Quantum Key Distribution

Today's lecture will present an application of many of the ideas already covered in the course.

What is QKD?

Have 2 parties Alice & Bob who want to send messages to each other such that no third party (eavesdropper, Eve) can listen.

Observation: Can do this if Alice & Bob share a secret key that is as long as the message.

message	H	E	L	L	O	
key	X	R	L	E	P	
"add"	F	W	X	Q	E	← encrypted message

Send encrypted message to Bob (could be overheard by Eve)
Bob "subtracts" key ⇒ H E L L O

Why is this secure? Without knowledge of key, could try all keys. If try key X R L E P will decrypt H E L L O.
However, if try key S V F N W will decrypt M A R C H.
Therefore, for every possible message, ∃ some key, so guessing key is equiv. to guessing message. In other words, the encryption gives no information. ← guess encryption

Thus, secure message sending can be reduced to sharing key, hence QKD. We will look at doing this quantum mechanically, hence QKD. In the scenario we consider, it is not possible classically.

Scenario: Alice and Bob are connected via an authenticated (know who they are talking to) public (Eve can listen in) classical channel and an insecure (↳ Eve can modify arbitrarily) quantum channel.

Alice and Bob have their own private randomness (unknown to Eve)

Alice and Bob have secure labs

BB84 protocol: BB = Bennett – Brassard, the inventors, although, ideas go back to Wiesner in 70s.

Idea: Send key bits in quantum states. If Eve tries to read these, she necessarily disturbs the state, i.e. introduces errors. By observing these errors, Alice & Bob detect eavesdropping.

Protocol:

① Alice picks a random basis A_i (X or Z) and a random bit X_i (0 or 1) and generates the corresponding state

$(X,0) \Rightarrow |+\rangle$

$(X,1) \Rightarrow |-\rangle$

$(Z,0) \Rightarrow |0\rangle$

$(Z,1) \Rightarrow |1\rangle$

She sends to Bob.

② Bob picks a random basis B_i ($\{|+\rangle,|-\rangle\}$ or $\{|0\rangle,|1\rangle\}$) and measures in that basis, recording the outcome Y_i.

③ Repeat many times.

remaining steps use public channel

SIFTING ④ Bob announces B_i for all i and Alice and Bob discard rounds where $A_i \neq B_i$

PARAMETER ESTIMATION ⑤ Alice picks a random subset from the remainder and announces to Bob. He tells Alice the error rate and they abort if too high. These bits are discarded.

ERROR CORR. ⑥ Alice and Bob correct their strings by public communication

PRIVACY AMP. ⑦ Alice and Bob compress their string to a shorter one

e.g.

			discard		discard			
A_i :	X	X	Z	X	Z	X	...
X_i :	0	1	1	1	0	0	
						remaining string of Alice	
B_i :	X	Z	Z	Z	Z	X	
Y_i :	0	0	0	1	0	0	
	announce		announce [error]		remaining string of Bob		

Remaining strings X_i: 0 0 1 0 1 1 1 0 1 1 → correct → 0 0 1 0 1 1 1 0 1 1

Y_i: 0 0 1 1 1 1 1 0 0 1 → 0 0 1 0 1 1 1 0 1 1

↑ some errors ↑

priv. amp. ↓

1 0 1 1 0

1 0 1 1 0

error correction and privacy amplification are classical procedures — I won't discuss these in detail.

Intuitively, Eve wants to find X_i and can do so by measuring in same basis as Alice. However, she cannot guess the basis correctly very often, and if wrong, she has a good chance of introducing errors.

Notes: We don't abort on any errors — some errors will occur without eavesdropping.

When doing the security analysis, assume all errors due to E

Eve knows the protocol and can do any physical operation.

What does it mean for protocol to be secure?

Want Protocol outputs string S_A to Alice and S_B to Bob such that

- $S_A = S_B$ (correctness)

- $\rho_{SE} = \frac{\mathbb{I}}{d} \otimes \rho_E$ (string is secret)

Unfortunately, we cannot guarantee these properties. One reason is that the protocol can always abort.

