Quantenkryptographie (Teil 2)
- Sicherheitsbetrachtungen

Prof. Dr. Jörg Hettel
Hochschule Kaiserslautern
Fachbereich Informatik

Agenda

1. Einführung
2. Wiederholung BB84
3. Qubits und Messbasen
4. Zusammengesetzte Systeme
5. Verschränkung
6. Anwendung von Verschränkung
7. Shared Randomness
8. Schmidt-Darstellung
9. Dichtematrizen
10. Partielle Spur
11. Verschränkungsmaß
12. Entropie und Monogamie
13. Entanglement Swapping
14. Entanglement Distillation
15. CHSH-Ungleichung (klassisch)
16. CHSH-Ungleichung (Quantenversion)
17. CHSH-Ungleichung (Simulation)
18. Ekert-Protokoll
19. **Sicherheit und DIQKD**
20. Zusammenfassung

Sicherheit "klassischer Kryptographie"

- Klassische Verfahren
  - Symmetrische Verfahren
    - One Time Pad ⇒ perfekt sicher
    - AES, 3DES ⇒ "nicht perfekt" sicher, kein Sicherheitsbeweis
  - Public Key / Asymmetrische Verfahren
    - RSA, Diffie-Helman => Sicherheit beruht auf nicht bewiesenen Annahmen.
    - Sicherheit beruht auf der Intuition: "schwer zu lösen".
    - Durch Quantencomputer angreifbar.

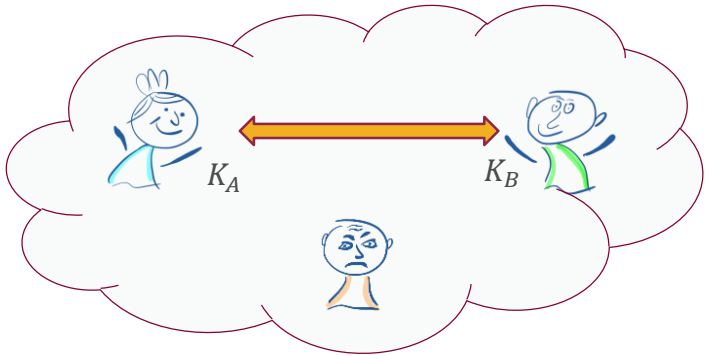
Sicherheit in der QKD

- Quantenverfahren: Schlüsseltausch
  - BB84 – Prepare and Measurement
    - Nicht-Unterscheidbarkeit von nicht-orthogonalen Zuständen.
    - Entdeckung eines Lauschers möglich.
    - Benutzte Komponenten sind angreifbar.
  - Ekert 91 – Verschränkungsbasiert
    - Beruht auf Verschränkung.
    - Sicherheitsbeweis ist möglich.
    - Kann auf ein modifiziertes BB84-Protokoll (mit Austausch verschränkter Qubits) angewendet werden.

Mathematische Definitionen

- Da die Quantenphysik eine probabilistische Theorie ist, kann die Sicherheit auch nur über Wahrscheinlichkeiten definiert werden.
  - Angabe der Sicherheit erfolgt mit Schranken.

- Die (Epsilon-) Sicherheit eines Protokolls besteht aus:
  - Epsilon-Korrektheit
  - Epsilon-Geheim



Mathematische Definitionen

- Epsilon-Korrekt
  - Hier wird gefordert, dass die Wahrscheinlichkeit für eine Nicht-Übereinstimmung der Schlüssel von Alice und Bob beliebig klein gemacht werden kann

$$Prob(K_A \neq K_B) \leq \varepsilon$$

- Epsilon-Geheim
  - Hier wird gefordert, dass die Kenntnis von Eve über den ausgetauschten Schlüssel beliebig klein gemacht werden kann.
  - Man fordert, dass Eve "genügend entkoppelt" ist und der erzeugte Schlüssel gleichverteilt und unkorreliert ist, also im Prinzip (mathematisch inexakt):

$$\left| \rho_{K_A K_B E} - \frac{1}{n} \mathbb{I}_{AB} \otimes \rho_E \right| \leq \varepsilon$$

Voraussetzungen

- Getroffene Annahmen:
  - Die Theorie der Quantenphysik ist korrekt.
    - Die Vorhersage von Qubit-Verhalten und Messergebnissen stimmen mit der Wirklichkeit überein.
  - Quantenphysik ist umfassend.
    - Es können alle möglichen Phänomene erklärt werden, Eves Informationsgewinn kann nur über die "Quantenphysik" erfolgen.
  - Authentifizierende Kommunikation ist möglich.
    - Alice und Bob können sicher sein, dass sie wirklich miteinander kommunizieren.

