



Bundesamt  
für Sicherheit in der  
Informationstechnik

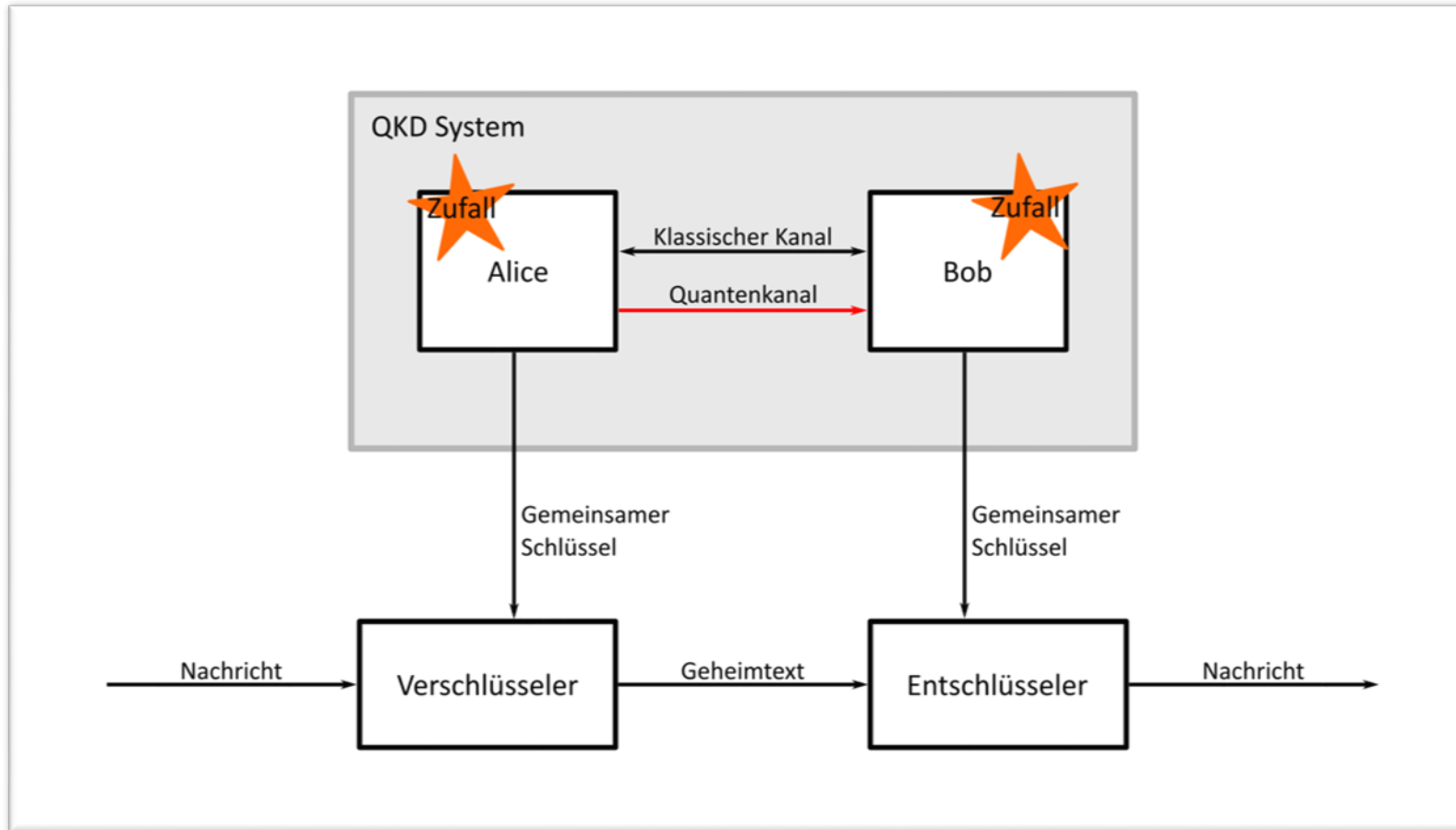
# Basiswissen: Quantensichere Kryptografie - Quantum Key Distribution

Stephanie Reinhardt, KM 21 „Vorgaben an und Entwicklung von Kryptoverfahren“, BSI

22.Juni 2022

Was ist Quantum Key Distribution?

