Applied Mathematical Sciences, Vol. 2, 2008, no. 16, 787 - 791

Cryptanalysis on Chen-Qiu-Zheng Blind Signature Scheme[1][2][3]

Chun-I Fan

Department of Computer Science and Engineering
National Sun Yat-sen University
Kaohsiung, Taiwan
cifan@faculty.nsysu.edu.tw

Lin-Chuan Wu

Department of Computer Science and Information Engineering
Chung Hua University
Hsinchu, Taiwan
lcwu@chu.edu.tw

Vincent Shi-Ming Huang

Department of Computer Science and Engineering
National Sun Yat-sen University
Kaohsiung, Taiwan
kayeaco@gmail.com

Abstract

Chen, Qiu, and Zheng proposed a Rabin-like blind signature scheme, which is based on the square-root problem. Although their scheme is simple and efficient, it can be compromised when choosing some particular blinding factors. In this manuscript, the scheme is demonstrated as not being secure.

Keywords: Blind Signatures, Security, Privacy, Cryptology

[1] This work was supported in part by the National Science Council of the ROC (Taiwan) under grant NSC96-2219-E-110-002 and NSC96-2221-E-110-071-MY3.

[2] This research was also partially supported by TWISC@NCKU, National Science Council of the ROC (Taiwan) under grant NSC96-2219-E-006-009.

[3] A preliminary version of this paper was presented at National Information Security Conference 2002, Taichung, Taiwan.

1 Introduction

Rabin's digital signature scheme [1] is based on the square-root problem. Its security is relying on the difficulty of finding the square roots of a quadratic residue under a modulus n and it has been proved to be as hard as factoring n [1]. Compared with the RSA signature scheme [2], the signature verification only requires one modular multiplication. The idea of blind signatures was first proposed by Chaum in 1982 [3]. The scheme is based on the RSA cryptosystem [2]. In addition to the unforgeability of the signatures, it satisfies two requirements: the contents of messages are unknown to the signer when signing and the signer cannot trace the signed messages after the senders have revealed the signatures publicly. Due to the unlinkability property, blind signatures can protect the senders' privacy in electronic transactions and they have been applied to anonymous electronic voting and untraceable electronic cash systems [3]. In 2001, Chen, Qiu, and Zheng also proposed an efficient blind signature scheme [4] based on Rabin's scheme of [1]. In this manuscript we propose an attack on the Rabin-like blind signature scheme of [4] and show that their scheme can be compromised if the senders select some particular blinding factors.

2 Preliminary

In this section we review related mathematical foundations and define some notations used in the manuscript. Let $\mathbb{Z}_n^* = \{k \in \mathbb{Z}_n | GCD(k,n) = 1\}$ be the multiplicative group under modulus n where n is a positive integer. An integer a is called a quadratic residue (QR) in $\mathbb{Z}_n^*$ if there exists an integer $x \in \mathbb{Z}_n^*$ such that $x^2 \equiv_n a$. If no such x exists, a is called a quadratic non-residue (QNR) in $\mathbb{Z}_n^*$. The set of all quadratic residues under modulus n is denoted by $\mathbb{Q}_n$ and the set of all quadratic non-residues under modulus n is denoted by $\overline{\mathbb{Q}_n}$. That is,

$$\mathbb{Q}_n = \{a \in \mathbb{Z}_n^* | \exists x \in \mathbb{Z}_n^*, x^2 \equiv_n a\} \tag{1}$$

and

$$\overline{\mathbb{Q}_n} = \mathbb{Z}_n^* - \mathbb{Q}_n \tag{2}$$

Let p be an odd prime and a be an integer. The Legendre symbol $\left(\frac{a}{p}\right)$ is defined below.

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{if } p|a \\ 1, & \text{if } a \in \mathbb{Q}_p \\ -1, & \text{if } a \in \overline{\mathbb{Q}_p} \end{cases} \tag{3}$$

Let n be a product of two distinct odd primes p and q, i.e., $n = pq$. An integer $a \in \mathbb{Z}_n^*$ is a quadratic residue under modulus n if and only if $a \in \mathbb{Q}_p$ and $a \in \mathbb{Q}_q$. Let $n \geq 3$ be an odd integer with prime factorization $n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$ and let a be an integer. The Jacobi symbol is defined below.

