Public-Key Encryption from Homogeneous CLWE

Andrej Bogdanov[1], Miguel Cueto Noval[2], **Charlotte Hoffmann**[2] and Alon Rosen[3]

[1]Chinese University of Hong Kong
[2]Institute of Science and Technology Austria
[3]Bocconi University and Reichman University

Introduction

- Public-key encryption schemes are based on relatively few computational assumptions

Introduction

- Public-key encryption schemes are based on relatively few computational assumptions
- **New assumption:** homogeneous Continuous Learning with Errors (hCLWE) [BRST21]

Introduction

- Public-key encryption schemes are based on relatively few computational assumptions
- **New assumption:** homogeneous Continuous Learning with Errors (hCLWE) [BRST21]
- LWE $\rightarrow$ hCLWE [GVV22]

Introduction

- Public-key encryption schemes are based on relatively few computational assumptions
- **New assumption:** homogeneous Continuous Learning with Errors (hCLWE) [BRST21]
- LWE $\rightarrow$ hCLWE [GVV22]
- Used in [BRST21] to show hardness of learning mixtures of Gaussians

Introduction

- Public-key encryption schemes are based on relatively few computational assumptions
- **New assumption:** homogeneous Continuous Learning with Errors (hCLWE) [BRST21]
- LWE $\rightarrow$ hCLWE [GVV22]
- Used in [BRST21] to show hardness of learning mixtures of Gaussians

Our Contribution

- Four public-key encryption schemes based on hCLWE

Introduction

- Public-key encryption schemes are based on relatively few computational assumptions
- **New assumption:** homogeneous Continuous Learning with Errors (hCLWE) [BRST21]
- LWE $\rightarrow$ hCLWE [GVV22]
- Used in [BRST21] to show hardness of learning mixtures of Gaussians

Our Contribution

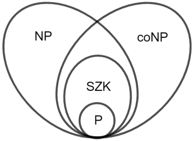
- Four public-key encryption schemes based on hCLWE
- Proof that hCLWE is in SZK (Statistical Zero Knowledge)

Introduction

- Public-key encryption schemes are based on relatively few computational assumptions
- **New assumption:** homogeneous Continuous Learning with Errors (hCLWE) [BRST21]
- LWE $\rightarrow$ hCLWE [GVV22]
- Used in [BRST21] to show hardness of learning mixtures of Gaussians

Our Contribution

- Four public-key encryption schemes based on hCLWE
- Proof that hCLWE is in SZK (Statistical Zero Knowledge)



Homogeneous CLWE [BRST21]

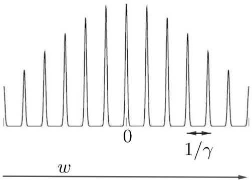
- Secret $w \in \mathbb{R}^n$: $\|w\| = 1$

Homogeneous CLWE [BRST21]

- Secret $w \in \mathbb{R}^n$: $\|w\| = 1$
- Samples $\mathrm{y} \in \mathbb{R}^n$:
  - normally distributed in $w^\perp$
  - noisy discrete Gaussian in direction w.

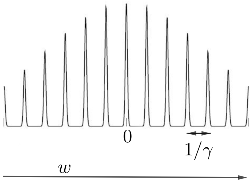
Homogeneous CLWE [BRST21]

- Secret $w \in \mathbb{R}^n$: $\|w\| = 1$
- Samples $y \in \mathbb{R}^n$:
  - normally distributed in $w^\perp$
  - noisy discrete Gaussian in direction w.



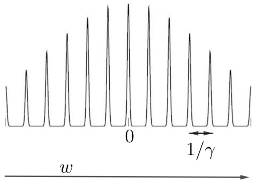
Homogeneous CLWE [BRST21]

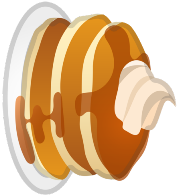
- Secret $w \in \mathbb{R}^n$: $\|w\| = 1$
- Samples $y \in \mathbb{R}^n$:
  - normally distributed in $w^\perp$
  - noisy discrete Gaussian in direction w.



