On the unconditional Security of QKD Schemes

quant-ph/9912053

Talk Outline

- Introduction to Quantum Information
- The BB84 Quantum Cryptosystem
- Eve’s attack
- Bounding Eve’s information
- Security and Reliability

Works on Security

- C.A. Fuchs, N. Gisin, R.B. Griffiths, C. S. Niu, A. Peres, 1997: optimal eavesdropping.
- E. Biham, T. Mor, 1997: limited attacks.
- D. Mayers, 1998: results on POVMs.
- H.K. Lo and H.F. Chau 1999, security using quantum fault tolerance.
- E. Biham, M. Boyer, P. O. Boykin, T. Mor, V. Roychowdhury, 1999: Information vs. Disturbance.
- M. Ben-Or, 1999: based on compression.
- P. Shor and J. Preskill, 2000: based on quantum codes.

What Are qubits?

- Qubits are normalized vectors from a complex space:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$|00\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, |01\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, |10\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, |11\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

$$|y\rangle = a|0\rangle + b|1\rangle = \begin{pmatrix} a \\ b \end{pmatrix}, \langle y| \equiv \begin{pmatrix} a^* & b^* \end{pmatrix}$$

- Quantum operations are ***Unitary Operators*** on this space.

$$|y_1\rangle = U|y_0\rangle$$

- Measurement of Qubits is a set of positive operators that sum to *I*, which give output *k* with a given probability:

$$\sum_i E_i = I \qquad p_k = tr\left(E_k |y\rangle\langle y|\right)$$

Let's Measure Some Example

q u b i t s !

- See that $E_0+E_1=I$, and E's are positive, so they define a measurement

$$E_0 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

$$E_1 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

$$tr\left(E_i \left| \; \right\rangle\left\langle j \right|\right) = d_{i,j}$$

•The above measurement, tells exactly which state was sent, |0> or |1>, consider the two following states:

$$\left|+\right\rangle \equiv \frac{\left|0\right\rangle+\left|1\right\rangle}{\sqrt{2}}$$

$$\left|-\right\rangle \equiv \frac{\left|0\right\rangle-\left|1\right\rangle}{\sqrt{2}}$$

$$tr\left(E_i\left|+\right\rangle\left\langle+\right|\right) = tr\left(E_i\left|-\right\rangle\left\langle-\right|\right) = \frac{1}{2}$$

This measurement gives E_0 and E_1 with equal probability!

A Measurement for the +,- Basis

- See that $E_+ + E_- = I$, and E's are positive, so they define a measurement

$$E_+ = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \qquad tr\left(E_+ |+\rangle\langle +|\right) = tr\left(E_- |-\rangle\langle -|\right) = 1$$

$$E_- = \frac{1}{2}\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \qquad tr\left(E_- |+\rangle\langle +|\right) = tr\left(E_+ |-\rangle\langle -|\right) = 0$$

•The above measurement, tells exactly which state was sent, |+> or |->, but nothing about |0> or |1>:

$$tr\left(E_+ |i\rangle\langle i|\right) = tr\left(E_- |i\rangle\langle i|\right) = \frac{1}{2}$$

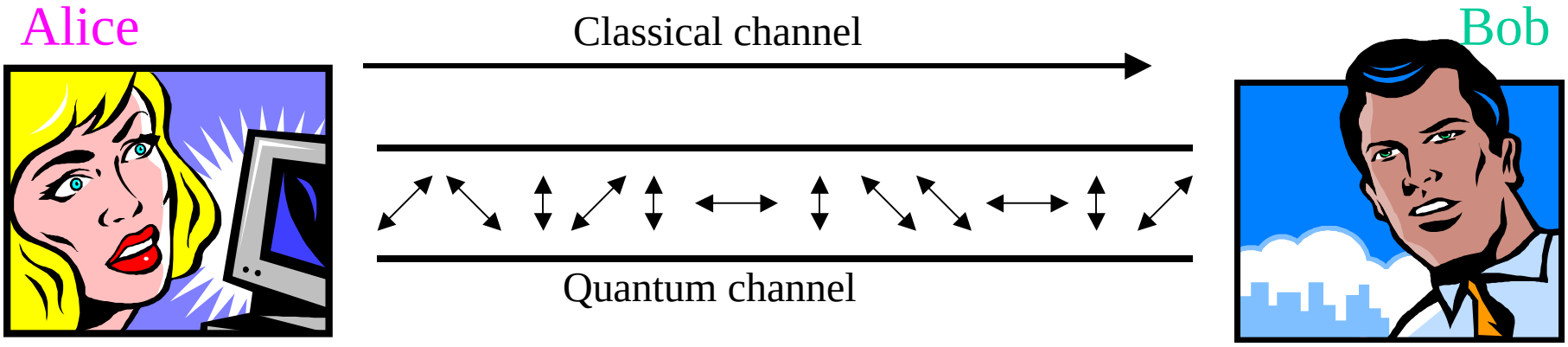
This measurement gives E_+ and E_- with equal probability!

