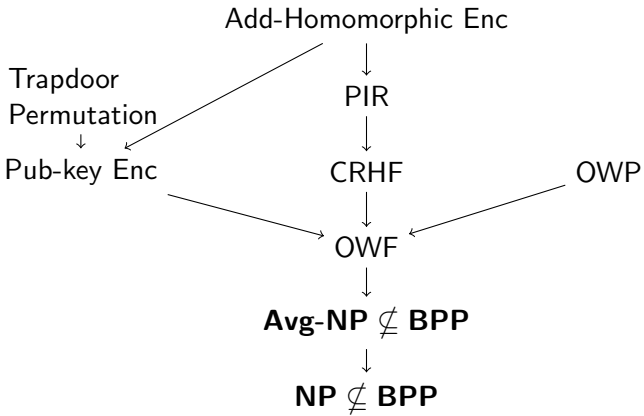
On Basing Search SIVP on NP-Hardness

Tianren Liu

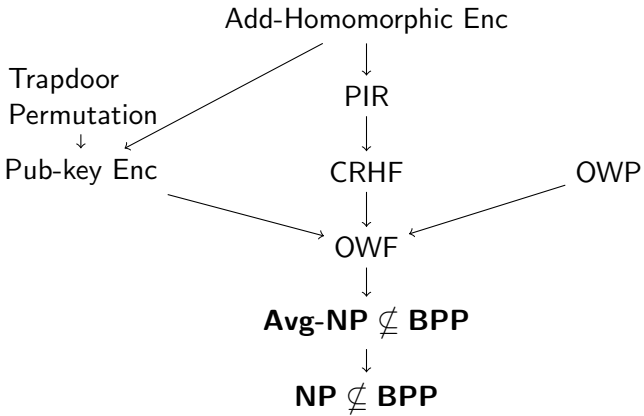
liutr@mit.edu

Sixteenth IACR Theory of Cryptography Conference

Assumptions and Primitives in Cryptography



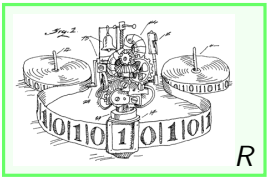
Assumptions and Primitives in Cryptography



Can we prove the security of a cryptographic primitive from the minimal assumption **NP** $\not\subseteq$ **BPP**? (Brassard 1979)

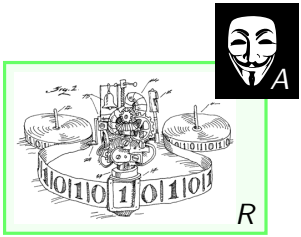
(Black-box) Security Proofs

To prove the security of X based on $\mathbf{NP} \not\subseteq \mathbf{BPP}$, find a (p.p.t.) reduction R s.t. for any oracle A that "breaks the security of X", R^A solves SAT



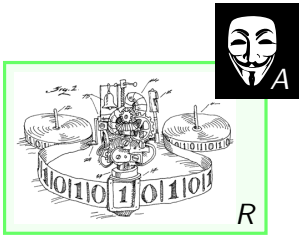
(Black-box) Security Proofs

To prove the security of X based on $\mathbf{NP} \not\subseteq \mathbf{BPP}$, find a (p.p.t.) reduction R s.t. for any oracle A that "breaks the security of X", R^A solves SAT



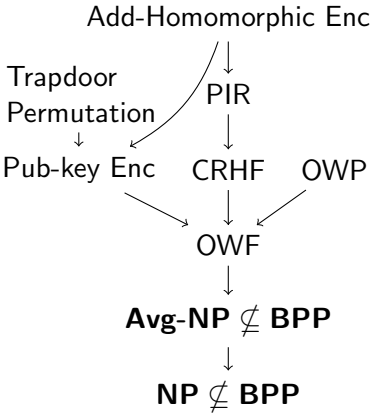
(Black-box) Security Proofs

To prove the security of X based on $\mathbf{NP} \not\subseteq \mathbf{BPP}$, find a (p.p.t.) reduction R s.t. for any oracle A that "breaks the security of X", R^A solves SAT



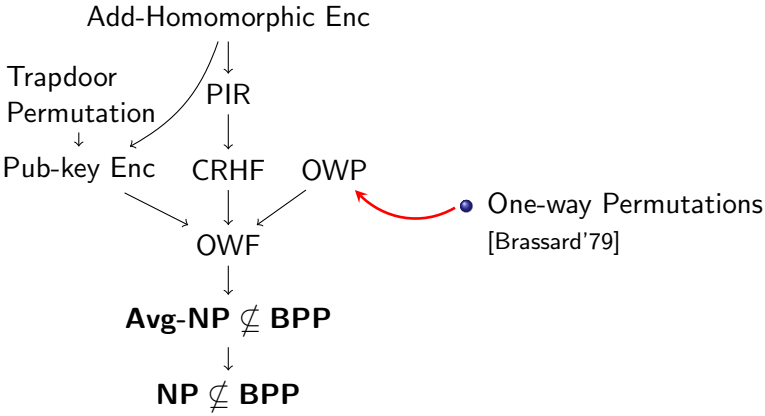
$$\left(x\right) \begin{cases} \text{accepts w.p.} \geq 2/3, & \text{if } x \in \text{SAT} \\ \text{accepts w.p.} \leq 1/3, & \text{if } x \notin \text{SAT} \end{cases}$$

Impossibility Results

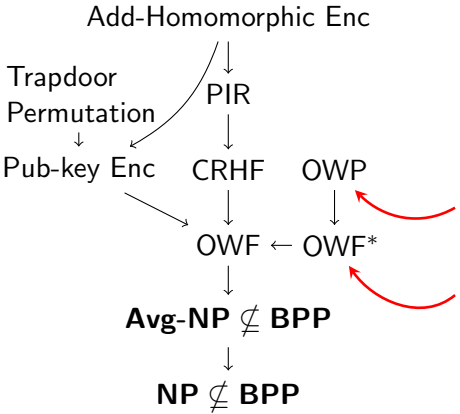


- No known cryptographic scheme based on **NP** $\not\subseteq$ **BPP**.
- Several negative results* [Brassard'79, . . .]

Impossibility Results

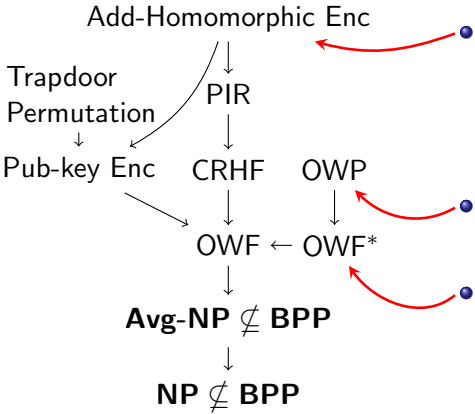


Impossibility Results



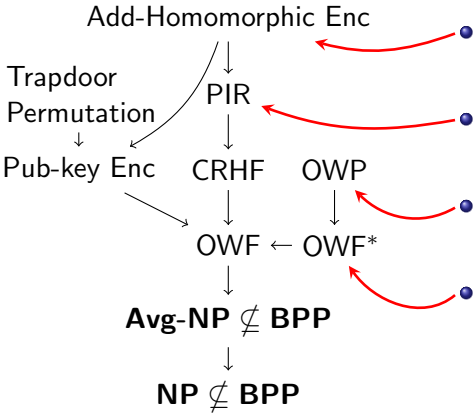
- One-way Permutations
  [Brassard'79]
- Size-Verifiable One-way Functions
  [Akavia-Goldreich-Goldwasser-Moshkovitz'06,
  Bogdanov-Brzuska'14]

Impossibility Results



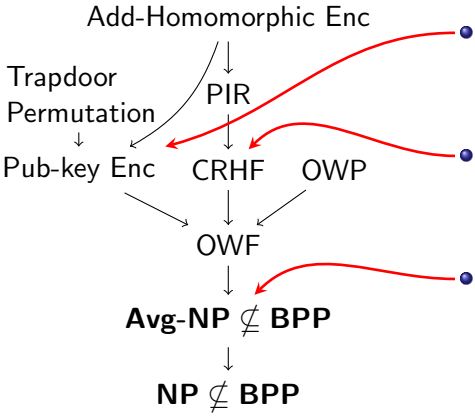
- Add-Homomorphic Encryption
  [Bogdanov-Lee'13]
- One-way Permutations
  [Brassard'79]
- Size-Verifiable One-way Functions
  [Akavia-Goldreich-Goldwasser-Moshkovitz'06, Bogdanov-Brzuska'14]

Impossibility Results



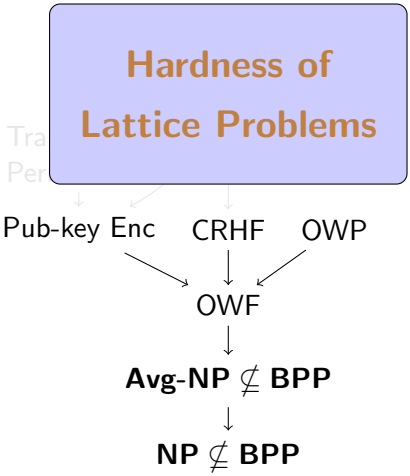
- Add-Homomorphic Encryption
  [Bogdanov-Lee'13]
- Private Information Retrieval
  [Liu-Vaikuntanathan'16]
- One-way Permutations
  [Brassard'79]
- Size-Verifiable One-way Functions
  [Akavia-Goldreich-Goldwasser-Moshkovitz'06, Bogdanov-Brzuska'14]

Impossibility Results (restricting the reductions)

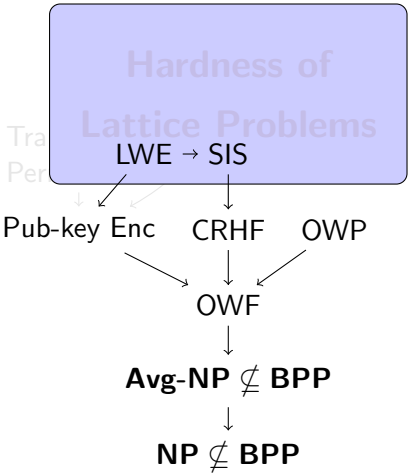


- Public-key Encryption Scheme, via "smart" reduction [Goldreich-Goldwasser'98]
- Collision-resistant Hash Functions, via constant-adaptive reduction [Haitner-Mahmoody-Xiao'09]
- Average-case NP, via non-adaptive reduction [Bogdanov-Trevisan'06]

A New Hope

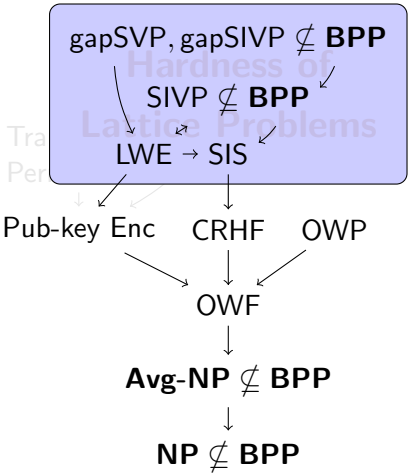

Hardness of
Lattice Problems
Pub-key Enc
CRHF
OWP
OWF
Avg-NP ⊈ BPP
NP ⊈ BPP

A New Hope



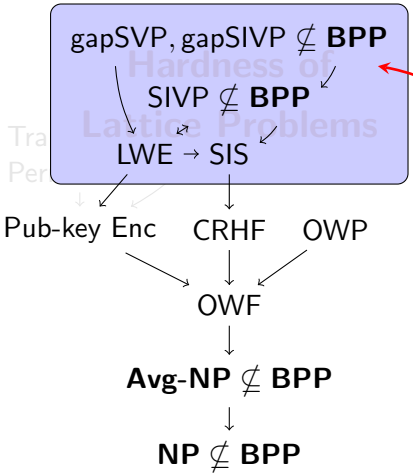
- A successful history of lattice-based cryptography [GGH'97, Regev'05, GPV'08, Gentry'09, BV'11, ...]

