AUTO–ID LABS

A Mutual Authentication Protocol for RFID Using IDEA

Dan Liu (Fudan University),
Yuqing Yang (Fudan University),
Junyu Wang (Fudan University),
Hao Min (Fudan University)

Auto-ID Labs White Paper WP-HARDWARE-048

March 2009

***Keywords**: Authentication, IDEA, protocol, data link*

Dan Liu
Master Student
Auto-id Lab in Fudan University, China.
Email: liudan@fudan.edu.cn

Yuqing Yang
Doctorate Student
Auto-id Lab in Fudan University, China
Email: yqyang@fudan.edu.cn

Junyu Wang
Associate Director of Auto-id Lab in Fudan University, China
Email: junyuwang@fudan.edu.cn

Hao MIn
Director of Auto-id Lab in Fudan University, China
Email: hmin@fudan.edu.cn

Contact:

Contact Address: 825 Zhangheng Rd, Zhangjiang High-Tech Park, Shanghai 201203, China
Phone/fax: +86-02151355188
Email: liudan@fudan.edu.cn
Website: http://www.autoidlab.fudan.edu.cn

Hardware

Index

Abstract

A security enhanced tag developed by Fudan University is introduced in this paper. This tag is designed to be compatible with EPC Class 1 Generation 2 protocol (EPC C1G2), and can be extended to support mutual authentication and to encrypt communication between reader and tag. A mutual authentication scheme is proposed, and low cost cryptographic algorithm core is implemented in the tag to accomplish authentication and encrypted data exchange, in order to resist the tracing attack and common attacks. A whole tag chip, including RF/analog front end, digital core and EEPROM, has been taped out on SMIC 0.18 μm process.

This paper is organized as follows. Section 2 describes the proposed mutual authentication scheme. Section 3 compares some popular cryptographic algorithms from the perspective of cost, efficiency and security, and also introduces the chosen algorithm in this paper, International Data Encryption Algorithm (IDEA). Section 4 presents the data ciphering mode between reader and tag adopted in our design, i.e. the Output Feedback Mode (OFB). Section 5 gives more details about the secure tag, including the architecture and implementation of both RF/analog front end and the digital baseband core. The rest parts of this paper are the summary and the future works.

1 Related Work

Although RFID systems may emerge as one of the most pervasive computing technologies in history, there are still a vast number of problems that need to be solved before their massive deployment. One of the fundamental issues still to be addressed is privacy, which concludes association threat, location threat, preference threat, constellation threat, transaction threat, action threat and breadcrumb threat (Kim, J., Yang, C, Jeon, J, 2007).Misbehaviors of both readers and tags will lead to attacks to the system. The common attacks on the readers, tags and the air interface between them comprise: Tracking or Tracing, Tamper, Clandestine scanning, Counterfeit tags, Cloning tags, Eavesdropping, Replay, man-in-the-middle attack, Spoofing, Differential power analysis, Timing Attacks, Denial of Service, Physical Attacking and so on (P. Cuenca and L. Orozco-Barbosa, 2006.), (Kim, J., Yang, C, Jeon, J, 2007).

Several mechanisms have been proposed to solve the security and privacy issue of RFID systems. In some early papers, many simple solutions have been proposed to defend the tracing attack and clandestine scanning attack, e.g. “Killing" and "Sleeping" Command (A. Juels, R. L. Rivest, and M. Szydlo, 2003), Tag Password (Y. Xiao, X. Shen, B. Sun, and L. Cai, 2006), Blocking Tag (A. Juels, R. L. Rivest, and M. Szydlo, 2003). Then several light weight protocols for RFID tags are published, e.g. Tag Pseudonyms (S. A. Weis, 2005), PRF based authentication (D. Molnar, and D. Wagner, 2004), Non-Cryptographic Primitives (I.Vajda, Buttyan, 2003), HB (S. A. Weis, 2005), HB+ and HB++ (Julien Bringer, Hervé

Chabanne, Emmanuelle Dottax, 2006). Since the simple solutions can only solve the tracing attack and the security of the light weight protocols designed for RFID tags mentioned above is not clear, classic cryptography based authentication schemes have been developed. A simple two-way challenge-response algorithm based on AES is proposed by (Feldhofer et al. 2004). However, the key search problem dose not been mentioned. The researches on the implementation of public key encryption algorithms for RFID applications, e.g.ECC(Daniel HEIN, Johannes WOLKERSTORFER, Norbert FELBER, 2008), (Sandeep Kumar, 2006), (J. Wolkerstorfer, 2005), NTRU (Ali ATICI, Lejla BATINA, Benedikt GIERLICHS, Ingrid VERBAUWHEDE, 2008), are also published.

Considering the limitations of the simple solutions and light weight protocols, and the key search problem of the symmetry crypto based protocol, a novel symmetry crypto based mutual authentication protocol, combined with key search and update, is proposed and implemented in this paper.

