Efficient password – authenticated key agreement protocol for smart cards based on ECC

Sheetal Kalra*

Department of Computer Science and Engineering,
Guru Nanak Dev University, Regional Campus Jalandhar,
Punjab, 144001 India
E-mail: sheetal.kalra@gmail.com
*Corresponding author

Sandeep Sood

Department of Computer Science and Engineering,
Guru Nanak Dev University, Regional Campus Gurdaspur,
Punjab, 143521 India
E-mail: san1198@gmail.com

Abstract: Today, networks are no longer limited to servers and desktops. A lot of information transfer is done over mobile devices like smart cards, cell phones, PDAs etc. User authentication and session key agreement is an important aspect of a secure information system. In this paper, we propose an efficient password-authenticated protocol for smart cards which provides user authentication and session key agreement. This protocol is based on ECC and has the following merits: 1) The computation and communication cost is low; 2) The password can be freely chosen by the user; 3) There is no time synchronisation problem; 4) It prevents the offline dictionary attack even if the information stored in the smart card is compromised; 5) It provides for mutual authentication and session key agreement; 6) All well known attacks are prevented using our protocol; 7) The identity of the user changes dynamically for every new session.

Keywords: authentication; dynamic identity; elliptic curve cryptography; ECC; session key; smart cards; network security.

Reference to this paper should be made as follows: Kalra, S. and Sood, S. (2013) 'Efficient password – authenticated key agreement protocol for smart cards based on ECC', *Int. J. Multimedia Intelligence and Security*, Vol. 3, No. 1, pp.80–92.

Biographical notes: Sandeep K. Sood received his MTech (Computer Science and Engineering) in 1999 from the Guru Jambheshwar University Hisar (Haryana), India. He has completed his PhD in the Department of Electronics and Computer Engineering at Indian Institute of Technology Roorkee, India. His research interests include authentication protocols, computer and network security, cryptography and computer networks.

Sheetal Kalra completed her MCA (Masters in Computer Application) in the Department of Computer Science and Engineering in 2006 from Guru Nanak Dev University, Amritsar (Punjab) India. Her area of research includes public key cryptography, authentication protocols and computer network security.

1 Introduction

Authentication is the process of identifying the legitimate user of a particular application. Remote user authentication plays a significant role in implementing the security of such applications. Due to the ease of use, many password based authentication schemes have been developed by the researchers to authenticate legitimate users of various applications available over the internet. In order to login to a remote server, the user submits his identity and password in form of a login message to the server. Then based on the authentication protocol, necessary cryptographic parameters are generated which are used in the process of mutual authentication and key exchange. Mutual authentication is a process where the user and the server mutually authenticate each other's identity using the cryptographic parameters of the authentication protocol.

Smart cards are being widely used in number of network security protocol to achieve mutual authentication and key exchange between the user and the server. Over last few years, number of static identity based security protocols for smart cards have been developed by the researchers. The major drawback of these protocols is that the user may be able to change his password but he cannot change his static identity. The use of static identity may leak partial information about the legitimate user's authentication messages. A malicious user may use this information to launch various attacks on the authentication protocol to gather password of a legitimate user or access the server for his personal benefits. In this paper, we propose a dynamic identity based protocols for smart cards where the identity of a particular user changes for every login to the server. The use of dynamic identity achieves multifactor authentication based on password, identity and smart card and therefore are best suited for e-commerce applications and financial industry.

2 Smart cards and elliptic curve cryptography

Smart card is a tamper proof plastic card, almost the size of a credit card, with an embedded microprocessor and memory used for authentication process. Owing to their number of benefits such as low cost, portability etc., smart cards can be efficiently used to implement password based authentication protocols. Smart cards are mostly used to provide security in electronic processes like financial transactions, personal identification etc. In order to access a particular application, the smart card holder inserts his card into a card reader machine and enters his login ID and password. Based on that, the smart card along with the server computes the necessary cryptographic parameters which are used in the authentication process. In order to make them practical for widespread use, smart cards are constructed in such a way that their cost and size remains restricted. A typical smart card available in the market today has a RAM that ranges between 256 bytes and 1 kb, EEPROM between 1 kb and 16 kb, ROM between 6 kb and 24 kb. They have an inbuilt microprocessor typically clocked at a speed of mere 5 MHz. Any further increase in the processing capacity will increase the size as well as the cost of a smart card. Thus the authentication protocols designed for smart cards must involve minimum computation of the cryptographic parameters. Based upon the chip implanted within the card and the way data is read and written onto the card, smart cards may be divided into various categories such as contactless smart cards, multi-mode communication cards etc.

