Detector-device-independent quantum key distribution: From proof of principle to a high speed implementation

B. Korzh, A. Boaron, C. C. W. Lim, A. Martin, G. Boso, R. Houlmann, F. Bussières, R. Thew, and H. Zbinden

Group of Applied Physics, University of Geneva,
Chemin de Pinchat 22, CH-1211 Geneva 4, Switzerland

The security of quantum key distribution (QKD) depends only on the principles of quantum physics and can be proven 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 [1]. 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 (mdiQKD) protocol was proposed [2]. 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, mdiQKD possesses many drawbacks. Firstly, the achievable secure key rates (SKR) are significantly lower compared to conventional prepare and measure (P&M) QKD systems [3, 4]. This is mainly because a two-photon BSM relies on coincidence detections, which sets stringent requirements on the detector efficiency. Another factor is that a two-photon BSM implemented with linear optics is at most 50% efficient and, when using WCSs, the results from one of the bases cannot be used for the raw-key generation due to an inherent 25% error rate [5, 6]. Furthermore, the resource overhead in the finite-key scenario [7] is significantly larger compared to common P&M schemes [4, 8]. Finally, the technological complexity of mdiQKD 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.

We have recently proposed a QKD scheme that overcomes the aforementioned limitations but is still secure against all detector side-channel attacks [9]. This bridges the gap between the superior performance and practicality of P&M QKD schemes and the enhanced security offered by mdiQKD. Our scheme, referred to as detector-device-independent QKD (ddiQKD), essentially follows the idea of mdiQKD, however, instead of encoding separate qubits into two independent photons, we exploit the concept of a two-qubit single-photon (TQSP). This

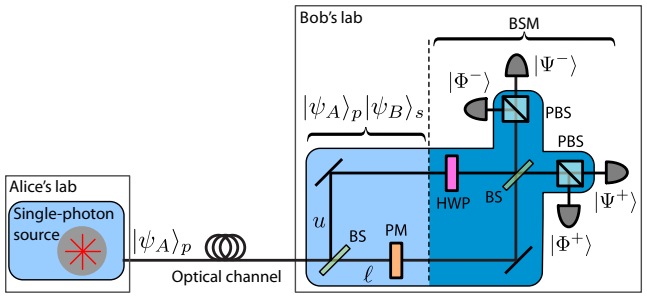

FIG. 1. The conceptual setup. Alice encodes her qubit $|\psi_A\rangle_p$ in the polarization DOF of a single photon, sends it to Bob who encodes his qubit $|\psi_B\rangle_s$ in the spatial DOF using a 50/50 beam splitter (BS) and a phase modulator (PM). Bob then performs a complete and deterministic Bell-State measurement (BSM) on both qubits using a half-wave plate (HWP), polarizing beam splitters (PBS) and single-photon detectors (SPDs). Components inside the shaded regions of Alice and Bob's labs are trusted devices, whilst the SPDs are untrusted.

scheme has the following advantages: (1) it requires only single-photon interference, (2) the linear-optical BSM is 100% efficient [10], (3) the secret key rate scales linearly with the SPD detection efficiency and (4) 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 protocol works as follows; see Fig. 1. Alice first prepares a single photon in the qubit state $|\psi_A\rangle_p$ chosen at random from the following set of BB84 states:

$$|\psi_A\rangle_p \in_r \begin{cases} |+\rangle &= \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle), \\ |-\rangle &= \frac{1}{\sqrt{2}}(|H\rangle - |V\rangle), \\ |+i\rangle &= \frac{1}{\sqrt{2}}(|H\rangle + i|V\rangle), \\ |-i\rangle &= \frac{1}{\sqrt{2}}(|H\rangle - i|V\rangle), \end{cases}$$

where the subscript p indicates this is a qubit in the polarization DOF of the photon. Alice sends $|\psi_A\rangle_p$ to Bob via an untrusted quantum channel. Upon reception of the photon, Bob encodes his random qubit state $|\psi_B\rangle_s$ in the spatial DOF (hence the subscript "s"). To achieve this, Bob sends the photon to a 50/50 beam splitter (BS). We denote $|u\rangle$ and $|\ell\rangle$ the states of the basis defined by the "upper" and "lower"arms after the BS, respectively. He then applies a phase φ chosen at random in the set $\{0, \pi/2, \pi, 3\pi/2\}$ on the lower arm to prepare the state $|\psi_B\rangle_s = (|u\rangle + e^{i\varphi}|\ell\rangle)$, yielding BB84 states in the spatial modes.

