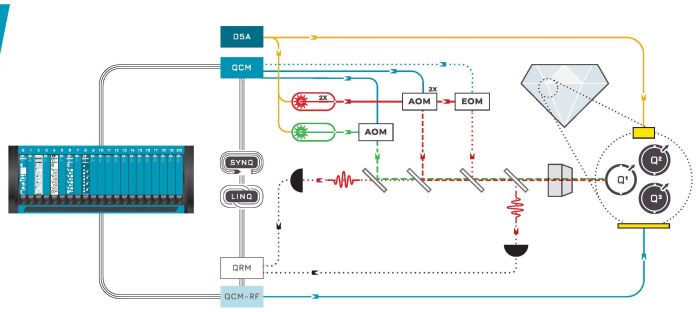
Applied Physics Letters

# Metropolitan single-photon distribution at 1550 nm for random number generation

Cite as: Appl. Phys. Lett. **121**, 194003 (2022); https://doi.org/10.1063/5.0112939
Submitted: 22 July 2022 • Accepted: 27 October 2022 • Published Online: 11 November 2022

Samuel Gyger, Katharina D. Zeuner, Thomas Lettner, et al.






AIP Publishing

Applied Physics Letters ARTICLE scitation.org/journal/apl

# Metropolitan single-photon distribution at 1550 nm for random number generation

Cite as: Appl. Phys. Lett. **121**, 194003 (2022); doi: 10.1063/5.0112939
Submitted: 22 July 2022 · Accepted: 27 October 2022 ·
Published Online: 11 November 2022

View Online Export Citation CrossMark

Samuel Gyger,[1,a)] Katharina D. Zeuner,[1] Thomas Lettner,[1] Sandra Bensoussan,[1,2] Martin Carlnäs,[1,2] Liselott Ekemar,[1,2] Lucas Schweickert,[1] Carl Reuterskiöld Hedlund,[3] Mattias Hammar,[3] Tigge Nilsson,[2] Jonas Almlöf,[2] Stephan Steinhauer,[1] Gemma Vall Llosera,[2] and Val Zwiller[1,a)]

## AFFILIATIONS

[1]Quantum Nanophotonics, KTH Royal Institute of Technology, Roslagstullsbacken 21, 10691 Stockholm, Sweden
[2]Ericsson AB, Torshamnsgatan 21, 164 40 Stockholm, Sweden
[3]Department of Electrical Engineering, KTH Royal Institute of Technology, 164 40 Kista, Sweden

[a)]**Authors to whom correspondence should be addressed:** gyger@kth.se and zwiller@kth.se

## ABSTRACT

Quantum communication networks will connect future generations of quantum processors, enable metrological applications, and provide security through quantum key distribution. We present a testbed that is part of the municipal fiber network in the greater Stockholm metropolitan area for quantum resource distribution through a 20 km long fiber based on semiconductor quantum dots emitting in the telecom C-band. We utilize the service to generate random numbers passing the NIST test suite SP800-22 at a subscriber 8 km outside of the city with a bit rate of 23.4 kbit/s.



Quantum communication is expected to follow in the footsteps of traditional data communication, which currently serves as the backbone of our modern information society. By extending the capabilities of the internet based on the transmission of so-called qubits, the fundamental resource for quantum information science, and creating entanglement between remote nodes, a quantum internet[1] is created. Multiple application areas[2] that will benefit from the new capabilities have been identified, including secure key exchange,[3] clock synchronization,[4] new fundamental limits in metrology,[5] and the linking of future quantum processors.[6] The multi-stage and multi-decade process of establishing a quantum internet necessitates intermediate steps for economic viability and technology validation. While national and global networks will require significant scientific research and engineering in the area of quantum repeaters,[7] metropolitan and inter-city networks are already feasible. Field deployments of quantum key distribution (QKD) systems outside of the lab have been thoroughly tested in metropolitan areas such as Vienna, Geneva, Boston, Calgary, and Tokyo[8] as well as a trusted node-based network in China[9] spanning more than 2000 km. Fiber lengths of more than 830 km between parties have been demonstrated using twin-field QKD,[10,11] which achieves a favorable rate-distance relationship by relying on single-photon interference in an untrusted middle station. In contrast to non-deterministic approaches, quantum dots have been employed as on-demand sources of entangled photons, e.g., close to the 850 nm band for QKD within university premises in Linz (Austria) and Rome (Italy).[12,13] Furthermore, recent results show the distribution of entangled photons generated by a quantum dot within the O-band (1310 nm) in deployed fiber links[14] as part of the Cambridge quantum network.[15]

