Loss-tolerant QKD with a twist

J. Eli Bourassa*, Ignatius William Primaatmaja, Charles Ci Wen Lim, Hoi-Kwong Lo
arXiv:2007.08299, *bourassa@physics.utoronto.ca

Introduction

Measurement device-independent quantum key distribution (MDI QKD) protocols allow two distant parties, Alice and Bob, to distribute a shared, secret cryptographic key, even in the presence of an eavesdropper, Eve, who has complete control of their quantum channels and the measurement devices employed in the protocol [1, 2]. Typically, Alice and Bob prepare a set of signal states, send them to a central measurement node potentially controlled by Eve, which then makes an announcement based on a measurement it may or may not have faithfully executed. The cost of the information-theoretic security in such a setting is that Alice and Bob need to trust and characterize the optical sources they employ to send signals to the measurement devices. Thus, a proper understanding of the source features and flaws, and knowing how to account for them in a security proof is especially valuable for quantifying the key rates offered by an MDI protocol.

In this work, we answer a seemingly simple question: how do you construct a security proof for an MDI QKD protocol that employs trusted, yet noisy – i.e. mixed – signal states, given that Eve may not hold the purification of the mixture? In the case state preparation noise can be trusted and characterized, but perhaps not reduced, we provide here a simple analytical and numerical toolbox for calculating an optimal secret key rate. Concentrating on the qubit signal state case, we find that the mixed states can be interpreted as providing Alice and Bob with a virtual shield system they can employ to reduce Eve's knowledge of the secret key. We then introduce a simple semidefinite programming method for optimizing the virtual twisting operations they can perform on the shield system to yield a higher key rate, along with an example calculation of fundamentally achievable key rates in the case of random polarization modulation error.

Background

Loss-tolerant QKD

The loss-tolerant protocol [3] uses basis mismatch statistics to infer phase error rates that cannot be directly observed in the case state preparation is non-ideal. In the tilted four state protocol, Alice and Bob each prepare four mixed qubit signal states $\{\rho_A^{i,x}\}$ and $\{\sigma_B^{j,y}\}$, that they will send respectively with probabilities $p^{i,x}$and $q^{j,y}$ to the central measurement node controlled by Eve. When Alice and Bob choose $(i,j)=(0,0)$ these are the key generation states, with (x,y) corresponding to their key bit values. Following the security proof of the loss tolerant protocol, we require that the sets of states $\{\rho_A^{i,x}\}$ and $\{\sigma_B^{j,y}\}$ each form a tetrahedron on the Bloch sphere, meaning the Bloch vectors cannot all lie in the same plane [3].

In our reframing of the loss-tolerant proof technique, we show how the initial states and detection probabilities are sufficient to solve for the Gramian matrix of Eve's system, which contains all the parameters required for calculation of the key rate formula from the six-state protocol, even with the inclusion of twisting operations.

Twisting operations

Typically, the security of QKD is analyzed in terms of Alice and Bob's ability to virtually distill maximally entangled EPR pairs, since measurement of such pairs yields perfectly correlated keys, and by the monogamy of entanglement, the results cannot be correlated with anyone else, including Eve. However, it is known that a larger class of states known as private states [4-7] are fundamentally what is required to produce secret key. Formally, private states can be constructed from an EPR pair if Alice and Bob take ancillary shield systems they control, and apply a "twisting" unitary operation between the EPR pair and the shields, the condition being that this twisting leave unaffected the measurement results that generate secret key. Since twisting does not change the key, private states can then be understood as deflecting some of Eve's attack on the systems that generate key to the shield systems. See Fig. 1 for a diagram of this concept.

In our technique, we show that the mixing noise of the signal states can be treated in a virtual picture as being equivalent to Alice and Bob employing shield systems that can be used to decrease Eve's knowledge of the key. Completely within this virtual picture, we can apply unitary twisting operations to the shields to decrease the phase errors of the protocol, increasing the secret key rate. We provide simple semi-definite programs to find the optimal twisting operations, yielding the optimal key rate under this framework.

