QUANTUM CRYPTOGRAPHY

QUANTUM COMPUTING
QUANTUM COMMUNICATION

ENCRYPTION (PRIVATE + PUBLIC KEY)
AUTHENTICATION
IDENTIFICATION
SIGNATURES
MPC
VERIFICATION

SECURITY ASSUMES PROBLEMS LIKE DDH/LWE ARE COMPUTATIONALLY HARD.

COMPUTATIONAL ASSUMPTIONS ARE NECESSARY

DDH (g^x, g^y, g^{xy}) IND (g^x, g^y, g^R)

(s, ε)-DDH PLAUSIBLE BUT UNPROVEN

SIMILAR FOR (s, ε)-LWE.

QUANTUM COMPUTERS > CLASSICAL FOR CERTAIN TASKS.

1994 Shor: DLOG IS EASY FOR QUANTUM CIRCUITS: SIZE $\approx O(n^3)$ WHICH CALCULATES DLOG OF n-BIT NUMBERS

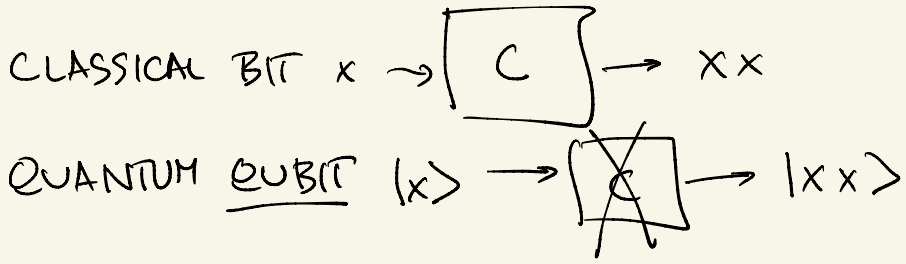
(BEST KNOWN CLASSICAL HAS SIZE $\approx 2^{\Theta(n^{1/3})}$).

MUCH CRYPTO WILL BE BROKEN!

LWE (STILL) CANNOT BE BROKEN EVEN BY A NOTIONAL QUANTUM COMPUTER.

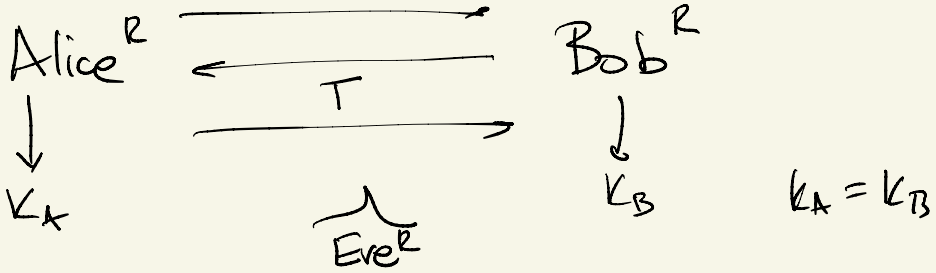
QUANTUM COMMUNICATION HAS FEATURES THAT CANNOT BE SIMULATED CLASSICALLY

EG.



KEY EXCHANGE

CLASSICAL



(T, K_A) CAN BE SIMULATED BY A PAIR OF INDEPENDENT RVs.

- DDH AND LWE-BASED PROTOCOLS
- SOME COMPUTATIONAL ASSUMPTION IS NECESSARY FOR SECURITY
- EVEN IF Alice, Bob, Eve HAVE A RANDOM ORACLE, STAT. SECURE KEY EXCHANGE IMPOSSIBLE.

