Finite-key analysis of high-dimensional time–energy entanglement-based quantum key distribution

Citation: Lee, Catherine, Jacob Mower, Zheshen Zhang, Jeffrey H. Shapiro, and Dirk Englund. "Finite-Key Analysis of High-Dimensional Time–energy Entanglement-Based Quantum Key Distribution." Quantum Information Processing 14, no. 3 (January 7, 2015): 1005–1015.

As Published: http://dx.doi.org/10.1007/s11128-014-0904-x

Publisher: Springer US

Persistent URL: http://hdl.handle.net/1721.1/107141

Version: Author's final manuscript: final author's manuscript post peer review, without publisher's formatting or copy editing

Quantum Inf Process manuscript No.
(will be inserted by the editor)

Finite-key analysis of high-dimensional time-energy entanglement-based quantum key distribution

Catherine Lee · **Jacob Mower** ·
Zheshen Zhang · **Jeffrey H. Shapiro** ·
Dirk Englund

Received: date / Accepted: date

Abstract We present a security analysis against collective attacks for a time-energy entanglement-based quantum key distribution protocol, given the practical constraints of single photon detector efficiency, channel loss, and finite-key considerations. We find a positive secure-key capacity when the key length increases beyond 10^4 for eight-dimensional systems. The minimum key length required is reduced by the ability to post-select on coincident single-photon detection events. Including finite-key effects, we show the ability to establish a shared secret key over a 200 km fiber link.

Keywords Quantum key distribution · Entanglement · Secure communication

1 Introduction

Quantum key distribution (QKD) [1,2] is currently at the forefront of experimentally achievable applications of quantum information theory. QKD enables the creation and distribution of random, information-theoretically secure keys that can be used with classical symmetric encryption schemes, such as the one-time pad, which provides perfect secrecy. Traditional QKD protocols [1,3,4] are based on discrete, two-state quantum systems, such as the orthogonal polarizations of single photons, providing at most one bit of information per single detected photon (or photon pair, in the case of entangled-photon QKD). However, in such discrete-variable protocols, the rate of key generation is typically limited by experimental constraints, such as the rate of generating photons or the saturation rate of single-photon detectors, making

---

This work was supported by the DARPA Information in a Photon program, through grant W911NF-10-1-0416 from the Army Research Office, and the Columbia Optics and Quantum Electronics IGERT under NSF grant DGE-1069420.

C. Lee · J. Mower · Z. Zhang · J. H. Shapiro · D. Englund
Research Laboratory of Electronics, Masschusetts Institute of Technology, Cambridge, MA 02139, USA
E-mail: cath@mit.edu

C. Lee
Department of Physics, Columbia University, New York, NY 10027, USA

it difficult to efficiently produce long keys. An alternate class of protocols encodes information in continuous variables, such as the amplitude and phase quadratures of coherent light [5,6]. These continuous variable QKD (CV-QKD) protocols take advantage of infinite-dimensional Hilbert spaces. However, their attainable channel length is generally shorter than that of single-photon QKD; the current demonstrated maximum is 80 km [7]. A QKD protocol that encodes information in continuous variables of single photons would combine the high-dimensional Hilbert spaces of CV-QKD with the increased channel lengths of single-photon QKD. Such a high-dimensional QKD protocol [8] could generate more than one bit of information per detected photon (or photon pair), producing secret key bits more quickly while also providing increased resilience to noise and loss [9].

High-dimensional QKD protocols have been implemented by encoding information in various photonic degrees of freedom, including position-momentum [10], time-energy [11–17], and orbital angular momentum (OAM) [18–21]. Of these, the time-energy basis is particularly appealing for implementations in today's telecommunications infrastructure. The time-energy correlations are compatible with wavelength division multiplexing (WDM) systems and robust in transmission through both fiber and free space, allowing for versatile, heterogeneous networks. Additionally, advanced time-energy-entangled (TEE) photon pair sources [22] and fast, efficient detectors [23] have been developed for the telecom band.

