Project title:

The role and limitations of quantum entanglement in communications security

Student name:

Gehad Mostafa Hasan Eldibany

Personal Identifier:

H8825846

Strand code:

SXP390

Topic area:

Quantum entanglement and quantum information (QEQI)

Wordcount:

Abstract: 281 words

Report: 4994 words (from introduction to the end of conclusion excluding tables and equations)

Note: I have created the figures/tables with no in-text citations.

Abstract

The security guaranteed by classical cryptography is based on the computational complexity of some problems and threatened by advancements in computational power and algorithms. With quantum computing maturing, there is a pressing need to find alternatives. The quantum properties of matter and radiation can provide stronger security protected by the laws of physics and the phenomenon of entanglement. In entanglement-based cryptography, encryption keys are encoded into the quantum states and transmitted through quantum channels that, unlike classical cryptography, can detect eavesdropping and allow the communicating parties to discard the keys whose security has been compromised. Many experiments have proven the success of this approach to cryptography with different protocols and physical designs. There have also been large-scale implementations of entanglement-based cryptography in quantum networks in Vienna, Tokyo, China, and Bristol, covering distances up to 1,120 km using optical fibres and satellite to transmit the quantum signals. This paper covers the theories and main concepts used in entanglement-based quantum key distribution (QKD). The protocols used in large-scale deployments are discussed as well as the concept of device-independent QKD protocols which are considered the key to practical attacks-free security. The results of proof-of-concept experiments are presented in addition to important field trials. Despite the initial success, there is still a gap between the theoretical models and the real-world implementations that prevents wide deployment of quantum-entanglement QKD. The paper discusses the challenges including the distance coverage, the communication rate and integration with existing infrastructure in addition to the nature of quantum entanglement itself. It further recommends areas for future research to bridge the gap between theory and application and make use of the advantages of different QKD protocols and setups in a combined system.

List of abbreviations

BSM	Bell state measurement
DI-QKD	Device-independent quantum key distribution
PQC	Post-quantum cryptography
QBER	Quantum bit error rate
QKD	Quantum key distribution

List of tables

		Page
Table 1	Results of DI-QKD experiments	16
Table 2	Results of DARPA, SECOQC and Tokyo Networks	20
Table 3	Results of free-space implementations	23
Table 4	Performance of photonic against atomic platforms	28

List of figures

Figure 1	General design of QKD	9
Figure 2	Preparation of entanglement with photons	11
Figure 3	Preparation of entanglement with atom traps	12
Figure 4	E91 measurements	13
Figure 5	BB84 vs BBM92	14
Figure 6	DIQKD general setting	15
Figure 7	Ion-traps setup of Nadlinger *et al.* (2022)	17
Figure 8	Schematic of DARPA Network	19
Figure 9	Schematic of SECOQC Network	20
Figure 10	Key rate and QBER in SECOQC Network	21
Figure 11	Schematic of Tokyo Network	22
Figure 12	Key rate and QBER in Tokyo Network	22
Figure 13	Attenuation improvement in Yin *et al.* (2020)	24
Figure 14	Weaknesses of quantum systems	25
Figure 15	Key rate in Bristol Network	26

Table of Contents

Abstract 2

List of abbreviations 3

List of tables 3

List of figures 3

Table of Contents 4

1. Introduction 6

1.1 Cryptography in the quantum era 6

1.2 Objectives 7

1.3 Scope of work 7

1.4 Methodology 7

2. Preliminaries 9

2.1 Quantum key distribution 9

2.2 Theoretical framework 10

2.2.1 Monogamy of quantum entanglement 10

2.2.2 Bell test 10

2.2.3 The no-cloning theorem 10

2.3 Entanglement preparation 11

3. Entanglement-based cryptography 13

3.1 Entanglement-based quantum key distribution 13

3.2 Device-independent quantum key distribution 15

3.3 Proof-of-concept experiments 16

4. Real-world implementations 19

4.1 Fibre-optic Networks 19

4.1.1 DARPA Quantum Network 19

4.1.2 SECOQC quantum key distribution network 20

4.1.3 Tokyo quantum key distribution network 21

4.2 Free-space optic channels 23

5. Practical challenges 25

5.1 Inherent weaknesses of quantum systems 25

5.2 Network scalability and communication rate 25

5.3 Integration with existing infrastructure 26

6. Discussion 28

6.1 Protocols 28

6.2 Platforms and deployment 28

7. Conclusion 30

7.1 Summary 30

7.2 Future research 30

References 31

1. Introduction

1.1 Cryptography in the quantum era

Quantum computing is a trending research topic, and recent experiments have shown results indicating that practical quantum applications could be achieved in the near future (Kim *et al.*, 2023). Although quantum computers will help solve difficult problems, they threaten the security of information and communications, which are currently encrypted using classical algorithms that depend on the computational complexity of mathematical operations. With quantum algorithms already proposed, such as Shor's and Grover's, the time it would take to break common classical ciphers will be much shorter and realisable.

To counter these threats, efforts have been directed towards developing quantum-resistance cryptography, known as post-quantum cryptography (PQC). Some PQC algorithms have been recently chosen for standardization (Alagic *et al.*, 2022). However, these algorithms are insecure in the long run as they depend on computational complexity as well and are vulnerable to advancements in both mathematics and quantum technology. Quantum cryptography, on the other hand, promises unconditional security guaranteed by the laws of quantum mechanics and surpasses the classical mathematical approaches with the ability to detect interception and passive eavesdropping.

One promising quantum method is the quantum key distribution (QKD), which secures the exchange of encryption keys via quantum channels. Bennet and Brassard (1984) proposed the first QKD protocol using polarized single photons. Since then, there have been many implementations to prove its security and cover larger distances. However, a perfect single-photon source is yet to be created (Thomas and Senellart, 2021), so there is a probability of emitting more than one photon per wavepacket. This could enable an unauthorised party to extract single photons, which renders the system vulnerable to eavesdropping (Rosenblum *et al.*, 2016) and reduces communication rate, i.e. the communications speed, due to the loss of photons exchanged between the authorised parties (Scarani *et al.*, 2009).

Another approach to QKD is based on the quantum entanglement phenomenon and provides stronger guarantees with security checks using Bell's theorem. This entanglement-based approach is the focus of this paper. It has been implemented in both lab and real-world settings and is considered the key to foolproof security.

1.2 Objectives

This review is divided into chapters with each addressing the following objectives in order:

- Providing an overview of the concepts and quantum principles used in cryptography.
- Explaining the entanglement-based QKD and its advantages and discussing the Device-Independent QKD (DI-QKD) protocol, as an example, with its recent experiments and their limitations.
- Exploring real-world implementations of QKD in existing networks.
- Highlighting the current challenges of deploying entanglement-based protocols and the areas future research should address.

1.3 Scope of work

This study is focused on QKD as an application of quantum entanglement in cryptography and communications security, with DI-QKD family as promising protocols. It discusses the general elements of entanglement-based QKD and DI-QKD. It does not discuss in detail specific DI-QKD experimental protocols, other entanglement-based QKD families (e.g. Measurement Device-Independent QKD or entangled versions of Twin-Field QKD), attacks and other applications of entanglement.

1.4 Methodology

For the literature search:

- Relevant keywords were used to find seminal papers covering the foundations of the topic and recent literature presenting the advancements in the field.

- Google Scholar and the Open University Library were used mainly, with results published recently on credible peer-reviewed journals, e.g. the Physical Review Journals and Nature, given priority.
- PROMPT criteria were used to evaluate the literature.
- Papers more than five years old were considered only for the coverage of the foundational concepts and experiments.

For the literature review, conceptual analysis and case study methods were used to provide an explanation of the theories and how they fit in the cryptography scenario and examine real-world implementations to identify the challenges and opportunities.

2. Preliminaries

2.1 Quantum key distribution

Encryption secures communication to prevent an unauthorized party, referred to as the adversary or Eve, from accessing the content of the messages. Classically, the encryption is done through computationally complex problems hiding the content of the messages exchanged between the authorized users, referred to as Alice and Bob, who do not share any initial secret. In the quantum scenario, the encryption process is done through a secret key securely shared between Alice and Bob through a quantum channel before sharing the encrypted message itself on a classical public channel as shown in Figure 1 (Bennett and Brassard, 1984).

