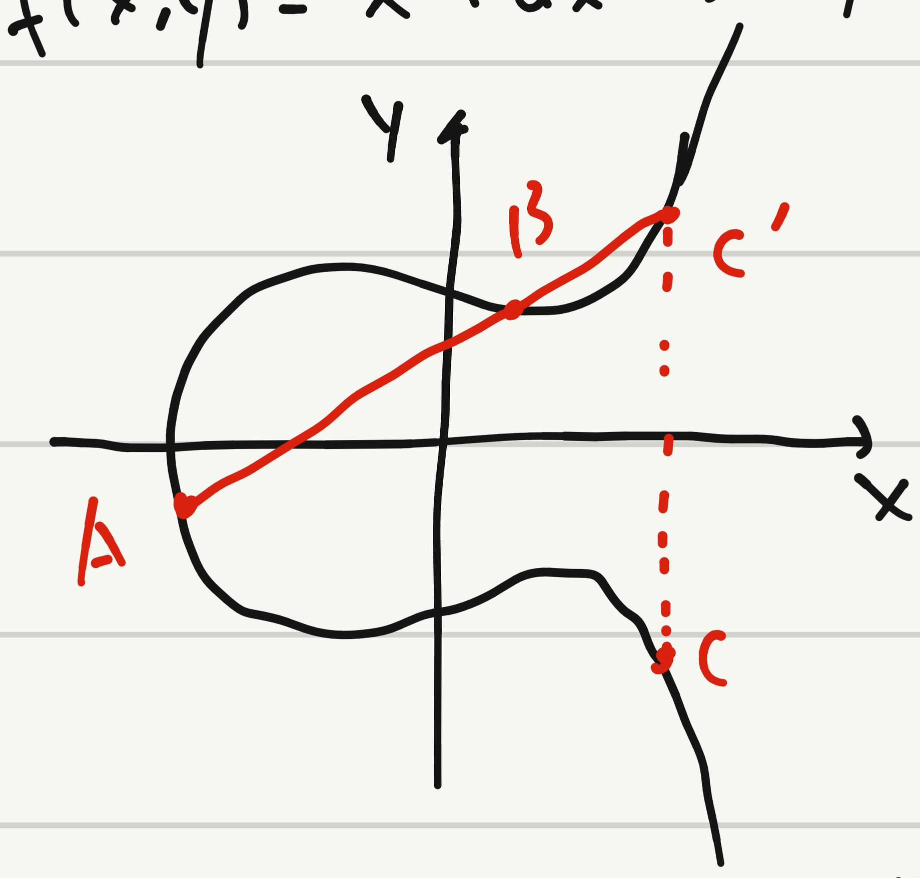
Generic Group Model

只以 Oracle 的方式提供G的信息.

即提供接口可以访问 e, g, 计算逆, 乘法等

接近通用群的构造：椭圆曲线

$f(x,y)=x^3+ax+b-y^2=0$



数学上群元素定义为 $\{(x,y)\in\mathbb{Q}^2 \mid f(x,y)=0\}\cup\{0\}$

0代表无穷远点.

乘法定义为 过A,B作直线与 $f=0$ 交于C'

$A+B=$ C' 关于x轴对称点C.

密码学中通常用 $\mathbb{F}_p^2$ 代替 $\mathbb{Q}^2$

Bilinear Map

$Gen(1^\lambda)\to(p,g,G,g_T,G_T,e:G\times G\to G_T)$, $G\cong G_T\cong \mathbb{Z}_p$.

生成两个椭圆曲线群E, E_T 的子群 G, G_T.

以及一个"双线性"函数 e s.t. $e(g^x,g^y)=g_T^{xy}$.

Decisional Bilinear Diffie-Hellman (DBDH)

$(p,g,G,g_T,G_T,g^x,g^y,g^z,g^{xyz})\approx_c(p,g,G,g_T,G_T,g^x,g^y,g^z,g^w)$

Identity-Based Encryption (IBE)

$\Pi=(Gen, IDKeyGen, Enc, Dec)$ master secret key

可信第三方 $Gen(1^\lambda)\to(pk, msk)$

认证 Alice 身份后提供 $IDKeyGen(msk,\text{"A"})\to sk_A$.

Bob 用 pk 加密 $Enc(pk,\text{"A"},m)\to c$

Alice 解密 $Dec(sk_A, c)\to m$.

安全性. Eve 可以访问一些 $\{ID_i\}$

在 $ID\notin\{ID_i\}$ 时, 至多以 $1/2+negl$ 区分两条信息.

用 Bilinear Map 实现 IBE.

Gen(1^λ): pk: $p, g, G, g_T, G_T, e, g^s, H:\{0,1\}^* \to G$.

msk: s

IDKeyGen(ID, msk): $h_{ID} = H(ID)$

$sk_{ID} = h_{ID}^s$

Enc(pk, ID, m): $\begin{cases} g^r \\ c = e(h_{ID}, g^s)^r \oplus m. \end{cases}$

Dec(sk_{ID}, (g^r, c)): $m = e(sk_{ID}, g^r) \oplus c$

Lattice-Based Cryptography

$L \subseteq \mathbb{R}^n$ 类似于 $\mathbb{R}^n$ 的 $\mathbb{Z}$-子空间.

由一组 $\mathbb{R}$ 上线性无关的基 $\vec{v_1}, \vec{v_2}, \cdots, \vec{v_n}$ 张成

$L = \{ a_1\vec{v_1} + a_2\vec{v_2} + \cdots + a_n\vec{v_n} \mid a_1, a_2, \cdots, a_n \in \mathbb{Z} \}$.

