Quantum Cryptography

Kevin Dang

December 7, 2009

Physics 494

What is Cryptography?

- Concealment of Information
- Identity Authentication

Why?

- Online Banking/ecommerce
- Emails Authentication
- Military Communication

What is wrong?

- Relies on factoring large numbers
    - Theoretically quantum computing can factor in much shorter time
    - Can be brute forced
    - Increasing computer power, moore's law
    - DES cracked in 8 hours in 1998

Is Perfect Cryptography possible?

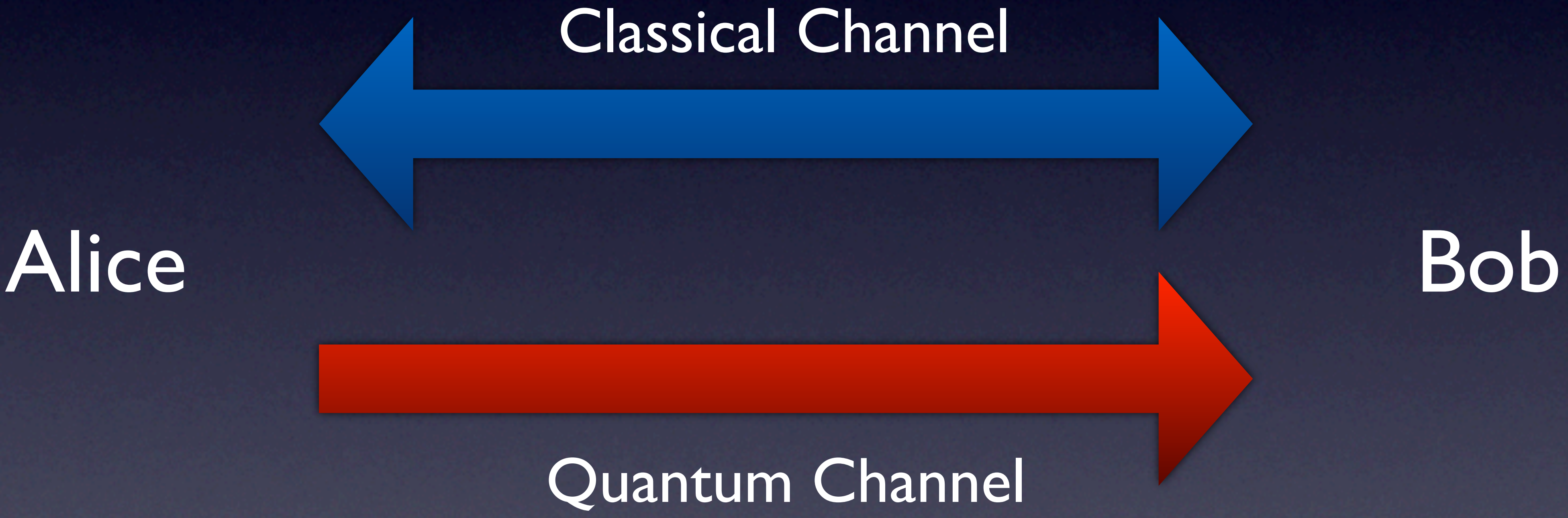
One Time Pad

- Proven to be unbreakable
- Modular addition of a random key and data
- Key is the same length as data and never reused

Quantum Key Distribution

- Quantum Indeterminacy
  - Measuring destroys information
- Polarization of Light
  - Bases: Rectilinear, Diagonal, Circular
  - Observing in the incorrect basis gives a random result