Homogeneous CLWE [BRST21]

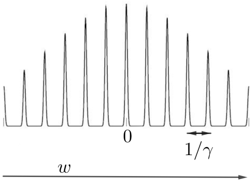
- Secret $w \in \mathbb{R}^n$: $\|w\| = 1$
- Samples $y \in \mathbb{R}^n$:
  - normally distributed in $w^\perp$
  - noisy discrete Gaussian in direction w.

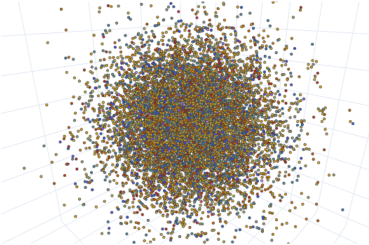




Homogeneous CLWE [BRST21]

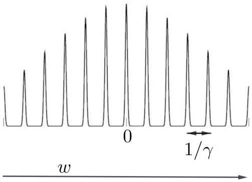
- Secret $w \in \mathbb{R}^n$: $\|w\| = 1$
- Samples $y \in \mathbb{R}^n$:
  - normally distributed in $w^\perp$
  - noisy discrete Gaussian in direction w.

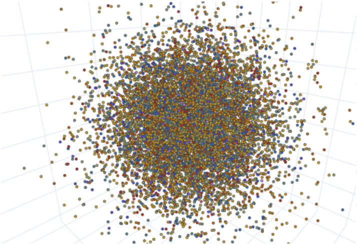


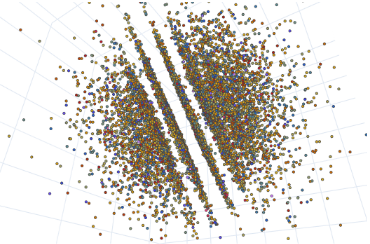


Homogeneous CLWE [BRST21]

- Secret $w \in \mathbb{R}^n$: $\|w\| = 1$
- Samples $y \in \mathbb{R}^n$:
  - normally distributed in $w^{\perp}$
  - noisy discrete Gaussian in direction w.

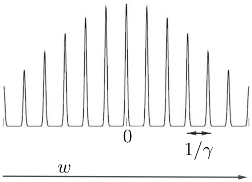


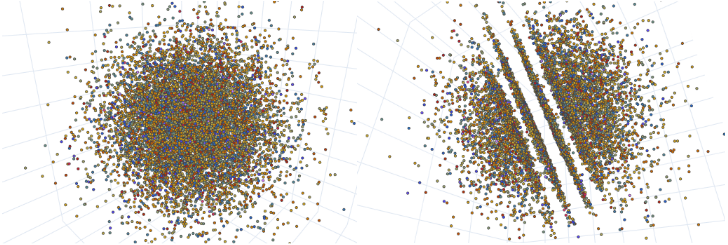




Homogeneous CLWE [BRST21]

- Secret $w \in \mathbb{R}^n$: $\|w\| = 1$
- Samples $y \in \mathbb{R}^n$:
  - normally distributed in $w^\perp$
  - noisy discrete Gaussian in direction w.

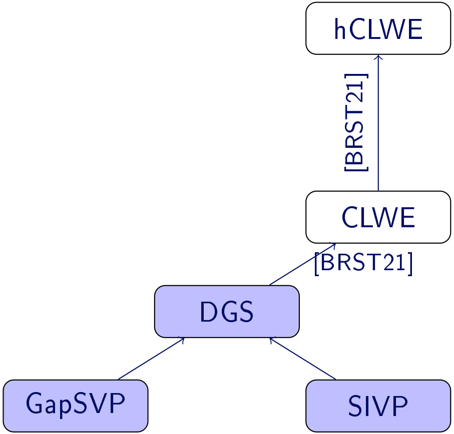




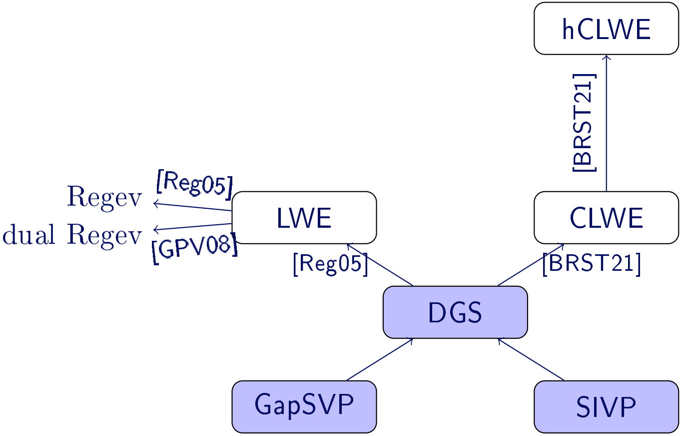
hCLWE assumption

Given a polynomial number of hCLWE samples, it is hard to distinguish them from standard normal samples.

