A Cross-Layer Solution to Improve Security and Privacy in RFID Systems

Anne Wei[†], Benoît Geller[††], GuoZhi Wei[†], Selma Boumerdassi[‡] and Éric Renault[‡‡]

[†] Université Paris XII, 61, Avenue du Général de Gaulle, 94010 Créteil Cedex, France
[††] SATIE – ENS Cachan, 61, Avenue du Président Wilson, 94235 Cachan Cedex, France
[‡] CNAM – CEDRIC, 292 rue Saint-Martin, 75003 Paris Cedex, France
[‡‡] GET / INT, 9 rue Charles Fourier, 91011 Évry Cedex, France

Summary
Due to advances in silicon manufacturing technology, Radio Frequency Identification (RFID) systems are useful in many applications such as automobile immobilizers, animal tracking, payment systems, automatic toll collection and inventory management. As RFID systems use both radio and wire communication, security issues become a critical concern. However, even if security and privacy solutions have been proposed for the past several years, a important study about transmission error influence on security solutions is still missing. Indeed, all radio communications depend upon error transmission rate, particularly for exchanged security messages. As a result, transmission errors can degrade the reliability and the stability of some security solutions. This paper first discusses some existing security proposals for RFID systems; then, it focuses on the influence of transmission errors on these security proposals. Finally, we suggest a novel cross-layer architecture designed to improve the reliability of security and privacy solutions.

Key words:
RFID, Cross-layer solution, Security and privacy, Transmission error effect.

Introduction

Due to tight integrated circuits equipped with radio antennas, Radio Frequency Identification (RFID) systems are suitable for many applications such as automobile immobilizers, animal tracking, payment systems, automatic toll collection and inventory management. For example, Delta Airlines together with the US Transportation Security Administration successfully performed a pilot project for using RFID tags for baggage handing at the airport of Jacksonville, Florida, USA [1]. Figure 1 presents a typical RFID system composed of three key elements (in referring to the Electronic Product Code (EPC) jointly developed by the Auto-ID Center and MIT):

- RFID tags carry object-identifying data.
- RFID readers read and write tag data.
- A database server stores both tag and reader data.

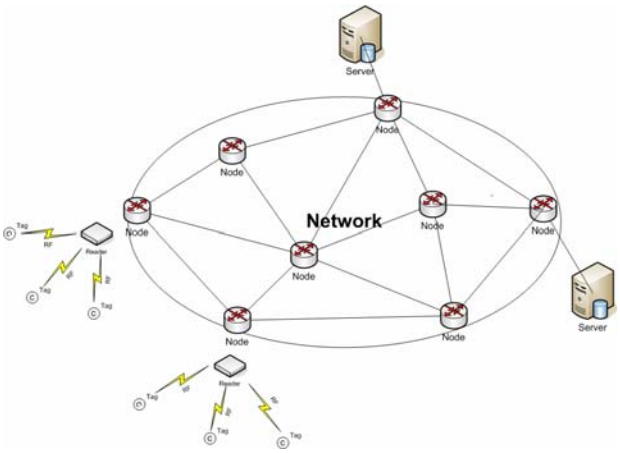


Fig. 1: RFID system architecture.

Basically, a reader broadcasts a radio frequency signal to get the data stored on the nearby tags. The data can be a static identification number, a user written data or a data computed by the tag. The database server can also access tag and reader data via a wire or wireless network. As critical information circulates in RFID systems, threats can take place in the tag-reader part, the reader-reader part or in the reader-server part. As a result, privacy and security become a key problem in RFID systems. For the past few years, some recent researches have focused on security solutions [3,4,5,6,7,8,9,10,11,12,13,14]. These security solutions are generally based on exchanged messages between two entities. However, the problem regarding exchanged messages involved by the transmission error rate is omitted. Indeed, without transmission performance estimation, several security solutions are not viable, even to be error-prone.

