A Hybrid Lattice Reduction and Quantum Search Attack on LWE

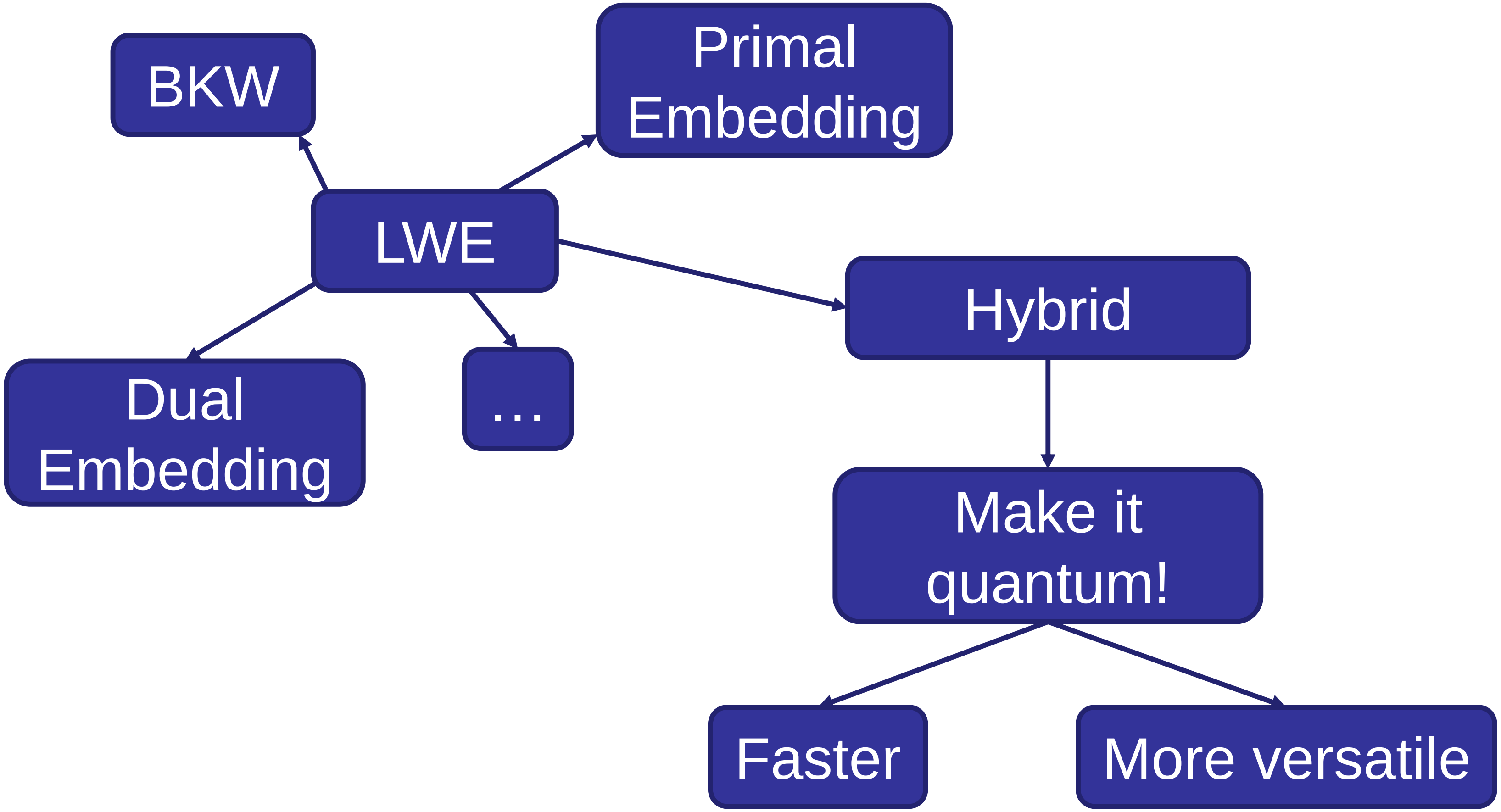
TECHNISCHE UNIVERSITÄT DARMSTADT

F. Göpfert, C. van Vredendaal, Thomas Wunderer

