Quantum channel characterization and effective entanglement

Marion Semmler

Scheinseminar Quantenoptik und Photonik
Friedrich-Alexander-Universität Erlangen-Nürnberg

29.07.2011
Outline

1. Motivation
2. Basics on quantum mechanics
3. Basics on information theory
4. Channel characterization
5. QKD protocols
6. Experimental implementation
7. Summary
Motivation
Motivation

**Figure**: Schematic information exchange
Motivation

Input-Signal
- Carrier of information
- Encoded

Example
- Binary signal
- Amplitude-encoded
- E.g. laser pulses

Figure: Amplitude-encoded signal
Motivation

Channel
- Medium that allows transmission of information
- Achieved by using electromagnetic signals

Examples
- Fibres, free-space
- Telephone cable (electronic)
- Data memory

Figure: Different channels
[Variouspictures, 2011]
Motivation

Output-Signal

- Carrier of information
- Needs to be decoded

Possible influence of the channel

- Smeared in time
- Amplitude and phase noise
- Damping (losses)

Figure: Disturbed signal

⇒ Channel characterization necessary
Basics on quantum mechanics
Basics on quantum mechanics

Pure states

- Pure state $|\psi\rangle$
- Composition of orthonormal basis
  \[ |\psi\rangle = a |0\rangle + b |1\rangle \]
- Normalization: $\langle \psi | \psi \rangle = |a|^2 + |b|^2 = 1$
- Coherent superposition of pure states $|\phi\rangle = \lambda_1 |\psi_1\rangle + \lambda_2 |\psi_2\rangle$

Density matrix of a pure state

- $\rho = |\psi\rangle \langle \psi | = |a|^2 |0\rangle \langle 0| + |b|^2 |1\rangle \langle 1| + ab^* |0\rangle \langle 1| + a^* b |1\rangle \langle 0|$
- $\rho = \begin{pmatrix} |a|^2 & ab^* \\ a^* b & |b|^2 \end{pmatrix} \Rightarrow \rho_{\text{diagonal}} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$
Basics on quantum mechanics

Mixed states

- Mixed state $\rho = \sum_i \lambda_i |\psi_i\rangle \langle \psi_i|$  
- Probabilities $\lambda_i$ with $\sum_i \lambda_i = 1$
- Statistical mixture of pure states $|\psi_i\rangle = a_i |0\rangle + b_i |1\rangle$ with $|a_i|^2 + |b_i|^2 = 1$
- Statistical mixture $\neq$ Coherent superposition

Density matrix of a mixed state

- $\rho = \lambda_1 |\psi_1\rangle \langle \psi_1| + \lambda_2 |\psi_2\rangle \langle \psi_2|$
- $\rho = \begin{pmatrix} \lambda_1 |a_1|^2 + \lambda_2 |a_2|^2 & \lambda_1 a_1 b_1^* + \lambda_2 a_2 b_2^* \\ \lambda_1 a_1^* b_1 + \lambda_2 a_2^* b_2 & \lambda_1 |b_1|^2 + \lambda_2 |b_2|^2 \end{pmatrix} \Rightarrow \rho_{\text{diagonal}} = \begin{pmatrix} \epsilon_1 & 0 \\ 0 & \epsilon_2 \end{pmatrix}$
- Eigenvalues $\epsilon_1, \epsilon_2 \neq 0$
Basics on quantum mechanics

Transition to more particles

For a single photon:

- 1 Hilbert space per photon
- $|\psi\rangle = a_1 |0\rangle + b_1 |1\rangle$
- $|\gamma\rangle = a_2 |0\rangle + b_2 |1\rangle$

For two photons:

- Joint Hilbert space
- Tensor product $|\Psi\rangle = |\psi\rangle_1 \otimes |\gamma\rangle_2 \rightarrow$ separable
- $|\Psi\rangle = a_1 a_2 |0\rangle_1 |0\rangle_2 + a_1 b_2 |0\rangle_1 |1\rangle_2 + b_1 a_2 |1\rangle_1 |0\rangle_2 + b_1 b_2 |1\rangle_1 |1\rangle_2$
Basics on quantum mechanics

