ERICSSON

Decoding quantum-safe encryption: Key to ensuring confidentiality in networks

Executive summary

Mobile networks are widely identified as critical national infrastructure necessary to ensure a functioning and prosperous society. At the most fundamental level, all secure communication relies on maintaining the confidentiality and integrity of the identity of participants and their communication. This is accomplished with cryptographic algorithms and protocols.

Quantum computing is not yet widely available, but it has the potential to speed up many previously intractable computational problems in fields such as financial modeling, pharmaceutical research, and materials research. The major potential upside of quantum computing and related technologies thus has provided an impetus for major investments in research and development.

The rapid technological advancements in quantum physics are also speeding up the emergence of quantum computers. These machines can potentially break many cryptographic algorithms that are currently in use, compromising the security of our current telecommunication networks.

Since quantum computers will become industrially useful well before being a threat to cryptography, it is worthwhile to distinguish general-purpose quantum computers from cryptographically relevant quantum computers (CRQCs) that are expected to specifically threaten existing cryptographic algorithms.

The realization of CRQCs is not expected to occur in the next decade but given the uncertainties with rapidly advancing technologies, it is prudent to prepare well in advance.

Quantum-resistant cryptography, also referred to as post-quantum cryptography (PQC), is a type of cryptography that is developed for classical computers. They are designed to resist potential attacks by both classical computers and CRQCs based on our current understanding of the best quantum algorithms and their limitations. PQC algorithms are also suitable for all types of implementations including software-only, hardware-assisted, and hardware-based.

Ericsson and the telecommunication industry prefer to use solutions that are widely used and proven to work at scale and are built on open and public standards and specifications.

In 5 to 10 years Ericsson believes, along with a significant share of 3GPP members, that the most effective and efficient approach to mitigating CRQC threat is by using quantum-resistant cryptography.

Ensuring a broad international policy consensus on the path forward of the realization of quantum-resistant cryptography is of utmost importance, to not only ensure the security of mobile communication systems but also cost-effective, interoperable, and timely realization at scale.

To further expedite the development toward a timely realization of quantum-resistant cryptography, standardization work is already ongoing in relevant standardization and industry bodies. These organizations are also developing technologies and guidelines for the use of quantum communication. Contributions are being made towards the NIST PQC standards, IETF, 3GPP, GSMA Post Quantum Task Network, CISA/DHS, and ATIS.

To ensure international policy consensus on PQC, Ericsson encourages timely and increased intergovernmental and international policy coordination in relevant forums and formats. This will allow the industry to realize secure, internationally harmonized, and interoperable PQC solutions on a global scale.

Introduction

Quantum physics developed in the early 1900s as a result of the contributions of figures like Max Planck, Niels Bohr, Erwin Schrödinger, Werner Heisenberg, and others. From the mid-20th century, researchers succeeded in developing methods for measuring and controlling individual atoms and photons. Around the same time, other researchers developed electronic components from semiconductors and superconductors, in which they could manipulate individual electrons. Examples of such structures are Josephson junctions, ion traps, and quantum dots. This knowledge has led to the development of quantum computers. A quantum computer can perform loads of calculations simultaneously thanks to the quantum property known as superposition, a property not available for the current, that is, classical computers.

In recent years, much has been written about the threat from the forthcoming quantum computing revolution to the security of existing ICT solutions and systems, including mobile networks. The future applications of quantum physics present not only a challenge but also an opportunity to enhance operations, energy efficiency, and the security of ICT systems.

While quantum computing is not yet widely available, it has the potential to speed up many previously intractable computational problems in fields such as financial modeling, pharmaceutical research, and materials research. The major potential upside of quantum computing and related technologies thus has provided an impetus for major investments in research and development. The rapid development of quantum computing does also, unfortunately, bring closer the realization of quantum computers capable of breaking many currently deployed cryptographic algorithms used in present day secure and confidential telecommunication networks, threatening the confidentiality of communication.

There are two complementary approaches to securing communication protocols against quantum computers: the development of quantum-resistant cryptographic algorithms, also called post-quantum cryptography (PQC), and the development of quantum communications technologies, that is, quantum key distribution (QKD). Widespread adoption of PQC is expected to happen in the near term, driven by organizations such as NIST, IETF, and major Internet service companies. Unlike PQC, QKD requires not only more time to mature the technology but also new hardware and changes to existing solutions and will therefore require a longer adoption period.

Cryptography

Cryptography is the field of coding information so that only the intended recipient can decode and read it. Cryptographic algorithms, or ciphers, are specific methods to perform this task. **Cryptographic algorithms** are divided further into symmetric ciphers, asymmetric ciphers, and hash algorithms. **Symmetric ciphers** use the same secret key for both encoding and decoding, necessitating that the two parties can securely communicate or establish a shared key. **Asymmetric ciphers** have two separate keys, one used for encryption and another for decryption, allowing the sender to encrypt information with one, usually public key, and only the holder of the other, private key can decode the message. Asymmetric ciphers are often used for key establishment for symmetric ciphers, digital identity, and digital signatures. **Cryptographic hashes** allow the creation of an impossible-to-forge fingerprint of any digital document. They are critical for protecting data integrity.

This report investigates both the threats quantum computing poses to modern mobile network security, and the opportunities quantum computing and related technologies such as quantum random number generation and quantum sensing can bring. A comprehensive analysis of the issue at hand requires an assessment of three topics, that is, quantum physics, cryptography, and mobile networks. A high-level

timeline of the parallel development in these three fields is shown in Figure 1. One key observation is that the research and development cycles are very different—early research demonstrations in quantum technologies can take decades from lab to commercial products. Conversely, cryptographic algorithms are expected to remain in use for several decades (such as AES, which was introduced in 2001 and is still in active use). While new mobile generations are introduced approximately once a decade, the long tail of earlier mobile generation equipment in operation implies the lifespan of a single "generation" is measured as several decades.

This document starts with a background description of key security mechanisms, including cryptography, available in mobile communication networks. Subsequently, both the negative and the positive impacts of quantum computing and related technologies are described in Section 3. In Section 4, the report covers the approach that the telecommunication industry, and Ericsson specifically, is taking to both mitigate and leverage quantum computing and related technologies in future mobile communication networks. In Section 5, the report provides some key public policy recommendations aimed at advising policymakers on how to uphold the common goal of safeguarding subscribers of mobile communication networks.

