논문 2008-6-3

Cramer-Shoup 공개키 암호 시스템의 안전성 증명에 관한 고찰

On the Security Proof of the Cramer-Shoup Public Key Cryptosystem

황성운*

Seong Oun Hwang

요 약 증명 가능한 안전성은 암호에서 어떤 암호 시스템의 안전성을 정형적으로 증명하는데 널리 사용되어 왔다. 본 논문에서는, 적응적 선택 암호문 공격에 대해 안전하다고 증명된 Cramer-Shoup 공개키 암호 시스템을 분석하고, 그 안전성 증명이 일반적 의미에서의 적응적 선택 암호문 공격에 대해서는 완전하지 않음을 보인다. 향후 연구 방향으로는 크게 두 가지 방향을 생각할 수 있다. 첫째는, 일반적 의미에서의 적응적 선택 암호문 공격에 대해서 완전하도록 Cramer-Shoup 공개키 암호 시스템을 수정하는 것이며, 둘째는 현재의 Cramer-Shoup 공개키 암호 시스템에 대하여 성공적으로 적응적 선택 암호문 공격을 할 수 있는 예를 보이는 것이다.

Abstract Provable security has widely been used to prove a cryptosystem's security formally in crpytography. In this paper, we analyze the Cramer-Shoup public key cryptosystem that has been known to be provable secure against adaptive chosen ciphertext attack and argue that its security proof is not complete in the generic sense of adaptive chosen ciphertext attack. Future research should be directed toward two directions: one is to make the security proof complete even against generic sense of adaptive chosen ciphertext attack, and another is to try finding counterexamples of successful adaptive chosen ciphertext attack on the Cramer-Shoup cryptosystem.

Key Words : provable security, reduction, public key cryptosystem

Ⅰ. Introduction

In cryptography, we say that a cryptographic system has provable security in an adversarial model, if one can formally state its security notions one wants the cryptosystem to achieve and show that these notions can be satisfied in the advaersarial model. Along with the adversarial model, we usually also assume that there exist some computationally intractable problems. To prove that a cryptosystem is secure against attackers with polynomially bounded computation capability, we usually use reduction + proof by contradiction technique [1].

Reduction refers to tranforming the tasking of solving one problem Π_1 to the task of solving another problem Π_2, which is denoted as "Π_1 is reducible to Π_2". When Π_1 is reducible to Π_2, it means that an algorithm solving the second task can be used in order to construct an algorithm that solves the first task.

In cryptography, Π_1 is usually a mathematical problem such as the discrete logarithm problem (given g and g^x, compute x) that are assumed to be difficult to solve, and Π_2 is a successful attack on the cryptosystem whose security we are going to prove. To prove Π_2 is secure against some specified attack, one reduces attacks (that is, efficient algorithms) which

*정회원, 홍익대학교 컴퓨터정보통신공학과 교수

접수일자 2008.10.1, 수정완료 2008.12.5

are assumed to be successful on the target cryptosystem, into efficient algorithms that contradict one of the known computational assumptions. Hence we conclude that the cryptosystem must provably secure against the above specified attack.

In 1998, Cramer and Shoup [2] proposed a new public key cryptosystem, the so-called Cramer-Shoup cryptosystem hereafter. The Cramer-Shoup cryptosystem was welcomed by the cryptographic community because (1) it was provably secure against adaptive chosen ciphertext attack, and (2) its proof security relies only on weaker assumptions, namely, decisonal Diffie-Hellman assumption and existence of universal one-way hash function, rather than strong assumptions such as random oracle model [3-5] and ideal cipher model [6].

In this paper, we analyze the Cramer-Shoup cryptosystem and discuss some missing points in its security proof.

II. Preliminaries

2.1 Negligible and Non-negligible

Definition 1 (Negligible). A function $f : N \rightarrow R$ is negligible if for every positive polynomial $p(\cdot)$ there exists an N such that for all $n > N$, $f(n) < 1/p(n)$.

The above definition considers the success probability of an algorithm to be negligible if as a function of input length the success probability is bounded by any polynomial fraction. Note that repeating the algorithm polynomially many times yields a new algorithm that also has a negligible success probability. An event that occurs with negligible probability would be highly unlikely to occur even if we repeated the experiment polynomially many times.

