dacoso
data communication solutions

# post quantum safe

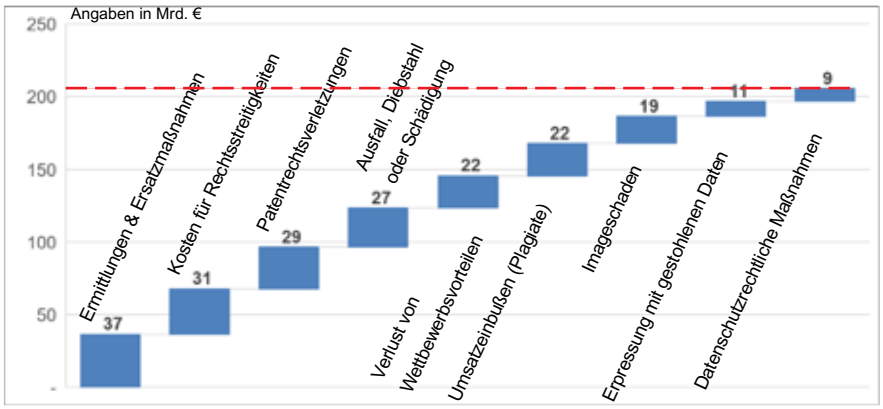
Workshop, Omnisecure Berlin, 21.01.2020


dacoso
data communication solutions

## Cyber-Kriminalität: immer mehr und immer ruinöser

**Schadenssummen durch Datendiebstahl, Industriespionage oder Sabotage**

- über 200 Mrd. €
- Befragung von über 800 Unternehmen in Deutschland im Jahr 2019




Nach wie vor viel zu wenige wirksame Schutzmaßnahmen

Quelle: https://de.statista.com/statistik/daten/studie/444719/umfrage/schaeden-durch-computerkriminalitaet-in-deutschen-unternehmen/

## Neues Risiko on top: Quanten-Computing wird Realität

dacoso
data communication solutions

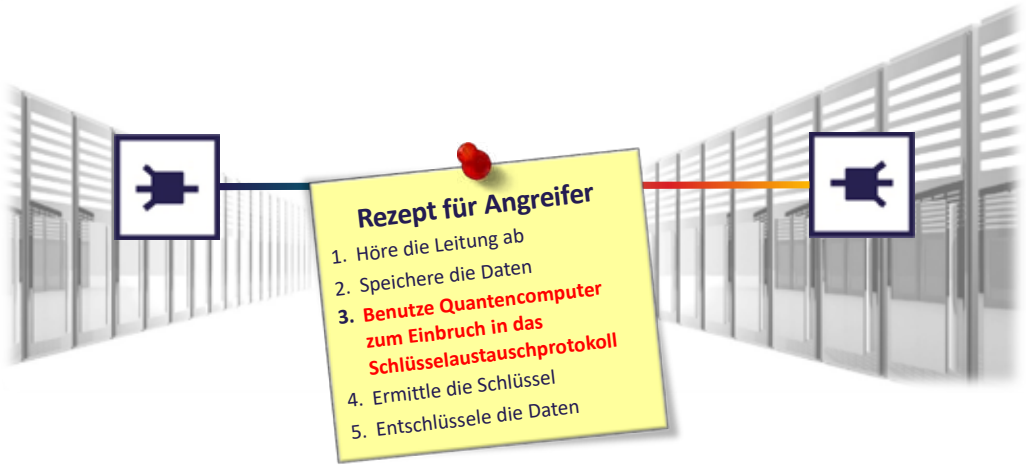

Google Quantum Supremacy Video:
https://www.youtube.com/watch?v=-ZNEzzDcllU





## Quanten-Computer: schnell – und deshalb gefährlich

dacoso
data communication solutions



## **Verschlüsselungs-Lösungen:** Grundlagen und Bausteine

dacoso
data communication solutions



## 3 wichtige Bausteine für Encryption

dacoso
data communication solutions

**Verschlüsselungs-Algorithmus**

0101
1001
1011

Verfahren zum Ver- und Entschlüsseln von Daten

**Authentifizierung**

Sicherstellen der Identität mittels digitaler Zertifikate

**Schlüsselaustausch**

Sicherer Austausch zwischen den Parteien zur Berechnung bzw. Austausch des Schlüssels

**Integritäts-Schutz und Sicherheits-Management**

Hardware- und Software-Vorkehrungen schützen gegen unerlaubtes Eindringen

**Interoperabilität -** sichere Schnittstelle für den Schlüsselaustausch

Mapping der Daten und Schlüsselinformation ins Transportprotokoll

**Zulassung**

Institution stellt konforme und sichere Implementierung fest

## 1. Verschlüsselungs-Algorithmus
Symmetrische Kryptografie

dacoso data communication solutions

**Beschreibung**

Jede symmetrische Verschlüsselung basiert auf einem bestimmten Algorithmus.
Bei einem Verschlüsselungsalgorithmus (Chiffre) wird in den Klartext eine Geheim-Information (Schlüssel) eingebracht und so der Geheimtext gebildet.
Der Schlüssel kann z.B. ein Passwort, eine Nummer oder eine zufällige Bitfolge sein.

