2017

Privacy-Preserving Mutual Authentication in RFID with Designated Readers

Fuchun Guo
University of Wollongong, fuchun@uow.edu.au

Yi Mu
University of Wollongong, ymu@uow.edu.au

Willy Susilo
University of Wollongong, wsusilo@uow.edu.au

Vijay Varadharajan
Macquarie University

Publication Details

Guo, F., Mu, Y., Susilo, W. & Varadharajan, V. (2017). Privacy-Preserving Mutual Authentication in RFID with Designated Readers. Wireless Personal Communications, 1-27.

Privacy-Preserving Mutual Authentication in RFID with Designated Readers

Abstract
We study privacy-preserving mutual authentication in radio-frequency identification systems with designated readers (PP-MADR in short). In PP-MADR, each tag has its designated-reader group instead of all readers, and only tags and their designated readers can authenticate each other. Other readers and adversaries cannot trace tags or know their designated readers. The most challenging task of constructing such a PP-MADR protocol is the verification of reader designation without compromising tag privacy. We found that traditional solutions are impractical due to linear storage growth on tags, linear computation growth on tags, or requiring new key generations for designated readers. In this paper, we show how to construct such an efficient PP-MADR protocol. In our protocol, each tag stores constant-size secret state and performs constant-time computation for mutual authentication. When a tag is created, the server does not generate new private keys for designated readers. Our protocol captures the strong privacy property, where tags cannot be traced and designated readers cannot be distinguished, even if tags are corrupted by adversaries.

Disciplines
Engineering | Science and Technology Studies

Publication Details
Guo, F., Mu, Y., Susilo, W. & Varadharajan, V. (2017). Privacy-Preserving Mutual Authentication in RFID with Designated Readers. Wireless Personal Communications, 1-27.

Journal Paper manuscript No.
(will be inserted by the editor)

Privacy-Preserving Mutual Authentication in RFID with Designated Readers

Fuchun Guo · Yi Mu · Willy Susilo · Vijay Varadharajan

the date of receipt and acceptance should be inserted later

Abstract We study privacy-preserving mutual authentication in Radio-frequency Identification (RFID) systems with designated readers (PP-MADR in short). In PP-MADR, each tag has its designated-reader group instead of all readers, and only tags and their designated readers can authenticate each other. Other readers and adversaries cannot trace tags or know their designated readers. The most challenging task of constructing such a PP-MADR protocol is the verification of reader designation without compromising tag privacy. We found that traditional solutions are impractical due to linear storage growth on tags, linear computation growth on tags, or requiring new key generations for designated readers. In this paper, we show how to construct such an efficient PP-MADR protocol. In our protocol, each tag stores constant-size secret state and performs constant-time computation for mutual authentication. When a tag is created, the server does not generate new private keys for designated readers. Our protocol captures the strong privacy property, where tags cannot be traced and designated readers cannot be distinguished, even if tags are corrupted by adversaries.

Keywords RFID Security · Authentication · Privacy

This work was supported by ARC Project DP110101951.

Fuchun Guo · Yi Mu · Willy Susilo
School of Computing and Information Technology, University of Wollongong, Wollongong NSW 2522, Australia
E-mail: {fuchun,ymu,wsusilo}@uow.edu.au

Vijay Varadharajan
Department of Computing, Macquarie University, Sydney, Australia
E-mail: vijay.varadharajan@mq.edu.au

1 Introduction

Privacy-preserving mutual authentication addresses the security and privacy issues in Radio-frequency Identification (RFID) systems. In such an authentication protocol, readers and tags can authenticate each other. It also hides the identities of tags against adversaries who cannot authenticate them. The existing privacy-preserving mutual authentication protocols can be classified into weak privacy based on symmetric cryptography (e.g., [11,14]) and strong privacy based on public-key cryptography (e.g., [40,1]). Roughly speaking, for weak privacy, the tag privacy will be compromised (can be traced) once the secret state on the tag is known; while for strong privacy the tag cannot be traced, even if the adversary corrupts the tag and obtains the secret state on it.

An RFID system consists of the three components: tags, readers and a backend server. We found that all existing mutual authentication protocols in the literature consider all readers as a single entity. This assumption, however, has at least two drawbacks. First, it cannot preserve tag privacy because all readers can identify tags. Second, if a reader is corrupted, the privacy of all RFID tags will be compromised. This single-entity assumption is accompanied by high-risk privacy issue. The potential solution to address these drawbacks is privacy-preserving mutual authentication with designated readers (PP-MADR). That is, each tag has its designated readers (in a group of readers), such that only the tag and its designated readers can authenticate each other. While for other readers and adversaries, they cannot trace tags or know their designated readers.

A PP-MADR protocol should consist of a reader authentication and a tag authentication. However, it is a daunting task to propose a PP-MADR protocol especially for reader authentication with preserved privacy. The tag must verify the reader is one of its designated readers without leaking any private information to readers, who are potential none designated readers or adversaries. We found traditional solutions require linear storage growth on a tag, or linear computation growth on a tag, or new key generations for designated readers to identify a new created tag. These solutions are impractical as RFID tags are passive with limited storage, and the number of tags could be huge in an RFID system.

1.1 Related Work

RFID authentication with preserved tag privacy has been widely studied in the last decade. Most of them focused on tag authentication and some of them were proposed for mutual authentication. The existing authentication protocols can be classified into the following two types.

The first type (e.g., [25,36,38,2,11,28,20,9,3,4,14,15]) is based on symmetric cryptography, using pseudo-random function and hash function, which offer a very efficient computation with a low cost.

The second type (e.g., [43,8,40,39,10,42,34,41]) is based on public-key cryptography, such as Elliptic Curve Cryptography (ECC). In this type, tags are required to perform exponentiations or point multiplications. Although public-key cryptography is more expensive compared to symmetric cryptography, Lee *et al.* [32] and Hein *et al.* [22] have shown that the ECC can be now realized on RFID tags.

Several privacy models [26,43,40,10,23,13] in the context of RFID have been proposed. In these privacy models, adversaries are divided into different classes, depending on restrictions regarding which oracles they can access. Among these privacy models, the notion of strong privacy provides the strongest privacy where no adversary can identify or trace a tag, even given all secrets stored on the tag [41]. However, only authentication protocols based on public-key cryptography can achieve strong privacy. When a tag is corrupted, symmetric-based authentication protocols can no longer preserve tag privacy because all tag communications are identifiable with the secret on the tag.

Several RFID authentication protocols were proposed to achieve strong privacy. Bringer *et al.* [8] and Liu and Ning [34] proposed zero-knowledge based authentication protocols. Peeters and Hermans [41] proposed more efficient protocols with the same technique. Vaudenay [43] firstly proposed a tag authentication protocol based on a generic public-key encryption (PKE) with a formal security proof. Paise and Vaudenay [40] extended the tag authentication in [43] to mutual authentication. For more efficient authentication, Canard *et al.* [10] proposed hash ElGamal based protocol. Oren and Feldhofer [39] and Saarinen [42] respectively used randomized Rabin encryption in protocol design. There are also some other authentication protocols [12,30,31,29] based on public-key cryptography, but they are later found insecure in [8,17, 35].

Very recently, Nan *et al.* [33] in *RFIDSec 2014* introduced privacy-preserving authorized RFID authentication protocols. The proposed protocols have the same motivation as the PP-MADR protocol in tag authentication for those authorized/designated readers only. However, this work didn't consider reader authentication. The proposed protocols mainly focused on how to let an online server authorize readers in tag authentication but the server does not know which tag is being authenticated. We note that our PP-MADR protocol does not requires an online server and hence the corresponding problem does not exist.

1.2 Our Contribution

In this work, we propose an efficient PP-MADR protocol with strong privacy. In comparison with trivial solutions and previous solution, our PP-MADR protocol captures the following nice features.

- The secret state stored on a tag is constant-size and independent of the number of tag's designated readers. It costs only a storage of several kilo bits.

- The computational cost on a tag for reader authentication is very small. We achieve this property by transferring most computations to readers.
- The computational time on a tag in mutual authentication is constant. If a reader is one of tag's designated readers, it can identify the tag via one mutual authentication.
- There is no new key generation for readers. In our protocol, the RFID system server does not need to compute new private keys for designated readers when creating a new tag. Each reader has one private key only.
- The privacy of a tag and its designated readers is well preserved. Our tag cannot be traced from mutual authentication, and designated readers are anonymous, even if the adversary obtains the secret state on the tag.

We evaluate our protocol in terms of computational cost, storage cost and hardware cost. The result shows that our protocol exhibits the above nice features without significantly increasing cost.

The rest of this is organized as follows. In Section 2, after formulating the requirements of PP-MADR, we introduce some solutions towards PP-MADR and the framework of ours. The algorithms of our solution are formalized in Section 3. Our PP-MADR scheme is proposed in Section 4, with security and privacy analysis in Section 5. We evaluate our scheme in Section 6, and conclude this work in Section 7.

2 The Solutions of PP-MADR

In privacy-preserving mutual authentication with designated readers (PP-MADR), each reader is assumed to be an independent entity. When a tag is created, some readers are selected and designated to identify this tag. A proposed PP-MADR protocol should satisfy the following properties:

1. For security, tags and their designated readers can authenticate each other.
2. For privacy, tags and their designated readers should be indistinguishable (cannot be traced) against other readers and adversaries.

A PP-MADR protocol is composed of reader authentication and tag authentication. We note that reader authentication in PP-MADR protocol should not only verify reader identity but also reader designation. I.e., the reader is one of designated readers. In the PP-MADR protocol, the reader authentication must be completed before the tag authentication; otherwise, the privacy of tags will be easily compromised.

Tag authentication with strong privacy has been well studied in the literature such as [40, 1, 23, 33]. In the following of this section, we propose a tag authentication protocol from identity-based cryptography, and introduce some solutions to reader authentication. After the analysis of these solutions, we propose the framework of our PP-MADR protocol.

2.1 Tag Authentication

The given tag authentication is associated with the following notations.

T:	The identity of a tag.
ID:	The identity of a reader.
MPK:	A master public key.
msk:	The master secret key of MPK.
w:	Random number.
d_T:	The private key of tag T.
d_{ID}:	The private key of reader ID.
σ_w:	Identification proof on w computed with d_T.
IBE:	Identity-based encryption.
$\mathbb{I}$:	A group of readers $\{ID_1, ID_2, \cdots, ID_k\}$.

In PP-MADR protocol, each reader is an independent entity. We cannot assume there exists a unique secret key shared by a tag and a reader as it will give a large number of keys stored on both tags and readers. We therefore adopt a tag authentication from identity-based encryption.

