When Simple Permutations Mix Poorly

Limited Independence Does Not Imply Pseudorandomness

Jesko Dujmovic
Boston & Northeastern University

Angelos Pelecanos
UC Berkeley

Stefano Tessaro
University of Washington

Block ciphers, k-wise independence, and pseudorandomness

The two sides of cryptography

Theory

Secure well-studied assumptions.

Impressive primitives

- secret/public-key encryption,
- fully homomorphic encryption, multi-party computation,
- indistinguishability obfuscation,
- many more!

Practice

Satisfied with heuristic security arguments.

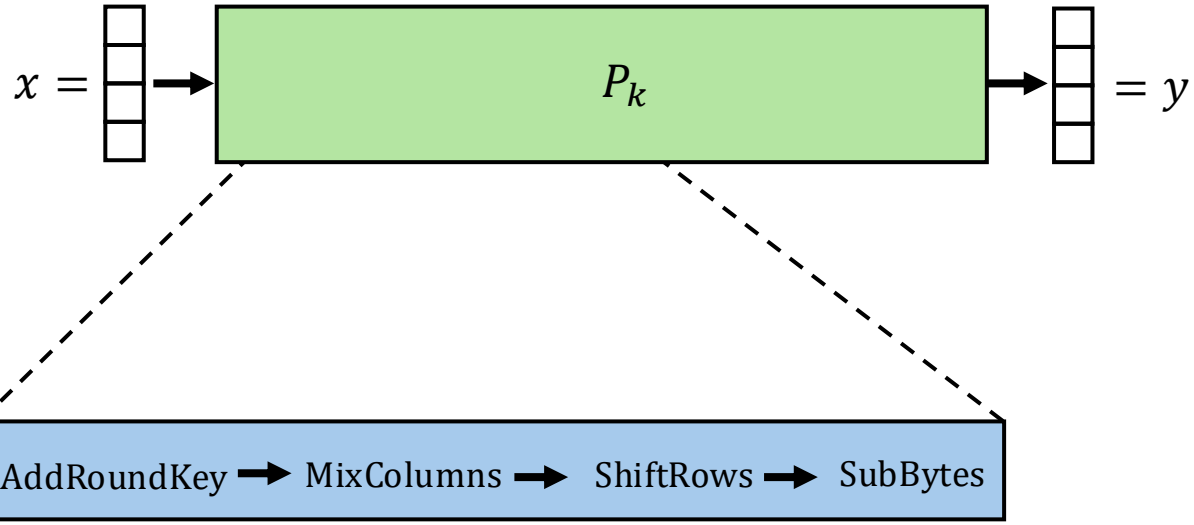
Need extremely efficient schemes.

Block ciphers, like AES.

