SCIENTIFIC REPORTS

OPEN

Received: 17 February 2016
Accepted: 29 June 2016
Published: 25 July 2016

N-dimensional measurement-device-independent quantum key distribution with $N+1$ un-characterized sources: zero quantum-bit-error-rate case

Won-Young Hwang[1], Hong-Yi Su[1] & Joonwoo Bae[2]

We study *N*-dimensional measurement-device-independent quantum-key-distribution protocol where one checking state is used. Only assuming that the checking state is a superposition of other *N* sources, we show that the protocol is secure in zero quantum-bit-error-rate case, suggesting possibility of the protocol. The method may be applied in other quantum information processing.

Quantum key distribution (QKD)[1,2] enables two remote users, normally called Alice and Bob, to generate key (private random sequence), which is not a possible task classically. QKD is not only a practically important field but also a theoretically appealing one.

After security of QKD for ideal devices was shown[1,3,4], problems due to imperfect devices protruded. Although a main problem due to imperfect source was resolved[5], problem due to imperfect detectors still had remained[6,7]. Then no-signaling QKD was discovered[8,9]. Remarkably, the no-signaling QKD's were found to be immune against the imperfect device problems, because security analysis of the protocol is based only on outcomes of detectors. Soon device-independent (DI) QKD's were found[10]. DI QKD has ideal security but not yet feasible. Measurement-device-independent (MDI) QKD was proposed[11] and demonstrated[12–15] in the background. MDI QKD is secure provided that source is ideal, that is, source is exactly in prescribed quantum states. Later protocols[16,17] with more relaxed condition adapt un-characterized source. The only assumption is that the sources are within 2-dimensional subspace.

It can be expected that MDI QKD can be generalized to N-dimensional case. However, security of MDI QKD with un-characterized source relies[16,17] on Shor-Preskill proof[4]. Thus it is not yet clear that N-dimensional MDI QKD with un-characterized source works. In this paper, we consider the N-dimensional MDI QKD with un-characterized source. The only assumption for security is that the sources are within N-dimensional subspace. In the protocol, a single quantum state is enough for checking eavesdropper, normally called Eve. (It is known that a single checking state is enough[18]). We show that the protocol is secure in zero quantum-bit-error-rate (QBER) case. This suggests possibility of N-dimensional MDI QKD with un-characterized source.

Results

For the protocol, each user prepares N encoding states. Let the states prepared by Alice and Bob denoted by $|\varphi_m\rangle$ and $|\varphi_m'\rangle$, respectively, where $m=0, 1, 2, \ldots, N-1$. Here nothing is assumed for 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,

$$\begin{aligned} |\varphi_N\rangle &= c_0|\varphi_0\rangle + c_1 e^{i\theta_1}|\varphi_1\rangle + \ldots + c_{N-1}e^{i\theta_{N-1}}|\varphi_{N-1}\rangle \\ |\varphi_N'\rangle &= c_0'|\varphi_0'\rangle + c_1' e^{i\theta_1'}|\varphi_1'\rangle + \ldots + c_{N-1}'e^{i\theta_{N-1}'}|\varphi_{N-1}'\rangle. \end{aligned} \quad (1)$$

[1]Department of Physics Education, Chonnam National University, Gwangju 61186, Republic of Korea. [2]Department of Applied Mathematics, Hanyang University (ERICA), Ansan, Gyeonggi-do, 15588, Republic of Korea. Correspondence and requests for materials should be addressed to W.-Y.H. (email: wyhwang@jnu.ac.kr)

Here c_m and c'_m are real numbers with constraints $\sum_m c_m^2 = 1$ and $\sum_m {c'_m}^2 = 1$, respectively, and θ_m and θ'_m are real. The protocol is as follows.

(1) Alice generates a random number i where $i = 0, 1, 2, \ldots, N$. She sends a state $|\varphi_i\rangle$ to Charlie. Here Charlie can be anyone. So Charlie can be either Eve or users themselves. (2) Bob independently generates a random number j where $j = 0, 1, 2, \ldots, N$. He sends a state $|\varphi'_j\rangle$ to Charlie. (3) Charlie performs a measurement on set of 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, $p(1|ij) \equiv p_{ij}$, conditional probability to get outcome 1 for each i, j. (5) For each measurement, if both i and j are less than N, the i and j become raw key. Otherwise, the data are used only for checking purposes. Then users do post-processing to get final key.

