Standardization of and Migration to Post-Quantum Cryptography (PQC)

ERICSSON

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

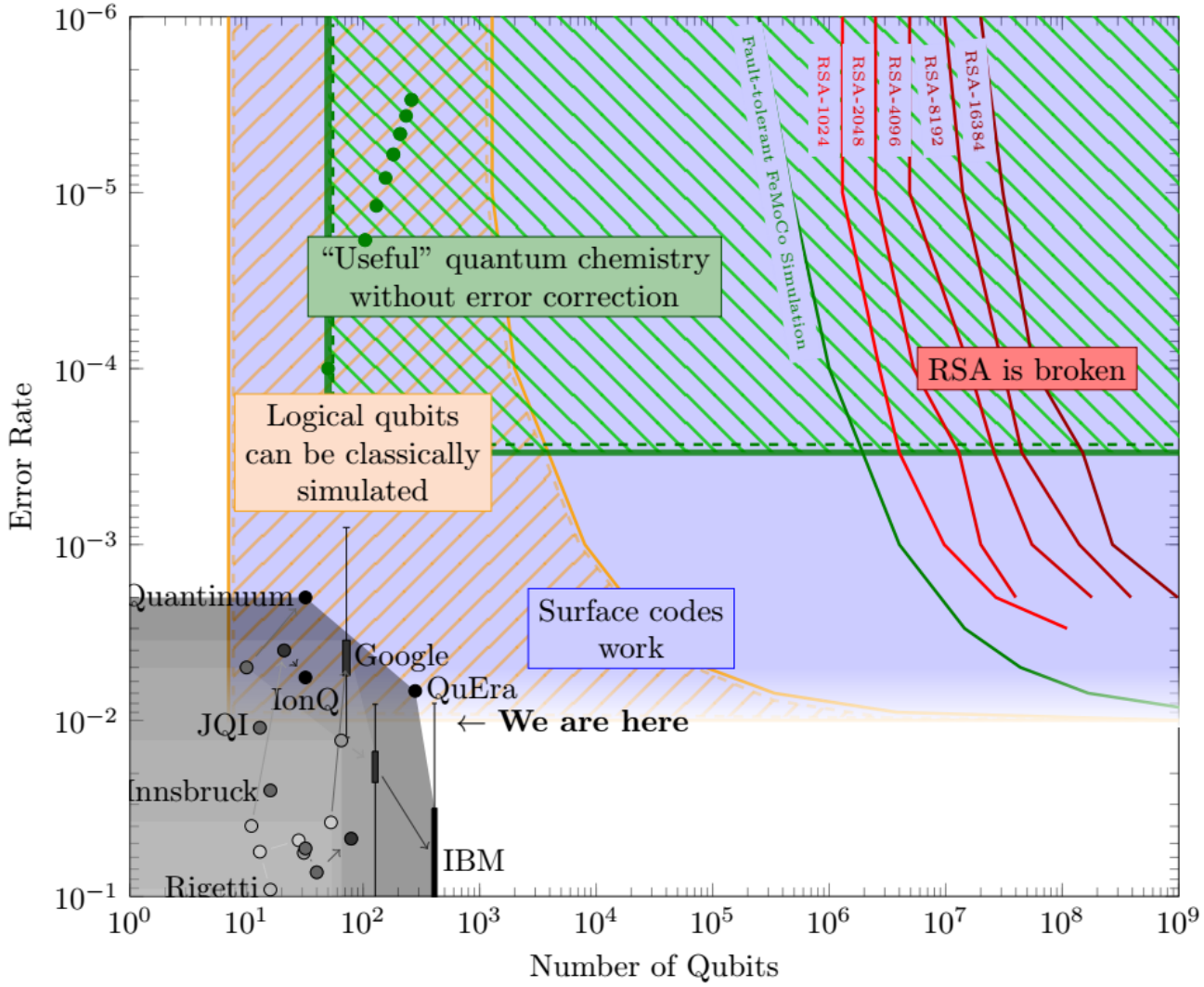
December 6, 2024

History of quantum and security

- 1976 – Diffie-Hellman key exchange
- 1977 – RSA cryptosystem
- **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 – integer factorization 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 (NSA) announced 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**
- **2024 – NIST states that non-quantum-resistant asymmetric crypto will be deprecated 2030 and disallowed 2035.**
- **2024 – NIST will publish first draft of FN-DSA and announce which of Classic McEliece, BIKE, and HQC to standardize.**