Key agreement schemes and digital signature schemes greatly benefit from the use of asymmetric cryptosystems (also known as public key systems) over symmetric cryptosystems because the later suffers from the inherent key distribution problem. Therefore the trends in the hardware industry are continuously shifting towards the use of public key systems even for mobile devices. Elliptic curve cryptosystem which is a public key system (PKS) is most suitable for cryptographic operations in constrained devices like smart cards, cell phones etc. Such devices due to their small size operate in constrained environment with limited CPU processing power, memory and bandwidth. In comparison to other PKSs, elliptic curve cryptosystems provide maximum security per bit for a given key size. This means for the same level of security, the length of key required in elliptic curve cryptography (ECC) is much smaller than in other PKS. For e.g., a key size of 166 bits in ECC and 1,024 bits in RSA provides equivalent security (Koblitz et al., 2000). Smaller key size implies faster computation even with limited resources. Thus ECC can very well be implemented in smart cards without increasing its computational resources and consequently its size and cost. Therefore the most efficient way to implement security with smart cards is to use a password based authentication scheme based on ECC.

Table 1 Notations

U_i	User i
S	Server
ID_i	Unique identification of user U_i
P_i	Password of user U_i
X	Private key of server based on ECC
y_i	Server's secret number for user U_i
P_s	Public key of server based on ECC
E_p	Elliptic curve equation over Z_p
P	Large prime number
Z_p	Algebraic group over p
E	Secure symmetric encryption system with secret key
D	Secure symmetric decryption system with secret key
H()	Secure public one way hash function
$\oplus$	XOR operation
$\vert$	Concatenation

3 Related work

Lamport (1981) proposed a password based authentication scheme for remote user authentication over an insecure channel. Since then researchers have proposed several schemes based on password based remote user authentication. All these schemes, have tried to improve Lamport's (1981) scheme in one way or the other. But none of them has succeeded to prevent all well known attacks possible by a malicious user. Password based authentication schemes are susceptible to password guessing attacks which can either be online password guessing or offline password guessing attack. Online password guessing attack can easily be prevented by locking the user's account after certain fixed number of trials. But, offline dictionary attack is a more serious problem where the adversary records the transaction data between the user and the server over a period of attack. An efficient scheme is one that can prevent offline dictionary attack. Another factor which makes most of the existing schemes susceptible to various attacks is the use of static identity for the user of the smart card for every session. The use of static identity leaks out the partial information of the user to the attacker. A solution to this problem is the use of dynamic identity. Use of dynamic identity makes the authentication system more secure to attacks as for every login the identity is computed afresh based on certain specific parameters. Smart card lost problem is still a key issue in many of the proposed schemes till date. Kocher et al. (1999) and Messerges et al. (2002) have mentioned that if the smart card is lost or stolen, the adversary can extract the secret information stored on the smart card by monitoring its power consumption. However, Fan et al. (2005) proposed a scheme in which the smart card lost problem was solved. But, the computation cost of their scheme is high as it is based on integer factoring problem. Liao et al. (2005) proposed a smart card based authentication scheme. But Sood et al. (2010b) analysed their scheme and found that it was susceptible to stolen smart card attack, malicious user attack, impersonation attack and offline password guessing attack. Yoon and Yoo (2006) proposed dynamic identity based mutual authentication as an improvement to Liao et al. (2005) scheme. Liou et al. (2006) proposed a dynamic identity based authentication scheme preserving the merits of Das et al. (2004) scheme and overcoming its drawbacks. Sood et al. (2010a) found that Liou et al. (2006) scheme was also susceptible to malicious user attack, impersonation attack and man-in-the middle attack. Juang et al. (2008) proposed a smart card based authentication scheme based on ECC. Their scheme achieves mutual authentication but the communication cost of the protocol is high. Wang et al. (2009) proposed an authentication scheme based on smart card which was also found susceptible to impersonation, stolen smart card, offline password guessing and denial-of-service attack by Sood et al. (2010b). Song (2010) proposed an advanced smart card based password authentication protocol. Although the scheme is secure against various attacks such as impersonation and man-in-the-middle attack but is computationally inefficient as it is based on exponential computation. Yeh et al. (2011) proposed two robust remote user authentication protocols using smart card in 2010. This scheme was based only on symmetric operations such XOR and Hash functions, still the cost of computation is quite high. Li and Hwang (2010) had developed a multi-factor authentication scheme which combines the advantage of smart card and biometric systems. This scheme is also based on exponential operations thus has a high computational cost as well. Sood (2011a) proposed a smart card based dynamic identity protocol which was secure against most of the well known attacks. But, the scheme had relatively very high cost as the scheme was based on exponential operations. Till date, most of the smart cards based authentication schemes have been based on either low security symmetric cryptography or asymmetric cryptography which involves high cost exponential operations. Very few schemes have been developed by the researchers which are based on ECC. In 2010, a password-authenticated key agreement scheme using smart cards was proposed by Khalique et al. (2010). Their scheme was based on ECC and had relatively low cost as compared to other schemes. Wang et al. (2011) proposed a key agreement mutual authentication scheme based on ECC for smart cards. Their scholarship proves the fact that ECC due to high security and smaller key lengths is best suited for smart cards.

