Ideal Lattices in Ring Learning with Errors (Ring-LWE)

Maria Francis, IIT Hyderabad

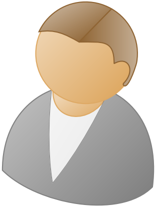
June 10, 2020

Overview

Public Key Cryptosystems

Key ingredients : A one-way function (do they exist?) and a public key K.
RSA:$K = (N, e)$

$$c = m^e \bmod N \longrightarrow$$



$$m = Dec_{K,sk}(c)$$

Alice

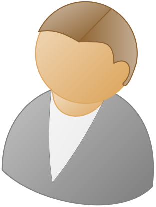
Bob

Decryption uses a trapdoor, for eg: if you know the factorization of N.

Public Key Cryptosystems

Key ingredients : A one-way function (do they exist?) and a public key K.
RSA:$K = (N, e)$

$$c = m^e \bmod N$$



$$m = Dec_{K,sk}(c)$$

Alice

Bob

Decryption uses a trapdoor, for eg: if you know the factorization of N.
RSA breaks when you have quantum computers!

Why Lattice Based Cryptography?

- Lattice problems are *conjectured* to be resistant to quantum attacks.
- Efficient representations and computations (almost linear).
- Security based on *worst-case hardness* of lattice problems –

Why Lattice Based Cryptography?

- Lattice problems are *conjectured* to be resistant to quantum attacks.
- Efficient representations and computations (almost linear).
- Security based on *worst-case hardness* of lattice problems – i.e. if one can break a *random instance* of the crypto scheme then one can solve a lattice problem on *every n-dimensional instance*.

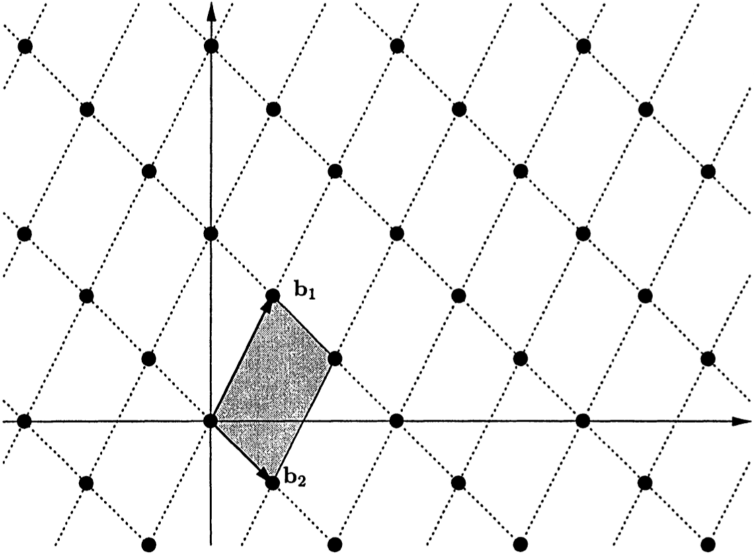
Why Lattice Based Cryptography?

- Lattice problems are *conjectured* to be resistant to quantum attacks.
- Efficient representations and computations (almost linear).
- Security based on *worst-case hardness* of lattice problems – i.e. if one can break a *random instance* of the crypto scheme then one can solve a lattice problem on *every n-dimensional instance*.
  - Everywhere else its average case assumptions.
  - Factoring from a certain distribution is hard – how should we choose this distribution?

Why Lattice Based Cryptography?

- Lattice problems are *conjectured* to be resistant to quantum attacks.
- Efficient representations and computations (almost linear).
- Security based on *worst-case hardness* of lattice problems – i.e. if one can break a *random instance* of the crypto scheme then one can solve a lattice problem on *every n-dimensional instance*.
  - Everywhere else its average case assumptions.
  - Factoring from a certain distribution is hard – how should we choose this distribution?
- Fully Homomorphic Encryption and many other "exotic" schemes!

Integer Lattices – Two Dimensional Example



Integer Lattices - Definitions

- All integral combinations of n linearly independent vectors $\mathbf{b_1}, \ldots, \mathbf{b_n}$ in $\mathbb{Z}^m$ $(m \geq n)$ is called lattice.

Integer Lattices - Definitions

- All integral combinations of n linearly independent vectors $\mathbf{b_1}, \ldots, \mathbf{b_n}$ in $\mathbb{Z}^m$ $(m \geq n)$ is called lattice.
- It is an infinite, regular, n-dimensional grid, additive subgroup of $\mathbb{Z}^n$.

Integer Lattices - Definitions

- All integral combinations of n linearly independent vectors $\mathbf{b_1}, \ldots, \mathbf{b_n}$ in $\mathbb{Z}^m$ $(m \geq n)$ is called lattice.
- It is an infinite, regular, n-dimensional grid, additive subgroup of $\mathbb{Z}^n$.
- $\mathbf{b}_i$s form a lattice basis represented as a matrix,

$$\mathbf{B} = [\mathbf{b_1}, \ldots, \mathbf{b_n}] \in \mathbb{Z}^{m \times n}.$$

Integer Lattices - Definitions

- All integral combinations of n linearly independent vectors $\mathbf{b_1}, \ldots, \mathbf{b_n}$ in $\mathbb{Z}^m$ $(m \geq n)$ is called lattice.
- It is an infinite, regular, n-dimensional grid, additive subgroup of $\mathbb{Z}^n$.
- $\mathbf{b}_i$s form a lattice basis represented as a matrix,

$$\mathbf{B} = [\mathbf{b_1}, \ldots, \mathbf{b_n}] \in \mathbb{Z}^{m \times n}.$$

- The lattice can be written as,

$$\mathcal{L}(\mathbf{B}) = \{\mathbf{Bx} : \mathbf{x} \in \mathbb{Z}^n\}.$$

One Lattice, Many Bases

The basis vectors of the previous example is :

$$\mathbf{b_1} = \begin{bmatrix} 1 \\ 2 \end{bmatrix}, \mathbf{b_2} = \begin{bmatrix} 1 \\ -1 \end{bmatrix}$$

.

One Lattice, Many Bases

The basis vectors of the previous example is :

$$\mathbf{b_1} = \begin{bmatrix} 1 \\ 2 \end{bmatrix}, \mathbf{b_2} = \begin{bmatrix} 1 \\ -1 \end{bmatrix}$$

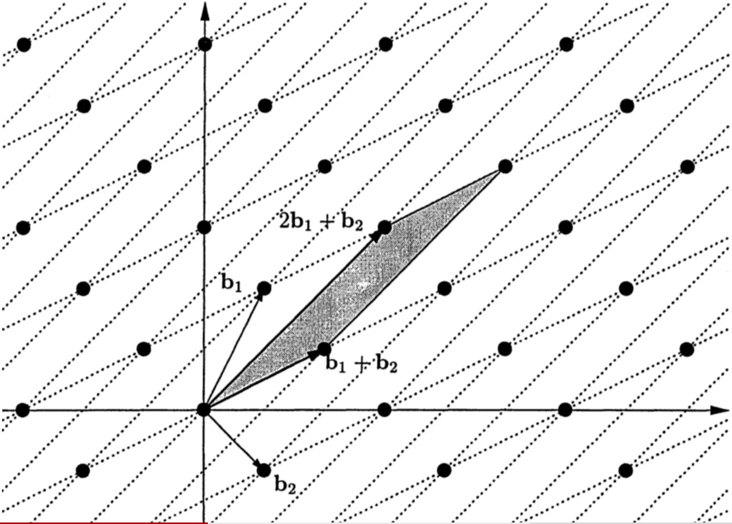
. The following vectors also generate the same lattice, $\mathcal{L}(\mathbf{b_1}, \mathbf{b_2})$

$$\mathbf{b_1}' = \mathbf{b_1} + \mathbf{b_2} = \begin{bmatrix} 2 \\ 1 \end{bmatrix}, \mathbf{b_2}' = 2\mathbf{b_1} + \mathbf{b_2} = \begin{bmatrix} 3 \\ 3 \end{bmatrix}$$

.

