I.J. Wireless and Microwave Technologies, **2011, 4, 65-69**
Published Online August 2011 in MECS (http://www.mecs-press.net)
DOI: 10.5815/ijwmt.2011.04.09

Available online at http://www.mecs-press.net/ijwmt

A New Three-party Key Exchange Protocol Based on Diffie-Hellman

Chunling Liu[a,*], Yufeng Wang[a], Qinxi Bai[a]

[a] *School of Mathematics & Information, Ludong University, Yantai, Shandong, China*

Abstract

The goal of key exchange protocol is to establish a common and secure session key using the interactive communications. The existing schemes are usually in the pattern of 'user-server-user', so are weak in reality. In this paper, a new three-party key exchange protocol based on Diffie-Hellman was proposed which contains the following characteristics: without server; providing key secrecy and forward secrecy; ensuring no key control; ensuring known-key secrecy.

Index Terms: Diffie-Hellman; Three-party Key Exchange; DLP

1. Introduction

An important problem in cryptography is how to create keys in exchange protocol, such as DES or AES, especially when two parties are far away[1]. In secure communications, key exchange protocol has an important role in the foundation [2]. Key exchange protocol is aiming to communicate safely in unsafely channel by the communication parties' interaction and to establish common session key. Communication parties' sharing key used to be a difficult problem before public key cryptography appears.

The procedure needs a safety channel, which means special messengers in physical. Public key cryptography's significant advantage is to exchange keys without safety channel. The earliest reality protocol is brought out by Diffie and Hellman, which is named Diffie-Hellman Exponential Key Exchange Protocol[3]. Its security closely related to the difficulty of computing discrete logarithm problem[4],[5]. The protocol can not only establish sharing key, also provide three-party and multy-party session key.

Some protocols depend on public key technology, and need PKI system. The cost is high. Some protocols need two parties share long random key. The key usually is chosen by appropriate program, and is difficult to be remembered and be saved. So a natural idea is to share easy remembering private key, and create high quality session key. Now, usually 3*PAKE* uses the model of user-server-user, which limits practical application.

A 3*PAKE* based on Diffie-Hellman is proposed , which could establish safe and reliable session key. Three users can communicate safely in the unsafely channel. The paper analyzes the efficiency and safety comparing with the existence protocol. A protocol is not only an algorithm, but also a communicating. The communication

This article is sponsored by the Talents Foundation of Ludong University(No.LY20062706)

* Corresponding author:
E-mail address: girllcl2008@163.com

procedure includes transferring messages by different participants in the agreed rules. So the protocol has a dimension, which called communication round. Usually, the cost of communication is larger than local computation [6]. The goal of key exchange protocol is to establish a common and secure session key using the interactive communications. The existing schemes are usually in the pattern of 'user-server-user', so are weak in reality. Thus we hope to minimize reduce the rounds of communication. The 3PAKE only needs two round communication, and it also can provide forward security and key security and against known key attack.

2. Prepared Knowledge

2.1. Discrete logarithm problem (DLP)

Security of some cryptography technology is based on DLP difficulty. The general DLP [6]: Given a finite cyclic group G ordered by n, and a generator α and an element β belong to G. Now solve an integer x ($0 \le x \le n-1$), which could meet $\alpha^x = \beta$.

2.2. Computational Diffie-Hellman problem(CDHP)

The general CDHP[7]: Given a finite cyclic group G, a generator α and an element α^a and an element α^b, now solve α^{ab}

CDHP has no a reality and feasible solution yet[8].

2.3. Diffie-Hellman Public Exchange Protocol

A classical Diffie-Hellman public exchange protocol exam of two parties is given. $Alice$ and Bob establish session key K on public channel[1].

1) $Alice$ or Bob choose a safety large prime p and a generator $\alpha \pmod p$, p and α are public.

2) $Alice$ chooses a private random number x ($1 \le x \le p-2$), Bob privately chooses a random y ($1 \le y \le p-2$)

3) $Alice$ sends $\alpha^x \pmod p$ to Bob, and Bob sends $\alpha^y \pmod p$ to $Alice$.

4) By using their respective received information, they calculate session key K, $Alice$ uses $K \equiv \left(\alpha^y\right)^x \pmod p$ to get K, Bob uses $K \equiv \left(\alpha^x\right)^y \pmod p$ to get K.

