Jeng-Shyang Pan
Ching-Nung Yang
Chia-Chen Lin
Editors

SMART INNOVATION, SYSTEMS AND TECHNOLOGIES ■ 21

Advances in Intelligent Systems and Applications – Volume 2

Proceedings of the International Computer Symposium ICS 2012 Held at Hualien, Taiwan, December 12–14, 2012

Springer

Smart Innovation, Systems and Technologies 21

For further volumes:
http://www.springer.com/series/8767

Jeng-Shyang Pan, Ching-Nung Yang,
and Chia-Chen Lin (Eds.)

Advances in Intelligent Systems and Applications – Volume 2

Proceedings of the International Computer Symposium ICS 2012 Held at Hualien, Taiwan, December 12–14, 2012

Springer

Editors

Prof. Jeng-Shyang Pan
Department of Electronic Engineering
National Kaohsiung University
of Applied Sciences
Taiwan
Republic of China

Prof. Chia-Chen Lin
Department of Computer Science
and Information Management
Providence University
Taiwan
Republic of China

Prof. Ching-Nung Yang
Department of Computer Science
and Information Engineering
National Dong Hwa University
Taiwan
Republic of China

ISSN 2190-3018 e-ISSN 2190-3026
ISBN 978-3-642-35472-4 e-ISBN 978-3-642-35473-1
DOI 10.1007/978-3-642-35473-1
Springer Heidelberg New York Dordrecht London

Library of Congress Control Number: 2012953485

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface

The field of Intelligent Systems and Applications has expanded enormously during the last two decades. Theoretical and practical results in this area are growing rapidly due to many successful applications and new theories derived from many diverse problems. This book is dedicated to the proceedings of International Computer Symposium (ICS). ICS is a biennial event and is one of the largest joint international IT symposiums held in Taiwan. Founded in 1973, its aim was to provide a forum for researchers, educators, and professionals to exchange their discoveries and practices, and to explore future trends and applications in computer technologies. ICS 2012 consists of twelve workshops. Totally, we received 257 submissions. The Program Committee finally selected 150 papers for presentation at the symposium. This volume contains papers from the following workshops. We would like to express our gratitude to all of the authors, the reviewers, and the attendees for their contributions and participation.

- Workshop on Computer Architecture, Embedded Systems, SoC, and VLSI/EDA
- Workshop on Cryptography and Information Security
- Workshop on Digital Content, Digital Life, and Human Computer Interaction
- Workshop on Image Processing, Computer Graphics, and Multimedia Technologies
- Workshop on Parallel, Peer-to-Peer, Distributed, and Cloud Computing
- Workshop on Software Engineering and Programming Languages

In ICS 2012, we are very pleased to have the following four distinguished invited speakers, who delivered state-of-the-art information on the conference topics:

- Professor Fedor V. Fomin from University of Bergen, Norway
- Professor L. Harn from University of Missouri-Kansas City, USA
- Professor C.-C. Jay Kuo from University of Southern California, USA
- Mr. Michael Wang, an Enterprise Architect, from Oracle, USA

ICS 2012 would not have been possible without the support of many people and organizations that helped in various ways to make it a success. In particular, we would like to thank the Ministry of Education of ROC (especially, the Computer Center of the MOE), National Science Council of ROC, Computer Audit Association of ROC, and Taiwan Association of Cloud Computing for their assistance and financial supports.

December 2012

Jeng-Shyang Pan
Ching-Nung Yang
Chia-Chen Lin

Organization

Honorary Chairs

Wei-ning Chiang	Ministry of Education, Taiwan
Cyrus Chin-yi Chu	National Science Council, Taiwan
Han-Chieh Chao	Computer Audit Association, Taiwan
Maw-Kuen Wu	National Dong Hwa University, Taiwan

Conference Chairs

Rong-Guey Ho	Computer Center of Ministry of Education, Taiwan
Wei-Pang Yang	National Dong Hwa University, Taiwan
Ruay-Shiung Chang	National Dong Hwa University, Taiwan

Conference Co-chairs

Shin-Feng Lin	National Dong Hwa University, Taiwan
Chenn-Jung Huang	National Dong Hwa University, Taiwan

Program Chairs

Ching-Nung Yang	National Dong Hwa University, Taiwan
Shiow-Yang Wu	National Dong Hwa University, Taiwan
Sheng-Lung Peng	National Dong Hwa University, Taiwan

Publicity Chairs

Cheng-Chin Chiang	National Dong Hwa University, Taiwan
Han-Ying Kao	National Dong Hwa University, Taiwan
Chung Yung	National Dong Hwa University, Taiwan

Local Arrangement Chairs

Wen-Kai Tai	National Dong Hwa University, Taiwan
Shi-Jim Yen	National Dong Hwa University, Taiwan
Min-Xiou Chen	National Dong Hwa University, Taiwan
Shou-Chih Lo	National Dong Hwa University, Taiwan
Chih-Hung Lai	National Dong Hwa University, Taiwan

Publication Chairs

Chia-Chen Lin	Providence University, Taiwan
Chang-Hsiung Tsai	National Dong Hwa University, Taiwan
I-Cheng Chang	National Dong Hwa University, Taiwan
Pao-Lien Lai	National Dong Hwa University, Taiwan

Registration Chairs

Guanling Lee	National Dong Hwa University, Taiwan
Mau-Tsuen Yang	National Dong Hwa University, Taiwan

Web Chairs

Chenn-Jung Huang	National Dong Hwa University, Taiwan
Hsin-Chou Chi	National Dong Hwa University, Taiwan
Tao-Ku Chang	National Taitung University, Taiwan

Workshop on Cryptography and Information Security

Chairs

Chin-Chen Chang	Feng Chia University, Taiwan
Jeng-Shyang Pan	National Kaohsiung University of Applied Sciences, Taiwan

Co-chairs

Ching-Nung Yang	National Dong Hwa University, Taiwan
Chia-Chen Lin	Providence University, Taiwan

Program Committee

Lakhmi C. Jain	University of South Australia, Austraila
Stelvio Cimato	University of Milan, Italy
Lein Harn	University of Missouri-Kansas City, USA
Asifullah Khan	Pakistan Institute of Engineering and Applied Sciences, Nilore, Pakistan
Cheonshik Kim	Sejong University, Korea
Lina Wang	Wuhan University, China
Daoshun Wang	Tsinghua University, China
Chu-Sing Yang	National Cheng Kung University, Taiwan
Hung-Min Sun	National Tsing Hwa University, Taiwan
Sung-Ming Yen	National Central University, Taiwan
Chun-I Fan	National Sun Yat-sen University, Taiwan
Jung-Hui Chiu	Chang-Gung University, Taiwan
Bo-Chao Cheng	National Chung Cheng University, Taiwan
Chih-Hung Wang	National Chiayi University, Taiwan
Chia-Mei Chen	National Sun Yat-sen University, Taiwan
Der-Chyuan Lou	Chang-Gung University, Taiwan
Jinn-Ke Jan	National Chung Hsing University, Taiwan
Shyong-Jian Shyu	Ming Chuan University, Taiwan
Wen-Chung Kuo	National Yunlin University of Science and Technology, Taiwan
Wu-Chuan Yang	I-Shou University, Taiwan
Yung-Cheng Lee	WuFeng University, Taiwan

Workshop on Image Processing, Computer Graphics, and Multimedia Technologies

Chairs

Chung-Lin Huang	National Tsing Hua University, Taiwan
Hsi-Jian Lee	Tzu Chi University, Taiwan

Co-chairs

I-Cheng Chang	National Dong Hwa University, Taiwan
Wen-Kai Tai	National Dong Hwa University, Taiwan
Chia-Hung Yeh	National Sun Yat-sen University, Taiwan

Program Committee

Chuan-Yu Chang	National Yunlin University of Science Technology, Taiwan
Bing-Yu Chen	Taiwan University, Taiwan
Chu-Song Chen	Academia Sinica, Taiwan
Jiann-Jone Chen	National Taiwan University of Science and Technology, Taiwan
Mei-Juan Chen	National Dong Hwa University, Taiwan
Wei-Ming Chen	National Ilan University, Taiwan
Fang-Hsuan Cheng	Chung Hua University, Taiwan
Cheng-Chin Chiang	National Dong Hwa University, Taiwan
Chin-Chuan Han	National United University, Taiwan
Shang-Hong Lai	National Tsing Hua University, Taiwan
Shin-Feng Lin	National Dong Hwa University, Taiwan
Chung-Ming Wang	National Chung Hsing University, Taiwan
Mau-Tsuen Yang	National Dong Hwa University, Taiwan

Workshop on Digital Content, Digital Life, and Human Computer Interaction

Chair

Yi-Ping Hung	National Taiwan University, Taiwan

Co-chairs

Cheng-Chin Chiang	National Dong Hwa University, Taiwan
Mau-Tsuen Yang	National Dong Hwa University, Taiwan

Program Committee

Chu-Song Chen	Academia Sinica, Taiwan
Mei-Juan Chen	National Dong Hwa University, Taiwan
Jen-Hui Chuang	National Chiao Tung University, Taiwan
Kuo-Liang Chung	National Taiwan University of Science and Technology, Taiwan
Pau-Choo Chung	National Cheng Kung University
Kuo-Chin Fan	National Central University, Taiwan
Chiou-Shann Fuh	National Taiwan University, Taiwan
Jun-Wei Hsieh	National Taiwan Ocean University, Taiwan
Chung-Lin Huang	National Tsing Hua University, Taiwan
Shang-Hong Lai	National Tsing Hua University, Taiwan
Chung-Nan Lee	National Sun Yat-sen University, Taiwan
Tong-Yee Lee	National Cheng Kung University, Taiwan
Hong-Yuan Mark Liao	Academia Sinica, Taiwan
Chia-Wen Lin	National Tsing Hua University, Taiwan
Chin-Teng Lin	National Chiao Tung University, Taiwan
Tyng-Luh Liu	Academia Sinica, Taiwan
Chia-Hung Yeh	National Sun Yat-sen University, Taiwan
Shiaw-Shian Yu	Industrial Technology Research Institute, Taiwan

Workshop on Parallel, Peer-to-Peer, Distributed, and Cloud Computing

Chair

Wang-Chien Lee	Pennsylvania State University, USA

Co-chair

Shiow-Yang Wu	National Dong Hwa University, Taiwan

Program Committee

Jiann-Liang Chen	National Taiwan University of Science and Technology, Taiwan
Ge-Ming Chiu	National Taiwan University of Science and Technology, Taiwan
Yeh-Ching Chung	National Tsing Hua University, Taiwan
Michael J. Franklin	UC Berkeley, USA
Kuen-Fang Jack Jea	National Chung Hsing University, Taiwan
Chung-Ta King	National Tsing Hua University, Taiwan
Chiang Lee	National Cheng Kung University, Taiwan
Chung-Nan Lee	National Sun Yat-sen University, Taiwan
Deron Liang	National Central University, Taiwan
Yao-Nan Lien	National Chengchi University, Taiwan
Chuan-Ming Liu	National Taipei University of Technology, Taiwan
Pangfeng Liu	National Taiwan University, Taiwan
Dusit (Tao) Niyato	Nanyang Technological University, Singapore
Wen-Chih Peng	National Chiao Tung University, Taiwan
Zheng Yan	Aalto University, Finland

Workshop on Software Engineering and Programming Languages

Chair

Wuu Yang	National Chiao Tung University, Taiwan

Co-chairs

Shih-Chien Chou	National Dong Hwa University, Taiwan
Chung Yung	National Dong Hwa University, Taiwan

Program Committee

Barrett Bryant	University of North Texas, USA
Wei-Ngan Chin	National University of Singapore, Singapore
Kung Chen	National Chengchi University, Taiwan
Tyng-Ruey Chuang	Academica Sinica, Taiwan
Pao-Ann Hsiung	National Chung Cheng University, Taiwan
Gwan-Hwan Hwang	National Taiwan Normal University, Taiwan
Wen-Hsiang Lu	National Cheng Kung University, Taiwan
Marjan Mernik	University of Maribor, Slovenia
Shin-Cheng Mu	Academica Sinica, Taiwa
Jiann-I Pan	Tzu Chi University, Taiwan
Yih-Kuen Tsay	National Taiwan University, Taiwan
Hsin-Chang Yang	National University of Kaohsiung, Taiwan

Workshop on Computer Architecture, Embedded Systems, SoC, and VLSI/EDA

Chair

Cheng-Wen Wu	Industrial Technology Research Institute, Taiwan

Co-chair

Hsin-Chou Chi	National Dong Hwa University, Taiwan

Program Committee

Robert Chen-Hao Chang	National Chung Hsing University, Taiwan
Yao-Wen Chang	National Taiwan University, Taiwan
Chung-Ho Chen	National Cheng Kung University, Taiwan
Tien-Fu Chen	National Chiao Tung University, Taiwan
Chung-Ping Chung	National Chiao Tung University, Taiwan
Shen-Fu Hsiao	National Sun Yat-sen University, Taiwan
Chun-Lung Hsu	Industrial Technology Research Institute, Taiwan
Ying-Jer Huang	National Sun Yat-sen University, Taiwan
Yin-Tsung Hwang	National Chung Hsing University, Taiwan
Gene-Eu Jan	National Taipei University, Taiwan
Yeong-Kang Lai	National Chung Hsing University, Taiwan
Gwo-Giun Lee	National Cheng Kung University, Taiwan
Tay-Jyi Lin	National Chung Cheng University, Taiwan
Tsung-Ying Sun	National Dong Hwa University, Taiwan
Chua-Ching Wang	National Sun Yat-sen University, Taiwan
Ro-Min Weng	National Dong Hwa University, Taiwan
An-Yeu Wu	National Taiwan University, Taiwan

Additional Reviewers

Bao Rong Chang
Jiann-Jone Chen
Cheng-Chieh Chiang
Shin-Yan Chiou
Chi-Hung Chuang
Jerry Chou
D.J. Guan
Wen-Zhong Guo
Kai-Lung Hua
JS Jang Jiang
Jong Yih Kuo
Yuchi Lai
Harn Lein
Wen-Hung Liao
Tzong-Jye Liu
Huang-Chia Shih
Raylin Tso
Chih-Hung Wang
Hsin-Min Wang
L.N. Wang
Shiuh-Jeng Wang
Wei-Jen Wang
Der-Lor Way
Tin-Yu Wu
Chao-Tung Yang
Martin Yang
C.Y. Yao

Contents

Track 1: Authentication, Identification, and Signature

Track 2: Intrusion Detection

Track 3: Steganography, Data Hiding, and Watermarking

Track 4: Database, System, and Communication Security

Track 5: Computer Vision, Object Tracking, and Pattern Recognition

Track 6: Image Processing, Medical Image Processing, and Video Coding

Track 7: Digital Content, Digital Life, and Human Computer Interaction

Track 8: Parallel, Peer-to-Peer, Distributed, and Cloud Computing

Track 9: Software Engineering and Programming Language

Track 10: Computer Architecture, Embedded Systems, SoC, and VLSI/EDA

A Secure ECC-Based RFID Authentication Scheme Using Hybrid Protocols

Yi-Pin Liao and Chih-Ming Hsiao

Department of Computer Science and Information Engineering, University of St. John, Taipei, Taiwan
{newsun87,cm}@mail.sju.edu.tw

Abstract. Radio Frequency Identification (RFID) has grown tremendously and has been widely applied in various applications. RFID tags are becoming very attractive devices installed a small microchip for identification of products. This chip functionality makes it possible to verify the authenticity of a product. It is well known that elliptic curve cryptosystem (ECC) receive much attention due to their small key sizes and efficient computations. Recently, some ECC-based authentication schemes are proposed to apply well to the limited resources of the tags. Unfortunately, these schemes ignore some security and operational issues. In this paper, we proposed a secure ECC-based RFID authentication scheme to achieve mutual authentication using both secure ID-verifier transfer and challenge-response protocols. Moreover, the proposed scheme can satisfy the security requirements of RFID. Performance analysis and function comparisons demonstrate that the proposed scheme is well suited for RFID tags with the scarceness of resources.

Keywords: Radio Frequency Identification, Elliptic curve cryptosystem, ID-verifier transfer.

1 Introduction

Recently, RFID has grown tremendously and has been widely applied in various applications such as inventory tracking, supply chain management, theft-prevention, and the like. Radio Frequency Identification (RFID) systems can identify hundreds of objects in a contactless manner at one time. Although RFID technology has potentials to improve our lives, it also presents a privacy risk. Privacy for RFID system is challenging problems due to tags response to nearby readers without discretion. In addition, other security issues make RFID tags an easy target for malicious attacks. Hence, it is essential to design authentication protocol that make RFID system more secure before it is viable for mass deployment. That is, privacy and authentication are the two main security issues that need to be addressed for the RFID technology. 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 [1-18] into non-public key cryptosystem (NPKC) based schemes and public key cryptosystem (PKC) based schemes.

J.-S. Pan et al. (Eds.): *Advances in Intelligent Systems & Applications*, SIST 21, pp. 1–13.
DOI: 10.1007/978-3-642-35473-1_1

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 [19]. That is, it is not possible to satisfy the requirements only with symmetric cryptographic algorithms such as hash algorithms and symmetric key encryption algorithms. To achieve significant consumer market penetration, RF tags will need to be priced in the US$0.05-US$0.10 range and contains only 500 to 5K gates. This causes many researchers deem the PKC based RFID systems to be infeasible at present. Fortunately, the CMOS technologies steadily advance and the fabrication costs decrease, which allows stronger security solutions on tags. Recently, a few papers [20-21] try to discuss the feasibility of PKC primitive cheap implementations on RFID tags; for example, Gaubatz et. al implements Rabin's encryption with cost about 17K gates [20], and Kaya and Savaş design NTRU public encryption which costs only about 3K gates [21].

Among PKC algorithms, elliptic curve cryptosystem (ECC) based algorithms would be best choice for RFID systems due to their small key sizes and efficient computations. 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. (2008) [22] presents the proposed RFID processor is composed of a microcontroller, an EC processor (ECP), and a bus manager, where the ECP is over $GF(2^{163})$. 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.

In this paper, we will adopt ECC primitives [23] 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) 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 discuss all possible vulnerabilities and requirements in RFID system. In section 3, we review the recent PKC based authentication schemes. Next, we propose a secure ECC-based authentication scheme for RFID system in section 4. Then, we make security analysis in section 5, and then performance and functionality comparisons are shown in section 6. Finally, the conclusion is given in section 7.

2 Essential System Requirements

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 some security issues. The system requirements are

defined in terms of mutual authentication, confidentiality, anonymity, availability, forward security and scalability.

(1) 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.
(2) 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.
(3) Anonymity: Anonymity is the most important security requirement for privacy [2]. 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.
(4) 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.
(5) 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.
(6) 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.

3 Related ECC-Based Works

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 [29]. For introducing ECC-based RFID schemes in this subsection, we should describe the concepts of ECC and related logarithms. In view of simplification, the details refer to [29]. Next, we will discuss some published schemes based on ECC in RFID system [30-32] as follows.

3.1 Tuyls et al.'s Scheme Using Schnorr Protocol [30]

Tuyls et al. (2006) [30] proposed an ECC-based RFID identification scheme using Schnorr identification protocol [33]. They claimed their scheme can resist against tag

counterfeiting, but Lee et al. (2008) [31] pointed their protocol suffers some weakness. The attacker can eavesdrops and collects the exchange messages aiming at a target tag. Hence, he/she can analyze the exchange messages to find the ID-verifier of the target tag. In other words, Tuyls et al.'s scheme is vulnerable to location tracking attack. Moreover, the attacker collects the exchange messages and the ID-verifier of the specific tag. Hence, he can identify the unknown tag as the specific tag using an active attack. Hence, the attacker can then use the ID-verifier to distinguish the tag from the past conversations easily. In other word, their protocol does not achieve forward security. 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 means that the server requires linear search to identity each tag and thus increases considerable computational cost. Hence, their protocol lacks scalability.

