Privacy-Preserving and Undeniable Authentication for Mobile RFID Tags

Jiannan Wei
School of Computer Science and Engineering,
Nanjing University of Science and Technology
Nanjing, China
jnwei@njust.edu.cn

Nan Li
School of Electrical Engineering and Computing
The University of Newcastle
Newcastle, Australia
nan.li@newcastle.edu.au

***Abstract*—Radio Frequency IDentification (RFID) is a technology that has been widely employed in many applications requiring automatic object identification. Security and privacy are critical issues that must be addressed when the technology is deployed in security sensitive applications. The prior RFID protocols based on symmetric and asymmetric (or public) key cryptography have limitations in either security or practicality. In particular, public key based RFID protocols can achieve stronger security but are also more expensive in terms of the computation cost. In this paper, we propose a new public key based RFID protocol that incurs much less computation cost compared with the prior protocols. The novelty behind our protocol is to securely reuse public key operations across different sessions so that in most of the sessions only symmetric key operations are required. We show that our protocol can achieve mutual authentication, strong anonymity, forward privacy and non-deniability with low computation and communication cost.**

***Index Terms*—RFID, privacy-preserving, mutual authentication, strong anonymity, non-deniability**

I. Introduction

Radio Frequency IDentification (RFID) is a wireless technology which has been widely used in many applications that require automatic object identification, such as supply-chain, retail, e-payment, and e-passport systems [1], [2]. Recently, it has been shown that the technology can also be applied in cloud data management and longer distance contactless sensing [3].

Security and privacy are among the most important requirements of an RFID system. As mentioned in several recommendations and guidelines for RFID systems, e.g., SEC 2009 585/586 and the NIST special publication [4], security and privacy should be built into RFID applications before their widespread use. One basic security requirement for RFID systems is to ensure tag authentication, that is, the reader identifies the tags in a correct and authenticated manner. Also, since RFID tags are usually attached to moving objects, it is desirable to keep these tags anonymous and untraceable, which is referred to as tag privacy. Due to the contactless access nature of the RFID system, if a tag always responds with the same data when it is queried, the tag can be easily traced.

This work was supported by National Natural Science Foundation of China under Grant 61702268. Jiannan Wei is the corresponding author.

Some additional security requirements for RFID systems have been introduced later due to the wide use of the technology in different new applications. One of the requirements is reader authentication, which means the tag can ensure the reader is the real one. This is important when the reader wants to update some information on the tag. Another requirement is to ensure non-deniability, which means a reader can prove to any third party that a tag has been successfully scanned. It can serve as a proof that a tag and the corresponding object is at a particular location at a certain time when a dispute arises. Such a requirement is desirable in many applications such as supply chain and retail systems.

We should note that most of the security requirements listed above can be achieved using efficient symmetric-key techniques such as cryptographic hash functions or pseudo-random functions. However, the non-deniability requirement requires public key techniques such as digital signature. Below we briefly review some previous works related to RFID authentication.

A. Symmetric Key Protocols

Since RFID tags are lightweight hardware devices, symmetric-key cryptography has been widely used in the design of secure RFID systems. One popular choice is to design RFID authentication protocols based on hash functions. Two typical works are the hash-lock based scheme [5], and the Ohkubo-Suzuki-Kinoshita (OSK) scheme [6] which is based on the idea of a hash chain. Since the OSK scheme can achieve forward privacy, meaning the privacy of an RFID tag in the past communications will still be preserved even if the tag is compromised at a later stage, many hash-chain based RFID protocols (e.g. [7]–[10]) were proposed after the seminal work of OSK [6]. Nevertheless, as mentioned before, symmetric key protocols cannot achieve the non-deniability property which is important in some applications.

B. Public Key Protocols

Public key cryptography, in particular Elliptic Curve Cryptography (ECC), has also been used in the design of many RFID protocols (e.g., [9]–[14]). In [9], [10], public key encryption based RFID protocols were proposed. The authors also showed that their public key based schemes can provide

stronger privacy guarantee than the symmetric-key based approaches when the adversary is able to corrupt the tags and get their internal states. In [12]–[14], several elliptic curve digital signature based RFID protocols were also proposed. Such protocols, in general, can achieve the non-deniability requirement since a tag has to send a digital signature to the reader for authentication. However, the computation cost is a major concern for these protocols since RFID tags have limited computation power.

