Quantum Cryptography Today and Tomorrow

Or,

How to Make and

Break Quantum Cryptosystems

(Without Being an Expert in Quantum Mechanics)

Summer Undergraduate Research Fellowship Seminar

Rick Kuhn
kuhn@nist.gov

Goals of Talk

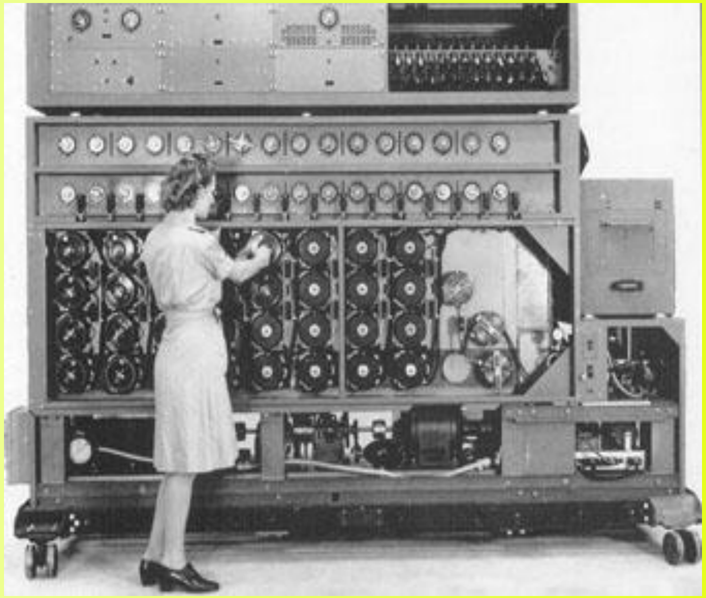
- *Very* brief summary of cryptography
  - Impact of technology
- Introduce basics of quantum cryptography
  - Learn a little bit about quantum mechanics along the way
- Explain two types of quantum crypto protocols
- Show how to break quantum crypto
  - To understand the engineering difficulties of going from theory to practice

Old Style Cryptography

- Shift of alphabet
  - e.g. Caesar cipher A=D, B=E, C=F
  - Probably never fooled anybody (except Caesar)
- Many more sophisticated systems developed from 1500s to mid-20th century
  - Substitution and transposition of letters
  - Some essentially unbreakable by manual means
- Made obsolete by computers circa 1940

Technology Determines What is Breakable

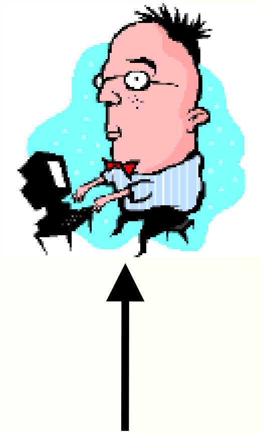
Enigma vs. Human – Enigma wins!



Turing's machine

Enigma vs. Computer
– computer wins!

Desch's machines – even faster



Weakest part of cryptosystem

Modern Cryptography

- One: hard problems in mathematics
  - Breaking the system requires an efficient algorithm for solving a hard problem – e.g. Factoring large numbers, discrete logarithms
  - Examples: RSA, El Gamal
  - Used in public key systems
  - Slow
- Two: information theory
  - Texts scrambled by repeated application of bit shifts and permutations
  - Examples: DES, AES
  - Used in private key systems
  - Fast

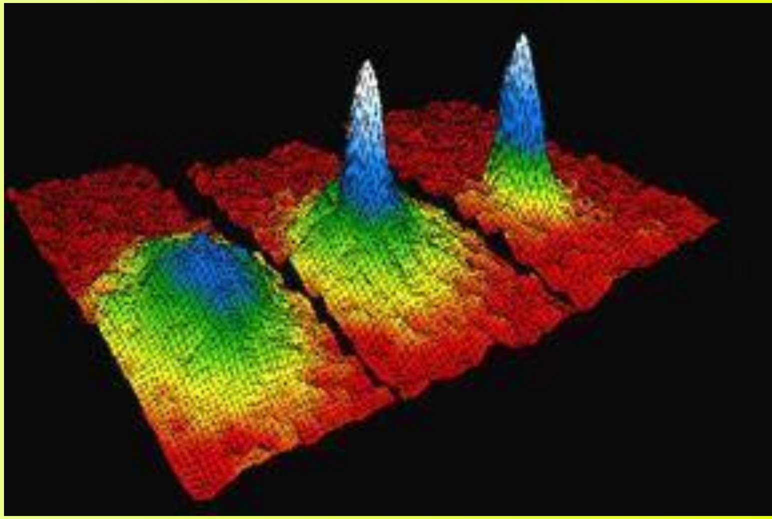
Technology Determines What is Breakable

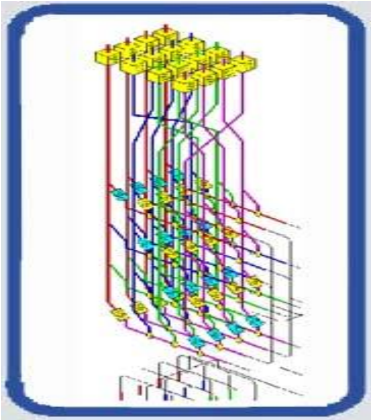
RSA Cryptosystem	$C = M^e \bmod n$ $d = e^{-1} \bmod ((p-1)(q-1))$

