Section 1

# Commitment Schemes

## Commitment Schemes

Digital analogue of a safe.

**Definition 1 (Commitment scheme)**

An efficient two-stage protocol (S, R) .

**Commit** The sender S has private input $\sigma \in \{0,1\}^*$ and the common input is $1^n$. The commitment stage result in a joint output $c$, the *commitment*, and a private output $d$ to S, the *decommitment*.

**Reveal** S sends the pair $(d, \sigma)$ to R, and R either accepts or rejects.

**Completeness:** R always accepts in an honest execution.

**Hiding:**. In commit stage: $\forall$ R$^*$, $m \in \mathbb{N}$ and $\sigma \neq \sigma' \in \{0,1\}^m$, $\{\mathrm{View}_{\mathrm{R}^*}(\mathrm{S}(\sigma), \mathrm{R}^*)(1^n)\}_{n\in\mathbb{N}} \approx_c \{\mathrm{View}_{\mathrm{R}^*}(\mathrm{S}(\sigma'), \mathrm{R}^*)(1^n)\}_{n\in\mathbb{N}}$.

## Commitment Schemes cont.

**Binding:** “Any" $\mathsf{S}^*$ succeeds in the following game with negligible probability in $n$:

> *On security parameter* $1^n$, $\mathsf{S}^*$ *interacts with* $\mathsf{R}$ *in the commit stage resulting in a commitment* $c$*, and then output two pairs* $(d, \sigma)$ *and* $(d', \sigma')$ *with* $\sigma \neq \sigma'$ *such that* $\mathsf{R}(c, d, \sigma) = \mathsf{R}(c, d', \sigma') = \texttt{Accept}$

## Commitment Schemes cont.

- wlg. we can think of $d$ as the random coin of S, and $c$ as the transcript
- Hiding: Perfect, statistical, computational
- Binding: Perfect, statistical. computational
- Cannot achieve both properties to be statistical simultaneously.
- For computational security, we will assume non-uniform entities:
  On security parameter $n$, the adversary gets an auxiliary input $z_n$ (length of auxiliary input does not count for the running time)
- Suffices to construct “bit commitments"
- (non-uniform) OWFs imply statistically binding, and statistically hiding commitments

# Perfectly Binding Commitment from OWP

Let $f\colon \{0,1\}^n \mapsto \{0,1\}^n$ be a permutation and let $b$ be a (non-uniform) hardcore predicate for $f$.

**Protocol 2 ((S, R))**

**Commit:**
S's input: $\sigma \in \{0,1\}$
S chooses a random $x \in \{0,1\}^n$, and sends $c = (f(x), b(x) \oplus \sigma)$ to R

**Reveal:**
S sends $(x, \sigma)$ to R, and R accepts iff $(x, \sigma)$ is consistent with $c$ (i.e., $f(x) = c_1$ and $b(x) \oplus \sigma = c_2$)

## Claim 3

Protocol 2 is perfectly binding and computationally hiding commitment scheme.

Proof: Correctness and binding are clear.
**Hiding:** for any (possibly non-uniform) algorithm A, let

$$\Delta_n^A = |\Pr[A(f(U_n), b(U_n) \oplus 0) = 1] - \Pr[A(f(U_n), b(U_n) \oplus 1) = 1]|$$

It follows that

$$|\Pr[A(f(U_n), b(U_n) \oplus 0) = 1] - \Pr[A(f(U_n), b(U_n) \oplus U) = 1]| = \Delta_n^A/2$$

Hence,

$$|\Pr[A(f(U_n), b(U_n)) = 1] - \Pr[A(f(U_n), U) = 1]| = \Delta_n^A/2 \quad (1)$$

Thus, $\Delta_n^A$ is negligible for any PPT

## Statistically Binding Commitment from OWF.

Let $g\colon \{0,1\}^n \mapsto \{0,1\}^{3n}$ be a (non-uniform) PRG

**Protocol 4 ((S, R))**

**Commit**

**Common input:** $1^n$

**S's input:** $\sigma \in \{0,1\}$

**Commit:**

1. R chooses a random $r \leftarrow \{0,1\}^{3n}$ to S
2. S chooses a random $x \in \{0,1\}^n$, and send $g(x)$ to S in case $\sigma = 0$ and $c = g(x) \oplus r$ otherwise.

**Reveal**: S sends $(\sigma, x)$ to R, and R accepts iff $(\sigma, x)$ is consistent with $r$ and $c$

Correctness is clear. Hiding and biding HW