This paper focuses on an improvement of transmission performance in order to support better security and privacy solutions. We propose a novel cross-layer architecture to estimate the transmission error effect and to optimise radio transmission performance. The remainder of the paper is organised as follows: after a brief introduction to RFID systems, Sec. 2 presents existing RFID privacy and security solutions succinctly. Sec. 3 analyses the influence of transmission errors on these security solutions. Then,

Manuscript received May 5, 2006.
Manuscript revised May 25, 2006.

this study allows to propose a novel cross-layer architecture for RFID systems. This novel architecture is capable of improving transmission performance, reliability and stability of security solutions. Sec. 5 concludes the paper.

2. RFID Privacy and Existing Solutions

2.1 RFID Systems

RFID systems have been first used during the Second World War to identify friend military aircraft. At the beginning of the 1990s, a first RFID normalisation appeared. Although different RFID systems have been in use for years, popular accounts of RFID technology typically refer to the Electronic Product Code developed by the Auto-ID Center in collaboration with the Massachusetts Institute of Technology and other universities. EPC (*Electronic Product Code*) makes future RFID tags as simple as possible in order to produce low-cost chips at about five dollar cents. Using an Object Name Service (ONS) database, information about tagged objects could be provided.
While avoiding the use of the radio spectrums dedicated to TV, first-aid organisations, radio maritime, air services and mobile telephones, some RFID systems operate in the low-frequency band (125-134.2 KHz), others operate in the UHF band (915 MHz) and the micro-wave (2.45 GHz). As a results, tag characteristics are divided into five classes depending upon their capabilities [2]:

- **Class 0** and **class 1** tags have a Read-Only and a Write-Once Read-Many memory respectively. They are frequently used as bar-code replacement or electronic article surveillance.
- **Class 2**, **class 3** and **class 4** tags have Read-Write memories. This allows them to be operated as devices. They are able to establish a sensor or a ad-hoc wireless networks.

As RFID systems are likely to be widespread deployed in the coming years with EPC standards, today privacy and security become a key risk involved by three types of threats [3]:

- **Corporate data security threats** concern corporate espionage, competitive marketing threats, infrastructure threats and trust perimeters.
- **Personal privacy threats** come from unique tag Ids.
- **Cloning threats** appear frequently in automobile immobilizer systems.

Because of their low cost, EPC tags (class 0 to class 2) will be largely used in the coming years. However, only 250 to 4000 gates are left available for security and privacy solutions. Although the number of gates will increase over the years, as manufacturing techniques and processes is improving, tag computation is below the public key encryption capability. As a result, lots of researches investigate some simple security solutions for hardware and software algorithms.

2.2 Privacy and Security Solutions

Privacy and security solutions can be divided into two groups: hardware solutions and software solutions.
Hardware solutions are related to some controls of process variations in each integrated circuit [9], killing a tag or blocking a tag. The idea of killing a tag before it is placed in the hand of consumers come from [10]. As consumers could use some readers to scan their own tags, a technique to protect tag's context is to kill the tag. Indeed, a *kill command* (an 8-bit password-protected command) can be used to destroy a tag. However, a killed tag is truly dead and can never be reactivated. This is a key disadvantage for the "killing tag" technique.
Different than the "killing tag" technique, the blocking tag method involves no modification to the consumer tag. Based on the "tree walking" method, a blocking-capable tag creates an RF environment to prevent unauthorised scanning of consumer items in order to "spam" misbehaving readers, i.e. there is no way to locate the protected tag's ID [11]. Generally, the bit used to "spam" misbehaving readers is one of 28-bit EPC management. In this case, the difficulty to find a tagged tag raises up to 2^{28}.
Software solutions are based on the exchange of messages to establish an authentication between two entities. Although [12] suggested an mutual authentication without any hash function, most software solutions use general hash functions (like *MD4* and *SHA-1*) to support access control and authentication. Then, the main security solutions for RFID systems can be divided into three categories:

- Locked/unlocked tag.
- Anonymous ID tag.
- Friend tags.