To profit from the unconditional security of QKD and allow for its implementation, the availability of random numbers is a crucial prerequisite.[16] This necessitates their generation as well as distribution within the quantum network.[17] The random output port of a photon passing through a symmetric beam splitter[18] and the unpredictability of a photon's arrival time[19] are both well-known ways to make optical quantum number generators.[20] Most of the time, these methods are used with attenuated lasers or spontaneous-parametric downconversion light sources. Modern optical quantum random number generators based on photon counting achieve Mbit/s random number rates, while phase measurement-based generators can achieve Gbit/s.[21] Commercial devices are available offering rates in the few tens to several 100 Mbit/s.[22] In contrast to these demonstrations, we generate triggered single photons from a quantum dot with pure single photons. This allows for monitoring of the source single photon character

and source verification through Bell tests, with the possibility of higher brightness than parametric sources.[23]

In this study, we implement a provider-subscriber service based on a quantum dot source providing triggered single photons in the telecom C-band through the metropolitan fiber infrastructure (STOKAB) located in Stockholm. A ≈20 km long fiber connects the source station in Stockholm to the subscriber in Kista, a neighboring industrial center. The fiber network provides a testbed for quantum information protocols based on single photons co-deployed in a real-world environment. The single-photon resource is used to generate random numbers via two different experiments involving a beam splitter and/or photon arrival time. Relying on true random processes resulting from the quantum dot emitter characteristics, we demonstrate validated random number distribution over metropolitan distances, serving as key functionality enabling future quantum networks.

The complete setup is shown in Fig. 1. The metropolitan fiber network consists of three nodes. The service provider is located at KTH Royal Institute of Technology, and two subscribers are connected using channels within the telecom C-band. The first one is located in Kista (E) outside of Stockholm using the public fiber network provided by STOKAB in the greater Stockholm area. The second one is located within KTH Royal Institute of Technology (K) connected using a table-top fiber spool. The source of single photons, hosted at KTH Royal Institute of Technology, consists of an MOVPE-grown InAs quantum dot on a GaAs substrate. The emission wavelength of 1550 nm is made possible by a metamorphic buffer layer[24] releasing the stress of the lattice mismatch by increasing the In content. The sample is described in detail in Ref. 25. It is mounted inside a cryostat (Montana Instruments CR-120) at an operating temperature of 18 K. The sample is moved using cryogenic positioners (Attocube), and the emitted photons are collected using a cryogenic objective (Attocube LT-APO/NIR NA = 0.8) and coupled to an SMF-28 fiber forming a confocal microscopy setup.

The quantum dot is excited into the p-shell using an 80 MHz picosecond pulsed laser at 1470 nm. We filter the exciton (X) emission and bi-exciton (XX) emission [spectrum in Fig. 2(a)] through an in-house built transmission spectrometer (TG). The single photons of the exciton are then sent through a 20.3 km long dedicated dark fiber of the STOKAB metropolitan fiber network with a total loss of 10.3 dB (public network 17.5 km/6.72 dB, remaining is internal infrastructure). A reflective notch filter with a spectral bandwidth of 0.7 nm and a rejection of 40 dB is used at the subscriber location to filter the input signal from the neighboring channels' crosstalk.[26] The signal is again coupled to a single-mode fiber and then sent toward two superconducting nanowire single photon detector (SNSPD) (Single Quantum EOS, nominal 30%/33% detection efficiency) using a fiber-based beam splitter with a splitting ratio of 49%/50.4%. The arrival time of the photons is recorded using a time-to-digital converter (Qutag) and stored on a local computer to be post-processed using the Extensible Timetag Analyzer ETA.[27]

The bi-exciton photons are sent through a 13.5 km long fiber spool within the lab (2.75 dB loss), split on a fiber-based beam splitter, and then detected with two SNSPDs (Single Quantum EOS, 75% and 76% efficiency) at the subscriber K. We monitor the single-photon character at the subscriber locations [Fig. 2(c)] to verify the viability of our input signal later used for random

