High-dimensional measurement-device-independent quantum key distribution on two-dimensional subspaces

Dellantonio, Luca; Sørensen, Anders S.; Bacco, Davide

Published in:
Physical Review A

Link to article, DOI:
10.1103/PhysRevA.98.062301

Publication date:
2018

Document Version
Publisher's PDF, also known as Version of record

High-dimensional measurement-device-independent quantum key distribution on two-dimensional subspaces

Luca Dellantonio,[1,2,*] Anders S. Sørensen,[1,2] and Davide Bacco[3,†]

[1]*The Niels Bohr Institute, University of Copenhagen, Blegdamsvej 17, DK-2100 Copenhagen Ø, Denmark*

[2]*Center for Hybrid Quantum Networks (Hy-Q), Niels Bohr Institute, University of Copenhagen, Blegdamsvej 17, DK-2100 Copenhagen Ø, Denmark*

[3]*CoE SPOC, DTU Fotonik, Department of Photonics Engineering, Technical University of Denmark, Orsteds Plads 340, DK-2800 Kongens Lyngby, Denmark*

(Received 18 July 2018; published 3 December 2018)

Quantum key distribution (QKD) provides ultimate cryptographic security based on the laws of quantum mechanics. For point-to-point QKD protocols, the security of the generated key is compromised by detector side channel attacks. This problem can be solved with measurement-device-independent QKD (mdi-QKD). However, mdi-QKD has shown limited performances in terms of the secret key generation rate, due to postselection in the Bell measurements. We show that high-dimensional (Hi-D) encoding (qudits) improves the performance of current mdi-QKD implementations. The scheme is proven to be unconditionally secure even for weak coherent pulses with decoy states, while the secret key rate is derived in the single-photon case. Our analysis includes phase errors, imperfect sources, and dark counts to mimic real systems. Compared to the standard bidimensional case, we show an improvement in the key generation rate.

DOI: 10.1103/PhysRevA.98.062301

I. INTRODUCTION

Digital security is important for several aspects of modern life. Classical cryptography only promises to make decryption hard, but not impossible. On the contrary, quantum key distribution (QKD) is based on the laws of physics, theoretically allowing parties to share cryptographic keys in an unconditionally secure way [1]. However, several physical requirements have to be satisfied to provide unconditional security, and most experimental implementations of QKD have proven to be vulnerable to attacks [2–11]. These attacks mainly exploit weaknesses in the detectors, whereas the sources are less vulnerable. To overcome this limitation, device-independent QKD (di-QKD) [1,12–14] and measurement-device-independent QKD (mdi-QKD) [15] were introduced to decrease the reliance on the physical setup. While di-QKD remains challenging due to technical limitations, including the need for extremely efficient detection [1], mdi-QKD is ready to be implemented in real networks.

Mdi-QKD was introduced by Lo *et al.* in Ref. [15]. Here, the two parties Alice and Bob only use photon sources, while the detection is performed by a third party, Charlie. Different degrees of freedom have been used to demonstrate the feasibility of this scheme (e.g., polarization, phase, time, and space) [15–17]. Compared to other QKD protocols, however, mdi-QKD has shown low key generation rates. To reduce this limitation, high-dimensional (Hi-D) encoding can be used to improve the photon information efficiency (PIE) [18]. Recent results have shown how spatial or temporal modes can be used to increase the dimension of the Hilbert space [19–23] for standard QKD. We propose a protocol, where Alice and Bob generate qudits (quantum states in N dimensions) encoded in different paths or time slots of the photons. These photons then interfere at Charlie's beam splitters (BSs), as shown in Fig. 1. As discussed below, the measurement projects the qubits into a two-dimensional subspace, which can be used for QKD. In the following, we analyze this high-dimensional mdi–QKD protocol, considering the main sources of errors, such as, imperfect photon generation, dark counts, and (unknown) phase shifts. We prove that high-dimensional mdi-QKD is unconditionally secure for coherent states with the decoy state technique [15,24], and we analyze the key generation rate for single-photon sources. In analogy to a similar result for standard QKD [23], we find that our Hi-D mdi-QKD protocol is advantageous, particularly in the detector saturation regime, where the time between photon clicks at Charlie's detectors is comparable to the detectors' dead time τ_d. We study the protocol both for time and space encoding, and we analyze the practical constraints that make one encoding better than the other. A different Hi-D mdi-QKD scheme was proposed in Ref. [18], but remains experimentally unfeasible, since discriminating Bell states in high dimensions is impossible by simple means [25,26]. In comparison, our protocol can be implemented without significant increase in the complexity of existing setups. In particular, for weak coherent states and time encoding, no change in the hardware is required.