Earth Simulator

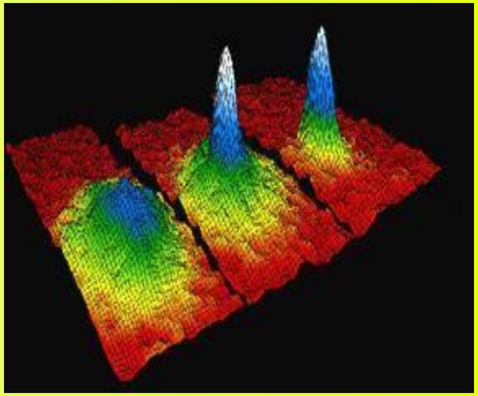
RSA vs. supercomputer: 40 Tflop/s (4×10^{12} flop/sec)
– RSA wins!

RSA vs. Quantum Computer
– computer wins!



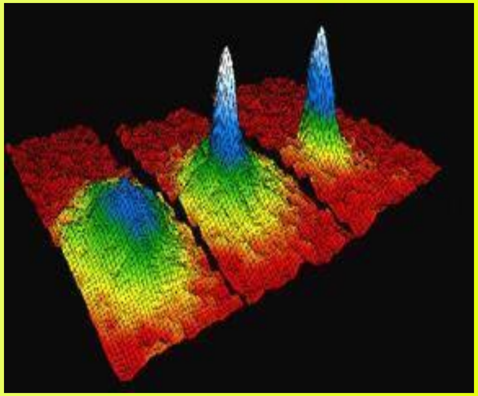


Modern Ciphers vs. Quantum Computer



- "Hard problem" variety
  - **Exponential** speedup – easily breaks algorithms such as RSA
  - If information requires long term protection (e.g. 20+ years), these algorithms are already dead
- "Information theory" variety
  - **Quadratic** speedup (so far)
  - Longer keys can keep them useful

Quantum Crypto – Why?

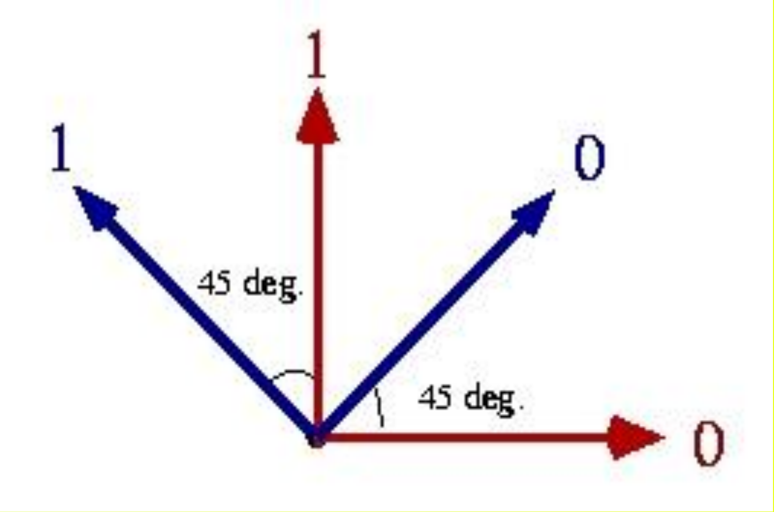


- Protect against attack by quantum computer
  - or any future machine
- Eavesdropping detection
  - Hard to do now
- High volume key distribution
  - If it can be made fast enough

Quantum Mechanics for Cryptography – Measurement Basis

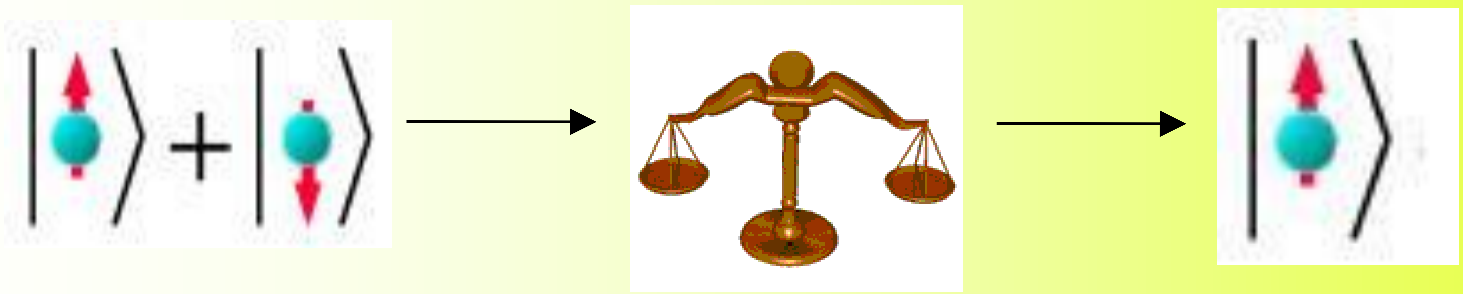
- **Basis** – frame of reference for quantum measurement
- Example – **polarization** vertical/horizontal vs. diagonal

