New (and Old) Proof Systems for Lattice Problems

Navid Alamati $\boxed{\text{Chris Peikert}}$ Noah Stephens-Davidowitz

PKC 2018

Zero-Knowledge Proofs [GoldwasserMicaliRackoff'85]

- A protocol allowing an unbounded Prover P to convince a skeptical, bounded Verifier V that some $x \in L$.

Zero-Knowledge Proofs [GoldwasserMicaliRackoff'85]

- A protocol allowing an unbounded Prover P to convince a skeptical, bounded Verifier V that some $x \in L$.
- The (honest) verifier learns nothing more than the truth of statement: $\exists$ efficient simulator S such that $\forall x \in L$:

$$\text{View}_V[P(x) \leftrightarrow V(x)] \approx S(x).$$

Zero-Knowledge Proofs [GoldwasserMicaliRackoff'85]

- A protocol allowing an unbounded Prover P to convince a skeptical, bounded Verifier V that some $x \in L$.
- The (honest) verifier learns nothing more than the truth of statement: $\exists$ efficient simulator S such that $\forall x \in L$:

$$\text{View}_V[P(x) \leftrightarrow V(x)] \approx S(x).$$

- Statistical ZK (SZK): "$\approx$" means statistically indistinguishable.

Zero-Knowledge Proofs [GoldwasserMicaliRackoff'85]

- A protocol allowing an unbounded Prover P to convince a skeptical, bounded Verifier V that some $x \in L$.
- The (honest) verifier learns nothing more than the truth of statement: $\exists$ efficient simulator S such that $\forall x \in L$:

$$\text{View}_V[P(x) \leftrightarrow V(x)] \approx S(x).$$

- Statistical ZK (SZK): "$\approx$" means statistically indistinguishable.
- Honest-verifier SZK $\equiv$ general SZK [GSV'98].

Zero-Knowledge Proofs [GoldwasserMicaliRackoff'85]

- A protocol allowing an unbounded Prover P to convince a skeptical, bounded Verifier V that some $x \in L$.
- The (honest) verifier learns nothing more than the truth of statement: $\exists$ efficient simulator S such that $\forall x \in L$:

$$\text{View}_V[P(x) \leftrightarrow V(x)] \approx S(x).$$

- Statistical ZK (SZK): "$\approx$" means statistically indistinguishable.
- Honest-verifier SZK $\equiv$ general SZK [GSV'98].
- SZK proofs are powerful: secure against unbounded malicious P^*, V^*.

Noninteractive SZK [GoldreichSahaiVadhan'99]

- Consists of only one message from P to V.

Noninteractive SZK [GoldreichSahaiVadhan'99]

- Consists of only one message from P to V.
- Both P and V have access to a uniformly random string.

Noninteractive SZK [GoldreichSahaiVadhan'99]

- Consists of only one message from P to V.
- Both P and V have access to a uniformly random string.

SZK versus NISZK

- ⋆ Both SZK and NISZK have complete problems [SV'97, GSV'99]

Noninteractive SZK [GoldreichSahaiVadhan'99]

- Consists of only one message from P to V.
- Both P and V have access to a uniformly random string.

SZK versus NISZK

- ⋆ Both SZK and NISZK have complete problems [SV'97, GSV'99]
- ⋆ SZK is closed under complement [SV'97], but NISZK is not known to be.

Noninteractive SZK [GoldreichSahaiVadhan'99]

- Consists of only one message from P to V.
- Both P and V have access to a uniformly random string.

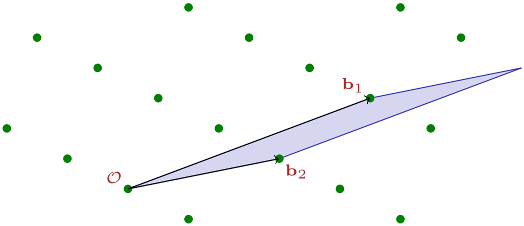
SZK versus NISZK

- ⋆ Both SZK and NISZK have complete problems [SV'97, GSV'99]
- ⋆ SZK is closed under complement [SV'97], but NISZK is not known to be.
- ⋆ NISZK is closed under complement $\iff$ NISZK $=$ SKZ [GSV'99]

Lattices

- An n-dimensional lattice $\mathcal{L} \subset \mathbb{R}^n$ is a discrete additive subgroup, generated by a (non-unique) basis $\mathbf{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$:

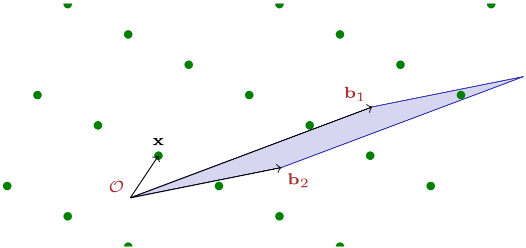
$$\mathcal{L} = \sum_{i=1}^{n} (\mathbb{Z} \cdot \mathbf{b}_i)$$



Lattices

- An n-dimensional lattice $\mathcal{L} \subset \mathbb{R}^n$ is a discrete additive subgroup, generated by a (non-unique) basis $\mathbf{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$:

$$\mathcal{L} = \sum_{i=1}^{n} (\mathbb{Z} \cdot \mathbf{b}_i)$$

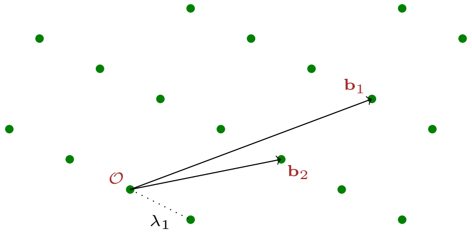


- Represent coset $\mathbf{x} + \mathcal{L} \in (\mathbb{R}^n / \mathcal{L})$ by unique $\bar{\mathbf{x}} \in (\mathbf{x} + \mathcal{L}) \cap \mathcal{P}(\mathbf{B})$.

