Generation QI
Summer School
on Quantum Cryptography

Theory of Quantum Cryptography

Contents

Chapter 1

Introduction to Quantum Mechanics

1.1 Theory

1.1.1 Axioms of quantum mechanics

What is the goal of a physical theory?:

1. Provide a framework to describe and predict the behavior of physical systems

2. Provide some explanation behind that framework

Note: Our focus is on quantum cryptography, so by no means is this an exhaustive presentation. In quantum mechanics, this is achieved by introducing a set of axioms. The role of the axioms is to answer the following questions

1. How to describe a physical system?

2. What kind of information can we get about a system?

3. What kind of changes can a system undergo?

4. What to do if there are several systems?

Axiom 1: States (question 1)

A state is a complete description of a physical system. In quantum mechanics, a state is a ray in a Hilbert space.

Definition 1 *Hilbert space*

(a) *Vector space(vector addition and multiplication by scalars) over complex numbers (we will use the Dirac's notation $|\psi\rangle$).*

Example 1 *2 dimensional space*

$$|0\rangle \equiv \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$
$$|1\rangle \equiv \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

(b) *Equipped with an inner product $\langle\psi|\phi\rangle$ that maps an ordered pair of vectors to $\mathbb{C}$ numbers with properties:*

1. *Positivity $\langle\psi|\psi\rangle > 0$ for $|\psi\rangle \neq 0$*
2. *Linearity $\langle\psi| (a|\phi_1\rangle + b|\phi_2\rangle) = a\langle\psi|\phi_1\rangle + b\langle\psi|\phi_2\rangle$*
3. *Skew symmetry $\langle\psi|\phi\rangle = \langle\phi|\psi\rangle^*$*

(c) *Complete in the norm (important in infinite-dimensional spaces to ensure convergence of eigenvectors expansion).*

(d) *Ray: equivalence class of vectors. Vectors belonging to the class differ by a multiplicative complex scalar factor (it is convenient to work choose $\langle\psi|\psi\rangle = 1$)*

Remark 1 *A combination of two states is a valid state (superposition principle)*

$$|\phi_1\rangle, |\phi_2\rangle \longrightarrow a|\phi_1\rangle + b|\phi_2\rangle \ .$$

Remark 2 *In superposition only the relative phase matters*

$$a|\phi_1\rangle + e^{i\beta}b|\phi_2\rangle \equiv e^{i\alpha}(a|\phi_1\rangle + e^{i\beta}b|\phi_2\rangle)$$
$$\forall\alpha \in [0, 2\pi), a, b \in \mathbb{R}$$

Axiom 2: Observables (question 2)

A self-adjoint operator representing a property of a physical system that can be measured.

Definition 2 *A self-adjoint operator*

Linear map on a vector space that its own adjoint

(a) *Maps vectors to vectors*

$$A : |\psi\rangle \rightarrow A|\psi\rangle$$

(b) Linear

$$A(a\,|\phi_1\rangle + b\,|\phi_2\rangle) = aA\,|\phi_1\rangle + bA\,|\phi_2\rangle$$

(c) Adjoint $A^\dagger$

$$\langle\psi|A\phi\rangle = \langle A^\dagger\psi|\phi\rangle$$

(d) Self-adjoint $A^\dagger$

$$\begin{aligned} A &= A^\dagger, \\ \langle\psi|A\phi\rangle &= (\langle\phi|A\psi\rangle)^*, \forall\,|\psi\rangle\,,|\phi\rangle \\ (A+B)^\dagger &= A^\dagger + B^\dagger \\ (AB)^\dagger &= B^\dagger A^\dagger \end{aligned}$$

(e) Self-adjoint operators have a spectral representation

$$A = \sum_a \lambda_a \mathbf{E}_a,$$

where λ_a are eigenvalues (real numbers) and $\mathbf{E}_a$ are eigenvectors (orthogonal projectors). Eigenvectors satisfy:

$$\begin{aligned} \mathbf{E}_a\mathbf{E}_{a'} &= \delta_{a,a'}\mathbf{E}_a \\ \mathbf{E}_a^\dagger &= \mathbf{E}_a\ . \end{aligned}$$

In Dirac's notation projectors are represented as

$$\begin{aligned} \mathbf{E}_a &= |a\rangle\,\langle a| \\ A\,|a\rangle &= a\,|a\rangle\,. \end{aligned}$$

Axiom 3: Measurement (question 3)

The measurement outcome of an observable A on a state is an eigenvalue of A. The post-measurement state is the corresponding eigenvector.

$$|\psi\rangle \xrightarrow{\text{result a}} \frac{\mathbf{E}_a\,|\psi\rangle}{||\mathbf{E}_a\,|\psi\rangle\,||}\ .$$

(a) Spectral decomposition of A

$$A = \sum_a \lambda_a \mathbf{E}_a\ .$$

(b) Probability of outcome

$$Prob(a) = ||\mathbf{E}_a \left|\psi\right\rangle ||^2 = \langle\psi|\mathbf{E}_a|\psi\rangle \ \ .$$

(c) Post-measurement state

$$\left|\psi\right\rangle \xrightarrow{\text{result a}} \frac{\mathbf{E}_a \left|\psi\right\rangle}{||\mathbf{E}_a \left|\psi\right\rangle ||} \ \ .$$

(d) Mean value

$$\langle A\rangle = \sum_a aProb(a) = \sum_a a \langle\psi|\mathbf{E}_a|\psi\rangle = \langle\psi|A|\psi\rangle \ \ .$$

Axiom 4: Dynamics (question 3)

Time evolution of a closed system is described by a unitary operator

$$\left|\psi(t)\right\rangle = U(t,t^{'}) \left|\psi(t^{t})\right\rangle , \text{where}$$

$$U(t,t^{'})^{\dagger}U(t,t^{'}) = U(t,t^{'})U(t,t^{'})^{\dagger} = \mathbb{I}$$

Schrödinger equation governs infinitesimal time evolution

$$\frac{d}{dt}\left|\psi(t)\right\rangle = -iH(t)\left|\psi(t)\right\rangle \ \ .$$

Axiom 5: Composite systems (question 4)

For two quantum systems A and B a joint state space of a composite is constructed as tensor product of individual systems. The same applies for a joint state.

$$\left|\psi_A\right\rangle \in \mathcal{H}_A, \ \left|\psi_B\right\rangle \in \mathcal{H}_B \ ,$$

$$\left|\psi_A\right\rangle \otimes \left|\psi_B\right\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B \ .$$

Example 2 *Two qubits system*

$$\left|0\right\rangle_A \otimes \left|0\right\rangle_B = \left|00\right\rangle_{AB} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} \ \ .$$

There can be situations, in which:

(a) States are not rays in Hilbert space and then no full information about a state is available, for example

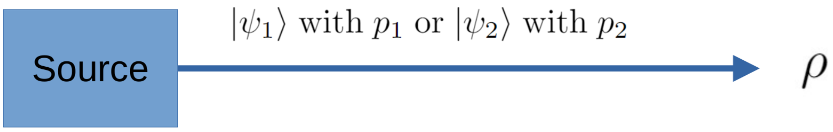

Figure 1.1: Density operator

$$\varrho = p_1 \left|\psi_1\right\rangle \left\langle\psi_1\right| + \left|\psi_2\right\rangle \left\langle\psi_2\right| \ .$$

(b) Measurements are not orthogonal projectors.

(c) Evolution is not unitary.

More generally the state is given as a density operator that is

1. Self-adjoint

$$\varrho = \varrho^\dagger$$

2. Positive

$$\langle\psi|\varrho|\psi\rangle \geq 0 \ \forall \left|\psi\right\rangle$$

3. Trace one

$$tr(\varrho) = 1$$

Axiom 3: Measurement (density operators)

(a) Spectral decomposition of A

$$A = \sum_a \lambda_a \mathbf{E}_a \ .$$

(b) Probability of outcome

$$Prob(a) = tr(\mathbf{E}_a \varrho) \ .$$

(c) Post-measurement state

$$\varrho \xrightarrow{\text{result a}} \frac{\mathbf{E}_a \varrho \mathbf{E}_a}{tr(\mathbf{E}_a \varrho)} \ .$$

(d) Mean value

$$\langle A \rangle = \sum_a a Prob(a) = \sum_a a tr(\mathbf{E}_a \varrho) = tr(A\varrho) \ .$$

Axiom 5: Composite systems (density operators)

$$\varrho_A \in \mathcal{H}_A, \ \varrho_B \in \mathcal{H}_B \ ,$$
$$\varrho_A \otimes \varrho_B = \varrho_{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B \ .$$

What to do if we have description of a composite system, and we want to focus on a single one?

Partial trace

$$\varrho = tr_A(\rho_{AB}) = \sum_i \langle i|_B \rho_{AB} |i\rangle_B$$

1.1.2 Quantum measurements: POVMs

Positive operator-valued measure (POVM) is a set of measurement operators $\{M_a\}_{a=0}^m$ (effects):

1. Effects are hermitian

$$M_a = M_a^\dagger$$

2. Effects are positive

$$M_a \geq 0$$

3. Effects form a complete set

$$\sum_a M_a = \mathbb{I}$$

4. Probability of outcome

$$Prob(a) = tr(M_a \rho)$$

In contrast to a projective measurement, for POVM the post measurement state is not uniquely defined. Naimark theorem states that POVMs can be implemented in terms of protective measurements and post-processing of outcomes on higher dimensional Hilbert spaces.

1.1.3 Classical and quantum information theory basics

Classical information theory

Consider random variable X. Each realization x of X belongs to an alphabet $\mathcal{X}$ with probability $p_X(x)$. Information content of a particular realization x is defined as

$$i(x) = -\log(p_X(x)) \ .$$

It measures "surprise" that one has learning the outcome of a random experiment. Information content concerns a particular x, what about random variable X? This is captured by **entropy**

$$H(X) \equiv -\sum_x p_X(x) \log(_X(x)) \ ,$$

For realizations with 0 probability $0 \log 0 = 0$.

Theorem 1 *Shannon's noiseless coding Entropy provides a rate of information compression rate.*

Entropy properties:

1. Non-negativity

$$H(X) \geq 0$$

2. Concavity: r.v.

$$X_B \ p_B(x) = q \times p_{x_1} + (1-q) \times p_{x_2}(x)$$
$$H(X_B) \geq qH(X_1) + (1-q)H(X_2)$$

3. Minimal value

$$H(X) = 0 \Leftrightarrow p_X(x) = \delta_{x,x_0}$$

4. Maximal value

$$H(X) \leq \log |\mathcal{X}|$$

Types of entropies

(a) Binary entropy

Source with two outcomes $p(0) = p$, $p(1) = 1 - p$

$$h_2(p) = -p \log p - (1-p)\log(1-p) \ .$$

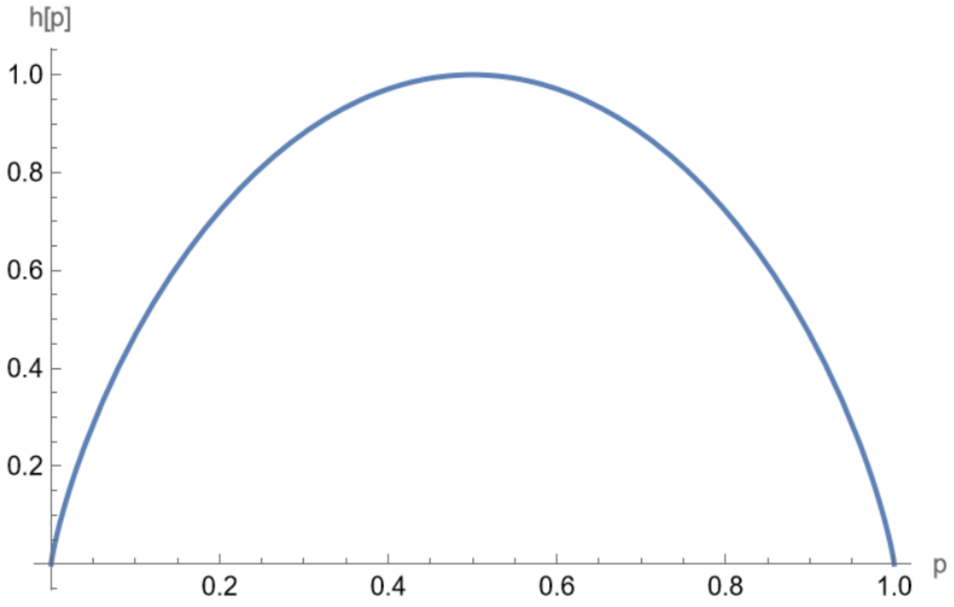

Figure 1.2: Binary entropy

(b) Conditional entropy

Two random variables X,Y. What is the uncertainty of X provided that one knows Y?

$$H(X|Y) = -\sum_{x,y} p_{X,Y}(x,y)\log\big(p_{X|Y}(x|y)\big) \ .$$

One has $H(X) \geq H(X|Y)$.

(c) Joint entropy

Two random variables X,Y. What is the uncertainty of X and Y?

$$H(X,Y) = -\sum_{x,y} p_{X,Y}(x,y)\log(p_{X,Y}(x,y)) \ .$$

(d) Mutual information

Measures correlations between r.v. X and Y, quantifies reduction of uncertainty of X due to dependence of Y on X

$$I(X;Y) \equiv H(X) - H(X|Y) \ .$$

In terms of probability distributions is the following

$$I(X;Y) = -\sum_{x,y} \log \left(\frac{p_{X,Y}(x,y)}{p_X(x) p_Y(y)} \right) .$$

It is symmetric

$$I(X;Y) = I(Y;X) .$$

Quantum information theory

What are quantum counterparts of those quantities? What is their interpretation? Quantum entropy (von Neumann) entropy

$$H(\varrho_A) = -tr(\varrho_A) \log(\varrho_A) .$$

Suppose that the state has eigendecomposition

$$\varrho = \sum_a p_a \left|\psi_a\right\rangle \left\langle a\right| ,$$

then

$$H(\varrho_A) = -\sum_a p_a \log p_a .$$

Quantum entropy has two interpretations: it quantifies uncertainty about the expected information gains in qubits upon receiving and measuring the sent state or it is quantum channel capacity, alternatively. Quantum entropy properties:

1. Non-negativity

$$H(\varrho) \geq 0$$

2. Concavity in density operators.

3. Minimal value

$$H(\varrho) = 0 \Leftrightarrow \varrho = \left|\psi\right\rangle \left\langle\psi\right|$$

4. Maximal value

$$H(\varrho) \leq \log d .$$

Types of quantum entropies

(a) Conditional quantum entropy

$$H(A|B)_\varrho \equiv H(AB)_\varrho - H(B)_\varrho \ ,$$

one has

$$H(A)_\varrho \geq H(A|B)_\varrho \ .$$

(b) Quantum mutual information

$$I(A;B) \equiv H(A)_\varrho + H(B)_\varrho - H(AB)_\varrho \ ,$$

one has

$$I(A;B) = H(A)_\varrho - H(A|B)_\varrho = H(B)_\varrho - H(B|A)_\varrho \ .$$

1.1.4 Quantum correlations: entanglement

Consider a composite quantum system ϱ_{AB} What kind of correlations this state can have?

1. Classical correlations

$$\varrho_{AB} = \sum_{i,j} p_{X,Y}(x_i, y_i) \left| x_i y_i \right\rangle \left\langle x_i y_i \right|$$

2. Quantum correlations: Entanglement

   The state is entangled if it is not separable

$$\left|\psi\right\rangle_{AB} \neq \left|\phi\right\rangle_A \otimes \left|\varphi\right\rangle_B \ .$$

   For mixed states it is the following

$$\varrho_{AB} \neq \sum_i p_i \varrho_A \otimes \varrho_B \ .$$

Example 3 *Entangled states*

- *Bell states*

$$
\begin{aligned}
|\Psi^{\pm}\rangle &= \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle) \ , \\
|\Phi^{\pm}\rangle &= \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle) \ .
\end{aligned}
$$

- *GHZ state*

$$
|GHZ\rangle = \frac{1}{\sqrt{2}}(|000\rangle \pm |111\rangle) \ .
$$

How to check whether the state is entangled?

