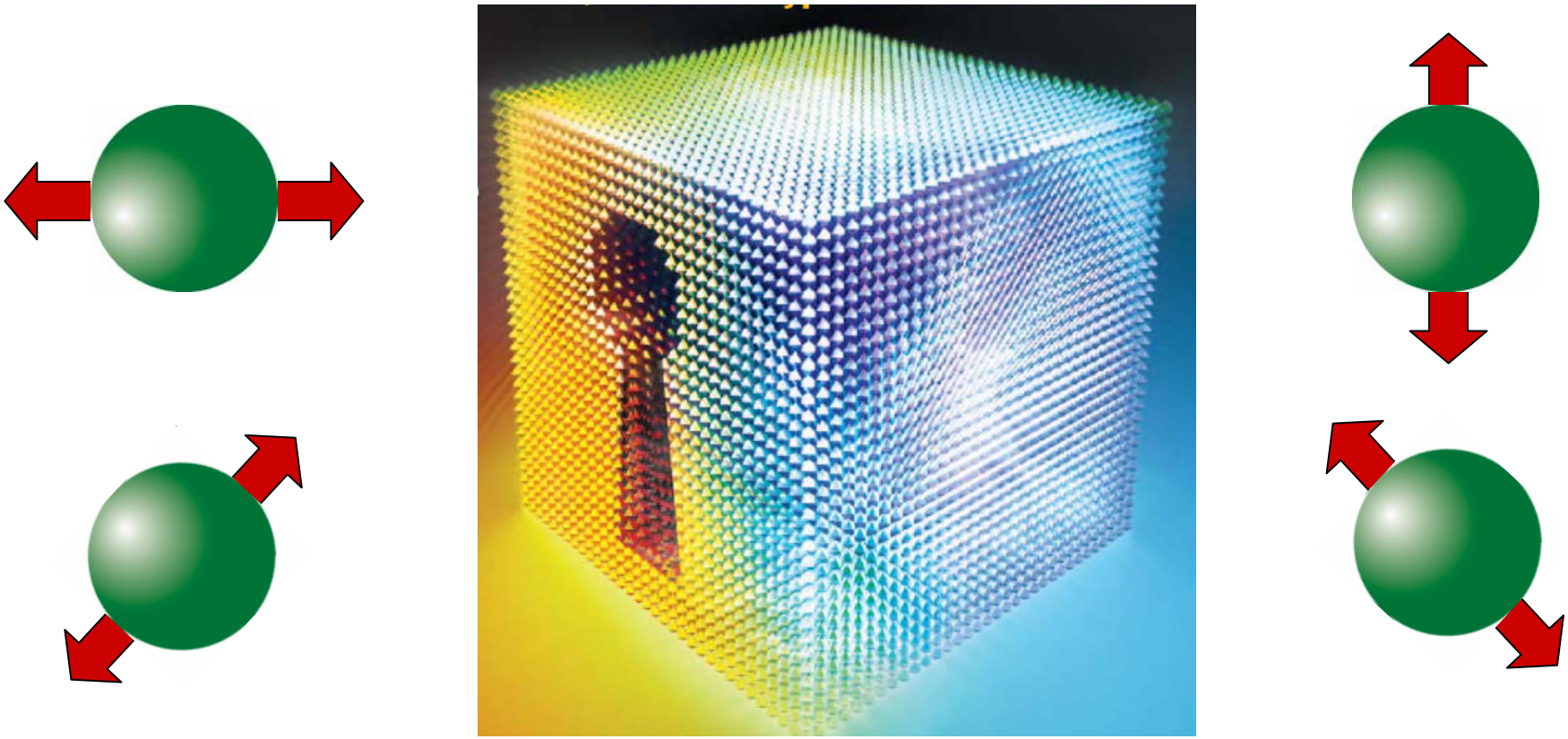
The security of quantum cryptography



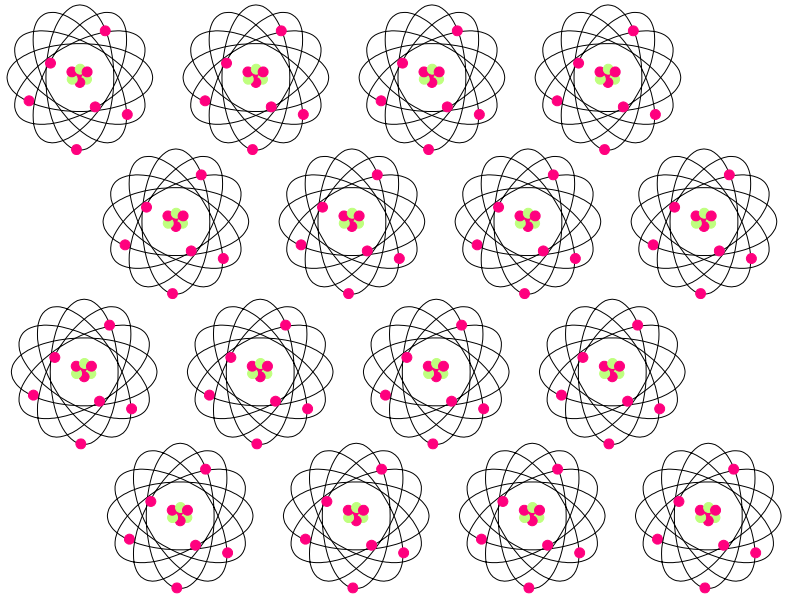
Institute for Quantum Information

John Preskill, Caltech

Biedenharn Lecture 2

8 September 2005

The *Quantum* Century



Though quantum theory is more than 100 years old, there are profound aspects of the difference between quantum and classical systems that we have begun to understand in just the past few years.

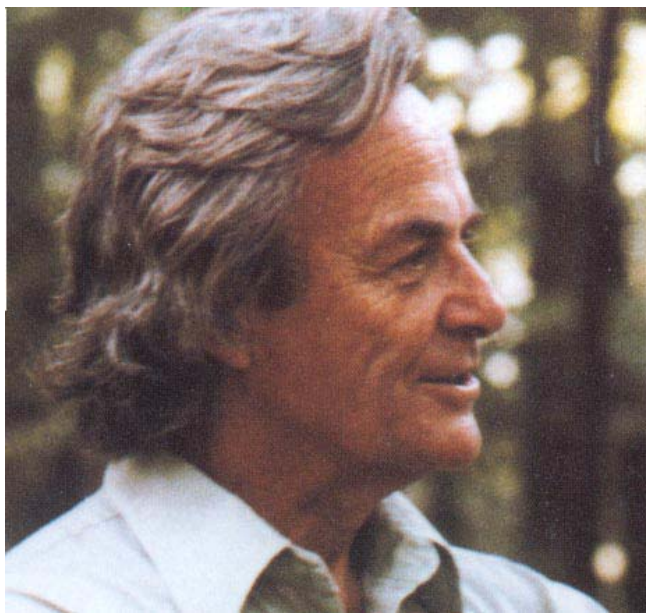
Theoretical Quantum Information Science

is driven by ...

Three ***Great*** Ideas:

1) Quantum Computation
2) Quantum Cryptography
3) Quantum Error Correction

Quantum Computation

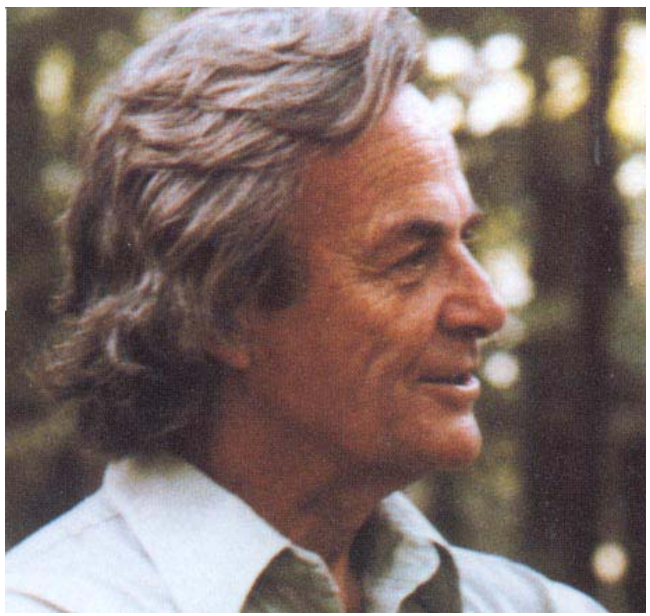


Feynman ‘81

Deutsch ‘85

Shor ‘94

A computer that operates on quantum states can perform tasks that are beyond the capability of any conceivable classical computer.



Feynman ‘81

Deutsch ‘85

Shor ‘94

Finding Prime Factors

1807082088687
4048059516561
6440590556627
8102516769401
3491701270214
5005666254024
4048387341127
5908123033717
8188796656318
2013214880557

$= ? \times ?$

Finding Prime Factors

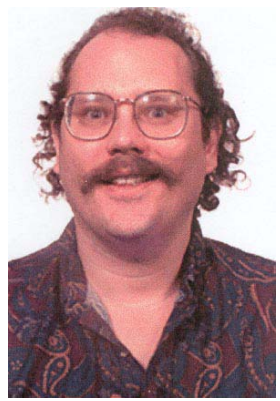
1807082088687
4048059516561
6440590556627
8102516769401
3491701270214
5005666254024
4048387341127
5908123033717
8188796656318
2013214880557

=

3968599945959
7454290161126
1628837860675
7644911281006
4832555157243

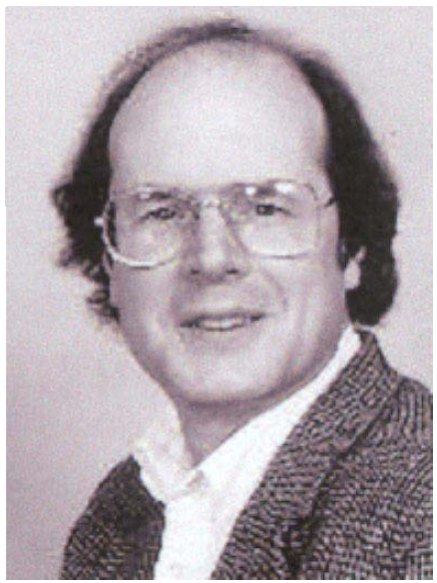
×

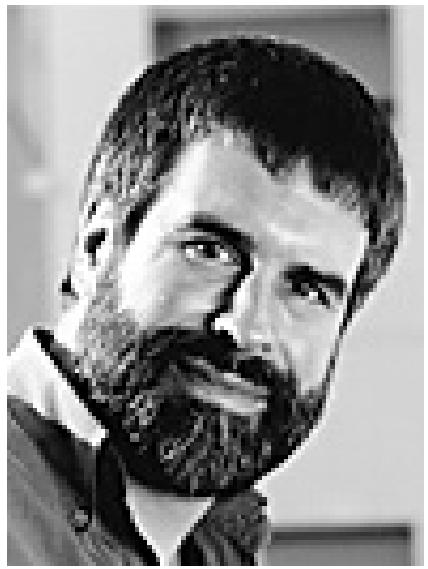
4553449864673
5972188403686
8972744088643
5630126320506
9600999044599



Shor ‘94

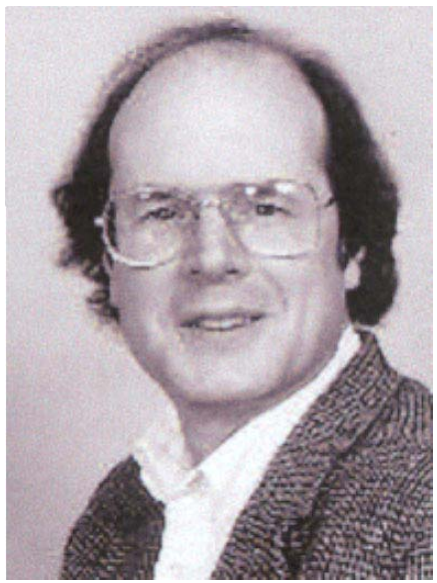
Quantum Cryptography

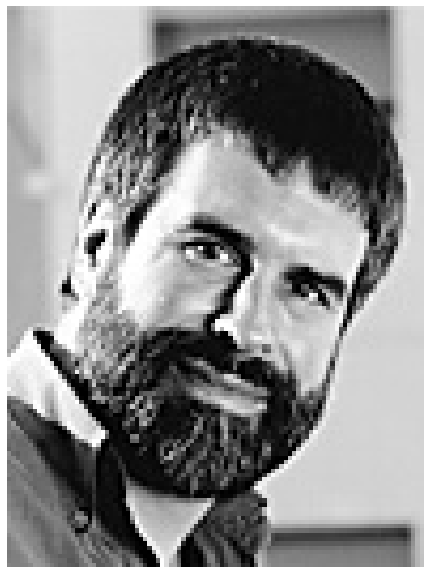




Bennett Brassard ’84

Eavesdropping on quantum information can be detected; key distribution via quantum states is *unconditionally* secure.





