An Efficient Two-Party Identity-Based Key Exchange Protocol based on ECDLP

Jayaprakash Kar
Department of Information Technology
Al Musanna College of Technology
Sultanate of Oman*

Banshidhar Majhi
Department of Computer Science & Engineering
National Institute of Technology
Rourkela,INDIA†

September 8, 2009

Abstract

This paper presents an efficient identity-based key exchange protocol based on the difficulty of computing a Elliptic Curve Discrete Logarithm Problem. As compared with the previously proposed protocols, it has better performance in terms of the computational cost and the communication steps. Key exchange protocols allow two parties communicating over a public network to establish a common secret key called session key to encrypt the communication data. Due to their significance by in building a secure communication channel, a number of key exchange protocols have been suggested over the years for a variety of settings.The proposed key exchange protocol provides implicit key authentication as well as the desired security attributes of an authenticated key exchange protocol.

Key word : authentication, identity-based, key exchange, ECDLP, security.

1 Introduction

A key establishment protocol allows principals to establish a common key for encrypting their communications over an insecure network. A two-party key exchange (or agreement)protocol is used to establish a common session key for two specified entities, in which both two entities contribute some information to derive the shared session key. If three or more participants want to communicate

*e-mail: jayaprakashkar@yahoo.com
†e-mail: bmajhi@nitrkl.ac.in

securely over an insecure network,they may employ a conference-key establishment protocol to compute a conference key [21]; Ingemaresson et al., 1982; [26] [27]. [19] first proposed a secure key exchange protocol. However, it does not allow two entities to authenticate each other, so their protocol requires an authentication channel to exchange the public keys. According to technical categories of authentication approach, key exchange protocols may be classified into a number of categories: public-key-based key exchange protocols. A public-key based key exchange protocol adopts public-key cryptographic techniques to achieve the purposes of user authentication and key exchange. On the way of key management, although the public-key-based key exchange protocol is better than password-based key exchange protocol. However, on-line access to get and verify public keys from a public key system in a network system is time-consuming. Moreover, it needs to require extra efforts to maintain public-keys in a public key system . On the other hand,an identity-based key exchange protocol can be regard as a variation of the public-key based key exchange protocol. An identity-based key exchange protocol is a protocol that uses users identity or some other information combined with his identity as ones public key to achieve user authentication and key exchange. Thus, a verifier does not verify the certificates of the public keys. Meanwhile, no on-line system authority is required.

In this paper, we will propose a new identity-based key exchange protocol based on the difficulty of computing a elliptic curve discrete logarithm problem. It reduces both the computational cost and the communication steps as compared to the previously proposed protocols.

Over the past years, many two-party authenticated key exchange protocols have been proposed. However, to our best knowledge, not all of them can meet the requirements of security and efficiency simultaneously.

The proposed key exchange protocol provides implicit key authentication as well as the desired security properties of an authenticated key exchange protocol.The remainder of this article is organized as follows.

In Section 3, we review briefly about various two-party key exchange protocols. Section 4 describes security goals and attributes, section 5 our new propose identity-based key exchange protocol. The security analysis of the new protocol is presented in Section 6. In Section 7, the performance comparison among the proposed protocol and the previously proposed identity-based key exchange protocols is presented. Section 8 gives our conclusions .

2 Background

In this section we brief overview of Elliptic Curve over finite field, Elliptic Curve Discrete Logarithm Problem,Key exchange and Elliptic Curve Diffe-Helman(ECDH).

2.1 The finite field F_p

Let p be a prime number. The finite field F_p is comprised of the set of integers $0, 1, 2, \ldots p-1$ with the following arithmetic operations [1] [2]:

- Addition: If $a, b \in F_p$, then $a + b = r$, where r is the remainder when $a + b$ is divided by p and $0 \leq r \leq p-1$. This is known as addition modulo p.
- Multiplication: If $a, b \in F_p$, then $a.b = s$, where s is the remainder when $a.b$ is divided by p and $0 \leq s \leq p-1$. This is known as multiplication modulo p.
- Inversion: If a is a non-zero element in F_p, the inverse of a modulo p, denoted a^{-1}, is the unique integer $c \in F_p$ for which $a.c = 1$.