Arbitrary state in joint Hilbert space

\[ |\Psi\rangle = a_1 a_2 |0\rangle_1 |0\rangle_2 + a_1 b_2 |0\rangle_1 |1\rangle_2 + b_1 a_2 |1\rangle_1 |0\rangle_2 + b_1 b_2 |1\rangle_1 |1\rangle_2 \]

Entangled states

- Entangled state \( \Psi \) between 1 and 2
- \[ |\Psi\rangle = \alpha_1 |0\rangle_1 |1\rangle_2 + \alpha_2 |1\rangle_1 |0\rangle_2 \] with \( \alpha_1, \alpha_2 \neq 0 \)
- not separable

Bell-states

- Maximally entangled for \( |\alpha_1| = |\alpha_2| = \frac{1}{\sqrt{2}} \)
- \[ |\Psi_{\text{Bell}}\rangle = \frac{1}{\sqrt{2}} (|0\rangle_1 |1\rangle_2 \pm |1\rangle_1 |0\rangle_2) \]
Basics on quantum mechanics

**Example: Effective entanglement**

- Alice tosses a coin
- Head: Alice sends $|H\rangle$ to Bob
- Tail: Alice sends $|V\rangle$ to Bob
- Effectively entangled state: $|\Psi\rangle = \frac{1}{\sqrt{2}} (|\text{head}\rangle_A |H\rangle_B + |\text{tail}\rangle_A |V\rangle_B)$

**Formal concept of effective entanglement**

- Wave function from tensor product $|\Psi\rangle = \sum_i |\psi_i\rangle_1 |\phi_i\rangle_2$
- Subsystem 1 with orthonormal basis $\langle \psi_i | \psi_j \rangle = \delta_{ij}$
- Subsystem 2 can have non-orthogonal basis $\langle \phi_i | \phi_j \rangle \neq \delta_{ij}$
- Random number generation (RNG) determines projective measurement $|\psi_i\rangle \langle \psi_i|\text{ in subsystem 1}$

[Bennett, 1992]
Basics on quantum mechanics

Discrete & Continuous Variables

- Measurement outcomes are discrete
- Polarization of single photon ($|H\rangle, |V\rangle$)
- Click-Detector

- Measurement outcomes span a continuous space
- Quadratures ($\hat{x}, \hat{p}$)
- Homodyne-Detector

**Figure:** Detection of discrete variables

**Figure:** Detection of continuous variables
Basics on quantum mechanics

Example: 50/50-Beamsplitter

- $|\psi\rangle_{in} = |1\rangle_{1} |0\rangle_{2} = a_{1}^{\dagger} |0\rangle_{1} |0\rangle_{2}$
- $\begin{pmatrix} a_{1}^{\dagger} \\ a_{2} \end{pmatrix} = \begin{pmatrix} t & r \\ -r & t \end{pmatrix} \cdot \begin{pmatrix} a_{3}^{\dagger} \\ a_{4} \end{pmatrix}$ with $|r| = |t| = \frac{1}{\sqrt{2}}$
- $|\psi\rangle_{out} = \frac{1}{\sqrt{2}} \left(a_{3}^{\dagger} + a_{4}^{\dagger}\right) |0\rangle_{3} |0\rangle_{4} = \frac{1}{\sqrt{2}} \left(|1\rangle_{3} |0\rangle_{4} + |0\rangle_{3} |1\rangle_{4}\right)$
- Entanglement between output modes

Figure: Source for entangled states
Example: Subsystem 2 described by coherent states

- $|\psi_0\rangle = |0\rangle, \ |\psi_1\rangle = |1\rangle \Rightarrow \langle \psi_0 | \psi_1 \rangle = 0$
- $|\phi_0\rangle = |\alpha\rangle, \ |\phi_1\rangle = |-\alpha\rangle$
- $\langle \phi_0 | \phi_1 \rangle = \langle \alpha | -\alpha \rangle \neq 0$
- Effectively entangled state $|\Psi\rangle = \frac{1}{\sqrt{2}} (|0\rangle_A |\alpha\rangle_B + |1\rangle_A |-\alpha\rangle_B )$
- RNG: random choice of projective measurement $|0\rangle \langle 0|$ or $|1\rangle \langle 1|$,
- Projection of the other subsystem in $|\alpha\rangle$ or $|-\alpha\rangle$, respectively

