Quantum Error Correcting Codes and Quantum Cryptography

Peter Shor
AT&T Labs
Florham Park, NJ

When the quantum prime factorization algorithm was announced in 1994, one reaction was that this would never work because errors would inevitably disrupt the computation.

How bad is the situation?
To do 10^9 steps on a quantum computer, you need to do each step with inaccuracy less than 10^{-9}. This seems virtually impossible to experimental physicists.

The same objection was raised to scaling up classical computers in the 1950's.

Von Neumann showed that you could build reliable classical computers out of unreliable classical components.

Currently, we don't use many of these techniques because we have *extremely* reliable chips, so we don't need them.

Classical fault-tolerance techniques.

1) Consistency checks

2) Checkpointing

3) Error-correcting codes

4) Massive redundancy

No-cloning theorem:

You cannot duplicate an unknown quantum state.

Heisenberg uncertainty principle:

You cannot complete measure a quantum state.

Doesn't get you very far (quantum or classical)

Doesn't work in quantum case

These work!

Doesn't seem to get you very far in quantum case.

Talk outline:

- Basics of quantum mechanics
- Quantum error correcting codes
  - a simple example
  - CSS codes
- Quantum cryptography
- Proof of security of quantum cryptography using CSS codes

The Superposition Principle:

If a quantum system can be in one of two mutually distinguishable states $|\,\mathbf{A}\rangle$ and $|\,\mathbf{B}\rangle$, it can be both these states at once. Namely, it can be in the *superposition* of states

$$\alpha\,|\,\mathbf{A}\rangle + \beta\,|\,\mathbf{B}\rangle$$

where α and β are both complex numbers and $|\alpha|^2 + |\beta|^2 = 1$.

If you look at the system, the chance of seeing it in state $\mathbf{A}$ is $|\alpha|^2$ and in state $\mathbf{B}$ is $|\beta|^2$.

The state of a quantum system is a unit vector in a complex vector space. A (complete von Neumann) measurement is a projection onto one of a set of d orthogonal basis vectors.

We call a two-dimensional quantum system a *qubit*.

Example: If you have a polarized photon, there can only be two distinguishable states, for example, vertical $|\updownarrow\rangle$ and horizontal $|\leftrightarrow\rangle$ polarizations.

All other states can be made from these two.

$$|\nearrow\rangle = \frac{1}{\sqrt{2}}|\leftrightarrow\rangle + \frac{1}{\sqrt{2}}|\updownarrow\rangle$$

$$|\nwarrow\rangle = \frac{1}{\sqrt{2}}|\leftrightarrow\rangle - \frac{1}{\sqrt{2}}|\updownarrow\rangle$$

$$\left|\circlearrowright\right\rangle = \frac{1}{\sqrt{2}}|\leftrightarrow\rangle + \frac{i}{\sqrt{2}}|\updownarrow\rangle$$

$$\left|\circlearrowleft\right\rangle = \frac{1}{\sqrt{2}}|\leftrightarrow\rangle - \frac{i}{\sqrt{2}}|\updownarrow\rangle$$

If you have two qubits, their joint state space is the tensor product of their individual state spaces (e.g., $\mathbb{C}^4$).

Two qubits can be in any superposition of the four states

$$|\updownarrow\updownarrow\rangle \quad |\updownarrow\leftrightarrow\rangle \quad |\leftrightarrow\updownarrow\rangle \quad |\leftrightarrow\leftrightarrow\rangle$$

This includes states such as an EPR (Einstein, Podolsky, Rosen) pair of photons,

$$\frac{1}{\sqrt{2}}(|\updownarrow\leftrightarrow\rangle - |\leftrightarrow\updownarrow\rangle) = \frac{1}{\sqrt{2}}(|\nearrow\nwarrow\rangle - |\nwarrow\nearrow\rangle),$$

where neither qubit alone has a definite state. These are called *entangled* states.

If you have n qubits, their joint state is described by a 2^n dimensional vector.

We now label basis vectors for each qubit by $|0\rangle$ and $|1\rangle$.

