RUB

RUHR-UNIVERSITÄT BOCHUM

Low Weight Discrete Logarithms and Subset Sum in $2^{0.65n}$ with Polynomial Memory

EUROCRYPT 2020, May 11.-15. 2020

Andre Esser and Alexander May
Horst Görtz Institute for IT Security
Ruhr University Bochum

hgi
Horst Görtz Institut
für IT-Sicherheit

Subset Sum

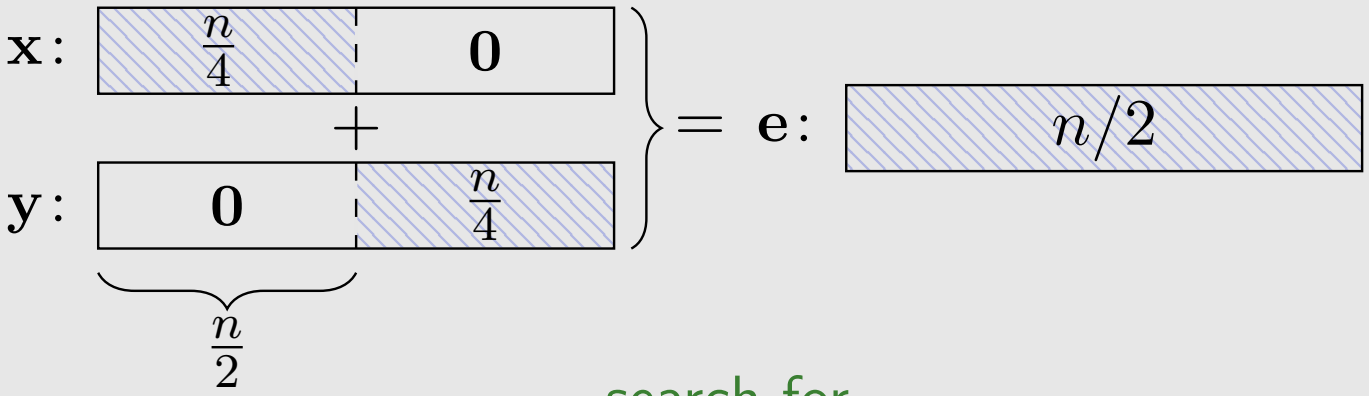
Subset Sum Problem

Given: $(a_1, \ldots, a_n, t, \omega)$, where $a_i, t \in \mathbb{Z}_{2^n}$ and $\omega \in \left[0, \frac{1}{2}\right]$

Find: $\mathbf{e} \in \{0,1\}^n$: $\sum e_i a_i = t \bmod 2^n$ and $\mathrm{wt}(\mathbf{e}) = \omega n$

- Random instance: $a_i \in_R \mathbb{Z}_{2^n}$
- Cryptanalytic applications (Decoding, LPN, SIS, DLP)
- $\mathbf{a} := (a_1, \ldots, a_n)$

A memoryless Meet-in-the-Middle



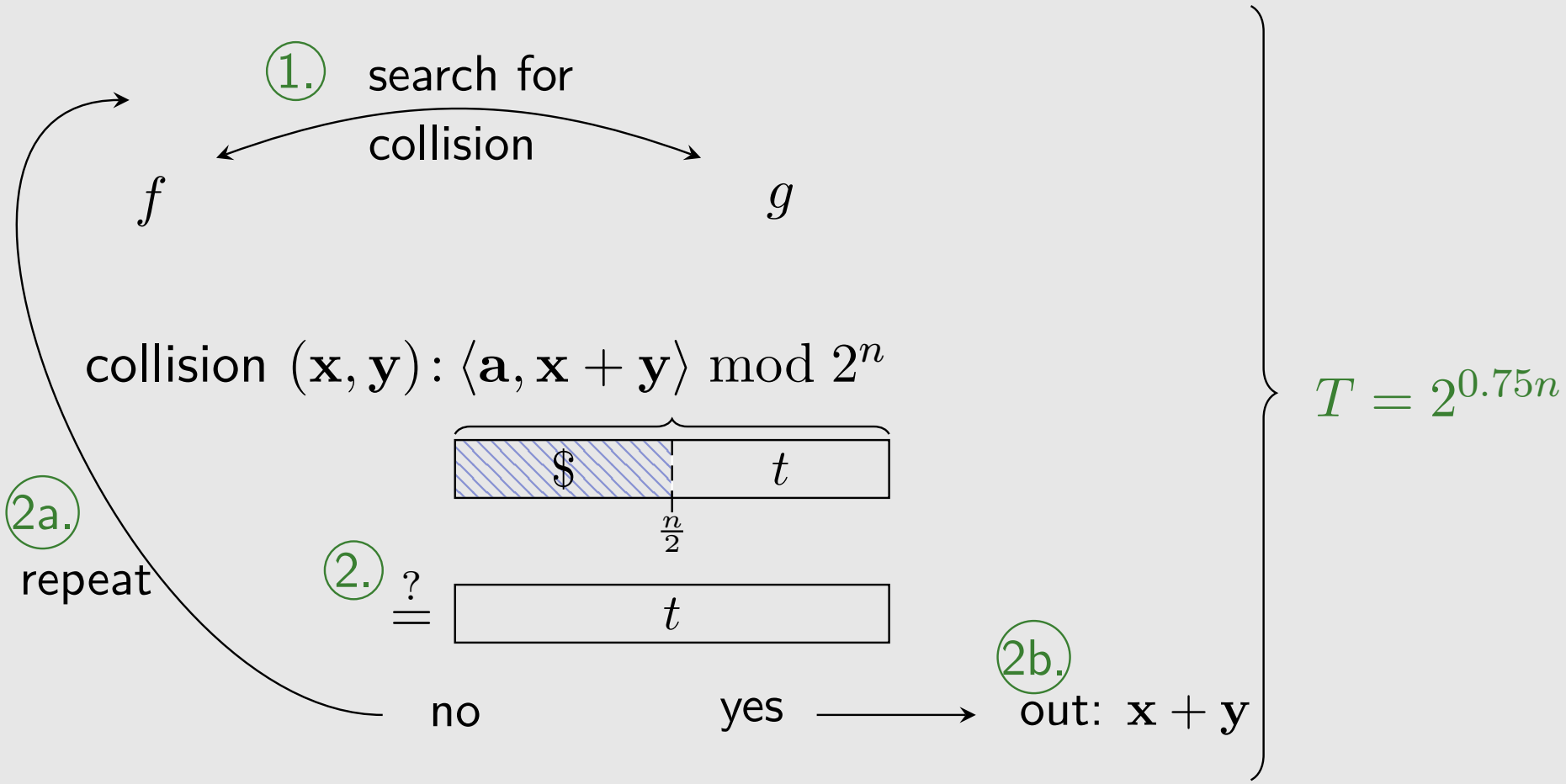
search for collision

$$f(\mathbf{x}) := \langle \mathbf{a}, \mathbf{x} \rangle \bmod 2^{\frac{n}{2}} \qquad g(\mathbf{y}) := t - \langle \mathbf{a}, \mathbf{y} \rangle \bmod 2^{\frac{n}{2}}$$

