JOURNAL OF INFORMATION SCIENCE AND ENGINEERING 18, 19-22 (2002)

On the Security of a Variation of Cramer-Shoup's Public Key Scheme

HUNG-MIN SUN
Department of Computer Science and Information Engineering
National Cheng Kung University
Tainan, 701 Taiwan
E-mail: hmsun@mail.ncku.edu.tw

In this paper, we show that a recently proposed variation of Cramer-Shoup's public key scheme is insecure against the *adaptive chosen ciphertext attack*. Moreover, we showed that the proposed scheme doesn't satisfy the *non-malleability* property, even under the weakest attack model — the *chosen plaintext attack*.

Keywords: cryptology, security, public-key cryptosystem, encryption, cryptanalysis

1. INTRODUCTION

At Crypto'98, Cramer and Shoup [1] proposed a public key cryptosystem that is provably secure against the *adaptive chosen ciphertext attacks*. Recently, Zhu, Chan, and Deng [2] proposed a variation of Cramer and Shoup's scheme (the Zhu-Chan-Deng scheme in short) which attempts to reduce Cramer and Shoup's public key cryptosystem in terms of both the size of the ciphertext and the computation required for decryption. However, in this paper, we show that the Zhu-Chan-Deng scheme is insecure against the *adaptive chosen ciphertext attacks*. Moreover, we also show that the Zhu-Chan-Deng scheme doesn't exhibit the *non-malleability* property, even under the weakest attack model — the *chosen plaintext attack*.

2. NOTATIONS OF ENCRYPTION SCHEME SECURITY

In the following, we first introduce security in public-key encryption. The notions involved were recently organized by Bellare, Desai, Pointcheval, and Rogaway [3].

Various notions of security for public key encryption were proposed in the past so as to evaluate the strength of a public key cryptosystem. Bellare, Desai, Pointcheval, and Rogaway [3] organized definitions of secure encryption by considering separately various possible *goals* and various possible *attack models*, and by then obtaining each definition as a pair consisting of a particular goal and a particular attack model. They considered two different goals: *indistinguishability* of *encryptions*, due to Goldwasser and Micali [4], and *non-malleability* (NM), due to Dolev, Dwork and Naor [5]. In-

Received March 1, 2000; accepted July 13, 2000.
Communicated by Hsu-Chun Yen.

distinguishability (IND) formalizes an adversary's inability to learn any information about the plaintext *m* underlying a challenge ciphertext. This captures a strong notion of privacy. Non-malleability (NM) formalizes an adversary's inability, given a challenge ciphertext *c*, to get a different ciphertext *c'* such that the corresponding plaintexts *m* and *m'* are *meaningfully related*, e.g. *m'* = 2*m*. This captures a sense in which ciphertexts can be tamper-proof. They considered three different attack models: *chosen plaintext attack* (CPA), *non-adaptive chosen ciphertext attack* (CCA1) due to Naor and Yung [6], and *adaptive chosen ciphertext attack* (CCA2) due to Rackoff and Simon [7]. Under CPA, the adversary is given the public-key and is able to obtain ciphertexts of plaintexts of his choice. Under CCA1, the adversary is given the public-key and is able to get access to an oracle for the decryption function before the challenge ciphertext *c* is given. Under CCA2, the adversary is given the public-key and is able to get access to an oracle for the decryption function at any time. By mixing and matching the goals {IND, NM} and the attack models {CPA, CCA1, CCA2} in any combination, six notions of security can be obtained. These are IND-CPA, IND-CCA1, IND-CCA2, NM-CPA, NM-CCA1, and NM-CCA2. In Fig. 1, we show the relations among these notions of security according to [3]. Note that for *A*, *B* ∈ {IND-CPA, IND-CCA1, IND-CCA2, NM-CPA, NM-CCA1, NM-CCA2} "A→B" denotes that an encryption scheme that is secure in the sense of *A* is also secure in the sense of *B*. This also implies that an encryption scheme that is insecure in the sense of *B* is also insecure in the sense of *A*.