# Quantum Key Distribution (QKD) = Quantenschlüsselaustausch



QKD-System Prepare-and-Measure

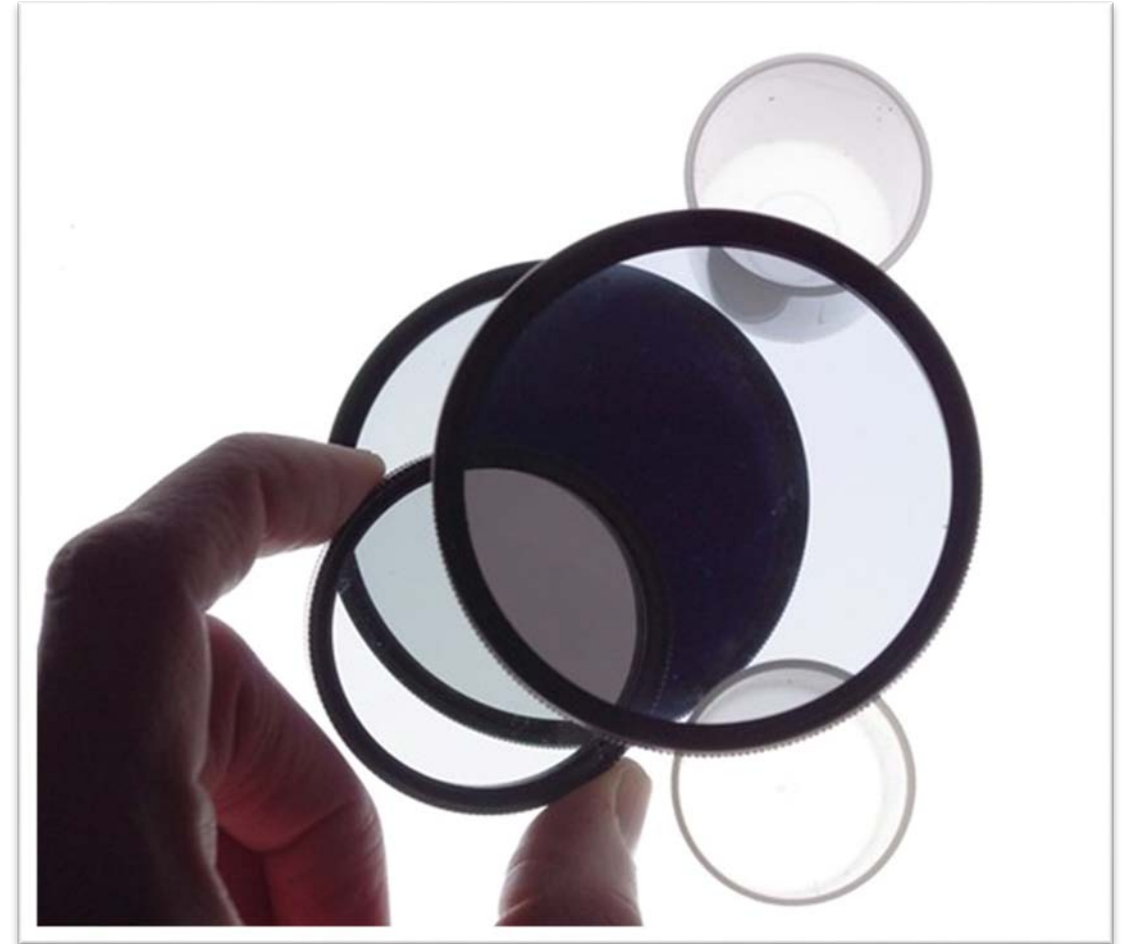
Benötigte Einzelteile:

- Photonenquelle
- Quantenkanal
- Messgerät
- Zufallszahlengeneratoren
- Authentisierter klassischer Kanal
- Schlüsselverwaltung

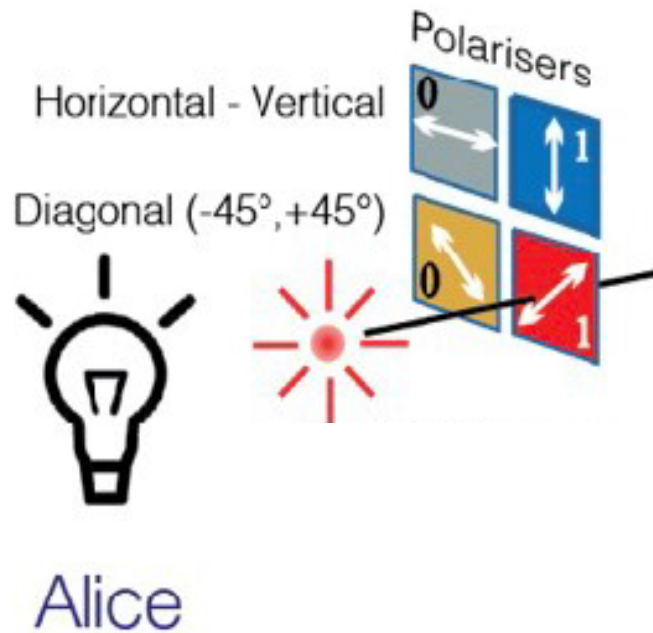
# Quantenmechanische Hintergründe

## Quantenzustand:

- Realisierung z.B. durch Polarisierung von Photonen
- Messungen verändern Quantenzustände
- Quantenzustände können nicht kopiert werden (No-Cloning-Theorem)

