

CSCI 1515 Applied Cryptography

This Lecture:

- PSI-Sum (Continued)
- Information Theoretic MPC (BGW)
- Introduction to FHE
- SWHE over Integers

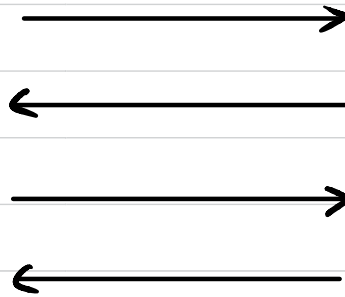
Private Set Intersection (PSI)

Alice



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

$V = \{v_1, v_2, \dots, v_n\}$



Bob



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

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

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

$$\text{PSI-SUM: } f((X, V), Y) = |X \cap Y|, \sum_{i: x_i \in Y} v_i$$

PSI-CA

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

Alice



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

$$k_A \xleftarrow{\$} \mathbb{Z}_q$$

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

$$\xrightarrow{H(X)^{k_A}, \{H(Y)^{k_A \cdot k_B}\}} \text{Shuffle}$$

Bob



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

$$k_B \xleftarrow{\$} \mathbb{Z}_q$$

$$H(X)^{k_A \cdot k_B} \cap H(Y)^{k_A \cdot k_B}$$

$$\downarrow \\ |X \cap Y|$$

PSI-SUM?

$$\text{PSI-SUM: } f((x, v), Y) = |x \cap Y|, \sum_{i: x_i \in Y} v_i$$

Alice



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

$$k_A \xleftarrow{\$} \mathbb{Z}_q$$

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

$$\xrightarrow{H(X)^{k_A}, \{H(Y)^{k_A \cdot k_B}\}} \text{Shuffle}$$

Bob



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

$$k_B \xleftarrow{\$} \mathbb{Z}_q$$

$$H(X)^{k_A \cdot k_B} \cap H(Y)^{k_A \cdot k_B}$$

$$\downarrow \\ |x \cap Y|$$

Feasibility Results

Computational Security:

Semi-honest Oblivious Transfer (OT)



semi-honest MPC for any function with $t < n$



malicious MPC for any function with $t < n$

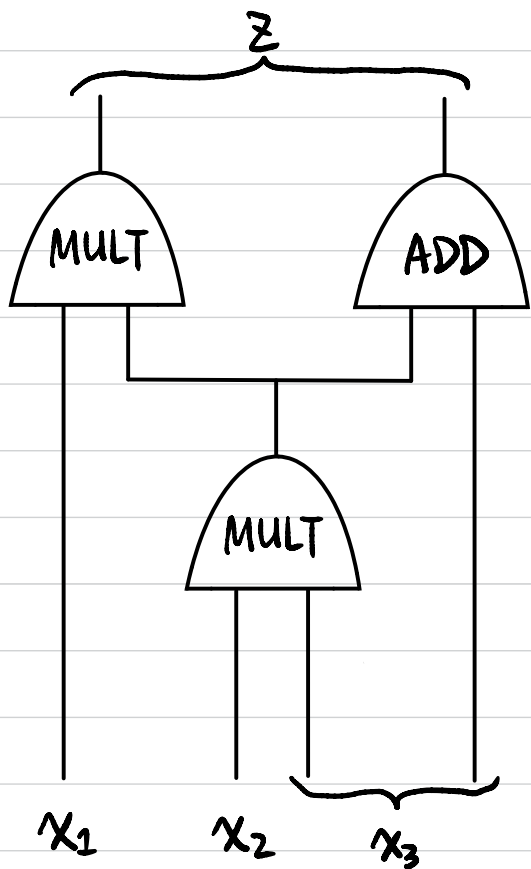
Information-Theoretic (IT) Security:

semi-honest/malicious MPC for any function with $t < n/2$

(honest majority)

↑
necessary

IT-MPC for any function with $t < n/2$ (BGW)



Throughout the protocol, we keep the invariant:

For each wire w :

If the value of the wire is $v^w \in \mathbb{F}$

the n parties hold a $(t+1)$ -out-of- n secret share of v^w

Each party P_i holds a random share $v_i^w \in \mathbb{F}$ s.t.