Annahmen über die Implementierungen

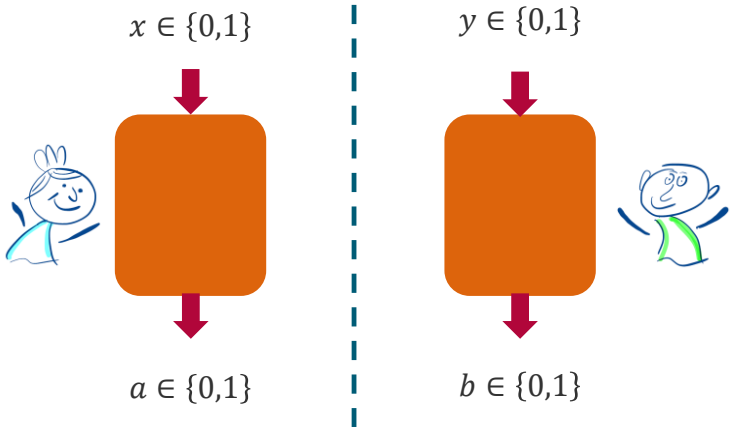
- Es wird implizit angenommen, dass
  - Alice und Bobs Labore isoliert (nicht zugänglich) sind.
  - Zustände exakt präpariert werden können.
  - Messapparaturen zuverlässig funktionieren.
  - Alice und Bob dasselbe "Timing" haben.

Idee: Device Independent QKD

- Sicherheitsdefinition unabhängig von der Zuverlässigkeit der benutzten Komponenten.
  - Den benutzten Apparaturen muss nicht vertraut werden.
    - Sind Black-Boxes für Alice und Bob.
  - Können unzuverlässig sein.
  - Können im Prinzip sogar von Eve stammen.
  - Ausnutzung der Monogamie-Eigenschaft von einem maximal verschränkten Qubit-Paar.

Idee

- Alice und Bob arbeiten je mit einer Black-Box.
  - Besitzen zwei Mögliche Eingaben und zwei mögliche Ausgaben.
  - Test der Apparaturen durch ein CHSH-Spiel.

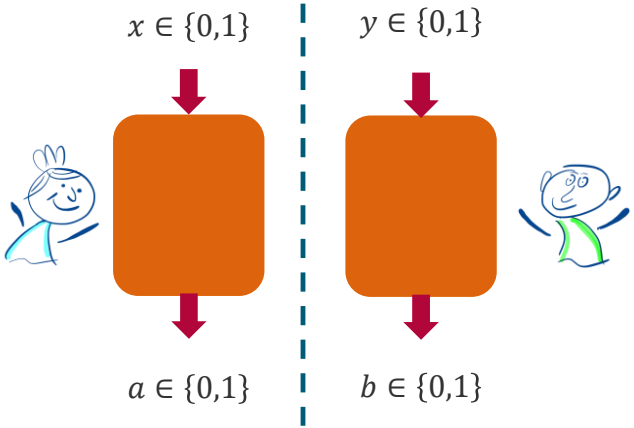


Alice und Bob geben zufällig jeweils 0 oder 1 in ihren Apparat und protokollieren die Ausgabe

