Supplementary Information: Quantum key distribution in a packet-switched network

Reem Mandil,[1,2,*] Stephen DiAdamo,[3,†] Bing Qi,[1,‡] and Alireza Shabani[1]

[1]*Cisco Quantum Lab, Los Angeles, California, USA*
[2]*University of Toronto, Toronto, Canada*
[3]*Cisco Quantum Lab, Garching bei München, Germany*

(Dated: August 24, 2023)

I. SUPPLEMENTARY METHODS

Here we explain how the secure key rate is calculated and describe the optimization process. We follow the notation of Ref. [1]. After completing the protocol described in Results section of the main text, Alice and Bob may distill a secure key of length

$$\ell = \left\lfloor s_{X,0} + s_{X,1} - s_{X,1}h(\phi_X) - n_X f_{EC} h(e_{obs}) - 6\log_2\frac{21}{\varepsilon_{sec}} - \log_2\frac{2}{\varepsilon_{cor}} \right\rfloor. \tag{1}$$

Here, $s_{X,0}$ and $s_{X,1}$ are the lower bounds on the number of bits generated from zero- and single-photon pulses, respectively. The term $s_{X,1}h(\phi_X)$ is the number of bits consumed during privacy amplification, where ϕ_X is the upper bound on the phase error rate associated with the single-photon events and $h(x) \coloneqq -x\log_2 x - (1-x)\log_2(1-x)$ is the binary entropy function. The term $n_X f_{EC} h(e_{obs})$ describes the bits consumed by the classical error correction algorithm [2] with efficiency f_{EC}, where n_X is the number of detection events in basis X. The post-processing stage ensures that Alice's and Bob's keys are identical expect with small probability ε_{cor} and secret except with small probability ε_{sec}. Supplementary Table 1 summarizes the parameter values used in the key rate analysis.

Supplementary Table 1. Key rate analysis parameters.

Parameter	**Value**
f_{EC}	1.16
ε_{cor}	10^{-15}
ε_{sec}	10^{-10}
p_{dc}	2×10^{-7}
η_{Bob}	0.15
e_{mis}	0.005
μ_3	0.0002

Next, we show how to estimate $s_{X,0}$, $s_{X,1}$, and ϕ_X. The number of zero-photon events satisfies [1]

$$s_{X,0} \geqslant \tau_0 \frac{\mu_2 n^-_{X,\mu_3} - \mu_3 n^+_{X,\mu_2}}{\mu_2 - \mu_3}, \tag{2}$$

where $\tau_n \coloneqq \sum_{k\in\mathcal{K}} e^{-k}k^n p_k/n!$ is the probability that Alice sends a n-photon state, and

$$n^{\pm}_{X,k} \coloneqq \frac{e^k}{p_k}\left[n_{X,k} \pm \sqrt{\frac{n_X}{2}\ln\frac{21}{\varepsilon_{sec}}}\right] \tag{3}$$

is the number of detection events in basis X for pulses of intensity k when considering the finite sample size. Here, $n_X = \sum_{k\in\mathcal{K}} n_{X,k}$. The detection numbers are given by

$$n_{X,k} = N q_x^2 p_k (1-(1-2p_{dc})e^{-\eta_{tot}\eta_{Bob}k}), \tag{4}$$

* reem.mandil@mail.utoronto.ca
† sdiadamo@cisco.com
‡ bingq@cisco.com

where $\eta_{tot} = 10^{(-0.2L-\sum_i loss_r^i)/10}$ denotes the overall transmittance of the channel including the fiber links of distance L (km) and the routers between Alice and Bob. Pulses belonging to different frames will have a different η_{tot}, so we take $\eta_{tot} \to \langle \eta_{tot} \rangle$ by averaging over all frames contributing to the key. Bob uses an active measurement setup with two single-photon detectors (InGaAs APDs) each with a dark count probability p_{dc}. The overall efficiency of Bob's measurement is given by η_{Bob}.

