Praktikable Post-Quanten-Migration

Stefan-Lukas_Gazdag@genua.de

23. Januar 2024

Die Migration zur Post-Quanten-Kryptografie

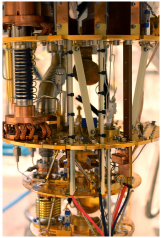
How it started:

How it's going:

Source: Wikimedia, Public Domain

Die wunderbare Welt der Quanten

- Quantum Computing
  - Quantum Computers
  - Quantum Supremacy
  - Quantum Advantage
- Quantum Cryptography
  - Quantum Key Distribution (QKD)
- Post-Quantum Cryptography (PQC)
  - aka Quantum-Safe Cryptography (QSC)
  - aka Quantum-Resistant Cryptography (QRC)



by UCL Mathematical

and Physical Sciences

Das Quantum-Trauma

Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*

Peter W. Shor†

Abstract

A digital computer is generally believed to be an efficient universal computing device; that is, it is believed able to simulate any physical computing device with an increase in computation time by at most a polynomial factor. This may not be true when quantum mechanics is taken into consideration. This paper considers factoring integers and finding discrete logarithms, two problems which are generally thought to be hard on a classical computer and which have been used as the basis of several proposed cryptosystems. Efficient randomized algorithms are given for these two problems on a hypothetical quantum computer. These algorithms take a number of steps polynomial in the input size, e.g., the number of digits of the integer to be factored.

https://arxiv.org/abs/quant-ph/9508027

Der Quantum-Schock

A fast quantum mechanical algorithm for database search

Lov K. Grover
3C-404A, Bell Labs
600 Mountain Avenue
Murray Hill NJ 07974
lkgrover@bell-labs.com

Summary

Imagine a phone directory containing N names arranged in completely random order. In order to find someone's phone number with a probability of $\frac{1}{2}$, any classical algorithm (whether deterministic or probabilistic) will need to look at a minimum of $\frac{N}{2}$ names. Quantum mechanical systems can be in a superposition of states and simultaneously examine multiple names. By properly adjusting the phases of various operations, successful computations reinforce each other while others interfere randomly. As a result, the desired phone number can be obtained in only $O(\sqrt{N})$ steps. The algorithm is within a small constant factor of the fastest possible quantum mechanical algorithm.

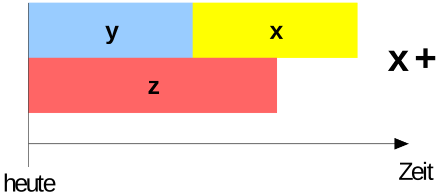
This paper applies quantum computing to a mundane problem in information processing and presents an algorithm that is significantly faster than any classical algorithm can be. The problem is this: there is an unsorted database containing N items out of which just one item satisfies a given condition - that one item has to be retrieved. Once an item is examined, it is possible to tell whether or not it satisfies the condition in one step. However, there does not exist any sorting on the database that would aid its selection. The most efficient classical algorithm for this is to examine the items in the database one by one. If an item satisfies the required condition stop; if it does not, keep track of this item so that it is not examined again. It is easily seen that this algorithm will need to look at an average of $\frac{N}{2}$ items before finding the desired item.

https://arxiv.org/abs/quant-ph/9605043

Tempus fugit

Wann muss man sich sorgen machen?
(nach Michele Mosca, University of Waterloo)

- Wie lange muss Krypto Angriffen standhalten? (*x* Jahre)
- Wie lange benötigen wir, um sicher zu werden? (*y* J.)
- Wie lange wird es dauern, einen großen Quantencomputer oder bessere Angriffe zu entwickeln? (*z* Jahre)



$$x+y>z?$$

Post-Quantum Cryptography

- Gitter-basierte Kryptographie
- Multivariate Kryptographie
- Code-basierte Kryptographie
- Isogenien in supersingularen elliptischen Kurven
- Hash-basierte Signaturen
- …

genua.

