Bright integrated photon-pair source for practical passive decoy-state quantum key distribution

S. Krapick,[1,*] M. S. Stefszky,[1] M. Jachura,[1,2] B. Brecht,[1] M. Avenhaus,[1,3] and C. Silberhorn[1,3]
[1]*Department of Physics, University of Paderborn, Warburger Str. 100, 33098 Paderborn, Germany*
[2]*Faculty of Physics, University of Warsaw, Hoża 69, 00-681 Warsaw, Poland*
[3]*Max-Planck-Institute for the Science of Light, Günther-Scharowsky-Str. 1, 91058 Erlangen, Germany*
(Received 25 September 2013; published 27 January 2014)

We report on a bright, nondegenerate type-I parametric down-conversion source, which is well suited for passive decoy-state quantum key distribution. We show the photon-number-resolved analysis over a broad range of pump powers and we prove heralded higher-order n-photon states up to $n = 4$. The inferred photon click statistics exhibit excellent agreements to the theoretical predictions. From our measurement results we conclude that our source meets the requirements to avert photon-number-splitting attacks.

DOI: 10.1103/PhysRevA.89.012329 PACS number(s): 03.67.Dd, 42.50.Dv, 42.50.Ex, 42.65.Lm

Quantum key distribution (QKD) has been a field of high interest for almost three decades now, since it allows two trustworthy parties, Alice and Bob, to communicate with unconditional security under certain constraints. However, realistic implementations of QKD schemes suffer from security loopholes [1–7] due to technical imperfections. Among these loopholes, the photon-number-splitting (PNS) attack [8] allows an eavesdropper, Eve, to take advantage of nonideal properties of real-world photon sources. In particular, photon-pair sources based on parametric down-conversion (PDC) emit signals with higher-order photon contributions, which could be intercepted and stored by Eve to gain information about the secret key during the classical phase of a standard prepare-and-measure protocol [9]. When Eve replaces a lossy quantum channel with a perfect one, she could mimic the detected click statistics of the lossy quantum channel and cannot be detected.

In 2007 Mauerer *et al*. proposed the passive decoy-state QKD protocol [10] and theoretically showed the circumvention of photon number splitting attacks, even in the presence of imperfect photon-pair sources based on PDC. It was also proven that the unconditionally secure transmission distance is on par with perfect single-photon sources [10,11]. The scheme is based on the idea of intermittent decoy states [12,13] within the quantum key string in order to detect Eve's presence. But, in contrast to active decoy schemes, the passive decoy approach turns the unavoidable higher photon-number components in a PDC into a real benefit by tagging them as intrinsic decoys. Importantly, this does not require the active modulation or phase randomization of the photon source's emission. The passive decoy scheme offers the distinct advantage that the PDC-based system itself does not open any side channels with distinguishing information for different intensities, because all required decoy states are postselected *after* transmission. However, the implementation of a reliable, bright, compact and efficient PDC source with a well-known photon-number distribution is crucial to achieve the desired performance.

In this paper we present a robust and bright integrated photon-pair source based on titanium-indiffused, periodically poled waveguide structures in lithium niobate (Ti:PPLN). It efficiently generates signal photons at around 803 nm and idler photons around 1573 nm. The former lend themselves to efficient photon-number-resolved detection, whereas the latter allow for low-loss transmission in fiber-based QKD systems. Our source is capable of splitting the generated pairs on chip in a spatiospectral manner [14]. This conveniently allows Alice to keep one half (signal) of the strictly correlated pairs for thorough photon-number analysis, whereas the other half (idler) can be transmitted to her trusted counterpart Bob.

The key feature of our source is that it meets the requirements for practical passive decoy-state QKD. In particular, we measured its click statistics using photon-number-resolving detectors and inferred the photon statistics from the measurement. We registered higher-order PDC photon numbers reliably and demonstrate heralded n-photon states up to $n = 4$, which can be employed as postselectable decoys in order to prevent PNS attacks. In the following, we verify that the detection statistics of our source behaves as expected for the different n-photon states. This will prove its applicability as a basic building block in highly secure QKD systems based on passive decoy-state selection.

