International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:5, No:12, 2011

Three Attacks on Jia et al.'s Remote User Authentication Scheme using Bilinear Pairings and ECC

Eun-Jun Yoon, *Member, IEEE,* and Kee-Young Yoo, *Member, IEEE*

Abstract—Recently, Jia et al. proposed a remote user authentication scheme using bilinear pairings and an Elliptic Curve Cryptosystem (ECC). However, the scheme is vulnerable to privileged insider attack at their proposed registration phase and to forgery attack at their proposed authentication phase. In addition, the scheme can be vulnerable to server spoofing attack because it does not provide mutual authentication between the user and the remote server. Therefore, this paper points out that the Jia et al. scheme is vulnerable to the above three attacks.

Keywords—Cryptography, authentication, smart card, password, cryptanalysis, bilinear pairings.

I. Introduction

IN regards to the Internet, the remote user authentication scheme is an important security mechanism for providing confidentiality and the integrity regarding communication messages. ISO 10202 standards have been established regarding the security of financial transaction systems that use integrated circuit cards (IC cards or smart cards) [1][2]. The main characteristics of a smart card are its small size and low-power consumption. In general, a smart card contains a microprocessor which can quickly manipulate logical and mathematical operations, known as RAM, used as a data or instruction buffer, and ROM, which stores the user's secret key and the necessary public parameters and algorithmic descriptions of the executing programs.

The merits of a smart card regarding password authentication are its simplicity and its efficiency in terms of the log-in and authentication processes. In 1993, Chang et al. [4] proposed a remote password authentication scheme with smart cards. Since then, a number of remote password authentication schemes with smart cards have been proposed [5][6][7][8][9][10].

In 2000, Joux [11] discovered the bilinear computational Diffie-Hellman problem regrading the groups over elliptic curves. This difficult problem can be considered as a new security assumption to develop cryptosystems. Bilinear pairings constitute an effective method to reduce the complexity of the discrete log problem in a finite field and provide an appropriate setting for the bilinear computational Diffie-Hellman problem to be resolved.

E.-J. Yoon is with the School of Computer Engineering, Kyungil University, 33 Buho-Ri, Hayang-Ub, Kyungsan-Si, Kyungsangpuk-Do 712-701, Republic of Korea e-mail: ejyoon@kiu.ac.kr.

K.-Y. Yoo is with the School of Computer Science and Engineering, College of IT Engineering, Kyungpook National University, Daegu 702-701, Republic of Korea e-mail: yook@knu.ac.kr.

Manuscript received July 21, 2011; revised July 21, 2011.

Recently, Das et al. [12] proposed a novel remote user authentication scheme using bilinear pairings, which allows a valid user to log in to the remote server, while prohibiting excessive users' with the same login-ID. In Das et al.'s scheme, time stamps are used to avoid replay attacks while sending an authentication request over a public channel and a flexible password changing function is provided.

However, Chou et al. [13] noted that verification of the scheme involves the subtraction of two components, which are passed over the public channel leading to the replay attack. Replay can be achieved by adding identical information to those two components, resulting in valid verification. To overcome the replay attack, Chou et al. also suggested that a modification was required. However, Thulasi et al. [14] found that both designs as illustrated in [12] and [13], are still insecure against forgery, replay and insider attacks. However, Thulasi et al. did not present a method to overcome these flaws.

Recently, Jia et al. [15] proposed a new remote user authentication scheme using bilinear pairings [11] and an Elliptic Curve Cryptosystem (ECC) [3], which can avoid the noted attacks. However, it was determined that the scheme is vulnerable to two attacks [16][17][18][19][20][21]; (1) Privileged insider attack at their proposed registration phase, in which a malicious insider can easily masquerade as a legal user in order to access the resources of other remote servers by using the obtained password of a legal user, (2) Forgery attack on their proposed authentication phase, in which an attacker easily masquerade as another legal user in order to access the resources of a remote server. In addition, the scheme can be vulnerable to a server spoofing attack because it does not provide mutual authentication between the user and the remote server. Therefore, this paper points out that the Jia et al.'s scheme is vulnerable to the above three attacks. As a result, there is no quick tweak that can be applied to make Jia et al.'s scheme can withstand the attack. For this reason, the Jia et al.'s scheme is insecure for practical application [22][23].