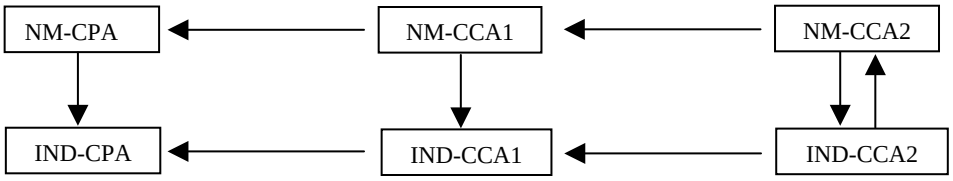

Fig. 1. The relations among the notions of security.

Note that from Fig. 1, we understand that the strongest security notions in public-key encryption are NM-CCA2 and IND-CCA2, which have been shown to be equivalent in [3].

3. REVIEW OF THE ZHU-CHAN-DENG SCHEME

Let p be a large prime such that its discrete logarithm is intractable, and let g be a primitive element in Z_p. Let $h(\ )$ be a hash function chosen from the family of universal one-way hash functions. Each user has a secret key pair (x, y), where $x, y \in_R Z_{p-1}$, and a public key pair (w_1, w_2), where $w_1 = g^x \pmod p$ and $w_2 = g^y \pmod p$. Let $m \in Z_p$ be the message to be encrypted. The sender randomly chooses $r \in_R Z_{p-1}$ and computes $u = g^r \pmod p$, $v = m w_1^r \pmod p$, $\alpha = h(u, v)$, and $\beta = w_1^{\alpha} w_2^r \pmod p$. The ciphertext is (u, v, β).

Given a ciphertext (u, v, β), the decryption algorithm is executed by a legal user who owns (x, y) as follows:

First he computes $\alpha = h(u, v)$ and then verifies whether $\beta \stackrel{?}{=} w_1^{\alpha} u^{y} \pmod{p}$. If it holds, then the decryption algorithm outputs 'reject'; otherwise, it outputs $m = vu^{-x} \pmod{p}$. Note that a ciphertext is valid if $\beta = w_1^{\alpha} u^{y} \pmod{p}$ because $w_1^{\alpha} u^{y} = w_1^{\alpha} g^{ry} = w_1^{\alpha} (g^{y})^{r} = w_1^{\alpha} w_2^{r} = \beta \pmod{p}$. It is clear that $m = vu^{-x} \pmod{p}$ because $vu^{-x} = mw_1^{r} (g^{r})^{-x} = mw_1^{r} (g^{x})^{-r} = mw_1^{r} w_1^{-r} = m \pmod{p}$.

4. SECURITY ANALYSIS OF THE ZHU-CHAN-DENG SCHEME

Theorem 1: The Zhu-Chan-Deng scheme is insecure in the sense of NM-CPA.

Proof: We assume that an adversary knows only the public key of the legal receiver. Given a challenge ciphertext (u, v, β), an adversary can easily to make a different ciphertext (u', v', β') such that the corresponding plaintext m and m' have a meaningful relation: $m' = cm$, where c is an arbitrary constant in Z_p. Such a ciphertext (u', v', β') is made by $u' = u$, $v' = cv \pmod{p}$ and $\beta' = \beta \cdot w_1^{-\alpha} w_1^{\alpha'} \pmod{p}$, where $\alpha = h(u, v)$ and $\alpha' = h(u', v')$. The ciphertext will be valid because the verification of $\beta' \stackrel{?}{=} w_1^{\alpha'} u'^{y} \pmod{p}$ is correct. Its correctness can be examined as follows:

$w_1^{\alpha'} u'^{y} = w_1^{\alpha'} u^{y} = w_1^{\alpha} u^{y} w_1^{-\alpha} w_1^{\alpha'} = \beta \cdot w_1^{-\alpha} w_1^{\alpha'} = \beta' \pmod{p}$. On the other hand, the corresponding plaintext m' is exactly equal to cm because $v' u'^{-x} = c\, vu^{-x} = c\, mw_1^{r} (g^{r})^{-x} = c\, mw_1^{r} (g^{x})^{-r} = c\, mw_1^{r} w_1^{-r} = cm \pmod{p} = m'$. Therefore, the Zhu-Chan-Deng scheme is insecure in the sense of NM-CPA. ❑

Theorem 2: The Zhu-Chan-Deng scheme is insecure in the sense of NM-CCA1, NM-CCA2, and IND-CCA2.

