Migrating Telecom to Quantum-Resistant Cryptography on a Global Scale

ERICSSON

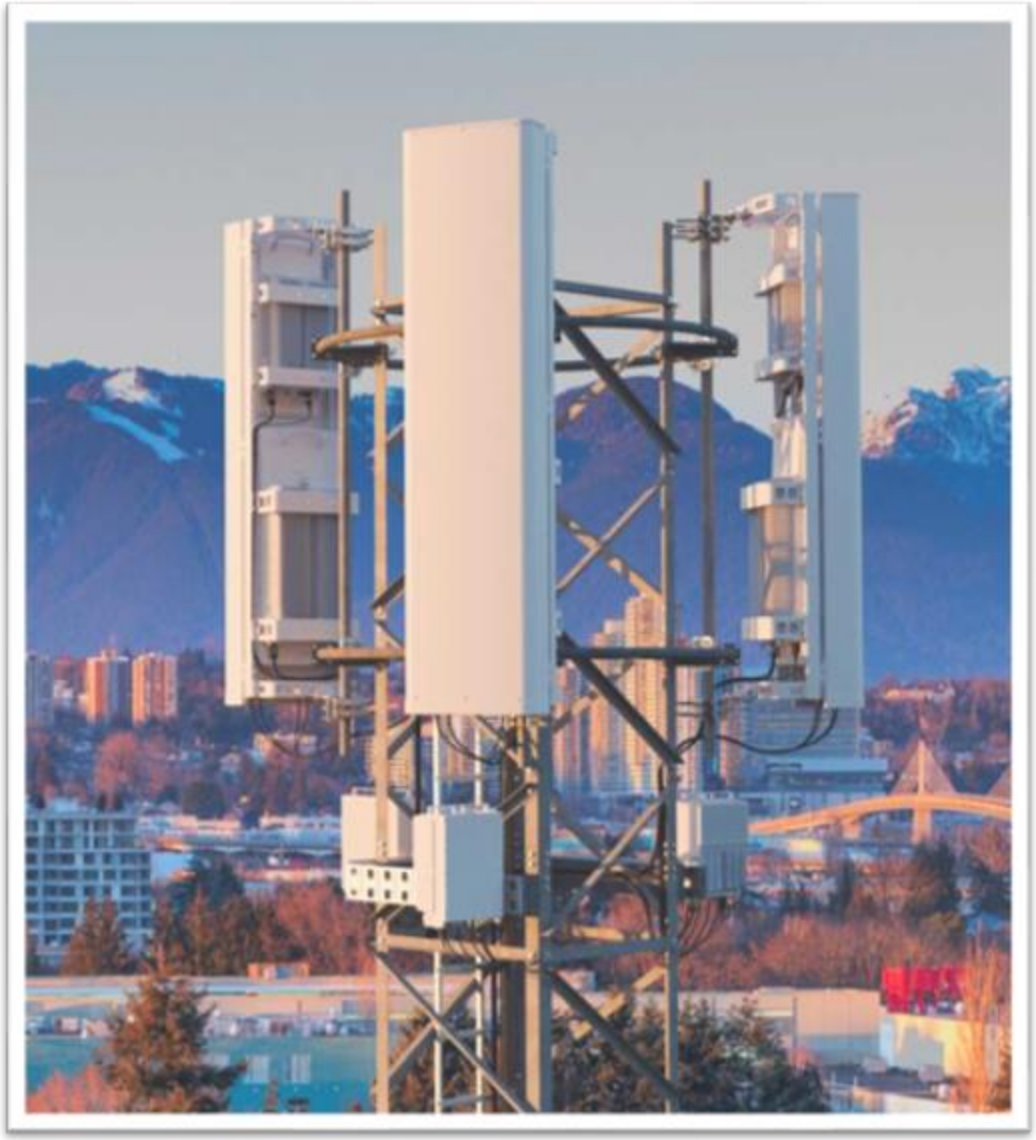
John Preuß Mattsson
Expert Cryptographic Algorithms and Security Protocols, Ericsson
MSc Engineering Physics/Theoretical Computer Science
MSc Business Administration and Economy

Sep 25, 2025

4G, 5G, and 6G – truly global standards

Characteristics of the telecom industry

- Highly regulated
- Mostly licenced spectrum
- High reliance on standardization (3GPP, ORAN, GSMA, etc.)
- **Critical infrastructure**
- **Increased use for mission critical and industry**
- **High security and privacy requirements**
- Rapid technological evolution
- High competition & consolidation
- Operators, infrastructure, smartphone, and chipset vendors

