h_da
HOCHSCHULE DARMSTADT
UNIVERSITY OF APPLIED SCIENCES

Hochschule Darmstadt

– Fachbereich Informatik –

Performanz Evaluation von PQC in der Authentifizierungsphase von TLS 1.3 unter variierenden Netzwerkcharakteristiken

Abschlussarbeit zur Erlangung des akademischen Grades

Bachelor of Science (B.Sc.)

vorgelegt von

Ronja Wolf

Matrikelnummer: 761118

Referent	:	Prof. Dr. Andreas Heinemann
Korreferent	:	Johanna Henrich

ERKLÄRUNG

Ich versichere hiermit, dass ich die vorliegende Arbeit selbstständig verfasst und keine anderen als die im Literaturverzeichnis angegebenen Quellen benutzt habe.

Alle Stellen, die wörtlich oder sinngemäß aus veröffentlichten oder noch nicht veröffentlichten Quellen entnommen sind, sind als solche kenntlich gemacht.

Die Zeichnungen oder Abbildungen in dieser Arbeit sind von mir selbst erstellt worden oder mit einem entsprechenden Quellennachweis versehen.

Diese Arbeit ist in gleicher oder ähnlicher Form noch bei keiner anderen Prüfungsbehörde eingereicht worden.

Darmstadt, 05. Dezember 2022

Ronja Wolf

INHALTSVERZEICHNIS

ABBILDUNGSVERZEICHNIS

ABKÜRZUNGSVERZEICHNIS

AES Advanced Encryption Standard

CRYSTALS Cryptographic Suite for Algebraic Lattices

DES Data Encryption Standard

ECDH Elliptic-curve Diffie-Hellman

ECDSA Elliptic Curve Digital Signature Algorithm

EdDSA Edwards-curve Digital Signature Algorithm

FALCON Fast Fourier lattice-based compact signatures over NTRU

GAN Global Area Network

IETF Internet Engineering Task Force

NIST National Institute of Standards and Technology

OQS Open Quantum Safe

OSI Open Systems Interconnection

PAN Personal Area Network

PQC Post-Quanten-Kryptographie

RSA Rivet-Shamir-Adleman

TLS Transport Layer Security

Teil I

THESIS

1 EINLEITUNG

In Transport Layer Security (TLS) 1.3 wird ein Handshake durchgeführt, bei dem ein Schlüsselaustausch sowie die Authentifizierung des Servers gegenüber dem Client durchgeführt wird. Bei Bedarf kann auch eine beidseitige Authentifizierung durchgeführt werden. Erst im Anschluss findet die eigentliche Kommunikation statt. Aktuell werden dabei für die Authentifizierung die klassischen asymmetrischen Verfahren Edwards-curve Digital Signature Algorithm (EdDSA), Elliptic Curve Digital Signature Algorithm (ECDSA) und Rivet-Shamir-Adleman (RSA) verwendet. In dieser Arbeit soll betrachtet werden, inwiefern sich die Performanz von TLS 1.3 verändert, wenn stattdessen Post-Quanten-Kryptographie (PQC) Verfahren, d. h. kryptographische Verfahren, die gegen Quantencomputer resistent sind, eingesetzt werden.

1.1 MOTIVATION

Die Entwicklung von Quantencomputern schreitet voran. Wenn Quantencomputer jedoch einsatzfähig sind, wird es mit ihnen möglich sein, viele der aktuell verwendeten kryptographischen Algorithmen zu brechen. Dies liegt daran, dass diese auf Berechnungen basieren, die auf klassischen Computern nicht in einer vertretbaren Zeit durchführbar sind. Dies sind vor allem die Primfaktorzerlegung und der diskrete Logarithmus. Quantencomputer können diese Berechnungen aufgrund ihrer Eigenschaften jedoch schneller durchführen. Davon sind auch die im TLS 1.3 Handshake verwendeten Algorithmen betroffen.

Um zu verhindern, dass hierdurch Probleme entstehen, müssen rechtzeitig PQC-Algorithmen identifiziert werden, mit denen die dann unsicherern Algorithmen ersetzt werden können. Dabei ist zu beachten, dass diese andere Charakteristika haben. Damit der Einsatz von PQC-Algorithmen gelingen kann, muss bekannt sein, wie sich diese unter verschiedenen Netzwerkbedingungen verhalten.

