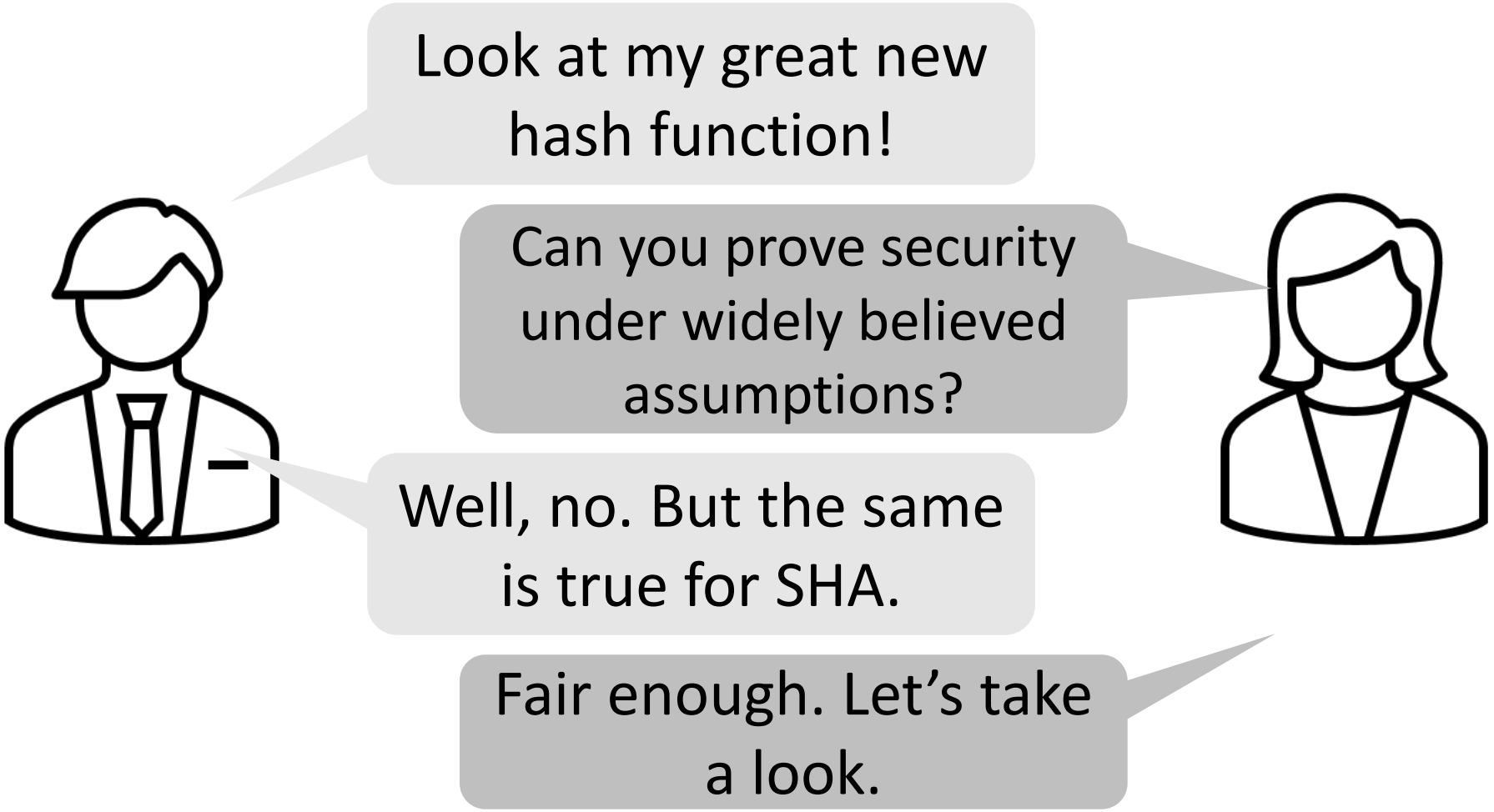
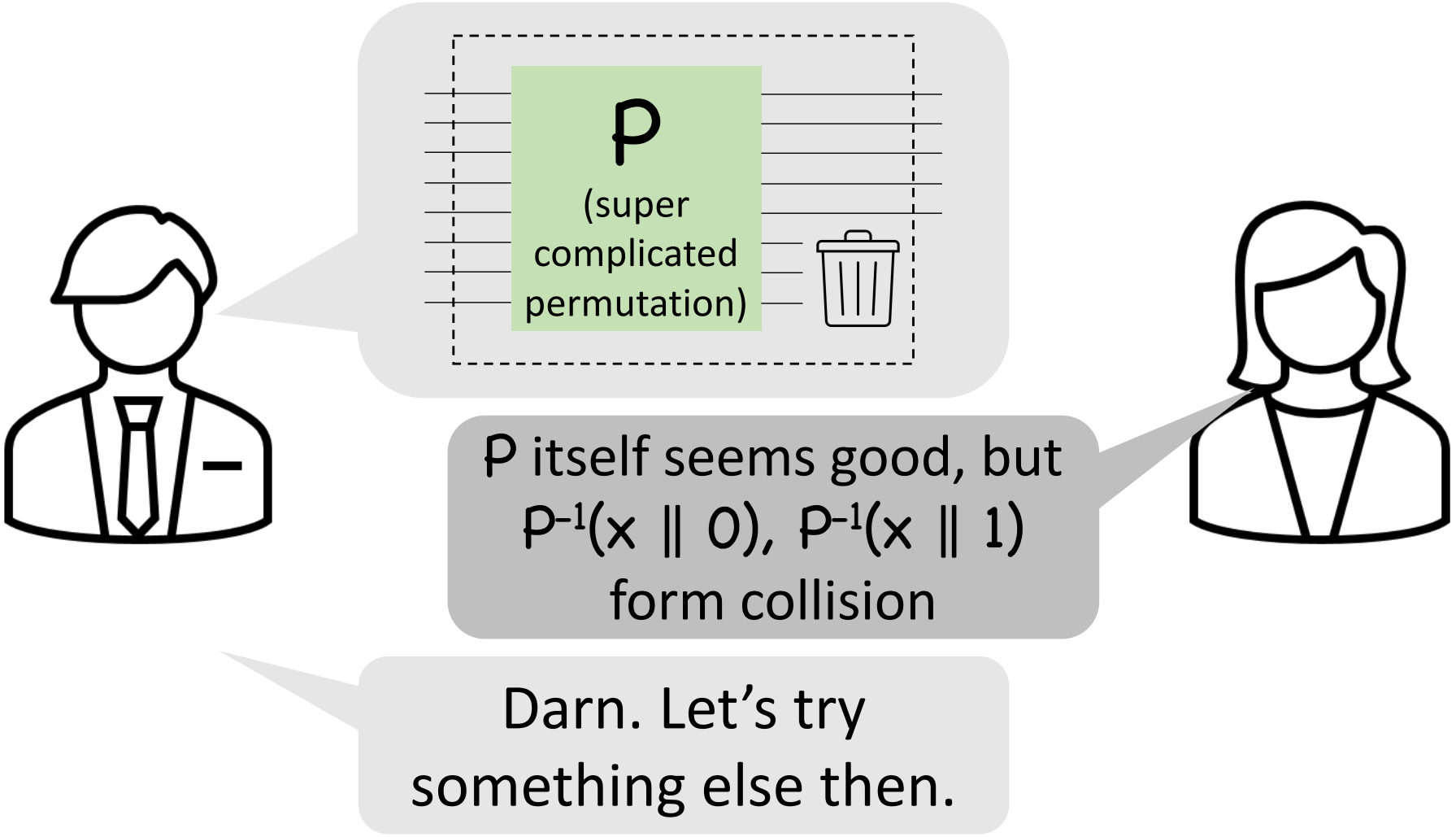
