симо от времени суток и погодных условий, что является важным для нужд национальной экономики и обороны. Однако, согласно характеристикам механизма построения РСА-изображений, геометрические искажения и, своего рода, мультипликативный шум, известный как когерентное оптическое излучение, зачастую, искажают полученное изображение. Классификация РСА-изображений является основой их интерпретации. Из-за влияния спекл-шума традиционные технологии классификации изображений работают недостаточно хорошо. В статье описан предложенный нами эффективный метод классификации поляриметрических РСА-изображений, основывающийся на поляриметрических свойствах, данных об интенсивности рассеянного излучения и метода нечеткой кластеризации С-средних.

Методика. Совместив рассеивающие свойства полностью поляриметрического РСА-изображения и данные об интенсивности рассеянного излучения, мы получили результат предварительной классификации РСА-изображения. Окончательный результат классификации поляриметрического РСА-изображения был получен с помощью алгоритма нечеткой кластеризации С-средних.

Результаты. Экспериментально доказано, что предложенный метод превосходит традиционные методы классификации полностью поляриметрических РСА-изображений.

Научная новизна. В предложенном методе учитываются не только свойства полностью поляриметрических РСА-данных, но и информация о статистических характеристиках. Метод позволяет получить хорошие результаты классификации поляриметрических РСА-изображений с сохранением рассеивающих свойств (в некоторой степени).

Практическая значимость. Экспериментальные исследования показали, что предложенный алгоритм сохраняет текстуру и детали РСА-изображения лучше, чем традиционные методы, и дает лучший результат классификации полностью поляриметрических РСА-изображений. Метод может использоваться для решения задач интерпретации РСА-изображений.

Ключевые слова: *поляриметрическое РСА-изображение, когерентное оптическое излучение, классификация изображений, H/α/A/SPAN, распределение Вишарта, метод нечеткой кластеризации С-средних*

Рекомендовано до публікації докт. техн. наук В.В. Гнатушенком. Дата надходження рукопису 15.10.14.

Hongyan Kang

Heze University, Heze, Shandong, China

ANALYSIS AND REALIZATION OF RFID GROUPING-PROOF PROTOCOL BASED ON ELLIPTIC-CURVES CRYPTOGRAPHY

Хунянь Кан

Університет Хецзе, м. Хецзе, провінція Шаньдун, КНР

АНАЛІЗ І РЕАЛІЗАЦІЯ ПРОТОКОЛУ ОБМІНУ СИГНАЛІВ РАДІОЧАСТОТНОЇ ІДЕНТИФІКАЦІЇ НА ОСНОВІ ЕЛІПТИЧНОЇ КРИПТОГРАФІЇ

Purpose. With the wide application of RFID (Radio Frequency Identification) systems, scholars have become highly concerned about the design of efficient and secure grouping-proof protocols. Responding to the problems of privacy protection, security and efficiency of existing grouping-proof protocols, a new ECC (Elliptic Curves Cryptography) based RFID grouping-proof protocol is proposed after the analysis of existing grouping proof protocols.

Methodology. Some ECC-based grouping-proof protocols cannot resist impersonation attack and other common attacks, since there is no reader and verifier authentication or the reader and the verifier can be untrusted, one can also query the tags actively to collect the attack tuple and trick genuine reader and verifier. So we propose a scheme can realize the authorized access and mutual authentication of tags, readers, and verifier.

Findings. This paper attempts to expound on the initialization phase, the authorization phase, the group proof generation phase, and the group proof verification phase of the new grouping-proof protocol, and also make analyses in terms of privacy preservation, untraceability, reader anonymity, tag anonymity, authorization and authentication, etc.

Originality. In comparison to currently available ECC-based grouping-proof protocols, this protocol can realize the authorized access and mutual authentication of tags, readers, and backend servers.

Practical value. Analysis results show that this new project meets the security and privacy requirements of RFID system grouping-proof protocols, demonstrating better scalability and higher efficiency than similar protocols.

Keywords: *grouping-proof protocol, authorization authentication, mutual authentication, Elliptic Curves Cryptography, RFID*

Introduction. In recent years, it was found that RFID systems had to prove that certain items must COEXIST in some applications. There are many application scenarios of this type: A doctor prescribes medicines in the same prescription to reduce dosage risks for his patients; in the pharmaceutical industry, drug manufacturers ensure that drugs and prescriptions are sold together; at airports, boarding pass, passport and baggage are generated as a group to ensure security. In these applications, it is insufficient to ensure the security of a single entity. It is necessary to verify whether multiple entities are simultaneously in a group. The completeness and security of these entities can be guaranteed only in this approach. Identification and coexistence proof of group tags is called tag grouping proof.

