Post-Quanten-Kryptographie: Schutz privater Kommunikation für ein neues Zeitalter

Peter Schwabe

Max-Planck-Institut für Sicherheit und Privatsphäre

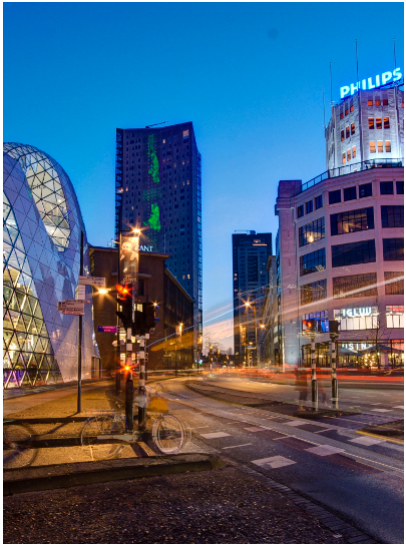
18. November 2025

Mein Weg nach Bochum

- **2001–2007: Aachen**
  Informatikstudium (Diplom)

Mein Weg nach Bochum

- **2001–2007: Aachen**
  Informatikstudium (Diplom)
- **2008–2011: Eindhoven**
  Promotion im Mathematik-Department



Mein Weg nach Bochum

- **2001–2007: Aachen**
  Informatikstudium (Diplom)
- **2008–2011: Eindhoven**
  Promotion im Mathematik-Department
- **2011–2012: Taipei**
  Postdoc an der Academia Sinica und NTU

Mein Weg nach Bochum

- 2001–2007: Aachen
  Informatikstudium (Diplom)
- 2008–2011: Eindhoven
  Promotion im Mathematik-Department
- 2011–2012: Taipei
  Postdoc an der Academia Sinica und NTU
- Since 2013: Nijmegen
  Vom “Universitair Docent” zum Professor

Seit September 2020: MPI-SP

- Gegründet 2019
- Büros noch auf dem RUB Campus
- Im Augenblick 14 Forschungsgruppen

- Ziel:
  - 18 Forschungsgruppen
  - Ungefähr 250–300 Mitarbeiter

Seit September 2020: MPI-SP

[Eine kleine Demo]

RSA basiert auf Faktorisierung

Gegeben $n = p \cdot q$, finde p und q

RSA? X25519?

RSA basiert auf Faktorisierung

Gegeben $n = p \cdot q$, finde p und q

X25519 basiert auf “diskretem Logarithmus” (DLP)

Gegeben $A = g^a$ und g, finde a

RSA? X25519?

RSA basiert auf Faktorisierung

Gegeben $n = p \cdot q$, finde p und q

X25519 basiert auf “diskretem Logarithmus” (DLP)

Gegeben $A = g^a$ und g, finde a

- Fast alle Schlüsselaustauschprotokolle und Signaturverfahren nutzen RSA oder DLP-basierte Verfahren

RSA? X25519?

RSA basiert auf Faktorisierung

Gegeben $n = p \cdot q$, finde p und q

X25519 basiert auf "diskretem Logarithmus" (DLP)

Gegeben $A = g^a$ und g, finde a

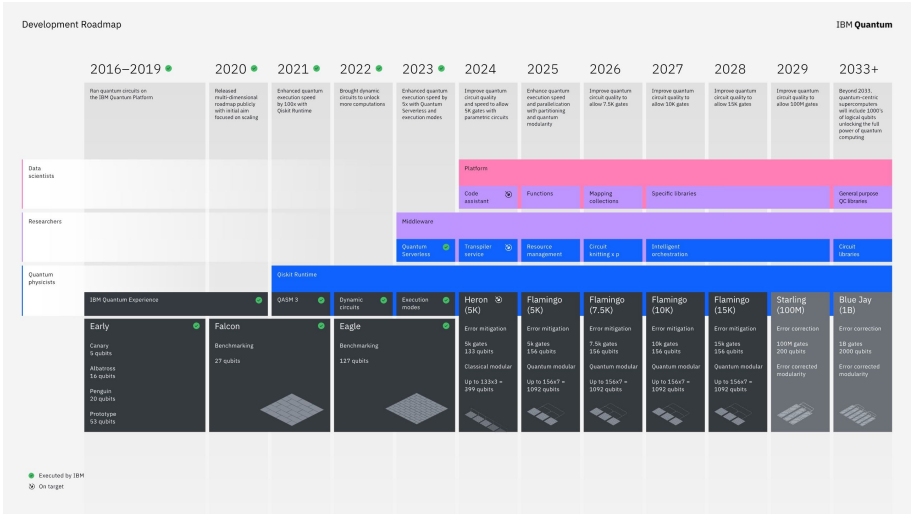
- Fast alle Schlüsselaustauschprotokolle und Signaturverfahren nutzen RSA oder DLP-basierte Verfahren
- DLP und Faktorisierung sind verwandte Probleme $\rightarrow$ wir haben eine **Krypto Monokultur**

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.



