Foundations of Interactive Proofs
Tutorial 3

Recall that a *commitment scheme* over a message space $\mathcal{M}$ is a triple of PPT algorithms $(\mathsf{Setup}, \mathsf{Commit}, \mathsf{Open})$ with the following template:

- $\mathsf{Setup}(1^n)$: on input the security parameter n (in unary), sample public parameters pp (we assume w.l.o.g. that pp includes 1^n).
- $\mathsf{Commit}(\mathsf{pp}, m)$: on input the public parameters and a message $m \in \mathcal{M}$, outputs (as a randomized algorithm) a pair (c, d) where c is called the *commitment* and d the *opening*.
- $\mathsf{Open}(\mathsf{pp}, c, m, d)$: on input the public parameters, a commitment c, a message m, and an opening d, output a bit $b \in \{0, 1\}$.

A commitment scheme must be *correct*, *binding*, and *hiding*:

- **Correctness.** For all $m \in \mathcal{M}$,

$$\Pr[\mathsf{pp} \leftarrow \mathsf{Setup}(1^n), (c, d) \leftarrow \mathsf{Commit}(\mathsf{pp}, m) \ : \ \mathsf{Open}(\mathsf{pp}, c, m, d) = 1] = 1.$$

- **Binding.** For every PPT adversary $\mathcal{A}$,

$$\Pr[m_0 \neq m_1 \ \wedge \ \forall b \in \{0, 1\}, \mathsf{Open}(\mathsf{pp}, c, m_b, d_b) = 1] \leq \mathsf{negl}(n),$$

  where probabilities are over the choice of $\mathsf{pp} \leftarrow \mathsf{Setup}(1^n)$ and $(c, (m_b, d_b)_{b \in \{0,1\}}) \leftarrow \mathcal{A}(\mathsf{pp})$.
- **(Strong) hiding.** For every stateful PPT adversary $\mathcal{A}$,

$$|\Pr[\mathcal{A}(c_0) = 1] - \Pr[\mathcal{A}(c_1) = 1]| \leq \mathsf{negl}(n),$$

  where the probabilities are over the choice of $(\mathsf{pp}, m_0, m_1) \leftarrow \mathcal{A}(1^n)$ and $(c_b, d_b) \leftarrow \mathsf{Commit}(\mathsf{pp}, m_b)$ for $b = 0, 1$.

In this tutorial, we will explore constructions of commitment schemes.

1 Commitments from Pseudorandom Generators

A *pseudorandom generator* is a procedure that produces a long string which *looks* random (to any polynomial-time machine) from a short seed. Formally, a function $G : \{0, 1\}^n \to \{0, 1\}^m$ is a pseudorandom generator (PRG) if $m = m(n) > n$ is a polynomially-bounded function and for every PPT adversary $\mathcal{A}$,

$$|\Pr[x \leftarrow \{0, 1\}^m \ : \ \mathcal{A}(x) = 1] - \Pr[s \leftarrow \{0, 1\}^n, x \leftarrow G(s) \ : \ \mathcal{A}(x) = 1]| \leq \mathsf{negl}(n).$$

Remark

One of the most celebrated results of cryptography is the proof by Håstad, Impagliazzo, Levin, and Luby that pseudorandom generators are equivalent to one-way functions (functions that are polytime-computable but hard to invert in polynomial time), an assumption widely regarded as the weakest and most fundamental assumption in cryptography.

Let $G : \{0, 1\}^n \to \{0, 1\}^{3n}$ be a length-tripling PRG. We would like to use this PRG to build a commitment scheme over $\mathcal{M} = \{0, 1\}$. Consider the following attempt:

- $\mathsf{Setup}(1^n)$: set $\mathsf{pp} = 1^n$.
- $\mathsf{Commit}(\mathsf{pp}, m)$: if $m = 0$, sample $s \leftarrow \{0, 1\}^n$ and set $c = G(s)$, $d = s$. Else, sample $c \leftarrow \{0, 1\}^{3n}$ and set $d = \texttt{random}$. Output (c, d).

Question 1. How would one define the Open algorithm for this commitment scheme? Does it satisfy binding? Does it satisfy hiding?

Question 2. We modify $\mathsf{Setup}(1^n)$ to return $\mathsf{pp} \leftarrow \{0,1\}^{3n}$. Construct an alternative candidate commitment scheme where for every $m \in \{0,1\}$, an opening is a valid preimage by G to *some* string.

Question 3. Prove that any adversary that breaks binding can be turned into a distinguisher for the PRG.

Question 4. Prove that the scheme is statistically hiding, with a cheating probability bounded by 2^{-n}.

2 Commitments from the discrete logarithm assumption

The scheme of the previous section achieves a statistical hiding property. An interesting and non-trivial question is to build a commitment scheme where hiding is *perfect*. Building such a scheme from an arbitrary one-way function is a long-standing open problem. However, one can derive a perfectly-hiding commitment scheme using number-theoretic assumptions. In this section, we focus on the *discrete logarithm problem*: let $\mathbb{G}$ be a cyclic group of prime order p with a generator g. The discrete logarithm problem over $\mathbb{G}$ states that for every PPT $\mathcal{A}$,

$$\Pr[x \leftarrow \mathbb{Z}_p \ : \ \mathcal{A}(g^x) = x] \leq \mathsf{negl}(n).$$

Question 5. The definition of the discrete logarithm problem above is slightly informal and technically incorrect. Can you fix it?

Question 6. Consider the following attempt at building a perfect commitment scheme over $\mathcal{M} = \mathbb{Z}_p$:

- $\mathsf{Setup}(1^n)$: output the description of a group $\mathbb{G}$ of order p and a generator g.
- $\mathsf{Commit}(\mathsf{pp}, m)$: on input $m \in \mathbb{Z}_p$, return $(c, d) = (g^m, \perp)$.
- $\mathsf{Open}(\mathsf{pp}, c, m, d)$: check whether $c = g^m$ and output 1 if the check passes.

Can you identify the problem with the above construction?

Question 7. Find a fix to the above construction using another generator h and a *blinding term* to properly hide the message m.

Question 8. Prove that any adversary that breaks binding can be turned into an attacker on the discrete logarithm assumption.

Question 9. Prove that the scheme is perfectly hiding.