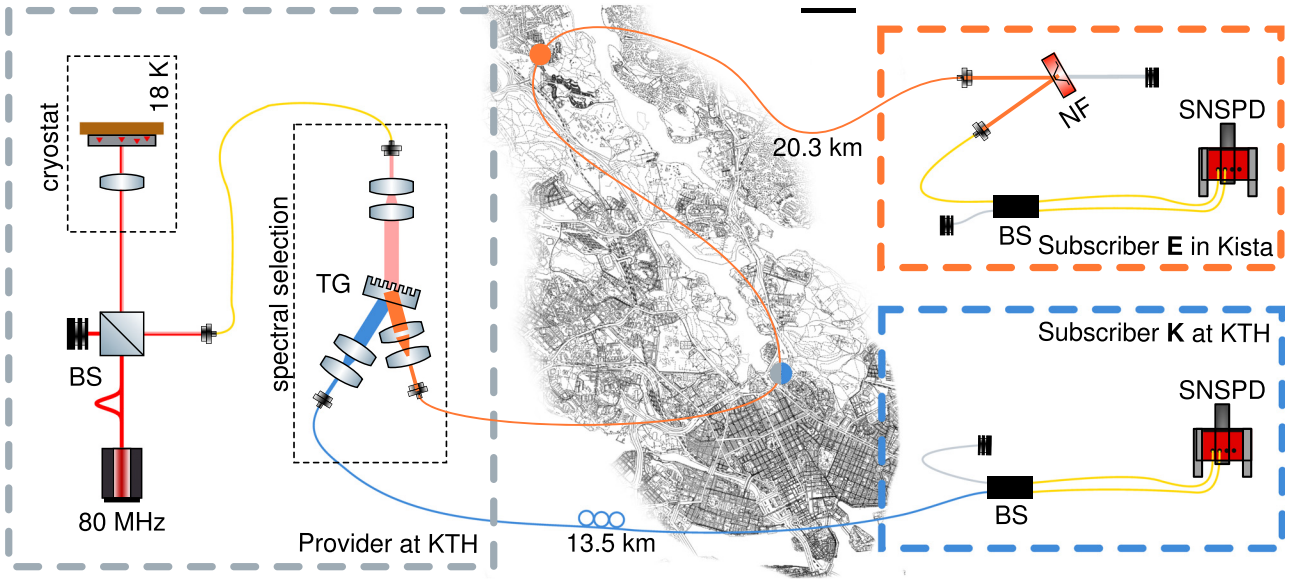
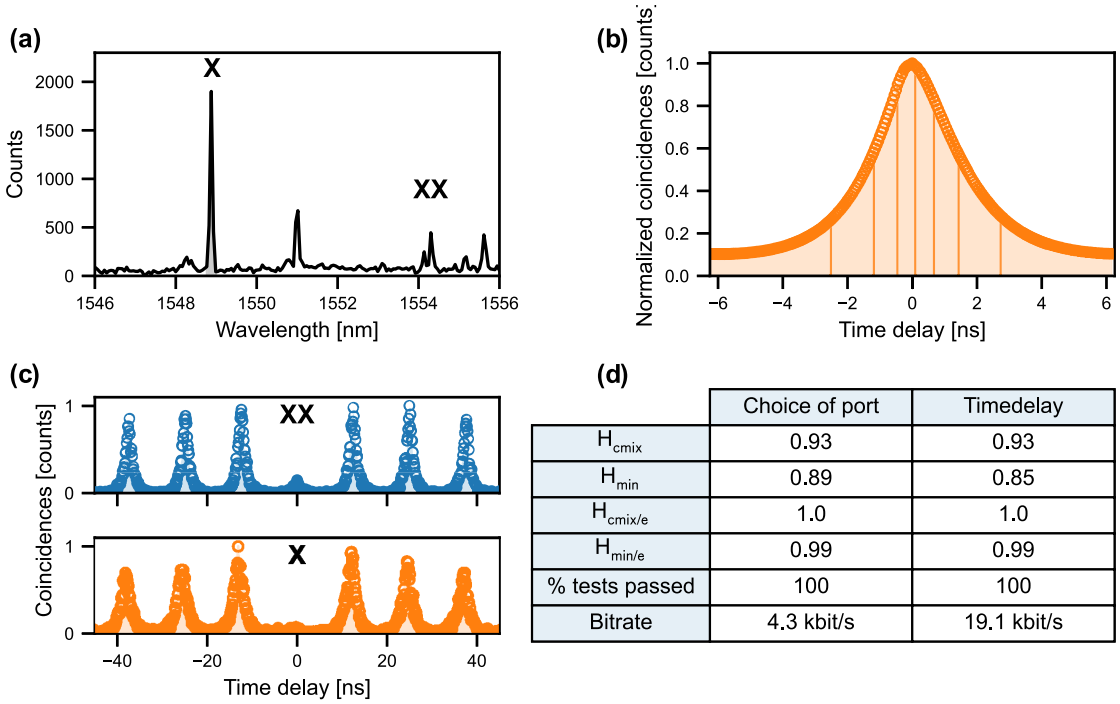