The locked/unlocked tag technology proposed by the MIT is based on a hash access control scheme [13]. It uses the difficulty of inverting a one-way hash function to prevent unauthorised readers from reading tag contents. In this design, a tag must store a metaID and has two possible states: locked and unlocked. At initial phase, the reader owns a key for each tag. When a tag is locked, it sends a metaID to the reader and offers no other functionality. To

unlock a tag, a reader must send the key associated to the metaID received from the tag. Then the tag computes a hash function with the received key and compares it to the stored metaID.

The anonymous ID tag [14] is self-protected as an adversary would not know that different anonymous ID belong to the same tag. These different anonymous ID can be generated using a probabilistic public key encryption, a common key encryption or a hash chain. In fact, a real tag ID is stored in a back-end database with more security protections than any low-cost tag can provide.

Finally, friend tags are protected by some challenge-response protocols. [5] proposed a hash chain technique to protect read/write query and data transmission while [6] involved removing label IC complexity and supported an authentication by using a challenge-response, re-encryption and shared secrets.

Generally, these security and privacy solutions are based on the exchange of messages between tags and readers. For example, a locked/unlocked tag could be locked by a erroneous message involved by a transmission error rather than a security attack. As a result, both security and privacy solutions should be studied while taking into account transmission errors.

3. Influence of Transmission Error on Security Solutions

When a tag or a reader of an RFID system receives an erroneous authentication message, it is hardly possible to determine if this error comes from a transmission error or from a countermeasure as a noisy channel or a storage medium could cause serious transmission errors. A solution to come over this kind of transmission errors is *error correction coding*. In 1948, Shannon demonstrated in a landmark paper that, by proper encoding of the information, errors generated by a noisy channel can be reduced to any desired level without sacrificing the rate of information transmission, as long as the information rate is smaller than the capacity of the channel [15]. Since Shannon's work, much effort has been expended on the problem of devising efficient coding methods such as FEC (*Forward Error Correction*) and ARQ (*Automatic Retransmission Request*). However, RFID systems are generally low-cost systems. Supporting FEC in addition to computation at privacy and security solutions becomes a major challenge.

3.1 Analysis of the Influence of Transmission Errors

Whatever the involved security solution, transmission errors have a negative influence. Before developing our analysis, let introduce the following notations.

For the reader/server part:

- N_{RS}: the number of necessary messages to establish an authentication.
- S_{RS}: the message size (in bytes).
- T_{RS}: the bit error rate in the network.
- P_{RS}: the probability for at least one error occurred.

P_{RS} is defined as follows:

$$P_{RS} = 1-(1-T_{RS})^{8N_{RS}\times S_{RS}} \quad (1)$$

For the tag/reader part:

- N_{TR}: the number of necessary messages to establish an authentication.
- S_{TR}: the message size (in bytes).
- T_{TR}: the bit error rate in the radio frequency part.
- P_{TR}: the probability for at least one error occurred.

P_{TR} is defined as follows:

$$P_{TR} = 1-(1-T_{TR})^{8N_{TR}\times S_{TR}} \quad (2)$$

Then, let P_{error}: be the probability for an authentication procedure to fail. As an error may occur either in the tag/reader part or in the reader/server part, P_{error} is defined as follows:

$$P_{error} = 1-(1-P_{RS})(1-P_{TR}) \quad (3)$$

From Eq. 1 and Eq. 2, this can be reduce to:

$$P_{error} = 1-(1-T_{RS})^{8N_{RS}\times S_{RS}}(1-T_{TR})^{8N_{TR}\times S_{TR}} \quad (4)$$

This highlights that P_{error} mainly depends upon both bit error rates and message sizes. Fig. 2 presents the transmission error probability as a function of the bit error rate for various message sizes. The graph shows that the probability for a transmission error is 27% for 100-byte messages and 78% for 800-byte messages when the bit error rate of the RF channel is 10^{-4}. This shows that the transmission error rate must be taken into account.

