


Reducing the number of single-photon detectors in quantum-key-distribution networks by time multiplexing

Jakob Kaltwasser , Joschka Seip , Erik Fitzke , Maximilian Tippmann , and Thomas Walther ^{*}
Institute for Applied Physics, Technische Universität Darmstadt, Schlossgartenstraße 7, 64289 Darmstadt, Germany

 (Received 25 May 2023; accepted 4 January 2024; published 24 January 2024)

We demonstrate a method to reduce the number of single-photon detectors (SPDs) required in multiparty quantum key distribution (QKD) networks by a factor of 2 by using detector time multiplexing (DTM). We implement the DTM scheme for an entanglement-based time-bin protocol and compare QKD results with and without DTM in our QKD network with four users. When small efficiency losses are acceptable, DTM enables cost-effective, scalable implementations of multiuser QKD networks.

DOI: [10.1103/PhysRevA.109.012618](https://doi.org/10.1103/PhysRevA.109.012618)

I. INTRODUCTION

Fundamental and technical advances in combination with existing quantum algorithms such as Shor's algorithm [1], will enable quantum computers to break the current asymmetric encryption schemes [2–4]. One promising way to restore security is to use quantum key distribution (QKD) in conjunction with symmetric encryption methods [5–7].

In recent years, various QKD protocols, methods, and networks have been demonstrated [8–16]. One main experimental challenge of practical QKD setups is to provide a high quantum key rate sufficient to encrypt the high data rates achieved in today's digital communication. Despite progress in the realization of long distance fiber-based [12,13,17–20] and satellite-based two-party QKD [9,10], the distance between the parties still remains a major challenge due to the transmission losses as long as quantum repeaters are not accessible in a scalable manner [21]. Of course, large distances in QKD can be achieved when resorting to networks with trusted nodes [9].

Another major challenge in the further development of practical QKD systems is the scalability regarding the number of users, i.e., to ensure that a high number of communication parties can be connected. Only with well-developed QKD networks providing keys for many users, the technology will become relevant for a wide range of applications. Each pair of parties exchanging a key should not have to trust the other parties connected to the network. This can be achieved by implementing entanglement-based protocols in combination with wavelength-division multiplexing (WDM) as used in various QKD networks [14,22–24]. To address both, the scalability in the number of users and the compatibility with existing telecom infrastructure, our group has recently demonstrated a robust, entanglement-based, multiuser QKD network operating around 1550 nm [25].

In the present paper, we provide a method to further improve the scalability of this network by halving the required

number of single-photon detectors (SPDs). The SPDs are the major cost driver for such networks and reducing their number greatly reduces the cost for implementation. Therefore, our approach is based on detector time multiplexing (DTM) and allows to reduce the necessary number of SPDs per receiver unit from two to one.

In the following, we will introduce the concept of DTM and demonstrate its implementation in our QKD network together with WDM (cf. Fig. 1). Furthermore, we thoroughly evaluate the performance of DTM compared to the regular QKD setup and find only a small reduction in the quantum key rates. Moreover, we identify the causes for these losses and show that they are, in principle, remediable to a significant extent.

II. SETUP AND CONCEPT

The principle architecture of our setup is a star-shaped QKD network in which a high number of user pairs can be connected to a central photon source, allowing multiple pairs of users to simultaneously and independently exchange secret quantum keys. The source generates entangled photon pairs with a broad type-0 spontaneous parametric down-conversion (SPDC) spectrum [22,26], which is split by WDM into various frequency channels, specified to a width of 50 GHz. Each user receives the photons from one such channel. The basic concept of this network has already been successfully demonstrated to work in a telecom environment by our group [25]. All connected parties can exchange keys pairwise with each other, independently of all other parties. Since the photon pairs generated from SPDC are entangled in frequency due to energy conservation, the frequencies symmetric to the left and the right of the central frequency ω_0 of the SPDC spectrum are entangled, as depicted in Fig. 1. Hence, by assigning quantum channels symmetrically positioned around the central frequency ω_0 to a pair of users, these users obtain entangled photons from which they derive their quantum key. Any user pairing is possible by assigning those channels of the photon-pair spectrum to the party pairs willing to exchange secret keys.

^{*}thomas.walther@physik.tu-darmstadt.de

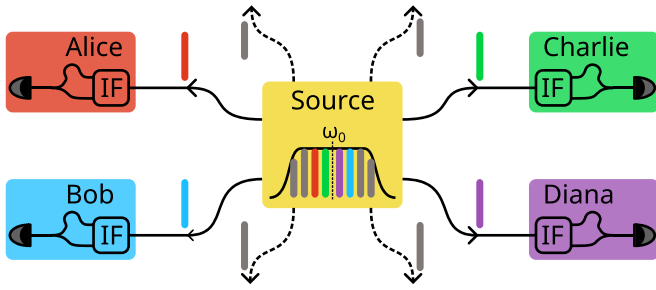


FIG. 1. Operating principle of an entanglement-based star-shaped QKD network combining WDM with DTM. Multiple users are connected to the central photon pair source, where the entangled photons cover a broad spectrum and are demultiplexed into several frequency channels. Two users connected via channels with symmetric spacing around the central frequency ω_0 receive entangled photon pairs due to energy conservation in the SPDC process. The receiver units are equipped with identical imbalanced interferometers (IFs). Due to DTM, each receiver unit only needs one SPD.