In this paper, we propose a novel and efficient password authenticated and key agreement protocol for smart cards based on ECC. Our protocol is an efficient scheme that provides user authentication, session key agreement, protects user's anonymity, prevents offline dictionary attack even if the information stored in the smart card is compromised, and also our scheme has low communication and computation cost compared to other schemes proposed by the researchers. Our scheme is a dynamic identity based scheme. A nonce based system is used in the scheme so there is no serious time – synchronisation problem.

In Section 4 of this paper, we first review the Sood's (2011b) scheme for smart cards. In Section 5, we propose our robust authenticated scheme based on ECC. In Section 6, we analyse the security of our scheme against all well known attacks. Then a computation and communication cost comparison of other schemes is done with our scheme in Section 7. Section 8 concludes the paper.

4 Review of Sood protocol

In this section, we review the protocol for smart cards proposed by Sood (2011b). It consists of four phases: registration phase, login phase, verification, session key agreement phase and password change phase.

4.1 Registration phase

User registers himself with the server by submitting his identity ID_i and password P_i in encrypted form using a session key SS. The server computes the security parameters $N_i = H(ID_i \mid P_i) \oplus H(X)$, $A_i = H\ (ID_i \mid P_i) \oplus P_i \oplus H(y_i)$, $B_i = y_i \oplus ID_i \oplus P_i$ and $D_i = H\ (H(ID_i \mid y_i) \oplus X)$ where y_i is the server's secret number for user U_i. The server issues the smart card to the user with the parameters $(N_i, A_i, B_i, H\ (\ ))$.

4.2 Login phase

User submits his ID_i^* and P_i^* while login. Then the smart card verifies the user by calculating $y_i^* = B_i \oplus ID_i^* \oplus P_i^*$, $A_i^* = H(ID_i^* \mid P_i^*) \oplus P_i^* \oplus H(y_i^*)$ and compares $A_i*? = A_i$. After that the smart card computes $H(X) = N_i \oplus H\ (ID_i \mid P_i)$, $CID_i = H(ID_i \mid y_i) \oplus H(H(X) \mid T)$ and $M_i = H(ID_i \mid H(X) \mid y_i \mid T)$, where T is current date and time of the input device. The smart card then sends the login request message (CID_i, M_i, T) to the server.

4.3 Verification and session key agreement phase

The server after receiving the login request from the user, checks the validity of timestamp and computes $D_i^* = (CID_i \oplus H(H(X) \mid T) \oplus X)$ and finds D_i corresponding to D_i^* in the database and then finds $y_i \oplus X$ and $ID_i \oplus H\ (X \mid y_i)$ corresponding to D_i^* from the database. Now the server S computes y_i from $y_i \oplus X$ and ID_i from $ID_i \oplus H\ (X \mid y_i)$. After this the server S computes $M_i^* = H\ (ID_i \mid H(X) \mid y_i \mid T)$ and compares $M_i^*? = M_i$.

Upon verifying this, the session SK = $H (H (X) \mid ID_i \mid T \mid y_i)$ is computed and is used for further communication.

4.4 Password change phase

The user inserts his smart card into a card reader and enters his identity ID_i^* and password P_i^*. The smart card computes $y_i^* = B_i \oplus ID_i^* \oplus P_i^*$, $A_i^* = H (ID_i^* \mid P_i^*) \oplus P_i^* \oplus H (y_i^*)$ and compares the computed value of $A_i^*? = A_i$. Once the authenticity of the cardholder is verified, the user U_i enters his new password P_i^{new} and then smart card computes $N_i^{new} = N_i \oplus H (ID_i \mid P_i) \oplus H (ID_i \mid P_i^{new})$, $A_i^{new} = H (IDi \mid P_i^{new}) \oplus P_i^{new} \oplus H (y_i)$ and $B_i^{new} = y_i \oplus ID_i \oplus P_i^{new}$. Then the smart card updates the values of N_i, A_i and B_i stored in its memory with N_i^{new}, A_i^{new} and B_i^{new}.

5 Proposed protocol

In the protocol proposed by Sood (2011b) the authentication scheme is entirely based on symmetric cryptographic primitives of hash functions. In this section, we propose a protocol which is based on the cutting edge technology of ECC. The major advantages of our protocol are:

1 It provides mutual authentication which is a very important security aspect of any key exchange algorithms. Our proposed protocol achieves mutual authentication without significant increase in the computation cost.

2 In Sood's (2011b) protocol the concept of dynamic identity is very well implemented, but it is based on logical clocks which may cause time synchronisation problem. Our proposed protocol uses a nonce based scheme and logical clocks are not used. Hence there is no time synchronisation problem.

3 Asymmetric cryptographic primitives provide maximum security against brute force attacks as compared to symmetric primitives. Moreover, ECC which is based on the hard problem of elliptic curve discrete logarithm problem (ECDLP) and there is no polynomial time algorithm available to solve it. Therefore the use of public key cryptography greatly enhances the security of any authentication scheme. Hence we propose a protocol based on ECC which provides mutual authentication and session key agreement at a low computation cost.