Lattices

- An n-dimensional lattice $\mathcal{L} \subset \mathbb{R}^n$ is a discrete additive subgroup, generated by a (non-unique) basis $\mathbf{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$:

$$\mathcal{L} = \sum_{i=1}^{n} (\mathbb{Z} \cdot \mathbf{b}_i)$$



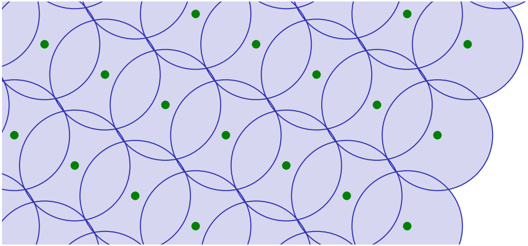
- Represent coset $\mathbf{x} + \mathcal{L} \in (\mathbb{R}^n/\mathcal{L})$ by unique $\bar{\mathbf{x}} \in (\mathbf{x} + \mathcal{L}) \cap \mathcal{P}(\mathbf{B})$.
- Minimum distance: length of shortest nonzero lattice vector

$$\lambda_1(\mathcal{L}) = \min_{\mathbf{0} \neq \mathbf{v} \in \mathcal{L}} \|\mathbf{v}\|.$$

Lattices

- An n-dimensional lattice $\mathcal{L} \subset \mathbb{R}^n$ is a discrete additive subgroup, generated by a (non-unique) basis $\mathbf{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$:

$$\mathcal{L} = \sum_{i=1}^{n} (\mathbb{Z} \cdot \mathbf{b}_i)$$



- Represent coset $\mathbf{x} + \mathcal{L} \in (\mathbb{R}^n / \mathcal{L})$ by unique $\bar{\mathbf{x}} \in (\mathbf{x} + \mathcal{L}) \cap \mathcal{P}(\mathbf{B})$.
- Minimum distance: length of shortest nonzero lattice vector

$$\lambda_1(\mathcal{L}) = \min_{\mathbf{0} \neq \mathbf{v} \in \mathcal{L}} \|\mathbf{v}\|.$$

- Covering radius: maximum distance from the lattice

$$\mu(\mathcal{L}) = \max_{\mathbf{x} \in \mathbb{R}^n} \mathsf{dist}(\mathbf{x}, \mathcal{L}).$$

The Smoothing Parameter [MicciancioRegev'04]

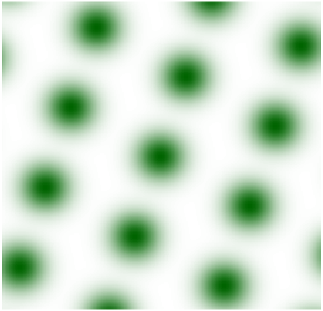
- $\eta_\varepsilon(\mathcal{L})$ = minimal Gaussian 'blur' that 'smooths out' $\mathcal{L}$

  (up to error ε: think $2^{-n} \le \varepsilon \le 1/2$)

The Smoothing Parameter [MiccioncioRegev'04]

- $\eta_\varepsilon(\mathcal{L})$ = minimal Gaussian 'blur' that 'smooths out' $\mathcal{L}$

  (up to error ε: think $2^{-n} \leq \varepsilon \leq 1/2$)



The Smoothing Parameter [MicciancioRegev'04]

- $\eta_\varepsilon(\mathcal{L})$ = minimal Gaussian 'blur' that 'smooths out' $\mathcal{L}$

  (up to error ε: think $2^{-n} \leq \varepsilon \leq 1/2$)

The Smoothing Parameter [MicciancioRegev'04]

- $\eta_\varepsilon(\mathcal{L})$ = minimal Gaussian 'blur' that 'smooths out' $\mathcal{L}$

  (up to error ε: think $2^{-n} \leq \varepsilon \leq 1/2$)

The Smoothing Parameter [MicciancioRegev'04]

- $\eta_\varepsilon(\mathcal{L})$ = minimal Gaussian 'blur' that 'smooths out' $\mathcal{L}$

(up to error ε: think $2^{-n} \leq \varepsilon \leq 1/2$)

Applications

- Worst-case to average-case reductions [MR'04,Regev'05]

The Smoothing Parameter [MicciancioRegev'04]

- $\eta_\varepsilon(\mathcal{L})$ = minimal Gaussian 'blur' that 'smooths out' $\mathcal{L}$

(up to error ε: think $2^{-n} \leq \varepsilon \leq 1/2$)

Applications

- Worst-case to average-case reductions [MR'04,Regev'05]
- Constructions of cryptographic primitives [GPV'08,...]