**FIG. 1.** Metropolitan quantum link in the Stockholm region for quantum random number generation. Metropolitan fiber links with two subscribers, one in Stockholm (K) and one in Kista (E) marked on the map with a blue and an orange circle, respectively. Single photons at 1550 nm are generated at the provider in Stockholm using a semiconductor quantum dot. The dot is excited using p-shell excitation. The exciton emission is filtered using a transmission spectrometer (TG) and sent through dedicated fibers of the municipality fiber network to the subscriber in Kista. There, the emission is filtered using a notch filter in reflection to suppress crosstalk of classical communication signals in the network. The bi-exciton emission is sent through a fiber spool and detected at KTH. At both subscribers, the photons are sent on a fiber beam splitter and detected using superconducting nanowire single photon detectors (SNSPD). The scale bar is 1 km. Map Data by OpenStreetMap Contributors. Map adapted with permission from Oliver O'Brien.




| | Choice of port | Timedelay |
|---|---|---|
| $H_{cmix}$ | 0.93 | 0.93 |
| $H_{min}$ | 0.89 | 0.85 |
| $H_{cmix/e}$ | 1.0 | 1.0 |
| $H_{min/e}$ | 0.99 | 0.99 |
| % tests passed | 100 | 100 |
| Bitrate | 4.3 kbit/s | 19.1 kbit/s |

**FIG. 2.** Randomness generation at the subscriber. (a) Spectra of the QD at ≈18 K with the exciton transition (X) at 1549 nm marked. (b) A start-stop measurement between all photons at the subscriber location is modulo folded into the repetition rate of the laser. Variable bin widths are used to achieve a uniform probability and are labeled with $2^n$ different bit combinations. Borders between eight temporal regions, representing 3 bits, are indicated by vertical lines. The experiment used $2^6$ bins for six random bits from each time difference. When including the randomness contained within the jitter of the SNSPDs and digitization noise of the timing electronics, 8 bits can be extracted. (c) Second-order photon correlation measurement, proofing the single-photon character at the subscriber location. The $g^{(2)}(0)$ value is monitored, while at the same time, the arrival port and time are used to generate random bits. The uncorrected multi-photon probability is $g^{(2)}(0) = 0.19 \pm 0.05$ at the subscriber K (top) and $g^{(2)}(0) = 0.21 \pm 0.05$ at the subscriber E (bottom). (d) The table summarizes the properties of the port of entry and the arrival time as randomness source at the subscriber E (X). The compression entropy estimated using the cmix algorithm $H_{cmix}$, the estimated minimal entropy $H_{min}$, the extracted compression entropy $H_{cmix/e}$, the estimated extracted minimal entropy $H_{min/e}$, the test pass rate, and the bit rate are compared.

number generation. We measure an uncorrected multi-photon probability of $g^{(2)}(0) = 0.19 \pm 0.05$ at the subscriber K (top, XX) and $g^{(2)}(0) = 0.21 \pm 0.05$ at the subscriber E (bottom, X), calculated from the counts in a bin (width 12.5 ns) at zero time delay vs the normalized counts of ten bins (two-third of the repetition rate) on each side. At the provider, we measure $g^{(2)}(0) = 0.21 \pm 0.08$ for the bi-exciton (XX) and $g^{(2)}(0) = 0.12 \pm 0.01$ for the exciton (X) (see the supplementary material).

We investigate two methods to generate random numbers from the pure single-photon resource. Due to the remote location outside of the provider lab and, thus, more realistic conditions, we focus on results generated at subscriber location E. The evaluation of data generated at subscriber location K can be found in the supplementary material.

As a first method, we use the randomness extracted by allocating the bit values 0 and 1 to the respective output ports of a beam splitter. In a second method, we use the time between subsequent photon emissions as the source of randomness.

The quality of the randomness source is determined by computing the lower bound on the entropy $H_{min}$ using the NIST SP 800–90B[28] test suite for independent and identically distributed (IID) and non-IID random numbers. Utilizing modern compression algorithms, the upper bound on the entropy as a close approximation to the true entropy can be calculated.[29] We compress the data using the Lempel–Ziv–Markov chain (LZMA) algorithm (as implemented in the Python standard library) to calculate $H_{LZMA}$ and the cmix software,[30] which is a state-of-the-art compression implementation, to calculate $H_{cmix}$. Both values are calculated by comparing the file size before and after compression excluding the control headers of the file format.