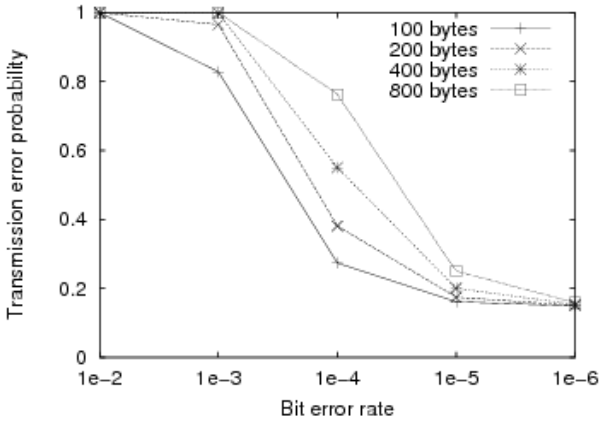


Fig 2: Transmission error probability for various message sizes.

Table 1: Message sizes and number of messages used in security solutions.

Security solutions	*Algorithms*	*Estimated message size*	*Number of messages*	*References*
Locked-unlocked tag	Hash Based Access Control	128 bits V	4	[13]
Locked-unlocked tag	Randomised Access Control	160 bits	*n*	[13]
Anonymous ID tag	Probabilistic Public Key Encryption	96 bits	3	[14]
Anonymous ID tag	Common Key Encryption	128 bits	3	[14]
Anonymous ID tag	Hash Chain	96 bits	3	[14]
Friend tag	Hash Chain with Challenge/Response	96 bits	4	[5]
Friend tag	Authentication with Challenge/Response	32 bits	2	[6]
Friend tag	Common Key Encryption with Challenge/Response	128 bits	3	[6]
Friend tag	Share Secrets with Challenge/Response	128 bits	5	[6]

3.2 Effectiveness with Existing Security Proposals

As shown in Eq. 4, the bit error rate, the message size and the number of messages are the elements that influence stability and effectiveness of security solutions the most. Table 1 gathers these arguments for the security solutions presented in Sec. 2.2. Using data from Table 1, we first analyse the influence of the bit error rate on anonymous ID tags and then on friend tag solutions.

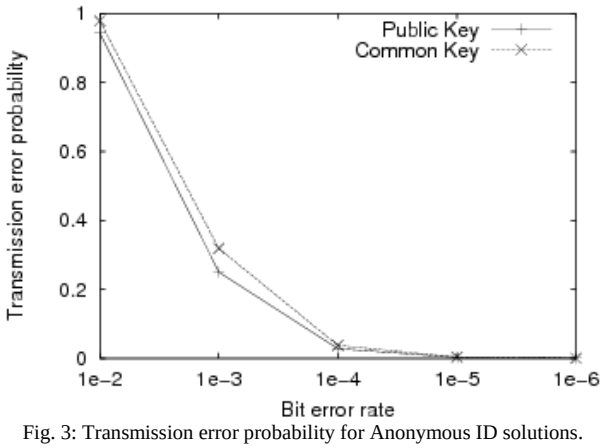


Fig. 3: Transmission error probability for Anonymous ID solutions.

Fig. 3 compares two solutions for anonymous ID tags: the first one uses a probabilistic public key encryption and the second one a common key encryption. It shows that, to allow these solutions to support stability and effectiveness, the bit error rate must be close to 10^{-5}.

Fig. 4 compares different friend tag solutions. It shows that the friend tag authentication can be used if the bit error rate is equal to 10^{-4} while the other solutions cannot work with a bit error rate greater than 10^{-5}.