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. The largest quantum computer currently has around 1000 unstable physical qubits.
- It is 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 30 years. **Some signs that investment is slowing down.**
- **IBM's roadmap for 2033+ is now 2000 qubits.**
- **Breakthroughs in quantum error correction.**



Landscape of Quantum Computing in 2023 by Sam Jaques

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, 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:

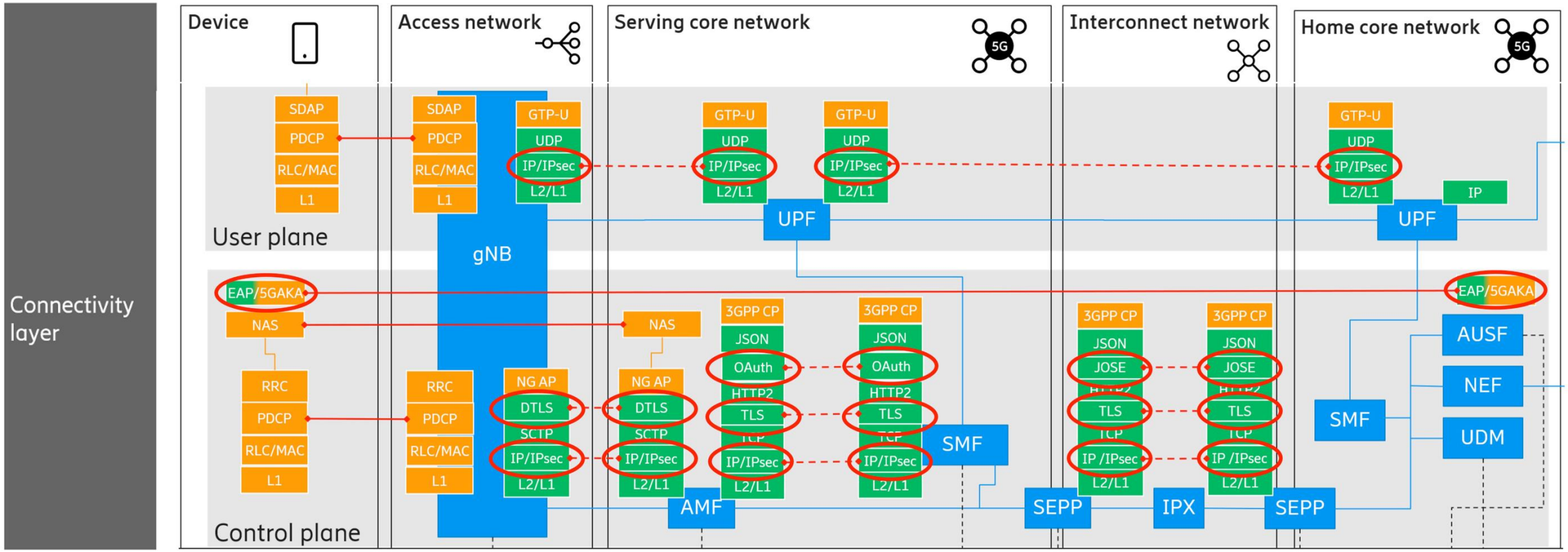
— "**A very good summary of the impact of Cryptographically Relevant Quantum Computers (CRQCs) on symmetric cryptography was recently given in a statement by the Internet Engineering Task Force (IETF)**. The IETF statement refers to UK NCSC whitepaper that says symmetric algorithms with at least 128-bit 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 very use high-performance 256-bit algorithms)

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

Impact on 3GPP 5G connectivity layer

- Making something “quantum-resistant” means supporting quantum-resistant public-key algorithms instead of RSA and ECC everywhere.
- Migration involves inventory, crypto agility, prioritization, development, deployment, and to disable standalone RSA/ECC.
- 5G relies on IETF protocols like X.509, CMP, CRL, OCSP, IKEv2, TLS, DTLS, JOSE, EAP-TLS, and EAP-AKA-FS for almost all uses of public-key cryptography.



Standardization of post-quantum cryptography (PQC)

- Post-Quantum Cryptography (PQC) is public key cryptography that is secure against CRQCs.
  - Can run in software on classical computers just like RSA and ECC.
  - All governments trusts code-based (1978), hash-based (1979), and lattice-based (1998) cryptography.
    - Standardization and discussions are about which optimalisations that should be made.