One Lattice, Many Bases

The grids are different, the intersection points are the same.



Lattice Invariants of $\Lambda = \mathcal{L}(\mathbf{B})$

- $det(\Lambda)$ is the n-dimensional volume of the fundamental parallelepiped $\mathcal{P}(\mathbf{B})$ spanned by basis vectors.

Lattice Invariants of $\Lambda = \mathcal{L}(\mathbf{B})$

- $det(\Lambda)$ is the n-dimensional volume of the fundamental parallelepiped $\mathcal{P}(\mathbf{B})$ spanned by basis vectors.
- Given a norm $|| \ ||$ on $\mathbb{R}^n$ (usually Euclidean norm or infinity norm):
  - $\lambda_1(\Lambda)$ is the norm of the shortest nonzero vector $v \in \Lambda$.

Lattice Invariants of $\Lambda = \mathcal{L}(\mathbf{B})$

- $det(\Lambda)$ is the n-dimensional volume of the fundamental parallelepiped $\mathcal{P}(\mathbf{B})$ spanned by basis vectors.
- Given a norm $|| \; ||$ on $\mathbb{R}^n$ (usually Euclidean norm or infinity norm):
  - $\lambda_1(\Lambda)$ is the norm of the shortest nonzero vector $v \in \Lambda$.
  - $\lambda_i(\Lambda)$ is the i-th successive minima defined as

$$\lambda_i(\Lambda) := \min_S(\max_{v \in S} ||v||),$$

where S runs over all l.i. sets $S \subset \Lambda$ with $|S| = i$.

Computational Lattice Problems

1. Shortest Vector Problem (SVP) : Find a shortest nonzero vector $v \in \Lambda$.
2. Shortest Independent Vector Problem (SIVP) : Find l.i. vectors $v_1, \ldots, v_n$ in Λ such that $\max_i ||v_i|| = \lambda_n(\Lambda)$.
3. Closest Vector Problem (CVP): given any target vector $w \in \mathbb{R}^n$ find the closest lattice point $v \in \Lambda$ to w.

Computational Lattice Problems

- There are approximation variants, SVP$_\gamma$, CVP$_\gamma$, SIVP$_\gamma$.
  Let $\gamma \geq 1$, SVP$_\gamma$: find a vector v with $||v|| \leq \gamma\lambda_1(\Lambda)$.

Computational Lattice Problems

- There are approximation variants, SVP$_\gamma$, CVP$_\gamma$, SIVP$_\gamma$.
  Let $\gamma \geq 1$, SVP$_\gamma$: find a vector v with $||v|| \leq \gamma\lambda_1(\Lambda)$.
- For "search" lattice problems, corresponding "decision" lattice problems and approx variants are there.

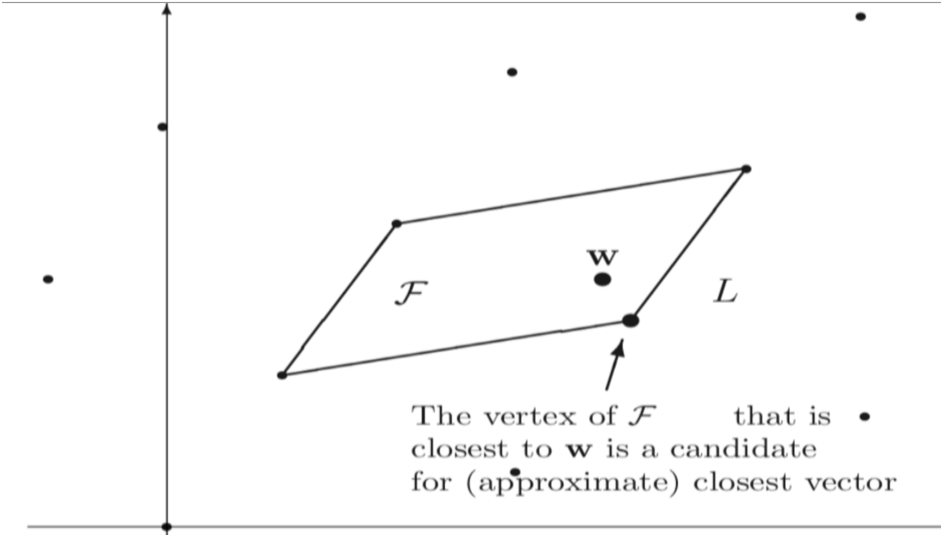
Computational Lattice Problems

- There are approximation variants, SVP$_\gamma$, CVP$_\gamma$, SIVP$_\gamma$.
  Let $\gamma \geq 1$, SVP$_\gamma$: find a vector v with $||v|| \leq \gamma\lambda_1(\Lambda)$.
- For "search" lattice problems, corresponding "decision" lattice problems and approx variants are there.
- Decision SVP : Given Λ and length d, decide if the shortest vector is shorter than d or not.

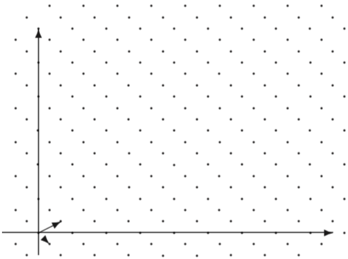
Computational Lattice Problems

- There are approximation variants, SVP$_\gamma$, CVP$_\gamma$, SIVP$_\gamma$.
  Let $\gamma \geq 1$, SVP$_\gamma$: find a vector v with $||v|| \leq \gamma\lambda_1(\Lambda)$.
- For "search" lattice problems, corresponding "decision" lattice problems and approx variants are there.
- Decision SVP : Given Λ and length d, decide if the shortest vector is shorter than d or not.
- GapSVP$_\gamma$: approximation version of the decision SVP, decide if the shortest vector is shorter than d or if it is longer than $\gamma \cdot d$.