The BB84 (4-state) Scheme

- Alice wishes to generate a shared secret key with Bob using a quantum channel and an authenticated classical channel.
- Alice selects each bit randomly and then the basis:

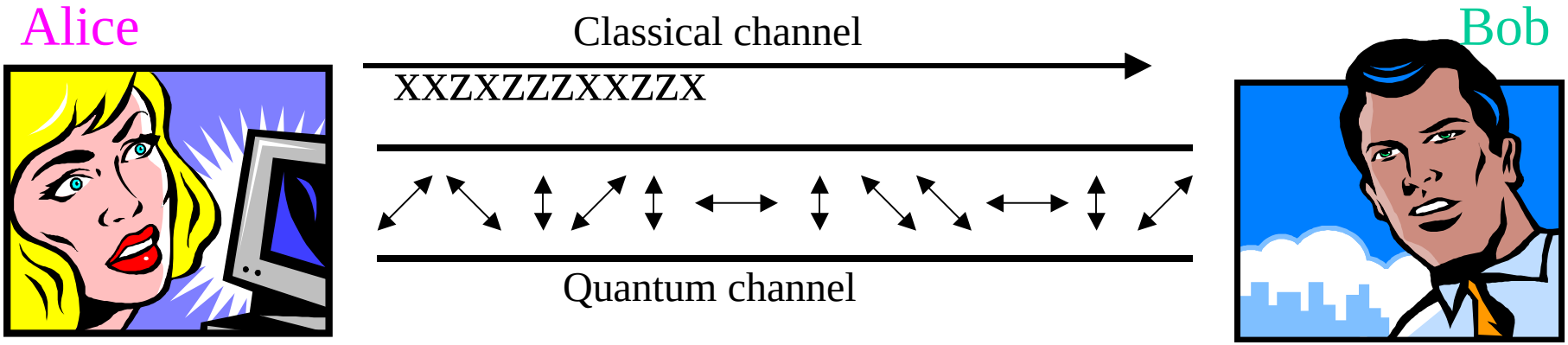
$$|0_z\rangle = |0\rangle \qquad |0_x\rangle = |+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

$$|1_z\rangle = |1\rangle \qquad |1_x\rangle = |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$



BB84 (Cont.)

- *After* Bob receives all the qubits, Alice announces on the classical channel which bases were used.
- Now Bob measures in Alice's basis (z and $\{E_0,E_1\}$ or x and $\{E_+,E_-\}$). The sent qubit and measured qubit should agree. These values will be used to form the key.



Eavesdropping

- In addition to Alice and Bob, there is Eve:

- Eve is not very nice and she wants the key. In an attempt to learn about the key, she may listen to the classical channel and do *quantum operations* on the channel and some qubits at her lab. Quantum operations are unitary.

$$\left|00...0\right\rangle_{Eve}\left|i\right\rangle_{Alice} \xrightarrow{U_{eve}} \sum_{j}\left|E_{i,j}\right\rangle_{Eve}\left|j\right\rangle_{Bob}$$

No Cloning of Qubits

- Unitarity of quantum operations means that qubits can't be copied exactly (no-cloning):

Proof:

$$|E\rangle|0\rangle|0\rangle \xrightarrow{U} |E_0\rangle|0\rangle|0\rangle$$

$$|E\rangle|0\rangle|+\rangle \xrightarrow{U} |E_+\rangle|+\rangle|+\rangle$$

The left side of above is normalized, and unitary operations preserve length, so the right side is normalized. Inner product is preserved so inner product of the left sides and right sides are equal:

$$\langle 0|+\rangle = \frac{1}{\sqrt{2}} \qquad \text{So:} \qquad \langle E_0 | E_+ \rangle = \sqrt{2} > 1$$

Any attempt to learn qubits, disturbs them, so Eve causes

Errors!

An Example Attack:

(Measure and Resend)

- A simple attack Eve could perform is to measure each qubit in a random basis and send the result on to Bob.
- Half the time, Eve guesses the basis correctly, and learns the bit. When she does not guess correctly, the error rate is 50%. In total, this attack gives Eve half the bits, but causes a 25% error rate.

CNOT Attack

In the z basis it works

$$|0_z\rangle|0_z\rangle_E \rightarrow |0_z\rangle|0_z\rangle_E$$
$$|1_z\rangle|0_z\rangle_E \rightarrow |1_z\rangle|1_z\rangle_E$$

In the x basis:

$$|+\rangle|0_z\rangle_E \rightarrow |0_z\rangle|0_z\rangle_E + |1_z\rangle|1_z\rangle_E = |+\rangle|+\rangle_E + |-\rangle|-\rangle_E$$

Hence, in the x basis, Bob's outcome becomes random!!

In general any interference by EVE leads to errors.