3.2 Batina et al.'s Scheme Using Okamoto Protocol [31]

Batina et al. (2007) [32] proposed an ECC-based RFID identification protocol using Okamoto's identification protocol [34]. Although they claimed their protocol can avoid active attacks, Lee et al. (2008) [31] pointed their protocol is vulnerable to location tracking attack. Similarly, a scalability problem and forward secrecy also exists in Batina et al.'s scheme.

3.3 Lee et al.'s Scheme Based on Random Access Control [32]

To solve all the requirements for RFID systems, Lee et al. (2008) [31] designed a new RFID protocol based on ECDLP. However, the works in [35-36] showed Lee et al.'s vulnerability against tracking attacks and forgery attacks. The failure of the security proof is caused by neglecting the possibility that an attacker can use multiple sets of authentic communication history [35]. The result shows that a tag can be traced by an attacker. Besides, Bringer et al. [36] 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.

4 The Proposed Scheme

This paper proposes an ECC-based mutual authentication schemes that satisfies all the requirements in RFID system. To assure the security of the ID-verifier transmitted from the tag over radio frequency, 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.

4.1 Setup Phase

In the setup phase, the server generates system parameters. The server chooses a random number $x_S \in Z_n$ as its private key and sets $P_S (= x_S P)$ as its public key. It also chooses $x_T \in Z_n$ as the private key of each tag and sets public key $Z_T (= x_T P)$ as the tag's ID-verifier. Hence, the server inserts the entry $\{Z_T, x_T\}$ of each tag into its database. Moreover, each tag stores $\{Z_T, x_T\}$ and system parameters in the memory. The system parameters and the storage of each entity are summarized in Table 1.

Table 1. The system parameters and the storage of each entity

System parameters	$P_S (= x_S P)$: Server's public key. P : Base point in $E(Z_p)$, whose order is n .
Server storage	Each tag's entry [Z_T, x_T], server private key x_S and common parameters(P , n)
Tag storage	The tag's public key Z_T as ID-verifier, private key x_T and common parameters (P_S , P , n)

4.2 Authentication Phase

The authentication phase is depicted in Fig. 1. 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 $R_2 = r_2 P$. Then it sends R_2 along with query message to the tag.

Step 2. After receiving the query message $< Query, R_2 >$, the tag chooses a random number $r_1 \in Z_n$ and computes $R_1 = r_1 P$. And then the tag computes two temporary secret keys $TK_{T1} = r_1 R_2$ and $TK_{T2} = r_1 P_S$. Next, the tag computes $Auth_T = Z_T + TK_{T1} + TK_{T2}$ to encrypt the ID-verifier Z_T , and sends $< Auth_T, R_1 >$ to the server.

Step 3. After receiving $< Auth_T, R_1 >$, the server recovers two temporary secret keys by way of computing $TK_{S1} = r_2 R_1$ and $TK_{S2} = x_S R_1$. Next, the server utilizes the following equation to retrieve the ID-verifier Z_T of the tag:

$$\begin{aligned} &\mathrm{Auth}_T - \mathrm{TK}_{S1} - \mathrm{TK}_{S2} = (Z_T + \mathrm{TK}_{T1} + \mathrm{TK}_{T2}) - \mathrm{TK}_{S1} - \mathrm{TK}_{S2} \\ &= (Z_T + r_1 R_2 + r_1 x_S P) - r_2 R_1 - x_S r_1 P = (Z_T + r_1 r_2 P + r_1 x_S P) - r_2 r_1 P - x_S r_1 P \quad (1) \\ &= Z_T \end{aligned}$$

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, the server calculates $\mathrm{Auth}_S = x_T R_1 + r_2 Z_T$ and sends back $< \mathrm{Auth}_S >$ to be authenticated by the tag.

Step 4. Next, the tag computes $r_1 Z_T + x_T R_2$ and checks if the value is equal to the received Auth_S. If it is equal, the tag conforms that the server is authentic.

5 Security Analysis

In this section, we will analyze the security of the proposed scheme to verify whether the system 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.

5.1 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 $< \mathrm{Auth}_T, R_1 >$ to the server. The message $\mathrm{Auth}_T (= Z_T + \mathrm{TK}_{T1} + \mathrm{TK}_{T2})$ can be interpreted as an encryption of Z_T with the temporary secret keys $(\mathrm{TK}_{T1}, \mathrm{TK}_{T2})$. The attacker cannot decrypt Z_T from Auth_T since the security of both TK_1 and TK_{T2} is based on ECDHP.

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 $< \mathrm{Auth}_S >$ to the tag. The message $\mathrm{Auth}_S (= x_T R_1 + r_2 Z_T)$ can be interpreted as an encryption of $r_2 Z_T$ with the secret key of $x_T R_1$. In other hand, as step 4 of the authentication phase, the

message $\text{Auth}_S (= r_1 Z_T + x_T R_2)$ can be regarded as an encryption of $r_1 Z_T$ with the secret key of $x_T R_2$. Since neither (r_2, x_T) nor (r_1, x_T) is known by the attacker, the ID-verifier Z_T cannot be extracted from Auth_S.

By I1and I2, a secure ID-verifier transfer protocol can be achieved.

I3: The freshness of exchange messages $< \text{Auth}_S, \text{Auth}_T >$ 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.

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 ID-verifier (i.e. Z_T) embedded in the received Auth_T. As step 3 of the authentication phase, the server receives message $< \text{Auth}_T, R_1 >$. According to I1, only the server can decrypt Z_T by way of calculating $\text{Auth}_T - TK_{S1} - TK_{S2}$. 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

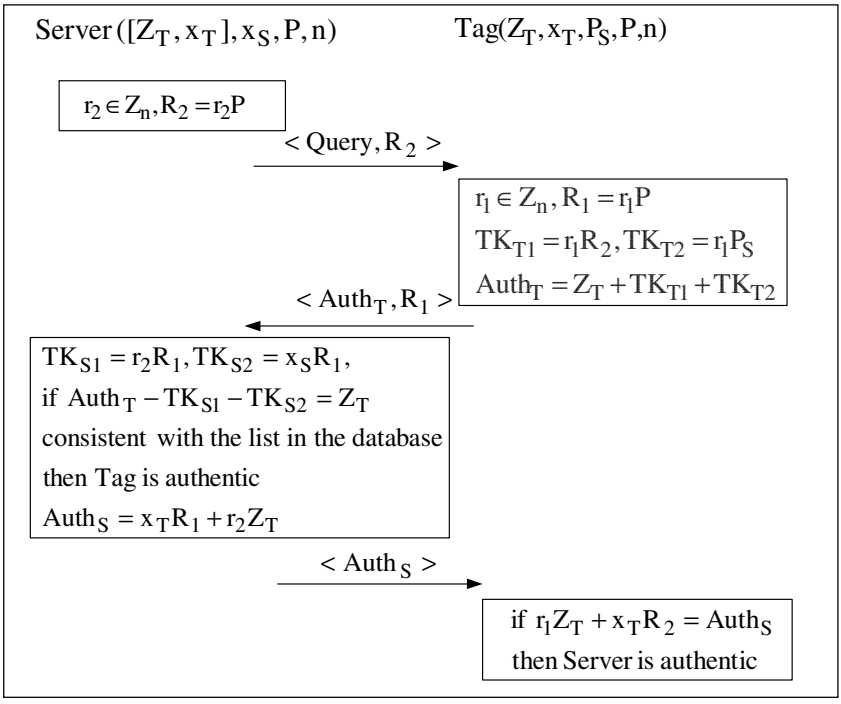

Fig. 1. The proposed scheme

is authentic by checking the correctness of ID-verifier (i.e. Z_T) embedded in the received $Auth_S$. As step 4 of the authentication phase, the tag receives message $Auth_S$ can be deduced as follows:

$$Auth_S = x_T R_1 + r_2 Z_T = x_T(r_1 P) + r_2(x_T P) = r_1(x_T P) + x_T(r_2 P) = r_1 Z_T + x_T R_2 \quad (2)$$

After receiving $Auth_S$, only the tag with $\{Z_T, x_T\}$ can compute $r_1 Z_T + x_T R_2$ 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.

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 $< Auth_T, Auth_S >$. Hence, the proposed protocol can achieve ID-verifier confidentiality.

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 by monitoring the exchanged messages according to SR2. Moreover, the exchange messages $< Auth_T, Auth_S >$ 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.

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.

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, by way of physical attack on a corrupted tag. 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.

SR6: Scalability
Proof: According to step3 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.

5.2 Attack Analysis

Next, we will prove that the proposed scheme can resist the following attacks

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).

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 $< Auth_T, R_1 >$ 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.

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.

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.

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.

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, there is no shared secret key in all of the tags. That is, the attacker cannot use the revealed secret to clone some other tags.

6 Performance and System Requirements Comparisons

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 includes the estimation of computation cost and communication cost. We focus the performance analysis in tag since the server is regarded as a powerful device. In this section, we analyze the efficiency of the proposed scheme. In general, all ECC protocols include a few point scalar multiplications and additions. Besides EC point scalar multiplication and addition, general modular operations are also needed for the computation of the authentication protocols. Recently, Lee et al. [22] proposed a compact architecture of an EC-based security processor for RFID. It is composed of a microcontroller, an EC processor (ECP), and a bus manager, where the ECP is over $GF(2^{163})$. ECP, which computes EC point scalar multiplications, is composed of a controller, MALU (Modular Arithmetic Logic Unit) and a register file. Since the modular operations can be performed in parallel with the EC point scalar multiplication, the former operations do not contribute to the latency. In the proposed scheme, the tag performs five point scalar multiplication computations and three point addition computations. Moreover, the server performs five point multiplication computations and three point addition computations.

Table 2 shows that the comparison among the existing ECC-based schemes in computation cost and communication cost. Seemingly, other ECC-based schemes [30, 32-33] are more efficient than the proposed scheme in tag's performance. However, they do not only provide mutual authentication but also suffer from some attacks discussed above. Hence, the performance of the proposed scheme is reasonable and acceptable. Moreover, we summarize the comparisons of system requirements among the existing ECC-based schemes in Table 3. The result concludes that our scheme is more secure and practical in real applications.

Table 2. Performance comparisons among ECC-based authentication schemes for RFID system

		Ours	Tuyls et al. [30]	Batina et al. [32]	Lee et al. [33]
Computation cost (ECm, ECa)*	Tag	(5,3)	(1,0)	(2,1)	(2,0)
	Server	(5,4)	(2,1)	(3,2)	(4,2)

ECm: ECC point scalar multiplication. ECa: ECC point addition.

Table 3. System requirements comparisons among ECC-based authentication schemes for RFID system

	Ours	Tuyls et al. [30]	Batina et al. [32]	Lee et al. [33]
Mutual authentication	Yes	No	No	No
Confidentiality	Yes	No	No	Yes
Anonymity	Yes	No	No	No
Availability	Yes	Yes	Yes	Yes
Forward security	Yes	No	No	Yes
Scalability	Yes	No	No	Yes

7 Conclusion

We present an ECC-based authentication scheme for RFID combined with hybrid protocols, including secure ID-verifier transfer and challenge-response protocols. Previously proposed schemes based on ECC cannot satisfy the requirements of RFID systems, including mutual authentication, confidentiality, anonymity, forward security and scalability. In this paper, the proposed scheme can be proven to satisfy all essential system requirements through security analysis. Performance analysis of the proposed scheme is well suited for RFID tags embedded a compact architecture of an EC-based security processor. In addition, we conclude that the proposed scheme can be applied well to other authentication applications which are similar to RFID environment.

References

1. EPCglobal: Specification for RFID Air Interface, `http://www.epcglobalinc.org`
2. Chien, H.Y., Chen, C.H.: Mutual Authentication Protocol for RFID Conforming to EPC Class 1 Generation 2 Standards. Computers Standards & Interfaces 29(2), 254–259 (2007)
3. Duc, D.N., Park, J., Lee, H., Kim, K.: Enhancing Security of EPCglobal Gen-2 RFID Tag against Traceability and Cloning. In: Proc. 2006 Symp. Cryptography and Information Security (2006)

4. Juels, A.: Strengthening EPC Tag against Cloning. In: Proc. ACM Workshop Wireless Security, WiSe 2005, pp. 67–76 (2005)
5. Yeh, T., Wang, Y., Kuo, T., Wang, S.: Securing RFID systems conforming to EPC Class 1 Generation 2 standard. Expert Systems with Applications 37, 7678–7683 (2010)
6. Chien, H.Y., Huang, C.W.: Security of Ultra-Lightweight RFID Authentication Protocols and Its Improvements. ACM Operating System Rev. 41(2), 83–86 (2007)
7. Li, T., Wang, G.: Security Analysis of Two Ultra-Lightweight RFID Authentication Protocols. In: Venter, H., Eloff, M., Labuschagne, L., Eloff, J., von Solms, R. (eds.) New Approaches for Security, Privacy and Trust in Complex Environments. IFIP, vol. 232, pp. 109–120. Springer, Boston (2007)
8. Peris-Lopez, P., Hernandez-Castro, J.C., Estevez-Tapiador, J.M., Ribagorda, A.: LMAP: A Real Lightweight Mutual Authentication Protocol for Low-Cost RFID Tags. In: Proc. Second Workshop RFID Security (July 2006)
9. Peris-Lopez, P., Hernandez-Castro, J.C., Estevez-Tapiador, J.M., Ribagorda, A.: EMAP: An Efficient Mutual-Authentication Protocol for Low-Cost RFID Tags. In: Meersman, R., Tari, Z., Herrero, P. (eds.) OTM Workshops 2006. LNCS, vol. 4277, pp. 352–361. Springer, Heidelberg (2006)
10. Peris-Lopez, P., Hernandez-Castro, J.C., Estevez-Tapiador, J.M., Ribagorda, A.: M^2AP: A Minimalist Mutual-Authentication Protocol for Low-Cost RFID Tags. In: Ma, J., Jin, H., Yang, L.T., Tsai, J.J.-P. (eds.) UIC 2006. LNCS, vol. 4159, pp. 912–923. Springer, Heidelberg (2006)
11. Chien, H.Y.: SASI: A New Ultralightweight RFID Authentication Protocol Providing Strong Authentication and Strong Integrity. IEEE Trans. Dependable and Secure Computing 4(4), 337–340 (2007)
12. Weis, S.A., Sarma, S.E., Rivest, R.L., Engels, D.W.: Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems. In: Hutter, D., Müller, G., Stephan, W., Ullmann, M. (eds.) Security in Pervasive Computing 2003. LNCS, vol. 2802, pp. 201–212. Springer, Heidelberg (2004)
13. Chien, H.Y.: Secure Access Control Schemes for RFID Systems with Anonymity. In: Proc. 2006 Int'l Workshop Future Mobile and Ubiquitous Information Technologies, FMUIT 2006 (2006)
14. Lim, J., Oh, H., Kim, S.-J.: A New Hash-Based RFID Mutual Authentication Protocol Providing Enhanced User Privacy Protection. In: Chen, L., Mu, Y., Susilo, W. (eds.) ISPEC 2008. LNCS, vol. 4991, pp. 278–289. Springer, Heidelberg (2008)
15. Liu, A.X., Bailey, L.R.A.: A privacy and authentication protocol for passive RFID tags. Computer Communications 32, 1194–1199 (2009)
16. Kang, S.Y., Lee, D.G., Lee, I.Y.: A study on secure RFID mutual authentication scheme in pervasive. Computer Communications 31, 4248–4254 (2008)
17. Cho, J.S., Yeo, S.S., Kim, S.K.: Securing against brute-force attack: A hash-based RFID mutual authentication protocol using a secret value. Computer Communications 34, 391–397 (2011)
18. Juels, A., Molner, D., Wagner, D.: Security and Privacy Issues in E-Passports. In: Proc. First Int'l Conf. Security and Privacy for Emerging Areas in Comm. Networks, SecureComm 2005 (2005)
19. Burmester, M., Medeiros, B., Motta, R.: Robust, anonymous RFID authentication with constant key-lookup. Cryptology ePrint Archive: listing for 2007 (2007/402) (2007)

20. Gaubatz, G., Kaps, J.P., Ozturk, E., Sunar, B.: 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 2005 (2005)
21. Kaya, S.V., Savas, E., Levi, A., Erçetin, Ö.: Public key cryptography based privacy preserving multi-context RFID infrastructure. Ad Hoc Networks 7, 136–152 (2009)
22. Lee, Y.K., Sakiyama, K., Verbauwhede, I.: Elliptic-Curve-Based Security Processor for RFID. IEEE Trans. on Computers 11(57) (November 2008)
23. Koblitz, N.: Elliptic curve cryptosystems. Mathematics of Computation 48, 203–209 (1987)
24. Bono, S., Green, M., Stubblefield, A., Juels, A., Rubin, A., Szydlo, M.: Security analysis of a cryptographically enabled RFID device. Pre-print, `http://www.rfidanalysis.org` (May 4, 2006)
25. RFID Journal: EPC Tags Subject to Phone Attacks. News Article (February 24, 2006), `http://www.rfidjournal.com/article/articleview/2167/1/1/` (May 4, 2006)
26. Chen, Y., Chou, J.S., Sun, H.M.: A novel mutual authentication scheme based on quadratic residues. Computer Networks 52, 2373–2380 (2008)
27. Cao, T., Shen, P.: Cryptanalysis of some RFID authentication protocols. Journal of Communications 3(7) (December 2008)
28. Yeh, T.C., Wua, C.H., Tseng, Y.M.: Improvement of the RFID authentication scheme based on quadratic residues. Computer Communications 34, 337–341 (2011)
29. Koblitz, N.: Elliptic curve cryptosystems. Mathematics of Computation 48, 203–209 (1987)
30. Tuyls, P., Batina, L.: RFID-Tags for Anti-counterfeiting. In: Pointcheval, D. (ed.) CT-RSA 2006. LNCS, vol. 3860, pp. 115–131. Springer, Heidelberg (2006)
31. Lee, Y.K., Batina, L., Verbauwhede, I.: EC-RAC (ECDLP Based Randomized Access Control): Provably Secure RFID authentication protocol. In: IEEE International Conference on RFID, pp. 97–104 (2008)
32. Batina, L., Guajardo, J., Kerins, T., Mentens, N., Tuyls, P., Verbauwhede, I.: Public-Key Cryptography for RFID-tags. In: Fifth IEEE International Conference on Pervasive Computing and Communications Workshops, pp. 217–222 (2007)
33. Schnorr, C.-P.: Efficient Identification and Signatures for Smart Cards. In: Brassard, G. (ed.) CRYPTO 1989. LNCS, vol. 435, pp. 239–252. Springer, Heidelberg (1990)
34. Okamoto, T.: Provably Secure and Practical Identification Schemes and Corresponding Signature Schemes. In: Brickell, E.F. (ed.) CRYPTO 1992. LNCS, vol. 740, pp. 31–53. Springer, Heidelberg (1993)
35. Deursen, T., Radomirović, S.: Attacks on RFID Protocols. Cryptology ePrint Archive: listing for 2008 (2008)
36. Bringer, J., Chabanne, H., Icart, T.: Cryptanalysis of EC-RAC, a RFID Identification Protocol. In: Franklin, M.K., Hui, L.C.K., Wong, D.S. (eds.) CANS 2008. LNCS, vol. 5339, pp. 149–161. Springer, Heidelberg (2008)

A Dynamic Approach to Hash-Based Privacy-Preserving RFID Protocols

Chih-Yuan Lee[1], Hsin-Lung Wu[1], and Jen-Chun Chang[1]

Department of Computer Science and Information Engineering,
National Taipei University,
New Taipei City, Taiwan
s710083108@webmail.ntpu.edu.tw, {hsinlung,jcchang}@mail.ntpu.edu.tw

Abstract. We study how to design a hash-based identification protocol in a RFID system which obtains security and privacy against active adversaries. Here, an active adversary can not only track a tag via successful or unsuccessful identifications with legal or illegal readers but also perform a compromised attack. In *SPC 2003*, Weis et al. used the technique of the randomized hash lock to design a privacy-preserving protocol against such active adversaries. However, in their protocol, the time complexity of identifying a requested tag is linear in the number of legal tags. It is still an open problem to design a protocol which obtains privacy against active adversaries and has a sublinear time complexity of tag identification.

