Privacy Challenges in RFID Systems

Yong Ki Lee, Lejla Batina, and Ingrid Verbauwhede

1 Introduction

Radio frequency identification (RFID) is the technology to identify or track an object using wireless communication. Most RFID systems are composed of three parts: RFID tags, readers, and servers. A tag is attached to an object and it communicates with a reader to transfer its identity and possibly to exchange some data. A server collects and utilizes data of tags via readers. In general, there are two types of tags: active tags and passive tags. Active tags have a battery and can initiate communication, while passive tags derive energy from a reader's carrier signal.

RFID applications are radically expanding from supply chains management and access control and inventory to health care, new-born's safety, road pricing, transport control, etc. [1]. In short, RFID systems are expected to replace the bar code systems completely in near future. However, this expansion induces various security and privacy issues. If no proper security solution is applied, tags can allow for an unauthorized identification and/or tracking. Moreover, most of the international and/or industrial standards use either a simple password-based access control or they have no security at all to keep implementations of a tag very cheap [2, 3]. This can cause serious security and privacy risks since an eavesdropped password can be easily used to compromise or track a tag.

Recently, many security solutions were designed using cryptographic hash functions or private-key encryption algorithms that require less hardware and power resources than public-key algorithms. However, due to the limitations of hash functions and private-key algorithms, they cannot satisfy all the desired properties for general RFID systems, which are system scalability and security against cloning attacks, replay attacks, tracking attacks, and Denial of Service (DoS) attacks [4].

Y.K. Lee (✉) and I. Verbauwhede
University of California, Los Angeles, 56-125B Engineering IV Building 420 Westwood Plaza, Los Angeles, CA 90095-1594, USA
e-mail: jfirst@ee.ucla.edu

L. Batina and I. Verbauwhede
ESAT/SCD-COSIC, Katholieke Universiteit Leuven, Kasteelpark Arenberg 10, B-3001, Belgium

D. Giusto et al. (eds.), *The Internet of Things: 20th Tyrrhenian Workshop on Digital Communications*, DOI 10.1007/978-1-4419-1674-7_39,

In this chapter, we give an overview of security and privacy solutions for RFID not only for the standards but also in the research community. Depending on the required security and/or operational properties, different cryptographic primitives are needed. In addition, we present our novel authentication protocols, which satisfy all the required properties for RFID systems such as scalability, anticloning, and protection against tracking and impersonation attacks [5].

2 Overview

2.1 Desired Properties in RFID Systems

There are some generally required operational and cryptographic properties for RFID systems as follows:

1. *System scalability*: Some randomized authentication protocols, e.g. [6,7], are not scalable since the computational workload on the server increases linearly with the number of tags. Considering that in general RFID systems include a large number of tags, this is a required property.
2. *Anticloning*: If a group of tags shares the same secret key and uses it for the authentication, the tags are vulnerable to cloning attacks. If an attacker succeeds to crack one of the tags, he can use the revealed secret to clone some other tags. Therefore, a secret key should be pertinent only to a single tag so that a revealed secret key cannot be used for any other tag.
3. *Replay attack (impersonation attack)*: An attacker should not be able to generate a valid set of messages for a new challenge if he does not know the secret keys of a tag. An attacker may actively query a tag and/or perform some polynomial time computation utilizing known information such as the system parameters and the history of exchanged messages.
4. *Anonymity (security against tracking attacks)*: If an attacker can differentiate between different tags from the exchanged messages, he is possibly able to track a tag, and hence its owner, and collect data for malicious purposes. Therefore, the messages should be properly randomized so that it is infeasible to extract any information about a specific tag.
5. *Backward/forward anonymity*: Even if all the information of a tag (including the secret keys) is revealed to an attacker at a certain moment, an attacker should not be able to track a tag in the past or future communications. We put this strong property as an option in the proposed protocols.
6. *Denial of service (DoS) attacks*: In some of the proposed RFID protocols, tags update their secret information to randomize the responses to a reader. In general, the secret updates must be synchronized between a tag and a server. Otherwise, the later authentications will fail since a server cannot recognize the updated secret of a tag. However, a perfect synchronization cannot be guaranteed in RFID systems since it can be easily disturbed by an attacker. The solution to overcome

the DoS attack is that tags block the secret updates after certain number of unsuccessful authentications. However, this causes tracking attacks since the responses of tags become fixed.

