Unconditionally secure Oblivious Polynomial Evaluation protocol

Li Luyao^{1,2} Duan Zongtao¹ Wang Qinglong¹ Wang Jing¹ Dai Ming^{1,2}

¹School of Information Engineering, Chang'an University, Xi'an 710064, China

²China Transport Telecommunications & Information Center, Beijing 100011, China

Abstract:

Oblivious polynomial evaluation is a protocol involving two parties: a sender whose input is a polynomial $f(x)$ and a receiver whose input is a value a . Most of existing Oblivious Polynomial Evaluation protocols were built based on some cryptographically intractable problems which made them a higher computation complexity. By using some random and hiding secure information in them, this paper presents an unconditionally secure oblivious polynomial evaluation protocol. It does not rely on any cryptographic assumption and involves only simple computation. Further, our protocol does not include any third party and is more practice.

Keywords: Multi-party computation; oblivious transfer; oblivious polynomial evaluation; unconditional security

1. Introduction

Oblivious Polynomial Evaluation (OPE) ^[1] is a protocol including two parties: A sender who has a polynomial $f(x)$, a receiver who has a secret value a . At the end of the protocol the receiver obtains $f(a)$. The OPE safety requirements: after the protocol running completely, the sender cannot get any information of both a and $f(a)$, while the receiver learned not more about $f(x)$ than $f(a)$. As a two parties protocol Oblivious Polynomial Evaluation can be used in many applications such as protocols for private comparison of data, for mutually authenticated key exchange based on passwords, and for anonymous coupons.

Yao[2] and Goldreich, Micali, and Wigderson[3] proposed two OPE schemes by using a Boolean circuit to represent the function $f(x)$ and then simulating the

computation of this circuit in some oblivious way. The computational or communicational overhead of their protocols depends linearly on the circuit size of the function f and so their protocols were far from being practical. Noar and Pinkas first considered a simple case where f is a polynomial over a finite field[1]. One is the existence of a secure 1-out-of-2 Oblivious Transfer protocol-OT^[4, 5, 6] and the other is that Noisy Polynomial Interpolation Problem^[7] is a difficult problems. However, it was later shown in [20] that the second assumption may be much weaker than expected.

Chang proposed three OPE schemes in [9]. The first two were based on 1-out-of-2 Oblivious Transfer protocol. The third one involved a trusted third party and was perfectly secure. Li also presented two OPE schemes in [18]. One was constructed by directly using 1-out-of-n[19] and the other worked with the help of an untrusted third party. In [13-15], the authors constructed several unconditionally secure OPE schemes also by using a trusted off-line third party. Lindell and Pinkas[8] proposed another OPE protocol based on non-standard Decisional Diffie-Hellman(DDH) assumption which is yet to be well studied. The authors of [16] proposed an OPE protocol without using a third party. They claimed that their scheme was unconditionally secure. However, it has been proved not true[17].

Oblivious polynomial evaluation has been proved to be a useful building block, and can be used to solve numerous cryptographic problems; such as secure equality of strings, set intersection, comparing information, anonymous coupons, anonymous initialization for metering, approximation of a Taylor series, RSA key generation, oblivious keyword search and more [1,27].

The security of existing OPE protocols can be

classified two types. The first is computational security and the second is unconditional security (also called information-theoretic security). For the first type, it is assumed that an attacker has only limited computational resources. For the second, the attacker has unlimited computational resources.

The goals of OPE can be summarized as follows:

- Correctness: For any polynomial and any input, Bob always obtains the correct value after running the protocol.
- Alice's security: Bob learns nothing more about except what can be deduced from.
- Bob's security: Alice learns nothing about.

This paper presents a new unconditionally secure OPE protocol that involves neither a cryptographically intractable problem nor a third party. Our OPE protocol only needs simple operation and thus is more efficient.

The rest of this paper is organized as follows: Section 2 gives our proposed OPE scheme. The security of our OPE scheme is analyzed in section 3. Section 4 introduces the efficiency and section 5 concludes this paper.

