$J \int$ *Skripte*

Kryptologie ICS.KRYPTO

Folien zur Präsenz 13, Teil 1 «Quantenkryptographie und Quantencomputer», FS 24, V6.2

https://www.youtube.com/watch?v=39KY2cue6JE

©Josef Schuler, dipl. math., dipl. Ing. NDS ETHZ, MSc Applied IT-Security, Feldhof 25, 6300 Zug, j.schuler@bluewin.ch resp. josef.schuler@hslu.ch

Einleitung

Agenda, Verweise zur Literatur

- Wir behandeln zwei aktuelle Themen
  - Quantenkryptographie (resp. Quanten-Schlüsselverteilung),
    - Siehe dazu Kap. 18 im JS Skript „Einführung in die Kryptologie“.
    - Keine Literaturhinweise im Lehrbuch von C. Paar [CP-D].
  - Quantencomputer
    - Siehe dazu Kap. 16.8 im JS Skript „Einführung in die Kryptologie“.
    - In [CP-D] gibt es einige wenige Stellen dazu, S. 26, 104, 166.
- **Quantenkryptographie teilt sich in die zwei Teile …**
  - ... Quanten-Schlüsselverteilung (QKD = Quantum Key Distribution)
  - … „Allgemeine“ Quantenkryptographie (z.B. Quantenzufallszahlengeneratoren) → wir besprechen nur Ersteres.
- **Beachten Sie, dass …**
  - ... Sie im Modul ISF die Themen Quantencomputer & -kryptographie schon einmal besprochen haben. Ich versuche – wie in den anderen Fällen, wo eine Betrachtung schon in anderen Modulen stattfand – eine alternative Sichtweise zu bieten.

Lernziele

- Ich kann d. Schlüsselbits bei einem Quantenschlüsselaustausch bestimmen.
- Ich kann berechnen, wie viele Ausgangsbit nötig sind, um n Bit Schlüssel nach dem Quantenschlüsselaustausch zu haben.
- Ich kann d. Stärken & Schwächen der Quantenschlüsselverteilung aufzählen.
- Ich kann die Anzahl Qbits berechnen, um einen RSA mit Modulus N zu brechen (resp. N zu faktorisieren), resp. um eine Elliptische Kurve mod p zu brechen.
- Ich kann aufgrund der Qbits die Sicherheit von RSA und EC in Bezug auf den Einsatz von Quantencomputer vergleichen.
- Ich kenne eine (weitere) Begründung, warum der AES auch mit 256 Bit Schlüssellänge standardisiert ist.

Die Slogans zu dieser Präsenz

(1) Titelbild = das ist die grosse Kunst: so einfach zu erklären, so dass es noch richtig ist.

(2) Quantenkryptographie und Quantencomputer haben per se nicht viel miteinander zu tun.

(3) Quantencomp. werden nach AI d. nächste „Revolution“ sein.

Quantum Cryptography

Quantum Key Distribution, respectively

Quantum Cryptography

A form of cryptography that protects information using quantum effects

„General“ Quantum Cryptography

- Used to protect quantum or classical data
- Can only be used on a quantum computer
- Will be necessary one day for quantum networks
- Allows exotic uses (unclonable data, quantum money, etc.)

Quantum Key Distribution (QKD)

- Only used to securely exchange classical keys
- Can be used today
- Requires special hardware
- Implementation security must be assessed carefully

Security Protocols for the simplified OSI Stack

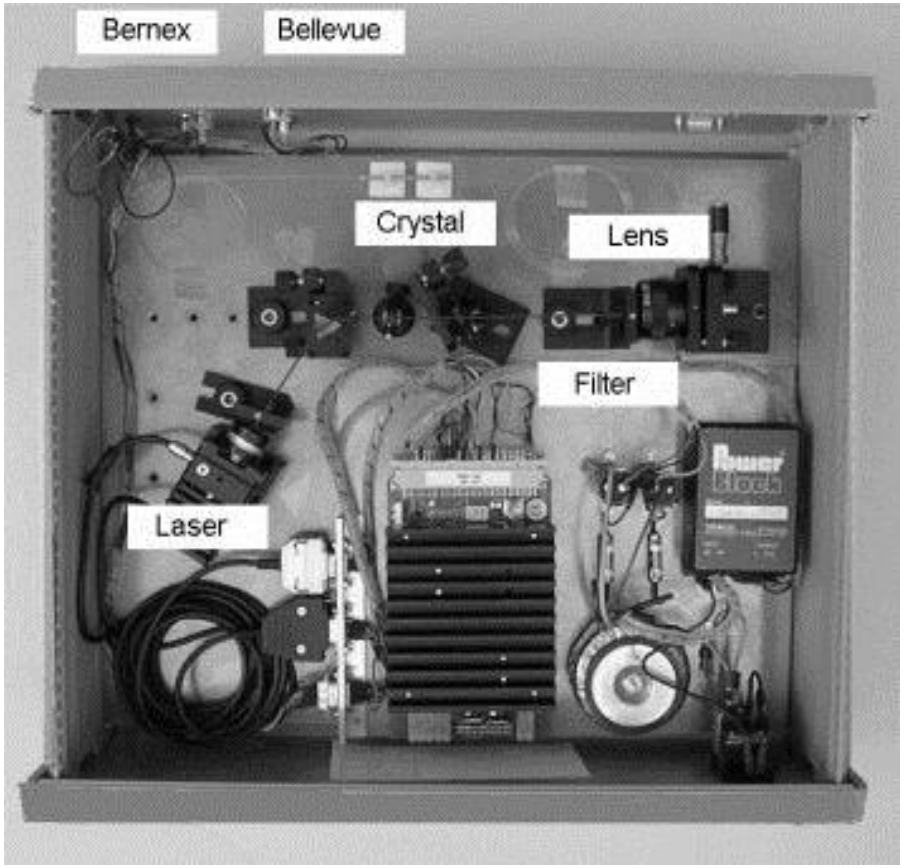
Communication layers	Security protocols
Application layer	ssh, S/MIME, PGP, http digest
Transport layer	SSL, TLS, WTLS (*)
Network layer	IPsec
Data Link layer	CHAP, PPTP, L2TP, WEP (WLAN), A5 (GSM), Bluetooth
Physical layer	Frequency Hopping (**), Glasfaserkabel (***), Quantum Key Distribution

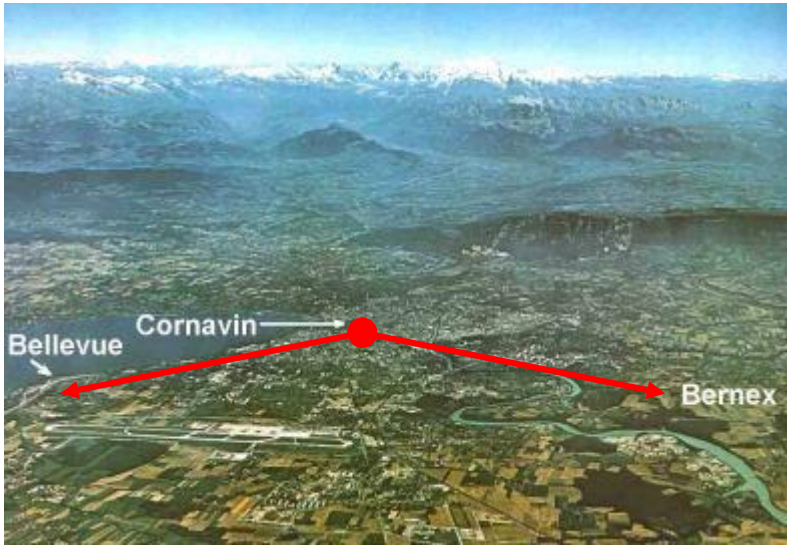
(*) Wireless TLS

(**) Mit regelmässigem Wechseln der Funkfrequenz, wollte man das reine Abhören verhindern.

(***) So ca. Ende der 1990-er Jahre glaubte man, dass Glasfaserkabel nicht abgehört werden können.