The remainder of this paper is organized as follows: Section 2 summarizes the underlying primitives with respect to the bilinear pairings and ECC based ElGamal cryptosystem. Section 3 reviews Jia et al.'s scheme and then presents and proves its security problems in Section 4. Finally, the conclusion is presented in Section 5.

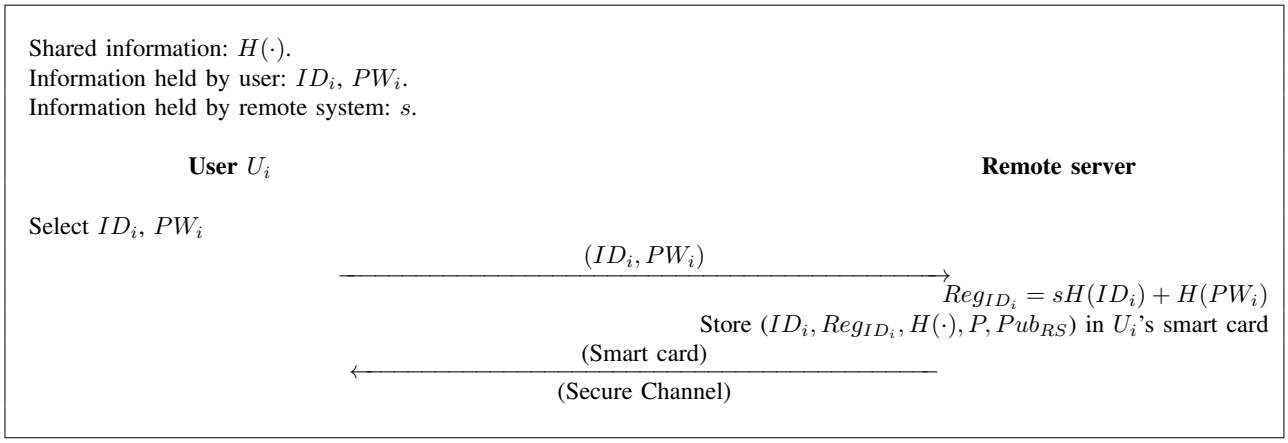

Fig. 1. The registration phase of Jia et al.'s scheme

II. Preliminary Information

This section summarizes the underlying primitives [3][11] used throughout this paper.

A. Bilinear Pairings

Let G_1 be an additive cyclic group generated by P in which the order is a prime q, and G_2 be the multiplicative cyclic group of the same order q. A bilinear pairing is a map $\hat{e} : G_1 \times G_1 \rightarrow G_2$ with the following properties:

1) **Bilinear:** For $\forall P$, $\hat{e}(P+Q,R) = \hat{e}(P,R)\hat{e}(Q,R)$ and $\hat{e}(P,Q+R) = \hat{e}(P,Q)\hat{e}(P,R)$. In particular, for any $a,b \in Z_q^*$, $\hat{e}(aP,bQ) = \hat{e}(P,Q)^{ab} = \hat{e}(P,abQ) = \hat{e}(abP,Q)$.
2) **Non-degenerate:** There exists $P,Q \in G_1$, such that $\hat{e}(P,Q) \neq 1$.
3) **Computable:** There is an efficient algorithm to compute $\hat{e}(P,Q)$ for all $P,Q \in G_1$. We note that the Weil and Tate pairings associated with super singular elliptic curves or varieties can be modified to create such bilinear maps.

B. ECC based ElGamal Cryptosystem

Let $GF(p)$ be a finite field, while p is a large prime integer. The elliptic curve that is often used in the cryptosystem is defined by the equation:

$$y^2 \equiv a^3 + ax + b(\mathrm{mod}p) \tag{1}$$

where $a,b \in GF(p)$ and $4a^3 + 27b^2(\mathrm{mod}p) \neq 0$.

