

# Cryptanalysis on a novel unconditionally secure oblivious polynomial evaluation protocol

Wang Qinglong

School of information engineering, chang'an university  
Shaanxi Road Traffic Detection and Equipment Engineering  
Technology Research Centre  
Xi'an China  
qlwang@chd.edu.cn

Xu Li

School of information engineering, chang'an university  
Xi'an China  
xuli@chd.edu.cn

**Abstract**— Vanishree et.al proposed a novel unconditionally oblivious polynomial evaluation protocol and they claimed that can fulfill both sender and receiver's security. Here, this protocol is cryptanalyzed. We find that it has a fatal fault which cannot implement the receiver's security at all and show the detail analyzing process.

**Keywords**- oblivious polynomial evaluation, oblivious transfer, multi-party computation

## I. INTRODUCTION

Assume that there are two parties, Alice who has a polynomial  $f$  and Bob who has an input  $x$ . They want to collaborate in a way for Bob to compute  $f(x)$  such that Alice learns nothing about  $x$  and Bob learns only  $f(x)$  and nothing more. A protocol achieving this task for any polynomial  $f$  and any input  $x$  is called an Oblivious Polynomial Evaluation protocol (OPE for short). Actually, Oblivious polynomial evaluation can be regard as a special case of Oblivious Transfer (OT) and was introduced in [2]. In [2,6], an OPE protocol over finite field was given and the security of the protocol is based on two assumptions. One assumption is the existence of a secure 1-out-of-2 Oblivious Transfer protocol (denoted as  $OT_2^1$ ) while the other is the intractability of a Noisy Polynomial Interpolation Problem. In [1], three OPE protocols were proposed. The security of the first two protocols is based on the existence of a secure  $OT_2^1$  while the third protocol involves a third party who does not collude with others. [5,10] introduced an OPE protocol based on assumption of decisional composite residuosity problem<sup>[4]</sup>. In [9], two OPE protocols were presented based on the assumption of existing a secure Oblivious Transfer protocol. [7,8,12] are two information-theoretically secure OPE protocols with the help of an off-line third party who pre-distributes some data during a setup phase. The protocol presented in [3] is based on an assumption that the Decisional Diffie-Hellman (DDH) assumption also holds over  $Z_{n^2}$ , where  $n$  is the product of two large primes. [11] (named as VG protocol) proposed an unconditionally secure OPE scheme which do not depend on any intractable assumption. However,

we show that their protocol has a fatal fault and is not secure at all.

## II. INTRODUCTION OF VG PROTOCOL

### A. Input

Sender: a  $k$ th degree polynomial  $P$  over a finite field  $\mathcal{F}$  :

$$P(\alpha) = \sum_{i=0}^k a_i \alpha^i .$$

Receiver: a value  $x \in \mathcal{F}$  .

### B. Initialization

Sender chooses an arbitrary generator of  $\mathcal{F}$ ,  $g_S$ , and a random element  $r_S \in \mathcal{F}$ . Receiver also chooses an arbitrary generator,  $g_R$ , and three random elements  $r_{R1}, r_{R2}, r_{R3} \in \mathcal{F}$ . All computations of the protocol are done in  $\mathcal{F}$ .

### C. Protocol

Step 1: Sender computes  $m_1$  defined as,  $m_1 = a_0 g_S^{r_S}$  and sends it to Receiver.

Step 2: Receiver computes  $m_{2i}$ ,  $0 \leq i \leq k$  defined as,  $m_{20} \triangleq m_1 g_R^{r_{R1}} - r_{R2}$  and  $m_{2i} \triangleq x^i g_R^{r_{R3}}$  for  $1 \leq i \leq k$  and sends them to Sender.

Step 3: Sender computes  $m_3$  defined as,  $m_3 \triangleq \sum_{i=1}^k a_i m_{2i} = g_S^{r_S} \left( \sum_{i=1}^k a_i x^i \right) g_R^{r_{R3}}$ , and sends it to Receiver.

Step 4: Receiver computes  $m_4$  defined as,  $m_4 \triangleq m_3 \left( g_R^{r_{R3}} \right)^{-1} g_R^{r_{R1}} + r_{R2}$ , and sends it to Sender. Clearly,  $m_4 \triangleq \sum_{i=1}^k a_i m_{2i} = g_S^{r_S} \left( \sum_{i=1}^k a_i x^i \right) g_R^{r_{R1}} + r_{R2}$ .