1.2 PROBLEMSTELLUNG UND ZIEL

In dieser Arbeit sollen die klassischen kryptographischen Algorithmen, die bei TLS 1.3 zur Authentifizierung verwendet werden, durch PQC-Algorithmen, wie z. B. Fast Fourier lattice-based compact signatures over NTRU (FALCON), ersetzt werden. In dem Auswahlprozess der National Institute of Standards and Technology (NIST) haben sich dabei besonders Cryptographic Suite for Algebraic Lattices (CRYSTALS) Dilithium, FALCON und SPHINCS+ als vielversprechende Kandidaten für Algorithmen zur digitalen Signatur hervorge-

tan.

Allerdings ist in der realen Welt kein ideales Netzwerk vorhanden und es treten Störfaktoren, wie etwa der Verlust von Paketen oder Latenz auf. Diese Störfaktoren haben einen Einfluss auf die Performanz des Algorithmus. Da TLS 1.3 jedoch ein Protokoll ist, das an verschiedenen Stellen in der Praxis zum Einsatz kommt und hier die Performanz durchaus eine wichtige Rolle spielt, ist die Performanz für den Benutzer von großer Bedeutung.

In dieser Arbeit soll zunächst nur die Authentifizierung mittels PQC-Verfahren durchgeführt werden. Es wird angenommen, dass für den Schlüsselaustausch ein klassisches Verfahren verwendet wird. Dieses bleibt bei allen Versuchen unverändert, sodass nur Auswirkungen durch die Verwendung von PQC-Algorithmen in der Authentifizierungsphase auf die Performanz des TLS-Handshake bewertet werden.

Die konkrete Fragestellung der Arbeit ist, inwiefern sich die Performanz des Handshakes von TLS 1.3 unter der Verwendung verschiedener PQC-Algorithmen in der Authentifizierungsphase verändert, wenn verschiedene Netzwerkparameter manipuliert werden.

Ziel der Arbeit ist es, daraus ableiten zu können, welche Algorithmen für die Verwendung in der Authentifizierungsphase von TLS 1.3 unter realen Netzwerkbedingungen geeignet sind. Dies ist relevant für die Verwendung des Algorithmus in einer Netzwerkumgebung.

1.3 RELATED WORK

Crockett et al. entwarfen 2019 eine Implementierung von PQC im TLS 1.3 Handshake. Dabei wurden verschiedene, in der Literatur vorhandene Grundkonzepte diskutiert [CPS19]. Dabei geben sie eine Empfehlung, wie eine Implementierung aussehen kann. In der Arbeit selbst wird darauf hingewiesen, dass eine Prüfung der Algorithmen sowohl unter Veränderung einzelner Netzwerkparameter als auch unter realistischen Netzwerkbedingungen notwendig ist.

Paul et al. untersuchten 2022, wie Zertifkatsketten für die Authentifizierung mit PQC-Verfahren aussehen könnten [Pau+22]. Dabei verwenden sie "Mixed Certificate Chains", bei denen innerhalb derselbsen Zertifikatskette verschiedene Algorithmen angewandt werden. Diese Arbeit soll diese Konzepte aufgreifen, sie betrachtet jedoch, wie sich die Performanz des Handshakes bei der Veränderung einzelner Netzwerkparameter verhält.

Henrich hat in ihrer Masterarbeit untersucht, wie sich die Verwendung von PQC-Algorithmen im Schlüsselaustausch von TLS1.3 unter veschiedenen Netzwerkbedingungen verhält [Hen22]. Sie kommt dabei zu dem Ergeb-

nis, dass insbesondere Kyber, Saber, NTRU und NTRU Prime auch bei variierenden Netzwerkparametern eine sehr gute Performanz haben und teils noch schneller als Elliptic-curve Diffie-Hellman (ECDH) sind. In Analogie dazu soll in dieser Arbeit die Authentifizierung betrachtet werden.

Das dabei verwendete Framework zur Emulation verschiedener Netzwerkszenarien wurde in einer Arbeit von Paquin et al. aus dem Jahr 2020 [PST20] vorgestellt.