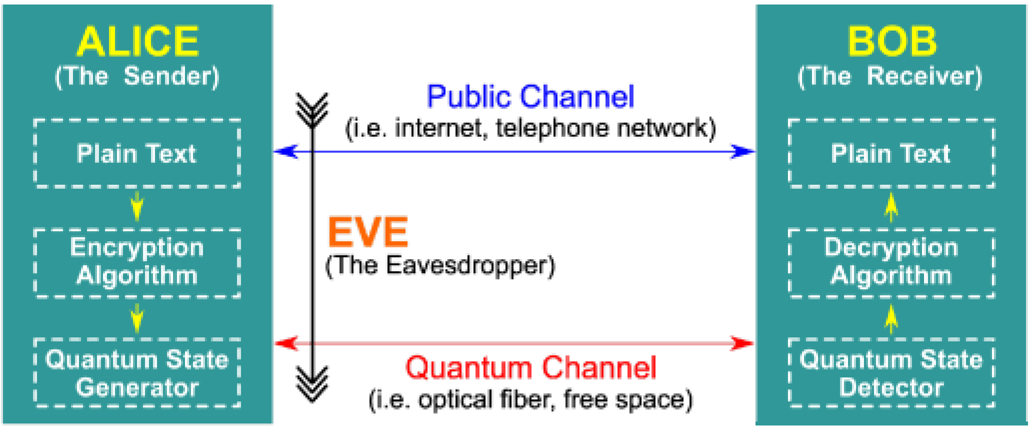

Figure 1. The generic design of the dual-channel QKD system (Nurhadi and Syambas, 2018)

The reason why the encrypted messages cannot be shared directly on the quantum channel is related to the quantum decoherence and fidelity, which will be discussed in Section 5.1. For now, we can say that the quantum signals shared on the quantum channels are prone to losses. During the key generation and exchange process, i.e. the key distribution, the lost signal can be discarded, but if an encrypted message is shared using quantum signals, the loss of signals will result in the loss of parts of the message itself. This applies to all the vulnerabilities associated with the quantum channel; they will directly affect or expose the communication itself rather than the encryption process, in case of quantum direct communication (Scarani *et al.*, 2009).

2.2 Theoretical framework

Besides the core quantum principles, including superposition and Heisenberg's uncertainty, the following concepts play a key role in quantum cryptography:

2.2.1 Monogamy of quantum entanglement

The Einstein- Podolsky-Rosen (EPR) paradox addressed the correlation between two spatially separated particles that interacted in the past and were left in a state where the measurement of a property of one particle gives information with certainty about a property of the other particle. This state is what is now known as the quantum entanglement, and the correlation associated with it, unlike the classical correlation, is restricted. That is, in a bipartite system, if Particles A and B are entangled, Particle A cannot share correlation with Particle C. This is called the monogamy of quantum entanglement (Coffman, Kundu and Wootters, 2000).

In the entanglement-based QKD scenario, the entanglement between the particles, e.g. photons, sent to Alice and Bob prevents Eve from obtaining the information encoded into the particles.

2.2.2 Bell test

Bell's theorem puts a limit to the correlation that could be explained classically by local hidden variables. Clauser *et al.* (1969) showed that the amount of correlation between the measurements of two particles should violate a Bell inequality to be attributed to entanglement between the particles. They formulated the CHSH inequality which is commonly expressed as $|S| \leq 2$. The *S* value will be covered in detail in Section 3.1, but it is worth noting now that $|S|$ has a maximum value of $2\sqrt{2}$, if the particles are maximally entangled. These values together are used to test the security of the entanglement-based QKD protocol. Any attempt at eavesdropping would disturb the system and affect the amount of violation of Bell inequality. The closer the value of $|S|$ to $2\sqrt{2}$, the more secure the protocol, with systems with values under 2 lacking the security guaranteed by the laws of quantum mechanics.

2.2.3 The no-cloning theorem

One difference between the classical and quantum approaches to cryptography is explained by the no-cloning theorem, which states that no device can perform a perfect cloning of arbitrary quantum states, it rather must be designed for a specific, known quantum state. Using the linearity of quantum mechanics, the cloning process is described below by a unitary operator *U*. Suppose that *U* is amplifying an arbitrary photon $|\psi\rangle$ so that $U|\psi\rangle = |\psi\rangle|\psi\rangle$. If the polarization state $|\psi\rangle = \alpha|\uparrow\rangle + \beta|\longrightarrow\rangle$, the cloning can be expressed in two ways, first:

$$\begin{aligned} U|\psi\rangle &= |\psi\rangle|\psi\rangle = (\alpha|\uparrow\rangle + \beta|\longrightarrow\rangle)(\alpha|\uparrow\rangle + \beta|\longrightarrow\rangle) \\ &= \alpha^2|\upuparrows\rangle + \alpha\beta|\uparrow\longrightarrow\rangle + \beta\alpha|\longrightarrow\uparrow\rangle + \beta^2|\rightrightarrows\rangle \end{aligned} \quad (1)$$

And linearly as:

$$U|\psi\rangle = U(\alpha|\uparrow\rangle + \beta|\longrightarrow\rangle) = \alpha U|\uparrow\rangle + \beta U|\longrightarrow\rangle = \alpha|\upuparrows\rangle + \beta|\rightrightarrows\rangle \quad (2)$$

The two results show a conflict, as the outcome of (1) ≠ the outcome of (2) for all values of *α* and *β*. This confirms the impossibility of cloning arbitrary quantum states, unlike classical states, which correspond to *α* = 0 and *β* =1 (or vice versa) and for which both results are the same and hence can be cloned (Wootters and Zurek, 1982).

2.3 Entanglement preparation

It takes two processes to establish entanglement-based QKD: (i) preparation of entangled qubits, and (ii) transmission of the entangled qubits which will be discussed in Section 4.

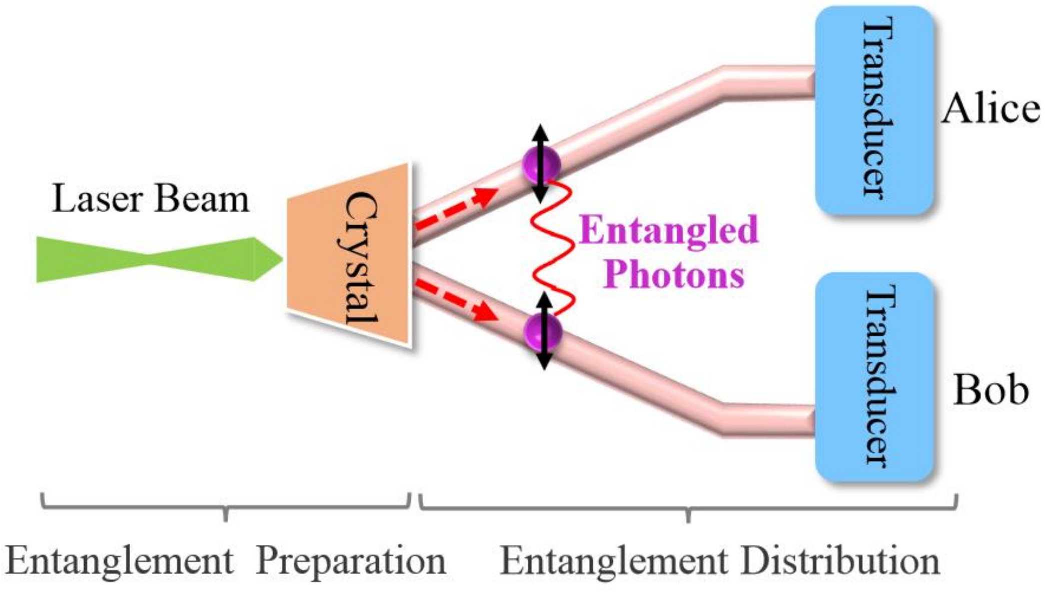

Figure 2. Schematic showing the preparation of entangled-photons (Li *et. al.*, 2023)

The experiments reported in this paper used photonic and atomic platforms to prepare entanglement. Figure 2 shows that entangled photons are basically generated by passing a laser beam through a crystal that splits the photons into entangled photons pairs. Ursin *et al.* (2007) used this setup in a large-scale deployment with beta-barium-borate crystal to produce the singlet state:

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}\left(|\mathrm{H}\rangle_\mathrm{A}|\mathrm{V}\rangle_\mathrm{B} - |\mathrm{V}\rangle_\mathrm{A}|\mathrm{H}\rangle_\mathrm{B}\right), \tag{3}$$

with H the horizontally polarised photon state and V the vertically polarised. The results are covered in Section 4.2.

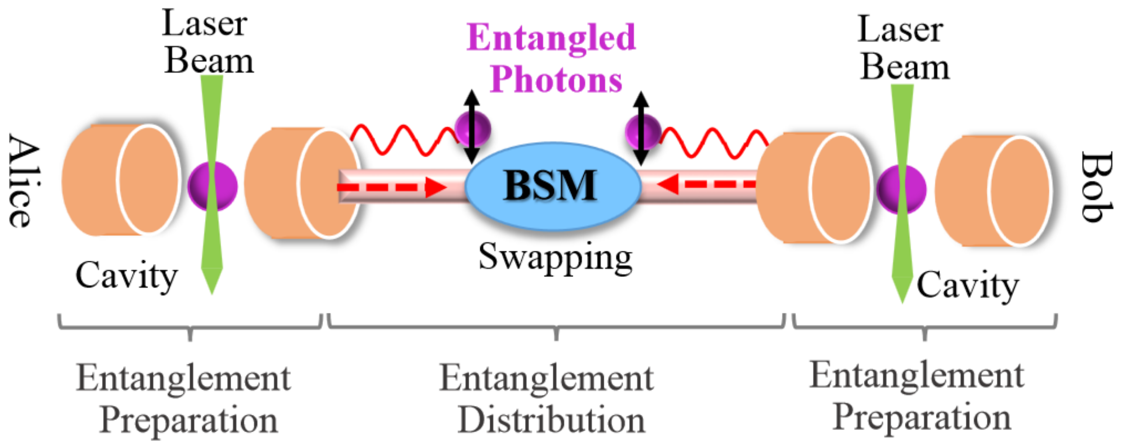

Figure 3. Schematic of entanglement preparation by exciting trapped atoms simultaneously (Li *et. al.*, 2023)

Nadlinger *et al.* (2022) and Zhang *et al.* (2022) used setups similar to Figure 3 to prepare entanglement using ions and atoms traps. The atoms in the cavity are simultaneously excited so that each emits a photon entangled with the atom's quantum state. The photons are then directed through a quantum channel to a beam splitter where the Bell state is measured (BSM) and entanglement swapping occurs so that the users' atoms get entangled.

