University of Tartu Prof. Dr. Dominique Unruh

Quantum Cryptography

Short notes, fall 2018

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@ut.ee.

Contents

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.*[1]*.*

$\mathbb{C}^n$ 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.[2]

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

[1] Or any complex vector space isomorphic to $\mathbb{C}^n$

[2] I.e., $(a + bi)^* = a - bi$.

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 $M \in \mathbb{C}^{n\times m}$, 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).

Definition 3 (Dirac notation) *In the* Dirac notation*, a vector Ψ 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 P_V onto $V = \operatorname{span}\Psi$ we write $P_V = |\Psi\rangle\langle\Psi|$. (Try it out and evaluate $P_V|\Phi\rangle$!)

Definition 4 (Trace) *The* trace $\operatorname{tr} M$ *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 $|1\rangle, \ldots, |n\rangle$ 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 $|1\rangle, \ldots, |n\rangle$ such that $M = \sum_i \lambda_i |i\rangle\langle i|$ where λ_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 $A = UDV$.*

Definition 10 (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 $B_1 \times B_2 = \{|i, j\rangle\}$.*[3]

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

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

Further reading: [NC00, Section 2.1]

2 One Qubit

Definition 11 (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 12 (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 $U|\Psi\rangle$.*

[3] There exists a more general category theoretical definition using a universal property, but for our purposes this specialisation is sufficient.

In the case of polarisation, a typical transformation would be to rotate the polarisation by an angle of α. 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 13 (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.*[4]

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 $|no\rangle$.[5]

An example for a measurement is a polarising filter. If the filter lets only vertically polarised light through, it corresponds to a measurement with $|\text{yes}\rangle = |\updownarrow\rangle$ 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 $|\updownarrow\rangle$ 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 14 (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

$$H|0\rangle = \tfrac{1}{\sqrt{2}}(|1\rangle + |0\rangle)$$
$$H|1\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

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 15 (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

$$X|0\rangle = |1\rangle$$
$$X|1\rangle = |0\rangle$$

[4] Of course, the labelling yes/no is arbitrary. Any other two labels are possible.

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

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

Definition 16 (Rotation) *The rotation by angle θ 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 17 (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 θ:

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

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 $B_{\frac{\pi}{4}}$:

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

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

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

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 $B_{-\frac{\pi}{4}}$ 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 $B_{\frac{\pi}{4}}$ and $B_{-\frac{\pi}{4}}$ 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].

4 Larger quantum systems

Definition 18 (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 $|b_1\rangle, \ldots, |b_n\rangle$ are the basis vectors, and $b_1, \ldots, b_n$ 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 $|b_i\rangle = (0, \ldots, 0, 1, 0, \ldots, 0)^t$ where the 1 is at the i-th position.

We abbreviate $x \otimes \ldots \otimes x$ (n components) as $x^{\otimes n}$. See Definition 10 for the definition of $\otimes$.

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

Definition 19 (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 20 (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., $P_iP_j = 0$ 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 21 (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 20.

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

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

or equivalently

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

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 one the qubit above the $\oplus$. For example,

represents the operation defined by

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

Definition 23 (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

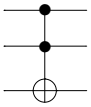
Again, the two $\times$ do not have to be on adjacent lines.

Definition 24 (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:

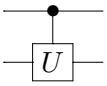


As with the CNOT, the two dots can be on arbitrary lines, not only those adjacent to the $\oplus$. Furthermore, the symbol generalises to more than two controlling qubits in the obvious way.

Definition 25 (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*

$$C(U)|0, j\rangle = |0, j\rangle$$
$$C(U)|1, j\rangle = |1\rangle \otimes U|j\rangle.$$

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 26 (Composite systems and states) *Given n quantum systems $\mathcal{H}_i$, the* composite system *is $\mathcal{H}_1 \otimes \ldots \otimes \mathcal{H}_n$.*

Given n quantum states $|\Psi_i\rangle \in \mathcal{H}_i$, the composite state *consisting of n independent subsystems in states $|\Psi_i\rangle$ is*

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

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.

Definition 28 (Composite measurements) *Given a measurement M_1 specified by projections $P_1, \ldots, P_n$ on $\mathcal{H}_1$ and a measurement M_2 specified by projections $P'_1, \ldots, P'_m$ 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 $i = 1, \ldots, n$ and $j = 1, \ldots, m$. (I.e., the possible outcomes of M are pairs i, j with $i = 1, \ldots, n$ and $j = 1, \ldots, m$.)*

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 $P_1, \ldots, P_n$, then M' consists of $P_1 \otimes I, \ldots, P_n \otimes I$.

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 $polylog(1/\varepsilon) + exp(n)$ 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 φ which is physically irrelevant). The construction is very efficient in terms of the error ε, 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 $f : \{0,1\} \to \{0,1\}$. We ask the question which of the following two cases applies:

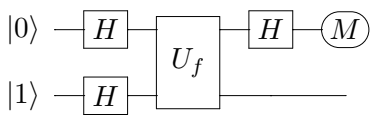
- f is constant ($f(0) = f(1)$), or
- f is balanced ($f(0) \neq f(1)$).

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

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

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

Deutsch's algorithm performs the following operations:



(Here —(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 algorihm, the Deutsch-Jozsa algorithm, can even handle functions $f : \{0,1\}^n \to \{0,1\}$ 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].

9 Density Operators

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

Definition 29 (Quantum state probability distribution) *A* quantum state probability distribution *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 quantum state probability distributions.

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

Then applying U to the quantum state probability distribution E leads to the quantum state probability distribution

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

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

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

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

After measuring the outcome j, the system state is described by the following quantum state probability distribution:

$$\left\{ \frac{Q_j|\Psi_i\rangle}{\|Q_j|\Psi_i\rangle\|} \ @ \ \frac{p_i\|Q_j|\Psi_i\rangle\|^2}{\Pr[\textit{Outcome } j]} \right\}_i.$$

Definition 32 (Extending the state space) *Let $E = \{|\Psi_i\rangle @ p_i\}_i$ be an quantum state probability distribution 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 quantum state probability distribution 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 quantum state probability distributions physically indistinguishable if all sequences of operations according to Definitions 30, 31, and 32 lead to the same probabilities of measurement outcomes.*

A density operator is a compact representation of a quantum quantum state probability distribution. This representation looses some information contained in the description of an quantum state probability distribution,[6] 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 state probability distribution over $\mathcal{H}$. The* density operator (density matrix, mixed state) *corresponding to E is the linear transformation ρ_E on $\mathcal{H}$ defined as follows:*

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

We call ρ a density operator over $\mathcal{H}$ if it is a density operator for some quantum state probability distribution 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 $|\Psi\rangle \in \mathcal{H}$.

[6] E.g., the following two quantum state probability distributions 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 $|-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$.

- A pure state is a density operator of the form $|\Psi\rangle\langle\Psi|$ (i.e., a density operator corresponding to an quantum state probability distribution 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 ρ leads to the state $U\rho U^\dagger$.

Definition 36 (Measurement) *Let $M = \{Q_1, \ldots, Q_n\}$ 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 ρ with M, the outcome j has probability

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

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

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

Then extending the state ρ 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 state probability distributions.

Theorem 2 *Let E, E' be quantum state probability distributions over $\mathcal{H}$ and ρ, ρ' 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 ρ and does not assume that there is some hidden quantum state probability distribution behind this state that contains more information than the density operator ρ.

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 $\operatorname{tr} \rho = 1$).

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 $\mathrm{tr}_B : S(\mathcal{H}_A \otimes \mathcal{H}_B) \to S(\mathcal{H}_A)$ *is the linear transformation defined by*

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

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 $\rho^A := \mathrm{tr}_B \rho$ describes the state resulting from destroying (or locking away) the B-part of the system. Or equivalently, ρ^A represents all information that can be extracted about the state ρ 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*

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

We call Ψ a *purification* of ρ. 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 $\mathcal{E} : S(\mathcal{H}) \to S(\mathcal{H}')$ of the form*

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

where $E_k : \mathcal{H} \to \mathcal{H}'$ 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 operator E_k are called the* Kraus operators *of $\mathcal{E}$.*

Quantum operations describe all operations that can be applied to a mixed state ρ, 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 *$\mathcal{E} : S(\mathcal{H}) \to S(\mathcal{H}')$ is a quantum operation if and only if it satisfies the following three conditions:*

- *It is linear.*
- *It is trace-preserving (i.e., $\operatorname{tr} \mathcal{E}(\rho) = \operatorname{tr} \rho$).*
- *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].

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 $\mathrm{SD}(X, Y)$ *between X and Y is defined as*

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

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*

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

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 $\mathrm{SD}(R, I)$ is sufficiently small.

Lemma 4
- *The statistical distance* SD *is a metric (on the set of probability distributions over a given set A).*
- *For any (possibly randomized) function F we have that*

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

If F is injective, equality holds.

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

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

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

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 $\mathrm{TD}(\sigma, \rho)$ *as*

$$\mathrm{TD}(\sigma, \rho) := \tfrac{1}{2} \operatorname{tr}|\sigma - \rho|.$$

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*

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

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 σ and ρ 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*

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

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

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

Lemma 7
- *The trace distance* 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*

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

  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*

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

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 $\mathrm{tr}\, P\rho \geq 1 - \varepsilon$ (i.e., the measurement $\{P_{yes} := P, P_{no} := 1 - P\}$ returns yes with high probability).*

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

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

(b) There are states $|\Psi_i\rangle \in \mathrm{im}\, P$ 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 ρ', the measurement would always return yes, i.e., ρ' satisfies the property specified by P.)

This lemma gives a criterion to show that the trace distance between some state ρ 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*

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

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 ρ and σ 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+09], and about 140 km through a wireless connection [SMWF+07].

Definition 43 (Security of QKD) *Let a QKD protocol π 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

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

By P_{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 π is ε-secure if the following holds: For every adversary Eve, we have that

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

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 $|\widetilde{xy}\rangle$ with $a, b \in \{0,1\}^n$ for the state $|\beta_{x_1y_1}\rangle \otimes |\beta_{x_2y_2}\rangle \otimes |\beta_{x_3y_3}\rangle \otimes \ldots \otimes |\beta_{x_ny_n}\rangle$. In particular, $|\widetilde{0\ldots0}\rangle = |\beta_{00}\rangle^{\otimes n} = \sum_{x\in\{0,1\}^n} |x\rangle \otimes |x\rangle$. (Note: we implicitly assume here that the qubits are reordered that the first qubits of each Bell state come before all the second qubits.)

The states $|\widetilde{xy}\rangle$ with $x, y \in \{0,1\}^n$ form a basis of $\mathbb{C}^{2^{2n}}$ ($2n$-qubit systems).

We will analyze the following QKD protocol:

Definition 45 (QKD protocol)
Parameters:

- *m: Number of qubits exchanged over the channel.*
- *q: Number of qubit pairs checked during Bell test ($q < n$).*
- *n: Length of raw key ($n = m - q$).*
- *t: Maximum number of errors in raw key.*
- *H: Parity check matrix of a linear binary error correcting code with n bit codewords, correcting t errors. (See Definition 48.)*
- *k: Bitlength of unencoded messages in that code. (H is a $\mathbb{F}_2^{(n-k)\times n}$ matrix.)*
- *ℓ: The length of the final key.*
- *s: the length of the seed of the universal hash function.*
- *$F : \{0,1\}^s \times \{0,1\}^n \to \{0,1\}^\ell$: a universal hash function. (See Definition 51.)*

Protocol:

Step 1. *Alice prepares the $2m$-qubit state $|\widetilde{00}\rangle$ and sends the second half of each qubit pair to Bob over the insecure quantum channel. (We call the joint state of Alice, Bob, Eve after this state ρ_{init}.)*

Step 2. *Alice and Bob perform the "Bell test" (see Definition 46 below). (This reduces the number of qubit pairs from m to n. We call the joint state ρ_{test}.)*

Step 3. *Alice and Bob measure their respective n-qubit quantum systems in the computational basis. Call the measurement outcomes K_A, K_B. ("Raw keys.". We call the joint state ρ_{raw}.)*

Step 4. *Alice sends $\sigma := HK_A$ to Bob (over the authenticated channel). Bob finds e with $He = \sigma + HK_B$ and $|e| \leq t$. Then Bob updates his key to be $K'_B := K_B \oplus e$. (Such an e is unique and can efficiently be found if it exists by definition of error correcting codes. We call the joint state ρ_{corr}.))*

Step 5. *Privacy amplification: Alice picks $S \in \{0,1\}^s$ and sends S to Bob. Alice computes $K''_A := F(S, K_A)$, Bob computes $K''_B := F(S, K'_B)$. K''_A and K''_B are the final key. (If all goes well, $K''_A = K''_B$.)*

We claim that for suitable choices of parameters, this protocol is a secure QKD protocol in the sense of Definition 43. We now proceed to analyze the protocol step by step. After Step 1, Alice and Bob have m qubits each, but besides that, we make not claims about the structure of ρ_{init}. (Since the communication went over the insecure channel, Eve could have modified it arbitrarily.)

13.1 Bell test

We now describe Step 2 in more detail, and analyze what we can say about the state ρ_{test} after that step.

Definition 46 *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 ρ using one of the following measurements:*
  - *$P_{yes} := |\beta_{00}\rangle\langle\beta_{00}| + |\beta_{01}\rangle\langle\beta_{01}|$ and $P_{no} := 1 - P_{yes}$. (I.e., we check that the state is not $|\beta_{10}\rangle$ or $|\beta_{11}\rangle$.)*
  - *$P_{yes} := |\beta_{00}\rangle\langle\beta_{00}| + |\beta_{10}\rangle\langle\beta_{10}|$ and $P_{no} := 1 - P_{yes}$. (I.e., we check that the state is not $|\beta_{01}\rangle$ or $|\beta_{11}\rangle$.)*
- *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).

For the analysis, we fix the following notation:

For $x, y \in \{0,1\}^m$, by $|x.y|$ we denote the number of bitpairs in xy that are not 00. More precisely, $|x.y| = |\{i : x_i \neq 0 \vee y_i \neq 0\}|$.

