Security Analysis of Shim's Authenticated Key Agreement Protocols from Pairings

Hung-Min Sun and Bin-Tsan Hsieh[†]
Department of Computer Science,
National Tsing Hua University, Hsinchu, Taiwan, R.O.C.
hmsun@cs.nthu.edu.tw
[†]Department of Computer Science and Information Engineering,
National Cheng Kung University, Tainan, Taiwan, R.O.C.
bintsan@csie.ncku.edu.tw

Abstract

Recently, Shim proposed a tripartite authenticated key agreement protocol from Weil pairing to overcome the security flaw in Joux's protocol. Later, Shim also proposed an ID-based authenticated key agreement protocol which is an improvement of Smart's protocol in order to provide the forward secrecy. In this paper, we show that these two protocols are insecure against the key-compromise impersonation attack and the man-in-the-middle attack respectively.

Keywords: Cryptanalysis, Weil Pairing, ID-based, Key Agreement, Authentication

1 Introduction

Traditionally, asymmetric cryptographic schemes are based on either the discrete logarithm problem or the factoring problem. The most concerned issue in implementation of cryptographic schemes is the computation cost of modular exponentiation. To overcome such a problem, the elliptic curve cryptography becomes a good choice because it reduces the computation cost while remaining the same security level. It is noticed that the decision of Diffie-Hellman is regarded as a hard problem in discrete logarithm, however, it is not a hard problem in elliptic curve cryptography due to Weil pairing [1]. Weil pairing is a new primitive and is interesting to cryptography societies. Several cryptographic schemes [2][3][4][5][6] are designed based on the Weil pairing, and enjoy the convenience of the property of Weil pairing.

For a sound authenticated key exchange protocol, Wilson and Menezes [7] defined several desirable security attributes. We show these attributes in the following. Here we assume A and B are two honest entities.

1. **Known-Key Security** In each round of key agreement protocol, A and B should generate a unique secret key. Each key generated in one protocol round is independent and should not be exposed if other secret keys are compromised.

2. **Forward Secrecy** The Forward Secrecy property is that if A and B's secret keys are compromised, the session keys used in the past should not be recovered.

3. **Key-Compromise Impersonation** A protocol which is secure against the key compromise impersonation attack means that if A's secret key is compromised, the adversary who knows the value can not impersonate others to A.

4. **Unknown Key-Share** After the protocol, A ends up believing he shares a key with B, and B mistakenly believes that the key is instead shared with an adversary. Therefore, a sound authenticated key agreement protocol should prevent the unknown key-share situation.

In 2000, Joux [2] proposed a tripartite Diffie-Hellman key agreement protocol based on the Weil pairing. However, Shim [5] pointed out that Joux's protocol suffers from the man-in-the-middle attack and further proposed an improved tripartite authenticated key agreement protocol. Shim employed the public key infrastructure to overcome the security flaw in Joux's protocol and claimed that the improved protocol can withstand some attacks [5], such as the man-in-the-middle attack, the key-compromise impersonation attack, and the unknown key-share attack.

On the other hand, Smart [4] proposed an ID-based authenticated key agreement protocol based on Weil pairing. Later, Shim [6] pointed out that Smart's protocol does not provide the forward secrecy which is an important security requirement of an authenticated key agreement protocol. Shim [6] further proposed an efficient ID-based authenticated key agreement protocol to provide the forward secrecy. Shim also gave more security analysis to show that the proposed protocol provides other attractive security properties of an authentication key agreement protocol [7][8], such as known-key security, forward secrecy, key compromise impersonation resilience, and unknown key-share resilience.

In this paper, we show that both Shim's protocols are still insecure against the key-compromise impersonation attack and the man-in-the-middle attack respectively. The rest of this paper is organized in the following. In Section 2, we briefly review Shim's tripartite authenticated key agreement protocol from Weil pairing and show its insecurity. In Section 3, we review Shim's ID-based authenticated key agreement protocol from Weil pairing and point out its weakness. We conclude this paper in Section 4.

