



# Hybrid Attacks and the Lattice Estimator

Martin Albrecht\*

Ben Curtist†

Michael Walter†

\*Royal Holloway, University of London

†Zama

{ben.curtis, michael.walter}@zama.ai

martin.albrecht@royalholloway.ac.uk

## Overview

- Lattice Estimator
  - Better Estimates
  - Examples
- Hybrid Attacks

# *How do we pick secure parameters?*

-EVERY FHE DEVELOPER, EVER

# LWE problem

The diagram illustrates the LWE problem equation:  $\mathbf{b} = \mathbf{A} \cdot \mathbf{s} + \mathbf{e} \pmod{q}$ . Matrix  $\mathbf{b}$  is a yellow vertical rectangle with dimension  $m$  indicated by a vertical line to its left. Matrix  $\mathbf{A}$  is a yellow vertical rectangle with dimension  $n$  indicated by a horizontal line above it. Matrix  $\mathbf{s}$  is a gray vertical rectangle. Matrix  $\mathbf{e}$  is a gray vertical rectangle. The equation is shown with an equals sign between  $\mathbf{b}$  and  $\mathbf{A}$ , a dot between  $\mathbf{A}$  and  $\mathbf{s}$ , a plus sign between  $\mathbf{s}$  and  $\mathbf{e}$ , and the text  $\pmod{q}$  to the right of  $\mathbf{e}$ .

$$\mathbf{A}_{i,j} \leftarrow \mathbb{Z}_q$$

$$\mathbf{s}_j \leftarrow \mathcal{D}_s$$

$$\mathbf{e}_i \leftarrow \mathcal{D}_e$$

# LWE problem

The diagram illustrates the LWE equation:  $\mathbf{b} = \mathbf{A} \cdot \mathbf{s} + \mathbf{e} \pmod{q}$ . Matrix  $\mathbf{b}$  is a yellow vertical rectangle with height  $m$ . Matrix  $\mathbf{A}$  is a yellow rectangle with width  $n$ . Matrix  $\mathbf{s}$  is a gray vertical rectangle with width  $n$ . Matrix  $\mathbf{e}$  is a gray vertical rectangle with width  $n$ . The equation is shown as  $\mathbf{b} = \mathbf{A} \cdot \mathbf{s} + \mathbf{e} \pmod{q}$ .

**Search-LWE:** given  $(\mathbf{A}, \mathbf{b})$ , find  $\mathbf{s}$

**Decision-LWE:** given  $(\mathbf{A}, \mathbf{b})$ , determine whether:

1  $\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e} \pmod{q}$ , or

2  $\mathbf{b} \leftarrow \mathcal{U}(\mathbb{Z}_q^m)$

**LWE Estimator  
vs  
Lattice Estimator**

---

**Lattice Estimator is  
v2.0 of the LWE Estimator**

**What does the  
lattice estimator  
do, anyway?**

---

LWE parameters  $(n, q, \sigma)$



Lattice Estimator



Security estimate  $\lambda$

# What does the output mean?

---

```
dual : rop:  $\approx 2^{175.0}$ , mem:  $\approx 2^{95.6}$ , m:  $\approx 2^{11.9}$  ...  
dual_hybrid : rop:  $\approx 2^{123.5}$ , mem:  $\approx 2^{92.5}$ , m:  $\approx 2^{11.1}$  ...  
dual_mitm_hybrid : rop:  $\approx 2^{113.7}$ , mem:  $\approx 2^{84.6}$ , m:  $\approx 2^{11.0}$  ...  
primal_bdd : rop:  $\approx 2^{168.3}$ , red:  $\approx 2^{168.1}$ , ...  
primal_usvp : rop:  $\approx 2^{169.0}$ , red:  $\approx 2^{169.0}$ , ...  
primal_hybrid : rop:  $\approx 2^{114.7}$ , red:  $\approx 2^{113.9}$ , ...
```



# What does the output mean?

---

```
dual : rop:  $\approx 2^{175.0}$ , mem:  $\approx 2^{95.6}$ , m:  $\approx 2^{11.9}$  ...  
dual_hybrid : rop:  $\approx 2^{123.5}$ , mem:  $\approx 2^{92.5}$ , m:  $\approx 2^{11.1}$  ...  
dual_mitm_hybrid : rop:  $\approx 2^{113.7}$ , mem:  $\approx 2^{84.6}$ , m:  $\approx 2^{11.0}$  ...  
primal_bdd : rop:  $\approx 2^{168.3}$ , red:  $\approx 2^{168.1}$ , ...  
primal_usvp : rop:  $\approx 2^{169.0}$ , red:  $\approx 2^{169.0}$ , ...  
primal_hybrid : rop:  $\approx 2^{114.7}$ , red:  $\approx 2^{113.9}$ , ...
```

# What does the output mean?

---

```
dual : rop:  $\approx 2^{175.0}$ , mem:  $\approx 2^{95.6}$ , m:  $\approx 2^{11.9}$  ...  
dual_hybrid : rop:  $\approx 2^{123.5}$ , mem:  $\approx 2^{92.5}$ , m:  $\approx 2^{11.1}$  ...  
dual_mitm_hybrid : rop:  $\approx 2^{113.7}$ , mem:  $\approx 2^{84.6}$ , m:  $\approx 2^{11.0}$  ...  
primal_bdd : rop:  $\approx 2^{168.3}$ , red:  $\approx 2^{168.1}$ , ...  
primal_usvp : rop:  $\approx 2^{169.0}$ , red:  $\approx 2^{169.0}$ , ...  
primal_hybrid : rop:  $\approx 2^{114.7}$ , red:  $\approx 2^{113.9}$ , ...
```

