Fully Anonymous Secret Sharing

Allison Bishop, Matthew Green, Yuval Ishai, Abhishek Jain, Paul Lou

Proof Trading & City College, CUNY — JHU — Technion & AWS — NTT Research & JHU — UCLA

Fully Anonymous Secret Sharing—Overview

An {S, M, U}-**fully anonymous secret sharing** scheme satisfies *{S, M, U}-anonymity* (respectively) and *anonymous reconstruction*.

We systematically study notions of anonymity.

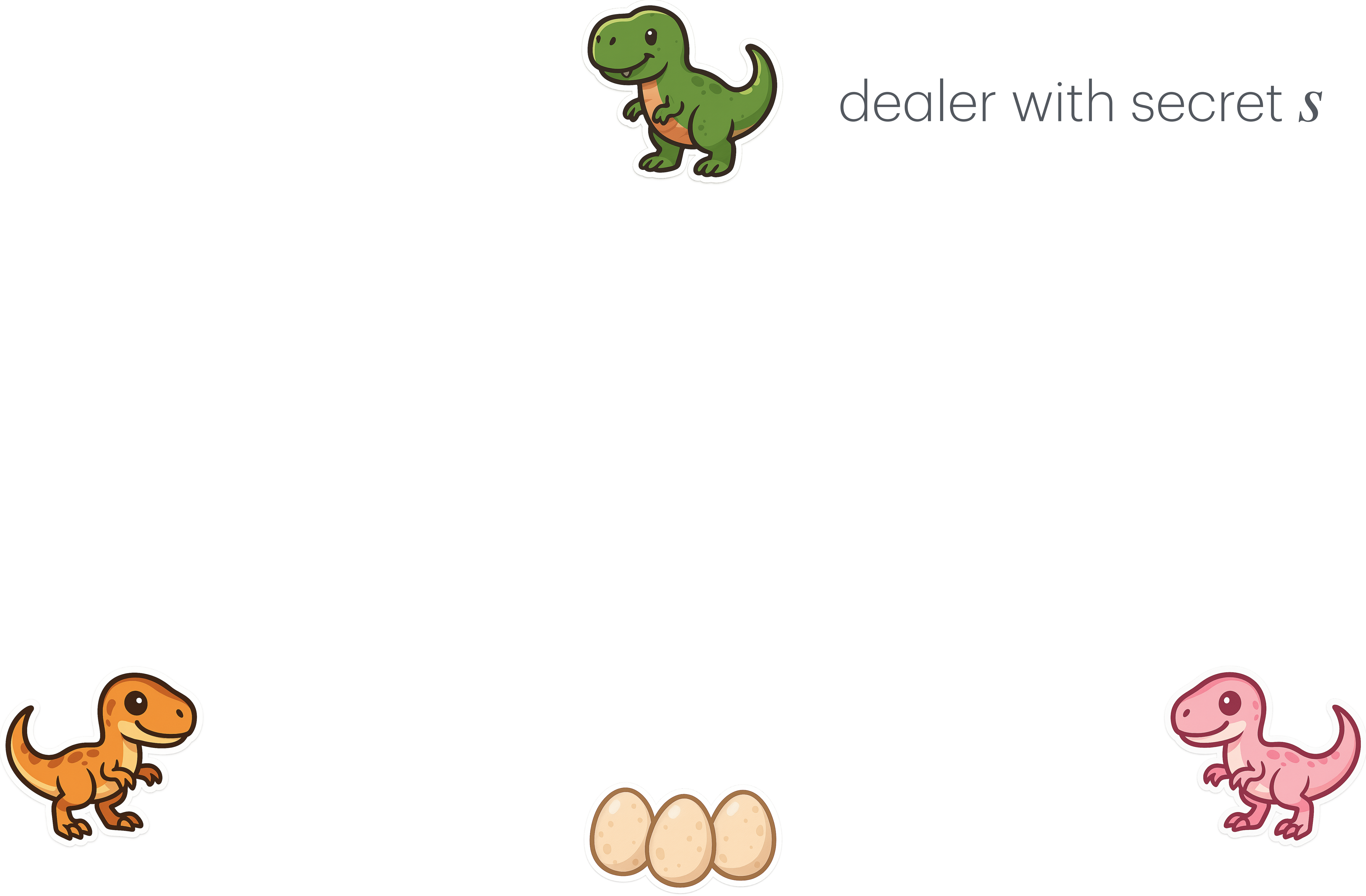
S-Anonymous $\subsetneq$ M-Anonymous $\subsetneq$ U-Anonymous

Additionally, we desire *robust reconstruction*—reconstruction in the presence of multiple dealers, ideally for an unbounded number.

We give info-theoretic upper and lower bounds on share sizes that are nearly tight. We show that use of cryptography circumvents the lower bounds!

Motivating Various Definitions of Share Anonymity— {S, M, U}-Anonymity

Warm-up: Shamir's Secret Sharing



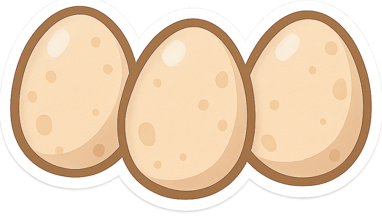
dealer with secret s

n parties

Warm-up: Shamir's Secret Sharing

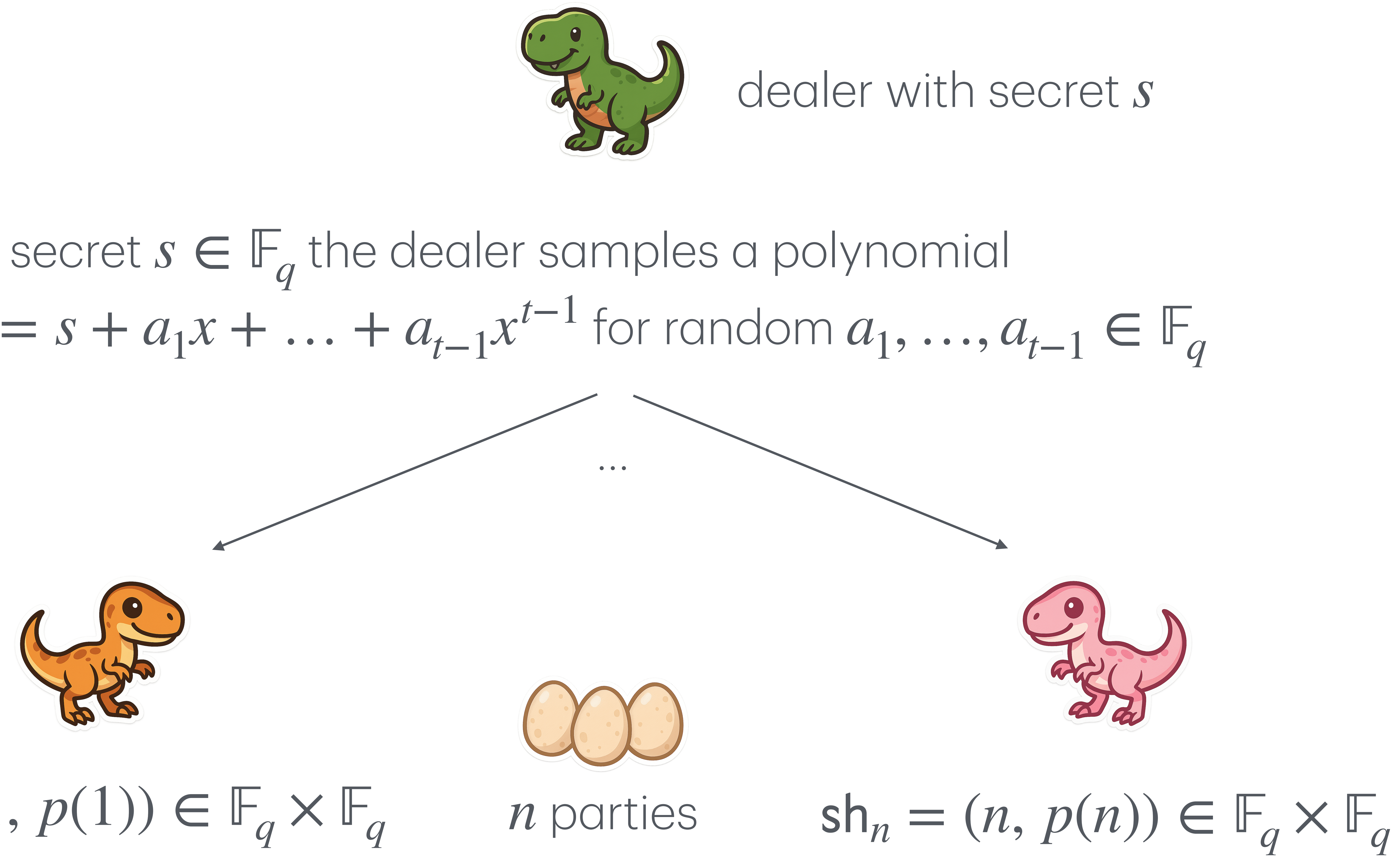
dealer with secret s

For a secret $s \in \mathbb{F}_q$ the dealer samples a polynomial $p(x) = s + a_1 x + \ldots + a_{t-1} x^{t-1}$ for random $a_1, \ldots, a_{t-1} \in \mathbb{F}_q$



n parties

Warm-up: Shamir's Secret Sharing



dealer with secret s

For a secret $s \in \mathbb{F}_q$ the dealer samples a polynomial

$p(x) = s + a_1 x + \ldots + a_{t-1} x^{t-1}$ for random $a_1, \ldots, a_{t-1} \in \mathbb{F}_q$

…

$\mathsf{sh}_1 = (1, p(1)) \in \mathbb{F}_q \times \mathbb{F}_q$

n parties

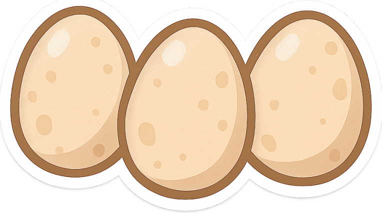
$\mathsf{sh}_n = (n, p(n)) \in \mathbb{F}_q \times \mathbb{F}_q$

Warm-up: Shamir's Secret Sharing

dealer with secret s

Perfectly correct, information-theoretic secrecy, with optimal share size $\approx \log n$.

$\mathsf{sh}_1 = (1,\, p(1)) \in \mathbb{F}_q \times \mathbb{F}_q$



n parties

$\mathsf{sh}_n = (n,\, p(n)) \in \mathbb{F}_q \times \mathbb{F}_q$

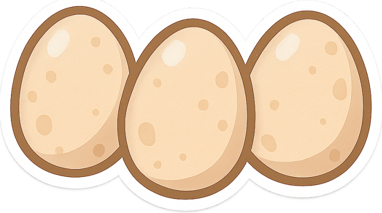
Warm-up: Shamir's Secret Sharing

dealer with secret s

Perfectly correct, information-theoretic secrecy, with optimal share size $\approx \log n$.

Each party's share reveals its identity!

$\mathsf{sh}_1 = (1,\, p(1)) \in \mathbb{F}_q \times \mathbb{F}_q$



n parties

$\mathsf{sh}_n = (n,\, p(n)) \in \mathbb{F}_q \times \mathbb{F}_q$

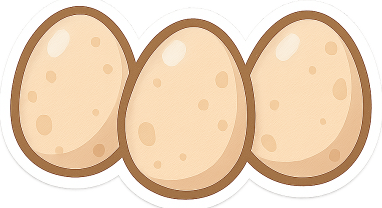
Warm-up: Shamir's Secret Sharing

dealer with secret s

Basic question: Can a party's share hide its identity?

i.e. can we achieve **"share anonymity"**?

Each party's share reveals its identity!



$\mathsf{sh}_1 = (1, p(1)) \in \mathbb{F}_q \times \mathbb{F}_q$

n parties

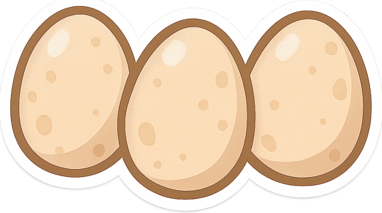
$\mathsf{sh}_n = (n, p(n)) \in \mathbb{F}_q \times \mathbb{F}_q$

Warm-up: Permuted Shamir's Secret Sharing

dealer with secret s

1. For a secret $s \in \mathbb{F}_q$, the dealer samples a polynomial $p(x) = s + a_1 x + \ldots + a_{t-1} x^{t-1}$ for random $a_1, \ldots, a_{t-1} \in \mathbb{F}_q$.

2. **Additionally picks a permutation π on n elements.**



n parties

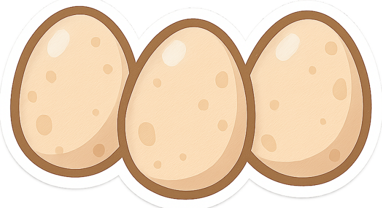
Warm-up: Permuted Shamir's Secret Sharing

dealer with secret s

1. For a secret $s \in \mathbb{F}_q$, the dealer samples a polynomial $p(x) = s + a_1 x + \ldots + a_{t-1} x^{t-1}$ for random $a_1, \ldots, a_{t-1} \in \mathbb{F}_q$.

2. **Additionally picks a permutation π on n elements.**

$\mathsf{sh}_1 = (\pi(1), p(\pi(1)))$



n parties

$\mathsf{sh}_n = (\pi(n), p(\pi(n)))$

Warm-up: Permuted Shamir's Secret Sharing

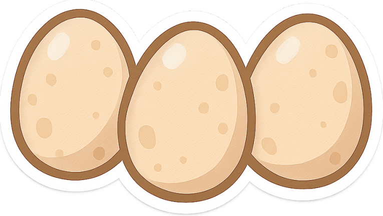
dealer with secret s

1. For a secret $s \in \mathbb{F}_q$, the dealer samples a polynomial $p(x) = s + a_1 x + \ldots + a_{t-1} x^{t-1}$ for random $a_1, \ldots, a_{t-1} \in \mathbb{F}_q$.

2. **Additionally picks a permutation π on n elements.**

π is hidden. So party's identity is hidden!

