QUANTUM CRYPTOGRAPHY

THE SECURITY OF THE CRYPTOGRAPHIC TECHNOLOGIES WE SHOWED HOW TO ACHIEVE IN THIS COURSE (ENCRYPTION, SIGNATURES, MULTIPARTY COMPUTATION, SUCCINCT CERTIFICATES) CAME AT A PRICE: WE HAD TO MAKE UNPROVEN ASSUMPTIONS THAT PROBLEMS LIKE DDH AND LWE ARE HARD TO SOLVE BY A COMPUTATIONALLY EFFICIENT ADVERSARY, WHICH WE MODELED AS A BOOLEAN CIRCUIT OF MODERATE SIZE. ON THE OTHER HAND, THE HONEST PARTIES IN THE PROTOCOLS HAD TO BE IMPLEMENTED EFFICIENTLY.

QUANTUM COMPUTERS CHANGE THE PICTURE IN TWO SUBSTANTIAL WAYS:

1) THEY ENABLE EXPONENTIAL SPEEDUPS IN SOME COMPUTATIONS, THEREBY CHANGING THE NOTION OF "EFFICIENT";
2) THEY ENABLE MODES OF COMMUNICATION THAT CANNOT BE SIMULATED CLASSICALLY, FOR EXAMPLE THE TRANSMISSION OF "INFORMATION" THAT CANNOT BE COPIED WITHOUT DESTROYING IT.

BOTH FEATURES HAVE CONSEQUENCES FOR CRYPTOGRAPHY. IN 1994 PETER SHOR DISCOVERED A QUANTUM CIRCUIT OF SIZE ABOUT n^3 THAT FINDS THE DISCRETE LOGARITHM OF AN n-BIT NUMBER MODULO A SAFE PRIME (AND MORE), THEREBY

RENDERING MANY OF THE PROTOCOLS DESCRIBED IN THIS CLASS INSECURE ONCE AN EFFICIENT SCALABLE QUANTUM COMPUTER IS BUILT. IN CONTRAST IT IS STILL NOT KNOWN IF QUANTUM CIRCUITS CAN EFFICIENTLY BREAK THE LWE ASSUMPTION. THERE IS A SIGNIFICANT EFFORT TO UPGRADE OR REDESIGN PROTOCOLS SO THAT THEY REMAIN SECURE EVEN AGAINST QUANTUM ATTACKERS.

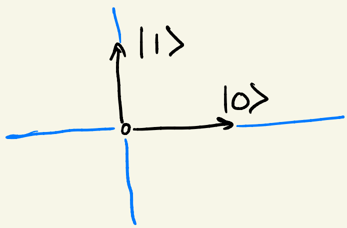
IN THIS LECTURE I WILL TALK NOT ABOUT THE THREAT OF QUANTUM COMPUTERS AS CRYPTOGRAPHIC ADVERSARIES, BUT OF THE OPPORTUNITIES THAT QUANTUM COMMUNICATION (AND RUDIMENTARY COMPUTATION) BRING TO PROTOCOL DESIGN.

ONE SUCH IMPORTANT TASK IS KEY EXCHANGE, I.E. Alice AND Bob NEED TO OUTPUT A COMMON RANDOM KEY SO THAT THE JOINT DISTRIBUTION OF THE TRANSCRIPT AND THE KEY ARE SIMULATABLE BY A PAIR OF INDEPENDENT RANDOM VARIABLES (INTUITIVELY THE KEY IS "COMPUTATIONALLY INDEPENDENT" OF THE TRANSCRIPT.) WE SHOWED PROTOCOLS THAT ARE SECURE ASSUMING THE DDH OR LWE ASSUMPTIONS. IN CONTRAST STATISTICALLY SECURE KEY EXCHANGE IS IMPOSSIBLE (EVEN IF Alice, Bob, AND Eve HAVE A RANDOM ORACLE).

IT TURNS OUT THAT IF Alice AND Bob CAN SEND EACH OTHER QUBITS (QUANTUM BITS), THERE ARE KEY

EXCHANGE PROTOCOLS THAT NOT EVEN A COMPUTATIONALLY UNBOUNDED Eve CAN BREAK.