Let P_{ok} be the projector $\sum_{|x.y| \leq t} |\widetilde{xy}\rangle\langle\widetilde{xy}| \otimes I_E$ (where I_E 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 precisely, given a state $\rho \in S(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E)$, $T(\rho) := p\tilde{\rho}$ where $\tilde{\rho}$ is the state after passing the Bell test and p is the probability of passing the Bell test. Note that $\tilde{\rho} = \frac{T(\rho)}{\operatorname{tr} T(\rho)}$.[7]

Recall that ρ_{init} is the state that Alice and Bob hold in the QKD protocol before the Bell test. If $\rho_{init} = |\widetilde{0\dots0}\rangle\langle\widetilde{0\dots0}|$ (i.e., Eve has not disturbed the state), then the Bell test passes with probability 1. If $\rho_{init} = |\widetilde{xy}\rangle\langle\widetilde{xy}|$ where for more than t indices i, $x_i y_i \neq 00$ (i.e., Eve has disturbed a lot), the Bell test passes with probability at most $\delta_q := (1 - \frac{t+1}{2m})^q$. 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, δ_q converges exponentially fast to 0 for $m, q \to \infty$.

[7] 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 ≤ 1.

Lemma 10 *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 $\tilde{\rho} := \frac{T(\rho)}{\operatorname{tr} T(\rho)}$ (the state after passing the Bell test). Let $P_{success} := \operatorname{tr} T(\rho)$ (the probability of passing the Bell test).

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

In the following, let *t-Error* denote the set of states $|\Psi\rangle$ that are a superposition of states $|\tilde{x}\rangle$ with $|x| \leq t$, and with an arbitrary state on Eve's side. (In other words, in $|\Psi\rangle$, at most t bad qubit pairs occur.) Formally,

$$t\text{-}Error := span\{|\tilde{x}\rangle \otimes |\Psi^E\rangle : |x| \leq t, |\Psi^E\rangle \text{ arbitrary}\}.$$

Let $S_{\text{Ideal}}^{t\text{-}Error}$ be the set of all states that are mixtures of states in *t-Error*. Formally,

$$S_{\text{Ideal}}^{t\text{-}Error} := \Big\{\sum_i p_i |\widetilde{\Psi_i}\rangle\langle\widetilde{\Psi_i}| : \sum_i p_i = 0, \forall i.\, p_i \geq 0, \forall i.\, |\Psi_i\rangle \in t\text{-}Error\Big\}.$$

We have

Lemma 11 *For any adversary Eve, there exists a state $\rho_{test}^{ideal} \in S_{\text{Ideal}}^{t\text{-}Error}$ such that $\operatorname{TD}(\rho_{test}, \rho_{test}^{ideal}) \cdot P_{success} \leq \sqrt{\delta_q}$. Here $P_{success}$ is the probability of passing the Bell test.*

To see this, note that $\rho_{test} = \frac{T(\rho_{init})}{\operatorname{tr} T(\rho_{init})}$ and $P_{success} = \operatorname{tr} T(\rho_{init})$, and that $S_{\text{Ideal}}^{t\text{-}Error}$ is the set of all states $\sum_i p_i |\Psi_i\rangle$ with $|\Psi_i\rangle \in \operatorname{im} P_{ok}$. Then Lemma 8 implies $\operatorname{TD}(\tilde{\rho}, \rho') \leq \sqrt{\frac{\delta_q}{P_{success}}}$ from we $\operatorname{TD}(\rho_{test}, \rho_{test}^{ideal}) \cdot P_{success} \leq \sqrt{\delta_q}$ immediately follows.

Note: compare this lemma with the definition of secure QKD schemes (Definition 43). Basically, the lemma shows that the protocol until Step 2 is a secure QKD-protocol, except that the set of ideal state S_{Ideal} is replaced by $S_{\text{Ideal}}^{t\text{-}Error}$ which consists of states where Alice and Bob have Bell pairs with at most t errors. So basically, we have shown that we have a $\sqrt{\delta_q}$-secure "t-error Bell state distribution protocol".

13.2 Measuring the raw key

In Step 3, Alice and Bob measure the raw key K_A, K_B. Note that the raw key is not necessarily a good key yet. For example, we do not have the guarantee that $K_A = K_B$, and Eve might have partial information about K_A or K_B.

But the raw key is not all bad. In this section we analyze what useful properties it does have.

Lemma 12 *If $\rho_{test} \in S_{\text{Ideal}}^{t\text{-}Error}$, then, after Step 3, with probability 1 we have $|K_A \oplus K_B| \leq t$.*

This was proven on a homework sheet. Since Lemma 11 guarantees that ρ_{test} will be close to $S_{\text{Ideal}}^{t\text{-}Error}$, we know that $|K_A \oplus K_B| \leq t$ with high probability.

Lemma 13 *If $\rho_{test} \in S_{\text{Ideal}}^{t\text{-}Error}$, then, for any algorithm that accesses only Eve's state in ρ_{raw} and outputs a guess K_E of Alice's key, we have $\Pr[K_A = K_E] \leq (3n+1)^t 2^{-n}$.*

This was shown in the practice session.

Lemma 13 allows us to quantify the so-called min-entropy of the raw key. The min-entropy is a measure of uncertainty that has a lot of importance in cryptography, and is defined as follows:

Definition 47 (Min-entropy) *Let $\mathcal{H}_K \otimes \mathcal{H}_B \otimes \mathcal{H}_E$ with $\mathcal{H}_K = \mathbb{C}^{\mathbf{K}}$ be a tripartite system. Let ρ be a cqq-state[8] on this system. ($\mathcal{H}_K$ represents the part of the state containing the key, $\mathcal{H}_E$ Eve's part of the system, and $\mathcal{H}_B$ any other parts of the system not belonging to the key or Eve.)*

We define the min-entropy as:

$$H_\infty(K|E)_\rho := -\log \max_{i,M} \Pr[K = M \text{ given } \rho].$$

Here $i \in \mathbb{N}$, and M ranges over arbitrary quantum algorithms with input in $\mathcal{H}_E$ and classical output.

By "$\Pr[K = M$ given $\rho]$" we mean the following probability: Measure the system $\mathcal{H}_K$ in the computational basis. Run the algorithm M on system $\mathcal{H}_E$. Then the outcomes of the two measurements are equal.

The intuition behind this definition is again that $2^{-H_\infty(K|E)_\rho}$ is the maximum probability that Eve guesses the key K (contained in $\mathcal{H}_K$) while having access to the system $\mathcal{H}_E$. Notice that the definition assumes that the subsystem $\mathcal{H}_K$ contains a classical key. The definition of min-entropy generalizes to the case that all systems contain quantum data. However, in that case the definition is considerably less intuitive.

By definition of H_∞, we can restate Lemma 13 as follows:

Lemma 14 *If $\rho_{test} \in S_{\text{Ideal}}^{t\text{-}Error}$ then*

$$H_\infty(K_A|E)_{\rho_{raw}} \geq -\log\big((3n+1)^t 2^{-n}\big) = n - t\log(3n+1).$$

(Here in slight abuse of notation we write K_A for Alice's subsystem.)

Let

$$S_{\text{Ideal}}^{raw} := \{\rho : K_A, K_B \text{ are classical in } \rho,\ H_\infty(K_A|E)_\rho \geq n - t\log(3n+1),\\ |K_A \oplus K_B| \leq t \text{ in } \rho\}$$

From Lemma 13 and Lemma 14 we immediately get:

Lemma 15 *If $\rho_{test} \in S_{\text{Ideal}}^{t\text{-}Error}$ then $\rho_{raw} \in S_{\text{Ideal}}^{raw}$.*

[8] A *cqq-state* means a state that is classical (c) in the first component, and potentially quantum (q) in the second and third. More precisely, $\rho = \sum_x p_i |x\rangle\langle x| \otimes \rho_i$ with $\rho_i \in S(\mathcal{H}_B \otimes \mathcal{H}_E)$.

And combining this with Lemma 11, we get

Lemma 16 *For any adversary Eve, there exists a state* $\rho_{raw}^{ideal} \in S_{\text{Ideal}}^{raw}$ *such that* $\text{TD}(\rho_{raw}, \rho_{raw}^{ideal}) \cdot P_{success} \leq \sqrt{\delta_q}$. *Here* $P_{success}$ *is the probability of passing the protocol up to this point.*

(We used here implicitly that the trace distance can only decrease under quantum operations (Lemma 7) and that Step 3 is a quantum operation. We also used that the probability of success $P_{success}$ does not change after the Bell test any more, since the protocol can only abort during the Bell test.)

Basically, Lemma 16 shows that until Step 3, we have a $\sqrt{\delta_q}$-secure "leaky and not-exactly-the-same key distribution protocol".

13.3 Error-correction

In Step 4, make sure that Alice and Bob have the same key. To understand this step, we need some basics about error correcting codes, first.

Definition 48 (Error correcting code) *A (linear binary)* error correcting code *with codewords of length* n, *messages of length* m, *and correcting* t *errors consists of the following parts:*

- *A polynomial-time encoding algorithm that maps* $m \in \{0,1\}^k$ *into a codeword* $c \in \{0,1\}^n$. *Since the code is linear,* $c = Gm$ *for some fixed matrix* $G \in \mathbb{F}_2^{n \times k}$ *(the "generator matrix"). Let* C *be the set of all codewords, i.e., the image of* G.
- *A polynomial-time decoding algorithm that maps a codeword* $c \in C$ *to the original message* m *with* $c = Gm$. *(This can be done, e.g., by solving the linear equation system* $c = Gm$ *for unknown* m.*)*
- *A parity check matrix* H, *that is defined such that* $Hc = 0$ *iff* $c \in C$. *We call* Hc' *the syndrome of* c'. *Since* $H(c \oplus e) = He$ *for* $c \in C$, *the syndrome of a codeword with errors* e *only depends on the errors* e, *not on* c.
- *A polynomial-time error correction algorithm. Given a* $c' \in \{0,1\}^n$ *such that there exists a* c *with* $|c \oplus c'| \leq t$, *the algorithm finds* c. *(Think of* c' *as a codeword with errors.)*

Note that if H is a parity check matrix of a code that corrects t errors, then we have the following property: Given $\sigma = He$ for some e with $|e| \leq t$, we can efficiently find e. This is done as follows: Find some c' with $Hc' = \sigma$. Then $H(c' \oplus e) = 0$, hence $c := c' \oplus e$ is a valid codeword, and $|c \oplus c'| \leq t$. Thus the decoding algorithm applied to c' returns c. And thus we can compute $e := c \oplus c'$.

This is what we do in Step 4. Assume that $|K_A \oplus K_B| \leq t$. Then Bob searches an e such that $He = H(K_A \oplus K_B)$. This will be $e = K_A \oplus K_B$. Hence $K'_B = K_A$. Thus we have:

Lemma 17 *If* $\rho_{raw} \in S_{\text{Ideal}}^{raw}$, *then in* ρ_{corr} *we have* $K'_B = K_A$. *(With slight abuse of notation, we now refer to Bob's system by* K'_B.

Thus Step 4 makes sure that Alice and Bob have the same key. However, sending σ over the network means that Eve learns additional information about the key. The following fact about min-entropy shows that Eve cannot learn more than $n-k$ bits (where $n-k$ is the length of σ).

Lemma 18 (Chain rule) *For any density operator ρ, $H_\infty(X|YE)_\rho \geq H_\infty(XY|E)_\rho - \ell$ if Y is an ℓ-bit system.*[9]

From Lemma 18, we can conclude that the min-entropy decreases at most by $n-k$, hence:

Lemma 19 *If $\rho_{raw} \in S^{raw}_{\text{Ideal}}$, then $H_\infty(K_A|E)_{\rho_{corr}} \geq H_\infty(K_A|E)_{\rho_{raw}} - (n-k) \geq k - t\log(3n+1)$.*

Let

$$S^{corr}_{\text{Ideal}} := \{\rho : K_A, K'_B \text{ are classical in } \rho,\ H_\infty(K_A|E)_\rho \geq k - t\log(3n+1),\ K_A = K'_B \leq t \text{ in } \rho\}$$

From Lemma 17 and Lemma 19 we then immediately have:

Lemma 20 *If $\rho_{raw} \in S^{t\text{-}Error}_{\text{Ideal}}$ then $\rho_{corr} \in S^{corr}_{\text{Ideal}}$.*

And combining this with Lemma 16, we get

Lemma 21 *For any adversary Eve, there exists a state $\rho^{ideal}_{corr} \in S^{corr}_{\text{Ideal}}$ such that $\text{TD}(\rho_{corr}, \rho^{ideal}_{corr}) \cdot P_{success} \leq \sqrt{\delta_q}$. Here $P_{success}$ is the probability of passing the protocol up to this point.*

(We used here implicitly that the trace distance can only decrease under quantum operations (Lemma 7) and that Step 4 is a quantum operation on the joint state of Alice, Bob, Eve. We also used that the probability of success $P_{success}$ does not change after the Bell test any more, since the protocol can only abort during the Bell test.)

Basically, Lemma 24 shows that until Step 4, we have a $\sqrt{\delta_q}$-secure "leaky key distribution protocol".

13.4 Privacy amplification

After Step 4, Alice and Bob have the same key (with high probability), but Eve might still have partial information about that key. To get rid of the remaining knowledge of Eve, Alice and Bob perform "privacy amplification". The idea here is to apply a function F to the key such that, if Eve has only partial knowledge of the input K_A to F, then Eve has (close to) no knowledge about the output of F. That is, F should transform something weakly random into something (close to) uniformly random. The main tool is a so-called strong quantum randomness extractor (or simple strong quantum extractor).

[9] This even holds if X and Y are not classical. Notice that our definition of H_∞ only allows to talk about classical X, Y, but more general definitions exist [Ren05].