DFG Deutsche Forschungsgemeinschaft

CROSSING

Motivation

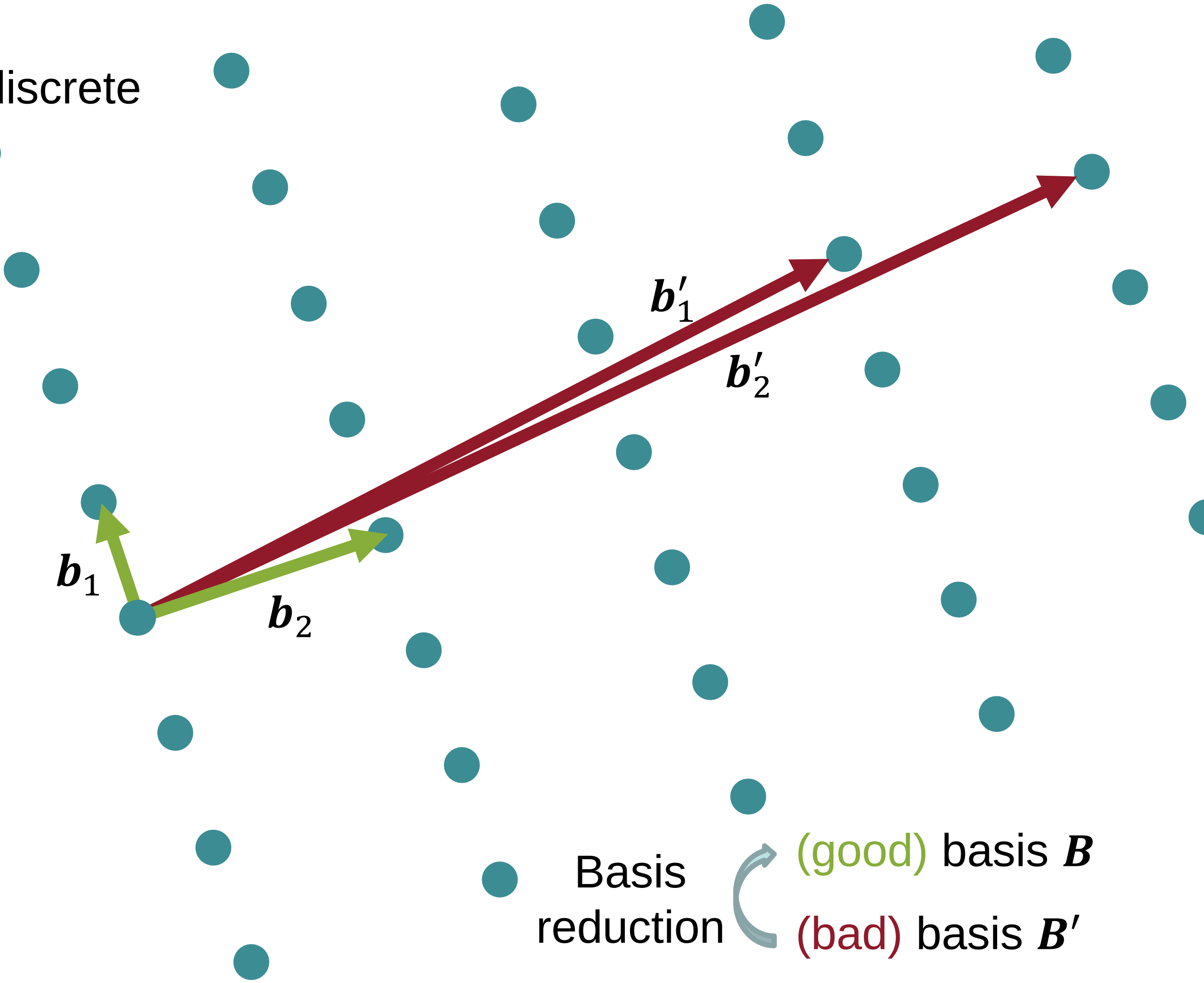

BKW
Primal Embedding
LWE
Hybrid
Dual Embedding
…
Make it quantum!
Faster
More versatile

