

# Quantum Cryptography

Short notes, WS 2010/11

Last Update: February 2, 2011

**Important note:** These notes are not supposed to be self-contained. Instead, they are intended as a reminder about which topics were discussed in the lecture. If you find mistakes in these notes, please send them to [unruh@mmci.uni-saarland.de](mailto:unruh@mmci.uni-saarland.de).

## Contents

<b>1</b>	<b>Linear Algebra</b>	<b>3</b>
<b>2</b>	<b>One Qubit</b>	<b>5</b>
<b>3</b>	<b>Elitzur-Vaidman Bomb Testing</b>	<b>7</b>
<b>4</b>	<b>Larger quantum systems</b>	<b>9</b>
<b>5</b>	<b>Multi-qubit gates</b>	<b>10</b>
<b>6</b>	<b>Composite Systems</b>	<b>12</b>
<b>7</b>	<b>Sets of Elementary Gates</b>	<b>13</b>
<b>8</b>	<b>The Deutsch-Jozsa Algorithm</b>	<b>14</b>
<b>9</b>	<b>Density Operators</b>	<b>16</b>
<b>10</b>	<b>Partial Trace and Purification</b>	<b>19</b>
<b>11</b>	<b>Quantum Operations</b>	<b>19</b>
<b>12</b>	<b>Trace distance</b>	<b>21</b>
<b>13</b>	<b>Quantum key distribution</b>	<b>23</b>
<b>14</b>	<b>Quantum Commitments</b>	<b>31</b>
	14.1 Bounded quantum storage model . . . . .	34
<b>15</b>	<b>Zero-knowledge proofs</b>	<b>37</b>

<b>16 Factoring</b>	<b>41</b>
<b>Symbol index</b>	<b>46</b>

# Quantum Cryptography

Lecture on 2010-10-26

## 1 Linear Algebra

In the following, we refresh the basic definitions from linear algebra that will be needed during the course. In all definitions, we will restrict our attention to the finite dimensional case only.

**Definition 1 (Hilbert space)** *The  $n$ -dimensional Hilbert space is  $\mathbb{C}^n$ , the  $n$ -dimensional complex vector space.<sup>1</sup>*

$\mathbb{C}^n$  is endowed with the following inner product:

$$\langle \Psi, \Phi \rangle := \sum_{i=1}^n \Psi_i^* \Phi_i$$

where  $x^*$  is the complex conjugate of  $x$ .<sup>2</sup>

The (Euclidean) norm  $\|\cdot\|$  is defined by

$$\|\Psi\| := \sqrt{\langle \Psi, \Psi \rangle} = \sqrt{\sum_{i=1}^n \Psi_i^* \Psi_i} = \sqrt{\sum_{i=1}^n |\Psi_i|^2}.$$

We call two vectors  $\Psi$  and  $\Phi$  orthogonal if  $\langle \Psi, \Phi \rangle = 0$ . We call  $\Psi$  orthogonal to a subspace  $V \subseteq \mathbb{C}^n$  if  $\Psi$  is orthogonal to all  $x \in V$ .

Furthermore, we call a vector *normalised* if  $\|\Psi\| = 1$ , and we call a *set* of vectors *orthogonal* if they are pairwise orthogonal, and we call a set of vectors *orthonormal* if they are all normalised and pairwise orthogonal.

**Definition 2 (Conjugate transpose)** *Given a matrix  $M \in \mathbb{C}^{n \times n}$ , we define  $M^\dagger$  as the complex conjugate of the transposition of  $M$ , i.e.,  $(M^\dagger)_{ij} = (M_{ji})^*$ . (This is the analogue of transposition.)*

We have  $(M^\dagger)^\dagger = M$  and  $\langle Mx, y \rangle = \langle x, M^\dagger y \rangle$  (and vice-versa).

<sup>1</sup>Or any complex vector space isomorphic to  $\mathbb{C}^n$

<sup>2</sup>I.e.,  $(a + bi)^* = a - bi$ .

**Definition 3 (Dirac notation)** In the Dirac notation, a vector  $\Psi$  in  $\mathbb{C}^n$  is written  $|\Psi\rangle$ . By  $\langle\Psi|$  we denote the function mapping  $|\Phi\rangle$  to  $\langle\Psi, \Phi\rangle$  (or equivalently:  $\langle\Psi|$  is the row vector  $|\Psi\rangle^\dagger$ ).

In particular, we can now write  $\langle\Psi|\Phi\rangle$  for the inner product  $\langle\Psi, \Phi\rangle$ . And for the projection onto  $P_V$  onto  $V = \text{span } \Psi$  we write  $P_V = |\Psi\rangle\langle\Psi|$ . (Try it out and evaluate  $P_V|\Phi\rangle$ !)

**Definition 4 (Trace)** The trace  $\text{tr } M$  of a matrix  $M \in \mathbb{C}^{n \times n}$  is  $\sum_i M_{ii}$ .

The trace can also be computed as  $\sum_i \langle i|M|i\rangle$  for any orthonormal basis  $|1\rangle, \dots, |n\rangle$  of  $\mathbb{C}^n$ .

**Definition 5 (Hermitian matrices)** A matrix  $M \in \mathbb{C}^{n \times n}$  is called Hermitian, if  $M = M^\dagger$ . (This is the analogue of symmetric matrices.)

A Hermitian matrix  $M$  can be diagonalised, i.e., there is an orthonormal basis  $|1\rangle, \dots, |n\rangle$  such that  $M = \sum_i \lambda_i |i\rangle\langle i|$  where  $\lambda_i$  are the eigenvalues of  $M$ .

**Definition 6 (Positive matrices)** A matrix  $M \in \mathbb{C}^{n \times n}$  is positive if for all  $|\Psi\rangle \in \mathbb{C}^n$  we have  $\langle\Psi|M|\Psi\rangle \geq 0$ .

Note that positive is meant in the sense of positive semidefinite (or nonnegative), i.e., we allow, e.g.,  $M = 0$ .

A positive Hermitian matrix has only nonnegative eigenvalues  $\lambda_i \geq 0$ .

**Definition 7 (Absolute value of a matrix)** For a positive Hermitian matrix  $M$ , let  $\sqrt{M}$  be the positive matrix satisfying  $(\sqrt{M})^\dagger(\sqrt{M}) = M$ . For a (not necessarily positive or Hermitian) matrix  $M$ , we define  $|M| := \sqrt{M^\dagger M}$ .

The matrix  $|M|$  is always positive Hermitian. For a positive Hermitian matrix  $M$ , we have  $|M| = M$ . For a diagonal matrix  $M$ , we get  $|M|$  by taking the absolute value of every element on the diagonal.

For a positive Hermitian  $M$ , we can compute  $\sqrt{M}$  by first diagonalising  $M$  as  $UDU^\dagger$  (with unitary  $U$  and diagonal  $D$ ), and then computing  $\sqrt{D}$  (by taking the square root of each diagonal element individually) and then computing  $\sqrt{M} = U\sqrt{D}U^\dagger$ . Since for a matrix  $M$ , we have that  $M^\dagger M$  is positive Hermitian, we can use this procedure to compute  $|M|$ .

**Definition 8 (Unitary matrices)** A matrix  $M \in \mathbb{C}^{n \times n}$  is unitary if  $M^\dagger M = MM^\dagger = I$  where  $I$  is the identity matrix. (Unitary matrices are the analogue to rotation matrices.)

Note: If  $M$  is unitary, then  $\|Mx\| = \|x\|$  and  $\langle Mx, My\rangle = \langle x, y\rangle$ .

**Definition 9 (Projections)** A matrix  $M \in \mathbb{C}^{n \times n}$  is a projection if for all  $x$  we have  $MMx = Mx$  (or equivalently,  $MM = M$ ).

The orthogonal projection  $P_V$  onto a subspace  $V \subseteq \mathbb{C}^n$  is defined by  $P_V(u + v) = v$  where  $v \in V$  and  $u$  is orthogonal to  $V$ . (Note that any state  $x \in \mathbb{C}^n$  can be represented uniquely as such a sum  $x = u + v$ .)

For a one-dimensional subspace  $V = \text{span}\{v\}$  with  $\|v\| = 1$ , we have that  $P_V x = v\langle v, x \rangle$ .

**Lemma 1 (Singular value decomposition)** For any square matrix  $A \in \mathbb{C}^{n \times n}$ , there are unitary matrices  $U, V \in \mathbb{C}^{n \times n}$  and a diagonal matrix  $D \in \mathbb{C}^{n \times n}$  with only nonnegative real entries such that  $A = UDV$ .

## 2 One Qubit

**Definition 10 (Qubit)** A single qubit is represented by a vector  $|\Psi\rangle \in \mathbb{C}^2$  with  $\| |\Psi\rangle \| = 1$ .

There are two kinds of operations on qubits, unitary transformations and measurements.

**Definition 11 (Unitary transformations on qubit)** A unitary transformation on a qubit  $|\Psi\rangle$  is represented by a unitary matrix  $U \in \mathbb{C}^{2 \times 2}$ . The qubit after the transformation is  $U|\Psi\rangle$ .

In the case of polarisation, a typical transformation would be to rotate the polarisation by an angle of  $\alpha$ . In this case we have

$$U = \begin{pmatrix} \cos \alpha & \sin \alpha \\ -\sin \alpha & \cos \alpha \end{pmatrix}$$

which can be easily verified to be unitary.

**Definition 12 (Projective measurements)** A projective measurement on a qubit is defined by two orthonormal vectors  $|yes\rangle$  and  $|no\rangle$ . The outcomes of the measurement can be yes or no.<sup>3</sup>

When applying the measurement to a qubit  $|\Psi\rangle$ , the probability for the yes outcome is  $|\langle yes|\Psi\rangle|^2$ , and the probability for the no outcome is  $|\langle no|\Psi\rangle|^2$ .

In case of a yes outcome, the resulting state is  $|yes\rangle$ , and in case of a no outcome, the resulting state is  $|no\rangle$ .<sup>4</sup>

<sup>3</sup>Of course, the labelling yes/no is arbitrary. Any other two labels are possible.

<sup>4</sup>Up to a scalar factor of absolute value 1. To be completely exact, the state after measuring yes is  $\frac{\langle yes|\Psi\rangle}{|\langle yes|\Psi\rangle|} \cdot |yes\rangle$  (and analogous for no), but this should not worry us now. Furthermore, scalar factors (called a *global phase*) do not have physical meaning anyway.

An example for a measurement is a polarising filter. If the filter lets only vertically polarised light through, it corresponds to a measurement with  $|\text{yes}\rangle = |\uparrow\rangle$  and  $|\text{no}\rangle = |\leftrightarrow\rangle$ , and a yes-outcome corresponds to the fact that the photon passes the filter. In this case, the resulting photon will be vertically polarised (i.e., in the  $|\uparrow\rangle$  state). (In the no-outcome, the photon is destroyed, so talking about the resulting photon does not make sense in that case.)

A few typical unitary transformations on qubits are:

**Definition 13 (Hadamard)** *The Hadamard gate (usually denoted  $H$ ) is defined by*

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

*or equivalently*

$$\begin{aligned} H|0\rangle &= \frac{1}{\sqrt{2}}(|1\rangle + |0\rangle) \\ H|1\rangle &= \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{aligned}$$

The Hadamard gate is useful for introducing superpositions as it takes a classical bit ( $|0\rangle$  or  $|1\rangle$ ) and transforms it into a superposition.

**Definition 14 (Bit flip)** *The bit flip (also called not-gate or X-gate) is defined by*

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

*or equivalently*

$$\begin{aligned} X|0\rangle &= |1\rangle \\ X|1\rangle &= |0\rangle \end{aligned}$$

The bit flip corresponds to a negation. It can, however, be applied in superposition.

**Definition 15 (Rotation)** *The rotation by angle  $\theta$  is defined by*

$$R_\theta = \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix}$$

*or equivalently*

$$\begin{aligned} R_\theta|0\rangle &= \cos \theta|0\rangle + \sin \theta|1\rangle \\ R_\theta|1\rangle &= -\sin \theta|0\rangle + \cos \theta|1\rangle \end{aligned}$$

**Definition 16 (Phase shift)** *The phase shift  $S$  is defined by*

$$S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$

or equivalently

$$\begin{aligned}S|0\rangle &= |0\rangle \\ S|1\rangle &= i|1\rangle\end{aligned}$$

More generally, we can parametrise the phase shift by an angle  $\theta$ :

$$S_\theta = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix}$$

or equivalently

$$\begin{aligned}S_\theta|0\rangle &= |0\rangle \\ S_\theta|1\rangle &= e^{i\theta}|1\rangle\end{aligned}$$

Note that  $S = S_{\frac{\pi}{2}}$ .