Bennett Brassard ’84

Quantum Cryptography

Alice

Eve

Bob

Privacy is founded on principles of fundamental physics, not the assumption that eavesdropping requires a difficult computation. Gathering information about a quantum state unavoidably disturbs the state.

Quantum Error Correction

Shor ‘95

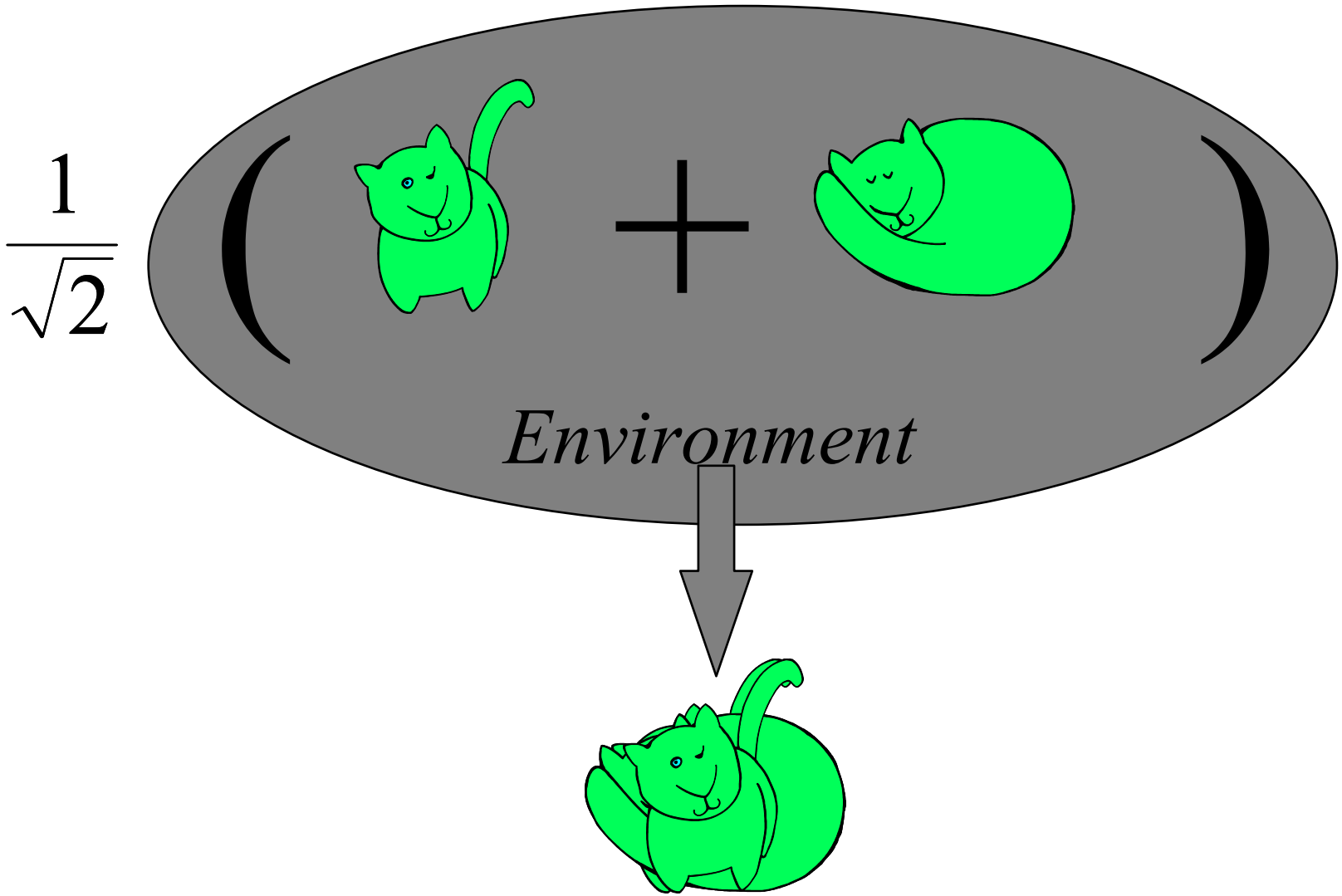
Steane ‘95

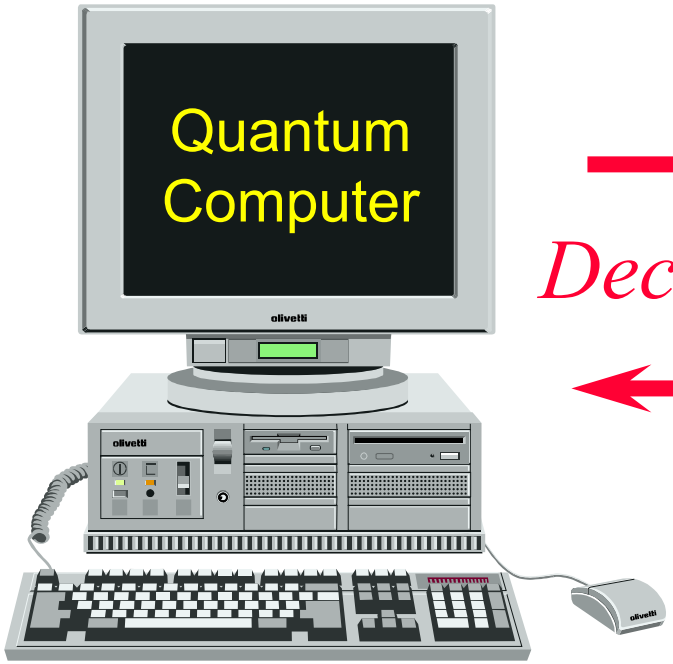
Quantum information can be protected, and processed fault-tolerantly.

Shor ‘95

Steane ‘95

Decoherence





Decoherence

Environment

ERROR!

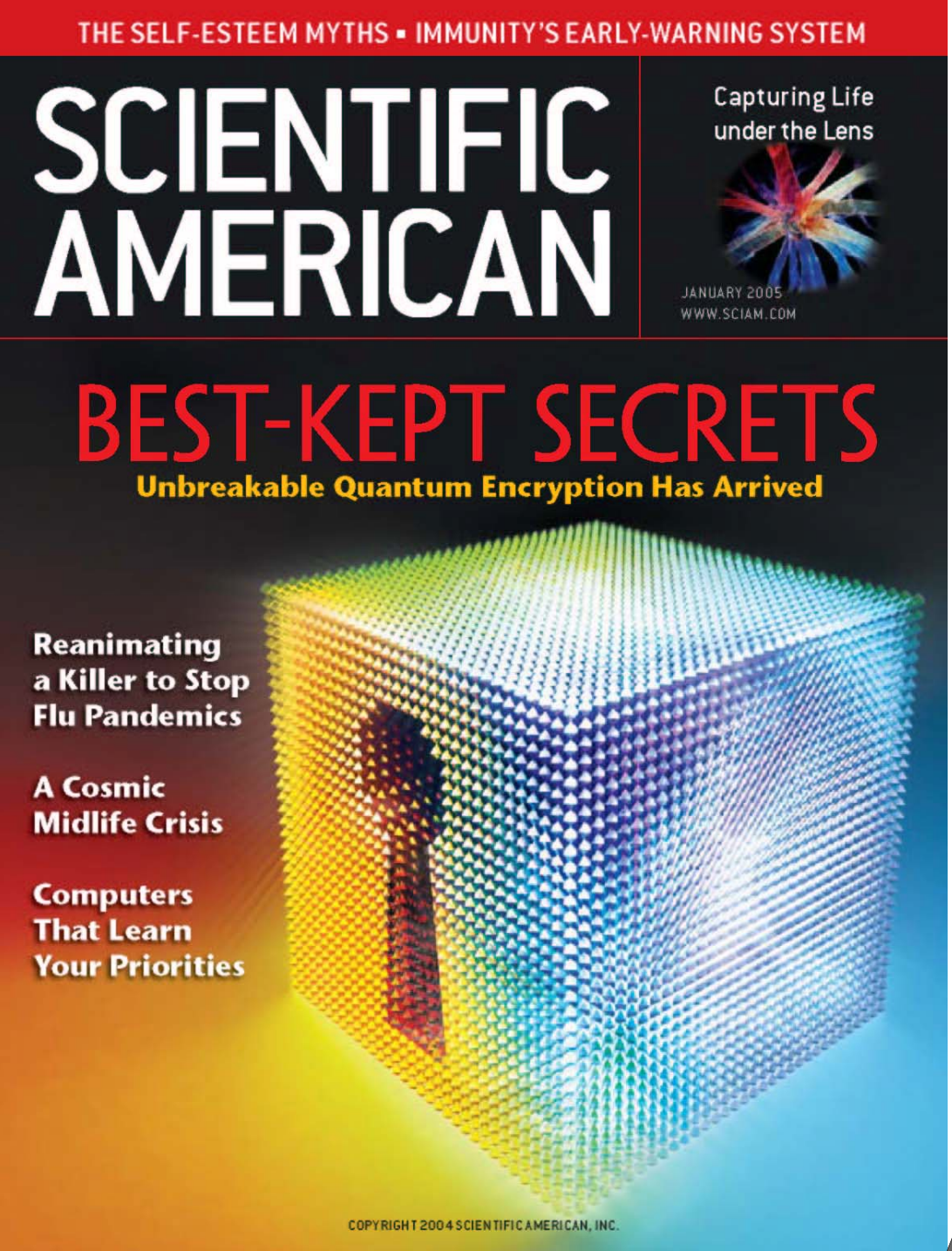
If quantum information is cleverly encoded, it *can* be protected from decoherence and other potential sources of error. Intricate quantum systems *can* be accurately controlled.

Theoretical Quantum Information Science

is driven by ...

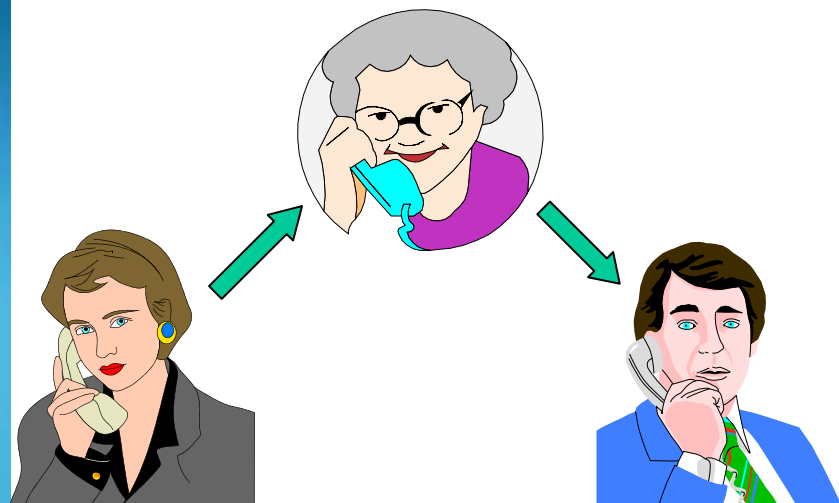
Three ***Great*** Ideas:

1) Quantum Computation
2) Quantum Cryptography
3) Quantum Error Correction



Note: Quantum key distribution, unlike large-scale quantum computing, is feasible with existing technology...