Prepare and Measure Protocols



Classical Channel

Alice

Bob

Quantum Channel

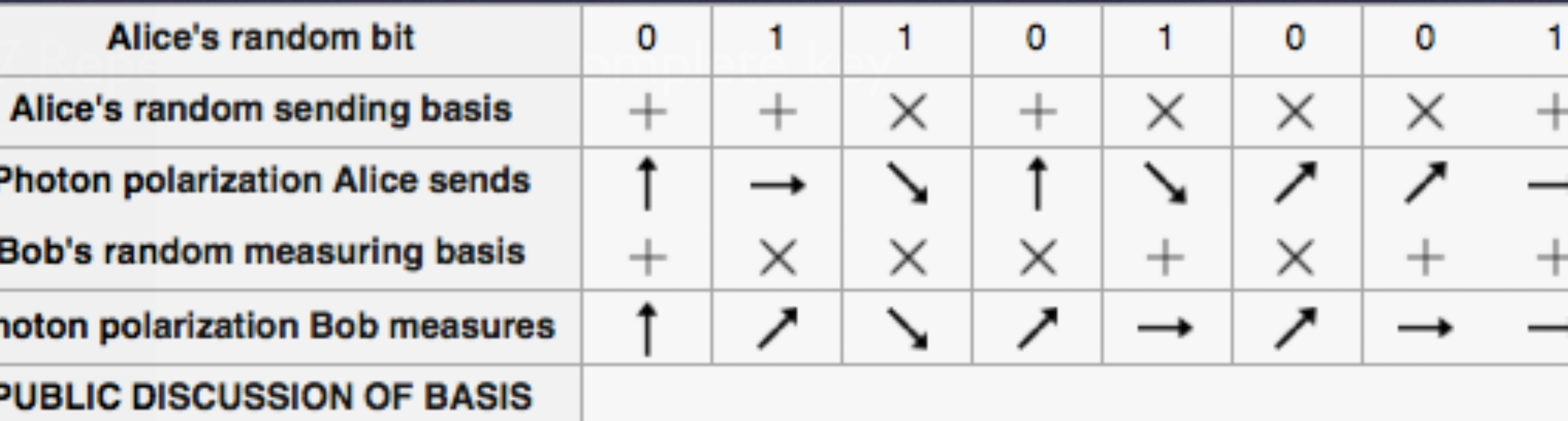
2. Alice prepares a corresponding photon and sends it to Bob

3. Bob measures the photon in random basis

4. Alice and Bob publicly compare bases

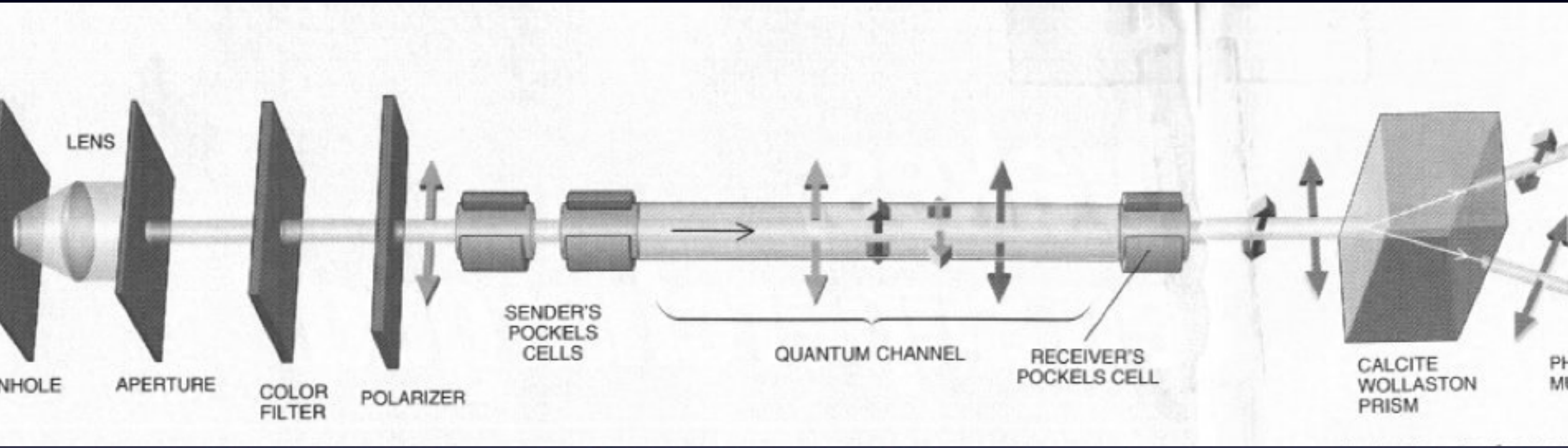
5. Measurements using different bases are discarded