$\mathsf{sh}_1 = (\pi(1), p(\pi(1)))$



n parties

$\mathsf{sh}_n = (\pi(n), p(\pi(n)))$

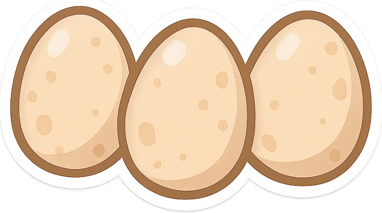
Warm-up: Permuted Shamir's Secret Sharing

dealer with secret s

Perfectly correct, information-theoretic secrecy, with optimal share size $\approx \log n$
AND satisfies *share anonymity* ***(we term as Single-dealer or S-Anonymity)***!

π is hidden. So party's identity is hidden!

$\mathsf{sh}_1 = (\pi(1),\, p(\pi(1)))$



n parties

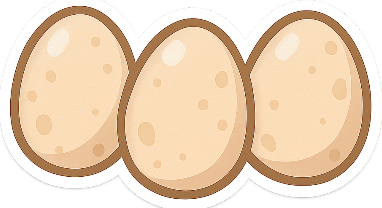
$\mathsf{sh}_n = (\pi(n),\, p(\pi(n)))$

Warm-up: Permuted Shamir's Secret Sharing

dealer with secret s

Does this permutation **anonymize** all interesting information while preserving perfect correctness and optimal share sizes?

π is hidden. So party's identity is hidden!



$\mathsf{sh}_1 = (\pi(1), p(\pi(1)))$

n parties

$\mathsf{sh}_n = (\pi(n), p(\pi(n)))$

Multi-Dealer Anonymity (M-Anonymity)

dealer 1 with secret s_1

dealer 2 with secret s_2

Can an adversary distinguish between the following two distributions?

Distribution 1: A set of unauthorized shares produced by dealer 1.

Distribution 2: A set of some unauthorized shares from dealer 1 and some unauthorized shares from dealer 2.

Multi-Dealer Anonymity (M-Anonymity)

dealer 1 with secret s_1

dealer 2 with secret s_2

Can an adversary distinguish between the following two distributions?

Distribution 1: A set of unauthorized shares produced by dealer 1.

Distribution 2: A set of some unauthorized shares from dealer 1 and some unauthorized shares from dealer 2.

Previously motivated and studied by [Eldridge-Beck-Green-Heninger-Jain USENIX '24] for abuse-resistant location tracking (e.g. abuse-resistant Apple Airtags).

Warm-up: Permuted Shamir's Secret Sharing

dealer 1 with secret s_1

dealer 2 with secret s_2

Permuted Shamir's Secret Sharing does not satisfy **M-Anonymity**!

Warm-up: Permuted Shamir's Secret Sharing

dealer 1 with secret s_1

dealer 2 with secret s_2

Permuted Shamir's Secret Sharing does not satisfy **M-Anonymity**!

Imagine Adversary selects parties $\{1,2\}$ and receives the following two shares from the challenger:

$$\mathsf{sh}_1^{(1)} = (\pi_1(1),\, p(\pi_1(1)))$$

$$\mathsf{sh}_2^{(2)} = (\pi_2(2),\, p(\pi_2(2)))$$

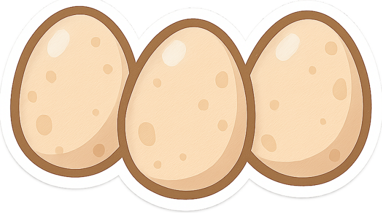
$1/n$ probability that $\pi_1(1) = \pi_2(2)$. This is impossible if these two shares came from the same dealer!

Warm-up: Random Shamir's Secret Sharing

dealer with secret s

For a secret $s \in \mathbb{F}_q$, the dealer samples a polynomial
$p(x) = s + a_1 x + \ldots + a_{t-1} x^{t-1}$ for random $a_1, \ldots, a_{t-1} \in \mathbb{F}_q$.

…



$\mathsf{sh}_1 = (\$, p(\$))$

n parties

$\mathsf{sh}_n = (\$, p(\$))$

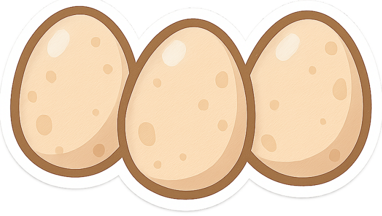
Warm-up: Random Shamir's Secret Sharing

dealer with secret s

Additionally satisfies a stronger notion than M-Anonymity:

- any unauthorized set of shares is **uniform random (U-Anonymity)**.

$\mathsf{sh}_1 = (\$, p(\$))$



n parties

$\mathsf{sh}_n = (\$, p(\$))$

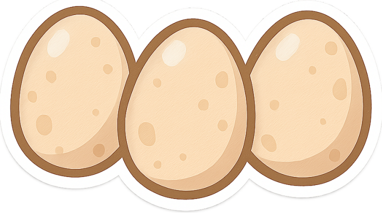
Warm-up: Random Shamir's Secret Sharing

dealer with secret s

However, correctness error is now $1/q$.

For negligible correctness error, the share size is now $\omega(\log n)$.

$\mathsf{sh}_1 = (\$,\ p(\$))$



n parties

$\mathsf{sh}_n = (\$,\ p(\$))$

Fully Anonymous Secret Sharing—Overview

An {S, M, U}-**fully anonymous secret sharing** scheme satisfies *{S, M, U}-anonymity* (respectively) and *anonymous reconstruction*.

We systematically study notions of anonymity.

S-Anonymous $\subsetneq$ M-Anonymous $\subsetneq$ U-Anonymous

Additionally, we desire *robust reconstruction*—reconstruction in the presence of multiple dealers, ideally for an unbounded number.

Robust and Anonymous Reconstruction

But wait… how do we reconstruct with many dealers?

k many dealers

Suppose they all emit Shamir secret shares of their own secrets.

Given a set of shares, how can we recover all secrets corresponding to authorized sets?

Robust Reconstruction

k many dealers

Suppose they all emit Shamir secret shares of their own secrets.

Given a set of shares, how can we recover all secrets corresponding to authorized sets?

Easy solution: Each dealer tags its shares with a dealer ID.

Problem: Violates M-Anonymity.

Robust Reconstruction

k many dealers

Suppose they all emit Shamir secret shares of their own secrets.

Given a set of shares, how can we recover all secrets corresponding to authorized sets?

Easy solution: Each dealer tags its shares with a dealer ID.

Problem: Violates M-Anonymity.

[Eldridge, Beck, Green, Heninger, Jain USENIX '24] gave an error-correcting code based M-anonymous scheme that handles a **constant** number of dealers for the **threshold** access structure.

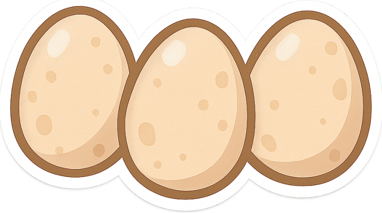
Anonymous Reconstruction

dealer with secret s

The reconstruction algorithm for Shamir's secret sharing is polynomial interpolation, which does not need to use party identities, i.e. which parties hold which shares.

This is what we refer to as **anonymous reconstruction**.

$\mathsf{sh}_1 = (\$, p(\$))$



n parties

$\mathsf{sh}_n = (\$, p(\$))$

Anonymous Reconstruction

dealer with secret s

Non-example for anonymous reconstruction: Consider an access structure over three parties $\{p_1, p_2, p_3\}$ where the minimal authorized sets are $\{\{p_1\}, \{p_2, p_3\}\}$. Consider the following scheme:

$\mathsf{sh}_1 = s$ $\mathsf{sh}_2 = s \oplus r$ $\mathsf{sh}_3 = r$

Anonymous Reconstruction

dealer with secret s

Non-example for anonymous reconstruction: Consider an access structure over three parties $\{p_1, p_2, p_3\}$ where the minimal authorized sets are $\{\{p_1\}, \{p_2, p_3\}\}$. Consider the following scheme:

$\mathsf{sh}_1 = s$ $\qquad$ $\mathsf{sh}_2 = s \oplus r$ $\qquad$ $\mathsf{sh}_3 = r$

Fix (not S-Anon): $\mathsf{sh}_1 = (1,\ s)$ $\qquad$ $\mathsf{sh}_2 = (2,\ s \oplus r)$ $\qquad$ $\mathsf{sh}_3 = (3,\ r)$

Fully Anonymous Secret Sharing—Overview

An {S, M, U}-**fully anonymous secret sharing** scheme satisfies *{S, M, U}-anonymity* (respectively) and *anonymous reconstruction*.

S-Anonymous $\subsetneq$ M-Anonymous $\subsetneq$ U-Anonymous

Additionally, we desire *robust reconstruction*—reconstruction in the presence of multiple dealers, ideally for an unbounded number.

Technical Challenge of Building FASS Schemes for Arbitrary Access Structures

The Technical Challenge

dealer with secret s

Most known methods [Ito, Saito, Nishizeki '87, Benaloh, Leichter '90, Liu, Vaikuntanathan '18, Appelbaum, Beimel, Farràs, Nir, Peter '19] of constructing secret sharing schemes for arbitrary access structures breaks the access structure into ANDs and ORs and uses recursive composition!

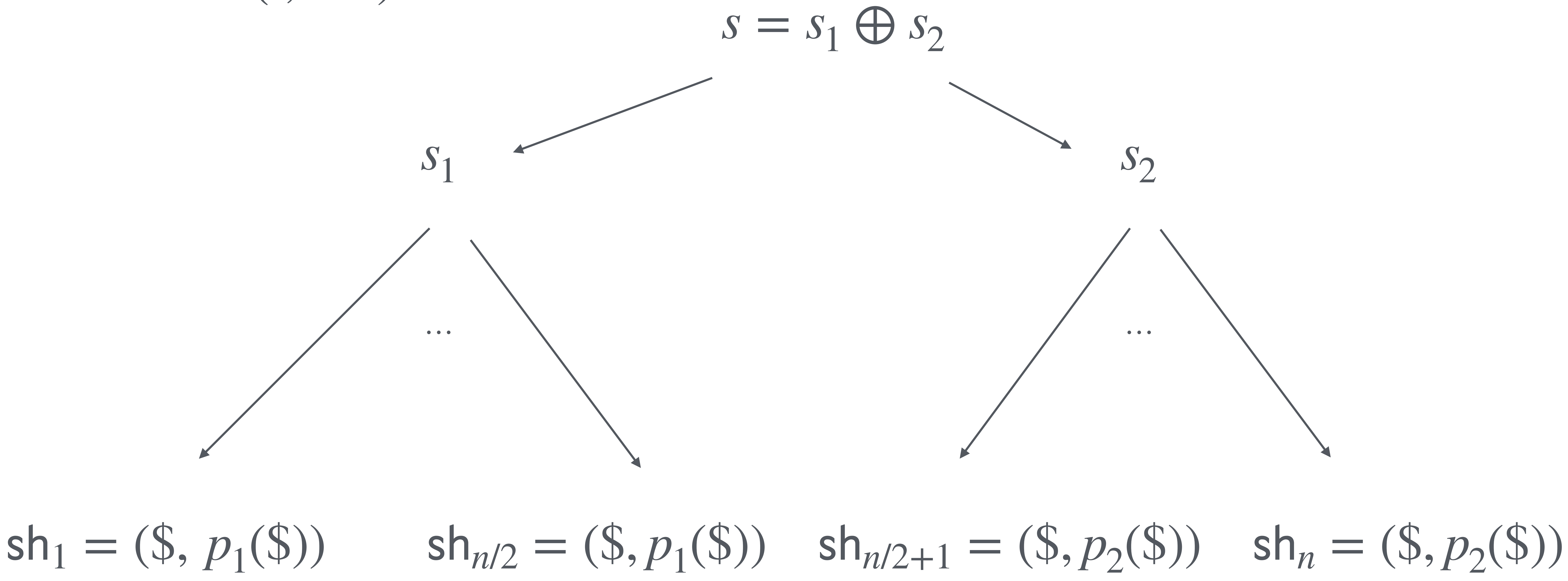
This kills anonymity!

Example: Consider an access structure that is an AND of two $(t, n/2)$- thresholds.

The Technical Challenge

Consider an access structure that is an AND of two $(t, n/2)$- thresholds.

dealer with secret s



$s = s_1 \oplus s_2$

s_1

s_2

...

...

$\mathsf{sh}_1 = (\$,\ p_1(\$))$

$\mathsf{sh}_{n/2} = (\$, p_1(\$))$

$\mathsf{sh}_{n/2+1} = (\$, p_2(\$))$

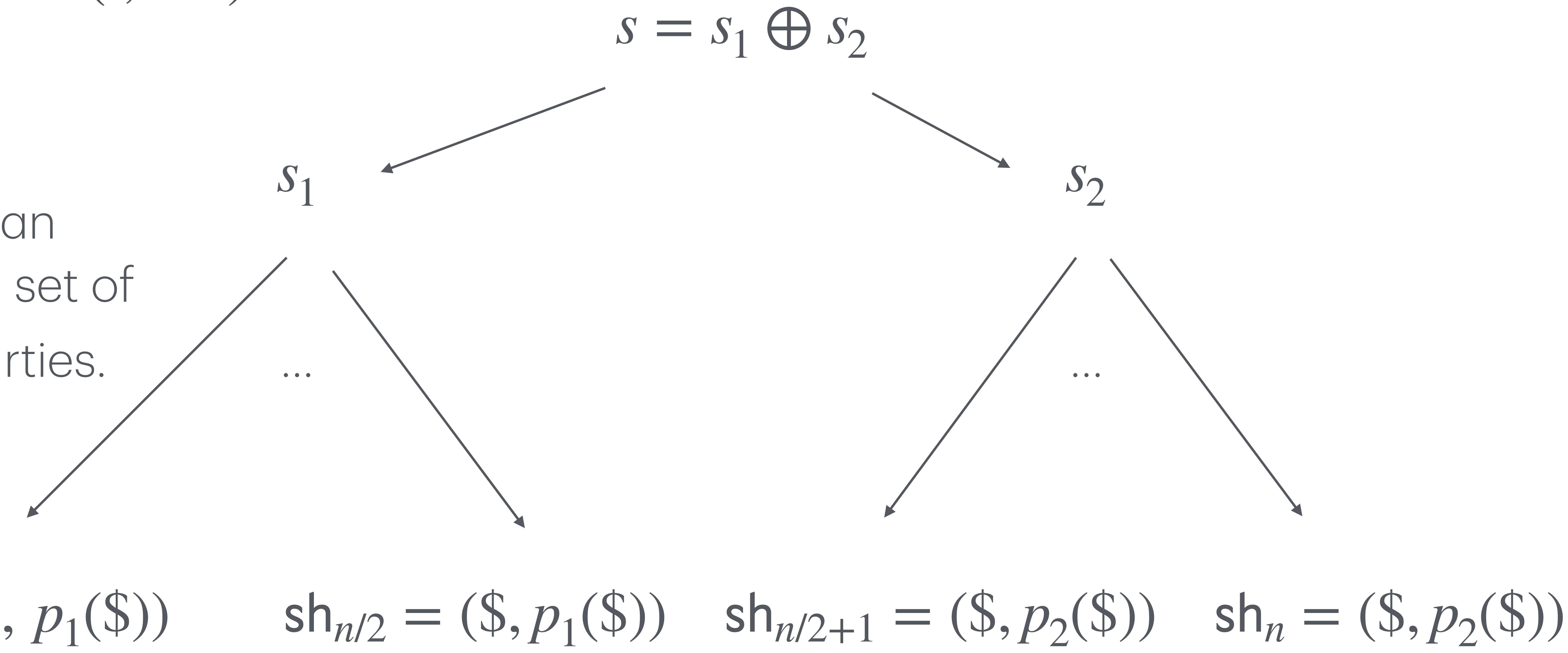
$\mathsf{sh}_n = (\$, p_2(\$))$

The Technical Challenge

Consider an access structure that is an AND of two $(t, n/2)$- thresholds.

dealer with secret s

Consider an unauthorized set of $t + 1$ left parties.



