Performance Guarantees in Quantum Key Distribution Networks

Fengyou Sun and Yuming Jiang
Department of Information Security and Communication Technology,
NTNU, Norwegian University of Science and Technology, Trondheim, Norway

***Abstract*—This paper aims to present a mathematical tool useful for quantum key distribution network configuration. In particular, the paper studies the throughput of secret key distribution in a quantum key distribution network with trusted repeaters. In addition, the backlog of secret keys at a trusted repeater is also investigated. The analysis is based on the queueing principle of secret keys in the trusted repeater, implied by that the transmission of secret keys in the network is store-and-forward. The obtained results are applied to a discrete-variable protocol with weak coherent pulse sources, where realistic system parameters are integrated in the analysis. It is shown that, if the secret key rates on the transmission path are different, the transient throughput of secret key distribution through the network also vary, located between an upper bound and a lower bound on the secrete key distribution rate.**

***Index Terms*—Quantum key distribution network; trusted repeater; key rate**

I. Introduction

Quantum technology era is coming as a second quantum revolution relative to the first one on quantum theory a century ago [1], e.g., China launched the first ever quantum satellite in 2016 [2], Google and Microsoft plan to bring quantum computers out of lab in 2017 [3], and Google contends that small quantum devices will be commercialized in five years [4]. It is imperative to realize that the conventional cryptography becomes frail in front of quantum computers, which operate by manipulation of qbits and can easily solve some mathematical problems that are complex for conventional computers and are the basis of conventional cryptography. While quantum computers take away the shield in conventional communication, quantum physics guarantees a new cryptography weapon, namely quantum key distribution (QKD). QKD is the first quantum technology ready for commercialization, and the generated secret keys are deemed as secure for all future as at the creation time, without putting restrictions on the adversary's resources or emerging side-channels [5].

However, QKD has two limitations that inhibit its wide spread and deployment, i.e., short operational distance and low key rate. The primary factor limiting the key rate is the detector's deadtime. Another crucial factor is channel loss. Moreover, the key rate is constrained by the security requirement [6]. Because the quantum states are fragile, the longer the quantum signals travel the easier they lose to decoherence. Consequently, the maximal distance of secure QKD decreases with increasing losses and increasing detector noise. To extend the operational distance, quantum repeater is a perfect choice to overcome the loss problem and form an effective quantum channel. Unfortunately, quantum repeaters rely on elaborated quantum operations and on quantum memories that cannot be realized with current technologies [7]. With a pay to trust, trusted repeaters relieve the impracticable requirements of quantum repeaters, are implementable with current technology, and have been deployed [8], [9].

In this paper, we consider QKD trusted repeater networks. We aim to provide a mathematical tool useful for QKD network configuration in practice. In particular, we establish a close relationship between distance and key rate at network scale and investigate the impact of network properties on the throughput of secret key distribution through the network. It is worth noting that while the secret key rate is a defining characteristic of a QKD link, i.e., it is a reflection of channel loss, detector efficiency, and security requirement at the link, the analysis of secret key distribution throughput of a QKD network requires a network perspective and different combinations of available resources may result in extremely different network performance. In practice, the implementation technology of trusted repeater implies that the transmission of secret keys in the network is store-and-forward and follows a queueing principle. Based on this, we obtain an expression of secret key distribution throughput of the network as a function of secret key rates at each link. In addition, we investigate the backlog of secrete keys at the trusted repeater.

Though trusted repeaters are relatively easier to implement than quantum repeaters, the throughput analysis of secret key distribution in an end-to-end QKD network is not trivial. We solve this problem by transforming the network into a min-plus linear system based on the min-plus convolution operation [10]. This convolution approach has been utilized for performance analysis of other types of networks, such as wireless networks [11] where the wireless channel is treated as a queueing system and latency metrics are analyzed. In the present paper, particularly, we extend the analysis to secret key rate analysis in QKD networks.

The remainder of this paper is structured as follows. In Sec. II, some basics of quantum key distribution are introduced. In particular, three new concepts of secret key rates are defined with respect to the stochastic nature of raw key rate in a time slot. In addition, the queueing principle of secret keys in the trusted repeater network is formulated, based on which some generic results for secret key throughput and backlog are derived. In Sec. III, the obtained results are applied to a

concrete protocol, where the statistical property of transient throughput is further investigated. Specifically, the impacts of different distance configurations are illustrated. In addition, backlog results are also presented and mean value analysis is discussed. Finally, the paper is concluded in Sec. IV.

II. Theory

A. Quantum Key Distribution

A generic QKD setting consists of two authorized partners, Alice and Bob, and two communication channels, a quantum channel used to share quantum signals and an authenticated classical channel used to transmit classical messages. Eve is a hypothetical adversary, tapping into the quantum channel and listening to the exchanges on the classical channel. The Heisenberg uncertainty principle ensures that any attempt to measure a quantum state changes it and the no-cloning theorem guarantees that an unknown quantum state can not be duplicated while keeping the original intact, which means that eavesdropping is thus detectable in principle and is the key idea behind QKD [12]. In other words, the quantum channel is the additional resource in QKD, without which information-theoretically secure key distribution is impossible through public communication only [13].