3. A New 3PAKE Based on Diffie-Hellman

A new 3*PAKE* based on Diffie-Hellman is brought up, and the following is detailed protocol procedure. Table 1 intuitively describes the protocol implementation.

3.1. Initialization Process

F_q is a finite field, A, B and C are users, public key of A is y_A, private key is x_A, B's public key is y_B, and private key is x_B, C's public key is y_C, private key is x_C. Every user's public key and private key have the function relation $y = g^x$, that is to say $y_A = g^{x_A}$, $y_B = g^{x_B}$, $y_C = g^{x_C}$.

3.2. Protocol Process

If A, B, C want to establish session key, the protocol process is shown in table 1.

- **Round 1**

User A chooses a random constant number a in F_q, calculates and makes public of $T_{AB} = y_B^{ax_A}$, $T_{AC} = y_C^{ax_A}$, and sends T_{AB}, T_{AC} respectively to user B, C.

User B randomly chooses constant number b in F_q, calculates and make public $T_{BA} = y_A^{bx_B}$, $T_{BC} = y_C^{bx_B}$, and sends T_{BA}, T_{BC} respectively to user A, C.

User C randomly chooses constant number c in F_q, calculates $T_{CA} = y_A^{cx_C}$, $T_{CB} = y_B^{cx_C}$ and makes them public, and sends T_{CA}, T_{CB} respectively to user A, B.

- **Round 2**

User A receives $T_{BA} = y_A^{bx_B}$ sent by B, and $T_{CA} = y_A^{cx_C}$ sent by C, A Calculates like this:

$$T_{BA}^{x_A^{-1}} = y_B^{\ b} = g^{bx_B},\ T_{CA}^{x_A^{-1}} = y_C^{\ c} = g^{cx_C},\ K = g^{ax_A} \cdot g^{bx_B} \cdot g^{cx_C} = g^{ax_A+bx_B+cx_C}.$$

User B receives $T_{AB} = y_B^{ax_A}$ sent by A, and $T_{CB} = y_B^{cx_C}$ sent by C, B Calculates like this:

$$T_{AB}^{x_B^{-1}} = y_A^{\ a} = g^{ax_A},\ T_{CB}^{x_B^{-1}} = y_C^{\ c} = g^{cx_C},\ K = g^{ax_A} \cdot g^{bx_B} \cdot g^{cx_C} = g^{ax_A+bx_B+cx_C}.$$

User C receives $T_{AC} = y_C^{ax_A}$ sent by A, and $T_{BC} = y_C^{bx_B}$ sent by B, C Calculates like this:

$$T_{AC}^{x_C^{-1}} = y_A^{\ a} = g^{ax_A},\ T_{BC}^{x_C^{-1}} = y_B^{\ b} = g^{bx_B},\ K = g^{ax_A} \cdot g^{bx_B} \cdot g^{cx_C} = g^{ax_A+bx_B+cx_C}.$$

K is the three-party session key of A, B and C.

Table 1. Proposed protocol

Protocol \ Users		User A	User B	User C
Public key		y_A	y_B	y_C
Private key		x_A	x_B	x_C
Round 1	Random	a	b	c
	Calculating and sending	$T_{AB} = y_B^{\,ax_A} \to B$, $T_{AC} = y_C^{\,ax_A} \to C$.	$T_{BA} = y_A^{\,bx_B} \to A$, $T_{BC} = y_C^{\,bx_B} \to C$.	$T_{CA} = y_A^{\,cx_C} \to A$, $T_{CB} = y_B^{\,cx_C} \to B$.
Round 2	Receiving	T_{BA}, T_{CA}	T_{AB}, T_{CB}	T_{AC}, T_{BC}
	Calculating	$T_{BA}^{\,x_A^{-1}} = y_B^{\,b} = g^{bx_B}$, $T_{CA}^{\,x_A^{-1}} = y_C^{\,c} = g^{cx_C}$, $K = g^{ax_A+bx_B+cx_C}$.	$T_{AB}^{\,x_B^{-1}} = y_A^{\,a} = g^{ax_A}$, $T_{CB}^{\,x_B^{-1}} = y_C^{\,c} = g^{cx_C}$, $K = g^{ax_A+bx_B+cx_C}$.	$T_{AC}^{\,x_C^{-1}} = y_A^{\,a} = g^{ax_A}$, $T_{BC}^{\,x_C^{-1}} = y_B^{\,b} = g^{bx_B}$, $K = g^{ax_A+bx_B+cx_C}$.