2 On the security of Shim's tripartite authenticated key agreement protocol

The protocol proposed by Shim is a one round tripartite authenticated key agreement protocol which enables three parties to obtain a common session key in a single round. We describe the protocol as follows:

2.1 Setup

`System Setup`

Let p be a prime such that $p = 6q - 1$ for some prime q, and E be a supersingular elliptic curve defined by $y^2 = x^3 + 1$ over F_p. Let P be a points generator of the group with order $q = (p+1)/6$ and the set of points form a cyclic group, denoted as G_1. Let G_2 be the subgroup of $F^*_{p^2}$ that contains all elements of order q. The modified Weil pairing on the curve E is a bilinear mapping $\hat{e} : G_1 \times G_1 \rightarrow G_2$ that has the following properties:

(1) Bilinear: For any $P, Q \in G_1$ and $a, b \in Z$, we have $\hat{e}(aP, bQ) = e(P, Q)^{ab}$.

(2) Non-degenerate: $\hat{e}(P, P)$ is a generator of G_2.

(3) Computable: Let $P, Q \in G_1$, there is an efficient algorithm to compute $\hat{e}(P, Q) \in G_2$.

`Key Setup`

The public domain parameters $\{p,\ q,\ E,\ P,\ \hat{e}\}$ are common to all entities. A user R's public key is denoted as $Y_R = rP$, where r is R's secret key. $Cert_R$ denotes the certificate of user R.

2.2 Shim's tripartite authenticated key agreement protocol

First, A, B, and C choose random numbers x, y, and z and compute $T_A = x(aP)$, $T_B = y(bP)$, $T_C = z(cP)$, respectively. Next, they broadcast the computed values and their certificates to others.

$$
\begin{aligned}
A &: T_A = x(aP), Cert_A \\
B &: T_B = y(bP), Cert_B \\
C &: T_C = z(cP), Cert_C
\end{aligned}
$$

The keys computed by A, B, and C are:

$$
\begin{aligned}
K_A &= \hat{e}(T_B, T_C)^{ax\hat{e}(Y_B, Y_C)^a} = \hat{e}(P, P)^{abcxyz\hat{e}(P,P)^{abc}} \\
K_B &= \hat{e}(T_A, T_C)^{by\hat{e}(Y_A, Y_C)^b} = \hat{e}(P, P)^{abcxyz\hat{e}(P,P)^{abc}} \\
K_C &= \hat{e}(T_A, T_B)^{cz\hat{e}(Y_A, Y_B)^c} = \hat{e}(P, P)^{abcxyz\hat{e}(P,P)^{abc}}
\end{aligned}
$$

2.3 Key compromise impersonation attack on Shim's tripartite authenticated key agreement protocol

In this subsection, we give the following scenario to show that Shim's protocol is insecure against the key compromise impersonation attack. That is an adversary Adv who knows A's secret key a can impersonate B to A.

First, the adversary Adv selects a random number u and computes $T_B^{'} = uP$. Next, Adv sends $T_B^{'}$ and $Cert_B$ to A. Assuming C is honest, therefore, A receives two messages from Adv and C as follows:

$$Adv \rightarrow A : T_B^{'} = uP, Cert_B$$
$$C \rightarrow A : T_C = z(cP), Cert_C.$$

Upon the received messages, A computes the session key K_A:

$$K_A = \hat{e}(T_B^{'}, T_C)^{ax\hat{e}(Y_B,Y_C)^a} = \hat{e}(P,P)^{axucz\hat{e}(P,P)^{abc}}.$$

Similarly, Adv receives the two messages from honest A and C as follows:

$$A \rightarrow Adv : T_A = x(aP), Cert_A$$
$$C \rightarrow Adv : T_C = z(cP), Cert_C.$$

Finally, Adv can compute the common session key K_E:

$$K_E = \hat{e}(T_A, T_C)^{u\hat{e}(Y_B,Y_C)^a} = \hat{e}(P,P)^{axucz\hat{e}(P,P)^{abc}}.$$

Namely, with the knowledge of A's secret key a, Adv can impersonate B to A. Moreover, Adv can surely perform the same steps above to cheat C simultaneously.

