Lattice-Based Encryption

Vadim Lyubashevsky
INRIA / ENS, Paris
Lattice-Based Encryption Schemes

1. NTRU [Hoffstein, Pipher, Silverman ‘98]

2. LWE-Based [Regev ‘05]

3. Ring-LWE Based [L, Peikert, Regev ’10]

4. “NTRU-like” with a proof of security [Stehle, Steinfeld ‘11]
Subset Sum Problem

Subset-Sum Based [L, Palacio, Segev ‘10]

LWE-Based [Regev ‘05]

Ring-LWE Based [L, Peikert, Regev ‘10]

“NTRU-like” with a proof of security [Stehle, Steinfeld ‘11]

NTRU [Hoffstein, Pipher, Silverman ‘98]
THE SUBSET SUM PROBLEM
Subset Sum Problem

\[ a_i, \ T \text{ in } \mathbb{Z}_M \]

\[ a_i \text{ are chosen randomly} \]
\[ T \text{ is a sum of a random subset of the } a_i \]

\[ a_1 \ a_2 \ a_3 \ \ldots \ a_n \quad T \]

Find a subset of \( a_i \)'s
that sums to \( T \) (mod \( M \))
Subset Sum Problem

\[ a_i, \ T \text{ in } \mathbb{Z}_{49} \]

\( a_i \) are chosen randomly

\( T \) is a sum of a random subset of the \( a_i \)

\[
\begin{align*}
15 & \quad 31 & \quad 24 & \quad 3 & \quad 14 & \quad 11 \\
\end{align*}
\]

\[ 15 + 31 + 14 = 11 \pmod{49} \]
How Hard is Subset Sum?

\[ a_i, T \text{ in } \mathbb{Z}_M \]

\[ a_1 \ a_2 \ a_3 \ \ldots \ \ a_n \ \ T \]

Find a subset of \( a_i \)'s that sums to \( T \) (mod \( M \))

**Hardness Depends on:**

- Size of \( n \) and \( M \)
- Relationship between \( n \) and \( M \)
Complexity of Solving Subset Sum

"generalized birthday attacks"  
[FlaPrz05, Lyu06, Sha08]  

"lattice reduction attacks"  
[LagOdl85, Fri86]
Subset Sum Crypto

Why?

- simple operations
- exponential hardness
- very different from number theoretic assumptions
- resists quantum attacks
Subset Sum is “Pseudorandom”

[Impagliazzo-Naor 1989]:

For random $a_1,\ldots,a_n$ in $\mathbb{Z}_M$ and random $x_1,\ldots,x_n$ in $\{0,1\}$, distinguishing the distribution

$$(a_1,\ldots,a_n, a_1x_1+\ldots+a_nx_n \mod M)$$

from the uniform distribution $U(\mathbb{Z}_M^{n+1})$ is as hard as finding $x_1,\ldots,x_n$
What About Public-Key Encryption?

- Many early attempts
- None of them had proofs of security
- All seem to be broken
CRYPTOSYSTEM BASED ON SUBSET SUM

[L, PALACIO, SEGEV 2010]
Subset Sum Cryptosystem

- Semantically secure based on Subset Sum for $M \approx n^n$
- Main tools
  - Subset sum is pseudo-random
  - Addition in $Z_q^n$ is “kind of like” addition in $Z_M^n$ where $M=q^n$
- The proof is very simple
Facts About Addition

Want to add $4679 + 3907 + 8465 + 1343 \mod 10^4$

Adding $n$ numbers (written in base $q$) modulo $q^m \rightarrow$ carries < $n$

If $q \gg n$, then Adding with carries $\approx$ Adding without carries

(i.e. in $\mathbb{Z}_M$)  (i.e. in $\mathbb{Z}_q^n$)
So...

NOT Pseudorandom!