II. PROTOCOL DEFINITION

Most QKD protocols are based on mutually unbiased bases (MUBs). Usually, the computational Z basis ($\{|0\rangle, |1\rangle\}$

*luca.delantonio@nbi.ku.dk

†dabac@fotonik.dtu.dk

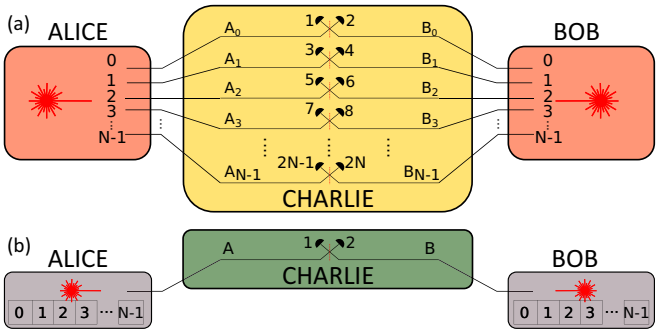

FIG. 1. Schematic of the proposed setup for Hi-D-mdi QKD. (a) Space is used to encode information in different paths (multicore fibers can be used as transmission channels). $2N$ single-photon detectors are necessary for this configuration. (b) Time-encoding scheme, where different time slots are used to encode the qudits. The number of detectors is independent of the dimension N.

for qubits) is less susceptible to errors than the X basis ($\{|\phi_0\rangle, |\phi_1\rangle\}$, with $|\phi_0\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ and $|\phi_1\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$). This is also the case for the encodings in Fig. 1, where different wave packets may dephase, but are unlikely to switch from one bin to another. Thus, the Z basis is used for key generation, and the X basis for error estimation. Generalizations of the Z and X bases are, respectively, $\{|0\rangle, |1\rangle, \ldots, |N-1\rangle\}$ and $\{|\phi_0\rangle, \ldots, |\phi_{N-1}\rangle\}$. Here, $|\phi_i\rangle$ are the N orthonormal superpositions of all the elements of the Z basis, with equal and real weights. As an example, for $N = 4$:

$$|\phi_0\rangle = \tfrac{1}{2}(|0\rangle + |1\rangle + |2\rangle + |3\rangle), \tag{1a}$$

$$|\phi_1\rangle = \tfrac{1}{2}(|0\rangle - |1\rangle - |2\rangle + |3\rangle), \tag{1b}$$

$$|\phi_2\rangle = \tfrac{1}{2}(|0\rangle + |1\rangle - |2\rangle - |3\rangle), \tag{1c}$$

$$|\phi_3\rangle = \tfrac{1}{2}(|0\rangle - |1\rangle + |2\rangle - |3\rangle). \tag{1d}$$

Our N-dimensional mdi-QKD protocol for two MUBs is given by the following procedure.

(i) Alice and Bob choose, with probability $P_b \in (0, 1)$, the Z basis and, with probability $1 - P_b$, the X basis.

(ii) Alice and Bob randomly generate one of the N qudits in the chosen basis and send it to Charlie.

(iii) Whenever Charlie gets a coincidence click of two detectors, he publicly announces the outcome of his measurement. Otherwise, the event is discarded.

(iv) Steps (i) to (iv) are repeated to have enough statistics to estimate the quantum bit error rate (QBER) and sufficiently many bits of key.

(v) Alice and Bob announce their bases and estimate the QBER. If the QBER is too high, they abort the protocol.

(vi) Alice and Bob proceed with classical error correction and privacy amplification.

