Quantenkryptographie (Teil 2) - Schmidt-Darstellung

Prof. Dr. Jörg Hettel
Hochschule Kaiserslautern
Fachbereich Informatik

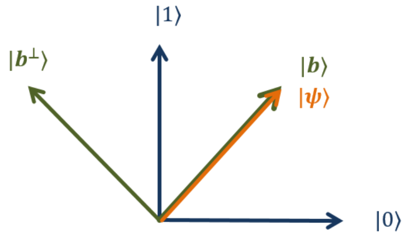
Agenda

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

Schmidt-Darstellung

- Für ein allgemeines Qubit $|\Psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ können wir immer eine Basis
  - $|b\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$
  - $|b^{\perp}\rangle = -\beta\,|0\rangle + \alpha\,|1\rangle$

  wählen, so dass gilt
  - $|\Psi\rangle = |b\rangle$



- Ein separables 2-Qubit-System
  - $|\Psi\rangle = (\alpha_1\,|0\rangle_A + \beta_1\,|1\rangle_A) \otimes (\alpha_2\,|0\rangle_B + \beta_2\,|1\rangle_B)$

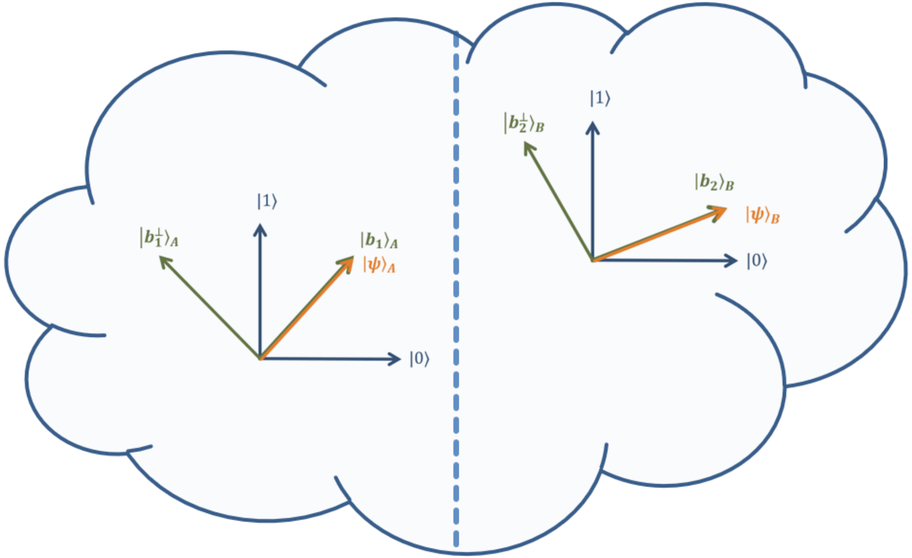
  kann somit immer in folgender Form geschrieben werden
  - $|\Psi\rangle = |b_1\rangle_A |b_2\rangle_B$

  mit $|b_1\rangle_A = \alpha_1\,|0\rangle_A + \beta_1\,|1\rangle_A$ und $|b_2\rangle_B = \alpha_1\,|0\rangle_B + \beta_1\,|1\rangle_B$

Schmidt Dekomposition

- Schmidt-Darstellung für ein separables System

$$|\Psi\rangle = |\Psi\rangle_A \otimes |\Psi\rangle_B = |b_1\rangle_A |b_2\rangle_B$$



Schmidt Dekomposition

- Ein verschränktes allgemeines bi-partites System A-B kann immer in folgender Form geschrieben werden
  - $|\Psi\rangle = \sqrt{\lambda_1}|b_1\rangle_A|b_2\rangle_B + \sqrt{\lambda_2}\left|b_1^\perp\right\rangle_A\left|b_2^\perp\right\rangle_B$

  mit $\lambda_1 + \lambda_2 = 1$ $(\lambda_1, \lambda_2 \in \mathbb{R})$ und $\{|b_1\rangle_A, \left|b_1^\perp\right\rangle_A\}$ bilden eine Orthonomalbasis des Systems A und $\{|b_1\rangle_B, \left|b_2^\perp\right\rangle_B\}$ bilden eine Orthonomalbasis des Systems B.
  - Gilt natürlich auch insbesondere für 2-Qubit-Systeme.

- Bemerkung: Die Berechnung von $\{|b_1\rangle_A, \left|b_1^\perp\right\rangle_A\}$, $\{|b_1\rangle_B, \left|b_2^\perp\right\rangle_B\}$ und λ_1, λ_2 kann über eine "Singulärwertzerlegung" erfolgen.
  - Standardoperation für Matrizenrechnung.

