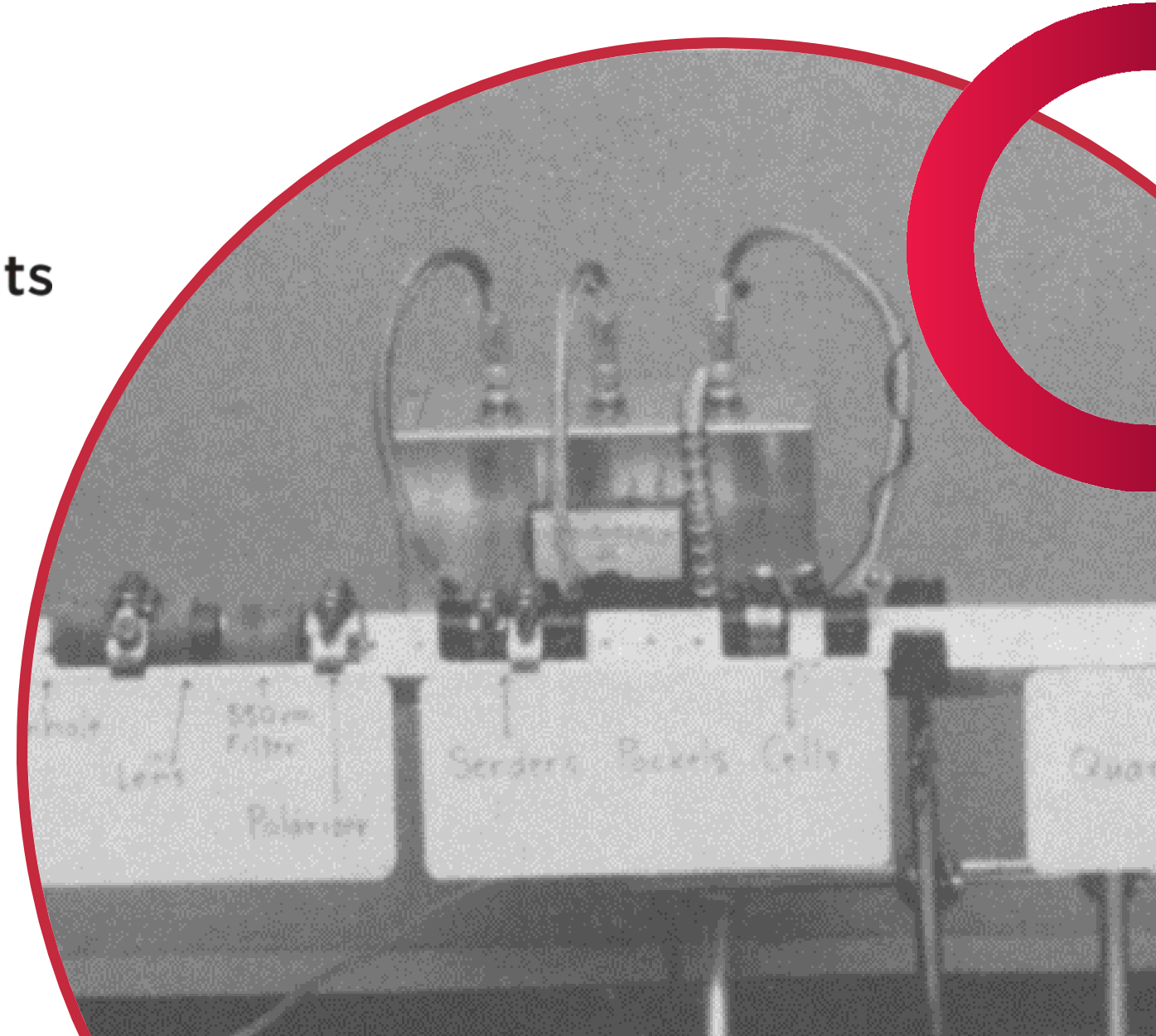
UNIVERSITY OF WATERLOO | IQC Institute for Quantum Computing

QSYS Quantum School for Young Students

QUANTUM KEY DISTRIBUTION

RAMY TANNOUS
+ John Donohue



Stuff to Recall

Superposition is a relative concept
depending on a choice of mutually exclusive states

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \quad |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} \qquad |0\rangle = \frac{|+\rangle + |-\rangle}{\sqrt{2}} \quad |1\rangle = \frac{|+\rangle - |-\rangle}{\sqrt{2}}$$

The particle is both
"0" AND "1"
at the same time

BUT

When measured in the 0/1 basis,
it will be found as
"0" OR "1"
randomly

Measurement Basis
Defines which "question"
I ask the particle

The particle is both
"+" AND "-"
at the same time

BUT

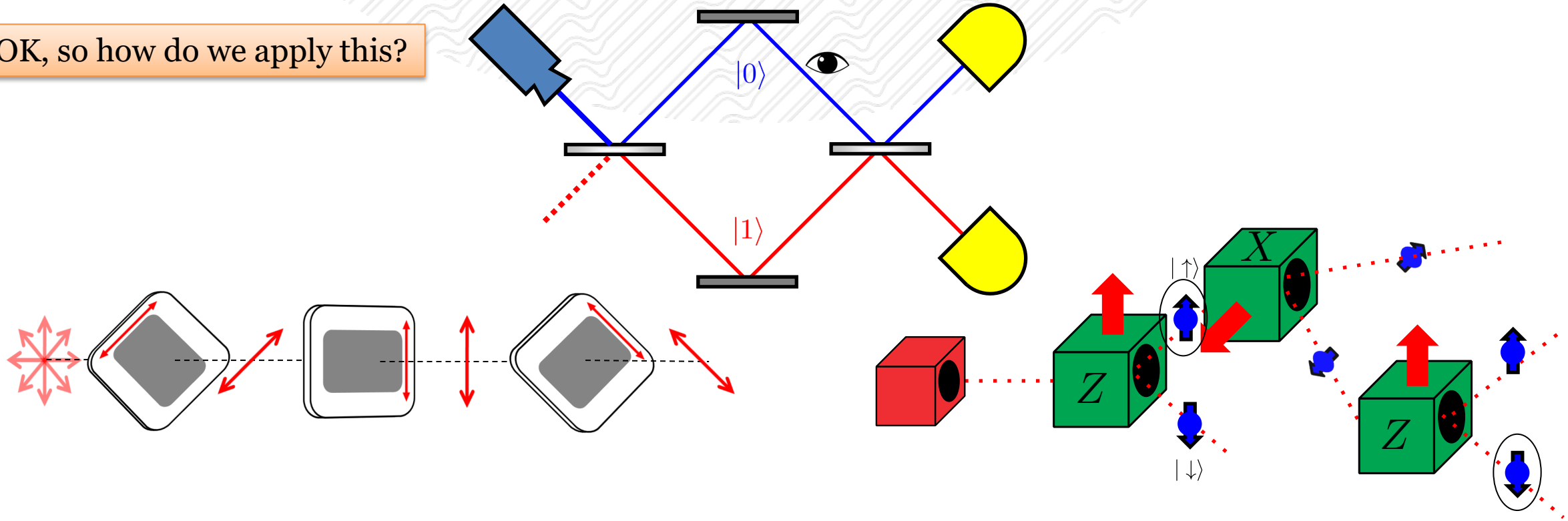
When measured in the +/- basis,
it will be found as
"+" OR "-"
randomly

Stuff to Recall

Measurement asks the photon a **question**

When forced to answer, the quantum state can change

OK, so how do we apply this?



