Improved Yen-Joye's Authenticated Multiple-key Agreement Protocol*

Min-Shiang Hwang† Chih-Wei Lin† Cheng-Chi Lee‡

Institute of Networks and Communications†
Chaoyang University of Technology
168 Gifeng E. Rd., Wufeng,
Taichung County, Taiwan 413, R.O.C.
Email: mshwang@cyut.edu.tw
Fax: 886-4-23742337

Department of Computer and Information Science‡
National Chiao-Tung University
1001 Ta Hsueh Road,
Hsinchu, Taiwan, R.O.C.
Email: cclee@cis.nctu.edu.tw

April 2, 2002

*This research was partially supported by the National Science Council, Taiwan, R.O.C., under contract no.: NSC90-2213-E-324-004.

Improved Yen-Joye's Authenticated Multiple-key Agreement Protocol

Abstract

In this article, we propose an authenticated multiple-key agreement protocol. The protocol not only secure to against the unknown-key attack but also more efficient than the other protocols.

Keywords: Cryptography, key agreement, key authentication, unknown-key attack.

1 Introduction

Diffie and Hellman first proposed key agreement protocol to establish a session key for two parties [1]. However, the protocol was later proven to be vulnerable to the *unknown key attack* by Diffie et al. [2] because the protocol did not include any key authentication process during the negotiation between the two parties [7, 9].

In 1997, Harn first proposed the authenticated key agreement protocol [3] without using a one-way hash function [6]. In 1998, Harn and Lin proposed an authenticated multiple-key agreement protocol based on the Diffie-Hellman distribution scheme [4]. There are two main features in this protocol: it without using a one-way hash function and it enable two communication entities to share multiple secret keys.

Later, the Yen-Joye [11] indicated that the Harn-Lin protocol is not secure because an attacker can successfully forge a short-term public key pair and pass the verification equation. Then, they proposed an improved the Harn-Lin protocol to get rid of this shortcoming. However, in 1999, Wu et al. [10] pointed out that the Yen-Joye protocol is insecure and can be successfully attacked the same way the Harn-Lin protocol is. Wu et al. then proposed a protocol to enhance the security. Nevertheless, the protocol violated the original expectation of the Harn-Lin protocol that no one-way hash function should be used in the authenticated key agreement protocol.

In this article, we shall propose a modification of the Yen-Joye protocol. The modification does not only ameliorate the security but also is more efficient than Harn's protocol proposed in 2001 [5].

2 Review of the Yen-Joye Protocol

In this section, we shall briefly review the Yen-Joye protocol [11]. There are two phases in the protocol. The first phase is the authentication phase where two users exchange n temporary random public keys in an authenticated way. The second phase is the key-sharing phase where the users share $n^2 - 1$ secret keys with each other.

There are two users *Alice* and *Bob* who want to establish the multiple keys by the protocol. Here, we only describe what Alice has to do because of Bob has to do basically the same thing Alice does. Initially, the system has a large prime p, and α is a primitive number in $GF(p)$. Alice has a long-term secret key x_A and the corresponding long-term public key $y_A = \alpha^{x_A} \bmod p$. Then Alice randomly generates two short-term secret keys k_{A1} and k_{A2} and computes their corresponding short-term public keys $r_{A1} = \alpha^{k_{A1}} \bmod p$ and $r_{A2} = \alpha^{k_{A2}} \bmod p$, respectively. The range of r_{A1} and r_{A2} is set to be $(\lceil p/2, p-1 \rceil)$ so that no attacker can forge the keys. Alice computes the signature s_A through r_{A1} and r_{A2} as

$$s_A = x_A - (r_{A1} \cdot r_{A2}) \cdot k_A \bmod (p-1), \tag{1}$$

where $k_A = k_{A1} \cdot k_{A2} \bmod p$. Finally, Alice sends $r_{A1}, r_{A2}, s_A, cert(y_A)$ to Bob, where $cert(y_A)$ is a certificate for Alice's public key y_A. After receiving them, Bob verifies them via the computation as follows:

$$y_A \equiv ?(r_{A1} \cdot r_{A2})^{(r_{A1} \cdot r_{A2})} \alpha^{s_A} \bmod p. \tag{2}$$

If it holds, Bob establishes the multiple secret keys in the second phase. Bob can derive the session keys as follows:

$$\begin{cases} K_1 = r_{A1}^{k_{B1}} \bmod p, \\ K_2 = r_{A2}^{k_{B1}} \bmod p, \\ K_3 = r_{A1}^{k_{B2}} \bmod p, \\ K_4 = r_{A2}^{k_{B2}} \bmod p. \end{cases}$$

Here, three of the four keys can be used because of *perfect forward secrecy* [8]. Thus, three authenticated session keys can be established in this protocol.

