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

With the advance of quantum computers, security researchers face the challenge of securing their data against *"Harvest now, decrypt later"-attacks* that could become available in the future. Shor's algorithm[17], when implemented on a sufficiently powerful quantum computer, could be used to break many public-key cryptography schemes. Rosenpass aims to provide a *post-quantum-secure authenticated key exchange* that works in a *hybrid post-quantum security scheme* together with WireGuard. Due to the ongoing development of Post-quantum-Ciphers, Rosenpass is implemented to provide hybrid post-quantum security in tandem with WireGuard[3].

CCS CONCEPTS

• **Security and privacy** → *Security protocols*; **Web protocol security**; **Public key encryption**; **Key management**; Security requirements.

KEYWORDS

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

ACM Reference Format:
Philip Kastura-Sahl. 1980. PQC WireGuard as a new VPN: WireGuard + Rosenpass. In *Proceedings of IT-Security Seminar (ITSEC).* ACM, New York, NY, USA, 3 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

ITSEC, WiSe 2023/24, Heidelberg

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

1 INTRODUCTION

Shor's Algorithm, developed in 1994 by Peter Shor, is one of the few known algorithms that could be used to break existing public key cryptography such as RSA and some Diffie-Hellman variants. With the rise of ever more powerful quantum computers, security researchers are facing the possibility of traditional *pre-quantum cryptography* becoming insecure. The Open Quantum Safe Project[1] & NIST[1] aim to improve and standardize *post-quantum cryptography* to the point of it being able to supersede existing schemes that would be deemed insecure using sufficiently powerful quantum computers.
PQ-WireGuard[13] first modified WireGuard and implemented new PQ[2] forward secrecy & pq Authentication by replacing the Diffie-Hellman handshake with a key-encapsulation mechanism[3].

1.1 WireGuard & Rosenpass

WireGuard is a modern VPN that intends to be more performant than OpenVPN, whilst being able to run on a variety of computers and platforms[4]. Rosenpass functions as an Add-on to WireGuard, adding PQC[4] whilst keeping the established security intact. Whilst some WireGuard implementations are considered complete[5], Rosenpass is still under development[6]. Apart from implementing PQC, Rosenpass also implements a statless responder to protect against replay attacks of the first protocol message.

1.2 Problem Definition

Even though Quantum Computers don't yet have a sufficient number of qubits, data could be harvested already, making it vulnerable to decryption attacks in the future, a surveillance strategy known as *Harvest now, decrypt later*. Yet PQC has not yet reached the point of adoption to be replacing pre-quantum cryptography, as seen in

[1] NIST – National Institute of Standards and Technology
[2] pq – post-quantum
[3] KEM – key-encapsulation mechanism
[4] PQC – post-quantum cryptography

the Post-Quantum Cryptography Standardization effort where algorithms such as SIDH have been eliminated due to major security flaws in their design[10]. Therefore, Rosenpass has been designed to implement Hybrid PQC[12], Rosenpass providing encryption deemed the most post-quantum resistant and working together with the known to be pre-quantum secure WireGuard. The handshake between WireGuard and Rosenpass as well as the individual connections between Rosenpass and WireGuard Clients and Server needed to be designed in such a way that neither one of the ciphers could be broken alone so that a potential attacker would need to always attack both ciphers.

2 CIPHERS

The Rosenpass developers have chosen a combination of Classic McEliece and CRYSTALS-Kyber, notably finalists of the NIST Post-Quantum Cryptography Standardization effort[2]. While symmetric ciphers are generally considered to be secure, not all asymmetric ciphers are equally vulnerable to Shor's algorithm.

2.1 KEM vs. NIKE

Established asymmetric ciphers *Non-Interactive Key Exchange*, as the name implies, this enables two parties to know each other's public keys and agree on a symmetric shared key without requiring any interaction[11]. While a NIKE[5] is not inherently insecure against attacks by quantum computers, PQC usually relies on a *Key encapsulation mechanism*. KEMs[6] are considered a more viable solution, because they are able to provide both pq-resistance as well as today's security guarantees. Hybrid PQC can be implemented using KEMs by using a combiner, which enables the use of multiple algorithms while keeping the scheme secure as long as one of the algorithms remains secure[9].

2.2 Classic McElice

Classic McEliece decodes linear codes using an algorithm that introduces errors and derives a public key using *binary goppa codes*. Binary goppa codes are error correcting code from the class of general Goppa codes, they can be used to encode messages whilst introducing errors[8]. The Classic McEliece public keys tend to be larger than other ciphers, at least 261120 Bytes$^{(\text{for mceliece348864})}$, whereas their ciphertext is 96 Bytes$^{(\text{for mceliece348864})}$.