2 Authentication Scheme

An authentication scheme to solve the RFID security and privacy issues is proposed in this section. The scheme includes key searching, mutual authentication and key/ID updating, which can resists most attacks between reader and tag including tracing, tracking, cloning, counterfeiting and eavesdropping (Juels, 2006). Reader finds the key for authentication of a specific tag through the temporary ID from the tag called metaID as index in the database. A 3-pass mutual authentication verifies both reader and tag. After a successful mutual authentication the authentication key and metaID for tag are updated by the reader, which provides the forward security for the system.

It is assumed that there is a key table for each tag in data base, which is only available for the valid reader. The key table is comprised of a metaID (the index of the key table) and a Ka (the content of the current authentication key). Only those principals possessing the same (metaID, Ka) pair can pass the mutual authentication. Readers need to be initialized by loading a copy of key table.

The illustration of the proposed scheme procedure between RFID Reader and Tag is shown in Figure 1. The procedure is described below. In this part, the following operators and variables are used:

$E_K(X)$: Conventional encryption result of plaintext X with K as the key. It is assumed that;

$D_K(X)$: Conventional decryption result of ciphertext X with K as the key;

||: Conjunction of two or more messages;

$H(X)$: one way function;

$\oplus$: Exclusive OR operation;

R_1: Random number generated by Reader to verify Tag;

R_2: Random number generated by Tag to verify Reader, is used as the key for data ciphering after authentication;

R_3: Random number generated by Reader as the new authentication key for Tag;

K^i_{authen},metaID$_i$: the current authentication key and ID of Tag;

K^{i+1}_{authen},metaID$_{i+1}$: the new authentication key and ID of Tag generated by Reader;

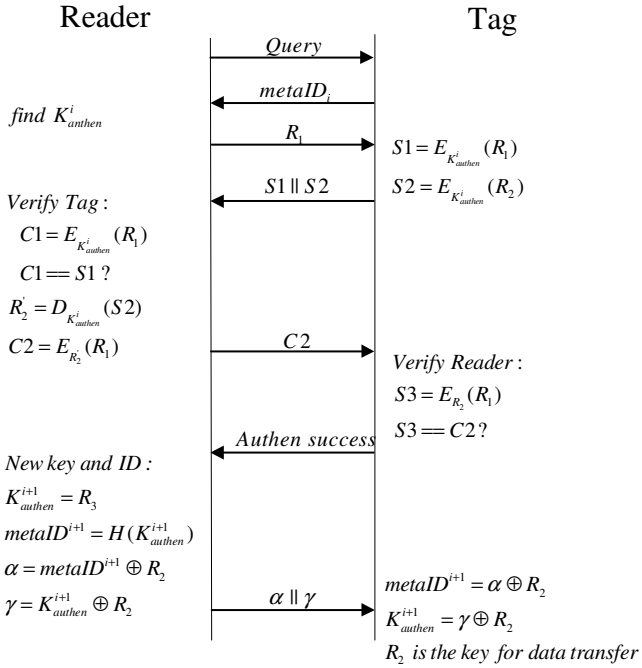

Fig. 1: The proposed mutual authentication procedures.

(1) Reader requires ID of tag by issuing Query.

(2) Tag returns its ***metaID$_i$***.

(3) Reader generates a random number ***R_1*** and sends it to tag. Reader finds the corresponding ***K^i_{authen}*** with the received ***metaID$_i$*** as index.

(4) Tag encrypts ***R_1*** with ***K^i_{authen}***; and generates a random number ***R_2***, encrypts ***R_2*** with ***K^i_{authen}***; backscatters the cipher text {***S1***//***S2***} to reader.

(5) Reader get received {***S1***//***S2***}. Reader verifies tag by checking ***$E_{K^i_{authen}}$*** (***R_1***)==***S1***.If equal, the authentication process continues, otherwise fails. If tag is valid, reader decrypts ***S2*** with ***K^i_{authen}*** to get ***R_2***from tag and encrypt ***R_1*** with ***R_2***. Finally reader sends the cipher text ***C2*** to tag.

(6) Tag verifies reader by checking ***E_{R2}*** (***R_1***)==***C2***.If equal, the authentication process continues, otherwise fails. If the reader is valid, tag returns "***authen sucess***" to reader.

(7) Reader generates a random number ***R_3*** as the new authentication key ***K^{i+1}_{authen}*** for the present tag and computes the corresponding new metaID by ***metaID$_{i+1}$=H(K^{i+1}_{authen})***. ***R_3*** must be carefully chosen to guarantee that the random number is unique. Reader

exclusive OR the new (***metaID***$_{i+1}$, ***K***$^{i+1}_{authen}$) pair with ***R***$_2$ respectively and send them to tag.

