

CSCI 1515 Applied Cryptography

This Lecture:

- Private Set Intersection
- Introduction to Fully Homomorphic Encryption
- Somewhat Homomorphic Encryption over Integers

Private Set Intersection (PSI)

Alice



Input: $X = \{x_1, x_2, \dots, x_n\}$



Bob



Input: $Y = \{y_1, y_2, \dots, y_n\}$

$$\text{PSI: } f(X, Y) = X \cap Y$$

$$\text{PSI-CA: } f(X, Y) = |X \cap Y|$$

Applications:

- Password Breach Alert (Chrome, Edge, Firefox, iOS Keychain, ...)
- Ads Conversion Measurement (Google)
- Privacy-Preserving Inventory Matching (J.P. Morgan)
- Private Contact Discovery (Signal)

Private Set Intersection (PSI)

Alice



Input: $X = \{x_1, x_2, \dots, x_n\}$

$H(x_1), \dots, H(x_n)$ →

Bob



Input: $Y = \{y_1, y_2, \dots, y_n\}$

$H(y_1), \dots, H(y_n)$



$X \cap Y$

Is it (semi-honest) secure?

Is it possible to achieve ZPC / MPC with 1 round of communication?

DDH-based PSI

Cyclic group G of order q with generator g , where DDH holds.

$H: \{0,1\}^* \rightarrow G$ (modeled as Random Oracle)

Alice



Input: $X = \{x_1, x_2, \dots, x_n\}$

$$a \leftarrow \mathbb{Z}_q$$

$$\leftarrow H(Y)^b := \{H(y_1)^b, \dots, H(y_n)^b\}$$

$$\underline{H(Y)^{b \cdot a} := \{H(y_1)^{b \cdot a}, \dots, H(y_n)^{b \cdot a}\}}$$

$$\rightarrow H(X)^a := \{H(x_1)^a, \dots, H(x_n)^a\}$$

Bob



Input: $Y = \{y_1, y_2, \dots, y_n\}$

$$b \leftarrow \mathbb{Z}_q$$

$$H(Y)^{b \cdot a} \cap H(X)^{a \cdot b}$$



$$X \cap Y$$

Is it (semi-honest) secure?

PSI-CA?

$$\text{PSI-CA: } f(X, Y) = |X \cap Y|$$

Alice



Input: $X = \{x_1, x_2, \dots, x_n\}$

$$a \leftarrow \mathbb{Z}_q$$

$$\leftarrow H(Y)^b := \{H(y_1)^b, \dots, H(y_n)^b\}$$

$$\underline{H(Y)^{b \cdot a} := \{H(y_1)^{b \cdot a}, \dots, H(y_n)^{b \cdot a}\}}$$

$$\rightarrow H(X)^a := \{H(x_1)^a, \dots, H(x_n)^a\}$$

Bob



Input: $Y = \{y_1, y_2, \dots, y_n\}$

$$b \leftarrow \mathbb{Z}_q$$

$$H(Y)^{b \cdot a} \cap H(X)^{a \cdot b}$$



$$X \cap Y$$

Fully Homomorphic Encryption (FHE)

$$\begin{array}{l} \text{Enc}(m_1) \\ \text{Enc}(m_2) \end{array} \begin{array}{l} \searrow \\ \nearrow \end{array} \text{Enc}(m_1 + m_2)$$

Additively Homomorphic

↑
Exponential ElGamal / Paillier / Regev

$$\begin{array}{l} \text{Enc}(m_1) \\ \text{Enc}(m_2) \end{array} \begin{array}{l} \searrow \\ \nearrow \end{array} \text{Enc}(m_1 \cdot m_2)$$

Multiplicatively Homomorphic

↑
RSA / ElGamal

Fully Homomorphic: Additively & Multiplicatively Homomorphic

Homomorphic Evaluation:



Application: Outsourcing Storage & Computation

Server



Client



Data x

Key sk

$ct \leftarrow \text{Enc}(x)$

$\leftarrow ct$

$\leftarrow f$

$ct' \leftarrow \text{Eval}(f, ct)$

$\xrightarrow{ct'}$

$f(x) \leftarrow \text{Dec}_{sk}(ct')$

Application: Privacy-Preserving Query

Server



Client



Query x

Key sk

$ct \leftarrow \text{Enc}(x)$

ct ←

Search / ML / LLM / ...