2. Our protocol

2.1. System Settings

Set p as a big prime number and assume Alice has a polynomial $f(x) = \sum_{i=0}^k a_i x^i$ of $Z_p \setminus \{0\}$. Bob has a secret value $j \in Z_p \setminus \{0\}$. All the algorithm operation in this paper is in Z_p except specification.

2.2. Protocol introduction

Step1 Bob randomly selects $j, R, R_2, r_i, c_i, 0 \leq i \leq k$

in Z_q^* , satisfying $\sum_{i=0}^k r_i c_i = 0$. Bob calculates

$$\Phi_1 = Y_0 \parallel Y_1 \parallel \dots \parallel Y_K \text{ where } Y_i = Rj^i + r_i, 0 \leq i \leq k.$$

Set $\Phi_1' = R_2 r_0 \parallel \dots \parallel R_2 r_k$, sending Φ_1, Φ_1' to Alice.

Step2 Alice randomly selects a vector $\beta = (\beta_0 \dots \beta_k)$ by solving the equation

$$\sum_{i=0}^k \beta_i R_1 r_i = 0. \quad \text{Alice also randomly selects } R_1 \in_R Z_p^*. \quad \text{Calculates and sends to Bob}$$

$$\Delta_1 = R_1 \sum_{i=0}^k a_i Y_i.$$

Step3 Bob randomly selects $b_1 \in_R Z_p$. Calculates and sends to Alice $\Phi_2 = \Delta_1 r_0^{-1} + b_1 + c_0$.

Step4 Alice calculates and sends to Bob $\Delta_2 = \Phi_2 - R_1 a_0 + \beta_0$.

Step5 Bob randomly selects $b_2 \in_R Z_p$. Calculates and sends to Alice $\Phi_3 = (\Delta_2 - b_1) r_0 r_1^{-1} + b_2 + c_1$.

Step6 Alice calculates and sends to Bob $\Delta_3 = \Phi_3 - R_1 a_1 + \beta_1$.

Step7 Bob randomly selects $b_3 \in_R Z_p$. Calculates and sends to Alice $\Phi_4 = (\Delta_3 - b_2) r_1 r_2^{-1} + b_3 + c_2$.

Step8 Alice calculates and sends to Bob $\Delta_4 = \Phi_4 - R_1 a_2 + \beta_2$.

Step9 Bob randomly selects $b_4 \in_R Z_p$. Calculates and sends to Alice $\Phi_5 = (\Delta_4 - b_3) r_2 r_3^{-1} + b_4 + c_3$.

Step10 Alice calculates and sends to Bob $\Delta_5 = \Phi_5 - R_1 a_3 + \beta_3$.

Stepk+2 Bob calculates and sends to Alice $\Phi_{k+2} = (\Delta_{k+1} - b_k) r_{k-1} r_k^{-1} + c_k$.

Stepk+3 Alice calculates and sends to Bob $\Delta_{k+2} = (\Phi_{k+2} - R_1 a_k + \beta_k) \cdot R_2^{-1}$.

After received Δ_{k+2} , Bob calculates $\Delta_{k+2} r_k R_1^{-1}$

which is equal to $f(j)$.

2.3. Prove of correctness

Lemma 1: our protocol is correct if the parties are semi-honest.

Prove: assume Alice and Bob are semi-honest, then having

$$\Delta_1 = \sum_{i=0}^k a_i Y_i = R \sum_{i=0}^k a_i j^i + \sum_{i=0}^k a_i r_i = Rf(j) + \sum_{i=0}^k a_i r_i$$

$$\begin{aligned} \Phi_2 &= \Delta_1 r_0^{-1} + b_1 + c_0 \\ &= r_0^{-1} R_1 Rf(j) + R_1 a_0 + R_1 r_0^{-1} \sum_{i=1}^k a_i r_i + b_1 + c_0 \end{aligned}$$

$$\begin{aligned} \Delta_2 &= \Phi_2 - R_1 a_0 + \beta_0 \\ &= r_0^{-1} R_1 Rf(j) + r_0^{-1} R_1 \sum_{i=1}^k a_i r_i + b_1 + c_0 + \beta_0 \end{aligned}$$

