Public-Key Encryption and Injective Trapdoor Functions from LWE with Large Noise Rate

<u>Liheng Ji</u> Yilei Chen

Tsinghua University, Shanghai Qi Zhi Institute

Learning with errors

·So far, most cryptographic primitives from LWE require the noise rate $\alpha < o(1/\left(\sqrt{n}\log n\right))$.

·public-key encryption schemes [Reg05]
·Trapdoor functions [MP11]
·fully homomorphic encryption [BV11, GSW13],
……

·What if LWE under this setting is not secure?

Try LWE with larger noise rates!

01

Background

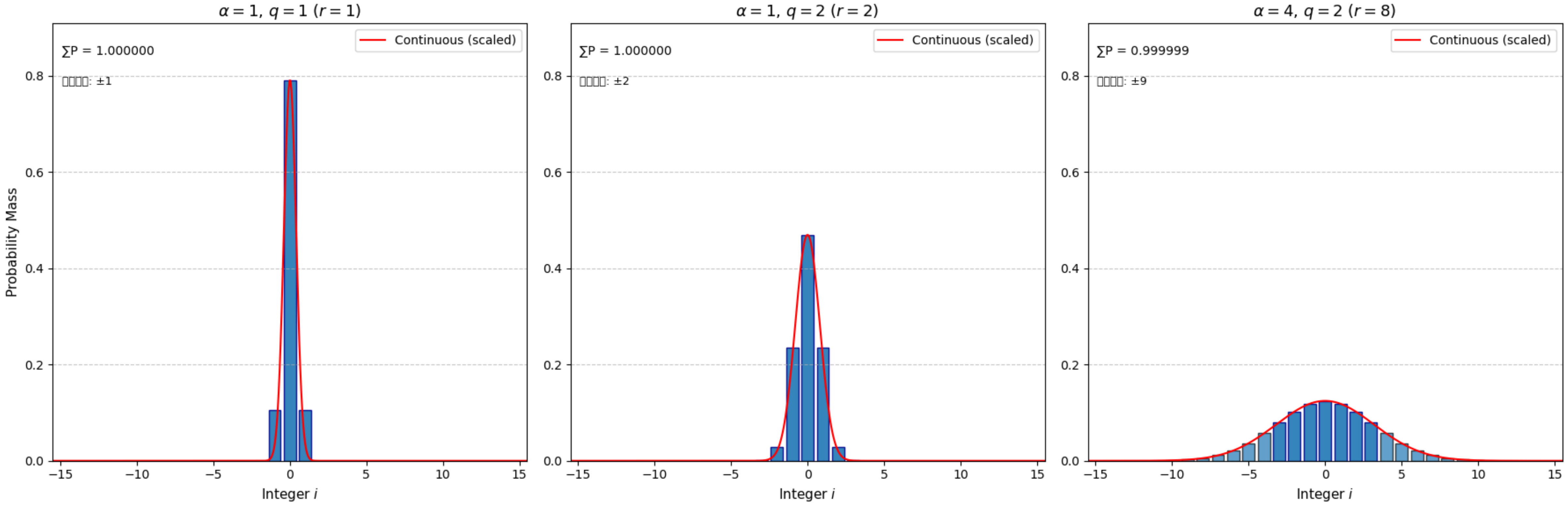
Introduction to LWE

Discrete Gaussian distribution

Tsinghua University

Continuous Gaussian: $\forall\, x \in \mathbf{R},\ D_r(x) := \dfrac{e^{-\pi x^2/r^2}}{r}.\quad (r \in \mathbf{R}^+)$

Discrete Gaussian: $\forall\, i \in \mathbf{Z}, \Psi_{\alpha,q}(i) := \displaystyle\int^{x=i+1/2} D_{\alpha q}(x)\mathrm{d}x\ (q \in \mathbf{Z},\ q \geq 2,\ \alpha \in \mathbf{R}^+)$



When $r \to \infty$, this distribution is almost uniform.
When $r \to 0$, this distribution tends to be identically zero.