In this work, we revisit this open problem. We modify the protocol of Weis et al. by using a dynamic key management scheme to manage tag identities stored in the back-end database instead of a static approach. For privacy, our protocol obtains the same privacy level as the protocol of Weis et al.. For performance, the amortized cost of tag identification of our protocol is almost twice the optimal amortized cost by a competitive analysis. For practical implementation, our protocol is very suitable to be realized in RFID systems due to its online property.

1 Introduction and Related Works

RFID (Radio-Frequency Identification) is a technology in which one can identify objects or people by embedding tags, a small microchip capable of wireless data transmission. By tagging wares in shops, one can speed up the process of registration with wireless scanning. RFID tags have several characteristics. First of all, each tag has an identifier to represent itself. Moreover, such identifiers are long enough so that it has a unique code. When a tiny tag is implanted within an object, finding such a tag means discovering the corresponding object. Second, tag identification via radio frequency allows tagged objects to be read multiple times at a distance. These characteristics introduce security and privacy issues. Objects embedded with insecure tags may reveal private information as they are queried by legal or illegal readers. For the privacy issue, objects embedded with tags that do not reveal any sensitive information may also be tracked by

J.-S. Pan et al. (Eds.): *Advances in Intelligent Systems & Applications*, SIST 21, pp. 15–23.
DOI: 10.1007/978-3-642-35473-1_2

the implanted tags. This is because the tag responses to the requesting readers are possible to help locate the tagged objects by analyzing information from the protocol view between the embedded tag and the reader. This may cause objects to reveal their private data such as their identifications in the future. We refer the readers to Juels' excellent survey [4] on the privacy issue.

In [3,2], formal definitions of privacy are given. Privacy of tags is defined by the ability of adversaries to trace tags by using their responses to readers' interrogations. The authors define two degrees of privacy for RFID tags. Adversaries who try to distinguish two given tags only from their successful identifications with a legitimate reader are called passive adversaries. On the other hand, adversaries who try to differentiate two given tags from their successful or unsuccessful identifications with any reader (legal or illegal) are called active adversaries. In [2], privacy against passive adversaries is called universal traceability whereas privacy against active adversaries is called existential traceability.

On one hand, for privacy-preserving protocols against passive adversaries, Alomair et al. propose a nice protocol in which tag identification can be obtained with constant time [3]. On the other hand, Weis et al. give an identification protocol called the randomized hash lock [7] which obtains privacy against active adversaries. However, in this protocol, the time complexity of tag identification is linear in n where n is the number of legitimate tags. To improve the time efficiency of tag identification, Molnar and Wagner [5] propose a tree-based protocol in which tag identification can be done within $O(\log n)$. However, in [1], Avoine et al. propose new attacks on RFID privacy called compromised attacks in which adversaries may know secrets of some tags. Avoine et al. show that one can obtain compromised attacks for the tree-based protocols with high successful probability. Note that the compromised attacks threat not only tree-based protocols but also those protocols in which the tag identities have high correlation. In this paper, we allow active adversaries perform compromised attacks. It is still an open problem whether there is a privacy-preserving protocol against active adversaries which has identification complexity in sublinear in n.

1.1 Our Contributions

In this work, we construct a privacy-preserving protocol whose privacy level is the same as the protocol of Weis et al [7]. In fact, our proposed protocol obtains privacy against active adversaries and against compromised attacks. In order to improve the efficiency of tag identification, we use a dynamic key management scheme called the move-to-front scheme to store tag identities in the back-end database. By a competitive analysis, the amortized cost of our proposed protocol is almost twice the amortized cost of the optimal key management scheme. We also show that, in some cases, our proposed protocol has amortized constant time to obtain tag identification while the original randomized-hash-lock protocol may require linear time to do it. For practical implementation, the proposed move-to-front key management scheme is easy to implemented by using a data structure such as linked lists.

The remaining part of the paper is organized as follows. In Section 2, we give necessary privacy definitions and some notations. We also introduce the randomized-hash-lock protocol of Weis et al. there. In Section 3, we propose our move-to-front protocol and its efficiency analysis. Finally we conclude in Section 5.

2 Preliminaries

In our proposed protocol, we assume that communication channel between the reader and the back-end database is secure while communication channel between the reader and each tag is insecure. For convenience, we use the following notation in the rest of the paper.

Notation	Corresponding Meaning
n	Number of tags participating in the RFID system
ID_k	Identity of the k-th tag
$h()$	Hash operation

2.1 Privacy Definitions

Here, we give two definitions for the RFID privacy.

Definition 1. *[3](Universal Untraceability) An RFID protocol is universally untraceable if an adversary cannot track a tag based on information obtained from the protocol view between the tag and a legal reader.*

Definition 2. *[3](Existential Untraceability) An RFID protocol is existentially untraceable if an active adversary cannot track a tag based on its responses to multiple interrogation even if the tag has not been able to accomplish mutual authentication with an authorized reader.*

For more formal definitions of the above two definitions, we refer the readers to [3].

2.2 The Randomized-Hash-Lock Protocol

In [7], Weis et al. propose a hash-based RFID identification protocol which obtains existential untraceability. Usually, because of using hash functions and randomness, their protocol is called randomized-hash-lock protocol. Their protocol is describes as follows.

Setup. There are n identities $ID_1, \ldots, ID_n$ which are stored in a fixed array in the back-end database. The i-th tag has ID_i as its identity. Each Tag and each reader have random number generators and share a hash function h.

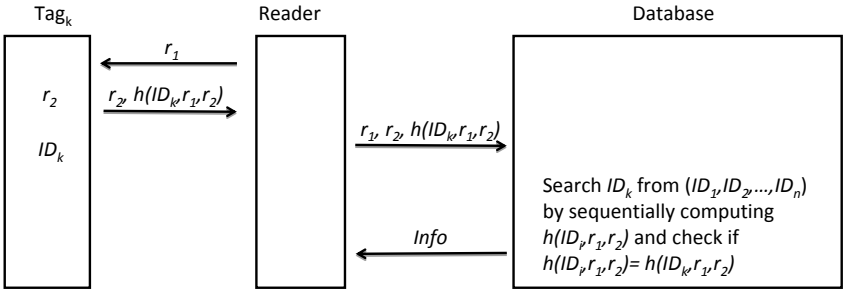

Fig. 1. One single round of the protocol of Weis et al. in [7]

Identification Process. The identification process goes as follows. The implemented version is illustrated in Fig. 1.

1. The reader requests the tag and sends a random string r_1 to it.
2. The k-th tag generates a random string r_2 and computes $h(ID_k, r_1, r_2)$. Next the tag sends them as well as r_1 and r_2 to the reader which passes them to the database.
3. Assume that the tag identities are stored in the linked list whose order is $(ID_1, \ldots, ID_n)$. To identify the tag, the database sequentially computes $h(ID_i, r_1, r_2)$ and check if it is equal to $h(ID_k, r_1, r_2)$ for i from 1 to n.
The above protocol of Weis et al. obtains existential untraceability.

3 MTF Protocol

In this section, we propose a hash-based RFID protocol which uses a dynamic key management scheme in the back-end database. For convenience, we call the proposed protocol $\mathcal{MTF}$.

Setup. There are n identities $ID_1, \ldots, ID_n$ which are stored by using a linked list in the database. We illustrate such a linked list in Figure 2. The i-th tag has ID_i as its identity. Each Tag and each reader have random number generators and share a hash function h.

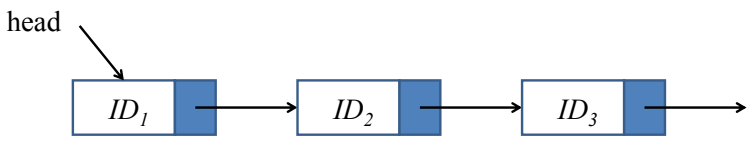

Fig. 2. A linked list of Tag identities

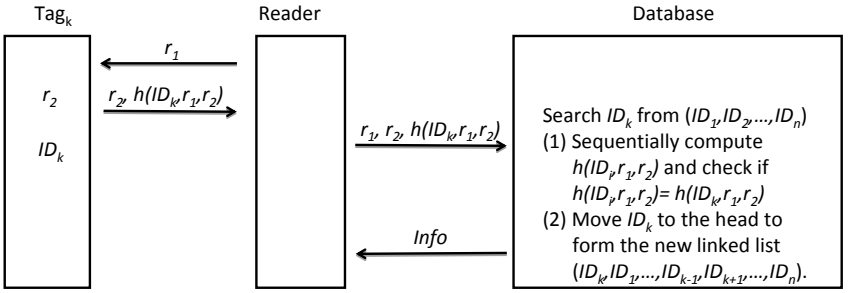

Fig. 3. One single round of protocol $\mathcal{MTF}$

Identification Process. Now the identification process goes as follows. The implemented version is illustrated in Fig. 3.

1. The reader requests the tag and sends a random string r_1 to it.
2. The k-th tag generates a random string r_2 and computes $h(ID_k, r_1, r_2)$. Next the tag sends them as well as r_1 and r_2 to the reader which passes them to the database.
3. Assume that the tag identities are stored in the linked list whose order is $(ID_1, \ldots, ID_n)$. To identify the tag, the database sequentially computes $h(ID_i, r_1, r_2)$ and check if it is equal to $h(ID_k, r_1, r_2)$ for i from 1 to n. After finding ID_k, the database updates the linked list by moving ID_k to the first position of the linked list. The order of the resulting linked list is $(ID_k, ID_1, \ldots, ID_{k-1}, ID_{k+1}, \ldots, ID_n)$.

The difference between our protocol and protocol of Weis et al. is that the database of our protocol updates the order of the lists of tags while the database of the protocol of Weis et al. does not. Here we give an example to illustrate the modification of the linked list after identifying a specific tag in Figure 4. In this example, after Tag 5 is found, it is moved to the head of the linked list.

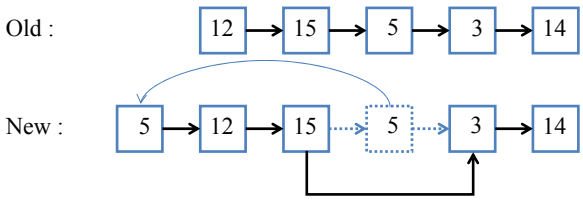

Fig. 4. The updated linked-list after one round of protocol $\mathcal{MTF}$

3.1 Security Analysis

$\mathcal{MTF}$ inherits from the security and the privacy proofs of the randomized-hash-locked protocol in [7] since $\mathcal{MTF}$ does not modify the information exchanged or the internal content of the tag. In fact, the protocol view of $\mathcal{MTF}$ is the same as the one of the randomized-hash-locked protocol and $\mathcal{MTF}$ only change the way of key management in the back-end database. As a result, protocol $\mathcal{MTF}$ obtains the same security and privacy level as the randomized-hash-lock one. Therefore, $\mathcal{MTF}$ has existential untraceability.

4 A Competitive Analysis on Efficiency

Let n be the number of items in the linked-list. Given a protocol $\mathcal{P}$, we define the cost $\mathsf{C}_{\mathcal{P}}(i)$ of the protocol $\mathcal{P}$ to identify tag i by the number of cryptographic hash operations used by the back-end database. Let σ be the requested tag sequence of length m, that is $\sigma = (i_1, i_2, \ldots, i_m)$ where i_k means that Tag i_k is requested by the reader in the k-th order. In addition, let $\mathsf{C}_{\mathcal{A}}(\sigma)$ be the cost of the protocol $\mathcal{A}$ on the requested tag sequence σ, that is

$$\mathsf{C}_{\mathcal{A}}(\sigma) = \sum_{k=1}^{m} \mathsf{C}_{\mathcal{A}}(i_k).$$

Static Offline Optimal Protocol: Let f_i be the frequency of accessing the i-th tag on a requested tag sequence σ. Suppose we know f_i for each $1 \leq i \leq n$. An obvious way to reduce the cost of searching tags is to arrange the tag list in a decreasing order of the frequencies. For convenience, we assume that f_i is decreasing with respect to i. We call such a list a static offline optimal tag list. Let $\mathcal{SOOP}$ be the randomized-hash-lock protocol which uses such a static offline optimal tag list in the back-end database. It is easy to see that

$$\mathsf{C}_{\mathcal{SOOP}}(\sigma) = \sum_{i=1}^{n} i f_i.$$

We call $\mathsf{C}_{\mathcal{SOOP}}(\sigma)$ the static offline optimal cost on σ. The main drawback of protocol $\mathcal{SOOP}$ is that we do not know the frequency f_i initially. Thus one cannot expect to arrange the tag list in a static offline optimal tag list.

Optimal Self-organizing Protocol: A self-organizing protocol can move the identity of the requested tag into any position of the linked list after the database finds or inserts it. Given a requested tag sequence σ, the optimal self-organizing protocol on σ is a self-organizing protocol which obtains the minimal cost on σ. Note that the optimal self-organizing protocol knows the whole requested sequence σ as the static offline optimal protocol. Furthermore, it can perform exchanges of tag identities after identifying a tag whereas the static offline optimal protocol cannot. Note that the complexity of exchanges of tag identities

can be easily obtained in a linked list. Let $\mathsf{C}_{\mathcal{OPT}}(\sigma)$ be the cost of the optimal self-organizing protocol on σ. Clearly we have

$$\mathsf{C}_{\mathcal{OPT}}(\sigma) \leq \mathsf{C}_{\mathcal{SOOP}}(\sigma)$$

for any sequence σ. Similar to the static offline optimal protocol, the drawback of the optimal protocol is that it should be implemented by an offline key management scheme.

Move-to-Front Protocol: This is just our proposed protocol $\mathcal{MTF}$. In this protocol, after identifying or inserting a tag, the algorithm moves the identity of the requested tag to the head of the linked list while preserving the relative order of the other tags. Obviously its key management scheme on tag identities is an online scheme. Hence $\mathcal{MTF}$ is suitable to be used in the back-end database of the RFID system. Given a requested sequence σ, let $\mathsf{C}_{\mathcal{MTF}}(\sigma)$ be the cost of the Move-to-Front protocol on σ. By the same argument in the seminar result of [6], it can be proved that

$$\mathsf{C}_{\mathcal{MTF}}(\sigma) \leq 2\mathsf{C}_{\mathcal{OPT}}(\sigma)$$

for any sequence σ if the protocol starts from the empty linked list. On the other hand, if the protocol starts from a nonempty list, then we have

$$\mathsf{C}_{\mathcal{MTF}}(\sigma) \leq 2\mathsf{C}_{\mathcal{OPT}}(\sigma) + O(n^2)$$

for any sequence σ. As a corollary, we have

$$\mathsf{C}_{\mathcal{MTF}}(\sigma) \leq 2\mathsf{C}_{\mathcal{SOOP}}(\sigma) + O(n^2)$$

for any sequence σ.

4.1 Some Examples

Here we consider some distributions on tag-accessing frequency.

Example 1. Define $f_i \doteq 2^{n-i}$ for $1 \leq i \leq n$. Suppose σ is any requested sequence in which the frequency of the i-th tag is f_i for $1 \leq i \leq n$. Then, the cost of the static offline optimal protocol is as follows:

$$\begin{aligned}\mathsf{C}_{\mathcal{SOOP}}(\sigma) &= \sum_{i=1}^{n} i f_i \\ &= \sum_{i=1}^{n} i 2^{n-i} \\ &= 2^{n+1} - n - 2.\end{aligned}$$

Note that the length of σ is

$$m = \sum_{i=1}^{n} f_i = \sum_{i=1}^{n} 2^{n-i} = 2^n - 1.$$

Since $\mathsf{C}_{\mathcal{MTF}}(\sigma) \leq 2\mathsf{C}_{\mathcal{SOOP}}(\sigma) + O(n^2)$, we have

$$\mathsf{C}_{\mathcal{MTF}}(\sigma) \leq 2\mathsf{C}_{\mathcal{SOOP}}(\sigma) + O(n^2) = 2(2^{n+1} - n - 2) + O(n^2).$$

The amortized cost of $\mathcal{MTF}$ protocol for the requested sequence σ is

$$\frac{\mathsf{C}_{\mathcal{MTF}}(\sigma)}{m} \leq \frac{2(2^{n+1} - n - 2) + O(n^2)}{2^n - 1} \leq 4$$

if n is large enough.

On the other hand, the worst static case occurs when tags are listed in an increasing order according to frequencies f_i's. The cost is $\sum_{i=1}^{n} i2^{i-1} = (n-1)2^n - 3$. The amortized cost is at least $\frac{(n-1)2^n-3}{2^n-1} \geq n - 1$.

Example 2. In this example, we show that $\mathcal{MTF}$ has a better performance than $\mathcal{SOOP}$. Suppose σ is a requested sequence such that

$$\sigma = (n, \underbrace{n-1, , \ldots, n-1}_{2}, \ldots, \underbrace{i, \ldots, i}_{n-i+1}, \ldots, \underbrace{1, \ldots, 1}_{n}).$$

Clearly the frequency $f_i = n - i + 1$ for $1 \leq i \leq n$ in the sequence σ. The cost of the static offline optimal protocol is as follows:

$$\begin{aligned} \mathsf{C}_{\mathcal{SOOP}}(\sigma) &= \sum_{i=1}^{n} i f_i \\ &= \sum_{i=1}^{n} i(n - i + 1) \\ &= \frac{n(n+1)(2n+1)}{6}. \end{aligned}$$

Next, the length of σ is

$$m = \sum_{i=1}^{n} f_i = \sum_{i=1}^{n} n - i + 1 = \frac{n(n+1)}{2}.$$

So the amortized cost of $\mathcal{SOOP}$ for σ is at least $\frac{2n}{3}$. Let us see the cost $\mathsf{C}_{\mathcal{MTF}}(\sigma)$. We have

$$\mathsf{C}_{\mathcal{MTF}}(\sigma) \leq \sum_{i=1}^{n} n + (i-1) = \frac{3n^2 - n}{2}.$$

Thus the amortized cost of $\mathcal{MTF}$ protocol for the requested sequence σ is

$$\frac{\mathsf{C}_{\mathcal{MTF}}(\sigma)}{m} \leq 3.$$

5 Conclusion

In this paper, we construct a hash-based RFID identification protocol called $\mathcal{MTF}$ which obtains existential untraceability and can be against compromised attacks. In addition, via a competitive analysis, $\mathcal{MTF}$ has almost twice optimal amortized cost on the time efficiency of tag identification. Moreover, in a practical sense, the proposed $\mathcal{MTF}$ protocol is suitable to be implemented in RFID systems due to its online property.

