New Time-Memory Trade-Offs for Subset Sum – Improving ISD in Theory and Practice

Andre Esser[1] Floyd Zweydinger[2]

27 April 2023

[1] Technology Innovation Institute, UAE

[2] Ruhr University Bochum, Germany

Results

- Unifying the Landscape of Time-Memory Trade-Offs for Subset Sum
- Translates to Information-Set-Decoding for Code-based crypto
- Implementation and new record computations
- From this new estimates for code based cryptography

Preliminaries

Random Subset Sum Problem

Given: $(\mathbf{a}, t = \sum_{i=1}^{n} \mathbf{a}_i \cdot \mathbf{e}_i)$, with $\mathbf{a} := (a_1, \ldots, a_n) \in \mathbb{Z}_{2^n}^n$, $\mathbf{e} \in \{0,1\}^n$, $\mathrm{wt}(\mathbf{e}) = \frac{n}{2}$

Find: $\mathbf{e} \in \{0,1\}^n$

- Cryptographic Application: Hard problem for post-quantum cryptography
- Algorithmic tool used in Cryptanalysis
- Best attacks on McEliece/BIKE/HQC use a lot of memory

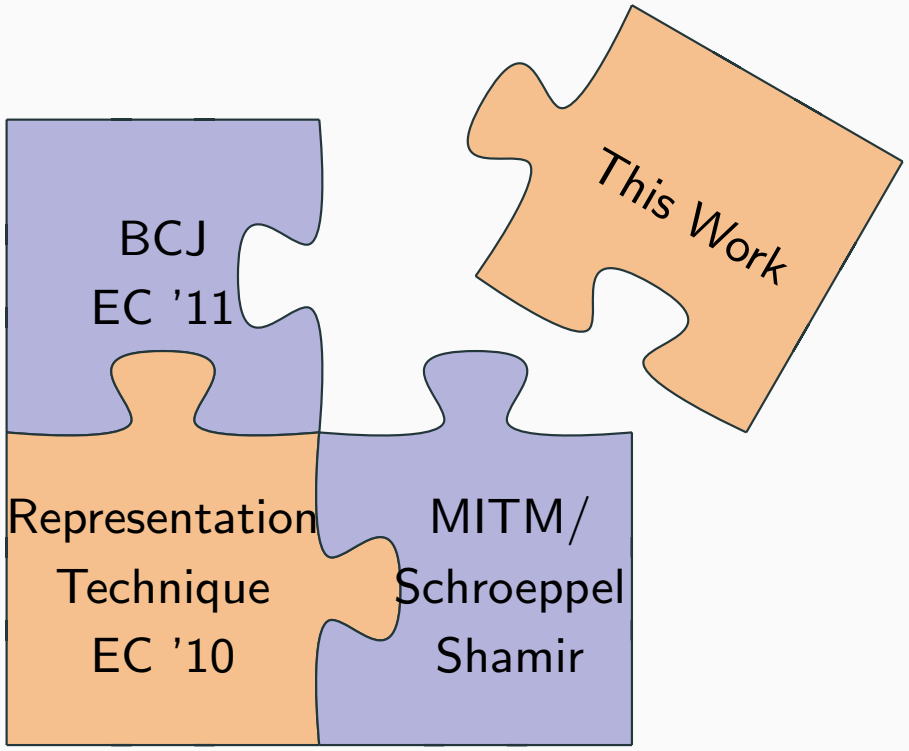
Preliminaries

Random Subset Sum Problem

Given: $(\mathbf{a}, t = \sum_{i=1}^{n} \mathbf{a}_i \cdot \mathbf{e}_i)$, with $\mathbf{a} := (a_1, \ldots, a_n) \in \mathbb{Z}_{2^n}^n$, $\mathbf{e} \in \{0,1\}^n$, $\mathrm{wt}(\mathbf{e}) = \frac{n}{2}$

Find: $\mathbf{e} \in \{0,1\}^n$

- Cryptographic Application: Hard problem for post-quantum cryptography
- Algorithmic tool used in Cryptanalysis
- Best attacks on McEliece/BIKE/HQC use a lot of memory



Meet in the Middle (Horowitz, Sahni JACM '74)

$$t = \sum_{i=1}^{n} a_i x_i \qquad \text{mod } 2^n$$

$$t = \sum_{i=1}^{n/2} a_i x_i + \sum_{i=n/2+1}^{n} a_i x_i \qquad \text{mod } 2^n$$

Meet in the Middle (Horowitz, Sahni JACM '74)

$$t = \sum_{i=1}^{n} a_i x_i \qquad \text{mod } 2^n$$

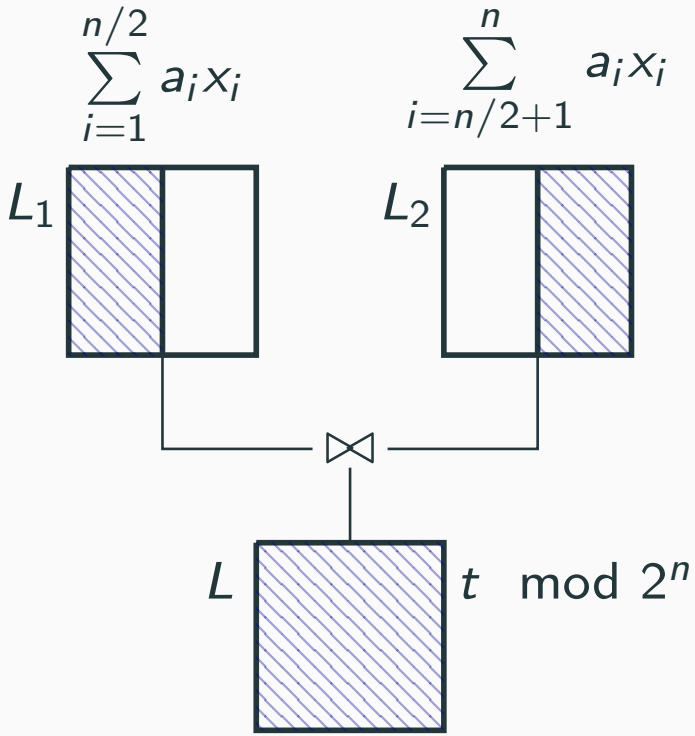
$$t = \sum_{i=1}^{n/2} a_i x_i + \sum_{i=n/2+1}^{n} a_i x_i \qquad \text{mod } 2^n$$

$$\sum_{i=1}^{n/2} a_i x_i \qquad \sum_{i=n/2+1}^{n} a_i x_i$$

Meet in the Middle (Horowitz, Sahni JACM '74)

$$t = \sum_{i=1}^{n} a_i x_i \mod 2^n$$

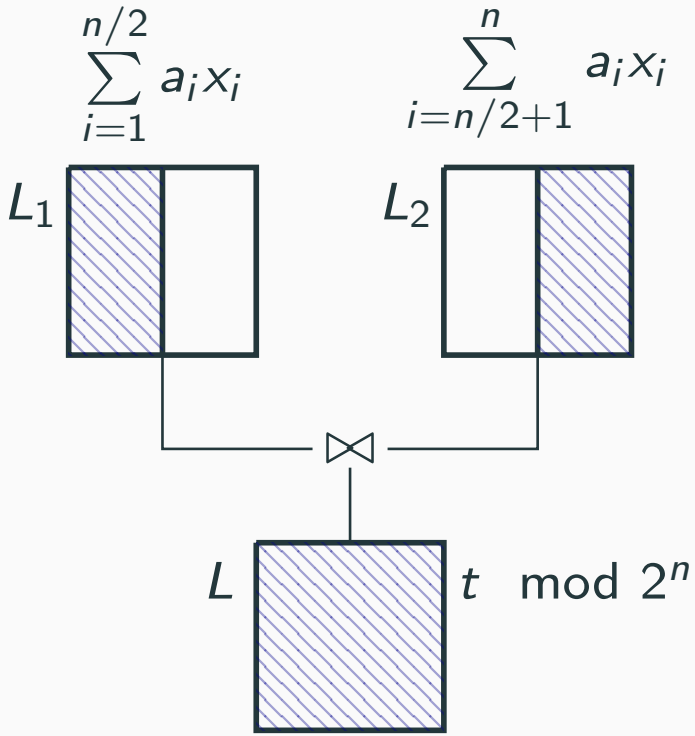
$$t = \sum_{i=1}^{n/2} a_i x_i + \sum_{i=n/2+1}^{n} a_i x_i \mod 2^n$$



Meet in the Middle (Horowitz, Sahni JACM '74)

$$t = \sum_{i=1}^{n} a_i x_i \mod 2^n$$

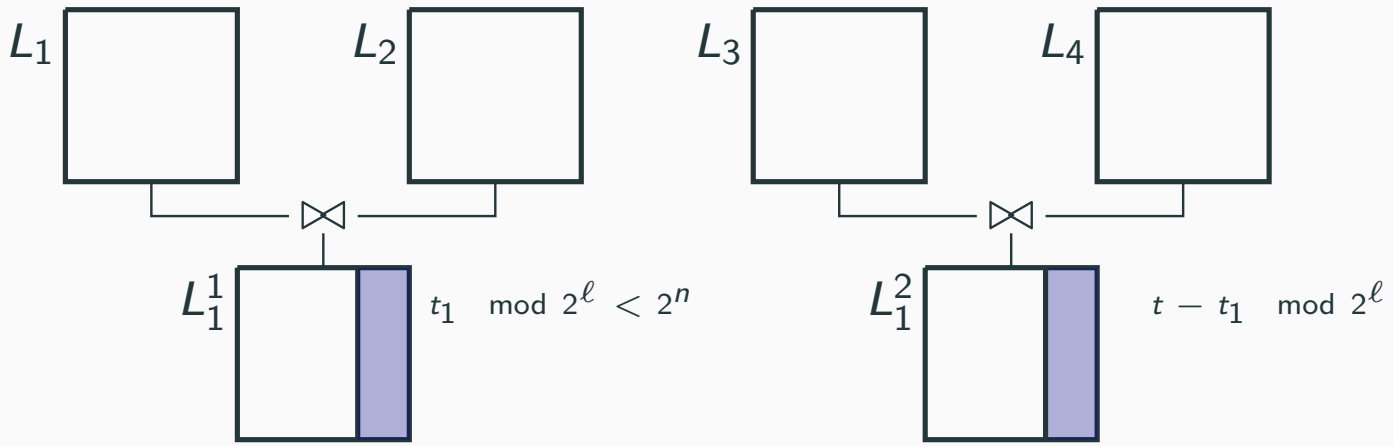
$$t = \sum_{i=1}^{n/2} a_i x_i + \sum_{i=n/2+1}^{n} a_i x_i \mod 2^n$$