The number of single-photon events satisfies

$$s_{X,1} \geqslant \frac{\tau_1 \mu_1 [n^-_{X,\mu_2} - n^+_{X,\mu_3} - \frac{\mu_2^2-\mu_3^2}{\mu_1^2}(n^+_{X,\mu_1} - \frac{s_{X,0}}{\tau_0})]}{\mu_1(\mu_2-\mu_3) - \mu_2^2 + \mu_3^2}. \tag{5}$$

The number of zero- and single-photon events in basis Z, $s_{Z,0}$ and $s_{Z,1}$, respectively, may be calculated using the same expressions by replacing $X \to Z$.

The phase error rate of the single-photon events in basis X is estimated as

$$\phi_X \leqslant \frac{v_{Z,1}}{s_{Z,1}} + \gamma\Big(\varepsilon_{sec}, \frac{v_{Z,1}}{s_{Z,1}}, s_{Z,1}, s_{X,1}\Big), \tag{6}$$

where $\gamma(\cdot)$ is the estimation uncertainty given by

$$\gamma(a,b,c,d) \coloneqq \sqrt{\frac{(c+d)(1-b)b}{cd\log 2}\log_2\Big(\frac{c+d}{cd(1-b)b}\frac{21^2}{a^2}\Big)} \tag{7}$$

and $v_{Z,1}$ is the number of bit errors in the single-photon events in basis Z estimated as

$$v_{Z,1} \leqslant \tau_1 \frac{m^+_{Z,\mu_2} - m^-_{Z,\mu_3}}{\mu_2 - \mu_3}. \tag{8}$$

Here, $m^{\pm}_{Z,k}$ is the number of bit errors in basis Z for pulses of intensity k when considering the finite sample size and is given by

$$m^{\pm}_{Z,k} \coloneqq \frac{e^k}{p_k}\left[m_{Z,k} \pm \sqrt{\frac{m_Z}{2}\ln\frac{21}{\varepsilon_{sec}}}\right], \tag{9}$$

where $m_Z = \sum_{k\in\mathcal{K}} m_{Z,k}$ is the number of bit errors in basis Z. The error numbers are given by

$$m_{Z,k} = N(1-q_x)^2 p_k (p_{dc} + e_{mis}(1 - e^{-\eta_{tot}k})), \tag{10}$$

where e_{mis} is the error rate due to optical misalignment.

Finally, the bit error rate in basis X is calculated as

$$e_{obs} = \frac{m_X}{n_X}, \tag{11}$$

where m_X is the number of bit errors in basis X, calculated analogously to m_Z.

The numerical optimization returns the parameters $\{q_x, p_{\mu_1}, p_{\mu_2}, \mu_1, \mu_2\}$ that maximize the secure key rate $R \coloneqq \ell/N$ for a given number, N, of pulses that are routed to Bob (i.e., N is the difference between the number of sent pulses, N_0, and the number of pulses discarded in the routing process). The decoy intensities satisfy $\mu_1 > \mu_2 + \mu_3$ and $\mu_2 > \mu_3 \geqslant 0$. We fix the vacuum decoy state to be $\mu_3 = 0.0002$. We scale R by N/N_0 to obtain the secure key rate in bits per sent pulse (see Supplementary Note 2 for these results). The results in the main text are further scaled by $(1 - T_g^0/T_f^0)R_t$, where $R_t = 1$ GHz, to show the secure key rate in bits per second.

II. SUPPLEMENTARY NOTE 1

Here we discuss and compare the effects of using storage versus no storage in a network routing protocol. Supplementary Fig. 1 depicts the photon losses experienced by a payload in a router implementing these two types of strategies. We may describe the transmittance of a fiber delay line in a storage routing protocol as