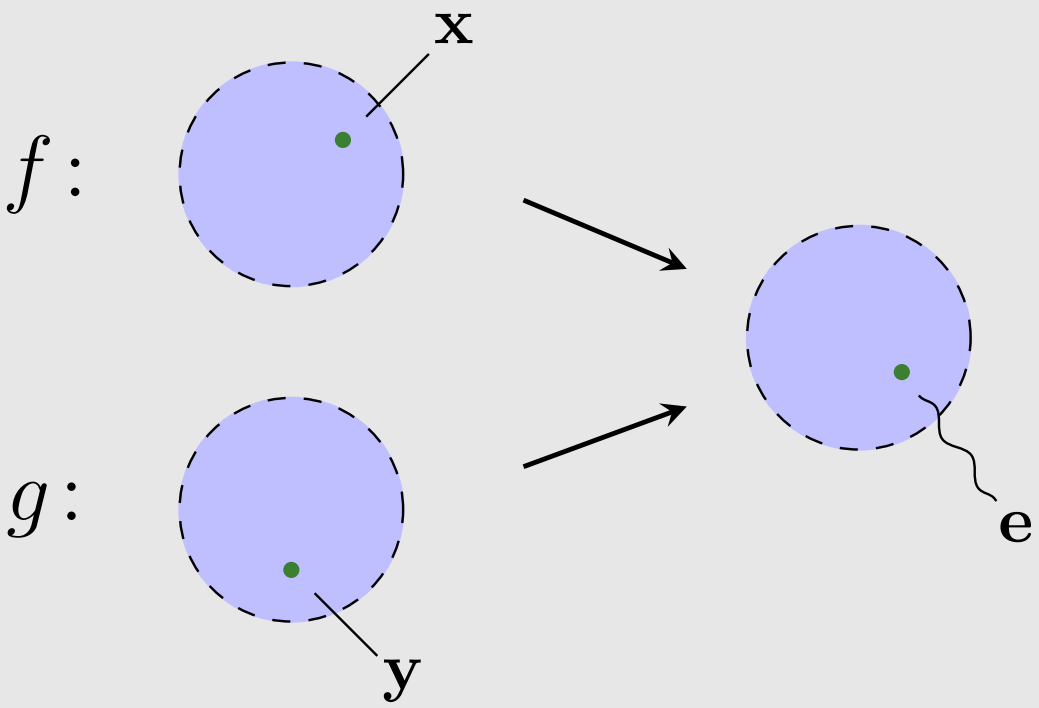
collision: $$\langle \mathbf{a}, \mathbf{x} \rangle = t - \langle \mathbf{a}, \mathbf{y} \rangle \mod 2^{\frac{n}{2}}$$

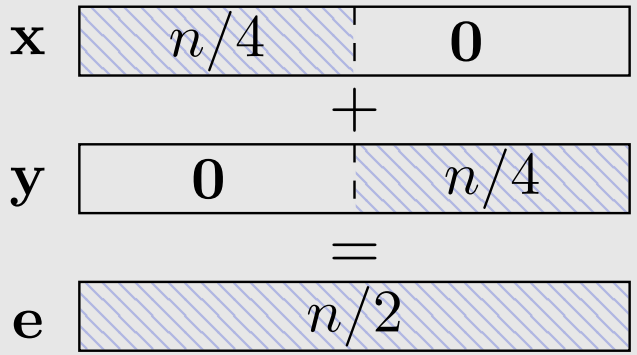
$$t = \langle \mathbf{a}, \mathbf{x} + \mathbf{y} \rangle \bmod 2^{\frac{n}{2}}$$

