S. KIMMEL

# Quantum Cryptography

Goals :

- Qualitative understanding of Quantum measurement

## Cryptography


(Notation: $\{0,1\}^n$ = set of n-bit strings. E.g. $\{0,1\}^2 = \{00,01,10,11\}$)

# Best Crypto Method: secret key

## Secret Key Protocol

0. Alice and Bob share a secret bitstring $s \in \{0,1\}^n$
1. Using $s$ and $m$, Alice creates encrypted message $\bar{m}$ where $\bar{m}_i = m_i \oplus s_i$

   $i$ signifies $i^{th}$ bit of string

   $\oplus$: addition mod 2

| $\oplus$ Truth Table | | |
|---|---|---|
| $x$ | $y$ | $x \oplus y$ |
| 0 | 0 | 0 |
| 0 | 1 | 1 |
| 1 | 0 | 1 |
| 1 | 1 | 0 |

2. Alice sends $\bar{m}$ to Bob.
3. Bob decrypts $\bar{m}$ by setting $m_i = \bar{m}_i \oplus s_i$

Why Secure? See PSet 1.

## Problem with Secret Key Crypto?

- Step 0.
  - → How can Alice and Bob share a secret key?
  - → Big problem for e-commerce

Quantum lets Step 0 occur securely

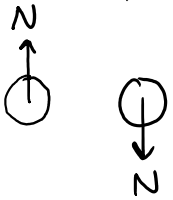
S. KIMMEL

# Quantum Bit (qubit)

- Quantum Bit → 2-state system
- (qubit) → 2-state quantum system

ex:


electron orbital (s or p)




spin of electron (up or down)

photon polarization (horizontal or vertical)

Use photon polarization for crypto

- Fast (speed of light)
- Easy to send (see PSet 1)

Polarizer Demo ~$10^{20}$ photons/second from bulb

Q: If insert diagonal filter between horizontal + vertical polarizers, how much light will come through?

A. None B. A little C. A lot

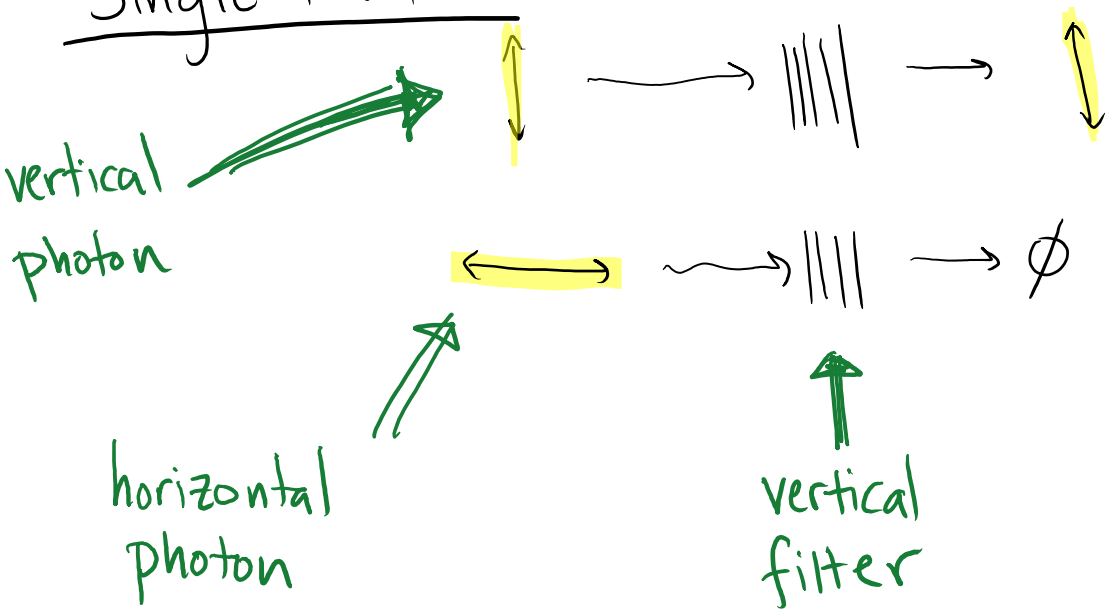
S.KIMMEL

Q: If insert diagonal filter between horizontal + vertical polarizers, how much light will come through?

A. None  **B. A little**  C. A lot

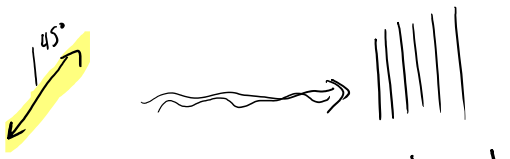
Now:

## Single Photon:



S.KIMMEL

What will happen:




right diagonally polarized photon

vertical filter

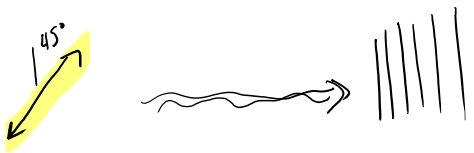
A) A vertically polarized photon appears with ½ energy of original.

B) A right diagonal polarized photon appears with ½ energy of original.

C) A right or left diagonally polarized photon appears with equal probability.

D) A vertically polarized photon appears with probability ½ and no photon exits with probability ½.

What will happen:




right diagonally polarized photon

vertical filter

A) A vertically polarized photon appears with ½ energy of original.

B) A right diagonal polarized photon appears with ½ energy of original.

C) A right or left diagonally polarized photon appears with equal probability.

D) A vertically polarized photon appears with probability ½ and no photon exits with probability ½.

Quantum Measurement: "Are you vertical or horizontal? Choose and stick with your choice!"

First example of quantum weirdness. Take advantage of weirdness for crypto.