$s = s_1 \oplus s_2$

s_1

s_2

...

...

$\mathsf{sh}_1 = (\$, p_1(\$))$

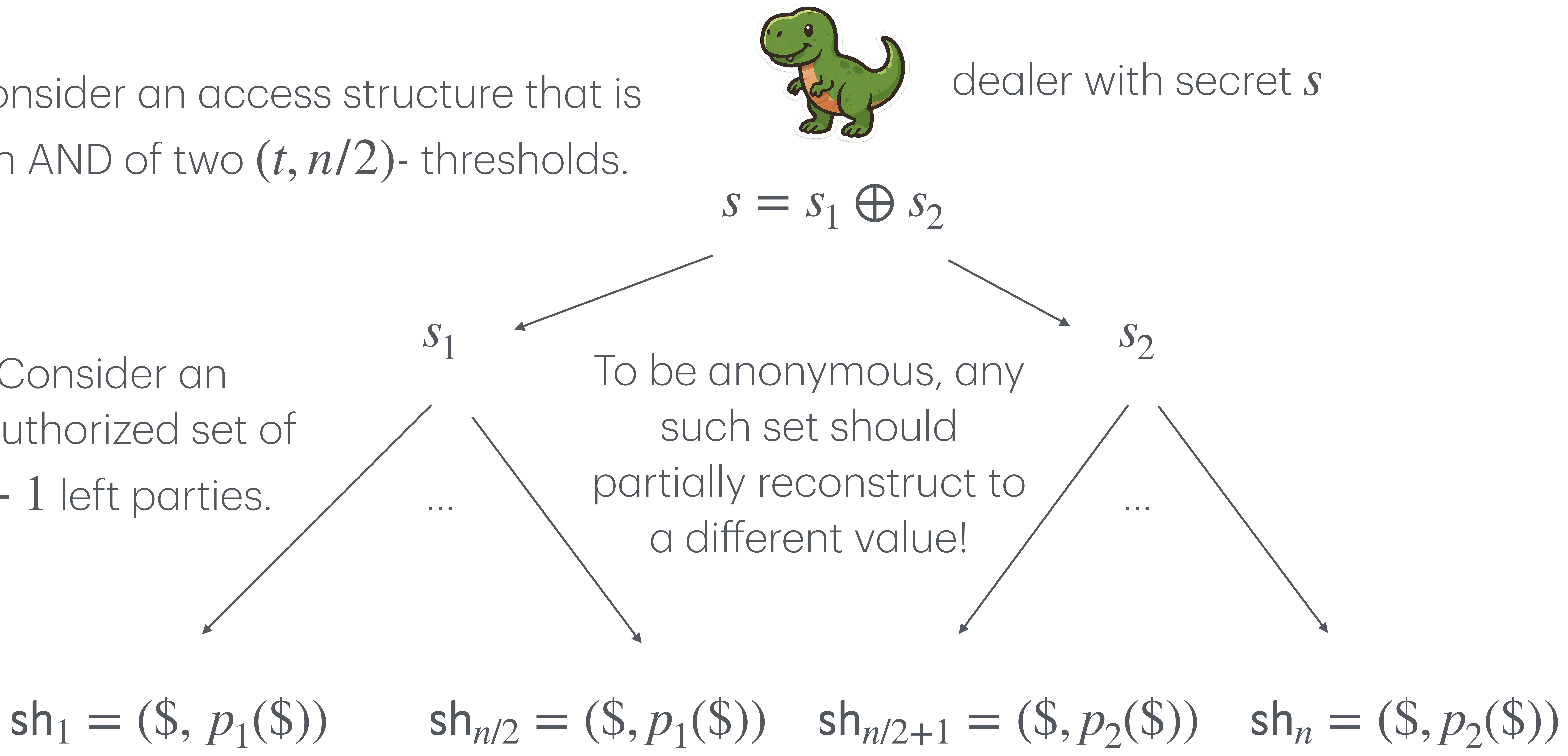
$\mathsf{sh}_{n/2} = (\$, p_1(\$))$

$\mathsf{sh}_{n/2+1} = (\$, p_2(\$))$

$\mathsf{sh}_n = (\$, p_2(\$))$

The Technical Challenge

Consider an access structure that is an AND of two $(t, n/2)$- thresholds.



dealer with secret s

$s = s_1 \oplus s_2$

s_1

s_2

Consider an unauthorized set of $t+1$ left parties.

To be anonymous, any such set should partially reconstruct to a different value!

...

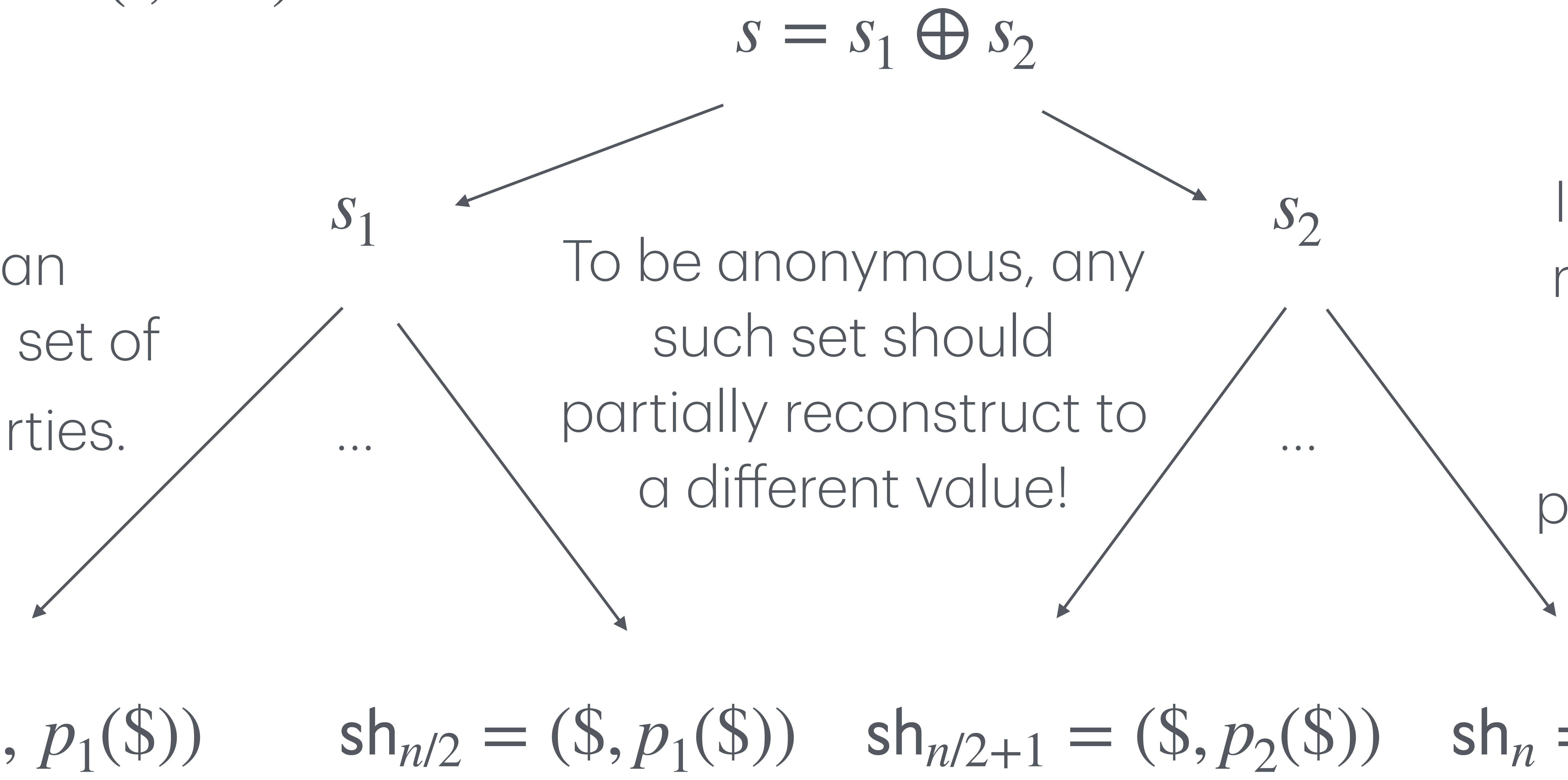
...

$\mathsf{sh}_1 = (\$, \ p_1(\$))$ $\mathsf{sh}_{n/2} = (\$, p_1(\$))$ $\mathsf{sh}_{n/2+1} = (\$, p_2(\$))$ $\mathsf{sh}_n = (\$, p_2(\$))$

The Technical Challenge

Consider an access structure that is an AND of two $(t, n/2)$- thresholds.

dealer with secret s



$s = s_1 \oplus s_2$

s_1 ... s_2 ...

Consider an unauthorized set of $t + 1$ left parties.

To be anonymous, any such set should partially reconstruct to a different value!

Intuitively: This means right side share has to be large enough to account for many possible reconstruction paths!

$\mathsf{sh}_1 = (\$, p_1(\$))$ $\mathsf{sh}_{n/2} = (\$, p_1(\$))$ $\mathsf{sh}_{n/2+1} = (\$, p_2(\$))$ $\mathsf{sh}_n = (\$, p_2(\$))$

Prior Work:

Anonymous Reconstruction:

- [Stinson, Vanstone '88]: Studied anonymous reconstruction for threshold access structures with perfect correctness, privacy, and distinct share values.
- [Phillips, Phillips '92]: Studied anonymous reconstruction ideal secret sharing (share size equal to secret size). Showed impossible for (t, n)-threshold for $t \notin \{1, n\}$.
- [Blundo, Stinson '97]: Considered (t, n)-threshold and an infinite class of non-threshold access structures. Showed a lower bound that the bit length of the shares needs to be $\Omega(\log n)$ additively larger than the number of bits needed to represent the secret.
- [Kishimoto, Okada, Kurosawa, Ogata '02]: Slightly tightens the constant in the lower bound above. Tight for the case of $t = 2$.

Prior Work:

Share Anonymity and FASS:

- [Guillermo, Martin, O'Keefe '03]:
  - Considered our notion of S-Anonymity under the name "*strong combinatorial cryptographic anonymity*". Considered anonymous reconstruction as "*submission anonymity*".
  - Proposed constructions achieving S-FASS for a special class of access structures with strong symmetry properties.
  - Observed permuted Shamir's secret sharing is S-FASS for threshold access structures.
- [Paskin-Cherniavsky, Olimid '20]
  - Their definition of *Decisional Share-Unpredicability* is morally M-Anonymity.
  - Gives a construction achieving (implicitly) statistical U-FASS for arbitrary access structures.

Prior Work:

Share Anonymity and FASS:

- [Eldridge, Beck, Green, Heninger, Jain '24]
  - Constructed statistical U-FASS with robust reconstruction (for constant many dealers) for threshold access structure.
  - Gave practical applications for M-FASS with robust reconstruction for abuse-resistant location tracking.

Our Work: A Systematic Study of FASS.

Information-theoretic contributions:

- New upper bound: Improve the share size of the U-FASS scheme from PO'20.
- Nearly matching lower bound on share size.
    - Implies the upper-bound is a near-optimal generic construction for any monotone access structure.

In contrast, in standard secret sharing there's an **exponential gap** between known upper and lower bounds on share sizes.

Our Work: A Systematic Study of FASS.

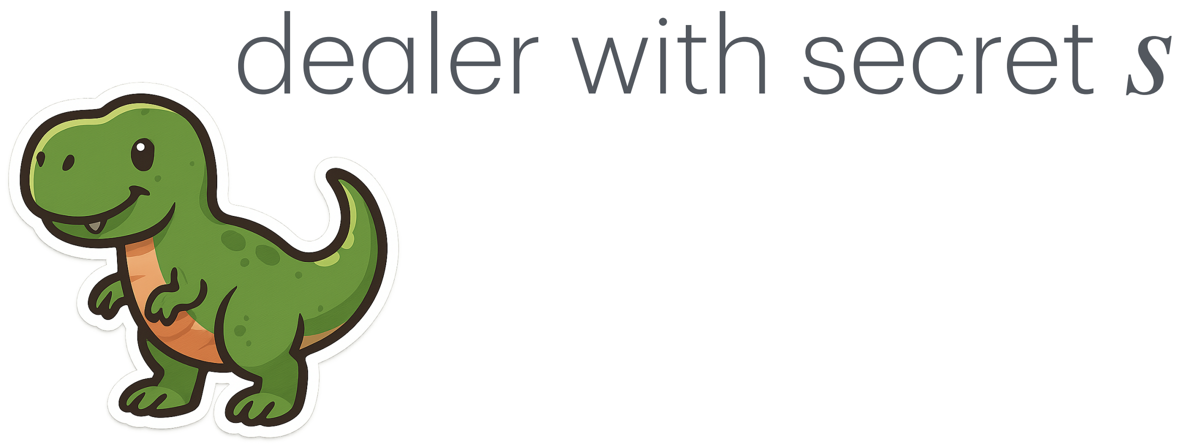
Computational Contributions:

- A **generic compiler** from any secret sharing scheme (with info-theoretic or computational secrecy) for any monotone access structure **to a computational M-fully anonymous secret sharing scheme** for the same access structure.
  - Preserves the share size of the underlying scheme.
  - Secrecy based on the hardness of LWE.
- Computational FASS schemes for specific graph access structures using other assumptions, e.g. OWF, DLIN. **Circumvents info-theoretic lower bound.**
- All our computational schemes enjoy **unbounded dealer** *robust reconstruction*.