Definition 49 (Strong quantum extractor) *A function $F : S \times X \to Y$ is a* strong (k, ε)-quantum extractor *iff the following holds:*

Consider a multi-partite quantum system $\mathcal{H}_X \otimes \mathcal{H}_E$ with $\mathcal{H}_X = \mathbb{C}^X$. Let $\mathcal{H}_S := \mathbb{C}^S$, $\mathcal{H}_Y := \mathbb{C}^Y$. Consider a cq-state ρ (i.e., ρ is of the form $\rho = \sum_x p_x |x\rangle\langle x| \otimes \rho_x$). Assume that $H_\infty(K|E)_\rho \geq k$.

Let

$$\rho_{extr} := \sum_{x,s} \tfrac{1}{|S|} p_x |F(s,x)\rangle\langle F(s,x)| \otimes \rho_x \otimes |s\rangle\langle s| \in S(\mathcal{H}_Y \otimes \mathcal{H}_E \otimes \mathcal{H}_S).$$

That is, ρ_{extr} is the result of adding a register S containing a random value (the seed) to ρ and then replacing X by $F(S, X)$.

Let

$$\rho_{perf} := \left(\sum\nolimits_y \tfrac{1}{|Y|} |y\rangle\langle y|\right) \otimes \left(\sum\nolimits_x p_x \rho_x\right) \otimes \left(\sum\nolimits_r \tfrac{1}{|R|} |r\rangle\langle r|\right) \in S(\mathcal{H}_Y \otimes \mathcal{H}_E \otimes \mathcal{H}_S).$$

That is, ρ_{perf} is the result of adding a register S containing a random value (the seed) to ρ and then replacing X by a random value from Y.

Then $\mathrm{TD}(\rho_{extr}, \rho_{perf}) \leq \varepsilon$.

Intuitively, this means that as long as $H_\infty(K|E)_\rho \geq k$, one cannot distinguish between $F(S, X)$ and uniformly random Y, even given E and S.

For comparison, here is the definition of a classical strong extractor:

Definition 50 (Strong extractor) *A function $F : S \times X \to Y$ is a* strong (k, ε)-extractor *iff the following holds:*

Consider random variables $X \in X$ and E with $H_\infty(X|E) \geq k$. Let $S \in S$ and $Y \in Y$ be uniformly random and independent of each other and X, E.

Then

$$\mathrm{SD}\Big((F(S,X), E, S);\ (Y, E, S)\Big) \leq \varepsilon.$$

This is the same as the strong quantum extractor, except that now all registers are classical (even E), which makes notation much simpler. In particular, a strong (k, ε)-quantum extractor is a strong (k, ε)-extractor.

Examples for strong quantum extractors are so-called universal hash functions (a.k.a. two-universal hash functions):

Definition 51 (Universal hash function) *A function $f : S \times X \to Y$ is a* universal hash function (UHF) *iff for all $x, y \in X$ with $x \neq y$, we have that*

$$\Pr[f(s,x) = f(s,y) : s \xleftarrow{\$} S] \leq \tfrac{1}{|Y|}.$$

Here $s \xleftarrow{\$} S$ means that s is uniformly randomly chosen from S.

Universal hash functions are known to be strong extractors, even in the quantum case:

Lemma 22 (Leftover hash lemma, quantum-variant) *Let $f : S \times X \to Y$ be a universal hash function with $|Y| \leq 2^\ell$. Let $k \geq 0$. Let $\varepsilon := 2^{-\frac{1}{2}(k-\ell)-1}$. Then f is a strong (k, ε)-quantum extractor.*

We can now analyze Step 5. Before Step 5, we have the state ρ_{corr}. If $\rho_{corr} \in S^{corr}_{\text{Ideal}}$, then $K_A = K'_B$ in ρ_{corr}, and thus also $K''_A = K''_B$ in ρ_{priv}.

Furthermore, if $\rho_{corr} \in S^{corr}_{\text{Ideal}}$, then $H_\infty(K_A|E)_{\rho_{corr}} \geq k - t\log(3n+1) =: d$. Let $\rho^{AE}_{corr} := \text{tr}_B \rho_{corr}$ and $\rho^{AE}_{priv} := \text{tr}_B \rho_{priv}$. Note that ρ_{priv} differs from ρ_{corr} besides other things in that the seed S is now added to Eve's state E. Then $H_\infty(K_A|E)_{\rho^{AE}_{corr}} \geq d$, and ρ^{AE}_{priv} is the state ρ_{extr} from Definition 49 (if we set $\rho := \rho^{AE}_{corr}$ in that definition). Since F is a strong (d, γ)-quantum extractor by Lemma 22 for $\gamma := 2^{-\frac{1}{2}(d-\ell)-1}$, it follows by Definition 49 that ρ^{AE}_{priv} has statistical distance γ from a state of the form $\rho^{AE}_{ideal} := \left(\sum_y \frac{1}{|Y|}|y\rangle\langle y|\right) \otimes \rho_E$ for some ρ_E. (ρ_E here contains the second and the third tensor factor of ρ_{priv} from Definition 49.)

Let $\mathcal{E}$ denote the quantum operation that copies the (classical) register A into a register B. Since $K''_A = K''_B$ in ρ_{priv} (still assuming $\rho_{corr} \in S^{corr}_{\text{Ideal}}$), we have that $\rho_{priv} = \mathcal{E}(\rho^{AE}_{priv})$. Let $\rho_{ideal} := \mathcal{E}(\rho^{AE}_{ideal})$. Since $\text{TD}(\rho^{AE}_{priv}, \rho^{AE}_{ideal}) \leq \gamma$, with Lemma 7 we get $\text{TD}(\rho_{priv}, \rho_{ideal}) = \text{TD}(\mathcal{E}(\rho^{AE}_{priv}), \mathcal{E}(\rho^{AE}_{ideal})) \leq \gamma$. Furthermore, note that $\rho_{ideal} = \left(\sum_y \frac{1}{|Y|}|y\rangle\langle y| \otimes |y\rangle\langle y|\right) \otimes \rho_E \in S_{\text{Ideal}}$.

Thus we have:

Lemma 23 *If $\rho_{corr} \in S^{corr}_{\text{Ideal}}$, then there is a $\rho_{ideal} \in S_{\text{Ideal}}$ with $\text{TD}(\rho_{priv}, \rho_{ideal}) \leq \gamma$.*

Combining this with Lemma 24 we get

Lemma 24 *For any adversary Eve, there exists a state $\rho^{ideal} \in S_{\text{Ideal}}$ such that $\text{TD}(\rho_{priv}, \rho^{ideal}) \cdot P_{success} \leq \sqrt{\delta_q} + \gamma$. Here $P_{success}$ is the probability of passing the protocol up to this point.*

Since ρ_{priv} is the final state of the protocol from Definition 45, and $\delta_q = (1 - \frac{t+1}{2m})^q$ and $\gamma = 2^{-\frac{1}{2}(k-t\log(3n+1)-\ell)-1}$, we immediately get:

Theorem 5 (Security of QKD) *The protocol from Definition 45 is ε-secure in the sense of Definition 43 for*

$$\varepsilon := \left(1 - \tfrac{t+1}{2m}\right)^{q/2} + 2^{-\frac{1}{2}(k-t\log(3n+1)-\ell)-1}.$$

Further reading: [NC00, Section 12.6]. (However, things are a very vague there.)

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 *open phase* (also known as

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 open phase, both Alice and Bob have no input. Bob outputs a bit $b' \in \{0,1\}$ or aborts.[10] 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 open 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 52 (Correctness) *We call a commitment protocol* ε_C-correct *if for honest Alice and Bob, and for any Alice-input* $b \in \{0,1\}$*, when executing the commit and the open phase, the probability that Bob outputs* $b' = b$ *in the open phase is at least* $1 - \varepsilon_C$*.*

Definition 53 (Hiding) *We call a commitment protocol* ε_H-hiding *if the following holds: Fix some malicious Bob. Let* ρ_b *be the state of honest Alice's and malicious Bob's system after performing the commit phase with Alice-input* b*. Then*

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

Definition 54 (Binding) *We call a commitment protocol* ε_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 open phase. Then*

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

Intuitively, this means that Alice cannot open as 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 25 (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*

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

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

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

[10] 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.

Lemma 26 (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 $\mathrm{tr}_A|\Psi\rangle\langle\Psi| = \mathrm{tr}_A|\tilde{\Psi}\rangle\langle\tilde{\Psi}|$. Then there are orthonormal sets of states*

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

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 27 (Purification of the commit phase) *Assume a commitment protocol π that is ε_C-correct, ε_H-hiding, and ε_B-binding. Then there is a commitment protocol $\tilde{\pi}$ that is ε_C-correct, ε_H-hiding, and ε_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 27 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 6 (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 ε_C-correct ε_H-hiding ε_B-binding commitment protocols might exist for small but non-zero $\varepsilon_C, \varepsilon_H, \varepsilon_B$. A more careful analysis, however, excludes this [May97].

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 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 open 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 Ψ_i. More precisely, 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 $|\Psi_1\rangle, \ldots, |\Psi_m\rangle$ 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 $\tilde{x}_i$.
- *Open 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 7 (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, $m \geq (4+\delta)n$. Then there is a negligible function μ 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 open phase can be shown to be secure.

For the proof of Theorem 7, we need a variant of the definition of min-entropy, the smooth min-entropy. We only give the formal definition in the classical case:

Definition 55 (Smooth min-entropy) *Fix $\rho \in S(\mathcal{H}_X \otimes \mathcal{H}_Y \otimes \mathcal{H}_Z)$. The* (conditional) smooth min-entropy $H_\infty^\varepsilon(X)$ *is defined as $H_\infty^\varepsilon(X|Y)_\rho := \sup_{\rho'} H_\infty(X|Y)_\rho$. Here ρ' ranges over all positive ρ' with $\operatorname{tr}\rho \leq 1$ and $\mathrm{TD}(\rho,\rho') \leq \varepsilon$.*

Intuitively, having smooth min-entropy $\alpha = H_\infty^\varepsilon(X)$ means having min-entropy α except in rare cases which happen with probability at most ε.

Note: we quantify over all ρ' with $\operatorname{tr}\rho \leq 1$, which makes the definition less intuitive, because ρ' is not a quantum state in that case. If you change the definition to require "$\operatorname{tr}\rho = 1$", you get a similar definition, and the results in this section still apply (possibly with slightly changed values for the ε's). However, the definition as defined here behaves better in certain settings and was introduced in [Ren05]. Some definitions also use a different distance measure than TD, e.g., the "purified distance" [Tom16].

Theorem 8 (Uncertainty relation) *Fix a constant $\lambda > 0$. Let $\rho \in S(\mathcal{H}_X \otimes \mathcal{H}_Y)$ with $\mathcal{H}_X = \mathbb{C}^{2^m}$ and with Y being classical. Let $b_1, \ldots, b_m \in \{+, \times\}$ be uniformly and independently chosen bases ($+$ denotes the computational, and $\times$ the diagonal basis). Let x_i denote the result of measuring the i-th bit of X in ρ in basis b_i. Then there exists a negligible ε such that*

$$H_\infty^{\varepsilon(m)}(x_1, \ldots, x_m | b_1, \ldots, b_m, Y) \geq 0.48m.$$

This theorem states that if we are given an arbitrary state ρ (that about which we may know as much 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 8 is shown in [DFR$^+$07] (Corollary 3.4 in the full version). (Without the Y register.)

The chain rule (Lemma 18) also holds for smooth min-entropy:

Lemma 28 (Chain rule [Ren05]) *For any density operator ρ, $H_\infty^\varepsilon(X|YE)_\rho \geq H_\infty^\varepsilon(XY|E)_\rho - n$ if Y is an n-bit system.*[11]

Lemma 29 (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*

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

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

Intuitively, this lemma means that if we have an uncertainty α 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 29 is shown in [DFR$^+$07] (Corollary 4.3 in the full version).

Lemma 30 *Let $\varepsilon > 0$. Let ρ be a cq-state consisting of quantum systems X and E. I.e., we have a state $\rho = \sum_{xb} p_{xb} |x\rangle\langle x| \otimes \rho_x$.*

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

Then

$$\Pr[X = \tilde{X}] \leq 2^{-H_\infty^\varepsilon(X|E)} + \tfrac{3}{2}\varepsilon.$$

[11] This even holds if X and Y are not classical.

Notice that for $\varepsilon = 0$, this follows from the definition of min-entropy (Definition 47).

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+07]. For definitions of min-entropy in the quantum case and a lot of results concerning these, see [Ren05]. A proof that the definition of min-entropy as given here is equivalent to that in [Ren05] can be found in [KRS09].

15 Revocable quantum time vaults

A time vault TV is, intuitively, a kind of encryption which can be broken in time T, but not in time $\ll T$.

The idea behind this is that one can use a time vault to send messages into the future. If Alice wants Bob to have some information m after time T, but not before that, she sends $TV(m)$ to Bob, and Bob will only be able to compute m after time T.

A physical intuition for a time vault is that of a strong box with a timer. The strong box opens automatically at time T, but cannot be opened earlier.

Mathematically, a time vault is modeled as a probabilistic algorithm TV that takes a message m and returns a time vault $TV(m)$. Additionally, there should be another algorithm Dec that the honest recipient can use to recover m from $TV(m)$.

A time vault should, ideally, have the following security:

Definition 56 (T-hiding time vault) *We call a time vault TV T-*hiding *if the following holds: For any probabilistic T-time adversary B^*, there is a negligible μ such that for for any η, and any m_0, m_1 (in the message space of TV), we have that $|\Pr[P_0 - P_1]|$ is negligible in η where $P_i := \Pr[b = 1 : V \leftarrow TV(m_i), b \leftarrow B^*(1^\eta, V)]$.*

Here T and TV may implicitly depend on the security parameter η. And $x \xleftarrow{\$} A$ means that x that is the output of algorithm A.

We say TV is T-hiding against quantum adversaries *if the above holds for all quantum T-time adversaries B^*.*

This means that before time T, no adversary can find out anything about the message m from $TV(m)$ (except with negligible probability).

