PT Jurnal Cendekia Indonesia
Journal of Information Systems and Business Technology
Homepage: https://journal.jci.co.id/jisbt
Vol. 1 No. 3 (2025) Page: 93-98
E-ISSN: 3109-8886

Jaringan Komputer Quantum dan Penerapan Quantum Key Distribution pada Keamanan Data Perbankan

[1]Fadhil Adiyatma Putra, [2]Ahmad Nur Syafri, [3]Bayu Isma Setiaji

[123]Sistem Informasi, Ilmu Komputer, Unvesitasitas Pamulang, Kota Tangerang Selatan, Indonesia

[1]fadhilputra68@email.com, [2]afri7573@email.com, [3]bayyuusetaiji057@gmail.com

Abstract

The development of quantum computing has a significant impact on cybersecurity, particularly in the banking sector, which relies heavily on data confidentiality and integrity. Classical cryptographic algorithms are at risk of becoming vulnerable due to the ability of quantum computers to break encryption systems using algorithms such as Shor's, raising the need for new security technologies based on quantum mechanical principles. This study analyzes the concept of quantum computer networks, identifies implementation challenges, and examines case studies of Quantum Key Distribution (QKD) applications in banking data security systems. The research method used is a descriptive approach through literature analysis and case studies of QKD applications in global financial networks. The results show that QKD can improve the security of encryption key exchanges through an eavesdropping detection mechanism that relies on changes in the state of photons, thus enabling communications that are theoretically impossible to intercept without detection. Case studies of the SwissQuantum Network and financial networks in China demonstrate that the implementation of QKD has successfully improved the security of data communications between bank branches and data centers. However, this study also identified several key challenges, such as high infrastructure costs, limited transmission distances, and the complexity of integration with existing cryptographic systems and conventional networks. Furthermore, human resource readiness, regulatory support, and long-term investment are key factors in the successful implementation of this technology. This study concludes that QKD is a promising security solution for the banking sector in facing future quantum computing threats, although its adoption requires strategic planning, technological readiness, and comprehensive policies.

Keywords*: Quantum Computing, Cybersecurity, Quantum Key Distribution (QKD), Banking Data Security, Quantum Networks*

Abstrak

Perkembangan komputasi kuantum memberikan dampak besar terhadap keamanan siber, khususnya di sektor perbankan yang sangat bergantung pada kerahasiaan dan integritas data. Algoritma kriptografi klasik berisiko menjadi rentan akibat kemampuan komputer kuantum dalam memecahkan sistem enkripsi dengan algoritma seperti Shor, yang memunculkan kebutuhan akan teknologi keamanan baru yang berbasis prinsip mekanika kuantum. Penelitian ini menganalisis konsep jaringan komputer kuantum, mengidentifikasi tantangan implementasinya, serta mengkaji studi kasus penerapan Quantum Key Distribution (QKD) dalam sistem keamanan data perbankan. Metode penelitian yang digunakan adalah pendekatan deskriptif melalui analisis literatur dan studi kasus penerapan QKD pada jaringan keuangan global. Hasil penelitian menunjukkan bahwa QKD dapat meningkatkan keamanan pertukaran kunci enkripsi melalui mekanisme deteksi penyadapan yang mengandalkan perubahan keadaan foton, sehingga memungkinkan komunikasi yang secara teoritis tidak bisa disadap tanpa terdeteksi. Studi kasus SwissQuantum Network dan jaringan finansial di Tiongkok menunjukkan bahwa penerapan QKD berhasil meningkatkan keamanan komunikasi data antar cabang bank dan pusat data. Namun, penelitian ini juga menemukan sejumlah tantangan utama, seperti tingginya biaya infrastruktur, keterbatasan jarak transmisi, serta kompleksitas integrasi dengan sistem kriptografi dan jaringan konvensional yang sudah ada. Selain itu, kesiapan sumber daya manusia, dukungan regulasi, dan investasi jangka panjang menjadi faktor kunci dalam keberhasilan penerapan teknologi ini. Penelitian ini menyimpulkan bahwa QKD merupakan solusi keamanan yang menjanjikan bagi sektor perbankan dalam menghadapi ancaman komputasi kuantum di masa depan, meskipun adopsinya memerlukan perencanaan strategis, kesiapan teknologi, dan kebijakan yang komprehensif..