4 The communication cost of our scheme is equivalent to the schemes based on symmetric primitives such as hash functions but is significantly lower than the other schemes based on the ECC. With a low communication cost and increased efficiency our protocol can very well be implemented for smart cards which are constrained devices with limited computational resources. This protocol is a nonce based protocol and the identity of the user changes dynamically every time when the user is authenticated by the server. The user's identity is always hidden to the attacker in an insecure communication channel. This provides an extra level of security and prevents many well known attacks possible otherwise.

Registration phase

In order to become a legitimate user $U_{i,}$ the user submits his identity ID_i and the server issues a password P_i for the user. Then the server computes some security parameters and stores them on the smart card of the user U_i. The smart card is then issued to the user U_i using a secure channel.

Precomputation and login phase

The user inserts his smart card into a card reader to login onto the server S. The user U_i submits his ID_i and P_i. The smart card on verifying the authenticity of the user U_i, sends the user's verifier information to the server. The parameters in the precomputation phase are calculated afresh before every login of the user.

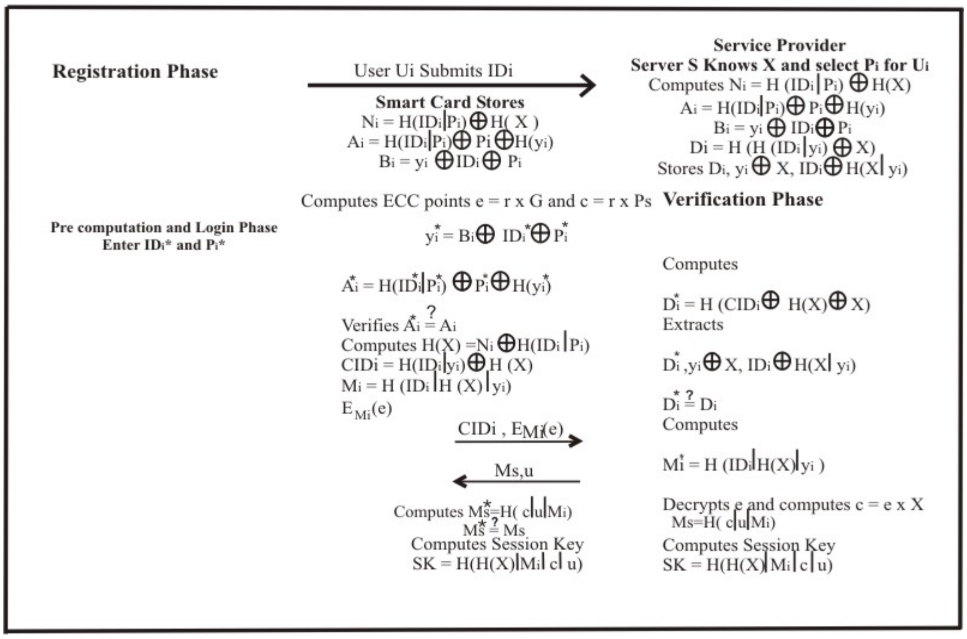
Verification and session key agreement phase

In this phase the server S and user U_i mutually authenticate each other by means of verification information. After mutual authentication, the server S and user U_i agree upon a common session key for further communication.

Password change phase

The user U_i can change his password without the intervention of the server. The user U_i authenticates himself to the smart card before changing his password.

Figure 1 Proposed protocol


Registration Phase
User Ui Submits IDi
Service Provider
Server S Knows X and select P_i for U_i
Computes $N_i = H(ID_i | P_i) \oplus H(X)$
$A_i = H(ID_i | P_i) \oplus P_i \oplus H(y_i)$
$B_i = y_i \oplus ID_i \oplus P_i$
$D_i = H(H(ID_i | y_i) \oplus X)$
Stores D_i, $y_i \oplus X$, $ID_i \oplus H(X | y_i)$
Smart Card Stores
$N_i = H(ID_i | P_i) \oplus H(X)$
$A_i = H(ID_i | P_i) \oplus P_i \oplus H(y_i)$
$B_i = y_i \oplus ID_i \oplus P_i$
Computes ECC points e = r x G and c = r x Ps
Verification Phase
Pre computation and Login Phase
Enter ID_i* and P_i*
$y_i^* = B_i \oplus ID_i^* \oplus P_i^*$
$A_i^* = H(ID_i^* | P_i^*) \oplus P_i^* \oplus H(y_i^*)$
Verifies $A_i^* \overset{?}{=} A_i$
Computes $H(X) = N_i \oplus H(ID_i | P_i)$
$CIDi = H(ID_i | y_i) \oplus H(X)$
$M_i = H(ID_i | H(X) | y_i)$
$E_{Mi}(e)$
CIDi , $E_{Mi}(e)$
Ms,u
Computes $Ms^* = H(c | u | M_i)$
$Ms^* \overset{?}{=} Ms$
Computes Session Key
$SK = H(H(X) | M_i | c | u)$
Computes
$D_i^* = H(CID_i \oplus H(X) \oplus X)$
Extracts
$D_i^*, y_i \oplus X, ID_i \oplus H(X | y_i)$
$D_i^* \overset{?}{=} D_i$
Computes
$M_i^* = H(ID_i | H(X) | y_i)$
Decrypts e and computes c = e x X
$Ms = H(c | u | M_i)$
Computes Session Key
$SK = H(H(X) | M_i | c | u)$

