1

Development and Implementation of RFID Technology

Huiyun Li
Shenzhen Institute of Advanced Technology, Chinese Academy of Sciences, China

1. Introduction

Radio Frequency Identification (RFID) is an automated identification technology that uses tags to transmit data upon RFID reader queries. Compared to barcodes identification technology, RFID tags provide a unique identifier, which raises concerns over user privacy, such as clandestine tracking and inventorying [1]. In its original version, a RFID tag responds to a reader query with its fixed unique serial number. This fixed unique serial number enables tracking of tags and the bearers, possibly without the bearers' knowledge or consent. In addition to the unique serial number, some tags carry information about the objects they are attached to. Thus, a retail store or a person owning such tags might be under threat of clandestine inventorying.

Enormous research effort has been paid in attempt to solve the problem of consumer privacy and industrial espionage in the RFID world. However, most methods demand heavy or frequent cryptographic operations on RFID tags, which contradict the low cost demand of RFID tags ($0.05-0.10). Typically, a low-cost tag should only store hundreds of bits and have 5K-10K logic gates, only a fraction of the gates can be devoted to security tasks. The trade-off between cryptographic operations and low-cost has become a significant challenge in designing RFID tags, and this challenge has impeded RFID being the replacement of barcode technology for cost sensitive item-level applications, such as in supply chains, libraries and rental shops.

To solve this problem, a new RFID structure is proposed. Except the fixed unique serial number, tags carry only the IDs in disguise to avoid eavesdropping and clandestine tracking. The database, on the other hand, is responsible for protecting the information security, integrity and non-repudiation. This chapter discusses and presents the implementation of this passive ultra high frequency (UHF) RFID system, based on EPC Class 1 Generation 2 UHF RFID (abbreviate as Gen 2) protocols [1-2].

2. Communication between reader and tag

For a passive RFID system, the communication between the reader and the tag is fully controlled by the reader, i.e. the tag can't send data unless triggered by the reader [3]. The communication from the reader to the tag is referred to as the forward link, while the communication from the tag to the reader is referred to as the reverse link.

Source: Development and Implementation of RFID Technology, Book edited by: Cristina TURCU,
ISBN 978-3-902613-54-7, pp. 554, February 2009, I-Tech, Vienna, Austria

2.1 Forward link (from reader to tag)

A continuous RF wave is transmitted from the reader to the tag through the forward link. The data is sent from the reader to the tag as short gaps in this continuous wave in amplitude shift key (ASK) modulation with Pulse Interval Encoding (PIE). Figure 1 shows the Gen 2 protocol PIE encoding, where the duration of data '0' is T0, the duration of data '1' is between 1.5 T0 and 2 T0, the value of Pulse Width (PW) is from 0.265T0 to 0.525T0. The value of T0 is between 6.25μs and 25μs. So the data rate of forward link is between 26.7Kbps and 128Kbps. Figure 2 demonstrates the transmission example of amplitude shift key (ASK) modulation with Pulse Interval Encoding (PIE).

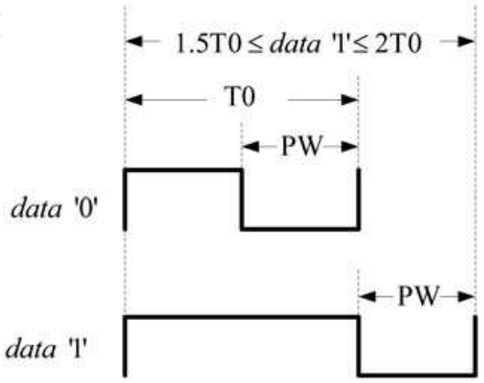

Fig. 1. Gen 2 Forward link PIE encoding

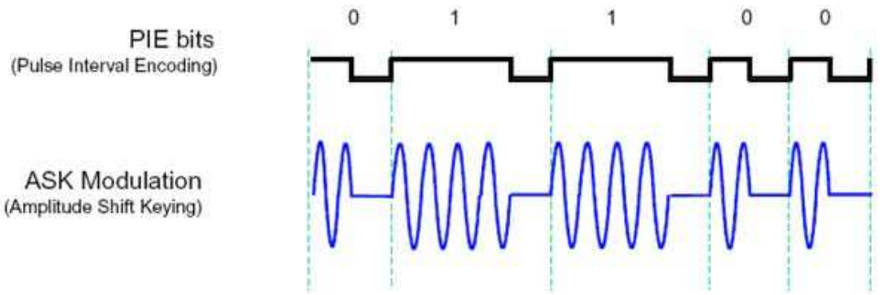

Fig. 2. Forward link transmission of ASK modulation with PIE encoding [3]

2.2 Reverse link (from tag to reader)

The reverse link in a RFID system is done using backscattering scheme. The modulation of the chip impedance can be done using either ASK or PSK. In ASK modulation, the chip impedance is varied between perfect match and complete mismatch. In PSK modulation, the real part of the chip impedance is kept in match with the antenna, while the imaginary part is varied between two capacitive and inductive values.

