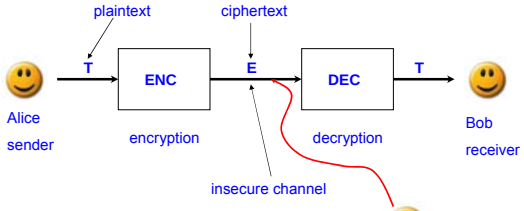
Cryptography

Lecture 9

Classical Cryptography



Eve
eavesdropper

- $ENC(T, K_E) = E$, with K_E the encryption key
- $DEC(E, K_D) = T$, with K_D the decryption key
- combining: $DEC(ENC(T,K_E),K_D) = T$

Encryption protocols

- Caesar's protocol:
  - *ENC* = *DEC* = shift(–,–), where shift (*T*,*n*)=*T*', the string obtained from *T* by shifting each character *n* steps
  - Original message and encrypted one highly correlated.
- One-Time-Pad protocol of Vernam cipher:
  - Alice generates a random number of bits and uses that as her random key *K*.
  - Assume Alice and Bob both share *K*:
    - $K_E = K_D = K$
    - $ENC(T, K) = DEC(T, K) = T \oplus K$
    - $DEC(ENC(T,K),K) = DEC(T \oplus K,K) = (T \oplus K) \oplus K = T \oplus (K \oplus K) = T$

One-Time-Pad protocol example

Original message T	0 1 1 0 1 1
Encryption key K	1 1 1 0 1 0
Encrypted message E	1 0 0 0 0 1
Public channel	↓ ↓ ↓ ↓ ↓ ↓
Received message E	1 0 0 0 0 1
Decryption key K	1 1 1 0 1 0
Decrypted message T	0 1 1 0 1 1

Two issues:
1) Generation of a new key *K* is required each time a new message is sent. Otherwise, the text can be discovered through statistical analysis. Hence the name "One-Time-Pad".
2) The protocol is secure only insofar as the key *K* is not intercepted by Eve.

Private key

So far, we assumed that the pair of keys K_E and K_D are kept secret. In fact, only one key was needed. A protocol where the two keys are computable from each other, and thus requiring that *both* keys be kept secret, is said to be private key.

Public-key cryptography

- RSA (Rivest, Shamir, and Adleman, 1978): the knowledge of one key does not enable us to calculate the second one, since the computation will be hard (more than polynomial in the length of the first key).
- Suppose Bob has such a pair of keys K_E and K_D:
  - K_E in public domain.
  - He can safely advertise the protocol, i.e., *ENC*(–,–) and *DEC*(–,–).
  - He guards K_D for himself.
  - Alice uses K_E on her message.
  - If Eve intercepts the encrypted text, she cannot retrieve Bob's decryption key, so the message is safe.
  - Bob has two computable functions:
    - $F_E(–) = ENC(–, K_E)$
    - $F_D(–) = DEC(–, K_D)$

F_E is a trapdoor function: easy to compute, hard to invert without extra information

Pros and cons of public-key cryptography

- Pro:
  - It solves the key distribution problem.
- Cons:
  - The computation of the private key from the public key *appears* to be hard.
  - Public-key protocols tend to be considerable slower than their private-key peers.
- Best of both worlds:
  - Use public-key cryptography to distribute a key K_E of some private-key protocol, rather than the entire text message. Once Alice and Bob safely share K_E they can use the faster private-key scheme.
  - Sending a binary K_E will be the only concern the rest of this class.

Other topics in cryptography

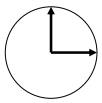
- Secure communication
- Intrusion detection: Alice and Bob would like to determine whether Eve is, in fact, eavesdropping.
- Authentication: we would like to ensure that nobody is impersonating Alice and sending false messages (outside the context of this course).

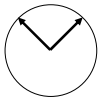
Quantum Key Exchange I: The BB84 Protocol

- 1984: Charles Bennett & Gilles Brassard introduced the first quantum key exchange (QKE) protocol, named BB84.
- Why using the quantum world?
  - Classical: Eve can make copies of arbitrary portions of the encrypted bit stream and store them somewhere.
  - Quantum: With qubits Eve cannot make perfect copies of the qubit stream due to the no-cloning theorem.
  - Classical: Eve can listen without affecting the bitstream, i.e., her eavesdropping does not leave traces.
  - Quantum: Measuring the qubit stream alters it.

