AFRL-AFOSR-JP-TR-2020-0003

Practical Quantum Cryptography with Ultra-High Encryption Rates

Ci Wen Lim
NATIONAL UNIVERSITY OF SINGAPORE
21 LOWER KENT RIDGE ROAD
SINGAPORE, 119077
SG

06/12/2020
Final Report

Air Force Research Laboratory
Air Force Office of Scientific Research
Asian Office of Aerospace Research and Development
Unit 45002, APO AP 96338-5002

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
12-06-2020	Final	01 Jul 2018 to 31 Dec 2019

4. TITLE AND SUBTITLE
Practical Quantum Cryptography with Ultra-High Encryption Rates

5a. CONTRACT NUMBER

5b. GRANT NUMBER
FA2386-18-1-4033

5c. PROGRAM ELEMENT NUMBER
61102F

6. AUTHOR(S)
Ci Wen Lim

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
NATIONAL UNIVERSITY OF SINGAPORE
21 LOWER KENT RIDGE ROAD
SINGAPORE, 119077 SG

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
AOARD
UNIT 45002
APO AP 96338-5002

10. SPONSOR/MONITOR'S ACRONYM(S)
AFRL/AFOSR IOA

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
AFRL-AFOSR-JP-TR-2020-0003

12. DISTRIBUTION/AVAILABILITY STATEMENT
A DISTRIBUTION UNLIMITED: PB Public Release

13. SUPPLEMENTARY NOTES

14. ABSTRACT
The PI has developed a method to obtain reliable secret key rates for QKD with untrusted devices. The advantage of this method, as compared to the original approach, is that in principle it can be applied to arbitrary DIQKD scenarios, not only those based on specialized Bell inequalities. The only existing approach that can be applied to DIQKD with such generality is based on bounding the guessing probability Pg(A0|E) instead, which is generally not optimal. This method outperforms both of these approaches in some cases. Importantly, it gives good results in regimes with substantial noise, which are likely to be experimentally relevant. With this approach, one could now explore DIQKD implementations aimed at maximizing a different Bell expression (or maximizing the key rate directly) instead of CHSH.

15. SUBJECT TERMS
high-dimensional QKD, Time-bin encoding

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			VERGIEN, CHRISTOPHER
Unclassified	Unclassified	Unclassified	SAR		19b. TELEPHONE NUMBER *(Include area code)* 315-227-7002

Report for AOARD Grant FA2386-18-1-4033

"Practical Quantum Cryptography with Ultra-High Encryption Rates "

Name of Principal Investigators: LIM CI WEN

- e-mail address : Charles.lim@nus.edu.sg
- Institution : National University of Singapore
- Mailing Address : NATIONAL UNIVERSITY OF SINGAPORE, 21 LOWER KENT RIDGE ROAD SINGAPORE 119077
- Phone : +65 65162127
- Fax : N.A

Period of Performance: July/01/2018 – December/31/2019

Abstract: Quantum computers are machines that can break todays' most prevalent encryption techniques in minutes. Recent progress in experimental quantum computing has indicated that this threat is no longer theoretical but real. If successfully implemented, quantum computers can be used to decrypt any nation's trade secrets, confidential communication, and military documents. Quantum key distribution (QKD) is the only solution that is secure against such threats. More specifically, the security of QKD is solely dependent on the laws of quantum physics and not on how powerful the adversaries could be. This nicely implies that QKD's security is long-term and can be used to encrypt highly sensitive data requiring long-term security.

One major bottleneck in practice is poor secret key rate. Current QKD systems are implemented using two-level quantum states and thus could only generate one secret bit per photon detected. Considering that channel loss is typically very high in practice, this means that only hundreds of photons could be detected in one second. Consequently, only tens of secret bits could be produced per second. For practical applications, this level of throughput is clearly not practical. We need QKD to generate secret key rates in the order of megabits to be compatible with today's digital communication rates.