For simplicity (when not otherwise specified), we describe the protocol in the space encoding of Fig. 1(a), with straightforward generalization to the time encoding. Assume first that Alice and Bob both choose the Z basis. Whenever they send the same element $|i\rangle$, two photons arrive at the same BS and bunch together. There is thus no coincidence event, and the outcome is discarded. When Alice and Bob generate different states $|i\rangle$ and $|j\rangle$ ($i \neq j$), these photons necessarily end up in different detectors, and Charlie gets a coincidence click. The measurement collapses the state onto the two-dimensional space $\{|i\rangle_A \otimes |j\rangle_B; |j\rangle_A \otimes |i\rangle_B\}$, with the first state being Alice's and the latter Bob's. As an eavesdropper, Eve cannot distinguish whether Alice sent the state $|i\rangle$ and Bob $|j\rangle$ or vice versa and thus can only guess with 50% probability the bit of key. In the X basis, interference only allows half of all possible coincidence clicks to happen, and this permits determining the QBER relative to all two-dimensional subspaces. For example, consider the case $N = 2$, and assume that both Alice and Bob send states with the same phase. Then, only coincidences on the same side of the BSs of Fig. 1(a) are allowed. If Alice and Bob choose different phases, opposite outcomes are permitted. This concept is generalizable to $N > 2$, considering that the detection collapses the state onto a two-dimensional subspace, so that only the relative phases within this subspace matter. Alice and Bob can thus determine the contributions $\epsilon_x^{i,j}$ to the QBER ϵ_x, where $i, j = 0, \ldots, N-1$ are all possible indices of the two-dimensional subspaces of the composite Hilbert space. For finite key length and high dimensions, there may be insufficient statistics to estimate each individual error rate, $\epsilon_x^{i,j}$. In this case, the QBER can be determined by merging all X measurements into a single error rate, ϵ_x. The QBER for the N-dimensional protocol can thus be estimated with the same resources as for the standard two-dimensional protocol [27]. If the error rates $\epsilon_x^{i,j}$ are different (e.g., due to different detectors), a better key rate can be obtained by treating the errors independently. For simplicity, we restrict ourselves to the simplest strategy and only consider a single error rate, ϵ_x.

III. SECRET KEY RATE

We first prove that our Hi-D protocol is unconditionally secure, both for single-photon sources and for coherent states with the decoy state method [24]. Then, we investigate all elements of the setup—sources, channels, and detectors—to determine the QBER and the raw key generation rate per application of the protocol (R_p) in the single-photon case and for realistic experimental conditions. Finally, we consider the detector saturation regime.

In order to prove that Hi-D mdi-QKD is unconditionally secure, we show that the security of the N-dimensional protocol follows from the two-dimensional case [15,28–30]. The key argument is that, whenever Charlie announces a coincidence click, the wave function is projected onto a two-dimensional subspace, with all other states being erased by the measurement. As an example, consider Fig. 1(a), and assume that one of detectors 1 and 2 and one of detectors 7 and 8 click. The system is thus projected onto the Bell states $(|0\rangle_A|3\rangle_B \pm |3\rangle_A|0\rangle_B)/\sqrt{2}$, with the sign determined by the parity of the measurement (clicks in 1 and 7 or in 2 and 8 lead to a plus, clicks in 1 and 8 or in 2 and 7 lead to a minus). It follows that, if Alice and Bob both choose the X basis, all states other than $|0\rangle$ and $|3\rangle$ are erased by the measurement. On the other hand, if the Z basis is used, the parties have to have chosen these particular states as qudits. Every successful realization of the Hi-D protocol is thus equivalent to an application of the

two-dimensional protocol, with the specific states identified by Charlie's measurement.

To complete the security proof, we follow Ref. [15] and consider the virtual qudit approach [31]. We imagine that both parties prepare an entangled state of two qudits, of which one is sent to Charlie and the other (the virtual one) is kept. The traveling photons are then encoded in the basis states by measuring the virtual qudits. Since these measurements can be postponed until after Charlie's outcome is revealed, and since this outcome projects the state onto a two-dimensional subsystem, the protocol is equivalent to the entanglement-based protocol for qubits [32,33].

The secret key rate r can be derived from Refs. [15,31,34,35] as

$$r = R[1 - H(\epsilon_x) - f(\epsilon_z)H(\epsilon_z)], \tag{2}$$

where R is the raw key rate, $f(x) \geqslant 1$ is an inefficiency function for the error correction, and $H(x)$ is the binary entropy. The same security proof can be adapted to the case of weak coherent pulses with the decoy state technique [15]. Since the measurement collapses the system to a two-dimensional subspace, high-dimensional entanglement cannot be fully exploited with the current settings. It is thus not surprising that the Hi-D protocol can be described in terms of standard mdi-QKD protocols. However, as we see in the following, our protocol still allows for improvements.

With the protocol proven to be unconditionally secure, we now estimate the key rate taking into account realistic sources, channels, and detectors. Above and in the following we assume identical channels and detectors [36].