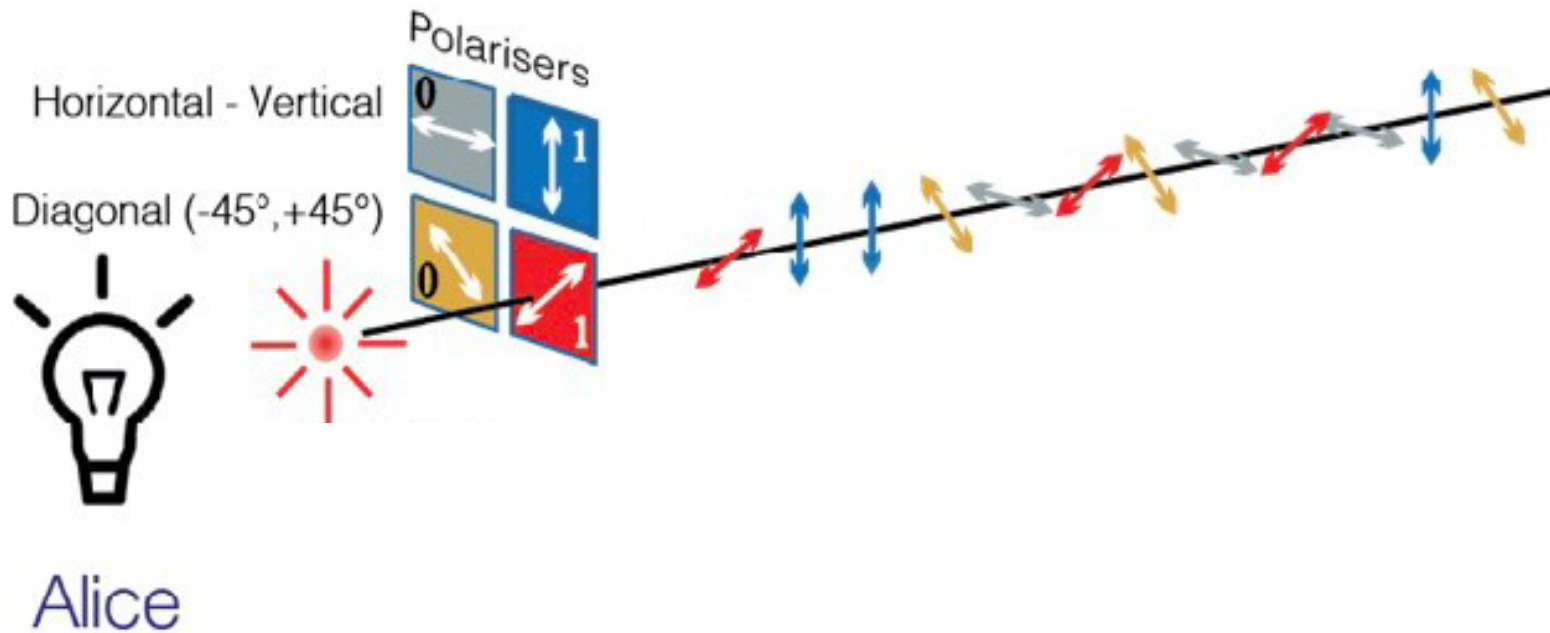


# Beispiel: Durchführung eines Prepare-and-Measure QKD-Protokolls

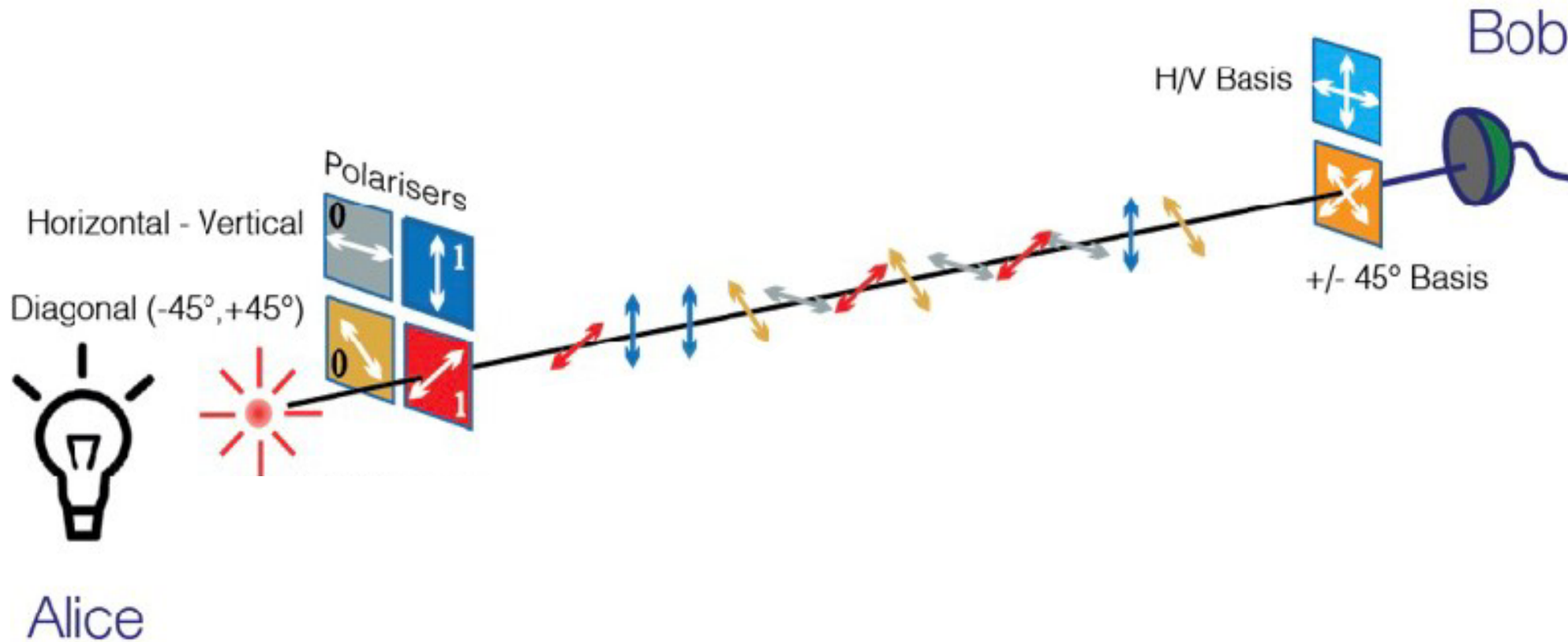


# Beispiel: Durchführung eines Prepare-and-Measure QKD-Protokolls

Bob