Beispiel

- Betrachte den verschränkten Zustand $|\Psi\rangle = \frac{1}{2}\left(|00\rangle - |01\rangle + |10\rangle + |11\rangle\right)$
- Koeffizientenmatrix $C = \begin{pmatrix} c_{|00\rangle} & c_{|01\rangle} \\ c_{|10\rangle} & c_{|11\rangle} \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$
- Singulärwertzerlegung $C = U \cdot \Lambda \cdot V^\dagger$
- Ergibt die Matrizen $U = \frac{1}{\sqrt{2}}\begin{pmatrix} -1 & -1 \\ -1 & 1 \end{pmatrix}, \quad \Lambda = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad V^\dagger = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$
- Zustand in neuer Basis $|\Psi\rangle = \frac{1}{\sqrt{2}}\left(|b_1\rangle_A |b_2\rangle_B + |b_1^\perp\rangle_A |b_2^\perp\rangle_B\right)$

Basistransformationen

- Basistransformation für System A:

$$
\begin{aligned}
|b_1\rangle_A &= U\,|0\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}-1 & -1\\ -1 & 1\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}-1\\-1\end{pmatrix} = \frac{-1}{\sqrt{2}}(|0\rangle + |1\rangle)\\
|b_1^{\perp}\rangle_A &= U\,|1\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}-1 & -1\\ -1 & 1\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}-1\\1\end{pmatrix} = \frac{-1}{\sqrt{2}}(|0\rangle - |1\rangle)
\end{aligned}
$$

- Basistransformation für System B:

$$
\begin{aligned}
|b_2\rangle_B &= V^{\dagger}\,|0\rangle = \begin{pmatrix}-1 & 0\\ 0 & 1\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}-1\\0\end{pmatrix} = -\,|0\rangle\\
|b_2^{\perp}\rangle_B &= V^{\dagger}\,|1\rangle = \begin{pmatrix}-1 & 0\\ 0 & 1\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}0\\1\end{pmatrix} = |1\rangle
\end{aligned}
$$

Beispiel: Berechnung mit Python

Schmidt-Darstellung

In [1]:
```
from sympy.physics.quantum import Dagger

from scipy import linalg
from math import sqrt

import numpy as np

np.set_printoptions(precision=5, suppress=True)
```

In [2]:
```
print("Zustand: (|00> - |01> + |10> + |11>)/2\n")
print("Koeffizientenmatrix" )
C = np.array([ [1.0, -1.0],
               [1.0,  1.0]]
            )/2
print(C)

print("\nCheck: Summe der quadrierten Elemente")
print( np.sum(C**2) )

U, S, V_dag = linalg.svd(C,full_matrices=False)

print("\nMatrix U")
print(U)

print("\nDiagonalelemente der Matrix S")
print(S)

print("\nMatrix V_dag")
print(V_dag)
```

```
Zustand: (|00> - |01> + |10> + |11>)/2

Koeffizientenmatrix
[[ 0.5 -0.5]
 [ 0.5  0.5]]

Check: Summe der quadrierten Elemente
1.0

Matrix U
[[-0.70711 -0.70711]
 [-0.70711  0.70711]]

Diagonalelemente der Matrix S
[0.70711 0.70711]

Matrix V_dag
[[-1. -0.]
 [ 0.  1.]]
```

In [3]:
```
print("Basis-Vektoren Teil 1")
print(U[:,0])
print(U[:,1])
```

```
Basis-Vektoren Teil 1
[-0.70711 -0.70711]
[-0.70711  0.70711]
```

In [4]:
```
print("Basis-Vektoren Teil 2")
V = Dagger(V_dag)
print(V[:,0])
print(V[:,1])
```

```
Basis-Vektoren Teil 2
[-1. -0.]
[0. 1.]
```

"Partitionierung" eines W-Zustandes: (AB)C

- Betrachte den verschränkten Zustand $|\Psi\rangle_{ABC} = \frac{1}{\sqrt{3}}(|001\rangle + |010\rangle + |100\rangle)$

- Zerlegung in AB-C

$$C = \begin{pmatrix} c_{|00\rangle|0\rangle} & c_{|00\rangle|1\rangle} \\ c_{|01\rangle|0\rangle} & c_{|01\rangle|1\rangle} \\ c_{|10\rangle|0\rangle} & c_{|10\rangle|1\rangle} \\ c_{|11\rangle|0\rangle} & c_{|11\rangle|1\rangle} \end{pmatrix} = \begin{pmatrix} 0 & \frac{1}{\sqrt{3}} \\ \frac{1}{\sqrt{3}} & 0 \\ \frac{1}{\sqrt{3}} & 0 \\ 0 & 0 \end{pmatrix}$$