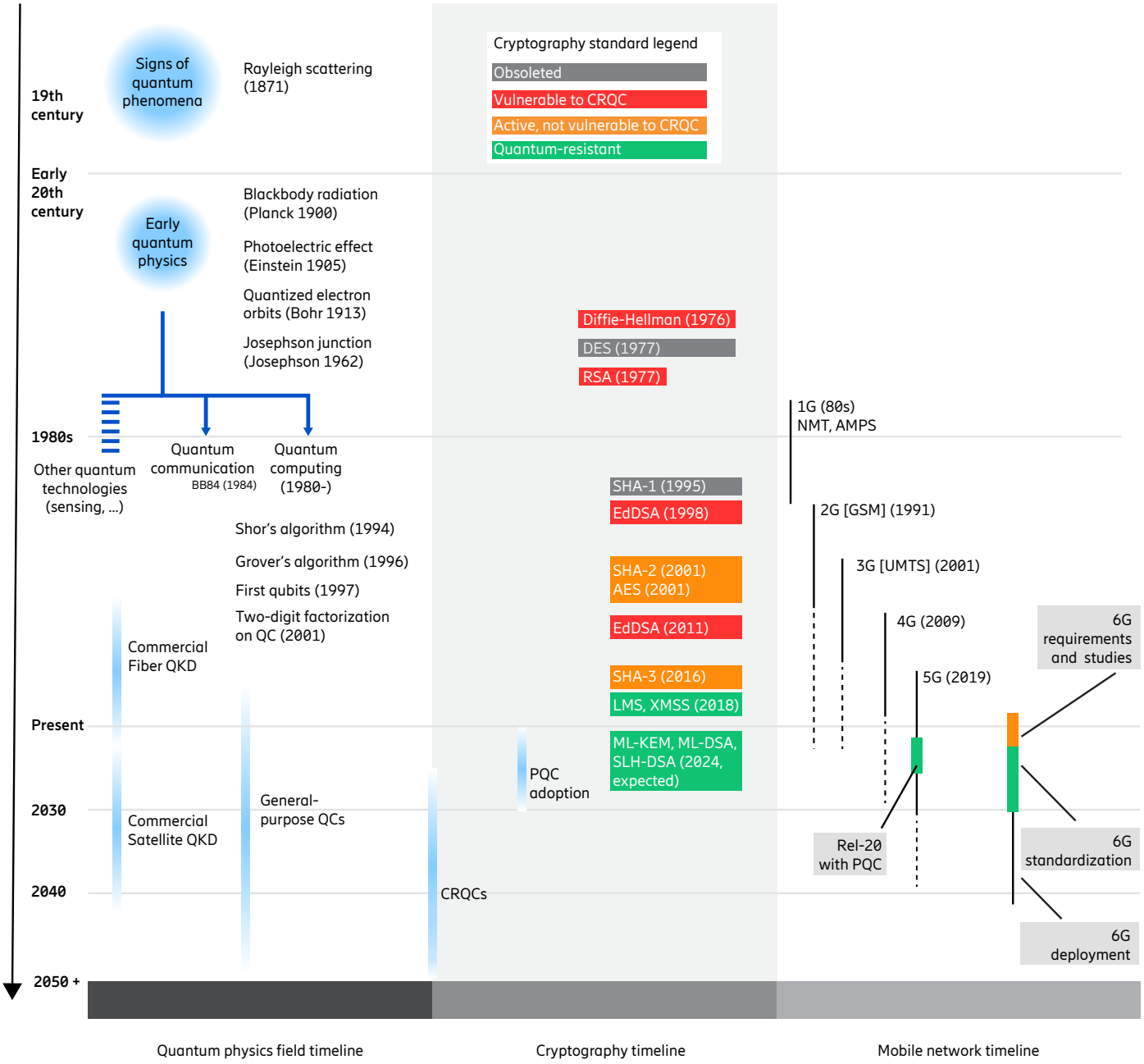


Figure 1: High-level timeline of key technological developments in quantum physics, cryptography, and mobile networks.

Mobile telecommunication networks

By the end of 2023, mobile networks were globally serving over 5.6 billion people [17], with rapid adoption of 5G at over 1.6 billion subscribers and expected mobile data traffic annual growth of over 20% [25]. Mobile networks are widely identified as critical national infrastructure necessary to ensure a functioning and prosperous society. It is almost impossible to imagine a modern society without the ubiquitous availability of voice, text, and mobile broadband access at hand, anytime, from any personal computing device, whether at home, in the office, or on the move. Mobile networks are also used widely in industry and commerce, increasingly facilitating machine-to-machine communication in warehouses, ports, and vehicle-to-vehicle communication, being open and flexible to meet all kinds of business needs.

The importance of mobile communication to end-users, economy, and society also highlights the criticality of security. The continuously evolving security landscape of mobile networks is shaped by knowledge and insights gained from the previous generations of mobile networks. This wealth of experience is passed on to the next generations and will continue to shape future security improvements in 5G and 6G.

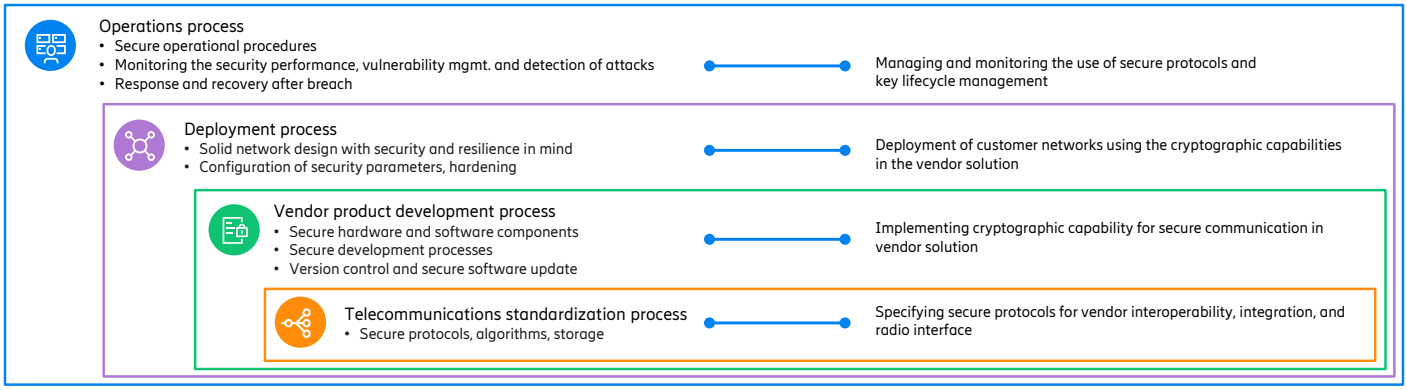
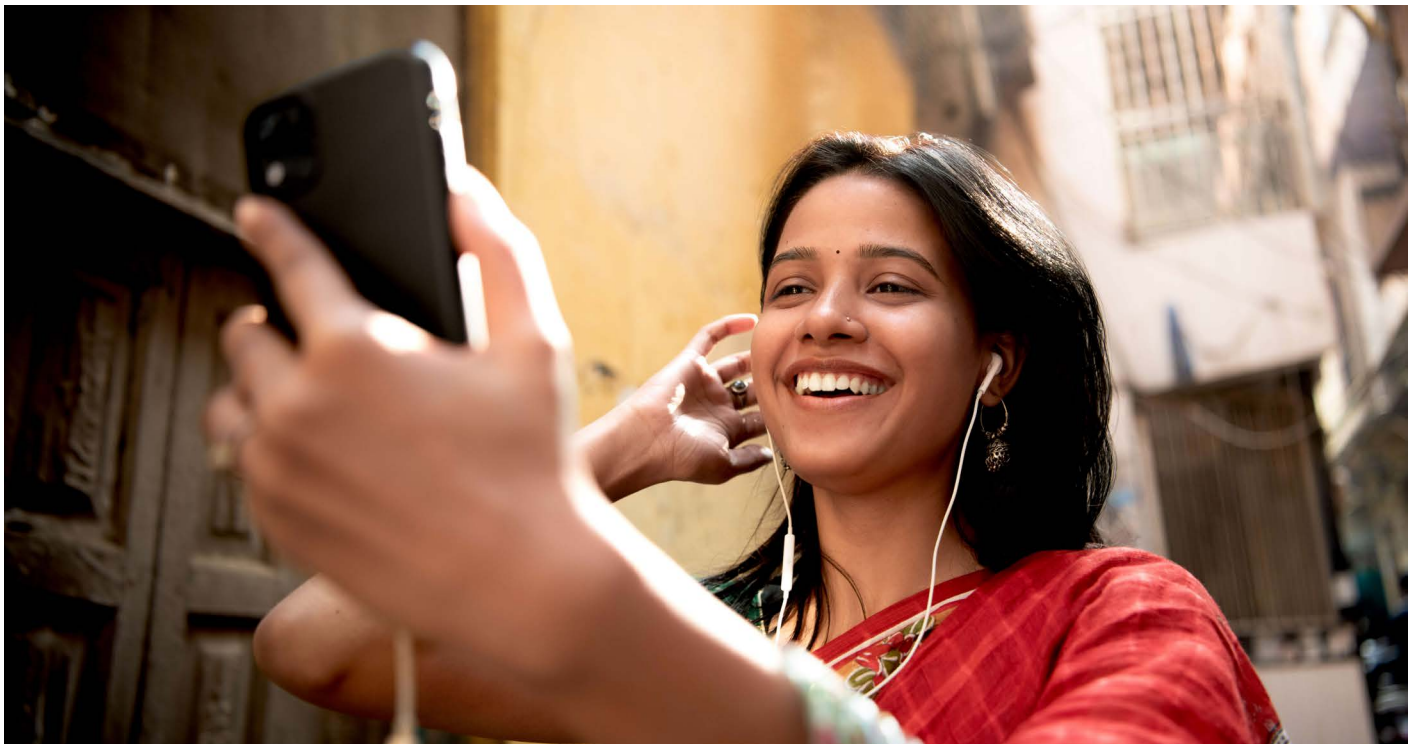