Reductions

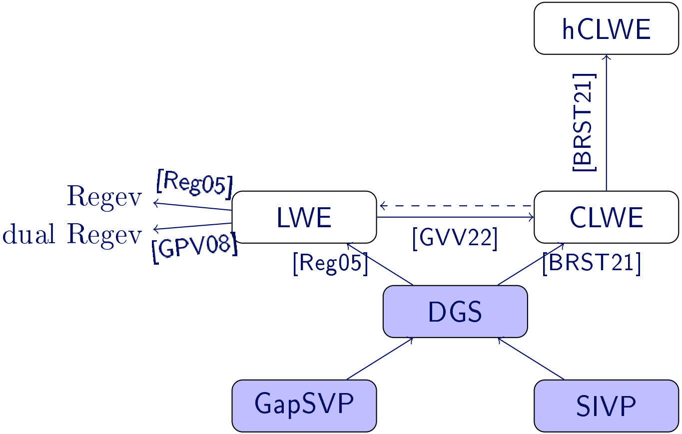


Reductions



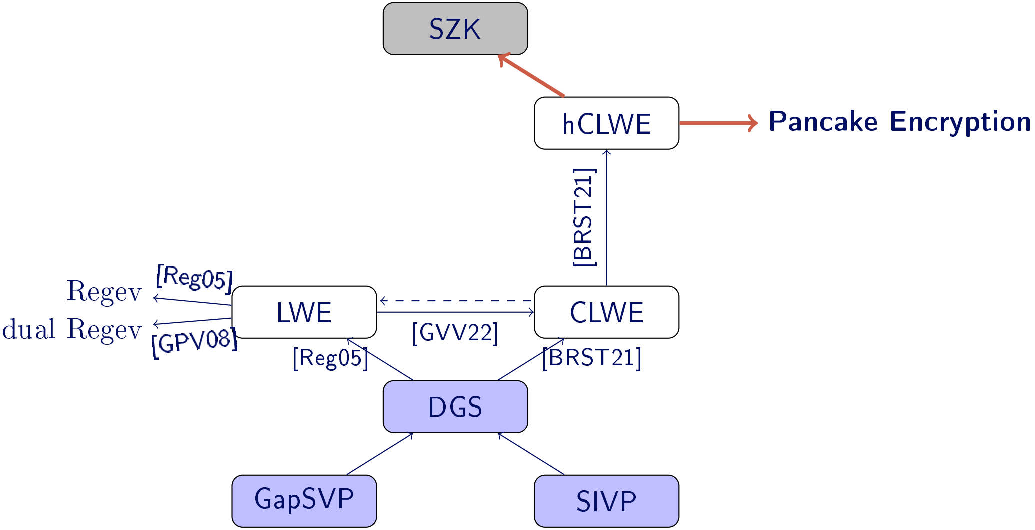
hCLWE
[BRST21]
Regev
[Reg05]
LWE
CLWE
dual Regev
[GPV08]
[Reg05]
[BRST21]
DGS
GapSVP
SIVP