Recent theoretical studies have introduced new techniques to provide provable security against the class of collective attacks for TEE-based QKD schemes, combining elements of single-photon and CV-QKD security proofs [16,24]. However, these proofs assume that their respective procotols generate infinitely long keys. To show security in the realistic regime of finite-length keys, we must extend the previous proofs. Here, we consider the recently proposed dispersive-optics QKD protocol (DO-QKD) [16] and show that it is secure against collective attacks, given the practical constraints of single-photon detector efficiency, channel loss, and finite-key considerations [25–33].

2 Case study: DO-QKD

Figure 1(a) presents a schematic of the DO-QKD setup. Alice produces time-energy-entangled photon pairs by spontaneous parametric down-conversion (SPDC). The largest possible dimension d of the protocol is given by the Schmidt number, i.e., the number of possible information eigenstates in the system. This is approximately $d \equiv \sigma_{\mathrm{coh}}/\sigma_{\mathrm{cor}}$ [34,13], where σ_{coh} is the coherence time of the SPDC pump field, and σ_{cor} is the correlation time between photons, which is set by the phase-matching bandwidth of the SPDC source. Alice keeps one photon and sends the other into the quantum channel to Bob. Alice and Bob measure their photons in the time or frequency bases. The time basis (TB) corresponds to direct detection of photon arrival time; the frequency basis (FB) is implemented by direct detection after passage through a group-velocity dispersive element. When Alice measures in the FB, she applies normal group-velocity dispersion (GVD) to her photon, and when Bob measures in the FB, he applies anomalous GVD of equal magnitude.

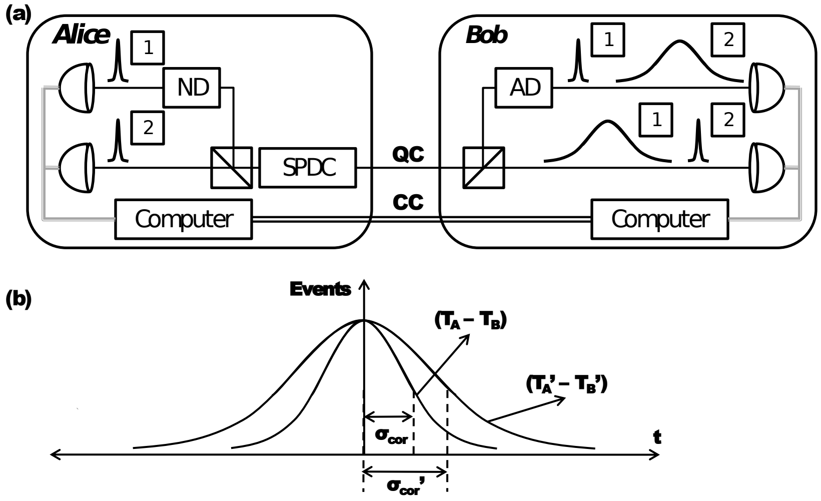

Fig. 1 (a) Schematic of the DO-QKD setup. Alice holds the SPDC source, keeps one photon, and sends the other to Bob. In case 1, Alice measures in the FB, and in case 2, she measures in the TB. Bob must measure in the same basis as Alice for their measurements to be correlated. QC is quantum communication, CC is classical communication, ND is normal dispersion, and AD is anomalous dispersion. (b) Depiction of decreased photon correlations measured by Alice and Bob, from the ideal correlation time σ_{cor} to the observed σ'_{cor}

If Alice and Bob both record photons in the TB, they obtain narrow timing correlations with width corresponding to T_J. If only one party measures in the FB, the timing correlations are broadened to approximately the magnitude of the applied GVD. Since this magnitude is chosen to be $\gg T_J$, the timing correlations are severely diminished if Alice and Bob choose opposite measurement bases. If Alice and Bob both record photons in the FB, the original correlations between their photons can be recovered, since the GVD is nonlocally cancelled in the limit of long σ_{cor} [35, 16].

