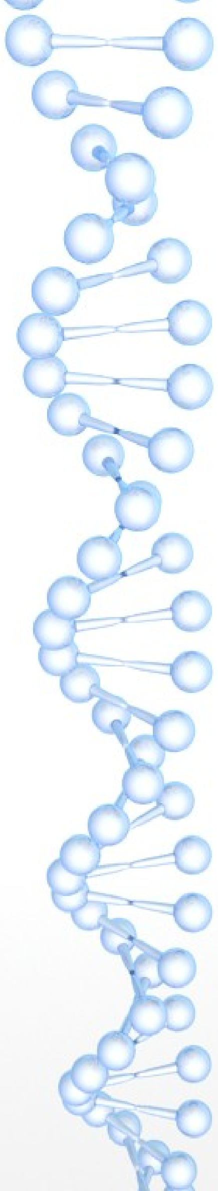
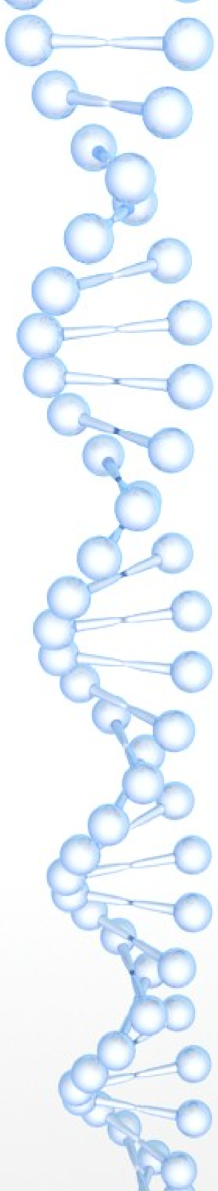


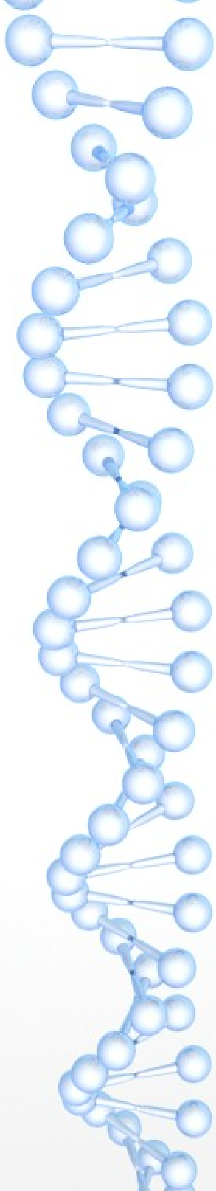
Towards quantum-resistant 5G and beyond with eAES and 256-bit block ciphers

Quantum computers able to crack existing encryption are due <u>within this decade</u>, according to leading subject matter experts, coming from horizons as diverse as fundamental quantum physics, applied quantum IT research and quantum-safe cryptography.



The issue posed by QIT to current & future nets

- Currently used ciphers in GSM networks up to and including 5G use 128-bit block ciphers with 128-bit keys for encryption of the communications, with the exception of ZUC, a stream cipher, with similar characteristics however, as to what regards quantum IT resistance.
- This is due to the fact Grover’s algorithm halves the key space when run on a powerful enough quantum computer, making 128-bit symmetric ciphers worth only about 64 bits of security, which is insufficient even today.