(8) Tag receives the messages and get the new (***metaID***$_{i+1}$, ***K***$^{i+1}_{authen}$) pair by exclusive-OR operation with ***R***$_2$. Tag updates the metaID and authentication key. And tag sends an "***Update success***" to reader.

(9) Reader receives the "***Update success***" message and replace the old (***metaID***$_i$, ***K***$^1_{authen}$) pair with the new (***metaID***$_{i+1}$, ***K***$^{i+1}_{authen}$) pair.

(10) ***R2*** will be used as the key to encrypt the data exchanged between reader and tag after the successful authentication.

After a successful authentication, reader and tag can exchange data via a ciphered channel.

3 Encryption Algorithm

Since the performance of Cryptographic algorithms directly affect the performance of secure tag, it is important to choose a suitable cryptographic algorithm, where "suitable" means that the algorithm should provide sufficient security, and must have the ability to complete operation at the required time, with no more size and power than passive tag can afford.

When the cost of a passive RFID tag is 5 cents (the silicon will cost roughly 2.5 cents), the size of the die can be calculated according to the following equation.

$$Die = \frac{wafer\_cost}{Die\_number * Die\_yield}$$

When taped out by 0.18μm technology, the chip cost an area of about 0.6mm, which can provide about 13K equivalent gats for the digital baseband. That is to say, only about 5K gates can be used for the secure module.

The incident power can be calculated according to the following equation:

$$P_D = kP_t \frac{G_t G_r \lambda^2}{(4\pi R)^2}$$

When the reading range is 5 m, a typical range of the UHF RFID system, the power for a passive tag is about 5.3μ*W*. According to ISO 18000-6C, the response time for tags to reader's command is defined as the parameter *T1*, which can be calculated as:

$$\max\{\frac{10}{BLF}, RTcal\} \times (1-FT) - 2\mu s \le T_1 \le \max\{\frac{10}{BLF}, RTcal\} \times (1+FT) + 2\mu s .$$

When the back scatted link frequency is 40K, the response time T1 is about 262 μs.

There are many popular symmetrical crypto algorithms, e.g. DES, AES, TEA, IDEA, RC5, LFSR (stream cipher) and so on, and asymmetrical crypto algorithms, e.g. ECC, RSA. In

recent years, there are some efforts on the implementation of ECC for RFID tags (Sandeep Kumar, 2006),(J. Wolkerstorfer, 2005), (L.Batina, J. Guajardo. et al, 2007). Unfortunately, the results show that ECC is still not suitable for passive RFID tags.

Security (bits)	Symmetric Encryption Algorithm	Hash Algorithm	Mini Size of Public keys (bits)		
			DSA/DH	RSA	ECC
80	---	SHA-1	1024	1024	160
112	3DES	---	2048	2048	224
128	AES-128	SHA-256	3072	3072	256
192	AES-192	SHA-384	7680	7680	384

Table 1: NIST Guidelines for the equivalent strengths of various cryptographic algorithms

]

Encryption Algorithm	Key (bit)	Plaintext (bit)	Cycles required	Equipment Gates Num.	Average Power	technology (um)
AES(Martin Feldhofer ,2004)	128	128	1016	3595	8.15uA	0.35
TEA(P.Israsena ,2006)	128	64	64	2355	12.34uW	0.18
Hash (SHA-1) (J.-P. Kaps, 2006)	/	192(in) 160(out)	405	4276	26.73 uW (1.2V)	0.13
Stream-cipher (1 LFSR)	Random num width (max: 32)	64	92	685	0.1582 uW	0.18
DES(Axel Poschmann, 2006)	56	64	144	2309	2.14uW	0.18
ECC (without extra register) (Sandeep Kumar, 2006)	Field=113	/	195159	About 10K	/	0.35

ECC(J. Wolkerstorfer, 2005)	GF(2^191)	/	>175K	About 350K (0.35mm^2)	30uW	0.18
IDEA (our work)	128	64	320	4660	3uW	0.18

Table 2: performance of some popular cryptographic algorithm

Generally speaking, the security of symmetrical crypto algorithm is determined by its key length. But different algorithms in the same security level have different key length and plaintext data width. National Institute of Standards and Technology (NIST, USA) recommends the different crypto-key length according to alternative algorithms in the same security level, which is shown in Table 1. The 128 bit crypto-key is considered to have enough security (Arjen K. 2001).

The performance of several popular cryptographic algorithms for RFID application is given in table 2, which shows that International Data Encryption Algorithm (IDEA) is a good choice considering the tradeoffs between security strength and hardware cost. IDEA is considered as one of the most important post-DES cryptographic algorithms, due to its high immunity to attacks (A. Tanenbaum., 1997).