3 On the security of Shim's ID-based authenticated key agreement protocol

The protocol is an ID-based authenticated key agreement protocol in which a user's identity is regarded as his public key. The details of the protocol is described as follows:

3.1 Setup

`System Setup`

The system setup is the same as in the previous protocol with an extra hash function. The hash function $H : \{0,1\}^* \rightarrow G_1$ used in the protocol is a mapping of user's ID to an element in G_1.

`Key Setup`

The key generation center computes his public key $P_{pub} = sP$, where $s \in_R Z_q^*$ is the center's secret key. The center publishes the system parameters $params = \{G_1, G_2, e, q, P, P_{pub}, H\}$. Each user i sends his $ID_i \in \{0,1\}^*$ to the center. The center computes $Q_i = H_2(ID_i)$ and returns $S_i = sQ_i$ to user i via a secure channel. User i keeps S_i as his private key.

3.2 Shim's ID-based authenticated key agreement protocol

Two parties A and B run the protocol as follows:

Step 1. A computes $T_a = aP$, where a is a random number, and sends it to B.

Step 2. B computes $T_b = bP$, where b is a random number, and sends it to A.

Step 3. A computes $Q_B = H(ID_B)$ and the shared secret

$$\begin{aligned} K_{AB} &= e(aP_{pub} + S_A, T_b + Q_B) \\ &= e(P,P)^{abs} e(Q_A, P)^{bs} e(P, Q_B)^{as} e(Q_A, Q_B)^s \end{aligned}$$

Step 4. B computes $Q_A = H(ID_A)$ and the shared secret

$$\begin{aligned} K_{BA} &= e(T_a + Q_A, bP_{pub} + S_B) \\ &= e(P,P)^{abs} e(Q_A, P)^{bs} e(P, Q_B)^{as} e(Q_A, Q_B)^s \end{aligned}$$

Step 5. The session key is $K = kdf(K_{AB}||A||B) = kdf(K_{BA}||A||B)$, where $kdf()$ is a public key derivation function.

We briefly depict the scenario of Shim's protocol in figure 1.

$$\begin{array}{ccc} A & & B \\ T_a = aP & & \\ & \xrightarrow{T_a} & \\ & & T_b = bP \\ & \xleftarrow{T_b} & \\ Q_B = H(ID_B) & & Q_A = H(ID_A) \\ K_{AB} = e(aP_{pub} + S_A, T_b + Q_B) & & K_{BA} = e(T_a + Q_A, bP_{pub} + S_B) \end{array}$$

Figure 1: ID-based authenticated key agreement protocol

3.3 Man-in-the-middle attack on Shim's ID-based authenticated key agreement protocol

In this subsection, we demonstrate that an adversary Adv can perform the following steps, referred to as man-in-the-middle attack, to obtain the session keys computed by A and B, respectively.

Step 1. Adv intercepts T_a from A. He computes $Q_A = H(ID_A)$ and sends $T'_a = a'P - Q_A$ to B, where a' is selected by E.

Step 2. Adv intercepts T_b from B. He computes $Q_B = H(ID_B)$ and sends $T'_b = b'P - Q_B$ to A, where b' is selected by E.

