QUANTUM CRYPTOGRAPHY
Master of Logic, University of Amsterdam, 2018
TEACHERS: Jan Czajkowski, Yfke Dulek, and Christian Schaffner

Homework problem set 3

Please hand in your solutions to these exercises in digital form (typed, or scanned from a neatly hand-written version) through Canvas no later than **Friday 29 June, 20:00h**.

Problem 1: Parallel repetition of non-local games

Consider the following cooperative game G. Alice receives an input bit s, and Bob an input bit t. They are promised that $(s,t) \in_R \{(0,0),(0,1),(1,0)\}$. They generate output bits $a, b \in \{0,1\}$ respectively, and win if $a \vee s \neq b \vee t$.

(a) Analyze the winning probability p_{win} for the trivial strategy $a = s$ and $b = t$. Can any classical strategy do better?

(b) In the two-parallel version $G^{(2)}$ of this game, Alice and Bob receive *two* pairs (s_0, t_0) and (s_1, t_1), selected independently and uniformly at random from $\{(0,0),(0,1),(1,0)\}$. (Alice gets (s_0, s_1), Bob gets (t_0, t_1).) They win if their responses (a_0, a_1) and (b_0, b_1) are such that $a_i \vee s_i \neq b_i \vee t_i$ for all $i \in \{0,1\}$. Of course, Alice and Bob can win with probability p^2_{win} if they simply repeat the strategy from part (a) twice. But maybe they can do better?
Describe a classical strategy for $G^{(2)}$ with a winning probability of at least $\frac{2}{3}$.

(c) Suppose Alice and Bob have a valid classical strategy for $G^{(2)}$ which wins with probability q. Describe a classical strategy for G guaranteeing the same winning probability q. (Recall that Alice and Bob may have shared randomness, but they may not communicate.)

(d) Is the strategy you found in (b) optimal?

Problem 2: A Simple Quantum Bit Commitment Protocol, Continued

Recall the bit commitment protocol we discussed in the exercise session. In the *commit phase*, Alice commits to bit b by preparing the state $|\psi_b\rangle = \sqrt{\alpha}|bb\rangle + \sqrt{1-\alpha}|22\rangle$, and sending the second qutrit to Bob. In the *open phase*, she reveals the classical bit b and sends the first qutrit over to Bob, who checks that the pure state is the correct one, by making a measurement with respect to any orthogonal basis containing $|\psi_b\rangle$.

In class, we computed Bob's cheating probability,

$$P_B^* = \Pr[\text{Bob guesses } b \text{ after the commit phase}],$$

to be $\frac{1}{2} + \frac{\alpha}{2}$. Next, let's calculate Alice's cheating probability P_A^*, given by

$$\frac{1}{2}(\Pr[\text{Alice opens } b = 0 \text{ successfully}] + \Pr[\text{Alice opens } b = 1 \text{ successfully}])$$

(a) Let the underlying Hilbert space be $\mathcal{H} \otimes \mathcal{H}_s \otimes \mathcal{H}_t$, where $\mathcal{H}_t$ corresponds to the qutrit that is sent to Bob in the commit phase, $\mathcal{H}_s$ to the qutrit that is sent during the opening phase, and $\mathcal{H}$ is any auxiliary system that Alice might use. For the most general strategy, we can assume that she prepares the pure state $|\phi\rangle$, as it can always be purified on $\mathcal{H}$.

We can write $|\phi\rangle = \sum_i \sqrt{p_i}|i\rangle|\tilde{\psi}_{i,b}\rangle$ where $\{|i\rangle\}$ and $\{|\tilde{\psi}_{i,b}\rangle\}$ are Schmidt bases of $\mathcal{H}$ and $\mathcal{H}_s \otimes \mathcal{H}_t$ respectively. Note that depending on the bit b Alice tries to open, she can use a different Schmidt basis of $\mathcal{H}_s \otimes \mathcal{H}_t$. Hence, the reduced density matrix on $\mathcal{H}_s \otimes \mathcal{H}_t$ is $\sigma^b_{s,t} = \sum_i p_i |\tilde{\psi}_{i,b}\rangle\langle\tilde{\psi}_{i,b}|$. However, the part in $\mathcal{H}_t$ which is sent to Bob in the commitment phase does not depend on b and we use σ_t to denote Bob's reduced density matrix after the commit phase, i.e. just a qutrit. Now, compute the probability of dishonest Alice successfully opening bit b in terms of the squared fidelity between the states $|\psi_b\rangle$ and $\sigma^b_{s,t}$.

