Higher-Dimensional Quantum Cryptography for Maritime Infrastructures

Thomas Unglaub, Aaron Frederick Lye and Niklas Kostrzewa
German Aerospace Center (DLR), Institute for the Protection of Maritime Infrastructures
Fischkai 1, 27572 Bremerhaven, Germany
{thomas.unglaub, aaron.lye, niklas.kostrzewa}@dlr.de

***Abstract*—Quantum cryptography has emerged as a rapidly advancing field in recent years and represents one of the first practical applications of quantum physics beyond purely theoretical research. Despite its potential, current quantum cryptographic systems remain highly sensitive to noise. High-dimensional implementations offer a promising strategy to enhance robustness. In this work, we investigate high-dimensional quantum key distribution protocols. Particular emphasis is placed on maritime communication scenarios, where harsh environmental conditions, atmospheric turbulence, and platform motion introduce significant noise and instability.**

***Index Terms*—High-dimensional quantum communication, maritime infrastructure, qudit, quantum communication, higher-dimensional quantum systems, quantum cryptography**

I. Introduction

Maritime infrastructures such as seaways, ports, offshore wind farms, oil rigs, pipelines and underwater cables are dependent on networks of information technology and operational technology, making them susceptible to cyber attacks. Due to the criticality of these systems, successful attacks could lead to negative outcomes such as the disruption of power supplies, disturbance in maritime commerce, internet connection failures or endangerment of life at sea. A strong cryptographic foundation, combined with provably correct system design, represents a well-founded mitigation strategy that offers quantifiable guarantees for the confidentiality, integrity, and authenticity of data and services across these networks.

In recent years, there has been a substantial amount of research on quantum computers. If this research succeeds in the construction of a large-scale universal quantum computer, due to the algorithms presented by Shor in [40] this computer will break many of the public-key cryptographic systems that are currently considered secure.

To provide protection against an attacker having access to a quantum computer new cryptographic primitives have to be used. Moreover, as the set of potential threat actors in the maritime domain includes foreign governmental agencies and organized crime, i.e., actors with substantial resources, the adaptation of new cryptography should be addressed in a timely manner. But maritime infrastructures are complex networks of cyber-physical systems and strong safety requirements stipulated in international legislation make the introduction of new cryptography to this field a significant challenge. Even traditional cyber security is severely underdeveloped in the maritime domain.

In this paper we discuss the potential of quantum cryptography for maritime infrastructures. We develop an argument why maritime quantum cryptography should use higher dimensions and discuss specific cases.

The paper is organized as follows. First we give an overview over first establishments of quantum key distribution (QKD) in real world applications (Section II). Then QKD will be presented as a protocol providing information-theoretic security and the two-dimensional QKD is discussed in Section III. In Section IV, we discuss high-dimensional quantum key distribution (HD-QKD) including a protocol that encodes information in multiple subspaces. This approach increases noise resilience and enables more robust key distribution. Practical implementations of HD-QKD are discussed, demonstrating its feasibility for secure maritime communication. Section V contains a conclusion and outlines further research directions.

II. Real world deployments

In the following we give an overview over first establishments of QKD in real world applications.

A. From fiber optics to satellites

The principle of QKD was introduced in [3]. The authors proposed photons as carriers of information, as they can be generated, transmitted, and measured in a controlled manner. Different degrees of freedom (DoF) can be used to encode information in a photon. Polarization or frequency can be used to represent qubits $|0\rangle$ and $|1\rangle$. A first demonstration followed in 1991 over 32 cm of fiber [2]. Since then, research has led to increasingly large fiber-based QKD networks.

Early large-scale fiber networks include the DARPA network in 2004 with 10 stations in Massachusetts [22]. In Europe, the SECOQC network in Vienna (2008) and the Id Quantique network in Geneva (2009–2011) are notable [15]. Similar demonstrations followed in China [17] and Russia [14]. Despite progress, fiber-based QKD is distance-limited, which motivated satellite approaches.

In 2017, the Chinese Micius satellite enabled entanglement distribution over 2,400 km between ground stations [49]. This was part of the QUESS mission and enabled international QKD experiments between China and Austria [48]. Combined with a 2,000 km fiber backbone in China [45], this formed the first satellite-integrated QKD network [30]. Further satellite plans were announced [24].