2.2 Security of RFID Standards

New standards such as ISO/IEC and EPCglobal emerged owing to growing applications for various industries. The existing standards are established depending on applications and radio frequencies. Some of the most prominent examples are ISO/IEC 14443/15693 for contactless smart cards, ISO 11784∼5/14223 for animal tracking, and ISO/IEC 18000 for item managements. EPCglobal has announced four standards, which are all for item management with passive RFID tags: Class-0 UHF (Ultra High Frequency), Class-1 Generation-1 HF (High Frequency), Class-1 Generation-1 UHF and Class-1 Generation-2 UHF [8]. Although standards from EPCglobal are industrial standards, they draw great attention from the RFID community. Especially, EPCglobal class-1 Gen-2 has been standardized as the ISO/IEC 18000-6C in 2006. This cooperation of ISO/IEC and EPCglobal results in more confidence of EPCglobal for RFID vendors and wider variety and lower prices for end-users.

The security features of the major standards are summarized in Table 1 [2, 8]. In most of the standards, authentication features are based on a simple password system and many others do not have any protection. Therefore, the security can be easily compromised since a password can be simply eavesdropped. For the privacy protection, a tag is killed when a product is purchased by an end-user. However, simply killing a tag is not desirable since there are many situations and environments where a tag can be utilized after the purchase [9, 10]. The cover-coding in EPCglobal Class-1 Gen-2 is used to mask reader-to-tag communications, where a reader performs an XOR operation for data encryption with a random number from a tag. Then, a tag can recover the received messages by doing another XOR operation. Assuming that the signal from a tag to a reader is too weak to be eavesdropped by an

Table 1 Security features in RFID standards

Standards	Security features
EPCglobal Class-0 Gen-0 UHF	Self destruct feature (24-bit password)
EPCglobal Class-1 Gen-1 HF	Self destruct feature (24-bit password)
EPCglobal Class-1 Gen-1 UHF	Self destruct feature (8-bit password) Cover-coding for reader-to-tag communication
EPCglobal Class-1 Gen-2 UHF	Self destruct feature (32-bit password) Access control (32-bit password)
ISO/IEC 18000-3	48-bit password for reading
ISO/IEC 18000-2/14443/15693, ISO 11784∼5	None in standard

attacker, this cover-coding scheme is an effective encryption scheme. However, an enhanced receiver or an implanted receiver near to a tag can make the cover-coding scheme useless.

2.3 Security for Non-standard RFID

In order to protect the privacy of tags, many solutions are proposed in the literature using different cryptographic primitives. Cryptographic primitives can be classified into four categories: Random number generators (RNG), cryptographic hash functions, private-key algorithms, and public-key algorithms. Most of the RFID standards use only RNG, which is not sufficient to provide the requirements. Therefore, nonstandard solutions rely on stronger cryptographic primitives to enable stronger security and privacy protection.

First of all, in order to protect from replay attacks, authentications should be a challenge-response type. A generic challenge-response RFID protocol can be defined as in Fig. 1 [4] where k is private information such as a tag's secret key and ID. In order to facilitate the privacy requirements, the function f must be a one-way function whose output is undistinguishable from random. This function can be constructed with one of the cryptographic primitives.

2.3.1 Protocols Using Hash Functions

The function f in Fig. 1 can be replaced with a hash function as shown in Fig. 2, where multiple hash inputs need to be combined with some operations such as the string concatenation or the bitwise XOR operation.

In this case, however, the system is not scalable since a reader (or server) needs to compute $H(\mathrm{ID}_i, c, r)$ for each tag index i until a match is found. If there is a match, a tag is recognized as a valid one, otherwise rejected. Some relevant works can be found in [6, 7, 11–16]. Some of the published work does not satisfy either

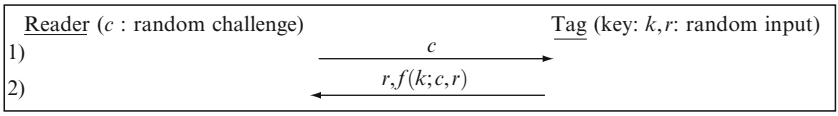

Fig. 1 A generic challenge-response RFID protocol

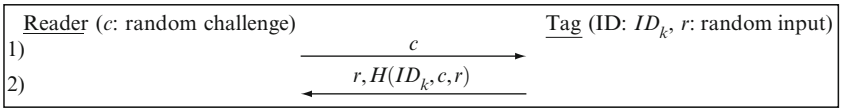

Fig. 2 Hash based randomized access control (H-RAC)

system scalability or the privacy requirement, and the others are vulnerable to the Denial of Service attacks. If the privacy is required, the system eventually becomes unscalable as shown in Fig. 2. This is due to the use of hash functions.

