Document Version
Final published version

Citation (APA)
Beauchamp, T. R., Sebastián-Lombraña, A., Gauthier, S., Romero, J. J., Martin, V., Wehner, S., & Ortiz, L. (2025). Towards a common framework for quantum information networking. In V. Martin, N. Yu, & C. Qian (Eds.), *QuNet '25: Proceedings of the 2nd Workshop on Quantum Networks and Distributed Quantum Computing* (pp. 56-59). Association for Computing Machinery (ACM). https://doi.org/10.1145/3749096.3750025

Towards a common framework for quantum information networking

Extended Abstract

Thomas R. Beauchamp
Delft University of Technology
Delft, The Netherlands

Alberto Sebastián-Lombraña
Universidad Politécnica de Madrid
Madrid, Spain

Scarlett Gauthier
Delft University of Technology
Delft, The Netherlands

Juan Jose Romero
Universidad Politécnica de Madrid
Madrid, Spain

Vicente Martin
Universidad Politécnica de Madrid
Madrid, Spain

Stephanie Wehner
Delft University of Technology
Delft, The Netherlands

Laura Ortiz
Universidad Politécnica de Madrid
Madrid, Spain

ABSTRACT

Designing and developing future quantum information networks is currently a cutting-edge topic. However, advances made in quantum cryptographic networks and independently in entanglement-based networks create the need for a unified framework for quantum information networking. This work attempts to set a path to a common paradigm for future quantum information networking.

CCS CONCEPTS

• **Networks** → **Network architectures**; *Network management*; • **Security and privacy** → **Key management**; • **Hardware** → **Quantum technologies**;

1 INTRODUCTION

Quantum information networks will be essential infrastructures for enabling quantum technologies. Indeed, quantum information and communication technologies are driving the second quantum revolution [18].

However, several very promising network paradigms are being developed in parallel. On the one hand, quantum cryptography networks are based on reasonably mature technologies, such as quantum key distribution (QKD) [21, 28]. Initiatives such as the European Quantum Communications Infrastructure (EuroQCI) [11] are therefore showing the potential of quantum-enhanced secure communications, but also proving that quantum information networking is feasible [9]. On the other hand, an entanglement-based quantum internet would enable general-purpose quantum applications beyond cryptography, including quantum metrology, coordination of decisions, and scalable quantum computing [35].

A notable example of the former is the Madrid Quantum Communications Infrastructure (MadQCI) [27], a metropolitan-wide quantum-communication testbed network with a strong focus on industrial applicability. So far only quantum cryptography systems have been installed and tested.

The most significant contemporary instance of the latter will be the Quantum Internet Alliance (QIA) prototype network [1]. QIA has a moonshot mission to build a full-stack prototype that will validate all key sub-systems of an entanglement-based network. The goal is to do so by the end of the decade (2030). Key milestones towards meeting this goal have already been demonstrated [16, 24, 30]. Full systems tests will push the boundaries of what is possible with quantum network technologies.

These two examples of quantum information networks pursue similar goals, but their frameworks, approaches, designs, and implementations differ significantly, from the most abstract to the most concrete. This work aims to describe these two milestones, MadQCI and the QIA prototype, setting a path towards a common framework for quantum information networking. A common framework would benefit all areas of quantum information networking by facilitating technological or methodological transfer between domains and creating opportunities for accelerated advancement.

QuNet '25, September 8–11, 2025, Coimbra, Portugal

ACM ISBN 979-8-4007-2097-0/25/09.
https://doi.org/10.1145/3749096.3750025

2 QUANTUM CRYPTOGRAPHIC NETWORKS. MADQCI

MadQCI is a quantum-communication test bed network focused on quantum cryptography systems, such as QKD. These systems are capable of growing symmetric key material, by transmitting and processing quantum information and executing specific-purpose algorithms called quantum protocols [4, 5]. Thus, its fundamental applications are cryptographic, to replace other key-agreement primitives vulnerable to quantum computing [29].

QKD as a quantum-communications technology is close to commercial readiness and well-established standards are set, proposed at ETSI GS QKD [15] and ITU-T Y.3800 [31]. However, i) it is supported by a limited set of transmission and information-processing techniques, called "prepare and measure", and ii) it is a specific-purpose technology, whose programming is given when manufactured.