(a) Peres-Horodecki criterion

Consider a bipartite state

$$
\varrho_{AB} = \sum_{ijkl} = q^{ij}_{kl} \left|i\right\rangle \left\langle j\right|_A \otimes \left|k\right\rangle \left\langle l\right|_B \ ,
$$

one defines partial transpose in the following way

$$
\begin{aligned}
\varrho_{AB}^{T_B} \equiv \sum_{ijkl} &= q^{ij}_{kl} \left|i\right\rangle \left\langle j\right|_A \otimes (\left|k\right\rangle \left\langle l\right|_B)^T \\
&= q^{ij}_{kl} \left|i\right\rangle \left\langle j\right|_A \otimes \left|l\right\rangle \left\langle k\right|_B \\
&= q^{ij}_{lk} \left|i\right\rangle \left\langle j\right|_A \otimes \left|k\right\rangle \left\langle l\right|_B
\end{aligned}
$$

The state is separable if its partial transposition is a quantum state (has non-negative eigenvalues). It is necessary and sufficient in dimension (2,2) and (2,3).

(b) Entanglement witnesses

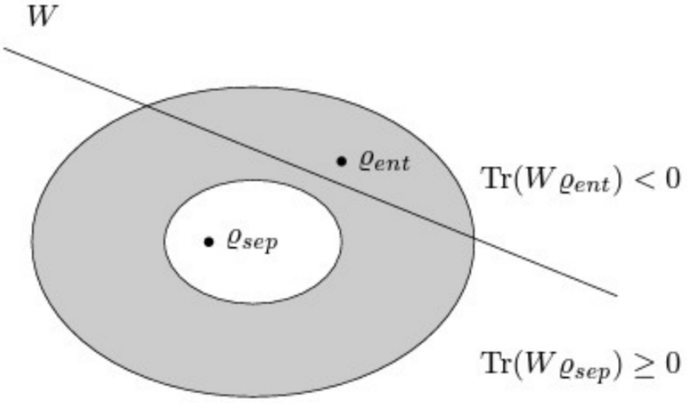
W
ϱ_{ent}
ϱ_{sep}
$\mathrm{Tr}(W\varrho_{ent}) < 0$
$\mathrm{Tr}(W\varrho_{sep}) \geq 0$

Figure 1.3: Entanglement witnesses. [8]

1.1.5 Examples of quantum protocols: Dense coding and teleportation

Dense coding

How to send 2 classical bits using one qubit?

Alice and Bob share a quantum state

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{AB}$$

Alice encoding

$$\begin{aligned} 00 &\longrightarrow |\Psi^+\rangle \\ 01 &\xrightarrow{\sigma_3} |\Phi^+\rangle \\ 10 &\xrightarrow{\sigma_1} |\Psi^-\rangle \\ 11 &\xrightarrow{i\sigma_2} |\Psi^-\rangle \quad , \end{aligned}$$

where

$$\sigma_1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$
$$\sigma_2 = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$
$$\sigma_3 = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \quad .$$

are Pauli matrices. Alice sends her part to Bob, Bob performs measurement

$$00 \longrightarrow |\Psi^+\rangle$$
$$01 \xrightarrow{\sigma_3} |\Phi^+\rangle$$
$$10 \xrightarrow{\sigma_1} |\Psi^-\rangle$$
$$11 \xrightarrow{i\sigma_2} |\Psi^-\rangle \ .$$

Teleportation

Alice wants to communicate unknown quantum state to Bob How to do it? She can measure the state and transfer gained information via classical communication means, but such approach has poor because of no-cloning theorem. Thee is another way: she shares with Bob entangled state. She can move unknown qubit to Bob, erasing it at her site.
Alice qubit state

$$|q\rangle_A = a\,|0\rangle_A + b\,|1\rangle_A$$

Alice and Bob shared state:

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{AB}$$

The total state:

$$\begin{aligned} |\psi\rangle_{AA'B} = \frac{1}{2}[&|\Psi^+\rangle_{AA'}\,(a\,|0\rangle_B + b\,|1\rangle_B) \\ &+ |\Psi^-\rangle_{AA'}\,(a\,|0\rangle_B - b\,|1\rangle_B) \\ &+ |\Phi^+\rangle_{AA'}\,(a\,|1\rangle_B + b\,|0\rangle_B) \\ &+ |\Phi^-\rangle_{AA'}\,(a\,|1\rangle_B - b\,|0\rangle_B)] \end{aligned}$$

Alice measures her total state in the Bell basis obtaining to result corresponding to (correction needed, Alice needs to send measurement result to Bob)

$$\begin{aligned}
&|\Psi^+\rangle_{AA'} \quad \text{Bob state is} \quad a\,|0\rangle_B + b\,|1\rangle_B \\
&|\Psi^-\rangle_{AA'} \quad \text{Bob state is} \quad a\,|0\rangle_B - b\,|1\rangle_B \xrightarrow{\sigma_3} a\,|0\rangle_B + b\,|1\rangle_B \\
&|\Phi^+\rangle_{AA'} \quad \text{Bob state is} \quad a\,|1\rangle_B + b\,|0\rangle_B \xrightarrow{\sigma_1} a\,|0\rangle_B + b\,|1\rangle_B \\
&|\Phi^-\rangle_{AA'} \quad \text{Bob state is} \quad a\,|1\rangle_B - b\,|0\rangle_B \xrightarrow{i\sigma_2} a\,|0\rangle_B + b\,|1\rangle_B \ .
\end{aligned}$$

1.2 Assignments

Assignment 1.2.1

Verify that the map $(x, y) = \sum_i^N x_i, y_i^*$ is an inner product $(x, y \in \mathbb{C}^N)$.

Assignment 1.2.2

Which of the following density operators represents a quantum state?

$$\frac{1}{2}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \frac{1}{2}\begin{bmatrix} 1 & i \\ i & 1 \end{bmatrix}, \frac{1}{2}\begin{bmatrix} 1 & i \\ -i & 1 \end{bmatrix}, \begin{bmatrix} 0.1 & i \\ -i & 0.9 \end{bmatrix}$$

Assignment 1.2.3

Suppose V is a vector space with basis vectors 0 and 1,and A is a linear operator from V to V such that $A|0\rangle = |0\rangle$ and $A|1\rangle = -|1\rangle$.Give a matrix representation for A, with respect to the input basis $|0\rangle, |1\rangle$. Provide the form of that operator in the $|+\rangle, |-\rangle$ basis, where $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.

Assignment 1.2.4

Express Pauli operators in outer product notation.

Assignment 1.2.5

What are possible measurement outcomes and their probabilities when observable σ_Z is measured on the state $|+\rangle$?

Assignment 1.2.6

What are possible measurement outcomes and their probabilities when observable $\sigma_Z \otimes \sigma_Z$ is measured on the state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$?

Assignment 1.2.7

Show that $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ cannot be written as $|a\rangle|b\rangle$ for any qubit states $|a\rangle, |b\rangle$.

Assignment 1.2.8

Consider a state $p|\Psi\rangle\langle\Psi| + (1-p)\frac{I}{4}$, where $|\Psi\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$. Using Peres–Horodecki criterion determine values of p, for which this state is entangled.

Assignment 1.2.9

Define two boxes: The Popescu-Rohrlich box is characterized by the following probability distribution:

$$P^{\mathrm{PR}}(ab \mid xy) = \begin{cases} \frac{1}{2} & a \oplus b = xy \\ 0 & \text{otherwise} \end{cases}$$

where $\oplus$ is addition modulo 2, and perfectly correlated (independent of the inputs) classical box, i.e.

$$P^{c}(ab \mid xy) = \begin{cases} \frac{1}{2} & a \oplus b = 0 \\ 0 & \text{otherwise} \end{cases} \tag{1.1}$$

Consider a box defined as follows:

$$P_{\epsilon}^{\mathrm{PR}} = \epsilon P^{\mathrm{PR}} + (1-\epsilon)P^{\mathrm{c}}$$

- Verify that this box is a proper non-signaling box
- Calculate value of CHSH polynomial given by $E_{00} + E_{01} + E_{10} - E_{11}$, where $E_{xy} = P(a = b \mid xy) - P(a \neq b \mid xy)$ is the correlator for the pair of measurements x, y.

Chapter 2

Quantum Key Distribution (QKD)

2.1 Theory

2.1.1 Threats to classical cryptography by quantum computing

Mathematical problems that are believed to be hard are the main building block of modern cryptography.

Problem 1 (Prime factorization) *Let $N = pq$ for some odd prime numbers p, q which are not know. Find a proper factor of N.*

Problem 2 (Discrete logarithm) *Suppose g is an element of a group G. A number x that satisfies the following equation*

$$g^x = b$$

is called a discrete logarithm of b to the base g. Given g and b, find x.

Both of them can be efficiently solved on quantum computer by algorithms proposed by P.Shor in [15]. It turns out that above problems can be generalised to so called Hidden Supgroup Problem (see [9]).

Problem 3 (Hidden supgroup problem) *Let f be a function from a finitely generated group G to a finite set X such that f is constant on the cosets of a supgroup K, and distinct on each coset. Given a quantum black box for performing the unitary transform $U|g\rangle|h\rangle = |g\rangle|h \oplus f(g)\rangle$, for $g \in G$, $h \in X$, and $\oplus$ an appropriately chosen binary operation on X, find a generating set for K.*

Order-finding, discrete logarithms, and many other problems are instances of this problem. When the group G is abelian, then above problem can be solved effectively on quantum computer by an algorithm similar to Shor's algorithm. This implies that large-scale quantum computer is a real threat to modern protocols like RSA, DH or ECDH.
Attacks against symmetric cryptography also had been considered. For example H.Kuwakado and M.Maorii [10] introduced a quantum algorithm (similar to Simon's algorithm [17]) that can effectively solve so called distinguishing problem.

Problem 4 *(Distinguishing problem) Let V be either the 3-round Feistel cipher with internal permutations (FP) or a random permutation (RP) on $\{0,1\}^{2n}$. Determine whether V is the FP or the RP by making queries to V. Notice that the query to the inverse mapping V^{-1} is not allowed.*

This result is not as spectacular as Shor's result because it does not hack any commonly used cryptographic protocol, but it gives some insights that symmetric protocols have to be reviewed in terms of resistance against quantum computing.

2.1.2 Quantum Key Distribution protocols

The most famous Quantum Key Distribution Protocol is BB84 proposed by H.Bennet and G.Brassard in [3].

Protocol 1 (BB84)

1. *Alice prepares $2n$ qubits, each randomly in one of the four states $|0\rangle, |1\rangle, |+\rangle, |-\rangle$ and sends them along the quantum channel to Bob.*

2. *For each qubit that Bob receives, he chooses at random one of two bases ($\{|0\rangle, |1\rangle\}$ or $\{|+\rangle, |-\rangle\}$) and measures the qubit with respect to that basis.*

3. *Alice tells Bob via classical channel which basis she used for each qubit. They keep the bits where Bob has used the same basis for his measurement as Alice for the preparation. Those n bits are forming the so-called sifted key.*

4. *Alice and Bob choose a subset of the sifted key to estimate the error rate. They do so by announcing publicly the bit values of the subset. If they differ in too many cases, they abort the protocol.*

5. *Finally, Alice and Bob obtain a joint secret key from the remaining bits by performing classical error correction and privacy amplification.*

Roughly speaking, security of the above protocol is based on no-cloning theorem and the observation that whenever Eve conducts a measurement in a wrong basis, she introduces a disturbance which can be detected by Alice and Bob.
Some implementations of the BB84 protocol are vulnerable to so called Photon Splitting Number attack. Due to that, SARG04 protocol has been introduced [14].

Protocol 2 (SARG04)

1. *Alice sends a sequence of* n *signals to Bob. For each signal, Alice randomly chooses one of the four sets* ($\{(|0\rangle, |+\rangle), (|0\rangle, |-\rangle), (|1\rangle, |+\rangle), (|1\rangle, |-\rangle)\}$) *and sends one of the two states in the set to Bob.*

2. *For each signal, Bob performs the polarization measurement using one of the two bases* ($\{|0\rangle, |1\rangle\}$ *or* $\{|+\rangle, |-\rangle\}$) *randomly.*

3. *For each signal, Alice publicly announces the choice of the set from which the state was selected.*

4. *For each signal, Bob compares his measurement outcome to the two states in the set.*

5. *If his measurement outcome is orthogonal to one of the states in the set, then he concludes that the other state has been sent, which is conclusive result. On the other hand, if his measurement outcome is not orthogonal to either of the states in the set, he concludes that is is an inconclusive result. He broadcast if he got the conclusive result or not for each signal.*

6. *Alice randomly chooses some bits as test bits and announces their locations. Bob estimates the bit error rate from the test bits by taking the ratio of the number of incorrect conclusive test bits to the total number of conclusive test bits.*

7. *Alice and Bob retain only the conclusive untested bits.*

8. *They perform bit error correction and privacy amplification on the remaining bit string.*

In this protocol, Alice and Bob do not publicly announce their measurement bases. They only announce which measurement are conclusive and which are not, so even if Eve intercepts and stores some photons, she still does not know how to measure them.

The BB84 protocol uses 4 different states, but H.Bennet's made an observation that using so much states is redundant! So he introduced in [2] a QKD protocol that uses only two non-orthogonal states $|0\rangle$ and $|+\rangle$.

Protocol 3 (B92)

1. *Alice sends a string of photons in a* $|0\rangle$ *or* $|+\rangle$ *state, chosen randomly.* $|0\rangle$ *state will correspond to the bit* 0 *whereas* $|+\rangle$ *state will correspond to the bit* 1*.*
2. *Bob randomly chooses between* $\{|0\rangle, |1\rangle\}$ *and* $\{|+\rangle, |-\rangle\}$ *bases, to measure the polarisation of the received photon.*
3. *If Bob is measuring in the* $\{|0\rangle, |1\rangle\}$*, there are two possible circumstances: if the photon is in the state* $|0\rangle$*, then the measurement outcome will be* $|0\rangle$ *with the probability* 1 *whereas if the incident photon is the state* $|+\rangle$*, then the measurement outcome will be either* $|0\rangle$ *or* $|1\rangle$ *with the probability* 0.5*. Thus, if only the outcome is* $|1\rangle$*, Bob can infer confidently that the state of the photon is* $|+\rangle$*.*
4. *Similar argument will be applicable if Bob is measuring in the diagonal basis, where the measurement outcome* $|-\rangle$ *will indicate that the incident state of the photon is* $|0\rangle$*.*
5. *After the transmission of the string of photons, Bob announces the instances in which the measurement outcome was either* $|1\rangle$ *or* $|-\rangle$ *and the rest are discarded by both of them.*
6. *For the verification of eavesdropping, Bob and Alice publicly share part of the generated random bit string and if the error crosses a tolerable limit, the protocol is aborted. If not, they are now able to generate a secure and symmetric key between them.*

The three protocols above are of the prepare and measure type but in 1991 A.Ekert introduced [7] a QKD protocol that is based on entanglement.