Reductions



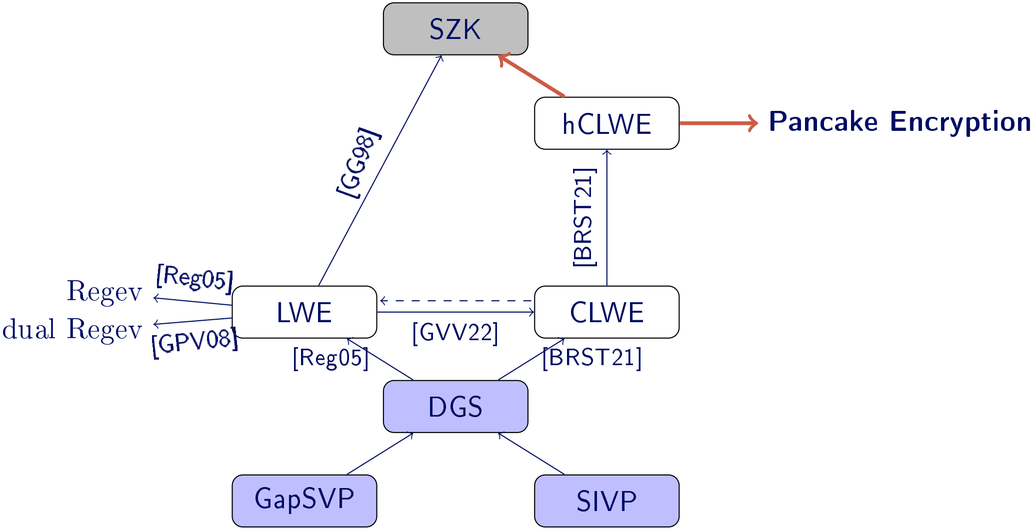
hCLWE
[BRST21]
Regev
[Reg05]
LWE
CLWE
dual Regev
[GPV08]
[GVV22]
[Reg05]
[BRST21]
DGS
GapSVP
SIVP

Reductions



SZK
hCLWE
Pancake Encryption
[BRST21]
Regev
[Reg05]
dual Regev
[GPV08]
LWE
CLWE
[GVV22]
[Reg05]
[BRST21]
DGS
GapSVP
SIVP

Reductions



SZK
hCLWE
Pancake Encryption
[GG98]
[BRST21]
Regev
[Reg05]
dual Regev
[GPV08]
LWE
CLWE
[GVV22]
[Reg05]
[BRST21]
DGS
GapSVP
SIVP

The Pancake Encryption Scheme

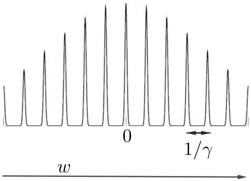
- Secret key: $\mathrm{w} \leftarrow \mathbb{R}^n$, $\|w\| = 1$

The Pancake Encryption Scheme

- Secret key: $\mathrm{w} \leftarrow \mathbb{R}^n$, $\|w\| = 1$
- Public key: $\mathrm{A} \in \mathbb{R}^{n \times m}$ consisting of m hCLWE samples with secret direction w

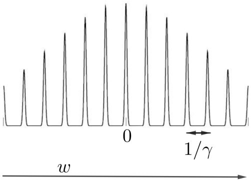
The Pancake Encryption Scheme

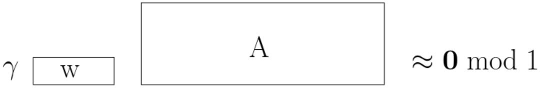
- Secret key: $\mathsf{w} \leftarrow \mathbb{R}^n$, $\|w\| = 1$
- Public key: $\mathsf{A} \in \mathbb{R}^{n \times m}$ consisting of m hCLWE samples with secret direction w



The Pancake Encryption Scheme

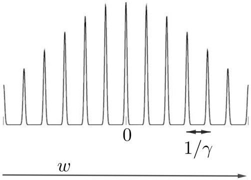
- Secret key: w $\leftarrow \mathbb{R}^n$, $\|w\| = 1$
- Public key: A $\in \mathbb{R}^{n \times m}$ consisting of m hCLWE samples with secret direction w





The Pancake Encryption Scheme

- Secret key: $\mathrm{w} \leftarrow \mathbb{R}^n$, $\|w\| = 1$
- Public key: $\mathrm{A} \in \mathbb{R}^{n \times m}$ consisting of m hCLWE samples with secret direction w

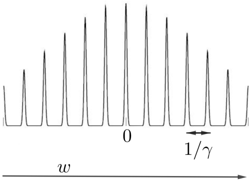


$$\gamma \; \boxed{\mathrm{w}} \; \boxed{\mathrm{A}} \approx \mathbf{0} \bmod 1$$

- Enc(0): sample $\mathrm{t} \leftarrow \{\pm 1\}^m$ and output $c := \mathrm{round}(\mathrm{At})$