Similar developments followed worldwide. Japan demonstrated space-to-ground laser communication [23]. The ESA initiated programs such as ScyLight and SAGA to support EuroQCI and QCI4EU infrastructure [46]. Projects such as QKDSat with Arqit, QEYSSat in Canada, Russian satellite efforts [14], NASA's NSQL initiative [41] and Indian demonstrations [10, 32] show global activity toward satellite-based QKD.

These efforts clearly show that QKD has moved beyond academic research and despite the availability of post-quantum cryptography, states continue to pursue quantum key distribution.

B. Realization of QKD systems in the maritime domain

QKD for maritime systems was theoretical sketched in [33] and practical implementations in maritime environments are already underway. A prominent example is the quantum communication network established at the Port of Rotterdam, where a scaleable fiber-based QKD infrastructure connects port authorities and logistics stakeholders via a central hub architecture, enabling secure key exchange for critical operational and logistics data [35]. Similar pilot projects demonstrate QKD transmission where critical data were secured using Toshiba's multiplexed QKD system over 140 km of submarine fiber. The system successfully demonstrated stable quantum key exchange under real maritime communication conditions [37]. Another project showed successfully quantum communication with vessels on water [36]. Furthermore, recent research proposes a simulation of an unmanned areal vessel-assisted and satellite-integrated QKD network, where dynamic airborne relay nodes enable QKD over extended maritime distances under realistic environmental conditions [25].

III. Quantum Key Distribution Protocols

In this section we recall the main principle of QKD protocols in two-dimensional complex Hilbert space $\mathcal{H}_2$.

A. Main concepts

In all QKD protocols, two legitimate parties, traditionally called Alice and Bob, aim to establish a shared secret key using quantum mechanical phenomena. More specifically, the fundamental power of quantum cryptography is based on two core principles of quantum mechanics.

1) No-cloning Theorem [47], i.e., no quantum state can be copied in such a way as it can be done classically.
2) Each interaction with the quantum state changes the quantum states. Malicious manipulation can be quickly detected by the trustworthy parties [29].

QKD protocols, despite their apparent diversity, can be abstractly described as consisting of three fundamental phases. These phases can be summarized as follows (for more details we refer to [29]):

1) **Quantum State Distribution:** Alice and Bob receive quantum states prepared by a source. The states can be transmitted directly from Alice to Bob, or shared via an entangled source, depending on the specific protocol.
2) **Measurement:** Both parties perform measurements on their respective quantum states. The choice of measurement basis may be random or predetermined, depending on the protocol design. The measurement outcomes form the raw data from which the secret key will be extracted.
3) **Classical Post-Processing:** Alice and Bob communicate over a public classical channel to reconcile their measurement outcomes, detect potential eavesdropping, and distill a shared secret key. This phase typically includes sifting, error correction, and privacy amplification.

This three-phase abstraction provides a unified view of QKD protocols, highlighting the essential roles of quantum transmission, measurement, and classical post-processing in establishing secure keys.

B. BB84 protocol

As an illustrative example of the three-phase QKD framework, we consider the BB84 protocol introduced in [3]. The protocol can be naturally described in terms of the three phases outlined above:

1) **Quantum State Distribution:** Alice prepares a sequence of qubits, each randomly encoded in one of two bases: the rectilinear basis $\{|0\rangle, |1\rangle\}$ or the diagonal basis $\{|+\rangle, |-\rangle\}$, where $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, i.e., the two superpositions of $|0\rangle$ and $|1\rangle$ with equal probability. She then sends these qubits to Bob over a quantum channel.
2) **Measurement:** Bob independently chooses a random basis (rectilinear or diagonal) for each incoming qubit and measures it. If Bob's chosen basis matches Alice's preparation basis, the measurement outcome will coincide with Alice's bit; otherwise, the outcome is random.
3) **Classical Post-Processing:** After all qubits have been transmitted and measured, Alice and Bob communicate over a public classical channel to reveal the bases used for each qubit (but not the measurement outcomes). They discard all bits for which their bases differ. The remaining bits form a raw key, which is further processed through error correction and privacy amplification to produce a secure shared key.