(b) Then give the following upper bound on Alice's cheating probability:

$$P_A^* \leq \frac{1}{2}\left(F^2(\sigma_t, \rho_0) + F^2(\sigma_t, \rho_1)\right)$$

Hint: use the fact that the fidelity is non-decreasing under taking partial trace, in particular tracing out system $\mathcal{H}_s$.

(c) Remember the property of fidelity that for any three density matrices ρ_1, ρ_2, ρ_3, it holds that $F^2(\rho_1, \rho_2) + F^2(\rho_1, \rho_3) \leq 1 + F(\rho_2, \rho_3)$. Give an upper bound to Alice's cheating probability in terms of α.

(d) The bound on Alice's cheating probability that we just obtained is tight. There is a simple cheating strategy that allows Alice to achieve this bound, without even making use of the auxiliary system $\mathcal{H}$. What state(s) of two qutrits can she prepare?

(e) Finally, by combining the calculations so far on Alice and Bob's cheating probabilities, determine the α that minimizes the overall cheating probability of the protocol. What is the overall cheating probability?

Problem 3: Quantum computing on encrypted data

Alice wants Bob to perform some quantum circuit for her. She encrypts her n-qubit state $|\psi\rangle$ using a quantum one-time pad. Call the X-keys to the quantum one-time pad $\vec{a} = (a_1, ..., a_n)$, and the Z-keys $\vec{b} = (b_1, ..., b_n)$. She then sends the encrypted state to Bob. In this exercise, you will investigate how Bob can perform a quantum circuit C, consisting of gates $G_1, ..., G_k$, on this state such that the following holds:

(Correctness) If Bob follows the protocols for the gates $G_1, ..., G_k$ in the correct order, then the resulting state can be decrypted to $C|\psi\rangle$ by Alice, who can only do Pauli operations and classical computation.

(Security) If Bob does not know the keys $\vec{a}$ and $\vec{b}$, he does not learn anything about Alice's input state $|\psi\rangle$.

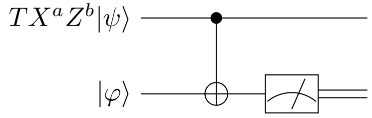
(a) Bob performs the Clifford gates (e.g., $X, Z, H, P, CNOT$) by directly applying them to the encrypted qubits. Alice uses her classical computation power to update her key vectors $\vec{a}$ and $\vec{b}$ after each gate application. Describe in detail the classical computations Alice must perform to update her keys after Bob applies (i) a phase gate P and (ii) a $CNOT$ gate.

(b) Find expressions for x, y and z (in terms of 0, 1, a, and b) such that

$$TX^aZ^b = P^yX^xZ^zT.$$

(c) For the rest of this exercise, consider $n = 1$. Let $X^aZ^b|\psi\rangle$ describe the state of Alice's encrypted input qubit. After Bob applies a T gate, P^y is an error on the output state: Bob cannot continue his computation correctly without removing it first. However, Bob does not know y and therefore he cannot perform $(P^y)^\dagger$. Should Alice tell him y? Why or why not?

(d) If Alice is allowed to use quantum communication at this point, she can send Bob an encrypted magic state to help him resolve the error P^y. What state $|\varphi\rangle$ should she send? Assume that Bob will apply the following circuit:



where the measurement is in the computational basis. On the top wire, the output state should be of the form $X^cZ^dT|\psi\rangle$, i.e., a quantum one-time pad encryption of $T|\psi\rangle$.

(e) Bob will send the measurement outcome back to Alice. Describe how Alice can compute the new key c, d from that outcome, combined with her knowledge of a and b.