The employed BBM92 protocol [27–29] uses the distribution of photon pairs entangled in time and phase. This protocol is very well suited to implement scalable wavelength-multiplexed multiparty networks [25]. A major advantage over polarization-entangled protocols is its independence from polarization greatly enhancing the robustness of the transmission. Furthermore, unlike pure phase-coding protocols [5], we do not need active phase modulators.

The concept of phase-time coding for two parties is shown in detail in Fig. 2. As indicated, it can be easily adapted for more parties. We implemented it for four parties. In this case, the photon-pair spectrum is split up into four channels.

To implement the protocol, we use a photon-pair source containing a laser-generating 300 ps long pulses at 1550 nm with a repetition frequency of 109.89 MHz. These pulses then pass through an imbalanced interferometer, transforming

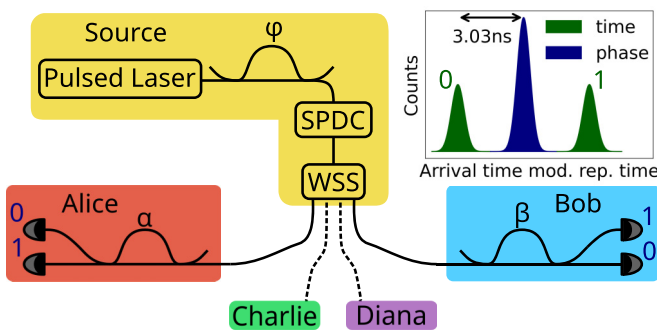


FIG. 2. Schematic setup of our multiparty QKD with phase-time coding without DTM. The source (yellow box) and the exemplary receivers Alice, Bob, Charlie and Diana got identical imbalanced interferometers (only shown here for Alice and Bob), with a specified phase $\varphi, \alpha, \beta, \gamma, \delta$. We use a 3.03 ns delay in these interferometers. This delay generates a histogram of the photon arrival times, sketched at the top right used to gain key bits in the time basis, marked green. The phases of the interferometers are used to gain key bits in the phase basis due to the entanglement of the photons. The phase basis is marked blue and the corresponding bits are tagged at the detectors.

them into well-separated double pulses, with a specific phase relation. These pulses are then frequency-doubled in a second harmonic generation stage. Finally, we use SPDC [22,26] to generate the photon pairs in a fiber-coupled periodically poled lithium niobate (PPLN) crystal. The photons are demultiplexed into the respective frequency channels and sent to a pair of parties who want to exchange a secret key. For WDM, we use a wavelength-selective switch (WSS) allowing to arbitrarily swap the communication pairs which results in larger flexibility compared to WDM on the DWDM grid with fixed filters. However, with a fixed party-setting in the WSS, it is completely analogous to using the DWDM grid with an arrayed waveguide grating (AWG) or similar filters. In the users’ receiver stations the photons each pass through another interferometer with an identical delay as in the source interferometer. Finally, the photons are detected in single-photon detectors (*ID Quantique* ID220) connected to the two interferometer outputs. All components in the receiver setups operate in a range of $1550 \text{ nm} \pm 30 \text{ nm}$ and are therefore not sensitive to the assignment of different wavelengths to each user.

In the time basis, three arrival times are possible per repetition cycle determined by the paths in the interferometers of the source and at the receiver: early arrival (short path in both interferometers), late arrival (long path in both interferometers), and arrival during the central time bin as a mixture of short and long paths, respectively. A qualitative arrival-time histogram is shown in Fig. 2. The key bits in the phase basis are given by the correlation between the two interferometer outputs A_i at Alice’s interferometer and B_j at Bob’s interferometer, with $i, j \in \{0, 1\}$. Their detection probability in the central time bin depends on the sum of the phases of the source- and receiver interferometers [8]

$$P_{A_i, B_j}(\alpha, \beta, \varphi) = \frac{1}{4}[1 + (-1)^{i+j} \cos(\alpha + \beta - \varphi)]. \quad (1)$$

In the standard configuration, each receiver unit requires two SPDs. However, by employing DTM the necessary number of SPDs is cut in half.

Detector time multiplexing

Detector time multiplexing (DTM) has been recently used in setups to build photon-number-resolved detectors [30–32] and measuring higher-order photon correlations [33]. In these applications, the splitting of a pulse into several distinguishable time bins is used to obtain information about the photon number of the pulse via the detection probability per bin.