**Further reading:** [NC00, Section 1.2.1, 1.3.1], and [NC00, Section 4.2] for the single qubit gates.

### 3 Elitzur-Vaidman Bomb Testing

A *beam splitter* is a device into which a photon can enter in two positions (call them *up* and *down*), and exit in two positions (call them *up* and *down*, too). The input to the beam splitter is a qubit that is represented as a superposition between  $|\text{up}\rangle$  and  $|\text{down}\rangle$ . Then the beam splitter performs the following linear transformation  $B_{\frac{\pi}{4}}$ :

$$\begin{aligned}B_{\frac{\pi}{4}}|\text{up}\rangle &= \frac{1}{\sqrt{2}}(|\text{up}\rangle + |\text{down}\rangle) \\ B_{\frac{\pi}{4}}|\text{down}\rangle &= \frac{1}{\sqrt{2}}(-|\text{up}\rangle + |\text{down}\rangle)\end{aligned}$$

Another variant of the beam splitter is given by the linear transformation

$$\begin{aligned}B_{-\frac{\pi}{4}}|\text{up}\rangle &= \frac{1}{\sqrt{2}}(|\text{up}\rangle - |\text{down}\rangle) \\ B_{-\frac{\pi}{4}}|\text{down}\rangle &= \frac{1}{\sqrt{2}}(|\text{up}\rangle + |\text{down}\rangle)\end{aligned}$$

Note that  $B_{\frac{\pi}{4}}$  and  $B_{-\frac{\pi}{4}}$  are unitary, and that  $B_{\frac{\pi}{4}}B_{-\frac{\pi}{4}} = B_{-\frac{\pi}{4}}B_{\frac{\pi}{4}} = 1$ .

The *Elitzur-Vaidman bomb tester* is the following construction. We are given a box that may or may not contain a bomb. The bomb explodes if a single photon falls onto it. We want to find out whether the box contains a bomb. To do so, we take a  $B_{\frac{\pi}{4}}$  beam splitter and send an  $|\text{up}\rangle$  photon through it. The state that comes out of the beam splitter is  $\frac{1}{\sqrt{2}}(|\text{up}\rangle + |\text{down}\rangle)$ . Now we put the box in the path of the  $|\text{down}\rangle$  photon. Assume for the moment that a bomb is in that box. Then the box constitutes a measurement whether the photon takes the up- or the down-path. Since the state of

the photon is  $\frac{1}{\sqrt{2}}(|\text{up}\rangle + |\text{down}\rangle)$ , the measurement outcome will be up or down, each with probability  $\frac{1}{2}$ . In the case of a down-outcome, the bomb explodes. In the case of an up-outcome, the resulting state is  $|\text{up}\rangle$  (i.e., the photon takes the upper path). Then the photon passes the  $B_{-\pi/4}$  beam splitter and is transformed into  $\frac{1}{\sqrt{2}}(|\text{up}\rangle - |\text{down}\rangle)$ . Now we measure whether the photon is in the up state or the down state (by simply putting a photon detector in at the end of both paths). With probability  $\frac{1}{2}$  the photon will be up (conditioned on the fact that the bomb did not explode), with probability  $\frac{1}{2}$  it will be down. Altogether we get the following predictions for this experiment.

Event	Probability
Bomb explodes	$\frac{1}{2}$
Photon is in up-path	$\frac{1}{4}$
Photon is in down-path	$\frac{1}{4}$

On the other hand, if no bomb is in the box, the box has no effect on the photon. In this case, the experiment consists of two beam splitters  $B_{\pi/4}$  and  $B_{-\pi/4}$  in a row. Because these beam splitters are inverses of each other, they cancel each other out, and the photon coming out of the second beam splitter will be in state  $|\text{up}\rangle$ . Thus in this case we get the following probabilities:

Event	Probability
Bomb explodes	0
Photon is in up-path	1
Photon is in down-path	0

In other words, if the outcome of the experiment is “down”, we know for sure that there is a bomb in the box without having caused it to explode. Unfortunately, with probability  $\frac{1}{2}$  the bomb still explodes. The experiment can, however, be improved to make the probability of the bomb exploding arbitrarily small (homework).

**Further reading:** For the modelling of the beam splitter: [NC00, Section 7.4] (uses some physics we have not discussed yet). For the bomb tester: [Wik, Elitzur-Vaidman bomb-tester].

[NC00] M. Nielsen and I. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, Cambridge, 2000.

[Wik] Wikipedia contributors. Wikipedia, the free encyclopedia (english edition). <http://en.wikipedia.org>.

# Quantum Cryptography

Lecture on 2010-11-02

## 4 Larger quantum systems

**Definition 17 (Quantum states)** An  $n$ -dimensional quantum state is represented by a vector  $|\Psi\rangle \in \mathbb{C}^n$  with  $\| |\Psi\rangle \| = 1$  (here  $\mathbb{C}^n$  is a Hilbert space).

In most cases, we assume some canonical orthonormal basis of  $\mathbb{C}^n$  (representing the classical possibilities of the system) which we call the *computational basis*. We then use the following convention: If  $|b_1\rangle, \dots, |b_n\rangle$  are the basis vectors, and  $b_1, \dots, b_n$  are some labels we assign to these vectors sorted according to some natural ordering (e.g., for an  $m$ -qubit system (i.e.,  $n = 2^m$ )  $b_i$  is the bitstring  $b_i \in \{0, 1\}^m$  which is the binary representation of  $i - 1$ ), then  $|b_i\rangle = (0, \dots, 0, 1, 0, \dots, 0)^t$  where the 1 is at the  $i$ -th position.

There are two kinds of operations on quantum states, unitary transformations and measurements.

**Definition 18 (Unitary transformation)** A unitary transformation on a quantum state  $|\Psi\rangle \in \mathbb{C}^n$  is represented by a unitary matrix  $U \in \mathbb{C}^{n \times n}$ . The state after the transformation is  $U|\Psi\rangle$ .

**Definition 19 (Measurement)** A (projective) measurement on a Hilbert space  $\mathcal{H}$  is specified by a family  $\{P_i\}_{i \in I}$  of orthogonal projections on  $\mathcal{H}$  labelled with the possible measurement outcomes  $i \in I$ . The projections have to be pairwise orthogonal, i.e.,  $P_i P_j = 0$  for  $i \neq j$ . And the projections sum to 1, i.e.,  $\sum_i P_i = 1_{\mathcal{H}}$  where  $1_{\mathcal{H}}$  is the identity on  $\mathcal{H}$ .

When measuring a state  $|\Psi\rangle \in \mathcal{H}$ , the outcome  $i$  occurs with probability

$$\|P_i|\Psi\rangle\|^2.$$

If the outcome  $i$  occurs, the state after the measurement (post-measurement state) is

$$\frac{P_i|\Psi\rangle}{\|P_i|\Psi\rangle\|}.$$

A special case of a measurement is the complete measurement in which every projection is the projection onto a one-dimensional subspace.

Note that we can also represent a measurement by giving the images  $V_i$  of the projectors  $P_i$  instead of the projectors themselves. This is equivalent, as the  $P_i$  can be recovered from  $V_i$  and vice versa.

**Definition 20 (Complete measurement)** A complete measurement on  $\mathcal{H}$  is specified by an orthonormal basis  $B = \{|i\rangle\}_{i \in I}$  of  $\mathcal{H}$  labelled with the possible measurement outcomes  $i \in I$ .

When measuring a state  $|\Psi\rangle \in \mathcal{H}$ , the outcome  $i$  occurs with probability

$$|\langle i|\Psi\rangle|^2.$$

and the corresponding post-measurement state is

$$\frac{\langle i|\Psi\rangle}{|\langle i|\Psi\rangle|} \cdot |i\rangle$$

(which is  $|i\rangle$  up to a (physically irrelevant) scalar factor  $\frac{\langle i|\Psi\rangle}{|\langle i|\Psi\rangle|}$  of absolute value 1, the global phase).

Note that the complete measurement with basis  $\{|i\rangle\}_{i \in I}$  has the same effect as the measurement with projectors  $\{P_i\}_{i \in I}$  where  $P_i := |i\rangle\langle i|$ . Thus complete measurements are a special case of measurements as in Definition 19.

**Further reading:** [NC00], Section 2.2.1, 2.2.2, and 2.2.5 for states, unitary evolution, and projective measurements, respectively. Section 2.2.7 for information in the global phase.

## 5 Multi-qubit gates

**Definition 21 (Controlled NOT)** The CNOT gate on  $\mathbb{C}^4$  is defined to be the linear operation defined by

$$\begin{aligned} \text{CNOT}|00\rangle &= |00\rangle \\ \text{CNOT}|01\rangle &= |01\rangle \\ \text{CNOT}|10\rangle &= |11\rangle \\ \text{CNOT}|11\rangle &= |10\rangle \end{aligned}$$

or equivalently

$$\text{CNOT}|a, b\rangle = |a, a \oplus b\rangle \quad (a, b \in \{0, 1\})$$

where  $\oplus$  denotes XOR.

In circuits, we write CNOT as follows:



The dot represents the controlling qubit, and the  $\oplus$  represents the qubit that is conditionally flipped. The dot does not have to be on the qubit above the  $\oplus$ . For example,



represents the operation defined by

$$|a, b, c\rangle \mapsto |a \oplus c, b, c\rangle \quad (a, b, c \in \{0, 1\})$$

**Definition 22 (SWAP)** The SWAP gate on  $\mathbb{C}^4$  is defined to be the linear operation defined by

$$\text{SWAP}|a, b\rangle = |b, a\rangle.$$

The swap gate is represented by



Again, the two  $\otimes$  do not have to be on adjacent lines.

**Definition 23 (Toffoli)** The Toffoli gate on  $\mathbb{C}^8$  is defined to be the linear operation defined by

$$\text{Toffoli}|a, b, c\rangle = |a, b, (a \cdot b) \oplus c\rangle$$

where  $\cdot$  is the multiplication modulo 2, or equivalently, the and-operation.

The Toffoli gate is usually represented as follows:

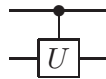


As with the CNOT, the two dots can be on arbitrary lines, not only those adjacent to the  $\oplus$ . Furthermore, the symbol generalises to more than two controlling qubits in the obvious way.

**Definition 24 (Controlled- $U$ )** Given a unitary transformation  $U \in \mathbb{C}^n$ , the controlled- $U$  gate  $C(U)$  is defined to be the linear operation on  $\mathbb{C}^{2n}$  defined by

$$\begin{aligned} C(U)|0, j\rangle &= |0, j\rangle \\ C(U)|1, j\rangle &= |1\rangle \otimes U|j\rangle. \end{aligned}$$

The controlled- $U$  is depicted as follows:



Again, the dot can be on an arbitrary qubit.

**Further reading:** [NC00], Section 4.3

## 6 Composite Systems

**Definition 25 (Tensor product)** Given two Hilbert spaces  $\mathbb{C}^n, \mathbb{C}^m$  with orthonormal bases  $B_1 = \{|i\rangle\}, B_2 = \{|j\rangle\}$ , the tensor product (or Kronecker product)  $\mathbb{C}^n \otimes \mathbb{C}^m$  is the Hilbert space  $\mathbb{C}^{nm}$  with basis  $B_1 \times B_2 = \{|i, j\rangle\}$ .<sup>5</sup>

Given two vectors  $|\Psi_1\rangle = \sum_i \alpha_i |i\rangle \in \mathbb{C}^n$  and  $|\Psi_2\rangle = \sum_j \beta_j |j\rangle \in \mathbb{C}^m$ , their tensor product is given by

$$|\Psi_1\rangle \otimes |\Psi_2\rangle = \sum_{i,j} \alpha_i \beta_j |i, j\rangle \in \mathbb{C}^n \otimes \mathbb{C}^m.$$

Given two linear operations  $M_1 : \mathbb{C}^n \rightarrow \mathbb{C}^n$  and  $M_2 : \mathbb{C}^m \rightarrow \mathbb{C}^m$ , we define the linear operation  $M_1 \otimes M_2$  to be the unique linear operation satisfying

$$(M_1 \otimes M_2)|i, j\rangle = (M_1|i\rangle) \otimes (M_2|j\rangle).$$

We abbreviate  $x \otimes \dots \otimes x$  ( $n$  components) as  $x^{\otimes n}$ .

**Definition 26 (Composite states)** Given  $n$  quantum states  $|\Psi_i\rangle \in \mathcal{H}_i$ , the composite system consisting of  $n$  independent subsystems in states  $|\Psi_i\rangle$ , the state of the overall system is

$$|\Psi_1\rangle \otimes \dots \otimes |\Psi_n\rangle \in \mathcal{H}_1 \otimes \dots \otimes \mathcal{H}_n.$$

**Definition 27 (Composite unitary operations)** Given a composite system  $\mathcal{H}_1 \otimes \mathcal{H}_2$ , performing the unitary operation  $U_1$  on  $\mathcal{H}_1$  and  $U_2$  on  $\mathcal{H}_2$  independently is equivalent to performing the unitary operation  $U_1 \otimes U_2$  on  $\mathcal{H}_1 \otimes \mathcal{H}_2$ .

A special case is performing an operation  $U$  only on  $\mathcal{H}_1$  and not touching  $\mathcal{H}_2$ . This is represented by  $U \otimes I$  where  $I$  is the identity.

[NC00] M. Nielsen and I. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, Cambridge, 2000.

---

<sup>5</sup>There exists a more general category theoretical definition using a universal property, but for our purposes this specialisation is sufficient.

