PQ-WireGuard: we did it again.

Mathilde Raynal[1,2] Aymeric Genêt[1,2] Yolan Romailler[3†]

[1] École Polytechnique Fédérale de Lausanne, Switzerland
[2] Kudelski Security, Switzerland
[3] SICPA, Switzerland

Extended Abstract

Virtual Private Networks (VPN) offer security and privacy properties for internet users such as authentication, confidentiality, or identity-hiding. In 2017, Jason Donenfeld introduced WireGuard [Don17], a fast and secure open-source VPN based on "modern" cryptography that aims to replace more complex solutions such as OpenVPN. With the arrival of quantum computers, the security of these VPN solutions is threatened. A fork of OpenVPN using post-quantum alternatives was proposed by Microsoft's team [PEK], and concurrently, Hülsing and his team formally introduced quantum security in the WireGuard protocol [HNS+20]. In the quantum adversarial scenario, the PQ-WireGuard software keeps its leading role in terms of computation and communication cost over PQ-OpenVPN.

We follow the process of Hülsing et al. and integrate the Key Encapsulation Mechanism (KEM) CRYSTALS-Kyber [BDK+18]—a candidate of the NIST PQC competition—in the WireGuard protocol. Similarly, we focus on the quantum resistance of the handshake, as the data encryption itself relies on symmetric encryption, and doubling the key size is enough to obtain quantum security. The Fujioka construction [FSXY12] that lies at the core of the post-quantum handshake combines two KEMs to create a secure Authenticated Key Exchange (AKE). Post-quantum security of the AKE is obtained by using KEMs that are quantum secure. One KEM instance serves an authentication purpose and is used with long-term keys, while the second KEM instance is used with ephemeral keys. Using two Kyber instances, we build the post-quantum handshake around the Fujioka AKE construction. We then detail how we tweak the parameters of Kyber to reach more appealing results. Noticing that the decapsulation failure rate is disproportionate

[†]This work was done while working at Kudelski Security.

compared to the probability of a packet drop, we compromise on the decapsulation failure rate of the instance working with ephemeral keys and accept a rate as low as 10^{-6}. Exploiting this extra slack, we augment the outputs' compression while maintaining an acceptable decapsulation failure rate. By trial and error, we find new parameters that lead to smaller ciphertexts, a better performance, and, as a side effect, increased security with arguments that can be borrowed from schemes based on the learning with rounding problem. Because of decapsulation failure attacks, this trick cannot be applied on the Kyber instances working with long-term keys. As result, we propose a PQ-WireGuard prototype that is experimentally faster than prior work, at the cost of two additional IP packets.

We quickly observe the limitations of Kyber, and arrive at the conclusion that the need for extra IP packets cannot be removed without compromising the security or getting an excessive decapsulation failure rate. We identify the bottleneck as the ciphertext size of the Kyber instance working with long-term keys. We see that Kyber excels regarding speed performances and is a great fit where the running time is prime, whereas bandwidth-restrained scenarios can be addressed by using lighter schemes.

We then introduce a second post-quantum handshake variant using the del Pino construction [dPLP16], that combines a KEM and a Digital Signature Algorithm (DSA) to create a secure AKE. The use our optimized Kyber scheme as the KEM instance, and we show that the Rainbow signature algorithm [DS05]—another candidate of the NIST PQC standardization competition—is an excellent fit for the DSA instance because of its small signature size. As exchanging the long-term public key is a one-time cost, the relatively large public key size of Rainbow is amortized as only a 32 bytes fingerprint can be used during the frequent handshakes. As a result, we propose a PQ-WireGuard prototype that is lighter than prior work, at the cost of few milliseconds of overhead on each participant.

To conclude, we introduce in this presentation three variants of the WireGuard protocol offering post-quantum security. The last two are either experimentally faster or lighter than prior works, while remaining extremely competitive in the counterpart. The results we present should be used as motivation to start the process of integration of PQ crypto in security infrastructures.

Finally, we highlight the fact that our implementation is in Go compared to the software of Hülsing et al. which lies in the Linux kernel, and we leave for future work the port of our implementations to the Linux kernel or integration of optimizations, expecting further increase in performance.

References

[BDK+18] Joppe W. Bos, Léo Ducas, Eike Kiltz, Tancrède Lepoint, Vadim Lyubashevsky, John M. Schanck, Peter Schwabe, Gregor Seiler, and Damien Stehlé. CRYSTALS - Kyber: A CCA-secure module-lattice-based KEM. In *2018 IEEE European Symposium on Security and Privacy, EuroS&P 2018, London, United Kingdom, April 24-26, 2018*, pages 353–367. IEEE, 2018.

[Don17] Jason A. Donenfeld. WireGuard: Next generation kernel network tunnel. In *24th Annual Network and Distributed System Security Symposium, NDSS 2017, San Diego, California, USA, February 26 - March 1, 2017*. The Internet Society, 2017.

[dPLP16] Rafaël del Pino, Vadim Lyubashevsky, and David Pointcheval. The whole is less than the sum of its parts: Constructing more efficient lattice-based AKEs. In Vassilis Zikas and Roberto De Prisco, editors, *Security and Cryptography for Networks - 10th International Conference, SCN 2016, Amalfi, Italy, August 31 - September 2, 2016, Proceedings*, volume 9841 of *Lecture Notes in Computer Science*, pages 273–291. Springer, 2016.

[DS05] Jintai Ding and Dieter Schmidt. Rainbow, a new multivariable polynomial signature scheme. In John Ioannidis, Angelos Keromytis, and Moti Yung, editors, *Applied Cryptography and Network Security*, pages 164–175, Berlin, Heidelberg, 2005. Springer Berlin Heidelberg.

[FSXY12] Atsushi Fujioka, Koutarou Suzuki, Keita Xagawa, and Kazuki Yoneyama. Strongly secure authenticated key exchange from factoring, codes, and lattices. In Marc Fischlin, Johannes Buchmann, and Mark Manulis, editors, *Public Key Cryptography – PKC 2012*, pages 467–484, Berlin, Heidelberg, 2012. Springer Berlin Heidelberg.

[HNS+20] Andreas Hülsing, Kai-Chun Ning, Peter Schwabe, Florian Weber, and Ralf Zimmermann. Post-quantum WireGuard. *IACR Cryptol. ePrint Arch.*, 2020:379, 2020.

[PEK] Christian Paquin, Karen Easterbrook, and Kevin Kane. Post-quantum Cryptography VPN.