Cryptanalysis of an Authenticated Key Agreement Protocol for Wireless Mobile Communications

Debiao He*

School of Mathematics and Statistics, Wuhan University, Wuhan, People's Republic of China

Email: hedebiao@163.com

Abstract*:* With the rapid progress of wireless mobile communication, the authenticated key agreement (AKA) protocol has attracted an increasing amount of attention. However, due to the limitations of bandwidth and storage of the mobile devices, most of the existing AKA protocols are not suitable for wireless mobile communication. Recently, Lo et al. presented an efficient authenticated key agreement protocol based on elliptic curve cryptography and included their protocol in 3GPP2 specifications. However, in this letter, we point out that Lo et al.'s protocol is vulnerable to an off-line password guessing attack and the Dennig-Sacco attack.

Key words*:Authenticated key agreement; Off-line password guessing attack; Wireless mobile communication; 3GPP2*

1. Introduction

In 2005, Sui et al. proposed an improved authenticated key agreement (AKA) protocol [1] for wireless mobile communications. Their scheme provided perfect forward secrecy but was vulnerable to an off-line password attack problem [2]. To enhance the security, Lu et al. proposed an enhanced AKA protocol for wireless mobile communication in 2007 [2]. Later, Chang et al. [3] pointed out that the Lu et al.'s scheme cannot resist against the parallel guessing attack. Chang et al. [3] proposed an improved protocol. However, Lo et al. [4] demonstrated that the Chang et al.'s protocol does not offer the mutual authentication property. Lo et al. also proposed an improved scheme using elliptic curve cryptography (ECC), included their protocol in 3GPP2 specifications and claimed their scheme could withstand various attacks. However, in this letter, we will propose an off-line password guessing attack against Lo et al.'s protocol.

2. Review of Lo et al.'s scheme

Before the review of Lo et al.'s protocol [5], we first introduce some notations as follows, which is common with that used in [5].

- A, B: The abbreviation/identity of the participator Alice (client) and Bob (server) individually;
- E: an elliptic curve defined over a finite field Fq with large group order;
- n: a secure large prime;
- P, Q: two points in E with large order n;
- D: a uniformly distributed dictionary of size $|D|$;
- S: a low-entropy password shared between Alice and Bob, which is randomly chosen from D;
- t: the value t is derived from the password S in a predetermined way, which is uniformly distributed in Z_n^*;
- H: a secure one-way hash function.

Lo et al.'s protocol is illustrated in Fig. 1. The detail steps are described as follows.

Step 1: Alice (A) picks a random number $d_A \in [1, n-1]$ and computes $Q_A = (d_A + t)P$, where t is an integer which is predetermined by the corresponding password and P is a point in the elliptic curve. Then A sends out its identity A and Q_A to Bob (B).

Step 2: B also chooses a random number $d_B \in [1, n-1]$ and then computes $Q_B = (d_B - t)P$, $Y = Q_A - tP$, $K_B = d_B Y$ and $H_B = H(K_B \| Y)$. Next, B sends the Q_B and H_B to A.

Step 3: A computes $X = Q_B + tP$ and then computes $K_A = d_A X$. Next, A verifies the equality of $H(K_A \| d_A P)$ and H_B. If it does not hold, the protocol is terminated. Otherwise, A sends the $H_A = H(K_A \| X)$ to B and sets the session key to K_A.

Step 4: When B receives the message, it checks the equality of $H(K_B \| d_B P)$ and H_A. Only if the equality holds, B agrees the session key K_B. Otherwise, B terminates the protocol.