Protocol 4 (E91)

1. *The source centre chooses the EPR pair* $|\Psi_{-}\rangle = 1/\sqrt{2}(|01\rangle + |10\rangle)$*, sends the first particle to Alice and second particle to Bob.*

2. *Alice makes measurement with a basis randomly chosen between* $\{\sigma_z, \sigma_x, \frac{\sigma_x+\sigma_z}{\sqrt{2}}\}$ *whereas Bob makes a measurement with a basis randomly chosen between* $\{\sigma_x, \frac{\sigma_z-\sigma_x}{\sqrt{2}}, \frac{\sigma_x+\sigma_z}{\sqrt{2}}\}$*. They record the measurement results and broadcast the measurement basis which they used, through the classical channel.*

3. *They divide the measurements results into two groups - one is the test qubits* G_1 *where they chose* $\{\sigma_x, \sigma_z\}$ *(Alice's bases) and* $\{\frac{\sigma_x+\sigma_z}{\sqrt{2}}, \frac{\sigma_z-\sigma_x}{\sqrt{2}}\}$ *(Bob's bases). Second group* G_2 *consists of qubits where they chose the same measurement bases.*

4. *The group* G_1 *is used to calculate if* $CHSH$ *inequality is violated. If* $CHSH \ll 2\sqrt{2}$ *they abort the protocol. If* $CHSH \approx 2\sqrt{2}$ *then the measurements outcomes of qubits from* G_2 *group are a raw key.*

5. *They perform bit error correction and privacy amplification on the raw key.*

Whenever Alice and Bob measure the value $S \approx 2\sqrt{2}$, they can be sure to share a maximally entangled state and that the secret key obtained from measurement is random and did not exist before the measurement.

2.1.3 Security of the BB84 protocol

Generally proving security of a particular protocol is a hard task, because the proof has to take into account every possible type of attack. Much easier approach is to start with something which is secure and then reduce it to the desired protocol without loss of security. Using that approach P.Shor and J.Preskill proved the security of the BB84 protocol [16].

They start with the entanglement based QKD protocol in which EPR pairs are securely distributed from Alice to Bob and the secret key is generated from measuring them. In the first modification EPR pairs are replaced with states encoded in randomly selected $CSS_{z,x}(C_1, C_2)$ code, which are defined as follows.

Definition 1 *Suppose* C_1 *and* C_2 *are* $[n, k_1]$ *and* $[n, k_2]$ *are classical linear codes such that* $C_2 \subset C_1$ *and* $C_1, C_2^{\perp}$ *both correct* t *errors. We define quantum states* $|x + C_2\rangle$ *as*

$$|x + C_2\rangle := \frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} |x + y\rangle.$$

A vector space spanned by the above vectors is called $CSS(C_1, C_2)$ *code (CSS acronym refers to Calderbank-Shor-Steane). It is a quantum* $[n, k_1 - k_2]$ *code correcting errors on up to* t *qubits.*

We consider a family parameterized by bit strings z, x equivalent to $CSS(C_1, C_2)$, which we denote as $CSS(C_1, C_2)_{z,x}$. Codewords in $CSS(C_1, C_2)_{z,x}$ have the following form

$$|\xi_{v_k,z,x}\rangle = \frac{1}{\sqrt{|C_2|}} \sum_{w \in C_2} (-1)^{z \cdot w} |v_k + w + x\rangle.$$

After the first modification the secure QKD protocol is obtained. But this protocol requires quantum memory and usage of quantum computer which is not desired. The second modification of the protocol allows Bob to measure his qubit instantly after receiving them and also allows to not to take into account phase errors in used CSS codes. After few minor technical modifications the protocol is reduced to BB84 without loss of security.

It is strongly recommended to go through the proof following section 12.6.5 from [11] which explains it with details.

Reader interested more in quantum error correcting codes and CSS codes in particular should go through section 10.4.2 from [11].

2.1.4 Bounds on key rate

Problem 5 *How to obtain a secret key from a cqq-state*

$$\rho^{ABE} = \sum_{x \in \mathcal{X}} P(x) |x\rangle\langle x|^A \otimes \rho_x^{BE}$$

using local quantum operations and one-way classical communication? How much key can we obtain?

At first we will consider an asymptotic case, namely we will take n-copies of cqq-states

$$(\rho^{ABE})^{\otimes n} = \sum_{x^n} P(x^n) |x^n\rangle\langle x^n|^A \otimes \rho_{x^n}^{BE}.$$

We want to quantify the answer for above question but to do that we need few definitions.

Definition 2 *A one-way key distillation protocol consist of*

- *A channel T, such that $x^n \xrightarrow{T} (\ell, m)$ where $\ell \in \{1, \ldots, L\}$ (steering variable) and $m \in \{1, \ldots, M\}$ (possible values of key).*
- *A family of POVMs $D^{(\ell)} = (D_m^{(\ell)})_{m=1}^M$ on Bob side parameterized by ℓ.*

It is called (n, ε)-protocol if

- *$P(K_A \neq K_B) \leqslant \varepsilon$.*

- *$\| \sum_{m=0}^{M-1} P(K=m)|m\rangle\langle m| - \frac{1}{M}\sum_{m=0}^{M-1}|m\rangle\langle m|\|_1 \leqslant \varepsilon$.*

- *There is a state σ_0 such that for all m*
  $\| \sum_{x^n,\ell} P(X^n = x^n, \Lambda = \ell | K = m)|\ell\rangle\langle\ell| \otimes \rho^E_{x^n} - \sigma_0\|_1 \leqslant \varepsilon$.

Definition 3 *We call R an achievable rate if for all n there exist (n,ε)-protocol with $\varepsilon \to 0$ and $1/n \log M \to R$ as $n \to \infty$.*

We define the one-way secret key capacity of a cqq-state ρ as

$$K_{\rightarrow}(\rho) := \sup\{R : R \textit{ achievable}\}.$$

Lower bound for one-way secret key capacity of a cqq-state was proved by I.Devetak and A.Winter in [6].

Theorem 1 *For every cqq-state ρ,*

$$K_{\rightarrow}(\rho) \geqslant I(A:B) - I(A:E).$$

They proved above theorem by introducing particular protocol of secret key distillation.

There are also bounds for one-shot case, which means that only one copy of a state can be used. One-shot lower and upper bounds on secret key rates has been proved by J.Renes and R.Renner in [12]. To formulate their theorem, definition of smoothed min- and max-entropies is needed.

Definition 4 *Let $\rho = \rho_{AB}$ be a bipartite density operator. The min-entropy of A conditioned on B is defined by*

$$H_{min}(A|B)_\rho := -\inf_{\sigma_B} D_\infty(\rho_{AB} \| Id_A \otimes \sigma_B)$$

where the infimum ranges over all normalized density operators σ_B on subsystem B and where

$$D_\infty(\tau\|\tau') := \inf\{\lambda \in \mathbb{R} : \tau \leqslant 2^\lambda \tau'\}.$$

Definition 5 *Let $\rho = \rho_{AB}$ be a bipartite density operator. The max-entropy of A conditioned on B is defined by*

$$H_{max}(A|B)_\rho := \sup_{\sigma_B} 2\log F(\rho^{AB}, Id^A \otimes \sigma_B),$$

where the supremum is over positive, normalized states σ_B and $F(\rho,\sigma) := \|\sqrt{\rho}\sqrt{\sigma}\|_1$ is the fidelity of ρ and σ.

Definition 6 *Let $\rho = \rho_{AB}$ be a bipartite density operator $\varepsilon \geqslant 0$. The ε-smooth min- and max-entropy of A conditioned on B are given by*

$$H^{\varepsilon}_{min}(A|B)_{\rho} := \sup_{\rho'} H_{min}(A|B)_{\rho'},$$
$$H^{\varepsilon}_{max}(A|B)_{\rho} := \inf_{\rho'} H_{max}(A|B)_{\rho'},$$

where the supremum ranges over all density operators $\rho' = \rho'_{AB}$ which are ε-close to ρ.

With above definitions we can finally formulate Renner-Renes bounds on one-shot secret key rate.

Theorem 2 *Given any $\varepsilon \geqslant 0$ and a state $\psi^{ABE} = \sum_x p_x|x\rangle\langle x|^A \otimes \varphi_x^{BE}$ and $\varepsilon = \varepsilon_1 + \varepsilon_2$, $\varepsilon' = \varepsilon_1' + \varepsilon_2$,*

$$\begin{aligned}
&\ell^{\varepsilon+\varepsilon'}_{secr}(A;B|E)_{\psi} \geqslant \sup_{(U,V)\leftarrow A}\left[H^{\varepsilon_1'}_{min}(U|EV)_{\psi} - H^{\varepsilon_1}_{max}(U|BV)_{\psi}\right]\\
&-4\log\frac{1}{\varepsilon_2} - 3\\
&\ell^{\varepsilon}_{secr}(A;B|E)_{\psi} \leqslant \sup_{(U,V)\leftarrow A}\left[H^{\sqrt{2\varepsilon}}_{min}(U|EV)_{\psi} - H^{\sqrt{2\varepsilon}}_{max}(U|BV)_{\psi}\right].
\end{aligned}$$

2.2 Assignments

Assignment 2.2.1

Fill the tables for BB84, B92 and SARG04 protocols. In this exercises H denotes $\{|0\rangle, |1\rangle\}$ basis and D denotes $\{|+\rangle, |-\rangle\}$ basis.

BB84:

Alice bits	0	1	1	0	1	1	0	0
Alice basis	H	H	D	H	D	D	D	H
Alice qubits	$\|0\rangle$	$\|1\rangle$	$\|-\rangle$	$\|0\rangle$	$\|-\rangle$	$\|-\rangle$	$\|+\rangle$	$\|0\rangle$
Bob basis	H	D	H	H	D	D	H	H
Bob qubits	$\|0\rangle$	$\|+\rangle$	$\|1\rangle$	$\|0\rangle$	$\|-\rangle$	$\|-\rangle$	$\|1\rangle$	$\|0\rangle$
Bob bits								
Final key								

B92:

Alice bits	1	0	0	1	0	0	1	1
Alice qubits	$\|+\rangle$	$\|0\rangle$	$\|0\rangle$	$\|+\rangle$	$\|0\rangle$	$\|0\rangle$	$\|+\rangle$	$\|+\rangle$
Bob basis	H	D	H	H	D	D	H	H
Bob qubits	$\|1\rangle$	$\|+\rangle$	$\|0\rangle$	$\|0\rangle$	$\|-\rangle$	$\|-\rangle$	$\|1\rangle$	$\|0\rangle$
Bob bits								
Final key								

SARG04:

Alice bits	0	1	1	0	1	1	0	0
Alice qubits	$\|0\rangle$	$\|+\rangle$	$\|-\rangle$	$\|1\rangle$	$\|+\rangle$	$\|-\rangle$	$\|0\rangle$	$\|1\rangle$
Bob basis	H	H	H	D	D	H	H	D
Bob qubits	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$	$\|-\rangle$	$\|+\rangle$	$\|1\rangle$	$\|0\rangle$	$\|+\rangle$
Alice classical information	$\|0\rangle$, $\|+\rangle$	$\|0\rangle$, $\|+\rangle$	$\|0\rangle$, $\|-\rangle$	$\|1\rangle$, $\|+\rangle$	$\|1\rangle$, $\|+\rangle$	$\|1\rangle$, $\|-\rangle$	$\|0\rangle$, $\|-\rangle$	$\|1\rangle$, $\|-\rangle$
Bob bits								
Final key								

Assignment 2.2.2

Suppose that Eve conducts naive intercept-resend attack on the BB84 protocol. What is the probability the her attack won't be detected?

Assignment 2.2.3

Suppose that Eve conducts naive intercept-resend attack on the B92 protocol. What is the probability the her attack won't be detected?

Assignment 2.2.4

Suppose that Alice uses a basis $\{\sin\theta|0\rangle+\cos\theta|1\rangle, \sin\big(\theta+\frac{\pi}{2}\big)|0\rangle+\cos\big(\theta+\frac{\pi}{2}\big)|1\rangle\}$ for some angle θ instead of $\{|+\rangle, |-\rangle\}$ in the BB84 protocol. Show that the probability that Eve's attack will be detected is now

$$p = \frac{1}{4}\sin^2(2\theta).$$

What angle maximizes this probability?

Assignment 2.2.5

Using the measurement directions of the E91 protocol, show that CHSH inequality is violated when Alice and Bob share a singlet state $|\Psi_-\rangle = 1/\sqrt{2}(|01\rangle + |10\rangle)$. Adding white noise to the projector onto the singlet, what is the maximal proportion of noise that still leads to a violation of the CHSH inequality?

Observables used in E91 protocol: $A_1 = \sigma_z$, $A_2 = \sigma_x$, $B_1 = \frac{\sigma_z+\sigma_x}{\sqrt{2}}$, $B_2 = \frac{\sigma_z-\sigma_x}{\sqrt{2}}$.

$S := |\langle A_1, B_1\rangle + \langle A_1, B_2\rangle + \langle A_2, B_1\rangle - \langle A_2, B_2\rangle|$

Assignment 2.2.6

Show that the code defined by

$$|x + C_2\rangle = \frac{1}{\sqrt{|C_2|}}\sum_{y\in C_2}(-1)^{u\cdot y}|x + y + v\rangle$$

and parameterized by u and v are equivalent to $CSS(C_1, C_2)$ in the sense that they have the same error-correcting properties.

Assignment 2.2.7

Determine the subsystems of a state

$$\rho = p|\Phi_+\rangle\langle\Phi_+|_{AB} + \frac{1-p}{4} Id_{AB},$$

where $|\Phi_+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and calculate von Neumann entropies $S(A)$ and $S(B)$.

Assignment 2.2.8

Calculate mutual information for the following state

$$|\phi\rangle_{AB} = \frac{1}{\sqrt{2}}|00\rangle_{AB} + \frac{1}{2}|01\rangle_{AB} + \frac{1}{2}|11\rangle_{AB}.$$

Hint: Write down a density matrix and determine states of subsystems using explicit formulas for partial trace.

Assignment 2.2.9

Calculate the Devetak-Winter lower bound for one-way secret key capacity of the following states:

1. $\rho_{ABE} = \left[\frac{1}{N}\sum_{i=0}^{N} |i\rangle\langle i|_A \otimes |i\rangle\langle i|_B\right] \otimes \rho_E$,
2. $\rho_{ABE} = \frac{1}{9}|0\rangle\langle 0|_A \otimes |0\rangle\langle 0|_B \otimes |1\rangle\langle 1|_E + \frac{4}{9}|1\rangle\langle 1|_A \otimes |1\rangle\langle 1|_B \otimes |0\rangle\langle 0|_E + \frac{4}{9}|2\rangle\langle 2|_A \otimes |2\rangle\langle 2|_B \otimes |0\rangle\langle 0|_E$,
3. $\rho_{ABE} = \frac{1}{N}\sum_{i=0}^{N} |i\rangle\langle i|_A \otimes |i\rangle\langle i|_B \otimes |i+1 \mod N\rangle\langle i+1 \mod N|_E$.
   Hint: Note that the state $|i+1 \mod N\rangle\langle i+1 \mod N|_E$ can be obtained from $|i\rangle\langle i|_E$ by applying a local unitary transform.

Assignment 2.2.10

Show that if ρ_{AB} is a product state $\rho_{AB} = \rho_A \otimes \rho_B$, then:

$$H_{min}(A|B)_\rho = -\log_2 \|\rho_A\|_\infty,$$

where $\|\rho_A\|_\infty$ is a norm of the greatest eigenvalue of ρ_A.

Assignment 2.2.11

Show that if ρ_{AB} is a pure state, then:

$$H_{min}(A|B)_\rho = -2\log_2 \mathrm{Tr}\sqrt{\rho_A}.$$

Assignment 2.2.12

Show that

$$H^{\varepsilon}_{max}(A|B)_{\rho} = -H^{\varepsilon}_{min}(A|C)_{\rho}$$

for a purification ρ_{ABC} of a state ρ_{AB}.

Hint: min- and max-entropy are dual in the sense that

$$H_{max}(A|B)_{\rho} = -H_{min}(A|C)_{\rho}$$

for a pure state ρ^{ABC}.

Assignment 2.2.13

To calculate mutual information $I(A:B)$ of a state $\rho_{AB} = p|\Phi_{+}\rangle\langle\Phi_{+}|_{AB} + \frac{1-p}{4}Id_{AB}$, one has to calculate von Neumann entropy of the whole state. Calculate it.