Eavesdropping for Dummys

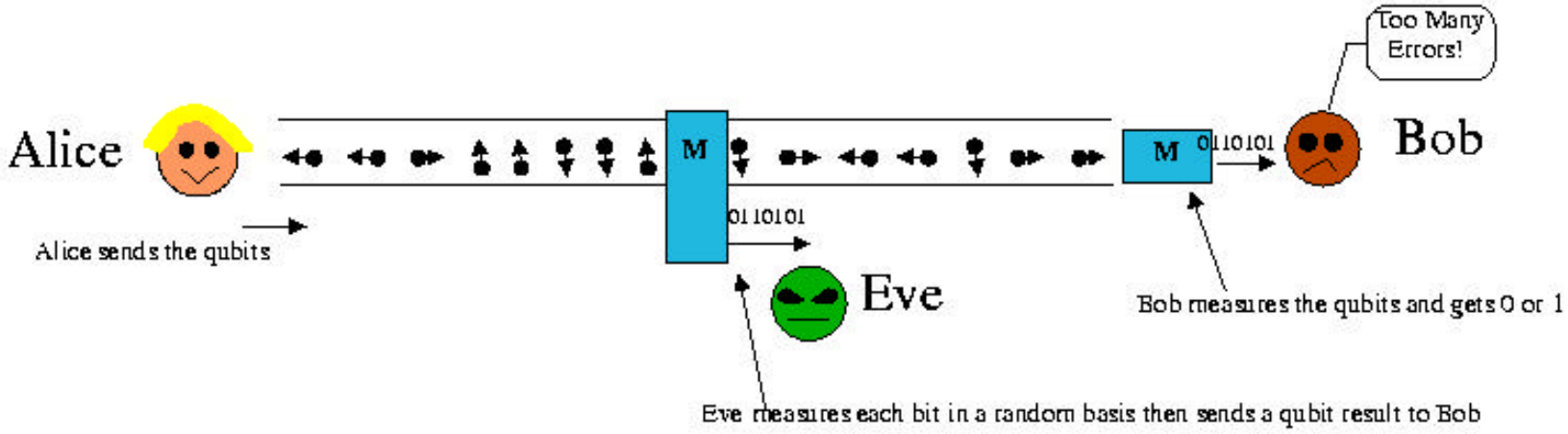
Eve tries to learn the value of the qubits without causing so many errors that Alice and Bob abort. The laws of quantum mechanics place limits on Eve's power:

A simple attack Eve can perform is measure/resend. She guesses a basis to measure, and resends the result she measures to Bob. This attack causes a 25% error rate:

$$P(0_x \to 1_z) = P(1_z \to 0_x) = |\langle 0_x | 1_z \rangle|^2 = \frac{1}{2}$$

$$P(0_z \to 1_x) = P(1_x \to 0_z) = |\langle 0_z | 1_x \rangle|^2 = \frac{1}{2}$$

When she guesses the basis correctly, which she does half of the time, she causes no error. When she guesses the basis incorrectly, again half the time, she causes 50% errors:



The Measure of Information

We talk about Eve's information so we need to quantify it. We use standard information theory notations.

The entropy of a random variable is defined as:

$$H(X) = -\sum_x p(x)\log_2 p(x)$$

For a uniform distribution with 2^n elements, see that H(X)=n. Entropy is measured in bits. It is a measure of how much information is required to describe an outcome, on average.

The conditional entropy is defined as:

$$H(X|Y) = -\sum_{x,y} p(x,y)\log_2 p(x|y) = \sum_y p(y)H(X|Y=y)$$

Conditional Entropy is a measure of how much information is required on average to describe an outcome of X given Y.

The mutual information between two variables is defined as:

$$I(X;Y) = H(X) - H(X|Y)$$

Eve's Information for the Measure/Resend Attack

The information between Alice and Eve we call I(A;E). Alice chooses bits randomly, so H(A)=1. There is 1 bit of entropy for each bit. The relative entropy H(A|E) is needed. For the measure/resend attack, Eve knows each bit except with probability 1/4. This gives:

$$I(A:E)=H(A)-H(A|E)=1+(\frac{1}{4}\log_2(\frac{1}{4})+\frac{3}{4}\log_2(\frac{3}{4}))$$

$$=\frac{3}{4}\log_2 3-1\approx 0.189\,bits$$

This does not seem like a lot, but it is when compared to Bob's information in this case. Recall, Bob also has a 25% error rate in this attack

$$I(A:B)=H(A)-H(A|B)=1+(\frac{1}{4}\log_2(\frac{1}{4})+\frac{3}{4}\log_2(\frac{3}{4}))$$

$$=\frac{3}{4}\log_2 3-1\approx 0.189\,bits$$

Smarter Eavesdropping

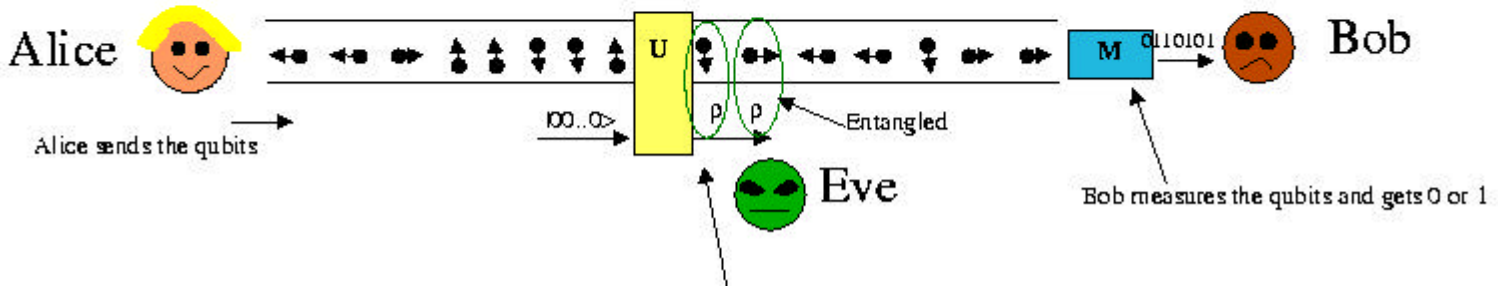
The measure/resend attack gives Eve as much information as Bob. When Eve guesses the basis correctly, Eve, Bob, and Alice have the same bit. When Eve guesses incorrectly, she and Bob each have a 50/50 chance of having it correctly. This situation could be accomplished by Alice just announcing half the bits, and Eve and Bob guessing the other half. BB84 is insecure in this case.

