Lightweight Certificateless Two-Factor Authentication Protocol Using Smart Cards

Wenying Zheng[1], Ziyuan Gui[2], Dengzhi Liu[2], Xiong Li[3], Bing Chen[1]

[1] College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, China
[2] School of Computer & Software, Nanjing University of Information Science & Technology, China
[3] Hunan University of Science and Technology, China
{zhengwy0501, guizy_nuist, liudzdh}@126.com, lixiongzhq@163.com, cb_china@nuaa.edu.cn

Abstract

User authentication and key agreement in smart cards is a critical issue due to the open and complex wireless communication environment. In order to protect the user's privacy and sensitive data in smart cards, many two-factor authentication protocols have been proposed, yet most of them cannot withstand various attacks. In this paper, we summarize the security requirements for smart cards and propose a secure lightweight certificateless authentication protocol with password change. Moreover, the proposed protocol satisfies anonymity, mutual authentication and session key agreement as well as resists many attacks. The performance analysis demonstrate that the proposed protocol is secure and highly practical.

Keywords: Certificateless authentication, Smart card, Anonymity, Two-factor, Password change

1 Introduction

With the rapid development of e-commerce, e-health and e-government, user authentication has become an essential mechanism to ensure the security of the user's private information. Owing to the high level of portability and simplicity, smart card based password authentication has been widely used in various applications, such as personal financial records, medical records and access control systems [1]. Smart cards have already become an essential part of human life. However, Smart cards authenticate with the server in an open channel, which faces many security threats [2]. Due to the openness of wireless communications, the privacy information of smart card users may be intercepted by the malicious entities, so the smart card and server secure authentication is particularly important [3, 29].

Many password-based authentication protocols have been studied for a long time [4-8], and smart cards have been extensively used for various kinds of daily applications. However, due to the complex environment of the wireless sensor networks and the resource-constrained characteristics of smart cards, these technologies still have many challenges regarding usability [9], privacy [10] and security [11].

According to the above background, we design a lightweight certificateless two-factor authentication protocol to address these issues. The proposed protocol can achieve many security properties in smart cards, such as users' anonymity, mutual authentication, session key agreement, lost-smart-cards attack resistance, reply attack resistance and so on. Our contribution can be summarized as follows: (1) We use certificateless public key cryptography to design the authentication protocol without pairing, which efficiently avoids the problem of certificate storage and distribution as well as key escrow problem. As far as we know, it is the first time to use certificateless public key cryptography in smart cards. (2) We design a mechanism that the user can change the password locally without interacting with the server. Hence, this mechanism economizes the energy consumption. (3) We analyze security properties of the proposed protocol and compare it with the other protocols [12-13] in terms of mutual authentication, anonymity, session key agreement and several attacks resistance.

The rest of the paper is organized as follows: We briefly discuss some related works in Section 2. In Section 3, elliptic curve group, system model and security requirements are presented. In Section 4, Our proposed two-factor authentication protocol is described in detail. In Section 5, we analyze the security properties of the proposed protocol. The performance of our protocol is evaluated in Section 6. We make concluding remarks in Section 7.

2 Related Work

To protect the privacy and sensitive data of users, a great number of two-factor authentication schemes have been proposed for practical applications in the

*Corresponding Author: Bing Chen; E-mail: cb_china@nuaa.edu.cn
DOI: 10.3966/160792642018121907025

recent years.

In 2004, Das et al. present a first ID-based dynamic authentication scheme using smart cards [14]. Their scheme allows the user to change their password freely and does not maintain any verifier table. They assume that the private parameters stored in the smart card cannot be revealed. However, recent researches have demonstrated that the private information stored in smart cards could be extracted by power analysis [15]. Over the last few years, there are many anonymous authentication schemes using dynamic ID have been proposed [16-21].

Fan *et al*. proposed a robust remote authentication scheme with smart cards in 2005 [22]. They claim that their protocol not only achieves the low-computation requirement, but also can resist the replay attack and the offline dictionary attack. However, Fan et al.'s scheme is less efficient than recent schemes based on elliptic curve cryptography. In 2008, Juang et al. proposed a robust and efficient authentication and key agreement scheme [23]. Although Juang et al.'s scheme has many merits, such as low computation and communication cost, no need for any password or verification table in the server and so on. However, Sun et al. found that Juang et al.'s scheme suffers several weaknesses, such as the session-key problem and inability of password change. Hence, they proposed an enhanced authentication scheme [24] to address these problems and maintain the benefits of the original scheme in 2009.

