

Adaptive Security in SNARGs via iO and Lossy Functions

Brent Waters
NTT Research,
UT Austin

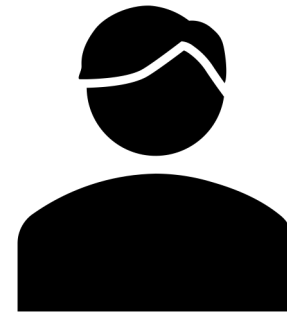
Mark Zhandry
NTT Research

What Are SNARGs?

(Succinct Non-interactive Arguments)



x, w

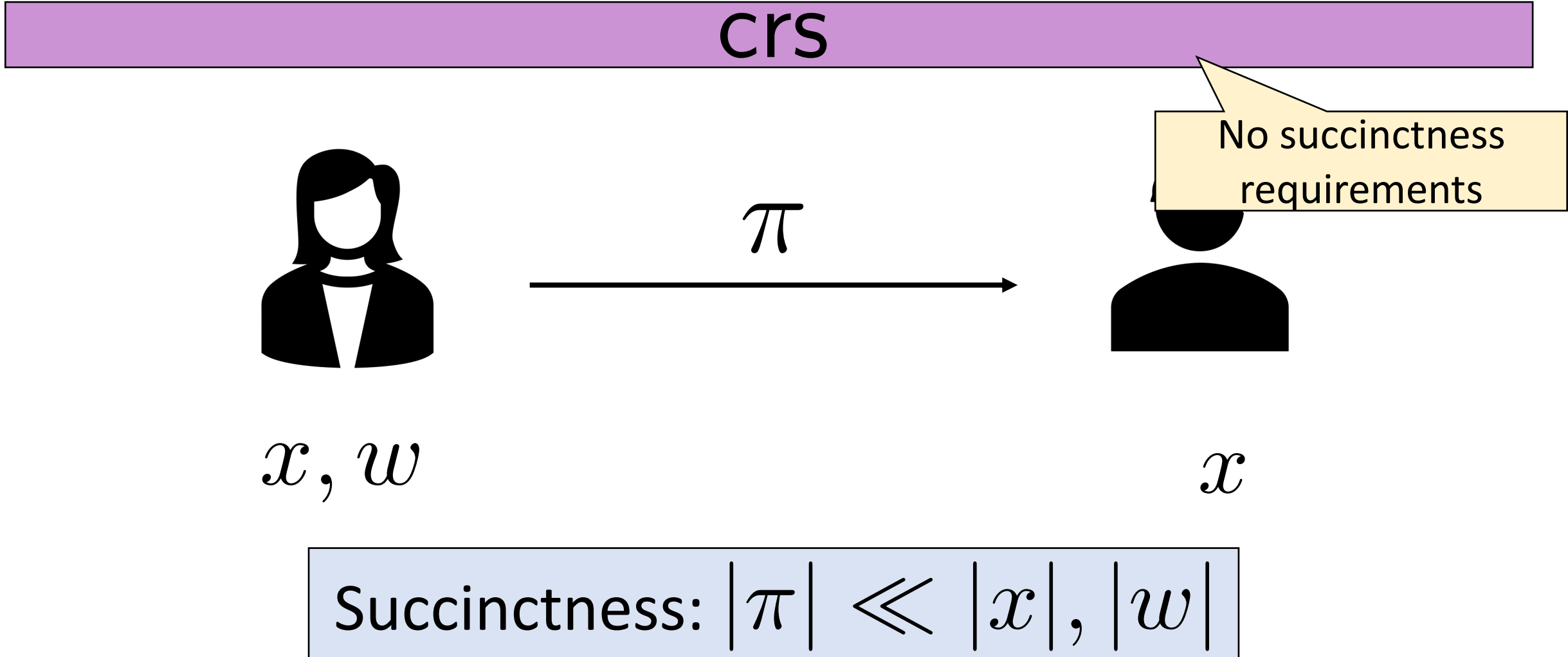


x

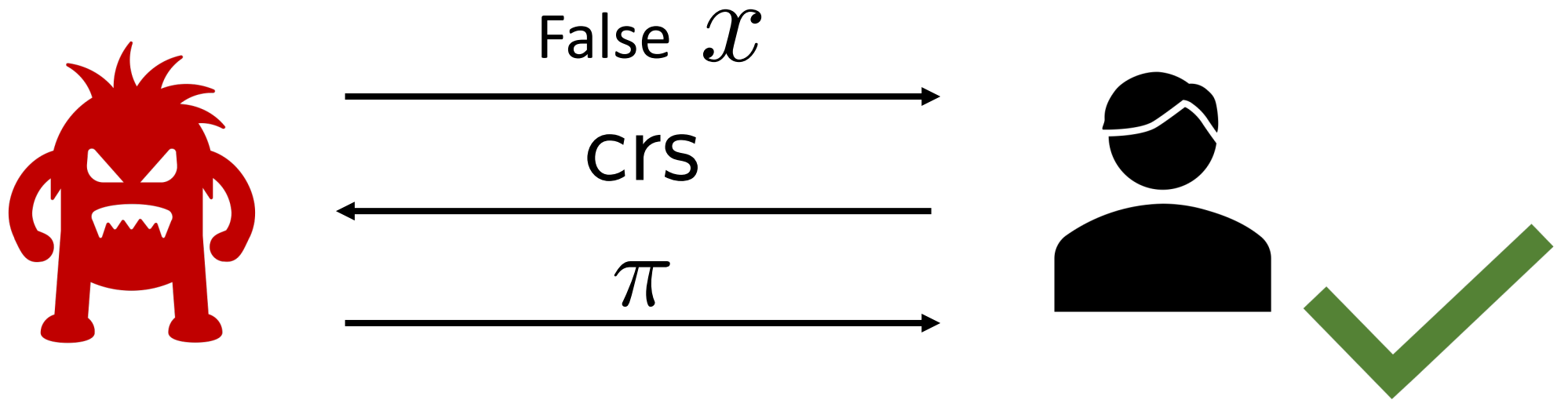
Succinctness: $|\pi| \ll |x|, |w|$

What Are SNARGs?

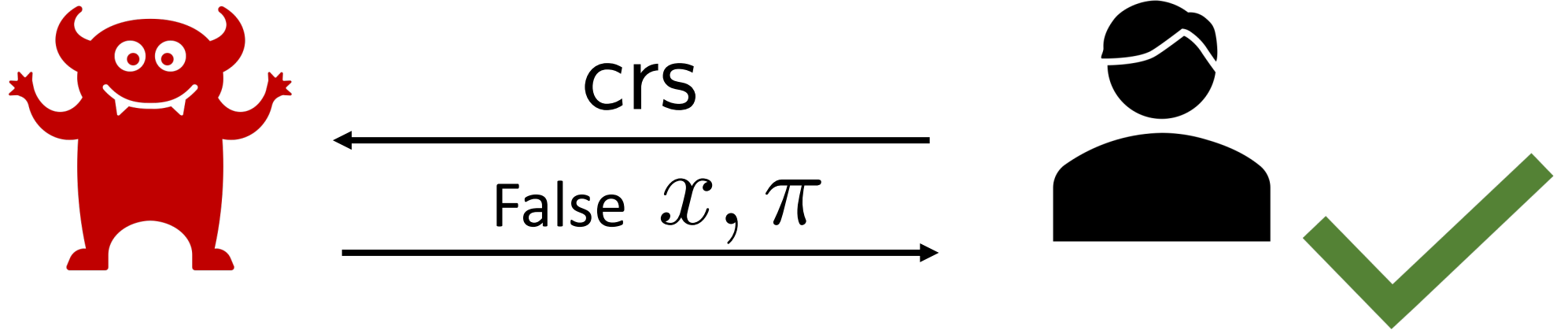
(Succinct Non-interactive Arguments)



Selective Soundness for SNARGs



Adaptive Soundness For SNARGs



Theorem [Waters-Wu'24]: There exists an adaptively sound SNARG for NP, assuming all of the following:

- Subexponentially secure Indistinguishability Obfuscation
- Subexponentially secure One-Way Functions (OWF)
- Polynomially secure **perfectly re-randomizable** OWFs

Known from discrete logs, factoring, or perfect group actions. **Not** known from LWE

Theorem [THIS WORK]: There exists an adaptively sound SNARG for NP, assuming all of the following:

- Subexponentially secure Indistinguishability Obfuscation
- Subexponentially secure One-Way Functions
- *Polynomially secure “**Very**” Lossy Functions*

