First International Conference on Emerging Trends in Engineering and Technology

A Novel Protocol for Smart Card Using ECDLP

Debasish Jena[1], Saroj Kumar Panigrahy[2], Pradip Kumar Biswal[3], Sanjay Kumar Jena[4]
[1, 3] *Centre for IT Education, Bhubaneswar-750 010, Orissa, India*
[2, 4] *National Institute of Technology Rourkela, Rourkela-769 008, Orissa, India*
debasishjena@hotmail.com, skp.nitrkl@gmail.com, pkbiswal@hotmail.com, skjena@nitrkl.ac.in

Abstract

In this paper, we propose a novel protocol for smart card based on Elliptic Curve Discrete Logarithm Problem (ECDLP). We believe that applications of smart card technology should be benefited more from advantages of public key cryptography, specifically, in initiation and maintenance of secure channel. This paper introduces a public key cryptographic protocol for secure entity authentication, data integrity and data confidentiality. The proposed secure channel protocol uses a combination of secure public key system, secret key and a use of public encryption system to achieve the desired goal. In this paper, signature authentication along with signature encryption for smart card based on Digital Signature Authentication (DSA) using ECDLP has been proposed. Signature encryption is useful in protocols that guarantee the anonymity of the participants and its message. The proposed scheme can be easily extended to M-Commerce, Financial transactions and healthcare applications, where, the requester needs a signature on the message.

Keywords- *Smart Card, Digital Signature, Elliptic Curve, ElGamal, Digital Cash, RSA, ECDLP.*

1. Introduction

Over the years sub-exponential time algorithms were developed to solve cryptographic application problems [1, 2], which are based on the intractability of hard mathematical problem such as integer factorization. As a result, key size grew more than 1000 bits. So as to attain a reasonable level of security in constrained environments, where bandwidth minimization, computational problem and memory utilization is a great issue, carrying out thousand bit operations becomes an impractical approach to providing adequate security. This is more evident in the mobile phones, pagers and PDAs that has very limited power and battery life.

In this paper, we propose a new protocol based on DSA using ECDLP. This paper aims to examine two aspects of elliptic curve cryptography (ECC), namely, its security and efficiency, so as to provide grounds as to why the ECC is most suitable for constrained environments. We begin by introducing the different mathematical problems and the various algorithms that solve them. An overview of implementation methods and considerations will be provided followed by comparisons in the performance of ECC with other public key cryptography (PKC). Lastly, validity of the proposed scheme has been made.

With growing importance of sender privacy in smart card such as “digital cash” protocol, signature schemes are gaining momentum. Smart card protocol is a form of digital signature in which the signer will have to ask for the certificate from the Certifying Authority, as also a third party (Banker) could able to verify without knowing the secrets of both the parties that are involved in signature. The electronic payment system is one of the most important applications in electronic commerce. The services need to be authenticated and secure. Non-repudiation is one of the vital aspects where the requester and the service providers can be prohibited of denying the action made on the transaction made between them. Signature scheme is most widely used mechanism for the purpose. Anyone who has a smart card will able to communicate securely with the servers. Security is the major concern for smart card system and cryptography is the best solution. A digital certificate contains public key of the user which is signed by the certifying authority digitally. In order to verify the certificate zero knowledge proof has been used.

The rest of the paper is organized as follows. In section 2, basic concept of elliptic curve is discussed. In section 3, the proposed protocol is discussed using a communication illustration between a requester and a signer. The correctness of the proposed protocol has been made in section 4. In section 5, online digital cash transaction in banking system is explained where

978-0-7695-3267-7/08 $25.00 © 2008 IEEE
DOI 10.1109/ICETET.2008.126

IEEE computer society

proposed protocol is being used. Finally, section 6 describes the concluding remarks.

2. Elliptic Curve over Finite Field

The use of Elliptic Curve Cryptography was initially suggested by Neal Koblitz [3] and Victor S. Miller [2] and after that many researchers have suggested different applications of Elliptic Curve Cryptosystems. Elliptic curve cryptosystems over finite field have some advantages like (i) the key size can be much smaller compared to other cryptosystems like RSA, Diffie-Hellman since, only exponential-time attack is known so far, if the curve is carefully chosen [3] and (ii) elliptic curve discrete logarithms might be still intractable even if factoring and multiplicative group discrete logarithm are broken. ECC is also computationally efficient than the first generation public key systems such as RSA and Diffie-Hellman.