In Gen 2 protocol, Tags encode the backscattered data as either FM0 or Miller modulation. FM0 inverts the phase at every symbol boundary; a data '0' has an additional mid-symbol phase inversion, as shown in Figure 3.

Miller encoding inverts its phase between two data '0's, a data '1' has an additional mid-symbol phase inversion. The Miller subcarrier waveform is the baseband waveform multiplied by a square-wave at M times the symbol rate, and the value of M can be 2, 4 or 8 (selected by the reader). Figure 4 demonstrates Miller encoding when M is 2, 4 and 8

respectively [3]. Figure 5 illustrate the reverse link transmission of ASK and PSK modulation in Miller encoding.

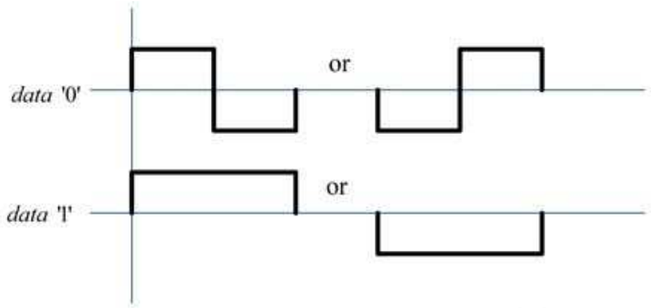

Fig. 3. Gen 2 reverse link FM0 encoding

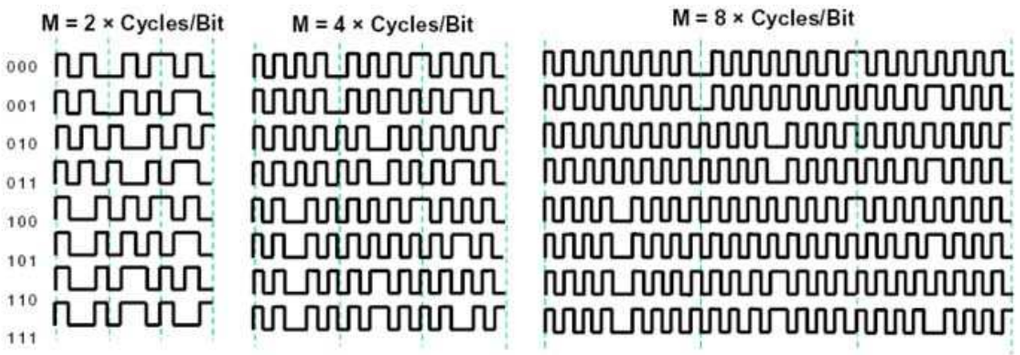

Fig. 4. Gen 2 Miller encoding [3]

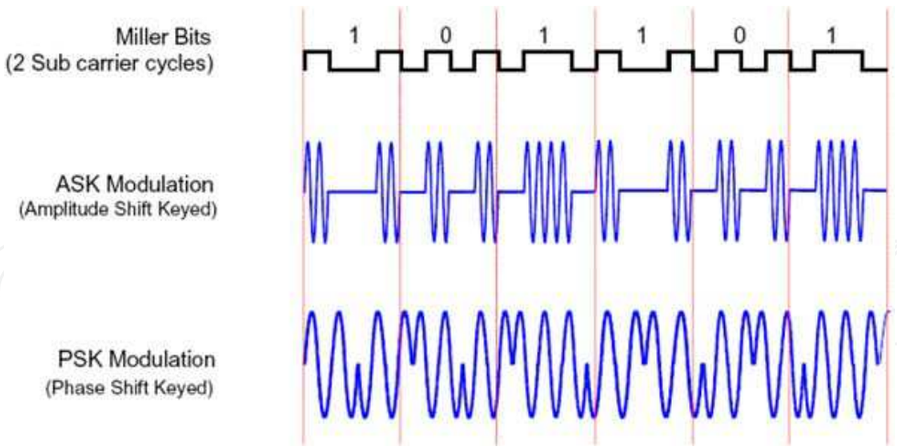

Fig. 5. Reverse link transmission in either ASK or PSK modulation with Miller encoding [3]

3. Tag implementation

In the following section, the implementation of a passive UHF RFID tag is discusses. Figure 6 shows a block diagram of RFID tag using backscatter modulation. The tag consists of tag antenna and tag chip. The tag chip contains a RF-analog front end, a digital control block, and a non-volatile memory.