  - Horizontal filter, light gets through = 0
  - Vertical filter, light gets through = 1
  - 45 deg. filter, light = 0
  - 135 deg. filter, light = 1



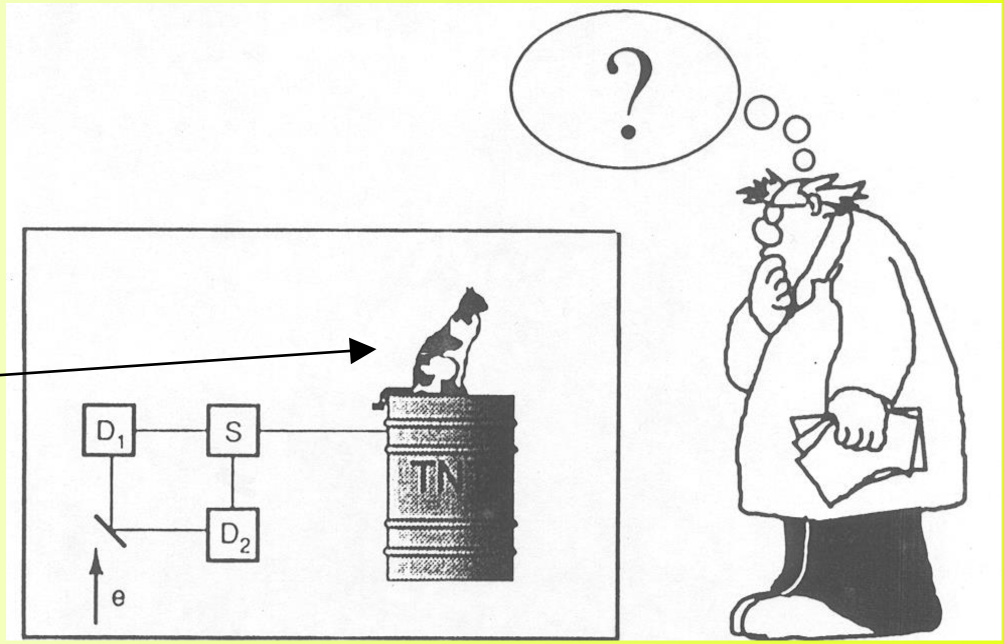
Quantum Mechanics for Cryptography- **Superposition**

- **Superposition** – in “2 states at once” (at least think of it that way), until measured



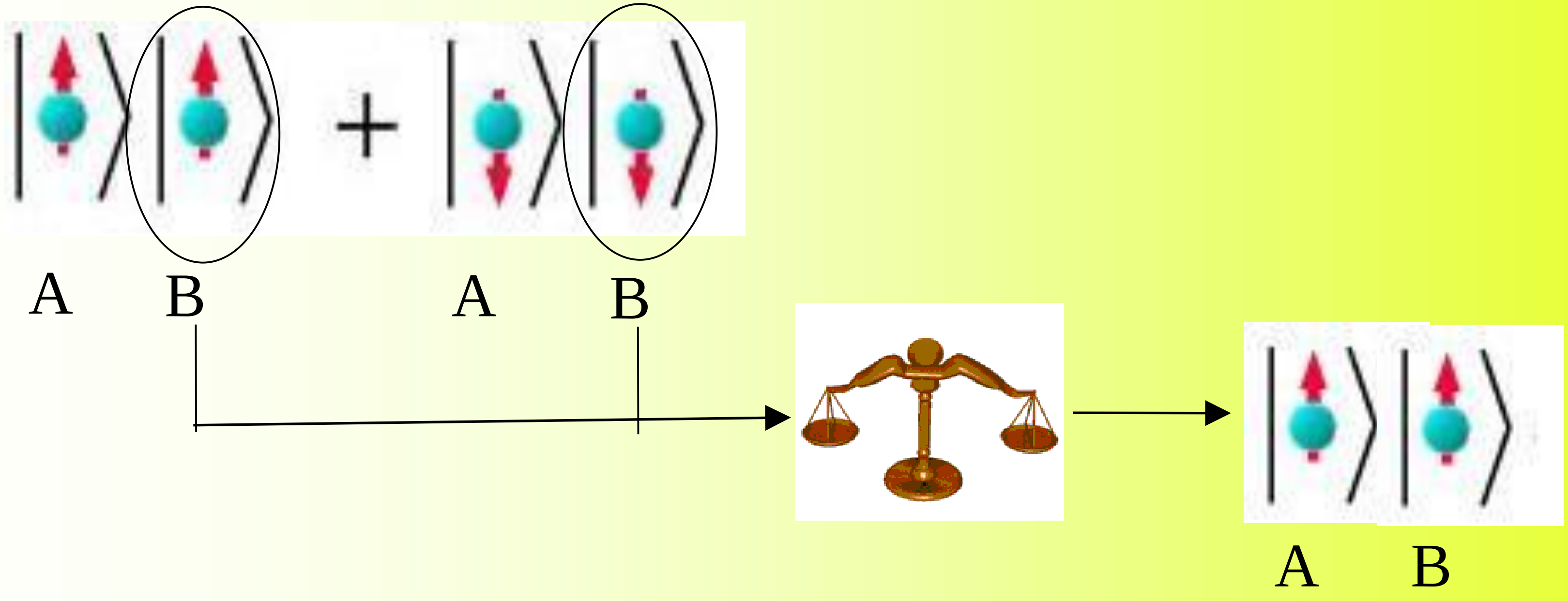
Probability of either result can be varied