Folklore Algorithm

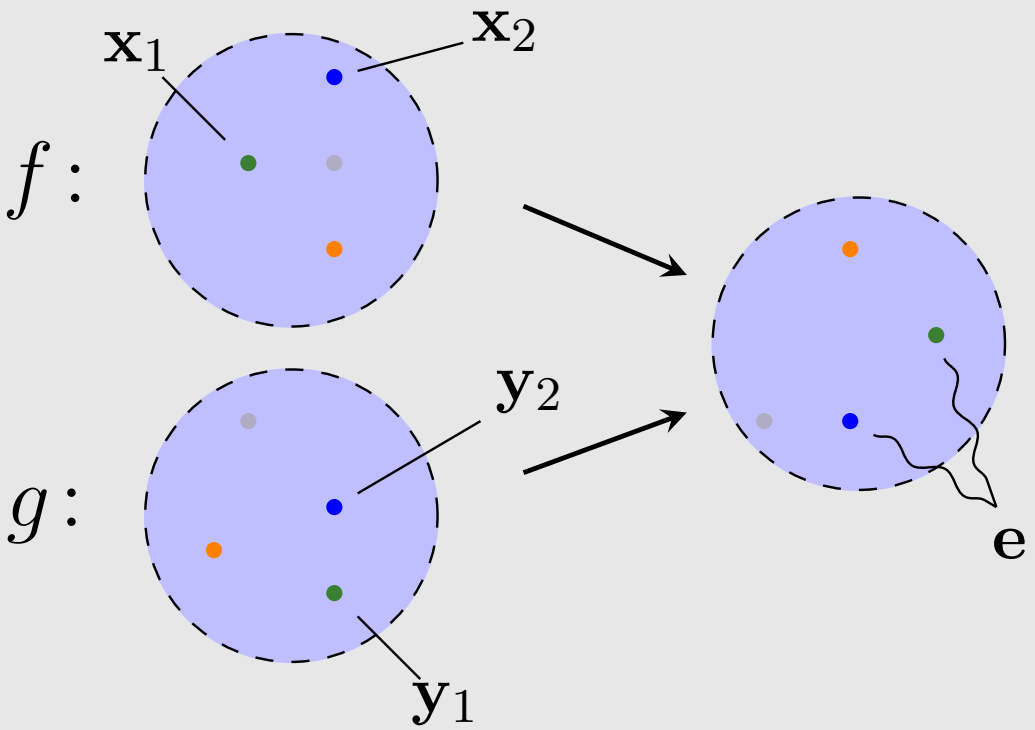


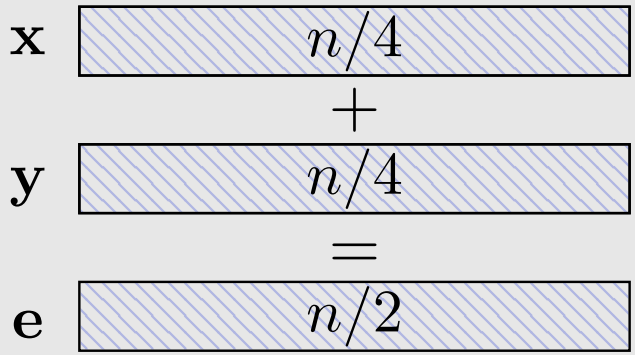
The Representation Technique





The Representation Technique

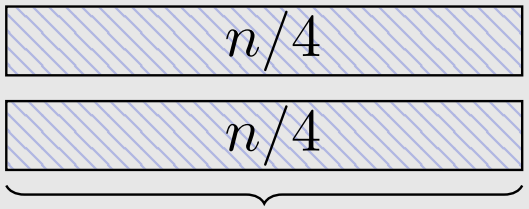




many representations

Goal: increase domain and #useful collisions

The memoryless BCJ Algorithm



increased size

$\Rightarrow$ increased modulus

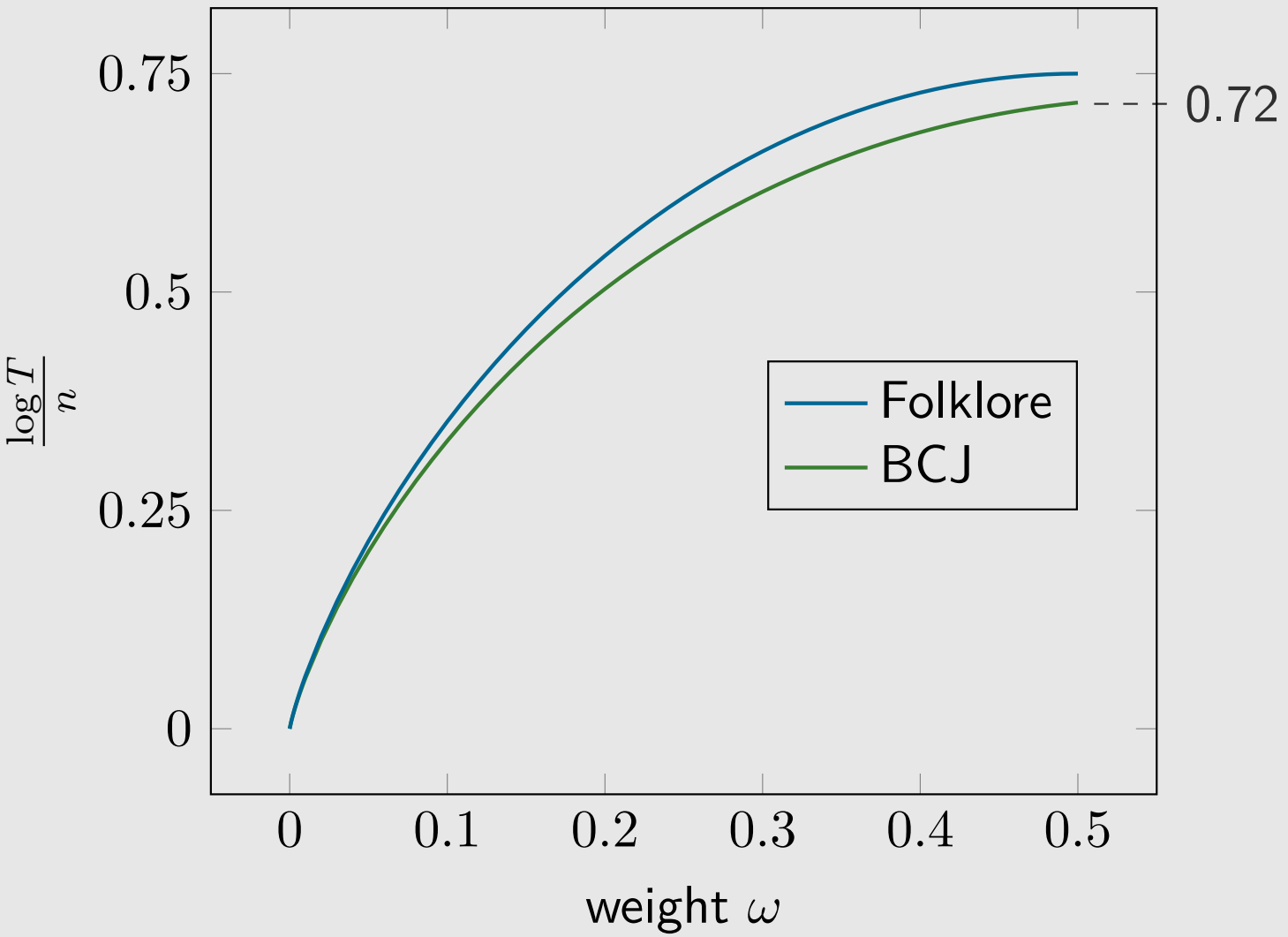
more collisions

many good collisions

$$T = \left(\frac{\#\text{good Colls}}{\#\text{all Colls}}\right)^{-1} \cdot T_C$$

$$= 2^{0.72n}$$

Folklore vs. BCJ



Discrete Logarithms

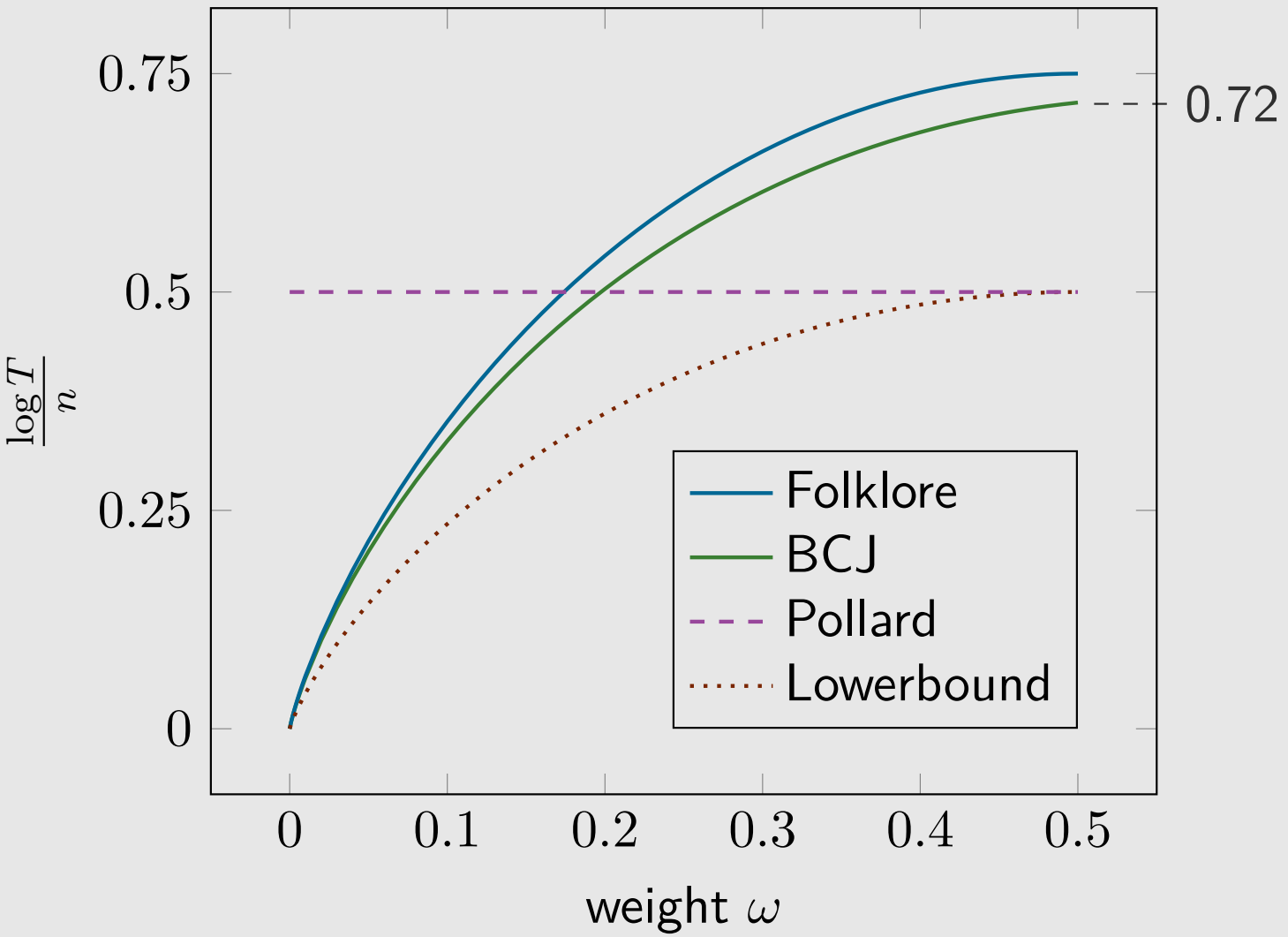
(low weight) DLP

Given: group G with $|G| \approx 2^n$ generated by g, $\beta \in G$ and $\omega \in \left[0, \frac{1}{2}\right]$