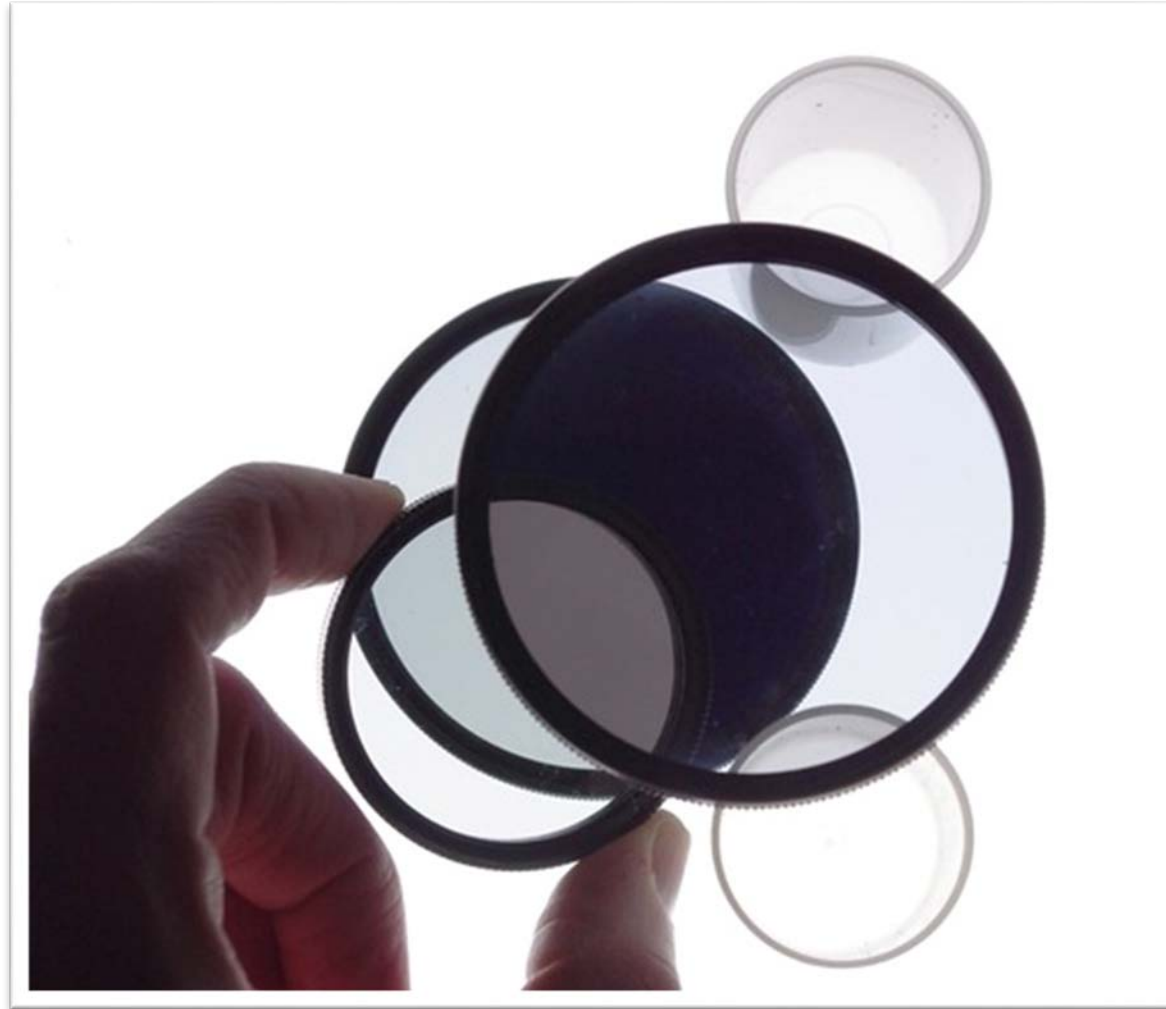


# Beispiel: Durchführung eines Prepare-and-Measure QKD-Protokolls



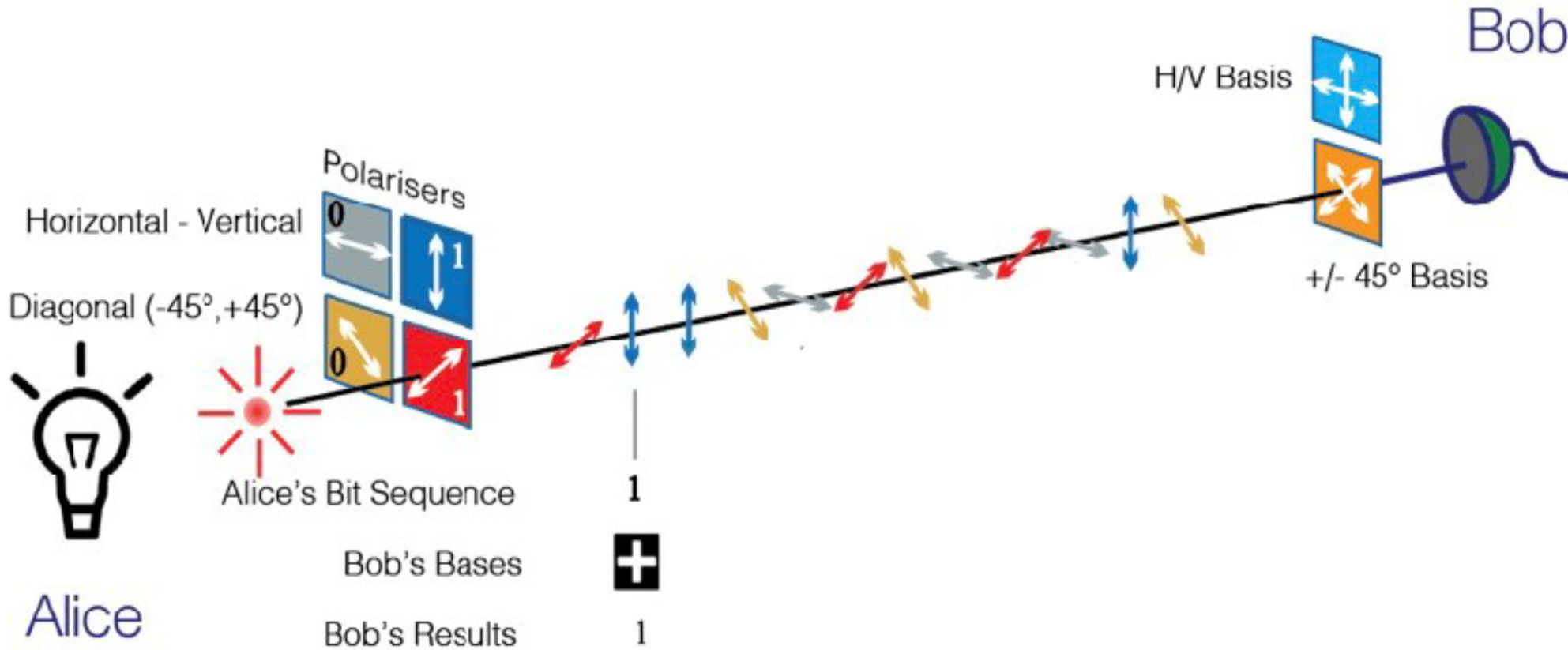
Quelle: Springer "Optical Wireless Communications"