WARNING: Alice, Bob, and Eve appear in this talk.



Quantum cryptography

1, Cryptography and security

2. Quantum key distribution: key from entanglement

3. Quantum key distribution: the four-state protocol

4. Quantum error correction: secure key from entanglement

5. Security proof for the four-state protocol

Cryptography

In a cryptographic protocol, two or more parties perform a task while protecting privileged information from unauthorized parties.

For example, Alice might wish to send a secret to Bob, without allowing the eavesdropper Eve to learn the secret.

Typical classical cryptographic protocols are *computationally secure.* This means that the security is founded on an (unproven) assumption that a certain computation that would break the protocol is too *hard* for the adversary to execute.

If the adversary might have a *quantum computer*, the usual assumptions about classical cryptography need to be reexamined.

Alice

Bob

One-time pad

Stronger than computational security is *information-theoretic security*. This means that even an adversary with unlimited computational power is unable to break the protocol.

A classical protocol for secret communication that is information-theoretically secure is the *one-time pad*. If Alice and Bob share a string of random bits (the “key”), then that key can be used to encipher and decipher a message. If Eve knows nothing about the key then she will not learn anything about the message by intercepting the ciphertext.

The key should be used only once (if it is used repeatedly information-theoretic security will be compromised), and then should be destroyed to ensure that Eve will not acquire a copy.

Alice

Eve

Bob

Message: HI BOB

01001000 01001001 00100000 01000010 01001111 01000010
01110100 10111001 00000101 10101001 01011100 01110100

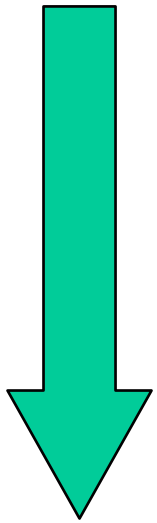
00111100 11110001 00100101 11101011 00010011 00110110

Alice

Message: HI BOB

01001000 01001001 00100000 01000010 01001111 01000010
01110100 10111001 00000101 10101001 01011100 01110100

Eve



Bob

00111100 11110001 00100101 11101011 00010011 00110110
01110100 10111001 00000101 10101001 01011100 01110100

01001000 01001001 00100000 01000010 01001111 01000010

HI BOB

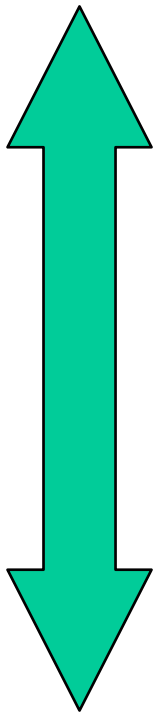
Alice

Eve

Bob

Message: HI BOB

01110100 10111001 00000101 10101001 01011100 01110100



Alice and Bob can communicate privately if they share a random key that Eve doesn't know.

01110100 10111001 00000101 10101001 01011100 01110100

HI BOB

One-time pad

But what if Alice and Bob possess no shared secret random key? Perhaps they are far apart, and have never met. Or perhaps they have already consumed the key they previously shared, and do not dare to reuse it. They could ask their friend Charlie to act as an intermediary, distributing the key to Alice and Bob, but can Charlie be trusted? Perhaps Charlie is covertly in cahoots with Eve.

Alice

Bob

Public-key cryptography (Diffie-Hellman '76)

Classically, this difficulty can be overcome by "public key cryptography." In public key cryptography, there are two keys, one public and one private. Everyone (including Alice and Eve) knows the public key, which is used for enciphering, but only Bob knows the private key, which is used for deciphering. Thus, anyone can send an encrypted message to Bob, but only Bob can read it! Actually, it is possible in principle to infer the private key from the known public key, but this requires a computation that is believed to be prohibitively difficult.

Alice

Public key cryptography uses a *1-way function* f, a function that is easy to compute, but hard to invert unless the private key is known:

Bob

Alice encrypts message a, obtaining ciphertext b: $a \rightarrow b = f(a)$

Bob decrypts ciphertext, recovering message: $b \rightarrow a = f^{-1}(b)$

Digital signature

Alice

Bob

Public key cryptography uses a *1-way function* f, a function that is easy to compute, but hard to invert unless the private key is known:

Alice encrypts message a, obtaining ciphertext b: $a \rightarrow b = f(a)$

Bob decrypts ciphertext, recovering message: $b \rightarrow a = f^{-1}(b)$

Aside from encryption/decryption, public key cryptography also allows Alice to verify that a message was actually sent by Bob (or at least by someone who knows the private key). Bob *signs* his message using the private key, and Alice verifies his signature using the public key. Anyone can verify Bob's signature, but only Bob can sign.

Bob appends signature a to message b: $b \rightarrow a = f^{-1}(b)$

Alice verifies Bob's signature: $a \rightarrow b = f(a)$

RSA (Rivest-Shamir-Adleman '77)

RSA is a widely used public key crypto-system whose security is founded on the presumed difficulty of factoring large numbers.

Bob generates two prime numbers p and q (primality is easy to check), computes their product $N=pq$ and the Euler function $\varphi(N)=(p-1)(q-1)$. He choses $e < \varphi(N)$ co-prime to $\varphi(N)$, and computes $d=e^{-1} \pmod{\varphi(N)}$. Bob announces e and N (the public key) but he keeps secret d and $\varphi(N)$ (the private key).

Alice encrypts $a < N$ by computing

$$b = f(a) = a^{e} \pmod{N}$$

Bob decrypts by computing

$$a = f^{-1}(b) = b^{d} \pmod{N} = a \pmod{N}$$

It works because of Euler's theorem:

$$a^{\varphi(N)} = 1 \pmod{N}$$ (where a is co-prime to N).

RSA

Bob generates two prime numbers p and q (primality is easy to check), computes their product $N=pq$ and the Euler function $\varphi(N)=(p-1)(q-1)$. He choses $e < \varphi(N)$ co-prime to $\varphi(N)$, and computes $d=e^{-1} \pmod{\varphi(N)}$. Bob announces e and N, but he keeps d and $\varphi(N)$ secret.

A quantum computer (or any superfast factoring machine) can break RSA! If Eve can factor N she easily computes $\varphi(N)$ and d.

In fact it suffices to compute the *order* of $b=a^e \pmod{N}$ which is the same as the order of $a \pmod{N}$ and to "invert" e modulo $Order(a)$. Therefore, Eve can crack RSA if she can determine the period of a function (an abelian hidden subgroup problem).

There are other public-key schemes, but these, too are (or might be) vulnerable to quantum attacks...

Alice

Quantum cryptography?

Bob

Thus, if and when quantum computers become available, much of classical cryptography will become obsolete. But that won't happen for a while, so do Alice and Bob need to worry about it today? Possibly. Sometimes, it is important for a secret to remain confidential for a long time in the future. What if Alice is telling Bob about the classified design of a nuclear weapon, or the identities of covert agents who have penetrated Al Qaeda? How certain can Alice and Bob be that today's communications, intercepted and archived (but not yet decoded) by the adversary, will not be deciphered in, say, 30 years?

So quantum computing may be bad news for cryptologists. But while quantum theory taketh away, quantum theory also giveth: *quantum key distribution* is information-theoretically secure!


Enjoy
Coca-Cola

Alice

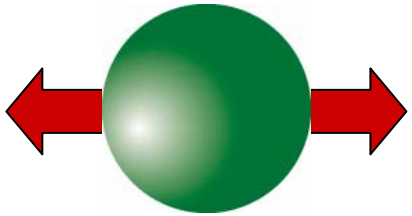
Quantum key distribution and the one-time pad

Bob

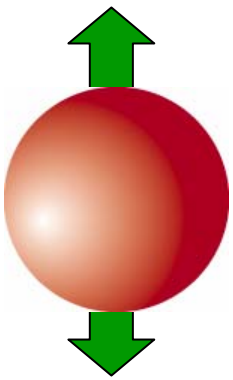
But what if Alice and Bob possess no shared secret random key? Perhaps they are far apart, and have never met. Or perhaps they have already consumed the key they previously shared, and do not dare to reuse it. They could ask their friend Charlie to act as an intermediary, distributing the key to Alice and Bob, but can Charlie be trusted? Perhaps Charlie is covertly in cahoots with Eve.

They can solve the problem of distributing a secure (classical) key by using quantum information. Furthermore, quantum key distribution (unlike quantum computation) is feasible with today's technology.

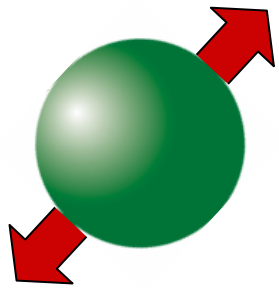
Photon polarization as a qubit



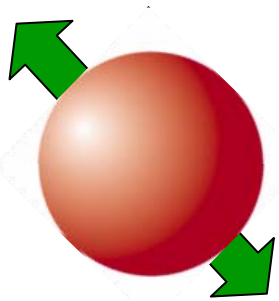
$= |0\rangle$



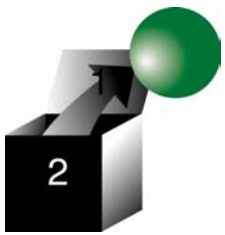
$= |1\rangle$

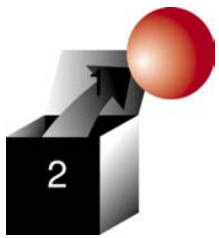


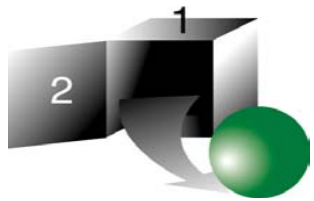
$= \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle \right)$

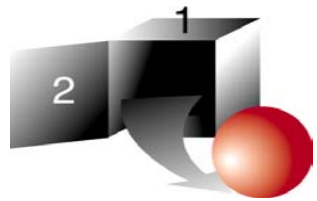


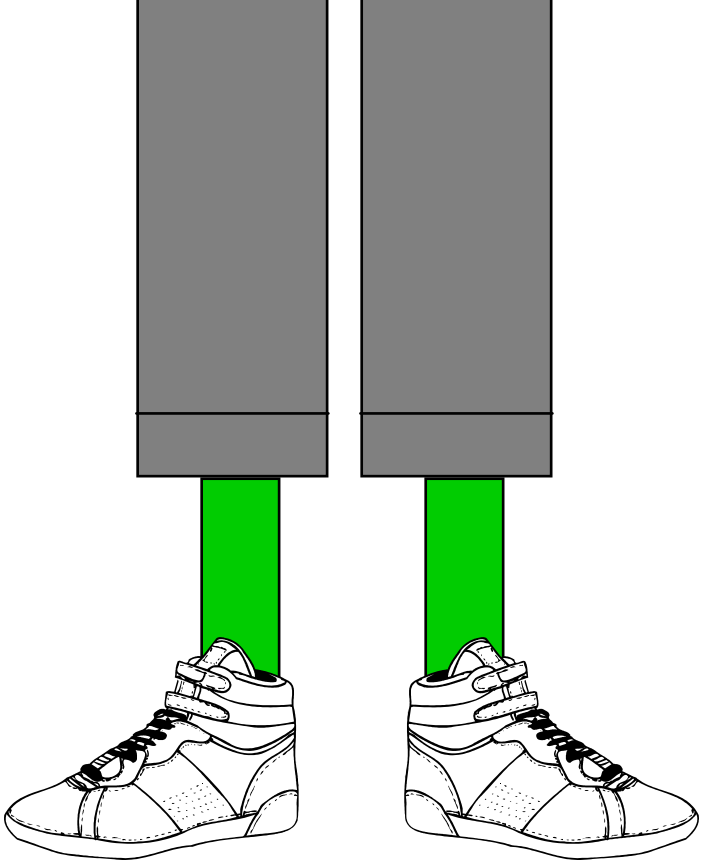
$= \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle \right)$