Siehe https://www.ibm.com/quantum/blog/ibm-quantum-roadmap-2025

“Damit ist es wahrscheinlich, dass selbst ohne Disruptionen ein krypotanalytisch [sic] relevanter Quantencomputer in höchstens 16 Jahre realisierbar ist”

—BSI: Entwicklungsstand Quantencomputer, Jan. 2025

Post-Quanten Kryptographie (PQC)

Definition

Post-Quanten Kryptographie ist (asymmetrische) Kryptographie, die Angriffen von sowohl klassischen *als auch Quantencomputern* standhält.

Post-Quanten Kryptographie (PQC)

Definition

Post-Quanten Kryptographie ist (asymmetrische) Kryptographie, die Angriffen von sowohl klassischen *als auch Quantencomputern* standhält.

5 verschiedene Ansätze

- Gitterbasierte Kryptographie (Schlüsselaustausch und Signaturen)
- Codebasierte Kryptographie (überwiegend Schlüsselaustausch)
- Multivariate Kryptographie (überwiegend Signaturen)
- Hash-basierte Signaturen (nur Signaturen)
- Isogenienbasierte Kryptographie (*it's complicated*. . .)

Wann müssen wir uns Sorgen machen?

“Harvest now, decrypt later”

https://en.wikipedia.org/wiki/Utah_Data_Center#/media/File:EFF_photograph_of_NSA's_Utah_Data_Center.jpg

Wann müssen wir uns Sorgen machen?

“Harvest now, decrypt later”

https://en.wikipedia.org/wiki/Utah_Data_Center#/media/File:EFF_photograph_of_NSA's_Utah_Data_Center.jpg

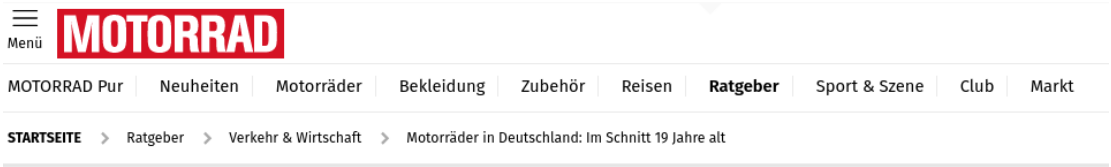
Der Satz von Mosca

$$X + Y > Z$$

- X: Wie lange müssen verschlüsselte Daten sicher sein?
- Y: Wie lange brauchst Du, um auf PQC umzustellen?
- Z: Wie lange dauert es, bis wir einen kryptographisch relevanten Quantencomputer haben?

Falls $X + Y > Z$, dann solltest Du Dir Sorgen machen.

Wann müssen wir uns Sorgen machen? (Teil 2)



Menü MOTORRAD

MOTORRAD Pur | Neuheiten | Motorräder | Bekleidung | Zubehör | Reisen | **Ratgeber** | Sport & Szene | Club | Markt

STARTSEITE > Ratgeber > Verkehr & Wirtschaft > Motorräder in Deutschland: Im Schnitt 19 Jahre alt

MOTORRÄDER IN DEUTSCHLAND SIND MEISTENS ALT

Motorräder: Im Durchschnitt grad erwachsen

Youngtimer dominieren: In Deutschland sind zugelassene Motorräder im Schnitt 19,1 Jahre alt.

Jens Kratschmar • 09.08.2022

Der NIST PQC Wettbewerb

- Inspiriert von zwei früheren NIST Krypto Wettbewerben:
  - AES, von 1997 bis 2000
  - SHA3, von 2007 bis 2012

Der NIST PQC Wettbewerb

- Inspiriert von zwei früheren NIST Krypto Wettbewerben:
  - AES, von 1997 bis 2000
  - SHA3, von 2007 bis 2012
- NIST legt Kriterien fest, jeder darf Vorschläge einreichen
- Auswahl durch einen offenen Prozess über mehrere Runden
- Entscheidungen werden von NIST getroffen

Der NIST PQC Wettbewerb

- Inspiriert von zwei früheren NIST Krypto Wettbewerben:
  - AES, von 1997 bis 2000
  - SHA3, von 2007 bis 2012
- NIST legt Kriterien fest, jeder darf Vorschläge einreichen
- Auswahl durch einen offenen Prozess über mehrere Runden
- Entscheidungen werden von NIST getroffen
- PQC Wettbewerb:
  - Ankündigung im Februar 2016
  - Aufruf zur Einreichung im Dezember 2016 (nach Community Input)
  - Deadline für Einreichungen: November 2017

