Najmeh Soroush

Learning With Errors

Lattice Based Crypto Course June 2019

UNIVERSITÉ DU LUXEMBOURG

Outline:

- Introduction; What is LWE?
- Hardness of LWE
- Public Key Encryption Scheme with LWE
- Public Key Exchange with LWE

History of LWE

European Association for Theoretical Computer Science

About EATCS
How to Join
Organization
Bulletin
Conferences
Awards
Publications
Schools

Home
Contact
Social Media
Site Map
Members

2018 Gödel Prize

The 2018 Gödel Prize is awarded to Professor Oded Regev for his paper:

- On lattices, learning with errors, random linear codes, and cryptography Journal of the ACM, volume 56, issue 6, 2009 (preliminary version in the 37th annual Symposium on Theory of Computing, STOC 2005.)

This year the prize will be awarded at the 45th International Colloquium on Automata, Languages, and Programming to be held during July 9-13, 2018 in Prague, Czech Republic.

Regev's paper introduced the Learning With Errors (LWE) problem, and proved its average-case hardness assuming the worst-case (quantum) hardness of various well-studied problems on point lattices in Rn. It also gave an LWE-based public-key encryption scheme that is much simpler and more efficient than prior ones having similar worst-case hardness guarantees; this system has served as the foundation for countless subsequent works. Lastly, the paper introduced elegant and powerful techniques, including a beautiful quantum algorithm, for the study of lattice problems in cryptography and computational complexity. Regev's work has ushered in a revolution in cryptography, in both theory and practice. On the theoretical side, LWE has served as a simple and yet amazingly versatile foundation for nearly every kind of cryptographic object imaginable—along with many that were unimaginable until recently, and which still have no known constructions without LWE. Toward the practical end, LWE and its direct descendants are at the heart of several efficient real-world cryptosystems.

LWE-Crypto!

Standard-Crypto!

Security based on a worst-case problem

Security based on a Av-case problem

No Quantum attacks “YET”

Broken by Quantum alg

Very Simple Computations

Usually Heavy Computations, Exponentiation

RSA

$N=pq$

$(e,d)=1$ [mod $(p-1)(q-1)$]

$Pk=(N,e)$, $Sk=d$, $Enc(m,PK)=m^{e}$

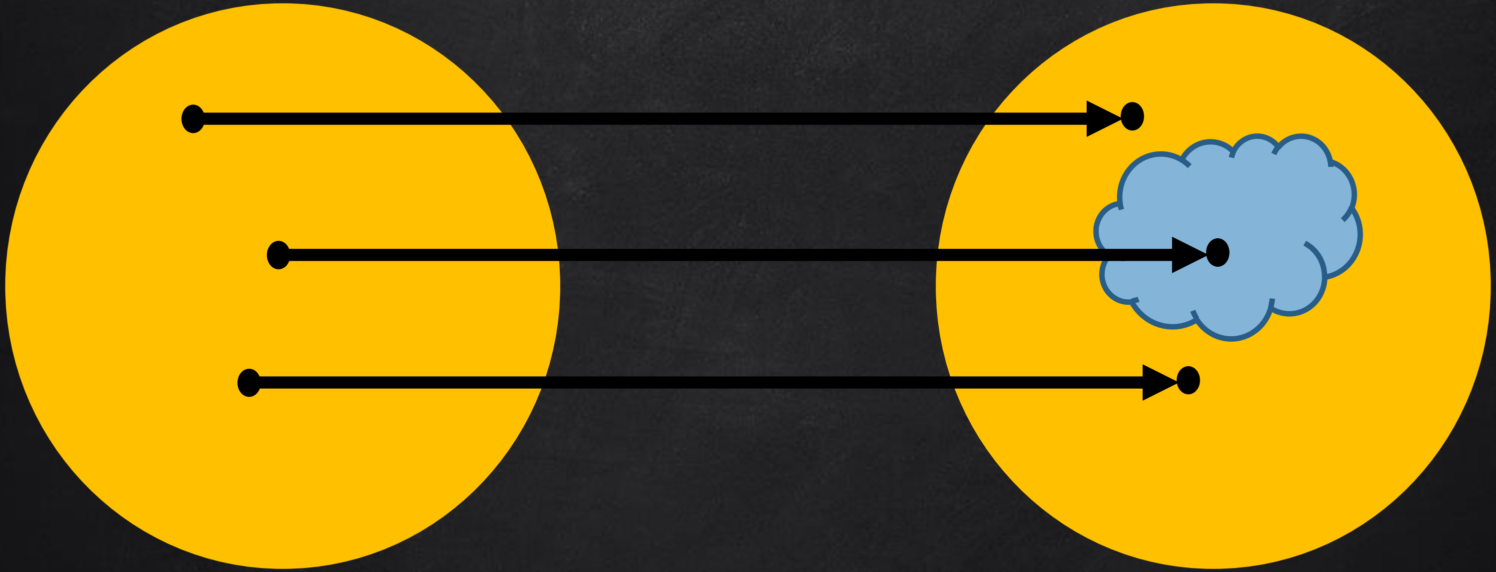
$Dec(c,SK)=c^{d}$

How do you pick a “good” , p and q in RSA?