2.2 Elliptic Curve over F_p

Let $p \geq 3$ be a prime number. Let $a, b \in F_p$ be such that $4a^3 + 27b^2 \neq 0$ in F_p. An elliptic curve E over F_p defined by the parameters a and b is the set of all solutions $(x, y), x, y \in F_p$, to the equation $y^2 = x^3 + ax + b$, together with an extra point O, the point at infinity. The set of points $E(F_p)$ forms a abelian group with the following addition rules [4]:

1. Identity : $P + \mathcal{O} = \mathcal{O} + \mathcal{P} = \mathcal{P}$, for all $P \in E(F_p)$
2. Negative : if $P(x, y) \in E(F_p)$ then $(x, y)+(x, -y) = \mathcal{O}$, The point $(x, -y)$ is dented as -P called negative of P.
3. Point addition: Let $P((x_1, y_1), Q(x_2, y_2) \in E(F_p)$,then $P + Q = R \in E(F_p)$ and coordinate $(x_3, y_3)$of R is given by $x_3 = \lambda^2 - x_1 - x_2$ and $y_3 = \lambda(x_1 - x_3) - y_1$ where $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$
4. Point doubling : Let $P(x_1, y_1) \in E(K)$ where $P \neq -P$ then $2P = (x_3, y_3)$ where $x_3 = (\frac{3x_1^2 + a}{2y_1})^2 - 2x_1$ and $y_3 = (\frac{3x_1^2 + a}{2y_1})(x_1 - x_3)$- y_1

2.3 Elliptic Curve Discrete Logarithm Problem (ECDLP)

Given an elliptic curve E defined over a finite field F_p,a point $P \in E(F_p)$ of order n, and a point $Q \in < P >$,find the integer $l \in [0, n-1]$such that $Q = lP$. The integer l is called discrete logarithm of Q to base P,denoted $l = log_p Q$ [4].

2.4 Key exchange

Key exchange protocols allow two parties to agree on a secret shared secret key that they can use to do further encryption for a long message. One of these protocols is the Diffie-Hellman, which is the most used one. The Elliptic curve Diffie-Helman is considered as an extension to the standard Diffie- Hellman.

2.5 Elliptic Curve Diffie-Helman

Elliptic curve Diffie-Helman protocol (ECDH) is one of the key exchange protocols used to establishes a shared key between two parties. ECDH protocol is based on the additive elliptic curve group. ECDH begin by selecting the underlying field $F(P)$ or $GF(2^k)$, the curve E with parameters a,b and the base point P. The order of the base point P is equal to n. The standards often suggest that we select an elliptic curve with prime order and therefore any element of the group would be selected and their order will be the prime number n [**?**]. At the end of the protocol,the communicating parties end up with the same value K which is a point on the curve.

3 Two-Party Key Exchange Protocol

Numerous Diffie-Hellman based authenticated key agreement protocol and authenticated key agreement with key confirmation protocols have been designed to add authentication (and key confirmation) to the Diffie-Hellman protocol; however,many have subsequently been found to have flaws. One of the well-known authenticated key agreement (AK) protocol in the Diffie-Hellman family is MTI protocol by Matsumoto, Takashima and Imai [5]. They designed three infinite families of key agreement protocols to provide implicit key authentication in the classical Diffie-Hellman key agreement protocol. However, the security analysis against active adversary is only heuristic. Law et al. [6] pointed out flaws in the protocols and presented an efficient authenticated key agreement protocol, often called MQV protocol. The security analysis of MQV protocol against active adversary is also heuristic. Both MTI and MQV family of protocols are certificate-based. There are many ID-based key agreement protocols based on pairing. Scott [7] proposed an ID based key agreement protocol where each user selects his own personal identity number (PIN) and a trusted PKG issues each user an individual secret associated with the identity of corresponding user. A value is calculated from both the individual secret and PIN number and placed inside a hardware token. The individual secret can be reconstructed from their memorized PIN number,identity and token.Another ID-based authenticated key agreement was proposed by Smart [24] that combines the idea of Boneh and Franklin [11] with the tripartite Diffie-Hellman protocol of Joux [13]. The scheme uses weil pairing and requires all users involved in the key agreement to be clients of the same PKG. The protocol allows efficient ID-based escrow facility for sessions that enables low enforcement agencies to decrypt messages encrypted with the session keys, after having obtained the necessary warrants. Chen and Kudla [9] developed an ID-based authenticated key agreement protocol more efficient than Smart's protocol [24]. They have suggested a mechanism to turn escrow off which can also be applied to Smart's protocol [24] (the escrow-free environment may be desirable for personal communications the users wish to keep confidential even from the PKG). They also provided a modification that allows key agreement between users under different PKGs.None of the