We use DTM to reduce the number of detectors per receiver module. Due to the relatively short (300 ps long) laser pulses (full width at half maximum, FWHM), the width of the peaks in the histogram is much less than the time delay in the interferometers of 3.03 ns. Therefore, there are unused time intervals in between the peaks, even when the pulses broaden in time due to chromatic dispersion in the transmission links. Since the free time intervals themselves are longer than a peak width, further time bins can fit into the free intervals without interfering with the primary time bins. This can be used, for example, to increase the key rates by doubling the repetition rate of the photon source from 109.89 MHz to 219.78 MHz [25]. Alternatively, it can be used to realize DTM

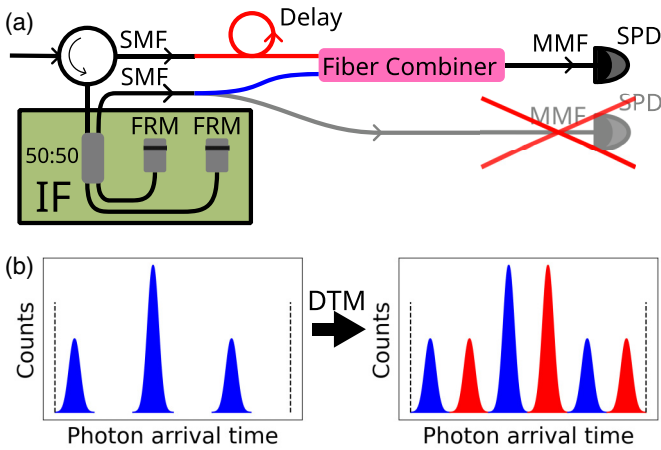


FIG. 3. (a) Scheme of a QKD receiver for phase-time coding. SMF: single-mode fibers with $8.2\ \mu\text{m}$ core diameter, MMF: multi-mode fibers with $62.5\ \mu\text{m}$ core diameter. The temperature-stabilized interferometer (IF) consists of a 50:50 beam splitter and two Faraday mirrors (FRM). In the usual setup, each IF output is connected to a separate SPD. For DTM, the receiver setup is modified: the interferometer outputs are combined by a $2 \times \text{SMF} \rightarrow \text{MMF}$ fiber combiner. (b) Resulting photon arrival histograms. Both interferometer outputs show the left histogram in the time domain. Due to the fiber section introducing a specific delay, one of the outputs (histogram in red) is shifted in time, so that it fits into the free time intervals between the peaks of the other output (blue histogram) when combined with the other output by the fiber combiner.

by combining both interferometer outputs into one fiber. In Fig. 3(b) the peak structure of a single interferometer output is shown on the left and the final peak structure with DTM on the right. With DTM, it becomes a six-peak structure, where one three-peak interferometer output is nested into the other. The shift between the peak structures is achieved by introducing a fiber with a specific length producing a delay in one of the outputs before the interferometer outputs are combined.

One way to combine the outputs is to use a 50:50 tap coupler. However, this gives rise to additional losses of half of the photons, thus significantly decreasing the key rate. A polarization combiner is not possible for our setup since the interferometer outputs are not in fixed orthogonal polarization states. Alternatively, a fiber combiner can be used to combine two single-mode inputs into one multimode output; due to energy conservation only a multimode output is possible. We use this principle to join the two single-mode interferometer outputs in our receivers into one multimode fiber (MMF), which is then connected to an SPD. Figure 3(a) displays the current setup of the receiver units and the necessary changes to implement DTM. The combiners we use are commercially available off-the-shelf components introducing additional insertion losses of about 5%.

With these physical changes implemented, it is possible to distinguish between the two interferometer outputs by the different arrival times of the photons of each output. The time bins can be assigned to two virtual detectors, which from then on are used in the data evaluation as the two detectors in the regular setup without DTM. Additionally, the DTM requires a change of the data acquisition and evaluation software

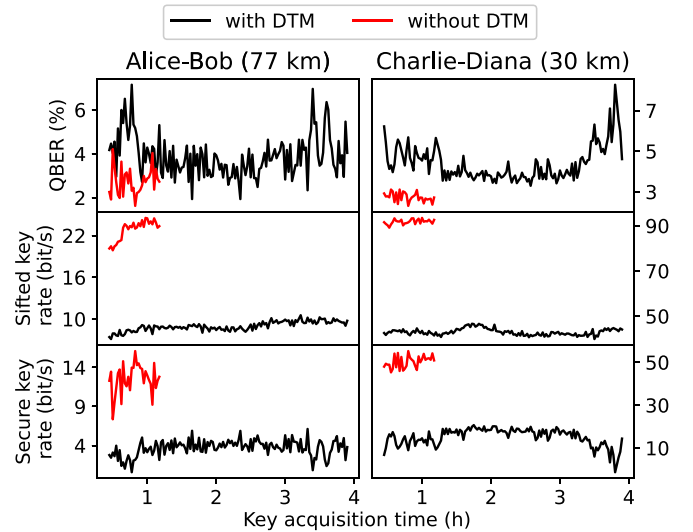


FIG. 4. QKD results with and without DTM for our four-party QKD setup. The data with DTM were acquired over an extended time period to demonstrate the long-term stability. The key rates show a systematic difference between the measurements with DTM and without DTM. Also note the different y scale for Alice-Bob and Charlie-Diana due to the different losses introduced by the different fiber lengths.

because it has to be able to distinguish the joint interferometer outputs. The virtual detectors can be assigned to the correct interferometer outputs using a cross-correlation evaluation of the first few exchanged key bits, which are discarded afterwards. With the cross correlation the absolute temporal offset between the virtual detectors can be identified. Together with the knowledge of which interferometer output has the longer propagation time to the combiner, the outputs can always be correctly assigned.