# What does the output mean?

---

```
dual : rop:  $\approx 2^{175.0}$ , mem:  $\approx 2^{95.6}$ , m:  $\approx 2^{11.9}$  ...  
dual_hybrid : rop:  $\approx 2^{123.5}$ , mem:  $\approx 2^{92.5}$ , m:  $\approx 2^{11.1}$  ...  
dual_mitm_hybrid : rop:  $\approx 2^{113.7}$ , mem:  $\approx 2^{84.6}$ , m:  $\approx 2^{11.0}$  ...  
primal_bdd : rop:  $\approx 2^{168.3}$ , red:  $\approx 2^{168.1}$ , ...  
primal_usvp : rop:  $\approx 2^{169.0}$ , red:  $\approx 2^{169.0}$ , ...  
primal_hybrid : rop:  $\approx 2^{114.7}$ , red:  $\approx 2^{113.9}$ , ...
```

Security estimate  $\lambda \approx 113.7$

# A (subset) of important output values

**rop**

**Ring operations**

(Total cost of the attack)

**m**

**Number of  
samples**

(LWE samples required)

**red**

**Cost of lattice  
reduction**

(BKZ)

# What's New?

**Better Estimates**

**Modularity**

**Input Changes**

# What's New?

## Better Estimates

More supported attacks















BKZ simulator

## Modularity

## Input Changes

# Better Estimates (1)

---

Attack	LWE Estimator	Lattice Estimator
Dual		
uSVP		
Decoding		
Hybrid-dual		
Hybrid-decoding		
Exhaustive Search		
Meet-In-The-Middle techniques		

# Better Estimates (1)

---

Attack
Dual
uSVP
Decoding
Hybrid-dual
Hybrid-decoding
Exhaustive Search
Meet-In-The-Middle techniques

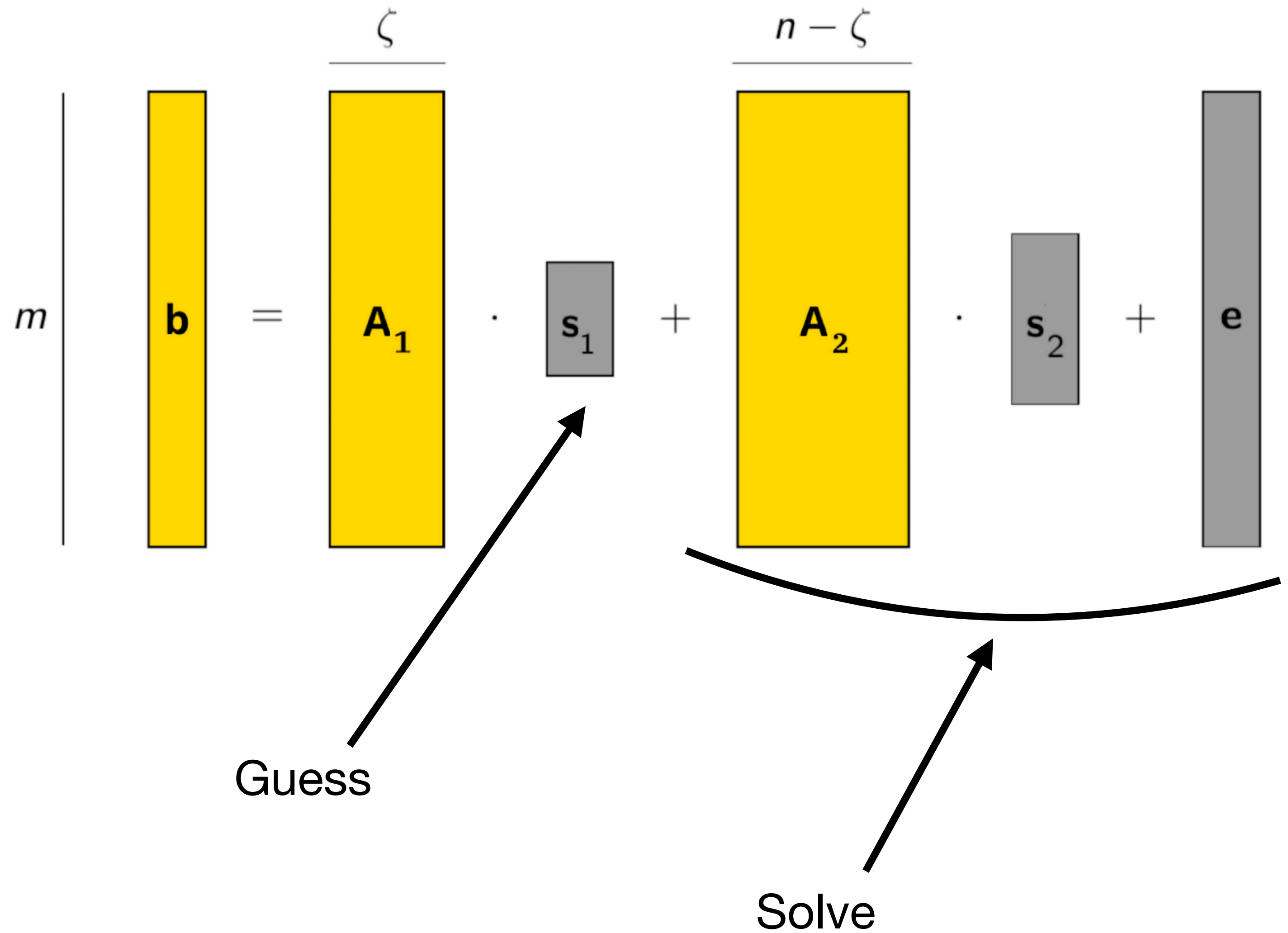
Lattice Estimator
?
?
?
?
?
?
?



