Bundesamt
für Sicherheit in der
Informationstechnik

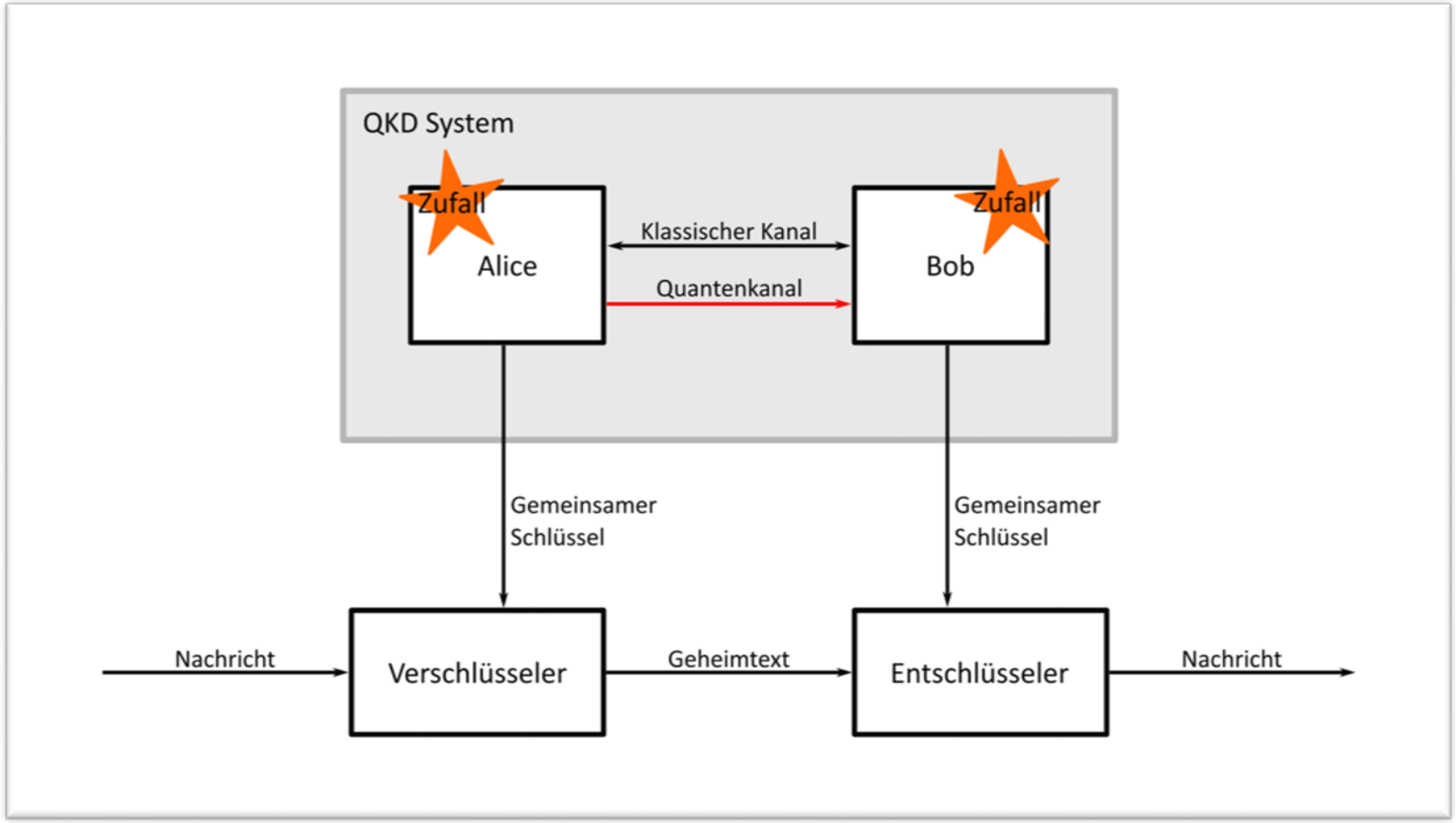
Basiswissen: Quantensichere Kryptografie - Quantum Key Distribution