Assignment 2.2.14

Using the definition of codewords in CSS codes, show that $|x + C_2\rangle = |x' + C_2\rangle$ if and only if $x - x' \in C_2$.

Assignment 2.2.15

Show that if ρ_{AB} is a product state $\rho_{AB} = \rho_A \otimes \rho_B$, then:

$$H_{max}(A|B)_{\rho} = 2\log_2 \mathrm{Tr}\sqrt{\rho_A}.$$

Assignment 2.2.16

Show that if ρ_{AB} is a pure state, then:

$$H_{max}(A|B)_{\rho} = \log_2 \|\rho_A\|_{\infty},$$

where $\|\rho_A\|_{\infty}$ is a norm of the greatest eigenvalue of ρ_A.

Hint

Explicit formulas for partial trace for 2-qubit system. Let

$$\rho_{AB} = \begin{bmatrix} a & b & c & d \\ e & f & g & h \\ i & j & k & l \\ m & n & o & p \end{bmatrix}.$$

Then

$$\rho_A = \operatorname{Tr}_B \rho_{AB} = \begin{bmatrix} a+f & c+h \\ i+n & k+p \end{bmatrix}$$

$$\rho_B = \operatorname{Tr}_A \rho_{AB} = \begin{bmatrix} a+k & b+l \\ e+o & f+p \end{bmatrix}.$$

Hint

Observe that density matrix of a state $p|\Phi_+\rangle\langle\Phi_+|_{AB} + \frac{1-p}{4} Id_{AB}$ is

$$\begin{bmatrix} \frac{p+1}{4} & 0 & 0 & \frac{p}{2} \\ 0 & \frac{1-p}{4} & 0 & 0 \\ 0 & 0 & \frac{1-p}{4} & 0 \\ \frac{p}{2} & 0 & 0 & \frac{p+1}{4} \end{bmatrix}.$$

Observe also that calculating eigenvalues of above matrix is equivalent to calculating eigenvalues of the following two matrices

$$\begin{bmatrix} \frac{p+1}{4} & \frac{p}{2} \\ \frac{p}{2} & \frac{p+1}{4} \end{bmatrix} \text{ and } \begin{bmatrix} \frac{1-p}{4} & 0 \\ 0 & \frac{1-p}{4} \end{bmatrix}.$$

Chapter 3

Device Independent (DI) and Semi-Device Independent QKD

3.1 Theory

3.1.1 Introduction

Story so far

- Classical cryptography based on the limitations on the adversary's computational capability!
- Quantum Cryptography provides a solution!
- Quantum Cryptography provide security based only on laws to physics!
- Quantum processes are not visible to the naked eye, need to trust the devices!
- Solution: Device Independent Quantum Cryptography, the strongest form of security known to mankind!

- Classical cryptography based on the limitations on the adversary's computational capability!
- Quantum Cryptography provides a solution!
- Quantum Cryptography provide security based only on laws to physics!
- Quantum processes are not visible to the naked eye, need to trust the devices!

- Solution: Device Independent Quantum Cryptography, the strongest form of security known to mankind!

  It is either AI or DI!Device Independent Outlook On Physics

Device independent outlook on physics

Quantum Mechanics:

- The flagship physical theory!
- Deeply mysterious!
- All set to fuel the key technological advances of the twenty-first century!
- The most precisely tested theory in the history of science!
- The universe we inhabit is governed by the laws of quantum mechanics!

  A seemingly ridiculous request: Forget, or at least suspend all what you have learnt about Quantum Mechanics!

A first principles approach

- **No assumptions** about the internal working of the device
- Instead of characterising a device by its hardware, we treat it like a **black box**!
- The black boxes have some buttons!
- The user can press these buttons and get some outputs!
- **Goal:** To characterise the device based solely on empirical input-output statistics! A first principles approach

- No assumptions about the internal working of the device
- Instead of characterising a device by its hardware, we treat it like a black box!
- The black boxes have some buttons!
- The user can press these buttons and get some outputs!
- Goal: To characterise the device based solely on empirical input-output statistics!

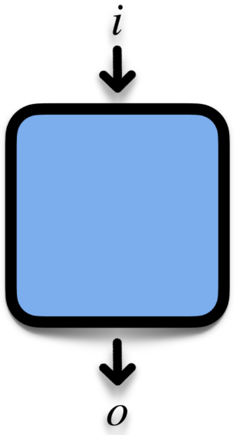

Figure 3.1: Black box

3.1.2 Characterising Black Boxes

- The input-output behaviour of a black box is described by a conditional probability distribution $p_{O|I}$, which specifies the probability of obtaining an outcome $O = o$ when the input selected by the user was $I = i$!

- Must satisfy:

  positivity: $p(O = o|I = i) \geq 0, \forall i, o$

  completeness: $\sum_o p(O = o|I = i) = 1, \forall i$

- Examples: Let O be a random variable over the set $o \in \{0, 1\}$ and I be a random variable over the set $i \in 0, 1$

  White-Noise (WN) Box: $p(O = o|I = i) = \frac{1}{2},\ \forall i, o$

  Deterministic (D) Box: $p(O = o|I = i) \in 0, 1,\ \forall i, o$

Bipartite Black Boxes

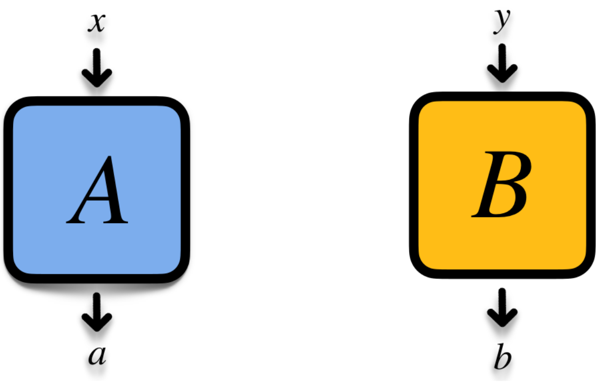

Figure 3.2: Bipartie black box

- Alice and Bob each have access to one part of a bipartite box

- Relevant to QKD protocols

- The two parts of the bipartite box are **separated in space**, i.e., Alice and Bob each have access to their part of the box but cannot access the other party's box!

- Without making any assumptions about the inner workings of the boxes, Alice and Bob input x, y to retrieve outputs a, b. This yields in the input-output statistics of the box!

- The boxes are completely described by the conditional probability distribution $p_{AB|XY}$, where $X(Y)$ and $A(B)$ are random variables describing Alice's (Bob's) input and output, respectively.

- In general, there are no restrictions on $p_{AB|XY}(a, b|x, y)$, except:
positivity: $p(a, b|x, y) \geq 0 \ \forall a, b, x, y$ and
completeness: $p(a, b|x, y) = 1$, $\forall x, y$.

Bell scenarios

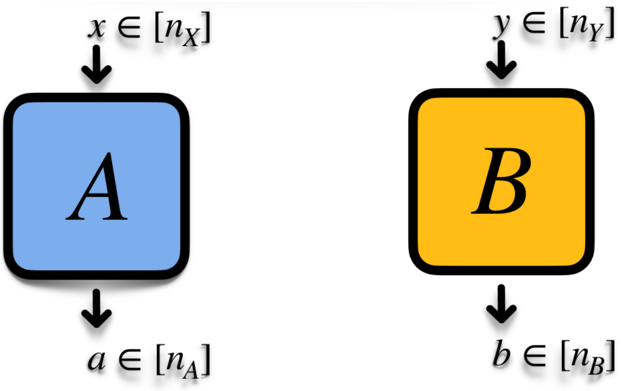

Figure 3.3: Bell scenarios

- We use $[n_D]$ to denote the set $\{0, \ldots, d-1\}$

- A bipartite Bell scenario is a tuple (n_X, n_Y, n_A, n_B) specifying the inputs and outputs of Alice and Bob!

- The $(2, 2, 2, 2)$ Bell scenario is the famous CHSH scenario!

- The $(3, 2, 2, 2)$ Bell scenario is the Bell scenario for Ekert-like DIQKD protocols!

The no-signalling conditions

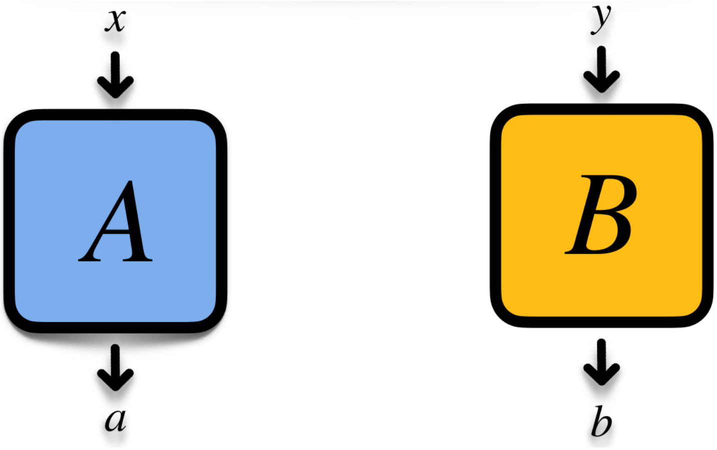

Figure 3.4: The no-signalling conditions

- The no-signaling conditions translate to the requirement that the individual components of the boxes produce an output independently of the other component, i.e., Alice's (Bob's) output should be independent of Bob's (Alice's) input.

- Alternatively, the no-signaling conditions are the requirement that the marginal probability distributions $p_{A|X}, p_{B|Y}$ are well-defined probability distributions!

Alice to Bob no-signalling condition

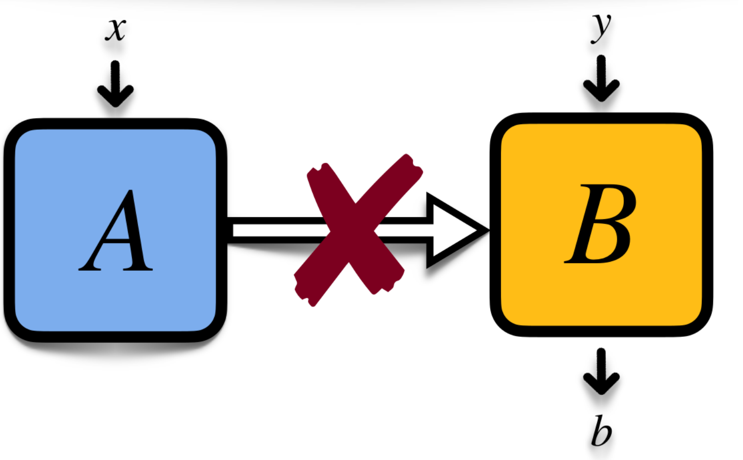

Figure 3.5: Alice to Bob no-signalling condition

- Bob looking at the statistics $p_{B|Y}$ produced by his part of the bipartite box should not be able to infer anything about Alice's input, i.e.,

$$\forall b, y, x, x^{'} \;\; p(b|y) = p(b|x, y) = \sum_a p(a, b|x, y) = p(b|x^{'}, y) = \sum_a p(a, b|x^{'}, y)$$

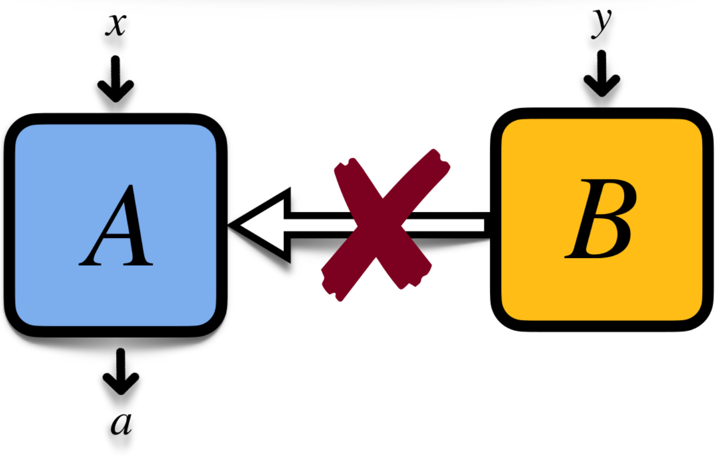

Figure 3.6: Bob to Alice no-signalling condition

Bob to Alice no-signalling condition

- Alice looking at the statistics $p_{A|Y}$ produced by his part of the bipartite box should not be able to infer anything about Alice's input, i.e.,

$$\forall a, y, x, x^{'} \; p(a|x) = p(a|x, y) = \sum_b p(a, b|x, y) = p(a|x, y^{'}) = \sum_b p(a, b|x, y^{'})$$

No-signalling polytope($\mathcal{NS}$)

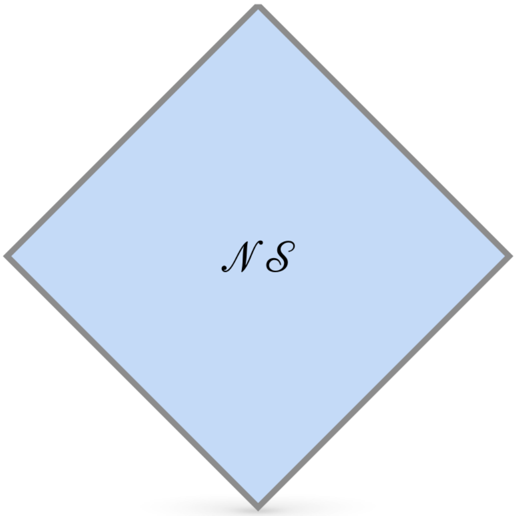

Figure 3.7: As the positivity, completeness and the no-singalling conditions constitute linear constraints on some real number $\{p(a, b|x, y)\}$, the set of boxes which satisfy the no-signalling conditions forms a convex polytope, i.e., a convex set with inite number of extremal points.

Hidden variable (classical) explantions

Let Alice and Bob share classical random variable Λ distributed according to a probability

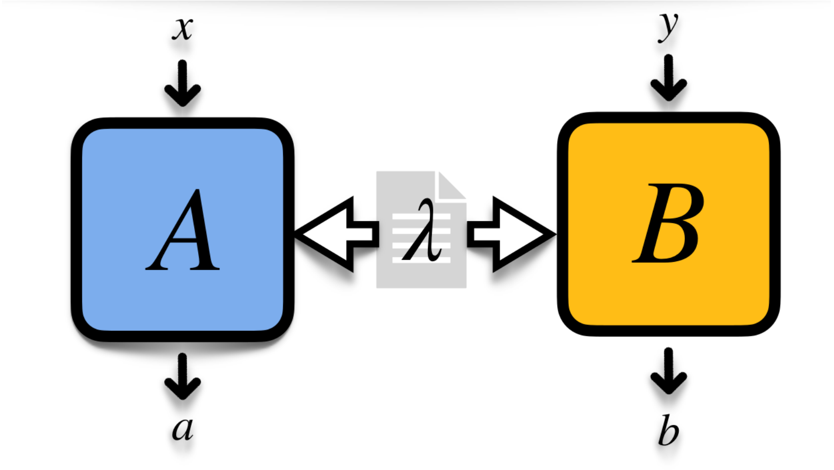

Figure 3.8: Hidden variable (classical) explantions.

distribution p_Λ , such that, it explains the statistics of their boxes,

$$p(a,b|x,y) = \sum_\lambda p(\lambda)p(a,b|x,y,\lambda)$$

- Parameter Independence (PI)

  Parameter independence or no-signalling at the Λ-level requires the distribution to remain no-signalling even when one has access to the hidden variable Λ , such that,

$$\forall b, y, x, x^{'}, \lambda$$
$$p(b|y,\lambda) = p(b|x,y,\lambda) = \sum_a p(a,b|x,y,\lambda) = p(b|x^{'},y,\lambda) = \sum_a p(a,b|x^{'},y,\lambda)$$

and

$$\forall a, x, y, y^{'}, \lambda$$
$$p(a|x,\lambda) = p(a|x,y,\lambda) = \sum_b p(a,b|x,y,\lambda) = p(a|x,y^{'},\lambda) = \sum_b p(a,b|x,y^{'},\lambda) \ .$$

- Outcome Independence (OI)

  Outcome independence (OI) requires Bob's (Alice's) outcome to be independent of Alice's (Bob's) outcome when condition on the inputs x, y , and the hidden variable λ , such that, a, b, x, y, λ,

$$p(a|x,y,b,\lambda) = p(a|x,y,\lambda)$$
$$p(b|x,y,a,\lambda) = p(b|x,y,\lambda) \ .$$

Local Hidden Variable (LHV) explantions

Local Hidden Variable (LHV) explanations are hidden variable explanations which satisfy parameter independence and outcome independence,

$$LHV \equiv PI \wedge OI$$

Recall that, a hidden variable explanation of box implies that,

$$p(a, b|x, y) = \sum_{\lambda} p(\lambda) p(a, b|x, y, \lambda),$$

using Bayes' Theorem,

$$p(a, b|x, y) = \sum_{\lambda} p(\lambda) p(a|x, y, b, \lambda) p(b|x, y, \lambda),$$

next, using OI

$$p(a, b|x, y) = \sum_{\lambda} p(\lambda) p(a|x, y, \lambda) p(b|x, y, \lambda),$$

finally, using PI , we arrive the well-known definition of LHV explanations,

$$p(a, b|x, y) = \sum_{\lambda} p(\lambda) p(a|x, \lambda) p(b|y, \lambda) \ .$$

Local (classical) boxes and deterministic resolution

In a Bell scenario (n_X, n_Y, n_A, n_B) the total number of deterministic boxes for Alice is $(n_X)^{n_A}$, for Bob is $(n_Y)^{n_B}$.

