A Lightweight RFID Authentication Protocol based on Elliptic Curve Cryptography

Ya-li Liu
College of Computer Science & Technology, Nanjing University of Aeronautics and Astronautics, Nanjing, China
College of Computer Science & Technology, Jiangsu Normal University, Xuzhou, China
Email: lyl1980115@163.com or ylliu@nuaa.edu.cn

Xiao-lin Qin*, Chao Wang, Bo-han Li
College of Computer Science & Technology, Nanjing University of Aeronautics and Astronautics, Nanjing, China
Email: {qinxcs@nuaa.edu.cn, wangc0809@163.com, bhli@nuaa.edu.cn}

***Abstract*—The security and privacy of the tag carrier has become the bottle neck of Radio Frequency Identification (RFID) system development further. In this paper, we propose a robust authentication protocol based on Elliptic Curve Cryptography (ECC), which meets the requirement of resource-limited RFID systems. Our protocol achieves mutual authentication and possesses lightweight feature by reducing the computation cost over the tag end. Moreover, the proposed protocol possesses remarkable security properties in RFID system and the immunity against the possible malicious attacks as well as an excellent performance through the detailed security analysis. Performance evaluation and function comparison demonstrate that our protocol makes a balance between cost and security in RFID authentication protocol. Compared to the previous relevant RFID authentication protocols, our protocol improves efficiency, enhances robustness, which is well suitable for RFID tags with the scarceness of resources.**

***Index Terms*—RFID, Lightweight, Public Key Cryptography (PKC), Elliptic Curve Cryptography (ECC)**

I. INTRODUCTION

Radio Frequency Identification (RFID) is increasingly becoming more popular in every aspect of our lives and works, which is expected to replace the current barcode technology in the near future. RFID is a wireless technology that allows the communication with passively powered devices, which plays a key role for identification purposes in the wide application scenarios of supply chain management, the anticounterfeiting of luxury goods, manufacturing, microchip fabrication industries, credit cards, e-passports, *etc*. Due to the intrinsic insecurity of the open wireless channel between the readers and the tags, security and privacy concerns [1] of RFID technology appears to be one of the most challenging areas. RFID systems are confronted with different security threats [2], such as eavesdropping, intercepting, modification, counterfeiting, traffic analysis, traceability, desynchronization *etc*. The need for privacy-preserving RFID protocols is evident [3~5], which is the fundamental solution to various security threats in RFID system. However, it is difficult to provide secure and privacy-preserving authentication protocols [6] in extremely constrained RFID systems with respect to memory, power, and energy of the tags.

Public Key Cryptography (PKC) based authentication significantly simplies the distribution of cryptographic keys. Elliptic curve cryptography (ECC) is emerging as an attractive public-key cryptosystem for mobile/wireless environments. The challenge of applying ECC in RFID environment is how to deal with the relative high computation cost associated with ECC algorithms to the resource-limited RFID platform. In 2007, Vaudenay [7] provided a formal model for RFID protocols and proved that PKC can assure the highest level of feasible privacy in RFID applications. ECC has gained much importance due to the equivalent security lever with the smaller key sizes, faster computations, lower power consumptions, as well as memory and bandwidth savings compared to traditional cryptosystems like RSA, so it is a promising primitive for passive RFID tags to provide various public-key services. Moreover, Elliptic Curve Discrete Logarithm Problem (ECDLP) can be regarded as one of the hardest mathematical problem among the public-key cryptosystem. Recently, the implementations in the field of RFID systems [8, 9] have shown that ECC is ready for RFID tags. Consequently, ECC increasingly becomes one of the most popular public-key cryptosystem to be applied widely in extremely constrained RFID systems in terms of memory type, power source and computation ability.

In this paper, we design an efficient authentication protocol based on ECC for resource-limited RFID systems. Compared with the previous related works, the proposed protocol has remarkable features as follows:

(1) Ensures security and privacy requirements by ECDLP and meanwhile avoids the risks neglected by previous ECC-based authentication protocols.

(2) Possesses remarkable privacy properties and the resistence to the typical malicious attacks considered in RFID systems.

*Corresponding author: qinxcs@nuaa.edu.cn

doi:10.4304/jcp.8.11.2880-2887

(3) Minimizes the computation cost on the tags to meet the implementation restrictions and puts the costly operations over the reader end, which makes it suitable for low-cost RFID systems.

(4) Equilibrates properly both security and performace for extremely constrained passive RFID tags.

The remainder of this paper is organized as follows. We present a critical review of the related work in Section 2. In Section 3 we then review some preliminaries briefly. Next our lightweight RFID authentication protocol based on ECC (LRAP) is described in Section 4. Section 5 addresses the presentations of security analysis. The performance evaluation is analyzed in Session 6. Finally, Section 7 concludes this paper.

II. Related Works

The research literatures of RFID authentication protocols are already quite extensive and growing, trying to solve RFID security and privacy problems. However, they all have certain flaws and vulnerabilities.

A series of ultralightweight RFID authentication protocols have been proposed in recently years. In 2006, Peris-Lopez *et al*. proposed a family of Ultralightweight RFID protocols LMAP, EMAP and M2AP [10~12]. These protocols only use simple bitwise operations to comply with the requirement of low-cost RFID tags, such as bitwise XOR, bitwise OR, bitwise AND, and Addiction mod 2^m. Unfortunally, it was later reported that these protocols are vulnerable to desynchronization attack and full-disclosure attack [13~15].