Find: $\alpha = \mathrm{dlog}_g \beta$ satisfying $g^\alpha = \beta$ and $\mathrm{wt}(\alpha) = \omega n$

- Time lower bound $\sqrt{\binom{n}{\omega n}}$ (MitM)
- $\omega = \frac{1}{2}$ *usual* case
- Pollard Rho ($T = 2^{0.5n}, M =$poly)

low-weight DLP Landscape

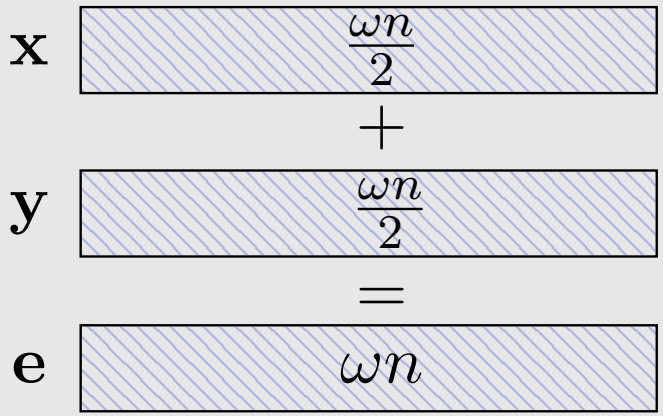


Use of Carry Bits

search for collision

$$f_1(x) := g^x \qquad f_2(y) := \beta g^{-y}$$

collision: $g^{x+y} = \beta = g^{\alpha}$



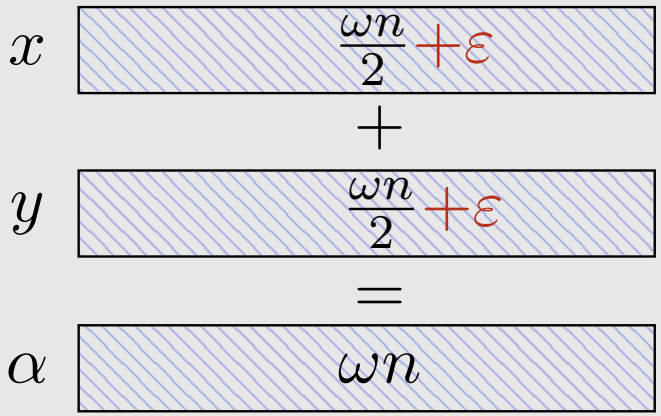
Use of Carry Bits

search for collision

$$f_1(x) := g^x \qquad f_2(y) := \beta g^{-y}$$

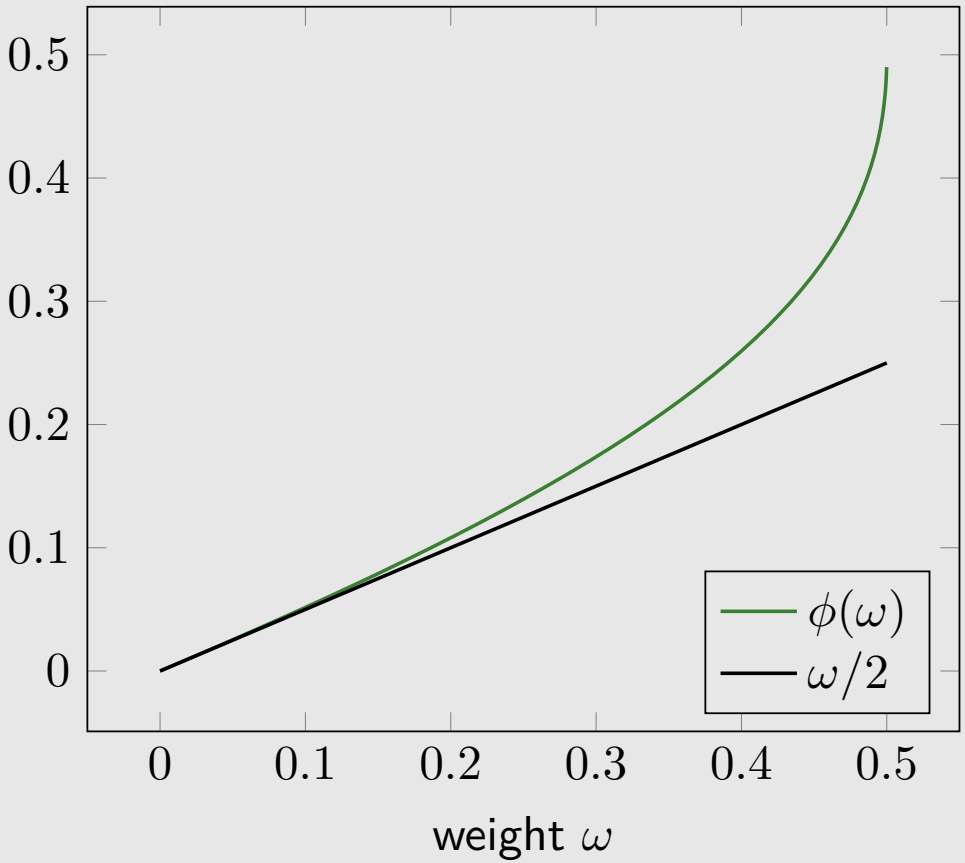
collision: $g^{x+y} = \beta = g^{\alpha}$

$x + y$ computed over $\mathbb{Z}$ $(\mathrm{mod}|G|)$



Increase the Weight

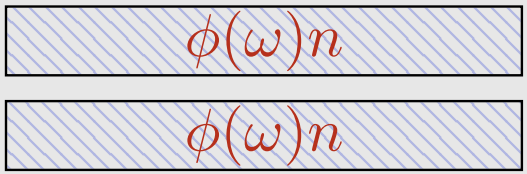
$$\mathsf{wt}(x) = \mathsf{wt}(y) = \frac{\omega n}{2} + \varepsilon = \underline{\phi(\omega)} n$$



