Detector-device-independent quantum key distribution

Charles Ci Wen Lim, Boris Korzh, Anthony Martin, Félix Bussières, Rob Thew, and Hugo Zbinden

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

(Received 15 October 2014; accepted 21 November 2014; published online 4 December 2014)

Recently, a quantum key distribution (QKD) scheme based on entanglement swapping, called measurement-device-independent QKD (mdiQKD), was proposed to bypass all measurement side-channel attacks. While mdiQKD is conceptually elegant and offers a supreme level of security, the experimental complexity is challenging for practical systems. For instance, it requires interference between two widely separated independent single-photon sources, and the secret key rates are dependent on detecting two photons—one from each source. Here, we demonstrate a proof-of-principle experiment of a QKD scheme that removes the need for a two-photon system and instead uses the idea of a two-qubit single-photon to significantly simplify the implementation and improve the efficiency of mdiQKD in several aspects. © 2014 AIP Publishing LLC.

[http://dx.doi.org/10.1063/1.4903350]
The protocol works as follows: see Fig. 1. Alice first prepares a single photon in the qubit state $|\psi_{A}\rangle_p$ chosen uniformly at random from the following set of BB84 states:

$$
|\psi_{A}\rangle_p \in \begin{cases} 
|+\rangle = \frac{1}{\sqrt{2}} (|H\rangle + |V\rangle), \\
|-\rangle = \frac{1}{\sqrt{2}} (|H\rangle - |V\rangle), \\
|+i\rangle = \frac{1}{\sqrt{2}} (|H\rangle + i|V\rangle), \\
|-i\rangle = \frac{1}{\sqrt{2}} (|H\rangle - i|V\rangle),
\end{cases}
$$

where the subscript $p$ indicates that 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 $|f\rangle$ the states of the basis defined by the “upper” and “lower” arms after the BS, respectively. He then applies a phase $\varphi$ chosen uniformly at random in the set $\{0, \pi/2, \pi, 3\pi/2\}$ on the lower arm to prepare the state $|\psi_{B}\rangle_s = (|u\rangle + e^{i\varphi}|f\rangle)$, yielding BB84 states in the spatial modes. Both DOFs are so far been created and manipulated independently of each other, and thus, the two-qubit state can be written as $|\psi_{A}\rangle_p \otimes |\psi_{B}\rangle_s$.

We then define the following Bell states:

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

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

A complete and deterministic BSM of these states is realized by first applying the unitary transformation $|Hu\rangle \rightarrow |Vu\rangle$ and $|Vu\rangle \rightarrow |Hu\rangle$ on the upper arm using a half-wave plate (HWP), followed by the recombination of the arms on a 50/50 BS, and finally by a projection in the $\{|H\rangle, |V\rangle\}$ basis using two polarizing beam splitters (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.

![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 BS and a phase modulator (PM). Bob then performs a complete and deterministic BSM on both qubits using a HWP, PBSs and SPDs. Components inside the shaded regions of Alice and Bob’s labs are trusted devices, whilst the SPDs are untrusted.](image)

To show how the raw key establishment works, let us first define the mutually unbiased bases $B_{X} = \{+i, -i\}$ and $B_{Y} = \{+i, -i\}$. The bit to be established is encoded in Alice’s state, i.e., $|+\rangle$ and $|-i\rangle$ encode bit 0 and $|-\rangle$ and $|+i\rangle$ encode bit 1. After the measurement phase, Bob announces 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. If more than one detector clicks, Bob announces a successful BSM and assigns a random bit value. Importantly, the 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 cannot gain information about the key by controlling Bob’s detectors.

From a security point of view, it is important to consider carefully the operation of Bob’s device. Strictly speaking, the mathematical description of his qubit, outlined previously, holds only if the light state entering the first BS is a single-photon excitation of a single optical-temporal mode. As with any other QKD scheme, it is not possible to guarantee this. Indeed, Eve may send multi-photon states through the quantum channel and break the qubit description. However, such an attack is only detrimental if she can interact with Bob’s prepared states, e.g., via unambiguous state discrimination measurements. This is not possible since the adversary can only interact with Alice’s qubits. In particular, Eve cannot access the output of Bobs interferometer. Additionally, if the input is a multi-photon state, then with an increased probability, more than one detector clicks, in which case Bob would pick a random bit value, increasing the errors in the raw bit string. This is due to the fact that the optical linear circuit of the BSM randomizes the encoded state.