Some research literatures focus on the hardware implementation of PKC on RFID tags. A recent work of Wolkerstorfer [16] is the first to claim that it is possible to have low-power and compact implementation of ECC, which meets the constraints imposed by EPC standards. Moreover, many authors investigated [8, 9, 17] the possibility of building RFID hardware that is capable of performing public key algorithms based on ECC.

In the following, PKC based RFID authentication protocols have been proposed. In 2011, Batina *et al*. [18] first proposed a privacy-preserving grouping-proof RFID protocol based on ECC. But Lv *et al*. [19] proved that the protocol [18] failed to resist the tracking attack and lost the untraceability. In the same article [19], Lv *et al*. proposed an intensive protocol. But in 2012, Wen-Tsai *et al*. pointed that [19] is impracticable for the public-key cryptography in [20]. In 2008, Sheikh *et al.* put forward ERAP[21]. In 2009, Santi *et al*. proposed a secure elliptic curve-based RFID protocol (SECRP) [22]. These protocols ensure the security and privacy of RFID tags and readers, but they really need a lot of resource to complete the whole processing of these protocols.

From the above analysis of the previous protocols, we can find that these schemes all have the deficiency, which make them vulnerable to various malicious attacks. This paper aims to propose a new lightweight RFID authentication protocol based on ECC to enhance robustness and improve efficiency.

III. Preliminaries

A. RFID System Model

The typical RFID system model has three components: Tags, Readers and a Backend Database. It is generally assumed that the channel between the readers and the backend database with higher performance is a secure link, so these two parts can be regarded as a whole. Tags are wireless transponders attached to objects for detection. Readers are transceivers that can query tags for identification of objects. The wireless channel between readers and tags established by readers is generally regarded as insecure link on account of confronting more serious circumstances, such as various malicious attacks. The backend database is the only trusted entity to all the tags and readers that may share some secret information with the authenticated tags.

Each tag will get a unique identifier *ID* during the enrollment, as well as an associated secret key *K*, which are written into the ROM memory of the authenticated tags and can not be revealed to any unauthorized entities. Besides, each tag has an Index as pseudonym for replacing *ID* to be transmitted over the wireless channel. Each index is written into the EEPROM memory of the authenticated tags and it will be used for authentication by updating after each successful session. During the enrollment, the backend database stores a list which contains the corresponding secret information of each authorized tag. The authorized reader can obtain the entry of the backend database by this access list. If a reader is authorized to access the tags T_1, T_2…, T_n, after authenticating itself to the backend database, the reader will get its access list. The Index information of the authenticated tags in backend database is listed in TABLE I. as follows:

TABLE I.
THE ACCESS LIST OF THE AUTHENTICATED TAGS IN BACKEND DATABASE

Index_1	ID_1	K_1
Index_2	ID_2	K_2
…	…	…
Index_n	ID_n	K_n

B. Elliptic Curve Cryptography (ECC) [23, 24]

Definition 1. An elliptic curve E is defined over a finite field F_q, which consists of all the points $(x, y) \in F_q \times F_q$ that satisfy an equation of the form $Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$ with $a_i \in F_q$, whose discriminant is non null, along with the point at infinity.

Definition 2. Elliptic Curve Point-Addition Operation

The neutral element of this operation is the point at infinity and the set of points is an Abelian group. Elliptic Curve Point-Addition Operation is a scalar n multiple point P, denoted as nP, which means n times addition of point P.

Let G be an additive cyclic group generated by the point P, whose order is a prime order $q>2^k$. Practically we can think of G as an additive subgroup of points over an elliptical curve E for a secure parameter $k \in E$. The

inverse problem of Elliptic Curve Point-Addition Operation is ECDLP described as follows.

Definition 3. Elliptic Curve Discrete Logarithm Problem (ECDLP)

Given two group elements P, $Q \in G$, to find an integer $a \in Z_q^*$, such that $Q = aP$ whenever such an integer exists, which turns out to be computationally hard to solve.

To achieve the same security level in cryptosystems, the key requirements based on ECC is shorter than those based on RSA. The details are shown in TABLE II.

TABLE II.
KEY LENGTH REQUIREMENTS FOR THE SAME SECURITY LEVEL

ECC	RSA
112bits	512bits
160bits	1024bits
224bits	2048bits
256bits	3072bits
384bits	7680bits
512bits	15360bits

IV. OUR PROTOCOL LRAP

A. Notations

We use the notations for entities and operations as summarized in TABLE III to simplify description.

TABLE III.
NOTATIONS OF LRAP

R	Reader	K_d	Decryption key of the genuine T
T	Tag	K_e	Encryption key of the genuine R
TDS	Trusted backend database, which contains *ID*, *IDS* and the secret key of the genuine T	F_q	A finite field
PRNG	Pseudo-random Number Generator[25]	E	An elliptic curve over F_q
IDS	Index-pseudonym of T in current authentication session	P	Generator of an additive cyclic subgroup over E
IDS^{old}	Index-pseudonym of T in previous authentication session	q	Order of P
IDS^{new}	Index-pseudonym of T in next authentication session	+	Addition mod 2^l, l=96
ID	Unique and static identification information of the	$\oplus$	Bitwise XOR

B. LRAP

LRAP comprises four stages: Initial Setup phase, Tag Identification phase, Mutual Authentication phase, and Updating phase. The length of all the information mentioned in LRAP is L-bits (96bits), which is compatible with all the encoding schemes (i.e. GTIN, GRAI) defined by EPCGlobal. Fig. I. illustrates the specification of our protocol in the appendix. The details of one authentication session are presented below.