The new Algorithm

search for collision

$f_1(x)$ $f_2(y)$



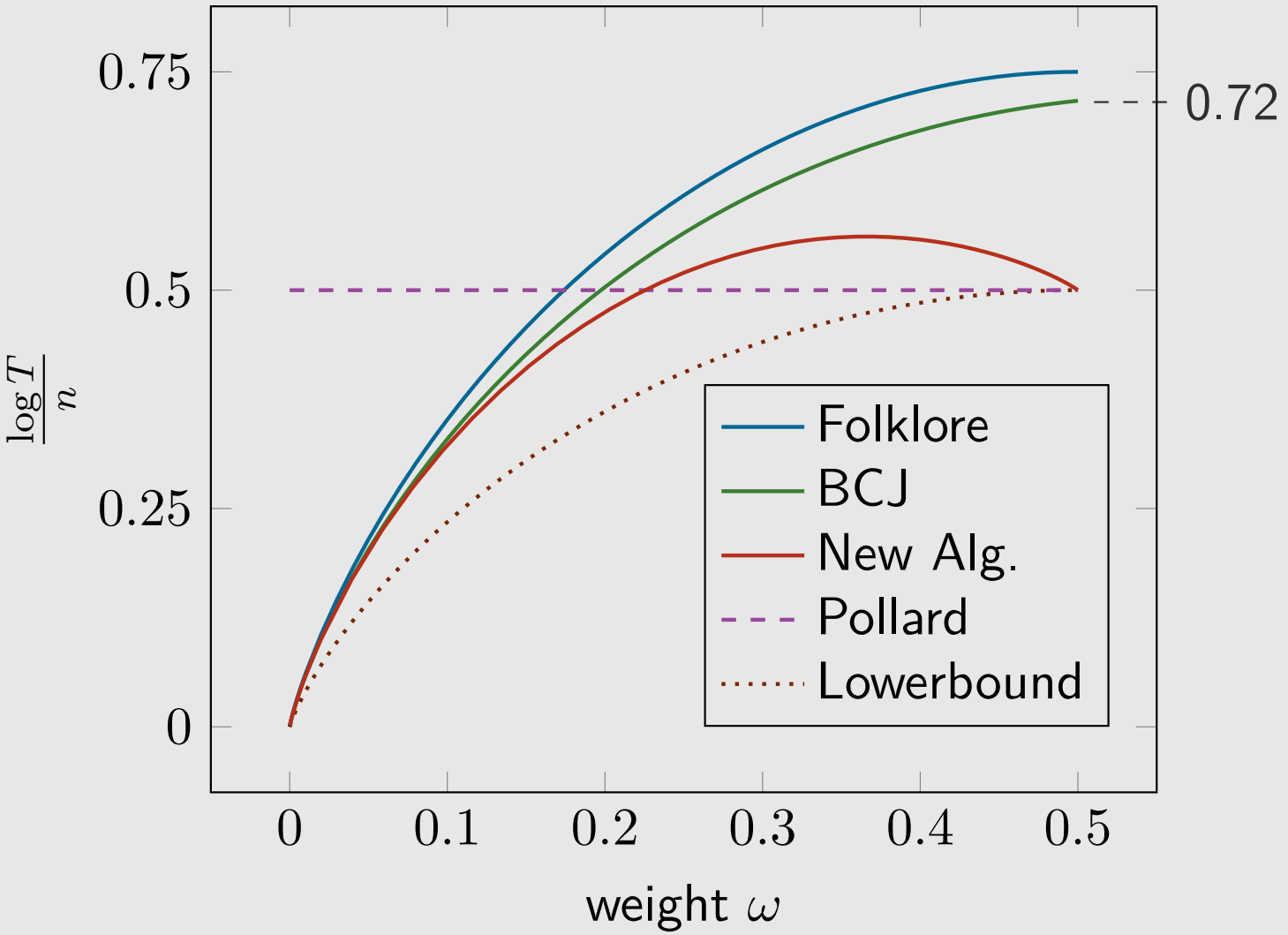
increased domainsize

$\Rightarrow$ more Representations

$$T = \left(\frac{\#\text{good Colls}}{\#\text{all Colls}}\right)^{-1} \cdot T_C$$

$$= 2^{(H(\omega)-H(\phi)/2)n}$$

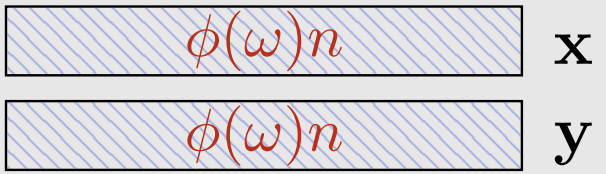
Updated low-weight DLP Landscape



A new Time-Memory-Tradeoff

search for collision

$f_1(\mathbf{x})$ $f_2(\mathbf{y})$



increased domain size

$\Rightarrow$ more representations

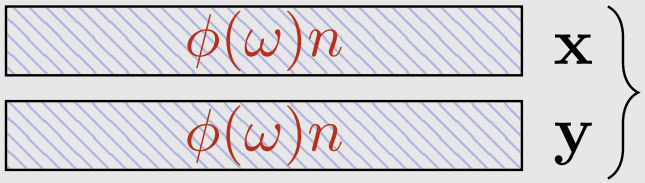
$$T = \left(\frac{\#\text{good Colls}}{\#\text{all Colls}}\right)^{-1} \cdot T_C$$