Figure 2: Holistic security approach – Ericsson trust stack, depicting the four layers of a holistic security approach on the left, and on the right, the different responsibilities and tasks related to each layer specific for cryptography



The security of deployed mobile networks is achieved through a holistic security approach across the four layers of the Ericsson trust stack, realized through collaboration between key stakeholders, including:

1. Secure operations of deployed networks to continuously monitor the security of mobile networks.
2. Deployment of network infrastructure and software, using secure processes to deploy secure configurations.
3. The development process of products and solutions by vendors, using secure processes, life-cycle management, and the use of secure standards.
4. Standardization of secure algorithms, protocols, and operational requirements in organizations such as NIST, ISO, IETF, 3GPP, and GSMA.

At the most fundamental level, all secure communication relies on maintaining the confidentiality and integrity of the identity of participants and their communication, for example, the transported data. This is accomplished using cryptographic algorithms and protocols. While the most widely used cryptographic algorithms, such as AES [38] and SHA2 [39] are defined by NIST, their development and implementation involve a global collaboration between researchers and security specialists from academia and industry, aiming to secure these standardized cryptographic algorithms. These standards are then used to develop secure network communications protocols, with the IETF being the hub for any Internet protocols including security protocols, such as IPsec [36], TLS [35], and QUIC [37]. Finally, the first and the last mile of a mobile network connection, that is, the radio interface, between the user's device and the Radio Access Network (RAN), is protected by security methods defined by 3GPP. These methods are designed to ensure the confidentiality and integrity of communications. In addition, many bodies such as the O-RAN Alliance, GSMA, ETSI, IEEE, and ISO/IEC among others define standards that impact the security of the design, development, deployment, and operation of a mobile network.

The multi-dimensional and operational nature of the mobile network from its inception to operation is schematically described in Figure 3, which provides an overview of the components of a modern 5G network, and how they communicate with the subscriber's mobile phone. The diagram describes how each communication leg is secured and which standardization bodies define the relevant secure communications standards. Practically all communication in a mobile network is secured whether over an open radio interface, between locations, or within a deployment, following zero trust principles [30] of protecting and authenticating all connections. The network is thus able to protect individual subscribers from traffic inspection and exploitation, protect sensitive customer data, and provide connectivity to individual applications and services – which often also employ their end-to-end protection mechanisms (blue line from device to service). Figure 3 also depicts key standard and technical bodies such as 3GPP, IETF, and O-RAN Alliance contributions or use of cryptographic standards used in an end-to-end mobile system.

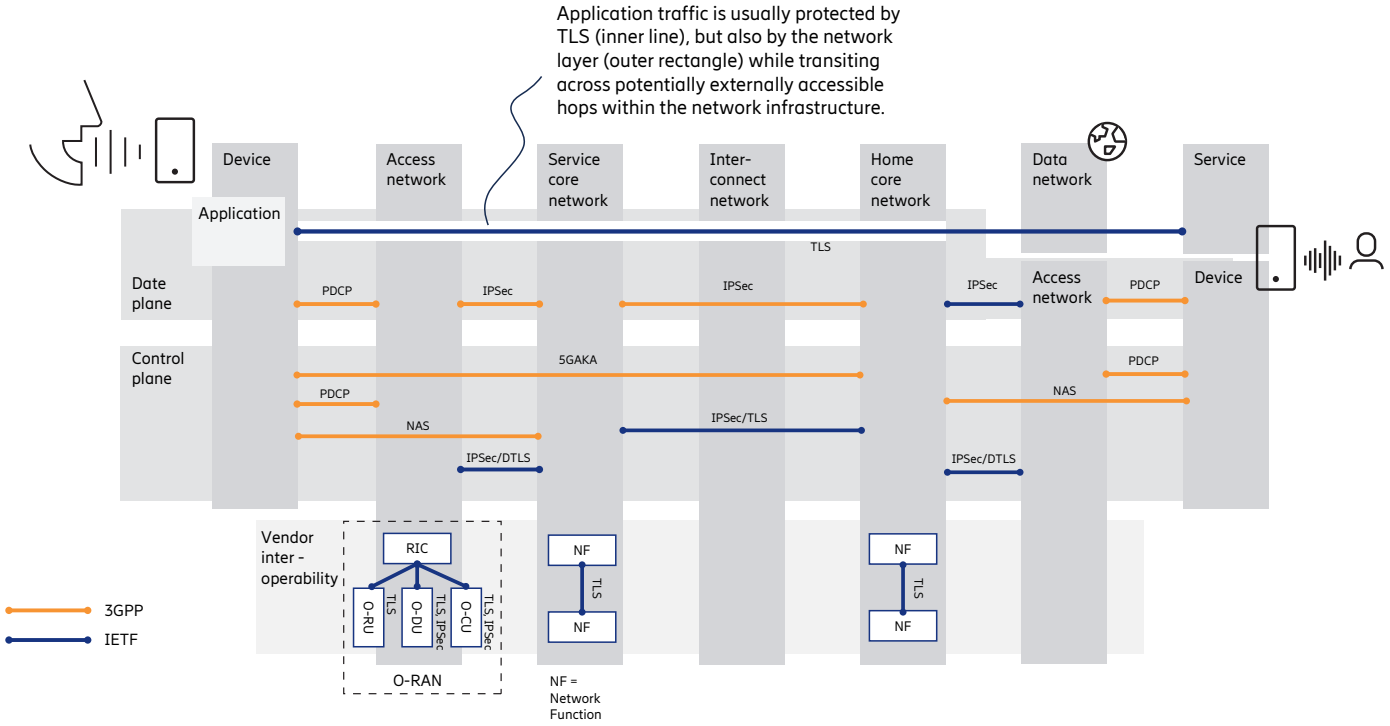


Figure 3: Schematic overview of end-to-end communication over a mobile network and the breadth of protocols employing cryptography for confidentiality and integrity protection. The figure also shows the organizations responsible for specifying the secure communication protocol.