Focus of this talk

Block ciphers

In practice, use block ciphers for secret-key encryption



AES

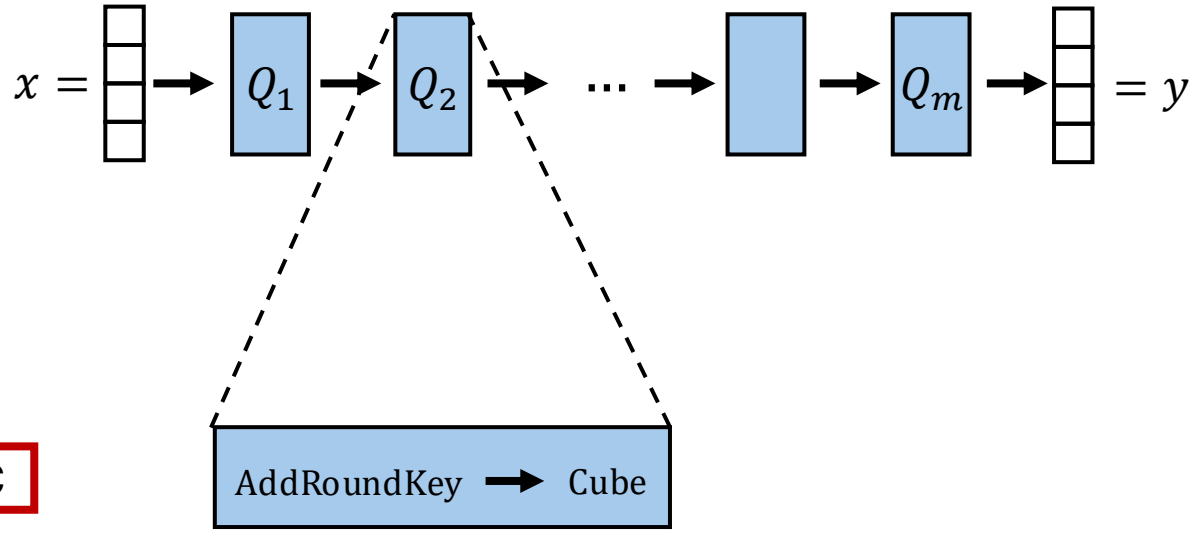
Permutation over $\{0,1\}^n$

Indexed by secret key k

Contains simple rounds

Block ciphers

In practice, use block ciphers for secret-key encryption



MiMC

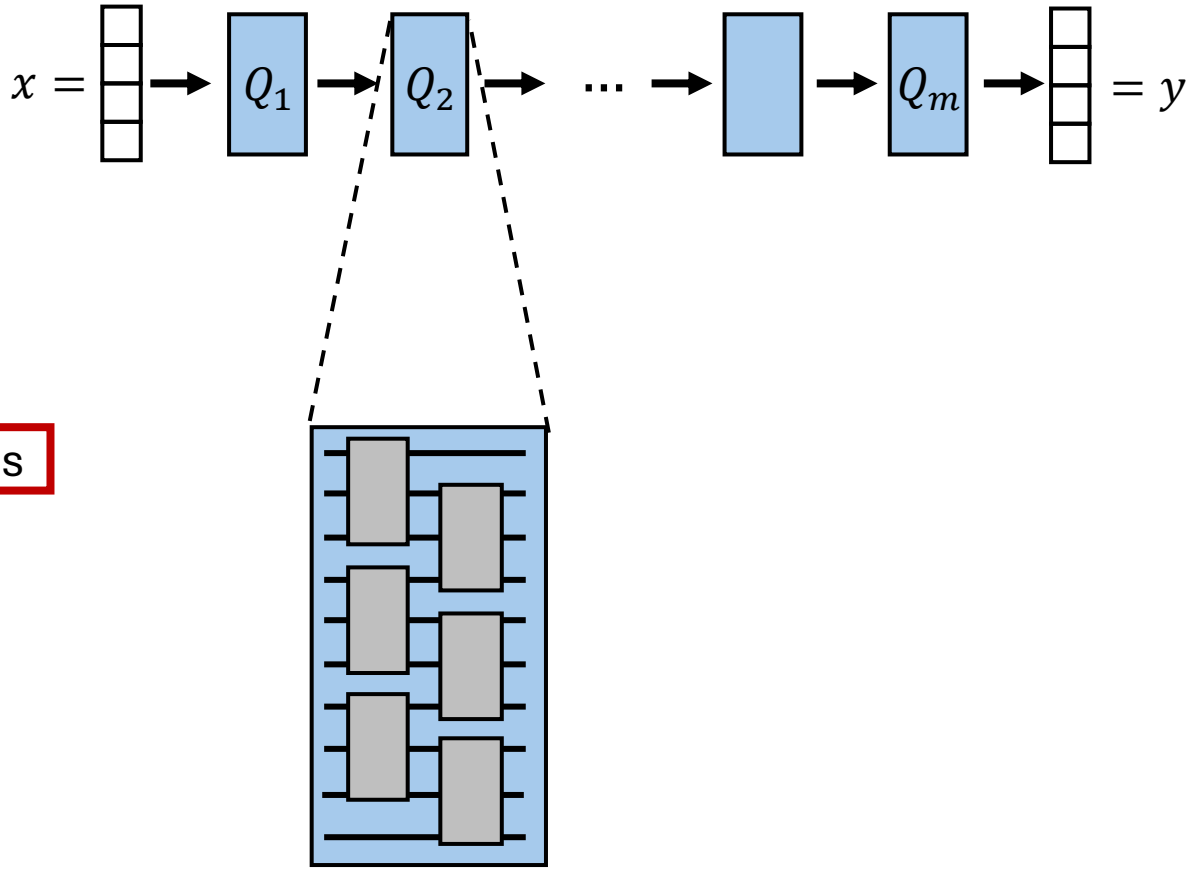
Permutation over $\{0,1\}^n$

Indexed by secret key k

Contains simple rounds

Block ciphers

In practice, use block ciphers for secret-key encryption



Random Local Circuits

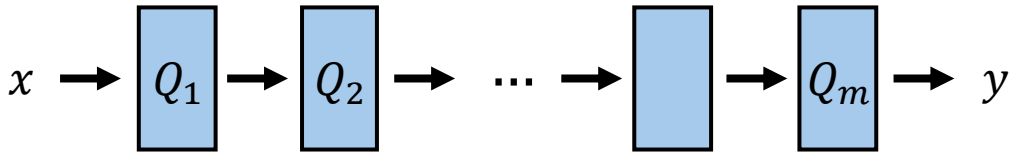
Permutation over $\{0,1\}^n$

Indexed by secret key k

Contains simple rounds

Block ciphers

In practice, use block ciphers for secret-key encryption



Permutation over $\{0,1\}^n$

Indexed by secret key k

Contains simple rounds

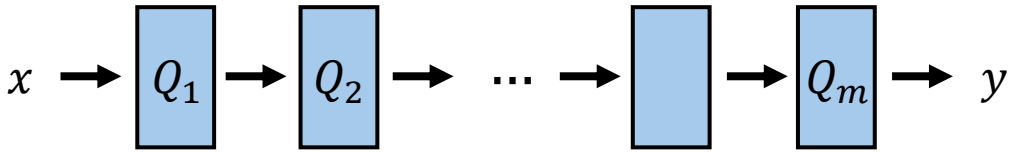
Single round has weak security, so repeat for m rounds.

Fundamental: Understand the security of block ciphers.

k-wise independence

Inherently difficult to prove security via reductions.

- One round is insecure, but enough rounds look secure.