2.3.2 Protocols Using Private-Key Algorithms

In order to obtain the system scalability, the function f should be invertible. By applying a secret-key algorithm, a tag can transfer its ID encrypted and a reader can decrypt the messages. However, if a tag uses its own secret key, which is different from the others, a reader needs to apply every possible key of all tags since a reader does not know a tag's ID at the moment. If a reader finds a proper key, he can verify a tag's ID by decrypting the messages. However, this procedure makes the system unscalable. Therefore, in order to overcome this problem, the secret key must be shared among tags so that a reader can apply the same secret key for any tag, which makes the system vulnerable to cloning attacks. The protocol as described in Fig. 3, where SE_K is a private-key encryption with the private key K, can be used. Note that the transmission of r in plain text is not necessary since the message can be decrypted without it. Some relevant work can be found in [17–19]. However, none of the previous work was able to overcome the limitation of private-key algorithms.

2.3.3 Protocols Using Public-Key Algorithms

In order to satisfy the desired cryptographic and operational properties mentioned in this paper, a public-key algorithm is indispensable as shown in [4]. A public-key algorithm can be directly applied to a generic challenge-response RFID protocol as in Fig. 4, where R_{SK} and R_{PK} are a reader's secret and public key pair. Since a reader can use the same decryption key for any of tags, the system is scalable while maintaining the security against cloning attacks.

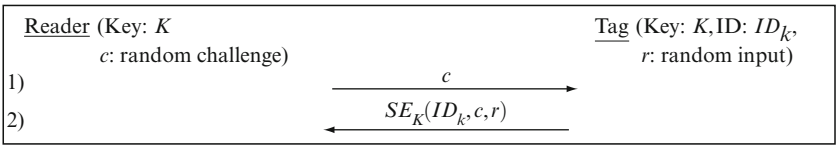

Fig. 3 Secret-key based randomized access control (SK-RAC)

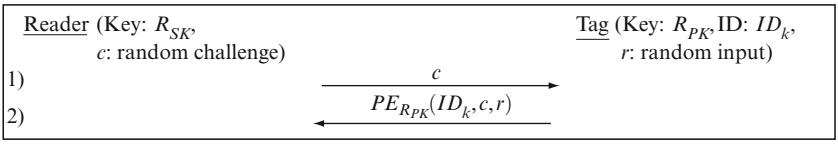

Fig. 4 Public-key based randomized access control (PK-RAC)

In many cases, however, authentication protocols are separately designed instead of directly applying a public-key encryption algorithm (as in Fig. 4) due to its high computational complexity. Some well-known public-key based authentication protocols are the Schnorr protocol [20] and the Okamoto protocol [21]. These protocols have security proofs in a classical model, but they are not proper for RFID systems since the vulnerability to tracking attacks remains, as shown in [22].

A compact public-key processor that is suitable for Fig. 4 can be found in [23], where a variant of Rabin cryptosystem is used. The EC-RAC protocol for efficient RFID authentication is proposed in [22]. However, it was broken in [24], and the randomized Schnorr protocol is proposed for the replacement. The revision of EC-RAC and its security analysis are presented in [5].

2.3.4 Comparison of Cryptographic Features

A comparison of cryptographic features for RFID systems is summarized in Table 2. The level 0 and level 1 are covered by some international standards, and the others can not be covered by standards since they require more complex cryptographic primitives. Depending on the allowed cryptographic primitives, achievable properties differ, and in order to satisfy all the properties, a public-key algorithm is required. However, some of the properties may not be needed depending on the application. For example, in systems with remote car key immobilizers, the number keys (tags) is not so big, so H-RAC could be enough.

In the remainder of this paper, we discuss Elliptic Curve based authentication protocols, which are presented in [5].