Let $E_p(a,b)$ denote the points over the elliptic curve defined by (1) and a special point O, called the point at infinity. Practically, $E_p(a,b)$ is considered to be an additive group. An elliptic curve cryptosystem using an ElGamal encryption and decryption scheme is defined as follows:

1) Let $P \in E_p(a,b)$ be a fixed point, a public point of $E_p(a,b)$, preferably a generator of $E_p(a,b)$.
2) User A chooses a random integer number s, where s is his/her private key.
3) With the private key, A computes public key $Pub = sP$.
4) User B who wants to transmit the message M to user A encodes the plaintext M onto a point P_m of the elliptic curve $E_p(a,b)$ and chooses a random integer k.
5) Encryption of user B is:
   $C_1 = kP$, $C_2 = P_m + kPub$.
   Here, $\{C_1, C_2\}$ is the ciphertext that can be transmitted to user A over a public channel.
6) Decryption of user A is:

$$\begin{aligned} C_2 - sC_1 &= P_m + kPub - skP \\ &= P_m + k(sP) - skP \\ &= P_m \end{aligned} \tag{2}$$

7) User A decodes P_m and obtains the plaintext M.

Further information regarding the elliptic curve cryptosystem encryption version ElGamal scheme can be found in [3]. If an attacker has $\{C_1, C_2\}$ and wants to obtain P_m, he/she must first get k. However, given P and kP, to compute k is an Elliptic Curve Discrete Logarithm Problem (ECDLP) that cannot be solved within acceptable interval.

III. Review of Jia et al.'s Scheme

This section briefly reviews Jia et al.'s scheme [15]. Jia et al.'s scheme consists of four phases; setup, registration, authentication, and password change.

A. Setup phase

Let G_1 be an additive cyclic group generated by P, in which the order is a prime q, and G_2 be the multiplicative cyclic group of the same order q. Define $\hat{e} : G_1 \times G_1 \rightarrow G_2$ as a bilinear map and $H(0,1)^* \rightarrow G_1$ as a cryptographic hash function. Suppose the remote server (RS) selects a private key s and computes his/her public key as $Pub_{RS} = sP$. Then, the server publishes the parameters $(G_1, G_2, \hat{e}, q, P, Pub_{RS}, H(\cdot))$ and keeps s secret.

B. Registration Phase

A legitimate user must first register with the remote server prior to receiving service from the server. If user U_i wants