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

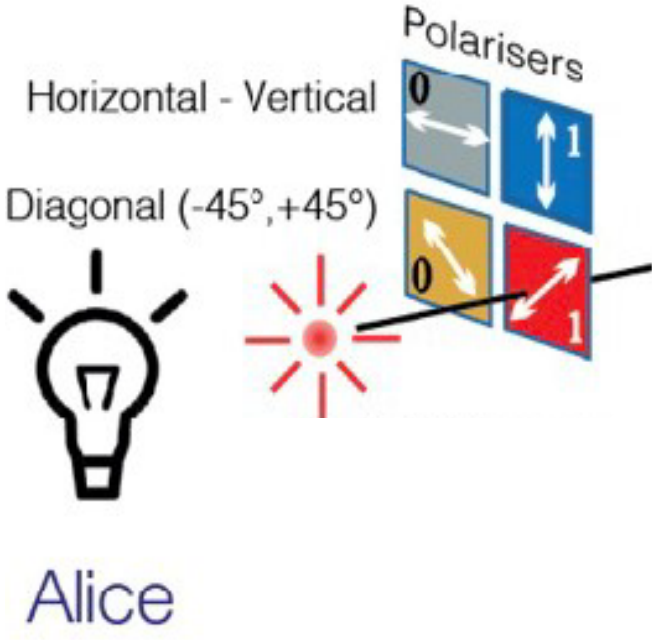
Bundesamt für Sicherheit in der Informationstechnik

Quantenmechanische Hintergründe

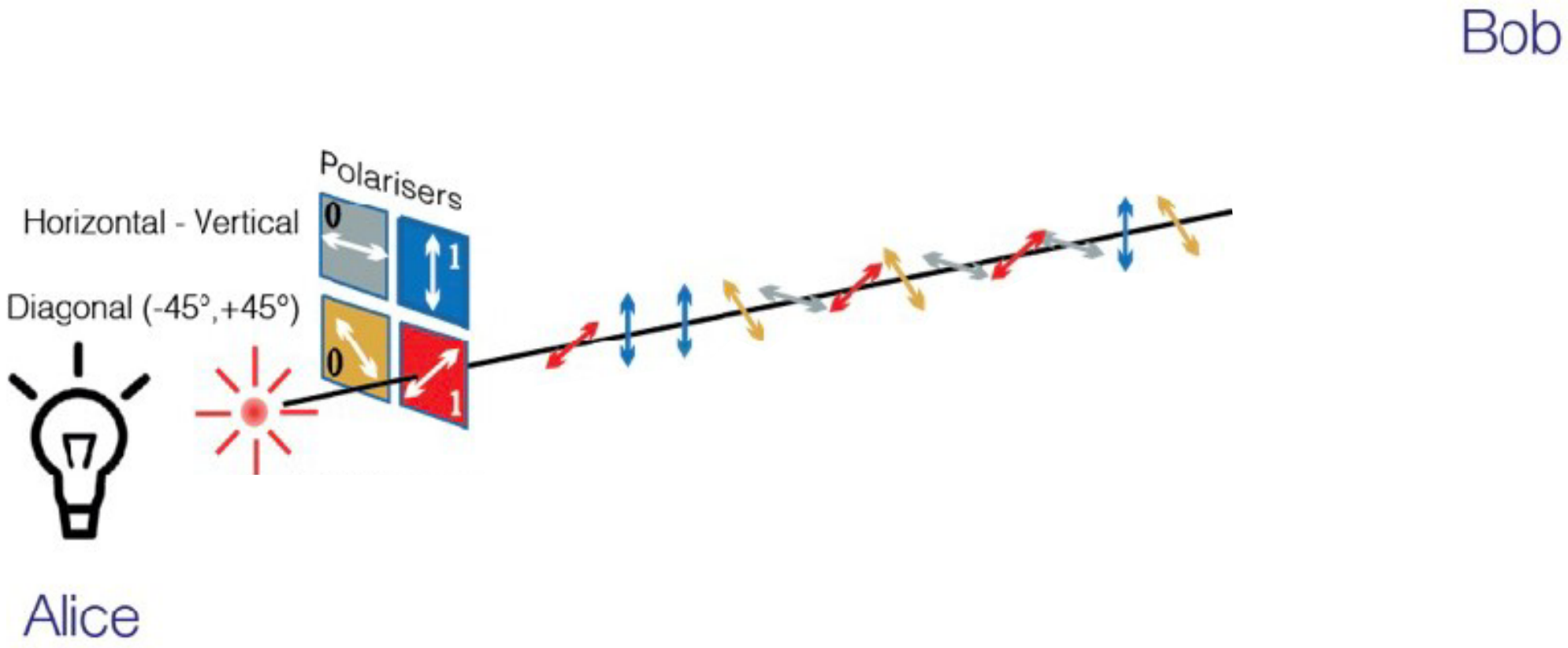
Quantenzustand:

