Day 3

Wednesday, July 22, 2020 10:35 PM

Covered so far

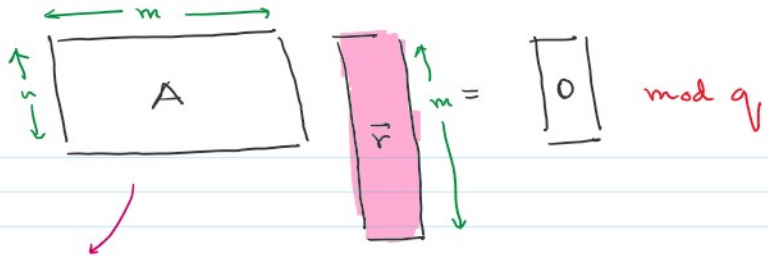
1) Lattices - definition — geometric / algebraic

2) computationally hard problems on lattices
   - SVP, CVP, SIVP
   - approximate and gap variants

3) Short integer solutions (SIS)

Short integer solutions (SIS)

n – # equations ≈ security parameter
m – # variables
q – modulus work $\mathbb{Z}_q$
β – "shortness"
think 1 for now



"short and wide"
$m > n$
underdetermined system

Find short $\vec{r}$

- solutions exist if $(\beta+1)^m > q^n$ // For $|\beta|=1$, $m > n \log q$
  i.e. $r_i \in \{-1, 0, 1\}$

- SVP on random q-ary lattices

4) Variants of SIS
   - normal form SIS
   - inhomogeneous SIS

5) SIS ⇒ CRHF ⇒ minicrypt
   "Direct" construction of SKE from SIS?

6) Smoothing a Lattice

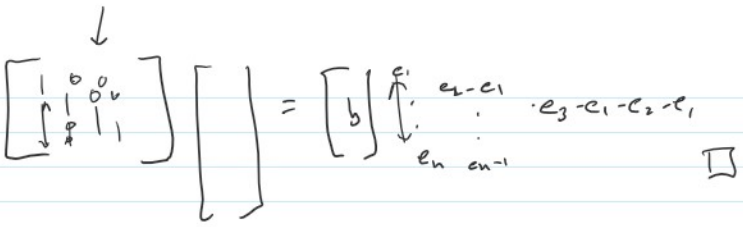
7) Worst-case to avg case reduction
   $SIVP_\gamma \leq SIS$

Today
1) Learning with errors — decision / search
2) search to decision
3) LWE to SIS

1) Learning with errors ← search
2) search to decision
3) LWE to SIS
4) PKE
   - Regev
   - dual Regev

Solving a system of equations

$$4x + 3y + 5z = 12 + e_1$$
$$2x + 5y + 1z = 22 + e_2$$
$$3x + 2y + 2z = 14 + e_3$$



Intuition: Gaussian elimination is brittle!!
- errors can grow uncontrollably

Secret $\vec{s}$

$$\langle \vec{a}_1, \vec{s} \rangle + e_1 = b_1$$
$$\vdots$$
$$\langle \vec{a}_m, \vec{s} \rangle + e_m = b_m$$

Learning With Errors (LWE) [Regev'05] // implicit in some prior work

- n – # variables
- m – # equations
- q – modulus work $\mathbb{Z}_q$ (swapped from SIS)
- χ – error distribution $\in \mathbb{Z}_q^m$ each $|e_i| \leq B$ "small"

ignoring the transpose notation. Hopefully obvious from context.

"short and wide"

$m > n$

~~underdetermined~~ ~~system~~ overdetermined single solution

Ch_{LWE}

$\vec{s} \xleftarrow{\$} \mathbb{Z}_q^n$

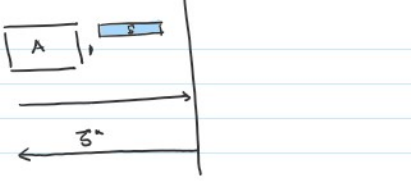
$A \xleftarrow{\$} \mathbb{Z}_q^{n \times m}$

