Long-distance quantum key distribution using concatenated entanglement swapping with practical resources

Aeysha Khalique
Barry C. Sanders

Long-distance quantum key distribution using concatenated entanglement swapping with practical resources

Aeysha Khalique\textsuperscript{a,b,*} and Barry C. Sanders\textsuperscript{b,c,d,e,f}
\textsuperscript{a}National University of Sciences and Technology, School of Natural Sciences, H-12 Islamabad, Pakistan
\textsuperscript{b}University of Science and Technology of China, Shanghai Branch, CAS Center for Excellence and Synergetic Innovation Center in Quantum Information and Quantum Physics, Shanghai, China
\textsuperscript{c}University of Science and Technology of China, Hefei National Laboratory for Physical Sciences at Microscale, Hefei, Anhui, China
\textsuperscript{d}University of Calgary, Institute for Quantum Science and Technology, Alberta, Canada
\textsuperscript{e}Institute for Quantum Information and Matter, California Institute of Technology, Pasadena, California, United States
\textsuperscript{f}Institute for Quantum Information and Matter, Annual Institute of Technology, Hefei, Anhui, China

Abstract. We explain how to share photons between two distant parties using concatenated entanglement swapping and assess performance according to the two-photon visibility as the figure of merit. From this analysis, we readily see the key generation rate and the quantum bit error rate as figures of merit for this scheme applied to quantum key distribution (QKD). Our model accounts for practical limitations, including higher-order photon pair events, dark counts, detector inefficiency, and photon losses. Our analysis shows that compromises are needed among the runtimes for the experiment, the rate of producing photon pairs, and the choice of detector efficiency. From our quantitative results, we observe that concatenated entanglement swapping enables secure QKD over long distances but at key generation rates that are far too low to be useful for large separations. We find that the key generation rates are close to both the Takeoka–Guha–Wilde and the Pirandola–Laurenza–Ottaviani–Banchi bounds.

Keywords: quantum key distribution; entanglement swapping; long-distance quantum communication.

Paper 161639P received Oct. 20, 2016; accepted for publication Jan. 5, 2017; published online Jan. 25, 2017.

1 Introduction

Quantum communication provides a means for secure communication in open channels.\textsuperscript{1} One of the primary goals of quantum communication is to develop the ability to communicate at arbitrary distances. Experimentally, communication distances have been limited to a few 100 km. Recently, quantum key distribution (QKD) of up to 200 km has been achieved with measurement-device-independent QKD.\textsuperscript{2} A distance of up to 250 km has been achieved using a subcarrier wave modulation method, which employs the Bennett–Brassard protocol.\textsuperscript{3} Quantum relays and repeaters are promising setups to achieve the ultimate goal of long-distance quantum communication.\textsuperscript{4} In principle, any distance is achievable using quantum relays. In practice, however, the allowed distance is limited by resource imperfections. These imperfections also limit the key generation rate, which will affect the efficacy of the system.

Quantum relays and repeaters have been investigated for long-distance key distribution\textsuperscript{5} which models the resources with approximations. We provide a rigorous model for a quantum relay setup based on entanglement swapping in which we have included the imperfections of the sources, the channels, and the detectors.\textsuperscript{6,7} This concatenated entanglement swapping setup is then extended to key distribution protocol,\textsuperscript{8} which relies on the Bennett–Brassard–Mermin\textsuperscript{9} protocol. In this paper, we explain our approach to model concatenated entanglement swapping and key distribution protocol based on such a swapping setup.\textsuperscript{10} Our approach could be useful for modeling long-distance quantum communication incorporating quantum memories and by extension quantum repeaters.

This paper is organized as follows: in Sec. 2, we explain the entanglement swapping process and discuss the resources proposed for an experimental setup. In Sec. 3, we present the model for a single swap and calculation of four-photon visibility based on that. The concatenated entanglement swapping setup for long-distance quantum communication and the corresponding results for visibility are shown in Sec. 4. In Sec. 5, we present the QKD protocol based on concatenated entanglement swapping and show the results for maximum key generation rates with optimized resource parameters. Finally, we conclude in Sec. 6.

2 Devices for Entanglement Swapping

The achievable distance in quantum communication can be increased by entanglement swapping. In this section, we briefly review the entanglement swapping procedure and the devices used in a swapping experiment. We explain the entanglement swapping procedure in Sec. 2.1 and the practical devices in Sec. 2.2.