2.1. Elliptic curve groups over F_q

A non-super singular Elliptic curve E over F_q can be written as

$$E: y^2 \bmod q = (x^3 + ax + b) \bmod q \qquad \ldots (1)$$
$$\text{where } (4a^3 + 27b) \bmod q \neq 0$$

The point P in the Elliptic curve is described by the coordinates (x, y) where $x, y \in F_q$ that satisfies the equation (2) together with a "point of infinity" denoted by O form an abelian group $(E, +, O)$ whose identity element is O.

2.1.1. Addition of two distinct points P and Q. The negative of the point $P = (x_1, y_1)$ is the point $-P = (x_1, -y_1)$. If $P(x_p, y_p)$ and $Q(x_q, y_q)$ are two distinct points such that P is not $-Q$, then

$$P + Q = R \qquad \ldots (2)$$
$$\text{where } R = (x_r, y_r)$$
$$s = (y_p - y_q)/(x_p - x_q) \bmod \quad q \qquad \ldots (3)$$

where *s* is the slope of the line passing through P and Q

$$\begin{aligned} x_r &= (s^2 - x_p - x_q) \bmod \quad q \\ y_r &= (-y_p + s * (x_p - x_r)) \bmod q \end{aligned} \qquad \ldots (4)$$

2.1.2. Doubling the point P. Provided that y_p is not 0,

$$\begin{aligned} &2P = R \\ &\text{where R} = (x_r, y_r) \end{aligned} \qquad \ldots (5)$$
$$s = ((3x_p^2 + a)/(2y_p)) \bmod q \qquad \ldots (6)$$
$$\begin{aligned} x_r &= (s^2 - 2x_p) \bmod q \\ y_r &= (-y_p + s(x_p - x_r)) \bmod q \end{aligned} \qquad \ldots (7)$$

The elliptic curve discrete logarithm problem is defined as follows [14].

Definition 1. Let E be an elliptic curve over a finite field F_q and let $P \in E(F_q)$ be a point of order n. Given $Q \in E(F_q)$, the elliptic curve discrete logarithm problem is to find the integer $d \in [0, n-1]$, such that $Q = dP$.