Theorem [THIS WORK]: $\text{LWE} \rightarrow$ “Very” Lossy Functions

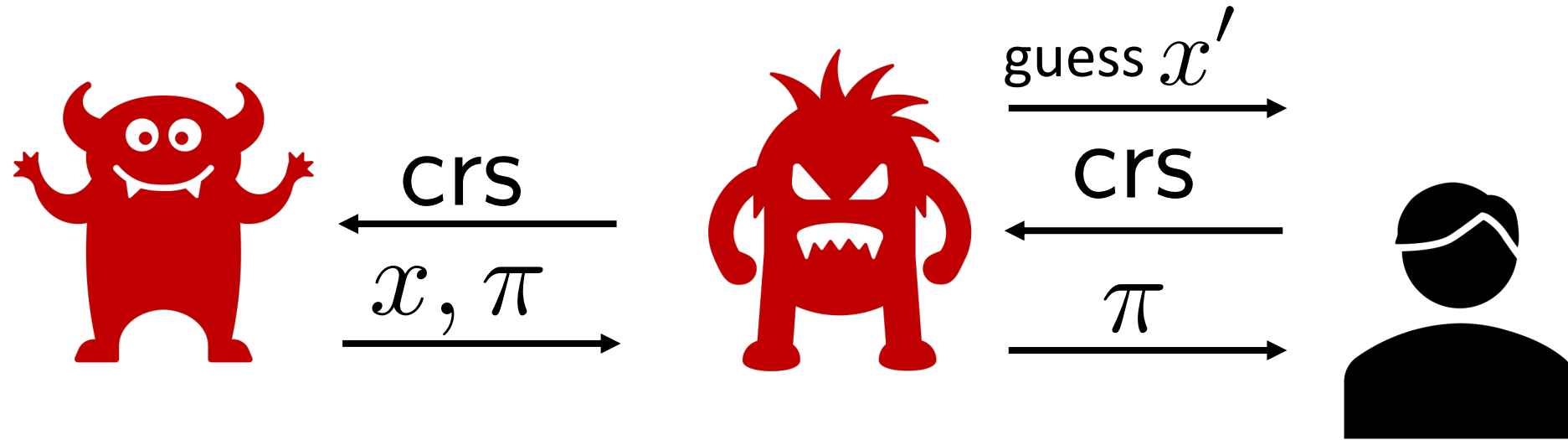
Existing LWE-based lossy functions not very lossy (e.g. [Peikert-Waters’08, Alwen-Krenn-Pietrzak-Wichs’13, Döttling-Garg-Ishai-Malavolta-Mour-Ostrovsky’19, Hofheinz-Hostáková-Kastner-Klein-Ünal’24])

Subsequent Work

Theorem [Waters-Wu'24b]: There exists an adaptively sound SNARG for NP, assuming all of the following:

- Subexponentially secure Indistinguishability Obfuscation
- Subexponentially secure One-Way Functions (OWF)
- ~~Polynomially secure perfectly re-randomizable OWFs~~

On Complexity Leveraging



Wins if $x' = x \quad \Rightarrow \quad \Pr[x' = x] = 2^{-|x|}$

Assume *sub-exponential* selective soundness + set security parameter $\gg |x|$
 \rightarrow even exponentially small success probabilities impossible

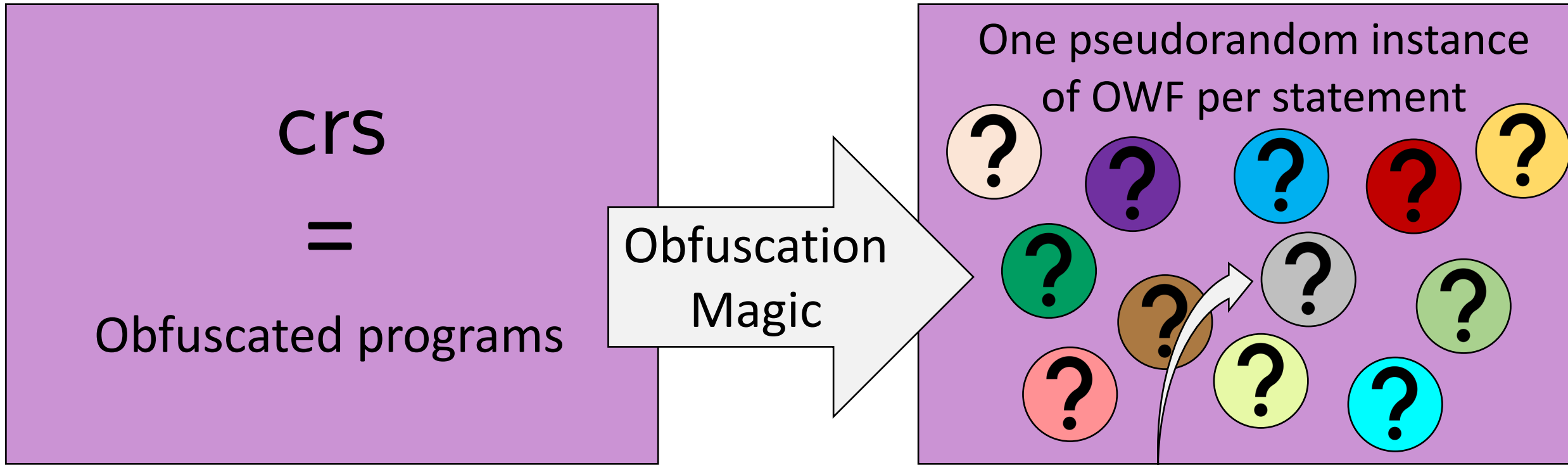
Problem: parameters grow with $|x| \rightarrow$ not succinct!