Now let us consider Eve's (Charlie's) measurement on the states $|\varphi_i\rangle$ and $|\varphi'_j\rangle$. In the most general collective attack, Eve attaches an ancilla $|e\rangle$ to the states and then applies a unitary operation to them[17]

$$U_{Eve}|\varphi_i\rangle|\varphi'_j\rangle|e\rangle|0\rangle_M = \sqrt{p(0|ij)}\,|\Gamma_{ij0}\rangle|0\rangle_M + \sqrt{p(1|ij)}\,|\Gamma_{ij1}\rangle|1\rangle_M. \tag{2}$$

Eve gets the outcome by measuring the quantum state indexed by M in basis of $|0\rangle$ and $|1\rangle$. Now let us consider the attack from Eve's viewpoint. Clearly she can get no information about key from the data with outcome 0 which are not used by the users. Thus she analyze the states for outcome 1, $|\Gamma_{ij1}\rangle$'s. For convenience, let us omit 1, $|\Gamma_{ij1}\rangle \equiv |\Gamma_{ij}\rangle$. We can see that Eqs (1) and (2) give constraints

$$\begin{aligned}
\sqrt{p_{Nn}}|\Gamma_{Nn}\rangle &= \sqrt{p_{0n}}\,c_0|\Gamma_{0n}\rangle + \sqrt{p_{1n}}\,c_1 e^{i\theta_1}|\Gamma_{1n}\rangle + \ldots + \sqrt{p_{N-1,n}}\,c_{N-1}e^{i\theta_{N-1}}|\Gamma_{N-1,n}\rangle \\
\sqrt{p_{mN}}|\Gamma_{mN}\rangle &= \sqrt{p_{m1}}\,c'_0|\Gamma_{m0}\rangle + \sqrt{p_{m1}}\,c'_1 e^{i\theta'_1}|\Gamma_{m1}\rangle + \ldots + \sqrt{p_{m,N-1}}\,c'_{N-1}e^{i\theta'_{N-1}}|\Gamma_{m,N-1}\rangle \\
\sqrt{p_{NN}}|\Gamma_{NN}\rangle &= \sum_{m,n}\sqrt{p_{mn}}\,c_m c'_n e^{i\theta_m}e^{i\theta'_n}|\Gamma_{mn}\rangle,
\end{aligned} \tag{3}$$

where $n = 0, 1, \ldots, N-1$ and $\theta_0 = \theta'_0 = 0$. Then Eve's goal is to maximize I_{EA} her information about Alice's or I_{EB} her information about Bob's. Eve is constrained only by Eq. (3) and the conditional probabilities p_{ij}'s. Let us consider the case when Eve maximizes I_{EA}. In this case she should discriminate mixed states $\rho_m = \sum_n \frac{p_{mn}}{p_m}|p_{mn} \times p_{mn}|$. So the I_{EA} is bounded by[1]

$$I_{EA} \le S(\rho) - \sum_m \frac{p_m}{\sum_{mn} p_{mn}} S(\rho_m) \tag{4}$$

where $p_m = \sum_n p_{mn}$ and $\rho = \sum_{mn}\frac{p_{mn}}{\sum_{mn}p_{mn}}|p_{mn} \times p_{mn}|$. Analogously we also get a bound

$$I_{EB} \le S(\rho) - \sum_n \frac{p_n}{\sum_{mn} p_{mn}} S(\rho_n) \tag{5}$$

where $\rho_n = \sum_m \frac{p_{mn}}{p_n}|p_{mn} \times p_{mn}|$ and $p_n = \sum_m p_{mn}$. The bounds can be used to obtain key rate[1].