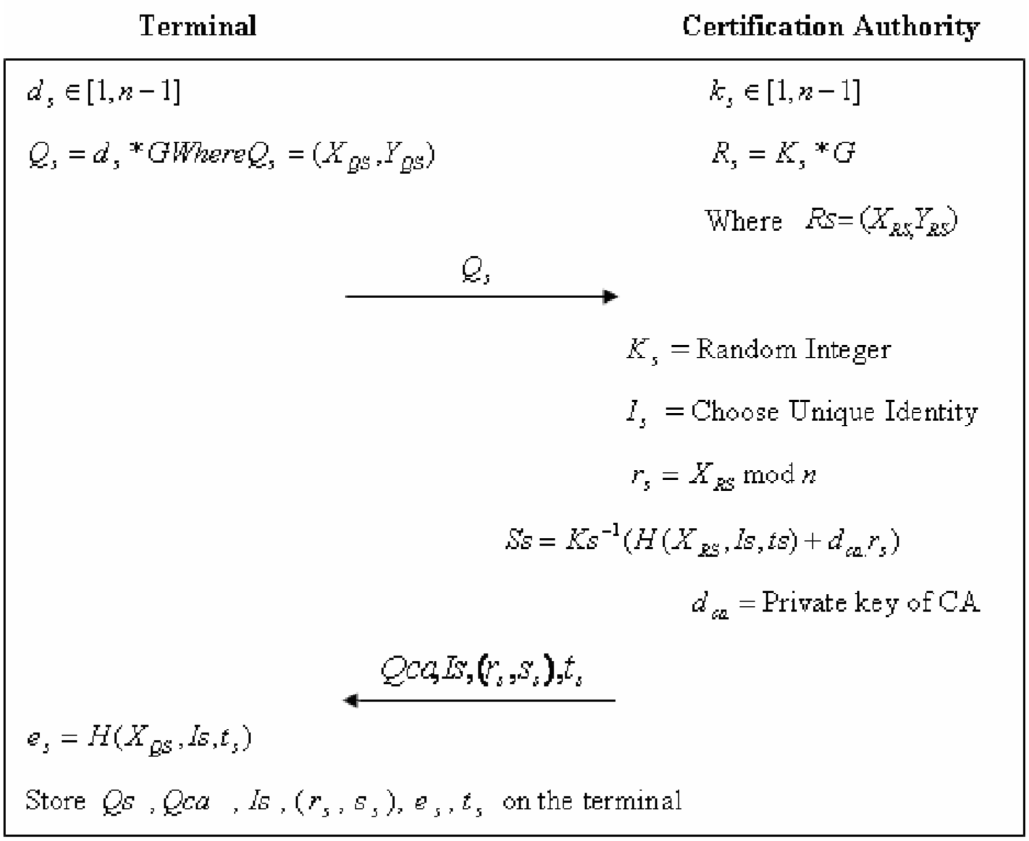
3. Proposed protocol for smart card

We propose a novel efficient and low computation protocol. Initially the curve parameters [7, 8, 9] must be agreed upon by terminal and certifying authority. Signer must have a key pair suitable for elliptic curve cryptography [10, 11], consisting of a private key d_u (a randomly selected in the interval $[1, n-1]$) and a public key Q where $Q = d_u G$. When a signer wants to send a signed message m to receiver, he/she must generate a digital signature [4]. The steps for our proposed protocol for smart card are explained as follows:

1. *Terminal* is a host defined as an off-card entity that requires establishing a secure channel with the smart card, application or smart card operating system (SCOS) as shown in Figure 1, i.e., what terminal initialization has to be made.

2. *Card/User* represents smart card. Typically a sufficient tamper resistant device which is relatively difficult to compromise; it has access to a variety of cryptographic algorithms and a good random number generator. A multi-application smart card platform will provide significant functionality that will strengthen the overall concept of dynamic application management as shown in Figure 2, i.e., what card initialization has to be made.

