Quantum Cryptography with local Bell tests

Charles Ci Wen Lim,[1,*] Christopher Portmann,[1,2] Marco Tomamichel,[2,3] Renato Renner,[2] and Nicolas Gisin[1]

[1] *Group of Applied Physics, University of Geneva, Switzerland.*
[2] *Institute for Theoretical Physics, ETH Zurich, Switzerland.*
[3] *Centre for Quantum Technologies, National University of Singapore, Singapore.*

FORMULATION OF PROBLEM

Quantum key distribution (QKD) has progressed much in both theory and practice [1]: various security proof techniques have been developed and milestones have been achieved in field tests. However, the gap between theory and practice has not been completely bridged. This impasse comes from the fact that the theoretical device models used by most security proof techniques often do not characterize the actual devices fully, and as a result, most security proofs do not apply. An immediate solution is to carefully characterize actual devices against theoretical models and include the discrepancies into the security analysis [2]. However, the task of characterizing an actual device is not trivial, as there are many ways a device can go wrong. As such, an incomplete characterization of actual devices is likely and this may be exploited by the adversary to break the security. Apart from the arduous task of identifying all possible discrepancies, we also have to consider the impact of including the additional parameters into the finite-key security analysis [3–6]. For instance, if the number of discrepancies is large, then the additional parameters required to characterize the discrepancies, together with its statistical fluctuations due to finite sample sizes, are likely to penalize the security performances. Therefore for practical quantum cryptography, it is of great interest to consider a paradigm shift in the assessment of security, namely a method that is able to tackle all possible discrepancies between theory and practice and compress it into a small number of parameters.

RESULTS

We propose the concept of self-testing QKD which is based on a novel local self-testing method [7]. In particular, devices are tested locally independent of the quantum channel, that is, Alice and Bob perform Clauser-Horne-Shimony-Holt (CHSH) tests on their own devices, independent of each other and the quantum channel (including the channel loss). As a result, the quantum channel is not included in CHSH test. Furthermore, our protocol adopts a tripartite model, that is, we introduce an additional party Charlie—not necessarily trusted by Alice and Bob—whose task is to perform a quantum exchange (similar to entanglement swapping) on the states sent by Alice and Bob and communicates the outcome pass or fail to them. Then, the security assessment of the quantum channel follows the channel estimation technique of BB84 QKD protocol, i.e., checking for errors in the bases X and Z. Therefore, by deriving the relation between CHSH test and a recent security proof technique (the smooth version of entropic uncertainty relation [6, 8, 9]), the finite-key security proof is obtained under the following assumptions:

1. Alice and Bob localities are secure.
2. Quantum devices do not have internal classical or quantum memories.
3. Alice and Bob have access to trusted classical devices like calculators and local trusted sources of randomness.
4. Alice and Bob have access to an authenticated, but otherwise insecure classical channel.
5. The marginal states remaining at Alice and Bob localities are independent of whether Charlie's quantum exchange passes or fails

Furthermore, our result—a lower bound on the secret key rate—is intuitively related to the almost tight finite-key analysis [6] of BB84 QKD protocol and it differs only by a term that is dependent on the CHSH value.

In this submission, we provide our protocol definition, the basic ideas behind the security and the finite-key simulation results. The technical results (including the bound on the secret key rate) are provided in the supplementary information.

Related Work. The main difference between self-testing QKD and device-independent QKD [10–13] lies in the use of CHSH test, in particular, we use it to test devices locally while they use it to test both the quantum channel and devices. Accordingly, self-testing QKD offers a more refined security assessment as compared to device-independent QKD.

Details

We start by defining the network topology of self-testing QKD which adopts the tripartite concept model of side-channel-free QKD [14, 15]. More specifically, the tripartite concept model involves three parties: Alice and

Bob want to perform quantum cryptography, while Charlie plays the role of a quantum exchange akin to a telephone exchange that connects phone calls. At the quantum level, Alice and Bob are connected to Charlie via unspecified quantum channels, e.g., optical fibers provided by Charlie or someone else. On the classical level, Alice and Bob are connected via an authenticated, but otherwise insecure classical channel, in addition, they also receive radio broadcasts from Charlie.