3. Entanglement-based cryptography

3.1 Entanglement-based quantum key distribution

Several quantum key distribution protocols have been proposed, but the first to exploit the phenomenon of entanglement was E91. In this protocol, entangled particles prevent anyone intercepting the communication from obtaining the information encoded into the quantum systems (e.g. particles), and Bell's theorem is used to test the security of the key distribution. E91 comprises a quantum channel where entangled spin-½ particles are emitted and sent along the *z*-axis towards Alice and Bob, the conventional placeholders for the authorised channel user. Both parties then measure the spin components along 3 directions as shown in Figure 4.

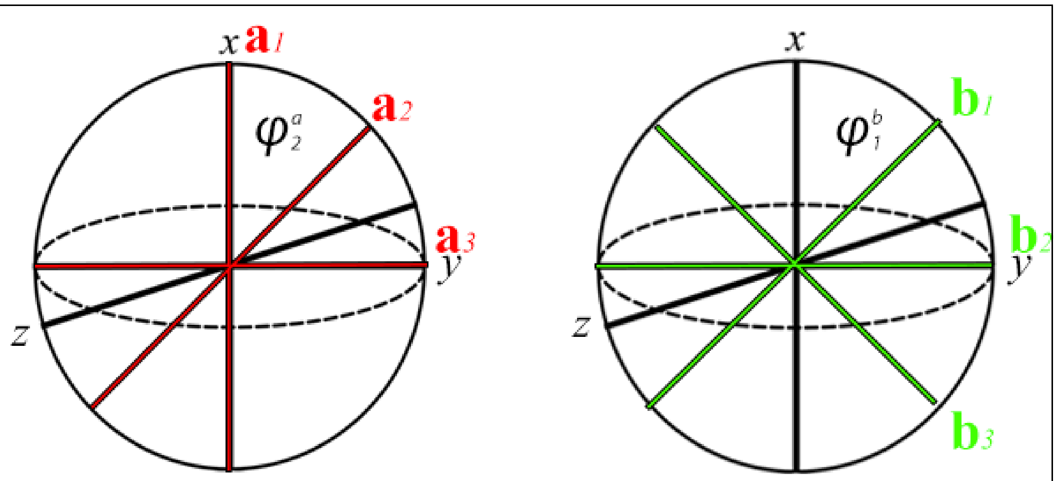

Figure 4. E91 measurement directions depicted on the Bloch sphere and expressed as vectors a_i for Alice and b_j for Bob (*i*,*j* = 1,2,3) in *xy*-plane. The angle φ is measured from the positive *x*-axis for all each measurement as follows: $\varphi_1^a = 0, \varphi_2^a = \frac{\pi}{4}, \varphi_3^a = \frac{\pi}{2}, \varphi_1^b = \frac{\pi}{4}, \varphi_2^b = \frac{\pi}{2}, \varphi_3^b = \frac{3\pi}{4}$, where *a* and *b* refer to Alice's and Bob's detectors.

For each pair of particles, the measurement direction is chosen randomly, and each measurement gives either a spin up or spin down. The results can be used to obtain the correlation:

$$E = P(\mathbf{a}_i = \mathbf{b}_j) - P(\mathbf{a}_i \neq \mathbf{b}_j) \tag{4}$$

where *P* is the probability that the measurement results of each pair agree or disagree. The results are expected to be perfectly anticorrelated when measurement angle of both users matches, i.e. $E(\mathbf{a}_2, \mathbf{b}_1) = E(\mathbf{a}_3, \mathbf{b}_2) = -1$.

The correlation of the results of the measurements at different angles are used to perform a Bell test to calculate the violation of Bell's inequality, where $|S| \leq 2$. For maximally entangled particles, |*S*| should be $2\sqrt{2}$. In the present scenario, *S* is expected to be:

$$S = E(\mathbf{a}_1, \mathbf{b}_1) + E(\mathbf{a}_3, \mathbf{b}_1) + E(\mathbf{a}_3, \mathbf{b}_3) - E(\mathbf{a}_1, \mathbf{b}_3) = -2\sqrt{2} \tag{5}$$

Alice and Bob announce publicly (in a classical channel) their measurement directions and the results of only the different directions to calculate *S*. If the value of *S* matches the above quantum expectation, then no eavesdropping occurred, and the users can use the anticorrelated results they did not announce to form the key. Otherwise, eavesdropping occurred, and the process shall be repeated (Ekert, 1991). Following Ekert's proposal, Bennett, Brassard and Mermin (1992) proposed an entanglement-based version of BB84 called BBM92 as shown in Figure 5.

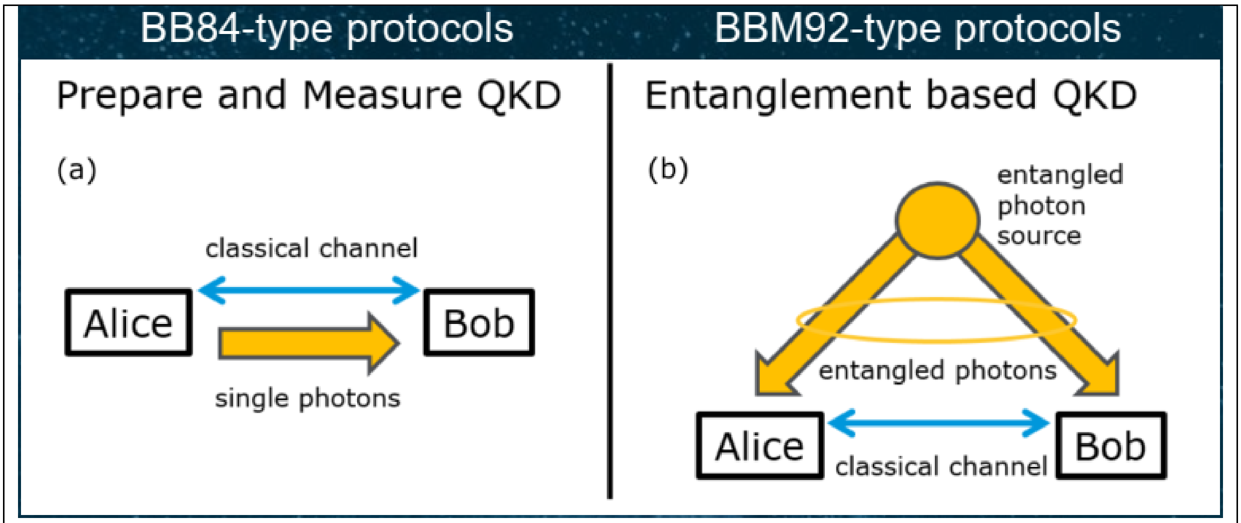

Figure 5. Schematic showing the difference in the designs of BB84 and BBM92. The yellow arrows represent the quantum channel and direction of photons. (Ecker, 2022)

3.2 Device-independent quantum key distribution

Despite its security guarantees, E91 assumes the devices are reliable. Device independent quantum key distribution builds on E91 but does not make this assumption. Figure 6 shows the general setting of this protocol in the worst-case scenario where Eve, the adversary, controls the particles source. Alice and Bob measure their particles to generate a key and do the Bell test. Alice and Bob choose between A_0, A_1, A_2 and B_1, B_2measurements, respectively, with possible outcomes a, b ∈ $\{-1, +1\}$. The raw key, later used to produce the secure key, is obtained from outcomes of the pair $\{A_0, B_1\}$, particularly, the quantum bit error rate (QBER), which is the probability of state mismatch *Q* where:

$$Q = P(a_0 \neq b_1) \tag{6}$$

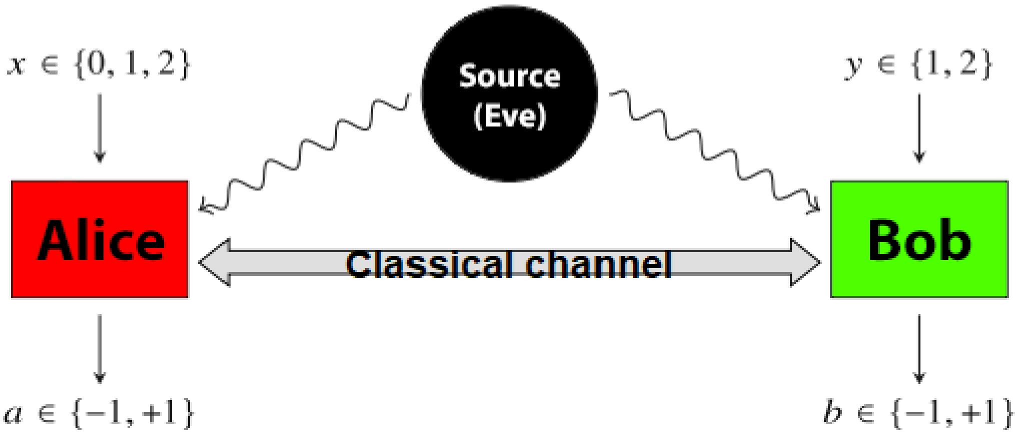

Figure 6 DIQKD setting, where Alice and Bob choose between {0,1,3} and {1,2} measurements, respectively, with outcomes ± 1. Modified from Wolf (2021)

In conjunction with *S*, the indicator of information obtained by Eve, the disagreement probability *Q* is used to estimate the classical post-processing required for error correction, privacy amplification and generation of the raw key. Thus, this protocol has two parameters *S* and *Q*. (Acín *et al.*, 2007) However, it requires an experimental setting efficient in entanglement distribution, detection, and key generation rate over communication-relevant distances. A large *S* and low *Q* should be achieved to generate a secure key known only to Alice and Bob, which is practically challenging, but recent the following experiments showed important results.