a) $|\Phi^+\rangle$

	$+$	$-$	$+i$	$-i$
$+$	0.49	0.01	0.25	0.26
$-$	0.01	0.50	0.25	0.27
$+i$	0.27	0.26	0.01	0.48
$-i$	0.24	0.23	0.50	0.01

b) $|\Psi^+\rangle$

	$+$	$-$	$+i$	$-i$
$+$	0.49	0.02	0.25	0.27
$-$	0.00	0.50	0.27	0.24
$+i$	0.29	0.23	0.49	0.00
$-i$	0.23	0.25	0.01	0.55

c) $|\Psi^-\rangle$

	$+$	$-$	$+i$	$-i$
$+$	0.00	0.48	0.28	0.25
$-$	0.54	0.00	0.25	0.23
$+i$	0.25	0.26	0.01	0.52
$-i$	0.26	0.24	0.50	0.01

d) $|\Phi^-\rangle$

	$+$	$-$	$+i$	$-i$
$+$	0.00	0.47	0.25	0.25
$-$	0.54	0.00	0.23	0.25
$+i$	0.26	0.26	0.48	0.00
$-i$	0.26	0.21	0.00	0.56

TABLE I. Theoretical and experimentally observed probabilities for each Bell state. Rows and columns correspond to Alice's and Bob's states $|\psi_A\rangle_p$ and $|\psi_B\rangle_s$, respectively. Given a certain Bell state k, for each $|\psi_A\rangle_p$ there are four possible $|\psi_B\rangle_s$: white cells should happen with probability $\Pr[k] = 0$, light grey cells with $\Pr[k] = 1/4$ and dark grey cells with $\Pr[k] = 1/2$. The experimentally observed probabilities are written in each cell.

We then define the following Bell states:

$$|\Phi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|H\rangle_p|u\rangle_s \pm |V\rangle_p|\ell\rangle_s), \quad (1)$$

$$|\Psi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|H\rangle_p|\ell\rangle_s \pm |V\rangle_p|u\rangle_s). \quad (2)$$

A complete and deterministic BSM of these states is realized by first applying the unitary transformation $|Hu\rangle \to |Vu\rangle$ and $|Vu\rangle \to |Hu\rangle$ on the upper arm using a half-wave plate (HWP), followed by recombination of the arms on a 50/50 BS, and finally by a projection in the $\{|H\rangle, |V\rangle\}$ basis using two PBSs on the two output arms followed by four SPDs. In this way, a click on each SPD corresponds to a projection on one of the four Bell states; see Fig. 1.

In order to establish a raw key Alice assigns a bit value to her encoded states, i.e. $|+\rangle$ and $|+i\rangle$ encode bit 0, and $|-\rangle$ and $|-i\rangle$ encode bit 1. After the measurement phase, Bob uses an authenticated channel to announce the success of the BSM and reveals the basis he used to encode his qubit. Subsequently, Alice announces whether Bob's basis choice was compatible with hers. Bob can then determine Alice's bit value according to Table I, which shows all of the possible combinations. For example, if $|\psi_B\rangle_s = |+\rangle$, the bit is 0 if he detected $|\Phi^+\rangle$ or $|\Psi^+\rangle$, and 1 otherwise. Importantly, knowledge of the bases used by Alice and Bob, along with which of the Bell states Bob obtained, does not reveal Alice's bit. Hence, Eve does not gain information on the key by controlling Bob's detectors.