$\vec{e} \leftarrow \chi^m$

$\vec{b} = \vec{s}^T A + \vec{e}$

$\vec{s} \stackrel{?}{=} \vec{s}'$

A_{LWE}

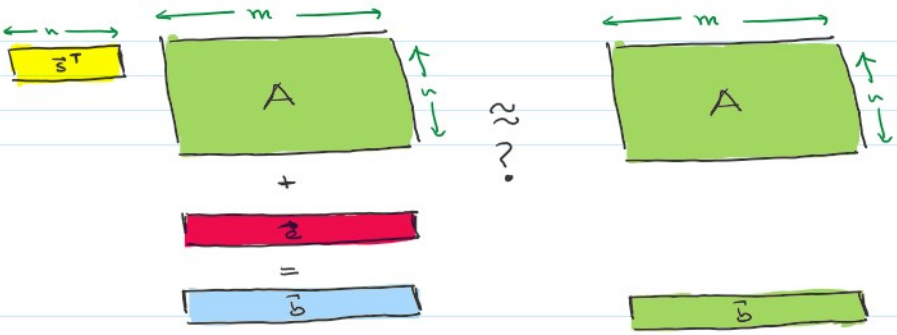


Ghazal

Search not useful for crypto
- half of $\vec{s}$ could be leaked.

Decisional LWE

- randomly sampled in $\mathbb{Z}_q^d$ ← dimension



Ch ← dLWE

$\vec{s} \xleftarrow{\$} \mathbb{Z}_q^n$

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

$\vec{e} \leftarrow \chi^m$

$c \xleftarrow{\$} \{0,1\}$

if $c = 0$

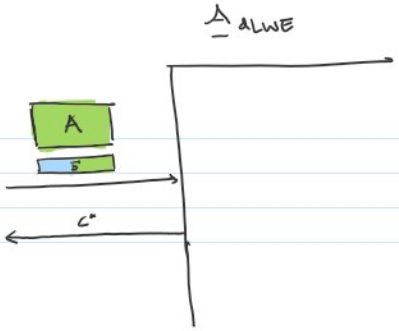
$\vec{b} = \vec{s}A + \vec{e}$

else

$\vec{b} \xleftarrow{\$} \mathbb{Z}_q^n$

$c = c^*$

↳ hard

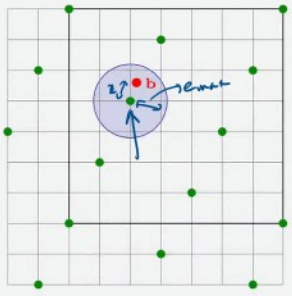


LWE as a Lattice Problem

- LWE lattice:

$$\mathcal{L}(\mathbf{A}) = \{\mathbf{z} \in \mathbb{Z}^m : \mathbf{z}^t \equiv \mathbf{s}^t\mathbf{A} \bmod q\}$$

- also a "dual lattice" of $\mathcal{L}^\perp$



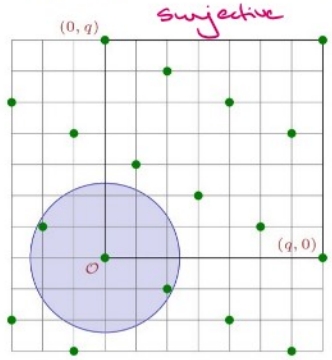
- LWE is bounded-dist decoding on $\mathcal{L}(\mathbf{A})$: given $\mathbf{b}^t \approx \mathbf{v}^t = \mathbf{s}^t\mathbf{A} \in \mathcal{L}(\mathbf{A})$, find $\mathbf{v}$.