# Beispiel: Durchführung eines Prepare-and-Measure QKD-Protokolls

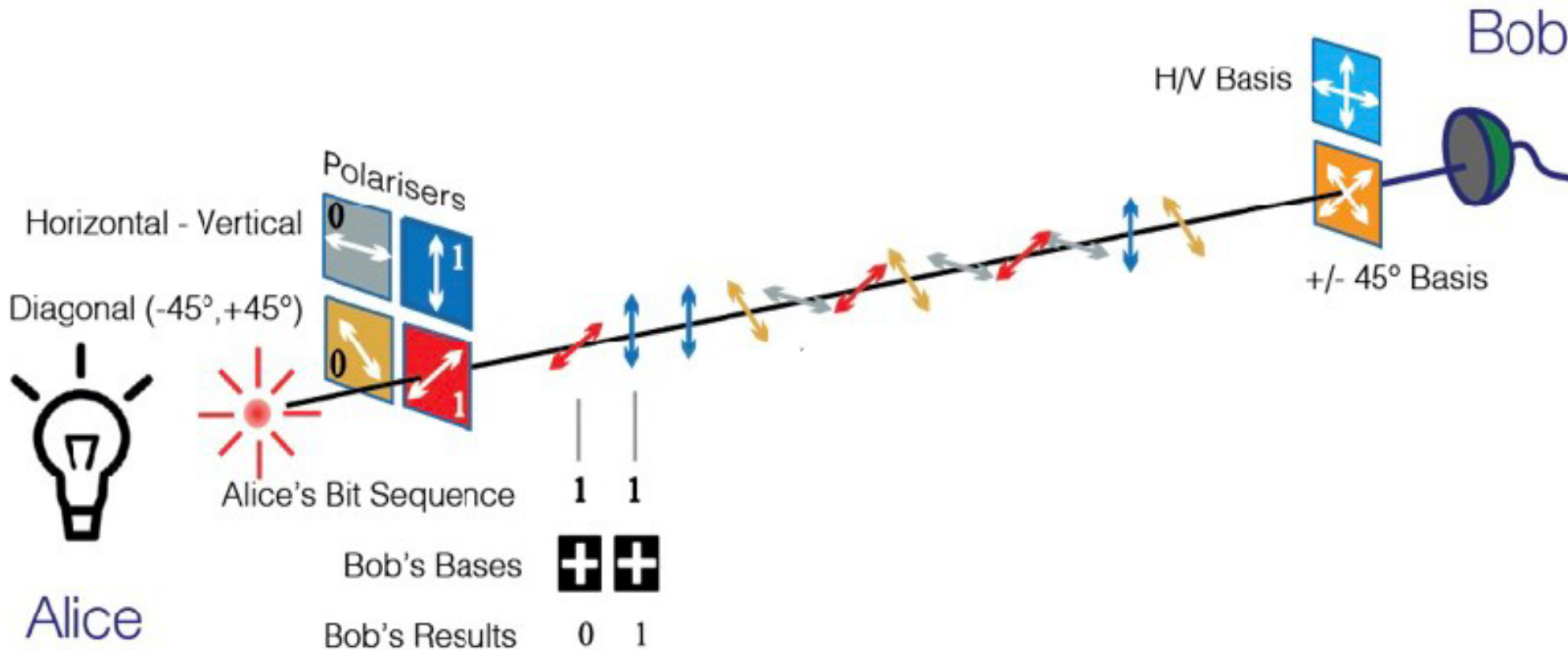




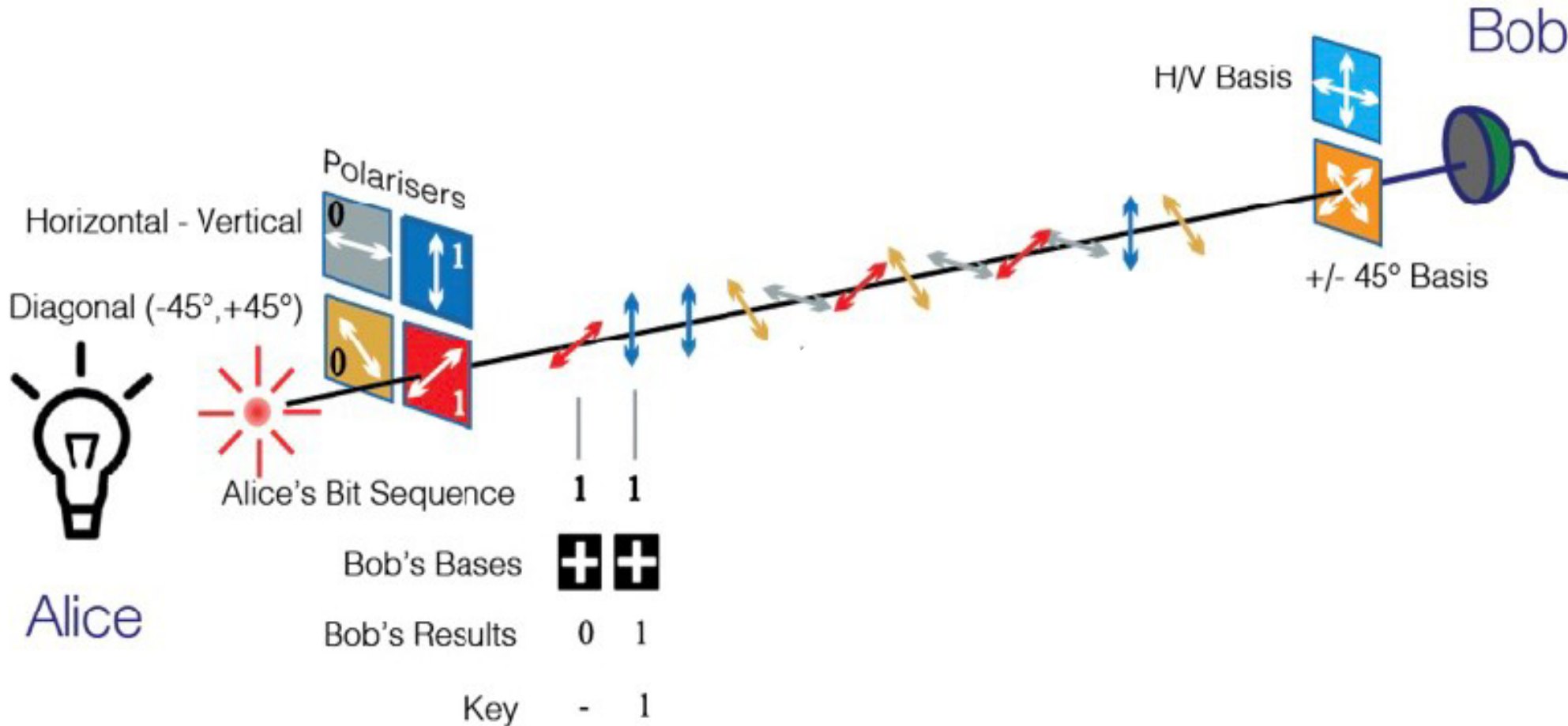
# Beispiel: Durchführung eines Prepare-and-Measure QKD-Protokolls