First, we write down the probability that Bob's binary detector generates a click from an arbitrary m-photon state:

$$p(\text{click}) = 1 - (1 - \eta_B)^m, \tag{1}$$

with Bob's overall transmission and detection efficiency $\eta_B = \eta_C \eta_{OC} \eta_{Det}$. Herein η_C denotes the length-dependent quantum channel efficiency, η_{OC} is the transmission of supplementary optical components, and η_{Det} labels Bob's detector efficiency. Note that Eq. (1) implies different click probabilities for different m-photon states.

Second, we assume that Alice's photon-number-resolving detector yields n photon detection events from an m-photon state with $m \geqslant n$. Consequently, the conditioned probability for a click at Bob's detector is

$$p(\text{click}|n) = \frac{p(\text{click} \cap n)}{p(n)} = \frac{\sum_{m=n}^{\infty} \binom{m}{n} \rho_m \eta_T^n (1-\eta_T)^{m-n} (1-(1-\eta_B)^m)}{\sum_{m=n}^{\infty} \binom{m}{n} \rho_m \eta_T^n (1-\eta_T)^{m-n}}, \tag{2}$$

*Corresponding author: krapick@mail.uni-paderborn.de

where $p(\text{click} \cap n)$ is the cumulative joint probability of a click event in Bob's detector from an m-photon state, while n out of m photons impinge on Alice's photon-number-resolving detector. The coefficients ρ_m describe the photon-number distribution of the m-photon state, which is Poissonian [15,16] for the spectrally multimode PDC sources like those expected in our case. The term η_T labels the overall efficiency of the photon-number-resolving detector and includes losses as well as the genuine detection efficiency. The efficiency η_T for our case is experimentally accessible as will be described below in Eq. (6).

Especially, in the limit of a low efficiency, $\eta_B \ll 1$, we can calculate the conditioned probabilities $p(\text{click}|n)$ for different n-photon states from Eq. (2), and find that the approximation

$$r(n) = \frac{p(\text{click}|n)}{p(\text{click}|1)} \approx \frac{n\eta_B}{\eta_B} = n, \tag{3}$$

is valid. This means that the fraction of Bob's click probabilities conditioned on different n and the click probability conditioned on the one-photon contribution scales approximately linear with n. At higher efficiencies η_B the values of $r(n)$ will decrease. Thus, at elevated pump power levels the impact of higher-order photon contributions as well as nonideal photon-number-resolving detector properties must be taken into account.

In order to realize photon-number resolution with Alice's detection apparatus, we implemented a time-multiplexing detector [17,18] (TMD) for signal wavelengths of 803 nm. The delay between individual time bins (∼127 ns) is set larger than the dead time of standard silicon avalanche photodiodes used for signal photon detection. The chosen architecture provides eight temporal output modes behind the TMD (photon numbers of $n \leqslant 8$) without losing photons by dead-time effects. Due to this limitation, we additionally take convolution effects [19,20] of higher-order photon contributions into account for the data analysis method [21] as well as for the theoretical predictions. A schematic of one possible passive decoy-state QKD implementation at Alice's side including the TMD is shown in Fig. 1.

For the experimental analysis, we derive the conditioned probabilities $p(\text{click}|n)$ as the fraction of measured click events in Bob's detector, given that an n-photon state is detected by Alice's nonideal TMD, and the total number of events:

$$p(\text{click}|n) = \frac{N(\text{click}|n)}{N(\text{click}|n) + N(\text{no click}|n)}. \tag{4}$$

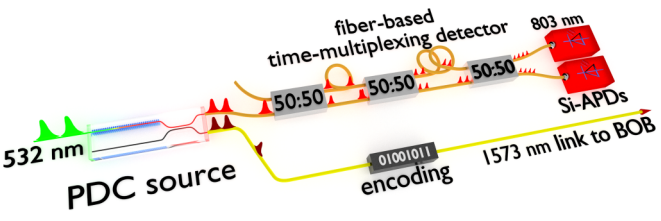

FIG. 1. (Color online) Alice's source configuration for passive decoy-state QKD: PDC signal photons (803 nm) are separated on chip from idler photons (1573 nm), fed into the eight-bin time multiplexer, and are detected with binary detectors (Si-APDs). The (encoded) idler photons are transmitted to Bob via the quantum channel.