In 2015, Chen et al. used symmetric key techniques to propose a secure user authentication scheme [25], and this scheme can resist lost-smart-card attack. However, we find out Chen et al.'s scheme cannot provide the server impersonation attack resistance and the user anonymity. To address these issues, we propose a lightweight certificateless authentication protocol using smart cards.

3 Preliminaries

In this section, we briefly describe the elliptic curve group and the definition of the computational Diffie-Hellman assumption. We also state the system model and security requirements for the proposed protocol.

3.1 Elliptic Curve Group

In this section, the concept of elliptic curve group will be introduced [26]. The basic definition of computational Diffie-Hellman (CDH) assumption also will be briefly described.

The elliptic curve defined by the equation $y^2 = x^3 + ab + b$ over a prime finite field F_p, where $a, b \in F_q$ and the discriminant $4a^3 = 27b^2 \neq 0 \bmod p$. p and n are two large prime numbers. G is a cyclic additive group with order n consisting of points on F_p and the point at infinity O. The group law is briefly defined as follows. Given two generators $P, Q \in Q$, the sum $P+Q$ can be viewed as the reflected point of R, where R is the intersection between the elliptic curve and the line l. l is determined by P and Q in case $P = Q$. Moreover, large multiples of a point P can be implemented as repeated addition operations: $mP = P + P \ldots\ldots + P$.

Computational Diffie-Hellman (CDH) assumption: Given a tuple $\{P, aP, bP\} \in G$, where $a, b \in Z_q^*$. The CDH problem is to compute the element abP.

3.2 System Model

In this section, we describe the system model of the proposed protocol. The working flow is illustrated in Figure 1. The system model consists of three entities which are the user, the smart card and the server. The user should register the server and preloads some public parameters in advance. The smart card is held by the user to authenticate the server [27].

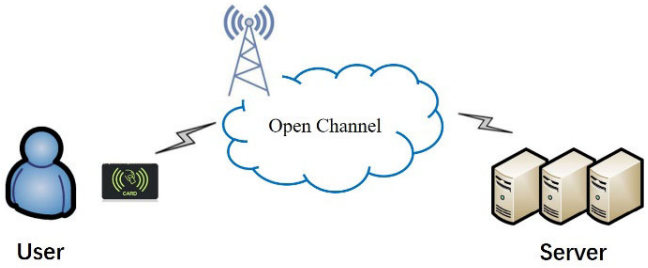


Figure 1. System Model of the Smart Card

The proposed protocol consists of four phases: initialization, registration, login and authentication as well as password change phases. In initialization phase, the server initializes the system and generates his master private key as well as some public parameters. In registration phase, some personal information of the user will be submitted to the server. Afterwards, the server verifies the validity of the user and sends a smart card to the user. The smart card contains the user personal information and some public parameters which will be used for the authentication phase. Note that, the registration phase is operated only once unless the user re-register. After that, the user is able to access the server in authentication phase. Only the user possesses both the correctness password and the valid smart card, then he can be successfully checked by the server. In addition, the authentication phase can be performed as many times as needed. In password change phase, the user can update their password locally. Note that, this phase does not require to interact with the server.

3.3 Security Requirements

In the wireless communication environment, the user use smart cards to authenticate with the server in

the open channel, which faces many security threats. To guarantee secure communications, the authentication phase should resist various attack. According to previous works [28], the authentication protocol for smart cards should reach the following security requirements.

(1) Anonymity: To protect the privacy of the smart card users, anonymity in the proposed protocol means that besides the user himself, no one can link a particular session to a particular identity. The user's real identity cannot be leaked to anyone, including the remote server.

(2) Mutual authentication: The security requirement of mutual authentication is used to confirm the validity of the user and the server, so as to achieve the purpose of identifying and preventing illegal third parties from participating in communications. The smart card and the server can authenticate each other in the authentication phase.

(3) Session key agreement: The requested user with smart cards and the server can share the secure session key after the successful authentication.

(4) Man-in-the-middle attack resistance: Man-in-the-middle attack means that the adversary can intercept messages between the smart card and the server. Afterwards, the adversary replaces their public keys and sends them to the requested entity. The original entities still seem to communicate with each other on the surface. The proposed protocol can resist the man-in-the-middle attack.

(5) Impersonation attack resistance: Impersonation attack means that the adversary can achieve some previous session information and can impersonate other legitimate users or the server.

(6) Offline dictionary attack resistance: This attack means that the adversary can guess the password of users and ceaselessly try to login the smart card, until the adversary finds out the real password of the user. Our protocol can withstand the offline dictionary attack.