However, T-hiding time-vaults do not capture all the useful properties that strongboxes with timers have. Consider as an example the following situation (that might come straight from a movie). Alice has to go to a meeting with criminals. Alice fears that she might not survive the meeting, unless she has some way to pressure the criminals into letting her leave alive. A possible approach is to leave some compromising information about the criminals in the hands of some trusted friend Bob (e.g., evidence photos). If Alice does not return within a day, Bob is supposed to reveal the information to the police. The problem with this is that Alice might not wish Bob to get these photos except if Alice does not return from the meeting safely. Using strongboxes with timers, Alice

could achieve her goal: She puts the information into the strongbox, and puts the timer to $T := 1\,day$. If Alice does not return alive, Bob can open the strongbox after a day and deliver the information to the police. If Alice does return alive before time T, she asks the strongbox back. When she gets it back, she will know that Bob did not keep the information and cannot deliver it to the police or anyone else.[12]

What happens if we use (digital) time vaults to implement the above? In this case, there is no way how Bob can give back the time vault to Alice. Of course, he could just give back the bitstring $TV(m)$ to Alice, but that will not convince her of anything, because Bob could have made a copy of $TV(m)$. So Alice will never know whether Bob did not decrypt a copy of $TV(m)$ at his leisure. So, the following property is obviously impossible with classical time vaults:

Definition 57 (Revocably hiding time vaults – informal) *We call a time vault TV T-*revocably hiding *if there is some algorithm Rev (revocation) such that the following holds (even for malicious Bob): If Alice sends $TV(m)$ to Bob, and Bob sends back some value X after time at most T, and Alice runs $Rev(X)$, and Rev returns 1, then Bob does not learn anything about m later (even when computing considerably more time than T).*

Note that the reason that revocably hiding time vaults are impossible in the classical setting comes from the fact that a malicious Bob can just copy $TV(m)$. So, an obvious idea is to use a quantum state as a time vault. Then, at least, it is not obvious that Bob can just break the protocol by copying $TV(m)$.

The following protocol is a first candidate for a revocable time vault:

Definition 58 (A quantum time vault) *Assume a T-hiding time vault TV that is secure against quantum adversaries. Then the quantum time vault QTV is defined as follows:*

- *Upon input a message $m \in \{0,1\}^n$, pick n random bases $B = B_1 \dots B_n \in \{+,\times\}^n$.*
- *Encode the bits of m using in the bases $B_1, \dots, B_n$. We call the resulting state $|m\rangle_B$.*
- *Compute $V \leftarrow TV(B)$.*
- *Return $(|m\rangle_B, V)$ (for sending to Bob).*

The revocation algorithm Rev is as follows:

- *Input: An n-bit quantum register X (supposedly the state $|m\rangle_B$ that Bob returned to Alice).*
- *Measure X in bases B, call the outcome m'.*
- *If $m = m'$, Rev returns 1.*

Unfortunately, QTV does not guarantee that Bob learns nothing about m. Bob can guess some of the bases B correctly, and thus get some of the bits of m. Thus QTV is not T-revocably hiding in the sense of Definition 57. We can only show the weaker property that Bob cannot guess all of m (for a uniformly random message m) assuming

[12] Of course, Bob can just refuse to give the strongbox back. But in that case, Alice will at least know that Bob is cheating her, and this might already be sufficient to deter Bob.

the revocation succeeded. We say that QTV is *T-revocably one-way*. Strengthening QTV to be T-revocably hiding is ongoing research (but it looks promising). Formally, what we can show is the following:

Lemma 31 *For any pair B_1^*, B_2^* of machines such that B_1^* runs in quantum-time T and B_2^* runs in quantum polynomial-time, there is a negligible μ such that for all η the following holds:*

$$\Pr[m = m^* \text{ and } ok = 1 : m \xleftarrow{\$} \{0,1\}^\eta, X \leftarrow QTV(m), \\ X' \leftarrow B_1^*(1^\eta, X), ok \leftarrow Rev(X'), m^* \leftarrow B_2^*(1^\eta)] \leq \mu(\eta).$$

Here B_1^*, B_2^* may share state (i.e., whatever B_1^* has stored, B_2^* has later access to).

Proof sketch. The lemma is shown by considering a sequence of "games". The first represents what happens in the lemma, and all subsequent games are slight modifications of it. We derive the lemma by deriving various facts about the games. Differences between the games are highlighted in blue.

Game 1 (Original protocol)
(a) $B \xleftarrow{\$} \{+,\times\}^\eta$.
(b) $V \leftarrow TV(B)$.
(c) $m \xleftarrow{\$} \{0,1\}^\eta$.
(d) Initialize the quantum register X with $|m\rangle_B$.
(e) Adversary B_1^* gets V, X.
(f) Measure X in basis B, outcome m'.
(g) $ok := 1$ iff $m = m'$.
(h) Adversary B_2^* is run. Returns m^*.

Game 1 describes the situation in the lemma. Thus to show the lemma, we need to show that $\Pr[m = m^* \wedge ok = 1 : Game\ 1]$ is negligible. (The notation $\Pr[E : \text{Game } i]$ means the probability that E holds in Game i.)

We now modify the previous game. Instead of picking m at random and initializing X with $|m\rangle_B$, we put Bell pairs into XY, and then measure Y in the basis B to figure out what m is.

Also, instead of testing whether $m = m'$ where m and m' are what we get when measuring X, Y in basis B, we directly measure whether X and Y have the same state in basis B. More formally, we apply to XY the measurement described by the projector $P_B^=$ where $P_B^= = \sum_m |m\rangle\langle m| \otimes |m\rangle\langle m|$.

Game 2 (Using EPR pairs)
(a) $B \xleftarrow{\$} \{+,\times\}^\eta$.
(b) $V \leftarrow TV(B)$.
(c) ~~$m \xleftarrow{\$} \{0,1\}^\eta$.~~
(d) Initialize the quantum registers XY with $|\beta_{00}\rangle^{\otimes\eta}$.

(e) *Adversary* B_1^* *gets* V, X.
(f) ~~*Measure* X *in basis* B*, outcome* m'.~~
(g) ~~$ok := 1$ *iff* $m = m'$.~~
(h) *Apply measurement* $P_B^=$ *to* XY. $ok := 1$ *if measurement succeeds.*
(i) *Measure* Y *in basis* B*, outcome* m.
(j) *Adversary* B_2^* *is run. Returns* m^*.

We have that

$$\Pr[m = m^* \wedge ok = 1 : Game\ 1] = \Pr[m = m^* \wedge ok = 1 : Game\ 2] \tag{2}$$

Roughly, the reason is that we also get the state $|m\rangle\langle m|_B$ in X when we initialize XY with Bell pairs and compute x by measuring Y in basis B.

Next, we remove all computations that take more than time T from the game. This will allow us to use the T-hiding property of TV later on. Instead, we apply a test that tells us whether the state of the system is such that Bob (B_2^*) cannot ever guess m. The test that we do is whether XY contains Bell pairs (with up to t errors for suitably chosen t). For this, we apply the measurement described by the projector P_t^{Bell} where P_t^{Bell} is the projector onto t-*Error* (which in turn is defined in Section 13).

Game 3 (Testing the state)
(a) $B \xleftarrow{\$} \{+,\times\}^\eta$.
(b) $V \leftarrow TV(B)$.
(c) *Initialize* XY *with* $|\beta_{00}\rangle^{\otimes\eta}$.
(d) *Adversary* B_1^* *gets* V, X.
(e) *Apply measurement* $P_B^=$ *to* XY. $ok := 1$ *if measurement succeeds.*
(f) *Apply measurement* P_t^{Bell} *to* XY. $tErr := 1$ *if measurement succeeds.*
(g) ~~*Measure* Y *in basis* B*, outcome* m.~~
(h) ~~*Adversary* B_2^* *is run. Returns* m^*.~~

We have the following fact:

$$\Pr[tErr = 0 \wedge ok = 1 : Game\ 3] \text{ negl.} \quad \Longrightarrow \quad \Pr[m = m^* \wedge ok = 1 : Game\ 2] \text{ negl.} \tag{3}$$

The reason for this is that $tErr = 1$ only (up to negligible error) if the state in XY is close to a t-error state in Game 3. (Essentially by Lemma 8.) Since up to the measurement P_t^{Bell}, the two games are identical, this implies that also the state in XY in Game 2 is close to a t-error state. However, if XY is close to a t-error state, then B_2^* will have negligible probability of guessing m, the result of measuring Y (assuming suitably chosen t). (This is analogous to showing that in a QKD protocol without entanglement purification/privacy amplification, the probability of guessing the key is negligible. Cf. **??**.)

We can now replace $TV(B)$ by $TV(0)$.

Game 4 (Using fake TV)
(a) $V \leftarrow TV(0)$.

(b) Initialize XY with $|\beta_{00}\rangle^{\otimes\eta}$.
(c) Adversary B_1^* gets V, X.
(d) $B \xleftarrow{\$} \{+,\times\}^\eta$.
(e) Apply measurement $P_B^=$ to XY. $ok := 1$ if measurement succeeds.
(f) Apply measurement P_t^{Bell} to XY. $tErr := 1$ if measurement succeeds.

We have that

$$\Big|\Pr[tErr = 0 \wedge ok = 1 : Game\ 3] - \Pr[tErr = 0 \wedge ok = 1 : Game\ 4]\Big| \text{ is negligible.} \quad (4)$$

This is because we have removed the call to B_2^*, and B_1^* runs in time T.[13] By definition of T-hiding no T-time algorithm can distinguish between $TV(B)$ and $TV(0)$, in particular not the code in Game 3.

Finally, we have

$$\Pr[tErr = 0 \wedge ok = 1 : Game\ 4] \text{ is negligible.} \quad (5)$$

Reason: Picking B at random and then testing whether X, Y are equal in that basis ($P_B^=$) is essentially a Bell test. (Here it is important that now B is not used before applying $P_B^=$, otherwise we could not consider it random.) Remember that in the analysis of our QKD protocol, after successfully performing the Bell test, the probability of not passing a measurement that checks if there are at most t errors, is negligible. A very similar computation shows (5).

We can now finish the proof. By (4,5) we have that $\Pr[tErr = 0 \wedge ok = 1 : Game\ 3]$ is negligible. By (3), this implies that $\Pr[m = m^* \wedge ok = 1 : Game\ 2]$ is negligible. And finally, by (2), this implies that $\Pr[m = m^* \wedge ok = 1 : Game\ 1]$ is negligible. Since Game 1 describes the situation in Lemma 31, that lemma follows. □

How to construct revocably hiding quantum time vaults? The protocol QTV from Definition 58 has the disadvantage that partial information about the message m is leaked. We would like a T-revocably hiding quantum time vault (as in Definition 57). This is ongoing research, we currently have two approaches (that both probably work):

- *Encode m in a larger codeword w such that knowledge about a part of w does not reveal anything about m.* The challenge here is choosing the right encoding and how to extend the proof idea of Lemma 31 to show that indeed no information about m is leaked.
- *Use the hashed message as key.* To send a message m, we first pick a random k, then we send $(QTV(k), H(k) \oplus m)$ where H is a suitable hash function. Even though $QTV(k)$ leaks some information about k, k is sufficiently uncertain that we do not learn anything about $H(k)$. Since nothing is known about $H(k)$, $H(k) \oplus m$ hides m. Probably the security of this scheme can only be shown in the so-called random oracle model. (Meaning the proof is based on a heuristic.)

[13] Here we are simplifying by assuming that all the other computation steps in Game 3 take no time at all. A precise proof would take these into account, then we would need that TV is a $(T + T')$-hiding time vault, where T' is the time spent in these additional computation steps.

16 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 59 (Proof systems) *We call a pair (P, V) of interactive machines a* proof *or* proof system *for the relation R with* soundness-error ε *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.)*[14]
- Soundness: *For any (potentially computationally unlimited) machine P^*, and for any $x \notin L_R$, we have* $\Pr[\langle P^*(), V(x)\rangle = 1] \leq \varepsilon$. *(I.e., except for probability ε, 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 60 (Zero-knowledge) *A pair (P, V) of interactive machines is* statistical zero-knowledge *if for any polynomial-time*[15] *V^* there exists a polynomial-time S and a negligible μ such that for all $(x, w) \in R$ and all $z \in \{0, 1\}^*$, we have*

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

(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 61 (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 $\phi : G_1 \to G_2$ is a graph isomorphism.*

[14] 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.

[15] In this section, we will call a machine polynomial-time its running-time is bounded by a polynomial in the length of its *first* argument.

Definition 62 (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 ψ_1 on the vertices of G_1 and computes $H := \psi_1(G_1)$. (Notice that now $\psi_1 : G_1 \to H$ 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 $\psi_i : G_i \to H$.*
- *V checks whether $\psi_i : G_1 \to H$ is an isomorphism. If so, V outputs 1.*

Theorem 9 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 59), except that P^* is allowed to be a quantum machine.

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

Definition 63 (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 μ such that for all $(x, w) \in R$ and all density operators ρ, we have*

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

(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 60) is a quantum state.

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 ρ, 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 ρ' is the state output by the simulator $S_1(x, \rho)$, then $\operatorname{tr} P_\perp \rho' = \frac{1}{2}$ and $P_\perp \rho' P_\perp / \operatorname{tr} P_\perp \rho' P_\perp = \langle P(x, w), V^*(x, \rho)\rangle$ 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 63 from S_1, we cannot directly follow the classical proof. Instead, we use the following lemma:

Lemma 32 (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 $q \in poly(1/p)$, 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 ρ.

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].

17 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 64 (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 65 (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* $\operatorname{ord} a$.

Lemma 33 (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 66 (Discrete Fourier transform) *The* discrete Fourier transform (DFT) *is a linear transformation on $\mathbb{C}^N$ represented by the matrix $D_N = 2^{-N/2} \left(\!\left(e^{2i\pi kl/N}\right)\!\right)_{kl} \in \mathbb{C}^{N \times N}$.*

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

Lemma 34 (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.*[16] *Note that N/p intuitively represents the frequency of x.*

Theorem 10 (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 11 (Order-finding) *Assume a group G in which exponentiation is feasible in polynomial-time. There is a polynomial-time quantum algorithm that returns* $\operatorname{ord} a$ *on input of $a \in G$.*

[16] If $p \nmid N$, this holds only approximately. In this exposition, we will not formulate exact bounds for the approximation.

