Improved Measurement-Device-Independent Quantum Key Distribution with Uncharacterized Qubits

Won-Young Hwang\textsuperscript{1,*}, Hong-Yi Su\textsuperscript{1}, and Joonwoo Bae\textsuperscript{2}

\textsuperscript{1} Department of Physics Education, Chonnam National University, Gwangju 61186, Republic of Korea
\textsuperscript{2} Department of Applied Mathematics, Hanyang University (ERICA), Ansan, Gyeonggi-do 15588, Republic of Korea.

We propose an improved bound for the difference between phase and bit error rate in measurement-device-independent quantum key distribution with uncharacterized qubits. We show by simulations that the bound considerably increases the final key rates.

PACS numbers: 03.67.Dd

I. INTRODUCTION

Quantum key distribution (QKD)\textsuperscript{[1]} enables two remote users Alice and Bob to generate key, which is not a classically possible task. QKD is not only a practically important field but also a theoretically appealing one. After security of QKD for ideal devices was shown\textsuperscript{[2,3]}, problems due to imperfect devices surfaced. Although a problem due to imperfect source was resolved\textsuperscript{[4]}, problems due to imperfect devices surfaced. Although security of QKD for ideal devices was shown\textsuperscript{[2,3]}, the field is important but also a theoretically appealing one.

Device-independent (DI) QKD was proposed\textsuperscript{[6]}.

II. MDI QKD WITH UNCHARACTERIZED QUBITS

For the protocol\textsuperscript{[8]}, each user prepares two encoding states. Let the states prepared by Alice and Bob denoted by $|\varphi_m\rangle$ and $|\varphi'_n\rangle$, respectively, where $m,n = 0,1$. Here nothing is supposed about the encoding states so they are completely un-characterized. Each user also prepares a checking state which is assumed to be a superposition of the encoding states. Alice's and Bob's checking states are, respectively,

$$|\varphi_2\rangle = c_0|\varphi_0\rangle + c_1 e^{i\theta} |\varphi_1\rangle,$$

$$|\varphi'_2\rangle = c'_0|\varphi'_0\rangle + c'_1 e^{i\theta'} |\varphi'_1\rangle.$$

(1)

Here $c_m$ and $c'_n$ are non-negative numbers and $\theta$ and $\theta'$ are real. The protocol is as follows.

1. Alice generates a random number $i$ where $i = 0,1,2$. She sends a state $|\varphi_i\rangle$ to Charlie. Here Charlie can be anyone. So Charlie can be either Eve (eavesdropper) or users themselves.
2. Bob independently generates a random number $j$ where $j = 0,1,2$. He also sends a state $|\varphi'_j\rangle$ to Charlie.
3. Charlie performs a measurement on the states $|\varphi_i\rangle$ and $|\varphi'_j\rangle$. The measurement can be any one which finally gives two outcomes 0 and 1. Charlie announces the outcome.
4. When the outcome is 0, users discard the data. Otherwise, they keep the data. By sacrificing some of the data for public discussion, users estimate, $p_{ij}$, conditional probability to get outcome 1 for each $i,j$.
5. Measurement data with both $i$ and $j$ less than 2 become raw key. Other data with either $i$ or $j$ is 2 are used for checking purposes. Users do post-processing to get final key.

Now let us consider Charlie’s measurement on the states $|\varphi_i\rangle$ and $|\varphi'_j\rangle$. In the most general collective attack, Eve attaches an ancilla $|\epsilon\rangle$ to the states and then applies a unitary operation to them\textsuperscript{[8]}

$$U_{Eve}|\varphi_i\rangle|\varphi'_j\rangle|\epsilon\rangle|0\rangle_M = \sqrt{p_{ij}^\epsilon} |\Gamma_{ij}\rangle|0\rangle_M + \sqrt{p_{ij}^\perp} |\Gamma_{ij}\rangle|1\rangle_M.$$

(2)

