Advances in quantum cryptography

By: Pirandola, S (Pirandola, S.)[1,2,3]; Andersen, UL (Andersen, U. L.)[4]; Banchi, L (Banchi, L.)[5]; Berta, M (Berta, M.)[6]; Bunandar, D (Bunandar, D.)[3]; Colbeck, R (Colbeck, R.)[7]; Englund, D (Englund, D.)[3]; Gehring, T (Gehring, T.)[4]; Lupo, C (Lupo, C.)[8]; Ottaviani, C (Ottaviani, C.)[1,2] ...More

View Web of Science ResearcherID and ORCID

ADVANCES IN OPTICS AND PHOTONICS
Volume: 12 **Issue:** 4 **Pages:** 1012-1236
DOI: 10.1364/AOP.361502
Published: DEC 31 2020
Document Type: Review
View Journal Impact

Abstract

Quantum cryptography is arguably the fastest growing area in quantum information science. Novel theoretical protocols are designed on a regular basis, security proofs are constantly improving, and experiments are gradually moving from proof-of-principle lab demonstrations to in-field implementations and technological prototypes. In this paper, we provide both a general introduction and a state-of-the-an description of the recent advances in the field, both theoretical and experimental. We start by reviewing protocols of quantum key distribution based on discrete variable systems. Next we consider aspects of device independence, satellite challenges, and protocols based on continuous-variable systems. We will then discuss the ultimate limits of point-to-point private communications and how quantum repeaters and networks may overcome these restrictions. Finally, we will discuss some aspects of quantum cryptography beyond standard quantum key distribution, including quantum random number generators and quantum digital signatures. (C) 2020 Optical Society of America

Keywords

KeyWords Plus: ORBITAL-ANGULAR-MOMENTUM; POLYNOMIAL-TIME ALGORITHMS; ERROR-CORRECTING CODES; OF-THE-ART; KEY DISTRIBUTION; UNCONDITIONAL SECURITY; CONTINUOUS-VARIABLES; ENTANGLEMENT DISTRIBUTION; PRIVACY AMPLIFICATION; ENTROPIC UNCERTAINTY

Author Information

Reprint Address:
University of York - UK Univ York, Dept Comp Sci, York YO10 5GH, N Yorkshire, England.
University of York - UK Univ York, York Ctr Quantum Technol, York YO10 5GH, N Yorkshire, England.
Massachusetts Institute of Technology (MIT) MIT, Res Lab Elect, 77 Massachusetts Ave, Cambridge, MA 02139 USA.
Corresponding Address: Pirandola, S (corresponding author)

+ Univ York, Dept Comp Sci, York YO10 5GH, N Yorkshire, England.

Corresponding Address: Pirandola, S (corresponding author)

+ Univ York, York Ctr Quantum Technol, York YO10 5GH, N Yorkshire, England.

Corresponding Address: Pirandola, S (corresponding author)

+ MIT, Res Lab Elect, 77 Massachusetts Ave, Cambridge, MA 02139 USA.

Addresses:

+ [1] Univ York, Dept Comp Sci, York YO10 5GH, N Yorkshire, England
+ [2] Univ York, York Ctr Quantum Technol, York YO10 5GH, N Yorkshire, England
+ [3] MIT, Res Lab Elect, 77 Massachusetts Ave, Cambridge, MA 02139 USA
+ [4] Tech Univ Denmark, Ctr Macroscop Quantum States BigQ, Dept Phys, DK-2800 Lyngby, Denmark
+ [5] Univ Florence, Dept Phys & Astron, Via G Sansone 1, I-50019 Sesto Fiorentino, FI, Italy
+ [6] Imperial Coll, Dept Comp, London SW7 2AZ, England
+ [7] Univ York, Dept Math, York YO10 5DD, N Yorkshire, England
+ [8] Univ Sheffield, Dept Phys & Astron, Sheffield S3 7RH, S Yorkshire, England
+ [9] Univ Leeds, Sch Elect & Elect Engn, Leeds LS2 9JT, W Yorkshire, England

[10] Int Islamic Univ Malaysia IIUM, Fac Sci, Jalan Sultan Ahmad Shah, Kuantan 25200, Pahang, Malaysia

[11] Univ Putra Malaysia, Inst Math Res INSPEM, Upm Serdang 43400, Selangor, Malaysia

[12] Univ Technol Sydney, Ctr Quantum Software & Informat, Sch Software, Sydney, NSW 2007, Australia

[13] Natl Univ Singapore, Dept Elect & Comp Engn, Singapore, Singapore

[14] Natl Univ Singapore, Ctr Quantum Technol, Singapore, Singapore

[15] Palacky Univ, Dept Opt, 17 Listopadu 50, Olomouc 77207, Czech Republic

[16] Univ Padua, Dipartimento Ingn Informaz, Via Gradenigo 6B, I-35131 Padua, Italy

[17] Univ Edinburgh, Sch Informat, 10 Crichton St, Edinburgh EH8 9AB, Midlothian, Scotland

