

---

Scheme	Commitment
	A bit-level commitment scheme based on a hash function $H$ . The commitment is implicitly broadcasted after the <b>Commit</b> step. Later, the sender reveals the committed value $m$ and the receivers run the <b>Open</b> function to verify its validity.
<b>Inputs:</b>	$\mathcal{P}_S : m$ , an input message to commit and later open. $sid$ : a unique session identifier (optional, for UC-security).
<b>Outputs:</b>	<i>valid</i> if the commitment is verified correctly.
	<b>Commit</b> $(m) \dashrightarrow (c, w)$ 1: Sample $w \xleftarrow{\$} \{0, 1\}^*$ , a random witness 2: $c \leftarrow H(m \parallel w \parallel sid)$ , a commitment to $m$ <b>return</b> $(c, w)$  <b>Open</b> $(m, c, w) \dashrightarrow valid$ 1: $c' \leftarrow H(m \parallel w \parallel sid)$ <b>return</b> <i>valid</i> if $c = c'$ , <b>ABORT</b> otherwise

---

## References