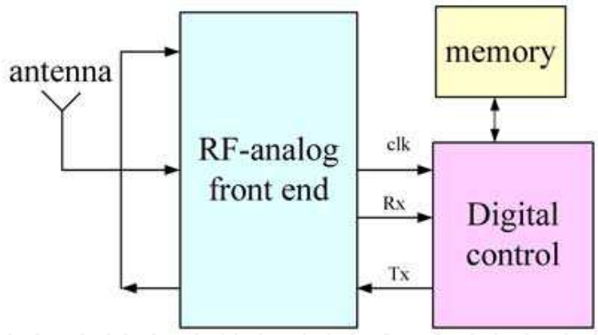

Fig. 6. Passive UHF RFID tag block diagram

3.1 RF-analog front end

The RF-analog front end includes a voltage rectifier, a demodulator, a clock generator, and a modulator [4], as shown in Figure 7.

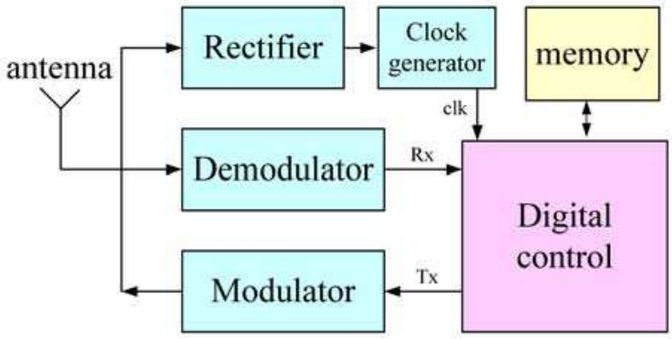

Fig. 7. RFID tag block diagram containing the RF-analog front end [4]

A. Rectifier

The rectifier has to supply the needed DC voltage with maximum efficiency possible. Figure 8 shows a multiple-stage rectifier that consists of diodes and capacitors [5]. All transistors and capacitors are set to be equal. The two input terminals V_{in} and *Gnd* are connected directly or via an impedance matching network to the UHF antenna (not shown), and is arbitrarily assigned as the ground node to the rectifier. The load capacitor C_L is large to store enough charge to complete signal processing tasks and to reduce the output ripple voltage. The output V_{out} is the input of clock generator.

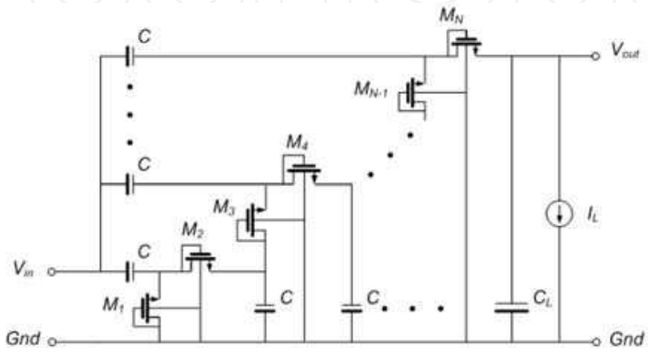

Fig. 8. Multi-stage rectifier [5]

B. Demodulator

Figure 9 shows the circuit schematic of ASK demodulator for forward link communication [6]. The ASK demodulator uses envelope detection and comparison with the average of the input voltage to recover baseband data. The envelope is transferred through a low pass filter to get its average value, and two values are then compared using a comparator. To deal with the voltage ripple from the envelope detector, the comparator needs hysteresis. The envelope detector uses 2-stage voltage multiplier to detect the envelope of the input RF signal. M3, which acts as a resistor, and the capacitor C make the low pass filter. The width and length of M3 determine the resistance. The input of the demodulator RF_{in} is the same as the difference of V_{in} and *Gnd* ($RF_{in} = V_{in} - Gnd$) shown in Figure 8, connected directly or via an impedance matching network to the UHF antenna. The output of the demodulator V_{out} is the input of later digital control block, and is the same as R_x shown in Figure 6.

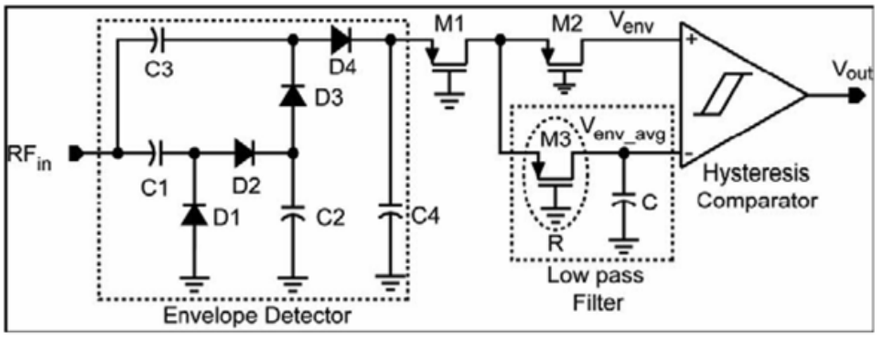

Fig. 9. Circuit schematic of the ASK demodulator [6].