Eve gets the outcome by measuring the quantum state indexed by $M$ in basis of $|0\rangle$ and $|1\rangle$. It is enough to consider only the data with the measurement outcome 1 because those with 0 is discarded. For convenience, let us omit 1 from now on, $|\Gamma_{ij}\rangle \equiv |\Gamma_{ij}\rangle$ and $p_{ij}^\epsilon \equiv p_{ij}$. Now we can see that Eqs. (1) and (2) give constraints

$$\sqrt{p_{2m}} |\Gamma_{2n}\rangle = \sqrt{p_{2m} c_0^m c_0^n} |\Gamma_{00}\rangle + \sqrt{p_{1n}} c_1 e^{i\theta} |\Gamma_{1n}\rangle,$$

(3)

$$\sqrt{p_{m2} |\Gamma_{m2}\rangle = \sqrt{p_{m1} c'_0 |\Gamma_{m0}\rangle + \sqrt{p_{m1} c'_1 e^{i\theta'} |\Gamma_{m1}\rangle},$$

(4)

$$\sqrt{p_{22}} |\Gamma_{22}\rangle = \sum_{m,n} \sqrt{p_{mn} c_m c'_n e^{i\theta_m} e^{i\theta'_n}} |\Gamma_{mn}\rangle.$$

(5)

*Email: wyhwang@jnu.ac.kr
where $\theta_0 = \theta'_0 = 0$, $\theta_1 = \theta$, and $\theta'_1 = \theta'$. Constraints (3) and (4) play key roles in security analysis.

For theoretical purposes, we consider an equivalent entanglement distillation protocol \[3\] \[9\]. In the hypothetical protocol, Alice and Bob prepare entangled states $(1/\sqrt{2})(|0\rangle_A_1|\varphi_0\rangle_{B_2} + |1\rangle_A_1|\varphi_1\rangle_{B_2})$ and $(1/\sqrt{2})(|0\rangle_{B_1}|\varphi'_0\rangle_{B_2} + |1\rangle_{B_1}|\varphi'_1\rangle_{B_2})$, respectively. Alice and Bob send quantum states indexed by $A_2$ and $B_2$ to Charlie, respectively. According to Charlie’s announcement when measurement outcome is 1, the users post-select their qubits indexed by $A_1$ and $B_1$, respectively. The post-selected state is given by \[8\]

$$\rho = \frac{1}{p_{00} + p_{11} + p_{01} + p_{10}} \cdot \sum_q P(|\sqrt{p_{00}}\gamma_{00}^{q}|A_1|0\rangle_B_1 + |\sqrt{p_{11}}\gamma_{11}^{q}|A_1|1\rangle_B_1 + |\sqrt{p_{01}}\gamma_{01}^{q}|A_1|0\rangle_B_1 + |\sqrt{p_{10}}\gamma_{10}^{q}|A_1|0\rangle_B_1).$$

(6)

Here $P[x] = |x|\langle x|$, $\Gamma_{mn} \equiv \sum_q \gamma_{mn}^q|q\rangle$, where $|q\rangle$ are a set of orthonormal bases. From normalization, $\sum_q |\gamma_{mn}^q|^2 = 1$. We consider four Bell states $|\varphi^{\pm}\rangle = (1/\sqrt{2})(|00\rangle \pm e^{i(\alpha_A + \alpha_B)}|11\rangle)$ and $|\psi^{\pm}\rangle = (1/\sqrt{2})(|01\rangle \pm e^{i(\alpha_A - \alpha_B)}|10\rangle)$ which are obtained by rotating each qubit by Pauli operator $\sigma_z$ with amount $\alpha_A$ and $\alpha_B$, respectively. Final key rate is given by $R = 1 - H(e_b) - H(e_p)$, where $H(x) = -x \log_2 x - (1 - x) \log_2(1 - x)$ is binary Shannon entropy and $e_b$ and $e_p$ are bit and phase error rates, respectively. Bit error rate is given by

$$e_b = \langle \psi^{\pm}\rangle|\rho|\psi^{\pm}\rangle + \langle \psi^{\pm}\rangle|\rho|\psi^{\pm}\rangle$$

$$= \frac{p_{01} + p_{10}}{p_{00} + p_{11} + p_{01} + p_{10}}$$

(7)

for arbitrary $\alpha_A$ and $\alpha_B$. Phase error rate is given by

$$e_p = \langle \varphi^{\pm}\rangle|\rho|\varphi^{\pm}\rangle + \langle \psi^{\pm}\rangle|\rho|\psi^{\pm}\rangle$$

$$\leq e_b + \sum_q \frac{|\sqrt{p_{00}}\gamma_{00}^{q} + e^{i(\alpha_A + \alpha_B)}|\sqrt{p_{11}}\gamma_{11}^{q}|^2}{2(p_{00} + p_{11} + p_{01} + p_{10})}.$$  (8)

