Commitment

allows one to commit to a chosen value while keeping it hidden to others, but can be revealed at a later time when the one opens * necessary parameter.

- hiding ; a given x and its commitment should be unrelatable.
  ⇒ should reveal no information about x
- binding ; there is no way that different values can result in the same commitment.
  ⇒ cannot change the value after committing.

Pedersen Commitment [Ped92]

- Setup(1^λ) ; choose a large prime q. and p s.t. $p = 2q+1$.
  choose $g \xleftarrow{\$} \mathbb{Z}_q^*$
  choose $a \xleftarrow{\$} \mathbb{Z}_q^*$ and compute $h := g^a$.
  output (p, q, g, h).

- Com(x) ; choose $r \xleftarrow{\$} \mathbb{Z}_p^*$
  output $c := g^x h^r$.

- Open(c, x, r) ; check whether c is equal to $g^x h^r$ or not.

Note that $Com(x_1; r_1) \cdot Com(x_2; r_2) = Com(x_1 + x_2; r_1 + r_2)$.

$(g^{x_1} h^{r_1} \cdot g^{x_2} h^{r_2} = g^{x_1 + x_2} \cdot h^{r_1 + r_2})$

⇒ proving linear relationships among committed value.

Sigma protocols are known in literature to prove knowledge of a committed value, equality of two committed values, and so on.

Moreover, "linear relationship" between Pedersen commitments can be shown.

[Given Com(x) and Com(y), one could show that $y = ax + b$ for some public a and b]