Quantum Key Distribution

- Secret keys and the one-time pad
- The BB84 quantum protocol
- The no-cloning theorem
- Implementations of BB84

Keys and Security

Alice

Secure channel

Bob

Alice and Bob use a secure channel to share **identical** copies of a key

Keys and Security

Alice

Bob

Secure channel

An eavesdropper can see the safe, but can't open it without the key

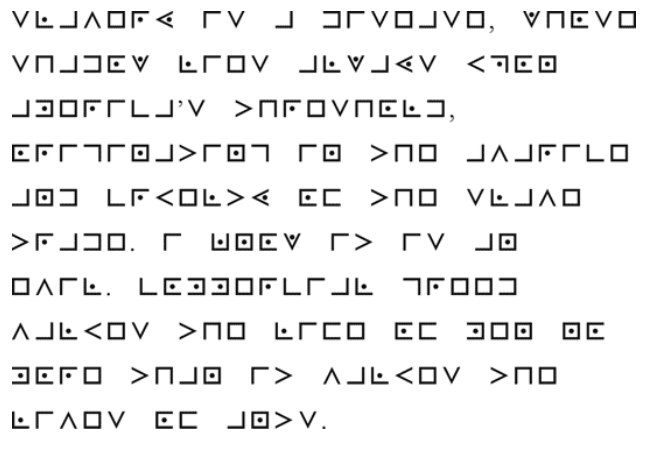
Public channel

Keys

- In real life, the key is **information** (i.e. Binary string)
- Alice and Bob have the information, but the eavesdropper doesn't

Safe
Key: The PIN Number

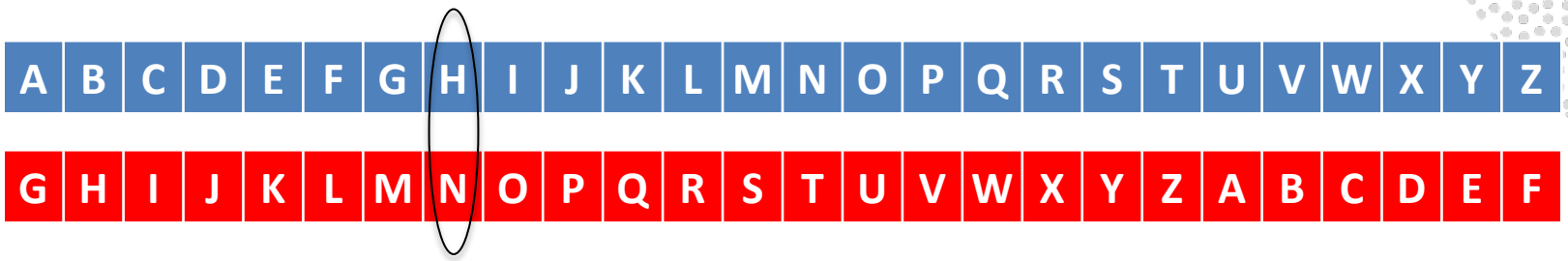
Door Lock
Key: Which pins to press



Secret Code
Key: Translation back to English

Question Break

The Caesar Cipher



HELLO —Encrypt→ NKRRU —Decrypt→ HELLO

= 6 letter shift

= NKRRU ciphertext

Big Problem!
If you know **one** encrypted letter,
you know **the whole message**!

Many apps and websites are
active that can crack theses

The Substitution Cipher

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Z	T	W	B	M	Q	K	I	N	V	H	J	U	O	X	C	S	P	G	A	R	F	L	Y	E	D

Random shuffle of the alphabet

HELLO —Encrypt→ IMJJX —Decrypt→ HELLO

 = 26 random substitutions

 = IMJJX ciphertext

Now have to test many more possibilities
26! ~ 400 trillion trillion

Still a big problem!
Once we crack a piece of the puzzle,
we can crack the whole thing

Context: US domestic policy
What could this ciphertext mean?

ABCCBCCBDDB

MISSISSIPPI

The One-Time Pad (aka Vernam cipher)

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T

A different Caesar cipher for each letter

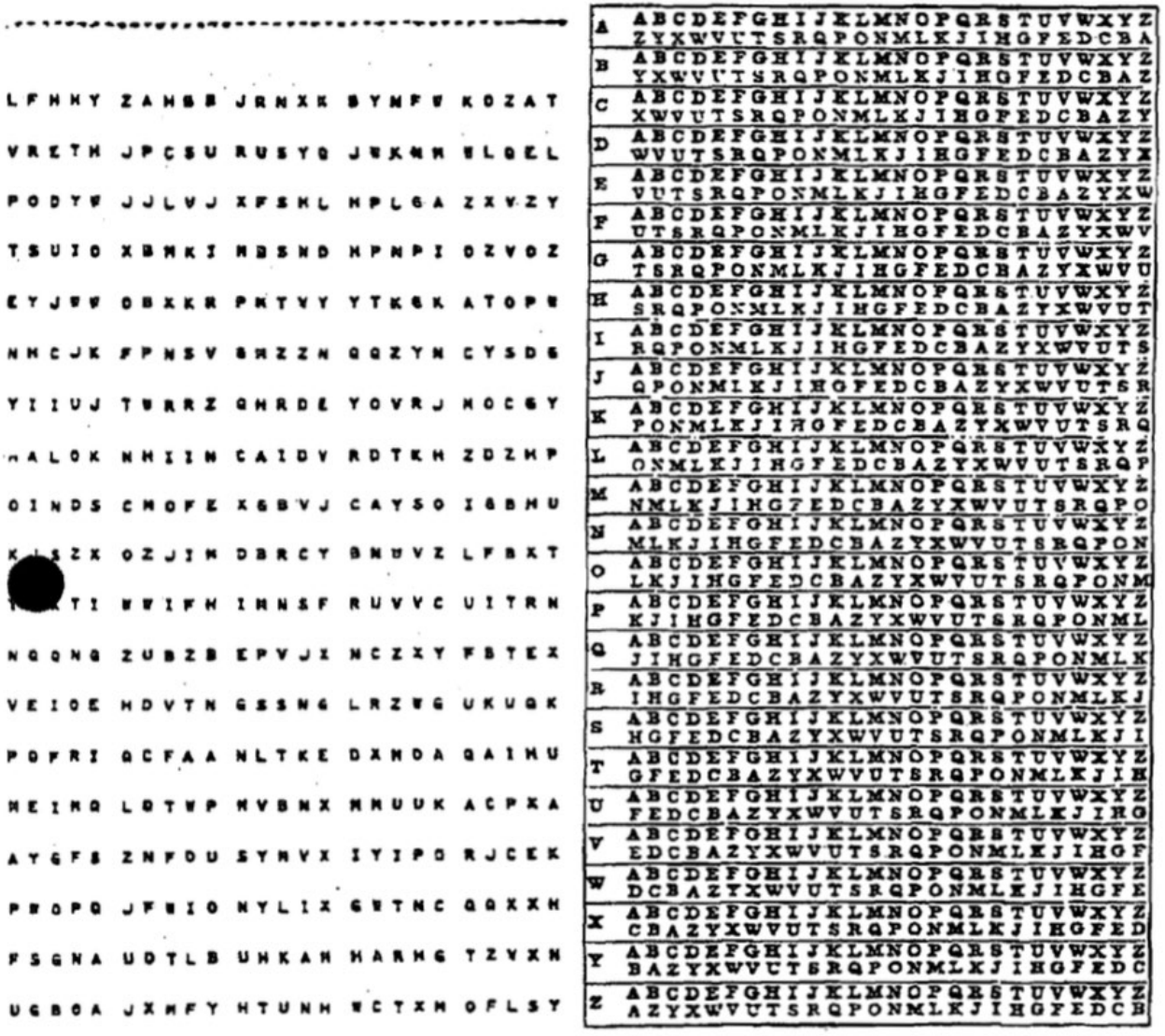
HELLO —Encrypt→ SUXOI —Decrypt→ HELLO

= 5 random shifts

= SUXOI ciphertext

History of One-Time Pad

- First described in 1882
- Rediscovered by Vernam in 1917
- Widely used in the World Wars



NSA DIANA one time pad - One-time pad - Wikipedia

The One-Time Pad

Message	01101000
Key	01001001
Cipher	00100001

Cipher	00100001
Key	01001001
Message	01101000

Message Bit \ Key Bit	0	1
0	0	1
1	1	0

Alice and Bob share a long random binary string

Encode and decode by adding mod 2 (XOR)

The One-Time Pad

Message	01101000
Key	01001001
Cipher	00100001

Cipher	00100001
Key	01001001
Message	01101000

8-bit key
2^8 possible keys
Number of possible keys = Number of possible messages

Perfectly secure!
But we're forgetting something…

One-Time Pad Big-Time Problem

Alice

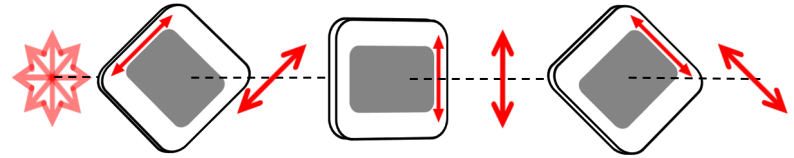
Bob

How do Alice and Bob securely share the key
in the first place?

