Current Quantum Cryptography Algorithm Is Optimal: A Proof

Oscar Galindo, Vladik Kreinovich, and Olga Kosheleva

University of Texas at El Paso
El Paso, Texas 79968, USA
ogalindomo@miners.utep.edu, vladik@utep.edu, olgak@utep.edu

Why Quantum . . .
Quantum . . .
Remaining Problems . . .
Quantum Physics: . . .
Measurements in . . .
Main Idea of Quantum . . .
A General Family of . . .
What Do We Want to . . .
Analyzing the . . .

1. Why Quantum Computing

- In many practical problems, we need to process large amounts of data in a limited time.
- To be able to do it, we need computations to be as fast as possible.
- Computations are already fast.
- However, there are many important problems for which we still cannot get the results on time.
- For example, we can predict with a reasonable accuracy where the tornado will go in the next 15 minutes.
- However, these computations take days on the fastest existing high performance computer.
- One of the main limitations: the speed of all the processes is limited by the speed of light $c \approx 3 \cdot 10^5$ km/sec.

Why Quantum . . .
Quantum . . .
Remaining Problems . . .
Quantum Physics: . . .
Measurements in . . .
Main Idea of Quantum . . .
A General Family of . . .
What Do We Want to . . .
Analyzing the . . .

2. Why Quantum Computing (cont-d)

- For a laptop of size ≈ 30 cm, the fastest we can send a signal across the laptop is $\dfrac{30\text{ cm}}{3\cdot 10^5\text{ km/sec}} \approx 10^{-9}$ sec.
- During this time, a usual few-Gigaflop laptop performs quite a few operations.
- To further speed up computations, we thus need to further decrease the size of the processors.
- We need to fit Gigabytes of data – i.e., billions of cells – within a small area.
- So, we need to attain a very small cell size.
- At present, a typical cell consists of several dozen molecules.
- As we decrease the size further, we get to a few-molecule size.

Why Quantum . . .
Quantum . . .
Remaining Problems . . .
Quantum Physics: . . .
Measurements in . . .
Main Idea of Quantum . . .
A General Family of . . .
What Do We Want to . . .
Analyzing the . . .

3. Why Quantum Computing (cont-d)

- At this size, physics is different: quantum effects become dominant.
- At first, quantum effects were mainly viewed as a nuisance.
- For example, one of the features of quantum world is that its results are usually probabilistic.
- So, if we simply decrease the cell size but use the same computer engineering techniques, then:
  - instead of getting the desired results all the time,
  - we will start getting other results with some probability.
- This probability of undesired results increases as we decrease the size of the computing cells.

Why Quantum . . .
Quantum . . .
Remaining Problems . . .
Quantum Physics: . . .
Measurements in . . .
Main Idea of Quantum . . .
A General Family of . . .
What Do We Want to . . .
Analyzing the . . .

4. Why Quantum Computing (cont-d)

- However, researchers found out that:
  - by appropriately modifying the corresponding algorithms,
  - we can avoid the probability-related problem and, even better, make computations faster.
- The resulting algorithms are known as algorithms of *quantum computing*.

Why Quantum . . .
Quantum . . .
Remaining Problems . . .
Quantum Physics: . . .
Measurements in . . .
Main Idea of Quantum . . .
A General Family of . . .
What Do We Want to . . .
Analyzing the . . .

5. Quantum Computing Will Enable Us to Decode All Traditionally Encoded Messages

- One of the spectacular algorithms of quantum computing is Shor's algorithm for fast factorization.
- Most encryption schemes – the backbone of online commerce – are based on the RSA algorithm.
- This algorithm is based on the difficulty of factorizing large integers.
- To form an at-present-unbreakable code, the user selects two large prime numbers P_1 and P_2.
- These numbers form his private code.
- He then transmits to everyone their product $n = P_1 \cdot P_2$ that everyone can use to encrypt their messages.
- At present, the only way to decode this message is to know the values P_i.