C. Modulator

The PSK backscatter modulation is for reverse link communication. The circuit diagram is shown in Figure 10 [7]. Transistor M_1 is a MOS varactor that operates in inversion or in cutoff, depending on the input signal, causing the variation of the capacitance seen at the output of the modulator. Transistor M_2, instead, does not affect the output capacitance, since it has a small width with respect to M_1, but determines the resistance at the output of the modulator, which is, essentially, its drain-source resistance. As a consequence, the channel

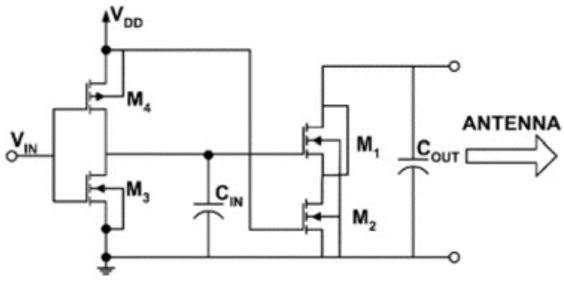

Fig. 10. PSK backscatter modulator.

length of M_2 has to be large enough so that the output resistance of the modulator is much larger than the antenna resistance. Such choice ensures that only a negligible fraction of the power at the antenna goes to the modulator, as required for the correct operation of the transponder. C_{OUT} is the capacitance seen at the output of the modulator and is due to the interconnections, the antenna and the input capacitance of the other stages which the

modulator is connected to. The capacitance C_{IN} has to be larger than the gate-source and gate-drain capacitance of M_1, in order not to degrade the variation of the output capacitance of the modulator. Once the value of C_{IN} is chosen, the two transistors M_3 and M_4 of the inverter have to be dimensioned to fix the switching time of the varactor so that the channel bandwidth occupation of the backscattered signal complies with the requirements. The input V_{in} is from digital control block, the same as T_x as shown in Figure 6.

D. Clock generator

The clock generator circuit is based on RC relaxation oscillator [14]. The principle of operation of the circuit is shown in Figure 11. The capacitor C_{osc} charges when the output is low and discharges when the output is high.

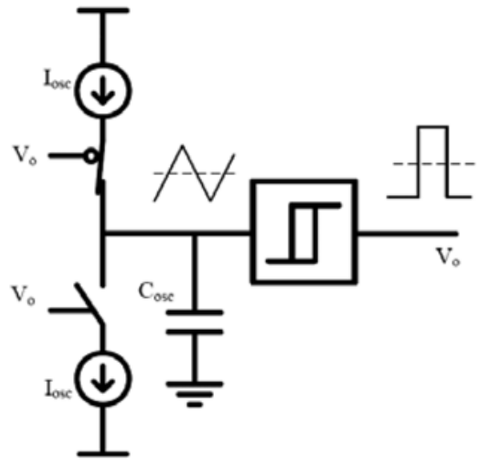

Fig. 11. Clock generation circuit [7]

3.2 Digital control block

The security of proposed secure low-cost RFID system depends largely on the digital control block of the RFID tags, which acts as an identification tag, carrying only the unique serial number and an ID number. The tag requires no secret key or PIN shared between tags and readers for authentication, thus eliminate the need of onerous work on key distribution and management.

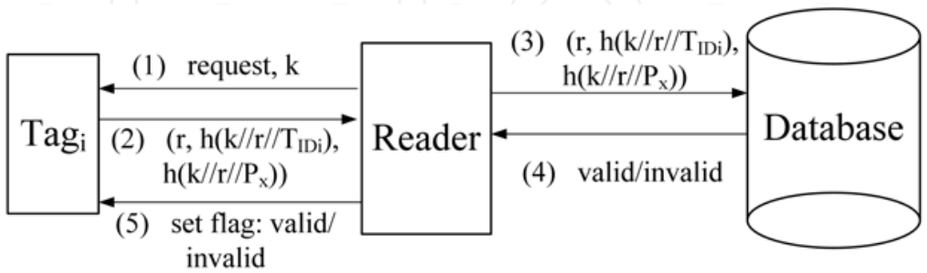

Fig. 12. Proposed Hash-block structure to enhance database searching efficiency and to prevent man-in-the-middle attacks.

The protocol is shown in Figure 12, the reader sends a random number "k" to tag_i at quering. Then tag_i generates a random number r and hashes it with random number k and the tag ID number "T_{IDi}"and P_x -- (r, h(k//r//T_{IDi}), h(k//r//P_x)), where // stands for

concatenation. The reader receives it and passes to the back-end database with the random number k -- (k, r, h(k//r//T_{IDi}), h(k//r//P_x)). The database then computes the hash using k, r, T_{IDi} and P_x. The calculated hash is compared to the received hash. When there is a match, the correct identification is confirmed. Then the database retrieves the information of the confirmed tag T_{IDi}.