1. Initial Setup Phase

(1) TDS selects two big prime numbers p_1, $q_1 \in Z_q^*$ and sets $N=p_1q_1 \in Z_q^*$.

(2) TDS selects one pseudo random number $K_d \in Z_q^*$ as the decryption key of the genuine tag and computes the encryption key K_e of the genuine reader as $K_e = K_d P$.

(3) TDS puts K_e into the genuine reader and put K_d into the genuine tag.

(4) The genuine tag T keeps its decryption key K_d secret and the genuine reader R keeps its encryption key K_e and N secret.

2. Tag Identification Phase

(1) R→T: R sends a "Hello" message to T as a query to initiate a new protocol session. This action will also power T and make it possible to complete the authentication process.

(2) T→R: Upon receiving R's query, T will respond to R with its current Index-pseudonym *IDS*.

(3) R: After receiving *IDS*, R uses it as an index to search the access list to obtain the matched entry in TDS. With this *IDS*, only the authorized reader can acquire the unique private information (*ID*) of the genuine T from TDS, by which R will carry out the next authentication stages.

(4) Tag Identification

If R could find a matched entry in TDS, it steps into the mutual authentication phase; Otherwise, it probes again and then the identification is retried but not with the same *IDS* (IDS^{new}) rather with the old one (IDS^{old}), which is backscattered by T upon request.

3. Mutual Authentication Phase

(1) The Encryption Process in R: After finding a matched record in TDS, which could be IDS^{next} or IDS^{old} of T, R will process the encryption operation as follows:

① R generates two L-bit pseudo random numbers $(n_1, n_2) \in F_q \times F_q$ as the plaintext by applying with PRNG[25];

② R computes the ciphertext $(\gamma_1, \gamma_2, \gamma_3) = E_{K_e}(n_1, n_2)$, $(\gamma_1, \gamma_2, \gamma_3) \in F_q \times F_q \times E$;

③ R generates one L-bit random number n_3 $(1 \le n_3 \le q-1)$ by using PRNG[25] and then computes $\gamma_3 = n_3 P$, $(c_1, c_2) = n_3 K_e$, $\gamma_1 = c_1 n_1 \bmod N$, $\gamma_2 = c_2 n_2 \bmod N$.

(2) R→T: Afterwards, R computes $A=(IDS+n_1+n_2) \oplus K_e$ and sends the messages $(\gamma_1, \gamma_2, \gamma_3) \| A$ to T, that is R actually conveys a random challenge to T. $(\gamma_1, \gamma_2, \gamma_3)$ is used to send the plaintext with a mask to T. The purposes of A include the authentication of R and the integrity of the challenge messages.

(3) Reader Authentication

At the tag side, upon receiving the challenge messages $(\gamma_1, \gamma_2, \gamma_3) \| A$ from R, T will process the decryption and authentication operations as follows:

① T decrypts (n_1, n_2) from the received ciphertext $(\gamma_1, \gamma_2, \gamma_3)$ by the equations of

$(c_1, c_2) = K_d\gamma_3$，$n_1 = \gamma_1 c_1^{-1} \bmod N$，$n_2 = \gamma_2 c_2^{-1} \bmod N$. Only the authorized T will make it to figure out the plaintext (n_1, n_2);

② T computes the local version of *A*' by the equation of $A'=(IDS+n_1+n_2) \oplus K_dP$, which is compared with the received value *A*.

③If *A*' is equal to *A*, R is authenticated successfully and it makes sure that T decrypts the plaintext (n_1, n_2) from R correctly, and that means and R is a genuine reader;

Otherwise, T will do nothing and R is regarded as the fake reader because the received messages may be modified by an adversary on the wireless channel between R and T or sent by an unauthenticated reader. So this current session is abandoned and T waits for proceeding with the next authentication session.

(4) T→R: After R is authenticated, T computes the response message *B* by the equation of $B= (n_1 \oplus n_2) + ID$. Afterwards, T transmits *B* to R and then T will proceed with the next Updating Phase.

(5) Tag Authentication

After receiving the response message *B* from T, R computes the local version of *B*' by the equation of $B'=(n_1 \oplus n_2) + ID$ and compares *B*' with the received value *B*.

If *B*' is equal to *B*, T is authenticated successfully, and that means T is a genuine tag, which indicates that R considers T with this unique *ID* as detected and proceeds with the next Updating Phase. So this current Mutual-Authentication session is valid.

Otherwise, T is regarded as the fake tag. So this current session is abandoned and T waits for proceeding with the next authentication session.

4. Updating Phase

After completing the mutual authentication phase successfully, R and T will update and synchronize the local value of *IDS* to resist tracking attack.

(1) Tag Updating

After authenticating R and then sending the message *B* to R, T will update its local value *IDS* as follows: $IDS^{old} = IDS$; $IDS^{new} = (IDS^{old} + n_1) \oplus (ID + n_2)$ and it will also keep the old values IDS^{old} stored in T to prevent desynchronization. Then R will proceed with the following updating operations.

