Regev Encryption

DH $A^s = b$

Our world: $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ p large

Vector spaces: $\mathbb{F}_p^k$, $\mathbb{F}_p^n$ $k > n$ large

● = needs specification

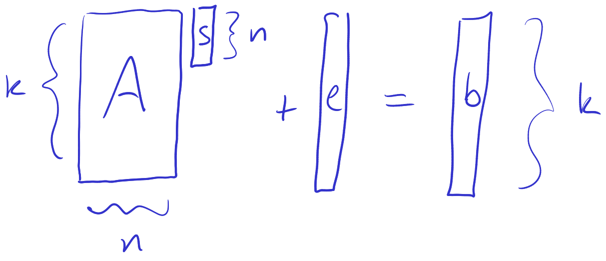
A private/public key pair

$s \in \mathbb{F}_p^n$ secret

$A \in M_{k \times n}(\mathbb{F}_p)$ public

$e \in \mathbb{F}_p^k$ small secret

"error"



g^{ab}

secret key
s

public key
A, $b = As + e$

Regev Encryption

$k > n$

Alice

message $\in \{0, 1\}$

(A, b)

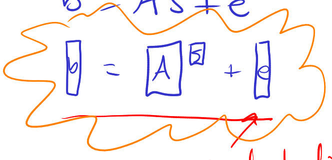
Bob

key pair

$s \in \mathbb{F}_p^n$ $e \in \mathbb{F}_p^k$ small secret

$A \in M_{k \times m}(\mathbb{F}_p)$

$b = As + e$

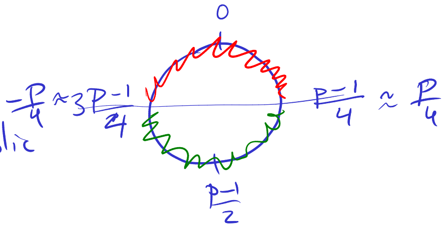


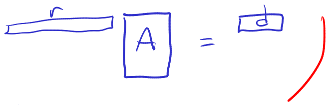
perturbation/error

Ephemeral key pair

$r \in \mathbb{F}_p^m$ private small

$d = r^T A \in \mathbb{F}_p^n$ public





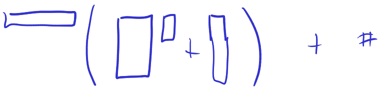
dimensions.

Mask message

(d, c)

Decrypt

$$c = \underbrace{r^T b}_{\text{mask}} + m\left(\frac{p-1}{2}\right) \in \mathbb{F}_p$$



$$c - ds \in \mathbb{F}_p$$

$[-\frac{p}{4}, \frac{p}{4}]$ = near 0

near $\frac{p-1}{2}$ = $[\frac{p}{4}, \frac{3}{4}p]$

decrypted: 0 1

Example

$p = 7$, $n = 2$, $k = 3$

Alice

message: 1

$$\left(\begin{pmatrix} 0 & 1 \\ 3 & 2 \\ 5 & 5 \end{pmatrix}, \begin{pmatrix} 3 \\ 4 \\ 5 \end{pmatrix}\right)$$

Bob

$s = \begin{pmatrix} 1 \\ 4 \end{pmatrix} \in \mathbb{F}_7^2$

$A = \begin{pmatrix} 0 & 1 \\ 3 & 2 \\ 5 & 5 \end{pmatrix}$ $e = \begin{pmatrix} -1 \\ 0 \\ 1 \end{pmatrix}$ randomly

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

Ephemeral key pair

$r = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}$ randomly

$$d = (1\ 0\ 1)\begin{pmatrix} 0 & 1 \\ 3 & 2 \\ 5 & 5 \end{pmatrix} = (5\ 6)$$

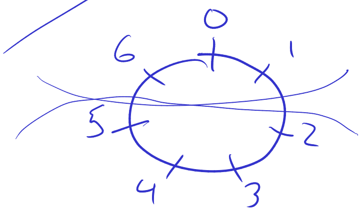
Mask:

$\swarrow \frac{p-1}{2}$

$((5\ 6), 4)$

Decrypt:

$$c = (1\,0\,1)\begin{pmatrix}3\\4\\5\end{pmatrix} + 1\cdot 3$$
$$= 1 + 3 = 4$$



$$c - ds$$
$$= 4 - (5\,6)\begin{pmatrix}1\\4\end{pmatrix}$$
$$= 4 - 1$$
$$= 3$$

$\Rightarrow$ plaintext $= 1$.

Why does this work?

$$c - ds = m\left(\frac{p-1}{2}\right) + r^T(As+e) - r^TAs$$

$$= m\left(\frac{p-1}{2}\right) + \underbrace{r^Te}_{\text{dot product of 2 "small" vectors.}}$$

$\Rightarrow$ round correctly to recover message.

The BIG Picture

structure	public	private	hard problem
$(\mathbb{Z}/p\mathbb{Z})^*$ g primitive	g^b	b	Discrete Log given g, g^b, find b
Ell. curves $P \in E(\mathbb{F}_p)$	bP	b	E.C. Discr. Log given P, bP, find b
isogeny-based E_1 = starting vertex	$\overset{\text{path}}{E_2 = b(E_1)}$ endpt	b	Isogeny path-finding given $E_1, E_2 = b(E_1)$ find b (path)
$\mathbb{F}_p^n, \mathbb{F}_p^k$	$A, As+e$	s	Learning with Errors given $A, As+e$, find s
$\mathbb{F}_p[x]/(x^n+n)$	$a, as+e$	s	Ring Learning with Errors given $a, as+e$, find s

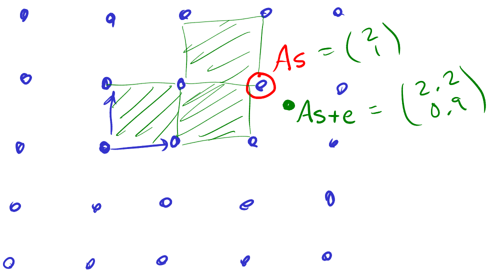
---

Why is Learning-with-Errors about lattices?

cols of A = a lattice Λ $\qquad$ As = vector in Λ

$As+e$ = vector near some elt of Λ

good basis/lattice



bad basis/lattice