New Constructions of Collapsing Hashes

Mark Zhandry (NTT Research & Princeton University)

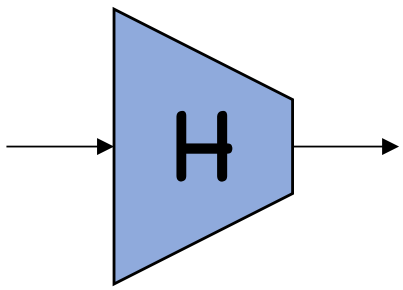
AND

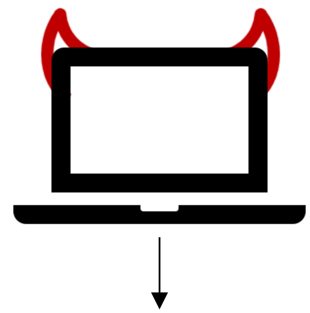
The Gap Is Sensitive to Size of Preimages:

Collapsing Property Doesn't Go Beyond Quantum Collision-Resistance for Preimages Bounded Hash Functions

Shujiao Cao (Chinese Academy of Sciences)
Rui Xue (Chinese Academy of Sciences)

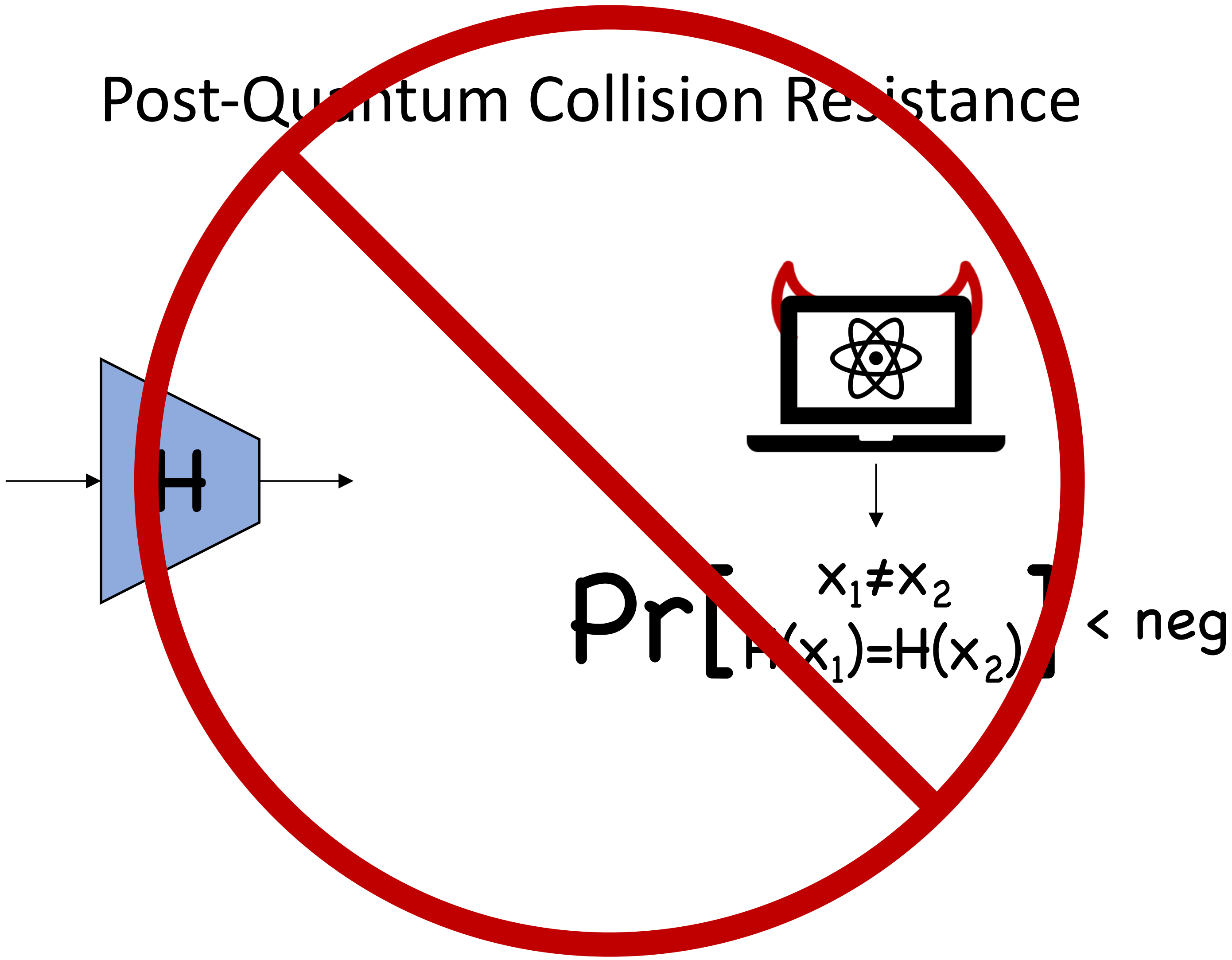
Classical Collision Resistance





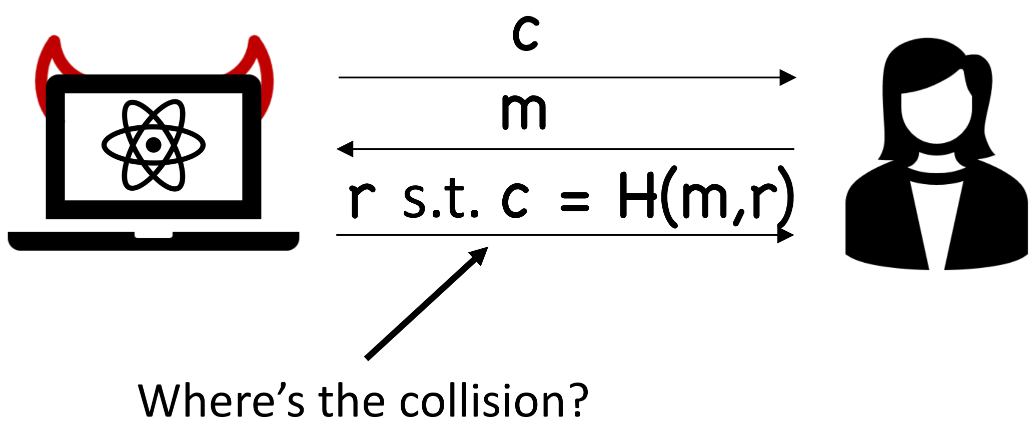
$$\Pr\left[\begin{matrix} x_1 \neq x_2 \\ H(x_1) = H(x_2) \end{matrix}\right] < \text{negl}$$