6. Quantum Computing Can Decode All Traditionally Encoded Messages (cont-d)

- Shor's algorithm allows quantum computers to effectively find P_i based on n.
- Thus, it can read practically all the secret messages that have been sent so far.
- This is one governments invest in the design of quantum computers.

Why Quantum . . .
Quantum . . .
Remaining Problems . . .
Quantum Physics: . . .
Measurements in . . .
Main Idea of Quantum . . .
A General Family of . . .
What Do We Want to . . .
Analyzing the . . .

7. Quantum Cryptography: an Unbreakable Alternative to the Current Cryptographic Schemes

- That RSA-based cryptographic schemes can be broken by quantum computing.
- However, this does not mean that there will be no secrets.
- Researchers have invented a quantum-based encryption scheme that cannot be thus broken.
- This scheme, by the way, is already used for secret communications.

Why Quantum ...
Quantum ...
Remaining Problems ...
Quantum Physics: ...
Measurements in ...
Main Idea of Quantum ...
A General Family of ...
What Do We Want to ...
Analyzing the ...

8. Remaining Problems And What We Do in This Talk

- In addition to the current cryptographic scheme, one can propose its modifications.
- This possibility raises a natural question: which of these scheme is the best?
- In this talk, we show that the current cryptographic scheme is, in some reasonable sense, optimal.

Why Quantum . . .
Quantum . . .
Remaining Problems . . .
Quantum Physics: . . .
Measurements in . . .
Main Idea of Quantum . . .
A General Family of . . .
What Do We Want to . . .
Analyzing the . . .

9. Quantum Physics: Possible States

- One of the main ideas behind quantum physics is that in the quantum world,
  - in addition to the regular states,
  - we can also have linear combinations of these states, with complex coefficients.
- Such combinations are known as *superpositions*.
- A single 1-bit memory cell in the classical physics can only have states 0 and 1.
- In quantum physics, these states are denoted by $|0\rangle$ and $|1\rangle$.
- We can also have superpositions $c_0 \cdot |0\rangle + c_1 \cdot |1\rangle$, where c_0 and c_1 are complex numbers.

Why Quantum . . .
Quantum . . .
Remaining Problems . . .
Quantum Physics: . . .
Measurements in . . .
Main Idea of Quantum . . .
A General Family of . . .
What Do We Want to . . .
Analyzing the . . .

10. Measurements in Quantum Physics

- What will happen if we try to measure the bit in the superposition state $c_0 \cdot |0\rangle + c_1 \cdot |1\rangle$?
- According to quantum physics, as a result of this measurement, we get:
  - 0 with probability $|c_0|^2$ and
  - 1 with probability $|c_1|^2$.
- After the measurement, the state also changes:
  - if the measurement result is 0, the state will turn into $|0\rangle$, and
  - if the measurement result is 1, the state will turn into $|1\rangle$.

Why Quantum . . .
Quantum . . .
Remaining Problems . . .
Quantum Physics: . . .
Measurements in . . .
Main Idea of Quantum . . .
A General Family of . . .
What Do We Want to . . .
Analyzing the . . .

11. Measurements in Quantum Physics (cont-d)

- Since we can get either 0 or 1, the corresponding probabilities should add up to 1; so:
  - for the expression $c_0 \cdot |0\rangle + c_1 \cdot |1\rangle$ to represent a physically meaningful state,
  - the coefficients c_0 and c_1 must satisfy the condition

$$|c_0|^2 + |c_1|^2 = 1.$$

Why Quantum . . .
Quantum . . .
Remaining Problems . . .
Quantum Physics: . . .
Measurements in . . .
Main Idea of Quantum . . .
A General Family of . . .
What Do We Want to . . .
Analyzing the . . .