To manage the security issues related to the delivery of key material, each node is implemented as a "trusted node", to enable key forwarding through the network —e.g., a Vernam cipher [34] to encrypt and decrypt a user key by performing hop-by-hop forwarding. Also, since prepare and measure techniques have a limited reach, this solution may be used to extend it, although it is not typical in metropolitan-wide networks to find nodes dedicated solely to this purpose, since most of them deliver services. For long distances, satellite links [10] could be used to overcome the reach limitation.

In practice, this approach has implications beyond security. Quantum information transmissions happen in each link independently of the rest, so each QKD pair controls and manages its own signalling and synchronisation —needed in QKD in the gigabauds order. On the contrary, the shared components have to be managed with a global scope. MadQCI uses as the principal network resource the "key association" or "key stream", as defined by the ETSI GS QKD group of standards. Other approaches are possible, for enabling the interoperability needed to enable long-range quantum internetworking, as EuroQCI pursues.

Finally, to enable all above mentioned functionalities, a complex infrastructure is required, ranging from an optical network to Ethernet network systems or computer systems. Actually, it is possible to share this quantum-network infrastructure to support other quantum communications and, therefore, the QKD systems would be quantum-application systems from its point of view: if the QKD systems were removed and other quantum-enabled systems were installed —e.g., quantum-synchronised clocks [25]—, the quantum-network infrastructure may remain unchanged.

3 ENTANGLEMENT-BASED QUANTUM INTERNET: QIA PROTOTYPE

A quantum internet is a general-purpose quantum network that enables entanglement generation between end nodes, to realize applications that are impossible or inefficient to realize on any classical communication network. Example applications of a quantum network include secure cloud computation [2, 7], secure communication protocols such as QKD [4, 20], anonymous leader election [32], improvements to metrology [22, 26] and many more [14, 35]. Depending on the properties of the end nodes, and the network connecting them, different types of applications may be realized, which have been classified into stages of quantum internet development [35]. A quantum internet application consists of multiple programs, one running at each end node participating in the application. Such programs interact with each other by classical message passing and quantum communication (entanglement generation) [16, 17, 33]. This enables the realization of security sensitive applications such as blind-quantum computing, but prohibits a centrally controlled program execution. We remark that this paradigm is exactly analogous to conventional internet applications, for example client-server applications, in which a separate program is executed on the client than on the server. This differentiates quantum internet applications from quantum computing applications, which consist of a single program, even when distributed over multiple quantum computers joined into a computing cluster. When talking about the composition of the network, the QIA prototype network makes use of the network stack from [12]. There are three layers relevant to the discussion here, the *physical layer* where actual attempts to make elementary entangled links between neighbouring nodes occur; the *link layer*, where the generation of elementary links is facilitated; and the *network layer* which is responsible for generating end-to-end entangled links across the network.

In order to execute instances of quantum network applications, end-to-end entangled links need to be generated between the end nodes involved. This requires the use of shared internal network components such as repeater chains [8, 19], junction nodes [3] and entanglement generation interfaces [6, 23] to enable generating links over extended distances. Use of these components may need to be shared between many groups of end nodes, thus they can be treated as network resources. The network then must solve the problem of allocating sets of resources to groups of end nodes, in order to fulfil the need for generation of end-to-end entangled links between groups of end nodes.

To achieve this, control of the QIA prototype network is initially based on an implementation of the network control architecture from [3]. This means that the network operates as a *generate-when-requested* network, with a central controller which periodically computes and distributes network schedules determining which resources can be used by which groups of end nodes and when. Note that these network schedules only regulate *access* to network resources, they do not, for example, determine which specific actions the nodes in the network need to take at the physical layer or when. In order for end nodes to have time and resources allocated to them in these network schedules, they need to submit demands to the central controller. These demands must encode the requirements for successfully completing the desired number of instances of the application that the end nodes will run. In particular, these demands are for the generation of a number of *packets of entanglement*, sets of coexisting entangled links generated with a minimum initial fidelity [3, 13].

4 CONCLUSION

From the discussion above, it is clear that quantum cryptography networks and entanglement-based networks have worked until now with their particular frameworks and strategies.