III. RESULTS

To evaluate the performance of the QKD setup with DTM, a key exchange lasting over four hours was performed. Keys were exchanged simultaneously between Alice and Bob with transmission distances from the source of 26.9 km and 50.4 km as well as between Charlie and Diana with transmission distances of 9.6 km and 20.4 km, respectively. The 26.9 km link to Alice is a deployed dark fiber link provided by *Deutsche Telekom* (cf. Ref. [25]). All other fibers are spooled fibers in the laboratory whose lengths were selected based on availability.

The resulting quantum bit error rate (QBER) and sifted key rate are displayed in Fig. 4; average values are tabulated in Table I. The secure key rate I_{sec} was estimated from the sifted key rate and the QBER was estimated as described in Ref. [25] using a formula from Refs. [34,35]. This approximation is sufficient for us even if it does not include several effects, such as for example finite key size effects. We only need a measure to compare the results with DTM to the results without DTM.

The secure key rate with DTM is about 70% lower than without DTM. This is due to two effects: the major reduction

TABLE I. Overview over the average key rates and quantum bit error rates (QBERs) from Fig. 4 with the user pairs Alice-Bob and Charlie-Diana with and without DTM.

DTM	User combination	Sifted key rate (bit/s)	QBER (%)	Secure key rate (bit/s)
yes	Alice-Bob	8.1	3.89	3.6
	Charlie-Diana	43.0	4.37	15.3
no	Alice-Bob	22.8	2.74	12.5
	Charlie-Diana	91.8	2.73	50.2

in the sifted key rate and the additional slightly increased QBER.

However, neither the lower sifted key rate nor the higher QBER could be attributed to the principle of DTM, at least not to this extent. The reason for the heavy drop in the sifted key rate and the large increase of the QBER was found in the dependence of our single-photon detectors' efficiencies on spatial modes in the MMF. The fiber combiner used in the DTM setup excites higher spatial modes in this fiber, to which our detectors are much less sensitive even though specified as multi-mode detectors.

This effect was verified with two MMFs spliced together with a small spatial misalignment of the cores to excite higher spatial modes. A simple power measurement was used to verify that the insertion loss introduced by the splice is negligible. This fiber is inserted into a setup where attenuated laser pulses were detected with the SPD. With the spliced MMF the count rates were around 24% lower compared to measurements with a regular MMF without such an offset splice due to the relatively large spatial mode dependency of the detection efficiency.

After identifying this effect, a control experiment with QKD between two parties was performed with two IDQube detectors from *ID Quantique* employing the same settings for detection efficiency and dead time as for the ID220 detectors. Figure 5 shows the results indicating that the effect does not occur with these detectors. The sifted key rates with DTM using IDQubes is more than twice as high as with the ID220s although both detector types have approximately the same detection efficiency and dead time. This observation corroborates our assumption that the ID220s' lower detection efficiency for higher spatial modes significantly reduces the key rates in our DTM setup.

Nevertheless, using DTM still decreases the key rate by around 23.6% even when IDQubes are used. Two reasons were identified: On the one hand DTM required additional fiber connections in our experimental setup introducing additional losses of around 5%, and the fiber combiner itself also leads to insertion losses of around 5% per receiver. This alone reduces the sifted key rate by around 10% due to losses. On the other hand DTM also leads to higher saturation of the detectors since now both interferometer outputs are detected at only one SPD. The effect of the saturation can be estimated using [36]

$$\frac{R_m}{R_e} \approx 1 - \tau R_m, \quad (2)$$

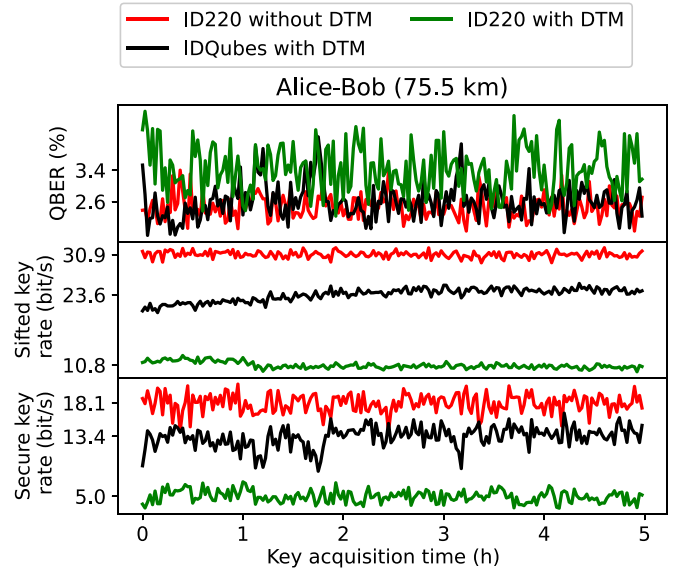


FIG. 5. QKD results for a two-party QKD setup with and without DTM. In the case of DTM, IDQubes are used additionally, since the ID220s were not able to detect different spatial modes equally efficient.

with the measured count rate R_m , the expected count rate R_e and the detector dead time τ , which is $10 \mu\text{s}$ in our setup.