# Quantum Cryptography

Lecture on 2010-11-09

**Definition 28 (Composite measurements)** *Given a measurement  $M_1$  specified by projections  $P_1, \dots, P_n$  on  $\mathcal{H}_1$  and a measurement  $M_2$  specified by projections  $P'_1, \dots, P'_m$  on  $\mathcal{H}_2$ , performing each of the measurements independently is equivalent to performing the measurement  $M$  specified by the projections  $P_{ij} := P_i \otimes P_j$  with  $i = 1, \dots, n$  and  $j = 1, \dots, m$ . (I.e., the possible outcomes of  $M$  are pairs  $i, j$  with  $i = 1, \dots, n$  and  $j = 1, \dots, m$ .)*

Note that the measurement that does nothing and has no effect on the state is given by the single projector  $I$  (the identity). Thus a measurement  $M$  on  $\mathcal{H}_1$  only extends to a measurement  $M'$  on  $\mathcal{H}_1 \otimes \mathcal{H}_2$  as follows: If  $M$  consists of  $P_1, \dots, P_n$ , then  $M'$  consists of  $P_1 \otimes I, \dots, P_n \otimes I$ .

**Further reading:** [NC00], Section 2.2.8.

## 7 Sets of Elementary Gates

The following theorem is a corollary of the so-called Solovay-Kitaev theorem:

**Theorem 1** *Fix  $\varepsilon > 0$ . Fix a unitary operation  $U$  operating on  $\mathbb{C}^{2^n}$  (an  $n$ -qubit operation).*

*Then there exists a  $\varphi \in \mathbb{C}$  with  $|\varphi| = 1$  (a global phase factor), and a quantum circuit  $C$  of size  $\text{polylog}(1/\varepsilon) + \text{exp}(n)$  containing only the gates CNOT,  $H$  (Hadamard),  $R_{\frac{\pi}{8}}$  (rotation by  $\frac{\pi}{8}$ ),  $S$  (phase shift) such that the following holds:*

*For all  $|\Psi\rangle \in \mathbb{C}^{2^n}$  with  $\| |\Psi\rangle \| = 1$ , we have that*

$$\| \varphi U |\Psi\rangle - U_C |\Psi\rangle \| \leq \varepsilon$$

*where  $U_C$  is the unitary transformation implemented by the circuit  $C$ .*

In other words, we can approximate any unitary transformation  $U$  by a circuit containing only the above-mentioned gates (up to a global phase factor  $\varphi$  which is physically irrelevant). The construction is very efficient in terms of the error  $\varepsilon$ , but becomes inefficient for larger systems (exponential in the number  $n$  of qubits).

As a consequence, we may assume any finite set of elementary gates that is powerful enough to implement CNOT, Hadamard, Rotation by  $\frac{\pi}{8}$  and phase shift (up to an

arbitrarily small error). The theorem above then implies that it does not matter which set of gates we choose. (Note that in a finite set of gates, the number of qubits a gate operates on is  $n = O(1)$ , so the exponential term  $\exp(n)$  in the complexity of the construction vanishes.)

**Fault tolerant computation.** In the above, we assumed that we are given error free gates, i.e., the gates always implement the unitary transformation they are supposed to implement. However, in practise we will have very noisy components that introduce errors on the qubits. Fortunately, it is possible to implement quantum circuits in a fault tolerant fashion (under reasonable assumptions about the gates and the error model). Then, given gates that have an error probability of approximately  $10^{-5}$ – $10^{-6}$ , we can get almost error free computation. In the following, we always assume error free gates and communication for simplicity.

**Further reading:** [NC00], Appendix 3 for the Solovay-Kitaev theorem (which gives Theorem 1) for the case  $n = 2$ , and Section 4.5 on how to get a larger value of  $n$ .

[NC00], Section 4.6 for fault tolerant computation (needs knowledge of the preceding sections on error correcting codes).

## 8 The Deutsch-Jozsa Algorithm

**Deutsch's algorithm.** Assume we are given a function  $f : \{0, 1\} \rightarrow \{0, 1\}$ . We ask the question which of the following two cases applies:

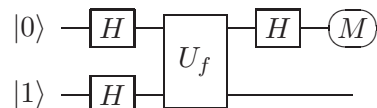
- $f$  is constant ( $f(0) = f(1)$ ), or
- $f$  is balanced ( $f(0) \neq f(1)$ ).

We further assume that  $f$  is implemented as a unitary transformation  $U_f$  on two qubits that performs the following operation:

$$U_f|x, y\rangle = |x, y \oplus f(x)\rangle \quad (x, y \in \{0, 1\})$$

(Such a unitary can be efficiently implemented if  $f$  has a poly-size classical circuit.)

Deutsch's algorithm performs the following operations:



(Here  $\text{---}\overline{M}$  denotes a complete measurement of the first qubit in the computational basis, i.e., we look whether it is  $|0\rangle$  or  $|1\rangle$ .)

Computing the output of this circuit, we get the following:

- If  $f$  is constant, then with probability 1 the measurement  $M$  has outcome 0.

- If  $f$  is balanced, then with probability 1 the measurement  $M$  has outcome 1.

Thus with one evaluation of  $f$  we have determined whether  $f$  is constant or balanced. Classically, we would have needed two evaluations.

An extension of this algorithm, the Deutsch-Jozsa algorithm, can even handle functions  $f : \{0,1\}^n \rightarrow \{0,1\}$  and decide whether they are constant or balanced (same number of 0 and 1 outputs). It needs only one evaluation of  $f$ . (There is no guarantee if  $f$  is neither constant nor balanced.)

**Further reading:** [NC00, Section 1.4.3].

[NC00] M. Nielsen and I. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, Cambridge, 2000.

# Quantum Cryptography

Lecture on 2010-11-16

## 9 Density Operators

Intuitively, a quantum ensemble is a probability distribution on quantum states.

**Definition 29 (Quantum ensemble)** A quantum ensemble  $E$  over a Hilbert space  $\mathcal{H}$  is a (possibly infinite) set of pairs  $E = \{(|\Psi_i\rangle, p_i)\}_i$  satisfying:

- For all  $i$  we have  $|\Psi_i\rangle \in \mathcal{H}$ .
- The vectors  $|\Psi_i\rangle$  are normalized ( $\| |\Psi_i\rangle \| = 1$ ).
- We have  $p_i \geq 0$  for all  $i$  and  $\sum_i p_i = 1$ .

The interpretation is that a system is in state  $|\Psi_i\rangle$  with probability  $p_i$ .  
Operations performed on quantum states generalise to ensembles.

**Definition 30 (Unitary transformation)** Let  $U$  be a unitary matrix on  $\mathcal{H}$ . Let  $E = \{(|\Psi_i\rangle, p_i)\}_i$  be an ensemble over  $\mathcal{H}$ .

Then applying  $U$  to the ensemble  $E$  leads to the ensemble

$$UE = \{(U|\Psi_i\rangle, p_i)\}_i.$$

**Definition 31 (Measurement)** Let  $M = \{Q_1, \dots, Q_n\}$  be a projective measurement over  $\mathcal{H}$  consisting of projectors  $Q_i$ . Let  $E = \{(|\Psi_i\rangle, p_i)\}_i$  be an ensemble over  $\mathcal{H}$ .

If we measure the state described by  $E$  with  $M$ , the outcome  $j$  has probability

$$\Pr[\text{Outcome } j] = \sum_i p_i \|Q_j |\Psi_i\rangle\|^2.$$

After measuring the outcome  $j$ , the system state is described by the following ensemble:

$$\left\{ \left( \frac{Q_j |\Psi_i\rangle}{\|Q_j |\Psi_i\rangle\|}, \frac{p_i \|Q_j |\Psi_i\rangle\|^2}{\Pr[\text{Outcome } j]} \right) \right\}_i.$$

**Definition 32 (Extending the state space)** Let  $E = \{(|\Psi_i\rangle, p_i)\}_i$  be an ensemble over  $\mathcal{H}$ . Let  $|\Gamma\rangle \in \mathcal{H}'$ ,  $\| |\Gamma\rangle \| = 1$ .

Then extending the state described by  $E$  by adding another quantum system described by  $|\Gamma\rangle$  results in the following ensemble over  $\mathcal{H} \otimes \mathcal{H}'$ :

$$E \otimes |\Gamma\rangle = \{(|\Psi_i\rangle \otimes |\Gamma\rangle, p_i)\}_i.$$

**Definition 33 (Physical indistinguishability)** We call two ensembles physically indistinguishable if all sequences of operations according to Definitions Definition 30, Definition 31, and Definition 32 lead to the same probabilities of measurement outcomes.

**Further reading:** [NC00, Section 2.4.1].

A density operator is a compact representation of a quantum ensemble. This representation loses some information contained in the description of an ensemble,<sup>6</sup> but it still contains enough information to predict the outcome of physical experiments.

**Definition 34 (Density operator)** Let  $E = \{(|\Psi_i\rangle, p_i)\}_i$  be a quantum ensemble over  $\mathcal{H}$ . The density operator (density matrix, mixed state) corresponding to  $E$  is the linear transformation  $\rho_E$  on  $\mathcal{H}$  defined as follows:

$$\rho_E = \sum_i p_i |\Psi_i\rangle\langle\Psi_i|.$$

We call  $\rho$  a density operator over  $\mathcal{H}$  if it is a density operator for some quantum ensemble  $E$  over  $\mathcal{H}$ . By  $S(\mathcal{H})$  we denote the set of all density operators over  $\mathcal{H}$ .

Note: The usage of the words *mixed state* and *pure state* is ambiguous. There are two usages:

- A mixed state is a density operator  $\rho \in S(\mathcal{H})$  and a pure state is a state described by a vector  $|\Psi\rangle \in \mathcal{H}$ .
- A pure state is a density operator of the form  $|\Psi\rangle\langle\Psi|$  (i.e., a density operator corresponding to an ensemble with only one entry), and a mixed state is a density operator that cannot be written as  $|\Psi\rangle\langle\Psi|$ .

**Lemma 2** The set  $S(\mathcal{H})$  consists of all positive Hermitian matrices with trace 1.

Due to its mathematical simplicity, one usually takes Lemma 2 as the definition of density operators.

**Definition 35 (Unitary transformation)** Let  $U$  be a unitary matrix on  $\mathcal{H}$ . Let  $\rho \in S(\mathcal{H})$  be a density operator over  $\mathcal{H}$ .

Then applying  $U$  to the state  $\rho$  leads to the state  $U\rho U^\dagger$ .

**Definition 36 (Measurement)** Let  $M = \{Q_1, \dots, Q_n\}$  be a projective measurement over  $\mathcal{H}$  consisting of projectors  $Q_i$ . Let  $\rho \in S(\mathcal{H})$  be a density operator over  $\mathcal{H}$ .

If we measure the state  $\rho$  with  $M$ , the outcome  $j$  has probability

$$\Pr[\text{Outcome } j] = \text{tr } Q_j \rho Q_j^\dagger = \text{tr } Q_j \rho.$$

After measuring the outcome  $j$ , the system state is  $\frac{Q_j \rho Q_j^\dagger}{\text{tr } Q_j \rho Q_j^\dagger}$ .

---

<sup>6</sup>E.g., the following two ensembles both have the same representation as a density operator:  $\{(|0\rangle, \frac{1}{2}), (|1\rangle, \frac{1}{2})\}$  and  $\{(|+\rangle, \frac{1}{2}), (|-\rangle, \frac{1}{2})\}$  with  $|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$  and  $|-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$ .

**Definition 37 (Extending the state space)** Let  $\rho \in S(\mathcal{H})$  be a density operator over  $\mathcal{H}$ .

Then extending the state  $\rho$  by adding another quantum system described by  $\sigma \in S(\mathcal{H}')$  results in the density operator  $\rho \otimes \sigma$  over  $\mathcal{H} \otimes \mathcal{H}'$

The following theorem states that density operators characterise physical indistinguishability of quantum ensembles.

**Theorem 2** Let  $E, E'$  be quantum ensembles over  $\mathcal{H}$  and  $\rho, \rho'$  the corresponding density operators. Then  $E$  and  $E'$  are physically indistinguishable if and only if  $\rho = \rho'$ .

Since in physics, there is no reason to assume that some distinction exists if it is principally impossible to measure it, one usually directly says that the physical system is in the state  $\rho$  and does not assume that there is some hidden ensemble behind this state that contains more information than the density operator  $\rho$ .

**Further reading:** [NC00, Section 2.4.1 and 2.4.2]. Note that they define a density operator as being positive Hermitian (and omit the condition  $\text{tr } \rho = 1$ ).

[NC00] M. Nielsen and I. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, Cambridge, 2000.

# Quantum Cryptography

Lecture on 2010-11-22

## 10 Partial Trace and Purification

**Definition 38 (Partial trace)** Let a bipartite system  $\mathcal{H}_A \otimes \mathcal{H}_B$  be given.

The partial trace  $\text{tr}_B : S(\mathcal{H}_A \otimes \mathcal{H}_B) \rightarrow S(\mathcal{H}_A)$  is the linear transformation defined by

$$\text{tr}_B \sigma \otimes \tau = \sigma \cdot \text{tr} \tau \quad \sigma \in S(\mathcal{H}_A), \tau \in S(\mathcal{H}_B).$$

We say that  $\mathcal{H}_B$  (or just  $B$ ) is traced out. Analogously we can also trace out  $\mathcal{H}_A$  or consider multipartite systems.

Given a state  $\rho \in S(\mathcal{H}_A \otimes \mathcal{H}_B)$ , the state  $\rho^A := \text{tr}_B \rho$  describes the state resulting from destroying (or locking away) the  $B$ -part of the system. Or equivalently,  $\rho^A$  represents all information that can be extracted about the state  $\rho$  from the  $A$ -part of the system alone.