After the measurement stage of the protocol, Alice and Bob sift their time-tagged data into frames of duration $d \times T_{\text{bin}}$, comprised of d bins of duration T_{bin}, where $T_{\text{bin}} \approx T_J$. They communicate their basis choices and keep only the data from frames during which they each registered a single detection event while using the same basis. Alice and Bob convert each detection event into a $\log_2 d$-bit symbol, based on the position of the event within the frame. They publicly compare a subset of their sifted keys to bound the information accessible to an eavesdropper, Eve. Then they use error correction and privacy amplification [36] to extract identical secret keys.

The security analysis of DO-QKD relies on Alice and Bob's estimates of characteristic parameters from their publicly compared data subset. Specifically, they must estimate the increase in their photons' correlation time from the ideal σ_{cor} to the experimentally measured σ'_{cor}, as depicted in Figure 1(b). They must also estimate the increase in their photons' correlation frequency; because of the GVD, this can be found from timing measurements. The precision of Alice and Bob's estimates increases with the sample size; however, publicly comparing a greater fraction of their measurements reduces the amount of raw key that can be used to generate the secure key. In practice, Alice and Bob have a finite number of measurements, so they must find the optimal compromise between the conflicting goals of accurately estimating parameters and maximizing the length of their secure key.

3 Finite-key analysis for arbitrary basis selection probabilities

3.1 Asymmetric basis selection

In the standard QKD protocols [1,3,2], Alice and Bob selected between the two measurement bases with equal probabilities, limiting the probability of generating a shared character of key to at most 50%. It was later suggested [37] that the efficiency of a QKD protocol could be increased asymptotically to 100% if Alice and Bob choose one measurement basis with a greater probability than the other, increasing the likelihood that Alice and Bob will make measurements in the same basis. We will take the same approach here.

Without further modification to our protocol, Eve could exploit Alice and Bob's asymmetric selection. If Eve were aware of Alice and Bob's basis choice probabilities, then by using only the dominant basis, she could eavesdrop while introducing fewer timing errors in that basis. This gives Eve a better chance of remaining undetected by Alice and Bob. To prevent this possibility, Alice and Bob must further modify their protocol: they divide their data according to the measurement basis used, and they estimate parameters, such as the correlation time, separately for each basis. If Eve chooses to eavesdrop in the TB, she introduces more errors in the FB [37].

When implementing DO-QKD using asymmetric basis selection, we assume that Alice and Bob choose to measure in the TB with probability $p > 1/2$; that is, Alice and Bob apply GVD to fewer than half of the signal photons. The exact value of p must then be chosen, along with other parameters, to optimize the secure-key capacity for a given finite number of measurements, as described below.

3.2 Finite-key effects on secure-key capacity

Outside the asymptotic limit, a protocol can be only ε_s-secure, where ε_s is the tolerated failure probability of the entire protocol [25]. The entire protocol is said to fail if, at its conclusion, unbeknownst to Alice and Bob, the eavesdropper holds information about their secret key. The security parameter ε_s is the sum of the failure probabilities of each stage of the protocol:

$$\varepsilon_s = \varepsilon_{EC} + \varepsilon_{PA} + n_{PE}\varepsilon_{PE} + \bar{\varepsilon}, \tag{1}$$

where $\varepsilon_{EC/PA/PE}$ are the probabilities that error correction, privacy amplification, or parameter estimation, respectively, fail, and n_{PE} is the number of parameters to be estimated [29]. Error correction fails if Alice and Bob are unable to obtain identical keys. Privacy amplification fails if it leaks information to the eavesdropper. Parameter estimation fails if the real parameter lies outside of the confidence interval set by ε_{PE}. The $\bar{\varepsilon}$ term in (1) accounts for the accuracy of estimating the smooth min-entropy, which characterizes the amount of secure information that can be extracted using privacy amplification [25]. Failure of any stage of the protocol implies that Alice and Bob are unaware that something has gone wrong [30].

