

Section 4

LWE

Linear equations

CSE208:
Advanced
Cryptography

Daniele
Micciancio

Introduction

Defining FHE

Bootstrapping

LWE

Linearity

Key Switching

Multiplication

FHE!!

Ring LWE

- 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

CSE208:
Advanced
Cryptography

Daniele
Micciancio

Introduction
Defining FHE
Bootstrapping
LWE
Linearity
Key Switching
Multiplication
FHE!!
Ring LWE

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 $f : (A, x) \mapsto (A, Ax \pmod{q})$ is a *One-Way Function*?
- For what values of n, m, q ?

One-Way Functions

CSE208:
Advanced
Cryptography

Daniele
Micciancio

Introduction

Defining FHE

Bootstrapping

LWE

Linearity

Key Switching

Multiplication

FHE!!

Ring LWE

Definition

$f : D \rightarrow R$ is a one-way function if for any PPT algorithm I
 $\Pr\{\text{InvertGame}(I)\} \approx 0$ where

InvertGame :

$x \leftarrow D$

$y = f(x)$

$x' \leftarrow I(y)$

return $(f(x') \stackrel{?}{=} y)$

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

One-Way?

CSE208:
Advanced
Cryptography

Daniele
Micciancio

Introduction

Defining FHE

Bootstrapping

LWE

Linearity

Key Switching

Multiplication

FHE!!

Ring LWE

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

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

CSE208:
Advanced
Cryptography

Daniele
Micciancio

Introduction

Defining FHE

Bootstrapping

LWE

Linearity

Key Switching

Multiplication

FHE!!

Ring LWE

- 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

CSE208:
Advanced
Cryptography

Daniele
Micciancio

Introduction

Defining FHE

Bootstrapping

LWE

Linearity

Key Switching

Multiplication

FHE!!

Ring LWE

- 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

CSE208:
Advanced
Cryptography

Daniele
Micciancio

Introduction

Defining FHE

Bootstrapping

LWE

Linearity

Key Switching

Multiplication

FHE!!

Ring 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

CSE208:
Advanced
Cryptography

Daniele
Micciancio

Introduction

Defining FHE

Bootstrapping

LWE

Linearity

Key Switching

Multiplication

FHE!!

Ring LWE

Notation:

- secret $s \leftarrow \mathbb{Z}_q^n$, usually chosen at random
- modulus $q(n) = \text{poly}(n)$
- $A \leftarrow \mathbb{Z}_q^{m \times n}$
- 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

CSE208:
Advanced
Cryptography

Daniele
Micciancio

Introduction

Defining FHE

Bootstrapping

LWE

Linearity

Key Switching

Multiplication

FHE!!

Ring LWE

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

CSE208:
Advanced
Cryptography

Daniele
Micciancio

Introduction

Defining FHE

Bootstrapping

LWE

Linearity

Key Switching

Multiplication

FHE!!

Ring LWE

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 ←  $\mathbb{Z}_q^n$ 
  b' = b + As
  s' = Adv(A, b')
  return (s' - s)
```

Decisional LWE (DLWE)

Definition

LWE distribution:

```
LWE[q, n, m] =  
do A ←  $\mathbb{Z}_q^{m \times n}$   
   s ←  $\mathbb{Z}_q^n$   
   e ←  $\chi^m$   
   b = As + e  
   return (A, b)
```

Definition

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

Decision to Search reduction

CSE208:
Advanced
Cryptography

Daniele
Micciancio

Introduction

Defining FHE

Bootstrapping

LWE

Linearity

Key Switching

Multiplication

FHE!!

Ring LWE

Theorem

If DLWE is hard, then LWE is hard

Decision to Search reduction

CSE208:
Advanced
Cryptography

Daniele
Micciancio

Introduction

Defining FHE

Bootstrapping

LWE

Linearity

Key Switching

Multiplication

FHE!!

Ring LWE

Theorem

If DLWE is hard, then LWE is hard

Proof:

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

$\text{Adv}'(A, b) :$

$s \leftarrow \text{Adv}(A, b)$

if $(As \approx b)$

then return "LWE"

else return "random"

Search vs Decision

CSE208:
Advanced
Cryptography

Daniele
Micciancio

Introduction

Defining FHE

Bootstrapping

LWE

Linearity

Key Switching

Multiplication

FHE!!

Ring LWE

- Is (Search) LWE harder than DLWE?

Theorem

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

Theorem

For any $m = \text{poly}(n)$, if Search LWE is hard, then DLWE is also hard for any $m = \text{poly}(n)$

LWE Search to Decision reduction (easy version)

CSE208:
Advanced
Cryptography

Daniele
Micciancio

Introduction

Defining FHE

Bootstrapping

LWE

Linearity

Key Switching

Multiplication

FHE!!

Ring LWE

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

$\text{Adv}(A, b)$:

$a \leftarrow \mathbb{Z}^m$

$A' = A + [\theta \dots \theta, a, \theta \dots \theta]$

$b' = b + \gamma a$

case $\text{Adv}(A', b')$ **of**

"LWE" : **return** $s_i = c$

"random" : **return** $s_i \neq c$

- Recover all entries of s , one at a time

(Decisional) LWE Assumption

CSE208:
Advanced
Cryptography

Daniele
Micciancio

Introduction

Defining FHE

Bootstrapping

LWE

Linearity

Key Switching

Multiplication

FHE!!

Ring LWE

- 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

CSE208:
Advanced
Cryptography

Daniele
Micciancio

Introduction

Defining FHE

Bootstrapping

LWE

Linearity

Key Switching

Multiplication

FHE!!

Ring 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 $i = 1, 2, \dots$
- DLWE: the b_i values are pseudorandom
- Idea: use b_i as a one-time pad to encrypt a message m

LWE Symmetric Encryption

CSE208:
Advanced
Cryptography

Daniele
Micciancio

Introduction

Defining FHE

Bootstrapping

LWE

Linearity

Key Switching

Multiplication

FHE!!

Ring LWE

Gen():

$s \leftarrow \mathbb{Z}_q^n$

return s

Enc(s, m):

$a \leftarrow \mathbb{Z}_q^n$

$e \leftarrow \chi$

$b = \langle a, s \rangle + e + m$

Dec($s, (a, b)$):

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

Is this a valid encryption scheme?

Symmetric Encryption

CSE208:
Advanced
Cryptography

Daniele
Micciancio

Introduction

Defining FHE

Bootstrapping

LWE

Linearity

Key Switching

Multiplication

FHE!!

Ring LWE

SKE (Gen, Enc, Dec)

Gen: () \rightarrow sk

Enc: (sk, m) \rightarrow c

Dec: (sk, c) \rightarrow m

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

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

Question

Is this a valid encryption scheme?

Correcting from errors

CSE208:
Advanced
Cryptography

Daniele
Micciancio

Introduction

Defining FHE

Bootstrapping

LWE

Linearity

Key Switching

Multiplication

FHE!!

Ring LWE

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

$\text{Enc}(s, m) = (a, b)$ where

$$a \leftarrow \mathbb{Z}_q^n, e \leftarrow \chi$$

$$b = \langle a, s \rangle + e + (q/p)m$$

$\text{Dec}(s, (a, b)) = \text{round}(c * p / q)$ where

$$c = b - \langle a, s \rangle \pmod{q}$$

Lemma

If $|e| < \beta$ then $\text{Dec}(s, \text{Enc}(s, m; a, e)) = m$

Question

For what value of β is the lemma correct?

IND-CPA security for symmetric encryption

CSE208:
Advanced
Cryptography

Daniele
Micciancio

Introduction

Defining FHE

Bootstrapping

LWE

Linearity

Key Switching

Multiplication

FHE!!

Ring LWE