The basis states of this vector space are:

$$|000\ldots00\rangle \quad |000\ldots01\rangle \quad \cdots \quad |111\ldots11\rangle$$

The high dimensionality of this space is one of the places where quantum computing obtains its power.

The Linearity Principle

The evolution of an *isolated* quantum system is linear.

Evolution of pure states in an isolated system can be described by matrices operating on the state space.

To preserve probability, the matrices must be *unitary*.

Von Neumann Measurements

Suppose you have a quantum state space $\mathbb{C}^n$. A von Neumann measurement corresponds to a complete set of orthogonal subspaces S_1, S_2, ... S_k. (Complete means the S_i span $\mathbb{C}^n$.)

Let Π_{S_i} be the projection matrix onto the i'th subspace S_i.

The corresponding von Neumann measurement operating on the quantum state $|\, v\rangle \in \mathbb{C}^n$ takes $|\, v\rangle$ to $\frac{1}{|\Pi_{S_i}|\, v\rangle|}\, \Pi_{S_i}\, |\, v\rangle$ with probability $\langle v \,|\, \Pi_{S_i}\, |\, v\rangle$.

The simplest situation is if each of the S_i is one-dimensional. Then $\Pi_{S_i} = |\, e_i\rangle \langle e_i \,| = e_i e_i^\dagger$, and the e_i form a basis of $\mathbb{C}^n$.

The simplest classical error correcting code is the repetition code.

$$\begin{aligned} 0 &\rightarrow 000 \\ 1 &\rightarrow 111 \end{aligned}$$

What about the quantum version?

$$\begin{aligned} |0\rangle &\rightarrow |000\rangle \\ |1\rangle &\rightarrow |111\rangle \end{aligned}$$

This works against bit flips

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

$$\sigma_x(2): \begin{array}{lcl} |000\rangle & \rightarrow & |010\rangle \\ |111\rangle & \rightarrow & |101\rangle \end{array}$$

Can measure "which bit is different?"
Possible answers: none, bit 1, bit 2, bit 3.
Applying σ_x to incorrect bit corrects error.

This works for superpositions of encoded $|0\rangle$ and $|1\rangle$.

$$\sigma_x(2) : \alpha\,|000\rangle + \beta\,|111\rangle \rightarrow \alpha\,|010\rangle + \beta\,|101\rangle$$

When this is measured, the result is "bit 2 is flipped," and since the measurement gives the same answer for both elements of the superposition, the superposition is not destroyed.

Thus, bit 2 can now be corrected by applying $\sigma_x(2)$.

Three-bit code

$$\begin{aligned} |0\rangle &\rightarrow |000\rangle \\ |1\rangle &\rightarrow |111\rangle \end{aligned}$$

What about a phase flip error

$$\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} ?$$

$$\begin{aligned} |E_0\rangle = |000\rangle &\rightarrow \quad |000\rangle = |E_0\rangle \\ |E_1\rangle = |111\rangle &\rightarrow -|111\rangle = |E_1\rangle \end{aligned}$$

A phase flip on any qubit gives a phase flip on the encoded qubit, so phase flips are three times as likely.

The same thing happens for a general phase error

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

Another 3-qubit code

The unitary transformation

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

takes phase flips to bit flips and vice versa:

$$H \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} H = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Suppose we apply H to the 3 encoding qubits and the encoded qubit. What does this do to our code?

Get new code

$$\begin{aligned} |0\rangle &\rightarrow \frac{1}{2}(|000\rangle + |011\rangle + |101\rangle + |110\rangle) \\ |1\rangle &\rightarrow \frac{1}{2}(|100\rangle + |010\rangle + |001\rangle + |111\rangle) \end{aligned}$$

$$
\begin{aligned}
|0\rangle &\rightarrow \frac{1}{2}(|000\rangle + |011\rangle + |101\rangle + |110\rangle) \\
|1\rangle &\rightarrow \frac{1}{2}(|100\rangle + |010\rangle + |001\rangle + |111\rangle)
\end{aligned}
$$

$|0\rangle$ is encoded as superpositions of states with an odd number of 0's; $|1\rangle$ is encoded as superpositions of states with an even number of 0's.

