Detector-device-independent QKD: security analysis and fast implementation

Alberto Boaron,[1, *] Boris Korzh,[1] Raphael Houlmann,[1, 2] Gianluca Boso,[1] Charles Ci Wen Lim,[3] Anthony Martin,[1] and Hugo Zbinden[1]

[1] *Group of Applied Physics (GAP), University of Geneva,*
Chemin de Pinchat 22, CH-1211 Geneva 4, Switzerland
[2] *ID Quantique SA, 3 Ch. de la Marbrerie, 1227 Carouge/Geneva, Switzerland*
[3] *Quantum Information Science Group, Computational Sciences and Engineering Division,*
Oak Ridge National Laboratory, Oak Ridge, TN 37831-6418, US

We present a rapid realization of the detector-device-independent quantum key distribution protocol. This protocol features improved security compared to a standard prepare and measure protocol. Our high-speed implementation allows to exchange 1 kbps of secret keys over 40 km and is still efficient at more than 90 km.

Quantum key distribution (QKD) enables the secure establishment of a random cryptographic key between two users, Alice and Bob[1]. Its security depends only on the principles of quantum physics and can be proven to be information-theoretically secure. However, one still has to be prudent about potential side-channel attacks in the practical implementation that may lead to security failures. For example, it has been shown that with detector blinding techniques, it is possible to remotely hack the measurement unit of some QKD systems[2]. Although it is possible to implement appropriate countermeasures for specific attacks, one may be wary that the adversary could devise new detector control strategies, unforeseen by the users.

To prevent all known and yet-to-be-discovered detector side-channel attacks, a measurement-device-independent QKD (MDI-QKD) protocol was proposed[3]. In this scheme, Alice and Bob each randomly prepare one of the four Bennett & Brassard (BB84) states and send it to a third party, Charlie, whose role is to introduce entanglement between Alice and Bob via a Bell-state measurement (BSM). Alice and Bob do not have to trust Charlie since any other non-entangling measurement would necessarily introduce some noise between them. Unfortunately, with MDI-QKD, achievable secure key rates (SKR) are significantly lower compared to conventional prepare and measure (P&M) QKD systems[4,5]. Furthermore, the technological complexity of MDI-QKD is greater due to the use of two-photon interference, requiring both photons to be indistinguishable in all degrees of freedom (DOFs): temporal, polarization and frequency.

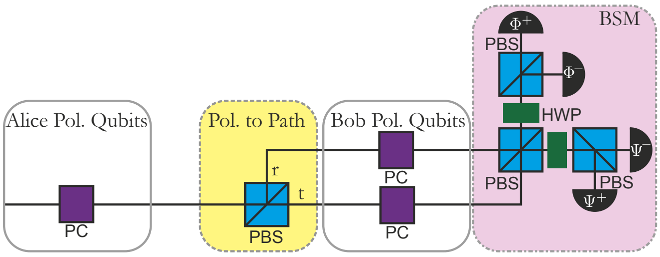

FIG. 1: Conceptual setup. PC: polarization controller; PBS: polarizing beam splitter; HWP: half-wave plate; BSM: Bell state measurement; FR: Faraday rotator.

We have recently proposed a QKD scheme that overcomes the aforementioned limitations but is still secure against detector side-channel attacks[6]. Our scheme, referred to as detector- device-independent QKD (DDI-QKD), essentially follows the idea of MDI-QKD. However, instead of encoding separate qubits into two independent photons, we exploit the concept of a two-qubit single-photon (TQSP). This scheme has the advantage that it requires only single-photon interference. Furthermore, it is expected that in the finite-key scenario the minimum classical post-processing size is similar to that of P&M QKD schemes.

The conceptual setup is presented in Fig. 1. Alice encodes a qubit $|\psi_A\rangle = \alpha_A \left|\tilde{H}\right\rangle + \beta_A \left|\tilde{V}\right\rangle$ in the polarization DOF of a single-photon and sends it to Bob. At the input of Bob a polarizing beam splitter (PBS) converts the polarization modes into spatial modes such that the qubit of Alice is converted to a state of the form $|\psi_A\rangle = \alpha_A |r\rangle + \beta_A |t\rangle$, where r and t represent the transmitted and reflected path of the PBS, respectively. Then, Bob encodes a qubit $|\psi_B\rangle = \alpha_B |H\rangle + \beta_B |V\rangle$ in the polarization DOF of the photon. The same polarization state needs to be encoded in the two paths. The state of the photon is then $|\psi_A\rangle \otimes |\psi_B\rangle$.

A BSM is performed by recombining the two spatial modes via a PBS and applying a projection in the basis $\{|+\rangle ; |-\rangle\}$ on both output arms using two additional PBSs. $|+\rangle$ and $|-\rangle$ correspond to $\frac{|H\rangle+|V\rangle}{\sqrt{2}}$ and $\frac{|H\rangle-|V\rangle}{\sqrt{2}}$, respectively. A click in one of the four outputs corresponds to a projection into one of the following Bell states:

$$\left|\Phi^{\pm}\right\rangle = 1/\sqrt{2}\left[|r\rangle|H\rangle \pm |t\rangle|V\rangle\right] \tag{1}$$

$$\left|\Psi^{\pm}\right\rangle = 1/\sqrt{2}\left[|r\rangle|V\rangle \pm |t\rangle|H\rangle\right]. \tag{2}$$

In order to exchange secret keys, the protocol is the following. Alice and Bob independently encode states randomly chosen out of the four following BB84 states $(|H\rangle ; |V\rangle ; |+\rangle ; |-\rangle)$. After sifting, one can not determine the bit sent by Alice only from the knowledge of which detector has clicked. Both the result of the BSM and the

Bob	$\vert\Phi^+\rangle$	$\vert\Phi^-\rangle$	$\vert\Psi^+\rangle$	$\vert\Psi^-\rangle$
H	0	0	1	1
V	1	1	0	0
+	0	1	1	0
-	1	0	0	1

TABLE I: Truth table used by Bob to extract the bit values.