Chris Peikert - https://youtu.be/K_fNK04yG4o?t=1405

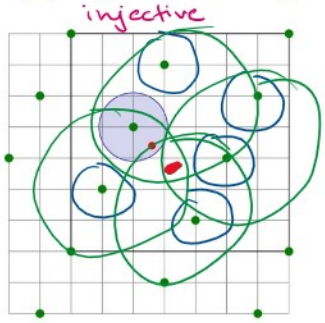
SIS versus LWE

SIS	LWE
$\mathbf{Az} = \mathbf{0}$, 'short' $\mathbf{z} \neq \mathbf{0}$	$(\mathbf{A}, \mathbf{b}^t = \mathbf{s}^t\mathbf{A} + \mathbf{e}^t)$ vs. $(\mathbf{A}, \mathbf{b}^t)$
Average-case SVP:	Average-case BDD:
$\mathcal{L}^\perp(\mathbf{A}) = \{\mathbf{z} \in \mathbb{Z}^m : \mathbf{Az} = \mathbf{0}\}$	$\mathcal{L}(\mathbf{A}) = \{\mathbf{z}^t \equiv \mathbf{s}^t\mathbf{A} \bmod q\}$

surjective



injective



http://cyber.biu.ac.il/wp-content/uploads/2017/01/slides-barilan5.pdf

---

q - modulus?

- for practice poly(n)

quantum reduction $q = \text{poly}(n)$

classical reduction $q \approx 2^n$

quantum: GapSVP ≤ LWE; SIVP

GapSVP ≤ LWE classical

X - error distribution?

↳ Require Gaussian for WC-to-AC reduction

other error distributions considered

"short secrets"

- essentially SIS in the normal form when $\mathbf{s} \leftarrow X$

Think about it!

---

search v decision LWE

(similar to CDH v DDH)

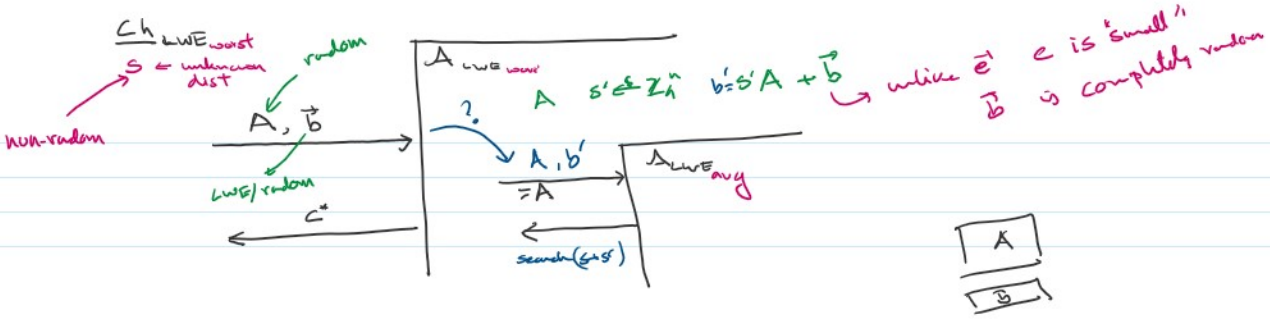
Search to Decision LWE Reduction

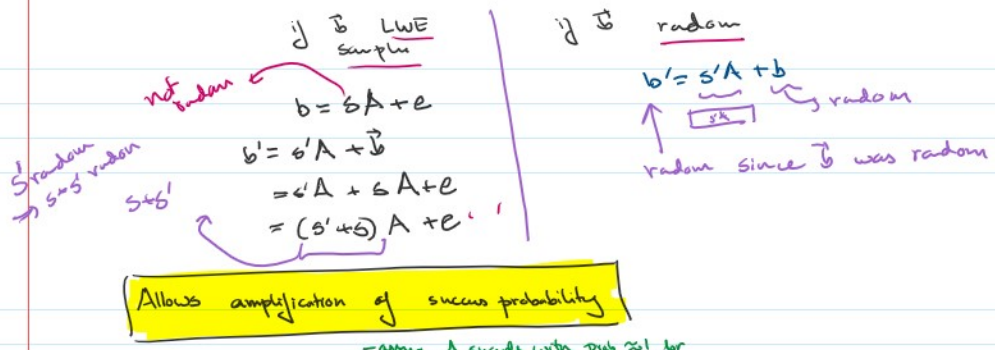
- given decision solver, can solve search LWE (not known in the DH setting)

Random self reduction

- given solver for LWE with random $\vec{s}$
can solve LWE for s with any distribution