On Complexity Leveraging

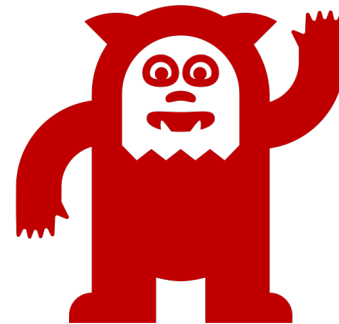
Complexity-leveraging is OK for SNARGs, *but...*

- Any security parameter that appears in π can only absorb losses independent of $|x|$ (though still potentially exponential)
- But can have separate security parameters affecting only the CRS which can absorb losses depending on $|x|$

Waters-Wu First Step: Many OWF Instances

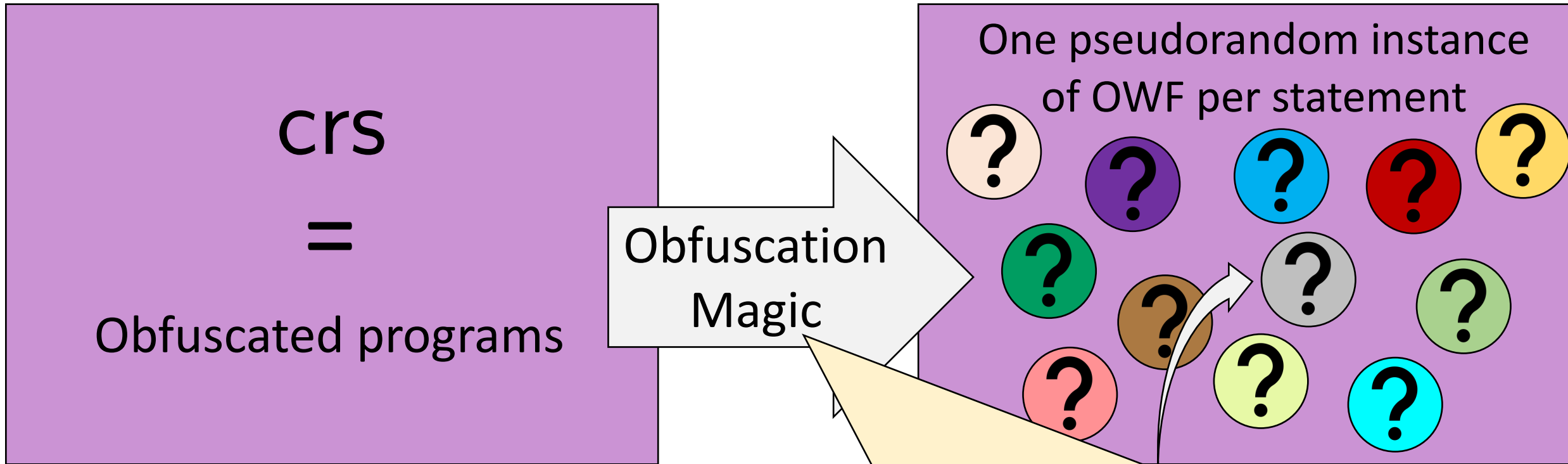


False x, π



$x, \text{💡}$

Waters-Wu First Step: Many OWF Instances



Complexity-leveraging based on the number of statements

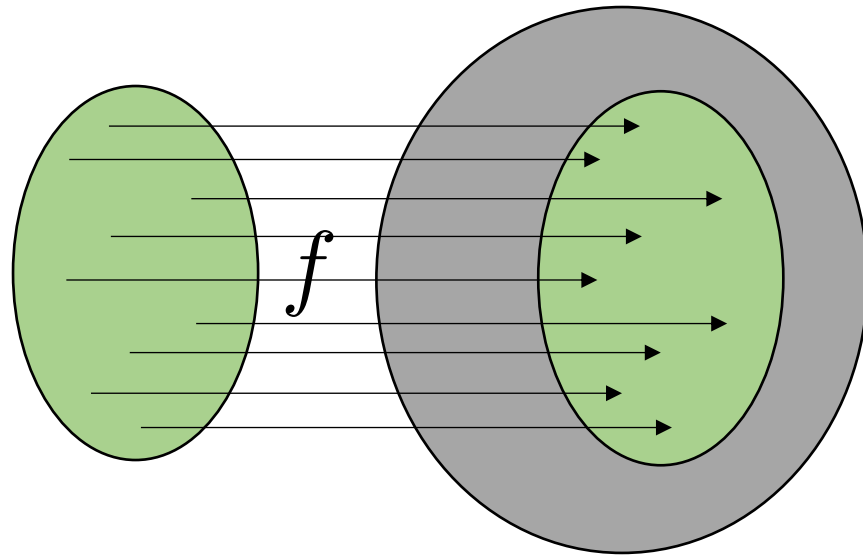
- CRS contains obfuscated programs \rightarrow large CRS
- Only OWF challenges in π , OWF not used yet \rightarrow small π



