Comparison of non-decoy single-photon source and decoy weak coherent pulse in quantum key distribution

Roberto G. Pousa,* Daniel K. L. Oi, and John Jeffers

SUPA Department of Physics, University of Strathclyde,
Glasgow, G4 0NG, United Kingdom

Advancements in practical single-photon sources (SPS) exhibiting high brightness and low $g^{(2)}(0)$ have garnered significant interest for their application in quantum key distribution (QKD). To assess their QKD performance, it is essential to compare them with the widely employed weak coherent pulses (WCPs) in the decoy state method. In this work, we analyze the non-decoy efficient BB84 protocol for an SPS, partially characterising its photon statistics by its $g^{(2)}(0)$ and mean photon number. We compare it to the 2-decoy efficient BB84 with WCPs within the finite-key analysis framework while optimizing the parameters of both protocols. Our findings indicate that the non-decoy SPS with a mean photon number of $\langle n \rangle = 0.5$ and $g^{(2)}(0) = 3.6\%$ can enhance the secure key generation over the 2-decoy WCP for block sizes under $4.66 \cdot 10^9$ sent signals (29 seconds of acquisition time) at a channel loss of 10 dB (52.5 km of optical fibre). Additionally, we demonstrate an increase in the maximum tolerable channel loss for SPSs with mean photon number $\langle n \rangle \geq 0.0142$ at block sizes below 10^8 sent signals (0.62 seconds of acquisition time). These results suggest that SPSs hold potential for key rate enhancement in short-range QKD networks, though further research is required to evaluate their key generation capabilities when integrated into the decoy method.

Introduction. Public key cryptosystems have long proposed secure communication schemes between parties using two keys, in which the sender (Alice) uses one key for encryption, randomly applying an operation whose mutually inverse is used for decryption. Although Alice publicly announces the encryption method, the decryption instructions must remain confidential to the intended receiver (Bob). Allowing anyone to encrypt a message, the parties can swap roles and converse secretly. In a classical public key system, it is not possible to guarantee the private key cannot be derived from the encrypted key by computational methods [1, 2]. Seeking a security proof method, quantum mechanics was introduced, leading to the development of the quantum key distribution (QKD) field after a lot of refinement [3].

QKD protocols utilize a quantum channel to transmit signals with complementary physical properties, e.g. in the BB84 protocol, the exploited quantum property to detect an eavesdropper (Eve) is the polarization of light [4]. When Eve attempts to monitor the channel measuring the polarization, she inevitably disturbs a certain number of signals due to the Heisenberg uncertainty principle. This causes errors, allowing Alice and Bob to detect Eve's presence and estimate the information leaked to her. By setting an error threshold, Alice and Bob have a criterion to abort the protocol if the error rate exceeds a certain level.

An ideal QKD system would employ a quantum source that consistently sends single-photons. Although ongoing research aims to approach this ideal behaviour [5], it is strictly unachievable in practice. Instead, in real QKD systems, this inherent nonideality of practical sources is exploited by the photon number splitting (PNS) attack

[6, 7]. In a BB84 protocol employing exclusively one source intensity, known as non-decoy, Eve, who fully controls the channel, can perform PNS attacks to effectively intercept the key whilst remaining undetectable by exploiting the multiphotons. By employing quantum nondemolition measurements [8], Eve identifies the number of photons contained in each pulse. He then blocks the single-photon pulses and splits the multiphoton pulses into single-photons, which are forwarded to Bob, while the remaining photons are stored and measured after basis reconciliation. Therefore, to ensure the security of the non-decoy protocol the click probability of Bob's detectors has to be greater than the multiphoton emission of Alice, $p_{\text{click}} > p_{\text{mp}}$. Otherwise, assuming all multiphoton emissions cause a detection event on Bob's apparatus through Eve's lossless channel, the expected detection rate by Bob can be reproduced by Eve exclusively using the sent multiphotons in a high-loss scenario. Compromising the secrecy of the entire shared key bit string. Consequently, only non-multiphoton detections can be considered secure events.

Weak coherent pulse (WCP) sources, which are attenuated lasers approaching the single-photon regime, have been the most commonly employed sources in prepare-and-measure QKD protocols due to their feasibility [9]. However, even strongly attenuated WCPs have a sufficiently high multiphoton emission to be vulnerable to PNS attacks in lossy channels, failing to fulfil $p_{\text{click}} > p_{\text{mp}}$. To mitigate such attacks and ensure the inequality is met, the decoy method was proposed [10], which underwent significant refinement [11–14]. This technique involves using multiple intensity levels for WCPs with identical characteristics to bound the multiphoton events, i.e. detections caused by multiphotons. While ensuring both parties agree on their single-photon and vacuum events estimate, which form the secure key. This accurate estimation occurs since the used WCPs produce equal count-

arXiv:2405.19963v1 [quant-ph] 30 May 2024

ing rates for a sent k-photon state, commonly known as yields, despite their distinct photon emission probabilities. In fact, deviations in the yields between different WCP intensities indicate the presence of an eavesdropper, who lacks knowledge regarding the transmitted distribution.

Alternative quantum sources, such as single-photon sources (SPS) based on defects in 2D materials or quantum dots, exhibit significantly lower multiphoton emission than attenuated WCPs [15–17]. Therefore, considering no decoy states, these low-$g^{(2)}(0)$ SPSs satisfy the $p_{\text{click}} > p_{\text{mp}}$ condition at higher channel losses than a WCP, emerging as promising candidates for non-decoy protocols. However, to evaluate the QKD performance of practical SPSs, it is necessary to compare it with a state-of-the-art decoy WCP protocol. Thus, this work analyses the key generation of an efficient BB84 protocol for non-decoy SPS, expanding the analysis of [18] to other SPS characteristics plus providing further theoretical aspects, and for 2-decoy WCP based on [19]. Note that efficient BB84 uses one basis (X basis) for key generation and the other (Z basis) for parameter estimation, doubling the efficiency of standard BB84 [20].

