CSE208: Advanced Cryptography (FHE)

Daniele Micciancio

UCSD

Fall 2023

Section 1

LWE

Linear equations

- q: integer modulus
- $\mathbb{Z}_q$: integers modulo q
- $A \in \mathbb{Z}_q^{n \times m}$: matrix
- $b \in \mathbb{Z}_q^n$

Problem

Given A, b, *find* $x \in \mathbb{Z}^m$ *such that* $Ax = b \pmod q$

Problem

Given A, b, *find* $x \in \{0,1\}^m$ *such that* $Ax = b \pmod q$

Linear equations

- q: integer modulus
- $\mathbb{Z}_q$: integers modulo q
- $A \in \mathbb{Z}_q^{n \times m}$: matrix
- $b \in \mathbb{Z}_q^n$

Problem

Given A, b, find $x \in \mathbb{Z}^m$ such that $Ax = b \pmod q$

Problem

Given A, b, find $x \in \{0,1\}^m$ such that $Ax = b \pmod q$

Question

Which problem can be efficiently solved?

Worst-case vs Average-case hardness

Problem

Given A, b, *find* $x \in \{0,1\}^m$ *such that* $Ax = b \pmod{q}$

- NP-hard: no polynomial time algorithm unless P=NP
- Is it hard to solve on the average?

Worst-case vs Average-case hardness

Problem

Given A, b, *find* $x \in \{0,1\}^m$ *such that* $Ax = b \pmod q$

- NP-hard: no polynomial time algorithm unless P=NP
- Is it hard to solve on the average?
- For what probability distribution?
  - $A \leftarrow \mathbb{Z}_q^{n \times m}$
  - $x \leftarrow \{0,1\}^m$
  - $b = Ax \pmod q$

Worst-case vs Average-case hardness

Problem

Given A, b, *find* $x \in \{0,1\}^m$ *such that* $Ax = b \pmod q$

- NP-hard: no polynomial time algorithm unless P=NP
- Is it hard to solve on the average?
- For what probability distribution?
  - $A \leftarrow \mathbb{Z}_q^{n \times m}$
  - $x \leftarrow \{0,1\}^m$
  - $b = Ax \pmod q$
- Is $f : (A, x) \mapsto [A, Ax \bmod q]$ is a *One-Way Function*?
- For what values of n, m, q?

One-Way Functions

Definition

$f : D \to R$ is a one-way function if for any PPT algorithm `I`

`Pr{InvertGame(I)}` $\approx$`0` where

```
InvertGame:
  x ← D
  y = f(x)
  x' ← I(y)
  return (f(x') ?= y)
```

One-Way Functions

Definition

$f : D \to R$ is a one-way function if for any PPT algorithm `I`

`Pr{InvertGame(I)}` $\approx$`0` where

```
InvertGame:
  x ← D
  y = f(x)
  x' ← I(y)
  return (f(x') ?= y)
```

- $D = \mathbb{Z}_q^{n \times m} \times \{0,1\}^m$
- $R = \mathbb{Z}_q^{n \times m} \times \mathbb{Z}_q^n$
- $f(A, x) = [A, Ax \bmod q]$
- Asymptotics: $q(m) = 2^{poly(m)}$, $n(m) = poly(m)$

One-Way?

- $A \leftarrow \mathbb{Z}^{n \times m}$
- $x \leftarrow \{0,1\}^m$
- $f(A,x) = [A, Ax] \bmod q$

Question

Is f a one-way function when

1. $q = 2^m$, $n = m$
2. $q = 2^m$, $n = m/2$
3. $q = m$, $n = m/2$
4. $q = m$, $n = \sqrt{m}$

Short Integer Solution (SIS) problem

- Parameters:
  - modulus q
  - dimensions $n < m$
  - bound β

Problem

SIS: Given $A \in \mathbb{Z}_q^{n \times m}$ *and* $b \in \mathbb{Z}_q^n$, *find* $x \in \mathbb{Z}^m$ *such that* $Ax = b \pmod q$ *and* $\|x\| \leq \beta$

- More generally: $x \in S \subset \mathbb{Z}^m$
- Special cases:
  - $S = \{x : \|x\| \leq \beta\}$
  - $S = \{0,1\}^m$
  - $S = \{x : \|x\|_\infty \leq \beta\}$

Systematic Form

- Assume $n < m$ (e.g., $n = m/2$)
- Let $A = [I, A'] \in \mathbb{Z}^{n \times m}$ for some $A' \in \mathbb{Z}^{n \times (m-n)}$

Lemma

If SIS is hard, then SIS' is hard

Learning With Errors (LWE)

- SIS': $A = [I, A'] \in \mathbb{Z}^{n \times m}$ where $n < m$ (say, $n = m/2$)
- Let $x = (e, s)$
- $Ax = [I, A'](e, s) = A's + e$

Problem

LWE: Given A' and b, find small e, s such that $A's + e = b$

Problem

LWE: Given A' and b, find small e, s such that $A's \approx b$

Notice:

