INFORMATICA, 2007, Vol. 18, No. 1, 125–136

An Efficient Two-Party Identity-Based Key Exchange Protocol *

Yuh-Min TSENG
Department of Mathematics, National Changhua University of Education
Jin-De Campus, Chang-Hua City 500, Taiwan, R.O.C.
e-mail: ymtseng@cc.ncue.edu.tw

Received: April 2006

Abstract. A key exchange (or agreement) protocol is designed to allow two entities establishing a session key to encrypt the communication data over an open network. In 1990, Gunther proposed an identity-based key exchange protocol based on the difficulty of computing a discrete logarithm problem. Afterwards, several improved protocols were proposed to reduce the number of communication steps and the communicational cost required by Gunther's protocol. This paper presents an efficient identity-based key exchange protocol based on the difficulty of computing a discrete logarithm problem. As compared with the previously proposed protocols, it has better performance in terms of the computational cost and the communication steps. The proposed key exchange protocol provides implicit key authentication as well as the desired security attributes of an authenticated key exchange protocol.

Key words: authentication, identity-based, key exchange, 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 securely over an insecure network, they may employ a conference-key establishment protocol to compute a conference key (Hwang and Yang, 1995; Ingemaresson *et al.*, 1982; Tseng, 2005a; Tseng, 2005b). Diffie and Hellman (1976) 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 (Ankney *et al.*, 1995; ANSI, 2001; Lee and Chang, 1996; Menezes *et al.*, 1995; Tseng, 2002), password-based key exchange protocols (Bellovin and Merritt, 1992; Jablon, 1996; Jablon, 1997; Kwon and Song 1999),

*This research was partially supported by National Science Council, Taiwan, R.O.C., under contract no. NSC95-2221-E-018-010.

identity-based key exchange protocols (Gunther, 1990; Hsieh *et al.*, 2002; Sadeednia and Safavi–Naini, 1998; Sadeednia, 2000; Tseng *et al.*, 2002), as well as another identity-based key exchange protocols based on Weil pairing (Shim, 2003; Smart, 2002). Here, we focus on the design of identity-based key exchange protocols based on the difficulty of computing a discrete logarithm problem as (Gunther, 1990; Hsieh *et al.*, 2002; Sadeednia and Safavi–Naini, 1998; Sadeednia, 2000; Tseng *et al.*, 2002).

A password-based key exchange protocol allows both two entities share a secret password in advance to provide the purposes of user authentication and key exchange. 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 (IEEE, 2000). 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 user's identity or some other information combined with his identity as one's 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.

Gunther (1990) first proposed an identity-based key exchange protocol based on the difficulty of computing a discrete logarithm problem (ElGamal, 1985). However, Gunther's protocol requires four communication steps (rounds). Afterwards, several improved protocols were proposed to reduce the number of communication steps and the communicational cost required by Gunther's protocol. Saeednia (2000) proposed an improved protocol based on Gunther's protocol, which reduces the number of communication steps. However, both Gunther's protocol and Saeednia's improved protocol require many exponentiation operations. In 2002, Hsien *et al.* (2002) proposed a slight modification of Saeednia's protocol such that the computational cost can be further reduced. Unfortunately, Tseng *et al.* (2002) presented that their improved protocol suffers from key-compromise impersonation attack, and proposed a new identity-based key exchange protocol.

In this paper, we will propose a new identity-based key exchange protocol based on the difficulty of computing a discrete logarithm problem. It reduces both the computational cost and the communication steps as compared to the previously proposed protocols. 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. The desirable security attributes of a key exchange protocol are summarized in the next section. In Section 3, we review briefly the Saeednia's protocol and other improved protocols. Section 4 describes a new identity-based key exchange protocol. The security analysis of the new protocol is presented in Section 5. In Section 6, the performance comparison among the proposed protocol and the previously proposed identity-based key exchange protocols is presented. Section 7 gives our conclusions.

2. Security Goals and Attributes

In the past, some desired security goals and attributes have been identified for an authenticated key exchange protocol (Blake–Wilson and Menezes, 1999; Diffie *et al.*, 1992; Kaliski, 2001). 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.