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

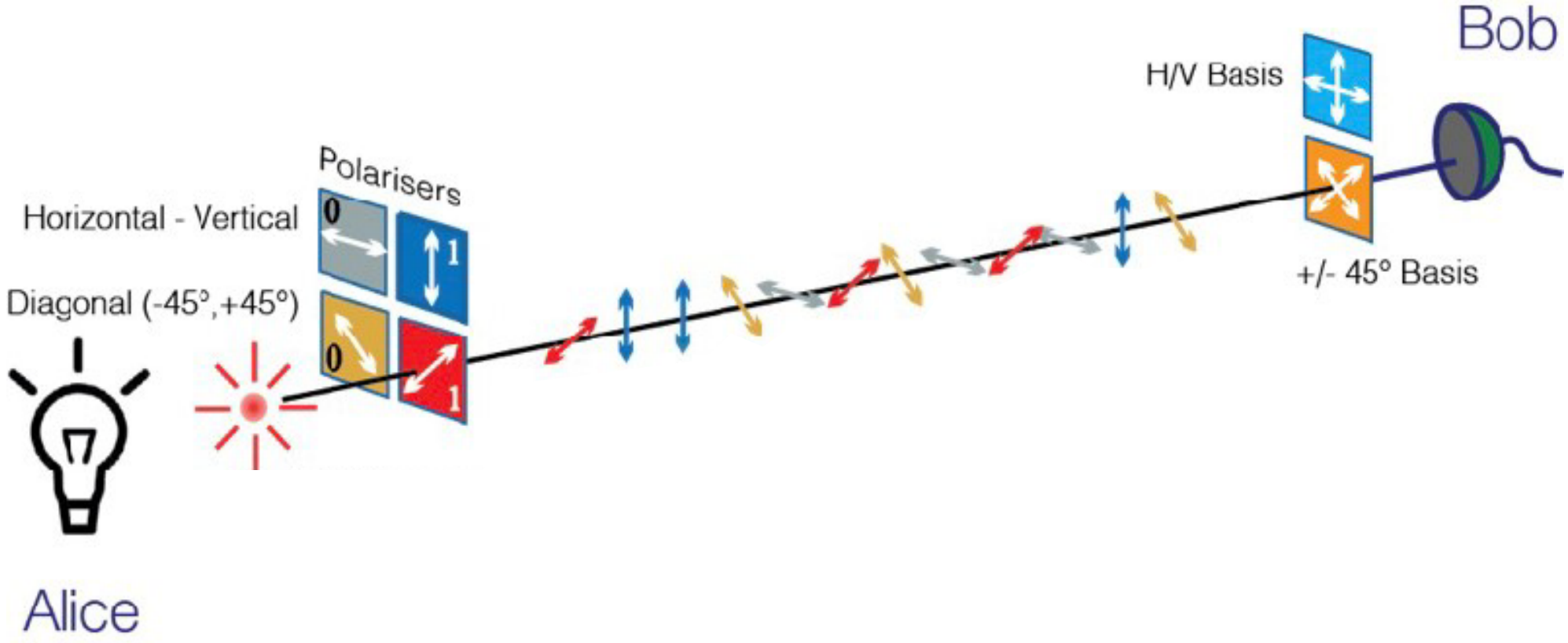
Beispiel: Durchführung eines Prepare-and-Measure QKD-Protokolls