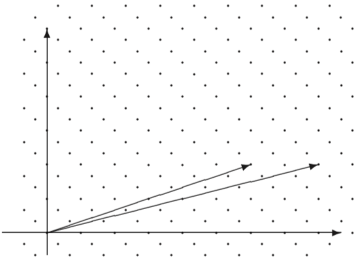
Using basis to solve CVP



A trapdoor for lattice-based cryptosystems

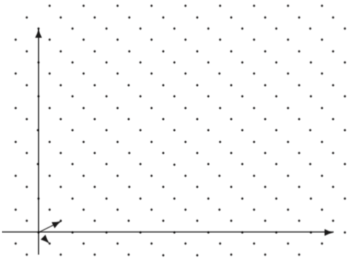


A "Good Basis"

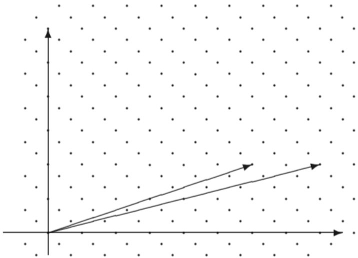


A "Bad Basis"

A trapdoor for lattice-based cryptosystems



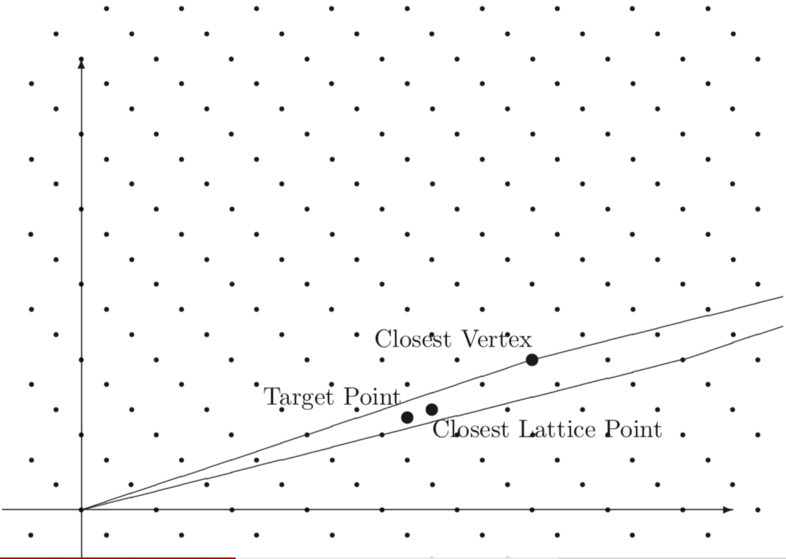
A "Good Basis"



A "Bad Basis"

Good bases : nearly orthogonal and short

A bad basis and CVP



Algorithms for Lattice Problems

- For $n = 2$, problem is very easy!
- For higher dimensions, LLL algorithm (1982) - runs in $poly(n)$ time, but the vector returned is an exponential multiple of the actual shortest vector.

Algorithms for Lattice Problems

- For $n = 2$, problem is very easy!
- For higher dimensions, LLL algorithm (1982) - runs in $poly(n)$ time, but the vector returned is an exponential multiple of the actual shortest vector.

Result

For $\gamma = poly(n)$, solving for very short vectors in high dimensions require $2^{\Omega(n)}$ time and space.

Lattice-based cryptography - Milestones

- Ajtai introduces SIS (1996) : first average case/worst case lattice problem reduction.
- Ajtai-Dwork : a PKC based on SIS
- J. Hoffstein, J. Pipher, J. H. Silverman : NTRU (1996)
- Regev (2005) : Learning with Errors problem. An efficient LWE solver implies an efficient quantum algorithm for SIVP.
- Micciancio, Lyubashevsky, (2002, 2006) : Ideal Lattices and their applications in collision resistant hash functions and digital signatures.
- Peikert, Lyubashevsky, Regev(2009,2010) : Ring-LWE
- Gentry (2009) : Fully Homomorphic Encryption

Learning With Errors [Regev '05]

- Parameters: n: dimension , q : an integer of $poly(n)$, χ : error distribution on $\mathbb{Z}$, vectors $\mathbf{a_i} \in {\mathbb{Z}_q}^n$ chosen uniformly at random.

Learning With Errors [Regev '05]

- Parameters: n: dimension , q : an integer of $poly(n)$, χ : error distribution on $\mathbb{Z}$, vectors $\mathbf{a_i} \in \mathbb{Z}_q{}^n$ chosen uniformly at random.

Given a linear system of $m \geq n$ approximate/noisy eqns, find secret $\mathbf{s} \in \mathbb{Z}_q{}^n$.

$$\langle \mathbf{a_1}, \mathbf{s} \rangle + e_1 = b_1 \pmod{q}$$
$$\langle \mathbf{a_2}, \mathbf{s} \rangle + e_2 = b_2 \pmod{q}$$
$$\vdots$$
$$\langle \mathbf{a_m}, \mathbf{s} \rangle + e_m = b_m \pmod{q}$$

Learning With Errors [Regev '05]

- Parameters: n: dimension , q : an integer of $poly(n)$, χ : error distribution on $\mathbb{Z}$, vectors $\mathbf{a_i} \in {\mathbb{Z}_q}^n$ chosen uniformly at random.

Given a linear system of $m \geq n$ approximate/noisy eqns, find secret $\mathbf{s} \in {\mathbb{Z}_q}^n$.

$$\begin{gathered}
\langle \mathbf{a_1}, \mathbf{s} \rangle + e_1 = b_1 \text{ (mod) } q \\
\langle \mathbf{a_2}, \mathbf{s} \rangle + e_2 = b_2 \text{ (mod) } q \\
\vdots \\
\langle \mathbf{a_m}, \mathbf{s} \rangle + e_m = b_m \text{ (mod) } q
\end{gathered}$$

In matrix notation,

$$\mathbf{As} + \mathbf{e} = \mathbf{b}.$$

Learning With Errors (LWE)

- Search: find $\mathbf{s} \in {\mathbb{Z}_q}^n$ given a system of $m \geq n$ noisy linear equations modulo q.

Learning With Errors (LWE)

- Search: find $\mathbf{s} \in {\mathbb{Z}_q}^n$ given a system of $m \geq n$ noisy linear equations modulo q.
- Decision: Distinguish with non-negligible probability between $\mathbf{A}, \mathbf{b} (= \mathbf{A}\mathbf{s} + \mathbf{e})$ and $\mathbf{A}, \mathbf{b}$, where $\mathbf{b}$ is chosen uniformly at random.

Learning With Errors (LWE)

- Search: find $\mathbf{s} \in {\mathbb{Z}_q}^n$ given a system of $m \geq n$ noisy linear equations modulo q.
- Decision: Distinguish with non-negligible probability between $\mathbf{A}, \mathbf{b}(= \mathbf{A}\mathbf{s} + \mathbf{e})$ and $\mathbf{A}, \mathbf{b}$, where $\mathbf{b}$ is chosen uniformly at random.
- Solving Search-LWE solves Decision-LWE. We will show that they are equivalent for q is a prime.

Error Distribution

- Number of equations is large enough for a unique solution with high probability.

Error Distribution

- Number of equations is large enough for a unique solution with high probability.
- Error too small or zero $\Rightarrow$ poly time Gaussian elimination will give solution or a very good guess.

Error Distribution

- Number of equations is large enough for a unique solution with high probability.
- Error too small or zero $\Rightarrow$ poly time Gaussian elimination will give solution or a very good guess.
- Errors too large $\Rightarrow$ more than one solution – the noise we add should be less than min distance.

Error Distribution

- Number of equations is large enough for a unique solution with high probability.
- Error too small or zero $\Rightarrow$ poly time Gaussian elimination will give solution or a very good guess.
- Errors too large $\Rightarrow$ more than one solution – the noise we add should be less than min distance.
- If the error is not randomly chosen then LWE becomes easy.

Error Distribution

- Number of equations is large enough for a unique solution with high probability.
- Error too small or zero $\Rightarrow$ poly time Gaussian elimination will give solution or a very good guess.
- Errors too large $\Rightarrow$ more than one solution – the noise we add should be less than min distance.
- If the error is not randomly chosen then LWE becomes easy.
- The typical choice for χ is discrete Gaussian -

Error Distribution

- Number of equations is large enough for a unique solution with high probability.
- Error too small or zero $\Rightarrow$ poly time Gaussian elimination will give solution or a very good guess.
- Errors too large $\Rightarrow$ more than one solution – the noise we add should be less than min distance.
- If the error is not randomly chosen then LWE becomes easy.
- The typical choice for χ is discrete Gaussian - better security but sampling in practice is non-trivial.