2.3 Kyper

Lattice-based ciphers such as CRYSTALS-Kyber are based on *lattice problems* such as the *Shortest Vector Problem* and *Learning with Errors*[16].
The SVP[7] is considered solved if the shortest possible vector measured by a given norm is found for a given lattice. Algorithms to solve SVP such as LLL[8] lattice basis reduction algorithm often require polynomial time

$$O(d^5 n \log^3 B)$$

, where

$$B = \max(\|b_1\|_2, \|b_2\|_2, \ldots, \|b_d\|_2)$$

[15], due to their complexity SVP is considered to be secure against traditional and quantum computers[7].
LWE[9] is a problem of differentiating random from uniform linear equations[14], it can be used to obfuscate the secret by introducing noise into the linear equations used inside the cipher.

3 IMPLEMENTATION

The Rosenpass Team has chosen to develop Rosenpass alongside WireGuard as an Add-on. Contrary to its predecessor WireGuard-PQ, Rosenpass only implements the post-quantum side and relies on WireGuard to provide sufficient pre-quantum security such that the entire system works as a hybrid post-quantum security scheme. This approach requires the development teams of both Rosenpass and WireGuard to work together to ensure compatibility, as well as administrators and users willingness to keep their installed Rosenpass and WireGuard versions compatible. Yet, choosing this approach enables the Rosenpass Team to focus solely on the development and proofing of Rosenpass without the technological depth of maintaining the pre-quantum security.

3.1 Proof

The Rosenpass Team provides a symbolic analysis using the *proverif* tool. Using proverif an automated security analysis can be executed on the provided Rosenpass implementations. A cryptographic proof of security is currently worked on, but has not yet been published[6][As of 10.03.2024].

3.2 Key Exchange

The Rosenpass Handshake works much like the traditional WireGuard handshake, needing to be refreshed every 2 minutes. Apart from using PQC, it differentiates itself by ensuring Non-Interruptibility through the use of a *Biscuit*. WireGuard provides Non-Interruptibility by including a Timestamp, the Rosenpass Team has wrapped the *Responder State* inside a Cookie, dubbed *Biscuit*[6].
For a visualization, see A.1.

3.3 WireGuard-Rosenpass Handshake

The Handshake between WireGuard and Rosenpass ensures that the Connection remains secure at all times. When the connection between WireGuard and its Client gets disconnected the entire communication naturally breaks down, Rosenpass is implemented to provide a *PSK* to WireGuard. When the Rosenpass Handshake fails, the PSK upon which WireGuard depends when working together with Rosenpass gets corrupted, prompting WireGuard to pause any communication, until both Handshakes work again[6].
For a visualization, see A.2.

4 CONCLUSION

Rosenpass poses a viable solution to secure networks against *"Harvest now, decrypt later"-attacks*, yet there is still a need for further development. A Proof of cryptographic security is still under development and the security of existing PQC remain unclear.

[5] NIKE – Non-Interactive Key Exchange
[6] KEM – Key encapsulation mechanism
[7] SVP – Shortest Vector Problem
[8] LLL – Lenstra–Lenstra–Lovász
[9] LWE – Learning with Errors

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.

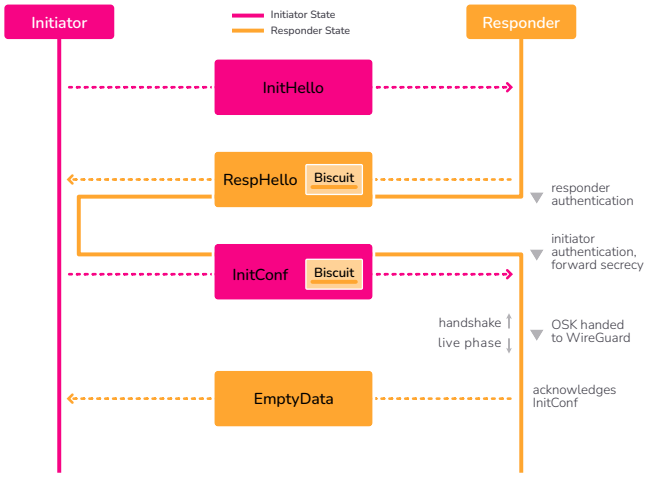
I am truly thankful for their dedication and collaboration, which has significantly enriched the quality of this work.

