Efficient Security and Privacy Protection for Emerging Smart RFID Communications

Mohammad Fal Sadikin
AG Computer Systems & Telematics, Freie Universität Berlin
Berlin, Germany
E-mail: fal.sadikin@fu-berlin.de
http://www.mi.fu-berlin.de/inf/groups/ag-tech/index.html

Marcel Kyas
AG Computer Systems & Telematics, Freie Universität Berlin
Berlin, Germany
E-mail: marcel.kyas@fu-berlin.de
http://www.mi.fu-berlin.de/inf/groups/ag-tech/index.html

Abstract

Due to its constrained nature, the use of smart RFID technology introduces tremendous security and privacy issues. This paper presents IMAKA-Tate: Identity protection, Mutual Authentication and Key Agreement using Tate pairing of Identity-based Encryption method. It is designed to tackle various challenges in the constrained nature of RFID applications by applying a light-weight cryptographic method with advanced-level 128 bit security protection. Thus, IMAKA-Tate protects the RFID system from various security and privacy threats (e.g. unauthorized tracking, cloning attack, etc.).

Keywords: Smart RFID Security; Privacy Preserving; Mutual Authentication.

1. Introduction & Motivation

The emerging of sensor integration to RFID system called smart RFID has recently attracted a lot of interest in research and development. It is a prominent technology that is projected to be massively deployed in various applications, ranging from e-Health, transportation, human and device tracking, to distinctive applications like in military system. Indeed, such technology introduces considerable advantages reaching from economical aspects like low cost implementation and maintenance, to technical aspects like reliability and accuracy, as well as its flexibility to be integrated in large-scale system.

Nevertheless, smart RFID system introduces tremendous security and privacy issues derived from the vulnerability nature of Wireless Sensor Network (WSN) applications, as well as various issues elicited from the use of tracking and positioning techniques itself. The following list outlines such issues that must be tackled in smart RFID system.

- The nature of RFID tag which basically can be read without authorization introduces tremendous security risks, particularly various risks from passive and active eavesdropping. This issue makes the RFID system is susceptible from various threats ranging from cloning attack, spoofing or data manipulation, collision attack, to various techniques of Man-in-the-Middle (MITM) attacks like Denial-of-Service (DoS), replay attack, and so on.
- By taking in to account common RFID communication is not mutually authenticated, the RFID system is highly susceptible from various impersonation techniques. This issue makes unauthorized parties can easily perform malicious activities related to privacy threats including unauthorized tracking, spying, or analyzing the information leakage to reveal the user activities.

Published by Atlantis Press

- Smart RFID tag is basically a device with limited resources in term of CPU, memory, bandwidth/data-rate, and energy/battery storage. Such limitations make the smart RFID tag is highly susceptible to various threats that are also common in WSN. One of them is various techniques of resource consumption attacks. These attacks are conducted by repeatedly sending packet to drain the battery and misspend the bandwidth.
- The constrained nature of RFID system makes the security enforcement is more complicated. On the other hand, common security and privacy solution, such as using Transport Layer Security (TLS/SSL) is not feasible. Indeed, TLS/SSL suffers from various problems reaching from various security threats (e.g. MITM attacks), to communication and computation overheads that would overburden the limited capabilities of smart RFID system.

This paper presents IMAKA-Tate, a light-weight identity protection and mutual authentication using Identity-based Encryption (IBE) method. Particularly, it relies on cryptographic Tate (ηT) pairing over super singular elliptic curves, ternary field $F_{3^{509}}$ [1]. IMAKA-Tate method is tailored to tackle the specific challenges for security and privacy in the constrained nature of smart RFID. Moreover, in order to achieve efficient communication overhead, the authentication mechanism fully relies on link layer security method, particularly over IEEE 802.15.4 which is commonly used to deliver low-data rate. Thus it is affordable to be applied in the restricted smart RFID environment.

The rest of this paper is organized as follows. In section II, we outline previous works that associates to our work. In section III presents the protocol design of IMAKA-Tate. In Section IV, we analyze the security aspects of IMAKA-Tate. Section V presents the computation analysis. Finally, we conclude our work in Section VI.

2. Related Work

Our work associates to broad field of research works as smart RFID system is established based on multi aspects of wireless communication system. This section resumes several existing solutions that relate to our work.

IMAKA-Tate [13] is our prior work which aims at providing novel security and privacy method tailored to tackle the security and privacy challenges in Wireless Indoor Positioning (WIP) system. Particularly, we demonstrated that our method provide security and privacy solution that is feasible for the constrained nature of WIP. In this paper, we follow up our work by analyzing how the IMAKA-Tate can also be used for specific challenges in the smart RFID system.

