INFORMATICA, 2010, Vol. 21, No. 2, 247–258

Analysis and Improvement on a Contributory Group Key Exchange Protocol Based on the Diffie–Hellman Technique *

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

Received: November 2008; accepted: April 2010

Abstract. In 2008, based on the two-party Diffie–Hellman technique, Biswas proposed a contributory group key exchange protocol called the Group-DH protocol. This contributory property is an important one of group key agreement. Unfortunately, in this paper we show that the proposed Group-DH protocol is not a contributory group key exchange protocol. Therefore, we propose an improved group key exchange protocol with verifiably contributory property based on the same Diffie–Hellman technique. When an identical group key is constructed, each participant can confirm that his/her contribution is actually included in the group key. We show that the improved protocol is provably secure against passive attacks under the decisional Diffie–Hellman assumption. As compared to the previously proposed group key exchange protocols, our protocol provides contributiveness and the required computational cost is suitable for low-power participants in a network environment.
Keywords: contributory property, group key agreement, provable security, decisional Diffie–Hellman problem.

1. Introduction

A two-party key exchange protocol is used to establish a common session key for two participants (Diffie and Hellman, 1976; Hwang *et al*., 2004; Tseng, 2007a; Yoon and Yoo, 2009). If three or more participants want to communicate securely over an insecure network, they may employ a group key exchange protocol to compute a group key. Ingemaresson *et al.* (1982) proposed the first group key exchange protocol. A group key exchange protocol allows participants to construct a group key to encrypt/decrypt transmitted messages among participants over an open channel. There are two kinds of group key exchange protocols: group key distribution (Burmester and Desmedt, 1994; Hwang and Yang, 1995; Moyer *et al.*, 1999) and group key agreement (Steiner *et al.*, 1998; Burmester and Desmedt, 2005; Tseng, 2005, 2007b). One point of the group key agreement protocol is that no participant can predict or predetermine the group key. A group

*This research was partially supported by National Science Council, Taiwan, R.O.C., under contract No. NSC97-2221-E-018-010-MY3.

key agreement protocol (or called contributory group key exchange protocol) involves all participants cooperatively establishing a group key. This contributory property is an important one of group key agreement, in which each participant can confirm that his/her contribution is actually included in the group key.

Biswas (2008) extended the two-party Diffie–Hellman technique (Diffie and Hellman, 1976) to propose two protocols: (1) key agreement with multiple two-party keys and (2) a contributory group key exchange protocol called the Group-DH protocol. The former allows two participants to exchange two public keys and generate multiple two-party keys (Chien and Jan, 2004; Lee *et al.*, 2008). The latter called the Group-DH protocol is an extension of the two-party Diffie–Hellman technique to generate a group key for participants of a large group. He made a performance comparison among the Group-DH protocol and other previously proposed protocols (Steiner *et al.*, 1996; Bresson *et al.*, 2002; Kim *et al.*, 2004a, 2004b) to present the efficiency of the Group-DH protocol. The author claimed that the proposed Group-DH protocol is a contributory group key exchange protocol. Unfortunately, we will show that the Group-DH protocol is not a contributory group key exchange protocol.

In this paper, we first show that Biswas's Group-DH protocol has a security weakness. In the Group-DH protocol, the group consists of a group controller and some participants. The group controller is responsible to exchange public keys with other participants of the group. We show that the group controller can predetermine the group key by oneself. Thus, the Group-DH protocol is not a contributory group key exchange protocol. This inspires us to propose an improved group key exchange protocol based on the same two-party Diffie–Hellman technique. The improved protocol is a contributory group key exchange protocol retaining the performance merits of the Group-DH protocol. In the improved protocol, each participant is assured that his/her contribution is actually included in the group key. We also demonstrate that the improved protocol is secure against passive attacks under the decisional Diffie–Hellman problem assumption (Diffie and Hellman, 1976; Boneh, 1998). Performance analysis demonstrates that the improved protocol is well suited for low-power devices with limited computing capability.

