1-2017

Universally composable RFID mutual authentication

Chunhua SU
Japan Advanced Institute of Science and Technology

Bagus SANTOSO
Institute for Infocomm Research

Yingjiu LI
Singapore Management University, yjli@smu.edu.sg

Robert H. DENG
Singapore Management University, robertdeng@smu.edu.sg

Xinyi HUANG
Fujian Normal University

DOI: https://doi.org/10.1109/TDSC.2015.2434376

Citation

SU, Chunhua; SANTOSO, Bagus; Yingjiu LI; DENG, Robert H.; and HUANG, Xinyi. Universally composable RFID mutual authentication. (2017). *IEEE Transactions on Dependable and Secure Computing.* 14, (1), 83-94. Research Collection School Of Information Systems.
Available at: https://ink.library.smu.edu.sg/sis_research/3341

Universally Composable RFID Mutual Authentication

Chunhua Su, Bagus Santoso, Yingjiu Li, Robert H. Deng, and Xinyi Huang

Abstract—Universally Composable (UC) framework provides the strongest security notion for designing fully trusted cryptographic protocols, and it is very challenging on applying UC security in the design of RFID mutual authentication protocols. In this paper, we formulate the necessary conditions for achieving UC secure RFID mutual authentication protocols which can be fully trusted in arbitrary environment, and indicate the inadequacy of some existing schemes under the UC framework. We define the ideal functionality for RFID mutual authentication and propose the first UC secure RFID mutual authentication protocol based on public key encryption and certain trusted third parties which can be modeled as functionalities. We prove the security of our protocol under the strongest adversary model assuming both the tags' and readers' corruptions. We also present two (public) key update protocols for the cases of multiple readers: one uses Message Authentication Code (MAC) and the other uses trusted certificates in Public Key Infrastructure (PKI). Furthermore, we address the relations between our UC framework and the zero-knowledge privacy model proposed by Deng *et al.* [1].

Index Terms—cryptographic protocol, RFID authentication, universal composability.

1 Introduction

RFID reader/tag mutual authentication is a major theme in RFID security and privacy research. It requires that an RFID tag authenticate itself to a reader and that the reader authenticate itself to the tag such that they are assured of each other's identities. In this paper, we focus on RFID mutual authentication protocols within the Universally Composable (UC) framework. Cryptographic protocols that are secure in the UC framework guarantee that the protocols remain secure even when composed concurrently with an unbounded number of instances of arbitrary protocols. This is known as the strongest (computational) security model for cryptographic protocols. A protocol which is secure under the UC-framework can thus be used to construct a fully trusted functionality under arbitrary protocol composition.

1.1 Related Work and Challenging Issue

The research in RFID security and privacy, especially RFID authentication protocols, is updating rapidly. Most of RFID authentication protocols can be classified into two approaches. One approach is based on symmetric-key techniques such as PRNGs, hash functions and block ciphers. Two typical works of this approach are the hash-lock based scheme [2] and the OSK scheme based on hash chain [3]. The other approach is based on public key techniques. For examples, Tuyls *et al.* proposed a scheme based on Elliptic Curve Cryptography (ECC) [4] and Vaudeney *et al.* proposed schemes based on certain CCA secure public key encryption [5, 6]. The public key based approach may provide stronger privacy guarantees than the symmetric-key based approach in the case of adversary making the corruption of tags and getting their internal states [5, 6].

The security model of RFID authentication protocols is another important issue. Avoine [7] first formalized an adversary model in RFID systems. Based on the adversary model, Juels and Weis defined the notion of strong privacy for analysing the privacy issues in RFID systems [8]. The security definitions in the existing works [7, 8, 9, 6] for RFID authentication protocols are built on the traditional game-based security model. The model first sets the goal of an adversary in RFID authentication, that is, under which conditions the adversary can win; then it models the adversary's attack as a series of queries to some oracles which model the execution of the protocol. The RFID protocol is proved to be secure if the probability of the adversary's success is negligible.

The most related works to ours are the forward formalization of privacy model for RFID systems[10, 11], which present certain RFID authentication protocols and authenticated key-exchange protocols in the UC framework. However, there are still some unclear points in their schemes and it is necessary to provide more concrete security analysis (See Section 3). Furthermore, they only consider the corruption of RFID tags, while in the UC framework, all parties' corruption should be considered. It is thus important for us to formulate the necessary conditions for designing a UC secure RFID mutual authentication scheme and implementing such scheme.

Challenging Issue. The RFID protocols in the related works are secure under the traditional stand-alone model. When those protocols are used in the concurrent way or being composed with other instances of the same or other protocols, they may not be secure anymore. The UC-framework guarantees that a provably secure protocol remains secure no matter it is used as a sub-

- *C. Su is with School of Information Science, Japan Advanced Institute of Science and Technology, 1-1 Asahidai, Nomi, Ishikawa, 923-1292 Japan, and State Key Laboratory of Cryptology, P. O. Box 5159, Beijing, 100878, China. E-mail: chsu@jaist.ac.jp*
- *B. Santoso is with Infocomm Security Department, Institute for Infocomm Research, 1 Fusionopolis Way, Singapore 138632*
- *Y. Li and R-H. Deng are with School of Information Systems, Singapore Management University, 80 Stamford Road, Singapore 178902*
- *X. Huang (Corresponding Author) is with Fujian Provincial Key Laboratory of Network Security and Cryptology, School of Mathematics and Computer Science, Fujian Normal University, Fuzhou, China, 350117, and State Key Laboratory of Cryptology, P. O. Box 5159, Beijing, 100878, China.*

protocol or as an independent protocol. When designing a UC secure RFID authentication protocol, one should not only model an attacker's behavior but also provide a comprehensive security proof by comparing the executions of two protocol processes, a real process and an ideal process. Furthermore, in the UC-secure framework, one should model both tag and reader's corruptions. All of these requirements pose a significant challenge in protocol design and analysis which has not been fully addressed before.

1.2 Our Contributions and Organization

In this paper, we target at UC-secure RFID mutual authentication. Our contributions can be summarized as follows:

1) We provide a stronger security framework for RFID mutual authentication protocol and define an ideal functionality to model the protocol and the adversary's behavior. We work out two ideal functionalities for authenticated key update. Furthermore, we prove that it is impossible to implement UC secure RFID mutual authentication protocol under the plain model (without any extra assumptions) and make further analysis on Le *et al.*'s UC secure protocols [10, 11].
2) We modify the public key encryption-based authentication protocols proposed in [5, 6] into a UC secure mutual authentication protocol. We construct our UC secure protocol based on the common reference string (CRS) which is used to generate a common public key for both reader and tag. Due to the pure theoretical flavor of the UC security framework, we provide certain optimized practical solutions to reduce the communication overhead.
3) We rely on PKI functionality to maintain trusted relationship between reader and tag which involves a trusted third party issuing certification for a legitimate reader to update the public keys in RFID tags as requested in RFID enabled supply chain management. For updating the readers' public keys, we propose two UC-secure key update protocols, of which one is based on Message Authentication Code (MAC) and the other relies on public key certificates in PKI.
4) We refine our preliminary result on the Universal Composable RFID mutual authentication scheme at RFID Sec' 11 Asia and provide a proof that the refined UC-secure RFID mutual authentication scheme satisfies the ZK-privacy proposed by Deng *et al.* at ESORICS 2010.

The organization of this paper. In the next section, we introduce the basic components for RFID mutual authentication and make a comparison between the traditional security model and our model, followed by the formal definition of universal composability framework. In Section 3, we model the functionalities of RFID mutual authentication and authenticated public key update, and show that designing a UC secure protocol for the implementation of an ideal RFID mutual authentication functionality in the plain model is non-trivial. In Section 4, we present our implementations of UC secure protocols for RFID mutual authentication as well as authenticated public key update, together with certain optimized solutions on reducing the communication cost. In Section 5, we provide the security proofs of our protocols under the UC framework. In Section 6, we make a comparison between the well-known ZK-privacy model and our UC-model. At last, we draw conclusions.

2 Preliminaries

In this section, we first give a brief description about RFID mutual authentication protocol, and then we compare the traditional game-based security model with simulation-based security model in UC-framework. After that, we introduce the security definitions in UC-framework, which shall consist of two definitions: firstly, it must specify how an arbitrary, probabilistic, polynomial-time adversary can interact with legitimate participants of a protocol; and secondly, it must state what the adversary should achieve in order to break the security of the protocol.

2.1 RFID Mutual Authentication Protocol

As a malicious reader could obtain unauthorized information from a tag during the tag authentication, so it is an important issue of authenticating the reader as well. As a countermeasure, Tsudik [12] proposed the YA-TRIP and YA-TRAP schemes based on timestamps to do the mutual authentication. An RFID mutual authentication scheme is such that the output is correct except with a negligible probability, it can be described as follows.

1) Initiate a reader R with certain keys for verifying tags' identities.
2) Create a set of tags, each tag T_i having a unique ID_i.
3) Execute a complete protocol between the reader R and a tag T_i, output the tag's ID_i to the reader and verify the reader to the tag.

Here, the reader may have real-time access to a database so as to identify a tag's ID.

There are two general models to formalize the security of interactive protocols: the game-based model and the simulation-based model. Game-based security model used in [9, 5, 6] has the advantages of easy-to-understand and simple-to-apply in the formalization of RFID authentication protocols. Unfortunately, such game-based security modes cannot be used to analyze the security of an RFID protocol when it is used as a sub-protocol in a composite setting.

We want to have an RFID Mutual Authentication with the following properties:

- Completeness: For any good tag and a good reader, in a good session of authentication, both tag and the reader accept each other.
- Soundness (Security against Impersonation): No good reader accepts a bad tag and no good tag accepts a bad reader in a good session of authentication. In a bad session, no good reader accepts a tag (regardless good or bad), and no good tag accepts a reader (regardless good or bad).
- Privacy: No information about a good tag is revealed in an authentication session (regardless good session or bad session).

2.2 Security Definition of UC Framework

A protocol that is secure within the framework [13, 14] proposed by Canetti is called universally composable (UC). We say that the protocol UC realizes the given functionality. In UC framework, a computationally limited entity called the environment $\mathcal{Z}$ has to distinguish between an execution of the protocol with adversary $\mathcal{A}$ and an execution of an ideal functionality with simulator $\mathcal{S}$.