Using ID220s without DTM, the detected count rates for Alice are around 19 500/s and 13 500/s at the two interferometer outputs. Bob receives count rates of around 9500/s and 6600/s. Using IDQubes with DTM, the detected count rate for Alice is around 22 000/s. Bob receives a count rate of around 12 500/s. This results in an additional decrease of the sifted key rate of around 11% due to saturation according to Eq. (2).

The insertion loss of the additional components and the additional fiber connections amount to an efficiency loss of 10%. In combination, both effects give a decrease of efficiency of 20%, which essentially describes the measured difference of 23.6% between QKD with and without DTM. The remaining difference of 3.6% may be accounted to measurement uncertainties and additional fiber connections in the DTM setup and to the fact that Eq. (2) is only an approximation. Thus, DTM operates as expected.

The QBER when using ID220 without DTM is similar to the QBER using IDQubes with DTM. However, the newer IDQubes also have lower dark count rates slightly reducing the QBER. Since we do not have access to four IDQubes, a check without DTM using IDQubes could not be performed and the exact effect of DTM on the QBER could not be determined. A possible cause for a slight increase of the QBER could be the potential crosstalk between time bins due to the reduced gap between adjacent time bins. Additionally, with DTM crosstalk in the phase basis is also possible because the time bins of the central peaks of both interferometer outputs lie directly next to each other in our case. It might be possible to reduce this effect by choosing a different time offset between the interferometer outputs so that the central peaks of the two outputs are further apart from each other, with a time-basis bin in between them. In Fig. 3(b) this would be the

case, when shifting the red histogram, so that the left small peak of it is right to the blue big peak. This should reduce at least the crosstalk in the phase basis.

IV. DISCUSSION AND OUTLOOK

Our experiments demonstrate the functionality of DTM, showing a good stability even for long key-exchange measurements over four to five hours.

However, we observe a major decrease of sifted key rate in our first attempts. We attribute this effect to the sensitivity of the detection efficiencies of our SPD used on spatial modes. A control measurement with a SPD, which detects all spatial modes equally efficient, has shown that, in principle, QKD with DTM works as expected and without unexpected losses in efficiency. Consequently, a requirement for the DTM are SPDs which can efficiently detect different and in particular higher spatial modes.

Only a small increase in QBER in case of DTM is not fully explained yet and needs further investigation. For that a comparative measurement with and without DTM should be performed with the IDQube detectors.

A major effect reducing the sifted key rate is the saturation of the detectors, limiting the possible count rates for shorter distances between the parties. In this case, the photon rates arriving at the receiver units are higher. Naturally, since both interferometer outputs are fed into a single detector, DTM is not suitable for high count rates since saturation becomes the dominant effect. The saturation effect could be reduced by using other detector types with lower dead time, such that the ratio of the measured to the actual rate in Eq. (2) approaches unity and the sifted-key rate further approximates the case without DTM. An exemplary alternative for other detectors would be commercially available superconducting-nanowire single-photon detectors (SNSPDs). These not only have a higher detection efficiency but also much lower dead times (e.g., IDQ ID281) [37].

For large transmission distances chromatic dispersion could be a limiting factor for DTM as it broadens the pulses in time, possibly leading to an overlap of time bins when interlacing them for DTM, as shown in Fig. 3(b). Our current interferometer delay of 3.03 ns is specifically chosen to match the requirement to get well distinguishable peaks according to our detector jitter and transmission distances including the possibility of higher repetition rates [25] or a DTM scheme, respectively. Using a quick calculation, one can derive the maximum allowed distance L between the photon-pair source and the parties before the DTM scheme stops working due to chromatic dispersion. Clearly, it depends on the pulse durations, dispersion of the fiber, repetition rate, and timing jitter of the detectors.

To estimate the influence of chromatic dispersion on DTM in our setup, all relevant functions are assumed to be Gaussian characterized by their standard deviation. Specifically, these are the pump pulse in the time domain $a(t)$ with width σ_a , the spectral distribution of the photon-pairs $\Phi(\omega)$ with width σ_Φ , as well as the detector jitter $j(t)$ with time width σ_j .

Under the simplified assumption of large dispersion or transmission distances, the resulting optical pulses at the

