Applied Mathematics & Information Sciences
An International Journal

A strong password-based remote mutual authentication with key agreement scheme on elliptic curve cryptosystem for portable devices

Xuelei Li, Fengtong Wen and Shenjun Cui

School of Mathematical Sciences, University of Jinan, Jinan, Shandong 250022, P R China

Received: Jun 1, 2011; Revised Oct. 4, 2011; Accepted Dec. 16, 2011
Published online: 1 May 2012

Abstract: In this paper, we cryptanalyze Kim et al.'s scheme and point out several weaknesses in their scheme. Off-line password guessing/dictionary attack could be effective. Moreover, we demonstrate that there is a mistake in their security analysis. To remedy the weaknesses, we propose a more secure, robust and practical scheme, which is designed for portable devices based upon the discrete logarithm on elliptic curve. In addition, the expensive synchronization clock system is replaced by nonce(ephemeral random number), and the new scheme provides more functions for security and flexibility, including key agreement, password change, secret number update, revocation and DoS-resistant. Finally, security analysis shows that our scheme could resist the known common attacks.

Keywords: Cryptosystem, Password-based authentication

1. Introduction

1.1. Backgrounds

As is well-known, the fast development of the electronics, networks and embedded software technologies makes our lives changed earthshakingly. The population of the portable devices with the embedded softwares, such as cell phones, PDAs, note-book PCs and other intelligent devices, makes our communications more and more convenient. The ubiquity of the universal serious bus(USB) storages is much more helpful in our daily life. Furthermore, the communication environment has changed a lot, especially the wireless networks and LAN (local area networks) are spreading widely nowadays. Thus it is concerned about secure communications over the insecure and public wireless network channels. In addition, the promotion of network bandwidth and the ability of computational performance become double-edged swords, such as the distributed computation, cloud computation and quantum computation. On the one hand, it makes our capability of interaction and computation much more efficient and rapid; on the other hand, it can be also used by the adversary to break down the authentication scheme, for example, the adversary could take advantage of the efficient computation to search the password using brute-force method with enough redundant information. All the above realities promote our research to propose a more secure, practical, efficient and flexible password-based remote mutual authentication with key agreement scheme using portable devices.

1.2. Related Works

A variety of password authentication schemes [1,2,4,5,7, 6,11,12,16–21] have been proposed, since Lamport [10] proposed his primitive research in 1981. The weaknesses in the related works have been pointed out, such as the expensive cost for storing the verifier tables, vulnerability to verifier table stolen attack, lacks of mutual authentication with key agreement and so on. In order to remedy the weaknesses caused by the verifier table, smart cards based password authentication schemes [1,6] have been presented, in which the verifier tables were not required any more. However, Kocher et al. [9], Messerges et al. [14] and Leng [13] showed that the smart cards were not secure, because the key information stored and protected by physical mechanisms in the smart cards could be revealed some-

[*] Corresponding author: e-mail: will8898@163.com

way. In another word, the tamper-resistant property of the smart card could be ignored in the ideal conditions. In 2009, Xu et al. [19] cryptanalyzed Lee-Chiu's [11] scheme and Lee-Kim-Yoo's [12] scheme under the assumption that the information stored in the smart card was revealed. They also pointed out that both of the schemes were subject to forgery attacks. In addition, Xu et al. proposed an improved scheme using smart cards with formal security proof. Furthermore, Rhee et al. [16] pointed out that the schemes using smart cards in [2] and [5] could not be immediately converted into schemes using common storage devices, because the impersonation attacks could be easily launched using the exposed information stored in the common storage devices. Rhee et al. [16] also proposed a remote user authentication scheme without using smart cards, which was more secure and practical using common storage devices. Recently in 2009, Yang et al. [20] proposed an ID-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem. Their scheme reduced the computation loads in the scheme [17], which required the associated certificate in the public-key cryptosystem; it also supported a session key agreement; in addition, compared with the related works based upon RSA or discrete logarithm problem, the proposed scheme was more efficient and practical for mobile devices. Because it had been proved that 160-bit key in the elliptic cryptosystem had the same security level with 1024-bit key in the RSA cryptosystem. In the same year, Kim et al. [7] presented a proposal as an enhancement of Yoon-Yoo's [21] scheme, which resolved the security flaws in Yoon-Yoo's scheme, such as revealing password attack, masquerading user or server attack and stolen verifier attack. In 2010, Hwang et al. [4] provided a defense mechanism to Kim-Lee-Yoo's [6] ID-based password authentication scheme, which was vulnerable to impersonation attacks and resource exhaustion attacks. The proposed defense mechanism not only accomplished mutual authentication and session key establishment, but also provided the idea of DoS-resistant in the authentication schemes.