A similar protocol using entanglement of qubits was developed by Bennett, Brassard and Mermin (BBM92) [4].

C. Noise consideration

Without noise, each QKD protocol works perfectly. They mainly differ in how they deal with noise. Quantum bit error rate (QBER) is one approach to quantify noise in such scenarios. QBER is defined as the ratio of detected errors N_{error} against the total amount of send qubits N_{total}:

$$\text{QBER} = \frac{N_{\text{error}}}{N_{\text{total}}}.$$

The acceptable threshold is defined by Alice and Bob in the end. Experiments substantiate to limit the QBER to 11% [39].

Accordingly, the BB84 protocol follows the general three-phase structure of QKD quantum state distribution, measurement, and classical post-processing and thus illustrates how fundamental quantum properties, the no-cloning theorem and the disturbance of quantum states upon measurement, ensure security against eavesdropping.

IV. High-dimensional quantum key distribution

As outlined in Section II quantum states are currently transmitted primarily via free-space channels. This also holds in maritime scenarios. Quantum communication on land is already challenging, but the situation becomes more difficult over water. On ships, constant motion induced by waves introduces alignment and stability issues that can significantly impact the performance of QKD systems [5]. Moreover, environmental factors strongly affect performance; cloudy weather can rapidly reduce the achievable key rate [18]. A promising approach to mitigate such environmental noise is HD-QKD. Building on the BB84 protocol, several works have demonstrated that high-dimensional entanglement is inherently more resilient to noise [9, 11, 1, 8, 52].

A. HD-QKD protocol

In HD-QKD, information is encoded not into two-level qubits $|0\rangle, |1\rangle$, but into d-dimensional qudits $|0\rangle, \ldots, |d-1\rangle$, i.e., we utilize the n-dimensional complex Hilbert space $\mathcal{H}_n$ now. There are several HD-QKD protocols. HD-BB84 is similar to the protocol which was shown in Section III-B [13]. The main challenge lies in the definition of the bases. The most common and widely investigated bases are the so called mutually unbiased bases (MUB). In theory a complete set of such bases $\mathcal{B}$ consists out of $d+1$ bases [21]. For dimension $d = p^n$, with p being any prime number and $n \in \mathbb{N}$, such a set of MUB can be found easily. However, finding MUB for $d \neq p^n$ is an open problem [12]. Extending the BB84 protocol to higher dimension, Alice would prepare their qudit in a set of MUB and Bobs measurement consists out of the same set of MUB.

To see the true nature of high-dimensional quantum communication, we want to present another protocol here which is promising to overcome extreme noise.

B. HD-QKD using subspaces

The protocol was developed by Mirdit Doda et. al [11]. A simplified version of this protocol is shown below:

1) **Quantum State Distribution:** An high-dimensional entangled quantum state ρ_{AB} is distributed by a source to Alice and Bob.
2) **Measurement:** Both parties choose from a set of MUB uniformly, independently and randomly a bases in a specific subspace. For a dimension d, we consider a decomposition into l mutually subspaces $\{\mathcal{H}_m\}_{m=1}^{l}$, each of dimension k. This decomposition satisfies the dimensional constraint $d = k \times l$.
3) **Classical Post-Processing:** Following quantum state transmission, Alice and Bob perform sifting via an authenticated classical channel. Each party publicly announces:
   a) The subspace index $m \in \{1, \ldots, l\}$ corresponding to their measurement basis choice, and
   b) the specific basis $\mathcal{B}_m^{(i)}$ used for the measurement.

   A round is retained only when both the subspace indices and basis choices coincide (i.e., $m_A = m_B$ and $\mathcal{B}_A = \mathcal{B}_B$). Retained rounds constitute the raw key from which the final secret key is distilled through error correction and privacy amplification protocols.

This protocol demonstrates enhanced noise resilience compared to conventional HD-QKD implementations [11].