A New Hope



- A successful history of lattice-based cryptography [GGH'97, Regev'05, GPV'08, Gentry'09, BV'11, ...]
- Based on **worst-case** hardness of lattice problems such as SIVP, gapSVP [Ajtai'96, MR'04, Regev'05, Peikert'09, LPR'10, MP'12, ...]

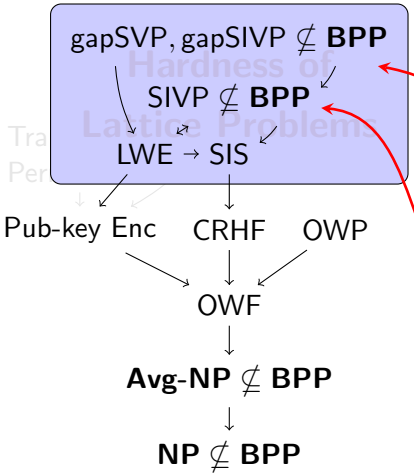
~~A New Hope~~



Impossibility Results [GG'00, MV'03,AR'04,GMR'04,PV'08]

$\text{gapSVP}_{\tilde{O}(\sqrt{n})}, \text{gapSIVP}_{\tilde{O}(\sqrt{n})}$ are not **NP**-hard unless polynomial hierarchy collapses.

A New Hope



Impossibility Results [GG'00, MV'03,AR'04,GMR'04,PV'08]

$\text{gapSVP}_{\tilde{O}(\sqrt{n})}, \text{gapSIVP}_{\tilde{O}(\sqrt{n})}$ are not **NP**-hard unless polynomial hierarchy collapses.

Our Result

Search problem $\text{SIVP}_{\tilde{O}(n)}$ is not **NP**-hard unless polynomial hierarchy collapses.

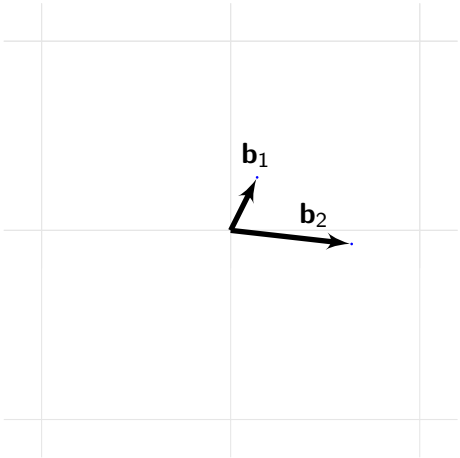
Lattice

- Full-rank discrete additive subgroup in $\mathbb{R}^n$

Lattice

- Full-rank discrete additive subgroup in $\mathbb{R}^n$
- Basis $B = (\mathbf{b}_1, \ldots, \mathbf{b}_n) \in \mathbb{R}^{n \times n}$

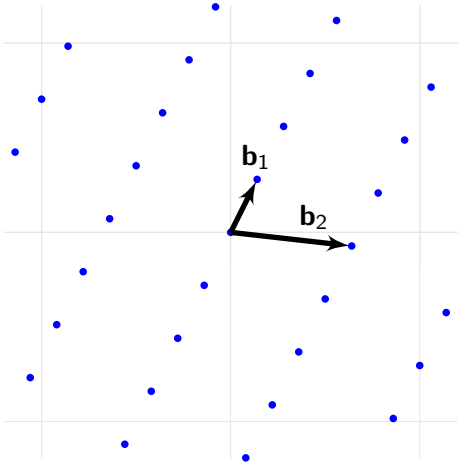
$$\mathcal{L}(B) := \{B\mathbf{z} \mid \mathbf{z} \in \mathbb{Z}^n\}$$



Lattice

- Full-rank discrete additive subgroup in $\mathbb{R}^n$
- Basis $B = (\mathbf{b}_1, \ldots, \mathbf{b}_n) \in \mathbb{R}^{n \times n}$

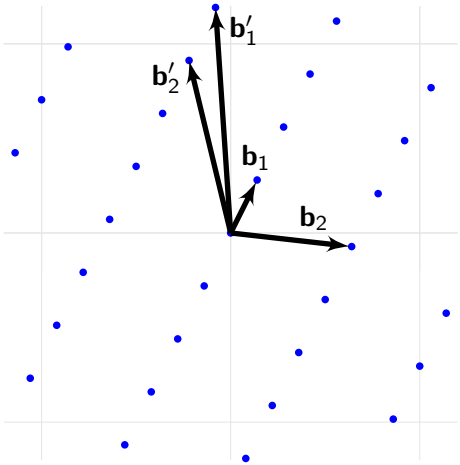
$$\mathcal{L}(B) := \{B\mathbf{z} \mid \mathbf{z} \in \mathbb{Z}^n\}$$



Lattice

- Full-rank discrete additive subgroup in $\mathbb{R}^n$
- Basis $B = (\mathbf{b}_1, \ldots, \mathbf{b}_n) \in \mathbb{R}^{n \times n}$

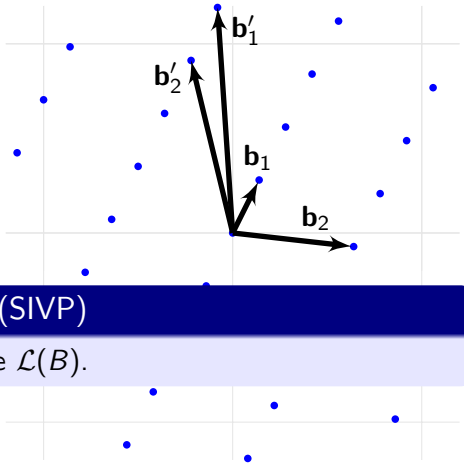
$$\mathcal{L}(B) := \{B\mathbf{z} \mid \mathbf{z} \in \mathbb{Z}^n\}$$



Lattice Problems

- Full-rank discrete additive subgroup in $\mathbb{R}^n$
- Basis $B = (\mathbf{b}_1, \ldots, \mathbf{b}_n) \in \mathbb{R}^{n \times n}$

$$\mathcal{L}(B) := \{B\mathbf{z} \mid \mathbf{z} \in \mathbb{Z}^n\}$$



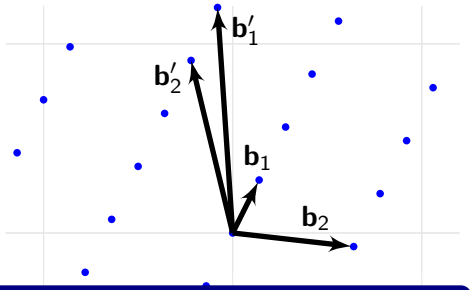
Shortest Independent Vector Problem (SIVP)

Search Find shortest basis in lattice $\mathcal{L}(B)$.

Lattice Problems

- Full-rank discrete additive subgroup in $\mathbb{R}^n$
- Basis $B = (\mathbf{b}_1, \ldots, \mathbf{b}_n) \in \mathbb{R}^{n \times n}$

$$\mathcal{L}(B) := \{B\mathbf{z} \mid \mathbf{z} \in \mathbb{Z}^n\}$$



Shortest Independent Vector Problem (SIVP)

Search Find shortest basis in lattice $\mathcal{L}(B)$.

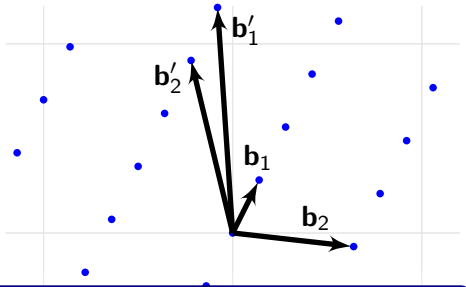
Decision Given a real d, distinguish between $\lambda_n(B) \leq d$ and $\lambda_n(B) > d$.

$\lambda_n(B) :=$ length of the shortest basis in lattice $\mathcal{L}(B)$.

Lattice Problems

- Full-rank discrete additive subgroup in $\mathbb{R}^n$
- Basis $B = (\mathbf{b}_1, \ldots, \mathbf{b}_n) \in \mathbb{R}^{n \times n}$

$$\mathcal{L}(B) := \{B\mathbf{z} \mid \mathbf{z} \in \mathbb{Z}^n\}$$



Shortest Independent Vector Problem (SIVP), γ-Approx.

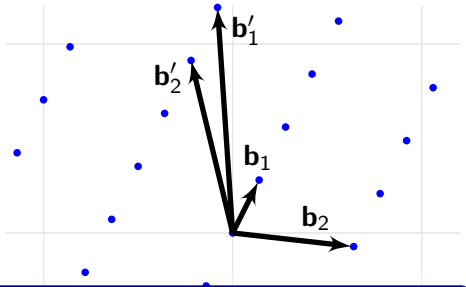
Search Find shortest basis in lattice $\mathcal{L}(B)$.

Decision Given a real d, distinguish between $\lambda_n(B) \leq d$ and $\lambda_n(B) > d$.
$\lambda_n(B) :=$ length of the shortest basis in lattice $\mathcal{L}(B)$.

Lattice Problems

- Full-rank discrete additive subgroup in $\mathbb{R}^n$
- Basis $B = (\mathbf{b}_1, \ldots, \mathbf{b}_n) \in \mathbb{R}^{n \times n}$

$$\mathcal{L}(B) := \{B\mathbf{z} \mid \mathbf{z} \in \mathbb{Z}^n\}$$



Shortest Independent Vector Problem (SIVP), γ-Approx.