Q: What security should hash functions satisfy when adversary is quantum?



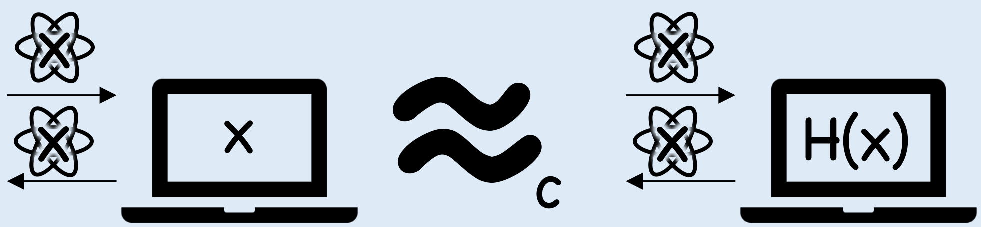
Post-Quantum Collision Resistance
H
$Pr[x_1 \neq x_2, H(x_1)=H(x_2)] < negl$

Thm [Ambainis-Rosmanis-Unruh'14,Unruh'16a]:
∃ PQ-CRHF that is not binding as a commitment (relative to an oracle)



Classically, generate collision via rewinding.
Rewinding problematic quantumly

Def [Unruh'16a]: Collapsing



Intuition: if H were injective, measuring x and H(x) both fully collapse input state. Collapsing says compressing H "as good as" injective

Now widely regarded as "right" notion of security for post-quantum hashing

What was previously known?