While our source generates to a very high degree pure single photons, the slightly different detection rates on the two channels (1:1.12) at subscriber E, caused by an imperfect beam splitter ratio combined with the different detection efficiencies, lead to biased random numbers in the first method. Events where both detectors click in the same excitation cycle are not excluded but generate two bits, while two events from the same detector are not possible due to the dead time of the detectors of 30 ns.

In the first method for random number generation, we estimate the lower bound of the entropy as $H_{min} = 7.1\,\text{bit/B}$ and the upper bound as $H_{LZMA} = 7.4\,\text{bit/B}$ and $H_{cmix} = 7.4\,\text{bit/B}$. We use two-universal hashing to extract the unbiased randomness,[31] by choosing a ratio between raw and result bits to reflect the estimation of the entropy using the NIST non-IID test. After correction for biasing, the

NIST IID test passes and estimates an entropy of $H_{\min/e} = 7.88\,\text{bit/B}$, the LZMA based compression method and cmix estimate $H_{\text{LZMA}/e} = H_{\text{cmix}/e} = 8.00\,\text{bit/B}$. This method generates random numbers with 4.3 kbit/s at the subscriber E for the beam splitter method. In comparison, subscriber K generated random numbers with 24.6 kbit/s (see the supplementary material).

To improve the bitrate, we use the time point of emission as a further source of randomness.

For the second method, the randomness of the spontaneous decay of the XX and X levels is used by subtracting the time difference between subsequent detection events. We take the time difference modulo the laser pulse period to remove the photon loss-induced time delay. The likelihood for different time outcomes is shown in Fig. 2(b). We divide the likelihood into bins with variable widths to make them equally probable and index them. Upon detection, the event is classified with the bin index, which is then used as the random bit result. As an example, we show eight regions with equal area, corresponding to 3 bits, in Fig. 2(b). We choose the minimal bin size to be 56 ps to avoid using randomness from the detection jitter and time digitization. This leads to 64 regions, corresponding to 6 bit per time difference. If one accepts the randomness within the digitization process, smaller bin sizes down to 1 ps are possible. The entropy is estimated similar to the port choice experiment and results in $H_{\min} = 6.8\,\text{bit/B}$, $H_{\text{LZMA}} = 7.4\,\text{bit/B}$, and $H_{\text{cmix}} = 7.3\,\text{bit/B}$. We again use the two-universal hashing to de-bias the data and estimate an entropy based on the NIST IID tests of $H_{\min/e} = 7.89\,\text{bit/B}$ and $H_{\text{LZMA}/e} = H_{\text{cmix}/e} = 8.00\,\text{bit/B}$ based on the compression methods. Subscriber E receives 19.1 kbit/s of unbiased random bits extracted from the time difference experiment. Due to lower loss and more efficient detectors, subscriber K receives 80.1 kbit/s of unbiased random bits (see the supplementary material) at the same time, while the emission rate of the bi-exciton is approximately four times lower.

We verify the properties of the generated random numbers at subscriber E using the NIST test suite,[32] where both sets of de-biased random data pass all included tests. The table in Fig. 2(d) summarizes the random data's properties, and the full test results are reported in the supplementary material. We emphasize that these tests do not replace the need to analyze and model such a system. This is because the physical process creating random numbers, not their statistical properties, is what makes them suitable for any cryptographic application.[33] A future direction is self-testing quantum random number generators,[21] where the violation of Bell's inequality or derived figures of merit can be used to prove randomness with different trust assumptions from purely classical adversaries to trustfree devices.

By combining the two methods on our data, we generated random numbers at a rate of 23.4 kbit/s at subscriber E and 104.7 kbit/s at subscriber K. By increasing the excitation repetition rate to 640 MHz (limited by the lifetime of the emitter) and using state of the art detectors at the receiver with a detection efficiency of ≈98%[34] (factor of 3), a jitter of ≈8 ps (Ref. 35) (an extra bit by the time binning) at a rate of ≈1 Mbit/s at subscriber E can be achieved. The rate is ultimately limited by the maximum emission rate of the source close to the lifetime of the transition (typically ≈450 ps for the bi-exciton and ≈1200 ps for the exciton[25]) and the losses between the provider and subscriber, where the former can be made faster using Purcell engineering. While monitoring the single photon character limits the attack surface on method one based on the beam splitter output, a single photon source with emission control, such as through Purcell enhancement, might be used to affect the creation time of photons in method two. As a first step, the source of the photons can be verified through a Bell test. The required trust in the physical device may be further reduced by self-certifying random number generation.