C. Ownership Transfer and Key Update

In some special applications, an RFID tag could change its owner several times throughout its lifetime. Hence, secure tag ownership transfer is another important research topic in the RFID systems.

In [15], Molnar et al. proposed a pseudonym protocol enabling ownership transfer of RFID tags, which is the first scheme explicitly considering ownership transfer. Since then, many RFID protocols dealing with ownership transfer are proposed (e.g., [16]–[22]).

One essential step in ownership transfer is updating the key/state of an RFID tag so that the previous owner cannot prove his/her ownership of the tag after the successful completion of the ownership transfer protocol. Although we don't deal with ownership transfer in this paper, key update is still a very important step in our protocol in order to achieve the goal of strong anonymity.

D. Motivation and Contribution of This Work

Both symmetric and public key based RFID protocols proposed in the literature have limitations in terms of security or practicality. Symmetric key based protocols are more efficient in computation cost, however, they cannot achieve the non-deniability property since the reader who shares the same secret key with the tag can create any fake proofs. On the other hand, public key based protocols can achieve the non-deniability property when a digital signature based tag authentication mechanism is used. Nevertheless, public key based protocols are much more expensive and hence less practical for RFID tags (particularly passive tags) which are very constrained devices.

The research gap motivated us to develop a new RFID protocol that can achieve non-deniability at a low cost. In this paper, we introduce a novel RFID protocol that can achieve all the security properties mentioned above at a much lower cost than the prior public key based protocols. Below we summarize the properties of our protocol.

- *Non-deniability at a low cost.* The main contribution of our work is a novel approach to realize the non-deniability property under a low cost. In particular, in order to reconcile the conflict between the non-deniability and the efficiency requirements, we propose a novel technique to reuse public key operations in multiple authentication sessions so that in most of the sessions only symmetric key operations are required by an RFID tag. The main difficulty in designing such a protocol is to ensure the security while reusing some components among multiple sessions.
- *Mutual authentication.* Our protocol allows tag and reader to authenticate to each other, and is robust to a variety of man-in-the-middle and interleaving attacks.
- *Strong user anonymity.* Our protocol can not only protect the identity of tag, but also ensure that tag is unlinkable among different sessions. We utilize the designated verifier signature and the hash chain techniques to achieve this goal.
- *Forward privacy.* Forward privacy can ensure that if the tag is exposed, the information transmitted earlier will not be disclosed. Our protocol uses a novel secret updating mechanism to ensure that forward privacy of the tag is ensured for different time epochs.

E. Paper Organization

The rest of the paper is organized as follows. We give the system model for an RFID protocol in Section II, which is followed by the security requirements in Section III. We then present our new RFID protocol in Section IV and analyze its security in Section V. We compare the performance of our protocol with the previous public key based protocols in Section VI, and conclude the paper in Section VII.

II. System Model

A traditional RFID system consists of three components: the tag containing electronic circuits, the reader (transceiver) that scans the tag and a back-end server that maintains tag-related data. An RFID reader transmits electronic waves to the tag to interrogate the data stored in the tag. When the tag is activated, the queried information can be returned.

In our system, for simplicity, we assume there exists a secure channel between the reader and the back-end server. That is, we will treat the reader and the back-end server as a single entity. The reader and the tag are connected via an insure wireless channel. The information transmitted between the tag and the reader is publicly accessible. We also assume that the decisions made by the tag or the reader is public and known to anybody including the adversary. Our system model is shown in Fig. 1.

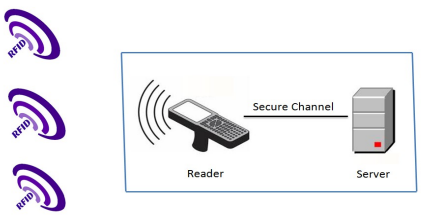

Fig. 1. Our RFID System Model

III. Security Requirement for an RFID System

In this section, we define the security requirements which are the criteria to evaluate the security of an RFID protocol.

We are particularly interested in the following security requirements: mutual authentication, strong anonymity, forward privacy and non-deniability.

