Utilizing postponed ephemeral and pseudo-static keys in tripartite and identity-based key agreement protocols

Atsushi Fujioka, Koutarou Suzuki, and Berkant Ustaoglu

NTT Information Sharing Platform Laboratories
3-9-11 Midori-cho Musashino-shi Tokyo 180-8585, Japan
{fujioka.astushi, suzuki.koutarou, ustaoglu.berkant}@lab.ntt.co.jp

Abstract. We propose an new one-round implicitly authenticated three-party protocol that extends Joux's protocol as well as a two-party identity-based protocol. Our protocols have a single communication round that consists of ephemeral (one-time) public keys along with certificates in the tripartite protocol, and identities in the identity-based setting. As such our protocols are communication efficient and furthermore do not require enhanced message format.

Keywords. Postponed ephemeral keys, pseudo-static keys, tripartite key agreement, identity based key agreement.

1 Introduction

Joux [3,4] proposed one-round three-party key agreement protocol that extended the well known unauthenticated Diffie-Hellman protocol [2]. Al-Riyami and Patterson [1] attempted to adapt well-known two-party protocols using Joux's technique to provide authentication. However, some of the utilized two-party protocols have known vulnerabilities which were also present in the resulting three-party protocols; and others relied on protocols that do not have formal security arguments even for the two-pass variants. We present a new protocol that uses postponed ephemeral key derivation and pseudo-static keys [7].

Sakai et. al. [5] first considered a two-party pairing-based protocol. The protocol is analogous to the two-party static Diffie-Hellman protocol and as such does not have many desirable security goals. We propose a new identity-based protocol that has most desirable security attributes expected from two-party key agreement protocols.

Notation. In the remainder G denotes a group of prime order q generated by P; the non-identity elements are denoted by G^*. The protocol takes place between three-parties: Alice, Bob and Charlie with static key pairs $(a, A = aP)$, $(b, B = bP)$, and $(c, C = cP)$, respectively; $a, b, c \in [1, q]$. The ephemeral (one-time) key pairs are $(x, X = xP)$, $(y, Y = yP)$, and $(z, Z = zP)$, respectively; $x, y, z \in [1, q]$. Let $\mathsf{e} : G \to \tilde{G}$ be a non-degenerate pairing from the group G into a group $\tilde{G}$, see e.g., [6] for details. Lastly, H, H' and H'' denote hash functions viewed as random oracles.

Security assumptions. For security of the protocols we require the bilinear Diffie-Hellman assumption which roughly states that given $(U, V, W) \in G^3$ it is infeasible to compute $\mathsf{e}(P, P)^{uvw}$ in polynomial time where $U = uP$, $V = vP$, and $W = wP$.

2 Tripartite protocol

We describe our protocol proposal and provide intuitive arguments for its security.

2.1 Description

We describe the actions of the first party Alice; her peers Bob and Charlie perform similar steps. Alice proceeds as follows:

Initialization. Perform the steps:

1. Select an ephemeral private key $x \in_R [1, q]$ and compute $X = xP$.
2. Create a session state contains (x, X).

Communication. Upon receiving $(\mathit{start}, \mathit{Alice}, \mathit{Bob}, \mathit{Charlie})$ Alice performs:

1. Activate a new session instance $(\mathit{Alice}, \mathit{Bob}, \mathit{Charlie}, x, X)$
2. Broadcasts $(1|\mathit{Alice}, \mathit{Bob}, \mathit{Charlie}, X)$.

Derivations. Upon receiving $(1|\mathit{Alice}, \mathit{Bob}, \mathit{Charlie}, Y)$ and $(1|\mathit{Alice}, \mathit{Bob}, \mathit{Charlie}, Z)$, Alice does the following:

1. Verify that $Y, Z \in G^*$.
2. Compute $F_A = H'(X)$, $F_B = H'(Y)$ and $F_C = H'(Z)$.
3. Compute

$$\begin{aligned}
\sigma_0 &= (\mathsf{e}(Y + B, Z + C))^{x+F_A a} &&= (\mathsf{e}(P, P))^{(x+F_A a)(y+b)(z+c)} \\
\sigma_1 &= (\mathsf{e}(Y + F_B B, Z + C))^{x+a} &&= (\mathsf{e}(P, P))^{(x+a)(y+F_B b)(z+c)} \\
\sigma_2 &= (\mathsf{e}(Y + B, Z + F_C C))^{x+a} &&= (\mathsf{e}(P, P))^{(x+a)(y+b)(z+F_C c)} \\
\sigma_3 &= (\mathsf{e}(Y + F_B B, Z + F_C C))^{x+F_A a} &&= (\mathsf{e}(P, P))^{(x+F_A a)(y+F_B b)(z+F_C c)}.
\end{aligned}$$

4. Compute

$$\kappa = H(\sigma_0, \sigma_1, \sigma_2, \sigma_3, \mathit{Alice}, X, \mathit{Bob}, Y, \mathit{Chalie}, Z).$$

Completion. To complete the session Alice does

1. Destroy session state.
2. Complete the session by accepting session key κ.

Optionally, the parties may perform key confirmation before accepting the session key.