Jemand muss es anpacken und untersuchen

Timeline

**This is a tentative timeline, provided for information, and subject to change.*

Date	
Feb 24-26, 2016	NIST Presentation at PQCrypto 2016: *Announcement and outline of NIST's Call for Submissions (Fall 2016), Dustin Moody*
April 28, 2016	NIST releases NISTIR 8105, Report on Post-Quantum Cryptography
Dec 20, 2016	Formal Call for Proposals
Nov 30, 2017	Deadline for submissions
Dec 4, 2017	NIST Presentation at AsiaCrypt 2017: *The Ship Has Sailed: The NIST Post-Quantum Crypto "Competition", Dustin Moody*
Dec 21, 2017	Round 1 algorithms announced (69 submissions accepted as "complete and proper")
Apr 11, 2018	NIST Presentation at PQCrypto 2018: *Let's Get Ready to Rumble - The NIST PQC "Competition", Dustin Moody*
April 11-13, 2018	First PQC Standardization Conference - Submitter's Presentations
January 30, 2019	Second Round Candidates announced (26 algorithms)
March 15, 2019	Deadline for updated submission packages for the Second Round

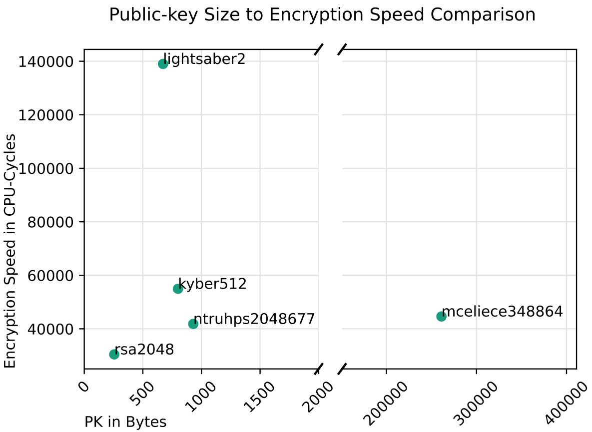
https://csrc.nist.gov/Projects/post-quantum-cryptography/workshops-and-timeline

Jemand muss es anpacken und untersuchen

May 8-10, 2019	NIST Presentation at PQCrypto 2019: Round 2 of the NIST PQC "Competition" - What was NIST Thinking? (Spring 2019), *Dustin Moody*
August 22-24, 2019	Second PQC Standardization Conference
July 22, 2020	Third Round Candidates announced (7 Finalists and 8 Alternates)
October 1, 2020	Deadline for updated submission packages for the Third Round
June 7-9, 2021	Third PQC Standardization Conference
July 5, 2022	Announcement of Candidates to be Standardized and Fourth Round Candidates
October 1, 2022	Deadline for updated submission packages for the Fourth Round
Nov 29-Dec 1, 2022	Fourth PQC Standardization Conference (Virtual)
August 24, 2023	Three Draft FIPS released for public comment • Draft FIPS 203, *Module-Lattice-Based Key-Encapsulation Mechanism Standard* • Draft FIPS 204, *Module-Lattice-Based Digital Signature Standard* • Draft FIPS 205, *Stateless Hash-Based Digital Signature Standard*
April 10-12, 2024	Fifth PQC Standardization Conference

https://csrc.nist.gov/Projects/post-quantum-cryptography/workshops-and-timeline

Alles wird immer schneller und kleiner - nicht



by Gerhard Cenko, Fraunhofer AISEC

genua.

PQC: eine nicht abschließende Wunschliste

- Mindestens zwei Verfahren **hybrid** nutzen
- **Krypto-Agilität** in jeder Bedeutung des Wortes
- Unterstützung **vieler** Verfahren
- **Abwärtskompatibilität** ohne Downgrade-Attacken (was auch immer…)
- Auch auf **Ressourcen-beschränkten** Systemen (oder Gateway davor)
- The list goes on and on and on and on…

Fragen der echten Welt

- Langfristig RSA-8192? Wir müssen doch erst zu 4096. Warum reicht 3072 nicht? Ist 2048 schon gebrochen?
- AES-256 statt AES-128? Puh, das ist aber langsamer, oder?
- SHA-3? Wurden denn SHA-2 schon gebrochen?

genua.

