

# Weakness of Shim's New ID-based Tripartite Multiple-key Agreement

## Protocol

Jue-Sam Chou\*, Chu-Hsing Lin\*\* and Chia-Hung Chiu\*\*

\*Department of Information management,

Nanhua university

No.32, Chung Keng Li, Dalin

Chaiyi, Taiwan

jschou@mail.nhu.edu.tw

\*\*Department of Computer Science and Information Engineering,

Tunghai University

No.181, Sec. 3, Taichung Port Rd., Situn District

Taichung, Taiwan

chlin@thu.edu.tw, hdilwy@islab.csie.thu.edu.tw

*Abstract* – Shim and Woo proposed a new ID-based tripartite multiple-key agreement protocol in 2005. In their scheme, they pointed out the vulnerable of Liu et al. protocol proposed in 2003. Although their scheme had solve the man-in-the-middle attack, but it still suffers from the impersonation attack, any malicious user can launch an impersonation attack on their protocol.

*Keyword* - ID-based, Weil-pairing, Impersonation attack, Tripartite authenticated key agreement

## 1. Introduction

The first one-round tripartite Diffie-Hellman key agreement protocol [1] was proposed by Joux in 2000. However, Joux's protocol does not authenticate the three communicating entities, and is vulnerable to the man-in-the-middle attack. Recently Liu et al. proposed an ID-based one round authenticated tripartite key agreement protocol with pairing[2,4-12] (LZC protocol) which results in eight session keys in the agreement. However, their scheme could not prevent the "unknown key share" attack proposed by Shim et al. in 2005[3]. In [3], they suggest a method to resist the unknown key share attack. This article will show that their

protocol is still vulnerable to the impersonation attack.

## 2. The Background

In this section, we will first briefly review the basic concept and some properties of bilinear pairing then review the Shim's protocol.

### 2.1. Bilinear pairing

Let  $\mathbb{G}_1$  be a cyclic group generated by  $P$ , whose order is a prime  $q$  and  $\mathbb{G}_2$  be a cyclic multiplicative group of the same order  $q$ . We assume that the discrete logarithm problem (DLP) in

both  $\mathbb{G}_1$  and  $\mathbb{G}_2$  are hard. Let  $e: \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$  be a pairing which satisfies the following conditions:

- (1) Bilinear:  $e(aP, bQ) = e(P, Q)^{ab}$ , for any  $a, b \in \mathbb{Z}$  and  $P, Q \in \mathbb{G}_1$ .
- (2) Non-degenerate: there exists  $P \in \mathbb{G}_1$  and  $Q \in \mathbb{G}_1$  such that  $e(P, Q) \neq 1$ .
- (3) Computability: there is an efficient algorithm to compute  $e(P, Q)$  for all  $P, Q \in \mathbb{G}_1$ .

### 2.2 Shim's protocol

(1) **Setup:** Key generation center (KGC) chooses a random  $s \in \mathbb{Z}_q^*$  and set  $P_{pub} = sP$ . The KGC publishes the system parameters  $\langle \mathbb{G}_1, \mathbb{G}_2, q, e, P, P_{pub}, H, H_1 \rangle$  and keep  $s$  as a secret master key, which is known only by itself.

(2) **Private key extraction:** A user submits his identity information ID to KGC. KGC computes the user's public key as  $Q_{ID} = H_1(ID)$  and returns  $S_{ID} = sQ_{ID}$  to the user as his private key.

(3) **Scheme:** Assume that there are three entities  $A, B, C$ . Each chooses two random numbers then computers their corresponding parameters. For examples,  $A$  chooses random numbers  $a$  and  $a'$ , and computes  $P_A = aP, P'_A = a'P, T_A = S_A + a^2P + a'P_{pub}$ .  $B$  chooses random numbers  $b$  and  $b'$ , and computes  $P_B = bP, P'_B = b'P, T_B = S_B + b^2P + b'P_{pub}$ .  $C$  chooses random numbers  $c$  and  $c'$ , and computes  $P_C = cP, P'_C = c'P, T_C = S_C + c^2P + c'P_{pub}$ . After the computing, they broadcast their values  $(P_A, P'_A, T_A), (P_B, P'_B, T_B)$  and  $(P_C, P'_C, T_C)$  to all the other parties.