Klassisch versus Quantum

- Ziel ist die Erfüllung folgender Gleichung

$$a \oplus b = x \cdot y$$



Klassische Gewinnwahrscheinlichkeit 0,75

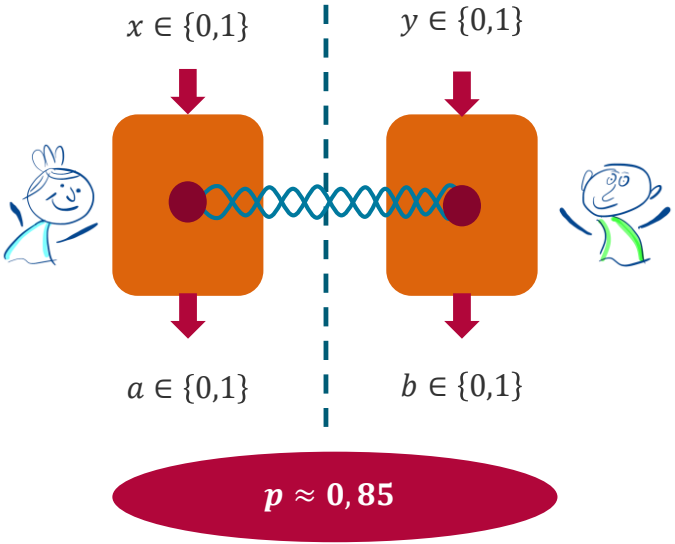
x	y	$x \wedge y$	$x \oplus y$	
0	0	0	$a(0) \oplus b(0)$	$\Rightarrow a(0) = b(0)$
0	1	0	$a(0) \oplus b(1)$	$\Rightarrow a(0) = b(1)$
1	0	0	$a(1) \oplus b(0)$	$\Rightarrow a(1) = b(0)$
1	1	1	$a(1) \oplus b(1)$	$\Rightarrow \boldsymbol{a(1) \neq b(1)}$

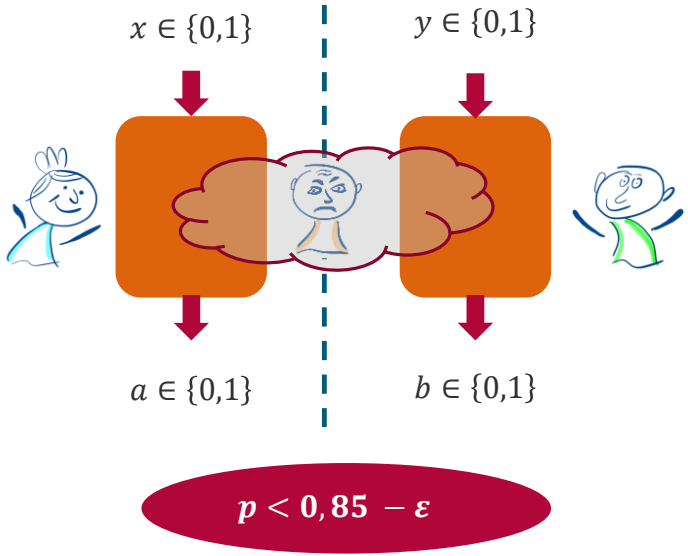
Widerspruch zu $a(1) \neq b(1)$:

$$b(1) = a(0) = b(0) = a(1)$$

Messstatistik "verrät" die Interna

- Gewinnwahrscheinlichkeiten
  - Klassisch: 0,75
  - Quantum: $\frac{1}{2} + \frac{1}{2\sqrt{2}} \approx 0{,}85$ (bei zwei maximal verschränkten Qubits)





Device Independent QKD

- Einzigen Forderungen sind:
  - Alice und Bobs Labore sind sicher bezüglich "Eindringlingen".
  - Beide besitzen einen vertrauenswürdigen Zufallsgenerator.
  - Vertrauenswürdiger Authentifizierungskanal ist vorhanden.
    - Alice und Bob können "zwischen den Runden" kommunizieren.
  - Durchführung eines sicheren "Post-Processings".
  - Quantenphysik ist korrekt und umfassend.

Zusammenfassung

- Für verschränkungsbasierte Protokolle kann ein "Sicherheitsbeweis" angegeben werden.
  - Die Sicherheit arbeitet mit Schranken (ε-Sicherheit).
  - Basiert auf ε-Korrektheit und einer ε-Geheimhaltung.
  - Es wird von idealen Randbedingungen und Implementierungen ausgegangen.

- Bei *Device Independent Quantum Key Distribution* untersucht man Protokolle, bei denen möglichst keine Annahmen mehr über Implementierungsdetails gemacht werden müsse.
  - Sicherheit ist durch statistische Tests überprüfbar.

Vielen Dank
für die Aufmerksamkeit!

Prof. Dr. Jörg Hettel
Hochschule Kaiserslautern
Fachbereich Informatik