Composing quantum protocols

Dominic Mayers
Département de mathématiques et informatique
Université de Sherbrooke
2500 boul. Université
Sherbrooke, Québec
CANADA J1K 2K1

Abstract

We consider the general problem of proving the security of a quantum protocol which calls other quantum protocols. We adopt the natural extension of Canetti's work to the quantum world. Canetti's general security definition essentially states that a protocol P, which is a potential subprotocol, securely realises an ideal task T if any environment (an application protocol under any attack) cannot distinguish between a call to the protocol P and a call to the ideal task T. As an example, we will consider how the real QKD protocols securely realise the ideal QKD task. With such a definition, we naturally obtain that, if an application protocol $P2$ securely realises an ideal task $T2$ when it calls many ideal task $T1_i$, then it still securely realises $T2$ if it calls real protocols $P1_i$ that securely realise the ideal tasks $T1_i$, instead of calling these ideal tasks directly. The model for real and ideal quantum protocols is the natural extension of the corresponding classical circuit model. The proof techniques are the same as in the classical world.

In practice, if we adopt the general security definition that is proposed above, some protocols do not securely realise their respective ideal task. This is true in the classical case, but perhaps this problem is more interesting in the quantum world. For example, there exists a relativistic bit commitment protocol based on relativity. This protocol is not so convenient to use, but it is the only known way to restore unconditional security in quantum cryptography. We will show that this

relativistic bit commitment protocol securely realises some kind ideal bit commitment, but we will need to use a variation on the general security definition (which is perhaps less convenient than the original definition, but better than nothing).