Discrete Gaussian

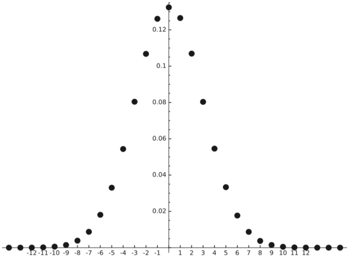
Definition

$D_{\Lambda,s}$ is a probability distribution on Λ obtained from a continuous Gaussian, that assigns mass to a lattice point that is inversely proportional to its length.

Discrete Gaussian

Definition

$D_{\Lambda,s}$ is a probability distribution on Λ obtained from a continuous Gaussian, that assigns mass to a lattice point that is inversely proportional to its length.

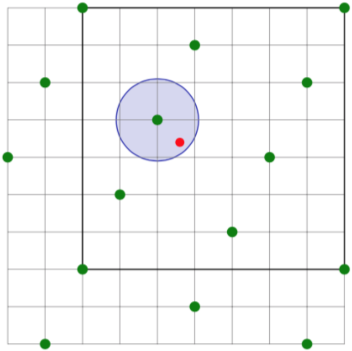


LWE as a lattice problem

- Consider $\mathcal{L}(\mathbf{A}) = \{\mathbf{z} \equiv A\mathbf{s} \bmod q\}$.

LWE as a lattice problem

- Consider $\mathcal{L}(\mathbf{A}) = \{\mathbf{z} \equiv A\mathbf{s} \bmod q\}$.
- LWE is a CVP problem on $\mathcal{L}(\mathbf{A})$: given $\mathbf{b} \approx \mathbf{v} = A\mathbf{s} \in \mathcal{L}(\mathbf{A})$, find $\mathbf{v}$.



Hardness Results of LWE [Regev'05,'09]

Theorem

Solving the LWE decision problem is at least as hard as quantumly solving SIVP$_{\gamma=poly(n)/\alpha}$ (and GapSVP$_\gamma$) on arbitrary n-dimensional lattices.

α is the error rate, $\approx (\sigma(\approx \sqrt{n} << q))/q$.

Hardness Results of LWE [Regev'05,'09]

Theorem

Solving the LWE decision problem is at least as hard as quantumly solving SIVP$_{\gamma=poly(n)/\alpha}$ (and GapSVP$_\gamma$) on arbitrary n-dimensional lattices.

α is the error rate, $\approx (\sigma(\approx \sqrt{n} << q))/q$.
Larger the error rate, smaller your gap!

Hardness Results of LWE [Regev '05,'09]

- An efficient LWE solver implies a poly-time quantum algorithm for any instance of the SIVP and GapSVP problem. – worst-case to average-case reduction.

Hardness Results of LWE [Regev '05,'09]

- An efficient LWE solver implies a poly-time quantum algorithm for any instance of the SIVP and GapSVP problem. – worst-case to average-case reduction.
- It is conjectured that there is no classical or quantum polynomial time algo that approximates GAPSVP (or SIVP) to within any poly factor $\Rightarrow$ LWE is a hard problem.

Hardness Results of LWE [Regev '05,'09]

- An efficient LWE solver implies a poly-time quantum algorithm for any instance of the SIVP and GapSVP problem. – worst-case to average-case reduction.
- It is conjectured that there is no classical or quantum polynomial time algo that approximates GAPSVP (or SIVP) to within any poly factor $\Rightarrow$ LWE is a hard problem.
- The actual reduction in (Regev '05) is in two steps:
  1. A quantum reduction from SIVP/ GapSVP to search LWE
  2. A classical reduction from Search LWE to decision LWE.

Hardness Results of LWE [Regev '05,'09]

- An efficient LWE solver implies a poly-time quantum algorithm for any instance of the SIVP and GapSVP problem. – worst-case to average-case reduction.
- It is conjectured that there is no classical or quantum polynomial time algo that approximates GAPSVP (or SIVP) to within any poly factor $\Rightarrow$ LWE is a hard problem.
- The actual reduction in (Regev '05) is in two steps:
  1. A quantum reduction from SIVP/ GapSVP to search LWE
  2. A classical reduction from Search LWE to decision LWE.
- Completely classical reductions under weaker parameters – (Peikert, '09).

Hardness Results of LWE [Regev '05,'09]

- An efficient LWE solver implies a poly-time quantum algorithm for any instance of the SIVP and GapSVP problem. – worst-case to average-case reduction.
- It is conjectured that there is no classical or quantum polynomial time algo that approximates GAPSVP (or SIVP) to within any poly factor $\Rightarrow$ LWE is a hard problem.
- The actual reduction in (Regev '05) is in two steps:
  1. A quantum reduction from SIVP/ GapSVP to search LWE
  2. A classical reduction from Search LWE to decision LWE.
- Completely classical reductions under weaker parameters – (Peikert, '09).
- The result works for $q > 2\sqrt{n}$. Open question : for smaller values of q. When q is very large ($\approx 2^{2n}$) there are attacks.

Search LWE to Decision LWE Classical Reduction

- Suppose we have an oracle $\mathcal{D}$ that solves decision LWE – distinguishes LWE samples taken from $A_{\mathbf{s},\chi}$ from uniform samples.

Search LWE to Decision LWE Classical Reduction

- Suppose we have an oracle $\mathcal{D}$ that solves decision LWE – distinguishes LWE samples taken from $A_{\mathbf{s},\chi}$ from uniform samples.
- $A_{\mathbf{s},\chi}$ - choose $\mathbf{a} \in {\mathbb{Z}_q}^n$ uniformly at random, e from χ and output $(\mathbf{a}, \langle \mathbf{a}, \mathbf{s} \rangle + e)$.
- Search LWE: To find $\mathbf{s}$.

Search LWE to Decision LWE Classical Reduction

- Suppose we have an oracle $\mathcal{D}$ that solves decision LWE – distinguishes LWE samples taken from $A_{\mathbf{s},\chi}$ from uniform samples.
- $A_{\mathbf{s},\chi}$ - choose $\mathbf{a} \in \mathbb{Z}_q{}^n$ uniformly at random, e from χ and output $(\mathbf{a}, \langle \mathbf{a}, \mathbf{s} \rangle + e)$.
- Search LWE: To find $\mathbf{s}$.
- It is enough to find $s_1 \in \mathbb{Z}_q$, other coordinates can be found similarly.

Search LWE to Decision LWE Classical Reduction

- Suppose we have an oracle $\mathcal{D}$ that solves decision LWE – distinguishes LWE samples taken from $A_{\mathbf{s},\chi}$ from uniform samples.
- $A_{\mathbf{s},\chi}$ - choose $\mathbf{a} \in \mathbb{Z}_q{}^n$ uniformly at random, e from χ and output $(\mathbf{a}, \langle \mathbf{a}, \mathbf{s} \rangle + e)$.
- Search LWE: To find $\mathbf{s}$.
- It is enough to find $s_1 \in \mathbb{Z}_q$, other coordinates can be found similarly.
- For a pair $(\mathbf{a}, b)$ choose a fresh $k \in \mathbb{Z}_q$.

