

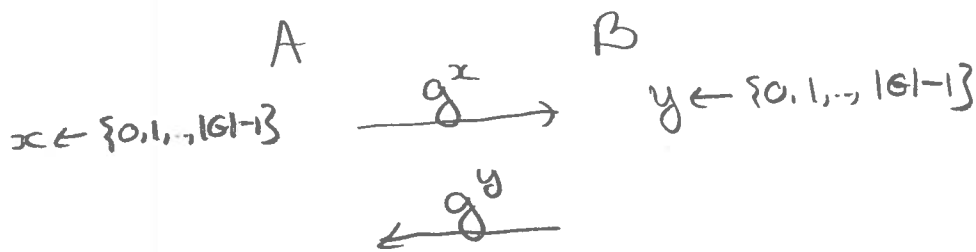
Today: Pedersen Commitment

PK Encryption

El-Gamal Enc

Recall: Previous lecture we covered DH Key Exchange.

$G$  is a cyclic group,  $g$  generator



key =  $g^{xy}$

for an eavesdropper who sees  $g^x, g^y$

The key is ind. from random in  $G$  if:

$$(g^x, g^y, g^{xy}) \approx (g^x, g^y, g^r)$$

DDH Assumption ↗

For which groups is it reasonable to assume the DDH Assumption?

Eg:  $\mathbb{Z}_p^*$  is a cyclic group (assuming  $p$  is a prime)

Moreover, we assume Discrete Log is hard in  $\mathbb{Z}_p^*$  L10.2

i.e.  $g^x \xrightarrow{\text{HARD}} x$  for  $x \leftarrow \{0, 1, \dots, p-1\}$  &  $g$  fixed generator.

However: DDH Assumption does not hold in  $\mathbb{Z}_p^*$

Example of cyclic group that we believe DDH holds:

Let  $p, q$  large prime numbers s.t.  $q \mid p-1$  (eg.  $p=2q+1$ )  
safe prime

Let  $g$  be a generator of a subgroup of  $\mathbb{Z}_p^*$  of order

$$q. \quad \langle g \rangle = \{1, g, g^2, \dots, g^{q-1}\}$$

(eg.  $p=2q+1$   $g$  any quadratic residue s.t.  $g \neq 1$ )

We believe DDH holds in  $\langle g \rangle$ .

Both constructions that we will see today:

(Pedersen Commitment & El-Gamal Enc,

use a cyclic  $g \in \mathbb{Z}_p^*$  of prime order, which is a subgroup of  $\mathbb{Z}_p^*$ .

For El-Gamal Enc we will rely on DDH

For Pedersen Com we will rely on DL. ← will use the fact that  $\text{GF}[\mathbb{Z}_q]$  is field

# Pedersen Commitment Scheme

40.3

Recall: A commitment scheme consists of 2 phases:

$\text{Commit}(x) \rightarrow$  Alg that given  $x$  produces a "commitment" to  $x$

$\text{Reveal}(\text{com}) \rightarrow$  "Opens" the commitment  $\text{com}$ , i.e., reveals  $x$ .

## Properties:

Hiding:  $\text{Commit}(x)$  reveals nothing about  $x$

Binding: Can only open  $\text{com}$  in one way

(i.e., cannot change  $x$ ).

Sometimes we want non-malleability:

Given  $\text{Commit}(x)$  cannot generate a commitment to a related value, say  $x+1$ .

## Pedersen Commitment

Setup:  $p, q$  large primes s.t.  $q | p-1$

$g$  a generator of order  $q$  subgroup of  $\mathbb{Z}_p^*$ ,

i.e.  $g \in \mathbb{Z}_p^*$  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  $\langle g \rangle$ .

Commit  $(x)$ : For  $x \in \mathbb{Z}_q$  ( $x \in \{0, 1, \dots, q-1\}$ ):  
 $g, h$

Choose at random  $r \leftarrow \mathbb{Z}_q$

Output  $\text{com} = g^x h^r \pmod{p}$ .

Reveal  $(\text{com})$ : reveal  $x, r$

Receiver verifies that  $\text{com} = g^x h^r \pmod{p}$

Hiding: Perfect hiding: Hiding holds even against  
 an unbounded adversary.

For any  $x \in \mathbb{Z}_q$   $g^x \cdot h^r$  is uniformly distributed in  $\langle g \rangle$

independent of  $x$ .

In other words  $\forall c \in \langle g \rangle \forall x \in \mathbb{Z}_q$  there exists unique

$$r \in \mathbb{Z}_q \text{ s.t. } \begin{aligned} g^x h^r &= c \\ &= g^z \text{ for some } z \in \mathbb{Z}_q \\ g^{x+ar} & \end{aligned}$$

$$\Rightarrow x + a \cdot r = z$$

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

Note that  $a$  has an inverse mod  $g$  since  $GF(g)$  is a field (since  $g$  is prime!).