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 $\mathcal{H}_B$ 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., $x = x' + k \operatorname{ord} a$ for some $k \in \mathbb{Z}$. Hence $|\Psi_3\rangle$ is $\operatorname{ord} a$-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 $N/\operatorname{ord} a$ (approximately). If we measure the system in the computational basis, we get a multiple of $N/\operatorname{ord} a$. From this we can compute an approximate divider of $\operatorname{ord} a$. Additional work needs to be done to recover the exact value of $\operatorname{ord} a$ from this, but this is a classical computation and omitted here.

Definition 67 (Discrete logarithm problem) *Let G be a (multiplicative) group and g a generator. Given $y \in G$, find y with $g^x = y$. (That value x is called the discrete logarithm* $\operatorname{dlog} y$ *of y.)*

Theorem 12 *Assume a group G with generator g in which exponentiation is feasible in polynomial-time. There is a polynomial-time quantum algorithm that returns* $\operatorname{dlog} a$ *on input of $a \in G$.*

Further reading: [NC00, Sections 5.1–5.3]

18 Quantum money

Real-world cash (implemented in terms of coins and bank notes) has the following properties:

- *Issued by bank.* There is an entity (called the *bank*) that can produce pieces of cash (called "coins" in the following for simplicity.
- *Unforgeability.* No-one besides the bank can produce more coins. Specifically, we wish that when given q valid coins, it is not possible to make $q+1$ valid coins out of it.
- *Transferability without involving the bank.* The current owner of a coin can pass on that coin to another party without needing to interact with the bank in the process.
- *Public verifiability.* Anyone can, given a coin, check whether it is indeed a coin (without involving the bank). With real-world cash, this is done by ensuring

that there are a number of publicly known but hard to reproduce features that a coin/banknote should have.

- *Anonymity.* When performing transactions (transferring coins), the identity of the involved parties does not have to be involved.

Notice that this only applies to cash. Money that is stored on a bank account does not have the transferability property, since we have to involve the bank to transfer the money to another account. Also, verification involves the bank here, too. (Anonymity typically is not given either, but could be implemented.)

Instead of physical coins and banknotes, we are interested in a cryptographic solution that satisfies the above four properties. With classical cryptography, this is impossible: If A has a coin c, then A can run the transfer protocol to give c to B. Then B has c. However, since A can, before running the transfer protocol, make a copy of his state, A will also still have c. Thus two coins c exist now, violating unforgeability. With quantum cryptography, this attack can be avoided. If the coin c involves a quantum state, then copying c might not be possible, thus after transferring c to B, A will not possess c any more (hopefully).

18.1 Wiesner's protocol

The first quantum money scheme was proposed by Wiesner already in the 1970s [Wie83]. That scheme does not have public verifiability, but its advantage is that it is quite simple to define and to analyze.

Definition 68 (Wiesner's quantum money) *Let η be the security parameter.*

- Issuing money. *The bank picks $s, x \xleftarrow{\$} \{0,1\}^\eta$, $B \xleftarrow{\$} \{+,\times\}^\eta$. We call s the serial number. Then the bank encodes $|\Psi\rangle := |x\rangle_B$. (I.e., the i-th qubit of $|\Psi\rangle$ is x encoded in basis B.) It issues the coin $(s, |\Psi\rangle)$ and stores (x, B) in its database at index s.*
- Transferring money. *To transfer a coin $(s, |\Psi\rangle)$ to another party, one just sends $(s, |\Psi\rangle)$.*
- Verification (by the bank). *Given a coin (s, C) where C is a quantum register,*[17]*, then the bank looks up (x, B) in the database at index s, measures C in bases B, and checks whether the outcome is x. If the database lookup and the check succeed, the bank accepts the coin. (Note: measuring in B and comparing with x is the same as measuring using the projector $|\Psi\rangle\langle\Psi|$ with $|\Psi\rangle := |x\rangle_B$.)*

We do not formalize the notion of unforgeability of quantum money here, but the following lemma states the essence of the unforgeability property of Wiesner's quantum money:

Lemma 35 *Fix an adversary A. Let Bank denote the bank's issuing algorithm, we write $C, s, x, B \leftarrow Bank$ to denote that C contains the quantum part of the coin, s is the serial*

[17] We do not write $|\Psi\rangle$ instead of C here, because that notation would imply that C is not entangled with other qubits the adversary may hold.

number, and x, B the information stored by the bank. Let Ver be the verification routine, we write $ok \leftarrow Ver(C, s, x, B)$ to denote the verification of (s, C) with when x, B are the information stored by the bank for serial number s. We leave the security parameter implicit.

Then

$$\Pr[ok_1 = 1 \text{ and } ok_2 = 1 : (C, s, x, B) \leftarrow Bank, (C_1, C_2) \leftarrow A(C, s), \\ ok_1 \leftarrow Ver(C_1, s, x, B), ok_2 \leftarrow Ver(C_2, s, x, B)]$$

is negligible in η.

The proof of this fact uses techniques we already know from the analysis of quantum key distribution and quantum time vaults.

Attacking Wiesner's scheme. However, besides the fact that it does not support verification, Wiesner's scheme has the problem that it is susceptible to a forgeability attack by an adversary that has access to a bank that verifies coins for him. (And such a public service should exist if Wiesner's money is make sense.) More specifically, assume that bank will, given some coin (s, C) submitted by A, perform the verification, tell A whether verification succeeded, and then return (s, C) (i.e., the post-measurement-state after measuring whether verification succeeded). Then A can produce a copy of the coin (s, C) as follows:

- Denote the η qubits of C by $C_1, \ldots, C_\eta$.
- For $i = 1, \ldots, \eta$ do:
  - Repeat until x_i, B_i are determined:
  - Pick $\hat{x}_i \stackrel{\$}{\leftarrow} \{0, 1\}$, $\hat{B}_i \stackrel{\$}{\leftarrow} \{+, \times\}$.
  - Send $(s, C_1 \ldots C_{i-1} | \hat{x}_i \rangle_{\hat{B}_i} C_{i+1} \ldots C_\eta)$ to the bank for verification. Note that even in case of a failed verification, the verification measurement does not change the states of $C_1, \ldots, C_\eta$.
  - If verification fails, $\hat{x}_i, \hat{B}_i$ are not the correct values for x_i, B_i.
  - As soon as all but one value of $(\hat{x}_i, \hat{B}_i)$ are excluded in this way, x_i, B_i are determined.
- Now $x = x_1 \ldots x_\eta$ and $B = B_1 \ldots B_\eta$ are determined and A can produce arbitrarily many valid coins $(s, |x\rangle_B)$.

Note that this attack only works if the bank hands back the coin even if verification fails. If we require the bank to destroy the coin upon failed verification, a more involved attack is needed, using techniques from the bomb tester (Section 3).

18.2 Aaronson-Christiano quantum money.

In [AC12], Aaronson and Christiano propose a quantum money scheme with public verification. To define this scheme, we first introduce some notation:

Let $\mathbb{F}_2$ be the finite field of size 2. (I.e., elements of $\mathbb{F}_2$ are essentially bits, with $+$ being the XOR operation, and $\cdot$ being normal multiplication.) Then $\mathbb{F}_2^n$ is a vector space (over $\mathbb{F}_2$). For a subspace $A \subseteq \mathbb{F}_q^n$, let $|A\rangle := |A|^{-1/2} \sum_{x \in A} |x\rangle$. Furthermore, let $A^\perp$ be the orthogonal complement of A, i.e., $A^\perp = \{y \in \mathbb{F}_2^n : \forall x \in A.\ x \cdot y = 0\}$ where $x \cdot y$ is the inner product of x and y. Given polynomials $p_1, \ldots, p_m$, let P_p denote the projector $\sum_x |x\rangle\langle x|$ where x ranges over all $x \in \mathbb{F}_2^n$ with $p_1(x) = \ldots p_m(x) = 0$.

Definition 69 (Aaronson-Christiano quantum money.) *The scheme is parametrized by n, d, m. Here d could be small (e.g., $d = 4$) and n, m would typically grow linearly with the security parameter.*

- Setup. *The bank picks a public/private key pair for a quantum secure signature scheme and publishes the public key.*
- Issuing money. *The bank picks a random subspace $A \subseteq \mathbb{F}_2^n$ of dimension $n/2$. (This can be done with high probability by picking $n/2$ random elements of $\mathbb{F}_2^n$ and use them as a basis for A.)*
  Then the bank picks m uniformly random multivariate polynomials $p_1, \ldots, p_m$ in n variables and of degree d such that $p_i(x_1, \ldots, x_n) = 0$ for all $(x_1, \ldots, x_n) \in A$. (Essentially, these p_i serve to describe the space A in a way that does not allow an adversary to recover A efficiently. There is an $O(n^d)$-time algorithm for picking the polynomials.)
  Then the bank picks m uniformly random multivariate polynomials $q_1, \ldots, q_m$ in n variables and of degree d such that $q_i(x_1, \ldots, x_n) = 0$ for all $(x_1, \ldots, x_n) \in A^\perp$. (The q_i describe $A^\perp$ which is redundant in principle because the p_i determine A and A determines $A^\perp$. But for efficient verification, we will need q_i, too.)
  The bank produces a signature σ on $(p_1, \ldots, p_m, q_1, \ldots, q_m)$. Finally, it returns the coin $(|A\rangle, p_1, \ldots, p_m, q_1, \ldots, q_m, \sigma)$.
- Transferring money. *To transfer a coin $(|A\rangle, p_1, \ldots, p_m, q_1, \ldots, q_m, \sigma)$ to another party, one just sends $(|A\rangle, p_1, \ldots, p_m, q_1, \ldots, q_m, \sigma)$.*
- Verification (by anyone knowing the banks public key). *Given a coin $(C, p_1, \ldots, p_m, q_1, \ldots, q_m, \sigma)$ where C is a quantum register, the verifier first verifies whether σ is a valid signature on $(p_1, \ldots, p_m, q_1, \ldots, q_m)$. (This ensures that $(p_1, \ldots, p_m, q_1, \ldots, q_m)$ are indeed issues by the bank and describe a valid coin.)*
  To check if C indeed contains $|A\rangle$ with $A = \{x \in \mathbb{F}_2^n : \forall i.\ p_i(x) = 0\}$ (as it should if it is a valid coin), we measure C with P_p, then apply $H^{\otimes n}$, then measure C with P_q, then apply $H^{\otimes n}$.
  Verification succeeds if the signature check and the two measurements succeed.

To see that verification actually succeeds, we need the following facts: The projector implemented by the measurements in the verification is $H^{\otimes n} P_q H^{\otimes n} P_p =: P$. First, for suitably chosen parameters n, m, d, with overwhelming probability we have that $x \in A$ iff

$\forall i.p_i(x) = 0$, and that $x \in A^\perp$ iff $\forall i.q_i(x) = 0$. Thus $P = H^{\otimes n} P_{A^\perp} H^{\otimes n} P_A$ where $P_A = \sum_{x \in A} |x\rangle\langle x|$ and $P_{A^\perp}$ analogous. Furthermore, it can be shown that $H^{\otimes n}|A\rangle = |A^\perp\rangle$. Thus $P|A\rangle = H^{\otimes n} P_{A^\perp} H^{\otimes n} P_A |A\rangle = H^{\otimes n} P_{A^\perp} H^{\otimes n} |A\rangle = H^{\otimes n} P_{A^\perp} |A^\perp\rangle = H^{\otimes n} |A^\perp\rangle = |A\rangle$. Thus honest coins pass verification with overwhelming probability. In fact, one can show that $P = |A\rangle\langle A|$, so only honest coins pass verification.

Furthermore, [AC12] shows that the scheme is unforgeable given some (strong) assumption about the hardness of finding solutions of multivariate polynomials.

Further reading: See [Wie83] for Wiesner's original proposal and [MVW12] for a security proof of that scheme. See [AC12] for the Aaronson-Christiano scheme.

19 A physical view on quantum mechanics

Note: In this section, we will use mathematics in a non-rigorous way. That is, we will *implicitly* assume that functions are continuous or differentiable whenever needed, that Dirac deltas[18] can be treated like ordinary functions, and more. This is common in theoretical physics.

Throughout this lecture, we have been using an abstraction of quantum mechanics that represents physical systems as consisting of a finite set of classical states (e.g., $|0\rangle$, $|1\rangle$, etc.) that can occur in superposition and on which we can perform various quantum operations. However, it is not immediately obvious how this related to the physical world. For example the location of a particle is a continuous variable. How is the speed of a particle modeled? How do forces between particles come into play in determining the behavior of particles? In this section, we will shed some light on these question. However, we can only give an idea here, for deeper understanding a full course or textbook on quantum mechanics is needed.

The wave function. We start by discussing how the state of a single particle can be represented. Classically, a particle can have a single position $x \in \mathbb{R}^3$ at any given time $t \in \mathbb{R}$. Thus, classically, we would describe the time evolution of a particle by a function $x : \mathbb{R} \to \mathbb{R}^3$ such that $x(t)$ is the location of the particle at time t. In a quantum setting, however, the location of a particle is not determined, the particle can be in a superposition of many different locations. Thus, at any time, the state of the particle is described by a function $\psi : \mathbb{R}^3 \to \mathbb{C}$, where $\psi(x)$ is the amplitude of the state being at location x. Or, to model the fact that the location may depend on the time, we add another parameter: $\psi : \mathbb{R}^3 \times \mathbb{R} \to \mathbb{C}$, where $\psi(x, t)$ is the amplitude of the state being at location x at time t.

[18] The Dirac delta δ is a function $\delta(x)$ such that $\delta(0) = \infty$ and $\delta(x) = 0$ elsewhere. It can be informally seen as a limit of functions δ_n where $\int_{-\infty}^{\infty} \delta_n(x)dx = 1$ for all n, and $\delta_n(x) \to 0$ for all $x \neq 0$. I.e., a limit of functions that get more and more concentrated around 0.