In this project we proposed to develop QKD models that are able to generate ultra-high secret key rates. More specifically, we planned to derive security proof techniques that will enable the development of practical QKD systems based on high-dimensional quantum signals. The 1-year project was carried out in two phases. In the first phase, we developed numerical techniques that can bound the set of quantum correlations derived from quantum networks. Then in the second phase, we applied these techniques to establish tight secret key rates for high-dimensional QKD protocols.

Introduction: The overarching goal of the project is to develop a security analysis toolbox that will enable the security of practical QKD systems based on coherent state transmission. To achieve this goal, the project will be carried out in two phases, which are carefully designed to leverage on the research group expertise and related on-going projects.

1. Characterization of quantum correlations in semi-device-independent networks: This node aims to develop a novel and general mathematical technique that will characterize the set of quantum correlations satisfying the Gram matrix of the prepared quantum signals. Its core goal is a semidefinite program that will bound the set of achievable quantum correlations for at least three parties.
2. Prove the security of semi-device-independent quantum cryptography: Here, the aim is to use the semidefinite programming framework developed in the first node to characterize the information-disturbance trade-off function in quantum key distribution. Its core goal is a plot showing the guessing probability of a quantum adversary versus the quantum channel error rate. Two applications are of interest here: (1) coherent-state quantum secure communication and (2) time-bin encoding quantum key distribution.

Experiment: We will make use of the Navescues-Pironio-Acin (NPA) method [9] to characterize the set of achievable quantum correlations. The NPA method is based on the observation that computing the set of achievable correlations—obtained from local measurements on a joint quantum system–is a semidefinite programming problem [17, 18]. More specifically, to decide whether a particular set of correlations is quantum or not, it is enough to compute a finite set of semidefinite certificates, which can be easily solved using popular solvers like CVX and YALMIP on high-end workstations.

The NPA method is, however, designed for entanglement-based protocols, where each node in the network is making some (randomly chosen) measurement on a joint/global quantum state. This setting is slightly different from our prepare-and-measure consideration, where one party (the transmitter) is sending some unknown signal (classical or quantum) to a set of receivers who are making random measurements. To overcome this slight difference, we propose to model the transmitter as a single measurement party (i.e., the measurement is fixed) embedded in an entanglement-based network. This in principle converts any prepare-and-measure network to an entanglement-based network. Therefore, with this theoretical fix, the NPA method also works for our consideration.

Our bounded-information condition is defined as an upper bound on the total amount of information the receivers can gain about x: the random variable describing the input alphabet. From the perspective of quantum information theory, this condition is synonymous to the Holevo's theorem, which, roughly speaking, states that the accessible information about x is upper bounded by the dimensionality of the exchanged signal states. For example, if x is encoded into a qubit (i.e., a two-dimensional quantum system), then the total amount of information the receivers can learn about x is at most 1 bit. Here, instead of using the Holevo's theorem as a condition, we use the overlap fidelities of the encoding states as a measurement of quantum indistinguishability. This condition is a purely information-theoretic constraint and thus is more general than the Holevo's theorem—it does not make any assumptions about the dimensionality of the exchanged signals. Moreover, it admits a linear structure and can be written as part of a semidefinite program.

By building this condition into the NPA method, we will obtain a mathematical toolbox (more precisely, a semidefinite program) that is fully capable of characterizing the quantum set of any semi-device-independent network based on the bounded-information condition. To test the tightness of our program, we will compare the findings against known analytical results. More specifically, we will compare our results against the ones derived using the optimal broadcasting machines [3, 4] and the bounded-dimension condition [10].

Main results:

Device-independent quantum key distribution (DIQKD) considers the problem of secure key exchange using devices which are untrusted or uncharacterized. In this setting, security is based entirely on the observation of non-local correlations, which are typically measured by a Bell inequality. In particular, if the correlations violate the inequality, then we say that they are non-local. This is necessary for secure key distribution, for it certifies that the key must come from measurements on an entangled state. While the se- curity of DIQKD is well understood from the monogamy property of non-local correlations, a formal security analysis is rather involved and tricky. This is because the dimension of the underlying shared quantum state is unknown, and most security proof techniques only apply to quantum systems with bounded dimension.

