ARTICLE IN PRESS

Ad Hoc Networks xxx (2013) xxx–xxx

Contents lists available at SciVerse ScienceDirect

Ad Hoc Networks

journal homepage: www.elsevier.com/locate/adhoc

A secure ECC-based RFID authentication scheme integrated with ID-verifier transfer protocol

Yi-Pin Liao *, Chih-Ming Hsiao

Department of Computer Science and Information Engineering, St. John's University, Taipei, Taiwan, ROC

ARTICLE INFO

Article history:
Received 7 June 2012
Received in revised form 31 December 2012
Accepted 22 February 2013
Available online xxxx

Keywords:
Internet-of-Things (IoT)
RFID
Public-key cryptographic (PKC)
Elliptic curve cryptosystem (ECC)
ID-verifier

ABSTRACT

IoT (Internet of Things) is a type of network where ICT (Information and Communication Technology) links any physical objects to the internet to perform information exchange. Owing to the congenital advantages RFID is expected to play a key role as enabling identification technology in IoT. At the same time, its integration with sensing technologies brings wide applicability in many productive sectors. On the other hand, security appears to be one of the most challenging areas about designing the RFID system. The problems of authentication and privacy are fundamental to RFID security. It is well known that elliptic curve cryptosystem (ECC) based algorithms would be best choice among PKC algorithms due to their small key sizes and efficient computations. In this paper, we proposed a secure ECC-based RFID authentication scheme integrated with ID-verifier transfer protocol. The proposed scheme can achieve mutual authentication and satisfy the essential requirements of RFID system. Performance evolution and function comparison demonstrate that the proposed scheme is well suited for RFID tags with the scarceness of resources.

1. Introduction

While more and more people regard Internet as global information and communication infrastructure, another big leap forward is coming related to the use of the Internet as a global platform for letting smart objects communicate, dialogue, compute and coordinate. The IOT (Internet-of-Things) is emerging scope promoting the development of technologies in the Information and Communication Technologies (ICT) sector at large. With ICT, IOT was complemented, and to some degree replaced, by communication between humans and machines (e.g., through word processing), by communication between humans enabled by machines (e.g., telephones or e-mail), and by machines communicating with each other (e.g., in B2B e-business). The IOT provides wide applicability in many productive sectors including, e.g., environmental monitoring, healthcare, inventory and product management, workplace and home support, security and surveillance. Hence, developing technologies and solutions for enabling such a vision is the main challenge ahead of us. From a system-level perspective, the IOT can be looked at as a highly dynamic and radically distributed networked system, composed of a very large number of smart objects producing and consuming information. Then, the conventional concept of the Internet as an infrastructure network reaching out to end-users' terminals will extend and leave space to a notion of interconnected smart objects forming pervasive computing environments [1]. In a general way, traditional IOT is formed by three layers shown in Fig. 1. The bottom is perception layer, whose function is cognizing and collecting information of objects. The middle is transportation layer. It consists of mobile phone networks, fixed telephone networks, broadcasting networks, and closed IP data networks for each carrier. The top is application layer, where abundant applications run. Typical applications includes smart traffic, precise agriculture, intelligent logistics, smart industry, environment protection, mining monitor, remote nursing, safety defense, smart govern-

* Corresponding author.
E-mail address: newsun87@mail.sju.edu.tw (Y.-P. Liao).

1570-8705/$ - see front matter © 2013 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.adhoc.2013.02.004

Please cite this article in press as: Y.-P. Liao, C.-M. Hsiao, A secure ECC-based RFID authentication scheme integrated with ID-verifier transfer protocol, Ad Hoc Netw. (2013), http://dx.doi.org/10.1016/j.adhoc.2013.02.004

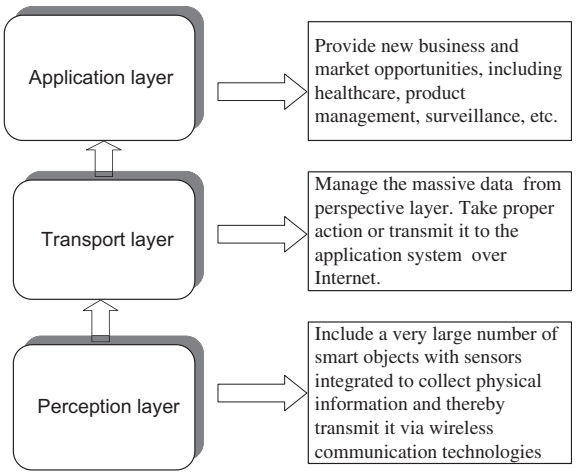

Fig. 1. The concept of IOT structure.

ment, etc. In the following, we make an attempt to describe the features and the research challenges that need to be addressed in every layer.

(1) *Perception layer*: A key issue for IoT is the development of appropriate means for identifying smart objects and enabling interactions with the environment. In this sense, key building blocks are expected to be represented by WSN (wireless sensor networking) technologies [2] and RFID [3–5]. In the last years, several aspects have been investigated in the IOT applications. Low-power communications is a well-established research field within the sensor networking community. This is of paramount importance for IoT scenarios, as battery replacement is a costly process to be avoided as much as possible, especially for large-scale deployments. More recently, advances in the field of nano-scale accumulators as well as energy harvesting techniques appear of prominent interest to limit the need for battery replacements [6,7]. Furthermore, the notion of distributing computation in order to reduce the communication overhead, which is generally termed in-network processing or in-network computing [8], is typically applied to wireless sensor networks that perform local measurements, as it would be the case of field measurements in IoT scenarios.

(2) *Transport layer*: With the appearance of a large sensor networks, various data streams coming from heterogeneous smart objects using wireless communication, including Bluetooth, RF, ZigBee, RFID, WiFi, etc. Transport layer is responsible to the transmission of the massive data from smart objects to their corresponding application systems over interconnected heterogeneous networks such IP-based networks, broadcasting networks, mobile/wireless networks. The result is a side effect of IOT type of scenarios. This means a potentially very large amount of information injected into the Internet. The control of information injected by "objects" and related data filtering techniques is a concern for pervasive scenarios [9]. Distributed flow control, in turn, is a well-studied traditional topic in networking and controls due to the large amount of work on TCP [10]. With millions of new devices connected to the Internet, 3G or LTE technology will not be able to cope, and the combined use of mobile phones, wireless connections and optic fiber will be vitally important in resolving oversaturation of mobile infrastructures. A number of measures have therefore been considered to help resolve the issue.

(3) *Application layer*: The increase in the usage of distributed sensor network systems, paving the way to making IOT a reality, is not simply a result of technological push; it is also driven by the market pull, since enterprises are increasingly realizing the commercial benefits of applications that can be realized with IOT technologies. Furthermore, the ensemble of applications and services leverage such technologies to open new business and market opportunities [11,12]. In terms of application fields and market sectors where IoT solutions can provide competitive advantages over current solutions, we do believe that some kinds of applications can play a leading role in the adoption of IoT technologies, including environmental monitoring; smart cities; smart business/inventory and product management; smart homes/smart building management; health-care and security and surveillance. Clearly, the scope of IoT is extremely wide. However, applications that are built on top of IoT may consistently improve the competitiveness of the solutions at hand. IoT adoption is therefore expected to be strongly driven by the market needs and by the market dynamics.

Security appears to be one of the most challenging areas about designing the Internet of Things (IoT). This is no excuse for smart objects to have less security than any other device on the Internet. On the other hand, smart objects forming the IoT can be extremely constrained (low processing and battery power, low memory, lack of user interface). Without guarantees in terms of system-level confidentiality, authenticity and privacy, the relevant enterprises and commences are unlikely to adopt IoT solutions on a large scale. IoT devices can be assumed very critical roles, such as monitoring as part of a home security system, or controlling as part of an intelligent transportation system. Compromise of such devices can be more catastrophic than that a typical device on the Internet (e.g., a PC, or a mobile phone). Security design begins with the selection of credential types. These are the credentials that will be used by the IoT devices for getting authorized for network access followed by application access. Certificates, id/password pairs, and SIMs are the possible choices being considered in the industry. Each one of these credential types as its own pros and cons. Id/password pairs are relatively light-weight, yet managing them in high quantities is not practical. Certificates provide a robust and established solution for large-scale device deployments, but their added cost and dependency on CA vendors are

Please cite this article in press as: Y.-P. Liao, C.-M. Hsiao, A secure ECC-based RFID authentication scheme integrated with ID-verifier transfer protocol, Ad Hoc Netw. (2013), http://dx.doi.org/10.1016/j.adhoc.2013.02.004

concerning to the service providers. SIMs are attractive but applicable to only a subset of deployments.

