TamKang University
Department of Electrical Engineering
Laboratory of Cryptography and Information Security

Technical Report

TR-98-8B

Two Protocol Attacks on Okamoto and Uchiyama's Cryptosystem

Marc Joye · Jean-Jacques Quisquater · Sung-Ming Yen

July 1, 1998

Two Protocol Attacks on Okamoto and Uchiyama's Cryptosystem

Marc Joye[1),*] Jean-Jacques Quisquater[2)] Sung-Ming Yen[1)]

July 1, 1998

[1)] Dept of Electrical Engineering, Tamkang University
Tamsui, Taipei Hsien, Taiwan 25137, R.O.C.
Email: {joye,yensm}@ee.tku.edu.tw

[2)] UCL Crypto Group, Dép. d'Électricité, Université de Louvain
Place du Levant 3, B-1348 Louvain-la-Neuve, Belgium
Email: jjq@dice.ucl.ac.be

Abstract. In 1995, Shamir proposed a variant of the RSA cryptosystem in which one the two secret primes is much larger than the other one. Some "attacks" were subsequently reported by Gilbert, Gupta, Odlyzko and Quisquater. In this report, we show that the cryptosystem recently proposed by Okamoto and Uchiyama (1998) is subject to similar attacks.

Indexing terms: Public-key cryptography, Protocol attacks, Protocol failures, p-Subgroup problem, Shamir's RSA for paranoids

1 Introduction

In 1995, Shamir introduced the so-called *RSA for paranoids* [6]. This is a variant of the RSA cryptosystem in which one the two secret primes is much larger than the other one. Some "attacks" were subsequently reported in [3]. In this report, we show that the cryptosystem proposed by Okamoto and Uchiyama [4] is subject to similar attacks.

The first attack is a *chosen-ciphertext attack*. Although aware of the existence of such an attack, Okamoto and Uchiyama do not give details how to precisely mount it.

Note that this first attack does *not* break Okamoto and Uchiyama's cryptosystem. It simply means that special care must be taken in the implementation of their system. In particular, appropriate redundancy has to

*Supported by the National Science Council of the Republic of China under contract NSC87-2811-E-032-0001.

TR-98-8B

be added to the messages prior to encryption. Nevertheless, as in [3], this attack enables to exhibit a second attack which is more insidious. If a user behaves differently depending on the message he receives, we can get one bit of his secret key. Further probes finally reveal the whole secret key.

2 Cryptosystem of Okamoto and Uchiyama

This section briefly reviews the cryptosystem of Okamoto and Uchiyama. We refer to the original paper [4] for a complete description.

System setup Each user selects two large k-bit primes p and q, and computes $n = p^2 q$. He also chooses $g \in (\mathbb{Z}/n\mathbb{Z})^*$ such that $g_p = g^{p-1} \bmod p^2$ has order p. The public parameters are n, g and k. The secret parameters are p and q.

Encryption A message m $(0 < m < 2^{k-1})$ is encrypted as

$$C = g^{m+rn} \bmod n, \tag{1}$$

where r is randomly chosen in $\mathbb{Z}/n\mathbb{Z}$.

Decryption Given the ciphertext C, message m is recovered from $C_p = C^{p-1} \bmod p^2$ by computing

$$m = \frac{L(C_p)}{L(g_p)} \bmod p, \tag{2}$$

where L denotes a logarithmic function over the p-Sylow subgroup of $(\mathbb{Z}/p^2\mathbb{Z})^*$.

3 Two Protocol Attacks

As in Shamir's RSA for paranoids, Okamoto and Uchiyama's cryptosystem supposes that the message to be encrypted is smaller than a given value. So, an attacker may discover the secret factorization of n by enciphering a larger message.

3.1 First attack

The first attack supposes that the attacker obtains the decryption corresponding to a *chosen* ciphertext. One can imagine that the user sends the message back to the attacker because it is meaningless or that the attacker can get access to the "user's bin" as in Davida's attack [1] (see also [2]).