- 1978: largest prime factors of p-1 , q-1 should be large
- 1981: largest prime factors of p+1 , q+1 should be large
- 1982: If the largest prime factor of p-1 and q-1 is p’ and q’, then p’-1 and q’-1 should have large prime factors
- 1984: If the largest prime factor of p+1 and q+1 is p’ and q’, then p’-1 and q’-1 should have large prime factors

Slide credit : Regev

Average-Case hardness

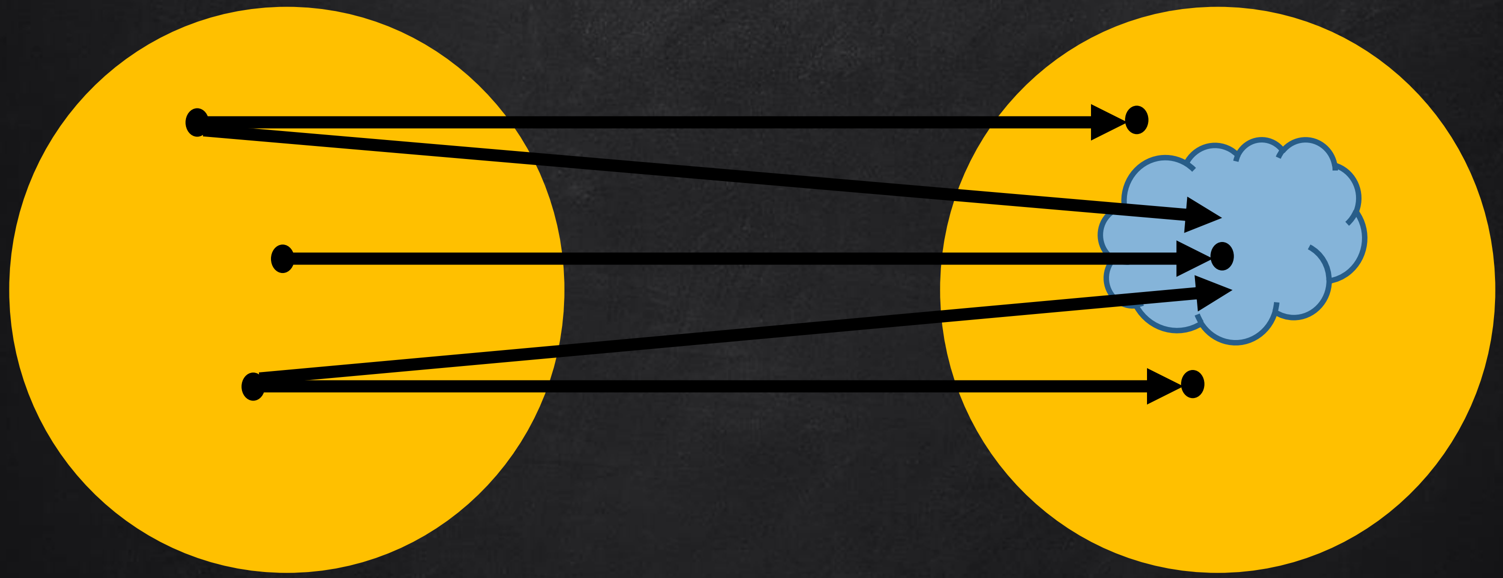


