Towards Quantum-resistant Virtual Private Networks


1 ADVA Optical Networking SE
2 Fraunhofer AISEC, Weiden i. d. Opf.
3 genua GmbH
4 Ludwig-Maximilians-Universität München

31th Crypto Day, 17/18 October 2019

In 1994 mathematician Peter Shor developed an algorithm [8] requiring a quantum computer to find the prime factors of a composite number in much less time than needed today. Shor’s algorithm is especially relevant for cryptography as many encryption schemes are based on the assumption that finding prime factors of a sufficiently large number is a computationally hard problem. A quantum computer that could run Shor’s algorithm to attack today’s cryptographic schemes does not yet exist, but recent advancements in the field of quantum computing suggest that such machines may become reality in the not too distant future [1, 9]. Indeed, first experimental implementations exist, notably [4, 10].

A patient attacker may intercept today’s network traffic and use a quantum computer in the future to break the cryptography employed [7] and the fear is that secret services are actively doing so [6].

Consequently, a new class of cryptographic schemes which are secure against attacks from quantum computers is being developed and standardized [5]. Although secure against quantum attacks, those new methods typically come with severe limitations compared to the ones used today, such as huge keys or high computational requirements.

For secure network communication, most VPN solutions use a key exchange method, like the Diffie-Hellman key exchange, or an asymmetric encryption scheme, like RSA, to derive a shared session secret. To make the protocols post-quantum safe not only the cryptographic primitives have to be replaced, but also the structure of the protocol has to be modified [11, 2].

In the IPsec protocol suite, the key exchange is handled by the IKEv2 protocol [3], which by design utilizes a single Diffie-Hellman key exchange. In the talk, we give an overview of existing quantum-resistant key exchange methods and their integration into the IKEv2 protocol to defy future quantum-based attacks. We discuss the progress in the NIST standardization efforts and explain how future implementations of the IPsec protocol suite can withstand quantum attacks.
References