- *Non-deniability*: The reader can prove to a third party that tag is indeed involved in the authentication protocol. In particular, a tag cannot deny that it participates in the protocol when a dispute occurs.
- *Mutual authentication*: Mutual authentication means that reader can be successfully authenticated, vice versa. Because the reader needs to ensure that the tag he quires is the real one, tag authentication is a basic security requirement in an RFID system. Reader authentication is important in some environments. For example, when a reader wants to change some information on a tag, the tag must ensure that the information is from a real reader.
- *Strong anonymity*: As mentioned in the introduction, privacy is an important security requirement for RFID systems. In general, we can separate privacy into two parts: weak privacy and strong privacy. The former means hiding the identity of an entity, and the latter is known as traceability or unlinkability, which means an attacker cannot link multiple communication sessions with the same tag.
- *Forward privacy*: It is essential that the current compromised tag information cannot be used to trace the tags previous transmitted information. In this paper, we will focus on forward privacy between different time epochs, which means compromising a tag (obtaining the tags internal state) during a time epoch does not affect the tags privacy in the previous time epochs.

IV. Our New RFID Protocol

In this section, we introduce our RFID protocol which achieves the above security properties. The notion that we use in the protocol is presented in Table I.

TABLE I
NOTATIONS USED IN THE PROTOCOL

Symbol	Definition
R	Reader
T	RFID tag
(x,X)	Private and Public key of tag
(y,Y)	Private and Public key of reader
K_i, $\overline{K}$	Shared secret key between T and R
r	Random number generated by the tag
C	A random challenge from the reader
t	The maximum number of sessions in a time epoch
M_i	A record maintained by the back-end server for tag i

1) *Setup.* In the key generation phase, P is the generator of a cyclic group of order q, choose $x, y \in \mathbb{Z}_q^*$, the private and public key pairs of the tag and the reader are (x, X) where $X = xP$ and (y, Y) where $Y = yP$. We use ID_i to denote the identity of the tag. Let K_i denote a symmetric key shared between the reader and the tag i. The t denote the maximum number of sessions between the reader and the tag in each time epoch. $\{H^m(K_i), H^{m+1}(K_i), \ldots, H^{m+t}(K_i)\}$ is a hash chain maintains for tag i and time epoch $\lfloor m/t \rfloor$(At the setup, we set $m = 0$, $H^0(K_i) = K_i$ and $H^{i+1}(K_i) = H(H^i(K_i))$). Let $\overline{K}$ denote the symmetric key which will be updated by the tag in each session, where $\overline{K} = K_i$ at the setup phase.
2) *Offline Phase.* The tag randomly chooses $r_i \in \mathbb{Z}_q^*$, and sets $R_i = r_i P$, $Q_i = r_i Y$, at the setup or the end of an epoch. This can be performed by the tag when it is offline. If tag i has been successfully identified by the reader, the value of R_i will be included in the record M_i at the back-end server side.
3) *Identification Phase.*
   - *Reader Challenge:* The reader randomly selects a challenge $C \in \{0,1\}^k$ and sends it to the tag.
   - *Tag Response:* After receiving C from the reader, the tag first calculates $v_i = h(R_i, Q_i, \overline{K}, C)$ and $s_i = xv_i + r_i \pmod q$. The tag then sends the pair $(T = \overline{K} \oplus R, s_i)$ to the reader and updates $\overline{K} = H(\overline{K})$.
   - *Tag Authentication:* Upon receiving the response from the tag, the reader authenticates the tag as follows.
     - In the database for the record M_i , search if $R_i \oplus T \in M_i$. If such a record is found, then compute $v' = h(R_i, yR_i, R_i \oplus T, C)$ and check whether $s_i P = v' X_i + R_i$. If the verification is successful, the tag ID_i is successfully identified. The reader checks if the hash chain for the current epoch is used up. If so, update the record M_i to the next epoch and set $b = 1$. Otherwise, set $b = 0$. The reader calculates $Z = h(R_i, yR_i, C, H(R_i \oplus T), b)$ and sends (Z, b) to the tag.
     - Otherwise, if the $R_i \oplus T$ cannot be found in the database, for $i = 1$ to n and $j = 1$ to t, compute $R' = H^{m+j}(K_i) \oplus T$, $v' = h(R', yR', H^{m+j}(K_i), C)$, and check whether $s_i P = v' X_i + R'$. If so, the authentication for tag ID_i is successful. The reader updates $R_i \leftarrow R'$, and checks if the hash chain for the current epoch is used up. If so, update the record M_i to the next epoch and set $b = 1$. Otherwise, set $b = 0$. Compute $Z = h(R, yR, C, H(R' \oplus T), b)$ and sends (Z, b) to the tag. The tag is rejects by the reader, if no tag is identified during the whole loop.
   - *Reader Authentication:* After receiving (Z, b), the tag checks whether $Z \stackrel{?}{=} h(R, Q, C, \overline{K}, b)$. The reader should authenticate itself to the tag.
     - If the equation is true, which means that the reader has also successfully authenticated, the tag accepts the reader. If $b = 1$, which means the hash chain in the reader side has been updated to the next epoch. The *Offline Phase* was performed by the tag to choose a new $r' \in \mathbb{Z}_q^*$ and compute