```
INDCPAgameSKE (b : {0, 1})
```

```
  sk ← Gen()
```

```
  b' ← A[LR]
```

```
  return b' : {0, 1}
```

```
LR (m0, m1) :
```

```
  ct ← Enc(sk, mb)
```

```
  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

CSE208:
Advanced
Cryptography

Daniele
Micciancio

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

Theorem

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

Introduction
Defining FHE
Bootstrapping
LWE
Linearity
Key Switching
Multiplication
FHE!!
Ring LWE

RR-CPA security

CSE208:
Advanced
Cryptography

Daniele
Micciancio

Introduction

Defining FHE

Bootstrapping

LWE

Linearity

Key Switching

Multiplication

FHE!!

Ring LWE

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

$\text{INDCPAgameSKE}(b : \{0, 1\})$

$sk \leftarrow \text{Gen}()$

$b' \leftarrow A[\text{RR}]$

return $b' : \{0, 1\}$

$\text{RR}(m) :$

$ct_0 \leftarrow \text{Enc}(sk, m)$

$ct_1 \leftarrow \mathbb{Z}_q^{n+1}$

return ct_b

- “Real or Random” oracle RR
- RR-CPA security also provides a form of anonymity

LeftRight vs RealRand security

CSE208:
Advanced
Cryptography

Daniele
Micciancio

Introduction

Defining FHE

Bootstrapping

LWE

Linearity

Key Switching

Multiplication

FHE!!

Ring LWE

Theorem

If a (SKE or PKE) scheme is IND CPA-RR secure, then it is also IND CPA-LR secure.

Remark

A (SKE or PKE) scheme can be IND CPA-LR secure, but not IND CPA-RR secure.

Compact LWE Encryption

CSE208:
Advanced
Cryptography

Daniele
Micciancio

Introduction

Defining FHE

Bootstrapping

LWE

Linearity

Key Switching

Multiplication

FHE!!

Ring LWE

- Ciphertext expansion: $\text{bitsize}(\text{ct}) / \text{bitsize}(m)$
- Compact LWE SKE ($\text{Gen}, \text{Enc}, \text{Dec}$)

$\text{Gen}()$:

$S \leftarrow \mathbb{Z}_q^{l \times n}$
return S

$\text{Enc}(S, m) = (a, b)$

$a \leftarrow \mathbb{Z}_q^n$

$e \leftarrow \chi^l$

$b = Sa + e + \text{round}((p/q)m)$

$\text{Dec}(S, (a, b))$:

$c \leftarrow b - S^t a \pmod q$

return $\text{round}(c * p / q)$

Theorem

Compact LWE SKE is correct and IND CPA-RR secure

Ciphertext Expansion

CSE208:
Advanced
Cryptography

Daniele
Micciancio

Introduction

Defining FHE

Bootstrapping

LWE

Linearity

Key Switching

Multiplication

FHE!!

Ring LWE

Compact LWE encryption:

- Key $S \in \mathbb{Z}_q^{l \times n}$
- Message $m \in \mathbb{Z}_p^l$
- Encryption $\text{Enc}(S, m) = (a, b)$ where $b = Sa + e + mp/q$
- Ciphertext $(a, b) \in \mathbb{Z}_q^{n+l}$

Question

What is the ciphertext/plaintext size ratio?

- Example:
 - $\text{Enc}(f, x; r) = (f(r), H(r) \oplus m)$ where $f : \{0, 1\}^k \rightarrow \{0, 1\}^k$
 - $\text{Enc}(f, \cdot) : \{0, 1\}^m \rightarrow \{0, 1\}^{m+k}$
 - Ciphertext expansion: $(m + k)/m = 1 + (k/m)$