Pseudorandom based on Subset Sum!
Column Subset Sum Addition Is Also Pseudorandom

\[
\begin{bmatrix}
4 & 6 & 7 & 9 \\
3 & 9 & 0 & 7 \\
8 & 4 & 6 & 5 \\
1 & 6 & 4 & 3
\end{bmatrix}
+ \begin{bmatrix}
1 \\
1 \\
0 \\
1
\end{bmatrix} = \begin{bmatrix}
0 \\
9 \\
8 \\
0
\end{bmatrix}
\]
“Hybrid” Subset Sum Addition Is Also Pseudorandom
Encryption Scheme

\[ A + s = \dagger \]

Public Key

\[ \mathbb{Z}_q^{n \times n}, \{0,1\}^n \]

\[ \{0,1\}^n \]

\[ 0 + m = u \]

\[ r = \dagger \]
Encryption Scheme

\[ A + s = \dagger \]

Is pseudo-random based on the hardness of the subset sum problem.

\[ r \]

\[ A + \]

\[ + \]

\[ 0 + m = \]

\[ u + v \]
Encryption Scheme

\[ A + s = \dagger \]

\[ \text{v} = r + (A + s + m) + \text{u} \]

\[ A + s + r + m = \text{v} \]
Encryption Scheme

\[ A + s = t \]

\[ A + t = v \]

\[ u + s = r \]

\[ A + s = v - m \]

\[ 0 + m = m \]
Encryption Scheme

\[ A \cdot s + \oplus = \dagger \]

\[ + \]

\[ 0 \quad m \]

\[ = \]

\[ u \quad v \]

\[ v - u \]

\[ = \]

\[ s \]

\[ m \]

represent 0 by \( m=0 \)
represent 1 by \( m=(q-1)/2 \)
CRYPTOSYSTEM BASED ON LWE

[REGEV 2005]
Encryption Scheme
(what we needed)

A + s = t

Pseudorandom

“small”

r

0 + m = u + v
Picking the “Carries”

• In Subset Sum: carries depended on $A$ and $s$

• What if ... we pick the “carries” independently at random from some distribution?
So...

Pseudorandom based on LWE [Reg ‘05]

Pseudorandom based on Subset Sum
(Decision) LWE Problem

Theorem [Regev '05] : There is a polynomial-time quantum reduction from solving certain lattice problems in the worst-case to solving LWE.

Lemma [AppCasPeiSah] : The distribution of $s$ can be the same as $e$
LWE vs. Subset Sum

• The Subset Sum assumption has “deterministic noise”
• The LWE assumption is more “versatile”
LWE / Subset Sum Encryption

\[
A_s + \dagger = r
\]

<table>
<thead>
<tr>
<th>n-bit Encryption</th>
<th>Have</th>
<th>Want</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public Key Size</td>
<td>(\tilde{O}(n) / \bar{O}(n^2))</td>
<td>(O(n))</td>
</tr>
<tr>
<td>Secret Key Size</td>
<td>(\tilde{O}(n) / \bar{O}(n^2))</td>
<td>(O(n))</td>
</tr>
<tr>
<td>Ciphertext Expansion</td>
<td>(\tilde{O}(n) / \bar{O}(1))</td>
<td>(O(1))</td>
</tr>
<tr>
<td>Encryption Time</td>
<td>(\tilde{O}(n^3) / \bar{O}(n^2))</td>
<td>(O(n))</td>
</tr>
<tr>
<td>Decryption Time</td>
<td>(\tilde{O}(n^2))</td>
<td>(O(n))</td>
</tr>
</tbody>
</table>
“Dual” Cryptosystem

\[ A = s + t \]

\[ r + 0 = u + v \]

Anything is a valid public key – useful for IBE [GenPeiVai ‘08]
“Dual” Cryptosystem

\[
A \cdot s = t
\]

\[
v - u \cdot s = m + u \cdot v
\]

represent 0 by \( m=0 \)
represent 1 by \( m=(q-1)/2 \)
“Dual” Cryptosystem

\[ A \times s = t \]

Also, “primal” cryptosystem:
Public key is pseudorandom
Prior to seeing the public key, anything is a valid ciphertext
CRYPTOSYSTEM BASED ON RING-LWE

[L, PEIKERT, REGEV 2010]
Source of Inefficiency of LWE

Getting just one extra random-looking number requires $n$ random numbers and a small error element.

