Advances in entanglement-based QKD for space applications

Contract No. 4000134348/21/NL/GLC/ov

Sebastian Ecker

21/06/2022
Outline

• Fundamentals of quantum key distribution (QKD)
  • Why QKD instead of classical cryptography?
  • QKD protocols
  • Sources of entangled photon pairs
  • Distribution of photons over long distances

• Advances in entanglement-based QKD
  • High-performance entangled photon pair sources
  • Integrated photonic entanglement sources
  • Wavelength division multiplexing
  • High-dimensional QKD
  • Adaptive optics for quantum receivers
  • Space-based quantum repeater
Quantum Key Distribution (QKD) – Why?

Secure communication relies on asymmetric cryptography (e.g. RSA)
Messages encrypted with public key, decrypted with private key.

Public key cryptography

Security based on computational hardness assumption
Shor's (quantum) algorithm: Massive speedup – breaks cryptosystems!

Until 10-20 years ago this threat was theoretical
2019/2020: first demonstrations of quantum advantage

Programmable quantum computer „around the corner“ (20, 30, 40 years?)
IBM, Google, Microsoft, Honeywell, Rigetti, Zapata,...
QKD Protocols

- Symmetric cryptography
- Assumption-free
- Security guaranteed by the laws of physics (Information-theoretic security)

QKD relies on one fundamental quantum mechanical principle:

- Outcome of measurement is not predetermined (quantum indeterminacy)
- Copying of quantum states is impossible (no-cloning theorem)
- Preparation in one “basis” makes information in another “basis” inaccessible

H/V and D/A basis mutually exclusive

Polarization of (single) photons

H/V and D/A basis

H and V orthogonal

D and A orthogonal

C. H. Bennett and G. Brassard, Theoretical Computer Science 560 (2014)

Secret key (for symmetric encryption), e.g. OTP
QKD Protocols

Why focus on entanglement-based protocols?

- Party owning the entangled photon source can be malicious (untrusted) – Satellites!
- Distribution of entanglement important for many quantum technological applications

E. Wille et al., Free-Space Laser Communications XXXII, p. 21. (2020)

C. Bennett, G. Brassard, and N. Mermin, Physical review letters 68, 5 (1992)
QKD Protocols

BBM92-protocol

\[ |\Phi^+\rangle = \frac{1}{\sqrt{2}} (|HH\rangle + |VV\rangle) \]
\[ = \frac{1}{\sqrt{2}} (|DD\rangle + |AA\rangle) \]

C. Bennett, G. Brassard, and N. Mermin, *Physical review letters* 68, 5 (1992)
Sources of entangled photon pairs

SPDC (second-order nonlinear process)

Pump laser
- CW / pulsed

\( \chi^{(2)} \)

Photon pair properties:
- (Non-classical) two-photon state
- Spontaneous emission, probabil.
- Highly correlated in time (ps)
- Half the frequency of pump
- 1-100 nm bandwidth

Engineering of photon pair sources:
- SPDC process (spectrum, collinear, polarization,..)
- Focal parameters (fiber coupling, pair rate)
- Overlap of several processes (Polarization entanglement!)
- Entanglement in different DoF

Single-photon detection
- SPAD
- SNSPD

medium timing jitter
- medium efficiency
- medium dead time
- low cost

low timing jitter
- high efficiency
- low dead time
- high cost / complexity
Distribution of photons over long distances

Optical fiber distribution (~0.2 dB/km)

Exponential scaling of loss – absorption limited
→ Maximal distances of a few hundred km

Quantum repeater (first lab demonstrations)

Satellite-based distribution

Quadratic scaling of loss – diffraction limited
→ Global coverage

Possible link configurations

Yin, J., et al., Science, 356, 6343 (2017)
S.P. Neumann, arXiv:2203.12417 (2022)
O. Lee, T. Vergoossen, and A. Ling, arXiv:1909.13061 (2019)
Micius satellite (QUESS mission)