The Pancake Encryption Scheme

- Secret key: $\mathrm{w} \leftarrow \mathbb{R}^n$, $\|w\| = 1$
- Public key: $\mathrm{A} \in \mathbb{R}^{n \times m}$ consisting of m hCLWE samples with secret direction w

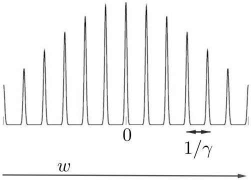


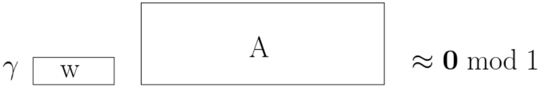
$$\gamma \; \mathrm{w} \; \mathrm{A} \approx \mathbf{0} \bmod 1$$

- Enc(0): sample $\mathrm{t} \leftarrow \{\pm 1\}^m$ and output $c := \mathrm{round}(\mathrm{At})$
- Enc(1): sample $\mathrm{g} \leftarrow \mathcal{N}(0, m)^n$ and output $c := \mathrm{round}(\mathrm{g})$

The Pancake Encryption Scheme

- Secret key: $\mathrm{w} \leftarrow \mathbb{R}^n$, $\|w\| = 1$
- Public key: $\mathrm{A} \in \mathbb{R}^{n\times m}$ consisting of m hCLWE samples with secret direction w

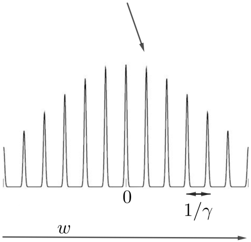


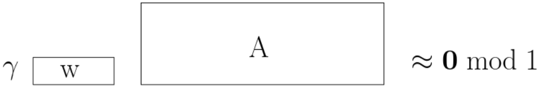


- Enc(0): sample $\mathrm{t} \leftarrow \{\pm 1\}^m$ and output $c := \mathrm{round}(\mathrm{At})$
- Enc(1): sample $\mathrm{g} \leftarrow \mathcal{N}(0, m)^n$ and output $c := \mathrm{round}(\mathrm{g})$
- Dec(c): $\gamma\langle \mathrm{w}, \mathrm{c}\rangle$ mod 1 ≈ 0 ? If yes: 0 If not: 1

The Pancake Encryption Scheme

- Secret key: $\mathrm{w} \leftarrow \mathbb{R}^n$, $\|w\| = 1$
- Public key: $\mathrm{A} \in \mathbb{R}^{n \times m}$ consisting of m hCLWE samples with secret direction w

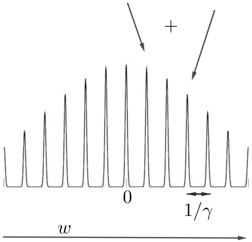


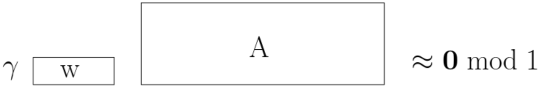


- Enc(0): sample $\mathrm{t} \leftarrow \{\pm 1\}^m$ and output $c := \mathrm{round}(\mathrm{At})$
- Enc(1): sample $\mathrm{g} \leftarrow \mathcal{N}(0, m)^n$ and output $c := \mathrm{round}(\mathrm{g})$
- Dec(c): $\gamma\langle \mathrm{w}, \mathrm{c}\rangle$ mod 1 ≈ 0 ? If yes: 0 If not: 1

The Pancake Encryption Scheme

- Secret key: $\mathrm{w} \leftarrow \mathbb{R}^n$, $\|w\| = 1$
- Public key: $\mathrm{A} \in \mathbb{R}^{n \times m}$ consisting of m hCLWE samples with secret direction w

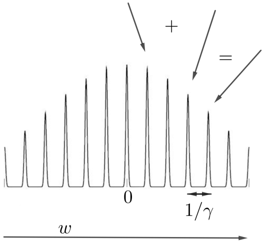


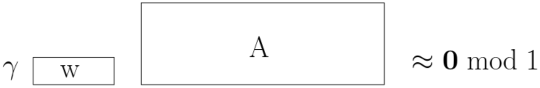


- Enc(0): sample $\mathrm{t} \leftarrow \{\pm 1\}^m$ and output $c := \mathrm{round}(\mathrm{At})$
- Enc(1): sample $\mathrm{g} \leftarrow \mathcal{N}(0, m)^n$ and output $c := \mathrm{round}(\mathrm{g})$
- Dec(c): $\gamma\langle \mathrm{w}, \mathrm{c} \rangle \bmod 1 \approx 0$? If yes: 0 If not: 1