The finite-key secure-key capacity for the DO-QKD protocol can then be written as [25–30]:

$$r_N = \frac{n}{N}\left(r_{DO} - \frac{1}{n}\log_2\frac{2}{\varepsilon_{EC}} - \frac{2}{n}\log_2\frac{1}{\varepsilon_{PA}} - (2\log_2 d + 3)\sqrt{\frac{\log_2(2/\bar{\varepsilon})}{n}}\right). \tag{2}$$

Here r_{DO} is the secure-key capacity in the asymptotic regime, which was derived in Ref. [16]. The units in (2) are bits per coincidence (bpc), i.e., bits per frame in which Alice and Bob each detect only one event. N is the number of instances in which Alice and Bob both detect a single photon in a measurement frame. The parameter $n = p^2 N$ denotes the number of frames in which Alice and Bob both chose the TB, where p is the probability that the TB is chosen. We assume that Alice and Bob use the same value of p. The subtracted terms on the right-hand side of Eq. (2) represent the corrections to r_{DO} due to the finite key length.

The factor n/N in (2) reflects the fact that not all of the coincidences detected by Alice and Bob contribute to key generation because some coincidences must be sacrificed for parameter estimation. In particular, we assume that all $m = (1-p)^2 N$ coincidences in the FB are used for parameter estimation. Alice and Bob also sacrifice m of the coincidences in the TB to estimate parameters for that basis, leaving $n - m$ coincidences in the TB for key generation.

For each value of N, we maximize r_N by optimizing the parameter set $\{\varepsilon_{PA}, \varepsilon_{PE}, \bar{\varepsilon}, p\}$; thus the basis choice probability p is a function of N, the number of signals exchanged. The security parameter ε_s is determined beforehand by Alice and Bob's security requirements, and ε_{EC} is fixed by the choice of error correction code. Additionally, the calculation of r_{DO} must be modified to include the effects of finite key length on parameter estimation.

3.3 Modified asymptotic secure-key capacity and parameter estimation

The asymptotic secure-key capacity r_{DO} is given by [16]:

$$r_{DO} = \beta I(A;B) - \chi(A;E), \tag{3}$$

where β is the reconciliation efficiency, $I(A;B)$ is Alice and Bob's Shannon information, and $\chi(A;E)$ is Alice and Eve's Holevo information. Since Alice and Bob use only measurements made in the TB for the key, their Shannon information is calculated using only the contribution from the TB. This calculation includes the effects of detection efficiency, timing jitter, and dark counts. To calculate the Holevo information, Alice and Bob must determine the covariance matrix of their data. To do this, they must estimate the increase in their photons' correlation time from σ_{cor} to σ'_{cor}, as depicted in Figure 1(b).

The covariance matrix $\mathit{\Gamma}$ is given by

$$\mathit{\Gamma} = \begin{pmatrix} \gamma_{AA} & (1-\eta)\gamma_{AB} \\ (1-\eta)\gamma_{BA} & (1+\varepsilon)\gamma_{BB} \end{pmatrix}, \tag{4}$$

where $\mathit{\Gamma}$ is a four-by-four matrix composed of four two-by-two submatrices. Each submatrix γ_{JK} for $J,K = A,B$ describes the covariance between the measurements of parties J and K. The submatrices are given by

$$\begin{aligned} \gamma_{AA} &= \begin{pmatrix} \frac{u+v}{16} & -\frac{u+v}{8k} \\ -\frac{u+v}{8k} & \frac{(u+v)(4k^2+uv)}{4k^2uv} \end{pmatrix}, \\ \gamma_{AB} = \gamma_{BA}^T &= \begin{pmatrix} \frac{u-v}{16} & \frac{u-v}{8k} \\ -\frac{u-v}{8k} & -\frac{(u-v)(4k^2+uv)}{4k^2uv} \end{pmatrix}, \\ \gamma_{BB} &= \begin{pmatrix} \frac{u+v}{16} & \frac{u+v}{8k} \\ \frac{u+v}{8k} & \frac{(u+v)(4k^2+uv)}{4k^2uv} \end{pmatrix}, \end{aligned}$$

where $u = 16\sigma_{\mathrm{coh}}^2$ and $v = 4\sigma_{\mathrm{cor}}^2$ [16]. In $\mathit{\Gamma}$, η represents the decrease in correlations, and ε represents the excess noise. These two parameters quantify the effects of an eavesdropper, channel noise, and setup imperfections. Without loss of generality, we assume that η and ε are the same for both bases.