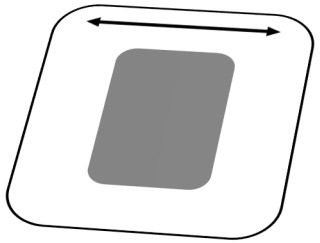
A Quantum Solution

Alice and Bob generate the key by sending polarization-encoded photons to each other

A Quantum Solution



Remember the three polarizers?



If the eavesdropper intercepts,
they'll disturb the polarization state

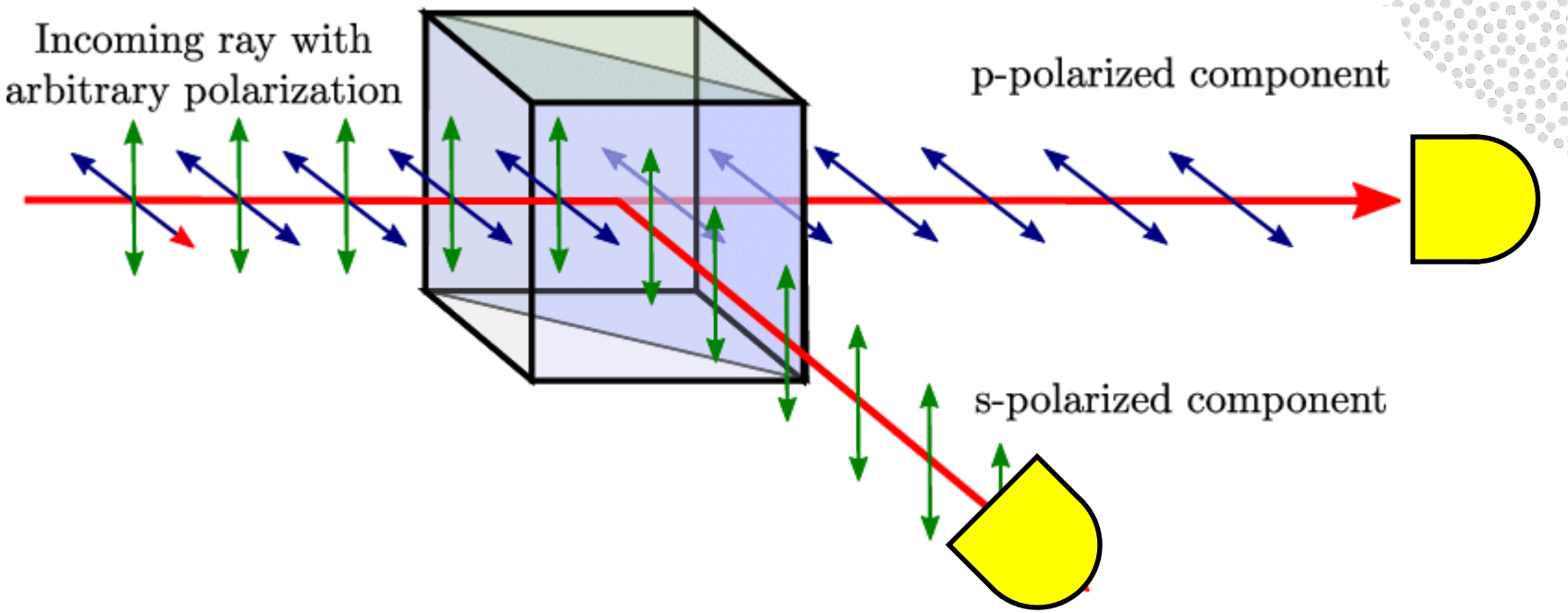
Polarization Qubits

	HV BASIS	±45° BASIS
0	→	↗
1	↑	↘

Encode binary “0” or “1” as a polarization state, with two possible bases

	H/V measurement	A/D measurement
→	H for sure	random
↑	V for sure	random
↗	random	D for sure
↘	random	A for sure

How To Measure Polarization



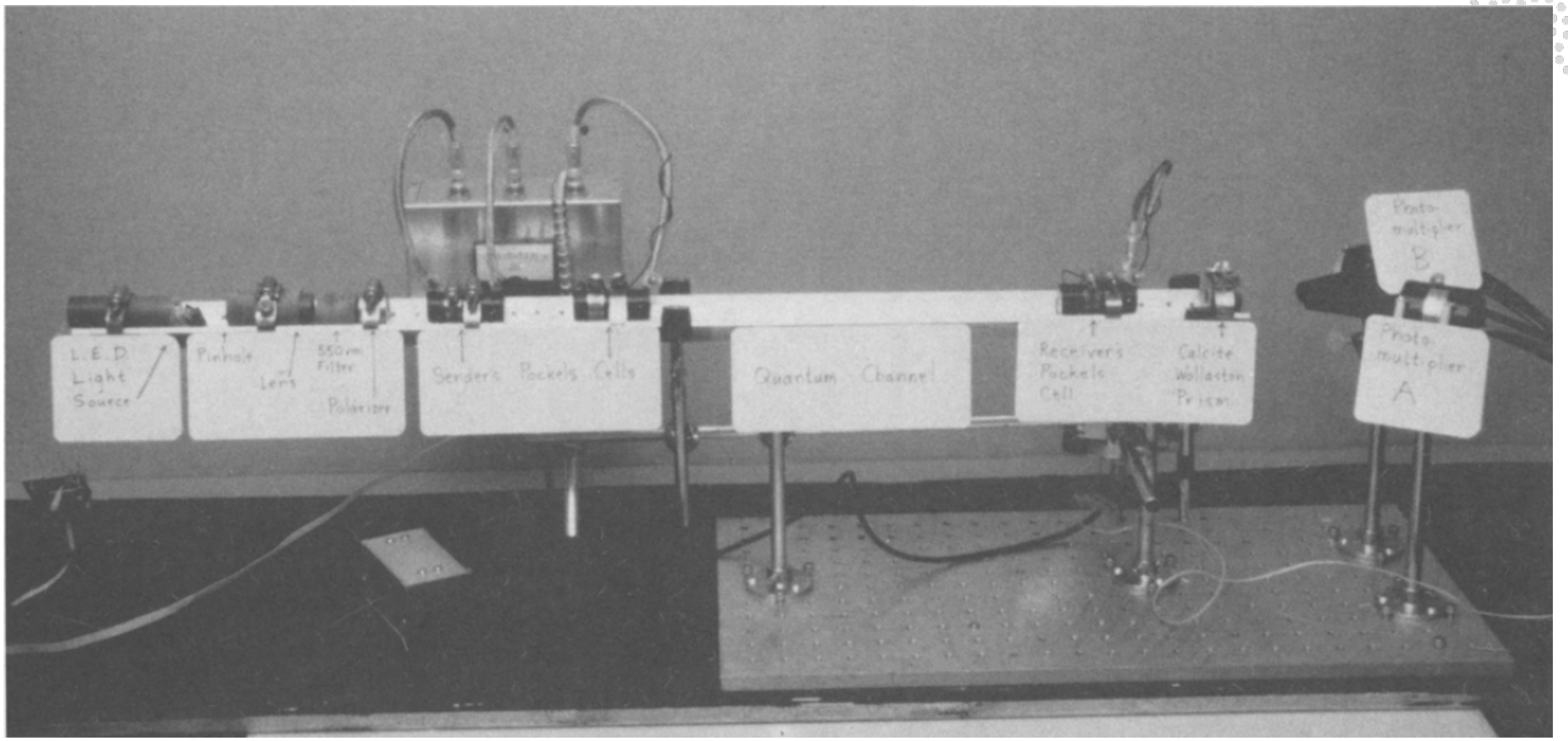
A polarizing beamsplitter diverts each polarization in a different direction