(2) Reader and TDS Updating

After authenticating T by the response *B*, that is after R and T authenticated each other, R will update its local value *IDS* by the equation of $IDS = (IDS + n_1) \oplus (ID + n_2)$. And then R will send the updating value *IDS* to TDS.

Till now, the protocol runs a whole round and the next authentication session will start from Tag Identification Phase.

V. Security Analysis

In this section, we will analyze the security performance of LRAP.

A. Data Confidentiality and Data Integrity

In the wireless channel between R and T, *ID* of the genuine tag is replaced by its current Index-pseudonym *IDS* as the response. In addition, all exchanged messages over the wireless channel mask the secret values of the unique identity *ID*, the encryption key K_e and the decryption key K_d with the random numbers (n_1, n_2, n_3) which are generated by the genuine reader. On account of the randomized challenge-response based on the dynamic (n_1, n_2, n_3) in different sessions, it is difficult to get any secret information about the genuine tag from the exchanged messages. Hence, the confidentiality of *ID*, K_e and K_d is assured.

Data integrity is assured as the secret values of *ID*, K_e, K_d and (n_1, n_2, n_3) are embeded in the exchanged messages $(\gamma_1, \gamma_2, \gamma_3) \| A$ and *B*, not being interpolated in the wireless channel between the tags and the readers. The verification of the consistency between the local version and the received version ensures the integrity of these secret values. If an adversary succeeds to modify the exchanged data over the wireless channel, the consistency verification will fail and the adversary can also be recognized. Hence, data integrity is also guaranteed.

B. Tag Anonymity

Only the authorized reader can identify the tag by its current Index-pseudonym *IDS* along with its corresponding tag entry in TDS. As the unique identity *ID* of the genuine tag is not transmitted in plaintext over R-T wireless channel, it is impossible for the adversary to extract the relevant information about *ID* of the genuine tag by intercepting the exchanged messages without the secret values of K_e, K_d and (n_1, n_2, n_3). So *ID* is never disclosed in the whole process of authentication session and the robustness of *ID* will not be compromised. Additionally, all public messages $(\gamma_1, \gamma_2, \gamma_3) \| A$ and *B* are anonymized and randomized to hide *ID* by the dynamic random numbers (n_1, n_2, n_3). Hence, tag anonymity can be guaranteed.

C. Mutual Authentication

LRAP provides mutual authentication between the tags and the readers by checking the consistency of the local values and the received values according to the same algorithm. The tag and the reader can authenticate each other, since only the legal entities has the secret key K_e and K_d, by which the legal entities can extract the dynamic random numbers (n_1, n_2, n_3). Specifically, after receiving the messages $(\gamma_1, \gamma_2, \gamma_3) \| A$, only the legal tag with the decryption key K_d can decrypt the message $(\gamma_1, \gamma_2, \gamma_3)$ and authenticate the reader by verifying the consistency of the received *A* and the local *A*'. Similarly, just the legal reader can obtain the corresponding information *ID* to the current response *IDS* by the tag's

entry in TDS and authenticate the tag by verifying the consistency of *B* and *B*'. So, only the legal reader and the legal tag have the ability to generate the consistent values which can be authenticated by the other party. Hence, mutual authentication between the readers and the tags is assured.

D. Resistance to Tracking Attack

Each tag dynamically updates *IDS* after every successful authentication session, and this update process involves the dynamic random numbers (n_1, n_2). Therefore, the successive *IDS* from the same tag look random, and the adversary cannot know what will be the next *IDS*. Moreover, the exchanged challenge-response messages $(\gamma_1, \gamma_2, \gamma_3) \| A$ and *B* of the same tag are randomized in each session, which also involves (n_1, n_2). This feature makes the exchanged data different for each tag reading so that the adversary cannot obtain the same response from the same tag in different sessions. As a consequence, it is impossible for the adversary to launch tracking attack through *IDS* or the exchanged messages and the location privacy of the tag owner is guarded. Hence, tracking attack can thus be prevented and all communications are unlinkable.

E. Resistance to Replay Attack

LRAP uses the randomized challenge-response to defend against replay attack, which ensures that the replay messages from the tag or the the reader will not be authenticated. The exchanged messages $(\gamma_1, \gamma_2, \gamma_3) \| A$ and *B* over the wireless channel are randomized and updated by the dynamically generated random numbers (n_1, n_2, n_3) in each session. The adversary can store all the exchanged messages during one successful authentication session to launch replay attack in the next session as follows.

Case ① Replay $(\gamma_1, \gamma_2, \gamma_3) \| A$

The adversary can replay $(\gamma_1, \gamma_2, \gamma_3) \| A$ of the previous session to impersonate a reader in current session. The tag can decrypt the plaintext (n_1, n_2) from $(\gamma_1, \gamma_2, \gamma_3)$ by using the decryption key K_d. Since the updated IDS^{new} in current session is not equal to IDS^{old} in previous session, the tag cannot verify the consistency between *A* and *A*' successfully and the adversary is regarded as the fake reader. Even if the tag cannot update *IDS* successfully in the previous session, the adversary can be regarded as the genuine reader by the consistency verification. Then the tag computes the response message *B* and sends it to the adversary. The replay attack in this case seems successful, but the adversary cannot obtain any secret information of the genuine tag from the intercepted messages because the unknown values of *ID*, K_e, K_d and (n_1, n_2, n_3) all involve in the construction of the exchanged messages and any internal state of the genuine tag is unchanged in the process of replay attack. So replay $(\gamma_1, \gamma_2, \gamma_3) \| A$ fails.