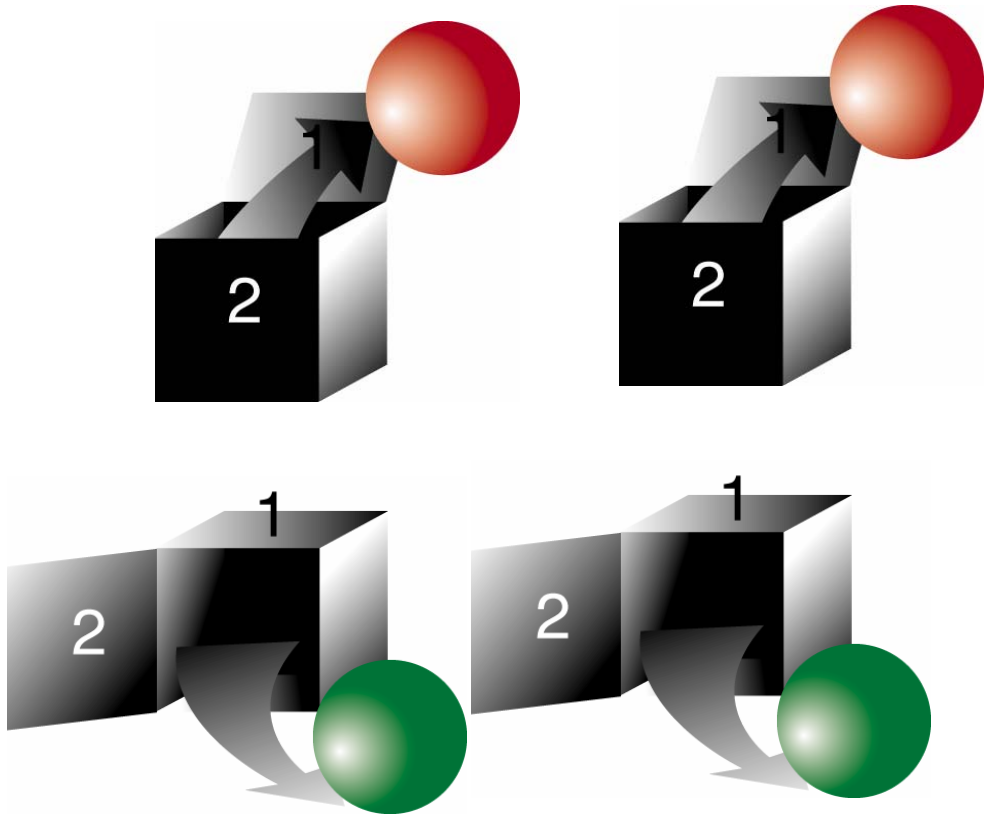












Classical Correlations

Quantum Correlations

Boxes are not like soxes!

EPR quantum key distribution

Here is one way to accomplish QKD. Suppose that Alice and Bob share many copies of the maximally entangled (EPR, Bell) state of two qubits:

Alice

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle_{AB} + |11\rangle_{AB}\right)$$

Bob

This state can be conveniently characterized as the simultaneous eigenstate with eigenvalue one of two commuting operators: $X \otimes X = 1 = Z \otimes Z$, where

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

denote the Pauli matrices.

EPR quantum key distribution

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle_{AB} + |11\rangle_{AB}\right)$$

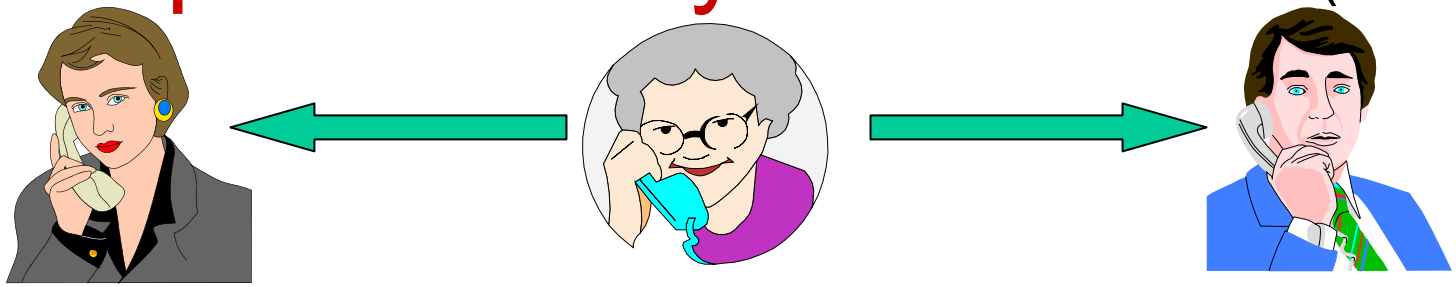
This state has the property that if Alice or Bob measures either X or Z, the outcome is random, e.g., $Z=1$ and $Z=-1$ occur each with probability 1/2. Furthermore, if they measure the same observable, Bob's outcome is perfectly correlated with Alice's, since $X \otimes X = 1 = Z \otimes Z$.

Consider this protocol:

1) On her half of each pair, Alice decides at random to measure either X or Z.
2) Bob does the same.
3) Through public discussion, Alice and Bob discard the results in the cases where they measured in different bases, retaining the rest.

Thus, Alice and Bob generate a shared random string.

EPR quantum key distribution (Ekert '91)



But … is it *secure?* Eve may have tampered with the pairs at some time in the past, and could have entangled them with a probe that she controls. After Alice and Bob publicly announce their bases, she might measure her probe to collect information about the key. If Eve *has* tampered with the pairs, the joint state of the pairs and Eve's probe has the form:

$$|\Phi\rangle_{ABE} = \frac{1}{\sqrt{2}}\left(\begin{array}{c} |00\rangle_{AB}|e_{00}\rangle_E + |01\rangle_{AB}|e_{01}\rangle_E \\ + |10\rangle_{AB}|e_{10}\rangle_E + |11\rangle_{AB}|e_{11}\rangle_E + \end{array} \right)$$

(where the $|e\rangle$'s need not be normalized or mutually orthogonal) --- or else it is a mixture of such states. *Suppose* that Alice and Bob can verify that each of their pairs satisfies $X \otimes X = 1 = Z \otimes Z$. Then...

EPR quantum key distribution (Ekert '91)

$$|\Phi\rangle_{ABE} = \frac{1}{\sqrt{2}}\Big(|00\rangle_{AB}|e_{00}\rangle_E + |01\rangle_{AB}|e_{01}\rangle_E + |10\rangle_{AB}|e_{10}\rangle_E + |11\rangle_{AB}|e_{11}\rangle_E + \Big)$$

Suppose that Alice and Bob can verify that each of their pairs satisfies $X \otimes X = 1 = Z \otimes Z$. If $Z \otimes Z = 1$, then the state must be

$$|\Phi\rangle_{ABE} = \frac{1}{\sqrt{2}}\Big(|00\rangle_{AB}|e_{00}\rangle_E + |11\rangle_{AB}|e_{11}\rangle_E + \Big)$$

And if also $X \otimes X = 1$ then it must be

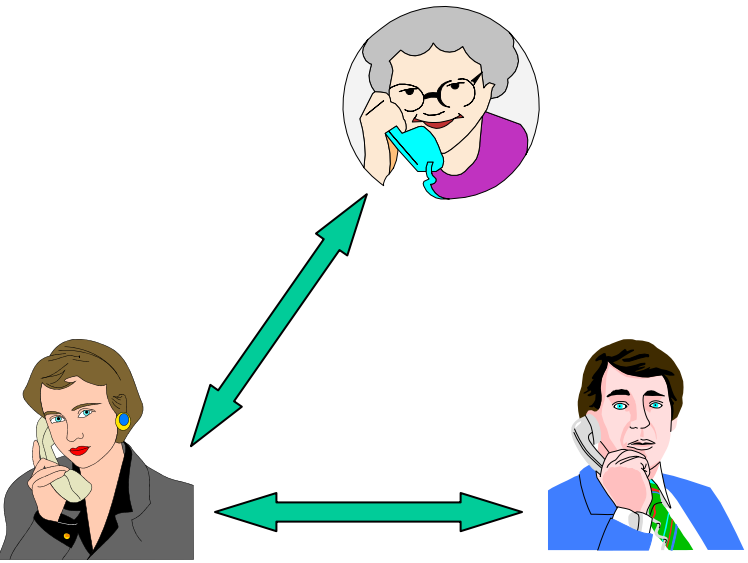
$$|\Phi\rangle_{ABE} = \frac{1}{\sqrt{2}}\Big(|00\rangle_{AB} + |11\rangle_{AB} \Big)|e\rangle_E = |\phi^+\rangle_{AB}|e\rangle_E$$

Thus the pairs are uncorrelated with Eve, and she can't learn anything about the key by measuring her probe!

Entanglement is "Monogamous"

Suppose that Alice and Bob can verify that each of their pairs satisfies $X \otimes X = 1 = Z \otimes Z$. If $Z \otimes Z = 1$, then the state must be

$$|\Phi\rangle_{ABE} = \frac{1}{\sqrt{2}}\left(|00\rangle_{AB} + |11\rangle_{AB}\right)|e\rangle_E = |\phi^+\rangle_{AB}\,|e\rangle_E$$



The more entangled Alice is with Bob, the less entangled she can be with Eve. If Alice and Bob are maximally entangled (share a Bell state) then neither Alice nor Bob can be entangled with Eve at all.

In contrast, if Alice and Bob are only *classically* correlated, there is no limitation on their classical correlations with Eve.

EPR quantum key distribution

$$|\phi^+\rangle_{AB} = \frac{1}{\sqrt{2}}\left(|00\rangle_{AB} + |11\rangle_{AB}\right)$$

How do Alice and Bob *verify* that their pairs are really in the state $|\phi^+\rangle$? They check that $X \otimes X = 1 = Z \otimes Z$ by conducting a statistical test. To generate an n bit key, they start out with $4n(1+\varepsilon)$ pairs. With high probability (if n is large), they measure in the same basis at least $2n$ times (otherwise, they abort the protocol). They randomly choose (say) n bits from these $2n$ bits of *sifted key*, and publicly compare. If all or nearly all of these bits agree, they have high statistical confidence that the remaining n bits were generated by measuring a state that was quite close to $|\phi^+\rangle^{\otimes n}$. (But how close is "close enough"? More on that later…)

BB84 quantum key distribution

(Bennett & Brassard '84)

$$|\phi^+\rangle_{AB} = \frac{1}{\sqrt{2}}\left(|00\rangle_{AB} + |11\rangle_{AB} \right)$$

EPR QKD illustrates that quantum entanglement is a potentially useful resource --- we can exploit it to perform a task that would otherwise be difficult (we can put the weirdness to work). But there is another way to look at the EPR protocol, such that entanglement makes no explicit appearance (and the protocol becomes easier to implement in practice).

Imagine that Alice prepares all of the $|\phi^+\rangle$ pairs herself, keeping half of each pair and shipping the other half to Bob. It would not in any way reduce the efficacy of the protocol if Alice measured X or Z on her half *before* sending off the other half. In effect, then, she prepares (equiprobably) and sends to Bob one of four possible states.