Total number of deterministic bipartite is $(n_X)^{n_A}(n_Y)^{n_B}$.

Definition 3 *Characterization of local behaviours*

A Box $p_{AB|XY}$ is local if and only if it is a convex mixture of local deterministic processes,

$$p(a, b|x, y) = \sum_{j} (n_X)^{n_A} \sum_{k} (n_Y)^{n_B} q_{j,k} \delta_{a=f_i(x)} \delta_{b=g_k(y)} \ ,$$

$$\textit{with } \lambda \equiv (j, k),\ q_{j,k} \geq 0,\ \forall j, k\ \sum_{j,k} q_{j,k} = 1 \ .$$

The local polytope ($\mathcal{L}$)

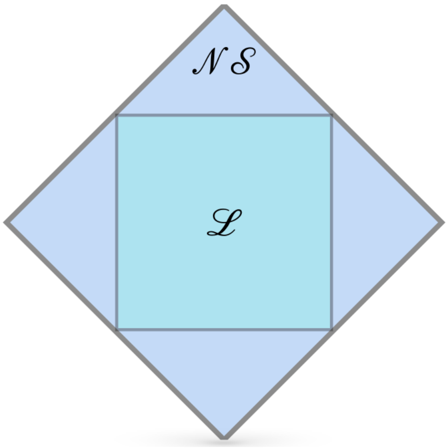

Figure 3.9: The set of all local boxes forms a convex polytope with $(n_X)^{n_A}(n_Y)^{n_B}$ deterministic boxes as extremal points! Because of PI , the local polytope is a subset of the no-signalling polytope $\mathcal{L} \subseteq \mathcal{NL}$.

Nonlocal boxes

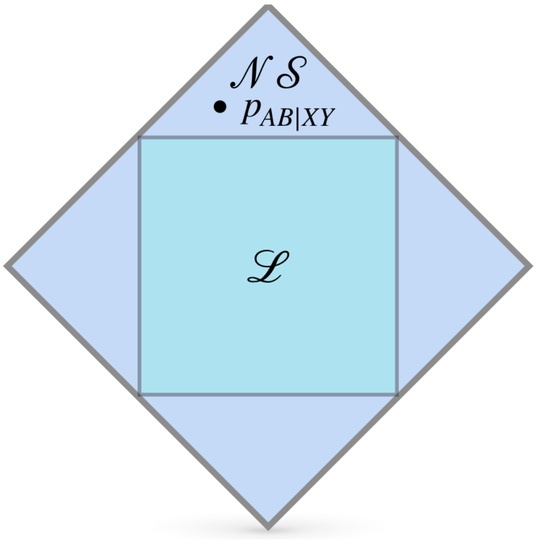

Figure 3.10: No signalling boxes that lie outside local polytope, are referred as nonlocal boxes!.A nonlocal box $p_{AB|XY} \in \mathcal{NS} \backslash \mathcal{L}$.

3.1.3 Bell inequalities

The notion of Bell inequalities

A criterion that separates some nonlocal box from all local boxes is generically called Bell inequality. Usually one considers linear Bell inequalities, i.e., criteria of the form,

$$I(p_{AB|XY}) = \sum_{a,b,x,y} \nu_{a,b,x,y} p(a,b|x,y) \leq I_{\mathcal{L}}$$

The functional $I(p_{AB|XY})$ is called the Bell functional and I_L is called the local bound of Bell functional! $I(pAB|XY) > I_{\mathcal{L}}$ implies that $p_{AB|XY} \in \mathcal{NS} \backslash \mathcal{L}$!

Tight Bell inequalities

- The most natural candidates for Bell inequalities are facets of the local polytope!
- Their number is inite, hence, it is in principle possible to list them all out!
- The non-trivial facets of the local polytope are called tight Bell inequalities!

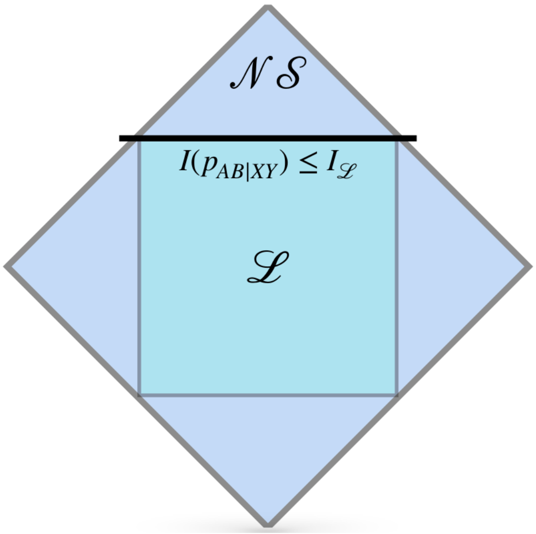

Figure 3.11: Tight Bell inequalities

Do not underestimate LHV explanations!

LHV models have enormous explanatory potential,

- The behaviour $p_{A|X}$ of one player can always be reproduced with LHV!
- LHV models can explain the behaviour presented in popular for as an astonishing feat of quantum entanglement, namely, two players always produce the same outcome when queried with the same input!

- LHV models can explain all bipartite behaviours in Bell scenarios wherein one of the parities has only one inputs, i.e., Bell scenarios of the form $(1, n_Y, n_A, n_B)$ and $(n_X, 1, n_A, n_B)$.

Simplest nontrivial Bell scenario: CHSH scenario

- The simplest Bell scenario where in $\mathcal{L} \subset \mathcal{NS}$ is $(2, 2, 2, 2)$, referred to as the Clauser-Horne-Shimony-Holt (CHSH) scenario!

- In this scenario, the no-signaling polytope is embedded in $\mathbb{R}^8$!

- The local polytope in the CHSH scenario has 16 extremal points!

- The local polytope in the CHSH scenario has 24 facets!

- 16 trivial positivity facets!

- 8 non trivial facets, all equivalent up to relabelling to celebrated Clauser-Horne-Shimony-Holt (CHSH) Bell inequality,

$$S = S(p_{AB|XY}) = \langle A_0 B_0 \rangle + \langle A_0 B_1 \rangle + \langle A_1 B_0 \rangle - \langle A_1 B_1 \rangle \leq 2$$

where

$$\langle A_x B_y \rangle = \sum_{a,b} (-1)^{a \otimes b} p(a, b|x, y) \ .$$

3.1.4 Nonlocal games and quantum boxes

Nonlocal games

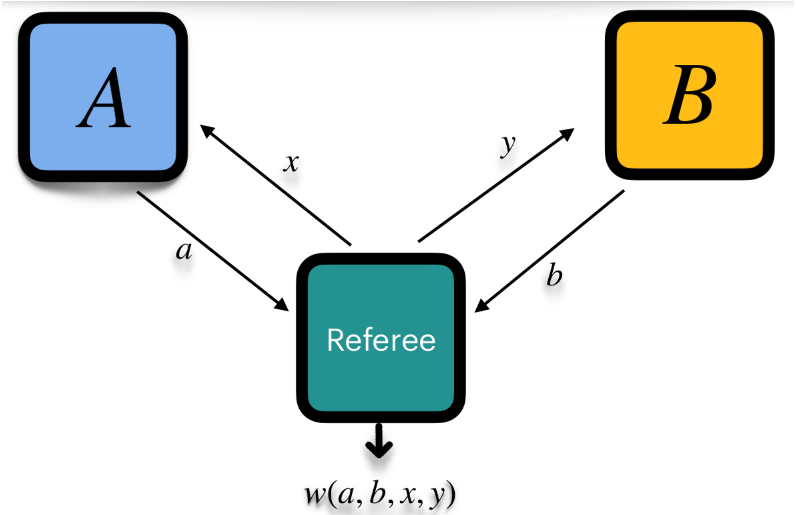

Figure 3.12: Nonlocal games

- Bell inequalities can also be phrased as nonlocal games!
- The Referee sends questions x, y to Alice and Bob respectively, based on priors q_{XY} , and decides according to their answer a, b whether they have won $(w(a, b, x, y) = 1)$ or lost $(w(a, b, x, y) = 0)$ the game.
- The winning probability for a given box $p_{AB|XY}$ is,

$$\omega(p_{AB|XY}) = \sum_{a,b,x,y} q(x, y)w(a, b, x, y)p(a, b|x, y) \leq \omega_{\mathcal{L}} \ .$$

Quantum boxes

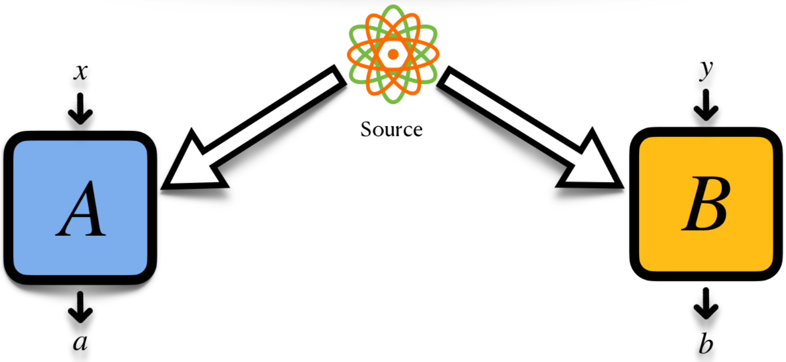

Figure 3.13: Quantum boxes

- Note that even though we assume that the bipartite box is quantum, we do not make assumptions on the internal workings of the box!
- The assumption that there is a bipartite state $\rho_{AB} \in B_+(\mathcal{H}_A \otimes \mathcal{H}_B)$ is no limitation since we do not restrict the dimension of the Hilbert spaces!

The set of quantum boxes

- Given a Bell scenario, the quantum set $\mathcal{Q}$ is defined as the set of all quantum boxes!
- The quantum set $\mathcal{Q}$ is convex, but does not form a polytope!
- Characterising $\mathcal{Q}$ is extremely difficult!

Maximal violation of the CHSH inequality

- The celebrated Clauser-Horne-Shimony-Holt (CHSH) Bell inequality,

$$S = S(p_{AB|XY}) = \langle A_0 B_0 \rangle + \langle A_0 B_1 \rangle + \langle A_1 B_0 \rangle - \langle A_1 B_1 \rangle \leq 2$$

where

$$\langle A_x B_y \rangle = \sum_{a,b} (-1)^{a \otimes b} p(a, b|x, y) \ .$$

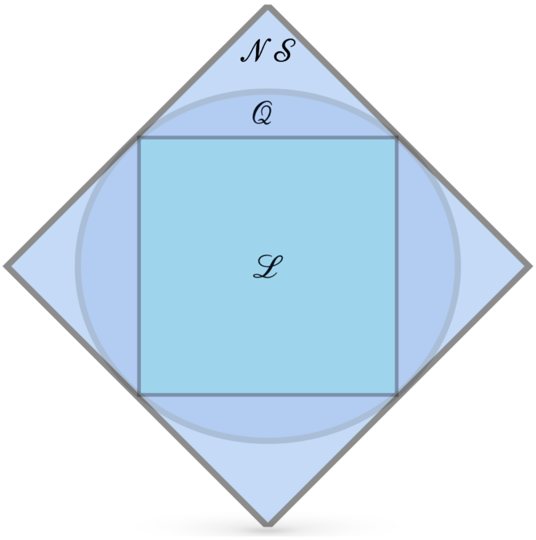

Figure 3.14: The set of quantum boxes

- Consider a quantum strategy entailing the maximally entangled state $|\psi^+\rangle$, with the following measurements: If $x = 0 = 0$, Alice measures the Z -operator, and if $x = 1$, she measures the X-operator.

- For Bob, $y = 0$ corresponds to measuring $\frac{(Z+X)}{2}$, and $y = 1$ corresponds to measuring $\frac{(Z-X)}{2}$.

- This strategy violates the CHSH inequality maximally, i.e., it achieves $S = 2\sqrt{2} > 2$, and $2\sqrt{2}$ is often referred to as the Tsirelson's bound!

- A no-signalling box, called the PR-Box can achieve a CHSH value, $S = 4$, $\forall a, b, x, y$,

$$p_{PR} \equiv p(a, b|x, y) = \begin{cases} \frac{1}{2}, & \text{if } x \cdot y = a \oplus b \\ 0, & \text{else.} \end{cases}$$

- The quantum box that achieves the Tsirelson's bound is,

$$p_{AB|XY} = \frac{1}{\sqrt{2}} p_{PR} + (1 - \frac{1}{\sqrt{2}}) p_{WN} \ ,$$

  where $p_{WN} \equiv p(a, b|x, y) = \frac{1}{4}, \ \forall a, b, x, y$.

CHSH scenario

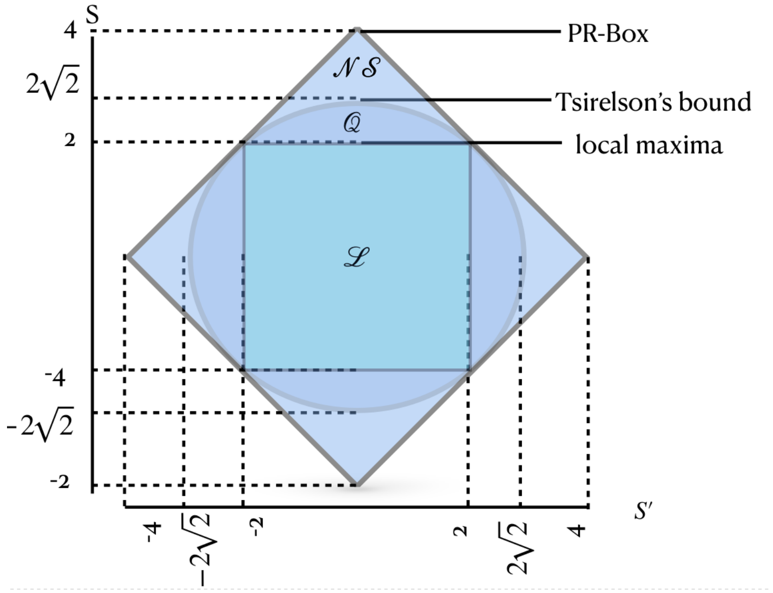

Figure 3.15: CHSH scenario

3.1.5 Device Independent Self Testing

- Self-testing refers to the art of making inferences based exclusively on observed statistics!
- Self-testing powers Device Independent Cryptography and all other applications!
- Question: what can we say about the underlying quantum realisation $Q \equiv (|\psi_{AB}\rangle, \{\Pi_a^x\}_{a,x}, \{\Pi_b^y\}_{b,y})$, given that we observe the box $p_{AB|XY}$!
- Inherent limitation: statements true only up to local isometries and auxiliary systems.
- The maximal violation of CHSH, $S = 2\sqrt{2}$, self-tests the quantum realization $Q \equiv (|\phi^+\rangle, \{Z, X\}, \{\frac{(Z+X)}{2}, \frac{(Z-X)}{2}\})$, up to local isometries!