two party key agreement protocols by Scott [7], Smart [24] and Chen and Kudla [9] were broken, although heuristic arguments are adopted to prove their security against active adversary. Shim citeS03 presented an ID-based key agreement protocol. However, Sun and Heish [10] showed that Shim's key agreement protocol is insecure against the man-in-the-middle attack. Another efficient ID-based authenticated key agreement protocol was proposed by McCullagh and Barreto [17] that can be used in either escrow or escrow-free mode. They also developed a scheme for key agreement between clients of different PKGs. The scheme is twice as efficient as the scheme in [9] without pre computation. Later, Xie [12] pointed out a flaw in it and removed this flaw by suggesting modifications for the protocol. Recently, Choo [14] showed that both the scheme and its modified variant are not secure if the adversary is allowed to reveal non-partner players who had accepted the same session key. Jeong et al. [15]proposed three simple single-round two-party key agreement protocols with detail security analysis in the security model of [16]. A practical two party-key exchange protocol comply with the following requirements.

1. The session key should be agreed by the communication parties instead of being assigned by the server directly.
2. Except the password, no extra secret information should be needed - the public key for example.
3. Computation and round efficiencies should be provided at the same time.

4 Security Goals and Attributes

In the past, some desired security goals and attributes have been identified for an authenticated key exchange protocol [18] . In general, the importance of providing these security goals and attributes is dependent on the applications. In the following, we first describe two kinds of fundamental security goals. An authenticated key exchange protocol should provide one of two kinds of security goals.

- Implicit key authentication. It means that each principal only shows the other principal,who can compute the session key.
- Explicit key authentication. It means that a principal is assured that another principal have actually computed the session key.

Although it is important to provide formal security proof on any cryptographic protocols,key exchange protocols remain one of the most challenging research issues. Until now, a provably secure two-pass authenticated key exchange protocol is still an important subject of research [22]. The notion of provable security makes several concrete security attributes to be presented as desirable.Several desirable security attributes have been presented in the past literatures. We summary these attributes as follows [25] a detail discussions):

1. Known-key security: In each run of a key exchange protocol, two specified entities should produce a unique session key. When an adversary has learned some other session key produced by previous runs, the adversary is unable to learn some other session key between the two entities.

2. Full forward secrecy: It means that if ones long-term private key is disclosed to some adversaries, they can not learn the previous session key. So this security goal makes the secrecy of previous session key not affected, even if the long-term private key loss. A further distinction is that a single entitys private key is compromised or the private keys of both participating entity are compromised. The former is called half forward secrecy, and the latter is called full forward secrecy.

3. Key-compromise impersonation. Assume that entities A and B are two principals. Suppose As secret key is disclosed. Obviously, an adversary who knows this secret key can impersonate A to other entities. However, it is desired in some situation that this disclosure does not allow the adversary to impersonate other entities to A.

4. Unknown key-share: When entities B believes the key is shared with some entity $C \neq A$, and A believes the key is shared with B. The above scenario can not be permitted. This scenario was first described in (Diffie et al., 1992).

5 New Identity-Based Key Exchange Protocol

Let A and B be two legal clients in the system who wish to establish a session key, and S be a trusted authentication server which chooses the system parameters and generating key pair for each user.