Briefly: Our Computational Contributions

Computational Contributions:

- A **generic compiler** from any secret sharing scheme (with info-theoretic or computational secrecy) *for any monotone access structure* to a computational M-fully anonymous secret sharing scheme for the same access structure.
    - Preserves the share size of the underlying scheme.
    - Secrecy based on the hardness of LWE.



Uses **Compute-and-compare Obfuscation** [Wichs, Zerdelis '17, Goyal, Koppula, Waters '17].

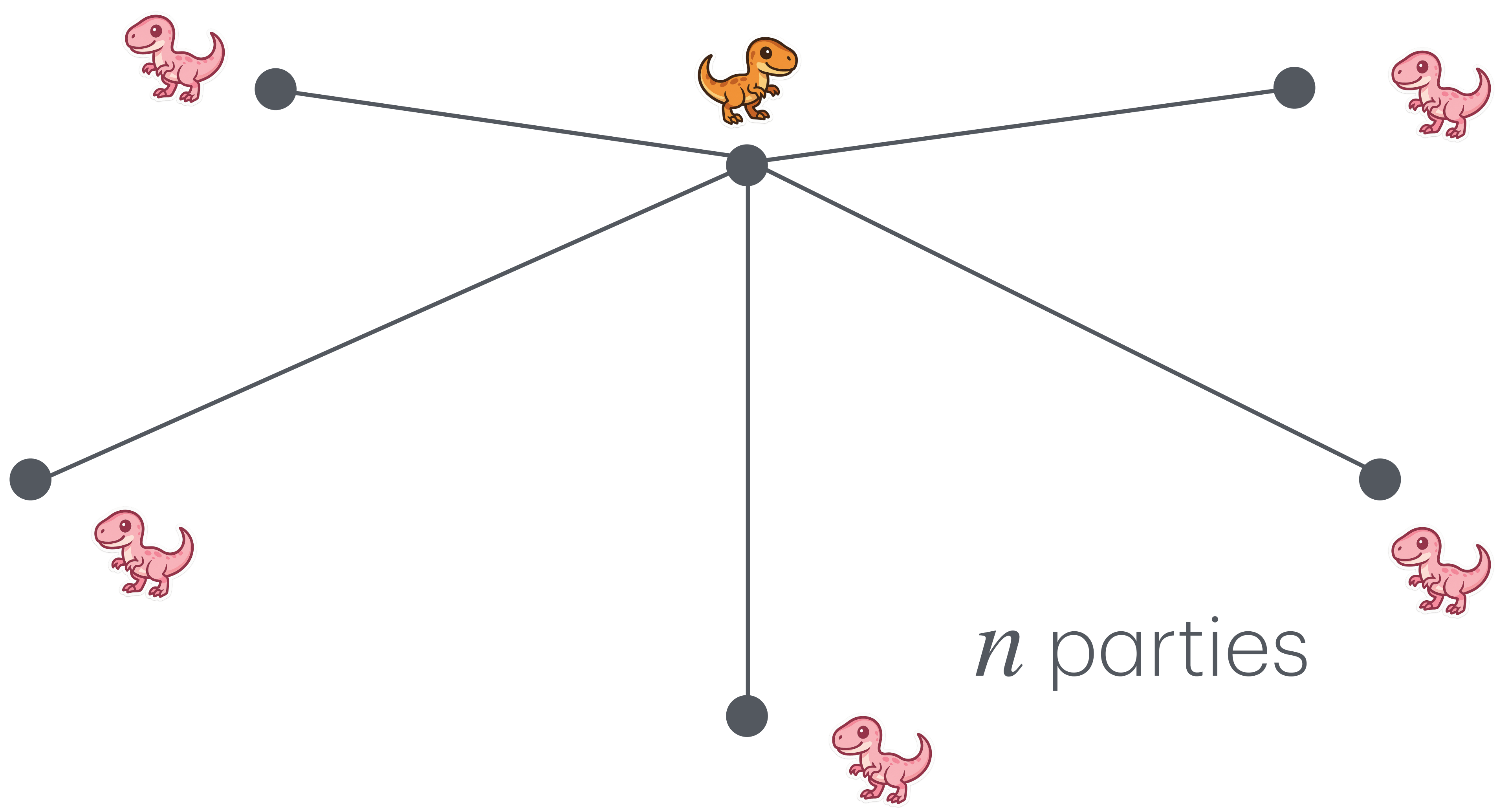
Briefly: Our Computational Contributions

Computational Contributions:

- Computational FASS schemes for specific graph access structures using other assumptions, e.g. OWF, DLIN. **Circumvents info-theoretic lower bound.**

Existence of OWF implies U-FASS for **star-graph** with unbounded robust reconstruction with shares size $O(\lambda)$, where λ is a security parameter.

Circumvents IT lower bound of $\Omega(n)$.



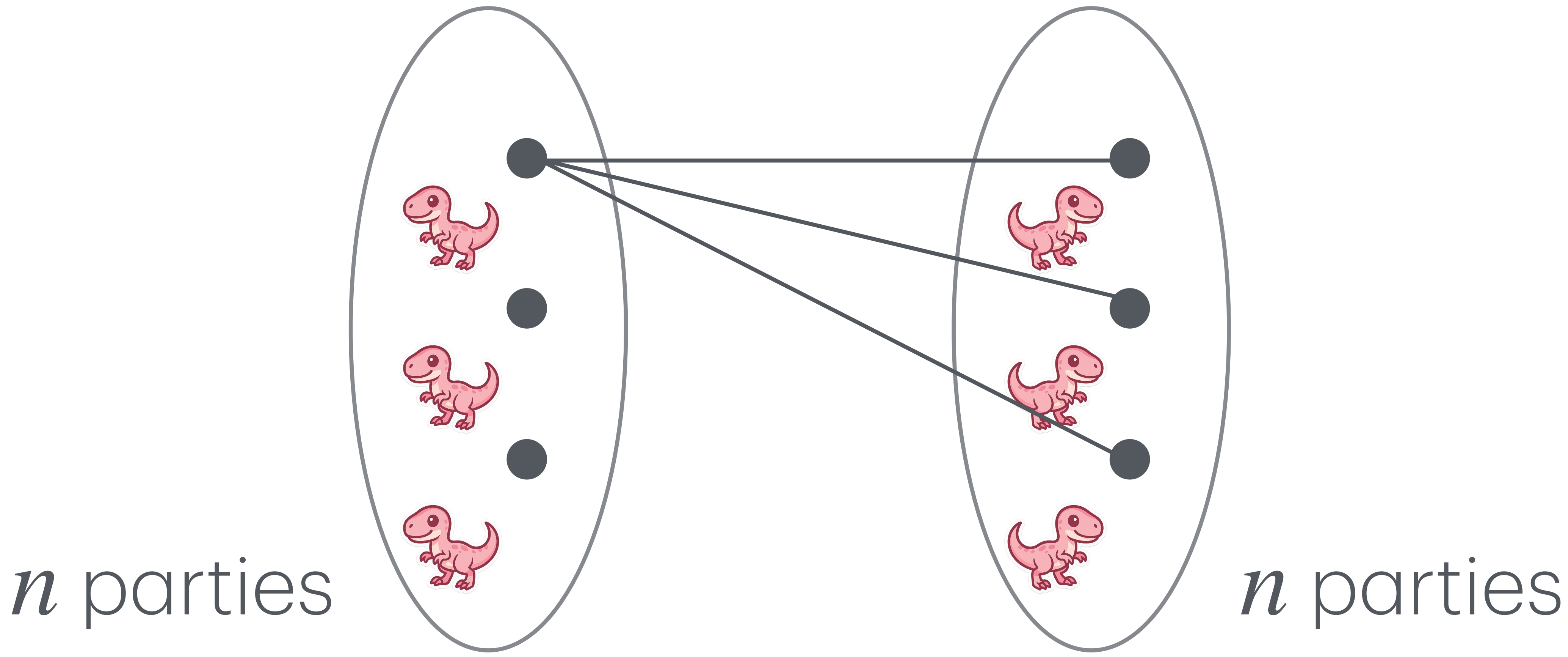
Briefly: Our Computational Contributions

Computational Contributions:

- Computational FASS schemes for specific graph access structures using other assumptions, e.g. OWF, DLIN. **Circumvents info-theoretic lower bound.**

Hardness of DLIN implies U-FASS for **complete bipartite graphs** with unbounded robust reconstruction with shares size $O(\lambda)$, where λ is a security parameter.

Circumvents IT lower bound of $\Omega(n)$.



Our Information-Theoretic Results

For the sake of time, will only detail the information-theoretic results:

Lower Bound: For every $m, d \in \mathbb{N}$, there is an n-party access structure $\mathscr{A}_{m,d}$ with $n = md + 1$, represented by a monotone DNF with $\ell = d^m$ minterms of degree $t = O(m)$, such that:

- Every U-FASS scheme for $\mathscr{A}_{m,d}$ has per-party share size $\Omega(\ell)$.
- $\mathscr{A}_{m,d}$ has a monotone CNF representation with $O(m)$ clauses of size $O(d)$.

Our Information-Theoretic Results

For the sake of time, will only detail the information-theoretic results:

Lower Bound: For every $m, d \in \mathbb{N}$, there is an n-party access structure $\mathscr{A}_{m,d}$ with $n = md + 1$, represented by a monotone DNF with $\ell = d^m$ minterms of degree $t = O(m)$, such that:

- Every U-FASS scheme for $\mathscr{A}_{m,d}$ has per-party share size $\Omega(\ell)$.
- $\mathscr{A}_{m,d}$ has a monotone CNF representation with $O(m)$ clauses of size $O(d)$.

Fix $d = 2$:

For every $m \in \mathbb{N}$, there is an access structure with $O(m)$ parties, with $\ell = 2^m$ minterms of degree $O(m)$ with per-party share size $\Omega(\ell)$.

Our Information-Theoretic Results

For the sake of time, will only detail the information-theoretic results:

Fix $d = 2$:

For every $m \in \mathbb{N}$, there is an access structure with $O(m)$ parties, with $\ell = 2^m$ minterms of degree $O(m)$ with per-party share size $\Omega(\ell)$.

Our Information-Theoretic Results

For the sake of time, will only detail the information-theoretic results:

Fix $d = 2$:

For every $m \in \mathbb{N}$, there is an access structure with $O(m)$ parties, with $\ell = 2^m$ minterms of degree $O(m)$ with per-party share size $\Omega(\ell)$.

Upper Bound: For any monotone DNF formula Φ with ℓ minterms of maximal degree t and statistical correctness parameter λ, there exists a U-FASS scheme realizing Φ that satisfies

- Perfect U-anonymity (implying perfect secrecy) and $2^{-\lambda}$ correctness error

- A per-party share size of $\tilde{O}(\lambda \ell t)$ for sharing a 1-bit secret.

Our Information-Theoretic Results

For the sake of time, will only detail the information-theoretic results:

Fix $d = 2$:

For every $m \in \mathbb{N}$, there is an access structure with $O(m)$ parties, with $\ell = 2^m$ minterms of degree $O(m)$ with per-party share size $\Omega(\ell)$.

Upper bound: $\tilde{O}(\ell)$

Information-Theoretic U-FASS

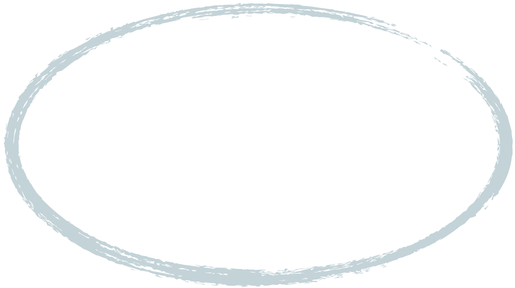
Any monotone access structure $\mathscr{A} : \{0,1\}^n \to \{0,1\}$ can be expressed as a monotone DNF.

e.g. the access structure $\{\{p_1\}, \{p_2, p_3\}\}$ can be expressed as

$$x_1 \vee (x_2 \wedge x_3).$$

a minterm of degree 2

Information-Theoretic U-FASS



[Paskin-Cherniavsky, Olimid ‘20] Information-theoretic solution:
Freshly share the secret for each minterm!

Information-Theoretic U-FASS

$$x_2 \wedge x_3.$$

Modifying an elegant solution from PO'20 for secrets $s \in \{0,1\}$:

- Sample random linearly independent vectors $\mathbf{v}_1, \mathbf{v}_2 \in \mathbb{F}^2$. Set $\mathbf{v}_3 = (s+1) \cdot \mathbf{v}_2$.

- Append $\mathbf{v}_i$ to Party i's share.

Perfect Reconstruction: Find the minimal linear dependency.

Perfect Secrecy: Unauthorized sets are distributed identically regardless of s.

Statistical U-Anonymity: For appropriate field size, linearly independent vectors are statistically close to random vectors.

Information-Theoretic U-FASS

$$x_1 \wedge \cdots \wedge x_t.$$

- Sample random linearly independent vectors $\mathbf{v}_2, \ldots, \mathbf{v}_n \in \mathbb{F}^{n-1}$.

  Set $\mathbf{v}_1 = (s+1) \cdot \mathbf{v}_2 + \sum_{i=3}^{t} \mathbf{v}_i$.

- Append $\mathbf{v}_i$ to Party $\boldsymbol{i}$'s share.

Perfect Reconstruction: Find the minimal linear dependency.

Perfect Secrecy: Unauthorized sets are distributed identically regardless of $\boldsymbol{s}$.

Statistical U-Anonymity: For appropriate field size, linearly independent vectors are statistically close to random vectors.

