Joint Conference of 1996 International Computer Symposium
December 19~21, Kaohsiung, Taiwan, R.O.C.

Comments on "An Oblivious Transfer Protocol and Its Application for The Exchange of Secrets"

Chiung-Ying Huang
Institute for Information Industry
Jonathan Jen-Rong Chen
Department of Information Management
National Defense Management College

ABSTRACT

Rabin[1] has devised a protocol whereby user A transfer a secret to user B with probability. Thus user B has 50% chance of receiving the secret and a 50% chance of receiving nothing. On the other hand, user B will know whether he has received the secret; user A will not. Clearly, the uncertainty must be agreeable to both users. Called the "oblivious transfer (OT scheme)". Harn and Lin[2] also proposed an OT scheme which is based on the discrete logarithm problem. However, protocol errors was found in such scheme. This paper shows an attack to break the scheme.

Keywords *: Oblivious Transfer, Discrete Logarithm, Factorization*

1. Introduction

In Rabin's protocol, user A has a 50% chance of sending user B two primes, p and q. User A will not know whether or not the transfer is successful. This protocol is based on the factorization large integer problem[7]. The oblivious transfer protocol can be used to flip coins by telephone, exchange secrets, and send certified mail[3][4][5]. We describe the protocol for coin flipping by telephone briefly[8].

Coin flipping protocol:

1. Alice selects two large primes p and q and sends $n = pq$ to Bob.
2. Bob checks if n is prime, a prime power, or even; if so, Alice cheated and loses. Bob picks an x and sends $a = x^2 (\mathrm{mod} n)$ to Alice.
3. Alice computes the four roots of a, picks one at random, and sends it to Bob.
4. Bob wins if he can factor n.

Harn and Lin[2] proposed an OT scheme based on discrete logarithm[6] problem. In such scheme, it shows the same functionality as Rabin[1]. However, protocol errors was found.

The rest of this paper was organized as follows: Section 2 provides a review of Harn and Lin's[2] scheme. Section 3 presents the attack to break the scheme. Conclusion remarks are finally made in section 4.

2. Paper Review

Harn and Lin's scheme is described here. The public values agreed by user A and user B.

$p : p = 4p' + 1$, p' is a prime number.

A selects secret $x \in [1, p-1]$ and $\gcd(x, p-1) = 1$, $x \in QNR_p$. A random selects a primitive root α mod p and announce as commit value.

The OT protocol is as follows:

1. A sends $m_s \equiv \alpha^x (\mathrm{mod}\ p)$ and $m_{1-s} \equiv x^x (\mathrm{mod}\ p)$ to B. $s \in \{0,1\}$ is secret to A.
2. B random selects secret b and $\gcd(b, p-1) \equiv 1$. B sends $C_1 \equiv m_0{}^b (\mathrm{mod}\ p)$ or $C_1 \equiv m_1{}^b (\mathrm{mod}\ p)$ to A.
3. A calculates and sends $C_2 \equiv C_1{}^{x^{-1}} (\mathrm{mod}\ p)$ (where x^{-1} satisfies $x \cdot x^{-1} \equiv 1 (\mathrm{mod}(p-1))$ to B.
4. B calculates $C_3 \equiv C_2{}^{b^{-1}} (\mathrm{mod}\ p)$. If $C_3 \equiv \alpha$ then B fails to get the secret x. On the other hand, if $C_3{}^{C_3} \bmod p \equiv m_s$ or m_{1-s} then $C_3 \equiv x$.

Example :

public $p : p = 29 = 4*7 + 1$,

A selects $x = 13$, and primitive root $\alpha = 3$, as commit value.

1. Let $s = 0$, $m_0 \equiv \alpha^x (\mathrm{mod}\ 29) \equiv 3^{13} (\mathrm{mod}\ 29) \equiv 19$,
   $m_1 \equiv 13^{13} (\mathrm{mod}\ 29) \equiv 9$,
2. B random select $b = 3$, and sends $C_1 \equiv m_0{}^b (\mathrm{mod}\ p) \equiv 19^3 (\mathrm{mod}\ 29) \equiv 15$ to

A.

