UNIVERSITÄT ZU LÜBECK

Postquantenkryptographie

Florian Chudigiewitsch

30. August 2023

IM FOCUS DAS LEBEN

Themen

Wo benutzen wir Kryptographie?

Wie funktioniert Kryptographie?

Quantencomputer

Die Rettung: Postquantenkryptographie

Überall und jederzeit!

- EC- und Kreditkarten, Geldautomat
- Account-Logins
- WLAN- und Mobilfunk-Netzwerke
- *Jeder* Aufruf einer Website (hoffentlich)
- Firmenhandys oder -laptops (hoffentlich)
- Elektronische Türschlösser
- Smart-Home Geräte (ca. 15 Milliarden Geräte weltweit)
- Etwas kreativer: Tankstellenpreise

Themen

Wo benutzen wir Kryptographie?

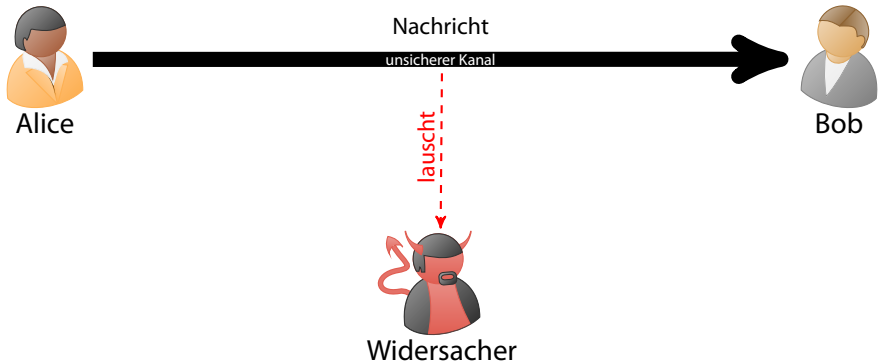
Wie funktioniert Kryptographie?

Quantencomputer

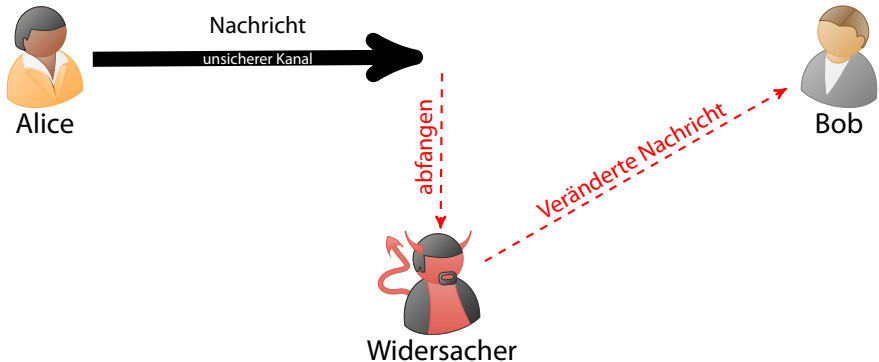
Die Rettung: Postquantenkryptographie

Protokolle

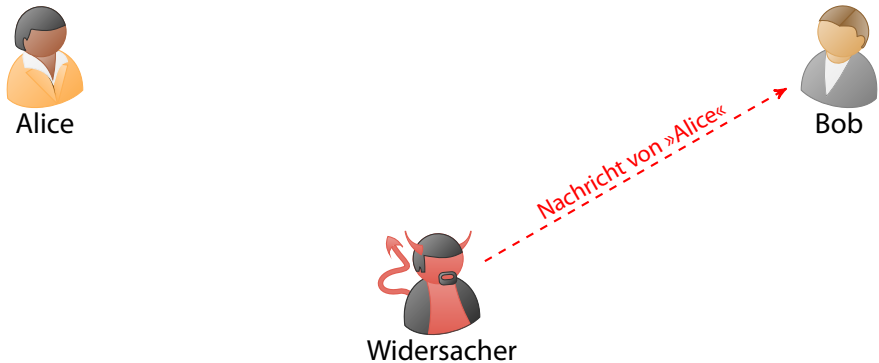
Vertraulichkeit (»Nur der Empfänger kann die Nachricht lesen«)