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{e_1} \left(\frac{a}{p_2}\right)^{e_2} \cdots \left(\frac{a}{p_k}\right)^{e_k} \tag{4}$$

Thus, the Jacobi symbol is a generalization of the Legendre symbol where n is not necessarily to be prime. Let $n \geq 3$ be an odd integer and $J_n = \left\{a \in \mathbb{Z}_n^* | \left(\frac{a}{n}\right) = 1\right\}$. $\tilde{\mathbb{Q}}_n = J_n - \mathbb{Q}_n$ is defined to be the set of pseudo-squares under modulus n. In addition, let $n = pq$ be a Blum integer, i.e., p and q are distinct primes and $p \equiv_4 q \equiv_4 3$. If $x \in \mathbb{Q}_n$, then $(x^{(n-p-q+5)/8} \bmod n)$ is a square root of x, and if $x \in J_n$, then

$$x^{2d} \equiv_n \begin{cases} x, & \text{if } x \in \mathbb{Q}_n \\ n - x, & \text{if } x \in \tilde{\mathbb{Q}}_n \end{cases} \tag{5}$$

where $d = (n - p - q + 5)/8$. Let $n = pq$ be a William integer, i.e., p and q are distinct primes and $p \equiv_8 3$ and $q \equiv_8 7$. Thus, the integer 2 is a quadratic non-residue under modulus n with Jacobi symbol $\left(\frac{2}{n}\right) = -1$. Hence, multiplication of any integer $x \in \mathbb{Z}_n^*$ by 2 or $(2^{-1} \bmod n)$ reverses the Jacobi symbol of x.

3 Review of Chen-Qiu-Zheng Blind Signature Scheme

Chen-Qiu-Zheng blind signature scheme of [4] is based on Rabin's signatures of [1]. There are two participants, a sender and a signer, in the blind signature scheme. A sender requests signatures from the signer, and the signer issues signatures on the blinded messages to the sender. The protocol consists of three phases: (i) requesting, (ii) signing, and (iii) extraction. A sender submits a blinded message to the signer in the requesting phase to request a blind signature. In the signing phase, the signer computes the signature on the blinded message and returns the result, called the blind signature, to the sender. Finally, the sender extracts the signature from the blind signature that she/he received in the extraction phase. Let $n = pq$ be a William integer and h be a one-way hash function, where p and q are kept secret by the signer. The details of the scheme are described as follows.

1. Requesting phase: To request the signature of a message m, the sender computes $h(m)$. She/He then randomly chooses a blinding factor $r \in \mathbb{Z}_n^*$ and computes $r^4 \bmod n$. The sender chooses appropriate bit

$$a = \begin{cases} 0, & \text{if } \left(\frac{h(m)}{n}\right) = 1 \\ 1, & \text{if } \left(\frac{h(m)}{n}\right) = -1 \end{cases} \tag{6}$$

such that $(2^{-a}h(m) \bmod n) \in J_n$. The sender then submits the blinded message $\tilde{m} = (2^{-a}r^4h(m) \bmod n)$ to the signer.

2. Signing phase: After receiving $\tilde{m}$, the signer computes $\tilde{s} = (2^{-a}r^4h(m))^d \bmod n$ where $d = (n - p - q + 5)/8$ is the private key of the signer, and sends the blind signature $\tilde{s}$ to the sender.

3. Extraction phase: The sender computes $s = (\tilde{s}r^{-2}) \bmod n$ and forms (s, a, b) such that $s^2(-1)^b2^a \equiv_n h(m)$ where $b = 0$ or 1. One can verify the signature (s, a, b) on m by checking the formula $s^2(-1)^b2^a \equiv_n h(m)$.

4 An Attack on Chen-Qiu-Zheng Blind Signature Scheme

We demonstrate that Chen-Qiu-Zheng blind signature scheme of [4] is not secure against the chosen-text attacks as follows.