We implemented a proof-of-principle experiment as illustrated in Fig. 2. We started with the generation of a pair of correlated photons by type-0 SPDC in a fiber-pigtailed periodically-poled lithium-niobate waveguide (PPLN-WG). The signal and idler photons were deterministically separated by dense wavelength division

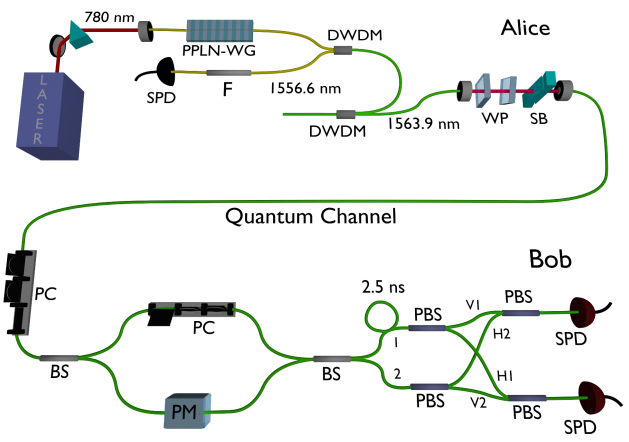

FIG. 2. Experimental realization of the proof-of-priciple ddiQKD protocol. Labelled components include, dense wavelength division multiplexers (DWDM), bandpass filter (F), waveplates (WP), Soleil-Babinet compensator (SB), polarization controllers (PC), phase modulator (PM), 50/50 beam splitters (BS), polarizing beam splitters (PBS) and single-photon detectors (SPD).

multiplexers. The polarization of the heralded signal photon was set to $|+\rangle$ before passing through a Soleil-Babinet, which allowed us to rotate the state around the equator of the Bloch sphere and prepare Alice's single-photon state. Bob's device consisted of a balanced interferometer, with a polarization controller in the upper arm acting as a HWP and a piezo phase modulator in the lower arm. The outputs of the BSM corresponding to $|\Phi^-\rangle$ and $|\Psi^-\rangle$ were delayed by 2.5 ns before being combined using two PBSs (see Fig. 2) with the other two outputs, which allowed the use of two detectors for all four outcomes. Bob's free-running InGaAs SPDs were cooled with a Stirling cooler to -90°C and had a dark count rate of less than 50 cps at 25% efficiency [11]. The detection events were recorded by a time-to-digital converter (TDC).

To analyze the detection outcomes for all combinations of Alice and Bob's settings, we fixed the state prepared by Alice and scanned the phase of Bob's interferometer. Table I shows the theoretical Bell-state announcement probability for every combination of Alice and Bob's settings. We complete this correlation table with the experimental results and find that the protocol functions as expected with an overall quantum bit error rate of $1.5 \pm 0.5\%$. The total detection rate was around 60 cps.

In order to implement the ddiQKD protocol in full, Alice and Bob need to randomly select four phase settings corresponding to the four BB84 states as outlined previously. We have recently developed a versatile QKD platform based on field programmable gate arrays (FPGAs) capable of operating at gigahertz frequencies [3]. All of the necessary components required for secret key establishment are integrated into the platform, including key sifting, error reconciliation, privacy amplification

and authentication, all running in real time. Using this platform, we have recently achieved a new QKD distance record of 307 km whilst using the coherent one-way protocol [4]. Crucially, this demonstration was carried out using compact InGaAs/InP single photon detectors, which achieve record low dark count rates [11] and are much more practical compared to detectors operating an cryogenic temperatures. Moreover, finite-key effects were also taken into account, something that has so far been neglected in all record distance QKD demonstrations.