Search LWE to Decision LWE Classical Reduction

- Suppose we have an oracle $\mathcal{D}$ that solves decision LWE – distinguishes LWE samples taken from $A_{\mathbf{s},\chi}$ from uniform samples.
- $A_{\mathbf{s},\chi}$ - choose $\mathbf{a} \in {\mathbb{Z}_q}^n$ uniformly at random, e from χ and output $(\mathbf{a}, \langle \mathbf{a}, \mathbf{s} \rangle + e)$.
- Search LWE: To find $\mathbf{s}$.
- It is enough to find $s_1 \in \mathbb{Z}_q$, other coordinates can be found similarly.
- For a pair $(\mathbf{a}, b)$ choose a fresh $k \in \mathbb{Z}_q$.
- Invoke $\mathcal{D}$ on pairs,

$$(\mathbf{a} + (l, 0, \ldots, 0), b + l \cdot k),$$

$l \in \mathbb{Z}_q$ chosen uniformly at random.

Search LWE to Decision LWE Reduction

- If we had the uniform distribution as input then we still have a uniform distribution

Search LWE to Decision LWE Reduction

- If we had the uniform distribution as input then we still have a uniform distribution $\Rightarrow \mathcal{D}$ rejects.

Search LWE to Decision LWE Reduction

- If we had the uniform distribution as input then we still have a uniform distribution $\Rightarrow \mathcal{D}$ rejects.
- If $k = s_1$, then we have $\langle \mathbf{a} + (l, 0, \ldots, 0), \mathbf{s} \rangle = b + l \cdot s_1$ which is the second input of the tuple

Search LWE to Decision LWE Reduction

- If we had the uniform distribution as input then we still have a uniform distribution $\Rightarrow \mathcal{D}$ rejects.
- If $k = s_1$, then we have $\langle \mathbf{a} + (l, 0, \ldots, 0), \mathbf{s} \rangle = b + l \cdot s_1$ which is the second input of the tuple $\Rightarrow \mathcal{D}$ accepts.

Search LWE to Decision LWE Reduction

- If we had the uniform distribution as input then we still have a uniform distribution $\Rightarrow \mathcal{D}$ rejects.
- If $k = s_1$, then we have $\langle \mathbf{a} + (l, 0, \ldots, 0), \mathbf{s} \rangle = b + l \cdot s_1$ which is the second input of the tuple $\Rightarrow \mathcal{D}$ accepts.
- If $k \neq s_1$, then since q is prime b is uniform

Search LWE to Decision LWE Reduction

- If we had the uniform distribution as input then we still have a uniform distribution $\Rightarrow \mathcal{D}$ rejects.
- If $k = s_1$, then we have $\langle \mathbf{a} + (l, 0, \ldots, 0), \mathbf{s} \rangle = b + l \cdot s_1$ which is the second input of the tuple $\Rightarrow \mathcal{D}$ accepts.
- If $k \neq s_1$, then since q is prime b is uniform $\Rightarrow \mathcal{D}$ rejects.

Search LWE to Decision LWE Reduction

- If we had the uniform distribution as input then we still have a uniform distribution $\Rightarrow \mathcal{D}$ rejects.
- If $k = s_1$, then we have $\langle \mathbf{a} + (l, 0, \ldots, 0), \mathbf{s} \rangle = b + l \cdot s_1$ which is the second input of the tuple $\Rightarrow \mathcal{D}$ accepts.
- If $k \neq s_1$, then since q is prime b is uniform $\Rightarrow \mathcal{D}$ rejects.
- Since $q = poly(n)$ we can try all these possibilities for k.

Search LWE to Decision LWE Reduction

- If we had the uniform distribution as input then we still have a uniform distribution $\Rightarrow \mathcal{D}$ rejects.
- If $k = s_1$, then we have $\langle \mathbf{a} + (l, 0, \ldots, 0), \mathbf{s} \rangle = b + l \cdot s_1$ which is the second input of the tuple $\Rightarrow \mathcal{D}$ accepts.
- If $k \neq s_1$, then since q is prime b is uniform $\Rightarrow \mathcal{D}$ rejects.
- Since $q = poly(n)$ we can try all these possibilities for k.
- q need not be prime or $poly(n)$ - (Peikert '09)

Efficiency of LWE

- LWE is efficient – all that we have is matrix multiplications and additions.

Efficiency of LWE

- LWE is efficient – all that we have is matrix multiplications and additions.
- Getting one $b_i \in \mathbb{Z}_q$ requires an n-dimensional mod q inner product.

Efficiency of LWE

- LWE is efficient – all that we have is matrix multiplications and additions.
- Getting one $b_i \in \mathbb{Z}_q$ requires an n-dimensional mod q inner product.
- Typically $O(n^2)$ work.

$$\begin{pmatrix} \cdots \mathbf{a_i} \cdots \end{pmatrix} \begin{pmatrix} \vdots \\ \mathbf{s} \\ \vdots \end{pmatrix} + e = b \in \mathbb{Z}_q$$

- Another issue – Rather large keys!

$$pk = \begin{pmatrix} \cdots \mathbf{a_i} \cdots \end{pmatrix}, \begin{pmatrix} \vdots \\ \mathbf{b} \\ \vdots \end{pmatrix}$$

Ring-Learning With Errors [Peikert, Lyubashevsky, Regev('09)]

Let $R = \mathbb{Z}[x]/\langle x^n + 1\rangle$ for n a power of 2.
$R_q = R/\langle q\rangle$, with q prime and $q = 1$ mod n.

R is a cyclotomic ring of integers $\mathcal{O}_K$.

Ring-Learning With Errors [Peikert, Lyubashevsky, Regev('09)]

Let $R = \mathbb{Z}[x]/\langle x^n + 1\rangle$ for n a power of 2.
$R_q = R/\langle q\rangle$, with q prime and $q = 1$ mod n.

R is a cyclotomic ring of integers $\mathcal{O}_K$.

- All elements of R_q can be uniquely represented by polynomials of $deg < n$, $R_q \cong {\mathbb{Z}_q}^n$.

Ring-Learning With Errors [Peikert, Lyubashevsky, Regev('09)]

Let $R = \mathbb{Z}[x]/\langle x^n + 1\rangle$ for n a power of 2.
$R_q = R/\langle q\rangle$, with q prime and $q = 1$ mod n.

R is a cyclotomic ring of integers $\mathcal{O}_K$.

- All elements of R_q can be uniquely represented by polynomials of $deg < n$, $R_q \cong {\mathbb{Z}_q}^n$.
- Linear representation, shorter keys

Ring-Learning With Errors [Peikert, Lyubashevsky, Regev('09)]

Let $R = \mathbb{Z}[x]/\langle x^n + 1\rangle$ for n a power of 2.
$R_q = R/\langle q\rangle$, with q prime and $q = 1$ mod n.

R is a cyclotomic ring of integers $\mathcal{O}_K$.

- All elements of R_q can be uniquely represented by polynomials of $deg < n$, $R_q \cong {\mathbb{Z}_q}^n$.
- Linear representation, shorter keys
- Operations in R_q efficient with FFT-like algorithms : $n \ log \ n$ operations $mod \ q$.

Ring-Learning With Errors [Peikert, Lyubashevsky, Regev('09)]

Let $R = \mathbb{Z}[x]/\langle x^n + 1\rangle$ for n a power of 2.
$R_q = R/\langle q\rangle$, with q prime and $q = 1$ mod n.

R is a cyclotomic ring of integers $\mathcal{O}_K$.