$$\begin{aligned} \Phi_3 &= (\Delta_2 - b_1) r_0^{-1} + b_2 + c_1 \\ &= (r_0^{-1} R_1 Rf(j) + r_0^{-1} R_1 \sum_{i=1}^k a_i r_i + \beta_0 + c_0) r_0^{-1} \\ &\quad + b_2 + c_1 \\ &= r_1^{-1} R_1 Rf(j) + r_1^{-1} R_1 \sum_{i=1}^k a_i r_i + r_0 r_1^{-1} (\beta_0 + c_0) \\ &\quad + b_2 + c_1 \end{aligned}$$

$$\begin{aligned} &= r_1^{-1} R_1 Rf(j) + R_1 a_1 + r_1^{-1} R_1 \sum_{i=2}^k a_i r_i \\ &\quad + r_0 r_1^{-1} (\beta_0 + c_0) + b_2 + c_1 \\ \Delta_3 &= \Phi_3 - R_1 a_1 + \beta_1 \\ &= r_1^{-1} R_1 Rf(j) + r_1^{-1} R_1 \sum_{i=2}^k a_i r_i + r_0 r_1^{-1} (\beta_0 + c_0) \\ &\quad + b_2 + c_1 + \beta_1 \end{aligned}$$

$$\begin{aligned} \Phi_4 &= (\Delta_3 - b_2) r_1^{-1} + b_3 + c_2 \\ &= (r_1^{-1} R_1 Rf(j) + r_1^{-1} R_1 \sum_{i=2}^k a_i r_i + r_0 r_1^{-1} (\beta_0 + c_0) \\ &\quad + \beta_1 + c_1) r_1^{-1} + b_3 + c_2 \\ &= r_2^{-1} R_1 Rf(j) + R_1 a_2 + r_2^{-1} R_1 \sum_{i=3}^k a_i r_i \\ &\quad + r_0 r_2^{-1} (\beta_0 + c_0) + r_1 r_2^{-1} (\beta_1 + c_1) + b_3 + c_2 \end{aligned}$$

$$\begin{aligned} \Phi_{k+2} &= (\Delta_{k+1} - b_k) r_{k-1}^{-1} + c_k \\ &= r_k^{-1} R_1 Rf(j) + R_1 a_k + r_0 r_k^{-1} (\beta_0 + c_0) + \dots \\ &\quad + r_{k-1}^{-1} r_k^{-1} (\beta_{k-1} + c_{k-1}) + c_k \end{aligned}$$

$$\begin{aligned} \Delta_{k+2} &= (\Phi_{k+2} - R_1 a_k + \beta_k) R_1^{-1} \\ &= (r_k^{-1} R_1 Rf(j) + R_1 a_k + r_0 r_k^{-1} (\beta_0 + c_0) + \dots \\ &\quad + r_{k-1}^{-1} r_k^{-1} (\beta_{k-1} + c_{k-1}) + c_k - R_1 a_k + \beta_k) R_1^{-1} \\ &= r_k^{-1} Rf(j) + R_1^{-1} r_0 r_k^{-1} (\beta_0 + c_0) + \dots \\ &\quad + R_1^{-1} r_{k-1}^{-1} r_k^{-1} (\beta_{k-1} + c_{k-1}) + R_1^{-1} (\beta_k + c_k) \end{aligned}$$

From $\sum_{i=0}^k \beta_i R_1 r_i = 0$ and $R_1 \neq 0$ we conclude

$\sum_{i=0}^k \beta_i r_i = 0$, then we can get the follow equation

$$\begin{aligned} \Delta_{k+2} r_k^{-1} &= (r_k^{-1} Rf(j) + R_1^{-1} r_0 r_k^{-1} (\beta_0 + c_0) + \dots \\ &\quad + R_1^{-1} r_{k-1}^{-1} r_k^{-1} (\beta_{k-1} + c_{k-1}) + R_1^{-1} (\beta_k + c_k)) r_k^{-1} \\ &= f(j) + R R_1^{-1} r_0 (\beta_0 + c_0) + \dots \\ &\quad + R R_1^{-1} r_{k-1} (\beta_{k-1} + c_{k-1}) + R R_1^{-1} r_k (\beta_k + c_k) \\ &= f(j) + R R_1^{-1} \sum_{i=0}^k r_i (\beta_i + c_i) \\ &= f(j) + R R_1^{-1} \sum_{i=0}^k r_i \beta_i + R R_1^{-1} \sum_{i=0}^k r_i c_i = f(j) \end{aligned}$$