1) Photon Source: As light does not interact easily with matter, it's a practical choice for quantum information processing, and quantum states of light can be transmitted to distant locations basically without decoherence [13]. Optical quantum cryptography is based on the use of single-photon Fock states, which are difficult to realize experimentally, and practical implementations rely on faint laser pulses or entangled photon pairs, in which both the photon and the photon-pair number distribution obey Poisson statistics [12], [14], i.e., given the mean photon number μ, the probability of finding n photons reads

$$P(n|\mu) = \frac{\mu^n}{n!}e^{-\mu}. \tag{1}$$

Particularly, the number of photon pairs per mode is thermally distributed within the coherence time of the photons and follows a Poisson distribution for larger time windows [12], [14]. After key distillation, the security is just as good with faint laser pulses as with Fock states, and the price to pay for using such sources is a reduction of the bit rate [15].

2) Channel Loss: The dominating effect of photonic channels is loss [5], which leaks information to the eavesdropper and imposes bounds on the secret key rate and on the achievable distance. For optical fibers, losses are due to scattering processes, and the transmission efficiency is expressed as [15]

$$\eta_T = 10^{-(\alpha l + L_c)/10}, \tag{2}$$

where α dB/km is the loss coefficient, l km is the fiber length, and L_c dB is Bob's detection loss. For free space channels, the losses are geometric and atmospheric, and the transmission efficiency is as follows [5], [13]

$$\eta_T = \frac{{d_r}^2}{(d_s + Dl)^2} \times 10^{-\alpha l/10}, \tag{3}$$

where d_r m and d_s m are the aperture diameter of the receiving and sending telescopes, D mrad is the beam divergence, l km is the channel range, and α dB/km is the atmospheric attenuation factor.

3) Key Rate: In QKD, quantum signals are first exchanged and measured on the quantum channel, statistics of the data are estimated and information are communicated on the classical channel; then, uncorrelated symbols are discarded and the leftover symbols are the raw key[1]. The raw key rate is expressed as [13]

$$\overline{R}_{raw} = \nu_S \text{Prob(Bob accepts)}, \tag{4}$$

where the first factor ν_S is the repetition rate, e.g., ν_S is the repetition rate of the source of pulses in case of pulsed sources and ν_S is the average rate of Alice's detection in case of heralded photon sources; the second factor depends on the protocol and hardware, e.g., losses and detectors.

However, the gathered information by a eavesdropper for a typical error rate is too high to use the raw key directly for cryptographic purpose [15], to fulfill security requirement, the key is further distilled, and the product of the raw key rate $\overline{R}_{raw}$ and secret fraction G is defined as the secrete key rate:

$$\overline{R} = \overline{R}_{raw} G, \tag{5}$$

e.g., in case of classical information postprocessing [13],

$$G = I(A:B) - \min\left(I_{EA}, I_{EB}\right), \tag{6}$$

where $I(A:B)$ is the Alice-Bob mutual Shannon information and $I_{E\cdot}$ is Eve's maximal information about the raw key of Alice or Bob.

B. Trusted Repeater Network

A QKD trusted repeater network is a connected graph: the vertices represent nodes (trusted repeaters) and the edges represent QKD links [8]. Trusted repeaters are equipped with classical memories, messages are encrypted and decrypted hop-by-hop, one-time pad encryption and unconditionally secure authentication are performed to ensure secrecy locally, and global information-theoretic security between end nodes is obtained provided that intermediate nodes are trusted [7].

Consider a QKD path of N nodes, $N_1, \ldots, N_N$, i.e., $N-1$ hops, $H_{1,2}, \ldots, H_{N-1,N}$. On the first hop $H_{1,2}$, key materials K are generated and shared between N_1 and N_2; on the second hop $H_{2,3}$, K are decrypted and encrypted by one-time pad using key materials $K_{2,3}$ shared between N_2 and N_3; in this way, K are transported from N_1 to N_3, and this process is repeated until K are transported to the destination N_N.

We treat the secret key rate as a stochastic process and focus on its temporal behavior with three new definitions.

Definition 1. *The secret key rate in time slot t is defined as instantaneous key rate:*

$$r(t) = R_{raw}(t) G, \tag{7}$$

[1]In the literature, the key rate after sifting is also called sifted key rate, while the key rate before sifting is called raw key rate, e.g., [15].

where R_{raw} is supposed random in time slot t, and the cumulative process through time $(s,t]$ is defined as cumulative key rate:

$$R(s,t) = \sum_{\tau=s+1}^{t} r(\tau). \tag{8}$$

Denote $R(t) \equiv R(0,t)$. The time average of the cumulative key rate is defined as transient key rate:

$$\overline{R}(t) = \frac{R(t)}{t}. \tag{9}$$

We investigate two network performance metrics, throughput and backlog, particularly, the rate throughput is a basic performance metric of the QKD network and the backlog are useful for trusted repeater buffer dimensioning. Results are summarized in the following theorems.