Learning with errors (LWE)

Tsinghua University

$\boldsymbol{s} \in \mathbf{Z}_q^n, \forall i \in [1,m]$: $\boldsymbol{a}_i \leftarrow \mathbf{Z}_q^n$, $e_i \leftarrow \Psi_{\alpha,q}$, $b_i := \left(\left\langle \boldsymbol{a}_i, \boldsymbol{s} \right\rangle + e_i\right) \bmod q$. Given $\left\{\left(\boldsymbol{a}_i, b_i\right)\right\}_i$, solve $\boldsymbol{s}$.

$\alpha > 0$: the noise rate

$$\begin{aligned} \left\langle \boldsymbol{a}_1, \boldsymbol{s} \right\rangle + e_1 &\equiv b_1 \pmod q \\ \left\langle \boldsymbol{a}_2, \boldsymbol{s} \right\rangle + e_2 &\equiv b_2 \pmod q \\ &\cdots \\ \left\langle \boldsymbol{a}_m, \boldsymbol{s} \right\rangle + e_m &\equiv b_m \pmod q \end{aligned}$$

When $\alpha \to 0$, e_i tends to be identically zero, and $\boldsymbol{s}$ can be solved by Gaussian elimination.
When $\alpha \to \infty$, e_i is almost uniform, and it's hard to solve $\boldsymbol{s}$.
When α is neither large nor small (most commonly $\alpha < o(1/\left(\sqrt{n}\log n\right))$), LWE can be use in cryptography:

- ·public-key encryption schemes [Reg05]
- ·signatures [GPV08]
- ·fully homomorphic encryption [BV11, GSW13],
- ·identity-based encryption [GPV08]
- ·attribute-based encryption [GVW13]
- ……

(t, ϵ)-hardness of decision LWE

Let n be the security parameter. Let $q = q(n)$ be a prime modulus. Let $m = m(n),\ \alpha = \alpha(n), t = t(n), \epsilon = \epsilon(n)$. We say the decision $\mathrm{LWE}(n, q, \alpha)$ is (t, ϵ)-hard if for every distinguisher $\mathcal{D}$ of running time t,

$$\left| \Pr_{\boldsymbol{A} \leftarrow \mathbf{Z}_q^{n\times m}, \boldsymbol{s} \leftarrow \mathbf{Z}_q^n, \boldsymbol{e} \leftarrow \Psi_{\alpha,q}^m} [\mathrm{D}\left(\boldsymbol{A}, \boldsymbol{A}^T \boldsymbol{s} + \boldsymbol{e}\right) = 1] - \Pr_{\boldsymbol{A} \leftarrow \mathbf{Z}_q^{n\times m}} [\mathrm{D}\left(\boldsymbol{A}, \mathrm{U}_q\right) = 1] \right| < \epsilon\,.$$

When $t = n^{\omega(1)}$ and $\epsilon = n^{-\omega(1)}$, we omit (t, ϵ) and simply say the decision LWE problem is hard.

02

Main Results

PKE and iTDF from Large Noise LWE

Result: PKE from Large Noise LWE

[Reg05]:

For some prime $q \in \mathrm{poly}(n)$, there exists a public-key encryption (PKE) scheme with CPA-security assuming the $(n^{\omega(1)}, n^{-\omega(1)})$-hardness of decision $\mathrm{LWE}(n, q, \alpha = o(1/(\sqrt{n}\log n)))$.

This work:

For some prime $q \in \mathrm{poly}(n)$, there exists a public-key encryption (PKE) scheme with CPA-security based on **one of** the following three assumptions:

(1) The $(n^{\omega(1)}, n^{-\omega(1)})$-hardness of decision $\mathrm{LWE}(n, q, \alpha = O(1/\sqrt{n}))$.