Identity-based encryption (IBE) [6] is a variant of PKE. There is a master key pair (MPK, msk), known as master public key and master secret key respectively (generated and kept by the RFID system server). In such a scheme, the public key of a user (e.g. reader) is the user's identity ID, while the private key d_{ID} is generated from ID and msk. When a message is encrypted with ID, it requires the private key d_{ID} of ID for successful decryption.

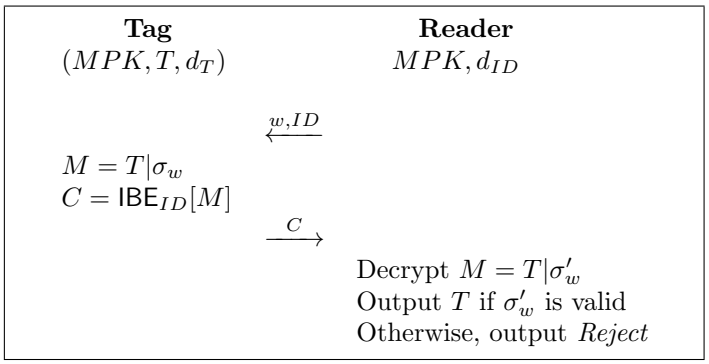

Fig. 1 The tag authentication from IBE.

The tag authentication works as follows. Upon receiving an authentication query (w, ID) from a reader ID, where w is a random number, the tag T runs an IBE encryption to encrypt (T, σ_w) with identity ID. Here, T is the identity of tag and σ_w is the corresponding identification proof[1]. Next, the ciphertext is sent to the reader. Finally, the reader decrypts (T, σ_w) using d_{ID}, and verifies the tag T through checking the identification proof σ_w. The tag authentication is depicted in the Fig 1.

[1] We can use a digital signature scheme to generate such a proof using the private key d_T of tag.

The response of tag is a ciphertext. Without a valid private key, the ciphertext cannot be successfully decrypted. Therefore, even if the adversary obtains the secret state on a tag, the tag still cannot be traced from the tag authentication (the view of ciphertext).

2.2 Reader Authentication

In PP-MADR protocol, the above tag authentication must be carried out after the reader authentication. I.e., the reader is ID and ID is one of tag T's designated readers.

We note that it is not hard to verify the identity of reader. For example, we can achieve reader identification from the above modified tag authentication. Instead of encrypting a message M, the tag encrypts a random number R. The reader proves its identity if it can decrypt and send R back to the tag.

The challenging task is the verification of reader designation. Let $\mathbb{I}_1, \mathbb{I}_2, \cdots, \mathbb{I}_L$ be all designated-reader groups known by all readers. At the beginning of reader authentication, the reader does not know which group was chosen for the tag. If we allow the tag to disclose its designated readers, the verification of reader designation can be quite simple and efficient. For example, we use a secure collision-resistant hash function H. The tag stores the hash value $h_{\mathbb{I}}$ of $\mathbb{I}$, and the reader proves that $ID \in \mathbb{I}$ and $H(\mathbb{I}) = h_{\mathbb{I}}$. It is easy for the tag to conduct these two verification. Unfortunately, this solution does not preserve tag privacy as their designated readers are disclosed. All adversaries can easily compromise tag privacy by launching a reader authentication.

For all solutions without disclosing $\mathbb{I}$, the reader must guess $h_{\mathbb{I}}$ in tag before conduct the proof of $ID \in \mathbb{I}$ and $H(\mathbb{I}) = h_{\mathbb{I}}$ to tag. Upon receiving such a proof, if $h_{\mathbb{I}}$ is the tag's reader group, the tag runs the mutual authentication as Fig 1 by encrypting $T|\sigma_w|R$. Otherwise, tag must still perform encryption by encrypting dummy identity to resist guessing attack on reader identity because any adversary can provide a proof of $ID \in \mathbb{I}$ and $H(\mathbb{I}) = h_{\mathbb{I}}$ to tag. We note that the mutual authentication time could be impractical due to the computation on tag especially when the reader is designated in N different reader groups $\mathbb{I}_1, \mathbb{I}_2, \cdots, \mathbb{I}_N$.

Another problem in the above solutions without disclosing designated readers is the tag privacy. When $\mathbb{I}$ or $h_{\mathbb{I}}$ is stored on the tag, the privacy about its designated readers will be compromised when the tag is corrupted and the adversary obtains the secret state on the tag. Hence, the secret state stored on tags must not reveal $\mathbb{I}$ in order to achieve strong privacy against adversaries who can corrupt tags.

Another potential way which is completely different from above solutions is generating unique keys associated with T and ID for reader ID, if the reader is designated to identify the tag T. For example, the server generates private key $d_{T|ID}$ for reader ID to identify the tag T, where the tag encrypts M using identity $T|ID$ (IBE) to respond query from ID. This solution, however, requires the RFID system server to generate new private keys for all designated

readers when a new tag is created. This new key generation therefore is also impractical for reader authentication.

2.3 Our PP-MADR Solution (Framework)

The construction of our PP-MADR protocol takes all above factors into account. That is, we should address the problems of liner growth of storage, linear growth of computation overhead, new key generation and privacy information leakage due to corruption.

To avoid all these drawbacks, we design the protocol in the following way. Firstly, an anonymous and short group token GT is computed to represent $\mathbb{I}$ for tag T. The anonymity means the adversary cannot distinguish designated readers from GT. Then, the secret state (T, d_T, GT) are uploaded to the tag. Finally, we construct the mutual authentication as follows (Fig 2).

Tag		**Reader**
(T, d_T, GT)		$MPK, d_{ID}, \mathbb{I}$
	$\xleftarrow{w, ID}$	
$M = R\|T\|\sigma_w$ $C = \mathsf{E}_{ID,\mathsf{GT}}[M]$ Store (ID, R)		
	$\xrightarrow{C}$	
		Decrypt $M = R'\|T\|\sigma_w$ Output T if σ_w is valid Otherwise, output *Reject*
	$\xleftarrow{R'}$	
Output ID if $R' = R$ Otherwise, output *Reject*		

Fig. 2 Our PP-MADR protocol (Framework).

(Reader→Tag) The reader (ID) randomly chooses a random number w and sends (w, ID) to the tag.

(Tag→ Reader) Upon receiving (w, ID), the tag chooses a random number R and computes identification proof σ_w, which is the same as tag authentication. Then, it encrypts (R, T, σ_w) with (GT, ID) in the way that successful decryption requires

- The private key d_{ID} of ID.
- $ID \in \mathsf{GT}$. I.e., $ID \in \mathbb{I}$.

Finally, the tag sends the ciphertext to the reader.

(Reader→ Tag) Upon receiving the ciphertext, the reader tries to decrypt it using d_{ID} and a designated-reader group $\mathbb{I}$. If the reader can decrypt (R', T, σ_w) and σ_w is valid, it outputs T and sends R' back to the tag.

(Tag) Upon receiving R' from the reader, the tag outputs reader identity ID if R' is equal to R. Otherwise, the tag outputs *reject*.

If there exists such a secure encryption scheme and GT is anonymous from the view of none-designated readers (without a valid private key), this protocol is a PP-MADR protocol. The mutual authentication is completed between a tag and its designated readers. The tag cannot be traced as the ciphertext needs a private key for decryption and it hides both tag identity and GT.

In comparison with introduced solutions in Section 2.2, this PP-MADR protocol exhibits the following advantages.

1. **Short storage on tags.** Our PP-MADR protocol only requires the tag to store a short group token GT for reader authentication. In our construction, GT is a constant-size group token independent of the number of designated readers in it. It is much shorter than storing linear-size $\mathbb{I}$ directly.
2. **Efficient computation on tags for reader authentication.** The structure of our PP-MADR protocol is quite similar with the given tag authentication except the additional random number R and the new encryption. Without considering the new encryption, our reader authentication only requires the tag to choose a random number and conduct bit string comparison.
3. **Constant-time computation on tags.** The mutual authentication only requires three moves between tag and reader. If the reader is one of designated readers, after three moves, the mutual authentication will return tag identity and reader identity. There is no case that the reader is a designated reader but the mutual authentication outputs *reject*. The tag in the protocol performs all computations only one time. Therefore, the computation time on tags is constant.
4. **No new key generation for readers.** Our protocol does not need to generate new private keys for all designated readers when a tag is created. Each reader only keeps one private key of its identity. Our protocol requires all readers to previously receive all designated-reader groups that include their identities. This requirement is also desired in the proof of reader designation without disclosing $\mathbb{I}$.
5. **Strong privacy on tags and their designated reader groups.** Even if the adversary corrupts a tag and obtains the secret state on it, the adversary cannot trace the tag from the mutual authentication (the view of ciphertext), or distinguish tag's designated-reader group from the group token. The privacy of both the tag and its designated readers is strongly preserved in our protocol.

In the following sections, we show how to construct such a PP-MADR protocol. We firstly formalize the algorithms in the protocol, and then give

the detailed description of each algorithm. The core of our protocol is the particular encryption requiring d_{ID} and $ID \in \mathsf{GT}$ for successful decryption. We note that there is no such an encryption in the literature. Our encryption notion is entirely new.

3 Algorithm Definitions

3.1 Definition of PP-MADR

Based on the introduced framework of our PP-MADR solution in Section 2.3, we now formally define the associated algorithms of our protocol in this section. Our scheme is composed of the following four algorithms.

- **Setup:** Taking as input the security parameter 1^λ and the upper bound size of designated-reader group n, the setup algorithm returns a master public key MPK and a master secret key msk. This algorithm is run by the RFID system server. msk is used to generate private keys for all readers and tags. MPK is published to all readers. Let $\mathbb{I}_1, \mathbb{I}_2, \cdots, \mathbb{I}_L$ be all potential designated-reader groups also published to all readers.
- **RKeyGen:** Taking as input a reader identity ID and the master secret key msk, the reader key generation algorithm returns a private key d_{ID} of ID. This private key is secretly generated by the server and delivered to the reader ID by a secure channel.
- **TSetup:** Taking as input a tag identity T, a designated reader group $\mathbb{I} = \{ID_1, ID_2, \cdots ID_k\}$ and the master secret key msk, the tag setup algorithm returns a private key d_T of T and a group token GT. This algorithm is run by the server. The identity, private key and group token are uploaded to the tag.
- **Authentication:** This is an interactive protocol. The reader takes as input the private key d_{ID}, MPK and its designated-reader group(s) $(\mathbb{I}_1, \mathbb{I}_2, \cdots, \mathbb{I}_N)$. The tag takes as input (T, d_T, GT). If the reader ID has been designated to identify the tag T, the mutual authentication will be successful. The tag outputs the identity of reader and the reader outputs the identity of tag. Otherwise, the reader outputs nothing about the tag, and the tag outputs *reject* in authentication.