Theorem 1 (Simple)**.** *Consider a QKD path of $N-1$ hops. The backlog at each hop is expressed as*

$$B_{i,i+1}(t) = R^*_{i-1,i}(t) - R^*_{i-1,i} \circledast R_{i,i+1}(t), \tag{10}$$

and the end-to-end throughput is expressed as

$$R_{1,N}(t) = R_{1,2} \circledast R_{2,3} \circledast \ldots \circledast R_{N-1,N}(t), \tag{11}$$

where $f \circledast g(t) = \inf_{0\leqslant s\leqslant t}\{f(s)+g(s,t)\}$ is the min-plus convolution.

Proof. The QKD link between two trusted repeaters is essentially a queueing system, with input process $r^*_{i-1,i}(t)$ and $R^*_{i-1,i}(t)$, service process $r_{i,i+1}(t)$ and $R_{i,i+1}(t)$, and output process $r^*_{i,i+1}(t)$ and $R^*_{i,i+1}(t)$, $\forall 2 \leqslant i \leqslant N$. The queueing principle is expressed through the backlog in the system, which is a reflected process of the temporal increment $X(t)$ [16], i.e.,

$$B_{i,i+1}(t+1) = \left[B_{i,i+1}(t) + X_{i,i+1}(t)\right]^+, \tag{12}$$

where $X_{i,i+1}(t) = r^*_{i-1,i}(t) - r_{i,i+1}(t)$ is the temporal increment in the system. Throughout this paper, $B_{i,i+1}(0) = 0$ is assumed, then the backlog function is expressed as

$$B_{i,i+1}(t) = \sup_{0\leqslant s\leqslant t}\left(R^*_{i-1,i}(s,t) - R_{i,i+1}(s,t)\right). \tag{13}$$

For a lossless system (trusted repeater), the output is the difference between the input and backlog, $R^*_{i,i+1}(t) = R^*_{i-1,i}(t) - B_{i,i+1}(t)$, which is further represented by [11]

$$R^*_{i,i+1}(t) = R^*_{i-1,i} \circledast R_{i,i+1}(t). \tag{14}$$

For an end-to-end QKD path, the secret key rate in the first hop $R_{1,2}(t)$ is the arrival process to the consecutive link, $R_{2,3}(t)$ is the service process for $R_{1,2}(t)$, etc., the cumulative throughput is expressed as

$$\begin{aligned} R_{1,N}(t) &= R_{1,2} \circledast R_{2,3} \circledast \ldots \circledast R_{N-1,N}(t) &(15)\\ &= \inf_{\boldsymbol{\tau}\in\mathscr{T}(t)} \sum_{i=2}^{N} R_{i-1,i}(\tau_{i-1},\tau_i), &(16)\end{aligned}$$

where $\mathscr{T}(t) = \{\boldsymbol{\tau} = (\tau_1,\ldots,\tau_N) : 0 \leqslant \tau_2 \leqslant \ldots \leqslant \tau_{N-1} \leqslant t\}$. □

For a complex network beyond line topology, the results are summarized in the following theorem, and it holds for both cyclic or acyclic routing [11].

Theorem 2 (Complex)**.** *Consider two input processes ${}^{\star}R^*_{i-1,i}(t)$ and ${}^{'}R^*_{i-1,i}(t)$, sharing one service process $R_{i,i+1}(t)$, let*

$$R^*_{i-1,i}(t) = {}^{\star}R^*_{i-1,i}(t) + {}^{'}R^*_{i-1,i}(t), \tag{17}$$

the backlog is expressed as

$$B_{i,i+1} = R^*_{i-1,i}(t) - R^*_{i-1,i}(t) \circledast R_{i,i+1}(t), \tag{18}$$

the service process ${}^{\star}R_{i,i+1}(t)$ for the input of interest ${}^{\star}R^*_{i-1,i}(t)$ is bounded by

$$R_{i,i+1}(t) \geqslant {}^{\star}R_{i,i+1}(t) \geqslant R_{i,i+1}(t) - {}^{'}R^*_{i-1,i}(t), \tag{19}$$

and the end-to-end throughput is bounded by

$$\begin{aligned} R_{1,2} \circledast R_{2,3} \circledast \ldots \circledast R_{N-1,N}(t) &\geqslant {}^{\star}R_{1,N}(t)\\ &\geqslant {}^{\star}R_{1,2} \circledast {}^{\star}R_{2,3} \circledast \ldots \circledast {}^{\star}R_{N-1,N}(t). \end{aligned} \tag{20}$$

Proof. The first inequality is intuitive. The second inequality follows the monotonicity of bivariate min-plus convolution [11], i.e., $f \circledast g \leqslant g$ if $f(t,t) = 0$ or $f \circledast g \leqslant f$ if $g(t,t) = 0$. □

