QUANTUM CRYPTOGRAPHY

PRESENTED BY

V.LACHIRAM  -06141A0538
Quantum cryptography
-the final battle?

CS4236 Principles of Computer Security
National University of Singapore

Jonas Rundberg, NT030157A
This presentation

- Quantum mechanics
  - Introduction
  - Notation
  - Polarized photons
  - Experiment

- Quantum cryptology
  - Key distribution
  - Eavesdropping
  - Detecting eavesdropping
  - Noise
  - Error correction
  - Privacy Amplification
  - Encryption
Introduction

- Spawned during the last century
- Describes properties and interaction between matter at small distance scales
- Quantum state determined by (among others)
  - Positions
  - Velocities
  - Polarizations
  - Spins
- qubits
Notation

- Bra/Ket notation (pronounced “bracket”)
- From Dirac 1958
- Each state represented by a vector denoted by an arrow pointing in the direction of the polarization
Notation

- Simplified Bra/Ket-notation in this presentation
- Representation of polarized photons:
  - horizontally: \( \rightarrow \)
  - vertically:
  - diagonally: \( \swarrow \text{and} \nwarrow \)
Polarized photons

- Polarization can be modeled as a linear combination of basis vectors and \( \psi \).
- Only interested in direction \( \psi \).
- \( a + b \) \( \psi \) will result in a unit vector \( \psi \) such that \( |a|^2 + |b|^2 = 1 \).
Polarized photons

- Measurement of a state not only measures but actually transforms that state to one of the basis vectors and .
- If we chose the basis vectors and when measuring the state of the photon, the result will tell us that the photon’s polarization is either or , nothing in between.
Experiment

- Classical experiment
- Equipment:
  - laser pointer
  - three polarization filters
- The beam of light i pointed toward a screen.
- The three filters are polarized at and respectively
Experiment

- The filter is put in front of the screen
- Light on outgoing side of filter is now 50% of original intensity
Experiment

- Next we insert a filter whereas no light continue on the output side
Experiment

- Here is the puzzling part...
- We insert a filter in between
- This increases the number of photons passing through
Experiment explained

- Filter is hit by photons in random states. It will measure half of the photons polarized as ←
Experiment explained

- Filter is perpendicular to that and will measure the photons with respect to , which none of the incoming photons match.
Experiment explained

- Filter measures the state with respect to the basis \{ \psi, \phi \}
Experiment explained

- Photons reaching filter will be measured as with 50% chance. These photons will be measured by filter as with 50% probability and thereby 12.5% of the original light pass through all three filters.
Quantum cryptology
Key distribution

- Alice and Bob first agree on two representations for ones and zeroes.
- One for each basis used, \{\,\,\}\ and \{\,\,\,\,\}\.
- This agreement can be done in public.
- Define
  \[
  1 = \; 0 = \quad \leftarrow \\
  1 = \quad 0 = \quad \nonumber 
  \]
Key distribution - BB84

1. Alice sends a sequence of photons to Bob. Each photon in a state with polarization corresponding to 1 or 0, but with randomly chosen basis.

2. Bob measures the state of the photons he receives, with each state measured with respect to randomly chosen basis.

3. Alice and Bob communicates via an open channel. For each photon, they reveal which basis was used for encoding and decoding respectively. All photons which has been encoded and decoded with the same basis are kept, while all those where the basis don't agree are discarded.
Eavesdropping

- Eve has to randomly select basis for her measurement.
- Her basis will be wrong in 50% of the time.
- Whatever basis Eve chose she will measure 1 or 0.
- When Eve picks the wrong basis, there is 50% chance that she'll measure the right value of the bit.
- E.g. Alice sends a photon with state corresponding to 1 in the \{\uparrow, \downarrow\} basis. Eve picks the \{\uparrow, \downarrow\} basis for her measurement which this time happens to give a 1 as result, which is correct.
## Eavesdropping