$$= 2^{(H(\omega)-H(\phi)/2)n}$$

A new Time-Memory-Tradeoff

search for collision

$f_1(\mathbf{x})$ $f_2(\mathbf{y})$



increased domain size

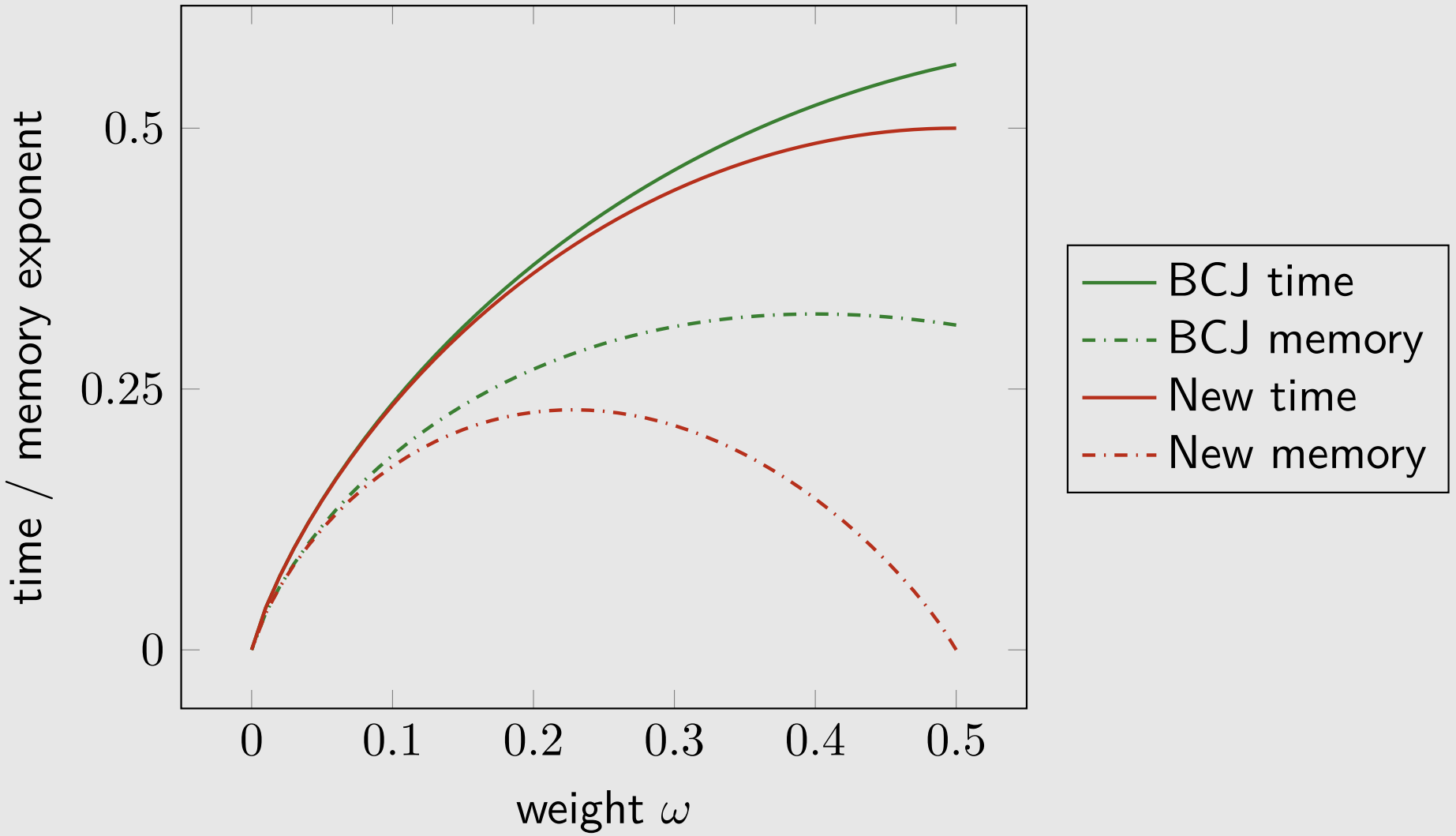
$\Rightarrow$ more representations

$$T = \sqrt{\left(\frac{\#\text{good Colls}}{\#\text{all Colls}}\right)^{-1}} \cdot T_C$$