Case ② Replay *B*

The adversary can replay *B* of the previous session to impersonate a tag in current session. On account of (n_1, n_2, n_3) being randomized dynamically and independent in different sessions, the reader cannot verify the consistency between the replay *B* from the adversary and the local *B*'of the genuine reader. So the adversary can be regarded as the fake tag and replay *B* also fails.

Based on the above analysis, replaying $(\gamma_1, \gamma_2, \gamma_3) \| A$ and *B* will not be verified. Hence, LRAP can resist replay attack.

F. Resistance to Counterfeit Attack

Case ① Tag Impersonation Resistance

The adversary tries to impersonate a genuine tag by forging the unknown decryption key K_d' in current session. After receiving the challenge $(\gamma_1, \gamma_2, \gamma_3) \| A$ from the genuine reader, it is impossible for the adversary to decrypt the genuine plaintext (n_1, n_2) from $(\gamma_1, \gamma_2, \gamma_3)$ according to the equations of $(c_1, c_2) = K_d \gamma_3$, $n_1 = \gamma_1 c_1^{-1} \bmod N$ and $n_2 = \gamma_2 c_2^{-1} \bmod N$ because the forged decryption key K_d' is not equal to the genuine decryption key K_d of the genuine tag. Even if the adversary clones a genuine tag, he cannot extract the genuine decryption key K_d and the genuine encryption key K_e since the randomized numbers (n_1, n_2, n_3) are different in each session. The difficulty of obtaining the genuine K_d and K_e is equivalent to attacking PRNG[25] by trying modify-and-test method to guess the genuine value of the random numbers (n_1, n_2, n_3).

Another scenario is: The forged tag may pretend to complete the consistency verfication of *A*' and *A* after receiving the genuine challenge $(\gamma_1, \gamma_2, \gamma_3) \| A$ and then computes the response message *B* by the equation of $B=(n_1 \oplus n_2) + ID$. On account of the mismatch between the forged values of n_1,n_2, *ID* and the geniue values in the genuine reader, it is clear that the genuine reader fails to verify the consistency between *B*' and *B*.

Therefore, Tag Impersonation cannot succeed.

Case② Reader Impersonation Resistance

The adversary tries to impersonate a genuine reader by forging the unknown encryption key K_e' in current session and sends the forged challenge $(\gamma_1, \gamma_2, \gamma_3)' \| A'$ to the genuine tag. After receiving $(\gamma_1, \gamma_2, \gamma_3)' \| A'$, the tag tries to decrypt the genuine plaintext (n_1, n_2, n_3) from $(\gamma_1, \gamma_2, \gamma_3)'$. On account of the forged encryption key K_e' not matching the genuine encryption key K_e, the genuine tag cannot obtain the genuine (c_1, c_2) according to the equation of $(c_1, c_2) = K_d \gamma_3 = K_d n_3 P = n_3 K_d P = n_3 K_e \neq n_3 K_e'$. Similarly, the consistency verification between the local *A*' and the received *A* is also unsuccessful. So the genuine tag regards the adversary as the fake reader.

Even if the adversary clones a genuine reader, the difficulty of obtaining the genuine K_d from K_e according to the equation of $K_e = K_d P$ is equivalent to attacking ECDLP. So it is impossible for the adversary to break through the whole RFID system, including the reader end and the tag end, by cloning a genuine reader.

Therefore, Reader Impersonation cannot succeed.

Hence, based on the above analysis of Case① and Case②, LRAP can defend against both the tag and the reader impersonation attack and has the property of strong unforgeability.

G. Resistance to Desynchronization Attack

The main aim of this attack is to make the tag and the reader update their local parameters respectively to different values, which leads to authenticate each other unsuccessfully for future authentication sessions. In LRAP, during the updating phase the tag stores both the old and the potential new values of Index-pseudonym *IDS* to avoid desynchronization attack. If the response message *B* sent from the tag to the reader are blocked by the adversary, the tag will update its *IDS* while the reader will not update the tag entry. Fortunately, this cannot cause to desynchronized state in our protocol, because the tag stores the updated IDS^{new} and the old IDS^{old} of the previous session. In the next authentication session the tag will respond IDS^{new} to the reader's new challenge, but the reader cannot find the matched tag entry. And then the reader send another challenge to the reader again, the tag will send IDS^{old} as the new response. With this IDS^{old}, the authorized reader can acquire the genuine tag entry from TDS and then carry out the next authentication stages. Therefore the tag and the reader remain synchronization successfully.

Another possible approach to desynchronization attack is to make the reader and the tag update their local data by using different the random numbers n_1 and n_2. But it is easy to be found that the exchanged messages are modified by the adversary over the wireless channel because of data integrity and mutual authentication in our protocol.

Hence, LRAP is immune to desynchronization attack.

VI. Performance Evaluation

In this session, our protocol LRAP is now examined from the point of view of computation cost, storage requirement and communication overhead.

