5G: Leap in Post-Quantum Cryptography

Basil Ugbomoiko
BTU Cottbus-Senftenberg

34th Crypto Day, 9/10 June 2022

The fifth generation of mobile broadband networks have used many cryptography techniques and theories due to the robust nature of services it is capable of providing. Previous generations used symmetric key cryptography for their privacy and security objecives and 5G used some advanced techniques for same functions. Clancy, Mcgwier & Chen (2019)

Quantum computing which relies on the laws of quantum physics largely operates on the features of Superposition and entanglement which enables it to outperform classical computers by exponentially increasing the speed of computation. While the technology was discovered in the 1980s, it has grown to become a major focal point in today's digital world.

In post-quantum cryptography, it is assumed that the hacker has a quantum computer. With this assumption in mind, new cryptosystems are developed and tested. Quantum computers will break the current cryptographic primitives hence the need for algorithms that will be secure even if the hacker has a quantum computer. This paper aims to review the deployment of 5G security features and consider the impact of Post-Quantum computing on the effectiveness of these features. Chamola, Jolfaei, Chanana, Parashari & Hassija (2021)

References

Vinay Chamola, Alireza Jolfaei, Vaibhav Chanana, Prakhar Parashari & Vikas Hassija (2021). Information Security in the Post Quantum Era for 5G and Beyond Networks: Threats to Existing Cryptography, and Post-Quantum Cryptography. *Computer Communications* **176**.

T. Clancy, Robert Mcgwier & Lidong Chen (2019). Post-quantum cryptography and 5G security: tutorial. 285–285.

Aakif Kuhafa, Gihan Niroshan, Nadeesha Rajakarunaratne & Raneesha Pomodh (2022). Cryptography in 5G - Mini Research Paper.

crypto day matters 34 (2022)
Beiträge vom 34. Kryptotag, 09.-10. Juni 2022, online.
doi:10.18420/cdm-2022-34-22