On the other hand, using normalization condition of the states in Eq. (1) and constraints (3)–(5), a term \[\sum_q |\sqrt{p_{00}}\gamma_{00}^{q} + e^{i(\alpha_A + \alpha_B)}|\sqrt{p_{11}}\gamma_{11}^{q}|^2\] can be upperbounded. The normalization condition gives

$$(c_0 - c_1)^2 \leq 1 \leq (c_0 + c_1)^2,$$

$$c_0^2, c_1^2 \leq 1 \leq (c'_0 + c'_1)^2.$$  (9)

Constraints (3) and (4) imply

$$(\sqrt{p_{00}}c_0 - \sqrt{p_{01}}c_1)^2 \leq p_{20} \leq (\sqrt{p_{00}}c_0 + \sqrt{p_{01}}c_1)^2,$$

$$(\sqrt{p_{00}}c_0 - \sqrt{p_{11}}c_1)^2 \leq p_{21} \leq (\sqrt{p_{00}}c_0 + \sqrt{p_{11}}c_1)^2,$$

$$(\sqrt{p_{01}}c_0 - \sqrt{p_{01}}c_1)^2 \leq p_{20} \leq (\sqrt{p_{01}}c_0 + \sqrt{p_{01}}c_1)^2,$$

$$(\sqrt{p_{10}}c'_0 - \sqrt{p_{11}}c'_1)^2 \leq p_{21} \leq (\sqrt{p_{10}}c'_0 + \sqrt{p_{11}}c'_1)^2.$$  (10)

where $\sqrt{p_{mn}}$‘s are fixed and $c_m$ are variables.

Constraint (5) gives upperbound for $\sum_q |\sqrt{p_{00}}\gamma_{00}^{q} + e^{i(\alpha_A + \alpha_B)}|\sqrt{p_{11}}\gamma_{11}^{q}|^2$, \[\sum_q |\sqrt{p_{00}}\gamma_{00}^{q} + e^{i(\alpha_A + \alpha_B)}|\sqrt{p_{11}}\gamma_{11}^{q}|^2 \leq \max_{c_0, c_1} f(c, c')$$  (11)

where

$$f(c, c') = \min \left\{ (\sqrt{p_{22}} + \sqrt{p_{01}}c_0c_1' + \sqrt{p_{10}}c_0'c_1 + \sqrt{p_{11}}(c_0c_1' - c_1c_0'))^2, \right.$$  \[\left(\sqrt{p_{22}} + \sqrt{p_{01}}c_0c_1' + \sqrt{p_{10}}c_0'c_1 + \sqrt{p_{11}}(c_0c_1' - c_1c_0')^2)$$

(12)

Optimization in Inequality (11) with constraints (3)–(10) can be done numerically. According to our computer calculations, when bit error rate is small enough such that final key rate is nonnegligible, $c_0c_1'$ and $c_1c_0'$ don’t become 0. Thus here we consider only the case when the $c$’s are not zero.

The fact that the term $\sum_q |\sqrt{p_{00}}\gamma_{00}^{q} + e^{i(\alpha_A + \alpha_B)}|\sqrt{p_{11}}\gamma_{11}^{q}|^2$ has an upperbound means that $\Delta = \sum_q |\sqrt{p_{00}}\gamma_{00}^{q} - e^{i(\alpha_A + \alpha_B)}|\sqrt{p_{11}}\gamma_{11}^{q}|^2$ has the same upperbound when $\alpha_A + \alpha_B = \theta + \theta' + \pi$. Hence we can obtain upperbound for phase error rate, which then, with bit error rate, gives the final key rate.