E-mail Addresses: stefano.pirandola@york.ac.uk

Funding

Funding Agency (Show details)	Grant Number
Engineering & Physical Sciences Research Council (EPSRC)	EP/M013472/1 EP/T001011/1 EP/P016588/1
European Commission European Commission Joint Research Centre	675662 820466 820474
Danmarks Grundforskningsfond	DNRF142
Grant Agency of the Czech Republic	1923739S
Ministry of Education, Youth & Sports - Czech Republic	LTC17086
United States Department of Defense Air Force Office of Scientific Research (AFOSR)	FA9550-16-1-0391
Office of Naval Research	
National Science Foundation (NSF)	

View funding text

Publisher

OPTICAL SOC AMER, 2010 MASSACHUSETTS AVE NW, WASHINGTON, DC 20036 USA

Journal Information

Impact Factor: Journal Citation Reports

Categories / Classification

Research Areas: Optics

Web of Science Categories: Optics

Document Information

Language: English

Accession Number: WOS:000603592000003

ISSN: 1943-8206

Other Information

IDS Number: PM1TZ

Cited References in Web of Science Core Collection: 990

Times Cited in Web of Science Core Collection: 12

See fewer data fields

1 of 252

Cited References: 990

Showing 30 of 990 **View All in Cited References page** *(from Web of Science Core Collection)*

1. **Quantum money from hidden subspaces** **Times Cited: 1**

By: Aaronson, S.; Christiano, P.
P 44 ANN ACM S THEOR Published: 2012
Publisher: ACM

2. **The Computational Complexity of Linear Optics** — Times Cited: 292
By: Aaronson, Scott; Arkhipov, Alex
STOC 11: PROCEEDINGS OF THE 43RD ACM SYMPOSIUM ON THEORY OF COMPUTING Book Series: Annual ACM Symposium on Theory of Computing Pages: 333-342 Published: 2011

3. **Measurement-device-independent quantum key distribution with quantum memories** — Times Cited: 41
By: Abruzzo, Silvestre; Kampermann, Hermann; Bruss, Dagmar
PHYSICAL REVIEW A Volume: 89 Issue: 1 Article Number: 012301 Published: JAN 2 2014

4. **Certified randomness in quantum physics** — Times Cited: 69
By: Acin, Antonio; Masanes, Lluis
NATURE Volume: 540 Issue: 7632 Pages: 213-219 Published: DEC 8 2016

5. **Device-independent security of quantum cryptography against collective attacks** — Times Cited: 828
By: Acin, Antonio; Brunner, Nicolas; Gisin, Nicolas; et al.
PHYSICAL REVIEW LETTERS Volume: 98 Issue: 23 Article Number: 230501 Published: JUN 8 2007

6. **From Bell's theorem to secure quantum key distribution** — Times Cited: 398
By: Acin, Antonio; Gisin, Nicolas; Masanes, Lluis
PHYSICAL REVIEW LETTERS Volume: 97 Issue: 12 Article Number: 120405 Published: SEP 22 2006

7. **Asymptotic entropic uncertainty relations** — Times Cited: 16
By: Adamczak, Radoslaw; Latala, Rafal; Puchala, Zbigniew; et al.
JOURNAL OF MATHEMATICAL PHYSICS Volume: 57 Issue: 3 Article Number: 032204 Published: MAR 2016

8. **Metric and classical fidelity uncertainty relations for random unitary matrices** — Times Cited: 1
By: Adamczak, Radoslaw
JOURNAL OF PHYSICS A-MATHEMATICAL AND THEORETICAL Volume: 50 Issue: 10 Article Number: 105302 Published: MAR 10 2017

9. **Continuous Variable Quantum Information: Gaussian States and Beyond** — Times Cited: 252
By: Adesso, Gerardo; Ragy, Sammy; Lee, Antony R.
OPEN SYSTEMS & INFORMATION DYNAMICS Volume: 21 Issue: 1-2 Article Number: 1440001 Published: JUN 2014

10. Title: [not available] — Times Cited: 1
By: AGGARWAL S
LEDGER-PITTSBURGH Volume: 3 Published: 2018

11. **Exploring the boundaries of quantum mechanics: advances in satellite quantum communications** — Times Cited: 12
By: Agnesi, Costantino; Vedovato, Francesco; Schiavon, Matteo; et al.
PHILOSOPHICAL TRANSACTIONS OF THE ROYAL SOCIETY A-MATHEMATICAL PHYSICAL AND ENGINEERING SCIENCES Volume: 376 Issue: 2123 Article Number: 20170461 Published: JUL 13 2018

12. **PRIMES is in P** — Times Cited: 347
By: Agrawal, M; Kayal, N; Saxena, N
ANNALS OF MATHEMATICS Volume: 160 Issue: 2 Pages: 781-793 Published: SEP 2004

13. **Generating hard instances of lattice problems** — Times Cited: 17
By: Ajtai, M.
P 28 ANN ACM S THEOR Published: 1996
Publisher: ACM

14. **Performance and structure of single-mode bosonic codes** — Times Cited: 55
By: Albert, Victor V.; Noh, Kyungjoo; Duivenvoorden, Kasper; et al.
PHYSICAL REVIEW A Volume: 97 Issue: 3 Article Number: 032346 Published: MAR 30 2018