Figure: Coherent states with opposite phases [Wittmann, 2011]
Basics on information theory
Basics on information theory

Shannon-Entropy

Analogy to thermodynamics:
- Information like incompressible fluid
- Source of information can be quantified by entropy
- Degree of randomness/disorder

Interpretation
- Entropy ↓: Redundancy/statistical regularity in information text
- Entropy ↑: Random information text/statistically independent
Basics on information theory

Alphabet

- $Z = \{z_1, z_2, \ldots, z_m\}$
- $z_i$: Symbol/letter/event
- $p_{z_i}$: Probability of a symbol

Self-information

- $I(p_{z_i}) = -\log_2(p_{z_i})$

Entropy

- Expectation value of self-information
- $H = \sum_{z_i \in Z} p_{z_i} \cdot I(p_{z_i}) = -\sum_{z_i \in Z} p_{z_i} \cdot \log_2(p_{z_i})$
### Basics on information theory

#### Ideal coin
- $p_{\text{head}} = \frac{1}{2}$, $p_{\text{tail}} = \frac{1}{2}$
- $H = -[p_{\text{head}} \cdot \log_2(p_{\text{head}}) + p_{\text{tail}} \cdot \log_2(p_{\text{tail}})]$
- $H = 1$
  - Outcome of flipping a perfect coin is completely uncertain

#### Biased coin
- $p_{\text{head}} = 0.6$, $p_{\text{tail}} = 0.4$
- $H = -[0.6 \cdot \log_2(0.6) + 0.4 \cdot \log_2(0.4)]$
- $H = 0.971$
  - Outcome of flipping a biased coin is less uncertain

**Figure:** Entropy of flipping a coin [Wikipedia, ]
Basics on information theory

**Conditional entropy**
- **Notation:** \( H(X|Y) \)
- Uncertainty about source \( X \) when \( Y \) is known
- \( H(X|Y) = - \sum_{x \in M} p(X|Y) \cdot \log_2(p(X|Y)) \leq H(X) \)

**Mutual information**
- **Notation:** \( I(X, Y) \)
- Measures the mutual dependence of the two variables
- \( I(X, Y) = H(X) - H(X|Y) = H(Y) - H(Y|X) \)
- \( I(X, Y) = 0 \iff X \& Y \) statistically independent
- \( I(X, Y) \) maximal \( \iff \) functional dependency
Channel characterization
Channel characterization

Definition: Channel

- Abstraction of physical medium that transmits information in space or time
- Characteristic parameter: capacity

Channel-capacity

- Supremum of all in time $\tau$ transmitted signs without errors $\Rightarrow$ maximum error-free bit rate
- $C = \frac{1}{\tau} \cdot \text{Max}_{p(x)} [I(X, Y)]$
- Dependence of type of channel

[Smith, 2010]
Channel characterization

**Formal definition of a quantum channel**
- Preservation of some quantum properties of transmitted state

**Possible applications of a quantum channel**
- Classical communication
- Quantum key distribution (QKD)
- Quantum repeater
- Quantum memory
- Quantum teleportation
QKD protocols
QKD protocols

Create correlation
- Entanglement-based scheme
- Prepare-and-measure scheme

Post processing - Key distillation
- Sifting of key elements
- Calculation of mutual information $I_{AB}, I_{AE}, I_{BE}$
- Privacy amplification
QKD protocols

Prepare-and-measure-scheme on the basis of BB84

- Alice uses a single-photon-source
- Alice chooses a random bit and a random basis to encode the qubit (e.g. “0”, “x”)
- Alice sends qubit (e.g. \( \downarrow \)) to Bob
- Bob measures state with random basis

Complementary pair of basis and bits

<table>
<thead>
<tr>
<th>Bit: 1</th>
<th>Bit: 0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basis: +</td>
<td>( \uparrow )</td>
</tr>
<tr>
<td>Basis: x</td>
<td>( \nearrow )</td>
</tr>
</tbody>
</table>

