Note that $Com(x)^a \cdot Com(y)^b = Com(ax+by)$ since Pedersen commitment supports addition.

$\Rightarrow$ also supports linear combinations.

Blind Evaluation of a Polynomial

Suppose Alice has a polynomial P of degree d and Bob has a point $s \in \mathbb{F}_p$.

Goal: Bob wishes to learn $Com(P(s))$.

i) naive method;

Bob learns P

① Alice sends P to Bob. and he computes $Com(P(s))$.

② Bob sends s to Alice. she computes $Com(P(s))$ and sends it to Bob.

Alice learns s.

ii) using Pedersen commitment;

① Bob sends to Alice $Com(1), Com(s), \cdots, Com(s^d)$

② Alice computes $Com(P(s)) = Com(1)^{a_0} \cdot Com(s)^{a_1} \cdot \cdots \cdot Com(s^d)^{a_d}$

where $P(x) = a_0 + a_1 x + \cdots + a_d x^d$.

$\Rightarrow$ Alice cannot learn s and Bob cannot learn $P(x)$. neither.

The remaining problem

$\Rightarrow$ "verifiable" polynomial evaluation.

i) making sure Alice computes her polynomials according to an assignment

ii) hiding the assignment $\Rightarrow$ masking polynomials.

iii) computing multiplications from two commitments

iv) non-interactive.

$\Rightarrow$ the use of pairing of elliptic curves

Think thing