# CIS 3362 11/10/25

Today: Quantum Cryptography
Wed: Quiz Review
Fri: Quiz

→ completely from Code Book

Send photons ⟶

---

fiber optic cable

each photon has an orientation ⊗, can spin anywhere 360°, / | \ —

Reader for a photon ⊕ HV ⊗ FB

Send a photon through HV reader on V, then try to read it again on HV reader then it'll definitely be V.

---

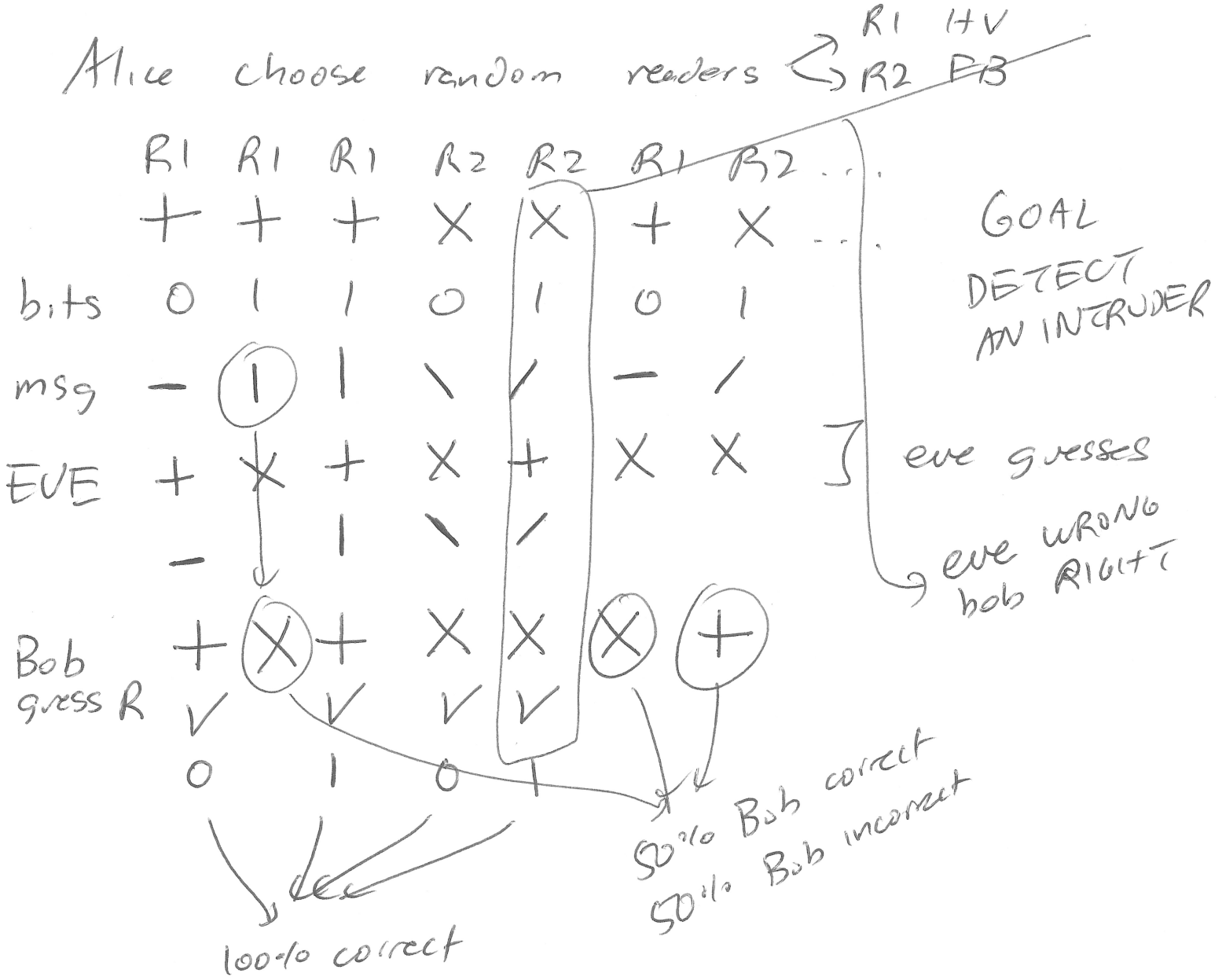
Send a photon through FB reader as F the 2nd FB reader will also read F

---

Issue if you send a V photon using HV reader but try to read it later with FB reader, you'll get each result ~ 50% of the time.