3. Security analysis

Lemma 2. Our protocol is unconditionally secure if the two parties are semi-honest.

Prove. First, we prove the Bob's security. Through the protocol, what Alice can get are $2k+4$ equations $\Phi_2, \dots, \Phi_{k+2}, Y_0, \dots, Y_k$, $\sum_{0 \leq i \leq k} \beta_i r_i = 0$,

$\sum_{0 \leq i \leq k} r_i c_i = 0$. (1) Alice cannot get any information

about $f(j)$ from $\Phi_2, \dots, \Phi_{k+2}$, because from Alice view each $\Phi_i, 2 \leq i \leq k+2$ includes two randomly selected varies b_i, c_i ; (2) Although Alice can get

$\sum_{i=0}^k Y_i = R \sum_{i=0}^k j^i + \sum_{i=0}^k r_i = R \sum_{i=0}^k j^i$ from Φ_1 , she

cannot get any information about j because the randomness of R . Also, as the random number of $r_i, 0 \leq i \leq k$ Alice cannot get any information about

j from $Y_i, 0 \leq i \leq k$; (3) As the randomness of R_2

Alice cannot get information about $r_i, 0 \leq i \leq k$ from Φ_1' . Then we conclude that Alice cannot get information about j from Φ_1' ; (4) Because there are total $3k+4$ unknown quantities $b_1, \dots, b_k, r_0, \dots, r_k, c_0, \dots, c_k, R, j$, Alice cannot get information from $2k+4$ equations $\Phi_2, \dots, \Phi_{k+2}, Y_0, \dots, Y_k, \sum_{0 \leq i \leq k} \beta_i r_i = 0, \sum_{0 \leq i \leq k} r_i c_i = 0$.

From the above analysis we conclude that Bob is secure.

Second, we prove Alice's security. (1) Obviously, Bob cannot get information about $\alpha_i, 0 \leq i \leq k$ from Δ_1 ; (2) Bob cannot get any information about $\alpha_i, 0 \leq i \leq k$ from $\Delta_2, \dots, \Delta_{k+2}$ because each $\Delta_i, 2 \leq i \leq k+2$ includes two unknown quantities $\alpha_{i-2}, \beta_{i-2}$; (3) At the end of the protocol, Bob gets $k+3$ equations $\Delta_1, \dots, \Delta_{k+2}, \sum_{i=0}^k \beta_i r_i = 0$ which include $2k+3$ unknown quantities $R_2, \alpha_i, \beta_i, 0 \leq i \leq k$, thus he cannot get any information about $\alpha_i, 0 \leq i \leq k$ from these equations.

From (1)(2)(3), we conclude that Alice is unconditionally secure.

4. Efficiency analysis

Compared with the most existing OPE protocol which need expensive computing on modular exponentiations, our protocol only need $O(k)$ simple additions, subtractions and multiplications which is of more practicability than others.

5. Conclusion

In this paper we propose a new unconditionally secure oblivious polynomial evaluation protocol which does

not rely on any cryptographic assumption. Also, our protocol only involves simple algorithm operation and does not include any third party which is more efficient.

Acknowledgements

The authors would like to thank the reviewers for their detailed reviews and constructive comments, which have helped improve the quality of this paper. This work was supported by the Fundamental Research Funds for the Central Universities under Grant No. CHD2009JC146; the Science & Technology Funds of Ministry of Transport of the P.R.CHINA under Grant No. 2012-364-208-600.