$R = r'P, Q = r'Y$.

– Otherwise, the authentication of the reader is failed, and the tag performs nothing.

V. Security analysis

We will analyze the security of the proposed RFID protocol in terms of the security requirements defined in Section III.

A. Mutual authentication between tag and reader

For mutual authentication, both tag authentication and reader authentication can be guaranteed in our protocol.

Tag authentication: For the tag authentication, we use the Schnorr signature [23] to achieve this goal. In each session, the reader sends a fresh challenge C to the tag, and the tag sends back an anonymized Schnorr signature (T, s) as a response. Then the reader checks to see if a valid Schnorr signature (R_i, s) can be recovered from the response. For the same time epoch, if the tag has been authenticated successfully before, then the reader has already had the value of R_i, and it can locate this value by a search over the database. Otherwise, the reader has to go through the hash chain for each tag to locate a value R' such that (R', s) form a valid signature. Since the Schnorr signature is existentially unforgeable under chosen message attacks [24], without knowing the private signing key no one can forge a valid signature. Also, since the reader uses a fresh nonce C as a challenge in each session, the attack cannot replay a signature, which has been used by the tag before, in a new session. Thus, we use the unforgeability of the Schnorr signature and the challenge-response mechanism to achieve tag authentication.

Reader authentication: In term of reader authentication, after receiving (Z, b) from the reader, the tag computes $h(R, Q, C, H(\overline{K}), b)$ and checks whether it equals to Z. The reader knows the reader's private key y can compute $yR = rY = Q$. Otherwise, due to the difficulty of the Diffie-Hellman problem, an adversary cannot calculate the value of Q. Also, since the value $\overline{K}$ is updated by the tag in each session, it serves as a nonce to prevent the replay attacks.

B. Strong anonymity of the tag

Strong anonymity of the tag guaranteed in our protocol implies tag anonymity and untraceability. During the execution of the anonymous authentication protocol in the Identification Phase, the response T is never repeated in different sessions although the same R is used during a time epoch (i.e., t sessions). This can be achieved by masking R using a symmetric key $\overline{K}$ shared between the reader and the tag. Since $\overline{K}$ is only known by the reader and the tag is updated in each session using the hash chain, the value of T is independent in different sessions if we treat the hash function as a random function. Also, due to the uniqueness of $\overline{K}$ and C in each session, the values of v and s are also different between different sessions. For the adversary, T and s are just fresh random values in each session. Thus, only the reader who is a designated verifier can recover and verify the signature.

C. Forward privacy

When a tag is compromised, our proposed protocol can achieve forward privacy for all the authentication sessions belonging to the previous time epochs. Forward privacy means that even if a tag is compromised, its privacy in the previous authentication sessions is still well preserved.

The adversary can obtain all the current state information of the tag which includes $(x, Y, X, \overline{K}, r_i, R_i = r_iP, Q_i = r_iY)$ when a tag is compromised during a time epoch. Since the tag updates the value of $\overline{K}$ in each session using a hash-chain, due to the one-wayness of the hash function, from $\overline{K} = H^i(K)$, the adversary cannot derive the previous keys $H^j(K)$. Also, since the values of (r_i, R_i, Q_i) are updated at the end of a time epoch, the adversary is not able to obtain such values for the previous time epochs. Therefore, the adversary is not able to trace the authentication sessions of the tag in the previous time epochs.

