Comparing CV-QKD with Other Security Protocols: An In-Depth Exploration of Privacy, Speed, and Cost

R.J.Kavitha[1], D.Ilakkiaselvan[1]

1. Department of Electronics and Communication Engineering, University College of Engineering Panruti.

Abstract:

This literature study investigates the security, speed, and cost of Continuous Variable Quantum Key Distribution, which (CV-QKD) with multiple unique security methods. Quantum key distribution has emerged as a promising technology for securing communications in an era where information security is of paramount importance. CV-QKD, a type of quantum key distribution, gets a lot of attention due to the way it can lets safe key exchange in long distances using continuous-variable quantum states.. The review begins by elucidating the fundamental principles of CV-QKD and delves into its theoretical underpinnings, highlighting its security advantages, such as the resistance to quantum attacks. Furthermore, the review examines the practical implementation of CV-QKD and explores its speed and efficiency in real-world scenarios. Comparative analysis is a key focus of this review, as it juxtaposes CV-QKD with other security protocols like discrete-variable QKD, classical cryptographic methods, and post-quantum cryptography. The examination encompasses the security guarantees, transmission speeds, and cost-effectiveness of these protocols, providing insights into the strengths and weaknesses of each approach. In the end, this review of the literature is a helpful tool for those who are seeking an in-depth knowledge of CV-QKD's position within the landscape of secure communication protocols, providing a nuanced take on its efficacy in the areas of security, speed, and cost-effectiveness when compared to its peers.

Key Words: CV-QKD (Continuous Variable Quantum Key Distribution**), DPSQKD** (Differential-Phase-Shifted Quantum Key Distribution)**, MIMO** (Multiple Input Multiple Out Put), **5G Communication**

Introduction

CV-QKD encryption represents a cutting-edge paradigm shift in the realm of secure communications. It differs fundamentally from classical encryption methods in several key aspects, harnessing the principles of quantum mechanics to achieve an unprecedented level of security. This brief introduction explores the fundamental differences between CV-QKD encryption and classical encryption, shedding light on why quantum encryption holds immense promise for the future of secure communication.

Classical Encryption

Classical encryption relies on mathematical algorithms to scramble plaintext data into cipher text. The integrity of classical encryption is dependent on the complexity of overcoming equations, such as factoring big numbers (RSA encryption) or filling discrete logarithm computations (Diffie-Hellman key exchange). Along with some commonly used protocols and algorithms

Symmetric Encryption:
Key-Based Encryption: Symmetric encryption makes use of the same key for both encryption and decryption. This key is only available to the sender and the receiver. Protocols: Common protocols include the Data Encryption Standard (DES), Triple DES (3DES), and Advanced Encryption Standard (AES). To encrypt data, these protocols utilize block cipher algorithms such as DES, 3DES, and AES. AES is one of the most used symmetric encryption techniques. It encrypts and decrypts data using keys of multiple bits (128-bit, 192-bit, or 256-bit).

Asymmetric Encryption (Public-Key Encryption):
Asymmetric encryption combines two keys for encryption and decryption: an external key for encrypting and a secret key for decryption. The public key may be used by anybody for encryption of data, while just the user of the secret key can decode it. RSA (Rivest-Shamir-Adleman), Diffie-Hellman, and Elliptic Curve Cryptography (ECC) are common asymmetric encryption algorithms. The RSA algorithm is a well-known asymmetric encryption method. It is dependent on the problem of factoring big semi prime integers to preserve security. Diffie-Hellman is commonly used for secure key exchange; however ECC provides adequate security with shorter key lengths.
Hash Functions: Data Integrity: Hash algorithms develop a fixed-size hash value from fed data. They are used to ensure the integrity of data and that it has not been tampered with during transmission. Protocols: SHA-256 (part of the SHA-2 family) and MD5 (less secure and no longer recommended) hash algorithms are frequently used in many protocols. The Secure Hash Algorithm 2 (SHA-2) family's SHA-256 algorithm produces a 256-bit hash code and is widely employed for data integrity checks.