3.3 Proof-of-concept experiments

Liu, W.-Z. *et al.* (2022) implemented a DI-QKD protocol using a photonic platform with a detection efficiency of 87.5%. For each round, Alice chooses a random binary input x ∈{1,2} and gets a binary outcome a∈{1,2}, while Bob chooses a triple input y ∈{1,2,3} and gets a binary outcome b∈{1,2}. The users consider the rounds where (x,y) = (1,3) the "key-generation round" with the rest of the rounds considered the "test round" to perform Bell test. Random post-selection was implemented. It reduces the need for error correction by discarding the measurement results that are likely to be full of error with few correlations. As a result, it might produce information insufficient to generate a secret key. As shown in Table 1, there is no record of QBER, which is necessary for the generation of the secret key. Instead, a lower bound for the key rate was calculated using the Shannon limit f_e=1, which is the maximum rate of reliable information in perfect error correction scenario. This is true only in cases of infinite keys, i.e. obtained from infinite information. In real-world setting, only finite keys can be obtained for information sources and environment limitations.

As no key was produced, the security analysis could not be done. The calculated Bell test score is almost at the violation threshold, which is problematic as Bell test is indicative of the information available to the eavesdropper.

Table 1. The outcomes of DI-QKD proof-of-concept experiments. The QBER was not reported in Liu, W.-Z. *et al.* (2022) as random basis selection was not implemented.

Experiment	**Nadlinger *et al.* (2022)**	**Zhang *et al.* (2022)**	**Liu, W.-Z. *et al.* (2022)**
Platform	Trapped ions	Trapped atoms	Photons
Distance/m	2	400	220
Fidelity	0.96 ± 0.01	≥ 0.89 ± 0.023	0.995 ± 0.0015
Bell inequality violation (|*S*| ≥ 2) OR winning probability *ω* ≥ 75%)	*S* = 2.677 ± 0.006	*S* =2.578 ± 0.075	*ω* = 0.7559 *S* ≈ 4 (2ω - 1)= 2.0472
Key generation rate/ bit s^{-1}	0.0639	0.07	2.60
QBER	0.0144 ± 0.0002	0.078 ± 0.009	-
Number of rounds (n)	1.5 x 10^6	3,342	2.4 x 10^8

Scarani *et al.* (2009) argued that QKD implementations could only be photonic, and no other system was expected to be usable in the future, but recent DI-QKD experiments using trapped atoms and ions showed remarkable results and generated actual keys with higher key rates.

Nadlinger *et al.* (2022) used trapped $^{88}Sr^+$ ions over 2 m in their DI-QKD implementation that resulted in a powerful 98,884-bit secure key. Although the key rate and distance reported in Table 1 are low for practical communications, this experiment achieved the highest fidelity and Bell test score with the lowest QBER, which are the requirements for a successful implementation of DI-QKD. Figure 7 shows the set up used.

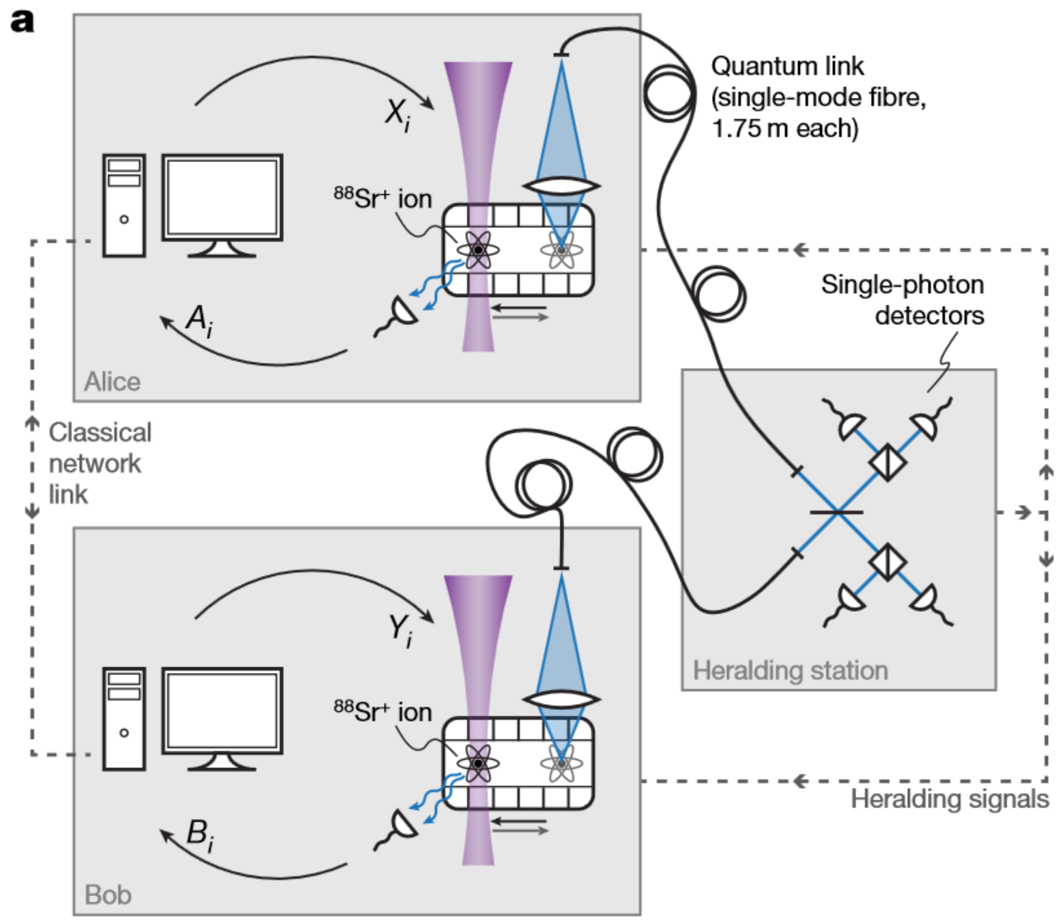

Figure 7. Schematic of the experimental design of Nadlinger et al. (2022) similar to the one in Section 2.3 with detectors to inform the parties of the successful transmission.

In Zhang *et al.* (2022), a DI-QKD protocol was implemented over a quantum channel formed by two optically trapped single ^{87}Rb atoms in buildings about 400 m apart (700 m fibre link). The two atoms were entangled by entanglement swapping, which includes two experiments, one in each building, starting with the generation of entangled atom-photon by exciting the atom and entangling the polarization of the emitted photon with the atomic spin. Photons are then split and guided through the fibre connection to the other building and the detection of the split photons by the detectors in both buildings heralds the successful entanglement between both atoms.

This experiment achieved a higher key rate compared to the trapped ions-based experiment with a compatible Bell violation. The rate could be higher with higher generation efficiency by adding more trapped atoms to the setup. Although the distance is higher than the distance in Nadlinger *et al.* (2022), it is still not practical in real-world setting, but as proof-of-concept the results are promising.

4. Real-world implementations

To take entanglement-based QKD out of the lab, we need networks to connect the users represented in this context by quantum nodes. The following real-world implementations set the foundations of quantum networks using optical fibres and free-space channels in terrestrial and satellite-to-ground field tests to achieve practical communications distances.