Grouping proof protocols fall into two types according to data collection method: serial grouping proof protocols and broadcasting grouping proof protocols. In data collection of a serial grouping proof protocol, the reader generates a query command and sends it to the first tag. After receiving the response from the first tag, the reader sends the query command to the second tag after processing the data received from the first tag. All other tags are processed sequentially. The reader generates grouping proof only when it receives the response from the last tag. In a broadcasting grouping proof protocol, the reader broadcasts a query command and all tags respond to the command. The reader then collects all these responses and generates a grouping proof according to these responses. An effective RFID grouping proof protocol shall, with guaranteed protocol security, reduce tag calculation to the greatest extent to expand its application range. To achieve this objective, this paper proposes an RFID grouping proof protocol based on ECC.

The remainder of this paper is organized as follows. Section 2 briefly reviews grouping-proof protocols based on symmetric cryptography, Gen2 Standards and ECC, and conclude their disadvantages. Section *3* we analyze the security requirements of grouping-proof protocols. We present a novel RFID grouping-proof protocol which consists of four steps in section *4*. Security analyses and comparisons of the proposed protocol and other related work are addressed in section *5*. Finally, we give the concluding remarks in section *6*.

Related work. This section describes and analyzes existing types of grouping proof protocols, then further concludes their disadvantages.

Grouping proof protocols based on symmetric cryptography. Juels et al. [1] were pioneers in the research of multiple tag scanning. They first introduced a proof approach with two coexistent tags based on the idea of mutual signature of two tags. It was called yoking-proof by the authors, implying that the two tags were scanned simultaneously. But the protocol then was proved that the solution by Juels was vulnerable to reply attacks. They resolved the security problem of reply attacks by introducing a timestamp to each session. Their newly designed protocol could provide coexistence proof for a group of tags. Considering that timestamps are predictable, Piramuthu [2] proved that timestamps failed to completely resist reply attacks and then suggested replacing timestamps with random numbers to resist this type of attacks. But the protocol was indicated that the grouping proof protocol based on random numbers was not secure in multi-session jamming attacks. Burmester et al. [3] proposed a security model based on Universal Composability Framework for tag grouping proof. The model was, however, found vulnerable to various impersonation attacks. Later, grouping proof protocols irrelevant to tag response sequence were proposed, and thus improved the efficiency of tag grouping proof protocols. However, there was a risk of tag identification leaks in their grouping proof protocol, which violated tag privacy.

Grouping proof protocols based on Gen2 Standards. The grouping proof protocol complied with Gen2 standards, which only Cyclic Redundancy Check Code (CRC) and pseudo-random number generator were used in grouping verification. However, there was a synchronous relationship between the verification processes of group tags, i.e. the response output of the current tag was the input to the next tag. In this design, response information of tags could not be processed concurrently. Chien et al. [4] consider that the protocol is vulnerable to reply attack while Peris-Lopez et al. [5] insist that the protocol is vulnerable to impersonation attack. To resolve security flaws, Chien et al. [4] proposes two grouping proof protocols: online mode and offline mode. Peris-Lopez et al. [5], however, also proved that these two protocols were vulnerable to impersonation attack.

Grouping proof protocols based on ECC. In order to achieve strong privacy preservation, it was necessary to introduce public key algorithm to RFID verification protocols to prevent tag identification leaks, and the possibility to introduce public keys, especially ECC to RFID protocols was discussed. Batina et al. [6] first put forward the privacy-preserving RFID grouping proof protocol based on ECC, which was however with timeout problem. Moreover, Lv et al. [7] indicated that it could not resist tracking attack and thus proposed an enhanced protocol. Ko et al. [8] later found the protocol by Lv et al. [7] with a flaw and further proved that it could not work and then proposed an enhanced protocol to resist tracking attack. In 2012, Lin et al. [9] proposed a protocol to improve the efficiency of Batina et al. [6], resolving the timeout problem in the generation of grouping proofs. A few follow-up pieces of literature similarly proved security and privacy-preserving problems of the above-mentioned protocols and proposed relevant improvement measures.

Security requirements of grouping-proof protocols. In a grouping proof RFID interaction protocol, the main purpose of adversary attack is to obtain grouping proofs p that can pass verification. However, the tag proved to be existent $\mathrm{T}_{i,j}$ does not actually participate in the protocol or is not a valid member of the group. Another purpose of the adversary attack is to obtain privacy information of tags and the reader, such as identification, location, and group information.

Attack channels of an adversary A fall into two types: the attack on information channels and attack on participating entities. Let's assume that an adversary can completely control the communication channels between tags and the reader as well as between the reader and the backend server. It cannot only arbitrarily read, delete, tamper, delay delivery and rep-lay any messages in the channels but also initiate any session with any entity anytime. Let us also assume that the adversary A can also capture any entity of tags and the reader anytime during protocol execution. For a corrupted entity, the adversary A can get the internal status data successfully but cannot get the private key of it.

Security requirements of RFID grouping proof protocols in the Internet of Things:

Strong privacy preservation: Only authorized readers can read the coexistence proof of a tag group. In addition, an attacker cannot get any identification or grouping information even if he maliciously captures all messages in all interactions.