The attacker first chooses a message $m' \geq 2^k$ (and thus $m' > p$). Next, he encrypts message m' according to Eq. (1). Let C' denote the corresponding ciphertext. When the user decrypts C', he obtains

$$\frac{L(C'^{p-1} \bmod p^2)}{L(g_p)} \bmod p = m' \bmod p \ . \tag{3}$$

Therefore, from $m' \bmod p$, the attacker finds the secret parameter p by evaluating

$$\gcd(m' - (m' \bmod p), n) \ . \tag{4}$$

Proof. Defining $m = m' \bmod p$, we can write $m' = \alpha p + m$ with $\alpha = \lfloor m'/p \rfloor > 0$. So, $\gcd(m' - (m' \bmod p), n) = \gcd(m' - m, n) = \gcd(\alpha p, p^2 q)$ gives p. □

Furthermore, replacing the attacker by an oracle, we can prove:

Corollary 1. *Completely breaking Okamoto and Uchiyama's cryptosystem is equivalent to factoring $n = p^2 q$.*

Proof. ($\Leftarrow$) Trivial.
($\Rightarrow$) Suppose that there exists a polynomial-time algorithm `Oracle` that can decrypt ciphertexts, i.e. given a ciphertext C, `Oracle` gives the cleartext $m =$ `Oracle`(C). We can therefore construct the following factorization algorithm:

1. Select a random message $m' \geq 2^k$ (and thus $m' > p$).
2. Encrypt m' to get the ciphertext C'.
3. Call the `Oracle` algorithm with input C'. The output is $(m' \bmod p)$.
4. Find the factor p by computing $\gcd(m' - (m' \bmod p), n)$. Hence $q = n/p^2$. □

Note that this result is not as general as the one presented in the original paper of Okamoto and Uchiyama. They proved that breaking their cryptosystem is equivalent to factoring whereas we actually just prove that *completely* breaking it is equivalent to factoring. More precisely, Okamoto and Uchiyama proved that, under the factoring intractability assumption, no adversary can break their system with *any* non-negligible probability. Corollary 1 only guarantees that, under the factoring intractability assumption, no adversary can break Okamoto and Uchiyama's cryptosystem with probability 1.

3.2 Second attack

Assume now that the attacker does *not* get access to $m' \bmod p$. As before, he encrypts a message m' to get the ciphertext C'. Suppose that the user "accepts" the message sent by the attacker. This means that he was able to decrypt C'; therefore the attacker knows that $p > m'$. If the user says that he cannot decrypt the message, then the attacker knows that $p < m'$. Further probes will finally reveal the secret value of p.

At first sight, this second attack seems unrealistic. However, as remarked in [3], one can imagine that message m' is the attacker's signature on a message promising a certain amount of money. The user will then be tempted to receive the money. Another realistic scenario (also in [3]) might be the use of Okamoto and Uchiyama's cryptosystem for session key exchange: the attack then just consists to test whether or not the user is able to encrypt session messages with m'.

4 Conclusions

This report exhibited some weaknesses in Okamoto and Uchiyama's cryptosystem. This does not mean that we are not confident in their cryptosystem. We just want to warn the reader that this system must be carefully implemented and properly used.

Acknowledgments

We acknowledge Tatsuaki Okamoto for sending us a preprint of [4]. More importantly, we gratefully acknowledge him for pointing out corrections to an earlier version of this report.

References

[1] G. Davida: Chosen signature cryptanalysis of the RSA (MIT) public key cryptosystem. Tech. Report TR-CS-82-2, Dept. of Electrical Engineering and Computer Science, University of Wisconsin, Milwaukee, USA, Oct. 1982.

[2] Y.G. Desmedt and A.M. Odlyzko: A chosen text attack on the RSA cryptosystem and some discrete logarithm schemes. In *Advances in Cryptology — CRYPTO '85*, LNCS 218, Springer-Verlag, pp. 516–522, 1986.

[3] H. Gilbert, D. Gupta, A.M. Odlyzko, and J.-J. Quisquater: Attacks on Shamir's 'RSA for paranoids'. Preprint (December 26, 1997).
Available at URL `<http://www.att.research.com/~amo/doc/crypto.html>`.

[4] T. Okamoto and S. Uchiyama: A new public-key cryptosystem as secure as factoring. To appear in *Advances in Cryptology — EUROCRYPT '98*, LNCS, Springer-Verlag, 1998.

[5] M.O. Rabin: Digitalized signatures and public-key functions as intractable as factorization. Tech. Report MIT/LCS/TR-212, MIT Laboratory for Computer Science, Jan. 1979.

[6] A. Shamir: RSA for paranoids. *CryptoBytes* **1** (1995), no. 2, pp. 1–4, 1995.