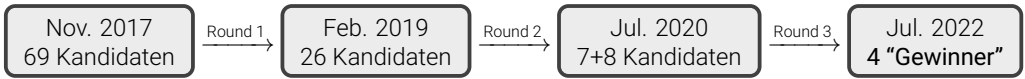
NIST PQC – wie es begann

Count of Problem Category	Column Labels		
Row Labels	Key Exchange	Signature	Grand Total
?	1		1
Braids	1	1	2
Chebychev	1		1
Codes	19	5	24
Finite Automata	1	1	2
Hash		4	4
Hypercomplex Numbers	1		1
Isogeny	1		1
Lattice	24	4	28
Mult. Var	6	7	13
Rand. walk	1		1
RSA	1	1	2
Grand Total	**57**	**23**	**80**

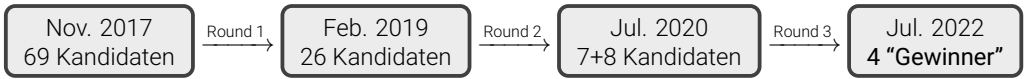
4 31 27

Übersicht aus einem Tweet von Jacob Alperin-Sheriff am 4. Dezember, 2017.

NIST PQC – Wie es weiterging



NIST PQC – Wie es weiterging



"The public-key encryption and key-establishment algorithm that will be standardized is ***CRYSTALS-KYBER****. The digital signatures that will be standardized are* ***CRYSTALS-Dilithium****, FALCON, and* ***SPHINCS***$^{+}$*. While there are multiple signature algorithms selected, NIST recommends* ***CRYSTALS-Dilithium*** *as the primary algorithm to be implemented"*

—NIST IR 8413-upd1

Wo sind wir jetzt?

Juli 2024

- CRYSTALS-Kyber standardisiert als ML-KEM (FIPS 203)
- CRYSTALS-Dilithium standardisiert als ML-DSA (FIPS 204)
- SPHINCS$^+$ standardisiert als SLH-DSA (FIPS 205)

Wo sind wir jetzt?

Juli 2024

- CRYSTALS-Kyber standardisiert als ML-KEM (FIPS 203)
- CRYSTALS-Dilithium standardisiert als ML-DSA (FIPS 204)
- SPHINCS$^+$ standardisiert als SLH-DSA (FIPS 205)

- Es gibt mehrere Post-Quanten Krypto Standards
- Es gibt Implementierungen, integriert in Software Bibliotheken
- Jetzt müssen wir Protokolle, Anwendungen, und Systeme updaten

Wo sind wir jetzt?

Juli 2024

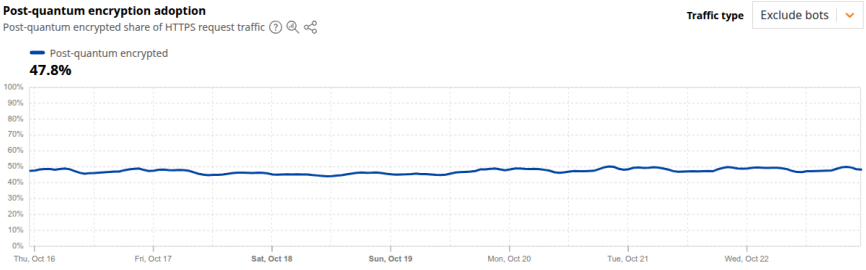
- CRYSTALS-Kyber standardisiert als ML-KEM (FIPS 203)
- CRYSTALS-Dilithium standardisiert als ML-DSA (FIPS 204)
- SPHINCS$^+$ standardisiert als SLH-DSA (FIPS 205)

- Es gibt mehrere Post-Quanten Krypto Standards
- Es gibt Implementierungen, integriert in Software Bibliotheken
- Jetzt müssen wir Protokolle, Anwendungen, und Systeme updaten

Wie schwer kann das schon sein?

[Antwort 1: Zurück zu unserer Demo]

Antwort 1: weitere positive Beispiele



https://radar.cloudflare.com/adoption-and-usage#post-quantum-encryption-adoption

- Mehrere hundert Milliarden Verbindungen pro Tag alleine bei Cloudflare
- ML-KEM wird auch in Signal und iMessage eingesetzt
- . . . auch in Cloud-Infrastruktur bei AWS
- Signaturen z.B. für Software-Updates in der kommenden Automobilgeneration

Antwort 2 – Ein Blick in die Geschichte: MD5

- MD5 ist eine kryptographische Hashfunktion
- Hashfunktionen sind “überall”

Antwort 2 – Ein Blick in die Geschichte: MD5

- MD5 ist eine kryptographische Hashfunktion
- Hashfunktionen sind “überall”
- **1991**: MD5 von Rivest vorgestellt

Antwort 2 – Ein Blick in die Geschichte: MD5

- MD5 ist eine kryptographische Hashfunktion
- Hashfunktionen sind “überall”
- **1991**: MD5 von Rivest vorgestellt
- **1993**: Kollisionen in der MD5 Kompressionsfunktion (den Boer, Bosselaers)