### Binding: Computationally binding

An all powerful adv. may open in two different ways, but a bounded adv (who cannot break DL) cannot.

Suppose adv. generates  $c \in \langle g \rangle$  together w.  $x \neq x'$  &  $r, r'$  s.t.

$$c = g^x h^r = g^{x'} h^{r'} \pmod{p}$$

$$\Rightarrow x + ar = x' + ar' \pmod{g}$$

$$\Rightarrow a = \frac{x - x'}{r - r'} \pmod{g}$$

Note that  $r - r' \neq 0$  (since o.w. it must be that  $x = x'$ ). Hence  $r - r'$  has an inverse mod  $g$

since  $GF(g)$  is a field (for prime  $g$ ).

Hence, such an adv broke DL in  $\langle g \rangle$ .

Given  $h = g^a$  he found  $a$ .

Non-malleable : No

$$\text{Given } c = \underset{\substack{\uparrow \\ \text{randomness}}}{\text{commit}(x; r)} = g^x h^r$$

one can easily compute

$$c \cdot g = g^{x+1} h^r = \text{commit}(x+1; r)$$

Not all applications need non-malleability.

## Public Key Encryption

Consists of three algorithms: KeyGen, Enc, Dec.

KeyGen: Takes as input a security parameter  $\lambda$   
in unary ( $1^\lambda$ ).  $\lambda \approx$  key size

The reason for giving it in unary is only syntactic:  
so we can say that KeyGen runs in poly time  
(in input length).

KeyGen( $1^\lambda$ ) outputs a pair (PK, SK).

Enc: Takes as input (PK,  $m$ ) and outputs ciphertext  $c$ .  
msg in msg space  $\mathcal{M}$ .

Dec : Takes as input  $(SK, c)$  and outputs  $m$ .  
 ciphertext

Correctness

$\forall (PK, SK)$  generated according to KeyGen,  $\forall m \in M$

$$Dec(SK, Enc(PK, m)) = m$$

(Often correctness is relaxed to hold with high prob over  $(PK, SK) \leftarrow KeyGen(\lambda)$ )

"Semantic Security" :  $\forall m, m' \in M$

$$(PK, Enc(PK, m)) \cong (PK, Enc(PK, m'))$$

In the formal def  $m$  &  $m'$  can be generated adv. as a function of  $PK$ .

(will be defined formally later)

Note : For semantic security to hold

KeyGen must be randomized &

Enc must be randomized.

Usually Dec is deterministic.

El-Gamal Enc Scheme (1984)

Let  $G = \langle g \rangle$  be a cyclic gp. w. generator  $g$

for which we believe DDH holds

$$(g^x, g^y, g^{xy}) \cong (g^x, g^y, g^r)$$

for  $x, y, r$  random in  $\{0, 1, \dots, |G|-1\}$ .

An example of such group

the set of all quadratic residues in  $\mathbb{Z}_p^*$ , for  $p$  which is a safe prime ( $p = 2q + 1$ ).

KeyGen: Choose at random  $x \leftarrow \{0, 1, \dots, |G| - 1\}$

Let  $SK = x$

$PK = g^x$

Output  $(PK, SK)$

Enc: Given  $PK = g^x$  & msg  $m \in G$ .

↑  
randomized

Choose at random  $y \leftarrow \{0, 1, \dots, |G| - 1\}$

Compute  $K = g^{xy}$

Output  $(g^y, K \cdot m)$

[ Note:  $K$  can be thought of a key obtained from a DH key Exchange, w.  $g^x$  &  $g^y$  ]

Dec: Given  $SK = x$  & ciphertext

$(a, b) (= (g^y, g^{xy} \cdot m))$

output  $m = b/a^x$



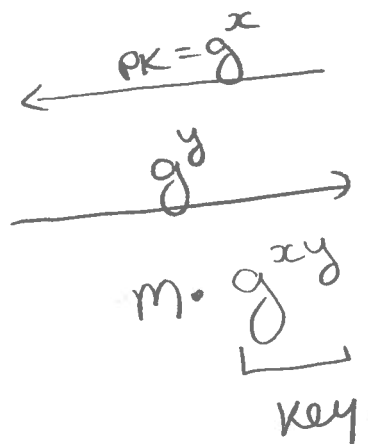
Correctness

Follows since

$$b/a^x = g^{xy \cdot m} / a^x = g^{xy \cdot m} / g^{yx} = m \quad \checkmark$$

Security: To prove security we need to prove that given  $PK = g^x$  & given  $g^y$  and  $m$ ,  $K = g^{xy}$  is uniformly distributed in  $G$ , and hence is a "good mask" for  $m$ .

This follows from the security of the DH Key Exchange, which is known to be secure under DDH.



Encrypt by multiplying by key

Decrypt by dividing by key