Quantum threats and opportunities

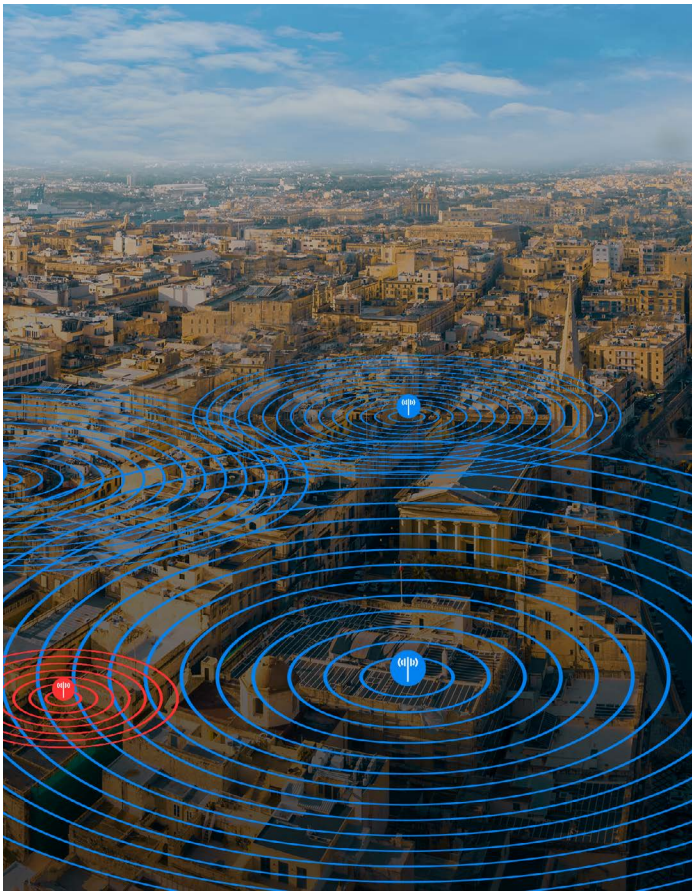
While quantum computers do not pose an immediate threat to mobile network security [31][41], the uncertainty relating to them being physically realized at sufficient capacity requires action now through the development of quantum-resistant aka post-quantum algorithms. In contrast, quantum phenomena can also be used to improve communication security from both technological and operational viewpoints, for example, by using quantum key distribution, quantum randomness, quantum sensing, and of course, quantum computers.

Quantum impact on secure communication

Why quantum computers pose a threat

Quantum computers can solve several types of computational problems faster than classical computers. While research is still ongoing to find the extent of problems uniquely suitable for quantum computers, several algorithms have already been identified which are believed to provide superior performance compared to algorithms on classical computers. Notably, Shor's algorithm puts any cryptosystem relying on discrete logarithms or integer factorization at risk. This means that it has the potential to compromise the most popular public key cryptographic systems such as RSA, elliptic curve cryptography (ECC), and any variant of the Diffie-Hellman key exchange protocol. When this is possible the industry and policymakers would face a massive problem in securing communications and identities, for example, public key cryptography, which is essential for authentication. To prevent such a situation and ensure a prompt and effective solution, cryptographic algorithms that can withstand quantum computers are currently being standardized. This is often referred to as post-quantum cryptography (PQC).

A lesser threat from quantum computing is Grover's algorithm, which is often cited as causing a halving of the security of symmetric cryptosystems such as AES. However, as Grover's algorithm cannot be run in parallel on multiple quantum computers, it does not provide any significant improvement in speed over classical computers. In any case, unlike the need to develop quantum-resistant algorithms for public key cryptography, existing algorithms, and their key lengths are not considered to be significantly affected [21] by quantum computers, implying that no major modifications are needed for software and hardware implementations of symmetric cryptography algorithms.



The threat of quantum computers varies drastically based on how the cryptographic algorithms are used, and how flexible the implementation is for updates. To protect data in transit over the Internet, there is a notable concern over the possibility of "store now, decrypt later" scenarios. This is a concern, particularly for data that must remain secret for decades and must be thus protected against even hypothetical future threats, thus necessitating a more rapid adoption of quantum-resistant methods. This "store now, decrypt later" threat is often cited as a reason for speeding up the deployment of quantum-resistant encryption. However, this threat is not unique to quantum technology and applies to any possible technology or method that can break prevailing security technologies and hence drives the logic to always act on the next potential technology development irrespective of its maturity including the maturity of counter solutions.

Given that the majority of Internet services security can be adjusted quite rapidly through software updates, countermeasures such as quantum-resistant public algorithms can be deployed promptly as they become available. In contrast, the development cycles are particularly slow for security systems embedded in hardware, which, for example, are used to secure firmware updates. Therefore, hardware security will need years or even decades of planning and gradual replacement of non-upgradeable field service units.

When will the threat become real?

The capability of a quantum computer can be measured as the number of quantum bits, or qubits, it can operate on, and their reliability over multiple computational steps. The quantum computers constructed so far have a limited number of qubits and a high error rate. Research and development over the last decades have steadily improved both measures, as is shown in Figure 4.

Since quantum computers will become industrially useful well before being a threat to cryptography, it is worthwhile to distinguish general-purpose quantum computers from cryptographically relevant quantum computers, or CRQCs, that are expected to specifically threaten existing cryptographic algorithms as described earlier. Fortunately for security professionals, while some form of useful quantum computers is expected to emerge within the next decade, the estimates given by experts on CRQC emergence are even further away and these estimates vary much more widely [16]. As shown in Figure 4, requirements for a CRQC are known with a gap between the current quantum computers and the technology readiness necessary for CRQC. The number of qubits and their error rate to break RSA from 1024 bits to 16,384 bits is shown in the top-right area of the diagram, whereas the current quantum computers are in the left bottom corner. While the gap appears big, the prevailing view is to expect continued improvements in quantum computers with the uncertainty in the speed of that development, not on whether it will occur at all.