1) Any $(t+1)$ shares can jointly recover v^w

2) Any t shares information theoretically hide v^w

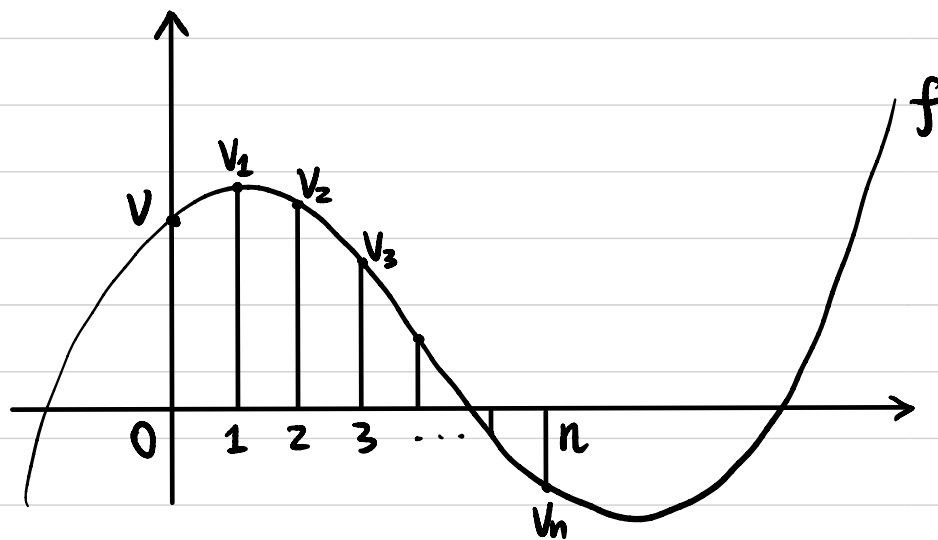
Shamir Secret Sharing Scheme

- Secret value $v \in \mathbb{F}$

- **Share**: ^{← How?} Sample a random degree- t polynomial $f: \mathbb{F} \rightarrow \mathbb{F}$ st. $f(0) = v$

$$f(x) = a_t x^t + a_{t-1} x^{t-1} + \dots + a_1 x + a_0$$

Party P_i 's share $v_i = f(i)$



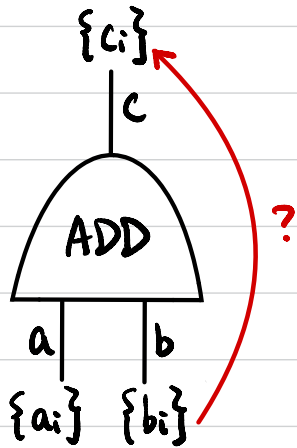
- **Reconstruct**:

Given $(t+1)$ shares: $(\alpha_1, v_{\alpha_1} = f(\alpha_1)), \dots, (\alpha_{t+1}, v_{\alpha_{t+1}} = f(\alpha_{t+1}))$

How to recover v ?

IT-MPC for any function with $t < n/2$ (BGW)

ADD gates:

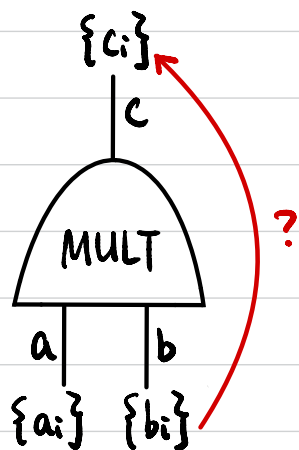


GIVEN: Deg- t poly $f_a(\cdot)$ s.t. $f_a(0) = a$. Shares $a_i = f_a(i)$
Deg- t poly $f_b(\cdot)$ s.t. $f_b(0) = b$. Shares $b_i = f_b(i)$

WANT: Deg- t poly $f_c(\cdot)$ s.t. $f_c(0) = a + b$. $f_c = ?$
Shares $c_i = f_c(i) = ?$

IT-MPC for any function with $t < n/2$ (BGW)

MULT gates:



GIVEN: Deg- t poly $f_a(\cdot)$ s.t. $f_a(0) = a$. Shares $a_i = f_a(i)$
Deg- t poly $f_b(\cdot)$ s.t. $f_b(0) = b$. Shares $b_i = f_b(i)$

WANT: Deg- t poly $f_c(\cdot)$ s.t. $f_c(0) = a \cdot b$. $f_c = ?$
Shares $c_i = f_c(i) = ?$

Attempt: $f_c = f_a \cdot f_b$
 $f_c(0) = f_a(0) \cdot f_b(0) = a \cdot b$
 $c_i = f_c(i) = f_a(i) \cdot f_b(i) = a_i \cdot b_i$

Problem?