REFERENCES

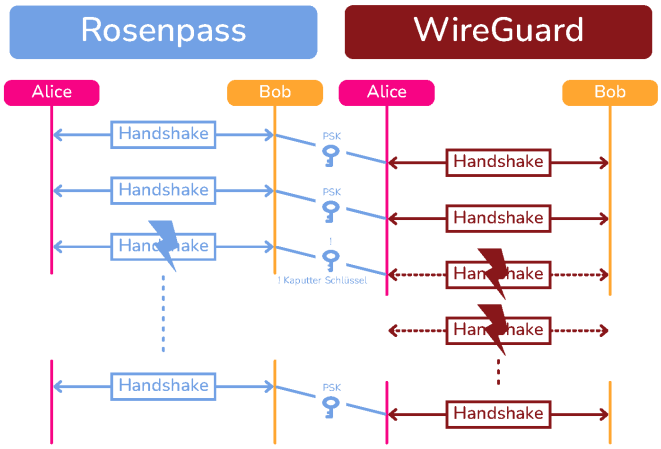
[1] [n. d.]. *Open Quantum Safe project.* https://openquantumsafe.org/about/#overview [Accessed 10.03.2024].
[2] [n. d.]. *Post-Quantum Cryptography Standardization.* https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization [Accessed 10.03.2024].
[3] [n. d.]. *Rosenpass – About.* https://rosenpass.eu/about/ [Accessed 10.03.2024].
[4] [n. d.]. *WireGuard: Next Generation Kernel Network Tunnel.* https://www.ndss-symposium.org/ndss2017/ndss-2017-programme/wireguard-next-generation-kernel-network-tunnel/ [Accessed 10.03.2024].
[5] [n. d.]. *Wireguard: Source Code Repositories and Official Projects.* https://www.wireguard.com/repositories/ [Accessed 10.03.2024].
[6] 2023. *Rosenpass Whitepaper.* https://rosenpass.eu/whitepaper.pdf [Accessed 10.03.2024].
[7] Gorjan Alagic, David Cooper, Quynh Dang, Thinh Dang, John M. Kelsey, Jacob Lichtinger, Yi-Kai Liu, Carl A. Miller, Dustin Moody, Rene Peralta, Ray Perlner, Angela Robinson, Daniel Smith-Tone, and Daniel Apon. 2022. Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process. https://doi.org/10.6028/NIST.IR.8413
[8] E. Berlekamp, R. McEliece, and H. van Tilborg. 1978. On the inherent intractability of certain coding problems (Corresp.). *IEEE Transactions on Information Theory* 24, 3 (1978), 384–386. https://doi.org/10.1109/TIT.1978.1055873
[9] Nina Bindel, Jacqueline Brendel, Marc Fischlin, Brian Goncalves, and Douglas Stebila. 2018. Hybrid Key Encapsulation Mechanisms and Authenticated Key Exchange. Cryptology ePrint Archive, Paper 2018/903. https://doi.org/10.1007/978-3-030-25510-7_12 https://eprint.iacr.org/2018/903.
[10] 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.
[11] Eduarda S. V. Freire, Dennis Hofheinz, Eike Kiltz, and Kenneth G. Paterson. 2012. Non-Interactive Key Exchange. Cryptology ePrint Archive, Paper 2012/732. https://eprint.iacr.org/2012/732 https://eprint.iacr.org/2012/732.
[12] 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.
[13] 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.
[14] Vadim Lyubashevsky, Chris Peikert, and Oded Regev. 2013. On Ideal Lattices and Learning with Errors over Rings. *J. ACM* 60, 6, Article 43 (nov 2013), 35 pages. https://doi.org/10.1145/2535925
[15] Phong Q. Nguyen and Damien Stehlé. 2009. An LLL Algorithm with Quadratic Complexity. *SIAM J. Comput.* 39, 3 (2009), 874–903. https://doi.org/10.1137/070705702 arXiv:https://doi.org/10.1137/070705702
[16] Oded Regev. 2009. On lattices, learning with errors, random linear codes, and cryptography. *J. ACM* 56, 6, Article 34 (sep 2009), 40 pages. https://doi.org/10.1145/1568318.1568324
[17] Peter W. Shor. 1997. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM J. Comput.* 26, 5 (Oct. 1997), 1484–1509. https://doi.org/10.1137/s0097539795293172

A IMPLEMENTATION

A.1 Key Exchange



A.2 WireGuard-Rosenpass Handshake



Talk 18 January 2024; Paper 31 March 2024