12. Operations on Quantum States

- We can perform *unitary* operations, i.e., linear transformations that preserve the property

$$|c_0|^2 + |c_1|^2 = 1.$$

- A simple example of a unary transformation is *Walsh-Hadamard (WH)* transformation:

$$|0\rangle \to |0'\rangle \stackrel{\text{def}}{=} \frac{1}{\sqrt{2}} \cdot |0\rangle + \frac{1}{\sqrt{2}} \cdot |1\rangle;$$

$$|1\rangle \to |1'\rangle \stackrel{\text{def}}{=} \frac{1}{\sqrt{2}} \cdot |0\rangle - \frac{1}{\sqrt{2}} \cdot |1\rangle.$$

- What is the geometric meaning of this transformation?

Why Quantum . . .
Quantum . . .
Remaining Problems . . .
Quantum Physics: . . .
Measurements in . . .
Main Idea of Quantum . . .
A General Family of . . .
What Do We Want to . . .
Analyzing the . . .

13. Operations on Quantum States (cont-d)

- By linearity: $c'_0 \cdot |0'\rangle + c'_1 \cdot |1'\rangle =$

$$c'_0 \cdot \left(\frac{1}{\sqrt{2}} \cdot |0\rangle + \frac{1}{\sqrt{2}} \cdot |1\rangle\right) + c'_1 \cdot \left(\frac{1}{\sqrt{2}} \cdot |0\rangle - \frac{1}{\sqrt{2}} \cdot |1\rangle\right) =$$

$$\left(\frac{1}{\sqrt{2}} \cdot c'_0 + \frac{1}{\sqrt{2}} \cdot c'_1\right) \cdot |0\rangle + \left(\frac{1}{\sqrt{2}} \cdot c'_0 - \frac{1}{\sqrt{2}} \cdot c'_1\right) \cdot |1\rangle.$$

- Thus, $c'_0 \cdot |0'\rangle + c'_1 \cdot |1'\rangle = c_0 \cdot |0\rangle + c_1 \cdot |1\rangle$, where

$$c_0 = \frac{1}{\sqrt{2}} \cdot c'_0 + \frac{1}{\sqrt{2}} \cdot c'_1 \text{ and } c_1 = \frac{1}{\sqrt{2}} \cdot c'_0 - \frac{1}{\sqrt{2}} \cdot c'_1.$$

- Let us represent each of the two pairs (c_0, c_1) and (c'_0, c'_1) as a point in the 2-D plane (x, y).
- Then the above transformation resembles the formulas for a clockwise rotation by an angle θ:

$$x' = \cos(\theta) \cdot x + \sin(\theta) \cdot y;$$

$$y' = -\sin(\theta) \cdot x + \cos(\theta) \cdot y.$$

Why Quantum . . .
Quantum . . .
Remaining Problems . . .
Quantum Physics: . . .
Measurements in . . .
Main Idea of Quantum . . .
A General Family of . . .
What Do We Want to . . .
Analyzing the . . .

14. Operations on Quantum States (cont-d)

- Specifically, for $\theta = 45^\circ$, we have $\cos(\theta) = \sin(\theta) = \dfrac{1}{\sqrt{2}}$ and thus, the rotation takes the form

$$x' = \frac{1}{\sqrt{2}} \cdot x + \frac{1}{\sqrt{2}} \cdot y; \quad y' = -\frac{1}{\sqrt{2}} \cdot x + \frac{1}{\sqrt{2}} \cdot y.$$

- In these terms, can see that the WH transformation from (c_0', c_1') and (c_0, c_1) is:
  - a rotation by 45 degrees
  - followed by a reflection with respect to the x-axis: $(c_0, c_1) \to (c_0, -c_1)$.
- One can check that if we apply WH transformation twice, then we get the same state as before.

Why Quantum . . .
Quantum . . .
Remaining Problems . . .
Quantum Physics: . . .
Measurements in . . .
Main Idea of Quantum . . .
A General Family of . . .
What Do We Want to . . .
Analyzing the . . .