It is clear that two shared secrets computed by A and B are

$$\begin{aligned} K_{AB} &= e(aP_{pub} + S_A, T'_b + Q_B) \\ &= e(aP_{pub} + S_A, b'P) \\ &= e(P, P)^{asb'} e(Q_A, P)^{sb'} \end{aligned}$$

and

$$\begin{aligned} K_{BA} &= e(T'_a + Q_A, bP_{pub} + S_B) \\ &= e(a'P, bP_{pub} + S_B) \\ &= e(P, P)^{a'sb} e(P, Q_B)^{a's}. \end{aligned}$$

After the masquerade, the adversary Adv can also compute the two shared secrets computed by A and B

$$\begin{aligned} K'_{AB} &= e(T_a, b'P_{pub}) e(Q_A, b'P_{pub}) \\ &= e(P, P)^{asb'} e(Q_A, P)^{sb'} \\ &= K_{AB} \end{aligned}$$

$$\begin{aligned} K'_{BA} &= e(T_b, a'P_{pub}) e(a'P_{pub}, Q_B) \\ &= e(P, P)^{a'sb} e(P, Q_B)^{a's} \\ &= K_{BA} \end{aligned}$$

The scenario of the man-in-the-middle attack is given in figure 2.

4 Conclusions and Remarks

In this paper, we have shown that both Shim's protocols from Weil pairing are insecure against the key-compromise impersonation attack and the man-in-the-middle attack respectively. Moreover, the fact that Shim's ID-based authenticated key agreement protocol is insecure against the man-in-the-middle attack implies that the protocol does not provide key-compromise impersonation resilience either. Because the man-in-the-middle attack can be regarded as two concurrent impersonation attacks to A and B without key compromising.

$$
\begin{array}{ccccc}
A & & E & & B \\
T_a = aP & & & & \\
 & \xrightarrow{T_a} & & & \\
 & & T'_a = a'P - Q_A & & \\
 & & & \xrightarrow{T'_a} & \\
 & & & & T_a = aP \\
 & & & \xleftarrow{T_b} & \\
 & & T'_b = b'P - Q_B & & \\
 & \xleftarrow{T'_b} & & & \\
K_{AB} = e(aP_{pub} + S_A, T'_b + Q_B) & & & & K_{BA} = e(T'_a + Q_A, bP_{pub} + S_B) \\
= e(P,P)^{asb'} e(Q_A, P)^{sb'} & & & & = e(P,P)^{a'sb} e(P, Q_B)^{a's}
\end{array}
$$

Figure 2: Man-in-the-middle attack on ID-based authenticated key agreement protocol

References

[1] P.S.L.M. Barreto, H.Y. Kim, B. Lynn, and M. Scott, "Efficient algorithms for Pairing-based cryptosystems", Proc. Crypto '02, Santa Barbara, CA, USA, pp. 354-369, August 2002.

[2] A. Joux, "An one round protocol for tripartite Diffie-Hellman", Proc. ANTS 4, LNCS 1838, pp. 385-394, 2000.

[3] D. Boneh, and M. Franklin, "Identity-based encryption from the Weil pairing", Advances in cryptology, Crypto '01, Santa Barbara, CA, USA, pp. 213-229, August 2001.

[4] N. P. Smart, "An ID-based authenticated key agreement protocol based on the Weil pairing", Electron. Lett., 38, (14), pp. 630-632, 2002.

[5] K. Shim, "Efficient one round tripartite authenticated key agreement protocol from Weil pairing", Electronics Letters, Vol. 39, No. 2, pp. 208-209, 2003.

[6] K. Shim, "Efficient ID-based authenticated key agreement protocol based on Weil pairing", Electron. Lett, 39, (8), pp. 653-654, 2003.

[7] S. B. Wilson, and A. Menezes, "Authenticated Diffie-Hellman key agreement protocols", Proceedings of the 5th Annual Workshop on Selected Areas in Cryptography (SAC '98), Lecture Notes in Computer Science, pp. 339-361, 1999.

[8] A. Menezes, M. Qu, and S. A. Vanstone, "Some key agreement protocols providing implicit authentication", Workshop on Selected Areas in Cryptography (SAC '95), pp. 22-32, 1995.