Secure quantum key distribution with an uncharacterized source

M. Koashi and J. Preskill, “Secure quantum key distribution with an uncharacterized source,” quant-ph/0208143.

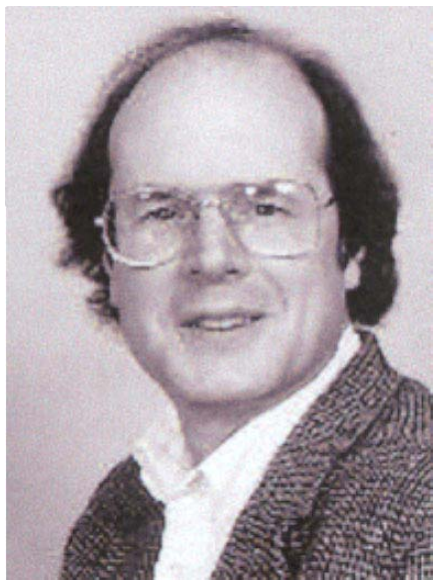
D. Gotttesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, “Security of quantum key distribution with imperfect devices,” quant-ph/0212066.

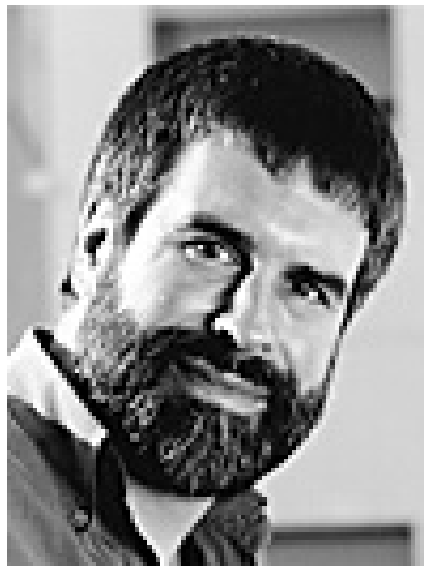
John Preskill, Caltech

16 December 2002

http://www.iqi.caltech.edu/

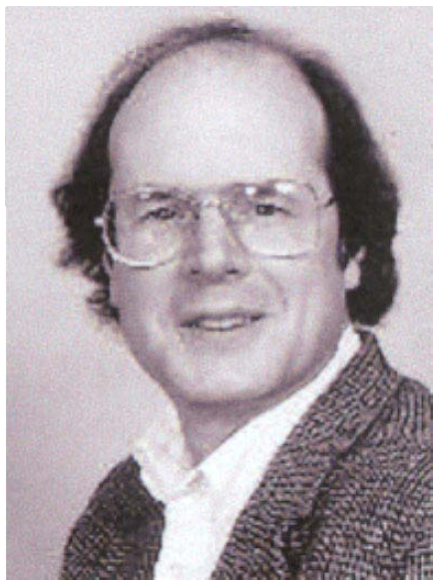
Quantum Cryptography

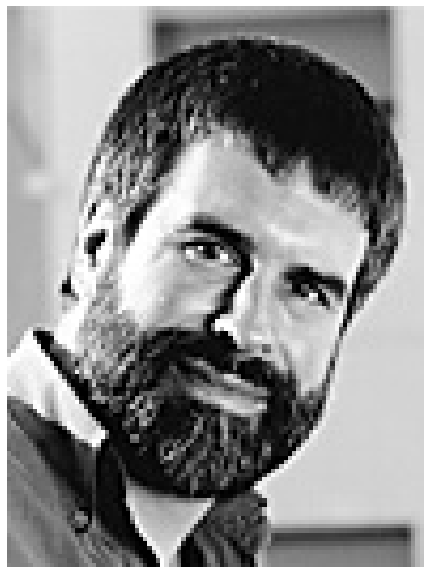




Bennett Brassard ’84

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.

Security of quantum key distribution

The "*unconditional security*" (security against arbitrary eavesdropping attacks) of the BB84 quantum key distribution scheme has been known since [Mayers '96], and is now widely understood. Perhaps the great challenges at the frontier of the theory of quantum cryptography now lie elsewhere. Why should security issues in QKD continue to attract attention?

Security proofs are premised on assumptions about the performance of the equipment used in the protocol. For both conceptual and practical reasons, it is useful to clarify and weaken these assumptions.

Security of quantum key distribution

- The security of QKD provides a fascinating setting for exploring quantitatively the tradeoff between information gain and disturbance of a quantum state, a fundamental feature of quantum information.
- Unlike other proposed quantum technologies, QKD is practical today!
- It is desirable to narrow the gap between the concept of quantum key distribution (simple and beautiful) and the security proofs (somewhat technical). Techniques developed for this purpose may be applicable in other contexts.

QKD for sale!

"Plug and play" 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

Security of quantum key distribution

- Mayers ’96: Perfect source and arbitrary uncharacterized detector. (Detector flaws do not effect rate of generation of final key from sifted key.)
- Shor-Preskill ’00: Applies if flaws in source and detector can be absorbed into Eve’s (basis-independent) attack.
- Inamori-Lütkenhaus-Mayers ’01: (Phase randomized) weak coherent states and uncharacterized detector.
- Koashi-Preskill ’02: Perfect detector and uncharacterized source (emitted states, averaged over key bit, are independent of the basis used).
- Gottesman-Lo-Lütkenhaus-Preskill ’02: Generic small flaws in source and detector, controlled by adversary. (Key generation rate is reduced by the flaws.)
- Ben-Or: QIP ’03.

Security of quantum key distribution

We will concentrate here on the proof of security for an *uncharacterized source*, which uses a new method (largely, it is a melding of ideas from Mayers ’96 and Shor-Preskill ’00).

Using the same (easy!) method, we can prove security in the case of an *uncharacterized detector,* recovering a somewhat strengthened version of the result of Mayers ’96 (a more general source and a higher rate of key generation).

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

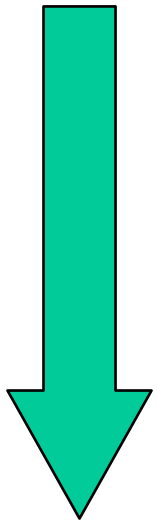
00111100 11110001 00100101 11101011 00010011 00110110

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

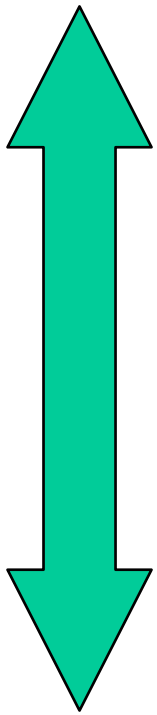
Alice

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

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.

BB84 quantum key distribution

Alice prepares one of four states:

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

Bob measures either X or Z.

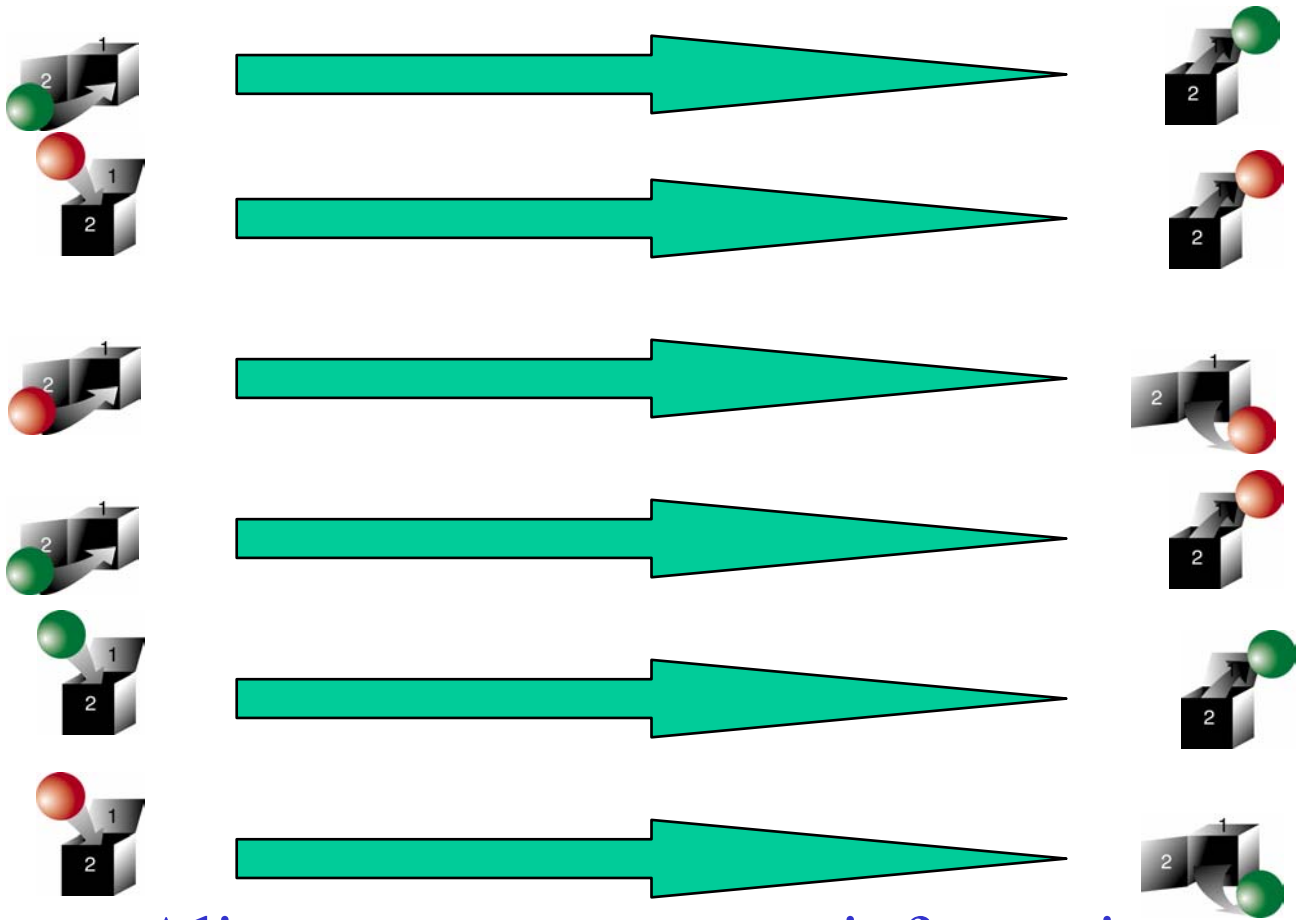
$$Z = 1: \quad |0\rangle = |\uparrow\rangle$$
$$Z = -1: |1\rangle = |\downarrow\rangle$$
$$X = 1: \quad (|0\rangle + |1\rangle)/\sqrt{2} = |\rightarrow\rangle$$
$$X = -1: (|0\rangle - |1\rangle)/\sqrt{2} = |\leftarrow\rangle$$

1) Alice sends a one-qubit signal, choosing a random basis (X or Z), and a random eigenvalue (+1 or -1).
2) Bob measures in a randomly chosen basis (X or Z).
3) Through public discussion, Alice and Bob discard the results in the cases where they used different bases, retaining the rest.

