변형 Diffie-Hellman 키교환 프로토콜

양 대 헌[†] · 이 경 희[††]

요 약

이 논문에서는 사전 연산이 가능한 세션 키와 복잡한 암호 프로토콜 디자인에 도움이 될 수 있는 변형된 Diffie-Hellman 키 교환 프로토콜을 보인다. 제안된 프로토콜은 Diffie-Hellman 키 교환 프로토콜을 간결화 하였으며 본래의 프로토콜과 같은 보안성을 가진다.

키워드 : 암호프로토콜, 키 교환, Diffie-Hellman, 선계산

One Variant of Diffie-Hellman Key Exchange Protocol

DaeHun Nyang[†] · KyungHee Lee[††]

ABSTRACT

In this paper, we propose a variant of Diffie-Hellman key exchange protocol to provide pre-computable session key and to give another version of Diffie-Hellman key exchange protocol that might be useful in designing more sophisticated cryptographic protocols. We prove the security of the key exchange protocol by reducing DH key exchange protocol to ours.

Key Words : Cryptographic protocol, Key Exchange, Diffie-Hellman, Precomputation

1. Introduction

We propose a variant of Diffie-Hellman key agreement protocol[1] that has been widely used for establishment of a common key between communicating parties in insecure environment. Our protocol has an advantage over the original Diffie-Hellman key exchange protocol in that the common key can be prepared by one party before the other party requests to establish a key. Owing to the pre-computable key, one can pre-encrypt messages to be sent before the other communicating party connects, which results in some efficiency and convenience of the following protocol actions.

Actually, the pre-computable key can be established by key transport protocol of public key cryptography such as ElGamal, but it has more overhead in terms of computation and communication. Compared to RSA, our scheme can be adopted to many discrete log based key exchange and authentication protocols such as DH-EKE, SPEKE, SSL, etc.

The proposed scheme is as secure as Diffie-Hellman key exchange protocol in the sense that Diffie-Hellman key exchange protocol is reduced to our protocol in polynomial time.

2. Diffie-Hellman Problem

Group G: All considered assumptions are based on cyclic finite groups. The order of a group is associated with a security parameter which classifies the group according to the difficulty of certain problems. Examples of G are Z_p^* and additive group of an elliptic curve.

Generator g: In the discrete logarithm settings, we also need a generator g which generates the group G, i.e., for

† 정 회 원 : 인하대학교 정보통신대학원 조교수
†† 정 회 원 : 수원대학교 전기공학과 조교수
논문접수 : 2007년 3월 22일, 심사완료 : 2007년 9월 10일

all $y \in Z_{|G|}$, there exists x such that $y \equiv g^x$.

3. Diffie-Hellman Assumption

For any computationally bounded adversary A within $poly(k)$,

$$P[g^{xy} = A(g, G, g^x, g^y)] < 1/poly(k),$$

where A has a Diffie-Hellman triple as its input and outputs a Diffie-Hellman key.

4. The Protocol

Let the communicating parties be A and B.

$$A \rightarrow B: X = g^x \bmod p, x \in_R Z_p^*$$
$$B \rightarrow A: Y = g^{xy} \bmod p, y \in_R Z_p^*$$

A and B shares a key $K = g^{xy} \bmod p$, because $K = g^{xy} \bmod p$ is equivalent to $K' = Y^{1/x} \bmod p$ which A is able to compute.

Note that to compute g^{xy} from $(g^x \bmod p,\ g^{xy} \bmod p)$ is equivalent to computing $g^{y/x}$ from $(g^x \bmod p,\ g^y \bmod p)$. It is easy to verify this: let $t = xy \bmod p - 1$. Then, $y = t/x \bmod p - 1$.

Now, the problem is to find $g^{t/x} \bmod p$ from $(g^x \bmod p,\ g^t \bmod p)$.

5. Security and Performance

In this section, we will provide an efficient algorithm to solve computational Diffie-Hellman problem in polynomial time given an oracle that is able to output $g^{y/x} \bmod p$ for an input $(g^x \bmod p,\ g^y \bmod p)$. This will show that our protocol is as hard as computational Diffie-Hellman is.

Let A be the oracle that breaks our protocol in polynomial time. That is, the oracle A can compute $g^{y/x} \bmod p$ from $(g^x \bmod p,\ g^y \bmod p)$ in polynomial time. If the oracle A exists, then we can solve computational Diffie-Hellman problem in polynomial time as follows:

Let an instance of computational Diffie-Hellman problem be $(X = g^x \bmod p,\ Y = g^y \bmod p)$.

(1) Given (X, Y), query to A, then it gives us $g^{y/x} \bmod p$.

