Cryptanalysis of ID-based Tripartite Authenticated Key Agreement Protocols

Kyungah Shim

KISA (Korea Information Security Agency),
78, Garak-Dong, Songpa-Gu, Seoul 138-803, Korea
kashim@kisa.or.kr

Abstract. In this paper, we show that the Nalla-Reddy's one round ID-based tripartite authenticated key agreement protocols are still insecure against the man-in-the-middle attacks. We also break the Nalla's ID-based tripartite authenticated key agreement protocol with signatures.

Key words : Tripartite key agreement protocol, man-in-the-middle attack, implicit key authentication, selective forgery.

1 Introduction

Joux [2] proposed an one round tripartite Diffie-Hellman key agreement protocol based on the Weil paring. Like the basic Diffie-Hellman key agreement protocol, it also suffers from the man-in-the-middle attacks because it does not attempt to authenticate the communicating entities. Al-Riyami and Paterson [5] proposed one round tripartite authenticated key agreement protocols which are designed to avoid the man-in-the-middle attacks by incorporating certified public keys. Nalla and Reddy [4] proposed three one-round tripartite ID-based key agreement protocols, ID-AK-1, ID-AK-2 and ID-AK-3, fusing the ideas of both ID-based approach and the tripartite key agreement protocol of Joux. In this paper, we show that the Nalla-Reddy's ID-based key agreement protocol are still insecure against the man-in-the-middle attacks. Recently, two ID-based tripartite authenticated key agreement protocols with signatures were proposed [4, 6]. We break the Nalla's ID-based tripartite authenticated key agreement protocol with signatures. We also present a selective forgery on the signature used in the Nalla's protocol.

2 Tripartite ID-based key agreement protocols

• **Setup** : Choose a large prime p such that $p = 2 \pmod 3$ and $p = 6q - 1$ for some prime q. Let E be a supersingular curve defined by $y^2 = x^3 + 1$ over $\mathbb{F}_p$. Let H_1 and H be a collision resistant hash function $H_1,\ H : \{0,1\}^* \to \mathbb{F}_p$. Let μ_q be the subgroup of $\mathbb{F}^*_{p^2}$ contains all elements of order q. The modified Weil pairing is defined by

$$\hat{e} : G_q \times G_q \to \mu_q, \quad \hat{e}(P, Q) = e(P, \phi(Q))$$

where $\phi(x,y) = (\zeta x, y)$, $1 \neq \zeta \in \mathbb{F}_{p^2}^*$ is a solution of $x^3 - 1 = 0 \pmod{p}$ and G_q is a group of points with order q. Let P be a generator of G_q. The key generation center (KGC) chooses a random $s \in \mathbb{Z}_q^*$ and set $P_{KGC} = s \cdot P$. The KGC publishes the system parameters $< p, q, E, P, P_{KGC}, \hat{e}, H_1, H >$ and keep s as a secret master key, which is known only by itself.

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

2.1 Nalla-Reddy's ID-based key agreement protocol, ID-AK1

Now, we describe Nalla-Reddy's ID-based key agreement protocol, ID-AK1. A, B and C respectively choose random numbers x, y and z and compute $R_A = x \cdot P$, $R_B = y \cdot P$ and $R_C = z \cdot P$ and broadcast these values. Once the communication is over, A, B and C computes K_A, K_B and K_C as follows, respectively.

$$\begin{aligned} K_A &= \hat{e}(R_B, R_C)^x \cdot \hat{e}(Q_A, P_{KGC}) \cdot \hat{e}(Q_B, P_{KGC}) \cdot \hat{e}(S_A, P), \\ K_B &= \hat{e}(R_A, R_C)^y \cdot \hat{e}(Q_A, P_{KGC}) \cdot \hat{e}(Q_C, P_{KGC}) \cdot \hat{e}(S_B, P), \\ K_C &= \hat{e}(R_A, R_B)^z \cdot \hat{e}(Q_A, P_{KGC}) \cdot \hat{e}(Q_B, P_{KGC}) \cdot \hat{e}(S_C, P). \end{aligned}$$

By bilinearity of the Weil pairing, all entities share the session key $K = \hat{e}(P,P)^{xyz} \cdot \hat{e}(Q_A + Q_B + Q_C, P)^s$.

