Cryptology ePrint Archive: Report 2011/588

Revisiting Symmetric Incoherent Optimal Eavesdropping in BB84 Protocol

Arpita Maitra and Goutam Paul

Abstract: The famous BB84 protocol relies on the conjugate bases $Z=\{|0\rangle$, $|1\rangle\}$ and $X=\left\{|+\rangle,|-\rangle\right\}$, where $|+\rangle = \frac{|0 \rangle + |1\rangle}{\sqrt{2}}$ and $|-\rangle = \frac{|0 \rangle - |1\rangle}{\sqrt{2}}$. Fuchs et. al. (Phy. Rev. A, 1997) presented an optimal eavesdropping strategy on the four-state BB84 protocol. Later Bru\ss~ (Phys. Rev. Lett., 1998) described the use of the basis $\left\{\frac{|0 \rangle + i|1\rangle}{\sqrt{2}}, \frac{|0 \rangle - i|1\rangle}{\sqrt{2}}\right\}$ along with the above two to show that the BB84 protocol with three conjugate bases (six-state protocol) provides improved security. Bru\ss~ had also shown that for the six-state protocol, the mutual information between Alice (the sender) and Eve (the eavesdropper) is higher when two-bit probe is used compared to the one-bit probe and hence provides a stronger eavesdropping strategy. In this paper, we revisit the problem towards a critical and concrete analysis in terms of Eve's success probability in guessing the qubits that Alice has sent. In this regard, we show that though Eve has more success probability in the four state BB84 than in the six state BB84, within the six state protocol she has the same success probability in guessing the qubit transmitted by Alice in both the two-bit and the one-bit probe. Finally, we propose a model of multi-round BB84 protocol, in which the advantage of Eve can be reduced arbitrarily, and with proper choice of parameters, the multi-round four state protocol can be made more secure than the multi-round six state protocol.

Category / Keywords: Bias, Advantage, BB84 Protocol, Key Distribution, Optimal Eavesdropping, Quantum Communication, Quantum Cryptography, Sequence

Date: received 30 Oct 2011, last revised 18 Feb 2012

Contact author: goutam paul at ieee org