Message Authentication Codes (MACs):
Data Authentication: MACs are used to confirm a message's authenticity and integrity by producing an identification tag that is attached to the message. Protocols: HMAC (Hash Based Message Authentication Code) is a general protocol that creates a MAC by combining a cryptographic hash function with a secret key. HMAC generally generates the authentication code using hash algorithms such as a SHA- and a secret key.
Digital Signatures:
Authentication and Integrity: Asymmetric cryptography is used in digital signatures to offer authentication and ensure the integrity of messages or documents. Protocols: RSA Digital Signatures, ECDSA (Elliptic Curve Digital Signature Algorithm), and DSA (Digital Signature Algorithm) are three popular digital signature technologies.
Popular methods for producing digital signatures include RSA and ECDSA. These traditional encryption methods are critical in safeguarding data and communications in a wide range of applications, from secure texting to e-commerce transactions. They are, however, vulnerable to quantum computer attacks, necessitating the development of quantum-resistant encryption methods such as lattice-based cryptography and code-based cryptography to meet future security demands.
CV-QKD Encryption: CV-QKD, on the other hand, uses quantum physics concepts, notably the features of quantum states of light (often continuous-variable states), to safely transfer cryptographic keys. It is based on physical rules rather than mathematical assumptions, providing security against quantum assaults that conventional encryption cannot.
Principles of CV-QKD:
Quantum Mechanics: CV-QKD is based on quantum mechanics concepts, namely the utilization of continuous-variable quantum states such as light quadrature amplitudes. CV-QKD enables two parties, Alice and Bob, to produce a shared cryptographic key over a quantum channel while detecting any eavesdropping efforts by an intruder, Eve. CV-QKD protocols include: Protocols for Gaussian Modulation: There are several CV-QKD techniques, the most prevalent of which is based on Gaussian modulation. Gaussian Modulation Continuous Variable QKD (GM-CVQKD) and Coherent-State CVQKD are two examples. Reverse-Reconciliation and Forward-Reconciliation: CV-QKD protocols can use a variety of error-correction and privacy-amplification techniques, including reverse-reconciliation and forward-reconciliation techniques. Techniques and Algorithms:
Homodyne or Heterodyne Detection: The quadrature amplitudes of quantum states are measured using homodyne or heterodyne detection techniques in CV-QKD. Error Correction and Privacy Amplification: Algorithms and approaches are used to rectify faults in the shared key while also increasing its security through privacy amplification. Squeezed States: Squeezed states of light can improve the security performance of CV-QKD methods.
Key Renewal:
Classical Encryption: Classical keys have a finite lifespan and must be periodically renewed, often over insecure channels. CV-QKD Encryption: CV-QKD keys can be renewed continuously during communication without interrupting the data flow, enhancing long-term security.
Challenges and Limitations: Multiple Input Multiple Output (MIMO) in 5G communication with Continuously Variable Quantum Key Distribution (CV-QKD) to has several challenges and limitations because this integration involves complex technologies and practical considerations. Below are some of the key challenges and limitations:
Transmission Distance: CV-QKD systems are generally limited in terms of transmission distance due to quantum signal degradation. This limitation can be problematic in MIMO systems that may span large geographical areas.
Quantum Signal Losses: Quantum signals are susceptible to losses as they travel through optical fibers or free-space channels. These losses can impact the rate and reliability of key distribution. Compatibility with Existing Infrastructure: Integrating CV-QKD into existing MIMO and beyond 5G communication systems can be challenging. Ensuring seamless compatibility and interoperability with classical components is a complex task.
Synchronization: Achieving precise synchronization between quantum and classical systems is crucial for successful integration but can be technically demanding. Scalability Issues: As the number of users or devices in a MIMO system increases, scaling CV-QKD key distribution can become challenging. This is particularly relevant for large-scale communication networks. Environmental Interference: Environmental factors, such as atmospheric conditions and temperature fluctuations, can affect the performance of quantum channels and, consequently, the reliability of CV-QKD. High Cost: Quantum technologies are currently costly to develop and implement. The initial investment in quantum hardware and infrastructure can be a significant barrier for widespread adoption. Quantum Resources: The availability of quantum resources, such as high-quality quantum sources and detectors, may restrict CV-QKD's practical application in MIMO systems. Key Rate vs. Data Rate: CV-QKD typically has a lower key generation rate compared to classical encryption methods. This trade-off between key rate and data rate needs to be carefully considered in high-speed MIMO communication systems.
Literature review:

This literature review shows output parameters of Throughput, Delay, Packet Loss, Convergence Time, Bit Error Rates, Collision Probability, Secure Key Rates, Quantum Bit Error Rate (Qber), Outage Probability, Secret Key Rate (Skr) are measured by using various algorithm and protocols

Authors	Year	Main findings	Outcomes measured	Algorithms used
Valliamai Ramanathan, A. Prabhakar, Prabha Mandayam	2023	We examined the security of the three and n-pulse Differential-Phase-Shifted Quantum Key Distribution (DPS QKD) protocols against single assaults. In the presence of these assaults, we calculated the relevant bit error rates and collision probability. We compared the resulting secure key rates to known theoretical lower bounds generated from a general individual attack.	•Bit Error Rates •Collision Probability •Secure Key Rates	3 and n pulse Differential Phase Shifted Quantum Key Distribution (DPS QKD) protocols
Nancy Alshaer, Tawfik Ismail	2022	UAV-based FSO systems combining the benefits of FSO and UAV mobility can be secured using CV-QKD and GMCS. System performance is affected by atmospheric turbulence, excess noise, and other impairments. Optimized system parameters and bore sight displacement tolerance of up to 7 cm can be achieved.	•Quantum Bit Error Rate (Qber) •Outage Probability •Secret Key Rate (Skr)	prepare and analyze Based on Gaussian modulation of quantum coherent states (GMCS), the CV QKD methodology
Haijin Ding, R. Wu, Qian Zhao	2018	Quantum Key Distribution (QKD) may be used to significantly improve the privacy and security of Networked Control Systems (NCS). The addition of QKD to NCS can enhance both security and speed by utilizing the most basic encryption method, XOR. A unique Kalman-filter embedded communication protocol that can make better use of the raw keys generated by QKD has been suggested.	•Privacy And Security Of Networked Control Systems (Ncs) •Overall Security Of Ncs •Control Performance	XOR
L. Mailloux, M. Grimaila, D. Hodson, R. D. Engle, C. McLaughlin, G. Baumgartner	2016	A thorough examination of the decoy state protocol enhances both performance and security in terms of detecting PNS assaults. Decoy state protocol can ensure that PNS attacks are detected with high confidence while also increasing the secure key generation rate at no extra expense. Security implementation assistance is offered for QKD system developers and users.	•Quantum Throughput •Security With Respect To Detecting Photon Number Splitting (Pns) Attacks •Secure Key Generation Rate	-

Table 1 shows the parameters measured and by which algorithm were used

Conclusion

In conclusion, this comprehensive literature review highlights the significance of Continuous Variable Quantum Key Distribution (CV-QKD) as a promising technology for bolstering information security in today's interconnected world. Through a meticulous examination of its theoretical foundations, practical implementation, and comparative analysis with other security protocols, this review underscores CV-QKD's resilience to quantum attacks and its potential for secure long-distance key exchange. While recognizing its advantages, we acknowledge the need for further research and development to address practical challenges and enhance its real-world efficiency. As information security remains paramount, CV-QKD emerges as a valuable tool in the arsenal of secure communication protocols, offering a balanced perspective on its strengths and weaknesses in terms of security, speed, and cost-effectiveness. Researchers, practitioners, and policymakers can find valuable insights within this review to inform their decisions and strategies in the realm of secure communications.