Thus, Alice and Bob generate a shared random string.

Alice

Bob

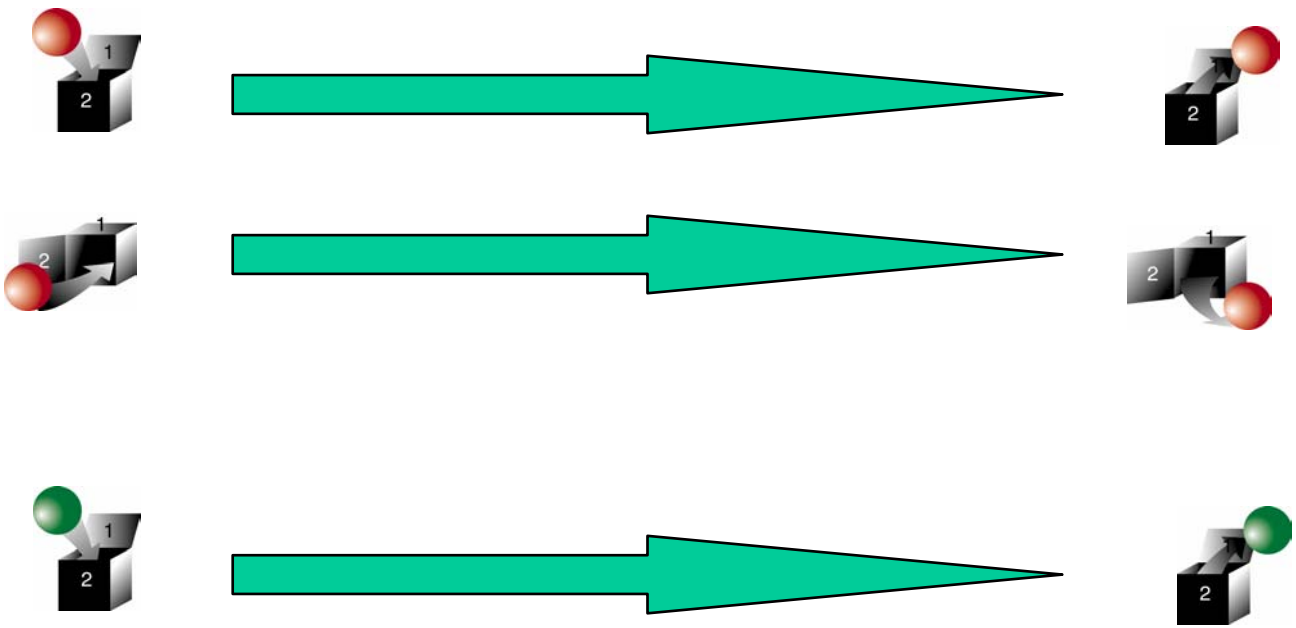


Alice can use quantum information (qubits) to send a random key to Bob.

Eve

Alice

Bob

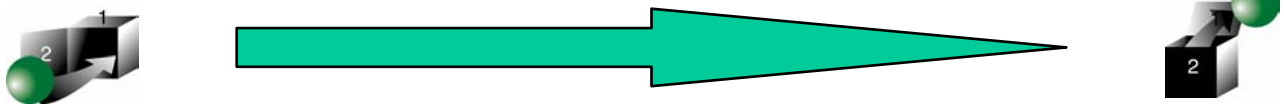


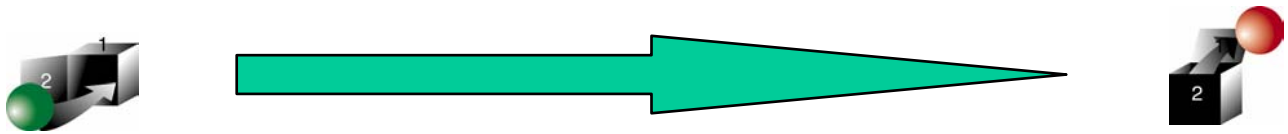
Alice can use quantum information (qubits) to send a random key to Bob.

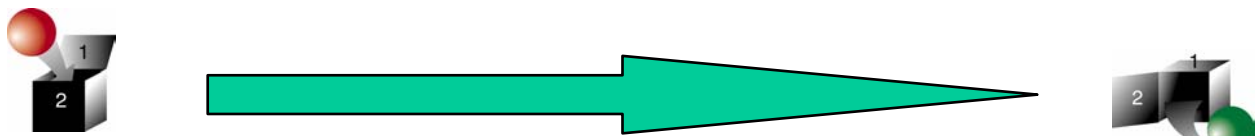
Eve

Alice

Bob







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

Eve

Quantum News

"Spooky action at a distance"

January 15, 1997 Volume 1, Issue 1

Alice Announces Doors She Used!!

Alice

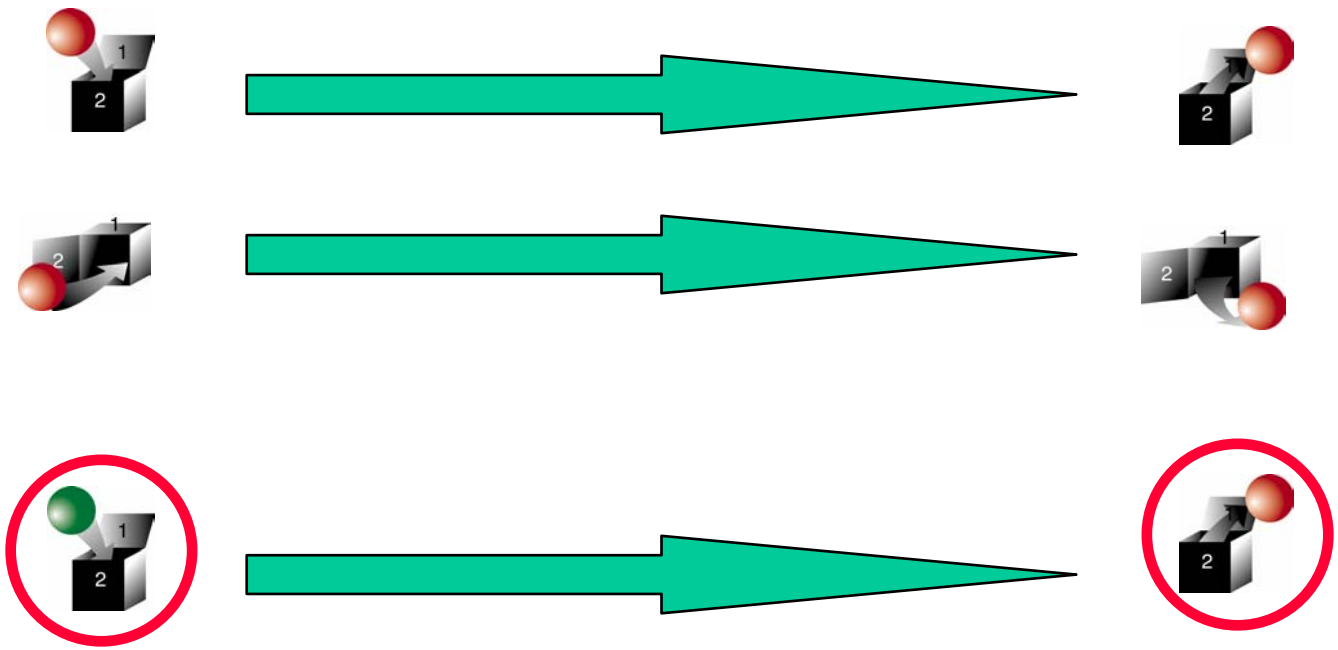
Lorem ipsum dolor sit amet, consectetuer adipiscing elit, sed diem nonummy nibh euismod tincidunt ut lacreet dolore magna aliguam erat volutpat. Ut wisis enim ad minim veniam, quis nostrud exerci tution ullamcorper suscipit lobortis nisl ut aliquip ex ea commodo consequat. Duis te feugifacilisi. Duis autem dolor in hendrerit in vulputate velit esse molestie consequat, vel illum dolore eu feugiat nulla facilisis at vero eros et accumsan et iusto odio dignissim qui blandit praesent luptatum zzril delenit au gue duis dolore te feugat nulla facilisi. Ut wisi enim ad minim veniam, quis nostrud exerci taion ullamcorper suscipit lobortis nisl ut aliquip ex en commodo consequat. Duis te feugifacilisi.per suscipit lobortis nisl ut aliquip ex en commodo consequat. Duis te feugifacilisi. Lorem ipsum dolor sit amet, consectetuer adipiscing elit, sed diem nonummy nibh euismod tincidunt ut lacreet dolore magna aliguam erat volutpat. Ut wisis enim ad minim veniam, quis nostrud exerci tution ullamcorper suscipit lobortis nisl ut aliquip ex ea commodo consequat. Duis te feugifacilisi. Duis autem dolor in hendrerit in vulputate velit esse molestie consequat, vel illum dolore eu feugiat nulla facilisis at vero eros et accumsan et iusto odio dignissim qui blandit praesent luptatum zzril delenit au gue duis dolore te feugat nulla facilisi.ipsum dolor sit amet, consectetuer adipiscing elit, sed diem nonummy nibh euismod tincidunt ut lacreet dolore magna aliguam erat volut-

Lorem ipsum dolor sit amet, consectetuer adipiscing elit, sed diem nonummy nibh euismod tincidunt ut lacreet dolore magna aliguam erat volutpat. Ut wisis