III. IMPROVED BOUND FOR PHASE ERROR RATE

Let us consider the quantity to be bounded. We get

$$\Delta = \sum_q |\sqrt{p_{00}}\gamma_{00}^{q} - e^{i(\alpha_A + \alpha_B)}|\sqrt{p_{11}}\gamma_{11}^{q}|^2$$

$$= p_{00} + p_{11} - 2\sqrt{p_{00}}\sqrt{p_{11}} \Re [e^{i(\alpha_A + \alpha_B)}|\gamma_0\rangle|\gamma_1\rangle],$$

(13)

where $\Re [z]$ is real part of a complex number $z$. Constraint (5) can be rewritten as

$$\sqrt{p_{00}}c_0c_1'|\Gamma_0\rangle + \sqrt{p_{11}}c_1c_0'\gamma_0|\Gamma_1\rangle = \sqrt{p_{22}}|\Gamma_2\rangle - \sqrt{p_{01}}c_0c_1'|\gamma_0\rangle - \sqrt{p_{10}}c_1c_0'\gamma_0|\Gamma_0\rangle,$$

(14)

from which we get

$$\Re [e^{i(\theta + \theta')}|\Gamma_0\rangle|\Gamma_1\rangle]$$

$$\leq \frac{\sqrt{p_{22}} + \sqrt{p_{01}}c_0c_1' + \sqrt{p_{10}}c_1c_0' - p_{00}c_0^2c_1^2 - p_{10}c_1^2c_0^2 - 2\sqrt{p_{00}}\sqrt{p_{11}}c_0c_1'}{2\sqrt{p_{00}}\sqrt{p_{11}}c_0c_1'}$$

(15)

by $||A|| + ||B|| \leq ||A|| + ||B||$ where $|A\rangle$, $|B\rangle$ are arbitrary states and $||A||$ is norm of $|A\rangle$. 
First we upperbound \( \Re\{e^{i(\theta+\phi)}\langle\Gamma_0|\Gamma_1\rangle\} \) with constraints [3] and [4].

\[
\Re\{e^{i(\theta+\phi)}\langle\Gamma_0|\Gamma_1\rangle\} \leq \max_{c,c'} \left\{ \frac{\sqrt{p_{22}} + \sqrt{p_{01}}c_0c_1' + \sqrt{p_{10}}c_0'c_1 - p_{00}c_0c_0' - p_{11}c_1c_1'}{2\sqrt{p_{00}}\sqrt{p_{11}}c_0c_0'c_1c_1'} \right\}.
\]

Maximization in Inequality (16) can be done similarly with the constants [3], [10].

Consider a case when the upperbound is negative, that is \( \Re\{e^{i(\theta+\phi)}\langle\Gamma_0|\Gamma_1\rangle\} \leq -|\Omega| \), then we can see that \( |\langle\Gamma_0|\Gamma_1\rangle| \) is lowerbounded by the absolute value of the upperbound, \( |\langle\Gamma_0|\Gamma_1\rangle| \geq |\Omega| \). Now it is easy to see that we can always choose \( \alpha_A + \alpha_B \) such that

\[
\Delta \leq p_{00} + p_{11} - 2\sqrt{p_{00}}\sqrt{p_{11}}|\Omega|.
\]

Now we can get upperbound for phase error rate by Inequalities [3] and [17], from which we can get final key rate.

Let us compare the two upperbounds. First consider a case when \( p_{00} = p_{11} = (1/2)(1 - e_0), p_{10} = p_{01} = (1/2)e_0, p_{20} = p_{21} = p_{12} = 1/4, \) and \( p_{22} = (1/2)e_0 \). The set of probabilities can be obtained by choosing that \( |\varphi_0\rangle = |0\rangle, |\varphi_1\rangle = |1\rangle, |\varphi_0'\rangle = |0\rangle, |\varphi_1'\rangle = |1\rangle, \)

\( |\varphi_2\rangle = (1/\sqrt{2})(|0\rangle + |1\rangle), |\varphi_2'\rangle = (1/\sqrt{2})(|0\rangle - |1\rangle) \), and measurement element for outcome 1 is \( |\varphi_+\rangle\langle\varphi_+| \). (Here we are not supposing that the measurements are done on the states actually. We consider the states and measurements in order to show that the set of probabilities are physically realizable. In the MDI QKD with uncharacterized qubits, security is shown regardless of how the set was generated.) We suppose channel between Alice and Charlie is depolarized [9]. But we suppose channel between Bob and Charlie is perfect because the measurement unit is controlled by Bob. Here the higher the depolarization probability is, the higher the bit error rate is. The final key rate and the quantity \( \Delta/[(2(p_{00} + p_{11} + p_{01} + p_{10}))] \) are shown in Fig-1 and Fig-2.