Mulkey, Kar and Katangur [3], purposed an efficient protocol for authentication and privacy in wireless networks IEEE 802.11 using IBE techniques. Particularly, they enhanced the existing WPA protocol by incorporating IBE based authentication methods. However, distinct to our work, we purpose a mutual authentication and key agreement with identity protection. Our proposed solution is to ensure the privacy preserving and to provide access control that only legitimate party can participate in the smart RFID system. Furthermore, to support large-scale system, we purpose in detail the enhancement of mutual authentication mechanism by transporting the authentication messages over Extensible Authentication Protocol (EAP) method.

One of earlier works on IBE authentication and key exchange was purposed by Kolesnikov and Sundaram, called Identity-Based Authenticated Key Exchange Protocol (IBAKE) [5]. In IBAKE method, the authors improved the limitation of Authenticated Key Exchange (AKE) that suffer from corrupt Key Management Service (KMS) or key escrow problem [6][7]. In order to achieve the integrity protection, IBAKE method also provides mutual authentication with perfect forward and backward secrecy. The sequence work of IBAKE is defined in RFC 6539 [8] that described how key exchange and encryption-decryption mechanism are performed using standard of Boneh-Franklin [9] and Boneh-Boyen [10]. Currently, they are also proposing in detail how to carry IBAKE messages using EAP in the on progressing work [11]. In conclusion, IBAKE is a potential security protocol for mutual authentication and privacy preserving. Nevertheless such protocol is not feasible for RFID system, since the protocol must be relied on upper layer method using TLS. Indeed, using TLS method can drain the limited capabilities of RFID tag. Moreover, it utilizes expensive cryptographic method that is too heavy for the smart RFID system.

In the context of IBE for WSN, Szczechowiak and Collier [4] proposed TinyIBE using ηT pairing to disprove the argument that using IBE is too heavy for sensor node. They demonstrated that it is feasible to enforce the ηT pairing even on at very constrained nodes. However, all nodes in the proposed solution are assumed as static node without movement. It is therefore not suitable for smart RFID tag that is highly mobile and pervasive computing. Furthermore, TinyIBE method only provides secure key distribution, instead of providing mutual authentication and identity protection. Thus, it does not protect various threats of MTIM attacks.

3. Proposed Scheme

This section describes IMAKA-Tate as proposed scheme to tackle various challenges in the constrained nature smart RFID system.

3.1. *Preliminaries*

To tackle the specific challenges in smart RFID system, IMAKA-Tate [13] early establishes encryption even before the authentication is started. In this context, the entire communication data including the RFID tag identity are transported in encrypted payload. Furthermore, to achieve light-weight and feasible communication overhead, we apply ηT pairing that is known as the fastest pairing method [2]. In Principal, the cryptographic processing relies on ternary field $F_{3^{509}}$ defined in [1], specifically using the extension field $F_{3^{509\,x\,6}}$. Such extension field is applied in order to provide advanced-level 128 bit security strength of IBE, which is about same security level as 3072 bit RSA method [1][3].

In the smart RFID networks, we propose two parties (i.e. RFID reader and RFID tag) perform mutual authentication to each other. Particularly, they communicate over standard IEEE 802.15.4f, which defines standard wireless Physical (PHY) and Media access control (MAC) for active RFID. In addition, each smart RFID tag has sufficient co-processor to perform cryptographic processing, as the tag is integrated in standard sensor platform, such as Imote2 with diverse options of core frequency (i.e. 104, 208, 312 and 416 MHz).

3.2. *Setup Phase*

On the setup phase, the Key Generation Function (KGF) privately distributes all parameters that are needed to construct the IBE method. The KGF is handled by the administrator, who privately preloads all parameters to each legitimate reader and smart RFID tag memory. It is to be noted that all parameters are shared prior to network deployment. In this case, the existence of KGF is no longer needed after the KGF successfully shares all parameters including private keys and all public parameters. This method is to ensure that only legitimate entity can participate in the smart RFID system.

During the setup phase, the KGF initially generates overall parameters that will be confidentially preloaded to each reader and RFID tag's memory. The generated secret parameters include a 128 bit integer master secret key *s*, where $s \in Z_q^*$. Supersingular elliptic curve define over $F_q^*, where\ F_q^* = F_{3^{509}}$. A random point on elliptic curve *P* as part of public parameter, where $P \in E(F_q)$. Additional random point as another part of public parameter *Q*, where $Q \in E(F_q)$ and $Q = sP$. Furthermore, the KGF also generates public parameter $g = e(P, P)$. In this context, *e* is a function that maps $E(F_{3^{509}})\ x\ E(F_{3^{509}}) \rightarrow F_{3^{509\,x\,6}}$. In addition, two more parameters are defined as hash functions. The first one is *H1*, it is hash function to convert a binary RFID identity to a 128 bit integer, where $H1 : \{0, 1\}^* \rightarrow Z_q^*$. The second one is *H2*, this hash function is to convert a parameter on extension filed $F_{3^{509\,x\,6}}$ to a 128 bit integer, where $H2 : F_q \rightarrow \{0, 1\}^n$.