5.1 Registration phase

The server S selects an elliptic curve equation E_p of the form $y^2 = (x^3 + ax + b) \bmod p$ over Z_p such that p is a large prime number $p > 2^{160}$ and $(4a^3 + 27b^2) \bmod p \neq 0$ where a, b ϵ $Z_{p.}$ Let G be the generator point with the prime order n, $n > 2^{160}$ where $n \times G = \boldsymbol{O}$ (point at infinity). The server selects a random number X as its private key and computes its public key $P_s = X \times G$.

1 Every user U_i is associated with a unique identifier ID_i. The user submits his ID_i to the server S using a secure communication channel. At the time of registration, the server chooses a password P_i for the user U_i which he can change immediately on getting the smart card. The server also chooses a random number y_i and computes the following security parameters: $N_i = H(ID_i \mid P_i) \oplus H(X)$, $A_i = H(ID_i \mid P_i) \oplus P_i \oplus H(y_i)$, $B_i = y_i \oplus ID_i \oplus P_i$, $D_i = H(H(ID_i \mid y_i) \oplus X)$. The value of y_i is chosen by the server in such a manner that the value of D_i remains unique for every user. The server stores $y_i \oplus X$ and $ID_i \oplus H(X \mid y_i)$ corresponding to D_i in its database.

2 Using a secure communication channel, a smart card is issued to the user by the server containing the security parameters N_i, A_i, B_i, H( ).

$$\textbf{Server} \rightarrow \textbf{User} : \textbf{Smart Card } (\mathbf{N_i},\ \mathbf{A_i},\ \mathbf{B_i},\ \mathbf{H}(\cdot))$$

5.2 Precomputation and login phase

Before every login the precomputation phase is completed by the smart card and parameters are calculated afresh and stored in the memory of the card reader machine. These parameters are then used at time of login by the user.

1 Smart card selects a random number r in Z_p* and computes $e = r \times G$ and $c = r \times P_s = (r \times X \times G)$. Before every login, smart card computes these points and then it stores (e, c) in the memory of the card reader machine for login.

2 Now, for login the user U_i inserts his smart card into the card reader and submits his ID_i^* and P_i^*. The smart card computes $y_i^* = B_i \oplus ID_i^* \oplus P_i^*$ and $A_i^* = H(ID_i^* \mid P_i^*) \oplus P_i^* \oplus H(y_i^*)$ and compares the value of A_i^* to the stored value of A_i to authenticate the user i.e., $A_i^* ?= A_i$. Here the smart card verifies the user.

3 Smart card computes the following security parameters: $H(X) = N_i \oplus H(ID_i \mid P_i)$, $CID_i = H(ID_i \mid y_i) \oplus H(X)$ and $M_i = H(ID_i \mid H(X) \mid y_i)$. Then smart card encrypts e using M_i as $E_{Mi}(e)$ and sends CID_i and $E_{Mi}(e)$ to the server S as its login request.

$$\textbf{Smart Card} \rightarrow \textbf{Server} : \mathbf{CID_i},\ \mathbf{E_{Mi}(e)}$$

5.3 Verification and session key agreement phase

Server computes the following security parameters after receiving the login request from the user.

1 Server computes $D_i^* = H(CID_i \oplus H(X) \oplus X)$ and finds the D_i equivalent to D_i^* in its database. In case the value of D_i^* does not match with the value of D_i stored in the database, the server revokes the login request and the authentication process is

terminated. At this time smart card is authenticated by the server. After authenticating the smart card, the server S extracts y_i from $y_i \oplus X$ in the database and finds ID_i from $ID_i \oplus H(X \mid y_i)$. Now server computes $M_i^* = H(ID_i \mid H(X) \mid y_i)$. Then the server decrypts e using M_i^* and selects a random number u and computes $c = e \times X$ i.e., $(r \times G \times X)$ and sends $M_s = H(c \mid u \mid M_i)$ and u to the smart card.

$$\textbf{Server} \rightarrow \textbf{Smart Card} : \mathbf{M_s},\ \mathbf{u}$$

Smart card computes $M_s^* = H(c \mid u \mid M_i)$ and compares it to the send value of M_s i.e., $M_s^*?=M_s$. If the values are not equal the smart card revokes the login phase. At this time server is authenticated by the smart card.

2 After the mutual authentication the session key $S_k = H(H(X) \mid M_i \mid c \mid u)$ is computed and used for further communication.