- Singulärwertzerlegung $C = U \cdot \Lambda \cdot V^\dagger$

$$U = \begin{pmatrix} 0 & 1 & 0 & 0 \\ \frac{1}{\sqrt{2}} & 0 & -\frac{1}{\sqrt{3}} & 0 \\ \frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{3}} & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \qquad \Lambda = \begin{pmatrix} \sqrt{\frac{2}{3}} & 0 \\ 0 & \sqrt{\frac{1}{3}} \\ 0 & 0 \\ 0 & 0 \end{pmatrix} \qquad V^\dagger = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Zerlegung eines W-Zustandes

- Schmidt-Darstellung $$|W\rangle = |\Psi\rangle_{ABC} = \sqrt{\frac{2}{3}}\,|b_1\rangle_{AB}\,|b_2\rangle_C + \frac{1}{\sqrt{3}}\,|b_1^\perp\rangle_{AB}\,|b_2^\perp\rangle_C$$

- Mit den beiden Basen

$$\begin{aligned} |b_1\rangle_{AB} &= \frac{1}{\sqrt{2}}\left(|01\rangle_{AB} + |10\rangle_{AB}\right) \\ |b_1^\perp\rangle_{AB} &= |00\rangle_{AB} \end{aligned}$$

$$\begin{aligned} |b_2\rangle_C &= |0\rangle_C \\ |b_2^\perp\rangle_C &= |1\rangle_C \end{aligned}$$

Beispiel: Berechnung mit Python

Schmidt-Darstellung

In [1]:
```
from sympy.physics.quantum import Dagger

from scipy import linalg
from math import sqrt

import numpy as np

np.set_printoptions(precision=5, suppress=True)
```

In [2]:
```
print("Zustand: (|001> + |010> + |100> )/sqrt(3)\n")
print("Koeffizientenmatrix" )
C = np.array([ [0.0,  1.0],
               [1.0,  0.0],
               [1.0,  0.0],
               [0.0,  0.0]]
            )/np.sqrt(3)


print(C)

U, S, V_dag = linalg.svd(C,full_matrices=False)

print("\nMatrix U")
print(U)

print("\nDiagonalelemente der Matrix S")
print(S)

print("\nMatrix V_dag")
print(V_dag)
```

```
Zustand: (|001> + |010> + |100> )/sqrt(3)

Koeffizientenmatrix
[[0.      0.57735]
 [0.57735 0.     ]
 [0.57735 0.     ]
 [0.      0.     ]]

Matrix U
[[ 0.       1.     ]
 [-0.70711  0.     ]
 [-0.70711  0.     ]
 [ 0.       0.     ]]

Diagonalelemente der Matrix S
[0.8165  0.57735]

Matrix V_dag
[[-1. -0.]
 [ 0.  1.]]
```

In [3]:
```
print("Basis-Vektoren Teil 1")
print(U[:,0])
print(U[:,1])
```

```
Basis-Vektoren Teil 1
[ 0.      -0.70711 -0.70711  0.     ]
[1. 0. 0. 0.]
```

In [4]:
```
print("Basis-Vektoren Teil 2")
V = Dagger(V_dag)
print(V[:,0])
print(V[:,1])
```

```
Basis-Vektoren Teil 2
[-1. -0.]
[0. 1.]
```

Zusammenfassung

- Die Schmidt-Darstellung ist eine "Normalform-Darstellung" für bi-partite Systeme.
  - Es gibt ein Standardverfahren für die Bestimmung dieser Darstellung.

- Schmidt-Darstellung eines Ein-Qubit-Systems:

$$|\Psi\rangle = |b\rangle$$

- Schmidt-Darstellung von Zwei-Qubit-Systemen:
  - Separierbar: $|\Psi\rangle = |b_1\rangle_A |b_2\rangle_B$
  - Verschränkt: $|\Psi\rangle = \sqrt{\lambda_1}|b_1\rangle_A |b_2\rangle_B + \sqrt{\lambda_2}\left|b_1^{\perp}\right\rangle_A \left|b_2^{\perp}\right\rangle_B$

Hasso Plattner Institut
Digital Engineering · Universität Potsdam

Vielen Dank
für die Aufmerksamkeit!

Prof. Dr. Jörg Hettel
Hochschule Kaiserslautern
Fachbereich Informatik