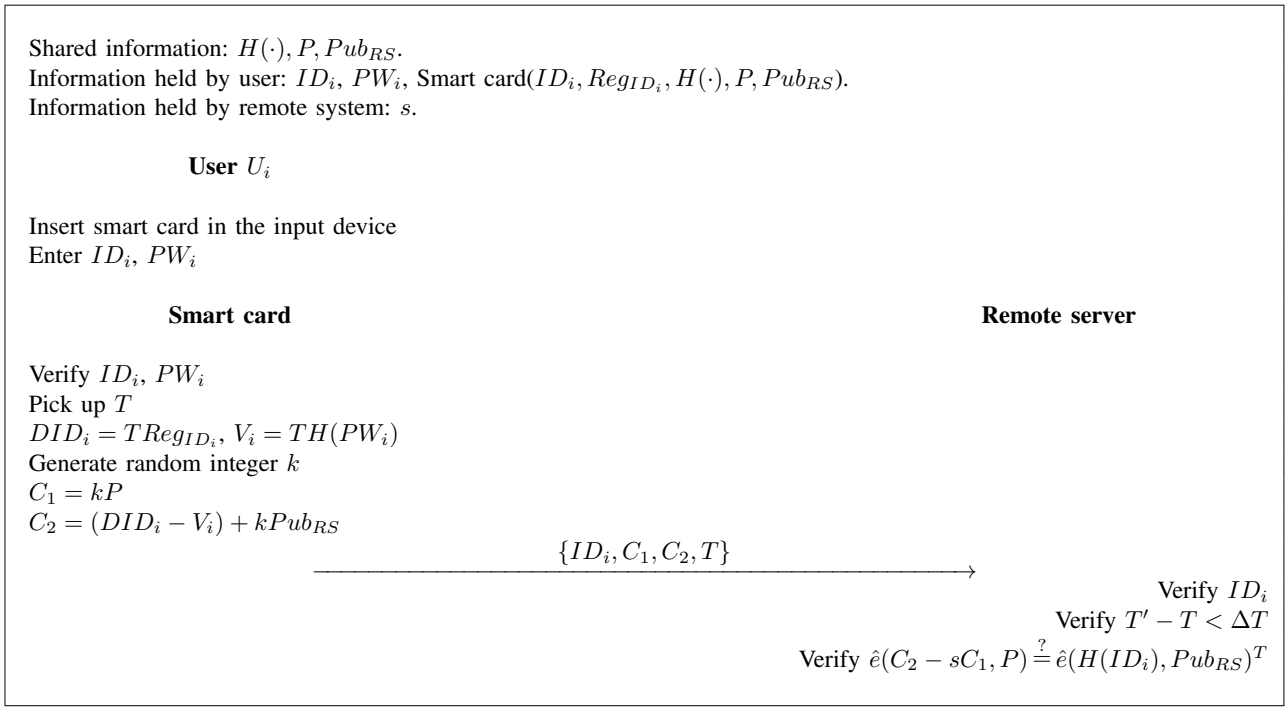

Fig. 2. The authentication phase of Jia et al.'s scheme

to register with the remote server, he/she and the server must execute the following steps:

1) U_i submits his/her identity ID_i and password PW_i to RS.
2) Upon receiving the registration request, RS computes $Reg_{ID_i} = sH(ID_i) + H(PW_i)$.
3) RS personalizes a smart card with the parameters: ($ID_i, Reg_{ID_i}, H(\cdot), P, Pub_{RS}$) and distributes the smart card to U_i over a secure channel.

Figure 1 shows the registration phase of Jia et al.'s scheme.

C. Authentication Phase

The authentication phase includes the user's login and RS's verification. When user U_i wants to log in to RS, he/she and the server must execute the following steps:

1) U_i inserts the smart card into the terminal and inputs his/her identity ID_i and password PW_i. If ID_i and PW_i are identical to those stored in the smart card, the smart card performs the next step.
2) Computes $DID_i = TReg_{ID_i}$, $V_i = TH(PW_i)$, here, T is the user system's timestamp.
3) Chooses a random integer k and computes $C_1 = kP$
4) Computes $C_2 = (DID_i - V_i) + kPub_{RS}$.
5) Sends a login request $\{ID_i, C_1, C_2, T\}$ to the remote server over the public channel.

Upon receiving the login request $\{ID_i, C_1, C_2, T\}$, RS performs the following steps to verify the login request:

6) Verifies the validity time between the RS's timestamp T' and the user system's timestamp T. If $T' - T < \Delta T$, then RS goes to the next step, otherwise it is rejected. Here ΔT denotes the time delay that is tolerable by both the user and the RS.
7) Checks to determine whether

$$\hat{e}(C_2 - sC_1, P) \stackrel{?}{=} \hat{e}(H(ID_i), Pub_{RS})^T \qquad (3)$$

holds or not. If it holds, RS accepts the login request, otherwise it is rejected.

We can easily confirm the validity of equation (2) as follows:

$$\begin{aligned}
\hat{e}(C_2 - sC_1, P) &= \hat{e}(((DID_i - V_i) + kPub_{RS}) - skP, P) \\
&= \hat{e}(DID_i - V_i + skP - skP, P) \\
&= \hat{e}(DID_i - V_i, P) \\
&= \hat{e}(TReg_{ID_i} - TH(PW_i), P) \\
&= \hat{e}(T(sH(ID_i) + H(PW_i)) - TH(PW_i), P) \\
&= \hat{e}(TsH(ID_i) + TH(PW_i) - TH(PW_i), P) \\
&= \hat{e}(TsH(ID_i), P) \\
&= \hat{e}(TH(ID_i), sP) \\
&= \hat{e}(H(ID_i), Pub_{RS})^T.
\end{aligned} \qquad (4)$$

Figure 2 illustrates the authentication phase of Jia et al.'s scheme.

Remarks: In step (1) of the authentication phase, Jia et al. [15] described the following arguments: *"If ID_i and PW_i are identical to those stored in the smart card, the smart card performs the next step."* However, because the password PW_i is never stored into the smart card at the registration phase, the