C. Noise resistance of HD-QKD

A key operational difference between qubit- and qudit-based schemes is the dimension dependence of the security bounds. While two-dimensional protocols such as BB84 tolerate a QBER of approximately 11% under coherent attacks, high-dimensional extensions exhibit systematically larger admissible error regions. Experimental implementations demonstrate secure key generation up to $\approx 19\%$ for $d = 4$ and $\approx 25\%$ for $d = 8$. This enlargement reflects a genuine modification of the information disturbance trade-off rather than a trivial encoding advantage [9].

In entanglement-based implementations, high-dimensional states further exhibit more robust nonlocal correlations, violations of generalized Bell inequalities persist under stronger admixture of noise than in qubit systems. Entanglement is encoded across multiple levels of the Hilbert space (DoFs). Consequently, noise, such as depolarizing or other incoherent processes, is effectively distributed across these levels [51]. This statistical spreading reduces the impact of local noise effects on the global entangled state, enhancing robustness and decreasing resistance to errors compared to entanglement in low-dimensional systems. Such multi-level encoding thus provides intrinsic error mitigation by leveraging the larger structure of the state space.

The HD-QKD protocol with subspaces (discussed in Section IV-B) shows an additional improvement. The two measurements used in the protocol (selecting the subspace and measuring the quantum state) can be seen as so-called filters [6]. Some entangled states do not violate Bell inequalities and thus exhibit behavior consistent with classical correlations. In the protocol presented above, the first measurement collapses the state into a definite outcome, while the second measurement reveals correlations typical of entanglement [34]. By applying this concept on HD-QKD using subspace, it can be shown that the visibility increases [42]. Therefore, when generating a key across the full space, the entangled (correlated) components contribute positively, whereas the unentangled (uncorrelated) components introduce errors that must be corrected, effectively reducing the net key rate. By performing post-selection, one can remove these uncorrelated components beforehand, preventing them from offering any advantage to an eavesdropper [34].

D. Practical realizations

HD-QKD protocols are becoming increasingly practical, as demonstrated by current experiments involving high-dimensional quantum states of entangled photons. While these protocols and their realization are still in the early stages and challenging to implement, as discussed in Section I, the most difficult aspect of two-dimensional QKD remains noise. This makes the focus on the realization of HD-QKD particularly valuable. A key factor for any quantum state is the DoF of the photon. These DoF can be interpreted in various ways. In the following, we will explore different methods and experiments that utilize the DoF of a photon. No single approach is independent, different DoF can be combined, enabling the realization of higher-dimensional systems.

1) Twisted Photons: Twisted photons is one common investigated approach for HD-QKD. The concept is based on exploiting the orbital angular momentum DoF of individual photons. Twisted photon states carrying quantized angular momentum values $\ell\hbar$ are generated using a phase-only spatial light modulator, which creates a helical phase profile $\exp(i\ell\phi)$ onto weak coherent pulses attenuated to the single-photon level [28]. The different states are encoded in a discrete set of angular momentum modes $\{\ell = -L, \ldots, +L\}$, forming a d-dimensional Hilbert space with $d = 2L + 1$ [44]. In recent experiments high-dimensional entanglement with three photons was created [27].

2) Frequency-bin entanglement: High-dimensional qudits can also be encoded in the frequency DoF of single photons, exploiting discrete frequency bins as a basis for a d-level quantum system. In such schemes, a continuous laser beam hits a beta-barium borate crystal. This crystal produced spontaneous parametric down-conversion which cause the photon into discretized frequency modes separated by intervals, allowing the preparation of states of the form:

$$|\Psi\rangle = \sum_{j=0}^{d-1} \sum_{k=0}^{d-1} c_{jk} \, |j\rangle_i \, |k\rangle_s \, .$$

This qudit $|\Psi\rangle$ represents a two-qudit state in the discrete d^2-dimensional subspace spanned by the orthonormal product states $|j\rangle_i |k\rangle_s$ where i and s correspond to the so-called idler and signal photon of the construction. The states $|j\rangle$ and $|k\rangle$ represent the frequency intervals and c_{jk} a factor for the likelihood of the respective combination [38]. Experimental demonstrations have generated frequency-entangled qudits with dimension exceeding $d > 10$ and characterized their spectral correlations using time-of-arrival and correlated spectral intensity measurements, as well as distributed these states over tens of kilometers of fiber [19].

