Computers and Electrical Engineering 37 (2011) 187–190

Contents lists available at ScienceDirect

Computers and Electrical Engineering

journal homepage: www.elsevier.com/locate/compeleceng

Analysis and improvement of an authenticated multiple key exchange protocol ☆

Qingfeng Cheng [a,b,*], Chuangui Ma [a]

[a] Zhengzhou Information Science and Technology Institute, Zhengzhou 450002, PR China
[b] Luoyang University of Foreign Languages, Luoyang 471003, PR China

ARTICLE INFO

Article history:
Available online 5 March 2011

ABSTRACT

In 2010, Vo et al. (2010) [7] proposed an enhancement of authenticated multiple key exchange protocol based on Lee et al.'s protocol. In this paper, we will show that Vo et al.'s multiple key exchange protocol cannot resist reflection attack. It means that their protocol fails to provide mutual authentication. Furthermore, we propose an improvement of Vo et al.'s protocol. Our proposed protocol with reflection attack resilience can really provide mutual authentication.

1. Introduction

Authenticated key exchange (AKE) plays an important role in secure communications. An AKE protocol allows two or more parties to agree upon a secret common session key over a public network, which will be used in the future communications. But the design of secure AKE protocols has always been a notorious hard problem.

In 2000, Joux [1] proposed the first usable pairing-based protocol for tripartite key exchange. But Joux's protocol cannot resist man-in-the-middle attacks. In 2001, Harn and Lin [2] proposed an efficient authentication key exchange protocol that enabled two parties to share multiple secret key in one round of message exchange. In 2003, Shim [3] pointed out that Harn and Lin's protocol was vulnerable to unknown key share attack. However, Zhou et al. [4] showed that Shim's attacks [3] on the Harn and Lin's authenticated multiple-key agreement protocol was invalid. Furthermore, they gave a new attack on the Harn and Lin's protocol and proposed an improved protocol. Unfortunately, Zhong [5] showed that Zhou et al.'s improved protocol was still insecure.

In 2008, Lee et al. [6] proposed two authenticated multiple key exchange protocols. Recently, Vo et al. [7] presented an impersonation attack on Lee et al.'s bilinear pairing-based AKE protocol and showed that Lee et al.'s protocol failed to provide authenticity. Furthermore, Vo et al. proposed a simple modification to Lee et al.'s protocol, called VLYK protocol. In this paper, we will show that the VLYK protocol also fails to provide authenticity and cannot resist reflection attack. Moreover, we propose an improvement of the VLYK protocol with reflection attack resilience. Our improved protocol can really provide mutual authentication and generate four session keys at a time. So it will be well suited for wireless mobile communications [8], where parties only have the low-power computing capability.

The rest of this paper is organized as follows. In Section 2, we introduce bilinear map and several Diffie–Hellman problems. In Section 3, we briefly review the VLYK protocol. In Section 4, we describe reflection attacks on the VLYK protocol. In Section 5, we propose an improvement of the VLYK protocol. Finally, the conclusions will be given in Section 6.

☆ Reviews processed and proposed for publication by Associate Editor Pro. N. Sklavos.
* Corresponding author at: Zhengzhou Information Science and Technology Institute, P.O. Box 1001-7410, Zhengzhou 450002, PR China.
E-mail addresses: qingfengc2008@sina.com (Q. Cheng), chuanguima@yahoo.com (C. Ma).

0045-7906/$ - see front matter © 2011 Elsevier Ltd. All rights reserved.
doi:10.1016/j.compeleceng.2011.02.005

2. Preliminaries

In this section, we introduce bilinear map and several Diffie–Hellman problems. Let G_1 be an additive group of order q, and G_2 be a multiplicative group of order q. Let $Q,W \in G_1$ and $e : G_1 \times G_1 \to G_2$ be a bilinear pairing that has the following properties:

- **Bilinearity**: For any Q, $W \in G_1$ and $(a, b \in Z_q^*$, we have $e(aQ, bW) = e(Q, W)^{ab}$.
- **Non-degeneracy**: There exists Q, $W \in G_1$ such that $e(Q, W) \neq 1$.
- **Computability**: For any Q, $W \in G_1$, there exists an efficient algorithm to compute $e(Q, W)$.