Untraceability: An attacker cannot identify the relationship between two proofs $\{P_i\}$ and $\{P_j\}$ through a captured grouping proof set $\{P_i\}$. This means that he cannot associate whether the generators of two grouping proofs belong to the same group, nor can he identify whether the generators of two proofs contain the same member.

Reader anonymity: In protocol execution, any attacker or tag cannot get the identification of a reader.

Tag anonymity: Similar to reader anonymity, neither an attacker nor a reader can get tag identification or grouping information.

Authorization: Valid grouping proofs are available only when authorized readers and valid group member tags correctly execute the protocol. Any unauthorized reader cannot get valid grouping proofs.

A novel RFID grouping-proof protocol. A grouping proof verification message shall be able to verify the following at the server:

(1) Reader and tag validity: verify that the message is generated by valid readers and tags. Tag validity falls into two aspects: First, if there is no attack on a tag, it can identify the correct master tag communication key. On the other hand, the tag and other tags participating in grouping proof generation are members of the same tag group.

(2) Validity of authorized reader access: This grouping proof verification message shall be able to prove that the reader has access to the tag group, i.e. already authorized access to the tag group.

(3) Grouping proof validity: Grouping proofs generated are valid only when authorized readers and valid group member tags correctly execute the protocol proof, as well as all tags of a tag group, participate in the generation of the grouping proofs.

The following principles shall be taken into account in protocol design to ensure correctness and security of a grouping proof protocol:

(1) In the generation of a grouping proof protocol, the correctness of tag grouping proof protocol must be guaranteed. In addition, the identifications of a single tag and reader must be authenticated. Only grouping proof information provided by valid tags and readers is acceptable.

(2) In the generation of a grouping proof protocol, the privacy and security of each individual tag shall be considered. Those of tags as an integrated group shall also be addressed.

(3) The improvement of grouping verification shall be considered from the complexity of individual tag, entire tag group, and verification processing.

A new RFID grouping proof protocol has been designed according to the above-mentioned functionality and security analysis of grouping proof protocols. The RFID system consists of three entities: tag, reader, and server. There are four phases in the RFID grouping proof protocol. They are respectively the initialization phase, the authorization phase, the grouping proof generation phase, and the grouping proof verification phase. In the initialization phase, communication keys are distributed to tags and readers. In the authorization phase, readers are authenticated. Readers that pass verification will be authorized read and write access to a certain tag group. In the grouping proof generation phase, coexistence proofs are generated for multiple tags. In the grouping proof verification phase, whether a group of tags can be read and written simultaneously is identified by authenticating the validity of grouping proofs.

The notations used in the protocol are shown in table 1.

Table 1

Notations in the Protocol

Notations	Meaning
P	Base point in the EC group
y , Y	Server's private key and public key
v , V	authorization private key and public key
$x_{G,i}$, $X_{G,i}$	Tag's group private key and public key
$x_{i,\mathrm{j}}$, $X_{i,j}$	Tag's private key and public key
k_k , K_k	Reader's private key and public key
$\dot{r}(x)$	The x-coordinate of x
r, c	Random number

The initialization phase. The backend server selects a random numb $y \in Z_l$ as its private key and calculate $Y(= yP)$ to get its public key. For tag $T_{i,j}$ select random number $x_{G,i}, x_{i,j} \in Z_l$ as its private key. $x_{G,i}$ Is the private key of the group of tag $T_{i,j}$. Its public key is $X_{G,i} = x_{G,i}P$. $x_{i,j}$ is its identification private key. Its public key is $X_{i,j} = x_{i,j}P$. For reader R_k , select a random number k_k as its private key. Its public key is $K_k = k_kP$. Calculate $X_i(= x_iP)$ to get the i th tag's identification ID_i and store $\{ID_i, y\}$ and other information in a database. Store $\{(x_{G,i}, x_{i,j}), Y, K_k\}$ in the tag.

Let us assume that each reader R_k has a unique identification ID_{R_k}. Calculate $X_{i,j}(= x_{i,j}P)$ to get the j th tag's identification $ID_{T_{i,j}}$. The initialization process of readers and tags is shown in fig.1.

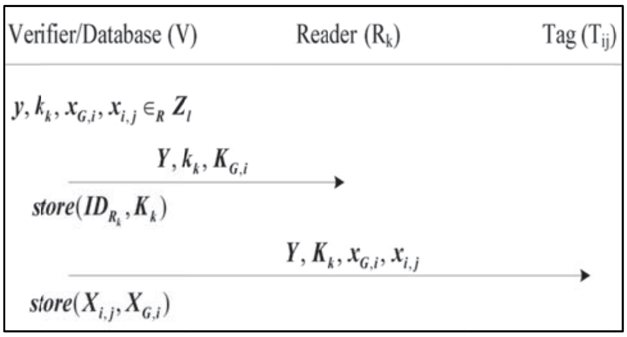


Fig. 1. The initialization phase

Verifier V generates registration information $(Y, k_k, K_{G,i})$ for reader R_k and send it to the reader. The verifier V also stores information (ID_{R_k}, K_k) to its registration database.