Kata Kunci: Jaringan Kuantum, Cloud Computing, Perbankan, Keamanan Data, Quantum Key Distribution (QKD)

A. PENDAHULUAN

Diterima Redaksi: 01-10-2025 | Selesai Revisi: 14-10-2025 | Diterbitkan Online: 31-10-2025

Perkembangan teknologi kuantum menghadirkan tantangan sekaligus peluang besar dalam dunia keamanan informasi, terutama karena semakin tingginya ketergantungan berbagai sektor terhadap sistem digital. Sektor perbankan merupakan salah satu bidang yang paling rentan terhadap ancaman komputasi kuantum, mengingat aktivitas operasionalnya sangat bergantung pada perlindungan data sensitif, seperti informasi nasabah, transaksi keuangan, dan komunikasi antar sistem internal. Algoritma kriptografi klasik seperti RSA dan Elliptic Curve Cryptography (ECC) selama ini dianggap aman karena membutuhkan sumber daya dan waktu komputasi yang sangat besar agar dapat dipecahkan oleh komputer konvensional. Namun, dengan munculnya komputer kuantum yang dapat melakukan faktorisasi bilangan prima dan pemecahan logaritma diskrit secara efisien melalui algoritma seperti Shor, sistem keamanan kriptografi tersebut berpotensi menjadi rentan dan tidak lagi relevan di masa depan.

Sebagai respons terhadap ancaman ini, konsep jaringan komputer kuantum mulai berkembang sebagai pendekatan baru untuk menjaga keamanan komunikasi data. Jaringan ini memanfaatkan qubit sebagai unit dasar informasi, yang memiliki sifat superposisi dan entanglement, memungkinkan pengolahan dan pengiriman informasi dengan tingkat keamanan yang jauh lebih tinggi dibandingkan sistem klasik. Prinsip mekanika kuantum ini memungkinkan deteksi dini terhadap upaya penyadapan, karena setiap intervensi dari pihak ketiga akan mengubah keadaan kuantum yang dapat terdeteksi oleh sistem. Oleh karena itu, jaringan komputer kuantum menawarkan paradigma baru dalam sistem komunikasi yang tidak hanya bergantung pada kompleksitas matematis, tetapi juga pada hukum fisika sebagai dasar keamanannya.

Salah satu teknologi kunci dalam jaringan komunikasi kuantum adalah Quantum Key Distribution (QKD), yang dirancang untuk mendistribusikan kunci enkripsi secara aman menggunakan foton tunggal sebagai pembawa informasi. QKD memungkinkan dua pihak yang berkomunikasi untuk menghasilkan dan berbagi kunci rahasia dengan jaminan keamanan teoritis, karena foton yang digunakan tidak dapat disalin tanpa mengubah keadaannya. Mekanisme ini menjadikan QKD sangat relevan untuk sektor perbankan yang memerlukan tingkat keamanan tinggi dalam pertukaran data, khususnya dalam komunikasi antar cabang, pusat data, dan sistem transaksi besar.

Berbagai penelitian dan implementasi awal menunjukkan bahwa QKD memiliki potensi besar dalam meningkatkan keamanan komunikasi di sektor keuangan. SwissQuantum Network adalah salah satu contoh implementasi nyata yang berhasil mengintegrasikan QKD dalam komunikasi antar lembaga keuangan dan pusat data perbankan. Selain itu, Tiongkok telah mengembangkan jaringan komunikasi kuantum berskala nasional yang mencakup sektor pemerintahan, militer, dan perbankan, serta menghubungkan berbagai kota melalui infrastruktur serat optik dan satelit kuantum. Meski demikian, adopsi teknologi QKD masih menghadapi sejumlah tantangan teknis dan nonteknis, seperti keterbatasan jarak transmisi, degradasi sinyal akibat kualitas serat optik, kompleksitas integrasi dengan sistem kriptografi konvensional, serta tingginya biaya pengadaan dan pemeliharaan infrastruktur.