(7) Reply attack resistance: The adversary can intercept the authentication messages from the smart card or the server and replay them to each user or the server, in order to achieve the purpose of deceiving the user or the server. The proposed protocol provides reply attack resistance.

(8) Lost-smart-card resistance: To some extent, the smart card symbolizes the legitimacy of the user. If the user lost the smart card and the smart card is obtained by malicious users, maybe the adversary can extract the private information of the user. In the proposed protocol, even if the user lost his smart card, the adversary cannot get any useful information.

(9) Privileged-insider attack Resistance: Privileged-insider attack mainly refers to the registration phase and the server is honest but curious. When the user sends the identity information to the server, the server obtains the user's real identity and leads to the leakage of the user's privacy. In the proposed protocol, the server cannot get the user's real identity, which can resist privileged-insider attack.

4 The Proposed Protocol

In this section, we propose a lightweight certificateless authentication protocol. The proposed protocol contains three entities, namely the user, smart card and the server respectively. In addition, our protocol consists of four phases: Initialization, registration, login and authentication and password change phases.

4.1 Initialization

The server performs the following operations firstly. Given the security parameter l, the server generates a prime q. G is a cyclic group with a prime order q, P is a generator of G. The server chooses a hash fuction: $H:\{0,1\}^* \times G \to Z_q^*$. Afterwards, the server randomly selects $x_s \in Z_q^*$ as the master private key and computes the public key $X_s = X_s P$ accordingly. The server publish the system parameters $param = \{q, P, G, H, X_s\}$ and keeps the master private key x_s secretly.

4.2 Registration

The user U_i with identity ID_i and password PW_i needs to perform the following operations with sever in this phase (shown as Figure 2).

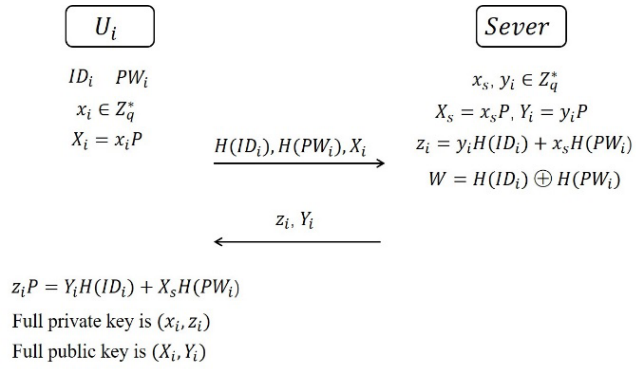


Figure 2. The Registration Phase

(1) U_i randomly picks $x_i \in Z_q^*$ as the partial private key and computes the partial public key $X_i = x_i P$.

(2) U_i computes $H(ID_i)$ and $H(PW_i)$, then sends $H(ID_i)$, $H(PW_i)$ and X_i to the server via a secure channel.

(3) After receiving the message from U_i, the server computes $W = H(ID_i) \oplus H(PW_i)$. After that, the server randomly selects $y_i \in Z_q^*$, and computes the partial public key $Y_i = y_i P$ and the partial private key

$z_i = y_i H(ID_i) + x_s H(PW_i)$ for the user U_i.

(4) The server sends the partial private key z_i and the partial public key Y_i to U_i through a secure channel. The full private key of U_i is (x_i, z_i) and the full public key of U_i is (X_i, Y_i).

(5) The user U_i checks the validity of z_i by verifying whether the formula $z_i = Y_i H(ID_i) + X_s H(PW_i)$. If the formula holds, U_i stores them in his database.

(6) The server writes $\{X_x, Y_i, W, R\}$ into SC and sends SC to U_i. Note that, R is a counter maintained by the smart card and the initial value of R is set to 0. If R reaches a preset threshold value n, then the login process will be terminated.

4.3 Login and Authentication

The user U_i inserts SC into the card reader and inputs his identity ID_i and password PW_i. Upon receiving ID_i and PW_i from U_i, SC computes $W^* = H(ID_i) \oplus H(PW_i)$ and checks whether $W^* = W$. If W^* and W are not equal, the smart card rejects the login request of the user. Once R reaches a preset threshold value n, the smart card will be locked and the user U_i cannot login anymore. If the equation holds, SC and the server performs the following operations (shown as Figure 3).