In the decoy method, the single-photon and vacuum events are lower-bounded by analysing the statistics from the implemented multiple source intensities. In contrast, the non-decoy protocol estimates secure non-multiphoton events, lumping together the single-photon and vacuum events, excluding the insecure multiphoton events from the total sifted events, i.e. instances shared by both parties when they chose the same basis. To avoid overestimating the non-multiphoton events, it is essential to upper bound the sent multiphotons and the multiphoton events received by Bob. The subsequent finite-key analysis will address the latter, while Alice's source characterisation will handle the former.

Source characterisation and multiphoton probability. Our goal is not to fully characterise the SPS [21], rather, we seek an estimate of the source statistics that upper bounds the multiphoton emissions. We denote the true photon emission probabilities of the SPS in the Fock basis as $\{P_k^{(SPS)}\}_{k \in \mathbb{N}}$ for the infinite Hilbert space, where the multiphoton emission probability is $P_{\text{mp}}^{(SPS)} = \sum_{k \geq 2} P_k^{(SPS)}$. We assume these true probabilities are not directly accessible. Instead, we estimate the photon number distribution of the SPS using the mean photon number $\langle n \rangle$ and the time-zero second-order correlation function $g^{(2)}(0)$. Consequently, the multiphoton probability can be upper-bounded as $P_{\text{mp}}^{(SPS)} \leq \bar{p}_{\text{mp}} = g^{(2)} \langle n \rangle^2 / 2$ [22]. Here, uppercase P represents the true emission probabilities, while lowercase p denotes bounded estimates.

To simulate the counts of Bob's apparatus as in a real experiment, we select the set of photon states emitted by Alice's source which reaches exactly $\bar{p}_{\text{mp}}$, ensuring no other combination of states exceeds this upper bound. We study two types of distributions. First, we examine

a pathological distribution where all the emission probabilities are null except three: vacuum, single-photon and K-photon probabilities $\{p_0, p_1, p_K\}$, where $K \geq 3$ is a fixed value. In this case, all multiphotons are K-photon states, and any possible distribution yields a lower upper bound than $\bar{p}_{\text{mp}}$. As expected, when K tends to infinity, the multiphoton probability approaches $\bar{p}_{\text{mp}}$, thus saturating the initial upper bound on the multiphoton probability.

We assume an SPS distribution that exhibits a monotonic decrease in its kth-order correlation functions $g^{(k+1)}(0) \leq g^{(k)}(0)$ for all $k \geq 2$, which is experimentally verifiable. Expressing each emission probability $p_k^{(MD)}$ in terms of its associated $g^{(k)}(0)$, the upper bound of the multiphoton probability is given by

$$
\begin{aligned}
p_{\text{mp}}^{(MD)} &= p_2^{(MD)} + \sum_{k=3}^{\infty} p_k^{(MD)} \\
&= \frac{g^{(2)}(0) \langle n \rangle^2}{2} + \sum_{k=3}^{\infty} \frac{k-1}{k}(-1)^k g^{(k)}(0) \langle n \rangle^k \\
&\leq \bar{p}_{\text{mp}}^{(MD)} = \bar{p}_{\text{mp}} + g^{(2)}(0) \underbrace{\sum_{k=3}^{\infty} \frac{k-1}{k}(-1)^k \langle n \rangle^k}_{<0},
\end{aligned}
$$

hence $\bar{p}_{\text{mp}}^{(MD)} \leq \bar{p}_{\text{mp}}$. Note that in any truncated Hilbert space, making the summation finite, this inequality holds. Though counterintuitive, we conclude that any distribution with states higher than two-photons decreases the overall multiphoton probability. Consequently, to simulate Bob's counts, we implement the distribution $\{p_k^{(MD)}\}_{k=0,1,2}$ with $p_{k>2}^{(MD)} = 0$, since it satisfies the equality $p_{\text{mp}}^{(MD)} = p_2^{(MD)} = \bar{p}_{\text{mp}}$. Thus, Alice's emission probabilities read as

$$
p_2^{(MD)} = \frac{g^{(2)}(0) \langle n \rangle^2}{2} \tag{1}
$$

$$
p_1^{(MD)} = \langle n \rangle - 2p_2^{(MD)} \tag{2}
$$

$$
p_0^{(MD)} = 1 - p_2^{(MD)} - p_1^{(MD)}. \tag{3}
$$

Furthermore, pre-attenuating Alice's source increases the maximum tolerable channel loss, defined as the highest loss that generates a positive key. We define this pre-attenuation by a transmissivity value η_{tr}, representing the fraction of signal that goes through the attenuator to the quantum channel. This transmissivity reduces the multiphoton probability quadratically $\bar{p}_m^{(att)} = g^{(2)}(0) \langle n \rangle^2 \eta_{\text{tr}}^2 / 2$, while decreasing the click probability at Bob's detectors linearly at a first-order Taylor approximation, $p_{\text{click}} = \sum_{n=0}^{\infty} p_k^{(MD)} [1 - (1 - p_{\text{dc}})(1 - \eta_{\text{tr}}\eta_{\text{ch}}\eta_{\text{det}})^n] \approx p_{\text{dc}} + (1 - p_{\text{dc}}) \eta_{\text{tr}}\eta_{\text{ch}}\eta_{\text{det}} \langle n \rangle$, where η_{ch} and η_{det} are the channel and detector efficiencies, respectively, and p_{dc} is the dark count probability. Although we compute the exact expression in our model, this approximation is valid

as states with two or more photons do not dominate the source photon emission. Therefore, the multiphoton probability decreases more rapidly than the click probability on Bob's side, widening the range of tolerable losses. This enhances the key generation at the high-loss regime where $\overline{p}_m^{(att)}$ dominates, obtaining the highest possible secure key by optimising η_{tr} for each channel loss. Additionally, the basis bias p_X, the probability of choosing the X basis by either party, is also optimised. Note that $p_Z = 1 - p_X$ for the parameter estimation basis. Setting an unequal bias has been reported as an exceptional strategy to increase the key generation [23, 24].