**Theorem 3 (Purification)** Let a state  $\rho \in S(\mathcal{H}_A)$  be given. Then for any space  $\mathcal{H}_B$  such that  $\dim \mathcal{H}_B \geq \dim \mathcal{H}_A$ , there is a quantum state  $|\Psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$  such that

$$\text{tr}_B |\Psi\rangle\langle\Psi| = \rho.$$

We call  $\Psi$  a *purification* of  $\rho$ . Note that the purification is not unique.

This theorem means that any mixed state can be considered as a part of some larger pure state (we usually call the added subsystem  $\mathcal{H}_B$  the *environment*).

In many cases, analysing a pure system may be simpler than analysing a mixed one. In these cases Theorem 3 allows to simplify the analysis.

**Further reading:** [NC00, Section 2.4.3] for the partial trace and [NC00, Section 2.5] for purification.

## 11 Quantum Operations

**Definition 39 (Quantum Operations)** A quantum operation  $\mathcal{E}$  is a map  $\mathcal{E} : S(\mathcal{H}) \rightarrow S(\mathcal{H}')$  of the form

$$\mathcal{E}(\rho) = \sum_k E_k \rho E_k^\dagger \tag{1}$$

where  $E_k : \mathcal{H} \rightarrow \mathcal{H}'$  are linear operators satisfying  $\sum_k E_k^\dagger E_k = I$  (where  $I$  is the identity on  $\mathcal{H}$ ).

We sometimes write  $\mathcal{E} = \{E_k\}_k$  to denote the fact that  $\mathcal{E}$  is the operation defined by (1). The operators  $E_k$  are called the Kraus operators of  $\mathcal{E}$ .

Quantum operations describe all operations that can be applied to a mixed state  $\rho$ , including unitary transformations, measurements (when the outcomes are erased). Also the partial trace is an example of a quantum operation.

Quantum operations are also called *superoperators*.

**Definition 40 (Composing operations)** Let  $\mathcal{E}$  and  $\mathcal{F}$  be two quantum operations (over  $\mathcal{H}_E$  and  $\mathcal{H}_F$ , respectively). Then  $\mathcal{E} \otimes \mathcal{F}$  is the linear operation defined by

$$(\mathcal{E} \otimes \mathcal{F})(\sigma \otimes \tau) = \mathcal{E}(\sigma) \otimes \mathcal{F}(\tau).$$

Note that  $\mathcal{E} \otimes \mathcal{F}$  is a quantum operation over  $\mathcal{H}_E \otimes \mathcal{H}_F$ .

**Theorem 4**  $\mathcal{E} : S(\mathcal{H}) \rightarrow S(\mathcal{H}')$  is a quantum operation if and only if it satisfies the following three conditions:

- It is linear.
- It is trace-preserving (i.e.,  $\text{tr } \mathcal{E}(\rho) = \text{tr } \rho$ ).
- It is completely positive. That is, for any vector space  $\tilde{\mathcal{H}}$  and any positive  $\rho \in S(\mathcal{H} \otimes \tilde{\mathcal{H}})$ , we have that  $(\mathcal{E} \otimes I)(\rho)$  is positive, too. (Here  $I$  is the identity on  $\tilde{\mathcal{H}}$ .)

**Further reading:** [NC00, Section 8.2].

[NC00] M. Nielsen and I. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, Cambridge, 2000.

# Quantum Cryptography

Lecture on 2010-11-30

## 12 Trace distance

Note: In the following, we will use random variables and probability distributions interchangeably. That is, if we say “ $X$  is a probability distribution over  $A$ ”, we may then use  $X$  as a random variable taking values in  $A$  and write  $\Pr[X = a]$  for the probability assigned by the distribution  $X$  to  $a$ .

**Definition 41 (Statistical distance)** *Let  $X$  and  $Y$  be probability distributions over some (countable) set  $A$ . Then the statistical distance  $\text{SD}(X, Y)$  between  $X$  and  $Y$  is defined as*

$$\text{SD}(X, Y) := \max_{T \subseteq A} |\Pr[X \in T] - \Pr[Y \in T]|.$$

Intuitively, the statistical distance tells us how good a sample chosen according to the distribution  $X$  and a sample chosen according to  $Y$  can be distinguished by an optimal statistical test  $T$ .

**Lemma 3 (Alternative definition of statistical distance)** *Let  $X$  and  $Y$  be probability distributions over some (countable) set  $A$ . Then*

$$\text{SD}(X, Y) = \frac{1}{2} \sum_{a \in A} |\Pr[X = a] - \Pr[Y = a]|.$$

This lemma is often taken as the definition of statistical distance. However, it does not have an operational meaning like Definition 41 and it does not generalise to uncountable sets  $A$ .

The statistical distance is often used in cryptography in definitions of security against computationally unlimited adversaries: If we have some random variable  $I$  that describes what the output/communication of the protocol should ideally look like (e.g., it should be stochastically independent of the secrets used in the protocol), and the random variable  $R$  describes the actual output/communication, then one would require that  $\text{SD}(R, I)$  is sufficiently small.

**Lemma 4** • *The statistical distance  $\text{SD}$  is a metric (on the set of probability distributions over a given set  $A$ ).*

- For any (possibly randomized) function  $F$  we have that

$$\text{SD}(F(X), F(Y)) \leq \text{SD}(X, Y)$$

If  $F$  is injective, equality holds.

(This means that applying a function to some data may not make it more distinguishable, it may only lose information.)

- Let  $X, Y, Z$  be stochastically independent. Then

$$\text{SD}((X, Z), (Y, Z)) \leq \text{SD}(X, Y)$$

where  $(X, Z)$  is the random variable describing pairs chosen according to  $X$  and  $Z$ .

(Adding independent information does not help in distinguishing.)

**Definition 42 (Trace distance)** Given density operators  $\sigma, \rho \in S(\mathcal{H})$ , we define the trace distance  $\text{TD}(\sigma, \rho)$  as

$$\text{TD}(\sigma, \rho) := \frac{1}{2} \text{tr}|\sigma - \rho|.$$

Here  $|M|$  denotes the absolute value of the matrix  $M$ , see Definition 7.

**Lemma 5 (Alternative definition of the trace distance)** Given density operators  $\sigma, \rho \in S(\mathcal{H})$  we have that

$$\text{TD}(\sigma, \rho) = \max_P |\text{tr} P\sigma - \text{tr} P\rho|.$$

Here  $P$  ranges over all orthogonal projectors on  $\mathcal{H}$ .

In other words, the trace distance tells us how good we can distinguish the states  $\sigma$  and  $\rho$  by a measurement  $\{P, 1 - P\}$ . This is analogous to Definition 41 since a quantum measurement is the analogue of a statistical test in the classical world.

This analogy is made even stronger by the following lemma:

**Lemma 6** Let  $X$  and  $Y$  be probability distributions over  $A$ . Let

$$\rho_X := \sum_{a \in A} \text{Pr}[X = a] |a\rangle\langle a| \in S(\mathbb{C}^A)$$

(in other words,  $\rho_X$  describes the distribution  $X$  over classical states  $|a\rangle$ ) and  $\rho_Y$  analogous.

Then  $\text{SD}(X, Y) = \text{TD}(\rho_X, \rho_Y)$ .

**Lemma 7** • The trace distance  $\text{TD}$  is a metric (on  $S(\mathcal{H})$ ).

- For any quantum operation  $\mathcal{E}$  and any  $\sigma, \rho \in S(\mathcal{H})$  we have that

$$\text{TD}(\mathcal{E}(\sigma), \mathcal{E}(\rho)) \leq \text{TD}(\sigma, \rho).$$

If  $\mathcal{E}$  applies a unitary (i.e.,  $\mathcal{E}(\rho) := U\rho U^\dagger$ ), then equality holds.

- Let  $\sigma, \rho \in S(\mathcal{H})$  and  $\tau \in S(\mathcal{H}')$ . Then

$$\text{TD}(\sigma \otimes \tau, \rho \otimes \tau) = \text{TD}(\sigma, \rho).$$

Note the one-to-one correspondence with the properties in Lemma 4.

**Lemma 8** *Let  $P$  be an orthogonal projector on  $\mathcal{H}$ , let  $\rho \in S(\mathcal{H})$ , let  $\varepsilon \geq 0$ . Assume that  $\text{tr } P\rho \geq 1 - \varepsilon$  (i.e., the measurement  $\{P_{\text{yes}} := P, P_{\text{no}} := 1 - P\}$  returns yes with high probability).*

*Then there is a state  $\rho' \in S(\mathcal{H})$  such that*

(a)  $\text{TD}(\rho, \rho') \leq \sqrt{\varepsilon}$ .

(b) *There are states  $|\Psi_i\rangle \in \text{im } P$  and values  $p_i$  with  $\sum_i p_i = 1$ ,  $p_i \geq 0$  such that  $\rho' = \sum_i p_i |\Psi_i\rangle\langle\Psi_i|$ . (In other words, when measuring  $\rho'$ , the measurement would always return yes, i.e.,  $\rho'$  satisfies the property specified by  $P$ .)*

This lemma gives a criterion to show that the trace distance between some state  $\rho$  and some set of states  $S$  is small: Find a projector  $P$  such that  $S$  consists of all states satisfying (b). Then show that with high probability, measuring  $P$  would succeed.

**Lemma 9 (Convexity of the trace distance)** *Let  $\rho = \sum_i p_i \rho_i$  and  $\sigma = \sum_i p_i \sigma_i$  with  $\sum_i p_i = 1$ ,  $p_i \geq 0$ . Then*

$$\text{TD}(\rho, \sigma) \leq \sum_i p_i \text{TD}(\rho_i, \sigma_i).$$

This lemma is sometimes useful because it allows to remove some initial random choices from the analysis

A generalisation of this lemma that does not require the probabilities  $p_i$  to be the same in  $\rho$  and  $\sigma$  also exists.

**Further reading:** [NC00, Section 9.2.1].

## 13 Quantum key distribution

The goal of quantum key distribution (QKD, a.k.a. quantum key exchange) is the following. Two parties Alice and Bob communicate over two kinds of channels. The first channel allows to send classical information and is authenticated (but not secret). The second channel allows to send qubits but is insecure (under the control of the adversary). Alice and Bob want to agree on a secret key by communicating only over these channels such that even a computationally unlimited adversary Eve that eavesdrops on the classical channel and controls the quantum channel cannot learn anything about the key. (But Eve is allowed to disrupt the communication.)

The basic idea of quantum key exchange is the following: If Alice sends to Bob qubits encoded in a random basis (unknown to Eve), then if Eve measures the qubits she will

necessarily introduce disturbances. Then Alice and Bob perform some checks on the qubits received by Bob, and if Eve eavesdropped, we may expect some of these checks to fail and Alice and Bob will abort the protocol. Otherwise, Alice and Bob use the transmitted qubits to derive a shared secret key.

There are various desirable properties that a QKD protocol should have:

- *Provable security.* It should be possible to actually prove the security of the protocol. This is a must, otherwise we do not gain much over the classical key exchange protocols.
- *Error tolerance.* The key exchange protocol should work even if the communication channel is noisy (introduces errors). This is difficult because a noisy channel also introduces disturbances that look similar to those introduced by an eavesdropper. So if Alice and Bob abort whenever there is a disturbance, the protocol will never succeed. If they choose not to abort, Eve may learn some information.
- *Realisability.* The protocol should not need to use a quantum computer. It should be executable using only simple operations like sending polarised photons and measuring the polarisation.
- *Arbitrary distance.* The key exchange protocol should work over an arbitrary distance. In realistic channels, the noise increases with the distance. From some distance on, the noise is too large to make key exchange possible. One solution is to add relays on the way that correct errors or perform other computations, but these relays should not be assumed to be secure (they might be under the control of Eve). Quantum error correction can be used in untrusted relays, but this needs a quantum computer.

The (rough) state of the art is listed in the following table:

	BB84 and others	Lo-Chau	this lecture
Provable security	yes	yes	yes
Error tolerance	yes	yes	no
Realisability	yes	no	no
Arbitrary distance	no	yes	no

Here BB84 and other stands for most of the currently investigated protocols of which (variations of) BB84 [BB84] are the most well-known. Lo-Chau stands for the protocol proposed in [LC99].

In this lecture, we analyse a simplification of the Lo-Chau protocol that does not need to use quantum error correction.

Most research today concentrates on trying to improve the range (distance) of QKD protocol with available technology. Current records lie in the order of 250 km [SWV<sup>+</sup>09], and about 140 km through a wireless connection [SMWF<sup>+</sup>07].

[BB84] Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public-key distribution and coin tossing. In *Proceedings of IEEE International*

*Conference on Computers, Systems and Signal Processing 1984*, pages 175–179. IEEE Computer Society, 1984.

- [LC99] H. K. Lo and H. F. Chau. Unconditional Security of Quantum Key Distribution over Arbitrarily Long Distances. *Science*, 283(5410):2050, 1999. Online available at <http://arxiv.org/abs/quant-ph/9803006>.
- [NC00] M. Nielsen and I. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, Cambridge, 2000.
- [SMWF<sup>+</sup>07] T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. G. Rarity, A. Zeilinger, and H. Weinfurter. Experimental Demonstration of Free-Space Decoy-State Quantum Key Distribution over 144 km. *Physical Review Letters*, 98(1):10504, 2007. Online available at [http://www.quantum.at/uploads/media/PRL\\_98\\_\\_010504\\_\\_2007\\_.pdf](http://www.quantum.at/uploads/media/PRL_98__010504__2007_.pdf).
- [SWV<sup>+</sup>09] D. Stucki, N. Walenta, F. Vannel, R. T. Thew, N. Gisin, H. Zbinden, S. Gray, C. R. Towery, and S. Ten. High rate, long-distance quantum key distribution over 250 km of ultra low loss fibres. *New Journal of Physics*, 11(7):075003, 2009.