BB84 protocol

- Alice wants to send Bob a key via a quantum channel.
- As in the One-Time-Pad protocol this key is a sequence of random (classical) bits.
- Alice will send a qubit each time she generates a new bit of her key.
- But which qubit should she send?
- She will use two different orthogonal bases:





"plus" basis $+ = \{|\rightarrow\rangle, |\uparrow\rangle\} = \{[1,0]^T, [0,1]^T\}$ "times" basis $\times = \{|\nwarrow\rangle, |\nearrow\rangle\} = \left\{\frac{1}{\sqrt{2}}[-1,1]^T, \frac{1}{\sqrt{2}}[1,1]^T\right\}$

State/Basis	+	x
$\|0\rangle$	$\|\rightarrow\rangle$	$\|\nearrow\rangle$
$\|1\rangle$	$\|\uparrow\rangle$	$\|\nwarrow\rangle$

- Basis states given by the table.
- What about superpositions?
  - If Bob measures photon using the + basis, he will only see photons as $|\rightarrow\rangle$ or $|\uparrow\rangle$.
  - What if Alice sends a $|\nearrow\rangle$ and Bob measures it in the + basis? Then it will be in a superposition of states

$$|\nearrow\rangle = \frac{1}{\sqrt{2}}|\uparrow\rangle + \frac{1}{\sqrt{2}}|\rightarrow\rangle$$

So there is a 50-50% chance of Bob's recording a $|0\rangle$ or a $|1\rangle$.

Four possible superpositions

- $|\nwarrow\rangle$ with respect to +, will be $\frac{1}{\sqrt{2}}|\uparrow\rangle - \frac{1}{\sqrt{2}}|\rightarrow\rangle$
- $|\nearrow\rangle$ with respect to +, will be $\frac{1}{\sqrt{2}}|\uparrow\rangle + \frac{1}{\sqrt{2}}|\rightarrow\rangle$
- $|\uparrow\rangle$ with respect to x, will be $\frac{1}{\sqrt{2}}|\nearrow\rangle + \frac{1}{\sqrt{2}}|\nwarrow\rangle$
- $|\rightarrow\rangle$ with respect to x, will be $\frac{1}{\sqrt{2}}|\nearrow\rangle - \frac{1}{\sqrt{2}}|\nwarrow\rangle$

BB84 step 1

- Alice flips a coin *n* times to determine which classical bits to send. She then flips the coin another *n* times to determine in which of the two bases to send those bits. She then sends the bits in their appropriate basis.
- Example for *n* = 12

Bit number	1	2	3	4	5	6	7	8	9	10	11	12
Alice's random bits	0	1	1	0	1	1	1	0	1	0	1	0
Alice's random basis	+	+	x	+	+	+	x	+	x	x	x	+
Alice sends	→	↑	↖	→	↑	↑	↖	→	↖	↗	↖	→
Quantum channel	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓

BB84 step 2

- As the sequence of qubits reaches Bob, he does not know which basis Alice used to send them, so to determine the basis by which to measure them he also tosses a coin. He then goes on to measure the qubit in those random bases.
- In our example:

Bit number	1	2	3	4	5	6	7	8	9	10	11	12
Bob's random bases	x	+	x	x	+	x	+	+	x	x	x	+
Bob observes	↗	↑	↖	↖	↑	↗	↑	→	↖	↗	↖	→
Bob;s bits	0	1	1	1	1	0	1	0	1	0	1	0

For about half of the time, Bob's basis will be the same as Alice's, in which case his result after measuring the qubit will be identical to Alice's original bit. The other half of the time, Bob's basis will differ from Alice's. In that case, the result of Bob's measurement will agree with Alice's original bit about 50% of the time.