QUBITS. LET'S START WITH A CLASSICAL COMPUTER WITH ONE BIT OF MEMORY. THE MEMORY CAN BE IN ONE OF THE TWO STATES $|0\rangle$ OR $|1\rangle$. IT WILL BE USEFUL TO THINK OF THEM AS UNIT VECTORS IN THE DIRECTION OF THE x AND y AXES:



A QUANTUM COMPUTER WITH 1 QUBIT OF MEMORY CAN BE IN EITHER ONE OF THESE TWO STATES BUT ALSO IN ANY SUPERPOSITION OF THE FORM

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \quad \text{WHERE } |\alpha|^2+|\beta|^2=1.$$

THUS THE STATE OF A 1-QUBIT QUANTUM COMPUTER IS A UNIT VECTOR $|\psi\rangle$ IN THE SPACE SPANNED BY $|0\rangle$ AND $|1\rangle$.*

NOW SUPPOSE Alice SENDS HER COMPUTER'S QUBIT $|\psi\rangle$ TO Bob. WHAT CAN Bob DO WITH IT? UNLESS Bob HAS ADDITIONAL MEMORY, THERE ARE EXACTLY TWO THINGS HE CAN DO:

---

* THE COEFFICIENTS α AND β CAN IN GENERAL BE COMPLEX NUMBERS BUT THIS IS NOT SO RELEVANT FOR THIS LECTURE SO YOU CAN THINK OF $|\psi\rangle$ AS A VECTOR IN THE PLANE.

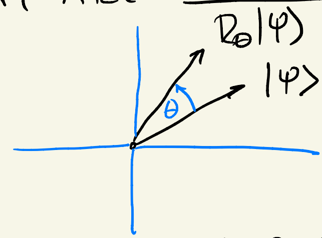
1) UNITARY TRANSFORMATIONS: REPLACE $|\psi\rangle$ BY $U|\psi\rangle$, WHERE U IS A UNITARY MATRIX, I.E. A MATRIX THAT PRESERVES UNIT LENGTH, AND THEREFORE ORTHOGONALITY.

FOR EXAMPLE, IF $N = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, THEN $N|0\rangle = |1\rangle$ AND $N|1\rangle = |0\rangle$, SO N IS THE (CLASSICAL) NOT OPERATOR. IN GENERAL,

$$N(\alpha|0\rangle + \beta|1\rangle) = \beta|0\rangle + \alpha|1\rangle.$$

ANOTHER CLASS OF UNITARY TRANSFORMATION THAT ARE INHERENTLY QUANTUM ARE ROTATIONS

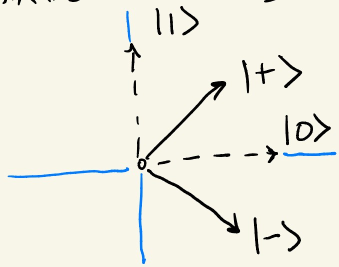
$$R_\theta = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$



THERE IS ALSO THE HADAMARD TRANSFORM

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

SO $H|0\rangle = \dfrac{|0\rangle + |1\rangle}{\sqrt{2}}$ AND $H|1\rangle = \dfrac{|0\rangle - |1\rangle}{\sqrt{2}}$. THESE STATES HAVE NAMES $H|0\rangle = |+\rangle$ AND $H|1\rangle = |-\rangle$.



2) MEASUREMENTS: GIVEN A STATE $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$,

WITH PROB. $|\alpha|^2$, Bob OBSERVES 0 AND $|\psi\rangle$ BECOMES $|0\rangle$
WITH PROB. $|\beta|^2$, Bob OBSERVES 1 AND $|\psi\rangle$ BECOMES $|1\rangle$.

IN PARTICULAR, Bob CANNOT OBSERVE THE AMPLITUDES α AND β DIRECTLY. THE ONLY POSTERIOR INFORMATION ABOUT $|\psi\rangle$ IS THE OUTCOME OF THE MEASUREMENT, BUT THE MEASUREMENT DESTROYS $|\psi\rangle$!

