Quantum Cryptography (spring 2021)	Dominique Unruh
Exercise Sheet 13	
Out: 2021-05-18	Due: 2021-05-25

This is a **bonus homework**. It can be used if you have less than 50% of the point total. (Recall that you need 50% to qualify for the exam.) But you are also welcome (and encouraged) to solve the homework if you do not need the points, for sake of learning.

1 Quantum proofs

Knowlets:	ProofSys ProblemID: QProofs
Time:	
Difficulty:	

Show that if (P, V) is a proof system (Definition 53 in the lecture notes), then it also is a quantum proof system as in the following definition:

Definition 1 (Quantum proof systems) *We call a pair (P, V) of interactive machines a* quantum proof system *for the relation R with* soundness-error ε *iff the following two conditions are fulfilled:*

- Completeness: *For any $(x, w) \in R$, we have that* $\Pr[\langle P(x, w), V(x)\rangle = 1] = 1$.
- Soundness: *For any (potentially computationally unlimited)* ***quantum*** *machine P^*, and for any $x \notin L_R$, we have* $\Pr[\langle P^*(), V(x)\rangle = 1] \leq \varepsilon$.

Notice that the only difference to Definition 53 in the lecture notes is the additional word **quantum**.

2 Zero-knowledge and discrete logarithm

Fix a group G of prime order q with generator g. (G, q, and g may depend on some implicit security parameter but are considered publicly known.) Let $R := \{(x, w) : g^w = x, w \in \{0, \ldots, q-1\}\}$.

Consider the following proof system for R (Schnorr's proof system for discrete logarithms):

- The prover P gets input $(x, w) \in R$.
- The verifier V gets input $x \in R$.
- The prover P chooses $b \xleftarrow{\$} \{0, \ldots, q-1\}$ and sends $a := g^b$ to the verifier V.
- The verifier chooses $r \xleftarrow{\$} \{0, \ldots, q-1\}$ and sends r to the prover P.
- The prover P computes $s := b + rw \bmod q$ and sends s to the verifier V.
- The verifier V checks whether $x, a \in G$ and $g^s = ax^r$.

This proof system is well-known to be a proof system. However, in the classical setting, it is unknown whether this proof system is zero-knowledge![1]

(a)

Knowlets:	ProofSys ProblemID: ZKDlogSound
Time:	
Difficulty:	

Show that (P, V) is a proof system with soundness-error $1/q$.

(b)

Knowlets:	QZK, DlogAlgo ProblemID: ZKDlogShor
Time:	
Difficulty:	

Show that (P, V) is statistical quantum zero-knowledge.

Hint: This has nothing to do with rewinding! It has a lot to do with Shor's algorithm.

[1] It is however "honest-verifier zero-knowledge". This is a weaker notion where the verifier is considered to behave honestly.