The remainder of this paper is organized as follows. Security definitions for contributory group key exchange protocols are given in the next section. In Section 3, we briefly review Biswas's Group-DH protocol and present its security weakness. Section 4 presents our improved protocol and its security analysis. In Section 5, the performance evaluation and comparisons are given. Finally, we draw our conclusions in Section 6.

2. Preliminaries

In this section, we introduce security definitions of a contributory group key exchange protocols, as well as the related system parameters.

2.1. *Parameters*

The following parameters are used throughout this paper:

- q: a large prime;
- p: a large prime such that $p = 2q + 1$;
- G_q: a subgroup of quadratic residues in Z_p^*, that is $G_q = \{i^2 | i \in Z_p^*\}$;
- g: a generator for the subgroup G_q;
- $H()$: a one-way hash function, H: $\{0,1\}^* \rightarrow \{0,1\}^l$, where l is the output length;
- n: the number of participants that want to establish a group key.

2.2. *Security Definitions*

In a group key exchange system, there exists a public network, in which group participants can unicast or broadcast messages to each other. A passive adversary (eavesdropper) may receive the transmitted messages in this public network and keep all transcripts of past executions. Note that this passive adversary cannot modify messages and send them to these participants.

As we all know, one point of a key agreement protocol over a key distribution protocol is that no participant can predict or predetermine the common group key. In many scenarios, the key distribution approach is not appropriate because the group controller might become a single failure point for the group's security. Meanwhile, in some cases, it is not possible for the group controller to be strongly trusted by other participants in the group. If the group controller U_n is strongly trusted by other participants, then some efficient group key distribution protocols (Burmester and Desmedt, 1994; Hwang and Yang, 1995) may be deployed in this environment.

In the following, we introduce security definitions of a contributory group key exchange protocol.

DEFINITION 1 [*Group key exchange (GKE)*]. Let $U = \{U_1, U_2, \ldots, U_n\}$ be group participants that take part in a protocol $\mathcal{P}$ to generate a group key. If all group participants follow this protocol $\mathcal{P}$ and obtain an identical key, $\mathcal{P}$ is called a group key exchange protocol.

DEFINITION 2 [*Passive attack*]. Passive attack means that a passive adversary A tries to learn the established group key from the transmitted messages over the public network, or to distinguish the group key from a random bit string efficiently.

DEFINITION 3 [*Contributiveness*]. Group participants cannot predict or predetermine the resulting group key individually. That is, each participant may ensure that his/her contribution was included in the group key.

DEFINITION 4 [*Security of contributory GKE protocol*]. Let $\mathcal{A}$ be a passive adversary and $\mathcal{P}$ be a group key exchange protocol. A contributory GKE protocol $\mathcal{P}$ is said to be secure if it satisfies: (1) withstanding passive attacks; (2) providing contributiveness.

REMARK. Due to both Biswas's protocol and our improvement are non-authenticated type, the above security definitions are slightly modified from Burmester and Desmedt's

(2005) group key exchange system, as well as Bresson and Manulis's (2008) contributory group key exchange system. In Burmester and Desmedt's system, they presented the security definitions for non-authenticated GKE protocol but didn't concern with contributiveness. While in Bresson and Manulis's system, the contributiveness is defined under an authenticated group key exchange protocol. Generally, authentication is achieved by involving some signature techniques (Gao *et al.*, 2009; Sun *et al.*, 2010). In an authenticated GKE protocol, the attack model must consider active adversaries that can modify the transmitted messages and actively send many queries to group participants.

3. Analysis of Biswas's Group-DH Protocol

In this section, we briefly review Biswas's group key exchange protocol based on the two-party Diffie–Hellman technique (Diffie and Hellman, 1976). He claimed that the proposed protocol is contributory. We will show that the proposed protocol is not a contributory group key exchange protocol because the participants cannot confirm that their contributions were involved in establishing the group key.