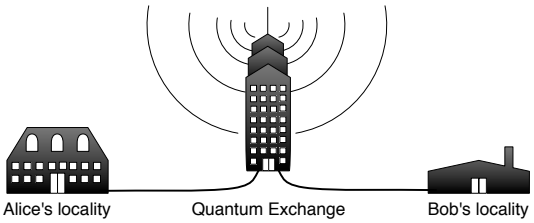

FIG. 1. **Quantum exchange**. Alice and Bob each send a quantum state to Charlie. Then, Charlie is supposed to make a quantum measurement on the quantum states and broadcast the outcome $\{\text{pass}, \text{fail}\}$ to both Alice and Bob. If the outcome is successful, Alice and Bob share an entangled quantum channel.

The role of Charlie as a quantum exchange is to establish an entangled quantum channel between Alice and Bob and this is accomplished by making a quantum measurement on the quantum states sent by Alice and Bob and communicating the outcome to them. Ideally, quantum exchange corresponds to entanglement swapping. Furthermore, quantum exchange also acts like a "Hilbert space filter" [16], filtering out all probing type side-channels, be it quantum or classical.

Next, we discuss the procedure for Alice. The same holds for Bob. The locality—typically a laboratory—of Alice is assumed to be secure, that is to say, leakage of unauthorized information is forbidden. Inside the secure locality, there are three devices: a source that claims to produce bipartite maximally entangled states and two measurement devices. The first measurement device has two settings $\{\mathsf{Z}, \mathsf{X}\}$ with binary outputs and the second measurement has three settings $\{\mathsf{U}, \mathsf{V}, \mathsf{P}\}$ where the first two settings produce binary outputs and the last setting allows Alice to keep one half and sends the other half of the bipartite state to Charlie.

By arranging the devices according to the self-testing setup [7], Alice has two choices, namely she can either select P and let one half of the bipartite state be sent to Charlie via the quantum channel or use the settings U, V to make a CHSH test. We refer to the former as sub-protocol Γ_{QKD} and the latter as sub-protocol Γ_{CHSH}.

The purpose of making a CHSH test is to enforce the uncertainty principle under minimal assumptions. More precisely, suppose Alice wants to generate a secret key from basis X and use basis Z for channel error rate estimation. Then from the entropic uncertainty relation [**?**

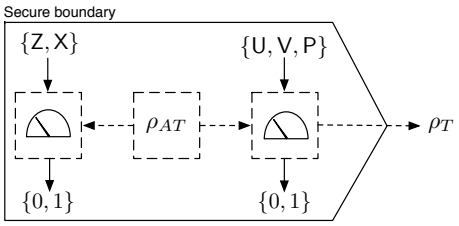

FIG. 2. **Schematic of self-testing setup**. Devices with dashed boundary represent untrusted devices. Note that the marginal state ρ_A is assumed to be independent of quantum exchange outcome.

], we know that the security of the key depends on the relationship between the quantum measurements corresponding to bases X and Z. If the quantum measurements commute, then keys generated from basis X cannot be secure. On the other hand, commuting quantum measurements cannot be used to violate CHSH inequality, in fact, the optimal CHSH value is necessarily given by anti-commuting quantum measurements [17]. This brings us to our first result which is a statement about the relation between CHSH test and the entropic uncertainty relation[1]. Roughly speaking, we bound the relationship of the quantum measurements corresponding to bases X and Z with the CHSH test that uses the same quantum measurements, which in turn allows us to bound the security.

In the following, we describe a single iteration of sub-protocols Γ_{QKD} and Γ_{CHSH}, i.e., the ith iteration. For sub-protocol Γ_{QKD} we adopt asymmetric encoding, that is, Alice selects a measurement setting $a_i \in \{\mathsf{X}, \mathsf{Z}\}$ with probabilities p_x and $1-p_x$, respectively, measures one half of the bipartite state with it and stores the measurement output in y_i. The other half of the bipartite system is sent to Charlie via a quantum channel. For sub-protocol Γ_{CHSH}, Alice measures the bipartite state using measurement settings chosen uniformly at random—she chooses two bit values u_i, v_i uniformly at random, where $u_i = 0$, $u_i = 1$, $v_i = 0$ and $v_i = 1$ correspond to measurement settings X, Z, U and V. Then, the outputs of X, Z and U, V are recorded in s_i and t_i, respectively.