References

1. Avoine, G., Dysli, E., Oechslin, P.: Reducing Time Complexity in RFID Systems. In: Preneel, B., Tavares, S. (eds.) SAC 2005. LNCS, vol. 3897, pp. 291–306. Springer, Heidelberg (2006)
2. Alomair, B., Poovendran, R.: Privacy versus scalability in radio frequency identification systems. Computer Communications 33(18), 2155–2163 (2010)
3. Alomair, B., Clark, A., Cuellar, J., Poovendran, R.: Scalable RFID systems: a privacy-preserving protocol with constant-time identification. In: Procedings of the 40th Annual IEEE/IFIP International Conference on Dependable Systems and Networks V, DSN 2010, Chicago, Illinois, USA. IEEE (2010)
4. Juels, A.: RFID security and privacy: a research survey. IEEE Journal on Selected Areas in Communications 24(2), 381–394 (2006)
5. Molnar, D., Wagner, D.: Privacy and security in library RFID: issues, practices, and architectures. In: Proceedings of the 11th ACM Conference on Computer and Communications Security, pp. 210–219 (2004)
6. Sleator, D., Tarjan, R.: Amortized efficiency of list update and paging rules. Communications of the ACM 28(2), 202–208 (1985)
7. Weis, S.A., Sarma, S.E., Rivest, R.L., Engels, D.W.: Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems. In: Hutter, D., Müller, G., Stephan, W., Ullmann, M. (eds.) Security in Pervasive Computing 2003. LNCS, vol. 2802, pp. 201–212. Springer, Heidelberg (2004)

An Extension of Harn-Lin's Cheater Detection and Identification

Lein Harn[1] and Changlu Lin[2]

[1] Department of Computer Science and Electrical Engineering
University of Missouri-Kansas City, MO 64110-2499, USA
harnl@umkc.edu
[2] Key Laboratory of Network Security and Cryptology
Fujian Normal University, Fujian, 350007, P.R. China
cllin@fjnu.edu.cn

Abstract. Cheater detection and identification are important issues in the process of secret reconstruction. Most algorithms to detect and identify cheaters need the dealer to generate and distribute additional information to shareholders. In a recent paper, algorithms have been proposed to detect and identify cheaters based on shares only without needing any additional information. However, more than t (i.e. the threshold) shares are needed in the secret reconstruction. In this paper, we extend the algorithms to the situation when there are exact t shares in the secret reconstruction. We adopt the threshold changeable secret sharing which shareholders work together to change the threshold t into a new threshold t' (i.e., $t' < t$) and generate new shares of a (t', n) secret sharing; while at the same time, maintain the original secret. Since $t' < t$, there are redundant shares. We also include discussion on how to select the new threshold t' in order to detect and identify cheaters successfully.

Keywords: Secret sharing, threshold changeable secret sharing, cheaters, redundant share.

1 Introduction

In a (t, n) secret sharing scheme, a dealer divides the secret into shares in such a way that any t (i.e., the threshold) or more than t shares can reconstruct the secret; while any fewer than t shares cannot obtain any information about the secret. Shamir's (t, n) secret sharing scheme [16] is based on the linear polynomial. Secret reconstruction uses Lagrange interpolating polynomial.

When shareholders present their shares in the secret reconstruction, dishonest shareholders (i.e. cheaters) can always exclusively derive the secret by presenting fake shares and thus the other honest shareholders get nothing but a fake secret. It is easy to see that Shamir's (t, n) secret sharing scheme does not prevent dishonest shareholders in the secret reconstruction. Cheater detection and identification are important features in order to provide fair reconstruction of a secret.

There are many research papers in the literature to propose algorithms for cheater detection and identification. Most of these algorithms

J.-S. Pan et al. (Eds.): *Advances in Intelligent Systems & Applications*, SIST 21, pp. 25–32.
DOI: 10.1007/978-3-642-35473-1_3

[17,4,15,6,5,11,9,14,13,1] assume that there are exact t shareholders participated in the secret reconstruction. The dealer needs to provide additional information to enable shareholders to detect and identify cheaters. Some algorithms [12,3] use error-correcting codes to detect and identify fake shares.

In a recent paper, Harn and Lin [7] proposed a new approach to detect and identify cheaters. The algorithm uses shares to detect and identify cheaters. When there are more than t (i.e., the threshold) shares in the secret reconstruction, the redundant shares can be used to detect and identify cheaters. In this approach, shares in a secret sharing scheme serve for two purposes; that are, (a) reconstructing the secret and (b) detecting and identifying cheaters. Since Harn and Lin's algorithm requires more than t shares in the secret reconstruction, the algorithm does not work if there are exact t shares. In this paper, we generalize Harn and Lin's algorithm to the situation when they are exact t shares in the (t, n) secret reconstruction. We adopt the threshold changeable secret sharing (TCSS) which shareholders work together to change the threshold t into a new threshold t' and generate new shares of a (t', n) secret sharing; while at the same time, maintain the original secret. Since $t' < t$, there are redundant shares. The new shares can be verified without revealing the secret and new shares. We also include discussion on how to select the new threshold t' in cheater detection and identification.

The Rest of This Paper Is Organized as Follows. In the next section, we briefly review Shamir's (t, n) secret sharing scheme [16] and Harn and Lin's algorithm [7]. In Section 3, we propose our generalized scheme. We conclude in Section 4.

2 Preliminaries

2.1 Review of Shamir's Secret Sharing Scheme [16]

In Shamir's (t, n) secret sharing scheme based on the polynomial, there are n shareholders and a mutually trusted dealer. The scheme consists of two algorithms:

Scheme 1: Shamir's (t, n) secret sharing scheme

1. Share generation algorithm: the dealer first picks a random polynomial of degree $t-1$, $f_i(x) = a_{t-1}x^{t-1} + \cdots + a_1 x + a_0 \pmod p$, such that the secret s satisfies $f(0) = a_0 = s$ and all coefficients, $a_0, a_1, \ldots, a_{t-1} \in \mathbb{Z}_p$, p is a prime with $p > s$. The dealer computes shares as, $f(x_i)$, for $i = 1, 2, \ldots, n$, and distributes each share $f(x_i)$ to shareholder U_i secretly.
2. Secret reconstruction algorithm: it takes any t or more than t shares, for example, with following t shares, $\{(x_1, f(x_1)), (x_2, f(x_2)), \ldots, (x_t, f(x_t))\}$, as inputs, and outputs the secret s using the Lagrange interpolating formula as

$$s = \sum_{i=1}^{t} f(x_i) \prod_{r=1, j\neq i}^{t} \frac{-x_j}{x_i - x_j} \pmod p.$$

We note that the above algorithms satisfy the basic requirements of the secret sharing scheme, that are, (1) with the knowledge of any t or more than t shares, shareholders can reconstruct the secret s; and (2) with the knowledge of any $t-1$ or fewer than $t-1$ shares, shareholders cannot obtain the secret s. Shamir's secret sharing scheme is unconditionally secure since the scheme satisfies these two requirements without making any computational assumption. For more information on this scheme, please refer to the original paper [16].

2.2 Review of Harn and Lin's Algorithm [7]

We briefly review the algorithm [7] to detect and identify cheaters using the property of strong t-consistency and majority voting mechanism. The algorithm assumes that there are more than t shareholders participated in the secret reconstruction.

Benaloh [2] presented a notion of t-consistency to determine whether a set of n (i.e., $n > t$) shares are generated from a polynomial of degree $t-1$ at most. Recently, Harn and Lin [8] proposed a new definition of strong t-consistency which is the extension of Benaloh's definition.

Definition 1 (Strong t-consistency [8]). *A set of n shares (i.e., $t < n$) is said to be strong t-consistent if (a) any subset of t or more than t shares can reconstruct the same secret, and (b) any subset of fewer than t shares cannot reconstruct the same secret.* □

It is obvious that if shares in Shamir's (t, n) secret sharing scheme are generated by a polynomial with degree $t-1$ exactly, then shares are strong t-consistent. Checking strong t-consistency of n shares can be executed very efficiently by using the Lagrange interpolating formula. In fact, to check whether n shares are strong t-consistent or not, it only needs to check whether the interpolation of n shares yields a polynomial with degree $t-1$ exactly. If this condition is satisfied, we can conclude that all shares are strong t-consistent. However, if there are some invalid shares, the degree of the interpolating polynomial of these n shares is more than $t-1$ with very high probability. In other words, these n shares are most likely to be not strong t-consistent.

- Method for Detecting Cheaters: If there are more than t shares in Shamir's (t, n) secret sharing scheme and all shares are valid, all shares must be strong t-consistent. Cheater detection is determined by checking the property of strong t-consistency of all shares.
- Method for Identifying Cheaters: If there are n (i.e., $n > t$, the threshold) shares in the secret reconstruction and there have some invalid shares, the reconstructed secrets must be inconsistent. This is because any t shares can construct a secret and there are $\binom{n}{t}$ different combinations. Any t shares including some invalid shares is very likely to reconstruct a different secret from the true secret reconstruct based on all valid shares. After cheaters being detected, if the true secret is the majority of reconstructed secrets, we can use

the majority voting mechanism to identify fake shares. The cheater identification method needs to figure out the majority of the reconstructed secrets first. A set, A, consisting of t valid shares is identified. Then, cheaters (i.e., having fake shares) can be identified one at a time by computing the reconstructed secret using shares in A and the testing share.

The primary advantage of Harn and Lin's algorithm is its simplicity. Shamir's (t, n) secret sharing scheme is capable to detect and identify cheaters without any modification. In [7], it also investigates the bounds of detection and identification which are functions of the threshold, the number of cheaters, and the number of redundant shares in the secret reconstruction. Interest readers can refer to the original paper.

Remark 1. As pointed out in [7], the computational complexity of method to detect cheaters is $O(1)$ and the complexity to identify cheaters is $O(j!)$, where j is the number of shares in the secret reconstruction. The method of cheater identification only works properly when there is small number of shares in the secret reconstruction.

3 Proposed Algorithm

From now on, we assume that there are t, where $t \leq n$, shareholders with their shares $\{(x_1, f(x_1)), (x_2, f(x_2)), \ldots, (x_t, f(x_t))\}$, obtained from a trusted dealer in Shamir's (t, n) secret sharing scheme want to reconstruct the secret.

The basic idea of our approach is to adopt the threshold changeable secret sharing (TCSS) which shareholders work together to change the threshold t into a new threshold t' and generate new shares of a (t', n) secret sharing; while at the same time, maintain the original secret. Since $t' < t$, there has enough redundant shares in the secret reconstruction to detect and identify cheaters; while at the same time, keep the same secret. The new shares of the (t', t') secret sharing scheme are generated and are used to reconstruct the secret. In our proposed algorithm, each shareholder M_i acts like a dealer to select a random $(t'-1)$-th degree polynomial $f_i(x)$ with the constant term $f_i(0) = f(x_i) \prod_{j=1, j\neq i}^{t} \frac{-x_j}{x_i - x_j} \pmod{p}$. Then, each shareholder M_i computes sub-shares $f_i(x)$ for other shareholders. After receiving all shares from other shareholders, each shareholder releases the sum of all sub-shares which is the share of sum of polynomials as $F(x) = \sum_{r=1}^{t} f_r(x) \pmod{p}$. The interpolation of all released sums can construct the polynomial $F(x)$ with constant term $F(0) = s$. The TCSS scheme in this algorithm is similar to the strong (n, t, n) verifiable secret sharing scheme proposed in [8]. However, in current application, there are t shareholders working together to change the threshold t into a new threshold t' and generate new shares. Thus, it is a (t, t', t) verifiable secret sharing scheme. In addition, these new shares can be verified without revealing the secret and new shares. We will give detail discussions in the extended version of this paper.

Scheme 2: Secret reconstruction algorithm

Step 1. For each shareholder M_i, uses his share $f(x_i)$ obtained from the dealer to compute $y'_i = f(x_i)\prod_{j=1,j\neq i}^{i} \frac{-x_i}{x_i-x_j} \pmod p$ and selects a random polynomial $f_i(x)$ with $(t'-1)$-th degree satisfying $f_i(0) = y'_i$. Then, shareholder M_i computes sub-shares, $f_i(x_j)$, for all other shareholders, M_j, for $j = 1, 2, \ldots, t$, $j \neq i$, and sends each sub-share $f_i(x_j)$ to shareholder M_j secretly. Shareholder M_i computes and keeps a self-generated sub-share $f_i(x_i)$. By the end of this step, every shareholder receives $t-1$ sub-shares from other shareholders.

Step 2. For each shareholder M_i, after receiving all sub-shares, $f_r(x_i)$, for $r = 1, 2, \ldots, t$, computes $z_i = \sum_{j=1}^{t} f_j(x_i) \pmod p$. z_i is the new share. In Theorem 1, we will prove that the threshold of z_i, for $i = 1, 2, \ldots, j$, is t'. z_i is t'. In the extended version of this paper, we will describe complete procedures to verify these new shares.

Step 3. With knowledge of z_i, for $i = 1, 2, \ldots, t$, shareholders can follow Harn and Lin's algorithm [7] to detect and identify cheaters. If there is no cheater, the secret s can be computed following Lagrange interpolating formula.

Theorem 1. *If shareholders act honestly and present valid shares in above algorithm, the threshold of z_i is t', and the secret s can be recovered successfully following Lagrange interpolating formula.*

Proof. If shareholders act honestly in the algorithm, each new share z_i is the additive sum of sub-shares of random polynomials $f_i(x)$, for $i = 1, 2, \ldots, t$, selected by shareholders. According to the property of secret sharing homomorphisms, z_i is the share of polynomial $F(x) = \sum_{r=1}^{t} f_r(x) \pmod p$. It is obvious that the degree of polynomial $F(x)$ is $t'-1$. Thus, the threshold of z_i, for $i = 1, 2, \ldots, t$, is t'. In addition, if each shareholder owns a valid share in Step 1, the random polynomial $f_i(x)$ selected by shareholder M_i satisfies $f_i(0) = y'_i = f(x_i)\prod_{j=1,j\neq i}^{i} \frac{-x_i}{x_i-x_j} \pmod p$. Knowing z_i, for $i = 1, 2, \ldots, t$, the secret s can be recovered since the polynomial $F(x)$ satisfies $F(0) = \sum_{i=1}^{t} f_j(0) \pmod p = \sum_{i=1}^{t} f(x_i)\prod_{j=1,j\neq i}^{t} \frac{-x_i}{x_i-x_j} \pmod p = s$. However, if there are some invalid shares, the secret s cannot be computed from the released new shares. □

Remark 2. Since the threshold of the new shares z_i is t', there are $t-t'$ redundant shares in above algorithm. In the following, we will discuss how to choose the new threshold t' in order to detect and identify cheaters in our proposed secret reconstruction algorithm.

3.1 Selecting t' in Our Design

Harn and Lin [7] have classified three types of attack according to the behavior of attackers; that are, (a) Type 1 attack - attackers present fake shares without any

collaboration; (b) Type 2 attack - shares are released synchronously and colluded attackers modify their shares to fool honest shareholders; and (c) Type 3 attack - shares are released asynchronously and colluded attackers modify their shares to fool honest shareholders. The bounds of detection and identification of cheaters are functions of the threshold, the number of cheaters, and the number of shares in the secret reconstruction. In a recent paper, Ghosting [10] has proposed a *wise cheating attack* on the cheater detection method based on the property of strong t-consistency. New bounds of detection of cheaters can be found. In the following, we list the bounds of detection and identification of cheaters incorporating the attack proposed by Ghosting [10].

Theorem 2. *Under Type 1 attack, Harn-Lin's scheme can successfully detect cheaters if $j \geq t+1$, and identify cheaters if $j - c > t$, where j is the number of shares, t is the threshold and c is the number of cheaters in the secret reconstruction.*

Theorem 3. *Under Type 2 attack, Harn-Lin's scheme can successfully detect cheaters if $j - c \geq t$, and identify cheaters if $\{(c < t) \cap (j - c \geq t+1)\} \cup \{(c \geq t) \cap (j - c > c + t - 1)\}$, where j is the number of shares, t is the threshold and c is the number of cheaters in the secret reconstruction.*

Theorem 4. *Under Type 3 attack, Harn-Lin's scheme can successfully detect cheaters if $j - c \geq t$, and identify cheaters if $\{j \geq t+1\} \cap \{j - c > c + t - 1\}$, where j is the number of shares, t is the threshold and c is the number of cheaters in the secret reconstruction.*

In this paper, we consider the situation when there are exact t shares in the secret reconstruction. In order to create redundant shares to detect and identify cheaters, the proposed secret reconstruction algorithm enables shareholders to work together to change the threshold from its original value t to a new value t' such that there are $t - t'$ redundant shares in the secret reconstruction. New shares of the (t', t') secret sharing scheme are generated and are used in the secret reconstruction.

Let us re-evaluate the upper and lower bounds in terms of the new threshold t'. In above theorems, the symbols, j is the number of participated shares, t is the threshold, and c is the number of cheaters in the secret reconstruction. In our proposed algorithm, the number of participated shares is t and the threshold is t'. From Theorems 2, 3 and 4, we can obtain the following results: (1) Under Type 1 attack, the proposed algorithm can successfully detect cheaters if $t' \leq t - 1$, and identify cheaters if $t' \leq t - c - 1$; (2) Under Type 2 attack, the proposed algorithm can successfully detect cheaters if $t' \leq t - c$, and identify cheaters if $\{c + 1 \leq t' \leq t - c - 1\} \cup \{t' \leq \min\{c, t - 2c\}\}$; (3) Under Type 3 attack, the proposed algorithm can successfully detect cheaters if $t' \leq t - c$, and identify cheaters if $t' \leq \min\{t - 1, t - 2c\}$. We summarize this result in Table 1.

We use the following example to explain how to choose the new threshold t' in our proposed algorithm to meet the requirements of cheater detection and identification. Assume that in Shamir's $(7, 15)$ secret sharing scheme, our proposed secret reconstruction algorithm needs to detect and identify at most two

Table 1. Bounds of the threshold t' when t and c are given

	Detectability	Identifiability
Type 1	$t' \leq t-1$	$t' \leq t-c-1$
Type 2	$t' \leq t-c$	$\{c+1 \leq t' \leq t-c-1\} \cup \{t' \leq \min\{t-1, t-2c\}\}$
Type 3	$t' \leq t-c$	$t' \leq \min\{t-1, t-2c\}$

Table 2. Maximum values of t' for $t = 7, n = 15$ and $c = 2$

	$t'_{\max}$ for detectability	$t'_{\max}$ for identifiability
Type 1	6	4
Type 2	5	4
Type 3	5	3

cheaters. From Table 1, we can compute the maximal values of the new threshold t'. We list the threshold values in Table 2.

4 Conclusion

We propose a generalized cheater detection and identification algorithm for Shamir's (t, n) secret sharing scheme. Our scheme allows shareholders to detect and identify cheaters using their shares only without needing any additional information. When t shareholders need to reconstruct the secret, shareholders work together to change the threshold to a new threshold so redundant shares can be used to detect and identify cheaters. New shares are generated and used in the secret reconstruction. We include discussion on how to choose the new threshold to meet the requirements of cheater detection and identification.

Acknowledgment. This research is in part supported by the National Natural Science Foundation of China under Grant No. 61103247, the Natural Science Foundation of Fujian Province under Grant No. 2011J05147, and the Foundation for Excellent Young Teachers of Fujian Normal University under Grant No. fjsdjk2012049.