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

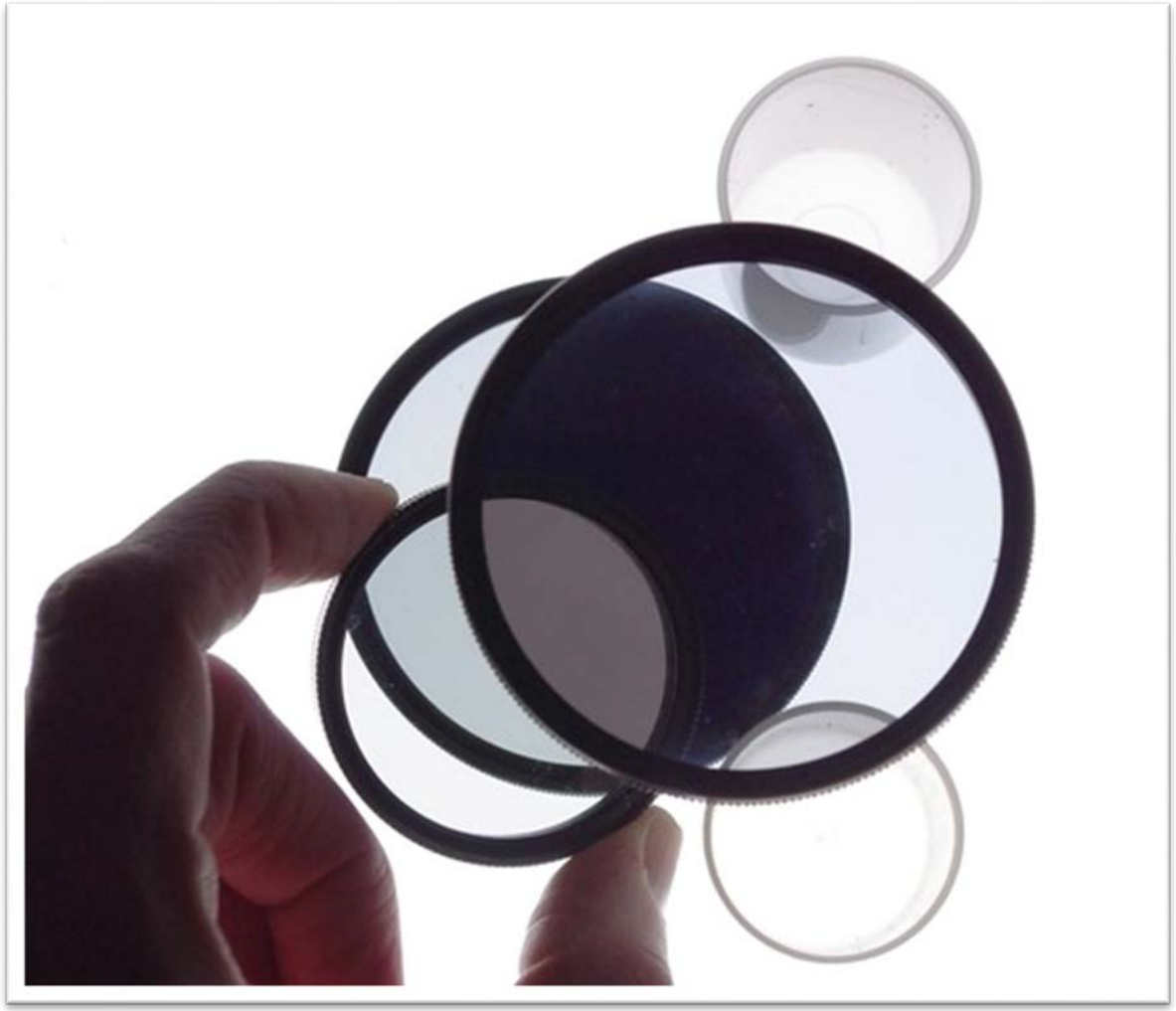


Beispiel: Durchführung eines Prepare-and-Measure QKD-Protokolls