- All elements of R_q can be uniquely represented by polynomials of $deg < n$, $R_q \cong {\mathbb{Z}_q}^n$.
- Linear representation, shorter keys
- Operations in R_q efficient with FFT-like algorithms : $n\ log\ n$ operations $mod\ q$.
- Same ring structures used in NTRU cryptosystems.

Ring-LWE

- Search : find secret ring element $s(x) \in R_q$ given

$$a_1 \cdot s + e_1 = b_1 \in R_q$$
$$a_2 \cdot s + e_2 = b_2 \in R_q$$
$$\vdots,$$

$e_i \in R$.

Ring-LWE

- Search : find secret ring element $s(x) \in R_q$ given

$$a_1 \cdot s + e_1 = b_1 \in R_q$$
$$a_2 \cdot s + e_2 = b_2 \in R_q$$
$$\vdots,$$

$e_i \in R$. χ is over short elements in R.

Ring-LWE

- Search : find secret ring element $s(x) \in R_q$ given

$$\begin{aligned} a_1 \cdot s + e_1 &= b_1 \in R_q \\ a_2 \cdot s + e_2 &= b_2 \in R_q \\ &\vdots, \end{aligned}$$

$e_i \in R$. χ is over short elements in R. Spherically symmetric Gaussian needed!

Ring-LWE

- Search : find secret ring element $s(x) \in R_q$ given

$$\begin{aligned} a_1 \cdot s + e_1 &= b_1 \in R_q \\ a_2 \cdot s + e_2 &= b_2 \in R_q \\ &\vdots, \end{aligned}$$

  $e_i \in R$. χ is over short elements in R. Spherically symmetric Gaussian needed!

- Decision : distinguish (a_i, b_i) from uniform $(a_i, b_i) \in R_q \times R_q$.

Ideal Lattices

- Let $f \in \mathbb{Z}[x]$ be an monic irreducible polynomial of degree n.

Ideal Lattices

- Let $f \in \mathbb{Z}[x]$ be an monic irreducible polynomial of degree n.
- Consider the following $\mathbb{Z}$-module isomorphism,

$$\psi : \mathbb{Z}[x]/\langle f \rangle \longrightarrow \mathbb{Z}^n$$
$$\sum_{i=0}^{n-1} a_i x^i + \langle f \rangle \longmapsto (a_0, \cdots, a_{n-1}).$$

Ideal Lattices

- Let $f \in \mathbb{Z}[x]$ be an monic irreducible polynomial of degree n.
- Consider the following $\mathbb{Z}$-module isomorphism,

$$\psi : \mathbb{Z}[x]/\langle f \rangle \longrightarrow \mathbb{Z}^n$$
$$\sum_{i=0}^{n-1} a_i x^i + \langle f \rangle \longmapsto (a_0, \cdots, a_{n-1}).$$

> This is called coefficient embedding.

Ideal Lattices

- Let $f \in \mathbb{Z}[x]$ be an monic irreducible polynomial of degree n.
- Consider the following $\mathbb{Z}$-module isomorphism,

$$\psi : \mathbb{Z}[x]/\langle f \rangle \longrightarrow \mathbb{Z}^n$$
$$\sum_{i=0}^{n-1} a_i x^i + \langle f \rangle \longmapsto (a_0, \cdots, a_{n-1}).$$

This is called coefficient embedding.

- All $\mathbb{Z}$-submodules (including ideals) in $\mathbb{Z}[x]/\langle f \rangle$ are isomorphic to $\mathbb{Z}$-submodules/sublattices of $\mathbb{Z}^N$.

Ideal Lattices

- Let $f \in \mathbb{Z}[x]$ be an monic irreducible polynomial of degree n.
- Consider the following $\mathbb{Z}$-module isomorphism,

$$\begin{aligned} \psi : \mathbb{Z}[x]/\langle f \rangle &\longrightarrow \mathbb{Z}^n \\ \sum_{i=0}^{n-1} a_i x^i + \langle f \rangle &\longmapsto (a_0, \cdots, a_{n-1}). \end{aligned}$$

This is called coefficient embedding.

- All $\mathbb{Z}$-submodules (including ideals) in $\mathbb{Z}[x]/\langle f \rangle$ are isomorphic to $\mathbb{Z}$-submodules/sublattices of $\mathbb{Z}^N$.
- Ideals in $\mathbb{Z}[x]/\langle f \rangle$ are ideal lattices.

Hardness Results in Ideal Lattices

There is a quantum reduction from a worst case lattice problem SVP$_{\gamma=poly(n)}$ on arbitrary ideal lattices to search Ring-LWE.
There is a classical reduction from search Ring-LWE to decision Ring-LWE for any ideal lattice in cyclotomic R.

Hardness Results in Ideal Lattices

There is a quantum reduction from a worst case lattice problem SVP$_{\gamma=poly(n)}$ on arbitrary ideal lattices to search Ring-LWE.
There is a classical reduction from search Ring-LWE to decision Ring-LWE for any ideal lattice in cyclotomic R.

Results are w.r.t. ideal lattices that have more structure. But no significant difference in security proofs versus general n-dim lattices.

- Decision Ring-LWE is needed for crypto – if you can break the crypto scheme then you can distinguish (a_i, b_i) from (a_i, b_i), etc, etc.

Embedding of R

- Coefficient embedding to embed R into $\mathbb{Z}^n$.

Embedding of R

- Coefficient embedding to embed R into $\mathbb{Z}^n$.
- $+$ is coordinate wise but $\cdot$ is not that easy to analyze.

Embedding of R

- Coefficient embedding to embed R into $\mathbb{Z}^n$.
- $+$ is coordinate wise but $\cdot$ is not that easy to analyze.
- Minkowski embedding/'canonical embedding' :

Embedding of R

- Coefficient embedding to embed R into $\mathbb{Z}^n$.
- $+$ is coordinate wise but $\cdot$ is not that easy to analyze.
- Minkowski embedding/'canonical embedding' :
  - Let z be the primitive $2n$th root of unity mod q, then roots of $x^n + 1$ mod q are $z^1, z^3, \ldots, z^{2n-1}$.

Embedding of R

- Coefficient embedding to embed R into $\mathbb{Z}^n$.
- $+$ is coordinate wise but $\cdot$ is not that easy to analyze.
- Minkowski embedding/'canonical embedding' :
    - Let z be the primitive $2n$th root of unity mod q, then roots of $x^n + 1$ mod q are $z^1, z^3, \ldots, z^{2n-1}$.
    - Now we have an embedding that is $+$ and $\cdot$ coordinate-wise.

$$f(x) \longmapsto (f(z^1), f(z^3), \ldots, f(z^{2n-1}))$$

Where are we going with this?

- Why coordinate wise multiplication?

Where are we going with this?

- Why coordinate wise multiplication?Search Ring-LWE to Decision Ring-LWE reduction

Where are we going with this?

- Why coordinate wise multiplication?Search Ring-LWE to Decision Ring-LWE reduction
- In plain LWE we worked by guessing the coordinates of the secret $\mathbf{s}$ one by one.

Where are we going with this?

- Why coordinate wise multiplication?Search Ring-LWE to Decision Ring-LWE reduction
- In plain LWE we worked by guessing the coordinates of the secret $\mathbf{s}$ one by one.
- Can we guess coefficients of $s \in R_q$ one by one?

Where are we going with this?