Definition 2 (Non-negligible). A function $f : N \rightarrow R$ is non-negligible if there exists a polynomial $p(\cdot)$ such that for all sufficiently large n's, it holds that $f(n) > 1/p(n)$.

An event that occurs with non-negligible probability would be highly likely to occur with probability closer to 1 if we repeated the experiment polynomially many times.

2.2 Computational Assumptions

In modern cryptography, many security notions can not be unconditionally guaranteed. They are based on complexity-theoretic model: security of a cryptosystem is conditional on various computational assumptions that certain problems are intractable. Before stating the security proof of the Cramer-Shoup cryptosystem, we describe related computational assumptions.

Definition 3 (Decisional Diffie-Hellman Assumption). Let G be a group of large prime order q, and consider the following two distributions: the distribution R of random quadruples $(g_1, g_2, u_1, u_2) \in G^4$; the distribution D of random quadruples $(g_1, g_2, u_1, u_2) \in G^4$, where g_1, g_2 are random, and $u_1 = g_1^r$ and $u_2 = g_2^r$ for random $r \in Z_q$. Given a quadruple coming from one of the two distributions, there is no polynomial-time distinguisher with a non-negligigle probability that determines whether the input comes from R or D.

Definition 4 (Universal One-way Hash Functions). A family of hash functions is said to be universal one-way [7] if it is infeasible for an attacker to choose an input x, draw a random hash function H, and then find a different input y such that $H(x) = H(y)$.

2.3 Indistinguishability Security from Adaptive Chosen Ciphertext Attack

An adaptive chosen ciphertext attack is an interactive form of attack in which an attacker sends a number of ciphertexts to be decrpted, then uses the results of these decryptions to select subsequent ciphertexts. It is known that the adaptive chosen ciphertext attack are generally applicable only when they have the property of ciphertext malleability - that is, a ciphertext can be modified in specific ways that will have a predictable effect on the decryption of that message.

Here we describe adaptive chosen ciphertext attack scenario from Rackoff and Simon [8]. First, the key generation algorithm generates the public key and private key for the cryptosystem. The attacker obtains the public key, but not the private key. The attacker makes a series of queries to a decryption oracle. The query is a ciphertext constructed in an arbitrary way by the attacker. The descryption oracle gives the resulting decryption to the attacker. Next, the attacker prepares two messages m_0, m_1 and give these to an encryption oracle.

The encryption oracle chooses $b \in \{0,1\}$ at random, encrypts m_b, and gives the resulting target ciphertext $c*$ to the attacker. After receiving the target ciphertext, the attacker continues to query c to the description oracle, subject only to the restriction that $c \neq c*$. At the end of the game, the attacker outputs its guessing value $b' \in \{0,1\}$. This completes the description of the attack scenario.

The attacker's advantage in this attack scenario is defined to be $|Pr[b' = b]-1/2|$. The cryptosystem is said to be secure against adaptive chosen ciphertext attack if for any efficient attacker, its advantage is negligible.

Ⅲ. Review of the Cramer-Shoup Cryptosystem

3.1 The Cramer-Shoup Cryptosystem

We assume that we have a group G of prime order q, where q is large. We also assume that plaintext messages are elements of G. We also use a universal one-way family of hash functions that map long bit strings to elements of Z_q.

Key Generation: The key generation algorithm runs as follows. Random elements $g_1, g_2 \in G$ are chosen, and random elements $x_1, x_2, y_1, y_2, z \in Z_q$ are also chosen. Next, the group elements $c = g_1^{x1}g_2^{x2}$, $d = g_1^{y1}g_2^{y2}$, $h= g_1^{z}$ are computed. Next, a hash function H is chosen from the family of universal one-way hash functions. The public key is (g_1, g_2, c, d, h, H), and the private key is (x_1, x_2, y_1, y_2, z).

Encryption: Given a message $m \in G$, the encryption algorithm runs as follows. First, it chooses $r \in Z_q$ at random. Then it computes $u_1 = g_1^r$, $u_2 = g_2^r$, $e = h^r m$, $\alpha = H(u_1, u_2, e)$, $v = c^r d^{r\alpha}$. The ciphertext is (u_1, u_2, e, v).