Quantum Key Distribution (QKD)

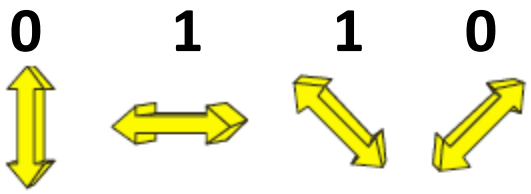




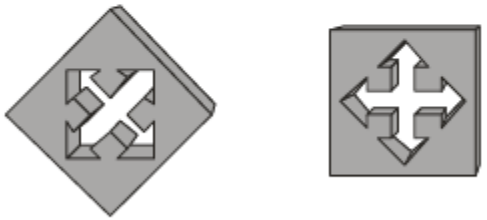
- Nicolas Gisin et al. University of Geneva
- Compact source emitting entangled photon pairs
- Quantum correlation over more than 10 km

The Polarization

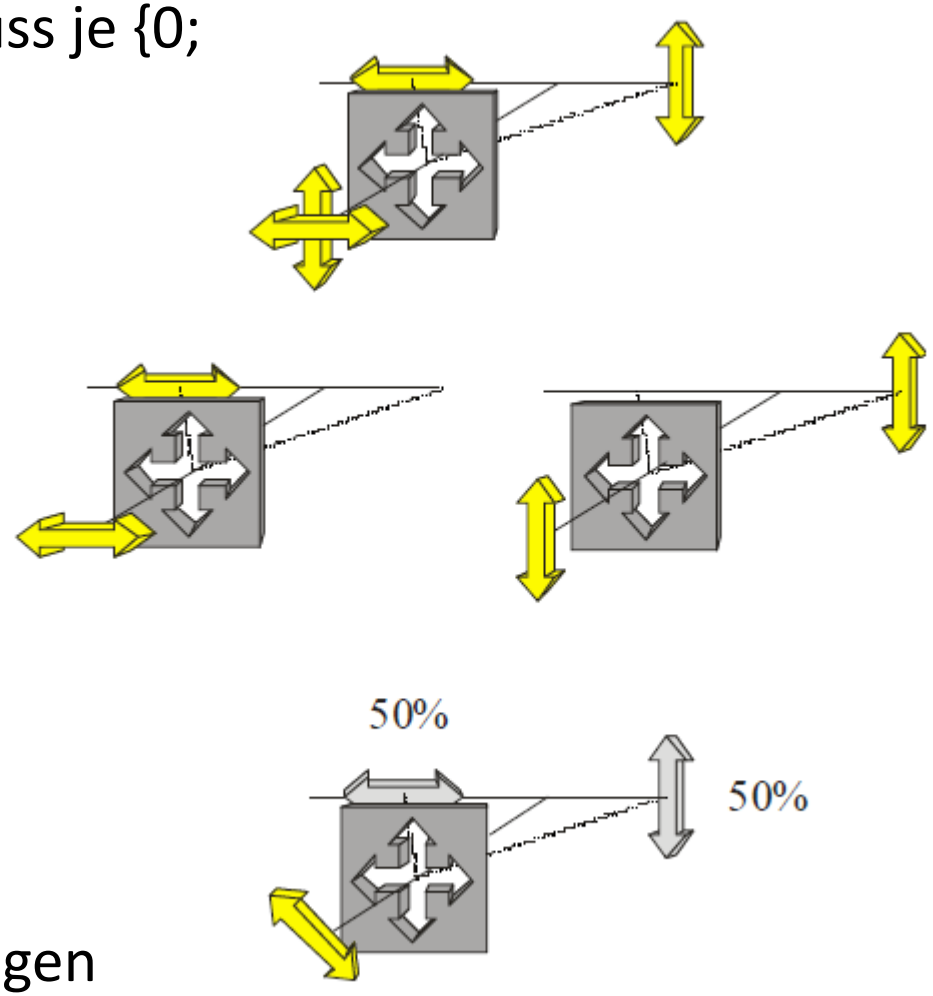
Den Zuständen senkrecht/waagrecht sowie schräg links/rechts muss je {0; 1} zugeordnet werden. Z.B.



Linear polarization states



Filters



Aufgabe 1

Wie viele mögliche Codierungen gibt es somit?

Quantum Key Exchange

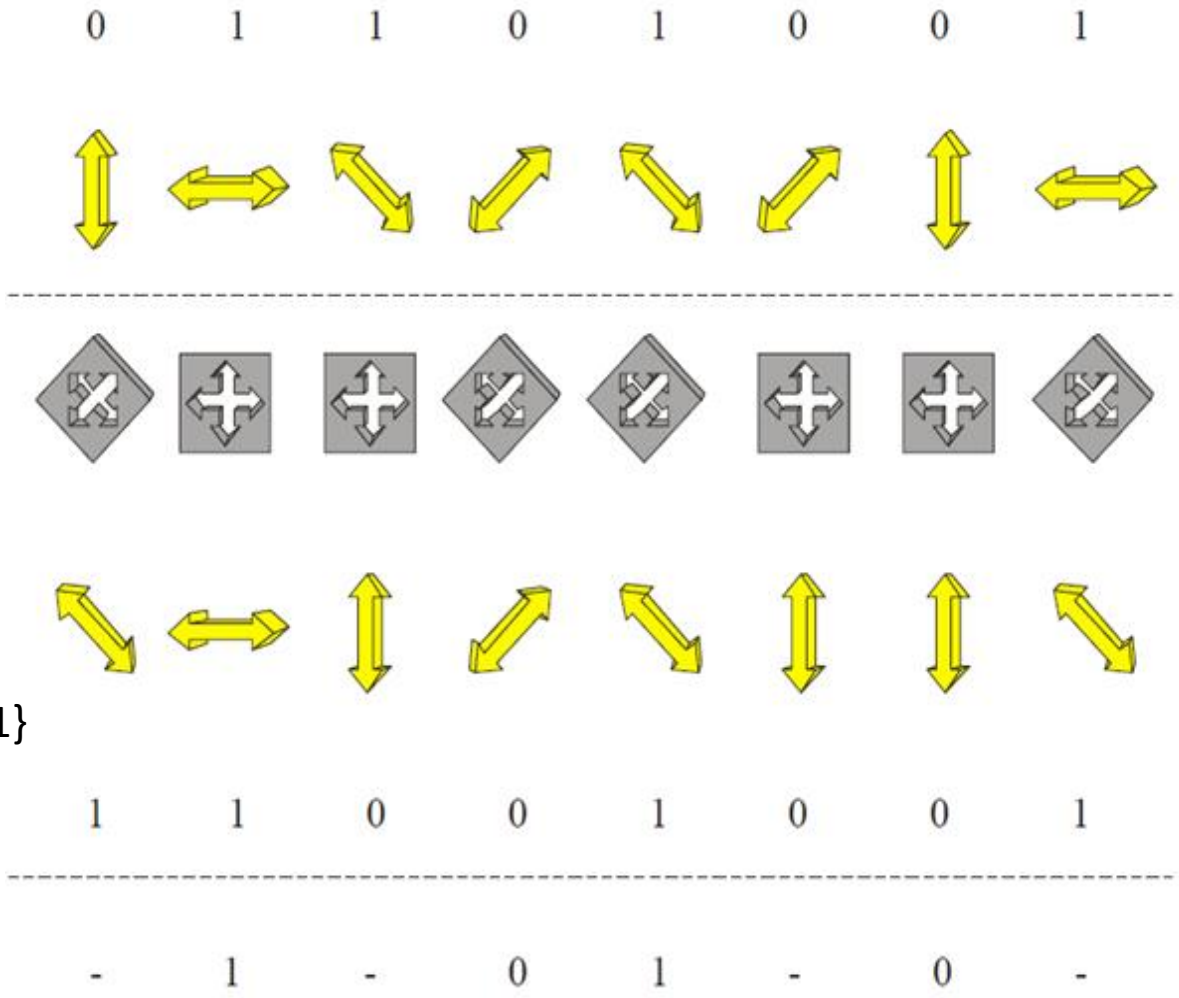
Sender Alice wählt zufällige Bits.

Alice schickt diese als Photonen, wählt die Polarisation.

Empfänger Bob wählt zufällig jeweils einen Filtertyp.