Instead of distributing the master secret key *s*, the KGF generates all private keys of all RFID devices and then preloads all the keys on the setup phase. This mechanism is conducted in order to simplify key distribution and to achieve feasible computation overhead. In the other word, the readers and RFID tags do not have to generate their own private keys, thus efficient computation effort can be achieved. The private key for each RFID tag generated by KGF is denoted as $T = \frac{1}{s+t}P$, where *s* is master secret key and t = *H1*(RFID tag MAC Address) is a public key of the RFID Tag. The same way to calculate reader private key $R = \frac{1}{s+r}P$, where *r* is public key of the reader calculated as $r = H1$(reader MAC Address). In overall the KGF preloads (*Private Key (T or R), e, P, Q, g, H1 and H2*) to each legitimate RFID Tag and RFID Reader's memory.

3.3. *Authentication and Key Negotiation Phase*

After all public parameters and private key are successfully distributed, the reader and the tag are now ready to carry out mutual authentication and simultaneously negotiate the primary session key. Figure 1 illustrates the mutual authentication and key agreement by performing encrypted three-way handshake negotiation. The following list describes the three-way handshake procedure [13].

1. We presume that the RFID tag initially sleeps and wakes up after receiving beacon frame broadcasted by the RFID reader. Hereafter, the tag calculates the reader public key as $r = H1(reader\ MAC\ address)$. Subsequently, the tag randomly generates two 128 bit integer i and w, where i is temporary session key.
2. The tag then generates two ciphertexts $C1 = w(Q + rP)$ and $C2 = i \oplus H2(g^w)$. The tag subsequently requests to join in the RFID system by sending the two ciphertexts to the reader. The tag also includes its MAC address $t = H1(tag\ MAC\ address)$ in the encrypted payload, in order to protect its identity from being revealed by unauthorized party. In this case, all contents in the message including the session key i and the tag MAC address are encrypted using the reader public key. Thus, only the reader can decrypt the message.
3. The reader receives and decrypts the messages using its private key R. The reader can recover the session key i by calculating $i = H2(e(R, C1)) \oplus C2$. In order to achieve efficient communication, the reader tentatively saves the key i and the value of $C1$ for further steps. Each message created by the tag in the three-way handshake will use the initial session key i and the value of $C1$ will be used to calculate primary session key.

The temporary session key are shared based on the pairing function calculated as follows.

$$i = H2(g^w) \oplus C2 \qquad (1)$$

since

$$\begin{aligned} e(R, C1) &= e\left(\frac{1}{s+r} P, w(Q + rP)\right) \\ &= e(P, Q + rP)^{\frac{w}{s+r}} \\ &= e(P, (s + r)P)^{\frac{w}{s+r}} \\ &= e(P, P)^w = g^w \qquad (2) \end{aligned}$$

4. In the second message of the three-way handshake, the reader generate x and j as two random 128 bit integers, where j is temporary session key for processing all messages created by the reader. The reader afterward generates and send two ciphertexts $C3 = x(Q + tP)$ and $C4 = j \oplus H2(g^x)$. The reader also includes the values of $C1$ and $C2$ in the encrypted message to be further verified by the tag.

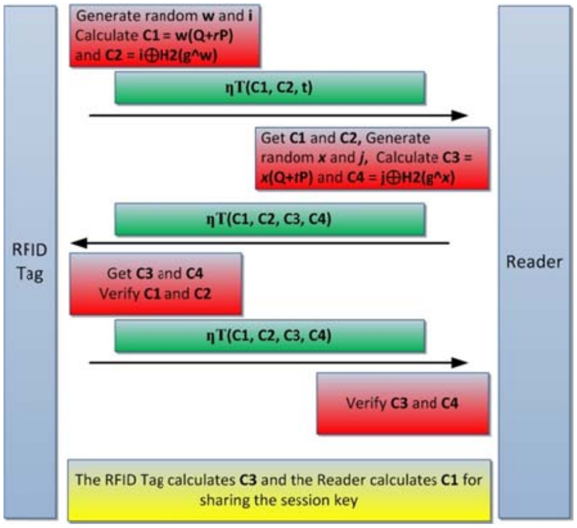

Fig. 1. Three-way handshake of IMAKA-Tate.

