ITU Journal
Future and evolving technologies

FREE I FAST I FOR ALL

The *ITU Journal on Future and Evolving Technologies (ITU J-FET)* is an international journal providing complete coverage of all communications and networking paradigms, free of charge for both readers and authors. The ITU Journal considers yet-to-be-published papers addressing fundamental and applied research. It shares new techniques and concepts, analyses and tutorials, as well as learning from experiments and physical and simulated testbeds. It also discusses the implications of the latest research results for policy and regulation, legal frameworks, the economy and society. This publication builds bridges between disciplines, connects theory with application, and stimulates international dialogue. Its interdisciplinary approach reflects ITU's comprehensive field of interest and explores the convergence of ICT with other disciplines. The ITU Journal welcomes submissions at any time, and on any topic within its scope.

Special issue on

Quantum-safe communication

Call for papers

Next-generation Information and Communication Technology (ICT) infrastructures face growing security challenges as advances in quantum computing threaten the long-term viability of widely deployed cryptographic mechanisms. In response, the research community has been developing quantum-safe security approaches capable of protecting communications against quantum-enabled adversaries. Two complementary directions have emerged: Quantum Key Distribution (QKD), which exploits fundamental principles of quantum mechanics to enable secure key establishment, and Post-Quantum Cryptography (PQC), which relies on classical cryptographic algorithms designed to resist quantum attacks. Each approach presents distinct technical challenges, ranging from the physical constraints and deployment complexity of QKD systems to the performance, implementation, and security analysis of candidate PQC algorithms.

Beyond algorithmic and protocol design, a central challenge lies in integrating quantum-safe technologies into existing and emerging ICT infrastructures. Realizing the benefits of QKD and PQC at scale requires their incorporation into the Internet and optical transport networks without compromising performance, reliability, or operational flexibility. This integration raises fundamental questions regarding network architecture, key management, protocol interoperability, and the coexistence of quantum and classical communication mechanisms.

Key open questions therefore extend from the design of quantum communication networks and hybrid quantum-classical security architectures to the evaluation of system-level performance in realistic deployment scenarios. In particular, the realization of large-scale quantum communication networks raises fundamental challenges related to long-distance scalability, the use of quantum repeaters, and the development of routing algorithms and communication protocols specifically tailored to quantum information exchange.

Addressing these challenges calls for interdisciplinary research spanning quantum physics, cryptography, and network engineering, with an emphasis on experimental validation and real-world applicability. In this context, this special issue invites contributions that advance the understanding and practical realization of quantum-safe communications, including novel architectures, protocols, integration strategies, and insights gained from experimental platforms and deployment experience..

Suggested topics (but not limited to):

Quantum communication networks & infrastructure	• Design and simulation of multi-node quantum network topologies and architectures • Quantum repeaters and entanglement distribution strategies for long-distance networks • Routing algorithms and communication protocols tailored for quantum networks • Integration of quantum links with classical telecom networks • Hybrid quantum-classical network infrastructures
Quantum-safe cryptography & security	• Advances in QKD protocols and quantum cryptographic schemes • Post-quantum cryptographic algorithms: design, implementation, and security evaluation • Hybrid cryptographic frameworks combining QKD and PQC • Migration strategies to quantum-safe solutions • Security proofs and threat models for quantum-safe communication protocols • Quantum-resistant authentication and key management techniques • Certification aspects of quantum-safe cryptographic implementations
Integration and performance in classical ICT infrastructure	• Techniques for deploying QKD over Internet and IP networks • Performance evaluation of quantum-enhanced networks • Adaptation of network protocols and management strategies for hybrid quantum–classical networks
Implementation, testbeds & deployment	• Results from experimental quantum network testbeds and field trials of QKD networks over fiber, free-space, or satellite links • Scalability challenges and performance evaluation of quantum-enhanced network architectures • Multi-node and multi-vendor interoperability experiments in quantum communication systems • Performance assessment of deployed quantum communication links (key rates, error rates, distance limitations) • Case studies from practical deployments

Keywords
Quantum communication, quantum repeaters, quantum key distribution (QKD), post-quantum cryptography (PQC), interoperability

Deadlines
Paper submission: 30 November 2026
Paper acceptance notification: 1 February 2027
Camera-ready paper submission: 1 March 2027

Paper submission
This special issue calls for original scientific papers. Submitted papers should not be under consideration for publication elsewhere.

Submissions must be made electronically using ScholarOne Manuscripts, where templates and guidelines are also available.

Publication
Papers will be published in the ITU digital library.

Additional information
Please visit the ITU Journal website at: https://www.itu.int/en/journal/j-fet/Pages/default.aspx. Inquiries should be addressed to Alessia Magliarditi at: journal@itu.int.