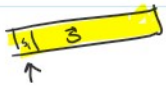
Assume decision LWE



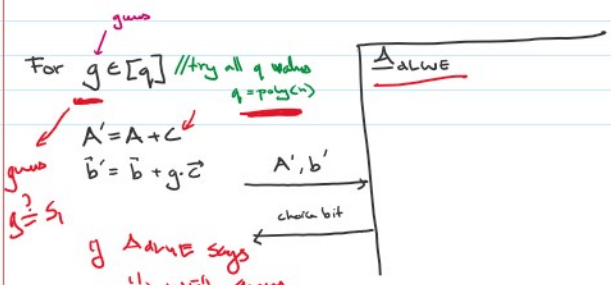


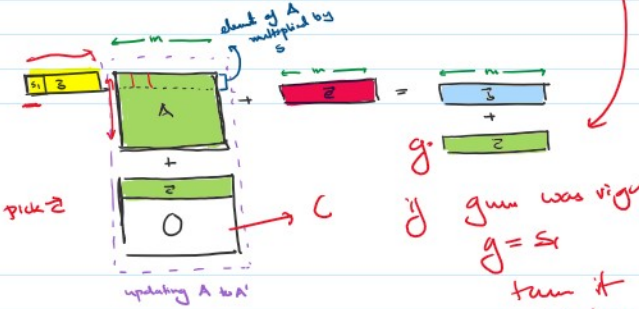
Search to Decision

- solve one element of $\vec{s}$ at a time.
w.l.o.g assume 1st element s_1

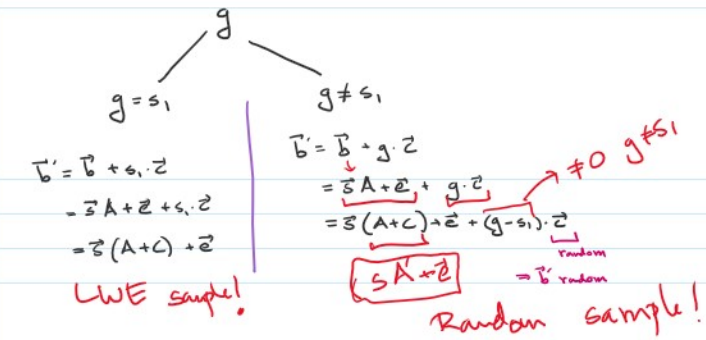


$s(A+C) + e$
$sA + e + sC$ ← $s_1 \vec{e}$
$sA' + e \neq \vec{b}$ ← fix $\vec{b}$?



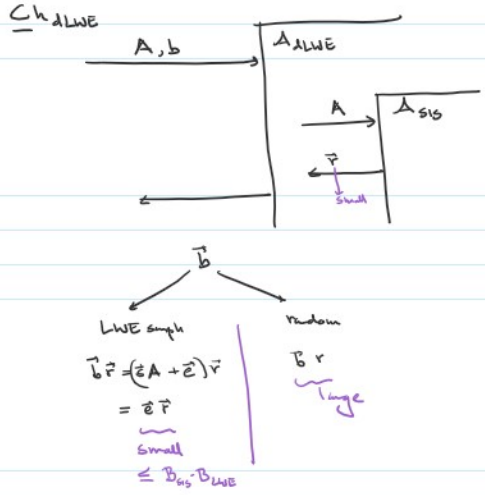


Does A_{dLWE} get this right distribution?