We then say that a protocol π **realizes** an ideal functionality $\mathcal{F}$ if there exists a simulator $\mathcal{S}$ which given access to $\mathcal{F}$ can simulate

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2015.2434376, IEEE Transactions on Dependable and Secure Computing

a run of π with the same input-output behavior. In doing so, $\mathcal{S}$ is given the inputs of the corrupted parties, and the information leaked on the execution of $\mathcal{F}$, and can specify the inputs of corrupted parties. Let $IDEAL_{\mathcal{F},\mathcal{S},\mathcal{Z}}$ and $REAL_{\pi,\mathcal{A},\mathcal{Z}}$ denote the view of environment $\mathcal{Z}$ in ideal world model and real world model, respectively. For any environment $\mathcal{Z}$, it holds:

$$IDEAL_{\mathcal{F},\mathcal{S},\mathcal{Z}} \equiv REAL_{\pi,\mathcal{A},\mathcal{Z}} \tag{1}$$

A protocol that is secure under UC-framework can be run in a network where many different and arbitrary protocols are being executed. $\mathcal{F}$ expects each incoming message to contain a special field consisting of its session ID (SID). That is, each call to a copy of $\mathcal{F}$ and each response from this copy should hold the SID of that copy.

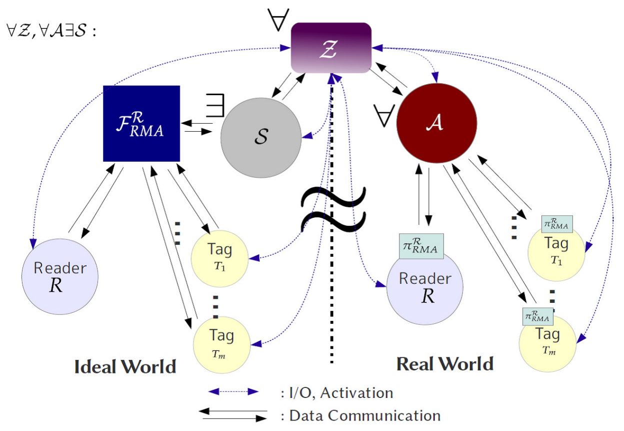
$\forall \mathcal{Z}, \forall \mathcal{A} \exists \mathcal{S}$:
$\forall$
$\mathcal{Z}$
$\mathcal{F}^{\mathcal{R}}_{\text{RMA}}$
$\exists$
$\mathcal{S}$
$\forall$
$\mathcal{A}$
$\approx$
Reader R
Tag T_1
Tag T_m
$\pi^{\mathcal{R}}_{\text{RMA}}$
Reader R
$\pi^{\mathcal{R}}_{\text{RMA}}$
Tag T_1
$\pi^{\mathcal{R}}_{\text{RMA}}$
Tag T_m
Ideal World
Real World
: I/O, Activation
: Data Communication

Fig. 1. The UC model of RFID Mutual Authentication

The Adversarial Power. In the UC RFID model, the adversary can corrupt and take full control of RFID tags and reader at will. The corruption strategy deals with the questions of when and how parties are corrupted. There are two main kinds of corruption:

- ◇ Static corruption: The adversary is given a fixed set of RFID tags or readers of which it controls. Uncorrupted parties remain honest and corrupted parties remain corrupted throughout the protocol runs.
- ◇ Adaptive corruption: Different from the static corruption, adaptive adversaries are given the capability of corrupting RFID tags or readers during the mutual authentication. The choice of which one to corrupt, and when, can be arbitrarily decided by the adversary and may depend on its view of the execution.

In this paper we deal with the static corruptions of RFID tags and readers assuming all the adversaries have polynomial computation capability.

3 The Functionality of RFID Mutual Authentication and Impossibility Result

Generally, the UC frameworl is a security assessment where security is defined by simulation of an ideal process and it is the assurance of secure composition with arbitrary protocol. In Canetti *et al.* [15], the author provide some examples such as of security failures in multiple protocol execution for ZK-knowledge proof or bit commitment. For the mutual RFID authentication in this paper, reader interacts with a tag in two sessions or two tags in one session concurrently. Then there is a potential attack as follows for the three round RFID authentication:

1) Reader sends two challenges c_1 and c_2 to and obtains the authentication corresponds r_1 from tag in session 1.
2) Reader sends a responce of r_1 as it is responce for r_2 in session 2, gets a successful authenticated in the last round with.
3) Then, reader do similarly to tag in session 1, and obtains some additional secret information inside a tag according the protocol specific design.

So we can see that running two instances of the same protocol in parallel is not secure, the similar security risk also applies to a read interacts with two tags concurrently. The security proof is the construction of the simulator, usually, a black box simulator.

3.1 The Ideal Functionality for RFID Mutual Authentication

To properly design a functionality which can model the mutual authentication and the adversary behavior is a very critical before building a excellent implementation. The functionality must model the adversary's attack and what kind of messages the adversary can use. For an ideal functionality, we have to consider the simulator's action inside the ideal functionality and follow three principles as follows:

1) The functionality should capture simulator's affection in the communication between RFID tags and reader in the ideal world. Simulator can be considered as an adversary in the ideal world.
2) The event of communication between two parties is allowed to be informed to the simulator. In the real world model, the message transferred between two parties maybe not be revealed to an adversary due to the security of the encryption system, however, the adversary can know that communication between two parties is going on.
3) The simulator can delay the timing of message transmission. In the real world model, the communication channel can be controlled by the adversary. So in the ideal functionality, the simulator also do the same and delay the message output.

Here, we define the ideal functionality of RFID mutual authentication $\mathcal{F}_{\text{RMA}}$ in Fig.2. Note that one functionality is correspond to one session id sid.

The `InitReader` and `InitTag` procedures can be included in the Setup procedure of real RFID mutual authentication scheme.

$\mathcal{F}_{\text{RMA}}$ is design to guarantees the following security against any static adversary as follows:

- Correctness: any tag and a reader who posses internal data satisfying the relation will get accepted unless the adversary stop the authentication process.
- Security against Impersonation: no tag/reader with internal data not satisfying the relation get accepted. Since in UC framework authentication result always delivered to the correct parties, a Man-In-the-Middle adversary can not make a tag (corrupted or non corrupted) be authenticated and accepted as a different tag.

The Functionality of RFID Mutual Authentication

The functionality $\mathcal{F}_{\mathrm{RMA}}$ is parameterized by a security parameter k and a relation $\mathcal{R}$. It interacts with an adversary $\mathcal{S}$ and a set of RFID tags and a reader.

1) Upon receiving a value (`InitReader, sid`, R, u) from some party R, if no party is recorded the "reader", record R as the "reader", store (R, u) to database, and send (`InitReader, sid`) to adversary. Else, ignore the value.
2) Upon receiving a value (`InitTag, sid`, R, T_i, ID_i, v_i) from some party T_i, if R is recorded as the "reader" and there is no record (R, T_i, ID, v) with any values of ID', v' in the database, store (R, T_i, ID_i, v_i) and send (`InitTag, sid`) to adversary. Else, ignore the value.
3) Upon receiving a message (`Authenticate, sid`, R, T_i) from R or T_i, if (R, u) and (R, T_i, ID_i, v_i) for some value u, ID_i, and v_i are recorded in the database, proceed as below. Otherwise, ignore the message. Generate a random value $r_i \in \{0,1\}^k$ and send (`Authenticate, sid`, $r_i, \mathcal{R}(u, v_i)$) to the adversary.
   3.1 If $\mathcal{S}$ returns (`Both, sid`, r_i) and $\mathcal{R}(u, v_i) = 1$, send (`Result, sid`, ID_i) to R and (`Result, sid, "accept"`) to T_i, otherwise send (`Result, sid, "reject"`) to R and T_i.
   3.2 If $\mathcal{S}$ returns (`ReaderAuthOnly, sid`, r_i) and $\mathcal{R}(u, v_i) = 1$, send (`Result, sid, "accept"`) to T_i, otherwise send (`Result, sid, "reject"`) to T_i. If adversary returns (`TagAuthOnly, sid`, r_i), if $\mathcal{R}(u, v_i) = 1$ send (`Result, sid`, ID_i) to R, otherwise send (`Result, sid, "reject"`) to R.

Fig. 2. The ideal functionality of RFID mutual authentication, $\mathcal{F}_{\mathrm{RMA}}$

- Anonymity: as long as the number of uncorrupted tag is more than one, adversary does not know which uncorrupted tag is being authenticated.
- Wide privacy: although the result of authentication is available to adversary, the adversary can not link the information to any tag unless it corrupts the corresponding tag.

The random value generated in Authenticate serves as the unique identifier for the message to give adversary privilege to delay or to halt the authentication process between the reader and the tag. We allow the adversary to delay or to halt the authentication process partially on one side of the party, e.g., only tag receives the authentication result but the reader does not, as this kind of attack (cut-off-message attack) can not be prevented [1]. The InitReader and InitTag procedures can be included in the Setup procedure of real RFID mutual authentication scheme.

We also consider RFID mutual authentication protocol where the new-joining readers want to update their public keys or authentication related keys into each tag and where the keys are needed to be updated after each authentication for security. We give out the ideal functionality for the key updating operations in Figure 3.

The Functionality of Authenticated Key Update

The functionality $\mathcal{F}_{\mathrm{KeyUpdate}}$ interacts with an adversary $\mathcal{S}$ and a set of RFID tags and some readers.

1) Upon receiving the first message (`RegisterKey`, $sid, K_P, iden_R$) from reader R, send (`Registered`, sid, K_P) to the $\mathcal{S}$; upon receiving ok from $\mathcal{S}$, and if sid is correct and this is the first request from R, then record the pair (`RegisterKey`, $R, iden_R, K_P$).
2) Upon receiving a message (`Update`, $sid, T_i, iden_R$) from reader R, send (`Update`, sid, T_i) to $\mathcal{S}$. After receiving an `ok` from $\mathcal{S}$ and if there is a recorded pair (sid, T_i), output (`NewKey`, sid, K_P) to tag T_i. Else output nothing.

Fig. 3. The ideal functionality of key update, $\mathcal{F}_{\mathrm{KeyUpdate}}$

3.2 Impossibility Result

In this section, we show that the $\mathcal{F}_{\mathrm{RMA}}$ functionality cannot be securely realized in the plain model without using additional cryptographic primitives like a common random string. Canetti *et al.* show broad impossibility results by demonstrating that large classes of two-party functionalities cannot be UC realized in the plain model [16]. The results indicate the security proof problems in the design of existing RFID mutual authentication protocols claimed to be UC secure.