BB84 quantum key distribution

Alice prepares one of four states:

Bob measures either X or Z.

$$Z = 1: \quad |0\rangle = |\uparrow\rangle$$
$$Z = -1: |1\rangle = |\downarrow\rangle$$
$$X = 1: \quad (|0\rangle + |1\rangle)/\sqrt{2} = |\rightarrow\rangle$$
$$X = -1: (|0\rangle - |1\rangle)/\sqrt{2} = |\leftarrow\rangle$$

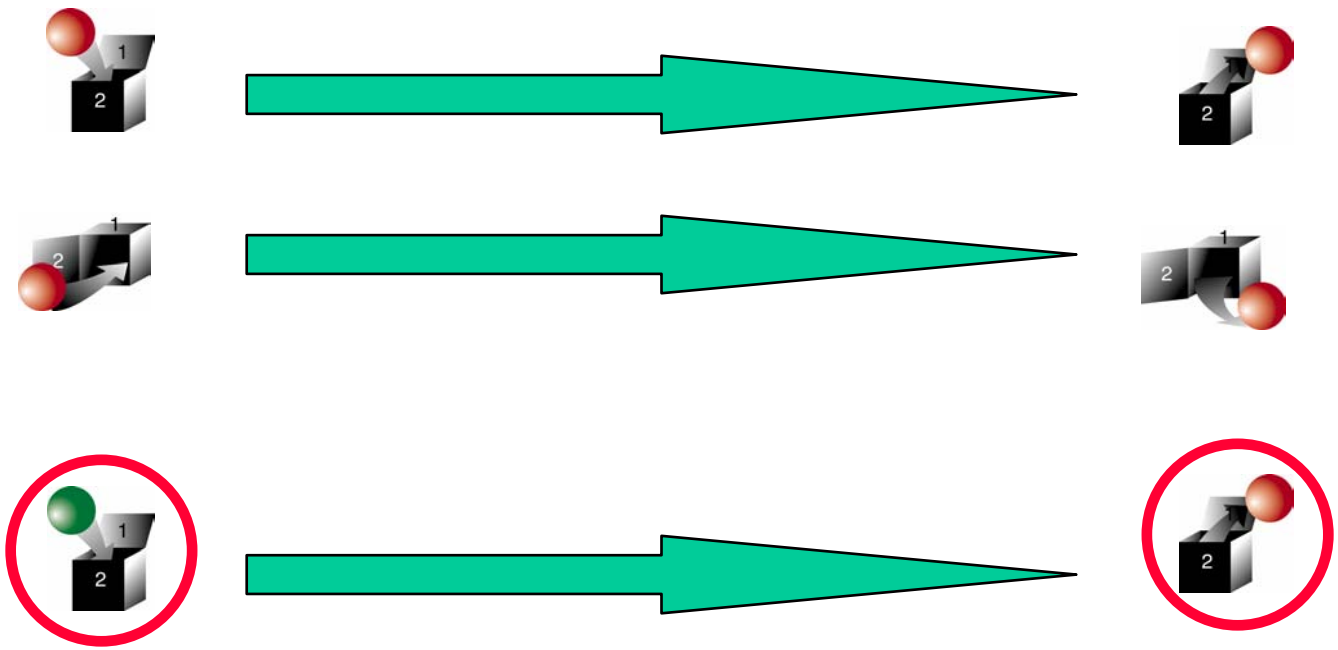
This is called the "four-state protocol" or the "BB84 protocol" (because it was first described by Bennett and Brassard in 1984 --- the idea of quantum cryptography was first conceived by Wiesner in the early '70's, but he was unable to get his work published). BB84 QKD (a "prepare and measure" protocol) is no less secure than EPR QKD which uses quantum entanglement to distribute the key.

Bennett-Brassard '84

Alice

Quantum key distribution, augmented by classical protocols that correct errors and amplify privacy, is *provably* secure against *arbitrary* eavesdropping attacks.

Bob



Alice can use quantum information (qubits) to send a random key to Bob.

Information vs. disturbance

Why is eavesdropping detectable? Because it is not possible to *collect information* that distinguishes among *nonorthogonal* quantum states without creating a detectable disturbance. In contrast, we can distinguish among orthogonal states (read classical information) without leaving any trace.

Consider a game in which Alice prepares either $|\uparrow\rangle$ or $|\rightarrow\rangle$ (chosen at random). Eve is supposed to guess which state Alice prepared. There is no strategy Eve can play that will win the game every time (her optimal probability of success is 85.4%), and no strategy that is better than a random guess leaves the state unmodified.

But if Alice prepares either $|\uparrow\rangle$ or $|\downarrow\rangle$, then Eve can win every time, without disturbing the state at all.

Information vs. disturbance

Suppose Alice prepares either $|\varphi\rangle$ or $|\psi\rangle$. To distinguish the two possible states, Eve performs a unitary transformation that rotates her probe while leaving Alice's state intact

$$U: \quad |\varphi\rangle_A \otimes |0\rangle_E \to |\varphi\rangle_A \otimes |e\rangle_E$$

$$|\psi\rangle_A \otimes |0\rangle_E \to |\psi\rangle_A \otimes |f\rangle_E$$

where $|e\rangle$ and $|f\rangle$ are normalized states. Since U preserves inner products,

$$\langle\psi|\varphi\rangle \cdot \langle f|e\rangle = \langle\psi|\varphi\rangle ,$$

and if $|\varphi\rangle$ and $|\psi\rangle$ are nonorthogonal, then $\langle f|e\rangle = 1$; the states of the probe are indistinguishable. Eve's measurement of the probe cannot reveal any information about whether the state is $|\varphi\rangle$ or $|\psi\rangle$. On the other hand if $|\varphi\rangle$ and $|\psi\rangle$ are orthogonal, the probe states can also be orthogonal. Eve can *copy* the info.

Information vs. disturbance

So we see that it is impossible to collect any information that distinguishes two nonorthogonal states without creating a disturbance. The same principle applies if Eve wants to distinguish the four BB84 states: $|\uparrow\rangle$, $|\rightarrow\rangle$, $|\downarrow\rangle$, $|\leftarrow\rangle$.

This is a powerful argument, but it is not quantitative. What if Eve collects just a little bit of information --- how big a disturbance must she cause? Or if she is permitted to alter the fidelity of the state slightly, how much information can she gain?

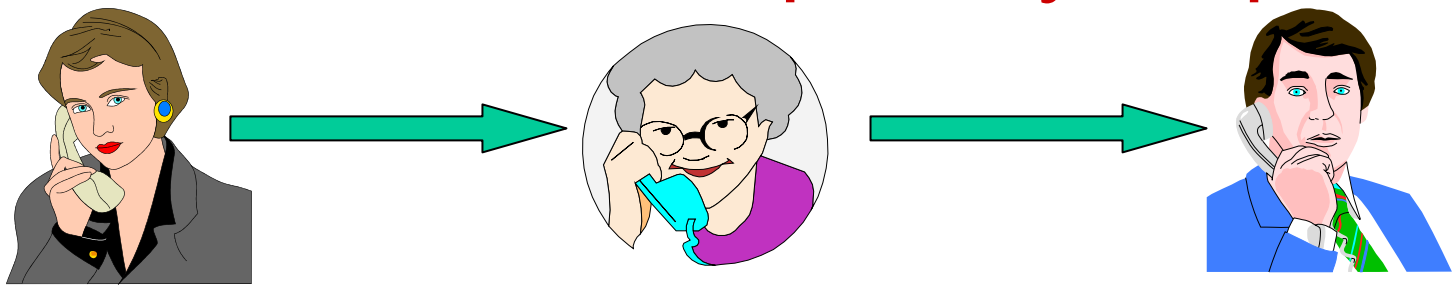
Quantum key distribution provides an excellent setting for studying the information/disturbance tradeoff, which is of fundamental interest in quantum information theory. We have well motivated ways to quantify both information gain and disturbance: what does Eve know about the key, and what error rate do Alice and Bob detect?

BB84 quantum key distribution

In the real world, communication channels (especially quantum channels) are imperfect. Therefore, Alice and Bob can expect to find some errors in their verification test even if Eve has not collected any information at all. Still, when errors occur, they (as cautious cryptologists) should pessimistically assume that the errors were caused by Eve's tampering.

Thus we must enhance the BB84 QKD protocol in two ways. First we should incorporate (classical) *error correction*, to ensure that Alice and Bob really have the same secret key. Second, we should include (classical) *privacy amplification*. After error correction, Alice and Bob agree on n bits about which Eve has only a little information. Then A. and B. both process the bits, extracting $k < n$ bits about which Eve has even less information.

Error correction and privacy amplification



For example, to do error correction, Alice and Bob both divide their private key bits into blocks of three.

(011)(101)(001) → (111)(100)(001)

(Bob's errors are shown in red.) Then Alice announces her "error syndrome": the location of the bit (if any) in each block that differs from the other two. She flips this bit and so does Bob.

(111)(111)(000) → (011)(110)(000)

Now each of Alice's blocks is a codeword of the 3-bit repetition code. Bob decodes his block by majority voting. If there is no more than one error in a block of three, then Bob's decoded bit agrees with Alice's.

(1) (1) (0) (1) (1) (0)

Error correction and privacy amplification

After error correction, Alice and Bob are likely to share the same bits. Next they perform privacy amplification to extract bits that are more secure. For example Alice and Bob might divide their corrected key bits into blocks of three. And in each block compute the parity of the three bits.

$[(1)\,(1)\,(0)]\quad[(0)\,(1)\,(0)]\quad[(1)\,(0)\,(0)]$

$[0]\quad[1]\quad[1]$

If Eve has a little bit of information about each corrected bit, she'll know less about the parity bit of a block.

Security of BB84

To make a precise statement about the security of the BB84 protocol, we consider the asymptotic behavior for very large key length. Then:

Theorem: For *any** attack by Eve, if the bit error rate observed in the verification test is low enough, then Bob's key agrees with Alice's with probability exponentially close to 1 (error correction succeeds), and Eve's information about the key is exponentially small (privacy amplification succeeds).

"Exponentially close/small" can be taken to mean $< \exp(- Ck)$ where k is the length of the final key and C is a constant; Eve's information is the *mutual information* of the key and the outcome of Eve's measurement of her probe. The theorem says that when Alice and Bob accept the key, they both have the same key and Eve knows almost nothing about it.

As cautious cryptologists, we make no assumptions about Eve's technological power. In particular, she might have a quantum computer, enabling her to make collective measurements on all the qubits at once. The security is *information-theoretic*.

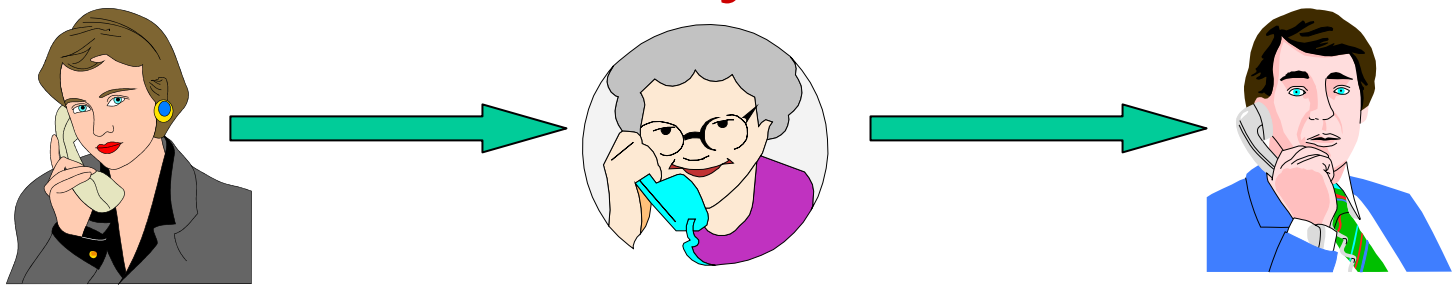
[*that is, any attack that passes the test with nonnegligible probability]

Security of BB84

As cautious cryptologists, we make no assumptions about Eve's technological power. In particular, she might have a quantum computer, enabling her to make collective measurements on all the qubits at once. The security is *information- theoretic*.