4.1 Fibre-optic Networks

4.1.1 DARPA Quantum Network

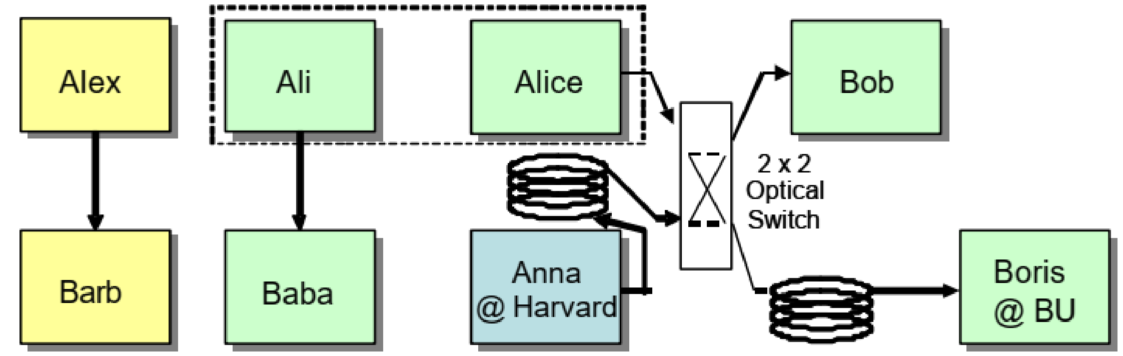

Figure 8. A schematic of the main nodes in the first QKD network DARPA Quantum Network (Eliott, 2005)

DARPA QKD network first operated through dark fibres, i.e. unused fibres, connecting the campuses of Harvard and Boston universities and BBN Technologies labs (Eliott *et al.*, 2005). It comprises 10 nodes and adopts mainly the prepare-and-measure protocol BB84 between the senders Alice and Anna and the receivers Bob and Boris shown in Figure 8. The sender-receiver pair can be changed using the optical switch that links the senders to different receivers. The Ali-Baba nodes constitute a free space system connected to the network through a relay between Alice and Ali. Alex and Barb are the entanglement nodes, but they have not been reported as operational in any recent literature. Table 2 shows the key results from DARPA experiments compared to results from other networks.

Table 2. Summary of the key results from the QKD networks. SECOQC and Tokyo QKD networks implemented other non-entanglement-based QKD protocols, but only the results of BBM92 are reported here in comparison with the non-Ent version BB84 implemented in DARPA

Network	**DARPA (Eliott *et al.*, 2005)**	**SECOQC (Peev *et al.*, 2009)**	**Tokyo (Sasaki *et al.*, 2011)**
Attenuation/ dB km^{-1}	0.21	0.25	1
Protocol	BB84 (prepare and measure)	BBM92 (entanglement-based QKD)	BBM92 (entanglement-based QKD)
QBER	3%	3.5%	5% to 7%
Key rate/ kbps	0.5 to 1	2.5	0.25
Distance/ km	10	16	1

4.1.2 SECOQC quantum key distribution network

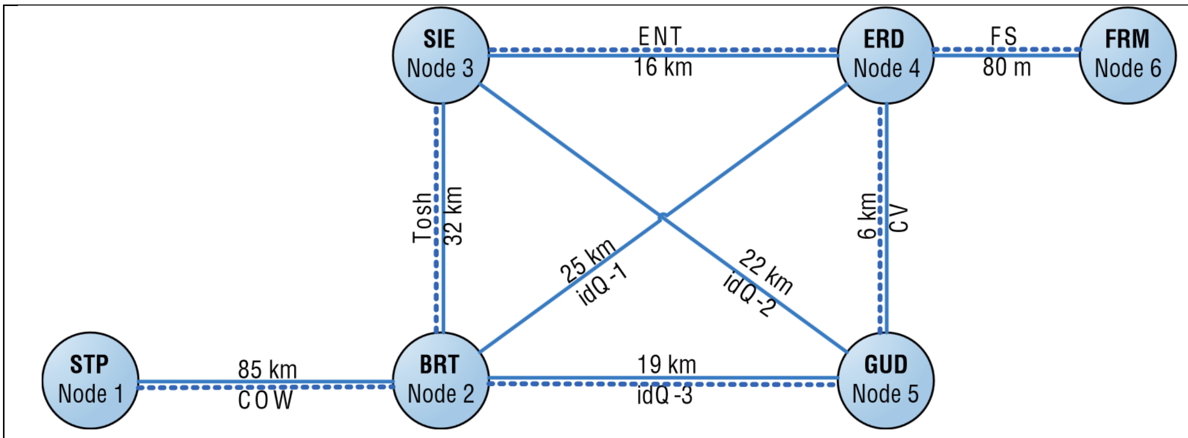

Figure 9. Schematic of the 6-node SECOQC QKD Network. SIE-ERD represents the entanglement-based QKD system (Peev *et al.*, 2009)

The Secure Communication based on Quantum Cryptography (SECOQC) launched a QKD network in Vienna, and the results from 2004 to 2008 were reported in Peev *et al.* (2009). The network comprises 6 nodes as shown in Figure 9, with SIE-ERD link constituting the entanglement-based QKD system. Figure 10 shows the results of the network implementation of BBM92 over 24 hours. The entanglement-based QKD system made use of stabilisation modules to secure a long-term stability of the key distribution and allow for a fully automated initiation. It was the first to achieve a long-term operation of entanglement-based QKD with automatic correction of the environmental effects without intervention from the user. With polarisation visibility above 90% throughout the operation, a stable key was generated using the measured correlations at a rate higher than 2 kbps.

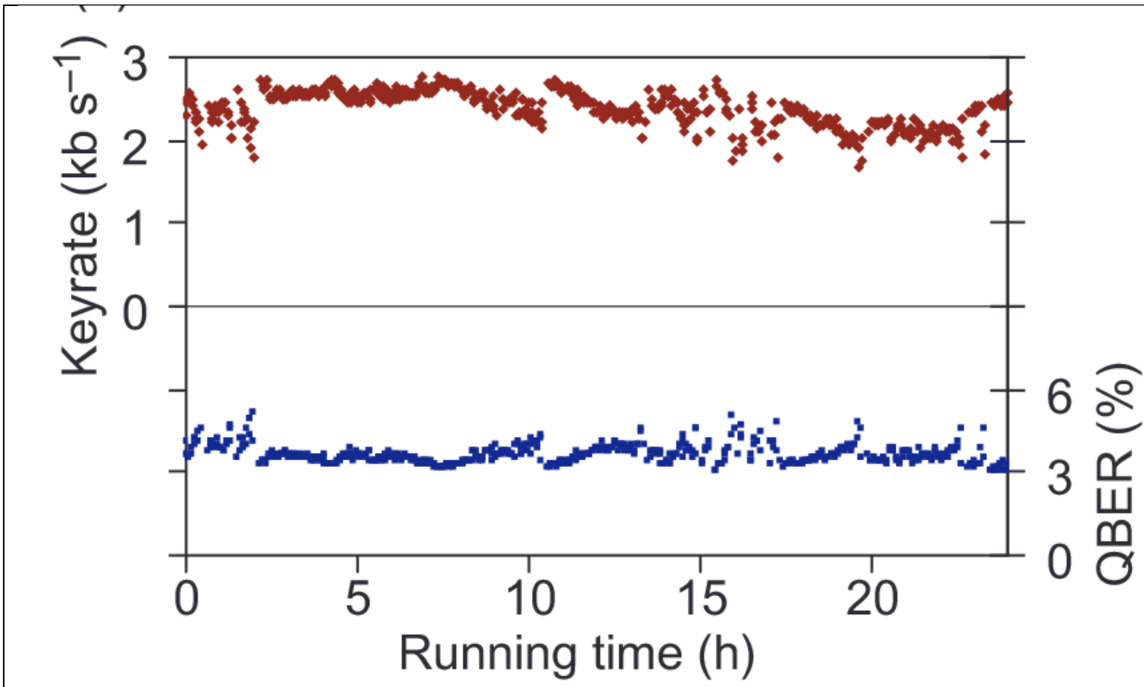

Figure 10. The secure key rate and QBER produced by the SECOQC entanglement-based QKD system as measured over 16 km in 24 hours. (Peev *et al.*, 2009)

4.1.3 Tokyo quantum key distribution network

Tokyo QKD Network is a cooperation between the EU and Japanese organisations that was launched in October 2010. It is a 6-node network implementing several QKD protocols including the entanglement-based QKD protocol BBM92 like the SECOQC QKD Network. Figure 11 shows the configuration of the network which adopts the same scheme as SECOQC's in its entanglement-based QKD system All Vienna. The software was upgraded to make a generic framework from the code used in the system generation in SECQC to facilitate the adaptation to different QKD implementations.