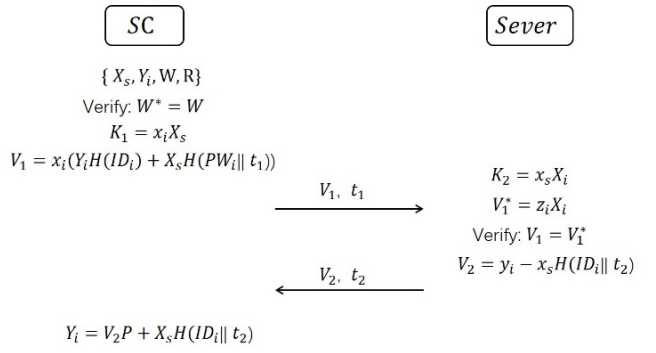


Figure 3. The Authentication Phase

(1) U_i inputs the partial private key x_i into SC and SC computes the session key $K_1 = x_i X_s$.

(2) Afterwards, the smart card SC computes the signature $V_1 = x_i(Y_i H(ID_i) + X_x H(PW_i \| t_1))$, where t_1 is the current timestamp. SC sends V_1 and t_1 to the server.

(3) Upon receving V_1 and t_1, the server checks the freshness of t_1 firstly. If t_1 is valid, the server computes the session key $K = K_2 = K_1 = x_s X_i$ and $V_1^* = z_1 X_1$.

(4) The server checks whether $V_1 = V_1^*$. If the equation holds, the server computes $V_2 = y_i - x_s H(ID_i \| t_2)$. Afterwards, the server sends V_2 and t_2 to SC, where t_2 is the current timestamp. Otherwise, the server abort this login and authentication.

(5) Once receving V_2 and t_2, SC checks the freshness of t_2. If t_2 is valid, SC verity the correctness of the equation $Y_i = V_2 P + X_s H(ID_i \| t_2)$ for the authentication of the server. If the equation holds, their session key is K and the server is legal. Otherwise, SC aborts this session.

4.4 Password Change

When the user U_i wants to change the password PW_i, U_i inserts SC into the card reader and enters the old password PW_i as well as identity ID_i. After that, the smart card performs the following operations.

(1) SC computes $W^{**} = H(ID_i) \oplus H(PW_i)$ and checks the validity of the old password by verifying whether the formula $W^{**} = W$. If the equaltion holds, the smart card requires the user to enter a new password PW^*. Otherwie, SC rejects the requirement of password change.

(2) Upon receiving a new password PW^*, SC computes $W^* = W \oplus H(PW_i) \oplus H(PW^*)$ and replaces W with W^* in the smart card.

5 Security Analysis

In this section, we analyze security properties of the proposed protocol. Our protocol can achieve all the security requirements mentioned in Section 3.

5.1 User Anonymity

The real identity of the requesting user U_i cannot be revealed by anyone from the transmitted messages, including the server. As specified in Subsection 4.2, the user sends $H(ID_i)$ and $H(PW_i)$ to the server. $H(ID_i)$ and $H(PW_i)$ are the hash values of his identity and password. We utilize the irreversibility and collision constraint of the one-way hash function, which means the direction of hash operation is not reversibility and cannot find two different inputs so that outputs is exactly the same. Hence, the adversary cannot acheive the identity of U_i from the transmitted channel. In addition, the server also cannot get the real identity of the user. Therefore, the proposed protocol provides the user anonymity.

5.2 Mutual Authentication

In registration phase of the proposed protocol, when the user U_i sends $H(ID_i)$ and $H(PW_i)$ to the server,

then the server seraches his database with the hash value of the user's identity. If it matches, the server confirms this user is legal. If not, then the server rejects this user. In addition, the server contains $H(ID_i)$ in advance and does not know the user's real identity. After the server authenticates the user's legitimacy, the server sends z_i and Y_i to the user. The user can authenticate the server using $z_i = Y_i H(ID_i) + X_s H(PW_i)$. Hence, the registration phase realizes mutual authentication. In authentication phase, only when the user U_i enters the correct ID_i and PW_i into the smart card to ensure that $W^* = H(ID_i) \oplus H(PW_i)$ is equal to W stored in the smart card, the smart card will continue to complete the subsequent authentication. In a word, only the legally registered user can send login request messages to the remote server through the smart card. Upon receving the requested messages from U_i, the server sends signature V_2 to SC. The smart card verifies the correctness of V_2 to authenticate the server. Therefore, the proposed protocol provides mutual authentication.

5.3 Session Key Agreement

After the login and authentication phase, the smart card and the server share a common session key $K = x_i X_s = x_s X_i = x_i x_s P$. The private key x_i and x_s are secretly stored in the user and the server, the adversary cannot achieve them. Even though the adversary gets X_s and X_i though the open channel, he still cannot generate the common session key because of the CDH problem. Therefore, the proposed protocol can achieve session key agreement.

