

---

**Scheme**    Commitment

---

A bit-level commitment scheme based on a hash function  $\mathsf{H}$ . The commitment is implicitly broadcasted after the **Commit** step. Later, the sender reveals the committed value  $m$  and the receivers run the **Open** function to verify its validity.

**Inputs:**  $\mathcal{P}_S : m$ , an input message to commit and later open.

$sid$ : a unique session identifier (optional, for UC-security).

**Outputs:**  $valid$  if the commitment is verified correctly.

**Commit**( $m$ ) $\dashrightarrow(c, w)$

- 1: Sample  $w \xleftarrow{\$} \{0, 1\}^*$ , a random witness
  - 2:  $c \leftarrow \mathsf{H}(m \parallel w \parallel sid)$ , a commitment to  $m$
- return**  $(c, w)$

**Open**( $m, c, w$ ) $\dashrightarrow valid$

- 1:  $c' \leftarrow \mathsf{H}(m \parallel w \parallel sid)$
- return**  $valid$  if  $c = c'$ , **ABORT** otherwise
- 

## References