References

[1]N. K. Kundu, S. P. Dash, M. R. Mckay, and R. K. Mallik, "Channel Estimation and Secret Key Rate Analysis of MIMO Terahertz Quantum Key Distribution," *IEEE Transactions on Communications*, vol. 70, no. 5, pp. 3350–3363, May 2022, doi: 10.1109/tcomm.2022.3161008.

[2]P. Papanastasiou, A. G. Mountogiannakis, and S. Pirandola, "Composable security of CV-MDI-QKD with secret key rate and data processing," *Scientific Reports*, vol. 13, no. 1, Jul. 2023, doi: 10.1038/s41598-023-37699-5.

[3]A. Máttar and A. Acín, "Implementations for device-independent quantum key distribution," *Physica Scripta*, vol. 91, no. 4, p. 043003, Mar. 2016, doi: 10.1088/0031-8949/91/4/043003.

[4]"QKPT: Securing Your Private Keys in Cloud With Performance, Scalability and Transparency," *IEEE Journals & Magazine | IEEE Xplore*. https://doi.org/10.1109/TDSC.2021.3137403

[5]"An FPGA-Based Physical Layer Approach for a CV-QKD Transmitter," *IEEE Conference Publication | IEEE Xplore*, Jul. 02, 2023. https://doi.org/10.1109/ICTON59386.2023.10207226

[6]"A Quantum Key Distribution Network Routing Performance Based on Software-Defined Network," *IEEE Conference Publication | IEEE Xplore*, Mar. 08, 2023. https://doi.org/10.1109/CCWC57344.2023.10099323

[7]J. Lai *et al.*, "Application and Development of QKD-Based Quantum Secure Communication," *Entropy*, Apr. 06, 2023. https://doi.org/10.3390/e25040627

[8]M. Boyer, R. Liss, and T. Mor, "Composable security against collective attacks of a modified BB84 QKD protocol with information only in one basis," *Theoretical Computer Science*, vol. 801, pp. 96–109, Jan. 2020, doi: 10.1016/j.tcs.2019.08.014.

[9]"Performance Evaluation and Security Analysis of UAV-Based FSO/CV-QKD System Employing DP-QPSK/CD," *IEEE Journals & Magazine | IEEE Xplore*, Jun. 01, 2022. https://doi.org/10.1109/jphot.2022.3164355

[10]D. Huang, S. Liu, and L. Zhang, "Secure Continuous-Variable Quantum Key Distribution with Machine Learning," *Photonics*, Nov. 13, 2021. https://doi.org/10.3390/photonics8110511

[11]"QKD-Enhanced Cybersecurity Protocols," *IEEE Journals & Magazine | IEEE Xplore*, Apr. 01, 2021. https://doi.org/10.1109/JPHOT.2021.3069510

[12]M. Erhard, A. Hochrainer, M. Fink, J. Handsteiner, T. Herbst, and T. Scheidl, "How to choose the best QKD network technology: three different satellite based scenarios compared," *International Conference on Space Optics — ICSO 2020*, Jun. 11, 2021. https://doi.org/10.1117/12.2599218

[13]R. Nandal, A. Nandal, K. Joshi, and A. K. Rathee, "A Survey and Comparison of Some of the Most Prominent QKD Protocols," *Social Science Research Network*, Jan. 01, 2021. https://doi.org/10.2139/ssrn.3769123

[14]G. Kato, M. Fujiwara, and T. Tsurumaru, "Advantage of the Key Relay Protocol Over Secure Network Coding," *IEEE Transactions on Quantum Engineering*, pp. 1–16, 2023, doi: 10.1109/tqe.2023.3309590.

[15]"A portable and compact decoy-state QKD sender," *IEEE Conference Publication | IEEE Xplore*, Jun. 21, 2021. https://doi.org/10.1109/CLEO/Europe-EQEC52157.2021.9541587

[16]"A portable and compact decoy-state QKD sender," *IEEE Conference Publication | IEEE Xplore*, Jun. 21, 2021. https://doi.org/10.1109/CLEO/Europe-EQEC52157.2021.9541587

[17]"Security of Satellite-Based CV-QKD under Realistic Assumptions," *IEEE Conference Publication | IEEE Xplore*, Jul. 01, 2020. https://doi.org/10.1109/ICTON51198.2020.9203397

[18]J. Lin, T. Upadhyaya, and N. Lütkenhaus, "Asymptotic Security Analysis of Discrete-Modulated Continuous-Variable Quantum Key Distribution," *Physical Review X*, vol. 9, no. 4, Dec. 2019, doi: 10.1103/physrevx.9.041064.