Our proposed protocol cannot ensure the forward privacy of a tag within one time epoch. Given the state information $(x, Y, X, \overline{K}, r_i, R_i = r_iP, Q_i = r_iY)$ of a tag, since the value of R is unchanged during a time epoch, the adversary can compute $\overline{K}' = T' \oplus R$ for some T' appeared in a previous authentication session s. The adversary knows that the tag is invloved in the session s if $\overline{K} = H^\ell(\overline{K}')$ for some integer ℓ.

D. Non-deniability

Our protocol can guarantee non-deniability which implies a tag cannot deny that it has involved in an authentication session. Such a property cannot be achieved using symmetric key techniques. Our protocol can achieve this property due to the use of the Schnorr signature for tag authentication. No one except the tag can create a valid signature due to the Schnorr signature is existentially unforgeable [24]. In order to prove that a tag is involved in an identification session, the reader can release $R, Q, \overline{K}$ that occurred in a successfully authenticated session with the communication transcript (C, T, s) to a third party who can check the validity of the signature via the equations $sP = h(R, Q, \overline{K}, C)X + R$ and $T = \overline{K} \oplus R$. In a particular session, the reader does not need to disclose its private key y in order to prove the involvement of a tag.

VI. Performance analysis

We analyze the performance of our protocol and compare it with some public key based protocols proposed in the literature. We will mainly focus on the performance of the tag, due to back-end server connected to the reader is assumed as a powerful device.

A. Computation and communication cost

For computation cost, the tag needs to do 2 exponentiation (i.e., scalar multiplication if implemented using ECC) operations for each time epoch (i.e., t sessions). For each online session, the tag needs to perform 3 hash operations. Therefore, for each time epoch, the tag needs to do a total of 2 exponentiation operations and $3t$ hash operations.

In terms of the communication cost, our protocol requires 3 rounds for mutual authentication in each session. The message length per session is shown in Table III, k=80. Here we assume that both of the hash functions have an output length of $|L|$. For ECC, we have $|L| = 2k$. The total length of the messages exchanged between the reader and the tag is $7k + 1$ bits.

B. Comparison

We compare the security and the performance of our protocol with some existing public key based RFID protocols in Table II and Table III, respectively. From the tables, we can see that our protocol provides strong security but incurs less computation overhead. In particular, our protocol requires a constant number of exponentiation operations in each time epoch, whereas other protocols require a linear number of exponentiation operations.

For the MSP430 family of RFID tags(according to the results of [25], [26]) , one hash function evaluation requires about 0.065ms, while one exponentiation (i.e., scalar multiplication) operation requires roughly 1.6s. We assume that each time epoch has t=10 sessions. We compare the accumulated running time of the tag for T sessions where $T = 10, 20, \ldots, 50$ in Table IV and Fig. 2 .

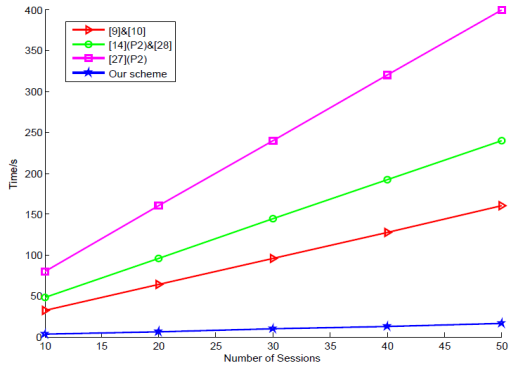

Fig. 2. Tag computation time ($t = 10$)

VII. Conclusion

Firstly, we reviewed the limitations of the existing symmetric key and public key based RFID authentication protocols. We then presented a novel public key based RFID protocol that can achieve all the necessary security requirements including mutual authentication, strong anonymity, forward privacy and non-deniability. The security and performance analysis implies that our protocol achieves strong security but incurs less computation cost compared with other public key based protocols.