## Quantum Cryptography

Lecture on 2010-12-01

**Definition 43 (Security of QKD)** *Let a QKD protocol  $\pi$  be given. Let  $n \in \mathbb{N}$ . Let  $\varepsilon > 0$ .*

*Let an adversary Eve be given (that has full control over the quantum channel between Alice and Bob, but can only listen to but not modify the classical channel between Alice and Bob). Then let  $\rho_{ABE}^{\text{Real}} \in S(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E)$  be the density operator describing the joint state of Alice's, Bob's and Eve's system in the case that Alice and Bob do not abort. Here  $\mathcal{H}_A = \mathcal{H}_B = \mathbb{C}^{2^n}$  because Alice's and Bob's final state consist of an  $n$ -bit key, and  $\mathcal{H}_E$  is some arbitrary Hilbert space defined by Eve.*

*Let  $S_{\text{Ideal}} \subseteq S(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E)$  be the set of all states of the form*

$$\left( \sum_{k \in \{0,1\}^n} 2^{-n} (|k\rangle\langle k| \otimes |k\rangle\langle k|) \right) \otimes \rho_E, \quad \rho_E \in S(\mathcal{H}_E).$$

*By  $P_{\text{success}}$  denote the probability that Alice and Bob do not abort the protocol and thus output a key (given a particular adversary Eve).*

*We say that  $\pi$  is  $\varepsilon$ -secure if the following holds: For every adversary Eve, we have that*

$$\exists \rho_{ABE}^{\text{Ideal}} \in S_{\text{Ideal}} : \quad \text{TD}(\rho_{ABE}^{\text{Real}}, \rho_{ABE}^{\text{Ideal}}) \cdot P_{\text{success}} \leq \varepsilon.$$

Intuitively this means that the keys output by Alice and Bob are the same with high probability, that these keys are almost uniformly distributed, and that Eve's information is almost independent of that key.

**Definition 44 (Bell states)** *The four Bell states are:*

$$\begin{aligned} |\beta_{00}\rangle &= \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle \\ |\beta_{01}\rangle &= \frac{1}{\sqrt{2}}|01\rangle + \frac{1}{\sqrt{2}}|10\rangle \\ |\beta_{10}\rangle &= \frac{1}{\sqrt{2}}|00\rangle - \frac{1}{\sqrt{2}}|11\rangle \\ |\beta_{11}\rangle &= \frac{1}{\sqrt{2}}|01\rangle - \frac{1}{\sqrt{2}}|10\rangle \end{aligned}$$

The four Bell states form a basis of  $\mathbb{C}^4$ .

As a shorthand, we write  $|\tilde{a}\tilde{b}\tilde{c}\tilde{d}\tilde{e}\tilde{f}\dots\rangle$  for the state  $|\beta_{ab}\rangle \otimes |\beta_{cd}\rangle \otimes |\beta_{ef}\rangle \otimes \dots$ . In particular,  $|\tilde{0}\dots\tilde{0}\rangle = |\beta_{00}\rangle^{\otimes n}$ . The states  $|\tilde{x}\rangle$  with  $x \in \{0,1\}^n$  form a basis of  $\mathbb{C}^{2^{2n}}$  ( $2n$ -qubit systems).

**Lemma 10** *Let a protocol  $\pi$  be given. Let  $n \in \mathbb{N}$ . Let  $\varepsilon > 0$ .*

*For every adversary Eve, let  $\rho_{ABE}^{\text{Real}} \in S(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E)$  be the density operator describing the joint state of Alice's, Bob's and Eve's system in the case that Alice and Bob do not abort.*

*Assume that for every adversary Eve, there is a state  $\rho_{ABE}^{\text{Ideal}}$  of the form  $\rho_{ABE}^{\text{Ideal}} = |\tilde{0}\dots\tilde{0}\rangle\langle\tilde{0}\dots\tilde{0}| \otimes \rho_E$  such that<sup>7</sup>*

$$\text{TD}(\rho_{ABE}^{\text{Real}}, \rho_{ABE}^{\text{Ideal}}) \cdot P_{\text{success}} \leq \varepsilon$$

where  $P_{\text{success}}$  is again the probability of not aborting.

*Then let  $\pi'$  be the protocol where Alice and Bob execute  $\pi$  and at the end of the protocol additionally measure each of their qubits in the computational basis (and forget the result). Then  $\pi'$  is an  $\varepsilon$ -secure QKD protocol.*

By virtue of Lemma 10, we only need to construct a protocol  $\pi$  as in Lemma 10.

In the following, we assume the QKD protocol we are constructing to be of the following form: Alice and Bob both expect qubits from Eve. That is, instead of Alice sending the qubits to Bob, both parties expect these qubits from an untrusted source. It is easy to see that if this protocol is secure, then the protocol where Alice produces and sends the qubits is also secure. This simplifies analysis as Eve's strategy can be completely described by the state she sends to Alice and Bob.

The state that Alice and Bob expect from Eve is  $|\tilde{0}\dots\tilde{0}\rangle$ , that is, Alice and Bob expect that the  $i$ -th qubit of Alice's system and the  $i$ -th qubit of Bob's system together are in the  $|\beta_{00}\rangle$  state. Of course, we do not assume that Eve indeed sends such a state.

**Definition 45** *Let a state  $\rho \in S(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E)$  be given with  $\mathcal{H}_A = \mathcal{H}_B = \mathbb{C}^m$ . Let  $q \in \mathbb{N}$ ,  $q \leq m$ . The Bell test is the following procedure:*

- *Choose  $q$  distinct indices  $i_1, \dots, i_q \in \{1, \dots, m\}$ .*
- *For each index  $i$ , measure the  $i$ -th Alice-Bob qubit pair of  $\rho$  using one of the following measurements:*
  - $P_{\text{yes}} := |\beta_{00}\rangle\langle\beta_{00}| + |\beta_{01}\rangle\langle\beta_{01}|$  and  $P_{\text{no}} := 1 - P_{\text{yes}}$ . (I.e., we check that the state is not  $|\beta_{10}\rangle$  or  $|\beta_{11}\rangle$ .)
  - $P_{\text{yes}} := |\beta_{00}\rangle\langle\beta_{00}| + |\beta_{10}\rangle\langle\beta_{10}|$  and  $P_{\text{no}} := 1 - P_{\text{yes}}$ . (I.e., we check that the state is not  $|\beta_{01}\rangle$  or  $|\beta_{11}\rangle$ .)

---

<sup>7</sup>Note that we implicitly reorder the qubits here in the sense that formally,  $|\tilde{0}\dots\tilde{0}\rangle\langle\tilde{0}\dots\tilde{0}|$  describes the state of Alice's and Bob's system when we order the qubits as follows: First qubit of Alice, first qubit of Bob, second of Alice, second of Bob, etc. On the other hand, when we wrote  $\sum_x (|x\rangle\langle x| \otimes |x\rangle\langle x|)$  we ordered them as follows: First qubit of Alice, second qubit of Alice, etc., first qubit of Bob, second of Bob, etc. This is just done for notational convenience.

- If this measurement returned no, abort.

Note that this test cannot be directly implemented by Alice and Bob because it performs measurements on the joint state of Alice and Bob that cannot be implemented locally. On the exercise sheet, however, we devise an equivalent test that can be implemented with local operations and classical communication (the latter will then be performed through the authenticated channel).

If  $\rho = |\tilde{0}\dots\tilde{0}\rangle\langle\tilde{0}\dots\tilde{0}|$ , then the Bell test passes with probability 1. If  $\rho = |\tilde{x}\rangle\langle\tilde{x}|$  where  $x$  has more than  $t$  bitpairs that are not 00, the Bell test passes with probability at most approximately  $(1 - \frac{t+1}{2m})^q$ . The exact bound is somewhat more complicated to compute, we just write  $\delta_q \approx (1 - \frac{t+1}{2m})^q$  for that bound. Note that for  $t = 0$ , even for  $q = m$ , this does not converge to 0, so we cannot use this test to ensure that there are no errors in the state. However, if  $t$  is a fixed fraction of  $m$ ,  $\delta_q$  converges exponentially fast to 0 for  $m, q \rightarrow \infty$ .

We fix the following notation:

By  $|x|$  we mean the number of bitpairs in  $x$  that are not 00.

Let  $P_{ok}$  be the projector  $\sum_{|x|\leq t} |\tilde{x}\rangle\langle\tilde{x}| \otimes I$  (where  $I$  is the identity on Eve's system  $\mathcal{H}_E$ ). That is, intuitively  $P_{ok}$  projects onto states that have at most  $t$  wrong qubit pairs. For notational convenience, we write  $P_{ok}(\rho) := P_{ok}\rho P_{ok}^\dagger$ .

Let  $T$  denote the (not trace-preserving) quantum operation describing the Bell test. More exactly, given a state  $\rho \in S(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E)$ ,  $T(\rho) := p\rho'$  where  $\rho'$  is the state after passing the Bell test and  $p$  is the probability of passing the Bell test. Note that  $\tilde{\rho} = \frac{T(\rho)}{\text{tr}T(\rho)}$  where  $\tilde{\rho}$  is the state after passing the Bell test.<sup>8</sup>

**Lemma 11** *Let a state  $\rho \in S(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E)$  be given with  $\mathcal{H}_A = \mathcal{H}_B = \mathbb{C}^m$ . Let  $q \in \mathbb{N}$ ,  $q \leq m$ .*

*Let  $\tilde{\rho} := \frac{T(\rho)}{\text{tr}T(\rho)}$  (the state after passing the Bell test). Let  $P_{success} := \text{tr}T(\rho)$  (the probability of passing the Bell test).*

*Then  $\text{tr}P_{ok}(\tilde{\rho}) \geq \frac{\text{tr}T(\rho) - \delta_q}{\text{tr}T(\rho)}$ . That is, the (hypothetical) test whether  $\tilde{\rho}$  indeed has at most  $t$  bad qubits will fail with probability at most  $\frac{\delta_q}{P_{success}}$ .*

(Note: In the present lecture, we have only shown this lemma under some restrictions on the form of  $\rho$ . In the next lecture, however, we will see how to get the lemma in its full generality.)

In the following, let  $t$ -Error denote the set of states  $|\Psi\rangle$  that are a superposition of states  $|\tilde{x}\rangle$  with  $|x| \leq t$ . (In other words, in  $|\Psi\rangle$ , at most  $t$  bad qubit pairs occur.) Formally,

$$t\text{-Error} := \text{span}\{|\tilde{x}\rangle : |x| \leq t\}$$

Using Lemma 8, we immediately get:

---

<sup>8</sup>This encoding of the Bell test is analogous to  $P_{ok}(\rho)$  where also both the post-measurement state and the probability are encoded in the operator  $P_{ok}(\rho)$  of trace  $\leq 1$ .

**Lemma 12** *Let a state  $\rho \in S(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E)$  be given with  $\mathcal{H}_A = \mathcal{H}_B = \mathbb{C}^m$ . Let  $q \in \mathbb{N}$ ,  $q \leq m$ .*

*Let  $\tilde{\rho} := \frac{T(\rho)}{\text{tr}T(\rho)}$  (the state after passing the Bell test). Let  $P_{\text{success}} := \text{tr}T(\rho)$  (the probability of passing the Bell test).*

*Then there exists a state  $\rho' \in S(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E)$  such that*

- $\rho' = \sum_i |\Psi_i\rangle\langle\Psi_i| \otimes \rho_i$  where each  $|\Psi_i\rangle \in t$ -Error. (In other words, in  $\rho'$ , at most  $t$  bad qubit pairs occur.)
- $\text{TD}(\tilde{\rho}, \rho') \leq \sqrt{\frac{\delta_q}{P_{\text{success}}}}$  and hence  $\text{TD}(\tilde{\rho}, \rho') \cdot P_{\text{success}} \leq \sqrt{\delta_q}$ .

# Quantum Cryptography

Lecture on 2010-12-14

**Definition 46 (Entanglement purification)** (Entanglement) purification is a process that needs only classical communication between Alice and Bob as well as local unitary operations and measurements and that achieves the following:

Assume that Alice and Bob share a state  $|\Psi\rangle \in \mathbb{C}^{2^l}$  with  $|\Psi\rangle \in t$ -Error (where Alice and Bob each hold half of each Bell pair). Then the result of applying the purification is a state  $|\tilde{0} \dots \tilde{0}\rangle \in \mathbb{C}^{2^n}$ .

**Lemma 13** There are values  $\alpha, \beta \in (0, 1)$  such that for sufficiently large  $n$  and  $l \geq \alpha n$  and  $t \leq \beta n$ , purification is possible.