2.2 Nalla's ID-based key agreement protocol with signatures

We describe Nalla's ID-based key agreement protocol with signatures. The identities of A, B and C are ID_A, ID_B and ID_C, respectively. Their public keys and private keys are as follows;

$$\begin{aligned} &A'\text{s public key} : Q_A = H_1(ID_A), \quad \text{private key} : S_A = s \cdot Q_A \\ &B'\text{s public key} : Q_B = H_1(ID_B), \quad \text{private key} : S_B = s \cdot Q_B \\ &C'\text{s public key} : Q_C = H_1(ID_C), \quad \text{private key} : S_C = s \cdot Q_C. \end{aligned}$$

A, B and C respectively choose random numbers a, b and c and compute $U_A = a \cdot P$, $U_B = b \cdot P$ and $U_C = c \cdot P$. A, B and C generate their signatures $V_A = a^{-1}(H(U_A) \cdot S_A)$, $V_B = b^{-1}(H(U_B) \cdot S_B)$ and $V_C = c^{-1}(H(U_C) \cdot S_C)$, respectively and broadcast these values.

$$\begin{aligned} &(1) \quad A : U_A = a \cdot P, \quad V_A = a^{-1}(H(U_A) \cdot S_A) \\ &(2) \quad B : U_B = b \cdot P, \quad V_B = b^{-1}(H(U_B) \cdot S_B) \\ &(3) \quad C : U_C = c \cdot P, \quad V_C = c^{-1}(H(U_C) \cdot S_C) \end{aligned}$$

A verifies

$$\hat{e}(U_B, V_B)\hat{e}(U_C, V_C) = \hat{e}(P_{KGC}, H(U_B)Q_B + H(U_C)Q_C).$$

If the equation holds, then A computes $k_A = \hat{e}(U_B, U_C)^a = \hat{e}(P, P)^{abc}$.

B verifies

$$\hat{e}(U_A, V_A)\hat{e}(U_C, V_C) = \hat{e}(P_{KGC}, H(U_A)Q_A + H(U_C)Q_C).$$

If the equation holds, then B computes $k_B = \hat{e}(U_A, U_C)^b = \hat{e}(P, P)^{abc}$.

C verifies

$$\hat{e}(U_A, V_A)\hat{e}(U_B, V_B) = \hat{e}(P_{KGC}, H(U_A)Q_A + H(U_B)Q_B).$$

If the equation holds, then C computes $k_C = \hat{e}(U_A, U_B)^c = \hat{e}(P, P)^{abc}$.

3 Cryptanalysis of tripartite ID-based key agreement protocols

3.1 Man-in-the-middle attacks on the ID-AK-1

An adversary E creates ephemeral private keys x', y' and z'. And E replaces R_A, R_B and R_C with $R'_A = x' \cdot P$, $R'_B = y' \cdot P$ and $R'_C = z' \cdot P$, respectively. Then A, B and C form session keys K_A, K_B, and K_C as follows, respectively.

$$\begin{aligned}
K_A &= \hat{e}(R'_B, R'_C)^x \cdot \hat{e}(Q_A, P_{KGC}) \cdot \hat{e}(Q_B, P_{KGC}) \cdot \hat{e}(S_A, P), \\
&= \hat{e}(P, P)^{xy'z'} \cdot \hat{e}(Q_A + Q_B + Q_C,\ P_{KGC}) \\
K_B &= \hat{e}(R'_A, R'_C)^y \cdot \hat{e}(Q_A, P_{KGC}) \cdot \hat{e}(Q_C, P_{KGC}) \cdot \hat{e}(S_B, P), \\
&= \hat{e}(P, P)^{x'yz'} \cdot \hat{e}(Q_A + Q_B + Q_C,\ P_{KGC}) \\
K_C &= \hat{e}(R'_A, R'_B)^z \cdot \hat{e}(Q_A, P_{KGC}) \cdot \hat{e}(Q_B, P_{KGC}) \cdot \hat{e}(S_C, P) \\
&= \hat{e}(P, P)^{x'y'z} \cdot \hat{e}(Q_A + Q_B + Q_C,\ P_{KGC}).
\end{aligned}$$

Then E who knows the values x', y' and z' is also able to compute these session keys from known values as follows ;

$$\begin{aligned}
K_A &= \hat{e}(R_A, P)^{y'z'} \cdot \hat{e}(Q_A + Q_B + Q_C,\ P_{KGC}), \\
K_B &= \hat{e}(R_B, P)^{x'z'} \cdot \hat{e}(Q_A + Q_B + Q_C,\ P_{KGC}), \\
K_C &= \hat{e}(R_C, P)^{x'y'} \cdot \hat{e}(Q_A + Q_B + Q_C,\ P_{KGC}).
\end{aligned}$$

When A subsequently sends a message to B and C encrypted under key K_A, E deciphers it, re-enciphers under K_B and K_C, and forwards them to B and C, respectively. Similarly, E deciphers messages encrypted by B or C under K_B or K_C, and re-enciphers them under K_A. Then A, B and C believe they communicate securely, while E reads all traffics.