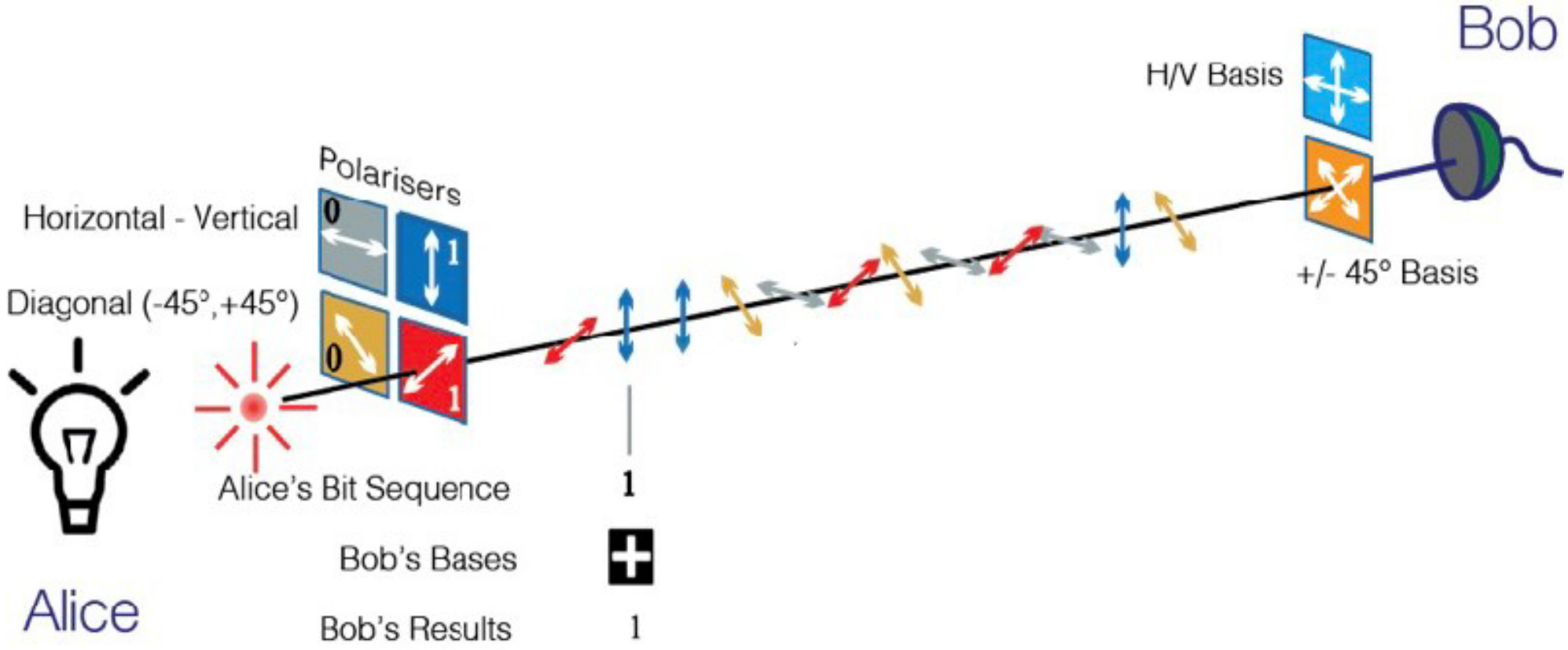


Quelle: Springer "Optical Wireless Communications"

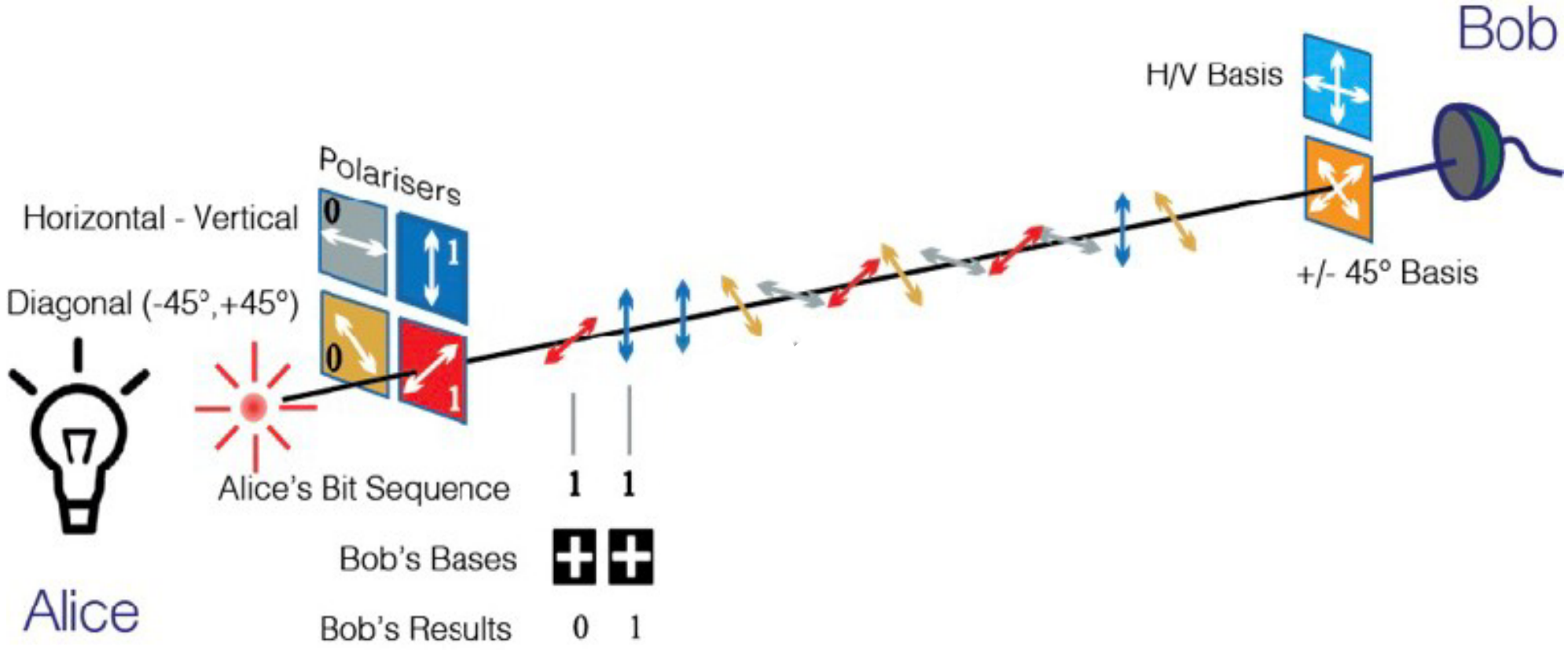
Beispiel: Durchführung eines Prepare-and-Measure QKD-Protokolls



