TEA algorithm in RFID system // Internet Technology and Secured Transactions (ICITST). Abu Dhabi, 2011: 509–513

[8] Shen Xiang, Liu Dan, Yang Yuqing, et al. A low-cost UHF RFID tag baseband with an IDEA cryptography engine // Internet of Things (IOT). Tokyo, 2010: 1–5

[9] ISO/IEC 18000-6 Radio frequency for item management, part 6: Parameters for air interface communication at 860 MHz to 960 MHz [S]. Switzerland: ISO/ IEC, 2006

[10] Zhou Xiaoguang, Wang Xiaohua. Design, simulation and application of RFID system. Beijing: Posts and Telecom Press, 2008: 10–12

[11] Dai Fangming. Design and VLSI implementation of a16 bits∑-△DAC [D]. Beijing: Peking University, 2007

[12] Liu Jing. ASIC design of UHF RFID reader digital baseband compatible withISo/IEC 18000.6C standards [D]. Shanghai: East China Normal University, 2011