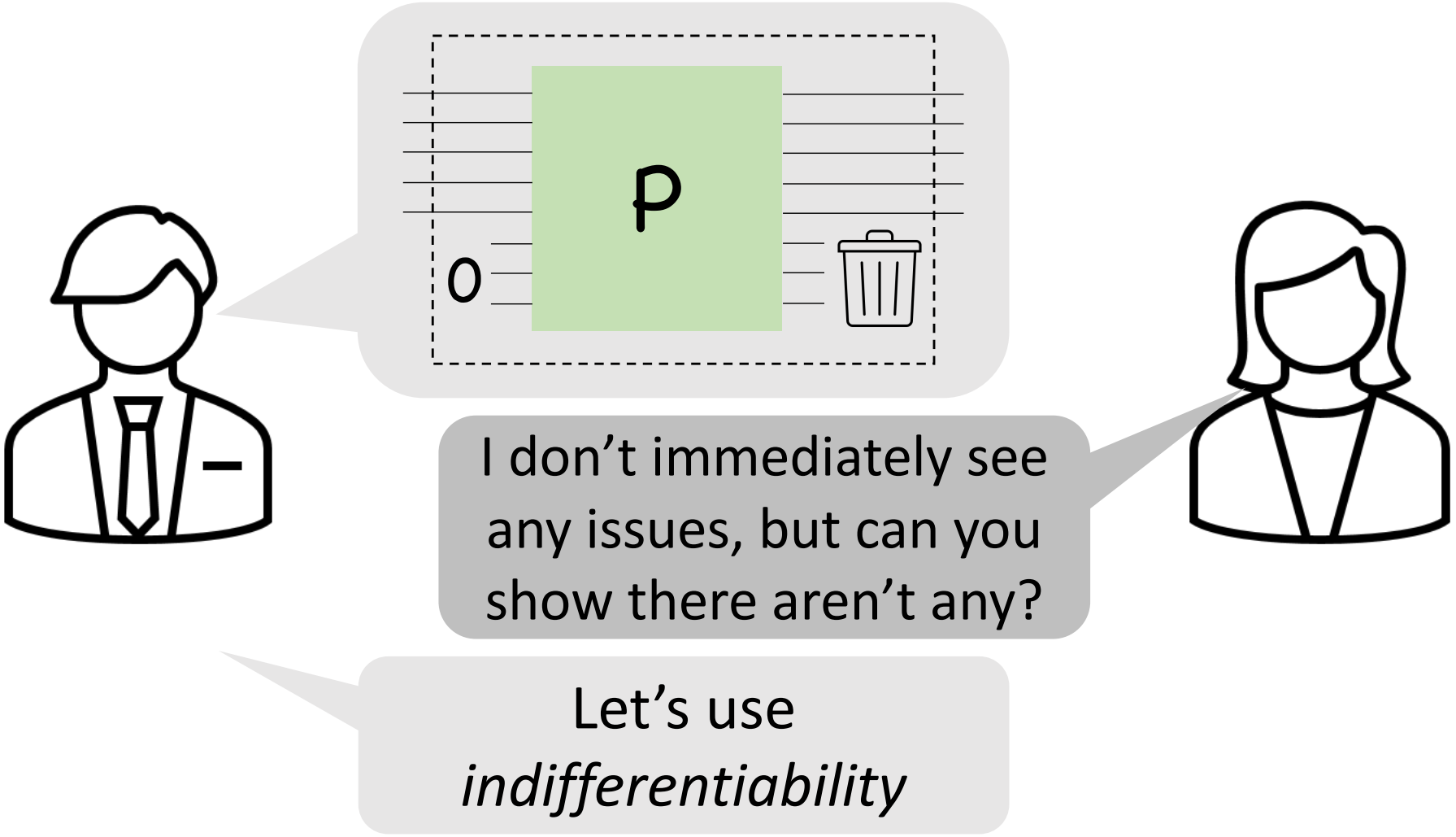
Redeeming Reset Indifferentiability and Applications to Post-Quantum Security