Fully Homomorphic Encryption (FHE)

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

Additively Homomorphic

↑
Exponential ElGamal / Paillier

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

Multiplicatively Homomorphic

↑
RSA / ElGamal

Fully Homomorphic: Additively & Multiplicatively Homomorphic

Fully Homomorphic Encryption (FHE)

Def A (public-key) homomorphic encryption scheme

$\Pi = (\text{KeyGen}, \text{Enc}, \text{Dec}, \text{Eval})$ w.r.t. function family F :

- $(pk, sk) \leftarrow \text{KeyGen}(1^\lambda)$
- $ct \leftarrow \text{Enc}_{pk}(m) \quad m \in \{0, 1\}$
- $m \leftarrow \text{Dec}_{sk}(ct)$
- $ct_f \leftarrow \text{Eval}(f, ct_1, \dots, ct_n) \quad f: \{0, 1\}^n \rightarrow \{0, 1\}$

- **Correctness:** $ct_i \leftarrow \text{Enc}_{pk}(m_i) \quad \forall i \in [n]$,
 $\forall f \in F, \quad ct_f \leftarrow \text{Eval}(f, ct_1, \dots, ct_n)$
 $\text{Dec}_{sk}(ct_f) = f(m_1, \dots, m_n)$

- **(CPA) Security:** $(pk, \text{Enc}_{pk}(m_0)) \stackrel{c}{\cong} (pk, \text{Enc}_{pk}(m_1))$.

Missing Requirement?

Fully Homomorphic Encryption (FHE)

Def A (public-key) homomorphic encryption scheme

$\Pi = (\text{KeyGen}, \text{Enc}, \text{Dec}, \text{Eval})$ w.r.t. function family F :

- $(pk, sk) \leftarrow \text{KeyGen}(1^\lambda)$
- $ct \leftarrow \text{Enc}_{pk}(m) \quad m \in \{0, 1\}$
- $m \leftarrow \text{Dec}_{sk}(ct)$
- $ct_f \leftarrow \text{Eval}(f, ct_1, \dots, ct_n) \quad f: \{0, 1\}^n \rightarrow \{0, 1\}$

• So far, it's trivial to construct FHE under the definition.

$\text{Eval}(f, ct_1, \dots, ct_n) = ?$

• If F is the set of **all** poly-sized Boolean circuits, then Π is **fully** homomorphic.

Application: Outsourcing Storage & Computation

Server



Client



Data x

Key sk

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

$\leftarrow ct$

$\leftarrow f$

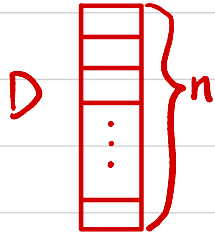
$ct' \leftarrow \text{Eval}(f, ct)$

$\xrightarrow{ct'}$

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

Application: Private Information Retrieval (PIR)

Server



Client



WANT: $D[i]$

While hiding i against Server

Application: Secure ZPC?

Alice



Input: x

$C(x, y)$

Bob



Input: y

Key sk

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

$\xleftarrow{ct}$

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

$\uparrow$
?

$\xrightarrow{ct'}$

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

FHE Constructions

Step 1: Somewhat Homomorphic Encryption (SWHE)

- over Integers
- from LWE (GSW)
- 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: $ct \leftarrow ct_1 \cdot ct_2$

(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 $e \ll p$

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: $ct \leftarrow ct_1 \cdot ct_2$

• Approximate GCD Problem:

Given poly-many $\{x_i = p \cdot q_i + s_i\}$, output p .

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

Best known attacks require 2^λ time.

SWHE over Integers

Attempt 3 (public-key)

- secret key: odd number p

public key: "encryptions of 0"

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

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

Sample a random $e \leftarrow p$

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: $ct \leftarrow ct_1 \cdot ct_2$

How homomorphic is it?