The correctness of PP-MADR scheme must satisfy that for all $(MPK, msk, ID, T, d_T, \mathsf{GT})$, if $ID \in \mathsf{GT}$, the mutual authentication between T and ID will be successful, i.e., the reader and the tag can identify each other.

3.2 Security Models

The PP-MADR protocol should satisfy the following security requirements.

- The identification proof σ_w is unforgeable without the valid key d_T.
- The message encrypted with (ID, GT) is indistinguishable without the private key d_{ID} or $ID \notin \mathsf{GT}$.

We define two security models to capture the security requirements of PP-MADR. They are **Tag Unforgeability** model for tag authentication against an adversary who has no private key of tag, and **Message Indistinguishability** model for reader authentication against an adversary who has no private key of one of designated readers. They are defined through game playing between a challenger and an adversary.

Tag Unforgeability. This model is to withstand all attacks of forging a valid proof σ_w without the private key d_T.

Setup: The challenger generates the master key pair with the security parameter λ and a private key of T. The master public key and tag identity T are sent to the adversary.

Query: The adversary makes authentication queries on w, and the challenger responds by generating σ_w, which is sent back to the adversary.

Win: The adversary outputs a valid identification proof σ_{w^*} on w^*, where w^* is generated by the challenger.

Definition 1 *The PP-MADR scheme is (t, q_k, ϵ)-secure with tag unforgeability if for all adversaries in t polynomial time who make q_k queries, we have ϵ is a negligible function associated with the security parameter λ.*

Message Indistinguishability. This model is to withstand all attacks in distinguishing message encrypted with (ID^*, GT^*) without the key d_{ID^*} or $ID^* \notin \mathsf{GT}^*$.

Initialization: The adversary outputs a designated-reader group $\{ID_1^*, ID_2^*, \cdots, ID_k^*\}$ and an identity ID^* for challenge. If $ID^* \in \{ID_1^*, ID_2^*, \cdots, ID_k^*\}$, the adversary cannot query the private key of ID^*; otherwise, the adversary can query all private keys.

Setup: The challenger generates the master key pair with the security parameter λ, and sends the master public key to the adversary.

Query: The adversary makes the following queries.

- The private keys of reader identities satisfying the condition stated in the initialization phase.
- The token $\mathsf{GT_i}$ for any designated-reader group $\mathbb{I}_i$.

Challenge: The adversary outputs two messages M_0, M_1 and a group token GT^* for challenge, where GT^* denotes $\{ID_1^*, ID_2^*, \cdots, ID_k^*\}$ generated in the query phase. The challenger randomly chooses a coin $c \in \{0, 1\}$ and generates a challenger ciphertext C^* on the message M_c encrypted with (ID^*, GT^*).

Win: The adversary outputs a guess c' of c and wins the game if $c' = c$.

Definition 2 *The PP-MADR scheme is* (t, q_k, ϵ) *selectively secure with message indistinguishability if for all adversaries in* t*-polynomial time who make* q_k *key queries, we have* ϵ *is a negligible function associated with the security parameter* λ*.*

3.3 Privacy Models

The PP-MADR protocol should satisfy the following requirements for strong privacy.

- The designated-reader group in the group token GT is indistinguishable. This privacy requirement is to preserve the privacy of designated readers, even if the adversary corrupts the tag and obtains the group token.
- The tag identity and its group token GT are indistinguishable from the view of ciphertext, even if the adversary obtains the secret state on the tag. This requirement is to stop an adversary from tracing tags.

We define **Reader Indistinguishability** model to capture the anonymity of designated-reader group $\mathbb{I}$ from the view of GT. The message indistinguishability implies the tag identity is indistinguishable against an adversary who has no private key of one of designated readers. We define **Token Indistinguishability** model to capture the anonymity of group token GT from the view of ciphertext against an adversary who has no private key of one of designated readers.

Reader Indistinguishability. This model is to withstand all attacks in distinguishing the designated-reader group without a private key of designated reader.

Initialization: The adversary outputs two designated-reader groups $\mathbb{I}_0 = \{ID_1^{*0}, ID_2^{*0}, \cdots, ID_{k_0}^{*0}\}$ and $\mathbb{I}_1 = \{ID_1^{*1}, ID_2^{*1}, \cdots, ID_{k_1}^{*1}\}$ for challenge. The adversary is not allowed to query the private key of any identity in the above two groups.

Setup: The challenger generates the master key pair with the security parameter λ, and sends the master public key to the adversary.

Query: The adversary makes the following queries.

- The private keys of reader identities satisfying the condition stated in the initialization phase.
- The token $\mathsf{GT_i}$ for any designated-reader group $\mathbb{I}_i$.

Challenge: The challenger randomly chooses a coin $c \in \{0, 1\}$ and generates GT^* from $\mathbb{I}_c$ for the adversary.

Win: The adversary outputs a guess c' of c and wins the game if $c' = c$.

Definition 3 *The PP-MADR scheme is* (t, q_k, ϵ) *selectively secure with reader indistinguishability if for all adversaries in* t*-polynomial time who make* q_k *key queries, we have* ϵ *is a negligible function associated with the parameter* λ*.*

Token Indistinguishability. This model is to withstand all attacks in distinguishing the group token from the view of ciphertext without a private key of designated reader.

Initialization: The adversary outputs two designated-reader groups $\mathbb{I}_0 = \{ID_1^{*0}, ID_2^{*0}, \cdots, ID_{k_0}^{*0}\}$ and $\mathbb{I}_1 = \{ID_1^{*1}, ID_2^{*1}, \cdots, ID_{k_1}^{*1}\}$ for challenge. The adversary is not allowed to query the private key of any identity in the above two groups.

Setup: The challenger generates the master key pair and sends the master public key to the adversary.

Query: The adversary makes the following queries.

- The private keys of reader identities satisfying the condition stated in the initialization phase.
- The token $\mathsf{GT_i}$ for any designated-reader group $\mathbb{I}_i$.

Challenge: The adversary outputs (ID^*, M^*) and $(\mathsf{GT}_0^*, \mathsf{GT}_1^*)$ for challenge, where $\mathsf{GT}_0^*, \mathsf{GT}_1^*$ are the group tokens for $\mathbb{I}_0$ and $\mathbb{I}_1$, respectively. The challenger randomly chooses a coin $c \in \{0, 1\}$ and generates C^* with $(\mathsf{GT}^*{}_c, ID^*)$ on M^* for the adversary.

Win: The adversary outputs a guess c' of c and wins the game if $c' = c$.

Definition 4 *The PP-MADR scheme is (t, q_k, ϵ) selectively secure with token indistinguishability if for all adversaries in t-polynomial time who make q_k key queries, we have ϵ is a negligible function associated with the parameter λ.*

4 Our PP-MADR Scheme

4.1 Cryptographic Background

Our PP-MADR scheme is built from a pairing group. Let $\mathbb{BG} = (\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, g_1, g_2, p, e)$ be the pairing group, where $\mathbb{G}_1, \mathbb{G}_2$ are the elliptic group and $\mathbb{G}_T$ is the multiplicative group. The three cyclic groups are of the same order p. Here, g_1 is a generator of $\mathbb{G}_1$ and g_2 is a generator of $\mathbb{G}_2$. e is the bilinear map capturing the three properties:

- For all $g_1 \in \mathbb{G}_1, h_2 \in \mathbb{G}_2$ and $a, b \in \mathbb{Z}_p$, we have $e(g_1^a, h_2^b) = e(g_1, h_2)^{ab}$.
- If g_1 is a generator of $\mathbb{G}_1$ and h_2 is a generator of $\mathbb{G}_2$, we have $e(g_1, h_2)$ is a generator of $\mathbb{G}_T$.
- There exists an efficient algorithm to compute $e(g_1, h_2)$.

4.2 Building Blocks

Membership encryption was first introduced by Guo, Mu, Susilo and Varadharajan in [21]. In this notion, the encryption takes as input an attribute A

and an anonymous token representing a set of attributes $\mathbb{A}$. Successful decryption requires that $A \in \mathbb{A}$ is true. We modify this encryption with two improvements to construct PP-MADR protocol. Firstly, taking as input GT and ID in encryption, successful decryption requires not only $ID \in \mathsf{GT}$ but also the private key d_{ID} of ID. Secondly, the group token GT is anonymous from the view of ciphertext for all adversaries who have no private key of the designated reader.

We utilize the BLS signature scheme [7] and Diffie-Hellman key exchange to generate the identification proof σ_w. The private key d_T of tag is a BLS signature on a secret random number $x \in \mathbb{Z}_p$. The core of identification proof is computed with $w \in \mathbb{G}_1$ and x as w^x. For simply understanding, x can be seen as the real private key of tag.

4.3 Scheme Description

Setup: Taking as input the security parameter 1^λ and the upper bound size n of designated-reader group, the setup algorithm works as follows.

- Choose a pairing group $(\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, p, e)$.
- Randomly pick $g_1, h_1 \in \mathbb{G}_1$ and $g_2, h_2 \in \mathbb{G}_2$ such that $\log_{g_1}^{h_1} = \log_{g_2}^{h_2}$.
- Randomly choose α, β from $\mathbb{Z}_p$ and compute

$$U = h_1,\ \ h_1^{\alpha},\ \ h_1^{\alpha^2},\ \ \cdots,\ h_1^{\alpha^n},\ \ h_1^{\beta},\ \ h_1^{\beta\alpha}, h_1^{\beta\alpha^2},\ \ \cdots,\ h_1^{\beta\alpha^n},\ \ g_1^{\alpha},\ \ h_2,\ \ h_2^{\beta}$$

- Compute the pairing $e(g_1, h_2)$.
- Pick a collision-resistant hash functions H defined as $H : \{0,1\}^* \to \mathbb{G}_1$.

The master public key MPK are composed of

$$\Big(\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, p, e, U, e(g_1, h_2), H\Big),$$

and the master secret keys are $(g_1, g_2, \alpha, \beta)$.

RKeyGen: Taking as input a reader identity $ID \in \mathbb{Z}_p^*$ and the master secret key, the key generation algorithm randomly chooses $s \in \mathbb{Z}_p$ and computes the private key d_{ID} of ID as

$$d_{ID} = \Big(g_2^{\frac{s}{(\alpha+ID)(\beta+ID)}},\ h_2^{\frac{s-1}{\alpha}},\ h_2^{s},\ h_2^{s\alpha},\ \cdots,\ h_2^{s\alpha^{n-2}}\Big).$$

TSetup: Taking as input a tag identity T, a designated-reader group $\mathbb{I} = \{ID_1, ID_2, \cdots ID_k\}$ and the master secret key msk, the tag setup algorithm works as follows.