1.3. Our Contributions

In this paper, we review Kim-Chung's [7] scheme and point out several weaknesses under their assumptions. An enhanced scheme is presented to remedy the weaknesses mentioned in this paper. The new scheme not only keeps all the merits of the original scheme, but also provides the functions of password change, secret number update, revocation and DoS-resistant to make our protocol much more flexible. Furthermore, the security of our scheme is based upon the secure one-way hash function and elliptic curve cryptosystem. It is designed for the portable devices without synchronization clock system. It can be implemented more practically and conveniently in the real environment. The ephemeral random number used only in the current session, which is called nonce as usual, could resist replay attacks, hide the key authentication information and compose the fresh session key, so the nonce plays an important role in our scheme. Finally, the security analysis shows that our scheme could resist the known common attacks.

1.4. Organizations

In section 2, we review and cryptanalyze Kim et al.'s [7] scheme. In section 3, we propose an improved scheme. The security analysis of our scheme is presented in section 4. At last, we conclude our work in section 5.

2. Kim-Chung's scheme

2.1. Review of Kim-Chung's Scheme

There are four phases in Kim et al.'s [7] scheme, which consists of registration phase, login phase, verification phase and password change phase. *1.Registration Phase*

(1) U_i chooses his ID_i and pw_i, then sends them to S over a secure channel. (2) S computes $K_1 = h(ID_i \oplus x) \oplus N_i$ and $K_2 = h(ID_i \oplus x \oplus N_i) \oplus h(pw_i \oplus h(pw_i))$, where x is the secret number kept by S privately and N_i is a random number unique to U_i. Then S computes $R = K_1 \oplus h(pw_i)$ and stores the key information $K_1, K_2, R, h(\cdot)$ into U_i's smart card.

(3) S sends the smart card to U_i over a secure channel.

2. Login Phase

When U_i wants to login the server S, performs the following steps: (1) U_i input his ID_i and pw_i after inserting his smart card into a card reader.

(2) Smart card computes $C_1 = R \oplus h(pw_i)$. If the equation $C_1 = K_1$ holds, S computes $C_1' = K_2 \oplus h(pw_i \oplus h(pw_i))$ and $C_2 = h(C_1' \oplus T_1)$, where T_1 is the current time of U_i.

(3) U_i sends the login request message $\{ID_i, T_1, C_1, C_2\}$ to S.

3. Verification Phase

Upon receiving the login request at time T_1', S performs the following steps:

(1) Checks whether ID_i is in the registration table and the time interval $T_1' - T_1 \leq \varDelta T$ is valid. If so, S computes $N_i' = C_1 \oplus h(ID_i \oplus x)$ and verifies if $h(h(ID_i \oplus x \oplus N_i') \oplus T_1)$ is equal to C_2. If so, S successfully authenticates U_i.

(2) S computes $C_3 = h(h(ID_i \oplus x \oplus N_i') \oplus C_2 \oplus T_2)$ and sends the message $\{T_2, C_3\}$ to U_i for mutual authentication.

(3) Upon receiving the responding message, U_i checks whether T_2 is a fresh time. If so, U_1 verifies whether the equation $h(C_1' \oplus C_2 \oplus T_2) = C_3$ holds. If so, U_i successfully authenticates S; otherwise terminates the current process.

4. Password Change Phase

When U_i wants to change his password pw_i, performs the following steps:

(1) U_i inserts his smart card into a card reader and keys ID_i with pw_i.

(2) Smart card computes $K_1' = R \oplus h(pw_i)$ and compares K_1' with K_1. If they are equal, U_i inputs his new password pw_i^*. The smart card computes $R^* = K_1' \oplus h(pw_i^*)$ and $K_2^* = K_2 \oplus h(pw_i \oplus h(pw_i)) \oplus h(pw_i^* \oplus h(pw_i^*))$, then replaces R and K_2 by R^* and K_2^*.