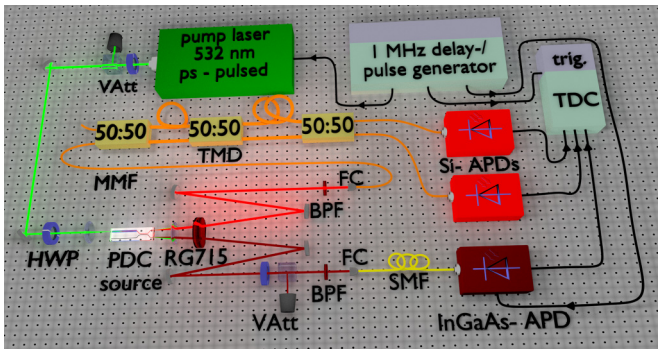

FIG. 2. (Color online) Experimental implementation of photon-number-resolving PDC analysis (VAtt: variable attenuator; HWP: half-wave plate; FC: fiber coupling; RG715: home-coated absorber; BPF: band pass filter; SMF: single-mode fiber; MMF: multimode fiber; TMD: time-multiplexing detector; APD: avalanche photodiode; TDC: time-to-digital-converter); see text for details.

Note, that $p(\text{click}|n)$ still has to be corrected for convolution effects.

We carry out pump-power-dependent measurements with the setup shown in Fig. 2, since the mean photon number of PDC states is related to the power of the pump pulse. Our pump laser offers ps pulses at 532 nm, which can be variably attenuated and coupled into our periodically poled waveguide structure. Generated signal and idler photons are demultiplexed on chip and separated into two output beams. Behind the waveguide chip, we clean up PDC photons from background and residual pump light using a home-coated absorber and narrowband dielectric filters. In the signal arm we address the TMD and, subsequently, two free-running silicon avalanche photodiodes (APD), both with $\eta_{Si} = 0.55$ detection efficiency. The idler arm consists of a variable attenuator, which mimics an arbitrary channel loss η_C. Behind this device, we address a gated InGaAs-APD, which offers 2.5 ns detection windows, a detection efficiency of $\eta_{Det} = 0.24$ and 1 μs dead time. It exhibits a dark count probability of $p_{dc} = 1.75 \times 10^{-4}$ per gate.

For the detection, all APDs are connected to a time-to-digital converter (TDC) offering 82 ps resolution. A home-programmed software analyzes the impinging signals for coincidences in order to extract the PDC click statistics at a specific pump power, i.e., mean photon number. Pump laser, TMD, and InGaAs-APD are synchronized, triggered, and delay compensated in terms of optical path differences by a delay generator running at 1 MHz repetition rate.

We analyze the photon-number-resolved click statistics of our PDC process at pump powers that range over two orders of magnitude. A high pump power forces the generation of higher-order photon states. The maximum accessible cw-equivalent pump power of 2 μW corresponds to a mean photon number of $\langle n \rangle = 0.84$, and it is determined by the saturation limit of our data acquisition system. At each pump-power level we can set arbitrary quantum channel transmission $0 < \eta_C \leqslant 1$ in the idler arm, mimicking different transmission distances of a real-world QKD system.

The Klyshko efficiencies [22] of our signal and idler arm η_T and η_B are given by the ratio of coincidence counts N_{coinc} and

TABLE I. Overview of the power-dependent Klyshko efficiencies at maximum channel transmission.