Information-Theoretic U-FASS

$$x_1 \wedge \cdots \wedge x_t.$$

- Sample random linearly independent vectors $\mathbf{v}_2, \ldots, \mathbf{v}_n \in \mathbb{F}^{n-1}$.

  Set $\mathbf{v}_1 = (s+1) \cdot \mathbf{v}_2 + \sum_{i=3}^{t} \mathbf{v}_i$.

- Append $\mathbf{v}_i$ to Party $\boldsymbol{i}$'s share.

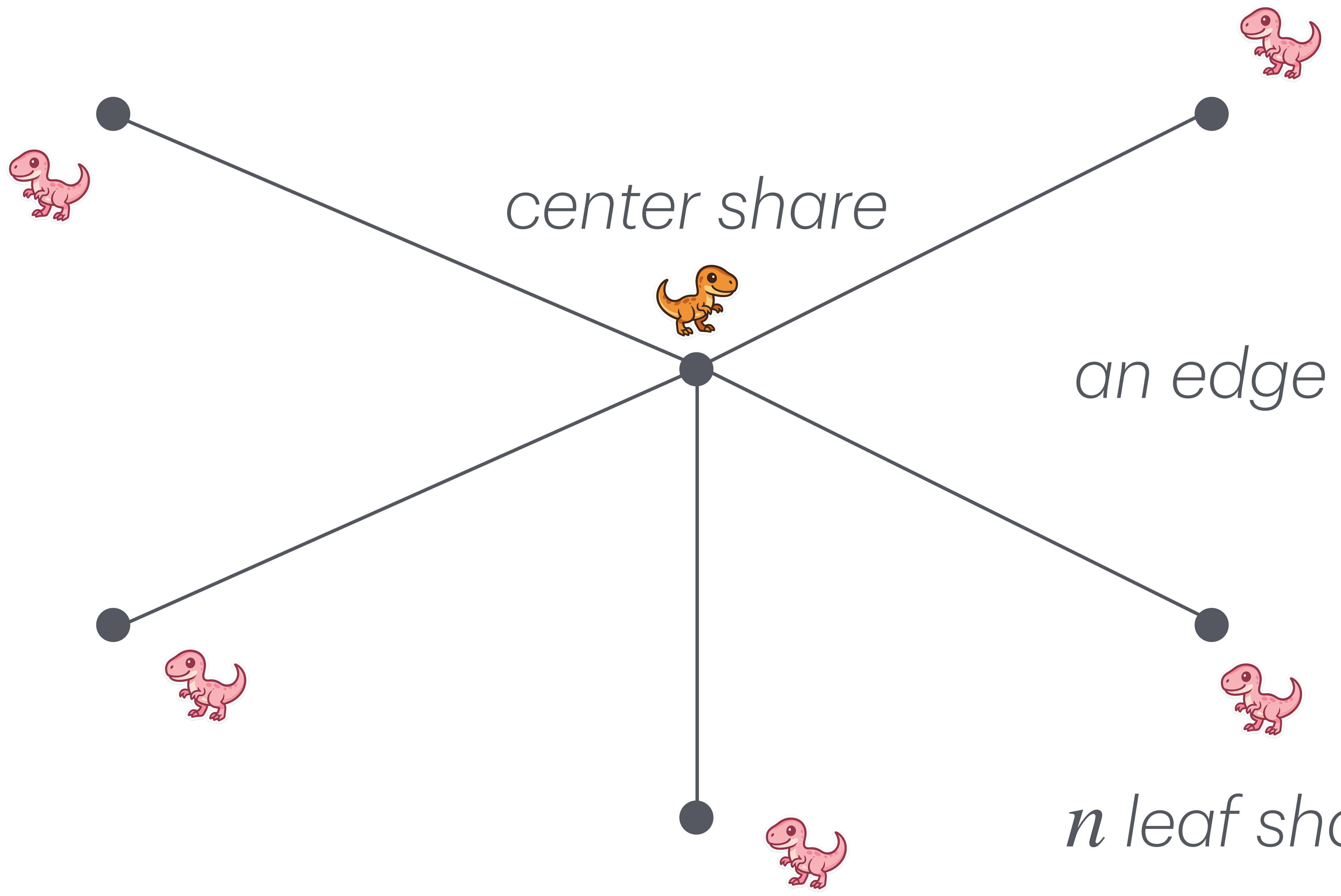
Per-party Share-size: $\tilde{O}(\ell n)$ where ℓ is the number of minterms.

Even for simple and explicit access structures, such as $(x_1 \vee x_2) \wedge (x_3 \vee x_4) \wedge \cdots \wedge (x_{n-1} \vee x_n)$*, the #minterms is exponential in* $\boldsymbol{n}$*.*

Is an exponential per-party share-size necessary?

A Linear Lower Bound for U-FASS

The *star-graph access structure* captures the bit complexity needed in a single share.

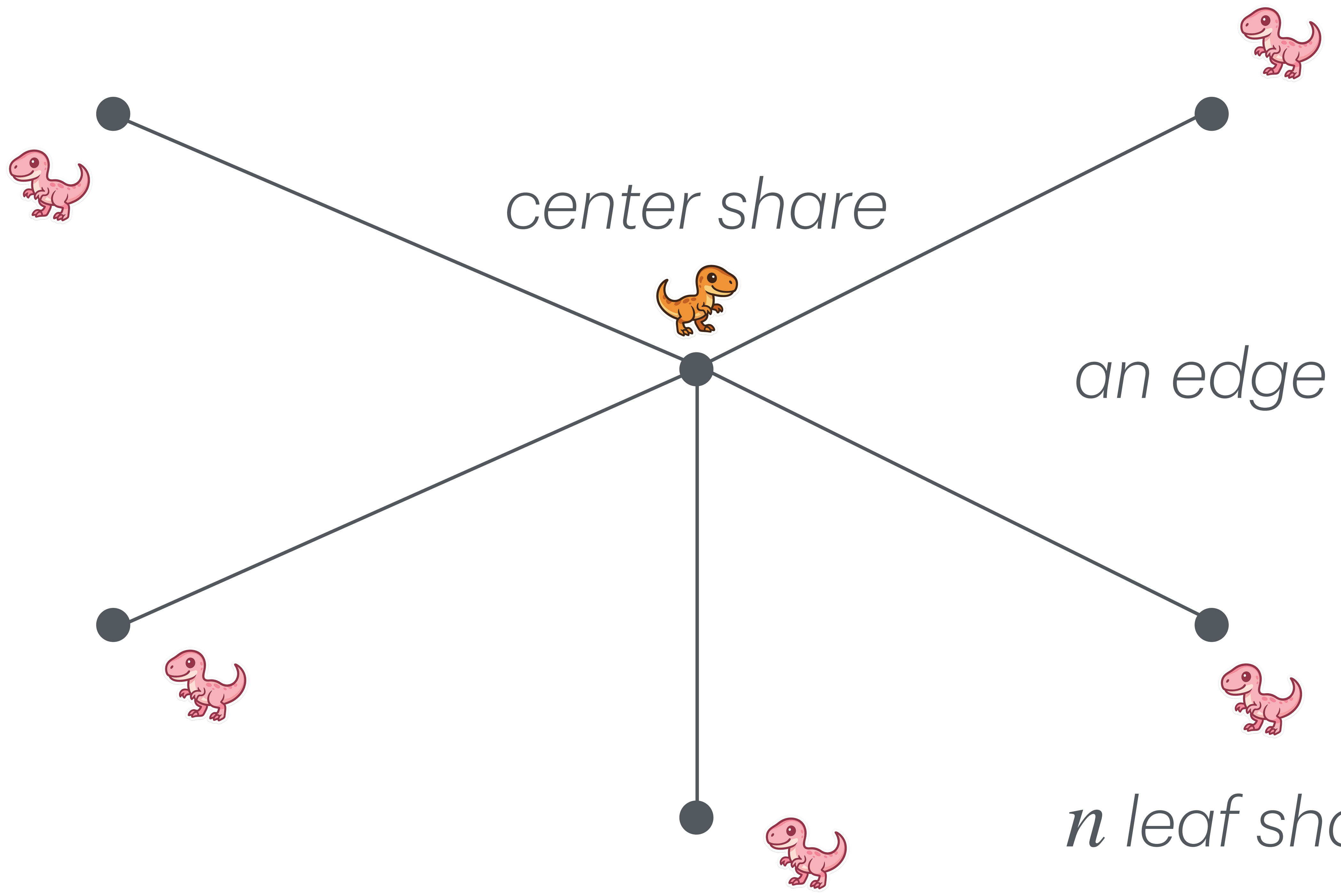


A Linear Lower Bound for U-FASS

Secrecy: Every leaf share must have at least one bit of entropy.

U-Anonymity: Leaf shares are conditionally independent.

Correctness: The central node can reconstruct from any of the leaf shares.



center share

an edge = min. authorized set

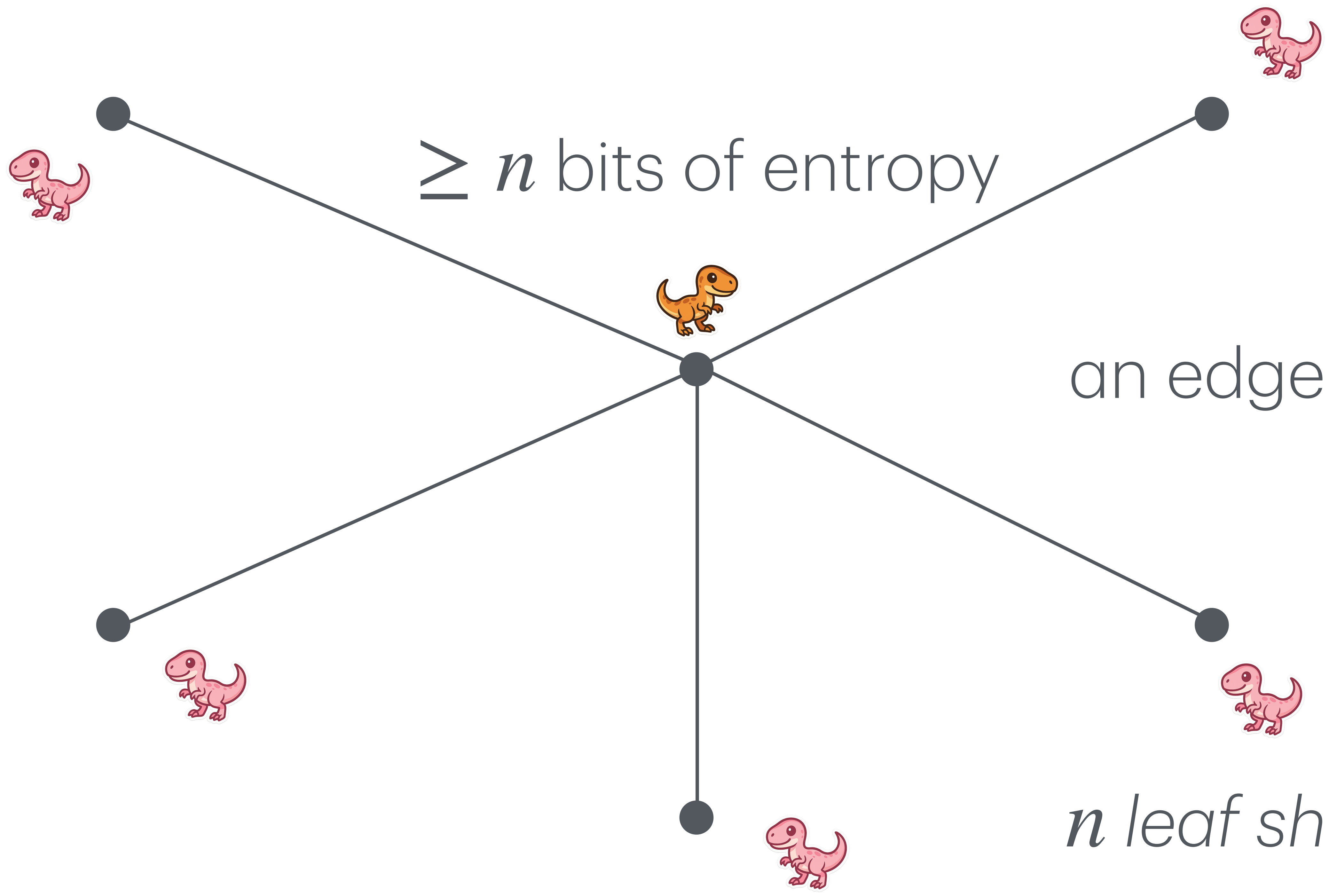
n leaf shares

A Linear Lower Bound for U-FASS

Secrecy: Every leaf share must have at least one bit of entropy.

U-Anonymity: Leaf shares are conditionally independent.

Correctness: The central node can reconstruct from any of the leaf shares.