(2) The $(2^{\omega(n^{\frac{1}{c_1}})}, 2^{-\omega(n^{\frac{1}{c_1}})})$-hardness of decision $\mathrm{LWE}(n, q, \alpha = O(1/\sqrt{n^{1-\frac{1}{c_1}}\log n}))$, for some constant $c_1 > 1$.

For example, let $c_1 = 2$, there exists a PKE scheme based on:

the $(2^{\omega(n^{\frac{1}{2}})}, 2^{-\omega(n^{\frac{1}{2}})})$-hardness of decision $\mathrm{LWE}(n, q, \alpha = O(1/(n^{\frac{1}{4}}\log^{\frac{1}{2}} n)))$.

(3) The $(2^{\omega\left(\frac{n}{\log^{c_2} n}\right)}, 2^{-\omega\left(\frac{n}{\log^{c_2} n}\right)})$-hardness of decision $\mathrm{LWE}(n, q, \alpha = O(1/\sqrt{\log^{c_2+1} n}))$, for some constant $c_2 > 0$.

For example, let $c_2 = 3$, there exists a PKE scheme based on:

the $(2^{\omega(\frac{n}{\log^3 n})}, 2^{-\omega(\frac{n}{\log^3 n})})$-hardness of decision $\mathrm{LWE}(n, q, \alpha = O(1/\log^2 n))$.

Result: (injective) TDF from Large Noise LWE

For some prime $q \in \mathrm{poly}(n)$, there exists a trapdoor function (TDF) family based on one of the following three assumptions.

(1) The $(n^{\omega(1)}, n^{-\omega(1)})$-hardness of search $\mathrm{LWE}(n, q(n), O(1/\sqrt{n}))$.

(2) The $(2^{\omega(n^{\frac{1}{c_1}})}, 2^{-\omega(n^{\frac{1}{c_1}})})$- hardness of search $\mathrm{LWE}(n, q(n), O(1/\sqrt{n^{1-\frac{1}{c_1}}}))$, for some constant $c_1 > 1$.

(3) The $(2^{\omega\left(\frac{n}{\log^{c_2} n}\right)}, 2^{-\omega\left(\frac{n}{\log^{c_2} n}\right)})$-hardness of search $\mathrm{LWE}(n, q(n), O(1/\sqrt{\log^{c_2+1} n}))$, for some constant $c_2 > 0$.

Specifically, assuming condition (1) or condition (2) with $c_1 \geq 2$, the TDF family is injective.

Result: PKE from constant-noise LPN

Yu, Zhang in CRYPTO2016 & this work:

There exists a PKE scheme with CPA-security assuming the $(2^{\omega(n^{\frac{1}{2}})}, 2^{-\omega(n^{\frac{1}{2}})})$-hardness of $\mathrm{LPN}(n, \mu)$, for some constant $0 < \mu < 1/2$.

Compared to [YZ16], our scheme achieves the same security while having a simpler construction.

03 Public-Key Encryption from Large Noise LWE

(Weakly correct) Regev's PKE [Reg05]

Tsinghua University

Let n be the security parameter, $q \in \mathrm{poly}(n)$ be a prime, $m \geq 2(n+1)\log q = \Theta(n\log n)$, $\alpha = \dfrac{1}{10\sqrt{m}} = \Theta\left(1/\sqrt{n\log n}\right)$.

Alice

Bob

$KeyGen(1^n)$:

·Sample $\boldsymbol{A} \leftarrow \mathbf{Z}_q^{n\times m}, \boldsymbol{s} \leftarrow \mathbf{Z}_q^n, \boldsymbol{e} \leftarrow \Psi_{\alpha,q}^m$.

·Compute $\boldsymbol{b} := \left(\boldsymbol{A}^T\boldsymbol{s} + \boldsymbol{e}\right) \bmod q$.

·Set $pk := (\boldsymbol{A}, \boldsymbol{b}),\ sk := \boldsymbol{s}$.