A bit flip on any qubit exchanges 0 and 1.

A phase flip on any qubit is correctible. E.g., $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ on bit 3.

$$\sigma_z(3)\,|E_0\rangle = \frac{1}{2}(|000\rangle - |011\rangle - |101\rangle + |110\rangle)$$

This is orthogonal to $\sigma_z(a)\,|E_b\rangle$ unless $a = 3$, $b = 0$.

So we can measure "which qubit has a phase flip?" and then correct this qubit.

The 9-qubit code

First quantum error correcting code discovered:

$$|0\rangle \rightarrow \frac{1}{2}(|000000000\rangle + |000111111\rangle + |111000111\rangle + |111111000\rangle)$$

$$|1\rangle \rightarrow \frac{1}{2}(|111000000\rangle + |000111000\rangle + |000000111\rangle + |111111111\rangle)$$

This code will correct any error in one of the nine qubits.

Two concatenated codes: the outer one corrects phase errors, and the inner one corrects bit errors.

If you have a bit flip: $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, it is corrected by comparison with the other two qubits in its group of three.

The 9-qubit code

$$|0\rangle \rightarrow \frac{1}{2}(|000000000\rangle + |000111111\rangle + |111000111\rangle + |111111000\rangle)$$

$$|1\rangle \rightarrow \frac{1}{2}(|111000000\rangle + |000111000\rangle + |000000111\rangle + |111111111\rangle)$$

If you have a phase flip on a single qubit: $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, it gives the same result as a phase flip on any of the other qubits in the same group of three.

The correction works exactly as it does in the three-qubit phase-correcting code.

Theorem: If you can correct a tensor product of t of any of the following three types of error

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

then you can fix any error restricted to t qubits.

Proof Sketch:
The identity matrix and σ_x, σ_y and σ_z for a basis for 2×2 matrices. One can thus decompose any error matrix into a sum of these four matrices. If the error only affects t qubits, it applies the identity matrix to the other qubits, so the decomposition never has more than t terms in the tensor product not equal to the identity.

Example in 3-qubit phase code

$$|0\rangle \rightarrow \frac{1}{2}(|000\rangle + |011\rangle + |101\rangle + |110\rangle)$$
$$|1\rangle \rightarrow \frac{1}{2}(|100\rangle + |010\rangle + |001\rangle + |111\rangle)$$

Suppose we apply a general phase error $\begin{pmatrix} 1 & 0 \\ 0 & e^{2i\theta} \end{pmatrix}$ to qubit 1, say. Can we correct this?

Rewrite error as $\begin{pmatrix} e^{-i\theta} & 0 \\ 0 & e^{i\theta} \end{pmatrix}$

We can do this, since global phase changes are immaterial.

$$\begin{aligned} |E_0\rangle \rightarrow e^{-i\theta}(|000\rangle + |011\rangle) + e^{i\theta}(|101\rangle + |110\rangle) \\ = \cos\theta(|000\rangle + |011\rangle + |101\rangle + |110\rangle) \\ -i\sin\theta(|000\rangle + |011\rangle - |101\rangle - |110\rangle) \end{aligned}$$

When we measure "which bit has a phase flip," we get "bit 1" with probability $|\sin^2\theta|$ and "no error' with probability $|\cos^2\theta|$.

The state has "collapsed," so our measurement is now correct.

We have a 9-qubit code that can correct any error in 1 qubit. How can we make more general quantum codes?

Better classical codes exist than repetition codes.

The $[7, 4, 3]$ Hamming code, for example.

The codewords are the binary row space of

$$\begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

This code maps 4 bits to 7 bits. The minimum distance between two codewords is 3, so it can correct one error.

Generator matrix for Hamming code:

$$G = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

To correct errors, we use the parity check matrix H. This is a generator matrix of $\mathbf{C}^{\perp} = \{v : v \cdot w = 0 \text{ for all } w \in \mathbf{C}\}$.

$$H = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{bmatrix}$$

$H \cdot v = 0$ if $v \in \mathbf{C}$.