- Why coordinate wise multiplication?Search Ring-LWE to Decision Ring-LWE reduction
- In plain LWE we worked by guessing the coordinates of the secret $\mathbf{s}$ one by one.
- Can we guess coefficients of $s \in R_q$ one by one?
- Coefficient multiplication – knowing one or more coefficients of s wont help us compute $a \cdot s \bmod qR$!

Where are we going with this?

- Why coordinate wise multiplication?Search Ring-LWE to Decision Ring-LWE reduction
- In plain LWE we worked by guessing the coordinates of the secret $\mathbf{s}$ one by one.
- Can we guess coefficients of $s \in R_q$ one by one?
- Coefficient multiplication – knowing one or more coefficients of s wont help us compute $a \cdot s \bmod qR$!
- With the new embedding we now have coordinate multiplication - $a \cdot s = (a_1 s_1, \cdots, a_n s_n)$.

What happens to the error distribution?

- Error distribution looks very different in canonical embedding!

What happens to the error distribution?

- Error distribution looks very different in canonical embedding!
- Consider $x^2 + 1$ splits modulo 13 as $x^2 + 1 = (x + 5)(x - 5)$ mod 13.

What happens to the error distribution?

- Error distribution looks very different in canonical embedding!
- Consider $x^2 + 1$ splits modulo 13 as $x^2 + 1 = (x + 5)(x - 5)$ mod 13.
- An element $ax + b$ in $\mathbb{Z}[x]/\langle x^2 + 1\rangle$ has canonical embedding

$$(5a + b, b - 5a) \in {\mathbb{Z}_{13}}^2$$

What happens to the error distribution?

- Error distribution looks very different in canonical embedding!
- Consider $x^2 + 1$ splits modulo 13 as $x^2 + 1 = (x + 5)(x - 5)$ mod 13.
- An element $ax + b$ in $\mathbb{Z}[x]/\langle x^2 + 1\rangle$ has canonical embedding

$$(5a + b, b - 5a) \in {\mathbb{Z}_{13}}^2$$

- If say our initial error distribution is uniform with $a, b \in \{-1, 0, 1\}$ then now its uniform over

$$\{(0,0), \pm(5,-5), \pm(1,1) \pm (6,-4), \pm(6,-4)\}$$

What happens to the error distribution?

- Error distribution looks very different in canonical embedding!
- Consider $x^2 + 1$ splits modulo 13 as $x^2 + 1 = (x + 5)(x - 5)$ mod 13.
- An element $ax + b$ in $\mathbb{Z}[x]/\langle x^2 + 1\rangle$ has canonical embedding

$$(5a + b, b - 5a) \in {\mathbb{Z}_{13}}^2$$

- If say our initial error distribution is uniform with $a, b \in \{-1, 0, 1\}$ then now its uniform over

$$\{(0,0), \pm(5,-5), \pm(1,1) \pm (6,-4), \pm(6,-4)\}$$

long elements relative to $q = 13$.

What happens to the error distribution?

- Error distribution looks very different in canonical embedding!
- Consider $x^2 + 1$ splits modulo 13 as $x^2 + 1 = (x + 5)(x - 5)$ mod 13.
- An element $ax + b$ in $\mathbb{Z}[x]/\langle x^2 + 1\rangle$ has canonical embedding

$$(5a + b, b - 5a) \in \mathbb{Z}_{13}{}^2$$

- If say our initial error distribution is uniform with $a, b \in \{-1, 0, 1\}$ then now its uniform over

$$\{(0, 0), \pm(5, -5), \pm(1, 1) \pm (6, -4), \pm(6, -4)\}$$

long elements relative to $q = 13$.
- We have error distributions that depend on q in very complicated ways.

Exploiting the symmetry of the canonical embedding

- Order the coordinates of the canonical embedding of $p(x) \in R_q$ as ith coordinate is $p(z^{2i-1})$.

Exploiting the symmetry of the canonical embedding

- Order the coordinates of the canonical embedding of $p(x) \in R_q$ as ith coordinate is $p(z^{2i-1})$.
- There exists a k such that the ith coordinate of $p(x)$ is the jth coordinate of $p(x^k)$!

Exploiting the symmetry of the canonical embedding

- Order the coordinates of the canonical embedding of $p(x) \in R_q$ as ith coordinate is $p(z^{2i-1})$.
- There exists a k such that the ith coordinate of $p(x)$ is the jth coordinate of $p(x^k)$!
- Define an automorphism for such a k,

$$\tau_k : R_q \to R_q, \tau_k(p(x)) := p(x^k)$$

Exploiting the symmetry of the canonical embedding

- Order the coordinates of the canonical embedding of $p(x) \in R_q$ as ith coordinate is $p(z^{2i-1})$.
- There exists a k such that the ith coordinate of $p(x)$ is the jth coordinate of $p(x^k)$!
- Define an automorphism for such a k,

$$\tau_k : R_q \to R_q, \tau_k(p(x)) := p(x^k)$$

- τ preserves norms in the coefficient embedding – $||\tau_k(p(x))|| = ||p(x^k)|| = ||p(x)||$

Search Ring-LWE to Decision Ring-LWE reduction

- $\mathcal{D}_j$ – distinguishes Ring-LWE samples with first $j-1$ coordinates (in canonical embedding) replaced by uniform random noise from samples in which j coordinates are replaced by uniform random noise.

Search Ring-LWE to Decision Ring-LWE reduction

- $\mathcal{D}_j$ – distinguishes Ring-LWE samples with first $j-1$ coordinates (in canonical embedding) replaced by uniform random noise from samples in which j coordinates are replaced by uniform random noise.
- To find s_i :
  - Compute τ_k such that the ith canonical coordinate is mapped to j.

Search Ring-LWE to Decision Ring-LWE reduction

- $\mathcal{D}_j$ – distinguishes Ring-LWE samples with first $j-1$ coordinates (in canonical embedding) replaced by uniform random noise from samples in which j coordinates are replaced by uniform random noise.
- To find s_i :
    - Compute τ_k such that the ith canonical coordinate is mapped to j.
    - Let $v_j \in R_q$ be $(0, 0, \ldots, 1, 0, \ldots, 0)$, jth position has 1,
    - $\alpha_l \in R_q$ be chosen uniformly random,
    - and k be our guess for s_i of s.

Search Ring-LWE to Decision Ring-LWE reduction

- Replace Ring-LWE samples (a_l, b_l) by

$$(\tau_k(a_l) + \alpha_l v_j, \tau_k(b_l) + k\alpha_l v_j + e_l{}'),$$

Search Ring-LWE to Decision Ring-LWE reduction

- Replace Ring-LWE samples (a_l, b_l) by

$$(\tau_k(a_l) + \alpha_l v_j, \tau_k(b_l) + k\alpha_l v_j + e_l{}').$$

- Since $\tau_k(b_l) = \tau_k(a_l)\tau_k(s_l) + \tau_k(e_l)$, the sample is

$$(\tau_k(a_l) + \alpha_l v_j, \boxed{\tau_k(a_l)\tau_k(s_l)} + k\alpha_l v_j + \boxed{\tau_k(e_l)} + e_l{}').$$

Search Ring-LWE to Decision Ring-LWE reduction

$$(\tau_k(a_l) + \alpha_l v_j, \tau_k(a_l)\tau_k(s_l) + k\alpha_l v_j + \tau_k(e_l) + {e_l}').$$

Search Ring-LWE to Decision Ring-LWE reduction

$$(\tau_k(a_l) + \alpha_l v_j, \tau_k(a_l)\tau_k(s_l) + k\alpha_l v_j + \tau_k(e_l) + e_l{}').$$

- If $k = s_i$, then the sample is for secret $\tau_k(s)$ and $\mathcal{D}_j$ accepts.