SIVP$_\gamma$ Find short basis whose length $\leq \gamma \cdot \lambda_n(B)$.

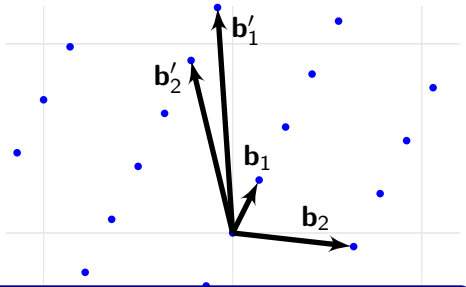
Decision Given a real d, distinguish between $\lambda_n(B) \leq d$ and $\lambda_n(B) > d$.

$\lambda_n(B) :=$ length of the shortest basis in lattice $\mathcal{L}(B)$.

Lattice Problems

- Full-rank discrete additive subgroup in $\mathbb{R}^n$
- Basis $B = (\mathbf{b}_1, \ldots, \mathbf{b}_n) \in \mathbb{R}^{n \times n}$

$$\mathcal{L}(B) := \{B\mathbf{z} \mid \mathbf{z} \in \mathbb{Z}^n\}$$



Shortest Independent Vector Problem (SIVP), γ-Approx.

SIVP_γ Find short basis whose length $\leq \gamma \cdot \lambda_n(B)$.

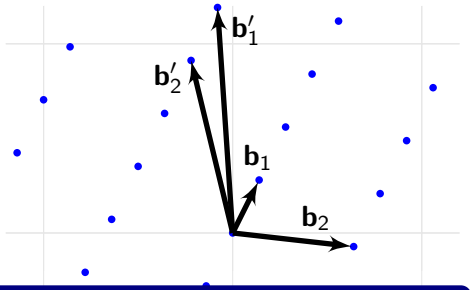
GapSIVP_γ Given a real d, distinguish between $\lambda_n(B) \leq d$ and $\lambda_n(B) > \gamma \cdot d$.

$\lambda_n(B) :=$ length of the shortest basis in lattice $\mathcal{L}(B)$.

Lattice Problems

- Full-rank discrete additive subgroup in $\mathbb{R}^n$
- Basis $B = (\mathbf{b}_1, \ldots, \mathbf{b}_n) \in \mathbb{R}^{n \times n}$

$$\mathcal{L}(B) := \{B\mathbf{z} \mid \mathbf{z} \in \mathbb{Z}^n\}$$



Shortest Vector Problem (SVP), γ-Approx.

SVP_γ Find short non-zero vector whose length $\leq \gamma \cdot \lambda_1(B)$.

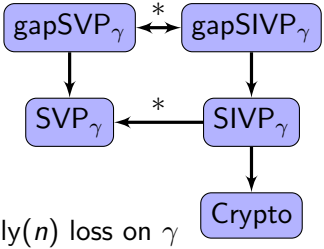
GapSVP_γ Given a real d, distinguish between $\lambda_1(B) \leq d$ and $\lambda_1(B) > \gamma \cdot d$.

$\lambda_1(B) :=$ length of the shortest non-zero vector in lattice $\mathcal{L}(B)$.

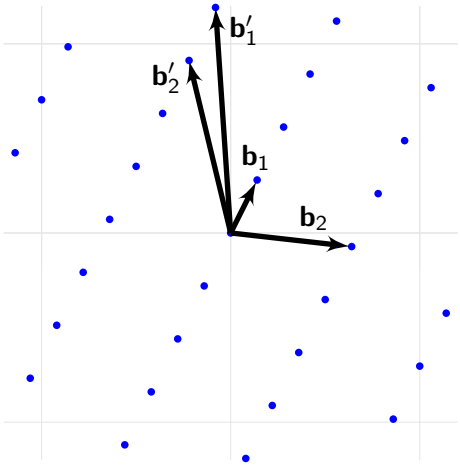
Lattice Problems

- Full-rank discrete additive subgroup in $\mathbb{R}^n$
- Basis $B = (\mathbf{b}_1, \ldots, \mathbf{b}_n) \in \mathbb{R}^{n \times n}$

$$\mathcal{L}(B) := \{B\mathbf{z} \mid \mathbf{z} \in \mathbb{Z}^n\}$$



$*$ poly(n) loss on γ



Lattice

Hardness of gapSIVP$_\gamma$

Hardness of SIVP$_\gamma$

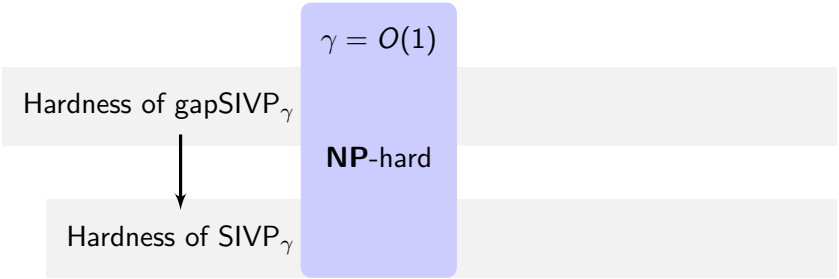
Lattice

Hardness of gapSIVP$_\gamma$ $\gamma = O(1)$ **NP**-hard

Hardness of SIVP$_\gamma$

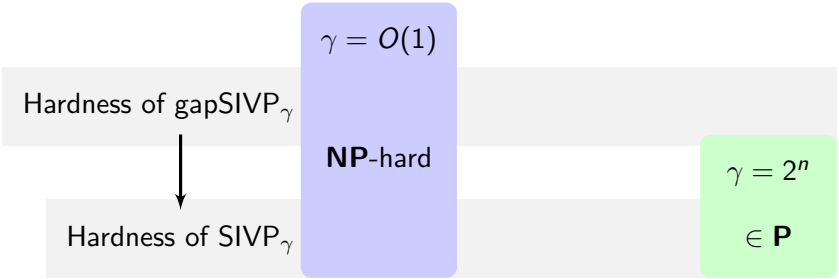
- gapSIVP$_\gamma \geq$ SAT for $\gamma = O(1)$ [Blömer-Seifert'99, Haviv-Regev'06]

Lattice



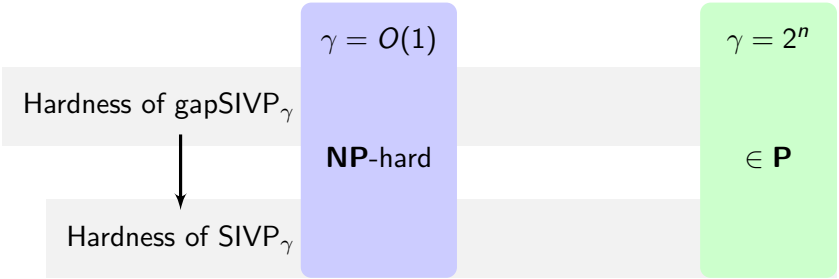
- gapSIVP$_\gamma \geq$ SAT for $\gamma = O(1)$ [Blömer-Seifert'99, Haviv-Regev'06]

Lattice



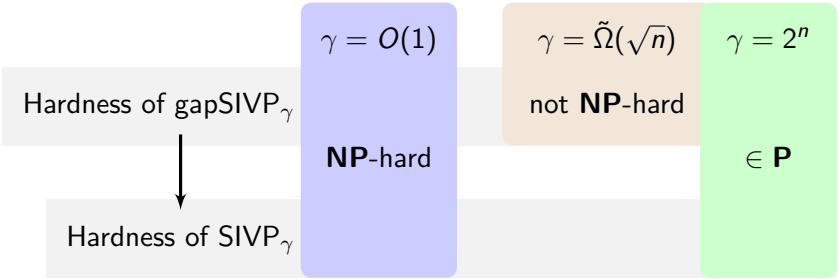
- SIVP$_\gamma \in$ **P** for $\gamma = 2^n$ [LLL]

Lattice



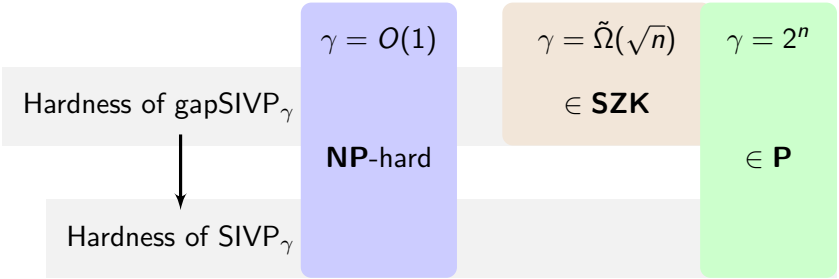
- SIVP$_\gamma \in$ **P** for $\gamma = 2^n$ [LLL]

Lattice



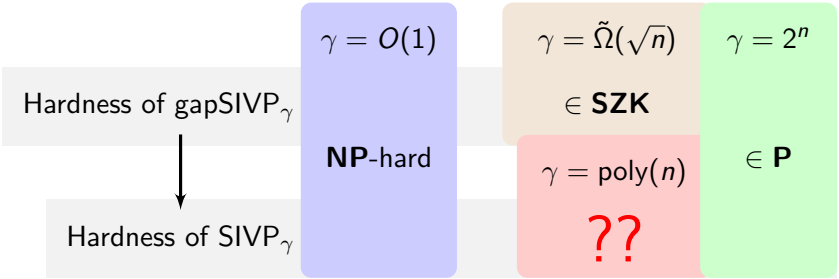
- gapSIVP$_\gamma \in$ **NP** $\cap$ **coNP** for $\gamma = \sqrt{n}$ [Ban'93, GMR'04]
- gapSIVP$_\gamma \in$ **NP** $\cap$ **coAM** for $\gamma = \sqrt{n/\log n}$ [BS'99, GMR'04]

Lattice

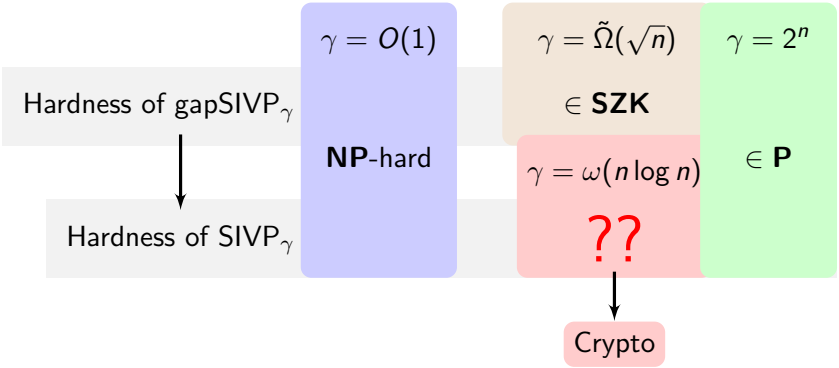


- gapSIVP$_\gamma \in$ **SZK** for any $\gamma = \omega(\sqrt{n \log n})$ [PV'08]