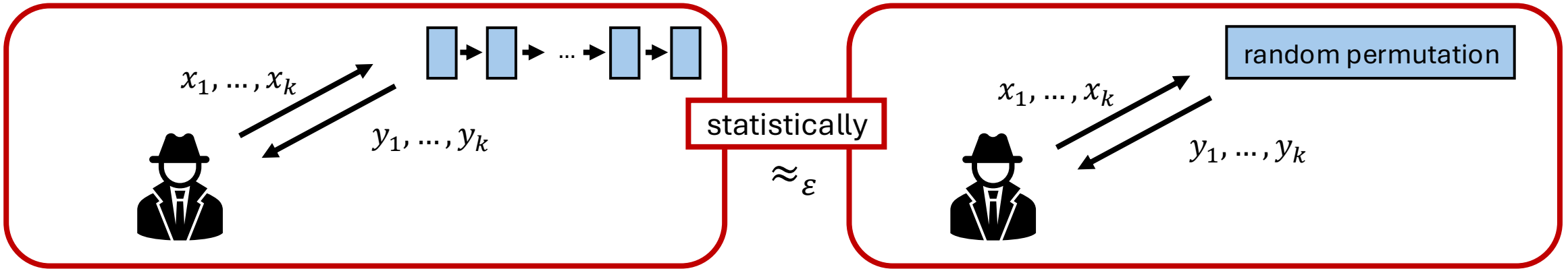


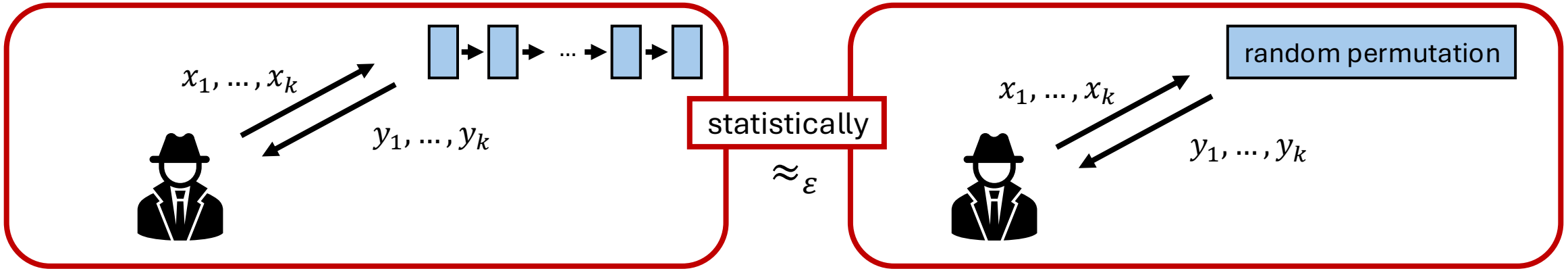
Instead, prove security against classes of attacks.

- Many exploit deviations in a few outputs.

linear [MY92] and differential [BS91] attacks

Motivates the study of k-wise independence





Main goal. Min # rounds to reach ε-close to k-wise independence.

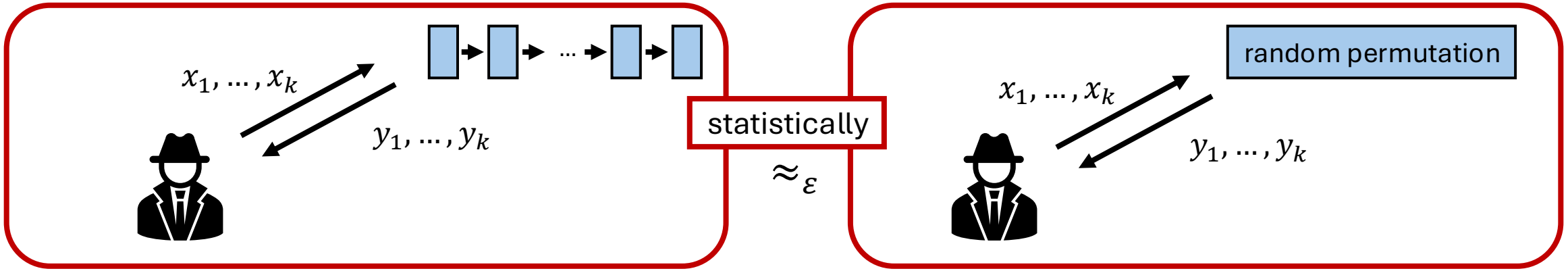
$\Rightarrow$ security against non-adaptive adversary with $\leq k$ queries.

Prior work.

Random local circuits: [Gow96, HMMR05, BH08, CHH+24, GH**P**25, GHKO25]

Substitution-Permutation Networks (like AES): [LTV21, L**P**TV23, Din25, BLS25]

Vaudenay's [Vau03] decorrelation theory also a form of k-wise.



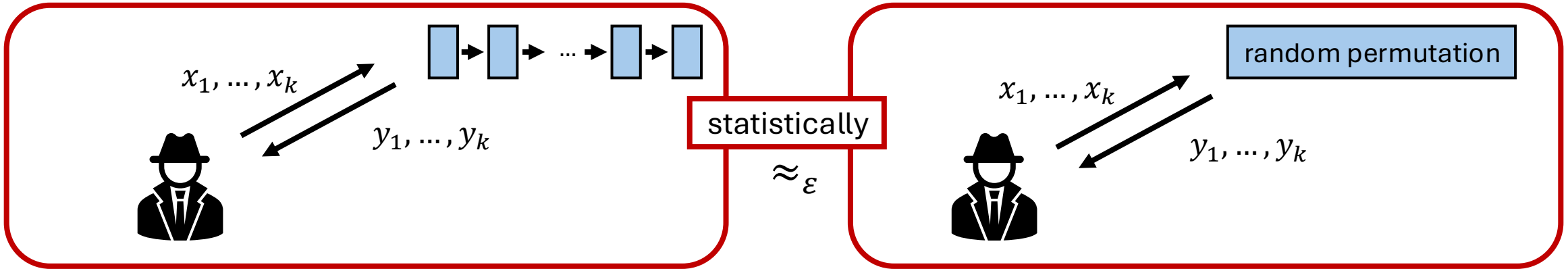
Main goal. Min # rounds to reach ε-close to k-wise independence.

