4 Computing on Encrypted Data

- Definition
- Applications
  - Privacy preserving computations
  - Delegation
  - Secure multi-party computation w. minimal communication.

- Construction

Fully Homomorphic Encryption

A notion suggested by [Rivest-Adleman-Dertouzos 78]

$Enc(PK, b_1)$, $Enc(PK, b_2)$

$\downarrow$

$Enc(PK, b_1 + b_2)$, $Enc(PK, b_1 \cdot b_2)$

First construction: [Gentry 2009]

Applications:

- Private delegation:

  A user can delegate all her private data to the cloud, by using FHE.
  The cloud can perform computations on the encrypted data, blindly, without learning any information.

- Secure computation w. minimal communication

- Verifiable computations.

⋮

Construction [Gentry-Sahai-Waters]

Uses Lattice-based cryptography

Assumption: Learning with Error

It is hard to solve noisy linear equations.

Namely: For random $A \leftarrow \mathbb{Z}_q^n$, $a_1, \ldots, a_m \leftarrow \mathbb{Z}_q^m$ ($m >> n$)

Given $a_1, A \cdot a_1 + e_1$

$a_2, A \cdot a_2 + e_2$ $\xrightarrow{\text{hard}}$ A

$\vdots$

$a_m, A \cdot a_m + e_m$

Decisional version:

$$\begin{matrix} a_1, & A a_1 + e_1 \\ \vdots & \\ a_m, & A a_m + e_m \end{matrix} \quad \approx \quad \begin{matrix} a_1, & u_1 \\ \vdots & \\ a_m, & u_m \end{matrix}$$

- We do not know how to break this assumption with quantum attacks! (as opposed to Factoring & DL)

- No sub-exp alg known.
- Reduces to worst-case hardness assumption on lattices.

The scheme

KeyGen: $PK = \begin{cases} A = (a_1 \mid \cdots \mid a_m) \leftarrow \mathbb{Z}_q^{k \times m} & q - \text{large prime} \\ sA + e & - m \text{ noise linear eqns.} \end{cases}$

Let $B = \begin{bmatrix} A \\ sA+e \end{bmatrix}$

$SK = s \leftarrow \mathbb{Z}_q^k$

$t = (-s, 1) \in \mathbb{Z}_q^{\frac{n}{k+1}}$ s.t. $t \cdot B \approx 0$

Encrypt (b):

Uses fixed (eff. computable) matrix $G \in \mathbb{Z}_q^{n \times m}$

efficiently computable function $G^{-1}: \mathbb{Z}_q^{n \times m} \to \mathbb{Z}_q^{m \times m}$

s.t. $G^{-1}(M) \in \{0,1\}^{m \times m}$ & $G \cdot \underbrace{G^{-1}(M)}_{\text{bit decomposition}} = M$

$Enc(b)$: $BR + bG$ $\quad R \leftarrow \{0,1\}^{m \times m}$

$Dec(t, C)$: Compute $t \cdot C$. if $t \cdot C \approx 0$ then output $b=0$.

Otherwise output $b=1$.

Semantic security: Follows from the LWE assumption: $B \cong U$

If B was uniform then BR would be truly random (given B), and thus $BR+bG$ would hide b information theoretically.

Homomorphic Operations:

$$C_1 = BR_1 + b_1 G$$

$$C_2 = BR_2 + b_2 G$$

$$C^+ = C_1 + C_2 = B\underbrace{(R_1+R_2)}_{\text{small}} + (b_1+b_2)G$$

$$C^\times = C_1 \cdot G^{-1}(C_2) = B\left(R_1 G^{-1}(C_2)\right) + b_1 C_2$$

$$= B\left(R_1 G^{-1}(C_2) + b_1 R_2\right) + b_1 b_2 G$$