In the two-party Diffie–Hellman key exchange technique (Diffie and Hellman, 1976), it allows two participants to generate a two-party shared key. Assume that two participants are U_i and U_j.U_i and U_j respectively possess two key pairs $(x_i \in Z_q^*,\ X_i = g^{x_i} \bmod p)$ and $(x_j \in Z_q^*,\ X_j = g^{x_j} \bmod p)$. Then, U_i and U_j can establish a shared key $g^{x_i x_j} \bmod p$. Biswas (2008) adopted the two-party Diffie–Hellman technique to propose a contributory group key exchange protocol, called the Group-DH protocol.

In the Group-DH protocol, let $U = \{U_1, U_2, \ldots, U_n\}$ be the set of participants that want to generate a common group key. Without loss of generality, let U_n be the group controller. U_n first constructs a two-party shared key with each group participants, respectively. Then, U_n and other participants in U use $n-1$ shared keys to generate a group key. The detailed steps are presented as follows:

Step 1. Initially, each participant U_i $(1 \leqslant i \leqslant n-1)$ selects a random value x_i in Z_q^*, and then computes and sends $X_i = g^{x_i} \bmod p$ to the group controller U_n. The group controller U_n also selects a random value x_n in Z_q^* and broadcasts $X_n = g^{x_n} \bmod p$ to each participant U_i. Thus, each participant U_i can compute a two-party shared key $K_i = g^{x_i x_n} \bmod p$ $(1 \leqslant i \leqslant n-1)$, with the group controller.

Step 2. The group controller U_n computes the group key$K = g^{\prod_{1 \leqslant j \leqslant n-1} K_j} \bmod p$ and $Y_i = g^{\prod_{1 \leqslant j \leqslant n-1, j \neq i} K_j} \bmod p$, for $i = 1, 2, \ldots, n-1$. Then, U_n respectively sends Y_i to U_i, where $1 \leqslant i \leqslant n-1$. Finally, each participant U_i $(1 \leqslant i \leqslant n-1)$ can generate the group key $K = Y_i^{K_i} \bmod p$.

Obviously, each participant can obtain the same group key $K = g^{K_1 K_2, \ldots, K_{n-1}} \bmod p$. However, in the following we show that Biswas's Group-DH protocol is not a contributory one because the group controller can predetermine the group key.

Claim 1. *In Biswas's Group-DH protocol, the group controller can predetermine the group key by himself. Thus, it is not a contributory group key exchange protocol.*

Proof. Let U_n be the group controller. In Step 1, U_n can construct a two-party shared key K_i with each participant U_i, for $i = 1, 2, \ldots, n-1$. The group controller U_n selects a predetermined group key R to replace the computing value $K = g^{\prod_{1 \leqslant j \leqslant n-1} K_j} \bmod p$ in Step 2. Then U_n computes $Y_i = (R)^{K_i^{-1}} \bmod p$, for $i = 1, 2, \ldots, n-1$. The group controller U_n respectively sends Y_i to U_i. Obviously, each participant U_i still obtains the same group key R by computing $R = Y_i^{K_i} \bmod p$. That is, the group key is predetermined only by the group controller U_n. Therefore, Biswas's Group-DH protocol is not contributory group key exchange one. □

4. Improvement and Security Analysis

4.1. *Our Improvement*

Here, we propose an improvement on Biswas's Group-DH protocol (Biswas, 2008). The system parameters are the same as ones in the Biswas's protocol reviewed in Section 2.1. The detailed steps are presented as follows.

Step 1. Each participant U_i $(1 \leqslant i \leqslant n-1)$ selects a random value x_i in Z_q^*, and then computes and sends $X_i = g^{x_i} \bmod p$ to the group controller U_n. The group controller U_n also selects a random value x_n in Z_q^* and sends $X_n = g^{x_n} \bmod p$ to each participant U_i. Then, each participant U_i and the group controller U_n can compute a two-party shared key $K_i = g^{x_i x_n} \bmod p$ $(1 \leqslant i \leqslant n-1)$.