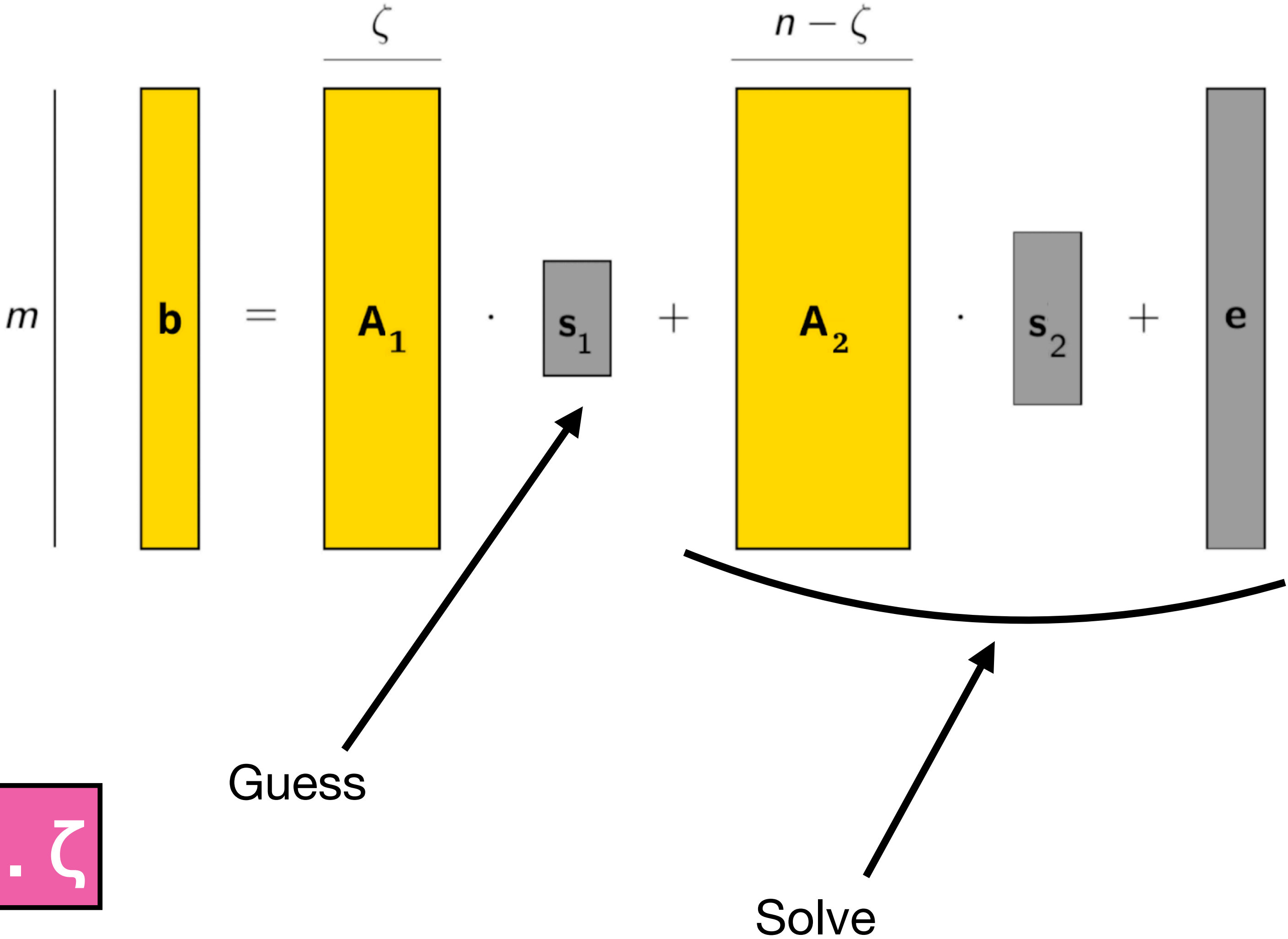
# Hybrid Attacks

$$\begin{array}{c} m \\ | \\ \mathbf{b} \end{array} = \begin{array}{c} \zeta \\ | \\ \mathbf{A}_1 \end{array} \cdot \begin{array}{c} \mathbf{s}_1 \end{array} + \begin{array}{c} n - \zeta \\ | \\ \mathbf{A}_2 \end{array} \cdot \begin{array}{c} \mathbf{s}_2 \end{array} + \begin{array}{c} \mathbf{e} \end{array}$$

# Hybrid Attacks



# Hybrid Attacks



# Hybrid (Dual) Attack

$$\begin{array}{ccccccc} & & & \zeta & & n - \zeta & \\ & & & \hline & & & & & & \\ m & \mathbf{b} & = & \mathbf{A}_1 & \cdot & \mathbf{s}_1 & + & \mathbf{A}_2 & \cdot & \mathbf{s}_2 & + & \mathbf{e} \end{array}$$

$$L = \{ \mathbf{x} \in \mathbb{Z}_q^m \mid \mathbf{x} \mathbf{A}_2 \equiv \mathbf{0} \pmod{q} \}$$