Launch: 2016
Sun-synchronous
488-584 km
630 kg
97.4° inclination

Satellite-based entanglement distribution over 1200 kilometers

Jian-Yin,1,2 Yuan Cao,1,2 Yu-Huai Li,1,2 Sheng-Kai Liao,1,2 Liang Zhang,1,2 Ji-Gang Ren,1,2 Wen-Qi Cai,1,2 Wei-Yue Liu,1,2 Bo Li,1,2 Hui Dat,1,2 Guang-Bing Li,1,2 Qi-Ming Lu,1,2 Yun-Hong Gong,1,2 Yu Xu,1,2 Shuang-Lin Li,1,2 Feng-Zhi Li,1,2 Ya-Yun Yin,1,2 Zi-Qing Jiang,1 Ming Li,2 Jian-Jun Jia,2 Ge Ren,4 Dong He,4 Yi-Lin Zhou,5 Xiao-Xiang Zhang,6 Na Wang,5 Xiang Chang,5 Zhen-Cai Zhu,5 Nai-Le Liu,5,6 Yu-Ao Chen,1,2 Chao-Yang Lu,1,2 Rong Shu,2,3 Cheng-Zhi Peng,1,2,6
Jian-Yu Wang,1,2,3,4 Jian-Wei Pan,1,2,3

Ground-to-satellite quantum teleportation

Ji-Gang Ren1,2, Ping Xu1,2, Hai-Lin Yong1,2, Sheng-Kai Liao1,2, Juan Yin1,2, Wei-Yue Liu1,2, Wen-Qi Cai1,2, Meng Yang1,2, Li Li1,2, Kui-Xing Yang1,2, Xuan Han1,2, Yong-Qiang Yao1,2, Ji Li2, Hai-Yan Wu1,2, Song Wang1,2, Lei Liu1,2, Ding-Quan Liu1,2, Yao-Wu Kuang1,2, Zhi-Ping He1,2, Peng Shang1,2, Cheng Guo1,2, Ru-Hua Zheng1,2, Kai Tian1,2, Zhen-Cai Zhu1,2, Nai-Le Liu1,2, Chao-Yang Lu1,2, Rong Shu2,3, Yu-Ao Chen1,2, Cheng-Zhi Peng1,2, Jian-Yu Wang1,2, Jian-Wei Pan1,2

Satellite–to–ground quantum key distribution

Sheng-Kai Liao1,2, Wen-Qi Cai1,2, Wei-Yue Liu1,2, Liang Zhang1,2, Ji-Gang Ren1,2, Juan Yin1,2, Qi Shen1,2, Rong Shu2,3, Meng Yang1,2, Feng-Zhi Li1,2, Xia Wei Chen1,2, Li-Hua Sun1,2, Rui-Jun Zhai1,2, Lin-Cai Wu1,2, Xiao-Jun Jiang1,2, Jian-Feng Wang4, Yong-Mei Huang2,2, Qi Wang2,2, Yi-Lin Zhou2,2, Lei Deng2,2, Tao Xu2,2, Yu Ma2,2, Tai Hu2,2, Chao Yang2,2, Yu-Ao Chen1,2, Nai-Le Liu1,2, Xiang-Bin Wang2,2, Zhen-Cai Zhu2,2, Chao-Ying Lu2,2, Rong Shu2,3, Cheng-Zhi Peng1,2, Jian-Yu Wang1,2 & Jian-Wei Pan1,2

C.M. Imran et al., “Satellite-Based QKD,” Opt. Photonics News – OSA (2018)

Physical Review Letters, 120(3), 30501 (2018)

Science, 356(6343), 1140–1144 (2017)

Nature, 549(7670), 70–73 (2017)

Nature, 549(7670), 43–47 (2017)

+ THE EUROPEAN SPACE AGENCY
Advances in entanglement-based QKD

Secret-key rate of Micius: 0.12 bits/s over 1120 km ground distance (entanglement-based protocol)

Operation at maximal capacity – little room for optimization

→ Fundamentally new techniques/methods are required for commercial success!

Advances should:

- Increase the secure key rate
- Reduce SWaP and complexity of quantum payloads
- Decrease the costs per secret bit

TRL of presented advances: Lab demonstrations and/or terrestrial free-space links

Yin et al., Nature 582, 501–505 (2020)
High-performance entangled photon pair sources

Performance parameters of entangled sources for QKD:
• **Fidelity** (>99%) – no potential
• **Heralding efficiency** (>50%) – no potential
• **Brightness** (>10^7 pairs/s/mW of pump power) – potential?