Acknowledgment

The authors would like to thank the anonymous reviewers. This work was supported by National Natural Science Foundation of China under Grant 61702268. Jiannan Wei is the corresponding author.

TABLE IV
Tag computation time ($t = 10$)

Number of Sessions	10	20	30	40	50
[9]	32	64	96	128	160
[10]	32	64	96	128	160
[14] (P2)	48.00	96.00	144.01	192.01	240.01
[27] (P2)	80	160	240	320	400
[28]	48	96	144	192	240
Our scheme	3.20	6.40	9.61	12.81	16.01

References

[1] K. Michael and L. McCathie, "The pros and cons of RFID in supply chain management," in *Mobile Business, 2005. ICMB 2005. International Conference on*. IEEE, 2005, pp. 623–629.

[2] A. Juels, D. Molnar, and D. Wagner, "Security and privacy issues in e-passports," in *First International Conference on Security and Privacy for Emerging Areas in Communications Networks, SecureComm 2005, Athens, Greece, 5-9 September, 2005*, 2005, pp. 74–88.

[3] S. Chen, M. Wu, H. Sun, and K. Wang, "CRFID: an RFID system with a cloud database as a back-end server," *Future Generation Comp. Syst.*, vol. 30, pp. 155–161, 2014.

[4] T. Karygiannis, B. Eydt, G. Barber, L. Bunn, and T. Phillips, "Guidelines for securing radio frequency identification (RFID) systems," *NIST Special publication*, vol. 80, pp. 1–154, 2007.

[5] S. A. Weis, S. E. Sarma, R. L. Rivest, and D. W. Engels, "Security and privacy aspects of low-cost radio frequency identification systems," in *Security in Pervasive Computing, First International Conference, Boppard, Germany, March 12-14, 2003, Revised Papers*, 2003, pp. 201–212.

[6] M. Ohkubo, K. Suzuki, and S. Kinoshita, "Efficient hash-chain based RFID privacy protection scheme," in *International Conference on Ubiquitous Computing–Ubicomp, Workshop Privacy: Current Status and Future Directions*, 2004.

[7] G. Avoine and P. Oechslin, "A scalable and provably secure hash-based RFID protocol," in *International Workshop on Pervasive Computing and Communication Security (PerSec)*, 2005, pp. 110–114.

[8] G. Avoine, E. Dysli, and P. Oechslin, "Reducing time complexity in RFID systems," in *Selected Areas in Cryptography*, 2005, pp. 291–306.

[9] S. Vaudenay, "On privacy models for RFID," in *Advances in Cryptolog – ASIACRYPT*, 2007, pp. 68–87.

[10] R.-I. Paise and S. Vaudenay, "Mutual authentication in RFID: security and privacy," in *ASIACCS 2008*, pp. 292–299.

[11] Y. K. Lee, K. Sakiyama, L. Batina, and I. Verbauwhede, "Elliptic-curve-based security processor for RFID," *Computers, IEEE Transactions on*, vol. 57, no. 11, pp. 1514–1527, 2008.

[12] J. Bringer, H. Chabanne, and T. Icart, "Cryptanalysis of EC-RAC, a RFID identification protocol," in *Cryptology and Network Security, 7th International Conference, CANS 2008, Hong-Kong, China, December 2-4, 2008. Proceedings*, 2008, pp. 149–161.

[13] M. Hutter, M. Feldhofer, and T. Plos, "An ECDSA processor for RFID authentication," in *Radio Frequency Identification: Security and Privacy Issues - 6th International Workshop, RFIDSec 2010, Istanbul, Turkey, June 8-9, 2010, Revised Selected Papers*, 2010, pp. 189–202.

[14] N. Li, Y. Mu, W. Susilo, F. Guo, and V. Varadharajan, "Privacy-preserving authorized RFID authentication protocols," in *Radio Frequency Identification: Security and Privacy Issues - 10th International Workshop, RFIDSec 2014, Oxford, UK, July 21-23, 2014, Revised Selected Papers*, 2014, pp. 108–122.

[15] D. Molnar, A. Soppera, and D. Wagner, "A scalable, delegatable pseudonym protocol enabling ownership transfer of RFID tags," in *Selected Areas in Cryptography, 12th International Workshop, SAC 2005, Kingston, ON, Canada, August 11-12, 2005, Revised Selected Papers*, 2005, pp. 276–290.