$\xrightarrow{pk}$

$Enc(pk, \beta \in \{0,1\})$:

·Sample $\boldsymbol{r} \leftarrow \{0,1\}^m$.

·Compute $\boldsymbol{c}_1 := \boldsymbol{A}\boldsymbol{r}, c_2 := \boldsymbol{r}^T\boldsymbol{b} + \left\lfloor \dfrac{q}{2} \right\rceil \cdot \beta$

·Set $\mathbf{c} := (\boldsymbol{c}_1, c_2)$

$\xleftarrow{\mathbf{c}}$

$Dec(sk, \boldsymbol{c})$:

·Compute $\Delta := \left(c_2 - \boldsymbol{c}_1^T\boldsymbol{s}\right) \bmod q$

$= \left(\boldsymbol{r}^T\boldsymbol{e} + \left\lfloor \dfrac{q}{2} \right\rceil \cdot \beta\right) \bmod q.$

·If $|\Delta| < \left\lfloor \dfrac{q}{2} \right\rceil /2$, output 0.

Correctness

A lemma for discrete Gaussian sums:
For any $\boldsymbol{r} \in \{0,1\}^n$, there exists some $\alpha = \Theta\left(1/\sqrt{Ham(\boldsymbol{r})}\right)$ such that, if $\boldsymbol{e} \leftarrow \Psi_{\alpha,q}^n$,
$\Pr_{\boldsymbol{e}}[\left|\boldsymbol{r}^T\boldsymbol{e}\right| < \left\lfloor \frac{q}{2} \right\rceil /2] > 2/3.$

$Dec(sk, \boldsymbol{c})$:

·Compute $\Delta := \left(c_2 - \boldsymbol{c}_1^T\boldsymbol{s}\right) \bmod q$

$= \left(\boldsymbol{r}^T\boldsymbol{e} + \left\lfloor \frac{q}{2} \right\rceil \cdot \beta\right) \bmod q.$

·If $\left|\Delta\right| < \left\lfloor \frac{q}{2} \right\rceil /2$, output 0.

·Otherwise, output 1.

Proof of correctness:
Since we choose $\alpha = \Theta(1/\sqrt{m}) = \Theta\left(1/\sqrt{Ham(\boldsymbol{r})}\right)$, we have $\left|\boldsymbol{r}^T\boldsymbol{e}\right| < \left\lfloor \frac{q}{2} \right\rceil /2$ with probability $>2/3$.

If $\beta = 0,$ then $\left|\Delta\right| < \left\lfloor \frac{q}{2} \right\rceil /2$ with probability $>2/3$.

If $\beta = 1,$ then $\left|\Delta\right| > \left\lfloor \frac{q}{2} \right\rceil /2$ with probability $>2/3$.

(Weakly correct) Regev's PKE [Reg05]

Tsinghua University

Let n be the security parameter, $q \in \mathrm{poly}(n)$ be a prime, $m \geq 2(n+1)\log q = \Theta(n \log n)$, $\alpha = \frac{1}{10\sqrt{m}} = \Theta\left(1/\sqrt{n \log n}\right)$.

Alice

Bob

$KeyGen(1^n)$:

·Sample $\boldsymbol{A} \leftarrow \mathbf{Z}_q^{n\times m}, \boldsymbol{s} \leftarrow \mathbf{Z}_q^n, \boldsymbol{e} \leftarrow \Psi_{\alpha,q}^m$.

·Compute $\boldsymbol{b} := \left(\boldsymbol{A}^T\boldsymbol{s} + \boldsymbol{e}\right) \bmod q$.

·Set $pk := (\boldsymbol{A}, \boldsymbol{b}),\ sk := \boldsymbol{s}$.

$\xrightarrow{pk}$

$Enc(pk, \beta \in \{0,1\})$:

·Sample $\boldsymbol{r} \leftarrow \{0,1\}^m$.