Table 2 Security and privacy features for RFID

Security level	Level 0	Level 1	Level 2	Level 3	Level 4
Primitives	Nothing	RNG	RNG, hash function	RNG, private-key	RNG, public-key
Authentication	Password	Cover coding	C/R	C/R	C/R
Replay attacks	Vulnerable	Vulnerable	Secure	Secure	Secure
Cloning attacks	Vulnerable	Vulnerable	Secure	Vulnerable	Secure
Tracking attacks	Vulnerable	Vulnerable	Secure	Secure	Secure
System scalability	Scalable	Scalable	Un-scalable	Scalable	Scalable
Examples	EPCglobal, ISO/IEC 18000-3	ISO/IEC 18000-6C	H-RAC	SK-RAC	PK-RAC, [5, 24]

Cover coding: password can be transmitted with cover coding
C/R challenge/response
[24]: Randomized Schnorr protocol, [5]: Revised EC-RAC

3 Authentication Protocol Design

3.1 System Parameters

RFID systems are in a somewhat different situation from conventional protocols. Unlike conventional authentication protocols, a tag's ID or public-key is not public information since revealing the ID (or public-key) on the fly can cause tracking attacks. Therefore, we also call a public key of a tag a *verifier*. Moreover, RFID protocols are many to one protocols, i.e. many RFID tags communicate with one server. Because of this, tags' verifiers can be kept securely in the server in order to be used for authentications.

First, we assign each tag two secret keys, x_1 (ID) and x_2 (password), similarly to conventional password protocols. Note that the ID is also secret information just like the password. The corresponding ID-verifier and password-verifier, $x_1 P$ and $x_2 P$, are securely stored in the server unlike general public-keys. For the attacking model, we suppose that an attacker knows the system parameters which can be revealed by cracking any of the tags. The system parameters and the storage of each entity are summarized in Table 3. Note that the base point P must be chosen to have a prime order as required by ECC standards [25, 26].

We consider authentication protocols as the combination of the secure ID transfer scheme and the secure password transfer scheme. These parts can be independently designed and analyzed, and can be composed differently depending on the application.

3.2 Component Design

In the ID transfer scheme (Fig. 5), a tag generates a random number r_{t1} and T_1, and transfers T_1 to the server. Then, the server responds with a random challenge r_{s1}, and a tag produces and transfers T_2 to the server. Finally, the server calculates a tag's ID-verifier $x_1 P (= X_1)$.

It is possible to use only the ID transfer scheme for a tag's authentication. The server may authenticate a tag by checking the existence of the decrypted ID-verifier

Table 3 System parameters

System parameters	y : Server's secret-key	$Y(= yP)$: Server's public-key
	x_1 : Tag's ID	$X_1(= x_1 P)$: Tag's ID-verifier
	x_2 : Tag's password	$X_2(= x_2 P)$: Tag's password-verifier
	P : Base point in the EC group	n : Prime order of P
Server's storage	y, X_1, x_1, X_2, P, n	
Tag's storage	x_1, x_2, Y, P, n	
Attacker's storage	Y, P, n : Publicly known information	

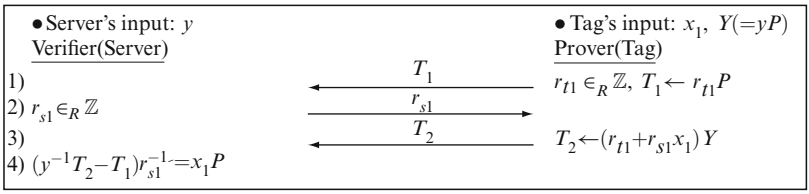

Fig. 5 Secure ID transfer (EC-RAC 1)

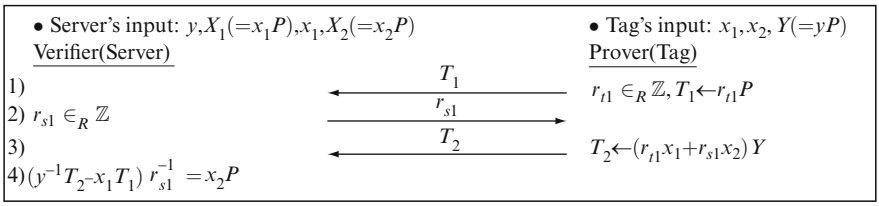

Fig. 6 Secure password transfer

in the list. However, a large number of tags may weaken the security level of the system since the probability that a randomly selected ID is identified as a valid one increases with the number of tags. Therefore, if the number of used tags is large, the password transfer scheme should be added.

Since the password transfer scheme (Fig. 6) is performed after the ID transfer scheme, the server already knows the tag's ID-verifier (X_1). Therefore, the server can look for x_1 and X_2, which are paired with X_1 in the local database.