Hingga kini, penelitian yang secara khusus membahas potensi dan tantangan implementasi QKD dalam sistem keamanan perbankan di negara berkembang masih relatif terbatas. Hal ini menunjukkan adanya kesenjangan penelitian yang perlu diteliti lebih lanjut, terutama dalam konteks kesiapan infrastruktur, sumber daya manusia, dan regulasi yang mendukung adopsi teknologi kuantum. Oleh karena itu, penelitian ini bertujuan untuk memberikan analisis komprehensif mengenai konsep jaringan komputer kuantum, mengidentifikasi tantangan utama dalam implementasi QKD, serta mengkaji studi kasus penerapannya pada sistem keamanan perbankan modern sebagai langkah untuk menghadapi ancaman komputasi kuantum di masa depan.

B. PELAKSAAAN DAN METODE

Penelitian ini mengadopsi pendekatan deskriptif kualitatif yang berfokus pada analisis literatur dan studi kasus implementasi Quantum Key Distribution (QKD) di sektor perbankan internasional. Data penelitian dikumpulkan dari berbagai sumber sekunder yang terpercaya, termasuk jurnal ilmiah internasional terkemuka, laporan teknis implementasi jaringan kuantum, publikasi lembaga penelitian, serta dokumentasi resmi dari institusi keuangan dan penyedia teknologi kuantum. Pemilihan sumber dilakukan secara selektif untuk memastikan bahwa informasi yang digunakan relevan, valid, dan terkini. Pendekatan ini dipilih karena memungkinkan peneliti untuk mendapatkan pemahaman yang komprehensif mengenai perkembangan teknologi QKD tanpa perlu melakukan eksperimen langsung yang membutuhkan infrastruktur khusus dan biaya tinggi.

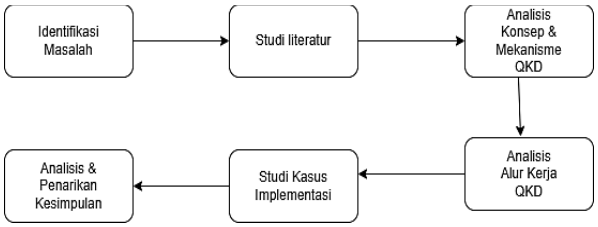
Analisis data dilakukan dengan mempelajari secara sistematis prinsip dasar jaringan komputer kuantum, mekanisme kerja QKD, serta model penerapannya dalam industri keuangan. Proses analisis mencakup identifikasi karakteristik teknis jaringan kuantum, pemahaman terhadap protokol QKD yang umum digunakan, serta evaluasi aspek keamanan yang dihasilkan dibandingkan dengan metode kriptografi klasik. Selain itu, penelitian ini juga membahas hubungan antara teknologi QKD dan kebutuhan keamanan dalam perbankan, khususnya terkait perlindungan komunikasi data antar cabang, pusat data, dan sistem transaksi bernilai tinggi.

Alur kerja QKD ditelaah secara konseptual melalui beberapa tahap utama, yaitu pembangkitan qubit, transmisi foton melalui media serat optik atau kanal bebas, pengukuran oleh penerima, tahap verifikasi dan koreksi kesalahan, serta deteksi penyadapan. Analisis difokuskan pada bagaimana perubahan polaritas, fase, atau intensitas

foton selama transmisi dapat menjadi indikator adanya intervensi pihak ketiga. Dengan pendekatan ini, penelitian berusaha menjelaskan hubungan antara prinsip mekanika kuantum dan tingkat keamanan yang dapat dicapai melalui QKD, baik secara teoritis maupun praktis.

Selain itu, penelitian ini juga menganalisis integrasi QKD ke dalam infrastruktur perbankan konvensional melalui kajian studi kasus yang ada. Analisis ini mencakup aspek teknis seperti kompatibilitas dengan jaringan serat optik yang sudah ada, kebutuhan perangkat keras tambahan, serta interoperabilitas dengan sistem kriptografi klasik yang masih digunakan. Faktor non-teknis, seperti kesiapan sumber daya manusia, dukungan kebijakan internal organisasi, dan pertimbangan biaya implementasi, juga dievaluasi untuk memberikan gambaran yang lebih menyeluruh.