Thm [Unruh'16a]: Random oracles are collapsing

Thm [Unruh'16b, Liu-Z'19]: LWE → Lossiness → Collapsing

Thm [Z'19]: Non-collapsing PQ-CRHF → quantum lightning/money (notoriously hard to construct)

Thm [Ambainis-Rosmanis-Unruh'14, Unruh'16a]: $\exists$ non-collapsing CRHF relative to *oracle*

Extreme 1: All standard-model PQ-CRHFs are collapsing?

Frustratingly wide gap

Extreme 2: *Only* standard-model collapsing hashes are LWE/lossy based?

Results of Cao-Xue'22
(concurrent and independent)

Thm [Cao-Xue'22]: $\exists$ collapsing hashes assuming an "almost regular" PQ-CRHF H (even if H itself is not collapsing)

Cor [Cao-Xue'22]: $\exists$ collapsing hashes assuming SIS is quantum hard

Note:
SIS → LWE [Regev'05] → $\exists$ collapsing hashes [Unruh'16b]
SIS *itself* is collapsing if modulus super-poly, assuming LWE [Liu-Z'19]
But [Cao-Xue'22] fundamentally different since no lossiness!

Results of Z'22
(concurrent and independent)

Thm [Z'22]: ∃ collapsing hashes assuming **any** one of the following:

- A "semi-regular" PQ-CRHF (major relaxation of "almost regular")
- Quantum hardness of LPN in essentially same parameter regimes known to imply classical collision resistance
- Quantum hardness of finding short cycles in exponentially large expander graphs (e.g. isogenies over elliptic curves)
- An *optimally* secure PQ-CRHF (no regularity assumed)

Trivial Cor: PQ Statistically hiding commitments and succinct arguments under any of the above assumptions

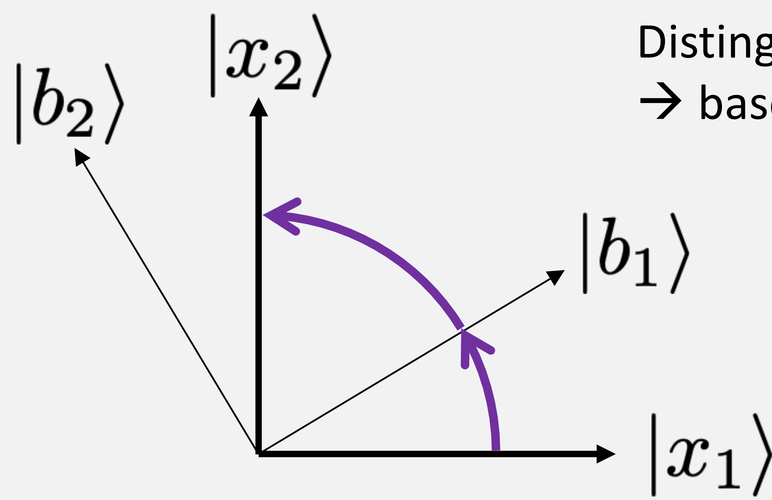
Starting point of both works

Thm [Cao-Xue'22, Z'22]: If H is a PQ-CRHF and is ≤poly-to-1, then H is collapsing