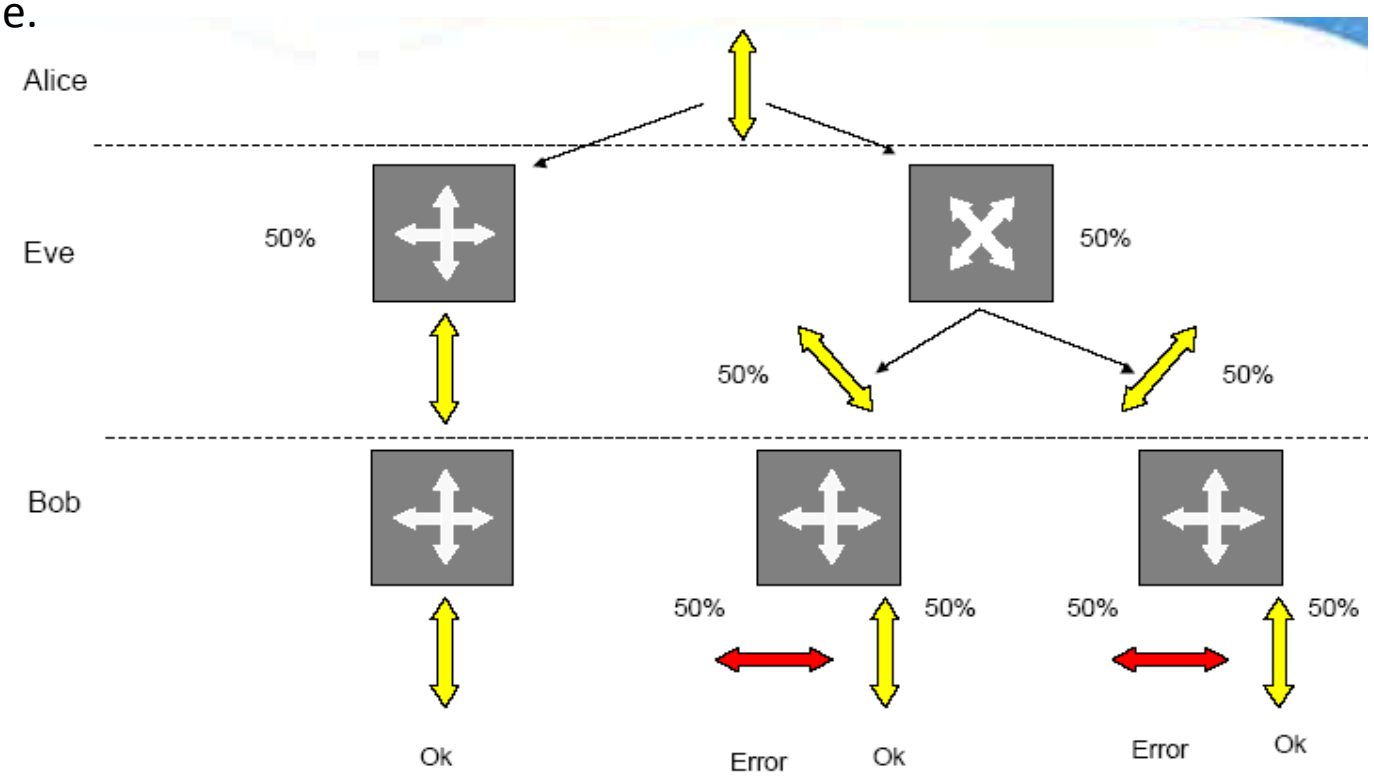
Bob erhält z.B. die folgenden Photonen.

Da er die Codierung kennt, kann er die Photonen an {0; 1} zuordnen.
Er telefoniert mit Alice und gibt ihr die Reihenfolge der gewählten Filter durch.
Aufgrund diese Information teilt sie ihm mit: «Du kannst das 2., 4., 5., & 7. Bit nehmen.



Eavesdropping Frage: Was passiert, wenn Eve abhört?

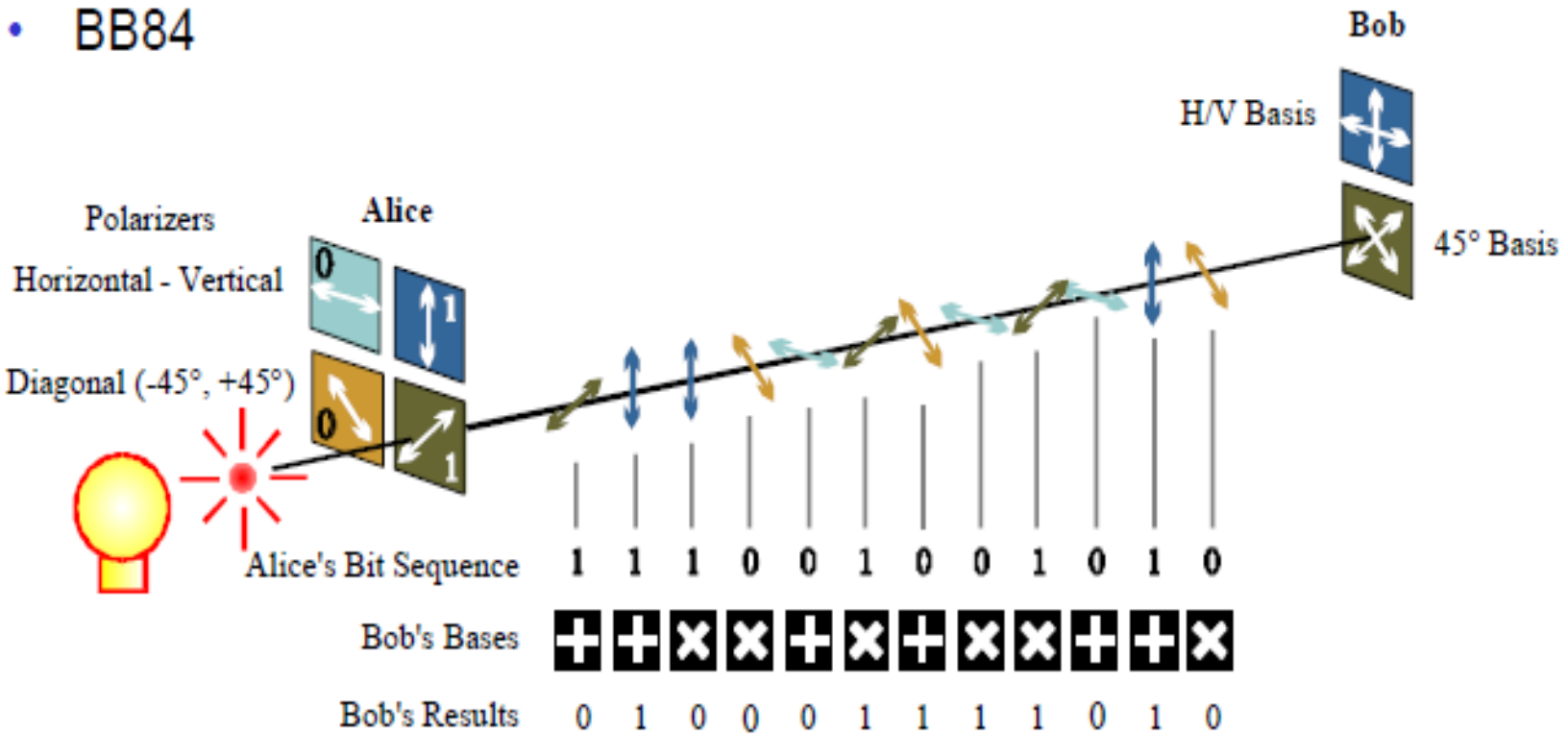
Eve muss auch einen Filtertyp nehmen. Sie nimmt im statistischen Mittel die Hälfte aller Filter falsch.
Wenn sie den korrekten Filter nimmt, dann passiert nichts, wenn sie den falschen Filter nimmt, sind im stat. Mittel die Hälfte der Bits mit falschem Filter gekippt. Also, wenn Eve abhört, verändert sie im stat. Mittel ein Viertel aller gesendeten Bits. Daher sendet z.B. Alice an Bob ca. die Hälfte aller „guten“ Bits über einen unsicheren Kanal zu. Alice vergleicht diese mit ihren Bits. Sind Bits verändert, so wurden sie abgehört und beginnen von vorne.