$H \cdot v$ is the *syndrome*. This syndrome gives the location of the incorrect bits.

Quantum Hamming code

$$|0\rangle \to \frac{1}{\sqrt{8}} \begin{pmatrix} & |0000000\rangle & + & |1110100\rangle \\ + & |0111010\rangle & + & |0011101\rangle \\ + & |1001110\rangle & + & |0100111\rangle \\ + & |1010011\rangle & + & |1101001\rangle \end{pmatrix} \quad (H)$$

$$|1\rangle \to \frac{1}{\sqrt{8}} \begin{pmatrix} & |1100010\rangle & + & |0110001\rangle \\ + & |1011000\rangle & + & |0101100\rangle \\ + & |0010110\rangle & + & |0001011\rangle \\ + & |1000101\rangle & + & |1111111\rangle \end{pmatrix} \quad (H + \bar{1})$$

The bit flip errors are correctible, since all elements in these superpositions are in the Hamming code (if you measure the syndrome, you know which bit to correct).

The phase flip errors are correctible since applying $H = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ to all 7 encoding qubits and to the encoded qubit takes the code to itself.

CSS codes (Calderbank & Shor, Steane)

Start with two binary codes such that

$$\{0\} \subseteq \mathbf{C}_2 \subseteq \mathbf{C}_1 \subseteq \mathbf{F}_2^n$$

(So $\{0\} \subseteq \mathbf{C}_1^\perp \subseteq \mathbf{C}_2^\perp \subseteq \mathbf{F}_2^n$)

The quantum code has basis elements corresponding to $v \in \mathbf{C}_1/\mathbf{C}_2$.

$$v \to \frac{1}{2^{k/2}} \sum_{x \in \mathbf{C}_2} |\, v + x \rangle$$

$k = \dim \mathbf{C_1} - \dim \mathbf{C_2}$
This will correct t errors, where

$$2t + 1 \leq \min(\mathrm{wt}\mathbf{C}_1, \mathrm{wt}\mathbf{C}_2^\perp)$$

$\mathbf{C}_1$ corrects bit errors
$\mathbf{C}_2^\perp$ corrects phase errors

rate: $\frac{\dim \mathbf{C_1} - \dim \mathbf{C_2}}{n}$

Suppose we have a CSS code with

$$\{0\} \subseteq \mathbf{C}_2 \subseteq \mathbf{C}_1 \subseteq \mathbf{F}_2^n.$$

What happens when we apply $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ to each qubit of it?

We start with the encoding of $v \in \mathbf{C}_1/\mathbf{C}_2$:

$$|\, E_v \rangle = |\mathbf{C}_2|^{-1/2} \sum_{x \in \mathbf{C}_2} |\, v + x \rangle \,.$$

When we apply $H^{\otimes n}$ to a state $|\, s \rangle$, we get a (-1) factor for each qubit where $|\, 1 \rangle$ goes to $|\, 1 \rangle$. Thus,

$$H^{\otimes n} |\, s \rangle = \frac{1}{2^{n/2}} \sum_{t \in \mathbf{F}_2^n} (-1)^{s \cdot t} |\, t \rangle$$

Applying this to the encoded state $|\, E_v \rangle$, we get

$$H^{\otimes n} |\, E_v \rangle = \frac{|\mathbf{C}_2|^{-1/2}}{2^{n/2}} \sum_{t \in \mathbf{F}_2^n} \sum_{x \in \mathbf{C}_2} (-1)^{(v+x) \cdot t} |\, t \rangle$$