Proof: Measure x, apply distinguisher, then measure x again

$\Longrightarrow$ collision with non-negligible probability

Ex: 2-to-1



Distinguishing advantage
→ bases far apart

x_1, x_2: colliding inputs

$|b_1\rangle$, $|b_2\rangle$: basis for distinguisher

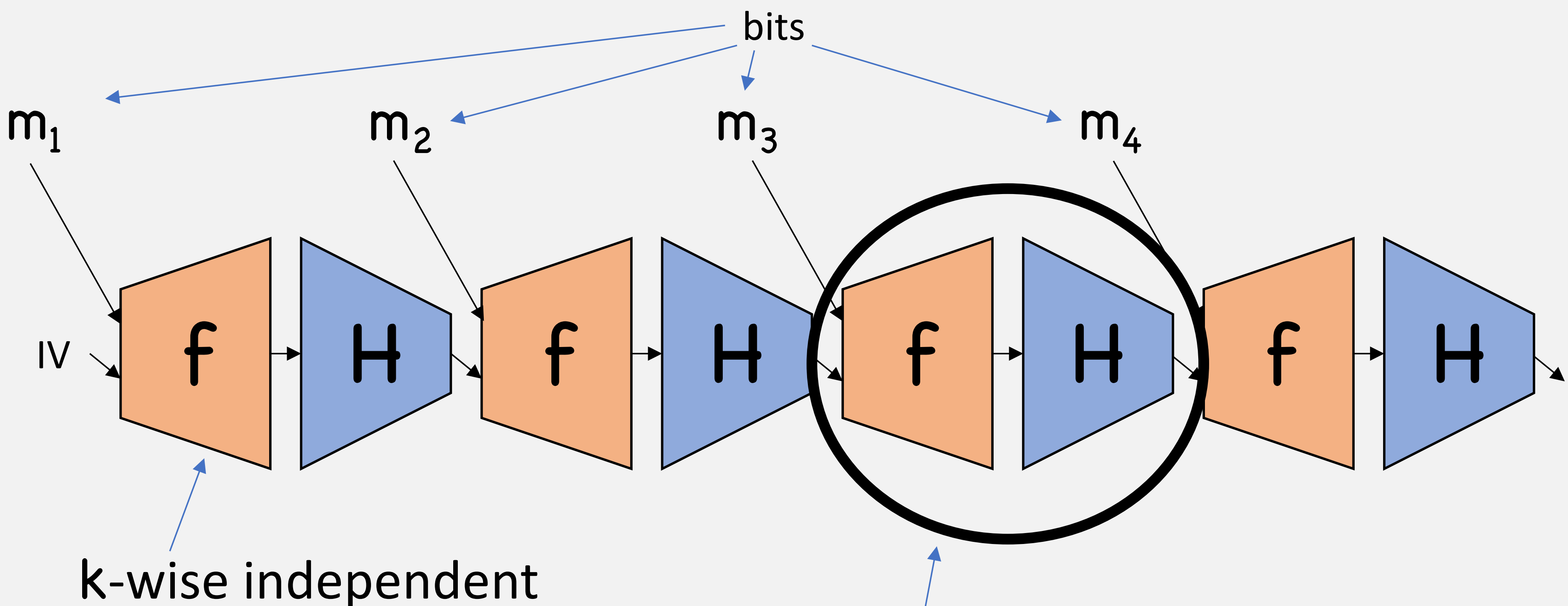
Extension

Thm [Cao-Xue'22]: If H is a PQ-CRHF and is *almost regular*, then $\exists$ collapsing H' built from H

Thm [Z'22]: If H is a PQ-CRHF and is *semi-regular*, then $\exists$ collapsing H' built from H

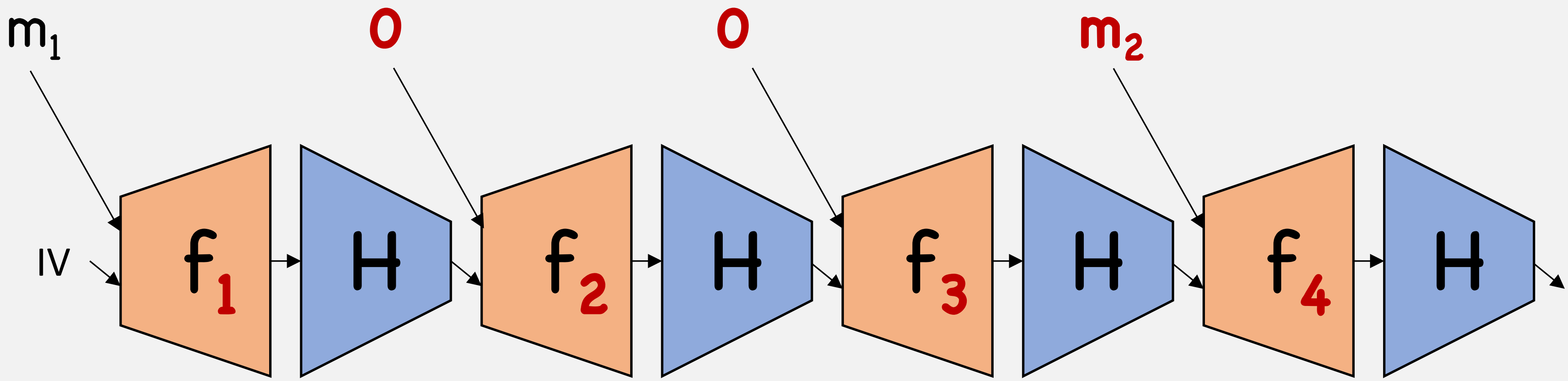
Almost/semi-regular: worst-case number of pre-images "not too far" from "expected"