**Table:** Bits and Basis

**Figure:** Complementary pair of basis
QKD protocols

Entanglement-based-scheme

- Alice & Bob use a source that can create entangled states
- $|\psi\rangle = \frac{1}{\sqrt{2}} (|H\rangle_A |V\rangle_B + |V\rangle_A |H\rangle_B )$
  $= \frac{1}{\sqrt{2}} (|45^\circ\rangle_A |45^\circ\rangle_B - |45^\circ\rangle_A |45^\circ\rangle_B )$
- Subsystems of $|\psi\rangle$ distributed to Alice and Bob
- Alice randomly chooses H/V- and $45^\circ$/-$45^\circ$-basis and measures
- Bob randomly chooses a basis and measures

Example: Alice’s basis $45^\circ$/-$45^\circ$

<table>
<thead>
<tr>
<th>Alice outcome p=0.5</th>
<th>↑</th>
<th>↑</th>
<th>↓</th>
<th>↓</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bob’s system</td>
<td>↑</td>
<td>↑</td>
<td>↓</td>
<td>↓</td>
</tr>
<tr>
<td>Bob’s basis</td>
<td>↓</td>
<td>✗</td>
<td>↑</td>
<td>✗</td>
</tr>
<tr>
<td>Bob’s outcome</td>
<td>?</td>
<td>↑</td>
<td>?</td>
<td>↑</td>
</tr>
</tbody>
</table>

Table: Bits and Basis
QKD protocols

Bob can not distinguish

Distribution of $|\Psi\rangle = \frac{1}{\sqrt{2}} (|H\rangle_A |V\rangle_B + |V\rangle_A |H\rangle_B)$

Measurement in Alice’s subsystem

$\equiv$

$|\Psi\rangle = \frac{1}{\sqrt{2}} (|head\rangle_A |H\rangle_B + |tail\rangle_A |V\rangle_B)$

Alice sends state according to her RNG

[Bennett, 1992]

Figure: Equivalence of different schemes [Wittmann, 2011]
QKD protocols

Entanglement-based scheme

- Entanglement of real physical systems
- \[ |\psi\rangle = \frac{1}{\sqrt{2}} (|H\rangle_A |V\rangle_B + |V\rangle_A |H\rangle_B) \]
- Two physical systems are shared
- Alice measures \(\rightarrow\) random outcome

Prepare-and-measure scheme

- Effectively entangled state
- \[ |\psi\rangle = \frac{1}{\sqrt{2}} (|\text{head}\rangle_A |H\rangle_B + |\text{tail}\rangle_A |V\rangle_B) \]
- Only one physical system is shared
- Alice uses RNG \(\rightarrow\) generates state to be transmitted accordingly
QKD protocols

Sifting of key-elements

- Publishing basis
- Discard measurements with different basis
- Discard Bob’s empty slots

Evaluation

- Publishing randomly chosen sequence of key-elements
- Evaluation of some properties of the quantum channel
- Calculation of correlation and mutual information $I_{AB}$
- Estimation of Eve’s maximum of information $I_{AE}, I_{BE}$
- Abortion of protocol if $I_{AE} - I_{AB} > 0$
Privacy amplification

- Aim: Reduce Eve’s Information
- Using a oneway function
- Length of secret key gets smaller

Example: XOR-operation

Table: XOR-operation

<table>
<thead>
<tr>
<th>Input</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 0</td>
<td>0</td>
</tr>
<tr>
<td>0 1</td>
<td>1</td>
</tr>
<tr>
<td>1 0</td>
<td>1</td>
</tr>
<tr>
<td>1 1</td>
<td>0</td>
</tr>
</tbody>
</table>

Figure: XOR-operation on the raw key shared by Alice and Bob
Experimental implementation
Experimental implementation

Effectively entangled state

$$|\psi\rangle = \frac{1}{\sqrt{2}} (|0\rangle_A |\alpha\rangle_B + |1\rangle_A |-\alpha\rangle_B)$$

Effect of the state by the channel

Figure: Continuous variable QKD in fibres [Wittmann et al., 2010]
Experimental implementation

Figure: Schematic of experimental setup [Wittmann et al., 2010]
Experimental implementation

