CS 65500
Advanced Cryptography

Lecture 22: MPC from Homomorphic Encryption

Instructor: Aarushi Goel

Spring 2025

Agenda

→ Public-Key Encryption

→ Decisional Diffie-Hellman Assumption

→ El Gamal Encryption

→ Threshold Encryption

→ Homomorphic Encryption

→ MPC from homomorphic encryption.

Public-Key Encryption

Syntax:

* $Gen(1^\lambda) \rightarrow sk, pk$
* $Enc(pk, m; r) \rightarrow c$
* $Dec(sk, c) \rightarrow m'$ or $\perp$

All of these are PPT algorithms

Correctness:

Let $(sk, pk) \leftarrow Gen(1^\lambda)$, $\forall m, r$, it holds that:

$$\Pr[Dec(sk, Enc(pk, m; r)) = m] \geq 1 - negl(\lambda)$$

Security:

Indistinguishability based (IND-CPA) $\equiv$ semantic security

+ correctness

Defining IND-CPA Security

indistinguishability — chosen plaintext attack.

Definition: A public key encryption scheme (Gen, Enc, Dec) is IND-CPA secure if $\forall$ n.u. PPT adversaries A, there exists a negligible function $negl(\cdot)$, s.t.,

$$\Pr\left[A(pk, Enc(pk, m_b; r)) = b \;\middle|\; \begin{array}{l} (pk, sk) \leftarrow Gen(1^\lambda), \\ r \xleftarrow{\$} \{0,1\}^*, \\ (m_0, m_1) \leftarrow A(pk, 1^\lambda), \\ b \xleftarrow{\$} \{0,1\} \end{array} \right] \leq \frac{1}{2} + negl(\lambda)$$

* One message security implies multi-messge security for public key enc

Decisional Diffie-Hellman Assumption

→ Given g^x, g^y for random x, y, g^{xy} should be *hidden*
ie., could still be used as a pseudorandom element

$$\Rightarrow (g^x, g^y, g^{xy}) \approx_c (g^x, g^y, g^R)$$

(i.e $p = 2q+1$ for some large prime q)

Definition: Let $(G, \cdot)$ be a cyclic group of order p (where p is a safe prime) with generator g, then the following two distributions are computationally indistinguishable:

* $\{x, y \xleftarrow{\$} \{0, \ldots, p-1\} : (G, p, g, g^x, g^y, g^{xy})\}$

* $\{x, y, R \xleftarrow{\$} \{0, \ldots, p-1\} : (G, p, g, g^x, g^y, g^R)\}$

Diffie-Hellman Key-Exchange

Sample random x

$X = g^x$

$\xrightarrow{X}$

Sample random y

$Y = g^y$

$\xleftarrow{Y}$

Output Y^x

Output X^y

* The final key $Y^x = X^y = g^{xy}$ remains hidden from an evesdropper if the DDH assumption holds.

El Gamal Encryption

* $Gen(1^\lambda) \rightarrow$ Sample a cyclic group G with generator g of order p.
  Sample $y \xleftarrow{\$} \{0, \ldots, p-1\}$. Let $Y = g^y$
  $pk = (G, g, Y)$, $sk = (G, g, y)$

* $Enc(pk, m) \rightarrow$ Parse $pk = (G, g, Y)$
  Sample $r \xleftarrow{\$} \{0, \ldots, p-1\}$
  $c = (R = g^r, X = g^m Y^r)$

* $Dec(sk, c) \rightarrow$ Parse $sk = (G, g, y)$, $c = (R, X)$
  $M = X \cdot R^{-y}$, for all possible messages, check
  if $g^m = M$. Output the corresponding m.

* decryption is efficient only for small message domains.

Security of El Gamal

* El Gamal encryption is secure if DDH holds.

Proof by Reduction:

Ch_{DDH}

$\alpha \xleftarrow{\$} \{0,1\}$

if $\alpha = 0$

$Z = (G, g, p, g^x, g^y, R = g^{xy})$

else:

$Z = (G, g, p, g^x, g^y, R = g^r)$

$Ch_{DDH} \xrightarrow{Z} B_{DDH}$

$B_{DDH} \xrightarrow{\alpha'} Ch_{DDH}$

B_{DDH}

Parse $Z = (G, g, p, g^x, g^y, R)$

$PK = (G, g, g^y)$

$B_{DDH} \xrightarrow{PK} A_{El\text{-}Gamal}$

$A_{El\text{-}Gamal} \xrightarrow{(m_0, m_1)} B_{DDH}$

$b \xleftarrow{\$} \{0,1\}$

$B_{DDH} \xrightarrow{(g^x,\ g^{m_b} \cdot R)} A_{El\text{-}Gamal}$

$A_{El\text{-}Gamal} \xrightarrow{b'} B_{DDH}$

if $b = b'$: $\alpha' = 0$

else : $\alpha' = 1$

$A_{El\text{-}Gamal}$

Threshold El Gamal (Semi-Honest Secure)

* Goal: Enable n-parties to generate a PK for El Gamal in such a way that SK is secret shared among them. Decryption of a ciphertext should only be possible if all n parties come together. For now we only focus on semi-honest corruption.