Here, we show that the impossibility result refers to non-trivial protocols, a non-trivial protocol has the property that if the real world adversary delivers all messages and does not corrupt any parties, then the ideal world adversary also delivers all messages (and does not corrupt any parties). Both the reader and the tag are ensured to pass the mutual authentication verifications at the end of a protocol execution (except perhaps with negligible probability), provided that (1) both the reader and the tag use some keys or randomness which satisfy a certain relation; and (2) the adversary passes all messages between reader and tags without modifying them or inserting any message of its own.

Theorem 1. *There does not exist a non-trivial protocol π that securely realizes the functionality $\mathcal{F}_{\mathrm{RMA}}$ in the plain model.*

Proof: Here, we can model all parties as Turing machine. Initially, the environment needs to provide the same inputs to the readers and the tags in the real world model and in the ideal world model. In the real world model, $\mathcal{A}$ can corrupt the tags executing the RFID mutual authentication, also $\mathcal{A}$ would eavesdrop the communication between the readers and the tags and sends it back to the environment $\mathcal{Z}$. In the ideal world, there is a simulator $\mathcal{S}$ which interacts with the ideal functionality $\mathcal{F}_{\mathrm{RMA}}$.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2015.2434376, IEEE Transactions on Dependable and Secure Computing

$\mathcal{S}$ can simulate what $\mathcal{A}$ has seen in the real world and report the simulated messages to $\mathcal{Z}$.

It is not required that ideal adversary to deliver messages which are sent by the ideal functionality to the dummy parties. Our definition concentrates on the security requirements in the case that the protocol generates output, then ?When dummy party receives an input from $\mathcal{Z}$, the input will be copied to the input tape of ideal functionality. Simulator $\mathcal{S}$ has to simulate the output of functionality $\mathcal{F}_{\rm RMA}$ without knowing the input copied to $\mathcal{F}_{\rm RMA}$.

- Every input value $\mathcal{S}$ received from $\mathcal{Z}$ is written on $\mathcal{A}$'s input-tape (as if coming from $\mathcal{A}$'s environment). Likewise, every output value written by $\mathcal{A}$ on its own output-tape is copied to $\mathcal{S}$'s own output-tape (to be read by $\mathcal{S}$'s environment $\mathcal{Z}$).
- When a tag or a reader is corrupted by the adversary in the real world execution, $\mathcal{S}$ shall simulate the corruption in the ideal world. Intuitively, it is difficult for $\mathcal{S}$ to provide a simulation for $\mathcal{Z}$ since $\mathcal{S}$ must send the correct identifiers of the reader and tags to $\mathcal{F}_{\rm RMA}$, while the only way of obtaining information about identifier is through a real execution of the protocol with $\mathcal{Z}$. The simulator must be able to extract the identifiers of the reader and tags from the messages seen by the adversary in the real world.

If there is a match conversation between a tag and a reader (the identities of the tag and the reader match) in the authentication of both real world and ideal world, $\mathcal{Z}$ outputs 1, otherwise $\mathcal{Z}$ outputs 0. When there is no match conversation, $\Pr[\mathcal{Z}$ outputs $0|R = (U, V) \neq 1$ in real world$] = 1 - negl(k)$, where $negl(k)$ is a negligible function, and $\Pr[\mathcal{Z}$ outputs $0|R = (U, V) \neq 1$ in ideal world$] = 1 - negl(k)$. It is difficult for $\mathcal{S}$ to provide a correct simulation for $\mathcal{Z}$ since $\mathcal{S}$ must send correct identities of both the tag and the reader, while its only way of obtaining such information is through a real authentication execution of the protocol with $\mathcal{Z}$. so $\mathcal{S}$ can simulate the output of 0 with the probability with 1/2+negl(k).

The *non-trivial* requirement is necessary since an protocol where no reader and tags can do anything on securely realizing the ideal functionality (note that in the ideal model, the simulator can never generate correct identifiers to the functionality). So we can claim the theorem above.

Analysis of Existing Schemes in UC Framework: RFID mutual authentication schemes under UC-framework are proposed in [10, 11]. They assume the existence of anonymous channels for that RFID security protocol and represent it using the ideal anonymous communication functionality$\mathcal{F}_{\rm com}$. However, the above result on the non-trivial requirement indicates some incompleteness of security proof in the scheme of [10, 11], whose security proof is without the extractability of during the RFID authentication communication. In UC security framework for RFID authentication, the environment $\mathcal{Z}$ can be model as probabilistic polynomial turing machine and its tapes are not copied to both adversary $\mathcal{A}$ and simulator $\mathcal{S}$. The environment $\mathcal{Z}$ generates all the inputs and sends them to the real tags and reader of real world and *dummy* tags and reader in both real work and ideal world.

Here we provide a brief analysis as follows:

1) In the security proof of [10], it is assumed that there is a trusted server which is modeled as an oracle $\mathcal{O}_{\mathcal{S}}$ and creates a database of keys $K_i, i = 1, ..., n$. The simulator can access the oracles in the ideal world simulation, however, in UC security model, the simulator should simulate all the oracles without interaction with them.
2) As in the authentication of [10, 11], both the reader and the tags have secret states during the protocol execution. In UC-framework, r_{tag}, k_{tag} are provided by $\mathcal{Z}$. In their proposal, they are encrypted by a pseudo-random function F, obviously, the simulator $\mathcal{S}$ can not extract r_{tag}, k_{tag} from the messages transferred between the tags and the reader. $F()$ should be a extractable function which allows the simulator to extract the identified information. For the session IDs sid_i and sid_j, the environment $\mathcal{Z}$ easily distinguish if simulator $\mathcal{S}$ fail to simulate the same results of the authentication.

Due to the one-wayness of pseudo-random function, it is impossible to be used to implement a UC secure RFID protocol. So in this paper, we use public key encryption to achieve the extractability and the requirements of UC security.

4 Our Implementations of UC Secure Mutual Authentication

On designing a UC secure protocol, we have to provide a relatively general and minimal assumption that can be realized by a number of quite different and alternative "set-up mechanisms". Here, the common reference string (CRS) model is used in our protocol. In this model, originally proposed in [17], all parties have access to a common string r that was ideally drawn from some publicly known distribution. It acts as a trusted third party which allows parties to register their identities together with an associated public key.

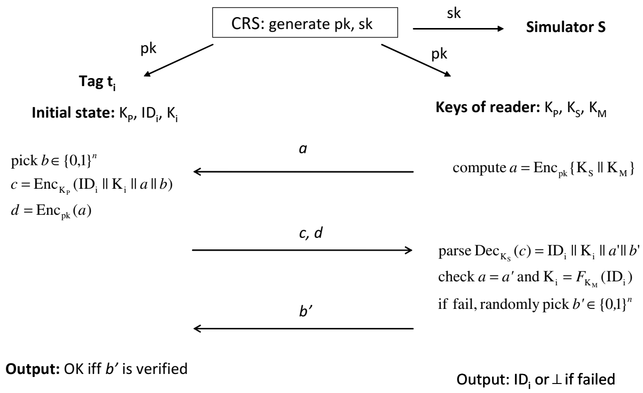
CRS: generate pk, sk
sk
Simulator S
pk
pk
Tag t_i
Initial state: K_P, ID_i, K_i
Keys of reader: K_P, K_S, K_M
a
pick $b \in \{0,1\}^n$
$c = \mathrm{Enc}_{K_P}(\mathrm{ID}_i \,||\, K_i \,||\, a \,||\, b)$
$d = \mathrm{Enc}_{pk}(a)$
compute $a = \mathrm{Enc}_{pk}\{K_S \,||\, K_M\}$
c, d
parse $\mathrm{Dec}_{K_S}(c) = \mathrm{ID}_i \,||\, K_i \,||\, a' \,||\, b'$
check $a = a'$ and $K_i = F_{K_M}(\mathrm{ID}_i)$
if fail, randomly pick $b' \in \{0,1\}^n$
b'
Output: OK iff b' is verified
Output: ID_i or $\perp$ if failed

Fig. 4. The sketch of our protocol

4.1 UC Secure Mutual Authentication Protocol for RFID

We first consider an RFID system comprising of a single legitimate reader R and a set of RFID tags $T_1, ..., T_n$. The reader and the tags are probabilistic polynomial time Turing interactive machine. Typically, each tag is a passive transponder identified by a unique ID and has only limited memory which can be used to store only several keys and/or state information. We modify the protocol from Paise and Vaudenay's scheme [5] based on a CCA-secure Public Key Cryptosystem (PKC). A PKC includes a key generator, an encryption algorithm, and a decryption algorithm. The correctness of a PKC ensures that the decryption of the encryption of any x is always x. The scheme is CCA-secure if all polynomial-time adversaries win the CCA game with negligible advantage. To achieve the extractability, both the reader and the tags use the same public key generated by CRS, which is the minimum condition on the realization of UC secure RFID authentication protocols.

The main issue is that an ideal-model simulator must be able to extract the identifiers from the adversary's input. So we let the reader generate the random challenge as a ciphertext a which contains K_S and K_M. Here, the message d is not sent for verification by the reader but for the simulator to extract K_S so that the protocol can be proved secure under UC-framework. A simulator knowing the associated decryption key can decrypt and obtain the information which is used in the ideal functionality. Note that for a UC protocol, the input is provided by the environment $\mathcal{Z}$. We give a more detailed description of protocol execution in Figure5:

UC Secure RFID Mutual Authentication Protocol π_{RMA}

Common reference string: A pk is generated as a common reference string, where pk is a public key for a CCA-secure encryption scheme Enc.

1) Initially, the environment $\mathcal{Z}$ provides both the tag and the reader with initial states as the inputs for mutual authentication. The reader installs key pair K_P, K_S, K_M and the tag T_i installs K_P. The reader uses a pseudorandom function F and generates $F_{K_M}(ID_i) = K_i$.
2) Upon receiving $(\texttt{InitReader}, sid, K_P, K_S, K_M)$, the reader computes $a = Enc_{pk}(K_S||K_M)$, after that the reader sends $(\texttt{Challenge}, sid, a)$ to the tag T_i.
3) Upon receiving $(\texttt{InitTag}, sid, K_P, ID_i, K_i)$, the tag T_i generates a random nonce $b \in \{0,1\}^n$ and computes $c = Enc_{K_P}(ID_i||K_i||a||b)$ and $d = Enc_{pk}(a)$. Then the tag T_i sends $(\texttt{TagIden}, sid, c, d)$ to the reader.
4) After receiving c, d, the reader computes $Dec_{K_S}(c)$ and parses $ID_i||K_i||a'||b'$; if $a' = a$ and $F_{K_M}(ID_i) = K_i$, outputs ID_i; if not, randomly sets $b' \in \{0,1\}^n$.
5) The reader sends $(\texttt{TagRandom}, sid, b')$ to the tag T_i. The tag checks that whether $b = b'$; if yes, the reader is authenticated.