References

1. Araki, T.: Efficient (*k*,*n*) Threshold Secret Sharing Schemes Secure Against Cheating from $n-1$ Cheaters. In: Pieprzyk, J., Ghodosi, H., Dawson, E. (eds.) ACISP 2007. LNCS, vol. 4586, pp. 133–142. Springer, Heidelberg (2007)
2. Benaloh, J.C.: Secret Sharing Homomorphisms: Keeping Shares of a Secret Secret. In: Odlyzko, A.M. (ed.) CRYPTO 1986. LNCS, vol. 263, pp. 251–260. Springer, Heidelberg (1987)
3. Blundo, C., De Santis, A., Gargano, L., Vaccaro, U.: Secret Sharing Schemes with Veto Capabilities. In: Cohen, G., Lobstein, A., Zémor, G., Litsyn, S.N. (eds.) Algebraic Coding 1993. LNCS, vol. 781, pp. 82–89. Springer, Heidelberg (1994)

4. Brickell, E.F., Stinson, D.R.: The Detection of Cheaters in Threshold Schemes. In: Goldwasser, S. (ed.) CRYPTO 1988. LNCS, vol. 403, pp. 564–577. Springer, Heidelberg (1990)
5. Carpentieri, M.: A perfect threshold secret sharing scheme to identify cheaters. Designs, Codes and Cryptography 5(3), 183–187 (1995)
6. Carpentieri, M., De Santis, A., Vaccaro, U.: Size of Shares and Probability of Cheating in Threshold Schemes. In: Helleseth, T. (ed.) EUROCRYPT 1993. LNCS, vol. 765, pp. 118–125. Springer, Heidelberg (1994)
7. Harn, L., Lin, C.: Detection and identification of cheaters in (t, n) secret sharing scheme. Designs, Codes and Cryptography 52(1), 15–24 (2009)
8. Harn, L., Lin, C.: Strong (n, t, n) verifiable secret sharing scheme. Information Sciences 180(16), 3059–3064 (2010)
9. He, J., Dawson, E.: Shared secret reconstruction. Designs, Codes and Cryptography 14(3), 221–237 (1998)
10. Ghosting, H.: Comments on Harn-Lin's cheating detection scheme. Designs, Codes and Cryptography 60(1), 63–66 (2011)
11. Kurosawa, K., Obana, S., Ogata, W.: t-Cheater Identifiable (k, n) Threshold Secret Sharing Schemes. In: Coppersmith, D. (ed.) CRYPTO 1995. LNCS, vol. 963, pp. 410–423. Springer, Heidelberg (1995)
12. McEliece, R.J., Sarwate, D.V.: On sharing secrets and Reed-Solomon codes. Communications of the ACM 24(9), 583–584 (1981)
13. Ogata, W., Kurosawa, K., Stinson, D.R.: Optimum secret sharing scheme secure against cheating. SIAM Journal on Discrete Mathematics 20(1), 79–95 (2006)
14. Pieprzyk, J., Zhang, X.-M.: Cheating Prevention in Linear Secret Sharing. In: Batten, L.M., Seberry, J. (eds.) ACISP 2002. LNCS, vol. 2384, pp. 121–135. Springer, Heidelberg (2002)
15. Rabin, T., Ben-Or, M.: Verifiable secret sharing and multiparty protocols with honest majority. In: Proceedings of the 21st Annual ACM Symposium on the Theory of Computing, pp. 73–85 (1989)
16. Shamir, A.: How to share a secret. Communications of the ACM 22(11), 612–613 (1979)
17. Tompa, M., Woll, H.: How to share a secret with cheaters. Journal of Cryptology 1(3), 133–138 (1989)

Cryptanalysis on the User Authentication Scheme with Anonymity

Yung-Cheng Lee

Department of Security Technology and Management, WuFeng University
Minhsiung, Chiayi 62153, Taiwan
yclee@wfu.edu.tw

Abstract. Nowadays, people obtain a variety of services through networks. Many systems provide services without verifying users, but in many applications, the users obtain services only after they are authenticated. Remote user authentication scheme provides the server a convenient way to authenticate users before they are allowed to access database and obtain services. For the sake of security, anonymity is an important requirement for some user authentication schemes. In 2012, Shin et al. proposed a smart card based remote user authentication scheme. Their scheme has merits of providing user anonymity, key agreement, freely updating password and mutual authentication. They also declared that their scheme provides resilience to potential attacks of smart card based authentication schemes. In this article, we show that their scheme cannot resist impersonation attack, denial-of-service attack and guessing attack. Furthermore, the scheme suffers high hash computation overhead and validations steps redundancy.

Keywords: Authentication, Anonymity, Smart Cards.

1 Introduction

Remote user authentication scheme is a widely used mechanism to allow users and servers communications via insecure channel, it is the most common method used to check the validity of the login message and authenticate the users. For security and efficiency consideration, many schemes authenticate users by using the smart cards [2, 4, 6, 7, 9-12, 14, 15, 17].

In 1981, Lamport [11] proposed the first remote password authentication scheme by using smart cards. However, Lamport's scheme has the drawbacks such as high hash overhead and vulnerable to stolen-verifier attack. Many schemes use one-way hash functions and exclusive-or operations to reduce the computing complexity in smart cards [3, 13, 16]. Hwang et al. [6] proposed a smart card based user authentication scheme in 2000. However, their scheme can not withstand masquerade attack. In 2002, Chien et al. [4] presented a scheme with merits of mutual authentication and freely updating password. But Ku et al. [9] showed that Chien et al.'s scheme is vulnerable to the reflection attack and insider attack. Ku et al. also proposed an improved scheme to fix the flaws. However, Yoon et al. [17] indicated that the improved scheme was also susceptible to parallel session attack and presented an improvement scheme.

J.-S. Pan et al. (Eds.): *Advances in Intelligent Systems & Applications*, SIST 21, pp. 33–39.
DOI: 10.1007/978-3-642-35473-1_4

Chien et al. [3] proposed an improved scheme to preserve user anonymity, however, Bindu et al. [1] showed that the scheme is vulnerable to the insider attack and man-in- the-middle attack. Lin et al. [13] presented a strong password authentication protocol with one-way hash function. But the scheme is insufficient of mutual authentication and user anonymity. Juang [7] presents a simple authentication scheme in 2004, but the users cannot change passwords freely and the scheme does not provide mutual authentication. Das et al. [5] and Liao et al. [12] introduced dynamic ID to achieve user's anonymity, but both schemes are vulnerable to insider attacks and neither scheme really provides user anonymity [14]. Khan et al. [8] and Tseng et al. [16] proposed remote authentication schemes to provide user anonymity. However, both schemes require time synchronization to resist replay attack [14].

In 2012, Shin et al. [14] proposed a remote user authentication scheme with merits of mutual authentication and user anonymity. The scheme overcomes the weaknesses of Das et al.'s scheme [5] and Liao et al.'s scheme [12]. However, in this article, we show that Shin et al.'s scheme is vulnerable to impersonation attack, denial-of-service attack and guessing attack.

The remainder of the article is organized as follows. Shin et al.'s smart card based remote user authentication scheme is briefly described in next Section. The security analysis of their scheme is analyzed in Section 3. Finally, we make conclusions.

2 Shin et al.'s Remote User Authentication Scheme

The scheme comprises four phases: registration phase, login phase, key agreement phase and password updating phases as follows.

2.1 Registration Phase

If the legitimate user U_i wants to join the system, U_i performs the following steps.

Step R-1. $U_i \Rightarrow S : \{ID_i, h(PW_i)\}$.

The user U_i chooses his/her identity ID_i and password PW_i and submits $\{ID_i, h(PW_i)\}$ to the server *S* via a secure channel.

Step R-2. The server computes user's TID_i, A_i and B_i.

After receiving $\{ID_i, h(PW_i)\}$, the server obtains the user's transform identity TID_i by $TID_i = h(ID_i \| h(PW_i))$ and computes A_i and B_i by:

$$A_i = h(K_U) \oplus K_S \tag{1}$$

$$B_i = (g^{A_i} \bmod p) \oplus h(PW_i) \tag{2}$$

Where g is a primitive element in Galois field *GF*(*p*), p is a large prime number, K_S is the server's secret key, and K_U is the common key of user for *S*.

Step R-3. $S \Rightarrow U_i$: Smart card.

The server stores $\{TID_i, B_i, h(\cdot), K_U\}$ in a smart card and sends it to the user.

2.2 Login Phase

If the user wants to log into the system, the login steps are as follows.

Step L-1. The user attaches smart card to a card reader and then keys in ID_i and PW_i.

Step L-2. $U_i \rightarrow S : \{DID_i, CTID_i, C_i, k_i\}$.

The smart card generates two nonces n_i and k_i, and computes:

$$CTID_i = TID_i \oplus n_i \tag{3}$$

$$C_i = h(B_i \oplus h((PW_i)) \oplus n_i \tag{4}$$

$$M_i = K_U \bmod k_i \tag{5}$$

$$DID_i = h^{M_i}(TID_i \oplus h(B_i \oplus h(PW_i))) \tag{6}$$

The user sends $\{DID_i, CTID_i, C_i, k_i\}$ along with the login request message to the server. Note that there has typo in Shin et al.'s scheme, DID_i should be computed by $h^{M_i}(TID_i \oplus h(B_i \oplus h(PW_i)))$ rather than by $h^{M_i}(TID_i \oplus B_i \oplus h(PW_i))$.

Step L-3. After receiving $\{DID_i, CTID_i, C_i, k_i\}$, the server computes A_i by:

$$A_i = h(K_U) \oplus K_S \tag{7}$$

Since $C_i = h(B_i \oplus h((PW_i)) \oplus n_i = h(g^{A_i}) \oplus n_i$, the nonce n_i can be recovered by:

$$n_i = C_i \oplus h(g^{A_i}) \tag{8}$$

With n_i and $CTID_i$, the user's transform identity TID_i is obtained by:

$$TID_i = CTID_i \oplus n_i \tag{9}$$

Then *S* checks whether the transform identity TID_i is in the database. If it isn't, the server terminates the connection; otherwise, continue the next steps.

Step L-4. The server authenticates the legitimate user.

The server computes $M_i = K_U \bmod k_i$. Then *S* obtains DID_i' by:

$$DID_i' = h^{M_i}(TID_i \oplus h(g^{A_i})) \tag{10}$$

If $DID_i' = DID_i$, *S* authenticates the user U_i. Otherwise, *S* stops the connection.

Step L-5. $S \rightarrow U_i : \{DID_S, CTID_S\}$.

The server generates a nonce n_S and computes $\{DID_S, CTID_S\}$ by:

$$DID_S = h(DID_i \oplus n_i \oplus n_S) \tag{11}$$

$$CTID_S = CTID_i \oplus n_S \tag{12}$$

The server forwards $\{DID_S, CTID_S\}$ to U_i.

Step L-6. The user U_i authenticates the server *S*.

On receiving $\{DID_S, CTID_S\}$, the user obtains n_S' by:

$$n_S' = CTID_S \oplus CTID_i \tag{13}$$

Thereby, U_i computes DID_S' with:

$$DID_S' = h(DID_i \oplus n_i \oplus n_S') \tag{14}$$

If $DID_S' = DID_S$, the user authenticates the remote server. Otherwise, U_i terminates the login steps.

Step L-7. $U_i \rightarrow S : \{DID_{iS}\}$.

After *S* is authenticated, U_i computes DIS_{iS} and sends it to *S*. Where

$$DID_{iS} = DID_S \oplus n_i \oplus (n_S + 1) \tag{15}$$

Step L-8. The server *S* authenticates the user U_i.

After receiving DIS_{iS}, the server obtains $(n_S + 1)'$ by:

$$(n_S + 1)' = DID_{iS} \oplus DIS_S \oplus n_i \tag{16}$$

The server *S* computes $(n_S + 1)$ and compares it with $(n_S + 1)'$. If $(n_S + 1)' = (n_S + 1)$, mutual authentication is obtained. Otherwise, *S* terminates connection with U_i.

2.3 Key Agreement Phase

After mutual authentication is obtained, the user and the server compute common session key SK_i and SK_S, respectively, by:

$$SK_i = h(B_i \oplus h(PW_i) \oplus n_i \oplus n_S) \tag{17}$$

$$SK_S = h((g^{A_i} \bmod p) \oplus n_i \oplus n_S) \tag{18}$$

The generated common session keys of SK_i and SK_S are the same since $B_i \oplus h(PW_i) = g^{A_i}$.

2.4 Password Updating Phase

When the user wants to change password, the steps are as follows.

Step U-1. $U_i \rightarrow S : \{DID_i, CTID_i, C_i, k_i, \text{Password updating Request}\}$

Similar to the login steps, the user attaches the smart card to a reader and forwards $\{DID_i, CTID_i, C_i, k_i, \text{Password updating Request}\}$ to the server.

Step U-2. The user and the server obtain mutual authentication.

Similar to the steps in the login phase, U_i and S obtain mutual authentication.

Step U-3. $U_i \rightarrow S : \{(E_{SK_i}(TID_i^*)\}$

U_i chooses a new password PW_i^* and the smart card computes new transform identity TID_i^* by $TID_i^* = h(ID_i \| h(PW_i^*))$. Then the smart card encrypts TID_i^* by using the session key SK_i and sends $(E_{SK_i}(TID_i^*)$ to the server.

Step U-4. The server replaces TID_i with TID_i^* in the database.

After receiving $(E_{SK_i}(TID_i^*)$, S decrypts it by using SK_S and replaces TID_i with TID_i^*. Next, S sends response message to U_i.

Step U-5. U_i replaces TID_i and B_i with TID_i^* and B_i^*, respectively.

After receiving the response message from S, U_i computes $B_i^* = B_i \oplus h(PW_i) \oplus h(PW_i^*)$. Then the user replaces the old values TID_i and B_i with TID_i^* and B_i^*, respectively.

3 Security Analysis on Shin et al.'s Scheme

In Shin et al.'s scheme, the smart card computes $DID_i = h^{M_i}(TID_i \oplus h(B_i \oplus h(PW_i)))$ at the login session, where $M_i = K_U \mod k_i$. Thus their scheme suffers high hash overhead if k_i is very large. Moreover, their scheme is vulnerable to the following attacks:

(1) ***Impersonation Attack***

Suppose that an adversary Eve (E, for short) wants to impersonate as the legitimate user U_i to login the system. Firstly, Eve intercepts $CTID_i$ from Step L-2 and $CTID_S$ from Step L-5. Then, with Eq.(12), n_S can be obtain by $n_S = CTID_S \oplus CTID_i$. Next, Eve intercepts DID_S from Step L-5 and DID_{iS} from Step L-7. Then, with Eq.(15), n_i also can be obtain by $n_i = DID_{iS} \oplus DID_S \oplus (n_S + 1)$. By n_i, the user's $h(g^{A_i})$ and TID_i also be obtained with Eq.(8) and Eq.(9). With TID_i and $h(g^{A_i})$, Eve impersonate as the legitimate user U_i with the steps as follows.

Step I-1. $E \rightarrow S : \{DID_i, CTID_i, C_i, k_i\}$

Eve selects two integers for nonces n_i and k_i, and chooses a small integer for M_i. Thereby she computes $\{CTID_i, C_i, DID_i\}$ by $CTID_i = TID_i \oplus n_i$, $C_i = h(g^{A_i}) \oplus n_i$ and $DID_i = h^{M_i}(TID_i \oplus h(g^{A_i}))$. Next, Eve sends $\{DID_i, CTID_i, C_i, k_i\}$ along with the login request message to S.

Step I-2. $S \rightarrow E : \{DID_S, CTID_S\}$.

After receiving $\{DID_i, CTID_i, C_i, k_i\}$, the server computes A_i and obtains $\{n_i, TID_i, M_i\}$ as the steps in login phase. Thereby the server authenticates the legitimate user. Note that $M_i = K_U \bmod k_i$ and Eve doesn't know K_U, so M_i is also unknown by Eve. The probability for Eve to pass the verification is $P = 1/2^{|k_i|}$.

If Eve chooses a very small k_i such that M_i is small enough, then the forwarded DID_i will pass the verification with very high probability. That is, in Step I-1, Eve should choose a very small k_i and selects an integer for M_i, where $M_i < k_i$. If Eve is authenticated, the server generates a nonce n_S, computes $\{DID_S, CTID_S\}$ and sends it to Eve.

Step I-3. $E \rightarrow S : \{DID_{iS}\}$.

After receiving $\{DID_S, CTID_S\}$, Eve obtains n_S by Eq.(13). Then DIS_{iS} can be obtained by Eq.(15). Next, Eve sends DIS_{iS} to the server.

Step I-4. *S* and Eve obtain a common session key.

After receiving $\{DID_S, CTID_S\}$, *S* and U_i obtain mutual authentication and a common session key.

Hereafter, the adversary can successfully to impersonate as a legitimate user to communicate with the server by using the common session key. Thus the Shin et al.'s scheme is vulnerable to the impersonation attack.

(2) ***Guessing Attack***

Similar to the cryptanalysis steps in the impersonation attack, Eve obtains n_S by $n_S = CTID_S \oplus CTID_i$ and knows n_i by $n_i = DID_{iS} \oplus DID_S \oplus (n_S + 1)$. With n_i, the user's transform identity TID_i will be obtained by $TID_i = CTID_i \oplus n_i$. Since $TID_i = h(ID_i \| h(PW_i))$ and user's identity ID_i is public, password PW_i can be easily guessed. Thus Shin et al.'s scheme cannot resist the guessing attack.

(3) ***Denial-of-Service Attack***

In password updating phase, Eve intercepts $(E_{SK_i}(TID_i^*))$ and sends a random message X to the server. After receiving X, the server will decrypted it to Y and replace the old transform identity TID_i with Y, where $Y = D_{SK_S}(X)$. Hereafter, the legitimate cannot login the system for services since $Y \neq TID_i^*$. Thus Shin et al.'s scheme cannot withstand denial-of-service attack.

4 Conclusions

Recently, Shin et al. proposed a remote authentication scheme. In this article, we show that their scheme is vulnerable to impersonation attack, denial-of-service attack and guessing attack. Furthermore, the scheme has drawbacks such as high hash overhead and validations steps redundancy.

Acknowledgment. This work was partial supported by the National Science Council of the Republic of China under the contract number NSC 101-2632-E-274-001-MY3.