Studi kasus yang dianalisis dalam penelitian ini mencakup SwissQuantum Network, jaringan komunikasi kuantum di Tiongkok, serta implementasi QKD oleh SK Telecom dalam mendukung keamanan komunikasi sektor keuangan. Setiap studi kasus dianalisis berdasarkan manfaat keamanan yang diperoleh, ruang lingkup penerapan, serta kendala teknis dan operasional yang muncul selama proses implementasi. Hasil analisis dari masing-masing studi kasus kemudian dibandingkan untuk mengidentifikasi pola umum, keunggulan, dan keterbatasan penerapan QKD dalam perbankan modern.



Gambar 1 Ilustrasi Alur Metode

C. HASIL DAN PEMBAHASAN

Peningkatan Keamanan

Hasil analisis menunjukkan bahwa QKD bisa memberikan perlindungan dalam proses pertukaran kunci enkripsi yang sangat kuat karena berdasarkan prinsip dasar mekanika kuantum. Setiap tindakan penyadapan akan menyebabkan perubahan pada keadaan foton, dan perubahan ini bisa dideteksi secara langsung. Dalam kasus studi SwissQuantum Network, QKD digunakan untuk melindungi komunikasi antar pusat data bank dengan tingkat deteksi penyadapan yang tinggi. Implementasi ini membuktikan bahwa QKD mampu memberikan tingkat keamanan yang tidak bisa dicapai oleh enkripsi biasa.
Selain meningkatkan keamanan dalam proses pertukaran kunci, penggunaan QKD juga meningkatkan rasa percaya terhadap sistem komunikasi perbankan.

Mekanisme deteksi penyadapan yang ada dalam QKD memastikan bahwa kunci enkripsi hanya digunakan ketika saluran komunikasi dalam kondisi aman. Hal ini menjadi kelebihan utama dibandingkan sistem enkripsi klasik yang tidak bisa mendeteksi adanya intervensi secara langsung. Keamanan yang ditawarkan oleh QKD menjadikannya sangat relevan untuk melindungi data perbankan yang sangat penting.

Informasi nasabah dan transaksi keuangan membutuhkan perlindungan tinggi karena memiliki nilai ekonomi besar. Dengan demikian, QKD berpotensi menjadi solusi keamanan yang efektif dalam menghadapi ancaman dari komputasi kuantum di masa depan. Selain masalah teknis keamanan, penggunaan QKD juga memberikan manfaat strategis bagi industri perbankan dalam mempertahankan reputasi serta kepercayaan nasabah.

Keamanan dalam komunikasi yang dijamin secara fisik melalui hukum mekanika kuantum mampu mengurangi kemungkinan bocornya data sensitif yang bisa merugikan lembaga keuangan. Dengan semakin tingginya kesadaran masyarakat tentang isu keamanan siber, adanya teknologi seperti QKD bisa menjadi cara untuk menunjukkan komitmen bank terhadap perlindungan data dan privasi nasabah.

Tantangan Implementasi QKD Di Lingkungan Perbankan

Meskipun memberikan tingkat keamanan yang tinggi, penerapan Quantum Key Distribution (QKD) masih dihadapkan dengan beberapa hambatan. Teknologi ini membutuhkan serat optik berkualitas tinggi, perangkat yang mampu mendeteksi foton tunggal, serta infrastruktur yang sulit dipelihara. Selain itu, jarak transmisi menjadi masalah besar karena kemampuan foton untuk tetap stabil berkurang setelah mencapai jarak tertentu. Beberapa bank yang sudah menerapkan QKD juga menyatakan bahwa mengintegrasikan teknologi ini dengan sistem keamanan yang sudah ada memerlukan perubahan besar dan investasi yang tinggi.

Tantangan teknis ini menunjukkan bahwa penerapan QKD tidak bisa dilakukan secara langsung di semua sistem perbankan. Kesiapan infrastruktur dan kemampuan teknis menjadi faktor penting yang harus dipertimbangkan sebelum penerapan dilakukan. Tanpa dukungan infrastruktur yang cukup, manfaat keamanan yang ditawarkan oleh QKD tidak bisa dimaksimalkan.

Selain aspek teknis, tantangan dalam penerapan QKD juga terkait dengan kesiapan sumber daya manusia dan regulasi. Operasional dan pemeliharaan sistem QKD membutuhkan tenaga ahli yang paham tentang teknologi kuantum. Oleh karena itu, penerapan QKD di lingkungan perbankan membutuhkan perencanaan yang matang, mencakup aspek teknologi, sumber daya manusia, serta kebijakan yang mendukung. Selain itu, tantangan dalam menerapkan QKD juga melibatkan aspek skala dan kelanjutan sistem.