“Very” Lossy Functions

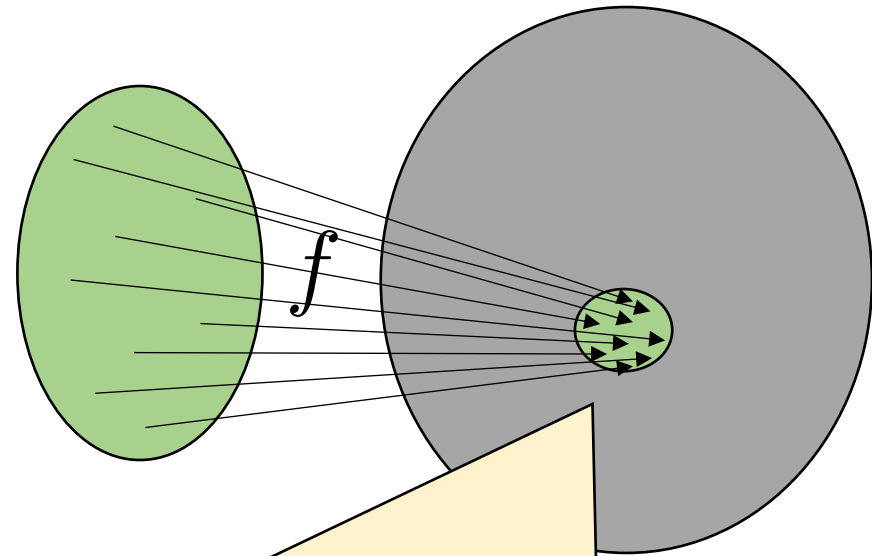
Strengthening of [Peikert-Waters’08]