Step 2. The group controller U_n selects a random value x in Z_q^* and computes $Y = g^x \bmod p$ and $Y_i = Y^{K_i^{-1}} \bmod p$, for $i = 1, 2, \ldots, n-1$. Then, U_n broadcasts $(Y_1, Y_2, \ldots, Y_{n-1})$ to each participant. Finally, each participant U_i $(1 \leqslant i \leqslant n-1)$ can compute the group key $K = H(Y_i^{K_i}, Y_1, Y_2, \ldots, Y_{n-1})$.

4.2. *Security Analysis*

Under the security definitions presented in Section 2.2, we show that the improved protocol is a secure contributory group key exchange protocol. We need two security assumptions: the Decision Diffie–Hellman assumption (Boneh, 1998) and a secure one-way hash function assumption (Bellare and Rogaway, 1993; NIST/NSA, 2005).

Assumption 1 [Decision Diffie–Hellman Assumption]. For a given $y_a = g^{x_a} \bmod p$ and $y_b = g^{x_b} \bmod p$, where x_a and x_b are randomly chosen from Z_q^*, the following two tuples of random variables $(y_a, y_b, g^{x_a x_b} \bmod p)$ and (y_a, y_b, R), where R is a random value in G_q, are computationally indistinguishable.

Assumption 2 [One-way Hash Function Assumption]. There exists a secure one-way hash function, $H\colon S = \{0,1\}^* \to L = \{0,1\}^l$, where l is a fixed-length, that satisfies the following requirements. (i) Given any $y \in L$, it's hard to find $x \in S$ such that $H(x) = y$. (ii) Given any $x \in S$, it's hard to find $x' \in S$ such that $x' \neq x$ and $H(x') = H(x)$. (iii) It's hard to find $x, x' \in S$ such that $x' \neq x$ and $H(x') = H(x)$.

In the following theorem, we show that the improved protocol is a group key exchange protocol with verifiably contributory property.

Theorem 1 [Contributiveness]. *Under the one-way hash function assumption, if an identical group key can be established by each participant, then each participant is assured that his/her contribution was included in the group key.*

Proof. According to the improved protocol, the group controller U_n broadcasts Y_i, for $i = 1, 2, \ldots, n-1$, to each participant. Each client U_i $(1 \leqslant i \leqslant n-1)$ may use his/her secret value K_i to compute an identical group key K. Since an identical group key K has been established, this means that the following equation holds.

$$\begin{aligned} K &= H(Y_1^{K_1}, Y_1, Y_2, \ldots, Y_{n-1}) = H(Y_2^{K_2}, Y_1, Y_2, \ldots, Y_{n-1}) = \cdots \\ &= H(Y_{n-1}^{K_{n-1}}, Y_1, Y_2, \ldots, Y_{n-1}). \end{aligned}$$

Under the one-way hash function assumption, we have an identical value V such that $V = Y_1^{K_1} \bmod p = Y_2^{K_2} \bmod p = \cdots = Y_{n-1}^{K_{n-1}} \bmod p$. Thus, we have

$$\begin{aligned} &Y_1 = V^{K_1^{-1}} \bmod p, \\ &Y_2 = V^{K_2^{-1}} \bmod p, \\ &\ldots \\ &Y_{n-1} = V^{K_{n-1}^{-1}} \bmod p. \end{aligned}$$

Since $K = H(Y_i^{K_i}, Y_1, Y_2, \ldots, Y_{n-1})$, we have $K = H(V, V^{K_1^{-1}}, V^{K_2^{-1}}, \ldots, V^{K_{n-1}^{-1}})$. Thus, we say that the group key K contains all participants' secret value K_i. Since $K_i = X_n^{x_i} \bmod p$, for $i = 1, 2, \ldots, n-1$, each participant ensures that his/her contribution x_i was included in the group key K. □

In the following theorem, we use the contradiction proof technique to prove that the improved protocol is secure against passive attacks under the Decision Diffie–Hellman assumption. Assume that there is an efficient algorithm A run by a passive attacker that can distinguish the established group key of the improved protocol from a random value. We can then adopt the algorithm A to be a subroutine to construct another efficient algorithm A' to solve the Decision Diffie–Hellman assumption.