The key and plaintext of IDEA are 128 bits and 64 bits respectively and it has 8 crypto rounds and an output round. Figure 2 illustrates the round operation of IDEA, each of which consists of Modular Multiplication operation by 4 times, addition operation by 4 times and XOR operation by 6 times. **X1**, **X2**, **X3**, **X4** and **Y1**, **Y2**, **Y3**, **Y4** are the input and output of each round calculation. $\mathbf{K^i_1}$, $\mathbf{K^i_2}$, $\mathbf{K^i_3}$, $\mathbf{K^i_4}$, $\mathbf{K^i_5}$ and $\mathbf{K^i_6}$ are the sub-key for the ***ith*** round calculation. All variables are 16 bit.

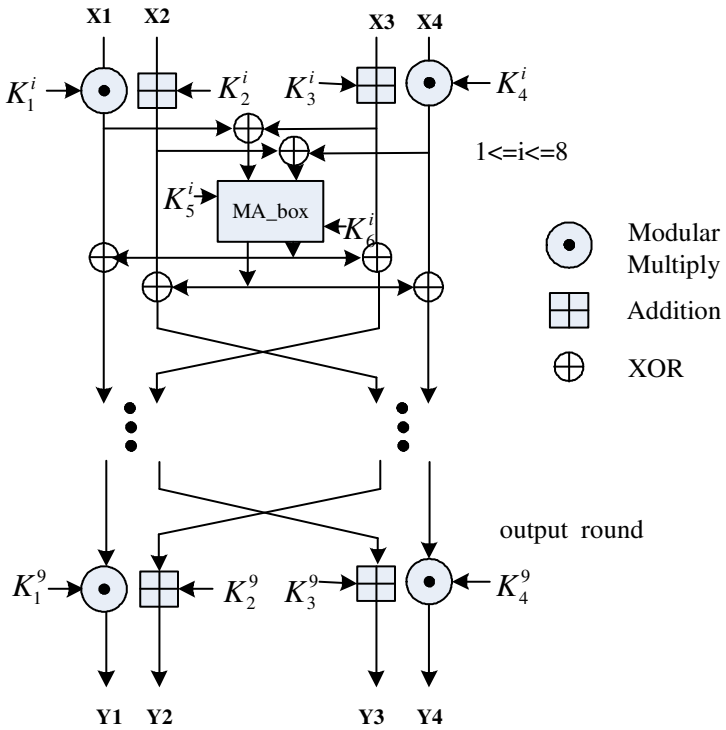

Fig. 2: The round operations of IDEA.

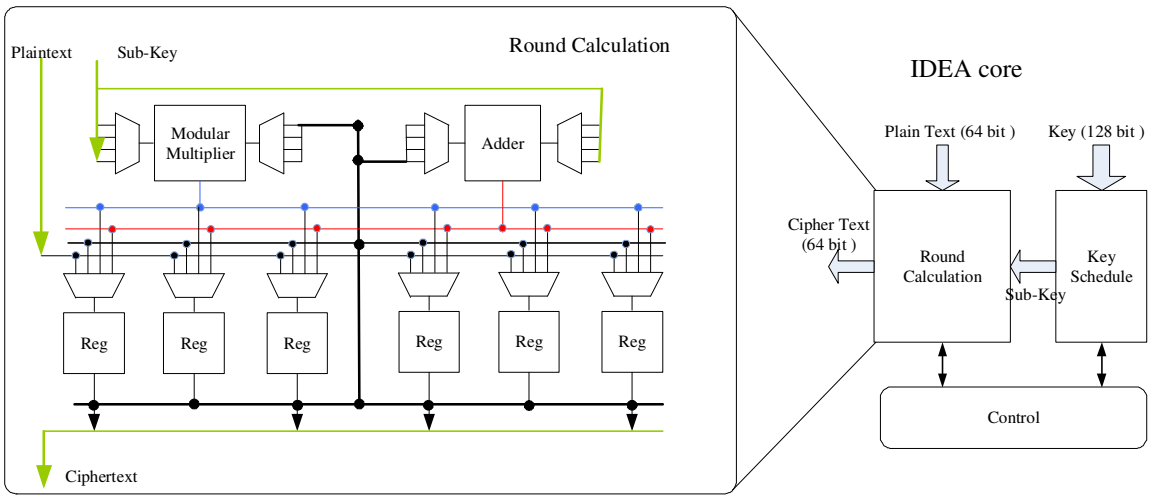

Fig. 3: The architecture of the IDEA core.

The architecture of IDEA core is shown in Figure 3. It consists of the Round Calculate module, the Key Schedule module and the Control module.

(1) Round Calculate module: completes all round operations and produces the ciphertext. A serial architecture, which only uses a single 16-bit Modular Multiplier and a single 16-bit Adder, is designed to reduce area and power of IDEA core. In order to reduce chip area, a 8 bit*8 bit booth multiplier is designed for the 16-bit Modular Multiplier.