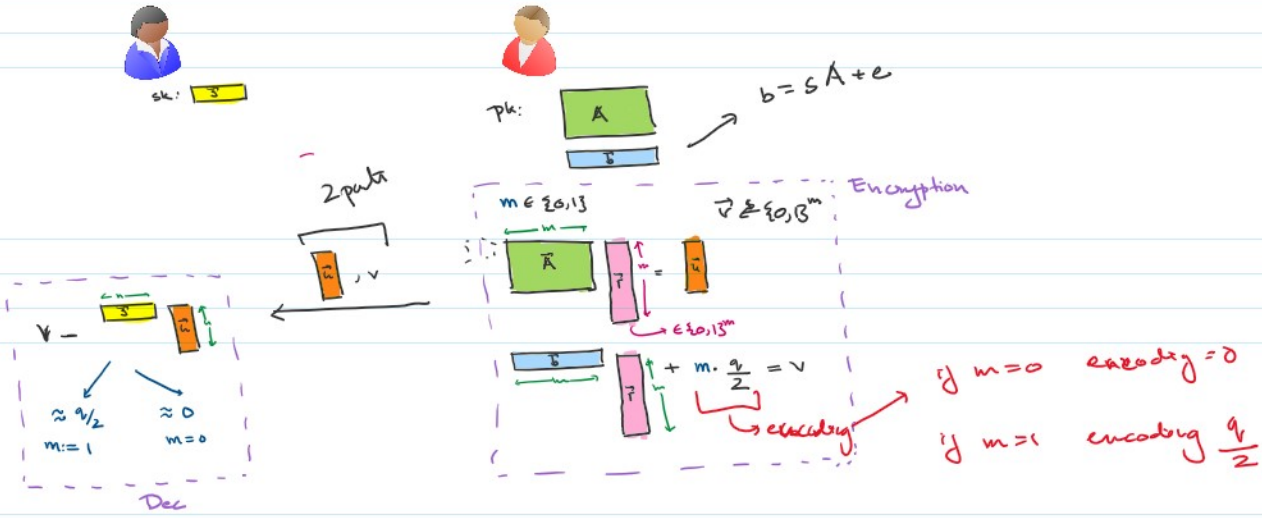
Run A_{dLWE} $n \cdot q$ times (if perfect correctness)

LWE to SIS



Public-key Encryption (today: non-efficient schemes)

1) [Regev05]



Correctness

$$v - \vec{s}\cdot\vec{u} = \vec{b}\vec{r} + m\cdot\frac{q}{2} - \vec{s}A\vec{r}$$
$$= \vec{s}A\vec{r} + \vec{r}\vec{e} + m\cdot\frac{q}{2} - \vec{s}A\vec{r}$$
$$= \vec{r}\cdot\vec{e} + m\cdot\frac{q}{2}$$

small because $\vec{e}$ small

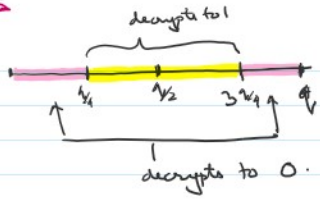
$\vec{r}\cdot\vec{e} \approx q/2$ if $m = 1$