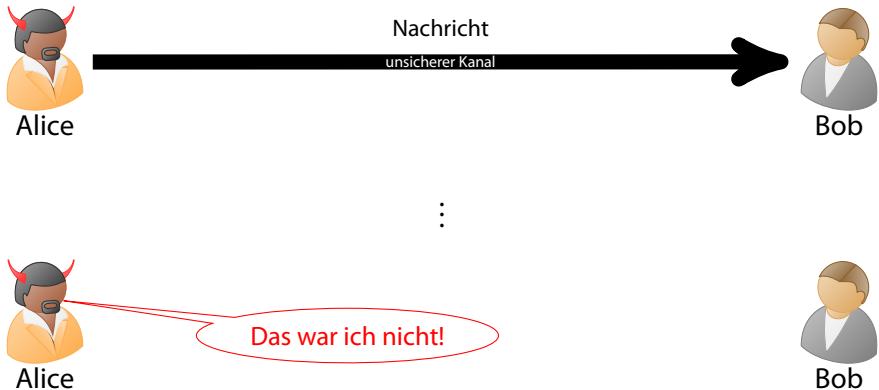
Integrität (»Die Nachricht wurde unterwegs nicht verändert«)



Authentizität (»Die Nachricht kommt wirklich von mir«)



Verbindlichkeit (»Ich kann die Nachricht nicht verleugnen«)



Daten verschlüsseln

Das Geheimnis austauschen

- Wenn 🔑 und 🗝 gleich sind, spricht man von *symmetrischer Verschlüsselung*

Das Geheimnis austauschen

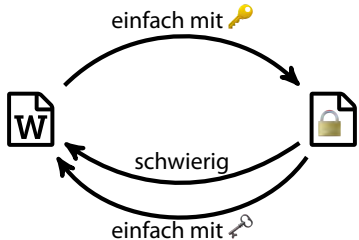
- Wenn 🔑 und 🗝 gleich sind, spricht man von *symmetrischer Verschlüsselung*
- Problem: Wie tauscht man die Schlüssel aus?

Das Geheimnis austauschen

- Wenn 🔑 und 🗝 gleich sind, spricht man von *symmetrischer Verschlüsselung*
- Problem: Wie tauscht man die Schlüssel aus?
- Durchbruch der Kryptographie: Asymmetrische Verschlüsselung

Im Kern: Wie kompliziert sind Berechnungen?

- Wir wollen, dass jeder leicht mit öffentlichen Schlüssel 🔑 verschlüsseln kann...
- ...aber nur bestimmte Personen, die den privaten Schlüssel 🗝 haben, sollen auch leicht entschlüsseln können
- Das erreichen wir mit sogenannten Einwegfunktionen



Einwegfunktionen: Ein (leicht vereinfachtes) Beispiel

- Multiplizieren ist leicht: $127 \cdot 131$

Einwegfunktionen: Ein (leicht vereinfachtes) Beispiel

- Multiplizieren ist leicht: $127 \cdot 131 = 16637$

Einwegfunktionen: Ein (leicht vereinfachtes) Beispiel

- Multiplizieren ist leicht: $127 \cdot 131 = 16637$
- Die Umkehrung (»Faktorisieren«) nicht so: $27661 = ? \cdot ?$

Einwegfunktionen: Ein (leicht vereinfachtes) Beispiel

- Multiplizieren ist leicht: $127 \cdot 131 = 16637$
- Die Umkehrung (»Faktorisieren«) nicht so: $27661 = ? \cdot 199$