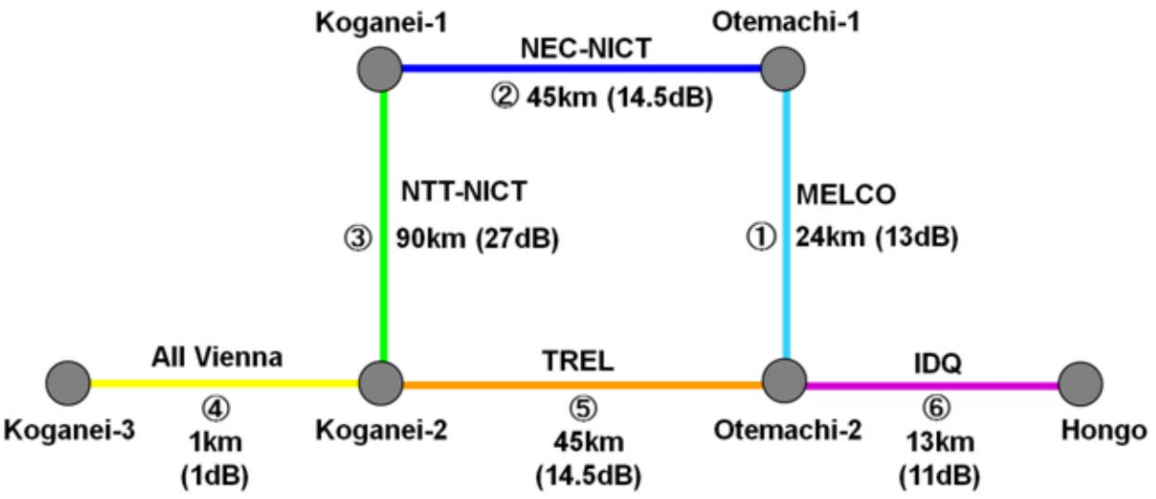

Figure 11. Schematic of the 6-node Tokyo QKD Network. The Koganei-2 – Koganei-3 link (4) (All Vienna) represents the entanglement-based QKD system. (Sasaki *et al.*, 2011)

Despite the similarities between the entanglement-based QKD system in Tokyo and Vienna networks, Table 2 shows that the results were noticeably different. This might be since around 50% of the fibres used in Tokyo QKD Network were aerial and thus affected by environmental fluctuations and crosstalk, which is the leakage of photons from other fibres due to flaws in the fibres.

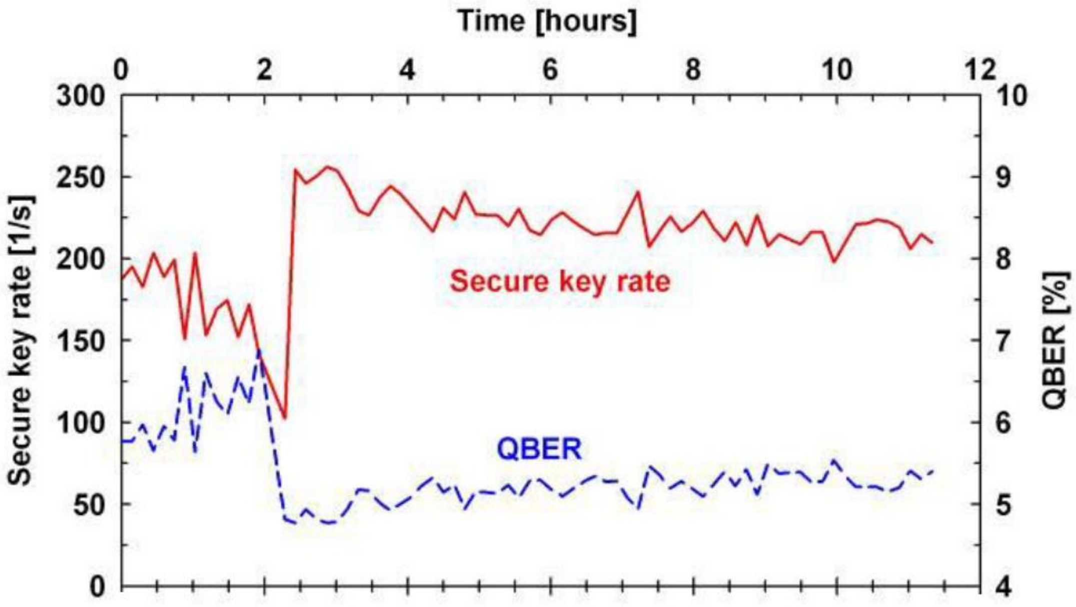

Figure 12. The secure key rate and QBER produced by the All-Vienna system as measured over 1 km in 12 hours. (Sasaki *et al.*, 2011)

Figure 12 shows the implementation key statistics over 12 hours. They dramatically changed after the second hour due to the automatic state alignment mechanism in the system, which optimises the alignment based on the measured correlations.

4.2 Free-space optic channels

To overcome the photon loss and decoherence over long distance, quantum networks should employ trusted relays or quantum repeaters to receive and pass the quantum signals in the same state over longer distances. However, this technology is still immature. Alternatively, satellites could be used to transmit the signals through free-space channels to points on the ground.

The first important field experiment towards using satellites in QKD was Ursin *et al.* (2007). They produced polarization-entangled pairs of photons on La Palma where one of the photons was measured locally and the other was transmitted through a transceiver to a telescope on Tenerife. Table 3 summarises the results in comparison with more recent free-space experiments in real-world settings.

Table 3. Summary of the results of the most prominent free space implementations of entanglement-based QKD.

Implementation	**Ursin *et al.* (2007)**	**Yin *et al.* (2017)**	**Yin *et al.* (2020)**
Setup	Terrestrial free-space channels	Satellite-to-ground	Satellite-to-ground
Protocol	E91	BBM92	BBM92
Distance/km	144	530-1000	1,120
Fidelity	Not reported	≥ 0.86	0.910 ± 0.007
Violation of Bell inequality (|*S*| ≥ 2)	2.508 ± 0.037	2.37 ± 0.09	2.56 ± 0.07
Key generation rate/bit s^{-1}	2.37	3.5	0.12
QBER	4.8% ± 1%	8.1% ± 1.59%	4.5% ± 0.37%

It should be noted that in free-space experiments tracking lasers are used, which could lead to crosstalk with the photon signal. In Ursin *et al.* (2007), the laser was directed in the opposite direction and interference filers were also used to eliminate the crosstalk.

Yin *et al.* conducted two experiments by sending photons from Micius, a satellite with an entangled-photon source and a measurement module, to ground observatories. In Yin *et al.* (2017), one photon of the entangled pair was measured locally at Micius and the other was sent to Delingha observatory. In Yin *et al.* (2020), one photon was sent to Delingha and the other was sent to Nanshan observatory. Both experiments covered much longer distances as shown in Table 1 with high Bell inequality violation. The fidelities in both experiments were high as well because of the high-efficiency telescopes used. The attenuation, i.e. the photon loss, was also low at nearly 0.03 dB km^{-1} as most of the transmission happened in empty space with the effective atmospheric thickness being around 10 km only. Figure 13 shows improved attenuation, which was reflected in the higher QBER and fidelity in Yin *et al.* (2020).

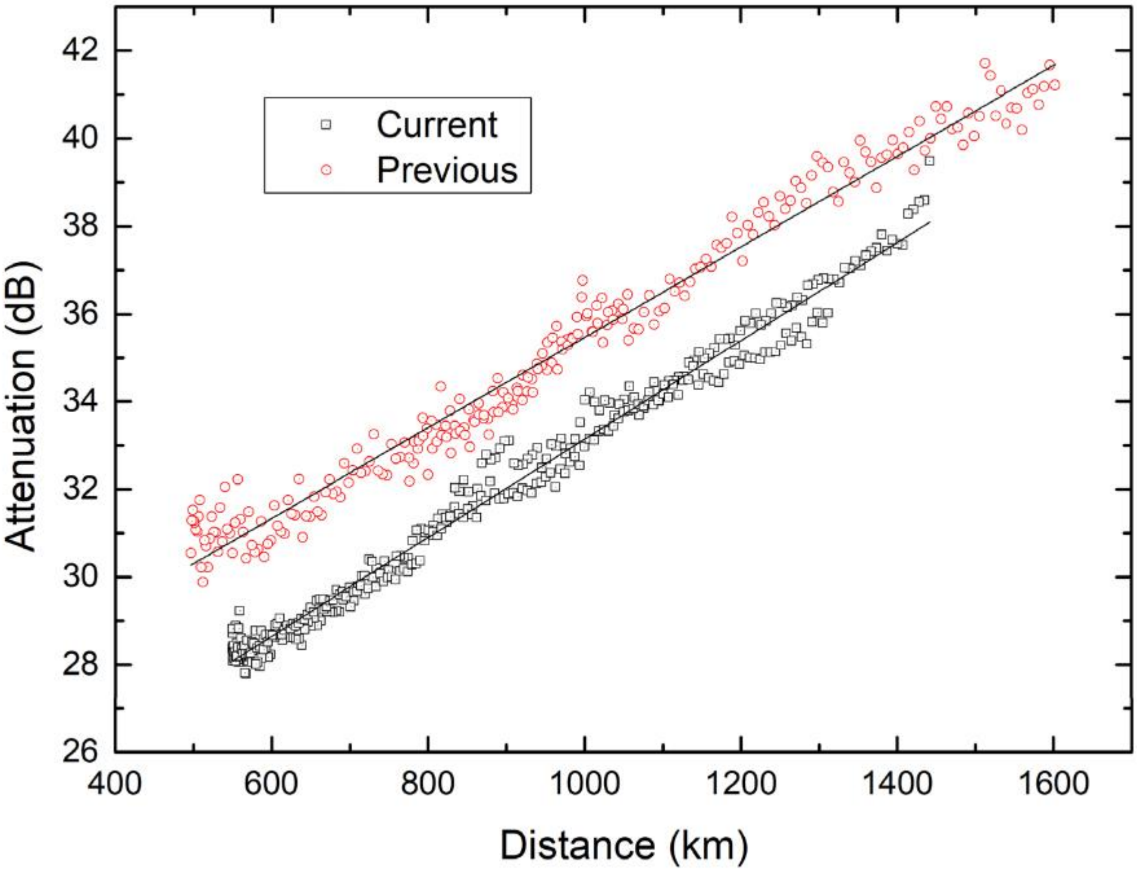

Figure 13. Comparison between the attenuation in Yin *et al.* (2017), in red, and Yin *et al.* (2020), in black, indicating improved efficiency (Yin *et al.*,2020)