Remark 1. *The queueing principle of the trusted repeater network indicates that the secret key rate of the consecutive nodes should be greater than the previous nodes', at least, greater than the secret key rate of the initial nodes, in view of network stability. It's different for lossy system.*

III. Application

A. Discrete-variable Protocol

Discrete-variable protocols use photon counting detection schemes, coding of bits can be based on any discrete quantum degree of freedom in principle, and free-space implementations and fiber-based implementations frequently use polarization and phase coding respectively [13]. The raw rate is essentially the product of the pulse rate ν, the transmission efficiency η_T, the detection efficiency η_B, and the number of photons $\mu(t)$ in a time slot t, i.e.,

$$R_{raw}(t) = pq\nu\eta_T\eta_B\mu(t), \tag{21}$$

where p is the sifting factor, e.g., $p = 1/2$ for the BB84 and the B92 protocol, and $p = 1/3$ for the six-state protocol [17]; and q ($q \leqslant 1$, typically 1 or $1/2$) is introduced in phase coding setups to account noninterfering path combinations [14].

The secret fraction formula for realistic photon signals is expressed as [15]

$$\begin{aligned} G = p_{post}p_{exp}\Bigg\{\frac{p_{exp}-S_m}{p_{exp}}\Bigg(1 - \log_2\Bigg[1 + 4e\frac{p_{exp}}{p_{exp}-S_m}\\ -4\left(e\frac{p_{exp}}{p_{exp}-S_m}\right)^2\Bigg]\Bigg) + f[e][e\log_2(e)\\ +(1-e)\log_2(1-e)]\Bigg\}, \end{aligned} \tag{22}$$

where p_{post} is the post-selection probability, p_{exp} is the probability that Bob detects a signal, S_0, S_1, and S_m are the probability that the signal contains zero, one, or more than one photon, and e is the signal error rate that is observable and $f[e]$ is the ratio of redundant bits to approach Shannon limit with error correction codes. Assume that the signal photon detection and the dark counts are independent, then [15]

$$p_{exp} = p_{exp}^{signal} + p_{exp}^{dark} - p_{exp}^{signal} p_{exp}^{dark}, \tag{23}$$

$$p_{exp}^{signal} = \sum_{i=1}^{\infty} S_i \sum_{j=1}^{i} \binom{i}{j} (\eta_B \eta_T)^j (1 - \eta_B \eta_T)^{i-j}, \tag{24}$$

$$p_{exp}^{dark} = d_B, \tag{25}$$

where d_B is the dark count, S_i is the probability that the source sends i photons, η_B is the detection efficiency, and η_T is the transmission efficiency.

For weak coherent pulse, the photon number is Poisson distributed [12]; thus, with mean μ,

$$S_m = 1 - (1+\mu)e^{-\mu}, \tag{26}$$

$$p_{exp}^{signal} = 1 - e^{-\eta_B \eta_T \mu}, \tag{27}$$

given a post-selection probability $p_{post} = 1$, the expected secret fraction G per time slot of an experiment is obtained. The cumulative key rate $R(s,t)$ also follows a Poisson distribution with mean

$$\lambda_{R(s,t)} = pq\nu\eta_T\eta_B\mu G \cdot (t-s), \tag{28}$$

and the moment generating function is expressed as

$$M_{R(s,t)}[-\theta] = e^{\lambda_{R(s,t)}\left(e^{-\theta}-1\right)}. \tag{29}$$

B. Metric analysis

We consider the simple network scenario only and results are summarized in the following corollaries.

Corollary 1 (Throughput)**.** *For weak coherent pulse, the lower bound λ_t^l and upper bound λ_t^u of the transient throughput λ_t, given a violation probability ϵ, are expressed as,*

$$\lambda_t^l = \sup_{\theta>0} \left\{ \lambda(-\theta) + \frac{\log(\epsilon) - \log\binom{t+N-2}{N-2}}{\theta t} \right\}, \tag{30}$$

$$\lambda_t^u = \inf_{\theta>0} \left\{ \lambda(\theta) - \frac{\log(\epsilon)}{\theta t} \right\}, \tag{31}$$

where $\lambda(-\theta) = \frac{\bigwedge_{2\leqslant i\leqslant N} \lambda_{i-1,i}\left(e^{-\theta}-1\right)}{-\theta}$ *and* $\lambda(\theta) = \frac{\bigvee_{2\leqslant i\leqslant N} \lambda_{i-1,i}\left(e^{\theta}-1\right)}{\theta}$*. In infinite time regime, the lower bound converges to the minimal average rate of all hops, i.e.,*

$$\lambda_{t\to\infty}^l = \bigwedge_{2\leqslant i\leqslant N} \lambda_{i-1,i}, \tag{32}$$

while the upper bound converges to the maximal average rate of all hops, i.e.,

$$\lambda_{t\to\infty}^u = \bigvee_{2\leqslant i\leqslant N} \lambda_{i-1,i}. \tag{33}$$