# Beispiel: Durchführung eines Prepare-and-Measure QKD-Protokolls

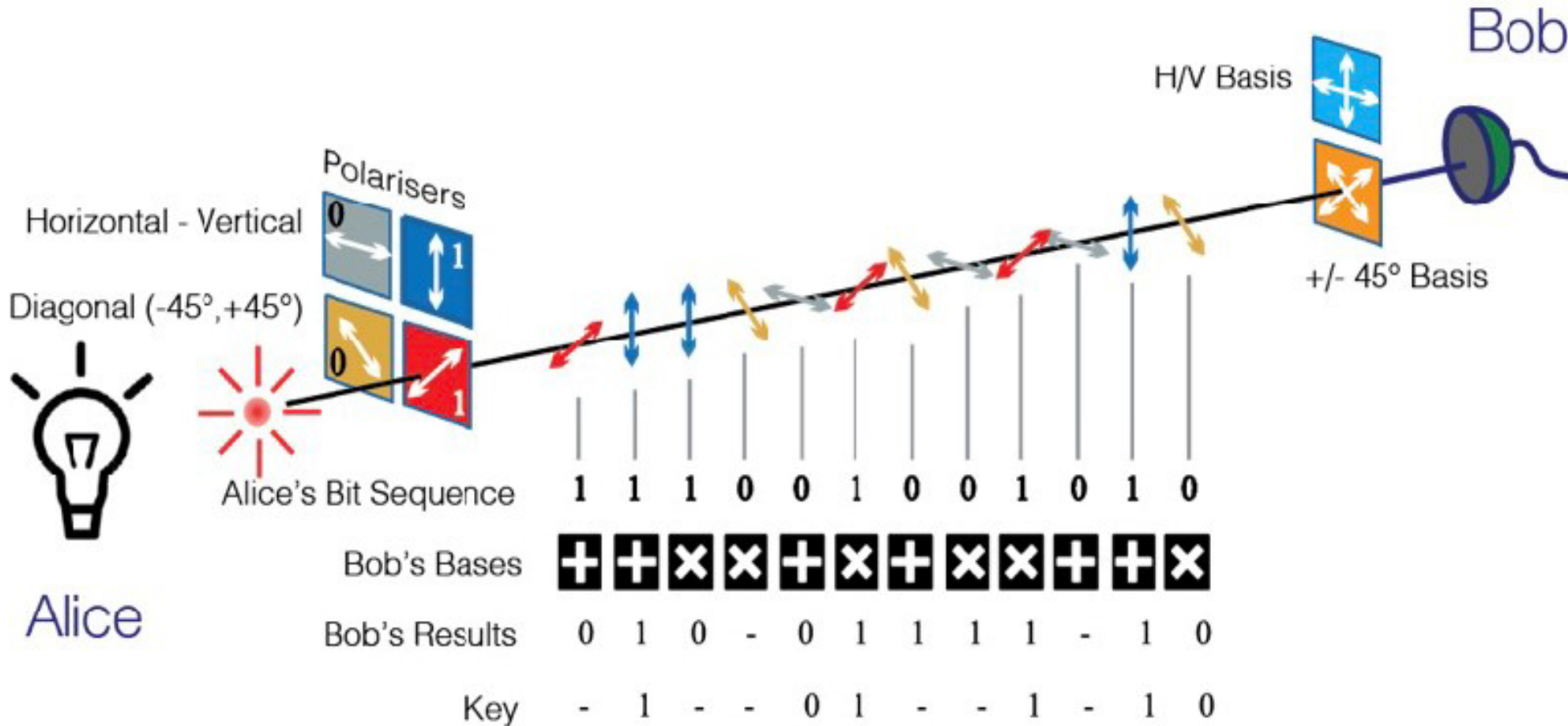


# Beispiel: Durchführung eines Prepare-and-Measure QKD-Protokolls



Quelle: Springer "Optical Wireless Communications"

# Beispiel: Durchführung eines Prepare-and-Measure QKD-Protokolls



Quelle: Springer "Optical Wireless Communications"

# Nachbearbeitung

## Lauschangriff

- Lauschen entspricht Messen der Quantenzustände
- Veränderung der Quantenzustände feststellbar
- Schlüssel verwerfen