Sources. In Hi-D mdi-QKD both Alice and Bob are required to generate qudits. These Hi-D photons have to interfere to generate the key and therefore need to be identical. We quantify the errors introduced by distinguishable photons, assuming different shapes of the emitted photons. This can be described by expanding Alice's state $|i_A\rangle_A$ $(i = 0, \ldots, N-1)$ in terms of Bob's wave function according to $|i_A\rangle_A \to \beta|i_B\rangle_A + \sqrt{1-|\beta|^2}|I\rangle_A$, where $|I\rangle_A$ shares the encoding of Bob's state (meaning that is in the same path or time slot), but is in one or more modes other than $|i_B\rangle_A$. If both parties use the Z basis, there should never be coincidences between detectors associated with the same BS in Fig. 1(a), and if the photons are in different paths it does not matter if they are distinguishable. Hence, the influence of distinguishable photons can be identified and never leads to errors in the key rate. However, for the X basis, there is a probability $|\beta|^2$ that the photons interfere correctly and a probability $1-|\beta|^2$ that they click at random detectors, thus incrementing the QBER ϵ_x by $(1-|\beta|^2)/2$.

Channels. The most general errors affecting qudits in transmission lines are bit flips and phase shifts [37]. We neglect the first ones, since the probability that a photon disappears and reappears in another spatially or temporally separated slot is small [20,21]. Instead, within the transmission channel any state $|i\rangle_J$ acquires a random phase, such that $|i\rangle_J \to e^{i\theta_i^J}|i\rangle_J$. Here, $i = 0, \ldots, N-1$ and $J = A$ and B indicates whether the qudit was generated by Alice or Bob. Like before, the Z basis is unaffected by phase noise, since bits of key are only exchanged when photons do not interfere. However, for any pair of elements in the X basis, interference prevents half of the allowed coincidence clicks. Whenever phase noise affects the qudits, wrong clicks happen with a probability $[1 - \langle\cos(\theta_i^A - \theta_j^A - \theta_i^B + \theta_j^B)\rangle]/2$, with $i \neq j$ (the case $i = j$ is automatically discarded). To quantify this effect, a noise model for the random variables $\theta_i^A - \theta_j^A$ and $\theta_j^B - \theta_i^B$ is required. Different models are better suited for different transmission lines and encoding schemes. In the space model, we consider a homogeneous situation, such that relative phases $\theta_i^A - \theta_j^A$ and $\theta_j^B - \theta_i^B$ are Gaussian distributed, with zero average and identical variance σ^2. In the time domain, phase drifts in the sources can be added as independent noise contributions. Here, we assume white noise between subsequent pulses, such that the variances of $\theta_i^A - \theta_j^A$ and $\theta_j^B - \theta_i^B$ are $|i-j|\sigma^2$. Alternatively, if the interferometer is slowly drifting, an appropriate model would be $|i-j|^2\sigma^2$.

Detection. For long distances, dark counts prevail over real clicks, increasing the QBER. We define P_{dc} as the probability that a single detector clicks without a photon, and we define $P_s = \eta 10^{-\alpha_0 d/10}$ as the probability that a photon arrives at a detector and clicks. Here, η is the detector's efficiency, α_0 the fiber loss coefficient, and d the distance separating both Alice and Bob from Charlie. In the Z basis, Alice and Bob verify if Charlie's announcement is compatible with the qudit they sent. A wrong bit of key is shared if and only if Alice and Bob send the same state and a bit flip (induced by dark counts) occurs. If none or one photon arrives, a random bit of key is shared with probabilities $4\frac{N-1}{N}(1-P_s)^2P_{\mathrm{dc}}^2(1-P_{\mathrm{dc}})^{2N-2}$ (zero photons arrive) and $4\frac{N-1}{N}P_s(1-P_s)P_{\mathrm{dc}}(1-P_{\mathrm{dc}})^{2N-2}$ (one photon arrives). In case both photons click at the detectors, the probability to share a correct bit is $\frac{N-1}{N}P_s^2(1-P_{\mathrm{dc}})^{2N-2}$. A wrong bit is produced by two photons bunching together and a different detector firing, which happens with probability $2\frac{N-1}{N}P_s^2P_{\mathrm{dc}}(1-P_{\mathrm{dc}})^{2N-2}$. From these, it is possible to find how many wrong bits of key are shared on average and thus to find the QBER ϵ_z and the raw rate per application of the protocol R_p in the Z basis.

