Quantum Cryptography

Homework Set 4

(Answer Sheet)

1 Min-Entropy and Collision-Entropy

For definitions of the min- and collision-entropy as well as Jensen's inequality, see the appendix of the lecture notes.

a) If X has no uncertainty (i.e. $H(X) = 0$), what is $\mathrm{H}_\infty(X)$?

Answer: $H(X) = 0 \implies \exists i : P_X(i) = 1 \implies \mathrm{Guess}(X) = 1 \implies \mathrm{H}_\infty(X) = 0$.

b) If X is uniformly distributed over the set $\mathcal{X}$, what is $\mathrm{H}_\infty(X)$?

Answer:

$$\mathrm{Guess}(X) = \frac{1}{|\mathcal{X}|}, \quad \mathrm{H}_\infty(X) = \log|\mathcal{X}|$$

c) Prove that $\mathrm{H}_\infty(XY) \geq \mathrm{H}_\infty(X)$.

Answer: Note that it is equivalent to prove that $\mathrm{Guess}(XY) \leq \mathrm{Guess}(X)$.

$$\mathrm{Guess}(XY) = \max_{x,y} P_{XY}(x,y) \leq \max_x \sum_y P_{XY}(x,y) = \max_x P_X(x) = \mathrm{Guess}(X).$$

d) Prove that $\mathrm{H}_\infty(X) \geq \mathrm{H}_\infty(X|Y)$.

Answer: Again, we prove the statement in terms of the guessing probability, i.e. that $\mathrm{Guess}(X) \leq \mathrm{Guess}(X|Y)$.

$$\begin{aligned}\mathrm{Guess}(X) &= \max_x P_X(x) = \max_x \sum_y P_{XY}(x,y) \\ &= \max_x \sum_y P_Y(y) P_{X|Y}(x|y) \\ &\leq \sum_y P_Y(y) \max_x P_{X|Y}(x|y) = \mathrm{Guess}(X|Y)\end{aligned}$$

e) Prove that $\mathrm{H}_\infty(X|Y) \geq \mathrm{H}_\infty(XY) - \log|\mathcal{Y}|$.

Answer: In terms of the guessing probability, the statement reads

$$\mathrm{Guess}(X|Y) \leq |\mathcal{Y}| \cdot \mathrm{Guess}(XY).$$

Proof:

$$\begin{aligned}\mathrm{Guess}(X|Y) &= \sum_y P_Y(y)\mathrm{Guess}(X|Y=y) = \sum_y P_Y(y) \max_x P_{X|Y}(x|y) \\ &= \sum_y \max_x P_{XY}(x,y) \leq \sum_y \max_{x,y'} P_{XY}(x,y') \\ &= \sum_y \mathrm{Guess}(XY) = |\mathcal{Y}| \cdot \mathrm{Guess}(XY).\end{aligned}$$

f) Prove that $\mathrm{H}_\infty(X|Y) \leq \mathrm{H}_2(X|Y) \leq \mathrm{H}(X|Y)$. *Hint:* Use Jensen's inequality to prove the second (rightmost) inequality.

Answer: To prove the left inequality, we first prove

$$\mathrm{H}_\infty(X) \leq H_2(X).$$

which is equivalent to proving that $\mathrm{Col}(X) \leq \mathrm{Guess}(X)$:

$$\mathrm{Col}(X) = \sum_x P_X(x) P_X(x) \leq \sum_x P_X(x) \max_y P_X(y) = \max_y P_X(y) = \mathrm{Guess}(X).$$

Now it follows that the above also holds for a conditional distribution $P_{X|Y}(x|y)$ for any y, and therefore also for the average over y.

Let us now prove the right inequality by applying Jensen's inequality twice,

$$\begin{aligned}H_2(X|Y) &= -\log \sum_y P_Y(y) \sum_x P_{X|Y}(x|y)^2 \leq -\sum_y P_Y(y) \log \sum_x P_{X|Y}(x|y)^2 \\ &\leq -\sum_y P_Y(y) \sum_x P_{X|Y}(x|y) \log P_{X|Y}(x|y) = H(X|Y).\end{aligned}$$

2 Privacy Amplification

Consider the hash function

$$f : \{0,1\}^{r\times n} \times \{0,1\}^n \to \{0,1\}^r, \quad (A,x) \mapsto Ax$$

where all operations are modulo two and where $r < n$.

a) Prove that f is a universal function, i.e. prove that for any $x, x' \in \{0,1\}^n$ such that $x \neq x'$, it holds that

$$P[f(A,x) = f(A,x')] \leq \frac{1}{2^r}$$

where A is a uniformly distributed random binary $r \times n$ matrix.