Lemma 1 *Jordan's Lemma Given any two hermitian operators $\hat{a}_0, \hat{a}_1 \in B(\mathcal{H})$ on an arbitrary Hilbert space $\mathcal{H}$ with eigenvalues ± 1 , then there exists a basis in which both operators are block diagonal with blocks of dimension at most two, and specifically,*

$$\hat{a}_0 = \bigoplus_A \sigma_z^A \bigoplus_\xi \lambda_{\xi,0} |\xi\rangle\langle\xi|$$

$$\hat{a}_1 = \bigoplus_A \left[\cos\theta_A \sigma_z^A + \sin\theta_A \sigma_x^A\right] \bigoplus_\xi \lambda_{\xi,1} |\xi\rangle\langle\xi|$$

- The one-dimensional blocks $\bigoplus\limits_{\xi} \lambda_{\xi,1}$ do not contribute to the violation of the Bell inequality, thus, can be discarded.

- Furthermore, by applying the unitary transformations all the operators can be brought in the following form

$$\hat{a}_0 = Z$$
$$\hat{a}_1 = \cos\theta_A Z + \sin\theta_A X$$

3.1.6 Device Independent QKD [18]

Consider the following QKD protocol,

- Alice and Bob have access to a bipartite quantum box, with binary inputs $x, y \in in\{0,1\}$ and binary outputs $a, b \in \{0,1\}$,

- They observe the probability distribution,

$$p(a,b|0,0) = p(a,b|1,1) = \frac{1}{2}, \text{if } a = b$$
$$p(a,b|0,1) = p(a,b|1,0) = \frac{1}{4}, \forall a,b.$$

- This is the distribution Alice and Bob observe if they implement the entanglement-based version of the BB84 protocol, wherein they share the maximally entangled two-qubit state, $|\psi^+ = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)\rangle$ and measure in either the X basis or in the Z basis.

Hacking a device-dependent QKD

In the Device Independent setting there are no assumptions on the Hilbert space dimension of the shared quantum system!

- Consider the following tripartite state in the Hilbert space $\mathbb{C}_4 \otimes \mathbb{C}_4 \otimes \mathbb{C}_4$

$$\rho_{ABE} = \sum_{z_0,z_1 \in [2]} |z_0 z_1\rangle_A \langle z_0 z_1| \otimes |z_0 z_1\rangle_B \langle z_0 z_1| \otimes |z_0 z_1\rangle_E \langle z_0 z_1|$$

- If Alice and Bob measure $Z \otimes I$ whenever $x = y = 0$, and $I \otimes Z$ whenever $x = y = 1$, they retrieve the same probability distribution!

- Notice, that Eve has a perfect copy of the local state, and hence, can perfectly guess the secret key, effectively rendering the protocol insecure!

DIQKD origins

- The initial idea of exploiting violation of Bell inequalities to prove the security of a QKD protocol goes back to the protocol proposed by Ekert in 1991.
- Mayers and Yao introduce self-testing, i.e., maximal violation of a Bell inequality implies the complete characterisation of the quantum devices (up to local isometries on auxiliary degrees of freedom).
- The irst security proof of a DIQKD protocol is attributed to Barrett, Hardy, and Kent. Although the protocol was not useful in practice, the work demonstrated that secure DIQKD was achievable in principle.
- Numerous works leading up to practical implementations last year!

DIQKD protocol

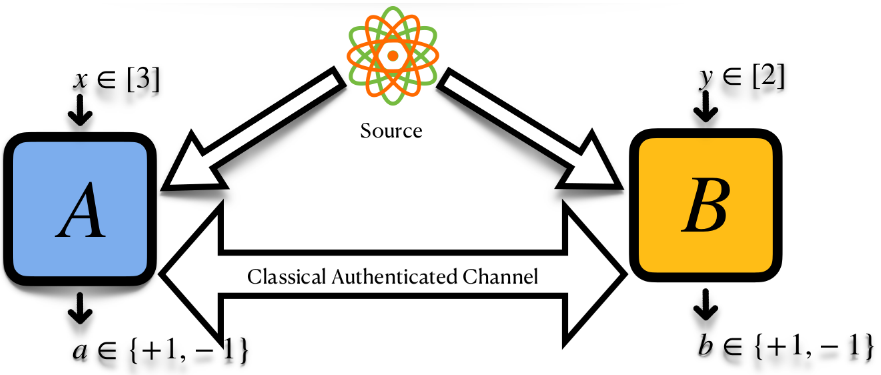

Figure 3.16: DIQKD protocol

- A source distributed states to Alice and Bob,
- Alice chooses between three different measurements A_x , with $x \in [3]$, while Bob chooses between two different measurements B_y , with $y \in [2]$, and they retrieve outcomes $a, b \in \{+1, -1\}$.
- Alice and Bob have access to an authenticated classical communication channel.
- The source as well as the measurement devices are assumed to be controlled by the Eavesdropper.

- The raw key is extracted from the outcomes of the pair $\{A_0, B_1\}$, such that Quantum Bit Error Rate (QBER), Q , is defined as the probability that Alice and Bob get different outcomes when measuring the pair A_0, B_1, i.e.

$$Q = p(a \neq b|0, 1)$$

- From QBER the parties estimate the amount of classical communication required for the error correction phase.
- The measurements A_1,A_2,B_0,B_1 are used to evaluate the value of CHSH inequality

$$S = \langle A_1 B_0 \rangle + \langle A_1 B_1 \rangle + \langle A_2 B_0 \rangle - \langle A_2 B_1 \rangle$$

- Based on Q and S, Alice and Bob estimate Eve's information!

A DIQKD protocol can be divided into three phases:

1. **Quantum transmission phase:**

   The parties use their devices to perform measurements and general their respective n -bit strings, $\overrightarrow{a}_0 = a_1 a_2 \ldots a_n$ and $\overrightarrow{b}_0 = b_1 a_2 \ldots b_n$.

2. **Parameter estimation phase:**

   The parties exchange classical information to estimate Bell violation S and the QBER Q . If the parameters allow for the generation of a secure key, i.e., the Bell violation is sufficiently high and the QBER is sufficiently low, they proceed. Otherwise, they abort the protocol.

3. **Classical post-processing phase**:

   The parties use the estimate they have on Eve's potential knowledge of the key to perform error correction and to produce the raw keys and perform privacy amplification to generate the final secure key.

A particular implementation:

- Alice and Bob share a noisy maximally entangled state,

$$\rho_{AB} = p\,|\phi^+\rangle\,\langle\phi^+| + (1-p)\frac{\mathbb{I}}{4}$$

- The measurement are

$$\begin{aligned} A_0 &= B_0 = Z \\ A_1 &= \frac{1}{2}(Z + X),\ B_2 = X \\ A_2 &= \frac{1}{2}(Z - X) \end{aligned}$$

- The CHSH violation and QBER for this protocol are, $S = 2\sqrt{2}$ and $Q = \frac{1}{2}(1-p)$, such that,

$$S = 2\sqrt{2}(1-2Q).$$

- Important to note the security is only based on the observed value of S and Q and not on the particular implementation!

Security Analysis against collective attacks

- In DIQKD we only have access to the input-output statistics the devices produces, and we need to prove security based exclusively on the observed statistics!

- One way, is finding a lower bound on the set key rate r given by the Devetak-Winter rate r_{DW}

$$r \geq r_{DW} = I(A_0 : B_1) - \chi(B_1 : E) \ ,$$

where $I(A_0 : B_1) = H(A_0) + H(B_1) - H(A_0, B_1)$, and $\chi(B_1 : E)$ is the Holevo quantity given by

$$\chi(B_1 : E) = H(\rho_B) - \frac{1}{2} \sum_{b_1 \in \{+1,-1\}} H(\rho_{E|b_1}) \ ,$$

where $\rho_E = Tr_{AB}(|\psi_{ABE}\rangle \langle\psi_{ABE}|)$ represents the state of Eve's quantum system, and $\rho_{E|b_1}$ denotes the state of Eve's system conditioned on Bob obtaining the result b_1 when measuring B_1.

- The optimal collective attack is to prepare the states such that $|\psi_{ABE}\rangle$ is the purification of ρ_{AB}.

- Without loss of generality, we assume uniform marginals, i.e.,

$$p(a|x) = p(b|y) = \frac{1}{2}, \forall a, b, x, y.$$

- Consequently, the mutual information between Alice and Bob has the expression

$$I(A_0 : B) = 1 - h_2(Q),$$

where h_2 is the binary entropy!

- Using Jordan's lemma, the second term can be bounded from above as follows,

$$\chi(B_1 : E) \leq h_2\left(\frac{1 + \sqrt{\left(\frac{S}{2}\right)^2 - 1}}{2}\right)$$

- Consequently, the lower bound for the secret key rate for the DIQKD protocol is given by,

$$r \geq r_{DI} = 1 - h_2(Q) - h_2\left(\frac{1+\sqrt{\left(\frac{S}{2}\right)^2 - 1}}{2}\right)$$

- Let's compare the device-independent lower bound r_{DI} with a device-dependent lower bound. For the device-dependent case, for the particular implementation, we have that,

$$r \geq r_{DD} = 1 - h_2(Q) - h_2\Big(Q + \frac{S}{2\sqrt{2}}\Big)$$

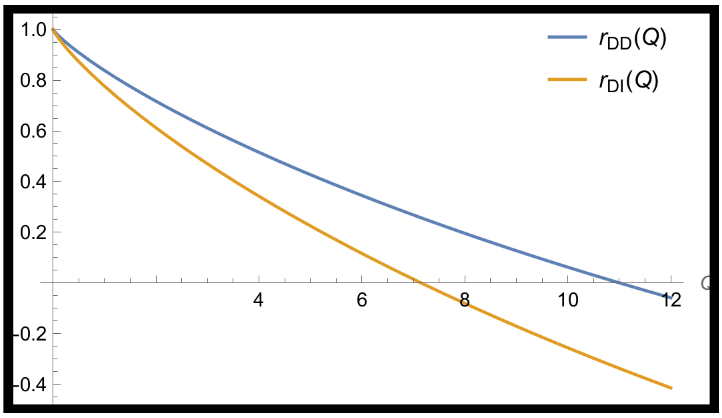

Figure 3.17: The secret key rate is strictly lower in the device-independent setting (as expected), but it is still possible to extract a secret key up to a QBER of ≈ 7.1% . The plot also shows critical QBER of 11% for the BB84 protocol.

Explicit attack

- Eve sends the state,

$$\rho_{AB}(S) = \frac{1+C}{2}P_{\phi^+} + \frac{1-C}{2}P_{\phi^-}$$

where $C = \sqrt{\left(\frac{S}{2}\right)^2 - 1}$ to the parties.

- She programs the measurements to be,

$$\begin{aligned} A_1 &= \frac{1}{\sqrt{1+C^2}}Z + \frac{C}{\sqrt{1+C^2}}X \ , \\ A_2 &= \frac{1}{\sqrt{1+C^2}}Z - \frac{C}{\sqrt{1+C^2}}X \ , \\ B_1 &= Z \ , \\ B_2 &= X \end{aligned}$$

and A_0 is the Z-measurement with probability $1-2Q$ and white-noise with probability $2Q$.

- For this attack, $B_1 = Z$, the Holevo quantity turns out to be,

$$\chi(B_1 : E) = h_2\left(\frac{1+\sqrt{\left(\frac{S}{2}\right)^2 - 1}}{2}\right)$$

saturating the lower bound r_{DI} on the secret key rate!

Finite-Key Analysis

- In a real experiment the protocol can only run for a finite number of rounds!
- To deal with the finite number of rounds, the main task is to bound the min-entropy,

$$H_{min} = (K_A^n|E),$$

which determines the length of the secret key.

- Collective attacks allow us to work under the IID (Independent and Identically Distributed) assumption, which greatly simplifies the security analysis!
- In the IID scenario, each round of the protocol is independent of the other rounds and all rounds are identical.
- This implies that the state ρ_{AB} of Alice and Bob's system after M rounds of the protocol is given by

$$\rho_{AB}^M = \rho_{AB}^{\otimes M} \ .$$

- In the IID scenario, Alice's raw key is given by $K_A^n = K_1 \dots K_n$, where K_i are IID random variables.
- Eve's information is given by $E = E_1 \dots E_n$, where E_i are IID quantum side information about K_i.
- To bound the von Neumann entropy $H(K_A^n|K_E)$, we use the chain rule and the IID assumption, such that,

$$\sum_i H(K_i|E_1, \dots, E_n, K_1, \dots, K_{i-1}) = \sum_i H(K_i|E_i) = nH(K_i|E_i) \ ,$$

thereby reducing the analysis of the entire protocol to the analysis of a single round.

- To bound the smooth min-entropy we use Tomamichel et al.'s result of *Quantum Asymptotic Equipartition Property*, which states that,

  $$H_{min}^{\epsilon}(K_A^n|E) = nH(K_1|E_1) - c_\epsilon\sqrt{n}$$

  where c_ϵ is a correction term independent of n.

- These simplifications only work because of the IID assumptions!

- Such strong assumptions must be avoided to get the ultimate form of security!

Security Analysis against coherent attacks

- Coherent attacks are the most general form of attacks!

- Eve can act differently in each round and so can the devices!

- de Finetti-type theorems or the post-selection technique reduce the security proofs of coherent attacks to a security proof for collective attacks for Device-Dependent QKD.

- As these techniques require that the Hilbert space dimension of the systems be known, they can no longer be applied in the Device-Independent QKD.

- Losing the IID assumptions implies that there can be interactions between the individual rounds of the protocol, hence the random variable K_A^n and the quantum side information E can no longer be expressed in the product form!

- Even worse, the requirements for the QAEP are now no longer fulfilled!

Entropy Accumulation Theorem (EAT)

- The Entropy Accumulation Theorem (EAT) fills the gap in the DIQKD case!

- Similar to QAEP, the EAT reduces the analysis of the whole protocol to that of a single round!

- Every round of the protocol is represented by a quantum channel $M_[i]$ that takes the state R_{i-1} as input and outputs classical data O_i and S_i as well as the quantum state R_i which is input to the next round M_{i+1} of the protocol.

- The system is entangled with its purifying system E.

- From the classical data O_i , S_i the parties can determine CHSH value!

- From the outputs, O_i they generate the secret key!

- The EAT provide a bound on the entropy by relating it to the worst case that can happen in each individual round of the protocol!

- Consider a single round i of the protocol isolated from the remaining rounds.

- The global state of the system σ , consists of the input state R_{i-1} to the channel M_i and the purifying system $R^{'}$ at this instant.

- The output of the channel M_i consists of some classical data O_i . S_i and a quantum state R_i .

- The conditional von Neumann entropy is hence evaluated for the states $(M_i \otimes \mathbb{I}_R)\sigma$, abbreviated as $M_i(\sigma)$:

$$H(O_i|S_i R^{'})_{M_i(\sigma)}$$

- Without IID assumption, we don't have access to the local state σ , so we take the minimum over all possible states σ that are compatible with the observed statistics.