We now explicitly calculate the QBER ϵ_x in the X basis, including phase noise and distinguishability. If no photons arrive at Charlie, half the coincidence clicks are correct and half are wrong, both occurring with probability $(1-P_s)^2N(N-1)P_{\mathrm{dc}}^2(1-P_{\mathrm{dc}})^{2N-2}$. With a single photon clicking, the probability to have a correct or a wrong coincidence click is $2P_s(1-P_s)(N-1)P_{\mathrm{dc}}(1-P_{\mathrm{dc}})^{2N-2}$. When both photons click at Charlie's detectors, the probabilities for the outcome to be correct or wrong are $P_s^2(1-P_{\mathrm{dc}})^{2N-2}[P_{\mathrm{good}}^{(X)} + (N-1)P_{\mathrm{dc}}P_{\mathrm{double}}^{(X)}]$ and $P_s^2(1-P_{\mathrm{dc}})^{2N-2}[P_{\mathrm{bad}}^{(X)} + (N-1)P_{\mathrm{dc}}P_{\mathrm{double}}^{(X)}]$, respectively. Here, $P_{\mathrm{double}}^{(X)} = (1+|\beta|^2)/N$ is the probability that both photons end up in the same detector. $P_{\mathrm{bad}}^{(X)} = [N(N-1) - 2|\beta|^2 f_N]/(2N^2)$ and $P_{\mathrm{good}}^{(X)} = [N(N-1) + 2|\beta|^2 f_N]/(2N^2)$ are the probabilities to have or not have the photonic interference spoiled by phase noise and distinguishability. The function f_N depends on the considered phase noise model. For the space encoding, we find $f_N = N(N-1)e^{-\sigma^2}/2$. For the time encoding, we find $f_N = [N(1-e^{-\sigma^2}) + e^{-N\sigma^2} - 1]/[2\sinh(\sigma^2/2)]^2$. With these results, it is possible

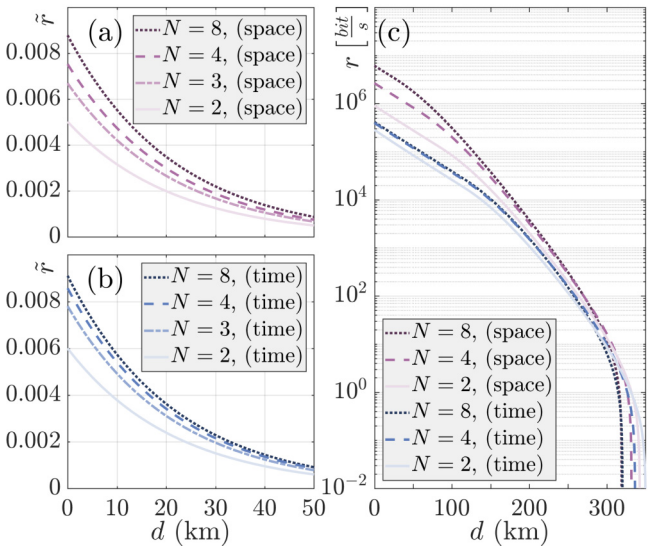

FIG. 2. Secure key rate as a function of distance. Plain lines refer to $N = 2$, dash-dotted lines to $N = 3$, dashed lines to $N = 4$, and dotted lines to $N = 8$. (a,b) No detector dead time, $\tau_d = 0$. The secret key rate without detector dead time $\tilde{r}$ is found using Eq. (2), with R substituted by R_p, i.e., $\tilde{r}$ is in *bit* per application of the protocol. (c) Secret key rate per second r as a function of distance. The dead time is $\tau_d = 20$ ns, and the minimum pulse separation is $\tilde{T}_p = 200$ ps ($\tau_d/\tilde{T}_p = 100$). Common parameters are $P_{\rm dc} = 1 \times 10^{-6}$, $f(\epsilon_z) = 1$, $|\beta|^2 = 0.85$, $\eta = 0.145$, and σ equal to 0.175 (time) or 0.325 (space). σ is chosen such that, for $N = 2$ when only including dephasing, there is a QBER ϵ_x of 1.5% (time) or 5% (space).