5.4 Man-in-the-Middle Attack Resistance

Suppose the adversary intercepts the requested messages sent by the smart card, then the adversary disguised as the server to deceive the user. The adversary must compute $V_2 = y_i - x_s H(ID_i \parallel t_2)$ and sends V_2 to U_i. However, the adversary cannot get the server's private key y_i and x_s. Hence, the adversary cannot disguise as the server. Similarly, the adversary cannot achieve the user's full private key (x_i, z_i) and can't disguised as the user. In a word, even though the adversary eavesdrops all the communications between the user and the server, he still cannot impersonate as U_i and the server to get private information.

5.5 Impersonation Attack Resistance

The proposed protocol can resist the server impersonation attack. If the adversary aiming to impersonate the server, he does not have the server's master private key x_s. Hence, it is impossible for the adversary to generate z_i and V_2 to pass the verification by U_i. If the adversary aiming to impersonate the user, he cannot get the user's full private key (x_i, z_i) and real identity. Therefore, the adversary cannot pass through the authentication of the server.

5.6 Offline Dictionary Attack Resistance

The proposed protocol can withstand offline dictionary attack. The login information V_1 and t_1 and the authentication information V_2 and t_2 are transmitted over open channel. These messages are all irrelevant with the password PW_i. If the adversary gets these messages, he cannot verify whether the guessed password is correct or not. In addition, the counter R maintained by the smart card and the initial value is zero. Once R reaches a preset threshold value n, the smart card will be locked and the adversary cannot login anymore.

5.7 Reply Attack Resistance

In the proposed protocol, we use timestamp t_1 and t_2 to withstand the reply attack. If the adversary intercepts the messages V_1, t_1 and V_2, t_2 from the smart card and the server respectively, then he replays messages to the smart card or the server. The adversary will fail to pass the authentication phase duo to the invalidity of the timestamp t_1 and t_2. Even if the adversary replays the message within the valid time, he still cannot compute the session key because the computational Diffie-Hellman problem.

5.8 Lost-Smart-Card Attack Resistance

Based on the above security analysis, the adversary cannot perform offline dictionary attack, impersonation attack and reply attack even if the adversary obtains the smart card and gets all communication messages. On the other hand, the adversary cannot get the user's identity and password. Once the number of failed logins reaches the threshold value n, the smart card will be locked. Therefore, the proposed protocol can resist lost-smart-card attack.

5.9 Privileged-insider Attack Resistance

In registration phase, the user sends $H(ID_i)$ and $H(PW_i)$ to the server insteal of user's identity and password. Hence, the server does not know the real identity and password of the user U_i. Therefore, the proposed protocol can resist the privileged-insider attack.

6 Performance Analysis

In this section, we compare the security properties and computational cost of the proposed protocol with two typical authentication protocols using elliptic

curves cryptography. Yeh et al. [12]'s protocol is a ECC-based remote authentication protocol, and Shi et al. [13]'s protocol is an efficient user authentication protocol which can prevent general security issues.

6.1 Security Comparison

We compare the security properties of our protocol with Yeh et al. [12] and Shi and Gong [13]'s protocol. As shown in Table 1, the protocol of Yeh et al. and Shi et al. does not provide real anonymity, and cannot resist impersonation attack, offline dictionary attack as well as lost-smart-card attack. For convenience, we use notations to indicate security properties as follows: "ANO" denotes user anonymity, "MA" denotes mutual authentication, "SKA" denotes session key agreement, "MAR" denotes man-in-the-middle attack resistance, "IAR" denotes impersonation attack resistance, "ODAR" denotes offline dictionary attack resistance, "RAR" denotes reply attack resistance, "LAR" denotes lost-smart-card attack resistance and "PAR" denotes privileged-insider attack.

Table 1. Security comparison

Scheme	Yeh's	Shi's	Ours
ANO	N	N	Y
MA	Y	Y	Y
SKA	Y	Y	Y
MAR	Y	Y	Y
IAR	N	N	Y
ODAR	N	N	Y
RAR	Y	Y	Y
LAR	N	N	Y
PAR	Y	Y	Y

6.2 Computational Cost Comparison

We compare the computational cost of the proposed protocol with Yeh et al. [12] and Shi and Gong [13]'s protocol. The computational cost of the authentication phase is prime concerned. For the convenience of evaluating the computational cost, some notations used in this section are defined as follows:

T_m : The time of executing a scalar multiplication operation.

