# 15 - Coherent attacks

27 grudnia 2010
10:13

15.1 Idea: We derive lower bound on QBER, which is exactly the same as for collective attacks. In a sense we will prove that coherent attacks are not more powerfull than collective.

The key idea is that symmetric states $\varrho_n^{sym}$ can be equivalently replaced by product states $\sigma^{\otimes n}$ keeping the values of all Renyi entropies approx the same. Hence the protocol in which A & B symmetrize their state by performing random permutations makes their protocol equally secure against collective as well as against coherent attacks.

15.2 Preeliminaries

Entanglement based approach. A & B would like to share $|\Phi_+\rangle_{AB}^{\otimes n}$
Due to attack by E / noise they effectively share $\varrho_{AB}^n$ which can be arbitrary (entangled across the different pairs etc...)
How much secure key they can extract?

- Main problem: We do not have a product structure, so we cannot apply Devetak-Winter theorem.

- Recall classical EC & PA. When we did not have i.i.d distributions or we did not work in asymptotic limit we had to use Renyi entropies rather than Shannon.
Recall theorem on PA: If we have $XZ$ rand variables and $H_2(X|Z=z) \geq c$ then after applying two-
$\llcorner$ eavesdropper knowledge
-universal hashing functions $K = u(X)$, $u \in \mathcal{U}$
$H(K|\mathcal{U}Z=z) \geq k - 2^{k-c}/\ln 2$ so we can extract approx $k \approx H_2(X|Z=z)$ bits of secret key

This was under assumption that error correction had been performed. If not:

$$k \approx H_2(X|Z=z) - m$$
$\llcorner$ number of bits revealed in EC

Asymptotically for i.i.d $XZ \to (XZ)^n$, $k \simeq nH(X|Z) - nH(X|Y) = n(I(X:Y) - I(X:Z))$
but this does not follow immediately from Renyi entropies
problem is that $H_2(X^n) = nH_2(X) \neq nH(X) = H(X^n)$
whereas we know that on typical sequences: $H_2(X^n) = H(X^n)$

15.3 Smooth Renyi entropies

technical modification to make Renyi entropies more "physical". (For example $H_0$ is not continuous in $p(x)$, and $H_\alpha(X^n) \neq H(X^n)$ for large $n$)

$$H_\alpha^\varepsilon(X) = \frac{1}{1-\alpha} \log\left( \inf_{\tilde{p}} \sum_x \tilde{p}(x)^\alpha \right)$$

$$H_\alpha^\varepsilon(X) = \frac{1}{1-\alpha} \log\left[ \inf_{\delta(P_X, \tilde{P}_X) < \varepsilon} \sum_x \tilde{p}(x)^\alpha \right]$$

where $\delta(P_X, \tilde{P}_X) = \frac{1}{2} \sum_x |p(x) - \tilde{p}(x)|$ – variational distance between prob. distributions

(for $\alpha = 0, \infty$ $H_\alpha^\varepsilon = \lim_{\alpha \to 0,\infty} H_\alpha^\varepsilon$)

- $H_\alpha^\varepsilon$ is continuous
- $\lim_{\varepsilon \to 0} \lim_{n \to \infty} \frac{1}{n} H_\alpha^\varepsilon(X^n) \longrightarrow H(X)$

Better PA + EC formula for key length.

There is also a bit modified form of the above PA theorem (Renner). Given $(XYZ)$ the number of secret bits that can be distilled via error correction and 2-universal hashing is

$$(*) \quad k \approx \underbrace{H_2^\varepsilon(X, Z) - H_0^\varepsilon(Z)}_{PA} - \underbrace{H_0^\varepsilon(X|Y)}_{\text{bits revealed in EC}}$$

(where $\varepsilon$ is roughly probability that Z learns the final key)

Notice that thanks to properties of smooth Renyi entropies, when we consider i.i.d situation so $XYZ \to (XYZ)^n$ then

$$k \approx n( H(X,Z) - H(Z) - H(X|Y)) =$$

$$= n(I(X:Y) - I(X:Z)) \quad \} \text{ Csiszar-Körner}$$

But remember that $(*)$ applies in general to arbitrary distributions

## 15.4 Privacy amplification and EC in the presence of q. adversary.

$$\varrho_{AE} = \sum_{x_1} p(x) |x\rangle\langle x| \otimes \varrho_E^x$$

$\uparrow$ E information

We can perform 2-universal hashing after which E can gain negligible information provided the length of the key is smaller than

$$k \approx S_2^\varepsilon(A, E) - S_0^\varepsilon(E)$$

where $S_\alpha^\varepsilon$ are q. smooth Renyi entropies

{ Idea by application of hashing function we turn $\varrho_{AB}$ into $\approx \frac{1}{|X|} \mathbb{1} \otimes \bar{\varrho}_E$ so E is decoupled from A

