Quantum Cryptography (fall 2013)	Prof. Dr. Dominique Unruh

Exercise Sheet 12

Out: November 30, 2013	Due: December 9, 2013

Problem 1: Aborting simulators

Let R, P, V be as in the lecture in the description of the graph isomorphism protocol.

In the classical case, we used the following two properties of the "aborting simulator" S_1 (described in the lecture):

Claim 1: If $(x, w) \in R$, then $\Pr[S_1(x, z) \text{ aborts}] = \frac{1}{2}$.
Claim 2: Assume that $(x, w) \in R$. Let $S_1(x, z)$ denote the distribution of the output of S_1 on inputs x, z. (Assume a special output symbol $\perp$ for abort.) Let $S_1(x, z)|\mathit{success}$ denote that distribution under the condition that $S_1(x, z) \neq \perp$. Then $S_1(x, z)|\mathit{success}$ has the same distribution as $\langle P(x, w), V(x, z)\rangle$.

These two claims can be shown as follows:

Consider the following games. In each game, we assume that V^* runs on input (x, z), and the notation $\alpha \leftarrow V^*[\beta]$ means that we send β to V^* and let α denote the answer/output. We write $\alpha \xleftarrow{\$} M$ for uniformly chosen $\alpha \in M$. *perm* denotes the set of permutations on the set of vertices of G_1. We assume $x = (G_1, G_2)$ and $w = \phi$, and that V^* never chooses an $i \notin \{1, 2\}$.

$$i^* \xleftarrow{\$} \{1,2\}, \quad \psi \xleftarrow{\$} \mathit{perm}, \quad H := \psi(G_{i^*}),$$
$$i \leftarrow V^*[H], \quad \mathit{out} \leftarrow V^*[\psi], \quad \text{if } i^* = i \text{ return } \mathit{out} \text{ else return } \bot \tag{1}$$
$$i^* \xleftarrow{\$} \{1,2\}, \quad \boldsymbol{\tau \xleftarrow{\$} \mathit{perm}}, \quad \textbf{if } \boldsymbol{i^* = 1} \textbf{ then } \boldsymbol{\psi := \tau} \textbf{ else } \boldsymbol{\psi := \tau \circ \phi^{-1}}, \quad H := \psi(G_{i^*}),$$
$$i \leftarrow V^*[H], \quad \mathit{out} \leftarrow V^*[\psi], \quad \text{if } i^* = i \text{ return } \mathit{out} \text{ else return } \bot \tag{2}$$
$$i^* \xleftarrow{\$} \{1,2\}, \quad \tau \xleftarrow{\$} \mathit{perm}, \quad \text{if } i^* = 1 \text{ then } \psi := \tau \text{ else } \psi := \tau \circ \phi^{-1}, \quad \boldsymbol{H := \tau(G_1)},$$
$$i \leftarrow V^*[H], \quad \mathit{out} \leftarrow V^*[\psi], \quad \text{if } i^* = i \text{ return } \mathit{out} \text{ else return } \bot \tag{3}$$
$$i^* \xleftarrow{\$} \{1,2\}, \quad \tau \xleftarrow{\$} \mathit{perm}, \quad H := \tau(G_1), \quad i \leftarrow V^*[H],$$
$$\text{if } \boldsymbol{i} = 1 \text{ then } \psi := \tau \text{ else } \psi := \tau \circ \phi^{-1},$$
$$\mathit{out} \leftarrow V^*[\psi], \quad \text{if } i^* = i \text{ return } \mathit{out} \text{ else return } \bot \tag{4}$$
$$\tau \xleftarrow{\$} \mathit{perm}, \quad H := \tau(G_1), \quad i \leftarrow V^*[H], \quad \text{if } i = 1 \text{ then } \psi := \tau \text{ else } \psi := \tau \circ \phi^{-1},$$
$$\mathit{out} \leftarrow V^*[\psi], \quad \boldsymbol{i^* \xleftarrow{\$} \{1,2\}}, \quad \text{if } i^* = i \text{ return } \mathit{out} \text{ else return } \bot \tag{5}$$
$$\tau \xleftarrow{\$} \mathit{perm}, \quad H := \tau(G_1), \quad i \leftarrow V^*[H], \quad \text{if } i = 1 \text{ then } \psi := \tau \text{ else } \psi := \tau \circ \phi^{-1},$$
$$\mathit{out} \leftarrow V^*[\psi], \quad \textbf{with probability } \boldsymbol{\tfrac{1}{2}} \textbf{ return } \boldsymbol{\mathit{out}} \textbf{ else return } \boldsymbol{\bot} \tag{6}$$
$$\boldsymbol{\mathit{out} \leftarrow \langle P(x,w), V^*(x,z)\rangle}, \quad \text{with probability } \tfrac{1}{2} \text{ return } \mathit{out} \text{ else return } \bot \tag{7}$$

(The parts that changed between two lines are highlighted in boldface.)