Set of all N=pq

Set of all RSA scheme

Slide credit : Regev

Worse-Case hardness

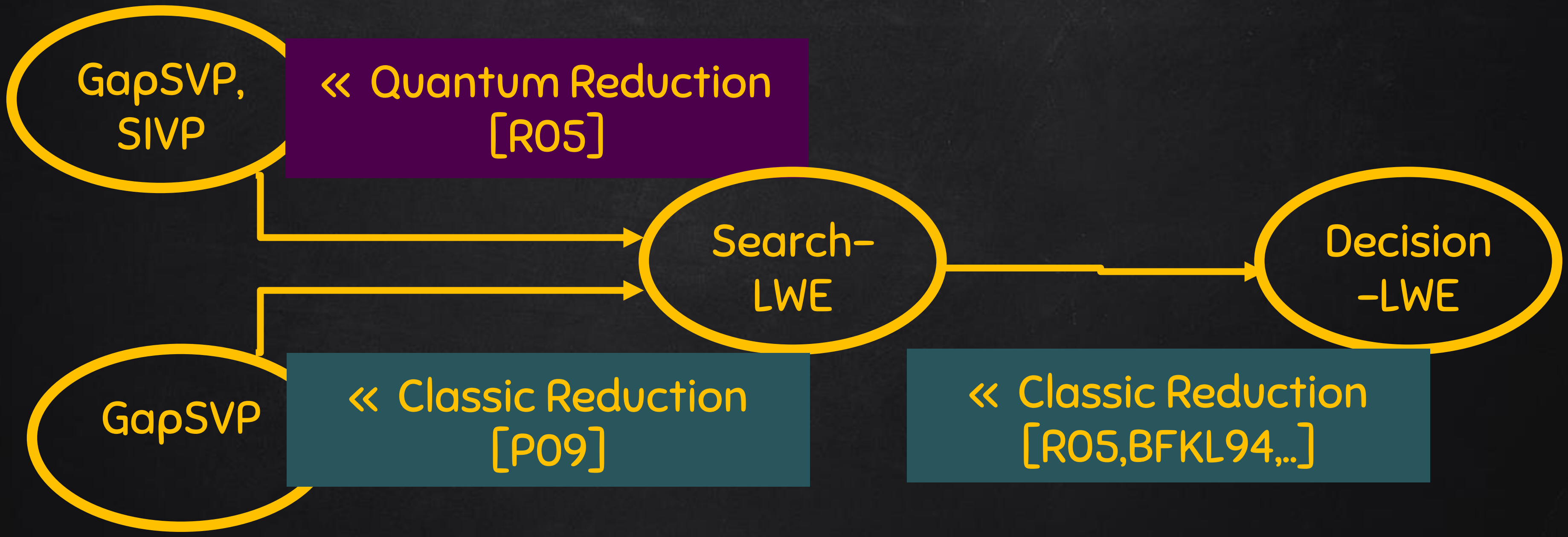


Much stronger security guarantee

It assures us that our distribution is correct

Slide credit : Oded Regev

Hardness of LWE



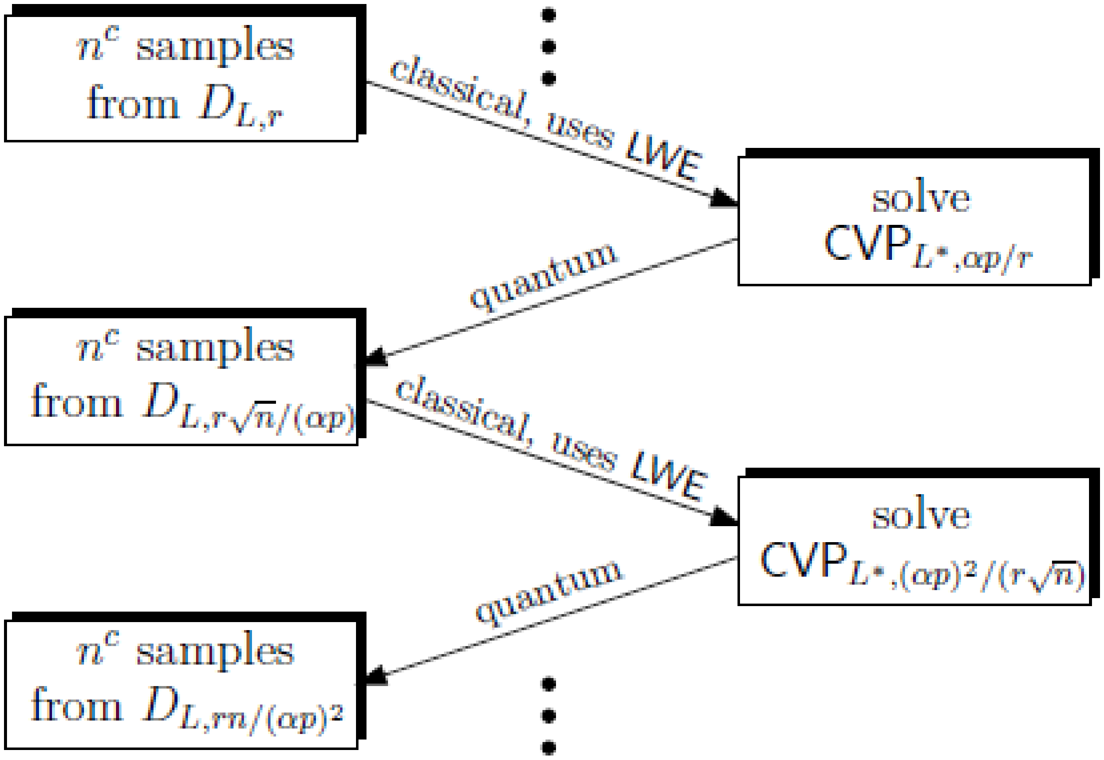


Figure 3: Two iterations of the algorithm

Learning With Errors

Najmeh Soroush

June 14, 2019

Approximate shortest vector problem

Let $\gamma \geq 1$.