15. Operations on Quantum States (cont-d)

- Indeed, due to linearity,

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

$$\frac{1}{\sqrt{2}}\cdot WH(|0\rangle) + \frac{1}{\sqrt{2}}\cdot WH(|1\rangle) =$$

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

$$|0\rangle.$$

- Similarly, $\mathrm{WH}(|1'\rangle) = |1\rangle$.

Why Quantum . . .
Quantum . . .
Remaining Problems . . .
Quantum Physics: . . .
Measurements in . . .
Main Idea of Quantum . . .
A General Family of . . .
What Do We Want to . . .
Analyzing the . . .

16. Measurements of Quantum 1-Bit Systems

- According to quantum measurement:
  - if we measure the bit 0 or 1 in each of the states $|0'\rangle$ or $|1'\rangle$,
  - then we will get 0 or 1 with equal probability 1/2.
- So, if we measure 0 or 1, then:
  - if we are in the state $|0\rangle$, then the state does not change and we get 0 with probability 1;
  - if we are in the state $|1\rangle$, then the state does not change and we get 1 with probability 1;
  - if we are in one of the states $|0'\rangle$ or $|1'\rangle$, then:
    * with probability 1/2, we get the measurement result 0 and the state changes into $|0\rangle$; and
    * with probability 1/2, we get the measurement result 1 and the state changes into $|1\rangle$.

Why Quantum . . .
Quantum . . .
Remaining Problems . . .
Quantum Physics: . . .
Measurements in . . .
Main Idea of Quantum . . .
A General Family of . . .
What Do We Want to . . .
Analyzing the . . .

17. Case of Quantum 1-Bit Systems (cont-d)

- We can also measure whether we have $|0'\rangle$ or $|1'\rangle$.
- In this case, similarly:
  - if we are in the state $|0'\rangle$, then the state does not change and we get $0'$ with probability 1;
  - if we are in the state $|1'\rangle$, then the state does not change and we get $1'$ with probability 1;
  - if we are in one of the states $|0\rangle$ or $|1\rangle$, then:
    * with probability $1/2$, we get the measurement result $0'$ and the state changes into $|0'\rangle$; and
    * with probability $1/2$, we get the measurement result $1'$ and the state changes into $|1'\rangle$.

Why Quantum . . .
Quantum . . .
Remaining Problems . . .
Quantum Physics: . . .
Measurements in . . .
Main Idea of Quantum . . .
A General Family of . . .
What Do We Want to . . .
Analyzing the . . .

18. Main Idea of Quantum Cryptography

- The sender – who, in cryptography, is usually called Alice – sends each bit
  - either as $|0\rangle$ or $|1\rangle$ (this orientation is usually denoted by $+$)
  - or as $|0'\rangle$ or $|1'\rangle$ (this orientation is usually denoted by $\times$).
- The receiver – who, in cryptography, is usually called Bob – tries to extract the information from the signal.
- Extracting numerical information from a physical object is nothing else but measurement.
- Thus, to extract the information from Alice's signal, Bob needs to perform some measurement.
- Since Alice uses one of the two orientations $+$ or $\times$, it is reasonable for Bob to also use one of these orientations.

Why Quantum ...
Quantum ...
Remaining Problems ...
Quantum Physics: ...
Measurements in ...
Main Idea of Quantum ...
A General Family of ...
What Do We Want to ...
Analyzing the ...

19. Sender and Receiver Must Use the Same Orientation

- If for some bit:
  - Alice and Bob use the same orientation,
  - then Bob will get the exact same signal that Alice has sent.
- The situation is completely different if Alice and Bob use different orientations.
- For example, assume that:
  - Alice sends a 0 bit in the $\times$ orientation, i.e., sends the state $|0'\rangle$, and
  - Bob uses the $+$ orientation to measure the signal.