Wishful thinking: get $n$ random numbers and produce $n$ pseudo-random numbers in “one shot”
Use Polynomials

\[ f(x) \text{ is a polynomial } x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0 \]

\[ R = \mathbb{Z}_p[x]/(f(x)) \text{ is a polynomial ring with } \]
  - Addition mod \( p \)
  - Polynomial multiplication mod \( p \) and \( f(x) \)

Each element of \( R \) consists of \( n \) elements in \( \mathbb{Z}_p \)

In \( R \):
  - \( \text{small} + \text{small} = \text{small} \)
  - \( \text{small} \times \text{small} = \text{small} \) (depending on \( f(x) \) )
Ring-LWE cryptosystem

Secret Key

\[ a \ast s + \ast = \star \]

Public Key

\[ r \ast \star + \ast + m - \star \ast a + \ast \ast = v - u \ast s \]

Encryption

\[ r \ast a + \ast = u \]

\[ r \ast \star + \ast + m = v \]

Decryption

\[ r \ast \ast \ast s + \ast + \ast + m - \ast \ast a + \ast \ast = v - u \ast s \]

\[ r + \ast - \ast s + m = \ast + m \]
Security

Pseudorandom??

\[ as + \_ = \top \]
\[ ra + \_ = u \]
\[ r\top + \_ + m = v \]
Theorem [LPR ‘10]: In cyclotomic rings, there is a quantum reduction from solving worst-case problems in ideal lattices to solving Decision-RLWE
Security

Pseudorandom based on Decision Ring-LWE!!
Ring-LWE Encryption

\[
\begin{align*}
\text{a} + \text{s} & = \text{t} \\
r + \text{a} & = \text{u} \\
r + \text{t} + \text{m} & = \text{v}
\end{align*}
\]

<table>
<thead>
<tr>
<th>n-bit Encryption</th>
<th>From LWE</th>
<th>From Ring-LWE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public Key Size</td>
<td>$\tilde{O}(n) / \tilde{O}(n^2)$</td>
<td>$\tilde{O}(n)$</td>
</tr>
<tr>
<td>Secret Key Size</td>
<td>$\tilde{O}(n) / \tilde{O}(n^2)$</td>
<td>$\tilde{O}(n)$</td>
</tr>
<tr>
<td>Ciphertext Expansion</td>
<td>$\tilde{O}(n) / \tilde{O}(1)$</td>
<td>$\tilde{O}(1)$</td>
</tr>
<tr>
<td>Encryption Time</td>
<td>$\tilde{O}(n^3) / \tilde{O}(n^2)$</td>
<td>$\tilde{O}(n)$</td>
</tr>
<tr>
<td>Decryption Time</td>
<td>$\tilde{O}(n^2)$</td>
<td>$\tilde{O}(n)$</td>
</tr>
</tbody>
</table>
1-ELEMENT CRYPTO SYSTEM BASED ON RING-LWE

[STEHLE, STEINFELD 2011]
Stehle, Steinfeld Cryptosystem

\[ f + g = a \mod p \]

Uniformly random

\[ u = 2a r + m \mod p \]

Pseudorandom based on Ring-LWE

\[ u g = 2 \left[ f r + g + g m \right] \]

“small” coefficients

\[ u g \mod 2 = g m \]

\[ u g \mod 2 = m \]

\[ g \]
NTRU CRYPTO SYSTEM

[HOFFSTEIN, PIPHER, SILVERMAN 1998]
NTRU Cryptosystem

\[
\begin{align*}
\frac{f}{g} &= a \mod p \\
\text{“looks” random} \\
\text{If } a \text{ is random, then pseudorandom based on Ring-LWE} \\
ug &= 2 \left[ fr + g \right] + gm \\
\text{Since } f, g \text{ are smaller, } p \text{ can be smaller as well}
\end{align*}
\]
(Textbook) NTRU Cryptosystem / Trap-Door Function

\[
\frac{f}{g} \quad - \text{Very small}
\]

\[
\frac{f}{g} = a \mod p \quad \quad \quad \quad u = 2ar + m \mod p
\]

\[
u g = 2fr + gm
\]

\[
u g \mod 2 = gm
\]

\[
u g \mod 2 = m
\]
References

• Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman (1998): NTRU: A Ring-Based Public Key Cryptosystem
• Oded Regev (2005): On lattices, learning with errors, random linear codes, and cryptography
• Vadim Lyubashevsky, Adriana Palacio, Gil Segev (2010): Public-Key Cryptographic Primitives Provably as Secure as Subset Sum
• Vadim Lyubashevsky, Chris Peikert, Oded Regev (2010): On Ideal Lattices and Learning with Errors over Rings
• Damien Stehlé, Ron Steinfeld (2011): Making NTRU as Secure as Worst-Case Problems over Ideal Lattices