Now let us consider zero QBER case when $p_{mn} = \delta_{mn}(1/N)$, $p_{mN} = p_{Nn} = 1/N^2$, and $p_{NN} = 1/N$. Here δ_{mn} is Kronecker delta. This conditional probabilities can be obtained by choosing that $|\varphi_m\rangle = |m\rangle$, $|\varphi'_n\rangle = |n\rangle$, $|\varphi_N\rangle = |\varphi'_N\rangle = \sum_m (1/\sqrt{N})|m\rangle$, and Eve's measurement is a one composed of $|\varphi_N^+\rangle\langle\varphi_N^+|$ and $1 - |\varphi_N^+\rangle\langle\varphi_N^+|$ with outcome 1 and 0, respectively. Here $|m\rangle$'s are mutually orthonormal states and a generalized Bell state $|\varphi_N^+\rangle = (1/\sqrt{N})(|00\rangle + |11\rangle + \ldots + |N-1, N-1\rangle)$. However, here we assume nothing about the states and measurements. Conversely, we show that if the conditional probabilities were obtained anyhow, we can get security and the states should be such. By inserting the conditional probabilities to the first and second of Eq. (3), we get $c_m = c'_n = 1/\sqrt{N}$. Combining this with the third of Eq. (3), we obtain $|\Gamma_{NN}\rangle = (1/N)(|\Gamma_{00}\rangle + e^{i(\theta_1+\theta'_1)}|\Gamma_{11}\rangle + \ldots + e^{i(\theta_{N-1}+\theta'_{N-1})}|\Gamma_{N-1,N-1}\rangle)$. Now by normalization condition ($|\Gamma_{NN}\rangle$, $|\Gamma_{NN}\rangle$) = 1, we get

$$|\Gamma_{mm}\rangle = e^{-i(\theta_m+\theta'_m)}|\Gamma_{00}\rangle. \tag{6}$$

Eq. (6) means that all $|\Gamma_{mm}\rangle$'s are essentially identical and that righthandside terms in Eqs (4) and (5) are zero, implying the security. Moreover, combining $c_m = c'_n = 1/\sqrt{N}$, Eq. (1), and normalization condition, we obtain that all $|\varphi_m\rangle$'s are orthogonal with one another and the same property holds for $|\varphi'_m\rangle$'s. We can also see that the states $|\varphi_N\rangle$ and $|\varphi'_N\rangle$ are expected ones.

Let us consider another set of conditional probabilites $p_{mn} = \delta_{mn}$ and $p_{iN} = p_{Nj} = p_{NN} = 1/N$. This corresponds to a case when Eve performs measurement in the encoding bases on each quantum states received, and announces 1 (0) when the same (different) outcomes are obtained. Analogously we get $c_m = c'_n = 1/\sqrt{N}$. Then we obtain $|\Gamma_{NN}\rangle = (1/\sqrt{N})(|\Gamma_{00}\rangle + e^{i(\theta_1+\theta'_1)}|\Gamma_{11}\rangle + \ldots + e^{i(\theta_{N-1}+\theta'_{N-1})}|\Gamma_{N-1,N-1}\rangle)$. Combined by normalization condition, we get that all $|\Gamma_{mm}\rangle$'s are orthogonal each other. The righthandside terms in Eqs (4) and (5) are N and there is no security clearly.

Discussion and Conclusion

In principle, the method is applicable to other set of conditional probabilities physically realizable. Within Eq. (3) with given conditional probabilities, optimize the bounds in Eqs (4) and (5). However, it does not seem to be feasible because of its complexity. Robustness of the method can be shown by the fact that functions involved here are all continuous. If the set of conditional probabilities are arbitrarily close to the ones discussed above, the bounds are also arbitrarily close to the given ones. Only with the assumption about dimensionality, security was obtained. It seems to be worthwhile to search for application of the method in other tasks in quantum information processing.

Good candidates for real implementation of the N-dimensional states seems to be time-bins of single photons which are adapted in the phase-reference-free MDI QKD[15,19] and round-robin-differential-phase-shift QKD[20–22]. Here the checking state can be made by opening optical switches such that all time-bins have non-zero possibility to contain a photon. Also spatial-bins may be a good candidate[23].

In conclusion, we studied N-dimensional MDI QKD where one checking state is used. With the assumption about dimensionality, Eq. (1), we showed that the protocol is secure in zero QBER case. In the case when Eve's does full measurement attack, the method also works. This suggests possibility of the protocol.