- Randomly choose $x \in \mathbb{Z}_p$ and computes d_T of T as

$$d_T = (d_T^1,\ d_T^2,\ d_T^3) = \Big(x,\ h_2^x,\ H^{\beta}(d_T^2, T)\Big).$$

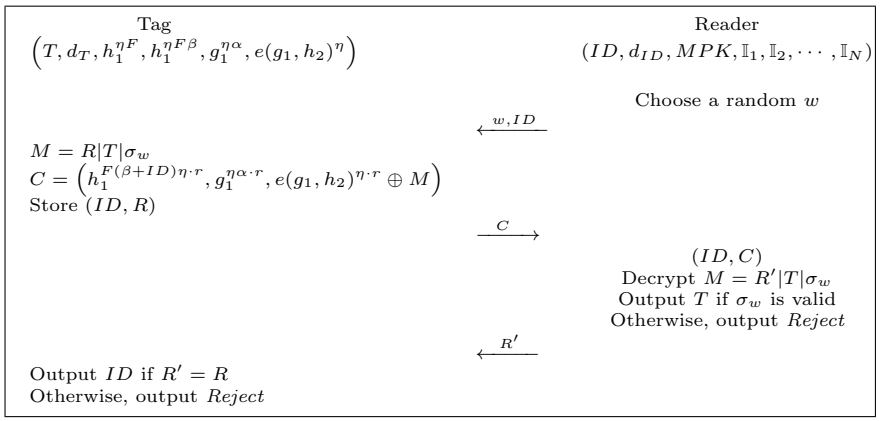

Fig. 3 The mutual authentication between tag and reader in our scheme.

– Randomly choose $\eta \in \mathbb{Z}_p$, and compute GT as

$$\mathsf{GT} = \left(h_1^{\eta F},\ \ h_1^{\eta F\beta},\ \ g_1^{\eta\alpha},\ \ e(g_1,h_2)^{\eta}\right),$$

where $F = \prod_{i=1}^{k}(\alpha + ID_i)$ and h_1^F is computed from U.

Authentication: The reader takes as input parameters $(ID, d_{ID}, MPK, \mathbb{I}_1, \mathbb{I}_2, \cdots, \mathbb{I}_N)$ and the tag takes as input $(T, d_T, h_1^{\eta F}, h_1^{\eta F\beta}, g_1^{\eta\alpha}, e(g_1,h_2)^{\eta})$, the mutual authentication works as follows (depicted in Fig 3).

– The reader randomly chooses $w \in \mathbb{G}_1$ and sends (w, ID) to the tag.
– Upon receiving (w, ID) from the reader, the tag randomly chooses $r, R \in \mathbb{Z}_p$ and works as follows.
  – Compute σ_w with d_T as $\sigma_w = \left(w^x d_T^3,\ \ d_T^2\right)$.
  – Set $M = R|T|\sigma_w$.
  – Generate the ciphertext (c_1, c_2, c_3) as

$$\left(h_1^{F(\beta+ID)\eta\cdot r},\ g_1^{\eta\alpha\cdot r},\ e(g_1,h_2)^{\eta\cdot r} \oplus M\right),$$

  which is forwarded to the reader. (ID, R) is stored for reader authentication.
– Upon receiving the ciphertext, the reader takes as input $(ID, d_{ID}, MPK, \mathbb{I}_1, \mathbb{I}_2, \cdots, \mathbb{I}_N)$ and computes

$$e_1 = e\left(c_1, g_2^{\frac{s}{(\alpha+ID)(\beta+ID)}}\right) = e(g_1,h_2)^{\frac{F}{\alpha+ID}\cdot r\eta s}. \quad (1)$$

Next, the reader takes as input $(ID, d_{ID}, \mathbb{I}_j)$ $(j = 1)$ and tries to decrypt M as follows.

– Let $F = \sum_{ID \in \mathbb{I}_j}(\alpha + ID)$, and b_i be the coefficient of α^i in $\frac{F}{\alpha+ID}$. Compute

$$e_2 = e\Big(c_2, \big(h_2^{\frac{s-1}{\alpha}}\big)^{b_0} \prod_{i=0}^{k-1} (h_2^{s\alpha^i})^{b_{i+1}}\Big) = e(g_1, h_2)^{\frac{F}{\alpha+ID} \cdot r\eta s - b_0 r\eta}. \quad (2)$$

– Compute $e(g_1, g_2)^{r\eta}$ by

$$e_3 = \Big(\frac{e_1}{e_2}\Big)^{\frac{1}{b_0}} = e(g_1, h_2)^{r\eta}. \quad (3)$$

– Extract the message by computing

$$M = e_3 \oplus c_3 = R'|T|\sigma_w.$$

– If T is a tag identity, continue the next procedure; otherwise, repeat this procedure with $j = j + 1$ until $j = N$.

Finally, the reader verifies $\sigma_w = (\sigma_1, \sigma_2)$ as follows and sends R' to the tag.

$$e(\sigma_1, h_2) = e\big(w, d_T^2\big) e\Big(H(d_T^2, T), h_2^{\beta}\Big). \quad (4)$$

– Upon receiving the random number R' from the reader, the tag outputs the reader identity ID if $R' = R$. Otherwise, the tag outputs *reject*.

4.4 Correctness Analysis

If ID is one of designated readers, the decryption is correct.

$$e_1 = e\Big(c_1, g_2^{\frac{s}{(\alpha+ID)(\beta+ID)}}\Big) = e\Big(h_1^{F(\beta+ID)r\eta}, g_2^{\frac{s}{(\alpha+ID)(\beta+ID)}}\Big) = e(g_1, h_2)^{\frac{F}{\alpha+ID} \cdot r\eta s}$$

$$\begin{aligned} e_2 &= e\Big(c_2, \big(h_2^{\frac{s-1}{\alpha}}\big)^{b_0} \prod_{i=0}^{k-1} (h_2^{s\alpha^i})^{b_{i+1}}\Big) \\ &= e\Big(g_1^{\alpha r\eta}, \big(h_2^{\frac{s-1}{\alpha}}\big)^{b_0} \prod_{i=0}^{k-1} (h_2^{s\alpha^i})^{b_{i+1}}\Big) \\ &= e\Big(g_1^{r\eta}, h_2^{(s-1)b_0} \prod_{i=1}^{k} (h_2^{s\alpha^i})^{b_i}\Big) \\ &= e(g_1, h_2)^{\frac{F}{\alpha+ID} \cdot r\eta s - b_0 r\eta} \end{aligned}$$

$$e_3 = \Big(\frac{e_1}{e_2}\Big)^{\frac{1}{b_0}} = \Big(\frac{e(g_1, h_2)^{\frac{F}{\alpha+ID} \cdot r\eta s}}{e(g_1, h_2)^{\frac{F}{\alpha+ID} \cdot r\eta s - b_0 r\eta}}\Big)^{\frac{1}{b_0}} = \Big(e(g_1, h_2)^{b_0 r\eta}\Big)^{\frac{1}{b_0}} = e(g_1, h_2)^{r\eta}$$

The authentication of T in the equation (4) is correct.

$$\begin{aligned} e(\sigma_1, h_2) &= e\Big(w^x H^\beta(d_T^2, T), h_2\Big) \\ &= e(w^x, h_2) e\Big(H^\beta(d_T^2, T), h_2\Big) \\ &= e(w, d_T^2) e\Big(H(d_T^2, T), h_2^\beta\Big). \end{aligned}$$

Let T be chosen from $\mathbb{Z}_p$. Using the bilinear pairing defined in [18], we have the group size satisfying $6|\mathbb{G}_1| \leq 2|\mathbb{G}_2| = |\mathbb{G}_T|$. Since $|M| = |\mathbb{Z}_p| + |\mathbb{Z}_p| + |\mathbb{G}_1| + |\mathbb{G}_2| \approx 3|\mathbb{G}_1| + |\mathbb{G}_2|$. We deduce the group element $e(g_1, h_2)^{r\eta} \in \mathbb{G}_T$ is long enough to XOR the message.

5 Security and Privacy

We analyze the security and privacy of our proposed PP-MADR scheme by using a reduction technique. That is, if there exists an adversary who can break the security or privacy against the PP-MADR, we construct an algorithm to solve some believed-to-be-hard mathematical problems.

5.1 Complexity Assumptions

The hard problems we adopt are modified from the aMSE-DDH problem [24]. Here, $\alpha, \omega, \gamma \in \mathbb{Z}_p$ are random exponents and, $g_1', h_1' \in \mathbb{G}_1, g_2', h_2' \in \mathbb{G}_2$ are group elements satisfying

$$\log_{g_1'}^{h_1'} = \log_{g_2'}^{h_2'}.$$

The Pairing-aMSE-DDH Problem and the Group-aMSE-DDH Problem are defined as follows.

Pairing-aMSE-DDH Problem:

Input:
(1) $g_2', \quad g_2'^{\alpha}, \quad g_2'^{\alpha^2}, \quad \cdots, \quad g_2'^{\alpha^{q-1}}$
(2) $g_2'^{\omega}, \quad g_2'^{\omega\alpha}, \quad g_2'^{\omega\alpha^2}, \quad \cdots, \quad g_2'^{\omega\alpha^q}$
(3) $h_1', \quad h_1'^{\alpha}, \quad h_1'^{\alpha^2}, \quad \cdots, \quad h_1'^{\alpha^{n+1}}$
(4) $h_2', \quad h_2'^{\alpha}, \quad h_2'^{\alpha^2}, \quad \cdots, \quad h_2'^{\alpha^n}$
(5) $h_2'^{\omega}, \quad h_2'^{\omega\alpha}, \quad h_2'^{\omega\alpha^2}, \quad \cdots, \quad h_2'^{\omega\alpha^n}$
(6) $f(x) \in \mathbb{Z}_p[x]$ has degrees $q > n$
(7) $g(x) \in \mathbb{Z}_p[x]$ has degrees $\leq q, g(0) \neq 0$
(8) $gcd(f(x), g(x)) = 1$
(9) $g_1'^{\alpha f(\alpha)}, \quad g_1'^{\alpha\gamma f(\alpha)} \; h_1'^{\gamma g(\alpha)}, \; Z$

Decide: $Z \stackrel{?}{=} e(g_1', h_2')^{f(\alpha)\gamma} \in \mathbb{G}_T$.