In this work, we demonstrate the operation of a metropolitan fiber link for the exchange of quantum resources. We use self-assembled quantum dots that emit at 1550 nm and transmit the generated photons over 20 km of fiber. We demonstrate high single-photon purity at the remote subscriber location and use the received single photons to generate quantum random numbers with a total bit rate of 23.4 kbit/s. This network and measurement apparatus are ready for use as a test-bed for future quantum network studies in realistic conditions outside of a controlled lab environment.

See the supplementary material for results from statistical randomness tests for subscriber E, single photon purity at provider, and randomness generation results for subscriber K.

We thank STOKAB for their valuable support in providing the fiber links. We thank the KTH Network infrastructure team for the support and assistance within the university network. We thank Patrik Usher for the technical support.

S.G. acknowledges funding from the Swedish Research Council under Grant Agreement No. 2016-06122 (Optical Quantum Sensing). M.H. acknowledges funding from the Swedish Research Council (VR, Grant Nos. 2016-03388 and 2020-04861). V.Z. acknowledges funding by the European Research Council under the Grant Agreement No. 307687 (NaQuOp), the Knut and Alice Wallenberg Foundation (KAW, "Quantum sensors"), and the Swedish Research Council (VR, Grant Nos. 638-2013-7152 and 2018-04251).

## AUTHOR DECLARATIONS

### Conflict of Interest

The authors have no conflicts to disclose.

### Author Contributions

Samuel Gyger and Katharina D. Zeuner contributed equally. Samuel Gyger and Gemma Vall Llosera conceived the demonstrator experiment. The sample was grown by Carl Reuterskiöld-Hedlund and Mattias Hammar. Sample characterization was performed by Katharina D. Zeuner and Thomas Lettner with the help of Stephan Steinhauer and Samuel Gyger. The experiment was performed by Samuel Gyger, Katharina D. Zeuner, and Thomas Lettner with the help of Lucas Schweickert, Sandra Bensoussan, Martin Carlnäs, Liselott Ekemar, and Stephan Steinhauer. The data analysis was performed by Samuel Gyger, Thomas Lettner, Tigge Nilsson, and Jonas Almlöf. Samuel Gyger wrote the manuscript with input from all authors. The project was conceived by Samuel Gyger, Katharina D. Zeuner, Gemma Vall Llosera, and Val Zwiller. Val Zwiller and Gemma Vall Llosera supervised the project.

**Samuel Gyger:** Conceptualization (equal); Formal analysis (equal); Investigation (equal); Methodology (equal); Project administration (equal); Supervision (equal); Writing – original draft (equal).

**Tigge Nilsson:** Formal analysis (supporting); Investigation (supporting); Software (equal). **Jonas Almlöf:** Data curation (supporting). **Stephan Steinhauer:** Investigation (supporting); Supervision (supporting). **Gemma Vall Llosera:** Funding acquisition (supporting); Supervision (supporting). **Val Zwiller:** Conceptualization (equal); Funding acquisition (equal); Methodology (equal); Project administration (equal); Supervision (equal). **Katharina D. Zeuner:** Conceptualization (supporting); Investigation (equal); Methodology (equal); Supervision (supporting). **Thomas Lettner:** Formal analysis (equal); Investigation (supporting); Software (supporting). **Sandra Bensoussan:** Investigation (supporting). **Martin Carlnäs:** Investigation (supporting). **Liselott Ekemar:** Investigation (supporting). **Lucas Schweickert:** Methodology (supporting); Software (supporting). **Carl Reuterskiöld-Hedlund:** Resources (equal). **Mattias Hammar:** Resources (equal).

## DATA AVAILABILITY

The data that support the findings of this study are available from the corresponding authors upon reasonable request.