From this attack we know to form a secure key it is neccesary that the error rate be less than 25%:

$$P_{secure} < 0.25$$

To find an error rate that is sufficient for security we must look at more sophisticated attacks for Eve. Consider the most general ***single particle attack***. Eve does a quantum computation (U) with each bit that Alice sends along with some ancilla bits which Eve controls. Eve sends a particle to Bob that is entangled with her probe:

$$|00...0\rangle|0_z\rangle_A \rightarrow |E_{00}\rangle|0_z\rangle_B + |E_{01}\rangle|1_z\rangle_B$$
$$|00...0\rangle|1_z\rangle_A \rightarrow |E_{10}\rangle|0_z\rangle_B + |E_{11}\rangle|1_z\rangle_B$$



Linearity and Unitarity

Quantum Mechanics is linear and unitary, we see how this restricts Eve:

$$|00...0\rangle|0_z\rangle_A \rightarrow |E_{00}\rangle|0_z\rangle_B + |E_{01}\rangle|1_z\rangle_B$$
$$|00...0\rangle|1_z\rangle_A \rightarrow |E_{10}\rangle|0_z\rangle_B + |E_{11}\rangle|1_z\rangle_B$$

The relations between the x and z bases are known:

$$|0_z\rangle = |0\rangle \quad |1_z\rangle = |1\rangle \quad |0_x\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \quad |1_x\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Due to linearity Eve's attack is also defined in the x basis:

$$|00...0\rangle|0_x\rangle_A \rightarrow \frac{1}{2}\left(|E_{00}\rangle + |E_{01}\rangle + |E_{10}\rangle + |E_{11}\rangle\right)|0_x\rangle_B + \frac{1}{2}\left(|E_{00}\rangle + |E_{01}\rangle - |E_{10}\rangle - |E_{11}\rangle\right)|1_x\rangle_B$$
$$|00...0\rangle|1_x\rangle_A \rightarrow \frac{1}{2}\left(|E_{00}\rangle - |E_{01}\rangle + |E_{10}\rangle - |E_{11}\rangle\right)|0_x\rangle_B + \frac{1}{2}\left(|E_{00}\rangle - |E_{01}\rangle - |E_{10}\rangle + |E_{11}\rangle\right)|1_x\rangle_B$$

Due to unitarity Eve's attack must preserve length, and orthogonality:

$$\langle E_{00}|E_{00}\rangle + \langle E_{01}|E_{01}\rangle = 1$$
$$\langle E_{10}|E_{10}\rangle + \langle E_{11}|E_{11}\rangle = 1$$

$$\langle E_{00}|E_{10}\rangle + \langle E_{01}|E_{11}\rangle = 0$$
$$\langle E_{10}|E_{00}\rangle + \langle E_{11}|E_{10}\rangle = 0$$

To pass the test, Eve must cause a low error rate. To get information she must keep her states distinguishable. These turn out to be incompatible goals.

Error and Information

By measuring error rates, Alice and Bob learn something about Eve's attack:

$$P(0_z \to 1_z) = \langle E_{01} | E_{01} \rangle \quad P(0_x \to 1_x) = \frac{1}{2}\left(1 + \Re(\langle E_{00} | E_{01} \rangle - \langle E_{00} | E_{11} \rangle - \langle E_{01} | E_{10} \rangle + \langle E_{10} | E_{11} \rangle)\right)$$

$$P(1_z \to 0_z) = \langle E_{10} | E_{10} \rangle \quad P(1_x \to 0_x) = \frac{1}{2}\left(1 - \Re(\langle E_{00} | E_{01} \rangle + \langle E_{00} | E_{11} \rangle + \langle E_{01} | E_{10} \rangle + \langle E_{10} | E_{11} \rangle)\right)$$

Laws of large numbers guarantee Alice and Bob that the error rate they measure is close to the above quantities when large numbers of bits are considered. To pass the test, the above quantities must be small. Recall the attack in the z basis:

$$|00...0\rangle |0_z\rangle_A \to |E_{00}\rangle |0_z\rangle_B + |E_{01}\rangle |1_z\rangle_B$$
$$|00...0\rangle |1_z\rangle_A \to |E_{10}\rangle |0_z\rangle_B + |E_{11}\rangle |1_z\rangle_B$$

