Quantum Cryptography with Weak Measurements

James E. Troupe and Jacob M. Farinholt

Abstract

We present a new prepare-and-measure quantum key distribution protocol that decouples the necessary quantum channel error estimation from its dependency on the single photon detection outcomes, for example by comparing a subset of the sifted key as in BB84. Rather than estimating and bounding Eve's coupling to the quantum channel from the statistics of the sifted key, we infer this information from weak measurements made equally on all of the received photons immediately prior to post-selection by the photon detectors. A significant benefit of this approach to estimating the quantum bit error rate of the channel between Alice and Bob is that the estimate is completely independent of the basis chosen for Bob's detectors. In fact, our new QKD protocol only requires Bob to perform strong measurements (i.e. the usual qubit measurements) in a single basis, e.g. the Z basis. This means that the new QKD protocol is inherently immune to any detection based attacks that utilize single photon detector control to selectively bias the estimated quantum bit error rate, for example, as in the demonstrated detector blinding attacks of V. Makarov and others.

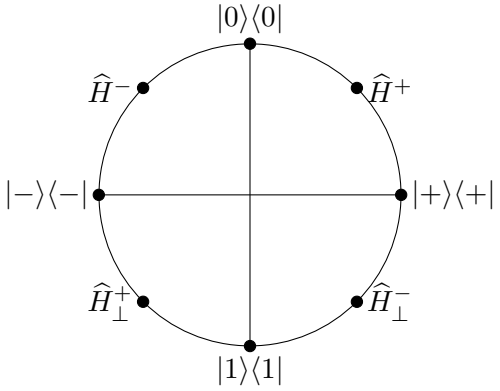

Figure 1: A view of the geometric relationship between the $\widehat{H}^\pm$ projectors that are weakly measured, their complements $\widehat{H}_\perp^\pm$, and the projectors onto the four states used in BB84.

In order to efficiently perform the channel estimation, the observables that are weakly measured are projections onto two of the four states equidistant from the four BB84 states (see Figure 1). If we assume that the noise on the quantum channel is unital, then the weak measurement results of any non-orthogonal pair of these four allows Alice and Bob to estimate the quantum bit error rate as well as estimate the coupling strength of the weak measurements themselves.[1] For concreteness

[1]By measuring all four of the projectors randomly, the unitality assumption can be replaced with the much weaker (and enforceable) assumption that the weak measurement coupling strengths of orthogonal pairs are equal.

	A WEAK MEASUREMENT QKD PROTOCOL
1	Alice generates a length $2n$ random string of bits $z \in \{0,1\}^{(2n)}$, encoding each bit in either the X or Z basis uniformly at random. Then she transmits each qubit to Bob.
2	Bob performs weak measurements of $\widehat{H}^+$ or $\widehat{H}^-$ chosen uniformly at random on each signal he receives, then he strongly measures in the Z basis, recording both of his measurement results.
3	Bob openly shares the weak measurement results with Alice, who uses them to estimate the bit and phase error rates. Alice also uses the weak measurement results to estimate and place bounds on the weak measurement coupling strength and the uncertainty of the weak measurement pointer states.
4	If the error rates are too high, the weak measurement strength exceeds a security parameter, or the weak measurement pointer uncertainty is too large, Alice aborts the protocol. Otherwise, she announces which signals were prepared in the Z basis. Alice and Bob perform classical post-processing on these signals to correct the errors and distill a smaller, length k secure key.

Table 1: Outline of a QKD protocol with weak measurements.

we will define the two projectors used in the protocol to be the pair of states to each side of the $+1$ eigenstate of Z, $|0\rangle$. The basic form of the protocol is given in Table 1.

The price paid for using weak measurements to perform estimation of the bit and phase errors of the quantum channel is that these weak measurements will themselves add to the error rate of the channel due to measurement disturbance. However, even for realistic, finite coupling strengths, the weak measurement induced error rate can be made significantly less than 0.1%. Thus, the secure key rate is very minimally affected. Additionally, we do not need to use any of the raw key to perform error estimation as in other QKD protocols.

We show that the new protocol is robust against imperfection in the quantum state of the source and errors in the weak measurement interaction – both biased and random noise in the projection observables. Additionally, we have shown that the protocol is still secure even if Eve completely controls the weak measurement outcomes as long as (1) Eve does not have the ability to interact with the photons between the weak measurement interaction and the final strong Z measurement, and (2) Eve has limited information about which observable was measured for each photon. Note that the distance between the weak measurement interaction and photon detector can be extremely short and is contained entirely within Bob's measurement device.