$$\mathbf{v} \leftarrow \mathbf{BKZ}_\beta(L)$$

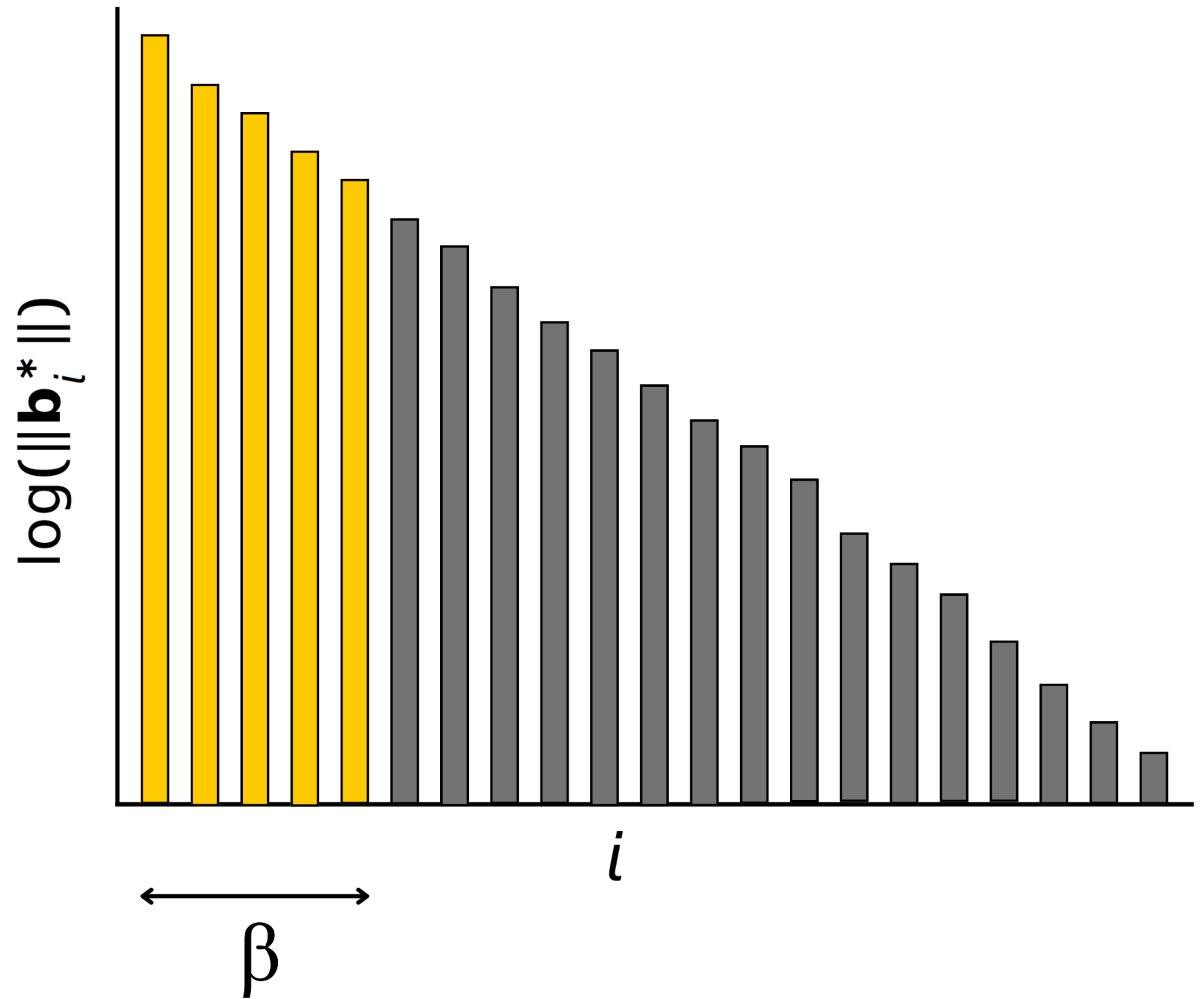
$$\langle \mathbf{v}, \mathbf{b} \rangle \approx \langle \mathbf{v}, \mathbf{A}_2 \mathbf{s}_2 + \mathbf{e} \rangle = \langle \mathbf{v} \mathbf{A}_2, \mathbf{s}_2 \rangle + \langle \mathbf{v}, \mathbf{e} \rangle = \langle \mathbf{v}, \mathbf{e} \rangle \pmod{q}$$

[CHHS19]: A Hybrid of Dual and Meet-in-the-Middle Attack on Sparse and Ternary Secret LWE. Jung Hee Cheon, Minki Hhan, Seungwan Hong, and Yongha Son

[BLLWZ21]: Hybrid Dual Attack on LWE with Arbitrary Secrets. Lei Bi, Xianhui Lu, Junjie Luo, Kunpeng Wang, and Zhenfei Zhang