Bennett-Brassard '84 PROPOSED STATISTICALLY SECURE QUANTUM KEY EXCHANGE (Alice, Bob, Eve ARE QUANTUM CIRCUITS)

1-QUBIT MACHINE

CLASSICAL : 1-BIT OF MEMORY
- STORE 0 OR 1 (STATE)
- NEGATE OR RESET (TRANSFORMATIONS)

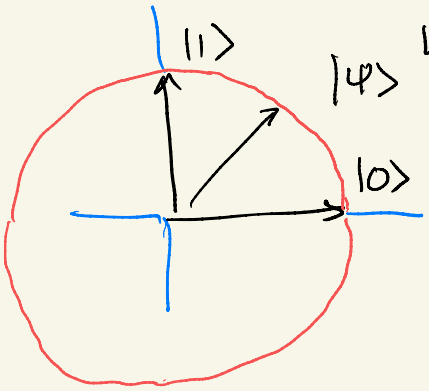
QUANTUM : STATE: $|0\rangle$ OR $|1\rangle$ (CLASSICAL MEMORY STATES)

BE IN A SUPERPOSITION STATE

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

LINEAR COMBINATION OF $|0\rangle$, $|1\rangle$

WHERE $|\alpha|^2 + |\beta|^2 = 1$



Alice $|\psi\rangle$ ⟶ Bob $|\psi\rangle$

$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \qquad |\alpha|^2 + |\beta|^2 = 1$

CANNOT OBSERVE α AND β DIRECTLY

PERFORM 2 TYPES OF OPERATIONS

1) UNITARY TRANSFORMATION $|\psi\rangle \rightarrow U|\psi\rangle$

WHERE U IS A UNITARY MATRIX

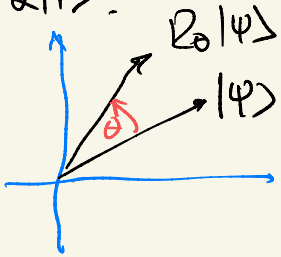
($\forall v$ OF LENGTH 1, Uv HAS LENGTH 1)

Ex1. $N = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ $\quad N|0\rangle = |1\rangle$, $N|1\rangle = |0\rangle$ NOT.

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

Ex2. ROTATIONS

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



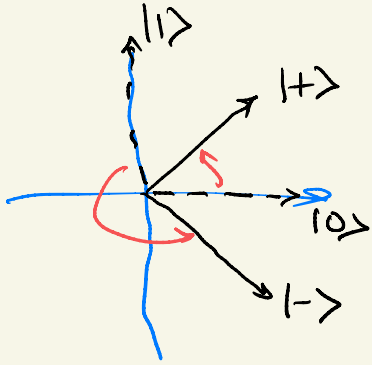
$$R_{\pi/4}|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}.$$

Ex 3. HADAMARD TRANSFORM

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

$$H|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \doteq |+\rangle$$

$$H|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} \doteq |-\rangle$$



INVERTIBLE (CANNOT ERASE A QUBIT)

2) PERFORM A MEASUREMENT

GIVEN A 1-QUBIT STATE $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

- W/P $|\alpha|^2$ OBSERVE 0 & REPLACE STATE WITH $|\psi\rangle = |0\rangle$
- W/P $|\beta|^2$ OBSERVE 1 & REPLACE STATE WITH $|\psi\rangle = |1\rangle$

Ex. $|\psi\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$ $\begin{cases} \text{W/P } 1/2 \to |0\rangle \\ \text{W/P } 1/2 \to |1\rangle \end{cases}$

$|\psi\rangle = |0\rangle$ $\begin{cases} \text{W/P } 1 \to |0\rangle \\ \text{W/P } 0 \to |1\rangle \end{cases}$

Alice $\xrightarrow{|\phi\rangle \text{ OR } |\psi\rangle}$ Bob

TASK: DISTINGUISH $|\phi\rangle$ FROM $|\psi\rangle$

Ex. $|\phi\rangle = |0\rangle$, $|\psi\rangle = |1\rangle$

MEASURE

$|\phi\rangle \to 0$ W/P 1

$|\psi\rangle \to 1$ W/P 1

Ex. $|\phi\rangle = |+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$, $|\psi\rangle = |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$

MEASURE?