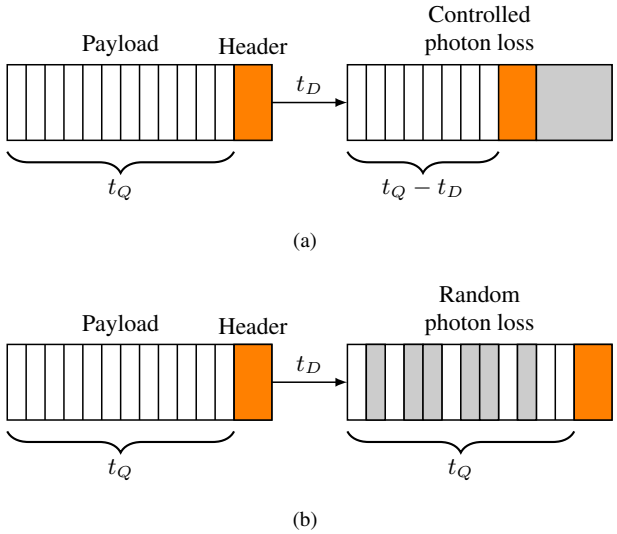
$$\eta_s = 10^{-\alpha_s t_D v_g/10}, \tag{12}$$

where $t_D = d_{proc} + d_{queue}$. Thus, the number of transmitted pulses in a quantum payload of duration t_Q in a storage routing protocol is given by $\eta_s R_t t_Q$. Similarly, the number of transmitted pulses in the no storage routing protocol is given by $R_t(t_Q - t_D)$.

Let us assume that equal proportions of random and controlled photon loss have the same effect on the key rate (valid so long as the detector noise is low compared to the signal). Then we expect a storage routing protocol to be favorable in the case where

$$\eta_s t_Q > t_Q - t_D. \tag{13}$$

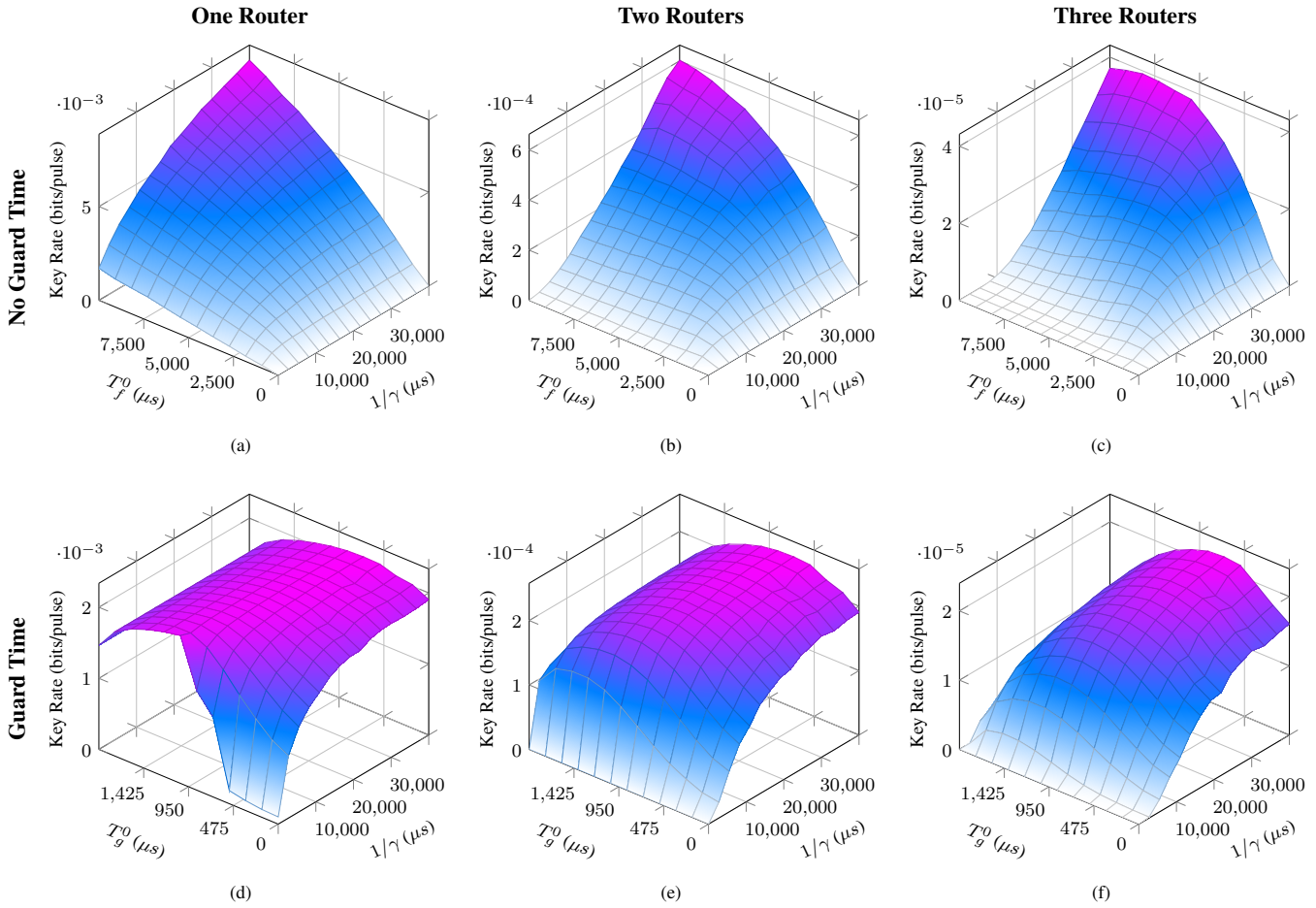
Note that this comparison assumes the same network delays in each type of routing protocol. However, the no storage routing protocol introduces smaller d_{trans} since frames will shrink by t_D at each router they encounter. This effect leads to smaller d_{queue} in the no storage routing protocol. The use of guard time in the storage routing protocol will also introduce smaller d_{trans}, however it is reduced by at most T_g.