Injective mode



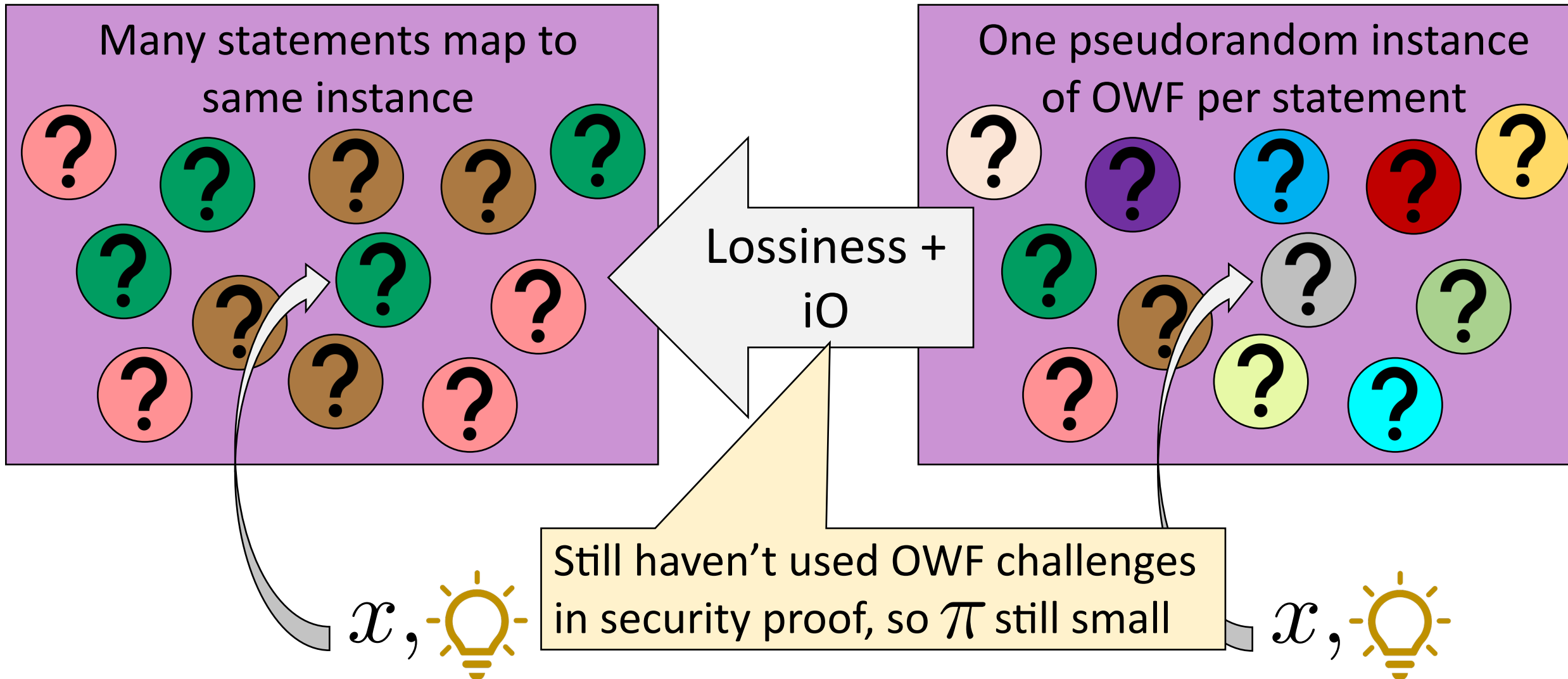
\approx_C

Lossy mode



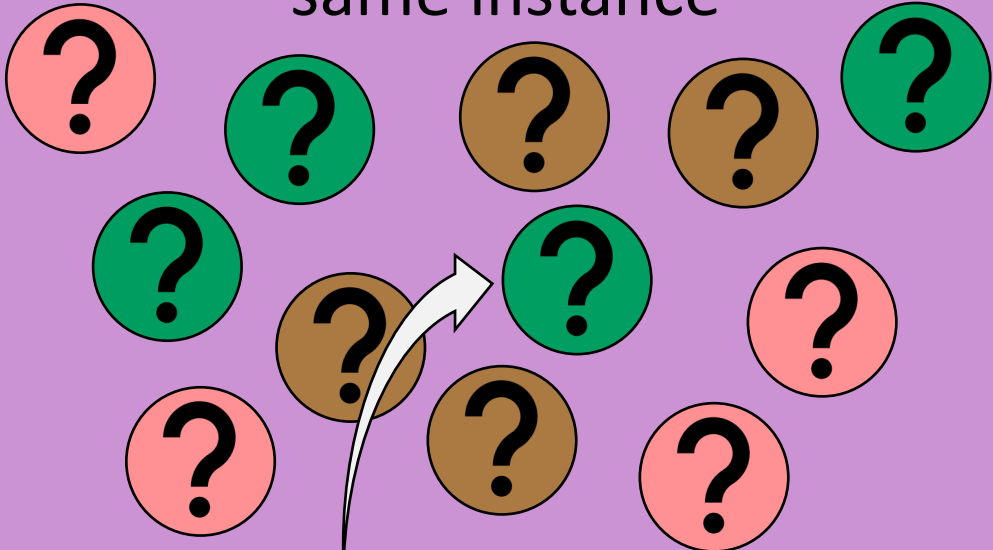
“Very” Lossy: lossy range size = $2^{\text{poly}(\lambda)}$, independent of domain size

Our Idea: Use Lossiness to Complete Proof




Our Idea: Use Lossiness to Complete Proof

Many statements map to
same instance



Now guess OWF instance (not statement)