3. *A* calculates and sends $C_2 \equiv C_1^{x^{-1}} \equiv 15^{13} (\text{mod } 29) \equiv 27.$ (x^{-1}=13)

4. *B* calculates $C_3 \equiv C_2^{b^{-1}} (\text{mod } p) \equiv 27^{19} (\text{mod } 29) \equiv 3. (b^{-1} \equiv 19)$

3 = α, *B* fails to receive the secret x.

3. The Attack

Now, users *B* may always obtain the secret x follow the same protocol. The attack is as follows:

1. (same as the origin scheme)
2. *B* random selects secret b and $\gcd(b, p-1) \equiv 1$. *B* always sends $C_1 \equiv (m_0 \cdot m_1)^b (\text{mod } p)$ to *A*.
3. (same as the origin scheme)
4. *B* calculates $C_3 \equiv C_2^{b^{-1}} (\text{mod } p)$. Now, $C_3 \equiv \alpha \cdot x$, since α is public to both *A* and *B*. Hence x is also known to *B*.

A has no knowledge about the data sends by *B*. *B* always get the secret x without any extra information from *A*.

Example :

public $p : p = 29 = 4*7 + 1$,

A selects x = 13, and primitive root $\alpha = 3$, as commit value.

1. Let $s = 0$, $m_0 \equiv \alpha^x (\text{mod } 29) \equiv 3^{13} (\text{mod } 29) \equiv 19$, $m_1 \equiv 13^{13} (\text{mod } 29) \equiv 9$,
2. *B* random select b = 3, and sends $C_1 \equiv (m_0 \cdot m_1)^b (\text{mod } p) \equiv (19 \cdot 9)^3 (\text{mod } 29) \equiv 2$ to *A*.
3. *A* calculates and sends $C_2 \equiv C_1^{x^{-1}} \equiv 2^{13} (\text{mod } 29) \equiv 14.$ (x^{-1}=13)
4. *B* calculates $C_3 \equiv C_2^{b^{-1}} (\text{mod } p) \equiv 14^{19} (\text{mod } 29) \equiv 10.$ $\alpha \cdot x \equiv 10 (\text{mod } 29), \because \alpha \equiv 3, \therefore x \equiv 13.$

4. Conclusion

The oblivious transfer is 50% probability for the receiver to get the secret or nothing. The proposed attack causes the receiver 100% obtain the secret. It is un-fair to the sender and against the OT rules. How to solve the problem and prevent both sides to send the forged data is under developing. It is believed to be solved in the recently future.

References

[1] M.O. Rabin, "Exchange of Secrets,", Dept. of Applied Physics, Harvard University, Cambridge, Mass, 1981.

[2] L. Harn and H.Y. Lin, "An Oblivious Transfer Protocol and Its Application For The Exchange of Secrets," Advances in Cryptology : ASICRYPT "91", pp.312-320.

[3] M. Blum, "Three Applications of Oblivious Transfer : 1. Coin Flipping by Telephone, 2. How to Exchange Secrets. 3. How to send Certified Electronic Mail." Dept. ECCS, Univ. of California, Berkely, Calif. (1981).

[4] M. Blum, "Coin-flipping by telephone - a protocol for solving impossible problems," IEEE Proceedings, Spring Compcon., 133-137.

[5] M. Blum, and M.O. Rabin, "How to Send Certified Electronic Mail," Dept. EECS, University of California, Berkely, Calif., 1981.

[6] Kenneth H/ Rosen, "Elementary Number Theory and Its Applications.", 3rd Edition, 1992.

[7] H.Riesl, Prime Numbers and Computer Methods for Factorization, Birkhauser, Boston, 1985.

[8] Dorothy Elizabeth Robling Denning, "Cryptography and Data Security," Purdue University.