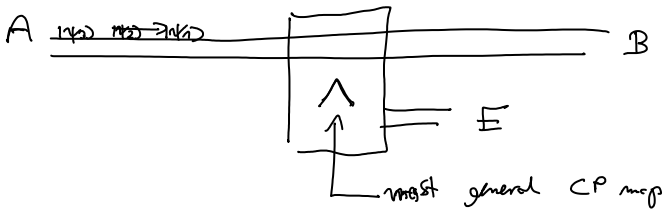
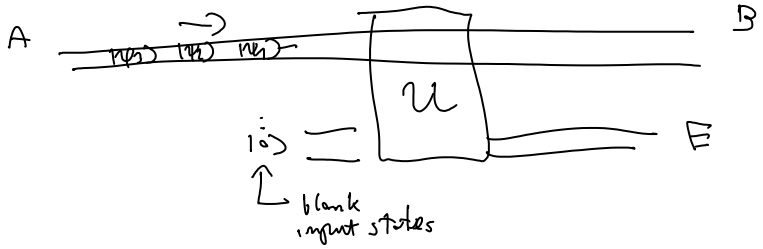
9 - QKD - security

25 października 2010
16:07

The essence of security of QKD is that error rate that A and B detects (QBER) allows them to upper-bound E information on the key. The higher the QBER the stronger might have been the interaction by E, hence larger information.
Remind BB84.



for security analysis we can always assum that E has access to all degrees of freedom so we can extend her subsystem in a way that Λ becames unitary



After the interaction E can wait until A and B perform all public communication and then performs measurement that provide her with information on A and B key.

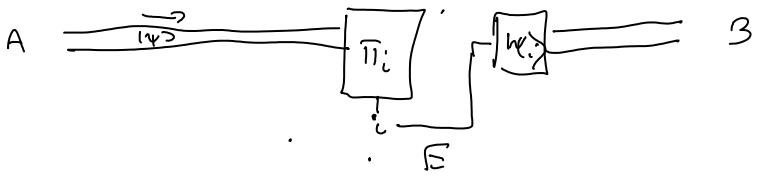
In order to procove security of BB84 (or other QKD) we need to find the optimal attack: i.e. the attack that yields the highest information on the key under given QBER. We should consider the most general attack allowed by QM.
Very difficult task.
So sometimes it is useful to consider some specific class of attacks - at lect this allows us to be sure when we are NOT secure.

8.1 Types of attacks

a) Intercept and resend

E performs measurement on flying state $|\psi\rangle$ (possibly general povm) and depending on measurement outcome i prepares state $|\psi_i\rangle$ which

she sends to B



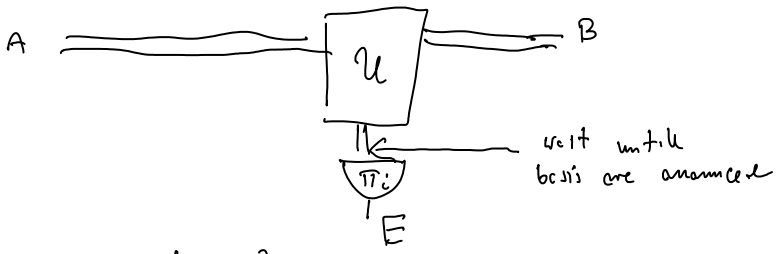
given QBER, find $\{\Pi_i, |\psi_i\rangle_B\}$ maximizing $I(A:E)$

QBER determines $I(A:B)$ { for symetric channel

After such an attack we may think that $p(x^n, y^n, z^n) = p(X,Y,Z)^n$ and apply C-K theorem.
Assuming one-way communication,