This information-theoretic security is sometimes called "unconditional security," meaning that Eve's attack is completely unrestricted. However there are conditions on the equipment used in the protocol --- Alice's source of BB84 states and Bob's detector that measures X or Z. For now we'll suppose that the source and the detector are perfect. More about this later...

Security of BB84



Theorem: For *any** attack by Eve, if the bit error rate observed in the verification test is low enough, then Bob's key agrees with Alice's with probability exponentially close to 1, and Eve's information about the key is exponentially small.

To explain what it means for the verification test to succeed (or fail) we need to specify the maximum error rate $\delta_{\max}$ that Alice and Bob should be willing to tolerate. Furthermore, for $\delta < \delta_{\max}$, we should be able to specify the asymptotic rate $R=k/n$ at which they can extract secure final key from sifted key by choosing appropriate schemes for error correction and privacy amplification.

[*that is, any attack that passes the test with nonnegligible probability]

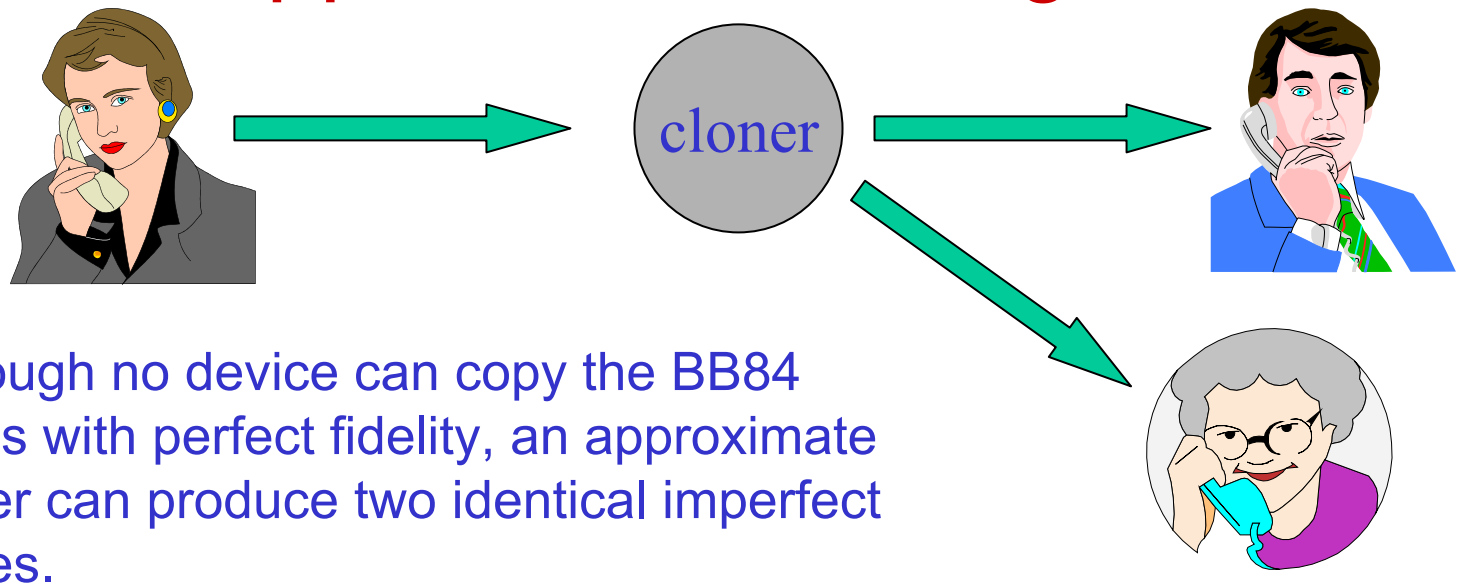
Intercept/resend attack

Suppose that *Eve* intercepts each qubit that Alice sends, deciding at random to measure in the X or Z basis, records the outcome, and then sends on to Bob the X or Z eigenstate found by her measurement.

This is a powerful attack: Alice cannot come to agreement with Bob on a key that Eve does not know. The reason is that, after the bases are announced, Eve can simulate Bob's outcomes (when he measures in a different basis than Eve's) with a random number generator, and Alice can't possibly know more about Bob's key than Eve does.

The intercept/resend attack generates an error rate $\delta = 1/4$; therefore, the maximum tolerable error rate satisfies $\delta_{\max} \leq .25$

Approximate cloning attack



Although no device can copy the BB84 states with perfect fidelity, an approximate cloner can produce two identical imperfect copies.

The optimal approximate cloner for the BB84 ensemble achieves a fidelity of 85.4%. If Eve sends one copy for herself and sends one to Bob, then the bit error rate will be 14.6%.

If the post-processing of the sifted key is achieved with only one-way communication from Alice to Bob, then Eve knows as much as Bob, and $\delta_{\max} \leq .146$. But two-way communication between Alice and Bob breaks the symmetry between Bob and Eve, so that a higher bit-error rate could be tolerable. In fact, for this two-way case, the intercept/resend strategy provides the best currently known upper bound on $\delta_{\max}$.

Bounds on the bit-error rate

The best upper bounds on the acceptable bit-error rate are:

Optimal cloner attack: $\delta_{\text{max,one-way}} \leq .146$
Intercept/resend attack: $\delta_{\text{max, two-way}} \leq .25$

Lower bounds found in proofs of security are:

$$\delta_{\text{max,one-way}} \geq .110$$
$$\delta_{\text{max, two-way}} \geq .189$$

We'll see where the 11% lower bound comes from...

QKD and QEC

In “prepare and measure” QKD, the error correction and privacy amplification applied during post-processing of the sifted key are *classical* protocols. Yet for proving security of e.g. BB84, the theory of *quantum* error correction is very helpful. Why?

QEC: the environment becomes entangled with our qubits. We remove the entanglement and recover a pure state by correcting both X errors and Z errors.

QKD: the eavesdropper collects information about the outcomes of our X and Z measurements by entangling her probe with the transmitted qubits.

QKD and QEC share the goal of protecting quantum states against entanglement with the outside world.

QECC's and the Security of QKD (Shor-Preskill '00)

- A quantum state encoded using a quantum error-correcting code remains pure -- the environment does not become entangled with the encoded quantum information, if the error rate is sufficiently low.

- Suppose that Alice sends to Bob qubits that are protected by a quantum error-correcting code.

- To collect information about the key bits, Eve must become entangled with the encoded state transmitted from Alice to Bob. But if the verification test shows that *quantum error correction will succeed*, then we can disentangle Eve, preventing her from acquiring information about the key. Hence, key distribution using encoded information is secure.

- In general, Alice and Bob need *quantum computers* if Alice is to encode using a QECC, and Bob is to correct the errors and decode the state.

QECC's and the Security of QKD (Shor-Preskill '00)

• But if the QECC is of the *CSS type* [Calderbank-Shor-Steane '96], then bit flip error correction and phase error correction can be separated. Bit flip error correction is needed to ensure the accuracy of the key, but phase error correction has no effect on the key; its purpose is to ensure privacy.

• Thus it is not necessary to *perform* phase error correction -- to ensure privacy, it is enough to know that it would have succeeded *if it had been done*.

• Using such reasoning based on *virtual quantum error correction*, we can prove that the BB84 quantum key distribution scheme, suitably augmented by classical error correction and privacy amplification, is secure against all possible eavesdropping strategies.

• E.g., a bit-error rate up to 11% is acceptable (if classical post-processing involves one-way communication from Alice to Bob).

7-qubit code (a *CSS code*)

One encoded qubit is embedded in the Hilbert space of a block of 7 qubits. The two-dimensional code space is the simultaneously eigenstate of 6 commuting "check operators" (which in principle could be measured simultaneously using a quantum computer). The code can correct one X error and one Z error in the block of 7 qubits.

$$
\begin{aligned}
M_{Z,1} &= Z\ I\ Z\ I\ Z\ I\ Z \\
M_{Z,2} &= Z\ Z\ I\ I\ Z\ Z\ I \\
M_{Z,3} &= Z\ Z\ Z\ Z\ I\ I\ I
\end{aligned}
$$

Corrects the bit-flip (X) errors. The three-bit string $(M_{Z,1}, M_{Z,2}, M_{Z,3})$ (if nonzero) points to the position of the error.

$$
\begin{aligned}
M_{X,1} &= X\ I\ X\ I\ X\ I\ X \\
M_{X,2} &= X\ X\ I\ I\ X\ X\ I \\
M_{X,3} &= X\ X\ X\ X\ I\ I\ I
\end{aligned}
$$

Corrects the phase (Z) errors. The three-bit string $(M_{X,1}, M_{X,2}, M_{X,3})$ (if nonzero) points to the position of the error.

The $\boldsymbol{M_Z}$'s commute with the $\boldsymbol{M_X}$'s , because each row of the $\boldsymbol{M_Z}$ matrix has an even number of "collisions" with each row of the $\boldsymbol{M_X}$ matrix; the bit-flip and phase error correction can be executed separately. The encoded operations can be chosen to be $\overline{Z} = I\ I\ I\ I\ Z\ Z\ Z$, $\overline{X} = I\ I\ I\ I\ X\ X\ X$ which commute with the check operators and are independent of them.

EPR QKD using the 7-qubit code

Alice and Bob share 7 EPR pairs, but the pairs are *noisy* (have imperfect fidelity). The noise could be due to tampering by Eve. Let's *assume* (for now) that the effect of Eve's tampering is first to apply X to at most one of Bob's 7 qubits and then to to apply Z to at most one (possibly the same one).

Alice measures the 3 Z check operators of the 7-qubit code: $(M_{Z,1}, M_{Z,2}, M_{Z,3})$, and if she finds a nontrivial syndrome, she applies X to the qubit identified by the syndrome. She reports her recovery operation to Bob, and he applies X to his corresponding qubit. Then Bob measures the 3 Z check operators and recovers again --- in this step he reverses the X error (if any) that Eve introduced. Alice and Bob then repeat this procedure for the 3 X check operators $(M_{X,1}, M_{X,2}, M_{X,3})$.

The state that Alice and Bob have obtained is the encoded EPR pair $|\bar{\phi}\rangle_{AB}$ with perfect fidelity (Eve is unentangled with the encoded state). Alice and Bob can now each measure the encoded operation $\bar{Z}$ to generate a secure bit. Alice and Bob managed to "purify" their noisy entanglement, extracting perfect entanglement that could then be used to generate the key.

EPR QKD using the 7-qubit code

So far, we have considered a protocol for which Alice and Bob need quantum computers to measure the collective obervables $(M_{Z,1}, M_{Z,2}, M_{Z,3})$ and $(M_{X,1}, M_{X,2}, M_{X,3})$. This was necessary for them to be able to implement correction of both the X errors and the Z errors.

But Alice and Bob generate the key bit by measuring $\overline{Z} = I\ I\ I\ I\ Z\ Z\ Z$ ... So there is no need to correct the Z errors --- they have no effect on the key. And if we don't correct these errors, there is no need to measure the check operators $(M_{X,1}, M_{X,2}, M_{X,3})$ that diagnose the Z errors.

What remains of our protocol? Alice and Bob measure $(M_{Z,1}, M_{Z,2}, M_{Z,3})$ and $\overline{Z}$, and Bob applies an error-correcting bit flip (if necessary) to make sure that his $\overline{Z}$ agrees with Alice's.

The reduced protocol is almost entirely classical: Alice prepares and sends bits (Z eigenstates) to Bob. Errors might occur in transit, which Bob corrects. Alice and Bob compute the parity of the last three key bits to determine one bit of their final key. *If* at most one of the qubits suffers an X error in the channel and at most one suffers a Z error, then Alice and Bob agree on the final key bit and Eve knows nothing about it.

QECC's and the Security of QKD

If the QECC is of the *CSS type*, then bit flip error correction and phase error correction can be separated. Bit flip error correction is needed to ensure the accuracy of the key, but phase error correction has no effect on the key; its purpose is to ensure privacy.