3. All entities share public values, i.e., large prime multiplicative order modulo p.



Terminal

Certification Authority

$d_s \in [1, n-1]$

$Q_s = d_s * G Where Q_s = (X_{QS}, Y_{QS})$

$k_s \in [1, n-1]$

$R_s = K_s * G$

Where $Rs = (X_{RS,} Y_{RS})$

Q_s

K_s = Random Integer

I_s = Choose Unique Identity

$r_s = X_{RS} \bmod n$

$Ss = Ks^{-1}(H(X_{RS}, Is, ts) + d_{ca}.r_s)$

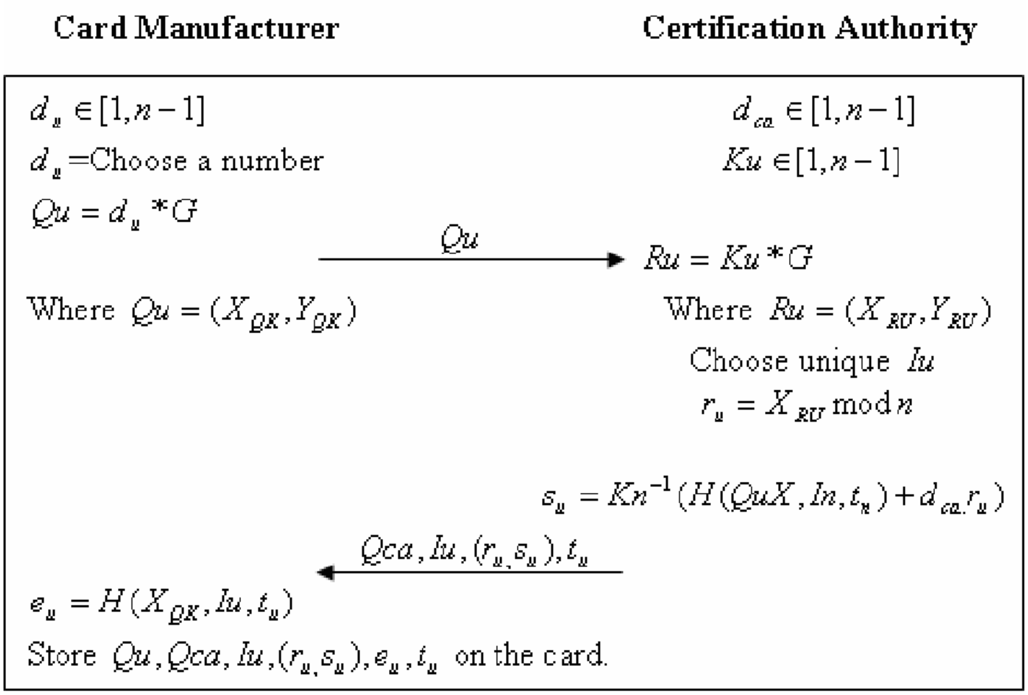
d_{ca} = Private key of CA

$Qca, Is, (r_s, s_s), t_s$

$e_s = H(X_{QS}, Is, t_s)$

Store Qs , Qca , Is , (r_s, s_s), e_s, t_s on the terminal

Figure 1. Terminal initialization



Card Manufacturer

Certification Authority

$d_u \in [1, n-1]$

d_u =Choose a number

$Qu = d_u * G$

$d_{ca} \in [1, n-1]$

$Ku \in [1, n-1]$

Qu

$Ru = Ku * G$

Where $Qu = (X_{QX}, Y_{QX})$

Where $Ru = (X_{RU}, Y_{RU})$

Choose unique Iu

$r_u = X_{RU} \bmod n$

$s_u = Kn^{-1}(H(QuX, In, t_u) + d_{ca}.r_u)$

$Qca, Iu, (r_u, s_u), t_u$

$e_u = H(X_{QX}, Iu, t_u)$

Store $Qu, Qca, Iu, (r_{u,} s_u), e_u, t_u$ on the card.