Additionally A and B need to exchange $H_0^\varepsilon(X,Y)$

bits for error correction so finally if we consider the full picture :

$$\rho_{ABE} = \sum_{x,y} p(x,y) |x\rangle\langle x| \otimes |y\rangle\langle y| \otimes \rho_E^{x,y}$$

A and B can distill :

$$(**) \quad K \simeq S_2^{\varepsilon}(A,E) - S_0^{\varepsilon}(E) - H_0^{\varepsilon}(A|B)$$

15.5 Security against coherent attacks

- Let us assume that after the attack by E all three parties share $\rho_{ABE}^{n}$
- After A & B perform measurements and sifting the total state can be written as:

$$\rho'^{n}_{ABE} = \sum_{x,y \in \{0,1\}^n} p(x,y) |x\rangle\langle x| \otimes |y\rangle\langle y| \otimes \rho_E^{xy}$$

So we can apply theorem (**) ....

Problem: How A & B can know the state $\rho'^{n}_{ABE}$ ?
They cannot. What they know is just QBER.
So in principle they could minimize (**) over all coherent attacks that provide given QBER. Not doable !

Solution A & B have to perform some additional operations on their parts to simplify the structure of $\rho^n_{ABE}$ and make analysis manageable

15.6 Simplifying the structure of $\rho_{ABE}{}^{n}$

- We will consider only $\rho_{AB}^{n}$ part and always grant E maximum information in the sense that E holds purification i.e $\rho_{AB}^{n} = \mathrm{Tr}_E(|\Psi_n\rangle_{ABE}\langle\Psi_n|)$.
- We do the same as in "collective attack case" i.e

$$\rho_{AB}^{n} \longrightarrow \rho'^{n}_{AB} = \frac{1}{4^n}\sum \left(\sigma_{k_1}\otimes\sigma_{k_1}\right)\otimes \dots \otimes\left(\sigma_{k_n}\otimes\sigma_{k_n}\right)\rho_{AB}^{n}\left(\sigma_{k_1}\otimes\sigma_{k_1}\right)\otimes \dots \otimes\left(\sigma_{k_n}\otimes\sigma_{k_n}\right)$$

$k_1 \dots k_n$

where $\sigma_k$ are Pauli operators acting on n-th qubit pair. So we get a state which is diagonal in Bell basis.

$$\rho_{AB}^{\prime n} = \sum_{i_1 \dots i_n = 1}^{4} \lambda_{i_1 \dots i_n} |\psi_{i_1}\rangle\langle\psi_{i_1}| \otimes \dots \otimes |\psi_{i_n}\rangle\langle\psi_{i_n}|$$

Notice we have got rid of entanglement between different pairs

- We perform a random permutation of all pairs (this is the key step)

$$\rho_{AB}^{\prime\prime n} = \frac{1}{n!} \sum_{\sigma \in S_n} \Pi_\sigma \rho_{AB}^{\prime n} \Pi_\sigma$$

$$\rho_{AB}^{\prime\prime n} = \sum_{\substack{n_1, n_2, n_3, n_4 \\ n_1+n_2+n_3+n_4 = n}} \mu_{n_1, n_2, n_3, n_4} \rho_{n_1, n_2, n_3, n_4}$$

where $\rho_{n_1, n_2, n_3, n_4} = \frac{1}{n!} \sum_{\sigma \in S_n} \Pi_\sigma |\psi_1\rangle\langle\psi_1|^{\otimes n_1} \otimes |\psi_2\rangle\langle\psi_2|^{\otimes n_2} \otimes |\psi_3\rangle\langle\psi_3|^{\otimes n_3} \otimes |\psi_4\rangle\langle\psi_4|^{\otimes n_4} \Pi_\sigma$

The state is permutationally invariant (symmetric) still hard to analyze but, ...

there is an interesting property of permutationally invariant states

15.7 Quantum de Finetti theorem

Theorem If $\rho_n$ is an n-partite permutationally invariant state that can be written as $\rho_n = \mathrm{Tr}_k(\rho_{n+k})$ (partial trace of some other permutationally invariant state) for all $k > 0$ then

$$\rho_n = \sum_\alpha p_\alpha \sigma_\alpha^{\otimes n}$$

(is a mixture of product states)

Note In practice it is enough to let $k$ be finite $0 < k < K$ and we will have approximate version $\varrho_n \approx \sum_\alpha p_\alpha \sigma_\alpha^{\otimes n}$

## 15.8 Reduction of Coherent attacks to Collective attacks

A & B perform parameter estimation on part of their states m-pairs. This way they estimate $\sigma_\alpha$, and they know that the remaining bits are in state $\sigma_\alpha^{\otimes n-m}$ where $\sigma_\alpha = \sum_{k=1}^{4} \lambda_k^{(\alpha)} |\psi_k\rangle\langle\psi_k|$ is some Bell diagonal state. So the problem is reduced to collective attacks!

## 15.9 Two way communication

All presented results were based on a simplifying assumption of one way communication.

For two-way communication the $QBER_{th} = 20\%$ for BB84

This is all based on entanglement distillation picture.