The Smoothing Parameter [MicciancioRegev'04]

- $\eta_\varepsilon(\mathcal{L})$ = minimal Gaussian 'blur' that 'smooths out' $\mathcal{L}$

(up to error ε: think $2^{-n} \leq \varepsilon \leq 1/2$)

Applications

- Worst-case to average-case reductions [MR'04,Regev'05]
- Constructions of cryptographic primitives [GPV'08,...]
- Algorithms for SVP and CVP [ADRS'15,ADS'15]

The Smoothing Parameter Problem [ChungDadushLiuPeikert'13]

Definition: γ-GapSPP$_\varepsilon$

- Given a lattice $\mathcal{L}$, is

$$\eta_\varepsilon(\mathcal{L}) \leq 1 \qquad \text{OR} \qquad \eta_\varepsilon(\mathcal{L}) > \gamma \quad ?$$

The Smoothing Parameter Problem [ChungDadushLiuPeikert'13]

Definition: γ-GapSPP$_\varepsilon$

- Given a lattice $\mathcal{L}$, is

$$\eta_\varepsilon(\mathcal{L}) \leq 1 \qquad \text{OR} \qquad \eta_\varepsilon(\mathcal{L}) > \gamma \quad ?$$

- Equivalent to 'classical' problems like GapSVP, up to $\approx \sqrt{n}$ factors.

The Smoothing Parameter Problem [ChungDadushLiuPeikert'13]

Definition: γ-GapSPP$_\varepsilon$

- Given a lattice $\mathcal{L}$, is

$$\eta_\varepsilon(\mathcal{L}) \le 1 \qquad \text{OR} \qquad \eta_\varepsilon(\mathcal{L}) > \gamma \quad ?$$

- Equivalent to 'classical' problems like GapSVP, up to $\approx \sqrt{n}$ factors.
  We're interested in non-trivial factors, where equivalence doesn't help.

The Smoothing Parameter Problem [ChungDadushLiuPeikert'13]

Definition: γ-GapSPP$_\varepsilon$

- Given a lattice $\mathcal{L}$, is

$$\eta_\varepsilon(\mathcal{L}) \leq 1 \qquad \text{OR} \qquad \eta_\varepsilon(\mathcal{L}) > \gamma \quad ?$$

- Equivalent to 'classical' problems like GapSVP, up to $\approx \sqrt{n}$ factors.
  We're interested in non-trivial factors, where equivalence doesn't help.

GapSPP is Central

The Smoothing Parameter Problem [ChungDadushLiuPeikert'13]

Definition: γ-GapSPP$_\varepsilon$

- Given a lattice $\mathcal{L}$, is

$$\eta_\varepsilon(\mathcal{L}) \leq 1 \qquad \text{OR} \qquad \eta_\varepsilon(\mathcal{L}) > \gamma \quad ?$$

- Equivalent to 'classical' problems like GapSVP, up to $\approx \sqrt{n}$ factors. We're interested in non-trivial factors, where equivalence doesn't help.

GapSPP is Central

- Replacing 'classic' problems w/GapSPP in proof systems [GG'98] and worst-case to average-case reductions [MR'04,R'05] subsumes the original results, and yields seemingly stronger ones.

The Smoothing Parameter Problem [ChungDadushLiuPeikert'13]

Definition: γ-GapSPP$_\varepsilon$

- Given a lattice $\mathcal{L}$, is

$$\eta_\varepsilon(\mathcal{L}) \leq 1 \qquad \text{OR} \qquad \eta_\varepsilon(\mathcal{L}) > \gamma \quad ?$$

- Equivalent to 'classical' problems like GapSVP, up to $\approx \sqrt{n}$ factors. We're interested in non-trivial factors, where equivalence doesn't help.

GapSPP is Central

- Replacing 'classic' problems w/GapSPP in proof systems [GG'98] and worst-case to average-case reductions [MR'04,R'05] subsumes the original results, and yields seemingly stronger ones.
- GapSPP $\in$ SZK $\subseteq$ AM $\cap$ coAM [CDLP'13], but classic problems $\in$ NISZK, coNP [AR'04,PV'08].

The Smoothing Parameter Problem [ChungDadushLiuPeikert'13]

Definition: γ-GapSPP$_\varepsilon$

- Given a lattice $\mathcal{L}$, is

$$\eta_\varepsilon(\mathcal{L}) \leq 1 \qquad \text{OR} \qquad \eta_\varepsilon(\mathcal{L}) > \gamma \quad ?$$

- Equivalent to 'classical' problems like GapSVP, up to $\approx \sqrt{n}$ factors.
  We're interested in non-trivial factors, where equivalence doesn't help.

GapSPP is Central

- Replacing 'classic' problems w/GapSPP in proof systems [GG'98] and worst-case to average-case reductions [MR'04,R'05] subsumes the original results, and yields seemingly stronger ones.
- GapSPP $\in$ SZK $\subseteq$ AM $\cap$ coAM [CDLP'13], but
  classic problems $\in$ NISZK, coNP [AR'04,PV'08].

Motivating Question

Are there noninteractive proof systems for GapSPP?

