Weak Value Assisted Quantum Key Distribution

James Troupe[1] and Jacob Farinholt[2]

[1]Center for Quantum Research, Applied Research Laboratories, The University of Texas at Austin, Austin, TX 78713
[2]Strategic and Computing Systems Department, Naval Surface Warfare Center, Dahlgren Division, Dahlgren, VA 22448

A *weak measurement* is a special type of POVM that minimizes the measurement disturbance of the system being measured. While any one weak measurement provides effectively negligible information about the system, averaging weak measurement results over many copies of identically prepared systems provides useful information about an observable in the time interval between two projective measurements. Using the von Neumman representation of the measurement interaction between the measuring device (MD) and the system, we have:

$$\widehat{H}_{int} = g(t)\widehat{P}_{MD} \otimes \widehat{A}, \tag{1}$$

where $g(t)$ is the coupling strength as a function of time. If the time integrated coupling g is very small compared to the MD's position uncertainty, then the MD's position will yield little information about the observable $\widehat{A}$, and the system will be almost undisturbed. However, with a large enough ensemble of weak measurement results from identically prepared systems, we can estimate the value of $\widehat{A}$.

If we also condition the weak measurement results on identical post-selected states, then the resulting weak measurements yield access to the *weak value*, given by

$$A_w = \frac{\langle\psi_f|\widehat{A}|\psi_i\rangle}{\langle\psi_f|\psi_i\rangle}. \tag{2}$$

More generally, if the initial state is a density operator ρ_i, then the weak value will be given by

$$A_w = \frac{\mathrm{Tr}\left[|\psi_f\rangle\langle\psi_f|\widehat{A}\rho_i\right]}{\mathrm{Tr}\left[|\psi_f\rangle\langle\psi_f|\rho_i\right]}. \tag{3}$$

The conditional shift in the mean values of the weak measurement results for each pre- and post-selected (PPS) ensemble are given by $\mu = g \times \mathrm{Re}[A_w]$. [1] This shift in the MD pointer is linear in the coupling strength, while the probability of collapsing the system's initial state into an orthogonal state is reduced quadratically in the coupling.

Recently [2], the authors proposed augmenting the BB84 protocol with weak measurement steps, and using the weak measurement results in the cases for which Alice and Bob's bases disagree as a method of assessing security. In particular, for each state Alice transmits, Bob weakly measures one of four carefully selected observables prior to strongly measuring in one of the two bases. Afterwards, Bob reveals his basis choices, and for the subset for which Alice and Bob's bases disagree, Alice publicly reveals the state she transmitted.

Using the weak measurement results on this subset, Bob calculates the weak values conditioned on all of the possible PPS ensembles. From this information, it is possible for Bob to characterize the effects of the channel on each of the four states Alice transmits. This ultimately provides more information about the quantum channel than the standard methods for calculating the QBER, without the need to reveal any subset of the distilled raw key. In particular, because the weak values are conditioned on both the state of the system immediately prior to, and immediately following the weak measurement, it follows that this protocol is secure against detector blinding attacks.

In this poster, we plan to review the weak value augmented BB84 protocol proposed in [2] and expand on the channel noise estimates, ultimately showing how one may explicitly calculate the true QBER using only the weak measurement results from the subset of cases for which the bases disagree.

References

[1] Yakir Aharonov and Lev Vaidman. Properties of a quantum system during the time interval between two measurements. *Phys. Rev. A*, 41:11–20, Jan 1990.

[2] James Troupe and Jacob Farinholt. A contextuality based quantum key distribution protocol. *arXiv:1512.02256 [quant-ph]*, 2015.