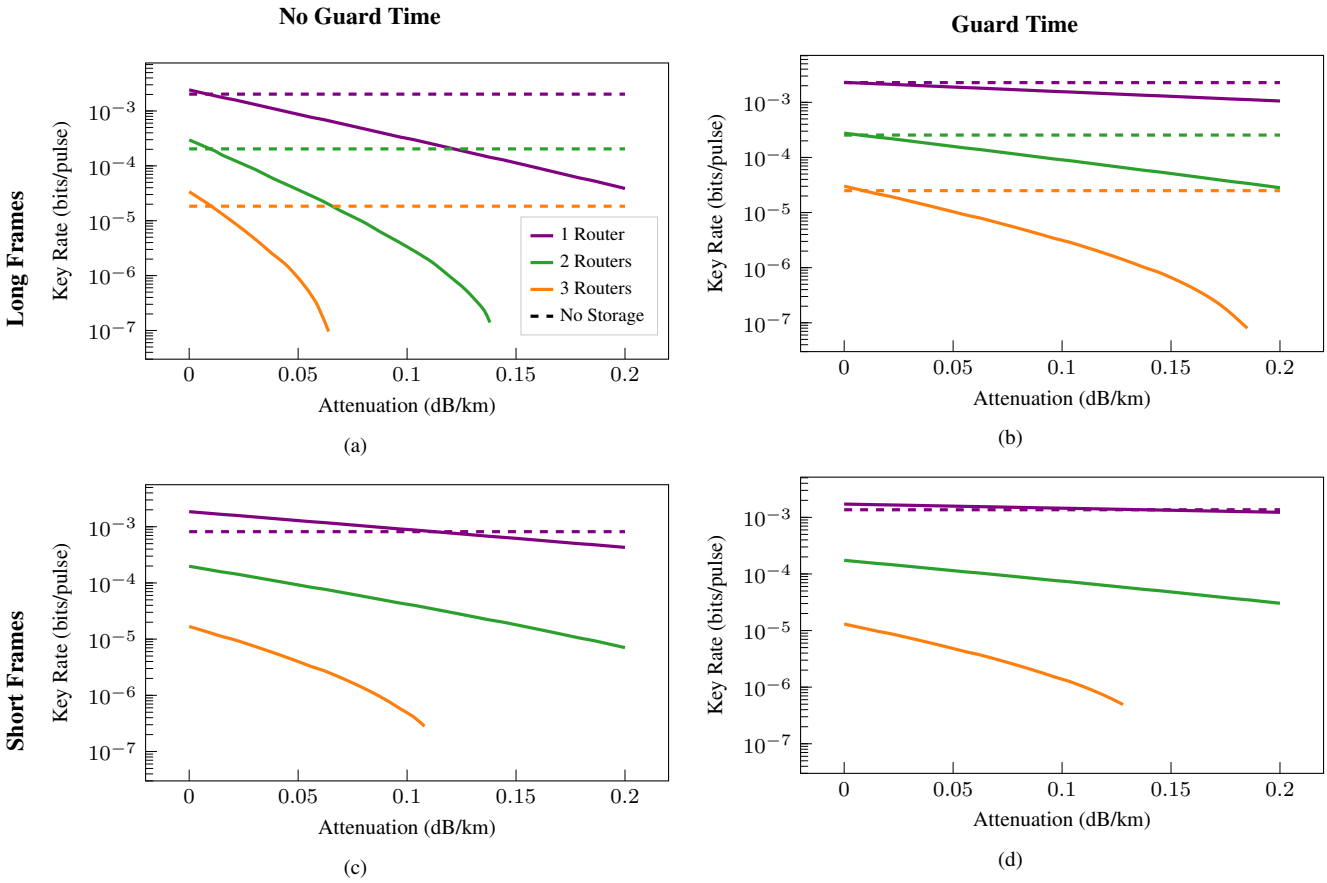
Supplementary Figure 1. **Effect on quantum payload during storage vs. no storage.** Schematic of a hybrid frame before and after passing a router in a packet-switched network. The duration of the quantum payload is denoted by t_Q. The delay time, t_D, is given by $d_{proc} + d_{queue}$. (a) No storage. (b) Storage.