When we reduce an EPR protocol to a "prepare and measure" protocol, a vestige of the QECC survives in the classical procedures we use to correct bit errors and amplify privacy. The power of the CSS code to correct X errors ensures that Alice and Bob have the same key bits. The power of the CSS code to correct Z errors ensures that Eve does not know the value of the *encoded* Z.

By testing many pairs (where Eve doesn't know in advance which pairs are used in the test and which are used to generate key), Alice and Bob can estimate the rates of X errors and Z errors, and then use a code that corrects the errors with high probability. Thus, in BB84, error correction and privacy amplification will succeed.

Key generation rate

To determine the rate at which Alice and Bob can extract secure final key from their sifted key, we consider the asymptotic *rates* of CSS codes with large block size (the number of encoded qubits divided by the block size). Recall Shannon's result for a classical bit flip channel: If n bits are transmitted with the bit error rate δ, then nR bits can be encoded with negligible error probability, where the achievable rate R is:

$$R = 1 - H_2(\delta), \quad H_2(\delta) = -\delta \log \delta - (1-\delta)\log_2(1-\delta)$$

Heuristically, there must be more than enough error syndromes to point to each of the typical errors, or:

$$\binom{n}{n\delta} \approx 2^{nH_2(\delta)}$$

We need to sacrifice a fraction $H_2(\delta)$ of the bits to correct errors.

In the case of CSS quantum codes, we need to sacrifice a fraction $H_2(\delta)$ of our qubits to correct bit flips and also a fraction $H_2(\delta_p)$ to correct phase flips, where δ_p is the phase error rate; thus he achievable rate for CSS codes is:

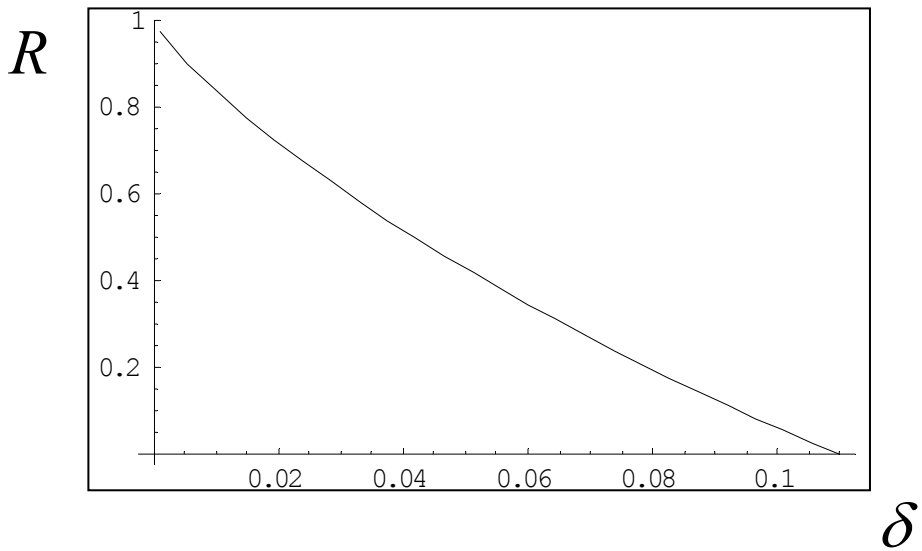
$$R = 1 - H_2(\delta) - H_2(\delta_p)$$

And if Eve has no information about what basis is used, the bit errors and phase errors occur at the same rate: $\delta = \delta_p$.

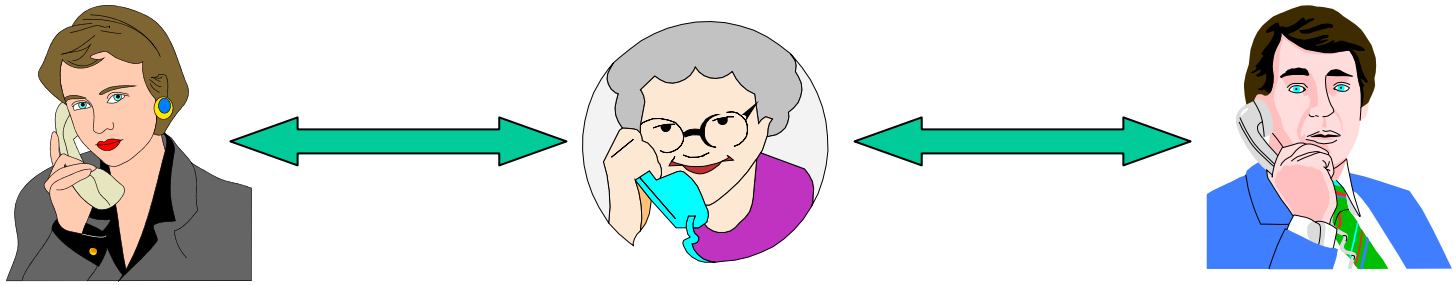
Security of BB84

Theorem: For *any* attack by Eve [such that the verification test succeeds with nonnegligible probability], if the test succeeds then Bob's key agrees with Alice's with probability exponentially close to 1, and Eve's information about the key is exponentially small. Secure final key can be extracted from sifted key at the asymptotic rate: $R = \mathrm{Max}\left(1 - 2H_2(\delta), 0\right)$ where δ is the bit error rate found in the verification test.

This rate hits zero for $\delta = .1100$.



Man-in-the-middle attack



The security of QKD could be threatened if Eve impersonates Bob when talking to Alice and impersonates Alice when talking to Bob (the “man-in-the-middle attack”).

Fortunately, there is an information-theoretically secure classical protocol that allows Alice and Bob to *authenticate* their classical communication, i.e., to verify that they are really talking to one another. Unfortunately, though, to carry out this protocol, Alice and Bob need to share a secret random key to begin with. This is a quandary: Alice and Bob need a secret key to generate a secret key using QKD!

Fortunately, the key generated in the QKD protocol is much longer than the key consumed by the authentication protocol. Quantum key *distribution* might better be called quantum key *expansion*: with a short seed key, Alice and Bob generate a long key. Later, they can use a short portion of the long key to authenticate another round of QKD, etc.

QKD for sale!

Quantum key distribution is *commercially available*:

Quantum Security... at last

Quantum Key Distribution System

Key distribution over optical fiber with absolute security

Main features

- First quantum cryptography system
- Security guaranteed by quantum physics
- Point-to point key distribution
- Standard optical fiber
- Distances up to 70 km
- Key rate up to 1000 bits/s
- Compact and reliable

Key distribution is a central problem in cryptography. Currently, public key cryptography is commonly used to solve it. However, these algorithms are vulnerable to increasing computer power. In addition, their security has never been formally proven.

Quantum cryptography exploits a fundamental principle of quantum physics - observation causes perturbation - to distribute cryptographic keys with absolute security.

id Quantique is introducing the first quantum key distribution system. It consists of an emitter and a receiver, which can be connected to PC's through the USB port.

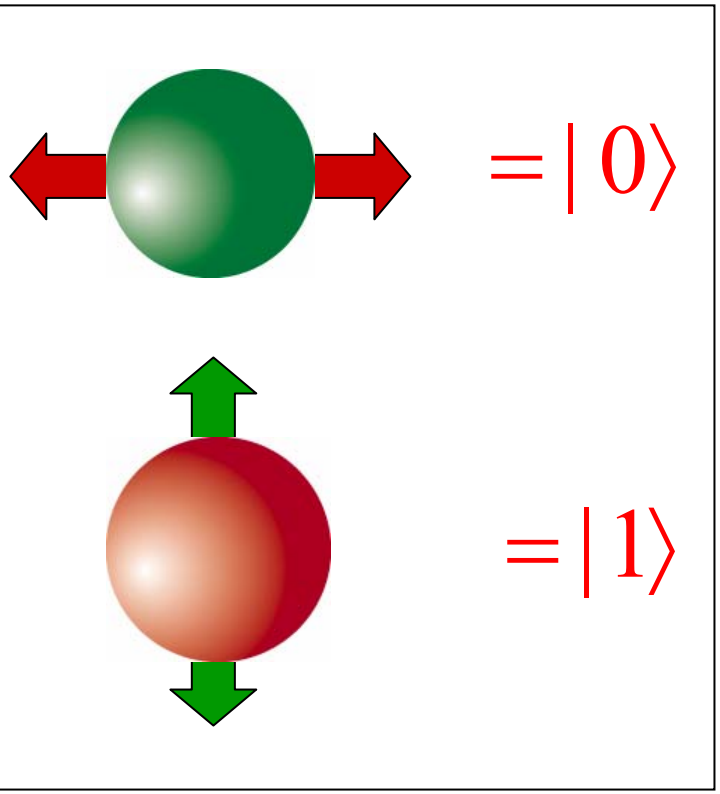
id Quantique

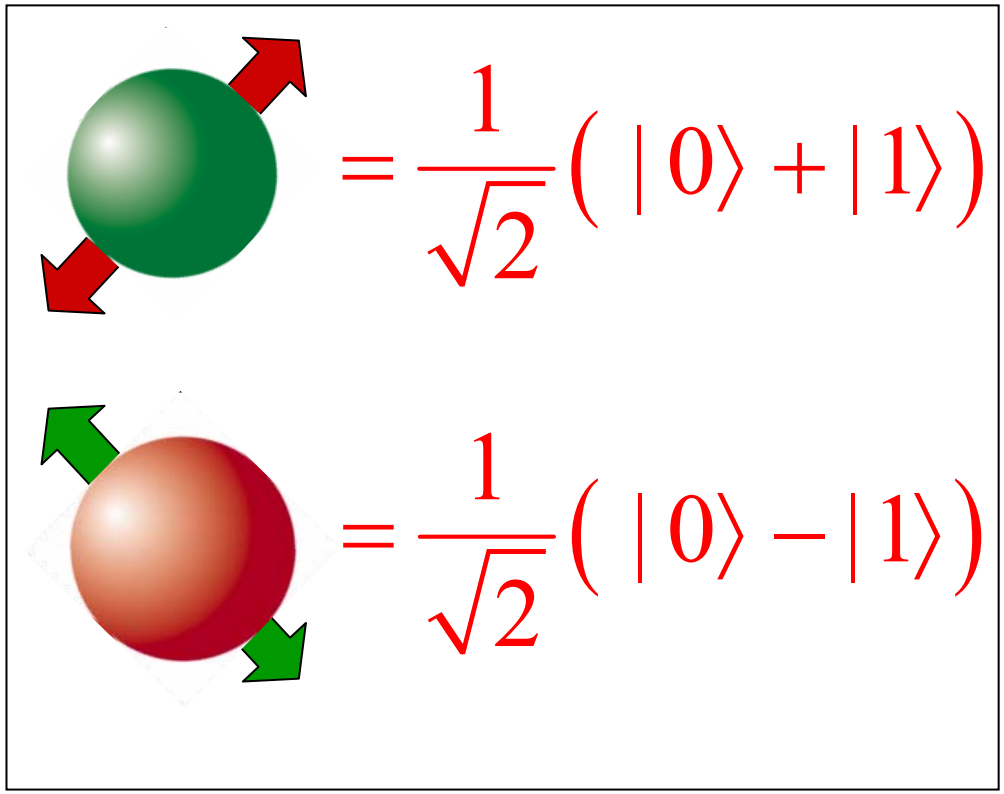
10, rue Cingria 1205 Genève Switzerland
Tel: (+41) 022 702 69 29 Fax: (+41) 022 781 09 80
email: info@idquantique.com
web: http://www.idquantique.com

id Quantique
A Quantum Leap for Cryptography

Quantum key distribution is *commercially available*.

