

# *Ligetron: Design and Deployment of ZK Applications Made Easy.*

Muthu Venkitasubramaniam

Co-founder, Ligero Inc.

Professor, Georgetown University

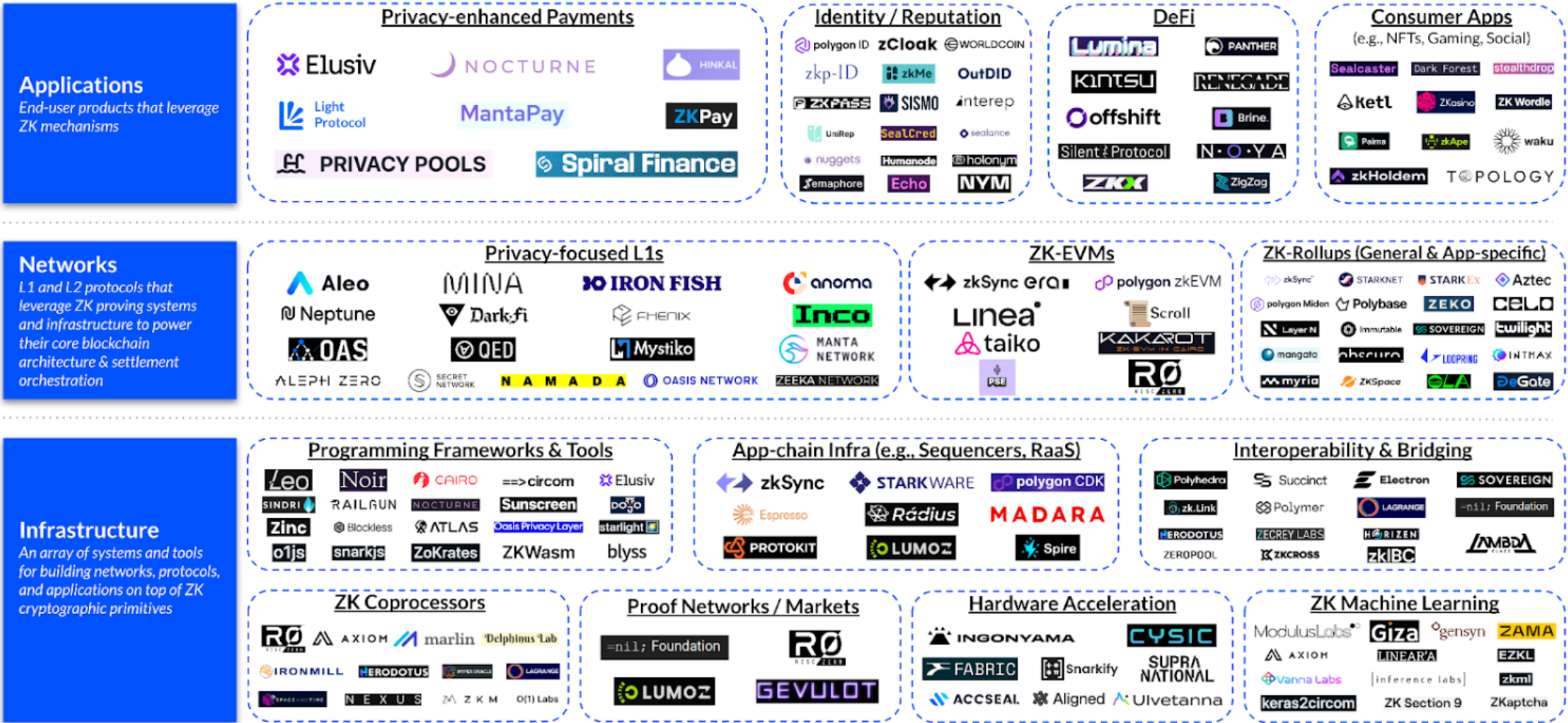
# From Promise to Practice: Why ZK for Privacy Is Still Niche?

- We don't care about privacy.
- DSL a barrier to adoption
- Require heavy hardware
- UX



Q4-2023

# Zero-Knowledge Landscape



\*This landscape is not exhaustive and contains Coinbase Ventures portfolio companies.