**Bekannte Verfahren**

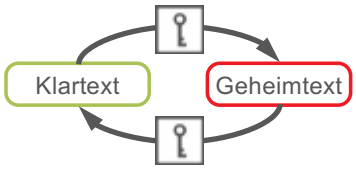
One Time Pad
AES / DES / 3DES

**Vorteil**

hohe Verschlüsselungs-Geschwindigkeit wenn in Hardware implementiert

**Nachteil**

Schlüsselaustausch über den gleichen Kommunikationsweg ist nicht sicher abdeckbar







## 1.Verschlüsselungs-Algorithmus
AES 256

dacoso data communication solutions

- Rijndeal gewann den Wettbewerb um die Nachfolge von DES (DES wurde erstmals 1994 geknackt) und wurde 2001 unter dem Namen AES von der NIST offiziell standardisiert.
- AES sind Blockchiffren auf Basis eines Substitutions-Permutations-Netzwerks (SPN). Das Verfahren wechselt bei jedem Schritt zwischen Substitution und Permutation (SP-Chiffre).
- Die Transformation des Klartextes erfolgt in mehreren Runden gleichen Aufbaus. Der Klartext wird dabei nicht als Ganzes, sondern in Blöcken verarbeitet, wodurch die Beziehung zwischen Klar- und Geheimtext verwischt wird (Konfusion). Bei AES 256 ist die Blocklänge auf 128 Bit und die Schlüsselgröße auf 256 Bit (14 Runden) festgelegt.

**Vorteile**

- komplette Schlüsselsuche aussichtslos
- sehr schnelles Verschlüsselungsverfahren
- geringer Aufwand für die Hardware-Implementierung
- hohe Durchdringung von AES 256

**Nachteile**

- relativ geringe Rundenzahl (14) von AES 256
- mathematisches Modell durch algebraische Formel näherbar - somit möglicherweise berechenbar
- effiziente krypto-analytische Verfahren bekannt – schneller als vollständige Schlüsselsuche

## 2. Authentifizierung

dacoso
data communication solutions

### Begriffsbestimmung

- Authentifizierung
  - Stellt die Prüfung bzw. den Nachweis einer behaupteten Eigenschaft einer Entität dar. Beispielsweise wird durch die Eingabe eines Passworts die vom Benutzer behauptete Identität verifiziert.
- Gängige Authentisierungsmethoden
  - Wissen (Passwort, PIN, Sicherheitsfrage, etc.)
  - Besitz (Chipkarte, TAN-Verfahren, Zertifikate, etc.)
  - Biometrie (Fingerabdruck, Gesichts-Erkennung, Iris-Erkennung, Tippverhalten, etc.)
- Was ist eine zertifikatsbasierte Authentifizierung?
  - Verwendung eines digitalen Zertifikats, um einen Benutzer, einen Computer oder ein Dokument zu identifizieren, bevor diesem Zugang zu einer Ressource, einem Netzwerk, einer Anwendung oder Ähnlichem gewährt wird.





## 3. Schlüsselaustausch
Asymmetrische Kryptografie

dacoso
data communication solutions

### Beschreibung

Die asymmetrische Kryptografie - auch Public-Key-Verfahren genannt – benötigt einen Schlüssel zum **Ver**schlüsseln (Public Key) und einen anderen Schlüssel zum **Ent**schlüsseln (Private Key) der Nachricht.

Der Public Key wird vom Besitzer des Private Keys (Empfänger) generiert und dem Absender übermittelt.

### Bekannte Verfahren

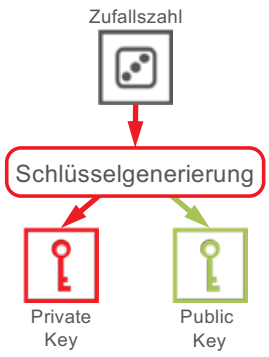
RSA / Digitale Signatur (DSA) / Diffie-Hellman (Elliptic Curve Cryptography: ECC) / McEliece (Post-Quanten-Cryptographie: PQC)

### Vorteil

Nur der Empfänger besitzt den Private Key, der nicht über den Kommunikationsweg übertragen wird.