Schrodinger's cat – dead *and* alive



Quantum Mechanics for Cryptography - **Entanglement**

- **Entanglement** – like superposition, but more so
  - Measuring one determines result for all
  - *No matter where they are in the universe!*
  - *Result is unpredictable, but same result for all*



Classical interlude – unbreakable cipher

1 0 1 1 0 0 1 0 1 0 0 1 1 1

XOR

0 0 1 0 01 1 0 1 0 1 1 0 1

↓

1 0 0 1 0 1 0 0 0 0 1 0 1 0

One time pad or Vernam cipher

Text	Random key	Ciphertext
C (3)	⊕U (21)	X (24)
A (1)	⊕D (4)	E (5)
T (20)	⊕I (9)	C (3)

All keys equally likely
Can't determine unique key
So can't determine original message

Key can never be reused
Key must be same length as message
=> impractical for most use

Quantum Key Distribution

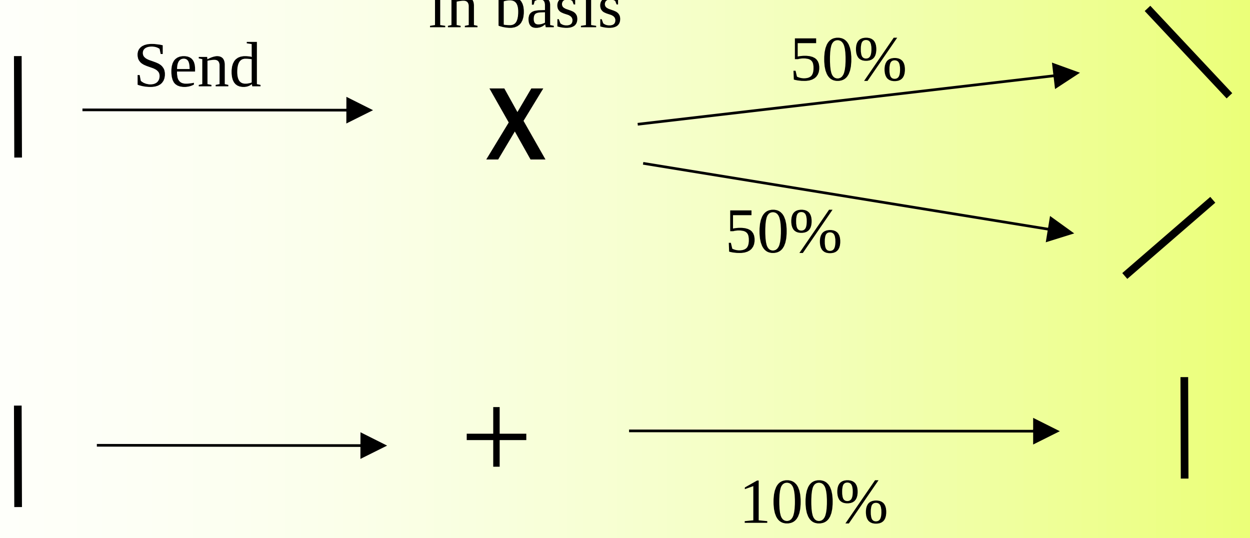
Alice

Bob

Polarized photons sent
from Alice to Bob

Bob
measures
in basis

Result



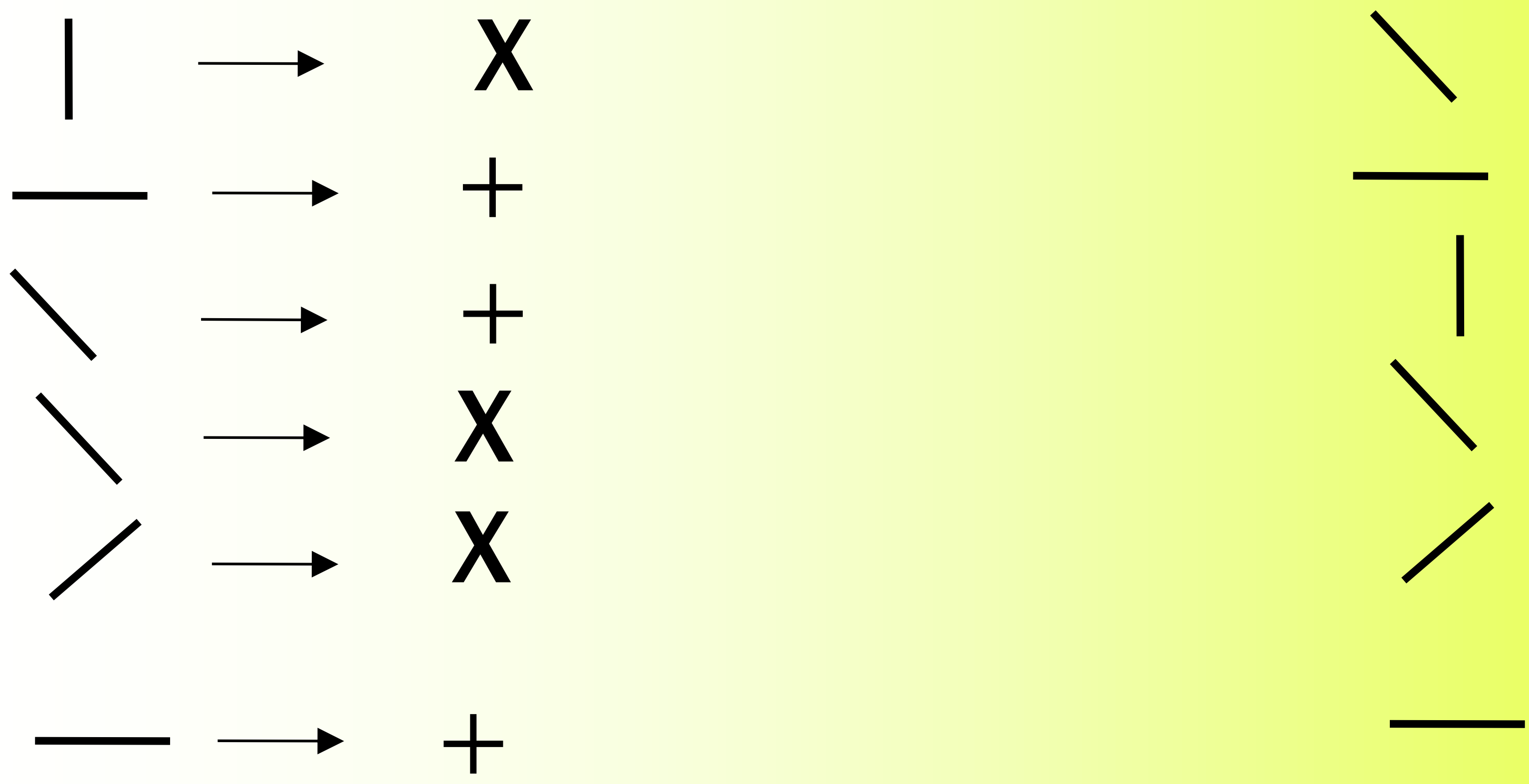
Quantum Key Distribution

BB84 protocol – Bennett and Brassard, 1984

Alice

Bob measures
in random basis

Result

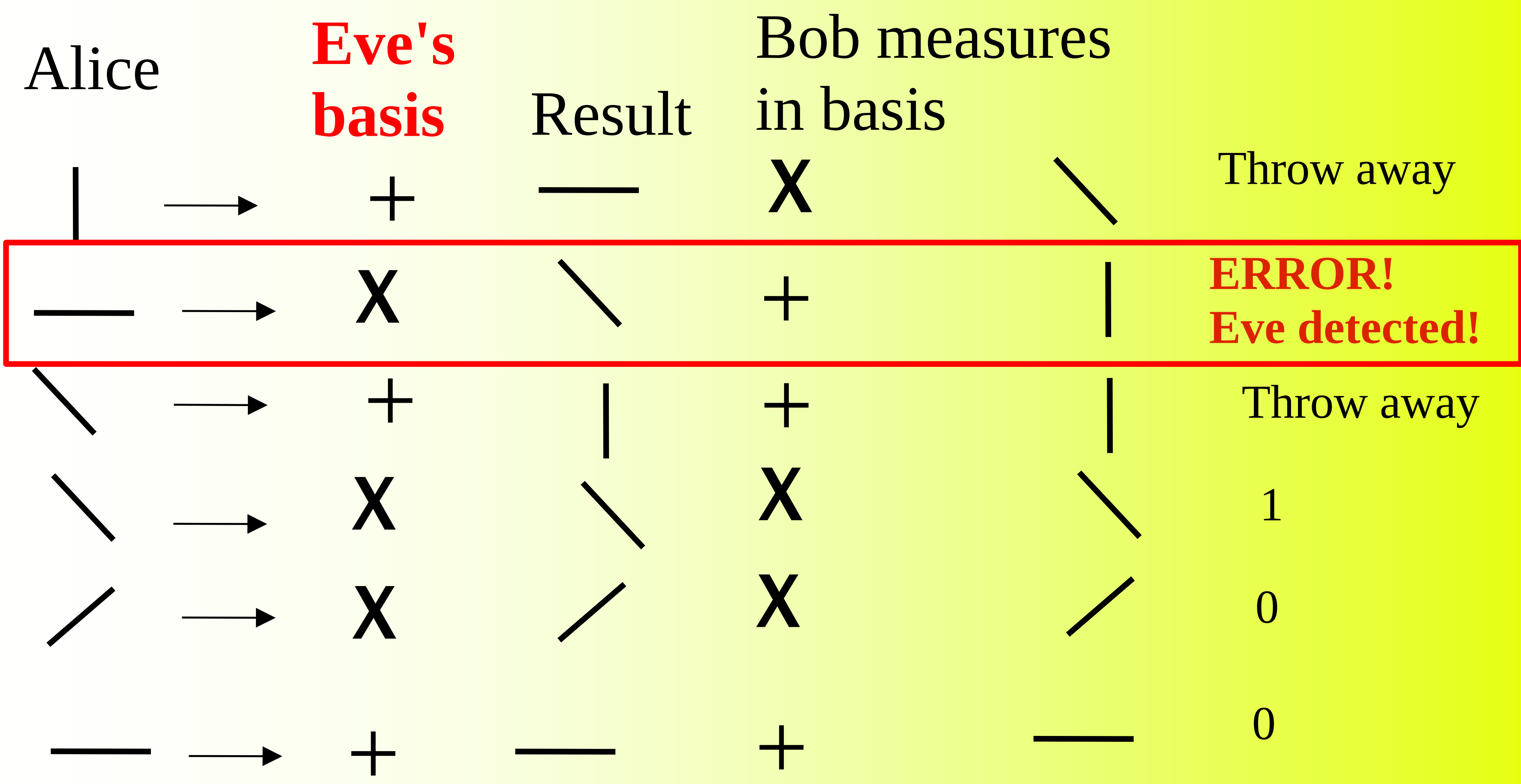


BB84 Quantum Key Distribution

Alice tells basis used

Bob compares w/ his basis

Quantum Key Distribution – detecting eavesdropping



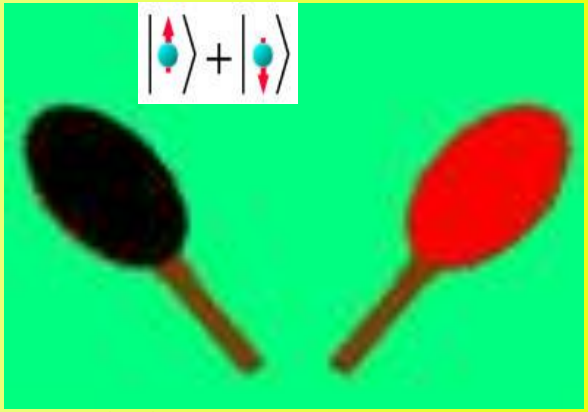
BB84 Result

- **Alice and Bob share a random bit string** that can be used as a one time pad for encryption/decryption

1 0 1 1 0 0 1 0 1 0 0 1 1 1 . . .

- **Eavesdropping is detected** as a 25% error rate in transmission

Ping Pong Protocols



- Beige, Kurtseifer, Englert, Weinfurter – 2002
- Several variations by different developers
- Outline:
  - Alice creates entangled pair
  - Alice sends one qubit to Bob
  - Bob rotates according to secret operation
  - Bob returns qubit to Alice
  - Alice measures with her qubit to determine operation
  - Security: need both qubits to measure;
    Eve does not know basis

Ping Pong Protocol

$|\uparrow\rangle|\uparrow\rangle + |\downarrow\rangle|\downarrow\rangle$ Create entangled pair

