Scheme Pedersen Commitment (PC)

The commitment scheme from [Ped91, Section3] parametrized by a group $\mathbb{G}$ of prime order q with a generator G (e.g., an elliptic curve $\mathsf{E}(\mathbb{G}, q, G)$), and a second generator H chosen independently[1] from G.

Inputs: m, an input message to commit and later open.
Outputs: *valid* if the commitment is verified correctly.

Commit$(m \in \mathbb{Z}_q) \dashrightarrow (C, w)$
1: Sample $w \xleftarrow{\$} \mathbb{Z}_q$, a random witness
2: $C \leftarrow w \cdot G + m \cdot H$ as the commitment of m.
return (C, w)

Open$(m, C, w) \dashrightarrow$ *valid*
1: $c' \leftarrow m \cdot G + w \cdot H$
return *valid* if $c \stackrel{?}{=} c'$, ABORT otherwise.

References

[Ped91] Torben Pryds Pedersen. Non-interactive and information-theoretic secure verifiable secret sharing. In *Annual international cryptology conference*, pages 129–140. Springer, 1991.

[1] Such that nobody knows x s.t. $H = x \cdot G$. This can effectively achieved via aggregation of commitments of independent random values following the instructions of [Ped91], or via $H \leftarrow \mathsf{Hash2Curve}(m)$ of a fixed message m (e.g., $m =$ "NOTHING UP MY SLEEVE") as we do.