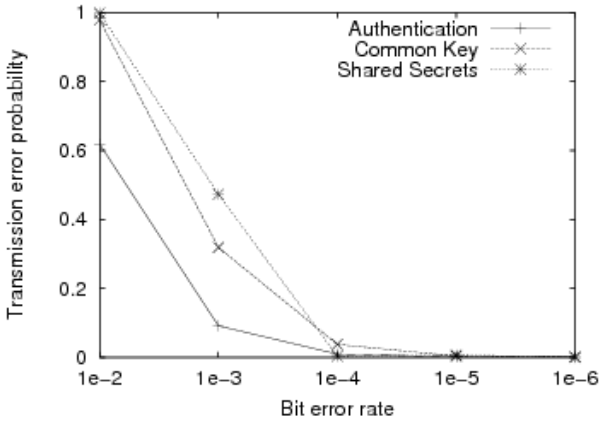


Fig. 4: Transmission error probability for Friend Tag solutions.

Table 2 summarises the minimal bit error rate (BER) for both anonymous ID tags and friend tags to support reliability and effectiveness.

It is clear that a reliable and efficient security solution should require the minimum number of messages, each with the smallest possible size. However, security solutions depend on sophisticated computations with necessary challenge/response messages. Moreover, an RFID system cannot provide a 10^{-5} bit error rate because of the radio transmission quality. It seems difficult to reduce the number and the size of messages or to improve the physical quality of radio transmissions. The solution may reside in a cross-layer architecture.

Table 2: Minimal bit error rate to support reliability and effectiveness of security solutions.

Security solutions	*Algorithms*	*Minimal BER*
Anonymous ID tag	Probabilistic Public Key Encryption	10^{-5}
Anonymous ID tag	Common Key Encryption	10^{-5}
Anonymous ID tag	Hash Chain	10^{-5}
Friend tag	Hash Chain with Challenge/Response	10^{-5}
Friend tag	Authentication with Challenge/Response	10^{-4}
Friend tag	Common Key Encryption with Challenge/Response	10^{-5}
Friend tag	Share Secrets with Challenge/Response	10^{-5}

4. A Cross-Layer Architecture Approach

To improve the reliability and the feasibility of security solutions, we suggest a cross-layer architecture approach to RFID systems. Fig. 5 illustrates this two-layer architecture design: at the highest layer, the functionality of RFID system is the same as in a classical RFID system; at the lowest layer, additional ARQ is added. Therefore, instead of the classical RFID procedure (i.e. the execution of the security algorithm), the two-layer architecture executes both the security algorithm and the ARQ before sending a message.

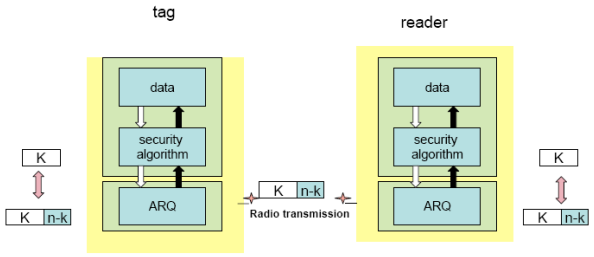


Fig. 5: Cross-layer design approach.

As pointed out in Sec. 3, there are two categories of techniques for controlling transmission errors in transmission systems: the FEC scheme and the ARQ scheme. In an FEC system, an error-correction code is used. When the receiver detects the presence of errors in a received message, it attempts to determine the error locations and then corrects the errors. In an ARQ system a code with good error-detecting capability is used. At the receiver, the syndrome of the received message is computed. If the syndrome is zero, the received message is assumed to be error-free and is accepted. Otherwise, the sender is instructed to retransmit the same message.

FEC systems are generally used in transmission systems supporting real-time applications such as GSM, GPS and WiMax (IEEE 802.16). Meanwhile, this kind of systems must embed some computation capability to work an error-correction code. RFID system is exceedingly diverse into five classes as indicated in Sec. 2.1. It is an interesting interplay between cost and security. This makes the FEC scheme not a good solution in this case.