5. The tag then receives and decrypts the message which contains temporary session key j using its private key T. It is conducted by calculating $j = H2(e(T, C3)) \oplus C4$. The tag further verifies the value of $C1$ and $C2$. The further step is then continued only if the two values are same as the two values of $C1$ and $C2$ generated by the tag on the first message. Otherwise, the tag aborts the authentication. The tag also saves the value of $C3$ in order to calculate the primary session key.
6. The tag then sends back the value of $C3$ and $C4$ to be verified by the reader. The reader then process the message using the session key i that has been collected before. The further step is continued if the received values are equal as the values generated by the reader on the second message. Otherwise, the reader sends failure notification to abort the connection.

Up to this step, both parties have mutually authenticated to each other. In addition, they also effectively succeed to share the 128 bit primary session key. It is conducted by computing the two random values of $C1$ and $C3$ that have been securely exchanged on the three-way handshake. In this case:

- The tag computes $H2(e(T, C3)^w)$

- The reader computes $H2(e(R, C1)^x)$

Both parties calculate the same session, since:

$$\begin{aligned} \mathrm{e}(R, \mathrm{C1})^x &= \mathrm{e}(R, w(\mathrm{Q} + r\mathrm{P}))^x \\ &= e\left(\frac{1}{s+r}\mathrm{P}, w(s\mathrm{P} + r\mathrm{P})\right)^x \\ &= e(\mathrm{P}, (s\mathrm{P} + r\mathrm{P}))^{\frac{wx}{s+r}} \\ &= e(\mathrm{P}, \mathrm{P})^{wx} \qquad (3) \end{aligned}$$

and

$$\begin{aligned} \mathrm{e}(\mathrm{T}, \mathrm{C3})^w &= \mathrm{e}(\mathrm{T}, x(\mathrm{Q} + t\mathrm{P}))^w \\ &= e\left(\frac{1}{s+t}\mathrm{P}, x(s\mathrm{P} + t\mathrm{P})\right)^w \\ &= e(\mathrm{P}, (s\mathrm{P} + t\mathrm{P}))^{\frac{wx}{s+t}} \\ &= e(\mathrm{P}, \mathrm{P})^{wx} \qquad (4) \end{aligned}$$

The reader and the tag generate fresh random values of *x* and *w* for every new session. Hence, such method provides perfect forward and backward secrecy that differentiates the past and the future session. In this case, even an adversary can compromise the tag as well as successfully recorded the past session, there is no chance for the adversary to compromise the future session.

3.4. *Mutual Authentication over EAP*

In order to achieve efficient and flexible communication that can be used for large-scale RFID system, IMAKA-Tate transports the authentication messages through standard EAP method as described in (RFC 3748) [12]. Figure 2 illustrates the IMAKA-Tate over EAP, which is described as follows.

1. Initiation request: Initially, the tag starts the three-way handshake by sending the two encrypted values of C1 and C2 to the reader. The tag also includes its identity (i.e. the tag public key) in the encrypted payloads. In this regards, only the targeted recipient, which is the legitimate reader can decrypt the message. This mechanism protects the tag identity from being revealed by unauthorized party. It is to be noted that the tag can easily find the reader MAC Address since it is periodically broadcasted by the reader through the beacon frame. Moreover, distinct to common EAP method, IMAKA-Tate over EAP bypass the identity exchange, since it works based on MAC Address.
2. EAP Request IBE Challenge: Upon receiving the initiation request, the reader decrypts the message, sequentially saves the value of C1 for calculating the primary session key. The reader challenges the legitimate tag as described in the three-way handshake, by sending the encrypted values of C3 and C4, as well as sends back the values of C1 and C2 to be further verified by the tag.

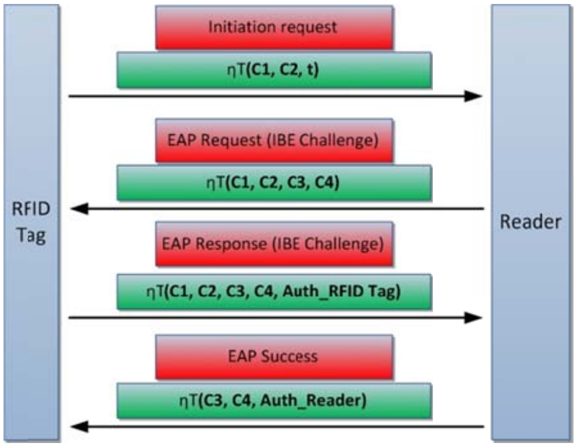

Fig. 1. IMAKA-Tate over EAP.