Alice and Bob can obtain values for η and ε using their estimate for σ'_{cor}. We define the parameter ξ, which quantifies the increase in the correlation time: $\sigma'^2_{\mathrm{cor}} = (1+\xi)\sigma_{\mathrm{cor}}^2$. Then, the relationship between η, ε, and ξ is given by

$$\varepsilon = \frac{-2\eta(d^2 - \frac{1}{4}) + \xi}{d^2 + \frac{1}{4}}. \tag{5}$$

Alice and Bob estimate ξ from their data and choose values of η and ε that maximize the Holevo information (thereby minimizing r_{DO}) and satisfy Eq. (5) and the following conditions [16]: (i) Eve cannot increase Alice and Bob's Shannon information by interacting with only Bob's photons due to the data processing inequality; (ii) the symplectic eigenvalues of the covariance matrix are greater than $\frac{1}{2}$ such that the Heisenberg uncertainty relation is satisfied; (iii) Eve can only degrade (and not improve) Alice and Bob's measured arrival-time correlation.

Alice and Bob sample only part of their data to estimate σ'_{cor}. In the finite-key regime, it is important to know how well their estimate represents the entire dataset.

Because Alice and Bob's arrival times, T_A and T_B, in a post-selected frame are jointly-Gaussian random variables, and the sequence of these measurements are statistically independent, their estimate for $\sigma'_{\rm cor}$, denoted $\hat{\sigma}'_{\rm cor}$, has a χ^2 distribution:

$$(m-1)\frac{\hat{\sigma}'^2_{\rm cor}}{\sigma^2_{\rm cor}} \sim \chi^2(1-\varepsilon_{PE}, m-1). \tag{6}$$

An upper bound on $\sigma'_{\rm cor}$ is then given by [30]:

$$(\sigma'_{\rm cor,max})^2 = \sigma^2_{\rm cor} + \frac{2}{\sqrt{m}}\,{\rm erf}^{-1}(1-\varepsilon_{PE})\hat{\sigma}'^2_{\rm cor}. \tag{7}$$

This bound is valid for the confidence interval $1-\varepsilon_{PE}$. Then, the largest possible estimate for ξ within the confidence interval is

$$\xi_{\rm max} = \frac{(\sigma'_{\rm cor,max})^2}{\sigma^2_{\rm cor}} - 1. \tag{8}$$

Alice and Bob can use their estimate for $\xi_{\rm max}$ to calculate the most pessimistic secure-key capacity through the symplectic decomposition of the covariance matrix [16].

4 Numerical results

Figure 2 plots the secure-key capacity for DO-QKD in the finite-key regime in bits per coincidence. Figure 2 assumes asymmetric basis selection, zero transmission loss, estimated correlation time $\hat{\sigma}'_{\rm cor} = 1.1\sigma_{\rm cor}$, security parameter $\varepsilon_s = 10^{-5}$, and error correction code failure probability $\varepsilon_{EC} = 10^{-10}$ [25,26]. The reconciliation efficiency is $\beta = 0.9$, which is possible using multilevel reverse reconciliation with low-density parity-check (LDPC) codes [38]. It was found that the secure-key capacity is not strongly altered by the choice of ε_s [25,30]. Likewise, for $d = 8$ we calculated $\max(r_N) = 1.94$ for security parameters between 10^{-4} and 10^{-7}, and found similar results for other d.

An important figure of merit is the smallest N at which Alice and Bob can obtain a useful amount of secure information. Figure 2 shows that this occurs around $N \approx 10^4$, for the chosen parameter values. The inability to obtain secure key at lower N values is due to the finite key length and its effect on Alice and Bob's parameter estimation. As N gets smaller, Alice and Bob must sacrifice a larger fraction of their measurements to estimate ξ to the desired accuracy. If N is too small, Alice and Bob have too few measurements left to use for key generation after sacrificing the required number for parameter estimation.