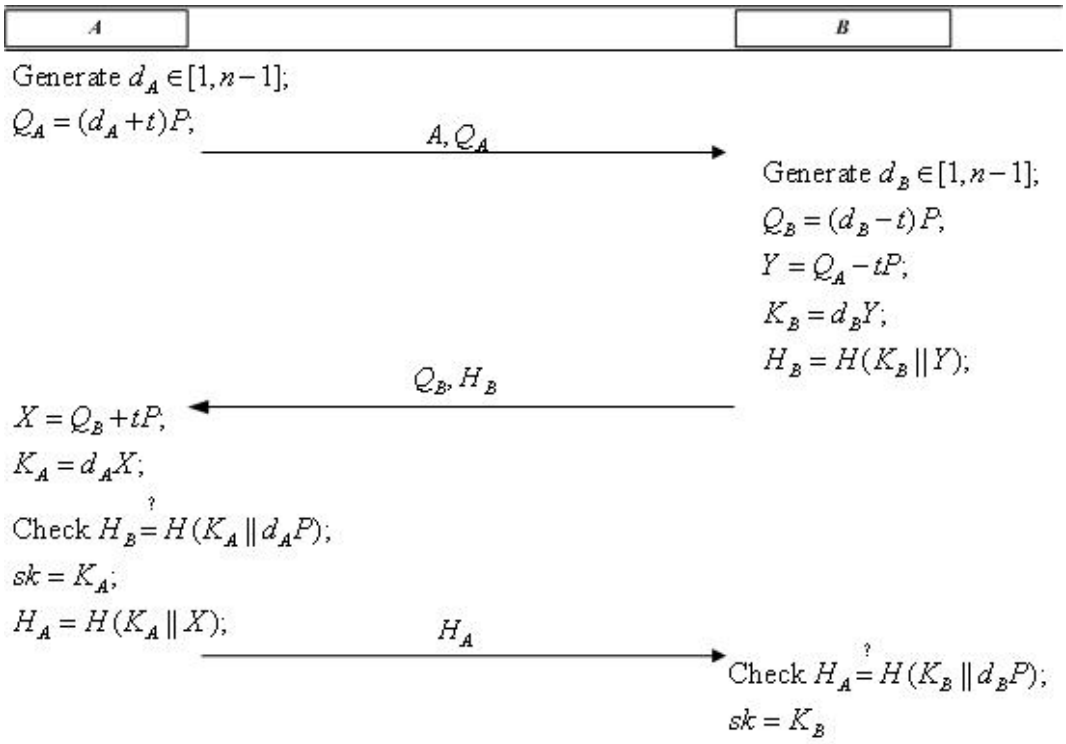

Fig. 1. Lo et al.'s scheme

3. Weakness in Lo et al.'s protocol

3.1. Off-line password guessing attack on Lo et al.'s protocol

Off-line password guessing attack succeeds when there is information in communications, which can be used to verify the correctness of the guessed passwords. In [5], Lo et al. claimed that their protocol can resist the off-line password guessing attack. However, in this section, we will show that the off-line password guessing attack, not as they claimed, is still effective in Lo et al.'s protocol. Our attack consists of two phases.

- **First phase**

1). The adversary C generates a random number $d_A \in [1, n-1]$, computes $Q_A = d_A P$, and sends A and Q_A to B.

2). Upon receiving A and Q_A, B also chooses a random number $d_B \in [1, n-1]$ and then computes $Q_B = (d_B - t)P$, $Y = Q_A - tP = (d_A - t)P$, $K_B = d_B Y = d_B(d_A - t)P = d_A d_B P - t d_B P$ and $H_B = H(K_B \| Y)$. Next, B sends the Q_B and H_B to A.

Upon receiving Q_B and H_B, the adversary C carry out the second phase as follows.

- **Second phase**

1). The adversary C chooses guess a password S' from D and derive the corresponding t'.

2). C computes $Y' = (d_A - t')P$, $(d_B P)' = Q_B + t'P$, $(d_A d_B P)' = d_A (d_B P)'$, $(td_B P)' = t'(d_B P)'$ and $K'_B = (d_A d_B P)' - (td_B P)'$.

3). C verifies the equality of $H(K'_B \| Y')$ and H_B. If it does hold, the adversary gets the correct password. Otherwise, C repeats Step 1, Step 2 and Step 3 in the second phase until finding the correct password.

From the above description, we know the adversary can get the password. Therefore, Lo et al.'s scheme is vulnerable to the off-line password guessing attack.

3.2. Denning-Sacco attack

Dennig-Sacco attack works when a user compromises an old shared session key sk and an attacker tries to find a long-term private key (e.g., user password S) or other session keys. This attack arises from the fact that compromising a fresh session key sk enables the scheme to be compromised. Such attacks have been known for some time. Refer to the Denning-Sacco attack in [6]. In Lo et al.' s authentication scheme, the following Denning-Sacco attack is possible. Our attack consists of two phases.

- **First phase**

1)An attacker records one run of Lo et al.'s authentication scheme and somehow obtains the old shared session key $d_A d_B P$ between A and B.

2) Since $Q_B = (d_B - t)P$ and $H_B = H(K_B \| Y)$ are open values from Steps1 and Steps2 of Lo et al.'s scheme , the attacker can find the long-term private password S included in $Q_A = (d_A + t)P$ by performing the following off-line password guessing attack.

- **Second phase**

1) The adversary C chooses guess a password S' from D and derive the corresponding t'.

2) The attacker checks if H_B and $H(d_A d_B P \| Q_A - t'P)$ are equal. If they are equal, the attacker has guessed the correct secret password $S = S'$. Otherwise, the attacker repeats the above verification process until $H(d_A d_B P \| Q_B + t'P)$ and H_B are equal i.e. finding the correct password.

From the above description, we know the adversary can get the password. Therefore, Lo et al.'s scheme is vulnerable to the Dennig-Sacco attack.

5. Conclusions

In this paper, we first reviewed Lo et al.'s protocol [5], and pointed out that their protocol can't resist the off-line password guessing attack and the Dennig-Sacco attack.

Reference

[1]. A.-F. Sui, L. C. K. Hui, S. M. Yiu, K. P. Chow, W. W. Tsang, C. F. Chong, K. H. Pun and H. W. Chan, An improved authenticated key agreement protocol with perfect forward secrecy for wireless mobile communication, 2005 IEEE Wireless Communications and Networking Conference, vol.4, pp.2088-2093, 2005.

[2]. R. Lu, Z. Cao and H. Zhu, An enhanced authenticated key agreement protocol for wireless mobile communication, Computer Standards & Interfaces, vol.29, pp.647-652, 2007.

[3]. C.-C. Chang and S.-C. Chang, An improved authentication key agreement protocol based on elliptic curve for wireless mobile networks, 2008 International Conference on Intelligent Information Hiding and Multimedia Signal Processing, pp.1375-1378, 2008.

[4]. J.-W. Lo, C.-C. Lee, M.-S. Hwang, A Secure and Efficient ECC-based AKA Protocol for Wireless Mobile Communications, International Journal of Innovative Computing, Information and Control, vol. 6, no. 11, pp. 5249-5258, 2010.

[5]. D. Denning, G. Sacco, Timestamps in key distribution systems, Communications of the ACM 24 (1981) 533–536.