- Ericsson has been very active in NIST, IETF, and 3GPP standardization and discussions. Influenced NIST to focus on practical security, small sizes for wireless, and suggested to make ML-DSA hedged.

- IETF (and later NIST) standardized **stateful** hash-based signatures (XMSS and LMS) in 2018.
  - NIST forbidding private key export is a major issue. NIST working on update to SP 800-208.
- NIST standardized ML-KEM (lattice), ML-DSA (lattice), and SLH-DSA (stateless hash) in 2024.
  - FN-DSA (lattice) will be published later in 2024.
  - A decision on code-based KEMs (subset of BIKE, HQC, and Classic McEliece) is expected end of 2024.
  - Selection of additional quantum-resistant signatures for Round 2 is expected in autumn 2024.
- ISO is working on standardization of Classic McEliece, ML-KEM, and FrodoKEM (unstructured lattice). Paywalled.

- US national security systems will use XMSS, LMS, ML-KEM, and ML-DSA without hybrid.
- European governments also recommends SLH-DSA, Classic McEliece and FrodoKEM. **Requires hybrid.**

Migration to post-quantum cryptography

- PQC migration is similar to the migration from 3DES to AES and SHA-1 to SHA-2. Difference is that there is no clear end year.

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

- When to stop using RSA and ECC depends on the protection lifetime and the availability of CRQCs. Protection lifetimes vary from days to decades.

- If CRQCs are ever built, early CRCRs will likely be very expensive and only used in targeted attacks to recover keys and ciphertexts that are of particular interest.

- Software is easier to update than hardware.

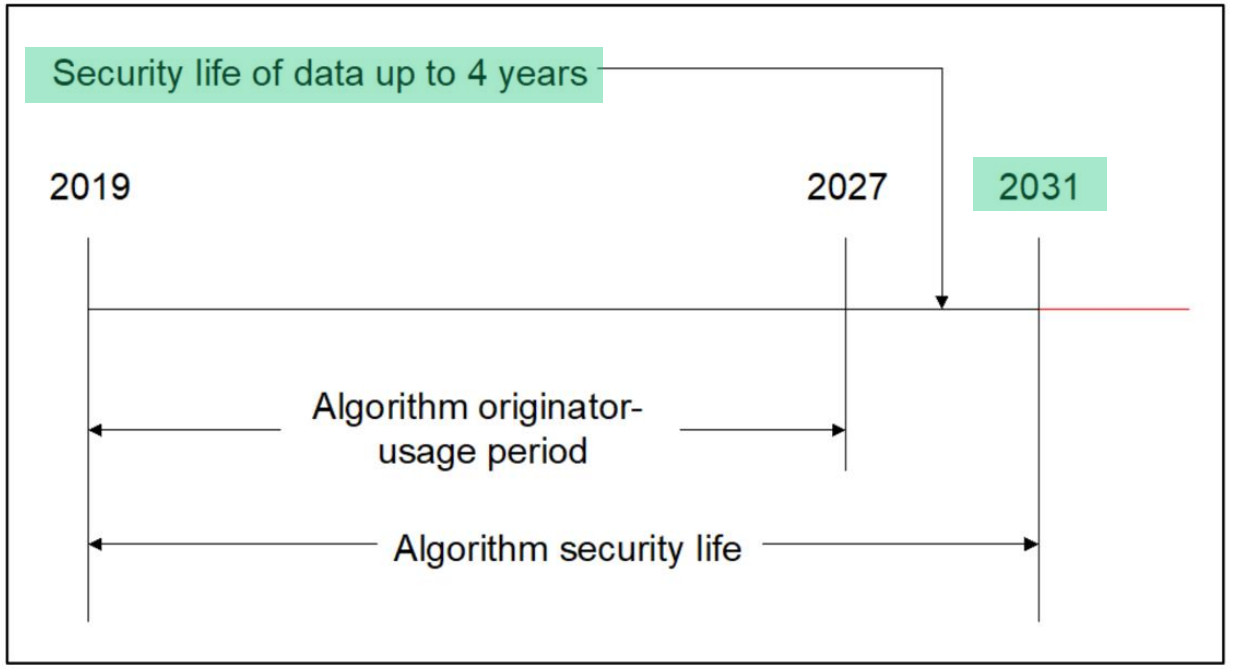
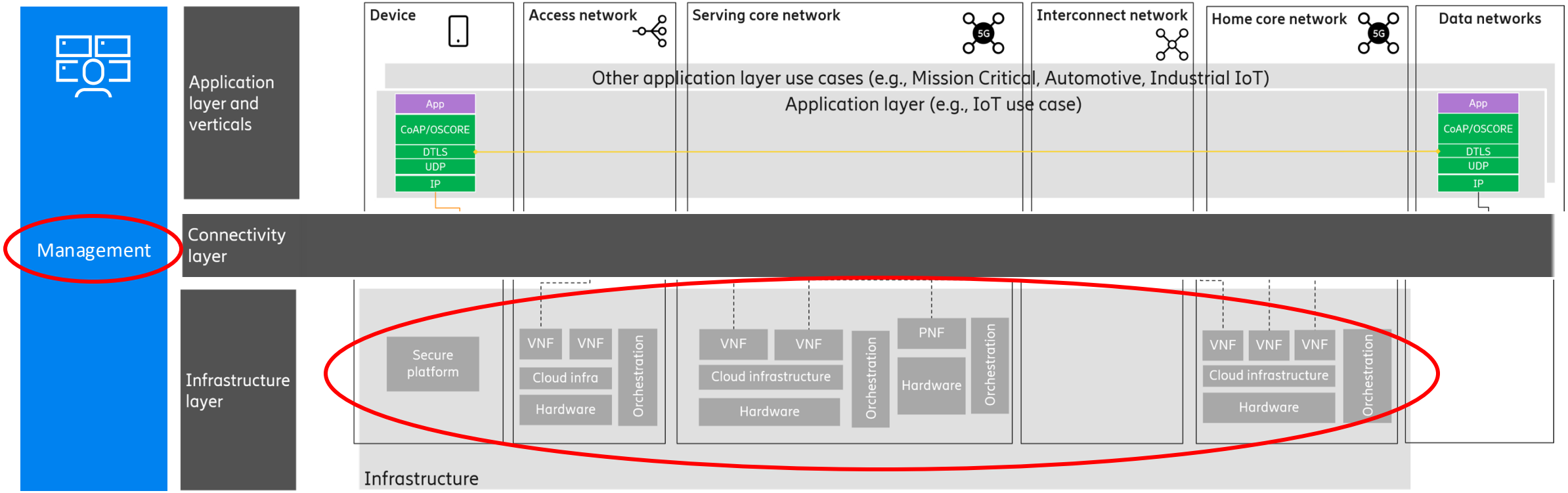