NOW SUPPOSE Alice SENDS Bob ONE OF TWO STATES $|\phi\rangle$ OR $|\psi\rangle$ BUT Bob DOESN'T KNOW WHICH ONE. CAN HE DETERMINE WHAT WAS SENT?

- IF $|\phi\rangle = |0\rangle$ AND $|\psi\rangle = |1\rangle$ THEN BY MEASURING Bob CAN TELL WHICH STATE WAS SENT WITH PROBABILITY ONE.
- IF $|\phi\rangle = |+\rangle$ AND $|\psi\rangle = |-\rangle$ THEN MEASURING WILL GIVE A RANDOM BIT IN BOTH CASES AND DESTROY ALL DISTINGUISHING INFORMATION. Bob CAN, HOWEVER, FIRST APPLY THE UNITARY H^{-1} (WHICH HAPPENS TO EQUAL H) SO THAT $H^{-1}|+\rangle = |0\rangle$, $H^{-1}|-\rangle = |1\rangle$ AND THEN DISTINGUISH THE TWO WITH A MEASUREMENT. WE CAN EFFECTIVELY THINK OF THIS DISTINGUISHER AS "MEASUREMENT IN THE BASIS $|+\rangle, |-\rangle$."

BY THE SAME REASONING ANY TWO ORTHOGONAL STATES CAN BE DISTINGUISHED PERFECTLY.

- WHAT IF $|\phi\rangle = |0\rangle$ AND $|\psi\rangle = |+\rangle$? THEN 1 CAN NEVER BE AN OUTCOME OF MEASURING $|\phi\rangle$, WHILE IT HAPPENS WITH PROBABILITY ½ WHEN MEASURING $|\psi\rangle$, SO Bob CAN DISTINGUISH THE TWO WITH PROBABILITY ½ – BUT IF HE FAILS THE INFORMATION IS FOREVER DESTROYED.

THE BENNETT-BRASSARD PROTOCOL

IN 1984 BENNETT AND BRASSARD PROPOSED A PROTOCOL FOR KEY EXCHANGE. Alice AND Bob ARE 1-QUBIT QUANTUM COMPUTERS WITH SOME ADDITIONAL CLASSICAL MEMORY. THEY CAN TALK TO ONE ANOTHER VIA AN UNAUTHENTICATED QUANTUM CHANNEL PLUS AN AUTHENTICATED CLASSICAL CHANNEL.*

LET'S START WITH A PROTOCOL THAT DOESN'T QUITE WORK AND UPGRADE IT LATER.

- Alice CHOOSES RANDOM BITS x AND y AND SENDS THE FOLLOWING QUBIT $|a\rangle$ TO Bob:

y \ x	0	1
0	$\|0\rangle$	$\|1\rangle$
1	$\|+\rangle$	$\|-\rangle$

* SOME AUTHENTICATION IS NECESSARY FOR OTHERWISE Eve CAN PLAY MAN-IN-THE-MIDDLE.

- Bob CHOOSES A RANDOM BIT y' AND MEASURES $|a\rangle$ IN THE BASIS

$$|0\rangle, |1\rangle \text{ IF } y'=0$$
$$|+\rangle, |-\rangle \text{ IF } y'=1.$$

LET $x' \in \{0,1\}$ BE THE MEASUREMENT OUTCOME.

- Alice AND Bob EXCHANGE y AND y' CLASSICALLY. IF $y' \neq y$ THEY RETRY THE PROTOCOL. IF $y'=y$, THEY OUTPUT x AND x' AS THEIR "SHARED KEY", RESPECTIVELY.

THE PROTOCOL IS CLEARLY FUNCTIONAL: IF Alice AND Bob PRODUCE AN OUTPUT IT MUST BE THAT $y=y'$ SO Bob'S MEASUREMENT IS PERFECTLY DISTINGUISHING AND $x=x'$.

IF Eve IS A PASSIVE EAVESDROPPER, SHE ONLY FINDS OUT THE VALUE $y=y'$ (GIVEN THAT THE RUN WAS SUCCESSFUL) BUT THIS VALUE IS INDEPENDENT OF THE KEY $x=x'$, SO THE PROTOCOL IS SECURE.