2.1 Entanglement Swapping with Perfect Devices

Entanglement swapping provides a means for entangling distant parties who have never interacted in the past. Figure 1 shows the entanglement of possibly distant parties A and B.
when their entangled partners, C and D, undergo a Bell-state measurement (BSM). BSM distinguishes between the four Bell states

\[ |\psi^+ \rangle = \frac{1}{\sqrt{2}} (|HV \rangle + |VH \rangle); \]
\[ |\psi^- \rangle = \frac{1}{\sqrt{2}} (|HV \rangle - |VH \rangle); \]
\[ |\phi^+ \rangle = \frac{1}{\sqrt{2}} (|HH \rangle + |VV \rangle); \text{ and} \]
\[ |\phi^- \rangle = \frac{1}{\sqrt{2}} (|HH \rangle - |VV \rangle), \]

\[ \text{(1)} \]

Entanglement swapping is evident from the fact that the combined entangled state of AC and BD is

\[ |\psi^+ \rangle_{AC} |\psi^+ \rangle_{BD} = \frac{1}{2} [|\psi^+ \rangle_{AB} |\psi^+ \rangle_{CD} + |\psi^- \rangle_{AB} |\psi^- \rangle_{CD} + |\phi^+ \rangle_{AB} |\phi^+ \rangle_{CD} + |\phi^- \rangle_{AB} |\phi^- \rangle_{CD}|. \]

\[ \text{(2)} \]

Thus, BSM on C and D projects A and B into the corresponding Bell state.

### 2.2 Resources

In a typical entanglement swapping setup, the relevant resources are the entanglement source, the channels, and the detectors. All these resources have imperfections. For convenience, we list the definition of parameters used in this paper in Table 1.

First, we consider a parametric down-conversion (PDC) entanglement source that produces multipairs of entangled photons. The state of the photons entangled in horizontal–vertical (H–V) polarization is

\[ |\chi \rangle = e^{i \chi} (\hat{a}^\dagger H \hat{a}^\dagger V + \hat{a}^\dagger V \hat{a}^\dagger H + i \hbar c) |\text{vac} \rangle \]
\[ = \text{sech} \chi e^{i \hbar c \chi / \Delta (\hat{a}^\dagger n + \hat{a}^\dagger \bar{n})} |\text{vac} \rangle, \]

\[ \text{(3)} \]

where \( \chi^2 \) is the multipair production rate of the source, and \( \hat{a}^\dagger H \) and \( \hat{a}^\dagger V \) are the creation operators for horizontally polarized photons in spatial modes A and C, respectively. The corresponding creation operators \( \hat{a}^\dagger V \) and \( \hat{a}^\dagger H \) are for vertically polarized photons.

We consider a fiber optic channel with distance-dependent loss coefficient \( \alpha \). The channel efficiency is

\[ \eta = e^{-(\alpha \ell + \Delta n)/10}, \]

\[ \text{(4)} \]

where \( \ell \) is the length of the fiber and \( \alpha_0 \) is the distance-independent loss. The same model can be employed to model free-space transmission.

A realistic detector is modeled as pairing of a perfect detector with a beam splitter (BS)\(^{11} \) as shown in Fig. 2. Both the detector’s intrinsic efficiency \( \eta_0 \) and the channel transmission efficiency \( \eta_t \) are included in the transmission efficiency of the BS, which in turn is \( \eta = \eta_0 \eta_t \). The dark counts of the detector are modeled by a thermal source of light, which represents stray photons incident on one port of the BS. These photons, which are at pseudotemperature \( T \), with \( T \) chosen as an adjustable parameter to model the detector, can be expressed by the state

\[ \hat{\rho}_T = (1 - e^{-\hbar \omega / k_b T}) \sum_{n=0}^\infty e^{-n \hbar \omega / k_b T} |n \rangle \langle n |, \]

\[ \text{(5)} \]

where \( |n \rangle \) is the photon number state.
The signal photons $\hat{\rho}_{\text{sig}}$ are incident on the other port. Threshold detectors have two possibilities, with $q = 0$ corresponding to no click and $q = 1$ corresponding to a click. The probability of detecting $q$ photons given $i$ incident photons is

$$P(q = 0 | i) = (1 - \varphi)(1 - \eta(1 - \varphi))^i = 1 - P(q = 1 | i),$$

where $i$ is the number of photons in the signal state $\hat{\rho}_{\text{sig}} = |i\rangle \langle i|$ and $\varphi$ is the dark count probability. The detectors are mutually independent and the conditional probability of detecting $q, r, s,$ and $t$ photons, each on one of the four detectors for $i, j, k,$ and $l$ incident signal photons, respectively, is the following product of four independent probabilities:

$$P(qrst | ijk) = P(q | i)P(r | j)P(s | k)P(t | l).$$ (7)

Now, we have a mathematical framework for each of the three pertinent devices, namely the sources, the channels, and the detectors.