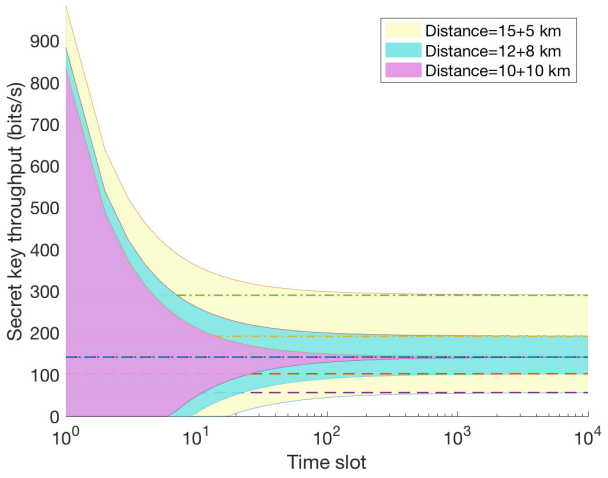

Fig. 1. Secret key throughput of a 2-hop network. The solid lines depict the analytical upper and lower bounds, the dotted lines depict the maximal and minimal means, and the shaded areas depict the upper and lower bound intervals. Distance matrix [15 5; 12 8; 10 10] km, $p = 1/2$, $q = 1$, $\nu = 10$ MHz, $\eta_B = 0.18$, $\mu = 0.1$, $\alpha = 0.2$ dB/km, $L_c = 1$ dB, $e = 0.01$, $f[e] = 1.16$, $d_B = 2 \times 10^{-4}$ /slot, $p_{post} = 1$, and $\epsilon = 0.001$. The parameter values are given in [15].

The results are illustrated in Fig. 1. It's shown that when the distance difference between different hops becomes big, the interval between the maximal and minimal mean rate becomes big, thus the jitter in the key throughput becomes big. This property also applies to the rate differences resulting from other parameters. In addition, it's shown the stochastic analysis is capable of characterizing the rate fluctuation in finite time regime before it converges to the mean interval in infinite time regime.

Lemma 1. *Consider the output process $R_{i-1,i}^*(s,t)$, $\forall (s,t]$ and $\forall \theta > 0$, the moment generating function is bounded by*

$$E\left[e^{\pm\theta R_{i-1,i}^*(s,t)}\right] \leqslant \sum_{\boldsymbol{\tau}\in\mathscr{T}(s,t)} \prod_{j=2}^{i} E\left[e^{\pm\theta R_{j-1,j}(\tau_{j-1},\tau_j)}\right], \tag{34}$$

where $\mathscr{T}(s,t) = \{\boldsymbol{\tau} = (\tau_1, \ldots, \tau_i) : s \leqslant \tau_2 \leqslant \ldots \leqslant \tau_{i-1} \leqslant t\}$.

Corollary 2 (Backlog)**.** *For weak coherent pulse, the lower bound $b_{i,i+1}^{l,t}$ and upper bound $b_{i,i+1}^{u,t}$ of backlog at each hop, given a violation probability ϵ, are expressed as*

$$b_{i,i+1}^{l,t} = \sup_{\theta>0} \frac{\log(\epsilon) - \log\left(b_l(\theta)\right)}{\theta t}, \tag{35}$$

$$b_{i,i+1}^{u,t} = \inf_{\theta>0} \frac{-\log(\epsilon) + \log\left(b_u(\theta)\right)}{\theta}, \tag{36}$$

where

$$b_l(\theta) = \binom{t+i-2}{i-2}^t e^{\sum_{s=0}^{t}(t-s)\left[\bigwedge_{2\leqslant j\leqslant i} \lambda_{j-1,j}(e^{-\theta}-1)+\lambda_{i,i+1}(e^{\theta}-1)\right]} \tag{37}$$

$$b_u(\theta) = \binom{t+i-2}{i-2} \sum_{s=0}^{t} e^{(t-s)\left[\bigvee_{2\leqslant j\leqslant i} \lambda_{j-1,j}(e^{\theta}-1)+\lambda_{i,i+1}(e^{-\theta}-1)\right]} \tag{38}$$

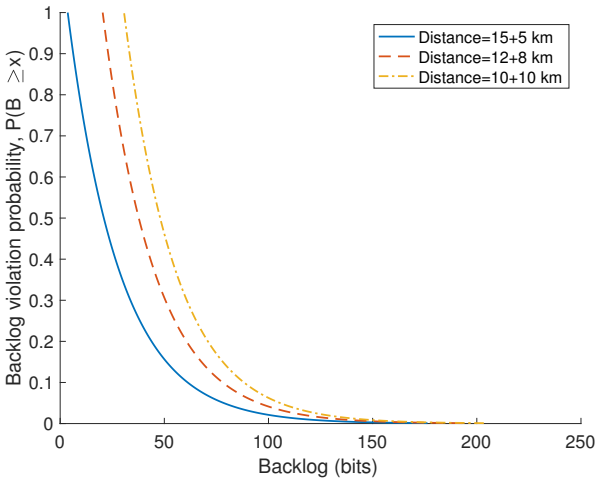

Fig. 2. Secret key backlog upper bound at the second hop of a 2-hop network. The violation probability increases with the distance decrease of the first hop. The parameter values are the same as in Fig.1.