## REFERENCES


[1]S. Wehner, D. Elkouss, and R. Hanson, "Quantum internet: A vision for the road ahead," Science **362**, eaam9288 (2018).
[2]ITU Focus Group, "Quantum information technology for networks use cases: Network aspects of quantum information technologies," Report No. FG QIT4N D1.2 (ITU-T Focus Group on Quantum Information, 2021).
[3]E. Diamanti, H.-K. Lo, B. Qi, and Z. Yuan, "Practical challenges in quantum key distribution," npj Quantum Inf. **2**, 16025 (2016).
[4]P. Kómár, E. M. Kessler, M. Bishof, L. Jiang, A. S. Sørensen, J. Ye, and M. D. Lukin, "A quantum network of clocks," Nat. Phys. **10**, 582–587 (2014).
[5]D. Gottesman, T. Jennewein, and S. Croke, "Longer-baseline telescopes using quantum repeaters," Phys. Rev. Lett. **109**, 070503 (2012).
[6]D. Cuomo, M. Caleffi, and A. S. Cacciapuoti, "Towards a distributed quantum computing ecosystem," IET Quantum Commun. **1**, 3–8 (2020).
[7]H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, "Quantum repeaters: The role of imperfect local operations in quantum communication," Phys. Rev. Lett. **81**, 5932–5935 (1998).
[8]H.-K. Lo, M. Curty, and K. Tamaki, "Secure quantum key distribution," Nat. Photonics **8**, 595–604 (2014).
[9]Y.-A. Chen, Q. Zhang, T.-Y. Chen, W.-Q. Cai, S.-K. Liao, J. Zhang, K. Chen, J. Yin, J.-G. Ren, Z. Chen, S.-L. Han, Q. Yu, K. Liang, F. Zhou, X. Yuan, M.-S. Zhao, T.-Y. Wang, X. Jiang, L. Zhang, W.-Y. Liu, Y. Li, Q. Shen, Y. Cao, C.-Y. Lu, R. Shu, J.-Y. Wang, L. Li, N.-L. Liu, F. Xu, X.-B. Wang, C.-Z. Peng, and J.-W. Pan, "An integrated space-to-ground quantum communication network over 4,600 kilometres," Nature **589**, 214–219 (2021).
[10]M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, "Overcoming the rate–distance limit of quantum key distribution without quantum repeaters," Nature **557**, 400–403 (2018).
[11]S. Wang, Z.-Q. Yin, D.-Y. He, W. Chen, R.-Q. Wang, P. Ye, Y. Zhou, G.-J. Fan-Yuan, F.-X. Wang, W. Chen, Y.-G. Zhu, P. V. Morozov, A. V. Divochiy, Z. Zhou, G.-C. Guo, and Z.-F. Han, "Twin-field quantum key distribution over 830-km fibre," Nat. Photonics **16**, 154–161 (2022).
[12]C. Schimpf, M. Reindl, D. Huber, B. Lehner, S. F. C. D. Silva, S. Manna, M. Vyvlecka, P. Walther, and A. Rastelli, "Quantum cryptography with highly entangled photons from semiconductor quantum dots," Sci. Adv. **7**, eabe8905 (2021).
[13]F. B. Basset, M. Valeri, E. Roccia, V. Muredda, D. Poderini, J. Neuwirth, N. Spagnolo, M. B. Rota, G. Carvacho, F. Sciarrino, and R. Trotta, "Quantum key distribution with entangled photons generated on demand by a quantum dot," Sci. Adv. **7**, eabe6379 (2021).
[14]Z.-H. Xiang, J. Huwer, J. Skiba-Szymanska, R. M. Stevenson, D. J. P. Ellis, I. Farrer, M. B. Ward, D. A. Ritchie, and A. J. Shields, "A tuneable telecom wavelength entangled light emitting diode deployed in an installed fibre network," Commun. Phys. **3**, 121 (2020).
[15]J. F. Dynes, A. Wonfor, W. W.-S. Tam, A. W. Sharpe, R. Takahashi, M. Lucamarini, A. Plews, Z. L. Yuan, A. R. Dixon, J. Cho, Y. Tanizawa, J.-P. Elbers, H. Greißer, I. H. White, R. V. Penty, and A. J. Shields, "Cambridge quantum network," npj Quantum Inf. **5**, 101 (2019).
[16]N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," Rev. Mod. Phys. **74**, 145–195 (2002).
[17]L. Huang, H. Zhou, K. Feng, and C. Xie, "Quantum random number cloud platform," npj Quantum Inf. **7**, 107 (2021).
[18]J. Rarity, P. Owens, and P. Tapster, "Quantum random-number generation and key sharing," J. Mod. Opt. **41**, 2435–2444 (1994).