### Nachteil

benötigt sehr hohe Rechenleistung
(im Vergleich ist AES 1.000 mal schneller als RSA)



## 3. Schlüsselaustausch
Diffie-Hellman-Verfahren

dacoso
data communication solutions

- Ermöglicht, dass zwei Kommunikationspartner über eine öffentliche, abhörbare Leitung einen geheimen Schlüssel (Private Key) in Form einer Zahl vereinbaren können, den nur diese kennen und ein potenzieller Lauscher nicht berechnen kann.
- Das Verfahren zählt zu den Krypto-Systemen auf Basis des diskreten Logarithmus. Diese basieren darauf, dass die diskrete Exponential-Funktion in gewissen zyklischen Gruppen eine Einwegfunktion ist. Das bedeutet, dass die Schlüsselgenerierung über eine sehr einfache mathematische Funktion erfolgt, für die Umkehrfunktion jedoch kein „schneller“ Algorithmus existiert.

**Vorteile**
- problemlose Schlüsselverteilung
- keine Übertragung des Private Keys durch unsichere Kanäle nötig
- obwohl der Algorithmus bekannt ist, ist der Rechen- und Zeitaufwand mit konventioneller Computertechnik derzeit zu hoch, um das Verfahren zu brechen

**Nachteile**
- hohe Rechenzeit bzw. hohe Rechenleistung benötigt
- ‚Man-in-the-middle‘ Attacke möglich – Abhilfe derzeit über ein spezielles Station-to-Station Protokoll (STS)
- ‚Shor‘-Algorithmus mittels Quantencomputer: macht das Verfahren prinzipiell angreifbar – keine post-quantum-safety gegeben




## Hybride Verschlüsselung
Symmetrisch + Asymmetrisch

dacoso
data communication solutions

- Durch geschickte Kombination von symmetrischen und asymmetrischen Verschlüsselungsverfahren ist es möglich, die einzelnen Vorteile beider Systeme zu verbinden, um so eine möglichst effiziente und sichere Verschlüsselung zu erhalten.
- Die Verschlüsselung der eigentlichen Daten erfolgt symmetrisch mit den Session Keys. Diese werden bei jeder Verschlüsselungs-Session zufällig von den zwei Parteien generiert.
- Somit wird die Datenmenge, die zur asymmetrischen Schlüsselgeneration übertragen wird, auf ein Minimum reduziert – das Problem des Schlüsselaustauschs daher elegant gelöst

- Beispiel:
  - Einsatz von Diffie-Hellmann als asymmetrisches Verfahren und AES als symmetrisches Verfahren
  - Dabei dient Diffie-Hellmann nur für den Schlüsselaustausch, wobei der ausgetauschte Schlüssel dann für die Verschlüsselung mit AES verwendet wird.