$\geq n$ bits of entropy

an edge = min. authorized set

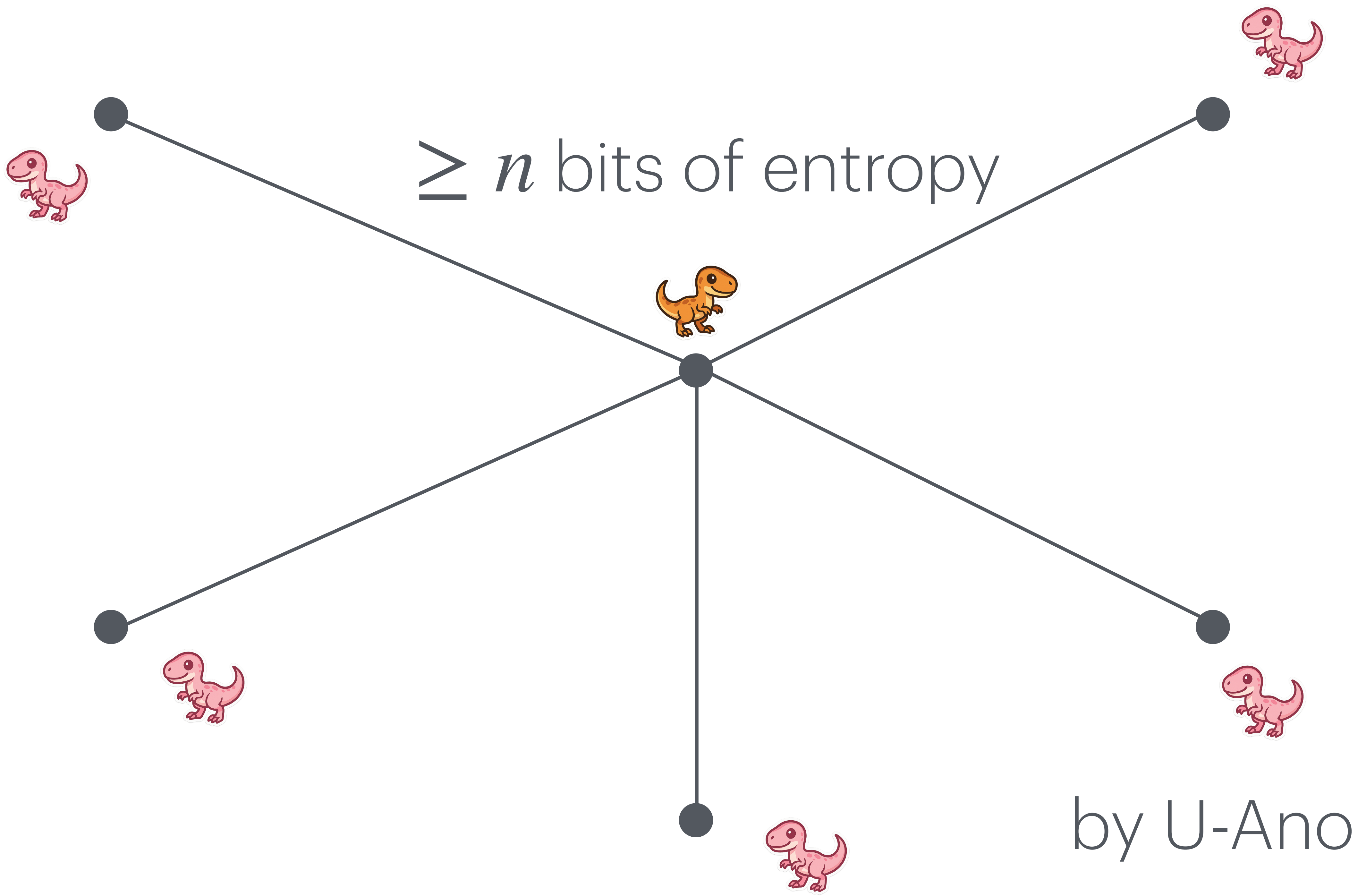
n leaf shares

A Linear Lower Bound for U-FASS

Secrecy: Every leaf share must have at least one bit of entropy.

U-Anonymity: Leaf shares are conditionally independent.

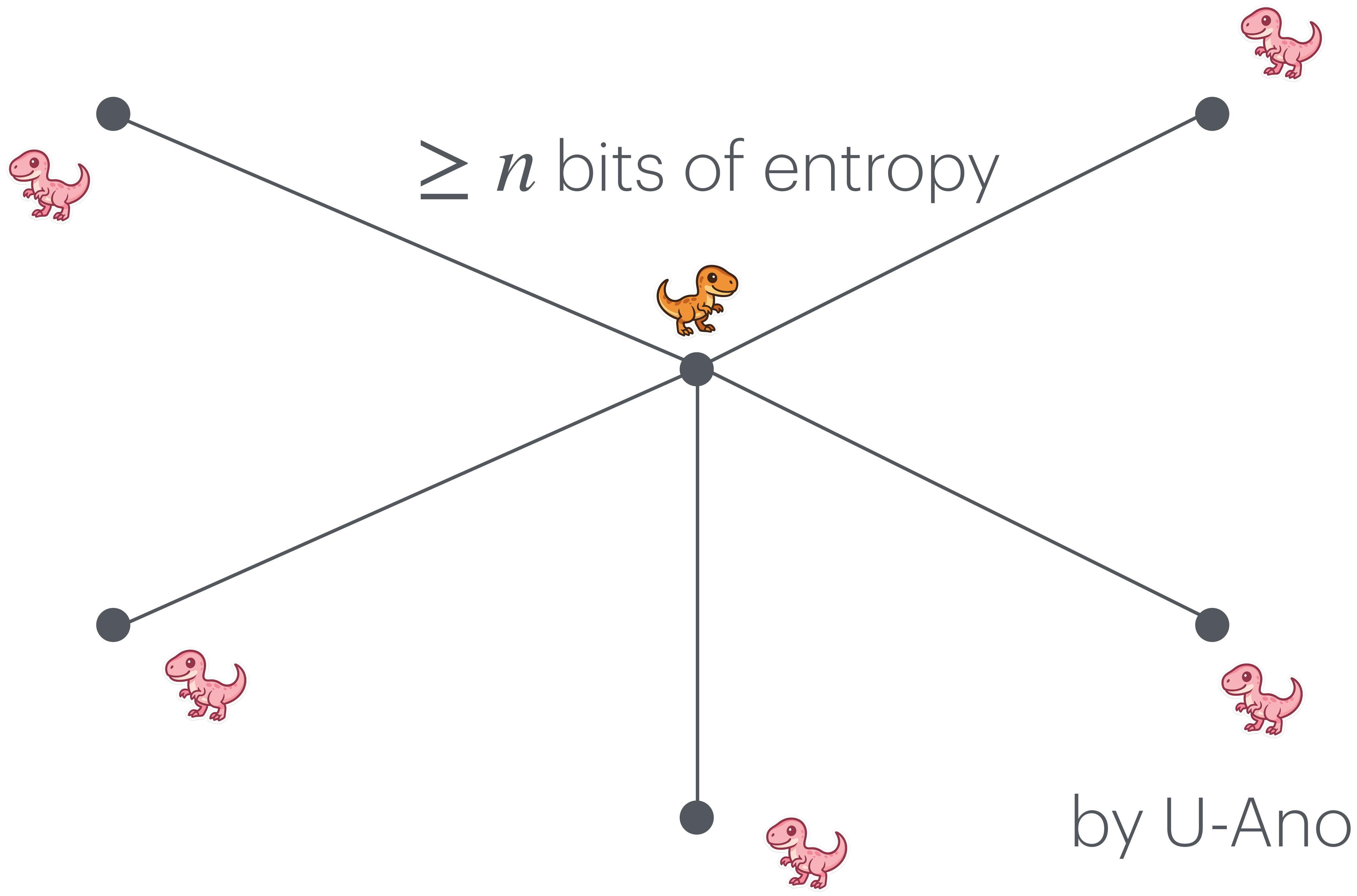
Correctness: The central node can reconstruct from any of the leaf shares.



by U-Anonymity $\geq n$ bits of entropy

A Linear Lower Bound for U-FASS

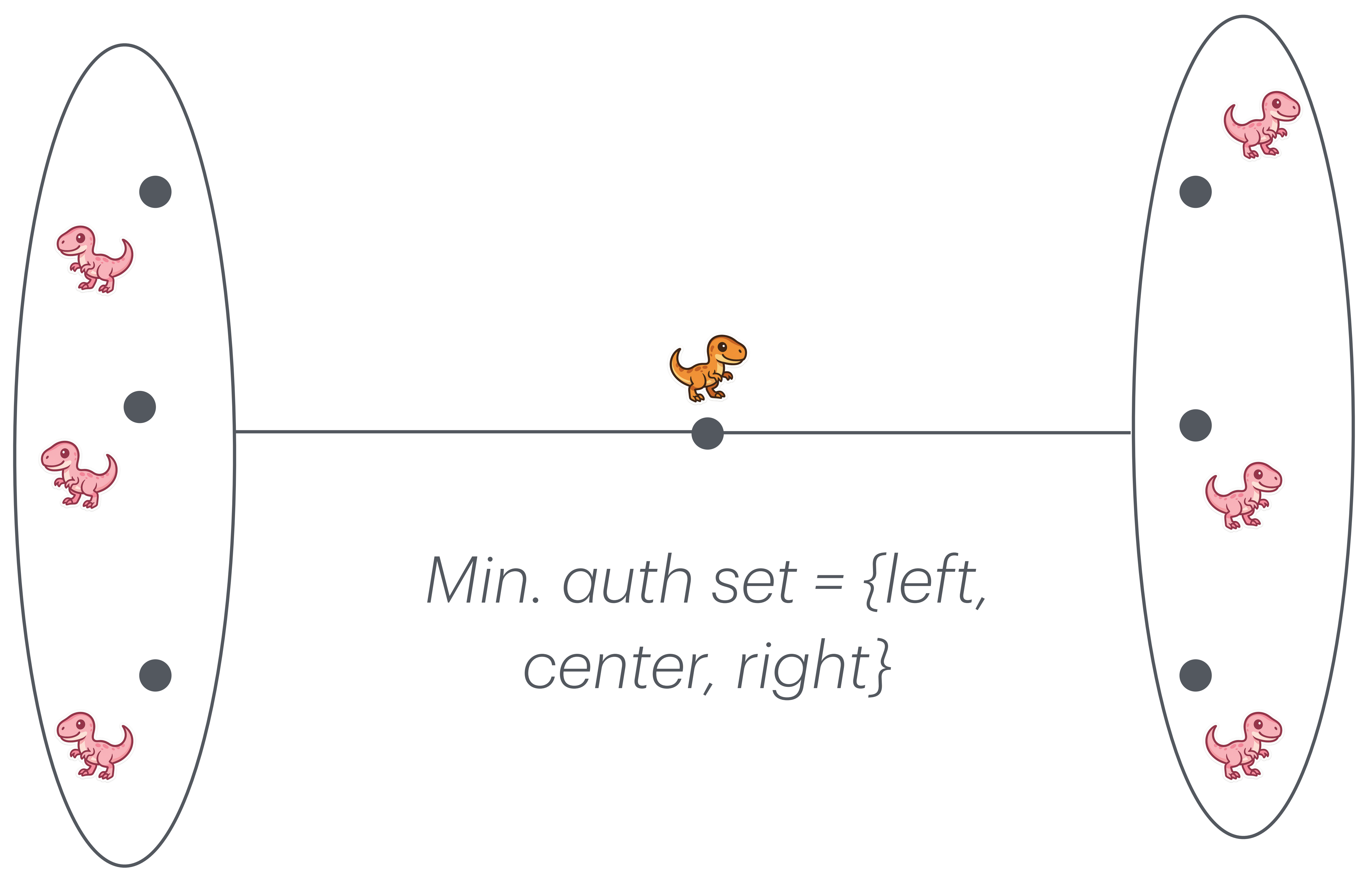
Conclusion: For any U-FASS scheme for the star-graph with $O(n)$ parties, the per-party share size is at least $\Omega(n)$ bits. (*N.B.*, there's a 1-bit solution for S-FASS).



by U-Anonymity $\geq n$ bits of entropy

A Quadratic Lower Bound for U-FASS

Now consider the $(2,n)$-star graph access structure.



n *left leaf shares*

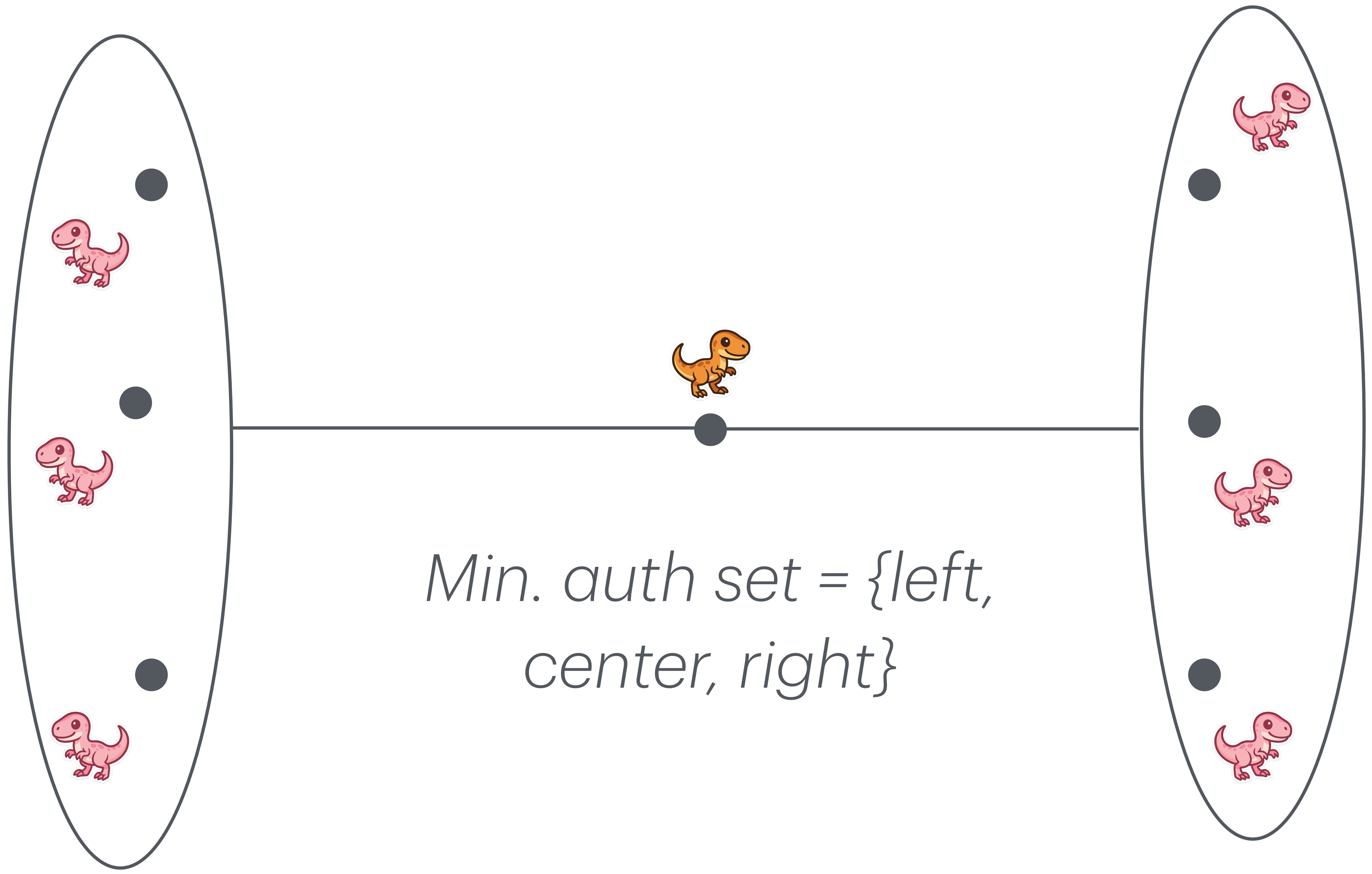
Min. auth set = {left, center, right}

n *right leaf shares*

A Quadratic Lower Bound for U-FASS

By prior argument, left and right shares each have at least $\Omega(n)$ bits of entropy.