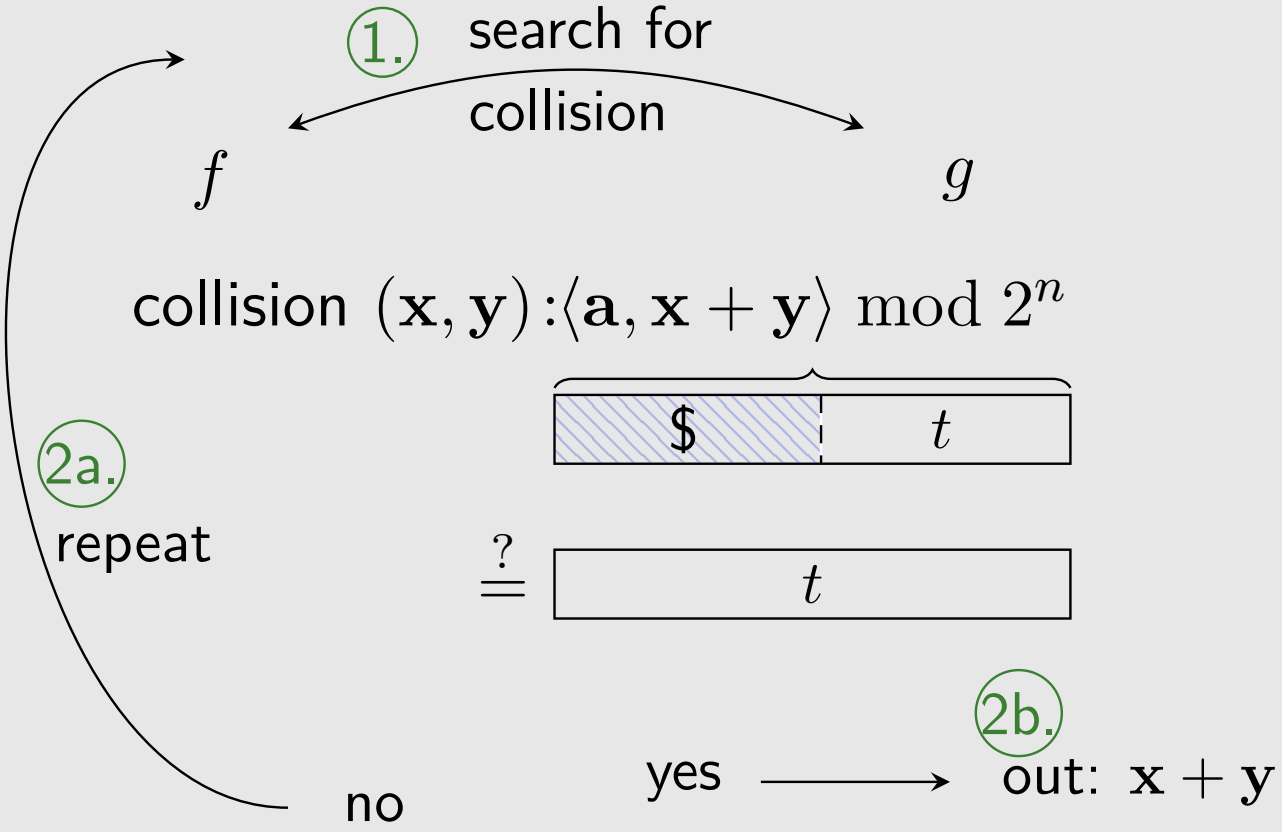
$$= 2^{\frac{H(\omega)n}{2}}$$

$$M = \left(\frac{\#\text{good Colls}}{\#\text{all Colls}}\right)^{-1}$$

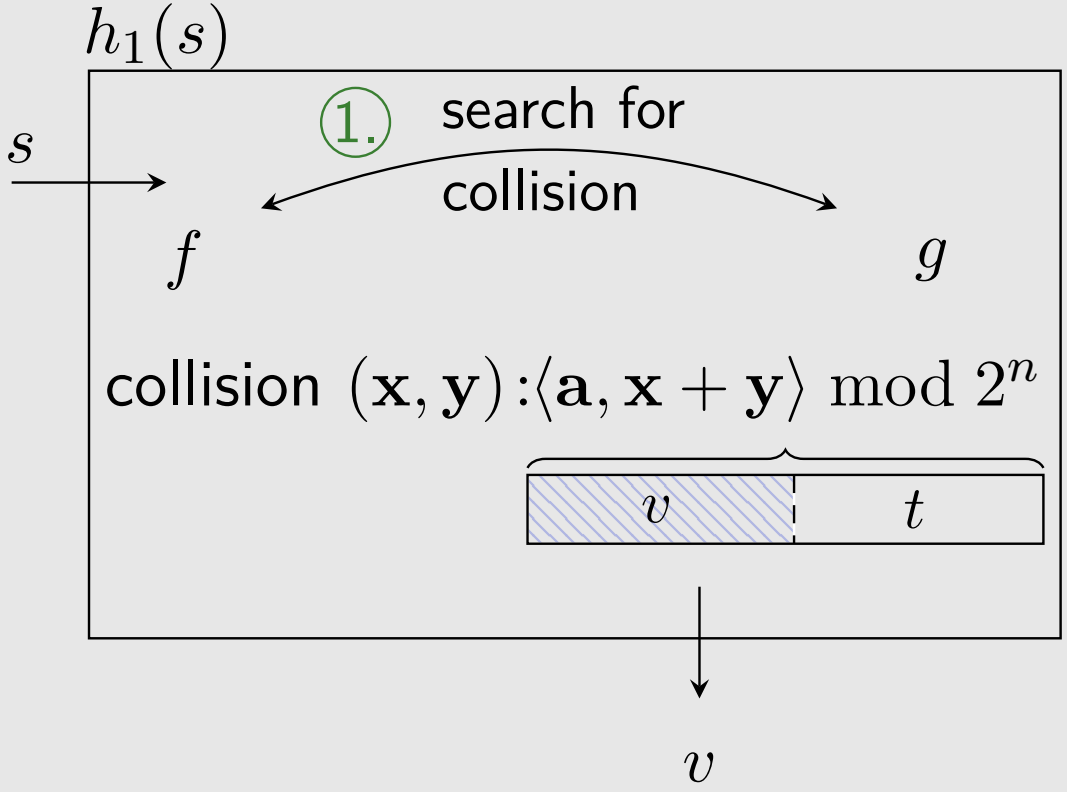
Achieving the Square-Root Bound

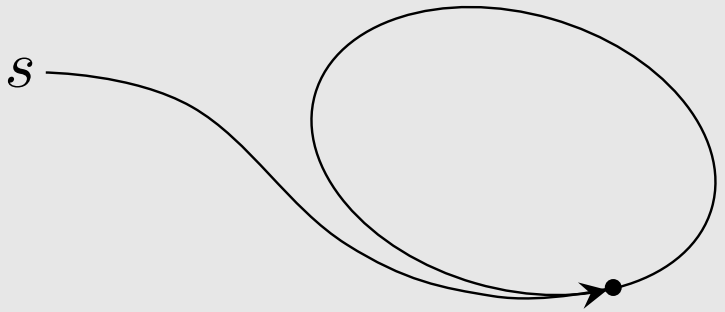


Back to Subset Sum

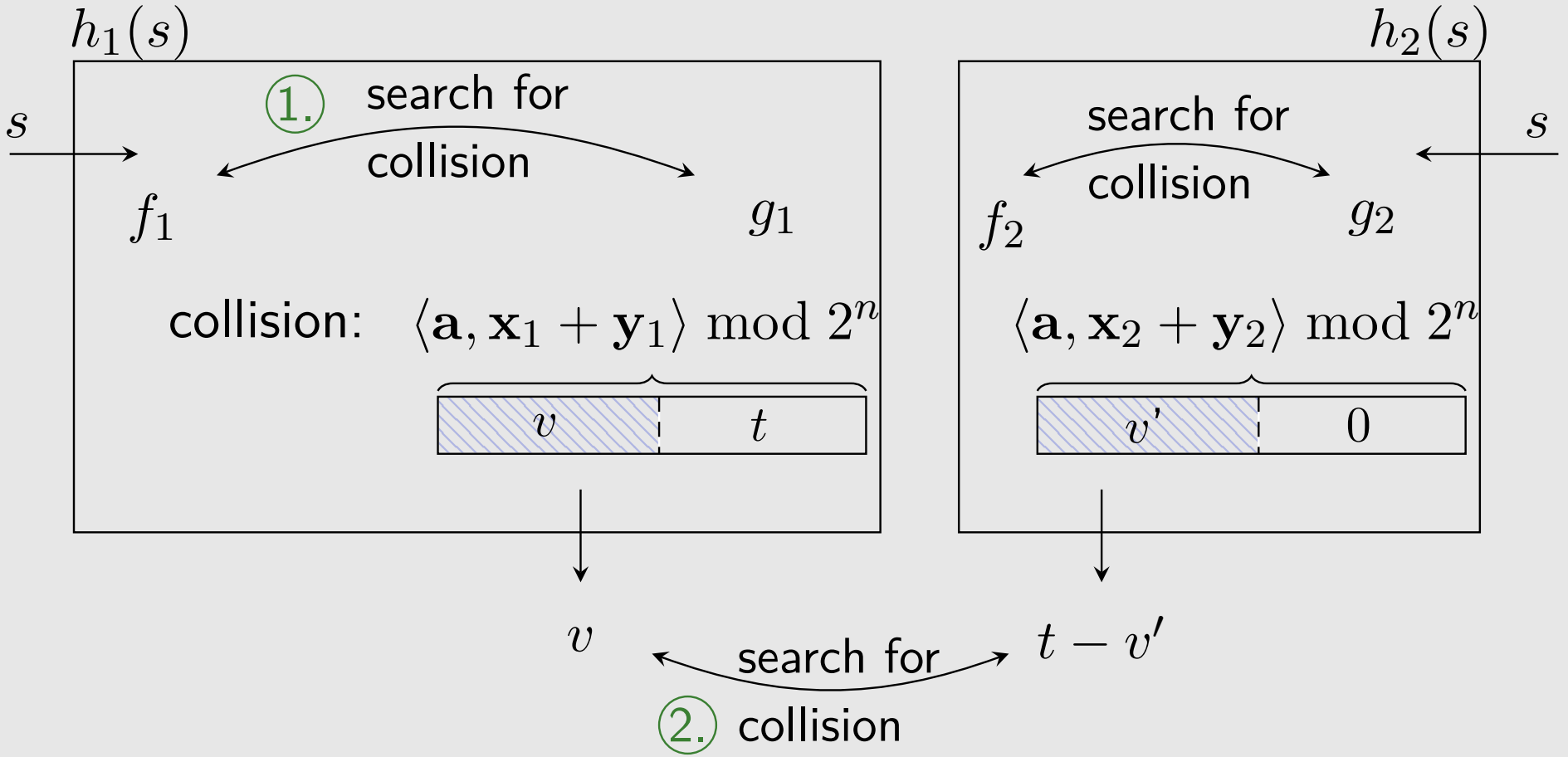


Back to Subset Sum





Back to Subset Sum

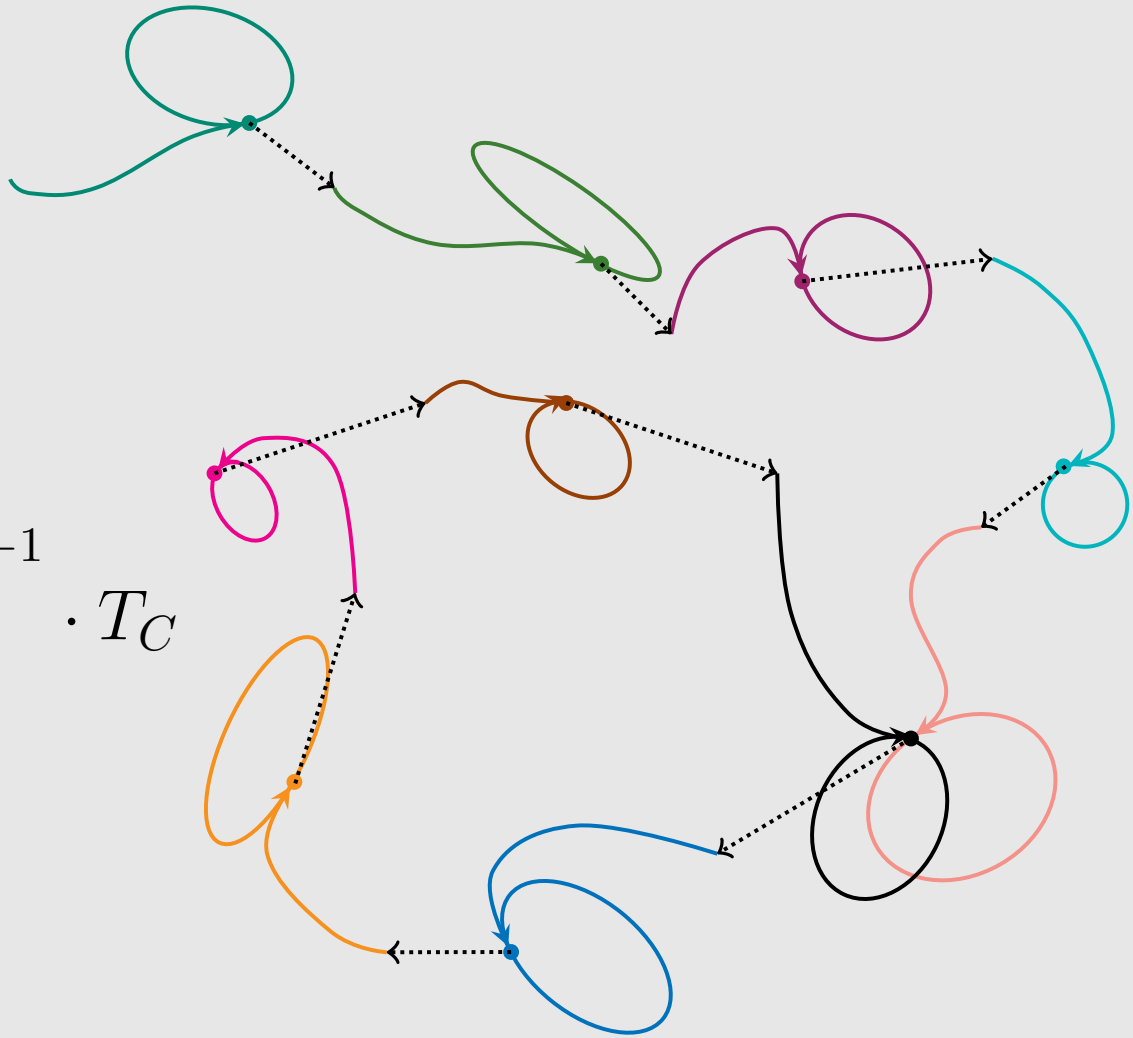