Since the queue length is a regenerative process, the absolute backlog lower bound is 0, in this way, only the upper bound makes sense in infinite time regime. It's intuitive that the backlog increases with the incoming secret key rate. The results are illustrated in Fig. 2.

Corollary 3. *Consider mean value analysis, let* $R_{i-1,i}(t) = \lambda_{i-1,i} \cdot t$*, the throughput is expressed as*

$$R_{1,N}(t) = \bigwedge_{2 \leqslant i \leqslant N} \lambda_{i-1,i} \cdot t. \tag{39}$$

Proof. Since

$$\bigwedge_{2 \leqslant i \leqslant N} \lambda_{i-1,i} \cdot t \leqslant R_{1,N}(t) \leqslant \bigvee_{2 \leqslant i \leqslant N} \lambda_{i-1,i} \cdot t, \tag{40}$$

the proof follows directly. □

Remark 2. *The result based on deterministic analysis is a conservative lower bound, and the upper bound is obtained from stochastic analysis. It indicates that, without considering the upper bound, the configuration in practice based on deterministic analysis is pessimistic.*

IV. Conclusion

In this paper, we investigated the rate performance of secret key distribution in a QKD trusted repeater network. We derived secret key distribution throughput formulas for both a simple and a complex topology network. Considering that the secret keys in the trusted repeater network are stored and forwarded hop-by-hop, the QKD link was modeled as a queueing system and the queueing principle was represented by the accumulation process of the keys at the repeaters. Based on this, the throughput was specifically expressed as a min-plus convolution of secret key rates at each link. In addition, an expression of backlog at each link was also obtained. We applied the obtained results to a discrete-variable protocol with weak coherent pulse sources, for which, more concrete formulas of throughput and backlog were derived, where realistic system parameters were integrated into the analytical framework, e.g., photon number, channel loss, and detector efficiency. We showed that, if the secret key rates at each link are not equal, the secret key throughput may have fluctuation even at steady state, and the approach to reduce the fluctuation is to reduce the difference of individual secret key rates. Applications to other protocols are our future work.

Appendix A
Proof of Corollary 1

Proof. Recall the definition of transient throughput,

$$\lambda_t = \frac{R_{1,N}(t)}{t}. \tag{41}$$

The lower bound of the transient throughput is expressed as [11]

$$\begin{aligned} & P\left\{R_{1,N}(t) \leqslant \lambda_t^l \cdot t\right\} && (42)\\ & \leqslant \sum_{\boldsymbol{\tau} \in \mathscr{T}(t)} e^{\sum_{i=2}^{N} (\tau_i - \tau_{i-1}) \lambda_{i-1,i} \left(e^{-\theta} - 1\right)} \cdot e^{\theta \lambda_t^l t} && (43)\\ & \leqslant \binom{t+N-2}{N-2} e^{\bigwedge_{2 \leqslant i \leqslant N} \lambda_{i-1,i} \left(e^{-\theta} - 1\right) t} \cdot e^{\theta \lambda_t^l t} && (44)\\ & = \binom{t+N-2}{N-2} e^{-\theta(\lambda(-\theta) - \lambda_t^l)t}. && (45) \end{aligned}$$

The upper bound of the transient throughput is expressed as [11]

$$\begin{aligned} & P\left\{R_{1,N}(t) \geqslant \lambda_t^u \cdot t\right\} && (46)\\ & \leqslant \inf_{\boldsymbol{\tau} \in \mathscr{T}(t)} e^{\sum_{i=2}^{N} (\tau_i - \tau_{i-1}) \lambda_{i-1,i} \left(e^{\theta} - 1\right)} \cdot e^{-\theta \lambda_t^u t} && (47)\\ & \leqslant e^{\bigvee_{2 \leqslant i \leqslant N} \lambda_{i-1,i} \left(e^{\theta} - 1\right) t} \cdot e^{-\theta \lambda_t^u t} && (48)\\ & = e^{-\theta(\lambda(\theta) + \lambda_t^u)t}. && (49) \end{aligned}$$

Observe $\lim_{n \to \infty} \frac{\log \binom{n}{k}}{n} = 0$, the lower and upper bounds, in infinite time regime, are expressed as

$$\begin{aligned} \lambda_{t \to \infty}^l &= \sup_{\theta > 0} \lambda(-\theta), && (50)\\ \lambda_{t \to \infty}^u &= \inf_{\theta > 0} \lambda(\theta). && (51) \end{aligned}$$