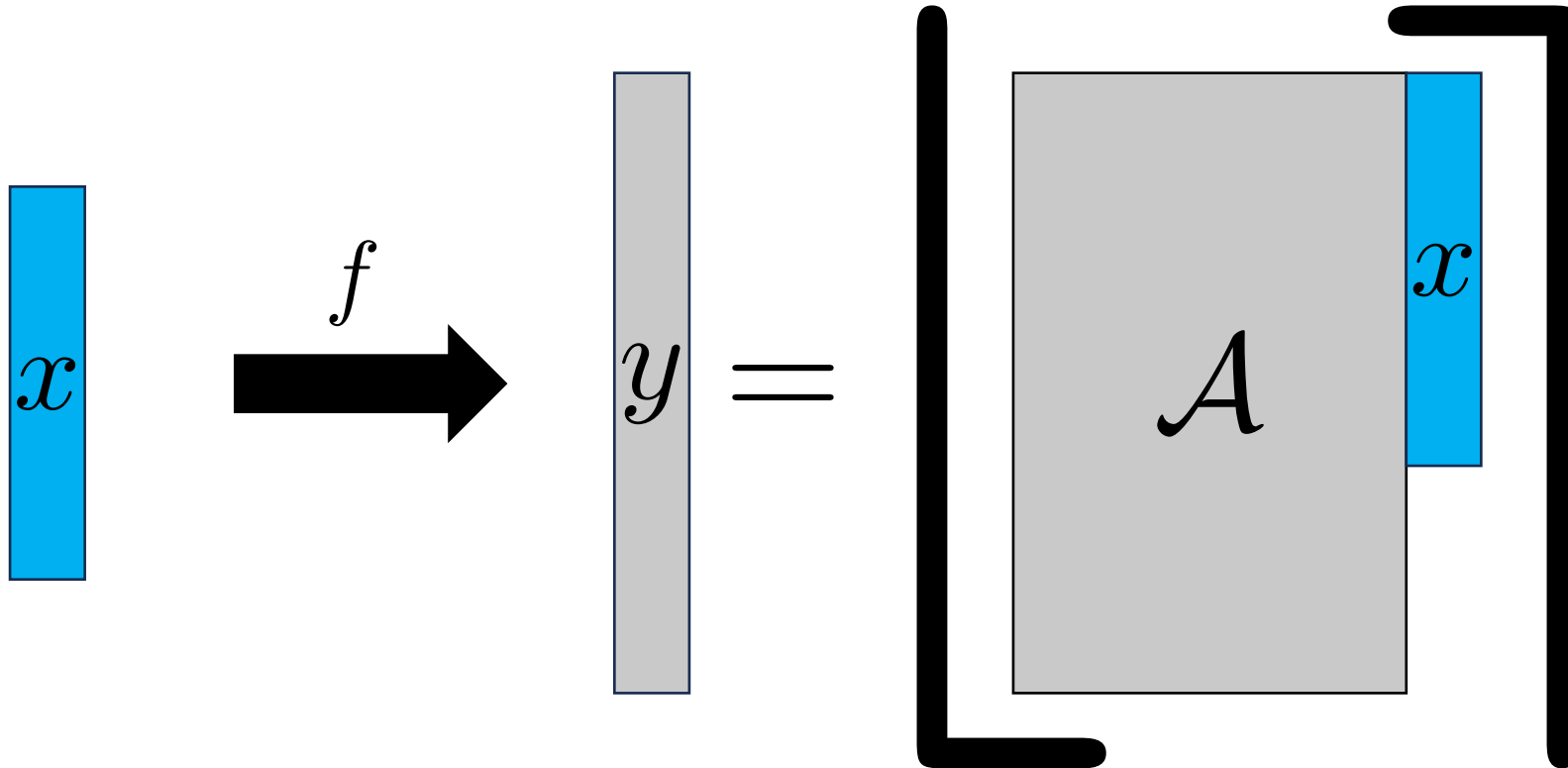
- ➔ Reduction loss = $\#(\text{instances})$
- ➔ Can set $\lambda_{\text{OWF}} = \text{polylog}(\#(\text{instances}))$
- ➔ Succinctness if $\#(\text{instances})$ is small exponential, but independent of $\#(\text{statements})$

x , 

Follows exactly from “very” lossy

Constructing Lossy Functions from LWE

[Alwen-Krenn-Pietrzak-Wichs'13]



 = short vector

Injective mode: A full rank

Lossy Mode

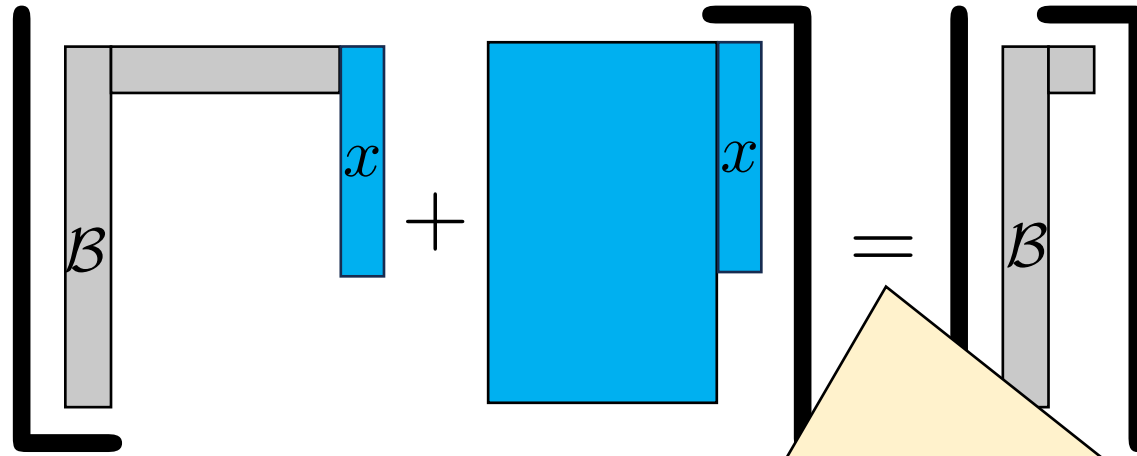
A diagram illustrating the decomposition of a matrix A . On the left is a gray rectangle labeled A . This is followed by an equals sign, then a gray L-shaped structure labeled B (representing the first column and the top row of A), followed by a plus sign, and finally a solid blue rectangle representing a short vector.