5. Practical challenges

5.1 Inherent weaknesses of quantum systems

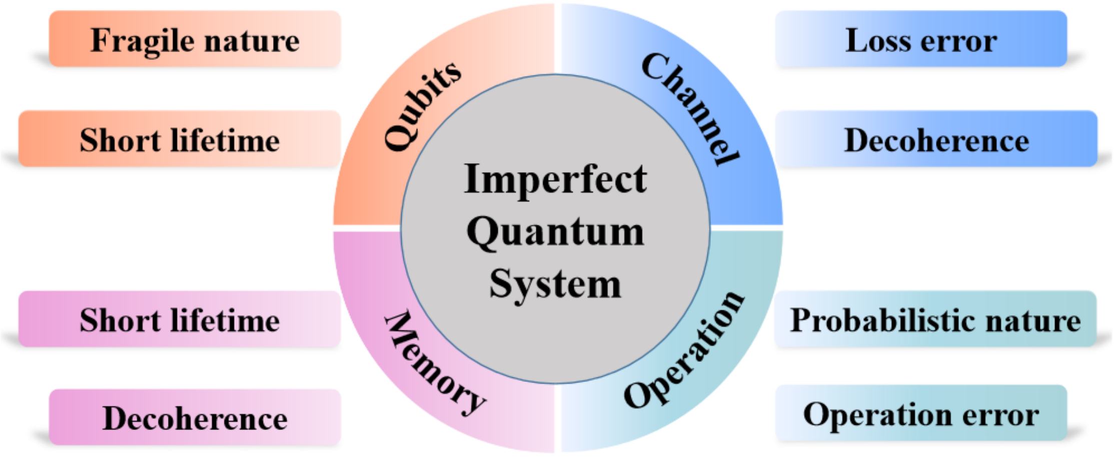

Figure 14. Weaknesses of the quantum systems components (Li *et al.*, 2023)

The quantum systems have weaknesses shown in Figure 14. In quantum communications, the information is encoded into qubits that are susceptible to state alteration and noise due to environmental factors, which eventually leads to the loss of information with the decrease of fidelity, which represents how close the received state is to the transmitted state. The transmission process and interaction with the environment also cause photon loss and quantum decoherence, which is the loss of quantum properties and transformation into a classical system. This prevents the preparation and end-to-end transmission of a perfect entanglement. The lifetime of qubits can be enhanced by using quantum memories. However, in addition to its cost, the quantum memory has a limited storage capacity and is subject to decoherence, as well. There are also the problems of the probability associated with all the quantum operation and error rates. This makes the quantum systems inherently difficult to control and operate in real-world settings (Li *et al.*, 2023).

5.2 Network scalability and communication rate

The examples in Section 4 show that the feasibility of an entanglement-based metropolitan area network was tested and confirmed nearly a decade ago. However, there are limitations to these models. DARPA is switch based where only the connected pairs at a certain time can exchange keys. SECOQC and Tokyo QKD networks are trusted node based, and it is not possible to trust that all nodes are safe from eavesdropping. The fully connected network is a third type that has been deployed recently. In this model, it is possible to share multipartite entanglement between several parties simultaneously. Joshi *et al.* (2020) successfully implemented a modified version of BBM92 in a metropolitan network in Bristol comprising 8 nodes connected through 28 links, with no need to trust the nodes. Liu, X. *et al.* (2022) also proposed a 40-user, 780-link network, but this type of network is complex and unscalable. It also produces a low key rate. Figure 15 shows the finite key rate in Bristol network against the lab results.

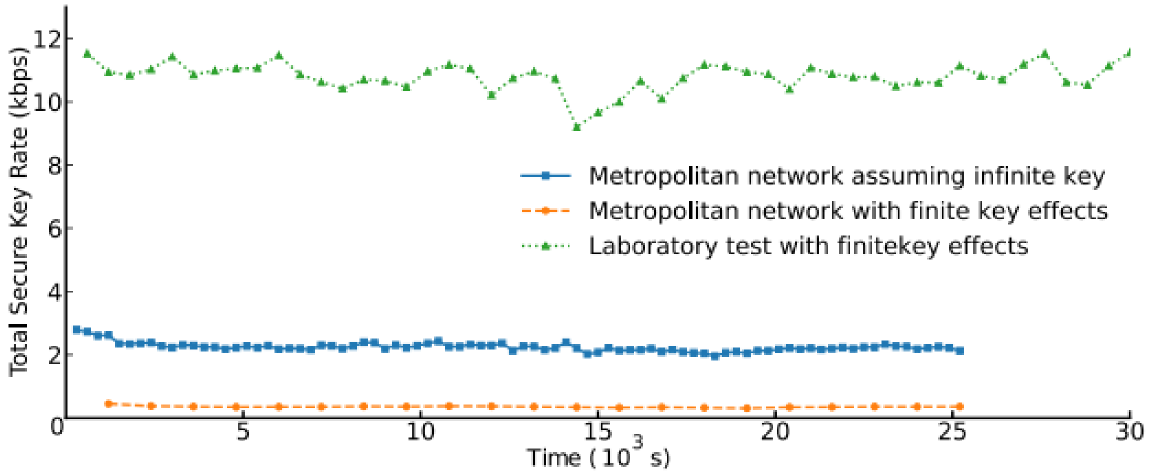

Figure 15. A 7-hour measurement of the key rate in Bristol network over ~17 km compared to the lab results (Joshi *et al.*, 2020)

In city-wide implementations, the key rate is affected by environmental factors, noise, and losses, which makes it challenging to achieve a practical communication rate.

5.3 Integration with existing infrastructure

For cost efficiency, the QKD networks should make use of the existing optical fibre infrastructure instead of establishing separate networks. Most of the field trials used already-deployed dark fibres, but for a global QKD to be realised, quantum signals should coexist with classical communications in used fibres as dark fibres are not abundant enough to cover practical communication areas. This coexistence is problematic as the quantum signals, where each pulse carries a few photons, are much weaker than the classical signals, where each pulse can carry millions of photons. Due to this weakness, quantum signals have a shorter transmission distance compared to classical signals. Quantum signals could also deteriorate and be altered by classical signals because of light-matter interactions and the noise quantum signals experience in classical channels (Mao *et al.*, 2018).

To overcome these problems, wavelength division multiplexing (WDM) is used for the transmission of different signals in the same fibre at different wavelengths. WDM results however in insertion losses, i.e. the loss of photons when the signal passes through the WDM component, which reduces the key rate and the transmission distance (Sharma *et al.*, 2021).

6. Discussion

6.1 Protocols

The communication security guaranteed by quantum entanglement is theoretical. It assumes that devices would not deviate from the ideal, theoretical model, while real-world setups are flawed. Compared to E91 and BBM92, DI-QKD is secure against manipulation of the entanglement preparation and distribution devices. However, it is not immune against flaws in the user’s detection and measurement devices, which lead to side-channel attacks that do not require the adversary to interact with the signals and consequently introduce disturbance to extract information about the communication. Proposed systems usually run security analyses and propose countermeasures, but a foolproof cryptosystem should inherently prevent the attacks. Measurement-device-independent QKD (MDI-QKD) can eliminate all side-channel attacks, but it requires a complex setup with a perfect characterisation of the entanglement sources. Navarrate *et al.* (2021) proposed that the absolute security of MDI-QKD depends on upper bounding the parameters describing the sources quality, which is yet to be achieved. A global implementation would also require more resources that compromise the practicality.

It can be concluded that there is no favourable protocol. So far, trade-offs are inevitable depending on the available resources and the goal and level of security required for a certain implementation. More field experimentation and optimisation are needed to decide on an entanglement-based protocol that is standardisable.

6.2 Platforms and deployment

Table 4. Brief evaluation of photonic and atom-based platforms based on the reported experiments

Platform	Photonic	Atom-based
Distance coverage	✓	
Long coherence time		✓
Maturity	✓	
Scalability	✓	
Real-world implementations	✓	

Table 4 briefly compares between photonic and atom-based platforms.

You might think that photonic platforms are winning, but the atom-based score higher in a vital aspect and could be a solution to the decoherence challenges.

For real-world quantum channels, the optical fibres could be the better option cost-wise, but before finding a mechanism for fibres to accommodate quantum and classical signals efficiently, optical fibres deployment will be either limited to dark fibres or costly. In terms of flexibility and covering longer distance, the free-space channels using satellites and telescopes score higher.

Currently, QKD is deemed an impractical security solution for the difficulty of controlling the quantum properties and the high deployment cost, but in the long run it will have more opportunities. In addition to benefiting from the quantum hardware that is actively being developed, the experiments reported here show that entanglement-based QKD is maturing and advancing. There are no favourable choices for the preparation and distribution processes until now, but this leads to the need to consider hybrid global deployments and work on the interoperability.

