CIS 3362 - 11/15/21

Quantum Cryptography Chat from Code Bode

| — \ / (particle could be in any orientation)

Reader + "forces" particle to be either | or —

Particles start | or — get "read" correctly with a + reader with probability 1.

Particles start / or \ get "read" as | 50% time and — 50% time.

Alice — Eve? — Bob

1000 bits

	Value	Reader	Send
1.	0	+	—
2.	1	X	/
3.	1	+	|
4.	0	+	—
5.	1	+	|
6.	0	X	\
7.	0	+	

Reader	Bob
+	— 0
+	50% |, 50% —
X	50% /, 50% \
+	— 0
X	50% /, 50% \
X	\ 0
+	— 0

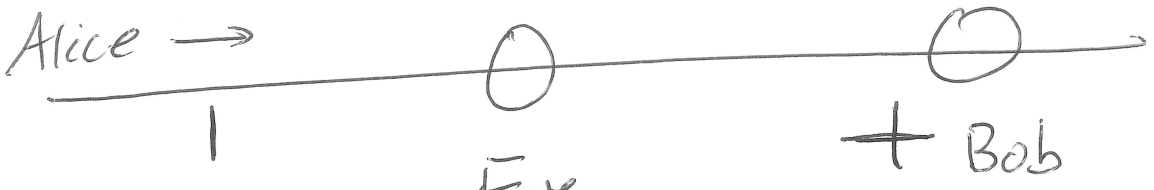
Afterwards Alice + Bob figure out which bits he used the right reader. (1,4,6,7)

If we start with n bits we expect $n/2$ to be thrown out since Bob guessed wrong. We have roughly $n/2$ bits left.

How do we figure out if someone was listening?

Of the ~~bits~~ readers that Bob guessed right, we'll sample k more bits.

What happens if Eve is <u>ALSO</u> reading bits?



+ 50% eve guesses right reader, Bob gets right bit

X 50% eve guesses wrong regardless of the position change, Bob gets the right answer 50% of these cases.

<u>Event</u>

Eve guesses right, Bob gets right bit 50%
Eve guesses wrong, Bob gets right bit 25%
Eve guesses wrong, Bob gets wrong bit 25%.

If we sample k bits and Eve was "listening" the probability Bob gets all right answers is $(\frac{3}{4})^k$.

So as an example, if

$n = 1000$

we're left with $\sim$ 500 bits

SAMPLE 100 bits, Probability all correct w/eve listening $\left(\frac{3}{4}\right)^{100} \sim 3.2 \times 10^{-13}$

If bits don't match $\Rightarrow$ throw out everything

If they do, the last 400 bits can be used for a shared key.

COULD DO: 1 TIME PAD (Plaintext XOR Key)

Or use this secret key for AES or another symmetric cipher system.

BIGGEST DRAWBACK: COST, TIME