$|+\rangle \to 0$ W/P $1/2$, 1 W/P $1/2$

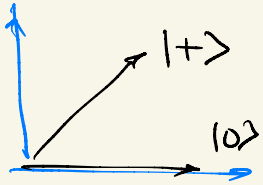
$|-\rangle \to 0$ W/P $1/2$, 1 W/P $1/2$

$|+\rangle = H|0\rangle$
$|-\rangle = H|1\rangle$
$\Big\}$ $H^{-1} = H$
$H^{-1}|+\rangle = |0\rangle$
$H^{-1}|-\rangle = |1\rangle$
$\xrightarrow{M}$ 0 w/p 1, 1 w/p 1

Ex 3. $|\psi\rangle = |0\rangle$ — 0 w/p 1

$|\phi\rangle = |+\rangle$ — 0 w/p 1/2, 1 w/p 1/2

MEASURE:

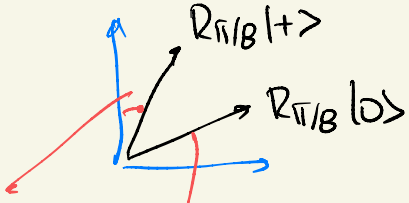


IF Bob GETS 1 → CAN BE SURE THAT Alice SENT $|\phi\rangle$

$$\left| P(\text{Bob}(|\psi\rangle) = 1) - P(\text{Bob}(|\phi\rangle) = 1) \right| = \frac{1}{2}$$

CAN DISTINGUISH WITH ADVANTAGE $\geq \frac{1}{2}$

BETTER: $R_{\pi/8}$



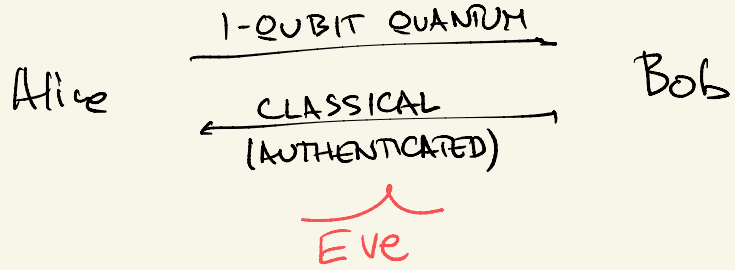
& MEASURE

1 WITH PROB. $\cos^2 \pi/8$

1 WITH PROB. $\sin^2 \pi/8$

$$\text{Adv} = \cos^2 \pi/8 - \sin^2 \pi/8 = \frac{1}{\sqrt{2}}$$

PROTOCOL: GOAL: Alice & Bob TO GET A 1-BIT SECRET KEY.



Alice CHOOSE RANDOM BITS x, y & SEND FOLLOWING QUBIT TO Bob

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

$= |q\rangle$

Bob CHOOSES A RANDOM y' AND

- IF $y'=0$: MEASURE $|q\rangle$ IN $|0\rangle, |1\rangle$ BASIS
- IF $y'=1$: MEASURE $|q\rangle$ IN $|+\rangle, |-\rangle$ BASIS

Alice, Bob EXCHANGE y, y'.

- IF $y \neq y'$ REPEAT
- IF $y = y'$ SET x, x' AS SECRET KEY.

FUNCTIONALITY. GIVEN $y = y'$, Bob PERFECTLY RECOVERS x SO $x' = x$ (RANDOM)

PASSIVE Eve OBSERVES ONLY $y \neq y'$ UNTIL $y = y' \rightarrow$ IND OF x.

MORE REALISTIC Eve IS HERSELF A 1-QUBIT QUANTUM COMPUTER

Alice $\xrightarrow{|a\rangle}$ Eve $\xrightarrow{|e\rangle}$ Bob

SUPPOSE Eve MEASURES $|a\rangle$ (IN $|0\rangle, |1\rangle$ BASIS)

$y=0$ $\quad |a\rangle = |0\rangle$ (½) OR $|1\rangle$ (½) — Eve FINDS SECRET x

$y=1$ $\quad |a\rangle = |+\rangle$ OR $|-\rangle$ → NO INFO FOR Eve

$|e\rangle = |0\rangle$ OR $|1\rangle$ INDEPENDENT OF $|a\rangle$ (GIVEN $y=1$)

ASSUMING $y'=y$ & Bob MEASURES IN $|+\rangle, |-\rangle$ BASIS

- 0 w/p ½
- 1 w/p ½

CHANGE CLASSICAL PART.