Lattice

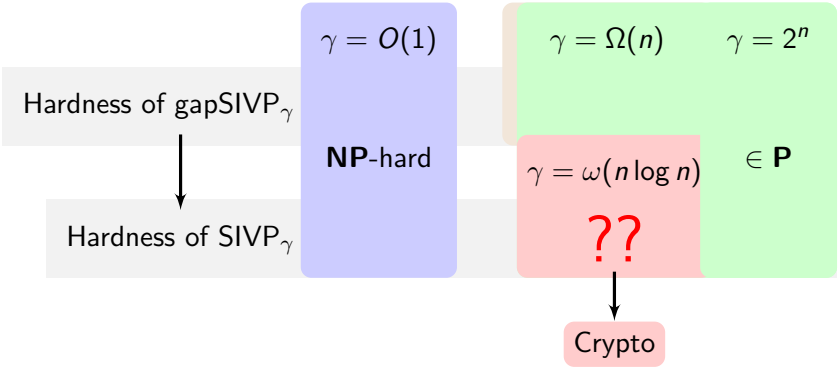

$\gamma = O(1)$
$\gamma = \tilde{\Omega}(\sqrt{n})$
$\gamma = 2^n$
Hardness of gapSIVP$_\gamma$
$\in$ **SZK**
NP-hard
$\gamma = \mathrm{poly}(n)$
$\in$ **P**
??
Hardness of SIVP$_\gamma$

Lattice



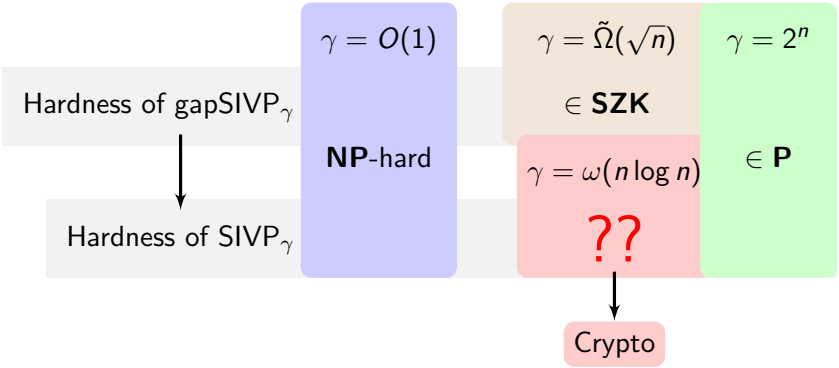
- SIVP$_\gamma$ $\Longrightarrow$ CRHF for any $\gamma = \omega(n \log n)$ [Micciancio-Regev'04]

Lattice

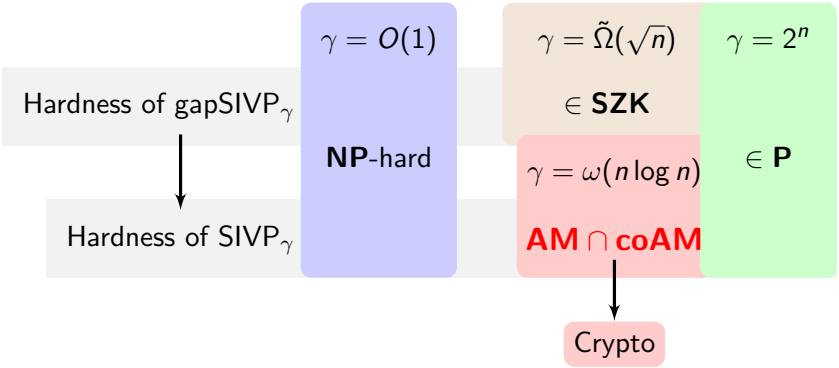


- In ideal lattices, gapSIVP$_n \in$ **P**

Lattice


$\gamma = O(1)$
$\gamma = \tilde{\Omega}(\sqrt{n})$
$\gamma = 2^n$
Hardness of gapSIVP$_\gamma$
$\in$ **SZK**
NP-hard
$\gamma = \omega(n \log n)$
$\in$ **P**
Hardness of SIVP$_\gamma$
??
Crypto

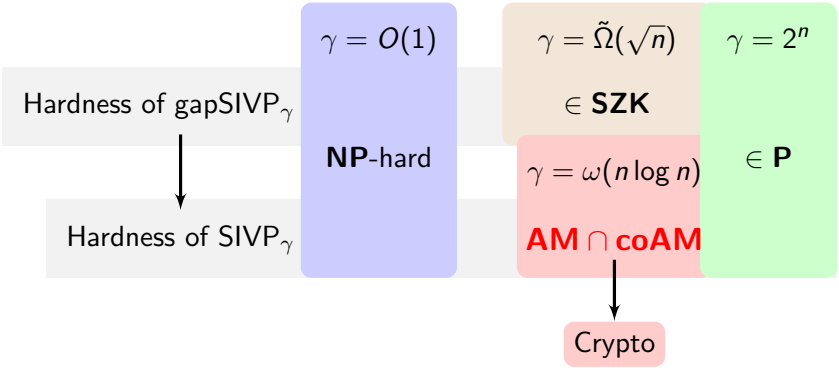
Lattice



Main Theorem

Any language that can be efficiently reduced to SIVP$_{\tilde{O}(n)}$ is in **AM** $\cap$ **coAM**.

Lattice



Main Theorem

Any language that can be efficiently reduced to SIVP$_{\tilde{O}(n)}$ is in **AM** $\cap$ **coAM**.

Thus it's not **NP**-hard unless polynomial hierarchy collapses.

Discrete Gaussian Sampling

$\mathrm{DGS}_{\mathcal{L},s}$ is distribution on a lattice $\mathcal{L}$ s.t. for all $\mathbf{v} \in \mathcal{L}$

$$\Pr\left[\mathbf{v} \leftarrow \mathrm{DGS}_{\mathcal{L},s}\right] \propto e^{-\frac{\|\mathbf{v}\|^2}{s^2}}$$

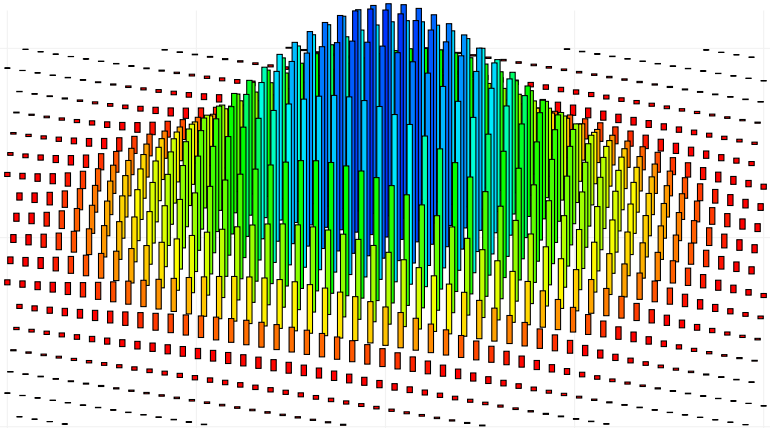
Discrete Gaussian Sampling

$\mathrm{DGS}_{\mathcal{L},s}$ is distribution on a lattice $\mathcal{L}$ s.t. for all $\mathbf{v} \in \mathcal{L}$

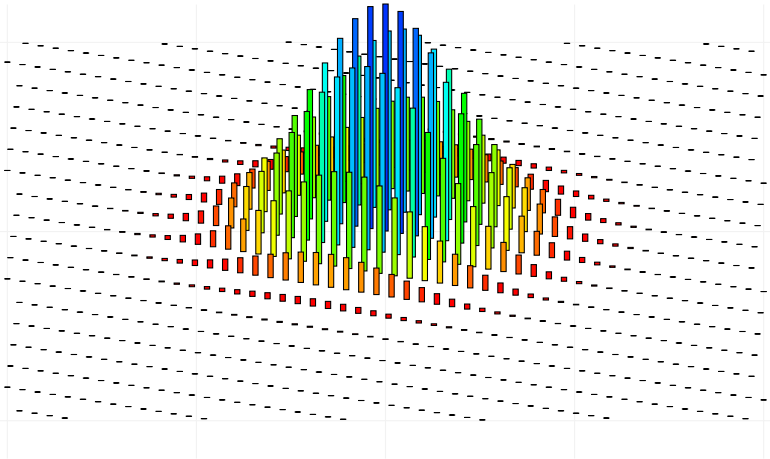
$$\Pr\left[\mathbf{v} \leftarrow \mathrm{DGS}_{\mathcal{L},s}\right] \propto e^{-\frac{\|\mathbf{v}\|^2}{s^2}}$$

Center: origin point $\mathbf{0}$
Parameter s: "standard deviation"