3.3 Authentication Protocol Construction

We propose three schemes that can be combined differently as summarized in Table 4, where [24] is included for comparison. In EC-RAC 1, we are just using the ID transfer scheme for a tag's authentication. The server authenticates a tag by checking the existence of a tag's ID-verifier in the list. This would be effective to minimize the computation workload on a tag if the number of tags is relatively small. Although EC-RAC 1 is comparable to the randomized Schnorr protocol [24] with similar cryptographic properties, EC-RAC 1 has better performance than the randomized Schnorr protocol in a server (the number of EC point multiplication is smaller).

The combination with the secure password transfer scheme can be done in two different ways resulting in EC-RAC 2 and 3 with different amounts of computation and security properties. All the protocols are scalable and secure against cloning attacks, replay attacks, tracking attacks, and DOA attacks.

Table 4 Authentication protocol constructions and their security properties

Protocols		EC-RAC 1	EC-RAC 2	EC-RAC 3	[24]
EC point multiplication	Server	2	4	4	3
	Tag	2	3	4	2
Properties	Number of tags	Small	Large	Large	Small
	Backward/forward un-traceability	Secure	Vulnerable	Secure	Unknown

Common properties: scalability, protection against cloning, replay, tracking, and DoS attacks
Unknown: there is no proof for the backward/forward un-traceability

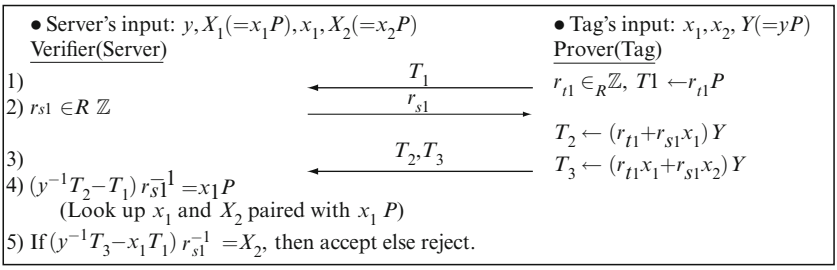

Fig. 7 EC-RAC 2 flow

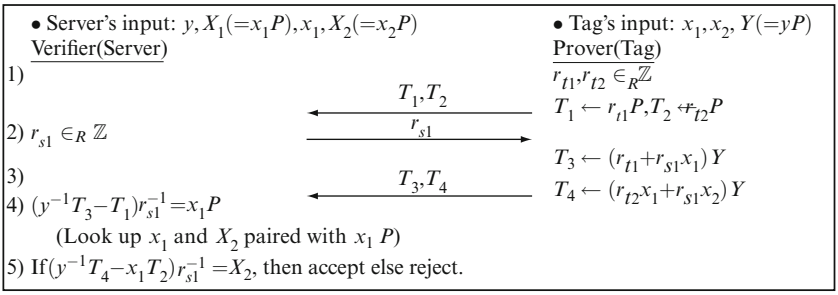

Fig. 8 EC-RAC 3 flow

The first combination is shown in Fig. 7, where the random point $T_1(= r_{t1}P)$ is used not only for the ID transfer scheme but also for the password transfer scheme. This minimizes the amount of computation on a tag, but it results in a weakness against forward/backward tracking attacks.

EC-RAC 2 can be revised to EC-RAC 3 (Fig. 8) to obtain security against forward/backward tracking attacks. In this case, a tag generates two random numbers and each one is used only once to encrypt its ID-verifier or password verifier.

4 Conclusion

We presented an overview of RFID authentication protocols and their achievable properties, which differ depending on the cryptographic primitives used. In addition, several Elliptic Curve based authentication protocols are presented, showing a much stronger properties in RFID systems.

Acknowledgments This work is supported in part by the IAP Programme P6/26 BCRYPT of the Belgian State, by FWO project G.0300.07, by the European Commission under contract number ICT-2007-216676 ECRYPT NoE phase II, by K.U. Leuven-BOF (OT/06/40), NSF CCF-0541472 and SRC.