Verifier V generates registration information $(x_{G,i}, x_{i,j})$ for each tag and send $\{(x_{G,i}, x_{i,j}), Y, K_k\}$ to tag $T_{i,j}$. The verifier V also stores information $(X_{i,j}, X_{G,i})$ to its registration database.

The authorization phase. When it first reads a tag group $X_{G,i}$, a reader needs verifier V to authorize read/write access to the tag group. The reader generates a random number r, calculate T_0, T_1 and send it to verifier V. The verifier calculates $X'_{G,i} = T_1 - yT_0$, and search its registration database to identify whether $X_{G,i} = X'_{G,i}$ exists. If $X_{G,i} = X'_{G,i}$ exists, the verifier generates a random number $v \in Z_l$ and sen $V = vP$ to the reader. Meanwhile, the verifier stores $(ID_{R_k}, X_{G,i}, v)$ to its authorization database. Otherwise, protocol execution aborted. A prompt of failure is returned. This type of authorization application is nonrecurring, i.e. not required for every information exchange unless the operation is changed to another tag group. See fig. 2 for the detailed process.

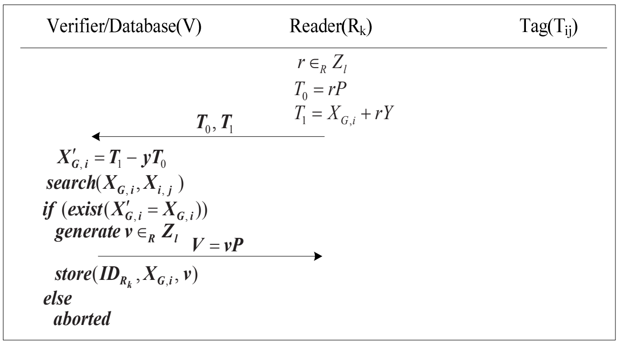


Fig. 2. The authorization phase

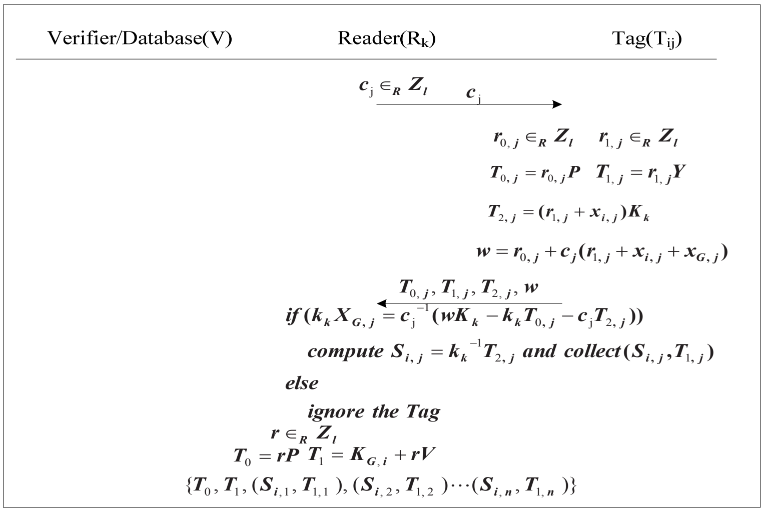

Verifier/Database(V)
Reader(R$_k$)
Tag(T$_{ij}$)
$c_j \in_R Z_l$
c_j
$r_{0,j} \in_R Z_l \quad r_{1,j} \in_R Z_l$
$T_{0,j} = r_{0,j}P \quad T_{1,j} = r_{1,j}Y$
$T_{2,j} = (r_{1,j} + x_{i,j})K_k$
$w = r_{0,j} + c_j(r_{1,j} + x_{i,j} + x_{G,j})$
$T_{0,j}, T_{1,j}, T_{2,j}, w$
$if\ (k_k X_{G,j} = c_j^{-1}(wK_k - k_k T_{0,j} - c_j T_{2,j}))$
$compute\ S_{i,j} = k_k^{-1} T_{2,j}\ and\ collect(S_{i,j}, T_{1,j})$
$else$
$ignore\ the\ Tag$
$r \in_R Z_l$
$T_0 = rP\ T_1 = K_{G,i} + rV$
$\{T_0, T_1, (S_{i,1}, T_{1,1}), (S_{i,2}, T_{1,2}) \cdots (S_{i,n}, T_{1,n})\}$