Secure key length estimation: asymptotic and finite-key analysis. We distinguish two scenarios for the secure key length (SKL) estimation: the asymptotic and finite-key analysis. In the asymptotic limit, we assume the experiment runs for an infinity time duration, resulting in a sufficiently large number of detection events in the key generation basis, allowing us to consider $p_X \to 1$, and a negligible phase error rate, $p_Z \to 0$. Consequently, the count rates converge to their underlying true expectation values. Asymptotic secure key rates were already proposed long ago such as the Devetak-Winter bound [25]. However, in this work, we compute the asymptotic key rates by simply setting a sufficiently large block size, which yields identical outcomes to the asymptotic formula.

However, in a real experiment, the obtained statistics are finite and subject to fluctuations from their expected outcomes. Consequently, studies were proposed to account for the effect of finite statistics [26]. Here, this issue is addressed as follows: with generality, we define the number of multiphoton states received by Bob as a finite set of independent Bernoulli random variable $\{X_1^B, X_2^B, \cdots, X_{N_S}^B\}$ with two possible outcomes $\{0, 1\}$. Its observed value is $X^B \equiv \sum_{i=1}^{N_S} X_i^B$ that satisfy $\Pr\left(X_i^B = 1\right) = P_{i,\text{click}|m} P_{i,m}^{(att)}$ for fixed fixed $m \geq 2$, i.e. the product of the conditional probability of a click when a multiphoton is sent after Alice's pre-attenuation and the probability of sending a multiphoton. Note that each random variable denoted by the subscript i is associated with a multiphoton state with a fixed number of photons $m \geq 2$, which may change for each variable, hence their probabilities too. To prevent an overestimation of the secure events, we assume the worst scenario where every sent multiphoton, which is untrustworthy, causes a click on Bob's apparatus, i.e. $P_{i,\text{click}|m} = 1$. Therefore, an expected value of X^B is expressed as $X^{B*} = \sum_{i=1}^{N_S} P_{i,m}^{(att)}$, where $N_S = R_{\text{rate}}t$ is the number of sent signals by Alice that forms the finite block, defined by the acquisition time t, i.e. the time the experiment is run, and the source repetition rate R_{rate}. However, since we lack access to the true attenuated photon emission probabilities of the SPS $P_{i,m}^{(att)}$, we bound them as $X^{B*} = \sum_{i=1}^{N_S} P_{i,m}^{(att)} \leq \sum_{i=1}^{N_S} \overline{p}_{\text{mp}}^{(att)} = N_S \overline{p}_{\text{mp}}^{(att)}$. Note that even if the legitimate parties had access to them from perfect SPS characterisation, they would not know how many photons Alice sends in each state. After sifting, the expected number of multiphoton events received by Bob in the key generation basis is $N_{\text{R,mp}}^{X*} = p_X^2 X^{B*} \leq N_S p_X^2 \overline{p}_{\text{mp}}^{(att)} = \overline{N}_{\text{R,mp}}^{X*}$.

In a real QKD experiment, Bob observes clicks from his detector and unfortunately, even if Bob measures the multiphoton events using a photon number resolving detector, his results cannot be trusted due to potential PNS attacks by Eve. Therefore, we need a consistent method that for a given expected value $N_{\text{R,mp}}^{X*}$ of a data block, derives an upper bound of the observed value $\overline{N}_{\text{R,mp}}^{X}$, whose tail probability is bounded with a parameter estimation failure probability as $\Pr\left[N_{\text{R,mp}}^{X} \geq \left(1 + \Delta^U\right) N_{\text{R,mp}}^{X*}\right] \leq \varepsilon_{\text{PE}} = 2\varepsilon_{\text{sec}}/3$.

Several methods were proposed to account for these statistical fluctuations in finite blocks for decoy WCP methods, such as the Gaussian analysis method [27], the Hoeffding inequality [19] and the multiplicative Chernoff bound [28]. However, an improved analytical Chernoff bound has reported tighter finite-key bounds, enhancing the key generation [29]. Here, for our 2-decoy WCP protocol, we employ this updated Chernoff bound with the decoy method of [28], as presented in the analysis of [30] but for a fibre link instead of a satellite-to-ground link. Our non-decoy SPS protocol of [18] has already shown massive key rate enhancements using the same updated Chernoff bound as the decoy WCP studies, compared to previous mathematical deviations applied to protocol probabilities [31]. Thus, we apply their Chernoff bound to estimate the upper bound of the observed value $\overline{N}_{\text{R,mp}}^{X} = \overline{N}_{\text{R,mp}}^{X*} + \Delta^U$ with $\Delta^U = \left(\beta + \sqrt{8\beta \overline{N}_{\text{R,mp}}^{X*} + \beta^2}\right)/2\overline{N}_{\text{R,mp}}^{X*}$ where $\beta = -\ln \varepsilon_{\text{PE}}$. The lower bound of the observed non-multiphoton events in the key generation basis is $\underline{N}_{\text{R,nmp}}^{X} = N_{\text{R}}^{X} - \overline{N}_{\text{R,mp}}^{X}$, where $N_{\text{R}}^{X} = N_S p_X^2 p_{\text{click}}$ is the observed number of detection events in the X basis by Bob. Likewise, $N_{\text{R}}^{Z} = N_S p_Z^2 p_{\text{click}}$ and $\underline{N}_{\text{R,nmp}}^{Z} = N_{\text{R}}^{Z} - \overline{N}_{\text{R,mp}}^{Z}$ are calculated for the parameter estimation basis. Note that here the security condition against PNS attacks $p_{\text{click}} > \overline{p}_{\text{mp}}^{(att)}$ is imposed because if it is not met, $\underline{N}_{\text{R,nmp}}^{X}$ is negative, resulting in no shared key, see eq. (5). The number of errors is determined as $m_X = N_S p_X^2 p_{\text{err}}$ and $m_Z = N_S p_Z^2 p_{\text{err}}$ for each basis, where given the error probability due to misalignment of the set-up p_{mis} the error probability reads as