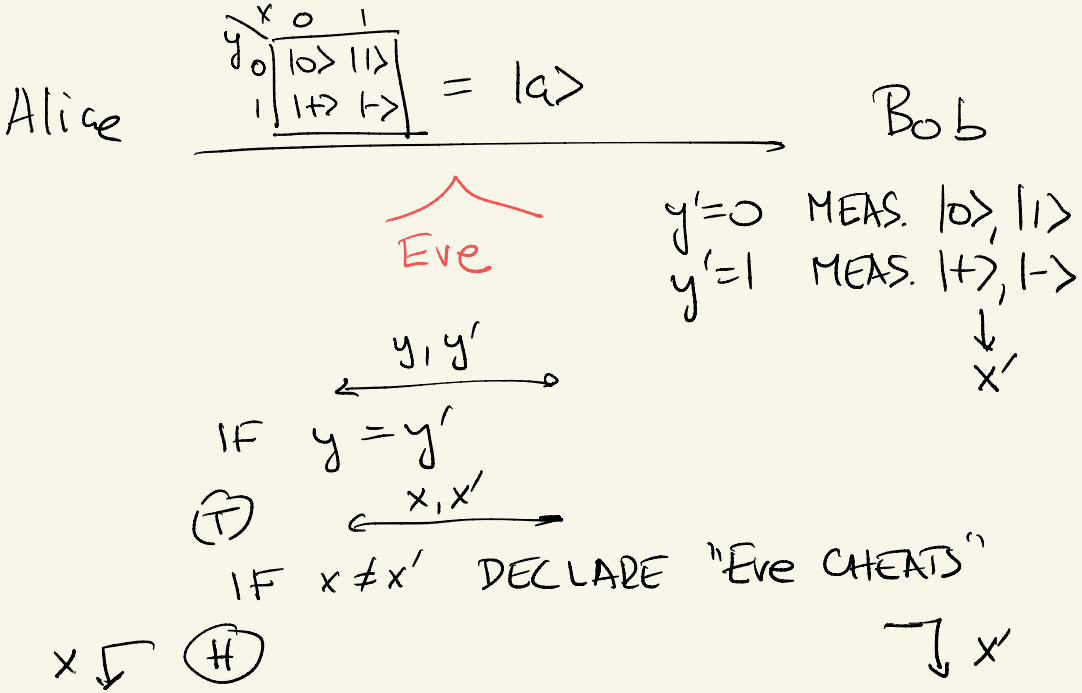
Alice, Bob EXCHANGE y, y'.

- IF $y \neq y'$ REPEAT
- IF $y = y'$, Bob FLIPS A COIN
  - IF HEADS, SET x, x' AS SECRET KEY.
  - (TEST) IF TAILS, EXCHANGE x, x' IF $x \neq x'$ DECLARE "Eve IS CHEATING" AND ABORT.

W/P $\geq \frac{1}{8}$ (y, y' & COIN FLIP) $x \neq x'$
& EVE'S CHEATING IS DETECTED.

1-BIT SHARED KEY PROTOCOL

- IF EVE MEASURES IN $|0\rangle, |1\rangle$ BASIS MEDDLING DETECTED W/P 1/8
- IF MEDDLING UNDETECTED, SECRET KEYS MAY DISAGREE!

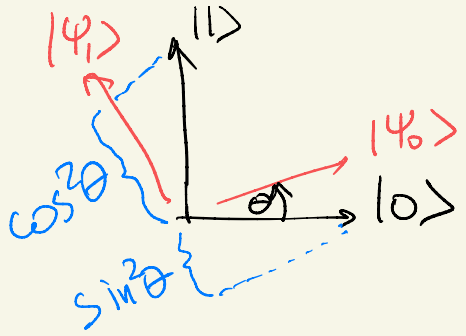


PRETEND Eve MEASURES IN BASIS $|0\rangle, |1\rangle$

IF $y = y' = 1$ AND T $\rightarrow$ P["Eve CHEATS"] $\geq \frac{1}{2}$.