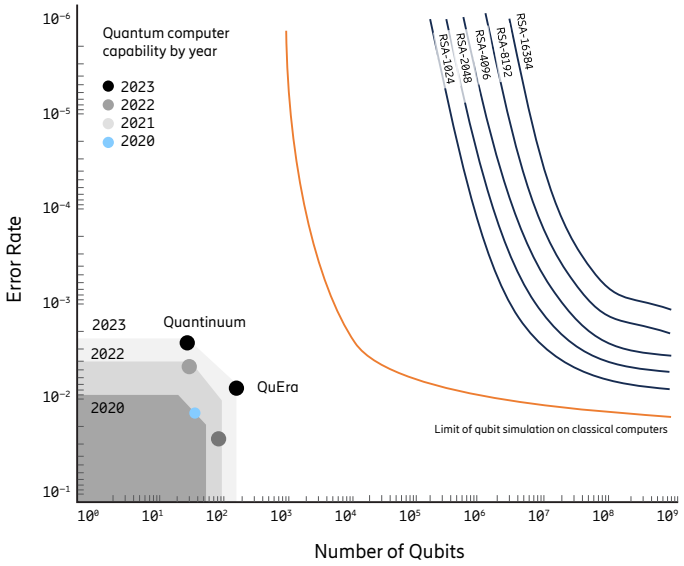
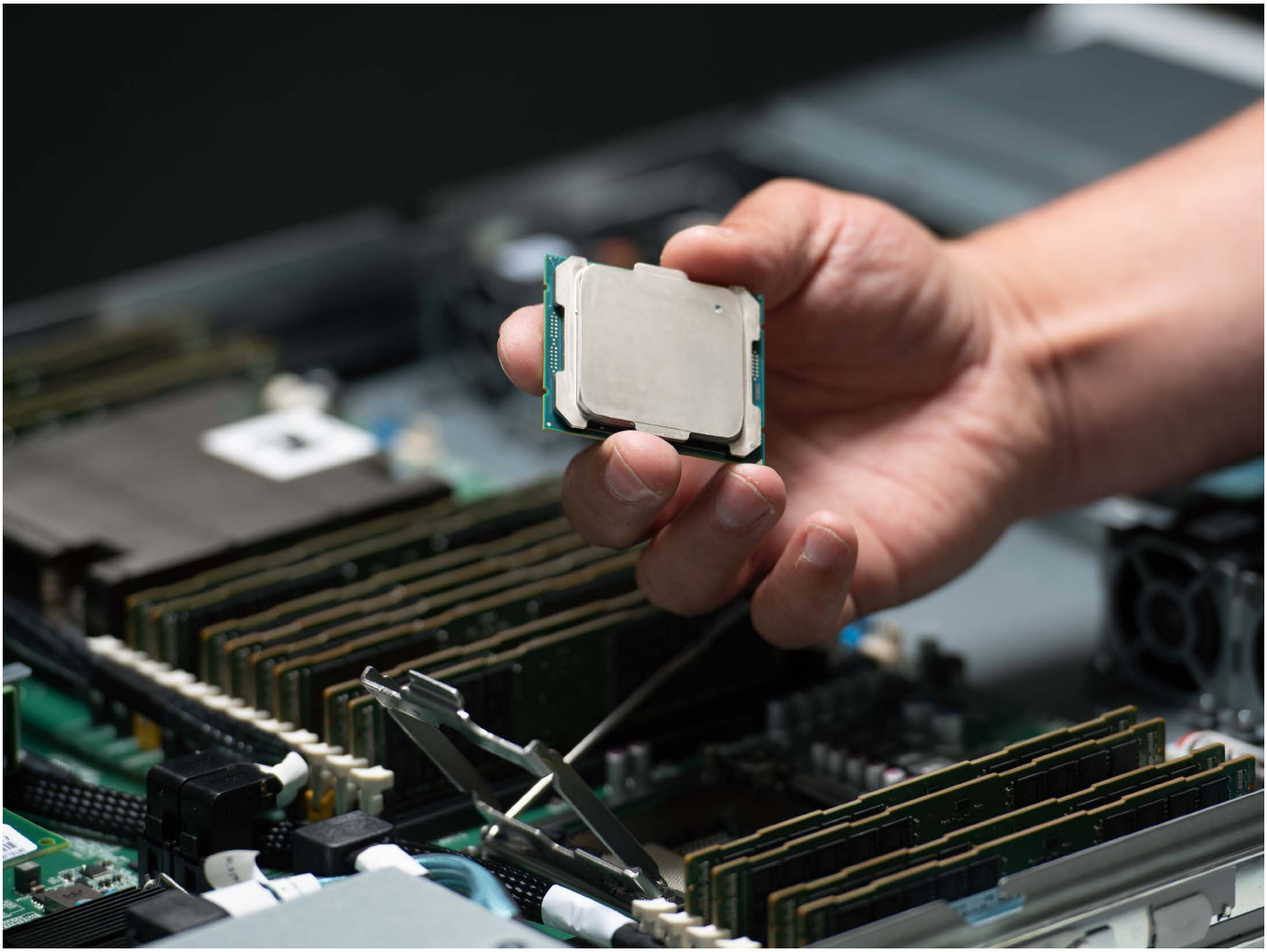


Figure 4: Development of quantum computers by the number of qubits and their error rate. The diagram shows approximately the capability boundary progression in the last four years. The top-right area of the diagram shows the required quantum computer capability to break RSA-1024 to RSA-16386 keys. The orange line demonstrates that current quantum computers can be simulated with classical computers. (Modified from [40], any mistakes on our part are ours alone.)

PQC as remediation

Quantum-resistant cryptography, also referred to as Post-Quantum Cryptography (PQC), is implemented for classical computers, which is also designed to resist attacks by a CRQC, based on what we currently understand about quantum computing algorithms and their limitations. PQC algorithms are also suitable for all possible implementations including, software-only, hardware-assisted, and hardware-based.

In 2017, NIST initiated a process to design new public key cryptographic algorithms that could resist any known attacks on both quantum and classical computations. Earlier work initiated by IRTF resulted in the parallel specification of two hash-based schemes (XMSS and LMS) resistant to quantum attacks as described in NIST 800-208 [26]. While XMSS and



LMS are applicable for certain scenarios such as code signing [42], especially when urgency arises, their use outside these narrowly defined niches has not been generally supported. Hence, the business and industry community awaits the planned 2024 standardization of the following three candidates selected in 2023: ML-KEM [27], ML-DSA [28], and SLH-DSA [29].

In parallel to the standardization effort, organizations such as IETF have been updating cryptographic protocols such as TLS and IPSec to support the upcoming quantum-resistant algorithms, implementing cryptographic software libraries and future-proofing hardware implementations. Many applications, such as Internet browsers, already have either planned, hidden, or open support to draft versions of PQC algorithms and are expected to rapidly conform to finalized standards.

Quantum communication

Quantum communications as opposed to quantum computing, is a field of quantum physics that studies the transmission of quantum states or information along two (or more) parties. Its objectives include distributing random bits, sharing entangled resources or information, or other tasks allowed by quantum mechanics, with the ultimate aim of creating quantum communication links and nodes to build the so-called quantum Internet. Currently, the most relevant application of quantum communication is quantum key distribution (QKD). This mechanism entails establishing a confidential cryptographic key that is shared between two parties, as outlined below.