Theorem 2 [Passive attack]. *Under the Decision Diffie–Hellman assumption, the improved protocol is secure against passive attacks.*

Proof. A passive attacker tries to learn secret information about the group key by listening to the communication channel. The passive attacker may obtain $X_i = g^{x_i} \bmod p$, for $i = 1, 2, \ldots, n$ and $Y_j = Y^{K_j^{-1}} \bmod p$, for $j = 1, 2, \ldots n-1$, where $K_j = g^{x_j x_n} \bmod p$. In the following we show that the passive attacker cannot get any information about the group key $K = H(Y_i^{K_i}, Y_1, Y_2, \ldots, Y_{n-1})$. Under the Decision

Diffie–Hellman Assumption, we shall prove that (X_i, Y_j, K) and (X_i, Y_j, K'), for $i = 1, 2, \ldots, n$ and $j = 1, 2, \ldots, n-1$, are computationally indistinguishable, where K' is a random value in G_q.

By contradiction, assume that there exists an algorithm A, which can efficiently distinguish (X_i, Y_j, K) from (X_i, Y_j, K'), for $i = 1, 2, \ldots, n$ and $j = 1, 2, \ldots, n-1$. Based on the algorithm A, we show that we can construct another algorithm A that can efficiently distinguish $(y_a, y_b, g^{x_a x_b} \bmod p)$ from (y_a, y_b, R), where $y_a = g^{x_a} \bmod p$, $y_b = g^{x_b} \bmod p$, and $x_a, x_b \in Z_q^*$.

Let y_a, y_b and R be the inputs of algorithm A'. Without loss of generality, assume that $X_1 = y_a = g^{x_a} \bmod p$ and $X_n = y_b = g^{x_b} \bmod p$. Then, algorithm A' randomly selects $s, t_1, t_2, \ldots, t_{n-2}$ from Z_q^* and computes the following values:

$$
\begin{aligned}
&X_1 = y_a, \qquad Y_1 = (g^s)^R \bmod p,\\
&X_2 = X_1^{t_1} \bmod p, \qquad Y_2 = Y_1^{t_1} \bmod p,\\
&X_3 = X_1^{t_2} \bmod p, \qquad Y_3 = Y_1^{t_2} \bmod p,\\
&\vdots\\
&X_{n-1} = X_1^{t_{n-2}} \bmod p, \qquad Y_{n-1} = Y_1^{t_{n-2}} \bmod p,\\
&X_n = y_b.
\end{aligned}
$$

Therefore, the algorithm A' has constructed X_i, for $i = 1, 2, \ldots, n$ and Y_j, for $j = 1, 2, \ldots, n-1$. The algorithm A' then calls A with these values. It is obvious that if $K' = H(g^s, Y_1, Y_2, \ldots, Y_{n-1})$ holds, then $R = g^{x_a x_b} \bmod p$ also holds. That is, A' can apply A to efficiently distinguish $(y_a, y_b, g^{x_a x_b} \bmod p)$ and (y_a, y_b, R), which is a contradiction for the Decision Diffie–Hellman problem assumption. Thus, the improved protocol is secure against passive attacks under the Decision Diffie–Hellman problem assumption. □

5. Discussions

For convenience, the following notations are used to measure the communicational cost and the computational complexity.

- $|m|$: the bit length of a transmitted message m;
- T_{EXP}: the time of executing a modular exponentiation;
- T_{INV}: the time of executing a modular inverse;
- T_{MUL}: the time of executing a modular multiplication;
- T_H: the time of executing the one-way hash function $H()$.