Fig. 3. The grouping proof generation phase

The grouping proof generation phase. Reader R_k generates a random number c_j and send it to the tag group $X_{G,i}$ via broadcast packets. After receiving the broadcast packets, tag $T_{i,j}$ selects random number $r_{0,j}$ an $r_{1,j}$, calculate $T_{0,j} = r_{0,j}P$, $T_{1,j} = r_{1,j}Y$, $T_{2,j} = (r_{1,j} + x_{i,j})K_k$ and $\mathrm{w = r_{0,j} +}$ $+\mathrm{c_j(r_{1,j} + x_{i,j} + x_{G,i})}$, and send $(T_{0,j}, T_{1,j}, T_{2,j}, w)$ back to reader R_k. The reader verifies $\mathrm{k_k X_{G,i} ? = c_j^{-1}(wK_k -}$ $\mathrm{-k_k T_{0,j} - c_j T_{2,j})}$. If the two sides are equal, tag $T_{i,j}$ belongs to group $X_{G,i}$. The reader then calculates $S_{i,j} = k_k^{-1} T_{2,j}$. Otherwise, the reader ignores the tag. Reader R_k selects a random number r and calculates $T_0 = rP$ and $T_1 = K_{G,i} + rV$. Reader R_k collects information of all tag group $X_{G,i}$ members' information $(S_{i,j}, T_{1,j})$, generates grouping proof information $(T_0, T_1, (S_{i,1}, T_{1,1}), (S_{i,2}, T_{1,2}), \cdots, (S_{i,n}, T_{1,n}))$, and send it to verifier V. See fig. 3 for the detailed process.

The grouping proof verification phase. Verifier V receives a group of information $\mathrm{(T_0, T_1, (S_{i,1}, T_{1,1}),}$ $\mathrm{(S_{i,2}, T_{1,2}), \cdots, (S_{i,n}, T_{1,n}))}$ requesting grouping proof verification. The verification process is shown in fig. 4.

Verifier V calculates $X_{G,i} = T_1 - vT_0$ and $S_j = yS_{i,j} - T_{1,j}$, search registration database $(X_{i,j}, X_{G,i})$, fetch all of tag group $X_{G,i}$'s tags $X_{i,j}$, and calculates

$$p_i = \dot{r}(yX_{i,1}) \oplus \dot{r}(yX_{i,2}) \oplus \cdots \oplus \dot{r}(yX_{i,n}) \qquad (1)$$

and

$$p'_i = \dot{r}(yS_1) \oplus \dot{r}(yS_2) \oplus \cdots \oplus \dot{r}(yS_n)\,. \qquad (2)$$

If $p_i = p'_i$, return prompt of success. Otherwise, return prompt of failure.

Provable security and security comparison. *Correctness.* Theorem 1. The grouping proof approach in this paper is correct.

Proof. Let us assume that grouping proofs are calculated in the above-mentioned processes. Then the grouping proof generation and verification process is as follows:

(1) Calculate the group of a tag

$$\begin{aligned}
&c^{-1}(wK_k - k_k T_{0,j} - cT_{2,j})) = \\
&= c^{-1}((r_{0,j} + c(r_{1,j} + x_{i,j} + x_{G,j}))K_k - \\
&\quad - k_k r_{0,j} P - c(r_{1,j} + x_{i,j})K_k) = \\
&= c^{-1}(r_{0,j}K_k + cr_{i,j}K_k + cx_{i,j}K_k + cx_{G,j}K_k - \\
&\quad - k_k r_{0,j} P - cr_{i,j}K_k - cx_{i,j}K_k) = \\
&= c^{-1}ck_k X_{G,j} = \\
&= k_k X_{G,j}.
\end{aligned} \tag{3}$$

The reader collects all members of tag group $X_{G,j}$ and generates their grouping proof.

(2) Verification

$$\begin{aligned}
S_{i,j} &= k_k^{-1} T_{2,j} = \\
&= k_k^{-1}(r_{1,j} + x_{i,j})K_k = \\
&= r_{1,j}P + x_{i,j}P;
\end{aligned} \tag{4}$$

$$\begin{aligned}
\mathrm{S_j} &= yS_{i,j} - T_{1,j} = \\
&= y(r_{1,j}P + x_{i,j}P) - r_{1,j}Y = \\
&= yX_{i,j}.
\end{aligned} \tag{5}$$

Calculate

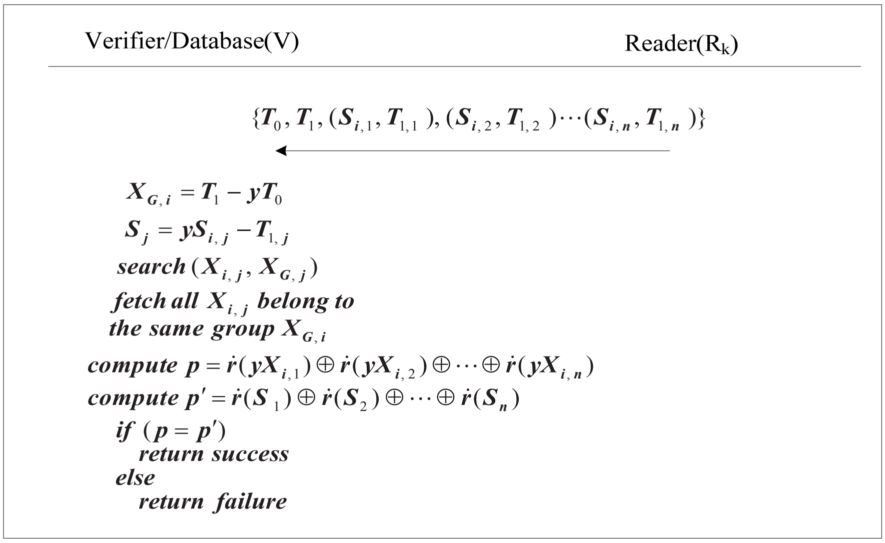
$$p_i = \dot{r}(yX_{i,1}) \oplus \dot{r}(yX_{i,2}) \oplus \cdots \oplus \dot{r}(yX_{i,n}) \tag{6}$$