Lorem Ipsum

Alice

Bob

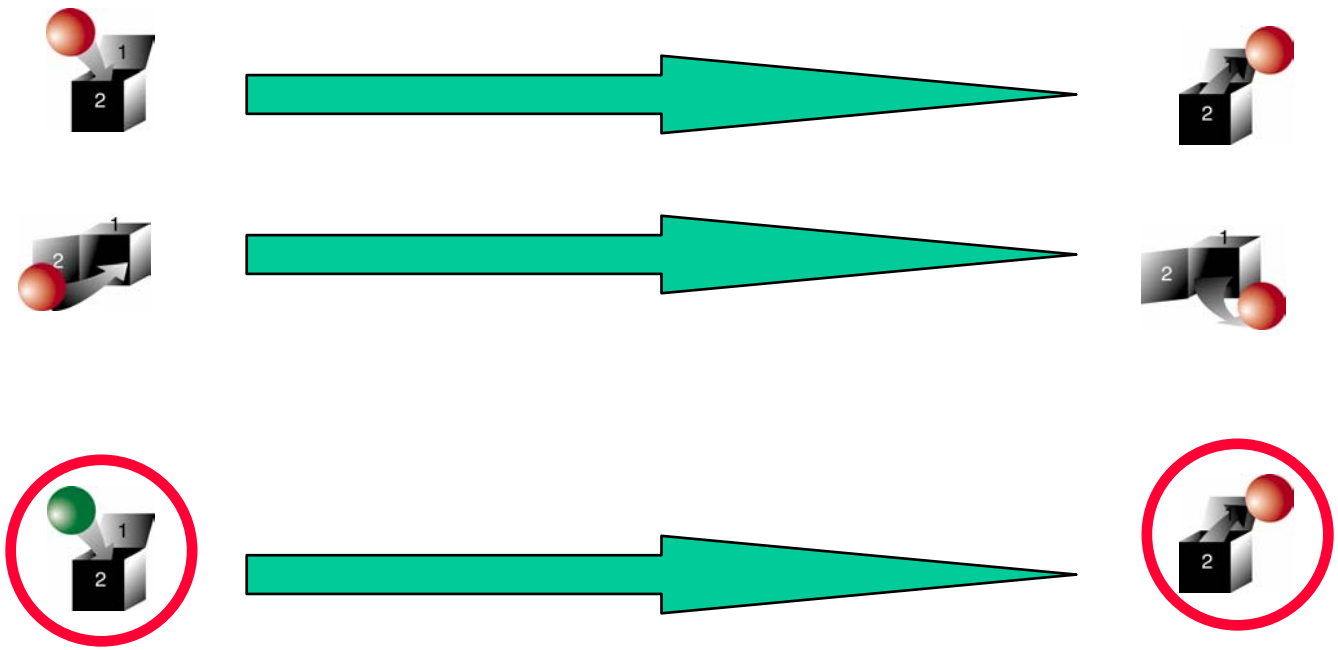


Alice can use quantum information (qubits) to send a random key to Bob.

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

The protocol works because: it is impossible to collect any information that distinguishes the nonorthogonal states $|\uparrow\rangle$, $|\rightarrow\rangle$, $|\downarrow\rangle$, $|\leftarrow\rangle$ without creating a disturbance.

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?

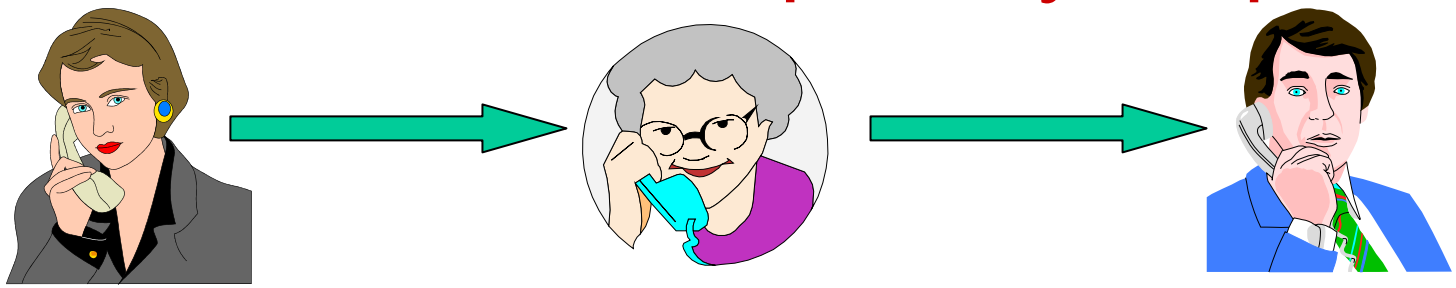
Quantum key distribution provides an excellent setting for studying the information/disturbance tradeoff, which is of fundamental interest in quantum information theory. We have well motivated ways to quantify both information gain and disturbance: what does Eve know about the key, and what error rate 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 $r < n$ 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 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 (such that the verification test succeeds with probability that is not exponentially small), if Alice and Bob accept the key then Bob's key agrees with Alice's with probability exponentially close to 1, the key is nearly uniformly distributed, and Eve's information about the key is exponentially small.

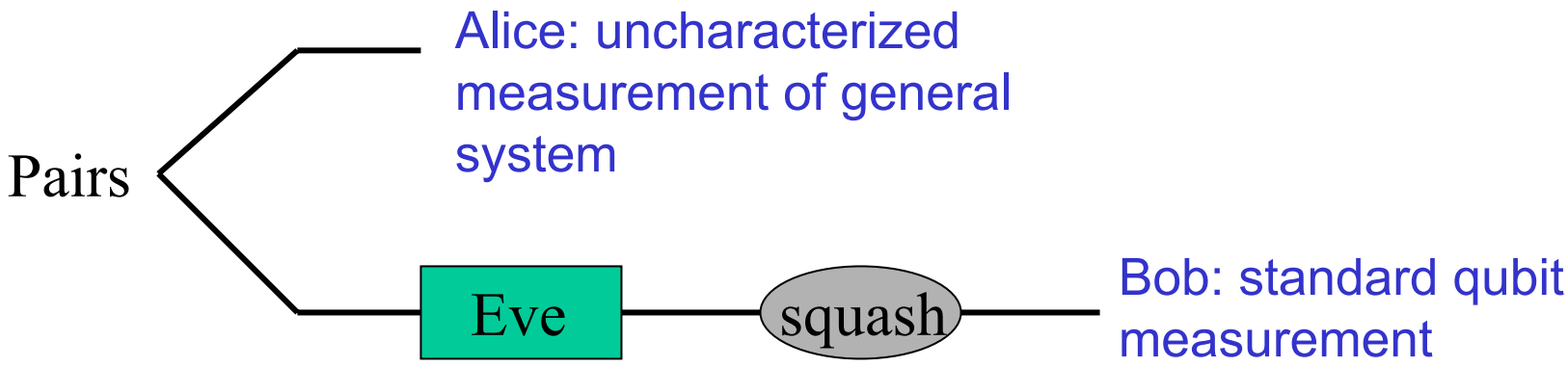
"Exponentially close/small/near" can be taken to mean $< \exp(-\alpha r)$ where r is the length of the final key and α is a constant; Eve's information is the mutual information of the key and the outcome of Eve's measurement of her probe. Informally, the theorem says that if Alice and Bob don't catch Eve (and abort the protocol) then Eve almost certainly knows almost nothing.

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.

Key distribution scenarios

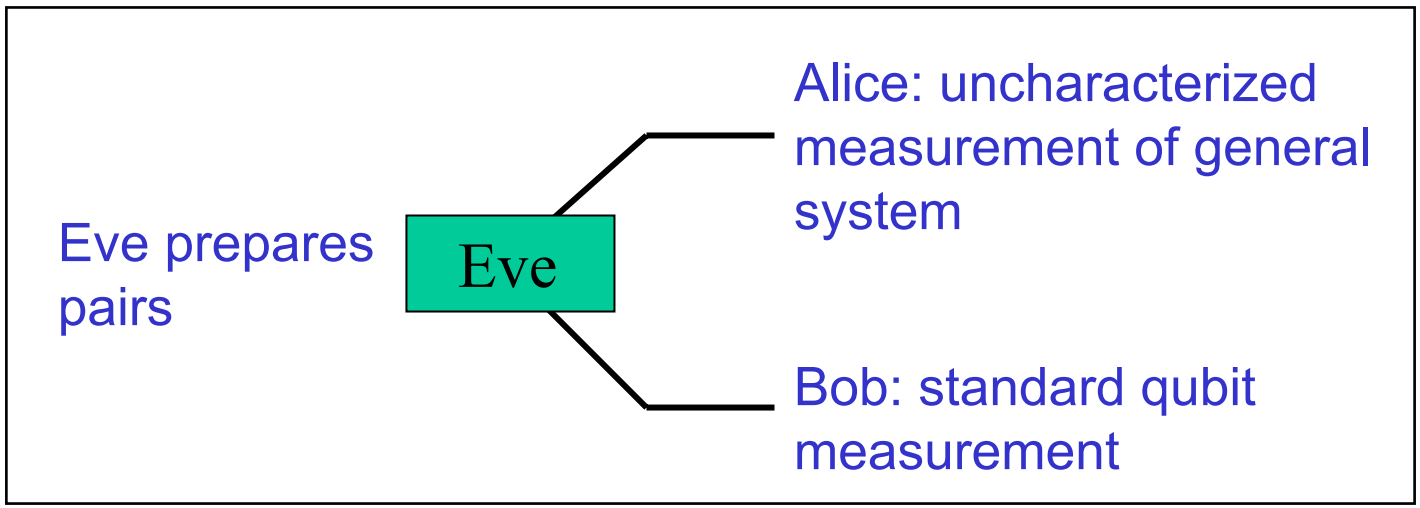


What does Eve know about Bob's key?

What does Eve know about Alice's key?