Currently, the applications of RFID system are much wider than that of wireless sensors. Wireless sensor networks have not yet reached the mainstream in the same way. Radio frequency identification devices and solutions can nowadays be considered a main communication technology, with a number of massive deployments. Especially since the adoption of EPC global Gen-2 [13] verified by EPC Global while phasing out Gen 1 in 2006. In this paper, we will adopt ECC primitives [14] to design an efficient RFID mutual authentication scheme. Compared with the related works based on ECC, the proposed authentication scheme has remarkable features as follows. (1) It integrates both secure ID-verifier transfer and challenge-response protocols to achieve mutual authentication; (2) It solves the security risks neglected by previous ECC-based works; (3) It is be proven to satisfy all of the requirements considered in RFID system through security analysis. (4) Our work can be applied well to other authentication applications which are similar to RFID environment. The remainder of this paper is organized as follows. In Section 2, we state the advantage to adopt RFID technology in wide applications. In Section 3, we describe the research background related to RFID authentication schemes. In Section 4, we discuss all possible vulnerabilities and essential requirements in RFID system. In Section 5, we review the recent PKC based authentication schemes. Next, we propose a secure ECC-based authentication scheme for RFID system in Section 6. Then, we make security analysis in Section 7, and then performance and functionality comparisons are shown in Section 8. Finally, the conclusion is given in Section 9.

2. RFID advantages

RFID is increasingly becoming more popular and is expected to replace the current barcode technology in the near future. RFID (radio frequency identification) is a means of storing and retrieving data through electromagnetic transmission using a radio frequency (RF)-compatible integrated circuit. In the following, we describe the advantages of using RFID in industrial interests.

2.1. Easy deployment with low cost

RFID Identification and proximity detection schemes that make use of inexpensive RFIDs became recently a promising choice for commercial deployments in the related fields. To achieve significant consumer market penetration, RFID tags can be priced in the US$0.05–US$0.10 range and contains only 500–5K gates. In a typical RFID application, tags are attached or embedded in objects that must be identified or tracked. By reading nearby tag IDs and then consulting a background database that provides mapping between IDs and objects, the reader can monitor the existence of the corresponding objects. In fact, the RFID technologies can be used to monitor in real-time product availability and maintain accurate stock inventory in retail applications. They can also play a role in after-market support, whereby users can automatically retrieve all data about the products they bought. Also, identification technologies can help in limiting thefts and in fighting counterfeiting by providing products with a unique identifier including a complete and trust-worthy description of the good itself.

2.2. Flexible integration with sensors

The RFID tags with sensors (sensor tags) use the same RFID protocols and mechanisms for reading tag IDs, as well as for collecting sensed data. Sensor tags are used in several applications including temperature sensing and monitoring, photo detection, and movement detection [15–17]. Hence, sensor tags can be properly used depending on the phenomena that are sensed.

The classification of sensor tags is based on the way sensor tags are powered up. Passive tags do not use batteries for communication and sensing, and as such, they are basically maintenance-free. These are of paramount importance for IoT scenarios, as battery replacement is a costly process to be avoided as much as possible, especially for large-scale deployments. However, the requirements of very low power sensors lead a lower quality of sensing. Semi-passive tags use power-generating circuits to generate power for RF components on the chip and battery power for powering up the rest of the chip. In comparison with passive sensor tags that can perform measurements only when interrogated by the readers, semi-passive sensor tags can perform independent measurements when they are not in the proximity of readers. This requires a greater amount of memory for storing measured values. Active sensor tags rely completely on batteries. Sensor tags in this class have more memory and improved range and functionality in comparison with semi-passive sensor tags. Active tags with integrated sensors are used in several applications including temperature sensing and monitoring vibration detection. Some tags have external buses that allow for attaching external sensors.

2.3. Combination with WSN node

As mentioned above, sensor tags have limited communication capabilities. The combination of RFID and WSN nodes brings alongside a number of challenges and issues [18,19]. We consider WSN nodes that act as tags in that they have a unique ID number that can be used in identifying objects or people. In addition, this kind of node can have multiple sensors and additional communication capabilities in comparison with RFID tags. In high-end applications, it is possible to integrate RFID tags with WSN nodes and wireless devices, such that the integrated tags can communicate with many wireless devices, not just the reader. Integrated tags and WSNs mainly rely on existing wireless standards such as Zigbee and WLAN. Another type of integration of RFID includes advanced WSN nodes with RFID capabilities. A wireless smart sensor platform studied in [20] uses wireless technologies such as Wi-Fi, Bluetooth, and RFID for communications in a point-to-point topology. The platform uses external sensors that are equipped with a smart sensor interface (SSI). The

Please cite this article in press as: Y.-P. Liao, C.-M. Hsiao, A secure ECC-based RFID authentication scheme integrated with ID-verifier transfer protocol, Ad Hoc Netw. (2013), http://dx.doi.org/10.1016/j.adhoc.2013.02.004

interface extracts data from sensors and provides a data communication interface to the central control unit.

3. Research context for security issue

Another key set of research challenges in IOT is security issues. Security represents a critical component for enabling the widespread adoption of IoT technologies and applications. The problems of authentication and privacy are fundamental to RFID security. Authenticity can be achieved by a secure protocol running between RFID tag and reader. If a unique secret information is stored on the tag and the tag can convince the reader to possess that information, the tagged product is declared to be authentic, respectively the person gains access and otherwise not. The required cryptographic primitives range from symmetric and asymmetric algorithms to hash functions and random number generators. We simply classify the RFID authentication schemes published in the literatures [13,21–38] into non-public key cryptosystem (NPKC) based schemes and public key cryptosystem (PKC) based schemes. In NPKC based schemes, we further divided it into four classes depending on the computational cost and the operations needed to tags. The first class called lightweight protocols refers to those schemes [13,21–24] that require a random number generator and simple functions like Cyclic Redundancy Code (CRC) checksum but not hash function, where Gen 2 is standard [13]. The second class called ultralightweight refers to those schemes [25–30] that involves only simple bit-wise operations (like XOR, AND, OR, etc.) on tags, where Peris-Lopez et al.'s schemes [27,28] are first proposed. The third class called simple is for those schemes [31–36] that should support random number generator cooperated with one-way hash functions on tags, where the hash lock protocol proposed by Weis et al. [31] is known as the prototype. The last class refers to those schemes that demand the support of conventional cryptographic functions like symmetric encryption, cryptographic one-way function but not public key algorithms. One of the main applications of this class is E-passport [37], which needs the operations of triple-DES and Message authentication code (MAC).

The suitability of PKC for RFID is an open research problem due to the limitation in tag cost, gate area and power consumption. Moreover, it was previously proven that PKC algorithms are necessary to solve the requirements of RFID system [38]. That is, it is not possible to satisfy the essential requirements only with symmetric cryptographic algorithms such as hash algorithms and symmetric key encryption algorithms. To achieve significant consumer market penetration, a few papers [39,40] try to discuss the feasibility of PKC primitive cheap implementations on RFID tags; for example, Gaubatz et al. [39] implements Rabin's encryption with cost about 17K gates, and Kaya et al. [40] design NTRU public encryption which costs only about 3K gates.

Among PKC algorithms, elliptic curve cryptosystem (ECC) based algorithms would be the best choice for RFID systems due to their small key sizes and efficient computations [41]. For example, a key size of 160 bits in ECC has a compatible security level with a key size of 1024 bits in RSA or DLP (Discrete Logarithm Problem) based cryptography. This makes ECC very attractive for small-footprint devices with limited computational capability, memory and low-bandwidth network connections. However, ECC is still considered to be impracticable for very low-end constrained devices like sensor networks and RFID tags. Very recently, Lee et al. [42] presents the proposed RFID processor is composed of a microcontroller, an EC processor (ECP), and a bus manager, where the ECP is over GF(2^{128}). For an efficient computation with restrictions on the gate area and the number of cycles, several techniques are introduced in the algorithms and the architecture level. As a result, the overall architecture takes 12.5K gates. Lee et al.'s scheme shows the plausibility of meeting both security and efficiency requirements even in a passive RFID tag. That is, an ECC based solution would be one of the best candidates for the RFID system.

4. Vulnerabilities and essential requirements in RFID system

From system-lever perspective, IOT consist of three layer mentioned above. Standards for network security such as TLS [43], IPSec [44] and SSH [45] typically can provide peer entity authentication between transport layer and application layer. We just aim at the perspective layer to discuss the major security challenges of RFID. Owing to the radio transmission nature of RFID, the information traveling in the air could easily be intercepted and eavesdropped. As RFID has been prevailing, the issues of security and privacy have raised many concerns. Hence, designing a practical RFID system is one of the most challenging tasks since it requires compact and power-efficient solutions, especially when security-related processing is needed.

In this section, we point out the inherent vulnerabilities and security issues for RFID system. To prompt the widespread applications in various fields, the design of authentication scheme satisfied the essential requirements of the RFID system need to be considered.

4.1. System architecture

In this subsection, we describe the system architecture of a RFID system. An RFID system consists of three entities: tags, RFID readers and the back-end server. Usually, RFID authentication is done between a back-end server and tags. An RFID reader relays messages between tags and a back-end server and does not need to concern credentials used in authentication methods and policy decision. The following are our advanced description for the elements of RFID authentication framework.