Fig. 5. UC Secure RFID Mutual Authentication Protocol, π_{RMA}

All tags and readers are connected through point-to-point communication channels. The channels are public, *i.e.*, the adversary $\mathcal{A}$ can read all data transmitted between all parties. The adversary is also responsible for delivering messages.

Optimized Implementations for Achieving Communication Efficiency: For an RFID authentication protocol, the communication of the protocol is the most time-consuming part compared to other tasks such as random number generation, encryption and authentication verification. We can use Elliptic Curve Cryptography as the building block of our protocol without any other cryptographic primitives. The first challenge a which is sent by the reader is a ciphertext with ECC encryption. The challenge could be 300-bit long for the reduction on communication overhead. ID_i could be chosen as 96 bits and K_i be 128 bits. Assuming the reader has real-time access to the database, it can search for the matched pair (ID_i, K_i) in the database. Thus the size of the response message c from the tag can be further reduced as $c = Enc_{K_P}(K_i||a||b)$.

4.2 UC Secure Protocol for RFID Public Key Update

We have already proposed a UC secure protocol for RFID mutual authentication without key update above, hereby we deal with the situations on updating the public keys in the cases of multiple readers. We focus on how to update the tags' keys for further authentication to other readers. The security against relay attack relies on the uniqueness of the session-identifier for each instance of the protocol.

(1) Multiple readers' public key update with message authentication code.

We assume that key update is executed during the reader's authentication to the tag. Here we apply Message Authentication Code (MAC) which is sometimes called a keyed (cryptographic) hash function. The MAC algorithm computes with a secret key and an arbitrary-length message to be authenticated, and outputs a MAC value. The MAC value protects both a message's data integrity as well as its authenticity, by allowing verifiers to detect any change to the message content. Any computationally bounded adversary cannot construct a new legal pair $(m; MAC_k(m))$, even after seeing n legal pairs $(m_i; MAC_k(m_i))$ where $i = 1, 2, ..., n$, except with negligible probability (Fig.6).

UC Secure Protocol for Public Key Update with MAC

Note that this protocol shares the same sid with the corresponding π_{RMA}

1) If a tag T_i is authenticated, the reader computes $e = MAC_{K_i}(b', K'_P)$, where b' is received from the tag T_i in π_{RMA}, and K'_P is a new public key of the reader.
2) The reader sends $(\texttt{KeyUpdate}, sid, K'_P, e)$ to the tag T_i. T_i checks whether $e = MAC_{K_i}(b', K'_P)$, if yes, T_i updates the public key as $K_P = K'_P$.

Fig. 6. UC Secure Protocol for Authenticated Public Key Update with MAC

(2) Multiple readers' public key update with certification.

To realize key update in ubiquitous RFID environments, where readers do not know each other beforehand, we can rely on a Public Key Infrastructure (PKI) for updating multiple readers' public keys with certification. In our model, the certificates from readers hand over their trust element to CA instead of proving the authenticity of digital certificate. Once tags are assured that CA you are dealing with is trust worthy indirectly tags trust in every other certificate the CA guarantees for. In Canetti *et al.*'s [18], a similar UC message authentication protocol based on Certification Authority (CA) is proposed. It first formulates an ideal functionality, $\mathcal{F}_{\mathrm{Cert}}$, that provides the ideal binding of messages to party identities, then it realizes $\mathcal{F}_{\mathrm{Cert}}$ using the signature scheme. In our protocol, we modify it in $\mathcal{F}_{\mathrm{Cert}}$-hybrid model to construction our UC secure key update protocol for multiple readers. Here, we describe the ideal functionality of certification as follows (Fig.7):

Functionality of Certification $\mathcal{F}_{\text{Cert}}$

Signature Generation: Upon receiving a value $(\texttt{Sign}, sid, m)$ from reader R, verify that $sid = (R, sid')$ where sid' is valid session ID. If verification successes, send $(Sign, sid, m)$ to adversary $\mathcal{S}$. Upon receiving $(\texttt{Signature}, sid, m, \sigma)$ from the $\mathcal{S}$, verify that no entry $(m, \sigma, 0)$ recorded. Then output an error message to $\mathcal{S}$ and halt. Else, output $(\texttt{Signature}, sid, m, \sigma)$ to $\mathcal{S}$, and record the entry $(m, \sigma, 1)$.

Signature Verification: Upon receiving a value $(\texttt{Verify}, sid, m, \sigma)$ from some tag T_i, hand $(\texttt{Verify}, sid, m, \sigma)$ to the $\mathcal{S}$. Upon receiving $(\texttt{Verified}, sid, m, \phi)$ from the $\mathcal{S}$, do:

1) If $(m, \sigma, 1)$ is recorded then set $f = 1$.
2) Else, if the reader is not corrupted, and no entry $(m, \sigma', 1)$ for any σ' is recorded, then set $f = 0$ and record the entry $(m, \sigma, 0)$. Else, if there is an entry (m, σ, f') recorded, then set $f = f'$. Else, set $f = \phi$, and record the entry (m, σ', ϕ).

Output $(\texttt{Verified}, sid, m, f)$ to T_i.

Fig. 7. Functionality of Certification $\mathcal{F}_{\text{Cert}}$

The basic idea is to introduce a Certification Authority (CA) in the RFID system to certify the public keys of those readers. Thus, the tag is only required to store the public key certificate of the CA. Whenever the reader wants to update its new public key to the tag, it signs on the new key and sends it together with its certificate. The tag verifies both the certificate of the reader and the signature of the new public key. It accepts the new public key if the verification succeeds. For more details, we present the protocol in Fig.8.

Authentication Key Update Protocol with Certification

1) Upon receiving $(\texttt{NewKey}, K'_P, K'_S)$, reader R first sets $sid' = (R, sid)$ and $m = (K'_P, T_i)$, sends $(\texttt{Sign}, sid', m)$ to $\mathcal{F}_{\text{Cert}}$.
2) Upon receiving the response $(\texttt{Signed}, sid', m, sig)$ from $\mathcal{F}_{\text{Cert}}$, and sends $(\texttt{KeyUpdate}, sid, R, m, sig)$ to tag T_i.
3) After receiving $(\texttt{KeyUpdate}, sid, R, m, sig)$, the tag T_i sets $sid' = (R, sid)$, sets $m' = (K'_P, T_i)$, sends $(\texttt{Verify}, sid', m', sig)$ to $\mathcal{F}_{\text{Cert}}$, and obtains a response $(\texttt{Verified}, sid', m', sig, f)$. If $f = 1$, then T_i updates its public key as K'_P. Else T_i halts without doing anything.

Fig. 8. UC Secure Protocol for Public Key Update with Certification

After the key update, T_i can run the mutual authentication protocol with multiple readers. The size of the certificate depends on the specific use case, for example, a standard X.509 certificate is 268 bytes or 292 bytes long for the key update protocol. Its trust model is centralized and hierarchical certificate management model. The certificate is trusted if the certificate really belongs to the reader shown on the certificate and it is valid if it is trusted and in its valid time period and not being revoked.

5 Proof of UC Security

Protocol π is said to securely realize $\mathcal{F}$ if for every $\mathcal{A}$ there exists an $\mathcal{S}$ such that $\mathcal{Z}$ cannot distinguish whether it is in the ideal world model or in the real world model with any non-negligible advantage over a random guess. Whenever $\mathcal{A}$ corrupts a party, $\mathcal{S}$ corrupts the same dummy party in the ideal process, and provides $\mathcal{A}$ which is activated by $\mathcal{S}$ internally with the internal state of the corrupted party. The environment $\mathcal{Z}$ uses a distinguishing algorithm to distinguish any discrete probability distributions D and D' from one sample and computational resource limit t. The output of $\mathcal{Z}$ is 1, if it decides on D, otherwise it is 0.

We give the security proofs of our protocols as follows:

Theorem 2. *Protocol π_{RMA} of Fig. 4 UC realizes $\mathcal{F}_{\text{RMA}}$ in the F_{CRS}-hybrid model.*

Proof. The formal model for testing whether our protocol realizes the ideal functionality $\mathcal{F}_{\text{RMA}}$ involves an environment $\mathcal{Z}$ that provides inputs to and obtains outputs from either (a) parties running a single execution of the protocol, plus an adversary $\mathcal{A}$ that controls some of the parties and all the communication, or (b) dummy parties that communicate only with $\mathcal{F}_{\text{RMA}}$ by sending it their inputs and receiving the outputs, plus a simulator $\mathcal{S}$ that also interacts with $\mathcal{F}_{\text{RMA}}$.

At first, the simulator $\mathcal{S}$ runs a copy of $\mathcal{A}$, and forwards all messages from $\mathcal{Z}$ to its internal $\mathcal{A}$ and reports them back to $\mathcal{Z}$. The simulator $\mathcal{S}$ proceeds as follows.

Simulating the case that neither the reader nor the tag is corrupted.

In the real world, $\mathcal{A}$ can not get any internal state of both the reader and the tag. For this reason, $\mathcal{A}$ can only obtain the exchanged messages in the communication between the reader and the tag. In the ideal world, the inputs from $\mathcal{Z}$ will be directly sent to $\mathcal{F}_{\text{RMA}}$, so the simulator $\mathcal{S}$ has to simulate only the messages exchanged between the reader and the tag in the real world.

- Before the authentication session, $\mathcal{S}$ can generate the keys and random coins used for both reader and tag before hand.
- Whenever $\mathcal{S}$ receives $(\texttt{ReadIden}, sid)$ from the functionality in the ideal world, it computes $a = Enc_{pk}(K_S||K_M)$ and sends a to its internal adversary A who interacts with $\mathcal{Z}$ as if it is the $\mathcal{A}$ in the real world. Note that K_S, K_M are selected by $\mathcal{S}$, and $\mathcal{Z}$ can not distinguish whether a is generated in the real world or in the ideal world due to the property of CCA-secure encryption.
- Whenever $\mathcal{S}$ receives $(\texttt{TagIden}, sid)$ from the functionality in the ideal world, it generates the key of the tag T_i and computes $c = Enc_{K_P}(ID_i||K_i||a||b)$ and $d = Enc_{pk}(a)$ and sends them to the internal $\mathcal{A}$. Note that ID_i, K_i are selected by $\mathcal{S}$, and $\mathcal{Z}$ can not distinguish whether a is generated in the real world or in the ideal world due to the property of CCA-secure encryption.