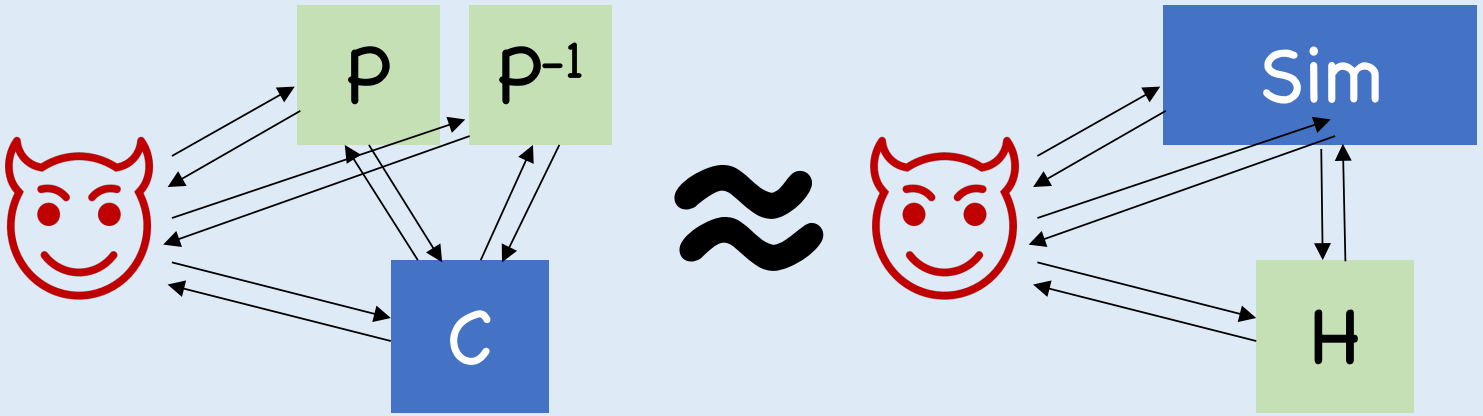
Mark Zhandry (Princeton & NTT Research)