The ARQ scheme is suitable for data transmission systems which have no strict real-time constraints. Furthermore, the ARQ scheme needs few computation capabilities. As a result, our cross-layer architecture approach should use an ARQ technique.

4.1 Cross-Layer Operations

Fig. 6 presents the operations of our cross-layer design from Fig. 5 for both the *sender* and the *receiver*:

- *Sender* at higher layer: the sender applies some security algorithms (e.g. common key encryption or hash chain) onto a *k*-bit message.
- *Sender* at lower layer: after applying ARQ the double-error correction with an additional (*n*-*k*) bits, the *n*-bit message is sent.
- *Receiver* at lower layer: ARQ detects the transmission error in the *k*-bit received message. If the received *k*-bit message is error-free, a notification (ACK) is sent back to the sender. Otherwise, a retransmission request is sent to the sender.
- *Receiver* at higher layer: the received *k*-bit message is checked by the security algorithm.

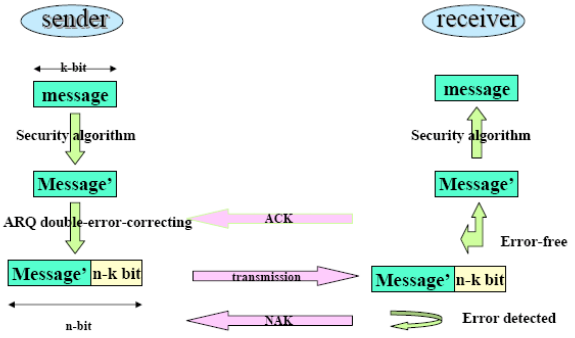


Fig 6: Cross-layer operations.

Let P_{ARQ} be the probability that a *k*-bit message is transmitted correctly and P_D be the probability for error detection. By definition, P_{ARQ} is defined by:

$$P_{ARQ} = (1 - P_D)\sum_{i=0}^{l} P_D^i \quad (5)$$

$$= 1 - P_D^l \quad (6)$$

Moreover, as P_D is defined as a function of the bit error rate (P_{BER}) with:

$$P_D = 1 - (1 - P_{BER})^k \quad (7)$$

the expression for P_{ARQ} as a function of the bit error rate is derived from Eq. 6 and Eq. 7 and is given by:

$$P_{ARQ} = 1 - (1 - (1 - P_{BER})^k)^l \quad (8)$$

The next section shows how our novel cross-layer architecture improves security solutions for RFID systems.

4.2 Improved Security Solutions

Let's consider that the target for the probability for a message to be transmitted correctly (P_{ARQ}) is 10^{-5} and that the transmission performance depends on three arguments: the radio transmission quality (the bit error rate), the size

Table 3: Parameter settings.

Security solutions	*Algorithms*	*Double error correction*	*k bits*	*n-k bits*
Friend tag	Hash Chain with Challenge/Response	BCH	96 bits	96
Friend tag	Authentication with Challenge/Response	BCH	32 bits	32
Friend tag	Common Key Encryption with Challenge/Response	BCH	128 bits	128

of exchanged messages and the number of re-transmission. As a radio transmission suffers more from noise and errors than a wire network link, the additional $n - k$ bit should be a double of k bit [16]. Table 3 presents the parameter settings from friend tags. Fig. 7 shows the improvement of some security solutions with our cross-layer architecture. It highlights that the probability of transmission errors is at least divided by two due to the ARQ scheme at low layer. As a 10^{-2}-bit error rate is a very bad case regarding the RFID transmission quality, the transmission improvement with our cross-layer architecture is noticeable. This way, our solution makes all security solutions more reliable and more efficient.

