Privacy Enhancing Technologies

Lecture 1: Intro + FHE

Why this class?

Privacy Enhancing Tech

look at "solutions"

Not a policy class

- This will be your 1st privacy class
- " " last
-

Goal: Computing "privately" over data

$$y_1, \ldots, y_n \leftarrow f(x_1, \ldots, x_n)$$

$x_1, \ldots, x_n$: data from n parties

$y_1, \ldots, y_n$

2nd half: private data analysis
how not to leak "too much" information from the outputs

1st half: cryptography
how to compute f without leaking information

Logistics

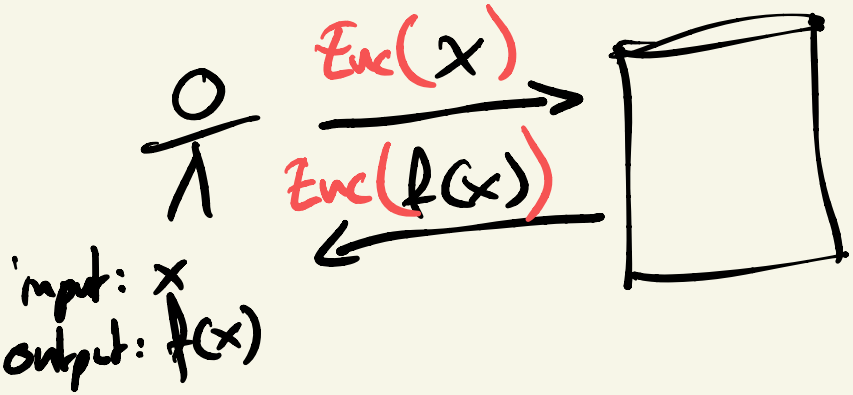
* spylab.ai/teaching/pets25
  - ↳ lecture notes, class notes
  - ↳ homeworks

* Moodle
  - ↳ announcements
  - ↳ Forum for Q&A

Grading: 50% Midterm (Nov 3)
50% Final (Dec 15)

Please use the feedback form!

Fully Homomorphic Encryption (FHE)



More formally:

FHE: (Gen, Enc, Dec, Eval)

as in standard Enc scheme

$$Eval(f, c_1, \ldots, c_n) \to c'$$

where $c_i = Enc_K(x_i)$

such that $Dec_K(c') = f(x_1, \ldots, x_n)$

Trivial solution : $Eval(f, c_1, \ldots, c_n)$

$c' \to (f, c_1, \ldots, c_n)$

$Dec(c') \to f(x_1, \ldots, x_n)$

Compactness : $|c'|$ indep. of $|f|$

Very non-trivial : proposed in 78
solved in 2009 Gentry

"Easy" to have some homomorphic property

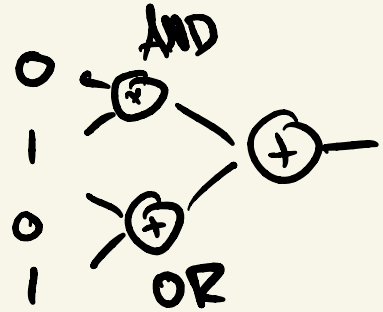
Ex : El Gamal

$$Enc(m) = (g^r, m \cdot h^r)$$

$$Enc(m_1) \cdot Enc(m_2) = (g^{r_1} \cdot g^{r_2}, m_1 \cdot h^{r_1} \cdot m_2 \cdot h^{r_2})$$

$$Enc(m_1 \cdot m_2) = (g^{r_1 + r_2}, m_1 m_2 h^{r_1 + r_2})$$

FHE over the integers



- Gen: key is a "large" odd p
- Enc(b): $c = p \cdot q + 2r + b$

  where q is "large" and r is "small"
- Dec(c): $(c \bmod p) \bmod 2$

Homomorphic:

$(c_1 + c_2) \bmod p = 2 \cdot r_1 + 2 \cdot r_2 + b_1 + b_2$

$\Rightarrow \bmod 2 = b_1 + b_2$

$(c_1 \cdot c_2) \bmod p = b_1 \cdot b_2 \pmod 2$

Bootstrapping

"reduce the noise after a few homomorphic operations"