[19]M. A. Wayne, E. R. Jeffrey, G. M. Akselrod, and P. G. Kwiat, "Photon arrival time quantum random number generation," J. Mod. Opt. **56**, 516–522 (2009).
[20]M. Herrero-Collantes and J. C. Garcia-Escartin, "Quantum random number generators," Rev. Mod. Phys. **89**, 015004 (2017).
[21]X. Ma, X. Yuan, Z. Cao, B. Qi, and Z. Zhang, "Quantum random number generation," npj Quantum Inf. **2**, 16021 (2016).
[22]*Quantum Random Number Generation: Theory and Practice, Quantum Science and Technology*, edited by C. Kollmitzer, S. Schauer, S. Rass, and B. Rainer (Springer International Publishing, Cham, 2020).
[23]J. Liu, R. Su, Y. Wei, B. Yao, S. F. C. da Silva, Y. Yu, J. Iles-Smith, K. Srinivasan, A. Rastelli, J. Li, and X. Wang, "A solid-state source of strongly entangled photon pairs with high brightness and indistinguishability," Nat. Nanotechnol. **14**, 586–593 (2019).
[24]M. Paul, F. Olbrich, J. Höschele, S. Schreier, J. Kettler, S. L. Portalupi, M. Jetter, and P. Michler, "Single-photon emission at 1.55 Mm from MOVPE-grown InAs quantum dots on InGaAs/GaAs metamorphic buffers," Appl. Phys. Lett. **111**, 033102 (2017).
[25]K. D. Zeuner, K. D. Jöns, L. Schweickert, C. Reuterskiöld Hedlund, C. Nuñez Lobato, T. Lettner, K. Wang, S. Gyger, E. Schöll, S. Steinhauer, M. Hammar, and V. Zwiller, "On-demand generation of entangled photon pairs in the telecom C-band with InAs quantum dots," ACS Photonics **8**, 2337 (2021).
[26]M. Fujiwara, S. Miki, T. Yamashita, Z. Wang, and M. Sasaki, "Photon level crosstalk between parallel fibers installed in urban area," Opt. Express **18**, 22199–22207 (2010).
[27]Z. Lin, L. Schweickert, S. Gyger, K. D. Jöns, and V. Zwiller, "Efficient and versatile toolbox for analysis of time-tagged measurements," J. Instrum. **16**, T08016 (2021).
[28]M. S. Turan, E. Barker, J. Kelsey, K. A. McKay, M. L. Baish, and M. Boyle, "Recommendation for the entropy sources used for random bit generation," Report No. NIST SP 800-90b (National Institute of Standards and Technology, Gaithersburg, MD, 2018).
[29]R. Avinery, M. Kornreich, and R. Beck, "Universal and accessible entropy estimation using a compression algorithm," Phys. Rev. Lett. **123**, 178102 (2019).
[30]See B. Knoll, https://github.com/byronknoll/cmix/tree/v19.1 for "Byronknoll/cmix" (2021).
[31]D. Frauchiger, R. Renner, and M. Troyer, "True randomness from realistic quantum devices," arXiv:1311.4547 (2013).
[32]A. L. Rukhin, J. Soto, J. R. Nechvatal, M. E. Smid, S. D. Leigh, M. Levenson, M. Vangel, N. A. Heckert, D. L. Banks, and L. E. Bassham, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," Report No. Pubs 800-22 Rev 1a (National Institute of Standards and Technology, 2010).
[33]M.-J. O. Saarinen, "SP 800-22 and GM/T 0005-2012 tests: Clearly obsolete, possibly harmful," in *IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)* (IEEE, 2022), pp. 31–37.
[34]D. V. Reddy, R. R. Nerem, S. W. Nam, R. P. Mirin, and V. B. Verma, "Superconducting nanowire single-photon detectors with 98% system detection efficiency at 1550 nm," Optica **7**, 1649–1653 (2020).
[35]I. E. Zadeh, J. W. N. Los, R. B. M. Gourgues, J. Chang, A. W. Elshaari, J. R. Zichi, Y. J. van Staaden, J. P. E. Swens, N. Kalhor, A. Guardiani, Y. Meng, K. Zou, S. Dobrovolskiy, A. W. Fognini, D. R. Schaart, D. Dalacu, P. J. Poole, M. E. Reimer, X. Hu, S. F. Pereira, V. Zwiller, and S. N. Dorenbos, "Efficient single-photon detection with 7.7 ps time resolution for photon-correlation measurements," ACS Photonics **7**, 1780–1787 (2020).