The Pancake Encryption Scheme

- Secret key: $\mathrm{w} \leftarrow \mathbb{R}^n$, $\|w\| = 1$
- Public key: $\mathrm{A} \in \mathbb{R}^{n \times m}$ consisting of m hCLWE samples with secret direction w





- Enc(0): sample $\mathrm{t} \leftarrow \{\pm 1\}^m$ and output $c := \mathrm{round}(\mathrm{At})$
- Enc(1): sample $\mathrm{g} \leftarrow \mathcal{N}(0, m)^n$ and output $c := \mathrm{round}(\mathrm{g})$
- Dec(c): $\gamma \langle \mathrm{w}, \mathrm{c} \rangle$ mod $1 \approx 0$? If yes: 0 If not: 1

Security of Encryption

Let A be the public key, $t \leftarrow \{\pm 1\}^m$, $N \leftarrow \mathcal{N}(0,1)^{n \times m}$ and $g \leftarrow \mathcal{N}(0,m)^n$. Then

$$(A, \mathrm{Enc}(0))$$

$$(A, \mathrm{Enc}(1)).$$

Security of Encryption

Let A be the public key, $\mathsf{t} \leftarrow \{\pm 1\}^m$, $\mathsf{N} \leftarrow \mathcal{N}(0,1)^{n \times m}$ and $\mathsf{g} \leftarrow \mathcal{N}(0,m)^n$. Then

$$(\mathsf{A}, \mathrm{Enc}(0)) = (\mathsf{A}, \mathrm{round}(\mathsf{At}))$$

$$(\mathsf{A}, \mathrm{Enc}(1)).$$

Security of Encryption

Let A be the public key, $t \leftarrow \{\pm 1\}^m$, $N \leftarrow \mathcal{N}(0,1)^{n \times m}$ and $g \leftarrow \mathcal{N}(0,m)^n$. Then

$$\begin{aligned}(A, \mathrm{Enc}(0)) &= (A, \mathrm{round}(At)) \\ &\approx_{\mathrm{hCLWE}} (N, \mathrm{round}(Nt))\end{aligned}$$

$$(A, \mathrm{Enc}(1)).$$

Security of Encryption

Let A be the public key, $\mathsf{t} \leftarrow \{\pm 1\}^m$, $\mathsf{N} \leftarrow \mathcal{N}(0,1)^{n\times m}$ and $\mathsf{g} \leftarrow \mathcal{N}(0,m)^n$. Then

$$\begin{aligned}
(\mathsf{A}, \mathrm{Enc}(0)) &= (\mathsf{A}, \mathrm{round}(\mathsf{At})) \\
&\approx_{\mathrm{hCLWE}} (\mathsf{N}, \mathrm{round}(\mathsf{Nt})) \\
&\approx_{\Delta=0.01} (\mathsf{N}, \mathrm{round}(\mathsf{g})) \\
& \qquad\qquad\qquad (\mathsf{A}, \mathrm{Enc}(1)).
\end{aligned}$$

Security of Encryption

Let A be the public key, $\mathsf{t} \leftarrow \{\pm 1\}^m$, $\mathsf{N} \leftarrow \mathcal{N}(0,1)^{n \times m}$ and $\mathsf{g} \leftarrow \mathcal{N}(0,m)^n$. Then

$$\begin{aligned}(\mathsf{A}, \mathrm{Enc}(0)) &= (\mathsf{A}, \mathrm{round}(\mathsf{At})) \\ &\approx_{\mathrm{hCLWE}} (\mathsf{N}, \mathrm{round}(\mathsf{Nt})) \\ &\approx_{\Delta=0.01} (\mathsf{N}, \mathrm{round}(\mathsf{g})) \\ &\approx_{\mathrm{hCLWE}} (\mathsf{A}, \mathrm{round}(\mathsf{g})) = (\mathsf{A}, \mathrm{Enc}(1)).\end{aligned}$$