1) *Implicit key authentication.* It means that each principal only shows the other principal, who can compute the session key.
2) *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 (Kaliski, 2001). 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 (refer to (Blake–Wilson and Menezes, 1999) 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 one's 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 entity's 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 A's 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).

3. Reviews of Identity-Based Key Exchange Protocols

Firstly, the Saeednia's key exchange protocol (Saeednia, 2000) is briefly reviewed as follow. In the system, there exists a trusted authority that is responsible for choosing system parameters and generating a key pair for each user. In the setup phase, the authority

chooses a large prime p such that $p-1$ has a large prime factor q. Let α be an element of order q in Z_p^*. Then, the authority possess a one way hash function $f()$ (Dobbertin, 1996; NIST/NSA, 2005) and a key pair (x, y), in which the private key $x \in Z_q$ is a random number and $y = \alpha^x \bmod p$ is a public key, and publishes α, p, q, y and $f()$.

For each user, the authority computes $I = f(ID)$, 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 in Z_q^*, and computes $r = \alpha^k \bmod p$ as the user's public key and $s = Ik + xr \bmod q$ 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

$$(r_A = \alpha^{k_A} \bmod p, s_A = I_A k_A + x \cdot r_A \bmod q)$$

and

$$(r_B = \alpha^{k_B} \bmod p, s_B = I_B k_B + x \cdot r_B \bmod q),$$

respectively, where $I_A = f(ID_A)$ and $I_B = f(ID_B)$.

Thus, A and B carry out the following steps to generate the session key shared between them.

Step 1 (round 1). A selects a random number $t_A \in Z_q$, and computes $u_A = \alpha^{t_A} \bmod p$. Then, A sends u_A, r_A and ID_A to B.

Step 2 (round 2). B also selects a random number $t_B \in Z_q$, and computes $u_B = \alpha^{t_B} \bmod p$. Then, B sends u_B, r_B and ID_B to A.

Key computation. A computes the session key K as follows:

$$\begin{aligned}
&I_B = f(ID_B),\\
&Z_1 = u_B^{s_A} \bmod p,\\
&Z_2 = (r_B^{I_B} y^{r_B})^{t_A} \bmod p,\\
&K = Z_1 Z_2 (u_B)^{t_A} \bmod p.
\end{aligned}$$

Meanwhile, B also computes the session key K as follows.

$$\begin{aligned}
&I_A = f(ID_A),\\
&Z_1 = (r_A^{I_A} y^{r_A})^{t_B} \bmod p,\\
&Z_2 = u_A^{s_B} \bmod p,\\
&K = Z_1 Z_2 (u_A)^{t_B} \bmod p.
\end{aligned}$$

It is clear that both two entities may compute the common key K, because of

$$\begin{aligned}
&Z_1 = u_B^{s_A} \bmod p = (r_A^{I_A} y^{r_A})^{t_B} \bmod p = \alpha^{t_B s_A} \bmod p,\\
&Z_2 = u_A^{s_B} \bmod p = (r_B^{I_B} y^{r_B})^{t_A} \bmod p = \alpha^{t_A s_B} \bmod p,
\end{aligned}$$

and

$$K = Z_1 Z_2 (u_B)^{t_A} \bmod p = Z_1 Z_2 (u_A)^{t_B} \bmod p.$$

Note that Saeednia also presented another simple key exchange protocol, in which the session key is $K = Z_1 Z_2 = \alpha^{s_A t_B + s_B t_A} \bmod p$, but it does not provide full forward secrecy.

Recently, Hsieh *et al.* (2002) proposed a slight modification of Saeednia's key exchange protocol, in which the computational cost can be reduced one modular multiplication and one modular exponentiation. Only the key computation phase is modified as follows:

***Key computation.** A computes the session key K as follows:

$$\begin{aligned} I_B &= f(ID_B), \\ Z_1 &= u_B^{t_A} \bmod p, \\ Z_2 &= (r_B^{I_B} y^{r_B})^{s_A} \bmod p, \\ K &= Z_1 Z_2 \bmod p. \end{aligned}$$

Meanwhile, B also computes the session key K as follows.

$$\begin{aligned} I_A &= f(ID_A), \\ Z_1 &= (r_A^{I_A} y^{r_A})^{s_B} \bmod p, \\ Z_2 &= u_A^{t_B} \bmod p, \\ K &= Z_1 Z_2 \bmod p. \end{aligned}$$