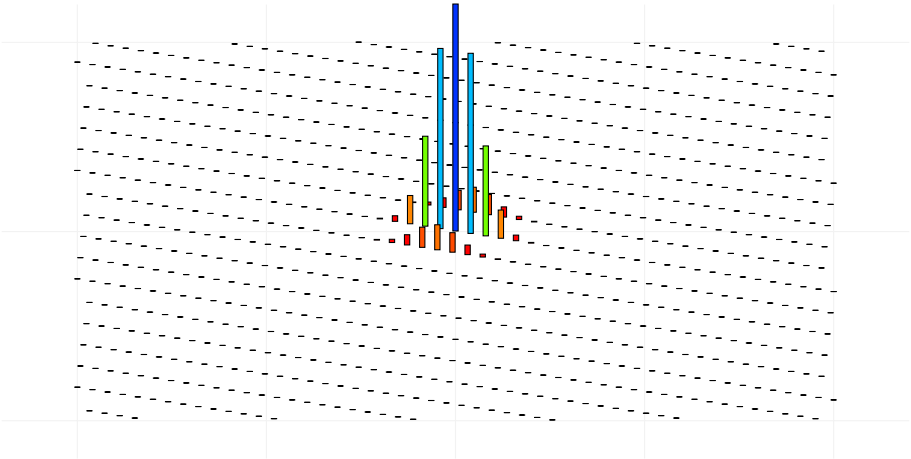
Discrete Gaussian Sampling



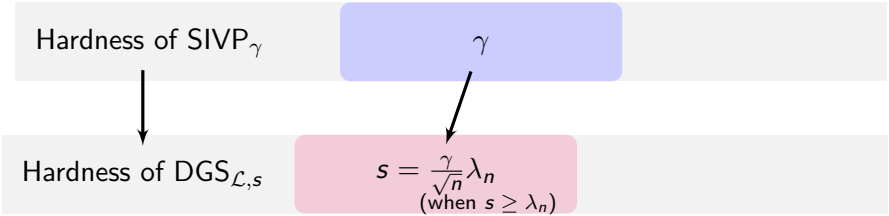
Discrete Gaussian Sampling



Discrete Gaussian Sampling

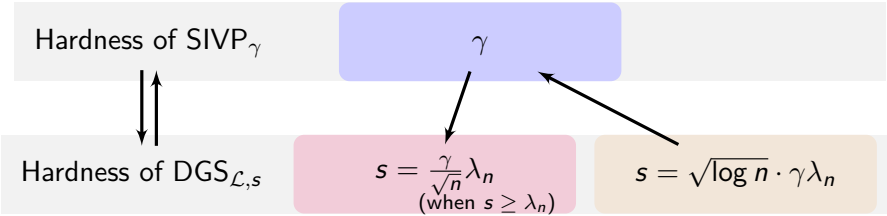


Discrete Gaussian Sampling



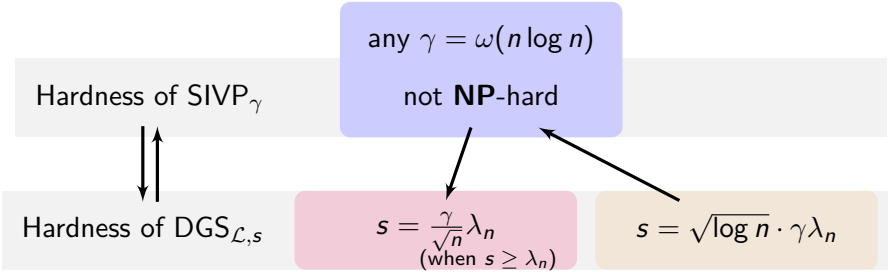
- A small basis can be sampled form DGS$_{\mathcal{L},s}$

Discrete Gaussian Sampling



- A small basis can be sampled form DGS$_{\mathcal{L},s}$
- A small basis allows sampling from DGS$_{\mathcal{L},s}$ [BLPRS'13]

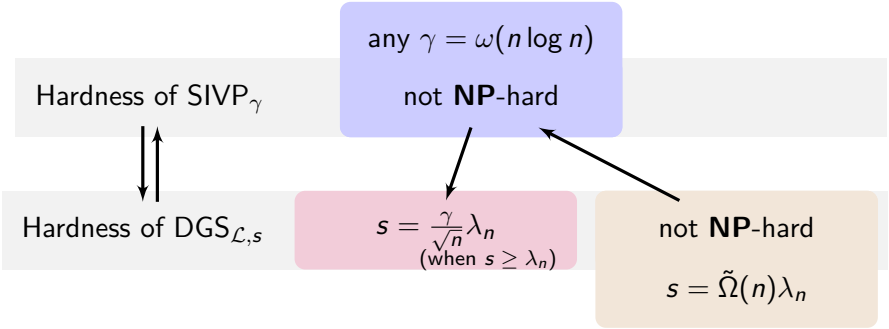
Discrete Gaussian Sampling



Main Theorem

Any language that can be efficiently reduced to $\mathrm{SIVP}_{\tilde{O}(n)}$ is in $\mathbf{AM} \cap \mathbf{coAM}$.

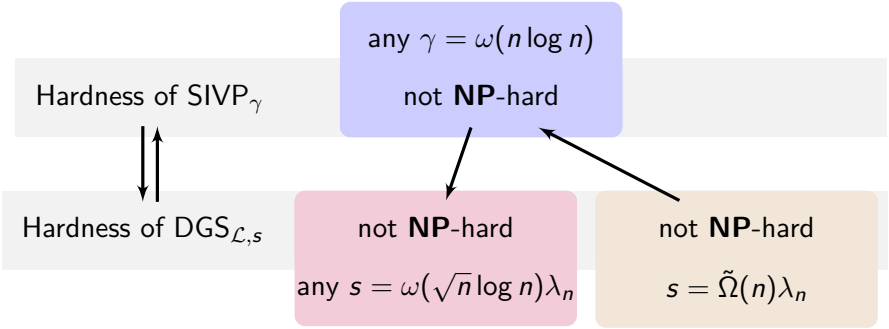
Discrete Gaussian Sampling



Main Theorem

Any language that can be efficiently reduced to $\mathrm{SIVP}_{\tilde{O}(n)}$ is in $\mathbf{AM} \cap \mathbf{coAM}$.

Discrete Gaussian Sampling



Stronger Theorem

Any language that can be efficiently reduced to $\mathrm{DGS}_{\tilde{O}(\sqrt{n})\lambda_n}$ is in $\mathbf{AM} \cap \mathbf{coAM}$.

Proof Outline

$\mathrm{DGS}_{s=\tilde{O}(\sqrt{n})\lambda_n}$

BPP

$\in \mathbf{AM} \cap \mathbf{coAM}$

Proof Outline

$\mathrm{DGS}_{s=\tilde{O}(\sqrt{n})\lambda_n}$

BPP

$\in \mathbf{AM} \cap \mathbf{coAM}$

Probability-Verifiable

BPP

$\in \mathbf{AM} \cap \mathbf{coAM}$

Proof Outline

$\mathrm{DGS}_{s=\tilde{O}(\sqrt{n})\lambda_n}$

BPP

$\in \mathbf{AM} \cap \mathbf{coAM}$

Probability-Verifiable

BPP

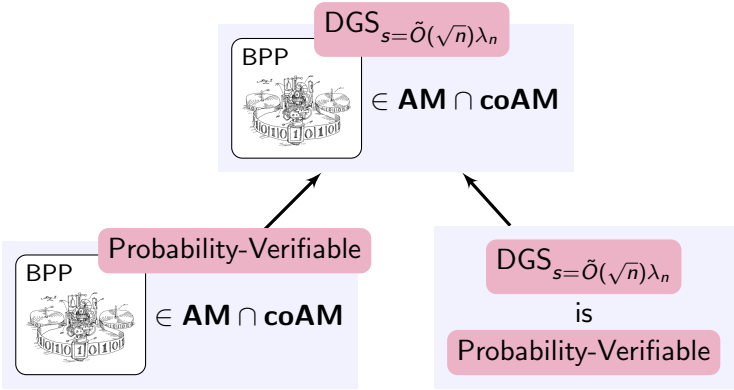
$\in \mathbf{AM} \cap \mathbf{coAM}$

$\mathrm{DGS}_{s=\tilde{O}(\sqrt{n})\lambda_n}$

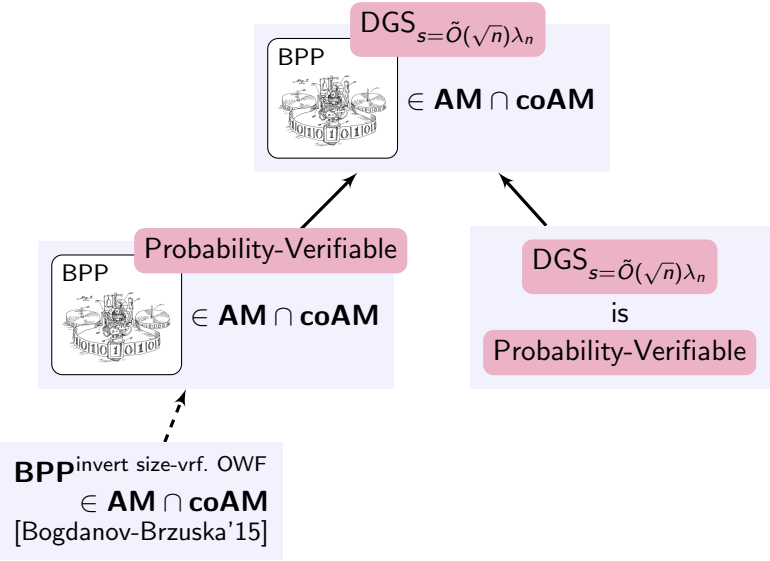
is

Probability-Verifiable

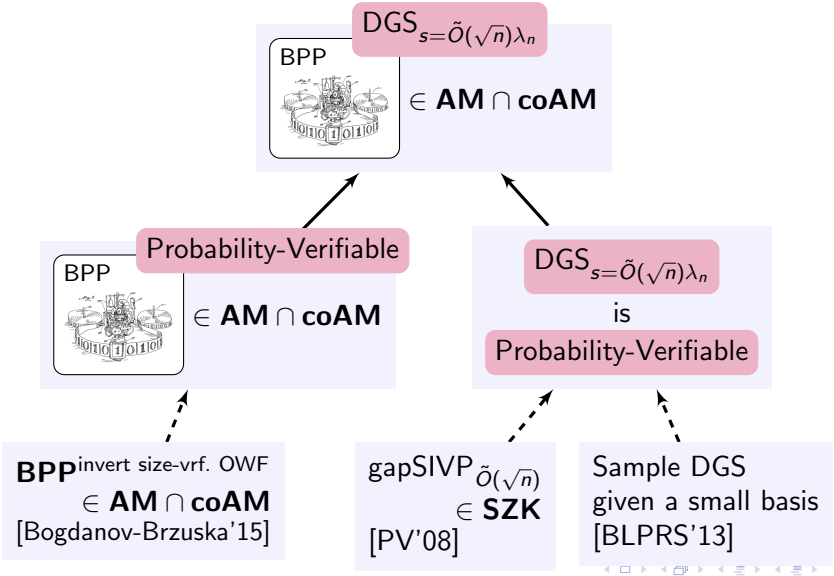
Proof Outline



Proof Outline



Proof Outline



Probability Verifiability

- A **sample problem**:
  Given the description of a distribution, sample from the distribution.

Probability Verifiability

- A **sample problem**:
  Given the description of a distribution, sample from the distribution.

  E.g. a lattice basis B specifies the distribution $\mathrm{DGS}_{\mathcal{L}(B),\lambda_n(B)}$

Probability Verifiability

- A **sample problem**:
  Given the description of a distribution, sample from the distribution.

  E.g. a lattice basis B specifies the distribution $\mathrm{DGS}_{\mathcal{L}(B),\lambda_n(B)}$

- A sample problem is **probability verifiable** if and only if
  Given a description of distribution D, and a point $\mathbf{v}$ in the domain, there is an Arthur-Merlin protocol to (lower) bound $\Pr[\mathbf{v} \leftarrow D]$.

Probability Verifiability

- A **sample problem**:
  Given the description of a distribution, sample from the distribution.