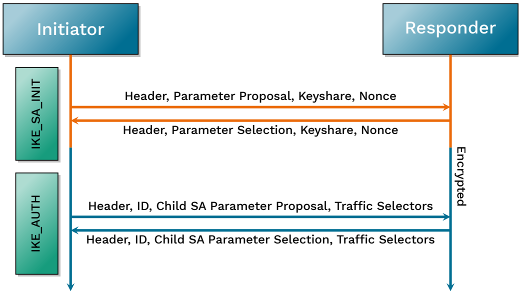
Fragen der echten Welt

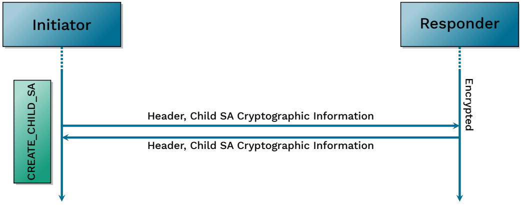
- Langfristig RSA-8192? Wir müssen doch erst zu 4096.
  Warum reicht 3072 nicht? Ist 2048 schon gebrochen?
- AES-256 statt AES-128? Puh, das ist aber langsamer, oder?
- SHA-3? Wurden denn SHA-2 schon gebrochen?

Aber auch erste (kleine) Migrationsschritte!

Internet Key Exchange (IKEv2)

What used to be complex enough…





Internet Key Exchange IKEv2 for IPsec

Using what’s already there

0	8	16	24
Last Substruc	**RESERVED**	Transform Length	
Transform Type	**RESERVED**	Transform ID	
Transform Attributes			

How about using reserved fields for post-quantum logic?

Internet Key Exchange IKEv2 for IPsec

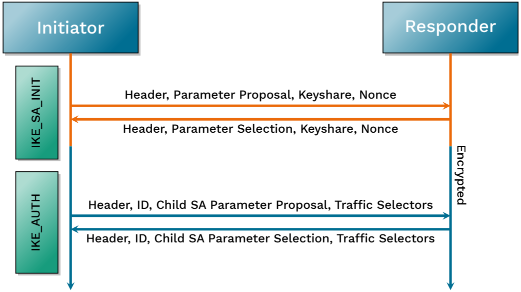
Using what’s already there

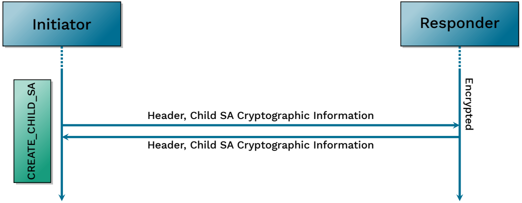
0	8	16	24
Last Substruc	RESERVED	Transform Length	
Transform Type	RESERVED	Transform ID	
Transform Attributes			

You can’t touch this! - MC Hammer (is not to blame for this)

Internet Key Exchange (IKEv2)

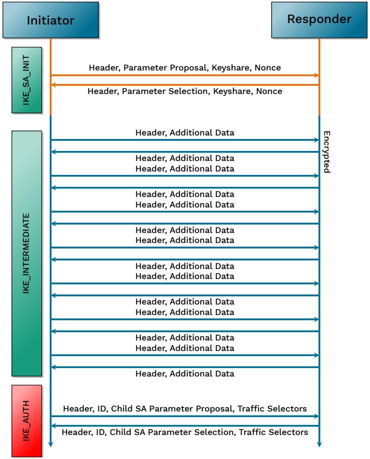
What used to be complex enough…

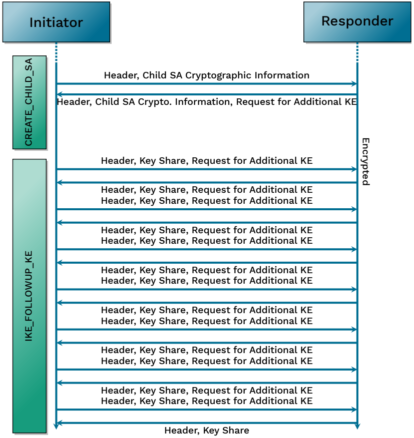




Internet Key Exchange (IKEv2)