T_a : The time of executing a point addition operation

T_h : The time of executing a one-way hash function

T_ε : The time of executing an elliptic curve polynomial computation.

In Table 2, we summarize the computational cost of the proposed protocol. In the registration phase, Yeh's protocol requires four one-way hash function operations and one scalar multiplication operation. Shi's protocol requires three one-way hash function operations and one scalar multiplication operation. Our protocol requires two one-way hash function operations, six scalar multiplication operations and one addition operation of point. In the login and authentication phase, Yeh's protocol requires eleven one-way hash function operations, six scalar multiplication operations, four addition operations of points and two elliptic curve polynomial computations. Shi's protocol requires twelve one-way hash function operations and six scalar multiplication operations. Our protocol requires three one-way hash function operations, nine scalar multiplication operations and two addition operations of points.

Table 2. Comparison of the Computational Cost

Scheme/Phase	Registration	Login/Authentication
Yeh's	$4T_h + T_m$	$11T_h + 6T_m + 4T_a + 2T_\varepsilon$
Shi's	$4T_h + T_m$	$12T_h + 6T_m$
Ours	$2T_h + 6T_m + T_a$	$3T_h + 9T_m + 2T_a$

To evaluate the computational cost of the proposed protocol, we set up simulation environment and quantify the computation time of the cryptographic operations used in the selected protocols. The simulation environment of the protocol is Windows 10 over an Inter(R) Core (TM) i5-7300HQ CPU, 2.50 GHz processor and 8.00 GB memory. The code were written in Ubuntu 12 operating system and the simulation is based on the PBC (pairing based cryptography). The simulation has been running several times by using C language and the results were averaged to make up for the randomness. The comparison of the running time is shown in Table 3. We can find that the proposed protocol is much more efficient than others in the login/authentication phase. Figure 4 illustrates that the time consumption of the authentication phase in Yeh et al.'s [12], Shi and Gong's [13] and our protocol linearly increases along with the number of requested users increasing. Figure 4 clearly demonstrates that the proposed protocol is more efficient than others.

The computational cost comparison demonstrates that the proposed protocol is more efficient that these two typical protocols, while the security comparison indicates that the proposed protocol is more secure than others. In summary, our protocol is more suitable for the Smart card applications.

Table 3. Comparison of the Running Time (In Milliseconds)

Scheme/Phase	Registration	Login/Authentication
Yeh's	31.076	103.164
Shi's	25.428	93.583
Ours	33.217	52.307

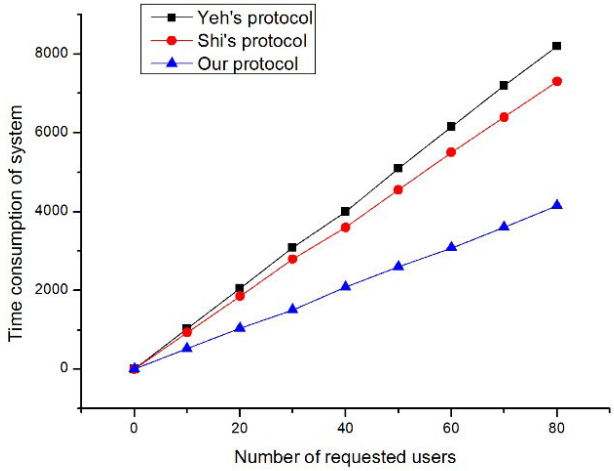


Figure 4. Running Time of the authentication Phase

7 Conclusion

Motivated by the practical needs to secure the authentication in smart cards, we proposed a lightweight certificateless two-factor authentication protocol against various attacks including privileged-insider attack, lost-smart-card attack and offline dictionary attack, and supports anonymity, mutual authentication and session key agreement. As far as we know, it is the first time to use certificateless public key cryptography in smart card authentication. Furthermore, the proposed protocol is low time-consumption and highly practical in smart card applications.

References

[1] H. Y. Chien, J. K. Jan, Y. M. Tseng, An Efficient and Practical Solution to Remote Authentication: Smart Card, *Computers & Security*, Vol. 21, No. 4, pp. 372-375, August, 2002.

[2] T. S. Messerges, E. A. Dabbish, R. H. Sloan, Examining Smart-Card Security under the Threat of Power Analysis Attacks, *IEEE Transactions on Computers*, Vol. 51, No. 5, pp. 541-552, May, 2002.

[3] V. C. Gungor, G. P. Hancke, Industrial Wireless Sensor Networks: Challenges, Design Principles, and Technical Approaches, *IEEE Transactions on Industrial Electronics*, Vol. 56, No. 10, pp. 4258-4265, February, 2009.