Putting a detector in each path works as an H/V measurement

By rotating the PBS, we can perform a D/A measurement, or any other angle

Question Break

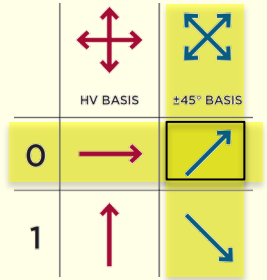
The BB84 Protocol



The BB84 Protocol

Step 1
Alice chooses
"0" or "1" randomly

Step 2
Alice chooses the
H/V or D/A basis randomly



"0"
"D/A"

Alice's Lab

Step 7
Repeat and repeat until a long, random binary string is built

Step 3
Alice encodes the appropriate qubit
and sends it to Bob as a single photon

Step 6
Alice and Bob publicly announce which bases they used,
keeping their bit values secret

I used the
"D/A" basis

I used the
"D/A" basis

Step 4
Bob randomly chooses
a measurement basis

Step 5
Bob records the result
of his measurement

"0"   "1"

"D/A"
"0"

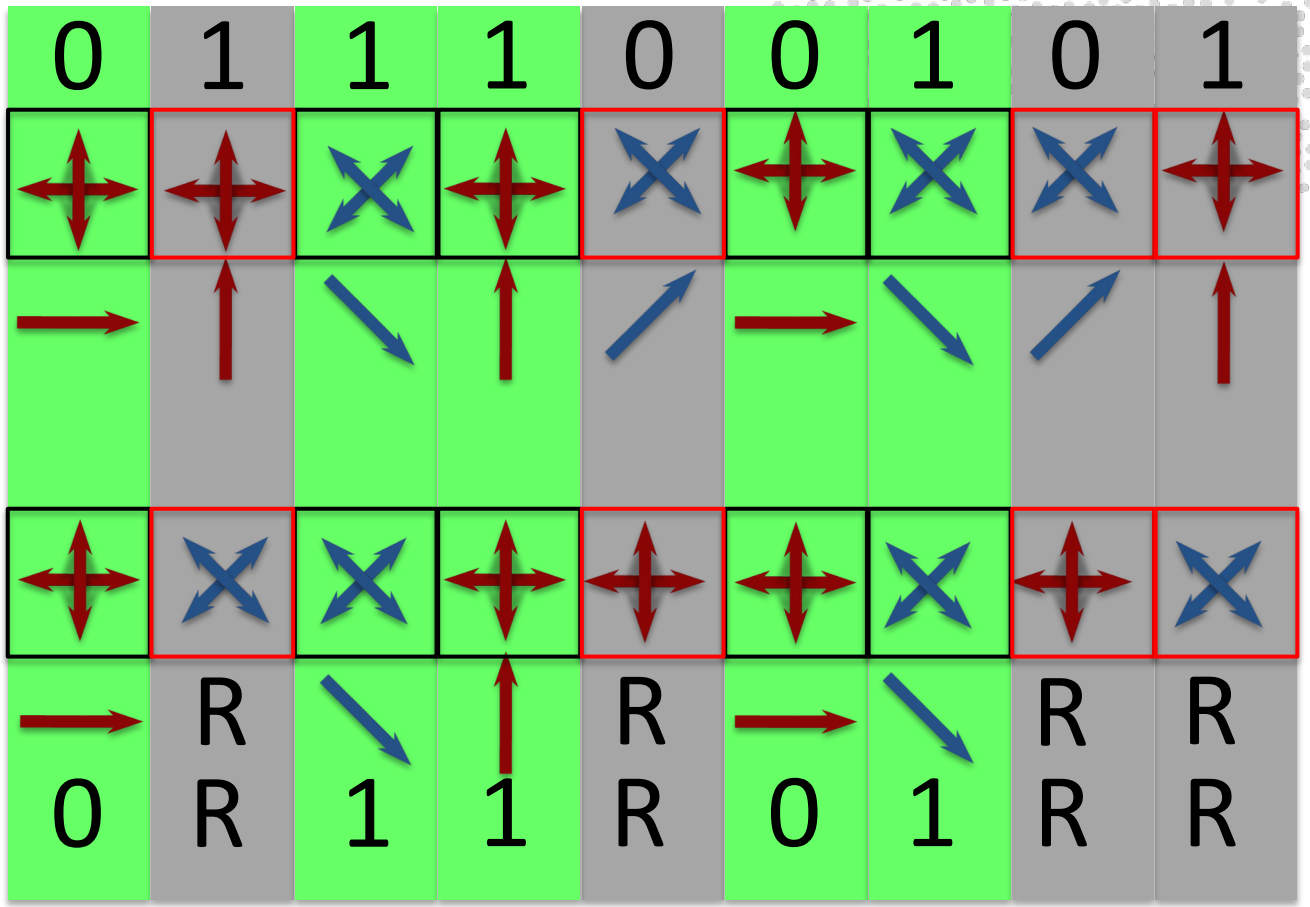
Bob's Lab

BB84 Example

1. Alice chooses a RANDOM bit
2. Alice chooses a RANDOM basis
3. Alice send the state to Bob

4. Bob measures in a RANDOM basis
5. Bob records the bit

6. Alice and Bob announce the basis



Alice and Bob are performing the BB84 protocol. In some of the rounds their basis selection doesn't match and results in a random measurement for Bob. What should Alice and Bob do to these cases to ensure they share the same key?