Ex. IF $|q\rangle = |+\rangle$ Eve $\rightarrow$ $|0\rangle$ OR $|1\rangle$
Bob $\rightarrow$ $x = \begin{cases} 0 & \text{W/P } 1/2 \\ 1 & \text{W/P } 1/2 \end{cases}$

$P[\text{CHEATING DETECTED} \mid \textcircled{T}] \geq \frac{1}{8}$.



$\theta \geq \pi/8$

Eve: PICKS BASIS $|\psi_0\rangle, |\psi_1\rangle$ & MEASURES $|a\rangle$ IN THIS BASIS

$\exists$ CHOICE OF y, e.g. $y=0$, S.T. $\sphericalangle(|\psi_0\rangle, |\psi_1\rangle)$ AND $(|0\rangle, |1\rangle)$ IS $\geq \pi/8$

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

WHEN $\frac{\pi}{8} \leq \theta \leq \frac{3\pi}{8}$.

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

$\downarrow$

$$P[x=x' \mid y=y'=0] > 0.08$$

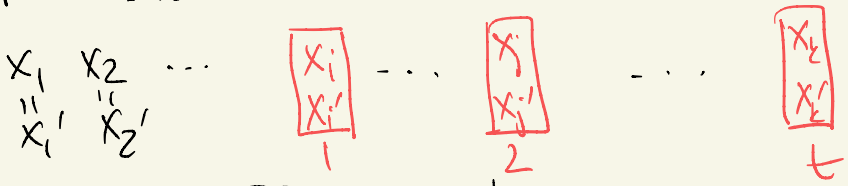
2 ISSUES: SOME PROBABILITY Eve MEDDLES BUT UNDETECTED
→ CAUSE $x \neq x'$ BUT NO TEST.

Alice $\xleftarrow{n \text{ ROUNDS OF QKE}}_{\text{INDEPENDENTLY}}$ Bob

IF Eve MEDDLES t TIMES

$$P(\text{UNDETECTED}) \leq (1-0.04)^t$$

WANT 0.96^t-SECURITY



DISAGREEMENTS CAN BE SOLVED NONINTERACTIVELY.

Eve COULD BE A MANY-QUBIT QC.

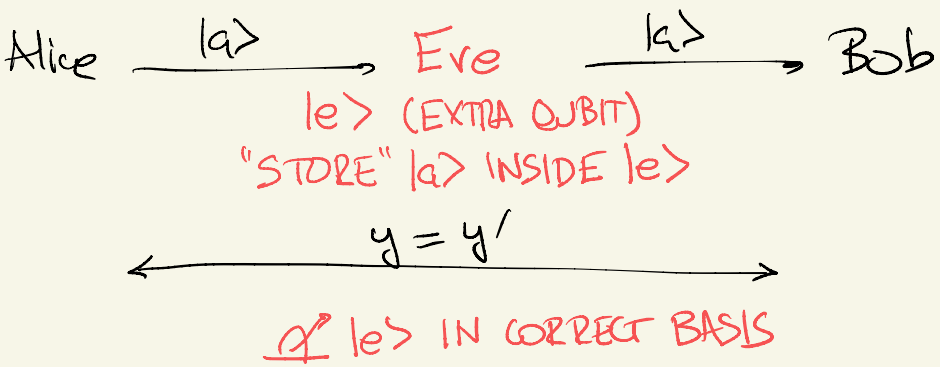
Ex. 2 QUBITS $|00\rangle$ $|01\rangle$ $|10\rangle$ $|11\rangle$

$U|\psi\rangle$ $\quad |\psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle$

Ex. $|ab\rangle \longrightarrow |a(a \text{ XOR } b)\rangle$

$U|00\rangle = |00\rangle \quad U|01\rangle = |01\rangle$

$U|10\rangle = |11\rangle \quad U|11\rangle = |10\rangle$



CAN'T BE IMPLEMENTED BECAUSE OF

NO-CLONING THEOREM

NO UNITARY $|qe\rangle \rightarrow |qq\rangle \quad \forall |q\rangle$.

SUPPOSE SHE COULD

$U|0e\rangle = |00\rangle$

$U|1e\rangle = |11\rangle$

$$U|+e\rangle = U\frac{|0e\rangle + |1e\rangle}{\sqrt{2}}$$

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

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

$$\neq |++\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$$