receivers can be derived as a convolution of the pump pulse and the spectral distribution of the photon-pairs, represented by the WSS channel transmission spectra. Furthermore, the detected pulses with width σ_{det} can be represented as a convolution of the optical pulses with the detector jitter and are thus again Gaussian. Now, assuming that DTM still works when the time bins overlap only up to 1% of their amplitude, this yields a standard deviation of $\sigma_{\text{det}} = 467$ ps for our detected pulses with 3.03 ns interferometer delays. Since the variance of a convolution of two Gaussian pulses results from the sum of the single variances, the maximum possible transmission length between photon-pair source and a receiver can be determined to $L = \frac{1}{\beta_2 \sigma_\Phi} \sqrt{\sigma_{\text{det}}^2 - \sigma_j^2 - \sigma_a^2}$. Using $\sigma_a = 128$ ps (FWHM of 300 ps), $\sigma_j = 106$ ps (FWHM of 250 ps [38]), $\sigma_\Phi = 2\pi \times 16.6$ GHz (according to a rough Gaussian estimation of a 50 GHz WSS-channel) and $\beta_2 = -2.171 \times 10^{-26} \text{ s}^2 \text{ m}^{-1}$ [$D = 17$ ps/(nm km)] as dispersion coefficient for standard single mode fiber, leads to a possible transmission length from source to receiver of about 200 km. Thus, in our setup with distances up to 77 km transmission losses will be the limiting factor with regard to distance, before chromatic dispersion comes into play. In general, even higher transmission distances are possible for WDM channels with smaller spectral widths. The WSS in our setup, for example, can use channels down to 6.25 GHz width. Approaches to further mitigate chromatic dispersion can be employed: Dispersion compensating modules in the transmitting fiber can be used to nearly eliminate the pulse broadening due to chromatic dispersion. Furthermore, interferometers with a higher delay are possible, increasing the separation and distinguishability of the peaks. The higher delays are no detriment for the key rate at shorter distances because one can fill the empty spaces between the time bins by using a multiple of the repetition rate [25].

In terms of the number of detectors required for a larger network, our setup can keep up with measurement device independent (MDI) protocols which only require as many detectors as connected users [15,18,19]. At the same time, we maintain the advantage over MDI protocols in terms of photon source scalability: In our setup, a single central photon source serves all users.

It has to be mentioned that the BBM92 protocol [27] as well as other non MDI protocols, have security issues with regard to loopholes due to side-channel attacks [39,40]. Since our DTM scheme is used with the BBM92 protocol it also suffers from these security issues. DTM as implemented is only a modification of the BBM92 protocol and does not change the protocol itself and thus does not affect the security proof of the protocol [41].

For the BBM92 security proof [41] the detection events must be equally modeled in the DTM scheme, i.e., the events should be decoupled from each other meaning that the dead time of the detector must not mask the next event. Otherwise an attacker could use multiphoton pulses to trigger both phase-basis events, but the second one could not be discovered due to the dead-time and thus the first event will not be discarded as invalid. Decoupling into two independent detection events can be easily achieved by applying a delay line after the interferometer output that has a longer transmission time than

the dead-time of the detector (for our detectors approximately 2 km). To avoid key imbalance due to the additional transmission losses in the delay line, an optical attenuator behind the other interferometer output can be used. We have not yet implemented such a long delay line in our DTM setup due to lack of availability of fibers with this length. Clearly, when using SNSPDs the delay will be short enough to not cause significant extra losses as they have dead times around 60 ns (e.g., IDQ ID281) [37], corresponding to about 12 m fiber length.

However, although the DTM scheme is secure according to the security proof, DTM will alter the security considerations with regard to possible side-channel attacks. It could open new ways to exploit these security loopholes. For example, an eavesdropper Eve could take advantage of the fact that one interferometer output will always lead to higher modes of the multimode output of the fiber combiner which may be polarization dependent leading to security problems [42]. Since the detector can be polarization dependent as well, these possible security issues are not DTM specific, but also possible in other non-MDI protocol implementations. The detectors we use are multimode, so could be vulnerable to such an attack irrespective of using the DTM scheme.

Another manipulation option that seems possible given the way DTM works is the following: Eve introduces delays at random times to shift Bob's time-bin histograms by one time-bin width. Thus, for Bob the "blue" peaks are shifted onto the "red" ones [cf. Fig. 3(b)]. In principle, this would make it possible for Eve to ensure that Alice and Bob use different events for their key after the postselection than with normal phase-time coding. This could potentially allow Eve to obtain information about the key by dictating events. However, it can be shown that such a manipulation by Eve would lead to a significant increase of the QBER. In the above example with a delay of one time-bin width, it can be derived that the time QBER would increase to 25 %, the phase QBER even up to 83.3 %. Even in the worst case, in which Eve also adjusts the phase of the source interferometer to her favor, the phase QBER would still increase to 16.7 %. This manipulation attempt would therefore be recognized due to a QBER higher than 11 % and is therefore not a valid attack [27,43].

On the other hand, the DTM scheme can mitigate some attack methods. For example, blinding one detector with classical light and using its dead time to dictate a key to the other one [40] becomes impossible, as only one detector is being used.

V. CONCLUSION

We presented the concept of DTM as a solution to reduce the number of SPDs needed to one per receiver in a multiparty QKD network. A similar approach was previously used only in a setup with a polarization entanglement protocol, which still required two detectors in the end [14] and needed polarization maintaining transmission links due to the protocol type. The reduction to only one SPD in our approach significantly lowers the cost per receiver module and thereby increases the scalability of such networks in terms of connected parties. This is an important step towards affordable and practical QKD networks, and thus the possibility of widespread use of this technology addressing the growing threats of quantum computing on current encryption techniques.