- *Tag.* The tag consists of an antenna connected to a microchip that can store and read data and possibly has some dedicated hardware to perform a small amount of computations. It mainly contains the identity-index information itself, and transmits this information in response to requests from the reader. It is identified as passive, semi-passive, and active according

Please cite this article in press as: Y.-P. Liao, C.-M. Hsiao, A secure ECC-based RFID authentication scheme integrated with ID-verifier transfer protocol, Ad Hoc Netw. (2013), http://dx.doi.org/10.1016/j.adhoc.2013.02.004

to whether it has its own battery. Passive tags are powered by the signal of an interrogating reader and can only work within short ranges (a few meters). Active tags maintain their internal state and power transmission using a battery. Semi-passive tags are battery assisted tags that use some battery power to maintain their internal volatile memory but may still rely on the reader's signal to power their transmission. They can initiate communication and operate over longer ranges (several meters), but are also more expensive and bulkier than passive tags. Passive tags, however, are also more popular and cheaper. In particular, passive tags are used more often in supply chain management.

- *Reader*. A RFID reader acts as "pass-through agents" without authentication method layer functionalities so that they are compatible with multiple authentication methods. It is often linked with back-end server that can perform computations on the data that it receives from tags. It consists of an RF transmitter and receiver, a control unit, and a memory unit. These instruments work together to exchange information over radio waves between it and an antenna attached to an RFID tag.
- *Back-end server*. A back-end server is a trusted party that maintains all identification information related to tags as database. It authenticates RFID readers beforehand and establishes a secure channel with each reader via pre-shared key or current well-known security mechanism such as SSL/TLS. With the accessed information from the tag as an index, the back-end server can retrieve the real identity from the corresponding record stored in the database.

4.2. Attack model and security issues

Next, we summarize the capabilities of an attacker. The following are a definition of an attack model used by an attacker to profile from RFID system.

4.2.1. Attack model

AM1: Eavesdropping. As communication between the tag and the reader is based on radio frequency, anyone can eavesdrop. The insecure communication allows an attacker to easily eavesdrop on the contents of the exchanged messages. The adversary can acquire the user's secret information via eavesdropping, or initiate another attack by using the eavesdropped message.

AM2: Traffic analysis. Traffic analysis is a method to analyze the messages eavesdropped during communication between the reader and tag. By analyzing the tag information, the attacker can acquire the information needed to connect the tag and identity of the tag owner. An attacker performs brute-force attacks using traffic analysis tools.

AM3: Physical attack. The tag has a fatal defect that makes it vulnerable to physical attack. This includes stealing and damaging tags that are in use to obtain the secret information residing in it. After acquiring its information, the attacker can counterfeit another tag or launch malicious attacks.

4.2.2. All considered issues for RFID system

With the foregoing capabilities, the attacker can raise the security issues using the attack model. In the subsection, all possible concerns will be discussed in the following.

4.2.2.1. Forgery problem. A forgery problem arises when an attacker impersonating a reader or tag is verified as a legitimate object and exploits this by performing the following attacks:

- *Replay attack*. An attacker can intercept transmitted information and resend it illegally in an attempt to deceive a legal device and pass the authentication. For example, unauthorized readers can listen and record the communication between an authorized reader and a RFID tag, and then replay the communication to essentially achieve the same outcome that a legitimate reader and tag would have achieved.
- *Tag masquerade attack*. An attacker could impersonate a target tag to a server without knowing the tag's internal secrets. It could communicate with a server and be authenticated as the tag.
- *Server spoofing attack*. An attacker might be able to impersonate a legitimate server to a compromised tag using knowledge of the tag's internal state.

4.2.2.2. Denial-of-Service (DoS) problem. In general, DoS causes loss of service to users. To provide privacy protection, most RFID authentication schemes update tag's secret information after a successful protocol run. This update is performed in the back-end database as well as in the tag. So synchronization of secret information between the database and the tag is crucial for subsequent authentications. The de-synchronization attack is a malicious action by an attacker which intentionally causes the database and a tag out of synchronization [46]. It leads to the failure in the interaction between the tag and the reader will fail. Moreover, an attacker can conduct this kind of attack by jamming the readers with hidden blocker tags [47].

4.2.2.3. Privacy problem.

- *Location tracking attack*. By using a malicious reader, the attacker can acquire the target tag information and find which tag it belongs to. To perform this kind attack, the attacker transmits the query continuously to the tag being traced. If the responses from the target tag are fixed or predictable, it results in a location privacy problem. For example, if the response of a tag to a server query is a static ID code, then the movements of the tag can be monitored, and the social interactions of an individual carrying a tag may be available to third parties without his/her knowledge. Even though the responses are not fixed, an attacker can possibly performs brute-force attacks using traffic analysis tools to acquire the information needed to identify the tag owner.

Please cite this article in press as: Y.-P. Liao, C.-M. Hsiao, A secure ECC-based RFID authentication scheme integrated with ID-verifier transfer protocol, Ad Hoc Netw. (2013), http://dx.doi.org/10.1016/j.adhoc.2013.02.004

- *Forward secrecy problem*. An attacker might be able to trace future transactions between a server and a compromised tag using knowledge of the tag's internal state, i.e. physical attack. That is, knowledge of a tag's internal state at time t can help to identify tag interactions that occur at time ($t_0 > t$). Hence, undetected compromises remain an ongoing concern.

4.2.2.4. Tag cloning attack. Since a large number of tags will be spread out in the RFID applications, an attacker may be able to capture a tag and make a counterfeit by way of probing the information residing in the tag. If a group of tags share common secret information and a reader authenticates tags by the shared secret, it will be possible to clone some other tags with the learned secret.

4.2.2.5. Scalability problem. If the computational workload of an authentication protocol increases linearly as the growing number of the tags, the system is not scalable. For example, when the server receives tag's response message to be authenticated, the database of the server must run the computations on all its records to find the matching record. The problem indicates that the back-end server always requires a linear search to identity a tag. In other words, the server must take $O(n)$ times to authenticate a tag, where n is the number of tags in the system, and therefore demands more searching cost when n is getting larger. Consider a huge database containing numerous records, and this record-by-record computations will overload the database and inevitably pull down the operational performance.

4.3. Security and operational requirements to be considered

To enhance the security strength of RFID system to be suitable for various applications, we define the system requirements that need to be considered when designing an authentication protocol to solve the foregoing security issues. The system requirements are defined in terms of mutual authentication, confidentiality, anonymity, availability, forward security and scalability.

- *Mutual authentication*. It is essential that authentication should occur between the objects of the RFID system. In cases when communication between only the tag and reader is insecure, the authentication process is performed between the tag and the database of the back-end server.
- *Confidentiality*. Confidentiality requires that all of the secret information is securely transmitted during all communications. Therefore, to ensure confidentiality, the tag transmit the encrypt information so that only the server can recognize it.
- *Anonymity*. Anonymity is the most important security requirement for privacy [13]. Anonymity is the property that adversary cannot trace tag by using interactions with tag. If the transmitted tag information cannot satisfy anonymity, an attacker with the same reader can continuously trace the owner of a specific tag or detect the real-time location of the tag owner by using readers dispersed over several locations.
- *Availability*. Authentication process should be run all the time between the server and the tag. To provide privacy protection, after a successful protocol run, most RFID authentication schemes update the secret information between the back-end database and the tag. Hence, the de-synchronization attack causing the secret information to refresh out of phase must be prevented.
- *Forward security*. It is essential that the previously transmitted information cannot be traced using the present transmission tag information. If the past location of the specific tag owner can be traced using the compromised information, it constitutes a serious privacy.
- *Scalability*. Scalability is a desirable property in almost any system, enabling it to handle growing amounts of work in a graceful manner. In RFID system, the server must find the matching record from the database to identify the tag, and a scalable RFID protocol should therefore avoid any requirement for work proportional to the number of tags. Hence, the computational workload must be sustained by the server with the growth for the amount of the tags.

4.4. System model

In the following, we describe the formal definition of the authentication protocol for RFID system. An RFID authentication scheme is made of the following algorithms:

- An algorithm SetupServer $(\cdot)$ is implemented by the back-end server to generate the common input (typically: system domain parameters, the public key P_s), the secret key x_s and initializes a database.
- An algorithm SetupTag (ID) is implemented by the back-end server to generate an ID-verifier Z_T, the private key x_T and its initial state S using the common input. When the tag is meant to be a legitimate one, the entry contained $\langle Z_T, x_T \rangle$ is inserted in the database.
- A two-party protocol between the back-end server and a tag in which the back-end server uses the common input, the database and the secret produces an output equal to $\perp$ if identification failed or some ID if it succeeded, and may update the database. To address mutual authentication, we enrich this definition by introducing an output on the tag side which should be OK or $\perp$.

5. Recent research work based PKC protocols

For recent PKC based authentication protocols of RFID systems, we further classify them into two kinds: (a) non-ECC (NECC) based schemes, and (b) ECC based schemes. We discuss the related works as follows.