This protocol effectively prevents man-in-the-middle attacks by having reader sends a random number first, which a rouge reader can not mimic without notice by a legitimate reader in the later communication.

The proposed tag has the following features. 1) The tag is passive. 2) The RFID system provides semi-duplex communication mode between the reader and the tag. 3) The RFID system adopts "ALOHA" anti-collision mechanism [8]. 4) The tag sends and receives signals in serial.

The order of signal receiving, handling and sending in tag digital control block is: decode received packet → checkout cyclic redundancy check (CRC) → handle command (generate random number, hash information, run anti-collision mechanism, read/write non-volatile memory) → add CRC → encode and send packet.

The hardware implementation of the proposed RFID tag is straightforward, consisting of a RF/analog front-end, a digital control block and a non-volatile memory. The architecture of the tag is demonstrated in Figure 13. The digital control block is the major and most important part of the chip, since it needs to implement anti-collision algorithm and authorization scheme, including a PIE (pulse interval encoding) down-link decoder, a up-link FM0 encoder, a slot-counter for ALOHA-based anti-collision, a random-number generator (RNG) for slot-counter and hashing, a command handler as the central controller, and an Hash block [9-10].

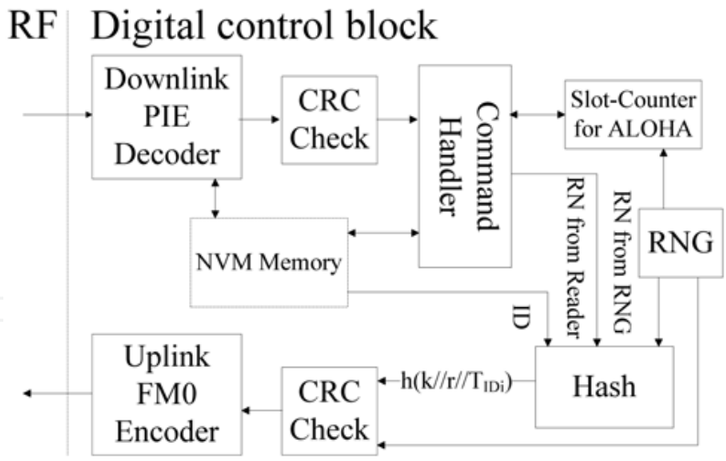

Fig. 13. Architecture of the tag digital control block

4. Reader implementation

An UHF RFID reader's structure is shown as Figure 14 [12]. From the function modules, UHF RFID reader consists of RF module and base-band module. It also consists of control part, transmission part and inception part. The transmission part and inception part can be known as RF module. The reader also includes I/O interface module and application program.

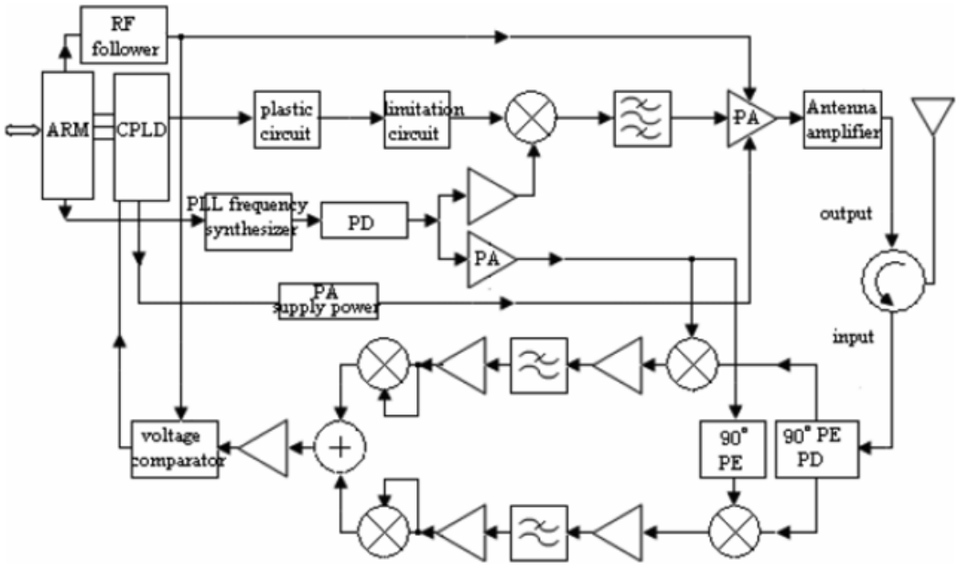

Fig. 14. UHF RFID Reader's structure [12]

4.1 Transmission part

Working flow of transmission part is shown as following:

1. The ARM Micro-controller receives operation commands from the computer, starts up application program and sends corresponding operation commands to the CPLD circuit.
2. The CPLD circuit forms base band signals to send to the plastic circuit and the limitation circuit to deal according to operation commands from the ARM Micro-controller. Then it sends the dealt signal to the mixer.
3. The mixer mixes the base band signal from the CPLD circuit and the LO signal and does ASK modulation.
4. The modulated signal is filtered by the filter, is amplified by the power amplifier, is amplified by the antenna amplifier and forms the final transmission signal.
5. The circulator sends the power signal from the antenna amplifier to the tag.