Apply the prior argument again to show that center node has $\Omega(n^2)$ bits of entropy.



n left leaf shares

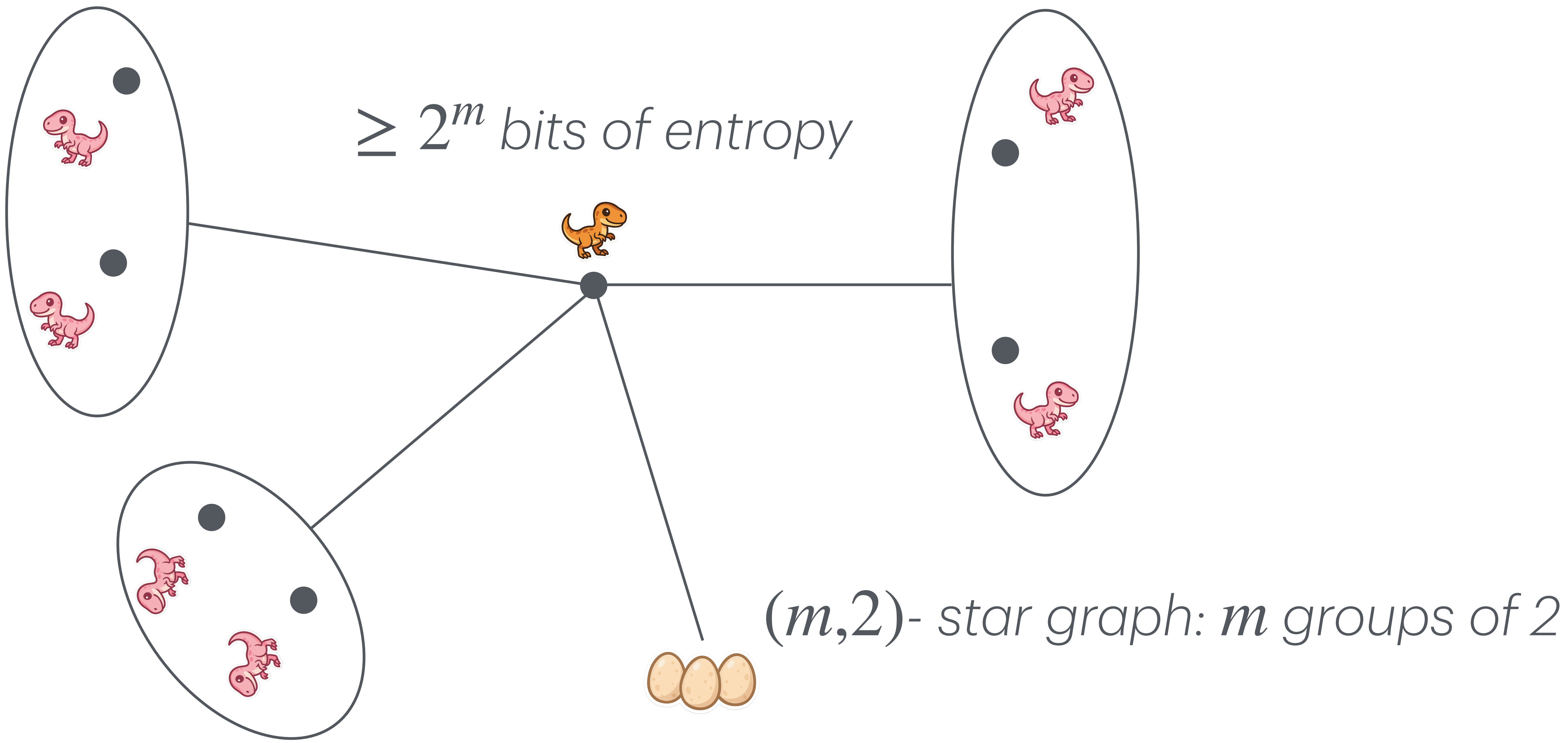
Min. auth set = {left, center, right}

n right leaf shares

An Exponential Lower Bound for U-FASS

Argument extends to (m, k) star graph for any $m, k \in \mathbb{N}$.

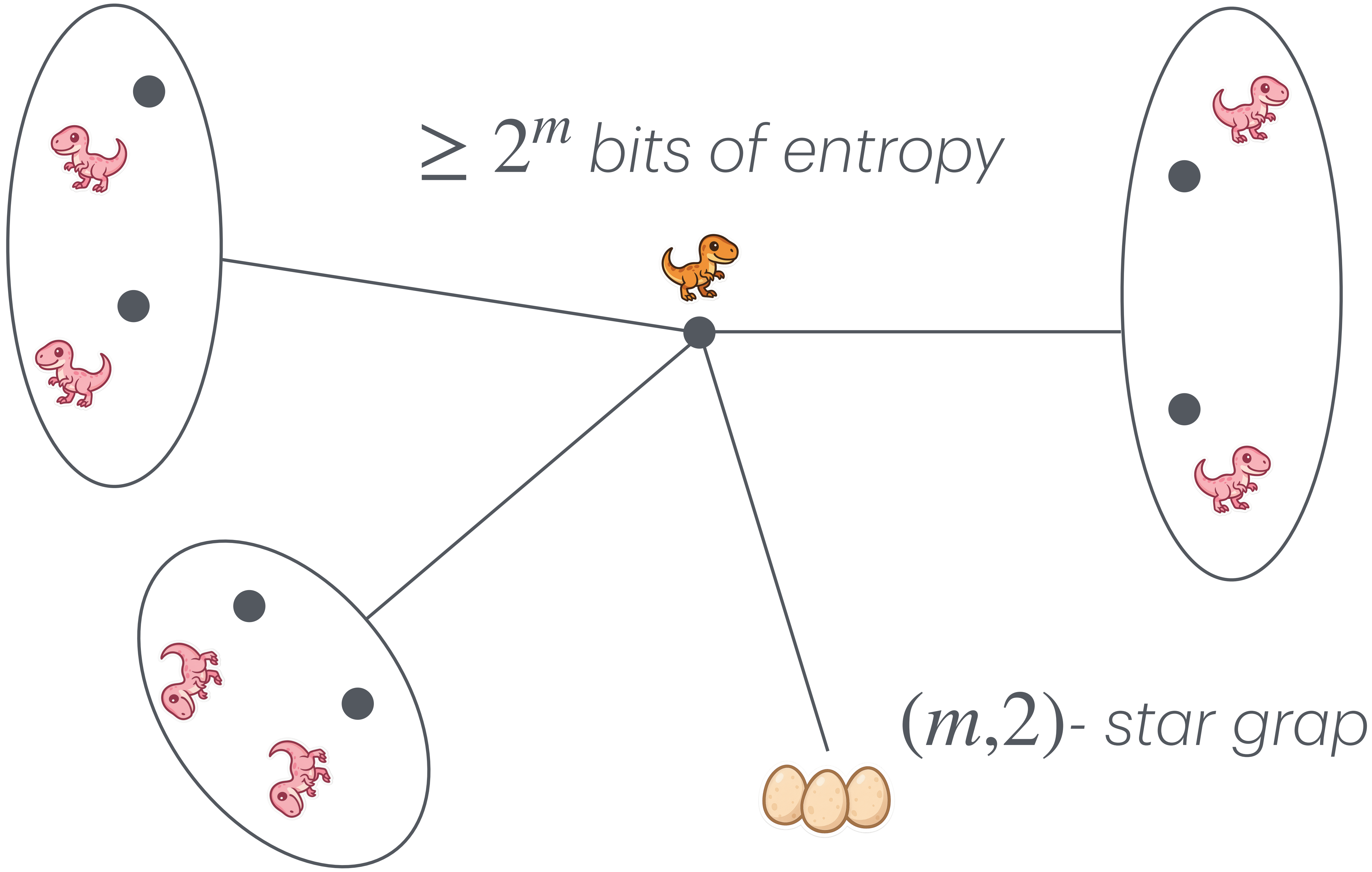
- lower bound of $\Omega(k^m)$ bits per-party.


$\geq 2^m$ *bits of entropy*
$(m,2)$- *star graph:* m *groups of 2*

An Exponential Lower Bound for M-FASS

Argument extends to (m, k) star graph for any $m, k \in \mathbb{N}$.

- lower bound of $\Omega(k^m)$ bits per-party.
- extends to M-FASS.



$(m,2)$*- star graph:* m *groups of 2*

Near-Optimal Information-Theoretic U-FASS

$$x_1 \wedge \cdots \wedge x_t.$$

- Sample random linearly independent vectors $\mathbf{v}_2, \ldots, \mathbf{v}_n \in \mathbb{F}^{n-1}$.

  Set $\mathbf{v}_1 = (s+1) \cdot \mathbf{v}_2 + \sum_{i=3}^{t} \mathbf{v}_i$.

- Party i's share is $\mathbf{v}_i$.

Per-party Share-size: $\tilde{O}(\ell n)$ where ℓ is the number of minterms.

Near-Optimal Information-Theoretic U-FASS

$$x_1 \wedge \cdots \wedge x_t.$$

- Sample uniform random vectors $\mathbf{v}_2, \ldots, \mathbf{v}_n \in \mathbb{F}^{t_{\max}-1}$. Set $$\mathbf{v}_1 = (s+1)\cdot\mathbf{v}_2 + \sum_{i=3}^{t}\mathbf{v}_i.$$

- Append $\mathbf{v}_i$ to party i's share.

Per-party Share-size: $\tilde{O}(\ell\, t_{\max})$ where ℓ is the number of minterms and $t_{\max}$ is maximum degree of any minterm.

Open Questions

- Does there exist information-theoretic FASS scheme for threshold access structures with perfect correctness and perfect U-Anonymity?
  - In the ramp (gap-threshold) setting, yes—[Con ‘25].
  - Simplest open case—$(3,5)$ threshold.
- Can you obtain a computationally efficient information-theoretic S-FASS scheme for the weighted threshold access structure?
  - Standard virtualization approach of Shamir’s secret sharing fails to achieve even S-Anonymity. Padding may break correctness.
- Are one-way functions sufficient for general computational FASS schemes?
- Does efficient computational U-FASS for CNFs imply any public-key primitives?

Thank you!

Appendix: Improved Info-theoretic Upper Bound

Information-Theoretic U-FASS

[Paskin-Cherniavsky, Olimid ‘20] Information-theoretic solution:
Freshly share the secret for each minterm!

Information-Theoretic U-FASS

[Paskin-Cherniavsky, Olimid ‘20] Information-theoretic solution:
Freshly share the secret for each minterm!

We’ll present a large-field version of their scheme.

Information-Theoretic U-FASS

[Paskin-Cherniavsky, Olimid ‘20] Information-theoretic solution:
Freshly share the secret for each minterm!

We’ll present a large-field version of their scheme.

$$x_1 \vee (x_2 \wedge x_3).$$

Information-Theoretic U-FASS

[Paskin-Cherniavsky, Olimid ‘20] Information-theoretic solution:
Freshly share the secret for each minterm!

We’ll present a large-field version of their scheme.

$$x_1 \vee (x_2 \wedge x_3).$$

Can ignore degree one minterms without affecting correctness, secrecy, nor anonymity. Give party 1 the secret.

Information-Theoretic U-FASS

[Paskin-Cherniavsky, Olimid '20] Information-theoretic solution:
Freshly share the secret for each minterm!

We'll present a large-field version of their scheme.

$$x_2 \wedge x_3.$$

Information-Theoretic U-FASS

[Paskin-Cherniavsky, Olimid '20] Information-theoretic solution:
Freshly share the secret for each minterm!

We'll present a large-field version of their scheme.

$$x_2 \wedge x_3.$$

Modifying an elegant solution from PO'20:

- Sample random linearly independent vectors $\mathbf{v}_1, \mathbf{v}_2 \in \mathbb{F}^2$. Set $\mathbf{v}_3 = (s+1) \cdot \mathbf{v}_2$.

- Append $\mathbf{v}_i$ to Party i's share.

Near-Optimal Information-Theoretic U-FASS

$$x_1 \wedge \cdots \wedge x_t.$$

- Sample uniform random vectors $\mathbf{v}_2, \ldots, \mathbf{v}_n \in \mathbb{F}^{t_{\max}-1}$. Set

$$\mathbf{v}_1 = (s+1) \cdot \mathbf{v}_2 + \sum_{i=3}^{t} \mathbf{v}_i.$$

- Append $\mathbf{v}_i$ to party i's share.

Per-party Share-size: $\tilde{O}(\ell t_{\max})$ where ℓ is the number of minterms and $t_{\max}$ is maximum degree of any minterm.

Statistical Correctness: Find a linear dependent set of a specific size for each minterm.

Perfect U-Anonymity: Uniform random vectors!