$$p_{\text{err}} = \frac{p_0 p_{\text{dc}}}{2} + \sum_{n=1}^{\infty} p_n \left[1 - (1 - p_{\text{dc}})(1 - \eta_{ch}\eta_{det}\eta_{att})^n\right] p_{\text{mis}}. \tag{4}$$

Note m_X is not publicly revealed and is only used to estimate the number of bits needed to perform error correction.

Subsequently, we blind ourselves to this simulation model and work with the observed outcomes to estimate the secure key length (SKL). We calculate the SKL for each finite block defined by the number of sent signals N_S.

The main steps of the efficient BB84 protocol proceed as follows: Alice sends N_S states from her pre-attenuated SPS and Bob measures them, obtaining N_R detection events. This block is split into three sub-blocks: the discarded events due to sifting $2p_X(1 - p_X)$, the events used for key generation p_X^2 and the events used for parameter estimation $(1 - p_X)^2$. Finally, the extracted SKL from the sifted key is given by [18]

$$\ell_{\text{SPS}} = \underline{N}_{\text{R,nmp}}^X \left[1 - H\left(\overline{\phi}^X\right)\right] - \lambda_{\text{EC}} - 2\log_2 \frac{3}{\varepsilon_{\text{sec}}} - \log_2 \frac{2}{\varepsilon_{\text{cor}}}, \quad (5)$$

where $1 - H\left(\overline{\phi}^X\right)$ represents the information leaked to Eve, bounded by the binary entropy $H(e) = -e \log_2 e - (1-e)\log_2(1-e)$. We set a phase error rate threshold of $\phi_{\text{th}}^X = 0.11$ (11 %) [32]. Thus, the legitimate parties abort the protocol if $\overline{\phi}^X \geq \phi_{\text{th}}^X$, assuming the presence of an eavesdropper. The parties publicly announce their errors in the parameter estimation basis m_Z to estimate the phase error rate caused by non-multiphotons in the key generation basis $\phi_X = m_Z/\underline{N}_{\text{R,nmp}}^Z$, which is upper-bounded for the N_R^X sample, that is not revealed, as $\overline{\phi}^X = \phi_X + \gamma^U\left(N_R^X, N_R^Z, \phi_X, \varepsilon_{\text{PE}}\right)$ using the γ^U function of [29] for the random sampling without replacement problem. λ_{EC} accounts for the number of bits used in the error correction code and we use the improved approximation of [33]. However, no practical code has reached a value below the Shannon limit of $1.16 N_R^X H(e_X)$ where $e_X = m_X/N_R^X$ is the quantum bit error rate. Therefore, if $\lambda_{EC}/N_R^X H(e_X) < 1.16$, we recover the Shannon limit to estimate the bits used in error correction. Finally, the last two terms represent the secrecy and correctness parameters, ε_{sec} and ε_{cor} respectively, which ensures the protocol is $\varepsilon_{\text{QKD}} = \varepsilon_{\text{sec}} + \varepsilon_{\text{cor}}$ secure in the composable security framework [34].

Since we lump together the vacuum and single-photon detection events into the non-multiphoton estimation, one may think adding a vacuum distribution allows us to estimate them separately and more accurately, hence enhancing the key rate. Here we show this is not the case. We consider two new scenarios: first, Bob knows exactly the vacuum contribution, $N_{\text{R,0}}^X = N_S p_X^2 p_0^{(\text{MD})} p_{\text{click}}$; second, Bob estimates a lower bound of the vacuum events. For the latter, using the mean photon number definition, we estimate the lower bound of the vacuum emission probability as $P_0 \geq \underline{p}_0 = 1 - \langle n \rangle$ and then the vacuum events as $\underline{N}_{\text{R,0}}^X = N_S p_X^2 \underline{p}_0 p_{\text{click}}$.