- The EAT then bounds the min-entropy as,

$$H^{\epsilon}_{min}(O^n|S^n, E)_\rho \geq \sum_{i=1}^{n} \min_{\sigma} H(O_i|S_i, R^{'})_\sigma - O(\sqrt{n})$$

- The bound is similar to the QAEP, the first term is linear in n , and the term proportional to $\sqrt{n}$ vanishes in the limit of large n (since we divide by n to compute the key rate).

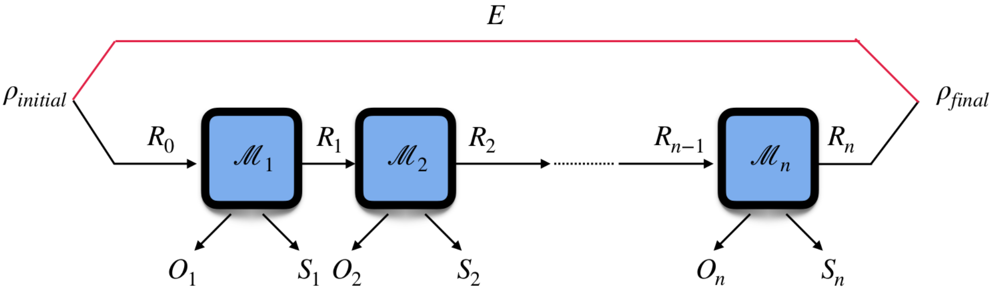

Figure 3.18: Entropy Accumulation Theorem (EAT).

3.1.7 Loopholes in Bell experiments

- Just like any test, Bell tests have loopholes, which can be exploited by Eve to hack DIQKD protocols!
- What is required to perform a loophole-free Bell test?
- In general, we need to assure the following two properties are fulfilled:
    1. No information about the input of one party is allowed to be known to the other party before the output is produced!
    2. The detection efficiency have to be sufficiently high!
- Loopholes arise when one or both of these requirements are not fulfilled in the experimental design or setup, which affects the validity of the results!

The locality loophole

- If the first requirement is not fulfilled, the very premises needed for the validity of a Bell inequality violation are not given!
- There exists a signalling classical model that accounts for the apparent non-locality of observed correlations!
- This is the locality loophole.
- Alice and Bob have to be separated far enough (at least tens of meters) and measurements have to be performed fast enough such that no light-speed communication can affect the respective measurements!
- One needs to send entangled states over such distance without doing much damage!
- Preferred substrate: photons!
- However, photonics experiments suffer from the issue of photon losses, which gives rise to the detection loophole!

The detection loophole

- In practice, the measurement devices are imperfect and sometimes fail to detect the incoming photons!

- This can exploited by an adversary to manipulate the input-output statistics that Alice and Bob observe!

- With faulty detectors of efficiency $\eta_A = \eta_B = \frac{1}{4}$, LHV models can achieve $S = 4$!

- Possible resolutions:

  1. Keep everything: the "no-click" event ($\perp$) as an additional outcome and check membership to the local polytope of a larger Bell scenario!
  2. Assign already existing measurement outcome to the "no-click" event ($\perp \rightarrow 0$) !

The detection loophole: Tilted Bell inequalities

- In a CHSH experiment, suppose Alice's detection efficiency is η_A , and Bob's detection efficiency is η_B , and the parties use the assignment strategy ($\perp \rightarrow +1$)!

- This effectively tilts the CHSH inequality,

$$S_{\eta_A \eta_B} = \eta_A \eta_B S + \eta_A(1-\eta_B)\langle A_0 \rangle + \eta_B(1-\eta_A)\langle B_0 \rangle + (1-\eta_A)(1-\eta_B)2 \leq 2 \ .$$

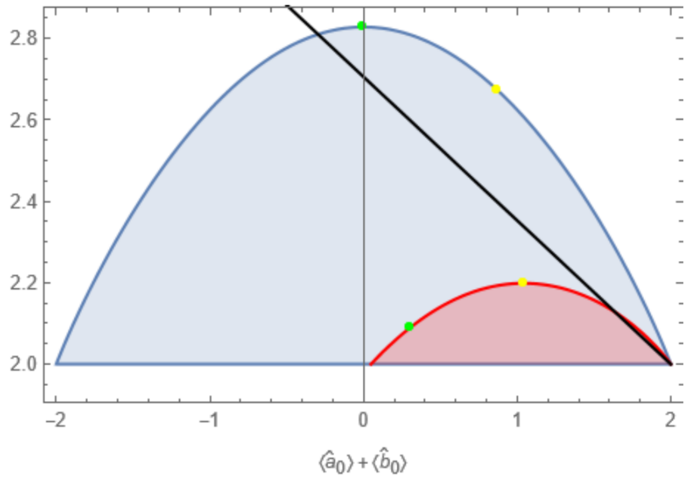

Figure 3.19: Tilted Bell inequalities.

3.1.8 Conclusions

- DIQKD is a necessity!

- Although there have been experimental demonstrations, the technology is still not practical!

- Limited to a few kilometres!
- Need of the hour to enable practical and noise-robust DIQKD across 100s of kilometres!
- The only way to ensure mass individual or institutional privacy in an AI-dominated world!

3.2 Assignments

Assignment 3.2.1 (Non-local games and boxes)

1. Show that for any distribution $p_{AB|XY} \equiv \{p(a,b|x,y)\}_{a,b,x,y\in\{0,1\}}$ the value of CHSH expression,

$$CHSH(p_{AB|XY}) \equiv \langle A_0B_0\rangle + \langle A_0B_1\rangle + \langle A_1B_0\rangle - \langle A_1B_1\rangle \ ,$$

where $\langle A_xB_y\rangle = \sum_{a,b\in\{0,1\}}(-1)^{a\oplus b}p(ab|xy)$, and the success probability of CHSH non-local game,

$$S_{CHSH}(p_{AB|XY}) \equiv \frac{1}{8}\sum_{a,b,x,y\in\{0,1\}} p(a\oplus b = x\cdot y|xy) \ ,$$

are related as follows,

$$CHSH(p_{AB|XY}) = 8S_{CHSH}(p_{AB|XY}) - 4 \ .$$

2. Show that the classical strategy of always producing 0 as the output saturates the CHSH inequality,

$$CHSH(p_{AB|XY}) \leq 2, \tag{3.1}$$

and saturates the CHSH inequality in the game form,

$$S_{CHSH}(p_{AB|XY}) \leq \frac{3}{4}.$$

3. Consider a quantum strategy entailing the maximally entangled state $|\phi^+\rangle$, with the following measurements: If $x = 0$, Alice measures the Z-operator and if $x = 1$, she measures the X-operator. For Bob, $y = 0$ corresponds to measuring $(Z + X)/\sqrt{2}$, and $y = 1$ corresponds to measuring $(Z - X)/\sqrt{2}$. Show that this strategy violates the CHSH inequality (3.1) maximally, i.e.,

$$CHSH(p_{AB|XY}) = 2\sqrt{2}$$

and,

$$S_{CHSH}(p_{AB|XY}) = \frac{2+\sqrt{2}}{4}.$$

4. Show that these strategies satisfy the no-signaling conditions.

5. Show via an example that correlations satisfying the no-signaling correlations can violate the CHSH inequality even more.

Hint

Consider a PR-box,

$$p(a,b|x,y) = \begin{cases} \frac{1}{2}, \text{ if } x \cdot y = a \oplus b, \\ 0, \text{ else.} \end{cases}$$

Assignment 3.2.2 (Detection Loophole)

In optical Bell tests, the detection loophole is an issue that arises when only a small percentage of the photons emitted are actually detected. This can be exploited by the adversary who is trying to intercept the message sent by Alice to Bob.

1. If Alice and Bob have detectors that are not perfect and they use a strategy where they assign a predetermined classical outcome, say (0), to every no-click outcome. For the strategy described above which attains $CHSH(p_{AB|XY}) = 2\sqrt{2}$ with perfect detectors, what would be the expression for the observed value of $CHSH(p_{AB|XY})$ given that the detection efficiency for Alice is η_A and for Bob is η_B?

2. Find the critical detection efficiency $\eta*$ for witnessing a loophole-free violation of the CHSH inequality $CHSH(p_{AB|XY}) \leq 2$ when $\eta_A = \eta$, and $\eta_B = 1$ with the set-up described above which reaches $CHSH(p_{AB|XY}) = 2\sqrt{2}$.

3. Find the critical detection efficiency $\eta*$ for witnessing a loophole-free violation of the CHSH inequality $CHSH(p_{AB|XY}) \leq 2$ when $\eta_A = \eta_B = \eta$ with the set-up described above which reaches $CHSH(p_{AB|XY}) = 2\sqrt{2}$.

Assignment 3.2.3 (DIQKD Protocols and Security)

Consider a particular implementation of the DIQKD scheme, similar to the Ekert's protocol, wherein Alice and Bob share the maximally entangled Bell state $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, Alice has three measurements $A_0 = Z$, $A_1 = \frac{1}{\sqrt{2}}(Z + X)$, $A_2 = \frac{1}{\sqrt{2}}(Z - X)$, while Bob has a couple of measurements $B_1 = Z$,$B_2 = X$. Where Z, X are Pauli operators. Suppose that the parties observe the behaviour $p_{AB|XY} \equiv \{p(a,b|x,y)\}_{a,b,x,y \in \{0,1\}}$.

The raw key is extracted from the outcomes of the pair $\{A_0, B_1\}$. The Quantum Bit Error Rate (QBER), Q, is a measure of the error rate in a quantum key distribution (QKD) system, defined as the probability that Alice and Bob get different outcomes when extracting the raw key,

$$Q = p(A \neq B|XY). \tag{3.2}$$

Apart from QBER, the parties also take into account the value of CHSH expression,

$$CHSH(p_{AB|XY}) \equiv \langle A_1 B_1 \rangle + \langle A_1 B_2 \rangle + \langle A_2 B_1 \rangle - \langle A_2 B_2 \rangle \,, \tag{3.3}$$

For the protocols specified above, the lower bound for the secret key rate against collective attacks is given by:

$$r \geq 1 - h_2(Q) - h_2 \left(\frac{1 + \sqrt{S/2)^2 - 1}}{2} \right), \tag{3.4}$$

where S is any violation of CHSH expression ($CHSH(p_{AB|XY})$), h_2 is the binary entropy.

1. Find the behavior $p_{AB|XY} \equiv \{p(a, b|x, y)\}_{a,b,x,y \in \{0,1\}}$ which Alice and Bob obtain as a result of the aforementioned protocol. Consequently, find the value of QBER (3.2) and the value of CHSH expression (3.3).

2. Consider a slightly different protocol wherein Alice and Bob share the state,

   $$\rho_{AB}(C) = \frac{1+C}{2} P_{\phi_+} + \frac{1-C}{2} P_{\phi_-},$$

   where $C = \sqrt{\left(\frac{S}{2}\right)^2 - 1}$, S is any violation of CHSH expression ($CHSH(p_{AB|XY})$), $P_{\phi_+} = |\phi^+\rangle\langle\phi^+| \,, P_{\phi_-} = |\phi^-\rangle\langle\phi^-|$, and $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and $|\phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$.

   The measurements are $A_0 = Z$, $A_1 = \frac{1}{\sqrt{1+C^2}} Z + \frac{1}{\sqrt{1+C^2}} X$, $B_1 = Z$, $A_2 = \frac{1}{\sqrt{1+C^2}} Z - \frac{1}{\sqrt{1+C^2}} X$, and $B_2 = X$. Find the value of QBER (3.2) and the value of CHSH expression (3.3) for this protocol.

3. Show that the secret key rate r (3.4) cannot be positive if $CHSH(p_{AB|XY}) = S \leq 2$.

4. Evaluate the key rate r (3.4) for both of the aforementioned protocols.

These exercises have been inspired from [1, 18].

Chapter 4

Quantum secured-internet challenges and achievement

4.1 Theory

4.2 Assignments

In every assignment, the Bell states are defined in the following way

$$
\begin{aligned}
|\Psi^{\pm}\rangle &= \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle) \ , \\
|\Phi^{\pm}\rangle &= \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle).
\end{aligned}
$$

Assignment 4.2.1 (Entanglement in NV centers)[4]

Using the formalism of quantum mechanics, show, how to create entanglement between two NV centers.

Hint

The state of the electron in NV center is the following

$$|NV_e\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle + |\downarrow\rangle)$$

The entangled state of the electron in NV center and the photon is the following

$$|NV_{ep}\rangle = \frac{1}{\sqrt{2}}(|\uparrow 1\rangle + |\downarrow 0\rangle)$$

In the case when only one detector clicks the two copies of the above state are projected to the following state:

$$|p\rangle = \frac{1}{\sqrt{2}}(|10\rangle + e^{i\theta}\,|01\rangle) \ .$$

Assignment 4.2.2 (Fidelity estimation from QBER)[5]

Alice and Bob share 20 copies of entangled state $\rho_{noise} = (1 - p_{err})\rho + p_{err} X\rho X$, where $\rho = |\Psi^-\rangle\langle\Psi^-|$. Estimate the fidelity of ρ_{noise} using QBER for the following cases:

(a)

basis	X	Z	Y	X	Y	Z	X	X	Z	Y	Y	Z	X	Y	X	Z	Z	X	Y	X
A outcome	1	0	0	1	1	1	0	1	0	1	0	1	0	0	1	0	1	0	1	0
B outcome	1	1	1	1	0	0	1	1	0	1	0	0	0	0	1	0	0	1	0	0

(b)

basis	Y	Y	Z	X	X	Y	Z	Z	X	Y	Y	Z	X	X	Y	X	Z	X	Y	Z
A outcome	1	0	1	1	0	1	0	1	0	0	0	1	1	0	0	1	0	0	1	0
B outcome	0	1	0	0	1	1	1	0	1	1	1	0	1	0	1	0	1	1	0	0

Hint

Fidelity to target state $|\Psi^-\rangle$ is equal

$$F(|\Psi^-\rangle) = 1 - \frac{QBER_X + QBER_Y + QBER_Z}{2} \text{ , where}$$
$$QBER_i \approx \frac{\#\{j | x_j^A = x_j^B, r_j = i\}}{\#\{j | r_j = i\}}$$

Assignment 4.2.3 (Quantum error correction code)[11]

Alice sends Bob a qubit $|\varphi\rangle = \alpha|0_L\rangle + \beta|1_L\rangle$ protected against errors by Shore code

$$|0_L\rangle \equiv \frac{(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)}{2\sqrt{2}} ,$$
$$|1_L\rangle \equiv \frac{(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)}{2\sqrt{2}} .$$

Assuming that on the transmission the following errors occur:

(a) Bit flip on qubits 1.

(b) Phase flip on one of the qubits 4,5,6 .

Show, how by measuring in the basis of Pauli's operators X and Z one can fix these errors. Wonder, how one can detect these errors. Draw the quantum circuit that realizes the Shore coding.

Assignment 4.2.4 (Teleportation and Entanglement Swapping)

(a) Consider Alice and Bob share a Bell pair $|\Phi^+\rangle_{AB} = \frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB})$. Let $|\varphi\rangle_{A'} = a\,|0\rangle_{A'} + b\,|1\rangle_{A'}$, where $a, b \in \mathbb{C}$ such that $|a|^2 + |b|^2 = 1$, be a qubit state unknown to Alice. Provide a protocol using local operations and classical communication (LOCC) allowing Alice to teleport $|\varphi\rangle$ to Bob.

Hint

Alice can perform a Bell state measurement $\{\Phi^+_{A'A}, \Phi^-_{A'A}, \Psi^+_{A'A}, \Psi^-_{A'A}\}$ and Bob can perform local Pauli operations X, Y, Z).

(b) Consider now three parties Alice, Charlie, and Bob, sharing Bell pairs $|\Phi^+\rangle_{AC_A}$ and $|\Phi^+\rangle_{C_BB}$, where Carlie holds C_AC_B. Provide an LOCC protocol to distribute a Bell pair between Alice and Bob.

