Generalized Oblivious Transfer Protocol

Partha Sarathi Roy*

Department of Pure Mathematics, University of Calcutta, India;
royparthasarathi0@gmail.com

Abstract. The notion of an important primitive in secure distributed cryptography, known as Generalized Oblivious Transfer (GOT) was introduced by Ishai and Kushilevitz (Proceeding of ISTCS97, IEEE Computer Society, 1997). In a GOT protocol, the *sender* holds a set M of secrets. The *receiver* is allowed to learn any qualified subset of secrets from that collection and nothing else, while the *sender* must remain oblivious regarding the selection that the *receiver* made. GOT has various applications such as in priced OT, in oblivious multivariate polynomial evaluation etc. However, up to the best of our knowledge all the GOT protocols that are proposed in the literature provide computational security that depends on some hardness assumption i.e., the security of the protocol boils down to some believe. As a result, research on information theoretic security for GOT is essential. Here, we discuss about information-theoretically secure GOT protocol based on secret sharing and distributed oblivious transfer.

References

1. Blakley G.R.: *Safeguarding cryptographic keys.* AFIPS 1979, 313-317 (1979)
2. C. Blundo, P. DArco, A.D. Santis, D. Stinson: *On unconditionally secure distributed oblivious transfer.* J. Cryptol. 20(3), 323-373 (2007).
3. Ghodosi H.: *Analysis of an Unconditionally Secure Distributed Oblivious Transfer.* J. Cryptol. (2013) 26: 75-79.
4. Ishai, Y., Kushilevitz, E.: *Private simultaneous messages protocols with applications.* In: Israel Symposium on Theory of Computing Systems, pp. 174-184 (1997).
5. Naor, M., Pinkas, B.: *Distributed oblivious transfer.* In: ASIACRYPT 2000, pp. 205-219 (2000).
6. Rabin M. O.: *How to exchange secrets by oblivious transfer.* Technical Report TR-81, Aiken Computation Laboratory, Harvard University, 1981.
7. Shamir A.: *How to share a secret.* Comm. ACM 22(11), 612-613 (1979).
8. Shankar B., Srinathan K., Pandu Rangan C.: *Alternative protocols for generalized oblivious transfer.* In: Proceeding of ICDCN08, pp. 304-309 (2008).
9. Tassa T.: *Generalized oblivious transfer by secret sharing.* Des. Codes Cryptogr. (2011) 58:11-21.

* Research supported in part by National Board for Higher Mathematics, Department of Atomic Energy, Government of India (No 2/48(10)/2013/NBHM(R.P.)/R&D II/695)