A. Discard these rounds

B. Alice shares what she sent

C. XOR the random cases

D. Keep them and try to correct for errors later

E. Try RSA instead

They can simply discard them with no consequence to security

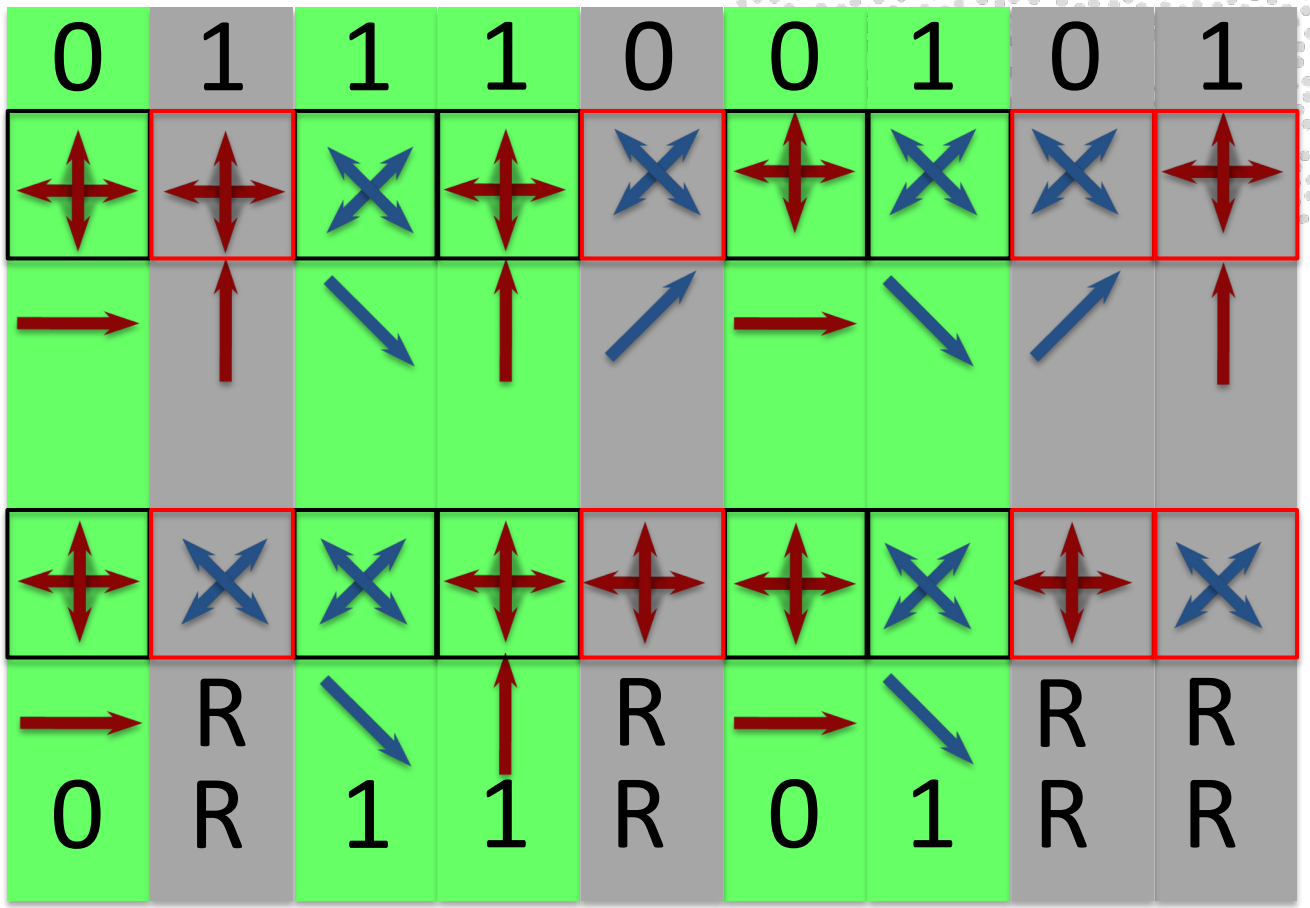
BB84 Example

Basis Reconciliation
Alice and Bob discard all bits
where their bases didn't match

This leaves them with the secret key

`01101`

What if there's
an eavesdropper?



0	1	1	1	0	0	1	0	1
✚	✚	✖	✚	✖	✚	✖	✖	✚
→	↑	↘	↑	↗	→	↘	↗	↑

✚	✚	✚	✚	✚	✚	✚	✚	✚
→	↑	R	↑	R	→	R	R	↑
0	1	R	1	R	0	R	R	1

✚	✖	✖	✚	✚	✚	✖	✚	✖
→	R	R	↑	R	→	R	R	R
0	R	R	1	R	0	R	R	R

Catching Eve

- If Alice and Bob make truly random basis choices,
  Eve will guess wrong half the time
- Half of the time Eve guesses wrong, they will introduce an error
- Therefore, an always-present eavesdropper
  will introduce an error rate of 25%!

What is the approximate probability that an eavesdropper can measure 100 qubits **without** introducing a **single** error?

A. One in 100

B. One in one million

C. One in one billion

D. One in one trillion

E. Absolute 0%

Error Estimation and Correction

Parity Check
See if addition of neighbouring bits
(modulo 2)
matches over the whole string

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

"Raw" Key

"Raw" Key

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

1	0	1	0
✓	✓	✗	✓

Communicate Publicly

1	0	0	0
✓	✓	✗	✓

✗	0	0	✗	1	0	✗	✗	✗	✗	0	1

Discard sets with errors
&
One bit from each
correct set
to maintain secrecy

✗	0	0	✗	1	0	✗	✗	✗	✗	0	1

0	0	1	0	0	1

Final Key

0	0	1	0	0	1

Final Key

Privacy Amplification

What if the eavesdropper didn't measure every time?
Could they have some partial information?
How do we distinguish that possibility from systematic errors?

- We must assume that all errors come from a potential eavesdropper!
- If the error rate is greater than 11%, no secret key is possible*
- If smaller than 11%, we can keep shrinking the key via parity checks until Eve has no information about the key left
- The higher the error rate, the less key we get to keep at the end of the day

Examples:

With an error rate of 4% and a 2,000 bit raw key, we can keep ~750 secret bits

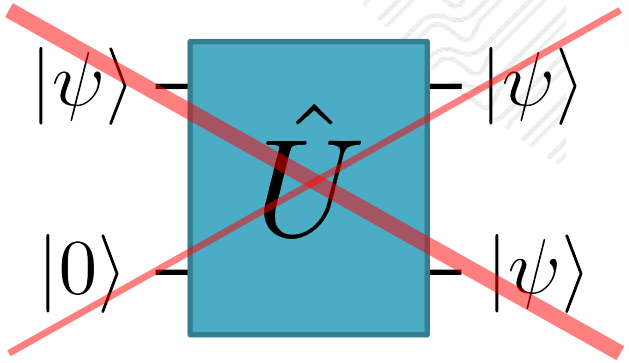
With an error rate of 8% and a 2,000 bit raw key, we can keep ~100 secret bits

*proof a bit complicated, see Shor & Preskill, Phys. Rev. Lett 85, 441 (2000).

A Loophole?

- Alice and Bob are generating a **random** key which they will use to encrypt **future** secret messages
- The only quantum part is the qubit transmission, all the rest is classical post-processing
- But what if Eve can make a copy of the bits?

The No-Cloning Theorem



There exists no unitary which can create a perfect copy of an unknown quantum state

W.K. Wootters & W.H. Zurek, Nature 299, 802 (1982)

$$\text{GOAL} : U|\psi\rangle|0\rangle = |\psi\rangle|\psi\rangle$$

$$\text{REALITY} : \hat{U}|0\rangle|0\rangle = |0\rangle|0\rangle$$

$$\hat{U}|1\rangle|0\rangle = |1\rangle|1\rangle$$

GOAL :

$U|\psi\rangle|0\rangle = |\psi\rangle|\psi\rangle$

What will our "cloning machine" do if given the state $|+\rangle$?

$\hat{U}|0\rangle|0\rangle = |0\rangle|0\rangle$

$\hat{U}|1\rangle|0\rangle = |1\rangle|1\rangle$

A. $|+\rangle|+\rangle$

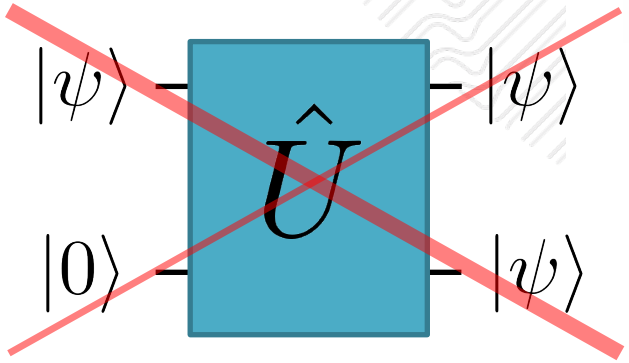
B. $|+\rangle|-\rangle$

C. $(|0\rangle|0\rangle + |1\rangle|1\rangle)/\sqrt{2}$

D. $(|0\rangle|1\rangle + |1\rangle|0\rangle)/\sqrt{2}$

E. None of the above

The No-Cloning Theorem



There exists no unitary which can create a perfect copy of an unknown quantum state