Look at my great new hash function!
Can you prove security under widely believed assumptions?
Well, no. But the same is true for SHA.
Fair enough. Let’s take a look.


P
(super complicated permutation)
P itself seems good, but $P^{-1}(x \| 0)$, $P^{-1}(x \| 1)$ form collision
Darn. Let's try something else then.


P
0
I don’t immediately see any issues, but can you show there aren’t any?
Let’s use *indifferentiability*

Def [Maurer-Renner-Holenstein'04]: *Indifferentiability*

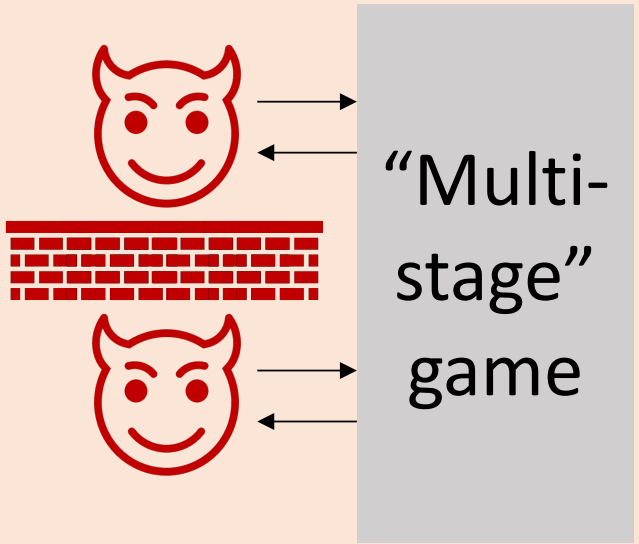


Note: Sim can be *stateful*

Thm [Maurer-Renner-Holenstein'04]: Indifferentiability composes, implies security for "single stage games"

This Work: An Exploration of *Reset* Indifferentiability

Limitation [Ristenpart-Shacham-Shrimpton'11]:

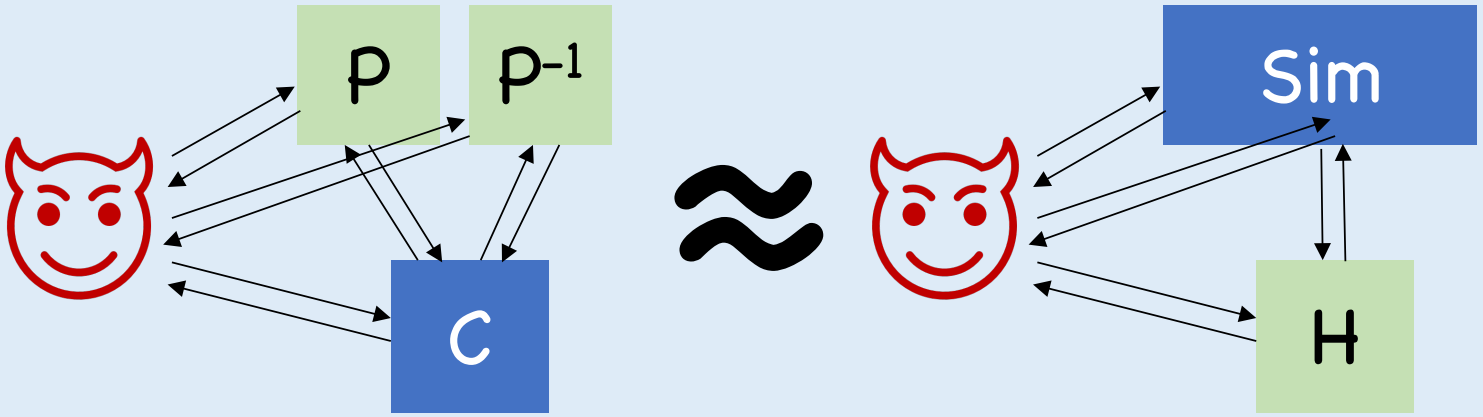


Problem: Sim's shared state breaks isolation

MRH composition fails

Examples: Deterministic encryption, KDM security, leakage resilience, etc.

Def [Ristenpart-Shacham-Shrimpton'11]: *Reset Indifferentiability*



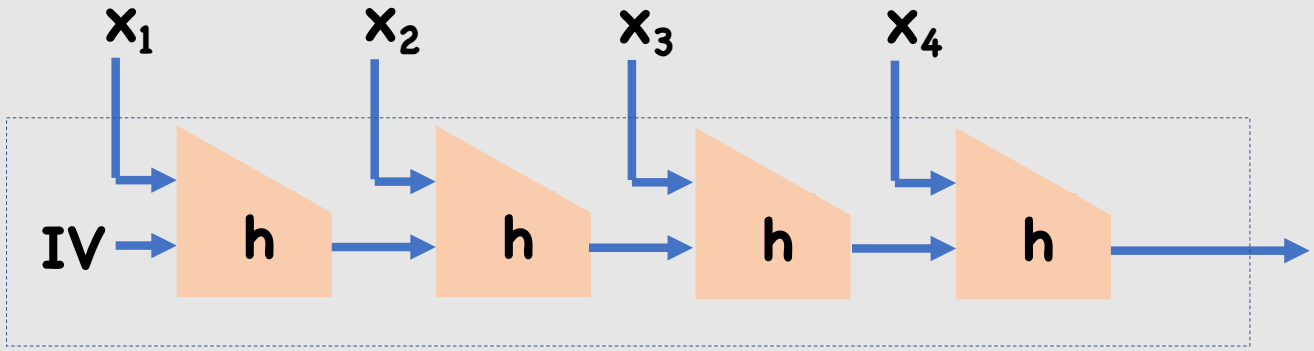
*****Now Sim must be *stateless******

Thm [Ristenpart-Shacham-Shrimpton'11]:
Reset indiff. implies security for general games

Thm [Ristenpart-Shacham-Shrimpton'11, Luykx-Andreeva-Mennink-Preneel'12, Demay-Gaži-Hirt-Maurer'13, Baecher-Brzuska-Mittelbach'13]:

No reset indifferentiable domain extension

E.g. Merkle-Damgård



Consequence: Reset indifferentiability largely abandoned

Observations

1. Domain extension not always necessary
   (e.g. deterministic encryption for fixed-size messages)

2. Essentially nothing else is known
   - Domain shrinkage?
   - Small ROs from ideal ciphers?
   - Vice versa?

Our Results for Reset Indifferentiability

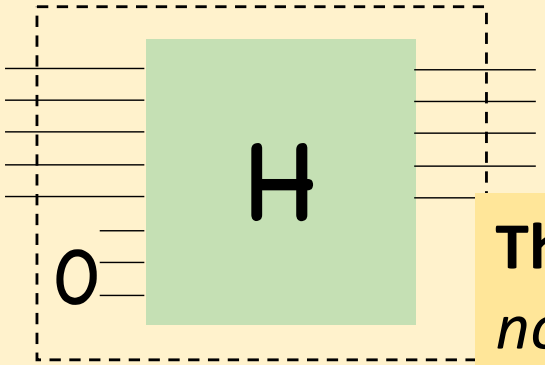
Thm: Domain extension impossibility holds even for *query unbounded* simulators