5.4 Password change phase

Before changing the password of the user, the identity and password is verified. The user U_i inserts his smart card into the card reader machine and enters his ID_i and P_i. The smart card computes $y_i^* = B_i \oplus ID_i^* \oplus P_i^*$ and $A_i^* = H(ID_i^* \mid P_i^*) \oplus P_i^* \oplus (y_i^*)$. Then the smart card compares the value of A_i^* with the stored value of A_i. Once the identity of the card holder is verified then he can enter his new password $P^{'}$. The smart card then computes the security parameters based on the new password i.e. $N_i^{'} = N_i \oplus H(\ ID_i \mid P_i\ ) \oplus H(ID_i \mid P_i')$, $A^{'} = H(ID_i \mid P_i^{'}) \oplus P_i^{'} \oplus H(y_i)$ and $B_i' = y_i \oplus ID_i \oplus P_i^{'}$. Password change phase is executed without any intervention of the server.

6 Security analysis

On monitoring the power consumption and using certain reverse engineering processes the sensitive information on the smart card can be compromised. So in case the user loses his smart card, an adversary can miss use this information for his benefits. An efficient password based authentication is one that prevents all well known attacks even if the information stored on the smart card is compromised. In this section, we analyse the security of the proposed protocol.

1 Provides mutual authentication: the major benefit of our scheme is that it provides mutual authentication. Not only the server has a chance to validate the smart card but the smart card also validates the authenticity of the server. In our protocol the security parameters (CID_i, $E_{Mi}(e)$) validate the smart card and the parameters (M_s, u) validate the authenticity of the server.

2 Preventing time synchronisation problem: major of the existing protocols makes use of logical clock to prevent replay attacks. The proposed scheme is a nonce based scheme and does not require any logical time clocks.

3 Preventing offline dictionary attack: in this type of attack the malicious user records the transaction data and attempts to guess the user's identity and password from the tapped messages. In our protocol on obtaining the transaction data $CID_i = H(ID_i \mid y_i) \oplus H(X)$ and $M_i = H(ID_i \mid H(X) \mid y_i)$ of the user U_i , the attacker will try to guess ID_i,

y_i and H(X). It is not possible for the attacker to guess all three parameters correctly at the same time in real polynomial time.

4 Preventing stolen smart card attack: in this type of attack the attacker can extract the information stored on the smart card. In our protocol the smart card stores N_i = H (ID_i | P) ⊕ H (X), A_i = H (ID_i | P_i) ⊕ P_i ⊕ H(y_i) and B_i = y_i ⊕ ID_i ⊕ P_i. But even after getting this information the attacker cannot generate CID_m = H(ID_m | y_m) ⊕ H(X) and M_m = H(ID_m | H(X) | y_m) as another legitimate user U_m. This is because he cannot calculate the values of ID_m and y_m even if he can find H(X) from his own smart card.

5 Preventing replay attack: in replay attack the malicious user tries to imitate as a legitimate user U_i by first listening to the communication channel and then trying to login to the server by replaying the same transmission data. But our protocol is nonce based protocol and the identity of the user changes dynamically with every login. The random numbers r and u are selected afresh for every login by the smart card and server respectively which hides the real identity of the user.

6 Preventing denial of service attack: if the attacker manages to get the smart card of a legitimate user, he may update the password so that the user U_i cannot access his card. This type of attack is known as denial of service attack. But in our protocol, the smart card verifies the identity ID_i and password P_i in the password change phase. In this phase the smart card computes y_i* = B_i⊕ ID_i* ⊕ P_i* and then A_i* = H(ID_i*|P_i*) ⊕ P_i* ⊕ H(y_i*), after which it compares the value of A_i and A_i*. In real polynomial time it is not possible to guess the value of ID_i and P_i correctly at the same time.

7 Preventing impersonation attack: impersonation is when the attacker forges the authentication messages of a legitimate user and the tries to modify the login request into CID_i*, E_{Mi}(e)* from CID_i, E_{Mi}(e). But attacker cannot obtain the correct values of ID_i, H(X) and y_i for computing the authentication parameters CID_i*, E_{Mi}(e)*. Therefore this type of attack will fail in very first step of verification and session key agreement phase of our protocol.

8 Preventing leak of verifier attack: this is the most common type of attack where the information stored on the server is compromised to calculate the security parameters. In our protocol the server stores y_i ⊕ X and ID_i ⊕ H(X | y_i) corresponding to D_i in its database. The attacker cannot find X as it is the master secret of the server S and therefore is unable to calculate y_i and ID_i from y_i ⊕ X and ID_i ⊕ H(X | y_i) respectively.

9 Preventing online dictionary attack: in case the attacker manages to get the smart card of a legitimate user U_i, and tries to login by guessing various user ID and password from the dictionary. But in our protocol it is not possible to guess the ID_i and P_i together in real polynomial time. Hence our protocol is safe against his type of attack also.