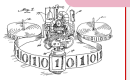
  E.g. a lattice basis B specifies the distribution $\mathrm{DGS}_{\mathcal{L}(B),\lambda_n(B)}$

- A sample problem is **probability verifiable** if and only if
  Given a description of distribution D, and a point $\mathbf{v}$ in the domain, there is an Arthur-Merlin protocol to (lower) bound $\Pr[\mathbf{v} \leftarrow D]$.

  I.e. the following promise problem is in **AM**

  YES instance $(D, \mathbf{v}, \hat{p})$ such that $\hat{p} = \Pr[\mathbf{v} \leftarrow D]$
  NO instance $(D, \mathbf{v}, \hat{p})$ such that $\hat{p} > \Pr[\mathbf{v} \leftarrow D] +$ "small"

BPP Probability-Verifiable

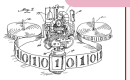


$\in \mathbf{AM} \cap \mathbf{coAM}$

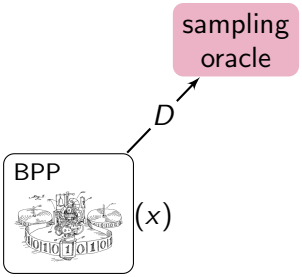
BPP

(x)

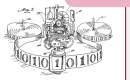
BPP Probability-Verifiable



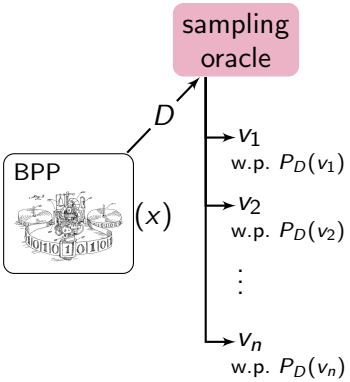
$\in \mathbf{AM} \cap \mathbf{coAM}$



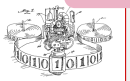
BPP Probability-Verifiable



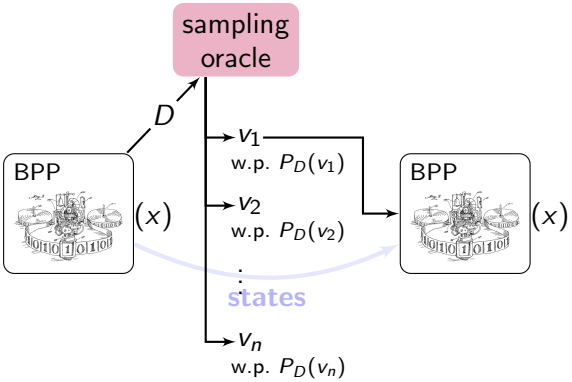
$\in \mathbf{AM} \cap \mathbf{coAM}$



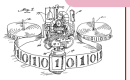
BPP Probability-Verifiable



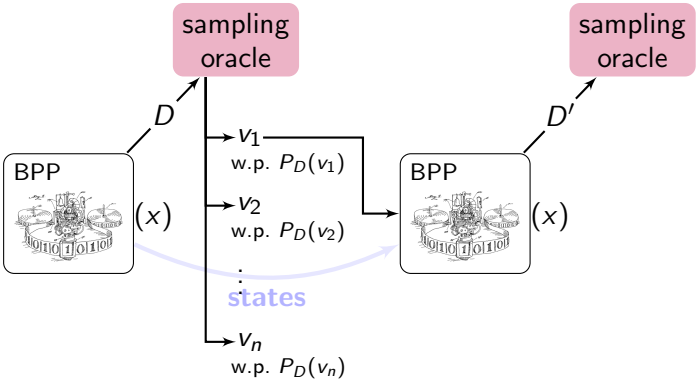
$\in \mathbf{AM} \cap \mathbf{coAM}$



BPP Probability-Verifiable

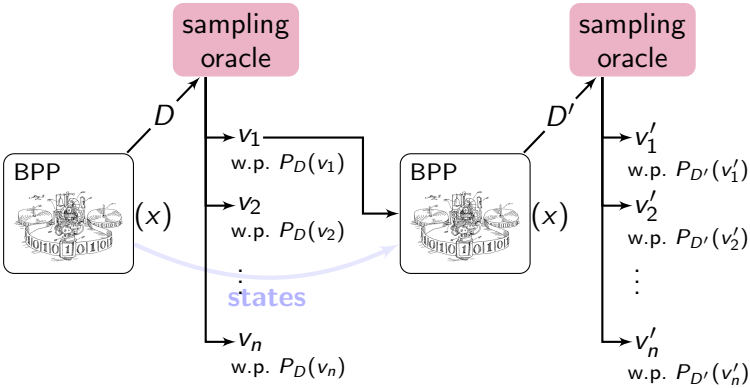


$\in \mathbf{AM} \cap \mathbf{coAM}$



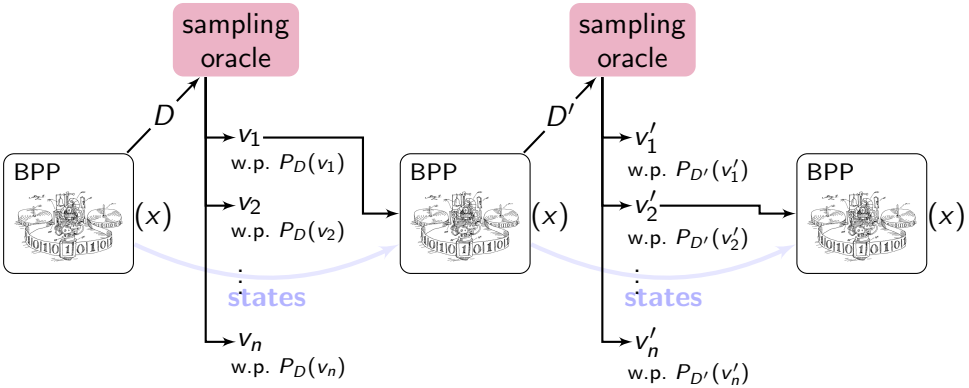
BPP Probability-Verifiable

$\in \mathbf{AM} \cap \mathbf{coAM}$

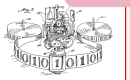


BPP Probability-Verifiable

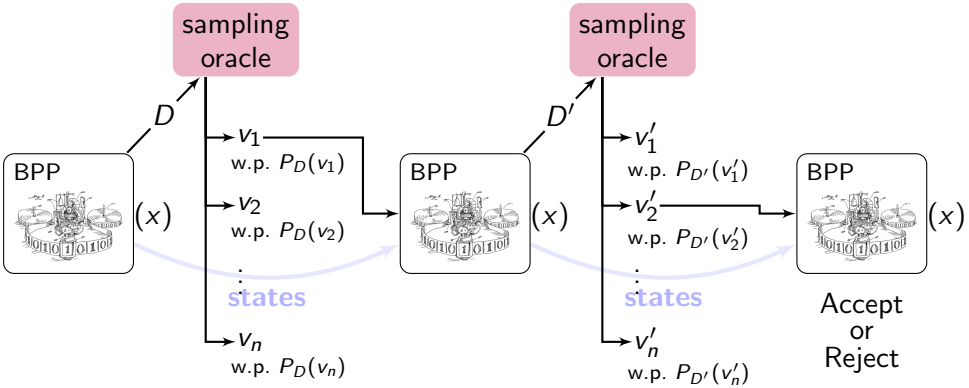
$\in \mathbf{AM} \cap \mathbf{coAM}$



BPP Probability-Verifiable



$\in \mathbf{AM} \cap \mathbf{coAM}$



BPP Probability-Verifiable

$\in \mathbf{AM} \cap \mathbf{coAM}$

- Every execution is determined by a valid transcript

$$(\text{reduction's randomness}, D_1, v_1, \ldots, D_t, v_t).$$

BPP Probability-Verifiable

$\in \mathbf{AM} \cap \mathbf{coAM}$

- Every execution is determined by a valid transcript

$$(\text{reduction's randomness}, D_1, v_1, \ldots, D_t, v_t).$$

- Its probability is $\frac{1}{2^{\text{randomness tape length}}} \cdot \prod_i P_{D_i}(v_i)$

BPP Probability-Verifiable

$\in \mathbf{AM} \cap \mathbf{coAM}$

- Every execution is determined by a valid transcript

$$(\text{reduction's randomness}, D_1, v_1, \ldots, D_t, v_t).$$

- Its probability is $\frac{1}{2^{\text{randomness tape length}}} \cdot \prod_i P_{D_i}(v_i)$
  which can be (lower) bounded by an Arthur-Merlin protocol.

BPP Probability-Verifiable

$\in \mathbf{AM} \cap \mathbf{coAM}$

- Every execution is determined by a valid transcript

$$(\text{reduction's randomness}, D_1, v_1, \ldots, D_t, v_t).$$

- Its probability is $\frac{1}{2^{\text{randomness tape length}}} \cdot \prod_i P_{D_i}(v_i)$
  which can be (lower) bounded by an Arthur-Merlin protocol.
- The probability that BPP$^{\text{sampling oracle}}$ $(x) \to$'accept'

$$= \sum_{\substack{\text{valid transcript} \\ \text{s.t. } x \text{ is accepted}}} [\text{Probablity of the transcript}]$$

BPP Probability-Verifiable

$\in \mathbf{AM} \cap \mathbf{coAM}$

- Every execution is determined by a valid transcript

$$(\text{reduction's randomness}, D_1, v_1, \ldots, D_t, v_t).$$

- Its probability is $\frac{1}{2^{\text{randomness tape length}}} \cdot \prod_i P_{D_i}(v_i)$
  which can be (lower) bounded by an Arthur-Merlin protocol.
- The probability that BPP$^{\text{sampling oracle}}$ $(x) \to$'accept'

$$= \sum_{\substack{\text{valid transcript} \\ \text{s.t. } x \text{ is accepted}}} [\text{Probablity of the transcript}]$$

  which can be (lower) bounded by an Arthur-Merlin protocol. [GS'86]

$\mathrm{DGS}_{s=\tilde{O}(\sqrt{n})\lambda_n}$ is Probability-Verifiable

Goal: Given $B, \mathbf{v}$, (lower) bound the probablity that $\mathbf{v} \leftarrow \mathrm{DGS}_{\mathcal{L}(B), s=\tilde{O}(\sqrt{n})\lambda_n(B)}$ in an Arthur-Merlin protocol.

$\mathrm{DGS}_{s=\tilde{O}(\sqrt{n})\lambda_n}$ is Probability-Verifiable

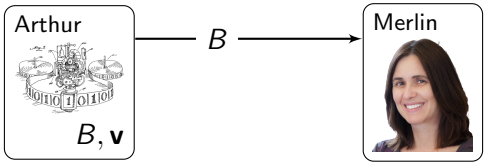
Goal: Given $B, \mathbf{v}$, (lower) bound the probablity that $\mathbf{v} \leftarrow \mathrm{DGS}_{\mathcal{L}(B), s=\tilde{O}(\sqrt{n})\lambda_n(B)}$ in an Arthur-Merlin protocol.