and

$$p_i' = \dot{r}(S_1) \oplus \dot{r}(S_2) \oplus \cdots \oplus \dot{r}(S_n)\,. \tag{7}$$

If $p = p'$, return prompt of success. Otherwise, return prompt of failure.

According to the CDH (Computational Diffie Hellman) assumption, $k_k X_{i,j} = x_{i,j}K_i$ and $yX_{i,j} = x_{i,j}Y$. To calculate their values, k_k, y and $x_{i,j}$ must be specified. These three values are, however, respectively stored in the reader, the verifier, and the tag. It is impossible for the attacker to influence all of them. Therefore, the protocol is correct.


Verifier/Database(V)
Reader(R_k)
$\{T_0, T_1, (S_{i,1}, T_{1,1}), (S_{i,2}, T_{1,2}) \cdots (S_{i,n}, T_{1,n})\}$

```
$X_{G,i} = T_1 - yT_0$
$S_j = yS_{i,j} - T_{1,j}$
search $(X_{i,j}, X_{G,j})$
fetch all $X_{i,j}$ belong to
the same group $X_{G,i}$
compute $p = \dot{r}(yX_{i,1}) \oplus \dot{r}(yX_{i,2}) \oplus \cdots \oplus \dot{r}(yX_{i,n})$
compute $p' = \dot{r}(S_1) \oplus \dot{r}(S_2) \oplus \cdots \oplus \dot{r}(S_n)$
if $(p = p')$
    return success
else
    return failure
```

Fig. 4. The grouping proof verification phase

Security. We consider the security requirements of RFID grouping proof protocols in the Internet of Things, i.e. strong privacy preservation, untraceability, reader anonymity, tag anonymity, and authorization. The following sections analyze the security of the protocol proposed in this paper from the five perspectives.

The approach proposed in this paper is modified based on the Schnorr scheme [10]. Thus, relevant adversaries in this approach can be changed to those of the Schnorr scheme. Literature [10] proves that under the OMDL (One More Discrete Logarithm) assumption, the Schnorr scheme is secure under active impersonation attack.

1. Strong privacy preservation. Strong privacy preservation implies that information of individual tags and privacy information of tag groups cannot be leaked in the process of grouping proof.

For a tag, the main privacy information transmitted in verification consists of group key and identification key $(x_{G,i}, x_{i,j})$. In the transmission process, group key and identification key are blinded via $T_{2,j} = (r_{1,j} + x_{i,j})K_k$ and $w = r_{0,j} + c_j(r_{1,j} + x_{i,j} + x_{G,j})$.

Also, $r_{0,j}, r_{1,j}$ updates every time it finishes verification. Therefore, it is impossible for an attacker to get any privacy information of a tag via secret keys.

For a tag group, an attacker cannot get privacy information of it if he fails to get its group key and identification key. In grouping proof information $(\mathrm{T_0}, \mathrm{T_1}, (\mathrm{S_{i,1}}, \mathrm{T_{1,1}}), (\mathrm{S_{i,2}}, \mathrm{T_{1,2}}), \cdots, (\mathrm{S_{i,n}}, \mathrm{T_{1,n}}))$, both $S_{i,j} = k_k^{-1}T_{2,j}$ and $\mathrm{T_{2,j}} = (\mathrm{r_{1,j}} + \mathrm{x_{i,j}})\mathrm{K_k}$ include random numbers. Therefore, the attacker cannot get identifications of readers and tags, nor identify which parts of the information represent identifications of readers and tags in the entire interaction process.

2. Untraceability. Untraceability implies that an attacker cannot trace tags or tag groups via captured grouping proof information.

In the same tag group, it can be found that each tag's response information is random. So it is with whether the same member is included. This means that an attacker cannot associate two verification processes of a tag via the random information. Thus, tags are untraceable.

It is possible that an attacker can capture multiple grouping proofs. However, parameters $r,\ c_j, r_{0,\,j}, r_{1,\,j}$ used in each generation process of group proofs are random numbers independently generated by readers and tags. The attacker cannot identify whether the generators of two random grouping proofs are identical. For grouping proofs, there are no common laws for the attacker to trace tags. Thus, tag groups are untraceable.