By combining Lemma 12, Lemma 13, and Lemma 10, we get the following result:

**Lemma 14** Let a state  $\rho \in S(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E)$  be given with  $\mathcal{H}_A = \mathcal{H}_B = \mathbb{C}^m$ . Let  $q \in \mathbb{N}$ ,  $q \leq m$ . Let  $\mathcal{P}$  denote entanglement purification that takes  $l := m - q$  qubit pairs and returns  $n$  qubit pairs and corrects  $t$  errors.

Let  $\tilde{\rho} := \frac{T(\rho)}{\text{tr} T(\rho)}$  (the state after passing the Bell test). Let  $\tilde{\rho}'$  be the result of removing the  $q$  qubits that were measured in the Bell-test. Let  $\hat{\rho} := \mathcal{P}(\tilde{\rho}')$  be the result of applying the purification  $\mathcal{P}$  to the remaining bits  $\tilde{\rho}'$ . Let  $\rho^*$  be the state resulting from measuring Alice's and Bob's state in the computational basis.

Let  $P_{\text{success}} := \text{tr} T(\rho)$  (the probability of not aborting the protocol).

Then there exists a state  $\rho' \in S_{\text{Ideal}}$  such that  $\text{TD}(\tilde{\rho}, \rho') \leq \sqrt{\frac{\delta_q}{P_{\text{success}}}}$  and hence  $\text{TD}(\tilde{\rho}, \rho') \cdot P_{\text{success}} \leq \sqrt{\delta_q}$ .

In other words, there is a  $\sqrt{\delta_q}$ -secure QKD protocol producing  $n$  key bits that needs  $m$  qubits of quantum communication.

Note that the Bell test can be implemented with only local operations and classical communication using the method described in Homework 6, Problem 4.

**Further reading:** [NC00, Section 12.6].

[NC00] M. Nielsen and I. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, Cambridge, 2000.

# Quantum Cryptography

Lecture on 2011-01-04

## 14 Quantum Commitments

A commitment protocol is a protocol with two parties, Alice and Bob (or sender and recipient). It consists of two phases, the commit and the unveil phase. In the commit phase, Alice runs with some input  $b \in \{0, 1\}$  and Bob has no input. No output is made. In the unveil phase, both Alice and Bob have no input. Bob outputs a bit  $b' \in \{0, 1\}$  or aborts.<sup>9</sup> Intuitively, we require that Bob will output the bit  $b'$  that Alice committed herself to in the first phase, that is, Alice cannot change her mind about the bit (binding property). On the hand, we do not want Bob to learn the bit  $b$  before the unveil phase (hiding property). In the following, we assume that Alice and Bob are quantum machines and have a quantum channel between them. Since commitments are not supposed to give security against outside adversaries (but rather against the case that Alice or Bob cheats), we do not need any authenticated or secret channels.

Formally, a secure commitment scheme is one that has the properties: correctness, hiding, and binding.

**Definition 47 (Correctness)** *We call a commitment protocol  $\varepsilon_C$ -correct if for honest Alice and Bob, and for any Alice-input  $b \in \{0, 1\}$ , when executing the commit and the unveil phase, the probability that Bob outputs  $b' = b$  in the unveil phase is at least  $1 - \varepsilon_C$ .*

**Definition 48 (Hiding)** *We call a commitment protocol  $\varepsilon_H$ -hiding if the following holds: Fix some malicious Bob. Let  $\rho_b$  be the state of honest Alice's and malicious Bob's system after performing the commit phase with Alice-input  $b$ . Then*

$$\text{TD}(\text{tr}_A \rho_0, \text{tr}_A \rho_1) \leq \varepsilon_H.$$

**Definition 49 (Binding)** *We call a commitment protocol  $\varepsilon_B$ -binding if the following holds: Fix some machines  $A, A_0, A_1$ . Let  $P_b$  be the probability that honest Bob outputs  $b' = b$  after interacting with  $A$  in the commit phase and  $A_b$  in the unveil phase. Then*

$$P_0 + P_1 \leq 1 + \varepsilon_B.$$

---

<sup>9</sup>We assume that Alice never aborts and that Bob does not abort in the commit phase. This is possible without loss of generality, since instead of aborting they may just send dummy messages.

Intuitively, this means that Alice cannot unveil  $b$  when she learns  $b$  after the commit phase. Note that it is always possible to get  $P_0 + P_1 = 1$  since  $A$  might just randomly choose  $b$  with probability  $P_b$  and then perform an honest commit.

**Lemma 15 (Schmidt decomposition)** *Fix some bipartite Hilbert space  $\mathcal{H}_A \otimes \mathcal{H}_B$  and some quantum state  $|\Psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ . Then there are orthonormal sets of states*

$$\{|\alpha_i\rangle\} \subseteq \mathcal{H}_A \quad \text{and} \quad \{|\beta_i\rangle\} \subseteq \mathcal{H}_B$$

and reals  $\lambda_i \geq 0$  with  $\sum_i \lambda_i^2 = 1$  such that

$$|\Psi\rangle = \sum_i \lambda_i |\alpha_i\rangle \otimes |\beta_i\rangle.$$

**Lemma 16 (Simultaneous Schmidt decomposition)** *Fix some bipartite Hilbert space  $\mathcal{H}_A \otimes \mathcal{H}_B$  and two quantum states  $|\Psi\rangle, |\tilde{\Psi}\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ . Assume that  $\text{tr}_A |\Psi\rangle\langle\Psi| = \text{tr}_A |\tilde{\Psi}\rangle\langle\tilde{\Psi}|$ . Then there are orthonormal sets of states*

$$\{|\alpha_i\rangle\} \subseteq \mathcal{H}_A \quad \text{and} \quad \{|\tilde{\alpha}_i\rangle\} \subseteq \mathcal{H}_A \quad \text{and} \quad \{|\beta_i\rangle\} \subseteq \mathcal{H}_B$$

and reals  $\lambda_i \geq 0$  with  $\sum_i \lambda_i^2 = 1$  such that

$$|\Psi\rangle = \sum_i \lambda_i |\alpha_i\rangle \otimes |\beta_i\rangle.$$

and

$$|\tilde{\Psi}\rangle = \sum_i \lambda_i |\tilde{\alpha}_i\rangle \otimes |\beta_i\rangle.$$

This lemma intuitively states that if two states are indistinguishable when looking only at the second system, then the corresponding vectors  $|\beta_i\rangle$  in the Schmidt decomposition can be chosen to be the same for both states.

**Lemma 17 (Purification of the commit phase)** *Assume a commitment protocol  $\pi$  that is  $\varepsilon_C$ -correct,  $\varepsilon_H$ -hiding, and  $\varepsilon_B$ -binding. Then there is a commitment protocol  $\tilde{\pi}$  that is  $\varepsilon_C$ -correct,  $\varepsilon_H$ -hiding, and  $\varepsilon_B$ -binding and that performs only unitary operations during the commit phase (that is, no honest party measures, and no classical channel is used between the parties).*

The basic idea of the transformation underlying Lemma 17 is to do the following:

- First, replace any use of a classical channel by sending the classical bit on a quantum channel, encoded in the computational basis. Here both the sender and the recipient measure the bit before/after sending to ensure that it is classical even if the other party is cheating.
- Second, generate random bits as follows: If a random bit is needed, take a bit in the  $|0\rangle$  state, apply Hadamard to it (resulting in the  $|+\rangle$  state), and measure the bit in the computational basis.

- Third, replace every measurement (including those introduced in the steps before) by a CNOT that stores the result the measurement would have onto a fresh quantum register. This register is never used again, thus storing the information in this register has the same effect as measuring.

**Theorem 5 (Impossibility of quantum bit commitment)** *There is no 0-correct 0-binding 0-hiding commitment protocol.*

Note that this theorem does not exclude the possibility of quantum bit commitment under additional assumptions, e.g., if the adversary is computationally bounded, or if it is bounded in the size of its quantum memory (see next section).

As stated, the theorem does not exclude that  $\epsilon_C$ -correct  $\epsilon_H$ -hiding  $\epsilon_B$ -binding commitment protocols might exist for small but non-zero  $\epsilon_C, \epsilon_H, \epsilon_B$ . A more careful analysis, however, excludes this [May97].

[May97] D. Mayers. Unconditionally Secure Quantum Bit Commitment is Impossible. *Physical Review Letters*, 78(17):3414–3417, 1997. Online available at <http://arxiv.org/abs/quant-ph/9605044>.

## Quantum Cryptography

Lecture on 2011-01-11

### 14.1 Bounded quantum storage model

In the bounded quantum storage model, we assume that there is an upper bound  $n$  on the amount of quantum of quantum memory the adversary can store over a longer period of time (where we do not specify that period of time, but require that between commit and unveil at least that time passes). In the bounded quantum storage model more is possible to design secure quantum commitment protocols without having to resort to any unproven computational assumption like the hardness of inverting some function (one-way function).

Consider the following protocol from [DFSS05]:

- Let  $m$  be some parameter.
- *Commit phase:* In the commit phase, Bob (the recipient) chooses  $m$  bits  $x_i \in \{0, 1\}$ , and  $m$  bits  $b_i \in \{0, 1\}$ . Then Bob encodes each  $x_i$  in a basis specified by  $b_i$ ; call the resulting qubit  $\Psi_i$ . More exactly, if  $b_i = 0$ , then  $x_i$  is encoded in the computational basis  $|0\rangle, |1\rangle$ ; if  $b_i = 1$ , then  $x_i$  is encoded in the diagonal basis  $|+\rangle, |-\rangle$ . Then Bob sends the qubits  $|\Psi_1\rangle, \dots, |\Psi_m\rangle$  to Alice.

If  $c = 0$  (Alice wants to commit to 0), then Alice measures all qubits in the computational basis; if  $c = 1$  (Alice wants to commit to 1), then Alice measures all qubits in the diagonal basis. Let the results of these measurements be  $\tilde{x}_i$ .

- *Unveil phase:* Alice sends  $c$  and all the bits  $\tilde{x}_i$  to Bob. Bob checks whether  $x_i = \tilde{x}_i$  for all  $i$  with  $b_i = c$ . If so, Bob outputs  $c' := c$ . Otherwise, Bob aborts.

#### **Theorem 6 (Commitment in the quantum bounded storage model [DFSS05])**

*Fix some constant  $\delta > 0$ . Let  $n$  denote the security parameter and assume that  $n$  is also the quantum memory bound of the adversary. Assume that in the above protocol,  $m \geq (4 + \delta)m$ . Then there is a negligible function  $\mu$  such that the above protocol is perfectly correct and hiding (i.e., 0-correct and 0-hiding) and  $\mu(n)$ -binding.*

Note that the protocol does not need any quantum storage on the side of Alice and Bob. Current technology does not allow to implement this protocol because it assumes that no errors occur on the quantum channel. However, a straightforward modification in which Bob accepts a certain amount of errors in his check in the unveil phase can be shown to be secure.

For the proof of Theorem 6, we need various tools.

**Definition 50 (Min-entropy)** Let  $X$  and  $Y$  be discrete random variables.

The min-entropy  $H_\infty(X)$  of  $X$  is defined as  $H_\infty(X) := -\log \max_x \Pr[X = x]$ .

The conditional min-entropy  $H_\infty(X|Y)$  is defined as  $H_\infty(X|Y) := \min_y H_\infty(X|Y = y)$  where  $X|Y = y$  stands for the random variable  $X$  under the condition  $Y = y$ .

The min-entropy  $H_\infty(X)$  is defined in such a way that  $2^{-H_\infty(X)}$  is the maximum probability one can have in guessing  $X$ . This relation to guessing makes the min-entropy particularly well-suited for cryptographic purposes.

Often, a random variable has a certain min-entropy up to a certain disturbance. This is captured by the following definition:

**Definition 51 (Smooth min-entropy)** Let  $X$  and  $Y$  be discrete random variables. Let  $\varepsilon > 0$ . For an event  $E$ , let  $H_\infty(XE) := -\log \max_x \Pr[X = x \text{ and } E \text{ holds}]$  and let  $H_\infty(XE|Y) := \min_y H_\infty(XE|Y = y)$ .

The smooth min-entropy  $H_\infty^\varepsilon(X)$  is defined as  $H_\infty^\varepsilon(X) := \max_E H_\infty(XE)$ , and the conditional smooth min-entropy  $H_\infty^\varepsilon(X|Y)$  is defined as  $H_\infty^\varepsilon(X|Y) := \max_E H_\infty(XE|Y)$ , where in both cases  $E$  ranges over all events with  $\Pr[E] \geq 1 - \varepsilon$ .

Intuitively, having smooth min-entropy  $\alpha = H_\infty^\varepsilon(X)$  means having min-entropy  $\alpha$  except in a rare case  $\neg E$  which has probability at most  $\varepsilon$ .

Notice that these definitions only refer to *classical* random variables. They cannot be applied to quantum systems. For example, if the adversary's system  $Y$  contains information about some classical or quantum system  $X$ , then  $H_\infty(X|Y)$  cannot be used to express the amount of information. There are, however, generalizations of the above definitions that apply also to quantum systems. See [Ren05].