$\mathrm{DGS}_{s=\tilde{O}(\sqrt{n})\lambda_n}$ is Probability-Verifiable

Goal: Given $B, \mathbf{v}$, (lower) bound the probablity that $\mathbf{v} \leftarrow \mathrm{DGS}_{\mathcal{L}(B), s=\tilde{O}(\sqrt{n})\lambda_n(B)}$ in an Arthur-Merlin protocol.

$\mathrm{DGS}_{s=\tilde{O}(\sqrt{n})\lambda_n}$ is Probability-Verifiable

Goal: Given $B, \mathbf{v}$, (lower) bound the probablity that $\mathbf{v} \leftarrow \mathrm{DGS}_{\mathcal{L}(B), s=\tilde{O}(\sqrt{n})\lambda_n(B)}$ in an Arthur-Merlin protocol.

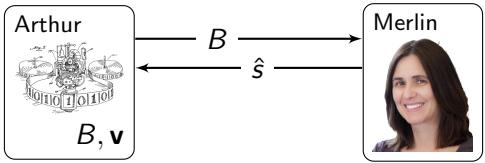


Arthur: Estimate $\lambda_n(B)$ for me

You can't cheat as gapSIVP $_{\sqrt{\frac{n}{\log n}}} \in \mathbf{NP} \cap \mathbf{coAM}$ [BS'99, GMR'04]

$\mathrm{DGS}_{s=\tilde{O}(\sqrt{n})\lambda_n}$ is Probability-Verifiable

Goal: Given $B, \mathbf{v}$, (lower) bound the probablity that $\mathbf{v} \leftarrow \mathrm{DGS}_{\mathcal{L}(B), s=\tilde{O}(\sqrt{n})\lambda_n(B)}$ in an Arthur-Merlin protocol.

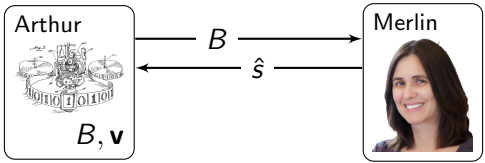


Arthur: Estimate $\lambda_n(B)$ for me
You can't cheat as gapSIVP $_{\sqrt{\frac{n}{\log n}}} \in \mathbf{NP} \cap \mathbf{coAM}$ [BS'99, GMR'04]

Merlin: Here it is
$\lambda_n(B) \leq \hat{s} < \sqrt{\frac{n}{\log n}} \cdot \lambda_n(B)$

$\mathrm{DGS}_{s=\tilde{O}(\sqrt{n})\lambda_n}$ is Probability-Verifiable

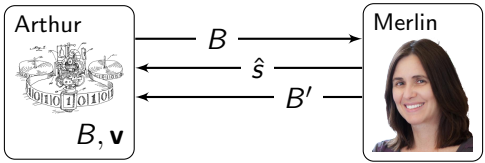
Goal: Given $B, \mathbf{v}$, (lower) bound the probablity that $\mathbf{v} \leftarrow \mathrm{DGS}_{\mathcal{L}(B), s=\tilde{O}(\sqrt{n})\lambda_n(B)}$ in an Arthur-Merlin protocol.



Arthur: Give me a small basis of $\mathcal{L}(B)$
I already knew $\lambda_n(B) \leq \hat{s}$

$\mathrm{DGS}_{s=\tilde{O}(\sqrt{n})\lambda_n}$ is Probability-Verifiable

Goal: Given $B, \mathbf{v}$, (lower) bound the probablity that $\mathbf{v} \leftarrow \mathrm{DGS}_{\mathcal{L}(B), s=\tilde{O}(\sqrt{n})\lambda_n(B)}$ in an Arthur-Merlin protocol.

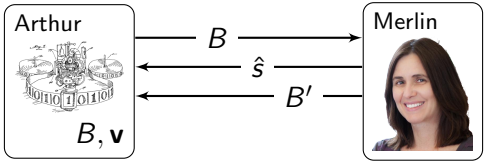


Arthur: Give me a small basis of $\mathcal{L}(B)$
I already knew $\lambda_n(B) \leq \hat{s}$

Merlin: Here it is
length of $B' \leq \hat{s}$

$\mathrm{DGS}_{s=\tilde{O}(\sqrt{n})\lambda_n}$ is Probability-Verifiable

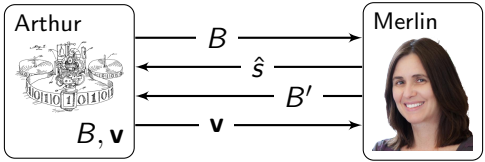
Goal: Given $B, \mathbf{v}$, (lower) bound the probablity that $\mathbf{v} \leftarrow \mathrm{DGS}_{\mathcal{L}(B), s=\tilde{O}(\sqrt{n})\lambda_n(B)}$ in an Arthur-Merlin protocol.



Arthur: I can sample from $\mathrm{DGS}_{\mathcal{L}(B), \sqrt{\log n} \cdot \hat{s}}$ by myself [BLPRS'13]

$\mathrm{DGS}_{s=\tilde{O}(\sqrt{n})\lambda_n}$ is Probability-Verifiable

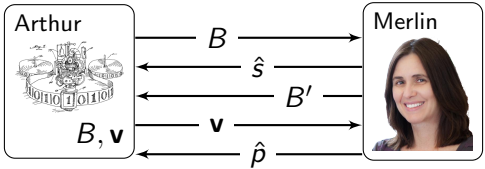
Goal: Given $B, \mathbf{v}$, (lower) bound the probablity that $\mathbf{v} \leftarrow \mathrm{DGS}_{\mathcal{L}(B), s=\tilde{O}(\sqrt{n})\lambda_n(B)}$ in an Arthur-Merlin protocol.



Arthur: I can sample from $\mathrm{DGS}_{\mathcal{L}(B), \sqrt{\log n} \cdot \hat{s}}$ by myself [BLPRS'13]
What's the prob. that $\mathbf{v}$ is sampled? [GS'86]

$\mathrm{DGS}_{s=\tilde{O}(\sqrt{n})\lambda_n}$ is Probability-Verifiable

Goal: Given $B, \mathbf{v}$, (lower) bound the probablity that $\mathbf{v} \leftarrow \mathrm{DGS}_{\mathcal{L}(B),s=\tilde{O}(\sqrt{n})\lambda_n(B)}$ in an Arthur-Merlin protocol.

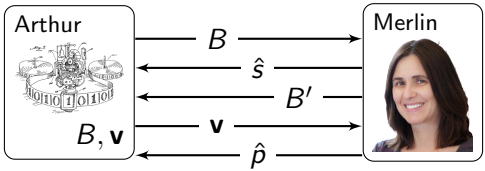


Arthur: I can sample from $\mathrm{DGS}_{\mathcal{L}(B),\sqrt{\log n}\cdot\hat{s}}$ by myself [BLPRS'13]
What's the prob. that $\mathbf{v}$ is sampled? [GS'86]

Merlin: The prob. is at least 0.000017653...

$\mathrm{DGS}_{s=\tilde{O}(\sqrt{n})\lambda_n}$ is Probability-Verifiable

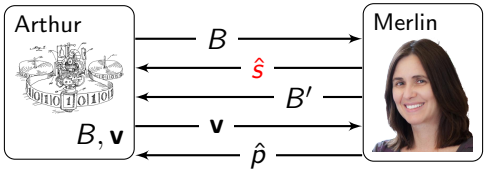
Goal: Given $B, \mathbf{v}$, (lower) bound the probablity that $\mathbf{v} \leftarrow \mathrm{DGS}_{\mathcal{L}(B), s=\tilde{O}(\sqrt{n})\lambda_n(B)}$ in an Arthur-Merlin protocol.



Arthur learns $\Pr\left[\mathbf{v} \leftarrow \mathrm{DGS}_{\mathcal{L}(B), \sqrt{\log n}\cdot\hat{s}}\right] \geq \hat{p}$. Problem Solved?

$\mathrm{DGS}_{s=\tilde{O}(\sqrt{n})\lambda_n}$ is Probability-Verifiable

Goal: Given $B, \mathbf{v}$, (lower) bound the probablity that $\mathbf{v} \leftarrow \mathrm{DGS}_{\mathcal{L}(B), s=\tilde{O}(\sqrt{n})\lambda_n(B)}$ in an Arthur-Merlin protocol.

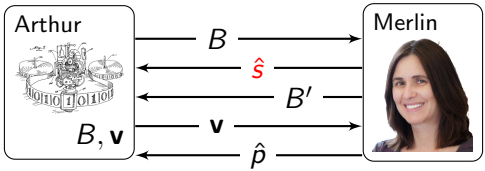


Arthur learns $\Pr\left[\mathbf{v} \leftarrow \mathrm{DGS}_{\mathcal{L}(B), \sqrt{\log n}\cdot\hat{s}}\right] \geq \hat{p}$. Problem Solved?

NO!! Merlin can change the distribution by the choice of $\hat{s}$.

$\mathrm{DGS}_{s=\tilde{O}(\sqrt{n})\lambda_n}$ is Probability-Verifiable

Goal: Given $B, \mathbf{v}$, (lower) bound the probablity that $\mathbf{v} \leftarrow \mathrm{DGS}_{\mathcal{L}(B), s=\tilde{O}(\sqrt{n})\lambda_n(B)}$ in an Arthur-Merlin protocol.

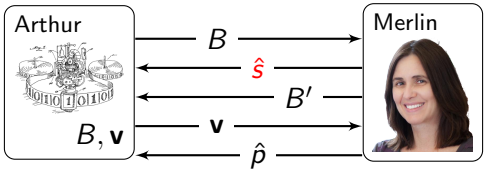


Arthur: Compute $s(B)$ for me

$s(\cdot)$ is an ad-hoc fucntion s.t. $\lambda_n(B) \leq s(B) < \tilde{O}(\sqrt{n}) \cdot \lambda_n(B)$ and "can be computed" in **AM**.

$\mathrm{DGS}_{s=\tilde{O}(\sqrt{n})\lambda_n}$ is Probability-Verifiable

Goal: Given $B, \mathbf{v}$, (lower) bound the probablity that $\mathbf{v} \leftarrow \mathrm{DGS}_{\mathcal{L}(B), s=\tilde{O}(\sqrt{n})\lambda_n(B)}$ in an Arthur-Merlin protocol.



Arthur: Compute $s(B)$ for me

$s(\cdot)$ is an ad-hoc fucntion s.t. $\lambda_n(B) \leq s(B) < \tilde{O}(\sqrt{n}) \cdot \lambda_n(B)$ and "can be computed" in **AM**.

