Supplementary Document for Optimised Multithreaded CV-QKD Reconciliation for Global Quantum Networks

Xiaoyu Ai and Robert Malaney
School of Electrical Engineering & Telecommunications,
University of New South Wales, Sydney, NSW 2052, Australia.

I. Analysing the Computational Complexity of SR

In this section, we elaborate on the analysis of the computational complexity of SR.

An LDPC matrix with block length N_R can be defined by the symbol and check node degree distribution polynomials, $\lambda(x) = \sum_{a=2}^{\Lambda} \lambda_a x^{a-1}$ and $\rho(x) = \sum_{b=2}^{P} \rho_b x^{b-1}$. Here, Λ and P are the highest degrees in $\lambda(x)$ and $\rho(x)$, respectively. We denote the total number of non-zero entries in an LDPC matrix as G, and adopt the well-known Belief Propagation (BP) decoder [1] for error correction. We define the total number of arithmetic operations of SR as $\sum_{j=0}^{m-1} E_j D_j$, where, for each $\mathbf{S_j}$, E_j is the number of arithmetic operations executed within a decoding iteration,[1] and D_j is the number of decoding iterations [2]. We note, in our GPU-based SR, E_j and D_j are different for the m slices of each block since m LDPC matrices are used to reconcile the m slices. For a channel with constant T and ξ, D_j is dependent on a target ϵ_{EC}, and on the polynomials $\lambda(x)$ and $\rho(x)$. Note, for N_R larger than approximately 10^5, D_j is independent of N_R (a result we will adopt later). Assuming the Gaussian approximation within the Density Evolution Algorithm, D_j is given by

$$D_j = \arg\min_{k} \{q_k = f(\gamma, k, \lambda(x), \rho(x)) \leq \epsilon_{EC}, k \in \mathbb{Z}^*\}\,, \tag{1}$$

where q_k is the BER after the k^{th} decoding iteration and given by [3]

$$q_k = f(\gamma, k, \lambda(x), \rho(x)) = \sum_{b=2}^{P} \rho_b \phi^{-1}\left(1 - L^{b-1}\right)\,. \tag{2}$$

Here, $L = 1 - \sum_{a=2}^{\Lambda} \lambda_a \phi\left(\log\gamma + (a-1)\, q_{k-1}\right)$, where $q_0 = 0$, and $\phi(v)$ is given by

$$\phi(v) = \begin{cases} 1 - \frac{1}{\sqrt{4\pi v}} \int_{-\infty}^{+\infty} \tanh\left(\frac{u}{2}\right) e^{-\frac{(u-v)^2}{4v}} du & v > 0 \\ 1 & v = 0\,. \end{cases} \tag{3}$$

Finding a closed solution to Eq. 2 is problematic due to the $\phi^{-1}(w)$ term (here $w = \phi(v)$). To make progress, the following approximation for Eq. 3 is used [3]

$$\phi(v) \approx \begin{cases} e^{-0.4527 v^{0.86} + 0.0218} & v > 0 \\ 1 & v = 0\,. \end{cases} \tag{4}$$

[1] In a BP decoder, a decoding iteration is one pass through the decoding algorithm.

We then find $\phi^{-1}(w)$ is given by

$$\phi^{-1}(w) \approx \begin{cases} \left(\frac{\log w - 0.0218}{-0.4527}\right)^{1.1628} & 0 < w < 1 \\ 0 & w = 1\,. \end{cases} \tag{5}$$

With this all in place, it is now possible to solve for D_j as given by Eq. 1.

Now we focus on the determination of E_j. When messages are propagated from the variable nodes to the check nodes, there are $2G$ multiplications and G additions [4]. When messages are propagating back to the variable nodes, there are $4G$ operations required ($2G$ multiplications and $2G$ additions) [4]. Therefore, E_j is obtained by [2], [4]

$$E_j = 7G = 7N_R\left(\frac{\sum_{b=2}^{P} \frac{\rho_b}{b}}{\sum_{a=2}^{\Lambda} \frac{\lambda_a}{a}}\right)\left(\sum_{b=2}^{P} b\rho_b\right)\,. \tag{6}$$

The decoding time of the whole reconciliation process, Δt, is given by

$$\Delta t = c_h \sum_{j=0}^{m-1} E_j D_j\,, \tag{7}$$

where c_h is a hardware-dependent constant representing the average time taken to complete an arithmetic operation. Clearly, by dividing N values into multiple blocks with length N_R and decoding these blocks simultaneously, Alice and Bob can reduce the decoding time by a factor of $N_d = \frac{N}{N_R}$.