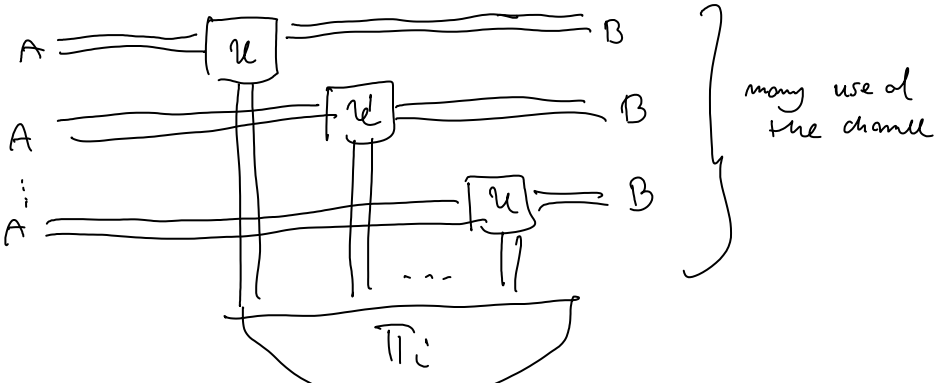
By Csiszar-Korner theorem, the distillable key can asymptotically be extracted at rate $R = \max\left[I(A:B) - I(A:E),\ I(A:B) - I(B:E) \right]$
So strictly speaking the optimal attack needs to maximize $\min(I(A:E), I(B:E))$.

b) individual attacks (more powerful)
E interacts with each state sent by A separately but waits with the measurement until bases are announced (requires long-time q. memory)



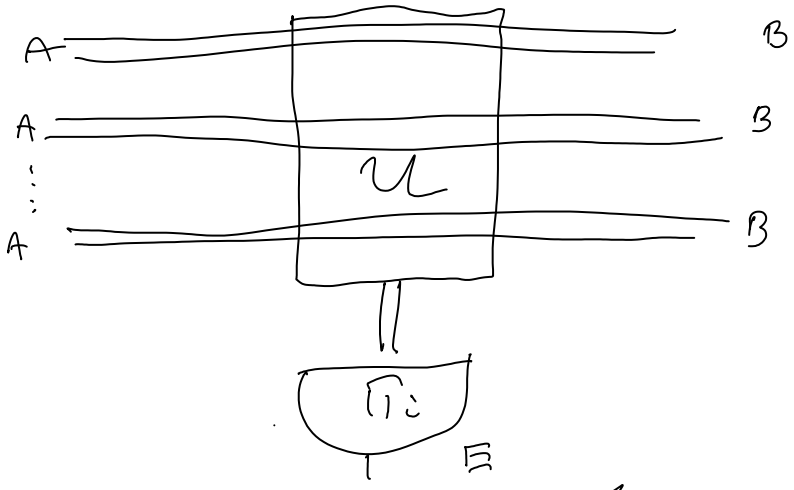
Find $\{\mathcal{U}, \Pi_i\}$ maximizing $I(A:E)$
C-K theorem applies $p(x^n, y^n, z^n) = p(X,Y,Z)^n$

c) collective attack
interaction is again with individual state but measurement is performed collectively on all states kept by E



We can no longer apply C-K theorem, since E does not measure each qubit independently

d) coherent attacks we allow coherent interaction with many probes



C-K does not apply !

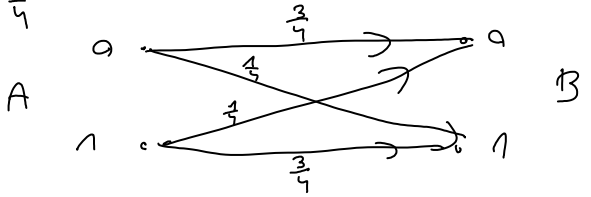
At the moment we can discuss only a), b) since only for this we have n independent realizations of (X,Y,Z) and C-K theorem applies.