The security of our scheme requires that the final light state (just before the SPDs), taken over all possible encoding choices, is independent of the input light state. In particular,

**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. The relative uncertainty for each measurement was 1%.

|       | $|\Phi^{+}\rangle$ | $|\Psi^{+}\rangle$ |
|-------|-------------------|-------------------|
| $|+\rangle$ | 0.49 | 0.01 | 0.25 | 0.26 | 0.49 | 0.02 | 0.25 | 0.27 |
| $|-\rangle$ | 0.01 | 0.25 | 0.25 | 0.27 | 0.00 | 0.50 | 0.27 | 0.24 |
| $|+i\rangle$ | 0.27 | 0.26 | 0.01 | 0.48 | 0.29 | 0.23 | 0.49 | 0.00 |
| $|-i\rangle$ | 0.24 | 0.23 | 0.50 | 0.01 | 0.23 | 0.25 | 0.01 | 0.53 |
| $|\Phi^{-}\rangle$ | $|\Psi^{-}\rangle$ | $|\Phi^{+}\rangle$ | $|\Psi^{+}\rangle$ | $|\Phi^{-}\rangle$ | $|\Psi^{-}\rangle$
| $|+\rangle$ | 0.00 | 0.28 | 0.28 | 0.25 | 0.00 | 0.28 | 0.25 | 0.25 |
| $|-\rangle$ | 0.25 | 0.00 | 0.25 | 0.23 | 0.25 | 0.00 | 0.23 | 0.25 |
| $|+i\rangle$ | 0.25 | 0.26 | 0.01 | 0.22 | 0.26 | 0.28 | 0.00 | 0.00 |
| $|-i\rangle$ | 0.26 | 0.24 | 0.50 | 0.01 | 0.26 | 0.21 | 0.00 | 0.53 |
for any input state with a given $n$-photon excitation, the average final state after passing through the linear optical circuit is a fixed state. This requirement is in fact similar to the one used in the security analysis of BB84, where the average of the BB84 states has to be independent of the basis choice.32

Once this requirement is met, the security of the scheme can be obtained following proof techniques for the BB84 QKD scheme. A common method to prove the security of P&M QKD schemes is to consider an equivalent entanglement-based version, where Alice and Bob make random measurements on bipartite quantum states distributed by the adversary. To this end, we point to a formalism that allows us to see Bob’s linear optical circuit as random measurements made on some entangled bipartite state.

First, let us relate the two different DOFs, i.e., $A_p$, $B_p$ denoting the polarization states of Alice and Bob, respectively, while $B_s$ denotes Bob’s spatial state. Since Alice is able to prepare the four polarization BB84 states correctly, it is equivalent to consider the entanglement-based version, where Alice first prepares a two-qubit maximally entangled state, $|\Phi^+\rangle$, and then performs a projective measurement on one half of the state to prepare the other half for Bob. Mathematically, we have $M_i \otimes \Pi_i^{(\Phi^+)} |\Phi^+\rangle_{A_B} \otimes |s\rangle_{B_s}$, where $M_i$ is the positive-operator valued measure (POVM) element corresponding to preparation $x \in \{+, -, +i, -i\}$ and $|s\rangle_{B_s}$ is an auxiliary state related to the spatial DOF.

Second, Alice sends the quantum systems $B_s$ and $B_t$ using a single photon through the quantum channel to Bob. At this point, the resulting state is not necessarily a single photon state. In this case, the state, after tracing out system $A_p$, is described by a bipartite density operator, $\rho_{C_s,C_t}$, whose dimension is unknown but fixed. To proceed, we use a result from Ref. 33, Lemma 1, which says that if, for any input state, the linear optical circuit (parameterized by $\phi$) outputs a state that is fixed on the average, the encoding can be seen as a purified measurement acting on the same input state and one half of a bipartite pure state, where the other half of the bipartite is the same output state. More formally, let the linear optical circuit be described by a set of completely positive trace-preserving maps, $\{\mathcal{E}_\phi\}_\phi$, taking the input quantum system $C_i$ to an output quantum system $D_i$, such that for any input quantum state $\rho_{C_i}$, the output quantum state is fixed over all possible encoding choices, i.e., $1/4 \sum_{\phi} \mathcal{E}_\phi(\rho_{C_i}) = \rho_{D_i}$ for any $\rho_{C_i}$. Then, the linear optical circuit is equivalent to making a joint measurement $\{F^{\phi}_{C,K}\}_\phi$ on the same input state, $\rho_{C_i}$, and one half of a bipartite pure state, $|\sigma\rangle_{K,D_i}$, living in a joint quantum system $K_i \otimes D_i$, where the other half gives the fixed state $\rho_{D_i}$. Therefore, the purification provides a method to analyze the security of our scheme in an entanglement-based picture, where Alice makes random BB84 measurements on one half of a bipartite quantum state and Bob makes random purified measurements on the other half.