### 3 Practical Single Swap: Coincidence Probabilities and Visibility

In practice, the entanglement swapping setup consists of two PDC sources. Figure 3 shows two parties A and B, which become entangled by BSM at the two inner ports. The BSM setup consists of a BS followed by polarization rotators and polarization BSs that separate the horizontal and vertical polarization photons. These photons are detected at the four photodetectors. The detector clicks corresponding to ideal BS outcomes for various Bell states are given in Table 2.

The fourfold coincidence is the conditional coincidence of detector clicks in spatial modes $a_1$ and $d_1$, shown in Fig. 3, given that the Bell measurement has resulted in the clicks (0101) or (1010) at the inner ports. These clicks at the inner detectors correspond to the measurement of the Bell state $|\psi^+\rangle$ as shown in Table 2. Out of various coincidences, $(q'r's't') \in \{(0101), (1010)\}$ occurs a maximum number of times, and the probability of occurrence of these coincidences is the maximum coincidence probability

$$Q_{\text{max}}(qrst) = \max_{q'r's't'} Q(q'r's't'|qrst; \chi, \varphi, \eta),$$

where $Q_{\text{max}}(qrst)$ depends on the resource parameters, $\chi, \varphi$, and $\eta$. The coincidences, $(q'r's't') \in \{(0110), (1001)\},$

<table>
<thead>
<tr>
<th>State</th>
<th>(qrst)</th>
</tr>
</thead>
<tbody>
<tr>
<td>$</td>
<td>\psi^+\rangle$</td>
</tr>
<tr>
<td>$</td>
<td>\psi^-\rangle$</td>
</tr>
<tr>
<td>$</td>
<td>\phi^+\rangle$</td>
</tr>
</tbody>
</table>

The conditional probability $Q$ is calculated by the following course of action on the photons produced by the two PDCs. The photons in the inner two channels undergo the action of BS $U_B$ yielding

$$|\Xi\rangle = U_B|x\rangle_A|x\rangle_C|x\rangle_{BD},$$

and the ideal detection of photons $i, j, k,$ and $l$ at the inner detectors is reflected by Fock projection $\Pi^{\text{inn}}_{ijkl}$, which yields the state

$$|\Xi\rangle_{ijkl}^{\text{out}} = \frac{\langle ijk\rangle_{CD}|\Pi^{\text{inn}}_{ijkl}|\Xi\rangle_{ijkl}}{P(ijk)},$$

at the outer ports. Here $P(ijk) = \langle \Xi|\Pi^{\text{inn}}_{ijkl}|\Xi\rangle$. The noisy detection at the inner ports produces a mixed state,

$$P^{\text{inn}}_{qrst} = \sum P(ijk|qrst)|\Xi\rangle_{ijkl}^{\text{out}}|\Xi\rangle_{ijkl}^\text{inn},$$

at the outer ports. Here, $P(ijk|qrst)$ is the conditional probability that $ijkl$ photons are detected ideally given actual detection $qrst$. This probability can be found from the known probability $P(qrst|ijkl)$ given in Eq. (7) using Bayes’ theorem

$$P(ijk|qrst) = \frac{P(qrst|ijkl)P(ijk)}{P(qrst)} = P(q | i)P(r | j)P(s | k)P(t | l)P(ijk)/P(qrst).$$ (14)

The conditional probability of detecting $i'j'k'l'$ photons at ideal outer detectors, given actual counts $qrst$ at the inner ones, after passing through the polarization rotators at angles $\delta_A$ and $\delta_B$, is

\[\text{Fig. 3 Experimental setup for single swap. q' and r' represent the clicks on detectors at A, and s' and t' are clicks on those at B. q, r, s, and t are the clicks at inner detectors. PR labels a polarizer rotator, PBS labels a polarizing BS, and BS labels a BS. PDC labels a PDC source.}\]
\[ P(i'j'k'l'|qrst) = \frac{\left| \langle i'j'k'l'|U(\delta_\alpha)U(\delta_\beta)\rho_{\text{out}}^{\text{intralink-}}U^\dagger(\delta_\alpha) \right|^2}{\left| U^\dagger(\delta_\beta)|i'j'k'l'\rangle \right|^2} \]

The fourfold coincidence probability \( Q \) of detecting actual photons \( q' r's't' \) at the outer four detectors given \( qrst \) at the inner ones is

\[ Q(q'r's't'|qrst) = \sum_{i'j'k'l'} P(q'r's't'|i'j'k'l'; \varrho, \eta) \times P(i'j'k'l'|qrst). \]

This expression for \( Q \) can thus be calculated using Eqs. (14) and (15).