III. SUPPLEMENTARY NOTE 2

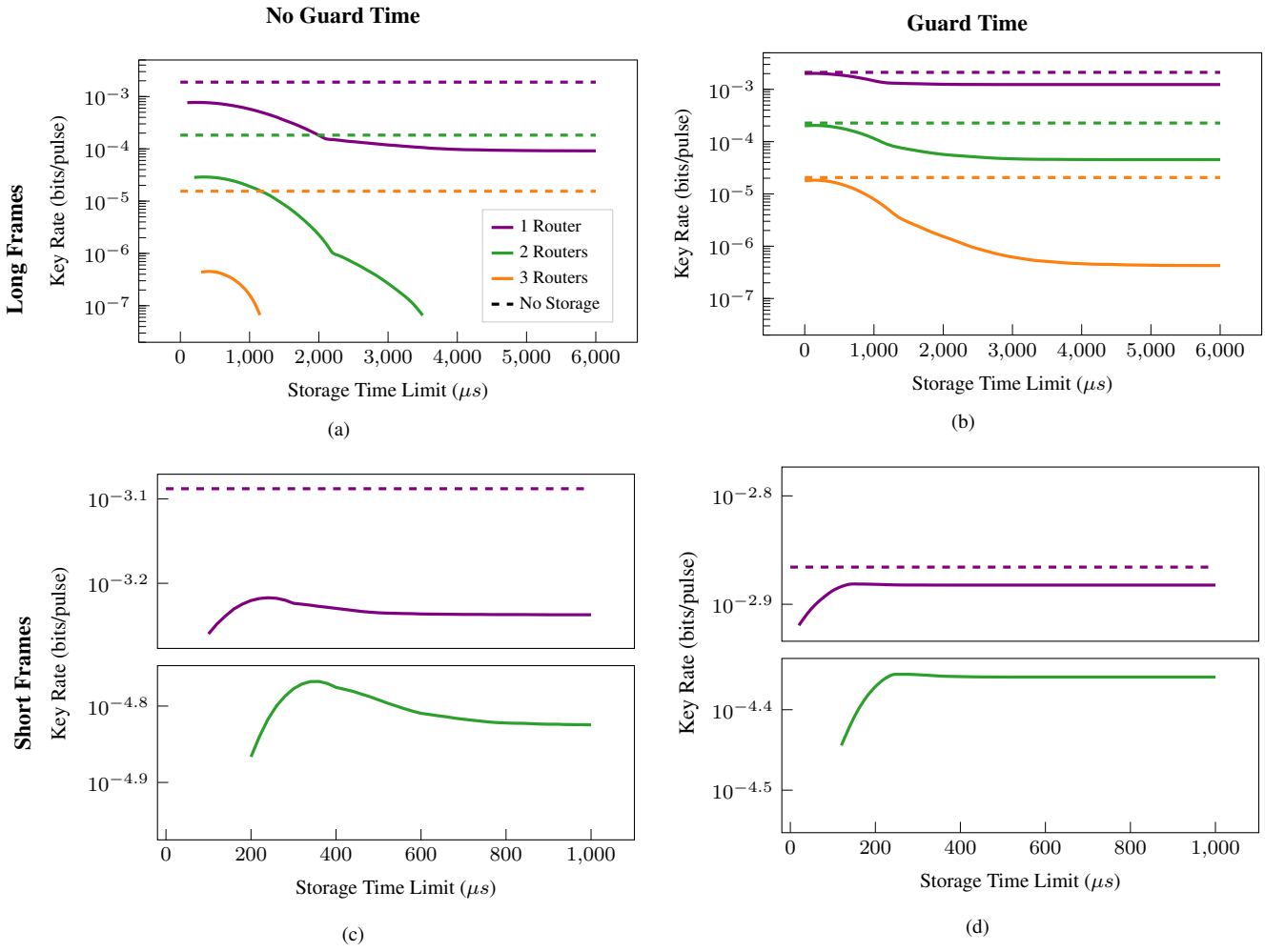
Here we present the simulated key rates in bits per pulse sent by Alice. Supplementary Figs. 2-5 exhibit the same general trends as their analogous plots in the main text.