**…das Beste aus beiden Verfahren ermöglicht effektiven Einsatz**

## Schlüsselaustausch: Wir brauchen zukunftssicheren Schutz

dacoso data communication solutions

**Quantum Key Distribution (QKD)**

Verfahren basiert auf Quantenmechanik

PHYSIK

**Post Quantum Cryptography (PQC)**

Verfahren basiert auf verbesserten Einwegverfahren

MATHEMATIK

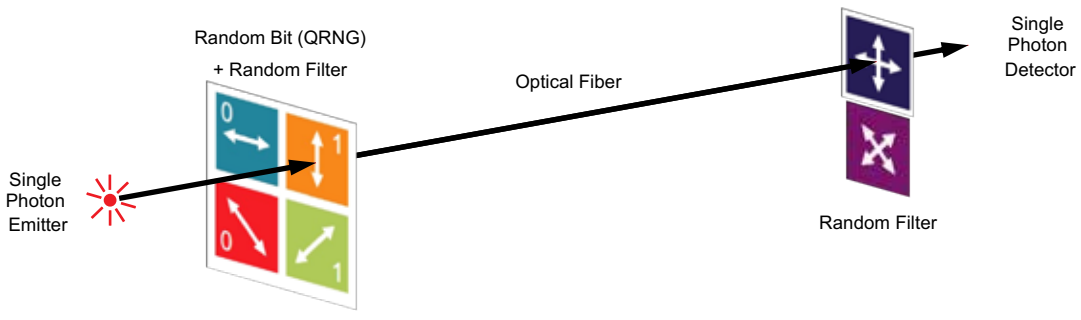




## Schlüsselaustausch: Quantum Key Distribution (QKD)

dacoso data communication solutions

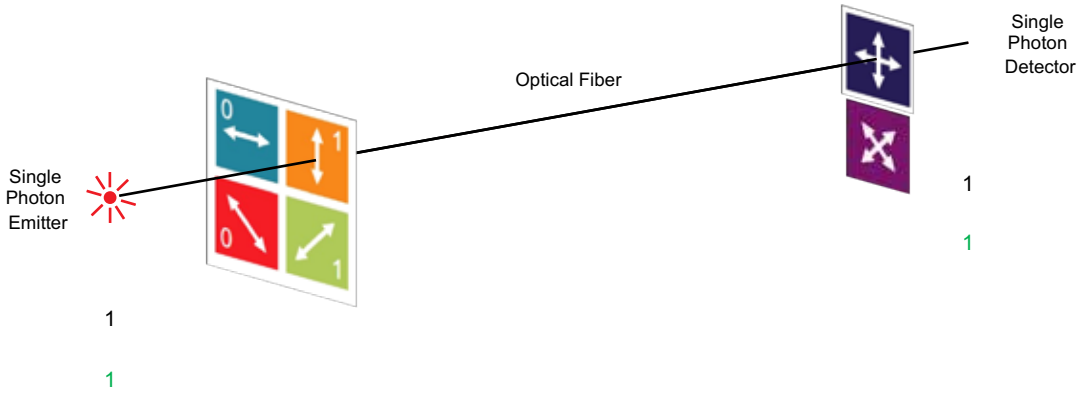
### QKD-Funktionsprinzip



## Schlüsselaustausch: Quantum Key Distribution (QKD)

dacoso data communication solutions

### QKD-Funktionsprinzip



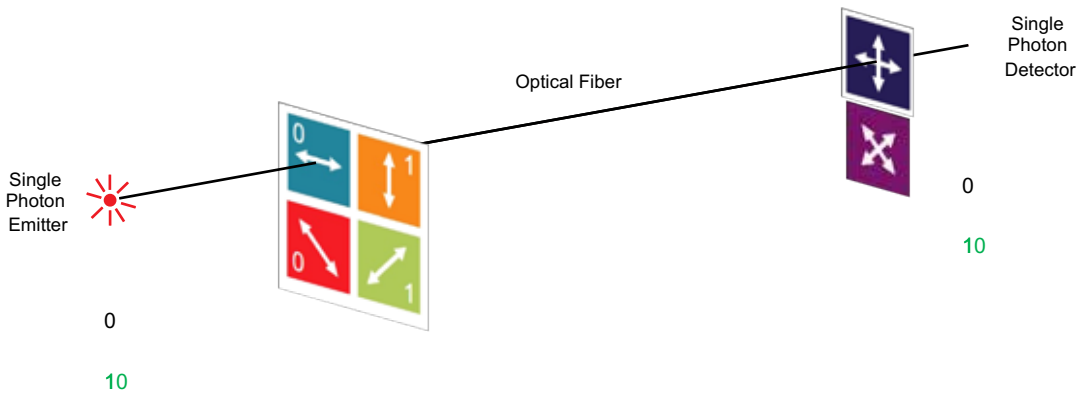





## Schlüsselaustausch: Quantum Key Distribution (QKD)

dacoso data communication solutions

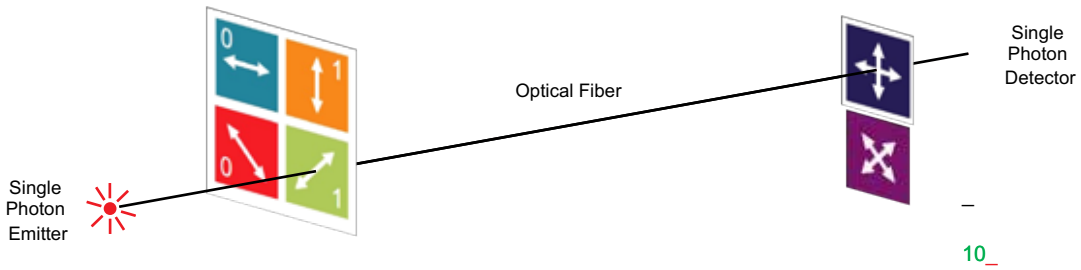
### QKD-Funktionsprinzip



## Schlüsselaustausch: Quantum Key Distribution (QKD)

dacoso data communication solutions