Background and Notation

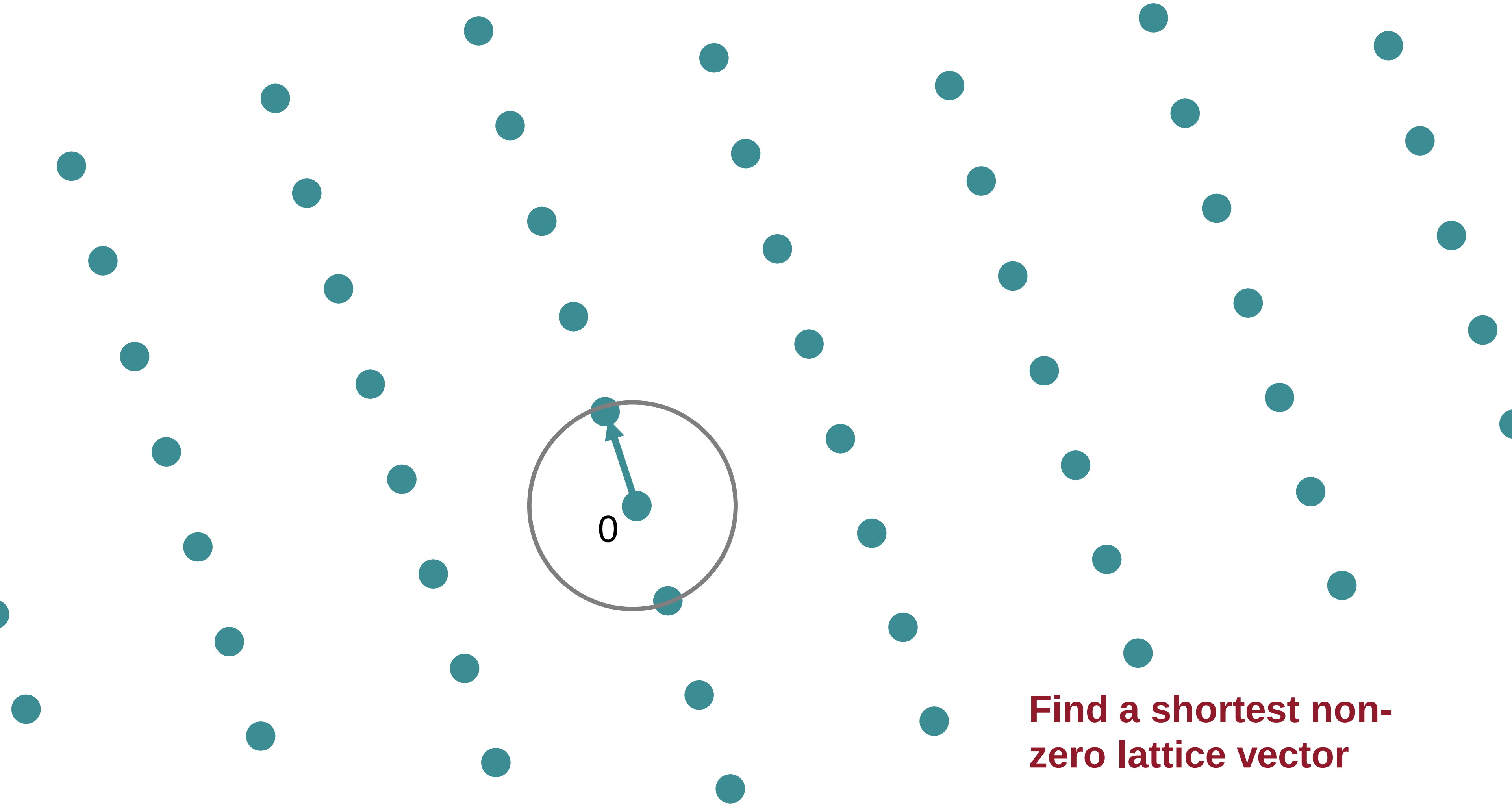
Lattices

n-dimensional **lattice** Λ: a discrete additive subgroup of $\mathbb{R}^n$

Basis of a lattice Λ: lin. ind. $\boldsymbol{B} = \{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\}$ such that $\Lambda = \mathbb{Z}\boldsymbol{b}_1 + \ldots + \mathbb{Z}\boldsymbol{b}_n$.

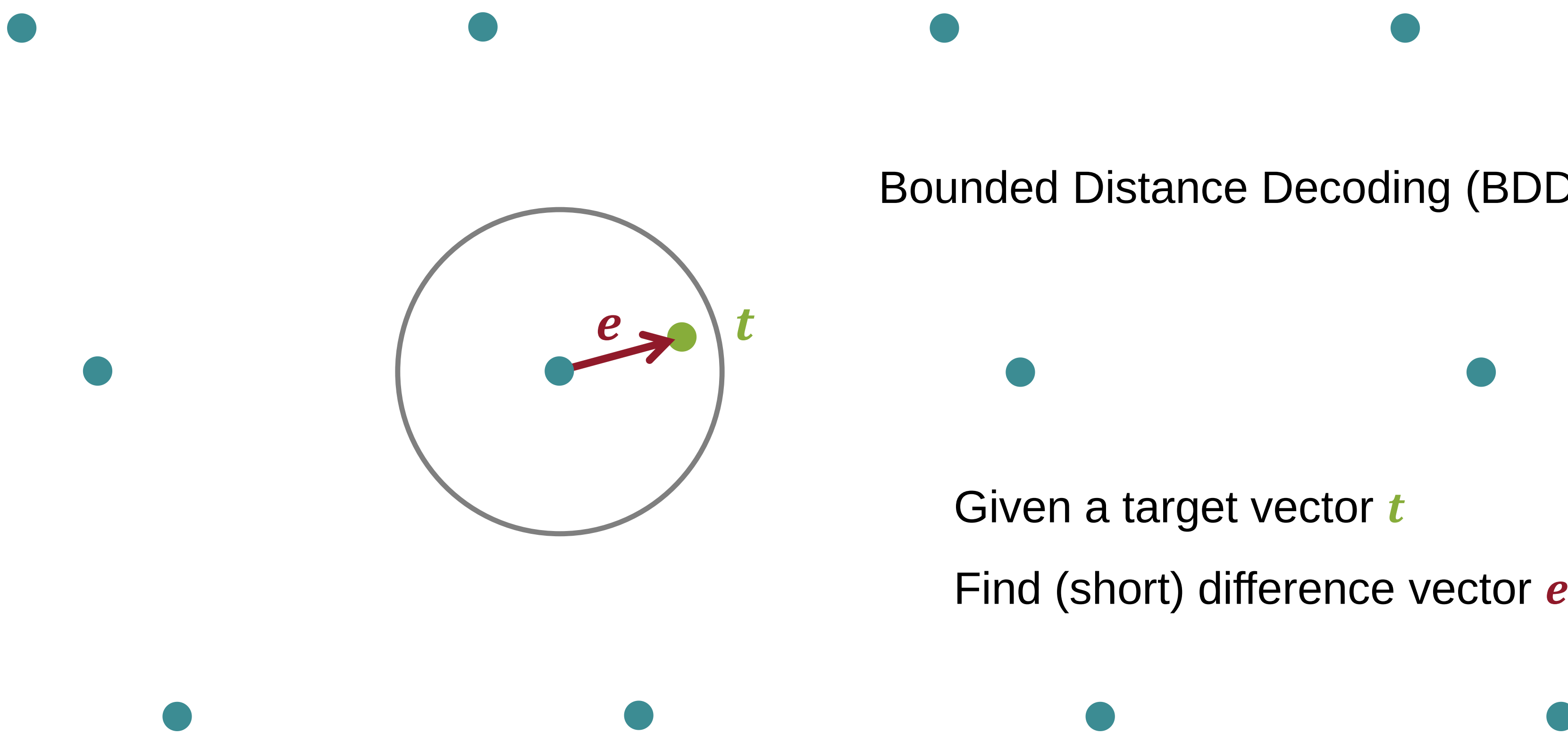


Shortest Vector Problem (SVP)



