Lecture 8

Sunday, September 29, 2024 6:47 PM

Somewhat Homomorphic Encryption

- We want to develop a HE scheme that supports arbitrary # & operatio
- One famous SHE in BGN (Boneh - Goh - Nissim) that suppor
  - Any number of addition
  - ONE multiplication

Bilinear Groups

Let

1. $\mathbb{G}$ and $\mathbb{G}_1$ are the (multiplicative) cyclic groups of finite order n
2. g is the gerator of $\mathbb{G}$
3. e is a bilinear map $e: \mathbb{G} \times \mathbb{G} \to \mathbb{G}_1$ s.t. $\forall\, u, v \in \mathbb{G}$ and $a, b \in \mathbb{Z}$ we have $e(u^a, v^b) = e(u,v)^{ab}$. We also require that $e(g,g)$ is the generator of $\mathbb{G}_1$

We say that $\mathbb{G}$ is a bilinear group if $\exists$ a group $\mathbb{G}_1$ and e satisfying the above.

- There is a practical way to construct such e

BGN public key

KeyGen:

1. Given a security parameter $\tau \in \mathbb{Z}^+$, run algorithm $\mathcal{G}(\tau)$ and outputs $(q_1, q_2, \mathbb{G}, \mathbb{G}_1, e)$ where $\mathbb{G}, \mathbb{G}_1$ are groups of order $n = q_1 q_2$, and $e: \mathbb{G} \times \mathbb{G} \to \mathbb{G}_1$
2. Pick two random generators $g, u \xleftarrow{R} \mathbb{G}$ (sampling at random) and set $h = u^{q_2}$ (h is a random generator of the subgroup $\mathbb{G}$ of order q_1)
3. The public key is $(n, \mathbb{G}, \mathbb{G}_1, e, g, h)$
   The private key is q_1

Encrypt

1. We assume that the message space is the set $\{0, 1, \dots, T\}$ and $T < q_2$ $(T = 1)$

1- We assume that the message space in the set $\{0, 1, \ldots, T\}$ and $T < q_2$ $(T=1)$

2- To encrypt a message m, pick a random $r \xleftarrow{R} \{0, 1, \ldots, n-1\}$

$$C = g^m h^r \in G$$

Decrypt

1- To decrypt C, use $Sk = q_1$

$$C^{q_1} = (g^m h^r)^{q_1} = (g^{q_1})^m \qquad h = u^{q_2} \longrightarrow \left(u^{r \cdot q_2}\right)^{q_1} = \left(u^{\cancel{q_1 q_2}}\right)^r = 1^r$$

Using discrete log

$$m = \log_{g^{q_1}} C^{q_1}$$

Homomorplic Properties

1. Addition

$$C_1 = g^{m_1} h^{r_1}, \quad C_2 = g^{m_2} h^{r_2}$$

$$C_1 \times C_2 = g^{m_1+m_2} h^{r_1+r_2}$$

2- Multiplication

1. Set $\underbrace{g_1 = e(g, g)}_{\text{order of } n}$ and $\underbrace{h_1 = e(g, h)}_{\text{order of } q_1}$

2- $h = g^{\alpha q_2}$ for some (known) $\alpha \in \mathbb{Z}$

3- Given two ciphertexts $c_1 = g^{m_1} h^{r_1}$ and $c_2 = g^{m_2} h^{r_2}$

4- Pick a random $r \in \mathbb{Z}_n$ and set $C = e(c_1, c_2) h_1^r \in G_1$

$$C = e(c_1, c_2) h_1^r = e(g^{m_1} h^{r_1}, g^{m_2} h^{r_2}) h_1^r$$

$$= g_1^{m_1 m_2} h_1^{m_1 r_2 + r_2 m_1 + \alpha q_2 r_2 r_1 + r = \tilde{r}}$$

$$= g_1^{m_1 m_2} \underline{h_1^{\tilde{r}}} \in G_1$$

q_1: How to get rid of this?

q_2: When can you perform the multi. operation the..?

FHE

Bootstrapping