In that the frequency control of the LO signal created by the frequency synthesizer, setting the modulation depth, gain control of the power amplifier are made by ARM microcontroller according to communication protocols and system's working conditions.

4.2 Inception part

Working flow of inception part is shown as following:

1. After receiving the signal from the reader, the tag gets some energy and is activated. The tag starts up to perform the reader's command and sends the returned response information to the antenna of the reader in the way of the backscatter modulation.
2. After the antenna receives the signal, the circulator sends the signal returned from the tag to 90°phase-excursion power divider to split the signal into two orthogonal ways. These two signals are sent to two ways same demodulation circuits to deal. Two ways signals mixes with two orthogonal LO signals respectively. Mixed signals are amplified by the amplifiers, filtered by the filters and amplified again and sent to the multipliers to deal. The multiplier makes the sent signal squared to make pulse signals from the negative polarity into the positive polarity.

3. The signals dealt by the two demodulation circuits are amplified again after they add together. Then they are sent to the voltage comparator after passing the capacitor coupling.
4. The voltage comparator compares the voltage of the complete amplified modulated signal with the set norm voltage, forms base band signal returned from the tag, coordinates the signal and sends the signal to the CPLD circuit.
5. The CPLD circuit decodes the received base-band signal, does CRC check, forms the information about the tag ID and sends the information the ARM micro-controller.
6. The ARM micro-controller deals the received information about the tag ID. In these circuits, in order to ensure the accuracy of the demodulation circuit, use the amplifier to create the exactly 2.5 V virtual ground voltages as the middle voltage of the circuits such as the amplifier and the multiplier to use to ensure the stability of the inception circuit.

4.3 Main-control part

The main control of the system governs system parts to work in phase and realizes anti-collision control function. Its structure is shown as Figure 15. The control part of UHF RFID reader mainly realizes following functions: (1) communication with application software of the computer and execute the commands from the
application system software; (2) complete quick real-time communication with tags; (3) the coding and the decoding of signals;(4) in some complex system, control part also executes anti-collision arithmetic; (5) encrypt and decrypt the transmitted data between tags and the reader, do ID validation between tags and the reader. Data exchange between control part and application software is done mainly by the communication interface of the reader. The interface can adopt RS-232 or RS-485. It also can adopt RJ45 or WLAN interface.

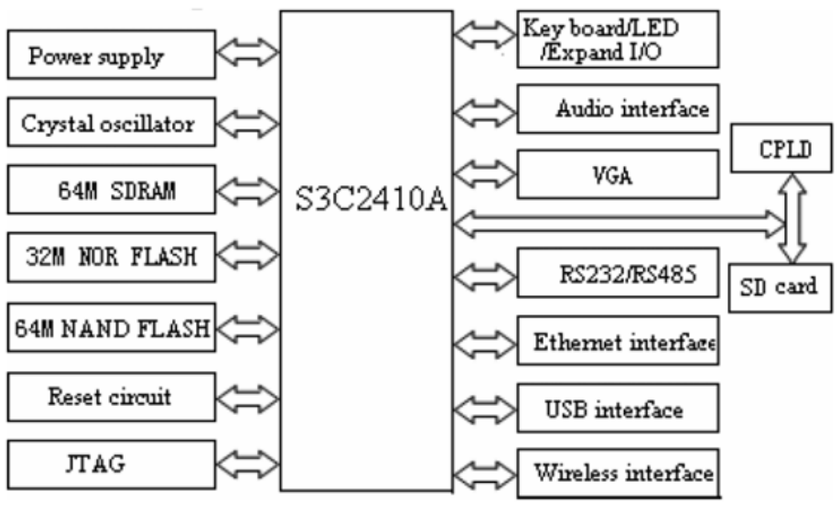

Fig. 15. Principle diagram of the main control part [12]

5. Single-chip reader implementation

To meet the demands of longer battery life and lower cost of mobile communication devices, the low-cost, low-power, single-chip reader draws great attention and thus the CMOS

technology is believed to be the most promising candidate toward the system-on-a-chip (SoC), which integrates all the functions of a RF transceiver, data converters, a digital baseband modem, an MPU, memory, and host interfaces [13].
Figure 16 illustrates the block diagram of the single-chip RFID reader. Baseband modulator and demodulator are implemented in hardware logic. Most of the other digital functionalities are implemented in software to support multi-protocols and flexibility.