5.1. NECC based scheme and their security flaws

Chen et al. [48] proposed a private mutual authentication scheme based on quadratic residues referred to Rabin cryptosystem. In Chen et al.'s scheme, the tag uses Rabin's encryption to produce dynamic pseudonym and the server

Please cite this article in press as: Y.-P. Liao, C.-M. Hsiao, A secure ECC-based RFID authentication scheme integrated with ID-verifier transfer protocol, Ad Hoc Netw. (2013), http://dx.doi.org/10.1016/j.adhoc.2013.02.004

performs only one decryption to obtain the real identify of tags without requiring linear search. However, Cao and Shen [49] found Chen et al.'s scheme suffers from forgery attack. Next, Yeh et al. [50] further pointed that Chen et al.'s scheme suffers the location privacy problem and replay attack. They further proposed an improvement scheme while preserving Chen et al.'s merits. However, the improvement requires three Rabin's encryptions and four hash operations on the tag side for each authentication. This computational overhead seems impractical for a power limited low cost tag.

5.2. ECC based schemes and their security analysis

Some features are especially attractive for security applications where computational power and integrated circuit space is limited, such as smart cards, PC cards, and wireless devices. Such is the case with elliptic curve groups, which were first proposed for cryptographic use independently by Neal Koblitz and Victor Miller in 1985 [41]. Some typical RFID authentication protocols utilize elliptic curve cryptography are: Schnorr protocol [51], Okamoto protocol [52], EC-RAC (ECC Based Randomized Access Control) protocol [53] and ECDLP-RK [54] protocol (ECDLP based Randomized Key). For introducing RFID schemes based on ECC, we first briefly describe the concepts of ECC and related logarithms in this subsection.

5.2.1. Primitives

The lowest level of the authentication scheme is cryptographic primitives. Primitives are algorithms that rely on mathematical hard problems. The intractability of these problems are typically exploited to provide the security of a cryptographic protocol. Next, the related theorem based on ECC is stated below.

5.2.1.1. Domain parameters of ECC.

- $F(q)$: the finite field over q, where q is a prime and represents the size of finite field.
- (a,b): the parameters of E elliptic curves $y^2 = x^3 + ax + b$ over $F(q)$.
- $P(x_p,y_p)$: a prime ordered generator point which is an element of the curve but $P \neq 0$.
- n: the order of the base point P.
- h: cofactor, $h = \#F(q)/n$.

5.2.1.2. Operations of ECC. The point addition is defined a way of adding two points, P1 and P2, that satisfy the elliptic curve equation, to produce a third point, P3, also on the curve. The point scalar multiplication is defined as $Q = k \cdots P = P + \cdots + P$ (k times).

5.2.1.3. Elliptic curve discrete logarithm problem (ECDLP). Let elliptic curve group be defined as above, which has generator P and order n. Given $(X, Y) \in E(F_q)$, to find the integer $c \in Z_n$, such that $Y = c \cdot X$ is called ECDLP and is considered as hard using a polynomial time algorithm.

5.2.2. Tuyls et al.'s scheme using Schnorr protocol

Tuyls and Batina [55] proposed an ECC-variant of the authentication protocol published by C. Schnorr. They claimed their scheme can resist against tag counterfeiting, but Lee et al. [53] pointed their protocol suffers some weakness. Next, the introduction and security analysis are as follows:

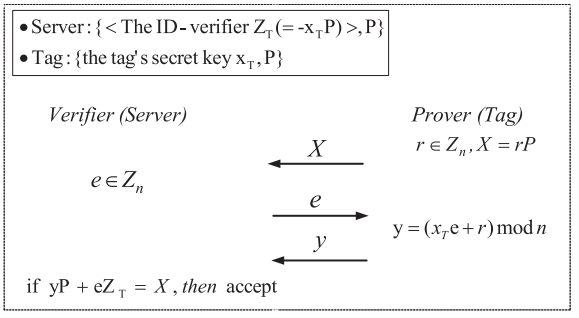

Fig. 2. Tuyls et al.'s scheme using Schnorr protocol.

(1) *Scheme description*: In Tuyls et al.'s scheme shown in Fig. 2, each tag keeps a secret key x_T and its public key $Z_T(=x_T P)$. For identity each tag, the server maintains the ID-verifier of each tag, i.e. public key Z_T, as the system database. Whenever receiving the response message from a legal tag, the server searches the proper ID-verifier Z_T stored in database to check whether $(yP + eZ_T) = X$ holds. The term $(yP + eZ_T)$ can deduces as follows:

$$(yP + eZ_T) = (x_T e + r)P - e x_T P) = rP = X \quad (1)$$

(2) *Security analysis*: The attacker can eavesdrops and collects the exchange message $\{X, e, y\}$ aiming at a target tag. Hence, he/she also can compute $(X - yP)e^{-1}$ and checks the result is equal to Z_T. The result indicates that the attacker can use Z_T to track the target tag. In other words, Tuyls et al.'s scheme is vulnerable to location tracking attack. Moreover, the attacker obtains the exchange message $\{X, e, y\}$ and public key Z_T of the specific tag. Hence, he can identify the unknown tag as the specific tag using an active attack as follows. In another conversation, when the unknown tag transfers X' to the reader, the attacker can impersonate the reader to query the unknown tag by sending a challenge $e'(=e + 1)$. If the tag responds y', then the attacker obtains the value $e'Z'_T$ by computing $(X' - y'P)$ and therefore can check whether the computed value $(e'Z'_T - eZ_T)$ is equal to Z_T. Hence, the attacker can then use Z_T to distinguish the tag from the past conversations easily. In other word, their protocol does not achieve forward secrecy. Especially, their protocol only considers tag-to-reader authentication, excluding reader-to-tag authentication. This makes tags easy to suffer malicious queries, because they are not capable of confirming whom they are talking to. In other hand, a scalability problem also exists in it. This is, because the server should fetch each tag's public key Z_T from its database to compute $(yP + eZ_T)$ for comparing with the received X^*. This means that the server requires linear search to identity each tag

and thus increases considerable computational cost. Hence, their protocol lacks scalability.

5.2.3. Batina et al.'s scheme using Okamoto Protocol

Batina et al. [56] proposed an ECC-variant of the authentication protocol published by Okamoto to avoid active attacks. Later, Lee et al. in 2008 [53] pointed out that Batina et al.'s scheme is unsafe for applications. Next, the introduction and security analysis are as follows:

(1) *Scheme description*: The Batina et al.'s scheme is shown in Fig. 3, where each tag keeps (x_{T1}, x_{T2}) as the secret keys and its public key $Z_T(=-x_{T1}P_1 - x_{T2}P_2)$ as ID-verifier. For identity each tag, the server maintains the ID-verifier of each tag as the system database. After finishing the message exchanges, the server accepts the tag if $y_1P_1 + y_2P_2 + eZ_T = X$, otherwise reject. The term $y_1P_1 + y_2P_2 + eZ_T$ can deduces as follows:

$$\begin{aligned}(y_1P_1 + y_2P_2 + eZ_T) &= (r_1 + ex_{T1})P_1 + (r_2 + ex_{T2})P_2 \\ &\quad + e(-x_{T1}P_1 - x_{T2}P_2) \\ &= r_1P_1 + r_2P_2 = X \end{aligned} \quad (2)$$

(2) *Security analysis*. The attacker can eavesdrops and obtains the exchange message $\{X, e, y_1, y_2\}$ aiming at a target tag. Hence, he/she can compute $(X - y_1P_1 - y_2P_2)e^{-1}$ and deduce as follow:

$$\begin{aligned}(X - y_1P_1 - y_2P_2)e^{-1} &= (r_1P_1 + r_2P_2 - (r_1 + ex_{T1})P_1 \\ &\quad - (r_2 + ex_{T2})P_2)e^{-1} - x_{T1}P_1 \\ &\quad - x_{T2}P_2 = Z_T \end{aligned} \quad (3)$$

The result indicates that the attacker can use Z_T to track the target tag. Similarly, a scalability problem and forward secrecy also exists in Batina et al.'s scheme. In view of simplification, this part of the security analysis is omitted.

5.2.4. Lee et al.'s scheme using ECDLP Based Randomized Access Control (EC-RAC) protocol

To solve all the requirements for RFID systems, Lee et al. [53] designed a new RFID protocol based on ECDLP. However, the works in [57,58] showed Lee et al.'s vulnerability against tracking attacks and forgery attacks. Next, the introduction and security analysis are as follows.