3. EAP Response IBE Challenge: Upon receiving the IBE Challenge, the tag decrypts the message and verifies the values of C1 and C2. The tag sends Auth_Tag if the values of C1 and C2 received from the reader are same as the Value s of C1 and C2 created on the initiation request. Otherwise the tag sends authentication failure and the connection is discarded. If the values are verified, the tag then saves the value of C3 created by the reader to further calculate the primary session key.
4. EAP Success: Upon receiving response IBE Challenge, the reader verifies the values of C3 and C4 sent by the tag. The reader send the encrypted EAP success if the values are matched as the values created by the reader on the EAP Request IBE Challenge. Otherwise the reader discards the connection by sending the authentication failure.

Up to this step, both parties have successfully carried out mutual authentication and negotiated the primary session key. In order to ensure the freshness of each established session, all generated random values in this case *t, w, u,* and *x* must be deleted each time the session will be established. In same way, all the random values are also eradicated when mutual authentication is not successfully conducted.

3.5. *EAP IMAKA-Tate Message Format*

IMAKA-Tate aims at providing light-weight security protocol that maintains the size of authentication payload as optimally minimum. This feature is to enable efficient communication overhead which mitigates the common problem RFID system (i.e. drainage of battery power). Figure 3 illustrates IMAKA-Tate packet format transported over EAP, including 6 Bytes packet header, 32-64 Bytes encrypted payload, and 2 Bytes Authentication message.

The packet header is structured as standard EAP fields defined in (RFC 3748), including one-octet Code, one-octet Identifier, two-octet Length and one-octet Type. In addition, IMAKA-Tate proposes complement header field called IMAKA-Tate Exchange, is one-octet in length that identifies the encrypted-authentication messages. The values are identified as follows.

- 1 = IBE Challenge-EAP Request/Respond
- 2 = IBE Failure Notification

Furthermore, IMAKA-Tate transports encrypted payload in IBE Request and Respond challenge message. The encrypted payloads are composed as follows.

- The Values of C1, C2, C3, and C4 are each encrypted 16 Bytes that are transported during the IBE Challenge request and respond message.
- Either the Encrypted Auth_Tag or Auth_Reader is 2 Bytes notification from the tag that is attached during the IBE Challenge respond message.

According to IMAKA-Tate packet format depicted in figure 3, the maximum size of authentication packet is 72 Bytes, which is transported during IBE Challenge respond message (see figure 2). Therefore, it is definitely suitable for RFID system that associates to limited resources (i.e. low-date rate, low CPU and battery power).

4. Security Analysis

In this section, we analyses the security strength of IMAKA-Tate [13] against various risks in smart RFID system. In addition, we discuss the security features that enable trust and integrity protection in large-scale smart RFID applications.

4.1. *Attacks from RFID Reader Side*

In RFID system, an adversary may impersonate as legitimate reader by creating rogue reader in order to elicit sensitive information. Hence, an adversary can exploit the sensitive information to perform malicious activities and attacks, which are listed as follows.

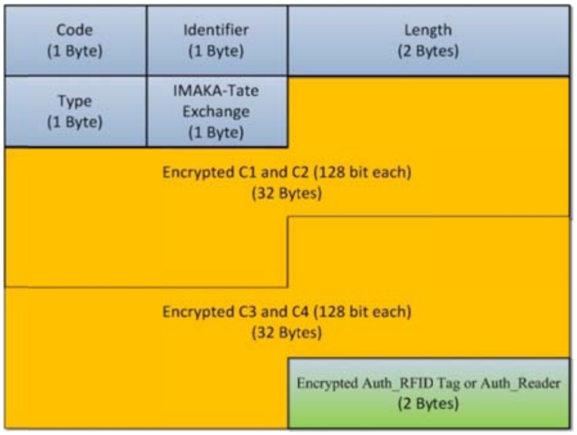

Fig. 1. Fig. 3. EAP IMAKA-Tate packet format.

- Spoofing information: An adversary may exploit the rogue reader to perform fraudulence, such as RFID data manipulation, reporting wrong identification, even it can be exploited to perform various MITM attacks (e.g. replay attack, Dos, etc.).
- Fooling RFID tags: The existence of rogue reader may be used to trick the legitimate RFID tags to reveal their credentials. In this case, the RFID tags are fooled that they are communicating with legitimate reader. Hence, an adversary can use the revealed credentials to impersonate as legitimate tags. In this case the attacker can launch various attacks based on impersonation technique (i.e. cloning attacks, tag emulating, and collision attack).

Nevertheless, an adversary cannot acquire the critical parameters (i.e. *e, P, Q, g, H1* and *H2*) that secretly pre-load before the network deployment. This issue makes the rogue reader calculates wrong session key and will not able to perform mutual authentication on the three-way handshake. Thus, IMAKA-Tate can mitigate the aforementioned threats by preventing the rogue reader to be connected and authenticated in the smart RFID system.