20. We Need Same Orientation (cont-d)

- For the state $|0'\rangle = \frac{1}{\sqrt{2}} \cdot |0\rangle + \frac{1}{\sqrt{2}} \cdot |1\rangle$:
  - with probability $\left|\frac{1}{\sqrt{2}}\right|^2 = \frac{1}{2}$, Bob will measure 0, and
  - with probability $\left|\frac{1}{\sqrt{2}}\right|^2 = \frac{1}{2}$, Bob will measure 1.
- The same results, with the same probabilities, will happen if Alice sends a 1 bit in the $\times$ orientation, i.e., $|1'\rangle$.
- Thus, by observing the measurement result, Bob will not be able to tell whether Alice send 0 or 1.
- The information will be lost.
- Similarly, the information will be lost if Alice uses a $+$ orientation and Bob uses a $\times$ orientation.

21. What If We Have an Eavesdropper?

- What if an eavesdropper – usually called Eve – gains access to the same communication channel?
- In non-quantum eavesdropping, Eve can measure each bit that Alice sends and thus, get the whole message.
- In non-quantum physics, measurement does not change the signal.
- Thus, Bob gets the same signal that Alice has sent.
- Neither Alice not Bob will know that somebody eavesdropped on their communication.
- In quantum physics, the situation is different.
- One of the main features of quantum physics is that measurement, in general, changes the signal.
- Eve does not know in which of the two orientations each bit is sent.

Why Quantum . . .
Quantum . . .
Remaining Problems . . .
Quantum Physics: . . .
Measurements in . . .
Main Idea of Quantum . . .
A General Family of . . .
What Do We Want to . . .
Analyzing the . . .

22. What If We Have an Eavesdropper (cont-d)

- So, she can select the wrong orientation for her measurement.
- As a result, e.g.,
  - if Alice and Bob agreed to use the $\times$ orientation for transmitting a certain bit,
  - but Eve selects a $+$ orientation,
  - then Eve's measurement will change Alice's signal – and Bob will only get the distorted message.
- For example, if Alice sent $|0'\rangle$, then:
  - after Eve's measurement,
  - the signal will become either $|0\rangle$ or $|1\rangle$, with probability $1/2$ of each of these options.

Why Quantum . . .
Quantum . . .
Remaining Problems . . .
Quantum Physics: . . .
Measurements in . . .
Main Idea of Quantum . . .
A General Family of . . .
What Do We Want to . . .
Analyzing the . . .

23. What If We Have an Eavesdropper (cont-d)

- In each of the options:
  - when Bob measures the resulting signal ($|0\rangle$ or $|1\rangle$) by using his agreed-upon $\times$ orientation ($|0'\rangle, |1'\rangle$),
  - Bob will get 0 or 1 with probability 1/2 – instead of the original signal that Alice has sent.

Why Quantum . . .
Quantum . . .
Remaining Problems . . .
Quantum Physics: . . .
Measurements in . . .
Main Idea of Quantum . . .
A General Family of . . .
What Do We Want to . . .
Analyzing the . . .

24. Quantum Cryptography Helps to Detect an Eavesdropper

- If there is an eavesdropper, then:
  - with certain probability,
  - the signal received by Bob will be different from what Alice sent.
- Thus, by comparing what Alice sent with what Bob received, we can see that something was interfering.
- Thus, we will be able to detect the presence of the eavesdropper.
- Let us describe how this idea is implemented in the current quantum cryptography algorithm.

Why Quantum . . .
Quantum . . .
Remaining Problems . . .
Quantum Physics: . . .
Measurements in . . .
Main Idea of Quantum . . .
A General Family of . . .
What Do We Want to . . .
Analyzing the . . .

25. Sending a Preliminary Message

- Before Alice sends the actual message, she needs to check that the communication channel is secure.
- For this purpose, Alice uses a random number generator to select n random bits $b_1, \ldots, b_n$.
- Each of them is equal to 0 or 1 with probability $1/2$.
- These bits will be sent to Bob.
- Alice also selects n more random bits $r_1, \ldots, r_n$.
- Based on these bits, Alice sends the bits b_i as follows:
  - if $r_i = 0$, then the bit b_i is sent in $+$ orientation, i.e., Alice sends $|0\rangle$ if $b_i = 0$ and $|1\rangle$ if $b_i = 1$;
  - if $r_i = 1$, then the bit b_i is sent in $\times$ orientation, i.e., Alice sends $|0'\rangle$ if $b_i = 0$ and $|1'\rangle$ if $b_i = 1$.