2.2. Cryptanalysis of Kim-Chung's Scheme

Kim et al. [7] claimed their scheme was secure under the following assumptions:

(I) We consider an adversary A has full control over the network, it could eavesdrop, record, intercept, modify and delay the messages online.

(II) An adversary has the ability to extract the key information stored in the smart card, such as by the method of physically monitoring its power consumption.

However, we demonstrate that off-line password guessing attack is effective under their cryptographic assumptions, which are aforementioned. In addition, we point out a mistake in their security analysis about the forward secrecy.

1. Password Dictionary Attack

If an adversary A could get the smart card and extract the key information stored in the smart card, then A can compute $h(pw_i) = K_1 \oplus R$, where K_1 and R are extracted from the smart card. A could launch off-line password dictionary attack with $h(pw_i)$ by the following method. First A chooses a candidate pw_i^* in a password dictionary D and computes $h(pw_i^*)$. If the equation $h(pw_i) = h(pw_i^*)$ holds, A could confirm the password by computing $h(K_2 \oplus h(pw_i^* \oplus h(pw_i^*)) \oplus T_1)$ and verifying whether $C_2 = h(K_2 \oplus h(pw_i^* \oplus h(pw_i^*)) \oplus T_1)$ holds. If it holds, pw_i^* is the correct password used in this scheme. If $h(pw_i^*) \neq h(pw_i)$ or $C_2 \neq h(K_2 \oplus h(pw_i^* \oplus h(pw_i^*)) \oplus T_1)$, A should delete the candidate from the password dictionary and choose the next candidate to find the correct password. Repeat the above operations, the password could be revealed by such dictionary attack. In addition, password brute-force guessing attack according to the above operations, must be effective to get the correct password. Compared password dictionary attack with brute-force guessing attack, the first method is efficient, but not always effective; inversely, password brute-force guessing attack is always effective, but not efficient.

We note that due to the collision of the hash function, the password we guessed may not be the one which the user used in practice. However, we do not care about it, just focus on the values which could help the adversary to login the server. In addition, passwords used in our daily life may be composed of Arabic numerals, such as in the financial, telecommunication fields. Thus off-line password guessing attack could be more threatening. We must pay attention to protect the information, which could be used by the attackers as the redundance for matching their guessed values. With enough redundant information, the attackers could reveal the key values(such as passwords, secret keys).

2. Secret Key Forward Secrecy

Kim et al. [7] pointed out that if the secret key x happened to be revealed, the attacker A can not impersonate other users by the revealed secret key x. Because the adversary A can not compute C_1 and C_2 in the login request without knowing N or PW. We demonstrate that their security analysis about *Secret Key Forward Secrecy* in section 4 [7] is not correct by the following operations. If A knows x and all the communications between users and the remote server are recorded by A, then he can compute $h(ID_j \oplus x)$ and $N_j' = h(ID_j \oplus x) \oplus C_1$, where ID_j is any legal user registered in S and ID_j, C_1 could be intercepted by A. Then C_2 can be computed by $C_2^* = h(h(ID_j \oplus N_j' \oplus x) \oplus T_1^*)$, where T_1^* is the current timestamp of the attacker. Thus the masquerading user attack could be successfully with the login requesting message $\{ID_j, C_1, C_2^*, T_1^*\}$. In addition, masquerading server attack could be also effective according to the following steps. A computes $C_3^* = h(h(ID_j \oplus x \oplus N_j') \oplus C_2 \oplus T_2^*)$ and sends $\{T_2^*, C_3^*\}$ to U_j, where ID_j and C_2 are intercepted online from the legitimate user U_j, N_j' is computed by the masquerading server. Finally, U_j confirms the identity of the server, who is impersonated by the adversary.

3. A new password-based authentication with key agreement scheme

There are five phases in our scheme: initialization phase, registration phase, login and mutual authentication with key agreement phase, secret update phase and revocation phase.