Send one qubit $|\uparrow\rangle + |\downarrow\rangle$ →

No change = 0
Transform = 1

← $|\uparrow\rangle + |\downarrow\rangle$ Return

<u>**Both** qubits needed to measure</u>

$|\uparrow\rangle|\uparrow\rangle + |\downarrow\rangle|\downarrow\rangle$

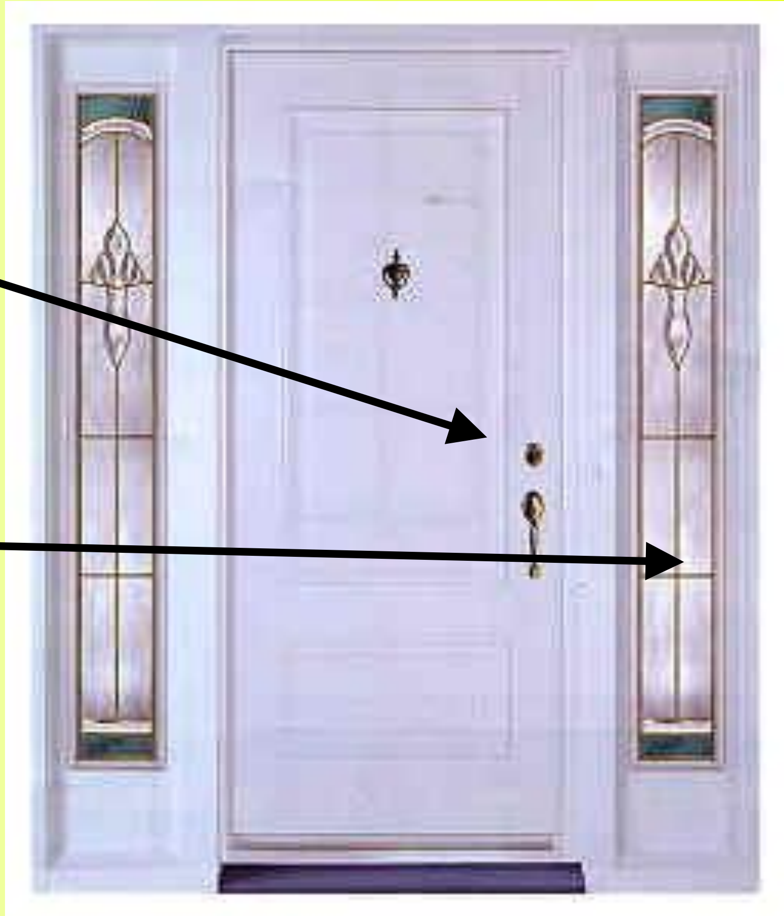
↓

 →

No change = 0
Transform = 1

Breaking Quantum Crypto Protocols

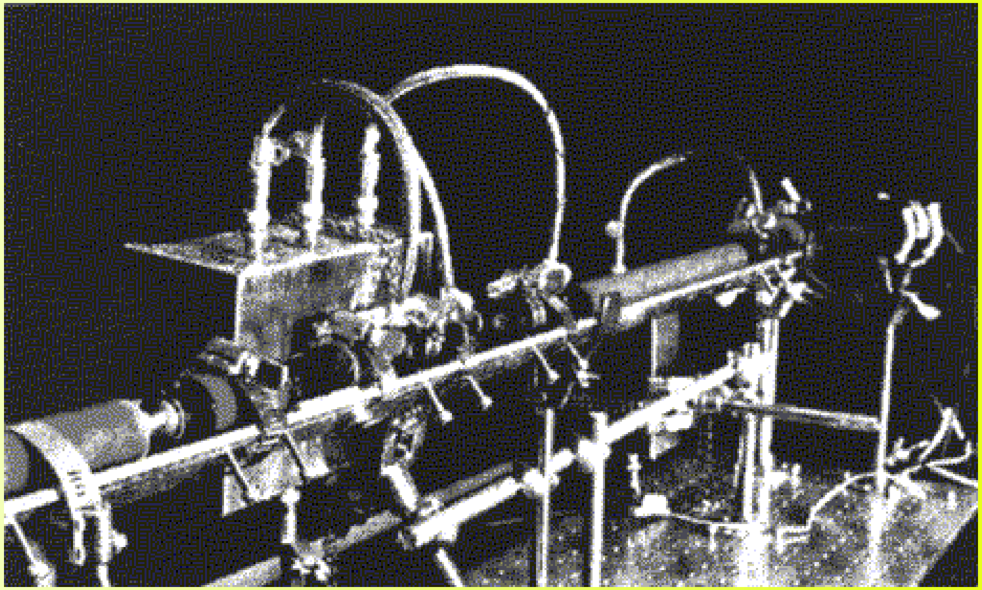
- Similar to breaking conventional crypto protocols
- Choose one:
  - Break crypto algorithm
  - Look for weaknesses and flaws in implementation (find an invalid assumption and exploit it)



Breaking Quantum Crypto

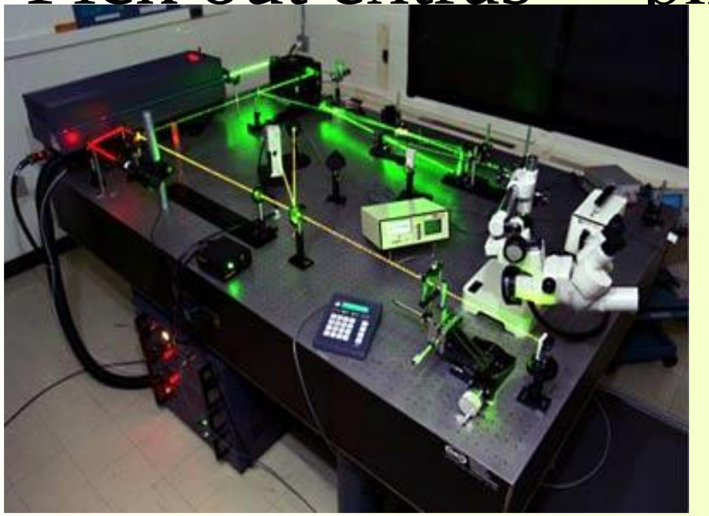
- Break underlying cryptography
  - No go – laws of physics make it unbreakable

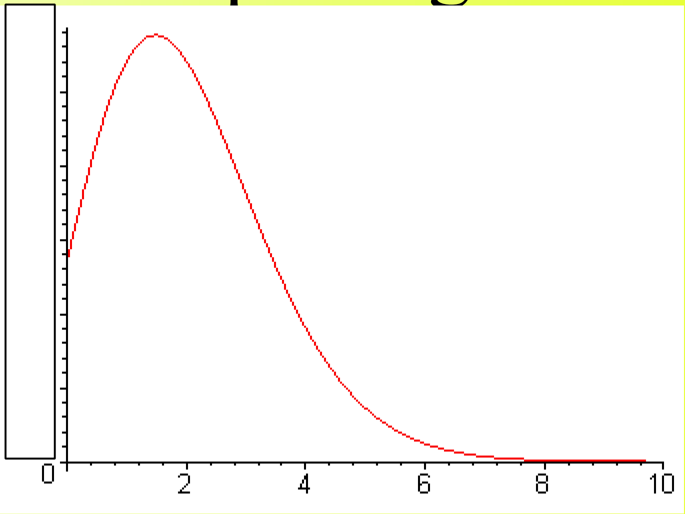
- Attack the implementation
  - Hardware
  - Protocols
  - Software