Search SVP$_\gamma$

Given a lattice basis $B \in \mathbb{Z}^{m\times n}$,
find $v \in \mathcal{L}(B)$ such that $0 \neq \|v\| \leq \gamma\lambda_1(\mathcal{L}(B))$.

Optimization SVP$_\gamma$

Given a lattice basis $B \in \mathbb{Z}^{m\times n}$,
find d such that $d \leq \lambda_1(\mathcal{L}(B)) \leq \gamma d$.

Promise SVP$_\gamma$ or GapSVP$_\gamma$

Given a lattice basis $B \in \mathbb{Z}^{m\times n}$ and a rational $r \in \mathbb{Q}$,
determine whether (B, r) belongs to the YES instance (=$\lambda_1(\mathcal{L}(B)) \leq r$) or to the NO instance ($\lambda_1(\mathcal{L}(B)) > \gamma r$).

Surprisingly:

$$\text{Search SVP}_\gamma \Rightarrow \text{Optimization SVP}_\gamma \Leftrightarrow \text{Promise SVP}_\gamma$$

Closest vector problem

Let $\gamma \geq 1$.

Search CVP$_\gamma$

Given a lattice basis $B \in \mathbb{Z}^{m \times n}$ and a vector $t \in \mathbb{Z}^m$,
find $v \in \mathcal{L}(B)$ such that $\|v - t\| \leq \gamma dist(t, \mathcal{L}(B))$.

Optimization CVP$_\gamma$

Given a lattice basis $B \in \mathbb{Z}^{m \times n}$ and a vector $t \in \mathbb{Z}^m$,
find d such that $d \leq dist(t, \mathcal{L}(B)) \leq \gamma d$.

Promise CVP$_\gamma$ or GapCVP$_\gamma$

Given a lattice basis $B \in \mathbb{Z}^{m \times n}$, a rational $r \in \mathbb{Q}$ and a vector $t \in \mathbb{Z}^m$,
determine whether (B, r, t) belongs to the YES instance (=$dist(t, \mathcal{L}(B)) \leq r$) or to the NO instance ($= dist(t, \mathcal{L}(B)) > \gamma r$).

Miscellaneous lattice problems

SIVP

Given a lattice basis $B \in \mathbb{Z}^{m \times n}$,
find n linearly independent vectors $v_1, ..., v_n \in \mathcal{L}(B)$ such that $0 \neq \|v_i\| \leq \gamma \lambda_i(\mathcal{L}(B))$.

Bounded distance decoding

Given a lattice basis $B \in \mathbb{Z}^{m \times n}$ and a vector $t \in \mathbb{Z}^m$ such that $dist(t, \mathcal{L}(B)) < \dfrac{\lambda_1(\mathcal{L}(B))}{n}$ for a given $n \in \mathbb{N}$,
find $v \in \mathcal{L}(B)$ such that $\|v - t\| < \dfrac{\lambda_1(dist(t, \mathcal{L}(B)))}{n}$.

Covering radius problem

Given a lattice basis $B \in \mathbb{Z}^{m \times n}$,
find the largest distance from any vector to the lattice.

Learning With Errors: Search Version

Oracle $\mathcal{O}_s^n$ which outputs samples of the form $(\mathbf{a}, \langle \mathbf{s}, \mathbf{a} \rangle + e)$,

- $\mathbf{a} \xleftarrow{\$} \mathbb{Z}_q^n$ is chosen freshly at random for each sample.
- $\mathbf{s} \in \mathbb{Z}_q^n$ is the "secret" (and it is the same for every sample).
- $e \xleftarrow{\$} \chi$ (noise distribution- usually is discrete Gaussian over $\mathbb{Z}$) is chosen freshly according to χ for each sample and $|e| \leq B << q$.

Definition

The search-LWE problem: Find the secret $\mathbf{s}$ given access to $\mathcal{O}_s^n$.

Definition

$\mathsf{LWE}_{n,q,\chi}$ assumption:

For any PPT algorithm $\mathcal{A}$: $\Pr\left[\mathcal{A}^{\mathcal{O}_s^n}(1^n) = \mathbf{s}\right] = \text{negligible}(n)$

Learning With Errors: Decision Version

Oracle $\mathcal{O}_s^n$ which outputs samples of the form $(a, \langle s, a\rangle + e)$, $\mathcal{R}$ an oracle which outputs uniformly random samples $(a, b) \xleftarrow{\$} \mathbb{Z}_q^n \times \mathbb{Z}_q$.