<table>
<thead>
<tr>
<th>Alice’s basis</th>
<th>Alice’s bit</th>
<th>Alice’s photon</th>
<th>Eve’s basis</th>
<th>Correct</th>
<th>Eve’s photon</th>
<th>Eve’s bit</th>
<th>Correct</th>
</tr>
</thead>
<tbody>
<tr>
<td>{ , , }</td>
<td>0</td>
<td>←</td>
<td>{ , , }</td>
<td>Yes</td>
<td>←</td>
<td>0</td>
<td>Yes</td>
</tr>
<tr>
<td>{ , , }</td>
<td>1</td>
<td>←</td>
<td>{ , , }</td>
<td>No</td>
<td>←</td>
<td>1</td>
<td>Yes</td>
</tr>
<tr>
<td>{ , , }</td>
<td>0</td>
<td>←</td>
<td>{ , , }</td>
<td>Yes</td>
<td>←</td>
<td>0</td>
<td>Yes</td>
</tr>
<tr>
<td>{ , , }</td>
<td>1</td>
<td>←</td>
<td>{ , , }</td>
<td>No</td>
<td>←</td>
<td>0</td>
<td>No</td>
</tr>
<tr>
<td>{ , , }</td>
<td>1</td>
<td>←</td>
<td>{ , , }</td>
<td>Yes</td>
<td>←</td>
<td>1</td>
<td>Yes</td>
</tr>
<tr>
<td>{ , , }</td>
<td>0</td>
<td>←</td>
<td>{ , , }</td>
<td>No</td>
<td>←</td>
<td>0</td>
<td>Yes</td>
</tr>
<tr>
<td>{ , , }</td>
<td>0</td>
<td>←</td>
<td>{ , , }</td>
<td>Yes</td>
<td>←</td>
<td>1</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Eves problem

- Eve has to re-send all the photons to Bob
- Will introduce an error, since Eve don't know the correct basis used by Alice
- Bob will detect an increased error rate
- Still possible for Eve to eavesdrop just a few photons, and hope that this will not increase the error to an alarming rate. If so, Eve would have at least partial knowledge of the key.
Detecting eavesdropping

- When Alice and Bob need to test for eavesdropping
- By randomly selecting a number of bits from the key and compute its error rate
- Error rate < $E_{\text{max}}$ ⇒ assume no eavesdropping
- Error rate > $E_{\text{max}}$ ⇒ assume eavesdropping (or the channel is unexpectedly noisy)
  Alice and Bob should then discard the whole key and start over
Noise

- Noise might introduce errors
- A detector might detect a photon even though there are no photons
- Solution:
  - send the photons according to a time schedule.
  - then Bob knows when to expect a photon, and can discard those that doesn't fit into the scheme's time window.
- There also has to be some kind of error correction in the over all process.
Error correction

- Suggested by Hoi-Kwong Lo. (Shortened version)
  1. Alice and Bob agree on a random permutation of the bits in the key
  2. They split the key into blocks of length k
  3. Compare the parity of each block. If they compute the same parity, the block is considered correct. If their parity is different, they look for the erroneous bit, using a binary search in the block. Alice and Bob discard the last bit of each block whose parity has been announced.
  4. This is repeated with different permutations and block size, until Alice and Bob fail to find any disagreement in many subsequent comparisons.
Privacy amplification

- Eve might have partial knowledge of the key.
- Transform the key into a shorter but secure key.
- Suppose there are n bits in the key and Eve has knowledge of m bits.
- Randomly choose a hash function where $h(x): \{0,1\}^n \rightarrow \{0,1\}^{n-m-s}$
- Reduces Eve's knowledge of the key to $2^{-s / \ln 2}$ bits.
Encryption

- Key of same size as the plaintext
- Used as a one-time-pad
- Ensures the crypto text to be absolutely unbreakable
What to come

- Theory for quantum cryptography already well developed
- Problems:
  - quantum cryptography machine vulnerable to noise
  - photons cannot travel long distances without being absorbed
Summary

- The ability to detect eavesdropping ensures secure exchange of the key
- The use of one-time-pads ensures security
- Equipment can only be used over short distances
- Equipment is complex and expensive
References

- [WWW1] Math Pages, Spin & Polarization
- [WWW2] Luisiana Tech University, Quantum Computation
  http://www2.latech.edu/~dgao/CNSM/quantumcomput.html
- [WWW3] Edmonton Community Network, Quantum Cryptography
  http://home.ecn.ab.ca/~jsavard/crypto/mi060802.htm
- [WIK1] Wikipedia - The free encyclopedia
  http://www.wikipedia.org/wiki/Bra-ket_notation
References

- [WIK2] Wikipedia -The free encyclopedia
- [WIK3] Wikipedia -The free encyclopedia
  http://www.wikipedia.org/wiki/Copenhagen_interpretation
- [GIT] Georgia Institute of Technology, The fundamental postulates of quantum mechanics
- [HP] Hoi-Kwong Lo, Networked Systems Department, Hewlett Packard, Bristol, December 1997, Quantum Cryptology
- [FoF] Forskning och Framsteg, No. 3, April 2003