# ZK Evolution (Practice Edition)

- **In the Beginning:** Reduce to an NP-complete problem (eg, Graph Hamiltonicity, Graph 3-Coloring)
- **Then:** Boolean and Arithmetic circuits
- **Since Blockchains:** R1CS, Circom, Cairo, Gnark, etc...
- **Today:** zkVMs

# What are zkVMs?

- ❑ Code application in a high-level language (C++/Rust)
- ❑ Compile to a popular VM (RISC-V, WASM)
- ❑ Prove correct execution of VM

# Challenges in ZK Design

- Circuit Representation (Graph 3COL  $\rightarrow$  zkVMs)
- Prover runtime (Polynomial  $\rightarrow$  Quasi-linear  $\rightarrow$  Linear)
- Today: Space complexity

**Main Question:** Do there exist **time and space preserving** ZK-SNARKs?

[BC12] Private-coin complexity-preserving succinct argument (from FHE)

[BHRRS20,21] Complexity-preserving ZKSNARKS [DLOG, unknown order]

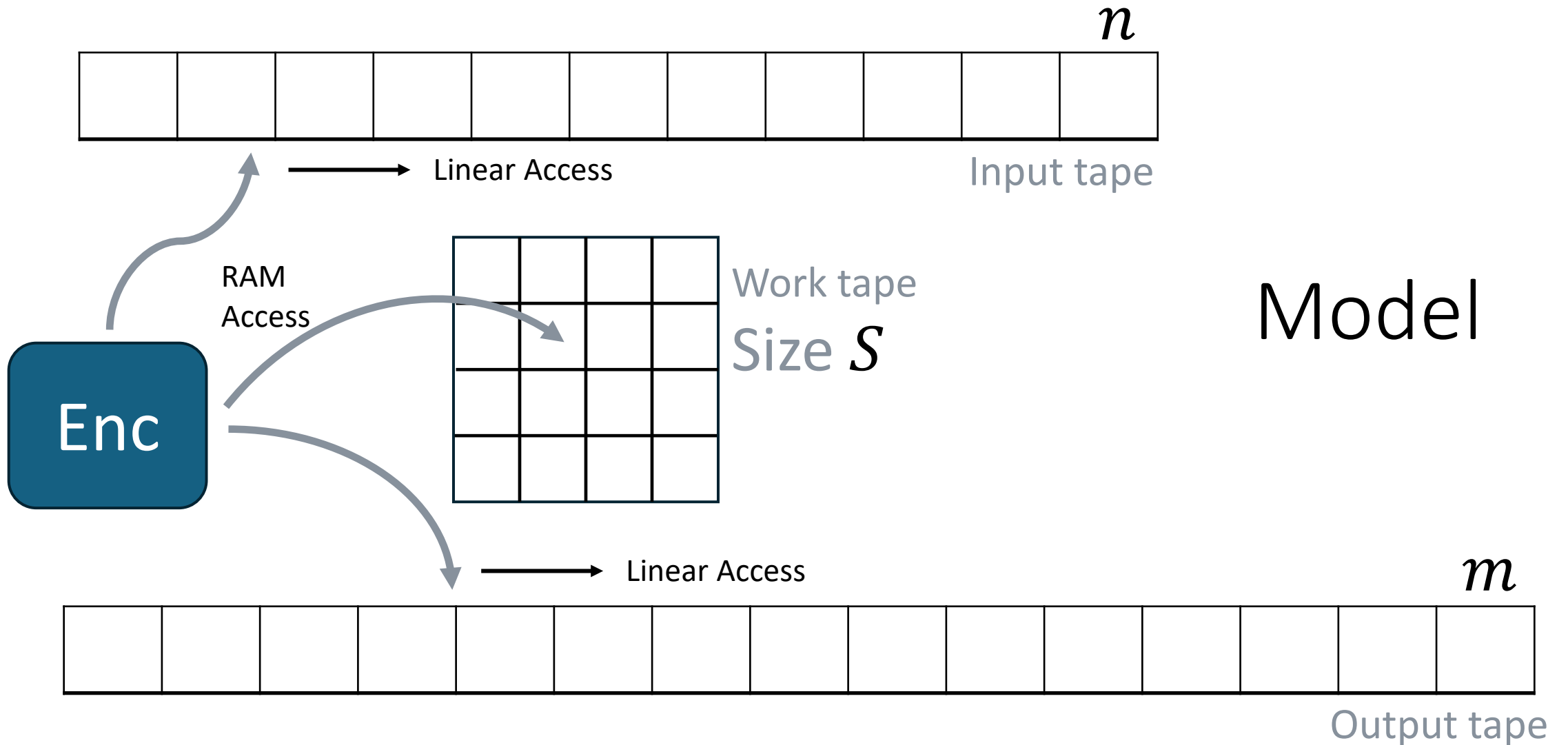
From minimal assumptions? in a black-box way?