From a technical point of view, our setup is already highly scalable with regard to simultaneously connected parties due to a broad photon-pair spectrum in conjunction with WDM [25]. WDM in combination with entanglement-based protocols solves the challenge of serving a large number of parties through only a single source, while DTM drastically reduces the implementation cost of the network.

The experimental implementation of DTM was realized by inserting a fiber introducing a specific time delay after one of the interferometer outputs and combining both interferometer outputs with a fiber combiner. The problems arising from spatial dependencies of our single-photon detectors were identified and we showed that the corresponding problems do not occur with detectors that properly detect all spatial modes with the same efficiency.

When considering the usage of SPDs which are able to detect higher spatial modes equally efficiently, there remains only one drawback for the DTM setup: detector saturation plays a major role because omitting one detector leads to an increase of the photon rate for the remaining detector. In our setup, DTM is therefore only useful at larger distances between the parties where the count rates are lower.

ACKNOWLEDGMENTS

This research was funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Grant No. SFB 1119–236615297. We thank P. Wagner from Deutsche Telekom Technik GmbH for lending us the WSS and fiber spools and F. Wissel from Deutsche Telekom Technik GmbH for the provision of a dark fiber test link.

-
- [1] P.W. Shor, Algorithms for quantum computation: Discrete logarithms and factoring, *Proceedings of the 35th Annual Symposium on Foundations of Computer Science* (IEEE, New York, 1994).
 - [2] R. A. Grimes, *Cryptography Apocalypse - Preparing for the Day When Quantum Computing Breaks Today's Crypto* (John Wiley & Sons, New York, 2019).
 - [3] E. Gerjuoy, *Am. J. Phys.* **73**, 521 (2005).
 - [4] D. Cheung, D. Maslov, J. Mathew, and D. K. Pradhan, *Theory of Quantum Computation, Communication* (Springer, New York, 2008), p. 96.
 - [5] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, *Rev. Mod. Phys.* **74**, 145 (2002).
 - [6] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, *Rev. Mod. Phys.* **81**, 1301 (2009).
 - [7] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, *Rev. Mod. Phys.* **92**, 025002 (2020).
 - [8] I. Marcikic, H. de Riedmatten, W. Tittel, H. Zbinden, M. Legré, and N. Gisin, *Phys. Rev. Lett.* **93**, 180502 (2004).
 - [9] Y.-A. Chen *et al.*, *Nature (London)* **589**, 214 (2021).
 - [10] S.-K. Liao, W.-Q. Cai, J. Handsteiner, B. Liu, J. Yin, L. Zhang, D. Rauch, M. Fink, J.-G. Ren, W.-Y. Liu, Y. Li, Q. Shen, Y. Cao,