[19]"Security Analysis of QKD Protocols: Simulation & Comparison," *IEEE Conference Publication | IEEE Xplore*, Jan. 01, 2020. https://doi.org/10.1109/IBCAST47879.2020.9044522

[20]H. Amellal, A. Meslouhi, A. E. Allati, and A. E. Haddadi, "QKD Protocols Security Between Theory and Engineering Implementation," *Springer eBooks*, Jan. 01, 2020. https://doi.org/10.1007/978-3-030-22277-2_29

[21]U. Ahsan, M. M. Khan, A. Arfeen, and K. Azam, "Security analysis of KXB10 QKD protocol with higher-dimensional quantum states," *International Journal of Quantum Information*, vol. 18, no. 08, p. 2150005, Dec. 2020, doi: 10.1142/s0219749921500052.

[22]M. Li and T. Wang, "Continuous-Variable Quantum Key Distribution Over Air Quantum Channel With Phase Shift," *IEEE Access*, vol. 8, pp. 39672–39677, 2020, doi: 10.1109/access.2020.2975155.

[23]M. Kumar, "Post-quantum cryptography Algorithm's standardization and performance analysis," *Array*, vol. 15, p. 100242, Sep. 2022, doi: 10.1016/j.array.2022.100242.

[24]B. Ouchao and A. Jakimi, "Performance Evaluation of Secure Key Distribution Based on the B92 Protocol," *International Journal of Advanced Engineering, Management and Science*, vol. 4, no. 6, pp. 466–469, 2018, doi: 10.22161/ijaems.4.6.6.

[25]H. Amellal, A. Meslouhi, and A. E. Allati, "Secure Big Data using QKD protocols," *Procedia Computer Science*, vol. 148, pp. 21–29, 2019, doi: 10.1016/j.procs.2019.01.003.

[26]B. Ouchao and A. Jakimi, "Performance Evaluation of Secure Key Distribution Based on the B92 Protocol," *International Journal of Advanced Engineering, Management and Science*, vol. 4, no. 6, pp. 466–469, 2018, doi: 10.22161/ijaems.4.6.6.

[27]A. Aguado, V. Lopez, J. Martinez-Mateo, M. Peev, D. Lopez, and V. Martin, "Virtual Network Function Deployment and Service Automation to Provide End-to-End Quantum Encryption," *Journal of Optical Communications and Networking*, vol. 10, no. 4, p. 421, Mar. 2018, doi: 10.1364/jocn.10.000421.

[28]A. Trizna and A. Ozols, "An Overview of Quantum Key Distribution Protocols," *Information Technology and Management Science*, vol. 21, pp. 37–44, Dec. 2018, doi: 10.7250/itms-2018-0005.

[29]A. Aguado, V. Lopez, J. Martinez-Mateo, M. Peev, D. Lopez, and V. Martin, "Virtual Network Function Deployment and Service Automation to Provide End-to-End Quantum Encryption," *Journal of Optical Communications and Networking*, vol. 10, no. 4, p. 421, Mar. 2018, doi: 10.1364/jocn.10.000421.

[30]N. Djeffal and M. Benslama, "Quantum key distribution in WDM router applications for secured data transmission," *Optical and Quantum Electronics*, vol. 48, no. 1, Dec. 2015, doi: 10.1007/s11082-015-0349-1.

[31]S. Guerrini, M. Chiani, and A. Conti, "Secure Key Throughput of Intermittent Trusted-Relay QKD Protocols," *2018 IEEE Globecom Workshops (GC Wkshps)*, Dec. 2018, Published, doi: 10.1109/glocomw.2018.8644402.