$$\text{coll.} \Rightarrow \langle \mathbf{a}, \mathbf{x}_1 + \mathbf{y}_1 + \mathbf{x}_2 + \mathbf{y}_2 \rangle = t \bmod 2^n$$

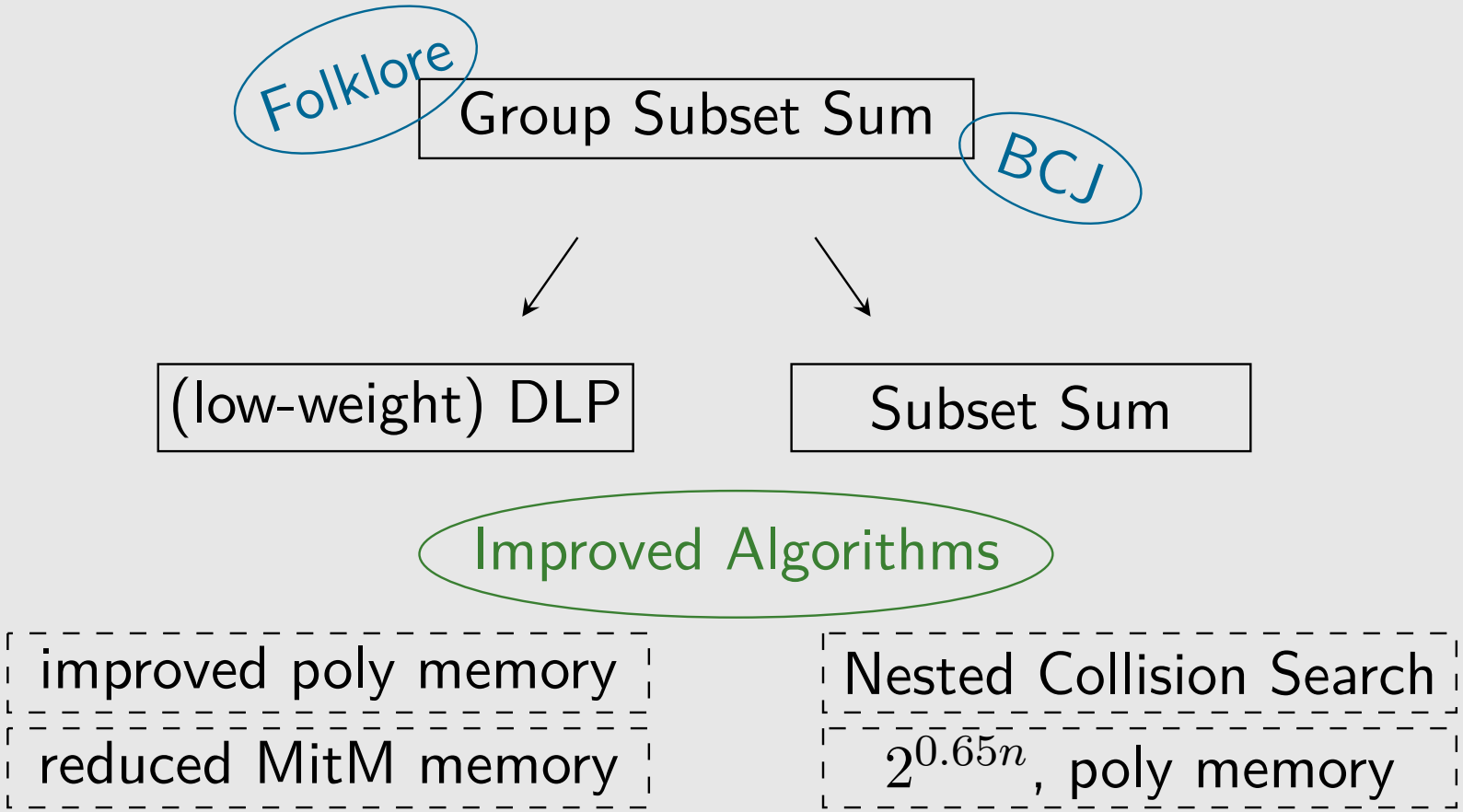
Nested Rhos

$$T = \left(\frac{\#\text{good Colls}}{\#\text{all Colls}}\right)^{-1} \cdot T_C$$

$$= 2^{0.65n}$$



Results


Folklore
Group Subset Sum
BCJ
(low-weight) DLP
Subset Sum
Improved Algorithms
improved poly memory
reduced MitM memory
Nested Collision Search
$2^{0.65n}$, poly memory