Aufgabe 2

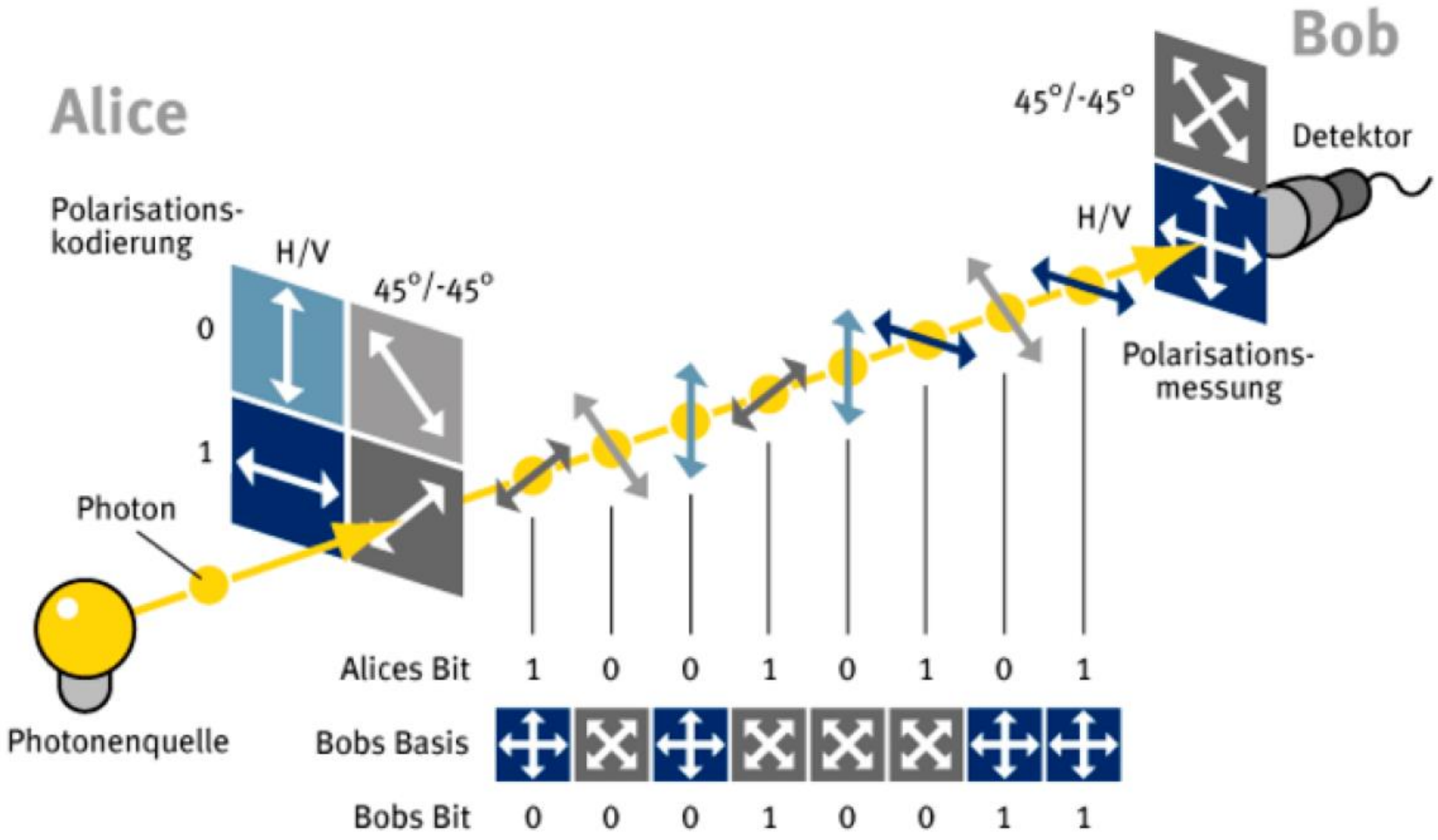
Welche Bits können nun verwendet werden? Achten Sie auf die Codierung!

- BB84



Aufgabe 3

Welche Bits können nun verwendet werden?



Drei entscheidende Fragen

Frage 1: Was hat man nach dem Austausch?

- Nach dem Austausch hat man – analog zu Diffie-Hellman – einen symmetrischen Schlüssel K ausgetauscht. Dieser Schlüssel ist aber nicht vom Sender – also Alice – direkt gewählt. Wenn Sie aber einen direkt gewählten Schlüssel K_{Alice} austauschen will, so kann sie diesen nun mit K verschlüsselt austauschen. In diesem Fall ist K „nur“ ein KEK = Key encryption Key → dies analog zum Elgamal.

Frage 2: Wie viele Bits braucht es?

Nehmen wir an, wir wollen einen 256 Bit AES Schlüssel austauschen. Wie viele Bits x müssen nun mittels QK resp. QSV ausgetauscht werden?

- Von x Bits sind ca. die Hälfte nicht brauchbar, da der falsche Filter gewählt wird.
- Ca. die Hälfte der guten Bits werden gebraucht, um zu überprüfen, ob man abgehört wurde.
- Also x/4 = 256 → x = 1024
- **Alternative:** Mit den korrekt ausgetauschten Bits könnte man eine Meldung MAC’en und zuschicken. So wüsste man auch, ob der Key nicht verfälscht wurde. Aber ev. gibt es dann andere Attacken.

Frage 3: Was ist nun Fundamental neu?

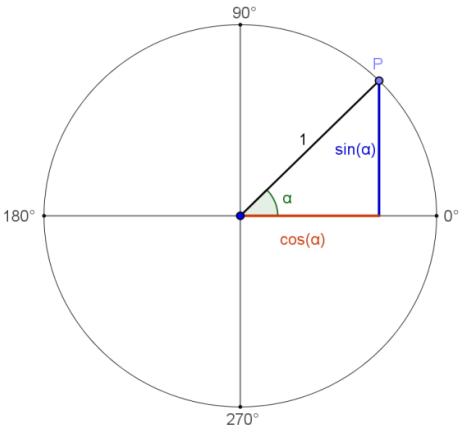
- Es kann zum ersten Mal Abhören entdeckt werden.
- Damit wird Abhören – was eigentlich eine passive Attacke ist – neu zu einer aktiven Attacke → Denial of Service = DOS.

Quantencomputer QC

Bit und Qubit, oft auch Qbit genannt

- Im klassischen Computer wird mit Bits (binary digits), also mit den Werten 0 und 1 gerechnet.
- Quantenbits gehorchen – im Gegensatz zu den klassischen Bits – nicht den Gesetzen der klassischen Mechanik, sondern den Gesetzen der Quantenmechanik. Ein Qubit (quantum bit) nimmt die Werte „0“ und „1“ oder etwas DAZWISCHEN an.
- Ein möglicher Vergleich:
  - In den ganzen Zahlen $\mathbb{Z}$ gibt es zwei Zahlen z mit Betrag $|z| = 1$, nämlich ± 1.
  - In den reellen Zahlen $\mathbb{R}$ gibt es unendlich viele Zahlen z mit Betrag $|z| = 1$, nämlich alle Zahlen, die auf dem Kreis mit Radius 1 liegen.

    D.h. sie erfüllen die Kreisgleichung $x^2 + y^2 = 1$ und können in der Form $(\cos(\alpha)\,;\sin(\alpha))$ dargestellt werden. Der Bezug zur 2-dim. Darstellung ist wichtig, denn ein Qubit wird $|q\rangle = a \cdot |0\rangle + b \cdot |1\rangle$ mit $a, b \in \mathbb{C}$ und $|a|^2 + |b|^2 = 1$ dargestellt. Wir gehen aber nicht näher auf diese Darstellung ein.



Bit und Qubit

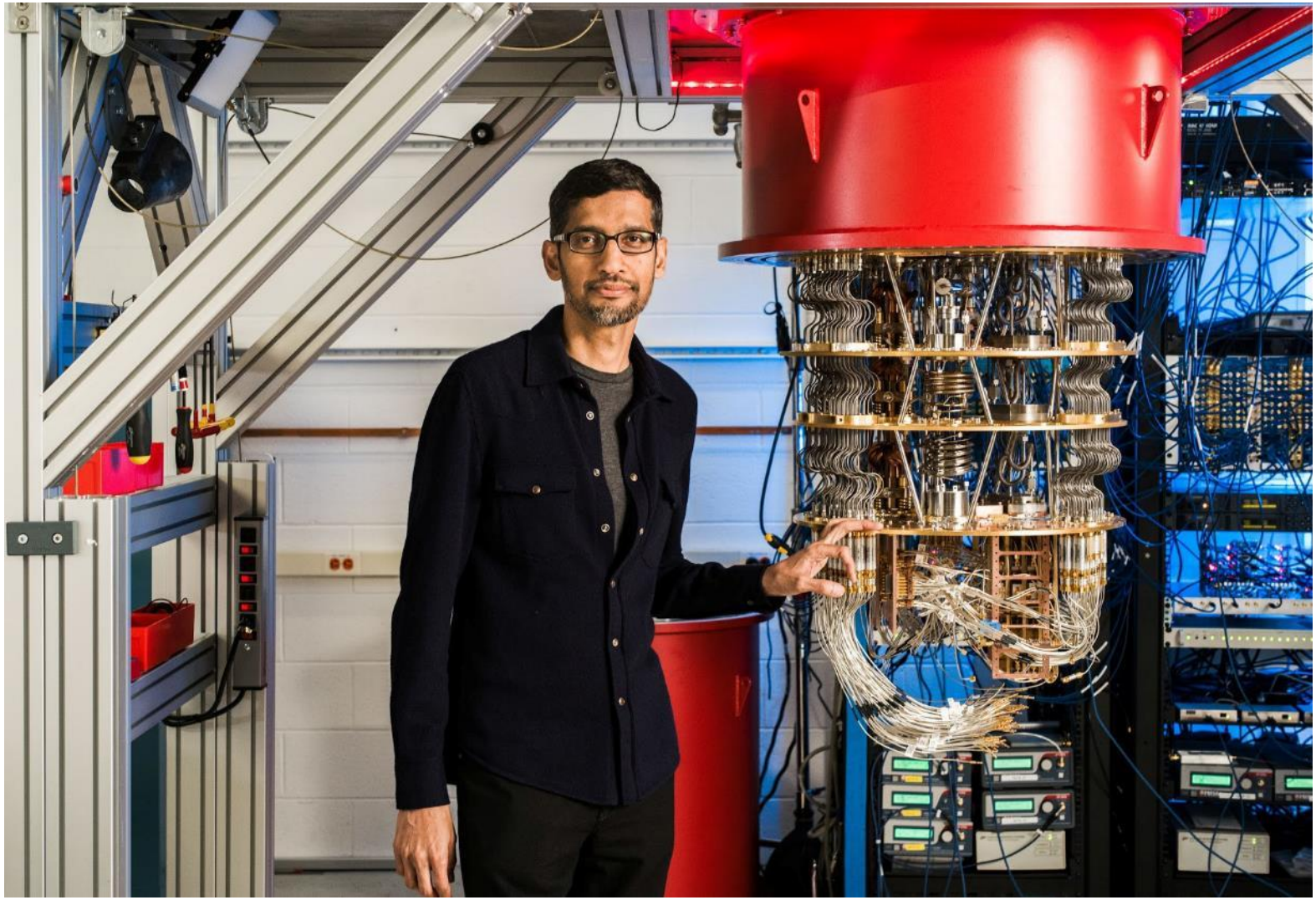
- Rechnen mit Bit wird mit klassischen Schaltkreisen wie das NOT-, AND-, OR- & XOR-Gatter umgesetzt; jeweils realisiert mit 0 = „Strom fliesst nicht“ und 1 = „Strom fliesst“.
- Das NOT-Gatter wird auf ein Bit angewandt (macht aus 0 eine 1 resp. umgekehrt). Die anderen Gatter werden jeweils auf 2 Bits angewandt.