Definition

Decisional $\mathsf{LWE}_{n,q,\chi}$ assumption:
For any PPT algorithm $\mathcal{A}$:

$$\left|\Pr\left[\mathcal{A}^{\mathcal{O}_s^n}(1^n) = 1\right] - \Pr\left[\mathcal{A}^{\mathcal{R}}(1^n) = 1\right]\right| = \text{negligible}(n)$$

Learning With Errors; Notation

- n : dimension, security parameter
- Our Universe is $\mathbb{Z}^n, \mathbb{Z}_q^n$, for some $q \geq 2$
- $\mathbf{s} = (s_1, s_2, \ldots, s_n) \in \mathbb{Z}_q^n$
- $\mathbf{a}_i = (a_{i1}, a_{i2}, \ldots, a_{in}) \in \mathbb{Z}_q^n, i = 1, \ldots, m$
- $\mathbf{e} = (e_1, e_2, \ldots, e_m) \in \mathbb{Z}_q^m$
- $\mathbf{b} = (b_1, b_2, \ldots, b_m)$
- $\alpha << 1$: error rate such that $\alpha q > \sqrt{n}$

Learning With Errors; Notation

$$\begin{cases} s_1 a_{11} + s_2 a_{12} + \ldots + s_n a_{1n} + e_1 = b_1 \\ s_1 a_{21} + s_2 a_{22} + \ldots + s_n a_{2n} + e_2 = b_2 \\ \vdots \\ s_1 a_{m1} + s_2 a_{m2} + \ldots + s_n a_{mn} + e_m = b_m \end{cases}, \begin{cases} \langle \mathbf{s}, \mathbf{a}_1 \rangle + e_1 = b_1 \\ \langle \mathbf{s}, \mathbf{a}_2 \rangle + e_2 = b_2 \\ \vdots \\ \langle \mathbf{s}, \mathbf{a}_m \rangle + e_m = b_m \end{cases}$$

$$A = \begin{bmatrix} | & | & & | \\ \mathbf{a}_1 & \mathbf{a}_2 & \ldots & \mathbf{a}_m \\ | & | & & | \end{bmatrix} \Rightarrow \mathbf{b}^t = \mathbf{s}^t A + \mathbf{e}^t$$

Decisional-LWE Versus SIS

SIS: Find a short vector $z \neq 0$ such that $Az = 0$.

- LWE $\leq$ SIS
- LWE has more application that SIS

Some properties of LWE

- Check a candidate solution $s' \in \mathbb{Z}_q^n$
- Shift the secret
- Random self-reduction
- Multiple secret: $(a, \langle s_1, a\rangle + e_1, \langle s_2, a\rangle + e_2, \dots, \langle s_k, a\rangle + e_k)$

Theorem

If there is an efficient solver for decisional $\mathsf{LWE}_{n,m,q,\chi}$*, then there is an efficient solver for search* $\mathsf{LWE}_{n,m',q,\chi}$*, where* $m' = O(\frac{nmq}{\epsilon^2})$

Theorem

LWE is no easier if the secret is drawn from the error distribution χ^n

Public-Key Encryption Scheme[R05]

Alice

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

Bob

$s \xleftarrow{\$} \mathbb{Z}_q^n$:secret key

$e \xleftarrow{\$} \mathbb{Z}_q^m$

$b^t = s^t A + e^t$

$\xrightarrow{\text{Public key: } b^t}$

$x \xleftarrow{\$} \{0,1\}^m$

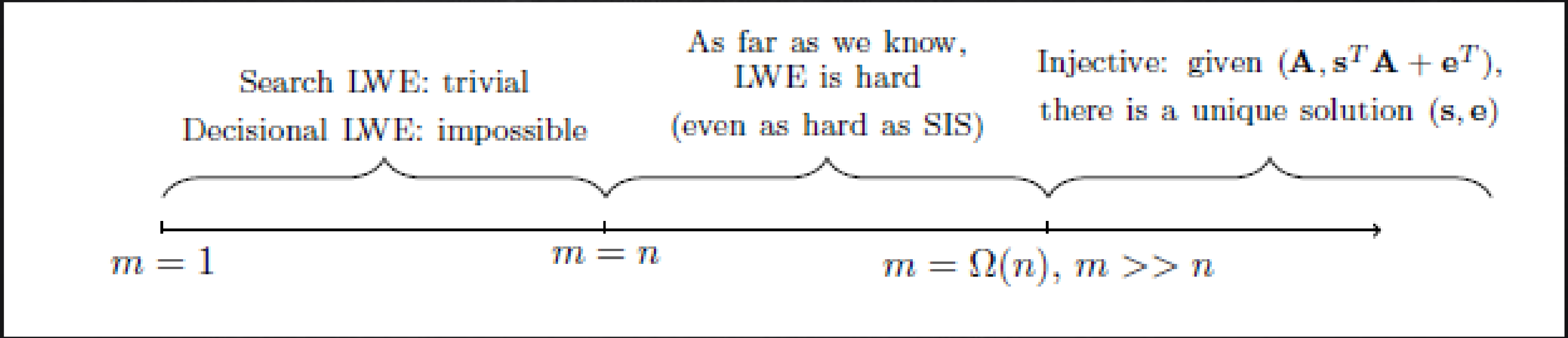
$u = Ax$

$u' = b^t x + bit \cdot \frac{q}{2}$

$\xleftarrow{\text{CT}=(u,u')}$

$u' - s^t u$

For which values of m is the LWE problem hard?