6. Measurements using same bases become the key

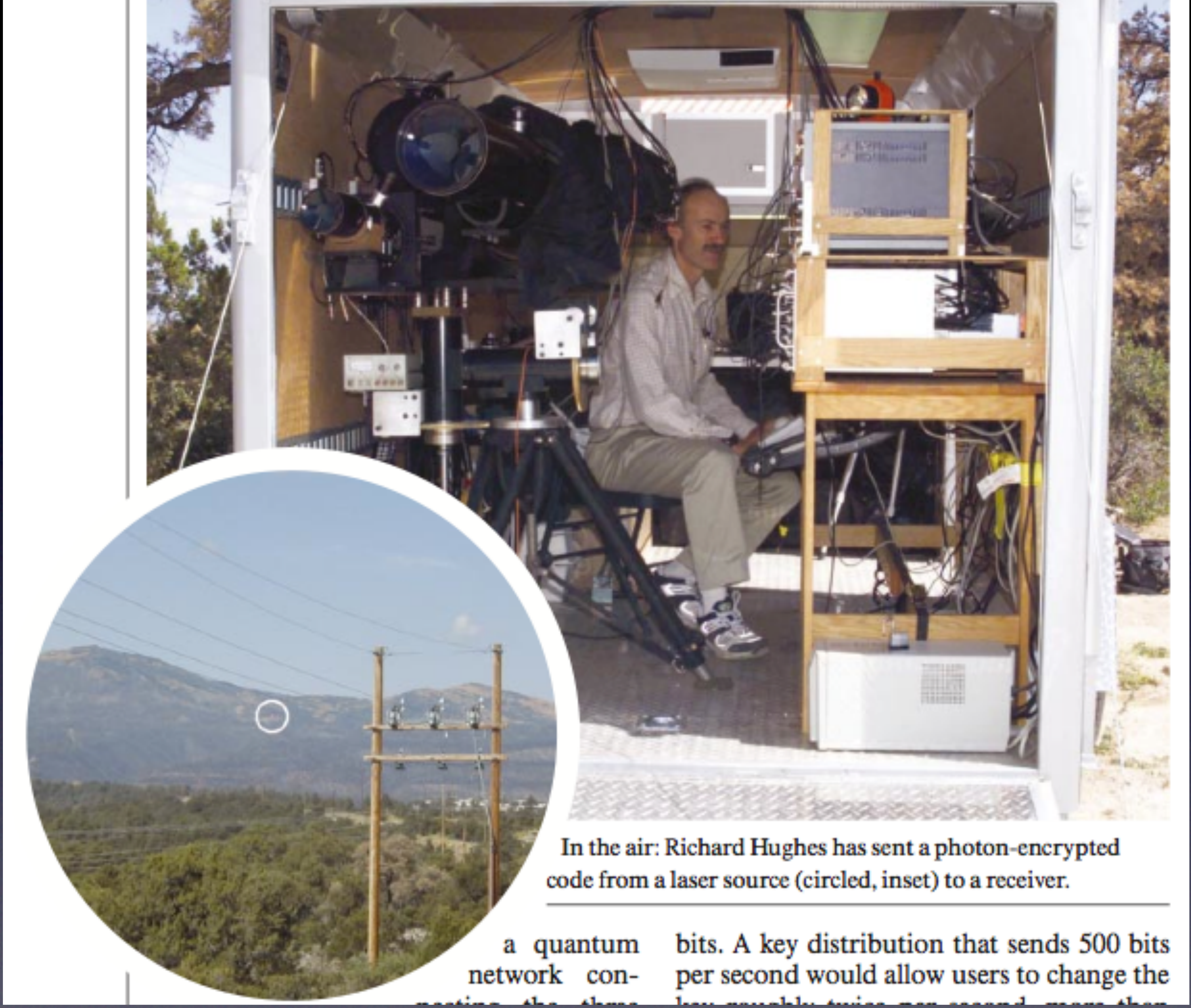


Alice's random bit	0	1	1	0	1	0	0	1
Alice's random sending basis	+	+	×	+	×	×	×	+
Photon polarization Alice sends	↑	→	↘	↑	↘	↗	↗	→
Bob's random measuring basis	+	×	×	×	+	×	+	+
hoton polarization Bob measures	↑	↗	↘	↗	→	↗	→	→
PUBLIC DISCUSSION OF BASIS								

Apparatus



http://www.cs.fsu.edu/~yasinsac/group/slides/bu



In the air: Richard Hughes has sent a photon-encrypted code from a laser source (circled, inset) to a receiver.