In the following, to keep things simpler, we will consider only one-dimensional space, i.e., the particle can be found somewhere on a line. Then $\psi : \mathbb{R} \times \mathbb{R} \to \mathbb{C}$, and $\psi(x,t)$ denotes the amplitude of the particle being at position $x \in \mathbb{R}$ at time t.

Definition 70 (Wave function) *A (one-dimensional one-particle time-dependent)* wave function *is a function* $\psi : \mathbb{R} \times \mathbb{R} \to \mathbb{C}$ *such that for all* t*, we have* $\int_{-\infty}^{\infty} |\psi(x,t)|^2 dx = 1$.

The wave function tells us where the particle can be found with what probability. For example, if we measure (at time t) whether the particle is somewhere in the interval $[a,b]$, the probability of yes is $\int_a^b |\psi(x,t)|^2 dx$. But the wave function encodes more then just the probability. For example, the phase of $\psi(x,t)$ encodes additional information such as the momentum of the particle, and is relevant for many quantum mechanical effects such as interference.

Time evolution. Now in the classical setting, the position of a particle at a certain point, together with it's velocity, determines it's future evolution. (Assuming that we know the potential in which the particle moves.) Namely, if the potential is $V(x,t)$, then $-\frac{\partial V(x,t)}{\partial x}$ is the force that acts on the particle at position x. And hence, if the particle has mass m, $-\frac{1}{m}\frac{\partial V(x,t)}{\partial x}$ is the acceleration of the particle. We can write this as a differential equation: $\frac{\partial^2 x(t)}{\partial t^2} = -\frac{1}{m}\frac{\partial V(x,t)}{\partial x}$. This determines $x(t)$ for all $t > t_0$ if x and $\frac{\partial x}{\partial t}$ are given at $t = t_0$.

Similarly, in the quantum case, if $\psi(x,t_0)$ is given for all x, then there is a differential equation that determines the future evolution of the particle.

Definition 71 (Schrödinger equation) *The (time-dependent one-dimensional one-particle)* Schrödinger equation *for a particle of mass* m *in a potential* $V : \mathbb{R} \to \mathbb{R}$ *is given by*

$$i\hbar \frac{\partial \psi(x,t)}{\partial t} = -\frac{\hbar^2}{2m}\frac{\partial^2 \psi(x,t)}{\partial x^2} + V(x,t).$$

Here $\hbar$ *is the so-called* reduced Planck constant, $\hbar \approx 6.62606957 \cdot 10^{-34} Js$ *(Joule seconds).*

So, given an initial state $\psi(x,t_0)$ for all x, and the potential $V(x,t)$ for all x,t, we can decide what $\psi(x,t)$ is for all $t \geq t_0$ by solving the Schrödinger equation.

Before we have a look at this, let us have a look at the components of the Schrödinger equation. The term $-\hbar^2 \frac{\partial^2 \psi(x,t)}{\partial x^2}$ turns out to be the squared momentum of the particle (for reasons that are beyond the scope of this exposition). And since the momentum is the velocity times the mass, $-\frac{\hbar^2}{m^2}\frac{\partial^2 \psi(x,t)}{\partial x^2}$ is the squared velocity v^2. And the kinetic energy K is $K = \frac{mv^2}{2}$. Hence the kinetic energy is described by the term $-\frac{\hbar^2}{2m}\frac{\partial^2 \psi(x,t)}{\partial x^2}$. And since we add to that the potential, the right hand side of the Schrödinger is nothing else but the energy of the particle at position x and time t. The operator that computes the energy given the wave function is called the *Hamiltonian* $\hat{H}(t)$, in our case $\hat{H}(t)\psi :=$

$-\frac{\hbar^2}{2m}\frac{\partial^2\psi(x,t)}{\partial x^2} + V(x,t)\psi(x,t)$.[19] So, the Schrödinger equation tells us that the differential of ψ (in the variable t) is $-\frac{i}{\hbar}\hat{H}(t)\psi(x,t)$, i.e., the energy times $-\frac{i}{\hbar}$. If $\hat{H}(t)\psi(x,t)$ were a constant E, we could then easily solve the differential equation $\frac{\partial\psi(x,t)}{\partial t} = -\frac{iE}{\hbar}$ and see that $\psi(x,t) = \psi(x,t_0)e^{-iEt/\hbar}$. Since $e^{-iEt/\hbar}$ as a function of t has an oscillating behavior (if you don't know what this function looks like, I recommend to visualize it), this tells us that the wave function oscillates over time, and oscillates faster if the energy E is higher. (This matches the fact that light with higher frequency has higher energy.)

Now, in principle, we can derive the behavior of a particle in any potential. (And easily generalize this to many particle systems.) However, in practice the Schrödinger equation is quite complex to solve, and therefore physicists often use the so-called time-independent Schrödinger equation to get a better understanding of the system and to solve the time-dependent case, as described in the following.

Time-independent Schrödinger equation. We now consider the special case where the potential does not depend on the time t, i.e., $V(x,t) = V(x)$ for all x, t. In this case, the Hamiltonian does not depend on t either, and we write $\hat{H}\psi := -\frac{\hbar^2}{2m}\frac{\partial^2\psi(x,t)}{\partial x^2} + V(x)$. Assume further that we are given $\psi_0(x) := \psi(x,t_0)$ for some t_0, i.e., the initial state at time t_0. It turns out that then we can then write ψ_0 as a linear combination of eigenvectors of $\hat{H}$ (possibly an infinite number of them). More precisely, we first solve the so-called time-independent Schrödinger equation:

Definition 72 (Time-independent Schrödinger equation) *The (one-particle one-dimensional)* time-independent Schrödinger equation *for a time-independent potential $V(x)$ is given by $\hat{H}\psi_0 = E\psi_0$ or equivalently $-\frac{\hbar^2}{2m}\frac{\partial^2\psi_0(x)}{\partial x^2} + V(x)\psi_0(x) = E\psi_0(x)$. In this equation, $\hbar, m, V$ are given, and $E \in \mathbb{R}$ and $\psi_0 : \mathbb{R} \to \mathbb{C}$ are to be found.*

What does the time-independent Schrödinger equation have to do with the time-dependent Schrödinger equation from above? Consider a solution ψ_0, E to the time-independent Schrödinger equation. It is then easy to verify that $\psi(x,t) := \psi_0(x)e^{-iEt/\hbar}$ satisfies the time-dependent Schrödinger equation (try it!).

So, generally, if we can write $\psi_0(x) = \sum_E \alpha_E\psi_E(x)$ or $\psi_0(x) = \int \alpha_E\psi_E(x)dE$ where ψ_E, E are solutions to the time-independent Schrödinger equation, then $\psi(x,t) := \sum_E \alpha_E\psi_E(x)e^{-iEt/\hbar}$ or $\psi(x,t) := \int \alpha_E\psi_E(x)e^{-iEt/\hbar}dE$ is the solution of the time-dependent Schrödinger equation with initial condition $\psi(x,t_0) = \psi_0(x)$.

Thus, finding solutions to the time-independent Schrödinger equation is crucial for the understanding of the time-evolution of a system with unchanging potential (or, in the more general case, of a system with unchanging Hamiltonian $\hat{H}$).

[19] In more general cases (e.g., multiple particles etc.), the Schrödinger equation is suitably generalized as follows: Let M be the set of all possible classical states of the system. (E.g., for two particles in three-dimensional space, $M := \mathbb{R}^3 \times \mathbb{R}^3$.) A wave function is $\psi : M \times \mathbb{R} \to \mathbb{C}$, and the Hamiltonian $\hat{H}(t)$ is an operator that, given a function $\psi : M \to \mathbb{C}$ returns a function $E : M \to \mathbb{R}$ where $E(m)$ is the energy at "position" m. ($\hat{H}(t)$ operates on ψ for each t individually.) And then the time evolution is then in this generic setting described via the Schrödinger equation $i\hbar\frac{\partial\psi(x,t)}{\partial t} = \hat{H}(t)\psi(x,t)$.

Example: Infinite potential well. We now apply what we have learned about the Schrödinger equation to a simple setting, the "infinite potential well" or "infinite square well". In this example, we assume that the potential is zero within a certain area, and infinite[20] outside of that area. That is,

$$V(x) = \begin{cases} 0, & (0 < x < L) \\ \infty, & (\text{otherwise}) \end{cases}$$

This corresponds to a particle inside a (one-dimensional) box, it can freely move inside, but can never leave the box.

First, consider a classical setting: A classical particle will be able to have any position inside the box, and can have arbitrary speed v (until it hits the wall, whereupon the speed becomes $-v$). In particular, the kinetic energy $E = \frac{mv^2}{2}$ can take any non-negative value.

Now intuitively, we would expect that in the quantum setting, the possible states of the particle in the well would be any superposition of the classical possibilities (i.e., $\int_0^L \int_0^\infty \alpha_{x,E}|x,E\rangle\, dE\, dx$ where $|x,E\rangle$ stands for a wave function where the particle has location x and kinetic energy E). Yet, we will see that the situation is quite different in the quantum setting!

As explained above, in the quantum setting, we first need to find solutions to the time-independent Schrödinger equation. I.e., we need to solve $-\frac{\hbar^2}{2m}\frac{\partial^2\psi_0(x)}{\partial x^2} + V(x)\psi_0(x) = E\psi_0(x)$.

We will assume $E > 0$. (A similar calculation shows that there is no solution with $E < 0$.) First, since $V(x) = \infty$ for $x \notin (0, L)$, we have $\psi_0(x) = 0$ for $x \notin (0, L)$. (We do not give a rigorous mathematical argument for this, but intuitively/physically, we expect the particle not to be at a place of infinite potential.) Furthermore, standard techniques for solving differential equations show that the solutions of the equation

$$-\frac{\hbar^2}{2m}\frac{\partial^2\psi_0(x)}{\partial x^2} = E\psi_0(x) \qquad (*)$$

are of the form $A\sin(kx) + B\cos(kx)$ with $k := \frac{\sqrt{2mE}}{\hbar}$. Since $V(x) = 0$ for $x \in (0, L)$, we have that on $(0, L)$, the solutions to the Schrödinger equation coincide with the solutions of $(*)$. Since furthermore, the solutions to the Schrödinger equation have to satisfy $\psi_0(0) = 0$, we have $B = 0$. And since $\psi_0(L) = 0$, we need $\sin(kx) = 0$. This implies that $k = n\pi/L$ for integers $n \geq 0$. Furthermore, $k = 0$ is excluded because then $\psi_0(x) = A \cdot 0$, which cannot satisfy $\langle\psi_0, \psi_0\rangle = \int_{-\infty}^{\infty} \psi_0^*(x)\psi_0(x)\, dx = 1$. So the Schrödinger equation only has solutions for $E = \frac{\hbar^2 k^2}{2m} = \frac{\hbar^2\pi^2}{2mL^2}n^2 =: E_n$ with $n > 0$. And in each such case, $\psi_0 = |n\rangle := A_n \sin(\frac{n\pi x}{L})$ for a suitable normalization factor A_n.

So, summarizing: All solutions $\psi(x,t)$ to the time-dependent Schrödinger equation are of the form $\psi(x,t_0) = \sum_{n\geq 1}\alpha_n|n\rangle$, and then $\psi(x,t) = \sum_{n\geq 1}\alpha_n e^{-iE_n t/\hbar}|n\rangle$. This fully describes all possible time-evolutions of the state of the particle.

[20] Allowing infinite potentials is, of course, a contradiction to the fact that we consider V to be a function $\mathbb{R} \to \mathbb{R}$, and not well-defined. A more rigorous treatment could, e.g., consider a sequence of potentials which converges to 0 in $(0, L)$ and to ∞ outside.

In particular, we see that the energy of the particle will always be a multiple of $\frac{\hbar^2\pi^2}{2mL^2}$. That is, only specific energies are possible! This is in stark contrast to the classical case where any $E > 0$ is possible. (Of course, we can have a superposition of different energies, so that the average energy is any possible value. But if we were to measure the energy of the system, we would always get one of the values E_n.)

This energy quantisation is not an artifact of our infinite potential. It also occurs in the similar but more complicated analysis of an electron in the electric field of the nucleus of an atom. There the electron will also be able to only take certain energies. (This is the reason why photons emitted from atoms can have only certain energies – the energies of the photons correspond to the differences between the different energy levels.)

Note also that $E = 0$ is also excluded. In other words, the kinetic energy of a particle in a box can never be zero – the particle never rests. This is related to Heisenberg's uncertainty relation: since we know where the particle is (in the box), there must be a certain small uncertainty about its momentum and hence its velocity. So the velocity cannot be zero.

Link to our formalism. So if in "real" physics, the state of a system is described as a wave function, why do we treat quantum mechanical systems so differently in quantum information theory (i.e., in this lecture)? Namely, we treat quantum states as elements from a finite dimensional Hilbert space. And operations on these are unitary transformations. In fact, this is not really different from the wave function formalism. What we do is simply to give names to individual orthogonal solutions of the Schrödinger equation (e.g., we write the wave function corresponding to energy E_n as $|n\rangle$). And it turns out that for any Hamiltonian (which must be a Hermitian operator), the Schrödinger equation then predicts a unitary time evolution on some initial wave function $|\Psi\rangle$. (I.e., for any Hamiltonian $\hat{H}$ and any t, there is a unitary transformation U such that for any solution ψ of the time-dependent Schrödinger equation, $|\psi_t\rangle = U|\psi_0\rangle$ where $|\psi_t\rangle := \psi(\cdot, t)$.) So our formalism captures the laws of quantum mechanics without describing details that are not important for our specific case.

20 Position-verification

In this section, we give an example how quantum cryptography may enable tasks that are impossible classically. We already saw one example, namely information-theoretically secure key distribution. In that case, however, we only get something that could also be achieved classically *when using computational assumptions*. Now, we consider a task that is impossible classically even if the adversary is assumed to be computationally limited, while in the quantum setting, security against computationally bounded adversaries may be achievable. (The latter is still a question of open research.)