Our Results

- Noninteractive (NISZK/coNP) proof systems for GapSPP, improving prior 'trivial' factors by $\approx \sqrt{n}$.

Our Results

- Noninteractive (NISZK/coNP) proof systems for GapSPP, improving prior 'trivial' factors by $\approx \sqrt{n}$.

	Prior γ	Our γ	Efficient-Prover γ
γ-GapSPP$_\varepsilon \in$ NISZK	$\sqrt{n \log(1/\varepsilon)}$	$\log(n)\sqrt{\log(1/\varepsilon)}$	$\sqrt{n \log^3(n) \log(1/\varepsilon)}$

Our Results

- Noninteractive (NISZK/coNP) proof systems for GapSPP, improving prior 'trivial' factors by $\approx \sqrt{n}$.

	Prior γ	Our γ	Efficient-Prover γ
γ-GapSPP$_\varepsilon \in$ NISZK	$\sqrt{n \log(1/\varepsilon)}$	$\log(n)\sqrt{\log(1/\varepsilon)}$	$\sqrt{n \log^3(n) \log(1/\varepsilon)}$
γ-GapSPP$_\varepsilon \in$ coNP	$\sqrt{n / \log(1/\varepsilon)}$	$\log(n)$	——

Our Results

- Noninteractive (NISZK/coNP) proof systems for GapSPP, improving prior 'trivial' factors by $\approx \sqrt{n}$.
- Bonus: improved SZK proof system for GapCRP (covering radius).

	Prior γ	Our γ	Efficient-Prover γ
γ-GapSPP$_\varepsilon$ $\in$ NISZK	$\sqrt{n \log(1/\varepsilon)}$	$\log(n)\sqrt{\log(1/\varepsilon)}$	$\sqrt{n \log^3(n) \log(1/\varepsilon)}$
γ-GapSPP$_\varepsilon$ $\in$ coNP	$\sqrt{n/\log(1/\varepsilon)}$	$\log(n)$	——
γ-GapCRP $\in$ SZK	$\omega(n\sqrt{\log n})$	$O(\sqrt{n})$	$\omega(n\sqrt{\log n})$

Our Results

- Noninteractive (NISZK/coNP) proof systems for GapSPP, improving prior 'trivial' factors by $\approx \sqrt{n}$.
- Bonus: improved SZK proof system for GapCRP (covering radius).

	Prior γ	Our γ	Efficient-Prover γ
γ-GapSPP$_\varepsilon \in$ NISZK	$\sqrt{n \log(1/\varepsilon)}$	$\log(n)\sqrt{\log(1/\varepsilon)}$	$\sqrt{n \log^3(n) \log(1/\varepsilon)}$
γ-GapSPP$_\varepsilon \in$ coNP	$\sqrt{n/\log(1/\varepsilon)}$	$\log(n)$	——
γ-GapCRP $\in$ SZK	$\omega(n\sqrt{\log n})$	$O(\sqrt{n})$	$\omega(n\sqrt{\log n})$

Two NISZK Proofs for GapSPP

1. A 'direct' proof (with efficient prover) for negligible ε.

Our Results

- Noninteractive (NISZK/coNP) proof systems for GapSPP, improving prior 'trivial' factors by $\approx \sqrt{n}$.
- Bonus: improved SZK proof system for GapCRP (covering radius).

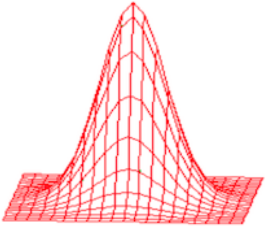
	Prior γ	Our γ	Efficient-Prover γ
γ-GapSPP$_\varepsilon$ $\in$ NISZK	$\sqrt{n \log(1/\varepsilon)}$	$\log(n)\sqrt{\log(1/\varepsilon)}$	$\sqrt{n \log^3(n) \log(1/\varepsilon)}$
γ-GapSPP$_\varepsilon$ $\in$ coNP	$\sqrt{n/\log(1/\varepsilon)}$	$\log(n)$	——
γ-GapCRP $\in$ SZK	$\omega(n\sqrt{\log n})$	$O(\sqrt{n})$	$\omega(n\sqrt{\log n})$

Two NISZK Proofs for GapSPP

1. A 'direct' proof (with efficient prover) for negligible ε.
2. A reduction to EntropyApproximation $\in$ NISZK for any $\varepsilon < 1/2$.

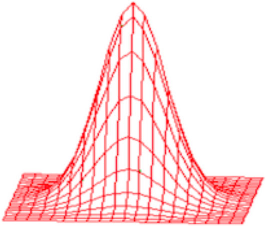
Direct Proof of GapSPP $\in$ NISZK

Discrete Gaussians over Lattices



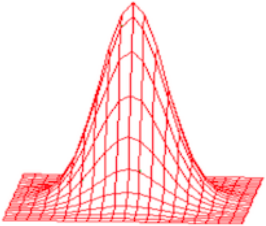
- Sample $\mathbf{x} \in \mathbb{R}^n$ from continuous Gaussian of width $\geq \eta(\mathcal{L})$.

