CIS 3362 11/13/24

Quiz 5

AIDS

1 SHEET OF NOTES FRONT + BACK

CALCULATOR

CAN DO ~~FAST~~ MOD EXPO IN ANY VALID WAY WITH WORK

E.G. $2^{36} \mod 33$

$$2^{36} = (2^5)^7 \times 2 = (32)^7 \times 2 \equiv (-1)^7 \times 2$$
$$\equiv -2 \equiv 31 \pmod{33}$$

SIMILAR TO 2023 QUIZ...

QUANTUM CRYPTOGRAPHY 11/13/24

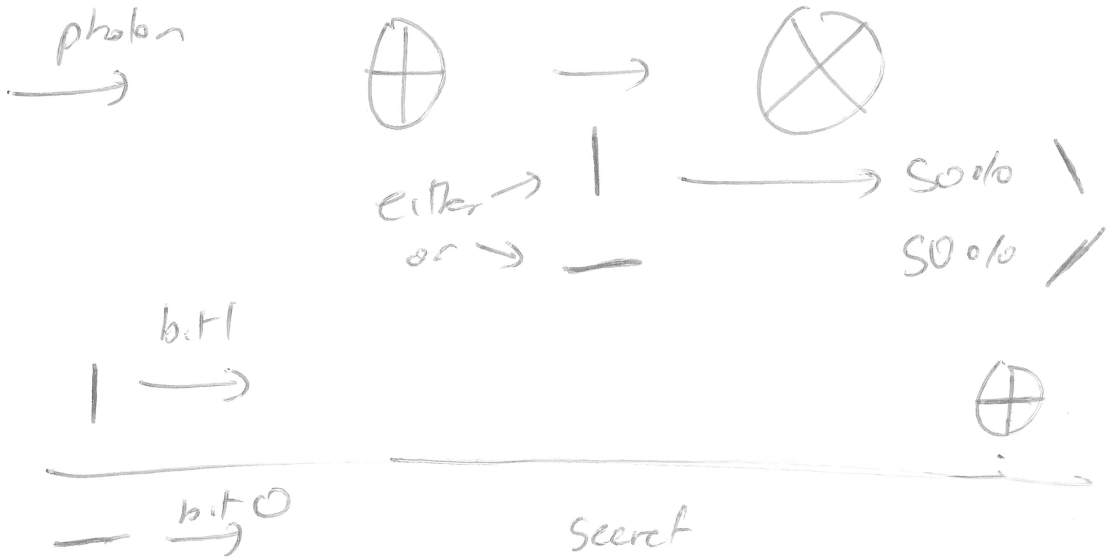
particles (photons) fiber optic cable

state when not observed is "unknown"
but if we try to observe a photon we'll "force" it into a particular state.

READERS 2 ORIENTATIONS

⊕ HV reader

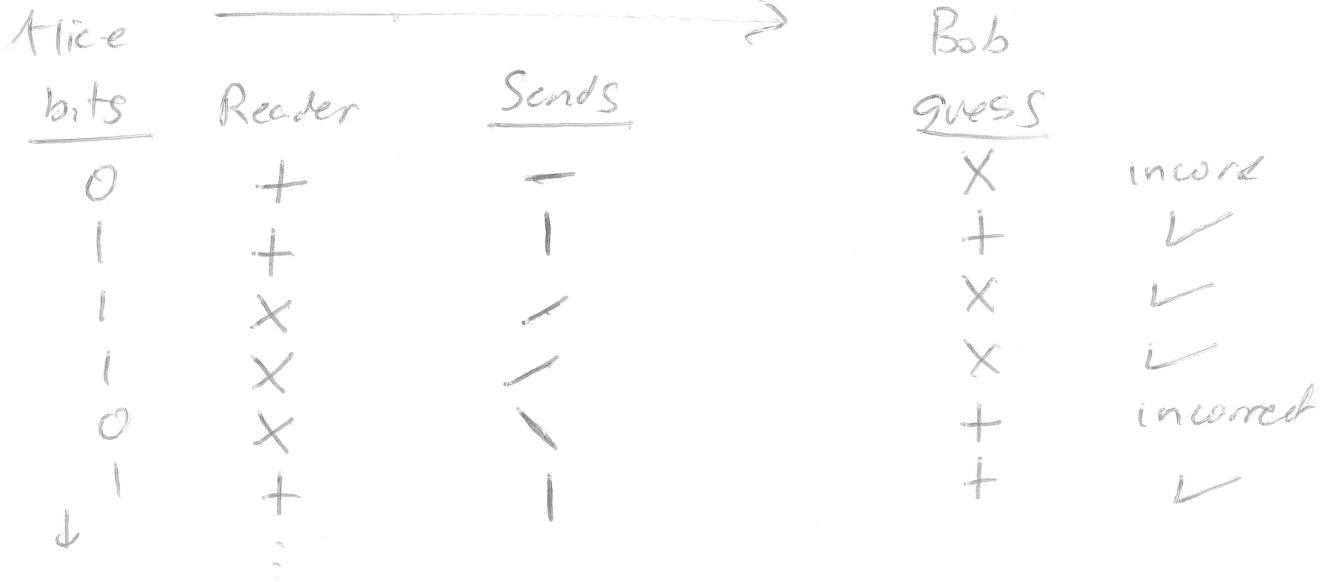
⊗ Diag reader



How to exchange a secret key with high probability knowledge that NO ONE ~~WAS~~ LISTENING.

Alice Bob

GOOD VERSION



If bob guesses the correct reader, then he'll receive the correct bit. If not, it'll random.

200 Pick Sample Bits Won't Use: bit # 7, 11, 12, 15, 22, ...

↳ Alice says OK correct reader on bits 7, 12, 30, ...
↳ on avg 100 bits (½ of sample)
↳ Bob tells Alice what he read.
If no one was listening all 100 bits will match what Alice sent.

↳ If this happens, we'll conclude NO ONE WAS LISTENING and use the other bits where Bob use right reader for the key

1800 left → 900 Bob right reader

BAD VERSION

Alice			Eve		Bob	
bit	Reader	Sent	eve's reader	now	guess	
0	+	—	X	\	X	
1	+	|	X	/	+	✓
1	X	/	+	|	X	✓
1	X	/	X	/	X	✓
0	X	\	X	\	+	
1	+	|	X	\	+	✓

IF Alice, Bob use same reader, but Eve a different reader, 50% time Bob will read a different bit than Eve sent.

Sample n bits

A+B match $\sim \frac{n}{2}$ bits.

A+B match AND Eve wrong $\sim \frac{n}{4}$ bits

The photon wiggles through correctly all $\frac{n}{4}$ probability times is $\left(\frac{1}{2}\right)^{\frac{n}{4}}$

$$p(\text{eve undected}) = \left(\frac{1}{2}\right)^{\frac{200}{4}} = \left(\frac{1}{2}\right)^{50} < 10^{-15}.$$

w/ $n = 200$

how label bit need send 1024 bit key exchanged + plan on sampling 500 bits

$1024 \times 2 + 500 + \text{buffer} = 2548$ → in real life

GOOD

really secure because physics behind

BAD

expensive + difficult !!!