Thm: In *unbounded* setting, in*distinguisha*bility→in*differentia*bility

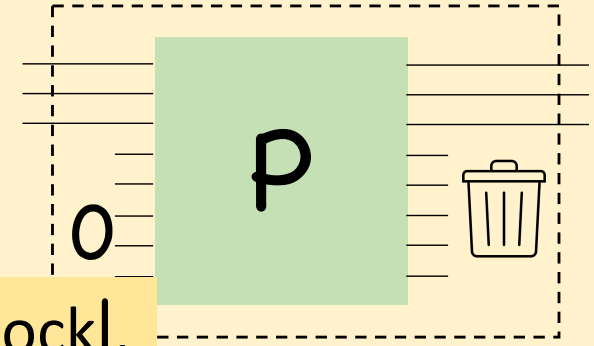
Domain shrinkage, ideal ciphers from RO's, vice versa, all have constructions that are indistinguishable against query unbounded attacks

Takeaway: useless for applications, but shows prior negative work inherently limited to domain extension

Thm: Domain shrinkage for random oracles



Thm: Ideal ciphers → ROs



ed |in|+|out|≤|block|

Thm: If |in|+|out| ≫ |block|, *not* reset indifferentiable

Thm: All results lift to *quantum* setting

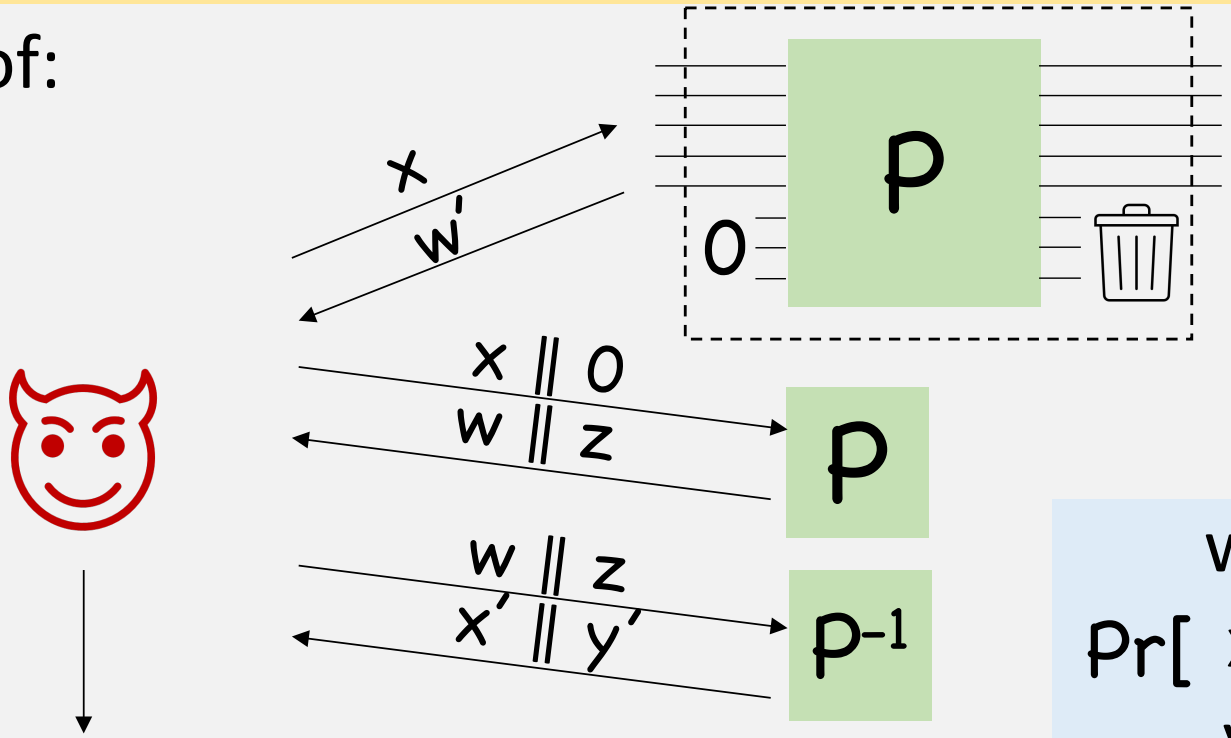
Previously, ideal cipher → ROs unknown, even under plain indifferentiability

Non-reset setting concurrently proved by [Czajkowski'21]; entirely different approach

Ideal ciphers → Reset Indifferentiable ROs

Thm: If |in|+|out| ≫ |block|, *not* reset indifferentiable

Proof:



w=w'