Group-aMSE-DDH Problem:

Input: (1) $g_2', \quad g_2'^{\alpha}, \quad g_2'^{\alpha^2}, \quad \cdots, \quad g_2'^{\alpha^{q-1}}$
(2) $g_2'^{\omega}, \quad g_2'^{\omega\alpha}, \quad g_2'^{\omega\alpha^2}, \quad \cdots, \quad g_2'^{\omega\alpha^q}$
(3) $h_1', \quad h_1'^{\alpha}, \quad h_1'^{\alpha^2}, \quad \cdots, \quad h_1'^{\alpha^{n+1}}$
(4) $h_2', \quad h_2'^{\alpha}, \quad h_2'^{\alpha^2}, \quad \cdots, \quad h_2'^{\alpha^n}$
(5) $h_2'^{\omega}, \quad h_2'^{\omega\alpha}, \quad h_2'^{\omega\alpha^2}, \quad \cdots, \quad h_2'^{\omega\alpha^n}$
(6) $f(x) \in \mathbb{Z}_p[x]$ has degrees $q > n$
(7) $g(x) \in \mathbb{Z}_p[x]$ has degrees $\leq q, g(0) \neq 0$
(8) $gcd(f(x), g(x)) = 1$
(9) $g_1'^{\alpha f(\alpha)}, \quad g_1'^{\alpha\gamma f(\alpha)}, \; Z, \; e(g_1', h_2')^{f(\alpha)\gamma}$

Decide: $Z \stackrel{?}{=} h_1'^{\gamma g(\alpha)} \in \mathbb{G}_1$.

Definition 5 *The Pairing/Group-aMSE-DDH problem is (t, ϵ)-hard if for all t-polynomial time adversaries, the maximum probability of solving this problem is ϵ.*

We give analysis under the generic group model based on [16]. Given the challenge instance of Pairing-aMSE-DDH problem, one can compute

$$g_1'^{\alpha f(\alpha)}, \quad g_2'^{A_1(\alpha)}, \quad g_2'^{\omega A_2(\alpha)}, \quad h_1'^{A_3(\alpha)}, \quad h_2'^{A_4(\alpha)}, \quad h_2'^{\omega A_5(\alpha)},$$

where $A_1(x), A_2(x), A_3(x), A_4(x), A_5(x)$ are polynomial functions with degrees $q-1, q, n+1, n, n$ at most, respectively. With the additional elements $g_1'^{\alpha\gamma f(\alpha)}, h_1'^{\gamma g(\alpha)}$, one can further compute

$$e(g_1', h_2')^{\alpha\gamma f(\alpha)\cdot A_4(\alpha)}, \quad e(g_1', h_2')^{\gamma g(\alpha) A_1(\alpha)}$$

towards computing $e(g_1', h_2')^{f(\alpha)\gamma}$. If $e(g_1', h_2')^{f(\alpha)\gamma}$ is computable from the above combinations, we should have

$$\gamma f(\alpha) = \gamma\alpha f(\alpha) A_4(\alpha) + \gamma g(\alpha) A_1(\alpha).$$

That is,

$$g(\alpha) A_1(\alpha) = f(\alpha)\big(1 - \alpha A_4(\alpha)\big).$$

Since $f(x)$ and $g(x)$ are co-prime, we have $f(x) | A_1(x)$. However, $A_1(x)$ has $q-1$ degrees at most, and therefore $A_1(x) \equiv 0$ and $xA_4(x) \equiv 1$. On the other hand, we have $0A_4(0) = 0$ which contradicts $xA_4(x) \equiv 1$. This contradiction indicates that $e(g_1', h_2')^{f(\alpha)\gamma}$ cannot be computed and it is independent of the given challenge instance.

Given the challenge instance of Group-aMSE-DDH problem, one can compute

$$g_2'^{A_1(\alpha)}, \quad g_2'^{\omega A_2(\alpha)}, \quad h_1'^{A_3(\alpha)}, \quad h_2'^{A_4(\alpha)}, \quad h_2'^{\omega A_5(\alpha)},$$

from lines (1), (2), (3), (4) and (5), where $A_1(x), A_2(x), A_3(x), A_4(x), A_5(x)$ are polynomial functions with degrees $q-1, q, n+1, n, n$ at most, respectively.

Let $Z = h_1'^{\gamma g_c(\alpha)}$ for some polynomial function $g_c(x)$. One can only use $g_2'^{A_1(\alpha)}$, $g_2'^{\omega A_2(\alpha)}$, $h_2'^{A_4(\alpha)}$, $h_2'^{\omega A_5(\alpha)}$ for pairing computations with Z. We have

$$e(g_1', h_2')^{\gamma \cdot g_c(\alpha) A_1(\alpha)}, \quad e(g_1', h_2')^{\gamma\omega \cdot g_c(\alpha) A_2(\alpha)},$$
$$e(h_1', h_2')^{\gamma \cdot g_c(\alpha) A_4(\alpha)}, \quad e(h_1', h_2')^{\gamma\omega \cdot g_c(\alpha) A_5(\alpha)},$$

which contain unknown exponents γ or $\gamma\omega$. They must be not $1_{\mathbb{G}_T}$ when used to decide Z.

According to the definition of Pairing-aMSE-DDH problem, $e(g_1', h_2')^{f(\alpha)\gamma}$ is independent of other group elements. Since only $g_1'^{\alpha\gamma f(\alpha)}$ contains the unknown exponent γ in other elements, one must use it in pairing computations. Therefore, the only matching types in comparison are pairings under the basics $e(g_1', h_2')$. I.E.,

- Deciding $e(g_1', h_2')^{\gamma \cdot g_c(\alpha) A_1(\alpha)}$ by computing

$$e\big(g_1^{\alpha\gamma f(\alpha)}, \ \ h_2'^{A_4(\alpha)}\big).$$

- Deciding $e(g_1', h_2')^{\gamma\omega \cdot g_c(\alpha) A_2(\alpha)}$ by computing

$$e\big(g_1^{\alpha\gamma f(\alpha)}, \ \ h_2'^{\omega A_5(\alpha)}\big).$$

For the above analysis, we deduce

$$g_c(\alpha) A_1(\alpha) = \alpha f(\alpha) A_4(\alpha)$$

or

$$g_c(\alpha) A_2(\alpha) = \alpha f(\alpha) A_5(\alpha).$$

That is, $g(\alpha)A_1(\alpha)$ must be computable from $\alpha f(\alpha)A_4(\alpha)$ or $g(\alpha)A_2(\alpha)$ must be computable from $\alpha f(\alpha)A_5(\alpha)$ to solve the problem. Since $f(x)$ and $g(x)$ are co-prime and $g(0) \neq 0$, we have

$$xf(x) | A_1(x) \text{ or } xf(x) | A_2(x).$$

$xf(x)$ has $(q+1)$-degrees. However, $A_1(x)$ has $q-1$ degrees and $A_2(x)$ has q degrees at most. We therefore have $A_1(x) \equiv A_2(x) \equiv 0$. This contradiction indicates that all pairings associated with $h_1'^{\gamma g(\alpha)}$ are independent of other group element, and therefore it is hard to decide whether $Z = h_1'^{\gamma g(\alpha)}$.

5.2 Proof of Security and Privacy

Tag Unforgeability. Our tag authentication utilizes the BLS signature scheme to generate a private key of T and the Diffie-Hellman technique for identification. w^x is aggregated with the signature d_T^3 for shorter length. Since the BLS scheme [7] is provably secure and key exchange is secure, we have σ_w on a random $w \in \mathbb{G}_1$ cannot be computed without the private key x. We avoid the detailed security analysis of tag unforgeability.

Theorem 1 (Message Indistinguishability) *When the Pairing-aMSE-DDH problem is (t, ϵ)-hard, the message indistinguishability of our scheme holds with (t', q_k, ϵ'). $t' = t - O(q_k t_e + n t_e)$ $\epsilon' = \epsilon$, where t_e denotes the time of a point multiplication in $\mathbb{G}_2$.*

Proof Suppose there exists an adversary $\mathcal{A}$ who can break the message indistinguishability. We construct an algorithm $\mathcal{B}$ that solves the Pairing-aMSE-DDH problem. The interaction between $\mathcal{A}$ and $\mathcal{B}$ is described as follows.

Initialization. Let $\mathbb{BG} = \{\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, p\}$ be the pairing group and $\{ID_1, ID_2, \cdots, ID_K\}$ be all identities of readers. The adversary outputs a designated-reader group $\mathbb{I}^* = \{ID_1^*, ID_2^*, \cdots, ID_k^*\}$ and an identity ID^* for challenge. If $ID^* \in \{ID_1^*, ID_2^*, \cdots, ID_k^*\}$, the adversary cannot make the private key query on ID^*. Otherwise, $ID^* \notin \mathbb{I}^*$ and the adversary can query all private keys.

Setup: $\mathcal{B}$ randomly chooses β_0, β_1 from $\mathbb{Z}_p$ and defines the polynomial functions $g(x)$ and $h(x)$ as

$$g(x) = (\beta_0 x + \beta_1 + ID^*) \prod_{i=1}^{k} \big(x + ID_i^*\big),$$
$$h(x) = \frac{\prod_{i=1}^{L} \big(x + ID_i\big)\big(\beta_0 x + \beta_1 + ID_i\big)}{g(x)}.$$

Let $f(x)$ be any q-degree polynomial function such that $h(x)|f(x)$. We have $f(x)$ and $g(x)$ are co-prime. $\mathcal{B}$ gets a challenge instance with the two polynomial functions $f(x), g(x)$. Then, $\mathcal{B}$ defines

$$\beta = \beta_0 \alpha + \beta_1, \quad g_1 = g_1'^{f(\alpha)}, \quad g_2 = g_2'^{f(\alpha)},$$
$$h_1 = h_1', \quad h_2 = h_2', \quad h_1^{\alpha^i} = h_1'^{\alpha^i},$$
$$h_1^{\beta\alpha^i} = h_1'^{\beta_0\alpha^{i+1} + \beta_1\alpha^i}, g_1^{\alpha} = g_1'^{\alpha f(\alpha)}, \quad h_2^{\beta} = h_2'^{\beta_0\alpha + \beta_1},$$
$$e(g_1, h_2) = e(g_1'^{f(\alpha)}, h_2') = e(\prod_{i=1}^{q} g_1'^{\alpha^{i-1} f_i}, h_2'^{\alpha}) e(g_1', h_2')^{f_0},$$

where f_i is the coefficient of x^i in $f(x)$. We have MPK is computable from the challenge instance. $\mathcal{B}$ computes MPK and sends it to the adversary.

Query:

For a private key query on ID, we have that

$$(x + ID)(\beta_0 x + \beta_1 + ID) \nmid g(x)$$

and

$$(x + ID)|f(x) \text{ or } (\beta_0 x + \beta_1 + ID)|f(x).$$

Let $f_{ID}(x)$ be the polynomial function defined as

$$f_{ID}(x) = f^0 \cdot \frac{(x+ID)(\beta_0 x + \beta_1 + ID)}{gcd\Big(f(x), (x+ID)(\beta_0 x + \beta_1 + ID)\Big)},$$

where f^0 is an integer and the coefficient of x^0 in $f_{ID}(x)$ is 1. We have $f_{ID}(x)$ is a polynomial function with one degree at most, and

$$\frac{f(x)f_{ID}(x)}{(x+ID)(\beta_0 x + \beta_1 + ID)}$$

is a polynomial function with $q-1$ degrees at most.