·Compute $\boldsymbol{c}_1 := \boldsymbol{A}\boldsymbol{r}, c_2 := \boldsymbol{r}^T\boldsymbol{b} + \left\lfloor \frac{q}{2} \right\rfloor \cdot \beta$

·Set $\mathbf{c} := (\boldsymbol{c}_1, c_2)$

$\xleftarrow{\mathbf{c}}$

$Dec(sk, \boldsymbol{c})$:

·Compute $\Delta := \left(c_2 - \boldsymbol{c}_1^T\boldsymbol{s}\right) \bmod q$.

·If $|\Delta| < \left\lfloor \frac{q}{2} \right\rfloor /2$, output 0.

·Otherwise, output 1.

Correctness:

$\Delta = \left(\boldsymbol{r}^T\boldsymbol{e} + \left\lfloor \frac{q}{2} \right\rfloor \cdot \beta\right) \bmod q$. Since

Tsinghua University

A Corollary of the Leftover Hash Lemma (LHL):

Let $\boldsymbol{A} \leftarrow \mathbf{Z}_q^{n\times m}$, $\boldsymbol{x} \leftarrow \mathrm{X}$, where X is a distribution on $\mathbf{Z}_q^m$. Then,

$$\mathrm{SD}\Big(\big(\boldsymbol{A}, \boldsymbol{A}\boldsymbol{x}\big), \big(\boldsymbol{A}, \mathrm{U}_q^n\big)\Big) \le \sqrt{\frac{q^n}{2^{H_\infty(\mathrm{X})}}},$$

where we denote the min-entropy of $\mathcal{X}$ by $H_\infty(\mathrm{X}) := -\log \max_{x\in Supp(\mathrm{X})} \Pr_{X\leftarrow \mathrm{X}}[X = x]$.

(Weakly correct) Regev's PKE [Reg05]

Tsinghua University

Let n be the security parameter, $q \in \mathrm{poly}(n)$ be a prime, $m \geq 2(n+1)\log q = \Theta(n\log n)$, $\alpha = \dfrac{1}{10\sqrt{m}} = \Theta\left(1/\sqrt{n\log n}\right)$.

Alice

Bob

$KeyGen(1^n)$:

·Sample $\boldsymbol{A} \leftarrow \mathbb{Z}_q^{n\times m}, \boldsymbol{s} \leftarrow \mathbb{Z}_q^n, \boldsymbol{e} \leftarrow \Psi_{\alpha,q}^m$.

·Sample $\boldsymbol{b} \leftarrow \mathbb{Z}_q^m$

·Set $pk := (\boldsymbol{A}, \boldsymbol{b}),\ sk := \boldsymbol{s}$.

By the hardness of (decision) $\mathrm{LWE}(n, q, \alpha)$, $(\boldsymbol{A}, \boldsymbol{b}) \approx_c \mathrm{U}_q^m$

Since $\boxed{H_\infty(\boldsymbol{r}) = m = \Theta(n\log n)}$, by LHL, we have

$$\mathrm{SD}\left(\left(\boldsymbol{A}, \boldsymbol{b}, \boldsymbol{A}\boldsymbol{r}, \boldsymbol{r}^T\boldsymbol{b}\right), \left(\boldsymbol{A}, \boldsymbol{b}, \mathrm{U}_q^{n+1}\right)\right) \leq \sqrt{\frac{q^{n+1}}{2^{H_\infty(\boldsymbol{r})}}} = \mathrm{negl}(n).$$

pk

Another distribution with:

(i) Smaller $Ham(\boldsymbol{r})$

(ii) Enough $H_\infty(\boldsymbol{r})$

$Enc(pk, \beta \in \{0,1\})$:

·Sample $\boldsymbol{r} \leftarrow \boxed{\{0,1\}^m}$.