Attenuation [dB]	SKR [kbps]
0.28	9.7
2.8	5.3
6.8	1.8

TABLE II: SKR obtained at the output of the system after distillation of block size of 10^7 bits for different attenuations.

state encoded by Bob are necessary to retrieve the bit of Alice, using Tab. I. From this table, we can clearly see that knowing which detector clicks gives no information about the state encoded by Alice. Furthermore, there is no correlation between which detector clicks and the choice of Bob.

The security of DDI-QKD is based on the following assumptions: i) Alice and Bob's random number generators as well as the classical post-processing are trusted. This basic assumption is necessary for all QKD schemes, including device-independent (DI-QKD) protocols. ii) Alice and Bob's linear optical circuits are fully characterized and cannot be influenced by any eavesdropper, commonly denoted as Eve. iii) Eve may exploit imperfect detectors via the optical fiber, but she has no physical access to the detectors, in particular she has no access to the outputs of the interferometer. iv) The detectors may have some defects, but are not from a malicious provider. This means they are independent of Eve.

Our security analsis shows that DDI-QKD and MDI-QKD are not equivalent. Nevertheless, under the very reasonable assumptions iii) and iv), it turns out that DDI-QKD is robust against detector side-channel attacks. We conclude that DDI-QKD is more secure than a normal P&M protocol.

We performed an exchange of secret keys with complete distillation - i.e. including finite key analysis and privacy amplification - at three different distances simulated with a variable attenuator. The result are depicted in Tab. II. We obtained a SKR of 1.8 kbps for an attenuation of 6.8 dB corresponding to a distance of 34 km.

We also performed exchange of secret keys for additional distances without taking into account the finite key analysis. The corresponding SKRs and QBERs as a function of the attenuation (converted into fiber distance considering losses of 0.2 dB/km) between Alice and Bob are plotted in Fig. 2. We obtained a SKR of 8.2 bps at 91 km.

In summary, the DDI-QKD protocol overcomes the main disadvantages of the MDI-QKD protocol whilst offering an improved level of security compared to standard P&M protocols. We realized an implementation of DDI-QKD using a platform capable of high speed operation in real-time using state of the art low-noise In-GaAs/InP detectors ideal for long distance QKD.

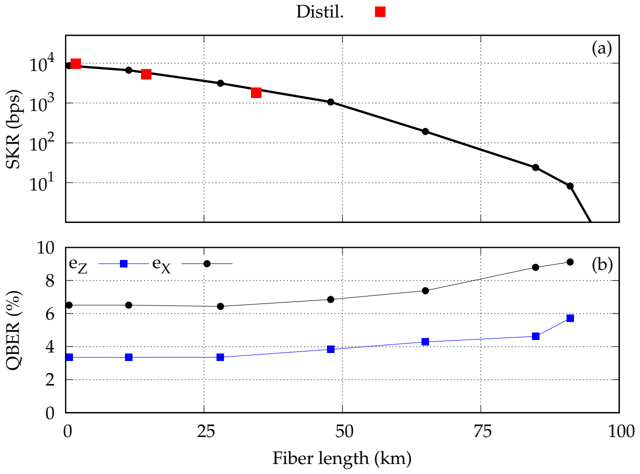

FIG. 2: (a) SKR as a function of the distance. The red squares correspond to complete distillation of a secret key. The black curve corresponds to the SKRs measured without taking into account the finite key statistics. (b) QBER in Z and X basis as a function of the distance.

Acknowledgments

We would like to acknowledge Jesús Martínez-Mateo for providing the error correction code, and Bing Qi and Marcos Curty for helpful discussions. We thank the Swiss NCCR QSIT and the European EMPIR MIQC2 for financial support. C. C. W. Lim acknowledges support from the Oak Ridge National Laboratory directed research and development program.

[*] Electronic address: `alberto.boaron@unige.ch`

[1] C. H. Bennett and G. Brassard, *Quantum Cryptography: Public Key Distribution and Coin Tossing*, Proc. IEEE Int. Conf. Comput. Syst. Signal Process. Bangalore, India p. 175 (1984).

[2] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, *Hacking commercial quantum cryptography systems by tailored bright illumination*, Nat. Photonics **4**, 686 (2010).

[3] H.-K. Lo, M. Curty, and B. Qi, *Measurement-Device-Independent Quantum Key Distribution*, Phys. Rev. Lett. **108**, 130503 (2012).

[4] N. Walenta, A. Burg, D. Caselunghe, J. Constantin, N. Gisin, O. Guinnard, R. Houlmann, P. Junod, B. Korzh, N. Kulesza, et al., *A fast and versatile quantum key distribution system with hardware key distillation and wavelength multiplexing*, New J. Phys. **16**, 013047 (2014), ISSN 1367-2630, 1309.2583, URL `http://stacks.iop.org/1367-2630/16/i=1/a=013047?key=crossref.67d93c8c06267e9ca8c64b7bd7ff240e`.

[5] B. Korzh, C. C. W. Lim, R. Houlmann, N. Gisin, M. J. Li, D. Nolan, B. Sanguinetti, R. Thew, and H. Zbinden, *Provably secure and practical quantum key distribution over 307 km of optical fibre*, Nat. Photonics **9**, 163 (2015).

[6] C. C. W. Lim, B. Korzh, A. Martin, F. Bussières, R. T. Thew, and H. Zbinden, *Detector-device-independent quantum key distribution*, Appl. Phys. Lett. **105**, 221112 (2014).