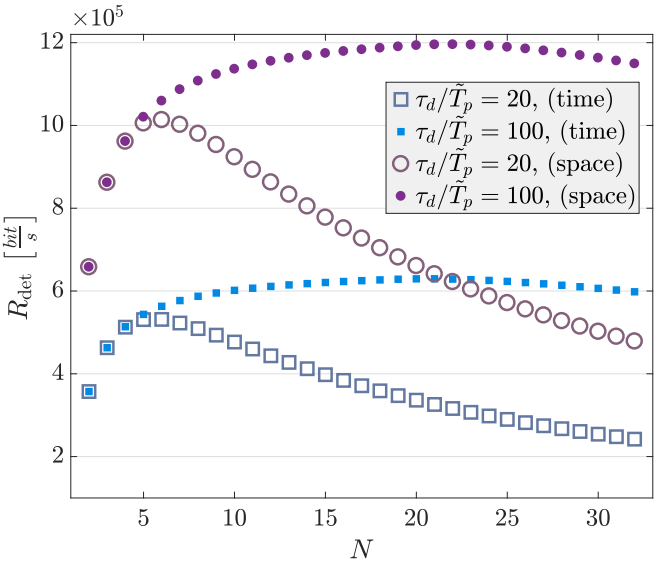

FIG. 3. Raw key per detector $R_{\rm det} = R/n_{\rm det}$ as a function of the dimension N, in the detector saturation regime. Violet circles (solid and empty) are used for the space encoding. Blue squares (solid and empty) are used for the time encoding. The number of pulses n within τ_d is optimized to achieve the highest rate. The maximum possible number of qubits $\tau_d/\tilde{T}_p$ is equal to either 20 (empty circles and squares) or 100 (solid circles and squares). $P_s = 0.2$, $\tau_d = 20$ ns, and $n_{\rm det} = 2N$ (space) or $n_{\rm det} = 2$ (time).

to find how many bits of key are wrong on average and thus to find the QBER ϵ_x in the X basis.

By merging the results above for sources, channel, and detection imperfection, we derive Figs. 2(a) and 2(b), where the secret key rate per application of the protocol is determined using Eq. (2), with R substituted by the raw key rate per application of the protocol R_p. From the plot we find the advantage of Hi-D mdi-QKD, as compared to standard mdi-QKD. The probability that Alice and Bob send the same state $|i\rangle$ (resulting in a useless event) asymptotically goes to zero. This implies that, for small $P_{\rm dc}$, the performance is improved by a factor of $2(N-1)/N$ compared to the standard mdi-QKD protocol, where half of the events are lost even if Alice and Bob select the same basis.

In the following, we study the regime where the detector's dead time τ_d is comparable to the timescale at which photons click at Charlie's detectors, and dark counts are negligible. We assume that during τ_d Alice and Bob send n pulses separated by $T_p = \tau_d/n$. In this regime, ordinary QKD has proven to gain advantage from high-dimensional encoding [23,38]. In the following, we extend this result to mdi-QKD, considering space and time encodings separately.

Space. For any dimension N of the Hilbert space, $2N$ detectors are used (see Fig. 1). The probability per pulse $P_{\rm hit}$ that a detector is hit by a photon is $P_{\rm hit} = \frac{1}{2N}[2P_s(1-P_s) + P_s^2(2N-1)/N]$. In the continuous limit ($t \gg T_p$), the cumulative distribution for a detector being hit within a time t is $1 - e^{-P_{\rm hit}t/T_p}$. From this, the probability $P_{\rm alive}$ that a detector is not dark can be found to be $P_{\rm alive} = P_{\rm hit}^{-1}/(P_{\rm hit}^{-1} + n)$, where we assume that a detector remains dark for a time τ_d, no matter how many photons arrive while it is dark. The average number of raw bits $N_{\rm raw}$ exchanged during a dead time τ_d is therefore

$$N_{\rm raw} = \frac{\tau_d}{T_p}\frac{(N-1)P_s^2 P_{\rm alive}^2}{N}. \tag{3}$$

Maximizing $N_{\rm raw}$ with respect to T_p, we find the maximum of $N_{\rm raw}$ (assuming $P_s \ll N$):

$$\frac{N_{\rm raw}^{(M)}}{\tau_d} = \max_{T_p}\left\{\frac{N_{\rm raw}(T_p, P_s, N)}{\tau_d}\right\} = \frac{P_s(N-1)}{4\tau_d}. \tag{4}$$

Time. In the time encoding, two detectors are used [see Fig. 1(b)], and the minimum time separation between two consecutive qudits is NT_p. Following the same procedure outlined above, we find $N_{\rm raw}$, which is the same as in Eq. (3), but divided by a factor of 2. This follows from the fact that, during a train of N pulses, the same detector cannot click twice, leading to a better performance of the space protocol for short distances (see Fig. 3). The maximum number of bits exchanged during the detector's dead time τ_d is thus ($P_s \ll N$)

$$\frac{N_{\rm raw}^{(M)}}{\tau_d} = \frac{P_s(N-1)}{8\tau_d N}. \tag{5}$$

Including the results found for the saturation regime, and limiting the interval T_p between consecutive pulses to some minimal value $\tilde{T}_p$, the raw key rate R can finally be

determined to be

$$R = \frac{N_{\text{raw}}^{(M)}}{\tau_d} R_p, \tag{6}$$

where the raw key rate per application of the protocol R_p assumes no detector dead time, $\tau_d = 0$. Here, $N_{\text{raw}}^{(M)}$ is either Eq. (4) (space encoding) or Eq. (5) (time encoding) when the optimal T_p is bigger than $\tilde{T}_p$. Otherwise, $N_{\text{raw}}^{(M)}$ is given by Eq. (3) with the substitution $T_p \to \tilde{T}_p$. Since the number of pulses is varied to reach the optimal performance, we evaluate the raw key rate in units of the detector dead time τ_d. Therefore, while R_p is in units of bits/pulse, R is in units of bits/s.