However, Tseng *et al.* (2002) have demonstrated that the above modified protocol does not achieve the security attribute of key-compromise impersonation. In addition, Tseng *et al.* also proposed another slight improvement on the key computation phase as follows:

***Key computation.** A computes the session key K as follows:

$$\begin{aligned} I_B &= f(ID_B, r_B), \\ Z_1 &= u_B^{s_A} \bmod p, \\ Z_2 &= (r_B y^{I_B})^{t_A} \bmod p, \\ K &= Z_1 Z_2 (u_B)^{t_A} \bmod p. \end{aligned}$$

Meanwhile, B also computes the session key K as follows.

$$\begin{aligned} I_A &= f(ID_A, r_A), \\ Z_1 &= (r_A y^{I_A})^{t_B} \bmod p, \\ Z_2 &= u_A^{s_B} \bmod p, \\ K &= Z_1 Z_2 (u_A)^{t_B} \bmod p. \end{aligned}$$

Note that the system setup phase has been modified as follows: The system authority chooses a random number k_i in Z_q^* and computes $r_i = \alpha^{k_i} \bmod p$ as the public key of the user i with identity ID_i . Then, the system authority computes $s_i = k_i + x \cdot f(ID_i, r_i) \bmod q$ as the corresponding user's private key.

4. New Identity-Based Key Exchange Protocol

In the setup phase, the system has the same parameters as that of the Saeednia's key exchange protocol. Any user who visits the system authority sends his ID_i to the authority, where ID_i is the identity string that may include the name, e-mail address, birthday or physical description corresponding to the user's identity. The system authority chooses a random number k_i in Z_q^* and computes $r_i = \alpha^{k_i} \bmod p$ as the user's public key. Then, the system authority computes $s_i = k_i + x \cdot f(ID_i, r_i) \bmod q$ as the user's private key. Thus, each legal user with the identity information ID_i has a key pair (r_i, s_i). Assumed that the users Alice (A) and Bob (B) are two legal users in the system. Thus, A and B have the key pairs

$$(r_A = \alpha^{k_A} \bmod p, s_A = k_A + x \cdot f(ID_A, r_A) \bmod q)$$

and

$$(r_B = \alpha^{k_B} \bmod p, s_B = k_B + x \cdot f(ID_B, r_B) \bmod q),$$

respectively. Thus, A and B carry out the following steps to generate the session key shared between them.

Step 1 (round 1). A selects a random number $t_A \in Z_q$, and computes $u_A = \alpha^{t_A} \bmod p$. Then, A uses her private key s_A to compute $v_A = t_A + s_A \cdot u_A \bmod q$, and sends u_A, r_A and ID_A to B.

Step 2 (round 2). B also selects a random number $t_B \in Z_q$, and computes $u_B = \alpha^{t_B} \bmod p$. Then, B uses his private key s_B to compute $v_B = t_B + s_B \cdot u_B \bmod q$, and sends u_B, r_B and ID_B to A.

Key computation

A computes the session key K_A as follows:

$$\begin{aligned} Z_A &= r_B \cdot y^{f(ID_B, r_B)} \bmod p = \alpha^{k_B} \cdot \alpha^{x \cdot f(ID_B, r_B)} \bmod p \\ &= \alpha^{k_B + x \cdot f(ID_B, r_B)} \bmod p = \alpha^{s_B} \bmod p \end{aligned}$$

and

$$\begin{aligned} K_A &= (u_B \cdot (Z_A)^{u_B})^{v_A} \bmod p = (\alpha^{t_B} \cdot (\alpha^{s_B})^{u_B})^{v_A} \bmod p \\ &= (\alpha^{t_B + s_B u_B})^{v_A} \bmod p = \alpha^{v_A v_B} \bmod p. \end{aligned}$$

Meanwhile, B also computes the session key K_B as follows.