The task we are considering is "position-verification". In this task, we have an entity, called the "prover" P who wishes to convince a "verifier" that he can be found as a given location. As a motivating example, assume that the prover wishes to access an online service that is only accessible to people that at a certain location, say inside a mall.

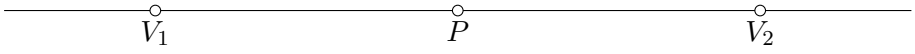


Figure 1: Basic setup for position-verification. A prover P and two verifiers V_1 and V_2.

Distance bounding. The simplest special case of this problem is distance bounding. In this case, the (honest) prover is in close proximity to the verifier. Now a protocol such as the following can be used: The verifier picks a random $r \in \{0,1\}^\eta$ and sends it to the prover. The prover sends r back to the verifier. The verifier measures the time Δ until he gets r back. Due to the limitation that information cannot travel faster than light, the verifier now knows that the prover cannot be farther away than $\Delta c/2$ where c is the speed of light. So, the prover has proven that he (or at some entity he collaborates with) is within distance $\Delta c/2$ of the verifier, therewith proving his location.

However, the disadvantage of distance bounding is that it requires a verifier in immediate proximity to the point where the prover supposedly is. This may be suitable for some applications (e.g., a contactless payment card wants to be sure that it is close to a reader before it transfers money to it). In other cases, however, we cannot assume that the verifier can be close. For example, if we wish to prove that the prover is inside a room, we would have to put up the verifier's receivers in the middle of the room, in the air, which is impractical (especially if the prover may be at any position in the room).

Classical position-verification. We now describe the basic approach how one would do position-verification in the classical setting, and why this does not work. For simplicity, we consider a one-dimensional setting in the following. That is, both prover and the verifier are on a line, with the verifier having two devices and the prover being in between. (See Figure 1.) All the results described in this section also generalize to the higher dimensional case, where we always assume that the prover is within the convex hull of the verifiers (i.e., we will need four verifiers for three-dimensional position-verification). We will also assume for simplicity that the distance between V_1 and P is the same as between V_2 and P, namely d.

Now, the most immediate idea would be to generalize the distance bounding scheme to the two-verifier case. That is, each verifier V_i sends a random number r_i at the same time to the prover. The prover is supposed to send each r_i back to V_i immediately upon reception. Each verifier checks that it gets the correct value r_i back within time $2d/c$.

Assume a malicious prover P^* who is not at position P. Without loss of generality, assume P^* is farther to the left by a distance d^*. Then the distance between P and V_2 is $(d+d^*)$, and the prover cannot send back r_2 within time $2d/c$ (he needs time $2(d+d^*)/c$. Similarly, a prover farther to the right will not respond to V_1 in time. It seems that the protocol is secure.

However, we have overlooked one possible attack. The protocol may be secure if the prover is only at a single location. But what if the malicious prover has several devices (or equivalently, if several malicious provers collude)? Consider the setup in Figure 2 (but ignore the labels on the lines for now). There are two malicious provers P_1^* and P_2^*

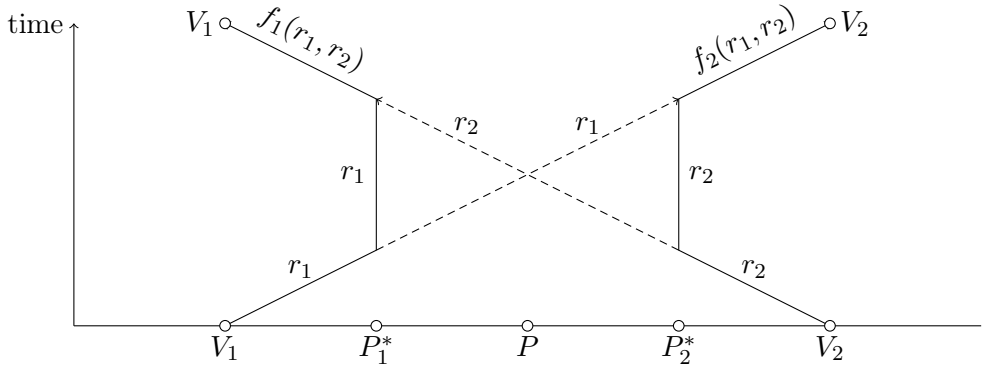


Figure 2: Attack setting for position verification. P_1^* and P_2^* are malicious provers that together try to convince the verifier that they are at position P.

located at distance $d/2$ to each side of the position P. Upon reception of r_1, P_1^* keeps r_1 for the time it would take for r_1 to reach P and come back to P_1^* (namely d/c). Then P_1^* forwards r_1 back to V_1. Similarly for P_2^*. In this attack, the time until r_i comes back to V_i is $2d/c$, the same time as in the case when there is an honest prover P (dashed line).

What if we use a more complex protocol? In general, instead of P having to simple echo r_1 and r_2 back to the respective verifier, we could require P to send $f_i(r_1, r_2)$ back to V_i. In this case, the attack is still simple. Using the message flow depicted in Figure 2, both verifiers will get the correct answer $f_i(r_1, r_2)$ in time.

This attack also easily generalize to the situation where the protocol has several rounds, i.e., if the verifiers send several messages and the prover has to answer to all of them. Altogether, this leads to a general impossibility for position-verification if the malicious prover is allowed to have several colluding devices.

Notice also that this attack works even if the malicious prover is required to be computationally limited: he does not perform any computation that is more complex than that performed by the honest prover (namely, evaluation of f_i).

Quantum position-verification. Notice that in the attack in against the general classical position-verification scheme, the malicious prover P_1^* takes value r_1 and forwards it to P_2^* while keeping a copy of r_1 to himself. If r_1 was quantum data, this would not in general be possible since P_1^* cannot copy quantum data. This leads to the following protocol idea:

- V_1 sends a qubit $|\Psi\rangle = H^B|x\rangle$ for random $x, B \in \{0, 1\}$.
- V_2 sends a random $c \in \{1, 2\}$.
- The prover P forwards $|\Psi\rangle$ to V_c. I.e., the value c tells him where to forward $|\Psi\rangle$ to.

The attack described in the classical setting does not work here any more because P_1^* (who gets $|\Psi\rangle$ first) has to decide whether to forward $|\Psi\rangle$ or to keep it. He cannot make the decision based on c, because he needs to forward $|\Psi\rangle$ before c can reach him. If he

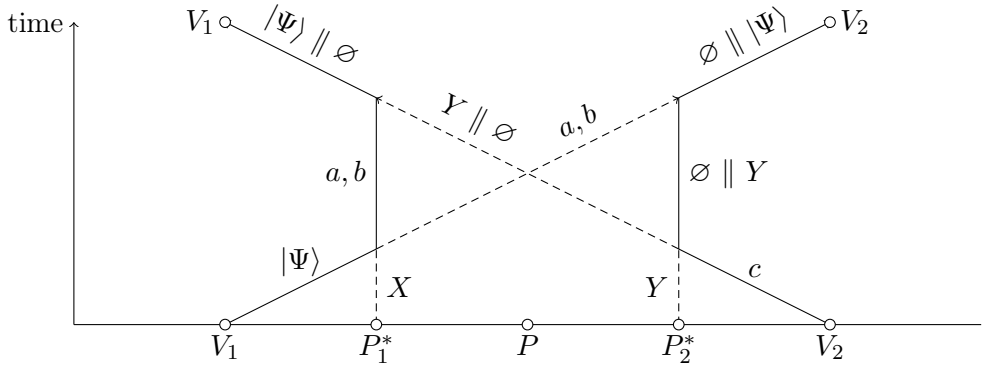
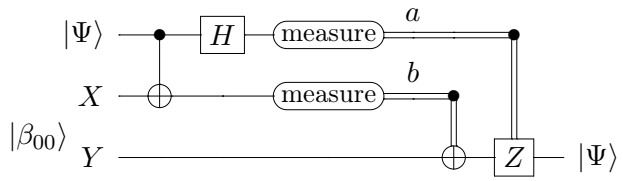


Figure 3: Attacking the quantum protocol. On arrows labeled with $t\|u$, t is sent in case $c = 1$ and u is sent in case $c = 2$. $\varnothing$ denotes an empty message.

forward $|\Psi\rangle$, P_2^* cannot send it back in time if $c = 1$. If he does not forward $|\Psi\rangle$, P_2^* will not get $|\Psi\rangle$ in time if $c = 2$.

Unfortunately, the protocol is not secure. There is a non-trivial attack against the protocol. For this, first recall the teleportation protocol:



In this protocol, Alice and Bob share a Bell pair XY (lower two lines), and Alice has a state $|\Psi\rangle$ (top line). Alice performs some operations on $|\Psi\rangle$ and her Bell pair half, resulting in classical values a, b. Given these values, Bob can now apply operations to Y that transform Y into $|\Psi\rangle$.

We can use teleportation to break the position-verification protocol as follows: Assume P_1^* and P_2^* share a Bell pair XY. When P_1^* receives $|\Psi\rangle$, he teleports $|\Psi\rangle$ to P_2^*. In other words, he only sends the classical information a, b to P_2^* which P_2^* can use to reconstruct $|\Psi\rangle$ from Y. So, if $c = 2$ and P_2^* is supposed to send $|\Psi\rangle$ to V_2, P_2^* can reconstruct $|\Psi\rangle$ and forward it to V_2 in time. This is depicted in Figure 3. (Consider only the right hand side of $\|$ in that figure for now.)

But what if $c = 1$? In this case, P_1^* needs to send $|\Psi\rangle$ to V_1^*, but he just "lost" the state $|\Psi\rangle$ by teleporting it to P_2^*. (The teleportation circuit destroys the state on Alice's side.) The trick here is that the teleported qubit can be received whoever has the second Bell pair half Y. So, if $c = 1$, P_2^* just has to send Y to P_1^*. As soon as Y reaches P_1^*, P_1^* can reconstruct $|\Psi\rangle$ from it, just in time to send it to V_1. (P_1^* was able to send a, b and keep it because a, b is classical information.) See Figure 3. (The messages sent in case $c = 1$ are on the left of the $\|$ symbols.) Notice that only classical information is duplicated, and that V_1 or V_2 gets its answer at the same time it would get it from the honest prover at location P (namely after time $2d/c$).

The protocol has been broken.

Generalizing the attack. Now, this attack only shows that our first idea for a quantum position-verification protocol can be broken. Unfortunately, the attack generalizes to arbitrary protocols! The generalization is not trivial, but the basic idea is the same: we teleport data from P_1^* to P_2^* and vice versa. And we move the end-point of the teleportation between P_1^* and P_2^* as needed. However, in the more general case, we may even teleport the teleportation end-point! And the end-point of that teleportation. And so on. With this idea (and nontrivial constructions), we get the following remarkable result:

Theorem 13 (Impossibility of quantum position-verification [BCF$^+$11]) *For any position-verification protocol communicating at most n qubits, there is an attack using entanglement that uses at most $2^{O(n)}$ qubits of preshared entanglement.*

This shows that, like in the classical case, we cannot expect to get secure position-verification without making any assumptions. Yet, this leaves the following possibilities:

1. There might be a position-verification protocol which can be broken only using $2^{\Omega(n)}$ qubits of preshared entanglement, but not with any polynomial amount. This would be the best possible outcome, since this would in particular mean a protocol that is secure against any polynomial-time attacker (in polynomial-time, one can use at most polynomially many qubits) *without using any computational assumptions.*

2. There might be a position-verification protocol which cannot be broken using αn qubits of preshared entanglement where α is some constant.

3. There might be a position-verification protocol which cannot be broken by polynomial-time malicious provers, given suitable computational assumptions.

Possibility 1 would be the ideal case, but this is currently a wide open research problem, no indications in favor or against possibility 1 are known.

A protocol as in possibility 2 has been shown to be possible [TFKW13]. However, in my opinion, it is doubtful whether the resulting attack model is realistic. At a first glance, it seems that a limitation to αn qubits of preshared entanglement is, for sufficiently large n, realistic because we can assume that the adversary has bounded quantum storage. Yet, in this particular setting, the assumption seems strong. Figure 4 illustrates this: It shows a setup how P_1^* and P_2^* can get n qubits of preshared entanglement at exactly the right time (namely, when they get the messages from V_1^* and V_2^*). Such a setup allows to break the protocol from [TFKW13] (and all other currently known quantum position-verification protocols in the bounded quantum storage model).

Finally, possibility 3 is probably the most likely one. Although currently, no provably secure protocol is known, it is likely to exist (ongoing research), and that would be a simple example of something impossible in the classical setting, but easy to achieve in the quantum setting.

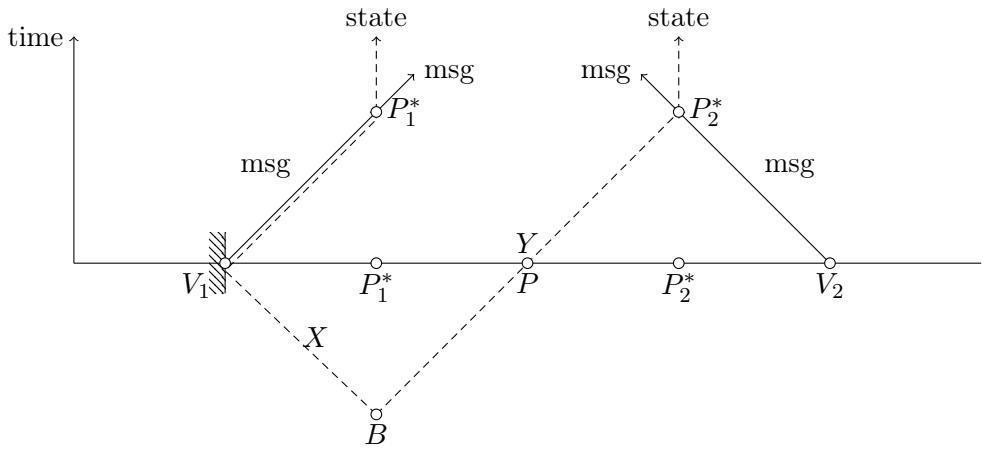


Figure 4: How to provide preshared entanglement without quantum storage. B is a Bell pair source that sends n Bell pairs, the first halves (X) to the left, and the second halves (Y) to the right. The actual protocol messages and the states that the provers keep are denoted simple "msg" and "state" because we are only concerned with how to get the preshared entanglement to P_1^* and P_2^* at the right moment, namely when the messages from V_1 and V_2 arrive. $\nparallel$ denotes a mirror placed close to V_1. (In more than one dimension, X might be sent in a different direction, resolving the problem that the mirror and V_1 have to be in the same place.)