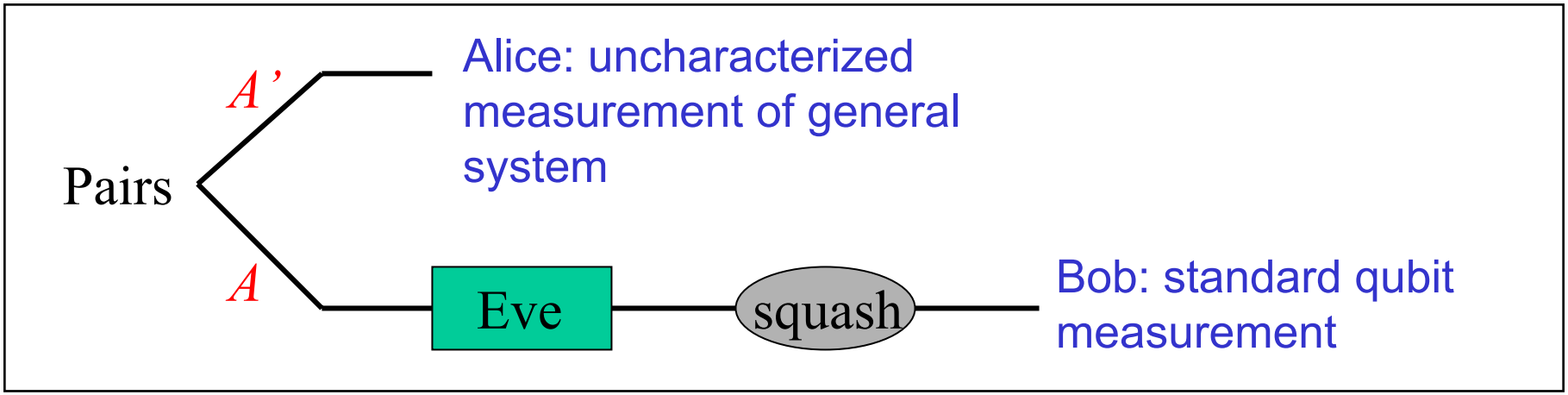
Key distribution scenarios

Security for either an uncharacterized source or an uncharacterized detector follows from security of a protocol in which Eve distributes pairs to Alice and Bob, where Alice receives a general system, and Bob receives a qubit



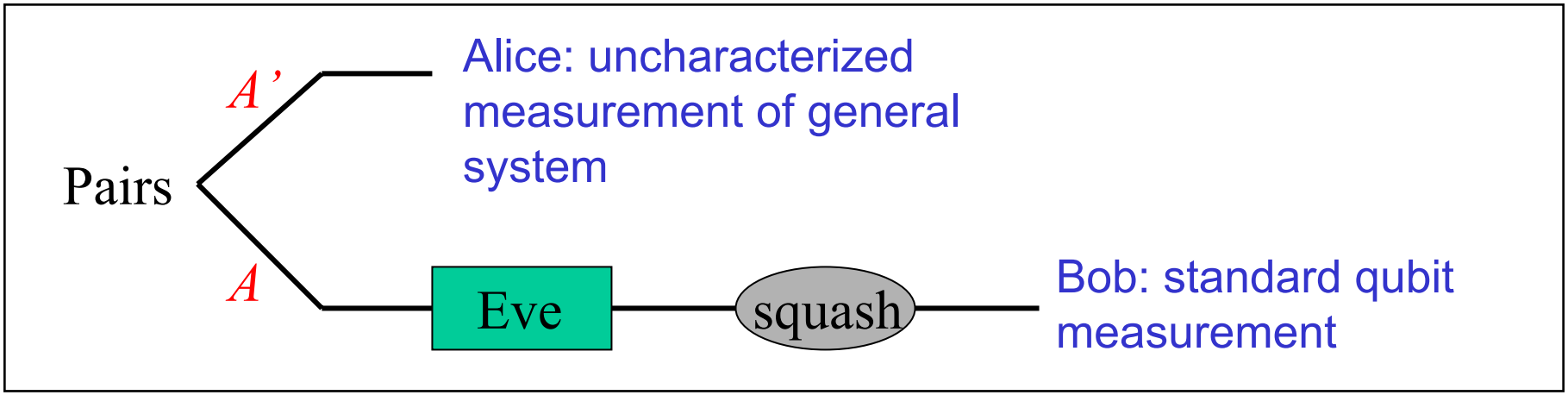
(Uncharacterized source if Alice sends to Bob; uncharacterized detector if Bob sends to Alice. In either case, we bound Eve's information about Bob's key.)

Uncharacterized source



To emit a state in her signal space A, Alice first prepares an entangled state of A and an auxiliary system A'. Then she measures A'. Let $a=0,1$ label Alice's basis choice (both bases equiprobable). Depending on the value of a, Alice performs one of two two-outcome POVMs: measurement M_0 if $a=0$ and measurement M_1 if $a=1$. In either case, the measurement outcome determines the value of Alice's key bit $g=0,1$ (the two key bit values might not be equiprobable). The source emits the state $\rho(a,g)$ with probability $p_{a,g}$.

Uncharacterized source



We can realize in this way any source that does not leak information to Eve about Alice's declared basis: Let $a=0,1$ label Alice's basis choice (both bases equiprobable) and $g=0,1$ the value of her key bit (the two key bit values might not be equiprobable). The source emits the state $\rho(a,g)$ with probability $p_{a,g}$ where

$$p_{0,0}\rho(0,0)+p_{0,1}\rho(0,1)=p_{1,0}\rho(1,0)+p_{1,1}\rho(1,1).$$

Although the emitted state, averaged over the key bit, is basis independent, the source imperfections could be basis dependent; e.g., the source is rotated when sending in the X basis, but not the Z basis.

Protocol 1: BB84

Let $\Omega=1,2,3,\ldots, 4n(1+\varepsilon)$.

(1) Alice creates random bit sequence $\{a_i\}$ (basis choice) and $\{g_i\}$ (key bits). Alice randomly chooses a subset R of Ω with size $|R|= 2n(1+\varepsilon)$.
(2) Bob creates random bit sequence $\{b_i\}$ (basis choice).

(3) Alice sends $\rho(a_i,g_i)$.for each i.
(4) Bob measures Z if $b_i=0$, and measures X if $b_i=1$, obtaining key bits $\{h_i\}$ ($h_i=0$ for outcome +1 and $h_i=1$ for outcome -1).

(5) Bob announces $\{b_i\}$ and Alice announces $\{a_i\}$ and R. If $T= \{ i \in R \mid a_i= b_i \}$ has size less than n, abort. Bob chooses a random subset $S \subseteq \{ i \in \Omega - R \mid a_i= b_i\}$ with size n (if that's not possible, abort).

(6) Alice and Bob compare g_i and h_i for $i \in T$ to determine the error rate δ. If δ is too large, abort.

(7) Bob applies a random permutation π to the positions of the n qubits in S and announces π. Bob announces a binary linear code C with $|C|= 2^r$ that corrects $n(\delta+\varepsilon)$ errors occuring in random positions, with probability exponentially close to unity.
(8) The sifted key κ_{sif} of length n is defined as the sequence $\{h_i\}_{i\in S}$. The final key κ_{fin} of length r is the coset $\kappa_{\text{sif}} + C^{\perp}$.
(9) Alice obtains κ_{sif} through encrypted communication with Bob (consuming τ bits of their previously shared secret key), and she computes κ_{fin}.

Key generation rate

(7) Bob applies a random permutation π to the positions of the n qubits in S and announces π. Bob announces a linear code C with $|C| = 2^r$ that corrects $n(\delta+\varepsilon)$ errors occuring in random positions, with probability exponentially close to unity.

(8) The sifted key $\kappa_{\rm sif}$ of length n is defined as the sequence $\{h_i\}_{i\in S}$. The final key $\kappa_{\rm fin}$ of length r is the coset $\kappa_{\rm sif} + C^{\perp}$.

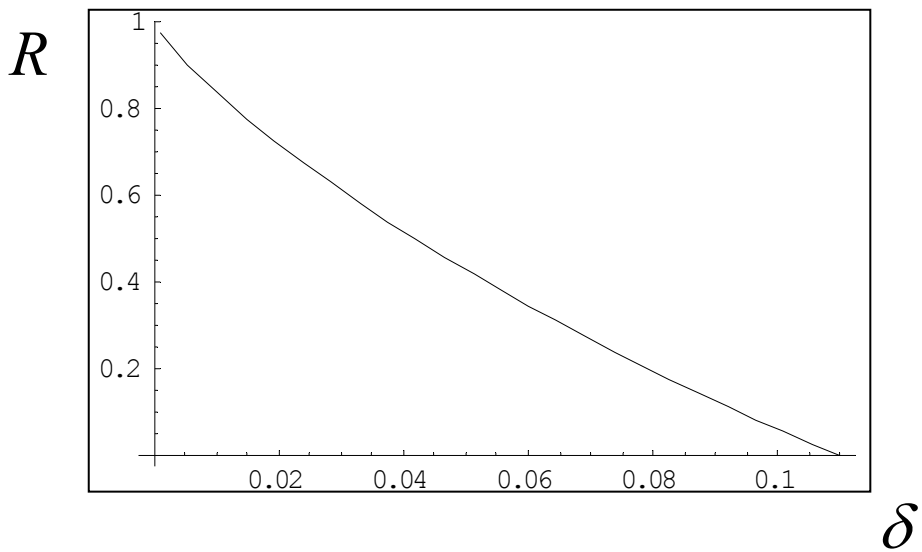
(9) Alice obtains $\kappa_{\rm sif}$ through encrypted communication with Bob (consuming τ bits of their previously shared secret key), and she computes $\kappa_{\rm fin}$.

In the limit of large n, the number of key bits sacrificed for error correction approaches $nH_2(\delta)$, where $H_2(\delta) = -\delta \log \delta - (1-\delta)\log_2(1-\delta).$

We will show that the final key length $r=n[1-H_2(\delta)]$, is achievable asymptotically, so that the rate of generation of final key from sifted key is

$$Rate = \mathrm{Max}\left(1-2H_2(\delta), 0\right).$$

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



Protocol 2: The Mayers basis-flip trick

In Protocol 1, the final key is determined by Bob in step 8; the final step 9 assures that Alice's key agrees with Bob's and leaks no info to Eve.

Now, Eve's information I_1 about Bob's key is unaffected if we replace: (3) Alice sends $\rho(a_i, g_i)$.for each i.
with:

(3') For $i \in \mathrm{R}$ Alice sends $\rho(a_i, g_i)$.