W.K. Wootters & W.H. Zurek, Nature 299, 802 (1982)

$$\text{GOAL} : U|\psi\rangle|0\rangle = |\psi\rangle|\psi\rangle$$

$$\text{REALITY} : \hat{U}|0\rangle|0\rangle = |0\rangle|0\rangle$$

$$\hat{U}|1\rangle|0\rangle = |1\rangle|1\rangle$$

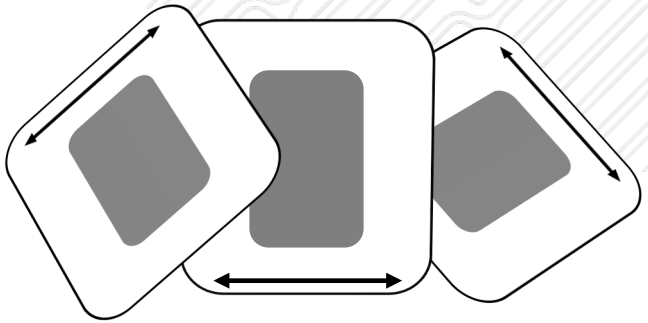
$$\hat{U}\frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)|0\rangle = \frac{1}{\sqrt{2}}\left(\hat{U}|0\rangle|0\rangle + \hat{U}|1\rangle|0\rangle\right)$$

$$= \frac{1}{\sqrt{2}}\left(|0\rangle|0\rangle + |1\rangle|1\rangle\right)$$

$$\neq \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)\frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)$$

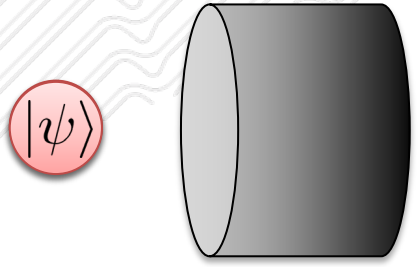
The Heart of QKD

Measurement Disturbance



When we measure a quantum state,
we disturb it

The No-Cloning Theorem



FORBIDDEN

Assumptions, classical channel is authenticated
(Eve can't pretend to be Alice or Bob)

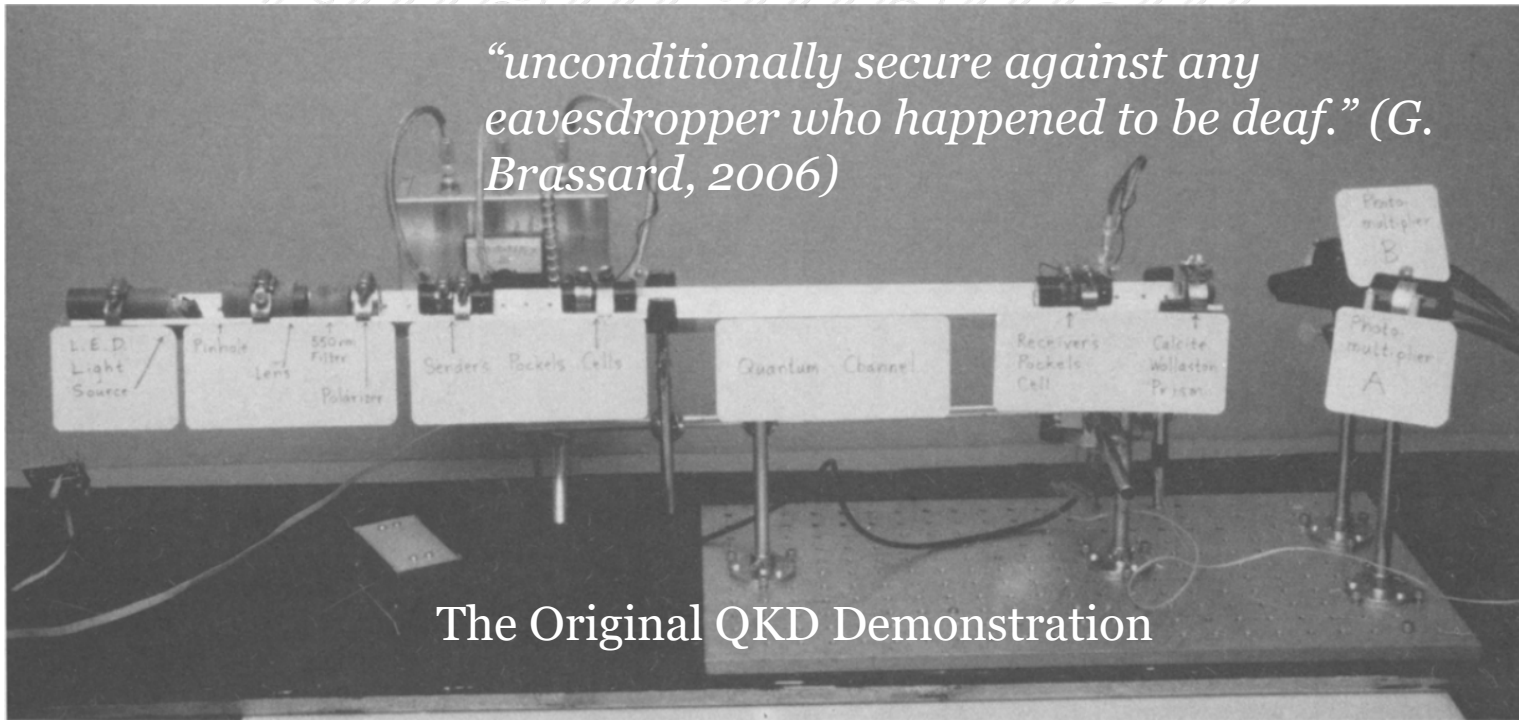
So what do we need in the lab?

- Single photon sources
  - Very difficult
  - Often use a very weak laser, which has a single photon on average
- Single photon detectors
  - Getting better and better, but expensive
  - Sometimes possible to hack, ruining security
- Ways to control photon polarization
  - Half-wave plates for polarization rotations, polarizing beam-splitters for measurement
  - Or encode qubits in an entirely different degree of freedom, like time
- A channel for single photons
  - Can use optical fiber, just like telecommunications
  - Can use free-space channels or even satellite links

Hacking QKD

QKD security is guaranteed by the laws of physics!

But compromised by the reality of engineering

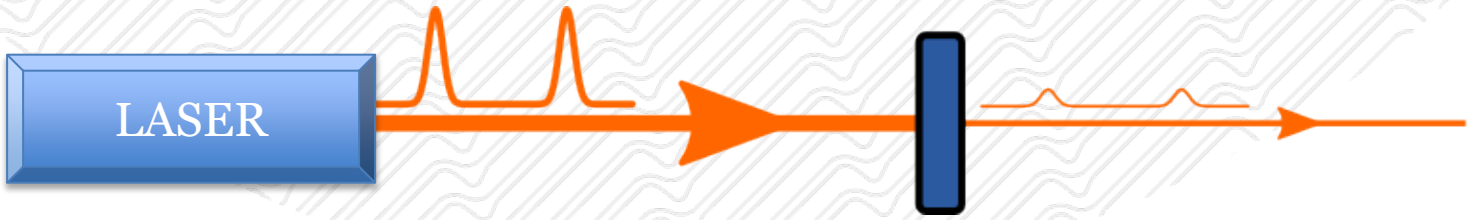


"unconditionally secure against any eavesdropper who happened to be deaf." (G. Brassard, 2006)