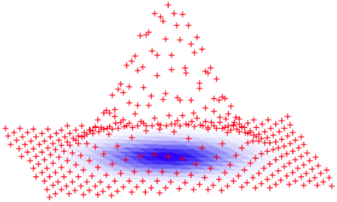
Discrete Gaussians over Lattices



- Sample $\mathbf{x} \in \mathbb{R}^n$ from continuous Gaussian of width $\geq \eta(\mathcal{L})$.
- Coset $\mathbf{c} = \mathbf{x} + \mathcal{L}$ is uniform* over $\mathbb{R}^n/\mathcal{L}$ [MR'04].

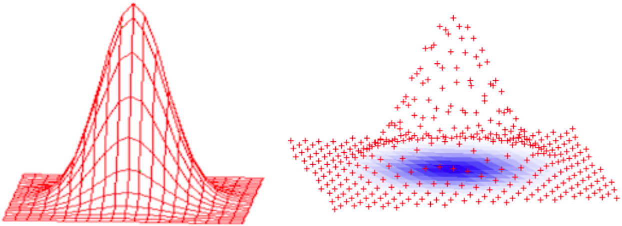
Discrete Gaussians over Lattices





- Sample $\mathbf{x} \in \mathbb{R}^n$ from continuous Gaussian of width $\geq \eta(\mathcal{L})$.
- Coset $\mathbf{c} = \mathbf{x} + \mathcal{L}$ is uniform* over $\mathbb{R}^n/\mathcal{L}$ [MR'04].
- Given coset $\mathbf{c}$, conditional distribution of $\mathbf{x}$ is discrete Gaussian $D_{\mathbf{c}+\mathcal{L}}$.

Discrete Gaussians over Lattices



- Sample $\mathbf{x} \in \mathbb{R}^n$ from continuous Gaussian of width $\geq \eta(\mathcal{L})$.
- Coset $\mathbf{c} = \mathbf{x} + \mathcal{L}$ is uniform* over $\mathbb{R}^n/\mathcal{L}$ [MR'04].
- Given coset $\mathbf{c}$, conditional distribution of $\mathbf{x}$ is discrete Gaussian $D_{\mathbf{c}+\mathcal{L}}$.
- $D_{\mathbf{c}+\mathcal{L}}$ has Gaussian-like properties, e.g., sharp concentration bounds.

Noninteractive Proof System [PeikertVaikuntanathan'08]

- Random String: uniform cosets $\mathbf{c}_i \leftarrow \mathbb{R}^n/\mathcal{L}$ for $i = 1, \ldots, m$.

Noninteractive Proof System [PeikertVaikuntanathan'08]

- Random String: uniform cosets $\mathbf{c}_i \leftarrow \mathbb{R}^n/\mathcal{L}$ for $i = 1, \ldots, m$.
- Prover: sample $\mathbf{e}_i \sim D_{\mathbf{c}_i+\mathcal{L}}$ for each i.

Noninteractive Proof System [PeikertVaikuntanathan'08]

- Random String: uniform cosets $\mathbf{c}_i \leftarrow \mathbb{R}^n/\mathcal{L}$ for $i = 1, \ldots, m$.
- Prover: sample $\mathbf{e}_i \sim D_{\mathbf{c}_i+\mathcal{L}}$ for each i.
- Verifier: accept iff each $\mathbf{e}_i \in \mathbf{c}_i + \mathcal{L}$ and $\sigma_1(\sum \mathbf{e}_i\mathbf{e}_i^T) \leq 3m$.

Noninteractive Proof System [PeikertVaikuntanathan'08]

- Random String: uniform cosets $\mathbf{c}_i \leftarrow \mathbb{R}^n/\mathcal{L}$ for $i = 1, \ldots, m$.
- Prover: sample $\mathbf{e}_i \sim D_{\mathbf{c}_i+\mathcal{L}}$ for each i.
- Verifier: accept iff each $\mathbf{e}_i \in \mathbf{c}_i + \mathcal{L}$ and $\sigma_1(\sum \mathbf{e}_i\mathbf{e}_i^T) \leq 3m$.
- Simulator: first sample $\mathbf{e}_i$ from continuous Gaussian as proof, then output cosets $\mathbf{c}_i = \mathbf{e}_i + \mathcal{L}$ as random string.

Noninteractive Proof System [PeikertVaikuntanathan'08]

- Random String: uniform cosets $\mathbf{c}_i \leftarrow \mathbb{R}^n/\mathcal{L}$ for $i = 1, \ldots, m$.
- Prover: sample $\mathbf{e}_i \sim D_{\mathbf{c}_i+\mathcal{L}}$ for each i.
- Verifier: accept iff each $\mathbf{e}_i \in \mathbf{c}_i + \mathcal{L}$ and $\sigma_1(\sum \mathbf{e}_i\mathbf{e}_i^T) \leq 3m$.
- Simulator: first sample $\mathbf{e}_i$ from continuous Gaussian as proof, then output cosets $\mathbf{c}_i = \mathbf{e}_i + \mathcal{L}$ as random string.

Completeness ✓

- Suppose $\eta(\mathcal{L}) \leq 1$: implied by $\lambda_1(\mathcal{L}^*) > \sqrt{n}$.
- Then $\sigma_1(\sum \mathbf{e}_i\mathbf{e}_i^T) \leq 3m$, by matrix concentration bounds on $D_{\mathbf{c}_i+\mathcal{L}}$.