If Eve's attack is to give good information in the z basis her states should be as close to orthogonal as possible, so the following should be small

$$\langle E_{00} | E_{10} \rangle, \ \langle E_{00} | E_{11} \rangle, \ \langle E_{01} | E_{10} \rangle, \ \langle E_{01} | E_{11} \rangle$$

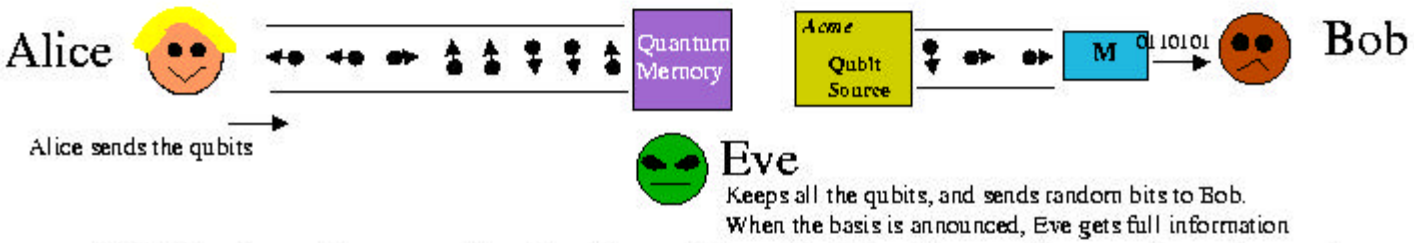
However, if the above are small, and the z error rate is small, this forces the x error rate to be large. Since the x error rate must be small enough to pass the test, then the above cannot be too small, and Eve cannot tell her states apart well. And hence cannot learn what Alice sent

Measure of Security

In quantum cryptography, a final key is formed when the test is passed. We would like to show that this key is secure:

$$I(A;E|T=pass)<e^{(\alpha-\beta n)}$$

This unfortunately, is not true. Consider the following attack:



While the above attack gives Eve full information, she almost never passes the test.

$$I(A;E|T=pass)=1 \qquad P(T=pass) \leq e^{\frac{-n}{16}}$$

This attack forces us to adopt a new security parameter. Either information is small, or the probability of passing the test is small:

$$P(T=pass)I(A;E|T=pass)\leq e^{\alpha-\beta n}$$

BB84 (Cont.)

- To detect the effects of Eve, Alice selects a random subset of the qubits to be announced as test bits. Alice and Bob compare these bits to learn the error rate.
- If the error rate is small enough, the test is "passed" and Alice announces the error correction information so Bob can correct his errors.
- Now, Alice and Bob have the same strings, but Eve may have some information. Alice announces privacy amplification information to reduce Eve's information to zero.

BB’84 vs. EPR Scheme

- BB’84 + teleportation is equivalent to the following protocol:

•Share EPR pairs

•Alice and Bob measure their qubits randomly in x and z basis. If their basis choice agrees on a pair then they know each other’s bits, otherwise their measurement results are uncorrelated.

•Alice announces her basis choice over the public channel. Now Bob knows the bit locations where they agree.

•The rest of the protocol is the same as in BB’84

Error Correction

- Alice sends a string *i*. Bob receives a string *j*. We assume they use a linear code with a parity check matrix *H* which is known to Eve. Alice announces on the classical channel: $H \cdot i_{info} = x_{Alice}$
- Bob computes:

$$H \cdot j_{info} = x_{Bob}$$

- Hence, Bob learns the syndrome of the errors:

$$H \cdot \left(i_{info} \oplus j_{info} \right) = x_{Alice} \oplus x_{Bob}$$

- *This syndrome gives info to Eve! It must be considered in the proof!*

Privacy Amplification

- Since Eve's gets some information from her attack and from the ECC syndrome, measures must be taken to reduce Eve's information.
- After Bob's errors are corrected, he knows Alice's string exactly. The key is defined by parities on this string:

$$k_l \equiv v_l \cdot i_{info}$$

- If Eve does not know even one bit in the bit mask for that key bit, she knows nothing about that key bit. Clearly there will be constraints on the *v*'s for security (e.g. no two can be the same).

Assumptions in Our Proof

- Error correction is a parity check code.
- All errors are to the maximum benefit of Eve.
- Bob waits to learn the basis before measuring. This may be assumed without loss of generality, it does not actually require Bob to have a Quantum Memory.
- We consider only symmetric attacks for Eve, which make some of the variables (j_T and i_I) independent. This may be done without loss of generality.

Eve's State

- With Alice's knowledge one may write Eve's transformation:

$$\left|0\right\rangle_{Eve}\left|i_{test}\right\rangle\left|i_{info}\right\rangle \xrightarrow{U_{Eve}} \sum_{j_t,j_i}\left|E'_{i_t,i_i,j_t,j_i}\right\rangle\left|j_{test}\right\rangle\left|j_{info}\right\rangle$$

- After the test bits are measured the state of Eve and Bob becomes:

$$\left|y_{i_I}\right\rangle = \sum_{j_I}\left|E_{i_I,j_I}\right\rangle\left|j_I\right\rangle$$

- With:

$$\left|E_{i_I,j_I}\right\rangle \equiv \frac{\left|E'_{i_I,j_I,i_T,j_T}\right\rangle}{\sqrt{\Pr\left(j_T \mid i_T,i_I,b,s\right)}}$$

Eve's State (Cont.)