$\vec{r}\cdot\vec{e} \approx 0$ if $m = 0$

$\vec{r}\cdot\vec{e} < \frac{q}{4}$

$\Rightarrow m\cdot\|\vec{e}\|_\infty \cdot m\cdot B < \frac{q}{4}$

$\Rightarrow B < \frac{q}{4m}$



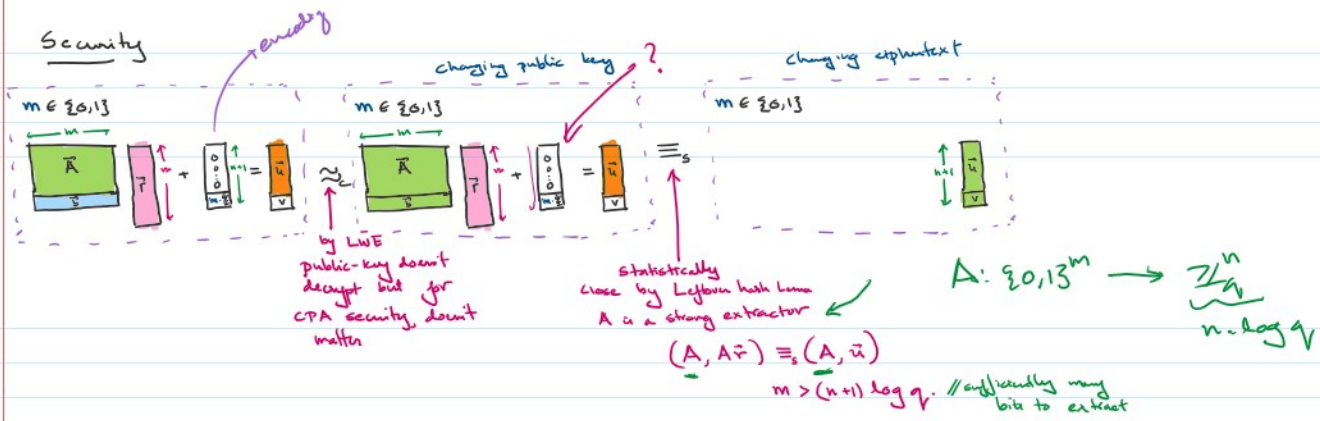
Security

encoding

changing public key ?

changing ciphertext

Security



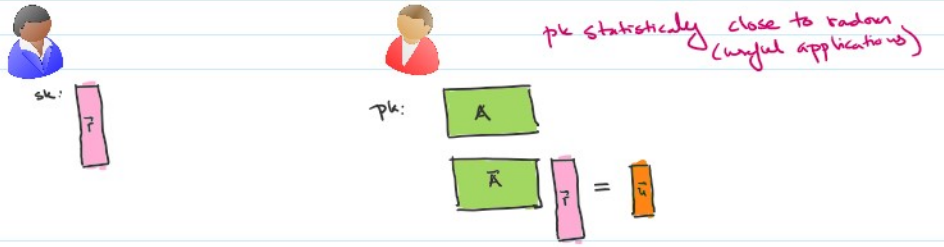
$A: \{0,1\}^m \to \mathbb{Z}_q^n$ — $n \cdot \log q$

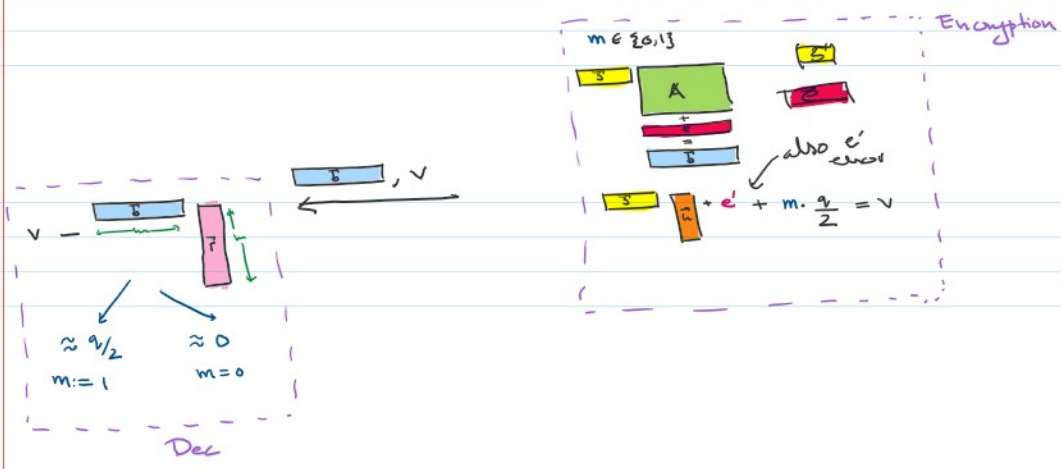
$(A, A\vec{r}) \equiv_s (A, \vec{u})$

$m > (n+1)\log q$. // sufficiently many bits to extract

Dual-Regev [Gentry-Peikert-Vaikuntanathan '08]

(switch roles of encryptor & decryptor)





Correctness

$$\begin{aligned} v - \vec{b}\cdot\vec{r} &= \vec{s}\cdot\vec{u} + e' + m\cdot\tfrac{q}{2} - \vec{s}A\vec{r} + \vec{e}\cdot\vec{r} \\ &= \vec{s}\cdot A\vec{r} + e' + m\cdot\tfrac{q}{2} - \vec{s}A\vec{r} + \vec{e}\cdot\vec{r} \\ &= m\cdot\tfrac{q}{2} + \underbrace{e' + \vec{e}\cdot\vec{r}}_{\text{small}} \end{aligned}$$

Security as before - order of hybrids change: first LHL, then LWE