Secret Key Encryption from LWE

- $\mathsf{SKE.KeyGen}(1^n)$ takes as input the security parameter n and outputs a secret key $sk = \mathbf{s} \leftarrow \mathbb{Z}_q^n$.
- $\mathsf{SKE.Enc}(sk = \mathbf{s}, \mu)$ takes as input a secret key $\mathbf{s}$ and a message $\mu \in \{0, 1\}$, and outputs a ciphertext

$$(\mathbf{a}, \langle \mathbf{a}, \mathbf{s} \rangle + e + \mu \cdot \lceil q/2 \rceil),$$

where $\mathbf{a} \leftarrow \mathbb{Z}_q^n$ and $e \leftarrow \chi$ are sampled afresh for each ciphertext.

- $\mathsf{SKE.Dec}(sk = \mathbf{s}, (\mathbf{a}, b))$ takes as input a secret key $\mathbf{s}$ and a ciphertext $(\mathbf{a}, b)$, and outputs a decryption:

$$\mu' := \begin{cases} 0 & \text{if } ||b - \langle \mathbf{a}, \mathbf{s} \rangle|| < q/4 \\ 1 & \text{otherwise.} \end{cases}$$

Public Key Encryption from LWE

- PKE.KeyGen(1^n) takes as input the security parameter n, samples $\mathbf{A} \leftarrow \mathbb{Z}_q^{n \times m}$ and $\mathbf{e} \leftarrow \chi^m$, and outputs a key-pair (pk, sk) where $sk = \mathbf{s} \leftarrow \mathbb{Z}_q^n$ and $pk = (\mathbf{A}, \mathbf{s}^T\mathbf{A} + \mathbf{e}^T)$.

- PKE.Enc($pk = (\mathbf{A}, \mathbf{b}^T), \mu$) takes as input a public key $(\mathbf{A}, \mathbf{b}^T)$ and a message $\mu \in \{0, 1\}$, samples a short vector $\mathbf{r} \leftarrow \{0, 1\}^m$, and outputs a ciphertext

$$(\mathbf{A}\mathbf{r}, \mathbf{b}^T\mathbf{r} + \mu \cdot \lceil q/2 \rceil).$$

- PKE.Dec($sk = \mathbf{s}, (\mathbf{u}, v)$) takes as input a secret key $\mathbf{s}$ and a ciphertext $(\mathbf{u}, v)$, and outputs a decryption:

$$\mu' := \begin{cases} 0 & \text{if } ||v - \mathbf{s}^T\mathbf{u}|| < q/4 \\ 1 & \text{otherwise.} \end{cases}$$

Public Key Encryption from LWE- Security Proof

Hybrid 1

- $pk = (\mathbf{A}, \mathbf{b}^T) = (\mathbf{A}, \mathbf{s}^T\mathbf{A} + \mathbf{e}^T)$ for $\mathbf{A} \leftarrow \mathbb{Z}_q^{n\times m}$, $\mathbf{s} \leftarrow \mathbb{Z}_q^n$, $\mathbf{e} \leftarrow \chi^m$
- $ct = \mathsf{PKE.Enc}(pk, 0) = (\mathbf{Ar}, \mathbf{b}^T\mathbf{r})$ for random $\mathbf{r} \leftarrow \{0,1\}^m$

Hybrid 2

- $pk = (\mathbf{A}, \mathbf{b}^T)$ for $\mathbf{A} \leftarrow \mathbb{Z}_q^{n\times m}$ and random $\mathbf{b} \leftarrow \mathbb{Z}_q^m$
- $ct = \mathsf{PKE.Enc}(pk, 0) = (\mathbf{Ar}, \mathbf{b}^T\mathbf{r})$ for random $\mathbf{r} \leftarrow \{0,1\}^m$

LWE- Assumption

Public Key Encryption from LWE- Security Proof

Hybrid 2

- $pk = (\mathbf{A}, \mathbf{b}^T)$ for $\mathbf{A} \leftarrow \mathbb{Z}_q^{n \times m}$ and random $\mathbf{b} \leftarrow \mathbb{Z}_q^m$
- $ct = \mathsf{PKE.Enc}(pk, 0) = (\mathbf{Ar}, \mathbf{b}^T\mathbf{r})$ for random $\mathbf{r} \leftarrow \{0,1\}^m$

