



Quantenkryptographie (Teil 2) - CHSH Ungleichung – Simulation

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

Quanten- kryptographie

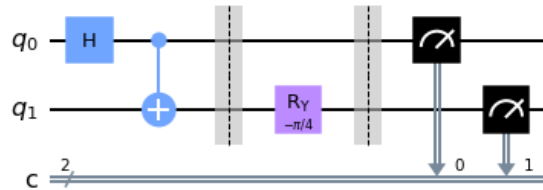
Prof. Dr. Jörg Hettel
Hochschule
Kaiserslautern
Chart 2

Korrelationsfunktionen

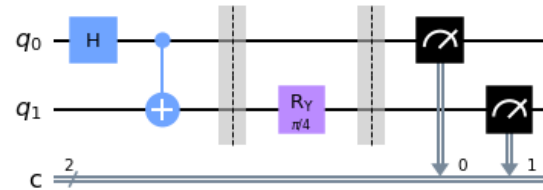
- Benötigt werden die vier Korrelationsfunktionen $E(\phi, \theta)$

$$S = E(0, \frac{\pi}{8}) + E(0, -\frac{\pi}{8}) + E(\frac{\pi}{4}, \frac{\pi}{8}) - E(\frac{\pi}{4}, -\frac{\pi}{8})$$

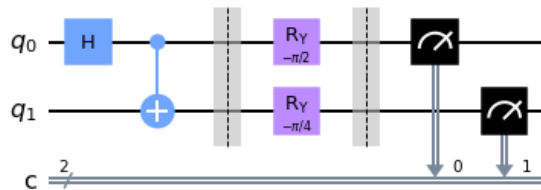
- Einzelne Funktionen können jeweils mit eigenem Schaltkreis ausgewertet werden.



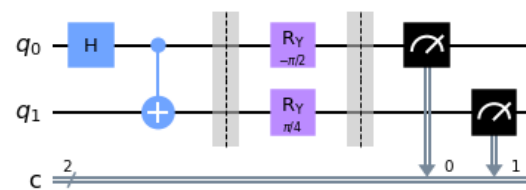
$$E(0, \frac{\pi}{8})$$



$$E(0, -\frac{\pi}{8})$$



$$E(\frac{\pi}{4}, \frac{\pi}{8})$$

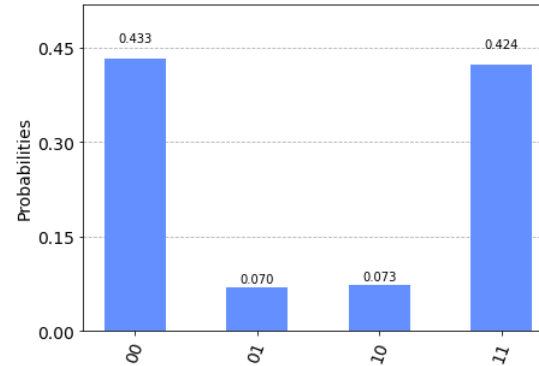
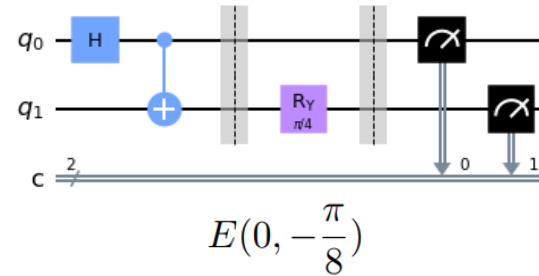
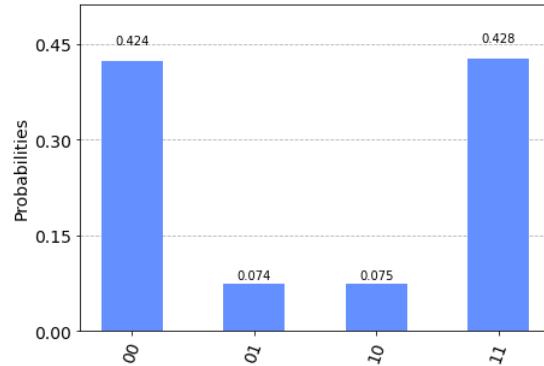
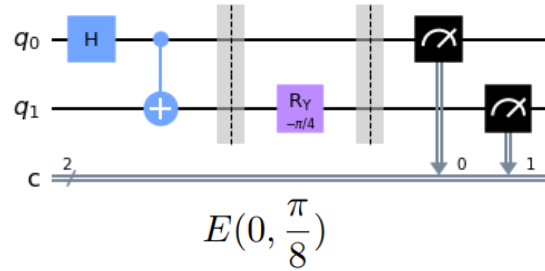