Alice ⊕ HO —V|→ ⊕ eve —→ ⊕ Bob

Describe a key exchange method via quatum particles.




Possible Eve guesses wrong + Bob guesses right

$$\frac{1}{2} \times \frac{1}{2} = \frac{1}{4}$$

Probability Bob gets correct reading in this case $\frac{1}{2}$

$\frac{1}{8} = \frac{1}{4} \times \frac{1}{2}$ → eve guesses wrong, bob guesses right, bob gets WRONG BIT!

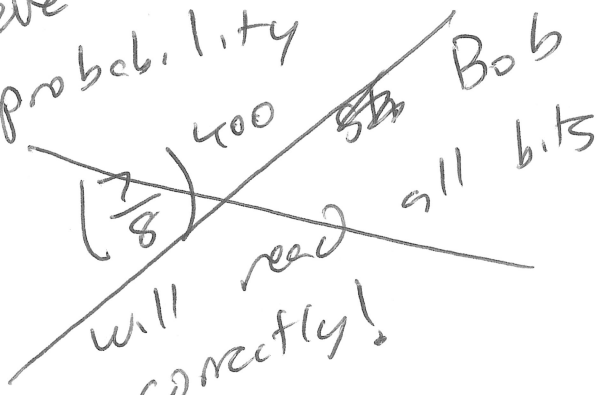
Idea: Send lots of bits say

$2 \times \underbrace{1024}_{\text{sent}} + \underbrace{400}_{\text{sample}} \sim 2500$

↑ 50% bob misses

Choose 400 bits at random to sample.

If eve was listening w/ probability $(\frac{1}{8})^{400}$ Bob will read all bits correctly!



to exchange secret key send $2X + S + \text{Buffer}$ bits.

Sample S bits. For all that Bob used the correct reader, verify Bob got the correct answer. If he did, the transmission was clean and no one was listening.

Figure out of the 2X bits which ones Bob picked correct reader + those bits are the secret key.

What will really happen →

~ 200 get thrown out since Bob guess wrong.

out of 200 left, eve guessed correctly ~ 100 times of the 100 that eve guessed ~~right~~ wrong + Bob got right probability Bob gets all of these correct is $(\frac{1}{2})^{100}$.

↑ probability eve is undetected

CIS 3362 ECC code explanation
11/10/2025

prime $\sim 2^{20}$ or $2^{24}$

$\frac{\text{prime}}{2^{16}} \sim 15, 16, 17, 18 \ldots$

max x is $\geq \frac{\text{limit}}{\pi} \times 2^{16}$

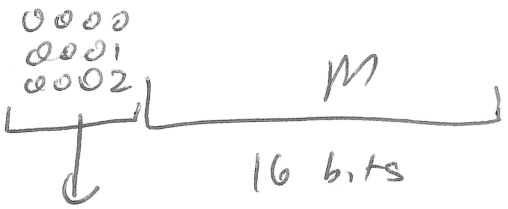
$0 \times 2^{16} + M$

$1 \times 2^{16} + M$

$2 \times 2^{16} + M$

$\vdots$

$(\text{limit}-1) \times 2^{16} + M \rightarrow < \text{limit} \times 2^{16}$




Value

$(i << \text{numbits}) + M$

tried

$0 \times 2^{16} + 10825$ ✗

$1 \times 2^{16} + 10825$ ✓

$\sim 70{,}000$

$x$ Value

I ~~am~~ trying

$= [0 \times 2^{\text{numbits}} + M]$

$\equiv M \bmod 2^{16}$