Quantum key distribution

The security of QKD relies on the physical restrictions of quantum state measurement, ensuring that on a theoretical level, QKD is secure against any form of eavesdropping. The key distribution process begins with Alice generating a random sequence of quantum states in orthogonal polarization or spin states, also known as the basis, which she sends over the public channel to Bob. Bob measures each received quantum state on a randomly chosen basis. Alice and Bob communicate their chosen bases only after the measurements have been completed. This process is repeated several times, and Alice and Bob compare a subset of their measurements to detect any errors that might have been introduced by noise or eavesdropping. This allows them

to agree on specific bits to use for a shared secret. The shared secret is then used by other security protocols such as TLS to secure messages using symmetric cryptography sent over a classical channel.

As QKD relies on physical phenomena, it can only be realized in physical hardware. The intrinsic physical nature of QKD also determines its current reach, such as the distance between two parties and the means of communication. Current QKD networks operate in point-to-point fiber or free-space links. Commercial point-to-point systems currently reach fiber link distances up to 150 to 200 km, with active research on extending the distance [1][2][3][4][5]. Free-space links on the Earth's surface are limited by the curvature of the Earth, but their range can be extended by using trusted satellites [15]. Since QKD relies on measurements of single (or few) quantum states, it suffers from noise especially over long distances, limiting the rate at which the two communicating parties can establish new key material, often down to kbit/s rates. Thus, while QKD can provide information-theoretical security using one time pad (OTP) encryption, the limited key bit rate practically mandates the use of symmetric cryptography (for example, AES), limiting the actual communication security to what is offered by the symmetric algorithm's computational complexity guarantees [6][7][11].

On a functional model level, QKD offers key agreement services, but not authentication or message confidentiality; for these services, we need to rely on traditional cryptography for traditional compute models. In other words, QKD can complement a traditional cryptographic system and its setup relies on pre-established authenticated communications channels. However, the existence of such an authenticated channel, presupposes that communicating parties either have managed to privately exchange a symmetric key in the past (for example, by physically meeting) or are using classical or quantum-resistant public key cryptography [11]. Physical distribution of keys is feasible for a small number of communicating parties but does not scale to thousands or millions of devices, necessitating the use of quantum-resistant public key infrastructure (PKI) for QKD device authentication at scale. Also, since QKD must be physically realized, the security of QKD key agreement protocol depends on the physical security of the devices, necessitating their protection against passive and invasive physical attacks, verified through procedures of certification of security technologies [12][13][14].

ITU-T, ETSI, and CEN/CENELEC have been active in defining the QKD conceptual framework and operational requirements, including interoperable interfaces for using QKD devices [19], with further standardization including specifications for physical parameters ongoing or planned [20]. Research on QKD is progressing strongly, with the potential to provide significant improvements in the future by combining PQC and QKD [23], extending the reach of QKD with twin-field approaches [22] and the development of quantum memories and repeaters [24].

Quantum randomness

While cryptography is (universally) fully deterministic, good cryptography requires a non-deterministic input in the form of unpredictable, that is, random keys. Conversely, the use of insufficient randomness is a common and often exploited vulnerability [9]. Thus, the quality of random number or bit generation is of utmost importance to communications security.

The practical generation of random numbers relies either on deterministic processes implemented either in software or hardware (pseudorandom number generation, PRNG) or on hardware capable of tapping into non-deterministic sources of randomness (true random number generation, TRNG). While PRNGs are deterministic, they can still be highly unpredictable when seeded by externally random events, such as human interaction, or a low-bitrate TRNG. In contrast, TRNGs are based on sampling a random event such as Zener noise, radioactive decay, or photon path splitting. TRNGs have been widely available for decades as discrete elements and are present in practically all modern CPUs with security subsystems.

The importance of true random numbers is highlighted by examples of using machine learning to attack some types of PRNGs with high success rates [10], highlighting the importance of high-quality cryptographic PRNGs. Similarly, numerous hardware-based sources of randomness that are presently in use rely on a chaotic process to generate randomness and can exhibit biases in their output when the initial conditions are known. Therefore, further development of hardware random number generation is looking to exploit quantum effects directly, labeled as quantum random number generation (QRNG). However, quantum computing does not pose known threats to (well-seeded cryptographic) PRNGs or currently deployed TRNGs. Thus, while QRNGs will improve the fundamental quality of random bit generation, they are more of an incremental change than a technological revolution.

Pathway to quantum-safe encryption for mobile telecommunications networks

Ericsson, a leading mobile network technology supplier, is committed to ensuring the security of its products and solutions by addressing the threat posed by CRQCs. Ericsson is active and collaborating with the relevant standardization and industry bodies, which are developing technologies and guidelines to utilize quantum computing, quantum communication, and development of quantum-resistant cryptography, including contributions to NIST PQC standards, IETF, 3GPP, GSMA Post Quantum Task Network, CISA/DHS, ATIS, and many more.

Ericsson's, and the telecommunication industry's approach, at large, is to use solutions that are widely used and proven to work at scale and are built on open and public standards and specifications. The consumers and businesses relying on mobile networks, in addition to confidentiality and integrity of communication also expect superior service continuity and interoperability with a wide range of mobile devices, chipsets, industrial solutions, and so on.

In the next 5 to 10 years, Ericsson believes, in consensus with a significant share of 3GPP members, the most effective and efficient approach to mitigate CRQC threat is through the use of quantum-resistant cryptography, for example, PQC. This is also the approach recommended by multiple national cybersecurity agencies in France, Germany, Netherlands, Sweden [7], the United Kingdom [32] and USA [31]. In addition, the European Commission, concluded in a whitepaper: "the Post-Quantum Cryptography (PQC) is a promising approach to make our communications and data resistant to quantum attacks, as it is based on mathematical problems hard to solve even by quantum computers. As a software-based solution, for which new dedicated hardware is not necessary, PQC allows for a swift transition to higher protection levels." [34]

The PQC approach includes incorporating quantum-resistant algorithms and network protocols primarily specified by NIST and IETF into 3GPP specifications as well as updating the protocols specific to mobile networks such as subscriber identity concealment with 5G-AKA. The technical standardization work in 3GPP will include the NIST-approved quantum-resistant algorithms as an update to 5G and from the outset for 6G once they become available. Ericsson is expecting mobile network solutions to support the use of quantum-resistant cryptography shortly after standardization. The objective is to work closely with mobile phone manufacturers, Internet service providers, and other technology ecosystem members, to enable secure, quantum-resistant communication from one mobile device to another, or a particular service, within a specific timeframe. Given the current uncertainties regarding CRQC development, speed of PQC migration on operational 5G networks, and time taken for the phase-out of older technologies, it is currently premature to make predictions about the need for PQC upgrades to 4G networks (see also Figure 1).
Beyond that, quantum-resistant encryption, quantum computing, and sensing can benefit mobile networks by optimizing resource allocation, reducing energy use and environmental footprint, and also in security. For instance, the use of quantum AI can improve both reactive and proactive operational security measures to defend and protect deployed mobile networks (see Figure 2 on the left, the top layer). The implementation of QRNGs can also be realized through integration into major chip designs. QKD can be used, at least initially, to increase the security of critical service provider backbone networks, with wider adoption expected once cost-effective, scalable, and dependable QKD solutions are available for mobile telecommunication networks.