**Theorem 7 (Uncertainty relation)** Fix a constant  $\lambda > 0$ . Let  $\rho \in S(\mathbb{C}^{2^m})$ . Let  $b_1, \dots, b_m \in \{+, \times\}$  be uniformly and independently chosen bases (+ denote the computational, and  $\times$  the diagonal basis). Let  $x_i$  denote the result of measuring the  $i$ -th bit of  $\rho$  in basis  $b_i$ . Then there exists a negligible  $\varepsilon$  such that

$$H_\infty^{\varepsilon(m)}(x_1, \dots, x_m | b_1, \dots, b_m) \geq (\frac{1}{2} - 2\lambda)m.$$

This theorem states that if we are given an arbitrary state  $\rho$  (that we may now as much about as we like), and then a basis is randomly chosen, then we will necessarily have approximately  $m/2$  bits of uncertainty about the outcome of measuring the state in this basis. In other words, for no state can we know what would be the outcome of measuring that state for each possible basis. (Although for particular fixed bases, we can certainly know the output: For example, if  $b$  is the computational basis and  $x = |0\rangle$ .)

Theorem 7 is shown in [DFR<sup>+</sup>07] (Corollary 3.4 in the full version).

**Lemma 18 (Min-entropy splitting)** Let  $X_0, X_1, B$  be random variables. Fix  $\varepsilon, \varepsilon' > 0$ . Then there exists a function  $C$  with range  $\{0, 1\}$  such that

$$H_\infty^{\varepsilon+\varepsilon'}(X_{\bar{C}}|C, B) \geq H_\infty^\varepsilon(X_0, X_1|B)/2 - 1 - \log \frac{1}{\varepsilon'}$$

where  $C := C(X_0, X_1, B)$  and  $\bar{C} := 1 - C$ .

Intuitively, this lemma means that if we have an uncertainty  $\alpha$  about  $X_0, X_1$ , then we have uncertainty approximately  $\alpha/2$  about  $X_0$  or  $X_1$ . (Where the random variable  $\bar{C}$  indicates which of the  $X_0, X_1$  is currently the uncertain one.)

Lemma 18 is shown in [DFR<sup>+</sup>07] (Corollary 4.3 in the full version).

**Lemma 19** *Let  $\varepsilon > 0$ . Let  $X$  and  $B$  be classical random variables and  $A$  be a quantum system of size  $n$ -qubits. I.e., we have a state  $\rho = \sum_{xb} p_{xb} |x\rangle\langle x| \otimes |b\rangle\langle b| \otimes \rho_{xb}$  with  $\rho_{xb} \in S(\mathbb{C}^{2^n})$ .*

*Let  $\tilde{X}$  denote the outcome of applying some quantum operation  $\mathcal{E}$  to  $A$  and then measuring  $A$  in some basis. Let  $X$  and  $B$  denote the outcome of measuring  $X$  and  $B$  in the computational basis.*

*Then*

$$\Pr[X = \tilde{X}] \leq 2^{-\frac{1}{2}(H_\infty^\varepsilon(X|B)) - n - 1} + 2\varepsilon.$$

Notice that, classically, the probability of guessing  $X$  is exponentially small in  $H_\infty^\varepsilon(X|B)$ . The present lemma states that additional  $n$  qubits of quantum information effectively decrease  $H_\infty^\varepsilon(X|B)$  by approximately  $n$  bits; the probability of guessing  $X$  is now exponentially small in  $H_\infty^\varepsilon(X|B) - n$ .

**Further reading:** For the Schmidt decomposition, see [NC00, Section 2.5]. For the impossibility of quantum commitment, see [May97]. For commitment in the bounded quantum storage model, see [DFSS05] and [DFR<sup>+</sup>07]. For definitions of min-entropy in the quantum case and a lot of results concerning these, see [Ren05].

[DFR<sup>+</sup>07] Ivan Damgård, Serge Fehr, Renato Renner, Louis Salvail, and Christian Schaffner. A tight high-order entropic quantum uncertainty relation with applications. In Alfred Menezes, editor, *Crypto 2007*, volume 4622 of *LNCS*, pages 360–378. Springer, 2007. Preprint at <http://arxiv.org/abs/quant-ph/0612014>.

[DFSS05] Ivan B. Damgård, Serge Fehr, Louis Salvail, and Christian Schaffner. Cryptography in the bounded quantum-storage model. In *Proceedings of FOCS 2005*, pages 449–458, 2005. A full version is available at <http://arxiv.org/abs/quant-ph/0508222>.

[May97] D. Mayers. Unconditionally Secure Quantum Bit Commitment is Impossible. *Physical Review Letters*, 78(17):3414–3417, 1997. Online available at <http://arxiv.org/abs/quant-ph/9605044>.

[NC00] M. Nielsen and I. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, Cambridge, 2000.

[Ren05] Renato Renner. *Security of Quantum Key Distribution*. PhD thesis, ETH Zurich, September 2005. Available at <http://arxiv.org/abs/quant-ph/0512258v2>.

# Quantum Cryptography

Lecture on 2011-01-18

## 15 Zero-knowledge proofs

A zero-knowledge proof is, intuitively speaking, a protocol in which a prover  $P$  is able to convince a verifier  $V$  of the truth of a statement  $x$  in such a way that the verifier learns nothing (except, of course, the fact that  $x$  is true).

More formally, we first fix a relation  $R$ . If  $(x, w) \in R$ , we say that  $w$  is a witness for the statement  $x$ . We defined the language  $L_R$  of true statements as follows:

$$L_R := \{x : \exists w. (x, w) \in R\}.$$

In other words,  $x \in L_R$  iff there is a witness for  $x$ .

We first define what it means for  $(P, V)$  to form a proof system (in the classical case). For this, we first introduce the following notation: For two machines  $A, B$ ,  $\langle A(a), B(b) \rangle$  denotes the output of  $B$  after an interaction of  $A$  and  $B$  where  $A$  gets input  $a$  and  $B$  gets input  $b$ .

**Definition 52 (Proof systems)** *We call a pair  $(P, V)$  of interactive machines a proof or proof system for the relation  $R$  with soundness-error  $\varepsilon$  iff the following two conditions are fulfilled:*

- *Completeness: For any  $(x, w) \in R$ , we have that  $\Pr[\langle P(x, w), V(x) \rangle = 1] = 1$ . (I.e., when the prover gets a valid witness  $w$  for  $x$ , then he manages to convince  $V$  of the truth of  $x$ .)<sup>10</sup>*
- *Soundness: For any (potentially computationally unlimited) machine  $P^*$ , and for any  $x \notin L_R$ , we have  $\Pr[\langle P^*(\cdot), V(x) \rangle = 1] \leq \varepsilon$ . (I.e., except for probability  $\varepsilon$ , no prover can convince  $V$  of a wrong statement  $x$ .)*

We can now define what it means that the verifier does not learn anything:

**Definition 53 (Zero-knowledge)** *A pair  $(P, V)$  of interactive machines is statistical zero-knowledge if for any polynomial-time<sup>11</sup>  $V^*$  there exists a polynomial-time  $S$  and a negligible  $\mu$  such that for all  $(x, w) \in R$  and all  $z \in \{0, 1\}^*$ , we have*

$$\text{SD}(\langle P(x, w), V^*(x, z) \rangle, S(x, z)) \leq \mu(|x|).$$

<sup>10</sup>Of course, one could also relax this condition and allow a certain error in the completeness instead of requiring probability 1. For simplicity, we stick to the present definition.

<sup>11</sup>In this section, we will call a machine polynomial-time if its running-time is bounded by a polynomial in the length of its *first* argument.

(I.e., the simulator can simulate anything  $V^*$  learns without knowing the witness  $w$ .)

An example for a zero-knowledge proof is the following:

**Definition 54 (Graph isomorphism)** *The relation  $R_{GI}$  is defined as follows:  $(x, w) \in R_{GI}$  iff  $x = (G_1, G_2)$  and  $w = \phi$  where  $G_1, G_2$  are graphs and  $\phi : G_1 \rightarrow G_2$  is a graph isomorphism.*

**Definition 55 (Graph isomorphism proof system)** *Let GIP denote the following protocol between machine  $P$  and  $V$ :*

- $P$  gets inputs  $x = (G_1, G_2)$  and  $w = \phi$ .
- $V$  gets input  $x$ .
- $P$  picks a uniformly random permutation  $\psi_1$  on the vertices of  $G_1$  and computes  $H := \psi_1(G_1)$ . (Notice that now  $\psi_1 : G_1 \rightarrow H$  is an isomorphism.)
- $P$  sends  $H$  to  $V$ .
- $V$  picks  $i \in \{1, 2\}$  uniformly and sends  $i$  to  $P$ .
- $P$  computes  $\psi_2 := \psi_1 \circ \phi^{-1}$  and sends  $\psi_i : G_i \rightarrow H$ .
- $V$  checks whether  $\psi_i : G_i \rightarrow H$  is an isomorphism. If so,  $V$  outputs 1.

**Theorem 8** *GIP is a statistical zero-knowledge proof system.*

We now present the definitions of zero-knowledge proofs for the quantum case. For two quantum or classical machines  $A, B$ ,  $\langle A(a), B(b) \rangle$  denotes the quantum state of  $B$  (or, if  $B$  is classical, its output) after an interaction of  $A$  and  $B$  where  $A$  gets input  $a$  and  $B$  gets input  $b$ . Here  $a$  and  $b$  may be classical values or density operators.

The definition of being a proof system (i.e., completeness and soundness) is word for word the same as in the classical case (Definition 52), except that  $P^*$  is allowed to be a quantum machine.

More interesting is the definition of statistical quantum zero-knowledge:

**Definition 56 (Quantum zero-knowledge)** *A pair  $(P, V)$  of interactive machines is statistical quantum zero-knowledge if for any polynomial-time quantum-machine  $V^*$  there exists a polynomial-time quantum-machine  $S$  and a negligible  $\mu$  such that for all  $(x, w) \in R$  and all density operators  $\rho$ , we have*

$$\text{TD}(\langle P(x, w), V^*(x, \rho) \rangle, S(x, \rho)) \leq \mu(|x|).$$

(I.e., the simulator can simulate anything  $V^*$  learns without knowing the witness  $w$ .)

Note that in this case, the “auxiliary input” that  $V^*$  gets (called  $z$  in the case of Definition 53) is a quantum state.

# Quantum Cryptography

Lecture on 2011-01-25

To show that GIP is statistical QZK, we need to construct a suitable simulator  $S$ . However, it turns out that the construction from the classical case does not directly carry over. The reason is that the simulator in the classical case uses rewinding: It tries to produce a simulation, and, if it fails, it tries again. In the quantum case, trying again is not necessarily an option, because the first try may have destroyed the input state  $\rho$ , so the second try will fail.

What does work, however, is constructing a polynomial-time simulator  $S_1$  that tries to produce a simulation and either produces a perfect simulation or aborts, and that aborts with probability exactly  $\frac{1}{2}$ . (More precisely, if  $(x, w) \in R$  and  $\rho'$  is the state output by the simulator  $S_1(x, \rho)$ , then  $\text{tr } P_{\perp} \rho' = \frac{1}{2}$  and  $P_{\perp} \rho' P_{\perp} / \text{tr } P_{\perp} \rho' P_{\perp} = \langle P(x, w), V^*(x, \rho) \rangle$  where  $P_{\perp}$  projects on the state denoting abort.)

The construction of this simulator is analogous to the classical case and the proof that it produces a perfect simulation with probability  $\frac{1}{2}$  also follows very closely the lines of the proof in the classical case.

To produce a simulator  $S$  in the sense of Definition 56 from  $S_1$ , we cannot directly follow the classical proof. Instead, we use the following lemma:

**Lemma 20 (Quantum rewinding lemma [Wat09])** *Let  $Q$  be a unitary operation from  $\mathcal{H}_{in} \otimes \mathcal{H}_{anc}$  to  $\mathcal{H}_{out} \otimes \mathcal{H}_{succ}$  with  $\mathcal{H}_{succ} = \mathbb{C}^2$ . (This implies that  $\dim \mathcal{H}_{in} \otimes \mathcal{H}_{anc} = \dim \mathcal{H}_{out} \otimes \mathcal{H}_{succ}$  since a unitary operation is a square matrix.)*

*Assume that there is a value  $p \leq \frac{1}{2}$  such that for any  $|\Psi\rangle \in \mathcal{H}_{in}$ , we have that applying  $Q$  to  $|\Psi\rangle \otimes |0\rangle$  and then measuring  $\mathcal{H}_{succ}$  in the computational basis gives outcome 1 (success) with probability  $p$  (not  $\geq p$ ). Let  $|\tilde{\phi}_{succ}\rangle$  denote the post measurement state in  $\mathcal{H}_{out}$  in that case.*

Consider the following algorithm (depending on a parameter  $q$ ):

1. Let  $|\Psi\rangle$  denote the input of the algorithm (in  $\mathcal{H}_{in}$ )
2. Initialize  $\mathcal{H}_{anc}$  with  $|0\rangle$ .
3. Apply  $Q$ .
4. Measure  $\mathcal{H}_{succ}$  in the computational basis.
5. If the outcome is 1, exit (successfully).
6. Apply  $Q^{\dagger}$ .
7. Apply FLIP to  $\mathcal{H}_{anc}$  where  $\text{FLIP } |0\rangle := |0\rangle$  and  $\text{FLIP } |x\rangle := -|x\rangle$  for  $x \neq 0$ .
8. Go to 3. (But at most  $q$  times.)

Then for a suitable  $q \in \text{poly}(1/p)$ , we have that

- The probability that  $R$  exits successfully is overwhelming.

- The post measurement state in  $\mathcal{H}_{out}$  in that case is  $|\tilde{\phi}_{succ}\rangle$ .