## Nachbearbeitung mit klassischen Methoden

- Abschätzen der Fehlerrate
- Sicherstellen, dass Schlüssel beider Parteien identisch zueinander sind
- Verringern des Wissens eines Angreifers

# QuNET-Demo am 10.08.2021

Bonn | 10. August 2021

Initiative QuNET demonstriert hochsichere und praxisnahe Quantenkommunikation

## Erste quantengesicherte Videokonferenz zwischen zwei Bundesbehörden

In Bonn haben heute erstmals zwei deutsche Bundesbehörden quantengesichert per Video kommuniziert. Das Projekt QuNET, eine vom Bundesministerium für Bildung und Forschung (BMBF) geförderte Initiative zur Entwicklung hochsicherer Kommunikationssysteme, zeigt damit, wie Datensouveränität in Zukunft gewährleistet werden kann. Diese Technologie wird nicht nur für Regierungen und Behörden wichtig sein, sondern auch um Daten des täglichen Lebens zu schützen.

Es war ein Vorgeschmack auf die Kommunikation der Zukunft – oder besser: die »Datensicherheit« der Zukunft. Denn als Bundesforschungsministerin Anja Karliczek heute zu einer Videokonferenz mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) einlud, war zumindest augenscheinlich für den Außenstehenden alles beim Alten. Gemeinsam mit Andreas Könen, Abteilungsleiter CI »Cyber- und IT-Sicherheit« im Bundesministerium des Innern, für Bau und Heimat (BMI) und BSI-Vizepräsident Dr. Gerhard Schabhüser unterhielt sich die Ministerin via Videostream.



Anja Karliczek (BMBF) und Martin Schell (Fraunhofer HHI) bei der Pressekonferenz und Demonstration der ersten quantengesicherten Videokonferenz zwischen deutschen Bundesbehörden. (© BMBF)

# Sicherheit von QKD

# Sicherheitseigenschaften: Theoretische Sicherheit

- Authentisierung des klassischen Kanals notwendig
- Sicherheitsversprechen von QKD:  
**QKD bietet informationstheoretische Sicherheit!**  
Problem: bleibt nur erhalten, wenn der Schlüssel mittels One-Time-Pad weiterverwendet wird
- Sicherheitskriterien und Sicherheitsbeweise weiterhin Forschungsthemen
- Sicherheit durch physikalische Methoden, nicht durch Schwierigkeit mathematischer Probleme

**Security in Quantum Cryptography**

Christopher Portmann\*  
*Department of Computer Science,  
ETH Zurich, 8002 Zurich,  
Switzerland*

Renato Renner†  
*Institute for Theoretical Physics,  
ETH Zurich, 8003 Zurich,  
Switzerland*

(Dated: February 2, 2021)

Quantum cryptography exploits principles of quantum physics for the secure processing of information. A prominent example is secure communication, i.e., the task of transmitting confidential messages from one location to another. The cryptographic requirement here is that the transmitted messages remain inaccessible to anyone other than the designated recipients, even if the communication channel is untrusted. In classical cryptography, this can usually only be guaranteed under computational hardness assumptions, e.g., that factoring large integers is infeasible. In contrast, the security of quantum cryptography relies entirely on the laws of quantum mechanics. Here we review this physical notion of security, focusing on quantum key distribution and secure communication.

arXiv:2102.00021v1 [quant-ph] 29 Jan 2021

<b>CONTENTS</b>	
I. Security from physical principles	2
A. Completeness of quantum mechanics	2
B. Correctness of quantum theory	3
II. Cryptographic security definitions	4
A. Real-world ideal-world paradigms	4
B. Abstract Cryptography	5
C. Example: the One-Time Pad	7
D. Abstract theory of cryptographic systems	8
E. Security definition	9
F. Interpretation of the security parameter	10
G. Instantiating systems	11
III. Defining Security of QKD	12
A. The real and ideal QKD systems	12
1. Ideal key	12
2. Real QKD system	13
3. Security	14
B. Reduction to the trace distance criterion	14
1. Trace distance	14
2. Simulator	16
3. Correctness & secrecy	16
4. Robustness	17
C. Other security criteria	17
1. Accessible information	17
2. Adversarial models	18
3. Expressing weaker security criteria within the AC framework	19
4. Variations of the trace distance criterion	19
IV. Assumptions for security	20
A. Standard assumptions for QKD	20
B. Necessity and justification of assumptions	21
C. Quantum hacking attacks	21
D. Countermeasures against quantum hacking	22
V. Security proofs for QKD	23
A. Protocol replacement	23
B. Raw Key Distribution and Parameter Estimation	24
C. Information Reconciliation	26
D. Privacy Amplification	27
E. Other approaches to prove security	28
VI. Alternative modeling of QKD	28
A. Adaptive key length	28
B. Source of entanglement	29
C. Imperfect randomness	30
D. Device-Independent QKD	30
E. Semi-device independent QKD	32
F. Memoryless adversaries	33
VII. Secure classical message transmission	33
A. Authentication	34
B. Quantum key distribution	35
C. One-Time Pad	36
D. Combining the subprotocols	36
VIII. Other cryptographic tasks	37
A. Secure quantum message transmission	37
1. Generic protocol	37
2. Concrete schemes	38
B. Key reuse in classical and quantum message transmission	39
C. Delegated quantum computation	40
D. Multi-party computation	41
1. Two-party computation and oblivious transfer	41
2. One-time Programs	41
3. Everlasting security	41
4. Impossibility results	42
E. Relativistic cryptography	42
F. Secure quantum message transmission with computational security	43
1. Defining composable and finite computational security	43

\* Electronic address: [chportma@ethz.ch](mailto:chportma@ethz.ch)  
† Electronic address: [renner@ethz.ch](mailto:renner@ethz.ch)