·Compute $\boldsymbol{c}_1 := \mathrm{U}_q^n,\ c_2 := \mathrm{U}_q + \left\lfloor \frac{q}{2} \right\rceil \cdot \beta$

·Set $\mathbf{c} := (\boldsymbol{c}_1, c_2)$

$\mathbf{c}$

$Dec(sk, \boldsymbol{c})$:

·Compute $\Delta := \left(c_2 - \boldsymbol{c}_1^T\boldsymbol{s}\right) \bmod q$.

·If $|\Delta| < \left\lfloor \frac{q}{2} \right\rceil /2$, output 0.

·Otherwise, output 1.

Correctness:

$\Delta = \left(\boldsymbol{r}^T\boldsymbol{e} + \left\lfloor \frac{q}{2} \right\rceil \cdot \beta\right) \bmod q$. Since

A Short and Sparse Distribution for r

Let $\Xi^{[m:n]}$ be the uniform distribution on the set:
$\left\{\boldsymbol{x} \in \{0,1\}^m \middle| \; Ham(\boldsymbol{x}) = n\right\}$.

When $m = \mathrm{poly}(n)$, we have $H_\infty\left(\Xi^{[m:n]}\right) = \log\binom{m}{n} = \Theta\left(\mathrm{nlog}m\right) = \Theta\left(\mathrm{nlog}n\right)$

Encryption with Short and Sparse $\boldsymbol{r}$

Let n be the security parameter, $q \in \mathrm{poly}(n)$ be a prime, $m = \mathrm{poly}(n), \alpha = \Theta\left(1/\sqrt{n}\right)$.

Alice

Bob

$KeyGen(1^n)$:

·Sample $\boldsymbol{A} \leftarrow \mathbf{Z}_q^{n\times m}, \boldsymbol{s} \leftarrow \mathbf{Z}_q^n, \boldsymbol{e} \leftarrow \Psi_{\alpha,q}^m$.

·Compute $\boldsymbol{b} := \left(\boldsymbol{A}^T\boldsymbol{s} + \boldsymbol{e}\right) \bmod q$.

·Set $pk := (\boldsymbol{A}, \boldsymbol{b}),\ sk := \boldsymbol{s}$.

Since $H_\infty(\boldsymbol{r}) = \Theta(n\log n)$, by LHL, we have

$$\mathrm{SD}\left(\left(\boldsymbol{A}, \boldsymbol{b}, \boldsymbol{A}\boldsymbol{r}, \boldsymbol{r}^T\boldsymbol{b}\right), \left(\boldsymbol{A}, \boldsymbol{b}, \mathrm{U}_q^{n+1}\right)\right) \leq \sqrt{\frac{q^{n+1}}{2^{H_\infty(\boldsymbol{r})}}} = \mathrm{negl}(n).$$

pk

By the hardness of (decision) $\mathrm{LWE}(n, q, \alpha)$,
$(\boldsymbol{A}, \boldsymbol{b}) \approx_c \mathrm{U}_q^m$

$Enc(pk, \beta \in \{0,1\})$:

·Sample $\boldsymbol{r} \leftarrow \Xi^{[m:n]}$

·Compute $\boldsymbol{c}_1 := \boldsymbol{A}\boldsymbol{r}, c_2 := \boldsymbol{r}^T\boldsymbol{b} + \left\lfloor \frac{q}{2} \right\rceil \cdot \beta$

$\mathbf{c}$

·Set $\mathbf{c} := (\boldsymbol{c}_1, c_2)$

$Dec(sk, \boldsymbol{c})$:

·Compute $\Delta := \left(c_2 - \boldsymbol{c}_1^T\boldsymbol{s}\right) \bmod q$.

·If $|\Delta| < \left\lfloor \frac{q}{2} \right\rceil/2$, output 0.

·Otherwise, output 1.