References

1. Seaner J (2006) EPC/RFID update. http://www.chemicalstrategies.org/pdf/workshop_events/JSeaner_RFID.pdf,EPCglobal
2. Phillips T, Karygiannis T, Kuhn R (2005) Security standards for the RFID market. IEEE Secur Priv 3(6):85–89
3. Razaq A, Luk WT, Shum KM, Cheng LM, Yung KN (2008) Second-generation RFID. IEEE Secur Priv 6(4):21–27
4. Burmester M, Medeiros B, Motta R (2008) Anonymous RFID authentication supporting constant-cost key-lookup against active adversaries. Int J Appl Cryptogr 1(2):79–90
5. Lee YK, Batina L, Verbauwhede I (2009) Untraceable RFID authentication protocols: revision of EC-RAC. In: IEEE international conference on RFID, pp 178–185
6. Ohkubo M, Suzuki K, Kinoshita S (2003) Cryptographic approach to "privacy-friendly" tags. In: RFID Privacy Workshop, MIT, Cambridge, MA
7. Weis SA, Sarma SE, Rivest RL, Engels DW (2003) Security and privacy aspects of low-cost radio frequency identification systems. In: The first international conference on security in pervasive computing – SPC'03
8. Karygiannis T, Eydt B, Barber G, Bunn L, Phillips T (2007) Guidelines for securing radio frequency identification (RFID) systems: Appendix A – RFID standards and security mechanisms. In: NIST Special Publication 800-98, pp A1–A5
9. Garfinkel SL, Juels A, Pappu R (2005) RFID privacy: an overview of problems and proposed solutions. IEEE Secur Priv 3(3):34–43
10. Kumar R (2003) Interaction of RFID technology and public policy. RFID Privacy Workshop, MIT, Boston, MA
11. Avoine G, Oechslin P (2005) A scalable and provably secure hash-based RFID protocol. In: IEEE international workshop on pervasive computing and communication security – Persec'05
12. Burmester M, van Le T, de Medeiros B (2006) Provably secure ubiquitous systems: universally composable RFID authentication protocols. In: IEEE/CreateNet international conference on security and privacy in communication networks – SECURECOMM'06
13. Gao X, Xiang Z, Wang H, Shen J, Huang J, Song S (2004) An approach to security and privacy of RFID system for supply chain. In: IEEE international conference on E-commerce technology for dynamic E-business – CEC-East'04
14. Lee YK, Verbauwhede I (2005) Secure and low-cost RFID authentication protocols. In: IEEE international workshop on adaptive wireless networks – AWiN05, pp 1–5
15. Tan CC, Sheng B, Li Q (2008) Secure and serverless RFID authentication and search protocols. IEEE Trans Wirel Commun, 7(4):1400–1407
16. Tsudik G (2006) YA-TRAP: yet another trivial RFID authentication protocol. In: IEEE international conference on pervasive computing and communications – PerCom'06

17. Feldhofer M (2004) An authentication protocol in a security layer for RFID smart tags. In: IEEE Mediterranean electrotechnical conference – IEEE MELECON'04
18. Feldhofer M, Dominikus S, Wolkerstorfer J (2004) Strong authentication for RFID systems using the AES algorithm. In: Cryptographic hardware and embedded systems – CHES'04, LNCS, vol 3156. Springer, Berlin
19. Toiruul B, Lee K (2006) An advanced mutual-authentication algorithm using AES for RFID systems. Int J Comput Sci Network Secur 6(9B):156–162
20. Schnorr C-P (1989) Efficient identification and signatures for smart cards. In: Advances in cryptology – CRYPTO'89, LNCS, vol 435, Springer, Berlin
21. Okamoto T (1992) Provably secure and practical identification schemes and corresponding signature schemes. In: Advances in cryptology – CRYPTO'92, LNCS, vol 740, Springer, Berlin
22. Lee YK, Batina L, Verbauwhede I (2008) EC-RAC (ECDLP based randomized access control): provably secure RFID authentication protocol. In: IEEE international conference on RFID, pp 97–104
23. Oren Y, Feldhofer M (2008) WIPR – a public key implementation on two grains of sand. In: Conference on RFID security, Budapest, Hungary. http://iss.oy.ne.ro/WIPR, July 2008
24. Bringer J, Chabanne H, Icart T (2008) Cryptanalysis of EC-RAC, a RFID identification protocol. In: International conference on cryptology and network security – CANS'08, LNCS, vol 5339, Springer, Berlin
25. NIST (1999) Recommended elliptic curves for federal government use. http://csrc.nist.gov/groups/ST/toolkit/documents/dss/NISTReCur.pdf
26. SECG (2000) SEC 2: recommended elliptic curve domain parameters. http://www.secg.org/download/aid-386/sec2_final.pdf