3.1. Initialization Phase

(1) The server chooses an elliptic curve $E_p(a, b)$, P is a generator of order q, where q is large prime number and $p = 2q + 1$, such that the discrete logarithm problem in the cyclic subgroup $\langle P \rangle$ is hard to be solved. The server chooses two proper hash functions $h(\cdot)$ and $H(\cdot)$, where $h(\cdot)$ is a one way hash function with an arbitrary-length input and a output in Z_p^*, $H(\cdot)$ is a secure session key derive function with a input in Z_p^* and a output string $\{0, 1\}^l$, where l is a secure parameter determined the length of the session keys. All the above parameters are public.

(2) The server chooses its secret key $x \in Z_p^*$ and keeps it in private. All the random numbers r_i, m_i, n_i, N_U, N_S, V, a, k_1, k_2 are in Z_p^* and the points $A_{i,1}, A_{i,2}$, C_1, C_2, C_3, C_4, K are on the elliptic curve $E_p(a, b)$. In addition, all the operations are mod p, where we omit it for simplicity.

3.2. Registration Phase

(1) U_i sends his chosen identity ID_i and password pw_i to S over a secure channel, where ID_i and pw_i are both in Z_p^*.

(2) S computes U_i's authentication information $A_i = (A_{i,1}, A_{i,2}) = (ID_i \cdot n_i \cdot r_i \cdot P + pw_i \cdot P, r_i \cdot P)$ where x is a secret key kept by S in private and $n_i = x - m_i$, m_i is a random number generated by S and kept in server's registration table with ID_i, r_i is a unique random number used in the authentication information only.

(3) S sends A_i to U_i over a secure channel and keeps the registration table $ID_i \| m_i$ in private.

(4) U_i stores A_i in his mobile devices privately and remember his identifier of ID_i with pw_i.

3.3. Login and Mutual Authentication with Key Agreement Phase

(1) U_i input his ID_i and sends $M_1 = \{ID_i, N_U, Hello!\}$ to S for asking login request.

(2) S checks whether ID_i is valid in its database, if so, S responds U_i with $M_2 = \{ID_i, N_U, N_S, V_S\}$, where $V_S = h(ID_i, N_U, N_S, V)$ is a client puzzle [4] to resist DoS-attack, V is a random number generated by S and keeps it in private temporarily. In addition, the difficulty of the client puzzle depends on the loading of the server's resource. For example, if S is over loading, then the client puzzle may be hard to be solved; else if S is processing the data as usual, then V_S may be easy to be solved; else if the server is idle, then the client puzzle may be responded with $NULL$, where $NULL$ represents a fixed string.

(3) Upon receiving the responded message M_2 from S, U_i tries to solve the client puzzle V_S by exhaustively searching to get the correct $V' = V$, such that $h(ID_i, N_U, N_S, V') = V_S$ After that U_i input his password pw_i, the mobile device computes $A'_{i,1} = A_{i,1} - pw_i \cdot P, t = h(N_U, N_S, V_S), C_1 = a \cdot t \cdot A'_{i,1}, C_2 = a \cdot A_{i,2}, C_3 = t \cdot A'_{i,1} + k_1 \cdot P$, where a and k_1 are nonces generated by U_i's device. U_i sends $M_3 = \{ID_i, V', C_1, C_2, C_3, A_{i,2}\}$ to S.

(4) After receiving U_i's login request message M_3, S checks whether ID_i is valid again and verifies if the client puzzle is correct by verifying the equation $h(ID_i, N_U, N_S, V') = V_S$. If the the equation holds, S continues the procedure, computing $A'_{i,1} = ID_i \cdot (x - m_i) \cdot A_{i,2}, t' = h(N_U, N_S, V_S)$, where m_i is extracted from the registration table database corresponding to ID_i. Then S verifies whether the equation $C_1 = C'_1$ holds, where $C'_1 = t' \cdot ID_i \cdot (x - m_i) \cdot C_2$. If so, S accepts U_i's login request and extracts $k_1 \cdot P$ from $C_3 - (t' \cdot A'_{i,1})$. After that, S computes the session key $sk = H(K_X)$, where K_X is the X-coordinate of K used for generating the session key, $K = k_2 \cdot (k_1 \cdot P)$ is the point on $E_p(a, b)$ and k_2 is a random number generated by S. Finally, S sends $M_4 = \{ID_i, C_4, C_5\}$ to U_i for mutual authentication, where $C_4 = t' \cdot A'_{i,1} + k_2 \cdot P, C_5 = [ID_i, t', k_1 \cdot P]_{sk}$. We note that the point on $E_p(a, b)$ can be regarded as two numbers in Z_p^*, when they were encrypted or decrypted in our scheme.