- If Eve is eavesdropping, she must reading the information that Alice transmits and sending that information onward to Bob.
- Eve also has to toss a coin each time (Alice's basis unknown)
  - Basis identical: accurate measurement, and she will send accurate information to Bob.
  - Basis different: agreement with Alice's only 50% of the time. However, the qubit has now collapsed to one of the two elements of *Eve's basis*. Bob will receive it in the wrong basis. His chances are 50-50 of getting the same bit as Alice has. Therefore Eve's eavesdropping will negatively affect Bob's chances of agreement with Alice, which can be detected.

BB84 step 3

- Bob and Alice publicly compare which basis they used or chose at each step. Each time they disagree, Alice and Bob scratch out the corresponding bit. At the end they are each left with a subsequence of bits sent and received in same basis. If Eve was not listening to the quantum channel, this subsequence should be exactly identical. On average its length will be *n*/2.
- For our example

Bit number	1	2	3	4	5	6	7	8	9	10	11	12
Alice's random basis	+	+	x	+	+	+	x	+	x	x	x	+
Public channel	⇕	⇕	⇕	⇕	⇕	⇕	⇕	⇕	⇕	⇕	⇕	⇕
Bob's random basis	x	+	x	x	+	x	+	+	x	x	x	+
Which agree?		ok	ok		ok			ok	ok	ok	ok	ok
Shared secret keys		1	1		1			0	1	0	1	0

BB84 step 4

- What if Eve was eavesdropping? Bob randomly chooses half of the *n*/2 bits and publicly compares them with Alice.
  - If they disagree by more than a tiny percentage (e.g., due to noise), they know Eve was listening in and then sending in what she received.
  - If the sequence is mostly similar, it means that either Eve has great guessing ability (improbable) or Eve was not listening in. They will use the remaining bits as private key.
- For our example

Bit number	1	2	3	4	5	6	7	8	9	10	11	12
Shared secret keys		1	1		1			0	1	0	1	0
Randomly chosen to compare			y						y	y		y
Public channel			⇕						⇕	⇕		⇕
Shared secret keys		1	1		1			0	1	0	1	0
Which agree?			ok						ok	ok		ok
Unrevealed secret keys		1			1			0			1	

BB84: #qubits?

- If we begin with *n* qubits, only *n*/2 qubits will be available after step 3.
- Furthermore, Alice and Bob publicly display half of the resulting qubits in step 4. This leaves *n*/4 of the original qubits.
- However, Alice can make her qubit stream as large as she wants: if she wants an *m* bit key, she simply starts with a 4*m* qubit stream.

Quantum Key Exchange II: The B92 Protocol

- Simplification of the BB84 protocol: the use of two different bases is redundant →
- The B92 protocol, invented by Charles Bennett, published in 1992.
- Main idea: Alice uses only one *nonorthogonal* basis.
- We will work out the protocol with the following example:

$$\{|\rightarrow\rangle, |\nearrow\rangle\} = \left\{[1,0]^T, \frac{1}{\sqrt{2}}[1,1]^T\right\}$$

Alice takes $|\rightarrow\rangle$ to be 0 and $|\nearrow\rangle$ to be 1.

Role of the nonorthogonal basis:

- All observables have an orthogonal basis of eigenvectors.
- Nonorthogonal basis → no observable whose basis of eigenvectors is the one we have chosen.
- No single experiment whose resulting states are precisely the members of our basis.
- In other words, no single experiment can be set up for the specific purpose of discriminating unambiguously between the nonorthogonal states of the basis.

B92 step 1

- Alice flips a coin *n* times and transmits to Bob *n* random bits in the appropriate polarization with a quantum channel.
- An example:

Bit number	1	2	3	4	5	6	7	8	9	10	11	12
Alice's random bits	0	0	1	0	1	0	1	0	1	1	1	0
Alice's qubits	→	→	↗	→	↗	→	↗	→	↗	↗	↗	→
Quantum channel	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓

B92 step 2

For each of the *n* qubits, Bob measures the received qubits in either the + or x basis. He flips a coin to determine which basis to use. Possible scenarios:

Used basis by Bob	Bob observes	Bob knows Alice must have sent	If Alice had sent	Then Bob should have received
+	$\|\uparrow\rangle$	$\|\nearrow\rangle$	$\|\rightarrow\rangle$	$\|\rightarrow\rangle$
+	$\|\rightarrow\rangle$	???	$\|\rightarrow\rangle$ or $\|\nearrow\rangle$	$\|\rightarrow\rangle$ (100%or50%)
x	$\|\nwarrow\rangle$	$\|\rightarrow\rangle$	$\|\nearrow\rangle$	$\|\nearrow\rangle$
x	$\|\nearrow\rangle$	???	$\|\nearrow\rangle$ or $\|\rightarrow\rangle$	$\|\nearrow\rangle$ (100%or50%)

B92 step 2 (cont'd), 3 & 4

For our example:

Bit number	1	2	3	4	5	6	7	8	9	10	11	12
Alice's random bits	→	→	↗	→	↗	→	↗	→	↗	↗	↗	→
Quantum channel	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓
Bob's random basis	x	+	x	x	+	x	+	+	x	+	x	+
Bob's observations	↖	→	↗	↖	↑	↖	→	→	↗	↑	↗	→
Bob's bits	0	?	?	0	1	0	?	?	?	1	?	?

Step 3. Bob publicly tells Alice which bits were uncertain and they both omit them.

Step 4. To detect whether Eve was listening in, they can sacrifice half of their hidden bits, as in Step 4 of BB84.

Quantum Key Exchange III: The EPR Protocol

- A completely different type of QKE protocol based on entanglement, proposed by Artur K. Ekert in 1991.
- We will discuss a simplified version of the protocol and point to the original version.
- It is possible to place two qubits in the entangled state: $\frac{|00\rangle + |11\rangle}{\sqrt{2}}$
- We have seen that when one of these qubits is measured, they both will collapse to the same value.
- Suppose Alice wants to send Bob a secret key.
  - A sequence of entangled pairs of qubits can be generated and sent.
  - When Alice and Bob wants to communicate, they can measure their respective qubits.
  - It does not matter who measures first, because both qubits will collapse to the same value.
  - Ready: Alice and Bob have a sequence of random bits that no one else has.

EPR protocol steps 1&2

Step 1. Alice and Bob are each assigned one of each of the pairs of a sequence of entangled qubits. When they are ready to communicate, they move to step 2.

Step 2. Alice and Bob separately choose a random sequence of bases to measure their particles. They then measure their qubits in their chosen basis.

Bit number	1	2	3	4	5	6	7	8	9	10	11	12
Alice's random bases	x	x	+	+	x	+	x	+	+	x	+	x
Alice's observations	↗	↖	→	↑	↗	→	↖	→	→	↗	→	↗
Bob's random bases	x	+	+	x	x	+	+	+	+	x	x	+
Bob's observations	↗	→	→	↗	↗	→	↑	→	→	↗	↖	→

EPR protocol step 3

Step 3. Alice and Bob publicly compare what bases were used and keep only those bits that were measured in the same bases.

Bit number	1	2	3	4	5	6	7	8	9	10	11	12
Alice's random bases	x	x	+	+	x	+	x	+	+	x	+	x
Public channel	⇕	⇕	⇕	⇕	⇕	⇕	⇕	⇕	⇕	⇕	⇕	⇕
Bob's random bases	x	+	+	x	x	+	+	+	+	x	x	+
Which agree?	ok		ok		ok	ok		ok	ok	ok		

If everything worked fine, Alice and Bob share a totally random secret key.

Problems:

1. the entangled pairs could have become disentangled;
2. Eve could have taken hold of one of the pairs, measured them, and sent along disentangled qubits.

Solution: step 4 of BB84, compare half of the bits

Ekert's original protocol

- More sophisticated, measurements with three instead of two different bases.
- Bell's inequality:
  - Requires three different bases.
  - If particles are independent, then the measurements will satisfy the inequality.
  - If the particles are dependent, i.e., entangled, then Bell's inequality fails.
- Ekert proposed to use Bell's inequality to check if Alice and Bob's bit sequences were entangled, when they were measured.
- Details: see book, page 277.

Reading

- This lecture: Ch 9.1-9.4 Cryptography
- Next (last) lecture: Ch 9.5 Teleportation & Ch 11 Hardware

Exam

- Mon Jan 25, 2010, 10-13h