Recently, security proof techniques based on semi- definite programming (SDP) have been proposed for standard QKD. In this so-called device-dependent (DD) setting, the underlying QKD devices are assumed to be suitably characterized. Our main result extends this approach to a wider range of settings, adapting to different levels of device characterization (see Fig. 1). At present, to prove the security of DIQKD, the current approaches are to either prove a reduction to qubit-level systems, or to

use a family of semi-definite programs (SDPs) known as the Navascués-Pironio-Acín (NPA) hierarchy to bound the adversary's guessing probability. However, neither of these approaches are general enough for most purposes. The former is restricted to protocols based on Bell inequalities with binary in- puts and outputs, while the latter only bounds the min- entropy, which often leads to sub-optimal bounds on the von Neumann entropy (the relevant quantity for com- puting secret key rates against general attacks). Here, we develop a generic computational toolbox that directly bounds the von Neumann entropy using the complete probability distribution of any DIQKD protocol.

The main mechanism of our toolbox is a technique for estimating the entropy production of a quantum channel acting on an unknown state under algebraic constraints. The simplest way to understand entropy production is to view it as the amount of entropy introduced to a sys- tem after performing some action on it. For instance, in the case of projective measurement, the entropy pro- duction is the entropy difference between the final post- measurement system and the initial system. Our toolbox bounds this entropy production via a (non-commutative) polynomial optimization performed over the measurement operators in the protocol. This can be evaluated using the SDPs in the NPA hierarchy. In this sense, switching from DI to sDI or DD scenarios translates to adding more constraints on the SDPs and hence stricter bounds on the eventual secret key rates.

SETTING AND METHODS

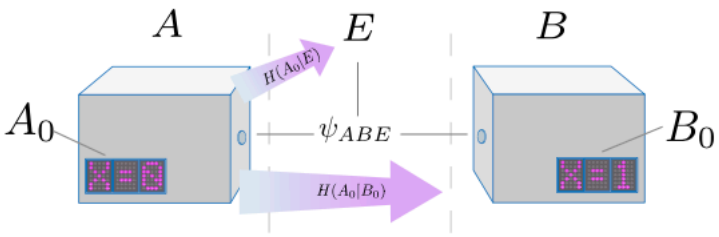

FIG. 2. **Basic situation:** By measuring her share of the joint state ψ_{ABE} with measurement A_0, Alice is (virtually) sending a raw key to Bob who (virtually) receives it by measuring B_0. Bob's uncertainty is quantified by the classical entropy $H(A_0|B_0)$. We assume that Eve has access to all classical communication and her share of the joint quantum state, which gives her some partial information on A_0 as well. This is quantified by the classical-quantum entropy $H(A_0|E)$.

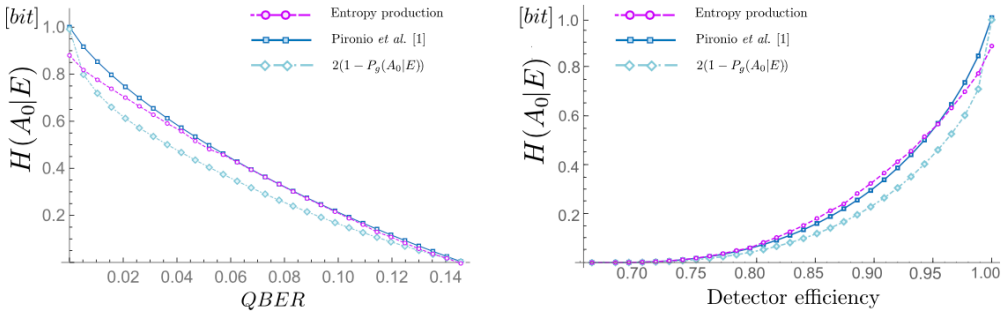

FIG. 4. **2-input 2-output DI protocols**: Lower bounds on $H(A_0|E)$ (in base 2) as a function of depolarizing noise (for the scenario studied in [2]) or detection efficiency (for the scenario studied in [34]). Our approach yields bounds close to or slightly better than the best known result [2] for these scenarios, which was based on the CHSH value alone. For comparison, we also show the indirect $P_g(A_0|E)$-based bound.