Full Post-Quantum Complexity

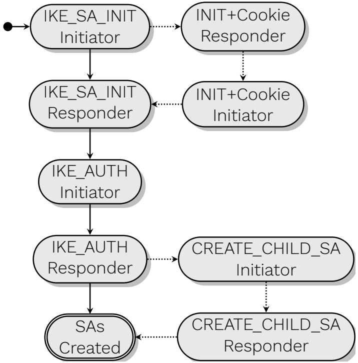


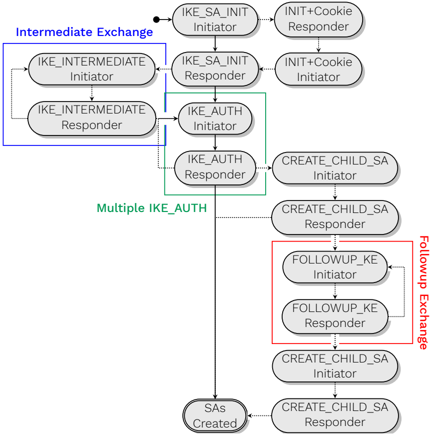


genua.

Internet Key Exchange (IKEv2)

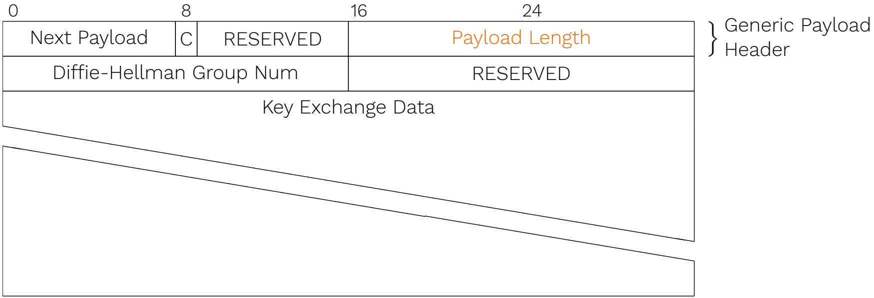
State Machines





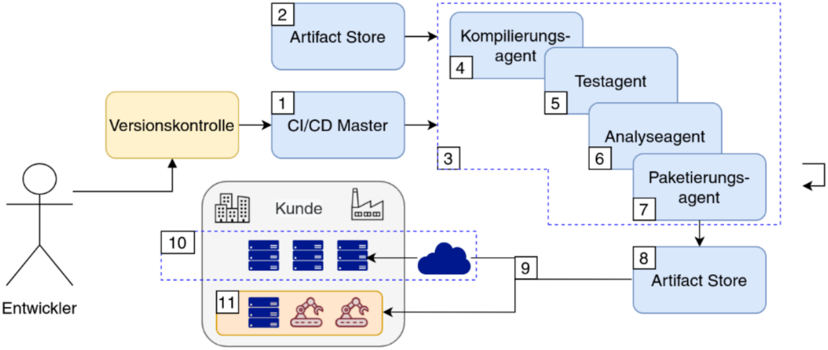
Internet Key Exchange (IKEv2)

Key Exchange Frame



genua.

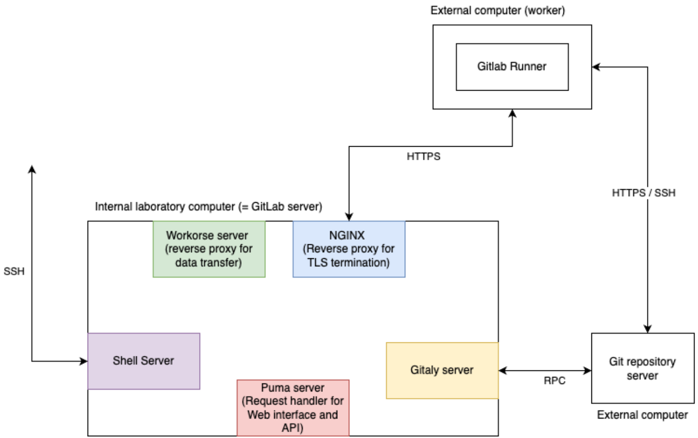
AMiQuaSy



Forschungsprojekt mit OTH Amberg-Weiden und Xitaso GmbH
Förderung über KMU-innovativ des BMBFs

genua.