Decryption: Given a ciphertext (u_1, u_2, e, v), the decryption algorithm runs as follows. It first computes $\alpha = H(u_1, u_2, e)$, and tests if $u_1^{x1+y1\alpha}u_2^{x2+y2\alpha} = v$. If this condition does not hold, the decryption algorithm outputs "reject"; otherwise it outputs $m = e/u_1^z$.

3.2 Security Proof of the Cramer-Shoup Cryptosystem

A high-level description for the security proof is as follows. We suppose that there exist an attacker who can break the Cramer-Shoup cryptosystem in the adaptive chosen ciphertext attack with a non-negligible advantage. Then we shall construct an efficient reduction algorithm to enable the simulator to answer a Decisional Diffie-Hellman (DDH) question, which contradicts the DDH assumption. The reduction algorithm involves the following stages.

Stage 1: On input $(g_1, g_2, u_1, u_2) \in G^4$, the simulator picks six random values $x_1, x_2, y_1, y_2, z_1, z_2 \in Z_q$ and computes $c = g_1^{x1}g_2^{x2}$, $d = g_1^{y1}g_2^{y2}$, $h = g_1^{z1}g_2^{z2}$. He then chooses a cryptographic hash function H and sends the public key (g_1, g_2, c, d, h, H) to the attacker. The private key for the simulator to use is $(x_1, x_2, y_1, y_2, z_1, z_2)$.

Stage 2: The attacker makes decryption queries $c = (u_1, u_2, e, v)$ to the simulator. The simulator computes $\alpha = H(u_1, u_2, e)$ and returns $m = e/u_1^{z1}u_2^{z2}$ to the attacker if $u_1^{x1+y1\alpha}u_2^{x2+y2\alpha} = v$. Otherwise, the simulator returns "reject" to the attacker. (Pre-challenge cryptanalysis phase)

Stage 3: The simulator receives from the attacker a pair of chosen plaintext m_0, m_1, flips a fair coin $b \in_U$

{0,1}, and encrypts m_b as follows: $e = u_1^{z1}u_2^{z2}m_b$, $\alpha = H(u_1, u_2, e)$, $v = u_1^{x1+y1\alpha}u_2^{x2+y2\alpha}$. The challenge ciphertext $c* = (u_1, u_2, e, v)$ is sent to the attacker.

Stage 4: The attacker continues the same stage 2 with the simulator. (Post-challenge cryptanalysis phase)

Stage 5: The attacker decides b′, that is, whether c* is the encryption of m_0 or m_1, and sends the bit b′ to the simulator. The distinguisher runs the simulator and the attacker together. Based upon b′, the distinguisher answers the question whether $(g_1, g_2, u_1, u_2) \in D$ or $(g_1, g_2, u_1, u_2) \notin D$ by outputing "yes" if the attacker's guessing bit b′ is equal to b, "no" otherwise.

If the quadruple comes from D, the simulation will be nearly perfect in quality because the joint distribution of the attacker's view and the hidden bit b in the simulated attack is statistically indistinguishable from that in the actual attack (by Lemma 1 [2]). Lemma 1 [2] implies in part that the attacker cannot discern the simulation from a real attack. Both the quality of the simulation and the assumption that the attacker can break the Cramer-Shoup cryptosystem with a non-negligible advantage mean that the attacker has a non-negligible advantage in guessing the hidden bit b. Therefore, the probability that the distinghisher will correctly determine is significantly greater than 1/2.

If the quadruple comes from R, $e = \varepsilon m_b$ where $\varepsilon = u_1^{z1}u_2^{z2}$, would be a perfect one-time pad. That is, no information is leaked during the decryption on the above stage 2. From the fact that the distribution of the hidden bit b is (essentially) independent from the attacker's view (by Lemma 2 [2]), the probability that the distinguisher will correctly determine is only 1/2.

Ⅳ. Discussion of the Cramer-Shoup Cryptosystem Security Proof

Claim 1: The security proof of the Cramer-Shoup cryptosystem [2] is not complete against the adaptive chosen ciphertext attack in the generic sense.

Note that $x_1, x_2, y_1, y_2, z_1, z_2$ is not fixed in the above security proof [2]. If they are fixed during the attack game, the reduction algorithm does not work. If they are fixed, all the resulting ciphertexts will be the same in the parts u_1, u_2 which will allow the attacker to discern the simulation from a real attack. However, we note that this case is more probable in real attack situation: the attacker makes encryption/decryption queries to find out the plaintext message or key corresponding to the target ciphertext under some specified public key.