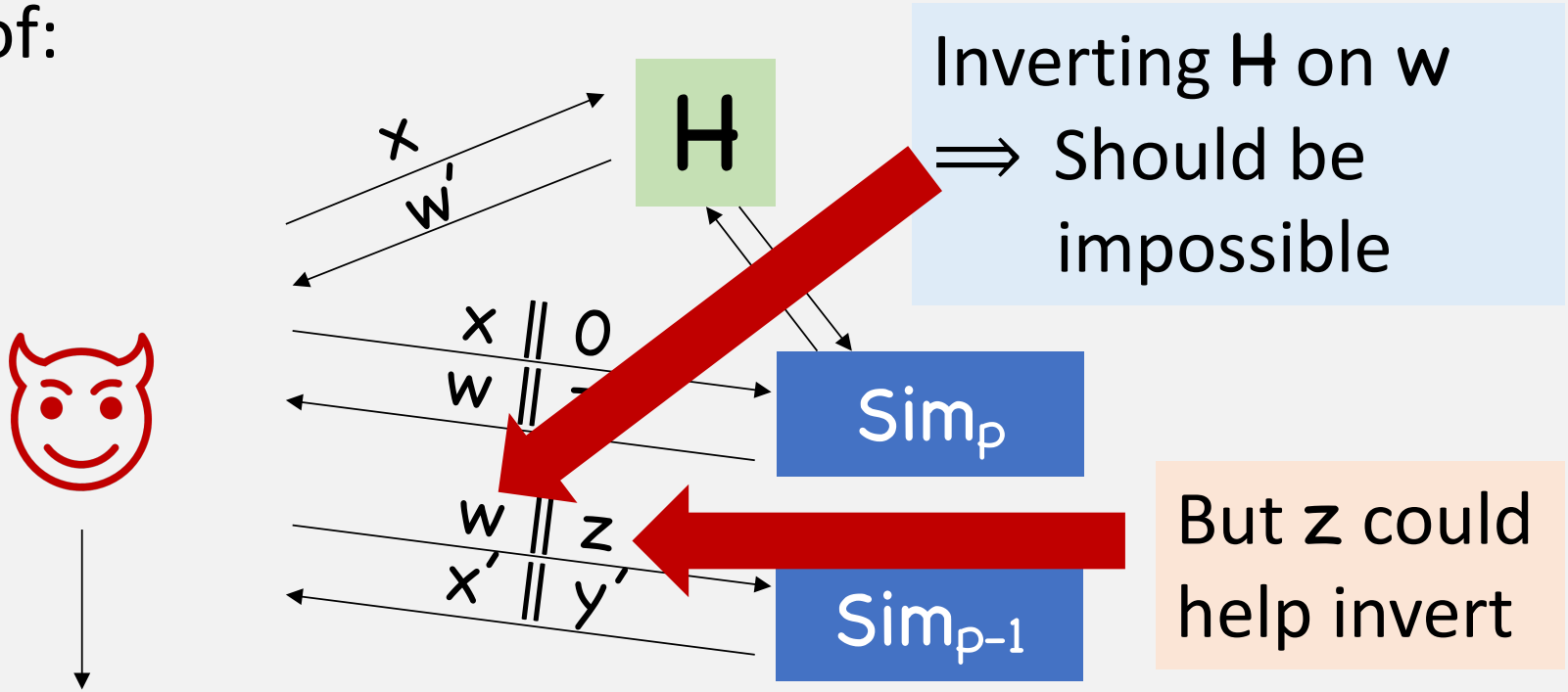
Pr[x=x'] = 1

y'=0

Check w=w', x=x', and y'=0

Thm: If |in|+|out| ≫ |block|, *not* reset indifferentiable

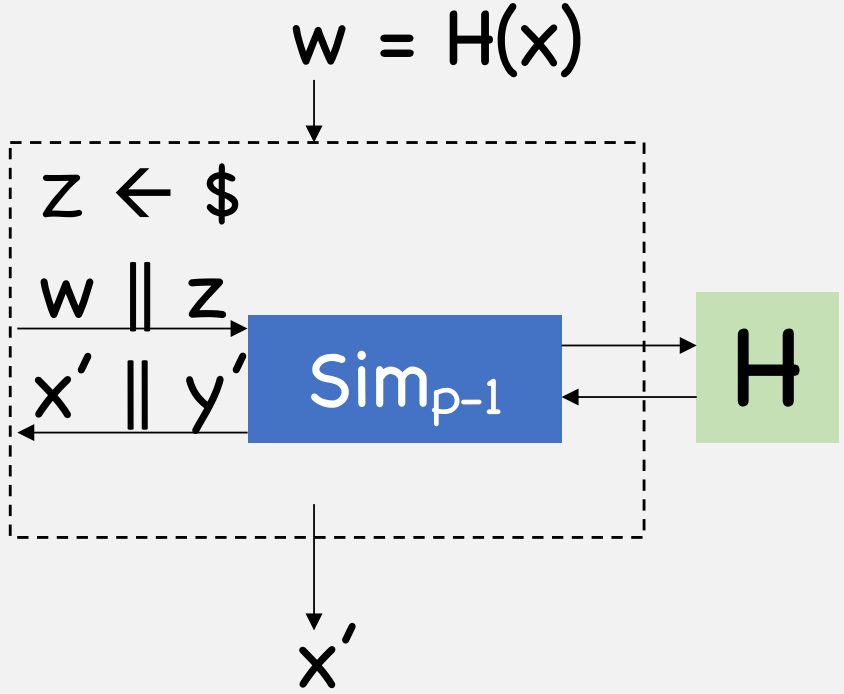
Proof:



Check w=w′, x=x′, and y′=0

Thm: If |in|+|out| ≫ |block|, *not* reset indifferentiable

Proof: Construct inverter for H



$$\Pr[x'=x] \geq \Pr[z \text{ “correct”}] = (\tfrac{1}{2})^{-(|block|-|out|)}$$

+

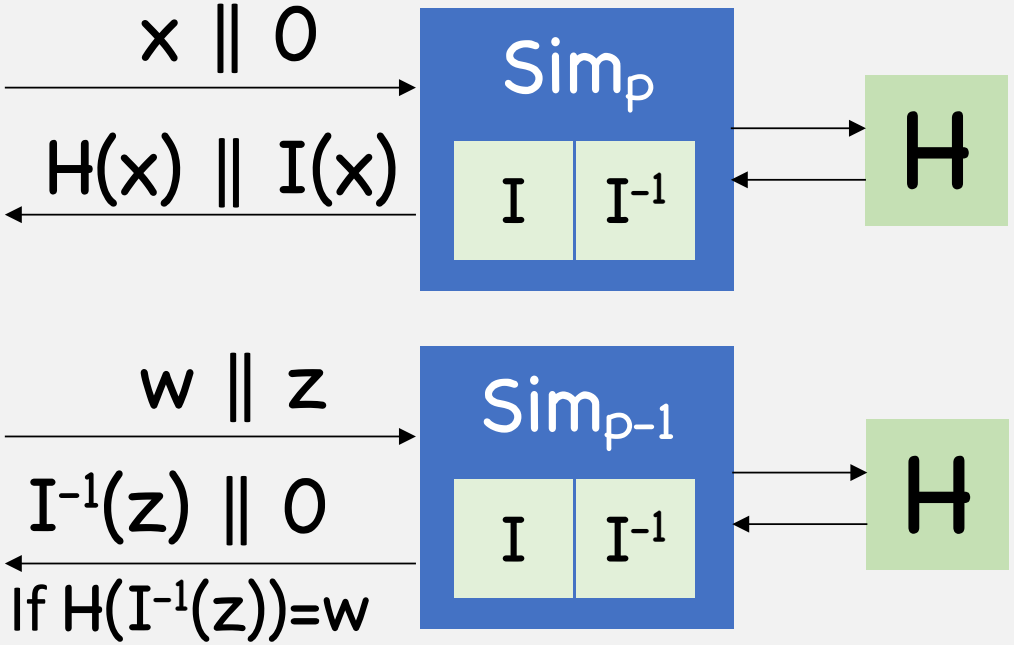
But, by one-wayness of ROs,

$$\Pr[x'=x] \leq O(\ q \times (\tfrac{1}{2})^{-|in|}\ )$$

$$q \geq \Omega(\ 2^{|in|+|out|-|block|}\ )$$

Thm: If |in|+|out|≤|block|, then reset indifferentiable

Proof idea: Statelessly encode x into z



Lingering issues:

- Simulate I without state
- Handling x ‖ y for y≠0?

Open Problems

1 Reset Indiff. ideal ciphers from ROs?

2 More efficient use of ideal ciphers?

3 What about other indiff. results?