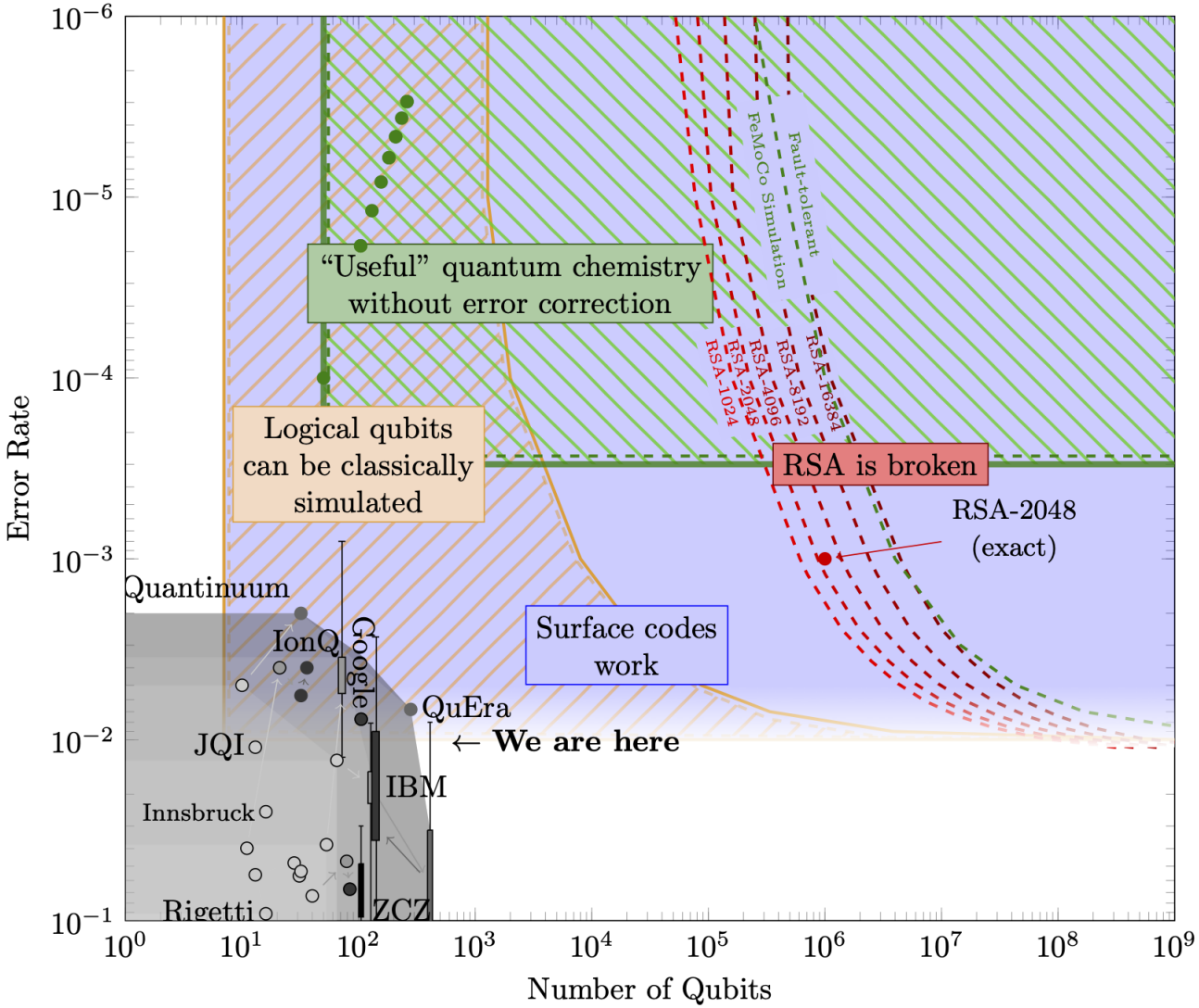


History of quantum and security

- **1978 – Code-based cryptography**
- **1979 – Hash-based cryptography**
- 1980 – Realization that a quantum computer can simulate things a classical computer cannot
- 1984 – Quantum Key Distribution (QKD)
- 1985 – Elliptic Curve Cryptography (ECC)
- 1986 – Grover's quantum algorithm—inverts any function using only $\sqrt{N}$ evaluations of the function
- 1994 – Shor's quantum algorithm – factorization and discrete logarithm in polynomial time instead of sub-exponential
- **1996 – Multivariate cryptography**
- **1998 – Lattice-based cryptography**
- 1998 – First working quantum computer with 2 physical qubits
- 2001 – First quantum key distribution network
- 2011 – Elliptic Curve Isogeny Cryptography
- **2015 – US government (NSA) announced that it is planning a transition to quantum-resistant cryptography**
- 2017 – NIST announces Post-Quantum Cryptography (PQC) standardization program
- 2018 – Standardization of stateful hash-based signatures (XMSS and LMS) by IETF and NIST
- **2022 – US government announced NSM-10 the quantum-resistant CNSA 2.0 suite required for National Security Systems**
- **2024 – NIST publishes final standards of ML-KEM, ML-DSA, and SLH-DSA**
- **2025 – CA, UK, EU timelines mandating migration to PQC for high-priority systems around 2030, and all systems 2035**
- **2025 – ML-KEM, ML-DSA, SLH-DSA mandatory upgrades for all Ericsson products. QKD forbidden to use in Ericsson products.**

Quantum impact on cryptography

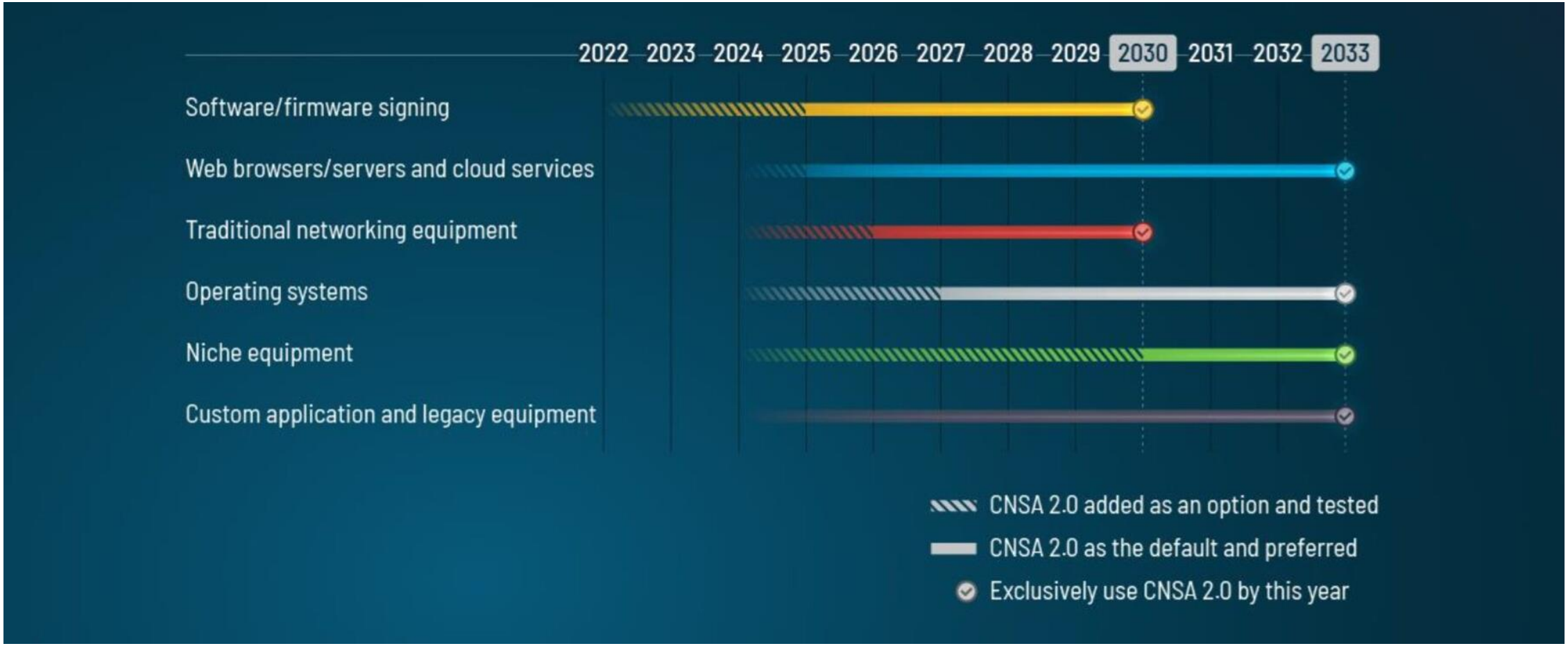
- Shor's quantum algorithm on a large and robust quantum computer would break the asymmetric crypto algorithms (RSA, ECC) we use today. Such a quantum computer is called a cryptographically relevant quantum computer (CRCQ).
- A CRCQ requires tens of millions of robust physical qubits and trillions of quantum gates. Unclear when or if CRQCs will be built. The emergence of a CRQC in the coming 10 years would be very unexpected. If the number of qubits doubles every two years, it takes 25 years.
- Not unlikely with CRCQs in 15–30 years. First CRCQs will likely be built by signal intelligence agencies using technology developed by industry.
- **IBM's roadmap for 2033+ is now 2000 qubits.**
- **Experimental breakthrough in error correction during 2024.**



