PQC Wireguard as a new VPN

Wireguard + Rosenpass

Philip Kastura-Sahl
philip.kastura-sahl@stud.uni-heidelberg.de
Ruprecht-Karls-Universität Heidelberg
Heidelberg, Germany

ABSTRACT

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Pellentesque eget ex ex. Etiam ultricies mi sit amet sem malesuada, nec egestas est gravida. Cras eu sagittis est. Nunc dignissim massa vel mauris varius pulvinar. Duis quis massa quis quam commodo pulvinar et ac quam. In hac habitasse platea dictumst. Nunc eu lacus mi. Donec a efficitur leo.

CCS CONCEPTS

• **Security and privacy** → *Key management*; **Digital signatures**; **Public key encryption**.

KEYWORDS

Post-quantum cryptography, Key-Encapsulation Method, Rosenpass, Wireguard, Crystals-Kyber, NIST

ACM Reference Format:
Philip Kastura-Sahl. 2024. PQC Wireguard as a new VPN: Wireguard + Rosenpass. In *Proceedings of IT-Security Seminar (ITSEC).* ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 LOREM IPSUM

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Pellentesque eget ex ex. Etiam ultricies mi sit amet sem malesuada, nec egestas est gravida. Cras eu sagittis est. Nunc dignissim massa vel mauris varius pulvinar. Duis quis massa quis quam commodo pulvinar et ac quam. In hac habitasse platea dictumst. Nunc eu lacus mi. Donec a efficitur leo.[1]

ITSEC, WiSe 2023/24, Heidelberg

ACM ISBN 978-x-xxxx-xxxx-x/YY/MM
https://doi.org/10.1145/nnnnnnn.nnnnnnn

Mauris a sodales ligula, id dictum arcu. Morbi ante nisl, vestibulum sed mauris vitae, vestibulum efficitur lacus. Maecenas laoreet lorem quis dui posuere convallis. Curabitur ac justo vel enim dictum rutrum id et nunc. Nunc porta lacus quis odio dignissim, quis tristique libero fringilla. Cras eleifend dictum molestie. Quisque ut leo nec ipsum suscipit imperdiet lobortis et turpis. Proin eget luctus nibh. Maecenas in finibus turpis. Integer dictum felis in purus malesuada finibus.[2]

2 SUSPENDISSE ORCI

Suspendisse orci purus, tincidunt sit amet metus eu, lacinia vehicula nulla. Phasellus lobortis ullamcorper mi vitae fringilla. Integer ante risus, condimentum at turpis nec, fringilla laoreet ante. Ut fringilla congue vestibulum. Cras placerat aliquet dolor, in consectetur elit dignissim id. Curabitur varius, erat et auctor cursus, urna leo ullamcorper ex, ut dictum nunc nisi eu mauris. Cras porttitor felis sed sem consectetur rhoncus nec a mauris. Curabitur mollis nisl nec purus bibendum efficitur. Integer posuere eleifend bibendum. Nulla dapibus, mauris nec consequat pulvinar, ante turpis mattis sapien, id fringilla enim diam ac nibh. Phasellus facilisis dolor ac est rhoncus, in dignissim lectus tincidunt.[8]

2.1 In ac malesuada

In ac malesuada eros. Donec eu quam nec quam commodo eleifend. Vestibulum ut ultrices tellus. Praesent varius rhoncus nisi at aliquet. Donec scelerisque, tellus quis auctor congue, mi nunc pharetra est, ut mollis orci dolor quis odio. Proin pellentesque eget quam vel tempus. Etiam viverra turpis id malesuada ultrices. Suspendisse sit amet lorem vel elit pretium sollicitudin. Suspendisse tincidunt semper urna, nec condimentum lorem consectetur ut. Aliquam elit nisl, vehicula vitae sollicitudin eget, dictum non eros.[3]

Vivamus ornare ex eget risus placerat placerat. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos himenaeos. Quisque eu risus ut nunc bibendum rhoncus non a urna. Nam sollicitudin, nibh ut laoreet vestibulum, dui lorem semper turpis, at rhoncus nulla sem molestie erat. Nulla eget interdum sem.