On can check that for any two consecutive games in this sequence, the output that is returned by the game has the same distribution.

Furthermore, the output of the first game is obviously the same as $S_1(x,z)$. And the output of the last game, conditioned on not being $\bot$, is the same as $\langle P(x,w), V^*(x,z)\rangle$. Since the outputs of the first and the last game have the same distribution, it follows that the distribution $S_1(x,z)$, conditioned on not aborting, is the same as $\langle P(x,w), V^*(x,z)\rangle$. This shows Claim 2.

Furthermore, in the last game, obviously $\Pr[\mathit{out} = \bot] = \frac{1}{2}$. Thus in the first game, $\Pr[\mathit{out} = \bot] = \frac{1}{2}$. Hence $\Pr[S_1(x,z) \text{ aborts}] = \frac{1}{2}$. This shows Claim 1.

In the following, let S_1^Q denote the "aborting simulator" in the quantum setting. I.e., $S_1^Q(x,\rho)$ is constructed like $S_1(x,z)$, except that it runs the quantum verifier $V^*(x,\rho)$ and returns the quantum state ρ' produced by V^*.

For simplicity, assume a state $|\bot\rangle$ that S_1^Q denotes to indicate failure, and assume that $P_\bot \rho' = 0$ for any state ρ' that V^* can output where $P_\bot := |\bot\rangle\langle\bot|$. (I.e., V^* never outputs $|\bot\rangle$). Let $\bar{P}_\bot := 1 - P_\bot$.

(a) Understand the proof in the classical case. In particular, understand why all the games are equivalent and where we use $(x,w) \in R$.

Note: This gives no points, but is helpful for the next problem. You don't need to write anything up for this problem.

(b) Show: If $(x,w) \in R$, then $\mathrm{tr}(P_\perp \cdot S_1^Q(x,\rho)) = \frac{1}{2}$. (I.e., S_1^Q aborts with probability exactly $\frac{1}{2}$.)

(c) Show: If $(x,w) \in R$, then

$$\frac{\bar{P}_\perp \cdot S_1^Q(x,\rho) \cdot \bar{P}_\perp}{\mathrm{tr}(\bar{P}_\perp \cdot S_1^Q(x,\rho) \cdot \bar{P}_\perp)} = \langle P(x,w), V^*(z,\rho)\rangle.$$

(I.e., conditioned on not aborting, $S_1^Q(x,\rho)$ outputs $\langle P(x,w), V^*(z,\rho)\rangle$.)

(d) Show: If $\frac{\bar{P}_\perp \cdot S(x,\rho) \cdot \bar{P}_\perp}{\mathrm{tr}(\bar{P}_\perp \cdot S(x,\rho) \cdot \bar{P}_\perp)} = \langle P(x,w), V^*(z,\rho)\rangle$ for some simulator S and $\mathrm{tr}(P_\perp \cdot S(x,\rho)) \leq \varepsilon$, then $\mathrm{TD}(S(x,\rho), \langle P(x,w), V^*(z,\rho)\rangle) \in O(\sqrt{\varepsilon})$.

(This shows that if we manage to construct a simulator S that aborts rarely and, conditioned on not aborting, has the right distribution, then we have statistical zero-knowledge.)

Hint: Apply Lemma 8 in the lecture notes to $S(x,\rho)$ to get a state $\tilde{\rho}$ with $\bar{P}_\perp \tilde{\rho} \bar{P}_\perp = \tilde{\rho}$ and $\mathrm{TD}(\rho_S, \tilde{\rho}) \leq \sqrt{\varepsilon}$ where $\rho_S := S(x,\rho)$. Then find upper bounds for $\mathrm{TD}(\bar{P}_\perp \rho_S \bar{P}_\perp, \bar{P}_\perp \tilde{\rho} \bar{P}_\perp)$, for $\mathrm{TD}(\tilde{\rho}, t_S \rho_V)$ where $\rho_V := \langle P(x,w), V^*(z,\rho)\rangle$ and $t_S := \mathrm{tr}\, \bar{P}_\perp \rho_S \bar{P}_\perp$, for $\mathrm{TD}(\rho_V, t_S \rho_V)$, and for $\mathrm{TD}(\rho_S, \rho_V)$ (in that order).

Problem 2: Quantum proofs

Show that if (P,V) is a proof system (Definition 59 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 59 in the lecture notes is the additional word **quantum**.

Problem 3: Zero-knowledge and discrete logarithm (bonus problem)

This problem is optional. But you can gain 8 extra points from it. This can help if you are below the 50 % required for participating in the exam.

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 $R := \{(x, w) : g^w = x, w \in \{0, \dots, q-1\}\}$.

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 $b \xleftarrow{\$} \{0, \dots, q-1\}$ and sends $a := g^b$ to the verifier V.
- The verifier chooses $r \xleftarrow{\$} \{0, \dots, q-1\}$ 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) Show that (P, V) is a proof system with soundness-error $1/q$.

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

Hint: This has nothing to do with rewinding!

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