(2) Key Schedule module: computes the sub-keys for each round.

(3) Control module: control the Round Calculate module and the Key Schedule module.

This core consumes about 4660 equivalent gates and can output 64 bit cipher text per 320 cycles. The average power is about 3uW on SMIC 0.18um process when the supply voltage is 1.8v.

4 Data Link Encryption

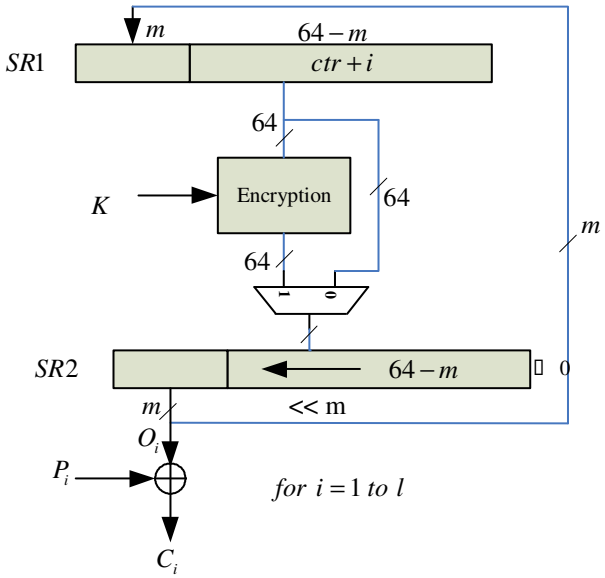

Fig. 4: The Output Feedback Mode (OFB) of the block cipher

When a secure channel is established after a successful authentication, reader and tag can exchange data via the channel. A stream cipher algorithm is usually adopted to encrypt the data between two communicating principals since the length of the data exchanged is unexpected. In order to reduce the cost of tag, the block cipher module used in the authentication procedure is also used to encrypt the data exchanged between reader and tag. The Output Feedback Mode (OFB) (H. Lipmaa, 2000) of the block cipher is used to encrypt the data which has unfixed length of message.

The illustration of the encrypt flow used Output Feedback Mode (OFB) by Tag or Reader is shown in Figure 4. The procedures are described below. In this part, the following operators and variables are used:

m**:* the minimum bits that can be encrypted or decrypted at a time. C_i, P_i and O_i. are m bit of the ciphertext, plaintext and the Feedback Output respectively. Each *m* bits of plaintext is called a minimum plaintext unit. In our example ***m is 16.

ctr: (64-***m***=64-16=32) bit, the initial value to be loaded into the least significant 32 bit of ***SR1***. It should be the same for both tag and reader and determined in advance.

SR1: the shift register which is 64 bit in our example. The initial value of ***SR1*** is {***r***||***ctr***}.

SR2: the shift register which is 64 bit in our example.

r: ***m***=16 bit, the initial value to be loaded into the most significant ***m*** bit of ***SR1***.

l: represents the count of words of the plaintext.

K: the key used to encrypt data and is fixed for a whole communication session between tag and reader but is random for different sessions. The key should be the same for both tag and reader and determined in advance.

$E_K(X)$: Conventional encryption result of plaintext X with K as the key.

$\oplus$: Exclusive OR operation;

R<<m: left shift the variable ***R*** by ***m*** bit and 0 is used to fill the least significant ***m*** of ***R***.

//: Conjunction of two or more messages;

shiftcounter: a counter with the initial value of 0 .

(1) If ***shiftcounter*** == (64/ ***m*** =64/16=4), ***shiftcounter*** is set to 0 and ***SR2***=E_K(***SR1***); else ***shiftcounter*** = ***shiftcounter*** +1;

(2) ***Oi*** = ***SR2***[63:48] and ***SR2*** = ***SR2<<16***;

(3) ***Ci*** = ***Pi*** $\oplus$ ***Oi***.

(4) If ***Pi*** is the last minimum plaintext unit then OFB is done; else go to (5);

(5) ***SR1*** = {***Oi*** || ***ctr*** + i}. Go to (1).

The advantages of the proposed OFB lie in:

(1) It can share the block cipher module with the authentication procedure thus reduce the cost of tag;

(2) It's flexible because ***m*** and the length of ***SR1***, ***SR2*** are programmable.

(3) It's faster to encrypt data since multiple bit can be encrypted at a time whereas stream cipher only encrypts one bit each time.