On one hand, QKD networks enable the growing of cryptographic keys. In particular, in MadQCI the main network resource is the "key stream", which is allocated by control mechanisms to serve cryptographic applications. On the other hand, entanglement based networks facilitate the generation of long-distance entangled links which can be consumed by applications running on end nodes. To achieve this, the control protocols of the QIA prototype network mediate access to the internal components of the network, which are treated as resources to be shared between (pairs of) users.

Whilst both network paradigms derive terminology from classical networking, differences in technological progression has led to focusing on different aspects. Although each approach has many benefits in their specific contexts, many questions arise when considering the road ahead for quantum information networking. Within this work, we lay out an opportunity to develop a wider and richer framework for quantum information networking.

ACKNOWLEDGMENTS

TRB, SG, and SW acknowledge support from the Quantum Internet Alliance (QIA). QIA has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No. 101102140. SW also acknowledges funding from NWO VICI. AS-L, JJR, VM, and LO acknowledge support from the Quantum Secure Networks Partnership (QSNP). QSNP has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No. 101114043.

ETHICS

This work does not raise any ethical issues.

REFERENCES

[1] Quantum Internet Alliance. 2025. Quantum Internet Alliance. (2025). https://quantuminternetalliance.org https://quantuminternetalliance.org [Accessed 29th April 2025].

[2] P. Arright and L. Salvail. 2006. Blind Quantum Computation. *International Journal of Quantum Information* 04, 05 (2006), 883–898.

[3] T. R. Beauchamp, H. Jirovská, S. Gauthier, and S. Wehner. 2025. A Modular Quantum Network Architecture for Integrating Network Scheduling with Local Program Execution. (March 2025). https://doi.org/10.48550/arXiv.2503.12582 arXiv:2503.12582 [quant-ph].

[4] C. H. Bennett and G. Brassard. 2014. Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science* 560 (Dec. 2014), 7–11. https://doi.org/10.1016/j.tcs.2014.05.025

[5] C. H. Bennett, G. Brassard, and N. D. Mermin. 1992. Quantum cryptography without Bell's theorem. *Phys. Rev. Lett.* 68 (Feb 1992), 557–559. Issue 5. https://doi.org/10.1103/PhysRevLett.68.557

[6] H. K. C. Beukers, M. Pasini, H. Choi, D. Englund, R. Hanson, and J. Borregaard. 2024. Remote-Entanglement Protocols for Stationary Qubits with Photonic Interfaces. *PRX Quantum* 5, 1 (March 2024), 010202. https://doi.org/10.1103/prxquantum.5.010202

[7] A. Broadbent, J. Fitzsimons, and E. Kashefi. 2009. Universal Blind Quantum Computation. In *2009 50th Annual IEEE Symposium on Foundations of Computer Science*. IEEE, Atlanta, Georgia, USA, 517–526. https://doi.org/10.1109/focs.2009.36

[8] C. Cabrillo, J. I. Cirac, P. García-Fernández, and P. Zoller. 1999. Creation of entangled states of distant atoms by interference. *Phys. Rev. A* 59 (Feb. 1999), 1025–1033. Issue 2.

[9] Y. Cao, Y. Zhao, Q. Wang, J. Zhang, S. X. Ng, and L. Hanzo. 2022. The Evolution of Quantum Key Distribution Networks: On the Road to the Qinternet. *IEEE Communications Surveys & Tutorials* 24, 2 (2022), 839–894. https://doi.org/10.1109/COMST.2022.3144219

[10] Y.-A. Chen, Q. Zhang, T.-Y. Chen, W.-Q. Cai, S.-K. Liao, J. Zhang, K. Chen, J. Yin, J.-G. Ren, Z. Chen, S.-L. Han, Q. Yu, K. Liang, F. Zhou, X. Yuan, M.-S. Zhao, T.-Y. Wang, X. Jiang, L. Zhang, W.-Y. Liu, Y. Li, Q. Shen, Y. Cao, C.-Y. Lu, R. Shu, J.-Y. Wang, L. Li, N.-L. Liu, F. Xu, X.-B. Wang, C.-Z. Peng, and J.-W. Pan. 2021. An integrated space-to-ground quantum communication network over 4,600 kilometres. *Nature* 589, 7841 (01 Jan 2021), 214–219. https://doi.org/10.1038/s41586-020-03093-8

[11] European Commission. 2024. The European Quantum Communication Infrastructure (EuroQCI) Initiative. (2024). https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci

[12] A. Dahlberg, M. Skrzypczyk, T. Coopmans, L. Wubben, F. Rozpundefineddek, M. Pompili, A. Stolk, P. Pawełczak, R. Knegjens, J. de Oliveira Filho, R. Hanson, and S. Wehner. 2019. A link layer protocol for quantum networks. In *Proceedings of the ACM Special Interest Group on Data Communication (SIGCOMM '19)*. Association for Computing Machinery, New York, NY, USA, 159–173. https://doi.org/10.1145/3341302.3342070

[13] B. Davies, T. Beauchamp, G. Vardoyan, and S. Wehner. 2024. Tools for the Analysis of Quantum Protocols Requiring State Generation Within a Time Window. *IEEE Transactions on Quantum Engineering* 5 (2024), 1–20. https://doi.org/10.1109/TQE.2024.3358674

[14] D. Ding and L. Jiang. 2024. Coordinating Decisions via Quantum Telepathy. (Sept. 2024). https://doi.org/10.48550/arXiv.2407.21723 arXiv:2407.21723 [quant-ph].

[15] Industry Specification Group Quantum Key Distribution. 2022. *Quantum Key Distribution (QKD); Control Interface for Software Defined Networks.* Standard. European Telecommunications Standards Institute, Sophia Antipolis, CH.

[16] C. Delle Donne, M. Iuliano, B. van der Vecht, G. M. Ferreira, H. Jirovská, T. J. W. van der Steenhoven, A. Dahlberg, M. Skrzypczyk, D. Fioretto, M. Teller, P. Filippov, A. R.-P. Montblanch, J. Fischer, H. B. van Ommen, N. Demetriou, D. Leichtle, L. Music, H. Ollivier, I. te Raa, W. Kozlowski, T. H. Taminiau, P. Pawełczak, T. E. Northup, R. Hanson, and S. Wehner. 2025. An operating system for executing applications on quantum network nodes. *Nature* 639, 8054 (March 2025), 321–328. https://doi.org/10.1038/s41586-025-08704-w

[17] C. Delle Donne, M. Iuliano, B. van der Vecht, G. M. Ferreira, H. Jirovská, T. J. W. van der Steenhoven, A. Dahlberg, M. Skrzypczyk, D. Fioretto, M. Teller, P. Filippov, A. R.-P. Montblanch, J. Fischer, H. B. van Ommen, N. Demetriou, D. Leichtle, L. Music, H. Ollivier, I. te Raa, W. Kozlowski, T. H. Taminiau, P. Pawełczak, T. E. Northup, R. Hanson, and S. Wehner. 2025. An operating system for executing applications on quantum network nodes. *Nature* 639, 8054 (March 2025), 321–328. https://doi.org/10.1038/s41586-025-08704-w Publisher: Nature Publishing Group.

[18] J. P. Dowling and G. J. Milburn. 2003. Quantum Technology: The Second Quantum Revolution. *Phil. Trans. Roy. Soc. Lond. A* 361, 1809 (2003), 1655–1674. https://doi.org/10.1098/rsta.2003.1227 arXiv:quant-ph/0206091

[19] L.-M. Duan, M. D. Lukin, J. I. Cirac, and P. Zoller. 2001. Long-distance quantum communication with atomic ensembles and linear optics. *Nature* 414, 6862 (Nov. 2001), 413–418.

[20] A. K. Ekert. 1991. Quantum cryptography based on Bell's theorem. *Physical Review Letters* 67, 6 (Aug. 1991), 661–663. https://doi.org/10.1103/PhysRevLett.67.661 Publisher: American Physical Society.

[21] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden. 2002. Quantum cryptography. *Rev. Mod. Phys.* 74 (Mar 2002), 145–195. Issue 1. https://doi.org/10.1103/RevModPhys.74.145

[22] D. Gottesman, T. Jennewein, and S. Croke. 2012. Longer-Baseline Telescopes Using Quantum Repeaters. *Phys. Rev. Lett.* 109 (2012), 070503. Issue 7. https://doi.org/10.1103/PhysRevLett.109.070503

[23] C. Jones, D. Kim, M. T. Rakher, P. G. Kwiat, and T. D. Ladd. 2016. Design and analysis of communication protocols for quantum repeater networks. *New Journal of Physics* 18, 8 (aug 2016), 083015. https://doi.org/10.1088/1367-2630/18/8/083015