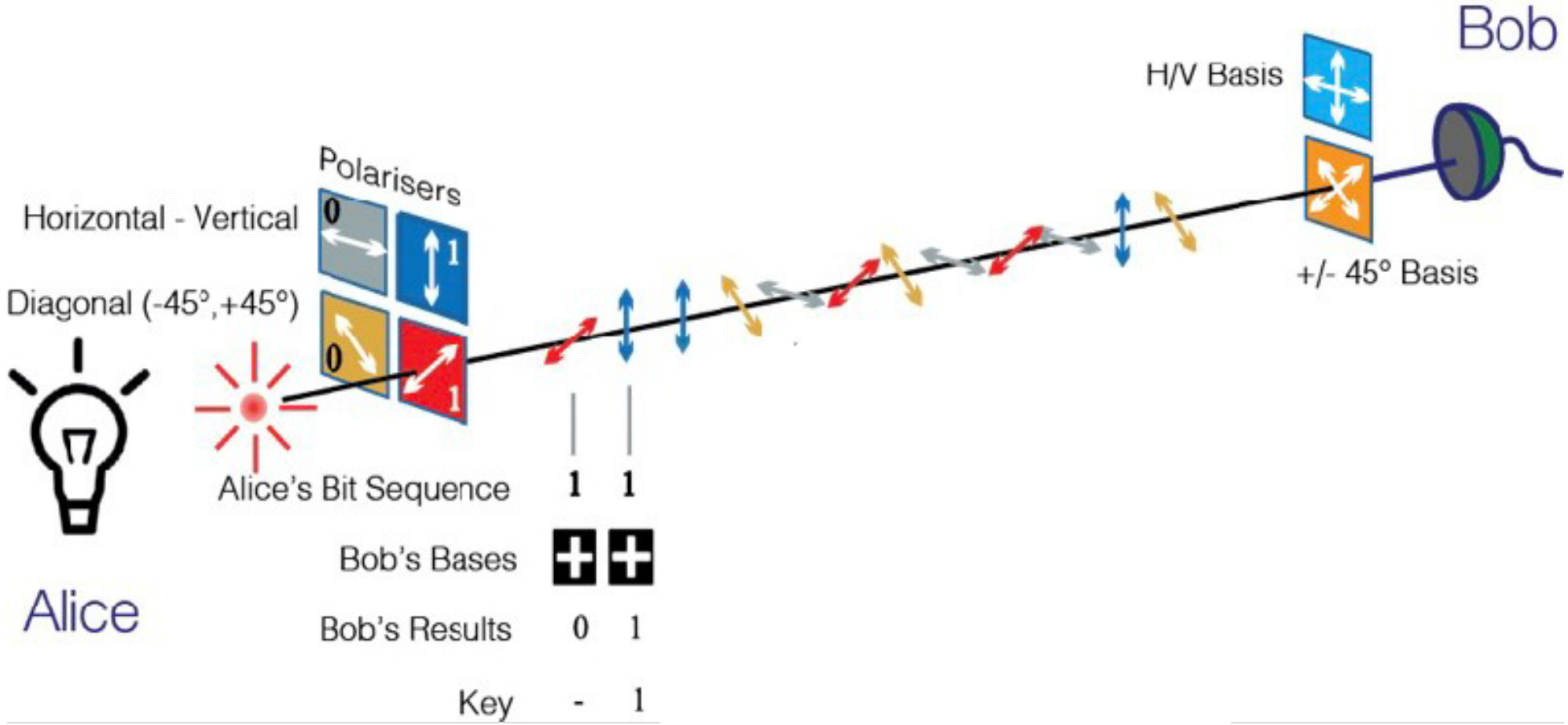
Beispiel: Durchführung eines Prepare-and-Measure QKD-Protokolls