Policy recommendations

Ericsson recommends a holistic approach to security. Ensuring the security of deployed mobile networks requires a cooperative approach across all the organizations involved in standardizing, developing, implementing, and operating them. The primary policy goal is to continue to ensure the security of the users of mobile networks.

A holistic security approach based on the Ericsson trust stack, also recognized in OECD Digital Economy papers [33], is a necessary foundation for a robust public security policy. This approach ensures comprehensive security considerations within and between each layer of the Ericsson trust stack (see Figure 2).

Confidentiality of communication and the integrity of end-users is one of several key considerations for industry and policymakers. This consideration is addressed in the context of the current encryption solutions as well as in the future, to ensure effective, scalable, interoperable, and timely available quantum-resistant cryptography.

Ericsson, the mobile industry at large, and cybersecurity agencies from France, Germany, Netherlands, Sweden, United Kingdom, USA, and the European Commission, believe that the most effective and efficient approach to mitigating confidentially and integrity threats from CRQC is using PQC.

It is crucial to establish a broad international policy consensus on the path toward quantum-resistant cryptography. This will not only ensure the security of mobile communication systems but also cost-effective, interoperable, and timely realization at a large scale.

To further the development toward a timely realization of quantum-resistant cryptography, standardization work is already ongoing in relevant standardization and industry bodies, which are developing technologies and guidelines to utilize quantum computing, quantum communication, and the development of quantum-resistant cryptography, including contributions to NIST PQC standards, IETF, 3GPP, GSMA Post Quantum Task Network, CISA/DHS, and ATIS.

To ensure international policy consensus on PQC, Ericsson encourages timely and increased intergovernmental and international policy coordination in relevant forums and formats. This will allow the industry to realize secure, internationally harmonized, and interoperable PQC solutions on a global scale.

ITU-T, ETSI, and CEN/CENELEC have been active in defining the QKD conceptual framework and operational requirements, including interoperable interfaces for using QKD devices, with further standardization including specifications for physical parameters ongoing or planned.

Furthermore, policymakers should also stimulate more research into quantum computing, cryptographically relevant quantum computers (CRQC), and quantum communication including quantum key distribution (QKD) networks. Quantum computing and sensing will also benefit mobile networks by optimizing resource allocation, reducing energy use and environmental footprint, and boosting security measures. Encouraging additional research to further the development of quantum random number generation should also be advocated.

A synergistic partnership between government and industry is the best way forward to realize quantum-resistant cryptography thereby ensuring the security of subscribers and the resilience of mobile networks.

References

1. Braun, R.P.; Geitz, M. The OpenQKD Testbed in Berlin. In Proceedings of the 2021 Asia Communications and Photonics Conference (ACP), Shanghai, China, 24–27 October 2021; pp. 1–3.
2. Rydlichkowski, P. OPENQKD project Work Package 7 review. In Proceedings of the QKD Days, Madrid, Spanish, 13 December 2022.
3. Martin, V.; Brito, J.P.; Ortíz, L.; Brito-Méndez, R.; Sáez-Buruaga, J.; Vicente, R.; Sebastián-Lombraña, A.; Rincón, D.; Pérez, F.; Sánchez, C.; et al. MadQCI: A Heterogeneous and Scalable SDN QKD Network Deployed in Production Facilities. 2023. https://arxiv.org/abs/2311.12791v2
4. Aguado, A.; Lopez, V.; Lopez, D.; Peev, M.; Poppe, A.; Pastor, A.; Folgueira, J.; Martin, V. The Engineering of Software-Defined Quantum Key Distribution Networks. IEEE Commun. Mag. 2019, 57, 20–26.
5. Qi, W. Overview of Quantum Communication Industry Development in China. In proceedings of the ETSI QSC Workshop 2023. 2023. https://docbox.etsi.org/Workshop/2023/02_QUANTUMSAFECRYPTOGRAPHY/TECHNICALTRACK/WORLDTOUR/CASQUANTUMNETWORK_QI.pdf
6. Mohammad, O.K.J.; Abbas, S.; El-Horbaty, E.-S.M.; Salem, A.-B.M. Advanced encryption standard development-based quantum key distribution. In Proceedings of the 9th International Conference for Internet Technology and Secured Transactions, London, UK, 8–10 December 2014.
7. French Cybersecurity Agency (ANSSI); Federal Office for Information Security (BSI); Netherlands National Communications Security Agency (NLNCSA); Swedish National Communications Security, Swedish Armed Forces, Position Paper on Quantum Key Distribution, January 2024. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/Quantum_Positionspapier.pdf
8. Bernstein, D.J.; Hülsing, A.; Lange, T.; Rekleitis, E.; Post-Quantum Cryptography – Integration Study, October 2022, ENISA. https://www.enisa.europa.eu/publications/post-quantum-cryptography-integration-study
9. MITRE, Common Weakness Enumeration: CWE-330: Use of Insufficiently Random Values, 2006. https://cwe.mitre.org/data/definitions/330.html
10. Hassan, M., Cracking Random Number Generators using Machine Learning – Part 1: xorshift128, NCC Group Research Report, October 2021. https://research.nccgroup.com/2021/10/15/cracking-random-number-generators-using-machine-learning-part-1-xorshift128/

11. Beullens, W.; D'Anvers, J-P; Hülsing A; Lange, T.; Panny, L.; de Saint Guilhem, C.; Smart, N.P.; Rekleitis, E.; Aktypi, A.; Grammatopoulos, A-V., Post-Quantum Cryptography – Current state and quantum mitigation, May 2021, ENISA, https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation

12. ETSI Group Specification QKD-016: Common Criteria Protection Profile V1.1.1. 2023. https://www.etsi.org/deliver/etsi_gs/QKD/001_099/016/01.01.01_60/gs_QKD016v010101p.pdf

13. ISO/IEC 23837-1:2023; Information Security—Security Requirements, Test and Evaluation Methods For Quantum Key Distribution—Part 1: Requirements. International Organization for Standardization: Geneva, Switzerland. https://www.iso.org/standard/77097.html

14. ISO/IEC 23837-2:2023; Information Security—Security Requirements, Test and Evaluation Methods For Quantum Key Distribution—Part 2: Evaluation and Testing Methods. International Organization for Standardization: Geneva, Switzerland. https://www.iso.org/standard/77309.html

15. The European Quantum Communication Infrastructure (EuroQCI) Initiative, https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci

16. Mosca, M.; Piani, M., Quantum Threat Timeline Report 2022, December 2022, Global Risk Institute. https://globalriskinstitute.org/publication/2022-quantum-threat-timeline-report/

17. Joiner, J.; Okeleke, K.; Borole, S.; Ballon, H.F.A., The Mobile Economy 2024, February 2024, GSMA Intelligence. https://data.gsmaintelligence.com/research/research/research-2024/the-mobile-economy-2024