Find a shortest non-zero lattice vector

Closest Vector Problem (CVP)



Bounded Distance Decoding (BDD)

Given a target vector $\boldsymbol{t}$

Find (short) difference vector $\boldsymbol{e}$

Learning with Errors (LWE)

$$\boldsymbol{b} = \boldsymbol{A} \cdot \underbrace{\boldsymbol{s}}_{\text{short}} + \underbrace{\boldsymbol{e}}_{\text{short}} \mod q$$

Given: $\boldsymbol{A} \in \mathbb{Z}_q^{m\times n}$, $\boldsymbol{b} \in \mathbb{Z}_q^{m}$ Find: $\boldsymbol{s} \in \mathbb{Z}_q^{n}$

The (Quantum)
Hybrid Attack
on LWE

Our approach

We solve the LWE instance $\boldsymbol{b} = \boldsymbol{A}\boldsymbol{s} + \boldsymbol{e} \bmod q$ as follows:

1. Transform LWE into SVP in some lattice Λ
2. Generate a basis $\boldsymbol{B}'$ of Λ of the form

$$\boldsymbol{B}' = \begin{pmatrix} \boldsymbol{B} & \boldsymbol{C} \\ \boldsymbol{0} & \boldsymbol{I}_r \end{pmatrix}$$

3. Solve SVP in Λ with our Quantum Hybrid Attack

Transforming LWE into SVP

$$\boldsymbol{b} = \boldsymbol{A}\boldsymbol{s} + \boldsymbol{e} \; mod \; q$$

$$\Downarrow$$

$$\boldsymbol{v} = \underbrace{\begin{pmatrix} \boldsymbol{s} \\ \boldsymbol{e} \\ 1 \end{pmatrix}}_{\text{short}} \in \Lambda = \{\boldsymbol{x} \in \mathbb{Z}^{n+m+1} : (\boldsymbol{A} | \boldsymbol{I}_m | -\boldsymbol{b})\boldsymbol{x} = \boldsymbol{0} \; mod \; q\}$$

The Quantum Hybrid Attack (Idea)

Setup: Find a shortest non-zero vector $\boldsymbol{v} \in \Lambda(\boldsymbol{B}') \subset \mathbb{Z}^d$, where $\boldsymbol{B}' = \begin{pmatrix} \boldsymbol{B} & \boldsymbol{C} \\ \boldsymbol{0} & \boldsymbol{I}_r \end{pmatrix}$

$$v = \begin{pmatrix} v_1 \\ \hline v_2 \end{pmatrix}$$

Find $\boldsymbol{v}_1 \in \mathbb{Z}^{d-r}$ with lattice-based techniques:

- Basis reduction as precomputation
- BDD-algorithms (Nearest Plane [Babai86])

Quantum-search for $\boldsymbol{v}_2 \in \mathbb{Z}^r$ (“Grover-like”)

Quantum vs. Classical Hybrid Attack

Quantum

Quantum search for $\boldsymbol{v}_2$

+ √-speed-up over brute-force

+ More versitile

+ Low memory consumption

+ No collision-finding probability

Classical

Meet-in-the-middle search for $\boldsymbol{v}_2$

+ √-speed-up over brute-force

- Requires highly structured keys

- Huge memory consumption

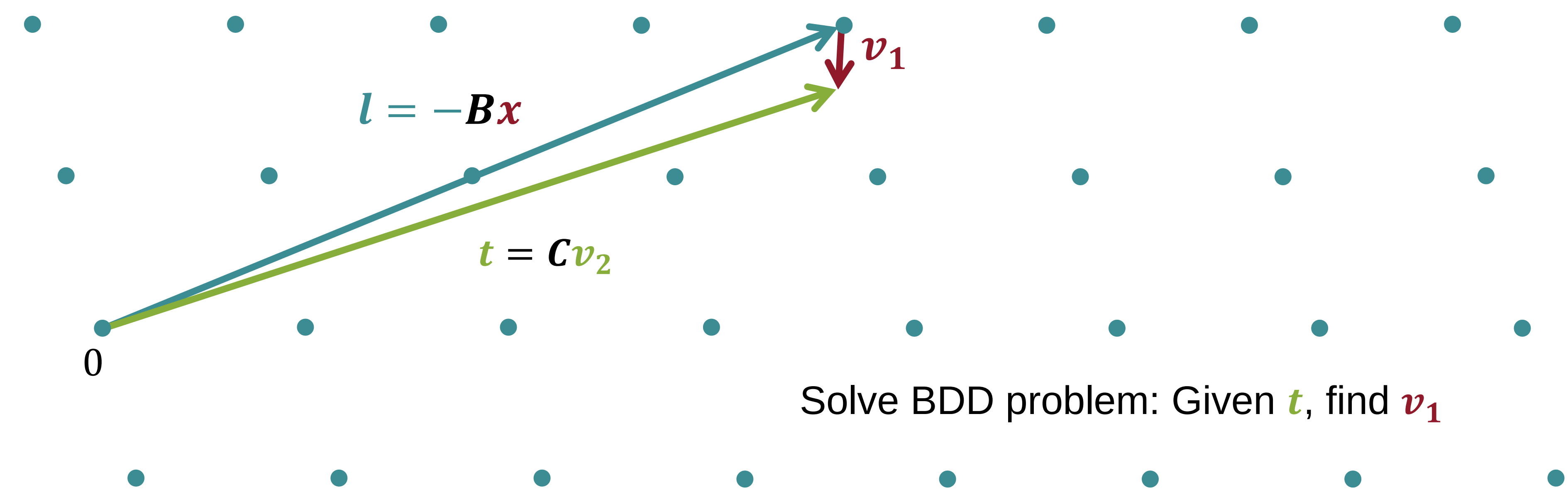
- Low collision-finding probability (might be $\approx 2^{-90}$)