3.2 Impersonation attacks on the Nalla's protocol with signatures

An adversary E randomly chooses $a \in \mathbb{Z}_q^*$ and computes

$$U_A = -a \cdot Q_A$$

$$V_A = a^{-1}(H(U_A) \cdot P_{KGC}).$$

Then E broadcasts these values masquerading A. We denote E_A the adversary E masquerading A.

$$\begin{array}{lll} (1) & E_A: & U_A = -a \cdot Q_A, \quad V_A = a^{-1}(H(U_A) \cdot P_{KGC}) \\ (2) & B: & U_B = b \cdot P, \quad V_B = b^{-1}(H(U_B) \cdot S_B) \\ (3) & C: & U_C = c \cdot P, \quad V_C = c^{-1}(H(U_C) \cdot S_C) \end{array}$$

On receiving the messages, B verifies

$$\hat{e}(U_A, V_A)\hat{e}(U_C, V_C) = \hat{e}(P_{KGC},\ H(U_A)Q_A + H(U_C)Q_C).$$

The equation holds, since

$$\begin{aligned} \hat{e}(U_A, V_A)\hat{e}(U_C, V_C) &= \hat{e}(-a \cdot Q_A,\ a^{-1}(H(U_A) \cdot P_{KGC}))\hat{e}(c \cdot P,\ c^{-1}(H(U_C) \cdot S_C)) \\ &= \hat{e}(Q_A,\ P)^{-H(U_A)s}\hat{e}(P, Q_C)^{H(U_C)s} \\ &= \hat{e}(P,\ Q_A)^{H(U_A)s}\hat{e}(P, Q_C)^{H(U_C)s} \\ &= \hat{e}(P_{KGC}, H(U_A)Q_A + H(U_C)Q_C). \end{aligned}$$

Then B computes $k_B = \hat{e}(U_A, U_C)^b = \hat{e}(P, P)^{abc}$.

C verifies $\hat{e}(U_A, V_A)\hat{e}(U_B, V_B) = \hat{e}(P_{KGC}, H(U_A)Q_A + H(U_B)Q_B)$. The verification also holds, and then C computes $k_C = \hat{e}(U_B, U_C)^a = \hat{e}(P, P)^{abc}$.

E can calculate the session key $k_A (= k_B = k_C)$ by computing $\hat{e}(U_B, U_C)^a = \hat{e}(P, P)^{abc}$ since a is generate by herself. Finally, E can succeed to impersonate A to B and C as well as the session key retrieval. Trivially, the protocol is insecure against the man-in-the-middle attacks. In fact, the weakness of the protocol against such active attacks is due to the fact that anyone who does not know each other's private key (S_{ID}) can generate a valid pair (U_A, V_A) by using the bilinearity and alternativity ($\hat{e}(P, Q) = \hat{e}(Q, P)^{-1}$) of the pairing. Thus, the protocol is totally broken.

3.3 Selective forgery of the signature used to the Nalla's protocol

The signature scheme used in the Nalla's protocol is as follows.

• **Signing** To sign a message $m = a \cdot P$, the signature of m is computed to be $V = a^{-1}(H(U_A) \cdot S_{ID})$.