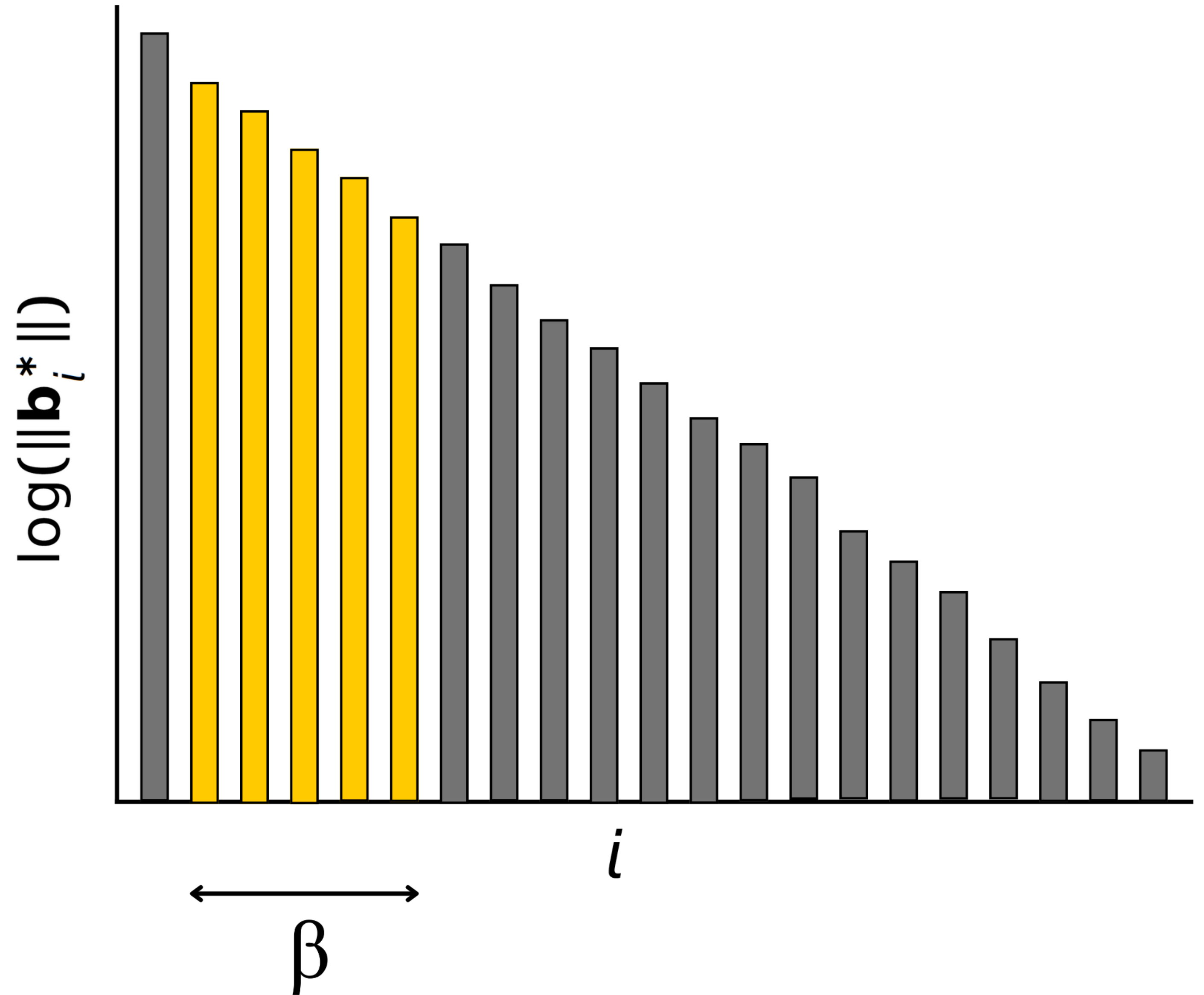
# Getting Short Vectors: BKZ

---



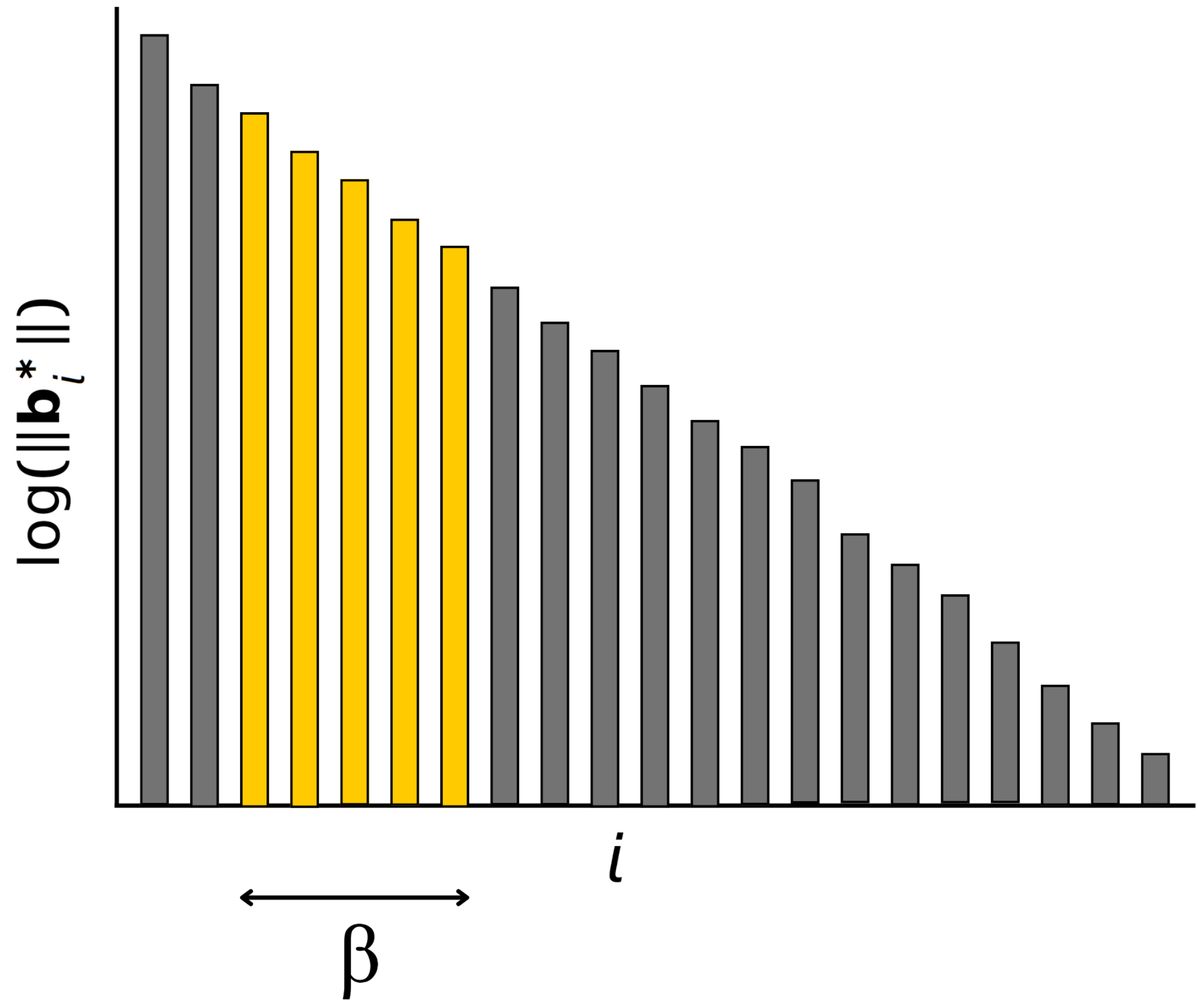
# Getting Short Vectors: BKZ

---

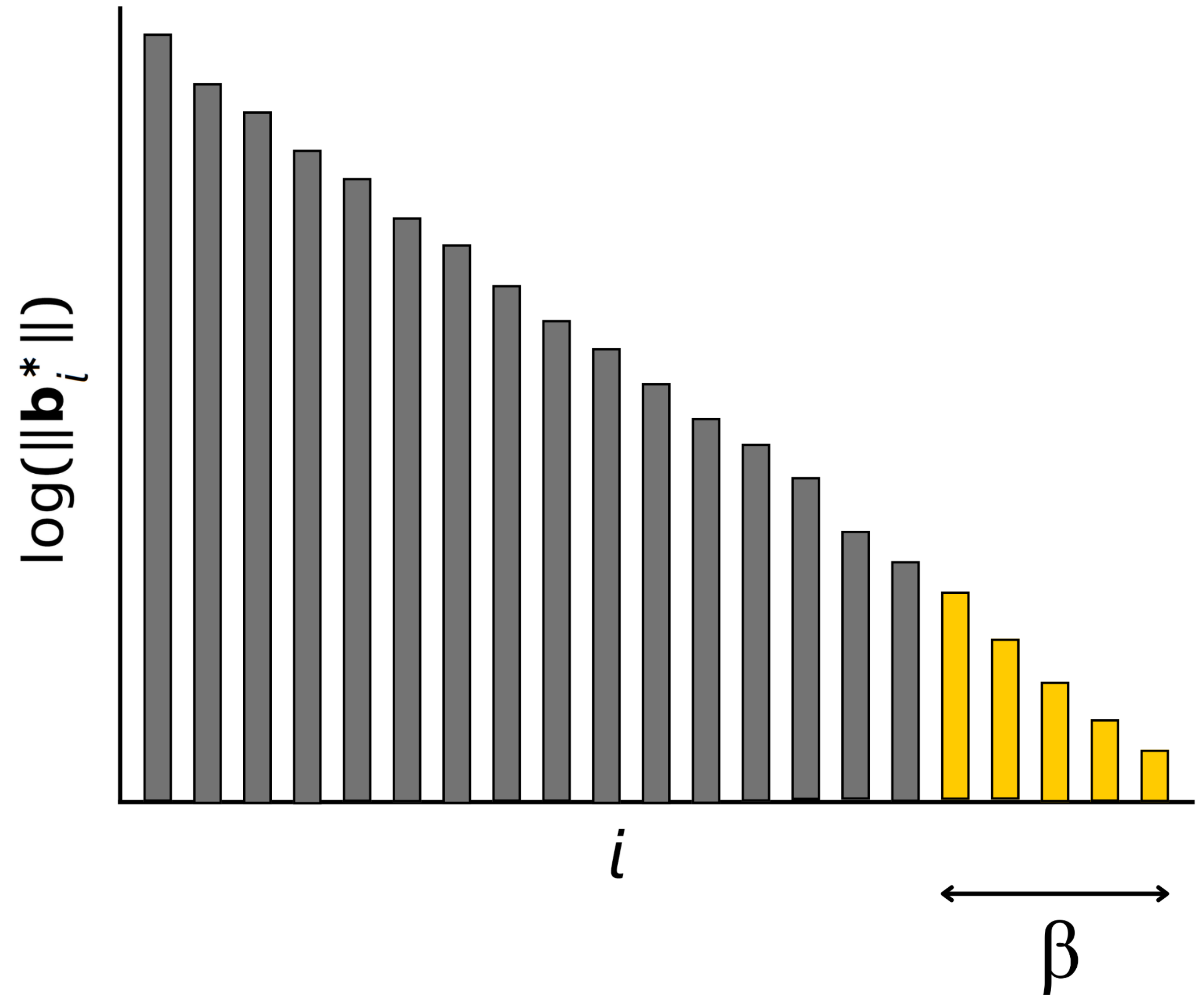


# Getting Short Vectors: BKZ

---

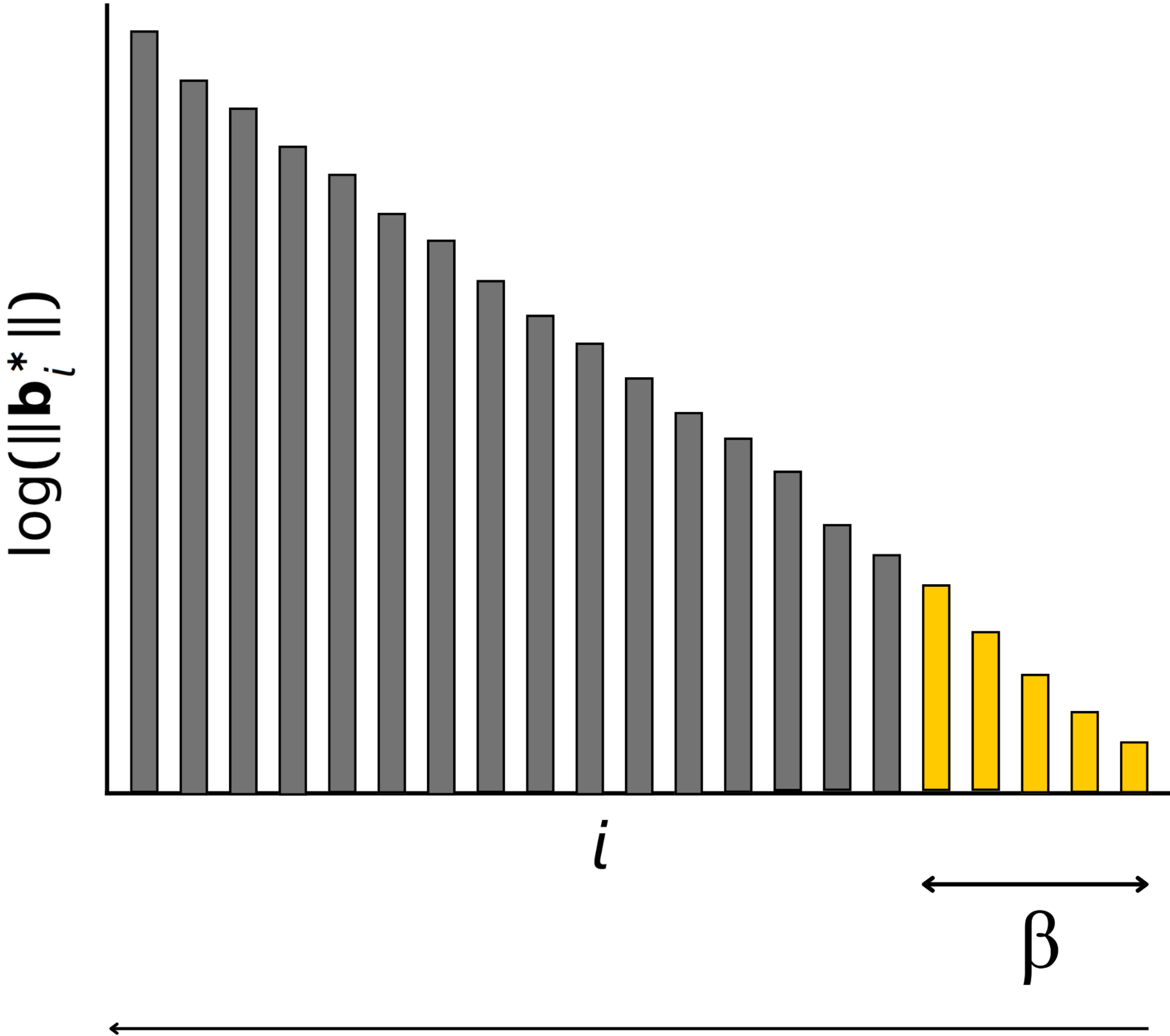


# Getting Short Vectors: BKZ





# Getting Short Vectors: BKZ



# Hybrid Attacks

$$\begin{array}{ccccccc}
 & & & \zeta & & n - \zeta & \\
 & & & \hline
 & & & \mathbf{A}^1 & & \mathbf{A}^2 & \\
 & & & \cdot & & \cdot & \\
 m & \mathbf{b} & = & & + & & + \\
 & & & \mathbf{s}^1 & & \mathbf{s}^2 & \\
 & & & \cdot & & \cdot & \\
 & & & & & & \mathbf{e}
 \end{array}$$

$$L = \{ \mathbf{x} \in \mathbb{Z}_q^m \mid \mathbf{x} \mathbf{A}_2 \equiv \mathbf{0} \pmod{q} \}$$

$$\mathbf{v} \leftarrow \mathbf{BKZ}_\beta(L)$$

$$\langle \mathbf{v}, \mathbf{b} \rangle \approx \langle \mathbf{v}, \mathbf{A}_2 \mathbf{s}_2 + \mathbf{e} \rangle = \langle \mathbf{v} \mathbf{A}_2, \mathbf{s}_2 \rangle + \langle \mathbf{v}, \mathbf{e} \rangle = \langle \mathbf{v}, \mathbf{e} \rangle \pmod{q}$$