Security of Encryption

Let A be the public key, $t \leftarrow \{\pm 1\}^m$, $N \leftarrow \mathcal{N}(0,1)^{n \times m}$ and $g \leftarrow \mathcal{N}(0,m)^n$. Then

$$\begin{aligned}(A, \mathrm{Enc}(0)) &= (A, \mathrm{round}(At)) \\ &\approx_{\mathrm{hCLWE}} (N, \mathrm{round}(Nt)) \\ &\approx_{\Delta=0.01} (N, \mathrm{round}(g)) \\ &\approx_{\mathrm{hCLWE}} (A, \mathrm{round}(g)) = (A, \mathrm{Enc}(1)).\end{aligned}$$

Proof Strategy

1. Define a suitable rounding function

Security of Encryption

Let A be the public key, $\mathsf{t} \leftarrow \{\pm 1\}^m$, $\mathsf{N} \leftarrow \mathcal{N}(0,1)^{n \times m}$ and $\mathsf{g} \leftarrow \mathcal{N}(0,m)^n$. Then

$$\begin{aligned}(\mathsf{A}, \mathrm{Enc}(0)) &= (\mathsf{A}, \mathrm{round}(\mathsf{At})) \\ &\approx_{\mathrm{hCLWE}} (\mathsf{N}, \mathrm{round}(\mathsf{Nt})) \\ &\approx_{\Delta=0.01} (\mathsf{N}, \mathrm{round}(\mathsf{g})) \\ &\approx_{\mathrm{hCLWE}} (\mathsf{A}, \mathrm{round}(\mathsf{g})) = (\mathsf{A}, \mathrm{Enc}(1)).\end{aligned}$$

Proof Strategy

1. Define a suitable rounding function
2. Show that the probability of Nt landing in a set $S = \mathrm{round}^{-1}(c)$ is approximately equal to its Gaussian measure $\mu(S)$ (Gaussian hypercontractivity)

Results

Scheme	Assumption	Dec. error	Sec. error	PK size	SK size
Pancake	hCLWE	$O(1/n)$	0.01	$\tilde{O}(n^3)$	n

Results

Scheme	Assumption	Dec. error	Sec. error	PK size	SK size
Pancake	hCLWE	$O(1/n)$	0.01	$\tilde{O}(n^3)$	n
Bimodal	$(0, 1/2)$-hCLWE	0	0.01	$\tilde{O}(n^3)$	n
Baguette	hCLWE(ℓ)	$O(1/n^\ell)$	0.01	$\tilde{O}(n^3)$	$n\ell$
Discretized [AD97]	hCLWE	$O(1/n)$	2^{-n}	$O(n^3)$	n

Results

Scheme	Assumption	Dec. error	Sec. error	PK size	SK size
Pancake	hCLWE	$O(1/n)$	0.01	$\tilde{O}(n^3)$	n
Bimodal	$(0, 1/2)$-hCLWE	0	0.01	$\tilde{O}(n^3)$	n
Baguette	hCLWE(ℓ)	$O(1/n^\ell)$	0.01	$\tilde{O}(n^3)$	$n\ell$
Discretized [AD97]	hCLWE	$O(1/n)$	2^{-n}	$O(n^3)$	n

$\rightarrow$ Bimodal + Discretized gives a scheme with perfect decryption and negligible security error.

Results

Scheme	Assumption	Dec. error	Sec. error	PK size	SK size
Pancake	hCLWE	$O(1/n)$	0.01	$\tilde{O}(n^3)$	n
Bimodal	$(0, 1/2)$-hCLWE	0	0.01	$\tilde{O}(n^3)$	n
Baguette	hCLWE(ℓ)	$O(1/n^\ell)$	0.01	$\tilde{O}(n^3)$	$n\ell$
Discretized [AD97]	hCLWE	$O(1/n)$	2^{-n}	$O(n^3)$	n

$\rightarrow$ Bimodal + Discretized gives a scheme with perfect decryption and negligible security error.

$\rightarrow$ hCLWE is in the class SZK (statistical zero-knowledge) $\rightarrow$ coNP.