Simulating the case that the reader is corrupted and the tag is not corrupted.

$\mathcal{A}$ corrupts the reader in the real world and obtains the secret internal state of the reader. However, the simulator $\mathcal{S}$ cannot gets the internal state of the corrupted tag. The simulation is as follows:

- $\mathcal{S}$ corrupts a reader in the ideal world. Then $\mathcal{S}$ can get $a = Enc_{pk}(K_S||K_M)$ from the corrupted reader. Because $\mathcal{S}$ can get sk from $\mathcal{F}_{\mathrm{CRS}}$, $\mathcal{S}$ can decrypt a to get K_S and K_M. $\mathcal{S}$ uses K_S and K_M as input to the ideal functionality later.
- $\mathcal{S}$ simulates tag's response by computing c, d as if it is generated by $\mathcal{A}$ in the real world execution.
- Finally, $\mathcal{S}$ sends the reader's identifier of K_S and K_M to $\mathcal{F}_{\mathrm{RMA}}$ which outputs the result to environment $\mathcal{Z}$. Because $\mathcal{S}$ can extract the same K_S, K_M used in protocol execution in the real world, $\mathcal{Z}$ will receive the same result as in the real world.

Simulating the case that the tag is corrupted and the reader is not corrupted.

$\mathcal{A}$ corrupts the tag in the real world and gets the secret internal state of the tag. The simulation is as follows:

- $\mathcal{S}$ simulates the reader's random challenge a by selecting K_S and K_M on its own.
- $\mathcal{S}$ can get $c = Enc_{K_P}(ID_i||K_i||a||b)$ and $d = Enc_{pk}(a)$ due to $\mathcal{A}$'s corruption against the reader. $\mathcal{S}$ decrypts d to get a, and then decrypts a to get K_S. Using K_S, $\mathcal{S}$ can decrypts c to get ID_i and K_i.
- Finally, $\mathcal{S}$ sends the tag's identifier of ID_i and K_i to $\mathcal{F}_{\mathrm{RMA}}$ which outputs the result to environment $\mathcal{Z}$.

Tag corrupted by the real world adversary $\mathcal{A}$ encrypts the same challenge a received from the reader and give back the same a obtained from the reader. Thus, the message a that the simulator in the ideal world can decrypt from d which is the same message that $\mathcal{S}$ computed in the first round, which bears no information about the real values of K_S and K_M.

Simulating the case that both the reader and the tag are corrupted.

The simulation is straightforward since $\mathcal{S}$ can extract all the identifiers of the reader and the tag.

Thanks to the CCA-secure encryption scheme with errorless decryption and extractability of the identifiers of the reader and the tag, $\mathcal{Z}$ can not distinguish whether it interacts with $\mathcal{A}$ in the real world or $\mathcal{S}$ in the ideal world, we thus claim the above theorem.

Theorem 3. *Based on the existence of CCA secure encryption, two Protocols for key update in Fig.5 and Fig.7 UC realize* $\mathcal{F}_{\mathrm{KeyUpdate}}$.

Let $\mathcal{A}$ be an adversary that interacts with parties running the protocol in the $\mathcal{F}_{\mathrm{Cert}}$-hybrid model. We construct an ideal-process adversary (simulator) $\mathcal{S}$ such that the view of any environment $\mathcal{Z}$ from an interaction with $\mathcal{A}$ and sba is distributed identically to its view of an interaction with $\mathcal{S}$ in the ideal process for $\mathcal{F}_{\mathrm{KeyUpdate}}$.

(1) Security Proof of the protocol based on MAC: Whenever $\mathcal{A}$ corrupts a reader or a tag, $\mathcal{S}$ corrupts the same reader and tag the ideal process, and provides its internal $\mathcal{A}$ with the internal state of the corrupted party. Because the protocol maintains no secret state at any time, so the simulation is straightforward without $\mathcal{Z}$'s distinguishability.

Because this protocol shares the same session ID sid with π_{RMA}, $\mathcal{S}$ can easily extract b'. As K'_P is transferred in plaintext, $\mathcal{S}$ can compute the same MAC $e = MAC_{K_i}(b', K'_P)$ as if it is generated in the real world.

(2) Security Proof of the protocol based on certification: In our protocol, reader and tag use $\mathcal{F}_{\mathrm{Cert}}$ to do the authentication for public key update. This extraction of reader's identifiers is easy for $\mathcal{S}$ to do because $\mathcal{A}$ works in the $\mathcal{F}_{\mathrm{Cert}}$-hybrid model, and any message sent by $\mathcal{A}$ to $\mathcal{F}_{\mathrm{Cert}}$ is seen by $\mathcal{S}$ during the simulation.

Simulating the reader. When an uncorrupted reader is activated with input $(\mathtt{KeyUpdate}, sid, K'_P)$, $\mathcal{S}$ obtains the new public key from $\mathcal{F}_{\mathrm{Cert}}$. Then, $\mathcal{S}$ simulates for the reader's interaction with $\mathcal{F}_{\mathrm{Cert}}$:

- $\mathcal{S}$ sends to its internal $\mathcal{A}$ the message $(\mathtt{Sign}, (R, sid), (K'_P, T_i))$ from $\mathcal{F}_{\mathrm{Cert}}$, and obtains a signature sig.
- Next, $\mathcal{S}$ sends internal $\mathcal{A}$ the message (sid, R, K'_P, sig), which is sent from the reader to the tag.
- If the reader is corrupted, then what $\mathcal{S}$ can do is to simulate $\mathcal{A}$ for the interaction with F_{Cert}. Whenever a corrupted reader sends a message $(\mathtt{Sign}, sid', K'_P)$ to F_{Cert}, $\mathcal{S}$ responds with $(\mathtt{Sign}, sid'', m'')$ to that reader, obtains a signature sig', and sends $(\mathtt{Signature}, sid'', m'', sig'')$ to the reader.

Simulating the tag. When a reader R delivers a message $(sid, reader, K'_P, sig)$ to an tag T_i, $\mathcal{S}$ first simulates tag's interaction (via $\mathcal{A}$) with $\mathcal{F}_{\mathrm{Cert}}$:

- Send $(\mathtt{Verify}, sid' = (R, sid), m' = (m, T_i), sig)$ to $\mathcal{A}$ (that is, if the reader is corrupted, or m' was signed in the past but with a signature different from sig) then send this message to reader R, and record the response of R.
- $\mathcal{F}_{\mathrm{Cert}}$ would instruct it to output $(\mathtt{Verified}, sid', (K'_P, T_i), sig, f = 1)$ to the tag T_i, and then deliver the message $(\mathtt{NewKey}, sid, K'_P)$ which was sent in the ideal process from $\mathcal{F}_{\mathrm{KeyUpdate}}$ to the tag T_i.

It is straightforward to verify that the simulation is perfect. That is, for any environment $\mathcal{Z}$ and $\mathcal{A}$, it holds that $\mathcal{Z}$'s view of an interaction with $\mathcal{S}$ and $\mathcal{F}_{\mathrm{Cert}}$ is distributed identically to its view of an interaction with parties running the protocol as in the $\mathcal{F}_{\mathrm{Cert}}$-hybrid model. □

5.1 On the practice of our scheme

Here, we discuss about the practical issue of implementing our UC secure framework for RFID tags. We summarized the characteristics of RFID, both active and passive, in the following table.

	active tag	passive tag
Singal	yes	no
Implementation cost	higher	lower
Battery	yes	no
Computation ability	Yes	lower
Cryptographic function	public key	symmetric key

Our UC secure mutual authentication scheme can only be applied to active tags according to requirement of public key encryption. Passive tags are generally smaller than active tags, and will therefore physically fit on a smaller surface area. As with active tags, many new capabilities have been developed for passive tags in recent years. For the implementation of our UC protocol, we can applied the schemes using in [19] which is a set of new, efficient, universally composable two-party protocols for evaluating reactive arithmetic circuits modulo n, where n is a safe RSA modulus of unknown factorization. For each protocol with s be the security parameter, we counted the number of exponentiations with an exponent of at least s bits. We can evaluate the computational to do the exponentiation modulo which is UC secure. It requires about $(90{\cdot}s{+}200{\cdot}\ln n)exp.n{+}(66{\cdot}s{+}40.5{\cdot}\ln n)exp.n^2$, where $exp.n$ is an exponentiation modulo on a tag or reader. Faster operations such as multiplications and divisions can be ignored compared to exponentiation modulo.

6 Arguments on UC and ZK-privacy

In section, we make a comparison of the ZK-privacy model proposed by Deng *et al.* [1]. We notice that if any tagT_i has no ability to create fresh randomness after being corrupted, considering the privacy of tags which have been corrupted is useless in practice. The parties and sets in ZK-privacy model are described as follows.

- $\mathcal{O}$ is a set of oracles consisting $SendTag$, $SendReader$, and $CorruptTag$ oracles.
- $\mathcal{B}$ is a "blinder", a special oracle which allows messages to be sent and received, but does not allow corruption.
- $\mathcal{C}$ is the set of clean tags, i.e., tags which are never been corrupted. $view_{\mathcal{A}}$ consists of (1)all transcripts of communication between $\mathcal{A}$ and the oracles in $\mathcal{O}$, (2)the pair $(b, \mathcal{T}, \mathcal{C})$, and (3)a poly($k$)-bit string $outstr$ which is outputted by $\mathcal{A}$.

Zero Knowledge Privacy: An RFID scheme is zero-knowledge private if for any PPT adversary $\mathcal{A}$ and distinguisher $\mathcal{D}$, there exists a simulator $\mathcal{S}$ s.t. the following is negligible in k.

$$\begin{aligned}&Adv^{ZKP}_{\mathcal{D},\mathcal{A},\mathcal{S}}(k,l,\sigma) :=\\ &\quad |\Pr[\mathcal{D}(Exp^{zkp-adv}_{\mathcal{A}}(k,l,\sigma;\omega_{Setup},\omega_{\mathcal{A}},\omega_{\mathcal{S}});\omega_{\mathcal{D}})=1]\\ &\qquad -|\Pr[\mathcal{D}(Exp^{zkp-sim}_{\mathcal{A}}(k,l,\sigma;\omega_{Setup},\omega_{\mathcal{A}},\omega_{\mathcal{S}});\omega_{\mathcal{D}})=1],\end{aligned} \tag{2}$$

where $l = poly(k)$ and the probability is taken over random coins $\omega_{\mathsf{Setup}}, \omega_{\mathcal{A}}, \omega_{\mathcal{S}}, \omega_g, \omega_{\mathcal{D}}$ used by $Setup()$, adversary $\mathcal{A}$, simulator $\mathcal{S}$, the algorithm choosing g, and distinguisher $\mathcal{D}$ respectively.