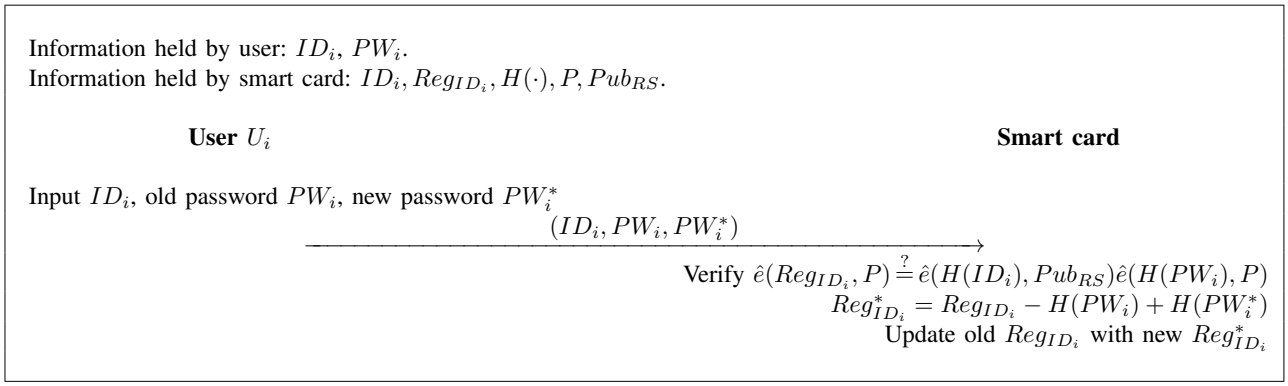

Fig. 3. The password change phase of Jia et al.'s scheme

terminal cannot verify the validity of the input password PW_i. Therefore, the sentence is incorrect. That is, the sentence must be changed to *"If ID_i is identical to one stored in the smart card, the smart card performs the next step."*

D. Password Change Phase

If user U_i wants to change his/her password without the need of RS's participation, he/she needs to perform the following steps:

1) U_i inputs his/her ID_i and old password PW_i.
2) The smart card computes $H(ID_i)$ and $H(PW_i)$.
3) The smart card determines whether
$$\hat{e}(Reg_{ID_i}, P) \stackrel{?}{=} \hat{e}(H(ID_i), Pub_{RS})\hat{e}(H(PW_i), P)$$
holds or not. If it holds the smart card allows the user to change his/her password and go to the next step, otherwise it is rejected.
4) The user inputs a new password PW_i^*.
5) The smart card computes a new $Reg^*_{ID_i} = Reg_{ID_i} - H(PW_i) + H(PW_i^*)$.
6) The smart card updates the old Reg_{ID_i} on the memory of smart card to set the new $Reg^*_{ID_i}$.

Figure 3 illustrates the password change phase of Jia et al.'s scheme.

IV. Cryptanalysis of Jia et al.'s Scheme

This section proves that Jia et al.'s scheme is vulnerable to a privileged insider attack at their proposed registration phase as well as a forgery attack at their proposed authentication phase [16][17]. In addition, the scheme can be vulnerable to a server spoofing attack because it does not provide mutual authentication between the user and the remote server [18][19][20][21].

A. Privileged Insider Attack at the Registration Phase

The registration phase of Jia et al.'s scheme is vulnerable to a privileged insider attack [16][17]. Jia et al. claimed that their scheme can resist an insider attack because the remote server does not maintain the password or verifier table for the login request verification. Contrary to their claims, the scheme still is vulnerable to an insider attack. In practice, it is likely that user U_i uses the same password PW_i to access several servers for his/her convenience. If the insider of the remote server RS has obtained PW_i, he/she can impersonate the user U_i to access other remote servers. In the registration phase of Jia et al.'s scheme, the user U_i sends his/her password PW_i to the RS with plaintext. It is very simple to mount an insider attack because the RS directly knows U_i's password PW_i, an inside attacker may obtain it and use it to login to other remote servers for the purpose of accessing data. Furthermore, if a user loses his/her smart card and it is found out by the insider, or the insider stole the user U_i's smart card, then the insider can easily impersonate the legitimate user U_i by using the password PW_i and the smart card at the authentication phase. Furthermore, if some users utilize the same password for multiple accounts, those will be compromised as well. As a result, Jia et al.'s scheme is vulnerable to an insider attack.

