LECTURE - 6

Regev Encryption

KeyGen$(1^n) \longrightarrow (sk, pk)$

where $sk = s \xleftarrow{\$} \mathbb{Z}_q^{n \times 1}$

$pk = A, b = As + e$ where

$A \leftarrow \mathbb{Z}_q^{m \times n}$, $e \leftarrow \chi^m$

$Enc(pk, \mu; r) \longrightarrow$ Compute $rA, rb + \mu\lfloor \frac{q}{2} \rfloor$

($\mu \in \{0,1\}$, $r \in \{0,1\}^m$)

$rb = rAs + re$

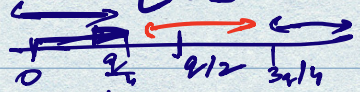
$Dec(sk, ct) \longrightarrow$ ($s \rightarrow (c_1, c_2)$)

We know: $rb = rAs + re$

Therefore, $c_2 - c_1 s = rAs + re + \mu\lfloor \frac{q}{2} \rfloor - rAs$

$= \mu\lfloor \frac{q}{2} \rfloor + re$

CORRECTNESS:



$\hookrightarrow \|re\| \leq \|e\| \cdot m$

Follows as long as $\|e\| < \frac{q}{4m}$

WHAT IS THE ERROR DISTRIBUTION χ ?

Discrete Gaussian over $\mathbb{Z}$

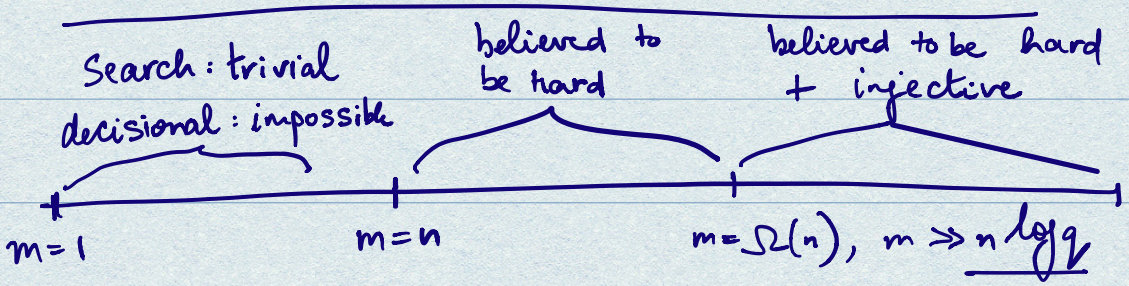
with mean $\mu = 0$, s.d. σ, $f(x) = \frac{1}{\sqrt{2\pi}\sigma} e^{\frac{-x^2}{2\sigma^2}}$

w.h.p. $\|e\| < \frac{q}{4m}$ when $\sigma \ll \frac{q}{4m}$, set it to $\frac{q}{4mn}$

(Why not, say, the uniform distribution?)

* Experimental evidence
* Gaussians maximize entropy for a fixed standard deviation

HARDNESS OF THE LWE PROBLEM.



(1 equation)

Injective: For $A, As+e$ $\nexists (s', e')$ s.t. $As'+e' = As+e$ $\neq (s, e)$

SECURITY : We will prove single-message security.

$(A, b, rA, rb+0)$ $b = As+e$ $\approx_c$ (by LWE) $(A, b, rA, rb + \lfloor \frac{q}{2} \rfloor)$ $\approx_c$

(A, b, rA, rb) $b \xleftarrow{\$} \mathbb{Z}_q^{n \times 1}$ $(A, b, rA, rb + \lfloor \frac{q}{2} \rfloor)$ $b \xleftarrow{\$} \mathbb{Z}_q^{n \times 1}$

Leftover Hash Lemma

(Simplified) (Impagliazzo-Lubin-Levy)

Let $H: K \times X \to Y$ be a universal hash function.

Let χ be a distribution over X such that $G.P.(\chi) \le t$.

Then $\forall$ unbounded $\mathcal{A}$,

$$\left| \Pr_{\substack{k \leftarrow K \\ x \leftarrow \chi}}[\mathcal{A}(k, H(k,x)) = 1] - \Pr_{\substack{k \leftarrow K \\ y \leftarrow Y}}[\mathcal{A}(k,y) = 1] \right| \le t \cdot |Y|$$

(k: A; $H(k,x)$: $H(A,r) = rA \in \mathbb{Z}_q^{1 \times n}$)

$$\le \frac{t}{2^m} \cdot 2^{n \log q}$$

$\forall$ unbounded $\mathcal{A}$,

$$\left| \Pr[\mathcal{A}(A, b, rA, rb) = 1] - \Pr[\mathcal{A}(A, b, \text{unif}^{1\times n}, \text{unif})] \right| \le \frac{1}{2^m} \cdot 2^{(n+1)\log q} \to 2n \log q$$

Note: χ is just unif over $\{0,1\}^m$.

H.W. Why is $H((A,b), r) = (rA, rb)$ a universal hash function? 2. 3.

For $m = 2n \log q$,

error is $\frac{1}{2^{2n \log q}} \cdot 2^{(n+1)\log q}$

$= 2^{(-n+1)\log q}$.