3) Time-bin entanglement: This approach is the least explored area in the realization of HD-QKD. One first approach was published in 2016 [7], nearly a decade later, a complete analysis of high-dimensional entanglement were published [20]. High-dimensional qudits can be encoded in the temporal DoF of single photons by exploiting discrete time bins as orthogonal basis states. In this approach, a photon is coherently delocalized over a sequence of well-defined temporal modes (time-bins), forming states of the form:

$$|\Psi\rangle = \sum_{p_A, p_B \in \{H,V\}} c_{p_A,p_B} \, |p_A, p_B\rangle \otimes \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} |kk\rangle \, .$$

The dimension d is encoded into the number of time-bins. p_A and p_B denotes to the polarization of two qudits which is horizontal or vertical and c_{p_A,p_B} is again a factor for the likelihood of the respective combination. An experiment demonstrating the realization of this approach was shown using the BBM92 protocol [50]. They employed an on-chip interferometric cascade, in which a sequence of integrated Mach-Zehnder interferometers coherently mixes the time-bin modes. With this concept it was possible to implement a $d = 8$ qudit.

V. Future Work

QKD offers promising alternatives to classical post-quantum cryptography. Compared to two-dimensional QKD, HD-QKD has advantages with respect to noise tolerance. This noise tolerance could be an important factor when deploying such a system in the maritime domain.

Future work should focus on large-scale field tests in realistic maritime scenarios to further evaluate the performance of HD-QKD under varying environmental conditions. In particular, long-distance ship-to-ship and ship-to-shore links require systematic investigation to assess stability, scalability, and integration into existing maritime communication infrastructures. Furthermore, a systematic comparison of different QKD protocols across various maritime infrastructure scenarios could be analyzed.

Applied QKD research usually focuses on the protocol level. However, security depends not only on physical principles but also on hardware and implementation details. In past the analysis of QKD hardware and implementations has revealed several vulnerabilities (cf. e.g. [31, 43, 26, 16]). Clearly, the whole system has to be designed and deployed with emphasis on security.

Quantum cryptography comprises more than QKD. In this article we focused on QKD, but further research should evaluate other quantum cryptography schemes with respect to their usefulness for maritime systems.

Acknowledgments

We would like to thank Marcus Huber for valuable discussions. His feedback and expertise greatly contributed to the development of this work.

References

[1] Helle Bechmann-Pasquinucci and Asher Peres. "Quantum cryptography with 3-state systems". In: *Physical Review Letters* 85.15 (2000), p. 3313.

[2] Charles H Bennett et al. "Experimental quantum cryptography". In: *Journal of cryptology* 5.1 (1992), pp. 3–28.

[3] Charles H. Bennett and Gilles Brassard. "Quantum cryptography: Public key distribution and coin tossing". In: *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*. 1984, pp. 175–179.

[4] Charles H. Bennett, Gilles Brassard, and N. David Mermin. "Quantum cryptography without Bell's theorem". In: *Physical Review Letters* 68 (5 Feb. 1992), pp. 557–559. DOI: 10.1103/PhysRevLett.68.557.

[5] Jean-Philippe Bourgoin et al. "Free-space quantum key distribution to a moving receiver". In: *Optics express* 23.26 (2015), pp. 33437–33447.

[6] Luc Bouten, Ramon Van Handel, and Matthew R James. "An introduction to quantum filtering". In: *SIAM Journal on Control and Optimization* 46.6 (2007), pp. 2199–2241.

[7] Thomas Brougham et al. "The information of high-dimensional time-bin encoded photons". In: *The European Physical Journal D* 70.10 (2016), p. 214.

[8] Nicolas J Cerf et al. "Security of quantum key distribution using d-level systems". In: *Physical review letters* 88.12 (2002), p. 127902.

[9] Daniele Cozzolino et al. "High-dimensional quantum communication: benefits, progress, and future challenges". In: *Advanced Quantum Technologies* 2.12 (2019), p. 1900038.

[10] Ministry of Defence. Press Information Bureau. *Quantum Communication between two DRDO Laboratories*. Dec. 9, 2020.