A. Computation Cost

According to the requirement of resource-constrained devices, all the operations used in LRAP are compliant with low-cost tags and can be very efficiently implemented on passive tags in hardware. Because encryption operation is more complex than decryption operation and random number generation to supply freshness is a costly operation for a tag, the operations of PRNG[25], Encryption and Elliptic Curve Point Addition is carried out by the reader and the relative lightweight operations of Decryption operation, Bitwise Addition mod 2^m (+), Bitwise XOR($\oplus$) and Elliptic Curve Point Addition are performed by the tag. The computation cost focuses on the frequency of costly operations about PRNG[25] and Elliptic Curve Point Addition over the reader and the tag respectively.

B. Storage Requirement

In LRAP, each tag stores its static identifier (*ID*), the old pseudonym IDS^{old}, the new pseudonym IDS^{new} and the decryption key K_d. All the strings are L bits (L=96) in compliance with the EPCglobal Gen2 tag used in data deliveries and thus each tag needs storage of 4L bits. *ID* and K_d are static values, thus stored in ROM. IDS^{old} and $IDS^{new}$are stored in a rewritable memory EEPROM for updating in different sessions. The reader stores the pseudonym *IDS* of the corresponding tag in current session and the encryption key K_e, which in total requires 2L bits storage.

C. Communication Overhead

Since the mutual authentication phase contributes most of the communication cost, the communication overhead in LRAP calculates the number of the exchanged messages between the reader and the tag over the wireless channel in one authentication session, which in total demands two challenge-response rounds (4Lbits) in the normal condition.

The comparison between LRAP and the previous relevant protocols is listed in TABLE IV from a performance perspective.

TABLE IV.
PERFORMANCE COMPARISON BETWEEN LRAP AND RELATED RFID AUTHENTICATION PROTOCOLS BASED ON ECC

		ERAP[21]	SECRP[22]	**LRAP**
Elliptic Curve Point Addition Operation Requirement	R	3L	L	2L
	T	3L	3L	2L
Random Number(PRNG) Requirement	R	2L	L	3L
	T	2L	L	0
Total Communication Messages for Mutual Authentication Over R-T Channel		3L	5L	4L

L designates the bit length of variables used (L= 96 bits)

The comparison in TABLE IV indicates that LRAP is superior to ERAP[21] and SECRP[22], especially in computation cost of costly operations over the tag end. Total communication overhead remains between ERAP[21] and SECRP[22]. The storage requirement is similar to these protocols[21, 22]. Hence, computation cost, storage requirement and communication overhead are lightweight except for the relatively light penalty of computation cost at the reader end.

VII. Conclusion

In this paper we propose a lightweight RFID authentication protocol based on ECC, called LRAP, without increasing computing burden at server end. To reduce the computation cost on the tag, our protocol puts the costly operations of PRNG and Encryption over the reader end. The security analysis shows that LRAP can be proven to enhance the essential security properties in RFID system with respect to user privacy against the

potential malicious attacks. The difficulty of attacking our protocol is based on ECDLP. In summary, LRAP is practical, secure and efficient, which makes a proper tradeoff between performace and security. It is expected that the results of this work is not limited to RFID systems but can be applied to other resource-limited environments.

ACKNOWLEDGMENT

This work is supported by the National Natural Science Foundation of China (61373015, 41301407), the Research Fund for the Doctoral Program of Higher Education of China (20103218110017), A Project Funded by the Priority Academic Program Development of Jiangsu Higher Education Institutions(PAPD), the NUAA Fundamental Research Funds (NP2013307), the Fundamental Research Funds for the Central Universities: the Funding of Jiangsu Innovation Program for Graduate Education (CX10B_112Z), the Funding for Outstanding Doctoral Dissertation in NUAA(BCXJ10-07), the Natural Science Foundation of Jiangsu Normal University for Grant(11XLA09), the National Natural Science Foundation of Jiangsu Province(BK20130819), the China Postdoctoral Science Foundation (20100481133) and the National Natural Science Cultivation Foundation of China (NS2012023), under which the present work was possible.

REFERENCES

[1] Y. Zuo, "Survivable RFID Systems: Issues, Challenges, and Techniques," *IEEE Transactions on Systems, Man, and Cybernetics-Part C: Applications and Reviews*, Vol.40, No.4, pp.406-418, 2010.

[2] A. Juels, "RFID Security and Privacy: A Research Survey," *IEEE Journal on Selected Areas in Communications*, Vol. 24, No. 2, pp. 381-394, 2006.

[3] Y. Liu, X. Qin, B. Li, L. Liu, "A Forward-Secure Grouping-proof Protocol for Multiple RFID tags," *International Journal of Computational Intelligence Systems*, Vol.5, No.5, pp.824-833, 2012.

[4] F. Xiao, Y. Zhou, J. Zhou, *et al*, "Security Protocol for RFID System Conforming to EPC-C1G2 Standard," *Journal of Computers*, Vol.8, No.3, pp. 605-612, 2013.

[5] X. Ren, X. Xu, Y. Li, "An One-way Hash Function Based Lightweight Mutual Authentication RFID Protocol," *Journal of Computers*, Vol.8, No.9, pp. 2405-2412, 2013.