Observation. In the second stage, both adversary $\mathcal{A}_2$ and simulator $\mathcal{S}_2$ are limited not to have any access to $\mathcal{C}-\{T_{i_g}\}$. If adversary is allowed to have access, it should be a blind access, otherwise, adversary can corrupt all the rest of clean tags in $\mathcal{C}-\{T_{i_g}\}$. However, if it is blind access, selecting g has no meaning. Note that selecting g here means that if the view of communication between reader and a clean tag T_j is distinguishable to that of communication between reader and a clean tag $T_k \neq T_j$, the simulator must be able to guess g correctly and simulate T_{i_g} accordingly. However, as there is no information on g passed to simulator, thus the only way to satisfy ZKP is that to require that: the view of communication between reader and any clean tag is indistinguishable to that between reader and any other clean tag.

We disassemble ZKP into two notions: simulatable zero knowledge (simulatable ZK) and anonymous zero knowledge (anonymous ZK).

- Intuitively, simulatable ZK is an adaptation of original zero knowledge notion where it only guarantees that the view is simulatable using public information. It guarantees the deniability, i.e., the communication transcript can not be used to ensure a third party that a communication between a tag and a reader has been taken place. But it does not put any restriction on public information, which means that the public information can still contain some information to identify the tags from the view.
- Anonymous ZK is a notion which guarantees that no one can guess the identity of a clean tag among a set of clean tags by communicating blindly with the particular clean tag and/or by corrupting other tags outside the set of clean tags.

We provide the experiment of simulatable zero-knowledge as follows:

Experiment $\mathbf{Exp}^{\mathtt{simzk-adv}}_{\mathcal{A}=(\mathcal{A}_1,\mathcal{A}_2)}(k,\ell,\delta)$

1) $g \leftarrow \$[1,\delta]$
2) $(\mathcal{T}, R, para) \leftarrow \mathsf{Setup}(k,\ell)$
3) $(\mathcal{C}, st) \leftarrow \mathcal{A}_1^{\mathcal{O}}(\mathcal{T}, R, para)$
   $\mathcal{C} = \{T_{i_1},\ldots,T_{i_\delta}\} \subseteq \mathcal{T}, \widehat{\mathcal{T}} := \mathcal{T} - \mathcal{C}$
4) $view_{\mathcal{A}} \leftarrow \mathcal{A}_2^{\mathcal{O}}\left(g, \widehat{\mathcal{T}}, \mathcal{B}\left(T_{i_g}\right), R, st\right).$
5) output $(g, view_{\mathcal{A}})$

Fig. 9. ZK experiment for adversary

Experiment $\mathbf{Exp}^{\mathtt{simzk-sim}}_{\mathcal{S}=(\mathcal{S}_1,\mathcal{S}_2)}(k,\ell,\delta)$

1) $g \leftarrow \$[1,\delta]$
2) $(\mathcal{T}, R, para) \leftarrow \mathsf{Setup}(k,\ell)$
3) $(\mathcal{C}, st) \leftarrow \mathcal{S}_1^{\mathcal{O}}(\mathcal{T}, R, para),$
   $\mathcal{C} = \{T_{i_1},\ldots,T_{i_\delta}\} \subseteq \mathcal{T}, \widehat{\mathcal{T}} := \mathcal{T} - \mathcal{C}$
4) $view_{\mathcal{S}} \leftarrow \mathcal{S}_2^{\mathcal{O}}\left(g, \widehat{\mathcal{T}}, R, st\right)$
5) output $(g, view_{\mathcal{S}})$

Fig. 10. ZK experiment for simulator

The main difference of simulatable ZKP experiments from original ZKP experiments is that in the second stage both the adversary and simulator receive the random value g.

Simulatable Zero Knowledge($\mathtt{simul-zk}$) An RFID scheme is *simulatable zero-knowledge* if for any PPT adversary $\mathcal{A}$ and distinguisher $\mathcal{D}$, there exists a simulator $\mathcal{S}$ s.t. the following is negligible in k.

$$\begin{aligned}&\mathbf{Adv}^{\mathbf{simzk}}_{\mathcal{D},\mathcal{A},\mathcal{S}}(k,\ell,\delta){:=}\\ &\quad \Big|\Pr\left[\mathcal{D}\left(\mathbf{Exp}^{\mathtt{simzk-adv}}_{\mathcal{A}=(\mathcal{A}_1,\mathcal{A}_2)}(k,\ell,\delta;\omega_{\mathsf{Setup}},\omega_{\mathcal{A}},\omega_g);\omega_{\mathcal{D}}\right)=1\right]\\ &\quad -\Pr\left[\mathcal{D}\left(\mathbf{Exp}^{\mathtt{simzk-sim}}_{\mathcal{S}=(\mathcal{S}_1,\mathcal{S}_2)}(k,\ell,\delta;\omega_{\mathsf{Setup}},\omega_{\mathcal{S}},\omega_g);\omega_{\mathcal{D}}\right)=1\right]\Big|,\end{aligned} \tag{3}$$

where $\ell = \mathrm{poly}(k)$ and the probability is taken over random coins ω_{Setup}, $\omega_{\mathcal{A}}$, $\omega_{\mathcal{S}}$, ω_g, $\omega_{\mathcal{D}}$ used by $\mathsf{Setup}(\cdot)$, adversary

$\mathcal{A}$, simulator $\mathcal{S}$, the algorithm choosing g, and distinguisher $\mathcal{D}$ respectively.

Anonymous Zero Knowledge($\mathtt{Anou-zk}$) An RFID system is said to be anonymous zero knowledge if the advantage of adversary defined as follows is negligible for any PPT adversary.

Experiment $\mathbf{Exp}^{\mathtt{anon-zk}}_{\mathcal{A}=(\mathcal{A}_1,\mathcal{A}_2)}(k,\ell,\delta)$

1) $g \leftarrow \$[1,\delta]$
2) $(\mathcal{T},R,para) \leftarrow \mathsf{Setup}(k,\ell)$
3) $(\mathcal{C},st) \leftarrow \mathcal{A}_1^{\mathcal{O}}(\mathcal{T},R,para)$, $\mathcal{C}=\{T_{i_1},\ldots,T_{i_\delta}\} \subseteq \mathcal{T}$, $\widehat{\mathcal{T}} := \mathcal{T}-\mathcal{C}$
4) $g' \leftarrow \mathcal{A}_2^{\mathcal{O}}\left(\widehat{\mathcal{T}},\mathcal{B}\left(T_{i_g}\right),R,st\right)$
5) if $g'=g$ output 1, otherwise output 0.

The advantage of the adversary can be defined as follows:

$$\mathbf{Adv}^{\mathtt{anon-zk}}_{\mathcal{A}}(k,\ell,\delta) := \left|\Pr[\mathbf{Exp}^{\mathtt{anon-zk}}_{\mathcal{A}:=(\mathcal{A}_1,\mathcal{A}_2)}(k,\ell,\delta)=1]-\frac{1}{\delta}\right| \quad (4)$$

Theorem 4. *Simulatable ZK + Anonymous $ZK \Rightarrow ZKP$*

We will prove the theorem by contradiction by showing that if ZKP is not satisfied but simulatable ZK is satisfied, then we can construct an adversary for breaking anonymous ZK.

Proof. The assumptions and preliminaries used in our proof are provided as following:

- Let $\mathcal{A}^{\mathtt{zkp}}$=$(\mathcal{A}_1^{\mathtt{zkp}},\mathcal{A}_2^{\mathtt{zkp}})$ and $\mathcal{D}_{\mathtt{zkp}}$ denote respectively the adversary and distinguisher of ZKP such that for all simulator $\widehat{\mathcal{S}}$, the following holds. $\mathbf{Adv}^{\mathbf{zkp}}_{\mathcal{D}_{\mathtt{zkp}},\mathcal{A}^{\mathtt{zkp}},\widehat{\mathcal{S}}}(k,\ell,\delta) > \epsilon$, where ϵ is non-negligible.
- Let $\mathcal{A}_2^{\mathtt{simzk}}$ denotes a copy of $\mathcal{A}_2^{\mathtt{zkp}}$ with additional **dummy input interface** for g. From the definition of simulatable ZK, we can treat $\mathcal{A}^{\mathtt{simzk}}$:=$(\mathcal{A}_1^{\mathtt{simzk}}(=\mathcal{A}_1^{\mathtt{zkp}}),\mathcal{A}_2^{\mathtt{simzk}})$ as an adversary of simulatable ZK. And since we assume that the simulatable ZK is satisfied, we can assume to have a simulator $\mathcal{S}$:=$(\mathcal{S}_1,\mathcal{S}_2)$ such that $\mathbf{Adv}^{\mathbf{simul-zk}}_{\mathcal{D},\mathcal{A}^{\mathtt{simzk}},\mathcal{S}}(k,\ell,\delta) < \phi$ holds for any distinguisher $\mathcal{D}$, where ϕ is negligible in k. W.l.o.g., we assume $(2^k-1)\phi < \epsilon$.

We construct an adversary of anonymous ZK $\mathcal{A}'$=$(\mathcal{A}'_1,\mathcal{A}'_2)$ as follows: $\mathcal{A}'_1$:=$(\mathcal{A}_1^{\mathtt{simzk}},\mathcal{S}_1)$, $\mathcal{A}'_2 := (\mathcal{D}_{\mathtt{zkp}},\mathcal{A}_2^{\mathtt{simzk}},\mathcal{S}_2)$.