Maybe: either abort or $S_A = S_B$, $\rho_{SE} = \frac{\mathbb{I}}{d} \otimes \rho_E$

Also not achievable. Example if v. lucky Eve could guess all of Alice's bases (i.e. $\{A_i\}$) and could measure in same basis — undetectable.

In this case, protocol will not abort, but $\rho_{SE} \neq \frac{\mathbb{I}}{d} \otimes \rho_E$.

NB: This also shows that we can never make a statement of the form given the protocol does not abort, the key is secure.

Instead, security statement is of the form

For any fixed strategy of Eve, except with some small probability, the protocol either aborts or outputs S_A & S_B such that $P(S_A \neq S_B)$ is small and $D(\rho_{S_A E}, \frac{\mathbb{I}}{d} \otimes \rho_E)$ is small.

Remember that D has operational meaning in terms of distinguishability — for small D, the states $\rho_{S_A E}$ and $\frac{\mathbb{I}}{d} \otimes \rho_E$ are almost indistinguishable

Security from Bell inequality violation

In 2nd half, I'll show an alternative idea on which to base security — Bell inequality violation. This idea was first introduced by Ekert in the Ekert 91 PRL.

Basic idea: if Alice and Bob share maximally entangled pairs, $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ then by measuring them in the same basis they get key. One way to check for max. ent. is Bell inequality violation.

Basic idea: Suppose Alice and Bob share states that violate a Bell inequality

$P_{XY|AB}$ Bell violating.

This means that the outcomes must have some randomness for some additional information, Λ. i.e. cannot have $X = f(A, \Lambda)$, $Y = f(B, \Lambda)$. Thus, the adversary cannot know X and Y perfectly.

This is the rough idea.

⑥ Relating non-locality to secrecy

Quantify non-locality using $I_2(P_{XY|AB}) := P(X=Y|A=0, B=3) + P(X\neq Y|0,1) + P(X\neq Y|2,1) + P(X\neq Y|2,3)$

(i.e. consider the case where Alice and Bob have 2 possible inputs each, $A \in \{0,2\}$, $B \in \{1,3\}$). CHSH inequality

We will show that if I_2 is small, then X is secret with respect to Eve.

Model Eve via an additional system with measurement setting C, outcome Z, so that overall we have $P_{XYZ|ABC}$. We will assume Eve generated a set of systems giving rise to $P_{XYZ|ABC}$ joint dist. We want to show that $I_2(P_{XY|AB})$ characterizes the secrecy.

That $P_{XYZ|ABC}$ is allowed means that there exists ρ_{ABE} and POVMs $\{E_x^a\}$, $\{F_y^b\}$, $\{G_z^c\}$ s.t. $P_{XYZ|ABC}^{(xyz|abc)} = \mathrm{tr}[\rho_{ABC}(E_x^a \otimes F_y^b \otimes G_z^c)]$.

However, not completely trivial to characterize this set. Therefore, we will consider only a necessary condition i.e. $P_{XYZ|ABC}$ non-signalling.

[N.B. Non-signalling means $P_{XY|ABC=c} = P_{XY|ABC=c'}$ $\forall c, c'$ etc.]

In other words, we'll allow the eavesdropper more power than she could really have. Since we still prove security, the protocol remains secure against quantum Eve.

Theorem: Let $P_{XYZ|ABC}$ be a NS prob. dist. with X and Y binary. It follows that

$$\underbrace{D\left(P_{XZ|A=a,C=c}, \tfrac{1}{2} P_{Z|C=c}\right)}_{\text{analogue of } D(\rho_{XE}, \frac{\mathbb{I}}{2}\otimes\rho_E)} \leq \frac{I_2}{2} \quad \forall a,c$$

Proof: For the proof we use a few simple properties of D proven in the exercises:

① D satisfies the triangle inequality, i.e. $D(P_X, Q_X) + D(Q_X, R_X) \geq D$

② $D(P_X, P_Y) \leq P(X \neq Y)$, and for binary X & Y, $D(1-P_X, P_X) = 2D(1$

$D(1-P_X, P_Y) \leq P(X=Y)$ and $D(P_X, P_Y) = D(1-P_X, 1-P_Y)$

[These relations also hold conditioned on something.]