A MORE REALISTIC ADVERSARY IS ONE THAT CAN MANIPULATE THE STATE $|a\rangle$ SENT FROM Alice TO Bob. ASSUMING THAT Eve HERSELF IS A 1-QUBIT QUANTUM COMPUTER, SHE CAN APPLY UNITARIES AND MEASUREMENTS TO $|a\rangle$ BEFORE FORWARDING IT OVER TO Bob.

SUPPOSE THAT Eve MEASURES $|a\rangle$ (IN THE BASIS $|0\rangle, |1\rangle$). IF $y=0$ Eve WILL THEN GET TO LEARN THE SHARED KEY $x=x'$. IF, HOWEVER, $y=1$ THEN Eve WILL DESTROY ALL INFORMATION ABOUT THE STATE $|+\rangle$ OR $|-\rangle$ SENT BY Alice: BOTH OF THESE WILL COLLAPSE TO $|0\rangle$ OR $|1\rangle$ WITH EQUAL PROBABILITY. IF y' IS ALSO EQUAL TO 1, THE OUTCOME OF Bob's MEASUREMENT x' WILL THEREFORE BE INDEPENDENT OF Alice's CHOICE x. THIS DISAGREEMENT CAN BE DETECTED BY AUGMENTING THE PROTOCOL WITH THE FOLLOWING TEST:

IF $y'=y$, THEY FLIP A RANDOM COIN

- IF HEADS, THEY REVEAL x AND x' AND <u>ABORT</u> IF $x \neq x'$. OTHERWISE THEY RETRY
- IF TAILS, THEY OUTPUT x AND x' AS THEIR "SHARED KEYS", RESPECTIVELY.

THUS Eve's ATTACK WILL CAUSE Alice AND Bob TO ABORT WHENEVER $y'=y=1$ AND $x'\neq x$, WHICH OCCURS WITH PROBABILITY $1/8$.

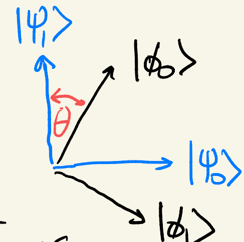
IN GENERAL, Eve CAN PERFORM HER MEASUREMENT IN ANY BASIS $|\psi_0\rangle, |\psi_1\rangle$ OF HER CHOICE. LET THE ANGLE BETWEEN TWO BASES $|\psi_0\rangle, |\psi_1\rangle$ AND $|\phi_0\rangle, |\phi_1\rangle$ BE THE SMALLEST OF THE ANGLES BETWEEN $\pm|\psi_0\rangle, \pm|\psi_1\rangle$ AND $\pm|\phi_0\rangle, \pm|\phi_1\rangle$. SINCE THE ANGLE BETWEEN $|0\rangle, |1\rangle$ AND $|+\rangle, |-\rangle$ IS $\pi/4$, BY THE TRIANGLE INEQUALITY

- THE ANGLE BETWEEN $|\psi_0\rangle, |\psi_1\rangle$ AND $|0\rangle, |1\rangle$ IS $\geq \pi/8$, OR
- THE ANGLE BETWEEN $|\psi_0\rangle, |\psi_1\rangle$ AND $|+\rangle, |-\rangle$ IS $\geq \pi/8$.

<u>Claim.</u> LET θ BE THE ANGLE BETWEEN $|\psi_0\rangle, |\psi_1\rangle$ AND $|\phi_0\rangle, |\phi_1\rangle$. LET e_b BE THE OUTCOME OF MEASURING $|\phi_b\rangle$ IN THE BASIS $|\psi_0\rangle, |\psi_1\rangle$. THE STATISTICAL DISTANCE BETWEEN e_0 AND e_1 IS $\cos^2\theta - \sin^2\theta$.