Let us presume that the rogue reader uses different parameters (i.e. *e', P', Q', g', H1'* and *H2'*). In this case, the rogue reader is not able to respond the three-way handshake requested by the tag. Moreover, the rogue reader is not able to find the crucial parameter called master secret key *s*, as it is known only by the KGF. Hence, the rogue reader is not able to correctly generate its private key. Let us presume that the rogue reader uses different master secret key $k \neq$ s. The rogue reader then incorrectly generates its public key $r_{Rog} \neq r$ and private key $R_{Rog} \neq R$:

$$r_{Rog} = H1\text{'}(rogue\ reader\ MAC\ address) \quad (5)$$

$$R_{Rog} = \frac{1}{k+r_{Rog}} P\text{'} \quad (6)$$

Moreover, the rogue reader cannot correctly calculate the initial session key *i*, since:

$$i \neq H2\text{'}(e\text{'}(R_{Rog}, C1)) \oplus C2 \quad (7)$$

Since the initial session key *i* is calculated incorrectly, the rogue reader cannot decrypt the initiation message *ηT(C1, C2, t)*. Hence, the rogue reader cannot find the tag MAC Address in order to respond the message. Moreover, the challenge is more complicated for adversary, as it is not possible to convert *t* value to tag MAC address based on the incorrect parameter *H1*', since:

$$t \neq H1\text{'}(tag\ MAC\ address) \quad (8)$$

An adversary may conduct social engineering to inquiry the tag's MAC Address attached on the user device. However, the adversary in this case the rogue reader is still not able to correctly generate the tag's public key and the two ciphertexts based on the incorrect parameters. This issue makes the tag is not able to calculate the temporary session key *j*. Let us presume that the rogue reader generates $t' \neq t$, *C3' ≠ C3* and *C4' ≠ C4*:

$$t' = H1\text{'}(tag\ MAC\ address) \quad (9)$$

$$C3\text{'} = x(Q\text{'} + t\text{'}P\text{'}) \quad (10)$$

$$C4\text{'} = j \oplus H2\text{'}(g'^{x}) \quad (11)$$

However the tag wrongly calculates the key *j*, since:

$$j \neq H2(e(T, C3\text{'})) \oplus C4\text{'} \quad (12)$$

Hence, the tag aborts the connection as the value of *C1* and *C2* attached on *ηT(C3', C4', C1, C2,)* cannot be verified.

Furthermore, both parties are not able to correctly generate and share the primary session key, as the tag calculates:

$$\begin{aligned} e(T, C3')^{w} &= e(T, x(Q' + t'P'))^{w} \\ &= e\left(\frac{1}{s+t} P, x(kP' + t'P')\right)^{w} \\ &= e(P, (kP' + t'P'))^{\frac{wx}{s+t}} \\ &= e(P, P')^{\frac{wx(k+t')}{s+t}} \quad (13) \end{aligned}$$

On the other hand the rogue reader calculates:

$$\begin{aligned} e'\left(R_{Rog}, C1\right)^{x} &= e'(R_{Rog}, w(Q + rP))^{x} \\ &= e'\left(\frac{1}{k+r_{Rog}} P', w(sP + rP)\right)^{x} \\ &= e'(P', (sP + rP))^{\frac{wx}{k+r_{Rog}}} \\ &= e'(P', P)^{\frac{wx(s+r)}{k+r_{Rog}}} \quad (14) \end{aligned}$$

By taking into account an adversary has chance to steal the unsupervised RFID tag. In this case, an adversary can copy all valid parameters (i.e. e, P, Q, g, H1 and H2) that are needed to impersonate as rogue reader. However, the master secret key *s* is owned only by the KGF and it is never shared to any party, neither to the reader nor to the tag. This challenge makes the adversary cannot generate the correct private key for the rogue reader. Let us presume that the rogue reader use incorrect master secret key $k \neq s$. The rogue reader incorrectly generates its private key R_{Rog}:

$$R_{Rog} = \frac{1}{k+r_{Rog}} P \quad (15)$$

Hence the rogue reader is not able to generate correct initial session key *i* as described in equation (1) and (2), since:

$$\begin{aligned} e\left(R_{Rog}, C1\right) &= e(R_{Rog}, w(Q + rP)) \\ &= e\left(\frac{1}{k+r_{Rog}} P, w(sP + rP)\right) \\ &= e(P, (sP + rP))^{\frac{w}{k+r_{Rog}}} \\ &= e(P, P)^{\frac{w(s+r)}{k+r_{Rog}}} = g^{\frac{w(s+r)}{k+r_{Rog}}} \quad (16) \end{aligned}$$

In this case:

$$i \neq H2(g^{\frac{w(s+r)}{k+r_{Rog}}}) \oplus C2 \quad (17)$$

4.2. *Privacy Issue and Attacks from RFID Tag*

As RFID tag can naturally be read without authorization, this issue introduces tremendous problem related to privacy of RFID user. An adversary can reveal the tag identity and observe sensitive information, in order to perform malicious activates, which are listed as follows.