[11] Mirdit Doda et al. "Quantum key distribution overcoming extreme noise: Simultaneous subspace coding using high-dimensional entanglement". In: *Physical Review Applied* 15.3 (2021), p. 034003.

[12] Thomas Durt et al. "On mutually unbiased bases". In: *International journal of quantum information* 8.04 (2010), pp. 535–640.

[13] Arindam Dutta et al. "Analysis for Satellite-Based High-Dimensional Extended B92 and High-Dimensional BB84 Quantum Key Distribution". In: *Advanced Quantum Technologies* 7.11 (2024), p. 2400149.

[14] Vladimir I. Egorov. *Quantum communication in Russia: status and perspective*. Presentation at the ITU Workshop on Quantum Information Technology (QIT) for Networks, Shanghai, China, https://www.itu.int/en/ITU-T/Workshops-and-Seminars/2019060507/Documents/Vladimir%20_Egorov_Presentation.pdf. June 5, 2019.

[15] Patrick Eraerds. *Quantum key distribution and 1 Gbit/s data encryption over a single fibre*. arXiv:0912.1798 [quant-ph] 2009. 2009.

[16] Ferenczi, Grangier, and Grosshans. *Calibration Attack and Defence in Continuous Variable Quantum Key Distribution*. CLEO-IQEC, 2007.

[17] "Field experiment on a robust hierarchical metropolitan quantum cryptography network". In: *Chinese Science Bulletin* 54.17 (2009), pp. 2991–2997. URL: arXiv:0906.3576..

[18] Gui-Ying Jiang et al. "Performance of Ship-Based QKD Under the Influence of Sea-Surface Atmospheric Turbulence". In: *Photonics*. Vol. 12. 4. MDPI. 2025, p. 340.

[19] Rui-Bo Jin et al. "Generation and distribution of high-dimensional frequency-entangled qudits". In: *arXiv preprint arXiv:1603.07887* (2016).

[20] Florian Kanitschar et al. "Harnessing high-dimensional temporal entanglement using limited interferometric setups". In: *Physical Review Applied* 22.5 (2024), p. 054054.

[21] Andreas Klappenecker and Martin Rötteler. "Constructions of mutually unbiased bases". In: *International Conference on Finite Fields and Applications*. Springer. 2003, pp. 137–144.

[22] Will Knight. *Quantum cryptography network gets wireless link*. June 7, 2005.

[23] Dimitar R. Kolev and Morio Toyoshima. "Satellite-to-ground optical communications using small optical transponder (SOTA) – received-power fluctuations". In: *Opt. Express* 25 (2017), pp. 28319–28329.

[24] Jeffrey Lin, P.W. Singer, and John Costello. "China's Quantum Satellite Could Change Cryptography Forever". In: *Popular Science* (Mar. 3, 2016).

[25] Wenhao Lin. "A UAV-assisted secure maritime communication system with dynamic quantum relaying and satellite collaboration". In: *Procedia Computer Science* 266 (2025), pp. 1065–1072.

[26] Makarov and Hjelme. "Faked states attack on quantum cryptosystems". In: *Journal of Modern Optics* 52 (2005).

[27] Mehul Malik et al. "Multi-photon entanglement in high dimensions". In: *Nature Photonics* 10.4 (2016), pp. 248–252.

[28] Gabriel Molina-Terriza, Juan P Torres, and Lluis Torner. "Twisted photons". In: *Nature physics* 3.5 (2007), pp. 305–310.

[29] Michael A Nielsen and Isaac L Chuang. *Quantum information and quantum computation*. 2000.

[30] Amy Nordrum. "China Demonstrates Quantum Encryption By Hosting a Video Call". In: *IEEE* (Oct. 3, 2017).

[31] National Security Agency/Central Security Service Search NSA. Quantum Key Distribution (QKD) and Quantum Cryptography (QC). 2020.

[32] Indian Space Research Organisation. *ISRO makes breakthrough demonstration of free-space Quantum Key Distribution (QKD) over 300 m*. Mar. 22, 2021.

[33] Maria Papathanasaki et al. “Quantum Cryptography in Maritime Telecommunications”. In: *2021 IEEE International Conference on Cyber Security and Resilience (CSR)*. 2021, pp. 530–535. DOI: 10.1109/CSR51186.2021.9527973.