Next, we describe DL and BDH problems:

- **Discrete logarithm (DL) problem**: Given two elements Q, $W \in G_1$. Find the integer n whenever such an integer exists, such that $Q = nW$.
- **Bilinear Diffie–Hellman (BDH) problem**: Let P is a generator of G_1. Given (P, aP, bP, cP) with $(a, b, c \in Z_q^*$, computes $e(P, P)^{abc} \in G_2$.

We say that G_2 satisfies the DL and BDH assumptions if no feasible adversary can solve the DL and BDH problems with non-negligible probability.

3. Review of VLYK protocol

In this section, we briefly review the VLYK protocol proposed by Vo et al. in 2010. Let P be a generator of a cyclic additive group G_1 of the prime order q, and G_2 be a cyclic multiplicative group of the prime order $q.e : G_1 \times G_1 \to G_2$ is a bilinear pairing. Each party i has a static private key $X_i \in Z_q^*$ and a static public key $Y_i(=X_iP)$. For more details about the VLYK protocol, refer to [7].

In the following description we suppose that two communications parties, A and B wish to communicate with each other.

Step 1. Party A chooses $a_1, a_2 \in Z_q^*$ randomly and computes $T_{A1} = a_1P$ and $T_{A2} = a_2P$, Let K_{A1} and K_{A2} be the x-coordinate values of T_{A1} and T_{A2}. Then party A computes $S_A = (a_1K_{A1} + a_2K_{A2})T_{A1} + X_AY_B$. Finally, party A sends the message $(T_{A1}, T_{A2}, S_A, Cert(Y_A))$ to party B.

Step 2. Similarly, party B chooses $b_1, b_2 \in Z_q^*$ randomly and computes $T_{B1} = b_1P$ and $T_{B2} = b_2P$, Let K_{B1} and K_{B2} be the x-coordinate values of T_{B1} and T_{B2}. Then party B computes $S_B = (b_1K_{B1} + b_2K_{B2})T_{B1} + X_BY_A$. Finally, party B sends the message $(T_{B1}, T_{B2}, S_B, Cert(Y_B))$ to party A.

Step 3. Upon receiving the message $(T_{B1}, T_{B2}, S_B, Cert(Y_B))$, party A takes out the x-coordinate values K_{B1} and K_{B2} from T_{B1} and T_{B2}, checks whether $e(S_B, P) = e(K_{B1}T_{B1} + K_{B2}T_{B2}, T_{B1})e(Y_A, Y_B)$, if $e(S_B, P) = e(K_{B1}T_{B1} + K_{B2}T_{B2}, T_{B1})e(Y_A, Y_B)$, then computes the session keys K_1, K_2, K_3, K_4 as follows:

$$K_1 = e(a_1T_{B1}, X_AT_{B1} + a_1Y_B) = e(P,P)^{a_1b_1(b_1X_A + a_1X_B)}$$
$$K_2 = e(a_1T_{B2}, X_AT_{B2} + a_1Y_B) = e(P,P)^{a_1b_2(b_2X_A + a_1X_B)}$$
$$K_3 = e(a_2T_{B1}, X_AT_{B1} + a_2Y_B) = e(P,P)^{a_2b_1(b_1X_A + a_2X_B)}$$
$$K_4 = e(a_2T_{B2}, X_AT_{B2} + a_2Y_B) = e(P,P)^{a_2b_2(b_2X_A + a_2X_B)}$$

Otherwise party A aborts.