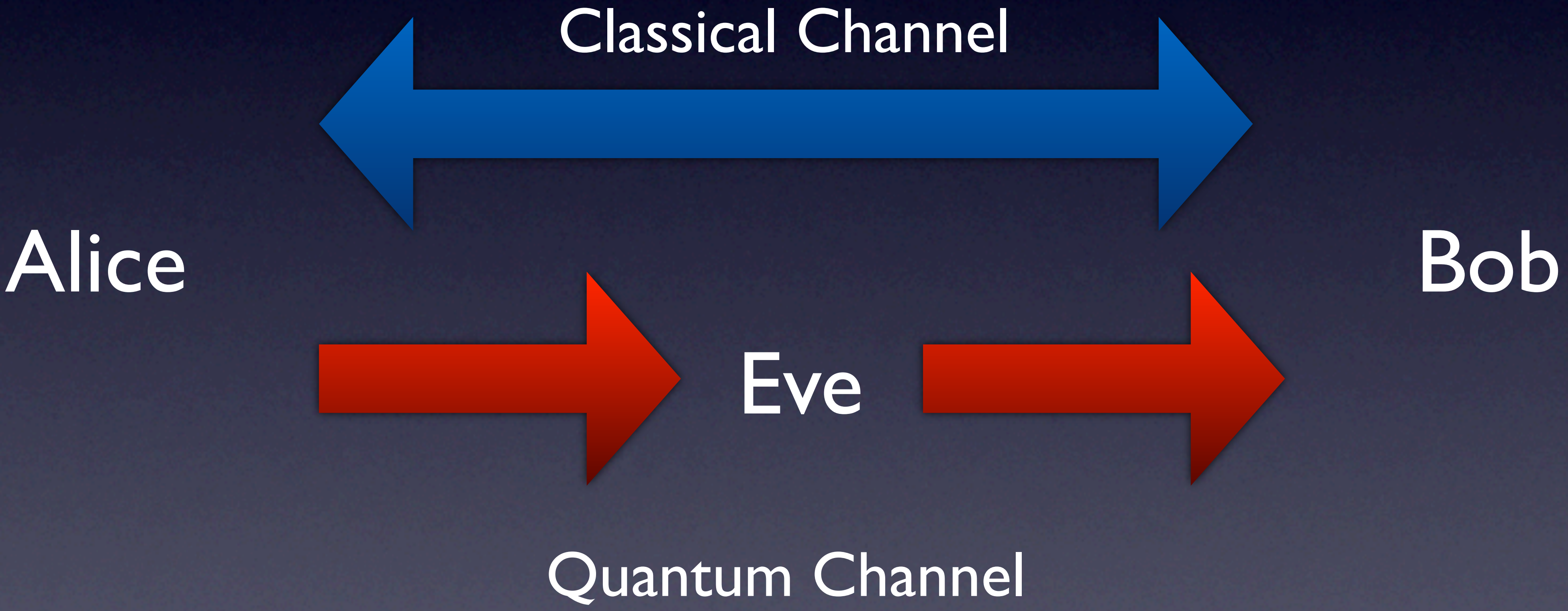
a quantum network con-

bits. A key distribution that sends 500 bits per second would allow users to change the

