Regev's cryptosystem $\mathbb{Z}_{11}$ $[0,1,2,3,4,5,6,7,8,9,10]$
$[0,1,2,3,4,5,-5,-4,-3,-2,-1]$

Key Generation:

$S \leftarrow \mathbb{Z}_{11}^{2}$
$S = \begin{pmatrix} 1 & -4 \end{pmatrix}^T$

$e \leftarrow \chi$
$e = (0,1,0)^T$

$P_r\left[\,|x \cdot e| \geq \frac{q}{4} : x \xleftarrow{\$} \{0,1\}^m\right]$ is small

$A = \begin{pmatrix} 2 & 4 \\ 0 & 5 \\ 3 & 0 \end{pmatrix}$ $b = As + e$

$b = \underbrace{\begin{pmatrix} 2 & 4 \\ 0 & 5 \\ 3 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ -4 \end{pmatrix}}_{As} + \underbrace{\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}}_{e} = \begin{pmatrix} 2-16 \\ -20 \\ 3 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} -3 \\ 3 \\ 3 \end{pmatrix}$

$sk := \begin{pmatrix} 1 \\ -4 \end{pmatrix}$

$pk := \left(\begin{pmatrix} 2 & 4 \\ 0 & 5 \\ 3 & 0 \end{pmatrix}, \begin{pmatrix} -3 \\ 3 \\ 3 \end{pmatrix}\right)$

$Enc(pk, M)$ $Enc\left(\left(\begin{pmatrix} 2 & 4 \\ 0 & 5 \\ 3 & 0 \end{pmatrix}, \begin{pmatrix} -3 \\ 3 \\ 3 \end{pmatrix}\right), (1)\right) =$

$x \cdot e = (1\ 1\ 1)\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = (1)$

$x \xleftarrow{\$} \{0,1\}^m$ $x = (1,1,1)^T$ A^T b

$c_1 = \begin{pmatrix} 2 & 0 & 3 \\ 4 & 5 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 5 \\ -2 \end{pmatrix}$

$c_1 := A^T x$ (A^T · x)

$c_2 := x \cdot b + M\left\lfloor \frac{q}{2} \right\rfloor$ $c_2 = (1\ 1\ 1)\begin{pmatrix} -3 \\ 3 \\ 3 \end{pmatrix} + (5) = (3) + (5) = (-3)$ (x · b, M ⌊q/2⌋)

return $C = (c_1, c_2) = \left(\begin{pmatrix} 5 \\ -2 \end{pmatrix}, (-3)\right)$

$Dec(sk, C)$:

$b = As + e$

$x \cdot b = x^T As + x \cdot e$

$= s^T \underbrace{A^T x}_{c_1} + x \cdot e$

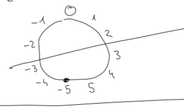
$S \cdot c_1 =$

$= (1\ -4)\begin{pmatrix} 5 \\ -2 \end{pmatrix} = (5-3) = (2)$

$x \cdot b = S \cdot c_1 + x \cdot e$

$(3) = (2) + (1)$

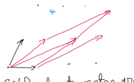
$c_2 - S \cdot c_1 = (-3) - (2) = (-5)$



Lattices and SIS

basis $\{b_i\}$ $B \rightsquigarrow B'$ $\mathcal{L} = \{a_1 b_1 + a_2 b_2 + \ldots : a_i \text{ integers}\}$

$\mathcal{L} \leftarrow dist(\mathcal{L}) = \alpha$



SVP shortest vector problem
CVP close vector problem

SIS shortest integer solutions

$A \xleftarrow{n \times m} \mathbb{Z}_q$

find me short integer $x \neq 0$ s.t.

$Ax = 0 \bmod q$

$\|x\| \leq \beta$

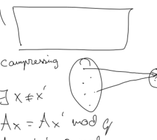
How big should β be?

When is it too easy? $(q\ 0\ 0\ 0\ 0\ 0\ \ldots)^T$

$\beta < q$

How to guarantee solution?

$n < m$



$\exists\, x \neq x'$

$Ax = Ax' \bmod q$

$A(x - x') = 0 \bmod q$

$(x - x')$ solution

Hash fn based on SIS:

$A \xleftarrow{n \times m} \mathbb{Z}_q$

$H(x) := Ax \bmod q$

x is a bit vector

$\{0,1\}^m \rightarrow \mathbb{Z}_q^n$

want it to be compressing

2^m domain size $\quad 2^{n \log_2 q} = q^n$

want compressing

$m > n \log_2 q$ $\quad x = (1\ 0\ 1\ 0\ 1)$

$x \neq x'$ $\quad x' = (0\ 1\ 1\ 0\ 1)$

$Ax = Ax' \bmod q$

$A(x - x') = 0 \bmod q$ $\quad x - x' = (1\ -1\ 0\ 0\ 0)$

solution $\in \{-1, 0, 1\}^m$ $\quad \in \{-1, 0, 1\}^m$

$\|x - x'\| \leq \sqrt{m}$

H is collision resistant if $SIS_{n,m,q,\sqrt{m}}$ is hard

Why would SIS even be hard

$Ax = 0 \bmod q$

$Az = 0 \bmod q$

$A(cx) = c(Ax) = c(0) \bmod q$

x and x' are kernel vectors

$A(x + x') = Ax + Ax' = 0 + 0 \bmod q$