3. Reader anonymity. Reader anonymity implies that any attacker cannot get the identity information of a reader. In interaction, a tag sends $T_{2,\,j} = (r_{1,\,j} + x_{i,\,j})K_k$ to a reader. An attacker cannot get identity information relevant to the reader via $T_{2,\,j}$. Thus, he cannot get the identification of the reader.

4. Tag anonymity. Tag anonymity implies that any attacker cannot get the identification of tag $T_{i,\,j}$. In interaction, select random numbers $r_{0,\,j}$ and $r_{1,\,j}$ and calculate $T_{0,\,j} = r_{0,\,j}P$, $T_{1,\,j} = r_{1,\,j}Y$, $T_{2,\,j} = (r_{1,\,j} + x_{i,\,j})K_k$ and $\mathrm{w} = \mathrm{r}_{0,\,\mathrm{j}} + \mathrm{c}_{\mathrm{j}}(\mathrm{r}_{1,\,\mathrm{j}} + {} + \mathrm{x}_{\mathrm{i},\,\mathrm{j}} + \mathrm{x}_{\mathrm{G},\,\mathrm{j}})$.

Since $r_{0,\,j}$ and $r_{1,\,j}$ update in each verification process, an attacker cannot get tag identification via tag response information.

5. Authorization. Authorization is composed of two aspects: Only authorized readers can successfully realize tag group proof; only tag group members can participate in and successfully complete group proof. When it executes the grouping proof protocol with an impersonation of a reader, an attacker can receive tag response information but cannot know the private key k_k of the authorized reader. Therefore, the grouping proof protocol cannot be generated because $k_k X_{G,\,i}\,?{=}\,c_j^{-1}(wK_k - k_k T_{0,\,j} - c_j T_{2,\,j})$ cannot be verified. Thus, the protocol can resist impersonation attack on readers.

An attacker may try to let tags outside a group participate and complete grouping proof via impersonation or replay at-tack. Since various random numbers are introduced in protocol interaction process, each session of a tag is independent. A replay attack is, thus, impossible. An attacker will not know the group key and identification private key of the current valid tag, nor will he/she get the authorization private key v. Therefore, the verifier V cannot calculate $X_{G,\,i} = T_1 - vT_0$ and $S_j = yS_{i,\,j} - T_{1,\,j}$, nor verify whether and $p_i' = \dot{r}(yS_1) \oplus \dot{r}(yS_2) \oplus \cdots \oplus \dot{r}(yS_n)$ are equal. Then grouping proof fails. The protocol is, thus, capable of resisting the impersonation attack.

Above all, only valid tags can pass tag group authentication. Similarly, only valid readers can generate grouping proofs.

Comparison in Security. The grouping approach based on ECC mostly adopts the idea of tag mutual signature and is a sequential processing process. Grouping proof efficiency inevitably reduced if there are too many tag group members. Table 2 illustrates the comparison between the protocol proposed in this paper and other schemes based on ECC.

Table 2

Comparisons of ECC-Based Grouping-Proof Protocol

	Batina [6]	Lv [7]	Ko [8]	Lin [9]	Proposed
Untraceability	×	√	×	×	√
Resist impersonation attack	×	×	×	×	√
Authorization	×	×	×	×	√
Scalability	√	√	√	√	√

Conclusions. With the continuous expansion of RFID application, the demand for tag grouping proof protocols is also growing. Security and efficiency flaws have been identified in existing grouping proof protocols through our analysis. On this basis, this paper proposes a highly reliable RFID group tag verification protocol, which can simultaneously verify multiple tags in an effective and secure manner within a short time. Comparatively speaking, link grouping proof protocol based on ECC has far lower generation efficiency than broadcasting grouping proof protocol. This paper has elaborated on this protocol, analyzed its security features, and compared it with existing grouping proof protocols based on ECC in detail. As revealed by the findings, the protocol designed in this paper is able to meet the security requirements of grouping proofs and is highly reliable with guaranteed accuracy and security.

Acknowledgements. This work was supported by scientific research project of Heze University (No. XY12KJ09) and the science and technology project of the Shandong province universities (No. J14LN21).

References / Список літератури

1. Juels, A. (2004), "Yoking-Proofs" for RFID Tags", *Proc. of the 2nd IEEE Annual Conference on Pervasive Computing and Communications Workshops*, pp. 138–143.

2. Selwyn Piramuthu (2006), "On Existence Proofs for Multiple RFID Tags", *IEEE International Conference on Perva-*

sive Services, Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing, pp. 317–320.

3. Mike Burmester, Breno de Medeiros and Rossana Motta (2008), "Provably Secure Grouping-Proofs for RFID Tags", *Lecture Notes in Computer Science*, vol. 5189, pp. 176–190.

4. Chien, H.Y., Yang, C.C., Wu, T.C. and Lee, C.F. (2011), "Two RFID-based solutions to enhance inpatient medication safety", *Journal of Medical Systems*, vol. 35, no. 3, pp. 369–375.