Noninteractive Proof System [PeikertVaikuntanathan'08]

- Random String: uniform cosets $\mathbf{c}_i \leftarrow \mathbb{R}^n/\mathcal{L}$ for $i = 1, \ldots, m$.
- Prover: sample $\mathbf{e}_i \sim D_{\mathbf{c}_i+\mathcal{L}}$ for each i.
- Verifier: accept iff each $\mathbf{e}_i \in \mathbf{c}_i + \mathcal{L}$ and $\sigma_1(\sum \mathbf{e}_i\mathbf{e}_i^T) \leq 3m$.
- Simulator: first sample $\mathbf{e}_i$ from continuous Gaussian as proof, then output cosets $\mathbf{c}_i = \mathbf{e}_i + \mathcal{L}$ as random string.

Zero Knowledge ✓

- Suppose $\eta(\mathcal{L}) \leq 1$.
- Then cosets $\mathbf{c}_i = \mathbf{e}_i + \mathcal{L}$ are uniform* in $\mathbb{R}^n/\mathcal{L}$, and $\mathbf{e}_i \sim D_{\mathbf{c}_i+\mathcal{L}}$ conditioned on $\mathbf{c}_i$.

Noninteractive Proof System [PeikertVaikuntanathan'08]

- Random String: uniform cosets $\mathbf{c}_i \leftarrow \mathbb{R}^n/\mathcal{L}$ for $i = 1, \ldots, m$.
- Prover: sample $\mathbf{e}_i \sim D_{\mathbf{c}_i+\mathcal{L}}$ for each i.
- Verifier: accept iff each $\mathbf{e}_i \in \mathbf{c}_i + \mathcal{L}$ and $\sigma_1(\sum \mathbf{e}_i\mathbf{e}_i^T) \le 3m$.
- Simulator: first sample $\mathbf{e}_i$ from continuous Gaussian as proof, then output cosets $\mathbf{c}_i = \mathbf{e}_i + \mathcal{L}$ as random string.

Soundness

- If $\lambda_1(\mathcal{L}^*) \le 1/10$, only $2^{-\Omega(n)}$-fraction of $\{\mathbf{c}_i\}$ have valid proof $\{\mathbf{e}_i\}$.

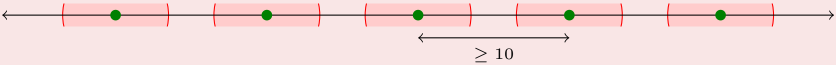
Noninteractive Proof System [PeikertVaikuntanathan'08]

- Random String: uniform cosets $\mathbf{c}_i \leftarrow \mathbb{R}^n/\mathcal{L}$ for $i = 1, \ldots, m$.
- Prover: sample $\mathbf{e}_i \sim D_{\mathbf{c}_i+\mathcal{L}}$ for each i.
- Verifier: accept iff each $\mathbf{e}_i \in \mathbf{c}_i + \mathcal{L}$ and $\sigma_1(\sum \mathbf{e}_i\mathbf{e}_i^T) \leq 3m$.
- Simulator: first sample $\mathbf{e}_i$ from continuous Gaussian as proof, then output cosets $\mathbf{c}_i = \mathbf{e}_i + \mathcal{L}$ as random string.

Soundness

- If $\lambda_1(\mathcal{L}^*) \leq 1/10$, only $2^{-\Omega(n)}$-fraction of $\{\mathbf{c}_i\}$ have valid proof $\{\mathbf{e}_i\}$.

  Intuition: projecting $\mathcal{L}$ and sufficiently small $\mathbf{e}_i$ onto span$(\mathbf{v}^*)$ yields



Unlikely that all the random $\mathbf{c}_i$ project to 'good' region.

Noninteractive Proof System [PeikertVaikuntanathan'08]

- Random String: uniform cosets $\mathbf{c}_i \leftarrow \mathbb{R}^n/\mathcal{L}$ for $i = 1, \ldots, m$.
- Prover: sample $\mathbf{e}_i \sim D_{\mathbf{c}_i+\mathcal{L}}$ for each i.
- Verifier: accept iff each $\mathbf{e}_i \in \mathbf{c}_i + \mathcal{L}$ and $\sigma_1(\sum \mathbf{e}_i \mathbf{e}_i^T) \leq 3m$.
- Simulator: first sample $\mathbf{e}_i$ from continuous Gaussian as proof, then output cosets $\mathbf{c}_i = \mathbf{e}_i + \mathcal{L}$ as random string.

Conclusion

Completeness, simulation (for $\eta \leq 1 \Longleftarrow \lambda_1^* > \sqrt{n}$)

& soundness (for $\lambda_1^* \leq 1/10$)

$\Downarrow$

this is a NISZK for $O(\sqrt{n})$-coGapSVP.

Noninteractive Proof System [PeikertVaikuntanathan'08]

- Random String: uniform cosets $\mathbf{c}_i \leftarrow \mathbb{R}^n/\mathcal{L}$ for $i = 1, \ldots, m$.
- Prover: sample $\mathbf{e}_i \sim D_{\mathbf{c}_i+\mathcal{L}}$ for each i.
- Verifier: accept iff each $\mathbf{e}_i \in \mathbf{c}_i + \mathcal{L}$ and $\sigma_1(\sum \mathbf{e}_i \mathbf{e}_i^T) \leq 3m$.
- Simulator: first sample $\mathbf{e}_i$ from continuous Gaussian as proof, then output cosets $\mathbf{c}_i = \mathbf{e}_i + \mathcal{L}$ as random string.