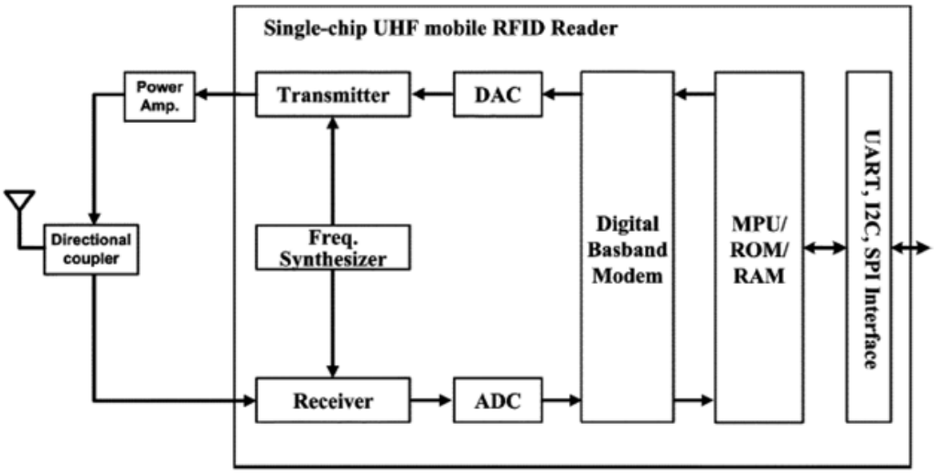

Fig. 16. Block diagram of the single-chip mobile RFID reader.

Figure 17 illustrates the receiver architecture of the RF transceiver. Among the various receiver architectures, the direct conversion receiver is adopted due to the backscattering communication solution. In the direct conversion receiver architecture, the transmitter carrier leakage to the receiver input is directly down-converted to DC. It can be removed by the DC offset cancellation (DCOC) feedback loop. However, the large transmitter carrier leakage leads to the saturation of the receiver RF front-end block. Hence, the low-noise amplifier (LNA) is bypassed in the backscatter detection mode for high P1dB characteristics to cope with very large transmitter carrier leakage.

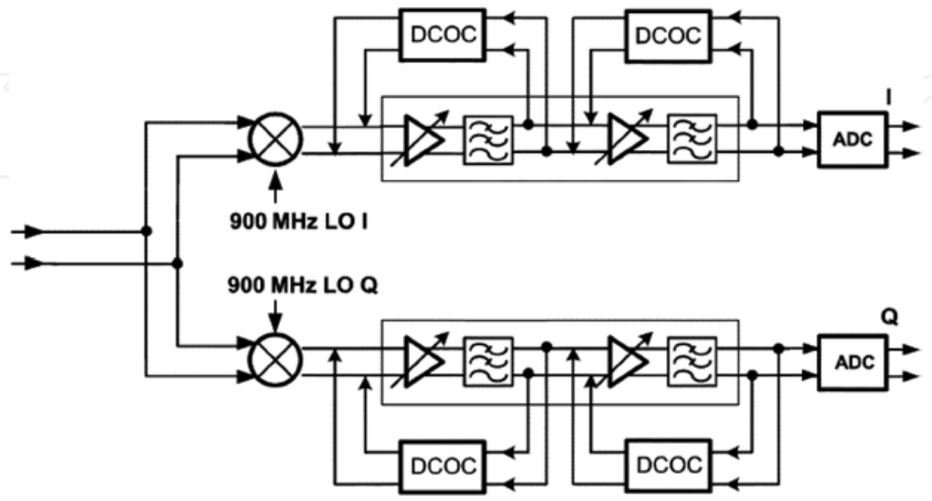

Fig. 17. Receiver architecture

The transmitter is implemented in the direct up-conversion architecture as illustrated in Figure 18. Baseband signals are transmitted to digital-to-analog converters (DACs) followed by the low-pass filters. Two identical mixers up-convert the baseband quadrature signals directly to the 900 MHz band, which is combined by current summing at the output. The transmitter supports both the SSB and the DSB modulation for the reader-to-tag communications and sends an unmodulated carrier for the tag-to-reader communications. In the DSB-ASK transmission, baseband signal is tied zero. In the SSB-ASK transmission, baseband signal is generated by the Hilbert transformer from the baseband signal. For generating 900 MHz LO signals with 200 and 500 kHz channel spacing, a frequency synthesizer based on a fractional-*N* phase-locked loop (PLL) derived from a 19.2 MHz crystal is implemented. A 1.8 GHz LO signal is generated by an integrated voltage-controlled oscillator (VCO) in the PLL and then the 900 MHz differential LO signals are obtained by a divide-by-two circuit.