$$
\begin{aligned}
H^{\otimes n} \,|\, E_v \rangle &= \frac{|\mathbf{C}_2|^{-1/2}}{2^{n/2}} \sum_{t \in \mathbf{F}_2^n} \sum_{x \in \mathbf{C}_2} (-1)^{(v+x)\cdot t} \,|\, t \rangle \\
&= \frac{|\mathbf{C}_2|^{1/2}}{2^{n/2}} \sum_{t \in \mathbf{C}_2^\perp} (-1)^{v \cdot t} \,|\, t \rangle \\
&= \frac{|\mathbf{C}_2|^{1/2}}{2^{n/2}} \sum_{t \in \mathbf{C}_2^\perp / \mathbf{C}_1^\perp} (-1)^{v \cdot t} \sum_{y \in \mathbf{C}_1^\perp} |\, t + y \rangle \\
&= \frac{1}{2^{k/2}} \sum_{t \in \mathbf{C}_2^\perp / \mathbf{C}_1^\perp} (-1)^{v \cdot t} \left| \hat{E}_t \right\rangle .
\end{aligned}
$$

where $\left| \hat{E}_t \right\rangle$ is t encoded in the dual quantum code, corresponding to classical codes

$$\{0\} \subseteq \mathbf{C}_1^\perp \subseteq \mathbf{C}_2^\perp \subseteq \mathbf{F}_2^n.$$

Thus, $H^{\otimes n} \,|\, v \rangle$ is the Fourier transform of the vector v encoded in the dual quantum code.

Density Matrices

In quantum mechanics, the fundamental objects are often taken to be pure quantum states (unit vectors in $\mathbb{C}^n$).

For quantum information theory, we need to work with density matrices, which arise from probability distributions over pure states.

Density matrix ρ:
Hermitian trace 1 positive semi-definite matrix over $\mathbb{C}^n \times \mathbb{C}^n$.

A rank one density matrix corresponds to a pure state (i.e., vector in $\mathbb{C}^n$).

More on Density Matrices

Suppose a quantum system is in state v_i with probability p_i.

The density matrix is

$$\rho = \sum_i p_i v_i v_i^\dagger = \sum_i p_i \mid v_i \rangle \langle v_i \mid$$

The density matrix ρ gives as much information as possible about the outcomes of experiments performed on the system.

Two systems with the same density matrix ρ are indistinguisable.

Example

Consider a qubit which either is in state $|\updownarrow\rangle$ or state $|\leftrightarrow\rangle$, with probability $\frac{1}{2}$ for each state.

$$\rho = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \frac{1}{2}\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Consider a qubit which either is in state $|\swarrow\!\!\nearrow\rangle$ or state $|\nwarrow\!\!\searrow\rangle$, with probability $\frac{1}{2}$ for each state.

$$\rho = \frac{1}{4}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} + \frac{1}{4}\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Quantum Cryptography

First published in 1982, this was one of the first applications of quantum weirdness to computer science tasks.

The BB84 (Bennett and Brassard, 1984) protocol is a key distribution protocol. Two parties, Alice and Bob, are trying to agree on a key which any eavesdropper (Eve) will not be able to ascertain by listening to their conversation. The idea is to use the fact that any attempt to measure a quantum state must inescapably disturb it. Alice sends Bob photons. Bob chooses some of these photons at random and checks for disturbance, while others yield the secret key.

The model we discuss: Alice and Bob have a classical channel which Eve can eavesdrop, and a quantum channel which Eve can do anything to (you can't eavesdrop on a quantum channel without disturbing it). Since Eve can potentially cut the quantum channel, Alice and Bob don't have any guarantee that they will be able to agree on a key. The goal of the protocol is to make the chance of Eve knowing a key that Alice and Bob have agreed on very small.

So with very high probability, Alice and Bob will either agree on a key that Eve doesn't know, or decide that the quantum channel is too noisy for secure communication.