The Attack

Find v_1 approach if v_2 is known

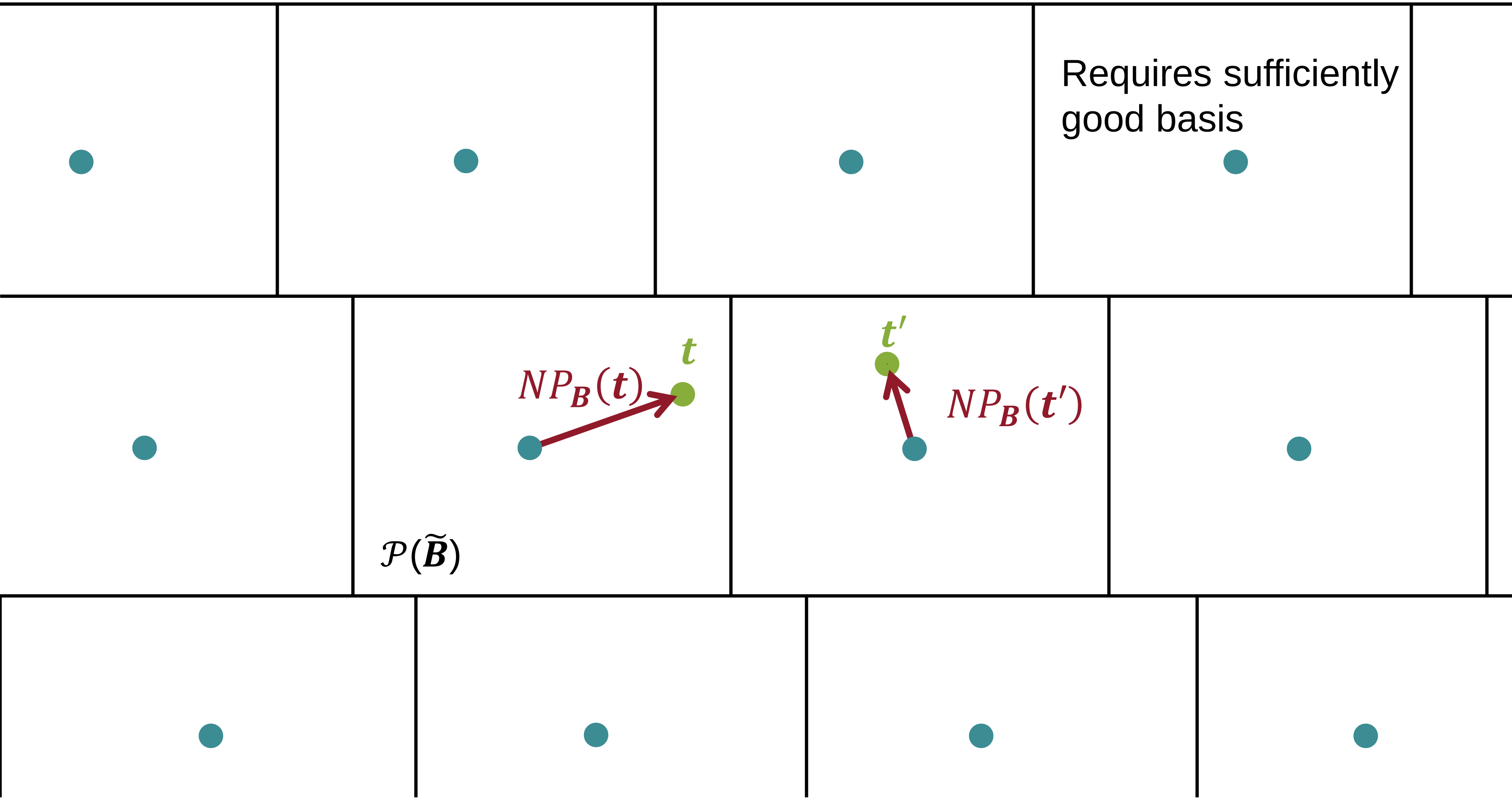
$$\boldsymbol{v} = \begin{pmatrix} \boldsymbol{v_1} \\ \boldsymbol{v_2} \end{pmatrix} = \begin{pmatrix} \boldsymbol{B} & \boldsymbol{C} \\ \boldsymbol{0} & \boldsymbol{I_r} \end{pmatrix} \begin{pmatrix} \boldsymbol{x} \\ \boldsymbol{v_2} \end{pmatrix} = \begin{pmatrix} \boldsymbol{Bx} + \boldsymbol{Cv_2} \\ \boldsymbol{v_2} \end{pmatrix}$$