Eine weitere Arbeit in diesem Bereich stammt von Sikeridis et al. aus dem Jahr 2020 und beschäftigt sich bereits mit der Performanz von PQC-Verfahren zur Authentikation in TLS 1.3 [SKD20]. In dieser Arbeit wurde der TLS 1.3 Handshake zwischen einem Client und realen Servern in verschiedenen Staaten durchgeführt, um zu überprüfen, inwiefern dies Auswirkungen auf die Performanz der Algorithmen hat. Diese Arbeit soll sich davon abgrenzen, indem sie gezielt einzelne Netzwerkparameter in einer Emulation manipuliert. Damit soll herausgefunden werden, welche Parameter einen entscheidenden Einfluss auf die Performanz haben.

1.4 VORGEHENSWEISE

Für diese Arbeit soll in einem Linux-Kernel der Aufbau einer TLS 1.3 Verbindung zwischen einem Server und einem Client durchgeführt werden. Dies geschieht unter verschiedenen Netzwerkparametern sowie mit verschiedenen PQC-Algorithmen in der Authentifizierungsphase von TLS 1.3.

Dafür wird für verschiedene PQC-Algorithmen eine Reihe an Versuchen durchgeführt, in denen verschiedene Netzwerkcharakteristiken verändert werden. Nach der erfolgreichen Authentifizierung des Servers gegenüber dem Client wird die Verbindung abgebrochen. Die Zeit zwischen dem Aufbau und dem Abbau der Verbindung wird gemessen und dient als Vergleichsgröße. Diese Versuche sollen ebenfalls unter verschiedenen Sicherheitsleveln durchgeführt werden.

Für den Verbindungsaufbau zwischen Client und Server werden Linux-Kernel-Tools verwendet. Die verschiedenen Netzwerkparameter werden mithilfe des Tools NetEm emuliert. Dabei sollen Veränderungen an folgenden Parametern betrachtet werden:

- Duplikate
- Jitter
- Korrupte Pakete
- Latenz

- Paketverlust
- Reordering
- Übertragungsrate

Diese werden zunächst einzeln betrachtet. Da sie in der Realität jedoch gemeinsam auftreten, können in einem späteren Versuch auch verschiedene Netzwerkparameter miteinander kombiniert werden.

Die eigentliche Authentifizierung wird mithilfe der Open Quantum Safe (OQS) Library [SM17] durchgeführt. Aufgrund des aktuellen Stands der NIST-Empfehlungen werden die folgenden Algorithmen betrachtet:

- SPHINCS$^+$
- Dilithium
- Falcon

Gegebenenfalls sollen die Ergebnisse in einer realen Netzwerkumgebung mit einem Server aus einer Cloudinstanz bestätigt werden. Dies soll jedoch nicht Kern der Arbeit sein.

Nach der Durchführung der Versuche sollten ausführliche Daten dazu vorliegen, wie sich die Laufzeit von TLS 1.3 unter verschiedenen Algorithmen, Algorithmenparametern und Netzwerkcharakteristiken verhält. Diese sollen im Anschluss miteinander verglichen werden.

Dabei werden sich voraussichtlich große Unterschiede zwischen den betrachteten Algorithmen zeigen. Aus dem Vergleich der Performanz von TLS 1.3 soll eine Empfehlung gegeben werden, welche Algorithmen für welche Art von Netzwerk am besten geeignet sind.

2 GRUNDLAGEN

2.1 NETZWERKE

Ein Computernetzwerk besteht mindestens aus zwei Computern, einem Übertragungsmedium und Protokollen, die festlegen, in welcher Form die Computer Daten austauschen Ein Computernetz kann sich physisch über einige Meter (dann spricht man von einem Personal Area Network (PAN)) bis über die gesamte Erde (dann spricht man von einem Global Area Network (GAN)) ausdehnen. Das Internet ist ein GAN. [Bau18a].