II. The Estimation of T and ξ_{ch} Using a Finite Number of Quantum Signals

In this supplementary document, we elaborate on the estimation of channel parameters, T and ξ_{ch}, from N_e quantum signals and determination of the upper bound of $S_{BE}^{\epsilon_{PE}}$ based on the estimated T and ξ_{ch} for a given N. Here, we closely follow the methodology in [5] (and references therein).

The parameter estimation at Step 4 of our protocol is a two-step process. Firstly, Alice and Bob estimate each coefficient in the covariance matrix between the shared states based on N_e (randomly selected) quantum signals sent from Bob. Then, Alice uses these estimated coefficients to determine T and ξ_{ch}. In the asymptotic regime, the estimation of T and ξ_{ch} is exact since Alice and Bob use an infinite number of quantum signals.

The following the two functions will be useful,

$$F_1(v_1, v_2) = \sqrt{\frac{v_1+\sqrt{v_1^2-4v_2}}{2}}\,, \tag{8}$$

$$F_2(v_1, v_2) = \sqrt{\frac{v_1-\sqrt{v_1^2-4v_2}}{2}}\,. \tag{9}$$

Alice can determine the Holevo Information between Bob and Eve's states χ_{EB} via [6]–[8]

$$\chi_{EB} = \chi_E - \chi_{E|B}\,, \tag{10}$$

where χ_E is Eve's von Neumann Entropy before Bob makes his heterodyne detection and $\chi_{E|B}$ is Eve's von Neumann Entropy after his detection. The term χ_E is given by

$$\chi_E = Z\left(\frac{\psi_1 - 1}{2}\right) + Z\left(\frac{\psi_2 - 1}{2}\right)\,, \tag{11}$$

where

$$Z(z) = (z+1)\log(z+1) - z\log z\,. \tag{12}$$

We define that $\psi_1 = F_1(\Psi_1, \Psi_2)$ and $\psi_2 = F_2(\Psi_1, \Psi_2)$ to be the symplectic eigenvalues of the covariance matrix of the shared states (before Bob's heterodyne detection) where

$$\Psi_1 = (V_A+1)^2(1-2T) + 2T + T^2\left(V_A + 1 + \chi_{ch}\right) \tag{13}$$

$$\Psi_2 = T^2\left((V_A+1)\xi_{ch} + 1\right)\,, \tag{14}$$

$$\chi_{ch} = \frac{1-T}{T} + \xi_{ch}\,. \tag{15}$$

The term $\chi_{E|B}$ is given by

$$\chi_{E|B} = Z\left(\frac{\theta_1 - 1}{2}\right) + Z\left(\frac{\theta_2 - 1}{2}\right) + Z\left(\frac{\theta_3 - 1}{2}\right)\,, \tag{16}$$

where θ_1, θ_2 and θ_3 are the symplectic eigenvalues of the covariance matrix of the shared states (after Bob's heterodyne detection). Specifically, we have $\theta_1 = F_1(\Theta_1, \Theta_2)$ and $\theta_2 = F_2(\Theta_1, \Theta_2)$ where

$$\begin{aligned}\Theta_1 = \Bigg(&\Psi_1\chi_d^2 + \Psi_2 + 1 \\ &+ 2\chi_d\left(T\left(V_A + 1 + \chi_{ch}\right) + (V_A+1)\sqrt{\Psi_2}\right) \\ &+ 2T\left(V_A^2 + 2V_A\right)\Bigg)\frac{1}{T^2\left(V_A + 1 + \chi\right)}\,,\end{aligned} \tag{17}$$

$$\Theta_2 = \left(\frac{V_A+1+\chi_d\sqrt{\Psi_2}}{T(V_A+1+\chi)}\right)^2\,, \tag{18}$$

$$\chi_d = \frac{2-\eta_d}{\eta_d} + \frac{2\chi_d}{\eta_d}\,, \tag{19}$$

$$\chi = \chi_{ch} + \frac{\chi_d}{T}\,, \tag{20}$$

where η_d is the detection efficiency and we set $\eta_d = 1$ for simplicity. It is known that $\theta_3 = 1$ under the assumption of Gaussian collective attack [8]. Therefore, we have $Z\left(\frac{\theta_3-1}{2}\right) = 0$.