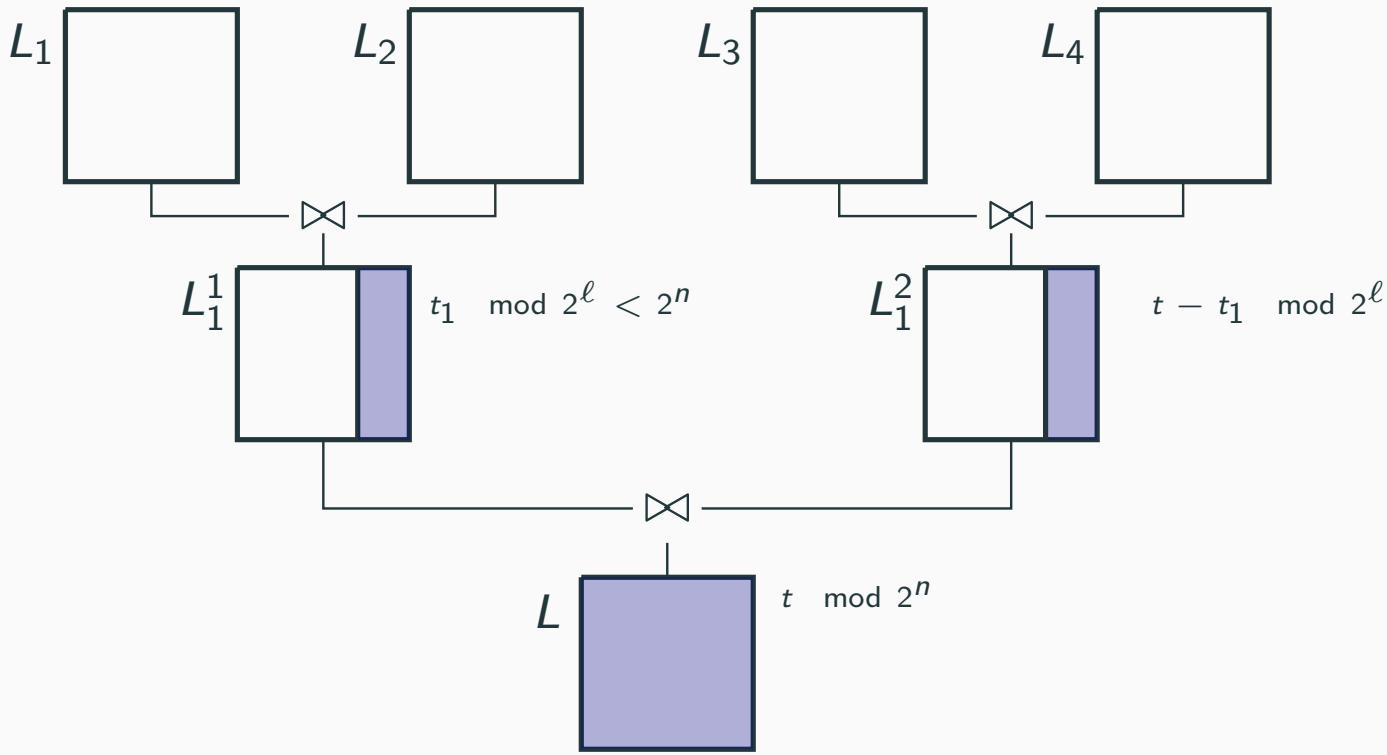
- Time: $\mathcal{O}(2^{\frac{n}{2}})$
- Space: $\mathcal{O}(2^{\frac{n}{2}})$

Shroeppel-Shamir (FOCS '79)

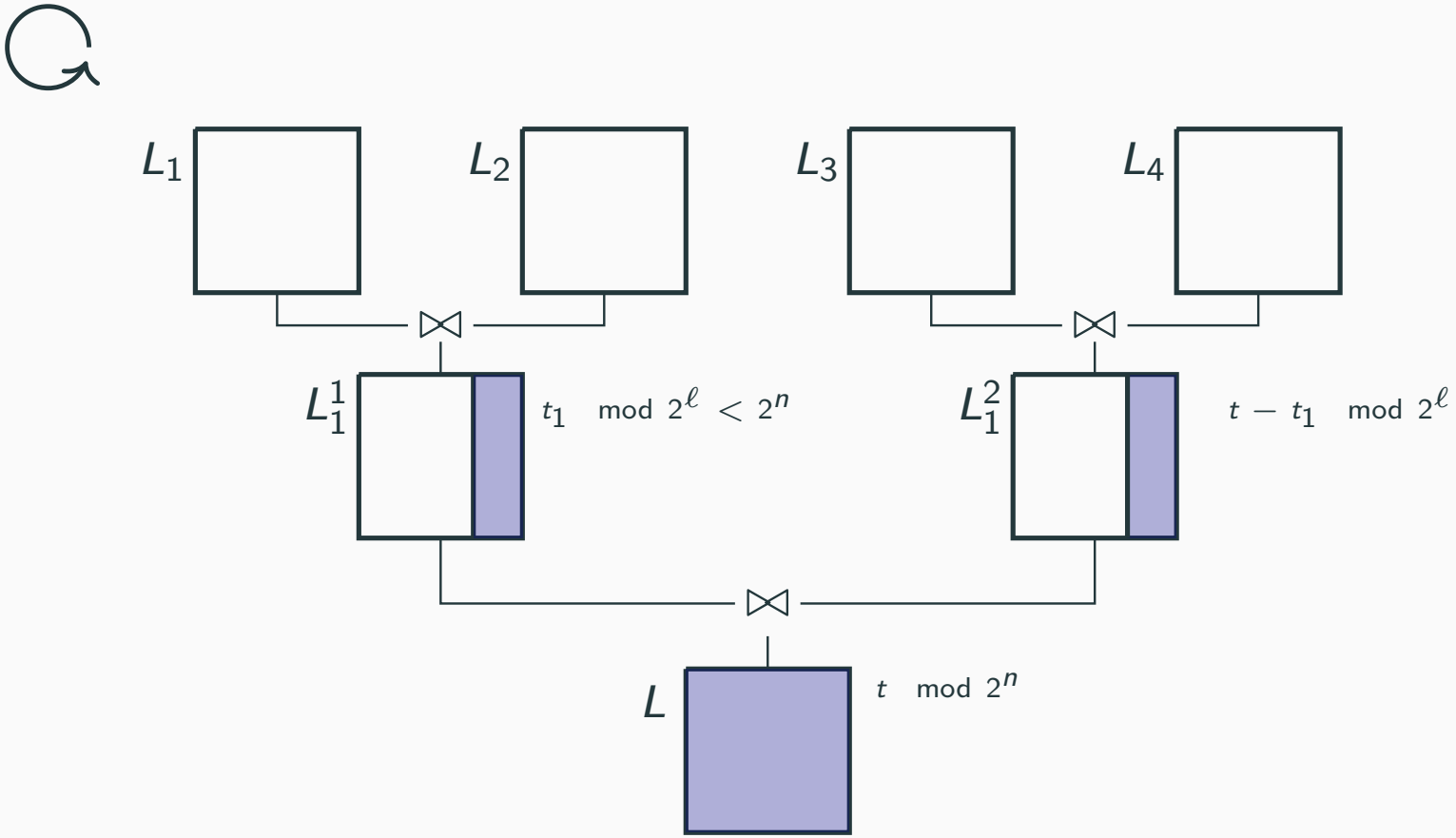
Shroeppel-Shamir (FOCS '79)