3 Improved Protocol

The Yen-Joye protocol is an improvement on the Harn-Lin protocol. However, according to Wu et al., the Yen-Joye protocol is no secure than its predecessor. They pointed out the Yen-Joye protocol cannot resist the same attack that bothers the Harn-Lin protocol. The attacker can forge a pair $\{r'_{A1}, r'_{A2}\}$ in the range $([p/2, p-1])$ to satisfy $r'_{A1}r'_{A2} = r_{A1}r_{A2}$ at the probability of greater than 1/18. Although Wu et al. later proposed an enhanced protocol with a one-way hash function, this improved protocol violates the original expectation from the Harn-Lin protocol that no one-way hash function should be used in the authenticated multiple keys agreement protocol. In 2001, the Harn-Lin proposed an improved authenticated multiple keys agreement protocol and claimed their protocol can eliminate the attack from [10, 11].

However, the Harn-Lin protocol is not as efficient as the Yen-Joye protocol. In this article, we propose two straightforward modifications to enhance the security of the Yen-Joye protocol. The proposed protocol can withstand the attack on Wu et al's scheme and is more efficient than [5]. First, we suggest that the pair of short-term public keys r_{A1} and r_{A2} in the generation phase should be prime numbers. This modification can help the new scheme prevent the attacker from forging another pair (r'_{A1}, r'_{A2}) because the prime numbers are unique. In addition, it can obey the original requirement of the Harn-Lin protocol that the range of r_{A1} and r_{A2} should be in $(1, p-1)$. Second, we suggest that the *great common divisor (GCD)* of r_{A1} and r_{A2} should be equal to 1. This suggestion is to prevent the attacker from finding the factor q of r_{A1} or r_{A2}. Furthermore, the range of r_{A1} and r_{A2} will fall in the $(\lceil p/2 \rceil, p-1)$ as the Yen-Joye protocol proposed. Both of the modifications of on the Yen-Joye protocol can make it secure against any forge of the pair (r_{A1}, r_{A2}). Besides, our modification protocol is more efficient than the Harn-Lin protocol [5] because we only do the exponentiation computation four times, less than six times required by the Harn-Lin protocol.

4 Conclusion

We have proposed an improved scheme to enhance the security of the Yen-Joye protocol. We require that r_{A1} and r_{A2} should be primes or $GCD(r_{A1}, r_{A2})$ should be equal to 1 to withstand the attack of forging another pair (r'_{A1}, r'_{A2}) so that $r_{A1} \cdot r_{A2} = r'_{A1} \cdot r'_{A2}$. The pair r_{A1} and r_{A2} should be made unique so that no attacker can find another pair to replace them. Furthermore, the Harn-Lin protocol [5] uses six exponentiation computations, while the Yen-Joye scheme four takes only. That means the Harn-Lin protocol is less efficient.

In this article, we have proposed two straightforward modifications to withstand the forgery attack on the Yen-Joye protocol. The proposed protocol retains the original expectation on the Harn-Lin protocol that the range of the short-term public key be $(1, p-1)$. Furthermore, the new protocol uses less exponentiation computations than the Harn-Lin protocol [5].

References

[1] Whitfield Diffie and M. Hellman, "New directions in cryptology," *IEEE Transations on Information Theory*, vol. IT-22, no. (6), pp. 644–654, 1976.

[2] Whitfield Diffie, Paul C. van Oorschot, and Michael J. Wiener, "Authentication and authenticated key exchanges," *Designs, Codes and Cryptography*, vol. 2, no. (2), pp. 107–125, 1992.

[3] Lein Harn, "Digital signatures for Diffe-Hellman public keys without using one-way function," *Electronics Letters*, vol. 33, no. (2), pp. 125–126, 1997.

[4] Lein Harn and Hung-Yu Lin, "An authenticated key agreement protocol without using one-way functions," in *Proceedings of the 8th National Conference on Information Security*, pp. 155–160, Kaohsiung, Taiwan, May 1998.

[5] Lein Harn and Hung-Yu Lin, "Authenticated key agreement without using one-way hash functions," *Electronics Letters*, vol. 37, no. (10), pp. 629–630, 2001.

[6] Min-Shiang Hwang, Chin-Chen Chang, and Kuo-Feng Hwang, "A watermarking technique based on one-way hash functions," *IEEE Transactions on Consumer Electronics*, vol. 45, no. 2, pp. 286–294, 1999.

[7] Cheng-Chi Lee, Min-Shiang Hwang, and Li-Hua Li, "A new key authentication scheme based on discrete logarithms," *Applied Mathematics and Computation*, accepted (March 12, 2002) and to appear.

[8] C. H. Lin and P. J. Lee, "Security of interactive DSA batch verification," *Electronics Letters*, vol. 30, no. (19), pp. 1592–1593, 1994.

[9] Eric Jui-Lin Lu and Min-Shiang Hwang, "An improvement of a simple authenticated key agreement algorithm," *Pakistan Journal of Applied Sciences*, vol. 2, no. 1, pp. 64–65, 2002.

[10] Tzong-Sun, Wei-Hua He, and Chien-Lung Hsu, "Security of authenticated multiple-key," *Electronics Letters*, vol. 35, no. (5), pp. 391–392, 1999.

[11] Sung-Ming Yen and M. Joye, "Improved authenticated multiple-key agreement protocol," *Electronics Letters*, vol. 34, no. (18), pp. 1738–1739, 1998.