- Rechnen mit Qubit wird mit Pauli-X-Gatter (spiegelt am 45^0-Winkel), Pauli-Z-Gatter (spiegelt am 0^0-Winkel), Hadamard-H-Gatter (spiegelt am $22{,}5^0$-Winkel) umgesetzt.
- Qubits können grundsätzlich mit allen quantenmechanischen Systemen realisiert werden:
  - Ionen in Ionenfallen
  - Elektronen in Quantenpunkten
  - Supraleitende Schaltkreise
  - Kernspins in Molekülen und Festkörpern
  - Photonen (für Qubits und damit Quanten Computing eher ungeeignet; im Gegensatz zur Quantenschlüsselverteilung).

Key Words zu Quantum Computing

- Revolutionäre neue Berechnungsmethode auf der Grundlage der Quantenmechanik.
- Kann bestimmte mathematische Probleme viel schneller lösen.
- Wichtige Anwendungen für
    - Wirtschaft
    - Meteorologie
    - Medizin
    - Sicherheit (nicht nur Krypto)
    - U.a.
- Sehr schwer zu bauen, derzeit gibt es nur Prototypen.
- Technologie wird schnell verbessert.
    - Cf. nachfolgende Folie mit einem heutigen Quantencomputer.
    - Die ersten Röhrencomputer waren auch riesige Schränke und konnten nur ganz wenige Sachen rechnen.
    - Die Miniaturisierung wird auch hier unaufhaltsam sein.
- Riesige Geschäftsmöglichkeiten.
- Grosse Player wie Amazon, Baidu, Google, IBM, Intel, Microsoft, … sind dabei.

Ein heutiger Quantencomputer

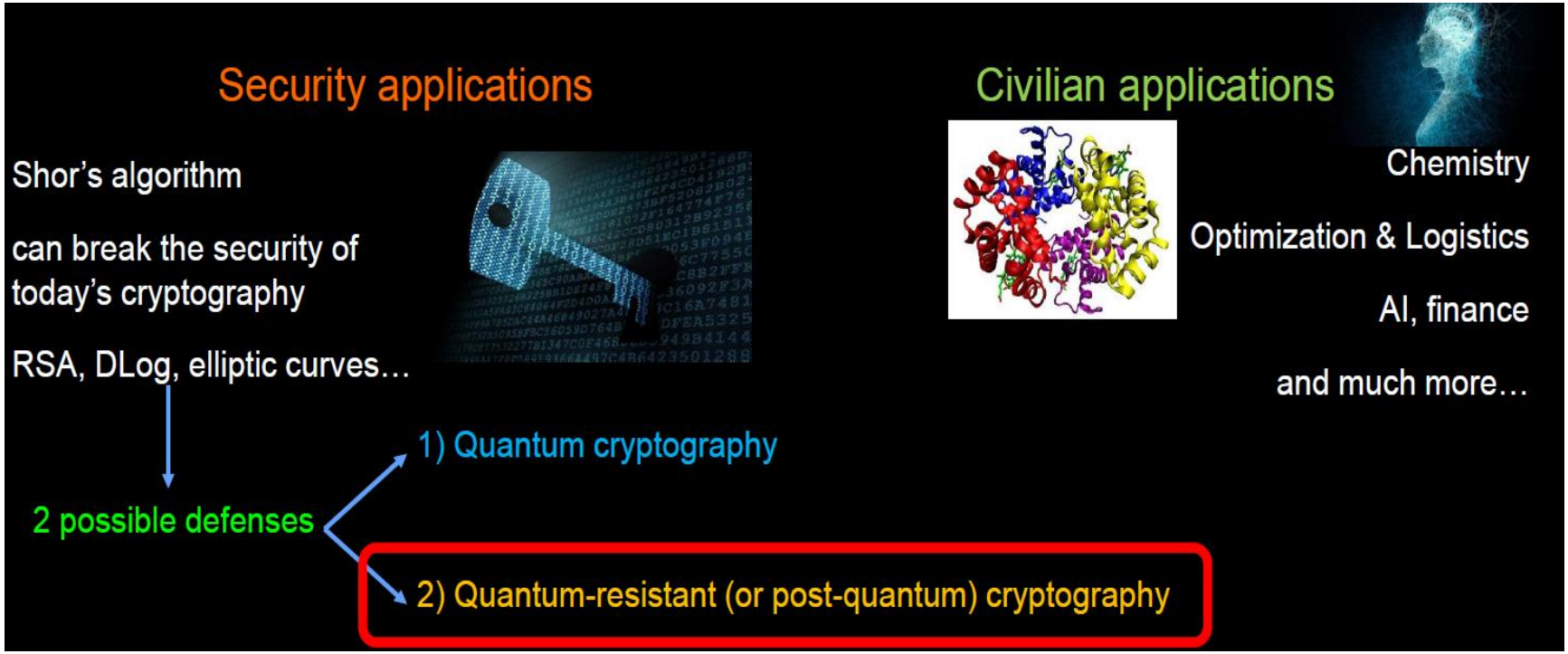


Quanten Comp.: Stand heute, die harten Fakts

1. Quantencomputer gibt es bereits in Form von Prototypen (noch nicht sehr leistungsfähig).
2. Der Bau von Qubits und die Manipulation von Qubits für Berechnungen ist schwierig (Aufwand skaliert exponentiell, starkes Rauschen).
3. Derzeitige Qubits sind nur für einige Millisekunden stabil.
4. Jede Berechnung, die auf einem Quantencomputer läuft, kann auch auf einem klassischen Computer simuliert werden (mit entsprechenden Speicher- und Zeitaufwand).
5. Es gibt keinen Beweis dafür, dass ein Quantencomputer mehr als einen „bescheidenen“ Geschwindigkeitszuwachs gegenüber einem klassischen Computer erzielen kann → z.Z. eher Spekulationen für einige wenige Problemfälle.
6. Die Anzahl der Qubits sind nur ein Kriterium, um die Leistung zu bewerten.
7. Trotzdem, Stand heute 1121 (verrauschte) Qubits bestätigt (IBM Condor)

Warum sind QC trotzdem interessant?

1. Ein „bescheidener“ Geschwindigkeitszuwachs in der Theorie bedeutet ggf. einen „enormen“ Geschwindigkeitszuwachs für viele praktische Probleme (Grovers, Shors Algorithmus u.a., quadratischer Geschwindigkeitszuwachs).
2. Die wenigen Problemkandidaten, die auf einem Quantencomputer leicht zu lösen sind, aber auf einem klassischen Computer (vermeintlich) schwer zu lösen sind, sind sehr wichtig!