P_p [nW]	20	50	100	200	500	1000	2000
η_B[%]	10.75	10.72	10.65	10.02	9.97	9.41	8.55
η_T[%]	17.76	17.76	17.72	17.66	17.21	16.58	15.47

the total number of single counts in the respective opposite arm, N_B and $\sum_{n\geqslant 1} N_T(n)$. In order to correct the Klyshko efficiencies for uncorrelated events, we estimate the number of accidentals beforehand as

$$N_{acc} = \frac{N_B \cdot \sum_{n\geqslant 1} N_T(n)}{N_{Trig}}, \tag{5}$$

where $\sum_{n\geqslant 1} N_T(n)$ is the accumulated number of detection events in the TMD, N_B denotes the number of click events in the InGaAs-APD and N_{Trig} is the number of trigger events within our measurement time. This correction provides us with a lower bound for the actual Klyshko efficiency, because higher-order photon contributions lead to an overestimation of the real values. We also subtract coincidences $N_{dc,B}$ and $N_{dc,T}$ caused by dark counts of the respective detector, and we finally find

$$\eta_T = \frac{N_{coinc} - N_{acc} - N_{dc,T}}{N_B} \tag{6}$$

for the Klyshko efficiency in the signal/TMD arm and

$$\eta_B = \frac{N_{coinc} - N_{acc} - N_{dc,B}}{\sum_{n\geqslant 1} N_T(n)} \tag{7}$$

for the Klyshko efficiency of the idler arm.

The results for different pump powers are shown in Table I and indicate that our calculated Klyshko efficiencies are only reliable at low pump powers, since we tend to overestimate accidentals—according to Eq. (5)—for increasing pump powers and, thus, will artificially decrease the Klysko efficiencies. In order to predict the behavior of different n-photon states in the following, we base our theoretical calculations on Klyshko efficiencies obtained at the lowest available pump power. Note that this will surely underestimate the influence of accidentals.

In order to ensure distinct detection probabilities for different n-photon states after transmission through the quantum channel, we analyze the click statistics and reconstruct the probabilities $p(\text{click}|n)$ therefrom using Eq. (4) and the inverse convolution matrix [19,21,23] of our TMD. A typical measurement result at the highest accessible pump power of 2 μW and with $\eta_C = 1$ is shown in Table II. We can clearly identify click events up to photon numbers $n = 4$ within 60 s of measurement time, which strongly indicates heralded four-photon states.

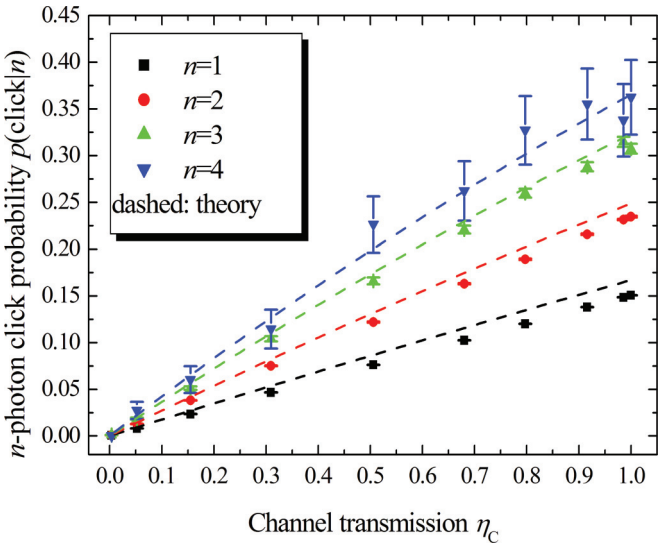

FIG. 3. (Color online) Dependencies of the n-photon click probabilities on the channel transmission at 2 μW cw-equivalent pump power; dashed: theory curves.

In Fig. 3 we plot $p(\text{click}|n)$ versus the channel transmission η_C, the latter of which represents an arbitrarily long transmission device between the two QKD parties. The distinct n-photon components clearly follow different slopes and show also higher detection probabilities for higher photon states. This verifies not only the high brightness of our source, but it also agrees excellently with the expected behavior. Our measurements closely match the theoretical curves calculated with Eq. (2), where we considered Poissonian distributions ρ_m as well as convolution effects. We also assumed Klyshko efficiencies of the low power regime, $\eta_T = 0.1776$ and $\eta_B = 0.1075$, respectively. Note, that the differences to the detection efficiencies η_{Si} and η_{Det} are caused by losses introduced by the implemented optical components.