[34] Sandu Popescu. “Bell’s inequalities and density matrices: revealing “hidden” nonlocality”. In: *Physical Review Letters* 74.14 (1995), p. 2619.

[35] Port of Rotterdam Authority. *Consortium of parties first in the world to build scalable quantum internet connection in Rotterdam port*. Published 14 May 2024. Accessed 22 February 2026 at 15:45 MEZ. May 2024. URL: https://www.portofrotterdam.com/en/news-and-press-releases/consortium-parties-first-world-build-scalable-quantum-internet-connection.

[36] Quantum Logistics. *China’s National Quantum Lab Tests QKD on Maritime Logistics Channels in South China Sea*. Accessed: 2026-02-22 16:00 MEZ. Mar. 2017. URL: https://www.quantumlogistics.com/articles2017/12/03302017.

[37] Quantum Logistics. *Maersk and Toshiba Launch First Cross-Border Quantum Key Distribution for Maritime Logistics*. Published 31 January 2024. Accessed 22 February 2026 at 15:55 MEZ. Jan. 2024. URL: https://www.quantumlogistics.com/articles2024/4/01312024.

[38] Sacha Schwarz, Bänz Bessire, and André Stefanov. “Experimental violation of a d-dimensional Bell inequality using energy-time entangled photons”. In: *International Journal of Quantum Information* 12.07n08 (2015), p. 1560026.

[39] Peter W Shor and John Preskill. “Simple proof of security of the BB84 quantum key distribution protocol”. In: *Physical review letters* 85.2 (2000), p. 441.

[40] Peter W. Shor. “Algorithms for quantum computation: discrete logarithms and factoring”. In: *Foundations of Computer Science*. IEEE Computer Society, 1994, pp. 124–134. DOI: 10.1109/SFCS.1994.365700.

[41] Joseph D. Touch and Lori W. Gordon. “Quantum Key Distribution in Space”. In: *Game Changer. Centre for Space, Policy and Strategy* (July 2020). aerospace.org;

[42] Thomas Unglaub. “Quantum key distribution against extreme noise effect using high dimensional entanglement with MUB”. Masterarbeit, Fakultät für Physik. MA thesis. Wien, Österreich: Universität Wien, 2023. DOI: 10.25365/thesis.73404.

[43] Makarov Vakhitov and Hjelme. “Large pulse attack as a method of conventional optical eavesdropping in quantum cryptography”. In: *Journal of Modern Optics* 48 (2001).

[44] Alipasha Vaziri, Gregor Weihs, and Anton Zeilinger. “Experimental two-photon, three-dimensional entanglement for quantum communication”. In: *Physical review letters* 89.24 (2002), p. 240401.

[45] Mike Wall. “China Launches Pioneering ‘Hack-Proof’ Quantum-Communications Satellite”. In: *Space.com. Purch* (Aug. 16, 2016).

[46] Eric Wille. *Space-based QKD at ESA. Presentation at the ITU webinar Quantum information technology. Episode 2: Joint Symposium on Quantum Transport Technology*. Apr. 28, 2021.

[47] William K Wootters and Wojciech H Zurek. “A single quantum cannot be cloned”. In: *Nature* 299.5886 (1982), pp. 802–803.

[48] Lin Xing. *China launches world’s first quantum science satellite*. Physics World. Institute of Physics. Aug. 16, 2016.

[49] Juan Yin. “Satellite-based entanglement distribution over 1200 kilometres”. In: *Science* 356.6343 (2017), pp. 1140–4. DOI: 10.1126/science.aan3211.. URL: arXiv:1707.01339..

[50] Hao Yu et al. “Quantum key distribution implemented with d-level time-bin entangled photons”. In: *Nature Communications* 16.1 (2025), p. 171.

[51] Feng Zhu et al. “Are high-dimensional entangled states robust to noise?” In: *arXiv preprint arXiv:1908.08943* (2019).

[52] Feng Zhu et al. “Is high-dimensional photonic entanglement robust to noise?” In: *AVS Quantum Science* 3.1 (2021).