$$\begin{aligned} Z_B &= r_A \cdot y^{f(ID_A, r_A)} \bmod p = \alpha^{k_A} \cdot \alpha^{x \cdot f(ID_A, r_A)} \bmod p \\ &= \alpha^{k_A + x \cdot f(ID_A, r_A)} \bmod p = \alpha^{s_A} \bmod p \end{aligned}$$

and

$$\begin{aligned} K_B &= (u_A \cdot (Z_B)^{u_A})^{v_B} \bmod p = (\alpha^{t_A} \cdot (\alpha^{s_A})^{u_A})^{v_B} \bmod p \\ &= (\alpha^{t_A + s_A u_A})^{v_B} \bmod p = \alpha^{v_A v_B} \bmod p. \end{aligned}$$

It is clear that A and B have the common session key $K = K_A = K_B = \alpha^{v_A v_B} \bmod p$.

5. 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 discrete logarithm problem (ElGamal, 1985) and the Diffie–Hellman scheme (Diffie and Hellman, 1976).

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 $s_A = k_A + x \cdot f(ID_A, r_A) \bmod q$ has two unknown variable variables k_A and x selected by the system authority, and the adversary wants to obtain two unknown variables from the transmitted messages, he must compute k_A and x from $r_A = \alpha^{k_A} \bmod p$ and $y = \alpha^x \bmod p$. Thus, it is equivalent to solving the discrete logarithm problem. In the proposed protocol, the adversary may find $Z_A = r_A \cdot y^{f(ID_A, r_A)} \bmod p = \alpha^{s_A}$. If the adversary tries to find s_A from $r_A \cdot y^{f(ID_A, r_A)} \bmod p$, he still faces the difficulty of 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 $K_A = (u_B \cdot (Z_A)^{u_B})^{v_A} \bmod p$ or $K_B = (u_A \cdot (Z_B)^{u_A})^{v_B} \bmod p$, 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 $v_A = t_A + s_A \cdot u_A \bmod q$ and $v_B = t_B + s_B \cdot u_B \bmod q$ 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 x of the system authority. In fact, the key pair $(r_i = \alpha^{k_i} \bmod p, s_i = k_i + x \cdot f(ID_i, r_i) \bmod q)$ may be viewed as a Schnorr's 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 x from (r_i, s_i) is equal to the difficulty of solving the Diffie–Hellman 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

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 2.

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 pre-session key K_1 established between A and B. Since $K_1 = \alpha^{v_{A1}v_{B1}} \bmod p$, we have

$$\begin{aligned} K_1 &= \alpha^{v_{A1}v_{B1}} \bmod p \\ &= \alpha^{(t_{A1}+s_A u_{A1})(t_{B1}+s_B u_{B1})} \bmod p \\ &= \alpha^{t_{A1}t_{B1}+s_A u_{A1}t_{B1}+t_{A1}s_B u_{B1}+s_A u_{A1}s_B u_{B1}} \bmod p \end{aligned}$$

   Suppose that there is another value K_2 established between A and B now. As the same reason, we have $K_2 = \alpha^{t_{A2}t_{B2}+s_A u_{A2}t_{B2}+t_{A2}s_B u_{B2}+s_A u_{A2}s_B u_{B2}} \bmod p$. First, because K_1 is the multiplicative product of four items $\alpha^{t_{A1}t_{B1}}$, $\alpha^{s_A u_{A1}t_{B1}}$, $\alpha^{t_{A1}s_B u_{B1}}$ and $\alpha^{s_A u_{A1}s_B u_{B1}}$, and each item's exponent consists of two unknown values, thus the adversary is unable to obtain the valid information (such as, $\alpha^{s_A s_B}$) 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 $K = \alpha^{v_A v_B} \bmod p$. 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 discrete logarithm problem. Moreover, because of the session key K includes the value of $\alpha^{t_A t_B}$, 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 user's 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 $K = \alpha^{v_A v_B} \bmod p$, 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.

6. Performance Comparison

For convenience, the following notations are used to analyze the computational cost. T_{mul} is the time for modular multiplication; $T_{\exp}$ is the time for modular exponentiation; T_f is the time of executing the one way hash function $f()$; Note that the time for computing modular addition operation is ignored, because they are much smaller than $T_{mul}, T_{\exp}$ and T_f.