Further reading: [CGMO09] for the impossibility of classical position-verification. [BCF+11] for the impossibility of information-theoretical quantum position-verification, as well as for definitions of the security notion in the quantum case. [TFKW13] how to get position-verification in the bounded quantum storage model.

References

[AC12] Scott Aaronson and Paul Christiano. Quantum money from hidden subspaces. In Howard J. Karloff and Toniann Pitassi, editors, *STOC 2012*, pages 41–60. ACM, 2012.

[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.

[BCF+11] Harry Buhrman, Nishanth Chandran, Serge Fehr, Ran Gelles, Vipul Goyal, Rafail Ostrovsky, and Christian Schaffner. Position-based quantum cryptography: Impossibility and constructions, 2011. Full version on IACR ePrint 2010/275.

[CGMO09] Nishanth Chandran, Vipul Goyal, Ryan Moriarty, and Rafail Ostrovsky. Position based cryptography, 2009. Full version on IACR ePrint 2009/364.

[DFR+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`.

[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`.

[KRS09] R. Konig, R. Renner, and C. Schaffner. The operational meaning of min- and max-entropy. *Information Theory, IEEE Transactions on*, 55(9):4337 –4347, September 2009. Online available at `http://authors.library.caltech.edu/15654/`.

[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`.

[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`.

[MVW12] Abel Molina, Thomas Vidick, and John Watrous. Optimal counterfeiting attacks and generalizations for wiesner's quantum money. arXiv:1202.4010v1 [quant-ph], February 2012.

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

[Pei16] Chris Peikert. A decade of lattice cryptography. *Foundations and Trends in Theoretical Computer Science*, 10(4):283–424, 2016. `https://web.eecs.umich.edu/~cpeikert/pubs/lattice-survey.pdf`.

[Reg09] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. *J. ACM*, 56(6):34:1–34:40, September 2009.

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

[SMWF+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`.

[SWV+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.

[TFKW13] Marco Tomamichel, Serge Fehr, Jedrzej Kaniewski, and Stephanie Wehner. One-sided device-independent qkd and position-based cryptography from monogamy games. In Thomas Johansson and Phong Q. Nguyen, editors, *Eurocrypt 2013*, volume 7881 of *LNCS*, pages 609–625. Springer, 2013. Full version is arXiv:1210.4359.

[Tom16] Marco Tomamichel. *Quantum Information Processing with Finite Resources*, volume 5 of *SpringerBriefs in Mathematical Physics*. Springer International Publishing, 2016.

[Unr11] Dominique Unruh. Lecture "Quantum Cryptography", fall 2011. Webpage is `http://www.cs.ut.ee/~unruh/qc11/`.

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

[Wie83] Stephen Wiesner. Conjugate coding. *SIGACT News*, 15(1):78–88, 1983. Manuscript written ca. 1970.

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

21 Lattice-based cryptography

In this section, we introduce one example of so-called *lattice-based cryptography* that is a candidate for classical cryptography secure against attacks using quantum computers.

21.1 Learning with errors

We first introduce a computational problem that forms the basis of the cryptosystem described in the next section.

We warm up with a slightly simpler to explain problem:

Informally, the binary computational LWE problem is, given a publicly known binary matric A, to find s given $As + e$ (where e is an error vector with "few" 1's).

Definition 73 (Binary computational LWE problem) *Fix parameters $n, m > 0$ (integers) and a $p \in [0,1]$. Let $A \xleftarrow{\$} \{0,1\}^{m \times n}$ (a uniformly random binary $m \times n$-matrix) and $s \xleftarrow{\$} \{0,1\}^n$ (a uniformly random binary n-vector), and let $e \in \{0,1\}^m$ be chosen by independently letting each e_i be 1 with probability p.*

The task of the binary decisional LWE problem (with parameters n, m, p) is to compute s given $A, b := As + e$.

It is generally believed that this problem is hard for suitable parameters. (I.e., the probability of guessing s is exponentially small for a polynomial-time adversary.)

Instead of asking an adversary to find s, we ask the simpler question: Is the vector b indeed of the form $As + e$, or is it just a random vector? (This is simpler, at least for relevant parameter choices, since if you can find s from $As + e$, you can also tell whether you got $As + e$ by just checking whether you do find s.)

Definition 74 (Binary decisional LWE problem) *Fix parameters $n, m > 0$ (integers) and a $p \in [0,1]$. Let $A \xleftarrow{\$} \{0,1\}^{m \times n}$ (a uniformly random binary $m \times n$-matrix) and $s \xleftarrow{\$} \{0,1\}^n$ (a uniformly random binary n-vector), and let $e \in \{0,1\}^m$ be chosen by independently letting each e_i be 1 with probability p. Let $r \xleftarrow{\$} \{0,1\}^m$.*

The task of the binary decisional LWE problem (with parameters n, m, p) is to distinguish the following two data:

- *A, $As + e$*
- *A, r*

It is generally believed that this problem is hard for suitable parameters. (I.e., the probability of guessing right is exponentially close to random guessing for a polynomial-time adversary.)

The binary LWE problem considered the problem of guessing a bitstring given A and $As + e$.

However, there is no reason per se to consider only bitstrings. Instead, we can fix an additional parameter q, and perform all operations modulo q. That is, A and s contain elements of $\mathbb{Z}_q$. And e is a vector consisting of "small" numbers in $\mathbb{Z}_q$. (By "small" we intuitively mean close to 0. So for example 1 would be small, but $q - 1 \equiv -1$ would also be small, but $q/2$ would not be.) Since now the errors e_i are not just 0 or 1, we need to specify a distribution χ that tells us how e_i is distributed. (We think of χ as a distribution that gives 0 or small values in $\mathbb{Z}_q$ with high probability.)

Definition 75 (Decisional LWE problem) *Fix parameters $n, m, q > 0$ (integers) and a distribution χ over $\mathbb{Z}_q$ Let $A \xleftarrow{\$} \mathbb{Z}_q^{m \times n}$ (a uniformly random binary $m \times n$-matrix) and $s \xleftarrow{\$} \mathbb{Z}_q^n$ (a uniformly random binary n-vector), and let $e \leftarrow \chi^m$ (i.e., e consists of m values independently chosen from χ). Let $r \xleftarrow{\$} \mathbb{Z}^m$.*

The task of the binary decisional LWE problem (with parameters n, m, q, χ) is to distinguish the following two data:

- *A, $As + e$*

- A, r

It is generally believed that this problem is hard for suitable parameters, with some distribution χ of small values.

21.2 Regev's cryptosystem

We now describe how to build a public key encryption scheme based on LWE. It is not the most efficient (it encrypts each bit separately) but it contains important ideas used in many modern lattice-based encryption schemes.

In the following we interpret the elements of $\mathbb{Z}_q$ as integers $\{-\lceil q/2 \rceil + 1, \ldots, \lfloor q/2 \rfloor\}$ (instead of, as usual, as integers $\{0, \ldots, q-1\}$). This is relevant whenever we say something like "$|x| \leq n$ as integers" for some $x \in \mathbb{Z}_q$.

And $\cdot$, applied to two vectors, is the inner product.

Definition 76 (Regev's cryptosystem) *Regev's cryptosystem is a public key encryption scheme with message space* $\{0,1\}$.

- ***Parameters.*** *The parameters n, m, q, χ from Definition 75. We assume that χ is chosen in a way such that $|x \cdot e| \geq q/2$ some small probability p_{error} when $x \xleftarrow{\$} \{0,1\}^m$ and $e \xleftarrow{\$} \chi^m$.*
- ***Key generation.*** *Generate A, b, s as in Definition 75. The secret key is s. The public key is (A, b).*
- ***Encryption.*** *To encrypt $\mu \in \{0,1\}$, pick $x \xleftarrow{\$} \{0,1\}^m$. Let $c_1 := A^T x$ and $c_2 := x \cdot b + \mu \lfloor q/2 \rfloor$ (all calculated in $\mathbb{Z}_q$).*
- ***Decryption.*** *To decrypt (c_1, c_2), we compute $t := c_1 - c_2 \cdot x$. If $|t| < q/4$ (where t is interpreted as an integer, see above), return message 0, otherwise return message 1.*

Lemma 36 (Correctness) *Decrypting the encryption of a message μ returns μ with probability at least $1 - P_{error}$.*

Lemma 37 (IND-CPA security (informal)) *If the decisional LWE problem is hard (for the parameters used in Definition 76) and if $m - n \log q$ is large enough (superlogarithmic), then an encryption of 0 and an encryption of 1 are indistinguishable.*

Further reading: [Pei16] gives an extensive overview of the basics of lattice-based cryptography. (Section 4.2 and 5.2 cover the material given here.) Regev's cryptosystem was originally proposed in [Reg09] together with an formal investigation of the hardness of LWE.

Index

Symbol index

Rev	Revocation algorithm for time vault	35
$TV(m)$	Classical time vault containing m	34
ρ_{raw}	State of A,B,E after raw key measurement in our QKD protocol	
S^{priv}_{Ideal}	Ideal states after privacy amplification	
ρ_{corr}	State of A,B,E after error correction in our QKD protocol	
L_R	Language for the relation R	39
$\langle A(a), B(b)\rangle$	B's output after interacting with A	39
R_{GI}	Relation for graph isomorphism	39
GIP	Proof system for graph isomorphism	40
$\operatorname{ord} a$	Order of group element a	42
$H_\infty(K)$	Min-entropy of K	
$\propto$	Proportional to	43
$\operatorname{dlog} y$	Discrete logarithm of y	43
$\mathbb{F}_q$	Finite field of size q	46
$\frac{\partial f}{\partial x}$	Function f differentiated in variable x	
$x \xleftarrow{\$} Y$	x is uniformly randomly chosen from set Y	28
$H^\varepsilon_\infty(X)$	Smooth min-entropy	32
CNOT	Controlled NOT gate	9
SWAP	SWAP gate	10
$C(U)$	Controlled-U gate	10
$S(\mathcal{H})$	Density operators over $\mathcal{H}$	14
X	Bit flip matrix/gate	5
R_θ	Rotation matrix/gate; rotation angle θ	6
S	Phase shift matrix/gate	6
S_θ	Phase shift matrix/gate; angle θ	6
S^{raw}_{Ideal}	Ideal states after raw key measurement	25
S^{corr}_{Ideal}	Ideal states after error correction	
ρ_{priv}	State of A,B,E after privacy amplification in our QKD protocol	
$S^{t\text{-}Error}_{\text{Ideal}}$	Ideal states after Bell test	24
tr_B	Partial trace ("tracing out B")	16
$\mathcal{E}$	Usually denotes a quantum operation	16
ρ_{init}	State of A,B,E after initial step in our QKD protocol	
ρ_{test}	State of A,B,E after Bell test in our QKD protocol	
$\operatorname{span} M$	Vector space spanned by vectors in M	
$\mathbb{R}$	Real numbers	
$\mathbb{C}$	Complex numbers	
$\mathbb{N}$	Natural numbers, excluding 0	
$\mathbb{Z}$	Integers	
$\lvert x.y\rvert$	Number of non-00 bitpairs in xy	
$\lvert x\rvert$	Absolute value of x (or Hamming weight)	
$\operatorname{im} P$	Image of the linear transformation P	

$\mathcal{H}$	Usually denotes a Hilbert space	
$H_\infty(K\|E)_\rho$	Conditional quantum min-entropy of K given E	25
t-*Error*	Set of Bell states with $\leq t$ errors	24
D_N	Discrete Fourier transform of size N	42
$\lfloor x \rfloor$	x rounded down to the next integer	
$\lceil x \rceil$	x rounded up to the next integer	
$\frac{\partial^2 f}{\partial x^2}$	Function f twice differentiated in variable x	
P_t^{Bell}	Measurement whether at most t error in Bell pairs	37
$P_B^=$	Measurement whether X, Y are equal in basis B	36
x^*	Complex conjugate of $x \in \mathbb{C}$	2
$\langle \Phi, \Psi \rangle$	Inner product of Φ and Ψ	2
$M^\dagger$	Conjugate transpose of matrix M	3
$\|x\|$	Norm (length) of a vector x	2
$\langle \Psi \|$	Dirac notation; the dual of $\|\Psi\rangle$	3
$\|\Psi\rangle$	Dirac notation; represents a vector with name Ψ	3
$\operatorname{tr} M$	Trace of a matrix M	3
$\langle \Phi \| \Psi \rangle$	Inner product of $\|\Phi\rangle$ and $\|\Psi\rangle$ (same as $\langle \Phi, \Psi \rangle$)	3
H	Hadamard matrix/gate	5
$\otimes$	Tensor product	4
$\mathrm{SD}(X, Y)$	Statistical distance between X and Y	17
$\mathcal{F}$	Usually denotes a quantum operation	16
$\|\widetilde{ab}\rangle$	Shorthand notation for tensor product of Bell states	22
$\|\beta_{ab}\rangle$	Bell state (ab determines which one)	21
S_{Ideal}	Set of all ideal states (after execution of QKD protocol)	21
$\rho_{ABE}^{\text{Ideal}}$	Ideal state after execution of QKD protocol	21
ρ_{ABE}^{Real}	State after execution of QKD protocol (case: no abort)	21
$x \leftarrow A$	x is output from algorithm A	34
$\mathrm{TD}(\rho, \sigma)$	Trace distance between ρ and σ	18
QTV	A quantum time vault	35
$H_\infty(K\|E)$	Conditional min-entropy of K given E	