Hybrid 3

- $pk = (\mathbf{A}, \mathbf{b}^T)$ for $\mathbf{A} \leftarrow \mathbb{Z}_q^{n \times m}$ and random $\mathbf{b} \leftarrow \mathbb{Z}_q^m$
- $ct = (\mathbf{u}, v) \leftarrow \mathbb{Z}_q^n \times \mathbb{Z}_q$

Left Over Hash Lemma

Public Key Encryption from LWE- Security Proof

Hybrid 3

- $pk = (\mathbf{A}, \mathbf{b}^T)$ for $\mathbf{A} \leftarrow \mathbb{Z}_q^{n \times m}$ and random $\mathbf{b} \leftarrow \mathbb{Z}_q^m$
- $ct = (\mathbf{u}, v) \leftarrow \mathbb{Z}_q^n \times \mathbb{Z}_q$

Hybrid 4

- $pk = (\mathbf{A}, \mathbf{b}^T)$ for $\mathbf{A} \leftarrow \mathbb{Z}_q^{n \times m}$ and random $\mathbf{b} \leftarrow \mathbb{Z}_q^m$
- $ct = \mathsf{PKE.Enc}(pk, 1) = (\mathbf{Ar}, \mathbf{b}^T\mathbf{r} + \lceil q/2 \rfloor)$ for random $\mathbf{r} \leftarrow \{0,1\}^m$

Left Over Hash Lemma

Public Key Encryption from LWE- Security Proof

Hybrid 4

- $pk = (\mathbf{A}, \mathbf{b}^T)$ for $\mathbf{A} \leftarrow \mathbb{Z}_q^{n\times m}$ and random $\mathbf{b} \leftarrow \mathbb{Z}_q^m$
- $ct =$ $\mathsf{PKE.Enc}(pk, 1) = (\mathbf{A}\mathbf{r}, \mathbf{b}^T\mathbf{r} + \lceil q/2 \rfloor)$ for random $\mathbf{r} \leftarrow \{0,1\}^m$

Hybrid 5

- $pk = (\mathbf{A}, \mathbf{b}^T) = (\mathbf{A}, \mathbf{s}^T\mathbf{A} + \mathbf{e}^T)$ for $\mathbf{A} \leftarrow \mathbb{Z}_q^{n\times m}$, $\mathbf{s} \leftarrow \mathbb{Z}_q^n$, $\mathbf{e} \leftarrow \chi^m$
- $ct = \mathsf{PKE.Enc}(pk, 1) = (\mathbf{A}\mathbf{r}, \mathbf{b}^T\mathbf{r} + \lceil q/2 \rfloor)$ for random $\mathbf{r} \leftarrow \{0,1\}^m$

LWE- Assumption

Public Key Encryption from LWE- Security Proof

Hybrid 1

- $pk = (\mathbf{A}, \mathbf{b}^T) = (\mathbf{A}, \mathbf{s}^T\mathbf{A} + \mathbf{e}^T)$ for $\mathbf{A} \leftarrow \mathbb{Z}_q^{n\times m}$, $\mathbf{s} \leftarrow \mathbb{Z}_q^n$, $\mathbf{e} \leftarrow \chi^m$
- $ct = \mathsf{PKE.Enc}(pk, 0) = (\mathbf{Ar}, \mathbf{b}^T\mathbf{r})$ for random $\mathbf{r} \leftarrow \{0,1\}^m$

Hybrid 2

- $pk = (\mathbf{A}, \mathbf{b}^T)$ for $\mathbf{A} \leftarrow \mathbb{Z}_q^{n\times m}$ and random $\mathbf{b} \leftarrow \mathbb{Z}_q^m$
- $ct = \mathsf{PKE.Enc}(pk, 0) = (\mathbf{Ar}, \mathbf{b}^T\mathbf{r})$ for random $\mathbf{r} \leftarrow \{0,1\}^m$