Since detectors are usually the limiting resource, we renormalize the raw key rate R in Eq. (6) with respect to the number of detectors n_{det} employed. This renormalization takes into account that $2N$ detectors could be used to perform N parallel applications of a two-dimensional protocol, possibly outperforming the Hi-D setup. The rates per resource are shown in Fig. 3, with the plain dots referring to $\tilde{T}_p = \tau_d/100$and the empty ones to $\tilde{T}_p = \tau_d/20$. Figure 3 shows that, with a limited rate of pulse generation (and thus finite $\tilde{T}_p$), there exists an optimal dimension N_{opt} for the best key rate: $N_{\text{opt}} = 2 + P_s\tau_d/\tilde{T}_p$ (for $P_s \ll N$). For $P_s\tau_d/T_p \gtrsim 1$, we see that with Hi-D mdi-QKD we increase the key rate *per detector*, due to the factor of $2(N-1)/N$ found above.

Our work allows, for given experimental conditions, one to evaluate *a priori* which is the best setting to be employed in order to achieve the highest secret key rate. As an example, Fig. 2(c) shows the secret key rate r as a function of distance. For these curves, we used Eqs. (6) and (2) to determine the raw (R) and the secret (r) key rates, respectively. With the chosen parameters, for short distances it is better to use Hi-D mdi-QKD in the space encoding, while for very long distances low-dimensional time encoding is preferable. Three regimes are visible in the plot. In the central region the rate scales as P_s^2, as two clicks are required. In the detector saturation regime, the probability for the detectors not to be dark is P_s^{-1}, meaning that the rate is linear in P_s. Finally, for large distances dark counts prevail, making QKD impossible. Note that for an accurate cost analysis the number of detectors employed must also be considered, as in Fig. 3.

IV. CONCLUSION

In conclusion, we have generalized the standard mdi-QKD protocol to higher dimensions N. In our analysis we consider the main sources of errors, and we prove the advantages of Hi-D mdi-QKD, particularly in the detector saturation regime. This result improves previous mdi-QKD schemes, allowing for higher communication rates. The considered generalization to Hi-D mdi-QKD is only one out of many possibilities (for instance, see Ref. [39]). An attractive feature of our proposal is that it can directly be implemented with existing technology. The protocol works by projecting the state onto a two-dimensional Hilbert space, through the Bell state measurement performed by Charlie. Genuine Hi-D Bell-state analyzers would allow higher key rates, by increasing the PIE and reducing the information acquired by Eve. However, discriminating Bell states with linear optics is challenging, leaving the Hi-D ones inaccessible [25]. The proposals in Refs. [40–42] for Hi-D Bell-state analysis may allow for genuine exploitation of high-dimensional Bell states, but they remain experimentally challenging. The present approach is thus the most attractive from a practical perspective.

ACKNOWLEDGMENTS

We thank D. Pastorello and S. Paesani for fruitful discussions. This work was supported by the Danish National Research Foundation through the Centers of Excellence Hy-Q (Grant No. DNRF139) and SPOC (Silicon Photonics for Optical Communications, Grant No. DNRF123), by the European Union Seventh Framework Programme under ERC Grant QIOS, by the People Programme (Marie Curie Actions) under REA Grant No. 609405 (COFUNDPostdocDTU), and by the Danish Council for Independent Research (DFF).