B. User Forgery Attack at the Authentication Phase

The authentication phase of Jia et al.'s scheme is vulnerable to a user forgery attack. In step (7) of the authentication phase, the remote server determines whether $\hat{e}(C_2 - sC_1, P) \stackrel{?}{=} \hat{e}(H(ID_i), Pub_{RS})^T$ holds or not. If it holds, RS accepts the login request. An attacker can easily perform the following user forgery attack to satisfy the verification equation (2):

1) Attacker intercepts a valid old login request $\{ID_i, C_1, C_2, T\}$ over the public channel which had successfully passed the verification equation (2).
2) Attacker chooses system's current timestamp T^*.
3) Attacker computes $C_1^* = T^{-1}T^*C_1 = T^{-1}T^*kP$.
4) Attacker computes $C_2^* = T^{-1}T^*C_2 = T^{-1}T^*((DID_i - V_i) + kPub_{RS}) = T^*Reg_{ID_i} - T^*H(PW_i) + T^{-1}T^*kPub_{RS}$.
5) Attacker sends a forged login request $\{ID_i, C_1^*, C_2^*, T^*\}$ to the remote server over public channel.
6) Upon receiving the forged login request $\{ID_i, C_1^*, C_2^*, T^*\}$, the RS will verify the validity time line between the RS's timestamp T' and the attacker's timestamp T^*. Since $T' - T^* < \Delta T$, the RS will proceed to the next step.

7) RS will determine whether

$$\hat{e}(C_2^* - sC_1^*, P) \stackrel{?}{=} \hat{e}(H(ID_i), Pub_{RS})^{T^*} \quad (5)$$

holds or not.

Since the above verification equation (3) always holds, the RS will accept the attacker's forged login request. We can easily confirm the validity of equation (3) as follows:

$$\begin{aligned}
&\hat{e}(C_2^* - sC_1^*, P) = \hat{e}(T^{-1}T^*C_2 - sT^{-1}T^*C_1, P) \\
&= \hat{e}(T^{-1}T^*((DID_i - V_i) + kPub_{RS}) - sT^{-1}T^*kP, P) \\
&= \hat{e}(T^{-1}T^*((TReg_{ID_i} - TH(PW_i)) + kPub_{RS}) - sT^{-1}T^*kP, P) \\
&= \hat{e}(T^*Reg_{ID_i} - T^*H(PW_i) + T^{-1}T^*kPub_{RS} - sT^{-1}T^*kP, P) \\
&= \hat{e}(T^*sH(ID_i) + T^*H(PW_i) - T^*H(PW_i) + sT^{-1}T^*kP - sT^{-1}T^*kP, P) \\
&= \hat{e}(T^*sH(ID_i), P) \\
&= \hat{e}(T^*H(ID_i), sP) \\
&= \hat{e}(H(ID_i), Pub_{RS})^{T^*}.
\end{aligned} \quad (6)$$

As a result, Jia et al.'s scheme is vulnerable to a user forgery attack.

C. Remote Server Spoofing Attack at the Authentication Phase

The authentication phase of Jia et al.'s scheme is vulnerable to a remote server spoofing attack. Jia et al.'s scheme performs unilateral authentication in that there is only user authentication but no authenticity regarding the remote server. Their scheme contains the risk of manipulating the user's data by setting up a fake server by an attacker [18][19][20][21]. Here, we assume that their scheme is deployed for e-banking or e-commerce applications and, in regarding to these applications, the user also wants to authenticate the validity of the remote party. However, in Jia et al.'s scheme, authentication is only achieved one-way and the user has no way to authenticate the remote server, so cannot trust the originality of the remote server. Hence, their scheme is susceptible to a server spoofing attacks.

V. Conclusions

This paper demonstrated that Jia et al.'s remote user authentication scheme using bilinear pairings and ECC is vulnerable to a privileged insider's attack at the registration phase, and a user forgery attack at the authentication phase. As a result, there is no quick tweak that can be applied to make Jia et al.'s scheme can withstand the attack. For this reason, the Jia et al.'s scheme is insecure for practical application. It is important that security engineers should be made aware of this, if they are responsible for the design and development of secure remote user authentication systems with key agreement. Our future works are to improve the design of the Jia et al.'s remote user authentication scheme, evaluate its efficiency and security, and study its practicality and communication impact.

Acknowledgements

We would like to thank the anonymous reviewers for their helpful comments.