15. **Large-alphabet quantum key distribution using energy-time entangled bipartite states** — Times Cited: 136
By: Ali-Khan, Irfan; Broadbent, Curtis J.; Howell, John C.
PHYSICAL REVIEW LETTERS Volume: 98 Issue: 6 Article Number: 060503 Published: FEB 9 2007

16. **Quantum Attacks on Classical Proof Systems The Hardness of Quantum Rewinding** — Times Cited: 27
By: Ambainis, Andris; Rosmanis, Ansis; Unruh, Dominique

2014 55TH ANNUAL IEEE SYMPOSIUM ON FOUNDATIONS OF COMPUTER SCIENCE (FOCS 2014) Book Series: Annual IEEE Symposium on Foundations of Computer Science Pages: 474-483 Published: 2014

17. **Secure quantum signatures using insecure quantum channels** — Times Cited: 39
By: Amiri, Ryan; Wallden, Petros; Kent, Adrian; et al.
PHYSICAL REVIEW A Volume: 93 Issue: 3 Article Number: 032325 Published: MAR 17 2016

18. **Distributed Domination on Graph Classes of Bounded Expansion** — Times Cited: 4
By: Amiri, Saeed Akhoondian; de Mendez, Patrice Ossona; Rabinovich, Roman; et al.
SPAA'18: PROCEEDINGS OF THE 30TH ACM SYMPOSIUM ON PARALLELISM IN ALGORITHMS AND ARCHITECTURES Pages: 143-151 Published: 2018

19. **Quantum key distribution over probabilistic quantum repeaters** — Times Cited: 16
By: Amirloo, Jeyran; Razavi, Mohsen; Majedi, A. Hamed
PHYSICAL REVIEW A Volume: 82 Issue: 3 Article Number: 032304 Published: SEP 9 2010

20. **Hybrid discrete- and continuous-variable quantum information** — Times Cited: 146
By: Andersen, Ulrik L.; Neergaard-Nielsen, Jonas S.; van Loock, Peter; et al.
NATURE PHYSICS Volume: 11 Issue: 9 Pages: 713-719 Published: SEP 2015

21. **30 years of squeezed light generation** — Times Cited: 119
By: Andersen, Ulrik L.; Gehring, Tobias; Marquardt, Christoph; et al.
PHYSICA SCRIPTA Volume: 91 Issue: 5 Article Number: 053001 Published: MAY 2016

22. **Experimentally realizable quantum comparison of coherent states and its applications** — Times Cited: 84
By: Andersson, Erika; Curty, Marcos; Jex, Igor
PHYSICAL REVIEW A Volume: 74 Issue: 2 Article Number: 022304 Published: AUG 2006

23. Title: [not available] — Times Cited: 19
By: Andrews, L. C.; Phillips, R. L.
Laser Beam Propagation through Random Media Published: 2005
Publisher: SPIE

24. **Definition and analysis of quantum E-voting protocols** — Times Cited: 1
By: Arapinis, M.; Kashefi, E.; Lamprou, N.; et al.
arXiv:1810.05083v3
[Show additional data]

25. **Practical device-independent quantum cryptography via entropy accumulation** — Times Cited: 43
By: Arnon-Friedman, Rotem; Dupuis, Frederic; Fawzi, Omar; et al.
NATURE COMMUNICATIONS Volume: 9 Article Number: 459 Published: JAN 31 2018

26. **SIMPLE AND TIGHT DEVICE-INDEPENDENT SECURITY PROOFS** — Times Cited: 18
By: Arnon-Friedman, Rotem; Renner, Renato; Vidick, Thomas
SIAM JOURNAL ON COMPUTING Volume: 48 Issue: 1 Pages: 181-225 Published: 2019

27. **MULTIPARTY QUANTUM SIGNATURE SCHEMES** — Times Cited: 25
By: Arrazola, Juan Miguel; Wallden, Petros; Andersson, Erika
QUANTUM INFORMATION & COMPUTATION Volume: 16 Issue: 5-6 Pages: 435-464 Published: APR 2016

28. **Quantum communication in noisy environments** — Times Cited: 2
By: Aschauer, H.
THESIS Published: 2005
Ph.d. thesis
Publisher: Ludwig-Maximilians-Universitat Munchen

29. **Long-distance quantum communication with entangled photons using satellites** — Times Cited: 130
By: Aspelmeyer, M; Jennewein, T; Pfennigbauer, M; et al.
IEEE JOURNAL OF SELECTED TOPICS IN QUANTUM ELECTRONICS Volume: 9 Issue: 6 Pages: 1541-1551 Published: NOV-DEC 2003

30. **Fundamental rate-loss trade-off for the quantum internet** — Times Cited: 33
By: Azuma, Koji; Mizutani, Akihiro; Lo, Hoi-Kwong
NATURE COMMUNICATIONS Volume: 7 Article Number: 13523 Published: NOV 25 2016

Showing 30 of 990 **View All in Cited References page**