References

1. Bindu, C.S., Reddy, P.C.S., Satyanarayana, B.: Improved Remote User Authentication Scheme Preserving User Anonymity. Int. J. of Computer Science and Network Security 8(3), 62–65 (2008)
2. Chang, C.C., Wu, T.C.: Remote Password Authentication with Smart Cards. IEE Proceedings-E138 3, 65–168 (1993)
3. Chien, H.Y., Chen, C.H.: A Remote Authentication Scheme Preserving User Anonymity. In: Proc. of the 19th In. Conference on Advanced Information Networking and Applications, AINA 2005, vol. 2, pp. 245–248 (2005)
4. Chien, H.Y., Jan, J.K., Tseng, Y.M.: An Efficient and Practical Solution to Remote Authentication: Smart Card. Computer Security 4(21), 372–375 (2002)
5. Das, M.L., Saxena, A., Gulati, V.P.: A Dynamic ID-Based Remote User Authentication Scheme. IEEE Trans. Consumer Electronics 50(2), 28–30 (2004)
6. Hwang, M.S., Li, L.H.: A New Remote User Authentication Scheme Using Smart Cards. IEEE Trans. on Consumer Electronics 1(46), 28–30 (2000)
7. Juang, W.S.: Efficient Password Authentication Key Agreement Using Smart Cards. Computer & Security 23, 167–173 (2004)
8. Khan, M.K., Kim, S.K., Alghathbar, K.: Cryptanalysis and Security Enhancement of A More Efficient & Secure Dynamic ID-Based Remote User Authentication Schemes. Computer Communications 34(3), 306–309 (2011)
9. Ku, W.C., Chen, S.M.: Weaknesses and Improvements of an Efficient Password Based Remote User Authentication Scheme Using Smart Cards. IEEE Trans. on Consumer Electronics 50(1), 204–207 (2004)
10. Kumar, M.: A New Secure Remote User Authentication Scheme with Smart Cards. Int. J. of Network Security 11(2), 88–93 (2010)
11. Lamport, L.: Password Authentication with Insecure Communication. Communications of the ACM 24(11), 770–772 (1981)
12. Liao, C.H., Chen, H.C., Wang, C.T.: An Exquisite Mutual Authentication Schemes with Key Agreement Using Smart Card. Informatica 33, 125–132 (2009)
13. Lin, C.W., Tsai, C.S., Hwang, M.S.: A New Strong Password Authentication Scheme Using One-Way Hash Functions. J. of Computer and Systems Sciences International 45(4), 623–626 (2006)
14. Shin, S., Kim, K., Kim, K.-H., Yeh, H.: A Remote User Authentication Scheme with Anonymity for Mobile Devices. International Journal of Advanced Robotic Systems 9, 1–7 (2012)
15. Sun, H.M.: An Efficient Remote User Authentication Scheme Using Smart Cards. IEEE Trans. on Consumer Electronics 4(46), 958–961 (2000)
16. Tseng, H.R., Jan, R.H., Yang, W.: A Bilateral Remote User Authentication Scheme That Preserves User Anonymity. J. of Security and Communication Networks 1(4), 301–308 (2008)
17. Yoon, E.J., Ryu, E.K., Yoo, K.Y.: Further Improvement of an Efficient Password Based Remote User Authentication Scheme Using Smart Cards. IEEE Trans. on Consumer Electronics 50(2), 612–614 (2004)

Deniable Authentication Protocols with Confidentiality and Anonymous Fair Protections

Shin-Jia Hwang, Yun-Hao Sung, and Jen-Fu Chi

Department of Computer Science and Information Engineering,
Tamkang University, Tamsui, New Taipei City, 251, Taiwan, R.O.C.
sjhwang@mail.tku.edu.tw, 697411758@s97.tku.edu.tw,
698410528@s98.tku.edu.tw

Abstract. Hwang and Chao proposed interactive deniable authentication protocols providing anonymity and fair protection both for senders and receivers. However, no non-interactive deniable authentication protocols are proposed to provide anonymity and fair protection both for senders and receivers. A non-interactive deniable authentication protocol with anonymity and fair protection is proposed to improve performance. Moreover, our protocol provides confidentiality but Hwang and Chao's protocol does not.

Keywords: Deniable authentication protocols, promise of digital signatures, signcryption, anonymity, intended receivers, confidentiality.

1 Introduction

Deniability and intended receiver properties are two security requirements of deniable authentication protocols (DAP). Even if the intended receiver reveals some secret information about the received data *m*, no one, expect the designated receiver, can be convinced that the sender sent the data *m*. After the first DAP[1], various DAPs are proposed. Those DAPs are classified into two classes. One is interactive DAPs [1-4] and one is non-interactive DAPs [5-6]. In general, non-interactive DAPs are more efficient than interactive DAPs, by reducing the communication cost [5].

Deniability of DAPs is provided since receivers have the same ability to produce the same authenticator as senders. However, a malicious receiver is able to prejudice sender's benefit by forging a valid authenticator. To remove this injurious problem, Hwang and Ma [7] proposed the first non-interactive DAP with sender protection. The sender protection property means that the sender can convince anyone that the authenticator is sent from him/her. Moreover, Hwang and Ma [8] also proposed a non-interactive DAP with anonymous sender protection to protect senders' identity privacy. To improve the efficiency of Hwang and Ma's DAP, Hwang and Chao [9] proposed a new DAP with anonymous sender protection.

However, only the sender protection [7-9] is not fair to the receivers. To protect both senders' and receivers' benefit and privacy, Hwang and Chao [10] proposed an interactive deniable authentication protocol with anonymous fair protection. To protect the receivers' benefit, in Hwang and Chao's protocol, the sender must also send

J.-S. Pan et al. (Eds.): *Advances in Intelligent Systems & Applications*, SIST 21, pp. 41–51.
DOI: 10.1007/978-3-642-35473-1_5

receiver some evidence that is validated only with the help of the sender. After receiving evidences, the receiver should interact with the sender to validate senders' evidences. To reduce the communication load caused by senders' evidences, our non-interactive protocol are proposed by adopting the concept in Kudla's non-interactive designated verifier (NIDV) proof scheme [11].

However, those protocols [7-10] provide (fair) protection for senders or receivers, without confidentiality. Without confidentiality, these non-interactive DAPs may reveal some sensitive information about senders or receivers since the messages are sent in plaintext. These revelations may damage sender's and receiver's benefit, and even destroy some announced security properties. Thus confidentiality is important for DAPs with senders'/receivers' protection.

To provide confidentiality may use symmetric cryptosystems. Two additional costs should be paid. One is the cost to construct the session keys between senders and receivers. One is the encryption/decryption cost for message. To efficiently provide signing and encryption at the same time, Zheng [12] first proposed the signcryption schemes. However, the signcryption scheme has the non-repudiation property resulting in that signcryption schemes cannot be used directly in DAPs. Thus Hwang and Sung [13] first proposed the promised signcryption scheme to design their non-interactive DAP with confidentiality and anonymous sender protection. However, there is no non-interactive DAP with confidentiality and anonymous sender protection is proposed. Being inspired of the promised signcryption scheme, our non-interactive DAP with confidentiality, anonymity, and fair protection is proposed.

Based on Schnorr signature scheme [14] and its promise [15], and NIDV proof scheme, Section 2 describes our DAP with confidentiality, anonymity, and fair protection. Session 3 is the brief security proof of our DAP. Session 4 gives the security and performance comparison between our protocol and Hwang and Chao's DAP. The last session is our conclusion.

2 Our Deniable Authentication Protocol with Confidentiality and Anonymous Fair Protection (DAP-CAFP)

Our DAP-CAFP has three parties: Sender A, Receiver B, and a trustworthy Judge J. Our DAP-CAFP consists of three phases: Setup, authentication, and clarification phases. A produces the promised signcryptext and the transferring evidence for B in the authentication phase. B proves the message is transferred by A for Judge J in the clarification phase.

Setup Phase

Some system parameters and functions are published in this phase. Two large public primes p and q are first chosen to satisfy $p= 2q$-1. The element g in Z_p^* with order q and the multiplicative cyclic-subgroup $G= <g>$ of Z_p^* of order q are published. The public symmetric-key encryption $E_k(m)$ and decryption function $D_k(m)$ are also published, where m is the message and k is the session key. Four one-way hash functions $H_{q1}(.)$, $H_{q2}(.)$, $H_G(.)$, and $H_l(.)$ are published for all legal users. $H_{q1}(.)$ and $H_{q2}(.)$ map from $\{0,1\}^*$ to Z_q^*, $H_G(.)$ maps from $\{0,1\}^*$ to $G= <g>$, and $H_l(.)$ maps from $\{0,1\}^*$ to

$\{0,1\}^l$, where l is the length of a bit string. Assume each user i has a randomly-chosen private key x_i from Z_q^* and a computed public key $y_i = g^{x_i} \bmod p$.

Authentication Phase

This phase consists of Signcrypt_PGen and Designcrypt_PVerify algorithms. By Signcrypt_PGen, Sender A generates the sender's promised signcryptext (C, V, S), the transferring evidence σ, and the proof (w, r, h, d) of the transferring evidence for B. By Designcrypt_PVerify, the intended receiver decrypts and verifies the promised signcryptext and validates the evidence. The validation of the evidence is only performed by the intended receiver.

Signcrypt_PGen Algorithm

Signcrypt_PGen consists of three major steps. The promised signcryptext is generated in Step 1. The transferring evidence is generated in Step 2. The proof of the transferring evidence is generated in Step 3.

Step 1: Sender A generates of the promised signcryptext (C, V, S) on the message m.

Step 1.1: Choose two random integers R and $k \in Z_q^*$.

Step 1.2: Compute $V = H_{q_1}(g^k \bmod p \| H_G(m) \| R \| y_B)$, $s = k + Vx_A \bmod p$, and $S = g^s \bmod p$, and $K = H_l((y_B)^s \bmod p)$.

Step 1.3: Encrypt m by the symmetric encryption function $C = E_K(m \| R)$.

Step 2: A computes the transferring evidence $\sigma = H_G(m)^{x_A} \bmod p$ for the intended Receiver B.

Step 3: A generates the proof of the transferring evidence σ for Receiver B.

Step 3.1: Choose three random integers w, r, and $t \in Z_q^*$.

Step 3.2: Compute $c = g^w y_B^r \bmod p$, $T = g^t \bmod p$, $M = H_G(m)^t \bmod p$, $h = H_{q_2}(c \| T \| M \| m \| R \| \sigma \| S)$, and $d = t - x_A(h + w) \bmod q$.

Finally, A transmits the promised signcryptext (C, V, S) and the transferring evidence σ with its proof (w, r, h, d) to B.

Designcrypt_PGen

Designcrypt_PGen consists of two steps. To decrypt and verify the promised signcryptext is in Step 1. Step 2 is the confirmation of the evidence σ.

Step 1: B designcrypts and verifies the promised signcryptext.

Step 1.1: Compute $K = H_l(S^{x_B} \bmod p)$.

Step 1.2: Performing the symmetric decryption function $m \| R = D_K(C)$ to gain the message m and the random number R.

Sept 1.3: Verify $V = H_{q_1}(S \times y_A^{-V} \bmod p \| H_G(m) \| R \| y_B)$. If $V = H_{q_1}(S \times y_A^{-V} \bmod p \| H_G(m) \| R \| y_B)$, Receiver B is convinced that the message m is sent by Sender A; otherwise, B rejects the promised signcryptext (C, V, S).

Step 2: B validates the proof of evidences.

Sept 2.1: Compute $c = g^w y_B^r \bmod p$, $T = g^d y_A^{(h+w)} \bmod p$, and $M = g^d y_A^{(h+w)} \bmod p$.

Sept 2.2: Verify $h = H_{q_2}(c \| T \| M \| m \| R \| \sigma \| S)$. If $h = H_{q_2}(c \| T \| M \| m \| R \| \sigma \| S)$, B is convinced that the sender knows the same discrete logarithm of σ and S; otherwise, B rejects the evidence.

Clarification Phase

If A declares that he/she did not transmitted the message m to B, the receiver's benefit is damaged. To protect receiver's benefit, B transmits Judge J the promise of signcryptext (V, S), the hash value $H_G(m)$, and the evidence σ. The clarification procedure between Sender A and Judge J are described below.

Sept 1: J validates (V, S) by $V = H_{q_1}(S \times y_A^{-V} \bmod p \| H_G(m) \| R \| y_B)$.

Step 2: J chooses two random numbers $a, b \in Z_q^*$, computes and sends $t = \sigma^a y_A^b \bmod p$ to A.

Step 3: A computes and returns $d_1 = t^{x_A^{-1}} \bmod p$ to J.

Step 4: After receiving d_1 form A, J computes $d_2 = H_G(m)^a g^b \bmod p$. If $d_2 \equiv d_1 \pmod p$, J stops and confirms that A is the real sender.

Step 5: J chooses two random numbers $a', b' \in Z_q^*$, computes and sends $t' = \sigma^{a'} y_A^{b'} \bmod p$ to A.

Step 6: A computes $d_1' = t^{\alpha x_A^{-1}} \bmod p$ and returns d_1' to J.

Step 7: After receiving d_1' form A, J computes $d_2' = H_G(m)^{a'} g^{b'} \bmod p$ and compares d_1' and d_2'. If $d_2' \equiv d_1' \pmod p$, J confirms that A is the real sender and stops to clarify; otherwise, J continues performing the following steps.

Step 8: If $(d_1 g^{-b})^{a'} \equiv (d_1' g^{-b'})^a \pmod p$, J confirms A is not the real sender, otherwise, J confirms A is.

Only $H_G(m)$ is sent to Judge, so the message confidentiality is still satisfied.

Sender A proves that he/she is the real sender of the promise of signcryptext by publishing s. Then anyone performs the following steps to decrypt the signcryptext to obtain m and transfer signcryptext (C, V, S) to a Schnorr signature (V, s) on m.

Step 1: Compute the session key $K = H_1((y_B)^s \bmod p)$.

Step 2: Perform the decryption $m \| R = D_K(C)$ with the session key K to gain $m \| R$.

Step 3: Check whether or not $V = H_{q_1}(g^s y_A^{-V} \bmod p \| H_G(m) \| R \| y_B)$ holds. If $V = H_{q_1}(g^s y_A^{-V} \bmod p \| H_G(m) \| R \| y_B)$, anyone is convinced that m is really sent by A. Otherwise, A is not the real sender.

3 Security Proof and Analysis

The underlying hard problem assumption is given below.

DDHP[16]**:** Let G be a group of order q, where q is a prime. Let g be a generator of G. Given g and the elements g^a, g^b, and g^t in G, determine whether $g^t = g^{ab}$.

DDHP Assumption**:** No polynomial-time algorithm solving DDHP with non-negligible probability exists.

Our protocol satisfies five properties: Message confidentiality, deniability, intended receiver, anonymity, and fair protection. The indistinguishable game for confidentiality is defined first. Some proofs are skipped in this conference version.

Definition 1 (Indistinguishable Game for Message Confidentiality)

Our DAP-CAFP satisfies indistinguishable security against chosen message attacks, if no polynomial-time adversary T winning the indistinguishable game with a non-negligible probability exists.

This game has two participators: Challenger U and Adversary T. U controls some oracles, Signcrypt_PGen oracle and four hash oracles.

Signcrypt_PGen Oracle S_p

Adversary T chooses a message m to query S_p. Then S_p returns U the corresponding promised signcryptext (C, V, S) and the evidence σ with its proof (w, r, h, d).

Hash Oracle H_V

Oracle S_p queries H_V by giving (g^k mod $p||H_p(m)||R||y_B$) and a digest value V'. H_V first check whether V' is null or not. If V' is null, H_V searches its local record. If ((g^k mod $p||H_p(m)||R||y_B$), V) exists, H_V returns the same digest V; otherwise, H_V returns a random value $V \in Z_q^*$ and saves ((g^k mod $p||H_p(m)||R||y_B$), V) into its local record. If V' is not null, H_V searches the local record first. If ((g^k mod $p||H_p(m)||R||y_B$), V) exists, H_V returns an error message; otherwise, H_V returns the inputted digest value V' and stores ((g^k mod $p||H_p(m)||R||y_B$), V') into its local record.

Hash Oracle H_{key}

Oracle S_p inputs the receiver's public key y_B and s to query H_{key}. H_{key} searches its local record. If a record ((y_B, s), K) exists, H_{key} returns the same value K; otherwise, H_{key} returns a random value $K \in \{0, 1\}^l$ and stores ((y_B, s), K) into its local record.

Hash Oracle H_p

Oracle S_p queries H_p for a message m. For the queried m, H_p returns the same digest X by searching its local record to find (m, X). Otherwise, H_p returns a random value $X \in G$ and saves (m, X) into its local record.

Hash Oracle H_h

Oracle S_p queries H_h by giving (c, T, M), an evidence σ, a message with a random number $m||R$, and a promise S. H_h searches its local record first. If (($c||T||M||m||\sigma||R||S$), h) is found, H_h returns the same h; otherwise, H_h returns a random value $h \in Z_q^*$ and stores (($c||T||M||m||\sigma||R||S$), h) into its local record.

This game consists of setup, probing, challenging and guessing phases.

Setup Phase

U generates all system parameters and the public/private key pairs of Sender A and Receiver B. Then Adversary T is given A's and B's public keys y_A and y_B, and the system parameters.

Probing Phase

T collects some promised signcryptexts (C, V, S) and its evidence σ with proof (w, r, h, d) by choosing a message m to query U. U utilizes the Signcrypt_PGen oracle $S_p(m)$ to return T the promised signcryptext (C, V, S) and its corresponding evidence σ with proof (w, r, h, d).

Challenging and Guessing Phase

T randomly sends two legal messages m_0 and m_1 with the same length to U. U chooses a random bit e and produces the provable promised signcryptext $((C', V', S'), \sigma', (w', r', h', d'))= S_p(m_e)$ with the help of the oracle S_p. U sends the provable promised signcryptext to T as a challenge.

Finally, T outputs a guessing bit e'. If $e'= e$, U returns '1' to show that Adversary T wins the game; otherwise, returns '0'. If T gives the correct e' with probability $1/2+\varepsilon$ and the winning advantage ε is non-negligible, he/she attacks successfully.

Theorem 1 (Message Confidentiality)

Let the symmetric encryption cryptosystem satisfy indistinguishable security against chosen ciphertext attacks (IND-CCA). Our protocol satisfies IND-CCA, if there is no probabilistic polynomial-time algorithm solving the DDHP with a non-negligible probability.

Proof

Let T be a polynomial-time adversary whose goal is to distinguish a message among two message candidates from a signcryptext under chosen message attack in our protocol. Suppose that T wins the indistinguishable game with probability $(1/2)+\varepsilon$, where ε is a non-negligible advantage. By using Adversary T as subroutines, a probabilistic polynomial-time algorithm U exists to solve the DDHP. Suppose that the DDHP instance is ($g^a \bmod p$, $g^b \bmod p$, $g^c \bmod p$).

Setup Phase

U generates Sender A's and Receiver B's public/private key pairs and the system parameters. Then Adversary T is given the system parameters and the public keys $y_A= g^{x_A} \bmod p$ and $y_B= g^b \bmod p$, where x_A is a randomly chosen integer by U.

Probing Phase

T collects some provable promised signcryptext $((C, V, S), \sigma, (w, r, h, d))$ on the legal chosen message m, and querying oracles S_p, H_V, H_{key}, H_p, and H_h. The producing procedure of the provable promised signcryptext by Oracle S_p is described below.

Step 1: Choose five random integers w, r, t, R, and k in Z_q^*.

Step 2: Get $V= H_V(g^k \bmod p||H_p(m)||R||y_B)$ by using the oracle H_p on the input (m, null digest) and then the hash oracle H_V on the input consisting of ($g^k \bmod p||H_p(m)||R||y_B$) and null digest.

Step 3: Compute $s= k+ Vx_A \bmod q$ and $S= g^s \bmod p$.

Step 4: Gain $K= H_{key}((y_B)^s \bmod p)$ by using the hash oracle H_{key}.

Step 5: Perform $C = E_K(m||R)$.

Step 6: Compute $c = g^w y_B{}^r \bmod p$, $\sigma = H_p(m)^{x_A} \bmod p$, $T = g^t \bmod p$, $M = H_p(m)^t \bmod p$, $h = H_h(c||T||M||m||R||\sigma||S)$, and $d = t - x_A(h + w) \bmod q$.

Step 7: Return $((C, V, S), \sigma, (w, r, h, d))$ to T.

