SOCIAL NETWORKS

LECTURE #16

Review.

1) Auction
2) Mixed Strategy Nash Equilibria

SIGNALING GAMES

- Two players (plus one): $\begin{cases} S = \text{Sender} & (\text{Sam}) \\ R = \text{Receiver} & (\text{Ram}) \end{cases}$
  $N = \text{Nature}$ (not strategic)

Information Asymmetric Game.
$\Rightarrow$ **TYPE** (private information)

(1) Nature selects a type t_i from

$$T = \{t_1, t_2, \dots, t_I\}$$

with probability $p(t_i)$

(2) Sam (Sender) observes (privately) t_i and selects a message m_j from

$$M = \{m_1, m_2, \dots, m_J\}$$

(3) Ram (Receive) observes m_j (but not t_i) and carries out an action a_k from

$$A = \{a_1, a_2, \ldots, a_k\}$$

$S_N = T$, $S_S = M$, $S_R = A$

Strategy Profile = $T \times M \times A$

Payoffs = $u_i : T \times M \times A \to \mathbb{R}$.

$u_S(t_i, m_j, a_k)$; $u_R(t_i, m_j, a_k)$

Nash Equilibria:

(A) POOLING EQUILIBRIUM.
All types of senders send the same message. GOOGLE

(B) SEPARATING EQUILIBRIUM.
All types of senders send different messages. FACEBOOK

(C) COMBINATION
Babbling →.

Deception, in these Nash equilibria?

Information Asymmetry.

1) Anonymity (k-Anonymity, Dark Web)
2) Encryption (Public Key Crypto System)
3) Privacy (Diff. Privacy)
4) Security (Firewall, Threat Analysis, ...)

Public Key Crypto Systems

⇒ Asymmetric Cryptography.

2 separate keys { Public/Verification key Vr_A
Private/Signaling key Sg_A.

Vr_A and Sg_A are mathematically linked
→ While they are computationally asymmetric.

ONE WAY FUNCTIONS.

Integer Factorization { Multiplication of two Integers.
vs.
Factoring a composite Integer.

Other examples:

(i) Discrete Logarithms.
(ii) Elliptic Curves.
(iii) Lattice Theory.

PROPERTIES

(i) It is computationally ~~for~~ easy for a user A to generate both

$$\begin{cases} Vr_A \\ Sg_A \end{cases}$$

(ii) It is computationally hard for another user to derive Sg_A from Vr_A.

(a) Anyone can verify A's identity using publicly available Vr_A
(b) Noone (using conventional computational resources) can assume/steal A's identity (e.g. the secret/private Sg_A).
(c) A can have many persistent heteronyms (anonymity/pseudonymity)
(d) A's identity can be linked to his biological/genetic identity.
(e) No secure key-exchange (using a third party) is necessary.

Example:

RSA (Rivest - Shamir - Adleman).

a) Choose two distinct prime numbers
$p, q \quad p \neq q$.

b) Compute $n = pq$. $\begin{cases} n = \text{public} \\ p, q = \text{private} \end{cases}$

$$\varphi(n) = \varphi(p)\,\varphi(q) = (p-1)(q-1)$$

φ = Euler's totient function.

c) Choose e s.t. e and $\varphi(n)$ are coprime.

$$\gcd(e, \varphi(n)) = 1.$$

$$\exists d, k \quad d \cdot e + k\varphi(n) = 1.$$

$$d \cdot e \equiv 1 \mod \varphi(n)$$

$$d \equiv e^{-1} \pmod{\varphi(n)}$$

d) $Vr = e \leftarrow$ Public

$Sg = d \leftarrow$ Private

e) M = Message

$$M|_{Vr} \equiv \cdot \; c \equiv m^e \pmod{n}$$

Polynomical in $\lg(e)$

Repeated squaring.

f) $m \equiv c^d \pmod n$

$c|_{sg} = m$ recoverd in polynomial time if one knows d

(Or. equivalently

$\varphi(n) = p \cdot q - p - q - 1$

$= n - p - q - 1$

$= n - (p+q) - 1$)

(or equivalently, factorization of n)

Use Fermat's Little Thm.

p = prime, $p \nmid a$

$\Rightarrow a^{p-1} \equiv 1 \pmod p$.

$m^{p-1} \equiv 1 \pmod p$

$(m^{p-1})^{k(q-1)} \cdot m \equiv m \pmod p$

$m^{ed-1} \cdot m \equiv m \pmod p$

$m^{ed} \equiv m \pmod p$

Similarly $m^{ed} \equiv m \pmod q$

$m^{ed} \equiv m \pmod n$

$c^d \equiv m \pmod n$.

SIGNALING GAME.

① $S \rightarrow \begin{cases} \text{Private Signing Key } Sg_S \\ \text{Public Verifying Key } Vr_S \end{cases}$

② S detects

(a) type/state $t_i \in T$ (e.g. y = BTC Wallet)

(b) message $m_j \in M$ (e.g. transfer x BTC to R $\wedge (y-x) \geq 0$)

(c) time-stamp u

③ S sends an augmented message to R

$$C \equiv \left(Vr_S, Vr_R, m_j, \#t_i\big|_{Vr_R}, u \right)\Big|_{Sg_S}$$

↑ Digest of the private type

④ R verifies

$$C\big|_{Vr_S} \Rightarrow$$

a) S did send the message.

b) Local properties m_j is consistent with t_i

$$y_S \geq x_{S \rightarrow R}$$

c) R performs an action consistent with m_j

$y_S := y_S - x_{S \to R}$

$y_R := y_R + x_{S \to R}$.

What about Global Properties ?

$y_S := y_S - x_{S \to R_1}$; $y_S := y_S - x_{S \to R_2}$; ....

$y_{R_1} := y_{R_1} + x_{S \to R_1}$; $y_{R_2} := y_{R_2} + x_{S \to R_2}$; ....

How does one ensure that the interleaving is correct ?

GLOBAL VERIFIERS.

Bit-Coin Miners.