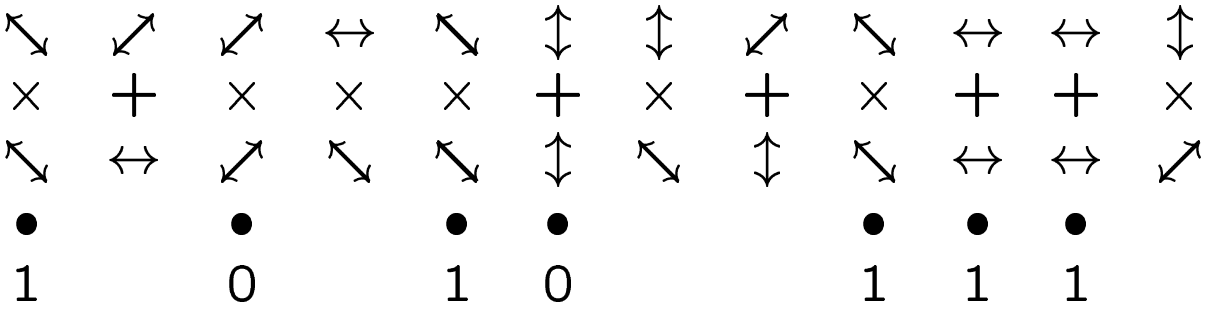
A) Alice sends random qubits in one of the four states.

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

B) Bob measures them randomly in either the $\{|0\rangle, |1\rangle\}$ basis or the $\frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$ basis

C) Alice and Bob reveal the sending and receiving bases, and obtain a string of bits that they agree on.

D) Some of these bits are used to test for errors; the rest form the key.



Because the density matrices for the two complementary bases are equal, i.e.,

$$\frac{1}{2}|\updownarrow\rangle\langle\updownarrow| + \frac{1}{2}|\leftrightarrow\rangle\langle\leftrightarrow| = \frac{1}{2}|\nearrow\rangle\langle\nearrow| + \frac{1}{2}|\nwarrow\rangle\langle\nwarrow|$$

Eve cannot measure which basis Alice sent her bits in. If Eve gains information in about one of the two possible complementary bases, she disturbs states sent in the other. Thus, if Eve gets any information, she incurs a probability to perturb the signals, and thus be detected.

But Alice and Bob's channel won't be perfect, so there will be some disturbance anyway. How can they do quantum cryptography given a noisy channel?

Quantum Cryptography over Noisy Channels

Alice and Bob use an error correcting code to fix any errors caused by noise.

They then apply a hash function to the resulting key to gain privacy.
We prove security in the case where they use a *linear* hash function.

Alice and Bob take an n-bit key $\mathbf{k}$, apply a 0-1 $n \times m$ matrix to it, and obtain an m-bit key $\mathbf{k}'$.

It took till 1996 to obtain a proof of security for quantum cryptography over noisy channels. We give a much simpler proof (discovered jointly with John Preskill) by using quantum error correcting codes.

The proof first shows a different key distribution protocol, based on error correcting codes, is secure, and then shows that the two protocols are equivalent in terms of what an eavesdropper can learn.

CSS key distribution protocol

Idea: Alice encodes the key using a CSS code. She sends the CSS code to Bob, interspersing it with test bits. Bob uses the test bits to find the error rate, and if the error rate is low enough, he decodes the key and uses it.

If the error rate is low, the CSS code delivers the encoded state with high fidelity. Thus, by the no-cloning theorem of quantum information, the code cannot leak much information, and the key is thus secure.

This code assumes that Bob has quantum memory, as he has to store the qubits until Alice tells him which are test bits and which are code bits.

So it is currently impractical.

CSS key distribution protocol

Problem: We have to make sure that Eve cannot detect which bits are being used for the code and which bits are being used for the test bits. (If she could, she could leave the test bits alone, and just measure the code bits).

Solution: We use one of a set of shifts of the CSS code. Instead of encoding

$$v \to |\mathbf{C}_2|^{-1/2} \sum_{x \in \mathbf{C}_2} |\, v + x \rangle$$

we pick a random $w \in \mathbf{F}_2^n/\mathbf{C}_2^\perp$, $z \in \mathbf{F}_2^n/\mathbf{C}_1$ and encode

$$v \to |\mathbf{C}_2|^{-1/2} \sum_{x \in \mathbf{C}_2} (-1)^{w \cdot x} |\, v + x + z \rangle$$

Adding z gives a random shift of the code, and changing the phase using w gives a random shift of the code in the Fourier transform space.