- *Scheme description*: The protocol flow is shown in Fig. 4. In this scheme, it is assumed that a server keeps the server's secret key x_S and inserts the entry $\langle Z_1(=x_{T1}P), x_{T1}, X_2(=x_{T2}P)\rangle$ of each tag to system database, and a tag stores $\{x_{T1}, x_{T2}, P_S(=x_SP)\}$, where (x_{T1}, x_{T2}) are similar to conventional password protocols which require two values for each tag, i.e. ID and Password. The public keys $x_{T1}P$ and $x_{T2}P$, are used as ID-verifier and Password-verifier which are securely stored in the server unlike general public keys. After decrypting $Z_{T1}(=x_{T1}P)$ by computing $(x_S^{-1}Y_2 - Y_1)$, the server searches for x_{T1} and $Z_{T2}(=x_{T2}P)$ partied with Z_{T1} and verifies that Z_{T2} is corrected by checking whether $(vP - x_{T1}Y_1)r_2^{-1} = Z_{T2}$.
- *Security analysis*: The failure of the security proof is caused by neglecting the possibility that an attacker can use multiple sets of authentic communication history [51]. An attacker can generate a random number c in place of r_2, and use it twice to response two different sets of message from a tag. A tag will generate two random numbers r_1 and r_2 for each of the authentication protocol. Hence, the exchanged messages in this protocol is $\{Y_1^{(1)}, Y_2^{(1)}, v^{(1)}\}$ and $\{Y_1^{(2)}, Y_2^{(2)}, v^{(2)}\}$) respectively, where

$$\left\{Y_1^{(1)}, Y_2^{(1)},\ v^{(1)}\right\} = \{r_1P,\ (r_1 + x_{T1})Y,\ r_1x_{T1} + cx_{T2}\}$$

$$\left\{Y_1^{(2)}, Y_2^{(2)}, v^{(2)}\right\} = \{r_2P,\ (r_2 + x_{T1})Y,\ r_2x_{T1} + cx_{T2}\}$$

Then, an attacker can perform the following calculation.

$$\begin{aligned}&\cdot(v^{(1)} - v^{(2)})^{-1} \cdot \left(Y_2^{(1)} - Y_2^{(2)}\right) \\ &= \{(r_1 - r_2)x_{T1})\}^{-1} \cdot (r_1 - r_2)P_S \cdot = x_{T1}^{-1}Y \end{aligned} \quad (4)$$

Since the result $x_{T1}^{-1}Y$ can be a fixed value for a specific tag, a tag can be traced by an attacker. Besides, Bringer et al. [58] show how tags can be tracked if the attacker has intercepted the same tag twice and that a tag can be impersonated if it has been passively eavesdropped three times. Similarly, their protocol only considers tag-to-reader authentication, excluding reader-to-tag authentication. This makes tags easy to suffer malicious queries.

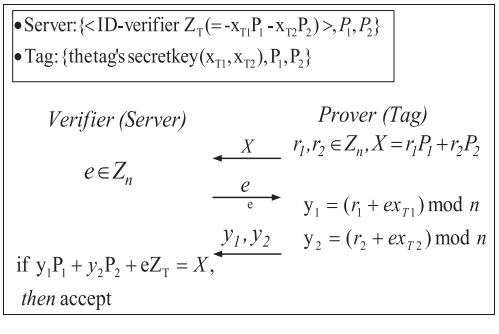

Fig. 3. Batina et al.'s scheme using Okamoto protocol.

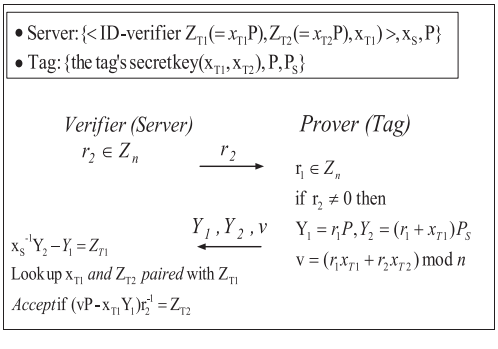

Fig. 4. Lee et al.'s scheme based on EC-RAC.

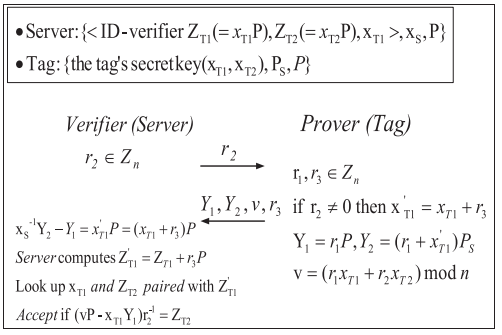

Fig. 5. The improvement of EC-RAC protocol by Zhang et al.'s scheme.

5.2.5. Zhang et al.'s scheme using ECDLP based randomized key (ECDLP-RK) protocol

To improve Lee et al.'s scheme using EC-RAC protocol and Tuyls et al.'s scheme using Schnorr protocol respectively, Zhang et al. [54] present an ECDLP-RK proposal shown in Fig. 5. Next, the introduction and security analysis are as follows:

- *Scheme description*: The different with the EC-RAC protocol as Fig. 5 is that tag generates a random r_3, calculate $x'_{T1} = x_{T1} + r_3$, exchange x_{T1} to x'_{T1}. While the server authenticates tag, database updates the all record $Z_{T1}(=x_{T1}P)$ to $Z'_{T1}(=x_{T1}P + r_3P)$, then looks to match. As for the improvement of Schnorr protocol, just like above mention improvement, tag generates a random r_3 when authenticate with reader. Then exchange the private key s to $x'_T = x_T + r_3$.
- *Security analysis*: Based on the ECDLP, even if attackers know about r_3 and x'_TP, they still cannot get any information about x_T. Furthermore, as the random r_3, the attacker also cannot track $Z'_T(= x'_TP)$. But as authentication add to update database, so this action increase in consumption with background server. In this case, Zhang et al.'s scheme causes the scalability problem. Furthermore, Zhang et al.'s scheme is also lack for mutual authentication.

6. The proposed scheme

This paper proposes an ECC-based mutual authentication schemes that satisfies the essential requirements in RFID system. To assure the security of the ID-verifier transmitted from the tag over radio communication, a secure ID-verifier transfer protocol need to be design. Moreover, a challenge-response protocol is involved to refresh the communication messages. The proposed scheme is secure against various types of attacks and completely solves the existing research problems. Our scheme consists of two phases: the setup phase and the authentication phase. In the proposed scheme, communication between the reader and back-end server is secure, while communication between each tag and reader is insecure. Fig. 6 shows the typical system of RFID applied to the proposed scheme.

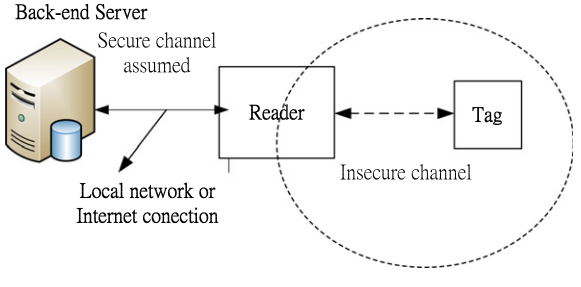

Fig. 6. The RFID system of the proposed scheme.

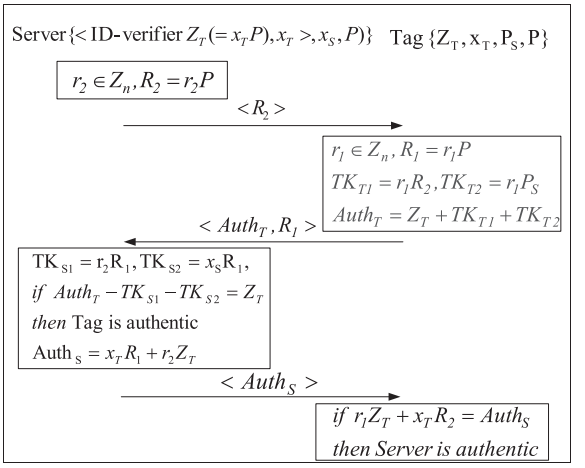

Fig. 7. The proposed scheme based on ECC.

6.1. Setup phase

In the setup phase, both the server and the tag are acquainted with the elliptic curve domain parameters $\{q, a, b, P, n, h\}$. The server keeps a random number $x_S \in Z_n$ as its private key and sets $P_S(=x_SP)$ as its public key. It also chooses $x_T \in Z_n$ as the private key of each tag and sets $Z_T(=x_TP)$ as the tag's ID-verifier or public key. Hence, the server inserts the entry $\{Z_T, x_T\}$ of each tag into its database. Moreover, each tag stores $\{Z_T, x_T\}$, the server public key P_S and domain parameters D into the memory.

6.2. Authentication phase

The authentication phase is depicted in Fig. 7. The interactions between the tag and the server are described as follows:

Step 1: The server generates a random number $r_2 \in Z_n$ and computes $R_2 = r_2P$. Then it sends R_2 along with query message to the tag.
Step 2: After receiving the query message $\langle Query, R_2 \rangle$, the tag chooses a random number $r_1 \in Z_n$ and computes $R_1 = r_1P$. And then the tag computes two temporary secret keys $TK_{T1} = r_1R_2$ and $TK_{T2} = r_1P_S$. Next, the tag encrypts the ID-verifier Z_T by computing $Auth_T = Z_T + TK_{T1} + TK_{T2}$, and sends $\langle Auth_T, R_1 \rangle$ to respond to the server.

Please cite this article in press as: Y.-P. Liao, C.-M. Hsiao, A secure ECC-based RFID authentication scheme integrated with ID-verifier transfer protocol, Ad Hoc Netw. (2013), http://dx.doi.org/10.1016/j.adhoc.2013.02.004

Step 3: After receiving $\langle Auth_T, R_1\rangle$, the reader recovers two temporary secret keys by way of computing $TK_{S1} = r_2R_1$ and $TK_{S2} = x_SR_1$. Next, the server utilizes them to retrieve the ID-verifier Z_T of the tag using the following equation:

$$\begin{aligned} Auth_T - TK_{S1} - TK_{S2} &= (Z_T + TK_{T1} + TK_{T2}) - TK_{S1} - TK_{S2} \\ &= (Z_T + r_1R_2 + r_1P_S) - r_2R_1 - x_SR_1 \\ &= (Z_T + r_1r_2P + r_1x_SP) - r_2r_1P - x_Sr_1P \\ &= Z_T \end{aligned} \quad (5)$$

Then, the reader searches tag's ID-verifier in the database. If it is found, the reader confirms the tag to be legitimate and obtains the corresponding private key x_T. Next, Then, the server calculates $Auth_S = x_TR_1 + r_2Z_T$ and sends back $\langle Auth_S\rangle$ to be authenticated by the tag.