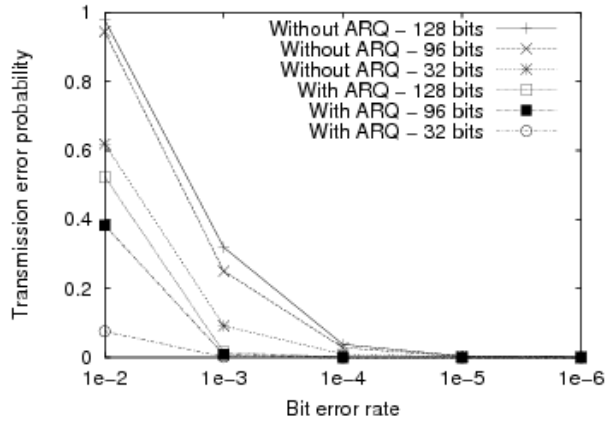


Fig. 7: Improvement of security solutions using our cross-layer design.

4.3 Discussion and Open Issue

Security and transmission error control usually deal with different aspects of telecommunications. Security solutions are based on some mathematical theories to support one-way calculation while error correction codes are built from Galois Field and Matrices. We believe that best solution is to study an integral solution with security and transmission error control. In 1978, McEliece [17] proposed a public-key crypto-system that was based on algebraic error-correcting codes, a problem known to be NP-hard [18]. Then in 1993, Stern worked on a protocol with identification while Kabatianski, Smeets and Johansson showed a systematic authentication codes via error correcting codes in 1996 [19,20]. Our future work will propose a solution integrated with error correcting codes and security.

5. Conclusion

Focussing on privacy and security solutions in RFID systems, we showed up that the problem of reliability and efficiency involved by radio transmission quality should not be underestimated. As it is difficult to reduce both transmission errors physically and the number of exchanged messages, we proposed a cross-layer architecture for RFID system. Using this two-layer architecture, we demonstrated that security solutions are more reliable and more efficient.

Our future works will focus on a integrated solution including correcting codes and security solutions.

References

[1] B. J. Feder, ”Delta to Invest in radio Tags for Luggage at Airports”, The New York Times, July 1, 2004.

[2] Auto-ID Center, Web pages. http://www.autoid.org. 2005.

[3] Simson L. Garfinkel, Ari Juels and Ravi Pappu ”RFID Privacy: An Overview of Problems and Proposed Solutions”, IEEE Computer Society on Security and Privacy, pp. 34-43, May/June, 2005.

[4] Ari Juels ”Minimalist Cryptography for RFID Tags”, 4th international Conf. Security in Communication Networks, pp. 149-164, September 8-10, Amalfi, Italy, 2004.

[5] Zongwei Luo, Terry Chan and Jenny S. Li ”A Lightweight Mutual Authentication Protocol for RFID Networks”, Proceedings of the IEEE International Conference on e-Business Engineering (ICEBE’2005) pp. 620-625, 12-18 Oct. 2005, BeiJing, China.

[6] Damith C. Ranasinghe, Daniel W. Engels and Peter H. Cole ”Security and Privacy Solutions for Low-Cost RFID System”, Proceedings of IEEE ISSNIP pp. 337-345, 5-8 Dec. 2005, Melbourne, Australia.

[7] Stephen August Weis, ”Security and Privacy in Radio-Frequency Identification Devices”, thesis (master), Dep of Electrical Engineering and Computer Science, Massachusetts Institute of Technology, 9 May,2003.

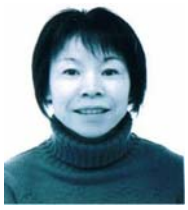
[8] Simson L. Garfinkel, ”Adopting Fair Information Practices in Low-Cost RFID System”, In Ubiquitious Computing, Sep. 2002.

[9] W. J Lee, Daihyun Lim and al, ”A Technique to build a secret key in integrated circuits for identification applications”, research repport of Massachusette Institute of Technology, No.472, 2004.

[10] S. E. Sarma, S.A.Weis and D.W.Engels, ”RFID systems ans Security and Privacy Implications”, Technical report MIT-AUTOID-WH-04, Auto Center, MIT,US, 2002.