Considering the computational complexity for the group controller in Step 1, the group controller U_n computes X_n, and K_i, for $i = 1, 2, \ldots, n-1$. Thus, it requires nT_{EXP}. In Step 2, the group controller U_n requires $nT_{\mathrm{EXP}} + (n-1)T_{\mathrm{INV}} + T_H$ to computes K, Y and Y_i for $i = 1, 2, \ldots, n-1$. Therefore, the computational complexity for the group controller is $2nT_{\mathrm{EXP}} + (n-1)T_{\mathrm{INV}} + T_H$. Let us discuss the computational

complexity for each participant U_i. In the improved protocol each participant U_i computes X_i, K_i and K, where $1 \leqslant i \leqslant n-1$. Thus, $3T_{\mathrm{EXP}} + T_H$ is required for each participant. By the performance evaluation for modular exponentiation and hash function on a personal digital assistant (PDA) device in Tseng (2007b), the improved protocol is suitable for low-power participant device in a network environment.

Here, let us analyze the communicational cost for the improved protocol. Obviously, each participant U_i sends only X_i to the group controller. The group controller broadcasts X_n and Y_i for $i = 1, 2, \ldots, n-1$ to all participants. Thus, the communicational costs of each participant and the group controller are $|p|$ and $n|p|$, respectively.

Because both Biswas's (2008) protocol and the improved protocol are non-authenticated, we consider several non-authenticated group key exchange protocols (including group key distribution and group key agreement). Table 1 lists the comparisons among a star-

Table 1
Comparisons between the previously proposed protocols and our improved protocol

	SGKD protocol (Burmester and Desmedt, 1994)	FGKA protocol (Burmester and Desmedt, 2005)	Biswas's Group-DH protocol (Biswas, 2008)	Improved protocol
Contributiveness	No	Yes	No (shown in Section 3)	Yes
Number of uni-casting	$n-1$	0	$2n-2$ (or $n-1$)[a]	$n-1$
Number of broadcasting	2	$2n$	1 (or 2)[a]	2
Uni-casting message size by each participant	$\|p\|$	0	$\|p\|$	$\|p\|$
Broadcasting message size by each participant	0	$2\|p\|$	0	0
Uni-casting message size by the group controller	$\|p\|$	No group controller	$\|p\|$	$\|p\|$
Broadcasting message size by the group controller	$(n-1)\|p\|$	No group controller	$(n-1)\|p\|$	$(n-1)\|p\|$
Computational costs for each participant	$2T_{\mathrm{EXP}}$	$4T_{\mathrm{EXP}}+$ $(2n-1)T_{\mathrm{MUL}}$	$3T_{\mathrm{EXP}}$	$3T_{\mathrm{EXP}} + T_H$
Computational costs for the group controller	$nT_{\mathrm{EXP}}+$ $(n-2)T_{\mathrm{MUL}}$	No group controller	$2nT_{\mathrm{EXP}}+$ $(2n-5)T_{\mathrm{MUL}}$	$2nT_{\mathrm{EXP}}+(n-$ $1)T_{\mathrm{INV}} + T_H$

[a] In Biswas's Group-DH protocol, the group controller may use a broadcasting to replace $n-1$ unicasting. Here we use the broadcasting to compare the message size.

based group key distribution (SGKD) protocol (Burmester and Desmedt, 1994), a famous group key agreement (FGKA) protocol (Burmester and Desmedt, 2005), Biswas's Group-DH protocol (Biswas, 2008) and the improved protocol. The comparisons are considered in terms of the contributory property, the required numbers of uni-casting and broadcasting, as well as both the message size and the computational complexity required for each participant and the group controller. According to Table 1, the computational complexity required by each participant in the SGKD protocol has the best performance but the SGKD protocol does not provide contributiveness. In the FGKA protocol, it is a contributory group key exchange protocol but each participant requires more computational costs as compared to other protocols. The computational complexity required by each participant in the improved protocol increases only T_H than one in Biswas's Group-DH protocol. The point of the improved protocol is to allow each participant can confirm that his/her contribution is involved in the established group key. On the contrary, the group controller in Biswas's Group-DH protocol is easy to predetermine the group key.