Memasang QKD secara luas membutuhkan persiapan jangka panjang agar teknologi ini bisa berkembang seiring

dengan perluasan jaringan perbankan. Jika tidak ada strategi pengembangan yang jelas, sistem QKD bisa terbatas hanya pada lingkungan tertentu. Karena itu, dibutuhkan pendekatan bertahap agar implementasi QKD bisa disesuaikan dengan kemajuan teknologi serta kebutuhan operasional bank.

Keterbatasan Penelitian dan Arah Penelitian Selanjutnya

Penelitian ini memiliki beberapa keterbatasan yang perlu diketahui. Keterbatasan utamanya adalah pendekatan penelitian yang bersifat deskriptif kualitatif dengan memanfaatkan studi literatur dan studi kasus. Penelitian ini belum melakukan uji coba atau simulasi langsung terhadap implementasi QKD di sistem perbankan tertentu, sehingga hasil yang didapatkan masih bersifat konseptual.

Selain itu, kajian yang dilakukan terbatas pada contoh implementasi QKD di beberapa negara yang sudah memiliki infrastruktur komunikasi kuantum yang berkembang. Kondisi ini menyebabkan hasil penelitian belum benar-benar menggambarkan kesiapan sektor perbankan di negara berkembang. Faktor regulasi, kesiapan sumber daya manusia, dan kondisi infrastruktur lokal belum dibahas secara mendalam.

Berdasarkan keterbatasan tersebut, penelitian selanjutnya disarankan untuk mengkaji penerapan QKD secara lebih empiris melalui simulasi atau uji coba di lingkungan perbankan tertentu. Penelitian lanjutan juga dapat memperluas fokus pada aspek kebijakan, regulasi, serta analisis kesiapan penerapan teknologi kuantum di sektor perbankan nasional.

Meskipun ada keterbatasan, penelitian ini diharapkan bisa menjadi dasar awal untuk pengembangan penelitian lebih lanjut terkait keamanan komunikasi perbankan menggunakan teknologi kuantum. Meski masih bersifat konseptual, hasil penelitian ini memberikan gambaran awal tentang potensi dan tantangan QKD dalam situasi nyata. Dengan dukungan penelitian yang lebih dalam, teknologi QKD diharapkan bisa dikaji lebih rinci dan sesuai dengan kebutuhan sektor perbankan di masa depan.

D. PENUTUP

Kesimpulan

Penelitian ini bertujuan untuk menganalisis penerapan Quantum Key Distribution (QKD) sebagai solusi untuk meningkatkan keamanan komunikasi di sektor perbankan internasional. Berdasarkan hasil analisis literatur dan studi kasus yang telah dijelaskan sebelumnya, dapat disimpulkan bahwa QKD menawarkan pendekatan keamanan yang sangat kuat dengan memanfaatkan prinsip dasar mekanika kuantum. Salah satu karakteristik utama QKD adalah kemampuannya untuk mendeteksi upaya penyadapan melalui perubahan kondisi foton, yang membedakannya secara mendasar dari metode kriptografi konvensional yang mengandalkan kompleksitas matematis.

Hasil pembahasan menunjukkan bahwa penerapan QKD secara signifikan meningkatkan keamanan pertukaran kunci enkripsi, terutama dalam komunikasi antar pusat data perbankan. Studi kasus SwissQuantum Network menunjukkan bahwa QKD dapat diimplementasikan secara praktis dalam lingkungan operasional perbankan dengan tingkat keandalan yang tinggi, membuktikan bahwa QKD bukan sekadar konsep teoritis, tetapi teknologi yang layak digunakan untuk melindungi data finansial yang sangat sensitif.

Namun, penelitian ini juga mengidentifikasi berbagai tantangan teknis dan operasional dalam implementasi QKD. Kebutuhan akan infrastruktur serat optik berkualitas tinggi, perangkat deteksi foton tunggal, serta sistem pendukung yang kompleks menyebabkan biaya implementasi dan pemeliharaan menjadi relatif tinggi. Selain itu, keterbatasan jarak transmisi dan kecepatan distribusi kunci dapat mempengaruhi kinerja sistem, terutama di lingkungan perbankan yang memiliki volume transaksi besar dan kebutuhan komunikasi real-time.