[16] B. Song, "Rfid tag ownership transfer," in *Proceedings of Workshop on RFID Security, Budapest, Hungary*, 2008.

[17] T. van Deursen, S. Mauw, S. Radomirovic, and P. Vullers, "Secure ownership and ownership transfer in RFID systems," in *Computer Security - ESORICS 2009, 14th European Symposium on Research*

TABLE II
SECURITY COMPARION AMONG PUBLIC KEY BASED PROTOCOLS

Protocol	[9]	[10]	[14] (P2)	[27] (P2)	[28]	Our scheme
Mutual authentication	×	√	×	×	√	√
Strong anonymity	√	√	√	√	√	√
Forward privacy	√	√	√	×	√	√
Non-deniability	×	×	√	√	√	√

TABLE III
PERFORMANCE COMPARISON AMONG PUBLIC KEY BASED PROTOCOLS

Protocol	[9]	[10]	[14] (P2)	[27] (P2)	[28]	Our scheme
Computation (per time epoch)	$2te$	$2te$	$3te$ + $3th$	$5te$	$3te$	2e+3h
Communication round (per session)	2	3	2	3	4	3
Message length	400b	480b	800b	800b	640b	561b

Notations: e – exponentiation, h – hash function evaluation, t – number of sessions in each epoch, b – bit

in Computer Security, Saint-Malo, France, September 21-23, 2009. Proceedings, 2009, pp. 637–654.

[18] K. Elkhiyaoui, E.-O. Blass, and R. Molva, "ROTIV: RFID ownership transfer with issuer verification," in *RFID. Security and Privacy*. Springer, 2011, pp. 163–182.

[19] G. Kapoor and S. Piramuthu, "Single RFID tag ownership transfer protocols," *IEEE Transactions on Systems, Man, and Cybernetics, Part C*, vol. 42, no. 2, pp. 164–173, 2012.

[20] W. Xin, Z. Guan, T. Yang, H. Sun, and Z. Chen, "An efficient privacy-preserving RFID ownership transfer protocol," in *Web Technologies and Applications*. Springer, 2013, pp. 538–549.

[21] N. Li, Y. Mu, W. Susilo, and V. Varadharajan, "Secure RFID ownership transfer protocols," in *Information Security Practice and Experience - 9th International Conference, ISPEC 2013, Lanzhou, China, May 12-14, 2013. Proceedings*, 2013, pp. 189–203.

[22] R. Doss, W. Zhou, and S. Yu, "Secure RFID tag ownership transfer based on quadratic residues," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 2, pp. 390–401, 2013.

[23] C. Schnorr, "Efficient signature generation by smart cards," *J. Cryptology*, vol. 4, no. 3, pp. 161–174, 1991.

[24] D. Pointcheval and J. Stern, "Security proofs for signature schemes," in *Advances in Cryptology - EUROCRYPT '96, International Conference on the Theory and Application of Cryptographic Techniques, Saragossa, Spain, May 12-16, 1996, Proceeding*, 1996, pp. 387–398.

[25] C. Pendl, M. Pelnar, and M. Hutter, "Elliptic curve cryptography on the WISP UHF RFID tag," in *RFID. Security and Privacy - 7th International Workshop, RFIDSec 2011, Amherst, USA, June 26-28, 2011, Revised Selected Papers*, 2011, pp. 32–47.

[26] P. Gope and T. Hwang, "A realistic lightweight authentication protocol preserving strong anonymity for securing RFID system," *Computers & Security*, 2015.

[27] Y. K. Lee, L. Batina, D. Singelée, and I. Verbauwhede, "Low-cost untraceable authentication protocols for RFID," in *Proceedings of the Third ACM Conference on Wireless Network Security, WISEC 2010, Hoboken, New Jersey, USA, March 22-24, 2010*, 2010, pp. 55–64.

[28] R. Peeters, J. Hermans, and J. Fan, "IBIHOP: proper privacy preserving mutual RFID authentication," in *Radio Frequency Identification System Security - RFIDsec'13 Asia Workshop Proceedings, Guangzhou, China, November 27, 2013*, 2013, pp. 45–56.