References

- [1] M. Naor and B. Pinkas, "Oblivious Transfer and Polynomial Evaluation," *Proc. of the 31st STOC, Atlanta, GA*, pp. 245–254, 1999.
- [2] O. Goldreich, S. Micali and A. Wigderson, "How to play any mental game or completeness theorem for protocols with honest majority," *Theory of Computing, ACM*, pp. 218–229, 1987.
- [3] A. C. Yao, "How to generate and exchange secrets," *Foundations of Computer Science, IEEE*, pp. 162–167, 1986.
- [4] M. Bellare, and S. Micali, "Non-interactive oblivious transfer and applications," *Lecture Notes in Computer Science*, pp. 547–557, 1990.
- [5] C. Blundo, P. D'Arco, A. D. Santis, and D. Stinson, "New results on unconditionally secure distributed oblivious transfer," *Proc of SAC '02*, pp. 291–309, 2002.
- [6] M. O. Rabin, "How to exchange secrets by oblivious transfer", *Tech. Memo TR-81, Aiken Computation Laboratory*, 1981.
- [7] D. Bleichenbacher and P. Nguyen, "Noisy polynomial interpolation and noisy Chinese remaindering," *Proc of Eurocrypt 2000*, pp. 53–69, 2000.
- [8] W. Du and Z. Zhan, "A practical approach to solve Secure Multi-party Computation problems," *Proc of Workshop on New Security Paradigm*, pp. 127–135, 2002.
- [9] Yan-Cheng Chang and Chi-Jen Lu, "Oblivious polynomial evaluation and oblivious neural

- learning,” *Proc of Asiacrypt 2001*, pp. 369-384, 2001.
- [10] C. Hazay, Y. Lindell, “Efficient oblivious polynomial evaluation with simulation-based security,” <http://eprint.iacr.org/2009/459.pdf>.
- [11] Huafei Zhu, Feng Bao, “Augmented oblivious polynomial evaluation protocol and its applications,” *Computer Security – ESORICS 2005*, pp. 222-230, 2005.
- [12] P. Paillier, “Public-key cryptosystems based on composite degree residuosity classes,” *Proc of Eurocrypt1991*, pp. 223-238, 1991.
- [13] R. Tonicelli, A. C. A. Nascimento, R. Dowsley, J. M. Quade, H. Imai, G. Hanaoka, A. Otsuka, “Information Theoretically Secure Oblivious Polynomial Evaluation: Model, Bounds, and Constructions,” *Information Security and Privacy*, pp. 62-73, 2004.
- [14] R. Tonicelli, A. C. A. Nascimento, R. Dowsley, J. M. Quade, H. Imai, G. Hanaoka, A. Otsuka, “Information-Theoretically Secure Oblivious Polynomial Evaluation in the Commodity-Based Model,” <http://eprint.iacr.org/2009/270.pdf>
- [15] A. Otsuka, A. C. A. Nascimento, H. Imai, “Unconditionally Secure Polynomial Evaluation And Its Application To Electronic Voting,” *IEIC Technical Report, Vol.104, No. 200*, pp. 157-164, 2004.
- [16] H. Vanishree, K. George, “A Novel Unconditionally Secure Oblivious Polynomial Evaluation Protocol” *Proc of IWISA 2009*, pp. 450-452, 2009.
- [17] WANG Qinglong, Xu Li, “Cryptanalysis on a Novel Unconditionally Secure Oblivious Polynomial Evaluation Protocol,” <http://eprint.iacr.org/2012/478.pdf>
- [18] Hong-Da Li, Dong-Yao Ji, Deng-Guo Feng, Bao Li, “Oblivious Polynomial Evaluation,” *Journal of computer science and technology. Vol.19, No.4*, pp. 550-554, 2004.
- [19] G. Brassard, C. Crépeau, J.M. Robert, “All-or-nothing disclosure of secrets,” *Proc of Advances in Cryptology - CRYPTO '86*, pp. 234-238, 1986.
- [20] D. Bleichenbacher, P. Nguyen, “Noisy polynomial interpolation and noisy Chinese remaindering,”