Considering the monotonicity of $\lambda(-\theta)$ and $\lambda(\theta)$, the derivatives are respectively

$$\begin{aligned} \frac{\partial}{\partial \theta} \lambda(-\theta) &= \frac{\widehat{\lambda} e^{-\theta}(\theta + 1) - \widehat{\lambda}}{\theta^2}, && (52)\\ \frac{\partial}{\partial \theta} \lambda(\theta) &= \frac{\breve{\lambda} e^{\theta}(\theta - 1) + \breve{\lambda}}{\theta^2}, && (53) \end{aligned}$$

letting $\frac{\partial}{\partial \theta} \lambda(-\theta) = 0$ and $\frac{\partial}{\partial \theta} \lambda(\theta) = 0$, we obtain

$$\begin{aligned} \lambda_{t \to \infty}^l &= \lim_{\theta \to 0} \lambda(-\theta) = \widehat{\lambda}, && (54)\\ \lambda_{t \to \infty}^u &= \lim_{\theta \to 0} \lambda(\theta) = \breve{\lambda}, && (55) \end{aligned}$$

where $\widehat{\lambda} = \bigwedge_{2 \leqslant i \leqslant N} \lambda_{i-1,i}$ and $\breve{\lambda} = \bigvee_{2 \leqslant i \leqslant N} \lambda_{i-1,i}$. □

APPENDIX B
PROOF OF LEMMA 1

Proof. Let $\mathscr{T}(s,t) = \{\boldsymbol{\tau} = (\tau_1, \ldots, \tau_i) : s \leqslant \tau_2 \leqslant \ldots \leqslant \tau_{i-1} \leqslant t\}$, consider the output process $R^*_{i-1,i}(s,t)$, $\forall (s,t]$ and $\forall \theta > 0$,

$$E\left[e^{\theta R^*_{i-1,i}(s,t)}\right] = E\left[e^{\theta \inf\limits_{\boldsymbol{\tau}\in\mathscr{T}(s,t)} \sum_{j=2}^{i} R_{j-1,j}(\tau_{j-1},\tau_j)}\right] \quad (56)$$

$$\leqslant E\left[\sup_{\boldsymbol{\tau}\in\mathscr{T}(s,t)} e^{\theta \sum_{j=2}^{i} R_{j-1,j}(\tau_{j-1},\tau_j)}\right] \quad (57)$$

$$\leqslant \sum_{\boldsymbol{\tau}\in\mathscr{T}(s,t)} E\left[e^{\theta \sum_{j=2}^{i} R_{j-1,j}(\tau_{j-1},\tau_j)}\right] \quad (58)$$

$$= \sum_{\boldsymbol{\tau}\in\mathscr{T}(s,t)} \prod_{j=2}^{i} E\left[e^{\theta R_{j-1,j}(\tau_{j-1},\tau_j)}\right], \quad (59)$$

$$E\left[e^{-\theta R^*_{i-1,i}(s,t)}\right] = E\left[e^{-\theta \inf\limits_{\boldsymbol{\tau}\in\mathscr{T}(s,t)} \sum_{j=2}^{i} R_{j-1,j}(\tau_{j-1},\tau_j)}\right] \quad (60)$$

$$= E\left[\sup_{\boldsymbol{\tau}\in\mathscr{T}(s,t)} e^{-\theta \sum_{j=2}^{i} R_{j-1,j}(\tau_{j-1},\tau_j)}\right] \quad (61)$$

$$\leqslant \sum_{\boldsymbol{\tau}\in\mathscr{T}(s,t)} E\left[e^{-\theta \sum_{j=2}^{i} R_{j-1,j}(\tau_{j-1},\tau_j)}\right] \quad (62)$$

$$= \sum_{\boldsymbol{\tau}\in\mathscr{T}(s,t)} \prod_{j=2}^{i} E\left[e^{-\theta R_{j-1,j}(\tau_{j-1},\tau_j)}\right]. \quad (63)$$

□

APPENDIX C
PROOF OF COROLLARY 2

Proof. Recall the backlog is expressed as

$$B_{i,i+1}(t) = \sup_{0\leqslant s\leqslant t} \left(R^*_{i-1,i}(s,t) - R_{i,i+1}(s,t)\right). \quad (64)$$

The lower bound is expressed as

$$P\left\{B_{i,i+1}(t) \leqslant x\right\}$$

$$= \prod_{s=0}^{t} P\left\{R^*_{i-1,i}(s,t) - R_{i,i+1}(s,t) \leqslant x\right\} \quad (65)$$

$$\leqslant \prod_{s=0}^{t} \left\{E\left[e^{-\theta\left(R^*_{i-1,i}(s,t) - R_{i,i+1}(s,t)\right)}\right] \cdot e^{\theta x}\right\} \quad (66)$$

$$\leqslant \prod_{s=0}^{t} \left\{ \sum_{\boldsymbol{\tau}\in\mathscr{T}(s,t)} \prod_{j=2}^{i} E\left[e^{-\theta R_{j-1,j}(\tau_{j-1},\tau_j)}\right] \cdot E\left[e^{\theta R_{i,i+1}(s,t)}\right] \cdot e^{\theta x}\right\} \quad (67)$$

$$\leqslant \prod_{s=0}^{t} \left\{ \binom{t+i-2}{i-2} e^{\bigwedge\limits_{2\leqslant j\leqslant i} \lambda_{j-1,j}(t-s)(e^{-\theta}-1)} \cdot e^{\lambda_{i,i+1}(t-s)(e^{\theta}-1)} \cdot e^{\theta x}\right\}, \quad (68)$$

where the first inequality follows Chernoff bound, and the last two inequalities follows Lemma 1.