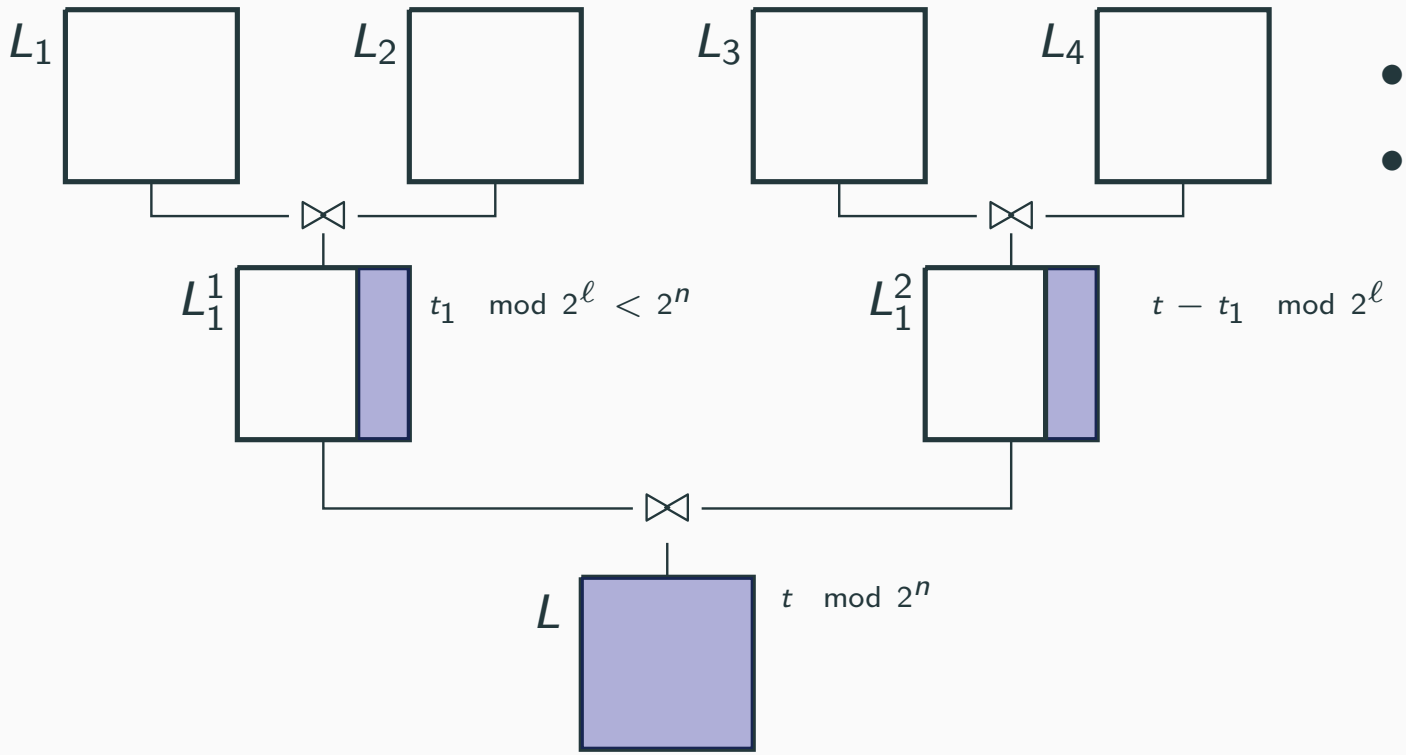
Shroeppel-Shamir (FOCS '79)



Shroeppel-Shamir (FOCS '79)



Shroeppel-Shamir (FOCS '79)



- Time: $\mathcal{O}(2^{\frac{n}{2}})$
- Space: $\mathcal{O}(2^{\frac{n}{4}})$

Representations Technique (Howgrave-Graham Joux EC '10)

Idea:

Blow up the search space while increasing the solution space even more.

Representations Technique (Howgrave-Graham Joux EC '10)

Idea:

Blow up the search space while increasing the solution space even more.

MITM	$\rightarrow$	Representations
$\{0,1\}^{\frac{n}{2}} \times \{0\}^{\frac{n}{2}}$		$\{x \in \{0,1\}^n \mid \mathrm{wt}(x) = \frac{n}{4}\}$

Representations Technique (Howgrave-Graham Joux EC '10)

Idea:

Blow up the search space while increasing the solution space even more.

MITM	$\rightarrow$	Representations
$\{0,1\}^{\frac{n}{2}} \times \{0\}^{\frac{n}{2}}$		$\{x \in \{0,1\}^n \mid \mathrm{wt}(x) = \frac{n}{4}\}$

Example: 10110010:

10100000	10010000	10000010	00110000	00100010	00010010
+	+	+	+	+	+
00010010	00100010	00110000	10000010	10010000	10100000

Representations Technique (Howgrave-Graham Joux EC '10)

Idea:

Blow up the search space while increasing the solution space even more.

MITM	$\rightarrow$	Representations
$\{0,1\}^{\frac{n}{2}} \times \{0\}^{\frac{n}{2}}$		$\{x \in \{0,1\}^n \mid \mathrm{wt}(x) = \frac{n}{4}\}$

Example: 10110010:

10100000	10010000	10000010	00110000	00100010	00010010
+	+	+	+	+	+
00010010	00100010	00110000	10000010	10010000	10100000

	MitM	Representations
Size	$2^{n/2}$	$\binom{n}{n/4} = 2^{0.81n}$

Representations Technique (Howgrave-Graham Joux EC '10)

Idea:

Blow up the search space while increasing the solution space even more.

MITM	$\rightarrow$	Representations
$\{0,1\}^{\frac{n}{2}} \times \{0\}^{\frac{n}{2}}$		$\{x \in \{0,1\}^n \mid \mathrm{wt}(x) = \frac{n}{4}\}$

Example: 10110010:

$$\begin{array}{cccccc} 10100000 & 10010000 & 10000010 & 00110000 & 00100010 & 00010010 \\ + & + & + & + & + & + \\ 00010010 & 00100010 & 00110000 & 10000010 & 10010000 & 10100000 \end{array}$$

	MitM	Representations
Size	$2^{n/2}$	$\binom{n}{n/4} = 2^{0.81n}$
$\mathbb{E}$(solutions)	1	$\binom{n/2}{n/4} = 2^{n/2}$

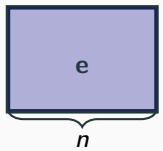
BCJ (Becker-Coron-Joux EC '11)

Problem:

How to examine a $2^{-n/2}$ fraction of the search space?

Level

0



BCJ (Becker-Coron-Joux EC '11)

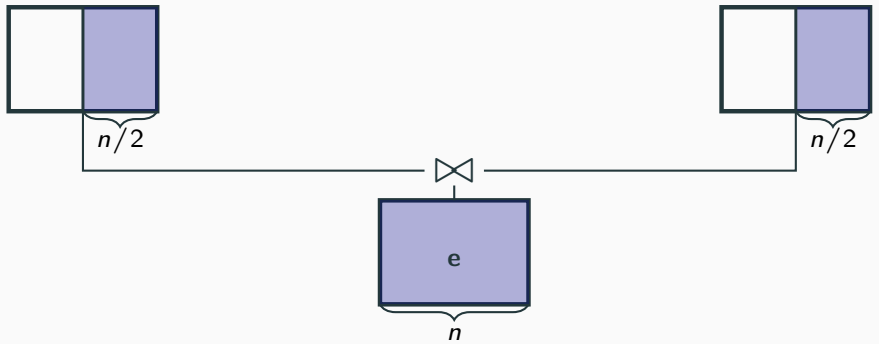
Problem:

How to examine a $2^{-n/2}$ fraction of the search space?

Level

1

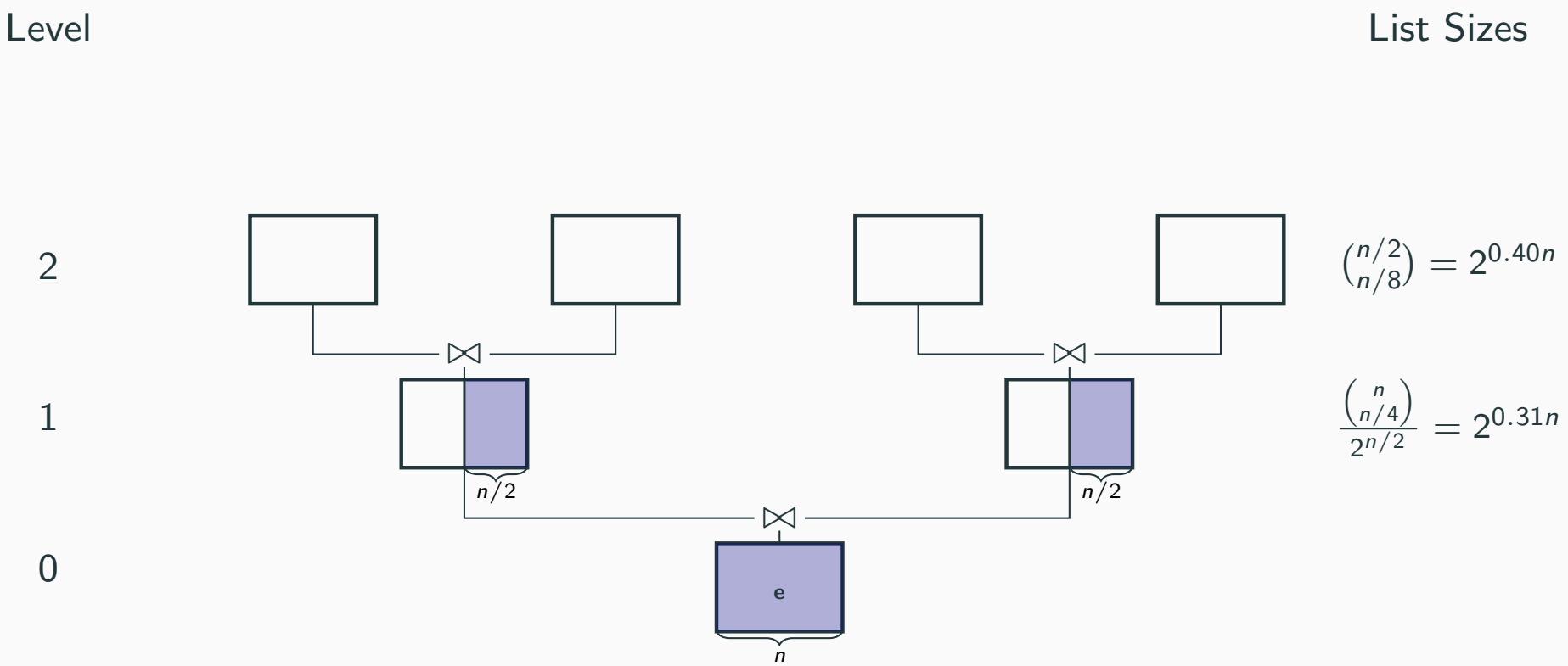
0



BCJ (Becker-Coron-Joux EC '11)