In the following, let us discuss participant authentication. Mutual authentication ensures each participant to confirm that other participants did actually join in the group key establishment process. Both Biswas's (2008) protocol and the improved protocol are non-authenticated group key exchange protocols. By its very nature, a non-authenticated group key exchange protocol cannot provide participant and message authentication, so it must rely on the authenticated network channel. Nevertheless, if the improved protocol is employed in cellular mobile networks (GPRS, 2002) or wireless local area networks (ANSI/IEEE, 2005), one alternative is that each participant may use the authentication procedures (Tseng, 2006; Tseng *et al.* 2008) provided by these attached networks to authenticate with the group controller each other in advance.

6. Conclusions

We have presented that Biswas's group key exchange protocol based on the Diffie–Hellman technique has a security weakness. Biswas's Group-DH protocol is not a real contributory and violates the contributory property of group key agreement. We have proposed a secure group key exchange protocol with verifiably contributory property based on the same two-party Diffie–Hellman technique. Meanwhile, we have demonstrated that the improved protocol is provably secure against passive attacks under the decisional Diffie–Hellman problem assumption.

Acknowledgments. The authors would like to thank the anonymous referees for their valuable comments and suggestions.

References

ANSI/IEEE: Wireless LAN Media Access Control (MAC) and Physical Layer (PHY) Specifications. ANSI/IEEE Std. 802.11: 2005 (E) Part 11, ISO/IEC 8802-11, 2005.

Bellare, M., Rogaway, P. (1993). Random oracles are practical: a paradigm for designing efficient protocols. In: *ACM Conference on Computer and Communications Security 1993 (ACM CCS '93)*, pp. 62–73.

Biswas, G.P. (2008). Diffie–Hellman technique: extended to multiple two-party keys and one multi-party key. *IET Information Security*, 2(1), 12–18.

Boneh, D. (1998). The decision Diffie–Hellman problem. In: *Proc. 3rd Algorithmic Number Theorey Symp.*, LNCS, Vol. 1423, pp. 48–63.

Bresson, E., Manulis, M. (2008). Contributory group key exchange in the presence of malicious participants. *IET Information Security*, 2(3), 85–93.

Bresson, E., Chevassut, O., Pointcheval, D. (2002). Dynamic group Diffie–Hellman key exchange under standard assumptions. In: *Proc. Advances in Cryptology – Eurocrypt 2002*, LNCS, Vol. 2332, pp. 321–336.

Burmester, M., Desmedt, Y. (1994). A secure efficient conference key distribution system. In: *Proc. Advances in Cryptology – Eurocrypt'94*, LNCS, Vol. 950, pp. 275–286.

Burmester, M., Desmedt, Y. (2005). A secure and scalable group key exchange system. *Information Processing Letters*, 94(3), 137–143.

Chien, H.Y., Jan, J.K. (2004). Improved authenticated multiple-key agreement protocol without using conventional one-way function. *Applied Mathematics and Computation*, 147(2), 491–497.

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

Gao, W., Wang, G., Wand, X., Yang, Z. (2009). One-round ID-based threshold signature scheme from bilinear pairings. *Informatica*, 20(4), 461–476.

General Packet Radio Services (GPRS) Service Description (Stage 2), TS 122 060, ETSI, June 2002.

Hwang, M.S., Yang, W.P. (1995). Conference key distribution schemes for secure digital mobile communications. *IEEE J. Sel. Areas Commun.*, 13(2), 416–420.

Hwang, M.S., Lo, J.W., Liu, C.H. (2004). Enhanced of key agreement protocols resistant to a denial-of-service attack. *Fundamenta Informaticae*, 61(3), 389–398.

Ingemaresson, I., Tang, D.T., Wong, C.K. (1982). A conference key distribution system. *IEEE Trans. Infom. Theory*, 28(5), 714–720.