7. Conclusion

7.1 Summary

This study has reviewed the use of quantum entanglement and quantum properties of particles in securing communications and covered important lab and real-world implementations. The monogamy of quantum entanglement together with the no-cloning theorem and Bell’s inequalities are used to design QKD protocols guaranteeing theoretical security. DI-QKD protocols are proposed as a step towards closing the gap between the theoretical security and the implementation security. Recent lab experiments using different entanglement preparation schemes have successfully generated secure encryption keys. Larger distances have been achieved recently in real-world implementations over entanglement-based links in large-scale terrestrial and satellite-assisted networks. Despite these advancements, the global deployment and standardisation of entanglement-based QKD face practical challenges, including the difficulty of controlling the environment-sensitive quantum systems. Achieving scalability and practical communication rates are also challenging with the current technologies. The high cost of constructing separate quantum networks requires addressing the challenging task of integrating QKD with the existing infrastructure used for classical communications. Currently, there is no winning entanglement-based QKD system, but there are opportunities in considering a combined system employing the advantages of different components in the preparation and distribution processes.

7.2 Future research

Future research and experiments should work on hybrid implementations and confirm the interoperability of QKD systems. Further optimization and field experimentation with DI-QKD and MDI-QKD could enhance the security provided by entanglement-based networks. Devising key rate optimization methods is also key to achieve practical communication rates with the current technology and working on mechanisms to integrate classical and quantum communications in the fibre networks in use.

References

Acín, A. *et al.* (2007) 'Device-independent security of quantum cryptography against collective attacks', *Physical review letters*, 98(23), pp. 230501–230501. Available at: https://doi.org/10.1103/PhysRevLett.98.230501.

Alagic, G. *et al.* (2022) *Status report on the third round of the NIST Post-Quantum Cryptography Standardization process*. NIST IR 8413-upd1. Gaithersburg, MD: National Institute of Standards and Technology (U.S.), p. NIST IR 8413-upd1. Available at: https://doi.org/10.6028/NIST.IR.8413-upd1.

Bennett, C.H. and Brassard, G. (1984) 'Quantum cryptography: Public key distribution and coin tossing', *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, 10-12 December 1984*, 175-179. Available at: https://dx.doi.org/10.1016/j.tcs.2014.05.025.

Bennett, C.H., Brassard, G. and Mermin, N.D. (1992) 'Quantum cryptography without Bell's theorem', *Physical Review Letters*, 68(5), pp. 557–559. Available at: https://doi.org/10.1103/PhysRevLett.68.557.

Clauser, J.F. *et al.* (1969) 'Proposed Experiment to Test Local Hidden-Variable Theories', *Physical Review Letters*, 23(15), pp. 880–884. Available at: https://doi.org/10.1103/PhysRevLett.23.880.

Coffman, V., Kundu, J. and Wootters, W.K. (2000) 'Distributed entanglement', *Physical Review A*, 61(5), p. 052306. Available at: https://doi.org/10.1103/PhysRevA.61.052306.

Ecker, S. (2022) 'Advances in entanglement-based QKD for space applications', *International Conference on Space Optics — ICSO 2022*, Dubrovnik, Croatia: SPIE, p. 79. Available at: https://doi.org/10.1117/12.2689972.

Ekert, A.K. (1991) 'Quantum cryptography based on Bell's theorem', *Physical Review Letters*, 67(6), pp. 661–663. Available at: https://doi.org/10.1103/PhysRevLett.67.661.

Elliott, C. (2005) 'The DARPA Quantum Network', in A. Sergienko (ed.) *Quantum Communications and Cryptography*. CRC Press (Optical Science and Engineering), pp. 83–102. Available at: https://doi.org/10.1201/9781420026603.ch4.

Elliott, C. *et al.* (2005) ‘Current status of the DARPA quantum network (Invited Paper)’, in E.J. Donkor, A.R. Pirich, and H.E. Brandt (eds). *Defense and Security*, Orlando, FL, pp. 138–149. Available at: https://doi.org/10.1117/12.606489.

Joshi, S.K. *et al.* (2020) ‘A trusted node–free eight-user metropolitan quantum communication network’, *Science Advances*, 6(36), p. eaba0959. Available at: https://doi.org/10.1126/sciadv.aba0959.

Kim, Y. *et al.* (2023) ‘Evidence for the utility of quantum computing before fault tolerance’, *Nature*, 618(7965), pp. 500–505. Available at: https://doi.org/10.1038/s41586-023-06096-3.

Li, Z. *et al.* (2023) ‘Entanglement-Assisted Quantum Networks: Mechanics, Enabling Technologies, Challenges, and Research Directions’, *IEEE Communications Surveys & Tutorials*, pp. 1–1. Available at: https://doi.org/10.1109/COMST.2023.3294240.

Liu, W.-Z. *et al.* (2022) ‘Toward a Photonic Demonstration of Device-Independent Quantum Key Distribution’, *Physical Review Letters*, 129(5), p. 050502. Available at: https://doi.org/10.1103/PhysRevLett.129.050502.

Liu, X. *et al.* (2022) ‘40-user fully connected entanglement-based quantum key distribution network without trusted node’, *PhotoniX*, 3(1), p. 2. Available at: https://doi.org/10.1186/s43074-022-00048-2.

Mao, Y. *et al.* (2018) ‘Integrating quantum key distribution with classical communications in backbone fibre network’, *Optics Express*, 26(5), p. 6010. Available at: https://doi.org/10.1364/OE.26.006010.

Nadlinger, D.P. *et al.* (2022) ‘Experimental quantum key distribution certified by Bell’s theorem’, *Nature (London)*, 607(7920), pp. 682–686. Available at: https://doi.org/10.1038/s41586-022-04941-5.

Navarrete, Á. *et al.* (2021) ‘Practical Quantum Key Distribution That is Secure Against Side Channels’, *Physical Review Applied*, 15(3), p. 034072. Available at: https://doi.org/10.1103/PhysRevApplied.15.034072.

Nurhadi, A.I. and Syambas, N.R. (2018) ‘Quantum Key Distribution (QKD) Protocols: A Survey’, in *2018 4th International Conference on Wireless and Telematics (ICWT)*.

2018 4th International Conference on Wireless and Telematics (ICWT), Nusa Dua: IEEE, pp. 1–5. Available at: https://doi.org/10.1109/ICWT.2018.8527822.

Peev, M. *et al.* (2009) 'The SECOQC quantum key distribution network in Vienna', *New Journal of Physics*, 11(7), p. 075001. Available at: https://doi.org/10.1088/1367-2630/11/7/075001.

Rosenblum, S. *et al.* (2016) 'Extraction of a single photon from an optical pulse', *Nature photonics*, 10(1), pp. 19–22. Available at: https://doi.org/10.1038/nphoton.2015.227.

Sasaki, M. *et al.* (2011) 'Field test of quantum key distribution in the Tokyo QKD Network', *Optics Express*, 19(11), p. 10387. Available at: https://doi.org/10.1364/OE.19.010387.

Scarani, V. *et al.* (2009) 'The security of practical quantum key distribution', *Reviews of Modern Physics*, 81(3), pp. 1301–1350. Available at: https://doi.org/10.1103/RevModPhys.81.1301.

Sharma, P. *et al.* (2021) 'Quantum Key Distribution Secured Optical Networks: A Survey', *IEEE Open Journal of the Communications Society*, 2, pp. 2049–2083. Available at: https://doi.org/10.1109/OJCOMS.2021.3106659.

Thomas, S. and Senellart, P. (2021) 'The race for the ideal single-photon source is on', *Nature nanotechnology*, 16(4), pp. 367–368. Available at: https://doi.org/10.1038/s41565-021-00851-1.

Ursin, R. *et al.* (2007) 'Entanglement-based quantum communication over 144 km', *Nature Physics*, 3(7), pp. 481–486. Available at: https://doi.org/10.1038/nphys629.

Wolf, R. (2021) *Quantum Key Distribution: An Introduction with Exercises*. Cham: Springer International Publishing (Lecture Notes in Physics). Available at: https://doi.org/10.1007/978-3-030-73991-1.

Wootters, W.K. and Zurek, W.H. (1982) 'A single quantum cannot be cloned', *Nature (London)*, 299(5886), pp. 802–803. Available at: https://doi.org/10.1038/299802a0.

Yin, J. *et al.* (2017) ‘Satellite-to-Ground Entanglement-Based Quantum Key Distribution’, *Physical Review Letters*, 119(20), p. 200501. Available at: https://doi.org/10.1103/PhysRevLett.119.200501.

Yin, J. *et al.* (2020) ‘Entanglement-based secure quantum cryptography over 1,120 kilometres’, *Nature*, 582(7813), pp. 501–505. Available at: https://doi.org/10.1038/s41586-020-2401-y.

Zhang, W. *et al.* (2022) ‘A device-independent quantum key distribution system for distant users’, *Nature*, 607(7920), pp. 687–691. Available at: https://doi.org/10.1038/s41586-022-04891-y.