(5) Upon receiving M_4, U_i's device extracts $k_2 \cdot P$ through $C_4 - t \cdot A'_{i,1}$ and computes $K = k_1 \cdot (k_2 \cdot P)$. Then U_i computes the session key $sk = H(K_X)$ and verifies C_5 by decrypting it. If the decrypted information ID_i, t' and $k_1 \cdot P$ in C_5 are correct, mutual authentication between U_i and S is completed successfully; otherwise the procedure should be terminated. U_i sends the message $M_5 = \{ID_i, C_6\}$ to S, where $C_6 = [ID_i, k_2 \cdot P]_{sk}$.

(6) Finally, S decrypts C_6 with sk, verifies whether the information is correct. If so, the session key $sk = H((k_1 \cdot k_2 \cdot P)_X)$ is generated and confirmed after the above steps. In addition, once there is a mistake in the checking or verifying procedures, the honest participant should terminate the procedure.

3.4. Secret Update Phase

(1) Password change phase: If U_i want to change his original password pw_i into a new one pw_i^*. After accessing to his device with ID_i, then U_i inputs pw_i and pw_i^* in proper sequence, the mobile device computes $A_{i,1}^* = A_{i,1} - pw_i \cdot P + pw_i^* \cdot P$ and replaces $A_{i,1}$ by $A_{i,1}^*$. The password change phase is completed off-line.

(2) Secret number update phase: The secret number x kept by S in private could be updated following the steps. S chooses a new secret number x^* and updates its registration table in the database through replacing m_i by $m_i^* = x^* - (x - m_i)$. Thus the secret number update phase could be also completed off-line.

3.5. Revocation Phase

If U_i's authentication information A_i and password pw_i happen to be revealed to the adversary together, he should revoke his original identity according to the traditional method. However, we provide a new way to revoke his authentication information without changing his ID_i. In details, the server could choose a new random number $\bar{m}_i$, when U_i want to revoke his identity, S could compute the new authentication information $\bar{A}_i = (\bar{A}_{i,1}, \bar{A}_{i,2}) = (ID_i \cdot \bar{n}_i \cdot \bar{r}_i \cdot P + p\bar{w}_i \cdot P, \bar{r}_i \cdot P)$, where $\bar{n}_i = x - \bar{m}_i$, $\bar{m}_i, \bar{r}_i$ and $p\bar{w}_i$ are new chosen for revocation phase. When U_i login the sever, S should verify U_i with x and $\bar{m}_i$, thus the original authentication information is not valid, which should be verified with $n_i = x - m_i \neq \bar{n}_i$. Thus the user's revocation phase is completely without changing his original identity.

4. Security analysis

4.1. Cryptographic Assumptions

1. Assumptions of the Elliptic Curve Cryptosystem

(1)Elliptic Curve Discrete Logarithm Problem (ECDLP): Given two points P and Q on $E_p(a,b)$, the elliptic curve discrete logarithm problem is to find an integer $s \in Z_p^*$ such that $Q = s \cdot P$.

(2) Elliptic Curve Diffier-Hellman Problem(ECDHP): Given a point $(s \cdot t) \cdot P$, the elliptic curve Diffier-Hellman problem is to find the two points $s \cdot P$ and $t \cdot P$.

(3) Computational Diffie-Hellman Problem(CDHP): Given three points P, $s \cdot P$ and $t \cdot P$ on $E_p(a,b)$, where $s, t \in Z_p^*$, the computation Diffie-Hellman problem(CDHP) is to find the point $(s \cdot t)P$ on $E_p(a,b)$.

Assume that all of the above three problems are difficult to be solved in polynomial-time, in other words, there are no efficient polynomial-time algorithm to solve the above problems. More details can be referenced in [15,8,3].

2. Assumptions of the Adversaries' Capabilities

(1) We consider an adversary A has full control over the network, it could eavesdrop, record, intercept, modify and delay the messages online.