Figure 2: Algorithm originator-usage period example

Application, infrastructure, and management layers

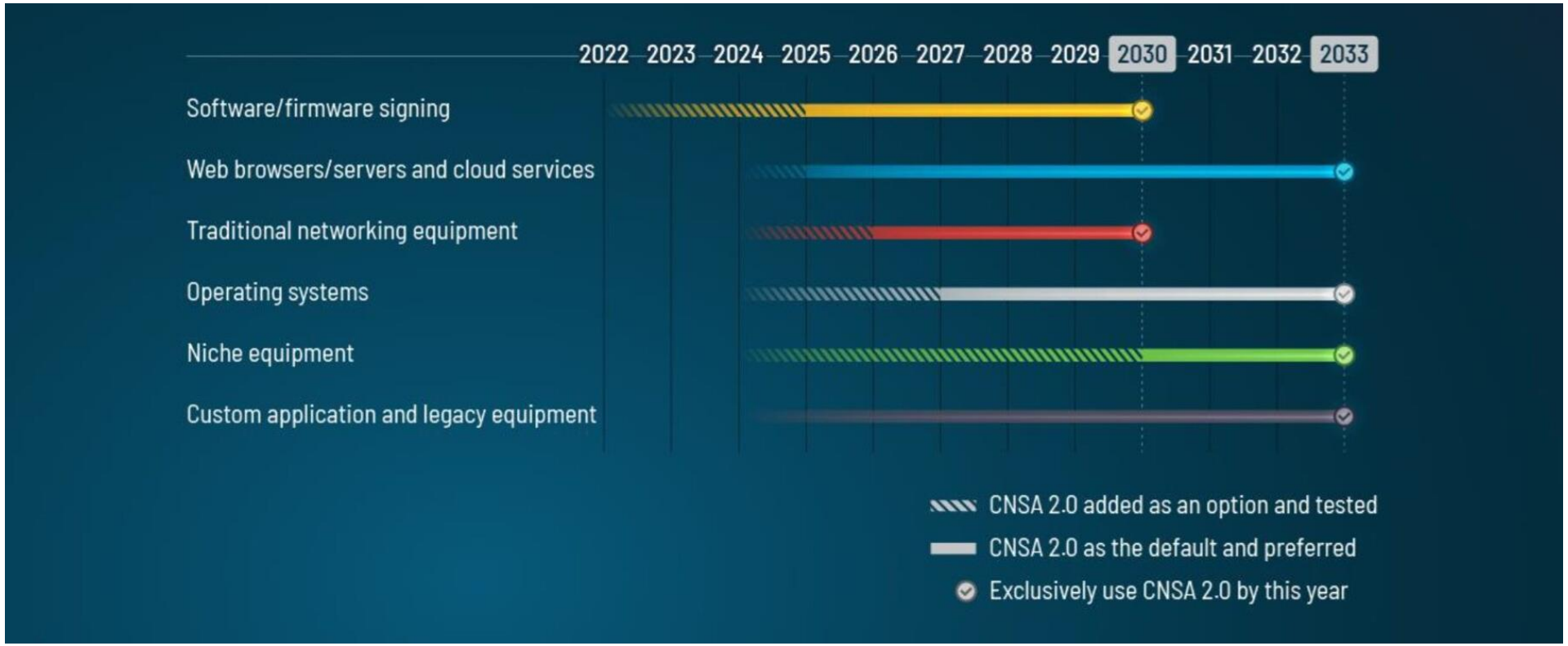
- In addition to the protocols in the connectivity layer the application layer also use DTLS-SRTP and MIKEY-SAKKE.
  - No PQC replacement for identity-based, attribute-based, and privacy-enhancing cryptography (pairing-based crypto).
  - PQC sizes will be problematic/impossible for constrained IoT.



- In addition to the protocols in the connectivity layer the infrastructure layer also uses SSH and MACsec keyed with EAP-TLS
- Signatures for secure boot, vendor certificates, remote attestation, firmware updates, software signing, etc, …
- **Work on quantum-resistant cryptography in infrastructure layer hardware has already started many years ago.**

US government CNSA 2.0 timelines

- US government has published timelines for the migration of national security systems to PQC.
- **NIST states that non-quantum-resistant asymmetric crypto will be disallowed after 2035.**
- European countries (e.g., ANSSI) also recommend migration to PQC by/around 2030.
- US has selected ML-KEM and ML-DSA with security level V as the general future public-key algorithms.
  - Also recommended by UK, Australia, Canada, New Zealand, **Germany, France, Netherlands**.
- The CNSA suite is used to protect classified information that often must stay confidential for 50+ years.



PQC requirements from various national bodies

- **Key Encapsulation Mechanisms (KEMs)**
  - NIST (USA): Standardizing ML-KEM; plans to standardize one or more code-based KEMs.
  - CNSA 2.0 (USA): Requires ML-KEM-1024 (Level 5) for National Security Systems (NSS).
  - NCSC (UK): Recommends ML-KEM-768 (Level 3).
  - BSI (Germany): Recommends ML-KEM-768 and ML-KEM-1024, FrodoKEM-976, FrodoKEM-1344, McEliece460896, McEliece6688128, McEliece8192128.
  - ANSSI (France): Recommends ML-KEM-768, ML-KEM-1024, and FrodoKEM as a conservative option.
  - NLNCSA (Netherlands): Recommends ML-KEM-768 and considers Classic McEliece and FrodoKEM acceptable.
  - South Korea and China: Developing their own PQC algorithms, differing from those of NIST.

- **Signature Algorithms**
  - NIST (USA): Standardizing ML-DSA, FN-DSA, SLH-DSA, and potentially one more after Round 4.
  - CNSA 2.0 (USA): Recommends ML-DSA-87 (Level 5) as a general signature and LMS/XMSS (single-tree) for firmware signing.
  - NCSC (UK): Recommends ML-DSA-65, SLH-DSA, and LMS/XMSS for long-term signatures.
  - BSI (Germany): Recommends SLH-DSA or ML-DSA (Levels 3 and 5), and LMS/XMSS in multi-tree variants for long-term signatures.
  - ANSSI (France): Recommends ML-DSA, FN-DSA (Levels 3 and 5), SLH-DSA, and LMS/XMSS.
  - NLNCSA (Netherlands): Recommends all NIST signatures and LMS/XMSS.