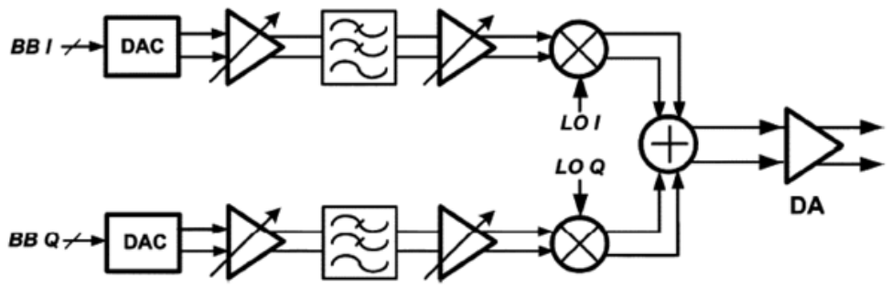

Fig. 18. Transmitter architecture

This single-chip UHF RFID reader for mobile phone applications has been implemented in a 0.18 m CMOS technology. It integrates an RF transceiver, data converters, a digital baseband modem, an MPU, memory, and host interfaces. Its die area is 4.5 mm x 5.3 mm including ESD I/O pads. The reader consumes a total current of 89 mA except external power amplifier with the 1.8 V supply voltage. The direct conversion RF transceiver architecture with the highly linear RF front-end circuit and DCOC circuit is used. It is suitable for the mobile phone reader with single-antenna architecture and low-power reader solution.

6. Reference

[1] Jin Li, Cheng Tao, "Analysis and Simulation of UHF RFID System", in proceedings of the 8th International Conference on Signal Processing, 2006.

[2] EPC™ Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz~960 MHz Version 1.0.9.

[3] Texas Instruments Proprietary Information, "UHF Gen 2. System Overview", 2005. http://rfidusa.com/superstore/pdf/UHF_System_Overview.pdf

[4] A. Ashry, K. Sharaf, "Ultra Low Power UHF RFID Tag in 0.13µm CMOS", in proceedings of International Conference on Microelectronics (ICM 2007), 2007.

[5] Department of Electronic & Computer Engineering, Chinese University of Hong Kong, "Single-Chip Passive UHF RFID Tags and Readers", 2005. http://www.ece.ust.hk /~rfid/phase1/power.htm

[6] N. Tran, B. Lee, JW. Lee, "Development of Long-Range UHF-band RFID Tag chip Using Schottky Diodes in Standard CMOS Technology", in proceedings of Radio Frequency Integrated Circuits (RFIC) Symposium, 2007.
[7] A. Facen, A. Facen, "A CMOS Analog Frontend for a Passive UHF RFID Tag", in proceedings of the 2006 international symposium on Low power electronics and design, 2006.
[8] EPC radio-frequency identi_cation protocols class-1 generation-2 RFID protocol for communications at 860 MHz-960 MHz Version 1.0.8.. EPCglobal, Dec. 2004.
[9] J. Wang, H. Li, F. Yu, "Design of Secure and Low-Cost RFID Tag Baseband", in proceedings of International Conference on Wireless Communications, Networking and Mobile Computing (WiCom), 2007.
[10] H. Li, F. Yu, Y. Hu, "A Solution to Privacy Issues in RFID Item-level application", in proceedings of IEEE International Conference on Integration Technology (ICIT), 2007.
[11] G. De Vita, G. Iannaccone, "Design criteria for the RF section of UHF and microwave passive RFID transponders", IEEE Transactions on Microwave Theory and Techniques, Vol. 53, pp. 2978 - 2990, 2005.
[12] W. Xiaohua, Z. Xiaoguang, S. Baisheng, "Design for UHF RFID Reader and Selection for Key Parts", in proceedings of 2007 2007 IEEE International Conference onAutomation and Logistics.
[13] I. Kwon, Y. Eo, H. Bang et al, "A Single-Chip CMOS Transceiver for UHF Mobile RFID Reader", IEEE Journal of Solid-State Circuits, Vol. 43, pp. 729-738, 2007.
[14] United States Government Accountability Office, "INFORMATON SECURITY: Radio Frequency Identification Technology in the Federal Government", 2005.

Development and Implementation of RFID Technology

Edited by Cristina Turcu

ISBN 978-3-902613-54-7
Hard cover, 450 pages
Publisher I-Tech Education and Publishing
Published online 01, January, 2009
Published in print edition January, 2009

The book generously covers a wide range of aspects and issues related to RFID systems, namely the design of RFID antennas, RFID readers and the variety of tags (e.g. UHF tags for sensing applications, surface acoustic wave RFID tags, smart RFID tags), complex RFID systems, security and privacy issues in RFID applications, as well as the selection of encryption algorithms. The book offers new insights, solutions and ideas for the design of efficient RFID architectures and applications. While not pretending to be comprehensive, its wide coverage may be appropriate not only for RFID novices but also for experienced technical professionals and RFID aficionados.

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821

IntechOpen