For $i \in \Omega$ - R Alice sends $\rho(a_i \oplus 1, g_i)$.

Mayers

Alice sends in the "right" basis in the test set, but in the "wrong" basis in the key-generating set. But Bob extracts his key and Eve launches her attack without knowing anything about Alice's key bits $\{g_i\}$. Therefore, only the states averaged over the $\{g_i\}$ are relevant to Eve and Bob, and these states are unchanged by the basis flip. Therefore, Protocol 1 and Protocol 2 are identical to Eve and Bob, and in particular, Eve's information about Bob's key is the same in either protocol: $I_1 = I_2$.

Note: we assume that Alice sends a product state: $\otimes_i \rho_i$
Otherwise, correlations between the test bits and key bits might spoil the equivalence. (Similarly, in the "time-reversed" situation, the signals are measured individually rather than collectively.)

Protocol 3: Increasing Eve's power

It won't change anything if we imagine that it is Bob rather than Alice who uses the wrong basis on the key-generating set. (All that matters is that they use the same basis for the test set and opposite bases for key generation.) Now we further modify Protocol 2 in Eve's favor, by allowing Eve to control Alice's source:

(3'') Eve prepares Bob's qubits and her ancilla system in any state she chooses.

Eve's maximum information about Bob's key is at least as large for Protocol 3 as for Protocol 2: $I_1 = I_2 \leq I_3$.

To complete the proof, we are to show that I_3 is small: Eve cannot predict Bob's key because Bob is measuring in the "wrong" basis.

Protocol 3 is secure because, in order to pass the verification test, Eve must send to Bob states that are close to the BB84 states; thus when Bob measures in the conjugate basis, it is hard for her to predict what Bob will find. The reduction to Protocol 3 is a simplification, as we no longer need to consider separately the attack by Eve and the (possibly defective) performance of Alice's source.

Mayers

Security of Protocol 3: Verification

In Protocol 3, Eve knows $\{a_i\}$ and $\{g_i\}$, and she can prepare any states she pleases; hence there is no loss of generality if we assume $a_i = g_i = 0$. But Eve doesn't know which are the test bits and which are the key bits.

The crux of proving security is showing that privacy amplification is effective in reducing Eve's information about Bob's key to a negligible amount…

First, what is learned from the verification test? The test set T (with size at least n) is chosen randomly, and the error rate ($Z=-1$) is δ. From classical sampling theory, if the qubits in the key-generating set S were also measured in the Z basis, the *joint* probability of finding more than $n(\delta+\varepsilon)$ errors in S and δ errors in T (for any strategy by Eve) would be

$$\text{Prob} \le \exp\left[-\varepsilon^2 n / 4\delta(1-\delta)\right].$$

Therefore, unless Eve uses a very inefficient strategy that passes the verification test with exponentially small probability, we conclude that the probability that the state ρ on $\mathcal{H}_E \otimes \mathcal{H}_S$, conditioned on the outcome of the test, has more than $n(\delta+\varepsilon)$ errors is exponentially small.

Security of Protocol 3: Permutation

Bob randomly permutes his qubits, after which the state in $\mathcal{H}_E \otimes \mathcal{H}_S$ shared by Eve and Bob is

$$\rho_{\text{sym}} = (N!)^{-1} \sum_{\pi} |\pi\rangle\langle\pi| \otimes \left(U_\pi \otimes I_E \right) \rho \left(U_\pi^\dagger \otimes I_E \right)$$

The linear code C used in privacy amplification can correct $n(\delta + \varepsilon)$ randomly distributed errors with high probability. Denote by $\mathcal{E}$ the set of correctable errors $\{e\}$, and by $P_{\mathcal{E}}$ the projector onto the space $\mathcal{H}_{\text{good}}$ spanned by $\{|e\rangle_Z\}$. Then the state ρ' resulting from applying $P_{\mathcal{E}}$ to ρ_{sym} is very close to ρ_{sym} :

$$\rho' = \frac{(P_{\mathcal{E}} \otimes I_E)\rho_{\text{sym}}(P_{\mathcal{E}} \otimes I_E)}{Tr\left[(P_{\mathcal{E}} \otimes I_E)\rho_{\text{sym}}\right]}; \quad F(\rho', \rho_{\text{sym}}) = Tr\left[(P_{\mathcal{E}} \otimes I_E)\rho_{\text{sym}}\right] \geq 1 - \eta$$

where η is exponentially small.

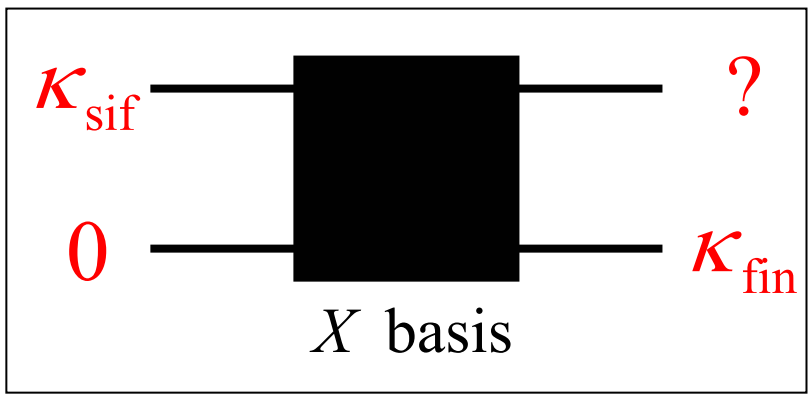
We will see that if the state ρ' instead of ρ_{sym} were used to generate the key bits, then Eve would have no information about the final key ($I_3 = 0$). Then it will be easy to show that Eve's information is exponentially small when ρ_{sym} is used...

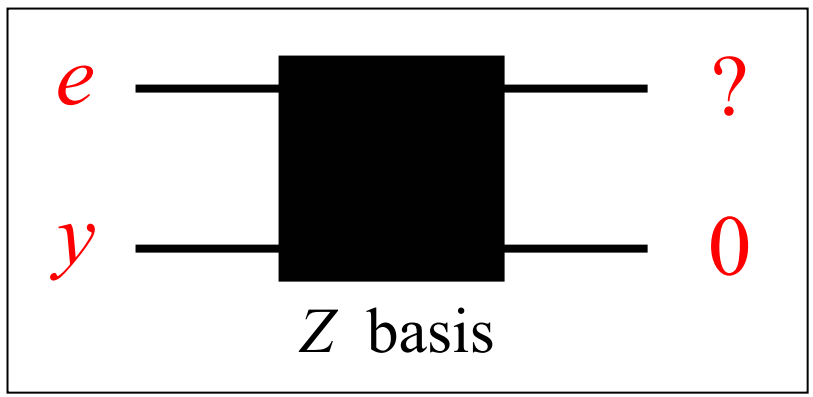
Security of Protocol 3: Virtual error correction

To prove that Eve has no information about Bob's final key if the state ρ' is used for key generation, we will use the concept of *virtual error correction*. The idea is that there is a procedure Bob *could have* used to completely remove Eve's entanglement with his qubits. This suffices to ensure privacy, even if Bob did not really use this procedure (cf., Shor-Preskill '00).

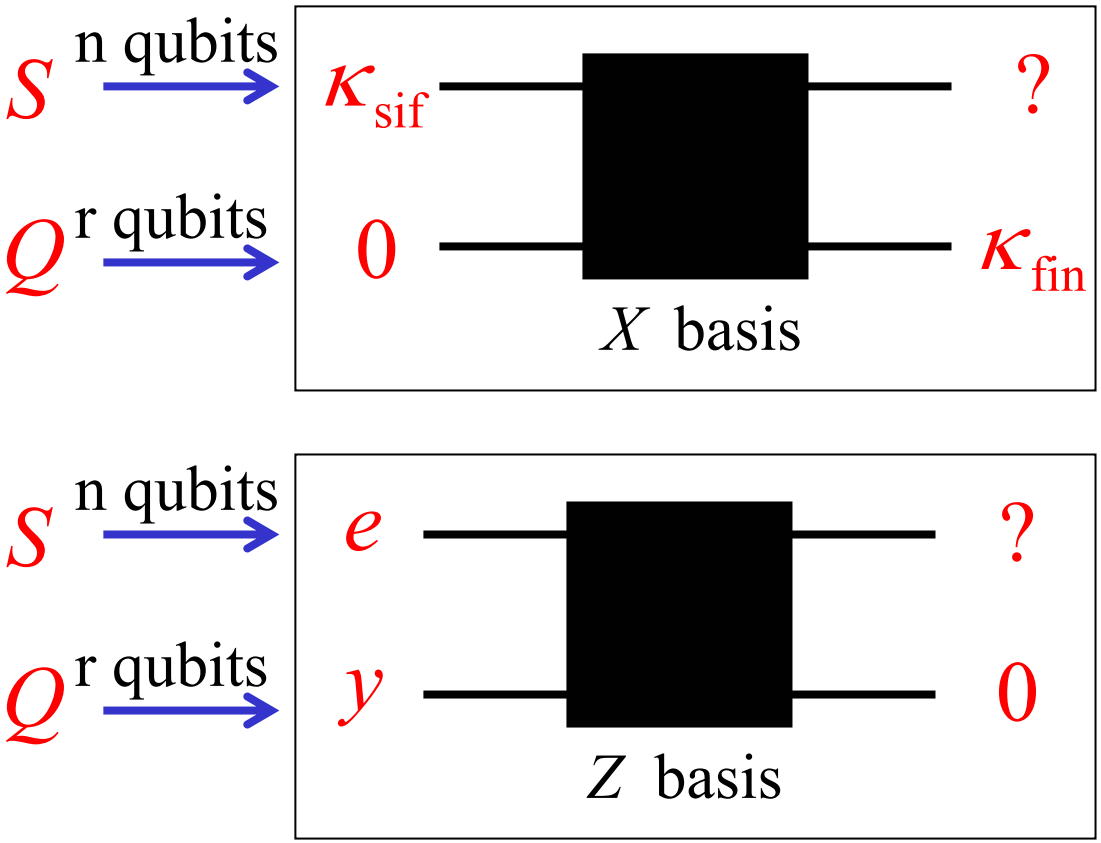
In Protocol 3, Bob measures his qubits in the Z basis for the verification test. To generate his final key, he measures his qubits in the X basis, and then applies the privacy amplification algorithm.