A diagram illustrating the multiplication of matrix A by a vector x . On the left, a gray rectangle labeled A and a blue vertical bar labeled x are enclosed in large square brackets. This is followed by an equals sign, then a gray L-shaped structure labeled B and a blue vertical bar labeled x are enclosed in large square brackets, followed by a plus sign, and then a blue rectangle and a blue vertical bar labeled x are enclosed in large square brackets. This is followed by another equals sign, and finally a gray L-shaped structure labeled B is enclosed in large square brackets.

 = short vector

$\#(\text{images}) \leq \|\text{col-span}(\mathcal{B})\| = 2^{\text{poly}(\lambda_{\text{LWE}})} ?$

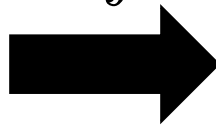
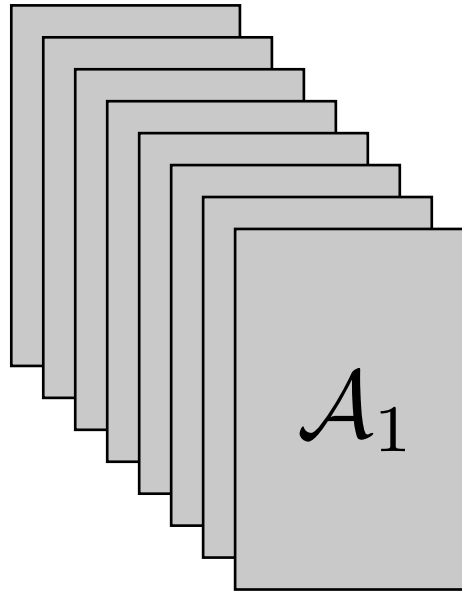
Problem: Rounding Boundaries



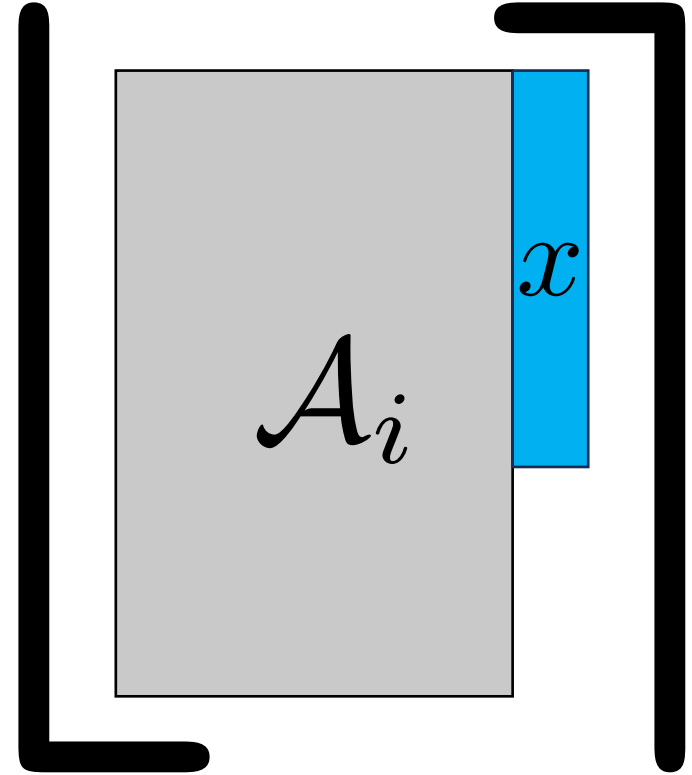
Only true far from rounding boundaries. Near rounding boundaries, output may statistically reveal x

Still lossy, but not *very* lossy

Our Solution: Stay Away From Rounding Boundaries



f
 $i,$



Whp, $\forall x$ there will exist some i
Only blow up image size by polynomial factor

for smallest i s.t. $A_i \cdot x$ is
far from rounding boundary

$\Rightarrow \#(\text{images}) \leq 2^{\text{poly}(\lambda_{\text{LWE}})}$

Thanks!