Attack Hardware Implementation

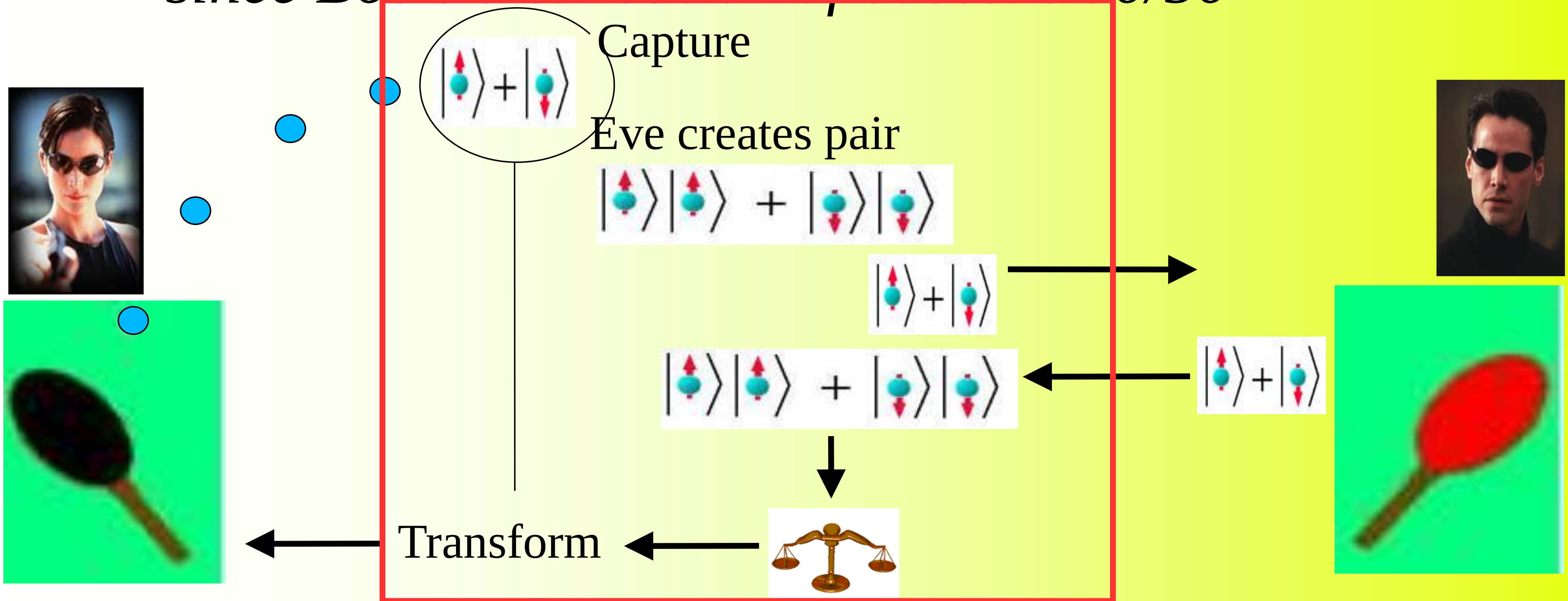
- BB84
- Attenuated lasers used to generate *average* of one photon per time slice
- Poisson process ensures that sometimes there will be more than one
- Pick out extras - “photon number splitting”





Attack the Protocol

- Eve captures qubit from Alice, creates entangled pairs, forwards one qubit to Bob
- Eve measures return qubit from Bob, duplicates his measurement on captured qubit, returns to Alice - *Eve can determine basis from stray qubits, since Bob's distribution of bases is 50/50*



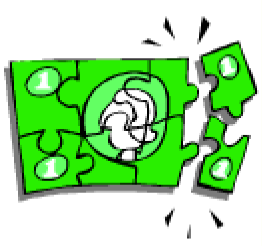
Attack Software Implementation

- Quantum crypto running in a TCP/IP network on top of ordinary servers and operating systems

- 'nuff said!

NIST Quantum Communication Testbed

- Scalable, high speed quantum network
- Provides a measurement infrastructure for quantum protocols, and testbed for experiments



Industrial Prospects and Tech Transfer

- Selling points
  - Protect secrets long-term/forever **$**
  - Distribute large volumes of key efficiently **$$**
- Currently two (count 'em!) commercial implementations of quantum crypto
- Potential markets?
  - Financial services (large key volume)
  - Government/military (long term secrecy, key dist.)
  - Ultra-high bandwidth networks, media/content distribution??

To Probe Further

- Introduction to quantum computing and crypto:
  - **qubit.org**
  - "Quantum Computing and Communications",- introductory technical article on NIST site below:
- NIST quantum information testbed:
  math.nist.gov/quantum

Questions?