Introduction to quantum information processing
Exercise sheet 4

Prof. Dr. Frank Wilhelm-Mauch
Nicolas Wittler
Raphael Schmit

text mod text mod **SS 2019** **Submission date 21th June**

***Note**: You may hand in your solutions in a group with up to three persons. Please provide your name to your solutions.*

Exercise 1: Secure QKD protocol? (*14 points*)

Consider the following protocol which intends to establish a common key between Alice and Bob: A machine prepares n pairs of qubits in the maximally-entangled Bell-singlet state

$$|\psi^-_{\text{Bell}}\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}.$$

Each pair is then split up and the qubits are distributed among Alice and Bob. Here, the first digit refers to the qubit Alice gets and the second to Bobs. Thus, both of them have a sequence of n qubits at the end. For each qubit they *randomly*, *independently* and *secretly* choose a basis in which they measure the qubit: Alice can choose from the set

$$\left\{Z_1, \frac{Z_1 + X_1}{\sqrt{2}}, X_1\right\} \equiv \{A_1, A_2, A_3\},$$

whereas Bobs basis is from

$$\left\{\frac{Z_2 + X_2}{\sqrt{2}}, X_2, \frac{-Z_2 + X_2}{\sqrt{2}}\right\} \equiv \{B_1, B_2, B_3\},$$

where X_i, Z_i are the usual Pauli matrices acting on qubit i. So, at the end both of them have a table with n rows, where row i shows the chosen basis and the measurement result for qubit i. Once they finished all the measurements, they publicly announce their columns of *measurement basis*, and by comparing both sequences they divide the sequences of *measurement results* into two different groups: group one contains all cases where both of them used *different* measurement basis, whereas all the other cases with the *same* measurement basis go into group two.

(a) Group one is used to do the Bell test: From the measurement results Alice and Bob compute the CHSH-correlation

$$S = \langle A_1 B_1\rangle - \langle A_1 B_3\rangle + \langle A_3 B_1\rangle + \langle A_3 B_3\rangle\,,$$

which is restricted by $-2 \leq S \leq 2$ according to classical physics. Calculate the correlation S, where the expectation value is to be taken for the state $|\psi^-_{\text{Bell}}\rangle$, and show that it is given by $S = -2\sqrt{2} < 2$. (*4 points*)

(b) Suppose the correlation S they computed from their measurement results equals $-2\sqrt{2}$, which tells them that their qubits were entangled. How can they construct a common key using the measurement results from group two? (*3 points*)

(c) Now take an eavesdropper Eve into account: Is there any chance that you could get knowledge about the key? Explain! What could Alice and Bob do in order to check whether somebody was eavesdropping/trying to eavesdrop? (*5 points*)

(d) A general question: Suppose Alice and Bob have a secret common key s made out of n digits. How can this key be used to en- and decrypt a message m being also n digits long? Is it secure supposed the key is only known to Alice and Bob? Explain shortly! (*2 points*)

Exercise 2: Modular multiplication (*13 points*)

Consider the function $f(x) = 7x \pmod{15}$ with integer inputs $0 \leq x \leq 15$. Note that all appearing numbers can be stored using four (qu)bits.

(a) Give the action of f for all different inputs in form of a table like

x (binary)	x (dec.)	$f(x)$ (dec.)	$f(x)$ (binary)
0000	0	0	0000
⋮	⋮	⋮	⋮

(*4 points*)

(b) Explain shortly why it is not possible to create a quantum circuit mapping an input qubit $|x\rangle$ to the output qubit $|f(x)\rangle$ using only four qubits. (*3 points*)

(c) Here, we are lucky and can overcome this problem quite easily by *declaring* $f(0) = 15$. With that, give a quantum circuit with the same action as $f(x)$ using only CNOTs and single-qubit rotations. (*6 points*)
Hint: In principle this can be done by writing down the matrix representation from the above table (*with* our declaration) and using the decomposition scheme from lecture. But there is also a more clever way: Inspect the binary representation of x and $f(x)$ and find the hidden rule transforming x to $f(x)$, which should be translated to a circuit rather easily.

Exercise 3: RSA and number theory (*13 points*)

(a) Prove that $xy \mod N \equiv (x \mod N)(y \mod N) \mod N$. (*4 points*)

(b) Find the period of the function $f(x) = b^x \mod N$ for $N = 1023$ and $b = 99$. (*4 points*)

(c) Verify $a^{(p-1)(q-1)} \equiv 1 \mod (pq)$ for $p = 7, q = 11$ and $a = 15$. (*5 points*)