Quantum-resistance key exchange

- ML-KEM is a lattice-based key encapsulation mechanism and can be used as a drop-in replacement for key exchange in TLS and IPsec as well as for public key encryption in SUCI (IMSI encryption).
- ML-KEM-1024 will be used by US government for protection of TOP SECRET information.
- Large sizes are problematic in some use cases.
- Classic McEliece often has the best performance for static authentication keys (S/MIME, SUCI, WireGuard, EDHOC, …) and is considered very conservative.

		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
mceliece348864	I	261,120	96	62,000	14,000

Inspired by Bas Westerbaan (Cloudflare)

Quantum-resistance key exchange

- While the code-based Classic McEliece uses binary Goppa codes, the code-based BIKE and HQC use QC-MDPC codes. BIKE and HQC are good alternatives to ML-KEM for ephemeral key exchange.

- Table 1.KEM Public key and ciphertext sizes in bytes. Total size is public key size plus ciphertext size which is a relevant measure when KEMs are used for ephemeral key exchange is protocols like TLS 1.3 and IKEv2.

- Table 2. KEM performance in cycles (50%) on 2023 AMD Ryzen 7 7700. Performance number from eBACS: ECRYPT Benchmarking of Cryptographic Systems by Bernstein and Lange (editors) https://bench.cr.yp.to/results-kem/amd64-hertz.html. Total is cycles for key gen + encapsulation + decapsulation.

Name	Category	Public key	Ciphertext	Total
ML-KEM-512	1	800	768	1568
BIKE-L1	1	1541	1573	3114
ML-KEM-512+BIKE-L1	1	2341	2341	4682
HQC-128	1	2249	4481	6730
ML-KEM-512+HQC-128	1	3049	5249	8298
FrodoKEM-640	1	9616	9720	19336

Name	Category	Key Gen	Encapsulation	Decapsulation	Total
ML-KEM-512 (kyber512)	1	15420	24443	18693	58556
HQC-128 (hqc128round4)	1	61311	170433	283249	514993
ML-KEM-512+HQC-128	1	76731	194876	301942	573549
BIKE-L1 (bikel1)	1	459202	83286	1069392	1611880
ML-KEM-512+BIKE-L1	1	474622	107729	1088085	1670436
FrodoKEM-640 (frodokem640shake)	1	2084314	2265633	2222733	6572680

Quantum-resistance signatures

— ML-DSA-87 (security level V) will be used by US government in national security systems.
— 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
FN-DSA-512	I	897	666	8*	0.5
SLH-DSA-128s	I	32	7,856	8,000	2.8
SLH-DSA-128f	I	32	17,088	550	7
$MAYO_1$	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)

IETF protocols and deployment plans

- IETF is planning to add ML-KEM and ML-DSA to all major protocols. IETF will recommend hybrids.
  - X25519MLKEM768 is the new de facto standard key exchange method in TLS 1.3
  - IKEv2 will always use hybrid key exchange for technical reasons.
  - IETF is discussing if two certificate chains or one certificate chain with composite keys and signatures should be used.

- DNSSEC and the Web will likely take a wait-and-see approach. May use MAYO (multivariate) or HAWK (lattice) security level I. Sometimes called PQC generation 2 and is likely 5 years from standardization.

- European governments might standardize the use of more conservative algorithms (FrodoKEM, Classic McEliece) with much slower performance in IETF protocols.

- Hybrid modes is a large discussion area. Hybrid modes means that PQC is used together with RSA or ECC.
  - US government says that hybrid is not recommended as it increases complexity. European governments say that hybrid is a must due to possibility of theoretical or implementation attacks.