Step 4: Next, the tag computes $r_1Z_T + x_TR_2$ and checks if the value is equal to the received $Auth_S$. If it is equal, the tag conforms that the server is authentic.

7. Security analysis

In this section, we will analyze the security of the proposed scheme to verify whether the essential requirements have been satisfied. For correctness analysis, an efficient and convincing formal methodology is needed to evaluate the proposed scheme. Before that, we make some reasonable assumptions to sustain the security analysis:

A1: The tag believes r_1 is fresh in every session.
A2: The reader believes r_2 is fresh in every session.
A3: x_S is unknown for anyone except the reader.
A4: Z_T and x_T are unknown for anyone except the tag and the server.
A5: The common parameters such as P_S may be known by way of physical attack on a corrupted tag.

7.1. System requirements analysis

In the following, we give an in-depth analysis of the proposed scheme in terms of system requirements. Before that, we draw some inferences to prove our authentication protocol as follows:

I1: The tag believes that the ID-verifier Z_T is securely transmitted to the server. As step 2 of the authentication phase, the tag sends response message $\langle Auth_T, R_1\rangle$ to the server. The message $Auth_T(=Z_T + TK_{T1} + TK_{T2})$ can be interpreted as an encryption of Z_T with the temporary secret keys (TK_{T1}, TK_{T2}). Moreover, only the server can use the secret temporary keys (TK_{S1}, TK_{S2}) matching (TK_{T1}, TK_{T2}) to decrypt Z_T by computing $(Auth_T - TK_{S1} - TK_{S2})$. Based on ECDLP, the attacker cannot deduce (TK_{T1}, TK_{T2}) and (TK_{S1}, TK_{S2}) from the collected messages. That is, the attacker cannot decrypt Z_T from $Auth_T$. Hence, Z_T is embedded in $Auth_T$ and securely transmitted to the server.
I2: The server believes that the ID-verifier Z_T is securely transmitted to the tag. As step 3 of the authentication phase, the server sends $\langle Auth_S\rangle$ to the tag. The message $Auth_S(=x_TR_1 + r_2Z_T)$ can be interpreted as an encryption of r_2Z_T with the temporary secret key of x_TR_1. In other hand, the message $Auth_S(=r_1Z_T + x_TR_2)$ can be regarded as an encryption of r_1Z_T with the temporary secret key of x_TR_2. Since neither (r_2, x_T) nor (r_1, x_T) is known by the attacker based on ECDLP, the ID-verifier Z_T cannot be extracted from $Auth_S$.

By I1 and I2, a secure ID-verifier transfer protocol can be achieved.

I3: The freshness of exchange messages $\langle Auth_S, Auth_T\rangle$ is assured in every session. By I1 and I2, the messages $Auth_T$ and $Auth_S$ are controlled using two random numbers (r_1, r_2). According to A1 and A2, two random numbers (r_1, r_2) is unpredictable and different in every session. That is, the attacker cannot reuse the previous messages to cheat the tag or the server.

7.1.1. SR1: Mutual authentication between the tag and the server

Proof. In general, the main goal of the authentication protocol shows that the communication entities can achieve mutual authentication. The server believes the tag is authentic by checking the correctness of the received $Auth_T$. As step 3 of the authentication phase, the server receives message $\langle Auth_T, R_1\rangle$. Based on ECDHP, the server can decrypt Z_T by way of calculating $(Auth_T - TK_{S1} - TK_{S2})$. If the result matches the entry listed in database, the identity of the tag is authenticated by the server. In other hand, the tag believes the server is authentic by checking the correctness of the received $Auth_S$. As step 4 of the authentication phase, the tag receives message $Auth_S(=x_TR_1 + r_2Z_T)$. The term $Auth_S$ can be deduced as follows: □

$$Auth_S = x_TR_1 + r_2Z_T = x_Tr_1P + r_2x_TP = r_1Z_T + x_TR_2 \quad (6)$$

After receiving $Auth_S$, only the tag with $\{Z_T, x_T\}$ can compute $r_1Z_T + x_TR_2$ using (r_1, R_2). If the computed result matches the received $Auth_S$, the tag believes the corresponding party owns the secret information $\{Z_T, x_T\}$. According to A4, the identity of the server is authenticated by the tag. Hence, we prove that the server and the tag authenticate each other. Moreover, the protocol can satisfy the system requirements discussed below.

7.1.2. SR2: ID-verifier confidentiality

Proof. During authentication process, the ID-verifier Z_T of the tag should be protected well over unsecure channel. According to I1 and I2, the attacker cannot extract Z_T from the collected messages $\langle Auth_T, Auth_S\rangle$. Hence, the proposed protocol can achieve ID-verifier confidentiality. □

7.1.3. SR3: Anonymity

Proof. RFID tags can respond with some messages whenever they receive a query message from a reader. Hence, anonymity is the most important security requirement for privacy. The attacker also cannot extract the ID-verifier Z_T

Please cite this article in press as: Y.-P. Liao, C.-M. Hsiao, A secure ECC-based RFID authentication scheme integrated with ID-verifier transfer protocol, Ad Hoc Netw. (2013), http://dx.doi.org/10.1016/j.adhoc.2013.02.004

by monitoring the exchanged messages according to SR2. Moreover, the exchange messages $\langle Auth_T, Auth_S \rangle$ are unpredicted variations in every session due to the freshness of two random numbers (r_1, r_2). The property is that an attacker cannot trace the location of the target by collecting the exchanged messages. Even though an attacker sends a malicious query to a targeted tag with a designed number r_2^* and EC point $R_2^* = r_2^* P$, the attacker cannot extract the ID-verifier from $Auth_T$ without knowing $TK_{T2}(= r_1 P_S = x_S R_1)$. Hence, the attacker cannot analyze the exchanged messages to trace the owner of a specific tag. □

7.1.4. SR4: Availability

Proof. According to SR2, the ID-verifier Z_T can be protected well during the authentication process. Hence, the proposed authentication scheme does not synchronously update the secret information to provide privacy protection between the tag and the back-end server. In other words, authentication protocol can be run all the time between the reader and the tags. □

7.1.5. SR5: Forward security

Proof. It is essential that the previously transmitted information cannot be traced using the present transmission tag information. We assume an attacker knows the secret keys of a tag, i.e. Z_T and x_T. However, an attacker still does not know random numbers temporarily generated and used inside of a tag and the server. Hence, the proposed scheme still provides on unpredictable variations in the past communication messages. □

7.1.6. SR6: Scalability

Proof. In back-end server, the entry $\langle Z_T, x_T \rangle$ matching each tag are listed as Fig. 7. According to step 3 in the authentication phase, the server extracts the ID-verifier Z_T from the received $Auth_T$, and then search the matched entry in database. This means the server does not requires linear search to identity each tag and thus save considerable computation cost while the number of the tags increases. □

7.2. Attacks analysis

7.2.1. AKR1: Replay attack resisting

Proof. Having intercepted previous communication, the attacker can replay the same message of the receiver or the sender to pass the verification of the system. Hence, the attacker may masquerade as the reader or the tag to launch replay attack by reusing previous $Auth_S$ or $Auth_T$. By I3, the action will fail because the freshness of the messages transmitted in the authentication phase is controlled by two random numbers, i.e. (r_1, r_2). □

7.2.2. AKR2: Tag masquerade attack resisting

Proof. The attacker may intercept and modify the previous message of the legal tag to pass the authentication of the server. If the attacker may construct a valid authentication message $\langle Auth_T, R_1 \rangle$ to pass the server's examination, he/she need to extract the ID-verifier Z_T from the previous $Auth_T$. By SR2, the ID-verifier Z_T is securely embedded in transmitted message over unsecure channel. Hence, the attacker cannot construct a valid authentication message without knowing the ID-verifier Z_T. That is, the tag masquerade attack will fail. □

7.2.3. AKR3: Server spoofing attack resisting

Proof. Server spoofing attack means the attacker may masquerade as the server to gain the benefits. The attacker constructs a valid message $Auth_S$, where the ID-verifier Z_T is also embedded. By SR2, the attacker cannot succeed without knowing the ID-verifier Z_T. □

7.2.4. AKR4: DoS attack resisting

Proof. According to SR4, the proposed authentication scheme does not synchronously update the secret information to provide privacy protection between the back-end databases. Hence, our scheme can eliminate the risk against DoS attack. □

7.2.5. AKR5: Location tracking attack resisting

Proof. According to SR2, the data transmitted between the server and the tag is well protected so that the tag's ID-verifier Z_T could not be retrieved from the message flow. Moreover, the message flow is provided on unpredictable variations in every session. Hence, the location tracking fail will fail. □

7.2.6. AKR6: Cloning attack resisting

Proof. If a group of tags share the same secret key and use it for the authentication, it is vulnerable to cloning attacks. In the proposed scheme, each tag owns its unique secret key x_T and ID-verifier Z_T. If one of group tags is captured, the attacker cannot use the known secrets $\{x_T, Z_T\}$ to derive the secrets of some other tag. That is, the attacker cannot use the revealed secret to clone some other tags. □

8. Performance and the comparison of system requirements

It is well-known that most of RFID tags have limited resources. Hence, it is very important issue for performance analysis in the real applications. In general, performance analysis has been evaluated based on different criteria such as storage requirements, computational cost, and

Please cite this article in press as: Y.-P. Liao, C.-M. Hsiao, A secure ECC-based RFID authentication scheme integrated with ID-verifier transfer protocol, Ad Hoc Netw. (2013), http://dx.doi.org/10.1016/j.adhoc.2013.02.004

Table 1
Performance evolution among ECC-based authentication schemes.