Beim Open Systems Interconnection (OSI) Referenzmodell (vgl. Abbildung 2.1) wird eine Netzwerkverbindung in sieben logische Schichten unterteilt. Es wird verwendet, um eine Kommunikation über ein Netzwerk darzustellen. Die einzelnen Schichten sind dabei durch Schnittstellen miteinander verbunden, sodass einzelne Protokolle leicht ausgetauscht werden können [Bau18b]

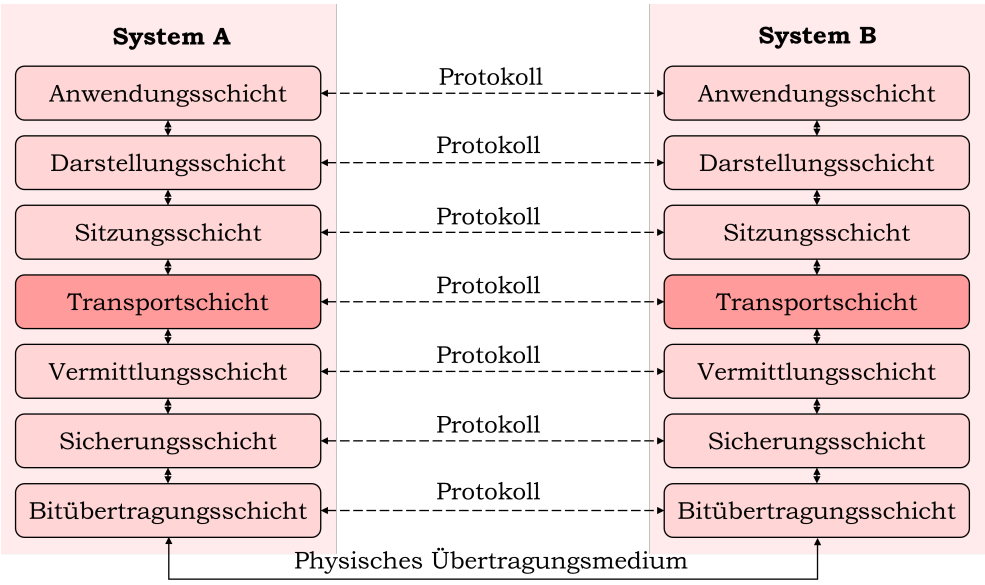

Abbildung 2.1: OSI-Referenzmodell mit hervorgehobener Transportschicht

2.2 KRYPTOGRAPHIE

Der Begriff Kryptographie bezeichnet die "Wissenschaft vom geheimen Schreiben" [Wät18]. Dabei wird der verschlüsselte Text als "Chiffretext" und der entschlüsselte Text als "Klartext" bezeichnet. Das Gegenstück der Kryptogra-

phie ist die Kryptanalyse, deren Ziel es ist, Kryptographie zu brechen. Kryptographie und Kryptanalyse bilden das Fachgebiet der Kryptologie [PP10].

2.3 TRANSPORT LAYER SECURITY

TLS ist ein 1996 durch die Internet Engineering Task Force (IETF) festgelegtes Protokoll mit dem Ziel, einen Standard für die sichere Kommunikation im über das Internet zu finden. Das Protokoll agiert auf der Transportschicht. Während die ursprünglichen Ziele des Protokolls Datensicherheit und -integrität waren, wurde in späteren Versionen zunehmend auch die Kommunikation mit anderen TLS-Versionen sowie die Möglichkeit des Ausbaus des Protokolls, z. B. durch neue Algorithmen, betrachtet [Kiz20].

2.4 POST-QUANTUM-KRYPTOGRAPHIE UND NIST

2.4.1 *Quanteninformatik*

Während die klassische Einheit in der Informatik aus einem Bit entstehen kann, das entweder den Wert 0 oder den Wert 1 annehmen kann, wird die Grundlage der Quanteninformatik durch sogenannte Qubits gebildet. Diese unterscheiden sich in einigen wesentlichen Punkten von den klassischen Bits [Jus20]:

1. Während der Wert eines klassischen Bits zu jedem Zeitpunkt eindeutig als 0 oder 1 identifiziert werden kann, können Qubits auch einen Wert zwischen 0 und 1 annehmen.
2. Wird der Wert eines Qubits gemessen, ist dieser immer 0 oder 1. Der Wert eines Qubits kann sich demnach durch die Messung verändern.
3. Eine Veränderung in einem Qubit kann eine instantane Veränderung in einem anderen Qubit hervorrufen.

