Quantum Cryptography

Homework Set 4

Please send your answers – either typeset on a computer, or handwritten (but readable) and scanned, preferably in PDF format – to `bouman@cwi.nl` *before May 2, 23h59. Do not forget to put your name on the first page. Good luck!*

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. there exists an i for which $P_X(i) = 1$), what is $\mathrm{H}_\infty(X)$?

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

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

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

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

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.

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.

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

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 $< 10^{-7}$.

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

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?