Proof (Z’22):



Idea: ≤poly-to-1 on image of previous step

Proof (Z'22):

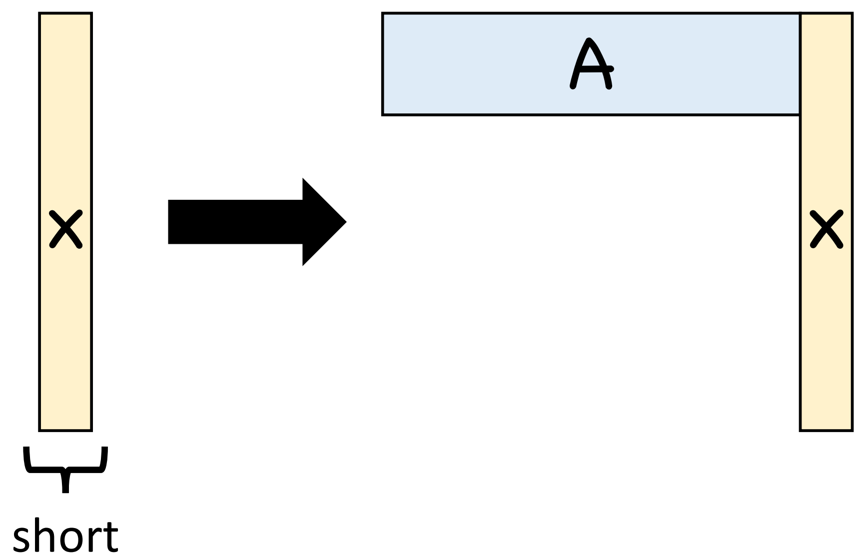


Technicalities...

Applications

SIS hash function

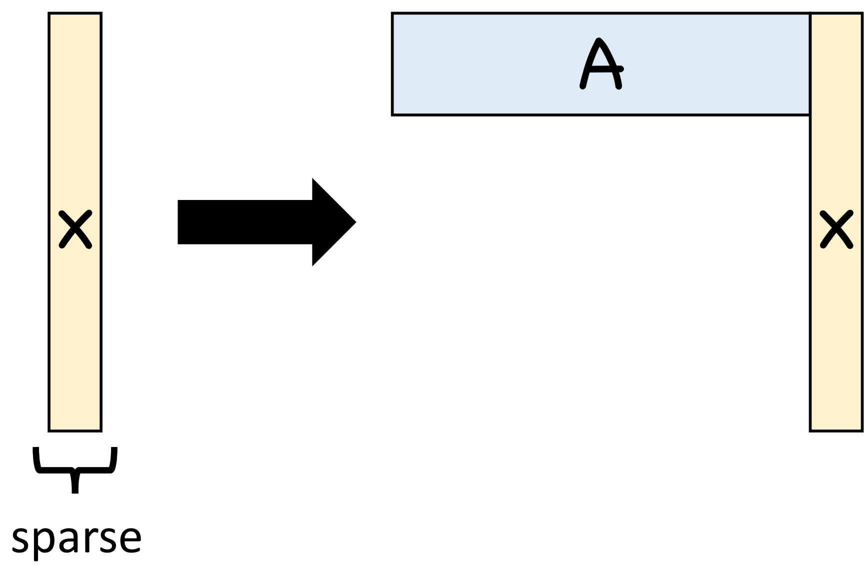
[Ajtai'96]