Results

Scheme	Assumption	Dec. error	Sec. error	PK size	SK size
Pancake	hCLWE	$O(1/n)$	0.01	$\tilde{O}(n^3)$	n
Bimodal	$(0, 1/2)$-hCLWE	0	0.01	$\tilde{O}(n^3)$	n
Baguette	hCLWE(ℓ)	$O(1/n^\ell)$	0.01	$\tilde{O}(n^3)$	$n\ell$
Discretized [AD97]	hCLWE	$O(1/n)$	2^{-n}	$O(n^3)$	n

→ Bimodal + Discretized gives a scheme with perfect decryption and negligible security error.

→ hCLWE is in the class SZK (statistical zero-knowledge) → coNP.

Open Problems

Results

Scheme	Assumption	Dec. error	Sec. error	PK size	SK size
Pancake	hCLWE	$O(1/n)$	0.01	$\tilde{O}(n^3)$	n
Bimodal	$(0, 1/2)$-hCLWE	0	0.01	$\tilde{O}(n^3)$	n
Baguette	hCLWE(ℓ)	$O(1/n^{\ell})$	0.01	$\tilde{O}(n^3)$	$n\ell$
Discretized [AD97]	hCLWE	$O(1/n)$	2^{-n}	$O(n^3)$	n

$\rightarrow$ Bimodal + Discretized gives a scheme with perfect decryption and negligible security error.

$\rightarrow$ hCLWE is in the class SZK (statistical zero-knowledge) $\rightarrow$ coNP.

Open Problems

- Make the PKE schemes more practical

Results

Scheme	Assumption	Dec. error	Sec. error	PK size	SK size
Pancake	hCLWE	$O(1/n)$	0.01	$\tilde{O}(n^3)$	n
Bimodal	$(0, 1/2)$-hCLWE	0	0.01	$\tilde{O}(n^3)$	n
Baguette	hCLWE(ℓ)	$O(1/n^{\ell})$	0.01	$\tilde{O}(n^3)$	$n\ell$
Discretized [AD97]	hCLWE	$O(1/n)$	2^{-n}	$O(n^3)$	n

→ Bimodal + Discretized gives a scheme with perfect decryption and negligible security error.

→ hCLWE is in the class SZK (statistical zero-knowledge) → coNP.

Open Problems

- Make the PKE schemes more practical
- Does SZK membership also hold for aperiodic mixtures of Gaussians?

Results

Scheme	Assumption	Dec. error	Sec. error	PK size	SK size
Pancake	hCLWE	$O(1/n)$	0.01	$\tilde{O}(n^3)$	n
Bimodal	$(0, 1/2)$-hCLWE	0	0.01	$\tilde{O}(n^3)$	n
Baguette	hCLWE(ℓ)	$O(1/n^\ell)$	0.01	$\tilde{O}(n^3)$	$n\ell$
Discretized [AD97]	hCLWE	$O(1/n)$	2^{-n}	$O(n^3)$	n

$\rightarrow$ Bimodal + Discretized gives a scheme with perfect decryption and negligible security error.

$\rightarrow$ hCLWE is in the class SZK (statistical zero-knowledge) $\rightarrow$ coNP.

Open Problems

- Make the PKE schemes more practical
- Does SZK membership also hold for aperiodic mixtures of Gaussians?
- Reduction from hCLWE to LWE?

Results

Scheme	Assumption	Dec. error	Sec. error	PK size	SK size
Pancake	hCLWE	$O(1/n)$	0.01	$\tilde{O}(n^3)$	n
Bimodal	$(0, 1/2)$-hCLWE	0	0.01	$\tilde{O}(n^3)$	n
Baguette	hCLWE(ℓ)	$O(1/n^{\ell})$	0.01	$\tilde{O}(n^3)$	$n\ell$
Discretized [AD97]	hCLWE	$O(1/n)$	2^{-n}	$O(n^3)$	n

$\rightarrow$ Bimodal + Discretized gives a scheme with perfect decryption and negligible security error.

$\rightarrow$ hCLWE is in the class SZK (statistical zero-knowledge) $\rightarrow$ coNP.

Open Problems

- Make the PKE schemes more practical
- Does SZK membership also hold for aperiodic mixtures of Gaussians?
- Reduction from hCLWE to LWE?

Questions?