Single photons as qubits

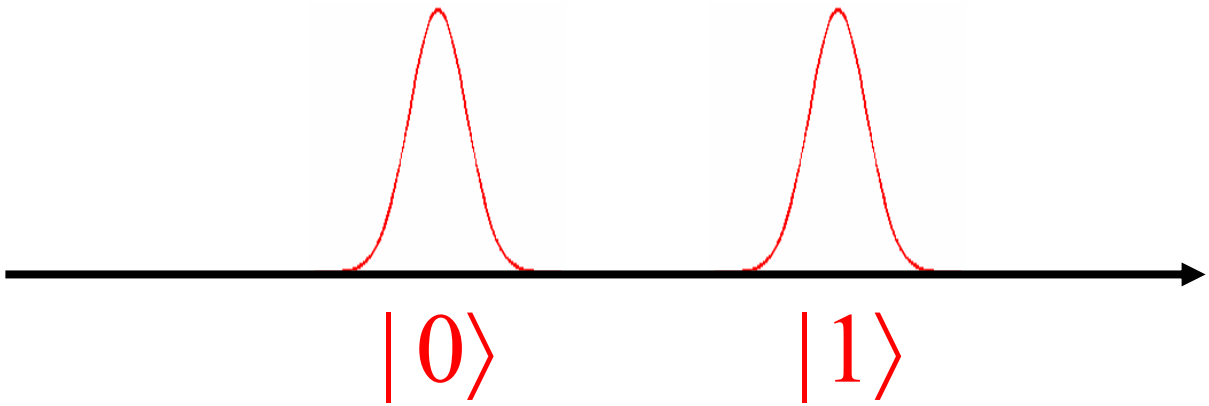




In realistic settings, the BB84 states are usually “single-photon” states transmitted through optical fibers. In principle, the qubit could be encoded in the photon polarization (“polarization encoding”). In practice, because of limitations arising from birefrigence in fibers, typically a qubit is encoded in a relative phase that is detected interferometrically.

Single photons as qubits

Alice



Bob

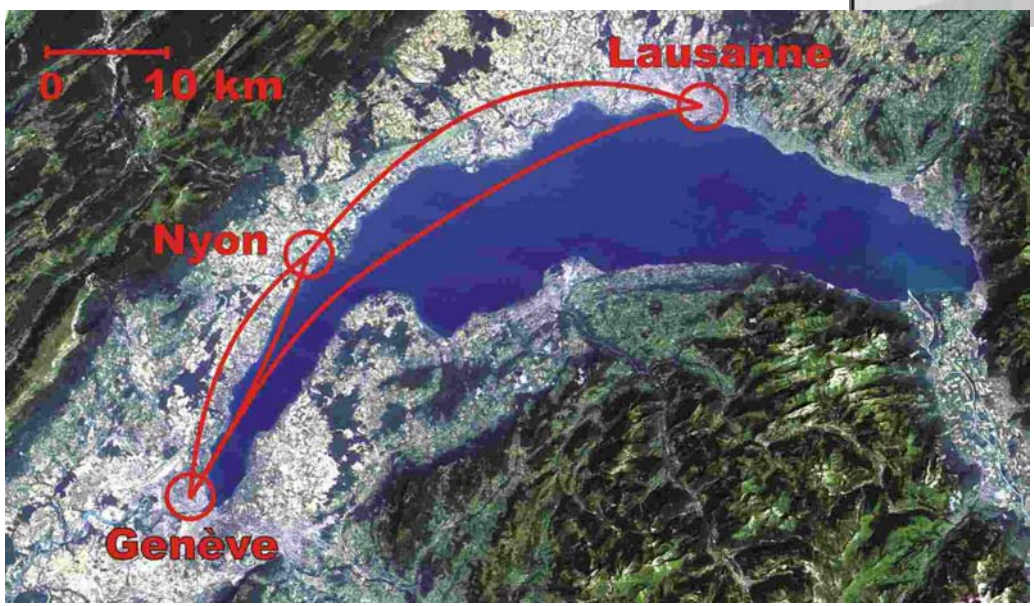
In practice, because of limitations arising from birefrigence in fibers, typically a qubit is encoded in the relative phase of a superposition of two single photon states in distinguishable modes ("phase encoding"). In the optical fiber the two modes are well separated spatially compared to the pulse width, and the relative phase can be measured using an (unbalanced) Mach-Zehnder interferometer, with photon detectors at each output port. The four BB84 signal states can be chosen to be:

$$\frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) \qquad \frac{1}{\sqrt{2}}\left(|0\rangle + i|1\rangle\right)$$

$$\frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right) \qquad \frac{1}{\sqrt{2}}\left(|0\rangle - i|1\rangle\right)$$

QKD for sale!

Quantum key distribution is *commercially available*:



For example, BB84 QKD has been achieved through a 67 km optical fiber under Lake Geneva.

Security of “realistic” QKD

Sources of single photons are under development but are not readily available and are not used in current QKD systems. Instead, weak coherent states are used:

$$|\alpha\rangle = e^{-|\alpha|^2/2} e^{\alpha a^\dagger} |0\rangle \approx e^{-|\alpha|^2/2} \left(|0\rangle + \alpha |1\rangle + \left(\alpha^2 / \sqrt{2} \right) |2\rangle \right)$$

For small α, the signal is usually the vacuum, occasionally a single photon, and more rarely two or more photons.

If e.g. polarization encoding is used for key distribution, and a multiphoton state is sent, security may be compromised. Eve can skim off the extra photon(s), wait until Alice and Bob announce their bases, and then measure in the correct basis, obtaining perfect polarization information at no cost in disturbance. Our privacy amplification scheme must be sufficiently powerful (and the coherent states sufficiently weak), to nullify this advantage.

Security of "realistic" QKD

$$|\alpha\rangle = e^{-|\alpha|^2/2} e^{\alpha a^\dagger} |0\rangle \approx e^{-|\alpha|^2/2} \left(|0\rangle + \alpha |1\rangle + \left(\alpha^2 / \sqrt{2} \right) |2\rangle \right)$$

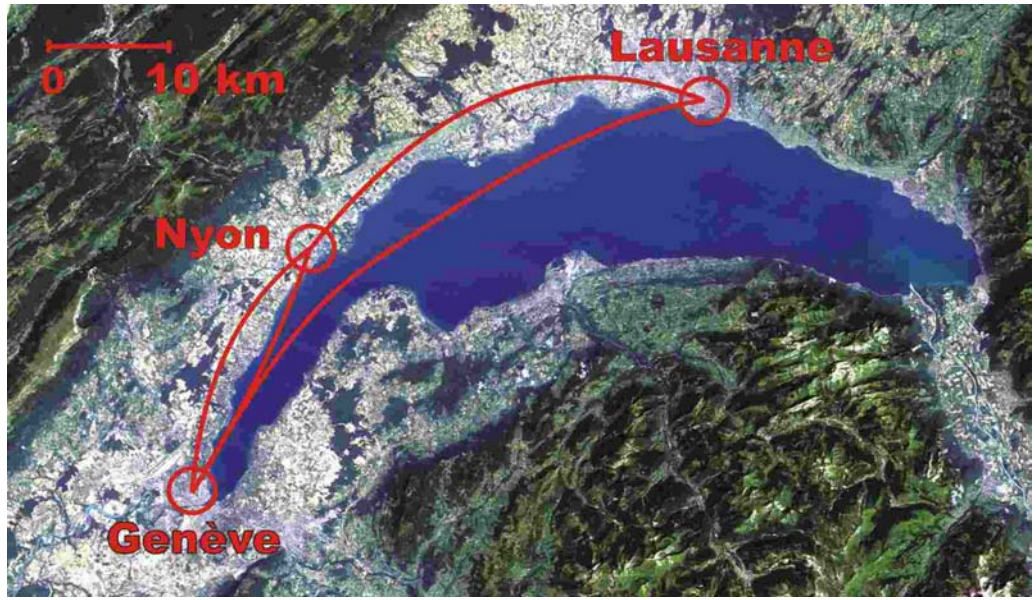
For small α, the signal is usually the vacuum, occasionally a single photon, and more rarely two or more photons.

Security *can* still be proven for imperfections like this one that leak some information to Eve about what basis is used to generate the key, as long as the leaked information can be bounded in some way (Gottesman-Lo-Lütkenhaus-Preskill '04).

In the case of (phase-randomized) weak coherent states, it suffices to bound the error rate for the single photon signals, which can be extracted by sending "decoy pulses" of modulated strength α. Secure key distribution is possible with existing detectors up to a range over 100 km (Lo-Ma-Chen '04) --- at longer range, pulses are so attenuated the detectors are overwhelmed by dark counts.

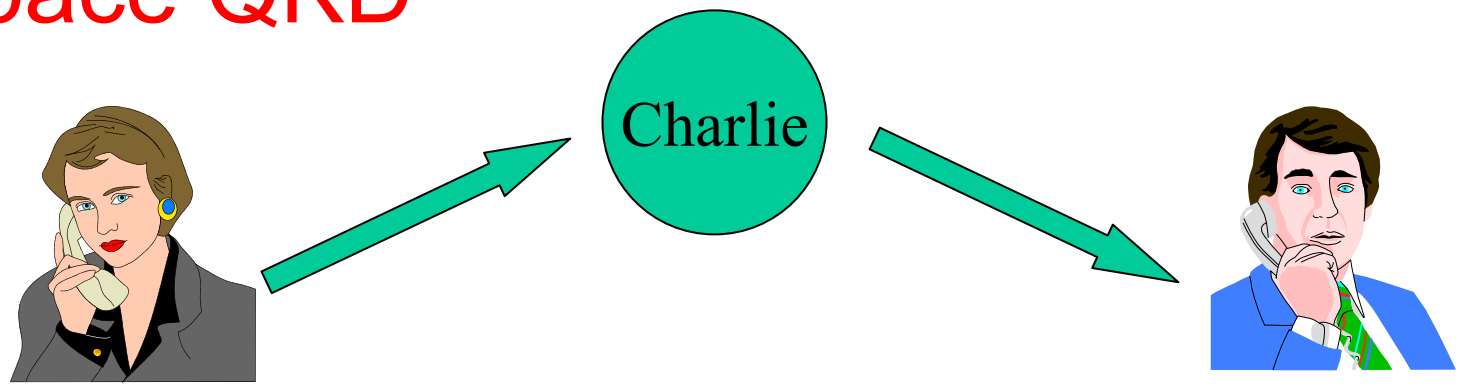
Quantum repeaters?

For example, BB84 QKD has been achieved through a 67 km optical fiber under Lake Geneva.



Today, the range of quantum key distribution is limited by absorption in optical fibers. Optical fiber used for classical communication comes equipped with repeaters that amplify signals, but the unknown signal states in e.g. BB84 cannot be amplified. What is needed are repeaters that use quantum error correction to protect encoded qubits from the effects of absorption. This could be a useful application for "intermediate scale" quantum computers that are powerful enough to implement quantum error recovery protocols.

Free-space QKD



Using spectral, temporal, and spatial filtering, QKD can be executed by sending photons through the atmosphere in broad daylight! This has been achieved in Los Alamos, with sender and receiver on separate mesas, 10 km apart.

It should be feasible to do QKD between a party on the ground and a satellite in low earth orbit. If the satellite (Charlie) can be regarded as a trusted intermediary, it can generate key k_A shared with Alice and key k_B shared with Bob, and then announce $k_{AB=} k_A \oplus k_B$, from which Bob can recover $k_{A=} k_{AB} \oplus k_B$.

Security of quantum cryptography

- Public key cryptography is *vulnerable* to quantum attack.
- Eavesdropping on *quantum* signals can be detected.
- Key generated from high-fidelity entangled states is *private*.
- Using quantum error correction, high-fidelity entanglement can be *distilled* from noisy entanglement.
- "Prepare and measure" quantum key distribution, augmented by error correction and privacy amplification is *secure* (against *any* attack) if the bit error rate is low enough.
- Security is *robust* against small equipment imperfections.
- Quantum technologies are available *today*.
- And … I *didn't* talk about many other (theoretical) frontiers in quantum cryptography: digital signatures, coin flipping, data hiding, etc.