Problem:

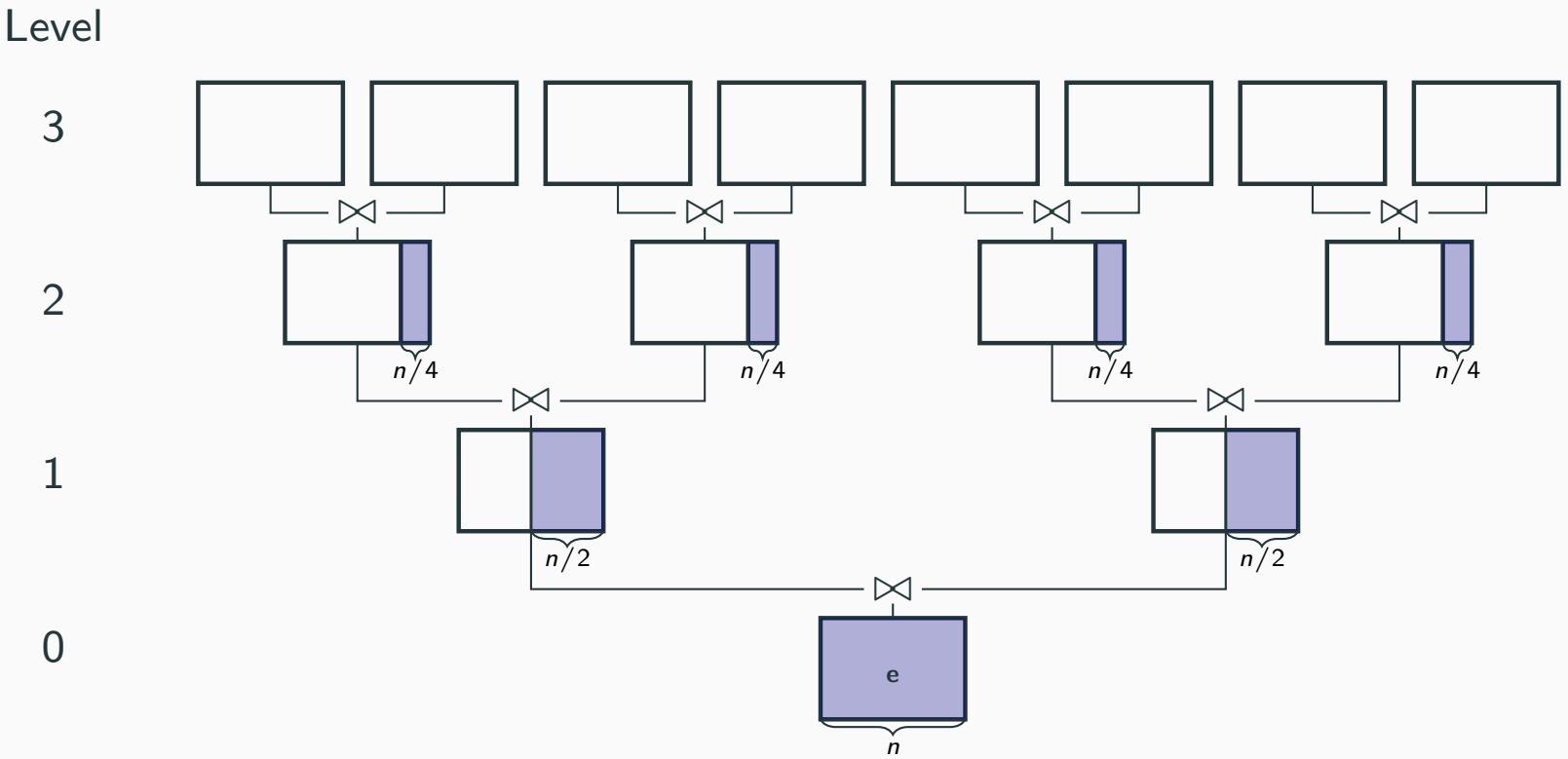
How to examine a $2^{-n/2}$ fraction of the search space?



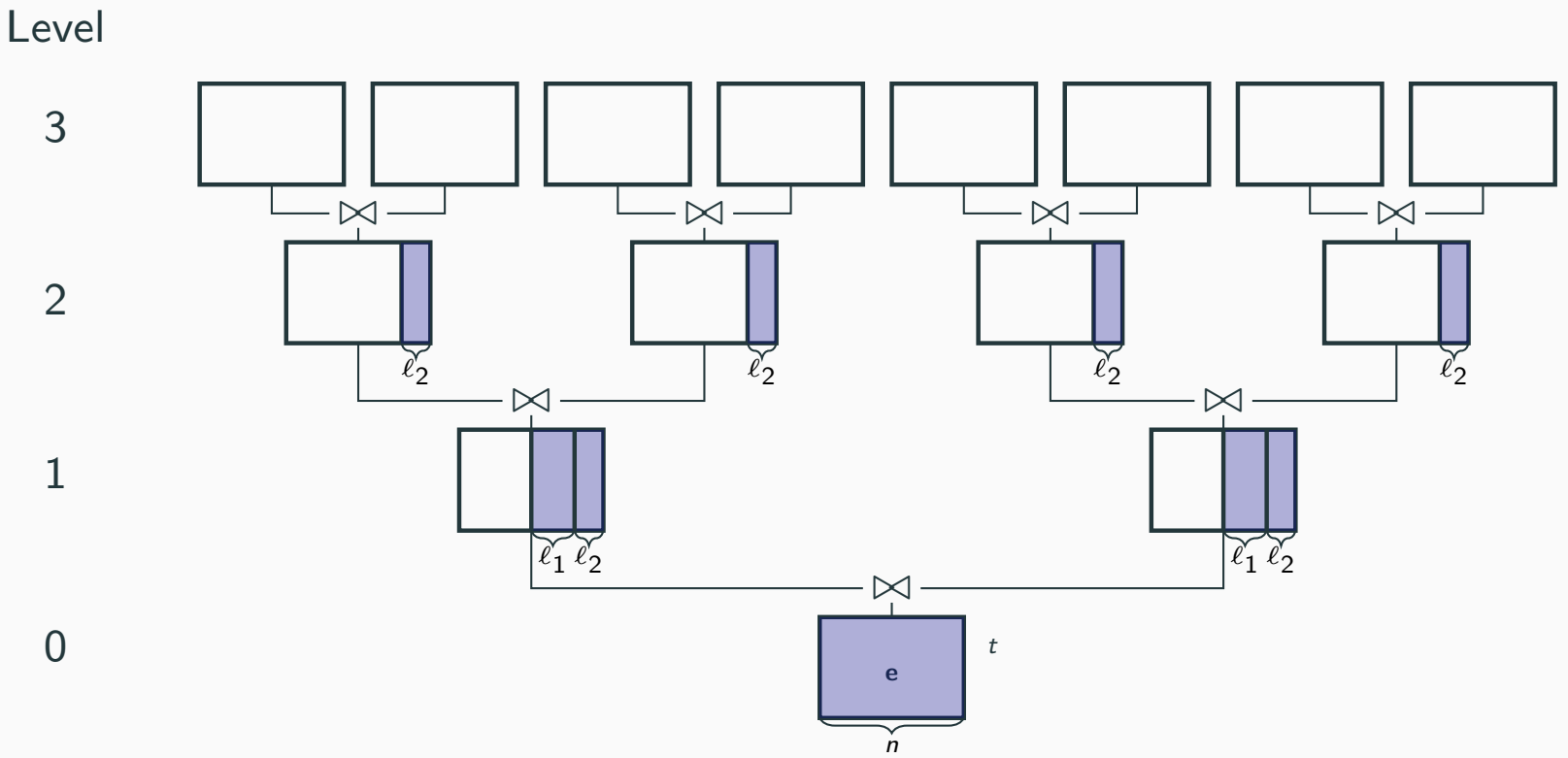
BCJ (Becker-Coron-Joux EC '11)

Problem:

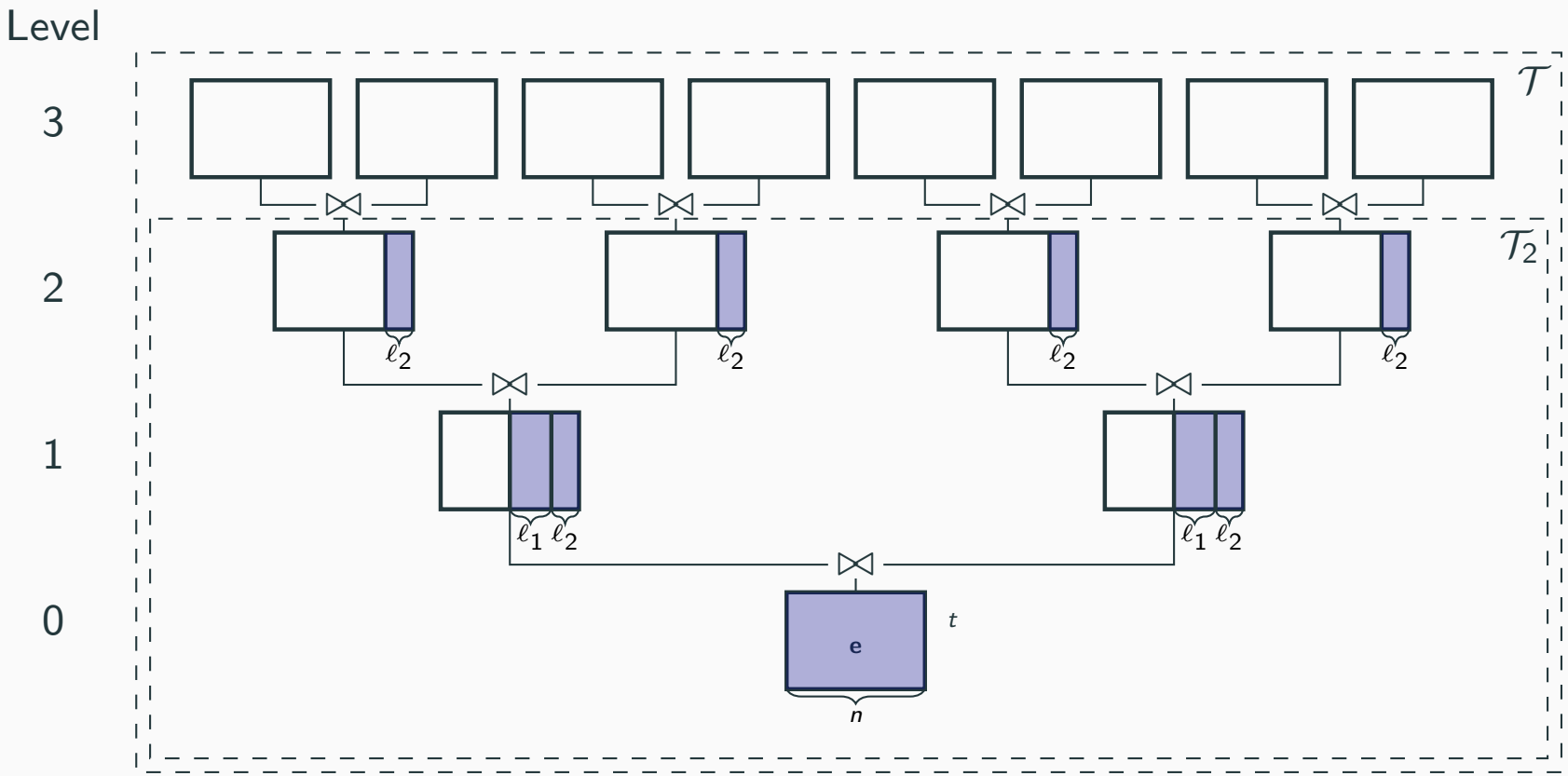
How to examine a $2^{-n/2}$ fraction of the search space?