The Original QKD Demonstration

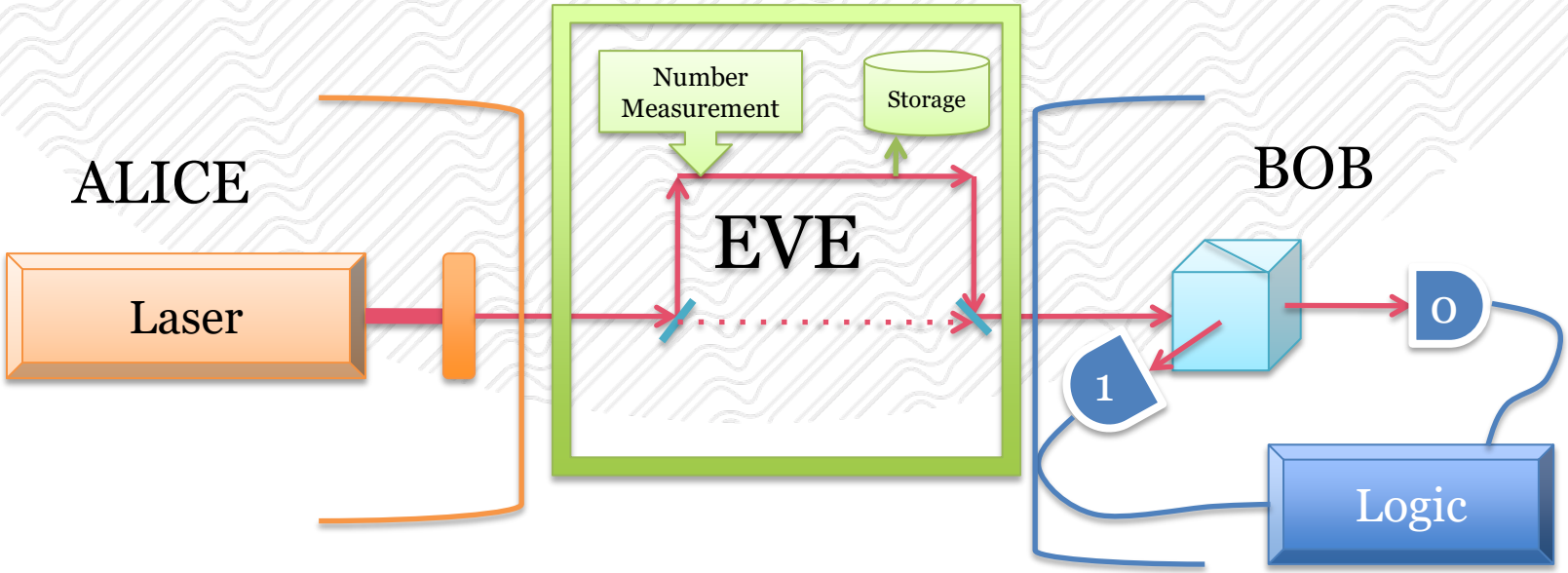
The Photon-Number Splitting Attack

- The easiest way to make photons: a weak laser beam



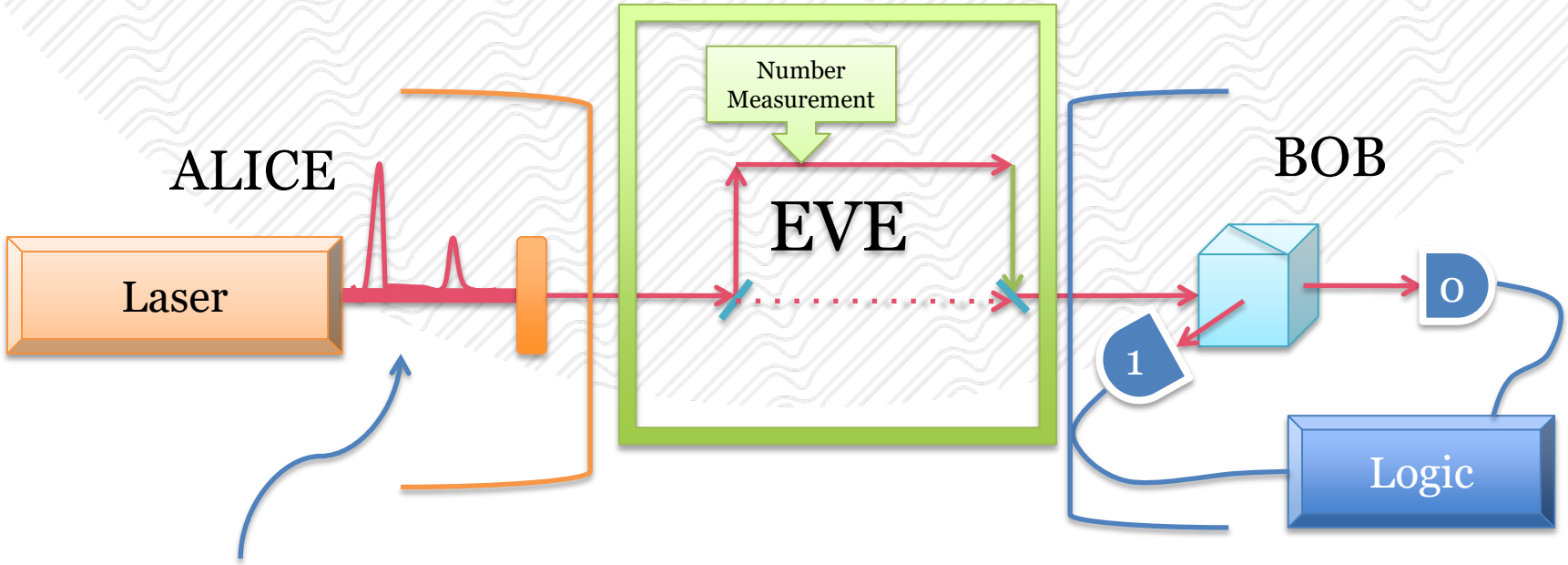
- Impossible to always have one photon using this scheme
- Multi photons = same polarization state
- Eve can take advantage to learn the bit without disturbing!

The Photon-Number Splitting Attack



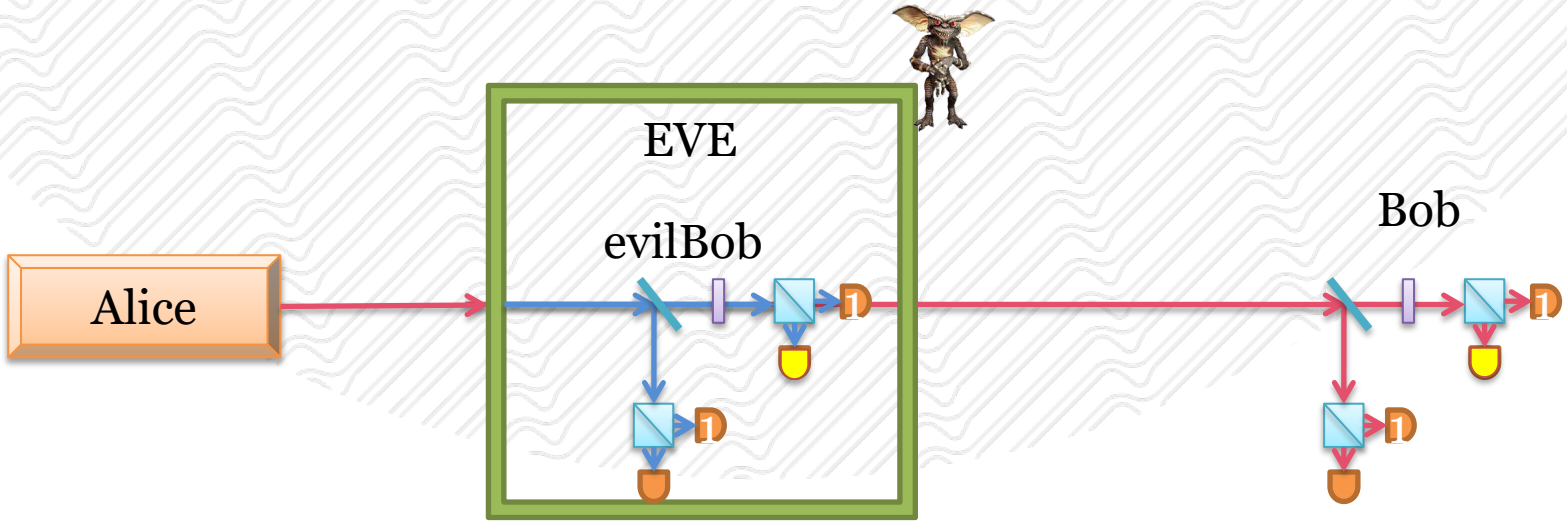
1. Alice sends a pulse, with average photon number < 1
2. Eve counts photons in the pulse
   a) If photons = 1, Eve blocks the pulse
   b) If photons > 1, Eve stores one and sends the rest to Bob
3. When Alice and Bob communicate basis information, Eve measures her stored photons in the correct basis and gets all information
4. If loss introduced by Eve < expected system loss, Alice and Bob notice nothing

The Decoy State Protocol



1. Alice now sends pulses of different average photon number
2. Eve still blocks pulses with only one photon, meaning she selectively blocks pulses with lower average photon number!
3. By comparing how many pulses arrive for different sizes of pulses, Alice and Bob can detect the photon number splitting attack

Detector Control Attack



- If Eve can control Bob's detectors, they can make sure Bob always sees the same results as them
- Most if not all photon detectors could be vulnerable

Is this level really the problem?