In the setup phase, the authority chooses the elliptic curve E defined over a finite field F_p two field elements $a, b \in F_p$, which defined the equation of the elliptic curve E over F_p i.e $y^2 = x^3+ax+b$ in the case $p \geq 3$, where $4a^3+27b^2 \neq 0$. Then, the authority possess a one-way hash function $\mathcal{H}$. Let d is the number to be randomly choose from the interval $[1, n-1]$, computes the point $Q = d \cdot P$, where P and Q are group element in $E(F_p)$. The key pair (d, Q), in which the private key d and Q is a public key, and publishes P, Q and $\mathcal{H}$. For each user, the authority computes $I = \mathcal{H}(ID)$, where ID is the identity string that may include the name, e-mail address, birthday or physical description corresponding to the user's identity. Then, the authority chooses a random number k from the interval $[1, n-1]$ and computes $R = k \cdot P$ as user's Public key and $s = k + d \cdot \mathcal{H}(ID)$ as the user's Private key. That is, each legal user i with the identity information ID_i has a key pair (R_i, s_i). Assumed that the users A and B are two legal users in the system. Thus, A and B have the key pairs

$R_A = k_A \cdot P, s_A = k_A + d \cdot \mathcal{H}(ID_A)$ and $R_B = k_B \cdot P, s_B = k_B + d \cdot \mathcal{H}(ID_B)$ respectively. Thus, A and B carry out the following steps to generate the session key shared between them.

1. Step-I (round 1). A selects the random number t_A from the interval $[1, n-1]$, and computes $U_A = t_A \cdot P$. Then, A uses her private key s_A to compute $v_A = t_A + s_A \cdot U_{A_x}$, where U_{A_x} is x-coordinate of point U_A and sends U_A, R_A and ID_A to B.

2. Step-II (round 2).B also selects a random number t_B from the interval $[1, n-1]$ and computes $U_B = t_B \cdot P$ and then B use his private key s_B and to compute $v_B = t_B + s_B \cdot U_{B_x}$, and sends U_B, R_B and ID_B to A.

5.1 Key Computation

To compute the the session key K_A, A will follows the following steps.

1. $Z_A = R_B + \mathcal{H}(ID_B) \cdot Q = k_B \cdot P + \mathcal{H}(ID_B) \cdot d \cdot P$
   $= (k_B + d \cdot \mathcal{H}(ID_B)) \cdot P = s_B \cdot P$

2. $K_A = v_A \cdot (U_B + U_{B_x} \cdot Z_A)$
   $= v_A \cdot (U_B + U_{B_x} \cdot s_B \cdot P)$
   $= v_A \cdot (t_B \cdot P + U_{B_x} \cdot s_B \cdot P)$
   $= v_A \cdot (t_B + U_{B_x} \cdot s_B) \cdot P)$
   $= (v_A \cdot v_B) \cdot P$

B also computes the session key K_B as follows

1. $Z_B = R_A + \mathcal{H}(ID_A) \cdot Q = k_A \cdot P + \mathcal{H}(ID_A) \cdot d \cdot P$
   $= (k_A + d \cdot \mathcal{H}(ID_A)) \cdot P = s_A \cdot P$

2. $K_B = v_B \cdot (U_A + U_{A_x} \cdot Z_B)$
   $= v_B \cdot (U_A + U_{A_x} \cdot s_A \cdot P)$
   $= v_B \cdot (t_A \cdot P + U_{A_x} \cdot s_A \cdot P)$
   $= v_B \cdot (t_A + U_{A_x} \cdot s_A) \cdot P)$
   $= (v_B \cdot v_A) \cdot P$

It is clear that A and B have the common session key $K = K_A = K_B = (v_A \cdot v_B) \cdot P$

6 Security Analysis

Here, let us discuss the security of the proposed protocol. The security of the proposed protocol is based on the difficulty of computing the elliptic curve discrete logarithm problem [20] and the DiffieHellman scheme [19].

- Firstly, we show that if an adversary eavesdrops the transmitted messages U_A, R_A, ID_A, U_B, R_B and ID_B between two entities, he is unable to obtain the secret key s_A of the user A from R_A and ID_A, or the secret key s_B of the user B from R_B and ID_B. Since $s_A = k_A + d \cdot \mathcal{H}(ID_A)$ has two

unknown variable variables k_A and d selected by the system authority, and the adversary wants to obtain two unknown variables from the transmitted messages, he must compute k_A and d from $R_A = k_A \cdot P$ and $Q = ç dot P$. Thus, it is equivalent to solving the elliptic curve discrete logarithm problem. In the proposed protocol, the adversary may find $Z_A = R_B + \mathcal{H}(ID_B) \cdot Q = s_B \cdot P$. If the adversary tries to find s_B from $R_B + \mathcal{H}(ID_B = s_B \cdot P$, he still faces the difficulty of elliptic curve solving the discrete logarithm problem.