* **Distributed Key Generation:**

1. Party 1 samples (G, g). Let G be of order p.
2. Each party i samples a random y_i and sends $Y = g^{y_i}$ to all parties.
3. All parties compute $Y = \prod Y_i$. $PK = (G, g, Y)$
4. Implicit $SK = (G, g, \sum y_i)$.

* **Encryption:** Exactly as in El Gamal.

* **Distributed Decryption:** Given a ciphertext (R, X), each party i, publishes $K_i^{-1} = R^{-y_i}$. All parties compute $K^{-1} = \prod K_i^{-1}$ & $M = X \cdot K^{-1}$.

Homomorphic Encryption

* Group Homomorphism: Two groups G and G' are homomorphic if there exists a function (homomorphism) $f: G \to G'$, such that $\forall x, y \in G$,
$f(x) +_{G'} f(y) = f(x +_G y)$

* Homomorphic Encryption: An IND-CPA secure public-key encryption is said to be homomorphic for any ciphertexts C, D, it holds that:
$$\Pr[\mathrm{Dec}(C) \underbrace{+_M}_{\text{addition over msg domain}} \mathrm{Dec}(D) = \mathrm{Dec}(C \underbrace{+_c}_{\text{add over ciphertext space.}} D)] \geq 1 - \mathrm{negl}(\lambda)$$

→ Interesting when $+_c$ does not require secret key

eg ElGamal: $(g^{r_1}, g^{m_1} \cdot y^{r_1}) \times (g^{r_2}, g^{m_2} \cdot y^{r_2}) = (g^{r}, g^{m_1+m_2} \cdot y^{r})$

MPC from Homomorphic Encryption

→ Recall in the GMW protocol, parties collectively evaluate the circuit on secret shared values using pair-wise OTs.

→ An alternate approach (avoids pairwise communication) : each wire value is kept encrypted (publicly) and the secret key is kept secret shared.

* Input - Sharing Phase: All parties encrypt their inputs and publish

* Circuit - Evaluation Phase: Each gate in the circuit is evaluated over encrypted values using homomorphism — HOW??

* Output Reconstruction Phase: Parties decrypt the output wires using threshold decryption.

→ Proposed by Ronald Cramer, Ivan Damgard & Jesper Nielson in 2001

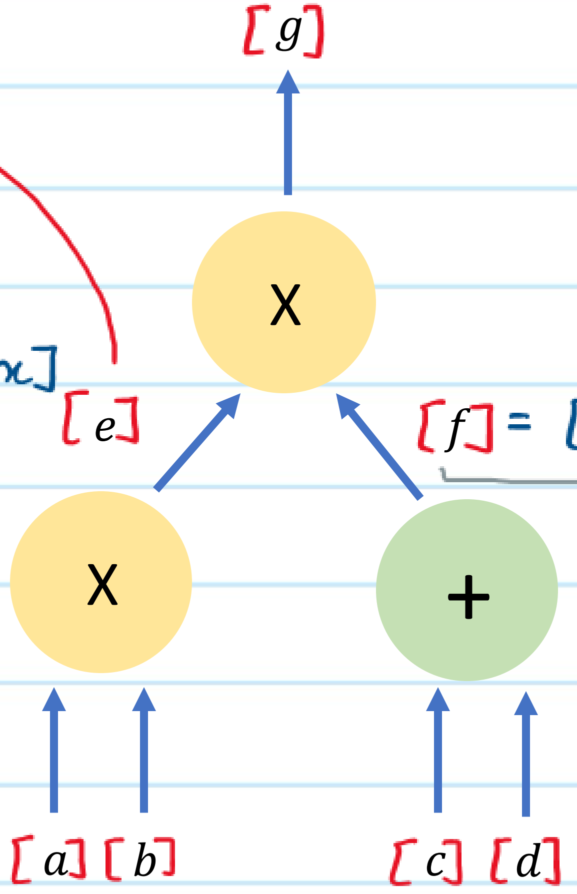
Circuit Evaluation Phase

generated using distributed keygen

→ Let's use $[m]$ to denote $\mathrm{Enc}(pk, m)$

Multiplication:

1. Each party i picks a random x_i, y_i and publishes $[x_i], [y_i], [x_i \cdot b], [y_i \cdot a]$.
2. All parties compute $[x+a], [y+b], [ay], [bx]$ where $x = \sum x_i$, $y = \sum y_i$
3. Each party publishes $[x_i \cdot y] = x_i \cdot [y]$.
4. All parties compute $[xy]$
5. Parties threshold decrypt $(x+a), (y+b)$. and compute $z = (x+a)(y+b)$
6. All parties compute $[a \cdot b] = [z] - [ay] - [bx] - [xy] = [e]$



$[f] = \underbrace{[c] + [d]}_{\text{Easy to compute}}$