A Simple Algorithm to Predict Committed Bit

Hyoung Joong Kim · Department of Control and Instrumentation Engineering
Kangwon National University Chunchon 200-701,
Koreakhj@kangwon.ac.kr

ABSTRACT

This paper presents a simple method to show that the committed bit based on pseudo-random sequence can be predicted with a probability very close to.

Keywords : Bit commitment protocol, Cryptography, Pseudo-random sequence.

1. Introduction

A bit commitment protocol comprises COMMIT protocol and DISCLOSURE protocol, involving a sender (Alice) and receiver (Bob). Alice wants to commit a bit during the COMMIT stage. However, she does not want to reveal it until sometime later, namely DISCLOSURE stage. Bob, on the other hand, wants to make sure that Alice cannot change her mind after she has committed to the bit up to DISCLOSURE stage. Bit commitment protocol is an important area in cryptography [1-6].

There are at least three variant of classical bit commitment protocol [6] :

(1) Bit commitment with symmetric key,
(2) Bit commitment using one-way function, and
(3) Bit commitment using pseudo-random sequence generator

Among them bit commitment using pseudo- random sequence [5] is quite simple to implement and easy to use. It is claimed that if Bob's random bit string is long enough, then there is no practical way Alice can cheat [6]. It was believed that this protocol requires exponential time complexity to predict committed bit exactly. Here in this paper we show that Bob can predict the committed bit with considerably high probability before DISCLOSURE stage.

Quantum bit commitment is a latest technology. It has been believed that quantum bit commitment might break a road for secure protocol. Unfortunately, it is also insecure [2-3]. Thus, security of classical methods

should be analyzed for further tight security.

Ⅱ. Bit Commitment Using Pseudo-Random Sequence

Bit commitment protocol using pseudo-random sequence is given as follows [5] :

COMMIT stage :

(1) Bob selects a random vector where for and sends it to Alice.

(2) Alice selects a seed and sends to Bob the vector where

(1)

DISCLOSURE stage :

(3) Alice sends Bob her random seed .

(4) Bob completes step (2) to confirm that Alice's committed bit was itself.

Note that denotes the th bit of a pseudo-random sequence generated on a random seed where Alice and Bob have the same pseudo-random sequence generator in mind. Here, we assume that any pseudo-random sequence generator works.

Ⅲ. Determination of Committed Bit

Let which is a function of Bob's random sequence (), Alice's committed bit () and the pseudo-random sequence on a random seed. Let the first elements of be the seed of the pseudo-random sequence generator. Since Bob knows the random number generator architecture, he can try to find out whether the seed generates or not.

Case (i) : If seed does not generate , Bob concludes that the committed bit is one.

Case (ii) : If seed does generate , Bob cannot conclude whether the committed bit is zero. The committed bit can be zero or one.

To avoid the difficulty in Case (ii), Bob changes the seed. First Bob recovers from, since he knows. Then Bob derives another seed' from the recovered .

Case (iii) : If seed' does not generate, Bob concludes that the committed bit is one.

Case (iv) : If the seed' does generate, Bob concludes that the committed bit is zero with a probability very close to, and the committed bit is one with a probability very close to.

The novelty here is the property of the seed'. When the seed' generates, the probability of is, which is very close to. When the seed' generates, the probability of is. This property of seed' helps in the determination of the committed bit.

The weak point of the protocol is its recoverability of seed in Equation (1). Thus, if there is a way to protect the seed from recovering, this protocol will remain safe.

Ⅳ. Conclusion

A simple algorithm is presented to predict the committed bit the protocol using pseudo-random sequence in this paper. It is shown that the committed bit can be predicted with high probability before DISCLOSURE stage.

■ References

[1] Blundo, C., Masucci, B., Stinson, D. R., and Wei, R., "Constructions and bounds for unconditionally secure non-interactive commitment schemes," *Designs, Codes, and Cryptography*, Vol.26, pp.97-110, 2002.

[2] Lo, H.-K. and Chau, H. F., "Is quantum bit commitment really possible?," Los Alamos preprint archive quant-ph/9603004, 1996.

[3] Lo, H.-K. and Chau, H. F., "Why quantum bit commitment and ideal quantum coin tossing are impossible," Los Alamos preprint archive quant-ph/9711065, 1997.

[4] Mollin, R. A., *An Introduction to Cryptography*, CRC Press, 2000.

[5] Naor, M., "Bit commitment using pseudo-randomness," *Journal of Cryptology*, Vol.4, No.2, pp.151-158, 1991.

[6] Schneier, B., *Applied Cryptography : Protocols, Algorithms, and Source Code in C*, 2nd Edition, John Wiley and Sons, 1996.

Acknowledgments

This work was in part supported by the Advanced Information Technology Research Center (AITrc), KAIST, under the auspices of the Ministry of Science and Technology, Korea. The author appreciates the discussions with Prof. V. Mani, Indian Institute of Science, India.

저자 소개

김 형 중
(Kim Hyoung Joong)
1978년 서울대 전기공학과 졸업
1986년 서울대 제어계측공학과 석사
1989년 서울대 제어계측공학과 박사
1989년 강원대 제어계측공학과 부임, 현 교수
관심분야 : 멀티미디어통신, 정보보호