The upper bound is expressed as

$$P\left\{B_{i,i+1}(t) \geqslant x\right\}$$

$$\leqslant \sum_{s=0}^{t} P\left\{R^*_{i-1,i}(s,t) - R_{i,i+1}(s,t) \geqslant x\right\} \quad (69)$$

$$\leqslant \sum_{s=0}^{t} E\left[e^{\theta\left(R^*_{i-1,i}(s,t) - R_{i,i+1}(s,t)\right)}\right] \cdot e^{-\theta x} \quad (70)$$

$$\leqslant \sum_{s=0}^{t} \sum_{\boldsymbol{\tau}\in\mathscr{T}(s,t)} \prod_{j=2}^{i} E\left[e^{\theta R_{j-1,j}(\tau_{j-1},\tau_j)}\right] \cdot E\left[e^{-\theta R_{i,i+1}(s,t)}\right] \cdot e^{-\theta x} \quad (71)$$

$$\leqslant \sum_{s=0}^{t} \binom{t+i-2}{i-2} e^{\bigvee\limits_{2\leqslant j\leqslant i} \lambda_{j-1,j}(t-s)(e^{\theta}-1)} \cdot e^{\lambda_{i,i+1}(t-s)(e^{-\theta}-1)} \cdot e^{-\theta x}, \quad (72)$$

where the first step follows union bound, the second step follows Chernoff bound, and the last two steps follow Lemma 1. □

REFERENCES

[1] T. Aymard de, M. Charles, H. Freeke, C. Ignacio, M. Richard, and C. Tommaso, "Quantum manifesto: a new era of technology," *Quantum Information Processing and Communication in Europe*, 2016.

[2] A. Abbott, D. Butler, D. Castelvecchi, D. Cressey, E. Gibney, H. Ledford, J. J. Lee, L. Morello, S. Reardon, J. Tollefson *et al.*, "2016 in news: The science events that shaped the year," *Nature*, vol. 540, no. 7634, pp. 496–499, 2016.

[3] C. Davide, "Quantum computers ready to leap out of the lab in 2017," *Nature*, vol. 7635, no. 541, pp. 9–10, 2017.

[4] M. Masoud, R. Peter, N. Hartmut, B. Sergio, D. Vasil, B. Ryan, F. Austin, S. Vadim, and M. John, "Commercialize quantum technologies in five years," *Nature*, vol. 543, no. 7644, pp. 171–174, 2017.

[5] N. Lütkenhaus, "Quantum key distribution," in *Quantum Information and Coherence*. Springer International Publishing, 2014, pp. 107–146.

[6] M. Dušek, N. Lütkenhaus, and M. Hendrych, "Quantum cryptography," *Progress in Optics*, vol. 49, pp. 381–454, 2006.

[7] R. Alléaume, C. Branciard, J. Bouda, T. Debuisschert, M. Dianati, N. Gisin, M. Godfrey, P. Grangier, T. Länger, N. Lütkenhaus *et al.*, "Using quantum key distribution for cryptographic purposes: a survey," *Theoretical Computer Science*, vol. 560, pp. 62–81, 2014.

[8] M. Peev, C. Pacher, R. Alléaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, J. Dynes *et al.*, "The secoqc quantum key distribution network in vienna," *New Journal of Physics*, vol. 11, no. 7, p. 075001, 2009.

[9] L. Salvail, M. Peev, E. Diamanti, R. Alléaume, N. Lütkenhaus, and T. Länger, "Security of trusted repeater quantum key distribution networks," *Journal of Computer Security*, vol. 18, no. 1, pp. 61–87, 2010.

[10] F. Baccelli, G. Cohen, G. J. Olsder, and J.-P. Quadrat, "Synchronization and linearity: an algebra for discrete event systems," 1992.

[11] F. Sun and Y. Jiang, "Towards a calculus for wireless networks," *arXiv preprint arXiv:1705.03714*, 2017.

[12] D. F. Walls and G. J. Milburn, *Quantum optics*. Springer Science & Business Media, 2007.

[13] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," *Reviews of modern physics*, vol. 81, no. 3, p. 1301, 2009.

[14] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Reviews of modern physics*, vol. 74, no. 1, p. 145, 2002.

[15] N. Lütkenhaus, "Security against individual attacks for realistic quantum key distribution," *Physical Review A*, vol. 61, no. 5, p. 052304, 2000.

[16] S. Asmussen, *Applied Probability and Queues*. Springer Science & Business Media, 2003, vol. 51.

[17] D. Bruß and N. Lütkenhaus, "Quantum key distribution: from principles to practicalities," *Applicable Algebra in Engineering, Communication and Computing*, vol. 10, no. 4, pp. 383–399, 2000.