Kim, Y., Perrig, A., Tsudik, G. (2004a). Group key agreement efficient in communication. *IEEE Trans. Comput.*, 53(7), 905–921.

Kim, Y., Perrig, A., Tsudik, G. (2004b). Tree-based group key agreement. *ACM Trans. Inf. Syst. Secur.*, 7(1), 60–96.

Lee, N.Y., Wu, C.N., Wang, C.C. (2008). Authenticated multiple key exchange protocols based on elliptic curves and bilinear pairings. *Computers and Electrical Engineering*, 34(1), 12–20.

Moyer, M.J., Rao, J.R., Rohatg, P. (1999). A survey of security issues in multicast communications. *IEEE Network*, 13(6), 12–23.

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

Steiner, M., Tsudik, G., Waidner, M. (1996). Diffie–Hellman key distribution extended to group communication. In: *Proc. 3rd ACM Conf. Computer Commun. Security*, pp. 31–37.

Steiner, M., Tsudik, G., Waidner, M. (1998). CLIQUES: a new approach to group key agreement. In: *Proc. 18th Int. Conf. Distributed Computing Syst. (ICDCS'98)*, pp. 380–387.

Sun, X., Li, J., Yin, H., Chen, G. (2010). Delegatability of an identity based strong designated verifier signature scheme. *Informatica*, 21(1), 117–122.

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

Tseng, Y.M. (2006). GPRS/UMTS-aided authentication protocol for wireless LANs. *IEE Proceedings – Communications*, 153(6), 810–817.

Tseng, Y.M. (2007a). An efficient two-party identity-based key exchange protocol. *Informatica*, 18(1), 125–136.

Tseng, Y.M. (2007b). A secure authenticated group key agreement protocol for resource-limited mobile devices. *The Computer Journal*, 50(1), 41–52.

Tseng, Y.M., Wu, T.Y., Wu, J.D. (2008). A pairing-based user authentication scheme for wireless clients with smart cards. *Informatica*, 19(2), 285–302.

Yoon, E.J., Yoo, K.Y. (2009). Robust key exchange protocol between set-top box and smart card in DTV broadcasting. *Informatica*, 20(1), 139–150.

Yuh-Min Tseng is currently a professor in the Department of Mathematics, National Changhua University of Education, Taiwan. He is members of IEEE Computer Society, IEEE Communications Society, IEICE and the Chinese Cryptology and Information Security Association (CCISA). In 2006, his paper obtained the Wilkes Award from *The British Computer Society*. He is also editors of three international journals: *Computer Standards & Interfaces*, *International Journal of Security and Its Applications,* as well as *Wireless Engineering and Technology.* His research interests include cryptography, network security, computer network and mobile communications.

Tsu-Yang Wu received the BS and the MS degrees in Department of Applied Mathematics, Tatung University, Taiwan, in 2003 and 2005, respectively. He is currently a PhD candidate in Department of Mathematics, National Changhua University of Education, Taiwan. His research interests include applied cryptography, pairing-based cryptography and computer network.

Bendradarbiaujant sukurto grupinio rakto, naudojančio Diffie–Hellman'o metodą, analizė ir patobulinimas

Yuh-Min TSENG, Tsu-Yang WU

2008 m. Biswas pasiūlė bendradarbiaujant sukurto grupinio rakto apsikeitimo tarp vartotojų protokolą Group-DH. Straipsnyje parodyta, kad šis protokolas nėra grupinis apsikeitimo raktais protokolas. Pasiūlytas patobulintas grupinio apsikeitimo raktais protokolas, kuriame panaudotas Diffie–HellmanÆo metodas. Kai suformuojamas grupinis raktas, kiekvienas dalyvis gali patvirtinti, kad jis dalyvavo kuriant šį raktą. Parodyta, kad patobulintas protokolas yra atsparus pasyviosioms atakoms ir tenkina skaičiavimo sudėtingumo reikalavimą.