We have now adapted the same high speed platform and low noise detectors for use with the ddiQKD protocol. On Alice's side, the states are prepared at a rate of 625 MHz, achieved with a pulsed laser which ensures that the phase is randomized from pulse-to-pulse. The state is encoded in the polarization DOF by using an ultrafast birefringence modulator scheme as used in Ref. [12]. All of the communication used for the classical post-processing and clock distribution is transfered between Alice and Bob using a two optical service channels, which are wavelength division multiplexed together with the quantum channel on a single fibre [3]. We use the signal from the service channels in order to stabilize the polarization in the quantum channel in real-time, a scheme similar to Ref. [13]. This ensures that on the input to Bob's device the states are well aligned and his qubit encoding can be done correctly. Bob encodes his qubit in the spatial DOF using a self-compensating Sagnac interferometer and a high speed birefringence modulator. As with the proof-of-principle experiment, only two single photon detectors are needed for the detection thanks to temporal multiplexing as described previously.

The new high speed ddiQKD implementation is being tested with both a weak coherent pulse emission from Alice's source, as well as a using the decoy state method. The former will suffer from a limited distance, which arises due to the prevention of the photon-number splitting attack. However, this is still attractive due to the simplicity of the implementation, for short distance, high speed implementations where the single photon detectors might be saturated regardlessly. The decoy state version of the source will achieve a significantly longer maximum distance.

In summary, the ddiQKD protocol overcomes the main disadvantages of the mdiQKD protocol whilst offering the same level of security. Here we present the main concepts of the protocol followed by a proof-of-concept experiment carried out with a heralded single photon source. We then go on to demonstrate the implementation of ddiQKD using a platform capable of high speed operation in real-time using state of the art low-noise InGaAs/InP detectors ideal for long distance QKD. This will yield SKRs and level of complexity comparable with existing GHz clocked systems using P&M protocols [3, 4], whilst eliminating any detector side channels, which is one of the main remaining concerns in the QKD community.

[1] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Nat. Photonics **4**, 686 (2010).

[2] H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. **108**, 130503 (2012).

[3] N. Walenta, A. Burg, D. Caselunghe, J. Constantin, N. Gisin, O. Guinnard, R. Houlmann, P. Junod, B. Korzh, N. Kulesza, M. Legré, C. C. W. Lim, T. Lunghi, L. Monat, C. Portmann, M. Soucarros, R. T. Thew, P. Trinkler, G. Trolliet, F. Vannel, and H. Zbinden, New J. Phys. **16**, 013047 (2014), 1309.2583.

[4] B. Korzh, C. C. W. Lim, R. Houlmann, N. Gisin, M. J. Li, D. Nolan, B. Sanguinetti, R. Thew, and H. Zbinden, Nature Photonics **9**, 163168 (2015).

[5] A. Rubenok, J. A. Slater, P. Chan, I. Lucio-Martinez, and W. Tittel, Phys. Rev. Lett. **111**, 130501 (2013).

[6] T. Ferreira da Silva, D. Vitoreti, G. B. Xavier, G. C. do Amaral, G. P. Temporão, and J. P. von der Weid, Phys. Rev. A **88**, 052303 (2013).

[7] M. Curty, F. Xu, W. Cui, C. C. W. Lim, K. Tamaki, and H.-K. Lo, Nat. Commun. **5** (2014).

[8] C. C. W. Lim, M. Curty, N. Walenta, F. Xu, and H. Zbinden, Phys. Rev. A **89**, 022307 (2014).

[9] C. C. W. Lim, B. Korzh, A. Martin, F. Bussires, R. Thew, and H. Zbinden, Applied Physics Letters **105**, 221112 (2014).

[10] D. Boschi, S. Branca, F. De Martini, L. Hardy, and S. Popescu, Phys. Rev. Lett. **80**, 1121 (1998).

[11] B. Korzh, N. Walenta, T. Lunghi, N. Gisin, and H. Zbinden, Appl. Phys. Lett. **104**, 081108 (2014).

[12] T. Lunghi, J. B. Brask, C. C. W. Lim, Q. Lavigne, J. Bowles, A. Martin, H. Zbinden, and N. Brunner, Phys. Rev. Lett. **114**, 150501 (2015).

[13] G. B. Xavier, N. Walenta, G. V. de Faria, G. P. Temporao, N. Gisin, H. Zbinden, and J. P. von der Weid, New Journal of Physics **11**, 045015 (2009).