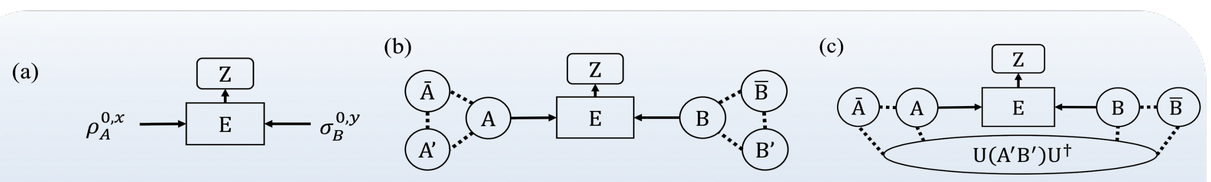

Fig. 1 – (a) A real MDI QKD protocol: Alice and Bob each prepare mixed states associated with bit (x,y) and basis (i,j) values. They send their states to a central node controlled by Eve, who makes an announcement Z. (b) A virtual version of the key generation states in the protocol: in a purified picture, Alice and Bob's mixed signal states are entangled with virtual qubits $\bar{A},\bar{B}$ which coherently store the bit values (x,y). Measurement of $\bar{A},\bar{B}$ in the computational basis yields the raw keys. The A,B systems are additionally purified by the A',B' systems to account for trusted noise in the source. Only the A,B systems are sent to Eve. (c) An alternative virtual purification: all purifications are related by unitary operations applied to, in general, a joint purifying ancilla, yielding private states in $\bar{A}\bar{B}A'B'$. These "twisting" operations can optimally boost the secret key rate as they can modify the phase error rates which Alice and Bob need to estimate. In (a)–(c), the signal states sent and the observed protocol statistics (detection and bit error rates) are the same.

Characterizing Eve's system

Our reframing of the loss-tolerant protocol proof technique can be summarized as:

1. Alice and Bob prepare the 16 states: $\rho_A^{i,x}\sigma_B^{j,y}=\sum_{\substack{m,m',\\ n,n'=H}}^{V} c_{m,m'}^{i,x}d_{n,n'}^{j,y}\,|m,n\rangle\langle m',n'|_{A,B}$
2. These states evolve to Eve and an announcement: $|m,n\rangle_{A,B}\rightarrow\sum_{z=P}^{F}|e_{m,n}^{z}\rangle_E|z\rangle_Z$
3. The detection probability impose constraints:

$$p_{det}^{i,j,x,y}=p(z=P|i,j,x,y)=p^{i,x}q^{j,y}\sum_{\substack{m,m',\\ n,n'=H}}^{V} c_{m,m'}^{i,x}d_{n,n'}^{j,y}\,\langle e_{m',n'}^{P}|e_{m,n}^{P}\rangle_E$$

4. Solve for Eve's Gramian matrix:

$$\vec{p}_{det}=\hat{\gamma}\vec{e}\implies\vec{e}=\hat{\gamma}^{-1}\vec{p}_{det}$$

$(\vec{p}_{det})_t=p_{det}^{i,j,x,y}$ — Detection probs.
$\hat{\gamma}_{ts}=p^{i,x}q^{j,y}c_{m,m'}^{i,x}d_{n,n'}^{j,y}$ — State information
$\vec{e}_s=\langle e_{m',n'}^{P}|e_{m,n}^{P}\rangle_E$ — Eve's Gramian

Optimal choice of virtual protocol

The key generation states, $p^{0,x}q^{0,y}\rho_A^{0,x}\sigma_B^{0,y}$ can be considered virtually:

$$|\zeta\rangle=\sum_{x,y}|x,y\rangle_{\bar{A}\bar{B}}\sum_{m,n=H}^{V}|\gamma_{m,n}^{x,y}\rangle_{A'B'}|m,n\rangle_{AB}$$

where we have constraints $\left\langle\gamma_{m',n'}^{x,y}\middle|\gamma_{m,n}^{x,y}\right\rangle_{A'B'}=p^{0,x}q^{0,y}c_{m,m'}^{0,x}d_{n,n'}^{0,y}$, since to generate key, Alice and Bob measure $\bar{A},\bar{B}$ in the computational basis. This purification is not unique, and so we have freedom to choose the virtual picture that yields the optimal key rate. Since Eve does not have access to $A'B'$ any purification will yield a suitable lower bound on the key rate.

We can parametrize all purifications using twisting unitary operations [4-7] applied to the virtual ancillary systems in $|\zeta\rangle$:

$$U_{\bar{A}\bar{B}A'B'}=\sum_{x,y=0}^{1}|x,y\rangle\langle x,y|_{\bar{A}\bar{B}}\otimes U_{A'B'}^{x,y}$$

Such an operation is entirely virtual, so it can be nonlocal in general and never needs to be executed in the real protocol.

To quantify the security, we employ the key rate formula from the six-state protocol [8-10]:

$$R_6=p_{det}^{0,0}\left(1-h_2(e_Z)-e_Zh_2\left[\frac{1+(e_X-e_Y)/e_Z}{2}\right]-(1-e_Z)h_2\left[\frac{1-(e_X+e_Y+e_Z)/2}{1-e_Z}\right]\right)$$

We find that the linear combinations $e_\pm=e_X\pm e_Y$ are linear functions with respect to the elements of Eve's Gramian matrix $\langle e_{m',n'}^{P}|e_{m,n}^{P}\rangle_E$, which are already known, as well as with respect to matrix elements $\left\langle\gamma_{m',n'}^{x',y'}\middle|U_{A'B'}^{x',y'\dagger}U_{A'B'}^{x,y}\middle|\gamma_{m,n}^{x,y}\right\rangle_{A'B'}$, the Gramian matrix of the twisted ancillary system states. Since our task is to modify the twisting operation to boost the key rate, these latter elements form the optimization variables of our problem.