2.4.2 *National Institute of Standards and Technology*

Das National Institute of Standards and Technology (übersetzt Nationales Institut für Standards und Technoligue) ist eine Bundesbehörde der Vereinigten Staaten, deren Hauptaufgabe Standardisierungsprozesse sind. In der Kryptographie war das NIST u. a. dafür verantwortlich, die Verschlüsselungsstandards Advanced Encryption Standard (AES) und Data Encryption Standard (DES) zu standardisieren.

LITERATUR

[Bau18a] Christian Baun. "Grundlagen der Computervernetzung". In: *Computernetze kompakt*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2018, S. 15–33. ISBN: 978-3-662-57469-0. DOI: 10.1007/978-3-662-57469-0_3. URL: https://doi.org/10.1007/978-3-662-57469-0_3.

[Bau18b] Christian Baun. "Protokolle und Protokollschichten". In: *Computernetze kompakt*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2018, S. 35–44. ISBN: 978-3-662-57469-0. DOI: 10.1007/978-3-662-57469-0_4. URL: https://doi.org/10.1007/978-3-662-57469-0_4.

[CPS19] Eric Crockett, Christian Paquim und Douglas Stebila. *Prototyping post-quantum and hybrid key exchange and authentication in TLS and SSH*. 2019.

[Hen22] Johanna Henrich. "Performanz Evaluation von PQC in TLS 1.3 unter variierenden Netzwercharakteristiken". Magisterarb. Hochschule Darmstadt, 2022.

[Jus20] Bettina Just. "Einführung". In: *Quantencomputing kompakt: Spukhafte Fernwirkung und Teleportation endlich verständlich*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2020, S. 1–4. ISBN: 978-3-662-61889-9. DOI: 10.1007/978-3-662-61889-9_1. URL: https://doi.org/10.1007/978-3-662-61889-9_1.

[Kiz20] Joseph Migga Kizza. "Computer Network Security Protocols". In: *Guide to Computer Network Security*. Cham: Springer International Publishing, 2020, S. 367–398. ISBN: 978-3-030-38141-7. DOI: 10.1007/978-3-030-38141-7_17. URL: https://doi.org/10.1007/978-3-030-38141-7_17.

[PP10] Christof Paar und Jan Pelzl. "Introduction to Cryptography and Data Security". In: *Understanding Cryptography: A Textbook for Students and Practitioners*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, S. 1–27. ISBN: 978-3-642-04101-3. DOI: 10.1007/978-3-642-04101-3_1. URL: https://doi.org/10.1007/978-3-642-04101-3_1.

[PST20] Christian Paquin, Douglas Stebila und Goutam Tamvada. "Benchmarking Post-quantum Cryptography in TLS". In: *International Conference on Post-Quantum Cryptography*. 2020.

[Pau+22] Sebastian Paul, Norman Lahr, Yulia Kuzovkova und Ruben Niederhagen. "Mixed Certificate Chains for the Transition to Post-Quantum Authentication in TLS 1.3". In: *Proceedings of the 2022 ACM Asia Conference onComputer and Communications Security*. 2022.

[SKD20] Dimitrios Sikeridis, Panos Kampanakis und Michael Devetsikiotis. "Post-Quantum Authentication in TLS 1.3: A Performance Study". In: *Network and Distributed Systems Security (NDSS) Symposium 2020*. 2020.

[SM17] Douglas Stebila und Michele Mosca. "Post-quantum key exchange for the Internet and the Open Quantum Safe project". In: *Selected Areas in Cryptography (SAC)*. 2017. URL: https://openquantumsafe.org/.

[Wät18] Dietmar Wätjen. "Grundlagen". In: *Kryptographie: Grundlagen, Algorithmen, Protokolle*. Wiesbaden: Springer Fachmedien Wiesbaden, 2018, S. 1–13. ISBN: 978-3-658-22474-5. DOI: 10.1007/978-3-658-22474-5_1. URL: https://doi.org/10.1007/978-3-658-22474-5_1.