$\mathcal{B}$ randomly chooses s' from $\mathbb{Z}_p$ and defines the random number s for d_{ID} as $s = (s'\omega\alpha + 1)f_{ID}(\alpha)$. We have

$$\begin{aligned} g_2^{\frac{s}{(\alpha+ID)(\beta+ID)}} &= g_2'^{\frac{f(\alpha)(s'\omega\alpha+1)f_{ID}(\alpha)}{(\alpha+ID)(\beta_0\alpha+\beta_1+ID)}} \\ &= g_2'^{\omega\alpha\frac{s'f(\alpha)f_{ID}(\alpha)}{(\alpha+ID)(\beta_0\alpha+\beta_1+ID)}} g_2'^{\frac{f(\alpha)f_{ID}(\alpha)}{(\alpha+ID)(\beta_0\alpha+\beta_1+ID)}}, \end{aligned}$$

which is computable from the challenge input of (1) and (2), respectively.

Since the coefficient of x^0 in $f_{ID}(x)$ is 1, we have

$$x \Big| (s'\omega x + 1)f_{ID}(x) - 1$$

such that

$$\begin{aligned} h_2^{\frac{s-1}{\alpha}} &= h_2'^{\frac{(s'\omega\alpha+1)f_{ID}(\alpha)-1}{\alpha}}, \\ h_2^{s\alpha^i} &= h_2'^{(s'\omega\alpha+1)f_{ID}(\alpha)\alpha^i} = h_2'^{\omega s'\alpha f_{ID}(\alpha)\alpha^i} \cdot h_2'^{f_{ID}(\alpha)\alpha^i}, \end{aligned}$$

which are all computable from the challenge input of (4) and (5) respectively. $\mathcal{B}$ computes

$$d_{ID} = \Big(g_2^{\frac{s}{(\alpha+ID)(\beta+ID)}},\ h_2^{\frac{s-1}{\alpha}},\ h_2^s,\ h_2^{s\alpha},\ \cdots,\ h_2^{s\alpha^{n-2}}\Big)$$

as above for the adversary, which is a valid private key of ID.

For the group token query on the designated-reader group $\{ID_1, ID_2, \cdots, ID_k\}$, the challenger randomly chooses $\eta \in \mathbb{Z}_p$ and computes $\big(h_1^{\eta F}, h_1^{\eta F\beta}, g_1^{\eta\alpha}, e(g_1,h_2)^\eta\big)$ for the adversary, where $F = \sum_{i=1}^k (\alpha + ID)$. Notice that the group token is computable from the master public key. The challenger can always respond queries from the adversary.

Challenge: The adversary outputs two messages (M_0, M_1) and (ID^*, GT^*) for challenge, where GT^* is computed from $\mathbb{I}^* = \{ID_1^*, ID_2^*, \cdots, ID_k^*\}$ as

$$\mathsf{GT}^* = \Big(h_1^{\eta F},\ \ h_1^{\eta F\beta},\ \ g_1^{\eta\alpha},\ \ e(g_1,h_2)^\eta\Big).$$

$\mathcal{B}$ randomly picks $c \in \{0,1\}^*$ and sets the challenger ciphertext as

$$\Big(h_1'^{\gamma g(\alpha)},\ \ g_1'^{\alpha\gamma f(\alpha)},\ \ Z \oplus M_c\Big).$$

Let $r\eta = \gamma$, if $Z = e(g_1', h_2')^{f(\alpha)\gamma}$, we have

$$\begin{aligned} h_1'^{\gamma g(\alpha)} &= h_1^{F(\beta+ID^*)\eta\cdot r} \\ g_1'^{\alpha\gamma f(\alpha)} &= g_1^{\alpha\eta\cdot r} \\ Z \oplus M_c &= e(g_1, h_2)^{\eta\cdot r} \oplus M_c, \end{aligned}$$

such that the challenge ciphertext is a valid ciphertext for M_c.

Win: The adversary $\mathcal{A}$ outputs a guess c' of c and $\mathcal{B}$ outputs c' as the solution to the hard assumption.

This completes the description of our simulation. The time cost of simulation is mainly dominated by the private key simulation, where each key requires $O(q+n)$ point multiplications in $\mathbb{G}_2$. No abortion occurs during the simulation. If $Z = e(g_1', h_2')^{f(\alpha)\gamma}$, the adversary can output a correct guess with probability of $\frac{1}{2}+\epsilon$; otherwise, we have Z is a random element and the adversary can guess only c with probability 1/2. This completes the security proof of Theorem 1.

Theorem 2 (Reader Indistinguishability) *When the Group-aMSE-DDH problem is (t,ϵ)-hard, the reader indistinguishability of our scheme holds with (t', q_k, ϵ'). $t' = t - O(q_k t_e + n t_e)$ $\epsilon' = \epsilon$, where t_e denotes the time of a point multiplication in $\mathbb{G}_2$.*

Proof Suppose there exists an adversary $\mathcal{A}$ who can break the reader indistinguishability. We can construct an algorithm $\mathcal{B}$ that solves the Group-aMSE-DDH problem. The interaction between $\mathcal{A}$ and $\mathcal{B}$ is described as follows.
Initialization. Let $\mathbb{BG} = \{\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, p\}$ be the pairing group and $\{ID_1, ID_2, \cdots, ID_L\}$ be all identities. The adversary outputs two groups $\mathbb{I}_0 = \{ID_1^{*0}, ID_2^{*0}, \cdots, ID_{k_0}^{*0}\}$ and $\mathbb{I}_1 = \{ID_1^{*1}, ID_2^{*1}, \cdots, ID_{k_1}^{*1}\}$ for challenge. The adversary is not allowed to query any identity in the above two groups.

Setup: $\mathcal{B}$ randomly chooses $\beta \in \mathbb{Z}_p, c \in \{0,1\}$ and sets

$$\begin{aligned} g(x) &= \prod_{i=1}^{k_c} \big(x + ID_i^{*c}\big), \\ h(x) &= \frac{\prod_{i=1}^{L} \big(x + ID_i\big)\big(\beta + ID_i\big)}{g(x)}, \end{aligned}$$

where β is one of the master secret keys. The remained simulation is the same as the proof of theorem 1. $\mathcal{B}$ computes and sends MPK to the adversary.

Query: The private key simulation and group token computation are the same as the proof of theorem 1.

Challenge: $\mathcal{B}$ sets the challenge group token as

$$\mathsf{GT}^* = \Big(Z,\ \ Z^{\beta},\ \ g_1'^{\alpha\gamma f(\alpha)},\ \ e(g_1', h_2')^{f(\alpha)\gamma}\Big).$$

Let $\eta = \gamma$, if $Z = h_1'^{g(\alpha)\gamma}$, we have

$$\begin{aligned} F^* &= \prod_{i=1}^{k_c}(\alpha + ID_i^{*c}) = g(\alpha), \\ h_1^{\eta F^*} &= h_1'^{g(\alpha)\gamma} = Z, \\ h_1^{\eta F^*\beta} &= h_1'^{g(\alpha)\gamma\beta} = Z^{\beta}, \\ g_1^{\alpha\eta} &= g_1'^{\alpha\gamma f(\alpha)}, \\ e(g_1, h_2)^{\eta} &= e(g_1', h_2')^{f(\alpha)\gamma}, \end{aligned}$$

such that GT^* is valid for $\mathbb{I}_c = \{ID_1^{*c}, ID_2^{*c}, \cdots, ID_{k_c}^{*c}\}$.

Win: The adversary $\mathcal{A}$ outputs a guess c' of c and $\mathcal{B}$ outputs c' as the solution to the hard assumption.

This completes the description of our simulation. The time cost and probability analysis are the same as the proof in theorem 1. This completes the security proof of Theorem 2.

Theorem 3 (Token Indistinguishability) *Reader indistinguishability implies token indistinguishability.*

Proof We note that the only difference between the two models is the definition of challenge phase. We can easily simulate the challenge ciphertext using the challenge group token.

Let GT^* be the challenge group token in the reader indistinguishability model. The challenger in the token indistinguishability model generates the challenge ciphertext using (ID^*, GT^*) instead of $(ID^*, \mathsf{GT}^*{}_c)$. When the two group tokens denote the same designated-reader group, the only difference is the random numbers η, η_c. We have

$$\begin{aligned} \mathsf{GT}^* &= \Big(h_1^{\eta^* F},\ h_1^{\eta^* F\beta},\ g_1^{\eta^*\alpha},\ e(g_1, h_2)^{\eta^*}\Big) \\ \mathsf{GT}_{\mathsf{c}}^* &= \Big(h_1^{\eta^* F},\ h_1^{\eta^* F\beta},\ g_1^{\eta^*\alpha},\ e(g_1, h_2)^{\eta^*}\Big). \end{aligned}$$

Let the challenge ciphertext from (ID^*, GT^*) be

$$C^* = \Big(h_1^{F(\beta+ID^*)\eta^*\cdot r}, g_1^{\eta^*\alpha\cdot r}, e(g_1, h_2)^{\eta^*\cdot r} \oplus M^*\Big).$$

It can be seen as a ciphertext for $(ID^*, \mathsf{GT}^*{}_c)$ by viewing the use of random number $r' = \frac{r\eta_c^*}{\eta^*}$ in encryption. That is, C^* is a valid challenge ciphertext in the token indistinguishability model. If the adversary can distinguish $\mathsf{GT}^*{}_c$ from the ciphertext, it means that we can reduce the attack to distinguish designated-reader group from the group token GT^*.

Table 1 The computational cost and storage cost of our protocol.

Entities	Computation	Storage
Server	$4\mathbb{G}_1 + \mathbb{G}_2 + \mathbb{G}_T + H$	$\lvert\mathbb{G}_1\rvert + \lvert\mathbb{G}_2\rvert + 2\lvert\mathbb{Z}_p\rvert$
Reader	$N(e + \mathbb{G}_T) + 4e + H$	$MPK + (N + n)\lvert\mathbb{G}_2\rvert$
Tag	$5\mathbb{G}_1 + \mathbb{G}_T$	$\lvert T\rvert + 4\lvert\mathbb{G}_1\rvert + \lvert\mathbb{G}_2\rvert + \lvert\mathbb{G}_T\rvert + \lvert\mathbb{Z}_p\rvert$

6 Evaluation of Our PP-MADR

The novelty of our PP-MADR protocol has been introduced in Section 2.3. In this section, we evaluate our PP-MADR scheme in terms of computational efficiency, storage efficiency and hardware requirement for RFID tags. We also give comparison and discuss the privacy of reader identity during transmission.