Dari sisi kesiapan organisasi, penerapan QKD memerlukan sumber daya manusia yang memiliki keahlian khusus dalam bidang teknologi kuantum dan keamanan jaringan. Integrasi QKD dengan sistem keamanan yang ada juga memerlukan perencanaan yang matang agar tidak mengganggu operasional perbankan. Oleh karena itu, tidak semua institusi perbankan memiliki kesiapan yang sama untuk mengadopsi teknologi ini.

Dibandingkan dengan metode keamanan konvensional, QKD memiliki keunggulan utama dalam ketahanannya terhadap ancaman dari komputasi kuantum di masa depan. Meskipun demikian, kriptografi konvensional masih unggul dalam hal fleksibilitas, kemudahan implementasi, dan efisiensi biaya. Berdasarkan hal tersebut, penelitian ini menyimpulkan bahwa QKD lebih cocok digunakan sebagai teknologi pelengkap, bukan pengganti sistem keamanan perbankan yang sudah ada.

Pendekatan hibrida yang menggabungkan QKD dengan algoritma kriptografi konvensional dianggap sebagai solusi yang paling realistis, karena dapat memberikan keseimbangan antara tingkat keamanan yang tinggi dan efisiensi operasional. Dengan pendekatan ini, bank dapat melindungi komunikasi penting menggunakan QKD, sambil tetap mempertahankan sistem konvensional untuk kebutuhan operasional lainnya.

Saran

Berdasarkan hasil penelitian dan kesimpulan yang telah diperoleh, terdapat beberapa saran yang dapat dipertimbangkan. Institusi perbankan disarankan untuk mulai mengkaji penerapan Quantum Key Distribution secara bertahap, khususnya pada jalur komunikasi yang memiliki tingkat sensitivitas tinggi, seperti komunikasi antar pusat data dan sistem transaksi bernilai besar.

Pendekatan ini memungkinkan peningkatan keamanan tanpa harus melakukan perubahan menyeluruh terhadap infrastruktur yang telah ada.

Selain itu, pihak perbankan perlu mempersiapkan sumber daya manusia yang kompeten di bidang teknologi kuantum dan keamanan jaringan melalui pelatihan dan kerja sama dengan lembaga riset atau penyedia teknologi. Dukungan kebijakan internal serta perencanaan investasi jangka panjang juga menjadi faktor penting untuk memastikan keberhasilan implementasi QKD secara berkelanjutan.

Untuk penelitian selanjutnya, disarankan dilakukan kajian yang lebih mendalam mengenai efisiensi biaya, performa sistem, serta pengembangan model integrasi QKD dengan sistem kriptografi konvensional dalam skala operasional yang lebih luas. Penelitian lanjutan juga dapat mengkaji aspek regulasi dan standar keamanan yang diperlukan untuk mendukung adopsi teknologi QKD di sektor perbankan.

Ucapan Terima Kasih
Penulis ingin menyampaikan rasa terima kasih kepada dosen pembimbing mata kuliah Jaringan Komputer yang telah memberikan bimbingan, arahan, dan masukan yang berguna selama proses penyusunan jurnal ini. Arahan dari dosen tersebut sangat membantu penulis dalam memahami konsep jaringan komputer kuantum serta penerapan Quantum Key Distribution (QKD) dalam konteks keamanan data di bidang perbankan.

Ucapan terima kasih juga disampaikan kepada Universitas Pamulang yang telah memberikan lingkungan belajar yang mendukung serta fasilitas yang memudahkan penulis dalam mengakses berbagai sumber literatur ilmiah yang relevan.

Bantuan dari institusi ini sangat membantu dalam proses penelitian dan penyusunan jurnal ini.

Selain itu, penulis menghargai kontribusi para peneliti dan penulis sebelumnya yang karyanya dijadikan rujukan utama dalam penelitian ini. Literatur yang digunakan memberikan dasar teoritis dan bukti empiris yang kuat dalam menganalisis konsep, tantangan, serta studi kasus penerapan QKD di bidang perbankan.

