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

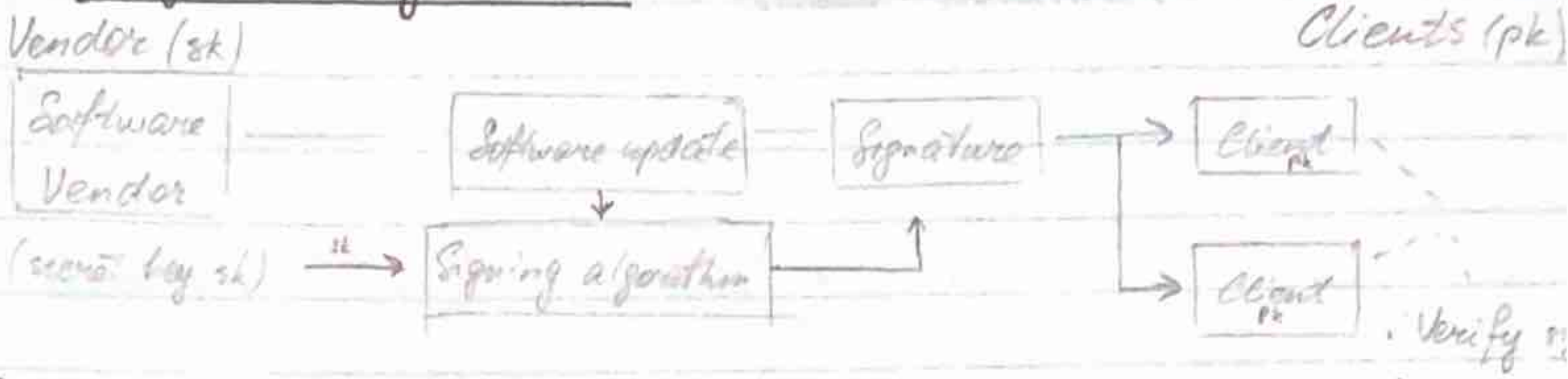
- Group G ; $\langle G \rangle = q$; hash func $H: G^2 \to M \times K$
- CPA secure (E_S, D_S) channel.

Receiver (Bob)		Sender (News)	
$a \leftarrow \mathbb{Z}_q$	$\xleftarrow{v \leftarrow g^{\beta}}$	$\beta \leftarrow \mathbb{Z}_q$	
	$\xrightarrow{u \leftarrow g^{a} v^{-i}}$		El Gamal pk
Take c_i		for j in $1..n$.	$u_j = g^{a} v^{j-i}$ so $u_i = g^{a}$
$w \leftarrow v^{a}$		$u_j \leftarrow u \cdot v^{j}$	
$k \leftarrow H(v, w)$		$w_j \leftarrow u_j^{\beta}$	
$m \leftarrow D_S(k, c_i)$	$\xleftarrow{(c_1, \dots, c_n)}$	$k_j \leftarrow H(v, w_j)$	El Gamal ct
		$c_j \leftarrow E_S(k_j, m_j)$	$(v, c_j) = (g^{\beta}, S)$

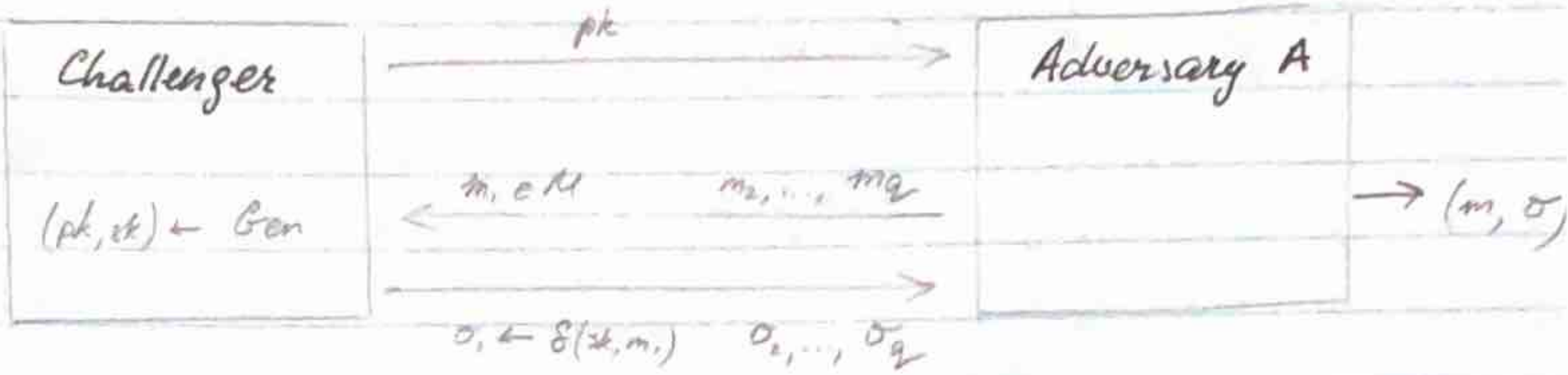
- The article i which Bob wants to read is encrypted with Bob's public key.
- Other articles encrypted with some other public keys (unknown).
- Bob can decrypt and read u_i, the article

Lecture 3

Digital Signatures



Security Game.



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

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

Q. Can this SS be secure?

↳ No, signatures can be forged: (1) Ask to sign m_0. Given σ_0.
(2) Forge (m_1, σ_0).

Euler Theorem.

- $(\mathbb{Z}_p)^*$ is called a cyclic group, that is

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

  g is called a generator of $(\mathbb{Z}_p)^*$.

Example. $p = 7$

$\{1, 3, 3^2, 3^3, 3^4, 3^5\} = \{1, 3, 2, 6, 4, 5\} = (\mathbb{Z}_7)^*$

- 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 $\mathbb{Z}_p$

- Solution. $x = (-b \pm \sqrt{b^2 - 4ac}) / 2a$ in $\mathbb{Z}_p$

1) Find $(2a)^{-1}$ in $\mathbb{Z}_p$ using Euclid

2) Find square root of $b^2 - 4ac$ in $\mathbb{Z}_p$ (if exists) using a square root algorithm.