The key enhancement showed by these two scenarios with a vacuum decoy state goes unnoticed for all channel losses. In particular, in the high-loss regime, even assuming Bob has complete knowledge of the vacuum contribution, the maximum tolerable loss increases by only 0.05 dB for one minute of acquisition time, see Figure 1. Therefore, due to its modest key rate increase, the extra experimental endeavour, considering the usual difficulty of creating a perfect decoy vacuum state in practice [12, 35], and the need for additional detector char-
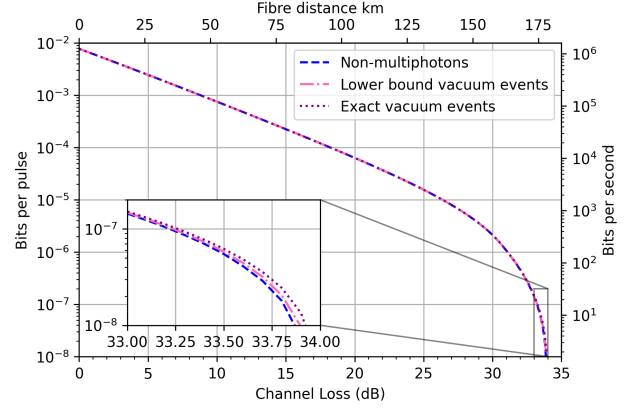

FIG. 1. The secure key of the non-decoy SPS protocol as a function of the channel loss (fibre distance) in a semi-log scale with optimised p_X and η_{tr}. The $g^{(2)}(0) = 0.036$ and the mean photon number $\langle n \rangle = 0.0142$ are fixed for 1 minute of acquisition time. The dashed blue curve represents the SKL using the non-multiphoton estimation, and the other two curves estimate separately the vacuum and single-photon events, the green dotted curve uses lower bound on the vacuum events $\underline{N}_{\text{R,0}}^X$ and the dashed purple curve uses the exact number of vacuum events $N_{\text{R,0}}^X$.

acterisation to estimate the vacuum contribution, is not worth considering. Thus, we also show the lower bound of the non-multiphoton events is not underestimated compared to estimating the events separately. As a result, we take this conservative approach and assume that Eve gains the same amount of information from the vacuum states as from the single-photon states.

As mentioned above, we also employ the updated Chernoff bound for a 2-decoy protocol with WCPs. Thus, we use the finite-key analysis and parameter optimisation of [30], considering one decoy state with a lower intensity than the signal state and a vacuum decoy state, whose secret key length is given by

$$\ell_{\text{WCP}} = \underline{N}_{\text{R,0}}^X + \underline{N}_{\text{R,1}}^X \left[1 - H(\bar{\phi}^X)\right] - \lambda_{\text{EC}} \\ - 6\log_2 \frac{21}{\varepsilon_{\text{sec}}} - \log_2 \frac{2}{\varepsilon_{\text{cor}}}, \quad (6)$$

where $\underline{N}_{\text{R,0}}^X$, $\underline{N}_{\text{R,1}}^X$ are the lower bounds of the vacuum and single-photon events respectively. Note that the rest of the parameters follow the same criteria as in the non-decoy SPS protocol. Finally, the secure key rate (SKR) is defined as $r_{\text{SPS}} = \ell_{\text{SPS}}/N_S$ and $r_{\text{WCP}} = \ell_{\text{WCP}}/N_S$ for non-decoy SPS and 2-decoy WCP, respectively.

Discussion. Here, we analyse the impact of different SPS characteristics on the secure key and the maximum tolerable loss for several finite blocks. The block size used to extract the secure key is defined by the number of signals sent by Alice which depends on the acquisition time of the experiment. We compare the results of the non-decoy SPS protocol with the 2-decoy WCP protocol. The fixed QKD parameters to all protocols and figures are shown in Table I.
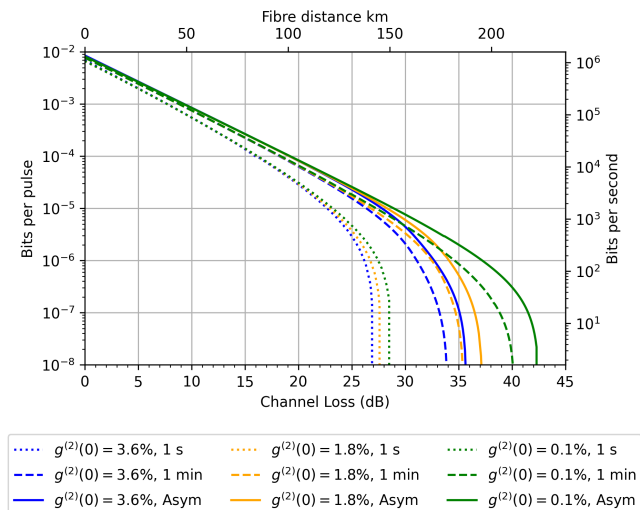
FIG. 2. Comparison of the secure key in a semi-log scale for the non-decoy SPS protocol with several second-order correlation functions $g^{(2)}(0)$ and block sizes, optimising the basis bias p_X and the transmissivity η_{tr} associated with Alice's source pre-attenuation for each channel loss. The SKR r_{SPS} and SKL ℓ_{SPS}, eq. (5), are represented by the bits per pulse and the bits per second, respectively. The $g^{(2)}(0) = 3.6\%$ (blue curves) corresponds to the quantum dot used in the QKD analysis of [18]. The $g^{(2)}(0) = 1.8\%$ (orange curves) is based on [36] and $g^{(2)}(0) = 0.1\%$ (green curves) is considered an optimistic case. The mean photon number is fixed to $\langle n \rangle = 0.0142$, which corresponds to the quantum dot of [18]. We consider two acquisition times (number of sent signals) of 1 second ($1.607 \cdot 10^8$), dotted curves, and 1 minute ($9.642 \cdot 10^9$), dashed curves, plus the asymptotic limit, solid curves.

Description	Parameter	Value
Source repetition rate	R_{rate}	160.7 MHz
Misalignment probability	p_{mis}	0.003
Dark count probability	p_{dc}	3.67×10^{-8}
Detector efficiency	η_{det}	0.6525
Fibre loss	l	0.1904 dB/km
Secrecy failure probability	$\varepsilon_{\mathrm{sec}}$	10^{-10}
Correctness failure probability	$\varepsilon_{\mathrm{cor}}$	10^{-15}

TABLE I. Baseline QKD protocol parameters based on the experiment of the quantum dot [18].