$\Rightarrow$ security against non-adaptive adversary with $\leq k$ queries.

More implications [LTV21]: Guard against…

$k = 2$: differential, linear attacks.

$k = 2^d$: (truncated) degree-d differential attacks [Lai94, Knu94].



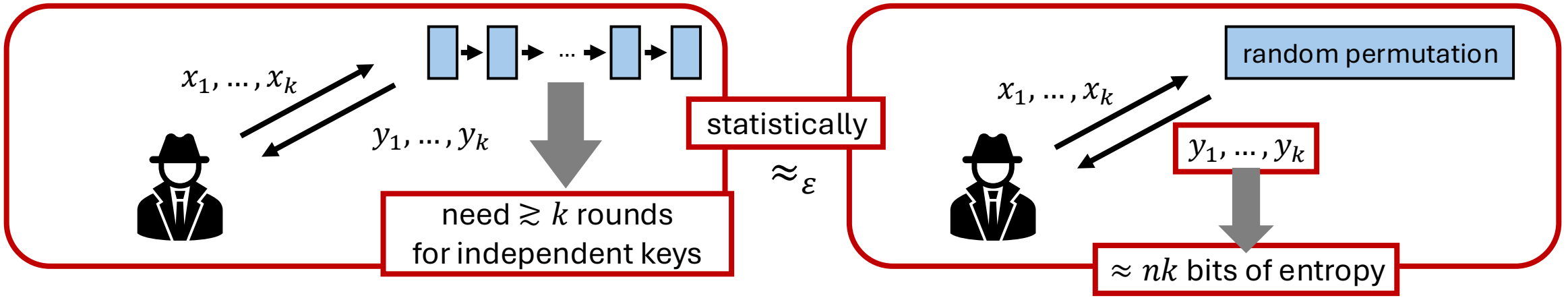
Main goal. Min # rounds to reach ε-close to k-wise independence.

$\Rightarrow$ security against non-adaptive adversary with $\leq k$ queries.

Quantitative comparison: block ciphers A, B

e.g., A is k-wise independent in fewer rounds than B

evidence that A is more "secure" than B



Main goal. Min # rounds to reach ε-close to k-wise independence.

$\Rightarrow$ security against non-adaptive adversary with $\leq k$ queries.

$\Rightarrow$ pseudorandom when $k \gg \text{poly}(n)$

AES has at most 14 rounds, so cannot say anything beyond $k \approx 14$.

Hope: k-wise independence is a good proxy for pseudorandomness.

Dream: block cipher is k-wise independent ⇒ pseudorandom.

for polynomial k, ideally $k = \Theta(1)$

False! A random polynomial of degree $k-1$:

$$f(x) = a_{k-1}x^{k-1} + \cdots + a_1 x + a_0$$

perfect k-wise independence

fails at $(k+1)$-wise independence

Exercise. Extend this counterexample to a permutation (hint: Feistel)

Implicit assumption: counterexample doesn't appear in "natural" block ciphers

Dream 2.0: "natural" block cipher is k-wise independent ⇒ pseudorandom.

for polynomial k, ideally $k = \Theta(1)$

What does "natural" mean?

The HMMR conjecture

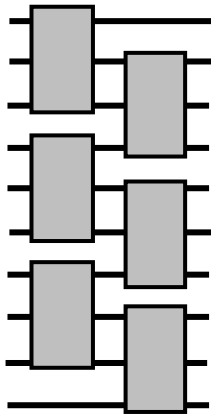
Hoory, Mager, Myers, and Rackoff [HMMR04] conjectured Dream 2.0:

Conjecture. Let P be a block cipher with simple rounds.
If $P^m \approx_{\text{negl}}$ 4-wise independent $\Rightarrow$ P^m is pseudorandom.