Business Insider 2018 Jan 16,
“A password for the Hawaii emergency agency was hiding in a public photo, written on a Post-it note.”

Well, maybe someday...

Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*

Peter W. Shor†

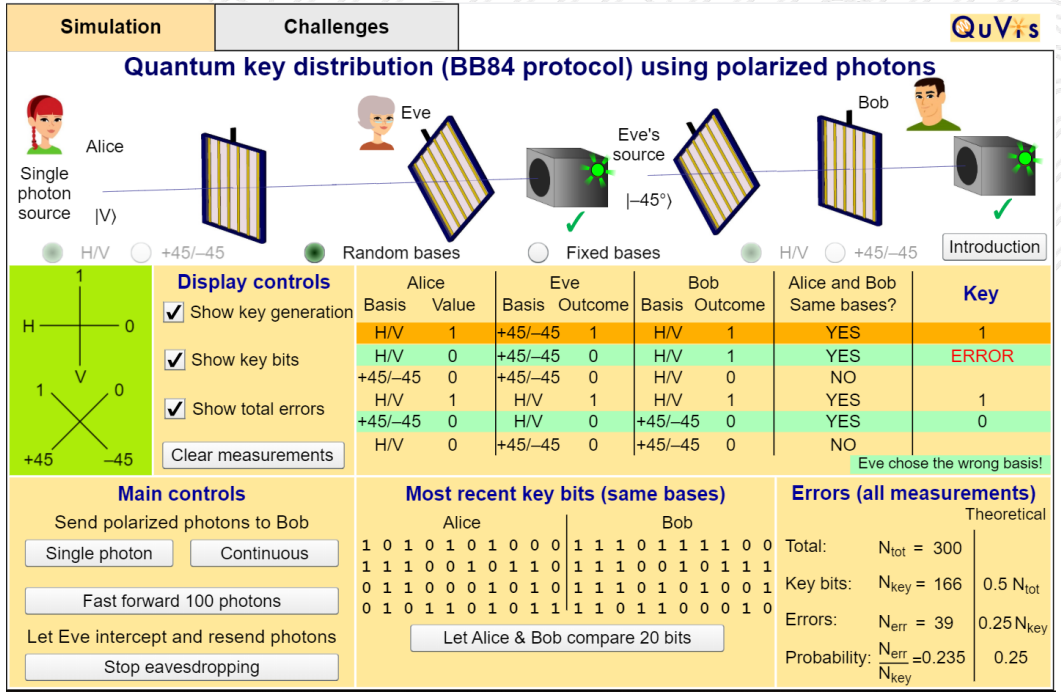
Abstract

A digital computer is generally believed to be an efficient universal computing device; that is, it is believed able to simulate any physical computing device with an increase in computation time by at most a polynomial factor. This may not be true when quantum mechanics is taken into consideration. This paper considers factoring integers and finding discrete logarithms, two problems which are generally thought to be hard on a classical computer and which have been used as the basis of several proposed cryptosystems. Efficient randomized algorithms are given for these two problems on a hypothetical quantum computer. These algorithms take a number of steps polynomial in the input size, e.g., the number of digits of the integer to be factored.

Keywords: algorithmic number theory, prime factorization, discrete logarithms, Church's thesis, quantum computers, foundations of quantum mechanics, spin systems, Fourier transforms

AMS subject classifications: 81P10, 11Y05, 68Q10, 03D10

Quantum Key Distribution



Try the simulator
by St. Andrew's University

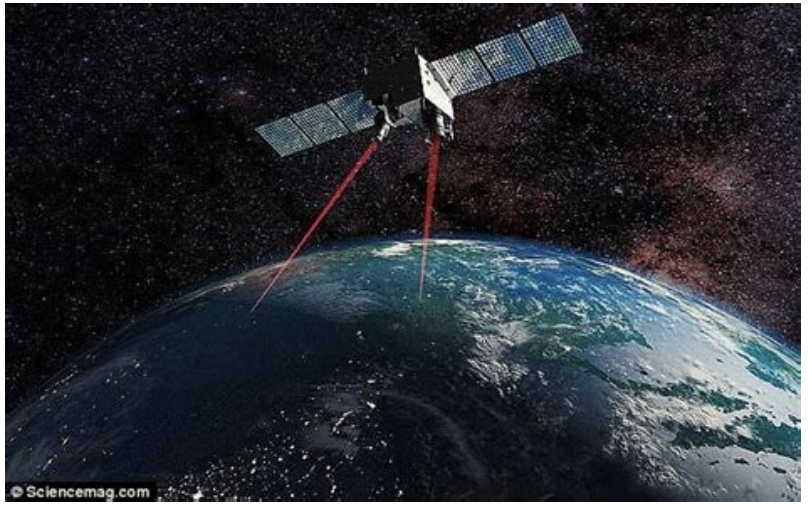
st-Andrews.ac.uk/physics/quvis
Quantum Cryptography (B92)

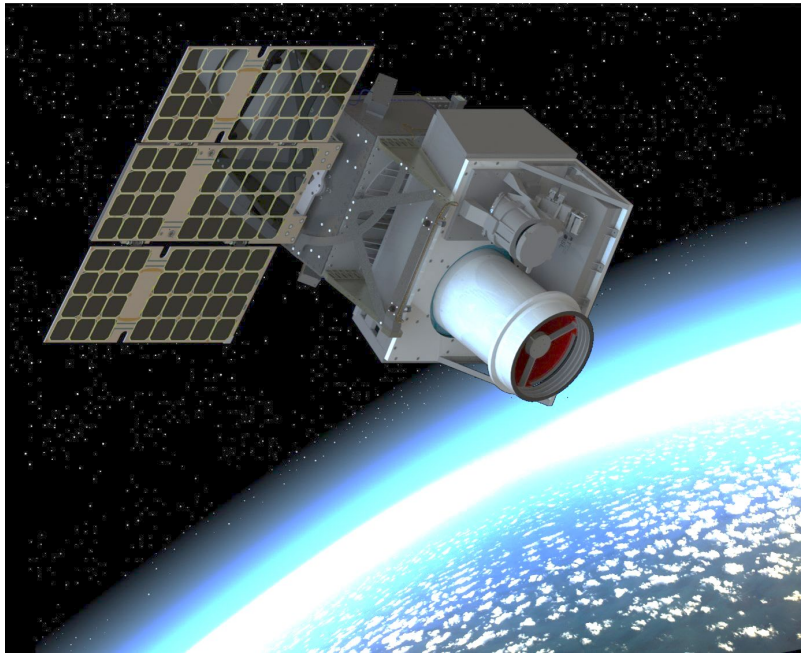
Many slides stolen from:
- Evan Meyer-Scott
- Electra Eleftheriadou
- Martin Laforest

Other types of protocols

- Six state
  - Three bases instead of only two
    - How does this help?
- Time bin
  - Different encoding
  - Do not always have to use polarization
- Entanglement based
  - Why not add more Quantum?

There is much more to QKD






IQC
IQC
QPL

Thank You