Attacks

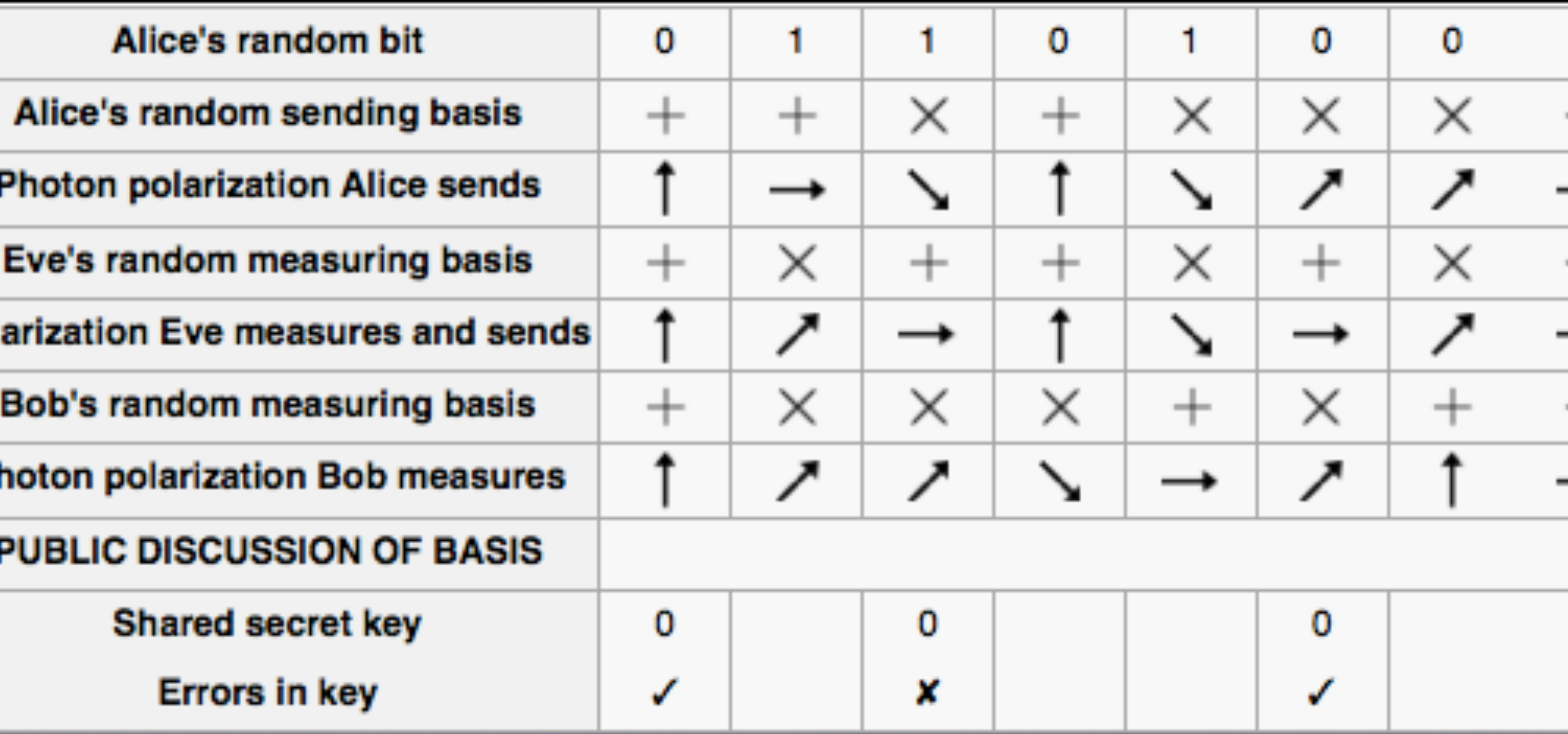
- Intercept and Resend
- Photon splitting
- Man in the Middle

Intercept and Resend



Intercept and Resend

- The attacker must guess the correct basis or information will be lost
- Solution: Bob and Alice compare a portion of their key
    - P = 1 - (3/4)^n
- P = 0.999999999 for n = 72



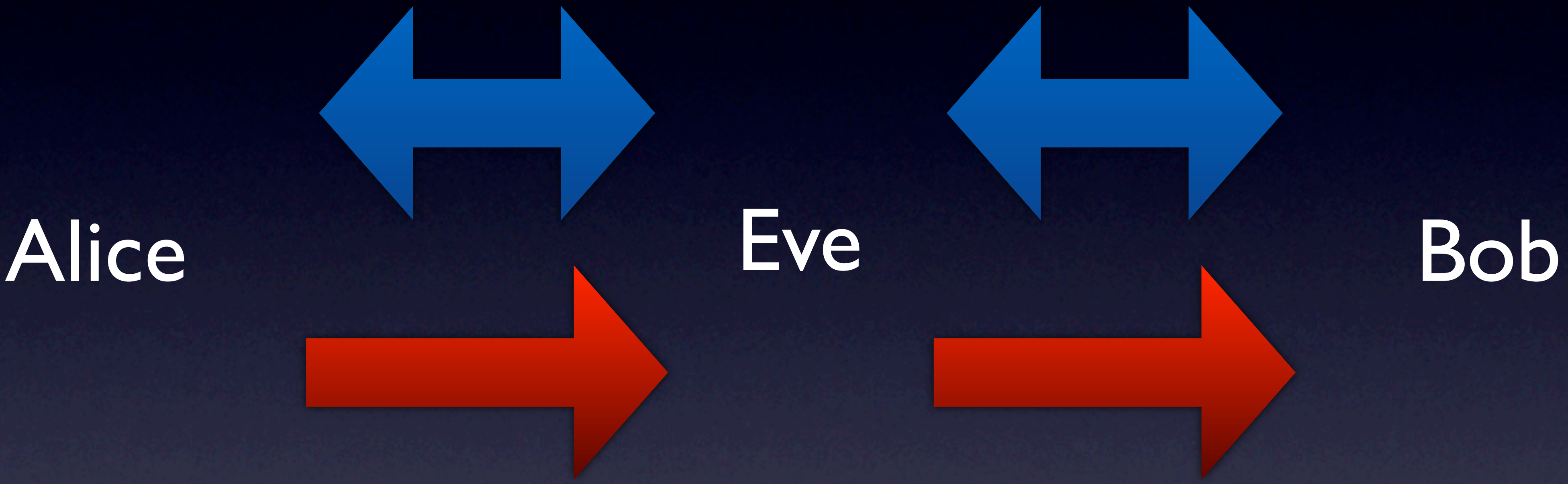
Alice's random bit	0	1	1	0	1	0	0
Alice's random sending basis	+	+	×	+	×	×	×
Photon polarization Alice sends	↑	→	↘	↑	↘	↗	↗
Eve's random measuring basis	+	×	+	+	×	+	×
arization Eve measures and sends	↑	↗	→	↑	↘	→	↗
Bob's random measuring basis	+	×	×	×	+	×	+
hoton polarization Bob measures	↑	↗	↗	↘	→	↗	↑
PUBLIC DISCUSSION OF BASIS							
Shared secret key	0		0			0	
Errors in key	✓		✘			✓	