We will construct a box that Bob could use. If the box receives X-basis eigenstates, it extracts the corresponding final key. But if it receives states in $\mathcal{H}_{\text{good}}$ (with correctable Z-basis errors), it extracts a random, private final key.





Security of Protocol 3: Virtual error correction



The box has two registers: an input register for the sifted key, and an output register where the final key will be recorded. Measuring the output register after the action of the box is equivalent to measuring the input in the X basis and processing it classically to find the final key.

But if the input is any state in $\mathcal{H}_{\text{good}}$ (with correctable errors in the Z basis), then the output is:

$$|0\rangle_Z = 2^{-r/2} \sum_{x=0}^{2^r-1} |x\rangle_X$$

When Bob measures in the X basis he obtains a random outcome that Eve can't possibly predict.

Security of Protocol 3: Virtual error correction

To understand how the box is constructed, we recall how the linear code C is used in the privacy amplification algorithm. The code is an r-dimensional subspace of $\mathbb{F}_2^{\,n}$. It has an $r \times n$ generator matrix G whose rows generate the code space. An r - bit message y can be encoded with G:

$$y \to y\,G\,.$$

There is a decoding function f such that if e is in the set $\mathcal{E}$ of correctable errors, then $f(y\,G + e) = y\,.$

Random errors of weight $n(\delta + \varepsilon)$ are contained in the set $\mathcal{E}$ of correctable errors with high probability.

Bob's final key κ_{fin} of length r is the coset $\kappa_{\text{sif}} + C^{\perp}$, where $C^{\perp}$ is the orthogonal complement of C. Note that the rows of G and hence the colums of the $n \times r$ matrix G^T span the space orthogonal to $C^{\perp}$; hence we can compute the final key by applying G^T to the n - bit input string x:

$$x \to x\,G^T\,.$$

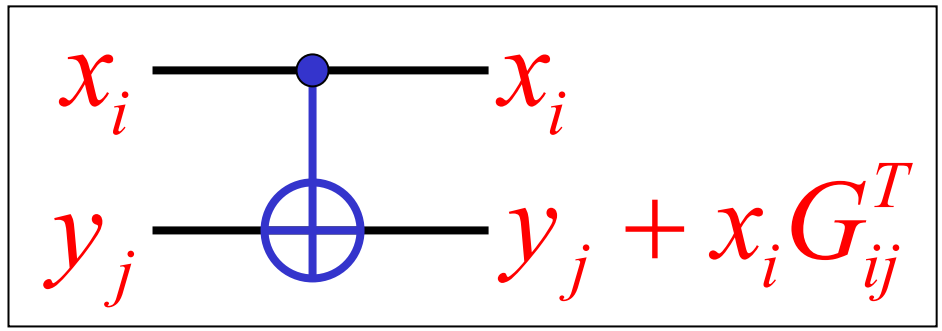
Our box will exploit the duality between constructing a C codeword with G and extracting a $C^{\perp}$ coset with G^T.

Security of Protocol 3: Virtual error correction

We can construct a circuit that performs the operation

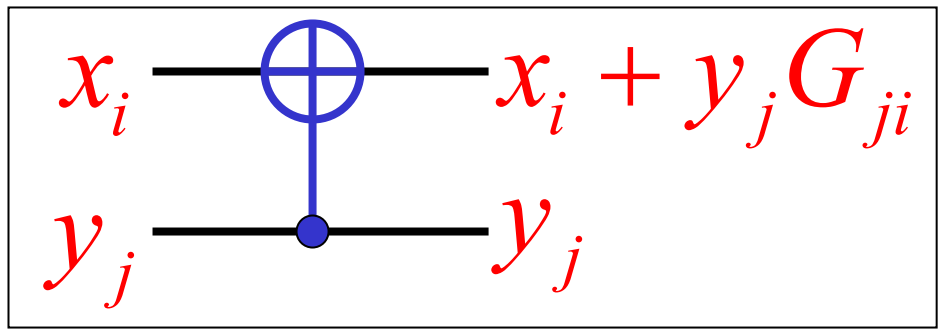
$$(x, y) \rightarrow (x, y + x\, G^T)$$

in the X basis: there is a controlled-NOT gate for each nontrivial matrix element.

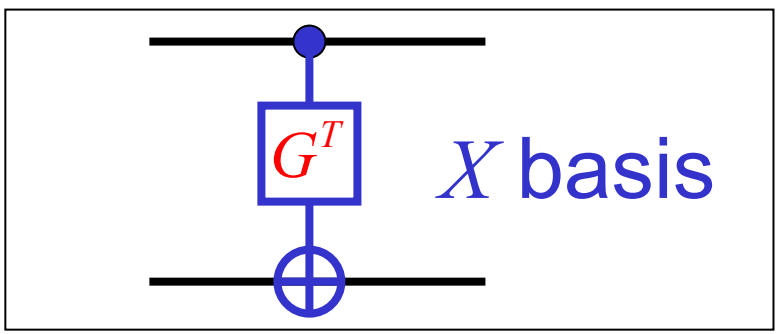


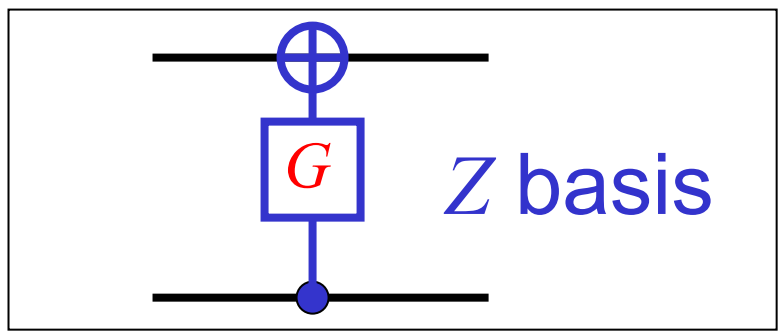
How does the circuit act in the Z basis? The CNOT reverses direction, so that the operation is

$$(x, y) \rightarrow (x + y\, G, y).$$

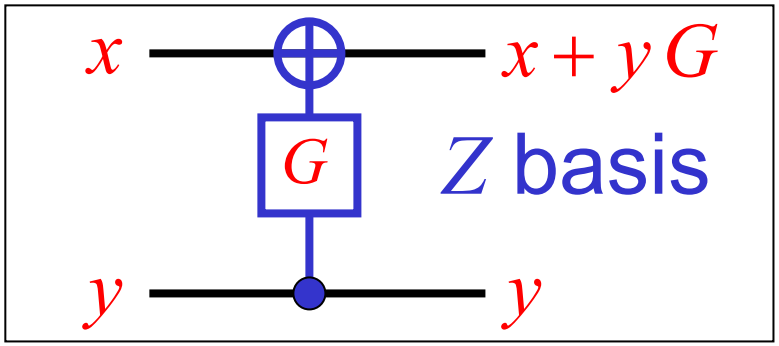


Thus the circuit that computes the $C^{\perp}$ coset in the X basis is a C encoder in the Z basis.

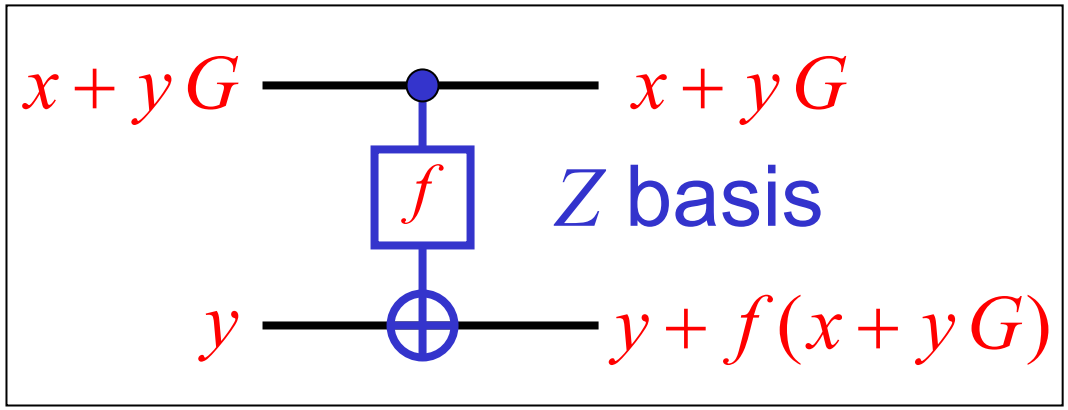




Security of Protocol 3: Virtual error correction

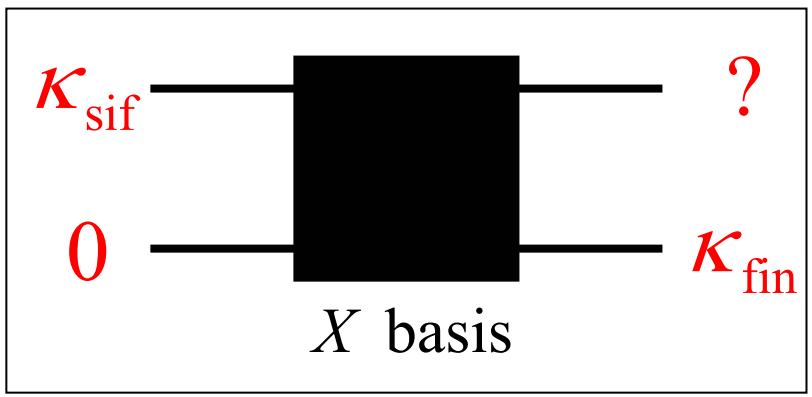


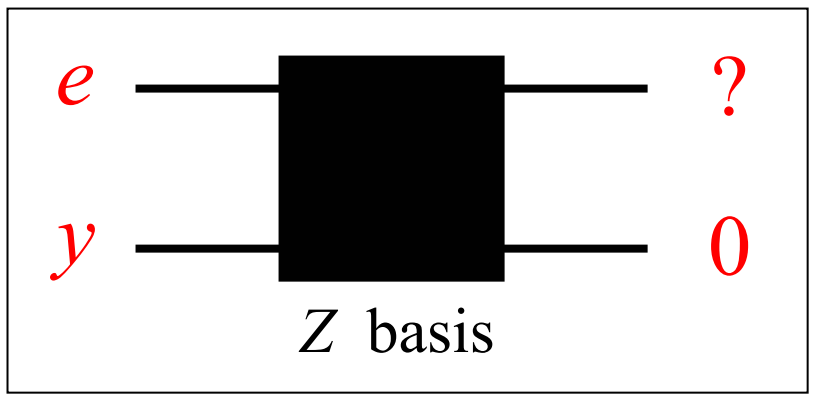
Now suppose that we append to this Z basis encoder a *decoder* that executes error correction:



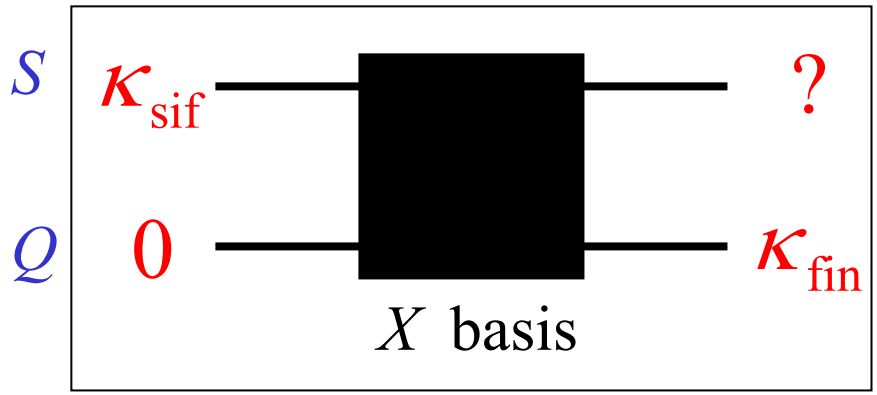
Then if x is a correctable error in the set $\mathcal{E}$, the decoder transforms the output register to the state $|0\rangle_Z$.

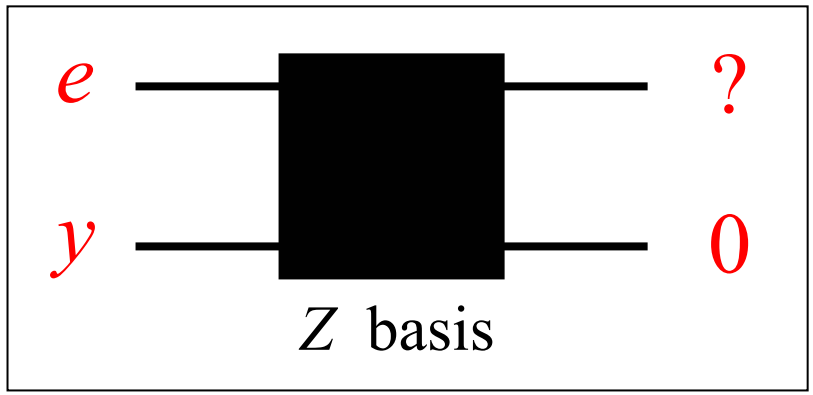
Furthermore, the action of the decoder circuit in the X basis preserves the value of the output register. We have constructed our box!





Security of Protocol 3: Bounding Eve's information





• Bob measures in the Z basis in the verification test and in the X basis to generate the key.

• If Bob uses the box, followed by an X-basis measurement, to find his final key, the result is the same as if he measured the sifted key in the X basis and then applied classical privacy amplification to the outcomes.

• We know from the verification test that the actual state ρ_{sym} used to generate the key is exponentially close in fidelity to a state ρ' with support on the correctable space $\mathcal{H}_{\text{good}}$.

• We have shown that if the state ρ' were used, then the state that Bob measures to find the final key would be $|0\rangle_Z$ -- the outcome is random and unknown by Eve. If the actual state is used instead, Bob measures a state that is exponentially close to $|0\rangle_Z$ -- the outcome is nearly random and Eve knows almost nothing.

Security of Protocol 3: Bounding Eve's information

• We have shown that if the state ρ' were used, then the state that Bob measures to find the final key would be $|0\rangle_Z$ -- the outcome is random and unknown by Eve. If the actual state is used instead, Bob measures a state that is exponentially close to $|0\rangle_Z$ -- the outcome is nearly random and Eve knows almost nothing.

Bounding Eve's information is not technically difficult...

$${}_Z\langle 0|\,\rho_Q\,|0\rangle_Z \geq 1-\eta,$$ where η is exponentially small.

In the worst case, Eve and Bob share a pure state. Bob's measurement prepares a state for Eve, and the information she can acquire about what was prepared, by Holevo's theorem, is bounded by her Von Neuman entropy:

$$I_3 \leq S(\rho_E) = S(\rho_Q) < H_2(\eta) + r\eta$$

The key is nearly random. If two states are exponentially close to one another, then the probability distributions they generate when measured are exponentially close to one another. The Shannon entropy of the r-bit key satisfies:

$$H_{\text{key}} \geq r(1-2\eta)$$

Security of Protocol 3: Bounding Eve's information

$$ {}_Z\langle 0 \,|\, \rho_Q \,|\, 0 \rangle_Z \;\geq\; 1-\eta \quad \Rightarrow \quad \begin{aligned} & I_1 \leq I_3 < H_2(\eta) + r\eta \;; \\ & r - H_{\text{key}} \leq \; 2r\eta \,. \end{aligned} $$

To establish a key that is truly randomly distributed, Bob can announce a random r-bit sequence w and add it to the key y generated by the BB84 protocol. Since Eve knows w, her information I about the new key is

$$ \begin{aligned} I &= H(\text{new key}) - H(\text{new key}|\text{Eve}) \\ &= r - H(\text{old key}|\text{Eve}) \\ &= r - H(\text{old key}) + I_1 \leq H_2(\eta) + 3r\eta \end{aligned} $$

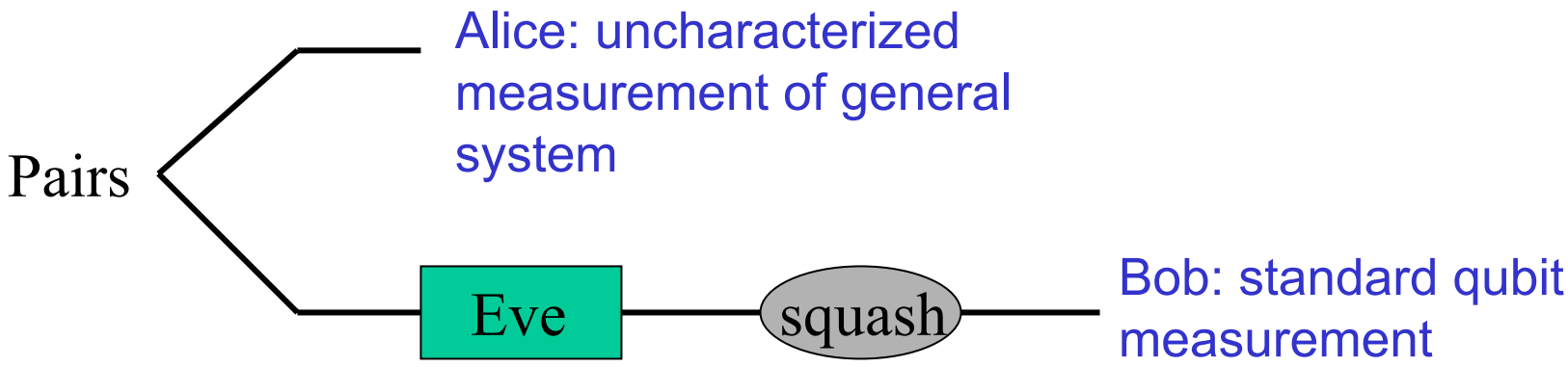
Security of BB84

Theorem: Security of BB84 with an uncharacterized source. Suppose that Alice's source emits products states, and that each signal, when averaged over Alice's key bits, is basis-independent; the source is otherwise uncharacterized. Suppose that Bob's detector is perfect. Suppose Eve uses a strategy that passes the verification test with a probability that is not exponentially small. Then for *any* such attack by Eve, Alice and Bob agree with high probability on a final key that is nearly uniformly distributed, and Eve's information about the final 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.

M. Koashi and J. Preskill, "Secure quantum key distribution with an uncharacterized source," quant-ph/0208143.

Key distribution scenarios



What does Eve know about Bob's key?

What does Eve know about Alice's key?

Security of BB84

Theorem: Security of BB84 with an uncharacterized detector. (Cf., Mayers '96.) Suppose that Alice's source can be realized by performing standard qubit measurements on half of an entangled state. Suppose that Bob's detector measures signals individually rather than collectively, but is otherwise uncharacterized. Suppose Eve uses a strategy that passes the verification test with a probability that is not exponentially small. Then for *any* such attack by Eve, Alice and Bob agree with high probability on a final key that is nearly uniformly distributed, and Eve's information about the final 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.

Security of BB84

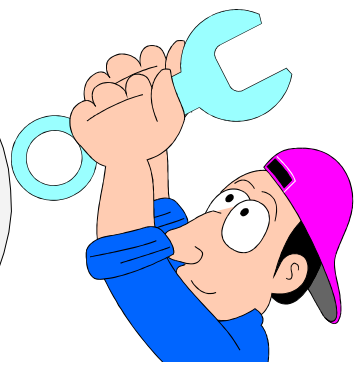
Neither theorem applies when both the source and the detector have small imperfections that depend on the basis used in the protocol, the case relevant to real-world implementations of QKD. It is intuitively clear that BB84 should remain secure if the imperfections are “sufficiently small.” Can we calculate how the key generation rate depends on the tolerance to which the equipment is characterized?