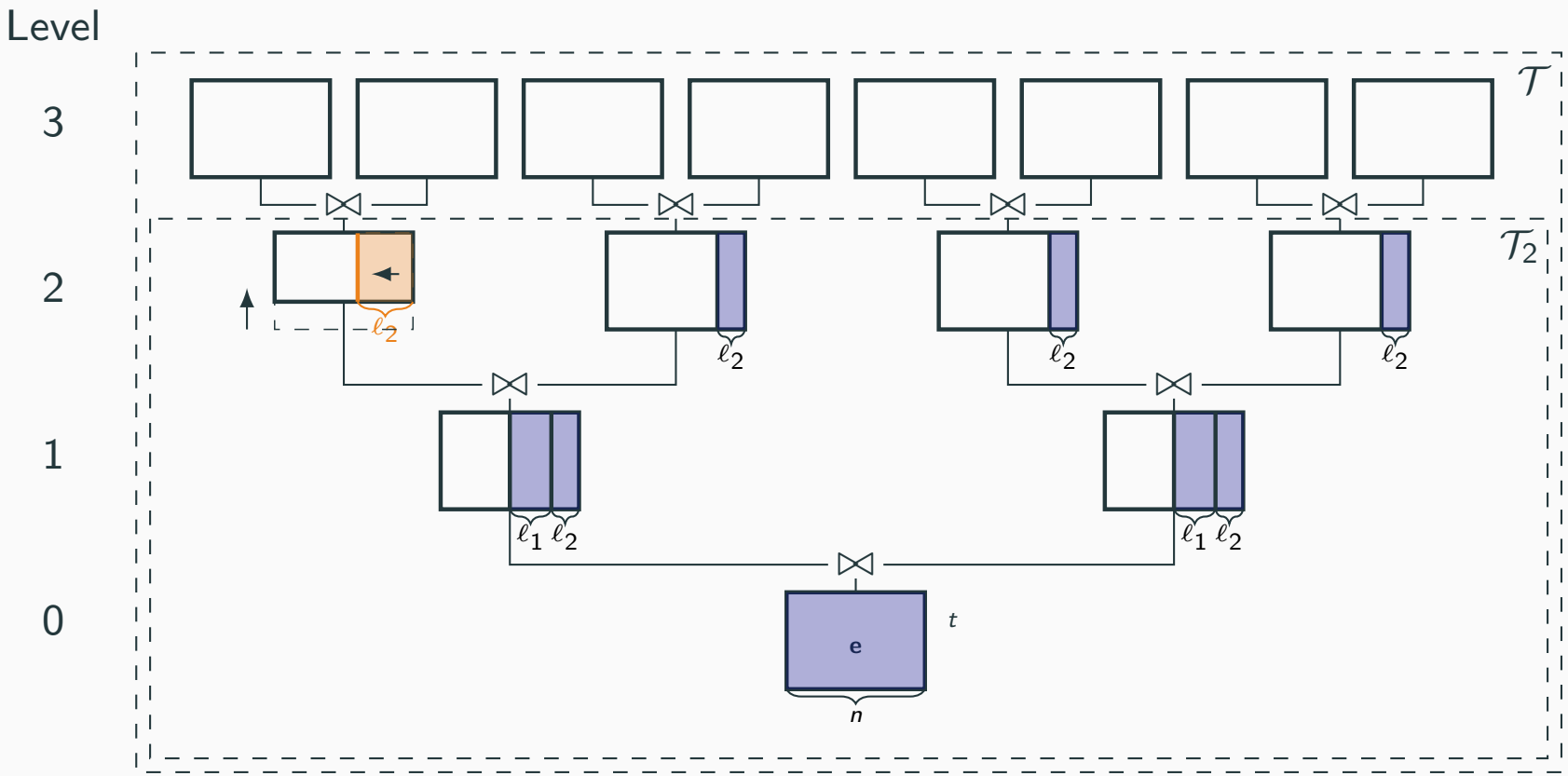
Contribution: New Time-Memory Trade-Off



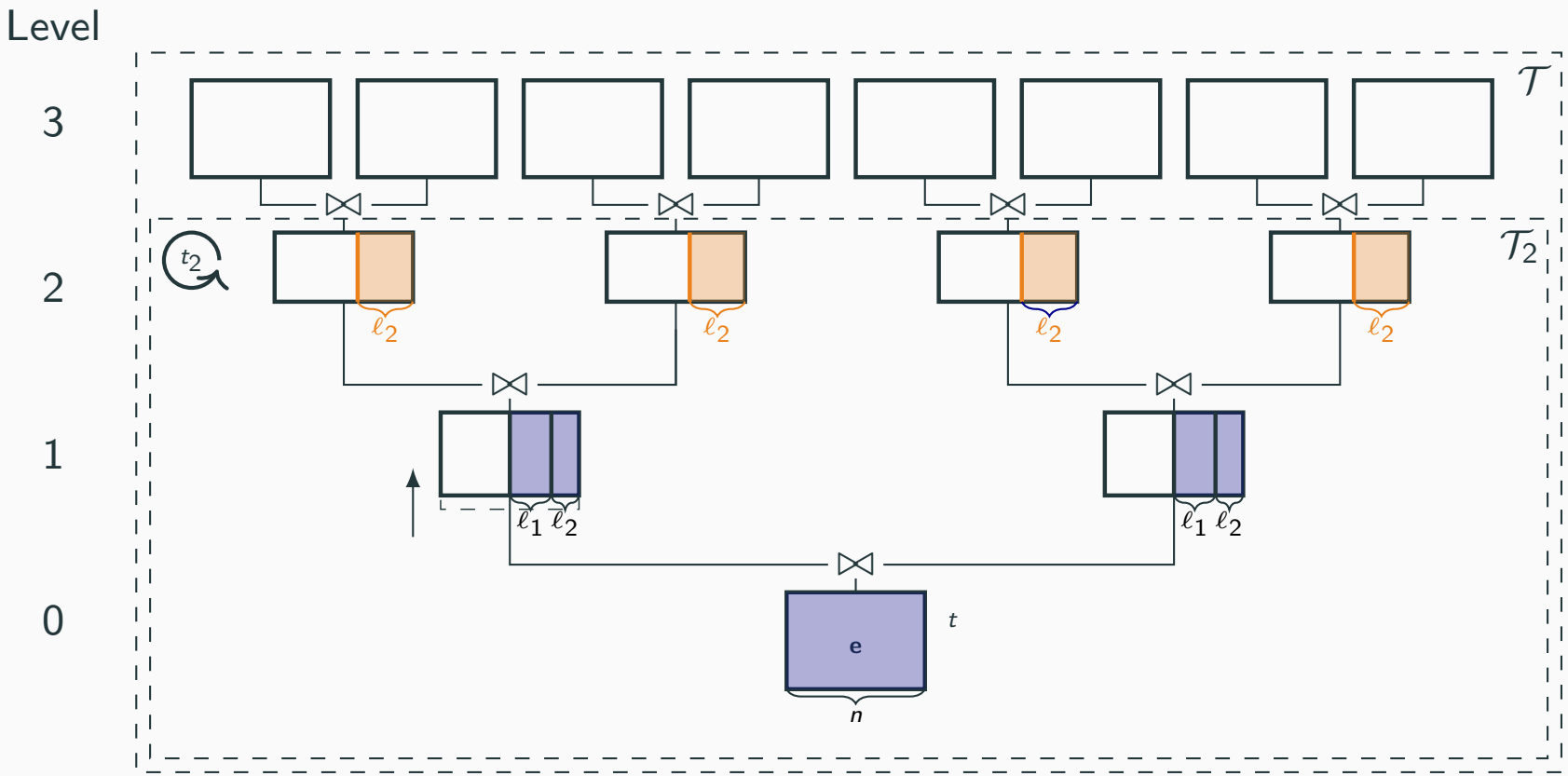
Contribution: New Time-Memory Trade-Off



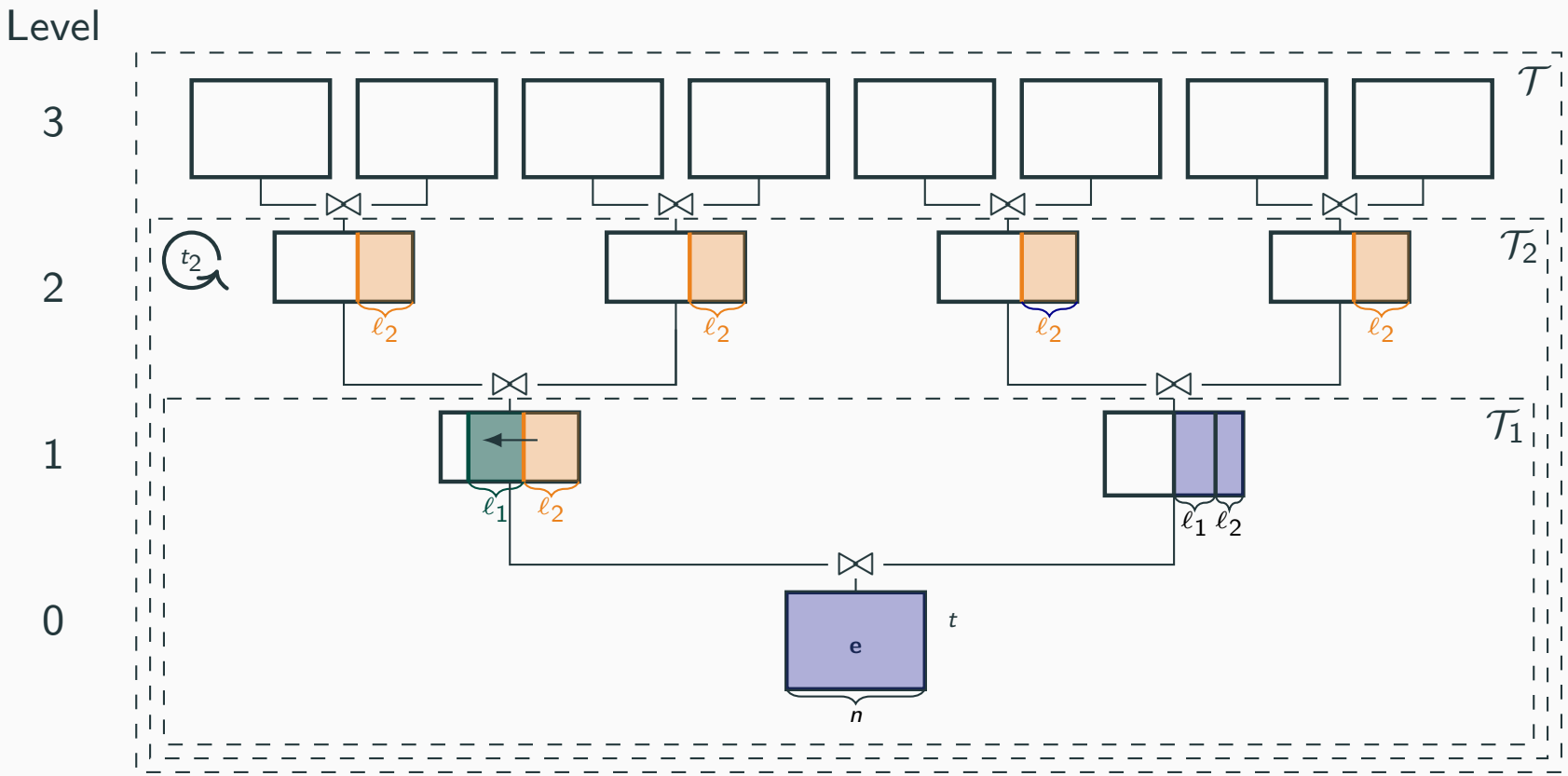
Contribution: New Time-Memory Trade-Off



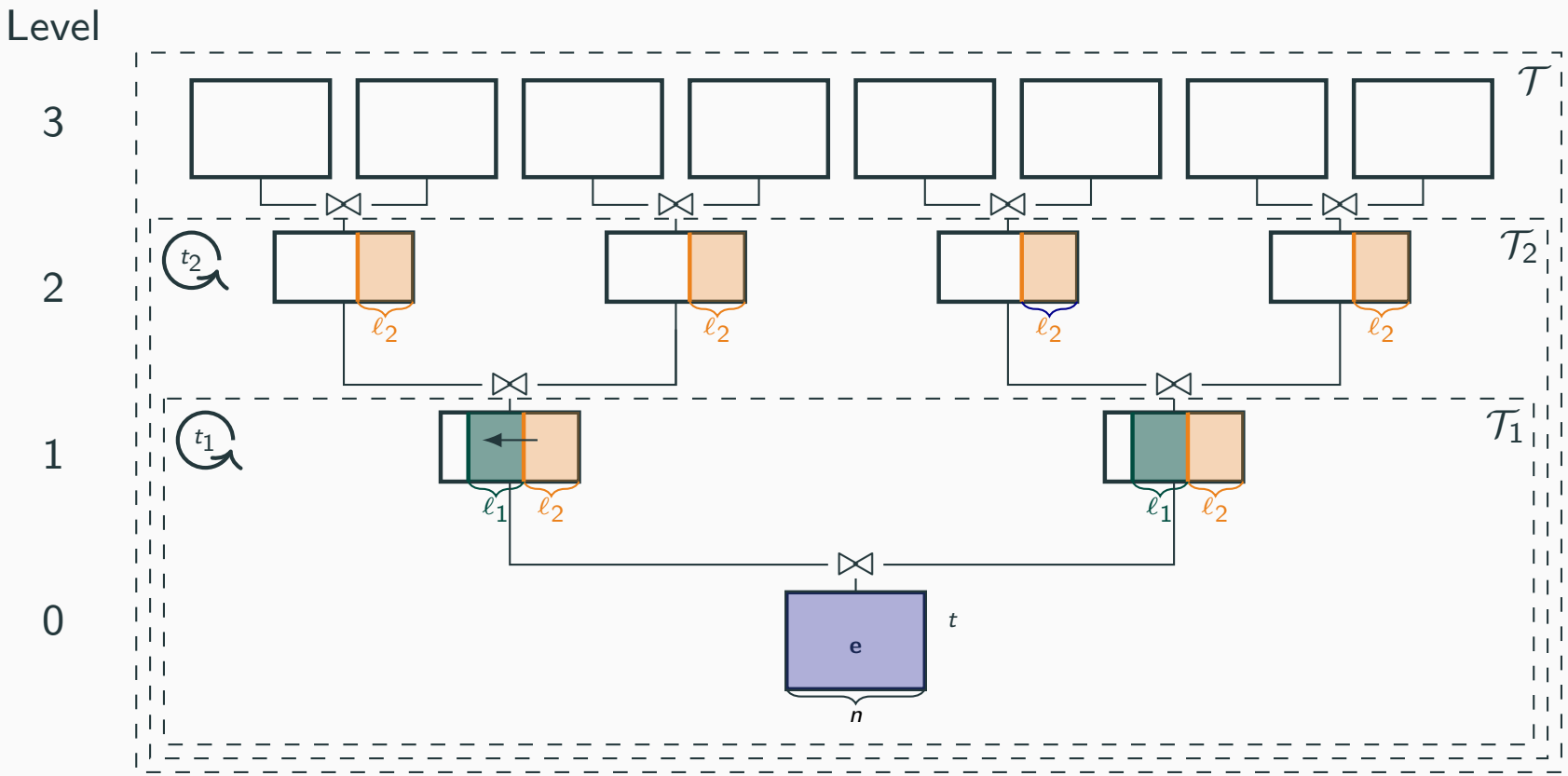
Contribution: New Time-Memory Trade-Off



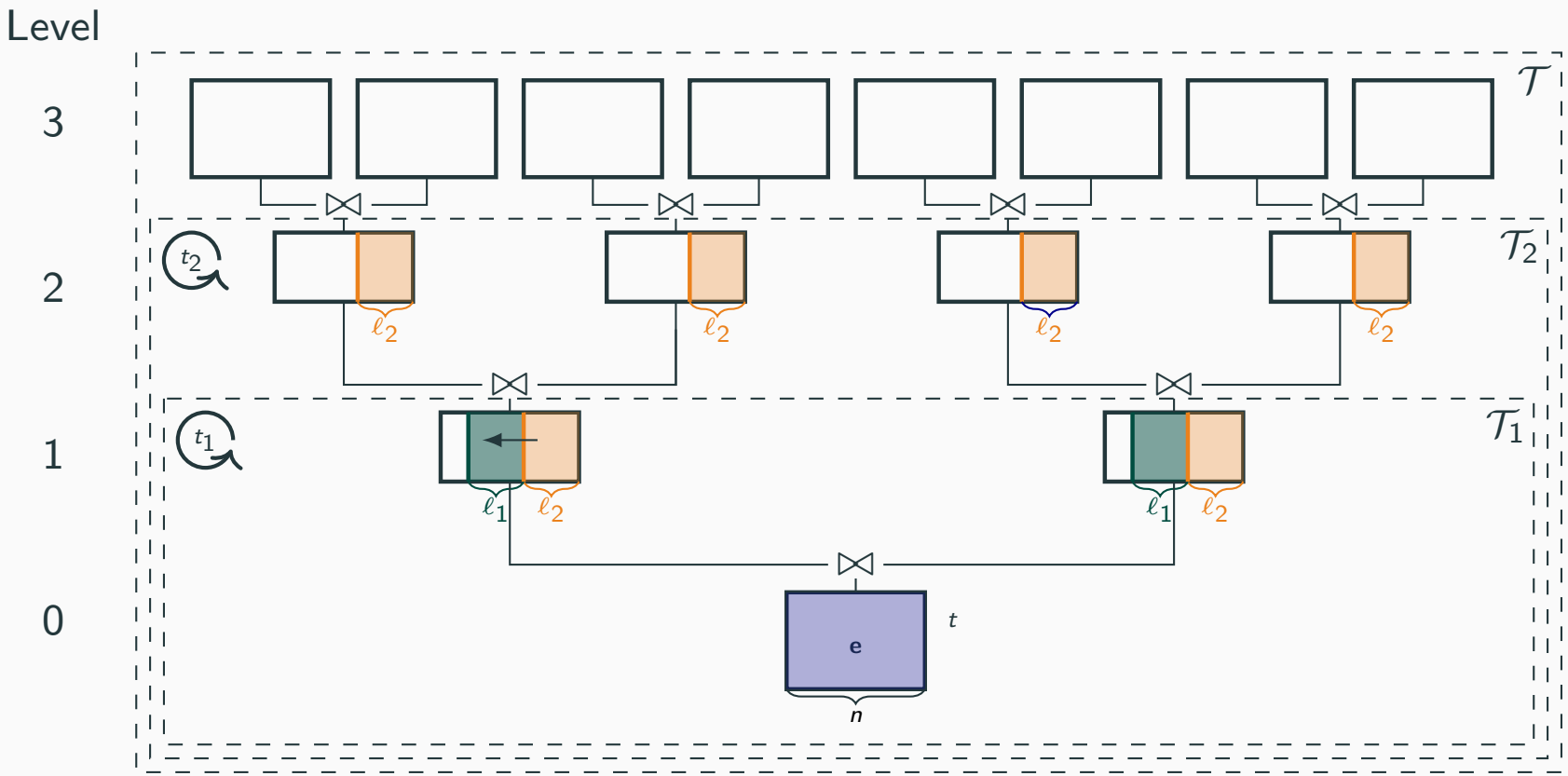
Contribution: New Time-Memory Trade-Off



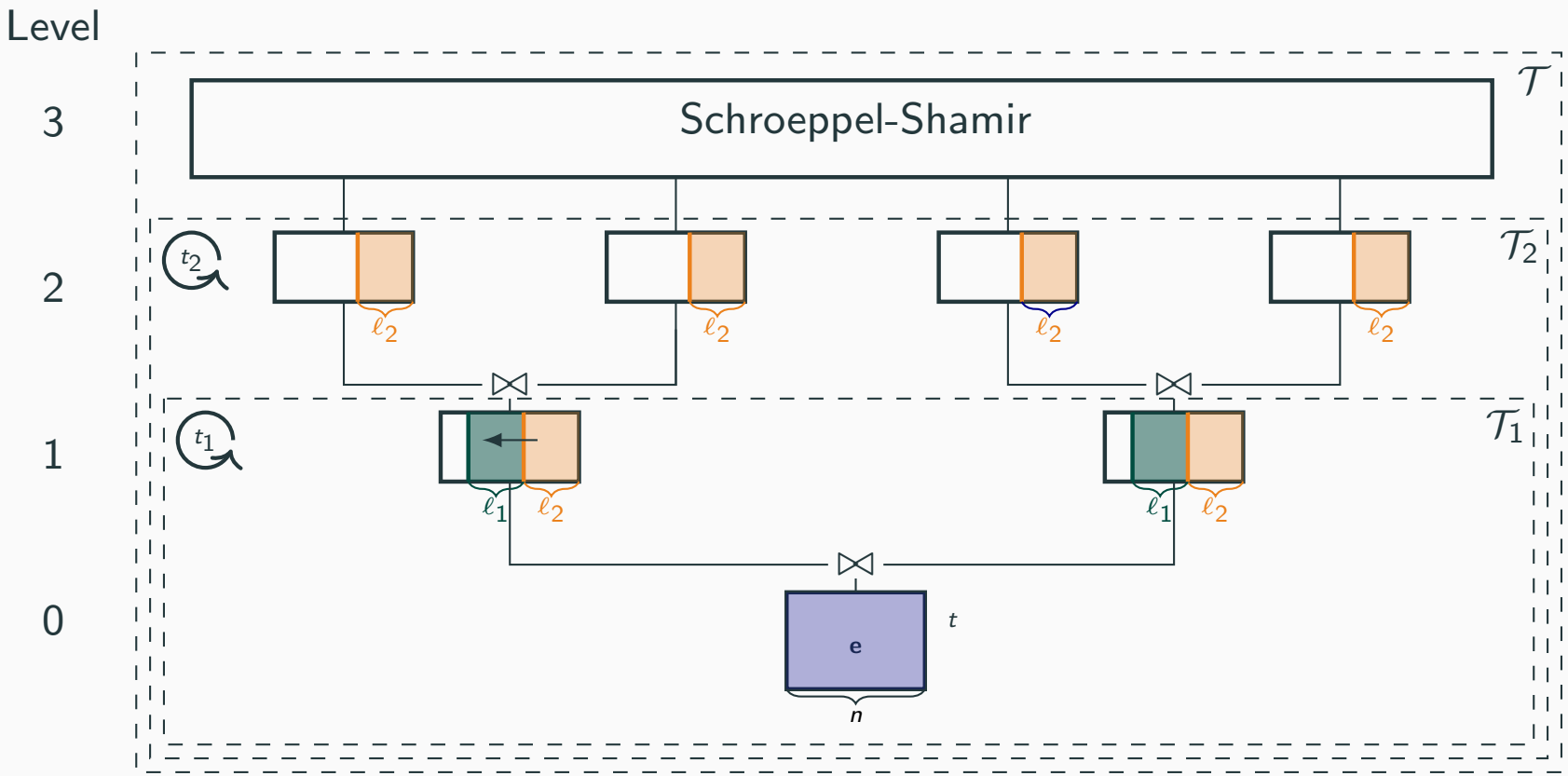
Contribution: New Time-Memory Trade-Off