http://en.wikipedia.org/wiki/Quantum_cryptog

Photon Splitting

- Extra photons could be split from the beam
- Solution: Single photon source instead of an attenuated laser

Man in the Middle



Alice

Eve

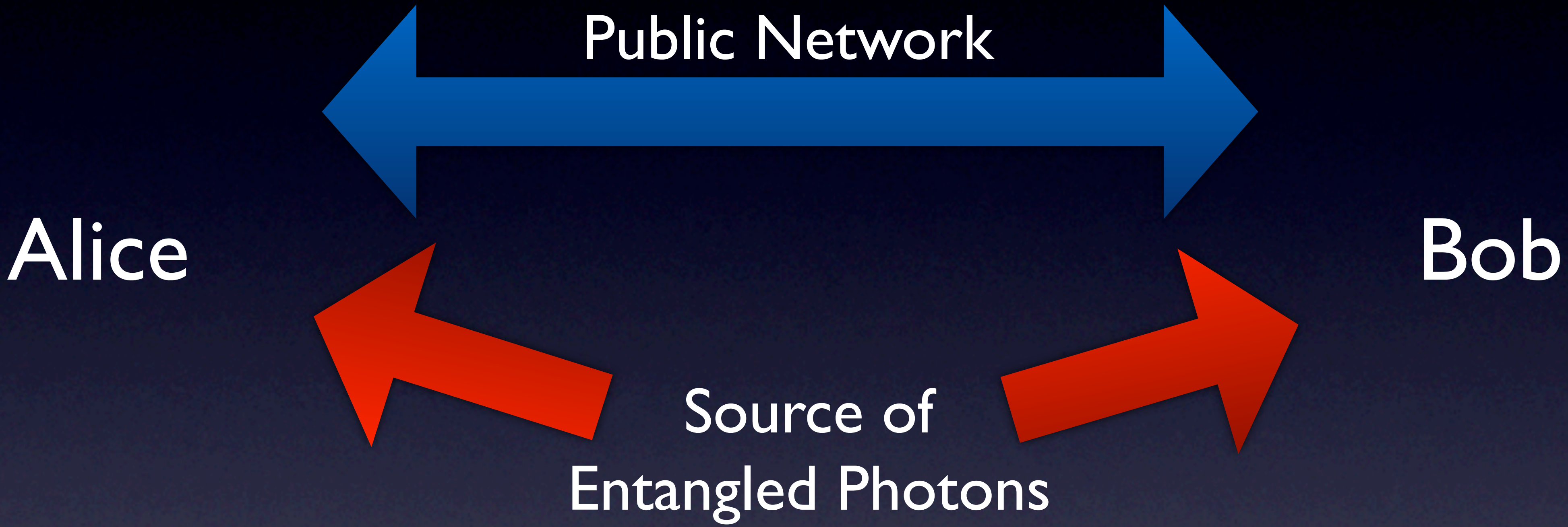
Bob

- Eavesdropper has control over public network.