Antwort 2 – Ein Blick in die Geschichte: MD5

- MD5 ist eine kryptographische Hashfunktion
- Hashfunktionen sind “überall”
- **1991**: MD5 von Rivest vorgestellt
- **1993**: Kollisionen in der MD5 Kompressionsfunktion
  (den Boer, Bosselaers)
- **1996**: Dobbertin, Bosselaers, Preneel: Bedenken gegen die Nutzung von MD5

Antwort 2 – Ein Blick in die Geschichte: MD5

- MD5 ist eine kryptographische Hashfunktion
- Hashfunktionen sind “überall”
- **1991**: MD5 von Rivest vorgestellt
- **1993**: Kollisionen in der MD5 Kompressionsfunktion
  (den Boer, Bosselaers)
- **1996**: Dobbertin, Bosselaers, Preneel: Bedenken gegen die Nutzung von MD5
- **2004**: Wang findet MD5 Kollisionen

Antwort 2 – Ein Blick in die Geschichte: MD5

- MD5 ist eine kryptographische Hashfunktion
- Hashfunktionen sind “überall”
- **1991**: MD5 von Rivest vorgestellt
- **1993**: Kollisionen in der MD5 Kompressionsfunktion
  (den Boer, Bosselaers)
- **1996**: Dobbertin, Bosselaers, Preneel: Bedenken gegen die Nutzung von MD5
- **2004**: Wang findet MD5 Kollisionen
- **2008**: ***Gefälschtes CA Zertifikat*** mit MD5
  (Sotirov, Stevens, Appelbaum, Lenstra, Molnar, Osvik, de Weger)

Antwort 2 – Ein Blick in die Geschichte: MD5

- MD5 ist eine kryptographische Hashfunktion
- Hashfunktionen sind “überall”
- **1991**: MD5 von Rivest vorgestellt
- **1993**: Kollisionen in der MD5 Kompressionsfunktion
  (den Boer, Bosselaers)
- **1996**: Dobbertin, Bosselaers, Preneel: Bedenken gegen die Nutzung von MD5
- **2004**: Wang findet MD5 Kollisionen
- **2008**: ***Gefälschtes CA Zertifikat*** mit MD5
  (Sotirov, Stevens, Appelbaum, Lenstra, Molnar, Osvik, de Weger)
- **2012**: Flame Malware nutzt Schwächen in MD5 in Windows Update

Antwort 2 – Ein Blick in die Geschichte: MD5

- MD5 ist eine kryptographische Hashfunktion
- Hashfunktionen sind “überall”
- **1991**: MD5 von Rivest vorgestellt
- **1993**: Kollisionen in der MD5 Kompressionsfunktion
  (den Boer, Bosselaers)
- **1996**: Dobbertin, Bosselaers, Preneel: Bedenken gegen die Nutzung von MD5
- **2004**: Wang findet MD5 Kollisionen
- **2008**: ***Gefälschtes CA Zertifikat*** mit MD5
  (Sotirov, Stevens, Appelbaum, Lenstra, Molnar, Osvik, de Weger)
- **2012**: Flame Malware nutzt Schwächen in MD5 in Windows Update

MD5 zu ersetzen war vergleichsweise “einfach”!

Was lernen wir daraus?

1. **Für einige (viele?) Anwendungen ist die Umstellung recht einfach.**
   - Sie verwenden schon jeden Tag PQC wahrscheinlich ohne es zu wissen
   - Ausrollen von PQC durch normale System-Updates

Was lernen wir daraus?

1. Für einige (viele?) Anwendungen ist die Umstellung recht einfach.
   - Sie verwenden schon jeden Tag PQC wahrscheinlich ohne es zu wissen
   - Ausrollen von PQC durch normale System-Updates
2. Die Umstellung *aller* Anwendungen wird schwer.
   - Wir müssen erstmal wissen, was alles umgestellt werden muss
   - PQC ist manchmal nicht einfach “drop-in” Ersatz
   - Wahrscheinlich müssen einige Geräte wirklich ersetzt werden

Was lernen wir daraus?

1. Für einige (viele?) Anwendungen ist die Umstellung recht einfach.
   - Sie verwenden schon jeden Tag PQC wahrscheinlich ohne es zu wissen
   - Ausrollen von PQC durch normale System-Updates
2. Die Umstellung *aller* Anwendungen wird schwer.
   - Wir müssen erstmal wissen, was alles umgestellt werden muss
   - PQC ist manchmal nicht einfach “drop-in” Ersatz
   - Wahrscheinlich müssen einige Geräte wirklich ersetzt werden

Die nächsten Jahre bleiben spannend!

Vielen Dank!!

https://cryptojedi.org