(A, b, rA, rb)

$\approx_{2^{(-n+1)\log q}} (A, b, \text{unif.}, \text{unif.})$

$= (A, b, \text{unif.}, \text{unif.} + \lfloor \frac{q}{2} \rfloor)$

$\approx_{2^{(-n+1)\log q}} (A, b, rA, rb + \lfloor \frac{q}{2} \rfloor)$

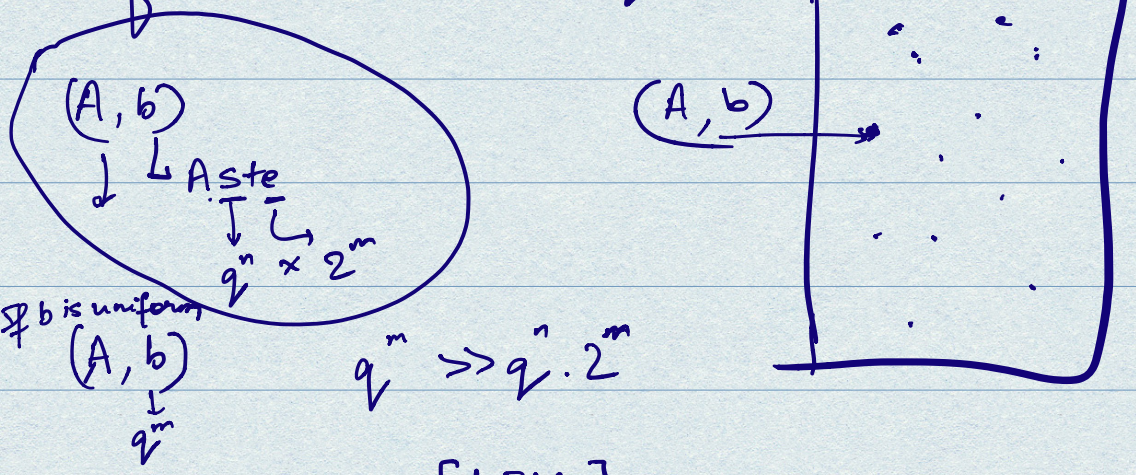
This proves single-message security.

In Regev, $\boxed{pk} = (A, b)$

where $b = As + e$.

This is "computationally i-dist."

from $b \xleftarrow{\text{unif.}} \mathbb{Z}_q^{n \times 1}$



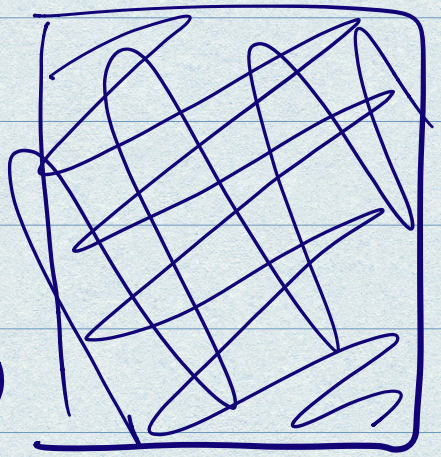
$q^m >> q^n \cdot 2^m$

[LPV]

"Dual" Regev

Another PKE scheme

where pk is "really" (statistically) random.



$(A, rA) \approx$ uniform

KeyGen$(1^n) \rightarrow pk, sk.$ $\hookrightarrow r$

$pk = (A, rA)$

where $A \xleftarrow{\$} \mathbb{Z}_q^{n \times m}$, $r \leftarrow \{0,1\}^m$

$$\begin{bmatrix} A \\ \\ \end{bmatrix}_{m \times n} = A'.$$

$[\, rA \,]_{1 \times n}$

$Enc(pk, \mu; \text{randomness}) \rightarrow$

Sample $s \xleftarrow{\$} \mathbb{Z}_q^{n \times 1}$, $e \leftarrow \chi^{m+1}$

Output $ct = \underbrace{(A's)}_{m+1 \times 1} + e + \begin{bmatrix} 0 \\ \vdots \\ \mu\lfloor \frac{q}{2} \rfloor \end{bmatrix}$

(written differently)

$$= \underbrace{(As + e)}_{m \times 1}, \quad rAs + e' + \mu\lfloor \frac{q}{2} \rfloor$$

Dec (c) :

Parse c as (c_1, c_2) (c_1: $m \times 1$)

$$rc_1 = rAs + re$$

$$c_2 - rc_1 = \cancel{rAs} + e' + \mu\left\lfloor \frac{q}{2} \right\rfloor - \cancel{rAs} - re$$

$$= e' - re + \mu\left\lfloor \frac{q}{2} \right\rfloor$$

"small" enough.

SECURITY OF DUAL REGEV.

Goal:

Show that $\underline{Enc(0)} \approx_\varepsilon \underline{Enc(1)}$

$\rightarrow (A, \underline{rA}, Ase, \underline{rAs}+e')$

$\approx_c$

$(A, \underline{rA}, Ase, \underline{rAs}+e' + \lfloor \frac{q}{2} \rfloor)$

By LHL,

$(A, rA) \approx (A, a)$ where $a \xleftarrow{s} \mathbb{Z}_q^{l \times n}$

That means

$(A, rA, Ase, rAse')$

$\approx_\varepsilon (A, a, Ase, as+e')$ where $\varepsilon = \frac{1}{2^m} \cdot 2^{negl}$

↳ An instance of $LWE_{m+l,n,q,\chi}$

(by LWE)

$\approx_c (A, a, uniform, uniform)$

$= (A, a, uniform, uniform + \lfloor \frac{q}{2} \rfloor)$

9.

10.

12.

13.

14.