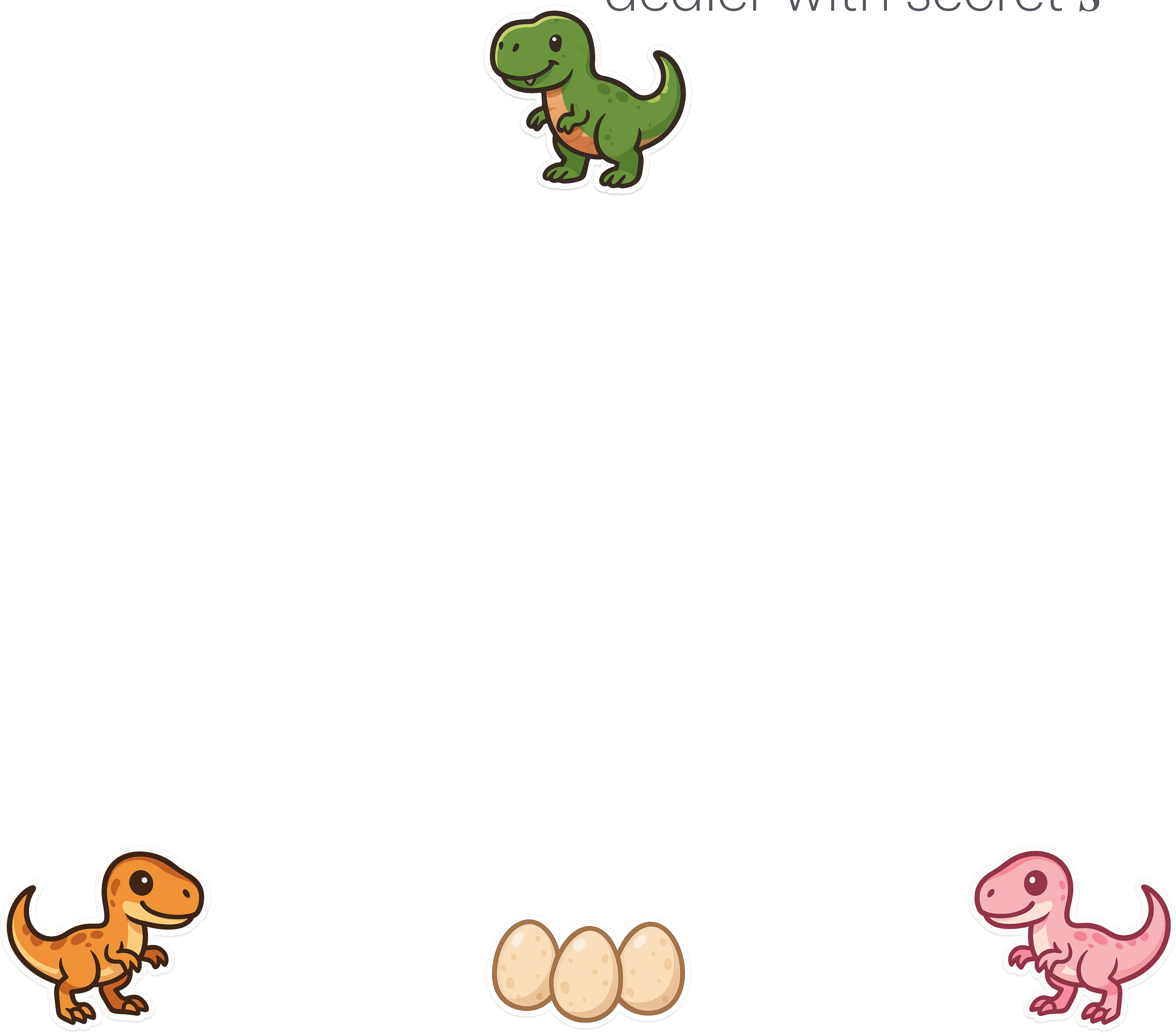
Appendix: Computational Compiler

Briefly: Our Computational Contributions

Computational Contributions:

- A **generic compiler** from any secret sharing scheme (with info-theoretic or computational secrecy) *for any monotone access structure* to a computational M-fully anonymous secret sharing scheme for the same access structure.
  - Preserves the share size of the underlying scheme.
  - Secrecy based on the hardness of LWE.

Consider any monotone access structure $\mathscr{A}$.



dealer with secret s

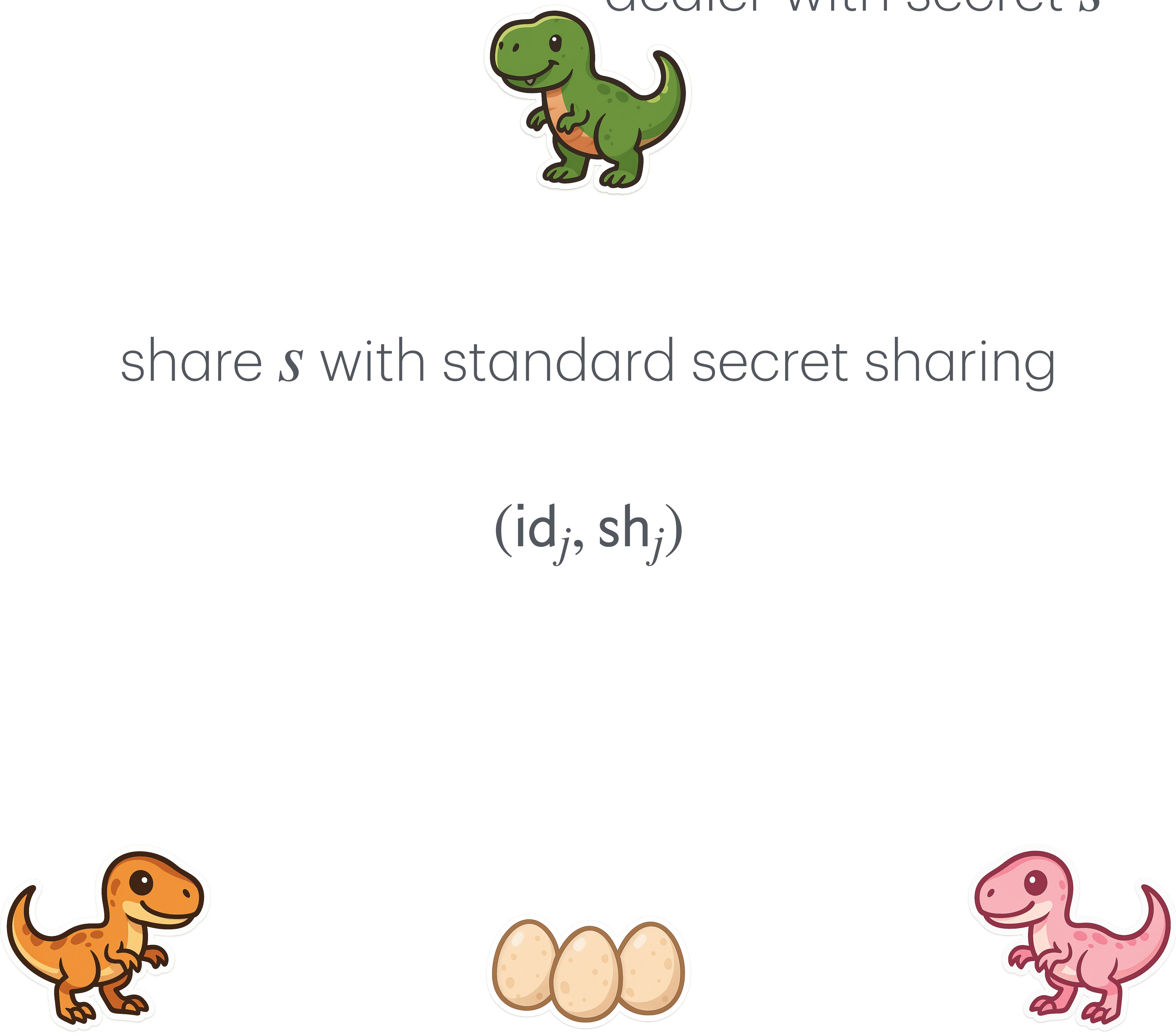
n parties

Briefly: Our Computational Contributions

Computational Contributions:

- A **generic compiler** from any secret sharing scheme (with info-theoretic or computational secrecy) *for any monotone access structure* to a computational fully anonymous secret sharing scheme for the same access structure.
  - Preserves the share size of the underlying scheme.
  - Secrecy based on the hardness of LWE.

Consider any monotone access structure $\mathscr{A}$.



dealer with secret s

share s with standard secret sharing

$(\mathsf{id}_j, \mathsf{sh}_j)$

n parties

Briefly: Our Computational Contributions

Computational Contributions:

- A **generic compiler** from any secret sharing scheme (with info-theoretic or computational secrecy) *for any monotone access structure* to a computational fully anonymous secret sharing scheme for the same access structure.
  - Preserves the share size of the underlying scheme.
  - Secrecy based on the hardness of LWE.

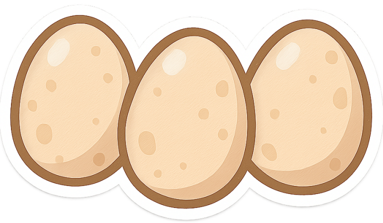
Consider any monotone access structure $\mathscr{A}$.

dealer with secret s

share s with standard secret sharing

$(\mathsf{id}_j, \mathsf{sh}_j)$

not anonymous, so encrypt it.



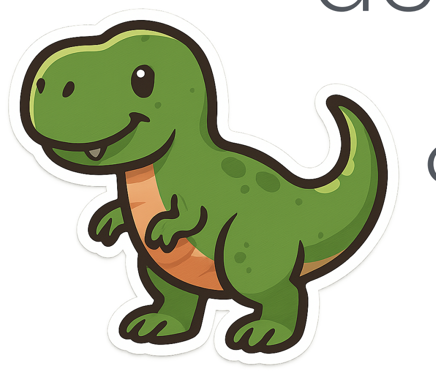
n parties

Briefly: Our Computational Contributions

Computational Contributions:

- A **generic compiler** from any secret sharing scheme (with info-theoretic or computational secrecy) *for any monotone access structure* to a computational fully anonymous secret sharing scheme for the same access structure.
    - Preserves the share size of the underlying scheme.
    - Secrecy based on the hardness of LWE.

Consider any monotone access structure $\mathscr{A}$.



dealer with secret s

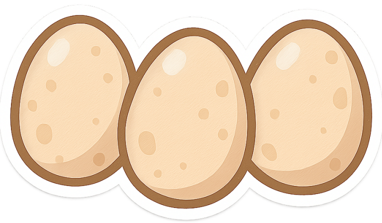
& secret key **sk**

share s with standard secret sharing

$(\mathsf{id}_j, \mathsf{sh}_j)$

not anonymous, so encrypt it.

$\mathsf{Enc}(\mathsf{sk}, \mathsf{Pad}((\mathsf{id}_j, \mathsf{sh}_j)))$



n parties

Briefly: Our Computational Contributions

Computational Contributions:

- A **generic compiler** from any secret sharing scheme (with info-theoretic or computational secrecy) *for any monotone access structure* to a computational fully anonymous secret sharing scheme for the same access structure.
  - Preserves the share size of the underlying scheme.
  - Secrecy based on the hardness of LWE.

Consider any monotone access structure $\mathscr{A}$.

dealer with secret s

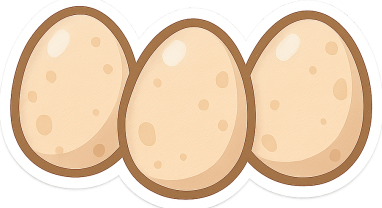
& secret key **sk**

Ideal obfuscation of function $f_{\mathsf{sk},s}$ that

(1) Decrypts input and strips padding.

(2) If reconstructs to s, output s, else output $\perp$.

$\mathsf{Enc}(\mathsf{sk}, \mathsf{Pad}((\mathsf{id}_j, \mathsf{sh}_j)))$



n parties

Briefly: Our Computational Contributions

Computational Contributions:

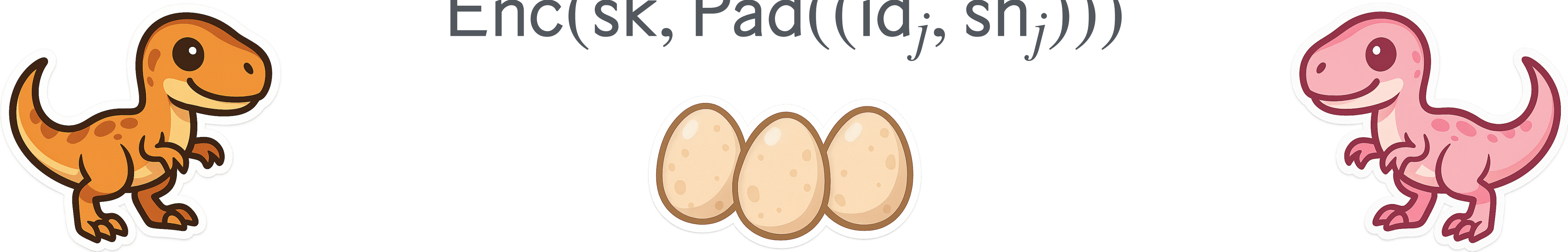
- A **generic compiler** from any secret sharing scheme (with info-theoretic or computational secrecy) *for any monotone access structure* to a computational fully anonymous secret sharing scheme for the same access structure.
  - Preserves the share size of the underlying scheme.
  - **Secrecy based on the hardness of LWE**.

Consider any monotone access structure $\mathscr{A}$.

dealer with secret s

& secret key **sk**

A variation using **Compute-and-compare Obfuscation** [Wichs, Zerdelis '17, Goyal, Koppula, Waters '17].



$\mathsf{Enc}(\mathsf{sk}, \mathsf{Pad}((\mathsf{id}_j, \mathsf{sh}_j)))$

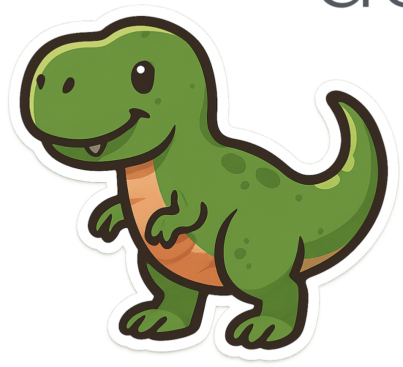
n parties

Briefly: Our Computational Contributions

Computational Contributions:

- A **generic compiler** from any secret sharing scheme (with info-theoretic or computational secrecy) *for any monotone access structure* to a computational fully anonymous secret sharing scheme for the same access structure.
  - Preserves the share size of the underlying scheme.
  - **Secrecy based on the hardness of LWE**.

Consider any monotone access structure $\mathscr{A}$.

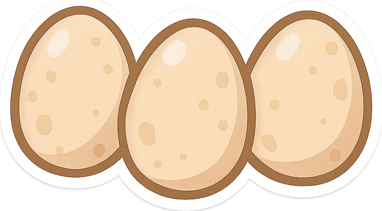


dealer with secret s

& secret key sk

Unbounded Robust Reconstruction: Use secret-key encryption scheme that when decrypting with the wrong key, results in $\perp$. (Minor modification)

$\mathsf{Enc}(\mathsf{sk}, \mathsf{Pad}((\mathsf{id}_j, \mathsf{sh}_j)))$



n parties