Landscape of Quantum Computing in 2025 by Sam Jaques

Migration timelines for telecom

- Countries and agencies globally generally align on migration timelines.
  - Migrate as soon as possible, prioritized systems by 2030, and all systems by 2035.
  - **Requirements are for deployments, standards and implementations are required much earlier.**
  - Only use standardized PQC algorithms. QKD is not endorsed.



Migration timelines for telecom

By 2031

- Carry out your early, highest-priority PQC migration activities
- Refine your plan so that you have a thorough roadmap for completing migration

By 2035

- Complete migration to PQC of all your systems, services and products

2. By **31.12.2030**:
   - The *Next Steps* have been implemented by all Member States.
   - The PQC transition for high-risk use cases has been completed.
   - PQC transition planning and pilots for medium-risk use cases have been completed.
   - Quantum-safe software and firmware upgrades are enabled by default.
3. By **31.12.2035**:
   - The PQC transition for medium-risk use cases has been completed.
   - The PQC transition for low-risk use cases has been completed as much as feasible.

The objective in the long-term (by the 2030s) is to **complete Canada's transition to post-quantum cryptography.** The

Table 2: Quantum-vulnerable digital signature algorithms

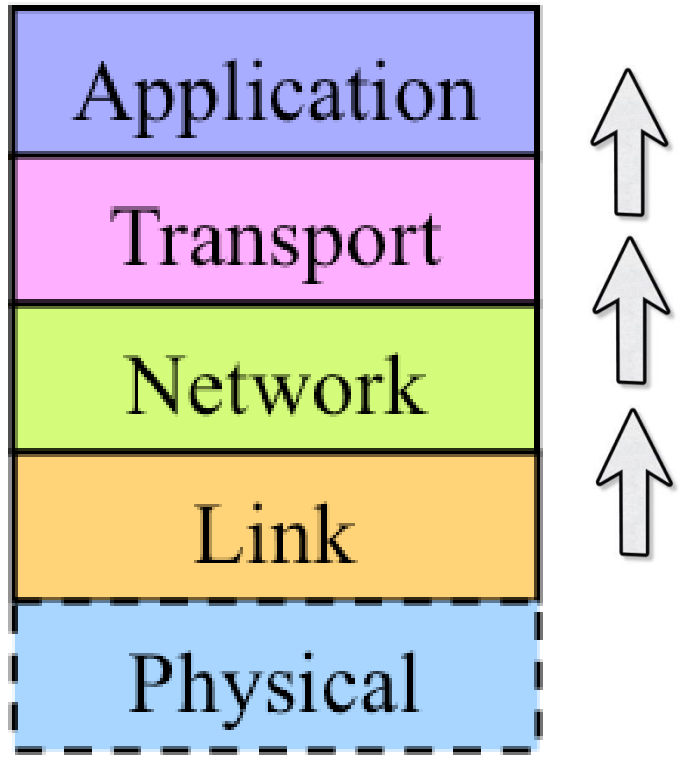
Digital Signature Algorithm Family	Parameters	Transition
ECDSA [FIPS186]	112 bits of security strength	***Deprecated*** after 2030 ***Disallowed*** after 2035
	≥ 128 bits of security strength	***Disallowed*** after 2035
EdDSA [FIPS186]	≥ 128 bits of security strength	***Disallowed*** after 2035
RSA [FIPS186]	112 bits of security strength	***Deprecated*** after 2030 ***Disallowed*** after 2035
	≥ 128 bits of security strength	***Disallowed*** after 2035

RecommandationLongTermePQ

1. Pour une utilisation de mécanismes asymétriques au-delà du 1er janvier 2030, il est recommandé d'utiliser au moins un mécanisme fondé sur un problème pour lequel aucune attaque utilisant l'algorithmique quantique n'est connue.
2. Si la fonctionnalité fournie par le mécanisme asymétrique est potentiellement vulnérable à une attaque rétroactive, il est recommandé d'utiliser au moins un mécanisme fondé sur un problème pour lequel aucune attaque utilisant l'algorithmique quantique n'est connue.