When receiving the other party's communicational parameters, each party performs his/her own verifying equation. For example,  $A$  checks whether the following equation holds.

$$\begin{aligned} e(T_B + T_C, P) &= e(S_B + b^2P + b'P_{pub} + S_C + c^2P + c'P_{pub}, P) \\ &= e(sP_B + b'sP + sP_C + c'sP, P) e(b^2, P) e(c^2, P) \\ &= e(Q_B + Q_C + P'_B + P'_C, P_{pub}) e(P_B, P_B) e(P_C, P_C). \end{aligned}$$

$B$  and  $C$  also do their corresponding verification to check if the equations hold.

If each equation holds, then  $A, B$  and  $C$  compute the eight session keys respectively, as in the LZC protocol, as follows.

$A$  computes:

$$\begin{aligned} K_A^{(1)} &= e(P_B, P_C)^a, K_A^{(2)} = e(P_B, P'_C)^a, K_A^{(3)} = e(P'_B, P_C)^a, \\ K_A^{(4)} &= e(P'_B, P'_C)^a, K_A^{(5)} = e(P_B, P_C)^{a'}, K_A^{(6)} = e(P_B, P'_C)^{a'}, \\ K_A^{(7)} &= e(P'_B, P_C)^{a'}, K_A^{(8)} = e(P'_B, P'_C)^{a'} \end{aligned}$$

$B$  computes:

$$\begin{aligned} K_B^{(1)} &= e(P_A, P_C)^b, K_B^{(2)} = e(P_A, P'_C)^b, K_B^{(3)} = e(P_A, P_C)^{b'}, \\ K_B^{(4)} &= e(P_A, P'_C)^{b'}, K_B^{(5)} = e(P'_A, P_C)^b, K_B^{(6)} = e(P'_A, P'_C)^b, \\ K_B^{(7)} &= e(P'_A, P_C)^{b'}, K_B^{(8)} = e(P'_A, P'_C)^{b'} \end{aligned}$$

$C$  computes:

$$\begin{aligned} K_C^{(1)} &= e(P_A, P_B)^c, K_C^{(2)} = e(P_A, P'_B)^c, K_C^{(3)} = e(P_A, P_B)^{c'}, \\ K_C^{(4)} &= e(P_A, P'_B)^{c'}, K_C^{(5)} = e(P'_A, P_B)^c, K_C^{(6)} = e(P'_A, P'_B)^c, \\ K_C^{(7)} &= e(P'_A, P_B)^{c'}, K_C^{(8)} = e(P'_A, P'_B)^{c'} \end{aligned}$$

We can find that

$$K_A^{(1)} = K_B^{(1)} = K_C^{(1)} = e(P, P)^{abc} = K^{(1)}. \text{ Similarly,}$$

we also have

$$K_A^{(i)} = K_B^{(i)} = K_C^{(i)} = K^{(i)}, \text{ for } i = 2, 3, \dots, 8. \text{ Each entity}$$

then takes the eight computed values  $K^{(i)}$

$(i = 1, 2, \dots, 8)$  as the final session keys, where

$$\begin{aligned} K^{(1)} &= e(P, P)^{abc}, K^{(2)} = e(P, P)^{abc'}, K^{(3)} = e(P, P)^{ab'c}, \\ K^{(4)} &= e(P, P)^{ab'c'}, K^{(5)} = e(P, P)^{a'bc}, K^{(6)} = e(P, P)^{a'bc'}, \\ K^{(7)} &= e(P, P)^{a'b'c}, K^{(8)} = e(P, P)^{a'b'c'} \end{aligned}$$

### 3. Our Attack

In this section, we show that how the Shim's protocol is insecure against the impersonation attack. Assume that there is an adversary  $X$ , who wants to impersonate  $B$  to communicate with  $A$  and  $C$  shown as follows:

**Step1:**  $X$  computes  $P_X = xP, P'_X = x'P - Q_B, T_X = x'P_{pub} + x^2P$  and broadcast them to  $A$  and  $C$ . After receiving the broadcast parameters sent by  $X$  and  $C$ ,  $A$  verify the equation and we will find that the equation would be hold show below:

$$\begin{aligned} e(T_X + T_C, P) &= e(x'P_{pub} + x^2P + S_C + c^2P + c'P_{pub}, P) \\ &= e(x'P + Q_C + c'P, P_{pub}) e(x^2P + c^2P, P) \\ &= e(x'P - Q_B + Q_B + Q_C + c'P, P_{pub}) e(xP, xP) e(cP, cP) \\ &= e(P'_X + Q_B + Q_C + c'P, P_{pub}) e(xP, xP) e(cP, cP) \\ &= e(Q_B + Q_C + P'_X + P'_C, P_{pub}) e(P_X, P_X) e(P_C, P_C) \end{aligned}$$

**Step2:**  $C$  can obtain his parameters sent from other parties and also pass his/her verification by the equation

$$e(T_A + T_X, P) = e(Q_A + Q_B + P'_X + P'_A) e(P_A, P_A) e(P_X, P_X)$$

**Step3:** After that,  $A$  can compute the session keys as follows.

$$\begin{aligned} K_A^{(1)} &= e(P_X, P_C)^a, K_A^{(2)} = e(P_X, P'_C)^a, K_A^{(3)} = e(P'_X, P_C)^a, \\ K_A^{(4)} &= e(P'_X, P'_C)^a, K_A^{(5)} = e(P_X, P_C)^{a'}, K_A^{(6)} = e(P_X, P'_C)^{a'}, \\ K_A^{(7)} &= e(P'_X, P_C)^{a'}, K_A^{(8)} = e(P'_X, P'_C)^{a'} \end{aligned}$$

And  $C$  can compute the session keys as follows:

$$\begin{aligned} K_C^{(1)} &= e(P_A, P_X)^c, K_C^{(2)} = e(P_A, P_X)^{c'}, K_C^{(3)} = e(P_A, P'_X)^c, \\ K_C^{(4)} &= e(P_A, P'_X)^{c'}, K_C^{(5)} = e(P'_A, P_X)^c, K_C^{(6)} = e(P'_A, P_X)^{c'}, \\ K_C^{(7)} &= e(P'_A, P'_X)^c, K_C^{(8)} = e(P'_A, P'_X)^{c'} \end{aligned}$$

Each entity,  $A$  and  $C$ , then takes the following eight computed values  $K^{(i)} (i=1, \dots, 8)$  as their final session keys

$$\begin{aligned} K^{(1)} &= e(P, P)^{ac}, K^{(2)} = e(P, P)^{ac'}, K^{(3)} = e(P, P)^{ac} e(Q_B, P)^{-ac}, \\ K^{(4)} &= e(P, P)^{ac'} e(Q_B, P)^{-ac'}, K^{(5)} = e(P, P)^{a'xc}, K^{(6)} = e(P, P)^{a'xc'}, \\ K^{(7)} &= e(P, P)^{a'xc} e(Q_B, P)^{-a'xc}, K^{(8)} = e(P, P)^{a'xc'} e(Q_B, P)^{-a'xc'} \end{aligned}$$

Finally, the adversary  $X$  can also get the same session keys  $K^{(1)}, K^{(2)}, K^{(5)}$  and  $K^{(6)}$  as  $A$  and  $C$

by computing:

$$\begin{aligned} K_X^{(1)} &= e(P_A, P_C)^x = e(P, P)^{axc} \equiv K^{(1)}, \\ K_X^{(2)} &= e(P_A, P'_C)^x = e(P, P)^{axc'} \equiv K^{(2)}, \\ K_X^{(5)} &= e(P'_A, P_C)^x = e(P, P)^{a'xc} \equiv K^{(5)}, \\ K_X^{(6)} &= e(P'_A, P'_C)^x = e(P, P)^{a'xc'} \equiv K^{(6)}. \end{aligned}$$

As a result,  $X$  can share these four keys  $K^{(1)}, K^{(2)}, K^{(5)}, K^{(6)}$  in the eight session keys. Under this situation,  $A$  and  $C$  think these four session keys are shared with  $B$ , but indeed, they are shared with  $X$ . Besides, both  $A$  and  $C$  come to share the same eight session keys. Thus, the impersonation attack on four of the eight session keys can be successfully mounted. More precisely, the attacker  $X$  can use these four session keys to communicate with  $A$  and  $C$ , and he can have one half of the probability to realize what the communication contents are between  $A$  and  $C$ .