### QKD-Funktionsprinzip




1

101

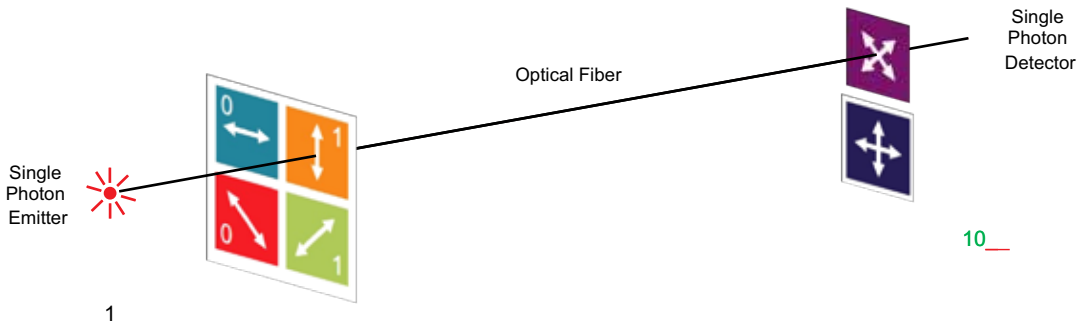




## Schlüsselaustausch: Quantum Key Distribution (QKD)

dacoso data communication solutions

### QKD-Funktionsprinzip



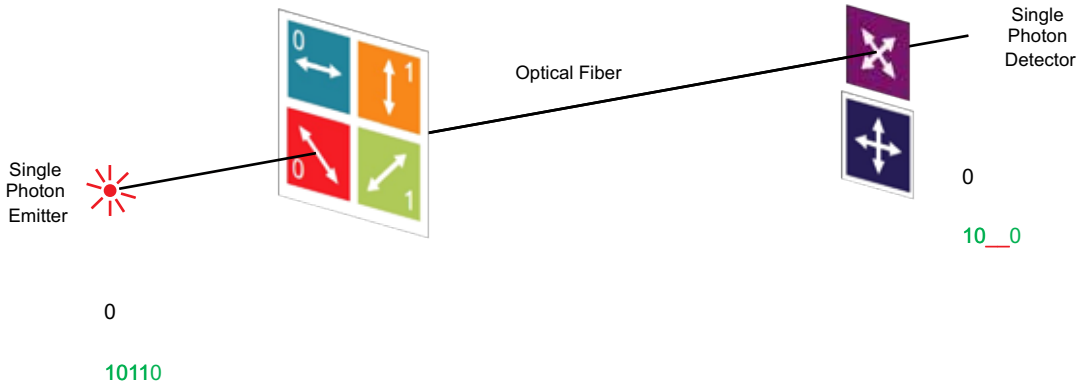

1

1011

## Schlüsselaustausch: Quantum Key Distribution (QKD)

dacoso data communication solutions

### QKD-Funktionsprinzip



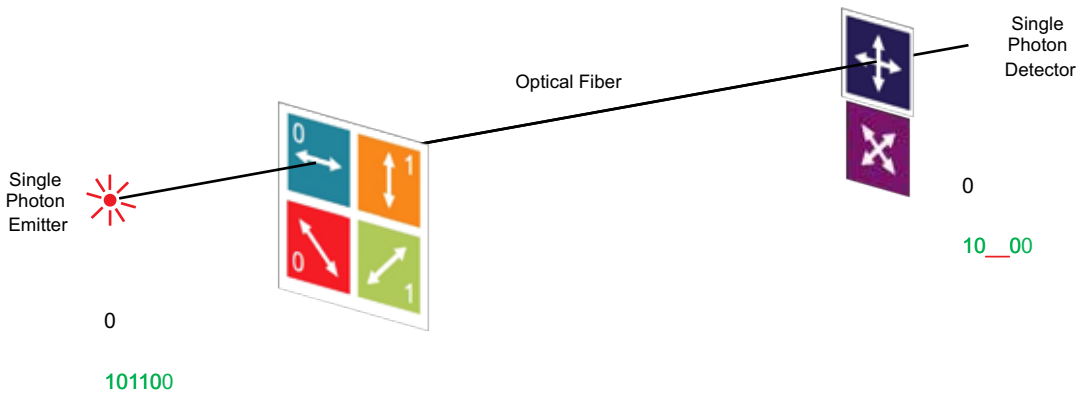





## Schlüsselaustausch: Quantum Key Distribution (QKD)

dacoso data communication solutions

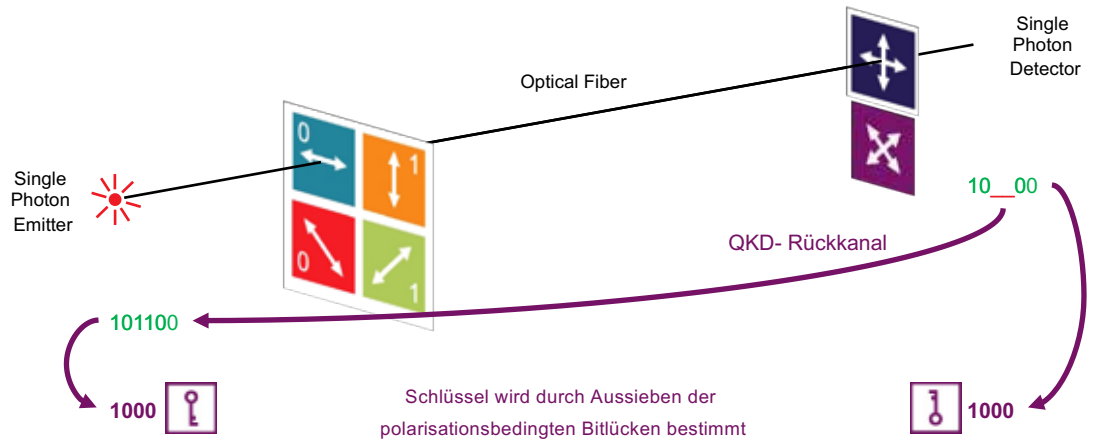
### QKD-Funktionsprinzip



## Schlüsselaustausch: Quantum Key Distribution (QKD)

dacoso data communication solutions

### QKD-Funktionsprinzip








## Schlüsselaustausch: Quantum Key Distribution (QKD)

dacoso data communication solutions

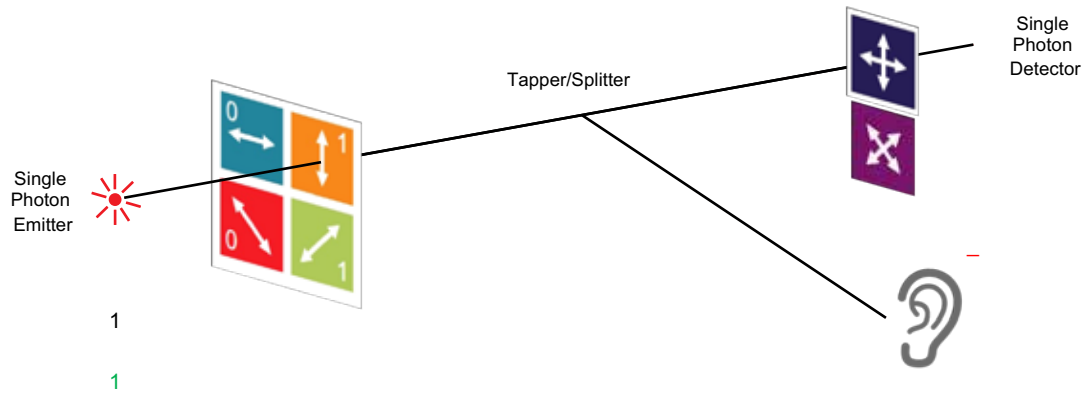
### QKD-Funktionsprinzip

- Hinter der Quantenkryptographie verbirgt sich kein Algorithmus. Vielmehr stellt die Quantenkryptographie eine technische Übertragungslösung zur Verfügung, um das Problem des sicheren Schlüsselaustausches zu beheben.
- Die Grundlage für den Quantenschlüsselaustausch ist die Polarisation von Photonen und die Gesetze der Quantenmechanik (Heisenberg'sche Unschärferelation).
- Die Übertragung des Schlüssels erfolgt über polarisierte Photonen, die auf Empfängerseite über ein Polarisationsfilter laufen, dessen Polarisationsebene jeweils zufällig ausgewählt wird („Siebmuster").
- Stimmt die jeweilige Polarisationsebene auf Sende- und Empfangsseite überein, dann ist das empfangene Quantenbit (Qbit) valid, also die Information Null oder Eins - andernfalls wird es verworfen.
- Die Validität basiert auf Übermittlung des „Siebmusters" zwischen Empfänger und Sender.
- Aus der Folge von Nullen und Einsen ermitteln beide Seiten den Schlüssel, der für die Chiffrierung und Dechiffrierung der geheimen Nachricht verwendet wird.