- An adversary may conduct unauthorized tracking based on the revealed identity. This issue definitely introduces tremendous problem as an adversary may conduct further malicious activates (e.g. espionage, theft, robbery, etc.).
- An adversary may conduct unauthorized tag reading in order to elicit sensitive information that can be used for impersonation activities (e.g. masquerading as legitimate RFID tag). This issue makes an adversary has chance to conduct unwanted activities such as fraudulence.

- An adversary can perform various techniques of resource consumption attacks based on the revealed identity. The adversary can waste the tag bandwidth and drain the battery by insistently sending packets to the revealed identity as destination address.
- An adversary initially reveals the user identity as one of requirements that is needed to successfully perform various attacks (i.e. replay attack, sybil attack, and various attacks based on revealed identity).

Nevertheless, IMAKA-Tate performs the encryption method that includes the tag identity since in the initiation request of mutual authentication. Particularly, the tag firstly hashes its MAC Address to 128 bit integer *n = H1(tag MAC address)*. Subsequently, it is enclosed to the encrypted payload of the initiation request *ηT(C1, C2, n)*. Hence, there is no chance for an adversary to reveal the user identity since it encrypts even before the mutual authentication is started.

4.3. *Security Features*

The following list outlines the security features offered by IMAKA-Tate [13], which is also match to provide trust and integrity protection in smart RFID environment.

- Mutual Authentication and Key Agreement: IMAKA-Tate establishes mutual authentication that each participant generates random challenge, which is encrypted by the corresponding public key of the recipient. Such mechanism ensures that only targeted recipient can decrypt and correctly answer the challenge. This procedure is conducted in mutual way. In this case, they exchange and verify the ciphertexts of (*C1, C2)* and (*C3, C4)*. This feature can also prevent various MITM attacks (e.g. replay attack, reflection attack, DoS, etc.). Furthermore, both parties simultaneously negotiate the primary session key based on the exchanged challenge. In particular, the reader and the tag calculate the same session key:

$$e(R, C1)^x = e(T, C3)^w = e(P, P)^{wx} \quad (18)$$

- Session robustness: On each established session, both participants freshly generate random 128 bit integer attached in the encrypted message that they exchange to each other. In particular, the tag generate random 128 bit w enclosed in chipper text $C1 = w(Q + rP)$, while the reader generate 128 bit x enclosed in $C3 = x(Q + tP)$. Thus, both participants generate the same session key. The reader generates:

$$H2(e(R, w(Q + rP))^x) = g^{wx} \quad (19)$$

And the tag generates:

$$H2(e(T, x(Q + tP))^w) = g^{wx} \quad (20)$$

Hence, in case an adversary with very good fortune is able to compromise the past session, he/she somehow will not able to compromise the following session, since the established session is always fresh and will not correspond to any past or even future session.

- Light-weight communication overhead: To achieve efficient battery and bandwidth consumptions, IMAKA-Tate maintains the communication overhead as minimum as possible. According to IMAKA-Tate packet format depicted in figure 3, the maximum size of authentication packet is only 72 Bytes, which is transported in EAP respond-IBE Challenge (see figure 2). Therefore, it is suitable for RFID system that associates to limited resources, such as low-date rate, limited CPU and battery.
- Light-weight cryptographic operation with high-level security strength: IMAKA-Tate uses 128 bit security strength of ηT paring. This method is known as the most light-weight cryptographic operation, even it is feasible for the most constrained sensor node [4]. In addition, such security strength is about same as the 3072 bit of RSA method. Thus, it is strong enough to protect the RFID system against various techniques of brute-force attacks.

5. Computation Analysis

In order to ensure that cryptographic processing in IMAKA-Tate is feasible for smart RFID system, we estimated computation overhead by conducting benchmark tests adopted from [3]. The benchmark tests estimated the computation overhead of all parameters that are needed to construct 128 bit ηT pairing over $F_{3^{509\,x\,6}}$. The code of such benchmark test is written in C++ adapted from [1], which was compiled with Visual Studio 2008. The benchmark test was executed in our platform under Windows 7 with 64-bit Intel 2 Cores at 1.8 GHz. In order to emulate the smart RFID system, we forced the processor to run in single core and scaling down the clock frequency according to three options of Imote2 platform (i.e. 104 MHz, 208 MHz and 416 MHz). In addition, to achieve accurate estimation the benchmark test executed the cryptographic operations in multiple times (i.e. 1000 iterations).