2 Beispiele von solchen Algorithmen

1) Grover Algorithmus

a) Der Grover-Algorithmus ist ein Quantenalgorithmus zur Suche in einer unsortierten Datenbank mit N Einträgen in $\mathcal{O}\left(\sqrt{N}\right)$ und mit $\mathcal{O}(\log N)$ Speicherbedarf. Er wurde von Lov Grover im Jahre 1996 veröffentlicht und gehört zu den ersten Quantenalgorithmen, für die bewiesen wurde, dass sie mit der Problemgrösse besser skalieren als der beste klassische Algorithmus. Im Fall des Grover-Algorithmus handelt es sich um einen quadratischen Speed up.

b) Auf einem klassischen Computer ist der prinzipiell schnellstmögliche Suchalgorithmus in einer unsortierten Datenbank die lineare Suche, die $\mathcal{O}(N)$ Rechenschritte erfordert. Der Grover-Algorithmus liefert damit eine quadratische Beschleunigung, was für grosse N beträchtlich ist.

c) Wie die meisten Quantenalgorithmen ist der Grover-Algorithmus ein probabilistischer Algorithmus, d.h., er gibt die korrekte Antwort mit hoher Wahrscheinlichkeit, wobei die Wahrscheinlichkeit einer fehlerhaften Antwort durch wiederholte Ausführung des Algorithmus verkleinert werden kann.

2 Beispiele von solchen Algorithmen

2) Shor's Algorithmus

a) Der Shor-Algorithmus ist ein Quantenalgorithmus zur Faktorisierung von zusammengesetzten Zahlen. Er ist einer der wichtigsten Quantenalgorithmen.

b) Die beste Variante des Shor's Algorithmus braucht für einen RSA mit N Bit Moduls $2N + 3$ Qubits bei fehlerfreien Quantencomputer.

c) Wegen dem Anwenden von Quantenfehlerkorrekturverfahren, schätzt man die benötigte Anzahl von Qubits für eine 2048-Bit-Zahl auf 10 bis 100 Millionen.

d) Der Algorithmus wurde 1994 von Peter Shor veröffentlicht.

e) Shor hat auch einen Quantenalgorithmus zum Berechnen des diskreten Logarithmus beschrieben, der ebenfalls als Shor-Algorithmus bezeichnet wird. Im Allgemeinen wird diese Bezeichnung jedoch für das Faktorisierungsverfahren verwendet.

Erste zusammenfassende Aussagen

- RSA (Faktorisierungsproblem), Disk. Log. Systeme, ECC usw. werden mit Quantencomputer und genügenden Qubits unsicher.
- Man arbeitet heute schon an neuen asymmetrischen Krypto-Verfahren, den sog. PQC = Post Quantum Cryptography Algorithmen (Begriff leider unglücklich, besser wäre Quantum-Resistant Crypt). Standardisierung ca. 2025. https://www.nist.gov/pqcrypto
- Blockchiffren sind viel resistenter als asymmetrische Verfahren, dennoch muss man beachten, dass die Angriffe mit QC auf Blockchiffren ca. im Quadrat besser sind als Brute-Force Attacken.
- Bei AES mit einem 128 Bit Schlüssel ist Brute Force ein Aufwand von $2^{128} \approx 3{,}4 \cdot 10^{38}$
- … mit QC wären es noch $\sqrt{2^{128}} = 2^{\frac{128}{2}} = 2^{64} \approx 1{,}8 \cdot 10^{19}$.
- … mit Merkle Hellman $k^{\frac{2}{3}}$ sind es $(2^{128})^{\frac{2}{3}} = 2^{128 \cdot \frac{2}{3}} = 2^{\frac{256}{3}} \approx 5 \cdot 10^{25}$
- … mit Merkle Hellman worst case $k^{\frac{1}{3}}$ sind es $(2^{128})^{\frac{1}{3}} = \sqrt[3]{2^{128}} \approx 7 \cdot 10^{12}$
- **Fazit 1:** Also ein 128 Bit AES genügt nicht mehr, da 2^{64} zu wenig sicher wäre.
- **Fazit 2:** Angriffe auf Blockchiffren mit Quantencomputer liegen damit zwischen dem $k^{\frac{2}{3}}$ Aufwand von Merkle Hellman und dem $k^{\frac{1}{3}}$ Aufwand des vermuteten worst case von Merkle Hellman.

Brute-Force	Merkle-Hellman mit $k^{2/3}$	Mit Quantencomputer mit $\sqrt{k} = k^{1/2}$	Merkle-Hellman vermutet mit $\sqrt[3]{k} = k^{1/3}$
2^{128}	$(2^{128})^{2/3} \approx 2^{85}$	$(2^{128})^{1/2} = 2^{64}$	$(2^{128})^{1/3} \approx 2^{43}$

ECC, RSA und Quantencomputer (QC)

- **Qubits**
  - Bei Quantencomputer wird mit Qubits gerechnet.
  - Bei k Bits im klassischen System braucht es …
    - … für die Faktorisierung von k Bits mit QC bei RSA $K \approx 2k$ Qubits.
    - … für d. DL-Probl. von k Bits mit QC bei EC $K \approx 5k + 8\sqrt{k} + 5log_2 k$ Qubits.
    - ***Achtung:*** diese Abschätzungen können sich mit besseren (Quanten-) Algorithmen (wesentlich) verändern. Zudem beruhen diese Abschätzungen auf fehlerfreie Quantencomputer. Mit Einsatz von Quantenfehlerkorrekturverfahren kann sich die Anzahl um Grössenordnungen vervielfachen.

- ***Beispiel***
  - 3072 Bit RSA ist im Rahmen der klassischen Methoden ungefähr gleich stark wie 256 Bit ECC.
- Es braucht nun:
  - Faktorisierung von k = 3072 Bits bei RSA $K \approx 2k = 2 \cdot 3072 = 6144$ Qubits
  - DL bei ECC, k = 256 Bits $K \approx 5 \cdot 256 + 8\sqrt{256} + 5log_2 256 = 1448$ Qubits
  - Für QC bräuchte es für ECC p = 1164 Bit um so stark wie ein RSA 3072 zu sein. D.h. der Sicherheitslevelunterschied von ECC und RSA ist mit/ohne QC unterschiedlich.

Qubits, Stand per 17. Nov. 21

Andreas Wallraff
Der Professor für Festkörperphysik an der ETH Zürich leitet dort das Quantum Device Lab.

Im TagesAnzeiger https://epaper.tagesanzeiger.ch/?idp=CeleraOne&new_user=no#read/20/Tages-Anzeiger/2021-11-17/34 erschien am 17. Nov. 2021 ein Interview von Prof. Wallraff.

Zusammenfassung:

- 2019: 53-Qubit-Prozessor von Google, präsentiert an einem konstruierten Problem, welches für die Praxis völlig irrelevant ist.
- 2021: IBM stellt einen 127-Qubit-Prozessor ohne Anwendung an einem Problem vor.
- Ankündigung von IBM: demnächst einen 433-Qubit-Prozessor vorzustellen.
- Ankündigung von IBM: 2023 einen 1121-Qubit-Prozessor.
- Es ist durchaus möglich, dass für ganz grosse Aufgaben 100’000-Qubit-Prozessoren nötig sein werden!

Das ganze Interview kann in Kap. 16.8 im JS Skript «Einführung in die Kryptologie» nachgelesen werden.

QC, die Zukunft

- 2019: 53-Qubit-Prozessor von Google, präsentiert an einem konstruierten Problem, welches für die Praxis völlig irrelevant ist.
- 2021: IBM stellt einen 127-Qubit-Prozessor ohne Anwendung an einem Problem vor.
- Ankündigung von IBM: demnächst einen 433-Qubit-Prozessor vorzustellen.
- Ankündigung von IBM: 2023 einen 1121-Qubit-Prozessor.
- Es ist durchaus möglich, dass für ganz grosse Aufgaben 100’000-Qubit-Prozessoren nötig sein werden!

Das ganze Interview kann in Kap. 16.8 im JS Skript «Einführung in die Kryptologie» nachgelesen werden.

Aufgabe 4

Betrachten Sie nun einen RSA mit einem 7680 Bit Moduls und eine im klassischen Sinne gleich starke Elliptische Kurve mit p gleich 384 Bit. Beantworten Sie die folgenden Fragen:

a) Wie viel Qubits braucht es für das Faktorisierungsproblem des RSA mit 7680 Bit Modulus mit einem Quantencomputer zu lösen?
b) Wie viel Qubits braucht es für das Lösen des diskreten Logarithmusproblems für EC mit p = 384 Bit mit einem Quantencomputer zu lösen?
c) Ist es nun immer noch richtig, dass ein 7680 Bit RSA und eine 384 Bit ECC gleich stark sind, wenn man die Quantencomputersicherheit betrachtet? Wer ist bez. der Angriffe mit einem Quantencomputer sicherer, der RSA 7680 oder der EC-384?
d) Wie gross müsste die Zahl der Bits des bez. Quantencomputer unsichereren Algorithmus sein, damit diese zwei Algorithmen bez. der Quantencomputersicherheit wiederum gleich stark wären?
e) Lesen Sie nun in [CP-D], S. 166, den Abschnitt „Blockchiffren und Quantencomputer“. Formulieren Sie nun die zwei wichtigsten Kernaussagen aus diesem Abschnitt.