Einwegfunktionen: Ein (leicht vereinfachtes) Beispiel

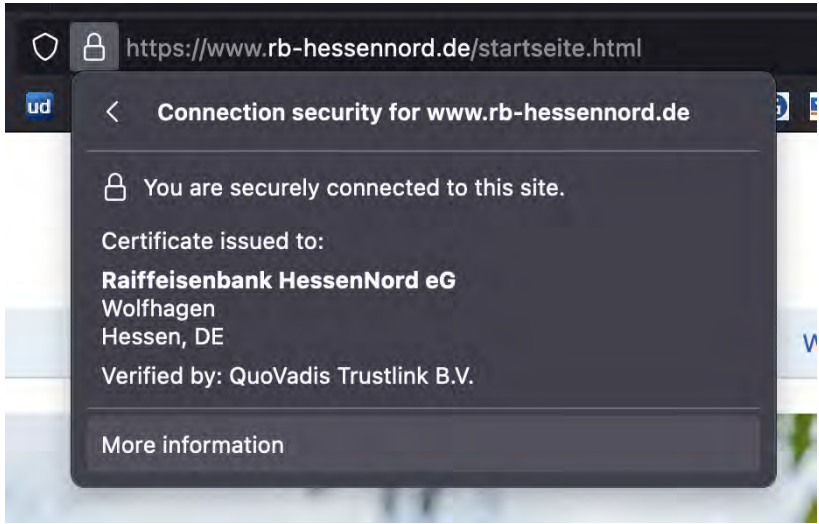
- Multiplizieren ist leicht: $127 \cdot 131 = 16637$
- Die Umkehrung (»Faktorisieren«) nicht so: $27661 = 139 \cdot 199$

Einwegfunktionen: Ein (leicht vereinfachtes) Beispiel

- Multiplizieren ist leicht: $127 \cdot 131 = 16637$
- Die Umkehrung (»Faktorisieren«) nicht so: $27661 = 139 \cdot 199$
- Mit »Geheimnis« geht es doch ganz gut: Wir haben eine Einwegfunktion gefunden 🥳

Einwegfunktionen: Ein (leicht vereinfachtes) Beispiel

- Multiplizieren ist leicht: $127 \cdot 131 = 16637$
- Die Umkehrung (»Faktorisieren«) nicht so: $27661 = 139 \cdot 199$
- Mit »Geheimnis« geht es doch ganz gut: Wir haben eine Einwegfunktion gefunden 🥳
- Auf der Schwierigkeit der Faktorisierung beruhen eine Großzahl der aktuell genutzten kryptographischen Protokolle! (RSA, Diffie-Hellman...)


https://www.rb-hessennord.de/startseite.html
ud
Connection security for www.rb-hessennord.de
You are securely connected to this site.
Certificate issued to:
Raiffeisenbank HessenNord eG
Wolfhagen
Hessen, DE
Verified by: QuoVadis Trustlink B.V.
More information

Technical Details

Connection Encrypted (TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, 256 bit keys, TLS 1.2)

The page you are viewing was encrypted before being transmitted over the Internet.

Encryption makes it difficult for unauthorised people to view information travelling between computers. It is therefore unlikely that anyone read this page as it travelled across the network.

Themen

Wo benutzen wir Kryptographie?

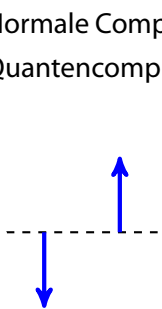
Wie funktioniert Kryptographie?

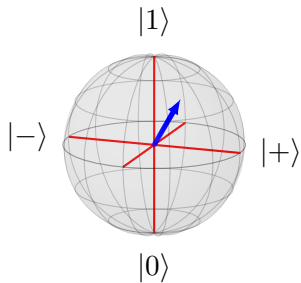
Quantencomputer

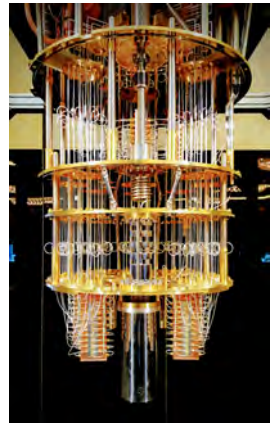
Die Rettung: Postquantenkryptographie

Was sind Quantencomputer?

- Normale Computer arbeiten mit »Bits« (0 und 1)
- Quantencomputer mit Qubits (Blochsphäre)







Was sind Quantencomputer?

Dadurch braucht man aber auch viel Mathe…

Definition

Der Zustand eines isolierten physikalischen Systems wird vollständig von einem Einheitsvektor $|\Psi\rangle$ in einem komplexen Hilbertraum beschrieben. Der Vektor heißt *Zustandsvektor* (oder *Wellenfunktion*) und der zugehörige Hilbertraum heißt *Zustandsraum* des Systems.