Lattice $\boldsymbol{\Lambda} = \boldsymbol{\Lambda}(\boldsymbol{B})$



Solve BDD problem: Given $\boldsymbol{t}$, find $\boldsymbol{v_1}$

Solving BDD: Babai‘s Nearest Plane



DFG Deutsche Forschungsgemeinschaft
TECHNISCHE UNIVERSITÄT DARMSTADT

The Algorithm (Simplified Idea)

Task: find a shortest non-zero vector in a lattice Λ

Input: a search space $S \subset \mathbb{Z}^r$, a basis $\boldsymbol{B}' = \begin{pmatrix} \boldsymbol{B} & \boldsymbol{C} \\ \boldsymbol{0} & \boldsymbol{I}_r \end{pmatrix}$

<u>Loop</u>:
- "Quantum-guess" $\boldsymbol{v}_2' \in S$ (black box for now)
  - Check if guess is correct:
    - Calculate $\boldsymbol{v}_1' = NP_{\boldsymbol{B}}(\boldsymbol{C}\boldsymbol{v}_2')$
    - If $\boldsymbol{v} = \begin{pmatrix} \boldsymbol{v}_1' \\ \boldsymbol{v}_2' \end{pmatrix}$ is sufficiently short
      - Return $\boldsymbol{v}$

Quantum Search (simplified)

- Let $S = \{s_1, \dots, s_k\}$ be a finite search space and $D = \{p_1, \dots, p_k\}$ be a probability distribution on S.
- Let $s \in S$ be a secret sampled from D. Task: find it!
- Choose a probability distribution $A = \{a_1, \dots, a_k\}$ on S.
- There exists a quantum algorithm (generalization of Grover's search algorithm) that finds s in roughly

$$L(A) = L(a_1, \dots, a_k) = \sum \frac{p_i}{\sqrt{a_i}}$$

loops (sampling from A and testing).

How to choose the distribution A

- Minimize the function $L(a_1, \dots, a_k) = \sum \frac{p_i}{\sqrt{a_i}}$ over all $a_1, \dots, a_k \in (0,1)$ with $a_1 + \cdots + a_k = 1$.
- Optimization with constraints in k variables (→ Lagrange)
- Optimal distribution $(\overline{a_1}, \dots, \overline{a_k})$ with $\overline{a_i} = \frac{p_i^{2/3}}{\sum p_i^{2/3}}$
- **Minimal number of loops**:

$$L_{min} = \left(\sum p_i^{2/3}\right)^{3/2}$$

Example (New Hope)

Take $S = \{-16, \ldots, 16\}^{200}$ and D to be the distribution on S given in the "New Hope" key exchange scheme [ADPS16]

- Classical brute-force search:

$$L_{classical} \approx 33^{200} \approx 2^{1009}$$

- Grover's quantum search:

$$L_{Grover} \approx \sqrt{33^{200}} \approx 2^{504}$$

- Our approach:

$$L_{our} \approx 2^{1.85 \cdot 200} \approx 2^{370}$$

Results

Runtime Analysis

Main result:

Let all notations be as before and $D = \{p_1, \ldots, p_k\}$ be the distribution from which v_2 is sampled.

Success probability:

$$p_{succ} \approx \prod_{i=1}^{m-r} \left(1 - \frac{2}{B\left(\frac{m-r-1}{2}, \frac{1}{2}\right)} \int_{-1}^{\max(-r_i,-1)} (1-y^2)^{\frac{m-r-3}{2}} dy \right)$$

where $B(\cdot,\cdot)$ denotes the Euler beta function, $r_i = \frac{R_i}{2\|\boldsymbol{v}_1\|}$ and R_i is the length of the i-th Gram-Schmidt vector in $\widetilde{\boldsymbol{B}}$.

Number of operations if successful: $\mathrm{T}_{hyb} \approx \frac{(m-r)^2}{2^{1.06}} \left(\sum p_i^{2/3} \right)^{3/2}$

Runtime Analysis

Remarks:

- T_{hyb} depends on the guessing-dimension r and the „quality“ δ (Hermite factor) of the basis $\boldsymbol{B}$
- Use precomputation (basis reduction) to change δ
- Balance precomputation and actual attack costs:

$$\mathrm{T}_{total}(r,\delta) = \frac{\mathrm{T}_{red}(r,\delta) + \mathrm{T}_{hyb}(r,\delta)}{p_{succ}(r,\delta)}$$

- Non-trivial optimization process in r and δ
- More details: see paper

Results

- Runtime depends on the cost of basis reduction (BKZ)
- How to model the SVP cost inside BKZ with block size β?
- Two (very) different ways in the literature:
  - Enumeration: $\mathrm{T}_{SVP} = 2^{0.27\beta\ln(\beta) - 1.019\beta + 16.1}$
  - Sieving: $\mathrm{T}_{SVP} = 2^{0.265\beta + 16.4}$
- $\mathrm{T}_{red} \approx dim * \#tours * \mathrm{T}_{SVP}$
- → We provide two different runtime estimates
- Compare our results with the LWE estimator (not claimed security levels!)