Why Quantum . . .
Quantum . . .
Remaining Problems . . .
Quantum Physics: . . .
Measurements in . . .
Main Idea of Quantum . . .
A General Family of . . .
What Do We Want to . . .
Analyzing the . . .

26. Receiving the Preliminary Message

- Independently, Bob selects n random bits $s_1, \ldots, s_n$.
- They determine how he measures the signal that he receives from Alice:
  - if $s_i = 0$, then Bob measures whether the i-th received signal is $|0\rangle$ or $|1\rangle$;
  - if $s_i = 1$, then Bob measures whether the i-th received signal is $|0'\rangle$ or $|1'\rangle$.

27. Checking for Eavesdroppers

- After this, for k out of n bits, Alice openly sends to Bob her bits b_i and her orientations r_i.
- Bob sends to Alice his orientations s_i and the signals b'_i that he measured.
- In half of the cases, the orientations r_i and s_i should coincide.
- In which case, if there is no eavesdropper,
  - the signal b'_i measured by Bob
  - should coincide with the signal b_i that Alice sent.
- So, if $b'_i \neq b_i$ for some i, this means that there is an eavesdropper.
- If there is an eavesdropper, then with probability $1/2$, Eve will select a different orientation.

Why Quantum . . .
Quantum . . .
Remaining Problems . . .
Quantum Physics: . . .
Measurements in . . .
Main Idea of Quantum . . .
A General Family of . . .
What Do We Want to . . .
Analyzing the . . .

28. Checking for Eavesdroppers (cont-d)

- In half of such cases, the eavesdropping with change the original signal.
- So, for each bit, the probability that we will have $b'_i \neq b_i$ is equal to $1/4$.
- Thus, the probability that the eavesdropper will not be detected by this bit is $1 - 1/4 = 3/4$.
- The probability that Eve will not be detected in all $k/2$ cases is the product $(3/4)^{k/2}$.
- For a sufficiently large k, this probability of not-detecting-eavesdropping is very small.
- Thus, if $b'_i = b_i$ for all k bits i, this means that with high confidence, there is no eavesdropping.
- So, the communication channel between Alice and Bob is secure.

Why Quantum . . .
Quantum . . .
Remaining Problems . . .
Quantum Physics: . . .
Measurements in . . .
Main Idea of Quantum . . .
A General Family of . . .
What Do We Want to . . .
Analyzing the . . .

29. Preparing to Send a Message

- Now, for each of the remaining $(n-k)$ bits, Alice and Bob openly exchange orientations r_i and s_i.
- For half of these bits, these orientations must coincide.
- For these bits, since there is no eavesdropping, Alice and Bob know that:
  - the signal b'_i measured by Bob
  - is the same as the signal b_i sent to Alice.
- So, there are $B \stackrel{\text{def}}{=} (n-k)/2$ bits $b_i = b'_i$ that they both know but no one else knows.

Why Quantum . . .
Quantum . . .
Remaining Problems . . .
Quantum Physics: . . .
Measurements in . . .
Main Idea of Quantum . . .
A General Family of . . .
What Do We Want to . . .
Analyzing the . . .

30. Sending and Receiving the Actual Message

- Now, Alice takes the B-bit message $m_1, \ldots, m_B$ that she wants to send.
- She forms the encoded message $m'_i \stackrel{\text{def}}{=} m_i \oplus b_i$, where $\oplus$ means addition modulo 2 (same as exclusive or).
- Alice openly sends the encoded message m'_i.
- Upon receiving the message m'_i, Bob reconstructs the original message as $m_i = m'_i \oplus b_i$.