The full version of the protocol adds the use of decoy states to ensure security against photon number splitting attacks when using weak coherent pulse sources. We compare the asymptotic secure key rate of the decoy state WM protocol to decoy state BB84 (see Fig. 2) and MDI-QKD (see Fig. 3). The performance of the new protocol is essentially identical to that of BB84 – without the vulnerability to detector blinding – and is significantly higher than that of MDI-QKD. In particular, we see that the WM protocol is far more robust to variations in intrinsic noise than MDI-QKD. While we do not claim that the protocol is "Measurement Device Independent," we do believe that it comes as close as is possible for a prepare-and-measure protocol. By completely removing detector blinding and control as an attack method and providing continuous monitoring of the channel parameters and verification of the weak measurement interaction implementation, the protocol can enable a very significant increase in the security of practical prepare and measure QKD systems. For full details please see `https://arxiv.org/abs/1702.04836`.

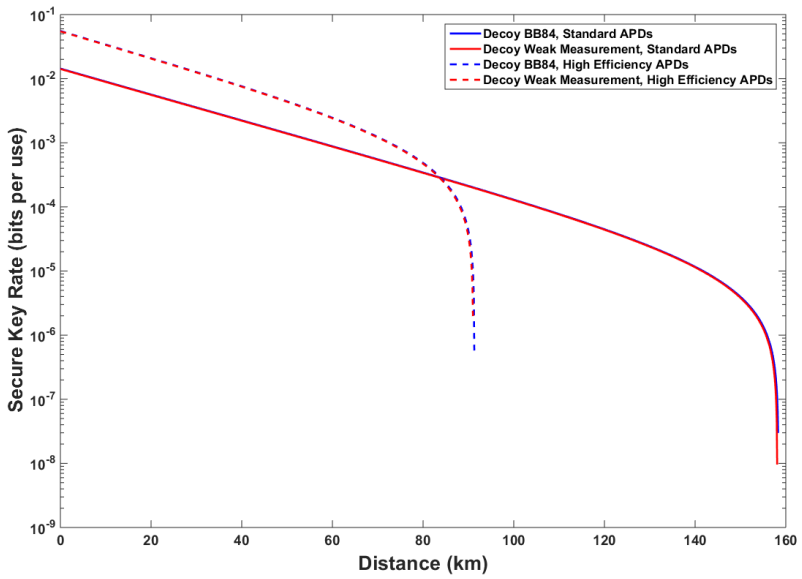

Figure 2: Comparison of secure key rates of Weak Measurement and BB84 protocols, both with Weak+Vacuum decoy states. The pulse intensities for each protocol are $\mu = 0.48$, $\nu = 0.05$, channel loss rate is 0.2 dB/km, and error reconciliation factor is $f = 1.22$. Solid lines use measurement devices with with total detection efficiency $\eta_d = 0.145$ and vacuum count rate $Y_0 = 6 \times 10^{-6}$. For dotted lines, $\eta_d = 0.55$ and $Y_0 = 5 \times 10^{-4}$. The weak measurement strength is $\sigma/g = 0.05$. The system intrinsic error rate in both cases is 1.5%.

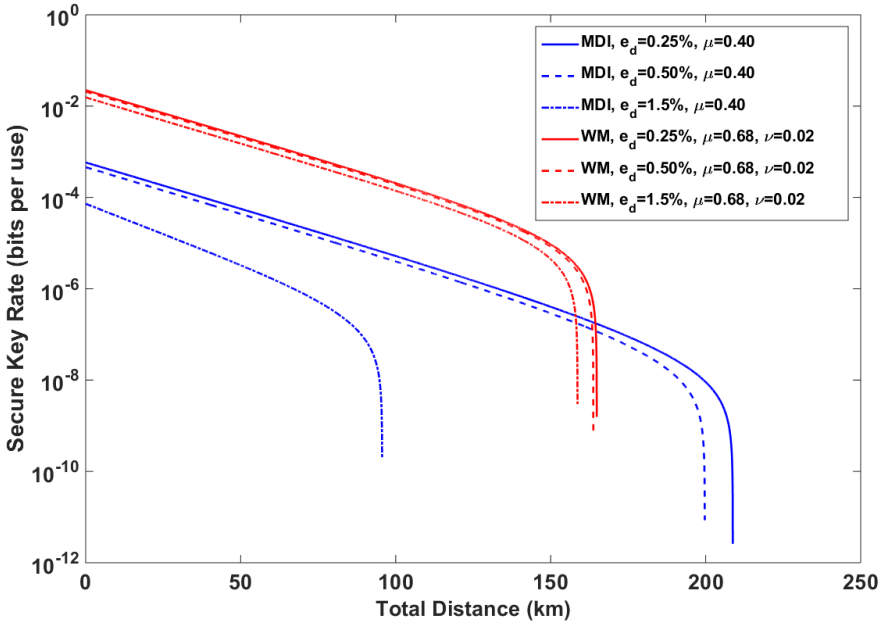

Figure 3: This figure shows the stability of WM-QKD as compared to MDI-QKD under increases in the intrinsic system error rate. The total detection efficiency is 14.5%, the channel loss rate is 0.2 dB/km, and the error reconciliation factor is $f = 1.16$.