In summary, we have developed a method to obtain reliable secret key rates for QKD with untrusted

de- vices. The advantage of our method, as compared to the original approach, is that in principle it can be applied to arbitrary DIQKD scenarios, not only those based on specialized Bell inequalities. The only exist- ing approach that can be applied to DIQKD with such generality is based on bounding the guessing probability Pg(A0|E) instead, which is generally not opti- mal. Our method outperforms both of these approaches in some cases, as shown in Fig. 4. Importantly, it gives good results in regimes with substantial noise, which are likely to be experimentally relevant. With this approach, one could now explore DIQKD implementations aimed at maximizing a different Bell expression (or maximizing the key rate directly) instead of CHSH.

Currently, our method scales rapidly in computa- tional difficulty as the number of inputs or outputs for the protocol increases—the polynomial in our key rate is generally of high order, hence a high NPA hierarchy level is needed to bound $\langle K \rangle_\rho$. Because of this, we currently do not have good bounds for DI scenarios with large numbers of inputs or outputs (though we find suboptimal bounds for some such cases). An important goal now would be to find ways to improve the tractability of our approach. This would enable the computation of key rates for DIQKD protocols with more measurement settings and/or outcomes, and at the same time, yield good bounds on the secret key rate in the noise regime that is representative of present experimental conditions.

List of Publications and any Significant Collaborations that resulted from your AOARD supported project: In standard format showing authors, title, journal, issue, pages, and date, for each category list the following:

a) papers published in peer-reviewed journals

- NT Islam, CCW Lim, C Cahall, B Qi, J Kim, DJ Gauthier, Scalable high-rate, high-dimensional time-bin encoding quantum key distribution, Quantum Science and Technology, 4, 035008.
- W Primaatmaja, E Lavie, KT Goh, C Wang, CCW Lim, Versatile security analysis of measurement-device-independent quantum key distribution, Physical Review A, 99, 062332.
- Y Wang, IW Primaatmaja, E Lavie, A Varvitsiotis, CCW Lim, Characterising the correlations of prepare-and-measure quantum networks, Nature Quantum Information, 5, 17.
- L Liu, Y Wang, E Lavie, C Wang, A Ricou, FZ Guo, CCW Lim, Practical quantum key distribution with non-phase-randomized coherent states, Physical Review Applied, 12, 024048.

b) conference presentations without papers

- EYZ Tan, R Schwonnek, KT Goh, IW Primaatmaja, CCW Lim, Computing secure key rates for quantum key distribution with untrusted devices, QCRYPT 2019, Montreal, Canada.
- W Primaatmaja, E Lavie, KT Goh, C Wang, CCW Lim, Versatile security analysis of measurement-device-independent quantum key distribution, QCRYPT 2019, Montreal, Canada.
- Y Wang, IW Primaatmaja, E Lavie, A Varvitsiotis, CCW Lim, Characterising the correlations of prepare-and-measure quantum networks, QCRYPT 2018, Shanghai, China.

c) manuscripts submitted but not yet published

- EYZ Tan, R Schwonnek, KT Goh, IW Primaatmaja, CCW Lim, Computing secure key rates for quantum key distribution with untrusted devices, arXiv preprint arXiv:1908.11372 (to be submitted to PRL)
- EYZ Tan, CCW Lim, R Renner, Advantage distillation for device-independent quantum key distribution, arXiv preprint arXiv:1903.10535 (submitted to PRL)