The above security proof does not reflect this kind of attack situation. It only applies to a form of adaptive chosen ciphertext attack, too restricted and artificial, requiring the change of public/private key during the attack game.

Claim 2: Even in the adaptive chosen ciphertext attack in the restricted sense, the security proof of the Cramer-Shoup cryptosystem does not guarantee the security on all instances of D.

We note that reduction here is different from standard (worst-case complexity) reductions. The attacker can only successfully attack the Cramer-Shoup cryptosystem on instances with certain probability with respect to a certain distribution of D, not on all instances.

Claim 3: Even in the adaptive chosen ciphertext attack in the restricted sense, the probability that the distinguisher makes an decision error may be high depending on the instances of D.

In order to decide whether or not the quadruple comes from D, the simulator will run this simulated attack several times with different x_1, x_2, y_1, y_2, z_1, z_2. If the attacker correctly determines b significantly more than half the time, the simulator is almost certain that the quadruple has the Diffie-Hellman property. Otherwise, he is almost certain that it doesn't.

During the attack game with the simulator, the values of x_1, x_2, y_1, y_2, z_1, z_2 are randomly selected by the simulator. Therefore, the attacker makes encryption and decryption queries for his chosen message under the corresponding pubic key which was generated by the simulator and used one time per query. However, even though the simulator runs the simulated attack game several times with different x_1, x_2, y_1, y_2, z_1, z_2, the probability the attacker correctly determines b remains the same as certain probability with respect to a certain distribution of D. In other words, the attacker cannot improve his guessing capability by repeating the game. Remember that the reduction algorithm intended to translate the attacker's capability to attack the cryptosystem to its capability to distinguish whether or not a given quadruple is in D. Therefore, the simulator (and accordingly distinguisher) cannot exploit the attacker's capability to attack the Cramer-Shoup cryptosystem to distinguish whether or not a given quadruple is in D.

The proof [2] depends on the precision level of the attacker's guessing, which may not establish a high degree of confidence. Therefore we conclude that though the attacker may have a non-negligible advantage in guessing the hidden bit b, the probability that the distinguisher makes an decision error may be close up to 1/2 on the worst case.

V. Conclusion

The result of this paper is that the Cramer-Shoup security proof is not complete against the adaptive chosen ciphertext attack in the generic sense. Future research should be directed toward two directions: one is to make the security proof complete even against generic sense of adaptive chosen ciphertext attack, and another is to try finding counterexamples of successful adaptive chosen ciphertext attack on the Cramer-Shoup cryptosystem.

참 고 문 헌

[1] Bellare, M.: Practice-Oriented Provable Security. Information Security Workshop '97 (1997).

[2] Cramer, R. and Shoup, V.: A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack. Advances in Cryptology - Crypto '98 (1998) 13-25.

[3] Fiat, A. and Shamir, A.: How to Prove Yourself: Practical Solutions of Identification and Signature Problems. Advances in Cryptology - Crypto '86 (1987) 186-194.

[4] Bellare, M. and Rogaway, P.: Random oracles are practical: a paradigm for designing efficient protocols. First ACM Conference on Computer and Communications Security (1993) 62-73.

[5] Bellare, M. and Rogaway, P.: Optimal asymmetric encryption. Advances in Cryptology - Eurocrypt '94 (1994) 92-111.

[6] Bellare, M., Pointcheval, D. and Rogaway, P.: Authenticated Key Exchange Secure Against Dictionary Attacks. Advances in Cryptology - Eurocrypt '00 (2000) 139-155.

[7] Naor, M. and Yung, M.: Universal one-way hash functions and their cryptographic applications. 21st Annual ACM Symposium on Theory of Computing (1989).

[8] Rackoff C., Simon, D.: Noninteractive zero-knowledge proof of knowledge and chosen ciphertext attack. Advances in Cryptology - Crypto '91 (1991) 433-444.

저자 소개

황 성 운(정회원)

- 1993년 서울대학교 수학과 학사 졸업
- 1998년 포항공과대학교 정보통신학과 석사 졸업
- 2004년 한국과학기술원 전자전산학과 박사 졸업
- 2008년 현재 홍익대학교 컴퓨터정보통신공학과 교수

<주관심분야: 정보보호, 계산이론>