Wann sollten wir beunruhigt sein?

A = Notwendige Zeit für Forschung, Standardisierung und Entwicklung von neuen Quanten-Resistenten Algorithmen und Quantencomputer.

B = Die Zeit, in der die heutigen Produkte (oder die darin verarbeiteten Informationen) sicher bleiben müssen.

C = Die Zeit, bis ein skalierbarer Quantencomputer mit stabilen Qubits gebaut ist.

Wenn A + B > C dann *sind wir in Schwierigkeiten, resp. zu spät dran!*

Man beachte, dass …

- … gewisse Daten (z.B. in der Medizin, oder sonstige Archivierungen) oder Produkte eine grosse Sicherheitszeit haben, ev. muss umverschlüsselt (ein 128 Bit AES wäre kaum mehr genügend → 256 Bit AES wird dann obligatorisch) oder umsigniert (Quanten-Resistente Algorithmen).

OK, wir sind …

- … immer noch im Zeitslot A.

Geht es konkreter?

- China (Schätzung gemäss McKinsey) investierte bis jetzt 4 – 17 Milliarden $.
- USA budgetierte Ende 2022 ca. 2,5 Milliarden $ in „The Plan for Quantum“ zu investieren.
- Die EU will bis ca. 2032 ca. 1 Milliarde € mit „EU Quantum Technologies Flagship “ in hunderte Forschungsprojekte stecken.
- The French Cybersecurity Agency (ANSSI) empfiehlt ab 2025 auf hybride Lösungen und ab 2030 komplett auf Quanten-Resistente Algorithmen zu wechseln.
- Die NSA (National Security Agency = grösster Auslandgeheimdienst der USA) setzt die Deadline für Quanten-Resistente Algorithmen im Bereich der Regierung auf 2035.
- Die Quantencomputing Forschung geht vorwärts.
- Die Anzahl von fehlerfreien (stabil und ohne Rauschen) Qubits wird eine neue Standardgrösse sein.
- Machen wir nicht den Fehler, aus der Vergangenheit zu extrapolieren: Wir müssen nichtlineare Fortschritte erwarten (cf. AI).
- ***Slogan (3) Quantencomp. werden nach AI die nächste „Revolution“ sein.***

Basis-Test PR 13_1

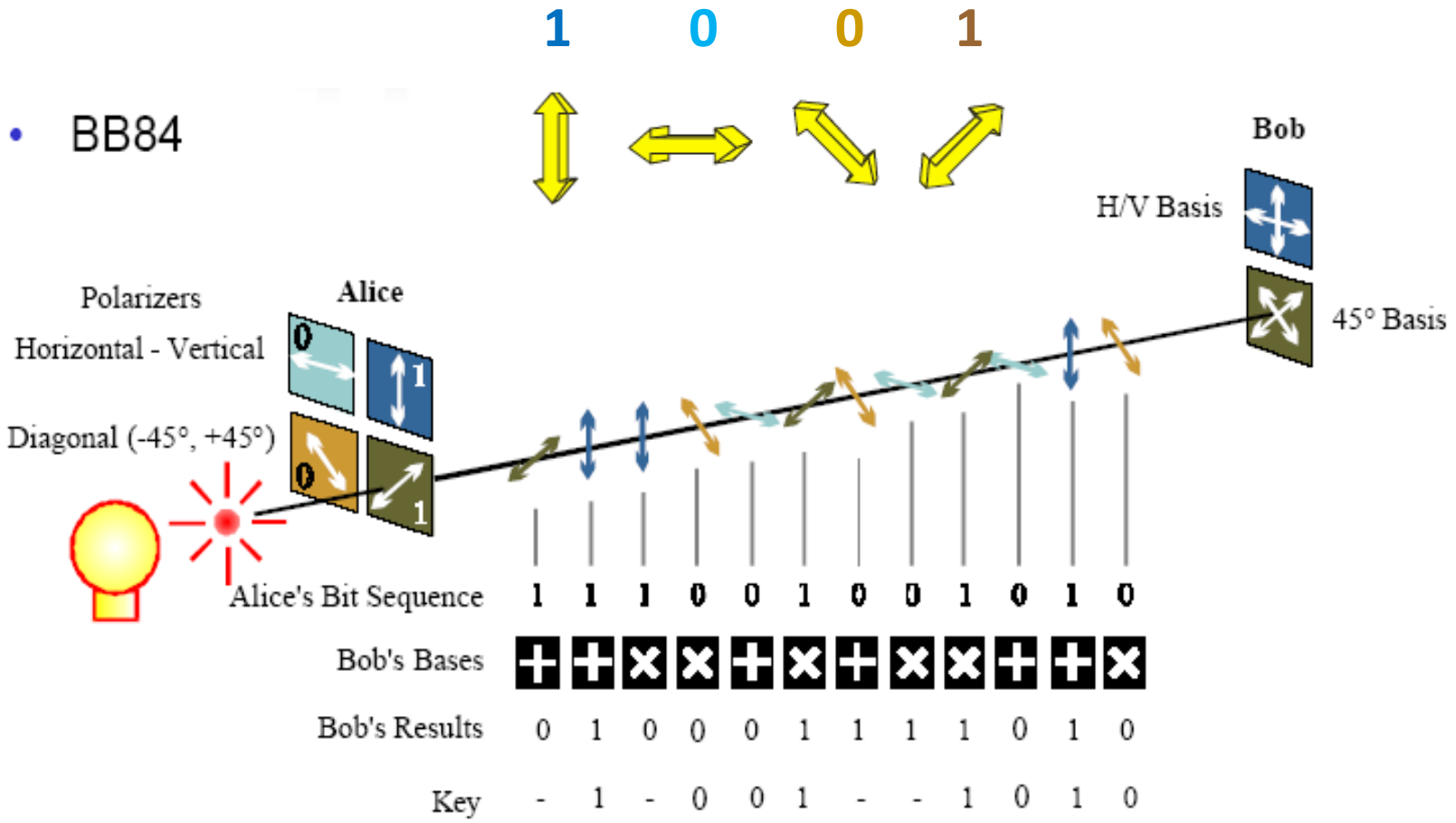
Aussage	Richtig oder falsch?	Begründung
Quantenkryptologie befasst sich nur mit dem Quantenschlüsselaustausch.	☐ richtig ☐ falsch	
Quantenkryptologie hat nichts mit Quantencomputer QC zu tun.	☐ richtig ☐ falsch	
Pro ausgetauschtes Schlüsselbit müssen im stat. Mittel 4 Bit übermittelt werden.	☐ richtig ☐ falsch	
Es gibt keine bekannten Attacken den Quantenschlüsselaustausch.	☐ richtig ☐ falsch	
Erst eine ca. 1200 Bit ECC ist in Bezug auf Quantencomputer in etwa gleich sicher wie ein 3072 Bit RSA.	☐ richtig ☐ falsch	
Asymmetrische Verfahren sind in Bezug auf Quantencomputer nicht so gefährdet.	☐ richtig ☐ falsch	
Ein n-Bit symmetrische Blockchiffre wird beim Einsatz von QC noch etwa die Sicherheit von n/2 Bit haben.	☐ richtig ☐ falsch	
In Bezug auf QC muss man z.Z. noch keine wirkliche Angst haben, darum werden auch noch keine Gegenmassnahmen diskutiert.	☐ richtig ☐ falsch	
Wenn eine Quantenschlüsselverteilung implementiert ist, so ist man gegen Denial of Service Attacken geschützt.	☐ richtig ☐ falsch	
Die Sicherheit bei einer Quantenschlüsselverteilung liegt darin, dass bemerkt wird, ob man abgehört worden ist oder nicht.	☐ richtig ☐ falsch	