Alice

Bob

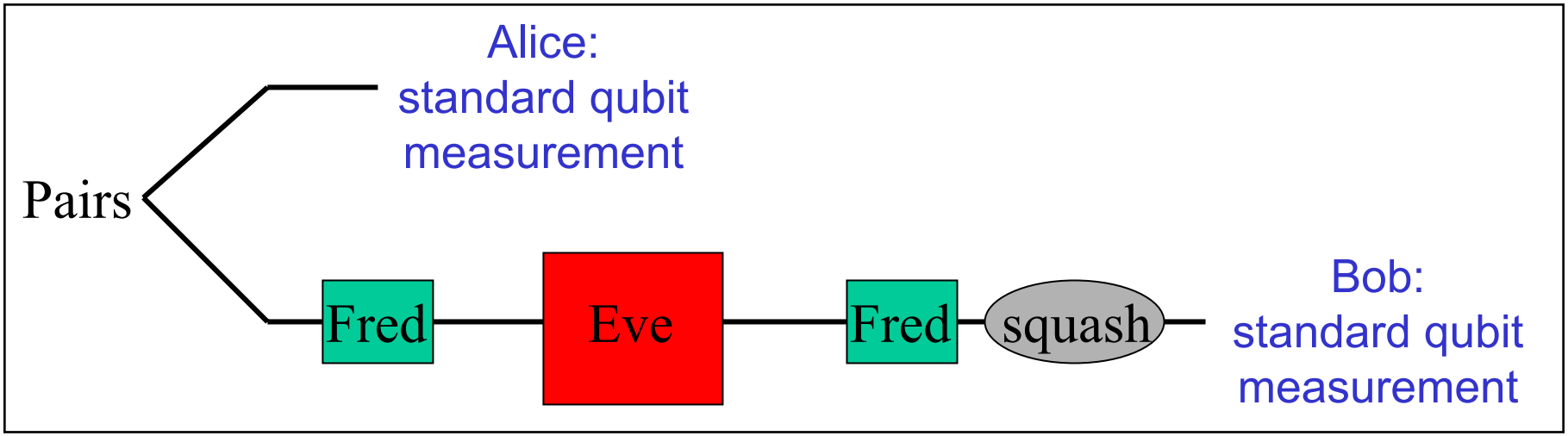
vs.

Eve



Fred

Security of BB84



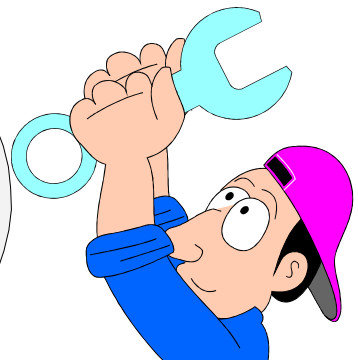
Fred knows the basis used, but the basis dependence of his attack is limited. Eve's attack is basis independent, but otherwise arbitrary.

Alice

Bob

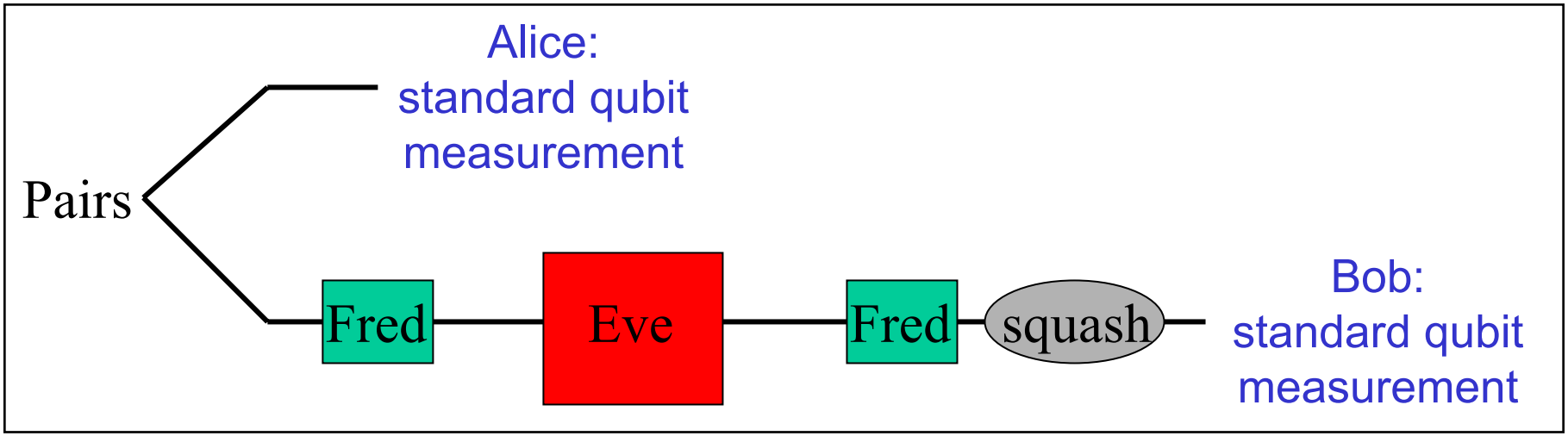
vs.

Eve



Fred

Security of BB84

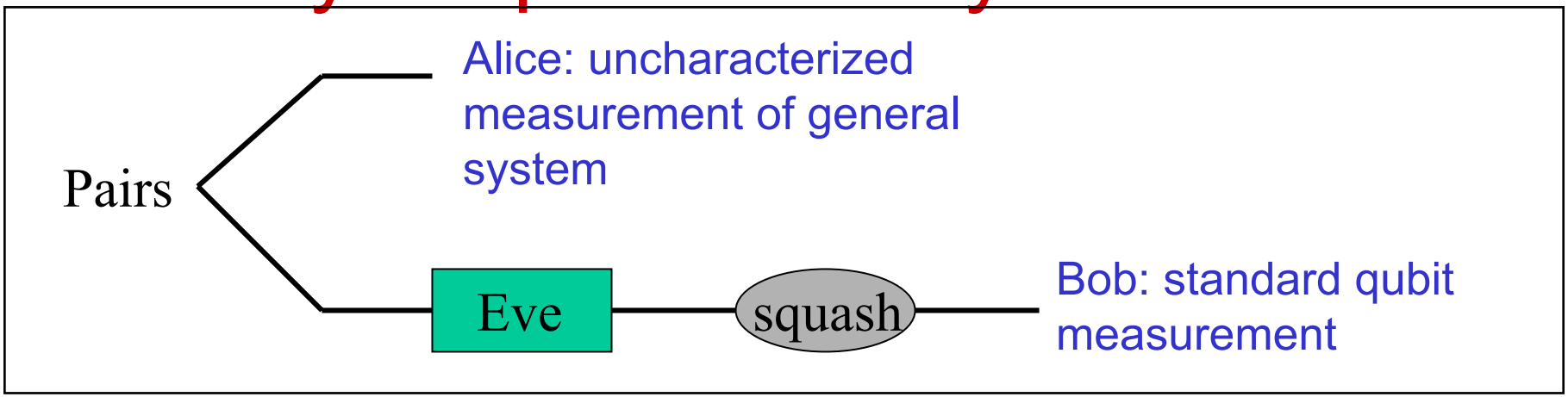


Fred knows the basis used, but the basis dependence of his attack is limited. Eve's attack is basis independent, but otherwise arbitrary.

In this scenario (still not the most general possible), security can be proven for generic sufficiently weak basis-dependent attacks by Fred.

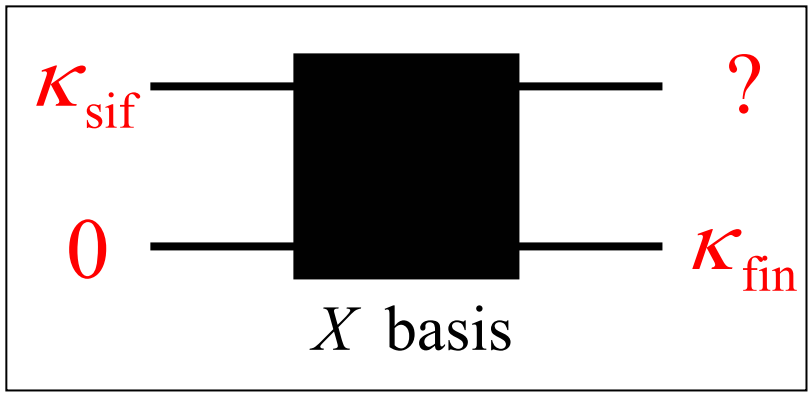
D. Gotttesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, "Security of quantum key distribution with imperfect devices," quant-ph/0212066.

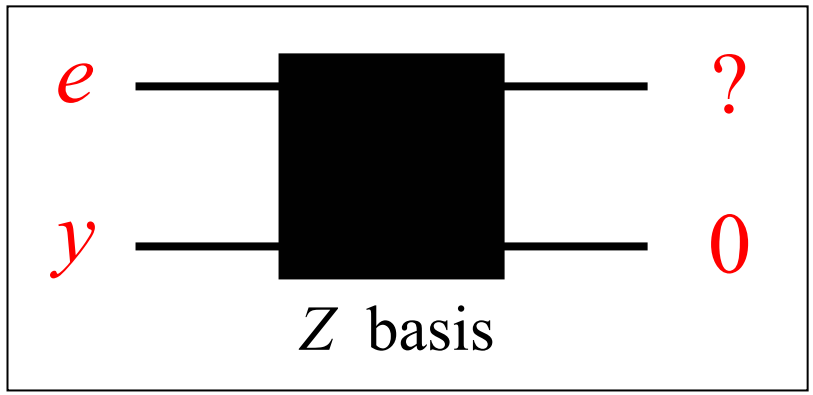
Security of quantum key distribution



- Perfect detector and uncharacterized source (emitted states, averaged over key bit, are independent of the basis used) [Koashi-Preskill ’02].
- Perfect source and arbitrary uncharacterized detector [Mayers ’96].
- Generic small flaws in source and detector, controlled by adversary. (Key generation rate is reduced by the flaws.) [Gottesman-Lo-Lütkenhaus-Preskill ’02].

Security of quantum key distribution





- Perfect detector and uncharacterized source (emitted states, averaged over key bit, are independent of the basis used) [Koashi-Preskill '02].
- Perfect source and arbitrary uncharacterized detector [Mayers '96].
- Generic small flaws in source and detector, controlled by adversary. (Key generation rate is reduced by the flaws.) [Gottesman-Lo-Lütkenhaus-Preskill '02].

Secure quantum key distribution with an uncharacterized source

M. Koashi and J. Preskill, “Secure quantum key distribution with an uncharacterized source,” quant-ph/0208143.

D. Gotttesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, “Security of quantum key distribution with imperfect devices,” quant-ph/0212066.

John Preskill, Caltech

16 December 2002

http://www.iqi.caltech.edu/