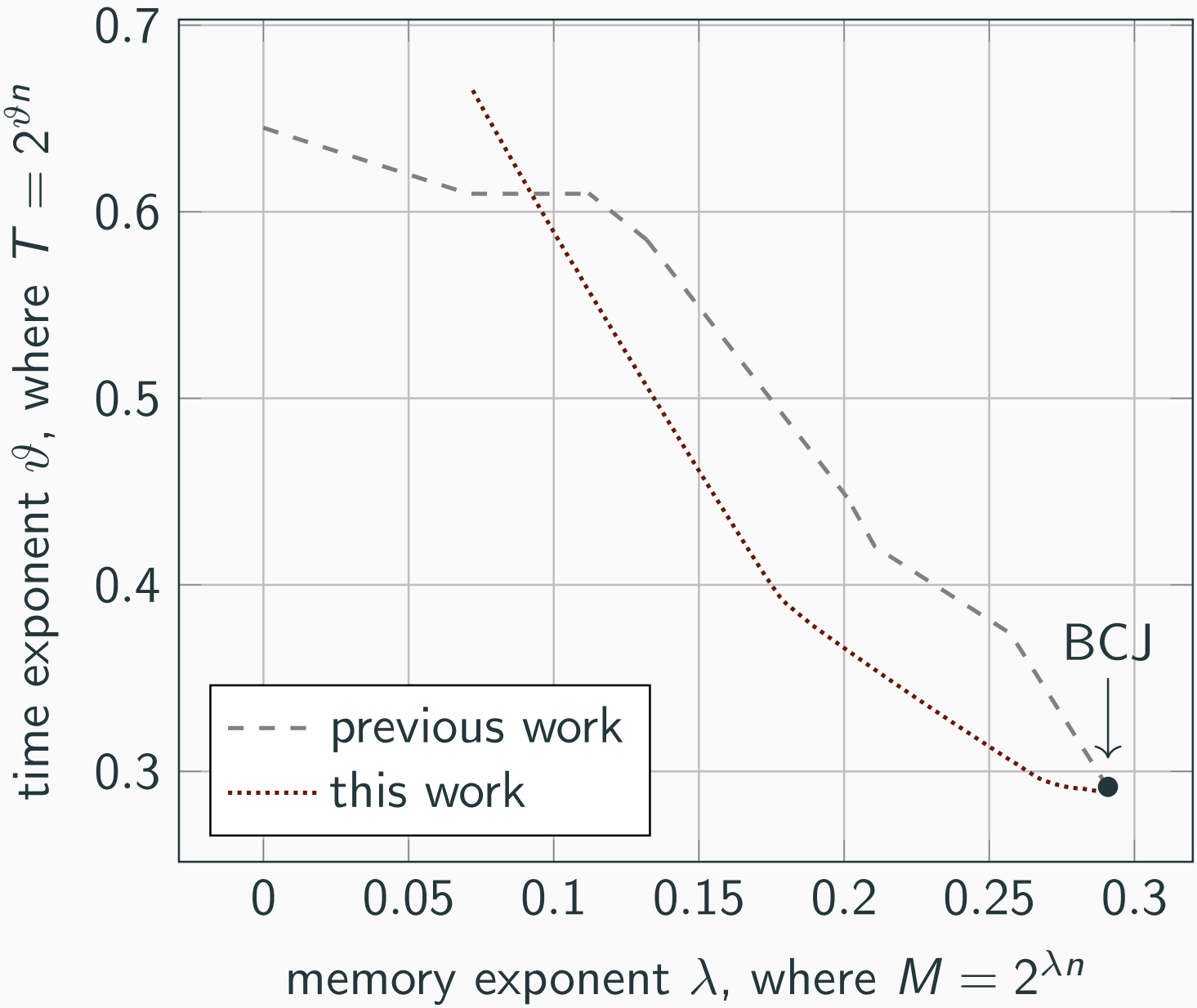
Contribution: New Time-Memory Trade-Off



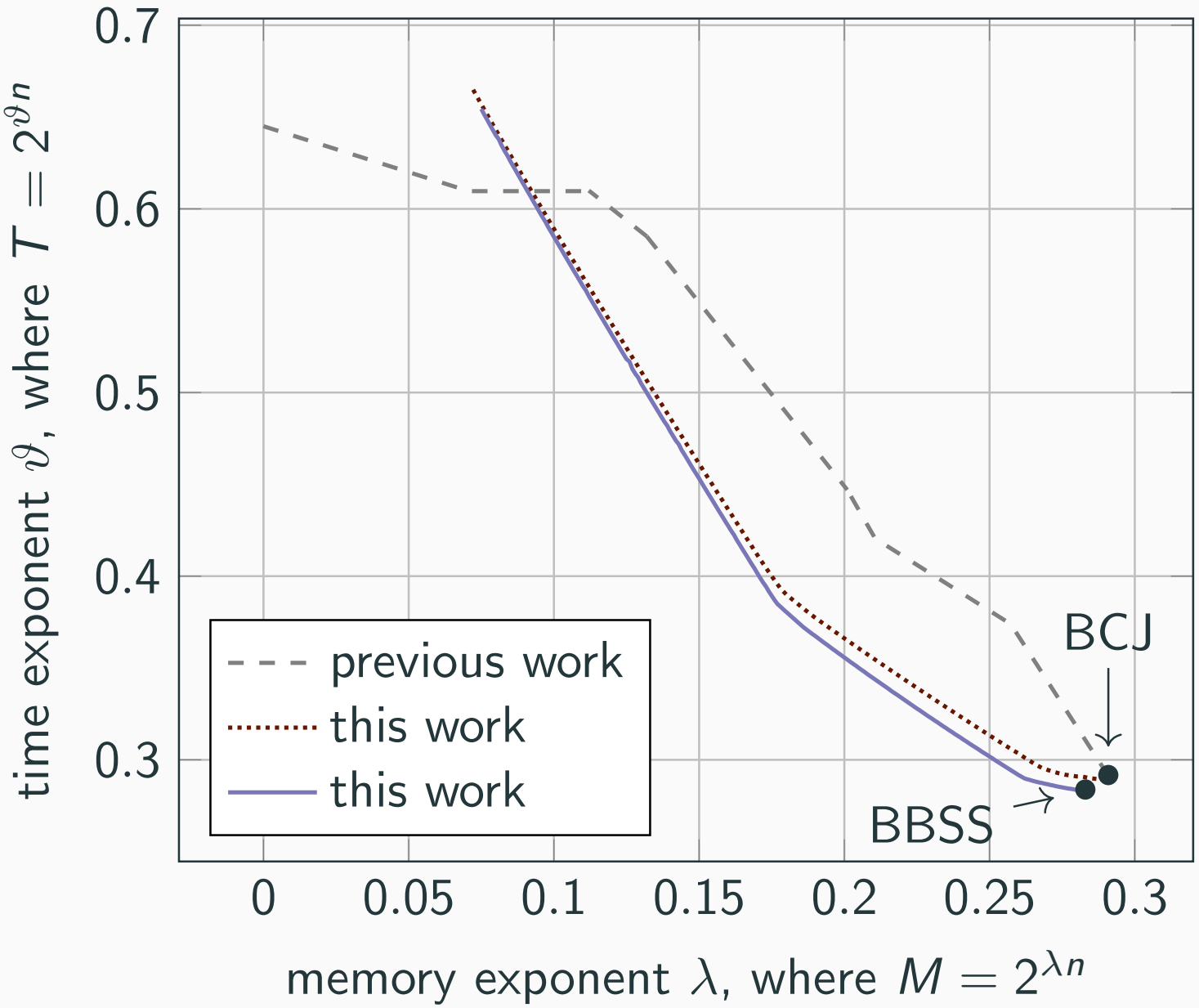
Contribution: New Time-Memory Trade-Off



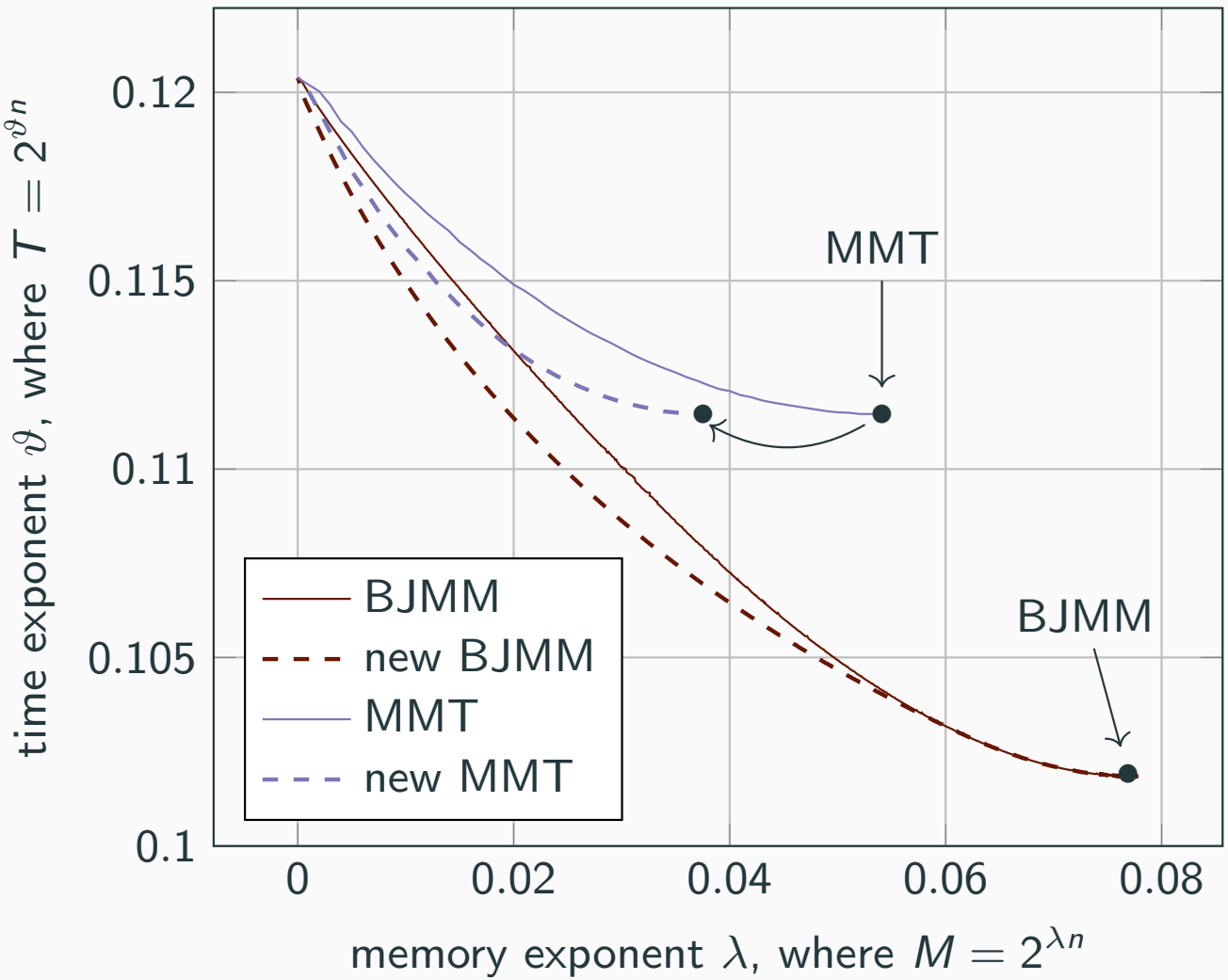
Results: Subset Sum



Results: Subset Sum



Results: Decoding



Estimating Security

		Cat. I AES-128	Cat. III AES-192	Cat. Va AES-256	Cat. Vb AES-256	Cat. Vc AES-256
McEliece	unlimited	1	1	1	1	1
	$M \leq 2^{80}$	1	2	2	2	1
	$M \leq 2^{60}$	2	1	5	5	6
BIKE	unlimited	3	3	3	-	-
HQC	unlimited	3	3	3	-	-

Conclusion

- Significant Speedups in the restricted memory regime $M \geq 2^{0.091n}$
- Unified Time-Memory Trade-Offs landscape for Subset Sum
- First non-trivial Time-Memory Trade-Offs for ISD

Conclusion

- Significant Speedups in the restricted memory regime $M \geq 2^{0.091n}$
- Unified Time-Memory Trade-Offs landscape for Subset Sum
- First non-trivial Time-Memory Trade-Offs for ISD

Thank You!

`https://eprint.iacr.org/2022/1329`

`https://github.com/FloydZ/decoding`