Then, note that $I_2(P_{XY|AB}) = P(X=Y|A=0, B=3) + P(X \neq Y|0,1) + \ldots$

for fixed $C=c$, $Z=z$

$$\geq D(1-P_{X|A=0,c}, P_{Y|B=3,c}) + D(P_{X|A=0,c}, P_{Y|B=1,c}) + D(P_{X|A=2}, P_{Y|$$
$$+ D(P_{X|A=2}, P_{Y|B=3})$$
$$\geq D(1-P_{X|A=0,c}, P_{X|A=0,c})$$
$$= 2D(P_{X|A=0,c}, \tfrac{1}{2})$$

Now take the expectation over Z on both sides:

LHS: $\sum_z P_{z|c} I_2(P_{XY|AB,cz}) = \sum_z P_{z|c} [P(X=Y|A=0, B=3, cz) + P(X \neq Y|0,1,c,z) + \ldots$

$= P(X=Y|A=0, B=3, c) + P(X \neq Y|0,1,c) + \ldots$

$= P(X=Y|A=0, B=3) + P(X \neq Y|0,1) + \ldots$ from NS.

$= I_2(P_{XY|AB})$

RHS $2\sum_z P_{z|c} D(P_{X|A=0,cz}, \tfrac{1}{2}) = 2D(P_{XZ|A=0,c}, \tfrac{1}{2}\sum_z P_{z|c})$

$\Rightarrow$ Desired relation for the case A=0.

By symmetry, (and ⓒ above) relation follows for A=2 as well.

Thus, low $I_2 \Rightarrow$ secrecy.

N.B. $I_2(P_{XY|AB})$ is a quantity that depends on Alice's & Bob's correlations alone.

⑧ So far we have shown how certain measurable correlations relate to secrec

A key dist. protocol must, in addition, do some test of the correlations pre

Want a test such that it only passes with reasonable prob. if I_2 small.

Protocol: ① Alice picks K randomly s.t. $K=0$ with prob. $1-\alpha$

$K=1$ — " — α

for some small α.

② Alice picks (A,B) randomly from $(0,1)$, $(2,1)$, $(2,3)$, $(0,3$

and tells Bob.

③ Alice and Bob make the corresponding measurements

④ Alice flips her outcome if $(A,B)=(0,3)$

⑤ If $K=0$, announce X,Y and abort if $X\neq Y$ else Return to ①

⑥ If $K=1$, X & Y are final key bit.

N.B. This protocol only generates 1 key bit. and doesn't tolerate any noise. However, it is nice to analyse. since no error corr. or priv. amp. needed

Note that step ④ is used to get correctness: If I_2 is 0, then $X=Y$ for $(A,B)=(0,1)$, $(2,1)$ or $(2,3)$ and $X\neq Y$ for $(0,3)$. More generall after flip. $P(X\neq Y)\leq \frac{I_2}{4}$.

Intuitively, the tests only pass (protocol not abort) with reasonably prob. if I_2 is small. However, the key is secret & $\frac{I_2}{4}$-correct, if $\frac{1}{2}\left|\frac{I_2}{2}\right.$ the correlations have value I_2.

Remarks:

- Although not shown here, we can prove a statement of the form of the security statement mentioned earlier (top o

- Big problem with the protocol as presently stated. Although there are NS correlations for which $I_2 = 0$ (NL box correlati seen in exercises), these are not quantum mechanically achievable. (*) However, by increasing the number of measurement choices, we can define an analogous quantity, I_N (for N settings), such that quantum correlati have $I_N \sim \frac{1}{N}$ (i.e. $\xrightarrow{N\to\infty} 0$)

(*) Thus, although secure, the protocol will always abort. Hence, important additional requirement of protocol: with certain quantum states and measurements, the protocol has low probability of abort.

- Quantum correlations satisfy $I_2 \geq 2 - \Gamma_2$ (Tsirelson bou These correlations can be used to generate key in other protoc