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

Abstract:

Quantum computers able to crack existing encryption are due within the next decade (this decade, by the time this speech will be published), according to leading subject matter experts, coming from horizons as diverse as fundamental quantum physics, applied quantum IT research and quantum-safe cryptography.

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. 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.

On top of that, recent advances in research by Microsoft's Q# compiler (a quantum IT compiler) team, the University of Oxford and Royal Holloway, University of London, have shown that Grover would have 25% better results than expected on AES > 128, due to unforeseen compiler optimizations. All in all, this makes the case for a new class of symmetric ciphers for the post-quantum era, that do not amount to merely doubling the key size, as AES-256 and ZUC-256 do.