Protocol definition

1. State preparation and distribution. Alice selects a sub-protocol $h_i \in \{\Gamma_{\text{QKD}}, \Gamma_{\text{CHSH}}\}$ where Γ_{QKD} is selected with probability $1 - p_s$ and Γ_{CHSH} with probability p_s. The measurement settings and outputs for Γ_{QKD} and Γ_{CHSH} are recorded in a_i, y_i

[1] Such a relation has also been obtained independently with a different proof technique (see Ref [7])

and u_i, v_i, s_i, t_i, respectively. Likewise, Bob records his choice of sub-protocol in h'_i and his measurement settings and outputs for sub-protocols Γ_{QKD} and Γ_{CHSH} in b_i, y'_i and u'_i, v'_i, s'_i, t'_i, respectively.

2. Quantum exchange. The Charlie receives quantum states from Alice and Bob, makes a quantum measurement which supposedly produces entanglement between Alice and Bob.

3. Sifting. Alice and Bob announce their sub-protocol and basis choices $\{h_i\}_i$, $\{h'_i\}_i$,$\{a_i\}_i$, $\{b_i\}_i$ over an authenticated classical channel and identify four sets,

1. Key generation, $\mathcal{X} := \{i : (h_i = h'_i = \Gamma_{\text{QKD}}) \wedge (a_i = b_i = \mathsf{X}) \wedge (f_i = \text{pass})\}$
2. Error rate estimation, $\mathcal{Z} := \{i : (h_i = h'_i = \Gamma_{\text{QKD}}) \wedge (a_i = b_i = \mathsf{Z}) \wedge (f_i = \text{pass})\}$
3. Alice and Bob CHSH test sets, $\mathcal{J} := \{i : h_i = \Gamma_{\text{CHSH}}\}$ and $\mathcal{J}' := \{i : h'_i = \mathsf{B}\}$, respectively.

The protocol repeats steps (1)-(3) as long as $|\mathcal{X}| < m_x$ or $|\mathcal{Z}| < m_z$ or $|\mathcal{J}| < j$ or $|\mathcal{J}'| < j$, where $m_x, m_z, j \in \mathbb{N}_1$. We refer to these conditions as the sifting condition.

4. Parameter estimation. To compute the average CHSH value from $\mathcal{J}$, Alice uses the following formula, $S_{\text{test}} := 8 \sum_{i\in\mathcal{J}} f(u_i, v_i|s_i, t_i)/|\mathcal{J}| - 4$, where $f(u_i, v_i|s_i, t_i) = 1$ if $s_i \oplus t_i = u_i \wedge v_i$, otherwise $f(u_i, v_i|s_i, t_i) = 0$. Similarly, Bob uses the same formula and arrives at S'_{test}. Next, both Alice and Bob publicly announce the corresponding bit strings $\{y_i\}_{i\in\mathcal{Z}}$, $\{y'_i\}_{i\in\mathcal{Z}}$ and compute the average error rate $Q_{\text{test}} := \sum_{i\in\mathcal{Z}} y_i \oplus y'_i/|\mathcal{Z}|$. If $\max\{S_{\text{test}}, S'_{\text{test}}\} < S_{\text{tol}}$ or $Q_{\text{tol}} < Q_{\text{test}}$, they abort the protocol.

5. One-way classical post-processing. Alice and Bob choose a random subset of size m_x of $\mathcal{X}$ for classical post-processing, and we let X and X' be random variables that taking the values from the corresponding strings $\{y_i\}_i$ and $\{y'_i\}_i$. Then, an information reconciliation scheme is applied, revealing at most leak_{IR}-bits of information. Finally, Alice and Bob apply privacy amplification to their bit strings to obtain a secret key of length ℓ.

Simulation results

For the simulation, we assume that the quantum channel is given by a depolarizing channel with channel error rate Q_{tol}.

From Figure 3, we observe that significant secret key rates are obtained from classical post-processing block size in the order 10^5 bits.

