Oblivious Transfer

- Sender has $m_1, \dots, m_n \in M$.
- Receiver has $i \in [1..n]$
- Goal. (1) Receiver learns m_i, and no other m_j.
  (2) Sender does not learn i

OT from El Gamal

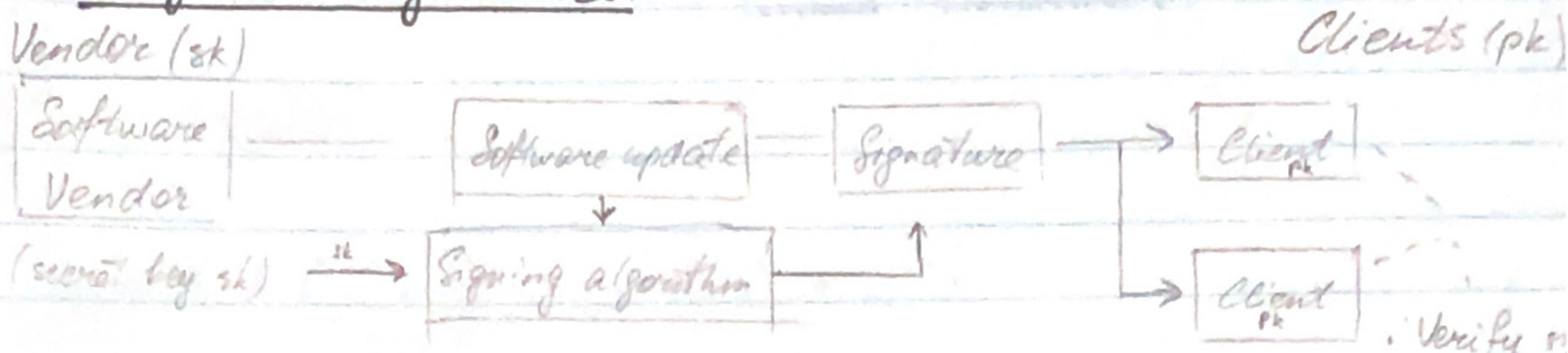
- Group G ; $\langle G \rangle = q$; hash func $H: G^2 \to M \times k$
- CPA secure (E_s, D_s) channel.

Receiver (Bob)		Sender (Alice)	
$a \leftarrow \mathbb{Z}_q$	$\xleftarrow{v \leftarrow g^B}$ $\xrightarrow{u \leftarrow g^a v^{-i}}$	$B \leftarrow \mathbb{Z}_q$	El Gamal pk $u_i = g^a v^{-i}$ so $u_i = g^a$
Take c_i		for j in $1..n$.	]
$w \leftarrow v^a$		$w_j \leftarrow u \cdot v^j$	
$k \leftarrow H(v, w)$		$w_j \leftarrow w_j^B$	
$m \leftarrow D_s(k, c_i)$	$\xleftarrow{(c_1, \dots, c_n)}$	$k_j \leftarrow H(v, w_j)$	El Gamal c_B
		$c_j \leftarrow E_s(k_j, m_j)$	] $(v, c_j) = (g^B, c_j)$

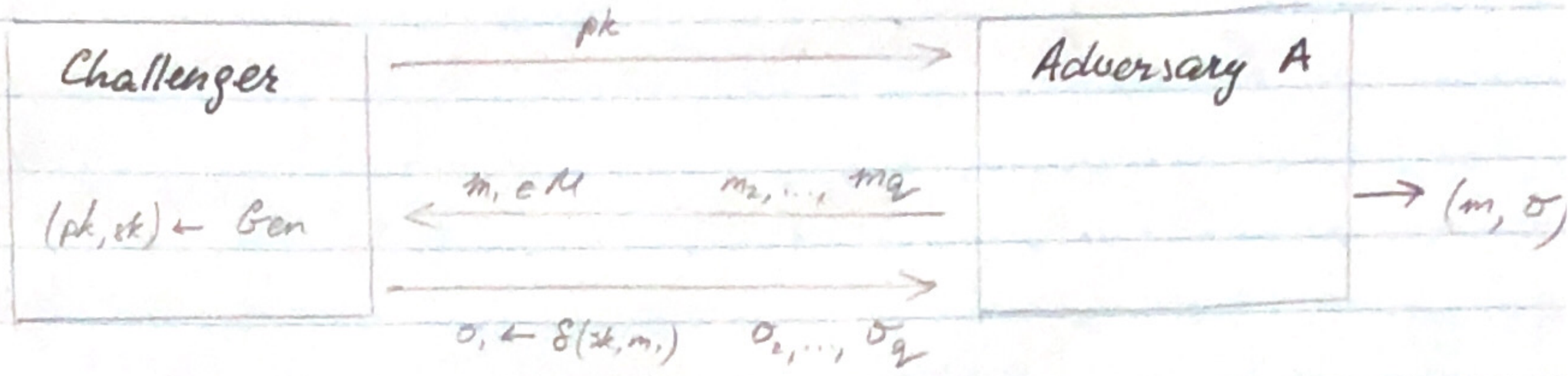
- The article i which Bob wants to read is encrypted with Bob's public key.
- Other articles encrypted with some other public keys (unknown).
- Bob can decrypt and read u_i, the article

Lecture 3

Digital Signatures



Security Game.



Adv wins if $V(pk, m, \sigma) =$ 'accept' and $m \notin \{m_1, \ldots, m_Q\}$

Secure Signature Scheme

Def. $SS = (Gen, S, V)$ is secure if for all eff A:

$$Adv_{SIG}[A, SS] = Pr[A \text{ wins}] < negl.$$

Example. $SS = (Gen, S, V)$. Attacker can find $m_0 \neq m_1$ s.t.

$$V(pk, m_0, \sigma) = V(pk, m_1, \sigma) \quad \forall \sigma, (pk, sk) \leftarrow Gen$$

Q. Can this SS be secure?

↳ No, signatures can be forged: (1) Ask to sign m_0. Gives σ_0.

(2) Forge (m_1, σ_0).

Hilroy

Euler Theorem

- $(Z_p)^*$ is called a cyclic group, that is

$\exists\ g \in (Z_p)^*$ such that $\{1, g, g^2, g^3, \ldots, g^{p-2}\} = (Z_p)^*$

g is called a generator of $(Z_p)^*$.

Example. $p = 7$

$\{1, 3, 3^2, 3^3, 3^4, 3^5\} = \{1, 3, 2, 6, 4, 5\} = (Z_7)^*$

- Not every element is a generator:

$\{1, 2, 2^2, 2^3, 2^4, 2^5\} = \{1, 2, 4\}$.

Solving Quadratic Equations (mod p)

- Solve: $ax^2 + bx + c$ in Z_p
- Solution: $x = (-b \pm \sqrt{b^2 - 4ac}) / 2a$ in Z_p

1) Find $(2a)^{-1}$ in Z_p using Euclid

2) Find square root of $b2 - 4ac$ in Z_p (if exists) using a square root algorithm.