In a practical passive decoy-state QKD system, a PNS attack will be detected by Alice and Bob, since the click probability of one-photon contributions would be increased artificially compared to the above statistics. Thus, even if Eve was able to replace parts of the lossy quantum channel by a perfect one for the attack, her presence can be recognized. This is due to the fact that it is still undecided during transmission which subset of n-photon number states will be employed as decoys. With our analysis scheme it is easy for Alice to anticipate how the click statistics at Bob's side should behave at distinct pump powers. Thus, our PDC source fulfills the necessary requirements for passive decoy-state QKD in terms of predictable photon statistics and accessibility to higher-order n-photon states in general. The seemingly growing mismatch between experimental data and theory curves for small n at large η_C

TABLE II. Typical click statistics at 2 μW pump power and with channel transmission $\eta_C = 1$.

	Zero-photon	One-photon	Two-photon	Three-photon	Four-photon
$N(\text{no click}\|n)$	49 244 089	6 157 356	334 960	10383	197
$N(\text{click}\|n)$	3 049 176	1 092 105	102 653	4608	112
$N_T(n)$	52 293 265	7 249 461	437 613	14991	309

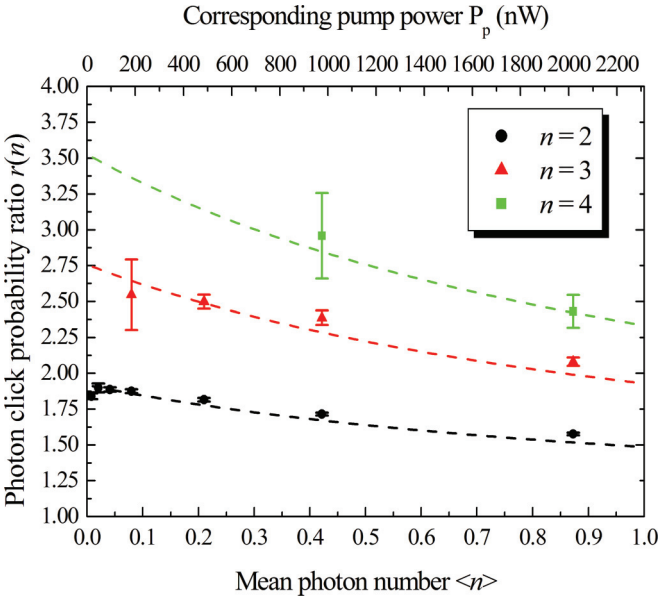

FIG. 4. (Color online) The click probability ratios $r(n)$ follow Poissonian distributions (dashed: theoretical predictions for $\eta_T = 0.1776$ and $\eta_B = 0.1075$).

can be explained by uncorrelated coincidences, which have an impact on $p(\text{click}|n)$. As stated above, by applying only Klyshko efficiencies from the low-power measurement to the theory, we underestimate accidentals for higher pump powers.

The applicability of our source over a large range of different brightnesses, as needed for optimization of the passive decoy scheme, is shown by the behavior for different mean photon numbers of the PDC states. In particular, we calculated $r(n)$ according to Eq. (3) from the individual deconvoluted click probabilities at variable channel transmissions. The average ratios are plotted against the mean photon number $\langle n \rangle$ in Fig. 4. We did not register significant three- and four-photon components at small mean photon numbers within acceptable measurement durations. However, our measurement data exhibit decreasing $r(n)$ at higher pump powers according to Poissonian statistics. This, on one hand, underlines the photon-number-resolving capabilities of our TMD, while on the other hand the very good agreement to the theory proves that the n-photon PDC states in our spectrally broad source [FWHM (803 nm) $\sim$ 0.7 nm] show almost pure Poissonian distributions. Remaining deviations from theory can be explained by the finite number of spectral modes in our source, and again by the impact of uncorrelated accidentals at higher mean photon numbers. The distinct detection probability ratios for different n-photon states are key to accessing higher-order photons as decoy states reliably. A PNS attack will change the above characteristics in a way that the ratios $r(n)$ decrease artificially due to the increased amount of one-photon contributions during classical PNS attacks and, thus, can be detected. Therefore, Fig. 4 shows that our source is usable at a broad range of pump powers.

