Oblivious Transfer and Bit Commitment Based on Quantum Communication

Pino Caballero-Gil
Daniel Escanez-Exposito

University of La Laguna, 38271 La Laguna, Tenerife, Spain

pcaballe@ull.edu.es

Abstract

In Quantum Key Distribution (QKD), a sender (Alice) and a receiver (Bob) who trust each other want to establish a shared secret key through quantum communication.
Unlike QKD, in two-party cryptographic protocols based on quantum communication, such as quantum oblivious transfer and bit commitment, Alice and Bob are not assumed to trust each other. This implies that the study of these protocols must consider both combinations of honest Alice with malicious Bob, and vice versa.
In Quantum Oblivious Transfer (QOT) Alice transfers with probability 1/2 a secret to Bob in such a way that she does not know whether he succeeded in obtaining the secret (concealing property), using quantum communication [1].
In Quantum Bit Commitment (QBC) Alice selects a binary value and commits it to Bob so that she cannot change her choice after committing it (binding property), while Bob does not know the selected value until Alice reveals it (hiding property), all of this using quantum communication [2].
QOT and QBC have been the subject of research over the last years in which several proposals and results have been presented, based on principles of quantum mechanics such as entanglement, superposition and non-cloning. One of those results is that QBC can be implemented from QOT and vice versa. Unfortunately, other results include different quantum no-go theorems showing that quantum mechanics does not allow implementations of such cryptographic primitives without further assumptions [3].
This work discusses the two main paths being taken to develop practical quantum protocols that minimize the risk of cheating. On the one hand, some developments are based on certain assumptions about the existence of functional primitives (e.g., QBC) [4], or on limitations in the technological potential of the malicious party (e.g., noisy-storage model) [5]. On the other hand, other developments are based on a relaxed definition of security that allows the malicious party to extract, with a given probability, certain information about the input/output of the honest party, leading to weak protocol definitions [6].

References

[1] Bennett, C.H., Brassard, G., Crépeau, C., Skubiszewska, M.H. (1991). Practical quantum oblivious transfer. Annual international cryptology conference, 351-366. Springer.
[2] Brassard, G., Crépeau, C. (1991). Quantum bit commitment and coin tossing protocols. Advances in Cryptology-CRYPTO'90, 49-61. Springer.
[3] Mayers, D. (1997). Unconditionally secure quantum bit commitment is impossible. Physical review letters, 78(17), 3414.
[4] Grilo, A.B., Lin, H., Song, F., Vaikuntanathan, V. (2021). Oblivious transfer is in MiniQCrypt. Annual International Conference on the Theory and Applications of Cryptographic Techniques, 531-561. Springer.
[5] Liu, Y., et al. (2014). Experimental unconditionally secure bit commitment. Physical review letters, 112(1), 010504.
[6] Aharonov, D., et al. (2016). A simpler proof of the existence of quantum weak coin flipping with arbitrarily small bias. SIAM Journal on Computing, 45(3), 633-679.