Rump Session 2016

Improved Reduction from BDD to uSVP

Shi Bai; Damien Stehlé; Weiqiang Wen

ENS de Lyon

Improved reduction from BDD to uSVP

–Shi Bai, Damien Stehlé and Weiqiang Wen

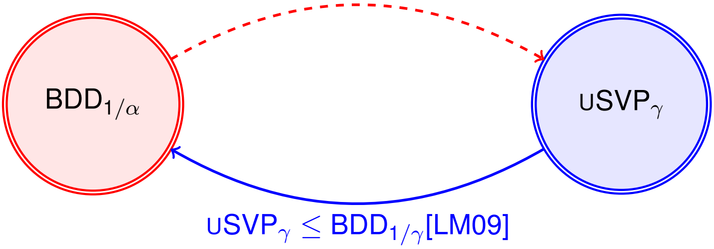
Bounded Distance Decoding (BDD$_\alpha$)

Let $\alpha > 0$. Given as inputs a lattice basis **B** and a vector **t** such that $\mathrm{dist}(\mathbf{t}, \mathcal{L}(\mathbf{B})) \leq \alpha \cdot \lambda_1(\mathbf{B})$, the goal is to find a lattice vector $\mathbf{v} \in \mathcal{L}(\mathbf{B})$ closest to **t**.

Unique Shortest Vector Problem (uSVP$_\gamma$)

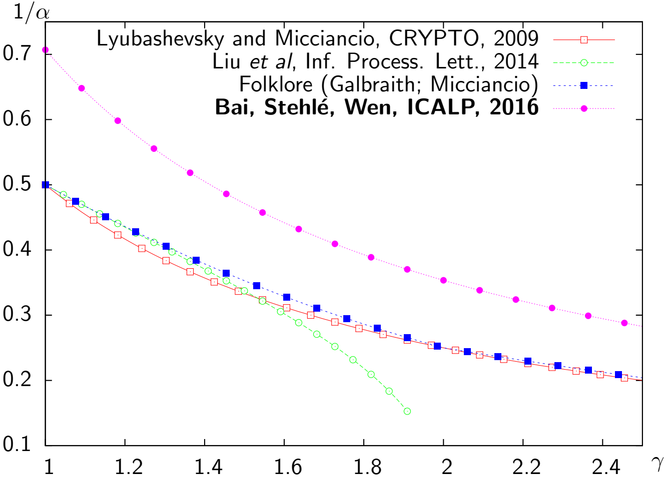
Let $\gamma \geq 1$. Given as input a lattice basis **B** such that $\lambda_2(\mathbf{B}) \geq \gamma \cdot \lambda_1(\mathbf{B})$, the goal is to find a non-zero vector $\mathbf{v} \in \mathcal{L}(\mathbf{B})$ of norm $\lambda_1(\mathcal{L}(\mathbf{B}))$.

Improved reduction from BDD to uSVP



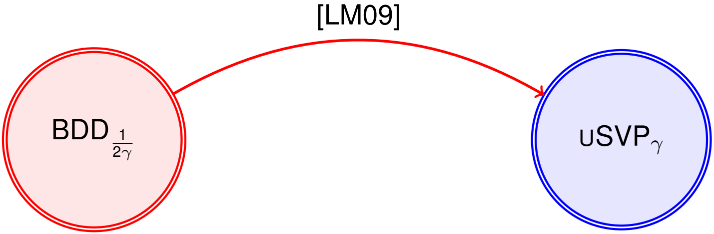
- $\alpha = 2\gamma$, Lyubashevsky and Micciancio, 2009.
- Slightly smaller α, Liu *et al*, 2014.
- (Even) slightly smaller α (more), Galbraith; Micciancio, 2015.
- $\boxed{\text{Our result: } \alpha = \sqrt{2}\gamma.}$

Improved reduction from BDD to uSVP



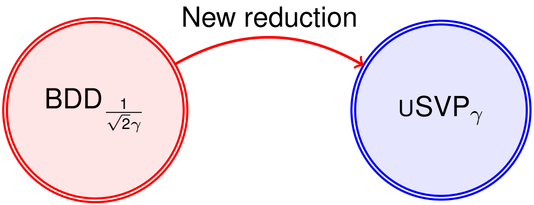
Improved reduction from BDD to uSVP

- Kannan's embedding.



Imporved reduction from BDD to uSVP

- Kannan's embedding + **Khot's *lattice* sparsification**.



Conjecture

- First conjecture: BDD and uSVP are computationally identical.

$$\mathrm{BDD}_{\frac{1}{c\cdot\gamma}} = \mathrm{uSVP}_{\gamma}$$

Note: for some constant c.

- Second conjecture: $\boxed{c = \sqrt{2}}$. In order to prove it, we need to improve the reduction from uSVP to BDD.