4. Analysis of Efficiency and Safety

4.1. Efficiency Analysis

Now, let's to analyze the protocol efficiency from computing cost and communication cost. Every user needs 4 exponentiations and 3 multiplications to establish a session key. Every time protocol runs, three users need 2 rounds of communication.

4.2. Security Analysis

1) Correctness and fairness

If members honestly run protocol, the session key will be the same. Every honest member provides the needed information of the session key in discussion. Every member can calculate session key only if he gets others' information. No one can establish session key himself.

2) Key confidentiality

The protocol can provide key confidentiality.

① Because of the difficulty of *CDHP*, competitor could not get any information about key by intercepted T_{AB}, T_{AC}, T_{BA}, T_{BC}, T_{CA} and T_{CB}.

②Supposed the enemy could distinguish session key and random string by non-negligible probability, which means they could solve *DLP* problem. It contracts with the difficulty of DLP problem.

3) Forward Security

The forward security of key exchange protocol based on Diffie-Hellman means even the attackers can get one or more private key, it could not affect session key's security previously created. That is to say the session key and private key are independent. Even x_A, x_B and x_C are leaked, the attackers can't destroy key

confidentiality. Every session key's establishment needs user's random number a , b c and $K = g^{ax_A+bx_B+cx_C}$ .If the attackers want to get these random numbers, they should solve *DLP* problem, which is difficult.

4) Known key security

Even attackers get some communication's session key, they couldn't get other communications' session key. That is to say session key is independent. The quality is known key security. The protocol is known key security. The final session is established by some random numbers. In the protocol, a , b , c are chosen randomly by A , B , C .To the attackers, getting one session key, has no help to other session keys.

5) No key control

Any party in the communication couldn't choose a predetermined value, meanwhile two parties contribute to the final session key. No one could control the key's chosen .The final session key $K = g^{ax_A+bx_B+cx_C}$, K depends on user A , B , C 's chosen random numbers and their private key, No party can determine the value of session key.

6) Anti-replay attack

Every session key is independent, and it has the characteristic of one-time password. It can defend replay attack.

5. Conclusion

The new 3*PAKE* based on Diffie-Hellman problem was proposed. Its security bases on DLP, and has better security. The protocol can establish effective three-party session key, and can provide key confidentiality, forward security, and no key control. Comparing with existence protocol, it is fit for practical applications not like the existing schemes in the pattern of 'user-server-user'.

References

[1] Wade Trappe and L. C. Washington, Cryptography and coding theory(in chinese),Beijing: Posts & Telecom Press, 2008.
[2] Yong-jun Ren , Jian-dong Wang, YiZhuang, Enhanced Identity-Based Authenticated Key Agreement Protocols in the Standard Model(in chinese), Journal of Electronics & Information Technology, 2009, vol.31,no.8, pp.1990-1995.
[3] W. Diffie and M. E. Hellman, New directions in cryptography, IEEE Transactions on Information Theory, 1976, vol.22.no.9,pp.644-654.
[4] Wenbo Mao,Modern Cryptography: Theory and Practice(in chinese),Beijing: Publishing house of Electronic Industry, 2004.
[5] W M Li, QY Wen, H Zhang,Verifier-based password-authenticated key exchange protocol for three-party (in chinese) ,Journal on Communications, 2008, vol.29,no.10,pp.149-152, 164.
[6] H M Sun, B C Chen, T Hwang,Secure key agreement protocols for three-party against guessing attacks,The Journal of Systems and Software, 2005, vol.75,no.1/2,pp.63-68.
[7] Alfred J. Menezes, Paul C. van Oorschot, Handbook of Applied Cryptography (in chinese),Beijing: Publishing house of Electronic Industry, 2005.
[8] L. Washington,Elliptic Curves: Number Theory and Cryptography, Chapman & Hall/CRC Press, 2003.