Yes\* [BBHV22] (Proof length  $T/S$ )

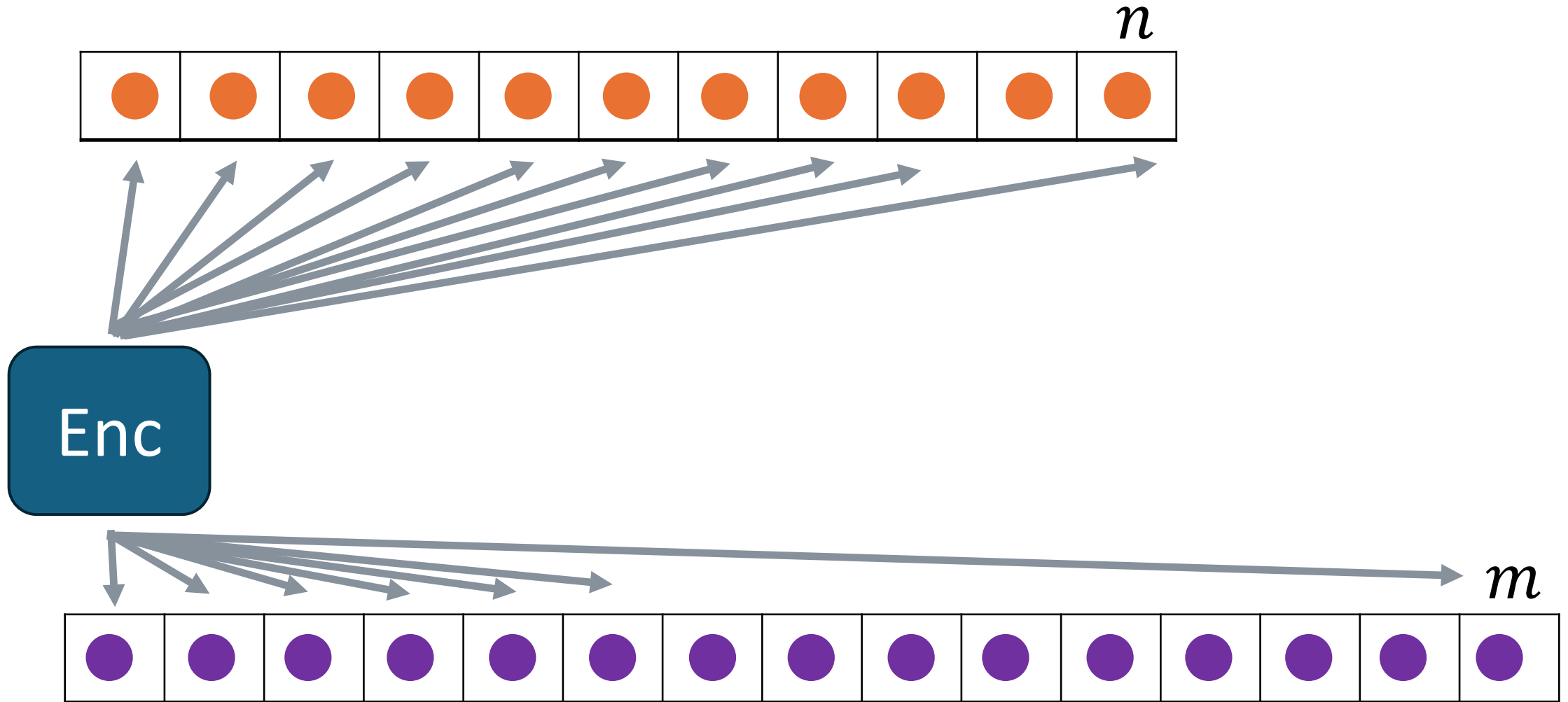
# Why is memory efficiency hard?