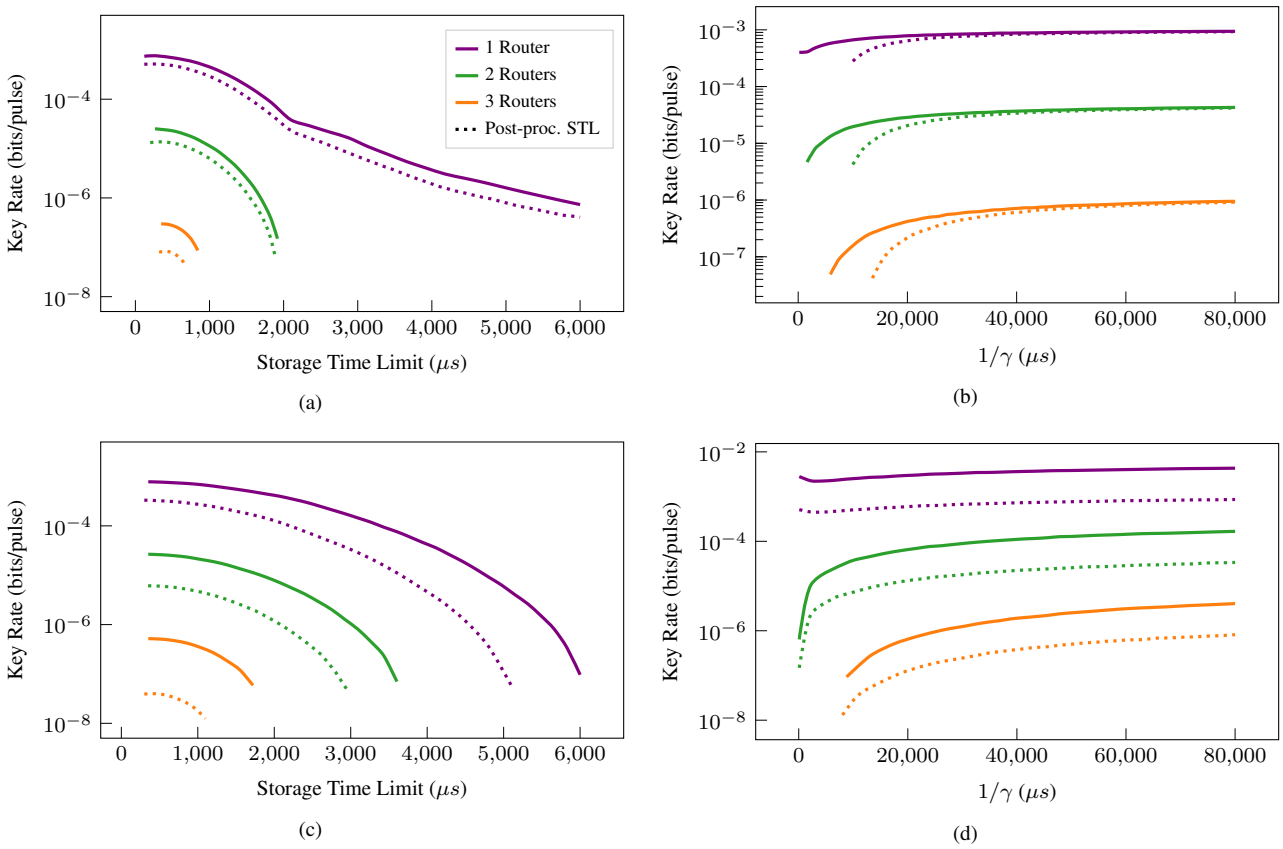
Supplementary Figure 2. **Secure key rates (bits per pulse) in a network with no storage during delays.** A total of 18,750 frames are generated by Alice in each user pair. The finite-size is $N \approx 10^{12}$. In plots (a)-(c), we fix the guard time to be zero and vary the initial frame length and average frame inter-arrival time, $1/\gamma$. In plots (d)-(f), we fix the initial frame length to 2,000 μs and vary the initial guard time and $1/\gamma$. Columns (left to right) are for user pairs A_{31} and B_{32}, A_{42} and B_{22}, and A_{22} and B_{31}. Color map changes from white to purple as the key rate increases.



