COM-440, Introduction to Quantum Cryptography, Fall 2025

Exercise # 12

We recall the notion of a (quantum-secure) pseudorandom function family (PRF) from class: a classical polynomial-time computable family $F = \{F_\lambda : \{0,1\}^{m(\lambda)} \times \{0,1\}^{n(\lambda)} \to \{0,1\}^{\ell(\lambda)}\}_\lambda$ is a quantum-secure PRF family if for every quantum polynomial-time algorithm $\mathcal{D}$ with oracle access,

$$\left| \Pr_{k \leftarrow_U \{0,1\}^m} \left[\mathcal{D}^{F_\lambda(k,\cdot)}(1^\lambda) = 1\right] - \Pr_{G \leftarrow_U \{\{0,1\}^n \to \{0,1\}^\ell\}} \left[\mathcal{D}^{G}(1^\lambda) = 1\right] \right| \leq \mathrm{negl}(\lambda) \; .$$

Here, in the second probability, the function G is chosen uniformly at random among all functions with the correct domain and range.

1. **Message authentication codes**

   A *message authentication code* (MAC) is specified by a triple of classical polynomial-time algorithms $(\mathsf{Gen}, \mathsf{Tag}, \mathsf{Ver})$ with the following properties:

   - Gen takes as input 1^λ and returns a key $k \leftarrow \mathsf{Gen}(1^\lambda)$
   - Tag takes as input a key k and message m and outputs a tag $\sigma \leftarrow \mathsf{Tag}_k(m)$
   - Ver takes as input k, m and σ and returns either "accept" or "reject"

   In addition, we impose the correctness requirement that for every λ and message m,

   $$\Pr_{k \leftarrow \mathsf{Gen}(1^\lambda)} [\mathsf{Ver}_k(m, \mathsf{Tag}_k(m)) = \text{“accept”}] = 1 \; .$$

   Furthermore, we say that $(\mathsf{Gen}, \mathsf{Tag}, \mathsf{Ver})$ is secure if for every quantum polynomial-time $\mathcal{A}$,

   $$\Pr_{\substack{k \leftarrow \mathsf{Gen}(1^\lambda) \\ m,\sigma \leftarrow \mathcal{A}^{\mathsf{Tag}_k(\cdot)}(1^\lambda)}} \left[\mathcal{A} \text{ did not query } m \wedge \mathsf{Ver}_k(m,\sigma) = \text{“accept”}\right] \leq \mathrm{negl}(\lambda) \; .$$

   Note that here, we only allow $\mathcal{A}$ to make classical queries to the tagging oracle for simplicity.

   (a) Read the definitions carefully and explain how a MAC can be employed to instantiate a classical authenticated channel as used in QKD, provided that the users Alice and Bob have a preshared key $k \leftarrow \mathsf{Gen}(1^\lambda)$.

   (b) Suggest a construction of a secure message authentication code from any quantum-secure PRF. Verify that your proposal is correct and sketch the proof of security.

2. **Bit commitment**
In this exercise we show that a secure bit commitment scheme can also be implemented from a suitable PRF family. Suppose thus that $F = (F_\lambda : \{0,1\}^{m(\lambda)} \times \{0,1\}^{n(\lambda)} \to \{0,1\}^{\ell(\lambda)})_\lambda$ is a secure PRF family with $\ell = 3m$. Consider the following commitment scheme, where Bob has a bit $b \in \{0,1\}$. In the commitment phase, Alice sends a uniformly random $r \in \{0,1\}^\ell$ to Bob. Bob selects a random $k \in \{0,1\}^m$. If $b = 0$ he sends $v = F(k, 0^n)$ to Alice and if $b = 1$ he sends $v = r \oplus F(k, 0^n)$. In the open phase, Bob sends k and b to Alice. Alice computes $F(k, 0^n) \oplus v$ and accepts if $b = 0$ and the result is 0^ℓ, or if $b = 1$ and the result is r. (You will notice that this scheme only evaluates the function $F(k, \cdot)$ at the point 0^n. This is because the construction does not require the "full power" of a PRF, only the fact that it provides a (seemingly) uniformly random output at some input.)

   (a) Show that this scheme is hiding, as long as malicious Alice is computationally bounded (and hence cannot break the PRF security).

   (b) Show that the scheme is ε-binding, for some ε depending on m to be determined.