Definition (Hilbertraum)

Ein *Hilbertraum* $\mathcal{H}$ ist ein Vektorraum über $\mathbb{C}$ mit einem Skalarprodukt $\langle \cdot \mid \cdot \rangle$, der vollständig bezüglich der durch das Skalarprodukt induzierten Norm ist, d. h. das jede Cauchy-Folge bezüglich der Norm zu einem Element des Raumes konvergiert.

Was sind Quantencomputer?

Dadurch braucht man aber auch viel Mathe…

Die vier Bell-Zustände sind
$\left|\Phi^+\right\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \left|\Phi^-\right\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle), \left|\Psi^+\right\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \left|\Psi^-\right\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle).$

Lemma
$\left|\Phi^+\right\rangle$ *kann nicht in das Produkt zweier Zustände jeweils eines Bits zerlegt werden.*

Proof.
Gäbe es eine solche Zerlegung von $\left|\Phi^+\right\rangle$, so könnten wir die Gleichung

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = (\alpha_0 |0\rangle + \alpha_1 |1\rangle) \otimes (\beta_0 |0\rangle + \beta_1 |1\rangle)$$

lösen. Es würde gelten $\alpha_0\beta_0 = \alpha_1\beta_1 = \frac{1}{\sqrt{2}}$ und $\alpha_0\beta_1 = \alpha_1\beta_0 = 0$. Das ist nicht möglich. □

Was sind Quantencomputer?

Dadurch braucht man aber auch viel Mathe…

$$|\Psi_0\rangle = |0\rangle\,|1\rangle$$

$$|\Psi_1\rangle = (H\,|0\rangle)(H\,|1\rangle) = |+\rangle\,|-\rangle = \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)|-\rangle$$

$$|\Psi_2\rangle = U_f\,|\Psi_1\rangle = U_f\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)|-\rangle = \frac{U_f(|0\rangle\,|-\rangle) + U_f(|1\rangle\,|-\rangle)}{\sqrt{2}}$$

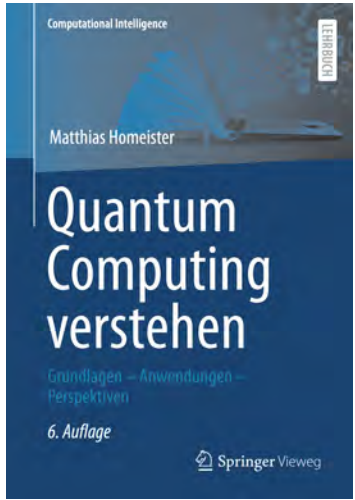
$$= \frac{(-1)^{f(0)}\,|0\rangle\,|-\rangle + (-1)^{f(1)}\,|1\rangle\,|-\rangle}{\sqrt{2}}$$ phase kickback

$$= \frac{(-1)^{f(0)}\,|0\rangle + (-1)^{f(1)}\,|1\rangle}{\sqrt{2}}\,|-\rangle$$

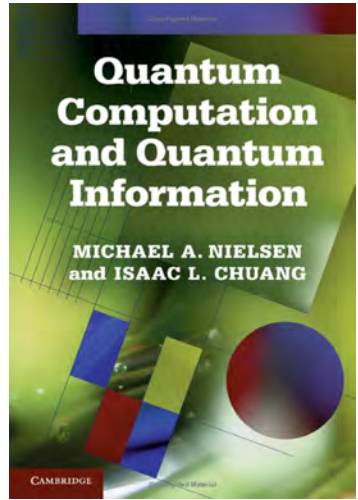
$$= \begin{cases} (\pm 1)\frac{|0\rangle+|1\rangle}{\sqrt{2}}\,|-\rangle & \text{if } f(0) = f(1) \\ (\pm 1)\frac{|0\rangle-|1\rangle}{\sqrt{2}}\,|-\rangle & \text{if } f(0) \neq f(1) \end{cases}$$

Der Faktor ± 1 kann Vernachlässigt werden, weil das Vorzeichen der Amplitude bei der Messung nicht wichtig sein wird.

Zum Weiterlesen



Für Interessierte



Für *sehr* Interessierte

Zum Beispiel: Viel schneller faktorisieren!

Der technische Stand…

Größte faktorisierte Zahl...