Why Quantum . . .
Quantum . . .
Remaining Problems . . .
Quantum Physics: . . .
Measurements in . . .
Main Idea of Quantum . . .
A General Family of . . .
What Do We Want to . . .
Analyzing the . . .

31. A General Family of Quantum Cryptography Algorithms: Description

- In the current quantum cryptography algorithm, Alice selects $+$ and $\times$ with probability 0.5.
- Similarly, Bob selects one of the two possible orientations $+$ and $\times$ with probability 0.5.
- It is therefore reasonable to consider a more general scheme, in which:
  - Alice selects the orientation $+$ with some probability a_+ (which is not necessarily equal to 0.5), and
  - Bob select the orientation $+$ with some probability b_+ (which is not necessarily equal to 0.5).
- Which a_+ and b_+ should they choose to make the connection maximally secure?
- I.e., to maximize the probability of detecting the eavesdropper?

Why Quantum . . .
Quantum . . .
Remaining Problems . . .
Quantum Physics: . . .
Measurements in . . .
Main Idea of Quantum . . .
A General Family of . . .
What Do We Want to . . .
Analyzing the . . .

32. What Do We Want to Maximize?

- We want to maximize the probability of detecting an eavesdropper.
- The eavesdropper also selects one of the two orientations $+$ or $\times$.
- Let e_+ be the probability with which the eavesdropper (Eve) select the orientation $+$.
- Then Eve will select $\times$ with the remaining probability $e_\times = 1 - e_+$.
- We know that Alice and Bob can only use bits for which their selected orientations coincide.
- If Eve selects the same orientation, then her observation will also not change this bit.
- Thus, we will not be able to detect the eavesdropping.

Why Quantum . . .
Quantum . . .
Remaining Problems . . .
Quantum Physics: . . .
Measurements in . . .
Main Idea of Quantum . . .
A General Family of . . .
What Do We Want to . . .
Analyzing the . . .

33. What Do We Want to Maximize (cont-d)

- We can detect the eavesdropping only when A and B have the same orientation, but E has a different one.
- There are two such cases:
  - the first case is when Alice and Bob select $+$ and Eve selects $\times$;
  - the second case is when Alice and Bob select $\times$ and Eve selects $+$.
- Alice, Bob, and Eve act independently.
- So, the probability of the 1st case is $p_1 = a_+ \cdot b_+ \cdot e_\times$, where:
  - a_+ is the probability that Alice selects $+$,
  - b_+ is the probability that Bob selects $+$,
  - $e_\times$ is the probability that Eve selects $\times$.

Why Quantum . . .
Quantum . . .
Remaining Problems . . .
Quantum Physics: . . .
Measurements in . . .
Main Idea of Quantum . . .
A General Family of . . .
What Do We Want to . . .
Analyzing the . . .

34. What Do We Want to Maximize (cont-d)

- Similarly, the probability p_2 of the 2nd case is $p_1 = a_\times \cdot b_\times \cdot e_+$
- These two cases are incompatible.
- So the overall probability p of detecting the eavesdropper is the sum of the above two probabilities:

$$p = a_+ \cdot b_+ \cdot e_\times + a_\times \cdot b_\times \cdot e_+.$$

- Taking into account that $a_\times = 1 - a_+$, $b_\times = 1 - b_+$, and $e_\times = 1 - e_+$, we get:

$$p = a_+ \cdot b_+ \cdot (1 - e_+) + (1 - a_+) \cdot (1 - b_+) \cdot e_+.$$

- This probability depends on Eve's selection e_+.
- We want to maximize the worst-case probability of detection, when Eve uses her best strategy:

$$J = \min_{e_+ \in [0,1]} \{a_+ \cdot b_+ \cdot (1 - e_+) + (1 - a_+) \cdot (1 - b_+) \cdot e_+\}.$$