Results: New Hope and Frodo

Attack	New Hope	Frodo-592	Frodo-752	Frodo-864
Dual	1346	446	485	618
Decoding	833	-	-	-
Qu. Hybrid	**725**	**254**	**310**	**377**

Table 1: BKZ with enumeration

Attack	New Hope	Frodo-592	Frodo-752	Frodo-864
Dual	389	173	184	219
Decoding	380	-	-	-
Qu. Hybrid	**384**	**171**	**189**	**221**

Table 2: BKZ with sieving

Results: Lindner-Peikert

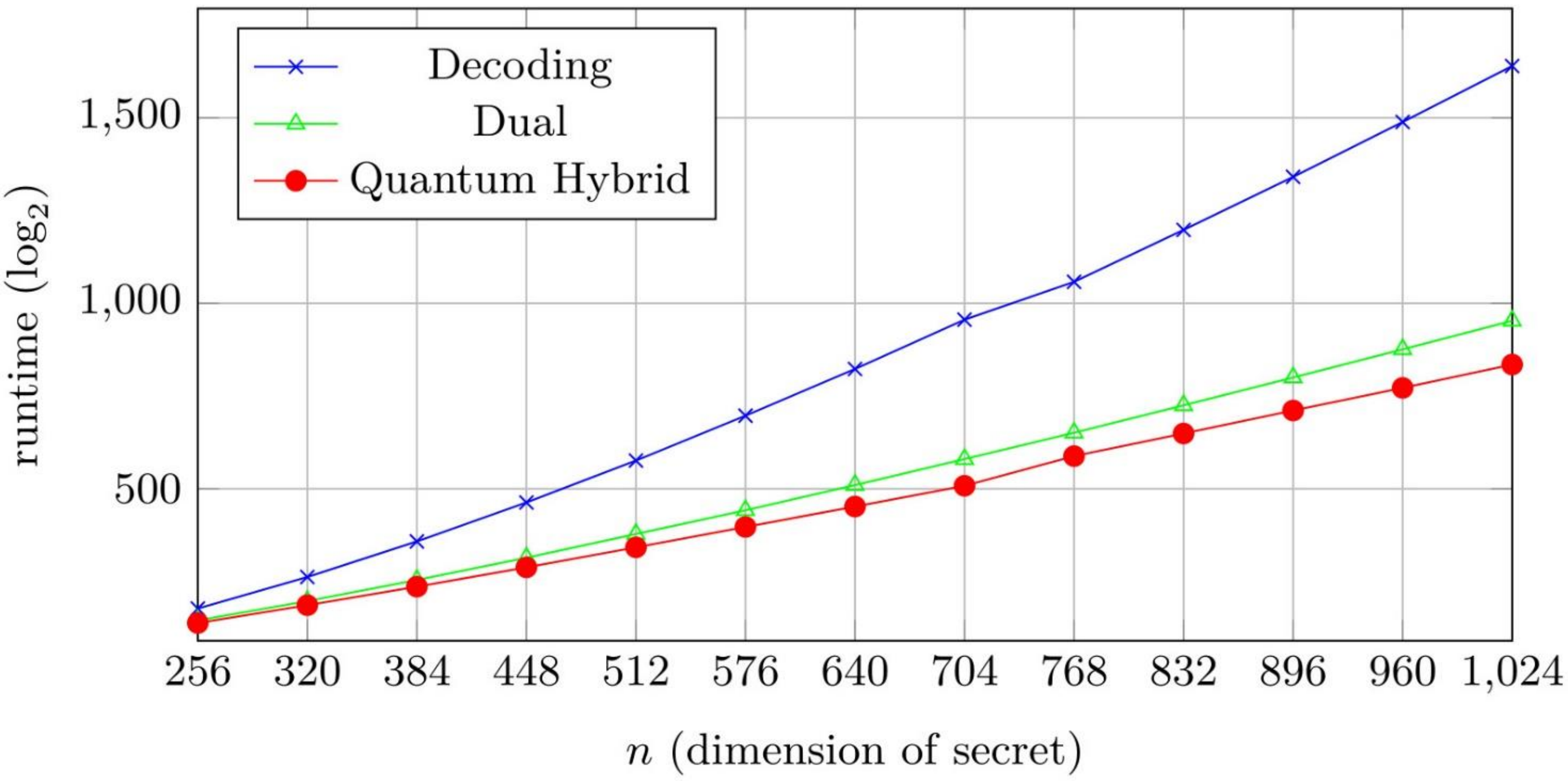


Figure 1: BKZ with enumeration

Results: Lindner-Peikert

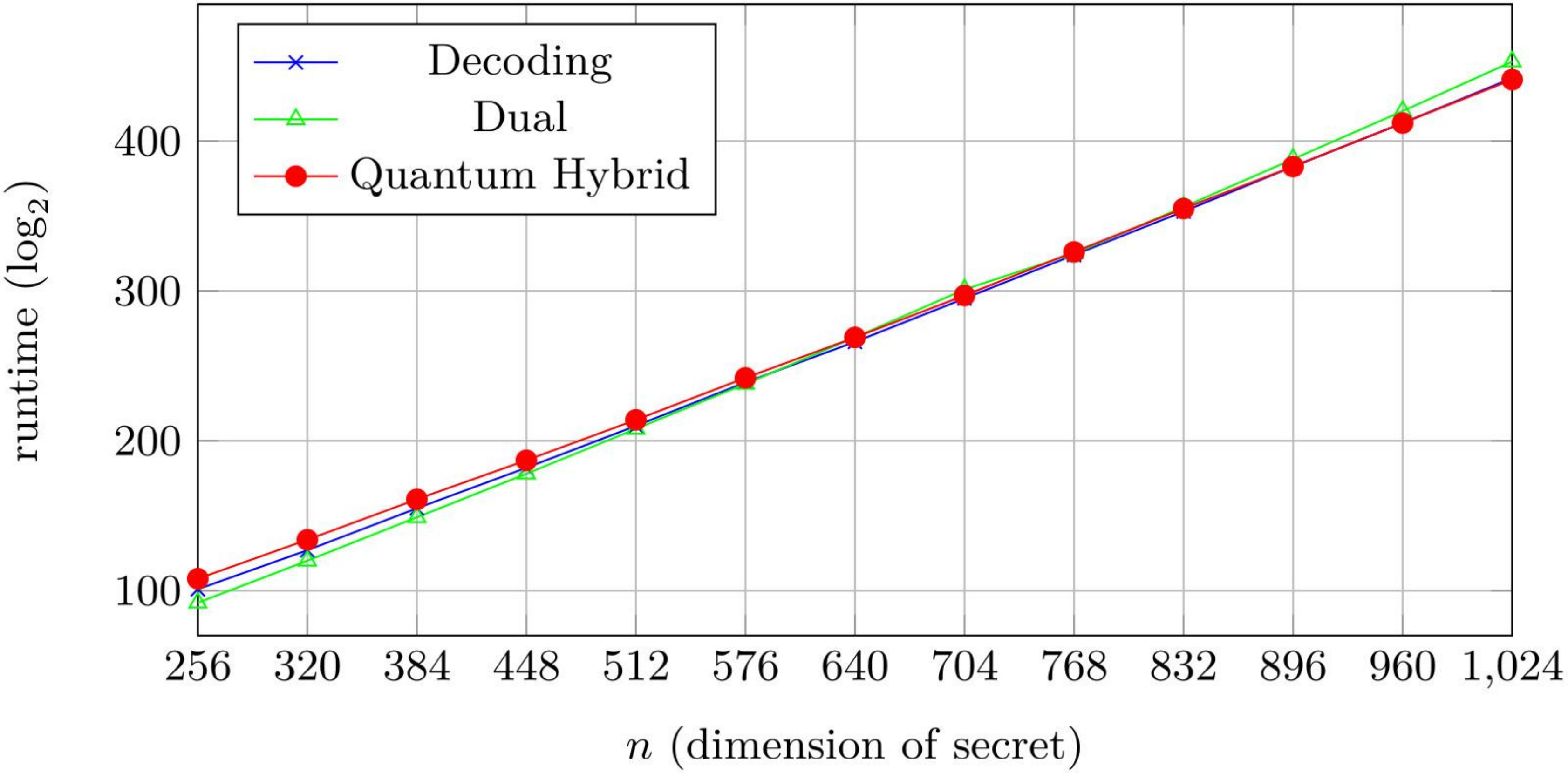


Figure 1: BKZ with enumeration

Conclusion

- New improved Quantum Hybrid Attack
- Detailed runtime analysis of the Quantum Hybrid
- New possibilities: apply Quantum Hybrid to non-uniform search spaces (e.g., LWE with Gaussian distribution)
- Outperforms other attacks in several instances

Thank you!

Questions?

Deutsche Forschungsgemeinschaft

Literature

[HG07] N. Howgrave-Graham. *A Hybrid Lattice-Reduction and Meet-in-the-Middle Attack against NTRU*.

[BGPW16] J. A. Buchmann, F. Göpfert, R. Player, and T. Wunderer. *On the Hardness of LWE with Binary Error.*

[Wun16] T. Wunderer. *Revisiting the Hybrid Attack: Improved Analysis and Refined Security Estimates*

[GvVW16] F. Göpfert, C. van Vredendaal, T. Wunderer. *The Quantum Hybrid Attack.*

[Babai86] L. Babai. *On Lovász' Lattice Reduction and the Nearest Lattice Point Problem.*

[Schank15] J. Schanck. *Practical Lattice Cryptosystems: NTRUencrypt and NTRUmls.*

[Grover96] L. K. Grover. *A Fast Quantum Mechanical Algorithm for Database Search.*

[BHMT02] G. Brassard, P. Høyer, M. Mosca, A. Tapp. *Quantum Amplitude Amplification and Estimation.*

[ADPS16] E. Alkim, L. Ducas, T. Pöppelmann, P. Schwabe. *Post-quantum Key Exchange - A New Hope.*