8.2 Simple Intercept-Resend attacks on BB84

8.2.1 E measures with p=1 either in ⊕ or ⊗ basis and resends the measured state to B

- QBER: $\frac{1}{2}$ - prob. that E measures in wrong basis × $\frac{1}{2}$ - prob that B measures wrong result

$= \frac{1}{4}$



$I(A:B) = 1 - h(QBER) \approx$ $\quad h(x) = -x\log x - (1-x)\log(1-x)$

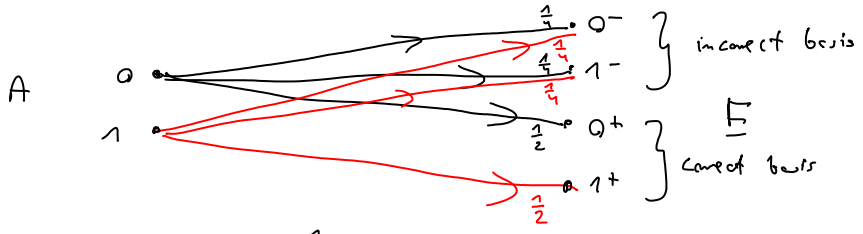
$\approx 0,189$ bits

- $I(A:E) = ?$

probability of error for E, $p_e^E = 25\%$ so it would seem that $I(A:E) = I(A:B)$ .... Wrong !

You should take into account the fact that

E learns by listening to public discussion by A and B whether she measured in a correct basis or not.



$$I(A:E) = \frac{1}{2} > I(A:B)$$

E has much more information than B.

Conclusion: detecting QBER=25% A and B know communication is not secure, they have to abort. (notice also that $I(B:E) = I(A:E)$)

8.2.2. Generalize previous attack to get also lower QBER.

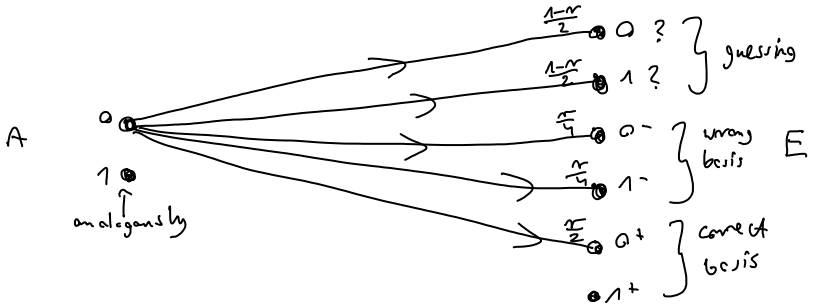
E attacks in the same way as before but just a fraction r of the flying photons

- QBER

$$QBER = \frac{r}{4} \qquad I(A:B) = 1 - h\left(\frac{r}{4}\right)$$

- $I(A:E)$

If E does not perform measurement she needs to guess



$$I(A:E) = \frac{r}{2} \qquad (= I(B:E))$$

By C-K theorem we can distill up to

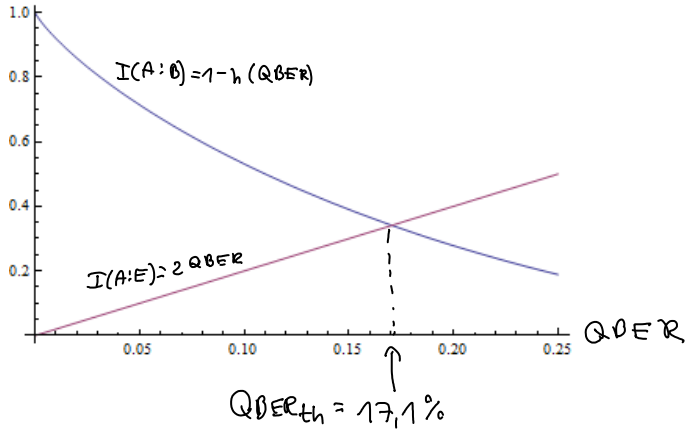
$$C_s = (I(A:B) - I(A:E)) = 1 - h\left(\frac{r}{4}\right) - \frac{r}{2}$$

What is the security condition? $C_s > 0$

$$1 - h\left(\frac{r}{4}\right) > \frac{r}{2}$$

Let us rephrase it using $QBER = \frac{r}{4}$

$$1 - h(QBER) > 2\,QBER$$



$QBER_{th} = 17{,}1\%$

Conclusion: If $QBER > 17{,}1\%$, A, B cannot distill any key.