2.2 Security arguments

In the random oracle model the idea of the security argument is use an adversary that distinguishes the session key from a randomly chosen key to solver a BDH instance. The adversary is intuitively allowed to obtain any private information that does not contain both ephemeral and static private key of a party. In other words the adversary is not given at least one of the private keys for every party. One of the group elements in the BDH instance is assigned as the public key for which the adversary is not given the corresponding private key. In the random oracle model the adversary has to query the oracle with the shared secrets to distinguish the session key from a randomly chosen session key. Since there are four shared secrets whose exponents are linearly independent a simulator can extract the BDH solution from the shared secrets.

3 Identity-based protocol

In this section we present the identity-based protocol. We assume there is a key generation center that publishes a master static public key S; the corresponding master secret is s such that $S = sP$. The public key corresponding to the identity *Alice* is $A = H''(\mathit{Alice})$, similarly, Bob's public key is $B = H''(\mathit{Bob})$. The static private keys of Alice and Bob are $S_a = sA$ and $S_b = sB$, respectively.

3.1 Description

We describe the actions of the first party Alice; her peer Bob performs similar steps. Alice proceeds as follows:

Initialization. Perform the steps:

1. Select an ephemeral private key $x \in_R [1, q]$ and compute $X = xP$.
2. Create a session state contains (x, X).

Communication. Upon receiving $(\mathit{start}, \mathit{Alice}, \mathit{Bob})$ Alice performs:

1. Send X to Bob.

Derivations. Upon receiving Y from Bob Alice does the following:

1. Verify that $Y \in G^*$.
2. Compute $F_A = H'(X)$ and $F_B = H'(Y)$.
3. Compute

$$\begin{aligned} \sigma_0 &= \mathsf{e}(xS + S_a, Y + F_B B) &&= (\mathsf{e}(P, P))^{s(x+a)(y+F_B b)} \\ \sigma_1 &= \mathsf{e}(xS + F_a S_a, Y + B) &&= (\mathsf{e}(P, P))^{s(x+F_A a)(y+b)} \\ \sigma_2 &= xY &&= xyP. \end{aligned}$$

4. Compute

$$\kappa = H(\sigma_0, \sigma_1, \sigma_2, \mathit{Alice}, X, \mathit{Bob}, Y).$$

Completion. To complete the session Alice does

1. Destroy session state.
2. Complete the session by accepting session key κ.

Optionally, the parties may perform key confirmation before accepting the session key.

3.2 Security arguments

As before in the random oracle model a simulator will extract a solution for the BDH challenge from adversary's H queries. As before for the test session for each peer the adversary does not possess either the ephemeral of the static private key. If the adversary has all static keys then by setting $X = V$ and $Y = U$ the simulator can solve the BDH challenge by computing $\mathsf{e}(\sigma_2, W) = \mathsf{e}(P, P)^{uvw}$. It remains to consider the case where the adversary either sets or queries for an ephemeral private key, without loss of generality we can assume the adversary sets or queries y. In that case the simulator sets $S = W$ and $B = V$. Note that the adversary cannot query for s or sB since otherwise the adversary can trivially compute the session key. The value U is set to equal either X or A depending on which of the two values the adversary does not query for. To extract the BDH solution one uses the fact that σ_0 and σ_1 have different exponents from which the multiple of uvw can be extracted even without the knowledge of y.

4 Conclusion

We presented a tripartite PKI-based and two-party ID-based key establishment schemes. The protocols utilize ideas used to obtain efficient two-party key agreement techniques. They are both communication and computation efficient, and provide most desirable security attributes.

References

1. S. S. Al-Riyami and K. G. Paterson. Tripartite authenticated key agreement protocols from pairings. In K. G. Paterson, editor, *9th IMA International Conference*, volume 2898 of *LNCS*, pages 332–359, Cirencester, UK, 2003. Springer Verlag.
2. W. Diffie and M. E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, IT-22(6):644–654, 1976.
3. A. Joux. A one round protocol for tripartite Diffie–Hellman. In W. Bosma, editor, *Algorithmic Number Theory 4th International Symposium, ANTS-IV, Proceedings*, volume 1838 of *LNCS*, pages 385–393. Springer, 2000.
4. A. Joux. A one round protocol for tripartite Diffie–Hellman. *Journal of Cryptology*, 17(4):263–276, 2004.
5. R. Sakai, K. Ohgishi, and M. Kasahara. Cryptosystems based on pairings. In *The 2000 Symposium on Cryptography and Information Security*, 2000.
6. J. H. Silverman. *The Arithmetic of Elliptic Curves*, volume 106 of *Graduate Text in Mathematics*. Springer-Verlag New York, Inc, New York, NY 10010, USA, 1986.
7. B. Ustaoglu. Comparing *SessionStateReveal* and *EphemeralKeyReveal* for Diffie-Hellman protocols (extended version). Cryptology ePrint Archive, Report 2009/353, 2009.