10 Preventing malicious user attack: in this type of attack a malicious user has his own smart card and can use it to gather various security parameters such as N_i = H(ID_i | P_i) ⊕ H(X) , A_i = H (ID_i |P_i) ⊕ P_i ⊕ H(y_i) and B_i = y_i ⊕ ID_i ⊕ $P_{i.}$ But he cannot generate smart card specific parameters CID_m = H(ID_m | y_m) ⊕ H(X) and M_m = H(ID_m | H(X) | y_m) for masquerading as another legitimate user U_m. This is because the values of CID_m and M_m are dependent on the values of ID_m, y_m and H(X) and there is no way to calculate ID_m and y_m from his own card.

11 Preventing server spoofing attack: in this type of attack the malicious user may set up a fake server by manipulating the security parameters of a legitimate user. But in our protocol, the session key $S_k = H(H(X) | M_i | c | u)$ cannot be computed by the malicious server as it has no way of computing the value of H(X), M_i and the entropies of c and u are very high. Also, the session key is calculated using a nonce and hence is different for every login session of the same user U_i.

7 Cost and functionality analysis

The communication and computation cost must be low for an authentication scheme to be efficient. The comparison of computation and communication cost is done in Table 2. Table 3 gives the functional comparison among various schemes based on smart cards and our scheme. We suppose that the password P_i, identity ID_i, X, y_i and block size of the secure symmetric cryptosystem all are 128-bit long. Also, the output size of the secure one-way hash function is 128 bits. Let T_H, T_E, T_S, T_{ECM} be the time for one hashing operation, one exponential operation, one symmetric or decryption operation and time for one multiplication of a number over elliptic curve respectively. The memory of the smart card stores N_i, A_i, B_i in our protocol. Therefore the memory needed in the card (E1) is 3 * 128 = 384 bits. The total number of bits transmitted in the authentication scheme is the communication cost for authentication (E2). In our protocol the total numbers of bits that travel are (CID_i, $E_{Mi}(e)$, M_s, u) i.e., 128 + 128 + 128 + 64 = 448 bits where u can be 64 bits and the output of the hash function and encryption system is 128 bits. The total time involved in the registration process is given by the parameter (E3). In our protocol it is $6T_H$. The parameters E4 and E5 represent the total time involved in the authentication process by the user and server respectively. In our protocol E4 is ($2T_{ECM} + 1T_S + 5T_H$) and E5 is ($1T_S + 4T_H$). Thus with a low communication and computational cost our proposed scheme provides security against all the well known attacks.

Table 2 Cost comparison among the related smart card schemes

	E1(bits)	*E2(bits)*	*E3*	*E4*	*E5*
Proposed protocol	384	448	$6T_H$	$5T_H + 1T_S + 2T_{ECM}$	$4T_H + 1T_S$
Juang et al. (2008)	640	1088	$2T_H + 1T_S$	$3T_H + 1T_S + 2T_{ECM}$	$4T_H + 2T_S + 1T_{ECM}$
Sood (2011)	384	384	$6T_H$	$6T_H$	$6T_H$
Wang et al. (2009)	256	768	$2T_H$	$3T_H$	$3T_H$
Liou et al. (2006)	384	640	$3T_H$	$4T_H$	$4T_H$
Yoon-Yoo (2005)	384	768	$3T_H$	$6T_H$	$4T_H$
Liao et al. (2005)	256	768	$2T_H$	$5T_H$	$4T_H$
Chien-Chen and Chen (2004)	384	512	$2T_H$	$2T_S + 2T_E$	$2T_H + 2T_S + 2T_E$
Das et al. (2004)	256	512	$2T_H$	$4T_H$	$3T_H$
Sood et al. (2010a)	384	384	$4T_H$	$7T_H$	$5T_H$

Notes: E1 Memory needed in the smart card
E2 Communication cost of authentication
E3 Communication cost of registration
E4 Computation cost of the user
E5 Computation cost of the service provider server

Table 3 Functionality comparison among smart card based authentication schemes

	C1	*C2*	*C3*	*C4*	*C5*	*C6*	*C7*	*C8*
Proposed scheme	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Juang et al. (2008)	Yes	Yes	Yes	No	Yes	Yes	No	Yes
Sood (2011)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
Wang et al. (2009)	No	No	No	No	No	No	No	No
Liou et al. (2006)	Yes	No	No	No	No	No	Yes	No
Yoon-Yoo (2005)	Yes	No	Yes	Yes	No	Yes	Yes	No
Liao et al. (2005)	Yes	No	No	No	No	No	No	No
Chien-Chen and Chen (2004)	Yes	Yes	Yes	Yes	Yes	No	Yes	No
Das et al. (2004)	Yes	No	No	No	No	No	No	No
Sood et al. (2010a)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No

Notes: C1 User’s anonymity
C2 Session key agreement
C3 Prevention from impersonation attack
C4 Prevention from malicious user attack
C5 Prevention from offline dictionary attack
C6 Prevention from stolen smart card attack
C7 Prevention from denial of service attack
C8 No time synchronisation

8 Conclusions

With the rapid development in network technologies like wireless networks, number of e-commerce applications have become popular. So a lot of sensitive information travels over the networks. In such a scenario, user authentication becomes very vital for a cooperate network to flourish. Password based authentication schemes using a smart card make an ideal choice for e-commerce applications over the cooperate networks. We have proposed an efficient scheme for smart cards based ECC. The use of ECC provides all the benefit of using an asymmetric cryptosystem even for a constrained environment of a typical smart card. With a low computational and communication cost it prevents all well known attacks by the malicious users of the network. The future scope includes the implementation of the protocol in an experimental setup using Java card.