In Figure 2, we show the impact of $g^{(2)}(0)$ on the secure key performance for channel losses (optical fibre distances) in the non-decoy SPS protocol. As expected, fixing the dark count probability means that the $g^{(2)}(0)$ value determines the drop-off of the secure key curves, hence the maximum tolerable loss. For a one-second time block (dotted curves), the improvement in the maximum tolerable loss is approximately 1 dB between the three $g^{(2)}(0)$ values, which is modest. However, for one minute of acquisition time (dashed curves), the difference in the range of tolerable losses among the $g^{(2)}(0)$ values exhibits a considerable increment since the secure key per-
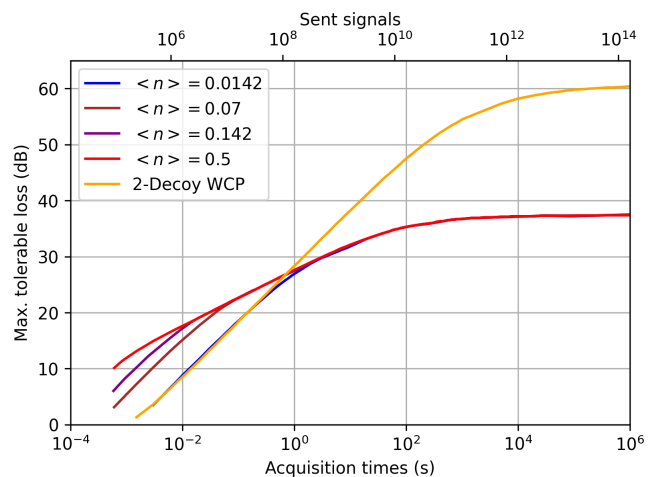
FIG. 3. Comparison of the maximum tolerable channel loss as a function of the acquisition time in a semi-log scale for the non-decoy SPS protocol with several mean photon numbers $\langle n \rangle$ and the 2-decoy WCP protocol (orange curve), optimising the free parameters in both protocols. The maximum loss is displayed as a function of the block size represented by the acquisition time or the number of sent signals by Alice. Here the second-order correlation function is fixed to $g^{(2)}(0) = 3.6\%$.

formance is already remarkably close to the asymptotic regime. The asymptotic key of $g^{(2)}(0) = 3.6\%$ (solid blue curve) is approached at one minute of acquisition time by halving the $g^{(2)}(0)$ (dashed orange line). It is worth mentioning that one hour of acquisition time is needed for $g^{(2)}(0) = 3.6\%$ to approach its asymptotic key rate. Therefore, halving the $g^{(2)}(0)$ from 3.6% to 1.8% produces similar key rates but for massively different block sizes, resulting in a reduction of approximately 98% in the acquisition time.

In Figure 3, we show the maximum tolerable channel loss varying the mean photon number $\langle n \rangle$ while fixing $g^{(2)}(0)$. A higher $\langle n \rangle$ represents a lower vacuum emission and higher single-photon and multiphoton emissions. Therefore, the higher $\langle n \rangle$ is, the lower acquisition time (number of sent signals) is required for the pre-attenuation of Alice's source to kick in. The SPS with $\langle n \rangle = 0.5$ (red curve) introduces the pre-attenuation even for the smallest acquisition time. This indicates that any other source with a mean photon number $\langle n \rangle > 0.5$ will not be able to cause a rise in the maximum tolerable loss, as the distribution will be pre-attenuated by Alice anyway. The point at which each curve converges to the curve with $\langle n \rangle = 0.5$ represents its first acquisition time in which the pre-attenuation is introduced. For acquisition times above one second, all the key curves reach the secure key of $\langle n \rangle = 0.5$ and their asymptotic limit is achieved above 100 seconds where the maximum loss is constant despite the rise of time. In particular, for the SPS of [18] (blue curve), there is an increase between 0.1 and 0.2 dB on the maximum tolerable loss for acqui-
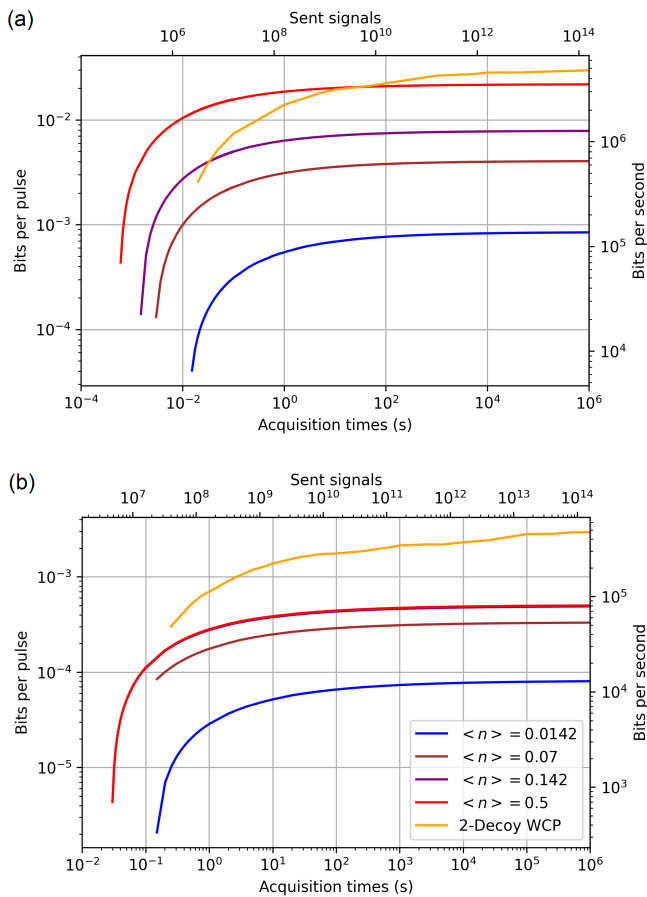
FIG. 4. Secure key as a function of the acquisition times (sent signals) in log-log scale for (a) 10 dB and (b) 20 dB of channel loss for the optimised non-decoy SPS protocol with various mean photon numbers $\langle n \rangle$ and the optimised 2-decoy WCP method (orange curve). Here the $g^{(2)}(0) = 0.036$.