18. NIST, Post-Quantum Cryptography – Security (Evaluation Criteria), January 2017. https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization/evaluation-criteria/security-(evaluation-criteria)

19. ETSI Group Specification QKD-020: Quantum Key Distribution (QKD); Protocol and data format of REST-based Interoperable Key Management System API, Draft version 0.3.1, November 2023. https://docbox.etsi.org/ISG/QKD/70-Drafts/0020_InteropKMS/QKD-020_InteropKMSv031.zip

20. CEN/CENELEC Focus Group on Quantum Technologies (FGQT), Standardization Roadmap on Quantum Technologies, Release 1, March 2023. https://www.cencenelec.eu/media/CEN-CENELEC/AreasOfWork/CEN-CENELEC_Topics/Quantum%20technologies/Documentation%20and%20Materials/fgqt_q04_standardizationroadmapquantumtechnologies_release1.pdf

21. National Cyber Security Centre (NCSC), Next steps in preparing for post-quantum cryptography, November 2023. https://www.ncsc.gov.uk/whitepaper/next-steps-preparing-for-post-quantum-cryptography

22. Zhou, L., Lin, J., Jing, Y. et al. Twin-field quantum key distribution without optical frequency dissemination. Nat Commun 14, 928 (2023). https://www.nature.com/articles/s41467-023-36573-2

23. M. Brauer et al., Linking QKD Testbeds across Europe, Entropy 2024, 26(2), 123. https://doi.org/10.3390/e26020123

24. Gera, S., Wallace, C., Flament, M. et al. Hong-Ou-Mandel interference of single-photon-level pulses stored in independent room-temperature quantum memories. npj Quantum Inf 10, 10 (2024). https://doi.org/10.1038/s41534-024-00803-2

25. Ericsson, Ericsson Mobility Report – Business Review 2024. https://www.ericsson.com/4912e3/assets/local/reports-papers/mobility-report/documents/2024br/emr-business-review-2024.pdf

26. Cooper, D.; Apon, D.; Dang, Q.; Davidson, M.; Dworkin, M.; Miller, C., Recommendation for Stateful Hash-Based Signature Schemes, NIST SP 800-208, 2020. https://csrc.nist.gov/pubs/sp/800/208/final

27. National Institute of Standards and Technology (2023) Module-Lattice-based Key Encapsulation Mechanism Standard. (Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) NIST FIPS 203 ipd. https://doi.org/10.6028/NIST.FIPS.203.ipd

28. National Institute of Standards and Technology (2023) Module-Lattice-Based Digital Signature Standard. (Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) NIST FIPS 204 ipd. https://doi.org/10.6028/NIST.FIPS.204.ipd

29. National Institute of Standards and Technology (2023) Stateless Hash-Based Digital Signature Standard. (Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) NIST FIPS 205 ipd. https://doi.org/10.6028/NIST.FIPS.205.ipd

30. Rose, S.; Borchert, O.; Mitchell, S.; Connelly, S., Zero Trust Architecture, NIST SP 800-207, 2020. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

31. National Security Agency (NSA), Quantum Key Distribution (QKD) and Quantum Cryptography (QC), 2021. https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/

32. National Cyber Security Centre (NCSC), Quantum security technologies, March 2020. https://www.ncsc.gov.uk/whitepaper/quantum-security-technologies

33. OECD, Enhancing the security of communication infrastructure, OECD Digital Economy Papers, September 2023. https://doi.org/10.1787/20716826

34. European Commission (EC), How to master Europe's digital infrastructure needs?, White Paper, February 2024. https://digital-strategy.ec.europa.eu/en/library/white-paper-how-master-europes-digital-infrastructure-needs

35. Rescorla, E., The Transport Layer Security (TLS) Protocol Version 1.3, no. 8446. RFC Editor, Aug-2018. https://datatracker.ietf.org/doc/html/rfc8446

36. Seo, K.; Kent, S., Security Architecture for the Internet Protocol, no. 4301. RFC Editor, Dec-2005. https://datatracker.ietf.org/doc/html/rfc4301

37. Iyengar, J.; Thomson, M., QUIC: A UDP-Based Multiplexed and Secure Transport, no. 9000. RFC Editor, May-2021. https://datatracker.ietf.org/doc/html/rfc9000

38. NIST, Advanced Encryption Standard (AES). NIST FIPS 197-upd1, updated May 9, 2023. https://doi.org/10.6028/NIST.FIPS.197-upd1

39. NIST, Secure Hash Standards (SHS). NIST FIPS 180-4, August 2015. http://dx.doi.org/10.6028/NIST.FIPS.180-4

40. Jaques, S., Landscape of Quantum Computing in 2023, Blog Post, 2023. https://sam-jaques.appspot.com/quantum_landscape_2023

41. CISA, Quantum-readiness: Migration to Post-Quantum Cryptography, 2023. https://www.cisa.gov/sites/default/files/2023-08/Quantum%20Readiness_Final_CLEAR_508c%20%283%29.pdf

42. National Security Agency (NSA), Announcing the Commercial National Security Algorithm Suite (CNSA) 2.0, September 2022. https://media.defense.gov/2022/Sep/07/2003071834/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS_.PDF

Glossary

3GPP	Third Generation Partnership Project
5G	5th generation of mobile network standards
5G-AKA	5G Authentication and Key Agreement
6G	6th generation of mobile network standards, upcoming
AES	Advanced Encryption Standard
ATIS	Alliance for Telecommunications Industry Solutions
CEN	The European Committee for Standardization
CENELEC	The European Electrotechnical Committee for Standardization
CISA	Cybersecurity and Infrastructure Security Agency
CRQC	Cryptographically Relevant Quantum Computer
DHS	Department of Homeland Security
ECC	Elliptic-curve cryptography
GSMA	Global System for Mobile Communications
ICT	Information and communication technology
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IPSec	Internet Protocol Security
IRTF	Internet Research Task Force
ISO	International Organization for Standardization
IEC	International Electrotechnical Commission
ITU-T	The International Telecommunication Union
LMS	Leighton–Micali Signatures, a quantum-resistant asymmetric cryptographic algorithm
NIST	National Institute of Standards and Technology
O-RAN	Open Radio Access Network
OTP	One Time Pad
PQC	Post Quantum Cryptography
PRNG	Pseudorandom number generator
QKD	Quantum key distribution
QRNG	Quantum random number generation
RSA	Rivest-Shamir-Adleman, an asymmetric cryptography method
SHA2	Secure Hash Algorithm 2
TLS	Transport Layer Security
TRNG	True random number generator
XMSS	Extended Merkle signature scheme, a quantum-resistant asymmetric cryptographic algorithm

Ericsson enables communications service providers, enterprises and the public sector to capture the full value of connectivity. The company's portfolio spans the following business areas: Networks, Cloud Software and Services, Enterprise Wireless Solutions, Global Communications Platform, and Technologies and New Businesses. It is designed to help our customers go digital, increase efficiency and find new revenue streams. Ericsson's innovation investments have delivered the benefits of mobility and mobile broadband to billions of people globally. Ericsson stock is listed on Nasdaq Stockholm and on Nasdaq New York.

ericsson.com