Then procedure of the adversary and simulator can be summarized as follows:

1) We run $\mathcal{A}'_1$ and at the end of the run, we retrieve states $st_{\mathcal{A}}$, $st_{\mathcal{S}}$ from $\mathcal{A}_1^{\mathtt{simzk}}$ and $\mathcal{S}_1$ respectively, and access to $\widehat{\mathcal{T}},\mathcal{B}\left(\mathcal{T}_{i_g}\right),R$.
    - Note that since the simulatable ZK is satisfied and $view_{\mathcal{A}}$ contains the pair $(\widehat{\mathcal{T}},\mathcal{C})$, $\mathcal{A}_1^{\mathtt{simzk}}$ and $\mathcal{S}_1$ are guaranteed to output the same set of clean tags $\mathcal{C}$.
2) For $\overline{g}=1$ to δ, we run the following steps.
    a) We run $\mathcal{A}_2^{\mathtt{simzk}}$ and $\mathcal{S}_2$ with the same input $\overline{g}$ and get $view_{\mathcal{A}}$, $view_{\mathcal{S}}$, as results of $\mathbf{Exp}^{\mathtt{simzk-adv}}_{\mathcal{A}}$, $\mathbf{Exp}^{\mathtt{simzk-sim}}_{\mathcal{S}}$ respectively.
        - All oracle queries from $\mathcal{A}_2^{\mathtt{simzk}}$ and $\mathcal{S}_2$ are forwarded to $\mathcal{O}$ and all answers are forwarded back to $\mathcal{A}_2^{\mathtt{simzk}}$ and $\mathcal{S}_2$ accordingly.
    b) We run $\mathcal{D}_{\mathtt{zkp}}$ with input $view_{\mathcal{A}}$ and randomly chosen random tapes for N times. Then, We run $\mathcal{D}_{\mathtt{zkp}}$ with input $view_{\mathcal{S}}$, and randomly chosen random tapes for N times. Let $p_{adv}(\overline{g})$=$\frac{\#\{\mathcal{D}_{\mathtt{zkp}}(view_{\mathcal{A}})=1\}}{N}$, $p_{sim}(\overline{g})$=$\frac{\#\{\mathcal{D}_{\mathtt{zkp}}(view_{\mathcal{S}})=1\}}{N}$.

At the end, we output $\overline{g}$ such that $|p_{adv}(\overline{g})-p_{sim}(\overline{g})|$ is the smallest.

- Using splitting lemma, with probability $\frac{1}{2}$, we can randomly choose random coins $\omega'_{\mathsf{Setup}},\omega'_{\mathcal{I}},\omega'_{A},\omega'_{S},\omega'_{g}$ such that for any random coin of distinguisher ω_D, the following holds:
$$\mathbf{Adv}^{\mathbf{zkp}}_{\mathcal{D}_{\mathtt{zkp}},\mathcal{A}^{\mathtt{zkp}},\widehat{\mathcal{S}}}(k,\ell,\delta;\omega'_{\mathsf{Setup}},\omega'_{\mathcal{I}},\omega'_{A},\omega'_{\mathcal{S}},\omega'_{g},\omega_D) > \frac{\epsilon}{2} \quad (5)$$
Let we choose such random coins at the beginning.
- Note that if $\overline{g}=g$, then $p_{adv}(\overline{g})$ and $p_{sim}(\overline{g})$ are the estimated values of the probability as follows: $\Pr\left[\mathcal{D}\left(\mathbf{Exp}^{\mathtt{simzk-adv}}_{\mathcal{A}}\left(k,\ell,\delta;\omega'_{\mathsf{Setup}},\omega'_{\mathcal{A}},\omega'_{g}\right);\omega_{\mathcal{D}}\right)=1\right]$ and $\Pr\left[\mathcal{D}\left(\mathbf{Exp}^{\mathtt{simzk-sim}}_{\mathcal{S}}\left(k,\ell,\delta;\omega'_{\mathsf{Setup}},\omega'_{\mathcal{A}},\omega'_{g}\right);\omega_{\mathcal{D}}\right)=1\right]$, respectively. Otherwise, if $\overline{g} \neq g$, they are those of: $\Pr\left[\mathcal{D}\left(\mathbf{Exp}^{\mathtt{zkp-adv}}_{\mathcal{A}}\left(k,\ell,\delta;\omega'_{\mathsf{Setup}},\omega'_{\mathcal{A}},\omega'_{g}\right);\omega_{\mathcal{D}}\right)=1\right]$ and $\Pr\left[\mathcal{D}\left(\mathbf{Exp}^{\mathtt{zkp-sim}}_{\mathcal{S}}\left(k,\ell,\delta;\omega'_{\mathsf{Setup}},\omega'_{\mathcal{A}},\omega'_{g}\right);\omega_{\mathcal{D}}\right)=1\right]$.
- Using Chernoff Bound, we can estimate the lower bound of N so that we can achieve high-precision estimations so that $|p_{adv}(\overline{g})-p_{sim}(\overline{g})|$ for any $\overline{g} \neq g$ is always larger than $|p_{adv}(\overline{g})-p_{sim}(\overline{g})|$ for $\overline{g}=g$ with high probability.

□

Theorem 5. *ZKP $\Rightarrow$ Simulatable ZK + AnonymousZK*

Proof. It is easy to see that ZKP $\Rightarrow$ Simulatable ZK holds. Thus, it is sufficient for us to show that any adversary $\mathcal{A}=(\mathcal{A}_1,\mathcal{A}_2)$ breaking anonymous ZK can be transform into an adversary $\mathcal{A}^{\mathtt{zkp}}=(\mathcal{A}_1^{\mathtt{zkp}},\mathcal{A}_2^{\mathtt{zkp}})$ and a distinguisher $\mathcal{D}$ which can distinguish between $\mathbf{Exp}^{\mathtt{zkp-adv}}_{\mathcal{A}}$ and $\mathbf{Exp}^{\mathtt{zkp-sim}}_{\mathcal{S}}$ for any simulator $\mathcal{S}$.

Let $\mathcal{A}_1^{\mathtt{zkp}}=\mathcal{A}_1$ and $\mathcal{A}_2^{\mathtt{zkp}}=\mathcal{A}_2$. Note that $\mathcal{A}_2^{\mathtt{zkp}}$ can output g (through $outstr$) with non-negligible advantage from$1/\delta$. However, since simulator does not get any information on g, information theoreticaly, simulator can only output the same g with probability $1/\delta$. □

Theorem 6. $\mathrm{IDEAL}_{\mathcal{F}^{\mathcal{R}}_{RMA}} \approx \mathrm{EXEC}_{\pi^{\mathcal{R}}_{RMA}} \Rightarrow \pi^{\mathcal{R}}_{RMA}$ *is ZKP.*

Proof. An environment can ask the adversary to always deliver the communication message between the reader and the tags, and the environment itself is the one who setup the initial data on the tags and the reader. Thus, if such simulator $\mathcal{S}$ does not exist, the environment can easily distinguish between ideal process and real process, contradicting the assumption that protocol $\pi^{\mathcal{R}}_{RMA}$ UC-realizes $\mathcal{F}^{\mathcal{R}}_{RMA}$.

Since $\mathcal{F}^{\mathcal{R}}_{RMA}$ does not give $\mathcal{S}$ any information on any party or interaction between parties, $\mathcal{S}$ must be able to simulate the communication between the reader and the tag without any information from the tag or reader.

We can show that a UC simulator $\mathcal{S}_{UC}$ in the ideal process with functionality $\mathcal{F}^{\mathcal{R}}_{RMA}$ can be used to construct the simulator

$\mathcal{S}^{\mathtt{simzk}}$ to prove simulatable ZK. Let $\mathcal{A}^{\mathtt{simzk}}$=($\mathcal{A}_1^{\mathtt{simzk}}, \mathcal{A}_2^{\mathtt{simzk}}$) be an adversary in $\mathbf{Exp}^{\mathtt{simzk-adv}}_{\mathcal{A}^{\mathtt{simzk}}=(\mathcal{A}_1^{\mathtt{simzk}},\mathcal{A}_2^{\mathtt{simzk}})}$. We can construct $\mathcal{S}^{\mathtt{simzk}}$=($\mathcal{S}_1^{\mathtt{simzk}}, \mathcal{S}_2^{\mathtt{simzk}}$) as follows : $\mathcal{S}_1^{\mathtt{simzk}} = \mathcal{A}_1^{\mathtt{simzk}}$, $\mathcal{S}_2^{\mathtt{simzk}} = (\mathcal{A}_2^{\mathtt{simzk}}, \mathcal{S}_{UC})$. Remind that from the proposition at the previous slide, $\mathcal{S}_{UC}$ must be able to simulate any tag requested by the environment, even without any prior information on the tags and the reader. Therefore, we can use $\mathcal{S}_{UC}$ to simulate the blind access to $\mathcal{T}_{i_g}$ for $\mathcal{A}_2^{\mathtt{simzk}}$.

Assume that $\pi^{\mathcal{R}}_{RMA}$ is not anonymous ZK. We show the construction of an environment $\mathcal{Z}$ which distinguishes ideal process and the real process using adversary of anonymous ZK $\mathcal{A}^{\mathtt{anonZK}}$. $\mathcal{Z}$ uses $\mathcal{A}^{\mathtt{anonZK}}$ as subroutine. First, $\mathcal{Z}$ chooses the random value g and $\mathcal{Z}$ setups the reader and the tags. All oracle queries from $\mathcal{A}^{\mathtt{anonZK}}$ are forwarded to the tags and the reader, and all the answers are forwarded back to $\mathcal{A}^{\mathtt{anonZK}}$. Then, $\mathcal{Z}$ requests the (UC) adversary to act as the blinder $\mathcal{B}$ of T_{i_g}, i.e., deliver any query oracle to T_{i_g}, and report the answer from T_{i_g}.

Notice that since the real process is exactly the same as the experiment of anonymous ZK, $\mathcal{A}^{\mathtt{anonZK}}$ will correctly guess g with non-negligible probability. However, in the ideal process, since the simulator (ideal process adversary) must simulate the blind access to T_{i_g} independently without any related information to T_{i_g}, information theoretically, $\mathcal{A}^{\mathtt{anonZK}}$ can not distinguish whether it is quering T_{i_g} or another tag. Thus, in ideal process, $\mathcal{A}^{\mathtt{anonZK}}$ can only correctly guess g with probability $1/\delta$. □

7 Conclusions

In this paper, we investigated the security definitions of RFID mutual authentication protocols under the UC framework and analyzed the impossibility of implementing a UC secure mutual authentication protocol in the plain model. Due to the extractability requirement, the design of a UC secure RFID mutual authentication protocol turns out to be challenging. We realized that the PKI involving trusted third parties is a necessary condition and that additional information should be sent to guarantee the extractability. The security of RFID mutual authentication and authenticated key update protocols are proved strictly under the UC framework. We also provided formal analysis to bridge ZK-privacy and UC secure framework, which shows that UC-framework implies ZK-privacy. The cryptographic primitives in the proposed UC secure protocols may be too costly to be incorporated into the standard low-cost RFID tags such as EPC Gen 2 tags.ãĂĂNonetheless, we believe that high-end RFID tags can implement the cryptographic components for the UC-security.