Time-space tradeoff for error correcting codes

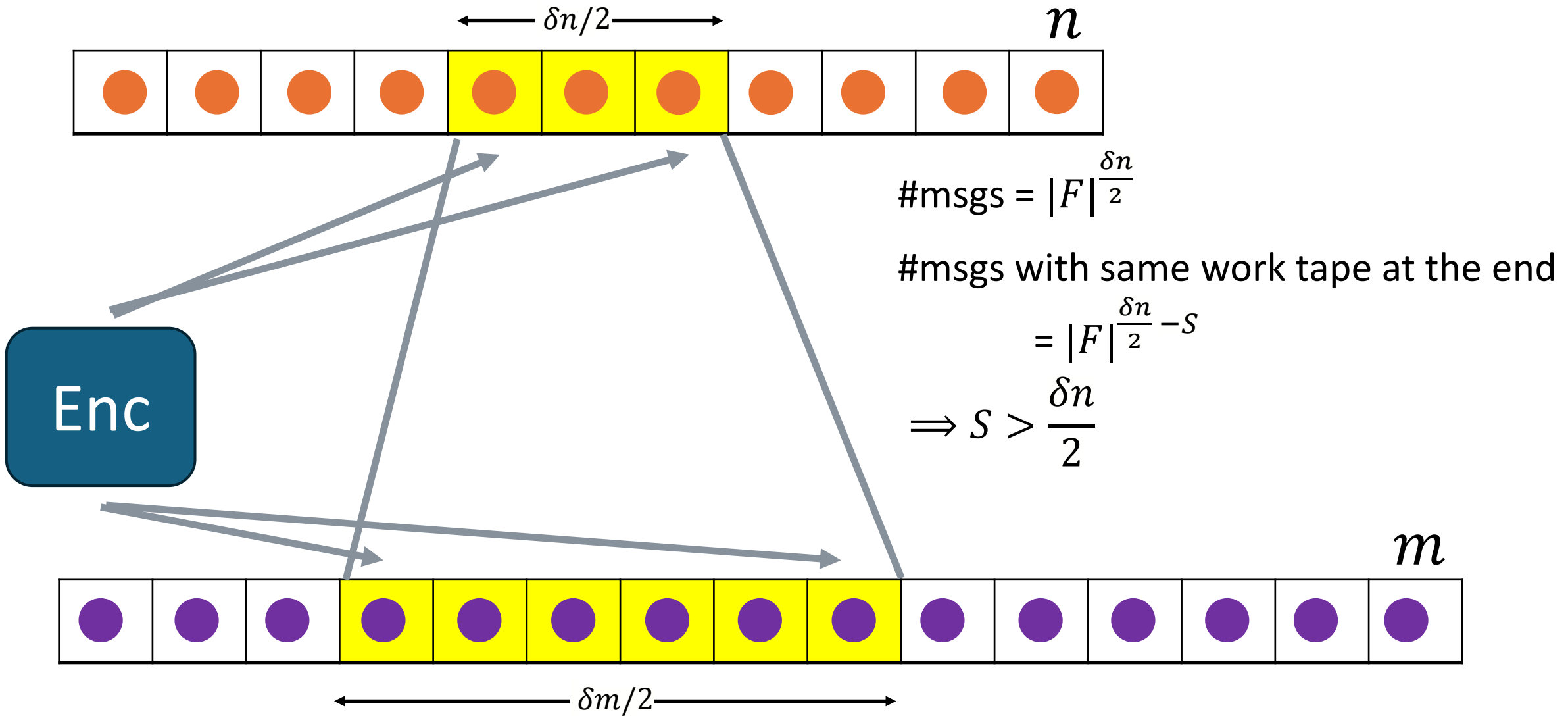
# Time-Space Tradeoff for ECC



# Time-Space Tradeoff for ECC



# Time-Space Tradeoff for ECC



# Time-Space Tradeoff for ECC

**Theorem:** For an  $r$  - pass encoding algorithm  $S > \frac{\delta n}{4r}$

i.e., If we need quasi-linear time constant-distance codes  
then, memory =  $\Omega(\text{message length})$

# Ligetron ZK

## The ZK Tech from Ligero Inc.

# Ligetrion ZK [WHV24]

- Ligetrion ZK\* is (the only) memory-efficient hash-based ZK-SNARK
- Ligetrion is ZK by default and transparent setup
- Ligetrion is a zkVM = zkWASM
- A scalable/portable implementation using WebGPUs

# Ligetron ZK Platform and Apps

# Ligetron ZK Development Platform

- ✓ Build **Anywhere** – All you need is a browser.
- ✓ Build in **Any Language** – C/C++, Rust, Circom
- ✓ Run **Everywhere** – Mobile, Laptop, Server, Raspberry PI

## ZK Anywhere Everywhere

[platform.ligetron.com](https://platform.ligetron.com)

[www.ligero-inc.com](https://www.ligero-inc.com)

✕ @ligero\_inc

Thank You