Step 4. Upon receiving the message $(T_{A1}, T_{A2}, S_A, Cert(Y_A))$, party B takes out the x-coordinate values K_{A1} and K_{A2} from T_{A1} and T_{A2}, checks whether $e(S_A, P) = e(K_{A1}T_{A1} + K_{A2}T_{A2}, T_{A1})e(Y_B, Y_A)$, if $e(S_A, P) = e(K_{A1}T_{A1} + K_{A2}T_{A2}, T_{A1})e(Y_A, Y_B)$, then computes the session keys K_1, K_2, K_3, K_4 as follows:7

$$K_1 = e(b_1T_{A1}, X_BT_{A1} + b_1Y_A) = e(P,P)^{a_1b_1(b_1X_A + a_1X_B)}$$
$$K_2 = e(b_2T_{A1}, X_BT_{A1} + b_2Y_A) = e(P,P)^{a_1b_2(b_2X_A + a_1X_B)}$$
$$K_3 = e(b_1T_{A2}, X_BT_{A2} + b_1Y_A) = e(P,P)^{a_2b_1(b_1X_A + a_2X_B)}$$
$$K_4 = e(b_2T_{A2}, X_BT_{A2} + b_2Y_A) = e(P,P)^{a_2b_2(b_2X_A + a_2X_B)}$$

Otherwise party B aborts.

4. Reflection attack on VLYK protocol

In this section, we will show that the VLYK protocol cannot resist reflection attack. It also means that the VLYK protocol fails to provide authenticity.

The adversary E can mount reflection attack on the VLYK protocol as follows:

Step 1. Party A chooses $a_1, a_2 \in Z_q^*$ randomly and computes $T_{A1} = a_1P$ and $T_{A2} = a_2P$, Let K_{A1} and K_{A2} be the x-coordinate values of T_{A1} and T_{A2}. Then party A computes $S_A = (a_1K_{A1} + a_2K_{A2})T_{A1} + X_AY_B$. Finally, party A sends the message (T_{A1}, T_{A2}, S_A, $Cert(Y_A)$) to party B.

Step 2. Upon intercepting the message (T_{A1}, T_{A2}, S_A, $Cert(Y_A)$), the adversary E lets $T_{B1} = T_{A1}$, $T_{B2} = T_{A2}$, $S_B = S_A$. Then E impersonates party B to send the message (T_{B1}, T_{B2}, S_B, $Cert(Y_B)$) to party A.

Step 3. Upon receiving the message (T_{B1}, T_{B2}, S_B, $Cert(Y_B)$), party A takes out the x-coordinate values $K_{B1}(=K_{A1})$ and $K_{B2}(=K_{A2})$ from $T_{B1}(=T_{A1})$ and $T_{B2}(=T_{A2})$. Then party A computes $e(S_B, P)$ as follows:

$$\begin{aligned} e(S_B,P) &= e(S_A,P) \\ &= e((a_1K_{A1}+a_2K_{A2})T_{A1}+X_AY_B,P) \\ &= e((a_1K_{A1}+a_2K_{A2})T_{A1},P)e(X_AY_B,P) \\ &= e((a_1K_{A1}+a_2K_{A2})P,a_1P)e(Y_B,Y_A) \\ &= e(a_1K_{A1}P+a_2K_{A2}P,a_1P)e(Y_A,Y_B) \\ &= e(K_{A1}T_{A1}+K_{A2}T_{A2},T_{A1})e(Y_A,Y_B) \\ &= e(K_{B1}T_{B1}+K_{B2}T_{B2},T_{B1})e(Y_A,Y_B) \end{aligned}$$

It means that $e(S_B, P)$ is equal to $e(K_{B1}T_{B1} + K_{B2}T_{B2}, T_{B1})e(Y_A, Y_B)$, so party A will compute the session keys K_1, K_2, K_3, K_4 as follows:

$$\begin{aligned} K_1 &= e(a_1T_{B1}, X_AT_{B1}+a_1Y_B) = e(P,P)^{a_1a_1(a_1X_A+a_1X_B)} \\ K_2 &= e(a_1T_{B2}, X_AT_{B2}+a_1Y_B) = e(P,P)^{a_1a_2(a_2X_A+a_1X_B)} \\ K_3 &= e(a_2T_{B1}, X_AT_{B1}+a_2Y_B) = e(P,P)^{a_2a_1(a_1X_A+a_2X_B)} \\ K_4 &= e(a_2T_{B2}, X_AT_{B2}+a_2Y_B) = e(P,P)^{a_2a_2(a_2X_A+a_2X_B)} \end{aligned}$$

So the adversary E has successfully cheated party A to believe that he has shared secret session keys with party B. However, party B does not involve in this session. It means that the VLYK protocol cannot provide authenticity.