However, the estimation of T and ξ_{ch} is not exact in the finite-key regime. The estimated T and ξ_{ch} are subject to statistical fluctuations that leads to a deviation of the estimated T and ξ_{ch} from their true values (since Alice and Bob use only N_e signals for the estimation at Step 4). The impact of using a finite number of quantum signals for parameter estimation in the security analysis is twofold. Firstly, the protocol will fail with a probability of ϵ_{PE} if the true value of T or ξ_{ch} is out of the confidence interval set by that ϵ_{PE}. Secondly, the amount of the deviation of the estimated T and ξ_{ch} from their true values is probabilistic. The lower and upper limits of the confidence interval of the estimated T for a given ϵ_{PE} are given by [9], [10]

$$T^L = \left(\hat{t} - \tau_{\epsilon_{PE}/2}\sqrt{\frac{\hat{\sigma}^2}{N_e V_A}}\right)^2\,, \tag{21}$$

$$T^U = \left(\hat{t} + \tau_{\epsilon_{PE}/2}\sqrt{\frac{\hat{\sigma}^2}{N_e V_A}}\right)^2\,, \tag{22}$$

where $\tau_{\epsilon_{PE}/2} = Q^{-1}(\frac{\epsilon_{PE}}{2})$; and $\hat{t}$ and $\hat{\sigma}$ are the estimators for T and ξ_{ch}, respectively. Similarly, the lower and upper limits of the confidence interval of the estimated ξ_{ch} for a given ϵ_{PE} are given by [9], [10]

$$\xi_{ch}^L = \frac{\hat{\sigma}^2 - \tau_{\epsilon_{PE}/2}\frac{\hat{\sigma}^2\sqrt{2}}{\sqrt{N_e}} + 1 + \xi_d}{\hat{t}^2}\,, \tag{23}$$

$$\xi_{ch}^U = \frac{\hat{\sigma}^2 + \tau_{\epsilon_{PE}/2}\frac{\hat{\sigma}^2\sqrt{2}}{\sqrt{N_e}} - 1 - \xi_d}{\hat{t}^2}\,, \tag{24}$$

respectively.

Based on the above, we can now determine $S_{BE}^{\epsilon_{PE}}$, i.e. the upper bound of χ_{BE} in the finite-key regime. Firstly, for the purpose of analysis, we set the expectation of $\hat{t}$ and $\hat{\sigma}$ as $\sqrt{\eta_d T}$ and $T\eta_d\xi_{ch}+1+\xi_d$, repectively. Then, we replace T and ξ_{ch} in Eqs. 13 to 15 and Eqs. 17 to 20 with T^L and ξ_{ch}^U, respectively. Next, we determine $S_{BE}^{\epsilon_{PE}}$ by using Eqs. 8, 9 to determine all the symplectic eigenvalues. Finally, we use Eq. 11, 16 and 10 to obtain $S_{BE}^{\epsilon_{PE}}$.

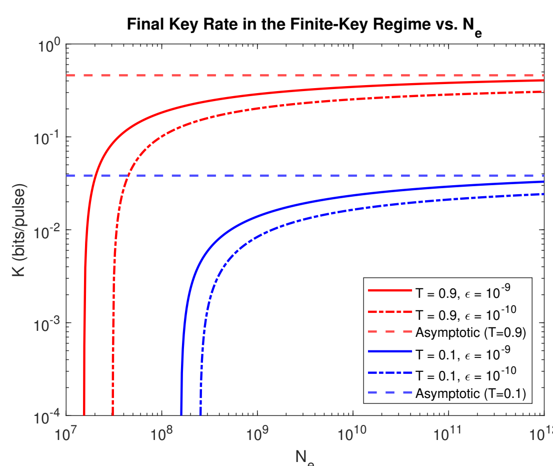

Fig. 1: K (in bits per pulse) vs. N_e. Here we adopt the standard CV-QKD setting except for N_o for all the curves. For all the curves, we assume $N_e = \frac{N_o}{2}$.

The motivation of setting a large N_e is to reduce the length of the confidence intervals when estimating T and ξ_{ch}. In Fig. 1, we compare the impact on K when setting different N_e. For all the curves in Fig. 1, we assume $N_e = \frac{N_o}{2}$. The "take-away" message is that, for a given ϵ, setting a large N_e is necessary for most CV-QKD deployments if a significant reduction of K is to be avoided.

In the satellite-based scenario, Alice and Bob starts the protocol with only N_o quantum signals because the satellite is only visible to the ground station for a limited time frame. In this section, we revisit the analysis of the final key rate in the finite-key regime and conduct a numerical search to show how the final key rate K is affected by N_e, for a given N_o and ϵ.