Akhir kata, penulis juga mengucapkan terima kasih kepada semua pihak yang secara langsung atau tidak langsung memberikan dukungan dan semangat selama proses penyusunan jurnal ini. Semoga penelitian ini dapat memberikan manfaat dan menjadi referensi awal bagi pengembangan kajian mengenai keamanan data di era komputasi kuantum.

E. DAFTAR PUSTAKA

[1] M. Takeoka, S. Guha, and M. Wilde, “Fundamental rate-loss tradeoff for optical quantum key distribution,” Nature Communications, 2014. doi:10.1038/ncomms6235
[2] V. Scarani et al., “The security of practical quantum key distribution,” Rev. Mod. Phys., 2009. doi:10.1103/RevModPhys.81.1301
[3] N. Gisin and R. Thew, “Quantum communication,” Nature Photonics, 2007. doi:10.1038/nphoton.2007.22
[4] H.-K. Lo, M. Curty, and K. Tamaki, “Secure quantum key distribution,” Nature Photonics, 2014. doi:10.1038/nphoton.2014.149
[5] S. Pirandola et al., “Advances in quantum cryptography,” Advances in Optics and Photonics, 2020. doi:10.1364/AOP.361502
[6] S. Aaronson, “The limits of quantum computers,” Scientific American, 2008. doi:10.1038/scientificamerican0508-62
[7] M. Razavi, “An introduction to quantum communications,” IEEE Communications Surveys & Tutorials, 2018. doi:10.1109/COMST.2018.2817460
[8] F. Xu et al., “Secure quantum key distribution with realistic devices,” Rev. Mod. Phys., 2020. doi:10.1103/RevModPhys.92.025002
[9] C. Elliott, “The DARPA quantum network,” Quantum Communications and Cryptography, 2006. doi:10.1007/0-387-23455-7_13
[10] A. Muller et al., “Quantum cryptography over 23 km of installed telecom fibre,” Europhysics Letters, 1997. doi:10.1209/epl/i1997-00336-0
[11] Y. Liu et al., “Experimental quantum key distribution over 404 km fiber,” Physical Review Letters, 2021. doi:10.1103/PhysRevLett.126.250502
[12] B. Fröhlich et al., “A quantum key distribution system for secure data transmission,” Nature, 2013. doi:10.1038/nature12493
[13] C. Panayi et al., “Memory-assisted quantum key distribution,” New Journal of Physics, 2019. doi:10.1088/1367-2630/ab5c12
[14] R. Bedington, J. Arrazola, and A. Ling, “Progress in satellite quantum key distribution,” npj Quantum Information, 2017. doi:10.1038/s41534-017-0014-4
[15] S. Wang et al., “Field test of quantum communication in bank networks,” Optica, 2022. doi:10.1364/OPTICA.454727
[16] H. Zbinden et al., “SwissQuantum: A quantum network,” IEEE Journal of Selected Topics in Quantum Electronics, 2011. doi:10.1109/JSTQE.2011.2108131
[17] J. Yin et al., “Satellite-to-ground entanglement distribution,” Science, 2017. doi:10.1126/science.aan3211
[18] M. Sasaki et al., “Field test of quantum key distribution in Tokyo,” Optics Express, 2011. doi:10.1364/OE.19.010387
[19] X. Zhang et al., “Intercity quantum communication network in China,” Nature Photonics, 2022. doi:10.1038/s41566-022-00979-y

[20] A. Brouwer et al., "Quantum security in financial communication," Journal of Financial Technology, 2022. doi:10.2139/ssrn.4032911
[21] D. Kasture et al., "Impact of quantum computing on cryptography," IEEE Access, 2020. doi:10.1109/ACCESS.2020.2968410
[22] R. Singh and S. Yadav, "Quantum-safe cryptography," Journal of Information Security and Applications, 2021. doi:10.1016/j.jisa.2021.103139
[23] Y. Chen et al., "A review of QKD networks," Entropy, 2020. doi:10.3390/e22040435
[24] L. Zhang et al., "Practical challenges in QKD deployment," Optics Communications, 2023. doi:10.1016/j.optcom.2023.129027
[25] P. W. Shor, "Algorithms for quantum computation," Proceedings of FOCS, 1994. doi:10.1109/SFCS.1994.365700