5. Improvement of VLYK protocol

In this section, we propose an improvement of the VLYK protocol. Our protocol can resist reflection attack and own the VLYK protocol's security attributes.

In the following description we suppose that two communications parties, A and B wish to communicate with each other.

Step 1. Party A chooses $a_1, a_2 \in Z_q^*$ randomly and computes $T_{A1} = a_1P$ and $T_{A2} = a_2P$, Let K_{A1} and K_{A2} be the x-coordinate values of T_{A1} and T_{A2}. Then party A computes $S_{A1} = (a_1K_{A1} + a_2K_{A2})T_{A1} + X_AY_B$, $S_{A2} = a_1a_2Y_B$. Finally, party A sends the message (T_{A1}, T_{A2}, S_{A1}, S_{A2}, $Cert(Y_A)$) to party B.

Step 2. Similarly, party B chooses $b_1, b_2 \in Z_q^*$ randomly and computes $T_{B1} = b_1P$ and $T_{B2} = b_2P$, Let K_{B1} and K_{B2} be the x-coordinate values of T_{B1} and T_{B2}. Then party B computes $S_{B1} = (b_1K_{B1} + b_2K_{B2})T_{B1} + X_BY_A$, $S_{B2} = b_1b_2Y_A$. Finally, party B sends the message (T_{B1}, T_{B2}, S_{B1}, S_{B2}, $Cert(Y_B)$) to party A.

Step 3. Upon receiving the message (T_{B1}, T_{B2}, S_{B1}, S_{B2}, $Cert(Y_B)$), party A takes out the x-coordinate values K_{B1} and K_{B2} from T_{B1} and T_{B2}, checks whether

$$e(S_{B1},P) = e(K_{B1}T_{B1}+K_{B2}T_{B2},T_{B1})e(Y_A,Y_B),$$
$$e(S_{B2},P) = e(T_{B1},T_{B2})^{X_A},$$

if $e(S_{B1},P) = e(K_{B1}T_{B1}+K_{B2}T_{B2},T_{B1})e(Y_A,Y_B)$, $e(S_{B2},P) = e(T_{B1},T_{B2})^{X_A}$, then computes the session keys K_1, K_2, K_3, K_4 as follows:

$$\begin{aligned} K_1 &= e(a_1T_{B1}, X_AT_{B1}+a_1Y_B) = e(P,P)^{a_1b_1(b_1X_A+a_1X_B)} \\ K_2 &= e(a_1T_{B2}, X_AT_{B2}+a_1Y_B) = e(P,P)^{a_1b_2(b_2X_A+a_1X_B)} \\ K_3 &= e(a_2T_{B1}, X_AT_{B1}+a_2Y_B) = e(P,P)^{a_2b_1(b_1X_A+a_2X_B)} \\ K_4 &= e(a_2T_{B2}, X_AT_{B2}+a_2Y_B) = e(P,P)^{a_2b_2(b_2X_A+a_2X_B)} \end{aligned}$$

Otherwise party A aborts.