4 Extending the Distance by Arbitrary Swaps

Communication distance can be extended by concatenating signal swaps. We analyze such a setup and calculate the corresponding visibility. We give a closed-form solution for calculation of \( Q_{\text{ext}}(qrst) \) for an arbitrary number of swaps in Sec. 4.1. In Sec. 4.2, we give our results for calculation of visibility for \( N \leq 3 \).

4.1 Closed-Form Solution for Calculation of \( Q_{\text{ext}}(qrst) \) for \( N \) Swaps

The configuration for concatenated \( N \) swaps is shown in Fig. 4. For \( N \) swaps, there are \( 2N - 1 \) BSMs. Ideally, successful BSM at the inner stations entangles distant parties \( A \) and \( B \) at the extreme ends. However, practically, the maximum probability of clicks at the outer detectors corresponding to clicks \( qrst \) at the inner ones is dependent on resource parameters \( \chi, \varrho \), and \( \eta \).

\[ Q_{\text{ext}}(qrst) = \max_{q'r's't'} Q(q'r's't'|qrst; \chi, \varrho, \eta), \]

where \( q = \{ q_1, q_2, \ldots, q_{2N-1} \} \), and the same goes for \( r, s, \) and \( t \).

The closed-form solution of the conditional probability \( P(i'j'k'l'|qrst) \) is Ref. 7

\[ P(i'j'k'l'|qrst) = \sum_{ijkl} P(ijklqrst) \frac{1}{\sqrt{2^{i+j+k+l}}} \frac{\left| \langle i'j'k'l'|U(\delta_\alpha)U(\delta_\beta)|\Xi\rangle^{\text{out}}_{ijkl} \langle \Xi|U(\delta_\alpha)U^\dagger(\delta_\beta)|i'j'k'l'\rangle}{\left| U^\dagger(\delta_\beta)|i'j'k'l'\rangle \right|^2} \]

\[ \times \frac{\left( \frac{\left| \langle i'j'k'l'|U(\delta_\alpha)U(\delta_\beta)|\Xi\rangle^{\text{out}}_{ijkl} \langle \Xi|U(\delta_\alpha)U^\dagger(\delta_\beta)|i'j'k'l'\rangle}{\left| U^\dagger(\delta_\beta)|i'j'k'l'\rangle \right|^2} \right)_{ijkl}^{\text{out}}}{\left( \frac{\left| \langle i'j'k'l'|U(\delta_\alpha)U(\delta_\beta)|\Xi\rangle^{\text{out}}_{ijkl} \langle \Xi|U(\delta_\alpha)U^\dagger(\delta_\beta)|i'j'k'l'\rangle}{\left| U^\dagger(\delta_\beta)|i'j'k'l'\rangle \right|^2} \right)^{\text{out}}_{ijkl}} \]

Here

\[ \Omega(\mu_n, \lambda_n, i_{N+n}, l_{N+n}) = \sum_{\gamma=0}^{\mu_n+\lambda_n} \mu_n + \lambda_n \]

\[ \times \left( \frac{i_{N+n} + l_{N+n} - \mu_n - \lambda_n}{i_{N+n} - \gamma} \right) (-1)^{\mu_n + \lambda_n - \gamma} \]

is the factor resulting from the BSM connecting the adjacent swaps.
visibility for \( N = 1, 2, \) and 3 for various distances. The achievable distance increases to more than 1000 km for \( N = 3 \), but at the expense of very low visibility. The increase in distance tends to saturate as the number of concatenations increases. The rapid fall-off in visibility and limiting distance are due to detector dark counts and inefficiencies. For perfect detectors with \( \eta_0 = 1 \) and \( \varphi = 1 \), an asymptotically large distance is achievable as shown in Fig. 8.