	Ours	Tuyls et al. [55]	Batina et al. [56]	Lee et al. [53]	Zhang et al. [54][c]
Memory (bit)					
Private key	163	163	326	326	326
Public key	489	163	326	326	326
Total (byte)	82	41	82	82	82
Computation					
ECm[a]	5	1	2	3	3
Time (s)[b]	0.32	0.064	0.128	0.192	0.192
Communication (byte)	82	61	82	82	82

[a] The number of ECC point scalar multiplication.
[b] The rough computational time of the operation on 5 MHz Tags.
[c] The improvement aiming at Lee et al.'s scheme based on EC-RAC protocol.

Table 2
Comparisons of system requirements among the existing ECC-based schemes.

	Ours	Tuyls et al. [55]	Batina et al. [56]	Lee et al. [53]	Zhang et al. [54]
Mutual authentication	Yes	No	No	No	No
Confidentiality	Yes	No	No	Yes	Yes
Anonymity	Yes	No	No	No	Yes
Availability	Yes	Yes	Yes	Yes	Yes
Forward secrecy	Yes	No	No	Yes	Yes
Scalability	Yes	No	No	Yes	No

communication overhead. We focus the performance analysis in tag since the server is regarded as a powerful device. In this section, we present the results of ECC based authentication schemes mentioned above. As a common cryptographic primitive, we have used a standardized 163-bit NIST elliptic curve defined over the finite field $F(2^{163})$, where a scalar multiplication with a 163 bit scalar can be done in 64 ms using a 5 MHz tag [59]. For achieving this operation, we applied the Montgomery-algorithm [60] using standard-projective coordinates. The input of the Montgomery-algorithm is not the complete point, but only its affine x coordinate. This way, the y coordinate of the curve points is practically unneeded during the runtime of the protocol, which lowers the size of the messages. The performance metric of the described authentication protocols is given in Table 1. The memory requirement of the protocols has been characterized by considering the storage in tags including the private key and the public key. The private key is defined as the secret key of the tag. The public key includes the tag's public key, server's public key and base point of elliptic curve. The computational cost has been evaluated with the numbers of point scalar multiplications in the finite field. As for the evaluation of the protocol communication overhead includes the number of communication messages in the authentication phase. In the proposed schemed, the memory requirement includes $\{x_T, Z_T, P_S, P\}$, where the private key x_T needs 163 bits and the public keys $\{Z_T, P_S, P\}$ need 489 bits (163 bits for the x-coordinate of one public key). Next, the computational cost includes five point scalar multiplications needed 0.32 ms (i.e. 64 ms $\times$ 5). Finally, the communication overhead includes messages $\{R_1, R_2, Auth_S, Auth_T\}$ needed 82 bytes (i.e. $163 \times 4/8 \fallingdotseq 82$) between the reader and the tag. Moreover, we summarize the comparisons of system requirements among the existing ECC-based schemes in Table 2. Although other ECC-based schemes [51–54] are more efficient than the proposed scheme in tag's computation time, the proposed scheme achieves higher level security requirement results including mutual authentication agreement and all mentioned attacks protection.

9. Conclusion

We present an ECC-based authentication scheme for RFID combined with secure ID-verifier transfer protocol. Previously proposed schemes based on ECC cannot satisfy all of the requirements of RFID systems, including mutual authentication, confidentiality, anonymity, forward security and scalability. The proposed scheme can be proven to satisfy the essential requirements through security analysis based on efficient and convincing formal methodology. Moreover, we made a performance analysis using the evolution based on storage requirements, computational cost and communication overhead. We also expect that the results of this work is not limited to RFID systems but can be applied to other authentication applications which are similar to RFID environment.

References

[1] M. Weiser, The computer for the 21st century, Sci. Am. (1991) 94–100.
[2] I. Akyilidiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, Wireless sensor network: a survey, Comput. Netw. 38 (4) (2002) 393–422.
[3] G. Roussos, V. Kostakos, RFID in pervasive computing: state-of-the-art and outlook, Pervasive Mob. Comput. 5 (2009) 110–131. http://dx.doi.org/10.1016/j.pmcj.2008.11.004.
[4] F. Michahelles, F. Thiesse, A. Schmidt, J.R. Williams, Pervasive RFID and near field communication technology, IEEE Pervasive Comput. 6 (3) (2007) 94–96.
[5] M. Murphy, J. Butler, Proactive Computing: RFID & Sensor Networks, Final Report on the Conference Organized by DG Information Society and Media, Networks and Communication Technologies Directorate,

