

COM-440, Introduction to Quantum Cryptography, Fall 2025

Exercise Solution # 12

1. Message authentication codes

- (a) Suppose that Alice and Bob have a preshared key $k \leftarrow \text{Gen}(1^\lambda)$.

When one of them needs to send a message m through CAC to the other one, the sender can send m together with $\sigma \leftarrow \text{Tag}_k(m)$, and the receiver on receiving a message m together with σ , checks whether $\text{Ver}_k(m, \sigma) = \text{"accept"}$, and accepts the message m if so.

In this way, Eve cannot make the receiver accept a message m that Alice and Bob never intended to send. This establishes a classical authenticated channel.

- (b) Consider the following MAC scheme based on a PRF.

- $\text{Gen}(1^\lambda)$ samples a key k uniformly at random from $\{0, 1\}^{m(\lambda)}$ where $m(\lambda)$ is the key length of the PRF.
- $\text{Tag}_k(m)$ outputs a tag $\sigma = F_\lambda(k, m)$.
- $\text{Ver}_k(m, \sigma)$ outputs “accept” if and only if $\sigma = F_\lambda(k, m)$.

From the construction, we can see that the scheme satisfies correctness:

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

Moreover, for every quantum polynomial-time \mathcal{A} ,

$$\Pr_{\substack{G \leftarrow_U \{0, 1\}^n \rightarrow \{0, 1\}^\ell \\ m, \sigma \leftarrow \mathcal{A}^{G(\cdot)}(1^\lambda)}} [\mathcal{A} \text{ did not query } m \wedge \sigma = G(m)] = \frac{1}{2^\ell} ,$$

because the function value of a uniformly random function G on a not queried position is uniformly random from the range.

Since PRF family cannot be distinguished from the uniformly random function G , we have that

$$\Pr_{\substack{k \leftarrow \text{Gen}(1^\lambda) \\ m, \sigma \leftarrow \mathcal{A}^{\text{Tag}_k(\cdot)}(1^\lambda)}} [\mathcal{A} \text{ did not query } m \wedge \text{Ver}_k(m, \sigma) = \text{"accept"}] \leq \text{negl}(\lambda) + \frac{1}{2^\ell} = \text{negl}(\lambda) ,$$

for $\ell(\lambda) = \Omega(\lambda)$. (If $\ell(\lambda) = o(\lambda)$, we can do parallel repetition to the PRF to increase the output length. Therefore, without loss of generality, we can assume $\ell(\lambda) = \Omega(\lambda)$.)

So the construction satisfies both correctness and security.

2. Bit commitment

(a) Suppose for contradiction that the scheme is not hiding. Then there exists a computationally bounded Alice that on input $r^b \oplus F(k, 0^n)$, outputs b with probability more than $\frac{1}{2} + \frac{1}{\text{poly}(\lambda)}$, where r^b denotes the all zero string 0^ℓ .

Then we can construct an adversary for the underlying PRF as follows: it samples $b \leftarrow \{0, 1\}$ and runs Alice to get r . Then it makes a query to the oracle on 0^n to get a output y , and then runs Alice on input $v = r^b \oplus y$. If Alice returns b , then the adversary outputs 1; otherwise, the adversary outputs 0.

It is easy to see that the above adversary outputs 1 with probability more than $\frac{1}{2} + \frac{1}{\text{poly}(\lambda)}$ if given access to the PRF, and outputs 1 with probability exactly $\frac{1}{2}$ if given access to a uniformly random function G (since the distribution of $v = r^b \oplus y$ does not depend on b if y is sampled uniformly at random). Thus this gives an efficient adversary for the PRF, which contradicts with the security of the PRF.

Therefore, this scheme is hiding.

(b) For binding, we can consider computationally unbounded adversary.

Bob can open the commitment in two differently ways if and only if for r chosen by Alice, there exists k_1, k_2 such that $r \oplus F(k_1, 0^n) = F(k_2, 0^n)$. In other words, $r \in R := \{F(k_1, 0^n) \oplus F(k_2, 0^n) : k_1, k_2 \in \{0, 1\}^m\}$. Note that R is a set of size at most 2^{2m} , so for the honest Alice, the event that the randomness r that Alice samples satisfies that $r \in R$ happens with probability at most $\frac{2^{2m}}{2^\ell} = \frac{1}{2^m}$.

Therefore, $p_0 + p_1 \leq 1 + \frac{1}{2^m}, m$ and thus the scheme is ε -binding for $\varepsilon = \frac{1}{2^m}$.