sition times within the interval of $[0.01, 0.1]$ seconds. A greater mean photon number than $\langle n \rangle > 0.0142$ is needed to tolerate higher losses than the 2-decoy state protocol for times below 0.62 seconds (10^8 sent signals). Consequently, an SPS with $\langle n \rangle > 0.0142$ would extend the range of tolerable losses compared to a decoy WCP system with a maximum tolerable channel loss of 25 dB or below. Outside this range, the superiority of the 2-decoy WCP is evident. However, it is worth mentioning the SPS with the highest mean photon number, $\langle n \rangle = 0.5$, for extremely short acquisition times of 0.01 seconds, the SPS protocol tolerates up to 9 dB (47 km) more channel loss (fibre distance) than the WCP protocol.

We also fix the channel loss and show the secure key rate versus time blocks. Note that for the fixed losses in Figure 4, a higher mean photon number than $\langle n \rangle = 0.5$ (red curve) would produce the same key rate, since it

would be pre-attenuated and $g^{(2)}(0)$ does not dominate in this low-loss regime. Therefore, $\langle n \rangle = 0.5$ shows the highest possible secure key generation for the SPS protocol at these channel losses. This principle is illustrated in Figure 4 (b) with 20 dB of channel loss, where the key results of $\langle n \rangle = 0.5$ (red curve) overlap with the secure key curve of $\langle n \rangle = 0.142$ (purple curve). In the regime when the block size tends to the asymptotic limit, the highest key rate (red curve) scales by a factor of 5 compared to the lowest $\langle n \rangle = 0.0142$. Furthermore, non-decoy SPS only shows an advantage over the 2-decoy WCP at 20 dB loss for extremely small acquisition times, where the 2-decoy method is unable to generate key. In Figure 4 (a) with a 10 dB of channel loss, the non-decoy SPS of $\langle n \rangle = 0.142$ (purple line) and $\langle n \rangle = 0.5$ (red line) outperform the secure key generation of the 2-decoy WCP (orange curve) for block sizes approximately below 0.03 seconds ($4.8 \cdot 10^6$ sent signals) and 29 seconds ($4.66 \cdot 10^9$ sent signals), respectively.

Conclusions. We demonstrate that the non-decoy SPS may enhance the key rate performance of the 2-decoy WCP for short acquisition times (small number of sent signals) in the low-loss regime. Additionally, the range of acquisition times where the non-decoy SPS surpasses the 2-decoy WCP can be potentially wider for channel losses below 10 dB (52.5 km of fibre). Within the same regime, at least a mean photon number as the quantum dot in [18] is required to tolerate higher losses over the 2-decoy WCP. Complementary SPS characteristics for both improvements include a $g^{(2)}(0) \leq 3.6\%$ and a source repetition rate of $R_{\text{rate}} \geq 160.7$ MHz. Through our theoretical key estimates, we present SPSs as a valid quantum source for short-range QKD, performing an efficient BB84 protocol with one unique source at Alice's side, thus avoiding experimental complexity associated with decoy methods. Nevertheless, further research is necessary to establish a fair comparison between WCPs and SPSs within the decoy method framework. Concretely, a comparison to decoy analysis using a Fock basis notation that aligns with the SPS approach outline here would be beneficial [37].

[1] M. E. Hellman, An overview of public key cryptography, IEEE Communications Magazine **40**, 42 (2002).

[2] J. Grollmann and A. L. Selman, Complexity measures for public-key cryptosystems, SIAM Journal on Computing **17**, 309 (1988).

[3] C. H. Bennett, G. Brassard, and A. K. Ekert, Quantum cryptography, Scientific American **267**, 50 (1992).

[4] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, Theoretical computer science **560**, 7 (2014).

[5] H. Wang, Y.-M. He, T.-H. Chung, H. Hu, Y. Yu, S. Chen, X. Ding, M.-C. Chen, J. Qin, X. Yang, *et al.*, Towards optimal single-photon sources from polarized microcavities, Nature Photonics **13**, 770 (2019).

[6] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Limitations on practical quantum cryptography, Physical review letters **85**, 1330 (2000).

[7] N. Lütkenhaus, Security against individual attacks for realistic quantum key distribution, Physical Review A **61**, 052304 (2000).

[8] V. B. Braginsky, Y. I. Vorontsov, and K. S. Thorne, Quantum nondemolition measurements, Science **209**, 547 (1980).

[9] D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden, Fast and simple one-way quantum key distribution, Applied Physics Letters **87** (2005).

[10] W.-Y. Hwang, Quantum key distribution with high loss: toward global secure communication, Physical review letters **91**, 057901 (2003).

[11] H.-K. Lo, X. Ma, and K. Chen, Decoy state quantum key distribution, Physical review letters **94**, 230504 (2005).