Figure 2. Card initialization

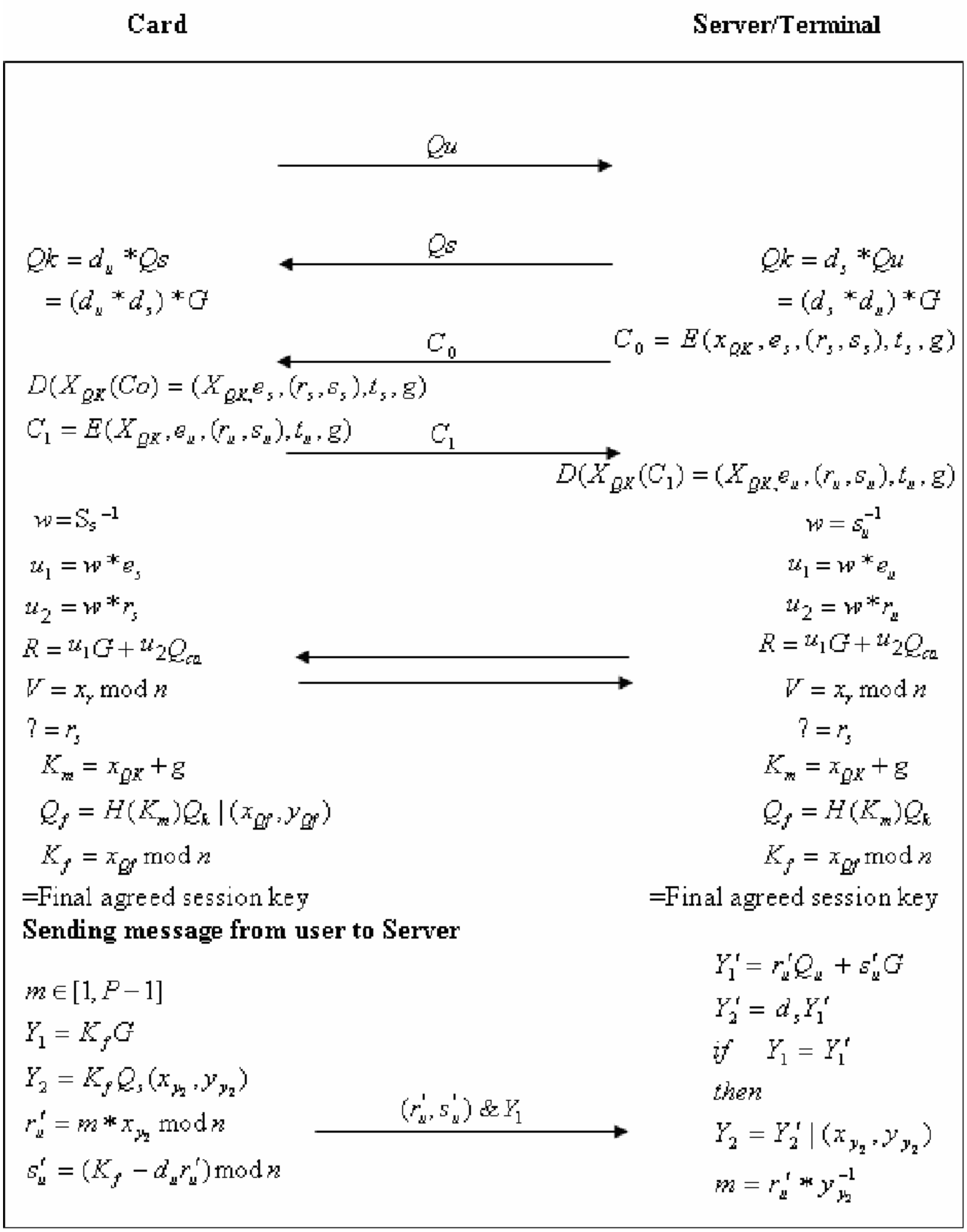


Figure 3. Mutual Authentication & Message Recovery

4. Each card has a Diffie-Hellman key agreement key pair. More specifically, card has private key agreement key y with corresponding public key Q_s. The card's key pair can be either generated off-card by the issuer or the application provider and subsequently loaded onto the card, or it can be generated on-card (if the functionality is provided by the card). In either case the public key has to be certified by the corresponding off-card entity, i.e., the issuer or an application provider.

5. The terminal has an ECC public encryption key, which is certified by the corresponding certification authority as shown in Figure 1.

6. The card and the terminal share a symmetric cryptosystem and a key generation function (e.g., a one- way function).

7. The card is capable of generating random numbers.

8. Each card (e.g., through a security domain) has a trusted copy of its owner's (e.g., certification authority, issuer or application provider) public certification key, whose corresponding private key is used by the off-card entity for issuing certificates (i.e., for the ECC keys) as shown in Figure 3.

Select K randomly between [1, $n-1$] and generate R , r , and s as after receiving (r,s) from signer, the receiver can verify the correctness of the signature on the message. Mutual authentication and key agreement between the terminal and the smart card is described in Figure 3.

Whenever there is a service request either by the card or by the terminal, there is an immediate key exchange. Once both the parties have the public key of one another then by using their private key, they can generate the secret key to encrypt the data required to have the mutual authentication. To protect the certificate from eavesdropper, it is sent through the encrypted format using the mutually agreed secret key x_{QK} .The server concatenates the certificate through the $e_s,(r_s,s_s),t_s,g$ to obtain the final mutual key of authentication. The encrypted message Co is then sent to the user then decrypts Co and then obtains the certificate and the generator g . The user then encrypts the data with the concatenation of $e_u,(r_u,s_u)$ with the certificate expiration date t_u and the random generator g . The encrypted data is known as C_1 , it is sent to the server which is then decrypted with the mutually agreed key and checks that whether g and t_u are valid or not. If it is valid, then the server finds the followings:

$$w = S_s^{-1}$$
$$u_1 = w * e_u$$
$$u_2 = w * r_u$$
$$R = u_1 G + u_2 Q_{ca}$$
$$V = x_r \bmod n$$

By using the previously known generator g, find K_f which will be the final session key. With the help of K_f , similarly, at the user end message is encrypted and sent to the server, where verification is done and message is decrypted as shown in Figure 3.