[32]A. Aguado *et al.*, "Hybrid Conventional and Quantum Security for Software Defined and Virtualized Networks," *Journal of Optical Communications and Networking*, vol. 9, no. 10, p. 819, Sep. 2017, doi: 10.1364/jocn.9.000819.

[33]A. R. Dixon *et al.*, "Quantum key distribution with hacking countermeasures and long term field trial," *Scientific Reports*, vol. 7, no. 1, May 2017, doi: 10.1038/s41598-017-01884-0.

[34]C. Lupo, C. Ottaviani, P. Papanastasiou, and S. Pirandola, "Continuous-variable measurement-device-independent quantum key distribution: Composable security against coherent attacks," *Physical Review A*, vol. 97, no. 5, May 2018, doi: 10.1103/physreva.97.052327.

[35]C. Lupo, C. Ottaviani, P. Papanastasiou, and S. Pirandola, "Continuous-variable measurement-device-independent quantum key distribution: Composable security against coherent attacks," *Physical Review A*, vol. 97, no. 5, May 2018, doi: 10.1103/physreva.97.052327.

[36]S. K. Ranu, G. K. Shaw, A. Prabhakar, and P. Mandayam, "Security with 3-Pulse Differential Phase Shift Quantum Key Distribution," *2017 IEEE Workshop on Recent Advances in Photonics (WRAP)*, Dec. 2017, Published, doi: 10.1109/wrap.2017.8468572.

[37]A. Yadav, M. M., R. Tiwari, and R. Jain, "Securing Cloud Computing Environment using Quantum Key Distribution," *International Journal of Computer Applications*, vol. 180, no. 41, pp. 43–45, May 2018, doi: 10.5120/ijca2018917112.

[38]P. S. Lakshmi and G. Murali, "Comparison of classical and quantum cryptography using QKD simulator," *2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS)*, Aug. 2017, Published, doi: 10.1109/icecds.2017.8390120.

[39]V. Burenkov, B. Qi, B. Fortescue, and H.-K. Lo, "Security of high speed quantum key distribution with finite detector dead time," *Quantum Information and Computation*, vol. 14, no. 3 & 4, pp. 217–235, Mar. 2014, doi: 10.26421/qic14.3-4-2.

[40]Q. Cai and Y. Tan, "Photon-number-resolving decoy-state quantum key distribution," *Physical Review A*, vol. 73, no. 3, Mar. 2006, doi: 10.1103/physreva.73.032305.

[41]M. Mafu and M. Senekane, "Security of Quantum Key Distribution Protocols," *Advanced Technologies of Quantum Key Distribution*, May 2018, Published, doi: 10.5772/intechopen.74234.

[42]J. Park, J. Kim, and N. Park, "Utilization of IPSec Protocol Applied with Quantum Key Distribution (QKD)," *Journal of Convergence Science, Technology, and Society*, vol. 1, no. 1, pp. 21–25, Jun. 2022, doi: 10.56366/jcsts.2022.1.1.21.

[43]O. K. Jasim, S. Abbas, E.-S. M. El-Horbaty, and A.-B. M. Salem, "Quantum Key Distribution: Simulation and Characterizations," *Procedia Computer Science*, vol. 65, pp. 701–710, 2015, doi: 10.1016/j.procs.2015.09.014.

[44]A. Parakh, "Quantifying the security of a QKD protocol," *2015 IEEE International Conference on Advanced Networks and Telecommuncations Systems (ANTS)*, Dec. 2015, Published, doi: 10.1109/ants.2015.7413637.

[45]X. Chen, B. Li, and Q. Zhou, "Lightweight and High-Performance Data Protection for Edge Network Security," *Wireless Communications and Mobile Computing*, vol. 2022, pp. 1–24, Feb. 2022, doi: 10.1155/2022/8458314.