[12] D. Rosenberg, J. W. Harrington, P. R. Rice, P. A. Hiskett, C. G. Peterson, R. J. Hughes, A. E. Lita, S. W. Nam, and J. E. Nordholt, Long-distance decoy-state quantum key distribution in optical fiber, Physical review letters **98**, 010503 (2007).

[13] T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. G. Rarity, *et al.*, Experimental demonstration of free-space decoy-state quantum key distribution over 144 km, Physical Review Letters **98**, 010504 (2007).

[14] D. Rusca, A. Boaron, F. Grünenfelder, A. Martin, and H. Zbinden, Finite-key analysis for the 1-decoy state qkd protocol, Applied Physics Letters **112** (2018).

[15] T. Vogl, Y. Lu, and P. K. Lam, Room temperature single photon source using fiber-integrated hexagonal boron nitride, Journal of Physics D: Applied Physics **50**, 295101 (2017).

[16] C. L. Morrison, M. Rambach, Z. X. Koong, F. Graffitti, F. Thorburn, A. K. Kar, Y. Ma, S.-I. Park, J. D. Song, N. G. Stoltz, *et al.*, A bright source of telecom single photons based on quantum frequency conversion, Applied Physics Letters **118** (2021).

[17] S. Thomas, M. Billard, N. Coste, S. Wein, H. Ollivier, O. Krebs, L. Tazaïrt, A. Harouri, A. Lemaitre, I. Sagnes, *et al.*, Bright polarized single-photon source based on a linear dipole, Physical review letters **126**, 233601 (2021).

[18] C. L. Morrison, R. G. Pousa, F. Graffitti, Z. X. Koong, P. Barrow, N. G. Stoltz, D. Bouwmeester, J. Jeffers, D. K. Oi, B. D. Gerardot, *et al.*, Single-emitter quantum key distribution over 175 km of fibre with optimised finite key rates, Nature Communications **14**, 3573 (2023).

[19] C. C. W. Lim, M. Curty, N. Walenta, F. Xu, and H. Zbinden, Concise security bounds for practical decoy-state quantum key distribution, Physical Review A **89**, 022307 (2014).

[20] H.-K. Lo, H. F. Chau, and M. Ardehali, Efficient quantum key distribution scheme and a proof of its unconditional security, Journal of Cryptology **18**, 133 (2005).

[21] R. Alléaume, F. Treussart, J.-M. Courty, and J.-F. Roch, Photon statistics characterization of a single-photon source, New Journal of physics **6**, 85 (2004).

[22] E. Waks, C. Santori, and Y. Yamamoto, Security aspects of quantum key distribution with sub-poisson light, Physical Review A **66**, 042315 (2002).

[23] Z. Wei, W. Wang, Z. Zhang, M. Gao, Z. Ma, and X. Ma, Decoy-state quantum key distribution with biased basis choice, Scientific reports **3**, 2453 (2013).

[24] Z.-W. Yu, Y.-H. Zhou, and X.-B. Wang, Reexamination of decoy-state quantum key distribution with biased bases, Physical Review A **93**, 032307 (2016).

[25] I. Devetak and A. Winter, Distillation of secret key and entanglement from quantum states, Proceedings of the Royal Society A: Mathematical, Physical and engineering sciences **461**, 207 (2005).

[26] J. Hasegawa, M. Hayashi, T. Hiroshima, and A. Tomita, Security analysis of decoy state quantum key distribution incorporating finite statistics, arXiv preprint arXiv:0707.3541 (2007).

[27] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, Practical decoy state for quantum key distribution, Physical Review A **72**, 012326 (2005).

[28] M. Curty, F. Xu, W. Cui, C. C. W. Lim, K. Tamaki, and H.-K. Lo, Finite-key analysis for measurement-device-independent quantum key distribution, Nature communications **5**, 3732 (2014).

[29] H.-L. Yin, M.-G. Zhou, J. Gu, Y.-M. Xie, Y.-S. Lu, and Z.-B. Chen, Tight security bounds for decoy-state quantum key distribution, Scientific Reports **10**, 1 (2020).

[30] J. S. Sidhu, T. Brougham, D. McArthur, R. G. Pousa, and D. K. Oi, Finite key effects in satellite quantum key distribution, npj Quantum Information **8**, 18 (2022).

[31] R. Y. Cai and V. Scarani, Finite-key analysis for practical implementations of quantum key distribution, New Journal of Physics **11**, 045024 (2009).

[32] P. W. Shor and J. Preskill, Simple proof of security of the bb84 quantum key distribution protocol, Physical review letters **85**, 441 (2000).

[33] M. Tomamichel, J. Martinez-Mateo, C. Pacher, and D. Elkouss, Fundamental finite key limits for one-way information reconciliation in quantum key distribution, Quantum Information Processing **16**, 1 (2017).

[34] R. Renner, Security of quantum key distribution, International Journal of Quantum Information **6**, 1 (2008).

[35] A. Dixon, Z. Yuan, J. Dynes, A. Sharpe, and A. Shields, Gigahertz decoy quantum key distribution with 1 mbit/s secure key rate, Optics express **16**, 18790 (2008).

[36] M. Rakhlin, A. Galimov, I. Dyakonov, N. Skryabin, G. Klimko, M. Kulagina, Y. M. Zadiranov, S. Sorokin, I. Sedova, Y. A. Guseva, *et al.*, Demultiplexed single-photon source with a quantum dot coupled to microres-

onator, Journal of Luminescence **253**, 119496 (2023).

[37] X.-B. Wang, L. Yang, C.-Z. Peng, and J.-W. Pan, Decoy-state quantum key distribution with both source errors and statistical fluctuations, New Journal of Physics **11**, 075006 (2009).