### 4. Conclusion

In this article, we introduce Shim and Woo's new

ID-based tripartite multiple-key agreement protocol. Although their scheme secure against the man-in-the-middle attack, but by the attack step in Section 3 that show it can not resist an impersonation attack. How to design a secure and efficient ID-based authenticated tripartite multiple-key agreement scheme to prevent all kinds of attacks remains an open problem.

*Reference:*

- [1] A. Joux, A one-round protocol for tripartite Diffie-Hellman, *Proceedings of the 4<sup>th</sup> International Algorithmic Number Theory Symposium (ANTS-IV)*, LNCS 1838, July, 2000, pp.385-394.
- [2] S. Liu, F. Zhang, K. Chen, ID-based tripartite key agreement protocol with pairing, *IEEE International Symposium on Information Theory*, 2003, pp. 136-143, or available at Cryptology ePrint Archive, Report 2002/122.
- [3] Kyungah Shim and Sungsik Woo, Weakness in ID-based one round authenticated tripartite multiple-key agreement protocol with pairings, *Applied Mathematics and Computation*, Vol.166, Issue: 3, July 26, 2005, pp. 523-530.
- [4] R. Barua, R.Dutta, P. Sarkar, Extending Joux Protocol to Multi Party Key Agreements", *Indocrypt 2003*, Also available at <http://eprint.iacr.org/2003/062>.
- [5] P. S. L. M. Berreto, H. Y. Kim and M.Scott, Efficient algorithms for pairing-based cryptosystems, *Advances in Cryptology – Crypto '2002*, LNCS 2442, Springer-Verlag (2002), pp. 354-368.
- [6] A. Boldyreva, Efficient Threshold Signature, Multisignature and Blind Signature Schemes Based on the Gap-Diffie-Hellman-Group Signature Scheme, *PKC2003*, LNCS 2139, Springer-Verlag, 2003, pp. 31-46.
- [7] D. Boneh, X. Boyen, Short Signature without Random Oracles, In Christian Cachin and Jan Camenisch, editors. *Proceedings of Eurocrypt 2004*, LNCS, Springer-Verlag, 2004.
- [8] D. Boneh, M. Franklin, Identity Based Encryption from the Weil Pairing, *SIAM J. of Computing*, Vol.32, No. 3, pp. 586-615, 2003, Extended Abstract in Crypto 2001.
- [9] D. Boneh, B. Lynn, H. Shacham, Short signature from the Weil pairing. In *Proceedings of Asiacrypt 2001*.
- [10] D. Boneh, I. Mironov, V. Shoup, A secure Signature Scheme from Bilinear Maps, *CT-RSA-2003*, pp. 98-110.
- [11] D. Boneh, A. Silverberg, Applications of Multilinear forms Cryptography, Report 2002/080, <http://eprint.iacr.org>, 2002.
- [12] E. Fujisaki, T. Okamoto, Secure Integration of Asymmetric and Symmetric Encryption Schemes, in *Advances in Cryptology – Crypto '99*, LNCS 1666, Springer-Verlag, 1999.
- [13] Chu-Hsing Lin, and Hsiu-Hsia Lin, Secure One-Round Tripartite Authenticated Key Agreement Protocol from Weil Pairing, *Proceedings of International Conference on Advanced Information Networking and Applications (AINA 2005)*, Vol.2, March 25-30, 2005, pp. 135-138.
- [14] Chu-Hsing Lin, K. J. Huang and H. H. Lin, Improving Shim's tripartite authenticated key agreement protocol based on Weil pairing, *Proceedings of 14th Information Security Conference*, Taipei, Taiwan, June 10-11, 2004, pp. 250-255.