
Article:
Razavi, M orcid.org/0000-0003-4172-2125, Leverrier, A, Ma, X et al. (2 more authors) (2019) Quantum key distribution and beyond: introduction. Journal of the Optical Society of America B: Optical Physics, 36 (3). QKD1-QKD2. ISSN 0740-3224

https://doi.org/10.1364/JOSAB.36.00QKD1

Quantum key distribution and beyond: introduction

MOHSEN RAZAVI,[1,*] ANTHONY LEVERRIER,[2] XIONGFENG MA,[3] BING QI,[4,5] AND ZHILIANG YUAN[6]

[1]*School of Electronic and Electrical Engineering, University of Leeds, Leeds, LS2 9JT, UK*
[2]*Inria Paris, France*
[3]*Center for Quantum Information, Institute for Interdisciplinary Information Sciences, Tsinghua University, Beijing 100084, China*
[4]*Quantum Information Science Group, Computational Sciences and Engineering Division, Oak Ridge National Laboratory, Oak Ridge, Tennessee 37831, USA*
[5]*Department of Physics and Astronomy, The University of Tennessee, Knoxville, Tennessee 37996, USA*
[6]*Toshiba Research Europe Limited, 208 Cambridge Science Park, Cambridge, CB4 0GZ, UK*
**m.razavi@leeds.ac.uk*

Abstract: This feature issue presents a collection of recent theoretical and experimental developments in the field of quantum key distribution (QKD) and its extension to other quantum cryptography protocols and devices. It encompasses work on a variety of QKD protocols, including continuous-variable, measurement-device independent, and twin-field QKD, as well as other newly proposed protocols, in platforms ranging from optical fiber through to wireless indoor and satellite links. It covers examples of hacking strategies and their countermeasures as well as applications of machine learning techniques in designing quantum networks. It also includes new developments in efficient superconducting photon-number resolving detectors as well as fast quantum random number generators. Distinctively, this feature issue demonstrates how different expertise in science and engineering can come together to produce an outcome that hopefully takes us one step closer to the wide-scale deployment of quantum communications technologies.

Quantum information science is in a transition phase to become a technology. Leading this trend, quantum key distribution (QKD) is arguably the most advanced quantum technology, promising information-theoretic security guaranteed by fundamental quantum mechanical laws of nature. Since the invention of the celebrated BB84 protocol, three decades ago, this field has been growing steadily, as witnessed by the recent intercontinental satellite QKD demonstration between China and Austria, as well as the 2000-km-long Beijing-Shanghai QKD link launched in 2017, among other initiatives pursued across the world. Despite these achievements, wide adoption of QKD technologies will benefit from continuous efforts in addressing a number of important challenges, including secure distribution of keys over long distances at high rates, integration of QKD networks with the existing infrastructure for data communications networks, providing easy access to end users at a low cost, and ensuring the security of practical settings. All these should come together in QKD services offered in future quantum communications networks. Such networks will then offer a platform for the deployment of other quantum communications technologies, i.e., beyond QKD applications, such as quantum digital signatures.

This feature issue on QKD and beyond has a collection of work that addresses the above challenges. Agnesi *et al.* demonstrate some new techniques for subnanosecond timing accuracy

for satellite communications [1]. This will enable high-rate low-noise long-distance satellite QKD links to be established. Novel structures for QKD networks have been presented at access, with wireless functionality [2], and core, featuring reconfigurability [3], layers with Cao *et al.* using software defined networking concepts to design QKD networks [4]. There is also an increasing interest in applying machine learning techniques to optimize the performance of QKD systems [5–7]. The security of practical implementations has also been addressed by devising hacking strategies [8–10], with their corresponding countermeasures, as well as by accounting for realistic imperfections and finite-key effects in the security analysis [2,11]. The feature issue also covers some less conventional protocols [12,13], relying on ambiguous state discrimination, as well as insight into multi-mode and high-dimensional QKD systems [14,15]. It also features new quantum secure direct communication techniques to solve the key-disclosure problem [16]. Last, but not least, the feature issue covers recent advancements in fast integrated quantum random number generators [17,18] and photon-number resolving detectors based on superconducting technology [19].

We hope that this feature issue provides a useful reference for the latest developments in the field, and stimulates further interdisciplinary collaborations to tackle the remaining deployment challenges of quantum communications technologies. We would like to express our gratitude to the former Editor-in-Chief, Grover Swartzlander, for his support and encouragement, and journal staff for their help and patience. Finally, we would like to thank all the authors and the dedicated reviewers, without whose efforts this feature issue would have not been possible.