Proof: From Fig. 1, we know that NM-CCA1 → NM-CPA. From Theorem 1, we know that the Zhu-Chan-Deng scheme is insecure in the sense of NM-CPA. Therefore, the Zhu-Chan-Deng scheme is also insecure in the sense of NM-CCA1. Similarly, from Fig. 1, we know that NM-CCA2 → NM-CCA1 and IND-CCA2 → NM-CCA2. Therefore, the Zhu-Chan-Deng scheme is also insecure in the sense of NM-CCA2 and IND-CCA2. ❑

5. CONCLUSIONS

In Cramer and Shoup's paper, they showed that their scheme is secure in the sense of NM-CCA2. (It is natural that their scheme is also secure in the sense of IND-CCA2 because both NM-CCA2 and IND-CCA2 are equivalent.) For the Zhu-Chan-Deng scheme, we have shown that it is insecure in the sense of NM-CCA2 and IND-CCA2. That is, the Zhu-Chan-Deng scheme is insecure against the adaptive chosen ciphertext attack. Moreover, we have shown that the Zhu-Chan-Deng scheme is insecure in the sense of NM-CPA, NM-CCA1, and NM-CCA2. Therefore, the Zhu-Chan-Deng

scheme does not exhibit the *non-malleability* property, even under the weakest attack model — the chosen plaintext attack.

ACKNOWLEDGMENTS

This work was supported in part by the National Science Council, Taiwan, under contract NSC-89-2213-E-006-118. We are grateful to anonymous reviewers for their valuable comments.

REFERENCES

1. R. Cramer and V. Shoup, "A practical public key cryptosystem provable secure against adaptive chosen ciphertext attack," *Advances in Cryptology-CRYPTO'98*, LNCS, Vol. 1462, Springer-Verlag, 1998, pp. 13-25.
2. H. Zhu, L. Chan, and X. Deng, "Variation of cramer-shoup public key scheme," *Electronics Letters*, Vol. 35, 1999, pp. 1150.
3. M. Bellare, A. Desai, D. Pointcheval, and P. Rogaway, "Relations among notions of security for public-key encryption schemes," *Advances in Cryptology-CRYPTO'98*, LNCS, Vol. 1462, Springer-Verlag, 1998, pp. 26-45.
4. S. Goldwasser and S. Micali, "Probabilistic encryption," *Journal of Computer and System Science*, Vol. 28, 1984, pp. 270-199.
5. D. Dolev, C. Dwork, and M. Naor, "Non-malleable cryptography," in *Proceedings of the 23rd Annual Symposium on Theory of Computing, ACM*, 1991, pp. 542-552.
6. M. Naor and M. Yung, "Public-key cryptosystems provably secure against chosen ciphertext attacks," in *Proceedings of the 22nd Annual Symposium on Theory of Computing, ACM*, 1990, pp. 427-437.
7. C. Rackoff and D. Simon, "Non-interactive zero-knowledge proof of knowledge and chosen ciphertext attack," *Advances in Cryptology-CRYPTO'91*, LNCS, Vol. 576, Springer-Verlag, 1992, pp. 433-441.

Hung-Min Sun (孫宏民) received his B.S. degree in applied mathematics from National Chung-Hsing University in 1988, his M.S. degree in applied mathematics from National Cheng-Kung University in 1990, and his Ph.D. degree in computer science and information engineering from National Chiao-Tung University in 1995, respectively. He was an associate professor with the Department of Information Management, Chaoyang University of Technology from 1995 to 1999. Currently he is teaching at the Department of Computer Science and Information Engineering, National Cheng Kung University. His research interests include cryptography, information theory, network security, reliability, distributed systems.