Higher brightness ≠ Higher key rate!

Accidental coincidences

Increased brightness required for:
• Lower timing jitter with SNSPDs (<10 ps)
• Multiplexed QKD

Brightness of state-of-the-art photon pair sources sufficient!
Integrated photonic entanglement sources

Photonic integrated circuits (PIC):
• Miniaturisation of table-top bulk optical setups
• Opto-electronic integration
• Primarily used in telecom, biomed and photonic quantum information processing

Integrated sources for space applications:
• Reduce SWaP
• Non-linearity inherent to the materials
• Robustness and phase-stability (misalignment of bulk optical setups)
• Scalability and existing fabs - costs (same as for CMOS fabrication)
• Multiple sources on a satellite (no single point of failure / parallelization)
Integrated photonic entanglement sources

Two candidate platforms meeting the requirements for QKD (brightness + integration level):

**Integrated periodically-poled waveguide sources**

- SPDC in a ppLN waveguide
- Hybrid material assembly
- Brightness ~ 5e6 pairs/(s⋅nm⋅mW)
- Dimension: few cm

**Monolithic III-V semiconductor sources**

- SPDC in GaAs structures
- Bragg reflection waveguides
- Brightness ~ 1e6 pairs/(s⋅nm⋅mW)
- Dimension: 1.2 mm
Integrated photonic entanglement sources

Considerations for space deployment:

- Electrical injection for full integration
- Efficient coupling into SM fibers (mode clean-up / guiding)
- Temperature-stability on 0.1° level must be guaranteed
- Packaging and assembly (launch conditions)

Obvious contender for replacing bulk optical components in space (except for Tx/Rx optics)

Interest in integrated optics for space applications is increasing:

- Integrated photonic source on ISS (SEAQUE) by NASA
- Photonic integrated circuits part of ESAs building missions

Electrically injected pair source

SEAQUE on ISS (launch 2022)

F. Boitier et al., Phys. Rev. Lett., 112, 18 (2014)

https://www.jpl.nasa.gov/news/space-station-to-host-self-healing-quantum-communications-tech-demo
https://www.esa.int/Enabling_Support/Space_Engineering_Technology/Space_Optoelectronics/Photronics
Wavelength-division multiplexing

Energy conservation in SPDC:
\[ \omega_{Alice} + \omega_{Bob} = \omega_{pump} \]

Frequency correlations!
\[ \Rightarrow \text{no active multiplexing necessary} \]

Realization with VHGs (volume holographic gratings)

Detection:
- Frequency unresolved
- Frequency resolved

J. Pseiner, L. Achatz, L. Bulla, M. Bohmann, and R. Ursin, Quantum Sci. Technology 6,3 (2021)
Wavelength-division multiplexing

WDM for telecom: each additional wavelength channel increases the total data rate

WDM for QKD: all frequencies were detected before, so where is the benefit?
rate/ freq. channel lower → less accidental coincidences
→ source brightness increased to optimum
→ ~ n-fold increase of secure key rate!
(n...number of wavelength channels)

Experimental results and scaling

Satellite implementation

Considerations for satellite implementation:
• No increase in complexity for quantum payloads
  (only prerequisite: broad SPDC spectrum)
• Quantum receivers can be easily upgraded
• Angle-of-arrival fluctuations in receivers problematic

J. Pfeifer, L. Achatz, L. Bulla, M. Bohmann, and R. Ursin, Quantum Sci. Technology 6, 3 (2021)
Wavelength-division multiplexing

Fully-connected 4 user-network via wavelength de-multiplexing and selective multiplexing of ITU channels

Realization for space-based scenarios:

1. n-user network multiplexed on satellite (as above)
   n simultaneous downlinks – all ground receivers are fully connected

2. De-multiplexing and selective multiplexing on ground (right figure)
   all users between two remote cities are simultaneously connected

- S. Wengerowsky, S. K. Joshi, F. Steinlechner, H. Hübel, and R. Ursin, 568, 225–228 (2018)
High-dimensional QKD

2-dim: \( \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \)  
\[ e.g. \frac{1}{\sqrt{2}} (|H\rangle + |V\rangle) \]

d-dim: \( \frac{1}{\sqrt{d}} \sum_{i=1}^{d} |i\rangle \)  
\[ e.g. \frac{1}{\sqrt{3}} (|\omega_1\rangle + |\omega_2\rangle + |\omega_3\rangle) \]

High-dimensional QKD protocols offer:

- **Noise resilience**: higher noise levels are tolerated (sun, light sources, detector dark counts, errors,...)