References

1. C. Agnesi, L. Calderaro, D. Dequal, F. Vedovato, M. Schiavon, A. Santamato, V. Luceri, G. Bianco, G. Vallone, and P. Villoresi, “Sub-ns timing accuracy for satellite quantum communications,” J. Opt. Soc. Am. B **36**, B59–B64 (2019).
2. S. Bahrani, O. Elmabrok, G. C. Lorenzo, and M. Razavi, “Wavelength assignment in quantum access networks with hybrid wireless-fiber links,” J. Opt. Soc. Am. B **36**, B99–B108 (2019).
3. E. Y. Zhu, C. Corbari, A. Gladyshev, P. G. Kazansky, H.-K. Lo, and L. Qian, “Toward a reconfigurable quantum network enabled by a broadband entangled source,” J. Opt. Soc. Am. B **36**, B1–B6 (2019).
4. Y. Cao, Y. Zhao, X. Yu, and J. Zhang, “Multi-tenant provisioning over software defined networking enabled metropolitan area quantum key distribution networks,” J. Opt. Soc. Am. B **36**, B31–B40 (2019).
5. F.-Y. Lu, Z.-Q. Yin, C. Wang, C.-H. Cui, J. Teng, S. Wang, W. Chen, W. Huang, B.-J. Xu, G.-C. Guo, and Z.-F. Han, “Parameter optimization and real-time calibration of a measurement-device-independent quantum key distribution network based on a back propagation artificial neural network,” J. Opt. Soc. Am. B **36**, B92–B98 (2019).
6. H. Zhang, P. Liu, Y. Guo, L. Zhang, and D. Huang, “Blind modulation format identification using the dbscan algorithm for continuous-variable quantum key distribution,” J. Opt. Soc. Am. B **36**, B51–B58 (2019).
7. Yaseera Ismail, Ilya Sinayskiy, and Francesco Petruccione, “Integrating machine learning techniques in quantum communication to characterize the quantum channel,” J. Opt. Soc. Am. B **36**, B116–B121 (2019).

8. S. M. Barnett, T. Brougham, S. Croke, and S. J. D. Phoenix, “Optimized attacks on twin-field quantum key distribution,” J. Opt. Soc. Am. B **36**, B122–B129 (2019).
9. M. S. Lee, M. K. Woo, Y.-S. Kim, Y.-W. Cho, S.-W. Han, and S. Moon, “Quantum hacking on a free-space quantum key distribution system without measuring quantum signals,” J. Opt. Soc. Am. B **36**, B77–B82 (2019).
10. S. Ren, R. Kumar, A. Wonfor, X. Tang, R. Penty, and I. White, “Reference pulse attack on continuous variable quantum key distribution with local local oscillator under trusted phase noise,” J. Opt. Soc. Am. B **36**, B7–B15 (2019).
11. Y. Wang, W.-S. Bao, C. Zhou, M.-S. Jiang, and H.-W. Li, “Finite-key analysis of practical decoy-state measurementdevice-independent quantum key distribution with unstable sources,” J. Opt. Soc. Am. B **36**, B83–B91 (2019).
12. H. Lu, “Ambiguous discrimination among linearly dependent quantum states and its application to two-way deterministic quantum key distribution,” J. Opt. Soc. Am. B **36**, B26–B30 (2019).
13. A. Gaidash, A. Kozubov, and G. Miroshnichenko, “Methods of decreasing the unambiguous state discrimination probability for subcarrier wave quantum key distribution systems,” J. Opt. Soc. Am. B **36**, B16–B19 (2019).
14. R. Kumar, X. Tang, A. Wonfor, R. Penty, and I. White, “Continuous variable quantum key distribution with multi-mode signals for noisy detectors,” J. Opt. Soc. Am. B **36**, B109–B115 (2019).
15. J. E. Bourassa and H.-K. Lo, “Entropic uncertainty relations and the measurement range problem, with consequences for high-dimensional quantum key distribution,” J. Opt. Soc. Am. B **36**, B65–B76 (2019).
16. J. H. Shapiro, D. M. Boroson, P. B. Dixon, M. E. Grein, and S. A. Hamilton, “Quantum low probability of intercept,” J. Opt. Soc. Am. B **36**, B41–B50 (2019).
17. T. Roger, T. Paraiso, I. De Marco, D. G. Marangon, Z. Yuan, and A. J. Shields, “Real-time interferometric quantum random number generation on chip,” J. Opt. Soc. Am. B **36**, BXXX–BXXX (2019).
18. L. Huang and H. Zhou, “Integrated Gbps quantum random number generator with real-time extraction based on homodyne detection,” J. Opt. Soc. Am. B **36**, BXXX–BXXX (2019).
19. M. Moshkova, A. Divochiy, P. Morozov, Y. Vakhtomin, A. Antipov, P. Zolotov, V. Seleznev, M. Ahmetov, and K. Smirnov, “High-performance superconducting photon-number-resolving detectors with 86% system efficiency at telecom range,” J. Opt. Soc. Am. B **36**, B20–B25 (2019).