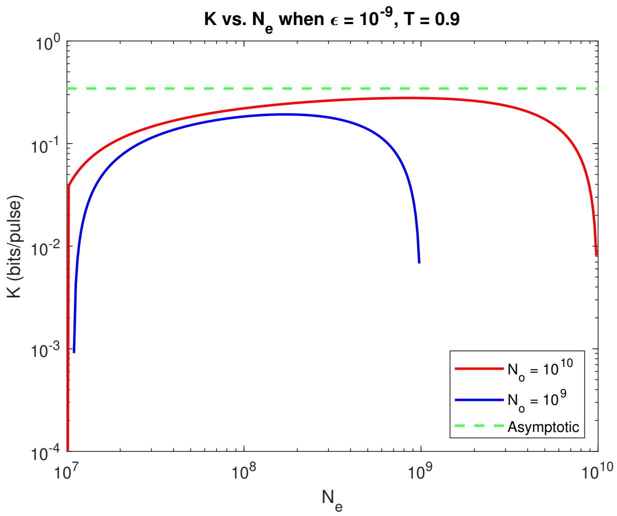

Fig. 2: K (in bits per pulse) vs. N_e when $N_o = 10^9$ (blue) and $N_o = 10^{10}$ (red). Here, we adopt the standard CV-QKD settings except that $N = 2\,(N_o - N_e)$ varies for different N_e.

We next consider a slightly different case where N_e is varied for a given N_o. In Fig. 2, we observe that K is cut off when N_e approaches 10^7 and 10^9 (for $N_o = 10^9$). At $N_e = 10^7$, the parameter confidence intervals are not consistent with a positive K. As N_e approaches N_o, K decreases rapidly since the number of quantum signals for reconciliation approaches zero. Similar remarks can also be applied for $N_o = 10^{10}$. In Fig. 2, we see that setting $N_e = \frac{N_o}{2}$ is an acceptable compromise between accommodating finite-key effects and preserving enough quantum signals for the post-processing.

References

[1] T. Richardson and R. Urbanke, *Modern Coding Theory*. Cambridge University Press, 2008.

[2] X. Ai, R. Malaney, and S. X. Ng, "A Reconciliation Strategy for Real-Time Satellite-Based QKD," *IEEE Communications Letters*, vol. 24, no. 5, 1062–1066, 2020.

[3] S.-Y. Chung, T. J. Richardson, and R. L. Urbanke, "Analysis of Sum-Product Decoding of Low-Density Parity-Check Codes Using a Gaussian Approximation," *IEEE Transactions on Information Theory*, vol. 47, no. 2, 657–670, 2001.

[4] V. A. Chandrasetty and S. M. Aziz, "FPGA Implementation of an LDPC Decoder Using a Reduced Complexity Message Passing Algorithm," *Journal of Networks*, vol. 6, no. 1, 36, 2011.

[5] S. Kish, E. Villaseñor, R. Malaney, K. Mudge, and K. Grant, "Feasibility Assessment for Practical Continuous Variable Quantum Key Distribution over the Satellite-to-Earth Channel," *Quantum Engineering*, vol. 2, no. 3, e50, 2020.

[6] F. Grosshans, "Collective Attacks and Unconditional Security in Continuous Variable Quantum Key Distribution," *Physical Review Letters*, vol. 94, 020504, 2005.

[7] M. Navascués, F. Grosshans, and A. Acin, "Optimality of Gaussian Attacks in Continuous-Variable Quantum Cryptography," *Physical Review Letters*, vol. 97, no. 19, 190502, 2006.

[8] S. Fossier, E. Diamanti, T. Debuisschert, R. Tualle-Brouri, and P. Grangier, "Improvement of Continuous-Variable Quantum Key Distribution Systems by Using Optical Preamplifiers," *Journal of Physics B: Atomic, Molecular and Optical Physics*, vol. 42, no. 11, 114014, 2009.

[9] A. Leverrier, F. Grosshans, and P. Grangier, "Finite-Size Analysis of a Continuous-Variable Quantum Key Distribution," *Physical Review A*, vol. 81, no. 6, 062343, 2010.

[10] P. Jouguet, S. Kunz-Jacques, E. Diamanti, and A. Leverrier, "Analysis of Imperfections in Practical Continuous-Variable Quantum Key Distribution," *Physical Review A*, vol. 86, no. 3, 032309, 2012.