<u>Proof.</u> ASSUME WITHOUT LOSS OF GENERALITY THAT THE ANGLE BETWEEN $|\phi_0\rangle$ AND $|\psi_1\rangle$ IS θ. THEN e_0 IS 1 WITH PROB. $\cos^2\theta$ AND 0 WITH PROB. $\sin^2\theta$, WHILE e_1 IS 1 WITH PROB. $\sin^2\theta$ AND 0 WITH PROB. $\cos^2\theta$. THE STATISTICAL DISTANCE IS

$$|P[e_0=1] - P[e_1=1]| = \cos^2\theta - \sin^2\theta.$$



IT FOLLOWS THAT WHEN Eve PERFORMS HER MEASUREMENT TO GET OUTCOME e, THERE IS SOME CHOICE OF $y \in \{0,1\}$, SAY $y=0$, FOR WHICH

$$|P[e=1 \mid y=0, x=0] - P[e=1 \mid y=0, x=1]| \leq \cos^2\frac{\pi}{8} - \sin^2\frac{\pi}{8} = \frac{1}{\sqrt{2}}.$$

SINCE y' IS INDEPENDENT OF x, y, e AND RANDOM,

$$|P[e=1 \mid y=y'=0, x=0] - P[e=1 \mid y=y'=0, x=1]| \leq \frac{1}{\sqrt{2}}.$$

AS x' IS A FUNCTION OF e, y' BUT NOT x, x' CANNOT DISTINGUISH BETWEEN $x=0$ AND $x=1$ ANY BETTER THAN e EVEN WHEN CONDITIONED ON $y=y'=0$, SO

$$\left|P[X'=1 \mid y=y'=0, x=0] - P[X'=1 \mid y=y'=0, x=1]\right| \le \frac{1}{2\sqrt{2}}.$$

WE CAN WRITE

$$P[X' \neq X \mid y=y'=0]$$

$$= \frac{1}{2} P[X'=0 \mid y=y'=0, x=0] + \frac{1}{2} P[X'=1 \mid y=y'=0, x=1]$$

$$= \frac{1}{2} - \frac{1}{2}\left(P[X'=1 \mid y=y'=0, x=0] - P[X'=1 \mid y=y'=0, x=1]\right)$$

SO

$$\left|2P[X' \neq X \mid y=y'=0] - 1\right| \le \frac{1}{2\sqrt{2}}$$

AND IT MUST BE THAT

$$P[X' \neq X \mid y=y'=0] \geq \frac{1}{2} - \frac{1}{4\sqrt{2}} \geq 0.32$$

SINCE $y=y'=0$ WITH PROBABILITY $1/4$

$$P[X \neq X'] \geq P[X \neq X' \mid y=y'=0] \, P[y=y'=0] = \left(\frac{1}{2} - \frac{1}{4\sqrt{2}}\right) \cdot \frac{1}{4} \geq 0.08$$

IN CONCLUSION, IF Eve PERFORMS ANY MEASUREMENT, Alice AND Bob WILL DETECT HER MEDDLING AND ABORT WITH PROBABILITY AT LEAST 4%. (THEY MIGHT FAIL TO TEST WITH ADDITIONAL PROB. 1/2.)

AS DESCRIBED THIS PROTOCOL HAS TWO WEAKNESSES: Alice AND Bob ONLY AGREE ON A SINGLE BIT OF SHARED KEY, AND Eve'S MEDDLING IS DETECTED ONLY WITH SOME CONSTANT PROBABILITY. BOTH WEAKNESSES CAN BE ELIMINATED BY REPEATING THE PROTOCOL INDEPENDENTLY n TIMES FOR

A SUFFICIENTLY LARGE n. IF EVE MEASURES IN t OUT OF THOSE n INSTANCES, HER MEDDLING CAN BE DETECTED EXCEPT WITH PROBABILITY $(1-0.08)^t$, WHICH CAN BE MADE SMALLER THAN A GIVEN SECURITY PARAMETER IF t IS CHOSEN SUFFICIENTLY LARGE. Alice's AND Bob's KEY, HOWEVER, IS NO LONGER GUARANTEED TO BE IDENTICAL (Eve COULD HAVE MEASURED SOME POSITIONS CAUSING DISAGREEMENTS) OR COMPLETELY SECRET (Eve COULD HAVE LEARNED A FEW BITS FROM HER MEASUREMENTS). IT IS STILL HOWEVER POSSIBLE FOR Alice AND Bob TO "EXTRACT" A SLIGHTLY SHORTER KEY THAT IS IDENTICAL AND STATISTICALLY SECURE.