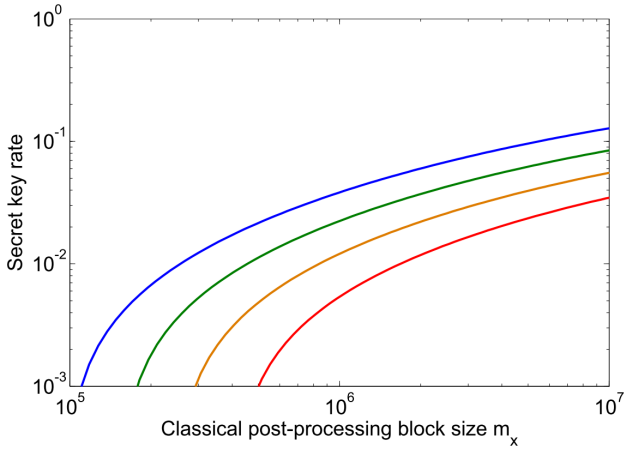

FIG. 3. **Secret key rate as a function of classical post-processing block size.** For a fixed channel error rate of $Q_{\text{tol}} = 1.5\%$, we plot the secret key rate for $S_{\text{tol}} \in \{2.825, 2.800, 2.775, 2.750\}$ from left to right. Note that in practice, S_{tol} depends only on quality of the source and the measurements, and is independent of the channel loss. In fact, CHSH value of around 2.81 was reported [**?**]

* ciwen.lim@unige.ch

[1] Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J Cerf, Miloslav Dušek, Norbert Lütkenhaus, and Momtchil Peev. The security of practical quantum key distribution. *Reviews of Modern Physics*, 81(3):1301–1350, 2009.

[2] Daniel Gottesman, Hoi-Kwong Lo, Norbert Lütkenhaus, and John Preskill. Security of quantum key distribution with imperfect devices. page 22, December 2002.

[3] Valerio Scarani and Renato Renner. Quantum Cryptography with Finite Resources: Unconditional Security Bound for Discrete-Variable Protocols with One-Way Postprocessing. *Phys. Rev. Lett.*, 100(20):200501, May 2008.

[4] Lana Sheridan, Thinh Phuc Le, and Valerio Scarani. Finite-key security against coherent attacks in quantum key distribution. *New Journal of Physics*, 12(12):123019, 2010.

[5] Masahito Hayashi and Toyohiro Tsurumaru. Simple and Tight Security Analysis of the Bennett-Brassard 1984 Protocol with Finite Key Lengths. page 9, July 2011.

[6] Marco Tomamichel, Charles Ci Wen Lim, Nicolas Gisin, and Renato Renner. Tight finite-key analysis for quantum cryptography. *Nat Commun*, 3:634, January 2012.

[7] Esther Hänggi and Marco Tomamichel. The Link between Uncertainty Relations and Non-Locality. *Physical Review*, pages 1–10, 2011.

[8] Mario Berta, Matthias Christandl, Roger Colbeck, Joseph M Renes, and Renato Renner. The uncertainty principle in the presence of quantum memory. *Nat. Phys.*, 6(9):659–662, July 2010.

[9] Marco Tomamichel and Renato Renner. Uncertainty relation for smooth entropies. *Physical Review Letters*, 106(11):110506, 2010.

[10] Artur K Ekert. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.*, 67(6):661–663, August 1991.

[11] Stefano Pironio, Antonio Acín, Nicolas Brunner, Nicolas Gisin, Serge Massar, and Valerio Scarani. Device-Independent Quantum Key Distribution Secure Against Collective Attacks. *New J. Phys.*, 11(4):45021, 2009.

[12] Esther Hänggi, Renato Renner, and Stefan Wolf. Efficient device-independent quantum cryptography. In *Advances in Cryptography — EUROCRYPT*, volume 6110 of *LNCS (Springer)*, pages 216–234, 2010.

[13] Lluis Masanes, Stefano Pironio, and Antonio Acin. Secure device-independent quantum key distribution with causally independent measurement devices. *Nature communications*, 2:13, 2010.

[14] Samuel L Braunstein and Stefano Pirandola. Side-Channel-Free Quantum Key Distribution. *Physical Review Letters*, 108(13):130502, March 2012.

[15] Hoi-Kwong Lo, Marcos Curty, and Bing Qi. Measurement-Device-Independent Quantum Key Distribution. *Physical Review Letters*, 108(13):130503, March 2012.

[16] Hoi-Kwong Lo and H F Chau. Unconditional Security Of Quantum Key Distribution Over Arbitrarily Long Distances. *Science*, 283(5410):2050–2056, 1998.

[17] Michael Seevinck and Jos Uffink. Local commutativity versus Bell inequality violation for entangled states and versus non-violation for separable states. *Phys. Rev. A*, 76(4), 2007.