Moreover, we find that e_+ only depends on $\mathrm{U}_+=U_{A'B'}^{0,0\dagger}U_{A'B'}^{1,1}$, and e_- only depends on $\mathrm{U}_-=U_{A'B'}^{0,1\dagger}U_{A'B'}^{1,0}$. Since the $U_{A'B'}^{x,y}$ can be defined independently of each other, the optimization of e_+ can be decoupled from the optimization of e_-, so we can overcome the nonlinearity introduced by $h_2(\cdot)$.

Taking stock, we have two independent objective functions $e_\pm$, which are linear with respect to the Gramian matrix of the ancillae, which is a positive semidefinite matrix by construction. Thus, these optimization problems take the form of semidefinite programs which can be solved numerically on a standard laptop in a few seconds using available packages for Python [11-12]. While previous literature on twisting operations had noted the opportunity for optimizing U [7], no explicit procedure was constructed. Here, we have closed this gap, increasing the practicality of utilizing a virtual twisting operation as a step in the security proof.

Example: random modulation error

As a study of fundamentally achievable key rates, we consider the following two-parameter (δ,p)-model for the initial states. We suppose Alice and Bob attempt to prepare the states $\{|H\rangle,|V\rangle,(|H\rangle+|V\rangle)/\sqrt{2},(|H\rangle-i|V\rangle)/\sqrt{2}\}$; however, each state is subject to a modulation error which we treat as a random variable. The resulting average states can be treated as having a constant offset angle from the ideal Bloch vector, parametrized by δ, as well as a depolarization noise parametrized by p, which shortens the Bloch vector and introduces incoherent mixing to the states.

In Fig. 2, we plot the asymptotic key rate found using our technique as a function of distance for various pairs (δ,p). We assume a Bell state detection scheme similar to [1], with overall detection efficiency of 50%, a dark count probability of 10^{-5} per pulse per detector, loss in fiber of 0.2 dB/km, and error correction efficiency of 1. For comparison with the key rate produced with our optimization, we plot the key rate calculated using a suboptimal purification, which was constructed by simply diagonalizing Alice and Bob's signal states and having the ancillary systems index the eigenvalues in decreasing order. We find that our technique provides a modest increase over the "naïve" purification one could have chosen, our technique's advantages being most significant as the depolarizing noise gets stronger (making the initial states more mixed), and at longer distances when the untrusted channel noises (loss and dark counts) accrue. Additionally, we see a better key rate can be produced by physically reducing state preparation noise; however, once one has improved the real states as best as possible, our technique provides confidence that one has optimized over all possible ancillary states of the purification that are consistent with the protocol statistics without worry that one has chosen a pessimistic virtual picture.

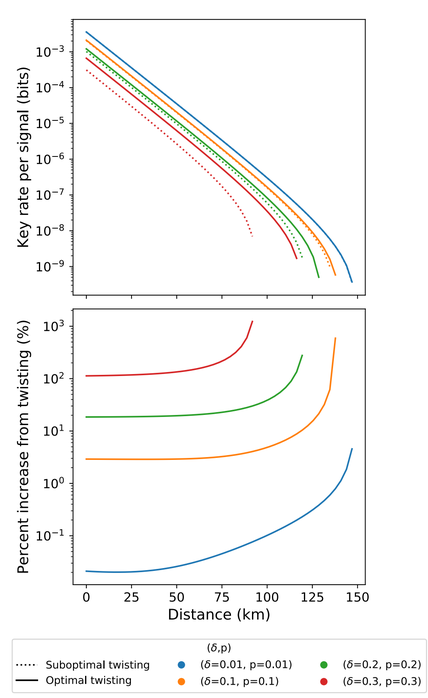

Fig. 2 – Key rate calculations for state preparation with random polarization modulation error

References

1. H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. 108, 130503 (2012).
2. S. L. Braunstein and S. Pirandola, Phys. Rev. Lett. 108, 130502 (2012).
3. K. Tamaki, M. Curty, G. Kato, H.-K. Lo, and K. Azuma, Phys. Rev. A 90, 052314 (2014).
4. K. Horodecki, M. Horodecki, P. Horodecki, D. Leung, and J. Oppenheim, Phys. Rev. Lett. 100, 110502 (2008).
5. K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, IEEE Transactions on Information Theory 55,1898 (2009).
6. J. M. Renes and G. Smith, Phys. Rev. Lett. 98, 020502 (2007).
7. K. Horodecki, M. Horodecki, P. Horodecki, D. Leung, and J. Oppenheim, IEEE Transactions on Information Theory 54, 2604 (2008).
8. H.-K. Lo, Quantum Info. Comput. 1, 8194 (2001).
9. R. Renner, "Security of quantum key distribution," (2005), arXiv:quant-ph/0512258.
10. V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lutkenhaus, and M. Peev, Rev. Mod. Phys. 81, 1301 (2009).
11. S. Diamond and S. Boyd, Journal of Machine Learning Research 17, 1 (2016).
12. A. Agrawal, R. Verschueren, S. Diamond, and S. Boyd, Journal of Control and Decision 5, 42 (2018).