Merlin: Sure ..... Here it is. $\hat{s} \approx s(B)$

$\mathrm{DGS}_{s=\tilde{O}(\sqrt{n})\lambda_n}$ is Probability-Verifiable

Goal: Given $B, \mathbf{v}$, (lower) bound the probablity that $\mathbf{v} \leftarrow \mathrm{DGS}_{\mathcal{L}(B), s=\tilde{O}(\sqrt{n})\lambda_n(B)}$ in an Arthur-Merlin protocol.

Need: function $s(\cdot)$ s.t. $\lambda_n(B) \leq s(B) < \tilde{O}(\sqrt{n}) \cdot \lambda_n(B)$
and "can be computed" in **AM**.

$\mathrm{DGS}_{s=\tilde{O}(\sqrt{n})\lambda_n}$ is Probability-Verifiable

Goal: Given $B, \mathbf{v}$, (lower) bound the probablity that $\mathbf{v} \leftarrow \mathrm{DGS}_{\mathcal{L}(B), s=\tilde{O}(\sqrt{n})\lambda_n(B)}$ in an Arthur-Merlin protocol.

Need: function $s(\cdot)$ s.t. $\lambda_n(B) \leq s(B) < \tilde{O}(\sqrt{n}) \cdot \lambda_n(B)$
and "can be computed" in **AM**.

$\mathrm{gapSIVP}_{\tilde{O}(\sqrt{n})} \in$ **SZK** [PV'08]:

$\mathrm{DGS}_{s=\tilde{O}(\sqrt{n})\lambda_n}$ is Probability-Verifiable

Goal: Given $B, \mathbf{v}$, (lower) bound the probablity that $\mathbf{v} \leftarrow \mathrm{DGS}_{\mathcal{L}(B), s=\tilde{O}(\sqrt{n})\lambda_n(B)}$ in an Arthur-Merlin protocol.

Need: function $s(\cdot)$ s.t. $\lambda_n(B) \leq s(B) < \tilde{O}(\sqrt{n}) \cdot \lambda_n(B)$
and "can be computed" in **AM**.

$\mathrm{gapSIVP}_{\tilde{O}(\sqrt{n})} \in \mathbf{SZK}$ [PV'08]:

A function $f(B, x) \in [0, 1]$,

$\mathrm{DGS}_{s=\tilde{O}(\sqrt{n})\lambda_n}$ is Probability-Verifiable

Goal: Given $B, \mathbf{v}$, (lower) bound the probablity that $\mathbf{v} \leftarrow \mathrm{DGS}_{\mathcal{L}(B), s=\tilde{O}(\sqrt{n})\lambda_n(B)}$ in an Arthur-Merlin protocol.

Need: function $s(\cdot)$ s.t. $\lambda_n(B) \leq s(B) < \tilde{O}(\sqrt{n}) \cdot \lambda_n(B)$
and "can be computed" in **AM**.

$\mathrm{gapSIVP}_{\tilde{O}(\sqrt{n})} \in$ **SZK** [PV'08]:

A function $f(B, x) \in [0, 1]$, that

- "can be computed" in **AM**

$\mathrm{DGS}_{s=\tilde{O}(\sqrt{n})\lambda_n}$ is Probability-Verifiable

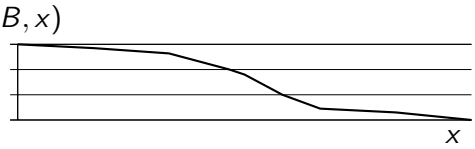
Goal: Given $B, \mathbf{v}$, (lower) bound the probablity that $\mathbf{v} \leftarrow \mathrm{DGS}_{\mathcal{L}(B), s=\tilde{O}(\sqrt{n})\lambda_n(B)}$ in an Arthur-Merlin protocol.

Need: function $s(\cdot)$ s.t. $\lambda_n(B) \leq s(B) < \tilde{O}(\sqrt{n}) \cdot \lambda_n(B)$
and "can be computed" in **AM**.

$\mathrm{gapSIVP}_{\tilde{O}(\sqrt{n})} \in$ **SZK** [PV'08]:

A function $f(B, x) \in [0, 1]$, that

- "can be computed" in **AM**
- decreasing on x



$\mathrm{DGS}_{s=\tilde{O}(\sqrt{n})\lambda_n}$ is Probability-Verifiable

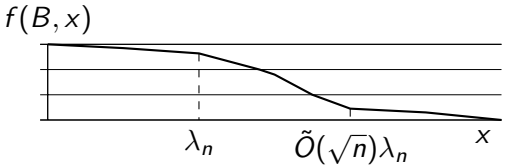
Goal: Given $B, \mathbf{v}$, (lower) bound the probablity that $\mathbf{v} \leftarrow \mathrm{DGS}_{\mathcal{L}(B), s=\tilde{O}(\sqrt{n})\lambda_n(B)}$ in an Arthur-Merlin protocol.

Need: function $s(\cdot)$ s.t. $\lambda_n(B) \le s(B) < \tilde{O}(\sqrt{n}) \cdot \lambda_n(B)$
and "can be computed" in **AM**.

$\mathrm{gapSIVP}_{\tilde{O}(\sqrt{n})} \in$ **SZK** [PV'08]:

A function $f(B, x) \in [0, 1]$, that

- "can be computed" in **AM**
- decreasing on x
- $f(B, \lambda_n(B)) > 2/3$
  $f(B, \tilde{O}(\sqrt{n}) \cdot \lambda_n(B)) < 1/3$



$\mathrm{DGS}_{s=\tilde{O}(\sqrt{n})\lambda_n}$ is Probability-Verifiable

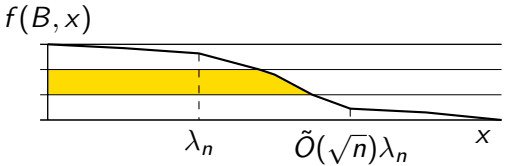
Goal: Given $B, \mathbf{v}$, (lower) bound the probablity that $\mathbf{v} \leftarrow \mathrm{DGS}_{\mathcal{L}(B), s=\tilde{O}(\sqrt{n})\lambda_n(B)}$ in an Arthur-Merlin protocol.

Need: function $s(\cdot)$ s.t. $\lambda_n(B) \le s(B) < \tilde{O}(\sqrt{n}) \cdot \lambda_n(B)$
and "can be computed" in **AM**.

$\mathrm{gapSIVP}_{\tilde{O}(\sqrt{n})} \in$ **SZK** [PV'08]:

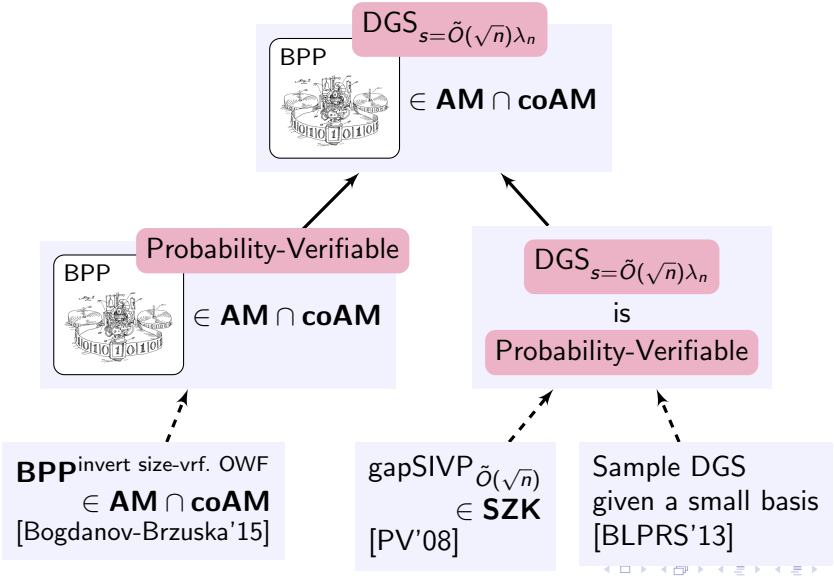
A function $f(B, x) \in [0, 1]$, that

- "can be computed" in **AM**
- decreasing on x
- $f(B, \lambda_n(B)) > 2/3$
  $f(B, \tilde{O}(\sqrt{n}) \cdot \lambda_n(B)) < 1/3$

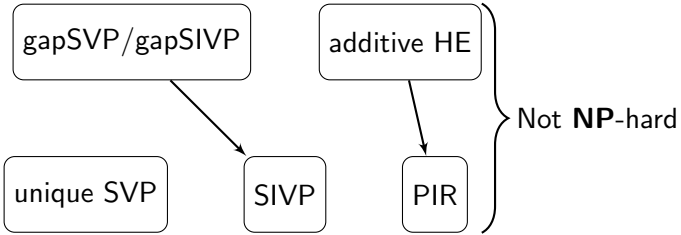


Define $s(B) := 3 \times$ [yellow area].

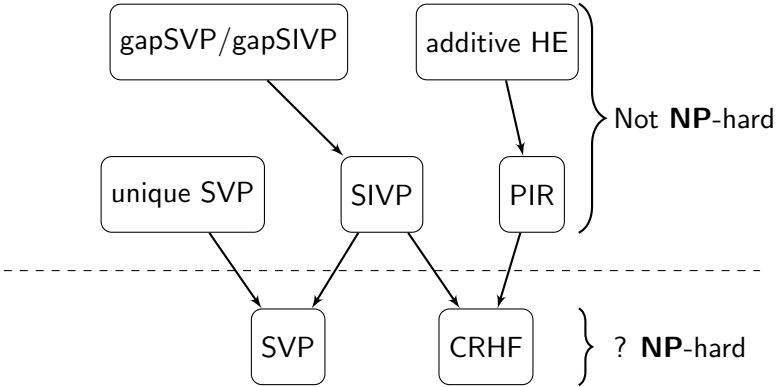
Summary


$\mathrm{DGS}_{s=\tilde{O}(\sqrt{n})\lambda_n}$
BPP
$\in \mathbf{AM} \cap \mathbf{coAM}$
Probability-Verifiable
BPP
$\in \mathbf{AM} \cap \mathbf{coAM}$
$\mathrm{DGS}_{s=\tilde{O}(\sqrt{n})\lambda_n}$
is
Probability-Verifiable
$\mathbf{BPP}^{\text{invert size-vrf. OWF}}$
$\in \mathbf{AM} \cap \mathbf{coAM}$
[Bogdanov-Brzuska'15]
$\mathrm{gapSIVP}_{\tilde{O}(\sqrt{n})}$
$\in \mathbf{SZK}$
[PV'08]
Sample DGS
given a small basis
[BLPRS'13]

Next Impossibility Result?



Next Impossibility Result?



Thank you!

The slides can be found on `liutianren.com`.