MORE QUBITS. IN OUR DISCUSSION SO FAR WE ASSUMED THAT Eve HAS ONLY ONE QUBIT OF QUANTUM MEMORY. IN THE SPIRIT OF CRYPTOGRAPHY WE SHOULD ALLOW Eve MORE QUBITS THAN Alice AND Bob. FOR CONCRETENESS SUPPOSE Eve HAS AN ADDITIONAL QUBIT $|e\rangle$. AFTER RECEIVING Alice's QUBIT $|a\rangle$ SUCH AN Eve CAN APPLY UNITARIES AND MEASUREMENTS ON THE JOINT STATE $|ae\rangle$. THIS STATE LIVES IN A 4-DIMENSIONAL SPACE SPANNED BY THE ORTHOGONAL UNIT VECTORS $|00\rangle, |01\rangle, |10\rangle, |11\rangle$.

APART FROM APPLYING UNITARIES ON $|a\rangle$ AND $|e\rangle$ SEPARATELY Alice CAN ALSO PERFORM "NON-SEPARABLE" UNITARIES, FOR EXAMPLE

$$X|00\rangle = |00\rangle, \quad X|01\rangle = |01\rangle$$
$$X|10\rangle = |11\rangle, \quad X|11\rangle = |10\rangle$$

WHICH HAS THE EFFECT OF XORING THE CONTENT OF THE FIRST QUBIT REGISTER INTO THE SECOND ONE.

THE EXTRA QUBIT CAN POTENTIALLY GIVE Eve QUITE A BIT OF ADVANTAGE: IF SHE COULD COPY THE CONTENTS OF $|a\rangle$ INTO HER REGISTER $|e\rangle$, AFTER OBSERVING THE VALUE $y=y'$ THAT DETERMINES THE MEASUREMENT BASIS, SHE CAN MEASURE $|e\rangle$ IN THE CORRECT BASIS AND RECOVER x WITHOUT ALERTING Alice AND Bob!

IT TURNS OUT, HOWEVER, THAT QUANTUM STATES CANNOT BE COPIED! SUPPOSE Eve INITIALIZES HER EXTRA QUBIT TO SOME STATE $|e\rangle = \alpha|0\rangle + \beta|1\rangle$. IN ORDER TO COPY $|a\rangle$ SHE NEEDS TO COME UP WITH SOME UNITARY C THAT WORKS LIKE THIS:

$$C|0e\rangle = |00\rangle, \quad C|1e\rangle = |11\rangle, \quad C|+e\rangle = |++\rangle, \quad C|-e\rangle = |--\rangle.$$

AS UNITARIES ARE LINEAR, THE FIRST TWO EQUATIONS SAY THAT

$$C|+e\rangle = C\frac{|0\rangle+|1\rangle}{\sqrt{2}}|e\rangle = \frac{1}{\sqrt{2}}(C|0e\rangle + C|1e\rangle) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

WHICH IS NOT THE SAME STATE AS

$$|++\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}} \cdot \frac{|0\rangle+|1\rangle}{\sqrt{2}} = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle).$$

(THEY CAN BE DISTINGUISHED BY A MEASUREMENT IN THE BASIS $|00\rangle, |01\rangle, |10\rangle, |11\rangle$.) THIS IMPORTANT TRIVIALITY GOES BY THE NAME OF THE QUANTUM NO-CLONING THEOREM.

THUS Eve CANNOT CLONE Alice'S MESSAGE, BUT PERHAPS SHE HAS SOME OTHER CLEVER ATTACK THAT EXPLOITS HER ABILITY TO STORE EXTRA QUBITS? Shor AND Preskill PROVED THAT THIS IS NOT THE CASE: Bennett's AND Brassard's PROTOCOL REMAINS SECURE EVEN IF Eve HAS ARBITRARILY MANY QUBITS.