Correctness:

$\Delta = \left(\boldsymbol{r}^T\boldsymbol{e} + \left\lfloor \frac{q}{2} \right\rceil \cdot \beta\right) \bmod q$. Since

$\Theta(1/\sqrt{n}) = O\left(1/\sqrt{H_\infty(\boldsymbol{r})}\right)$, we have $|\boldsymbol{r}^T\boldsymbol{e}| < \left\lfloor \frac{q}{2} \right\rceil/2$ with

A Short and Sparse Distribution for r

Let $\Xi^{[m:n]}$ be the uniform distribution on the set:

$\left\{ \boldsymbol{x} \in \{0,1\}^m \,\middle|\, Ham(\boldsymbol{x}) = n \right\}$.

When $n = o(m)$, we have $\mathrm{H}_\infty\left(\Xi^{[m:n]}\right) = \log\binom{m}{n} = \Theta\left(\mathrm{n}\log m\right) = \Theta\left(\mathrm{n}\log n\right)$

Not enough for $\boldsymbol{A} \leftarrow \mathbb{Z}_q^{n\times m}$

But still enough if $\boldsymbol{A} \leftarrow \mathbb{Z}_q^{\lambda\times m}$ for some $\lambda = o(n)$.

Our LWE-PKE ($\lambda = \log^2 n$)

Tsinghua University

Let n be the security parameter. Let $\lambda = \log^2 n, q = \mathrm{poly}(\lambda)$.
Let $k = \Theta\left(\lambda \log q / \log n\right)$ such that $H_\infty\left(\Xi^{[n:k]}\right) \geq 2(\lambda+1)\log q$. Let $\alpha = \Theta\left(1/\sqrt{k}\right) = \Theta\left(1/\sqrt{\log n \log\log n}\right)$.

Alice

Bob

$KeyGen\left(1^n\right)$:

·Sample $\boldsymbol{A} \leftarrow \mathbf{Z}_q^{\lambda\times n}, \boldsymbol{s} \leftarrow \mathbf{Z}_q^{\lambda}, \boldsymbol{e} \leftarrow \Psi_{\alpha,q}^{n}$.

·Compute $\boldsymbol{b} := \left(\boldsymbol{A}^T\boldsymbol{s} + \boldsymbol{e}\right) \bmod q$.

·Set $pk := \left(\boldsymbol{A}, \boldsymbol{b}\right)$, $sk := \boldsymbol{s}$.

Since $H_\infty(\boldsymbol{r}) = \Theta\left(k \log n\right)$, by LHL, we have

$$\mathrm{SD}\left(\left(\boldsymbol{A}, \boldsymbol{b}, \boldsymbol{A}\boldsymbol{r}, \boldsymbol{r}^T\boldsymbol{b}\right), \left(\boldsymbol{A}, \boldsymbol{b}, \mathrm{U}_q^{\lambda+1}\right)\right) \leq \sqrt{\frac{q^{\lambda+1}}{2^{H_\infty(\boldsymbol{r})}}} = \mathrm{negl}(n).$$

pk

By the hardness of (decision) $\mathrm{LWE}(\lambda, q, \alpha)$,
$(\boldsymbol{A}, \boldsymbol{b}) \approx_c \mathrm{U}_q^m$

$Enc\left(pk, \beta \in \{0,1\}\right)$:

·Sample $\boldsymbol{r} \leftarrow \Xi^{[n:k]}$

·Compute $\boldsymbol{c}_1 := \boldsymbol{A}\boldsymbol{r}, c_2 := \boldsymbol{r}^T\boldsymbol{b} + \left\lfloor \frac{q}{2} \right\rfloor \cdot \beta$

·Set $\mathbf{c} := (\boldsymbol{c}_1, c_2)$

$\mathbf{c}$

$Dec(sk, \boldsymbol{c})$:

·Compute $\Delta := \left(c_2 - \boldsymbol{c}_1^T\boldsymbol{s}\right) \bmod q$.

·If $|\Delta| < \left\lfloor \frac{q}{2} \right\rfloor /2$, output 0.

·Otherwise, output 1.