The issue posed by QIT to current & future nets

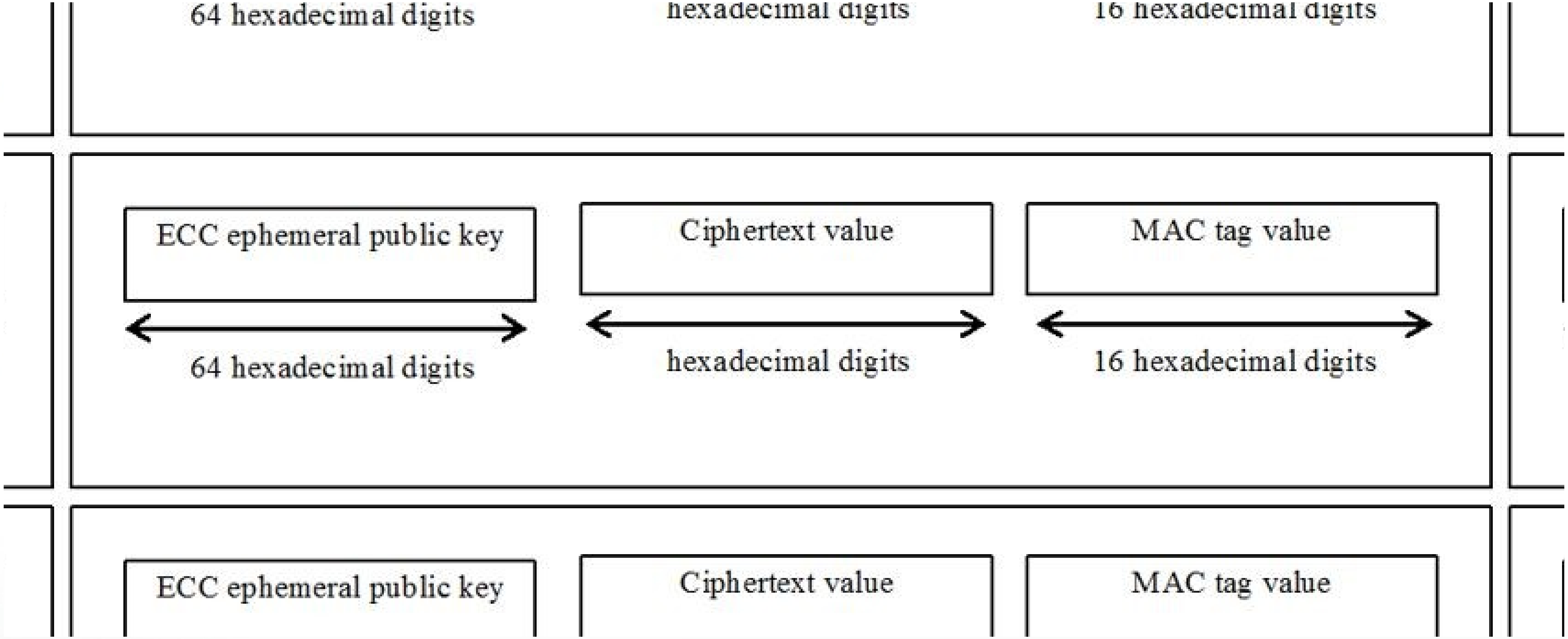
- This means that we can state with assurance that all of the world’s mobile communications that are being stored for later decryption will be decrypted, soon.
- With existing networks, this is not only within reach of state actors, but of organized crime, due to the ease of manipulating signaling networks, which, like civil aviation networks, were made with the assumptions that all parties accessing to it could be trusted, a serious design error…
- Once the attacker gets a quantum computer, he decrypts it.

The specific case of 5G

- In 5G and assuming a downgrading attack to 4G doesn’t work, a new technology SUCI/SUPI is used instead of the IMSI, supposed to defeat IMSI catchers and therefore, make illegal local area mobile communication eavedropping harder
- SUCI, however, is based on ECC (with very small keys)*, which is in any case vulnerable to quantum computing.
- In addition to that, 5G still uses 128-bit symmetric crypto to protect communication content, which will be broken too.

*cf. http://5gblogs.com/concealing-of-supi-into-suci/

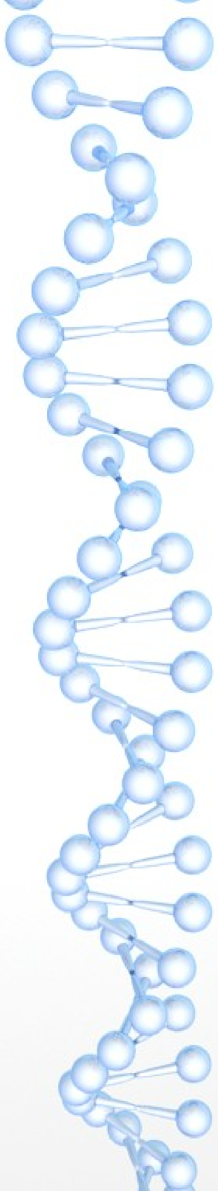
The specific case of 5G (illustration)