6.1 Computation and Storage

The server computes d_T and GT when a tag is created. With the master secret key, the server can firstly compute all exponents before point multiplication and exponentiation computation. Therefore, the main computational cost of server during the creation of tag comprises of four point multiplications in $\mathbb{G}_1$, one point multiplication in $\mathbb{G}_2$, one exponentiation in $\mathbb{G}_T$ and one group hashing operation.

The reader in our scheme mainly performs ciphertext decryption and σ_w verification (only after successful decryption). During the decryption in computing e_2, we have $h_{\mathbb{I}} = \left(h_2^{\frac{s-1}{\alpha}}\right)^{b_0} \prod_{i=0}^{k-1} (h_2^{s\alpha^i})^{b_{i+1}}$ that is independent of ciphertext. This operation is associated with private key and $\mathbb{I}$ only, and it can be pre-computed by the reader. For each designated-reader group, the decryption mainly costs two pairing computations and one exponentiation in $\mathbb{G}_T$. The σ_w verification costs three pairing computation and one group hashing operation. When the reader has N designated-reader groups, the reader must take as input $h_{\mathbb{I}}$ one by one in the pairing e_2 computation until the reader successfully decrypts the message or tries all of designated-reader groups.

The computational cost of tag is mainly dominated by σ_w computation for identification proof and ciphertext generation for reader authentication. We have σ_w costs one point multiplication in $\mathbb{G}_1$, and the ciphertext costs four point multiplications in $\mathbb{G}_1$ and one exponentiation in $\mathbb{G}_T$. Our protocol is constructed from bilinear pairing, but tags do not perform any pairing computation.

The server uploads T, d_T and GT to tag, where $d_T = (x, h_2^x, H^\beta(d_T^2, T))$ and $\mathsf{GT} = \left(h_1^{\eta F}, h_1^{\eta F\beta}, g_1^{\eta\alpha}, e(g_1, h_2)^\eta\right)$. We have $d_T = \lvert\mathbb{Z}_p\rvert + \lvert\mathbb{G}_1\rvert + \lvert\mathbb{G}_2\rvert$ and $\lvert\mathsf{GT}\rvert = 3\lvert\mathbb{G}_1\rvert + \lvert\mathbb{G}_T\rvert$. The group token is constant-size and independent of the number of designated readers. In our protocol, the sever only keeps its master secret key and the reader keeps MPK, d_{ID} and $h_{\mathbb{I}_1}, h_{\mathbb{I}_2}, \cdots, h_{\mathbb{I}_N}$. The cost of computation and storage is given in Table 1.

6.2 Hardware Requirement

We adopt public-key cryptography to construct PP-MADR protocol with strong privacy. The price to pay is the more complicated hardware for tags compared to other protocols adopting symmetric cryptography for weak privacy. Fortunately, our PP-MADR protocol does not increase the hardware cost on tags compared to the given tab authentication in Section 2.1.

The hardware implementation of a protocol on tags is composed of logic controller (algorithm), memory and basic modules such as pseudo-random number generator, point multiplication in $\mathbb{G}_1$ and exponentiation in $\mathbb{G}_T$. The public key cryptography is more expensive in implementation compared to symmetric cryptography due to the complicated modules for point multiplication and exponentiation. Our protocol requires a tag to perform $5\mathbb{G}_1 + \mathbb{G}_T$ for mutual authentication. Serial computations can be adopted to reduce the hardware resource, but it at least requires one module for point multiplication in $\mathbb{G}_1$ and one module for exponentiation in $\mathbb{G}_T$. Notice that the tag in the tag authentication from the proposed IBE schemes such as [5, 44, 19] also require both modules $\mathbb{G}_1$ and $\mathbb{G}_T$ to perform encryption. Therefore, the hardware requirement of our scheme is the same as the encryption algorithm of these IBE schemes.

Many hardware implementations (e.g. [32, 22, 27]) towards cheap processors for point multiplication and exponentiation have been proposed. They become useful when the tag must be equipped with low-cost hardware. Recently, the authors in [37] showed that identity-based key agreements are feasible on RFID tags equipped with MSP430F2618 microcontrollers. The agreements require pairing computation which needs both the modules of point multiplication in $\mathbb{G}_1$ and exponentiation in $\mathbb{G}_T$. It indicates that our PP-MADR protocol is also feasible for RFID systems when tags are equipped with the same kind of chips.

6.3 Tradeoff and Limitations

Our PP-MARD protocol provides strong privacy on tags and designated readers, such that tags are indistinguishable from authentication and designated readers are indistinguishable from authentication and the secret state on tag. The price to pay for this strong privacy is as follows.

RFID tags have to perform asymmetric computations such as the point multiplications in the elliptic curve group. We note that strong privacy cannot be realized using symmetric cryptography.

RFID readers have to perform computations in the linear of the number of their reader groups. If a reader has been designated in N groups, the worst case requires N times of decryption. We note that the designated reader group requires to be anonymous in the PP-MADR protocol, and therefore the guess procedure producing linear time in computation cannot be avoided.

In our PP-MADR protocol, we didn't consider how to update designated reader group or private key. The update on the designated reader group is

relatively easy. It requires the server to re-create the group token on tag and publish the new group. We note that the update on private key especially for readers is challenging, as we have to solve the key revocation problem. How to efficiently realize these extensions is out of scope of this work.

6.4 Comparison of Protocols

In this section, we compare our protocol with several related protocols introduced in Section 2. We summarize those protocols which are stated as follows.

- Protocol 1. This protocol is realized using a tag authentication protocol with weak privacy, where only those designated readers who have secret keys from the server can conduct mutual authentication.
- Protocol 1^+. This protocol is the same as Protocol 1 except that the adopted tag authentication protocol is based on an identity-based encryption with strong privacy. A more detailed description is given in the last paragraph of Section 2.2.
- Protocol 2. This protocol is realized using an identity-based encryption to achieve mutual authentication, where tag identity is encrypted if the reader is one of designated readers. The tag will disclose its designated readers $h_{\mathbb{I}}$ to all readers for each authentication query, such that a valid reader can generate a valid proof of $ID \in \mathbb{I}$ and $H(\mathbb{I}) = h_{\mathbb{I}}$.
- Protocol 2^+. This protocol is similar with Protocol 2 without disclosing its designated readers. The reader guesses $h_{\mathbb{I}}$ one by one. For each proof of $ID \in \mathbb{I}$ and $H(\mathbb{I}) = h_{\mathbb{I}}$ from the reader, the tag first checks whether $h_{\mathbb{I}}$ is its designated readers. If true, it uses an identity-based encryption to achieve tag authentication and reader authentication by encrypting $T|\sigma_w|R$ for identity ID. Otherwise, it encrypts a dummy string. The dummy encryption is desired to protect $h_{\mathbb{I}}$ as the proof of $ID \in \mathbb{I}$ and $H(\mathbb{I}) = h_{\mathbb{I}}$ can be generated by all adversaries.

The comparison of these protocols is given in Table 2. The privacy protection on designated readers requires linear computation on readers as the readers have to select a correct group first. Protocol 1^+ achieves the same privacy protections as ours but it requires the server to generate private keys for all designated readers when a tag is created. In comparison with Protocol 2, ours requires a linear computation on tags but provides strong privacy protection on designated readers. Our protocol is better than Protocol 2^+ in terms of computational efficiency and privacy protection. The only disadvantage of our protocols is requiring asymmetric computation on tag and linear asymmetric computation on readers. As we noted before, these two drawbacks are the tradeoff towards strong privacy on tag and reader.

Table 2 The comparison of protocols towards different privacy protection. Here, symmetric refers to those computations such as hashing operation, while asymmetric refers to those computations such as exponentiation and point multiplication.

Protocols	Tag	Readers
Protocol 1	One Symmetric	Linear Symmetric
Protocol 1^+	One IBE encryption	Linear IBE decryption
Protocol 2	One IBE encryption +One Symmetric	One IBE decryption +One Symmetric
Protocol 2^+	Linear IBE encryption +Linear Symmetric	Linear IBE decryption +Linear Symmetric
Our Protocol	One Asymmetric	Linear Asymmetric

Protocols	Privacy of Tag	Privacy of Readers	Disadvantage
Protocol 1	Weak Privacy	Weak Privacy	New Key & Linear
Protocol 1^+	Strong Privacy	Strong Privacy	New Key & Linear
Protocol 2	Strong Privacy	No Protection	No reader privacy
Protocol 2^+	Strong Privacy	Week Privacy	Linear Computation
Our Protocol	Strong Privacy	Strong Privacy	Asymmetric & Linear

6.5 Preserving Privacy on Reader Identity

In our PP-MADR protocol, the reader identity is transmitted in a plaintext. An adversary who eavesdrops the authentication will know ID is one of designated readers if the reader sends back the response R'. This issue does not compromise the privacy problem as in our security model, an adversary is not allowed to distinguish the group token GT with the help of readers. To enhance the security, in this section, we show how to hide the reader identity during transmission (Fig 4) against other adversaries who are not designated readers.

Our protocol uses a particular membership encryption $\mathsf{E}_{\mathsf{GT},ID}[M]$ such that successful decryption requires the private key of ID and $ID \in \mathsf{GT}$. Notice that if the encryptor uses GT in encryption without ID, where the ciphertext is

$$\Big(h_1^{F\beta\eta\cdot r}, \quad h_1^{F\eta\cdot r}, \quad g_1^{\eta\alpha\cdot r}, \quad e(g_1,h_2)^{\eta\cdot r}M\Big),$$

we have it is an identity-based broadcast encryption where all readers in GT can decrypt the message. For receiver ID, it firstly converts the ciphertext into

$$\Big(h_1^{F(\beta+ID)\eta\cdot r},\ g_1^{\eta\alpha\cdot r},\ e(g_1,h_2)^{\eta\cdot r}M\Big),$$

which is the $\mathsf{E}_{\mathsf{GT},ID}[M]$ encryption. Then, it runs the decryption as the description in our protocol. The security of this broadcast encryption is guaranteed by the message indistinguishability in Theorem 1.

The extended PP-MADR protocol for hiding reader identity is outlined as follows. The reader firstly sends an authentication query to the tag. Upon receiving the query, the tag runs the broadcast encryption on random keys K_1, K_2. If the reader ID is one of designated readers, it decrypts the random keys and uses K_1 to encrypt ID to the tag. The following protocol is the same as the original protocol except that $\mathsf{E}_{\mathsf{GT},ID}[M]$ could leak the reader identity ID. We use $K_2 \oplus \mathsf{E}_{\mathsf{GT},ID}[M]$ to denote an XOR encryption on $h_1^{F(\beta+ID)\eta\cdot r}$ with the random key K_2 to protect ID.