(c) Consider now Alice, Charlie and Bob sharing noisy states $\rho^p_{AC_A} := p\,|\Phi^+_{AC_A}\rangle\,\langle\Phi^+_{AC_A}| + (1 - p)\frac{1}{4}\mathbb{I}_{AC_A}$ and $\rho^p_{C_BB}$ for some $0 \leq p \leq 1$. Show that the entanglement swapping protocol considered in (b) results in a state of the form ρ^q_{AB} for some $0 \leq q \leq 1$ and compute q as a function of p.

Assignment 4.2.5 (Amplitude and phase damping channels)

Imagine that Alice sends half of Bell state $|\Phi^+\rangle$ through:

(a) amplitude damping channel ,

(b) phase damping channel.

Show, how looks the state after such transmission.

Hint

In our case, the channel is a quantum operation on one qubit state ρ described in the following way:

$$\varepsilon(\rho) = E_0 \rho E_0^\dagger + E_1 \rho E_1^\dagger \ ,$$

where operators

$$E_0^{AD} = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-\alpha} \end{pmatrix} \ ,$$
$$E_1^{AD} = \begin{pmatrix} 0 & \sqrt{\alpha} \\ 0 & 0 \end{pmatrix}$$

for amplitude damping channel and

$$E_0^{PD} = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-\beta} \end{pmatrix} \ ,$$
$$E_1^{PD} = \begin{pmatrix} 0 & 0 \\ 0 & \sqrt{\beta} \end{pmatrix}$$

for phase damping channel. α and β are probabilities of losing and scattering the photon respectively.

Assignment 4.2.6 (Entanglement purification)

Consider Alice and Bob holding two copies of the above noisy states, i.e. the initial states are $(\rho_{AB}^p)^{\otimes 2}$. Apply now the following purification protocol: Alice applies the unitary

$$|0\rangle \to \frac{1}{\sqrt{2}}(|0\rangle - i\,|1\rangle)$$
$$|1\rangle \to \frac{1}{\sqrt{2}}(|1\rangle - i\,|0\rangle)$$

to both of her subsystems, while Bob applies the unitary

$$|0\rangle \to \frac{1}{\sqrt{2}}(|0\rangle + i\,|1\rangle)$$
$$|1\rangle \to \frac{1}{\sqrt{2}}(|1\rangle + i\,|0\rangle)$$

on both of his subsystems. Next, Alice and Bob both apply a CNOT gate, given by a unitary

$$|i\rangle_c\,|j\rangle_t \to |i\rangle_c\,|i \oplus j\rangle_t$$

for $i, j \in \{0, 1\}$, where c and t denote the control and target system, respectively, to their two systems. Finally, Alice and Bob both measure their target system in a computational basis. If their results coincide they keep the state in the control system, otherwise they abort. Compute the probability of not aborting and the resulting state in the case of not aborting, both depending on p.

Assignment 4.2.7 (Filtering protocol)[13]

Perform the filtering protocol for the state $\rho_{AB} = p\,|\Phi^+\rangle\langle\Phi^+| + (1-p)\,|01\rangle\langle 01|$. Calculate p_{succ}, postmeasurement state $\hat{\rho}_{AB}$ in case of success and its fidelity F.

Hint

The local measurement is given by POVM's: $\{M_A^0, M_A^1\}$ and $\{M_B^0, M_B^1\}$, where

$$\begin{aligned} M_{A(B)}^1 &= (A_{A(B)}^1)^\dagger A_{A(B)}^1 \ , \\ M_{A(B)}^0 &= \mathbb{I} - M_{A(B)}^1, \\ A_A^1 &= \sqrt{\epsilon}\,|0\rangle\langle 0| + |1\rangle\langle 1| \ , \\ A_B^1 &= \sqrt{\epsilon}\,|1\rangle\langle 1| + |0\rangle\langle 0| \ . \end{aligned}$$

Chapter 5

Upper Bounds on Key Rates in QKD

5.1 Theory

5.2 Assignments

Assignment 5.2.1

Knowing that squashed entanglement $E_{sq}(\rho_{AB})$ is an upper bound on (bipartite) distillable key $K_D(\rho_{AB})$, show that $K_D(\rho_{AB}) \leq \frac{1}{2}\mathrm{I}(A:B)$.

Hint

1. $E_{sq}(\rho_{AB}) := \inf\left\{\frac{1}{2}\mathrm{I}(A:B|E)\ :\ \rho_{ABE} \text{ extension of } \rho_{AB}\right\}$.
2. Consider a specific action of the eavesdropper.

Assignment 5.2.2

Calculate squashed entanglement $E_{sq}(\rho_{AB})$ in the following cases

(a) $E_{sq}(\rho_A \otimes \rho_B)$,

(b) $E_{sq}(\Psi^{\pm})$, where $|\Psi^{\pm}\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle_{AB} \pm |11\rangle_{AB}\right)$,

(c) $E_{sq}(\rho_{AB}^{\otimes n})$, assuming $E_{sq}(\rho_{AB}) = x$.

Hint

1. $\mathrm{I}(A:B|E)_{\rho_{ABE}} = S(\rho_{AE}) + S(\rho_{BE}) - S(\rho_E) - S(\rho_{ABE})$, where $(\rho) = -\mathrm{Tr}\rho\log_2\rho$ is the von Neumann entropy and $S(\rho\otimes\sigma) = S(\rho) + S(\sigma)$.
2. Squashed entanglement is additive on tensor products, i.e, $E_{sq}(\rho_{AB}\otimes\sigma_{AB}) = E_{sq}(\rho_{AB}) + E_{sq}(\sigma_{AB})$.

Assignment 5.2.3

Knowing that the relative entropy of entanglement $E_r(\rho_{AB})$ is an upper bound on (device-dependent) secret key rate $K_D(\rho_{AB})$, the upper bound of the following

(a) $K_D(\Psi^+)$, where $|\Psi^+\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle_{AB} + |11\rangle_{AB}\right)$.

(b) $K_D(\alpha\Psi^+ + (1-\alpha)\Psi^-)$, where $|\Psi^-\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle_{AB} - |11\rangle_{AB}\right)$, and $\alpha \in [0,1]$.

Hint

$E_r(\rho) = \inf_{\sigma \in \mathrm{SEP}} S(\rho||\sigma)$, where $S(\rho||\sigma) = \mathrm{Tr}\rho \log_2 \rho - \mathrm{Tr}\rho \log_2 \sigma$ and SEP is the set of separable states.

Assignment 5.2.4

Show that relative entropy of entanglement $E_r(\rho)$ upper bounds its regularized version $E_r^\infty(\rho)$, i.e.,

$$E_r(\rho) \geq E_r^\infty(\rho) := \lim_{n\to\infty} \frac{1}{n} E_r(\rho^{\otimes n}).$$

Hint

Use the following additivity property of quantum relative entropy

$$S(\rho_1 \otimes \rho_2||\sigma_1 \otimes \sigma_2) = S(\rho_1||\sigma_1) + S(\rho_2||\sigma_2).$$

Assignment 5.2.5

For any fixed $\varepsilon \in (0, 1)$, the achievable region of secret key agreement from a single copy of an arbitrary multipartite quantum state $\rho_{\overrightarrow{A}} \equiv \rho_{A_1 \ldots A_M}$ satisfies

$$K_D^{(1,\varepsilon)}(\rho) \leq E_{h,GE}^{\varepsilon}(\overrightarrow{A})_\rho$$

where

$$E_{h,GE}^{\varepsilon}(: \overrightarrow{A} :)_\rho := \inf_{\sigma \in BS(:\overrightarrow{A}:)} D_h^{\varepsilon}(\rho||\sigma).$$

is the ε-hypothesis testing relative entropy of genuine entanglement of multipartite state $\rho_{\overrightarrow{A}}$, and $BS(: \overrightarrow{A} :)$ denotes the set of biseparable states. Calculate ε-hypothesis testing relative entropy upper bound on $K_{\mathrm{D}}^{(1,\varepsilon)}(\Psi_3^W)$, where $|\Psi_3^W\rangle = \frac{1}{\sqrt{3}}(|001\rangle + |010\rangle + |110\rangle)$.

Hint

1. If ρ is a pure state and it is one of the eigenvectors of σ, i.e., there exists decomposition $\sigma = p_0\rho + \sum_{i=1} p_i \gamma_i^\perp$, with $\sum_{i=0} p_i = 1$, $0 \leq p_i \leq 1$, $p_0 \neq 0$ and states $\gamma_i^\perp$ orthogonal to ρ then for any $\epsilon \in [0, 1]$:

   $$D_h^\varepsilon(\rho||\sigma) = -\log_2 \mathrm{Tr}[\Omega\sigma],$$

   with $\Omega = (1 - \varepsilon)\rho$.

2. Employ biseparable state $\pi_{\mathrm{W}} := |0\rangle\langle 0| \otimes \Phi_2^{\mathrm{W}}$, where $|\Phi_2^{\mathrm{W}}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$.

Assignment 5.2.6

Calculate upper bounds on the secret key rate $K_{DI}^{(iid)}(P)$ (in the non-signaling device-independent *iid* scenario) for isotropic devices $\mathrm{P}_{\mathrm{iso}}(\varepsilon) = (1-\varepsilon)\mathrm{PR} + \varepsilon\overline{\mathrm{PR}}$, inside (2,2,2,2) polytope, for $\alpha \in [0, 0.25]$, using

(a) Non-signaling squashed mutual information: $K_{DI}^{(iid)}(P) \leq \widehat{\mathrm{I}}(A:B)_P = \max_{x,y} \mathrm{I}(A:B)_{P_{x,y}}$, where $P_{x,y}$ is a probability distribution obtained with "x,y" measurement,

(b) Nonlocality cost: $K_{DI}^{(iid)}(P) \leq \mathcal{N}_C(P) = C(P)\log_2 \min\{|A|,|B|\}$, where $C(P) = \min\{\alpha \;:\; P = \alpha P_{NL}^{v} + (1-\alpha)P_L,\; \alpha \in [0,1]\}$, P_{NL}^{v} is a nonlocal vertex (extreme nonlocal device) and P_L is a local device.

Determine (estimate) region of ε where $\widehat{\mathrm{I}}(A:B)_{\mathrm{P}_{\mathrm{iso}}(\varepsilon)} \leq \mathcal{N}_C(\mathrm{P}_{\mathrm{iso}}(\varepsilon))$. Compare the calculated region with "quantum" region, i.e., $\varepsilon \in [\frac{1}{2} - \frac{1}{4}\sqrt{2}, 0.25]$.

Hint

1. The PR and $\overline{\mathrm{PR}}$ are vertices given by

$$\mathrm{PR}_{\mathrm{AB|XY}}(ab|xy) = \begin{array}{cc|cc|cc} & x & 0 & & 1 & \\ y & b \diagdown a & 0 & 1 & 0 & 1 \\ \hline 0 & 0 & \frac{1}{2} & 0 & \frac{1}{2} & 0 \\ & 1 & 0 & \frac{1}{2} & 0 & \frac{1}{2} \\ \hline 1 & 0 & \frac{1}{2} & 0 & 0 & \frac{1}{2} \\ & 1 & 0 & \frac{1}{2} & \frac{1}{2} & 0 \end{array} \qquad \overline{\mathrm{PR}}_{\mathrm{AB|XY}}(ab|xy) = \begin{array}{cc|cc|cc} & x & 0 & & 1 & \\ y & b \diagdown a & 0 & 1 & 0 & 1 \\ \hline 0 & 0 & 0 & \frac{1}{2} & 0 & \frac{1}{2} \\ & 1 & \frac{1}{2} & 0 & \frac{1}{2} & 0 \\ \hline 1 & 0 & 0 & \frac{1}{2} & \frac{1}{2} & 0 \\ & 1 & \frac{1}{2} & 0 & 0 & \frac{1}{2} \end{array}.$$

2. The mutual information of two random variables A and B with joint probability distribution P is given by

$$\mathrm{I}(A:B)_P = \sum_{a,b} P(a,b)\log_2 \frac{P(a,b)}{P(a)P(b)},$$

where $P(a) = \sum_b P(a,b)$.

3. There exists CHSH inequality and an operation tw$(\cdot)$ (called twirling), such that,

- $\mathrm{CHSH(PR)} = 4$, $\mathrm{CHSH}(\overline{\mathrm{PR}}) = -4$,
- $\mathrm{CHSH}(\mathrm{P}_{\mathrm{iso}}(\varepsilon)) = 4 - 8\varepsilon$, for $\varepsilon \in [0,1]$,

- Devices for which $-2 \leq \mathrm{CHSH} \leq 2$ are local devices.

- $\mathrm{tw}(P) \in \{\mathrm{P}_{\mathrm{iso}}(\varepsilon)\}$, for all P,

- $\mathrm{CHSH}(\mathrm{tw}(P)) = \mathrm{CHSH}(P)$.

Bibliography

[1] R. Arnon-Friedman. *Device-Independent Quantum Information Processing: A Simplified Analysis*. Springer Nature, 2020.

[2] C. H. Bennett. Quantum cryptography using any two nonorthogonal states. *Physical review letters*, 68(21):3121, 1992.

[3] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. *arXiv preprint arXiv:2003.06557*, 2020.

[4] H. Bernien, B. Hensen, W. Pfaff, G. Koolstra, M. S. Blok, L. Robledo, T. H. Taminiau, M. Markham, D. J. Twitchen, L. Childress, and R. Hanson. Heralded entanglement between solid-state qubits separated by 3 meters. *Nature 497, 86-90 (2013)*, 497(7447):86–90, apr 2012.

[5] A. Dahlberg, M. Skrzypczyk, T. Coopmans, L. Wubben, F. Rozpedek, M. Pompili, A. Stolk, P. Pawełczak, R. Knegjens, J. d. O. Filho, R. Hanson, and S. Wehner. A link layer protocol for quantum networks. *SIGCOMM '19 Proceedings of the ACM Special Interest Group on Data Communication (2019) 159-173*, 2019.

[6] I. Devetak and A. Winter. Distillation of secret key and entanglement from quantum states. *Proceedings of the Royal Society A: Mathematical, Physical and engineering sciences*, 461(2053):207–235, 2005.

[7] A. K. Ekert. Quantum cryptography based on bell's theorem. *Physical review letters*, 67(6):661, 1991.

[8] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki. Quantum entanglement. *Rev. Mod. Phys.*, 81:865–942, Jun 2009.

[9] R. Jozsa. Quantum factoring, discrete logarithms, and the hidden subgroup problem. *Computing in science & engineering*, 3(2):34–43, 2001.

[10] H. Kuwakado and M. Morii. Quantum distinguisher between the 3-round feistel cipher and the random permutation. In *2010 IEEE International Symposium on Information Theory*, pages 2682–2685. IEEE, 2010.

[11] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information 10th Anniversary Edition.* Cambrige University Press, 2010.

[12] J. M. Renes and R. Renner. One-shot classical data compression with quantum side information and the distillation of common randomness or secret keys. *IEEE Transactions on Information Theory*, 58(3):1985–1991, 2012.

[13] F. Rozpendek, T. Schiet, L. P. Thinh, D. Elkouss, A. C. Doherty, and S. Wehner. Optimizing practical entanglement distillation. *Phys. Rev. A*, 97:062333, Jun 2018.

[14] V. Scarani, A. Acin, G. Ribordy, and N. Gisin. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. *Physical review letters*, 92(5):057901, 2004.

[15] P. W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th annual symposium on foundations of computer science*, pages 124–134. Ieee, 1994.

[16] P. W. Shor and J. Preskill. Simple proof of security of the bb84 quantum key distribution protocol. *Physical review letters*, 85(2):441, 2000.

[17] D. R. Simon. On the power of quantum computation. *SIAM journal on computing*, 26(5):1474–1483, 1997.

[18] R. Wolf. *Quantum key distribution.* Springer International Publishing, 2021.