Alice’s part

- laser
- BS
- delay
- mod.
- BS
- att.
- Preparation
- monitor A
- BS
- pol. control

Alice
Experimental implementation

Transmission

quantum channel Transmission
Experimental implementation

Bob’s part

Detection

detection stage

monitor B

delay

Bob
Experimental implementation

Bob’s detection stage

Figure: Continuous variable QKD in fibres [Khan, 2011]
Experimental implementation

Entanglement verification

- Bob needs to check if the received state is entangled

Partial transpose of a density matrix

- State $\rho$ on joint Hilbert space $H_A \otimes H_B$
- $\rho = \sum_{ijkl} p_{ijkl} |i\rangle \langle j| \otimes |k\rangle \langle l|$
- Partial transpose $\rho^{TB}$
- $\rho^{TB} = \sum_{ijkl} p_{ijkl} |i\rangle \langle j| \otimes |l\rangle \langle k|$

Peres-Horodecki criterion

- If state $\rho$ is separable, $\rho^{TB}$ only has non-negative eigenvalues.
- If $\rho^{TB}$ has a negative eigenvalue, state is guaranteed to be entangled.

[Horodecki et al., 1996]
Experimental implementation

Negativity $\mathcal{N}(\rho)$

- Measures degree of entanglement
- $\mathcal{N}(\rho) = \frac{\|\rho^{TB}\|_1 - 1}{2}$
- $\mathcal{N}(\rho) = 0$ when state $\rho$ is separable
- $0 < \mathcal{N}(\rho) < 1$ when state $\rho$ is entangled
- Can even be calculated for effective entanglement

For a given channel transmission

The negativity $\mathcal{N}(\rho)$ depends on:

- Excess noise (e.g.: Rayleigh scattering in optical fibers)
- Initial overlap $\langle \alpha | -\alpha \rangle$
Experimental implementation

Excess noise

- Coherent state: minimal, symmetrical variance of 0.5
- Excess noise from quantum channel $\approx 5\%$
- $\Rightarrow$ Symmetrical variance of received state 0.525

Figure: Excess noise in received state [Wittmann et al., 2010]
Experimental implementation

Overlap

- Signal amplitude $|\alpha| \approx 0.5$
- $\Rightarrow$ Overlap $\langle \alpha | -\alpha \rangle = 0.606$
- No overlap $\leftrightarrow$ no secret key generation between Alice and Bob
- Full overlap $\leftrightarrow$ no usable key elements for Alice and Bob

Figure: Overlap $\langle \alpha | -\alpha \rangle$ [Wittmann et al., 2010]
Summary
Quantum mechanics

- Entangled state: \( |\Psi\rangle = \alpha_1 |0\rangle_1 |1\rangle_2 + \alpha_2 |1\rangle_1 |0\rangle_2 \)
- Effectively entangled state: \( |\Psi\rangle = \frac{1}{\sqrt{2}} (|head\rangle_A |H\rangle_B + |tail\rangle_A |V\rangle_B) \)

Information theory

- Shannon entropy: \( H = - \sum_{z_i \in Z} p_{z_i} \cdot \log_2(p_{z_i}) \)
- Mutual information: \( I(X, Y) = H(X) - H(X|Y) \)
- Capacity: \( C = \frac{1}{\tau} \cdot \max_{p(x)} [I(X, Y)] \)
Summary

QKD-protocols

- QKD: correlation + key distillation
- Equivalence of entanglement-based scheme and prepare-and-measure scheme

Experimental implementation

- Alice’s preparation setup
- Bob’s detection setup
- Entanglement verification by the use of negativity
References


Continuous-variable quantum key distribution protocols with a discrete modulation.
abs/1002.4083v2.

Quantum channel capacities.
CoRR, abs/1007.2855.

Variouspictures (2011).
http://www.thegreenwichphantom.co.uk/2007/09/laser-leanings,
http://www.genius-versand.de/shop/18942/Hama-CAT-6-Netzwerkkabel-PIMF-vergoldet-doppelt-geschirmt-5,00-m-45054.htm,
viewed on 11-07-16.

Wikipedia.
viewed on 11-07-16.

Quantum detection schemes and their application.