Source: http://5gblogs.com/wp-content/uploads/2019/05/Capture3.jpg

Immediate goal: a quantum-safe revision of 5G

- 5G should, in its next revision, include quantum-resistant ciphers, both for symmetric and asymmetric cryptography.
- Candidates are available and being discussed at the ITU-T interim meeting of SG17 / Q6 in Kuala Lumpur, Malaysia, as to what regards symmetric cryptography.
- Asymmetric cryptography could either wait for the NIST PQC competition’s end, or draw from ITU-T X.1197amd1



Our vision for 2030: 256-bit block ciphers

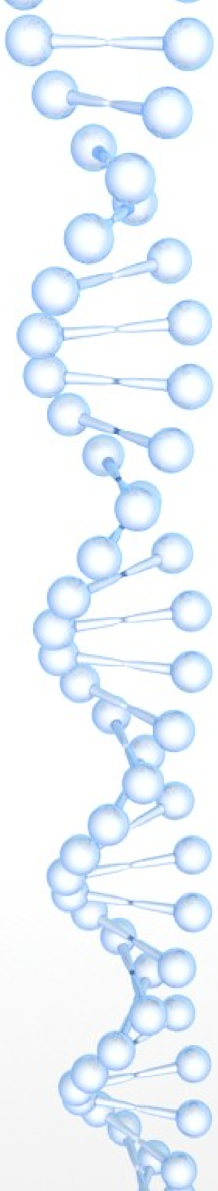
- By 2030, large enough quantum computers to crack pre-quantum crypto should be there, as mentioned before.
- Recent advances in applying advanced compilation techniques to Grover’s algorithm (meant to crack AES on quantum computers) question the security margin of AES > 128, cf. IACR e-print 2019/1146 from Microsoft.
- Quantum algebraic attacks set the block - not the key size - as the ultimate guard against quantum computers.

Concrete technical recommendations

- ITU-T X.1197 amendment 1, amended guidelines for the selection of cryptographic algorithms in IPTV, 2019, is the first ITU text to specify a list of valid examples and parameters for quantum-resistant cryptography in all categories needed by multimedia streaming (can be easily extended to VoIP / VoLTE / 5G / you name it), ranging from symmetric encryption to asymmetric signatures.
- At ISO/IEC SC27, CH started a study period on including eAES, an enhanced AES meant to resist quantum IT, while keeping backwards compatibility with existing server CPUs.

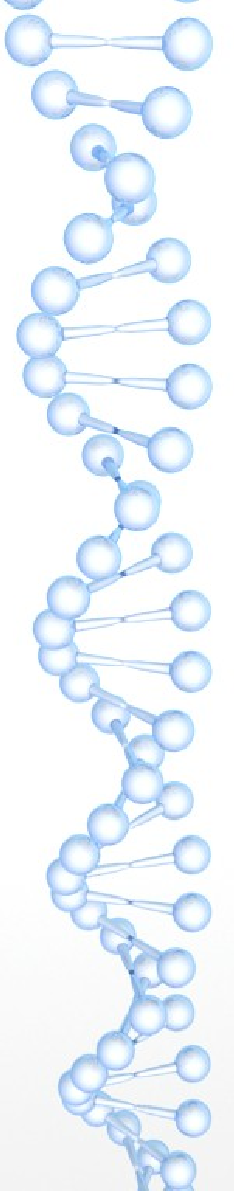
Future work and discussions

- Still in ISO/IEC SC27, after being asked by a leading cloud provider about it, we launched a discussion on setting the reference for quantum safety to 256-bit block ciphers, rather than AES-256, due to the aforementioned Microsoft paper.
- We expect the market to be ready to transition from 128-bit block to 256-bit block ciphers and equivalent stream ciphers by 2030. In the meantime, eAes provides a transitional solution that dramatically improves the security margin of AES-256 against large quantum IT, likewise side-channel attacks, with low CAPEX
- See IACR e-print 2019/1208 & 553 for details and exp. results.



Present, past & future solutions using eAES

- The github.com/Steppenwolfe65/CEX C++ lib. (GPLv3 license).
- Our proprietary software for ARM-based platforms.
- Our (e/sw)SIM/smart card patent for the use of eAes in a secure (mob.) financial transactions, data & voice context.
- Critical infrastructure and other high-security infra. (confidential).
- Some third party encryption software advertised in popular USB pendrives compatible with iDevices (base C# library now retired).
- Real-world 5G trial using eAes for encryption (TBA).
- An open-source (GPLv3-licensed) C library (TBA).



Thank you!

contact at qrcrypto dot ch (Switzerland)