2.  $\beta$

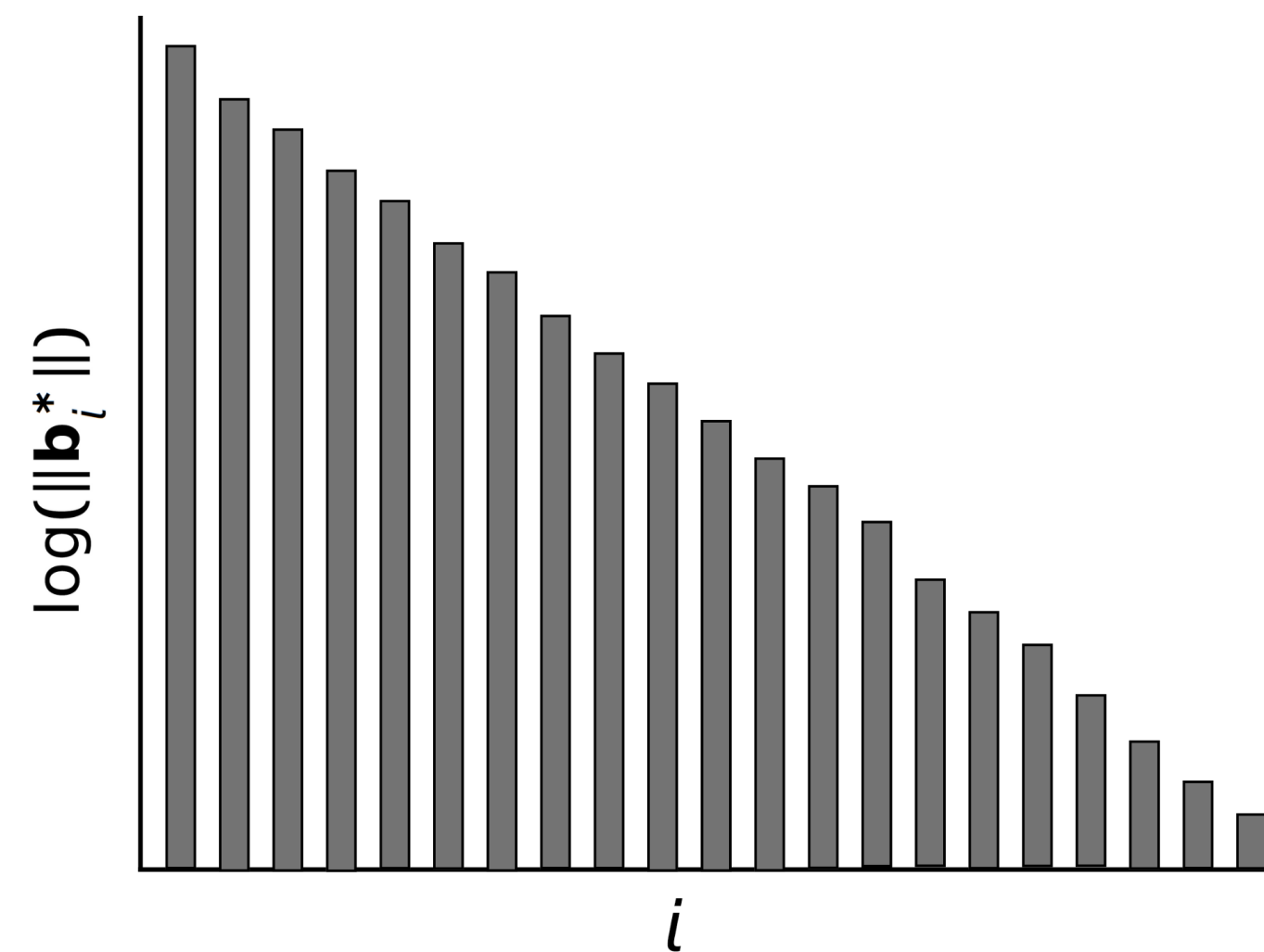
3.  $m$

[CHHS19]: A Hybrid of Dual and Meet-in-the-Middle Attack on Sparse and Ternary Secret LWE. Jung Hee Cheon, Minki Hhan, Seungwan Hong, and Yongha Son

[BLLWZ21]: Hybrid Dual Attack on LWE with Arbitrary Secrets. Lei Bi, Xianhui Lu, Junjie Luo, Kunpeng Wang, and Zhenfei Zhang

# Better Estimates (2): BKZ Simulator

- LWE Estimator Assumed GSA (only)
- Lattice Estimator includes BKZ Simulation



# What's New?

Better Estimates

**Modularity**

New code structure for  
ease-of-use

Input Changes

# No More estimator.py

---

```
+-- LWE Estimator
  +-- estimator.py

+-- Lattice Estimator
  +-- docs
  |   +-- ...
  +-- estimator
      +-- conf.py
      +-- cost.py
      +-- errors.py
      +-- ...
```

# What's New?

Better Estimates

Modularity

**Input Changes**

Input LWE parameters  
are more intuitive

# Simpler Parameter Representation (1)

---

```
n = 512
m = 1024
q = 8192
alpha_0 = alphaf(sqrt(10/4.0), q, sigma_is_stddev=True) # error
alpha_1 = alphaf(sqrt(21/4.0), q, sigma_is_stddev=True) # secret
_ = estimate_lwe(n, alpha_0, q, secret_distribution=alpha_1, reduction_cost_model=BKZ.sieve, m=m)
```

# Simpler Parameter Representation (1)

---

```
n = 512
m = 1024
q = 8192
alpha_0 = alphaf(sqrt(10/4.0), q, sigma_is_stddev=True) # error
alpha_1 = alphaf(sqrt(21/4.0), q, sigma_is_stddev=True) # secret
_ = estimate_lwe(n, alpha_0, q, secret_distribution=alpha_1, reduction_cost_model=BKZ.sieve, m=m)
```

```
params = LWEParameters(n=512, q=3329, Xs=D(σ=1.22), Xe=D(σ=1.22), m=512, tag='Kyber 512')
LWE.estimate(params)
```



# Simpler Parameter Representation (2)

---

```
secret_distribution = (0, 1)
secret_distribution = "normal"
secret_distribution = alpha
secret_distribution = ((-1, 1), 64)
```

## Simpler Parameter Representation (2)

---

```
secret_distribution = (0, 1)  
secret_distribution = "normal"  
secret_distribution = alpha  
secret_distribution = ((-1, 1), 64)
```

```
Xs=D(1.22)
```

```
Xs=UniformMod(2)
```

```
Xs=CenteredBinomial(2)
```

***How do we pick secure parameters?***

-FHE DEVELOPERS

# *How do we pick secure parameters?*

-FHE DEVELOPERS

<https://github.com/malb/lattice-estimator>

Contributions welcome!

- Benjamin Curtis
- Cedric Lefebvre
- Fernando Virdia
- Florian Göpfert
- James Owen
- Léo Ducas
- Markus Schmidt
- Martin Albrecht
- Michael Walter
- Rachel Player
- Sam Scott

# Summary

## More Features

Hybrid-dual  
Hybrid-decoding  
BKZ simulator

## Modularity

New code structure for  
ease-of-use

## Input Changes

Input LWE parameters  
are much more  
intuitive

# Questions?