Lösungen

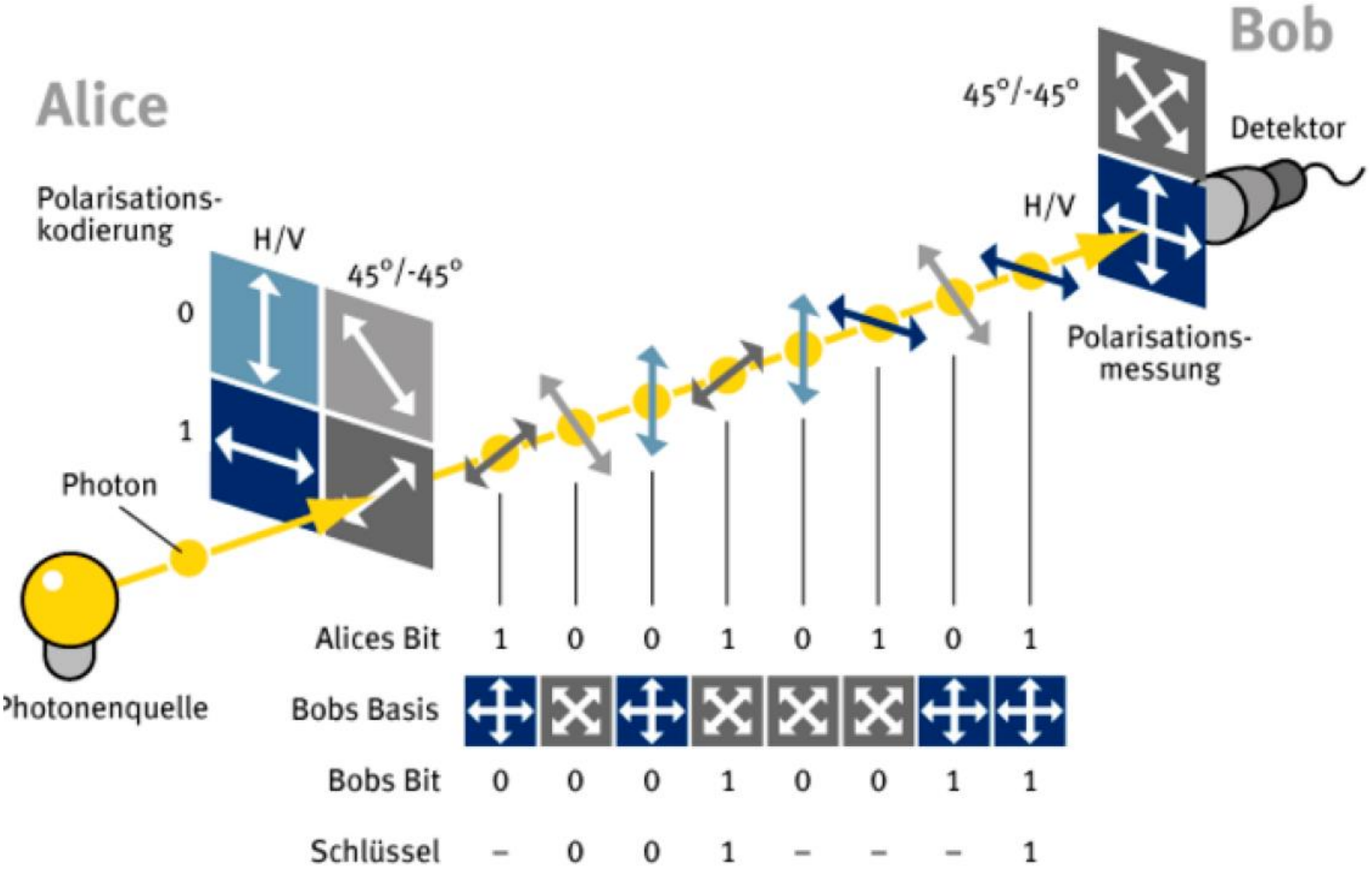
Aufgabe 1

Für die Zustände senkrecht/waagrecht und schräg je 2, damit gibt es 2*2 mögliche Codierungen.

Aufgabe 2 Die Codierung ist in diesem Fall anders und lautet:



Aufgabe 3


Alice
Bob
Polarisations-
kodierung
H/V
45°/-45°
0
1
Photon
Photonenquelle
45°/-45°
H/V
Detektor
Polarisations-
messung
Alices Bit 1 0 0 1 0 1 0 1
Bobs Basis
Bobs Bit 0 0 0 1 0 0 1 1
Schlüssel – 0 0 1 – – – 1

Aufgabe 4

a) $K \approx 2k = 2 \cdot 7680 = 15360$

b) $K \approx 5k + 8\sqrt{k} + 5 \cdot log_2 k = 5 \cdot 384 + 8\sqrt{384} + 5 \cdot log_2 384 \approx 2120$

c) Nein es ist nun nicht mehr richtig; ein 7680 Bit RSA ist in diesem Bezug sicherer!

d) Es ist die Gleichung $K \approx 5k + 8\sqrt{k} + 5 \cdot log_2 k = 15360$ auf k aufzulösen. Die Gleichung kann nicht formal gelöst werden. Für 4-stellige k überwiegt der lineare Teil, d.h. $5k \approx 15'360$ → k = 3072. Dieses k ist ein bisschen zu gross. Mittels trial and error findet man schnell, dass $k \approx 3'000$ Qbits eine gute Antwort ist (exakt – mit Solver gelöst - wären es $k \approx 2'973$).

e) Die zwei Kernaussagen

(1) «Die in der Praxis eingesetzten asymmetrischen Algorithmen wie RSA, Diffie-Hellman-Schlüsselaustausch oder elliptische Kurven werden durch Quantencomputer angreifbar. Symmetrische Algorithmen sind erheblich robuster gegen Quantencomputerangriffe, denn sie brauchen mehr Qubits.

(2) Bei symmetrischen Verfahren werden Schlüssellängen jenseits von 128 Bit benötigt, um Resistenz gegen Angriffe mit Quantencomputern zu gewährleisten.

Basis-Test PR 13_1

Aussage	Richtig oder falsch?	Begründung
Quantenkryptologie befasst sich nur mit dem Quantenschlüsselaustausch.	☐ richtig ☑ falsch	QK hat zwei Teile, Quantenschlüsselaustausch und Quantenzufallsgeneratoren.
Quantenkryptologie hat nichts mit Quantencomputer QC zu tun.	☑ richtig ☐ falsch	Das einzige, was man sagen kann ist, dass ein Quantenschlüsselaustausch immun gegen QC ist.
Pro ausgetauschtes Schlüsselbit müssen im stat. Mittel 4 Bit übermittelt werden.	☑ richtig ☐ falsch	Ca. die Hälfte der Bits dürfen nicht verwendet werden und ca. ¼ der Bits werden zur Überprüfung, ob man abgehört wurde verwendet.
Es gibt keine bekannten Attacken den Quantenschlüsselaustausch.	☐ richtig ☑ falsch	Mit DOS (Denial of Service) kann der Austausch torpediert werden.
Erst eine ca. 1200 Bit ECC ist in Bezug auf Quantencomputer in etwa gleich sicher wie ein 3072 Bit RSA.	☑ richtig ☐ falsch	Siehe Beispiel in den Folien.
Asymmetrische Verfahren sind in Bezug auf Quantencomputer nicht so gefährdet.	☐ richtig ☑ falsch	Vor allem asymmetrische Verfahren sind in Bezug auf QC gefährdet.
Ein n-Bit symmetrische Blockchiffre wird beim Einsatz von QC noch etwa die Sicherheit von n/2 Bit haben.	☑ richtig ☐ falsch	
In Bezug auf QC muss man z.Z. noch keine wirkliche Angst haben, darum werden auch noch keine Gegenmassnahmen diskutiert.	☐ richtig ☑ falsch	Es ist zwar richtig, dass man z.Z. noch keine Angst vor QC haben muss. Trotzdem läuft ein Wettbewerb, um Post-Quanten-Algorithmen zu evaluieren.
Wenn eine Quantenschlüsselverteilung implementiert ist, so ist man gegen Denial of Service Attacken geschützt.	☐ richtig ☑ falsch	Im Gegenteil, nur mit Abhören kann Eve es fertig bringen, dass Alice und Bob nie einen Schlüssel austauschen können.
Die Sicherheit bei einer Quantenschlüsselverteilung liegt darin, dass bemerkt wird, ob man abgehört worden ist oder nicht.	☑ richtig ☐ falsch	

Quellenangaben & Danksagung

- Ich habe wiederum einige Folien von Prof. Dr. A. Steffen, HSR übernommen. An dieser Stelle sei ihm wiederum herzlich gedankt.

- Weite Teile der Informationen zu Qubit habe ich aus dem Buch „Quantencomputing kompakt“ von Bettina Just, Technische Hochschule Mittelhessen.

- Viele Informationen und Inhalte zu Quantencomputer habe ich von Tommaso Gagliardoni, Kudelski Security, aus den Unterlagen zu seinem Vortrag „Quantum-Resistant Cryptography: Impact on OT and Cybersecurity, and Path to an Actionable Transition“, gehalten am 27. März 2024 an der HSLU I.

- An dieser Stelle an Alle ein herzliches Danke schön.