Step 5: sender computes  $m_5$  defined as,  $m_5 \triangleq \left( g_S^{r_S} \right)^{-1} (m_{20} + m_4)$  and sends them to Receiver.

Clearly,

$$m_5 = \left(g_S^{r_S}\right)^{-1} \left(a_0 g_S^{r_S} g_R^{r_{R1}} - r_{R2} + g_S^{r_S} \left(\sum_{i=1}^k a_i x^i\right) g_R^{r_{R1}} + r_{R2}\right) \\ = P(x) g_R^{r_{R1}}$$

Step 6: receiver computes  $P(x)$  as,  $m_5 \left(g_R^{r_{R1}}\right)^{-1} = P(x)$ .

### III. ANALYSIS OF VG PROTOCOL

Sender can easily get receiver's secret value  $x$  from  $m_{2i}$ ,  $1 \leq i \leq k$ , which sender received during step 2, as the following method:

Sender randomly selects two  $m_{2i}, m_{2(i+1)}$  and computes

$$m_{2(i+1)} \left(m_{2i}\right)^{-1} = x^{i+1} g_R^{r_{R3}} \left(x^i g_R^{r_{R3}}\right)^{-1} = x.$$

### IV. CONCLUSION

Most existing oblivious polynomial evaluation protocol was built under some intractable problems. Recently, Vanishree et.al presented an unconditionally secure OPE protocol without using third party. However, their protocol is not secure at all, because the sender can easily get receiver's secret value as above. Thus, a real unconditionally secure OPE protocol without third party needs further research.

### ACKNOWLEDGMENT

The Project was Supported by the Special Fund for Basic Scientific Research of Central Colleges, Chang'an University. (No. CHD2009JC146).

### REFERENCES

- [1] Y. C. Chang, C. J. Lu, "Oblivious polynomial evaluation and oblivious neural learning", in Theoretical Computer Science 341(1),2005, pp. 39–54.
- [2] M. Naor, B. Pinkas. Oblivious Transfer and Polynomial Evaluation. In Proc. of the 31st STOC, Atlanta, GA, 1999, pp. 245–254.
- [3] N. Gilboa. Two party RSA key generation. In CRYPTO 1999, pp. 116–129.
- [4] P. Paillier. Public-key cryptosystems based on composite degree residuosity classes. EUROCRYPT1991, pp. 223-238.
- [5] C Hazay, Y Lindell. Efficient oblivious polynomial evaluation with simulation-based security. International association for Cryptologic research, e-print IACR archive, <http://eprint.iacr.org/2009/459.pdf>.
- [6] M Naor, B Pinkas. Oblivious polynomial evaluation. SIAM J. of computing, v. 35, number 5, 2006, pp. 1254-1281.
- [7] Goichiro Hanaoka, Hideki Imai, Joern Mueller-Quade, et.al. Information Theoretically Secure Oblivious Polynomial Evaluation: Model, Bounds, and Constructions. Information Security and Privacy. Lecture Notes in Computer Science, 2004, Volume 3108/2004, pp.62-73.
- [8] R Tonicelli, Anderson C. A. Nascimento, R Dowsley, et.al. Information-Theoretically Secure Oblivious Polynomial Evaluation in the Commodity-Based Model. International association for Cryptologic research, e-print IACR archive, <http://eprint.iacr.org/2009/270.pdf>.
- [9] Hong-Da Li, Dong-Yao Ji, Deng-Guo Feng, et.al. oblivious polynomial evaluation. Journal of Computer Science and Technology, 2004, 19(4), pp.550-554.
- [10] Huafei Zhu, Feng Bao. Augmented Oblivious Polynomial Evaluation Protocol and Its Applications. Computer Security – ESORICS 2005, Lecture Notes in Computer Science, 2005, Volume 3679/2005, pp. 222-230.
- [11] H. Vanishree, Koshy George. A Novel Unconditionally Secure Oblivious Polynomial Evaluation Protocol. Proceedings of the 2009 International Workshop on Information Security and Application (IWISA 2009), Academy Publisher, Finland, 2009, pp.450-452.
- [12] Otsuka A, Nascimento A C A, Imai H. Unconditionally Secure Polynomial Evaluation And Its Application To Electronic Voting. IEIC Technical Report (Institute of Electronics, Information and Communication Engineers), VOL.104, NO. 200, 2004, pp. 157-164.