Conclusion

Completeness, simulation (for $\eta \leq 1 \Longleftarrow \lambda_1^* > \sqrt{n}$)

& soundness (for $\lambda_1^* \leq 1/10$)

$$\Downarrow$$

this is a NISZK for $O(\sqrt{n})$-coGapSVP.

- Can the same proof system work for GapSPP?

Soundness via Sparse Projections

Reverse Minkowski Theorem [RegevStephens-Davidowitz'17]

- Intuition: a lattice is not smooth $\Leftrightarrow$ it has a 'sparse' lattice projection.

Soundness via Sparse Projections

Reverse Minkowski Theorem [RegevStephens-Davidowitz'17]

- Intuition: a lattice is not smooth $\Leftrightarrow$ it has a 'sparse' lattice projection.
- More precisely: if $\eta(\mathcal{L}) > C \log n$ then there is a rank-k projection π such that $\det(\pi(\mathcal{L})) \geq 6^k$, for some k.

Soundness via Sparse Projections

Reverse Minkowski Theorem [RegevStephens-Davidowitz'17]

- Intuition: a lattice is not smooth $\Leftrightarrow$ it has a 'sparse' lattice projection.
- More precisely: if $\eta(\mathcal{L}) > C \log n$ then there is a rank-k projection π such that $\det(\pi(\mathcal{L})) \geq 6^k$, for some k.

Soundness

$$3m \geq s_1\left(\sum \mathbf{e}_i \mathbf{e}_i^T\right) \geq s_1\left(\sum \pi(\mathbf{e}_i)\pi(\mathbf{e}_i)^T\right) \geq \frac{1}{k} \sum \|\pi(\mathbf{e}_i)\|^2.$$

Soundness via Sparse Projections

Reverse Minkowski Theorem [RegevStephens-Davidowitz'17]

- Intuition: a lattice is not smooth $\Leftrightarrow$ it has a 'sparse' lattice projection.
- More precisely: if $\eta(\mathcal{L}) > C \log n$ then there is a rank-k projection π such that $\det(\pi(\mathcal{L})) \geq 6^k$, for some k.

Soundness

$$3m \geq s_1\left(\sum \mathbf{e}_i \mathbf{e}_i^T\right) \geq s_1\left(\sum \pi(\mathbf{e}_i)\pi(\mathbf{e}_i)^T\right) \geq \frac{1}{k}\sum \|\pi(\mathbf{e}_i)\|^2.$$

- So vol(legal $\{\pi(\mathbf{e}_i)\}$) $\leq 5^{km}$.

Soundness via Sparse Projections

Reverse Minkowski Theorem [RegevStephens-Davidowitz'17]

- Intuition: a lattice is not smooth $\Leftrightarrow$ it has a 'sparse' lattice projection.
- More precisely: if $\eta(\mathcal{L}) > C \log n$ then there is a rank-k projection π such that $\det(\pi(\mathcal{L})) \geq 6^k$, for some k.

Soundness

$$3m \geq s_1\Big(\sum \mathbf{e}_i \mathbf{e}_i^T\Big) \geq s_1\Big(\sum \pi(\mathbf{e}_i)\pi(\mathbf{e}_i)^T\Big) \geq \frac{1}{k}\sum \|\pi(\mathbf{e}_i)\|^2.$$

- So vol(legal $\{\pi(\mathbf{e}_i)\}$) $\leq 5^{km}$.
- But vol(possible $\{\pi(\mathbf{c}_i)\}$) $\geq 6^{km} \gg 5^{km} \geq$ vol(legal $\{\pi(\mathbf{e}_i)\}$), so most $\{\mathbf{c}_i\}$ have no valid proof $\{\mathbf{e}_i\}$.

Soundness via Sparse Projections

Reverse Minkowski Theorem [RegevStephens-Davidowitz'17]

- Intuition: a lattice is not smooth $\Leftrightarrow$ it has a 'sparse' lattice projection.
- More precisely: if $\eta(\mathcal{L}) > C \log n$ then there is a rank-k projection π such that $\det(\pi(\mathcal{L})) \geq 6^k$, for some k.

Soundness

$$3m \geq s_1\left(\sum \mathbf{e}_i\mathbf{e}_i^T\right) \geq s_1\left(\sum \pi(\mathbf{e}_i)\pi(\mathbf{e}_i)^T\right) \geq \frac{1}{k}\sum \|\pi(\mathbf{e}_i)\|^2.$$

- So vol(legal $\{\pi(\mathbf{e}_i)\}$) $\leq 5^{km}$.
- But vol(possible $\{\pi(\mathbf{c}_i)\}$) $\geq 6^{km} \gg 5^{km} \geq$ vol(legal $\{\pi(\mathbf{e}_i)\}$), so most $\{\mathbf{c}_i\}$ have no valid proof $\{\mathbf{e}_i\}$.
- Conclusion: $\approx \log n$ gap in $\eta(\mathcal{L})$ between completeness, soundness.