## Schlüsselaustausch: Quantum Key Distribution (QKD)

dacoso data communication solutions

### Quantum Key Distribution (QKD) – Angriff durch Abhören mittels Splitter



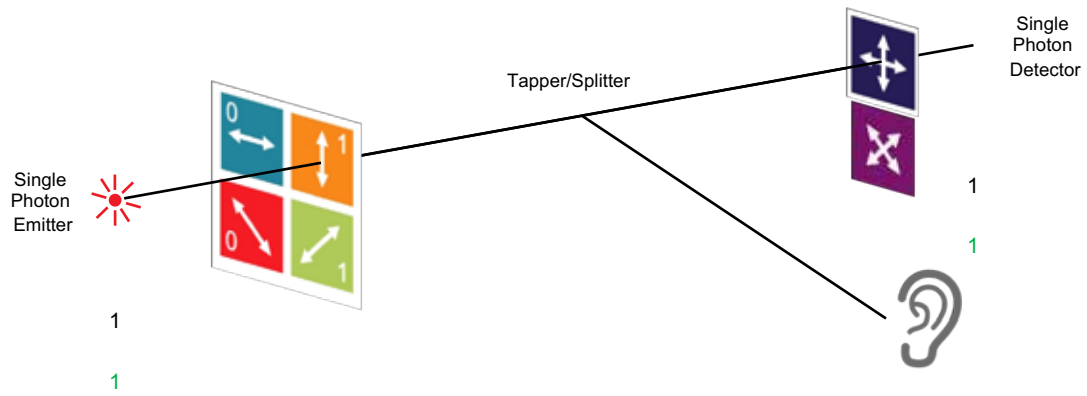

Durch Abhören gehen Photonen verloren – der Empfänger detektiert Angriffe.




## Schlüsselaustausch: Quantum Key Distribution (QKD)

dacoso data communication solutions

### Quantum Key Distribution (QKD) – Angriff durch Abhören mittels Splitter




Durch Abhören gehen Photonen verloren – der Empfänger detektiert Angriffe.

## Schlüsselaustausch: Quantum Key Distribution (QKD)

dacoso data communication solutions

### Quantum Key Distribution (QKD) - Angriff

- Was passiert, wenn ein Angreifer die Lichtquanten abfängt?
- In diesem Fall hinterlässt er eindeutige Spuren, denn nach den Gesetzen der Quantenmechanik kann ein System nicht beobachtet werden, ohne gestört zu werden.

**Klassische Mechanik**


**Quantenmechanik**

Einbruchserkennung

**„Physics"-Verfahren: Abhören von Quanteninformation zerstört den Schlüssel**





## Der Schlüsselaustausch für zukunftssicheren Schutz

dacoso data communication solutions

**Quantum Key Distribution (QKD)**

Verfahren basiert auf Quantenmechanik

PHYSIK

**Post Quantum Cryptography (PQC)**

Verfahren basiert auf verbesserten Einwegverfahren

MATHEMATIK

## Schlüsselaustausch: Post Quantum Cryptography (PQC)

dacoso data communication solutions

- aufwändige mathematische Einwegfunktionen, deren Rückrechnen selbst mit ausgeklügelten Algorithmen mittels Quantencomputer enorm viel Rechenzeit benötigt
- derzeit bekanntestes Verfahren: **McEliece,** das auf fehlerkorrigierenden Codes beruht (FEC)
- NIST Competition:
  - zweistufiges Auswahlverfahren zur Suche von Post-Quantum-Cryptography Algorithmen
  - erste Runde wurde in 2016 gestartet (19 code-based Verfahren shortgelistet)
  - zweite Runde wurde im Januar 2019 abgeschlossen: (7 Code-based Verfahren shortgelistet)
  - obwohl nicht geplant, ist es wahrscheinlich, dass NIST im Juni 2020 eine dritte Runde durchführen wird
  - es wird erwartet, dass die Arbeiten danach abgeschlossen und die Normenentwürfe zwischen 2022 und 2024 öffentlich zugänglich gemacht werden




## Gegenüberstellung der Verfahren

dacoso data communication solutions

| Quantum Key Distribution | Post-Quantum Cryptography |
|---|---|
| zusätzliche Geräte nötig | Software-Integration in existierenden Systemen |
| limitierte Reichweite | keine Reichweitenbeschränkungen |
| Funktion basiert auf Quanten-Eigenschaften | beruht auf der Stärke eines Berechnungsproblemes |
| langfristige Sicherheit gegen Angriffe | anfälliger für Fortschritte in der Rechenleistung |
| Sicherheitsgarantie durch Gesetze der Quantenphysik | Sicherheit nicht beweisbar |