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

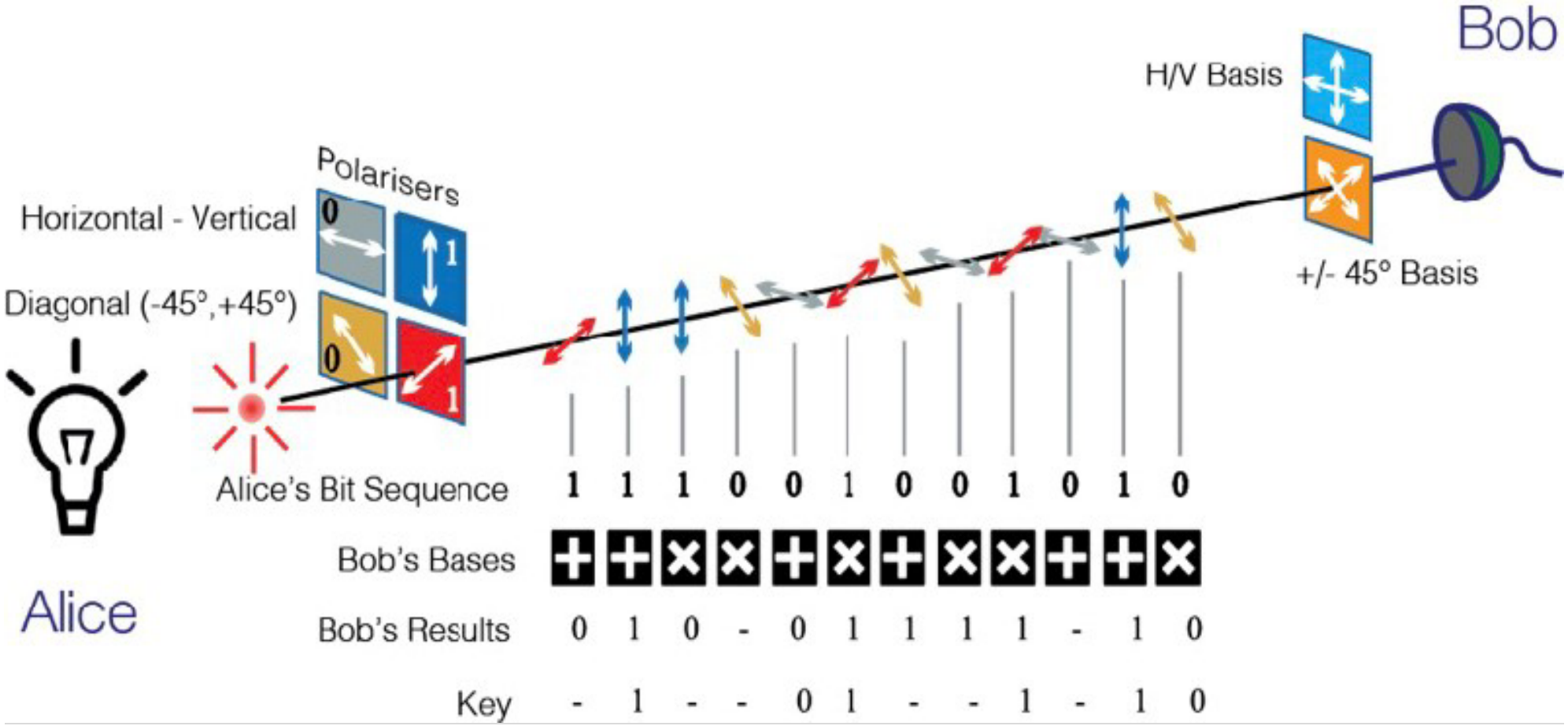


Beispiel: Durchführung eines Prepare-and-Measure QKD-Protokolls



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)

Bundesamt für Sicherheit in der Informationstechnik

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, 8092 Zurich,
Switzerland

Renato Renner†
Institute for Theoretical Physics,
ETH Zurich, 8093 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.

