On quantum key exchange with classical communication from one-way functions

Samuel Bouaziz

In this work, we study key agreement protocols : protocols between two parties, Alice and Bob, that share no common information but such that at the end of the protocol, they share a common key k. There is another party involved, the eavesdropper Eve, that has only access to the messages sent on the public channel, and we say that the protocol is secure if there is no Eve that can find the key k efficiently. We know from the literature that such a protocol cannot exist in the plain model [IR89]. We also know that if given access to a public-key encryption scheme, Alice and Bob can build such a secure key exchange.On the other side, if Alice and Bob are given a one-way function, - a function that is easy to compute but hard to invert - no such protocol can be secure [IR89, BM08]. This is an important result because a one-way function is one of the lowest assumption that can be used in cryptography to give more power to Alice and Bob.

With access to quantum computers and the use of quantum communication, there is a known information-theoretically secure key exchange protocol [BB84] with no assumptions needed. However, the proof of the security of this protocol rest heavily on the *no-cloning* theorem, that states that we cannot copy a qubit. This theorem prevents Eve from storing the messages that are sent on the public *quantum* channel, thus limiting the possibilities of her attacks. Could Eve break the protocol if Alice and Bob were to use a classical channel, despite having access to quantum computers ? Because of the classical channel, the no-cloning theorem would be of no use here, and Eve will be able to act more freely. It is shown in [BHK$^+$11] that there is a lower bound of $O(n^{5/2})$ for such attacks. However, it is still unknown whether there exists an attack for Eve that can work efficiently for any key-exchange protocol with quantum parties but classical communication. This is the question we attempt to answer in this work. Our first result shows the impossibility of a secure key exchange with a quantum Alice and Bob that communicates through a classical channel, with no other assumption. Then, we show that with classical access to the oracle, the classical result can be adapted to prove the impossibility of secure quantum key exchange over a classical channel. Finally, we work towards proving the same result with quantum access to the oracle.

References

[BB84] Charles Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. volume 560, pages 175–179, 01 1984.

[BHK$^+$11] Gilles Brassard, Peter Høyer, Kassem Kalach, Marc Kaplan, Sophie Laplante, and Louis Salvail. Merkle puzzles in a quantum world. In Phillip Rogaway, editor, *Advances in Cryptology – CRYPTO 2011*, pages 391–410, Berlin, Heidelberg, 2011. Springer Berlin Heidelberg.

[BM08] Boaz Barak and Mohammad Mahmoody-Ghidary. Merkle puzzles are optimal. *CoRR*, abs/0801.3669, 2008.

[Gro97] Lov K. Grover. Quantum mechanics helps in searching for a needle in a haystack. *Physical Review Letters*, 79(2):325–328, Jul 1997.

[IR89] Russell Impagliazzo and Steven Rudich. Limits on the provable consequences of one-way permutations. In *STOC 1989*, 1989.