As for the computational cost in our proposed protocol, any user i of two entities must compute four values u_i, v_i, Z_i, and K. It requires $4T_{\exp} + 3T_{mul} + T_f$ for each entity. Table 1 demonstrates the performance comparisons among the new protocol and the previously proposed identity-based key exchange protocols in terms of the computational cost, the number of the communication steps (rounds) and security attributes. The previously proposed identity-based key exchange protocols are reviewed in Section III that include Gunther's protocol (Gunther, 1990), Saeednia's protocol (Saeednia, 2000), Saeednia's simple protocol without forward secrecy (Saeednia, 2000), Hsien *et al.'s* protocol (Hsien *et al.*, 2002) and Tseng *et al.'s* protocol (Tseng *et al.*, 2002). From Table 1, it is clear that the new proposed protocol has better performance than the previously proposed protocols.

7. Conclusions

An identity-based key exchange protocol has an advantage, that to avoid the on-line 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. A new identity-based key exchange protocol based on the difficulty

Table 1

Comparisons among the new protocol and the previously proposed protocols

	Communication Steps (the number of rounds)	Computational cost for each entity	Known security weakness
Gunther's protocol (Gunther, 1990)	4	$6T_{\exp} + 3T_{mul} + T_f$	No
Saeednia's protocol (Saeednia, 2000)	2	$6T_{\exp} + 3T_{mul} + T_f$	No
Saeednia's simple protocol (Saeednia, 2000)	2	$5T_{\exp} + 2T_{mul} + T_f$	Without forward secrecy
Hsieh *et al.'s* protocol& (Hsien *et al.*, 2002)	2	$5T_{\exp} + 2T_{mul} + T_f$	Key-compromise impersonation
Tseng *et al.'s* protocol (Tseng *et al.*, 2002)	2	$5T_{\exp} + 3T_{mul} + T_f$	No
New proposed protocol	2	$4T_{\exp} + 3T_{mul} + T_f$	No

of computing the 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.

References

Ankney, R., D. Johnson and M. Matyas (1995). The unified model. Contribution to ANSI X9F1.

ANSI X9.63 (2001). Public key cryptography for the financial services industry: Key agreement and key transport using elliptic curve cryptography. ANSI. Working draft.

Bellovin, S.M., and M. Merritt (1992). Encrypted key exchange: Password-based protocols secure against dictionary attacks. In *Proc. 1992 IEEE Computer Society Conf. on Research in Security and Privacy*. pp. 72–84.

Blake–Wilson, S., and A. Menezes (1999). Authenticated Diffie–Hellman key agreement protocols. In *Proc. of the 5th Annual Workshop on Selected Areas in Cryptography (SAC '98). Lecture Notes in Computer Science*, **1556**. pp. 339–361.

Dobbertin, H. (1996). The status of MD5 after a recent attack. *CryptoBytes*, **2**(2), 1–6.

Diffie, W., and M.E. Hellman (1976). New directions in cryptography. *IEEE Trans. on Info. Theory*, **22**(6), 644–654.

Diffie, W., P.C. Oorschot and M.J. Wiener (1992). Authentication and authenticated key exchanges. *Designs, Codes and Cryptography*, **2**, 107–125.

ElGamal, T. (1985). A public key cryptosystem and signature scheme based on discrete logarithm. *IEEE Transactions on Information Theory*, **31**(4), 469–472.

Gunther, C. (1990). An identity-based key-exchange protocol. In *Advances in Cryptology – Eurocrypt'89*, *Lecture Notes in Computer Science*, **434**, Springer-Verlag. pp. 29–37.

Hsieh, B.T., H.M. Sun, T. Hwang and C.T. Lin (2002). An improvement of Saeednia's identity-based key exchange protocol. In *Information Security Conference 2002*. pp. 41–43.

Hwang, M.S., and W.P. Yang (1995). Conference key distribution schemes for secure digital mobile communications. *IEEE J. Sel. Areas Comm.*, **13**, 416–420.

IEEE Std 1363]-2000. (2000). Standard specifications for public key cryptography. IEEE.

Ingemaresson, I., T.D. Tang and C.K. Wong (1982). A conference key distribution system. *IEEE Trans. Infom. Theory*, **28**, 714–720.

Jablon, D.P. (1996). Strong password-only authenticated key exchange. *ACM Computer Communication Review*, **26**(5), 5–26.