5 Tag Architecture

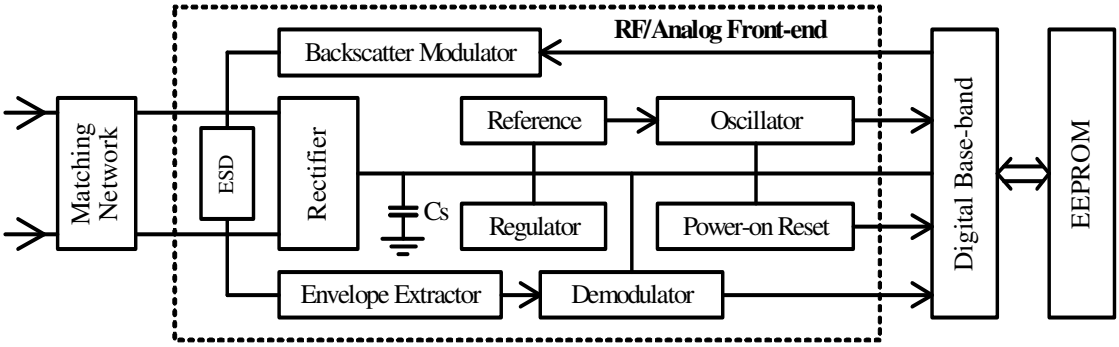

Fig. 5: Tag architecture.

Figure 5 depicts the architecture of our tag, where the circuit in the dotted line frame represents the RF/analog front-end. The circuit derives its power supply by rectifying the interrogating RF energy. A low voltage reference generator provides voltage and current references for the whole system. System clock is generated by a current controlled ring oscillator (Han Yifeng, 2005). The forward link data are demodulated from the extracted envelope of the carrier (Zhu Zheng, 2004). They are sent to the digital base-band for signal process with the clock and power-on reset signals. Backward modulation is achieved by utilizing the backscatter mechanism. According to the input FM0 coded signal, the backscatter modulator changes the input impedance of the tag to cause simultaneous phase-shift keying (PSK) and amplitude-shift keying (ASK) modulation of the backscattered electromagnetic wave. An energy storage capacitor C_S is employed to supply the chip in case of the interrogating energy gap.

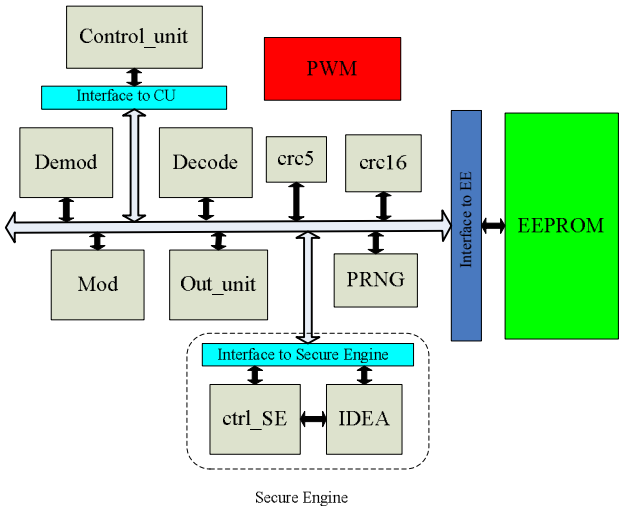

Fig. 6: The digital baseband core architecture.

The tag has two modes, C1G2 standard mode and security enhanced mode, which is optional to customers by programming the memory of tag. Tag in the C1G2 standard mode

supports 8 most frequently used EPC C1G2 commands and supports 5 more custom commands in the security enhanced mode. This chip can achieve the authentication protocol introduced in section 2 and ciphered communication with Readers using OFB.

The architecture of the baseband is shown in Figure 6. In this architecture the Finite State Machine (FSM) based control unit is used to take charge of control and data processing. Periphery modules are mostly used to do coding and decoding. Data received from analog front end is firstly demodulated ("Demod") and decoded ("Decode"). When the received data is verified by the CRC modules, Data from the PRNG module or the EEPROM module are controlled by the output control module ("Out_unit"), will be coded to FM0 or Miller code and sent to the analog front end (module "CRC" and "modu" involved).

The control unit also takes charge of the authentication process in the security enhanced mode. The security for both authentication and data ciphering is provided by the secure engine, which includes an IDEA core (IDEA) and a control module ("ctrl_SE"). The "ctrl_SE" decides the work mode of the IDEA core – the normal block cipher mode in authentication or the OFB mode in data exchange. The secure engine is only wake up in the security enhanced mode to decrease the power consumption.

All modules in this design work very independently, so it is easy to manage power in a higher level. Module level cloak-gating strategy is adopted. The power management module generates and gates clocks of every other module and the control unit does an accurate power control by controlling the switches in power management module.