- $A' \in \mathbb{Z}_q^{n \times n}$
- $A's = b$ is easy to solve
- $A's \approx b$ seems hard

LWE problem

Notation:

- secret $s \leftarrow \mathbb{Z}_q^n$, usually chosen at random
- modulus $q(n) = poly(n)$
- $A \leftarrow \mathbb{Z}_q^{m \times n}$
- error $e \leftarrow \chi^m$, usually $|e_i| \approx \sqrt{n}$
- $b = As + e \in \mathbb{Z}_q^m$

Problem

Search LWE: Given A and b, find s

- Each row of A gives an approximate equation $\langle a, s \rangle \approx b$
- if $m \gg n$, then s is uniquely determined
- Still, hard to find s

Uniform vs Small secrets

Lemma

If LWE is hard for $s \leftarrow \chi^n$, then it is hard for $s \leftarrow \mathbb{Z}_q^n$

Uniform vs Small secrets

Lemma

If LWE is hard for $s \leftarrow \chi^n$, then it is hard for $s \leftarrow \mathbb{Z}_q^n$

Proof: Assume *Adv* solves LWE with uniform $s \leftarrow \mathbb{Z}_q^n$

```
Adv'(A,b)
   s ← Z_q^n
   b' = b + As
   s' = Adv(A,b')
   return (s' - s)
```

Decisional LWE (DLWE)

Definition

LWE distribution:

```
LWE[q,n,m] =
  do A ← ℤ_q^{m×n}
     s ← ℤ_q^n
     e ← χ^m
     b = As+e
     return (A,b)
```

Definition

Decisional LWE (DLWE): distinguish LWE[q,n,m] from Uniform($\mathbb{Z}_q^{m\times(n+1)}$)

Decision to Search reduction

Theorem

If DLWE is hard, then LWE is hard

Decision to Search reduction

Theorem

If DLWE is hard, then LWE is hard

Proof:

- Assume `Adv` solves LWE
- Given `Adv'` that solves DLWE

```
Adv'(A,b):
   s ← Adv(A,b)
   if (As ≈ b)
      then return "LWE"
      else return "random"
```

Search vs Decision

- Is (Search) LWE harder than DLWE?

Theorem

If Search LWE is hard for any $m = poly(n)$, then DLWE is also hard for any $m = poly(n)$

Theorem

For any $m = poly(n)$, if Search LWE is hard, then DLWE is also hard

LWE Search to Decision reduction (easy version)

- Assume `Adv` can distinguish LWE from uniform
- Task: Given `A,b`, find `s` such that `As` $\approx$`b (mod q)`
- Assumption: `s` is unique (holds with very high probability)
- We show how to check if $s_i = \gamma$:

```
Adv(A,b):
  a ← ℤ^m
  A' = A + [0..0,a,0..0]
  b' = b + γ a
  case Adv(A',b') of
    "LWE"    : return s_i = c
    "random" : return s_i ≠ c
```

- Recover all entries of s, one at a time

(Decisional) LWE Assumption

- In the rest of the course we will just assume that DLWE is hard
- There are several variants of the assumption:
  - Uniform vs. small secret s
  - Different (always small) error distributions $e \leftarrow \chi$
  - Fixed vs unbounded number of samples m
  - Different values of q
  - Concrete hardness assumptions
- By and large all variants are equivalent up to polynomial reductions

How to Encrypt with LWE

- Fix secret $s \in \mathbb{Z}_q^n$
- LWE samples (a_i, b_i) where $a_i \in \mathbb{Z}_q^n$ and $b_i \in \mathbb{Z}$
- Polynomially many samples (a_i, b_i) for $i = 1, 2, ...$
- DLWE: the b_i values are pseudorandom
- Idea: use b_i as a one-time pad to encrypt a messate $\mathtt{m}$

LWE Symmetric Encryption


```
Gen():
   s ← $\mathbb{Z}_q^n$
   return s

Enc(s,m):
   a ← $\mathbb{Z}_q^n$
   e ← $\chi$
   b = $\langle a, s \rangle$ + e + m

Dec(s,(a,b)):
   return (b - $\langle a, s \rangle$)
```

Is this a valid encryption scheme?

Symmetric Encryption


```
SKE(Gen,Enc,Dec)
  Gen: () → sk
  Enc: (sk,m) → c
  Dec: (sk,c) → m
```

Correctness: for every $\texttt{sk} \leftarrow \texttt{Gen}()$ and $\texttt{m} \leftarrow [\texttt{M}]$, $\texttt{r} \leftarrow [\texttt{R}]$:

$$\texttt{Dec}(\texttt{sk}, \texttt{Enc}(\texttt{sk}, \texttt{m}; \texttt{r})) = \texttt{m}$$

Question

Is LWE a valid encryption scheme?