References

Chien, H.Y. and Chen, C.H. (2004) ‘A remote authentication scheme preserving user anonymity’, *Proc. Advanced Information Networking and Applications*, Vol. 2, pp.245–248.

Das, M.L., Saxena, A. and Gulati, V.P. (2004) ‘A dynamic ID based remote user authentication scheme’, *IEEE Transactions on Consumer Electronics*, Vol. 50, No. 2, pp.629–631.

Fan, C., Chan, Y. and Zhang, Z. (2005) ‘Robust remote authentication scheme with smart card’, *Computer Security*, Vol. 24, No. 8, pp.619–628.

Juang, W.S.,Chen, S.T. and Liaw, H.T. (2008) ‘Robust and efficient password –authenticated key agreement using smart cards’, *IEEE Transactions on Industrial Electronics*, Vol. 55, No. 6.

Khalique, A., Singh, K. and Sood, S. (2010) 'A password-authenticated key agreement scheme based on ECC using smart cards', Vol. 2, No. 3, pp.26–30.

Koblitz, N., Menezes, A. and Vanstone, S. (2000) 'The state of elliptic curve cryptography', *Designs, Codes Cryptography*, March, Vol. 19, Nos. 2/3, pp.173–193.

Kocher, P., Jaffe, J. and Jun, B. (1999) 'Differential power analysis', *Proc. CRYPTO 99*, pp.388–397.

Lamport, L. (1981) 'Password authentication with insecure communication', *Communications of the ACM*, November, Vol. 24, No. 11, pp.770–772.

Li, C.T. and Hwang, M.S. (2010) 'An efficient biometrics-based remote user authentication scheme using smart cards', *Journal of Network and Computer Applications*, Vol. 33, No. 1, pp.1–5.

Liao, I.E., Lee, C.C. and Hwang, M.S. (2005) 'Security enhancement for a dynamic ID-based remote user authentication scheme', *Proc. Conference on Next Generation Web Services Practice*, pp.437–440.

Liou, Y.P., Lin, J. and Wang, S.S. (2006) 'A new dynamic ID-based remote user authentication scheme using smart cards', *Proc. 16th Information Security Conference*, pp.198–205.

Messerges, T.S., Dabbish, E.A. and Sloan, R.H. (2002) 'Examining smart card security under the threat of power analysis attacks', *IEEE Transactions on Computers*, Vol. 51, No. 5, pp.541–552.

Preneel, B.(2007) 'A survey of recent developments in cryptographic algorithms for smart cards', *Computer Networks*, Vol. 51, No. 9, pp.2223–2233.

Song, R. (2010) 'Advanced smart card based password authentication protocol', *Computer Standards & Interface*, Vol. 32, Nos. 5/6, pp.321–325.

Sood, S.K. (2011a) 'An improved and secure smart card based authentication scheme', *International Journal of Multimedia and Security*, Vol. 2, No. 1, pp.75–89.

Sood, S.K. (2011b) 'Secure dynamic identity – based authentication scheme using smart cards', *Information Security Journal: A Global Perspective*, Vol. 20, No. 2, pp.1–11.

Sood, S.K., Sarje, A.K. and Singh, K. (2010a) 'An improvement of Liou et al.'s authentication scheme using smart cards', *International Journal of Computer Applications*, Vol. 1, No. 8, pp.17–24.

Sood, S.K., Sarje, A.K. and Singh, K. (2010b) 'An improvement of Liao et al.'s authentication scheme using smart cards', *Proc. 2nd IEEE International Advance Computing Conference*, February, pp.240–245.

Wang, R.C., Juang, W.S. and Lei, C.H. (2011) 'Robust authentication and key agreement scheme preserving the privacy of secret key', *Computer Communications*, Vol. 34, No. 3, pp.274–280.

Wang, Y., Liu, J., Xiao, F. and Dan, J. (2009) 'A more efficient and secure dynamic ID based remote user authentication scheme', *Computer Communications*, Vol. 32, No. 4, pp.583–585.

Yeh, K., Su, C., Li, Y. and Hung, Y. (2011) 'Two robust remote user authentication protocols using smart cards', *The Journal of Systems and Software*, Vol. 83, No. 12,pp.2556–2565.

Yoon, E. and Yoo, K. (2005) 'More efficient and secure remote user authentication scheme using smart cards', *Proc. of 11th International Conference on Parallel and Distributed System*, July, Vol. 2, pp.73–77.