Indirect Proof: GapSPP $\leq$ EntropyApproximation

- The previous proof system required $\varepsilon = \text{negl}$ for SZK.
  What about 'large' ε?

Indirect Proof: GapSPP $\leq$ EntropyApproximation

- The previous proof system required $\varepsilon = \mathrm{negl}$ for SZK. What about 'large' ε?
- $\eta(\mathcal{L}) \leq 1 \Rightarrow$ continuous Gaussian mod $\mathcal{L}$ is ε-uniform.

Indirect Proof: GapSPP $\leq$ EntropyApproximation

- The previous proof system required $\varepsilon = \text{negl}$ for SZK.
  What about 'large' ε?
- $\eta(\mathcal{L}) \leq 1 \Rightarrow$ continuous Gaussian mod $\mathcal{L}$ is ε-uniform.

  This distribution has high entropy.

Indirect Proof: GapSPP $\leq$ EntropyApproximation

- The previous proof system required $\varepsilon = \text{negl}$ for SZK.
  What about 'large' ε?

- $\eta(\mathcal{L}) \leq 1 \Rightarrow$ continuous Gaussian mod $\mathcal{L}$ is ε-uniform.

  This distribution has high entropy.

- $\eta(\mathcal{L}) \gg 1 \Rightarrow$ continuous Gaussian mod $\mathcal{L}$ is concentrated on a low-volume subset of $\mathbb{R}^n/\mathcal{L}$.

Indirect Proof: GapSPP $\leq$ EntropyApproximation

- The previous proof system required $\varepsilon = \mathsf{negl}$ for SZK.
  What about 'large' ε?
- $\eta(\mathcal{L}) \leq 1 \Rightarrow$ continuous Gaussian mod $\mathcal{L}$ is ε-uniform.

  This distribution has high entropy.
- $\eta(\mathcal{L}) \gg 1 \Rightarrow$ continuous Gaussian mod $\mathcal{L}$ is concentrated on a low-volume subset of $\mathbb{R}^n/\mathcal{L}$.

  This distribution has low entropy.

Indirect Proof: GapSPP $\leq$ EntropyApproximation

- The previous proof system required $\varepsilon = \text{negl}$ for SZK.
  What about 'large' ε?

- $\eta(\mathcal{L}) \leq 1 \Rightarrow$ continuous Gaussian mod $\mathcal{L}$ is ε-uniform.

  This distribution has high entropy.

- $\eta(\mathcal{L}) \gg 1 \Rightarrow$ continuous Gaussian mod $\mathcal{L}$ is concentrated on a low-volume subset of $\mathbb{R}^n/\mathcal{L}$.

  This distribution has low entropy.

- Yields a Karp reduction γ-GapSPP$_\varepsilon \leq$ EntropyApproximation, with $\gamma = O(\log(n)\sqrt{\log(1/\varepsilon)})$ for any $\varepsilon \in (0, 1/2)$.

Open Problems

1. NP proof system for GapSPP with $o(\sqrt{n})$ approximation factors?

Open Problems

1. NP proof system for GapSPP with $o(\sqrt{n})$ approximation factors?

2. (NI)SZK proof system for GapCRP with $o(\sqrt{n})$ factors?

Open Problems

1. NP proof system for GapSPP with $o(\sqrt{n})$ approximation factors?
2. (NI)SZK proof system for GapCRP with $o(\sqrt{n})$ factors?
3. [CDLP'13] gave SZK proof systems for GapSPP with constant factors. Can we get rid of the $\log n$ factor in NISZK for GapSPP?

Open Problems

1. NP proof system for GapSPP with $o(\sqrt{n})$ approximation factors?

2. (NI)SZK proof system for GapCRP with $o(\sqrt{n})$ factors?

3. [CDLP'13] gave SZK proof systems for GapSPP with constant factors.

   Can we get rid of the $\log n$ factor in NISZK for GapSPP?

4. NIZK for NP from lattice/LWE assumptions?

   [PV'08] gives an approach, but with a major barrier: NI proof for SVP/BDD/LWE.

Open Problems

1. NP proof system for GapSPP with $o(\sqrt{n})$ approximation factors?
2. (NI)SZK proof system for GapCRP with $o(\sqrt{n})$ factors?
3. [CDLP'13] gave SZK proof systems for GapSPP with constant factors. Can we get rid of the $\log n$ factor in NISZK for GapSPP?
4. NIZK for NP from lattice/LWE assumptions?

   [PV'08] gives an approach, but with a major barrier: NI proof for SVP/BDD/LWE.
5. (NI)SZK-completeness of GapSPP for some factors?

Open Problems

1. NP proof system for GapSPP with $o(\sqrt{n})$ approximation factors?

2. (NI)SZK proof system for GapCRP with $o(\sqrt{n})$ factors?

3. [CDLP'13] gave SZK proof systems for GapSPP with constant factors. Can we get rid of the $\log n$ factor in NISZK for GapSPP?

4. NIZK for NP from lattice/LWE assumptions?

   [PV'08] gives an approach, but with a major barrier: NI proof for SVP/BDD/LWE.

5. (NI)SZK-completeness of GapSPP for some factors?

Thanks!