- ... klassisch: 250 Ziffern (2700 CPU core-years)
  - 21403246502407449612644230728393335630086147151447550177977549208814180234471401366433455190958046796109928518724709145876873962619215573630474547705208051190564931066876915900197594056934574522305893259766974716817380693648946998715784949759374979 37
- ... mit Quantencomputer:

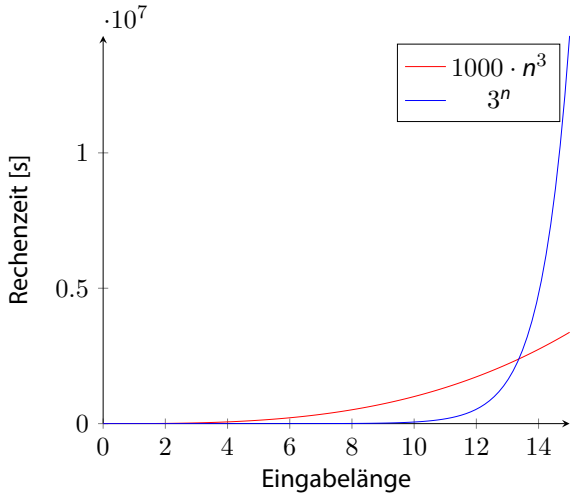
Der technische Stand…

Größte faktorisierte Zahl...

- ... klassisch: 250 Ziffern (2700 CPU core-years)
  - 2140324650240744961264423072839333563008614715144755017797754920881418023447140136643345519095804679610992851872470914587687396261921557363047454770520805119056493106687691590019759405693457452230589325976697471681738069364894699871578494975937497937
- ... mit Quantencomputer: 21

…und warum das egal ist

»Exponentielles vs. polynomielles Wachstum«: Ein Rechenbeispiel



…und warum das egal ist

Eingabegröße n	klassisch	Quantumcomputer
10	$5.9\ \mu$s	$0.1\ \mu$s
20	0.35 s	$0.8\ \mu$s
30	5.7 Stunden	$2.7\ \mu$s
40	38 Jahre	$6.4\ \mu$s
50	2 Millionen Jahre	$12.5\ \mu$s
60	$1.3 \cdot 10^{11}$ Jahre	$21.6\ \mu$s

…und warum das egal ist

»Harvest now, decrypt later«

Alle Daten, die Sie jetzt noch mit »Präquantenkryptographie« ins Internet senden, werden irgendwann entschlüsselt werden.

Themen

Wo benutzen wir Kryptographie?

Wie funktioniert Kryptographie?

Quantencomputer

Die Rettung: Postquantenkryptographie

Der Lichtblick

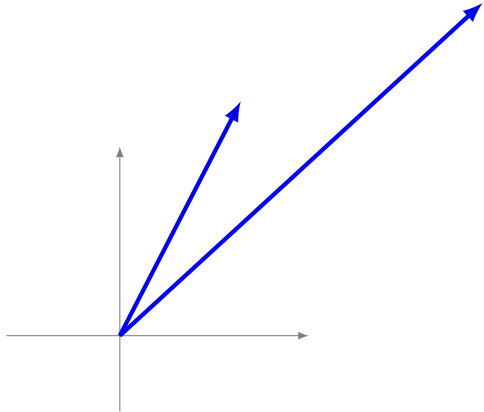
- Es gibt Einwegfunktionen, von denen wir glauben, dass Quantencomputer diese nicht umkehren können.
- Diese teilen sich in vier Kategorien:
  - Code-Basierte Verfahren
  - Hash-Basierte Verfahren
  - Gitter-Basierte Verfahren
  - Isogenie-Basierte Verfahren
- (Wir haben quasi ein »Faktorisierungs-Basiertes« Verfahren kennengelernt)

Mögliche Verfahren

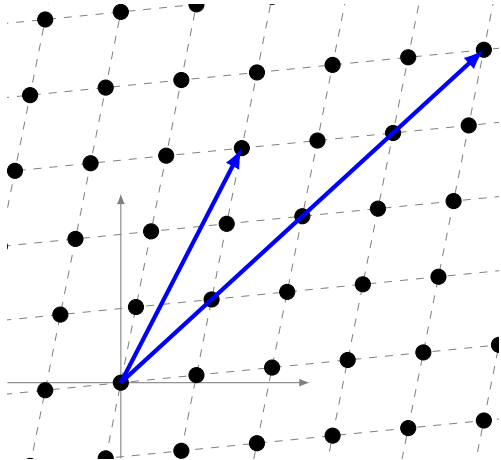
Standardisierungsverfahren des NIST

- Eingereicht: 82
- Für erste Runde nominiert: 69
- Für zweite Runde nominiert: 26
- Für dritte Runde nominiert: $7 + 8$ Reserve
- Für vierte Runde nominiert: $3 + 8$ Reserve