Migration to post-quantum cryptography

- What are the vulnerable algorithms RSA and ECC primarily used for?
  - Signatures/root-of-trust for soft-/firmware upgrades
  - Short-term signatures for authentication
  - Binding signatures for non-repudiation
  - Signatures/ root-of-trust in PKI
  - Public key encryption
  - Key exchange



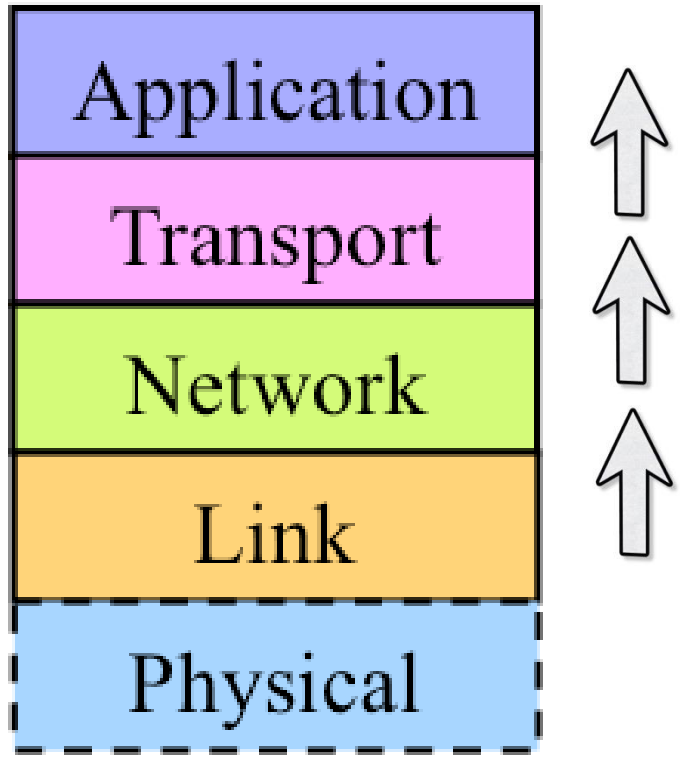
- Public-key cryptography used for protection at rest, in transit, and in use.
- Strong trend the last decades to move cryptography to higher layers to achieve end-to-end protection and cryptographic agility.
- Often protection on multiple layers.

Can quantum technologies be used for security?

- Leading security agencies assess that QKD is not mature. Long term, its only viable application is defence-in-depth for niche applications (physical-layer key exchange).
  - Not secure: availability, side-channels, hop-by-hop
  - Mentioning QKD as a practical solution is a distraction.

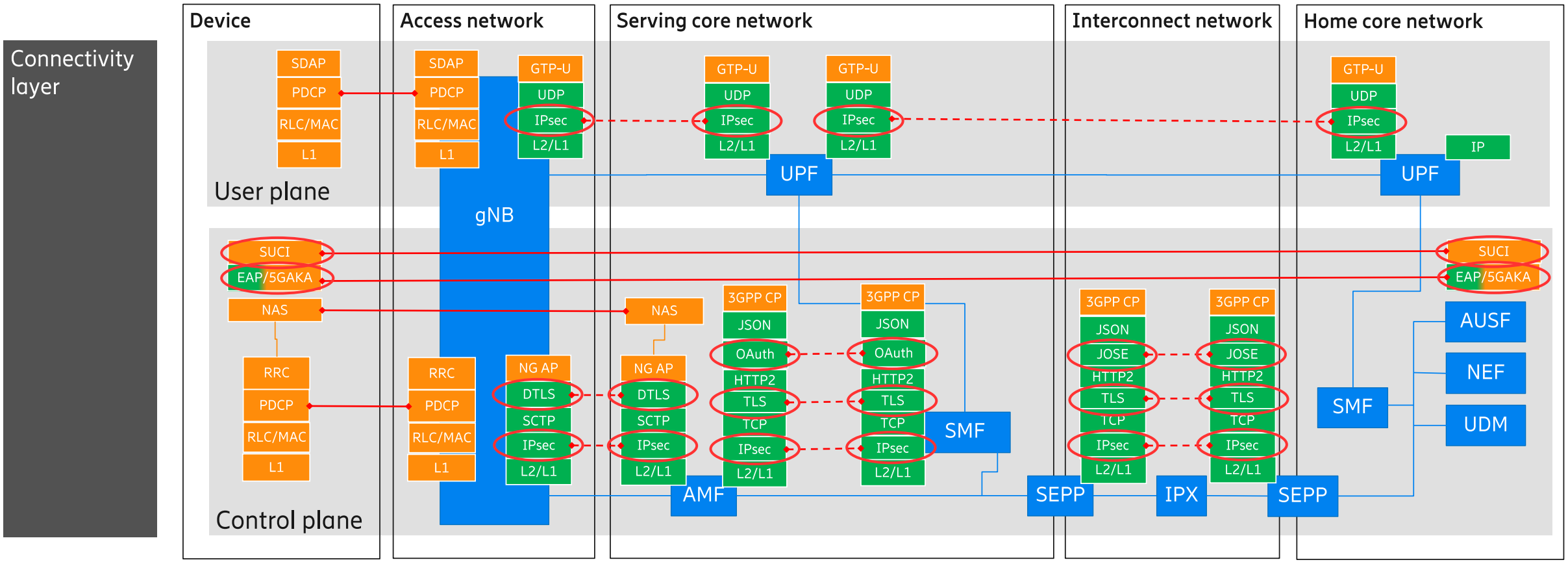
- No need to adopt QRNGs, which is still maturing technology with implementation issues. The main concerns with TRNGs are availability and trustworthiness, areas where QRNGs, to date, have exacerbate existing issues.