CONTENTS

* Electronic address: cbportma@ethz.ch
† Electronic address: renner@ethz.ch

Bundesamt für Sicherheit in der Informationstechnik

Sicherheitseigenschaften: Praktische Sicherheit

„Quantenhacker“ Vadim Makarov beim Lauschangriff

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

Praktische Fragen zum Einsatz von QKD

Einsatz von QKD:
Umgang mit Reichweiteneinschränkungen

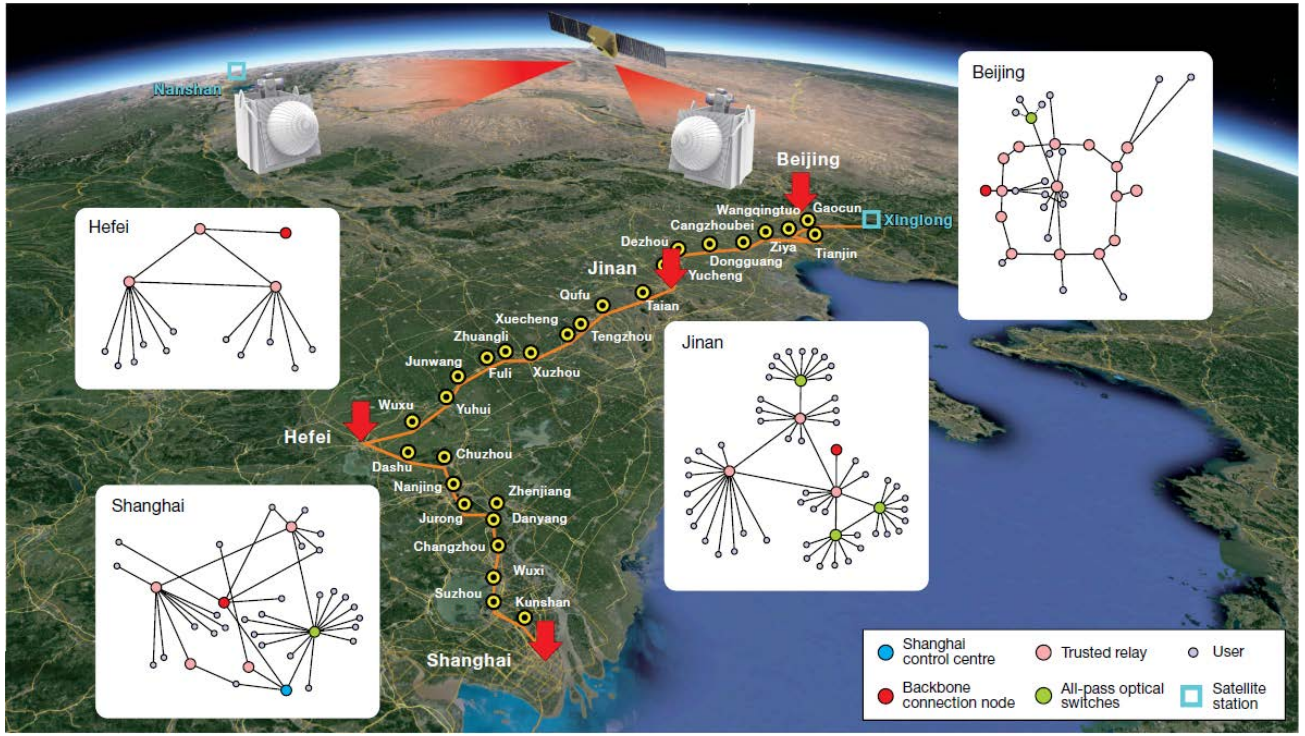
Option 1: „Trusted Nodes“

- 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 Kryptographie
  → 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

Bundesamt
für Sicherheit in der
Informationstechnik