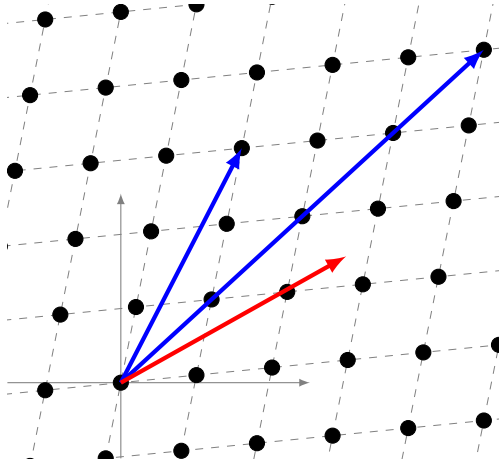
Beispiel Gitter: Closest Vector Problem



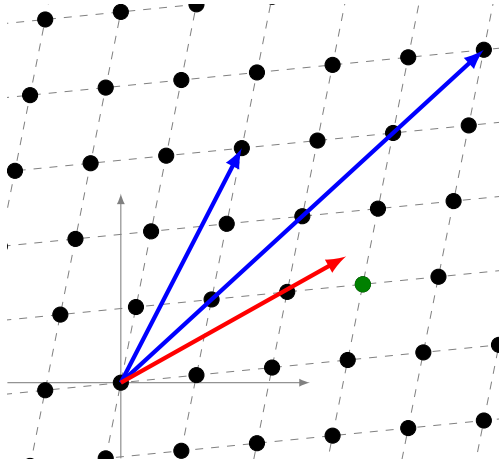
Beispiel Gitter: Closest Vector Problem



Beispiel Gitter: Closest Vector Problem



Beispiel Gitter: Closest Vector Problem



Herausforderungen

- Verfahren sind sehr komplex
- Wir können sie daher schlecht analysieren (schon bei klassischen Verfahren so)
- Beispiel (aus 4. Runde des NIST-Wettbewerbs):

SIDH/SIKE sogar auf klassischen Rechnern unsicher!

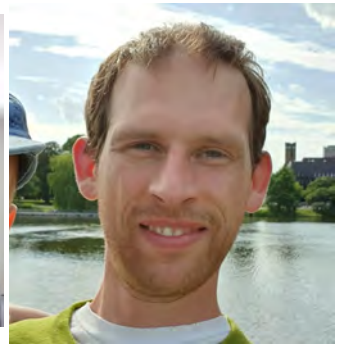
(Supersingular isogeny Diffie-Hellman key exchange)

Von der Theorie in die Praxis

- Postquantenkryptographie ist noch nicht so gut erforscht
- Wir brauchen auch Experten, welche die Verfahren Praktikern erklären können
- Implementierung der Verfahren enthält auch oft Fehler
- Zusammenarbeit ist also wichtig

Was hat die Uni Lübeck damit zu tun?

Sebastian Berndt
Kryptografie und
Algorithmik



Kim-Manuel Klein
Gittertheorie in der
Informatik

Maciej Liśkewicz
Quanteninformatik

Zusammenfassung

- Kryptographie ist immer und überall
- Weit verbreitete Verfahren werden durch Quantencomputer bedroht
- *Schon jetzt* kann alles, was verschickt wird, abgespeichert und später geknackt werden
- Postquantenkryptographie sucht Verfahren, die auch gegen Quantencomputer sicher sind

Zusammenfassung

- Kryptographie ist immer und überall
- Weit verbreitete Verfahren werden durch Quantencomputer bedroht
- *Schon jetzt* kann alles, was verschickt wird, abgespeichert und später geknackt werden
- Postquantenkryptographie sucht Verfahren, die auch gegen Quantencomputer sicher sind

Danke!