- Quantum sensors are extremely promising for military use!
  - Navigation with quantum inertial navigation systems
  - Submarine detection with quantum magnetometers
  - Tunnel detection with quantum gravimeters and gravity gradiometers

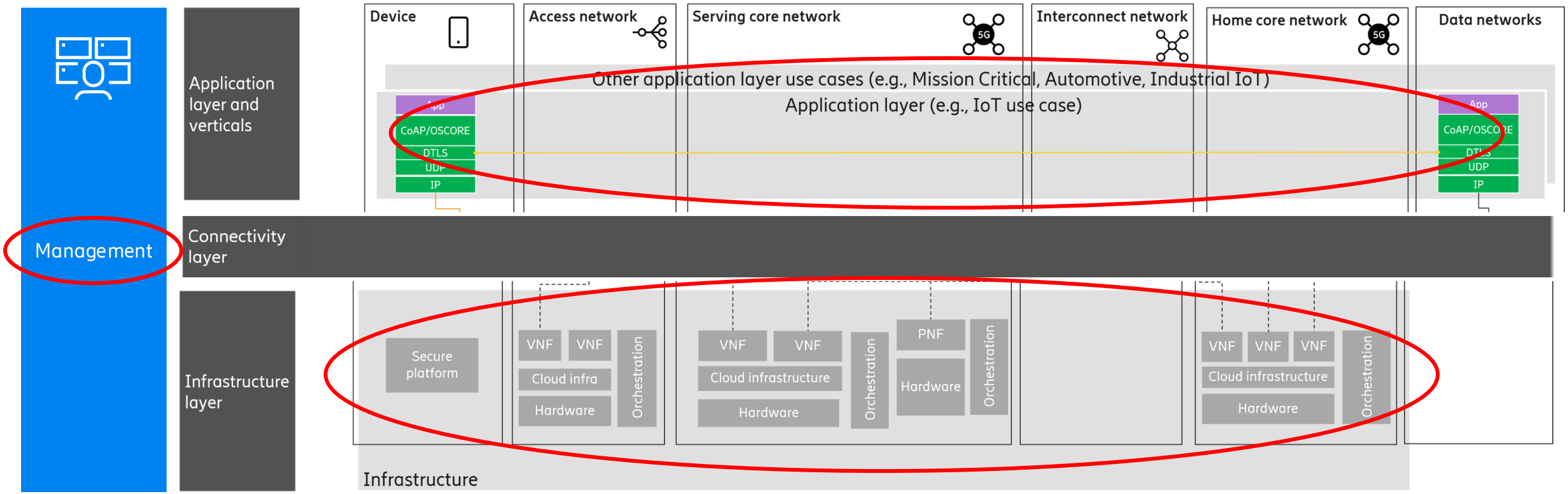


Public-key crypto in the 3GPP 5G connectivity layer

- Making something "quantum-resistant" means supporting quantum-resistant public-key algorithms instead of RSA and ECC everywhere. Can be as simple as upgrading software from OpenSSL 3.4 to 3.5.
- 5G relies on IETF protocols like IKEv2, TLS 1.3, DTLS, JOSE, Internet X.509 profile, CMP, CRL, OCSP, EAP-TLS, and EAP-AKA-FS for almost all uses of public-key cryptography.
  - IMSI encryption uses the SECG ECIES standard but augments it with X25519 (RFC 7748).



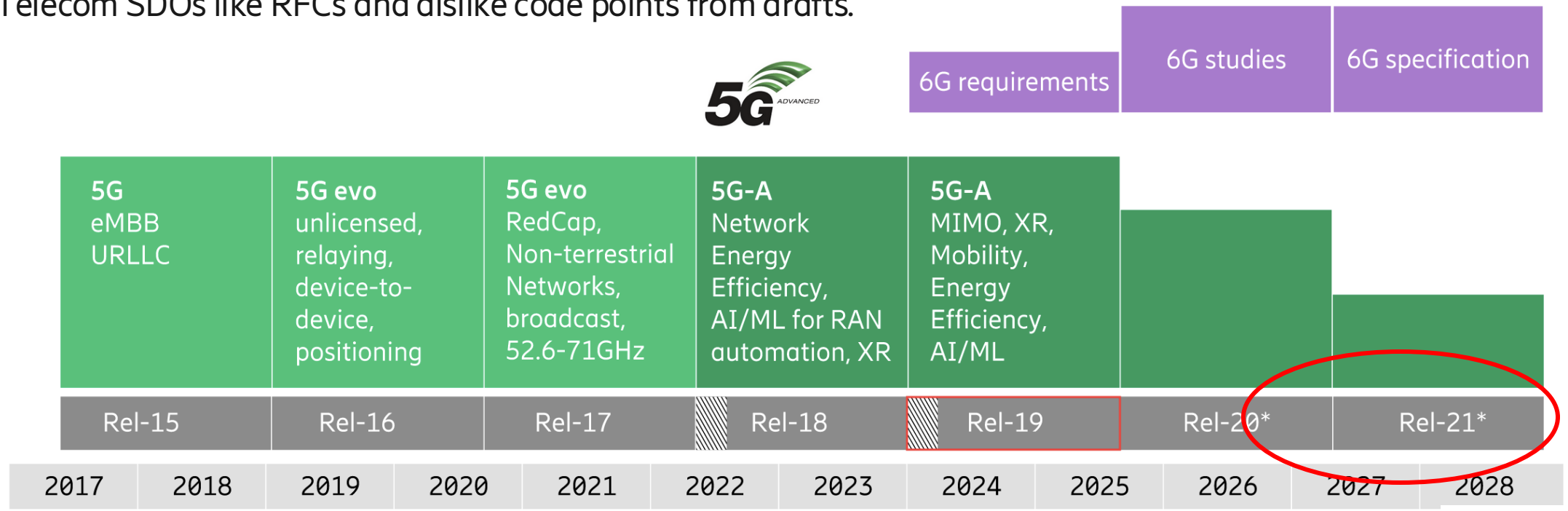
Application, infrastructure, and management layers



- In addition to the protocols in the connectivity layer application, management, and infrastructure layer also use public-key cryptography in DTLS-SRTP, MIKEY-SAKKE, ACE, COSE, SSH.
- Signatures for secure boot, remote attestation, firmware updates, software signing, etc., not standardized by 3GPP.
  - Firmware update for 5G nodes is a high-value target and migration needs to be prioritized.
  - Ericsson likely to support SLH-DSA-SHAKE-256s, ML-DSA-87, and Ed448.

3GPP 5G and 6G timelines

- 5G and 6G will both migrate to PQC. 6G will be fully quantum-resistant from the start.
- Focus on ML-KEM (FIPS 203), ML-DSA (FIPS 204), and SLH-DSA (FIPS 205).
  - Global standards designed be cryptographers from all over the world (mostly Europe).
- Need hardened (sometimes certified) software and hardware implementations of final NIST and IETF standards.
- Agreement to start normative work in Rel-20 after suggestion from Ericsson.
- Telecom SDOs like RFCs and dislike code points from drafts.