[6] Y. Liu, X. Qin, B. Li, L. Liu, "Cryptanalysis of a Scalable Grouping-proof Protocol for RFID Tags," *International Journal of Digital Content Technology and its Applications*, Vol. 6, No. 21, pp. 247- 254, 2012.

[7] S.Vaudenay, "On Privacy Models for RFID," *Proc. Adances in Cryptology (ASIA CRYPT'07)*, LNCS 4833, Springer-Verlag, Berlin, pp. 68-87, 2007.

[8] D. Hein, J. Wolkerstorfer, and N. Felber, "ECC is Ready for RFID—a Proof in Silicon," *In: R. Avanzi, L. Keliher, F. Sica (Eds.): SAC 2008*, LNCS 5381, pp. 401–413, Springer-Verlag, 2009.

[9] Y.-K. Lee, K. Sakiyama, L. Batina, and I. Verbauwhede, "Elliptic Curve based Security Processor for RFID," *IEEE Trans. Comput.* Vol.57, No.4, pp. 1514–1527, 2008.

[10] P. Peris-Lopez, J.C. Hernandez-Castro, J.M. Estevez-Tapiador, and A. Ribagorda, "LMAP: A Real Lightweight Mutual Authentication Protocol for Low-Cost RFID Tags," *Proc. Second Workshop RFID Security*, Graz, Austria, pp.12-14, July, 2006.

[11] P. Peris-Lopez, J.C. Hernandez-Castro, J.M. Estevez-Tapiador, and A. Ribagorda, "EMAP: An Efficient Mutual Authentication Protocol for Low-Cost RFID Tags," *Proc. OTM Federated Conf. and Workshop: IS Workshop (IS'06)*, LNCS 4277, Springer-Verlag, pp. 352–361, Nov. 2006.

[12] P. Peris-Lopez, J.C. Hernandez-Castro, J.M. Estevez-Tapiador, and A.Ribagorda, "M2AP: A Minimalist Mutual-Authentication Protocol for Low-Cost RFID Tags," *Proc. Int'l Conf. Ubiquitous Intelligence and Computing (UIC'06)*, LNCS 4159, pp. 912-923, 2006.

[13] T. Li and R. Deng, "Vulnerability Analysis of EMAP -An Efficient RFID Mutual Authentication Protocol," *Proc. Second Int'l Conf. Availability, Reliability and Security (AreS'07)*, pp. 238-245, 2007.

[14] T. Li and G. Wang, "Security Analysis of Two Ultra-Lightweight RFID Authentication Protocols," *Proc. 22nd IFIP TC-11 International Information Security Conference (IFIP SEC'07)*, Vol. 232, Springer, pp. 109-120, May, 2007.

[15] H. Y. Chien and C. W. Huang, "Security of Ultra-Lightweight RFID Authentication Protocols and Its Improvements," *ACM Operating System Rev.*,Vol. 41, No. 2, pp. 83-86, July, 2007.

[16] J. Wolkerstorfer, "Is Elliptic Curve Cryptography Suitable to Secure RFID Tags?" *Proc. Workshop on RFID and Lightweight Crypto*, Graz, pp. 13-15, July, 2005.

[17] L. Batina, J. Guajardo, T. Kerins, N. Mentens, P. Tuyls, and I. Verbauwhede, "An Elliptic Curve Processor Suitable for RFID-tags," *Cryptology ePrint Archive*, Report2006/227, 2006.

[18] L. Batina, Y.-K. Lee, and S. Seys, D. Singelée and I. Verbauwhede, "Privacy-preserving ECC-based grouping proofs for RFID," *In: Information Security*. Springer Berlin Heidelberg, pp. 159–165, 2011.

[19] C. Lv, H. Li, J. Ma, B. Niu and H. Jiang, "Security Analysis of a Privacy-Preserving ECC-Based Grouping-Proof Protocol," *Journal of Convergence Information Technology*, Vol. 6, No. 3, pp. 113-119, 2011.

[20] W. Ko, S. Chiou, E. Lu and H. Chang, "A Privacy-Preserving Grouping Proof Protocol Based on ECC with Untraceability for RFID," *Applied Mathematics*, Vol. 3 No. 4, pp. 336-341, 2012.

[21] S. I. Ahamed, F. Rahman, and E. Hoque, "ERAP: ECC based RFID Authentication Protocol," *Proc.12th IEEE Int. Work shop on Future Trends of Distrib. Comput. Syst. (FTDCS'08)*, pp. 219–225, 2008.

[22] S. Martınez, M. Valls, C. Roig, J.M. Miret, F. Gin´, "A Secure Elliptic Curve-Based RFID Protocol," *J.Comput.Sci.Tech.* Vol. 24, No. 2, pp. 308–318, 2009.

[23] N. Koblitz, "Elliptic Curve Cryptosystems," *Math. Comp.*, Vol. 48, No. 177, pp. 203–209, 1987.

[24] V. S. Miller, "Use of Elliptic Curves in Cryptography," *Proc. Cryptology-CRYPTO'85*, LNCS 218, Springer-Verlag, Berlin, pp: 417–426, 1986.

[25] P. Peris-Lopez, J. C. Hernandez-Castro, J. M. Estevez-Tapiador and A. Ribagorda, "LAMED – A PRNG for EPC Class-1 Generation-2 RFID Specification," *Computer Standards and Interfaces*, Vol. 31, pp. 88-97, Jan. 2009.