5. Peris-Lopez, P., Orfila, A., Hernandez-Castro, J.C. and Lubbe, J.C.A.V.D. (2011), "Flaws on RFID grouping-proofs Guidelines for Future Sound Protocols", *Journal of Network and Computer Applications*, vol. 34, no. 3, pp. 833–845.

6. Batina, L., Lee, Y., Seys, S., Singele, D. and Verbauwhede, I. (2011), "Privacy-preserving ECC-based grouping proofs for RFID", *Lecture Notes in Computer Science*, vol. 6531, pp. 159–165.

7. Lv, C., Li, H., Ma, J., Niu, B. and Jiang, H. (2011), "Security analysis of a privacy-preserving ECC-based grouping-proof protocol", *Journal of Convergence Information Technology*, vol. 6, no. 3, pp. 113–119.

8. Ko, W., Chiou, S., Lu, E., Chang, H. (2011), "An improvement of privacy-preserving ECC-based grouping proof for RFID", *Cross Strait Quad-Regional Radio Science and Wireless Technology Conference*, pp. 1062–1064.

9. Lin, Q., and Zhang, F. (2012), "ECC-based grouping-proof RFID for inpatient medication safety", *Journal of Medical Systems*, vol. 36, no. 6, pp. 3527–3531.

10. Bellare, M. and Palacio, A. (2002), "GQ and Schnorr Identification Schemes: Proofs of Security against Impersonation under Active and Concurrent Attacks", *Lecture Notes in Computer Science*, vol.2442, pp. 162–177.

Мета. Із широким вживанням систем радіочастотної ідентифікації стало актуальним завдання розробки ефективних і безпечних протоколів радіообміну. У результаті аналізу існуючих протоколів обміну систем радіочастотної ідентифікації для вирішення завдань забезпечення конфіденційності, безпеки та ефективності, запропонований новий протокол на основі еліптичної криптографії.

Методика. Деякі протоколи на основі еліптичної криптографії не можуть протистояти атаці шляхом підміни учасника та іншим поширеним видам атак, оскільки в них відсутня аутентифікація зчитуючого та перевірочного пристроїв, або ж зчитувач і верифікатор можуть бути невідомого походження, крім того зловмисник може сформувати набір атак, активно запрошуючи мітки, аби обдурити справжній зчитувач і верифікатор.

Результат. У статті зроблена спроба детального викладу етапів ініціалізації, авторизації, генерування підтвердження та його верифікації для нового протоколу обміну, а також аналізу протоколу на конфіденційність, непростежуваність, забезпечення анонімності зчитуючого пристрою та міток, авторизації, аутентифікації й тому подібне.

Наукова новизна. Порівняно з існуючими протоколами обміну на основі еліптичної криптографії, запропонований протокол дозволяє здійснювати авторизований доступ і взаємну аутентифікацію міток, зчитувачів і внутрішніх серверів.

Практична значимість. Аналіз результатів показав, що новий проект протоколу відповідає вимогам безпеки та конфіденційності, що пред'являються до протоколів обміну систем радіочастотної ідентифікації, демонструючи при цьому велику універсальність і ефективність порівняно з аналогічними протоколами.

Ключові слова: *протокол обміну, авторизація, аутентифікація, взаємна аутентифікація, еліптична криптографія, радіочастотна ідентифікація*

Цель. С широким применением систем радиочастотной идентификации перед учеными стала актуальной задача разработки эффективных и безопасных протоколов радиообмена. В результате анализа существующих протоколов обмена систем радиочастотной идентификации, для решения задач обеспечения конфиденциальности, безопасности и эффективности, предложен новый протокол на основе эллиптической криптографии.

Методика. Некоторые протоколы на основе эллиптической криптографии не могут противостоять атаке путём подмены участника и другим распространенным видам атак, поскольку в них отсутствует аутентификация считывающего и проверочного устройств или же считыватель и верификатор могут быть неизвестного происхождения, кроме того злоумышленник может сформировать набор атак, активно запрашивая метки, чтобы обмануть подлинный считыватель и верификатор.

Результат. В статье предпринята попытка подробного изложения этапов инициализации, авторизации, генерирования подтверждения и его верификации для нового протокола обмена, а также анализа протокола на конфиденциальность, непрослеживаемость, обеспечения анонимности считывающего устройства и меток, авторизации, аутентификации и т.п.

Научная новизна. В сравнении с существующими протоколами обмена на основе эллиптической криптографии, предложенный протокол позволяет осуществлять авторизованный доступ и взаимную аутентификацию меток, считывателей и внутренних серверов.

Практическая значимость. Анализ результатов показал, что новый проект протокола отвечает требованиям безопасности и конфиденциальности, предъявляемым к протоколам обмена систем радиочастотной идентификации, демонстрируя при этом большую универсальность и эффективность в сравнении с аналогичными протоколами.

Ключевые слова: *протокол обмена, авторизация, аутентификация, взаимная аутентификация, эллиптическая криптография, радиочастотная идентификация*

Рекомендовано до публікації докт. техн. наук В.І. Корнієнком. Дата надходження рукопису 15.09.14.