In summary, we have shown the suitability of our integrated photon-pair source for practical passive decoy-state QKD. We determined its photon-number-resolved emission characteristics. Our results prove distinct detection probabilities for different n-photon states up to $n = 4$ at arbitrary quantum channel efficiencies. The dependencies of the n-photon state click probability ratios on increasing mean photon numbers closely follow Poissonian distributions according to the spectral multimode character of our PDC. Together with the capability to reliably provide heralded four-photon states and the excellent agreement to theoretical predictions, the high brightness of our source fulfills the requirements for passive decoy-state QKD. This constitutes an important step towards real-world implementation of QKD schemes, where all security loopholes have to be eliminated.

The authors thank the Deutsche Forschungsgemeinschaft for funding this work within the Graduate Program on 'Micro- and Nanostructures in Optoelectronics and Photonics' (GRK 1464 II).

[1] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Nature Photon. **4**, 686 (2010).
[2] Chi-Hang Fred Fung, B. Qi, K. Tamaki, and H.-K. Lo, Phys. Rev. A **75**, 032314 (2007).
[3] V. Makarov and D. R. Hjelme, J. Mod. Opt. **52**, 691 (2005).
[4] B. Qi, Chi-Hang Fred Fung, H.-K. Lo, and X. Ma, Quant. Inf. Comp. **7**, 73 (2007).
[5] A. Lamas-Linares and C. Kurtsiefer, Opt. Express **15**, 9388 (2007).
[6] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, Quant. Inf. Comp. **4**, 325 (2004).
[7] Y.-L. Tang, H.-L. Yin, X. Ma, Chi-Hang Fred Fung, Y. Liu, H.-L. Yong, T.-Y. Chen, C.-Z. Peng, Z.-B. Chen, and J.-W. Pan, Phys. Rev. A **88**, 022308 (2013).
[8] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Phys. Rev. Lett. **85**, 1330 (2000).
[9] C. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing* (IEEE, New York, 1984), pp. 175–179.
[10] W. Mauerer and C. Silberhorn, Phys. Rev. A **75**, 050305 (2007).
[11] M. Curty, X. Ma, B. Qi, and T. Moroder, Phys. Rev. A **81**, 022310 (2010).
[12] W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003).
[13] H.-K. Lo, H. Chau, and M. Ardehali, J. Cryptology **18**, 133 (2005).
[14] S. Krapick, H. Herrmann, V. Quiring, B. Brecht, H. Suche, and C. Silberhorn, New J. Phys. **15**, 033010 (2013).
[15] W. Mauerer, M. Avenhaus, W. Helwig, and C. Silberhorn, Phys. Rev. A **80**, 053815 (2009).
[16] W. Helwig, W. Mauerer, and C. Silberhorn, Phys. Rev. A **80**, 052326 (2009).
[17] D. Achilles, C. Silberhorn, C. Śliwa, K. Banaszek, and I. A. Walmsley, Opt. Lett. **28**, 2387 (2003).
[18] M. J. Fitch, B. C. Jacobs, T. B. Pittman, and J. D. Franson, Phys. Rev. A **68**, 043814 (2003).
[19] D. Achilles, C. Silberhorn, A. B. U'Ren, C. Sliwa, K. Banaszek, and I. A. Walmsley, in *Conference on Lasers*

and Electro-Optics/International Quantum Electronics Conference and Photonic Applications Systems Technologies (Optical Society of America, Washington, DC, 2004), p. IThD3.

[20] D. Achilles, C. Silberhorn, and I. A. Walmsley, Phys. Rev. Lett. **97**, 043602 (2006).

[21] M. Avenhaus, H. B. Coldenstrodt-Ronge, K. Laiho, W. Mauerer, I. A. Walmsley, and C. Silberhorn, Phys. Rev. Lett. **101**, 053601 (2008).

[22] D. N. Klyshko, Sov. J. Quant. Electron. **10**, 1112 (1980).

[23] H. B. Coldenstrodt-Ronge and C. Silberhorn, J. Phys. B **40**, 3909 (2007).