- Considering another situation, if an adversary eavesdrops the transmitted messages U_A, R_A, ID_A, U_B, R_B and ID_B between two entities, he is still unable to obtain the established common session key. For computing the established common session key $K_A = v_A \cdot (U_B + U_{B_x} \cdot Z_A)$ or $K_B = v_B \cdot (U_A + U_{A_x} \cdot Z_B)$, the adversary must know v_A or v_B. However, both v_A and v_B are not transmitted in the proposed protocol. Thus, the adversary is also unable to compute v_A or v_B because $v_A = t_A + s_A \cdot U_{A_x}$ and $v_B = t_B + s_B \cdot U_{B_x}$ contain the users secret keys s_A and s_B, respectively.

- In the following, let us consider that any legal user i with a key pair (R_i, s_i) is unable to compute the secret key d of the system authority. In fact, the key pair $(R_i = k_i \cdot P, s_i = k_i + d \cdot \mathcal{H}(ID_i))$ may be viewed as a Schnorrs signature (Schnorr, 1990) generated by the system authority for the identity information ID_i. Pointcheval and Stern (1996) have shown that to compute the secret key d from (R_i, s_i) is equal to the difficulty of solving the DiffieHellman problem.

In fact, a provably secure two-pass authenticated key exchange protocol is still an important subject of research (Kaliski, 2001). Fortunately, the notion of provable security 132 Y.-M. Tseng makes several concrete security attributes to be identified as desirable. In the following, let us discuss that the new proposed protocol satisfies the desirable security attributes described in Section (Security Goal and Attribute).

1. Known-key security. If the session key K is disclosed, the protocol may withstand known-key attack. Suppose that the adversary has known a presession key K_1 established between A and B. Since $K_1 = v_{A_1} \cdot v_{B_1} \cdot P$ we have $K_1 = (t_{A_1} + s_A \cdot U_{A_{1_x}}) \cdot (t_{B_1} + s_B \cdot U_{B_{1_x}}) \cdot P = (t_{A_1} \cdot t_{B_1}) \cdot P + (s_A \cdot U_{A_{1_x}} \cdot t_{B_1}) \cdot P + (t_{A_1} \cdot s_B \cdot U_{B_{1_x}}) \cdot P + (s_A \cdot U_{A_{1_x}} \cdot s_B \cdot U_{B_{1_x}}) \cdot P$

   Suppose that there is another value K_2 established between A and B now. As the same reason, we have $K_2 = (t_{A_2} + s_A \cdot U_{A_{2_x}}) \cdot (t_{B_2} + s_B \cdot U_{B_{2_x}}) \cdot P$. First, because K_1 is the multiplicative addition of four items $(t_{A_1} \cdot t_{B_1}) \cdot P, (s_A \cdot U_{A_{1_x}} \cdot t_{B_1}) \cdot P, (t_{A_1} \cdot s_B \cdot U_{B_{1_x}}) \cdot P$ and $(s_A \cdot U_{A_{1_x}} \cdot s_B \cdot U_{B_{1_x}}) \cdot P$ and each items multiplication consists of two unknown values, thus the adversary is unable to obtain the valid information such as, (s_A, s_B) from K_1. Certainly, he/she

does not find another session key K_2 from K_1. Therefore, the proposed protocol can withstand known-key attack.

2. Full forward secrecy. If both secret keys of A and B are disclosed, the adversary tries to compute v_A or v_B, and then to compute $K = (v_A \cdot v_B \cdot) \cdot P$. However, to find v_A or v_B must require to know t_A or t_B from U_A or U_B, respectively. Thus, this will be equivalent to solving the elliptic curve discrete logarithm problem. Moreover, because of the session key K includes the value of $(t_A \cdot t_B) \cdot P$, which is still unknown to the adversary. Therefore, the proposed protocol can provide full forward secrecy.