Thm [Cao-Xue'22]: SIS is *almost* regular in many parameter settings

LPN hashing

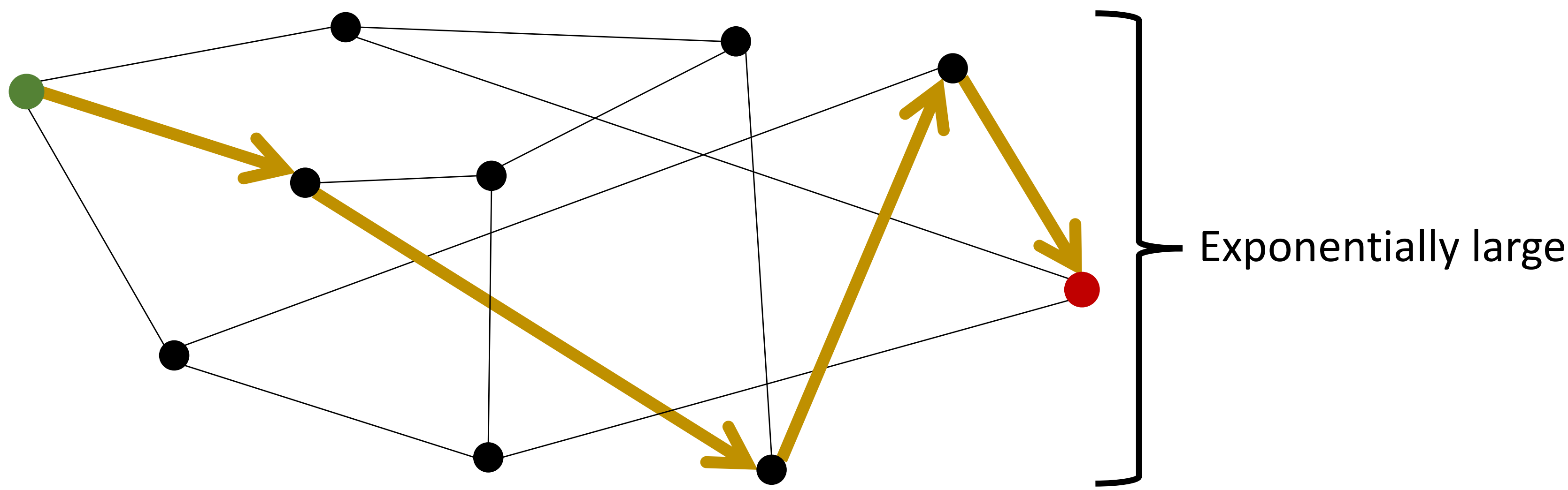
[Brakerski-Lyubashevsky-Vaikuntanathan-Wichs'19, Yu-Zhang-Weng-Guo-Li'19]



Thm [Z'22]: LPN hashing is *semi*-regular in many parameter settings

Expander-based hashing

[Charles-Lauter-Goren’07]



Thm [Alon-Benjamini-Lubetzky-Sodin’07]:
Non-backtracking walks on expanders mix

Cor [Z’22]: Expander hashing is *semi*-regular

Optimal Collision Resistance

Def: $H:\{0,1\}^m \rightarrow \{0,1\}^n$ is *optimally (PQ) collision resistant* if $\Pr[A$ outputs collision$] \leq poly/2^n$

Thm [Z'22]: If $m < n+O(\log n)$ and H is optimally PQ C.R., then H is collapsing

Proof: Optimal C.R. ⟹ hard to find x that collides with with super-poly values ⟹ collapsing by poly-to-1 case

Takeaway: Collapsing is perhaps more prevalent than previously thought

Thanks!