5 Long-Distance Quantum Key Distribution Protocol

The concatenated entanglement swapping setup described above is implemented in long-distance QKD protocol. The setup is shown in Fig. 9. Two distant users A and B are
connected by the concatenated entanglement swapping setup. Bell-state measurements at the intermediate stations ensure entanglement at the two extreme ends. The results of two-photon coincidence at the intermediate stations are sent to B, who calculates the visibility using these results and the two-photon coincidence at his and A’s stations by the formalism developed for concatenated swapping. The visibility is related to the quantum bit error rate (QBER)\(^1\)

\[
\text{QBER} = \frac{1 - V}{2} .
\] (20)

The key generation rate is

\[
R = R_{\text{Shor-Preskill}} R_{\text{sifted}} .
\] (21)

Here \(R\) comprises the sifted key rate

\[
R_{\text{sifted}} = \frac{1}{2} (\chi^2) 2^N 10^{-\alpha f/40} N^{4N} (\eta^2/2)^{2N-1} \eta^2 ,
\] (22)

and the key retained after error correction and privacy amplification

\[
R_{\text{Shor-Preskill}} = 1 - \kappa H_2(Q) - H_2(Q) ,
\] (23)

where \(\kappa\) is the reconciliation efficiency, with \(\kappa = 1\) for perfect reconciliation. The net key rate is the product of the two rates. The linear-optical BSM process employed here is probabilistically bounded by its maximum value of 1/2,\(^{13}\) which leads to a factor of \(\eta^2/2\) in \(R_{\text{sifted}}\) in Eq. (22). Deterministic BSM, however, can be done using hyperentanglement,\(^{14,15}\) which will require a source entangled in more than one degree of freedom.

We present the results obtained for maximized key generation rates \(R_{\text{max}}\) with optimum \(\chi, \eta_0, \) and \(\varphi\) in Fig. 10. There is a trade-off between \(\eta_0\) and \(\varphi\), as for very high efficiency, the contribution of dark counts in detected photons also increases, which lowers the visibility. We have used the trade-off corresponding to commonly used InGaAs detectors with

\[
\varphi = A \exp(\eta_0) ,
\] (24)

where typically \(A = 6.1 \times 10^{-7}\) and \(B = 17.16\).

Maximum key generation rates \(R_{\text{max}}\) and the optimal \(\chi\) and \(\eta\) are shown in Fig. 10. Distances up to 850 km are achievable for \(N = 3\), but at the cost of a very low key generation rate. We check the upper bound of the key generation rate and compare it with the Takeoka–Guha–Wilde (TGW) bound\(^17\) and a more recent tighter Pirandola–Laurenza–Ottaviani–Banchi (PLOB) bound.\(^18\) The TGW bound gives an upper bound on the key generation rate for nonrepeater-based QKD, which is

\[
R_{\text{TGW}} = \log_2 \left( \frac{1 + 10^{-\alpha f/10}}{1 - 10^{-\alpha f/10}} \right) .
\] (25)

and the PLOB bound for lossy channel is

\[
R_{\text{PLOB}} = \log_2 \left( \frac{1}{1 - 10^{-10 f/10}} \right) .
\] (26)

The upper bound for the concatenated entanglement swapping setup is calculated by setting \(R_{\text{Shor-Preskill}} = 1\) thus, \(R = R_{\text{sifted}}\). The comparison in Fig. 11 shows that the concatenated entanglement swapping key rates are close to the TGW and PLOB bound. Thus, quantum memories are needed to further increase the key generation rates resulting from concatenated entanglement swapping setup.

### 6 Conclusions

We have presented our approach for calculation of visibility between distant parties using concatenated entanglement swapping with an arbitrary number of swaps and its application to long-distance QKD.\(^6,19\) Our model incorporates the practical resources. The results show that large distances can be achieved by concatenated entanglement swapping, but this increase comes at the expense of atrociously low key generation rates. A trade-off is needed between experiment runtime, resource parameters, and key generation rates.
Acknowledgments

We thank Wolfgang Tittel, Michael Lamoureux, Artur Scherer, Norbert Lütkenhaus, and Pengqin Zhang for valuable discussions. BCS appreciates financial support provided by NSERC, Alberta Innovates Technology Futures, China’s 1000 Talent Plan, and by the Institute for Quantum Information and Matter, which is a National Science Foundation Physics Frontiers Center (NSF Grant PHY-1125565) with support of the Gordon and Betty Moore Foundation (GBMF-2644). This research has been enabled by the use of computing resources provided by WestGrid and Compute/Calcul Canada.

References


Aeysa Khalique received her doctorate in physics from Technische Universität Darmstadt, Germany. She is head of the physics department at the School of Natural Sciences at National University of Sciences and Technology, Islamabad, Pakistan. She is currently managing the quantum information group at the University of Sciences and Technology Islamabad.

Barry C. Sanders is AITF iCORE strategic chair in quantum information science and director of the Institute for Quantum Science and Technology at the University of Calgary. He holds a 1000-Talents Chair at the University of Science and Technology of China. He is editor-in-chief of New Journal of Physics and fellow of the Institute of Physics (U.K.), the Optical Society of America, and the American Physical Society, and recently received an Imperial College London Doctor of Science degree.