- The distribution of Eve's states for all cases of Bob's states is:

$$r_{Eve} \equiv tr_{Bob}\left(\left|y_i\right\rangle\left\langle y_i\right|\right) = \sum_j \left|E_{i,j}\right\rangle\left\langle E_{i,j}\right|$$

- Being generous people, we can assume that Eve keeps a state: $\left|j_i\right\rangle = \sum_j \left|E_{i,j}\right\rangle_1 \left|i \oplus j\right\rangle_2$

- This is only more informative to Eve since:

$$tr_2\left(\left|j_i\right\rangle\left\langle j_i\right|\right) = \sum_j \left|E_{i,j}\right\rangle\left\langle E_{i,j}\right| = r_{Eve}$$

A New Basis for Eve's States

- We define a new basis for Eve's states:

$$\left|h_i\right\rangle \equiv \frac{1}{2^n}\sum_l (-1)^{i\cdot l}\left|j_l\right\rangle \qquad \left|j_l\right\rangle = \sum_i (-1)^{i\cdot l} d_i \left|\hat{h}_i\right\rangle$$

$$d_i^{\,2} \equiv \left\langle h_i \middle| h_i \right\rangle$$

- This d turns out to have a meaning:

$$d_c^{\,2} = \frac{1}{2^{2n}}\sum_l \sum_k (-1)^{c\cdot k} \sum_j \left\langle E_{l,j} \middle| E_{l\oplus k, j\oplus k} \right\rangle$$

$$= \Pr\left(j_I = i_I \oplus c_I \mid i_T, j_T, \bar{b}_I, b_T, s\right)$$

Bounding Eve's Information I

(episode I: The Quantum Menace)

- If two quantum states (ρ_0, ρ_1) are sent with equal probability, the mutual information of any measurement is bounded by:

$$I \le \frac{1}{2} tr\left| r_0 - r_1 \right|$$

•Using the above, Eve's mutual information on one key bit, given all classical information and all other bits is bounded (α is general, v is the minimum distance of the PA and ECC)

$$I_{Eve} \le a + \frac{1}{a} \sum_{|c| > \hat{v}/2} d_c^{\,2}$$

Security Criterion

- Since mutual information is not small for all attacks (consider the measure/resend), we use the following security criterion:

$$\sum_{i_T, c_T, b, s} \Pr(Test = pass, i_T, c_T, b, s) I(A; E \mid i_T, c_T, b, s) \leq Ae^{-bn}$$

  - If the above is met, then the somewhat more intuitive criterion is also met:

$$\Pr\left(Test = pass \wedge I_{Eve} > Ae^{-bn/2}\right) \leq e^{-bn/2}$$

Bounding Eve's Information II

(episode II: Probability Strikes Back)

- Using the meaning of d^2 we obtain:

$$I_{Eve} \le a + \frac{1}{a} \sum_{|c_I| > \hat{v}/2} \Pr\left(c_I \mid i_T, c_T, \bar{b}_I, b_T, s\right)$$

- Averaging the above, gives the following:

$$\sum_{i_T, c_T} \Pr\left(Test = pass, i_T, c_T \mid b, s\right) I\left(A; E \mid i_T, c_T, b, s\right)$$

$$\le a + \frac{1}{a} \sum_{\substack{|c_I| > \hat{v}/2 \\ |c_T| < np_a}} \Pr\left(c_I, c_T \mid \bar{b}_I, b_T, s\right)$$

Bounding Eve's Information III

(episode III: Return of Classical Probabilities)

- By averaging over all basis choices, we get:

$$\sum_{i_T, c_T, b} \Pr(Test = pass, i_T, c_T, b \mid s) I(A; E \mid i_T, c_T, b, s)$$

$$\leq a + \frac{1}{a} \sum_{b} \Pr(b) \sum_{\substack{|c_I| > \hat{v}/2 \\ |c_T| < np_a}} \Pr(c_I, c_T \mid \bar{b}_I, b_T, s)$$

$$= a + \frac{1}{a} \sum_{b} \Pr(b) \sum_{\substack{|c_I| > \hat{v}/2 \\ |c_T| < np_a}} \Pr(c_I, c_T \mid b_I, b_T, s)$$

Bounding Eve's Information III (Cont)

Now we set the parameter v, and average over orders (s):

$$\hat{v} = 2n(p_a + e)$$

$$\sum_{i_T, c_T, b} \Pr(Test = pass, i_T, c_T, b, s) I(A; E \mid i_T, c_T, b, s)$$

$$= a + \frac{1}{a} \sum_{b,s} \Pr(b,s) \sum_{\substack{|c_I| > n(p_a+e) \\ |c_T| < np_a}} \Pr(c_I, c_T \mid b, s)$$

$$= a + \frac{1}{a} \Pr(|c_I| > n(p_a + e), |c_T| < np_a)$$

$$\leq 2\sqrt{\Pr(|c_I| > n(p_a + e), |c_T| < np_a)}$$

The last line can be bounded with Hoeffding's bound.