**Maximale Sicherheit durch Kombination beider Technologien**

## Was ist wirklich zukunftssicher?

dacoso
data communication solutions

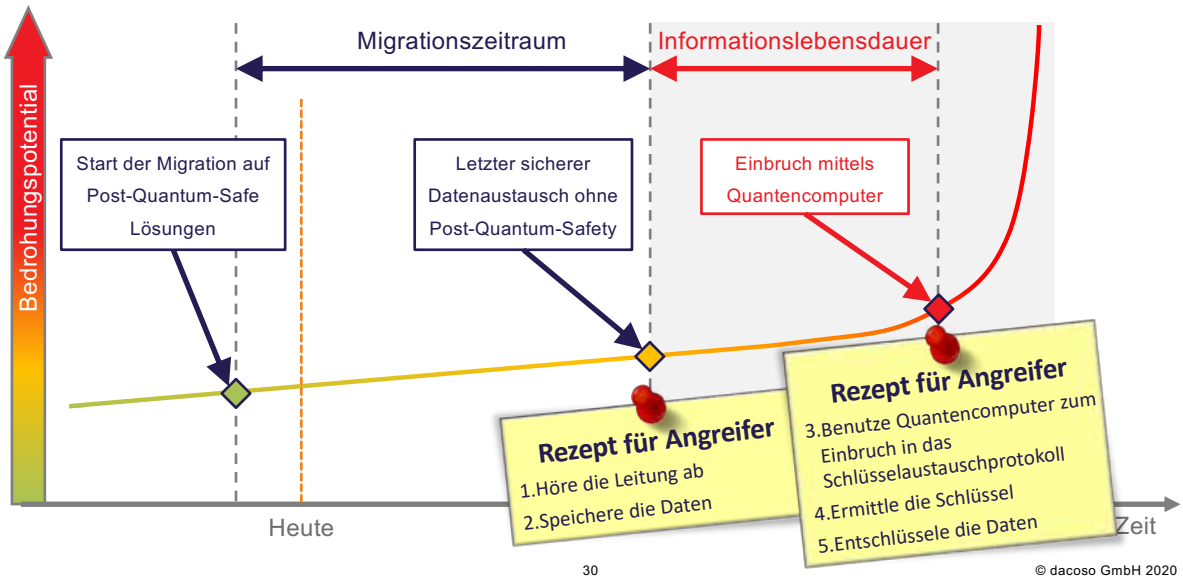
| | unsafe | postquantumsafe |
|---|---|---|
| Algorithmus | AES-128, AES-192, RSA, Diffie-Hellmann, Elliptic Curve Diffie-Hellmann | AES-256, Post-Quantum-Cryptography (PQC) |
| Informationstheorie | | One Time Pad (OTP) |
| Quantenmechanik | | Quantum-Key-Distribution (QKD) |





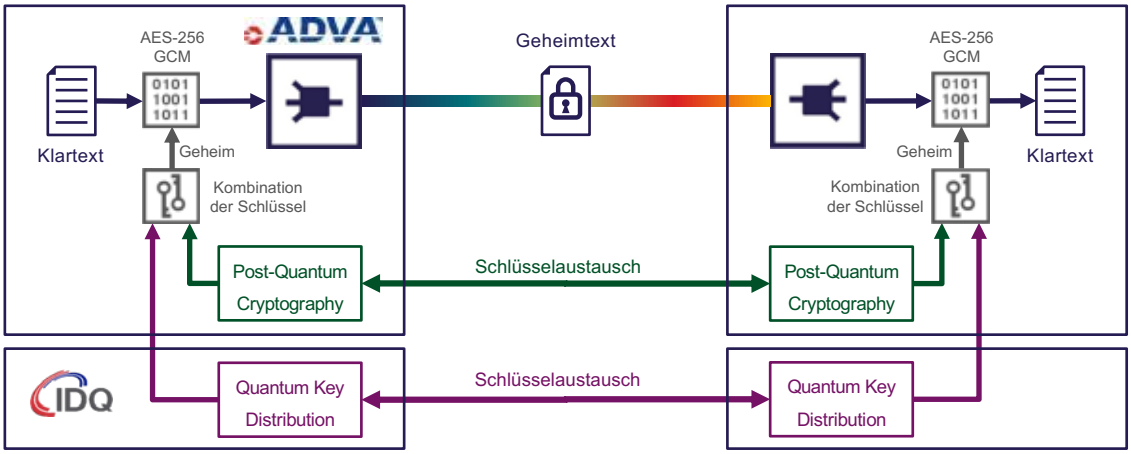
## Post-Quantum Safety: Handlungsspielraum

dacoso
data communication solutions



## Die Lösung für maximale Sicherheit

dacoso
data communication solutions







## Fazit

dacoso
data communication solutions

### Maximale Sicherheit

Kombination neuer, sicherer Schlüsselaustauschverfahren mit Quantenkryptografie

Zuverlässiger Schutz der Daten schon heute – noch vor Einsatz von Quantencomputern

Optimierte Lösung durch Kombination der Stärken von ADVA und ID Quantique

### dacoso: Alleskönner für Integration und Service

Wir übernehmen auch für die neuen Verfahren alle Schritte von der Planung und Installation bis hin zur Inbetriebnahme und dem dauerhaften Betrieb.

Mit unserem BSI-zertifizierten NOC/SOC erfüllen wir außerdem alle Anforderungen für eine „Managed Service“-Lösung.

**Es gibt neue beste Lösungen – und wir integrieren sie.**


Danke fürs Zuhören!