[24] V. Krutyanskiy, M. Galli, V. Krcmarsky, S. Baier, D. A. Fioretto, Y. Pu, A. Mazloom, P. Sekatski, M. Canteri, M. Teller, J. Schupp, J. Bate, M. Meraner, N. Sangouard, B. P. Lanyon, and T. E. Northup. 2023. Entanglement of Trapped-Ion Qubits Separated by 230 Meters. *Phys. Rev. Lett.* 130, 5 (Feb 2023), 050803. https://doi.org/10.1103/PhysRevLett.130.050803

[25] P. Kómár, E. M. Kessler, M. Bishof, L. Jiang, A. S. Sørensen, J. Ye, and M. D. Lukin. 2014. A quantum network of clocks. *Nature Physics* 10, 8 (Aug. 2014), 582–587. https://doi.org/10.1038/nphys3000 arXiv:quant-ph/1310.6045

[26] P. Kómár, E. M. Kessler, M. Bishof, L. Jiang, A. S. Sørensen, J. Ye, and M. D. Lukin. 2014. A quantum network of clocks. *Nature Physics* 10, 8 (June 2014), 582–587. https://doi.org/10.1038/nphys3000

[27] V. Martin, J. P. Brito, L. Ortíz, R. B. Méndez, J. S. Buruaga, R. J. Vicente, A. Sebastián-Lombraña, D. Rincón, F. Pérez, C. Sánchez, M. Peev, H. H. Brunner, F. Fung, A. Poppe, F. Fröwis, A. J. Shields, R. I. Woodward, H. Griesser, S. Roehrich, F. de la Iglesia, C. Abellán, M. Hentschel, J. M. Rivas-Moscoso, A. Pastor-Perales, J. Folgueira, and D. López. 2024. MadQCI: a heterogeneous and scalable SDN-QKD network deployed in production facilities. *npj Quantum Information* 10, 1 (02 Sept. 2024), 80. https://doi.org/10.1038/s41534-024-00873-2

[28] V. Martin, J. Martinez-Mateo, and M. Peev. 2017. *Introduction to Quantum Key Distribution.* John Wiley & Sons, Ltd, West Sussex, United Kingdom, 1–17. https://doi.org/10.1002/047134608X.W8354 arXiv:https://onlinelibrary.wiley.com/doi/pdf/10.1002/047134608X.W8354

[29] V. Mavroeidis, K. Vishi, M. D. Zych, and A. Jøsang. 2018. The Impact of Quantum Computing on Present Cryptography. *International Journal of Advanced Computer Science and Applications* 9, 3 (2018), 405–414. https://doi.org/10.14569/IJACSA.2018.090354

[30] J. V. Rakonjac, S. Grandi, S. Wengerowsky, D. Lago-Rivera, F. Appas, and H. de Riedmatten. 2023. Transmission of light–matter entanglement over a metropolitan network. *Optica Quantum* 1, 2 (Dec. 2023), 94. https://doi.org/10.1364/opticaq.501048

[31] ITU Telecommunication Standardization Sector. 2019. *Overview on networks supporting quantum key distribution.* Recommendation. International Telecommunication Union.

[32] S. Tani, H. Kobayashi, and K. Matsumoto. 2012. Exact Quantum Algorithms for the Leader Election Problem. *ACM Transactions on Computation Theory* 4, 1 (March 2012), 1–24. https://doi.org/10.1145/2141938.2141939

[33] B. van der Vecht, A. T. Yücel, H. Jirovská, and S. Wehner. 2025. Qoala: an Application Execution Environment for Quantum Internet Nodes. (Feb. 2025). https://doi.org/10.48550/arXiv.2502.17296 arXiv:2502.17296 [quant-ph].

[34] G. S. Vernam. 1926. Cipher Printing Telegraph Systems For Secret Wire and Radio Telegraphic Communications. *Transactions of the American Institute of Electrical Engineers* XLV (1926), 295–301. https://doi.org/10.1109/T-AIEE.1926.5061224

[35] S. Wehner, D. Elkouss, and R. Hanson. 2018. Quantum internet: A vision for the road ahead. *Science* 362 (Oct 2018), eaam9288. Issue 6412. https://doi.org/10.1126/science.aam9288 Publisher: American Association for the Advancement of Science.