Finally, the security of ddiQKD follows directly from that of the BB84 QKD scheme, with the additional benefit that detectors are excluded from the security analysis. In particular, the security can be obtained by using the entropic uncertainty relation proof technique27,34 in the asymptotic limit, and under the approximation that the BB84 polarization states are prepared correctly, the secret key fraction is $\alpha 1 - 2h(Q)$, where $h$ is the binary entropy function and $Q$ is the error rate of the sifted key. In fact, the finite-key security performance of ddiQKD with the decay-state method35-37 is expected to be similar to the one of Ref. 27, but with a slightly shorter maximum distance due to a higher overall dark count rate since four SPDs are needed instead of two.

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).38 The waveguide was pumped with a continuous wave diode laser (Topica DL100), and the signal and idler photons were deterministically separated by dense wavelength division multiplexers. The idler photon was detected by a free-running InGaAs single-photon detector (ID Quantique ID220). 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 operated at $-90{\degree}C$ and had a dark count rate of less than 50 cps at 25% efficiency.39 The detection events were recorded by a time-to-digital converter (TDC). The $g^{(2)}(0)$ of the single photons at Alice was about $10^{-3}$ in a 1 ns coincidence window. The probability of having a double detection at Bob was $<10^{-6}$.

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. Figure 3 shows four graphs, one for each of the polarization states chosen by Alice, representing the normalized probability of each Bell-state being announced at any given phase setting in Bob’s interferometer. The measurement points were fitted in order to calculate the visibility, with the highest average value obtained being $99.2\% \pm 1.5\%$ for the $|+\rangle$ input state and the lowest value of $96.0\% \pm 2.1\%$ for the $|\rangle$ state.

![FIG. 2. Experimental realization of the ddiQKD protocol. Labelled components include, dense wavelength division multiplexers (DWDM), bandpass filter (F), waveplates (WP), Soleil-Babinet compensator (SB), polarization controllers (PC), PM, 50/50 BS, PBS, and SPD.](image-url)
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 by selecting points from Fig. 3 closest to the desired settings for Bob. The experimental values coincide with the predictions with an overall quantum bit error rate, $Q$, of $1.5 \pm 0.5\%$. The total detection rate was around 60 cps.

While the concept of ddiQKD is fundamentally the same as mdiQKD, some subtleties need to be pointed out. For instance, in mdiQKD, the whole measurement device can be untrusted, whilst in ddiQKD, the trusted device boundary in Bob’s laboratory must include the linear optical elements, leaving only the SPDs as untrusted devices. This is a reasonable factor to consider, since it is typically the detectors themselves which are the most vulnerable part of a QKD system (see recent review$^4$ for attacks targeting the detectors), whilst it is much easier to fully characterize the linear optical elements.$^{40}$ This means that Eve can have full control of the detectors, e.g., she can control their response functions.$^{41}$ However, Bob has to ensure that no additional information, other than the outcome of the BSM, leaks out of his lab. As with any other one-way QKD system, including mdiQKD, to prevent Trojan-horse attacks,$^{42}$ attempting to use back reflections, Alice and Bob have to install optical isolators and spectral filters. For an extended discussion of the security assumptions, please refer to Ref. 29.

In practice, an implementation of ddiQKD using WCSs together with the decoy-state method could yield SKRs comparable with existing GHz clocked systems.$^{19–22}$ In particular, ultra-fast generation of polarization states could be achieved using a birefringence modulator scheme as used in Ref. 29. We would like to acknowledge Gustavo Lima, Guilherme Xavier, and Marcos Curty for stimulating discussions regarding the basic idea. We thank ID Quantique and Battelle for the PPLN-WG and the Swiss NCCR QSIT for financial support.

We would like to acknowledge Gustavo Lima, Guilherme Xavier, and Marcos Curty for stimulating discussions regarding the basic idea. We thank ID Quantique and Battelle for the PPLN-WG and the Swiss NCCR QSIT for financial support.

In summary, we demonstrated a proof-of-principle experiment of the ddiQKD protocol, which overcomes the main disadvantages of the mdiQKD protocol whilst offering the same level of security. Future theoretical work should focus on deriving a bound on the extractable key length in a finite key scenario. This work paves the way to practical, high-performance, and detector-side-channel free QKD.

FIG. 3. Experimental Bell-state measurement outcomes as a function of the phase setting inside Bob’s interferometer. Four sets of measurements are shown, one for each of the possible states sent by Alice.


$^{9}$H. Inamori, Algorithmica 34, 340 (2002).


$^{18}$Star-type networking is possible with P&M systems; however, the central node would have to be trusted.


For a WCS, \( P_1(l) = \mu e^{-\mu l} \), where \( \mu < 1 \) is the average photon number per pulse. Typical values of \( \mu \) are 10\%-30\% for practical InGaAs SPDs.

\[ P_1(l) = \mu e^{-\mu l} \]

In practice, this requirement could be fulfilled by adding appropriate filtering to ensure that the light state belongs to the correct optical mode.