Challenging and Guessing Phase

Adversary T sends U two legal messages m_0 and m_1 with the same length. After randomly choosing a bit e, U produces the provable promised signcryptext $((C', V', S'), \sigma', (w', r', h', d'))= S_p(m_e)$ by the following procedure.

Step 1: Let $S' = g^a \bmod p$ and choose a random value $V' \in Z_q^*$.
Step 2: Compute $g^{k'} = S' \times y_A^{-V'} \bmod p$.
Step 3: Choose three random integers w', r', and t' in Z_q^*. Then compute $c' = g^{w'} y_B^{r'} \bmod p$, $\sigma' = H_p(m_e)^{x_A} \bmod p$, $T' = g^{t'} \bmod p$, $M' = H_p(m)^{t'} \bmod p$, $h' = H_h(c'\|T'\|M'\|m_e\|R'\|\sigma'\|S')$, and $d' = t' - x_A(h' + w') \bmod q$.
Step 4: Obtain $V' = H_V(g^{k'} \bmod p \| H_p(m_e) \| R' \| y_B)$ by using the hash oracle H_V on the input consisting $(g^{k'} \bmod p \| H_p(m_e) \| R' \| y_B)$ and the digest value V'.
Step 5: Compute $K' = H_{key}(g^c \bmod p)$ with the help of the hash oracle H_{key}.
Step 6: Perform $C' = E_{K'}(m_e \| R')$.
Step 7: Send $((C', V', S'), \sigma', (w', r', h', d'))$ to the adversary T as a challenge.

On the challenge, T outputs the guessing bit e'. Finally, U returns '1', if $e' = e$ or T outputs nothing after its polynomial-time bound. Otherwise, U returns '0'.

Probability Analysis of *U* Solving DDHP

Notation Pr[*U_Fail*] denotes the failure probability of U solving DDHP. The analysis of the failure probability of U consists two cases. The message sent from sender to receiver consists of two parts. One is the promised signcryptext (C, V, S) and another is the proof $(\sigma, (w, r, h, d))$. The analysis of the promised signcryptext (C, V, S) is given first.

Case 1: $g^c \equiv g^{ab} \pmod p$ and $e' \neq e$.

In this case, U returns the incorrect answer of the yes-instance (g^a, g^b, g^c), where $g^c \equiv g^{ab} \pmod p$. Since T's losing probability Pr[$e' \neq e$] is (1/2)-ε, the failure probability is Pr[$e' \neq e$ and $g^c \equiv g^{ab} \pmod p$]= ((1/2)-ε)/$q$.

Case 2: $g^c \bmod p \neq g^{ab} \bmod p$ and $e' = e$.

Only when the collisions of H_{key} occurs, the encryption key K is correct. Assume H_{key} is an ideal hash function, so the collision probability of H_{key} is $1/2^l$. This case means that U returns the incorrect answer of no-instance (g^a, g^b, g^c) because $g^c \bmod p \neq g^{ab} \bmod p$. T's winning probability Pr[$e' = e$] is (1/2)+ε, so U's failure probability given $g^c \bmod p \neq g^{ab} \bmod p$ and the correct K is Pr[$e' = e$, $g^c \bmod p \neq g^{ab} \bmod p$, and K is correct]= (1/2+ε) $(1/2^l) \times (1\text{-}1/q)$.

So U's failure probability is Pr[*U_Fail*]= $\frac{(\frac{1}{2} - \varepsilon)}{q} + (1/2+\varepsilon) \times (1/2^l) \times (1\text{-}1/q) \leq \frac{1}{2q} + (1/2^l) \cdot \frac{1}{2q} + (1/2^l)$ is negligible, since both q and 2^l are large. So Pr[*U_Fail*] is negligible. Based on DDHP assumption, the confidentiality of our protocol is IND-CCA.

The digest $h' = H_h(c'\|T'\|M'\|m_e\|R'\|\sigma'\|S')$ provides negligible information about the message because h' is also randomized by the secret random number R'. Only the one knowing R' is able to adopt $h' = H_h(c'\|T'\|M'\|m_e\|R'\|\sigma'\|S')$ to distinguish the messages. On the other hand, the ones without the secret random value R' adopt the value h' to distinguish the messages with negligible probability. For the promised signcryptext (C, V, S), five cases are considered one by one without using the value h'.

Lemma 1 shows the promise property of our DAP-CAFP.

***Lemma* 1 (Promise Property):** The promise of Schnorr signature (V, S) on message m provides promise property in our protocol, where $S = g^s \pmod{p}$.

Proof: (This proof is skipped in this version.)
By Lemma 1, the deniability of our protocol is proved in Theorem 2.

***Theorem* 2 (Deniability)**
Our DAP-CAFP satisfies deniability property because both the intended receiver B and the sender A can generate the promised signcryptext (C, V, S) and the evidence σ with the proof (w, r, h, d).

Proof: (This proof is skipped in this version.)

Sender Anonymity
A DAP satisfies the sender anonymity against adaptively chosen message attacks if no probabilistic polynomial-time algorithm wins the sender anonymity game with non-negligible advantage more than 1/2.

Sender Anonymity Game
This game has two participators, an adversary and a challenger, and consists of three phases, Setup, probing, and challenging and guessing phases. In Setup phase, the challenger constructs the system parameters, the hash oracles, the encryption oracle, and two senders' and one receiver's public keys. Adversary knows the public keys and public parameters and functions. In the probing phase, by querying the encryption oracle, the adversary is allowed to choose some legal messages to obtain the promised signcryptexts and the evidences with the proofs that are from someone between the two senders. Finally, the adversary sends the challenger one un-queried message. In the challenging and guessing phase, the challenger first randomly selects one between the two senders. Then the challenger generates the challenge such that the promised signcryptext and the evidence with the proof on the received message are generated on behalf of the selected one. After receiving the challenge, the adversary guesses about who the chosen sender is.

***Theorem 3* (Sender Anonymity):** Except Sender A and the intended receiver B, no one wins the sender anonymity game against adaptively chosen message attacks with non-negligible advantage over 1/2 based on the hardness of DDHP in the random oracle model.

Proof: (The proof is skipped in this version.)

Receiver Anonymity
A DAP satisfies receiver anonymity against adaptively chosen message attacks if no probabilistic polynomial-time algorithm wins the following receiver anonymity game with non-negligible advantage more than 1/2.

Receiver Anonymity Game
This game has two participators, one adversary and one challenger. The game consists of setup, probing, and challenging and guessing phases. In Setup phase, the challenger constructs the system parameters, the hash and encryption oracles, and one sender's and two receivers' public keys. The adversary knows those public keys and public

parameters and functions. In the probing phase, the adversary chooses some legal random messages and queries the encryption oracle to obtain the promised signcryptexts and the evidences with the proofs that are from the sender sending to anyone between two receivers. Finally, the adversary sends the challenger one chosen message. In the challenging and guessing phase, the challenger first randomly chooses one receiver and generates the challenge that is the promised signcryptext and the evidence with the proof on the received message for the chosen receiver. Finally, the adversary guesses about who the receiver is.

***Theorem* 4 (Receiver Anonymity):** Except Sender A and the intended receiver B, no one can win the receiver anonymity game with non-negligible advantage against adaptively chosen message attacks based on the hardness of DDHP in the random oracle model.

Proof(The proof is skipped in this version.)

***Theorem* 5 (Intended Receiver):** The $((C, V, S), \sigma, (w, r, h, d))$ generated by the sender A can be verified only by the intended receiver B based on the hardness of DDHP in the random oracle model.

Proof: (The proof is skipped in this version.)

Fair Protections

Fair protections contain the sender and receiver protection. By the sender protection, Sender A can convince anyone that the message is actually sent by him/her. If A denies that the message is sent from him/her, B owns some evidence to prove that the message is actually from A, with the help of the trusted Judge J.

***Theorem* 6 (Sender Protections):** The sender protection of our protocol is based on the unforgeability of Schnorr signature scheme.

Proof: (The proof is skipped in this version. The proof is based on the results in [17])

***Theorem* 7 (Receiver Protections):** The receiver protection of our protocol is guaranteed by the undeniability of the Chaum and van Antwerpen's undeniable signature scheme.

Proof: (The proof based on the results in [18] is skipped in this version)

4 Comparison and Discussions

Table 1 shows the security property comparison between Hwang and Chao's DAP-AFP and our protocol. Both two protocols satisfy intended receiver, deniability, unforgeability, sender anonymity properties. Furthermore, the two protocols both provide sender and receiver protection. Only our protocol provides confidentiality property to prevent the sensitive information revelation. Moreover, our protocol is no-interactive for receiver protection, so our protocol efficiently provides the receiver protection by reducing communication cost.

Table 1. Security Property Comparison Two DAPs

	Hwang and Chao's DAP-AFP	Our Protocol
Intended Receiver	Yes	Yes
Deniability	Yes	Yes
Unforgeability	Yes	Yes
Sender Anonymity	Yes	Yes
Sender Protection	Yes	Yes
Receiver Protection	Yes(Interactive)	Yes(Non-interactive)
Confidentiality	No	Yes

5 Conclusions

Our non-interactive DAP not only satisfies the basic properties of deniable authentication protocols, but also provides some other useful properties: Confidentiality, sender anonymity, and fair protection. Beside the sender protection part, our protocol always keeps the confidentiality of transmitted message to prevent revealing the sensitive information.

References

1. Dwork, C., Naor, M., Sahai, A.: Concurrent Zero-Knowledge. In: Proc. of 30th ACM STOC 1998, Dallas, TX, USA, pp. 409–418 (1998)
2. Aumann, Y., Rabin, M.: Efficient Deniable Authentication of Long Messages. Presented at International Conference on Theoretical Computer Science in Honor of Professor Manuel Blum's 60th Birthday (1998), http://www.cs.cityu.edu.hk/dept/video.html
3. Deng, X., Lee, C.H., Zhu, H.: Deniable Authentication Protocols. IEE Proceeding-Computers and Digital Techniques 148(2), 101–104 (2001)
4. Fan, L., Xu, C.X., Li, J.H.: Deniable Authentication Protocol Based on Diffie-Hellman Algorithm. Electronics Letters 38(4), 705–706 (2002)
5. Shao, Z.: Efficient Deniable Authentication Protocol Based on Generalized ElGamal Signature Scheme. Computer Standards and Interfaces 26, 449–454 (2004)
6. Wang, B., Song, Z.X.: A Non-Interactive Deniable Authentication Scheme Based on Designated Verifier Proofs. Information Sciences 179, 858–865 (2009)
7. Hwang, S.J., Ma, J.C.: Deniable Authentication Protocols with Sender Protection. In: 2007 National Computer Symposium, NCS 2007, Wufeng, Taiwan, pp. 762–767 (2007)
8. Hwang, S.J., Ma, J.C.: Deniable Authentication Protocols with (Anonymous) Sender Protection. In: 2008 International Computer Symposium, ICS 2008, Tamsui, Taiwan, pp. 412–419 (November 2008)
9. Hwang, S.J., Chao, C.H.: An Efficient Non-Interactive Deniable Authentication Protocol with Anonymous Sender Protection. In: Cryptology and Information Security Conference, Taipei City, Taiwan, R.O.C. (2009)

10. Chao, C.H.: Deniable Authentication Protocols with Anonymous Fair Protections. M.S. thesis, University of Tamkang, Taipei country, Taiwan, R.O.C. (2009)
11. Kudla, C.J.: Special Signature Scheme and Key Agreement Protocols. Ph.D. dissertation, Royal Holloway, University of London, Egham, Surrey, England (2006)
12. Zheng, Y.: Digital Signcryption or How to Achieve Cost (Signature & Encryption) << Cost(Signature) + Cost(Encryption). In: Kaliski Jr., B.S. (ed.) CRYPTO 1997. LNCS, vol. 1294, pp. 165–179. Springer, Heidelberg (1997)
13. Hwang, S.-J., Sung, Y.-H.: Confidential Deniable Authentication Using Promised Signcryption. Journal of Systems and Software 84(10), 1652–1659 (2011)
14. Schnorr, C.-P.: Efficient Identification and Signatures for Smart Cards. In: Brassard, G. (ed.) CRYPTO 1989. LNCS, vol. 435, pp. 239–252. Springer, Heidelberg (1990)
15. Nguyen, K.: Asymmetric Concurrent Signatures. In: Qing, S., Mao, W., López, J., Wang, G. (eds.) ICICS 2005. LNCS, vol. 3783, pp. 181–193. Springer, Heidelberg (2005)
16. Diffie, W., Hellman, M.E.: New Directions in Cryptography. IEEE Transactions on Information Theory 22(6), 644–654 (1976)
17. Pointcheval, D., Stern, J.: Security Arguments for Digital Signatures and Blind Signatures*. Journal of Cryptology 13(3), 361–396 (2000)
18. Chaum, D., van Antwerpen, H.: Undeniable Signatures. In: Brassard, G. (ed.) CRYPTO 1989. LNCS, vol. 435, pp. 212–216. Springer, Heidelberg (1990)

A Novel Authentication Scheme Based on Torus Automorphism for Smart Card

Chin-Chen Chang[1,2], Qian Mao[2,3,*], and Hsiao-Ling Wu[1]

[1] Department of Information Engineering and Computer Science, Feng Chia University, No. 100, Wenhwa Rd., Seatwen, Taichung, 40724, Taiwan
{alan3c,wuhsiaoling590}@gmail.com
[2] Department of Computer Science and Information Engineering, Asia University, No. 500, Lioufeng Rd., Wufeng, Taichung, 41354, Taiwan
maoqiansh@gmail.com
[3] Department of Optical-Electrical and Computer Engineering, University of Shanghai for Science and Technology, No. 516, Jungong Rd., Yangpu, Shanghai, 200093, P. R. China

Abstract. A novel authentication scheme for smart card is proposed in this paper. In this scheme, the cardholder's photograph is printed on the card. Meanwhile, the compressed image of the same photograph is encrypted by the torus automorphism. The encrypted image is stored in the smart card. The secret keys for decryption are shared by a trusted third party and the user. Only when all the secret keys are presented can the original image be recovered. The recovered image should be the same as the photograph printed on the card. The combination of the image encryption using torus automorphism and secret sharing provides high security for the proposed authentication scheme.

Keywords: smart card, authentication, image encryption, torus automorphism, secret sharing.

1 Introduction

Smart cards are used extensively, but the threat exists for the card to be stolen and used by unauthorized people. Many user authentication schemes have been proposed to prevent the illegal use of smart cards [1-3]. In many authentication schemes, the cardholder's photograph is printed on the card, and it can be authenticated by other people when the card is used. However, this procedure cannot completely protect the cardholder, because people's faces change with time, the illegal user may resemble the cardholder, or the illegal user may replace the photo by her/his own photograph. All these issues make the authentication unreliable. Zhao and Hsieh proposed an authentication scheme based on image morphing. The photograph of the cardholder was morphed and hid in some cover image [4]. Thongkor and Amornraksa proposed another authentication scheme that hid the cardholder's ID in her/his photograph as a watermark [5]. In addition, many biometric methods also have been used to

* Corresponding author.

J.-S. Pan et al. (Eds.): *Advances in Intelligent Systems & Applications*, SIST 21, pp. 53–60.
DOI: 10.1007/978-3-642-35473-1_6

authenticate smart cards [6, 7]. All these authentication schemes improved the security of smart card.

Image encryption encrypts images by making them chaotic [8-10], which can also provide high security for smart cards. Torus automorphism is a dynamic system that can be used in image encryption, providing a high level of chaos [11]. Images scrambled by torus automorphism have high levels of chaos, and a certain number of the permutations from the original image can recover it [12, 13]. An image copyright protection scheme that uses torus automorphism has been proposed, and it provided good protection and a high-quality cover image [14].

In this paper, we proposed a novel authentication scheme that uses image encryption and secret sharing. The combination of these two methods achieved high security for the authentication. Section 2 presents some important theorems for our scheme, and the novel authentication scheme is proposed in Section 3. The security of the proposed scheme is analyzed in Section 4, and our conclusions are presented in Section 5.

2 Torus Automorphism for Image Encryption

The two-dimensional automorphism $\mathbb{F}_N$ of group G_N, denoted as $\mathbb{F}_N : G_N \to G_N$, where $G_N = \{0,1,\cdots,N-1\}\times\{0,1,\cdots,N-1\}$, is defined by the following map:

$$\mathbb{F}_N : X^{(n)} = A \cdot X^{(n-1)} = A^n \cdot X^{(0)} \Rightarrow \begin{bmatrix} x^{(n)} \\ y^{(n)} \end{bmatrix} = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}^n \cdot \begin{bmatrix} x^{(0)} \\ y^{(0)} \end{bmatrix} \mod N, \quad (1)$$

where $X^{(0)} = [x^{(0)} \quad y^{(0)}]^T$ is the initial state, $X^{(n)} = [x^{(n)} \quad y^{(n)}]^T$ is the nth state, and $X^{(0)}, X^{(n)} \in G_N$. In (1), $a_{ij} \in Z$ $(i, j = 1,2)$, $\det(A) = 1$, and the eigenvalues λ_1 and λ_2 of matrix A satisfy $\lambda_{1,2} \notin \{-1,0,1\}$. The parameter $r = a_{11} + a_{22}$ is defined as the trace of matrix A. Percival and Vivaldi proved that when $r^2 > 4$, the torus automorphism $\mathbb{F}_N$ has strong chaos [11].

For the torus automorphism $\mathbb{F}_N$, the iterations from the initial state form a set of orbits $\mathcal{O}(X) = \{X^{(0)}, X^{(1)}, X^{(2)}, \ldots\}$ that is periodic. That is to say, there exists an integer R such that $X^{(0)} = X^{(R)}$. The period R is defined as the recurrence time of the torus automorphism.

Since the matrix A in (1) is restricted by the conditions $\det(A) = 1$ and its trace t, the torus automorphism $\mathbb{F}_N$ is actually a two-parameter map. Therefore, (1) can be generalized in the following form [12]:

$$\mathbb{F}_N: \ X^{(n)} = A^n \cdot X^{(0)} \Rightarrow \begin{bmatrix} x^{(n)} \\ y^{(n)} \end{bmatrix} = \begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix}^n \cdot \begin{bmatrix} x^{(0)} \\ y^{(0)} \end{bmatrix} \mod N, \qquad (2)$$

where $a, b \in Z$. The recurrence time R of $\mathbb{F}_N$ depends on the values of a, b, and N. We can prove that the two different scrambling matrices,

$$A_1 = \begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix} \text{ and } A_2 = \begin{bmatrix} 1 & a+N \\ b+N & (a+N)(b+N)+1 \end{bmatrix}$$

lead to the same scrambling result, where N is the modulus in (1).
Prove:

$$\begin{bmatrix} x^{(n)} \\ y^{(n)} \end{bmatrix} = A_1 \cdot \begin{bmatrix} x^{(n-1)} \\ y^{(n-1)} \end{bmatrix} = \begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix} \cdot \begin{bmatrix} x^{(n-1)} \\ y^{(n-1)} \end{bmatrix} = \begin{bmatrix} x^{(n-1)} + ay^{(n-1)} \\ bx^{(n-1)} + aby^{(n-1)} + y^{(n-1)} \end{bmatrix} \mod N$$

$$\begin{bmatrix} x^{(n)} \\ y^{(n)} \end{bmatrix} = A_2 \cdot \begin{bmatrix} x^{(n-1)} \\ y^{(n-1)} \end{bmatrix} = \begin{bmatrix} 1 & a+N \\ b+N & (a+N)(b+N)+1 \end{bmatrix} \cdot \begin{bmatrix} x^{(n-1)} \\ y^{(n-1)} \end{bmatrix}$$

$$= \begin{bmatrix} x^{(n-1)} + ay^{(n-1)} + Ny^{(n-1)} \\ bx^{(n-1)} + Nx^{(n-1)} + aby^{(n-1)} + N(a+b)y^{(n-1)} + N^2 y^{(n-1)} + y^{(n-1)} \end{bmatrix}$$

$$= \begin{bmatrix} x^{(n-1)} + ay^{(n-1)} \\ bx^{(n-1)} + aby^{(n-1)} + y^{(n-1)} \end{bmatrix} \mod N$$

The recurrence time R of $\mathbb{F}_N$ can be found by simulations. The following table gives some examples. We see that the values of a and b in A_1 and A_2 are periodic with 128, therefore, when $N = 128$, A_1 and A_2 lead to the same recurrence time, as do A_3 and A_4.