PQC requirements from various national bodies

- Most government agencies are now recommending ML-KEM, ML-DSA, and SLH-DSA. However:
  - Some require hybridization of ML-KEM and ML-DSA, while other forbid hybridization.
  - Some allow all security levels, some recommend level 3, and some require level 5.
  - Some recommend SLH-DSA, while other forbid SLH-DSA.
  - Some require LMS/XMSS single-tree, while other recommend multi-tree.
  - P-256, P-384, and Brainpool curves are increasingly seen as regional algorithms with Curve25519/448 being the globally preferred curves with superior security and performance.
  - Some recommend SHA-3 (ML-KEM, ML-DSA, and Ed448 use SHA-3 internally) while other require SHA-2.
  - South Korea, China, (and Japan): Developing their own PQC algorithms, differing from those of NIST.

PQC key exchange and public-key encryption

- ML-KEM is a lattice-based key encapsulation mechanism and can be used as a drop-in replacement for key exchange in e.g., TLS and IPsec as well as for public key encryption.
- Large sizes and slow performance are problematic in some use cases.

		TLS key share size (in bytes)		Operation per s (higher is better)	
Algorithm	Security Level	**Client**	**Server**	**Client**	**Server**
X25519	✖	32	32	19,000	19,000
ML-KEM-512	I	800	768	45,000	70,000
ML-KEM-768	III	1,184	1,088	29,000	45,000
ML-KEM-1024	V	1,568	1,568	20,000	30,000
HQC-KEM-128	I	2,249	4,497	3,000	8,000
mceliece348864	I	261,120	96	62,000	14,000
FrodoKEM-640	I	9616	9729	400	800

Inspired by Bas Westerbaan (Cloudflare)

Quantum-resistance signatures

- ML-DSA is a lattice-based key signature algorithms and can be used as a drop-in replacement for signatures in e.g., TLS and IPsec. SLH-DSA is a more conservative hash-based signature algorithms.
- Large sizes and slow performance are problematic in some use cases.
- NIST has new competition for multivariate, isogeny, and lattice-based signatures.

		Sizes (bytes)		CPU time (lower is better)	
	Security level	Public key	Signature	Signing	Verification
Ed25519	✗	32	64	1 (baseline)	1 (baseline)
RSA-2048	✗	384	384	70	0.3
ML-DSA-44	II	1,312	2,420	4.8	0.5
SLH-DSA-128s	I	32	7,856	8,000	2.8
SLH-DSA-128f	I	32	17,088	550	7
FN-DSA-512	I	897	666	8*	0.5
$MAYO_1$	I	1,168	321	4.7	0.3
$MAYO_2$	I	5,488	180	5	0.2
UOV Is	I	66,576	96	2.5	2
SQISign I	I	64	177	60,000	500
HAWK-512	I	1,024	555	2	1

Inspired by Bas Westerbaan (Cloudflare)

New quantum-resistance security levels

- "bits of security" does not correlate with practical security when attacks cannot be effectively parallelized. A CRQC that can break RSA in a few hours would not pose any practical threat at all to symmetrical algorithms such as AES-128 and SHA-256. Even with millions of CRQCs it would take millions of years.
- AES-128, SNOW 3G, Keccak, and SHA-256 in 4G and 5G will remain secure for the foreseeable future.
- NIST has defined five security levels for quantum-resistance:

Level	Security Description
I	At least as hard to break as AES128 (exhaustive key search)
II	At least as hard to break as SHA256 (collision search)
III	At least as hard to break as AES192 (exhaustive key search)
IV	At least as hard to break as SHA384 (collision search)
V	At least as hard to break as AES256 (exhaustive key search)

IETF and 3GPP statements on symmetric cryptography

IETF Statement:

— "**The idea that symmetric cryptography will be practically affected by CRQCs is now seen as a misconception**. The "bits of security" concept does not work with algorithms that are not parallelizable and NIST is therefore transitioning to quantum-resistant security levels based on symmetric algorithms where level 1 is equivalent with AES-128, level 2 is SHA-256, etc. UK government assesses that "symmetric algorithms with at least 128-bit keys (such as AES) can continue to be used". **While classical supercomputers might be able to brute force AES-128 around the year 2090, a huge cluster of one billion CRQCs (according to one estimate costing one billion USD each) would take a million years of uninterrupted calculation to find a single AES-128 key.** Algorithms with quadratic (n^2) speedup like Grover's algorithm (which is proven to be optimal) will not provide any practical quantum advantage for breaking symmetric cryptography and likely not for any other problems."

3GPP Statement:

— "A very good summary of the impact of Cryptographically Relevant Quantum Computers (CRQCs) on symmetric cryptography was recently given in a statement by the Internet Engineering Task Force (IETF). The IETF statement refers to UK NCSC whitepaper that says symmetric algorithms with at least 128-bit keys (such as AES) can continue to be used. **SA3 agrees with IETF's analysis. Most other 128-bit algorithms such as SNOW 3G, ZUC, TUAK, KMAC128, Ascon, etc. are likely to have similar quantum overhead for Grover's algorithm which is known to be optimal**. Even if an algorithm has slightly lower quantum overhead than AES-128, SA3 believes the algorithm would still fulfill the requirement (comparable to key search on AES-128) for quantum resistance category 1"

(but 6G will likely use high-performance 256-bit algorithms)

Sam Jaques keynote at CHES 2024: "Qubits would cover the moon"

NIST 2024: "All NIST-approved symmetric primitives that provide at least 128 bits of classical security are believed to meet the requirements of at least Category 1 security"

6G will likely use 256-bit AEAD algorithms

- Work initiated (in 2017), partly because of worries regarding quantum attacks now seen as a misconception.
- ETSI SAGE has specified AES-256, SNOW 5G, and ZUC-256 in GCM-SST mode. Many benefits:
  - Much faster in both software and hardware
  - Longer authentication tags that behaves like ideal MACs
  - Compliance with government requirement
  - Improved security against multi-key attacks

Name	Tag length (bytes)	Forgery probability before first forgery	Forgery probability after first forgery	Expected number of forgeries
GCM_SST_14	14	$1 / 2^{112}$	$1 / 2^{112}$	$v / 2^{112}$
GCM_SST_12	12	$1 / 2^{96}$	$1 / 2^{96}$	$v / 2^{96}$
POLY1305	16	$1 / 2^{91}$	$1 / 2^{91}$	$v / 2^{91}$
GCM	16	$1 / 2^{116}$	1	$\delta \cdot v^2 / 2^{117}$

Table 1: Comparison between AES-GCM-SST, ChaCha20-Poly1305, and AES-GCM in unicast QUIC where the maximum packet size is 2^{16} bytes. v is the number of decryption queries and δ is the Bernstein bound factor.