Acknowledgment

Chunhua Su is supported by JSPS KAKENHI Grant Number 15K16005. Xinyi Huang is supported by National Natural Science Foundation of China (61472083, U1405255), Program for New Century Excellent Talents in Fujian University (JA14067), Fok Ying Tung Education Foundation (141065), Distinguished Young Scholars Fund of Department of Education, Fujian Province, China (JA13062).

References

[1] R. Deng, Y. Li, M. Yung, and Y. Zhao, "A new framework for rfid privacy," in *Computer Security ESORICS 2010*, ser. Lecture Notes in Computer Science, D. Gritzalis, B. Preneel, and M. Theoharidou, Eds. Springer Berlin Heidelberg, 2010, vol. 6345, pp. 1–18. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-15497-3_1

[2] S. Weis, S. Sarma, R. Rivest, and D. Engels, "Security and privacy aspects of low-cost radio frequency identification systems," in *Security in Pervasive Computing*, ser. Lecture Notes in Computer Science, D. Hutter, G. Muller, W. Stephan, and M. Ullmann, Eds. Springer Berlin Heidelberg, 2004, vol. 2802, pp. 201–212. [Online]. Available: http://dx.doi.org/10.1007/978-3-540-39881-3_18

[3] M. Ohkubo, K. Suzuki, and S. Kinoshita, "Efficient hash-chain based rfid privacy protection scheme," in *In International Conference on Ubiquitous Computing - Ubicomp, Workshop Privacy: Current Status and Future Directions, 2004*, 2007.

[4] P. Tuyls and L. Batina, "Rfid-tags for anti-counterfeiting," in *Proceedings of the 2006 The Cryptographers' Track at the RSA Conference on Topics in Cryptology*, ser. CT-RSA'06. Berlin, Heidelberg: Springer-Verlag, 2006, pp. 115–131. [Online]. Available: http://dx.doi.org/10.1007/11605805_8

[5] R.-I. Paise and S. Vaudenay, "Mutual authentication in rfid: Security and privacy," in *Proceedings of the 2008 ACM Symposium on Information, Computer and Communications Security*, ser. ASIACCS '08. New York, NY, USA: ACM, 2008, pp. 292–299. [Online]. Available: http://doi.acm.org/10.1145/1368310.1368352

[6] S. Vaudenay, "On privacy models for rfid," in *Proceedings of the Advances in Crypotology 13th International Conference on Theory and Application of Cryptology and Information Security*, ser. ASIACRYPT'07. Berlin, Heidelberg: Springer-Verlag, 2007, pp. 68–87. [Online]. Available: http://dl.acm.org/citation.cfm?id=1781454.1781461

[7] F. Armknecht, L. Chen, A.-R. Sadeghi, and C. Wachsmann, "Anonymous authentication for rfid systems," in *Radio Frequency Identification: Security and Privacy Issues*, ser. Lecture Notes in Computer Science, S. Ors Yalcin, Ed. Springer Berlin Heidelberg, 2010, vol. 6370, pp. 158–175. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-16822-2_14

[8] A. Juels and S. A. Weis, "Defining strong privacy for rfid," *ACM Trans. Inf. Syst. Secur.*, vol. 13, no. 1, pp. 7:1–7:23, Nov. 2009. [Online]. Available: http://doi.acm.org/10.1145/1609956.1609963

[9] C. Ma, Y. Li, R. H. Deng, and T. Li, "Rfid privacy: Relation between two notions, minimal condition, and efficient construction," in *Proceedings of the 16th ACM Conference on Computer and Communications Security*, ser. CCS '09. New York, NY, USA: ACM, 2009, pp. 54–65. [Online]. Available: http://doi.acm.org/10.1145/1653662.1653670

[10] M. Burmester, T. Van Le, B. De Medeiros, and G. Tsudik, "Universally composable rfid identification and authentication protocols," *ACM Trans. Inf. Syst. Secur.*, vol. 12, no. 4, pp. 21:1–21:33, Apr. 2009. [Online]. Available: http://doi.acm.org/10.1145/1513601.1513603

[11] T. Van Le, M. Burmester, and B. de Medeiros, "Universally composable and forward-secure rfid authentication and authenticated key exchange," in *Proceedings of the 2Nd ACM Symposium on Information, Computer and Communications Security*, ser. ASIACCS '07. New York, NY, USA: ACM, 2007, pp. 242–252. [Online]. Available: http://doi.acm.org/10.1145/1229285.1229319

[12] G. Tsudik, "A family of dunces: Trivial rfid identification and authentication protocols," in *Privacy Enhancing Technologies*, ser. Lecture Notes in Computer Science, N. Borisov and P. Golle, Eds. Springer Berlin Heidelberg, 2007, vol. 4776, pp. 45–61. [Online]. Available: http://dx.doi.org/10.1007/978-3-540-75551-7_4

[13] R. Canetti, "Universally composable security: A new paradigm for cryptographic protocols," in *Proceedings of the 42Nd IEEE Symposium on Foundations of Computer Science*, ser. FOCS '01. Washington, DC, USA: IEEE Computer Society, 2001, pp. 136–. [Online]. Available: http://dl.acm.org/citation.cfm?id=874063.875553

[14] B. Barak, R. Canetti, J. B. Nielsen, and R. Pass, "Universally composable protocols with relaxed set-up assumptions," in *45th Symposium on Foundations of Computer Science (FOCS 2004), 17-19 October 2004, Rome, Italy, Proceedings*, 2004, pp. 186–195. [Online]. Available: http://dx.doi.org/10.1109/FOCS.2004.71

[15] R. Canetti, "Security and composition of cryptographic protocols: A tutorial," Cryptology ePrint Archive, Report 2006/465, 2006, http://eprint.iacr.org/.

[16] R. Canetti, E. Kushilevitz, and Y. Lindell, "On the limitations of universally composable two-party computation without set-up assumptions," in *Advances in Cryptology EUROCRYPT 2003*, ser. Lecture Notes in Computer Science, E. Biham, Ed. Springer Berlin Heidelberg, 2003, vol. 2656, pp. 68–86. [Online]. Available: http://dx.doi.org/10.1007/3-540-39200-9_5

[17] M. Blum, P. Feldman, and S. Micali, "Non-interactive zero-knowledge and its applications," in *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing*, ser. STOC '88. New York, NY, USA: ACM, 1988, pp. 103–112. [Online]. Available: http://doi.acm.org/10.1145/62212.62222

[18] R. Canetti, "Universally composable signature, certification, and authentication," in *Proceedings of the 17th IEEE Workshop on Computer Security Foundations*, ser. CSFW '04. Washington, DC, USA: IEEE Computer Society, 2004, pp. 219–. [Online]. Available: http://dx.doi.org/10.1109/CSFW.2004.24

[19] J. Camenisch, R. Enderlein, and V. Shoup, "Practical and employable protocols for uc-secure circuit evaluation over $\mathbf{z}_n$," in *Computer Security ESORICS 2013*, ser. Lecture Notes in Computer Science, J. Crampton, S. Jajodia, and K. Mayes, Eds. Springer Berlin Heidelberg, 2013, vol. 8134, pp. 19–37. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-40203-6_2

Chunhua Su received the B.S. degree for Beijing Electronic and Science Institute in 2003 and recieved his M.S. and PhD of computer science from Faculty of Engineering, Kyushu UniversityãĂĂin 2006 and 2009, respectively. He is currently working as an Assistant Professor in School of Information Science, Japan Advanced Institute of Science and Technology.ãĂĂHe has worked as a Scientist in Cryptography & Security Department of the Institute for Infocomm Research, Singapore from 2011-2013. His research areas include algorithm, cryptography, data mining and RFID security & privacy.

Bagus Santoso received his B.E., M.E., and Dr.E. degrees in information and communication engineering from the University of Electro Communications in 2003, 2005, and 2009 respectively. He is a Scientist in Cryptography & Security Department of the Institute for Infocomm Research, Singapore. His current research involves the areas of cryptography and computational number theory. He received the SCIS Paper Prize from IEICE in 2007. He is a member of the International Association for Cryptologic Research.

Yingjiu Li is currently an Associate Professor in the School of Information Systems at Singapore Management University (SMU). His research interests include RFID Security and Privacy, Mobile and System Security, Applied Cryptography and Cloud Security, and Data Application Security and Privacy. He has published over 130 technical papers in international conferences and journals, and served in the program committees for over 80 international conferences and workshops. Yingjiu Li is a senior member of the ACM and a member of the IEEE Computer Society. The URL for his web page is http://www.mysmu.edu/faculty/yjli/

Robert H. Deng has been a Professor at the School of Information Systems, Singapore Management University since 2004. Prior to this, he was Principal Scientist and Manager of Infocomm Security Department, Institute for Infocomm Research, Singapore. His research interests include data security and privacy, multimedia security, network and system security. He was Associate Editor of the IEEE Transactions on Information Forensics and Security from 2009 to 2012. He is currently Associate Editor of IEEE Transactions on Dependable and Secure Computing, and member of Editorial Board of the Journal of Computer Science and Technology (the Chinese Academy of Sciences) and the International Journal of Information Security (Springer), respectively. He is the chair of the Steering Committee of the ACM Symposium on Information, Computer and Communications Security (ASIACCS). He received the University Outstanding Researcher Award from the National University of Singapore in 1999 and the Lee Kuan Yew Fellow for Research Excellence from the Singapore Management University in 2006. He was named Community Service Star and Showcased Senior Information Security Professional by (ISC)^2 under its Asia-Pacific Information Security Leadership Achievements program in 2010.

Xinyi Huang received his Ph.D. degree from the School of Computer Science and Software Engineering, University of Wollongong, Australia. He is currently a Professor at the School of Mathematics and Computer Science, Fujian Normal University, China, and the Co-Director of Fujian Provincial Key Laboratory of Network Security and Cryptology. His research interests include applied cryptography and network security. He has published over 100 research papers in refereed international conferences and journals. His work has been cited more than 1600 times at Google Scholar (H-Index: 23). He is an associate editor of IEEE Transactions on Dependable and Secure Computing, in the Editorial Board of International Journal of Information Security (IJIS, Springer) and has served as the program/general chair or program committee member in over 60 international conferences.