35. Analyzing the Optimization Problem

- Once the values a_+ and b_+ are fixed, the expression that Eve wants to minimize is a linear function of e_+:

$$p = a_+ \cdot b_+ - a_+ \cdot b_+ \cdot e_+ + (1 - a_+) \cdot (1 - b_+) \cdot e_+ =$$

$$a_+ \cdot b_+ + e_+ \cdot ((1 - a_+) \cdot (1 - b_+) - a_+ \cdot b_+).$$

- We want to minimize this expression over all possible values of e_+ from the interval $[0, 1]$.
- A linear function on an interval always attains its min at one of the endpoints.
- Thus, to find the minimum of the above expression over e_+, it is sufficient:
  - to consider the two endpoints $e_+ = 0$ and $e_+ = 1$ of this interval, and
  - take the smallest of the resulting two values.

36. Analyzing the Optimization Problem (cont-d)

- For $e_+ = 0$, the expression becomes $a_+ \cdot b_+$.
- For $e_+ = 1$, the expression becomes $(1 - a_+) \cdot (1 - b_+)$.
- Thus, the minimum of the expression can be equivalently described as:

$$J = \min\{a_+ \cdot b_+, (1 - a_+) \cdot (1 - b_+)\}.$$

- We need to find the values a_+ and b_+ for which this quantity attains its largest possible value.
- Let us first, for each a_+, find the value b_+ for which the J attains its maximum possible value.
- In the formula for J, $a_+ \cdot b_+$, is increasing from 0 to a_+ as b_+ goes from 0 to 1.
- The second expression $(1-a_+)\cdot(1-b_+)$ decreases from $1 - a_+$ to 0 as b_+ goes from 0 to 1.

37. Analyzing the Optimization Problem (cont-d)

- Thus, for small b_+, the first of the two expressions is smaller.
- So, for these b_+, $J = a_+ \cdot b_+$ and is, thus, increasing with b_+;
- For larger b_+, the second of the two expressions is smaller.
- Thus for these b_+, $J = (1 - a_+) \cdot (1 - b_+)$ and is, so, decreasing with b_+.
- So J first increases and then decreases.
- Thus, its maximum is attained at a point when J switches from increasing to decreasing, i.e., where:

$$a_+ \cdot b_+ = (1 - b_+) \cdot (1 - a_+), \text{ i.e.,}$$

$$a_+ \cdot b_+ = 1 - a_+ - b_+ + a_+ \cdot b_+, \text{ so } b_+ = 1 - a_+.$$

Why Quantum . . .
Quantum . . .
Remaining Problems . . .
Quantum Physics: . . .
Measurements in . . .
Main Idea of Quantum . . .
A General Family of . . .
What Do We Want to . . .
Analyzing the . . .

38. Analyzing the Optimization Problem (cont-d)

- Substituting $b_+ = 1 - a_+$ into the formula for J, we get

$$J = \min\{a_+ \cdot (1 - a_+), (1 - a_+) \cdot a_+\} = a_+ \cdot (1 - a_+).$$

- We want to find the value a_+ that maximizes this expression: it is $a_+ = 0.5$.
- Since $b_+ = 1 - a_+$, we get $b_+ = 1 - 0.5 = 0.5$.
- Thus, the current quantum cryptography algorithm is indeed optimal.
- Similar arguments show:
  - that the best is to use 45 degrees rotation, and
  - that the best is to have 0s and 1s in b_i with probability 0.5.

Why Quantum . . .
Quantum . . .
Remaining Problems . . .
Quantum Physics: . . .
Measurements in . . .
Main Idea of Quantum . . .
A General Family of . . .
What Do We Want to . . .
Analyzing the . . .

39. Acknowledgments

This work was supported in part by the US National Science Foundation grant HRD-1242122 (Cyber-ShARE).

Why Quantum . . .
Quantum . . .
Remaining Problems . . .
Quantum Physics: . . .
Measurements in . . .
Main Idea of Quantum . . .
A General Family of . . .
What Do We Want to . . .
Analyzing the . . .