The probability of choosing the TB, p, directly determines the number of measurements sacrificed, $m = (1-p)^2N$. For each value of N, the value of p is determined numerically to maximize the secure-key capacity. Figure 3 plots the TB selection probability p, the secure-key capacity using asymmetric basis selection, and the secure-key capacity using symmetric basis selection as functions of N for $d = 8$. Asymmetric basis selection clearly boosts the amount of secure information per coincidence, with p approaching 1 as the asymmetric secure-key capacity approaches

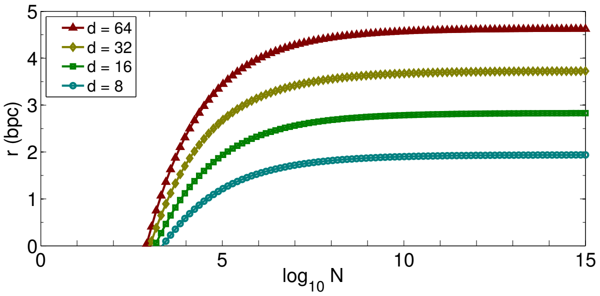

Fig. 2 Plot of DO-QKD finite-key secure-key capacities in bpc (bits per frame in which Alice and Bob each detect only one event) assuming Alice and Bob observe $\hat{\sigma}'_{\text{cor}} = 1.1\sigma_{\text{cor}}$ and detector jitter $T_J = 2\sigma_{\text{cor}}/3$, where σ_{cor} is the correlation time. The security parameter is $\varepsilon_s = 10^{-5}$, the failure probability of the error correction is $\varepsilon_{EC} = 10^{-10}$, and the reconciliation efficiency is $\beta = 0.9$. Alice's and Bob's system detection efficiencies are 93% [23], and the dark count rate is 1000 s^{-1}. All other parameters were chosen to match [16]. From top to bottom: $d = 64$, $d = 32$, $d = 16$, $d = 8$

its asymptotic value. In the symmetric case, where $p = 1/2$, Alice and Bob have on average only $N/2$ coincidences that were measured in the same basis: Around $N/4$ coincidences were measured in the TB, and $N/4$ in the FB. We continue to assume that the measurements made in the FB are used for parameter estimation, leaving only around $n = N/4$ measurements made in the TB for the key. With this assumption, the maximum possible secure-key capacity, even for large N, reaches only 25% of the asymptotic value. For all N that yield a positive amount of secure key, it is optimal to choose $p > 1/2$. However, while the asymmetric basis selection increases the secure-key capacity for all N that yield a positive amount of secure key, we see numerically that it does not change the minimum N required to obtain a positive amount of secure key.

Discrete-variable QKD protocols are generally able to extract a useful amount of secure information at $N \approx 10^5$ [39,25,26,28]. CV-QKD protocols require more measurements; for realistic parameter values, secure information is not obtained until $N \approx 10^8$ [30,7]. Although time is a continuous variable, DO-QKD performs more like a discrete-variable protocol when considering the minimum N required to obtain secure key: some secure key can be obtained even at $N \approx 10^4$.

We also see that even including finite-key effects, DO-QKD can reach a transmission distance > 200 km. This is longer than the maximum distance reached by CV-QKD protocols, which have so far seen transmission up to 80 km [7]. Figure 4 plots the asymmetric secure-key capacity as a function of channel length for dimension $d = 8$ and various values of N.

5 Conclusion

We have shown security against collective attacks for a high-dimensional QKD protocol in the finite-key regime. The protocol considered, DO-QKD, is robust to noise and can provide transmission of secure information at distances > 200 km of fiber.