P^m: m rounds of P

Each output bit depends on $\Theta(1)$ input bits.

Simple: Local gates



The HMMR conjecture

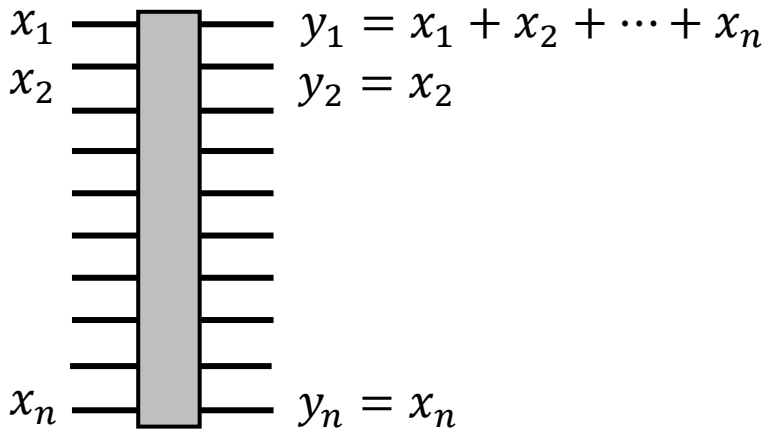
Hoory, Mager, Myers, and Rackoff [HMMR04] conjectured Dream 2.0:

Conjecture. Let P be a block cipher with simple rounds.
If $P^m \approx_{\text{negl}}$ 4-wise independent $\Rightarrow P^m$ is pseudorandom.

P^m: m rounds of P

Each output bit depends on $\Theta(1)$ input bits.

Not simple: Multi-bit parity (or SPN mixing)



The HMMR conjecture

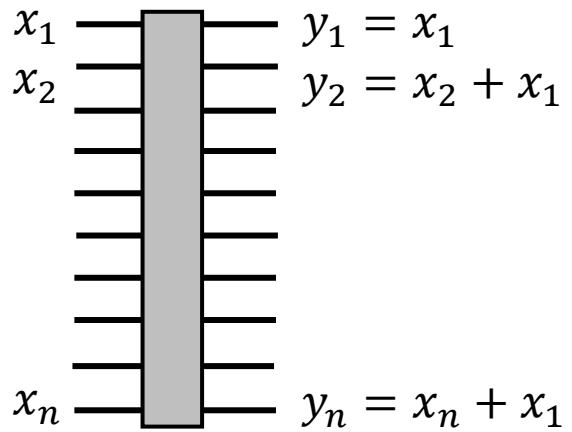
Hoory, Mager, Myers, and Rackoff [HMMR04] conjectured Dream 2.0:

Conjecture. Let P be a block cipher with simple rounds.
If $P^m \approx_{\text{negl}}$ 4-wise independent $\Rightarrow P^m$ is pseudorandom.

P^m: m rounds of P

Each output bit depends on $\Theta(1)$ input bits.

Simple: One input bit affects many output bits



The HMMR conjecture

Hoory, Mager, Myers, and Rackoff [HMMR04] conjectured Dream 2.0:

Conjecture. Let P be a block cipher with simple rounds.
If $P^m \approx_{\text{negl}}$ 4-wise independent $\Rightarrow P^m$ is pseudorandom.

P^m: m rounds of P

Counterexample for 3-wise

The HMMR conjecture

Hoory, Mager, Myers, and Rackoff [HMMR04] conjectured Dream 2.0:

Conjecture. Let P be a block cipher with simple rounds.
If $P^m \approx_{\text{negl}}$ 4-wise independent $\Rightarrow P^m$ is pseudorandom.

P^m: m rounds of P

Surprisingly strong conjecture, but standing for > 20 years.