Alice sends a random shift of the CSS quantum code

$$v \to |\mathbf{C}_2|^{-1/2} \sum_{x \in \mathbf{C}_2} (-1)^{w \cdot x} \, | \, v + x + z \rangle$$

$w \in \mathbf{F}_2^n / \mathbf{C}_2^\perp$ and $z \in \mathbf{F}_2^n / \mathbf{C}_1$ chosen at random.

Here Alice has chosen a random $v \in \mathbf{C}_1 / \mathbf{C}_2$. The random choises of Alice have the effect of making the quantum state Alice perfectly random (without knowledge of z, w, which Alice does not reveal until Bob has received the data). Thus Eve cannot distinguish between the code bits and the random test bits.

Calculations for previous slide:

The density matrix averaging over all encodings of v is

$$\frac{|\mathbf{C}_1|}{2^{2n}} \sum_{\substack{w \in \mathbf{F}_2^n/\mathbf{C}_2^\perp \\ z \in \mathbf{F}_2^n/\mathbf{C}_1}} \sum_{x_1, x_2 \in \mathbf{C}_2} (-1)^{w \cdot (x_1 + x_2)} \, | \, v + x_1 + z \rangle \langle v + x_2 + z \, |$$

$$= \frac{|\mathbf{C}_1|}{2^n |\mathbf{C}_2|} \sum_{z \in \mathbf{F}_2^n/\mathbf{C}_1} \sum_{x \in \mathbf{C}_2} | \, v + x + z \rangle \langle v + x + z \, |$$

Since Alice chooses a random $v \in \mathbf{C}_1/\mathbf{C}_2$, this state is indistinguishable from the maximally random density matrix $2^{-n} I$.

Equivalence to BB84

Alice sends a random shift of the quantum code

$$v \to |\mathbf{C}_2|^{-1/2} \sum_{x \in \mathbf{C}_2} (-1)^{w \cdot x} \, | \, v + x + z \rangle$$

Alice never needs to reveal w; since Bob wants to get the bits Alice sends and doesn't care about the phases, he doesn't need to correct the phase errors. Thus, the state Bob receives, for a given key v and a gien shift z, is the average over w of the quantum states encoded above, or the density matrix

$$2^{-n} \sum_{w \in \mathbf{F}_2^n / \mathbf{C}_2^\perp} \left(\sum_{x_1 \in \mathbf{C}_2} (-1)^{w \cdot x_1} \, | \, v + x_1 + z \rangle \right) \left(\sum_{x_2 \in \mathbf{C}_2} (-1)^{w \cdot x_2} \, \langle v + x_2 + z \, | \right)$$

Bob receives

$$2^{-n} \sum_{w \in \mathbf{F}_2^n / \mathbf{C}_2^\perp} \sum_{x_1, x_2 \in \mathbf{C}_2} (-1)^{w \cdot (x_1 + x_2)} \, | \, v + x_1 + z \rangle \langle v + x_2 + z \, |$$

$$= \frac{1}{|\mathbf{C}_2|} \sum_{x \in \mathbf{C}_2} | \, v + x + z \rangle \langle v + x + z \, |$$

This average destroys all the phase information, and thus is the same as the average over $x \in \mathbf{C}_2$ of $| \, v + x + z \rangle$. Now, we see the equivalence to BB84. The code $\mathbf{C}_1$ is the error correcting code used in BB84 to fix hash errors. The code $\mathbf{C}_2$ corresponds to the linear hash function in BB84, as adding any vector in $\mathbf{C}_2$ gives the same key, and is thus equivalent to multiplying by a generator matrix for $\mathbf{C}_2^\perp$.

Eve sees the same density matrix arising from the good bits of BB84 (those where Alice and Bob use the same basis for sending and receiving) and the CSS key distribution protocol. Thus, if one is secure, the other is as well.

Open Question:

This is one of several proofs of security for BB84 (Dominic Mayers; Biham, Boyer, Boykin, Mor, Roychowdhury; Michael Ben-Or).

However, none of these seem to extend to the 1992 key distribution protocol of Bennett, which has less symmetry available to work with. Can B92 be proved secure?