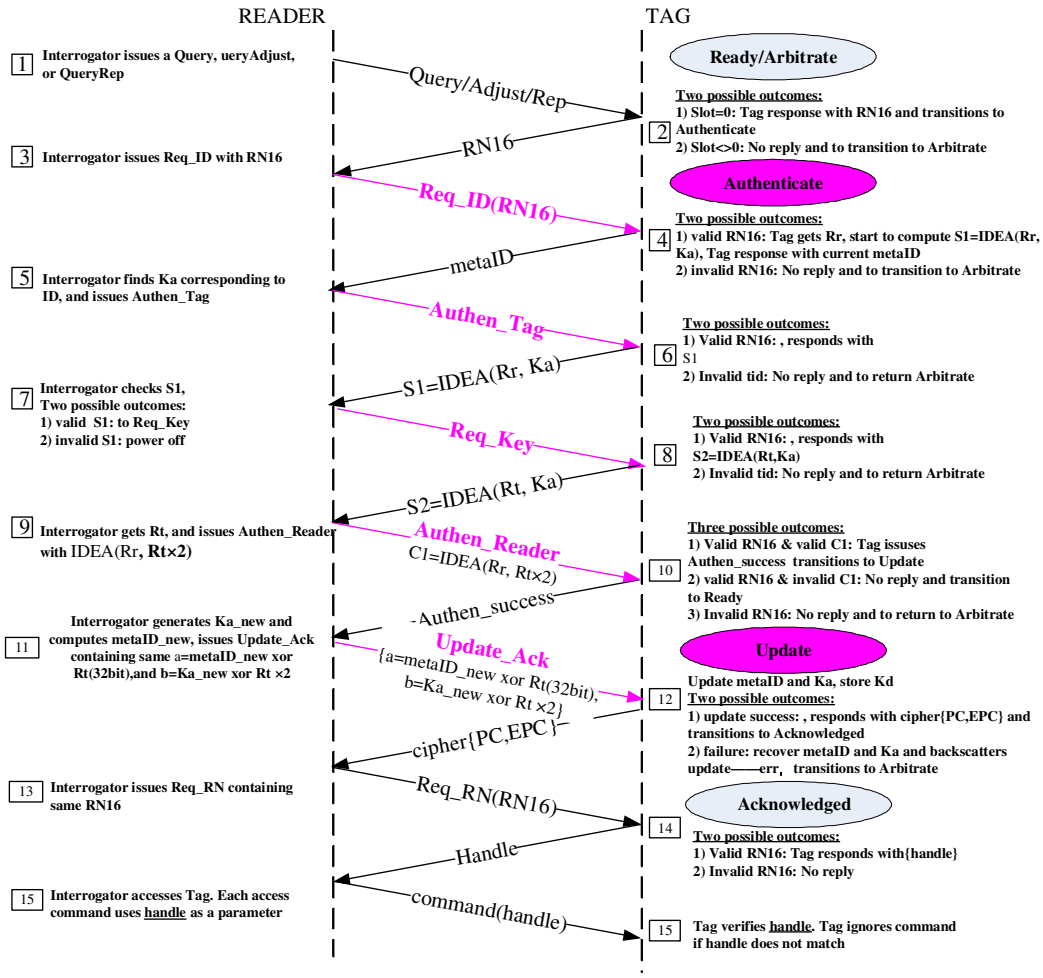

Fig. 7: The detailed protocol flow for the proposed authentication

The proposed protocol and the implementation of IDEA compatible with the ISO 18000-6C standard, which means the timing constraint in the specification. Compared to the standard ISO 18000-6C, two new states, Authenticate and Update, and five customized commands, Req_ID, Authen_Tag, Req_Key, Authen_Reader and Update_Ack, are defined (Fig. 7), which complete the mutual authentication and ID/Key update.

The RF/analog front end, digital baseband core and memory have been taped out in Nov. 2008 on SMIC 0.18um EE process. The whole chip area is 0.9mm *1.25mm (all memories included) and the cryptographic core consumes about 4000 equivalent gates. The specified operating frequency is 1.28 MHz. Fig.8 illustrates the simulation results of the two work mode, which shows that the tag can complete the whole authentication flow and the key update process in the secure mode, while it can work as a standard C1G2 tag in the other mode.

a) The protocol flow of the standard C1G2 Mode

b) The protocol flow of security enhanced Mode

Fig. 8: The simulation results of the tag

6 Summary

A new scheme for secure tag for RFID system, being implemented, is presented in this paper. The tag can not only communicate with EPC C1G2 Readers but also work in a higher security level, which contains mutual authentication and encrypted data exchange. Some cryptographic algorithms are analyzed and compared; International Data Encryption Algorithm (IDEA) is chosen to be used in low cost RFID tags. This tag can be applied in RFID systems where privacy and security are required. Additionally, other issues, including the key management and the synchronization problem (Sébastien CANARD, Iwen COISEL, 2008) between reader and tag when the key updating fails, will be the future work.

References

Kim, J., Yang, C, Jeon, J. (2007): A Research on Issues Related to RFID Security and Privacy, in IFIP International Federation for Information Processing, Volume 252, Integration and Innovation Orient to E-Society Volume 2, pp. 412-420, 2007.