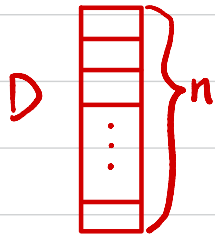
$ct' \leftarrow \text{Eval}(f, ct)$

→ ct'

$f(x) \leftarrow \text{Dec}_{sk}(ct')$

Application: Private Information Retrieval (PIR)

Server



Client



WANT: $D[i]$

While hiding i against Server

Query i

Key sk

$ct \leftarrow \text{Enc}(i)$

ct

$ct' \leftarrow \text{Eval}(f, ct)$

↑
?

ct'

$D[i] \leftarrow \text{Dec}_{sk}(ct')$

Fully Homomorphic Encryption (FHE)

- **Syntax:** A (public-key) homomorphic encryption scheme $\Pi = (\text{Gen}, \text{Enc}, \text{Dec}, \text{Eval})$ w.r.t. function family F :
 - $(pk, sk) \leftarrow \text{Gen}(1^\lambda)$
 - $ct \leftarrow \text{Enc}_{pk}(m) \quad m \in \{0, 1\}$
 - $m \leftarrow \text{Dec}_{sk}(ct)$
 - $ct_f \leftarrow \text{Eval}(f, ct_1, \dots, ct_n) \quad f: \{0, 1\}^n \rightarrow \{0, 1\}$
- **Correctness:** $\forall f \in F, \forall m_1, m_2, \dots, m_n \in \{0, 1\}$
 $\forall i \in [n], ct_i \leftarrow \text{Enc}_{pk}(m_i), \quad ct_f \leftarrow \text{Eval}(f, ct_1, \dots, ct_n)$
 $\text{Dec}_{sk}(ct_f) = f(m_1, \dots, m_n)$
- **(CPA) Security:** $(pk, \text{Enc}_{pk}(m_0)) \stackrel{c}{\approx} (pk, \text{Enc}_{pk}(m_1))$.
- **Compactness:** $|ct_f| \leq \text{fixed poly}(\lambda) \leftarrow \text{Why do we need this?}$
Independent of circuit size of f .
- If F contains **all** poly-sized Boolean circuits, then Π is **fully** homomorphic.

FHE Constructions

Step 1: Somewhat Homomorphic Encryption (SWHE)

- over Integers

- from RLWE (BFV)

Step 2: Bootstrapping

SWHE over Integers

Attempt 1 (Secret-key)

- secret key: odd number p ← Why odd?

- Enc(m): $m \in \{0, 1\}$

Sample a random q .

Output $ct = p \cdot q + m$

Encryption of 0 is a multiple of p .

- Dec(ct): $ct \bmod p$

- Eval ADD: $ct \leftarrow ct_1 + ct_2$

Eval MULT: $ct \leftarrow ct_1 \cdot ct_2$

Why is it homomorphic?

(CPA) Security?

SWHE over Integers

Attempt 2 (Secret-key)

- secret key: odd number p

- Enc(m): $m \in \{0, 1\}$

Sample a random q . Sample a random $e \ll p$ ^{noise}

Output $ct = p \cdot q + m + ze$

Encryption of 0 is small and even modulo p .

- Dec(ct): $[ct \bmod p] \bmod 2$

- Eval ADD: $ct \leftarrow ct_1 + ct_2$

Eval MULT: $ct \leftarrow ct_1 \cdot ct_2$

Why is it homomorphic?

(CPA) Security?

How homomorphic is it?

Approximate GCD Problem

Given polynomially many $\{x_i = p \cdot q_i + s_i\}$, find p .

Example parameters:

$$p \sim 2^{O(\lambda^2)}, \quad q_i \sim 2^{O(\lambda^5)}, \quad s_i \sim 2^{O(\lambda)}$$

Best known algorithms take $\sim 2^\lambda$ time

SWHE over Integers

Attempt 3 (public-key)

- secret key: odd number p

public key: "encryptions of 0" ← generic

$$\{x_i = p \cdot q_i + z e_i\}_{i \in [\lambda]}$$

- Enc(m): $m \in \{0, 1\}$

Sample a random $e \ll p$

Output $ct = (\text{random subset sum of } x_i\text{'s}) + m + ze$

Encryption of 0 is small and even modulo p .

- Dec(ct): $[ct \bmod p] \bmod 2$

- Eval ADD: $ct \leftarrow ct_1 + ct_2$

Eval MULT: $ct \leftarrow ct_1 \cdot ct_2$