$$E(\frac{\pi}{4}, -\frac{\pi}{8})$$

Quanten- kryptographie

Prof. Dr. Jörg Hettel
Hochschule
Kaiserslautern
Chart 4

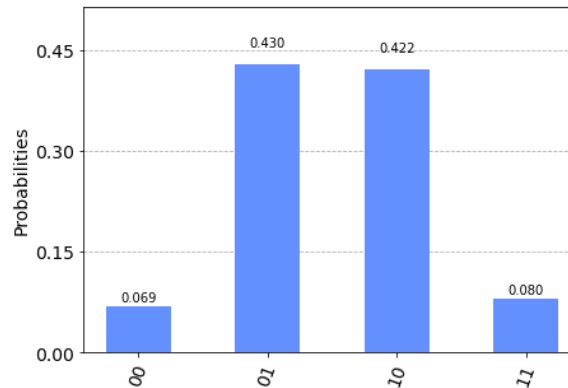
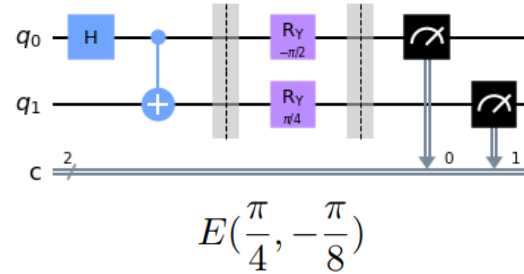
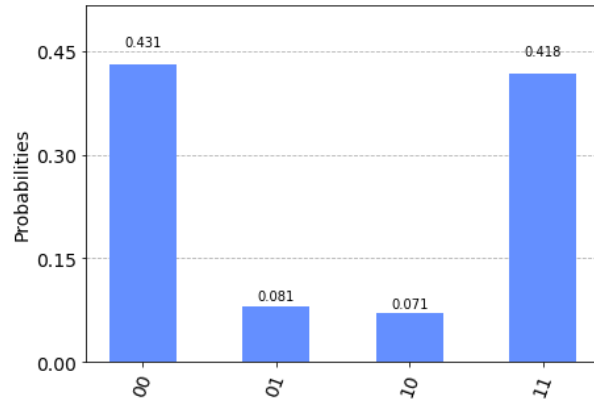
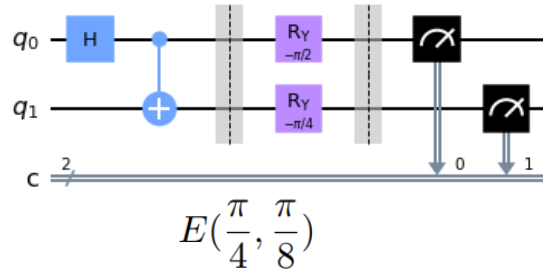
Simulation mit Qiskit