# Sicherheitseigenschaften: Praktische Sicherheit

Viele Seitenkanalgriffe werden untersucht

## Beispiel **Photon Number Splitting Attack**

- Annahme: mehr als ein Photon wird im selben Zustand gesendet
- Abfangen und Speichern der zusätzlichen Photonen
- Messen, nachdem die korrekten Basen verkündet werden



„Quantenhacker“ Vadim Makarov beim Lauschangriff

# Praktische Fragen zum Einsatz von QKD

# Einsatz von QKD: Umgang mit Reichweiteneinschränkungen

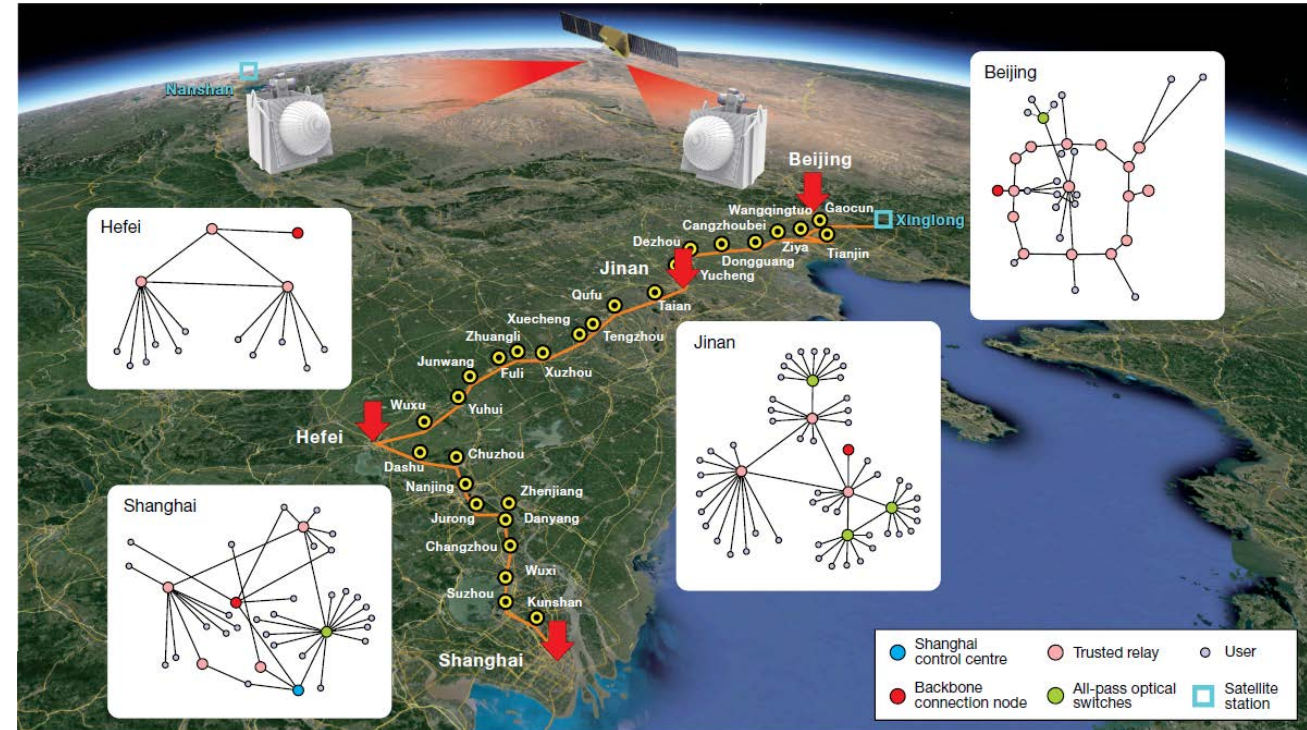
## Option 1: „Trusted Nodes“

- Ende-zu-Ende-Sicherheit über lange Distanzen nicht erreichbar

## Option 2: Satellitenbasierte QKD

## Option 3: Quantenrepeater

- Marktreife in den nächsten Jahren nicht zu erwarten



QKD-Netzwerk Chinas

# Einsatz von QKD: Verwendung der vereinbarten Schlüssel

- Verwendung zur Verschlüsselung z. B. mit AES
- Häufig diskutiert: Verschlüsselung mit One-Time-Pad
  - Schlüsselrate von QKD dafür zu niedrig
  - Alleinige Nutzung des OTP wird nicht empfohlen



Thomas Scheibitz: *One-Time Pad* (2012), Kunstmuseum Bonn

# Einschränkungen von QKD

## **Technologische Einschränkungen:**

- Vorverteilte Schlüssel für Authentisierung benötigt
- Reichweite fasergebundener QKD zurzeit etwa 100km
- Satelliten: Frage der Verfügbarkeit
- Passende Nutzung der verteilten Schlüssel

## **Politische und praktische Einschränkungen:**

- Spezialisierte kostenintensive Hardware benötigt
- Sicherheitsbeweise und Seitenkanäle müssen weiter erforscht werden
- Zulassung und Zertifizierung von Produkten notwendig

# Quantensichere Kryptografie: Fazit

# Fazit zur quantensicheren Kryptografie

- Quantentechnologien bedrohen die heute verwendete asymmetrische Kryptografie  
→ Umstellung auf quantensichere Alternativen kommt
- QKD kann Post-Quanten-Kryptografie ergänzen
- Fokus auf Post-Quanten-Kryptografie
- Neue Methoden nur hybrid nutzen
- Kryptoagilität einplanen



# Vielen Dank für Ihre Aufmerksamkeit!

## Kontakt

Stephanie Reinhardt

Bundesamt für Sicherheit in der Informationstechnik  
Referat KM 21 – Vorgaben an und Entwicklung von Kryptoverfahren

Godesberger Allee 185-189  
51375 Bonn

E-Mail: [stephanie.reinhardt@bsi.bund.de](mailto:stephanie.reinhardt@bsi.bund.de)