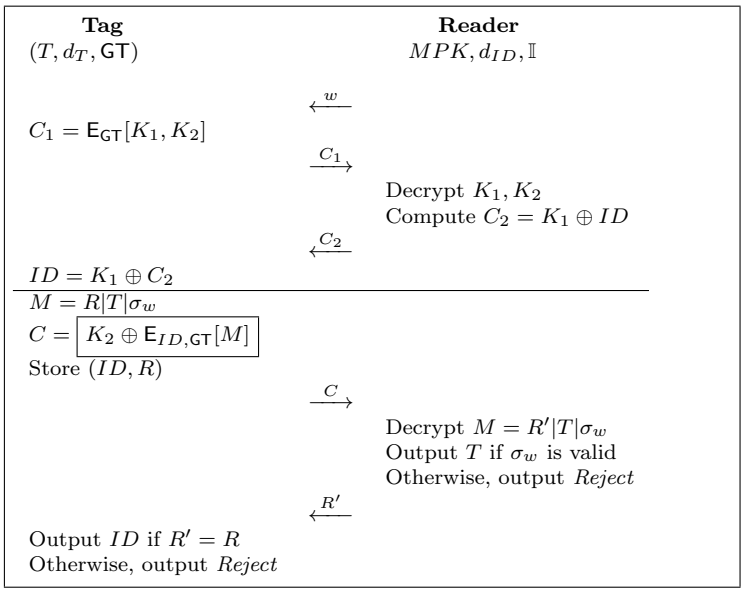

Fig. 4 Our Extended PP-MADR protocol.

This extended protocol hides the reader identity during transmission, such that only designated readers know the reader identity. The price to pay of this extension is double encryption on tag.

7 Conclusion

We proposed a privacy-preserving mutual authentication protocol with designated readers (PP-MADR) for RFID security. In this notion, only tags and their designated readers can authenticate each other. Other readers and adversaries cannot trace RFID tags or know their designated readers. In our protocol, the storage cost and computational cost on tags for mutual authentication are constant, independent of the number of designated readers. The RFID system server does not need to compute new keys for readers when a tag is created. Our protocol strongly preserves the privacy of tag and its designated readers even if the adversary can corrupt the tag and obtain its secret state. In comparison with other possible solutions, our protocol has demonstrated clear advantages.

References

1. Armknecht, F., Sadeghi, A.R., Visconti, I., Wachsmann, C.: On RFID privacy with mutual authentication and tag corruption. In: proc.ACNS'10, *LNCS*, vol. 6123, pp. 493–510 (2010)

2. Avoine, G., Dysli, E., Oechslin, P.: Reducing time complexity in RFID systems. In: Proc. SAC'05, *LNCS*, vol. 3897, pp. 291–306 (2005)
3. Berbain, C., Billet, O., Etrog, J., Gilbert, H.: An efficient forward private RFID protocol. In: Proc. ACM CCS'09, pp. 43–53. ACM (2009)
4. Billet, O., Etrog, J., Gilbert, H.: Lightweight privacy preserving authentication for RFID using a stream cipher. In: Proc. FSE'10, *LNCS*, vol. 6147, pp. 55–74 (2010)
5. Boneh, D., Boyen, X.: Efficient selective-id secure identity-based encryption without random oracles. In: Proc. EUROCRYPT'04, *LNCS*, vol. 3027, pp. 223–238 (2004)
6. Boneh, D., Franklin, M.K.: Identity-based encryption from the weil pairing. In: Proc. CRYPTO'01, *LNCS*, vol. 2139, pp. 213–229 (2001)
7. Boneh, D., Lynn, B., Shacham, H.: Short signatures from the weil pairing. In: Proc. ASIACRYPT'01, *LNCS*, vol. 2248, pp. 514–532 (2001)
8. Bringer, J., Chabanne, H., Icart, T.: Cryptanalysis of EC-RAC, a RFID identification protocol. In: Proc. CANS'08, *LNCS*, vol. 5339, pp. 149–161 (2008)
9. Canard, S., Coisel, I.: Data synchronization in privacy-preserving RFID authentication schemes. In: Proc. RFIDSec'08 (2008)
10. Canard, S., Coisel, I., Etrog, J., Girault, M.: Privacy-preserving RFID systems: Model and constructions. IACR Cryptology ePrint Archive p. 405 (2010)
11. Chien, H.Y., Chen, C.H.: Mutual authentication protocol for RFID conforming to epc class 1 generation 2 standards. Computer Standards & Interfaces **29**(2), 254–259 (2007)
12. Chou, J.S., Lee, G.C., Chan, C.J.: A novel mutual authentication scheme based on quadratic residues for RFID systems. IACR Cryptology ePrint Archive **2007**, 224 (2007)
13. Coisel, I., Martin, T.: Untangling RFID privacy models. Journal Comp. Netw. and Communic. **2013** (2013)
14. D'Arco, P.: An almost-optimal forward-private RFID mutual authentication protocol with tag control. In: Proc. WISTP'11, *LNCS*, vol. 6633, pp. 69–84 (2011)
15. D'Arco, P., Santis, A.D.: On ultralightweight RFID authentication protocols. IEEE Trans. Dependable Sec. Comput. **8**(4), 548–563 (2011)
16. Delerablée, C.: Identity-based broadcast encryption with constant size ciphertexts and private keys. In: Proc. ASIACRYPT'07, *LNCS*, vol. 4833, pp. 200–215 (2007)
17. van Deursen, T., Radomirovic, S.: Untraceable RFID protocols are not trivially composable: Attacks on the revision of EC-RAC. IACR Cryptology ePrint Archive p. 332 (2009)
18. Freeman, D., Scott, M., Teske, E.: A taxonomy of pairing-friendly elliptic curves. J. Cryptology **23**(2), 224–280 (2010)
19. Gentry, C.: Practical identity-based encryption without random oracles. In: Proc. EUROCRYPT'06, *LNCS*, vol. 4004, pp. 445–464 (2006)
20. Gilbert, H., Robshaw, M.J.B., Seurin, Y.: $HB^{\#}$: Increasing the security and efficiency of HB^{+}. In: Proc.EUROCRYPT'08, *LNCS*, vol. 4965, pp. 361–378 (2008)
21. Guo, F., Mu, Y., Susilo, W., Varadharajan, V.: Membership encryption and its applications. In: Proc. ACISP'13, *LNCS*, vol. 7959, pp. 219–234 (2013)
22. Hein, D.M., Wolkerstorfer, J., Felber, N.: ECC is ready for RFID - a proof in silicon. In: Proc. SAC'08, *LNCS*, vol. 5381, pp. 401–413 (2008)
23. Hermans, J., Pashalidis, A., Vercauteren, F., Preneel, B.: A new RFID privacy model. In: Porc. ESORICS'11, *LNCS*, vol. 6879, pp. 568–587 (2011)
24. Herranz, J., Laguillaumie, F., Ràfols, C.: Constant size ciphertexts in threshold attribute-based encryption. In: Proc. PKC'10, *LNCS*, vol. 6056, pp. 19–34 (2010)
25. Hopper, N., Blum, M.: Secure human identification protocols. In: Proc. ASIACRYPT'01, *LNCS*, vol. 2248, pp. 52–66 (2001)
26. Juels, A., Weis, S.A.: Defining strong privacy for RFID. ACM Trans. Inf. Syst. Secur. **13**(1) (2009)
27. Kerins, T., Marnane, W.P., Popovici, E.M., Barreto, P.S.L.M.: Efficient hardware for the tate pairing calculation in characteristic three. In: Proc. CHES'05, *LNCS*, vol. 3659, pp. 412–426 (2005)
28. Le, T.V., Burmester, M., de Medeiros, B.: Universally composable and forward-secure RFID authentication and authenticated key exchange. In: Proc. ASIACCS'07, pp. 242–252. ACM (2007)

29. Lee, Y., Batina, L., Verbauwhede, I.: Privacy challenges in RFID systems. In: Proc. The Internet of Things'10, pp. 397–407. Springer New York (2010)
30. Lee, Y.K., Batina, L., Verbauwhede, I.: EC-RAC (ECDLP based randomized access control): Provably secure RFID authentication protocol. In: Proc. IEEE International Conference on RFID'08, pp. 97–104 (2008). DOI 10.1109/RFID.2008.4519370
31. Lee, Y.K., Batina, L., Verbauwhede, I.: Untraceable RFID authentication protocols: Revision of EC-RAC. In: Proc. IEEE International Conference on RFID'09, pp. 178–185 (2009). DOI 10.1109/RFID.2009.4911179
32. Lee, Y.K., Sakiyama, K., Batina, L., Verbauwhede, I.: Elliptic-curve-based security processor for RFID. IEEE Trans. Computers **57**(11), 1514–1527 (2008)
33. Li, N., Mu, Y., Susilo, W., Guo, F., , Varadharajans, V.: Privacy-preserving authorized RFID authentication protocols. In: Proc. RFIDSec'14, LNCS (2014)
34. Liu, H., Ning, H.: Zero-knowledge authentication protocol based on alternative mode in RFID systems. Sensors Journal, IEEE **11**(12), 3235–3245 (2011)
35. Lv, C., Li, H., Ma, J., Zhang, Y.: Vulnerability analysis of elliptic curve cryptography-based RFID authentication protocols. Trans. Emerging Telecommunications Technologies **23**(7), 618–624 (2012)
36. Miyako Ohkubo, K.S., Kinoshita, S.: Cryptographic approach to "privacy-friendly" tags. In: Proc. RFID Privacy Workshop'03 (2003)
37. MolinaMarkham, A., Clark, S., Ransford, B., Fu, K.: Bat: Backscatter anything-to-tag communication. In: Wirelessly Powered Sensor Networks and Computational RFID, pp. 131–142. Springer New York (2013)
38. Molnar, D., Wagner, D.: Privacy and security in library RFID: issues, practices, and architectures. In: Proc. ACM CCS'04, pp. 210–219. ACM (2004)
39. Oren, Y., Feldhofer, M.: A low-resource public-key identification scheme for RFID tags and sensor nodes. In: Proc. WISEC'09, pp. 59–68. ACM (2009)
40. Paise, R.I., Vaudenay, S.: Mutual authentication in RFID: security and privacy. In: Proc. ASIACCS'08, pp. 292–299. ACM (2008)
41. Peeters, R., Hermans, J.: Wide strong private RFID identification based on zero-knowledge. IACR Cryptology ePrint Archive p. 389 (2012)
42. Saarinen, M.J.O.: The PASSERINE public key encryption and authentication mechanism. IACR Cryptology ePrint Archive p. 433 (2010)
43. Vaudenay, S.: On privacy models for RFID. In: Proc. ASIACRYPT'07, *LNCS*, vol. 4833, pp. 68–87 (2007)
44. Waters, B.: Efficient identity-based encryption without random oracles. In: Proc. EUROCRYPT'05, *LNCS*, vol. 3494, pp. 114–127 (2005)