(2) An adversary has the ability to corrupt the authentication information stored in the mobile devices, including smart cards.

(3) A could launch brute-force guessing attack to obtain the secrets pw_i with enough redundant information.

(4) The adversary could not get the temporary values processed in the local machine, such as the random numbers. If the random numbers could be revealed, it means that the ECDLP, ECDHP and CDHP can be solved. In addition, A could not get both A_i and pw_i or both $ID_i||m_i$ and x at the same time.

4.2. Security Analysis

1. Replay Attack

Replay attack could be resist in our scheme, because of the once used random numbers N_U, a, k_1 and N_S, V, k_2, which are generated by U_i and S separately. The authentication messages C_1, C_2 and C_4, C_5 are computed by the secret information $A'_{i,1}$ and nonces. Nonces replace the synchronization clock system to help our scheme to resist replay attack. Moreover, if the synchronization clock system is easy to be realized, our scheme could also be implemented using timestamps, similarly to Kim et al. schemes in [6].

2. Off-line Password Guessing Attack

Such attack could be avoided without the redundant information related to pw_i, such as $pw_i \cdot P$ or $A'_{i,1}$. Furthermore, the password brute-force guessing attack could also be avoided without any redundant information. Because the message C_i, where $i = 1, 2, \cdots, 6$, are protected by nonces, which the adversary could not obtained, the adversary can not find the matching information to launch such attacks. In addition, online password guessing attack could also be resistant by the related mechanisms, such as the false times of login request.

3. Impersonation Attack

The adversary could not impersonate U_i without knowing the key information $A'_{i,1}$ under the assumptions mentioned before, because the adversary can not forge the login request message C_1 and C_2. Thus the masquerading user attack is not effective in our scheme. The masquerading server attack could also be resisted due to the secrets m_i and x. Without knowing more than one of the secrets, the adversary could not forge the responding messages C_4 and C_5 used for mutual authentication and key agreement.

4. Brute-Force Guessing and Stolen Verifier Attack

There is no verifier table in our scheme, only a registration table, which is similar to the verifier table, but different from it. If the adversary could get the registration table, it does not threat our scheme without knowing x. Furthermore, it can not reveal any other secret infirmation, such as pw_i, x or $A_i, A'_{i,1}$. In addition, we point that the brute-force guessing attack on secret number x is not effective in our scheme without knowing any other redundant information $A'_{i,1}$ or the others for matching to the guessed values.

5. Secret Key Forward Secrecy

If the secret key x is leaked, the adversary could not get the other secret values or impersonate any participant without knowing the registration table. Because x is used to construct $A'_{i,1}$, which is used to authenticate U_i and compute the message C_4. Besides, there are another two secret information n_i and m_i in the participants' devices, which are unknown for the adversary to construct $A'_{i,1}$. In addition, x could be updated with registration table. After the updating phase, the original secret x is no longer useful with new registration table. Furthermore, the compromised secret key could not affect the security of the previous session keys or users' password, because of the nonces and the DLP on the elliptic curve.

6. Forward Security of The Session Key

The forward security of the session key, which is the basic property of key agreement scheme, is required in our scheme. Our scheme could protect the forward security of the session key. In details, if a session key sk is leaked, no matter is it used or fresh, the other session keys, which is generated in the past or in the future, can be protected to be revealed. The main idea in Diffier-Hellman's key exchange scheme is introduced into our scheme to protect session keys from varies of attacks, such as man-in-the-middle attack, parallel attack and forward security attack.

5. Conclusion

In this paper, we demonstrate that Kim et al.'s scheme is vulnerable to off-line password guessing attack and point out the mistake of secret key forward secrecy in the security analysis. In order to remedy the security flaws, we propose a new password-based authentication with key agreement scheme based upon the discrete logarithm problem on elliptic curve. The enhanced scheme can be implemented using the mobile devices and random numbers, it does not only achieve secure mutual authentication, but also provides the functionalities of key agreement, secrets update, user revocation and DoS-resistant property without using smart cards or synchronization clock system. The security analysis shows that our scheme is secure against the attacks mentioned in this paper. Our scheme is more secure, practical and flexible.

References

[1] H.Y.Chien, J.K.Jan and Y.M.Tseng, An efficient and practical solution to remote authentication: smart card, Computers & Security, 21: **372**, (2002).