Ya-li Liu was born in Xuzhou Jiangsu, P.R.China, in 1980. She is a Ph.D. Candidate in Nanjing University of Aeronautics and Astronautics, P.R. China. She is currently a Lecturer of Computer Science & Technology College in Jiangsu Normal University. Her main research interests include RFID authentication protocol and privacy protection technology, cryptography theory and its application, network and information security, provable security *etc*. Her recent research has been supported by the Funding of Jiangsu Innovation Program for Graduate Education and the Funding for Outstanding Doctoral Dissertation in NUAA.

Xiao-lin Qin was born in Nanjing Jiangsu, P.R.China, in 1953. He is currently a professor and Ph.D. supervisor in Nanjing University of Aeronautics and Astronautics, P.R. China. His main research interests include data management and security, especially in distributed environment *etc*.

Chao Wang was born in Nanjing Jiangsu, P.R.China, in 1989. He is currently a master in Nanjing University of Aeronautics and Astronautics, P.R. China. His main research interests include information security and privacy protection technology in RFID systems *etc*.

Bo-han Li was born in Yongji Jilin, P.R.China, in 1979. He is currently an associate professor and Master supervisor in Nanjing University of Aeronautics and Astronautics, P.R. China. His main research interests include spatial database, wireless sensor networks *etc*.

APPENDIX

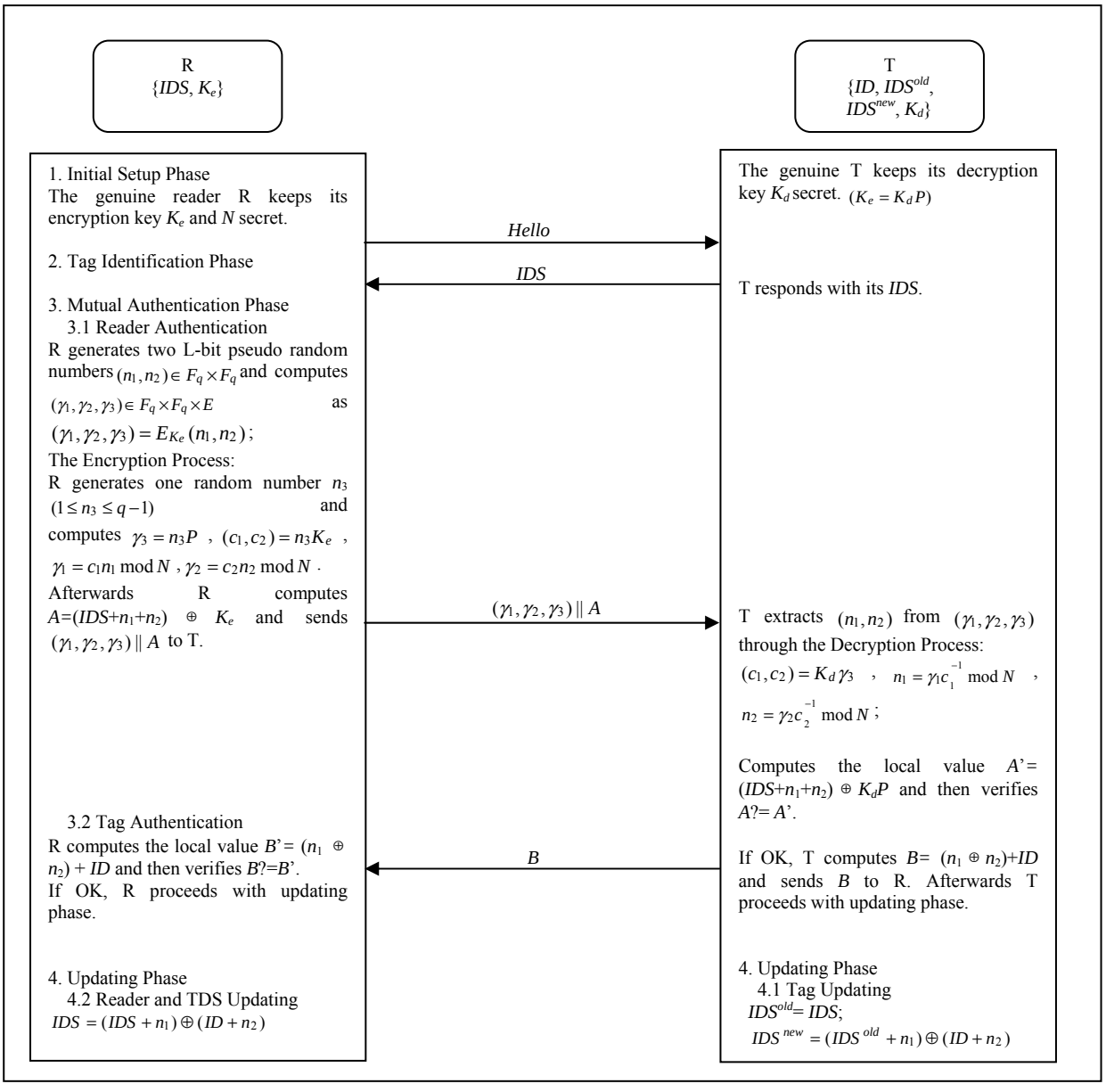

Fig. I. LRAP