Quantum Cryptography (spring 2020) Dominique Unruh

Exercise Sheet 10

Out: 2020-05-30 Due: 2020-06-02

This is a bonus homework. Each problem gives up to 10 points.

Problem 1: 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.

Problem 2: Regev's cryptosystem

In Regev's cryptosystem, we have an error term e that is initialized according to a distribution χ. In this homework, we investigate what happens, say due to a programmer error, e is not properly randomized.

(a) We have a faulty implementation of Regev's cryptosystem where $e = (0, \dots, 0)$ always. The adversary gets the public-key (A, b) and a ciphertext (c_1, c_2). How can the adversary compute the plaintext? (Describe the computation steps performed by the adversary.)

Hint: If in doubt, first try to figure out how to solve the computational LWE problem (i.e., find s) when $e = 0$ always.

Note: This was somewhat explained in the Q&A. So you get points for clarity of formulating what was said there.

(b) Now we have a slightly better implementation. e now indeed contains some noise, but too little. In fact, it turns out that with probability close to 1, only one component $e_i \neq 0$. (That is, for all $j \neq i$, $e_j = 0$.) Show that this is too little noise by giving an attack. (Given public key and ciphertext find the plaintext. Describe the computation steps performed by the adversary.)

(c) Now we have a different randomness failure. e is chosen properly, but $A = 0$. How to attack? (Given public key and ciphertext find the plaintext. Describe the computation steps performed by the adversary.)

(d) And now something completely different: Given a ciphertext (c_1, c_2) that is the encryption of some unknown $\mu \in \{0, 1\}$, how to compute a ciphertext (c'_1, c'_2) that decrypts to $1 - \mu$ (with high probability)?

Note: You do not need to prove that your solution is correct, it is enough to specify the algorithm.

Note: What you are showing here is that Regev's cryptosystem is malleable.

Problem 3: Alice and Bob are being clever

Alice and Bob had a few clever ideas. In each case, explain why the idea is not a good one.

1. Alice noticed that with a sufficiently strong laser pointer, she can make a beam that is still easily seen on the moon. Since Bob is on a holiday on the moon, they decide to do a key exchange. For this, they take an off-the-shelf QKD protocol (one that only requires that Alice sends randomly polarised photons, and that Bob measures in a random polarisation direction – no quantum computers needed). And as the photon source, Alice uses her laser pointer. That is, she sends short light flashes of the laser pointer through her polarisation filter as specified by the QKD protocol.

2. Alice and Bob want to use some QKD protocol over a long distance (300 km). Unfortunately, all QKD protocols and implementations they know of do not manage to do more than 250 km (because otherwise the error rate on the channel would become too high). Fortunately, in the middle between Alice and Bob lives Charlie, an untrusted yet helpful person. To get rid of the errors, they let Charlie work as an amplifier: Each qubit is sent to Charlie, and Charlie measures the qubit and resends it using a fresh photon.

3. In a usual QKD protocol Alice would first send the qubits. Then she would wait for Bob to receive these. Then Alice sends the bases in which she produced the check qubits (or some other classical information needed for the check/purification/privacy amplification; this depends on the protocol they use). Alice and Bob decide to be more efficient and do a "compressed QKD". Since it is only Alice that sends

something, anyway, she sends all information simultaneously. I.e., she sends the qubits and the classical information at the same time (over the quantum and the authenticated classical channel, respectively) and thus achieves at least doubled throughput.