Donec sed purus vel ex cursus venenatis. Duis maximus purus a velit pellentesque viverra. Morbi posuere faucibus rhoncus. Mauris volutpat viverra nisl in pellentesque.[4][6]

Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia curae; Praesent ullamcorper faucibus odio, eget blandit quam consequat sed. In hac habitasse platea dictumst. Maecenas nec purus vel mauris tempor sagittis id non sem. Vestibulum tempus, enim nec consequat fermentum, ipsum orci finibus urna, a hendrerit risus nisi eu urna. Ut quis massa ullamcorper, accumsan ante vitae, cursus turpis. Aliquam erat volutpat. Duis sit amet purus fringilla, rhoncus elit at, consectetur nunc.[5]

3 CRAS EUISMOD

Cras euismod sapien quam, non convallis mi euismod sed. Quisque dapibus orci a sem ornare, a imperdiet magna rutrum. Praesent luctus enim in pulvinar ullamcorper. Ut sem eros, tincidunt eu urna in, egestas ullamcorper leo. Suspendisse ante tortor, elementum eget libero iaculis, egestas semper ex. Etiam ut sapien accumsan nisi egestas bibendum vel a enim. Suspendisse sagittis nisl ut pharetra rutrum. Vivamus sed consectetur felis. Ut commodo erat id semper laoreet.[7]

4 DONEC FRINGILLA

Donec fringilla mi feugiat vestibulum porttitor. Mauris dictum risus in diam rutrum pharetra. Nulla efficitur libero at eros pretium vestibulum. Fusce eget erat molestie, porttitor ipsum et, venenatis dui. Cras id iaculis dolor, sed mollis odio. Nunc hendrerit quam et dolor accumsan gravida. Nam sapien lacus, maximus vel semper at, feugiat in lacus. Donec suscipit in mauris vitae porta.[9]

ACKNOWLEDGMENTS

I would like to express my sincere gratitude to the following individuals and teams who have contributed to the completion of this document:

- Prof. Dr. Heuveline & Mr. Machmeier for their guidance and support throughout the research and writing process.
- The Wireguard & Rosenpass teams for their respective Projects, their novice-friendly documentation, and beginner-friendly explainers.

I am truly thankful for their dedication and collaboration, which has significantly enriched the quality of this work.

REFERENCES

[1] [n. d.]. . https://www.ndss-symposium.org/ndss2017/ndss-2017-programme/wireguard-next-generation-kernel-network-tunnel/
[2] [n. d.]. . https://rosenpass.eu/whitepaper.pdf
[3] [n. d.]. . https://www.openssl.org/docs/man3.2/man3/EVP_EncryptInit_ex.html
[4] [n. d.]. . https://arstechnica.com/information-technology/2022/08/sike-once-a-post-quantum-encryption-contender-is-koed-in-nist-smackdown/
[5] [n. d.]. . https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization
[6] Wouter Castryck and Thomas Decru. 2022. An efficient key recovery attack on SIDH. Cryptology ePrint Archive, Paper 2022/975. https://eprint.iacr.org/2022/975 https://eprint.iacr.org/2022/975.
[7] Diana Ghinea, Fabian Kaczmarczyck, Jennifer Pullman, Julien Cretin, Stefan Kölbl, Rafael Misoczki, Jean-Michel Picod, Luca Invernizzi, and Elie Bursztein. 2022. Hybrid Post-Quantum Signatures in Hardware Security Keys. Cryptology ePrint Archive, Paper 2022/1225. https://eprint.iacr.org/2022/1225 https://eprint.iacr.org/2022/1225.
[8] Andreas Hülsing, Kai-Chun Ning, Peter Schwabe, Fiona Johanna Weber, and Philip R. Zimmermann. 2020. Post-quantum WireGuard. Cryptology ePrint Archive, Paper 2020/379. https://eprint.iacr.org/2020/379 https://eprint.iacr.org/2020/379.
[9] Douglas Stebila and Michele Mosca. 2016. Post-Quantum Key Exchange for the Internet and the Open Quantum Safe Project. Cryptology ePrint Archive, Paper 2016/1017. https://eprint.iacr.org/2016/1017 https://eprint.iacr.org/2016/1017.

Talk 18 January 2024; Paper 32 Columbus 2024