Table 1. Examples of Torus Automorphism

Matrix A	Modulus N	Recurrence Time R
$A_1 = \begin{bmatrix} 1 & 7 \\ 10 & 71 \end{bmatrix}$	128	32
$A_2 = \begin{bmatrix} 1 & 135 \\ 138 & 18631 \end{bmatrix}$	128	32

Table 1. (*continued*)

$A_3 = \begin{bmatrix} 1 & 3 \\ 4 & 13 \end{bmatrix}$	64	64
$A_4 = \begin{bmatrix} 1 & 67 \\ 68 & 4557 \end{bmatrix}$	64	64

3 Proposed Card-User Authentication

The structure of our proposed authentication scheme is shown in Fig. 1. First, a trusted third party, such as a bank, accepts a user's registration and then builds a smart card for the user. A photograph of the cardholder is printed on the card, while an encrypted image of the same photograph is stored in the card. When the smart card is used, the terminal, which may be in a shop or another place of business, reads the encrypted information and decrypts it. The secret key is shared by the bank and the cardholder. If the right keys are provided, the secret image will be decrypted correctly, which should look the same as the photograph printed on the card. By this means, the legality of the user is authenticated.

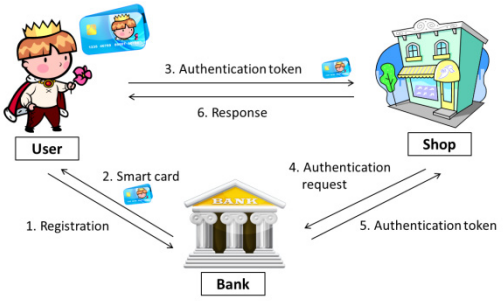

Fig. 1. Framework of the Proposed Authentication System

We assume that the original photograph is a gray image with a size of $N \times N$ and assume that the pixels' gray values vary from 0 to 255, then each pixel can be denoted as an eight-bit byte. Take the limited storage capacity of a smart card into consideration. There are only m ($m \le 8$) bits to represent each pixel's gray value in secret image $I^{(0)}$.

After that, the two-dimensional torus automorphism is used to encrypt the image. Assume that the map of the torus automorphism $\mathbb{F}_N$ is shown as (2) and that the recurrence time is R. Then, after n ($n < R$) iterations from the original image $I^{(0)}$, an arbitrary pixel with coordinates $[x^{(0)} \quad y^{(0)}]$ in $I^{(0)}$ is permutated to a new location with coordinates $[x^{(n)} \quad y^{(n)}]$ by (2). This permutation leads to an image, $I^{(n)}$, that

is strongly chaotic. Since $\{I^{(0)}, I^{(1)}, ..., I^{(n)}, ..., I^{(R)}\}$ is a torus automorphism system with recurrence time R, another $n' = R - n$ iterations from $I^{(n)}$ will recover the original image. That is to say $I^{(0)} = I^{(R)}$. Therefore, the decryption algorithm is shown as the following:

$$\begin{bmatrix} x^{(R)} \\ y^{(R)} \end{bmatrix} = A^{n'} \cdot \begin{bmatrix} x^{(n)} \\ y^{(n)} \end{bmatrix} \mod N, \quad x^{(R)}, y^{(R)}, x^{(n)}, y^{(n)} \in [1, N], \tag{3}$$

where $\begin{bmatrix} x^{(R)} & y^{(R)} \end{bmatrix} = \begin{bmatrix} x^{(0)} & y^{(0)} \end{bmatrix}$ if $n' = R - n$ and if A is same as that in (2). By this means, the original secret image is recovered.

Therefore, we use (2) to encrypt the original image $I^{(0)}$, and we use (3) to get the decrypted image $I^{(R)}$. To make $I^{(0)} = I^{(R)}$, both of the following requirements must be satisfied:

- The same matrix A must be used in encryption and decryption.
- The sum of the iterations in encryption and decryption should be the recurrence time R, *i. e.*, $n + n' = R$.

If either one of the requirements is not satisfied, the decrypted image is chaotic. An example is given in the following. The size of the original photo is 128×128 pixels. The scrambling matrix is A_1, and the recurrence time is 32, as shown in Table 1. Fig. 2 shows the experimental results. In this figure, (a) is the original image, (b) is same as (a) except that there are only four highest bits to represent each pixel, and (c), (d), (e), and (f) are scrambled images with 1, 9, 19, and 32 iterations from (b), respectively. The Peak Signal-to-Noise Ratio (PSNR) between (a) and (b) is 31.7 dB. The loss of image quality is due to the lack of the four lowest bits of each pixel. The PSNRs of (c), (d), (e), and (f) between (b) are 9.2 dB, 9.2 dB, 9.2 dB, and 90.3 dB, respectively. In fact, (f) is totally the same as (b), since 32 iterations from (b) can recover itself. And the intermediate images, which are (c), (d), and (e), are totally chaotic images.

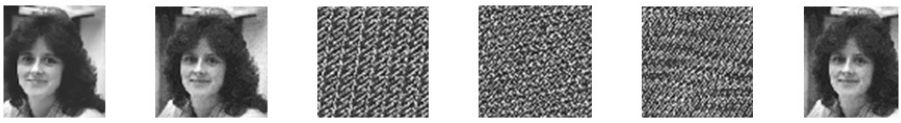

Fig. 2. Experimental Results of Image Encryption Using Torus Automorphism

Therefore, parameters a, b, and n' are crucial for successful decryption. In order to provide high security for the smart card, the three parameters must be kept safely. Therefore, a secret sharing algorithm is used in our scheme.

The t-out-of-k secret sharing scheme was proposed by Shamir [13]. If a secret message s is to be shared by k users, at least t $(2 \le t \le k)$ of whom can recover s cooperatively, then the sharing function $f(z)$ is:

$$f(z) = s + c_1 z + c_2 z^2 + ... + c_{t-1} z^{t-1}, \text{ where } z \in Z, \tag{4}$$

and c_1, c_2, ⋯, c_{t-1} are random numbers excepting 0. This function provides a point $\left(x_i, f(x_i)\right)$ $(1 \le i \le k)$ for the i^{th} user. And t of such points can solve (4), by which the message s can be recovered.

In order to protect a, b, and n', our secret sharing function is designed as follows:

$$f(z) = a + bz + n' z^2, \tag{5}$$

where a and b are parameters in matrix A in (2), and n' is the number of iterations for decryption. If three random numbers z_1, z_2, and z_3 ($z_1, z_2, z_3 \in Z$ and $z_1 \neq z_2 \neq z_3$) are chosen, then three points, $\left(z_1, f(z_1)\right)$, $\left(z_2, f(z_2)\right)$, and $\left(z_3, f(z_3)\right)$ can be computed by (5). The first point is kept secretly by the bank, and the second and the third points are kept secretly by the cardholder. When authentication occurs, the terminal gets the three points, one from the bank and two from the user, and then it can solve (5) and decrypt the secret image using a, b, and n'.

4 Security of the Proposed Scheme

The security of our proposed scheme depends on a, b, and n'. Parameters a and b construct the scrambling matrix A. In order to recover the original image successfully, the values of a and b in the decrypting algorithm must be the same as those in the encrypting algorithm (module N); otherwise, the original image can never be recovered, no matter how many iterations are processed on $I^{(n)}$. Therefore, parameters a and b provide a key space that has the size of N^2.

Parameter n' is the number of iterations for decryption. The initial image $I^{(0)}$ can be recovered if the encrypted image $I^{(n)}$ is iterated n' more times, where $n' = R - n$. Only when the correct number of iterations is executed can the initial image be recovered successfully. Since $1 \le n' < R$, the size of the key space provided by n' is $R - 1$.

Therefore, the key space S of the proposed authentication scheme is:

$$S = (R-1) \cdot N^2. \tag{6}$$

5 Conclusions

The proposed authentication scheme provides high security for smart cards by the combination of image encryption and secret sharing. The encryption method using torus automorphism provides high chaos, and it is difficult for illegal users to pass the authentication process. Our future work may focus on methods to improve the key space of the torus automorphism.

References

1. Sonwanshi, S.S., Ahirwal, R.R., Jain, Y.K.: An Efficient Smart Card Based Remote User Authentication Scheme Using Hash Function. In: Proc. 2012 IEEE Students' Conference on Electrical, Electronics and Computer Science, SCEECS, pp. 1–4 (2012)
2. Sood, S.K., Sarje, A.K., Singh, K.: Smart Card Based Secure Authentication and Key Agreement Protocol. In: Proc. 2010 International Conference on Computer and Communication Technology, ICCCT, pp. 7–14 (2010)
3. Matanovic, G., Mikuc, M.: Implementing Certificate-Based Authentication Protocol on Smart Cards. In: Proc. 2012 Proceedings of the 35th International Convention, MIPRO, pp. 1514–1519 (2012)
4. Zhao, Q.F., Hsieh, C.H.: Card User Authentication Based on Generalized Image Morphing. In: Proc. 2011 3rd International Conference on Awareness Science and Technology, iCAST, pp. 117–122 (2011)
5. Thongkor, K., Amornraksa, T.: Digital Image Watermarking for Photo Authentication in Thai National ID Card. In: Proc. 2012 9th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology, ECTI-CON, pp. 1–4 (2012)
6. Yahaya, Y.H., Isa, M., Aziz, M.I.: Fingerprint Biometrics Authentication on Smart Card. In: Proc. Second International Conference on Computer and Electrical Engineering, ICCEE, pp. 671–673 (2009)
7. Das, A.K.: Analysis and Improvement on an Efficient Biometric-Based Remote User Authentication Scheme Using Smart Cards. IET Information Security 5(3), 145–151 (2011)
8. Luo, X.Z., Fan, J.H., Wu, J.H.: Single-Channel Color Image Encryption Based on the Multiple-Order Discrete Fractional Fourier Transform and Chaotic Scrambling. In: Proc. 2012 International Conference on Information Science and Technology, ICIST, pp. 780–784 (2012)
9. Bhatnagar, G., Wu, Q.M.J.: Chaos-Based Security Solution for Fingerprint Data During Communication and Transmission. IEEE Transactions on Instrumentation and Measurement 61(4), 876–887 (2012)
10. Tao, R., Meng, X.Y., Wang, Y.: Image Encryption with Multiorders of Fractional Fourier Transforms. IEEE Transactions on Information Forensics and Security 5(4), 734–738 (2010)

11. Percival, I., Vivaldi, F.: Arithmetical Properties of Strongly Chaotic Motions. Physica D: Nonlinear Phenomena 25(1-3), 105–130 (1987)
12. Voyatzis, G., Pitas, I.: Chaotic Mixing of Digital Images and Applications to Watermarking. In: Proc. ECMAST 1996, vol. 2, pp. 687–694 (1996)
13. Chen, G., Mao, Y., Chui, C.: A Symmetric Image Encryption Scheme Based on 3D Chaotic Cat Maps. Chaos, Solitons, Fractals 21(3), 749–761 (2004)
14. Chang, C.C., Hsiao, J.Y., Chiang, C.L.: An Image Copyright Protection Scheme Based on Torus Automorphism. In: Proc. the First International Symposium on Cyber Worlds, pp. 217–224 (2002)
15. Shamir, A.: How to share a secret. Communications of the ACM 22(11), 612–613 (1979)

Cryptanalysis of a Provably Secure Certificateless Short Signature Scheme

Yu-Chi Chen[1], Raylin Tso[2], and Gwoboa Horng[1]

[1] Department of Computer Science and Engineering,
National Chung Hsing University, Taiwan
[2] Department of Computer Science, National Chengchi University, Taipei, Taiwan
{s9756034,raylin,gbhorng}@cs.nchu.edu.tw

Abstract. Certificateless public key cryptography, introduced by Al-Riyami and Paterson, simplifies the complex certificate management in PKI-based public key cryptography and solves the key escrow problem of identity-based cryptography. Huang et al. in 2007 showed security models of certificateless signature to simulate possible adversaries according to their attack abilities. Recently, Choi et al. proposed a certificateless short signature scheme. They claimed their scheme to be the only certificateless short signature scheme achieving the strongest security level presented by Huang et al.. They also give their security proofs to support their claim. However, we find that their scheme is not as secure as the authors claimed. In this paper, we give comments on the paper of Choi et al. including the cryptanalysis of their scheme and the weakness of the security proof.

Keywords: certificateless cryptography, certificateless signature, cryptanalysis, security models, short signature.

1 Introduction

Certificates of public keys must be fully managed and maintained by a trusted certificate authority (CA) in conventional public key infrastructure. CA plays an important role of authenticating the public keys. However, with development of wireless networks such as ad hoc networks, communication cost is required to decrease between users and CA. A straightforward solution is a cryptsystem which does not adopt CA. Therefore, both of identity-based public key cryptography (ID-PKC) [11] and certificateless public key cryptography (CL-PKC) [1] are developed without the trusted CA to manage certificates. Simultaneously, lower communication costs comparing with those of traditional cyptsystems are also achieved since a certificate is not required to be send along with a public key. Technically, ID-PCK and CL-PKC only depend on a trusted entity to generate keys. One of the security issues of ID-PKC is the *key escrow* problem in which the private key generator, the trusted entity in ID-PKC, has every user's secret key. However, the core of CL-PKC is the key generation center (KGC) which cannot have the user's actual secret key. The KGC only owns user's *partial secret*

J.-S. Pan et al. (Eds.): *Advances in Intelligent Systems & Applications*, SIST 21, pp. 61–68.
DOI: 10.1007/978-3-642-35473-1_7

key, which is the most different property from ID-PKC. As a result, CL-PKC is one of the most dependable methods to avoid the key escrow problem in practice.

Certificateless public key cryptography has attracted significant research attention, since it was first introduced by Al-Riyami and Paterson in 2003. Certificateless signature (CLS) therefore becomes popular for a decade [3,4,5,8,15]. Existential unforgeability is an important issue when designing a provably secure CLS scheme. As well-known, there are two types of adversaries in CLS: the first one is referred to as the Type I adversary acting as an outside attacker, and the second one is referred to as the Type II adversary acting as the curious KGC. Type I adversary can replace any user's public key, but it cannot access the system master key which is generated and held by the KGC. Type II adversary holds the system master key, but it cannot replace public keys of users.

Taking the security of CLS into consideration, the paper of Huang et al. [9] (the full version [10]) discuss the security models of CLS schemes in details. Adversaries are classified into Normal, Strong, and Super adversaries which are ordered by their attack abilities. Among them, the super Type I and II adversaries are more powerful than others respectively.

On the other hand, Boneh et al. [2] introduced the concept of short signatures in 2001, which are useful for systems with low bandwidth and/or low computation power. Inheriting the advantages of both certificateless cryptography and short signatures, certificateless short signatures are introduced and have come into limelight in recent years [5,6,7,13,14]. However, Shim [12] presented an attack which is performed by the Strong or Super Type I adversary and claimed that to design a secure short CLS schemes withstand the attack is an open problem. Recently, Choi et al. [5] proposed a CLS scheme and proved their scheme to be secure against both of the super Type I and II adversaries as the strongest security level.

In this paper, we find Choi et al.'s CLS scheme is not as secure as they proved. We thus cryptanalysis this scheme and indicate the weakness of the security proof. Choi et al.'s scheme is insecure against the Super or Strong Type I adversary in our analysis. Actually, there are some loopholes in the security proof, which causes that the proof seems correct but actually not.

The rest of this paper is organized as follows. We briefly describe the definition and security model of CLS in Section 2. We then review an efficient certificateless short signature, proposed by Choi et al. [5], in Section 3. We show the cryptanalysis of this scheme and point out the weakness of the security analysis in Section 4. Finally, the conclusions of this paper are given in Section 5.

2 Certificateless Signature (CLS)

2.1 Definition of CLS

A certificateless signature scheme involves three entities, the KGC, a user/signer, and a verifier. Generally, it consists of the following algorithms: Setup, Partial-Secret-Key-Extract, Set-Secret-Value, Set-Secret-Key, Set-Public-Key, CL-Sign, and CL-Verify:

- Setup: This algorithm, run by the KGC, takes a security parameter as an input, and then returns master-key and system parameter, params.
- Partial-Secret-Key-Extract: This algorithm, run by the KGC, takes params, master-key and a user's identity ID as inputs. It generates a partial-secret-key D_{ID}, and sends it to the user via a secure channel.
- Set-Secret-Value: This algorithm, run by a user, returns a secret value, r_{ID}.
- Set-Secret-Key: This algorithm, run by a user, takes the user's partial-secret-key D_{ID} and the secret value r_{ID} as inputs, then returns the user's full secret key.
- Set-Public-Key: This algorithm, run by a user, takes params and the user's full secret key as inputs, and returns a public key pk_{ID} for the user.
- CL-Sign: This algorithm, run by a signer/user, takes params, a message m, and the user's full secret key as inputs. It then generates σ as the signature for the message m.
- CL-Verify: This algorithm, run by a verifier, takes params, a public key pk_{ID}, a message m, a user's identity ID, and a signature σ as inputs. It returns 1 as the verifier accepts σ if σ is the signature of the message m, the public key pk_{ID}, and the user with identity ID. It returns 0 if not.

2.2 Security Model of CLS

For security of CLS, there are several adversaries which act as different roles. We usually assume that Type I adversary is an outsider and Type II adversary is the curious KGC. Both of their goals are to generate a forged signature existentially. Nevertheless, Huang et al. [10] classified the Type I and II adversaries into three levels based on their different abilities: Normal, Strong, and Super adversaries respectively. Since we want to show the security flaw of Choi et al. 's scheme[5] against Strong and Super Type I adversaries, in what follows, we only present Game Strong I which modelling the Strong Type I adversary and Game Super I which modelling the Super Type I adversary.[1]

Game Strong I. An adversary $\mathcal{A}$ interacts with a challenger $\mathcal{C}$. $\mathcal{A}$ acts as an outsider and it can replace any public key.

Setup: The challenger $\mathcal{C}$ runs Setup to generate the system parameters and sends them to $\mathcal{A}$.

Attack: $\mathcal{A}$ can query (1) the public key of identity ID, (2) the secret value of ID, (3) the partial-secret-key of ID, and (4) the signature of (m, ID, r_{ID}) where r_{ID} is a secret value. Moreover, $\mathcal{A}$ also can replace a public key with a new one, pk'_{ID}.

Forgery: $\mathcal{A}$ outputs a forged signature σ^* of (m^*, ID^*, r_{ID^*}).

$\mathcal{A}$ wins this game if and only if the following conditions hold.

[1] We will not present Game Normal I or any Game II modelling the normal Type I adversary or the Type II adversary, since these are not the major point discussed by this paper. However, readers can refer to the paper by Huang et al. [10] for more details.