Bit error rate that MDI QKD with uncharacterized qubit can tolerate is not that high as we can see in Fig-1. By the new bound, the tolerable bit error rate and the final key rate have been considerably improved.

Next let us consider the case [8] when four single-photon detectors with dark counting rate of \( d = 10^{-5} \) are used in the measurement unit. Here \( \eta \) denotes total transmission rate of the channel from Alice (Bob) to the measurement unit in the middle of channel and no Eve’s attack is assumed. The same states used in the depolarization case are chosen. Now we have \( p_{00} = p_{11} = \eta^2(1-d)^2/2 + 2\eta(1-\eta)d(1-d)^2 + 2(1-\eta)^2d^2(1-d)^2, p_{10} = p_{01} = p_{22} = 2\eta(1-\eta)d(1-d)^2 + 2(1-\eta)^2d^2(1-d)^2, \) and \( p_{20} = p_{21} = p_{12} = (p_{00} + p_{01})/2 \). The key rates by the two bounds and the original protocol [6] are described in Fig-3. Here the reason why the key rates do not differ much is that the bit error rate is not large.

![FIG. 1: Final key rate (y axis) versus bit error rate (x axis) for depolarization channel.](image1)

![FIG. 2: \( \Delta/[(2(p_{00} + p_{11} + p_{01} + p_{10}))] \) (y axis) versus bit error rate (x axis) for depolarization channel. \( \Delta/[(2(p_{00} + p_{11} + p_{01} + p_{10}))] \) is bound for gap between phase and bit error rates.](image2)

**IV. DISCUSSION AND CONCLUSION**

Inequality in (17) implies that if \( p_{00} = p_{11} \) and \( |\langle\Gamma_0|\Gamma_1\rangle| = 1 \) then the \( \Delta = 0 \) or the phase error rate equals bit error rate for a certain choice of Bell states. This can be confirmed by observing that the state \( |\Psi\rangle\langle\Psi| = \rho \) in Eq. [6] becomes \( |\Psi\rangle = \sqrt{p_{00}}(|0\rangle + e^{iA}|1\rangle)|\Gamma_0\rangle + \sqrt{p_{01}}|01\rangle|\Gamma_0\rangle + \sqrt{p_{10}}|10\rangle|\Gamma_0\rangle \), where \( e^{iA} = (\Gamma_0|\Gamma_1\rangle) \).

To summarize, MDI QKD with uncharacterized qubit has an advantage that the condition for security is weaker than that of normal MDI QKD’s. However, disadvantage is low tolerable bit error rate due to the overestimation for the phase error rate. Here we proposed an improved bound for phase error rate. By simulations we showed the bound considerably improved final key rates.

**Acknowledgement**

This study was supported by Institute for Information and Communications Technology Promotion (IITP) grant funded by the Korea Government (MSIP) (No.
FIG. 3: Final key rate multiplied by $p_{00} + p_{11} + p_{01} + p_{10}$ (y axis) versus total transmission loss by dB (x axis) for four single-photon detectors with dark counting. In the original protocol, ideal source is supposed and thus phase error rate is equal to bit error rate.

[1] V. Scarani et al., Rev. Mod. Phys. 81, 1301 (2009).
[2] D. Mayers, J. ACM 48, 351 (2001).
[3] P.W. Shor and J. Preskill, Phys. Rev. Lett. 85, 441 (2000).
[4] W.-Y. Hwang, Phys. Rev. Lett. 91, 057901 (2003).
[5] A. Acín et al., Phys. Rev. Lett. 98, 230501 (2007).
[6] H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. 108, 130503 (2012).
[7] Z.-Q. Yin et al., Phys. Rev. A 88, 062322 (2013).
[8] Z.-Q. Yin et al., Phys. Rev. A 90, 052319 (2014).
[9] M. A. Nielsen and I. L. Chuang, Quantum Computation and Quantum Information, (Cambridge Univ. Press, Cambridge, U.K., 2000.)