commitment

LECTURE 10 MON 3/11

Commitment Scheme

two phases:

- → commit(x) — produces x with a "commitment"
- → reveal(x) — "opens" the commitment and reveals x

properties:

- → hiding — commit(x) reveals nothing of x
- → binding — can only open in <u>one</u> way s.t. can't alter x
- → non-malleability* — given commit(x) can't generate a commitment to a related value. i.e. commit(x+1)

* sometimes desired

Pedersen commitment

implementation setup:

- → choose p, q large primes s.t. $p-1$ divides q
- → choose g as a generator of order q subgroup of $\mathbb{Z}_p^*$ $g \in \mathbb{Z}_p^*$ s.t. $|\langle g \rangle| = q$
- → choose at random $a \leftarrow \{1, 2, \dots, q-1\}$ and let $h = g^a$

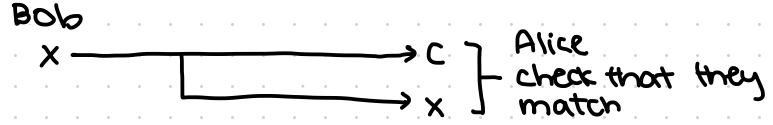
Note that h also generates $\langle g \rangle$

$\text{commit}_{g,h}(x)$:

for $x \in \mathbb{Z}_q$ $(x \in \{0, 1, \dots, q-1\})$, choose at random $r \leftarrow \mathbb{Z}_q$. output commitment $c = g^x h^r \bmod p$

reveal(com): reveals x and r

receiver verifies that $c = g^x h^r \bmod p$



Note

x is not nec-essarily plaintext

has unconditional hiding since $\forall c \in \langle g \rangle \quad \forall x \in \mathbb{Z}_q$, $\exists$ unique $r \in \mathbb{Z}_q$ s.t. $g^x h^r = g^{x+ar} = g^z$ for some $z \in \mathbb{Z}_q = c$

$\Rightarrow x + ar = z$

$\Rightarrow r = a^{-1}(z - x) \bmod q$

is computationally binding (meaning an all-powerful adversary could open but not a computationally bounded one)