Quanten-kryptographie

Prof. Dr. Jörg Hettel
Hochschule
Kaiserslautern
Chart 5

Simulation mit Qiskit



Quanten-kryptographie

Prof. Dr. Jörg Hettel
Hochschule
Kaiserslautern
Chart 6

Auswertung der Simulation

- Benötigt werden die vier Korrelationsfunktionen $E(\phi, \theta)$

$$S = E(0, \frac{\pi}{8}) + E(0, -\frac{\pi}{8}) + E(\frac{\pi}{4}, \frac{\pi}{8}) - E(\frac{\pi}{4}, -\frac{\pi}{8})$$

```
print("E1: {:.>3f}".format(E1))
print("E2: {:.>3f}".format(E2))
print("E3: {:.>3f}".format(E3))
print("E4: {:.>3f}".format(E4))
E = E1 + E2 + E3 - E4
print("Correlation {:.>3f}".format(E) )
print("Theoretical Value {:.>3f}".format(2*np.sqrt(2)) )
```

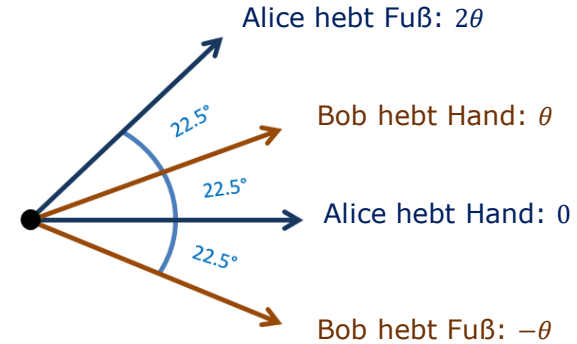
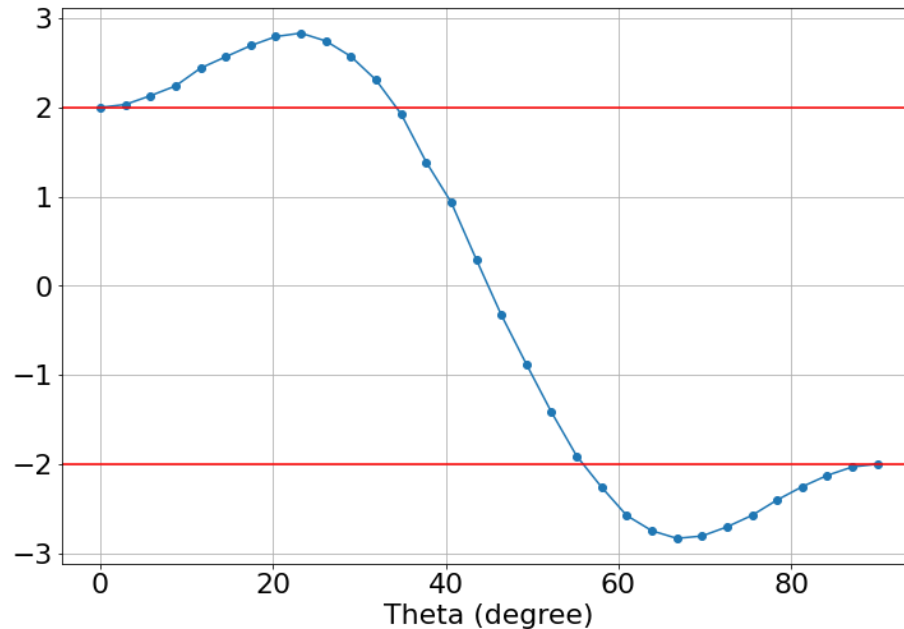
```
E1: 0.703600
E2: 0.714400
E3: 0.696400
E4: -0.703200
Correlation 2.817600
Theoretical Value 2.828427
```

Quanten- kryptographie

Prof. Dr. Jörg Hettel
Hochschule
Kaiserslautern
Chart 7

Abhängigkeit vom Winkel (Simulation mit Qiskit)

$$S = E(0, \theta) + E(0, -\theta) + E(2\theta, \theta) - E(2\theta, -\theta)$$



Quanten-kryptographie

Prof. Dr. Jörg Hettel
Hochschule
Kaiserslautern
Chart 8



Vielen Dank
für die Aufmerksamkeit!

Prof. Dr. Jörg Hettel
Hochschule Kaiserslautern
Fachbereich Informatik