Supplementary Figure 3. **Secure key rates (bits per pulse) in a network with storage during delays (unlimited).** In each plot, we fix the network parameters and vary the attenuation of the fiber storage lines. A total of 37,500 frames are generated by Alice in each user pair. The finite data size is $N \approx 10^{12}$. Unless displayed, the no storage routing protocol fails to produce a secure key. (a) $T_g^0 = 0$, $1/\gamma = 30,000\ \mu s$, $T_f^0 = 2,000\ \mu s$. (b) $T_g^0 = 800\ \mu s$, $1/\gamma = 30,000\ \mu s$, $T_f^0 = 2,000\ \mu s$. (c) $T_g^0 = 0$, $1/\gamma = 3,000\ \mu s$, $T_f^0 = 200\ \mu s$. (d) $T_g^0 = 80\ \mu s$, $1/\gamma = 3,000\ \mu s$, $T_f^0 = 200\ \mu s$.



Supplementary Figure 4. **Secure key rates (bits per pulse) in a network with storage during delays (unlimited) and STL implemented in post-processing.** In each plot, we fix the network parameters and vary the STL duration. The attenuation of the fiber storage lines is fixed at 0.16 dB/km. The network parameters are identical to Fig. 3.



Supplementary Figure 5. **Secure key rates (bits per pulse) in a network with storage during delays (limited).** The attenuation of the fiber storage lines is fixed at 0.16 dB/km. A total of 37,500 frames are generated by Alice in each user pair. $T_g^0 = 0$. (a) $1/\gamma = 15,000\ \mu s$, $T_f^0 = 2,000\ \mu s$. (b) STL $= 320\ \mu s$, $T_f^0 = 2,000\ \mu s$. (c) $1/\gamma = 50,000\ \mu s$, $T_f^0 = 10,000\ \mu s$. (d) STL $= 550\ \mu s$, $T_f^0 = 10,000\ \mu s$.

[1] Charles Ci Wen Lim, Marcos Curty, Nino Walenta, Feihu Xu, and Hugo Zbinden. Concise security bounds for practical decoy-state quantum key distribution Phys. Rev. A, 89:022307, 2014.

[2] Gilles Brassard and Louis Salvail. Secret-Key Reconciliation by Public Discussion. In Tor Helleseth, editor, Advances in Cryptology — EUROCRYPT '93, pages 410–423, Berlin, Heidelberg, 1994. Springer Berlin Heidelberg.