[1] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Phys. Rev. Lett. **98**, 230501 (2007).
[2] C.-H. F. Fung, B. Qi, K. Tamaki, and H.-K. Lo, Phys. Rev. A **75**, 032314 (2007).
[3] B. Qi, C.-H. F. Fung, H.-K. Lo, and X. Ma, Quantum Info. Comput. **7**, 73 (2007).
[4] Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo, Phys. Rev. A **78**, 042333 (2008).
[5] F. Xu, B. Qi, and H.-K. Lo, New J. Phys. **12**, 113026 (2010).
[6] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Nat. Photonics **4**, 686 (2010).
[7] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Opt. Express **18**, 27938 (2010).
[8] L. Lydersen, M. K. Akhlaghi, A. H. Majedi, J. Skaar, and V. Makarov, New J. Phys. **13**, 113042 (2011).
[9] L. Lydersen, J. Skaar, and V. Makarov, J. Mod. Opt. **58**, 680 (2011).
[10] C. Wiechers, L. Lydersen, C. Wittmann, D. Elser, J. Skaar, C. Marquardt, V. Makarov, and G. Leuchs, New J. Phys. **13**, 013043 (2011).
[11] S. Sajeed, I. Radchenko, S. Kaiser, J.-P. Bourgoin, A. Pappa, L. Monat, M. Legré, and V. Makarov, Phys. Rev. A **91**, 032326 (2015).
[12] D. Mayers and A. Yao, in *Proceedings of the 39th Annual Symposium on Foundations of Computer Science, 1998* (IEEE, New York, 1998), pp. 503–509.
[13] M. McKague, arXiv:1006.2352.
[14] S. L. Braunstein and S. Pirandola, Phys. Rev. Lett. **108**, 130502 (2012).
[15] H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. **108**, 130503 (2012).
[16] M. Bass, C. DeCusatis, and J. Enoch, *Handbook of Optics*, Vol. 2 (McGraw-Hill, New York, 2001).
[17] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, Nature **557**, 400 (2018).

[18] H. Chau, C. Wong, Q. Wang, and T. Huang, arXiv:1608.08329.
[19] D. Bacco, J. B. Christensen, M. A. U. Castaneda, Y. Ding, S. Forchhammer, K. Rottwitt, and L. K. Oxenløwe, Sci. Rep. **6**, 36756 (2016).
[20] Y. Ding, D. Bacco, K. Dalgaard, X. Cai, X. Zhou, K. Rottwitt, and L. K. Oxenløwe, npj Quantum Inf. **3**, 25 (2017).
[21] Y. Liu, T.-Y. Chen, L.-J. Wang, H. Liang, G.-L. Shentu, J. Wang, K. Cui, H.-L. Yin, N.-L. Liu, L. Li, X. Ma, J. S. Pelc, M. M. Fejer, C.-Z. Peng, Q. Zhang, and J.-W. Pan, Phys. Rev. Lett. **111**, 130502 (2013).
[22] N. T. Islam, C. C. W. Lim, C. Cahall, J. Kim, and D. J. Gauthier, Sci. Adv. **3**, e1701491 (2017).
[23] Z. Zhang, J. Mower, D. Englund, F. N. C. Wong, and J. H. Shapiro, Phys. Rev. Lett. **112**, 120506 (2014).
[24] H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005).
[25] J. Calsamiglia, Phys. Rev. A **65**, 030301 (2002).
[26] L. Vaidman and N. Yoran, Phys. Rev. A **59**, 116 (1999).
[27] M. Curty, F. Xu, W. Cui, C. C. W. Lim, K. Tamaki, and H.-K. Lo, Nat. Commun. **5**, 3732 (2014).
[28] H. Inamori, Algorithmica **34**, 340 (2002).
[29] W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003).
[30] X.-B. Wang, Phys. Rev. Lett. **94**, 230503 (2005).
[31] D. Gottesman, H.-K. Lo, N. Lutkenhaus, and J. Preskill, in *Proceedings of the International Symposium on Information Theory, 2004* (IEEE, New York, 2004), p. 136.
[32] H.-K. Lo and H. F. Chau, Science **283**, 2050 (1999).
[33] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
[34] H.-K. Lo, H. F. Chau, and M. Ardehali, J. Cryptol. **18**, 133 (2005).
[35] M. Koashi, New J. Phys. **11**, 045018 (2009).
[36] The extension to the asymmetric case in which detectors and/or channels are different can be done by keeping track of the different contributions from all possible two-dimensional mdi-QKD protocols. Equation (2) is then generalized by summing over all contributions to the raw key rate and the QBER.
[37] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).
[38] T. Zhong, H. Zhou, R. D. Horansky, C. Lee, V. B. Verma, A. E. Lita, A. Restelli, J. C. Bienfang, R. P. Mirin, T. Gerrits *et al.*, New J. Phys. **17**, 022002 (2015).
[39] Y. Jo and W. Son, Phys. Rev. A **94**, 052316 (2016).
[40] J. A. Smith and L. Kaplan, arXiv:1802.10527.
[41] S. K. Goyal, P. E. Boukama-Dzoussi, S. Ghosh, F. S. Roux, and T. Konrad, Sci. Rep. **4**, 4543 (2014).
[42] M. Dušek, Opt. Commun. **199**, 161 (2001).