P. Cuenca and L. Orozco-Barbosa (2006): RFID Systems: A Survey on Security Threats and Proposed Solutions, PWC 2006, LNCS 4217, pp. 159–170, 2006.

A. Juels, R. L. Rivest, and M. Szydlo, (2003):, The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy, Proceedings of the 8th ACM Conference on Computer and Communications Security, 2003, pp. 103-111.

Y. Xiao, X. Shen, B. Sun, and L. Cai, (2006):, Security and Privacy in RFID and Applications in Telemedicine, IEEE Communications Magazine, Vol. 44, No. 4, 2006, pp.64-72.

S. A. Weis, (2005):, Security Parallels Between People and Pervasive Devices, The 3rd IEEE Conference on Pervasive Computing and Communications Workshops-PERSEC'05, 2005, pp. 105-109.

D. Molnar, and D. Wagner (2004): Privacy and Security in Library RFID: Issues, Practices, and Architectures, Proceedings of the IV^ ACM Conference on Computer and Communications Security, 2004, pp. 210-219.

I. Vajda, and L. Buttyan (2003): Lightweight Authentication Protocols for Low-Cost RFID Tags, Proceedings of the 2nd Workshop on Security in Ubiquitous Computing, 2003, pp. 1-10.

S. A. Weis (2005), Security Parallels Between People and Pervasive Devices, The 3rd IEEE Conference on Pervasive Computing and Communications Workshops-PERSEC'05, 2005, pp. 105-109.

Julien Bringer , Hervé Chabanne , Emmanuelle Dottax (2006): HB++: a Lightweight Authentication Protocol Secure against Some Attacks, Proceedings of the Second International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing, p.28-33, June 29-29, 2006

Daniel HEIN, Johannes WOLKERSTORFER, Norbert FELBER, (2008): ECC is Ready for RFID - A Proof in Silicon, IAIK, TU Graz, Austria

Ali ATICI, Lejla BATINA, Benedikt GIERLICHS, Ingrid VERBAUWHEDE, (2008): Power analysis on NTRU implementations for RFIDs: First results, IAIK, TU Graz, Austria

Juels (2006): “A. RFID security and privacy: a research survey”, Selected Area in

Communications, IEEE Journal on Volume 24, Issue 2, Feb. 2006 Page(s):351-394

Arjen K (2001): Selecting Cryptographic Key Sizes. Cryptology, 14(4): 255-293, August 2001.

Martin Feldhofer (2004): strong Authentication for RFID Systems Using the AES Algorithm, Graz University, 2004

P. Israsena (2006): Securing Ubiquitous and Low-Cost RFID Using Tiny Encryption Algorithm, wireless Pervasive Computing, 2006 1st International Symposium on16-18 Jan.2006 Page(s):4pp.

J.-P. Kaps (2006): Energy comparison of AES and SHA-1 for ubiquitous computing, In E.Sha, editor, IFIP International Conference on Embedded and Ubiquitous Computing - EUC 2006, LNCS. Springer, 2006.

Axel Poschmann (2006): A Family of Light-Weight Block Ciphers Based on DES Suited for RFID Applications, Workshop on RFID Security, Graz, Austria, and July 2006.

Sandeep Kumar (2006): Are standards compliant elliptic curve cryptosystems feasible on RFID, Workshop on RFID Security 2006, Graz, Austria, July 2006.

L. Batina , J. Guajardo. et al (2007): Public-Key Cryptography for RFID-Tags, Fifth IEEE International Conference on Pervasive Computing and Communications Workshops (PerComW'07), pp. 217-222, March 2007

J. Wolkerstorfer (2005): Is Elliptic-Curve CryptographySuitable to Secure RFID Tags, Workshop on RFID and light-weirht Crypto, Graz, Austria, July 14th-15th 2005

A. Tanenbaum (1997): *Computer Networks*. 3rd Edition,Prentice Hall, Upper Saddle River, NJ, 1997

H. Lipmaa, P. Rogaway, D. Wagner (2000): Comments to NIST, concerning AES Modes of Operation: CTR-Mode Encryption, S mmetric Key Block Cipher Modes of Operation Workshop, 2000, available at: www.tcs.hut.fi/-helger/papers/lrwOO/html

Han Yifeng, Li Qiang, Min Hao (2005): A low voltage low power oscillator suitable for RFID transponder. Chinese Journal of Semiconductors, 2005, 26(4):775.

Zhu Zheng (2004): RFID analog front end design tutorial, Auto-ID Laboratory at University of Adelaide [Online], Jan. 2004. http://autoidlab.eleceng.adelaide.edu.au/Tutorial.html

Sébastien CANARD, Iwen COISEL,(2008): Data Synchronization in Privacy-Preserving RFID Authentication Schemes, RFIDSec08,