- **Increased key rate**: \( \log_2(d) \) bits/photon important in photon-starved scenarios

Many different high-dim QKD protocols are known

---

S. Ecker et al., Phys. Rev. X 9, 4 (2019)
L. Sheridan and V. Scarani, Phys. Rev. A, 82, 3 (2010)
High-dimensional QKD

High-dimensional entanglement in spatio-temporal properties comes “for free” in SPDC:

Energy conservation → Energy (time) entanglement

Momentum conservation → Momentum (spatial) entanglement

Path Entanglement

\[ \sum_{n=1}^{d} c_n |a_n\rangle_A |b_n\rangle_B \]

Time-bin Entanglement

\[ \sum_{n=1}^{d} c_n |t + n\Delta T\rangle_A |t + n\Delta T\rangle_B \]

Spatial mode Entanglement

\[ \sum_{l=1}^{d} c_l (|l\rangle_A |\bar{l}\rangle_B + \bar{|l\rangle}_A |l\rangle_B) \]

Frequency Entanglement

\[ \sum_{n=1}^{d} c_n |\omega_0 - n\Delta \omega\rangle_A |\omega_0 + n\Delta \omega\rangle_B \]
High-dimensional QKD

Free-space transmission of spatiotemporal properties

Spatial mode (OAM) transmission

Not robust
Decoherence due to atmospheric turbulence

Temporal mode transmission

Robust
Energy and temporal encodings can be used for satellite links
Adaptive optics for quantum receivers

AO systems long history in astronomy

Increasing relevance for optical comms
→ loss mitigation + single-mode operation

Benefits for space-based QKD:
• Loss reduction in up-or downlinks (geometrical loss)
• Multi-mode free-space beam converted into single spatial mode beam (compatibility with fiber networks)
• Avoidance of transverse spatial decoherence (for encoding in transverse spatial modes)
Space-based quantum repeater

Quantum repeater – only way to overcome direct transmission limit in optical fiber (polynomial instead of exponential scaling)

Entanglement swapping

The quantum repeater scheme:
- Division of long-distance links into elementary links
- Entanglement distribution between elementary links
- Storage of photons in quantum memories (QM)
- Nested entanglement swapping through all levels

Even for most optimistic estimates, fiber-based quantum repeater limited by a few thousand km

→ Truly global quantum networks require space-based quantum repeater!

H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, Phys. Rev. Lett., 81, 48 (1998)
Space-based quantum repeater

Single-node quantum repeater

Single satellite global quantum key distribution

M. Gündoğan et al., npj Quantum Inf., 7,1 (2021)

S. E. Wittig et al., Proc. Int. Astronaut. Congr. IAC, 8, September (2017)
Space-based quantum repeater

Hybrid space-based quantum repeater

K. Boone et al., Phys. Rev. A, 91, 5 (2015)
Space-based quantum repeater

Fully space-based quantum repeater

Comparison of QR schemes

GG…ground based scheme
OG…hybrid scheme
OO…fully space-based scheme

C. Lionni, H. Kampermann, and D. Bruß, New J. Phys., 23, 5 (2021)
Overview of advances and implications

High-performance entangled photon pair sources
- Increasing the secure key rate
- Only necessary for low timing jitter or multiplexing

Integrated photonic entanglement sources
- Reducing SWaP requirements
- Robustness, Scalability, Full integration

Wavelength division multiplexing
- Increasing the secure key rate substantially
- Enabling complex network topologies

High-dimensional QKD
- Increasing the secure key rate
- Resilience to noise

Adaptive optics for quantum receivers
- Increasing the secure key rate (geom. loss)
- Compatibility to fiber networks
- Wavefront distortions mitigated

Space-based quantum repeater
- Essential for global quantum communication
Final report

Thanks for your attention!

Questions?

sebastian.ecker@oeaw.ac.at