(2) Query to A with $(g^y \bmod p,\ g^{y/x} \bmod p)$ gives us $g^{1/x} \bmod p$.

(3) We can obtain $g^{xy} \bmod p$ by querying to A with $(g^{1/x} \bmod p,\ g^y \bmod p)$.

Thus, by querying 3 times with different inputs to A, we can solve Diffie-Hellman problem in polynomial time. QED.

Also, note that computing $g^{1/x}$ from g^x is called "inversion exponent problem" which is known to be as secure as the Diffie-Hellman problem in most cases[2], which is reducible to our problem.

One might concern that pre-encryption of some message in a server looks vulnerable in the sense that keys as well as corresponding encrypted messages must be securely stored in a server. When a server is attacked, the keys and encrypted messages are exposed to an attacker. However, if we assume the server compromise, it cannot be avoided to expose messages to an attacker even though our pre-computation is not applied. That is, our protocol does not make the system fragile and secure keeping of messages is another subject of matters and thus, is out of this paper's scope.

In fact, advantage of pre-encryption might be very small, because pre-encryption of massive data can be done using a random key and the random key can be encrypted to be sent to a client using DH key. Thus, the advantage is to eliminate only one encryption of a random key plus communication overhead which amounts only to one ciphertext. In spite of the 'not so big' advantage, it has a meaning that this key exchange protocol might be used as a building block for more sophisticated cryptographic protocols that has security proof equivalent to Diffie-Hellman key exchange protocol.

Also, in a very restricted environment that requires realtime response, it might be useful by saving even one encryption plus communication overhead of one ciphertext. For example, in wireless sensor network, sensor nodes usually are very power-sensitive and thus, the saving of even one symmetric key encryption and one transportation of ciphertext might be meaningful especially because the sending one bit of information requires one hundred times of power consumption of computation one operation in Mote.

6. Application

DH-EKE protocol is a famous password authenticated key exchange protocols, and it results in a session key looked like the Diffie-Hellman key: h(DH key), where h is a cryptographic hash function. Also, SPEKE has a similar structure whose resulting session key is $h(f(S)^{rq})$, where $f(S)$ is a function that converts S into a suitable DH base. Hereby, we can replace the DH part of the protocols with our construction. By doing so, we can get another variant of those protocols that have pre-computable session keys, where the number of exponentiation can be saved. Besides those, the most widely used key exchange and authentication protocol, SSL, has a method to establish a session key via Diffie-Hellman key exchange. This protocol also can be modified to accommodate our protocol.

7. Conclusion

In this paper, we presented a variant of Diffie-Hellman key exchange protocol, which is provably as secure as the original Diffi-Hellman protocol. The protocol is able to establish a pre-computable key, and thus, computation and communication for one encryption are saved. We leave as a future work to find some sophisticated protocols that our primitive might be more applicable.

Reference

[1] Whitfield Diffie, Martin Hellman, "New directions in cryptography," IEEE Transactions on Information Theory, IT-22(6), pp.644-654, November 1976.

[2] A.R. Sadeghi, M. Steiner, "Assumptions related to discrete logarithms: why subtleties make a real difference," Advances in Cryptology-Eurocrypt 2001, LNCS 2045, pp.243-260, Springer-Verlag, 2001.

양 대 헌

e-mail : nyang@inha.ac.kr

1994년 2월 한국과학기술원 과학기술 대학 전기 및 전자 공학과 졸업

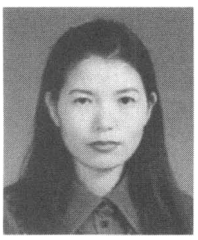
1996년 2월 연세대학교 컴퓨터 과학과 석사

2000년 8월 연세대학교 컴퓨터 과학과 박사

2000년 9월~2003년 2월 한국전자통신연구원 정보보호연구본부 선임연구원

2003년 2월~현 재 인하대학교 정보통신대학원 조교수

관심분야 : 암호이론, 암호프로토콜, 인증프로토콜, 무선 인터넷 보안



이 경 희

e-mail : hlee@suwon.ac.kr

1989년 서울대학교 식품영양학과 학사

1993년 연세대학교 전산과학과 학사

1998년 연세대학교 컴퓨터과학과 석사

2004년 연세대학교 컴퓨터과학과 박사

1993년 1월~1996년 5월 LG소프트(주) 연구원

2000년 12월~2005년 2월 한국전자통신연구원 선임연구원

2005년 3월~현 재 수원대학교 전기공학과 조교수

관심분야 : 정보보호, 영상처리, 컴퓨터비전, 인공지능, 패턴인식, 생체인식, 얼굴인식, 다중생체인식