Quantum Key Distribution (QKD)

Prashanta Kharel
Applied Physics Seminar
November 2012
Facebook helps you connect and share with the people in your life.

Sign Up
It’s free and always will be.

Your First Name
Your Last Name
Your Email
Re-enter Email
New Password
Birthday:
Month:  Day:  Year:

Why do I need to provide my birthday?

Female  Male

By clicking Sign Up, you agree to our Terms and that you have read our Data Use Policy, including our Cookie Use.

Sign Up
Classical Key Distribution

RSA Encryption

- Relies on two distinct large prime numbers
- Factorization of prime
- Exponential problem
- Limited only by computational power

Message: “SEAS”
“01000101”

Public Key
Encode
“01000101”

Private Key
Decode
“SEAS”

\[ c = m^e \pmod{n} \]
\[ m = c^d \pmod{n} \]
Quantum Key Distribution (QKD)

- relies on fundamental quantum mechanics
- unconditionally secure
- eavesdropper can be detected
**BB84-Protocol**

**RSA Encryption**
- Uses polarized light
- Uncertainty principle for single photons

**Calcite Crystal**

**Diagonal Basis**
- Measure
  - D
  - d
  - P = 1/2

**Rectilinear Basis**
- Measure
  - V
  - H
  - P = 1/2

Friday, December 7, 2012
BB84-Protocol

How to share a secret key?

Quantum Channel

Public Channel

<table>
<thead>
<tr>
<th>H/V Basis</th>
<th>D/d Basis</th>
</tr>
</thead>
<tbody>
<tr>
<td>H=0</td>
<td>D=0</td>
</tr>
<tr>
<td>V=1</td>
<td>d=1</td>
</tr>
</tbody>
</table>

Bits

0 1 1 0 1 1 0 0 1 0 1

Alice's Random Basis
D R D R R R R D R D D

Photon Alice Sends

Bob's Random Basis
D D R R R R D D R R D

Bits received by Bob
0 0 1 0 1 1 0 1 1 1

Bob Report Basis
D D R R R D D R R D

Alice confirms correct ones
OK OK OK OK OK OK OK

Shifted Key

0 0 1 0 1 1 1

Correlated measurements
Ekert’s Protocol

Three Conjugate Basis: H/V, D/d, L/R

\[(|HH⟩ + |VV⟩)/\sqrt{2}\]

- Shifted key is smaller
- More sensitive to eavesdropping
Conclusion

- 2009 Yamamoto, up to 105 km, 17 kbits/sec
- 2012 Shields, up to 90 km, ~1Gbits/sec

Future:
- High Key Generation rate
- Noisy channel
- QKD over longer distances
Questions
Sources


- N. Ilic, “The Ekert Protocol”, University of Waterloo

- Y. Yamamoto et al., “Quantum key distribution over 40 dB channel loss using superconducting single photon detectors,” arXiv, 2009