• **Verification** On receiving a message m and signature V, the verifier accepts the signature if and only if the following equation holds

$$\hat{e}(m, V) = \hat{e}(P_{KGC}, H(m) \cdot Q_{ID}).$$

Suppose that an adversary E eavesdrops on a communication among A, B and C. For a known pair $(U_A = a \cdot P,\ V_A = a^{-1}(H(U_A) \cdot S_A))$, she can forgery A's signature for a class of messages which have the form $U'_A = a'U_A = a' \cdot aP$ for an arbitrary a' as follows;

$$V'_A = a'^{-1}H(U'_A)H(U_A)^{-1}V_A = a'^{-1}a^{-1}H(U'_A) \cdot S_A.$$

Then the verification holds,

$$\begin{aligned}\hat{e}(U'_A,\ V'_A) &= \hat{e}(a'aP,\ a'^{-1}a^{-1}H(U'_A) \cdot S_A) \\ &= \hat{e}(P,\ Q_A)^{H(U'_A)s} = \hat{e}(P_{KGC},\ H(U'_A) \cdot Q_A).\end{aligned}$$

Thus, anyone who has obtained a valid pair (U_A, V_A) can forgery for the messages of the form $a' \cdot U_A$ for an arbitrary a'.

3.4 Modified ID-based tripartite key agreement protocol with signatures

A, B and C respectively choose random numbers a, b and c and compute (U_A, V_A) (U_B, V_B) and (U_C, V_C) and broadcast these values.

$$\begin{array}{lll}(1) & A: & U_A = a \cdot P,\quad V_A = H(U_A) \cdot S_A + a \cdot P_{KGC} \\ (2) & B: & U_B = b \cdot P,\quad V_B = H(U_B) \cdot S_B + b \cdot P_{KGC} \\ (3) & C: & U_C = c \cdot P,\quad V_C = H(U_C) \cdot S_C + c \cdot P_{KGC}\end{array}$$

A verifies

$$\hat{e}(V_B + V_C, P) = \hat{e}(P_{KGC},\ H(U_B)Q_B + H(U_C)Q_C + U_B + U_C).$$

If the equation holds, then A computes $k_A = \hat{e}(U_B, U_C)^a = \hat{e}(P, P)^{abc}$.

B verifies

$$e(V_A + V_C, P) = \hat{e}(P_{KGC},\ H(U_A)Q_A + H(U_C)Q_C + U_A + U_C).$$

If the equation holds, then B computes $k_B = \hat{e}(U_A, U_C)^b = \hat{e}(P, P)^{abc}$.

C verifies

$$\hat{e}(V_A + V_B, P) = \hat{e}(P_{KGC},\ H(U_A)Q_A + H(U_B)Q_B + U_A + U_B).$$

If the equation holds, then C computes $k_C = \hat{e}(U_A, U_B)^c = \hat{e}(P, P)^{abc}$.

4 Conclusion

The weakness of the ID-AK-1 against the man-in-the-middle attack is due to the fact that the protocol still does not provide the implicit key authentication attribute. In fact, to provide the implicit key authentication attribute, each entity should be assured that no other entity aside from specifically identified entities can possibly learn the value of a particular secret key. However, in ID-AK-1, anyone who knows P_{KGC} can compute $\hat{e}(Q_A+Q_B+Q_C, P_{KGC})$ even though the value should be calculated by only ones who knows the corresponding private keys S_A, S_B or S_C. Thus, the protocol cannot overcome the flaw of lack of authentication in the Joux's protocol. Also, we can easily see that ID-AK-2 and ID-AK-3 are totally broken by only eavesdroppers (in fact, it was showed by Chen in [1]). So, we need not analyze the security of the protocols against several active attacks including the man-in-the-middle attacks.

We have broken the Nalla's ID-based tripartite authenticated key agreement protocol with signatures and proposed a simple modified version.

References

1. Z. Chen, Security anlysis on Nalla-Reddy's ID-based tripartite key agreement protocols, available at http://eprint.iacr.org/2003/103.
2. A. Joux, A one round protocol for tripartite Diffie-Hellman, Proce. of ANTS 4, LNCS 1838, 2000, pp. 385-394.
3. D. Nalla, ID-based tripartite key agreement with signatures, available at http://eprint.iacr.org/2003/144.
4. D. Nalla and K. C. Reddy, ID-based tripartite authenticated key agreement protocols from pairings, available at http://eprint.iacr.org/2003/004.
5. S. S. Al-Riyami and K. G. Paterson, Authenticated three party key agreement protocols from pairing, available at http://eprint.iacr.org/2002/035.
6. F. Zhang, S. Liu and K. Kwangjo, 'ID-Based One Round Authenticated Tripartite Key Agreement Protocol with Pairings', 2003 IEEE International Symposium on Information Theory, Yokohama, JAPAN, 2003 or Cryptology ePrint Archive, Report 2002/122.