Correcting from errors

- Ciphertext modulus q
- Message modulus p (assume p divides q)
- Message space: $m \in \mathbb{Z}_p$

```
Enc(s,m) = (a,b) where
  a ← Z_q^n, e ←χ
  b = ⟨a,s⟩ + e + (q/p)m

Dec(s,(a,b)) = round(c*p/q)) where
  c = b - ⟨a,s⟩ mod q
```

Lemma

If $|e| < \beta$ *then* `Dec(s,Enc(s,m;a,e))= m`

Question

For what value of β *is the lemma correct?*

IND-CPA security for symmetric encryption


```
INDCPAgameSKE(b:{0,1})
  sk ← Gen()
  b' ← A[LR]
  return b':{0,1}

LR(m_0, m_1):
  ct ← Enc(sk, m_b)
  return ct
```

- Similar LR security definition can be given also for PKE: `A[LR](pk)` is given `pk` and oracle access to `LR`
- Previous PKE INDCPAgame allows only one query to LR

Question

Why can restrict PKE INDCPAgame to one query?

Security of LWE symmetric encryption

- Assume $|e| < \beta = q/(2p)$ for all $e \leftarrow \chi$
- Is LWE INDCPAgameSKE secure?

Theorem

Assume DLWE holds for a given $q(n)$ and any $m = poly(n)$. Then LWE symmetric encryption is INDCPA secure, i.e., any adversary Adv *has negligible advantage in the INDCPAgameSKE distinguishing game.*

RR-CPA security

- LWE encryption satisfies a stronger security property: ciphertext indistinguishability from random

```
INDCPAgameSKE(b:{0,1})
   sk ← Gen()
   b' ← A[RR]
   return b':{0,1}

RR(m):
   ct_0 ←Enc(sk,m)
   ct_1 ←Z_q^{n+1}
   return ct_b
```

- "Real or Random" oracle RR
- RR-CPA security also provides a form of anonimity

LeftRight vs RealRand security

Theorem

If a (SKE or PKE) scheme is `INDCPA-RR` *secure, then it is also* `INDCPA-LR` *secure.*

Remark

A (SKE or PKE) scheme can be `INDCPA-LR` *secure, but not* `INDCPA-RR` *secure.*

Ciphertext expansion

- Ciphertext expansion: `bitsize(ct)/ bitsize(m)`
- Example:
  - `Enc(f,x;r)= (f(r),H(r)⊕m)` where $f : \{0,1\}^k \to \{0,1\}^k$
  - `Enc(f,.)`: $\{0,1\}^m \to \{0,1\}^{m+k}$
  - Ciphertext expansion: $(m+k)/m = 1 + (k/m)$

Ciphertext expansion

- Ciphertext expansion: `bitsize(ct)/ bitsize(m)`
- Example:
  - Enc(f,x;r)= (f(r),H(r)$\oplus$m) where $f : \{0,1\}^k \to \{0,1\}^k$
  - Enc(f,.):$\{0,1\}^m \to \{0,1\}^{m+k}$
  - Ciphertext expansion: $(m+k)/m = 1 + (k/m)$
- LWE ciphertext expansion
  - $q = n$, $|e| < \beta \approx \sqrt{n} < q/(2p)$
  - m $\in \mathbb{Z}_p$: |m| = log p
  - (a,b) $\in \mathbb{Z}_q^{n+1}$: |(a,b)| = (n+1) log q
  - |(a,b)| / |m| = (n+1) (log q / log p) = O(n)

Compact LWE Encryption

- CompactLWE SKE (Gen,Enc,Dec)

```
Gen():
   S ← Z_q^{n×k}
   return S

Enc(S,M ∈ Z_p^{h×k}) = (A,B)
   A ← Z_q^{h×n}
   E ← χ^{h×k}
   B = AS + E + round((q/p)M)

Dec(S,(A,B)):
   C ← (B - AS) mod q
   return round(C*p/q)
```

Theorem

CompactLWE SKE is correct and INDCPA-RR secure

Ciphertext Expansion

Compact LWE encryption:

- Key $S \in \mathbb{Z}_q^{n \times k}$
- Message $M \in \mathbb{Z}_p^{h \times k}$
- Encryption Enc(S,M)= (A,B) where B = AS + E + M(p/q)
- Ciphertext $(A, B) \in \mathbb{Z}_q^{h \times (n+k)}$

Question

What is the ciphertext/plaintext size ratio?

Ciphertext Expansion

Compact LWE encryption:

- Key $S \in \mathbb{Z}_q^{n \times k}$
- Message $M \in \mathbb{Z}_p^{h \times k}$
- Encryption `Enc(S,M)= (A,B)` where `B = AS + E + M(p/q)`
- Ciphertext $(A, B) \in \mathbb{Z}_q^{h \times (n+k)}$

Question

What is the ciphertext/plaintext size ratio?

- |ct|/|m| = (1+n/k)(log q / log p)
- for k=n, p,q=poly(n): |ct|/|m| = O(1)