Search Ring-LWE to Decision Ring-LWE reduction

$$(\tau_k(a_l) + \alpha_l v_j, \tau_k(a_l)\tau_k(s_l) + k\alpha_l v_j + \tau_k(e_l) + e_l{}').$$

- If $k = s_i$, then the sample is for secret $\tau_k(s)$ and $\mathcal{D}_j$ accepts.
- Why?The first $j-1$ coordinates will be uniformly random.

Search Ring-LWE to Decision Ring-LWE reduction

$$(\tau_k(a_l) + \alpha_l v_j, \tau_k(a_l)\tau_k(s_l) + k\alpha_l v_j + \tau_k(e_l) + e_l{}').$$

- If $k = s_i$, then the sample is for secret $\tau_k(s)$ and $\mathcal{D}_j$ accepts.
- Why?The first $j-1$ coordinates will be uniformly random.
- Else $\mathcal{D}_j$ rejects – the jth coordinate is also uniformly random.

Search Ring-LWE to Decision Ring-LWE reduction

- What about the error in the samples with secret $\tau_k(s)$?

Search Ring-LWE to Decision Ring-LWE reduction

- What about the error in the samples with secret $\tau_k(s)$?
  - χ is spherically symmetric, depends only on norm.
  - τ_k preserves the norm.

Search Ring-LWE to Decision Ring-LWE reduction

- What about the error in the samples with secret $\tau_k(s)$?
  - χ is spherically symmetric, depends only on norm.
  - τ_k preserves the norm.
  - This implies τ_k preserves error distribution.

Search Ring-LWE to Decision Ring-LWE reduction

- What about the error in the samples with secret $\tau_k(s)$?
  - χ is spherically symmetric, depends only on norm.
  - τ_k preserves the norm.
  - This implies τ_k preserves error distribution.
- Can we move from 2^n cyclotomic polynomial rings to other univariate ideal lattices?

Search Ring-LWE to Decision Ring-LWE reduction

- What about the error in the samples with secret $\tau_k(s)$?
  - χ is spherically symmetric, depends only on norm.
  - τ_k preserves the norm.
  - This implies τ_k preserves error distribution.
- Can we move from 2^n cyclotomic polynomial rings to other univariate ideal lattices?
  - How to find an embedding that will give coordinate wise multiplication and with that a good guess for the secret?
  - The embedding should have symmetry as given by τ_k – that is rare!
  - The error distribution should be preserved.

Search Ring-LWE to Decision Ring-LWE reduction

- What about the error in the samples with secret $\tau_k(s)$?
  - χ is spherically symmetric, depends only on norm.
  - τ_k preserves the norm.
  - This implies τ_k preserves error distribution.
- Can we move from 2^n cyclotomic polynomial rings to other univariate ideal lattices?
  - How to find an embedding that will give coordinate wise multiplication and with that a good guess for the secret?
  - The embedding should have symmetry as given by τ_k – that is rare!
  - The error distribution should be preserved.
  - Other alternatives – Polynomial-LWE (Stehle, et.al 2009).

Implementations

- NewHope : Ring-LWE key exchange. About 200 bit quantum security.

Implementations

- NewHope : Ring-LWE key exchange. About 200 bit quantum security.
- Google has experimentally deployed NewHope+ECDH in Chrome canary.

Implementations

- NewHope : Ring-LWE key exchange. About 200 bit quantum security.
- Google has experimentally deployed NewHope+ECDH in Chrome canary.
- Frodo : removes the ring, just plain-lwe key exchange. Around 128-bit security.

Implementations

- NewHope : Ring-LWE key exchange. About 200 bit quantum security.
- Google has experimentally deployed NewHope+ECDH in Chrome canary.
- Frodo : removes the ring, just plain-lwe key exchange. Around 128-bit security.
- Many second round lattice-crypto entrants at the NiST PQC standardization contest.

Future Directions

- Fully classical proofs for all reductions.

Future Directions

- Fully classical proofs for all reductions.
- Other ring of integers where ring-LWE can be used.

Future Directions

- Fully classical proofs for all reductions.
- Other ring of integers where ring-LWE can be used.
- Multivariate Ideal Lattices (Francis, Dukkipati 2017) :
    - Have a characterization for multivariate ideal lattices based on coefficient mapping using Gröbner basis.

Future Directions

- Fully classical proofs for all reductions.
- Other ring of integers where ring-LWE can be used.
- Multivariate Ideal Lattices (Francis, Dukkipati 2017) :
  - Have a characterization for multivariate ideal lattices based on coefficient mapping using Gröbner basis.
  - How to extend it to build Ring-LWE? How to define the canonical embedding?

Some History

- NTRU submitted to Crypto 97 and rejected.

Some History

- NTRU submitted to Crypto 97 and rejected.
- Accepted in ANTS 98 - a biannual math conference.

Some History

- NTRU submitted to Crypto 97 and rejected.
- Accepted in ANTS 98 - a biannual math conference.
- Lattice Attacks on NTRU - Coppersmith and Shamir, Eurocrypt '97!

Some History

- NTRU submitted to Crypto 97 and rejected.
- Accepted in ANTS 98 - a biannual math conference.
- Lattice Attacks on NTRU - Coppersmith and Shamir, Eurocrypt '97!
- They even thought LLL algo will help!

Some History

- NTRU submitted to Crypto 97 and rejected.
- Accepted in ANTS 98 - a biannual math conference.
- Lattice Attacks on NTRU - Coppersmith and Shamir, Eurocrypt '97!
- They even thought LLL algo will help!
- Regev's paper came out in 2005!

Some History

- NTRU submitted to Crypto 97 and rejected.
- Accepted in ANTS 98 - a biannual math conference.
- Lattice Attacks on NTRU - Coppersmith and Shamir, Eurocrypt '97!
- They even thought LLL algo will help!
- Regev's paper came out in 2005!
- NTRU was accepted as an IEEE 13.63 standard in 2008. NiST in 2009 stated that NTRU appears to be the most practical in quantum resistant PKC.

Some History

- NTRU submitted to Crypto 97 and rejected.
- Accepted in ANTS 98 - a biannual math conference.
- Lattice Attacks on NTRU - Coppersmith and Shamir, Eurocrypt '97!
- They even thought LLL algo will help!
- Regev's paper came out in 2005!
- NTRU was accepted as an IEEE 13.63 standard in 2008. NiST in 2009 stated that NTRU appears to be the most practical in quantum resistant PKC.
- Story of resilience?

References

- On lattices, learning with errors, random linear codes, and cryptography. O. Regev (2009)
- On Ideal Lattices and Learning with Errors over Rings. V. Lyubashevsky, C. Peikert, O.Regev (2013)
- A Decade of Lattice Cryptography C. Peikert (2016)
- A Toolkit for Ring-LWE Cryptography - V.Lyubashevsky, C. Peikert, O. Regev (2013)
- Fully Homormorphic Encryption for Mathematicians – A.Silverberg (2013)
- Ring-LWE Cryptography for the Number Theorist – Y. Elias, Kristin E. Lauter, E. Ozman, K. E. Stange (2015)
- Course notes and expository lectures by Micciancio, Peikert, Vaikuntanathan.