BB84 Augmented with Weak Measurements and Immune to Detector Attacks

James Troupe

Applied Research Laboratories, University of Texas at Austin

A major obstacle to the use of QKD systems is the existence of physical implementation based side-channels that can compromise the security of the distributed keys. An important research area in QKD is the goal of Device Independent (DI-QKD) or Measurement Device Independent (MDI-QKD) QKD. The latter is particularly important as many of the side-channels demonstrated thus far rely on manipulation of the single photon detectors needed in BB84 based QKD systems.

The fundamental principle behind all detector based attacks is that the original BB84 protocol requires the assumption that the sample of raw key used to estimate the quantum bit error rate (QBER) of the channel is a fair sample of all of the signals sent from Alice to Bob. This is crucial since the estimated QBER is used to bound the amount of Eve's information about the raw key. Therefore, if Eve is able to violate the fair sampling assumption, she has the potential to evade detection and compromise the security of the final key. To maximize the key information available to her and to minimize the probability of her detection Eve should perform an intercept-resend attack on each photon and use her control of the detectors to make sure that Bob's detectors only report outcomes for photons where Eve and Bob's choice of measurement basis agree. This will give Eve the entire raw key without prodicing any errors in the sample used for estimating the QBER.

The QKD protocol proposed here uses the basic structure of BB84; however, the QBER of the channel is estimated using weak measurements of the observables used to encode the raw key information. In the situation where a system has been prepared in an initial state and post-selected in another final state, a sufficiently weak measurement at an intermediate time yields information about the weak value of the observable being weakly measured. Note that in general, the observables that are strongly measured to yield the initial and final states, as well as the observable being weakly measured, can be different for each other. The weak value of a quantum mechanical observable was introduced by Aharonov, *et al.* [1, 2] over two decades ago. The weak value is experimentally obtained from the result of measurements performed upon a pre-selected and post-selected (PPS) ensemble of quantum systems when the interaction between the measurement apparatus and each system is sufficiently weak. Unlike

the standard strong measurement of a quantum mechanical observable which disturbs the measured system and 'collapses' its state into an eigenstate of the observable, a weak measurement does not appreciably disturb the quantum system, and yields the weak value as the measured value of the observable. This is possible because very little information about the observable is extracted in a single weak measurement. Experimentally determining the weak value requires performing weak measurements on each member of a large ensemble of identical PPS systems and averaging the resulting values.

So, how do we use the weak measurements to detect Eve? Let us call the two bases used in the protocol X and Y. In the new protocol, in contrast to BB84, we keep the instances where Bob measures in a different basis from Alice's preparation. In all cases, immediately before Bob strongly measures each photon, i.e. the outcome of his detector, he weakly measures the photon in the opposite basis. For concreteness, let us say that Alice prepared the photon in an eigenstate of X, then Bob will perform a weak measurement of X on the photon and set his detectors to measure in the Y basis. Bob will then have a weak measurement result and a post-selection outcome for each photon. Because Bob's weak measurement is of the same observable used by Alice to encode the photon, the weak value must equal the eigenvalue of the state prepared by Alice. Therefore, if Alice tells Bob the initial eigenstate of each photon (remembering that this is only for cases where Alice and Bob's bases **disagree**), Bob can calculate the average of his weak measurement results conditional on the initial state. In a noise free channel these averages should yield weak values equal to the eigenvalues of the initial states. By using a large enough sample size Bob can use the strength of the correlation between the initial state and the weak measurement results to estimate the QBER of the channel.

Focusing on a detector based attack, we can see that the protocol will be effective in detecting Eve in the following way. Since Eve must correlate Bob's choice of basis with her own for all of the photon that are successfully detected by Bob, all of the photons that Bob weakly measures will have a **true** initial state that is equal to the final post-selected state. It can be easily shown that in all cases where the initial and final states are the same the weak measurement must yield the expectation value. In our example, the initial/final state is an eigenstate of X, while the observable being weakly measured is Y. Therefore, the conditional weak measurements will alway give zero. This is a reflection of the fact that Eve's intermediate strong measurement of the channel has completely uncorrelated Bob's weak measurement results from the initial state prepared by Alice. An important point is that with this protocol, Eve has actually made herseld much **more** detectable by utilizing the detector side-channel. If Eve had simply performed an intercept-resend attack on the channel Bob's conditional weak measurements would have only been attenuated by 50% instead of a full 100%.

The essential concept is that any channel noise, including that due to Eve, will manifest itself in the attenuation of Bob's conditional weak measurement results. In particular, even if Eve has control of Bob's detectors and weak measurement outcomes she cannot mimic the strength of correlation between

Bob's weak measurements and Alice's initial state because this state is unknown to her for each photon at the time that the measurement results are recorded by Bob.

In terms of practical implementation of the weak measurement augmented protocol, the only addition is the needed weak measurements at Bob's detection station. Similar weak measurements of photons have been performed regularly in many experiments, e.g. [3, 4]. An efficient way of perform the needed weak measurements is to utilize another degree of freedom of each of the photons such as it's transverse spatial wavefunction as the weak measurement "pointer" system. Weakly coupling this the additional degree of freedom to the observables used for encoding the key information provides the necessary weak measurement. An important requirement is that we must have access to and be able to strongly measure the pointer state associated with each photon in order to extract weak measurement results for each individual photon.

The main contribution of this work is to introduce a new method of performing QKD so that Bob's detectors do not have to be trusted. This new protocol has physical requirements very similar to BB84 and should lend itself to being integrated easily into QKD systems based on BB84. Because the protocol does not rely on entanglement or multi-photon interference as with other MDI-QKD approaches [5, 6], the secure key rate achievable with such a system should be comparable to that of BB84 based QKD systems while removing detector based side-channels.

References

[1] Y. Aharonov, D. Albert, and L. Vaidman, "How the result of a measurement of a component of spin of a spin-1/2 particle can turn out to be 100", *Physical Review Letters* **60**, 1351 (1988).

[2] Y. Aharonov and L. Vaidman, "Properties of a quantum system during the time interval between two measurements", *Physical Review A* **41**, 11 (1990).

[3] Lundeen and A. Steinberg, "Experimental Joint Weak Measurement on a Photon Pair as a Probe of Hardy's Paradox", *Physical Review Letters* **102**, 020404 (2009).

[4] Rozema, *et al.,* "Violation of Heisenberg's Measurement-Disturbance Rekationship by Weak Measurements", *Physical Review Letters* **109**, 100404 (2012).

[5] Valivarthi, *et al.*, "Measurement-device-independent quantum key distribution: from idea towards application", aXiv:1501.07307 (2015).

[6] Yan-Lin Tang, *et al.,* "Measurement-Device-Independent Quantum Key Distribution over 200 km", *Physical Review Letters* **113**, 190501 (2014).