Lemma 4.1 *Given two integers x and y in $\mathbb{Z}_n^*$ where $n = pq$ is a Blum integer, if $x^2 \equiv_n y^2$ and $x \neq \pm y \pmod n$, then $GCD((x + y) \bmod n, n) = p$ or q.*

Proof: By the Chinese Remainder Theorem, an integer w in $\mathbb{Z}_n^*$ can be represented by $< w_1, w_2 >$ where $w_1 = (w \bmod p)$ and $w_2 = (w \bmod q)$. For each $k = < k_1, k_2 >$ and $w = < w_1, w_2 >$ in $\mathbb{Z}_n^*$, $((k+w) \bmod n) = <(k_1 + w_1)$ mod p, $(k_2 + w_2)$ mod $q >$, $(kw$ mod $n) = < k_1w_1$ mod p, k_2w_2 mod $q >$, $(k^{-1}$ mod $n) = < k_1^{-1}$ mod p, k_2^{-1} mod $q >$, and $(-k$ mod $n) = < -k_1$ mod p, $-k_2$ mod $q >$. Besides, for every $< k_1, k_2 >$ and $< w_1, w_2 >$ in $\mathbb{Z}_n^*$, $< k_1, k_2 > = < w_1, w_2 >$ if and only if $k_1 \equiv_p w_1$ and $k_2 \equiv_q w_2$. Let $t = x^2$ mod n. The integer t has four square roots $\{< x_1, x_2 >, < x_1, -x_2 \bmod q >, < -x_1 \bmod p, x_2 >, < -x_1 \bmod p, -x_2 \bmod q >\}$. Thus, $y = < -x_1 \bmod p, x_2 >$ or $< x_1, -x_2 \bmod q >$ since $x \neq y \pmod n$. If $y =< -x_1 \bmod p, x_2 >$, then $((x + y) \bmod n) = < x_1, x_2 > + < -x_1 \bmod p, x_2 > = <0, 2x_2 \bmod q >$. Hence, $((x + y) \bmod n)$ can be divided by p and $GCD((x + y) \bmod n, n) = p$. If $y = < x_1, -x_2 \bmod q >$, then $((x + y) \bmod n) = < x_1, x_2 > + < x_1, -x_2 \bmod q > = < 2x_1 \bmod p, 0>$. Thus, $((x + y) \bmod n)$ can be divided by q and $GCD((x + y) \bmod n, n) = q$. Q.E.D.

If someone tries to compromise Chen-Qiu-Zheng blind signature scheme, she/he can send the blinded message $(2^{-a}r^2h(m) \bmod n)$, instead of

$(2^{-a}r^4h(m) \bmod n)$, to the signer without being detected by the signer because it is blinded, and then obtains the blind signature $\tilde{s} = (2^{-a}r^2h(m))^d \bmod n$ from the signer. By (5), $\tilde{s}^2 \equiv_n 2^{-a}r^2h(m)$ is with probability $\frac{1}{2}$. Hence, $\tilde{s}$ is a square root of $(2^{-a}r^2h(m) \bmod n)$ in $\mathbb{Z}_n^*$ with probability $\frac{1}{2}$, and $(\tilde{s}r^{-1} \bmod n)$ is a square root of $(2^{-a}h(m) \bmod n)$ in $\mathbb{Z}_n^*$ with probability $\frac{1}{2}$, too. The sender then randomly selects another blinding factor $\hat{r}$ in $\mathbb{Z}_n^*$, and sends the blinded message $(2^{-a}\hat{r}^2h(m) \bmod n)$ to the signer, so that she/he can receive the blind signature $\hat{s} = (2^{-a}\hat{r}^2h(m))^d \bmod n$ from the signer. Thus, $(\hat{s}\hat{r}^{-1} \bmod n)$ also is a square root of $(s^{-a}h(m) \bmod n)$. If $\hat{s}\hat{r}^{-1} \not\equiv \tilde{s}r^{-1} \pmod n$, which is with probability $\frac{1}{2}$, then $GCD(\hat{s}\hat{r}^{-1} + \tilde{s}r^{-1} \bmod n, n)$ is one of the prime factors of n by Lemma 4.1. The above attack can break Chen-Qiu-Zheng blind signature scheme of [4] with non-negligible probability $\frac{1}{2}$.

References

[1] M. RABIN, Digitalized signatures and public key functions as intractable as factorization. MIT/LCS/TR-212, MIT Laboratory for Computer Science, 1979.

[2] A. SHAMIR, L. ADLEMAN, and R. RIVEST, A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 1978, 21, (2), 120-126.

[3] D. CHAUM, Blind signatures for untraceable payments. Advances in Cryptology-CRYPTO'82, Plenum, 1983, 199-203.

[4] D. ZHENG, K. CHEN, and W. QIU, New Rabin-like signature scheme. Workshop Proceedings of the Seventh International Conference on Distributed Multimedia Systems, Knowledge Systems Institute, 2001, 185-188.

Received: September 30, 2007