[4] L. Lamport, Password Authentication with insecure communication, *Communications of the Acm*, Vol. 24, No. 24, pp. 770-772, November, 1981.

[5] W. H. Yang, S. P. Shieh, Password Authentication Schemes with Smart Cards, *Computers & Security*, Vol. 18, No. 8, pp. 727-733, December, 1999.

[6] S. M. Bellovin, M. Merritt, Encrypted Key Exchange: Password-Based Protocols Secure Against Dictionary Attacks, *Proceedings 1992 IEEE Computer Society Symposium on Research in Security and Privacy (SP)*, Oakland, CA, 1992, p. 72.

[7] J. Shen, T. Zhou, D. He, Y. Zhang, X. Sun, Y. Xiang, Block Design-based Key Agreement for Group Data Sharing in Cloud Computing, *IEEE Transactions on Dependable and Secure Computing*, July, 2017, DOI: 10.1109/TDSC.2017.2725953.

[8] J. Shen, D. Liu, Q. Liu, X. Sun, Y. Zhang, Secure Authentication in Cloud Big Data with Hierarchical Attribute Authorization Structure, *IEEE Transactions on Big Data*, May, 2017, DOI: 10.1109/TBDATA.2017.2705048.

[9] N. Gunson, D. Marshall, H. Morton, M. Jack, User Perceptions of Security and Usability of Single-factor and Two Factor Authentication in Automated Telephone Banking, *Computers & Security*, Vol. 30, No. 4, pp. 208-220, June, 2011.

[10] D. Wang, P. Wang, On the Anonymity of Two-factor Authentication Schemes for Wireless Sensor Networks: Attack, Principle and Solutions, *Computer Networks*, Vol. 73, No. C, pp. 41-57, July, 2014.

[11] M. Bond, O. Choudary, S. J. Murdoch, S. Skorobogatov, R. Anderson, Chip and Skim: Cloning EMV Cards with the Pre-play Attack, *2014 IEEE Symposium on Security and Privacy (SP)*, Berkeley, CA, 2014, pp. 49-64.

[12] H. L. Yeh, T. H. Chen, P. C. Liu, T. H. Kim, H. W. Wei, A Secured Authentication Protocol for Wireless Sensor Networks Using Elliptic Curves Cryptography, *Sensors*, Vol. 11, No. 5, pp. 4767-4779, December, 2011.

[13] W. Shi, P. Gong, A New User Authentication Protocol for Wireless Sensor Networks Using Elliptic Curves Cryptography, *International Journal of Distributed Sensor Networks*, Vol. 2013, No. 730831, pp. 51-59, April, 2013.

[14] M. L. Das, A. Saxena, V. P. Gulati, A Dynamic ID-based Remote User Authentication Scheme, *IEEE Transactions on Consumer Electronics*, Vol. 50, No. 2, pp. 629-631, May, 2004.

[15] T. H. Kim, C. Kim, I. Park, Side Channel Analysis Attacks Using AM Demodulation on Commercial Smart Cards with SEED, *Elsevier Science Inc.*, Vol. 85, No. 12, pp. 2899-2908, December, 2012.

[16] M. K. Khan, S. K. Kim, K. Alghathbar, Cryptanalysis and Security Enhancement of a More Efficient & Secure Dynamic ID-based Remote User Authentication Scheme, *Elsevier Science Publishers B. V.*, Vol. 34, No. 3, pp. 305-309, March, 2011.

[17] M. Kumar, M. K. Gupta, S. Kumari, An Improved Smart Card Based Remote User Authentication Scheme with Session Key Agreement during the Verification Phase, *Journal of Applied Computer Science & Mathematics*, Vol. 5, No. 11, pp. 38, December, 2011.

[18] R. Madhusudhan, R. C. Mittal, Dynamic ID-based Remote User Password Authentication Schemes Using Smart Cards: A Review, *Journal of Network & Computer Applications*, Vol. 35, No. 4, pp. 1235-1248, July, 2012.

[19] J. Shen, J. Shen, X. Chen, X. Huang, W. Susilo, An Efficient Public Auditing Protocol With Novel Dynamic Structure for Cloud Data, *IEEE Transactions on Information Forensics*

and Security, Vol. 12, No. 10, pp. 2402-2415, May, 2017.

[20] J. Shen, S. Chang, J. Shen, Q. Liu, X. Sun, A Lightweight Multi-layer Authentication Protocol For Wireless Body Area Networks, *Future Generation Computer Systems*, December, 2016, DOI: 10.1016/j.future.2016.11.033.