Answer: For any $x \neq x' \in \{0,1\}^n$, the difference $Ax - Ax' = A(x - x')$, when viewed as the function $\{0,1\}^{r\times n} \to \{0,1\}^r, A \mapsto A(x - x')$ is linear and surjective, hence $|\{A \in \{0,1\}^{n\times r} \mid A(x - x') = y\}|$ is constant for any $y \in \{0,1\}^r$. Therefore, for A chosen uniformly at random, $\Pr[Ax = Ax'] = 2^{-r}$.

Let X be a uniformly distributed n-bit string, held by Alice, and she wants to derive a cryptographic key from it. However, Eve holds $Y := g(X)$ for an arbitrary surjective function g from n bits to k bits.

b) Show that $\mathrm{H}_\infty(X|Y) = n - k$.

Answer:

$$\begin{aligned} H_\infty(X|Y) &= -\log \sum_y P_Y(y) \max_x P_{X|Y}(x|y) \\ &= -\log \sum_y P_Y(y) \max_x \frac{P_X(x)P_{Y|X}(y|x)}{P_Y(y)} \\ &= -\log \frac{1}{|\mathcal{X}|} \sum_y \max_x P_{Y|X}(y|x) \\ &= -\log \frac{|\mathcal{Y}|}{|\mathcal{X}|} = n - k, \end{aligned}$$

where the fourth equality follows since for every y there exists x such that $y = g(x)$ and thus $P_{Y|X}(y|x) = 1$.

Alice applies privacy amplification to X with the help of f, resulting in a shorter key K that is almost uniform when given Y.

c) Find the maximum length of the extracted key, such that it has statistical security (i.e. statistical distance from being uniform) of $< 10^{-7}$.

Answer: Let ℓ be the maximum length of the key and s the desired security. By the privacy amplification theorem,

$$s = \mathrm{SD}(P_{KAY}, P_{UAY}) \leq \frac{1}{2} \cdot 2^{-\frac{1}{2}(H_2(X|Y)-\ell)} \leq \frac{1}{2} \cdot 2^{-\frac{1}{2}(\mathrm{H}_\infty(X|Y)-\ell)}$$

Solving for ℓ yields

$$\ell = \lfloor 2\log_2(2 \cdot 10^{-7}) \rfloor + n - k = n - k - 45$$

Let $X = (X_1, X_2) \in \{0,1\}^2$ be uniformly distributed over its range, and let E be the qubit $H^{X_1}|X_2\rangle$, i.e.,

$$\rho_{XE} = \sum_{x_1,x_2\in\{0,1\}} P_{X_1X_2}(x_1,x_2)|x_1,x_2\rangle\langle x_1,x_2| \otimes H^{x_1}|x_2\rangle\langle x_2|H^{x_1}.$$

d) Find $\mathrm{H}_\infty(X) - \mathrm{H}_0(E)$.

Answer: Because X is uniform, it has full (min-)entropy, hence $\mathrm{H}_\infty(X) = \log_2 |\mathcal{X}| = 2$. The density matrix ρ_E equals

$$\rho_E = \tfrac{1}{4}|0\rangle\langle 0| + \tfrac{1}{4}|1\rangle\langle 1| + \tfrac{1}{4}H|0\rangle\langle 0|H + \tfrac{1}{4}H|1\rangle\langle 1|H = \begin{bmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{bmatrix},$$

and we see that it has full rank, i.e. rank two. Hence $\mathrm{H}_0(\rho_E) = \log \mathrm{rank}(\rho_E) = \log_2 2 = 1$. We conclude that $\mathrm{H}_\infty(X) - \mathrm{H}_0(E) = 2 - 1 = 1$.

e) Does there exist a better "encoding" of X into the qubit E, so that $\mathrm{H}_\infty(X) - \mathrm{H}_0(E)$ becomes smaller?

Answer: No, because ρ_E already has full rank.