Fully Homomorphic Encryption & Post quantum cryptography

Today: - Post quantum cryptography
  - LWE assumption
- Fully homomorphic encryption (FHE)
  - Definition
  - Applications
  - Construction

Post Quantum Cryptography

All the computational assumptions we have seen so far can be broken with a quantum computer.
Including: RSA, Discrete log in $\mathbb{Z}_p^*$ & in Elliptic curves.

Will modern crypto die with the birth of quantum computers?
Hopefully not...
There are assumptions that are believed to resist quantum attacks, and we know how to build crypto from such assumptions.

Learning With Error (LWE) Assumption

"Lattice-based" assumption, introduced by Regev 2004

LWE Assumption: It is hard to solve noisy linear equations.

Namely: For paramaters q, n, m $\begin{bmatrix} q \text{ prime} \\ m >> n \end{bmatrix}$, & error distribution χ_q

for random $s \leftarrow \mathbb{Z}_q^n$

random $a_1, \ldots, a_m \leftarrow \mathbb{Z}_q^n$

$e_1, \ldots, e_m \leftarrow \chi_q$ — error distribution

Given

$$\begin{matrix} a_1, & s \cdot a_1 + e_1 \\ a_2, & s \cdot a_2 + e_2 \\ \vdots & \\ a_m, & s \cdot a_m + e_m \end{matrix} \xrightarrow{\text{hard}} s$$

Decisional LWE

$$\begin{matrix} a_1, & s a_1 + e_1 \\ \vdots & \\ a_m, & s a_m + e_m \end{matrix} \cong \begin{matrix} a_1, & u_1 \\ \vdots & \\ a_m, & u_m \end{matrix} \qquad (u_1, \ldots, u_m) \leftarrow \mathbb{Z}_q^m$$

Matrix notation: $(A, sA + E) \cong (A, U)$ $\quad A \leftarrow \mathbb{Z}_q^{n \times m}$, $s \leftarrow \mathbb{Z}_q^n$, $u \leftarrow \mathbb{Z}_q^m$, $E \leftarrow \chi_q^{n \times m}$

We do not know how to break this assumption with quantum computers (as opposed to Factoring & DL).

* No known sub-exp. alg! Also, reduces to worst-case lattice assumption!

We can construct public key encryption, digital signatures, collision resistant hash functions, identity-base encryption, ... from Decisional LWE.

- Not used in practice because less efficient & because we do not have quantum computers.

- Recently, NIST solicited proposals for quantum resilient public key cryptographic alg.

April 11-13 2018: First Post-Quantum Cryptography Standardization Conference.

Today: Fully Homomorphic Encryption (FHE) from DLWE

A notion suggested by Rivest-Adleman-Dertouzos 78.

$$\mathrm{Enc}(pk, b_1), \quad \mathrm{Enc}(pk, b_2)$$

$$\downarrow$$

$$\mathrm{Enc}(pk, b_1+b_2), \quad \mathrm{Enc}(pk, b_1 \cdot b_2)$$

First construction: Genty 2009.

Brakerski-Vaikuntanathan 2011: From DLWE

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 computation

  ⋮

Construction [Gentry-Sahai-Wichs 2013]

KeyGen (1^n) : $A \leftarrow \mathbb{Z}_q^{(n-1)\times m}$ $\quad$ q - prime can be of size poly(n).
$m = O(n \cdot \log q)$

$$s \leftarrow \mathbb{Z}_q^n$$

$$PK = B = \begin{pmatrix} A \\ sA + e \end{pmatrix} \qquad e \leftarrow \chi_q^m$$

$$SK = t = (-s, 1) \in \mathbb{Z}_q^n$$

Note:

$$t \cdot B \approx 0$$

Encrypt(b):

$N = n\cdot(\lfloor \log q \rfloor + 1)$

Uses "gadget" matrix $G \in \mathbb{Z}_q^{n\times N}$ s.t. $\exists$ eff. computable function $G^{-1}: \mathbb{Z}_q^{n\times N} \longrightarrow \{0,1\}^{N\times N}$

s.t. $\forall M \in \mathbb{Z}_q^{n\times N}$ $\quad G\left(G^{-1}(M)\right) = M$

$$G = n\underbrace{\begin{pmatrix} 1 \; 2 \; \cdots \; 2^{\lfloor \log q \rfloor} & & \\ & \ddots & \\ & & 1 \; 2 \; \cdots \; 2^{\lfloor \log q \rfloor} \end{pmatrix}}_{N}$$

G^{-1} = bit decomposition function.

$$\text{Enc}(b): \underset{\substack{\rotatebox{90}{$\in$} \\ \mathbb{Z}_q^{n\times m}}}{\overset{\substack{PK \\ \|}}{B}} \cdot R + bG \quad \in \mathbb{Z}_q^{n\times N}$$

$R \leftarrow \{0,1\}^{m\times N}$

$$\text{Dec}(\underset{\substack{\| \\ (-\Delta,1)}}{t}, C): \quad \text{Compute } \underset{\mathbb{Z}_q^{1\times n}}{t}\cdot \underset{\mathbb{Z}_q^{n\times N}}{C}.$$

If $t\cdot C \approx 0$ then output $b=0$

O.w. output $b=1$.

Correctness: $t\,(BR + bG) = \overbrace{(tB)\cdot R}^{\approx 0} + b\,\overbrace{tG}^{\text{large}}$

Semantic Security: Follows from DLWE assumption:

$$B \cong U$$

If B was uniform $B \leftarrow \mathbb{Z}_q^{n \times m}$ then $B \cdot R$ for $R \leftarrow \{0,1\}^{m \times N}$ would have been truly random (given B)

[Follows from left-over hash lemma & from the fact that $n \log q < m$.]

Thus, $BR + bG$ would hide b information theoretically.

Homomorphic Operations:

$$C_1 = BR_1 + b_1 G$$

$$C_2 = BR_2 + b_2 G$$

$$C^+ = C_1 + C_2 = B\underbrace{(R_1 + R_2)}_{\text{small}} + \underbrace{(b_1 + b_2)}_{\substack{\text{addition}\\ \text{in } \mathbb{Z}_q}} G$$

$$C^\times = \underset{\in \mathbb{Z}_q^{n \times N}}{C_1} \cdot \underset{\in \mathbb{Z}_q^{N \times N}}{G^{-1}(C_2)} = B\left(R_1 \cdot G^{-1}(C_2)\right) + b_1 G \cdot G^{-1}(C_2)$$

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

$$= B \cdot \left(R_1 G^{-1}(C_2)\right) + b_1 BR_2 + b_1 b_2 G$$

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