[21] Y. Y. Wang, J. Y. Liu, F. X. Xiao, J. Dan, A More Efficient and Secure Dynamic ID-based Remote User Authentication Scheme, *Computer Communications*, Vol. 32, No. 4, pp. 583-585, March, 2009.

[22] C. I. Fan, Y. C. Chan, Z. K. Zhang, Robust Remote Authentication Scheme with Smart Cards, *Elsevier Advanced Technology Publications*, Vol. 24, No. 8, pp. 619-628, November, 2005.

[23] W. S. Juang, S. T. Chen, H. T. Liaw, Robust and Efficient Password-Authenticated Key Agreement Using Smart Cards, *IEEE Transactions on Industrial Electronics*, Vol. 55, No. 6, pp. 2551-2556, July, 2008.

[24] D. Z. Sun, J. P. Huai, J. Z. Sun, J. X. Li, J. W. Zhang, Z. Y. Feng, Improvements of Juang's Password-Authenticated Key Agreement Scheme Using Smart Cards, *IEEE Transactions on Industrial Electronics*, Vol. 56, No. 6, pp. 2284-2291, June, 2009.

[25] L. Chen, F. Wei, C. Ma, A Secure User Authentication Scheme against Smart-Card Loss Attack for Wireless Sensor Networks Using Symmetric Key Techniques, *International Journal of Distributed Sensor Networks*, Vol. 2015, pp. 1-10, April, 2015.

[26] A. Cilardo, L. Coppolino, N. Mazzocca, L. Romano, Elliptic Curve Cryptography Engineering, *Proceedings of the IEEE*, Vol. 94, No. 2, pp. 395-406, March, 2006.

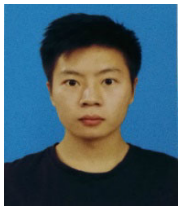
[27] D. Wang, D. B. He, P. Wang, C. H. Chu, Anonymous Two-Factor Authentication in Distributed Systems: Certain Goals Are Beyond Attainment, *IEEE Transactions on Dependable and Secure Computing*, Vol. 12, No. 4, pp. 428-442, July, 2015.

[28] Q. Xie, D. S. Wong, G. Wang, X. Tan, K. Chen, L. Fang, Provably Secure Dynamic ID-Based Anonymous Two-Factor Authenticated Key Exchange Protocol with Extended Security Model, *IEEE Transactions on Information Forensics & Security*, Vol. 12, No. 6, pp. 1382-1392, June, 2017.

[29] J. Shen, D. Liu, C. Lai, Y. Ren, X. Sun, A Secure Identity-Based Dynamic Group Data Sharing Scheme for Cloud Computing, *Journal of Internet Technology*, Vol. 18, No. 4, pp. 833-842, January, 2017.

Biographies

Wenying Zheng received the M.E. degree in Electronic Engineering from Chosun University, Gwangju, Korea, in 2009. She is currently working toward the Ph.D. degree at Nanjing University of Aeronautics and Astronautics, Nanjing, China. Her research interests include image security, image recognition, security systems and network security.



Ziyuan Gui received the B.S. degree in 2016 and is currently working toward the M.E. degree at Nanjing University of Information Science and Technology, Nanjing, China. He focuses on the security and privacy issues in cloud environment. His current research interests are key agreement and lightweight authenticated key exchange protocol.

Dengzhi Liu received the B.S. degree and the M.E. degree from Nanjing University of Information Science and Technology in 2014 and 2017, respectively. He is currently working toward the Ph.D. degree in the School of Computer and Software, Nanjing University of Information Science and Technology. He focuses on the security and privacy issues in cloud Computing. His current research interests include applied cryptography, network and data security, and cloud computing security.

Xiong Li received his master's degree in mathematics and cryptography from Shanxi Normal University (SNNU) in 2009 and Ph.D. degree in computer science and technology from Beijing University of Posts and Telecommunications (BUPT) in 2012. Dr. Li now is a lecturer of Hunan University of Science and Technology (HNUST). He has published more than 15 referred journal papers. His research interests include cryptography and information security, etc.

Bing Chen received the B.S. and M.S. degrees in computer engineering from the Nanjing University of Aeronautics and Astronautics (NUAA), Nanjing, China, in 1992 and 1995, respectively, and the Ph.D. degree from the College of Information Science and Technology, NUAA, in 2008. He has been with NUAA since 1998, where he is currently a Professor with the Computer Science and Technology Department. His main research interests include cloud computing, wireless communications, and cognitive radio networks.