Hoeffding's Bound

Hoeffding's bound may be applied to bound the probability of a mean of a set being different from the sampled mean. This is what is needed to bound the mutual information:

$$\sum_{i_T, c_T, b} \Pr\left(Test = pass, i_T, c_T, b, s\right) I\left(A; E \mid i_T, c_T, b, s\right)$$

$$\leq 2\sqrt{\Pr(\mid c_I \mid > n(p_a + e), \mid c_T \mid < np_a)}$$

$$\leq 2\sqrt{e^{-\frac{ne^2}{2}}}$$

Security has been shown, but this assumes that a code with the desired distance properties is available.

Reliability of the Key

- For high error protection we want the allowed error rate (p_a) to be as large as possible.
- For an (n,k,d) RLC $d/n>\delta$ except with:

$$\Pr(d/n < d) \le \frac{c(d)}{\sqrt{n}} 2^{n(H_2(d)-r/n)}$$

- If $\delta=(p_a+e)+1/n$, then almost all errors will be corrected (except an exponentially small fraction).

Security of the Key

- Recall the minimum distance of the PA+ECC is $v=2n(p_a+e)$. v is bounded below by the distance of the dual of the ECC+PA, which is a code:

$$\left(n, r^{\perp}, d^{\perp}\right), \text{where } d^{\perp} = n - r - m$$

$$\Pr\left(d^{\perp}/n < d^{\perp}\right) \leq \frac{c\left(d^{\perp}\right)}{\sqrt{n}} 2^{n\left(H_2\left(d^{\perp}\right) - (r-m-n)/n\right)}$$

  - With the following choice: $d^{\perp} = 2\left(p_a + e\right)$
  - Forcing all these probabilities to be exponentially small gives secrecy rates

Secrecy Rates for RLC

- To get exponentially small bounds in *n*, all the exponents need to be negative, which gives:

$$H_2(p_a + e + 1/n) < r/n$$

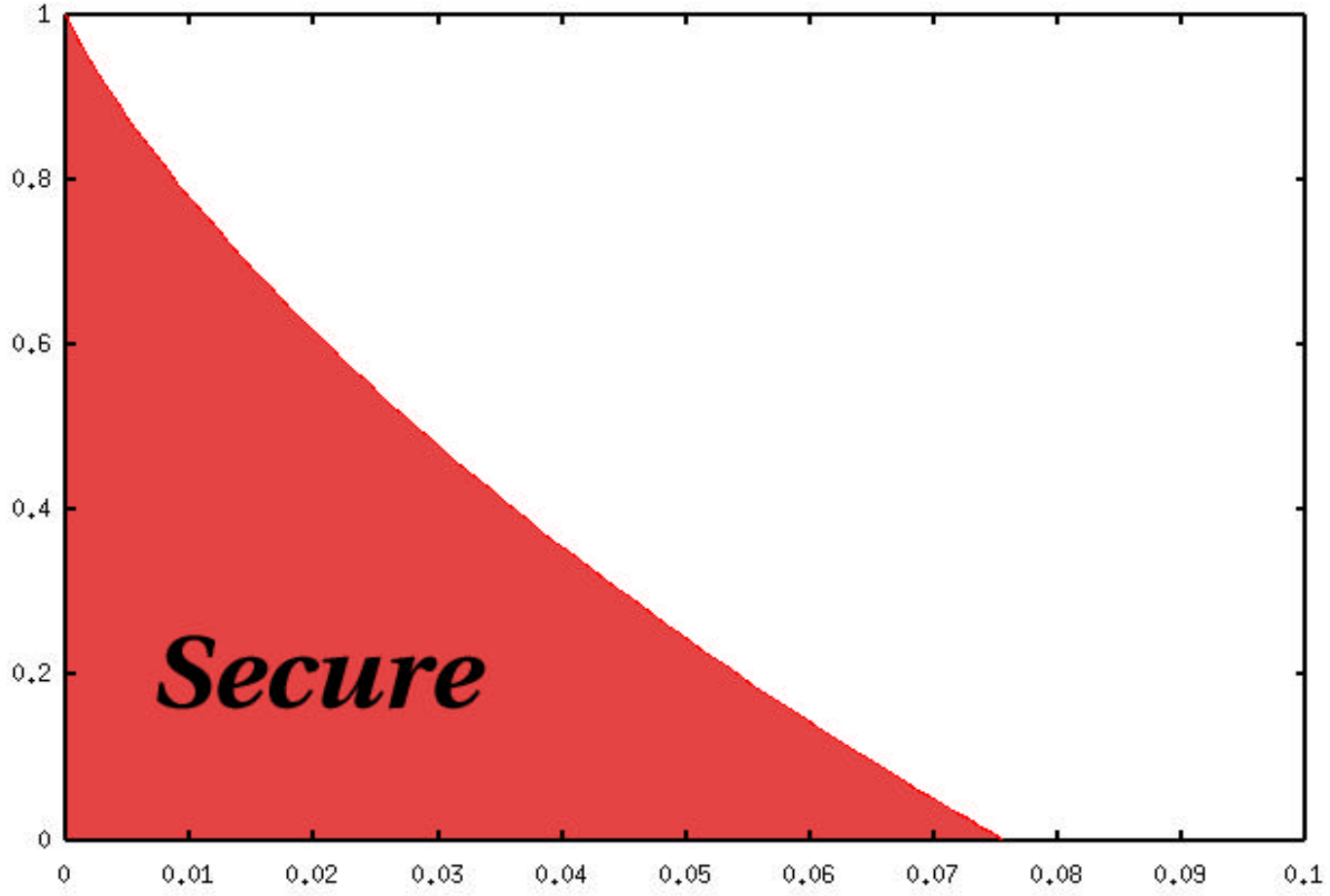
$$H_2(2p_a + 2e) + H_2(p_a + e + 1/n) < 1 - R_{secret}$$