Zum Glück gibt es Open-Source(-Moloche)



Offizielle Infos zu den gitlab-Komponenten:

`https://docs.gitlab.com/ee/development/architecture.html`

genua.

Standards werden kommen

NIST | Search CSRC | CSRC MENU

Information Technology Laboratory

COMPUTER SECURITY RESOURCE CENTER

NIST | COMPUTER SECURITY RESOURCE CENTER CSRC

UPDATES | 2023

Comments Requested on Three Draft FIPS for Post-Quantum Cryptography

August 24, 2023

NIST requests comments on the initial public drafts of three Federal Information Processing Standards (FIPS):

1. FIPS 203, *Module-Lattice-Based Key-Encapsulation Mechanism Standard*
2. FIPS 204, *Module-Lattice-Based Digital Signature Standard*
3. FIPS 205, *Stateless Hash-Based Digital Signature Standard*

These proposed standards specify key establishment and digital signature schemes that are designed to resist future attacks by quantum computers, which threaten the security of current standards. The three algorithms specified in these standards are each derived from different submissions to the NIST Post-Quantum Cryptography Standardization Project.

The public comment period for these three drafts is open through November 22, 2023. See the publication details (linked above) to download the drafts and for information on submitting comments.

***

Draft FIPS 203 specifies a cryptographic scheme called the Module-Lattice-Based Key-Encapsulation Mechanism Standard which is derived from the CRYSTALS-KYBER submission. A key encapsulation mechanism (KEM) is a particular type of key establishment scheme that can be used to establish a shared secret key between two parties communicating over a public channel. Current NIST-approved key establishment schemes are specified in NIST Special Publication (SP) 800-56A, *Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm-Based Cryptography*, and SP 800-56B, *Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography*.

The drafts of FIPS 204 and 205 each specify digital signature schemes, which are used to detect unauthorized modifications to data and to authenticate the identity of the signatory. FIPS 204 specifies the Module-Lattice-Based Digital Signature Standard, which is derived from CRYSTALS-Dilithium submission. FIPS 205 specifies the Stateless Hash-Based Digital Signature Standard derived from the SPHINCS$^+$ submission. Current NIST-approved digital signature schemes are specified in FIPS 186-5, *Digital Signature Standard*, and SP 800-208, *Recommendation for Stateful Hash-based Signature Schemes*. NIST is also developing a FIPS that specifies a digital signature algorithm derived from FALCON as an additional alternative to these standards.

FEDERAL REGISTER NOTICE

Document Number: 2023-18197

PARENT PROJECT

See: Post-Quantum Cryptography

RELATED TOPICS

Security and Privacy: digital signatures, key management, post-quantum cryptography

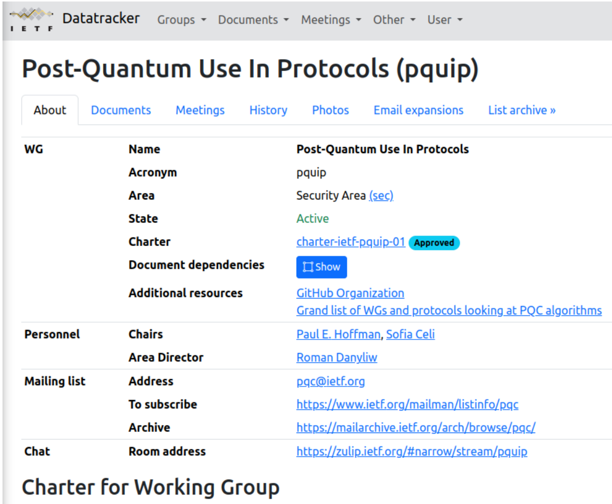
https://csrc.nist.gov/news/2023/three-draft-fips-for-post-quantum-cryptography

Von unterschiedlichen Seiten

https://www.etsi.org/technologies/quantum-safe-cryptography

genua.