We further calculated basic operations of each phase in IMAKA-Tate. The first phase is three-way handshake of mutual authentication, while the second phase is primary session key generation. Table I summarizes computation overhead of IMAKA-Tate calculated by each smart RFID tag. On the mutual authentication phase, each participant calculates the same parameters which are two Multiplication over $F_{3^{509x6}}$, one Exponentiation over $F_{3^{509x6}}$ and one ηT Pairing. After both parties have successfully authenticated to each other, they afterward generate the primary session key by each calculating one more ηT Pairing. It is to be noted that we only show the computation result of RFID tag, as we assume that the reader has stronger processor clock to process the cryptographic operation.

Table 1. Estimation of RFID Tag computation in 1000 Iterations.

Phase	Processor	Time Estimation
Mutual Authentication	104 MHz	57.32 *ms*
	208 MHz	35.93 *ms*
	416 MHz	23.57 *ms*
Generating Primary Session Key	104 MHz	54.54 *ms*
	208 MHz	34.34 *ms*
	416 MHz	22.79 *ms*

According to the benchmark test implied in Table I, the RFID tag at 416 MHz calculated both phases which are mutual authentication and generating primary session key in 0.046 sec. On the other hand, the RFID tag at 104 MHz calculated both phases in 0.11 sec. It is therefore concluded, IMAKA-Tate method is remarkably feasible to be applied in smart RFID system. It is even affordable for the smart RFID tag with lower co-processor clock at 104 MHz.

6. Conclusion

IMAKA-Tate offers light-weight identity protection and mutual authentication that satisfies the specific requirement for security and privacy in smart RFID system. In this regards, the proposed solution performs encryption of the smart RFID tag identity even before the mutual authentication is started. This method prevents the tag identity from being revealed by unauthorized party. Therefore, privacy preserving can be achieved well. Furthermore, the security analysis of IMAKA-Tate has demonstrated that it can mitigate various possible threats in the smart RFID system, including unauthorized tracking and tag reading, cloning attack, impersonation, and resource consumption attack. Moreover, we demonstrated in the computation analysis that IMAKA-Tate is feasible to be applied in the constrained nature of smart RFID system.

References

1. J.-L. Beuchat, E. Lpez-Trejo, L. Martnez-Ramos, S. Mitsunari, F. Rodrguez-Henrquez, “Multi-core implementation of the tate pairing over supersingular elliptic curves,” Proceedings of the 8th International Conference in Cryptology and Network Security, December, 2009.
2. X. Xiong, D. Wong, X. Deng, “Tinypairing: A fast and lightweight pairing-based cryptographic library for wireless sensor networks,” IEEE Wireless Communications and Networking Conference (WCNC), 2010.
3. C. Mulkey, D. Kar, A. Katangur, “Towards an Efficient Protocol for Privacy and Authentication in Wireless Networks,” The 12th International Conference on Security and Management, 2013.
4. P. Szczechowiak, M. Collier, Tinyibe: Identity-based encryption for heterogeneous sensor networks, in: 5th International Conference on Intelligent Sensors, Sensor Networks, and Information Processing, 2009.
5. V. Kolesnikov, G.S. Sundaram, “IBAKE: Identity-Based Authenticated Key Exchange Protocol, IACR Cryptology ePrint Archive,” 2011.
6. V. Kolesnikov and C. Rackoff, Key exchange using passwords and long keys. In Theory of Cryptography, LNCS volume 3876, Springer, 2006.
7. Vladimir Kolesnikov and Charles Rackoff. Password mistyping in two-factor- authenticated key exchange. In ICALP (2), pages 702-714, 2008.
8. V. Cakulev, G. Sundaram, and I. Broustis, “IBAKE: Identity-Based Authenticated Key Exchange,” RFC 6539, March 2012.
9. D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," in Proc. of CRYPTO 01, LNCS 2139, pp. 213-229, 2001.
10. D. Boneh and X. Boyen, "Efficient selective-ID secure identity based encryption without random oracles," In Proc. of EUROCRYPT, 2004.
11. V. Cakulev and I. Broustis, “An EAP Authentication Method Based on Identity-Based Authenticated Key Exchange,” draft-cakulev-emu-eap-ibake-03.txt, August 2012, work in progress.
12. B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, H. Levkowetz, “Extensible Authentication Protocol (EAP),” RFC: 3748, June 2004.

13. M.F. Sadikin, M. Kyas, "IMAKA-Tate: Secure and Efficient Privacy Preserving for Indoor Positioning Applications," The 5th Int. Conf. on Smart Communications in Network Technologies (SaCoNet), 2014.