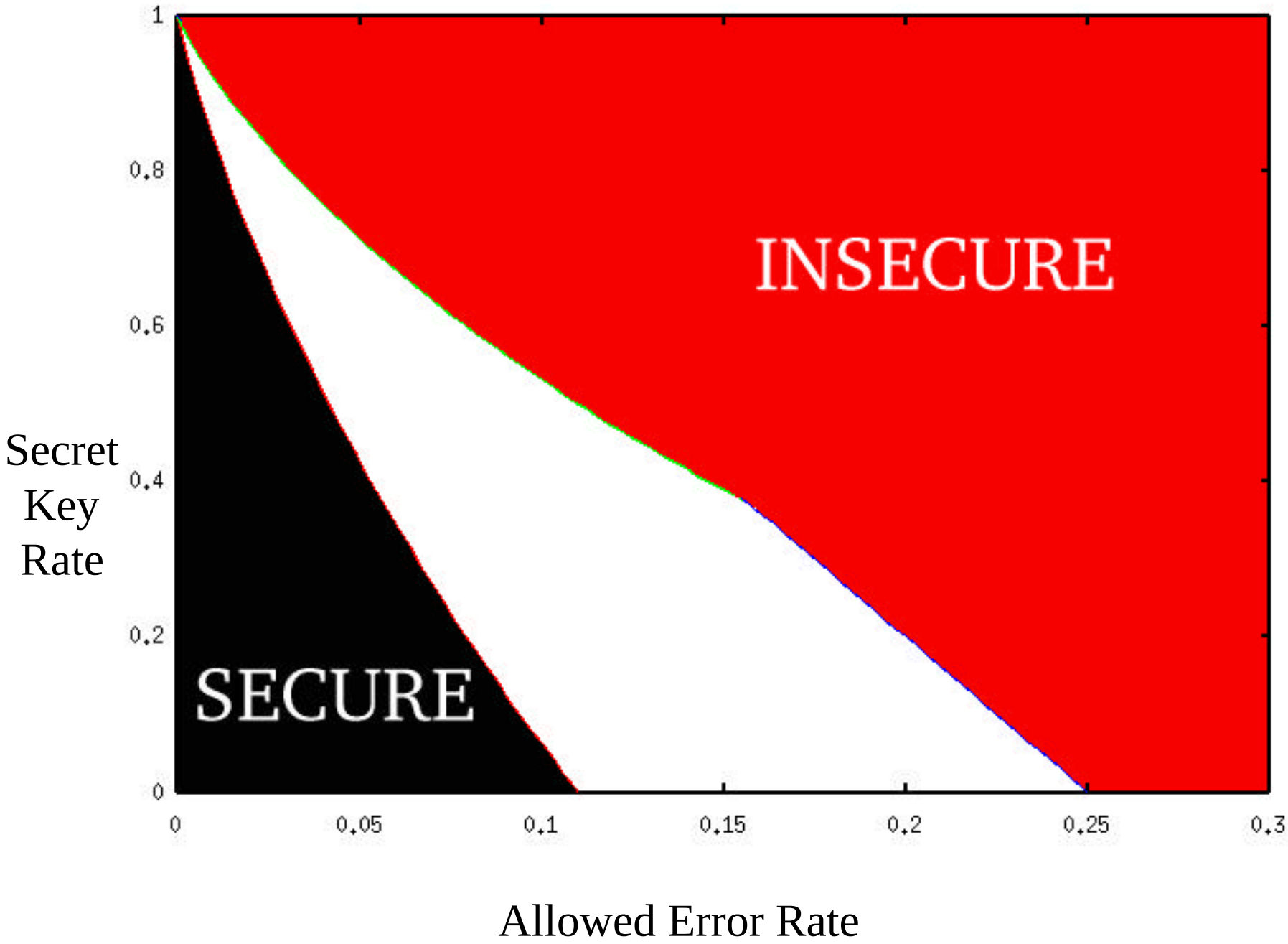
- As *n* tends to infinity, and ε tends to zero we have security when:

$$R_{secret} < 1 - H_2(2p_a) - H_2(p_a)$$

Plot of Secrecy Rate

$$R_{secret} < 1 - H_2(2p_a) - H_2(p_a)$$




Secret Key Rate
1
0.8
0.6
0.4
0.2
0
INSECURE
SECURE
0
0.05
0.1
0.15
0.2
0.25
0.3
Allowed Error Rate

Summary

- Theoretical BB84 is secure for users with a quantum channel and classical resources.
- A lower bound on secret key rates is obtained which is valid for all attacks.
- A threshold of 7.56% is obtained using RLC.