Step 4. Upon receiving the message (T_{A1}, T_{A2}, S_{A1}, S_{A2}, $Cert(Y_A)$), party B takes out the x-coordinate values K_{A1} and K_{A2} from T_{A1} and T_{A2}, checks whether

$$e(S_{A1}, P) = e(K_{A1}T_{A1} + K_{A2}T_{A2}, T_{A1})e(Y_B, Y_A),$$
$$e(S_{A2}, P) = e(T_{A1}, T_{A2})^{X_B},$$

if $e(S_{A1}, P) = e(K_{A1}T_{A1} + K_{A2}T_{A2}, T_{A1})e(Y_A, Y_B)$, $e(S_{A2}, P) = e(T_{A1}, T_{A2})^{X_B}$, then computes the session keys K_1, K_2, K_3, K_4 as follows:

$$K_1 = e(b_1T_{A1}, X_BT_{A1} + b_1Y_A) = e(P, P)^{a_1b_1(b_1X_A + a_1X_B)}$$
$$K_2 = e(b_2T_{A1}, X_BT_{A1} + b_2Y_A) = e(P, P)^{a_1b_2(b_2X_A + a_1X_B)}$$
$$K_3 = e(b_1T_{A2}, X_BT_{A2} + b_1Y_A) = e(P, P)^{a_2b_1(b_1X_A + a_2X_B)}$$
$$K_4 = e(b_2T_{A2}, X_BT_{A2} + b_2Y_A) = e(P, P)^{a_2b_2(b_2X_A + a_2X_B)}$$

Otherwise party B aborts.

Reflection attack resilience

Our improvement can resist reflection attack efficiently. If the adversary impersonates party B and lets $S_{B2} = S_{A2}$ mount reflection attack on our improvement, since $e(S_{B2}, P) = e(S_{A2}, P) = e(a_1a_2Y_B, P) = e(P, P)^{a_1a_2X_B} \neq e(P, P)^{a_1a_2X_A} = e(T_{A1}, T_{A2})^{X_A} = e(T_{B1}, T_{B2})^{X_A}$, the adversary E cannot pass the verification. Party A will abort the session. It means that the adversary E fails to mount reflection attack.

6. Conclusions

We have pointed out that the VLYK protocol is insecure against the reflection attack. To eliminate this security vulnerability, we propose an improved protocol, which successfully avoids the weakness existed in the original VLYK protocol.

Acknowledgment

This work was in part supported by the National High Technology Research and Development Program of China (No. 2009AA01Z417) and Key Scientific and Technological Project of Henan Province (No. 092101210502). The authors would like to thank the anonymous referees for their helpful comments.

References

[1] Joux A. A one round protocol for tripartite Diffie–Hellman. In: Proceedings of ANTS- IV: proceedings of the fouth international symposium on algorithmic number theory, LNCS, vol. 1838. Berlin: Springer; 2000. p. 385–94.
[2] Harn L, Lin H-Y. Authenticated key agreement without using one-way hash function. Electron Lett 2001;37(10):629–30.
[3] Shim K. Unknown key-share attack on authenticated multiple-key agreement protocol. Electron Lett 2003;39(1):38–9.
[4] Zhou H-S, Fan L, Li J-H. Remarks on unknown key-share attack on authenticated multiple-key agreement protocol. Electron Lett 2003;39(17):1248–9.
[5] Zhong S. An attack on the Zhou–Fan–Li authenticated multiple-key agreement protocol. Cryptologia 2007;31(4):324–5.
[6] Lee N-Y, Wu C-N, Wang C-C. Authenticated multiple key exchange protocols based on elliptic curves and bilinear pairings. Comput Electr Eng 2008;34(1):12–20.
[7] Vo D-L, Lee H, Yeun C-Y, Kim K. Enhancements of authenticated multiple key exchange protocol based on bilinear pairings. Comput Electr Eng 2010;36(1):155–9.
[8] Sklavos N, Zhang X. Wireless security and cryptography: specifications and implementations. CRC-Press, A Taylor and Francis Group, ISBN: 084938771X, 2007.

Qingfeng Cheng received his master degree in applied mathematical from National University of Defense Technology. He is currently a Ph.D. candidate in the Department of Information Research, Zhengzhou Information Science and Technology Institute, Zhengzhou, China. His research field is information security.

Chuangui Ma received his Ph.D. degree in mathematics in 1998 from Zhejiang University. He is currently a professor in the Department of Information Research, Zhengzhou Information Science and Technology Institute, Zhengzhou, China. His research field is information security.