[2] C.I.Fan, Y.C.Chan and Z.K.Zhang, Robust remote authentication scheme with smart cards, Computers & Security, 24(8): **619**, (2005).

[3] D.Hankerson, A.Menezes and S.Vanstone, Guide to elliptic curve cryptography (LNCS, Springer-Verlag, New York, USA, 2004).

[4] M.S.Hwang, S.K.Chong and T.Y.Chen, DoS-resistant ID-based password authentication scheme using smart cards, The Journal of System and Software, 83: **163**, (2010).

[5] M.K.Khan and J.Zhang, Improving the security of a flexible biometrics remote user authentication scheme, Computer Standards & Interfaces, 29(1): **82**, (2007).

[6] H.S.Kim, S.W. Lee and K.Y.Yoo, ID-based password authentication scheme using smart cards and fingerprints, ACM SIGOPS Operating Systems Review, 37(4): **32**, (2003).

[7] S.K.Kim and M.G.Chung, More secure remote user authentication scheme, Computer Communications, 32: **1018**, (2009).

[8] N.Koblitz, Elliptic curve cryptosystem, Mathematics of Computation 48: **203**, (1987).

[9] P.Kocher, J.Jaffe and B.Jun, Differential power analysis, Proc. CRYPTO'99: **388**, (1999).

[10] L.Lamport, Password authenticated with insecure communication, Communications of ACM, 24: **28**, (1981).

[11] N.Y.Lee and Y.C.Chiu, Improved remote authentication scheme with smart card, Computer Standards & Interfaces, 27(2): **177**, (2005).

[12] S.W.Lee, H.S.Kim and K.Y.Yoo, Improvement of Chien et al.'s remote user authentication scheme using smart cards, Computer Standards & Interfaces, 27(2): **181**, (2005).

[13] X.F.Leng, Smart card application and security, Information Security Technical Report, 14: **36**, (2009).

[14] T.S.Messerges, E.A.Dabbish and R.H.Sloan, Examining smart-card security under the threat of power analysis attacks, IEEE Transactions on Computers, 5(51): **541**, (2002).

[15] V.S.Miller, Use of elliptic curves in cryptography, Advances in cryptology, proceedings of CRYPTO'85, LNCS, Springer-Verlag, 218: **417**, (1986).

[16] H.S.Rhee, J.O.Kwon and D.H.Lee, A remote user authentication scheme without using smart cards, Computer Standards & Interfaces 31: **6**, (2009).

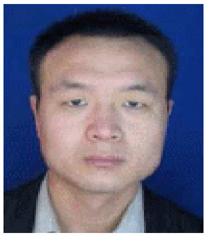
[17] X.Tian, D.S.Wong and R.W.Zhu, Analysis and improvement of authenticated key exchange protocol for sensor networks, IEEE Communications Letters, 9(11): **970**, (2005).

[18] F.Wen, X.Li, An improved dynamic ID-based remote user authentication with key agreement scheme, Comput Electr Eng (2011), doi:10.1016/j.compeleceng.2011.11.010.

[19] J.Xu, W.T.Zhu and D.G.Feng, An improved smart card based password authentication scheme with provable security, Computer Standards & Interfaces, 31: **723**, (2009).

[20] J.H.Yang and C.C.Chang, An ID-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem, Computers & Security, 28(3-4): **138**, (2009).

[21] E.Yoon and K.Yoo, More efficient and secure remote user authentication scheme using smart cards, in the Proceedings of 11th international Conference on Parallel and Distributed System, 2: **73**, (2005).



Xuelei Li is ” MS student in school of mathematical sciences, University of Jinan. He received the BS degree in the department of mathematics, Dezhou College in 2009. The security of computer, networks and information are his research interests.

Fengtong Wen is a associate Professor in school of mathematical sciences, University of Jinan.He received the Ph.D degree in cryptography from BUPT.In 2006,He has published more than 20 research articles in journals of mathematical and engineering sciences.His research interests include cryptography and information security.

Shenjun Cui is ” MS student in school of mathematical sciences, University of Jinan. She received the BS degree in the school of science, University of Jinan in 2009. cryptography is her research interests.