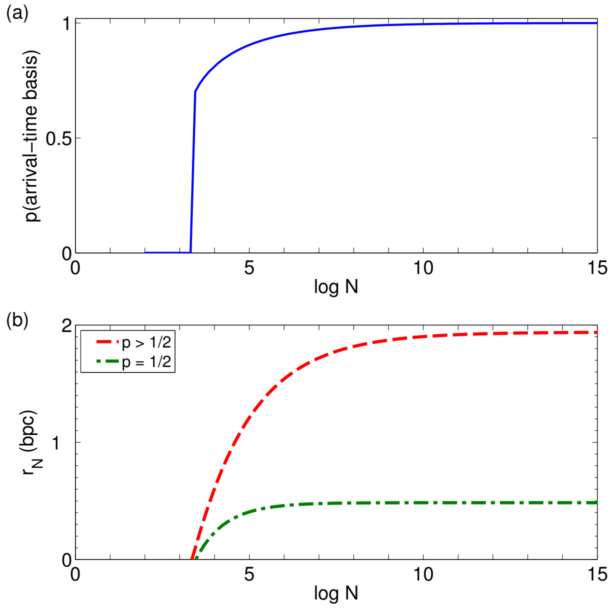

Fig. 3 (Color online) (a) Optimal value of p = probability of choosing the TB assuming asymmetric basis selection, for $d = 8$. (b) Comparison of the secure key capacity in bpc assuming asymmetric basis selection (dashed line), using the p shown in (a), and symmetric basis selection (dash-dotted line) for $d = 8$. For all N, the secure-key capacity is maximized by choosing $p > 1/2$. With symmetric basis selection ($p = 1/2$), the secure-key capacity is limited to 25% of the asymptotic value.

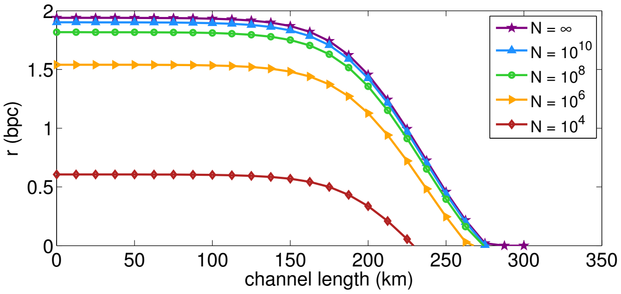

Fig. 4 Finite-key secure-key capacities in bpc versus channel length (loss) for different numbers of coincidences, N. $d = 8$ for all; transmission loss 0.2 dB/km; other parameters same as Figure 2 and [16]. From top to bottom: $N = \infty$, $N = 10^{10}$, $N = 10^8$, $N = 10^6$, $N = 10^4$

Working in the finite-key regime does not significantly affect the previously calculated secure-key capacity [16]: for experimentally achievable parameters, Alice and Bob can reach $> 90\%$ of the asymptotic secure-key capacity for a reasonable number of coincidences, $N \approx 10^8$, and a positive amount of secure key can be extracted after detection of as few as $N \approx 10^4$ coincidences.