Hybrid 3

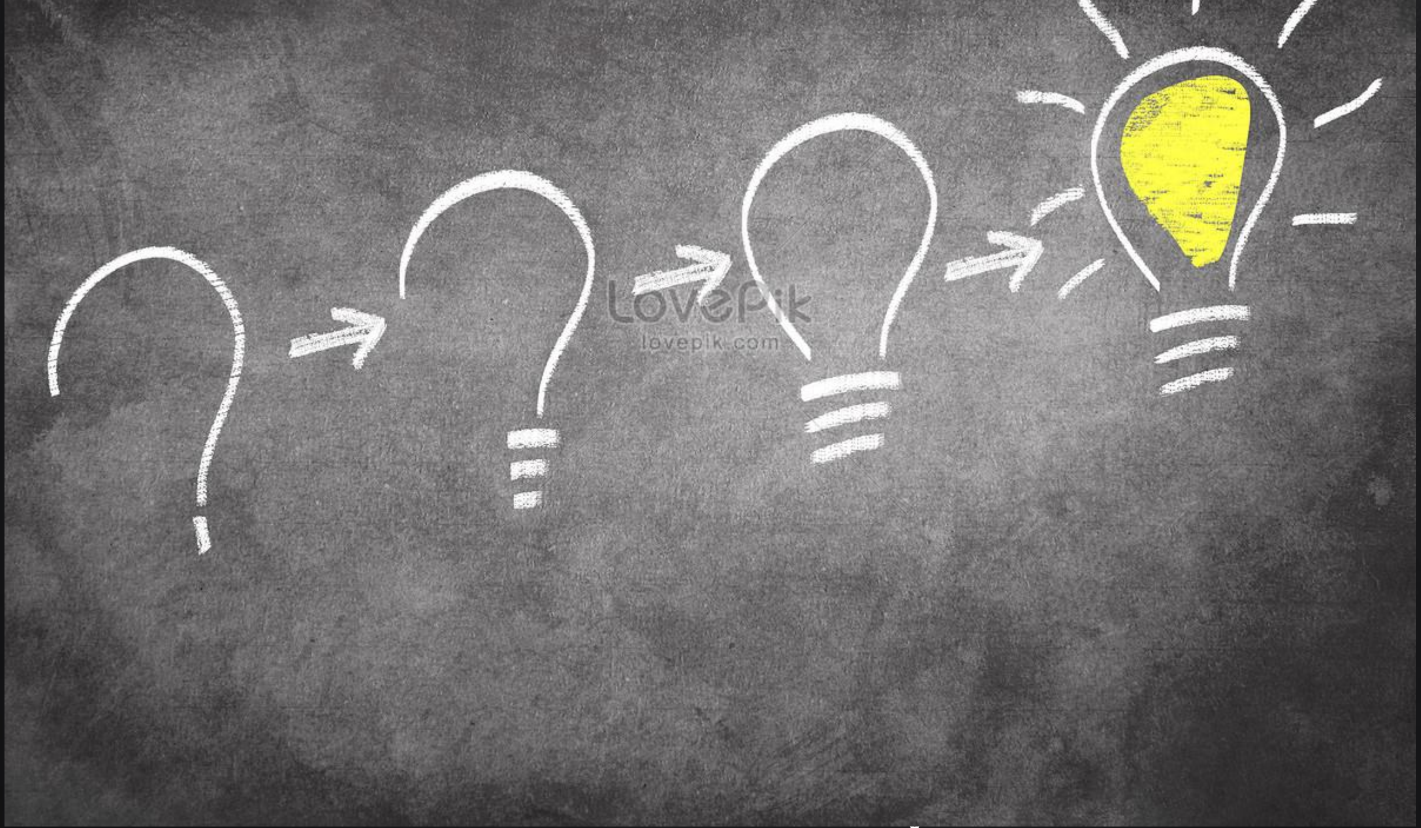
- $pk = (\mathbf{A}, \mathbf{b}^T)$ for $\mathbf{A} \leftarrow \mathbb{Z}_q^{n\times m}$ and random $\mathbf{b} \leftarrow \mathbb{Z}_q^m$
- $ct = (\mathbf{u}, v) \leftarrow \mathbb{Z}_q^n \times \mathbb{Z}_q$

Hybrid 4

- $pk = (\mathbf{A}, \mathbf{b}^T)$ for $\mathbf{A} \leftarrow \mathbb{Z}_q^{n\times m}$ and random $\mathbf{b} \leftarrow \mathbb{Z}_q^m$
- $ct = \mathsf{PKE.Enc}(pk, 1) = (\mathbf{Ar}, \mathbf{b}^T\mathbf{r} + \lceil q/2 \rceil)$ for random $\mathbf{r} \leftarrow \{0,1\}^m$

Hybrid 5

THANKS!



Dual Public-Key Encryption Scheme[GPV08]

Alice

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

Bob

$x \xleftarrow{\$} \{0,1\}^m$

$\xrightarrow{\text{Public key: } u=Ax}$

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

$$\mathbf{b}^t = \mathbf{s}^t A + \mathbf{e}^t$$

$$b' = s^t u + e' + bit \cdot \frac{q}{2}$$

$\xleftarrow{\text{CT}=(b^t, b')}$

Key Exchange from LWE[R05]

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

Alice		Bob
$s, e_1 \xleftarrow{\$} \mathbb{Z}^n$		$r, e_2 \xleftarrow{\$} \mathbb{Z}^n$
$u^t = s^t \cdot A + e_1$		$v = A \cdot r^t + e_2$
	$\xrightarrow{u^t}$	
	$\xleftarrow{v}$	
$k = s^t v + Error$		
		$k = s^t \cdot r + Error$

THANKS!