3GPP/ETSI/GSMA Algorithms

Algorithms for authentication and key generation:

Cipher	Proprietary	Proprietary	Proprietary	AES/Rijndael-256	Keccak
Input key size	128	128	128	128, 256	128, 256
Output key size	54	54	64	128, 256	128, 256
Name	COMP-128-1	COMP-128-2	COMP-128-3	MILENAGE(-256)	Tuak

Algorithms for encryption and integrity: (*A5/2 and GEA1 are export ciphers with no more than 40 bits effective security):

Cipher	Proprietary	Proprietary	KASUMI	KASUMI	KASUMI	SNOW 3G	SNOW 3G	AES	AES	ZUC	ZUC
Key size	64*	64	64	128	128	128	128	128	128	128	128
Mode	XOR	XOR	f8-mode	f8-mode	CBC-MAC	XOR	CW-MAC1	CTR	CMAC	XOR	CW-MAC2
Type	ENC	ENC	ENC	ENC	INT	ENC	INT	ENC	INT	ENC	INT
Tag size					32		32		32		32
GSM	A5/2	A5/1	A5/3	A5/4							
GPRS	GEA1	GEA2	GEA3	GEA4	GIA4	GEA5	GIA5				
UMTS				UEA1	UIA1	UEA2	UIA2				
LTE						128-EEA1	128-EIA1	128-EEA2	128-EIA2	128-EEA3	128-EIA3
NR						128-NEA1	128-NIA1	128-NEA2	128-NIA2	128-NEA3	128-NIA3

Already large deployments of FIPS 203–205

- With the publication of FIPS 203 (ML-KEM), FIPS 204 (ML-DSA), and FIPS 205 (SLH-DSA), Post-Quantum Cryptography (PQC) has quickly moved from research to implementation and deployment.

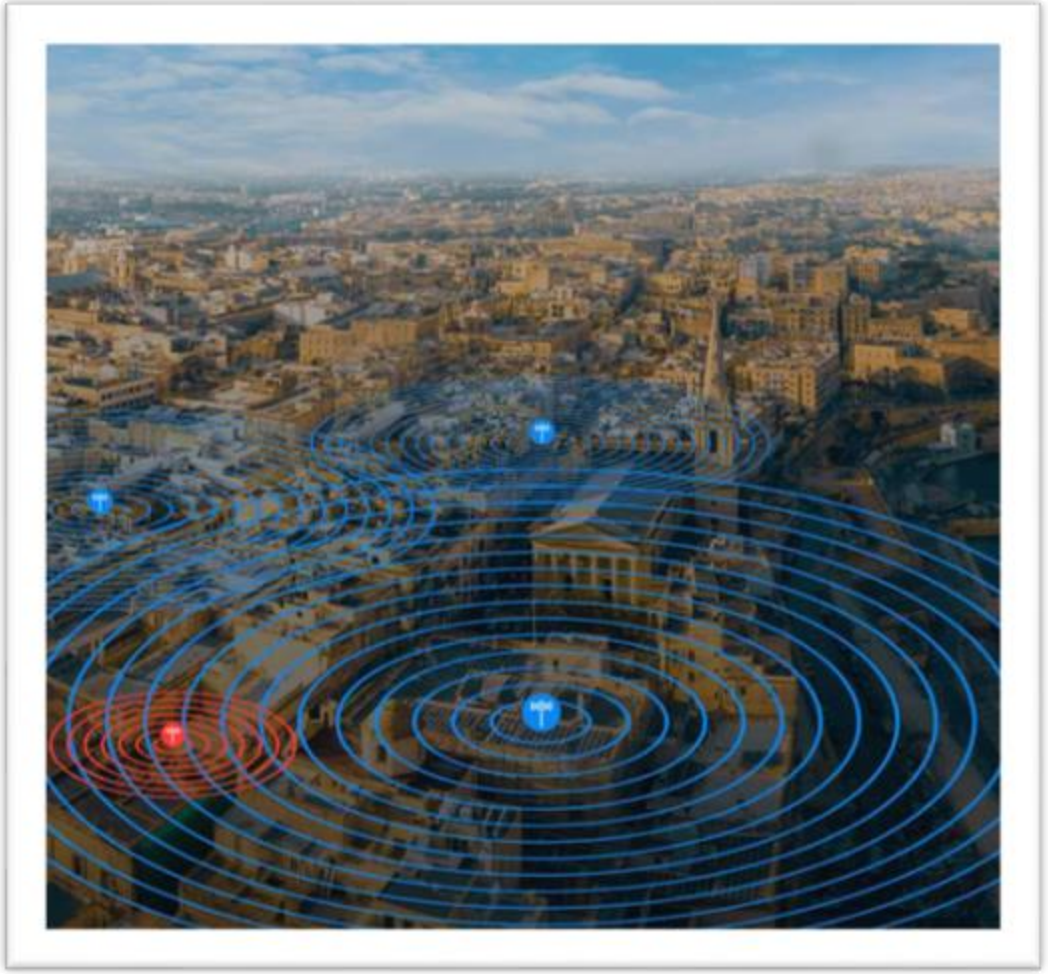
- In TLS, X25519MLKEM in has already seen massive implementation support and is the default in OpenSSL, Firefox, Chrome, Edge, Go, etc.
- Cloudflare reports that over 40% of all HTTPS client requests use PQC.
- OpenSSL 3.5 LTS supports ML-KEM, ML-DSA, and SLH-DSA.
- OpenSSH is now using mlkem768x25519 as the default key exchange,
- Many IKEv2 implementations support ML-KEM. IKEv2 always uses ML-KEM in hybrid with (EC)DHE.