Immer mehr davon


Datatracker Groups Documents Meetings Other User

Post-Quantum Use In Protocols (pquip)

About Documents Meetings History Photos Email expansions List archive »

WG	**Name**	**Post-Quantum Use In Protocols**
	Acronym	pquip
	Area	Security Area (sec)
	State	Active
	Charter	charter-ietf-pquip-01 Approved
	Document dependencies	Show
	Additional resources	GitHub Organization Grand list of WGs and protocols looking at PQC algorithms
Personnel	**Chairs**	Paul E. Hoffman, Sofia Celi
	Area Director	Roman Danyliw
Mailing list	**Address**	pqc@ietf.org
	To subscribe	https://www.ietf.org/mailman/listinfo/pqc
	Archive	https://mailarchive.ietf.org/arch/browse/pqc/
Chat	**Room address**	https://zulip.ietf.org/#narrow/stream/pquip

Charter for Working Group

https://datatracker.ietf.org/wg/pquip/about/

NIST wählt vier (erste) Kandidaten, nur einmal Verschlüsselung

For general encryption, used when we access secure websites, NIST has selected the CRYSTALS-Kyber algorithm. Among its advantages are comparatively small encryption keys that two parties can exchange easily, as well as its speed of operation.

For digital signatures, often used when we need to verify identities during a digital transaction or to sign a document remotely, NIST has selected the three algorithms CRYSTALS-Dilithium , FALCON and SPHINCS+ (read as "Sphincs plus"). Reviewers noted the high efficiency of the first two, and NIST recommends CRYSTALS-Dilithium as the primary algorithm, with FALCON for applications that need smaller signatures than Dilithium can provide. The third, SPHINCS+, is somewhat larger and slower than the other two, but it is valuable as a backup for one chief reason: It is based on a different math approach than all three of NIST's other selections.

https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms

BSI TR-02102-1

Empfohlene Verfahren: Die Schlüsselaustauschverfahren FrodoKEM-976 und FrodoKEM-1344 ([4, Abschnitt 2.5]) sowie Classic McEliece mit den Parametern mceliece460896, mceliece6688128 und mceliece8192128 als auch ihren entsprechenden Varianten mceliece460896f, mceliece6688128f und mceliece8192128f [3, Abschnitt 7] werden als kryptographisch geeignet eingeschätzt, um vertrauliche Informationen auf dem in dieser Technischen Richtlinie angestrebten Sicherheitsniveau langfristig zu schützen. Hierbei handelt es sich um eine sehr konservative Einschätzung, die einen erheblichen Sicherheitsspielraum im Hinblick auf künftige kryptoanalytische Fortschritte enthält. Es ist möglich, dass in künftigen Überarbeitungen dieser Richtlinie auch andere Parameterwahlen und PQC-Verfahren als technisch geeignet eingestuft werden.

FrodoKEM wird im Rahmen des PQC-Projektes der NIST nicht standardisiert werden. Dies liegt vor allem an Erwägungen zur Effizienz des Verfahrens, Zweifel an seiner Sicherheit bestehen aktuell nicht [2]. Classic McEliece wurde in die vierte Runde des NIST-Projektes aufgenommen und könnte möglicherweise an deren Ende standardisiert werden. Das BSI hält daher an der Empfehlung von FrodoKEM und Classic McEliece als PQC-Verfahren mit einem hohen Sicherheitsspielraum gegen künftige Angriffe fest.

In Kapitel 6 werden die hashbasierten Signaturverfahren XMSS und LMS sowie ihre Multi-Tree-Varianten empfohlen, die nach aktuellem Kenntnisstand als Quantencomputer-resistent gelten.

Zum jetzigen Zeitpunkt werden in dieser Technischen Richtlinie keine weiteren Post-Quanten-Verfahren empfohlen. Über eine mögliche Aufnahme der vom NIST im Juli 2022 zur Standardisierung ausgewählten Verfahren (siehe [2]) in die Technische Richtlinie wird erst nach Veröffentlichung der Standardisierungsentwürfe entschieden.

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.html

genua.

Migrationsschritte

- (Krypto-) Inventarisierung
- Nachfrage bei Herstellern erzeugen
- Update-/Migrations-Plan erstellen
- Nach Möglichkeit:
  - Tests mit erster PQ-Software (OQS, …)
  - Tests mit größeren Datenpaketen
  - Nutzung von PQ-Gateways
  - Anpassung Open-Source-Software

genua.

Fragen?

Stefan-Lukas_Gazdag@genua.de

www.square-up.org

www.pq-vpn.de

www.genua.de