Shortest Vector Problem 给定 $B = [v_1\ v_2 \cdots v_n]$ 求 L 中最短非 0 向量

Closest Vector Problem 给定 B 及一点 t, 求离 t 最近 L 中向量.

Learning with Error (LWE).

给定 A 与 $y = A\vec{x} + \overrightarrow{err} \pmod q$. 求 x.

这其实就是 Closest Vector Prob. $\overrightarrow{err} \sim$ Gaussian($\sigma = \sqrt{q}$)

LWE-based Private-Key Encryption

令 $sk = \vec{s} \in \mathbb{Z}_q^n$.

Enc(sk, m): uniform sample $\vec{a_i}$, sample err

返回 $(\vec{a}, c = \langle \vec{a}, \vec{s} \rangle + err + m[\frac{q}{2}])$

Dec(sk, ($\vec{a}$, c)): $c - \langle \vec{a}, \vec{s} \rangle = m[\frac{q}{2}] + err$.

令 $|err| < \frac{q}{4}$ 可以传递 1 bit 的 m.

LWE-based Public-key Encryption.

用0的若干个 privat-key 加密 当作公钥

$$pk \begin{cases} \vec{a}_1, & \langle \vec{a}_1, \vec{s} \rangle + e_1 = b_1 \\ \vec{a}_2, & \langle \vec{a}_2, \vec{s} \rangle + e_2 = b_2 \\ \vdots & \\ \vec{a}_m, & \langle \vec{a}_m, \vec{s} \rangle + e_m = b_m. \end{cases}$$

Enc: sample $c_1, c_2, \cdots, c_m \leftarrow \{0,1\}$

$$c = (\underbrace{\textstyle\sum c_i \vec{a}_i}_{\vec{a}^*}, \underbrace{\textstyle\sum c_i b_i}_{= \langle \vec{a}^*, \vec{s} \rangle + \sum e_i} + err)$$

$$= \langle \vec{a}^*, \vec{s} \rangle + \sum e_i + err$$

取 $m > n\log q$, err 远大于 $\sum e_i$

使 $(\vec{a}^*, \langle \vec{a}^*, \vec{s} \rangle + err)$ 统计意义上 $\approx_s$ 均匀分布

Homomorphic Encryption

加密是同态.

LWE: $Enc(m_1) + Enc(m_2) = Enc(m_1 + m_2)$

Robin: $Enc(b_1) \cdot Enc(b_2) = Enc(b_1 \oplus b_2)$

Fully Homomorphic Encryption (FHE). 对加和乘都有同态.

考虑LWE乘法

$$Enc(m) \quad \begin{bmatrix} A \\ SA + e_1 \end{bmatrix} + m_1 \cdot I. \qquad \begin{bmatrix} B \\ SB + e_2 \end{bmatrix} + m_2 \cdot I.$$

$$Dec: \begin{bmatrix} -s & 1 \end{bmatrix} \left(\begin{bmatrix} A \\ SA + e_1 \end{bmatrix} \begin{bmatrix} B \\ SB + e_2 \end{bmatrix} + \begin{bmatrix} A \\ SA + e_1 \end{bmatrix} m_2 + \begin{bmatrix} B \\ SB + e_2 \end{bmatrix} m_1 + m_1 m_2 \right)$$

$$= \begin{bmatrix} e_1 \end{bmatrix} \begin{bmatrix} B \\ SB + e_2 \end{bmatrix} + \begin{bmatrix} e_1 \end{bmatrix} m_2 + \begin{bmatrix} e_2 \end{bmatrix} m_1 + \begin{bmatrix} -s & 1 \end{bmatrix} m_1 m_2$$

噪声太大. 需要解决.

考虑矩阵 $G = \begin{bmatrix} 1\ 2\ 4\ 8 \cdots & & & 0 \\ & 1\ 2\ 4\ 8 \cdots & & \\ & & 1\ 2\ 4\ 8 \cdots & \\ 0 & & & \ddots \end{bmatrix} \in M_{n\times\lceil \log q\rceil}$

存在函数 G^{-1} 使 $M = G\cdot G^{-1}(M)$. 且 $G^{-1}(M)$ 为 01 阵. (二进制)

Enc(m) $\begin{bmatrix} A \\ \hline SA+e_1 \end{bmatrix} + m_1 G$ $\quad \begin{bmatrix} B \\ \hline SB+e_2 \end{bmatrix} + m_2\cdot G$

Dec: $C_1 \cdot G^{-1}(C_2) = \begin{bmatrix} A \\ \hline \ \end{bmatrix} G^{-1}(c_2) + m_1 G\cdot G^{-1}(c_2)$

$= \underbrace{\begin{bmatrix} A \\ \hline \ \end{bmatrix} G^{-1}(c_2) + \begin{bmatrix} B \\ \hline \ \end{bmatrix} m_1}_{\begin{bmatrix} D \\ \hline SD+e \end{bmatrix}} + m_1 m_2 G.$

← 由于 $G^{-1}(c_2)$ 与 m_1 都小

∴ 乘上 $\begin{bmatrix} -s & 1 \end{bmatrix}$ 后较小.

又 $m_1 \oplus m_2 = m_1 + m_2 - 2m_1m_2$

又不考虑 $m\in\{0,1\}$ 的话加法自然成立.

∴ 以上对 $\oplus$ 与 $\times$ 几乎是同态.

Somewhat HE
Circular Security } ⇒ FHE

C_{key} ↓

高噪声 C_m → Bootstrap → 低噪声 C_m

由 Circular. 有

key
↓
input: key
output: Dec(key, C_m)
↓
m

存在.

由 SHE 输入换为 Enc(key) 后输出变为 Enc(m).

密文肮脏程度只与上面模块有关

与输入 C_m 无关.