This lemma can be used to construct the simulator  $S$  from  $S_1$ : First, we purify  $S_1$  (i.e., replace measurements by CNOTs on ancilla qubits in  $\mathcal{H}_{anc}$  initialized with  $|0\rangle$ ), resulting in  $Q$ . Then  $S$  runs  $R$  and outputs the state  $|\tilde{\phi}_{succ}\rangle$ .

Notice that in the classical case, it is sufficient that  $S_1$  succeeds with probability  $\geq p$  (possibly dependent on the auxiliary input  $z$ ), while in the quantum case, we need that the simulator  $S_1$  succeeds with a probability  $p$  that is independent of the auxiliary input  $\rho$ .

Notice further that the above lemma only covers the case where the simulation is perfect. There is a variant of that lemma which also covers the case where  $S_1$  produces a state that has negligible trace distance from  $\langle P(x, w), V^*(x, \rho) \rangle$ . This allows to cover a wider range of protocols and even protocols that are only computationally QZK.

**Further reading:** An overview over zero-knowledge proofs in the classical case can be found in [Gol01, Chapter 4]. For quantum zero-knowledge, see [Wat09].

[Gol01] Oded Goldreich. *Foundations of Cryptography – Volume 1 (Basic Tools)*. Cambridge University Press, August 2001. Previous version online available at <http://www.wisdom.weizmann.ac.il/~oded/frag.html>.

[Wat09] John Watrous. Zero-knowledge against quantum attacks. *SIAM J. Comput.*, 39(1):25–58, 2009.

# Quantum Cryptography

Lecture on 2011-02-01

## 16 Factoring

Note: The following section will contain only a simplified exposition that is not complete but will give the rough idea of how to factor integers using quantum computers.

**Definition 57 (Factoring problem)** *Given a non-prime integer  $m > 1$ , find an integer  $d \mid m$  with  $d \neq 1$ ,  $d \neq m$  (a non-trivial divisor).*

**Definition 58 (Order finding problem)** *Let  $G$  be a (multiplicative) group. Given  $a \in G$ , find the smallest  $r > 0$  such that  $a^r = 1$  in  $G$ . This value  $r$  we denote  $\text{ord } a$ .*

**Lemma 21 (Reducing factoring to order-finding)** *Given an oracle that solves the order finding problem in groups  $G = \mathbb{Z}_m^\times$  (for arbitrary  $m > 1$ ), we can solve the factoring problem with probability at least  $\frac{1}{4}$  in polynomial-time using a single query to the order-finding oracle.*

The idea of the reduction is to compute  $\gcd(x^{r/2} + 1, m)$  and  $\gcd(x^{r/2} - 1, m)$  for random  $x$ . With probability at least  $\frac{1}{4}$  one of the two gcds will be a non-trivial divisor of  $m$ .

**Definition 59 (Discrete Fourier transform)** *The discrete Fourier transform (DFT) is a linear transformation on  $\mathbb{C}^N$  represented by the matrix  $D_N = 2^{-N/2}((e^{2i\pi kl/N})_{kl} \in \mathbb{C}^{N \times N}$ .*

Note that since  $2i\pi kl/N$  is an imaginary number, all entries of  $D_N$  have absolute value 1.

**Lemma 22 (Properties of the discrete Fourier transform)**

- *The discrete Fourier transform  $D_N$  is unitary.*
- *Frequency analysis: Given a vector  $x$  which is  $p$ -periodic (i.e.,  $x_i = x_{i+p \bmod N}$  for all  $i$ ; a special case would be a vectors with 1's at every  $p$ -th position),  $D_N x$  has entries (non-zero values) on the multiples of  $N/p$ .<sup>12</sup> Note that  $N/p$  intuitively represents the frequency of  $x$ .*

<sup>12</sup>If  $p \nmid N$ , this holds only approximately. In this exposition, we will not formulate exact bounds for the approximation.

**Theorem 9 (Realising the discrete Fourier transform)** *There is a quantum algorithm taking an  $n$  qubit state  $|\Psi\rangle$  as input and returning  $D_N|\Psi\rangle$  where  $D_N$  is the Fourier transform on  $\mathbb{C}^N$  with  $N = 2^n$ . This algorithm runs in polynomial time in  $n$ .*

**Theorem 10 (Order-finding)** *Assume a group  $G$  in which exponentiation is feasible in polynomial-time. There is a polynomial-time quantum algorithm that returns  $\text{ord } a$  on input of  $a \in G$ .*

The algorithm roughly goes as follows: Let  $a \in G$ . Let  $N = 2^n$  be sufficiently larger than  $|G|$ . The algorithm starts with a quantum state  $|0\rangle|0\rangle \in \mathcal{H}_X \otimes \mathcal{H}_Y$ , the first system  $\mathcal{H}_X := \mathbb{C}^N$  encoding integers  $\{0, \dots, N-1\}$ , and the second system  $\mathcal{H}_Y$  encoding group elements of  $G$ . It applies the Hadamard transform to every qubit of  $\mathcal{H}_X$ . This results in the state  $|\Psi_1\rangle \propto \sum_{x \in \{0,1\}^n} |x\rangle|0\rangle$  ( $\propto$  means equal up to a normalization factor). We can implement the unitary transformation  $U$  that takes  $|x\rangle|y\rangle$  to  $|x\rangle|y \oplus a^x\rangle$ . By applying  $U$  to  $|\Psi_1\rangle$ , we get  $|\Psi_2\rangle \propto \sum_{x \in \{0,1\}^n} |x\rangle|a^x\rangle$ . We then measure the system  $\mathcal{H}_Y$  in the computational basis. This results in a measurement outcome  $o = a^{x'}$  for some  $x'$ . The state after this measurement is  $|\Psi_3\rangle \propto \sum_a |a\rangle$  where the sum ranges over all  $a$  with  $a^x = o = a^{x'}$ , i.e.,  $x = x' + k \text{ord } a$  for some  $k \in \mathbb{Z}$ . Hence  $|\Psi_3\rangle$  is  $\text{ord } a$ -periodic. Thus, if we apply the Fourier transform  $D_N$ , we get a vector  $D_N|\Psi_3\rangle$  which has entries on multiples of  $N/\text{ord } a$  (approximately). If we measure the system in the computational basis, we get a multiple of  $N/\text{ord } a$ . From this we can compute an approximate divider of  $\text{ord } a$ . Additional work needs to be done to recover the exact value of  $\text{ord } a$  from this, but this is a classical computation and omitted here.

**Definition 60 (Discrete logarithm problem)** *Let  $G$  be a (multiplicative) group and  $g$  a generator. Given  $y \in G$ , find  $x$  with  $g^x = y$ . (That value  $x$  is called the discrete logarithm  $\text{dlog } y$  of  $y$ .)*

**Theorem 11** *Assume a group  $G$  with generator  $g$  in which exponentiation is feasible in polynomial-time. There is a polynomial-time quantum algorithm that returns  $\text{dlog } a$  on input of  $a \in G$ .*

**Further reading:** [NC00, Sections 5.1–5.3]

[NC00] M. Nielsen and I. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, Cambridge, 2000.

## Index

- basis
  - computational, 9
- BB84, 24
- beam splitter, 7
- Bell states, 26
- Bell test, 27
- bomb tester, 7
- bounded quantum storage, 34
- CNOT, 10
- commitment, 31
  - correctness of, 31
  - in bounded quantum storage model, 34
- complete measurement, 10
- completely positive, 20
- completeness
  - of a proof system, 37
- composite measurement, 13
- composite system, 12
- composite unitary, 12
- computational basis, 9
- conditional min-entropy, 35
  - smooth, 35
- conditional smooth min-entropy, 35
- conjugate transpose, 3
- controlled NOT, 10
- controlled- $U$  gate, 11
- convexity
  - of trace distance, 23
- correctness
  - of commitment, 31
- density matrix, 17
- density operator, 17
- Deutsch's algorithm, 14
- DFT, *see* discrete Fourier transform
- Dirac notation, 4
- discrete Fourier transform, 41
- discrete logarithm problem, 42
- distance
  - statistical, 21
  - trace, 22
- divisor
  - non-trivial, 41
- dlog, *see* discrete logarithm
- Elitzur-Vaidman bomb tester, 7
- ensemble
  - quantum, 16
- entanglement purification, 30
- environment, 19
- error
  - soundness-, 37
- factoring problem, 41
- fault tolerant computation, 14
- Fourier transform
  - discrete, 41
- global phase, 5, 10
- Hadamard gate, 6
- Hilbert space, 3
- inner product, 3
- key distribution, 23
- Kitaev theorem
  - Solovay-, 13
- Kraus operator, 20
- Kronecker product, 12
- Lo-Chau, 24
- matrix
  - density, 17
- measurement
  - complete, 10
  - projective, 9
- min-entropy, 35
  - conditional, 35
  - conditional smooth, 35
  - smooth, 35
- mixed state, 17

- non-trivial divisor, 41
- norm, 3
- normalised, 3
- not-gate, 6
- operator
  - density, 17
  - Kraus, 20
- order finding problem, 41
- orthogonal, 3
- orthogonal projection, 5
- orthonormal, 3
- partial trace, 19
- positive, 4
  - completely, 20
- projection, 5
- projective measurement, 9
- projective measurement, 5
- proof, 37
- proof system, 37
- pure state, 17
- purification, 19
  - entanglement, 30
- QKD, 23
  - security of, 26
- quantum ensemble, 16
- quantum key distribution
  - security of, 26
- quantum key distribution, 23
- quantum operation, 19
- quantum state, 9
- quantum storage
  - bounded, 34
- quantum zero-knowledge
  - statistical, 38
- qubit, 5
- security of QKD, 26
- smooth min-entropy, 35
  - conditional, 35
- Solovay-Kitaev theorem, 13
- soundness
  - of a proof system, 37
- soundness-error, 37
- state
  - mixed, 17
  - quantum, 9
- statistical distance, 21
- statistical quantum zero-knowledge, 38
- statistical zero-knowledge, 37
  - quantum, 38
- storage
  - bounded quantum, 34
- superoperator, 20
- SWAP, 11
- tensor product, 12
- Toffoli gate, 11
- trace, 4
- trace distance
  - convexity of, 23
- trace out, 19
- trace distance, 22
- unitary transformation, 5, 9
- Vaidman, 7
- X-gate, 6
- zero-knowledge
  - statistical, 37
  - statistical quantum, 38
- ZK, *see* zero-knowledge



## Symbol index

$\text{span } M$	Vector space spanned by vectors in $M$	
$\mathbb{C}$	Complex numbers	
$\mathbb{Z}$	Integers	
$\mathbb{N}$	Natural numbers, excluding 0	
$ x $	Absolute value of $x$	
$\mathcal{H}$	Usually denotes a Hilbert space	
$\text{im } P$	Image of the linear transformation $P$	
$\langle \Phi, \Psi \rangle$	Inner product of $\Phi$ and $\Psi$	3
$x^*$	Complex conjugate of $x \in \mathbb{C}$	3
$\ x\ $	Norm (length) of a vector $x$	3
$M^\dagger$	Conjugate transpose of matrix $M$	3
$ \Psi\rangle$	Dirac notation; represents a vector with name $\Psi$	4
$\langle \Psi $	Dirac notation; the dual of $ \Psi\rangle$	4
$\langle \Phi \Psi\rangle$	Inner product of $ \Phi\rangle$ and $ \Psi\rangle$ (same as $\langle \Phi, \Psi \rangle$ )	4
$\text{tr } M$	Trace of a matrix $M$	4
$H$	Hadamard matrix/gate	6
$X$	Bit flip matrix/gate	6
$R_\theta$	Rotation matrix/gate; rotation angle $\theta$	6
$S$	Phase shift matrix/gate	6
$S_\theta$	Phase shift matrix/gate; angle $\theta$	7
CNOT	Controlled NOT gate	10
SWAP	SWAP gate	11
$C(U)$	Controlled- $U$ gate	11
$S(\mathcal{H})$	Density operators over $\mathcal{H}$	17
$\mathcal{E}$	Usually denotes a quantum operation	19
$\mathcal{F}$	Usually denotes a quantum operation	19
$\text{SD}(X, Y)$	Statistical distance between $X$ and $Y$	21
$\text{TD}(\rho, \sigma)$	Trace distance between $\rho$ and $\sigma$	22
$\rho_{ABE}^{\text{Real}}$	State after execution of QKD protocol (case: no abort)	26
$\rho_{ABE}^{\text{Ideal}}$	Ideal state after execution of QKD protocol	26
$S_{\text{Ideal}}$	Set of all ideal states (after execution of QKD protocol)	26
$ \beta_{ab}\rangle$	Bell state ( $ab$ determines which one)	26
$t\text{-Error}$	Set of Bell states with $\leq t$ errors	28
$H_\infty(X)$	Min-entropy of $X$	35
$H_\infty^\varepsilon(X)$	Smooth min-entropy	35
$L_R$	Language for the relation $R$	37
$\langle A(a), B(b) \rangle$	$B$ 's output after interacting with $A$	37
$R_{GI}$	Relation for graph isomorphism	38
GIP	Proof system for graph isomorphism	38
$\text{ord } a$	Order of group element $a$	41
$D_N$	Discrete Fourier transform of size $N$	41
$\propto$	Proportional to	42
$\text{dlog } y$	Discrete logarithm of $y$	42