References

1. C.H. Bennett, G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing* (IEEE, New York, 1984), pp. 175–179
2. N. Gisin, G. Ribordy, W. Tittel, H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002)
3. A.K. Ekert, Phys. Rev. Lett. **67**, 661 (1991)
4. C.H. Bennett, G. Brassard, N.D. Mermin, Phys. Rev. Lett. **68**, 557 (1992)
5. T.C. Ralph, Phys. Rev. A **61**, 010303 (1999)
6. T.C. Ralph, Phys. Rev. A **62**, 062306 (2000)
7. P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, E. Diamanti, Nature Photonics **7**(5), 378 (2013)
8. H. Bechmann-Pasquinucci, W. Tittel, Phys. Rev. A **61**, 062308 (2000)
9. N.J. Cerf, M. Bourennane, A. Karlsson, N. Gisin, Phys. Rev. Lett. **88**, 127902 (2002)
10. L. Zhang, C. Silberhorn, I.A. Walmsley, Phys. Rev. Lett. **100**, 110504 (2008)
11. W. Tittel, J. Brendel, H. Zbinden, N. Gisin, Phys. Rev. Lett. **84**, 4737 (2000)
12. R.T. Thew, A. Acín, H. Zbinden, N. Gisin, Phys. Rev. Lett. **93**, 010503 (2004)
13. I. Ali-Khan, C.J. Broadbent, J.C. Howell, Phys. Rev. Lett. **98**, 060503 (2007)
14. R.T. Thew, S. Tanzilli, W. Tittel, H. Zbinden, N. Gisin, Phys. Rev. A **66**, 062304 (2002)
15. B. Qi, Opt. Lett. **31**(18), 2795 (2006)
16. J. Mower, Z. Zhang, P. Desjardins, C. Lee, J.H. Shapiro, D. Englund, Phys. Rev. A **87**, 062322 (2013)
17. J. Nunn, L.J. Wright, C. Söller, L. Zhang, I.A. Walmsley, B.J. Smith, Opt. Express **21**(13), 15959 (2013)
18. A. Mair, A. Vaziri, G. Weihs, A. Zeilinger, Nature **412**(6844), 313 (2001)
19. A. Vaziri, G. Weihs, A. Zeilinger, Phys. Rev. Lett. **89**, 240401 (2002). DOI 10.1103/PhysRevLett.89.240401
20. G. Molina-Terriza, A. Vaziri, J. Řeháček, Z. Hradil, A. Zeilinger, Phys. Rev. Lett. **92**, 167903 (2004)
21. M. Mafu, A. Dudley, S. Goyal, D. Giovannini, M. McLaren, M.J. Padgett, T. Konrad, F. Petruccione, N. Lütkenhaus, A. Forbes, Phys. Rev. A **88**, 032305 (2013)
22. T. Zhong, F.N.C. Wong, A. Restelli, J.C. Bienfang, Opt. Express **20**(24), 26868 (2012)
23. F. Marsili, V.B. Verma, J.A. Stern, S. Harrington, A.E. Lita, T. Gerrits, I. Vayshenker, B. Baek, M.D. Shaw, R.P. Mirin, S.W. Nam, Nature Photonics **7**(3), 210 (2013)
24. Z. Zhang, J. Mower, D. Englund, F.N.C. Wong, J.H. Shapiro, Phys. Rev. Lett. **112**, 120506 (2014)
25. V. Scarani, R. Renner, Phys. Rev. Lett. **100**, 200501 (2008). DOI 10.1103/PhysRevLett.100.200501
26. L. Sheridan, V. Scarani, Phys. Rev. A **82**, 030301 (2010). DOI 10.1103/PhysRevA.82.030301
27. L. Sheridan, V. Scarani, Phys. Rev. A **83**, 039901(E) (2011). DOI 10.1103/PhysRevA.83.039901
28. R.Y.Q. Cai, V. Scarani, New J. Phys. **11**, 045024 (2009)
29. L. Sheridan, T.P. Le, V. Scarani, New J. Phys. **12**(12), 123019 (2010)
30. A. Leverrier, F. Grosshans, P. Grangier, Phys. Rev. A **81**, 062343 (2010)
31. F. Furrer, T. Franz, M. Berta, A. Leverrier, V.B. Scholz, M. Tomamichel, R.F. Werner, Phys. Rev. Lett. **109**, 100502 (2012)
32. M. Tomamichel, C.C.W. Lim, N. Gisin, R. Renner, Nature Communications **32**, 634 (2012)
33. A. Leverrier, R. García-Patrón, R. Renner, N.J. Cerf, Phys. Rev. Lett. **110**, 030502 (2013)
34. C.K. Law, J.H. Eberly, Phys. Rev. Lett. **92**, 127903 (2004)
35. J.D. Franson, Phys. Rev. A **45**, 3126 (1992)
36. D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, A. Sanpera, Phys. Rev. Lett. **77**, 2818 (1996)
37. H.K. Lo, H.F. Chau, M. Ardehali, Journal of Cryptology **18**, 133 (2005)
38. J. Lodewyck, M. Bloch, R. García-Patrón, S. Fossier, E. Karpov, E. Diamanti, T. Debuisschert, N.J. Cerf, R. Tualle-Brouri, S.W. McLaughlin, P. Grangier, Phys. Rev. A **76**, 042305 (2007)
39. V. Scarani, H. Bechmann-Pasquinucci, N.J. Cerf, M. Dušek, N. Lütkenhaus, M. Peev, Rev. Mod. Phys. **81**, 1301 (2009)