4. Correctness of the proposed protocol

The verifier only verifies the pair (r,s) and message m by using the equations given in Figure 3. The correctness of the equation is as follows. The verifier has only digital signature (r,s,R) of message m for verification. The customer extracts the signature by using the equations given in Figure 3, therefore

$$\begin{aligned} Y_1' &= r_u' Q_u + s_u' G \\ &= r_u' d_u G + (K_f - d_u r_u') G \\ &= K_f G \\ &= Y_1 \end{aligned}$$

If $Y_1' = Y_1$ then

$$\begin{aligned} Y_2' &= d_s Y_1' \\ &= d_s Y_1 \\ &= d_s K_f G \\ &= Y_2 \end{aligned}$$

5. Transaction using the proposed protocol

The following procedure explains an untraceable off-line electronic payment protocol assuming that the consumer wants to purchase some goods from the merchant and that both have bank accounts with Bank.

A. Request for certificate by user or smart card

1. Customer asks for certificate from the certifying authority.
2. Certifying Authority issues a certificate to the card by putting the unique identity number and validity period.

B. Request for certificate by terminal or server

1. Terminal/Server asks for certificate from the certifying authority.

2. Certifying Authority issues a certificate to the server by putting the unique identity number and validity period.

C. Online transaction between Card and Terminal/ Server

1. After agreeing on the initial key, final session key is generated with the help of a generator.

2. With the help of new session key message is encrypted along with the certificate then sent to the receiver.

3. At the receiving end message and certificate is verified, if it is valid, then the encrypted message is decrypted using the above proposed protocol.

6. Conclusion

This paper suggests a secure and efficient protocol based on the Elliptic Curve Discrete Logarithm Problem for smart card. The scheme utilizes fewer number bits due to inherent property of elliptic curve as compared to its public key counterparts such as RSA. The proposed protocol is suitably illustrated using an online transaction for digital cash. The validation of the proposed scheme has been made.

7. References

[1] Alfred J. Menezes, "*Elliptic curve public key cryptosystem*", Auburn University, Kluwer Academic Publishers, Dordrech, London, 1993.

[2] V. Miller, "*Uses of Elliptic Curve in Cryptography*", Advances in Cryptography, Proceedings of Crypto'85, Lecture Notes on Computer Sciences, 218, Springer-Verlag, 1986, pp. 417-426.

[3] N. Koblitz, "*Elliptic Curve Cryptosystems*", Mathematics of Computation, 48, 1987, pp. 203-209.

[4] Jonson, D., Alfred Menezes. "*Elliptic curve DSA (ECDSA): An Enhanced DSA*", 24 February 2000. http://citeseer.nj.nec.com/cache/papers/cs/8755/ http://zSzzSzcacr.math.uwaterloo.cazSz~ajmenezezSzpublic ati onszSzecdsa.pdf/johnson99elliptic.pdf (8 Feb. 2004)

[5] T. ELGamel, "*A Public Key cryptosystem and a signature scheme based on Discreet logarithms*", IEEE Transaction on Information Theory, Vol.It-3 1, No. 4, July (1985), pg 469-481.

[6] Rivest. R.L. Shamir, and L. Adleman, "*A method for obtaining digital Signatures and Public key cryptosystem*'', Communications of the ACM, Vol. 21, No. 2, (1978) 120-126.

[7] Certicom, "Elliptic Curve Cryptography". http://www.certicom.coiti/reaserch

[8] N. Koblitz, "*CM-Curves with Good Cryptographic Properties*", Proceeding of Crypto'91, 1992.

[9] Doug Stinson, "*Cryptography Theory and Practice*", Second Edition, CRC Press, Inc, 2002.

[10] Menezes, P. van Oorschot, and S. Vanstone, "*Handbook of Applied Cryptography*", CRC Press, 1996.

[11] Ahmed Khaleed, M.Al-Kayali, "*Elliptic Curve cryptography and smart cards*", GISC Security Essentials Certification (GSEC), 2004.

[12] C.P .Schnorr, "Efficient signature generation by smart cards", *Journal of Cryptology*, 4(3):161-174, 1991.

[13] William stalling, "*Cryptography and network security*: *Principles and practice*", Second Edition, Prentice Hall, 1999.

[14] Popesu C., "A Secure Key Agreement Protocol Using Elliptic Curves", *International Journal of Computers and Applications*, Vol 27, 2005.