3. Key-compromise impersonation. Suppose that the secret key of B is disclosed. An adversary who knows this secret key tries to impersonate some entity A to B. Because of it is necessary to compute v_A for impersonating A, and it must be computed using the secret key s_A of A. In such case, impersonating A to B is impossible. Therefore, the proposed protocol can withstand key-compromise impersonation attack.

4. Unknown key-share. The kind of attack has a precondition, which is that the public key of the adversary must determine by oneself. Obviously, since the users public key is determined by the authority, it can withstand unknown key-share attack (Kaliski, 2001).

Finally, let us consider the security goal about key authentication. Suppose that there are two honest entities A and B, who want to execute the proposed key exchange protocol to establish a common session key. Since $K = (v_A \cdot v_B) \cdot P$, other entities must know either s_A or s_B to compute v_A or v_B for computing the session key . That is, no other entities can learn the session key. Thus, the new key exchange protocol provides implicit key authentication between A and B.

7 Performance Analysis

For convenience, the following notations are used to analyze the computational cost. T_{mul} is the time for sclar multiplication; T_{add} is the time for addition; T_H is the time of executing the one way hash function $\mathcal{H}()$; As for the computational cost in our proposed protocol, any user i of two entities must compute U_i, v_i, Z_i, and K. It requires $5T_{mul} + T_{add} + T_H$ for each entity.

8 Conclusion

An identity-based key exchange protocol has an advantage, that to avoid the online access of obtaining the public keys in a network environment, because of the verification of the public key in an identity-based system is embedded in the key establishing process between two entities. An efficient identity-based key exchange

protocol based on the difficulty of computing the elliptic discrete logarithm problem has been proposed. The proposed key exchange protocol provides implicit key authentication, and it provides the desired security attributes of an authenticated key exchange protocol. As compared with the previously proposed protocols, it reduces the computational cost.

In this research a new protocol for exchanging key between two parties with a trusted Server has been defined. This new protocol has two major advantages over all previous key exchange protocol, first this protocol does not leak any information that allow the adversary to verify the correctness of password guesses. The second one is that this protocol does not leak any information that allows to verify the correctness of password guesses. The proposed protocol is also easy to implement.The security of our system is based on Elliptic Curve Discrete Logarithm Problem (ECDLP). The primary reason for the attractiveness of ECC over systems such as RSA and DSA is that the best algorithm known for solving the underlying mathematical problem (namely, the ECDLP) takes fully exponential time. In contrast, sub-exponential time algorithms are known for underlying mathematical problems on which RSA and DSA are based, namely the integer factorization (IFP) and the discrete logarithm (DLP) problems. This means that the algorithms for solving the ECDLP become infeasible much more rapidly as the problem size increases than those algorithms for the IFP and DLP. For this reason, ECC offers security equivalent to RSA and DSA while using far smaller key sizes.The attractiveness of ECC will increase relative to other public-key cryptosystems as computing power improvements force a general increase in the key size. The benefits of this higher-strength per-bit include higher speeds, lower power consumption, bandwidth savings, storage efficiencies, and smaller certificates.

References

[1] K. H Rosen *"Elementary Number Theory in Science and Communication", 2nd ed., Springer-Verlag, Berlin, 1986.*

[2] A. Menezes, P. C Van Oorschot and S. A Vanstone *Handbook of applied cryptography. CRC Press, 1997.*

[3] D. Hankerson, A .Menezes and S.Vanstone. *Guide to Elliptic Curve Cryptography, Springer Verlag, 2004.*

[4] *"Certicom ECC Challenge and The Elliptic Curve Cryptosystem" available :http://www.certicom.com/index.php.*

[5] T. Matsumoto, Y. Takashima and H. Imai *" On Seeking Smart Public-key Distribution Systems". In Transactions of the IECE of Japan, E69, pp. 99-106, 1986.*

[6] L. Law, A. Menezes, M. Qu, J. Solinas, and S. Vanstone. *"An Efficient Protocol for Authenticated Key Agreement". Technical Report CORR 98-05,Department of C & O, University.of Waterloo, 1998. Also available at http://citeseer.nj.nec.com/law 98efficient.*