Backup algorithms and hybrids

- To meet time requirements, telecom will need to pick the first available PQC implementations and use them in production systems.
  - ML-KEM, ML-DSA, and SLH-DSA.
- Many early implementation have bugs and side-channels. Hybrid KEMs are a cheap defense-in-depth.
- HQC and Classic McEliece are good backup algorithms to ML-KEM.
- Standards for backup algorithms might not be available until later.

Key conclusions

- Industry need alignment around ML-KEM, ML-DSA, SLH-DSA and parameters.
- Telecom will likely use conservative options (high security level, hybrid KEMs, SHA-3, stateless, "pure", and "hedged" signatures).
- Quantum computer attacks will have no general practical effect on symmetric crypto (like AES-128).
- Discussions of QKD, QRNGs, and doubling symmetric key sizes in PQC migration are distractions.
- Quantum sensors are extremely promising for military use.
- **Mobile networks standards and products will have to support PQC algorithms soon for both 5G and 6G.**



Further reading

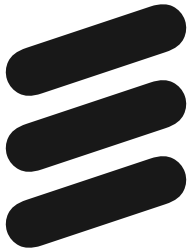
- Ericsson Technology Review, "Quantum technology and its impact on security in mobile networks"
  https://www.ericsson.com/en/reports-and-papers/ericsson-technology-review/articles/ensuring-security-in-mobile-networks-post-quantum
- NIST, "Constrained Radio Networks, Small Ciphertexts, Signatures, and Non-Interactive Key Exchange"
  https://csrc.nist.gov/csrc/media/Events/2022/fourth-pqc-standardization-conference/documents/papers/constrained-radio-networks-pqc2022.pdf
- New Scientist, "Cryptographers bet cash on when quantum computers will beat encryption"
  https://www.newscientist.com/article/2370022-cryptographers-bet-cash-on-when-quantum-computers-will-beat-encryption/
- NSA, "The Commercial National Security Algorithm Suite 2.0 and Quantum Computing FAQ"
  https://media.defense.gov/2022/Sep/07/2003071836/-1/-1/0/CSI_CNSA_2.0_FAQ_.PDF
- BSI, ANSSI, Dutch and Swedish NCSA, "Position Paper on Quantum Key Distribution"
  https://www.forsvarsmakten.se/contentassets/f7199ed1b90f41529b76970bdb5fce1c/position-paper-on-quantum-key-distribution.pdf
- Ericsson Blog, "Migration to quantum-resistant algorithms in mobile networks"
  https://www.ericsson.com/en/blog/2023/2/quantum-resistant-algorithms-mobile-networks
- NIST, "Post-Quantum Cryptography Project"
  https://csrc.nist.gov/projects/post-quantum-cryptography
- arXiv, "Quantum-Resistant Cryptography"
  https://arxiv.org/abs/2112.00399
- NISTIR 8547, "Transition to Post-Quantum Cryptography Standards"
  https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8547.ipd.pdf
- ANSSI, "Guide des Mécanismes cryptoraphiques"
  https://cyber.gouv.fr/sites/default/files/2021/03/anssi-guide-mecanismes_crypto-2.04.pdf

Further reading

- Status of quantum computer development
  https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Quantencomputer/Entwicklungstand_QC_V_2_0.html?nn=916616
- ANSSI plan for post-quantum transition
  https://pkic.org/events/2023/pqc-conference-amsterdam-nl/pkic-pqcc_jerome-plut_anssi_anssi-plan-for-post-quantum-transition.pdf
- Landscape of Quantum Computing in 2024
  https://sam-jaques.appspot.com/quantum_landscape_2024
- IBM Quantum Computing Roadmap
  https://www.ibm.com/quantum/technology#roadmap
- On factoring integers, and computing discrete logarithms and orders, quantumly
  http://kth.diva-portal.org/smash/get/diva2:1902626/FULLTEXT01.pdf
- IETF Statement on Quantum Safe Cryptographic Protocol Inventory
  https://datatracker.ietf.org/liaison/1942/
- 3GPP Statement on PQC Migration
  https://www.3gpp.org/ftp/tsg_sa/WG3_Security/TSGS3_118_Hyderabad/docs/S3-244307.zip
- Sam Jaques, "Quantum Attacks on AES"
  https://www.youtube.com/watch?v=eB4po9Br1YY&t=3227s
- FIPS 203 (ML-KEM), FIPS 204 (ML-DSA), and FIPS 205 (SLH-DSA) approved
  https://csrc.nist.gov/news/2024/postquantum-cryptography-fips-approved
- ML-KEM is Great. What's Missing?
  https://emanjon.github.io/Publications/ML-KEM%20is%20Great!%20What's%20Missing.pdf

Further reading

- National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems ‘
  https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/
- Timelines for migration to post-quantum cryptography
  https://www.ncsc.gov.uk/guidance/pqc-migration-timelines
- Cryptographic algorithms for UNCLASSIFIED, PROTECTED A, and PROTECTED B information
  https://www.cyber.gc.ca/en/guidance/cryptographic-algorithms-unclassified-protected-protected-b-information-itsp40111
- National Quantum Strategy roadmap: Quantum communication and post-quantum cryptography
  https://ised-isde.canada.ca/site/national-quantum-strategy/en/national-quantum-strategy-roadmap-quantum-communication-and-post-quantum-cryptography
- Quantum Key Distribution (QKD) and Quantum Cryptography (QC)
  https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/
- Expected and Unexpected Developments in Quantum Computing
  https://www.youtube.com/watch?v=nJxENYdsB6c
- PQC Dialogue with Government Stakeholders
  https://groups.google.com/a/list.nist.gov/g/pqc-forum/c/5_WPq6mFi68/m/bnW6vJbeEgAJ
- Galois Counter Mode with Strong Secure Tags (GCM-SST)
  https://datatracker.ietf.org/doc/html/draft-mattsson-cfrg-aes-gcm-sst
- Comments on EU Roadmap on Post-Quantum Cryptography
  https://emanjon.github.io/EU-comments/2025%20-%20EU%20Roadmap%20on%20PQC.pdf



https://www.ericsson.com/en/security