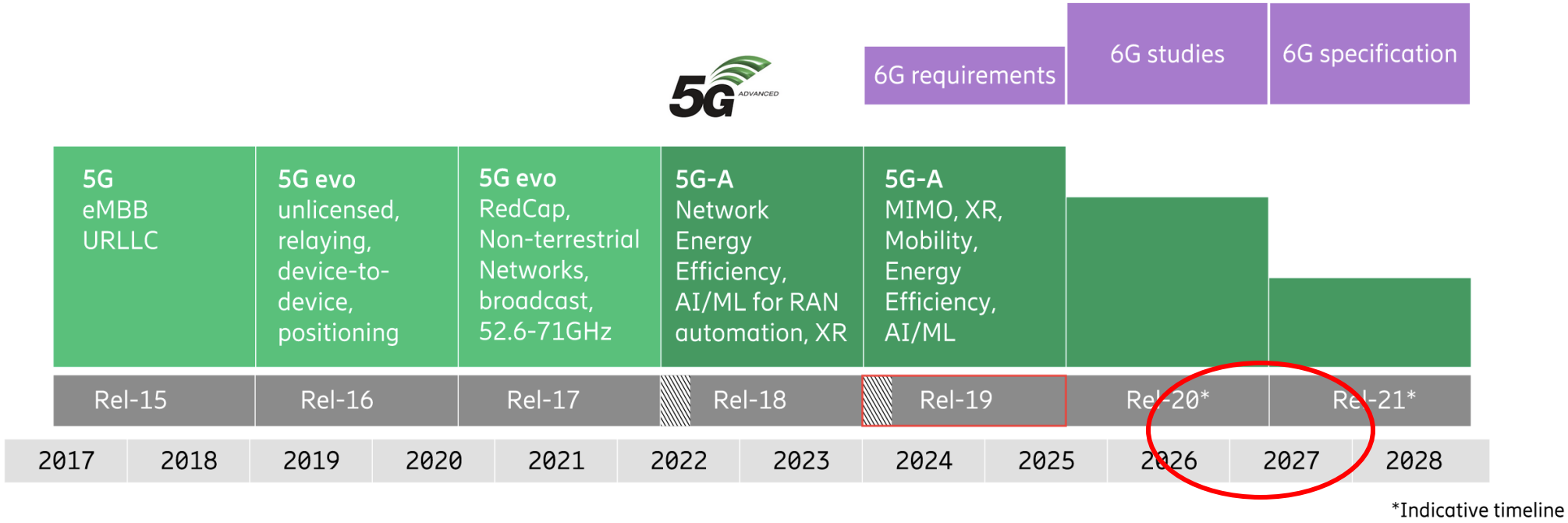
- Sizes are a major issue. Initial message in IKEv2 cannot be fragmented and IKEv2 will therefore always use hybrid mode. Some TLS servers does not accept large initial messages, these need to be updated.
  - TLS 1.2 will not get any updates. 5G mandates TLS 1.3 since Rel-15. NIST mandates TLS 1.3 since 2024.

Backup algorithms and hybrids

- Ericsson would like to see Classic McEliece as a backup algorithm to ML-KEM for static keys.
- Ericsson would like to see BIKE or HQC as a backup algorithm to ML-KEM for ephemeral keys.
- Ericsson's current plan is to use ECC+PQC hybrids for key exchange and long-term signatures.
  - Cheap defense-in-depth for key exchange.
  - Strong requirement from many European governments.
  - IETF will recommend hybrids in general.
  - To meet time requirements, we will need to pick the first available PQC implementations and use them in production systems. Many early implementation have bugs and side-channels.

3GPP 5G and 6G timelines

— 5G and 6G will both migrate to PQC. 6G will be fully quantum-resistant from the start.
— CNSA 2.0 forbids using non-standardized versions of the algorithms. 3GPP will follow this.
— Need hardened (sometimes certified) software and hardware implementations of final NIST and IETF standards.



*Indicative timeline

Key conclusions

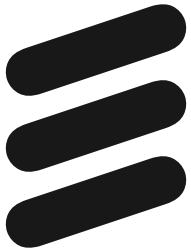
- If large robust quantum computers are ever built, they will break RSA and ECC in a few hours.
- Quantum computer attacks will have no practical effect on symmetric crypto (like AES-128).
- NIST has finalized standardization of the most important new quantum-resistant algorithms.
- PQC standardization will continue in NIST, IETF, and 3GPP in the next five years.
- When to migrate depends for how long protection is required, the value of the target.
- **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, “Announcing the Commercial National Security Algorithm Suite 2.0”
  https://media.defense.gov/2022/Sep/07/2003071834/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS_.PDF
- BSI, ANSSI, Dutch and Swedish NCSA, ”Position Paper on Quantum Key Distribution”
  https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/Quantum_Positionspapier.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 2023
  https://sam-jaques.appspot.com/quantum_landscape
- 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



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