References

[1] P. Peyret, G. Lisimaque and T. Y. Chua, Smart cards provide very high security and flexibility in subscribers management, *IEEE Transactions on Consumer Electronics*, Vol.36, No.3, 1990, pp. 744-752.
[2] D. Sternglass, The future is in the pc cards, *IEEE Spectrum*, Vol.29, No.6, 1992, pp. 46-50.
[3] N. Koblitz, Elliptic curve cryptosystems, *Math. Comp.*, Vol.48, 1987, pp. 203-209.
[4] C. C. Chang and T. C. Wu, Remote password authentication with smart cards, *IEEE Proceedings-E*, Vol.138, No.3,1993, pp. 165-168.
[5] K. Tan and H. Zhu, Remote password authentication scheme based on cross-product, *Computer Communications*, Vol.22, No. 4, 1999, pp. 390-393.
[6] M. S. Hwang, Cryptanalysis of a remote login authentication scheme Computer Communications, *Computer Communications*, Vol.22, No.8, 1999, pp. 742-744.
[7] A. Bottoni and G. Dini, Improving authentication of remote card transactions with mobile personal trusted devices, *Computer Communications*, Vol.30, No.8, 2007, pp. 1697-1712.
[8] J. Y. Liu, A. M. Zhou and M. X. Gao, A new mutual authentication scheme based on nonce and smart cards, *Computer Communications*, Vol.31, No.10, 2008, pp. 2205-2209.
[9] Y. Wang, J. Liu, F. Xiaoa and J. Dana, A more efficient and secure dynamic ID-based remote user authentication scheme, *Computer Communications*, Vol.32, No.4, 2009, pp. 583-585.
[10] H. C. Hsiang and W. K. Shih, Weaknesses and improvements of the yoon-ryu-yoo remote user authentication scheme using smart cards, *Computer Communications*, Vol.32, No.4, 2009, pp. 649-652.
[11] A. Joux, A one round protocol for tripartite diffie-hellman, *Proceedings of Algorithmic Number Theory Symposium*, LNCS 1838, Springer-Verlag, 2000, pp. 385-394.
[12] M. L. Das, A Saxena, V. P. Gulati and D. B. Phatak, A novel remote user authentication scheme using bilinear pairings, *Computers & Security*, Vol.25, No.3, 2006, pp. 184-189.
[13] J. S. Chou, Y. Chen and J. Y. Lin, Improvement of Manik et al.'s remote user authentication scheme, http://eprint.iacr.org/2005/450.pdf.
[14] G. Thulasi, M. L. Das and A. Saxena, Cryptanalysis of recently proposed remote user authentication schemes, http://eprint.iacr.org/2006/028.pdf.
[15] Z. Jia, Y. Zhang, H. Shao, Y. Lin and J. Wang, A remote user authentication scheme using bilinear pairings and ECC, *Proceedings of the Sixth International Conference on Intelligent Systems Design and Applications (ISDA'06)*, Vol.2, October 2006, pp. 1091-1094.
[16] W. C. Ku and S. M. Chen, 'Weaknesses and improvements of an efficient password based remote user authentication scheme using smart cards, *IEEE Trans. on Consumer Electronics*, Vol.50, No.1, 2004, pp. 204-207.
[17] W. C. Ku, H. M. Chuang and M. J. Tsaur, Vulnerabilities of Wu-Chieu's improved password authentication scheme using smart cards, *IEICE Trans. Fundamentals*, Vol.E88-A, No.11, 2005, pp. 3241-3243.
[18] R. J. Anderson, Why cryptosystems fail, *Proceedings of First ACM Conference on Computer and Communications Security*, USA, Nov. 1993, pp. 215-227.
[19] N. Asokan, H. Debar, M. Steiner and M. Waidner, Authenticating public terminals, *Computer Networks*, Vol.31, No.8, April 1999, pp. 861-870.
[20] E. J. Yoon, E. K. Ryu and K. Y. Yoo, An improvement of Hwang-Lee-Tang's simple remote user authentication scheme, *Computers & Security*, Vol.24, 2005, pp. 50-56.
[21] M. K. Khan and J. Zhang, Improving the security of 'a flexible biometrics remote user authentication scheme', *Computer Standards & Interfaces*, Vol.29, 2007, pp. 82-85.
[22] A. J. Menezes, P. C. Oorschot and S.A. Vanstone, *Handbook of applied cryptograph*, CRC Press, New York, 1997.
[23] B. Schneier, *Applied cryptography protocols, algorithms and source code in C: second edition*, John Wiley & Sons Inc, 1995.