Requirements

- Quantum Key Distribution is proven unconditionally secure under following requirements:
  - Eve cannot access Alice and Bob's encoding and decoding devices.
  - True random number generators
  - Public transmissions are authenticated

Entanglement Protocols



Public Network

Alice

Bob

Source of Entangled Photons

- Quantum Entanglement
  - Two objects with linked quantum states

Current Status

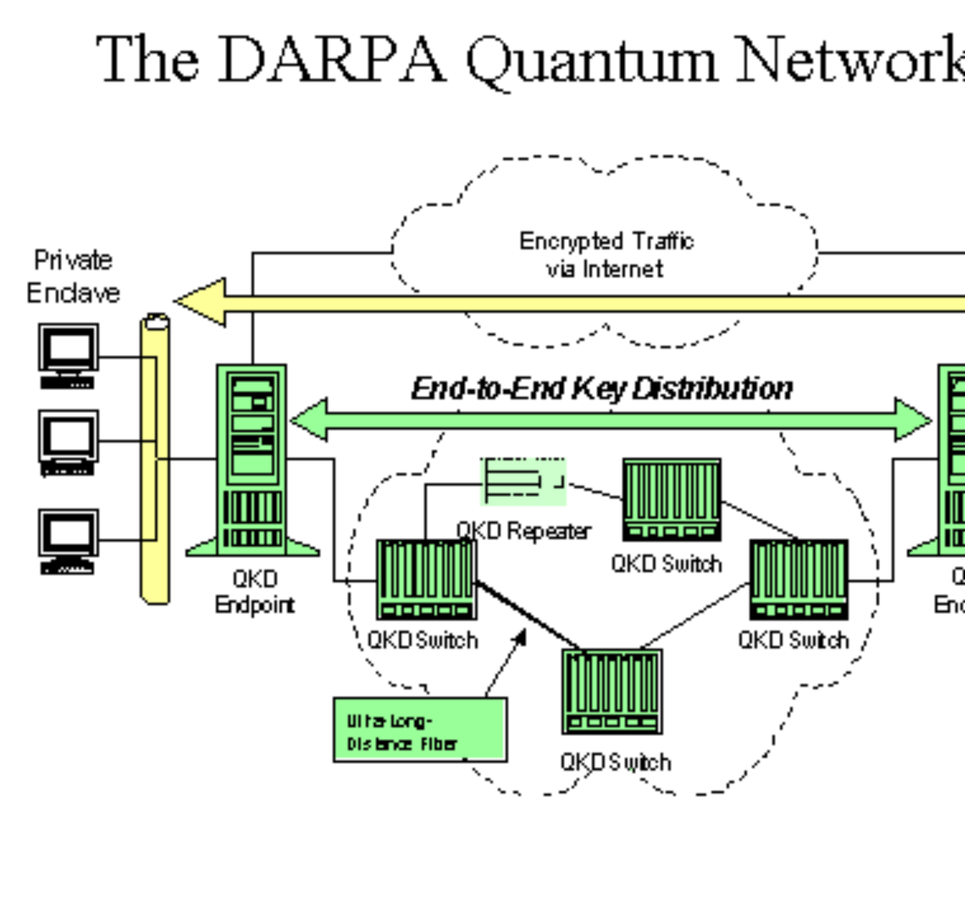
- Four companies currently offering quantum cryptography systems
- Secure Communication based on Quantum Cryptography (SECOQC)
  - EU Funded 11 million Euros
- DARPA Quantum Network
  - Currently 10 nodes

Darpa Quantum Networ

Problems

- One to one connection
- Slow
  - 1 Mbit/s (over 20 km)
  - 10 kbit/s (over 100 km)
- Range Limited
  - Max distance 148.7 km
  - Noise due to decoupling of

Future


The DARPA Quantum Network
Private Enclave
Encrypted Traffic via Internet
End-to-End Key Distribution
QKD Repeater
QKD Switch
QKD Endpoint
QKD Switch
QKD Switch
Ultra Long-Distance Fiber
QKD Switch
Q
End

- Rapidly Advancing
- Quantum Networks
  - Extended Range
  - Multiple Targets
- Large Implications in Cryptography

Bibliography

- http://en.wikipedia.org/wiki/Quantum_cryptography
- Quantum Communications and Cryptography by Alexander V. Sergienko
- Quantum Computation and Quantum Communication: Theory and Experiments by Mladen Pavicic