References

1. Scarani, V., Helle, B.-P., Cerf, N. J., Dusek, M., Lütkenhaus, N. & Peev, M. The security of practical quantum key distribution. *Rev. Mod. Phys.* **81,** 1301 (2009).
2. Nielsen, M. A. & Chuang, I. L. *Quantum computation and quantum information* (Cambridge universtiy press, Cambridge, UK, 2000).
3. Mayers, D. Unconditional security in quantum cryptography. *J. ACM* **48,** 351 (2001).
4. Shor, P. W. & Preskill, J. Simple proof of security of the BB84 quantum key distribution protocol. *Phys. Rev. Lett.* **85,** 441 (2000).
5. Hwang, W.-Y. Quantum key distribution with high loss: toward global secure communication. *Phys. Rev. Lett.* **91,** 057901 (2003).
6. Gottesman, D., Lo, H.-K., Lütkenhaus, N. & Preskill, J. Security of quantum key distribution with imperfect devices. *Quant. Inf. Comput.* **5,** 325 (2004).
7. Makarov, V., Anisimov, A. & Skaar, J. Effects of detector efficiency mismatch on security of quantum cryptosystems. *Phys. Rev. A* **74,** 022313 (2006).
8. Barrett, J., Hardy, L. & Kent, A. No signaling and quantum key distribution. *Phys. Rev. Lett.* **95,** 010503 (2005).
9. Acín, A., Gisin, N. & Masanes, L. From Bell's theorm to secure quantum key distribution. *Phys. Rev. Lett.* **97,** 010503 (2006).
10. Acín, A. *et al.* Device-independent security of quantum cryptography against collective attacks. *Phys. Rev. Lett.* **98,** 230501 (2007).
11. Lo, H.-K., Curty, M. & Qi, B. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **108,** 130503 (2012).
12. Rubenok, A., Slater, J. A., Chan, P., Lucio-Martinez, I. & Tittel, W. Real-world two-photon interference and proof-of-principle quantum key distribution immune to detector attacks. *Phys. Rev. Lett.* **111,** 130501 (2013).
13. Liu, Y. *et al.* Experimental measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **111,** 130502 (2013).
14. Tang, Z. *et al.* Experimental deomonstration of polarization encoding measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **112,** 190503 (2014).
15. Wang, C. *et al.* Phase-reference-free experiement of measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **115,** 160502 (2015).
16. Yin, Z.-Q. *et al.* Measurement-device-independent quantum key distribution with uncharacterized qubit sources. *Phys. Rev. A* **88,** 062322 (2013).
17. Yin, Z.-Q. *et al.* Mismatched-basis statistics enable quantum key distribution with uncharacterized qubit sources. *Phys. Rev. A* **90,** 052319 (2014).
18. Tamaki, K., Curty, M., Kato, G., Lo, H.-K. & Azuma, K. Loss-tolerant quantum cryptography with imperfect sources. *Phys. Rev. A* **90,** 052314 (2014).
19. Yin, Z.-Q. *et al.* Reference-free-independent quantum key distribution immune to detector side channel attacks. *Quantum Inf. Process.* **13,** 1237 (2014).
20. Sasaki, T., Yamamoto, Y. & Koashi, M. Practical quantum key distribution protocol without monitoring signal disturbance. *Nature* **509,** 475 (2014).
21. Takesue, H., Sasaki, T., Tamaki, K. & Koashi, M. Experimental quantum key distribution without monitoring signal disturbance. *Nature Photon.* **9,** 827 (2015).
22. Wang, S. *et al.* Experimental demonstration of a quantum key distribution without signal disturbance monitoring. *Nature Photon.* **9,** 832 (2015).
23. Etcheverry, S. *et al.* Quantum key distribution session with 16-dimensional photonic states. *Sci. Rep.* **3,** 2316 (2013).

Acknowledgements

This study was supported by Institute for Information and Communications Technology Promotion (IITP) grant funded by the Korea Government (MSIP) (No. R0190-16-2028, Practical and Secure Quantum Key Distribution).

Author Contributions

W.-Y.H. applied the method to analyse the protocol. H.-Y.S. and J.B. contributed to the analysis. All authors reviewed the manuscript.

Additional Information

Competing financial interests: The authors declare no competing financial interests.

How to cite this article: Hwang, W.-Y. *et al. N*-dimensional measurement-device-independent quantum key distribution with $N+1$ un-characterized sources: zero quantum-bit-error-rate case. *Sci. Rep.* **6**, 30036; doi: 10.1038/srep30036 (2016).