[46]N. Walk, T. Symul, P. K. Lam, and T. C. Ralph, "Unconditional security of Gaussian post-selected continuous variable quantum key distribution," *2013 Conference on Lasers & Electro-Optics Europe & International Quantum Electronics Conference CLEO EUROPE/IQEC*, May 2013, Published, doi: 10.1109/cleoe-iqec.2013.6801697.

[47]C. Harper, M. R. Grimaila, and G. Baumgartner, "An Evaluation of Security Standards Implementation in Quantum Key Distribution Systems," *INCOSE International Symposium*, vol. 23, no. 1, pp. 1475–1486, Jun. 2013, doi: 10.1002/j.2334-5837.2013.tb03100.x.

[48]S. Wang, Z.-F. Han, W. Chen, Z.-Q. Yin, D.-Y. He, and G.-C. Guo, "The QKD network: From metropolitan to wide area," *2013 IEEE Photonics Society Summer Topical Meeting Series*, Jul. 2013, Published, doi: 10.1109/phosst.2013.6614520.

[49]P. Y. A. Ryan and B. Christianson, "Enhancements to Prepare-and-Measure Based QKD Protocols," *Security Protocols XXI*, pp. 123–133, 2013, doi: 10.1007/978-3-642-41717-7_14.

[50]L. Oesterling, D. Hayford, and G. Friend, "Comparison of commercial and next generation quantum key distribution: Technologies for secure communication of information," *2012 IEEE Conference on Technologies for Homeland Security (HST)*, Nov. 2012, Published, doi: 10.1109/ths.2012.6459842.

[51]N. Saleem, A. Rahman, M. Rizwan, S. Naseem, and F. Ahmad, "Enhancing Security of Android Operating System Based Phones using Quantum Key Distribution," *ICST Transactions on Scalable Information Systems*, p. 165281, Jul. 2018, doi: 10.4108/eai.13-7-2018.165281.

[52]C. Lupo and Y. Ouyang, "Quantum Key Distribution with Nonideal Heterodyne Detection: Composable Security of Discrete-Modulation Continuous-Variable Protocols," *PRX Quantum*, vol. 3, no. 1, Mar. 2022, doi: 10.1103/prxquantum.3.010341.

[53]M. SUN, X. PENG, Y. SHEN, and H. GUO, "SECURITY OF A NEW TWO-WAY CONTINUOUS-VARIABLE QUANTUM KEY DISTRIBUTION PROTOCOL," *International Journal of Quantum Information*, vol. 10, no. 05, p. 1250059, Aug. 2012, doi: 10.1142/s0219749912500591.

[54]S. Rass, A. Wiegele, and P. Schartner, "Building a Quantum Network: How to Optimize Security and Expenses," *Journal of Network and Systems Management*, vol. 18, no. 3, pp. 283–299, Mar. 2010, doi: 10.1007/s10922-010-9162-0.

[55]T. S. Thangavel and A. Krishnan, "Performance of integrated quantum and classical cryptographic model for password authentication," *2010 Second International conference on Computing, Communication and Networking Technologies*, Jul. 2010, Published, doi: 10.1109/icccnt.2010.5591718.

[56]M. Elboukhari, M. Azizi, and A. Azizi, "Analysis of the Security of BB84 by Model Checking," *International journal of Network Security & Its Applications*, vol. 2, no. 2, pp. 87–98, Apr. 2010, doi: 10.5121/ijnsa.2010.2207.

[57]M. Elboukhari, M. Azizi, and A. Azizi, "Improving the Security of CHAP Protocol by Quantum Cryptography," *Studies in Computational Intelligence*, pp. 241–245, 2010, doi: 10.1007/978-3-642-15211-5_25.

[58]M. Elboukhari, M. Azizi, and A. Azizi, "Improving TLS Security By Quantum Cryptography," *International Journal of Network Security & Its Applications*, vol. 2, no. 3, pp. 87–100, Jul. 2010, doi: 10.5121/ijnsa.2010.2306.

[59]V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," *Reviews of Modern Physics*, vol. 81, no. 3, pp. 1301–1350, Sep. 2009, doi: 10.1103/revmodphys.81.1301.