Quantum Cryptography (fall 2017) Dominique Unruh

Exercise Sheet 9

Out: 2017-12-11 Due: 2017-12-18

Problem 1: Universal hash functions

(a) Let S be the set of all binary $\ell \times m$-matrices. I.e., $S = \mathbb{F}_2^{\ell \times m}$. Let X be the set of all m-bit vectors. I.e., $X = \mathbb{F}_2^m$. Let $Y = \mathbb{F}_2^\ell$. Let $F : S \times X \to Y$ be defined as $F(s, x) := sx$.

Show that F is a universal hash function.

Note: You may use the fact that for any fixed $z \neq 0$, and uniformly distributed $s \in \mathbb{F}_2^{\ell \times m}$, sz is uniformly distributed on $\mathbb{F}_2^\ell$. (Bonus points if you prove that fact, too.)

(b) **(Bonus problem)** Let $S := X := \mathbb{F}_{2^m}$ be a finite field (encoded in the standard way as an $\mathbb{F}_2$ vector space). Let $trunc_\ell(x)$ denote the first ℓ bits of x. Let $Y := \{0,1\}^\ell$. Let $F : S \times X \to Y$ be defined as $F(s, x) := trunc_\ell(sx)$.

Show that F is a universal hash function.

Note: You may use that $trunc_\ell(a - b) = trunc_\ell(a) - trunc_\ell(b)$. (This is immediate from the encoding of $\mathbb{F}_{2^m}$.)

Problem 2: Breaking a Protocol

Consider the following commitment protocol (where n is some security parameter).

- *Commit phase.* Alice wants to commit to a bit b. First, she chooses n uniformly random bits $x_1, \ldots, x_n \in \{0,1\}$. If $b = 0$ she encodes them in the computational basis; if $b = 1$, in the diagonal basis. I.e., if $b = 0, x_i = 0$, then $|\Psi_i\rangle := |0\rangle$, if $b = 0, x_i = 1$, then $|\Psi_i\rangle := |1\rangle$, if $b = 1, x_i = 0$, then $|\Psi_i\rangle := |+\rangle$, if $b = 1, x_i = 1$, then $|\Psi_i\rangle := |-\rangle$.

  Then Alice sends the qubits $|\Psi_1\rangle, \ldots, |\Psi_n\rangle$ to Bob.

- For each of the qubits, Bob randomly chooses whether to measure it in the computational or the diagonal basis. Let the outcomes of these measurements be denoted $\tilde{x}_i$.

- *Unveil phase.* Alice sends $b, x_1, \ldots, x_n$ to Bob.

- Bob checks whether $x_i = \tilde{x}_i$ for all i where Bob measured in the right basis (computational in the case of $b = 0$, diagonal in the case of $b = 1$).

The intuition behind this protocol is as follows: It is hiding because Bob cannot distinguish which bases Alice used. It is binding because of the following reason: If Bob measures some $|\Psi_i\rangle$ in, say, the computational basis, but $|\Psi_i\rangle$ was not one of $|0\rangle, |1\rangle$, then the outcome of the measurement is to some extend random, and Alice cannot predict the output $\tilde{x}_i$ of Bobs measurement. On the other hand, if Bob measures $|\Psi_i\rangle$ in the diagonal basis, but $|\Psi_i\rangle$ was not one of $|+\rangle, |-\rangle$, then the outcome of the measurement is again random, and Alice cannot predict the output $\tilde{x}_i$ of Bobs measurement. So whatever state $|\Psi\rangle$ Alice sends, there is some probability that she will not know $\tilde{x}_i$. And since to unveil both as $b = 0$ and as $b = 1$, Alice needs to know all $\tilde{x}_i$, she will fail.

Of course, this intuition cannot be correct since we know from the lecture that this (and any other) commitment protocol cannot be secure.

(a) Show that this protocol is perfectly hiding (i.e., ε_H-hiding for $\varepsilon_H = 0$).

(b) Show that this protocol is not ε_B-binding for any $\varepsilon_B < 1$. (I.e., it is possible for Alice to commit in a way such that she can unveil both as $b = 0$ and as $b = 1$.)

Note: You have to actually give an attack. It is not sufficient to say that there exists an attack due to Theorem 6 in the lecture notes and (a).

Hint: Think of Bell pairs. Try out what happens if you measure both qubits of $|\beta_{00}\rangle$ in the diagonal basis.

Problem 3: Schmidt Decomposition

(a) For a given state $|\Psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$, the Schmidt number is the smallest n such that a Schmidt decomposition $|\Psi\rangle = \sum_{i=1}^{n} \lambda_i |\alpha_i\rangle|\beta_i\rangle$ exists.

We call a state $|\Psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ entangled if $|\Psi\rangle$ *cannot* be written as $|\Psi\rangle = |\Psi_A\rangle \otimes |\Psi_B\rangle$.

Show that a state is entangled if and only if it has Schmidt number greater than 1. (This justifies using the Schmidt number as a measure of how entangled a state is.)

(b) Let a state $|\Psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ be given. Assume for simplicity that $\dim \mathcal{H}_A = \dim \mathcal{H}_B$. Show that $\mathrm{tr}_A |\Psi\rangle\langle\Psi|$ and $\mathrm{tr}_B |\Psi\rangle\langle\Psi|$ have the same eigenvalues.

Hint: Represent $|\Psi\rangle$ in its Schmidt decomposition. Then compute the partial trace tr_A and tr_B directly on that representation.