- F.-Z. Li, J.-F. Wang, Y.-M. Huang, L. Deng, T. Xi, L. Ma, T. Hu *et al.*, *Phys. Rev. Lett.* **120**, 030501 (2018).
- [11] J. Yin *et al.*, *Science* **356**, 1146 (2017).
- [12] A. Boaron, G. Boso, D. Rusca, C. Vulliez, C. Autebert, M. Caloz, M. Perrenoud, G. Gras, F. Bussi eres, M.-J. Li, D. Nolan, A. Martin, and H. Zbinden, *Phys. Rev. Lett.* **121**, 190502 (2018).
- [13] M. Pittaluga, M. Minder, M. Lucamarini, M. Sanzaro, R. I. Woodward, M.-J. Li, Z. Yuan, and A. J. Shields, *Nat. Photon.* **15**, 530 (2021).
- [14] Z. Huang, S. K. Joshi, D. Aktas, C. Lupo, A. O. Quintavalle, N. Venkatachalam, S. Wengerowsky, M. Lon ari c, S. P. Neumann, B. Liu *et al.*, *npj Quantum Inf.* **8**, 25 (2022).
- [15] G.-J. Fan-Yuan, F.-Y. Lu, S. Wang, Z.-Q. Yin, D.-Y. He, Z. Zhou, J. Teng, W. Chen, G.-C. Guo, and Z.-F. Han, *Photonics Res.* **9**, 1881 (2021).
- [16] G.-J. Fan-Yuan, F.-Y. Lu, S. Wang, Z.-Q. Yin, D.-Y. He, W. Chen, Z. Zhou, Z.-H. Wang, J. Teng, G.-C. Guo *et al.*, *Optica* **9**, 812 (2022).
- [17] J.-P. Chen, C. Zhang, Y. Liu, C. Jiang, W.-J. Zhang, Z.-Y. Han, S.-Z. Ma, X.-L. Hu, Y.-H. Li, H. Liu, F. Zhou, H.-F. Jiang, T.-Y. Chen, H. Li, L.-X. You, Z. Wang, X.-B. Wang, Q. Zhang, and J.-W. Pan, *Nat. Photon.* **15**, 570 (2021).
- [18] J.-P. Chen, C. Zhang, Y. Liu, C. Jiang, W. Zhang, X.-L. Hu, J.-Y. Guan, Z.-W. Yu, H. Xu, J. Lin, M.-J. Li, H. Chen, H. Li, L. You, Z. Wang, X.-B. Wang, Q. Zhang, and J.-W. Pan, *Phys. Rev. Lett.* **124**, 070501 (2020).
- [19] S. Wang, Z.-Q. Yin, D.-Y. He, W. Chen, R.-Q. Wang, P. Ye, Y. Zhou, G.-J. Fan-Yuan, F.-X. Wang, Y.-G. Zhu, P. V. Morozov, A. V. Divochiy, Z. Zhou, G.-C. Guo, and Z.-F. Han, *Nat. Photonics* **16**, 154 (2022).
- [20] Y.-L. Tang, H.-L. Yin, Q. Zhao, H. Liu, X.-X. Sun, M.-Q. Huang, W.-J. Zhang, S.-J. Chen, L. Zhang, L.-X. You, Z. Wang, Y. Liu, C.-Y. Lu, X. Jiang, X. Ma, Q. Zhang, T.-Y. Chen, and J.-W. Pan, *Phys. Rev. X* **6**, 011024 (2016).
- [21] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, *Nat. Commun.* **8**, 15043 (2017).
- [22] D. Aktas, B. Fedrici, F. Kaiser, T. Lunghi, L. Labont e, and S. Tanzilli, *Laser Photonics Rev.* **10**, 451 (2016).
- [23] S. Wengerowsky, S. K. Joshi, F. Steinlechner, H. H ubel, and R. Ursin, *Nature (London)* **564**, 225 (2018).
- [24] E. Y. Zhu, C. Corbari, A. Gladyshev, P. G. Kazansky, H.-K. Lo, and L. Qian, *J. Opt. Soc. Am. B* **36**, B1 (2019).
- [25] E. Fitzke, L. Bialowons, T. Dolejsky, M. Tippmann, O. Nikiforov, T. Walther, F. Wissel, and M. Gunkel, *PRX Quantum* **3**, 020341 (2022).
- [26] O. Alibert, V. D'Auria, M. De Micheli, F. Doutre, F. Kaiser, L. Labont e, T. Lunghi,  . Picholle, and S. Tanzilli, *J. Opt.* **18**, 104001 (2016).
- [27] C. H. Bennett, G. Brassard, and N. D. Mermin, *Phys. Rev. Lett.* **68**, 557 (1992).
- [28] J. Brendel, N. Gisin, W. Tittel, and H. Zbinden, *Phys. Rev. Lett.* **82**, 2594 (1999).
- [29] W. Tittel, J. Brendel, H. Zbinden, and N. Gisin, *Phys. Rev. Lett.* **84**, 4737 (2000).
- [30] D. Achilles, C. Silberhorn, C. Sliwa, K. Banaszek, I. A. Walmsley, M. J. Fitch, B. C. Jacobs, T. B. Pittman, and J. D. Franson, *J. Mod. Opt.* **51**, 1499 (2004).
- [31] M. J. Fitch, B. C. Jacobs, T. B. Pittman, and J. D. Franson, *Phys. Rev. A* **68**, 043814 (2003).
- [32] C. M. Natarajan, L. Zhang, H. Coldenstrodt-Ronge, G. Donati, S. N. Dorenbos, V. Zwiller, I. A. Walmsley, and R. H. Hadfield, *Opt. Express* **21**, 893 (2013).
- [33] M. Avenhaus, K. Laiho, M. V. Chekhova, and C. Silberhorn, *Phys. Rev. Lett.* **104**, 063602 (2010).
- [34] P. M. Notz, O. Nikiforov, and T. Walther, *Software bundle for data post-processing in a quantum key distribution experiment*, Technical Report (TU Darmstadt, Darmstadt, 2020).
- [35] D. Elkouss, A. Leverrier, R. Alleaume, and J. J. Boutros, Efficient reconciliation protocol for discrete-variable quantum key distribution, *2009 IEEE International Symposium on Information Theory* (IEEE, New York, 2009).
- [36] A. Patil, Dead time and count loss determination for radiation detection systems in high count rate applications, Ph.D. thesis, Missouri University of Science and Technology, 2010.
- [37] Gregoire Ribordy, ID 281 Superconducting nanowire system-Product brochure, ID Quantique SA (2021).
- [38] E. Fitzke, R. Krebs, T. Haase, M. Mengler, G. Alber, and T. Walther, *New J. Phys.* **24**, 023025 (2022).
- [39] J. Jogenfors, A. M. Elhassan, J. Ahrens, M. Bourennane, and J.- . Larsson, *Sci. Adv.* **1**, e1500793 (2015).
- [40] H. Weier, H. Krauss, M. Rau, M. F urst, S. Nauerth, and H. Weinfurter, *New J. Phys.* **13**, 073024 (2011).
- [41] E. Waks, A. Zeevi, and Y. Yamamoto, *Phys. Rev. A* **65**, 052310 (2002).
- [42] S. Sajeed, P. Chaiwongkhot, J.-P. Bourgoin, T. Jennewein, N. L utkenhaus, and V. Makarov, *Phys. Rev. A* **91**, 062301 (2015).
- [43] P. W. Shor and J. Preskill, *Phys. Rev. Lett.* **85**, 441 (2000).