[7] M. Scott. *"Authenticated ID-based Key Exchange and Remote Log-in with Insecure Token and PIN Number". Available at http://eprint.iacr.org/2002/164.*

[8] N. P. Smart. *"An Identity-based Authenticated Key Agreement Protocol Based on the Weil Pairing". In Electronic Letters, 38, pp. 630-632, 2002. Also available at http://www.iacr.org/2001/111.*

[9] L. Chen and C. Kudla. *"Identity Based Authenticated Key Agreement Protocols from Pairings". Available at http://eprint.iacr.org/2002/184.*

[10] H. M. Sun and B. T. Hsieh. *Security Analysis of Shim's Authenticated Key Agreement Protocols from Pairings. Available at http://eprint.iacr.org/2003/113.*

[11] D. Boneh and M. Franklin. *Identity-Based Encryption from Weil Pairing. In proceedings of Crypto 2001, LNCS 2139, pages 213-229, Springer-Verlag, 2001.*

[12] G. Xie *Cryptanalysis of Noel McCullagh and Paulo S. L. M. Barreto's Two-party Identity- Based Key Agreement. Available at http://eprint.iacr.org/2004/308.*

[13] A. Joux. *"A One Round Protocol for Tripartite Diffie-Hellman." In proceedings of ANTS 4, LNCS 1838, pp. 385-394, Springer-Verlag, 2000.*

[14] K. R. Choo. *"Revisit of McCullagh-Barreto Two-Party ID-Based Authenticated Key Agreement Protocols." Available at http://eprint.iacr.org/2004/343.*

[15] I. R. Jeong, J. Katz and D. H. Lee. *"One-Round Protocols for Two-Party Authenticated Key Exchange". In proceedings of ACNS 2004, LNCS 3089,pp. 220-232, Springer-Verlag, 2004*

[16] E. Bresson, O. Chevassut, and D. Pointcheval *"Dynamic Group Diffie-Hellman Key Exchange under Standard Assumptions". In proceedings of Eurocrypt 2002, LNCS 2332, pp.321-336, Springer-Verlag, 2002.*

[17] N. McCullagh and P. S. L. M. Barreto *" A New Two-Party Identity-Based Authenticated Key Agreement". In proceedings of CT-RSA 2005, LNCS 3376, pp. 262-274, Springer-Verlag, 2005.Also available at http://eprint.iacr.org/2004/122.*

[18] BlakeWilson, S., and A. Menezes (1999) *"Authenticated DiffieHellman key agreement protocols". In Proc. of the 5th Annual Workshop on Selected Areas in Cryptography (SAC 98). Lecture Notes in Computer Science,1556. pp. 339361.*

[19] Diffie, W., and M.E. Hellman (1976) *New directions in cryptography. IEEE Trans. on Info. Theory, 22(6),644654.*

[20] ElGamal, T. (1985). *"A public key cryptosystem and signature scheme based on discrete logarithm". IEEE Transactions on Information Theory, 31(4), 469472.*

[21] Hwang, M.S., and W.P. Yang *"Conference key distribution schemes for secure digital mobile communications".IEEE J. Sel. Areas Comm., 13, 416420.*

[22] Kaliski, B. (2001). *"An unknown key-share attack on theMQV key agreement protocol". ACMTrans. Information and System Security, 4(3), 275288.*

[23] Shim, K. (2003). *"Efficient ID-based authenticated key agreement protocol based on Weil pairing". Electronics Letters, 39(8), 653654.*

[24] Smart, N.P. (2002). *"An identity based authenticated key agreement protocol based on the Weil pairing". Electronics Letters, 38, 630632.*

[25] BlakeWilson, S., and A. Menezes (1999). *"Authenticated DiffieHellman key agreement protocols". In Proc. of the 5th Annual Workshop on Selected Areas in Cryptography (SAC 98). Lecture Notes in Computer Science, 1556. pp. 339361.*

[26] Tseng, Y.M. (2005a). *"An improved conference-key agreement protocol with forward secrecy". Informatica,16(2), 275284.*

[27] Tseng, Y.M. (2005b). *"A robust multi-party key agreement protocol resistant to malicious participants". The Computer Journal, 48(4), 480487.*