Correctness:

$\Delta = \left(\boldsymbol{r}^T\boldsymbol{e} + \left\lfloor \frac{q}{2} \right\rfloor \cdot \beta\right) \bmod q$. Since

The hardness of $\mathrm{LWE}(\lambda, q, \alpha)$

When n is the security parameter, $\lambda = \log^2 n$, $q = \mathrm{poly}(\lambda)$, $\alpha = \Theta\left(1/\sqrt{\log n \log\log n}\right)$,

the security of the scheme is based on the hardness of decision $\mathrm{LWE}(\lambda, q, \alpha)$,

i.e.,

the $(n^{\omega(1)}, n^{-\omega(1)})$-hardness of decision $\mathrm{LWE}\left(\log^2 n, \mathrm{poly}(\log n), \Theta\left(\frac{1}{\sqrt{\log n \log\log n}}\right)\right)$,

i.e.,

the $(2^{\omega\left(\sqrt{\log^2 n}\right)}, (2^{-\omega\left(\sqrt{\log^2 n}\right)})$-hardness of decision $\mathrm{LWE}\left(\log^2 n, \mathrm{poly}(\log^2 n), \Theta\left(\frac{1}{(\log^2 n)^{\frac{1}{4}}(\log\log^2 n)^{\frac{1}{2}}}\right)\right)$,

This is based on:

the $(2^{\omega(\sqrt{n})}, 2^{-\omega(\sqrt{n})})$-hardness of decision $\mathrm{LWE}\left(n, \mathrm{poly}(n), \Theta\left(\frac{1}{n^{\frac{1}{4}}\log^{\frac{1}{2}} n}\right)\right)$.

Result: PKE from Large Noise LWE

[Reg05]:

For some prime $q \in \mathrm{poly}(n)$, there exists a public-key encryption (PKE) scheme with CPA-security assuming the $(n^{\omega(1)}, n^{-\omega(1)})$-hardness of decision $\mathrm{LWE}(n, q, \alpha = o(1/(\sqrt{n}\log n)))$.

This work:

For some prime $q \in \mathrm{poly}(n)$, there exists a public-key encryption (PKE) scheme with CPA-security based on **one of** the following three assumptions:

(1) The $(n^{\omega(1)}, n^{-\omega(1)})$-hardness of decision $\mathrm{LWE}(n, q, \alpha = O(1/\sqrt{n}))$.

(2) The $(2^{\omega(n^{\frac{1}{c_1}})}, 2^{-\omega(n^{\frac{1}{c_1}})})$-hardness of decision $\mathrm{LWE}(n, q, \alpha = O(1/\sqrt{n^{1-\frac{1}{c_1}}\log n}))$, for some constant $c_1 > 1$. $(\lambda = \log^{c_1} n)$

For example, let $c_1 = 2$, there exists a PKE scheme based on:

the $(2^{\omega(n^{\frac{1}{2}})}, 2^{-\omega(n^{\frac{1}{2}})})$-hardness of decision $LWE(n, q, \alpha = O(1/(n^{\frac{1}{4}}\log^{\frac{1}{2}} n)))$. $(\lambda = \log^2 n)$

(3) The $(2^{\omega\left(\frac{n}{\log^{c_2} n}\right)}, 2^{-\omega\left(\frac{n}{\log^{c_2} n}\right)})$-hardness of decision $\mathrm{LWE}(n, q, \alpha = O(1/\sqrt{\log^{c_2+1} n}))$, for some constant $c_2 > 0$. $(\lambda = \log n(\log\log n)^{c_2})$

For example, let $c_2 = 3$, there exists a PKE scheme based on:

the $(2^{\omega(\frac{n}{\log^3 n})}, 2^{-\omega(\frac{n}{\log^3 n})})$-hardness of decision $\mathrm{LWE}(n, q, \alpha = O(1/\log^2 n))$. $(\lambda = \log n(\log\log n)^3)$

Thanks!