March 2006. <ftp://ftp.cordis.europa.eu/pub/ist/docs/ka4/au_conf670306_murphy_en.pdf>.
[6] G. Merrett, N. White, N. Harris, B. Al-Hashimi, Energy-aware simulation for wireless sensor networks, in: Proc. IEEE SECON, Rome, Italy, 2009, pp. 64–71.
[7] A. Kansal, J. Hsu, S. Zahedi, M.B. Srivastava, Power management in energy harvesting sensor networks, ACM Trans. Embed. Comput. Syst. 6 (4) (2007) 32.
[8] A. Giridhar, P.R. Kumar, Computing and communicating functions over sensor networks, IEEE JSAC 23 (4) (2005) 755–764.
[9] I. Carreras, I. Chlamtac, F. De Pellegrini, D. Miorandi, BIONETS: bio-inspired networking for pervasive communication environments, IEEE Trans. Veh. Technol. 56 (1) (2007) 218–229.
[10] J. Padhye, V. Firoiu, D. Towsley, J. Kurose, Modeling TCP throughput: a simple model and its empirical validation, in: Proc. ACM SIGCOMM, Vancouver, CA, 1998, pp. 303–314.
[11] L. Atzori, A. Iera, G. Morabito, The Internet of things: a survey, Comput. Netw. 54 (15) (2010) 2787–2805.
[12] The Internet of Things, ITU Internet Reports, 2005. <http://www.itu.int/internetofthings/>.
[13] EPCglobal. Specification for RFID Air Interface. <http://www.epcglobalinc.org>.
[14] Daniele Miorandi, Sabrina Sicari, Francesco De Pellegrini, Imrich Chlamtac, Internet of things: vision, applications and research challenges, Ad Hoc Network, 10, 2012, 1497–1516.
[15] N. Cho et al., A 5.1-uW UHF RFID Tag Chip Integrated with Sensors for Wireless Environmental Monitoring, European Solid-State Circuits Conf. (ESSCIRC), Grenoble, France, September 2005.
[16] H. Kitayoshi, K. Sawaya, Long range passive RFID-tag for sensor networks, in: Proc. 62nd IEEE Vehic. Tech. Conf., 2005.
[17] M. Philipose et al., Battery-free wireless identification and sensing, IEEE Pervasive Comput. 4 (1) (2005) 37–45.
[18] H. Liu, M. Bolic, A. Nayak, I. Stojmenovic, Taxonomy and challenges of the integration of RFID and wireless sensor networks, IEEE Netw. 22 (2008) 26–35.
[19] L. Zhang, Z. Wang, Integration of RFID into wireless sensor networks: architectures, opportunities and challenging problems, in: Proc. GCCW, 2006, pp. 463–469.
[20] H. Ramamurthy et al., Wireless industrial monitoring and control using a smart sensor platform, IEEE Sensor 7 (5) (2007) 611–618.
[21] H.Y. Chien, C.H. Chen, Mutual authentication protocol for RFID conforming to EPC class 1 generation 2 standards, Comput. Stand. Interfaces 29 (2) (2007) 254–259.
[22] D.N. Duc, J. Park, H. Lee, K. Kim, Enhancing security of EPCglobal Gen-2 RFID tag against traceability and cloning, in: Proc. 2006 Symp. Cryptography and Information, Security, 2006.
[23] A. Juels, Strengthening EPC tag against cloning, in: Proc. ACM Workshop Wireless Security (WiSe '05), 2005, pp. 67–76.
[24] T. Yeh, Y. Wanga, T. Kuo, S. Wang, Securing RFID systems conforming to EPC Class 1 Generation 2 standard, Exp. Syst. Appl. 37 (2010) 7678–7683.
[25] H.Y. Chien, C.W. Huang, Security of ultra-lightweight RFID authentication protocols and its improvements, ACM Oper. Syst. Rev. 41 (2) (2007) 83–86.
[26] T. Li, G. Wang, Security analysis of two ultra-lightweight RFID authentication protocols, in: Proceeding of 22nd IFIP TC-11 Int'l Information Security Conf., May 2007.
[27] P. Peris-Lopez, J.C. Hernandez-Castro, J.M. Estevez-Tapiador, A. Ribagorda, LMAP: A real lightweight mutual authentication protocol for low-cost RFID tags, in: Proc. Second Workshop RFID Security, July 2006.
[28] P. Peris-Lopez, J.C. Hernandez-Castro, J.M. Estevez-Tapiador, A. Ribagorda, EMAP: An efficient mutual authentication protocol for low-cost RFID tags, in: Proc. OTM Federated Conf. and Workshop: IS Workshop, November 2006.
[29] P. Peris-Lopez, J.C. Hernandez-Castro, J.M. Estevez-Tapiador, A. Ribagorda, M2AP: A minimalist mutual-authentication protocol for low-cost RFID tags, in: Proc. Int'l Conf. Ubiquitous Intelligence and, Computing (UIC'06), 2006, pp. 912–923.
[30] H.Y. Chien, SASI: A new ultralightweight RFID authentication protocol providing strong authentication and strong integrity, IEEE Trans. Dependable Secure Comput. 4 (4) (2007) 337–340.
[31] S.A. Weis, S.E. Sarma, R.L. Rivest, D.W. Engels, Security and privacy aspects of low-cost radio frequency identification systems, in: Proc. International Conference on Security in Pervasive Computing, 2003, pp. 454–469.
[32] H.Y. Chien, Secure access control schemes for RFID systems with anonymity, in: Proc. 2006 Int'l Workshop Future Mobile and Ubiquitous Information Technologies (FMUIT '06), 2006.
[33] Jihwan Lim, Heekuck Oh, SangJin Kim, A new hash-based RFID mutual authentication protocol providing enhanced user privacy protection, ISPEC, LNCS 4991 (2008) (2008) 278–289.
[34] Alex X. Liu, LeRoy A. Bailey, A privacy and authentication protocol for passive RFID tags, Comput. Commun. 32 (2009) 1194–1199.
[35] S.Y. Kang, D.G. Lee, I.Y. Lee, A study on secure RFID mutual authentication scheme in pervasive, Comput. Commun. 31 (2008) 4248–4254.
[36] J.S. Cho, S.S. Yeo, S.K. Kim, Securing against brute-force attack: a hash-based RFID mutual authentication protocol using a secret value, Comput. Commun. 34 (2011) 391–397.
[37] A. Juels, D. Molner, D. Wagner, Security and privacy issues in E-passports, in: Proc. First Int'l Conf. Security and Privacy for Emerging Areas in Comm. Networks (SecureComm '05), 2005.
[38] M. Burmester, B. Medeiros, R. Motta, Robust, Anonymous RFID Authentication with Constant Key-lookup, Cryptology ePrint Archive: Listing for 2007 (2007/402), 2007.
[39] G. Gaubatz, J.P. Kaps, E. Ozturk, B. Sunar, State of the art in ultra-low power public key cryptography for wireless sensor networks, in: Proc. in the Third IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOMW'05), 2005.
[40] S.V. Kaya, E. Savaş, A. Levi, Ö. Erçetin, Public key cryptography based privacy preserving multi-context RFID infrastructure, Ad Hoc Netw. 7 (2009) 136–152.
[41] N. Koblitz, Elliptic curve cryptosystems, Math. Comput. 48 (1987) 203–209.
[42] Y.K. Lee, K. Sakiyama, I. Verbauwhede, Elliptic-curve-based security processor for RFID, IEEE Trans. Comput. 57 (11) (2008).
[43] T. Dierks, E. Rescorla, RFC 5246 – The Transport Layer Security (TLS) Protocol Version 1.2, IETF, August 2008. <http://www.ietf.org/rfc/rfc5246.txt>.
[44] S. Kent, K. Seo, RFC 4301 – Security Architecture for the Internet Protocol, IETF, December 2005. <http://www.ietf.org/rfc/rfc4301.txt>.
[45] T. Ylonen, C. Lonvick, RFC 4251 – The Secure Shell (SSH) Protocol Architecture, IETF, January 2006. <http://www.rfc-editor.org/>.
[46] S. Bono, M. Green, A. Stubblefield, A. Juels, A. Rubin, M. Szydlo, Security analysis of a cryptographically enabled RFID device, In Proceedings of the USENIX Security Symposium, 2005.
[47] RFID Journal (2006), EPC Tags Subject to Phone Attacks. News Article, February 24, 2006. <http://www.rfidjournal.com/article/articleview/2167/1/1/> (04.05.06).
[48] Y. Chen, J.S. Chou, H.M. Sun, A novel mutual authentication scheme based on quadratic residues, Comput. Netw. 52 (2008) 2373–2380.
[49] T. Cao, P. Shen, Cryptanalysis of some RFID authentication protocols, J. Commun. 3 (7) (2008).
[50] T.C. Yeh, C.H. Wua, Y.M. Tseng, Improvement of the RFID authentication scheme based on quadratic residues, Comput. Commun. 34 (2011) 337–341.
[51] C.P. Schnorr, Efficient identification and signatures for smart cards, in: Gilles Brassard (Ed.), Advances in Cryptology – CRYPTO'89, Lecture Notes in Computer Science, 435, Springer-Verlag, 1989, pp. 239–252.
[52] T. Okamoto, Provably secure and practical identification schemes and corresponding signature schemes, in: E.F. Brickell (Ed.), Advances in Cryptology – CRYPTO'92, Lecture Notes in Computer Science, 740, Springer-Verlag, 1992, pp. 31–53.
[53] Y.K. Lee, L. Batina, I. Verbauwhede, EC-RAC (ECDLP Based Randomized Access Control): Provably Secure RFID Authentication Protocol, IEEE International Conference on RFID, 2008, pp. 97–104.
[54] Xinglei Zhang, Linsen Li, Yue Wu, Quanhai Zhang, An ECDLP-Based Randomized Key RFID Authentication Protocol, 2011 International Conference on Network Computing and Information Security.
[55] P. Tuyls, L. Batina, RFID-tags for anti-counterfeiting, Lect. Notes Comput. Sci. 3860 (2006) 115–131.
[56] L. Batina, J. Guajardo, T. Kerins, N. Mentens, P. Tuyls, I. Verbauwhede, Public-key cryptography for RFID-tags, in: Fifth IEEE International Conference on Pervasive Computing and Communications Workshops, 2007, pp. 217–222.
[57] T. Deursen, S. Radomirovíc, Attacks on RFID Protocols. In Cryptology ePrint Archive: listing for 2008 (2008/310), 2008.
[58] J. Bringer, H. Chabanne, T. Icart, Cryptanalysis of EC-RAC, a RFID identification protocol, in: International Conference on Cryptology and Network Security – CANS'08, Lecture Notes in Computer Science, Springer-Verlag, 2008.
[59] Gyozo Godor, Sandor Imre, Elliptic curve cryptography based authentication protocol for low-cost RFID tags, in: 2011 IEEE International Conference on RFID-Technologies and Applications, 2011.

Please cite this article in press as: Y.-P. Liao, C.-M. Hsiao, A secure ECC-based RFID authentication scheme integrated with ID-verifier transfer protocol, Ad Hoc Netw. (2013), http://dx.doi.org/10.1016/j.adhoc.2013.02.004

[60] M. Joye, S.-M. Yen, The montgomery powering ladder, in: CHES'02: Revised Papers from the 4th International Workshop on Cryptographic Hardware and Embedded Systems, Springer-Verlag, London, UK, 2003, pp. 291–302.

Yi-Pin Liao received the BS degree in Department of Electrical Engineering from the Tamkang University, Taipei, Taiwan, ROC in 1988, and the MS degree in Department of Electrical Engineering from the Tatung University, Taipei, Taiwan, ROC in 1990. He received his Ph.D in communication engineering in 2010 from Tatung University, Taipei, Taiwan, ROC. He is currently an associate professor of Computer Science and Information Engineering from the St. John's University, Taipei, Taiwan, ROC. His current research interests include information security, network security, identity authentication and mobile communication.

Chih-Ming Hsiao received the BS degree in computer science from Tatung Institute of Technology, Taiwan in 1994, and the MS and the PhD degree in Electrical Engineering from National Taiwan University of Science and Technology Taiwan, in 1996 and 2005, respectively. He is currently an assistant professor in the Department of Computer Science and Information Engineering at St. John's University, Taiwan. His research interests include distributed system, mobile computing, and vehicular ad hoc networks.

Please cite this article in press as: Y.-P. Liao, C.-M. Hsiao, A secure ECC-based RFID authentication scheme integrated with ID-verifier transfer protocol, Ad Hoc Netw. (2013), http://dx.doi.org/10.1016/j.adhoc.2013.02.004