[11] A. Juels, R. Rivest and M. Szydlo, ”The Blocker Tag: Selective Blocking of RFID tags for Consumer Privacy”, Proceedings of the 10th ACM Conference on Computer and

Communications Security, pp.103-111,2003, Washingtion, USA, October 27-30, 2003
[12] S. Boumerdassi, P.K. Diop, É. Renault and A. Wei, "A New Authentication Protocol for RFID Sensor Networks". In proceedings of IEEE SCVT, Enschede, The Netherlands, Nov. 2005.
[13] Stephen A. Weis, Sanjay E. Sarma, Ronald L. Rivest and Daniel W. Engels, "Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems", 1st International Conference on Security in Pervasive Computing, pp. 201-212, Boppard, Germany, March 2003.
[14] S. Kinoshita, M. Ohkubo, F. Hoshino and al, "Privacy Enhanced Active RFID Tag", Proceedings of 1st International Workshop on Exploiting Context Histories in Smart Environments, Mark Weal, University of Southampton, UK, Feb. 23, 2005.
[15] R.J.Benice and A. H. Frey,"An Analysis of Retransmission Systems", IEEE Trans, Commun, Technol, COM-12, pp. 135-45, Dec. 1964.
[16] A. Poli and L. Huhuet,"Codes Correcteurs - Theorie et Applications", MASSON, pp. 429-435, 1989.
[17] R. J. McEliece, "Public-key cryptosystem based on algebraic coding theroy", DSN Progress Rep.vol. 42-44, Jet Propusion Laboratory, California Institute of Technology, Passdena, CA, Februry 1978.
[18] E.R. Berlekamp, R. J. McEliece and N.J.A. Sloane, "On the inherent intractibility of certain coding problem", IEEE Trans. Info. vol. 24(5), pp. 384-386, 1978.
[19] Stern, "A new identification scheme based on syndrome decoding Crypto", no 773, LNCS Springer Verlag, pp.13-21,1993.
[20] Kabatianski, Smeets, Johansson *On the cardinality of systematic authentification codes via error correcting codes*. In IEEE Trans on Info Theory IT42, pp.566-578, 1996.



Anne Wei graduated from the Department of Electronic Engineering of the Shanghai University in 1986 and completed her PhD in 1999 at Institut National des Télécommunications, France. After two years in computing system company, she is now an associate professor at the Université Paris XII where she teaches computing and networks. She has been engaged in research on computer networks and on mobile systems post-3G using a chain of multi-carrying wireless communications.

Benoit Geller is an associate professor at the Université Paris XII. His research interests include error correction codes (turbo codes) and synchronisation of telecomunication systems. He works for some INCA europe projects and some France Telecom industrial projets.

Guozhi Wei is a PhD student at the Université Paris XII. His research interests include wireless network handover and security, especially in the area of Mobile IPv6. He received an MSc in computer science from the Université Paris VI.

Selma Boumerdassi is an associate professor at the Conservation National des Arts et Métiers, Paris, France, since 2000. Her research interests include wireless and mobile networks especially for routing and security, and RFID systems. She received a MSc in Computer Engineering in 1993 from the Institut National d'Informatique, Algeria, a MSc in Computer Science in 1995 and a PhD in Mobile Networks in 1999 from the Université de Versailles—Saint-Quentin-en-Yvelines, France, where she also served as an assistant professor.

Éric Renault is an associate professor at the Institut National des Télécommunications, Évry, France, since late 2001. His research interests include cluster and grid computing, high-performance messaging, RFID systems and security. He received both a MSc in Computer Engineering and a MSc in Computer Science in 1995 and a PhD in Parallel Computing in 2000 from the Université de Versailles—Saint-Quentin-en-Yvelines, France, where he also served as an assistant professor. In 2001, he was a research associate at Dartmouth College, NH.