Jablon, D.P. (1997). Extended password key exchange protocols. In *WETICE Workshop on Enterprise Security*. pp.248–255.

Kaliski, B. (2001). An unknown key-share attack on the MQV key agreement protocol. *ACM Trans. Information and System Security*, **4**(3), 275–288.

Kwon, T. and J. Song (1999). Secure agreement scheme for via password authentication. *Electronics Letters*, **35**(11), 892–893.

Lee, W.B., and C.C. Chang (1996). Integrating authentication in public key distribution system. *Information Processing Letters*, **57**, 49–52.

Menezes, A.J., M. Qu and S.A. Vanstone (1995). Some key agreement protocols providing implicit authentication. In *Proc. of 2nd Workshop on Selected Areas in Cryptography (SAC'95)*, Ottawa. pp. 22–32.

NIST/NSA, FIPS 180-2 (2005). *Secure Hash Standard (SHS)*. NIST/NSA, Gaithersburg, MD, USA.

Pointcheval, D., and Stern, J. (1996). Security proofs for signature schemes. In *Advances in Cryptology – Proceedings of EUROCRYPT '96*, *Lecture Notes in Computer Science*, **1070**, Springer-Verlag. pp. 387–398.

Saeednia, S., and R. Safavi–Naini (1998). A new identitity-based key exchange protocol minimizing computation and communication. In *Information Security Workshop (Proc. ISW'97)*, *Lecture Notes in Computer Science* **1396**, Springer-Verlag. pp. 328–334.

Saeednia, S. (2000). Improvement of Gunther's identity-based key exchange protocol. *Electronics Letters*, **36**(18), 1535–1536.

Schnorr, C.P. (1990). Efficient identification and signatures for smart cards. In *Advances in Cryptology – Proceedings of CRYPTO '89*, *Lecture Notes in Computer Science*, **435**, Springer-Verlag. pp. 235–251.

Shim, K. (2003). Efficient ID-based authenticated key agreement protocol based on Weil pairing. *Electronics Letters*, **39**(8), 653–654.

Smart, N.P. (2002). An identity based authenticated key agreement protocol based on the Weil pairing. *Electronics Letters*, **38**, 630–632.

Tseng, Y.M. (2002). Robust generalized MQV key agreement protocol without using one-way hash functions. *Computer Standards & Interfaces*, **24**(3), 241–246.

Tseng, Y.M., J.K. Jan and C.H. Wang (2002). Cryptanalysis and improvement of an identity-based key exchange protocol. *Journal of Computers*, **14**(3), 17–22.

Tseng, Y.M. (2005a). An improved conference-key agreement protocol with forward secrecy. *Informatica*, **16**(2), 275–284.

Tseng, Y.M. (2005b). A robust multi-party key agreement protocol resistant to malicious participants. *The Computer Journal*, **48**(4), 480–487.

Y.-M. Tseng received the BS degree in computer science and engineering from National Chiao Tung University, Taiwan, Republic of China, in 1988; and the MS degree in computer and information engineering from National Taiwan University in 1990 and the PhD degree in applied mathematics from National Chung-Hsing University in 1999. He is currently a professor in the Department of Mathematics, National Changhua University of Education, Taiwan. His research interests include applied cryptography, communication security, network security, and mobile communications. He is a member of IEEE Communications Society and the Chinese Cryptology and Information Security Association (CCISA). In 2005, his paper wined the runner-up paper of the Wilkes Award (*Computer Journal*). Now, he is an editor of the international journal *Computer Standards & Interfaces*.

Efektyvus tapatybės nustatymu pagrįstas apsikeitimo raktu protokolas

Yuh-Min TSENG

Straipsnyje pasiūlytas efektyvus tapatybės nustatymu pagrįstas apsikeitimo slaptuoju raktu tarp dviejų vartotojų protokolas, kurio patvarumas priklauso nuo diskretinio logaritmo apskaičiavimo sudėtingumo. Palyginus su žinomais protokolais, jis yra pranašesnis skaičiavimo išteklių ir duomenų perdavimo žingsnių prasme. Protokolas garantuoja rakto autentiškumą ir norimą apsikeitimo raktu slaptumą.