Two properties require many-round block ciphers ⇒ hard to cryptanalyze.

Quantum analog of this conjecture.

Our results

Conjecture. Let P be a block cipher with simple rounds.
If $P^m \approx_{\text{negl}}$ 4-wise independent $\Rightarrow P^m$ is pseudorandom.

P^m: m rounds of P

Main result: a refutation of the HMMR conjecture

Theorem [DPT26]. Exists block cipher P and m:

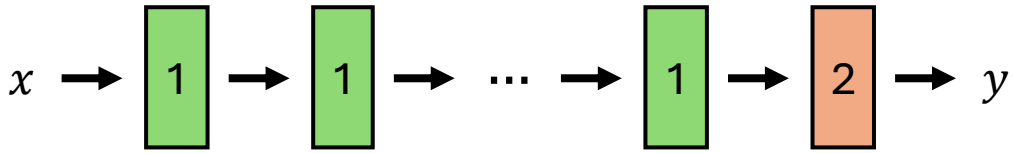
1. $P^m \approx_{\text{negl}}$ 4-wise independent.
2. Efficiently distinguish 5 outputs of P^m from random.

... and its extension from 4-wise to k-wise ∀ constant k.

Theorem [DPT26]. Exists block cipher P and m:

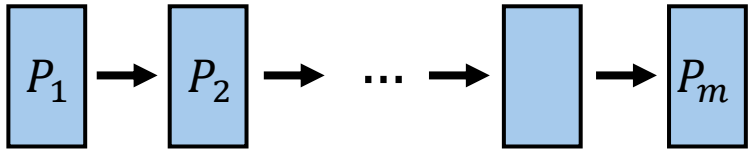
1. $P^m \approx_{\text{negl}}$ 4-wise independent.
2. Efficiently distinguish 5 outputs of P^m from random.

Warm-up. Allow different types of rounds



randomize non-special strings
keep special strings the same

phase two



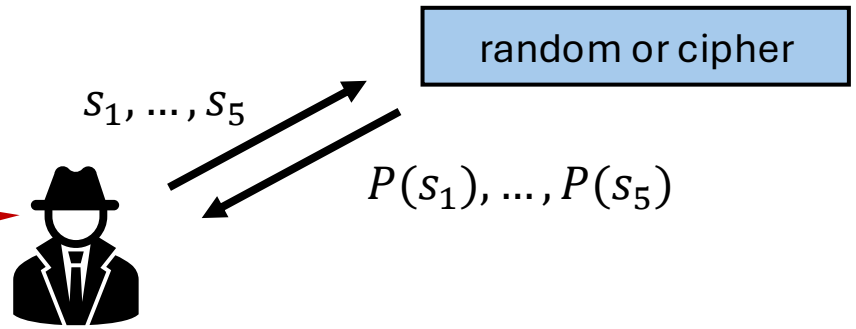
rounds must be identically distributed

WLOG. Consider permutation over Σ^n, for $\Sigma = \{\uparrow, 0,1,2,3,4,5,\dots\}$.

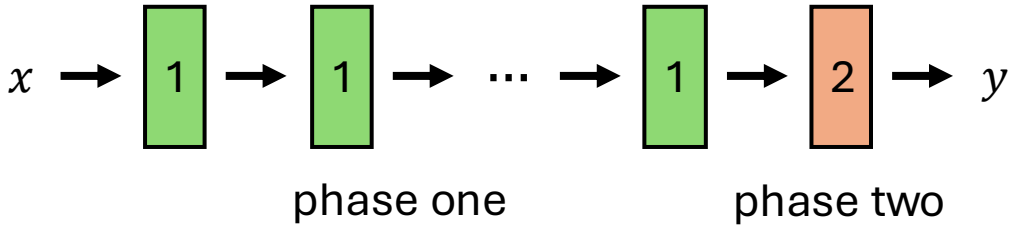
Idea. Special strings $s_x = \uparrow \uparrow \cdots \uparrow x$, for $x \in [5]$ such that

$$P(s_1) + \cdots + P(s_5) = 0^n.$$

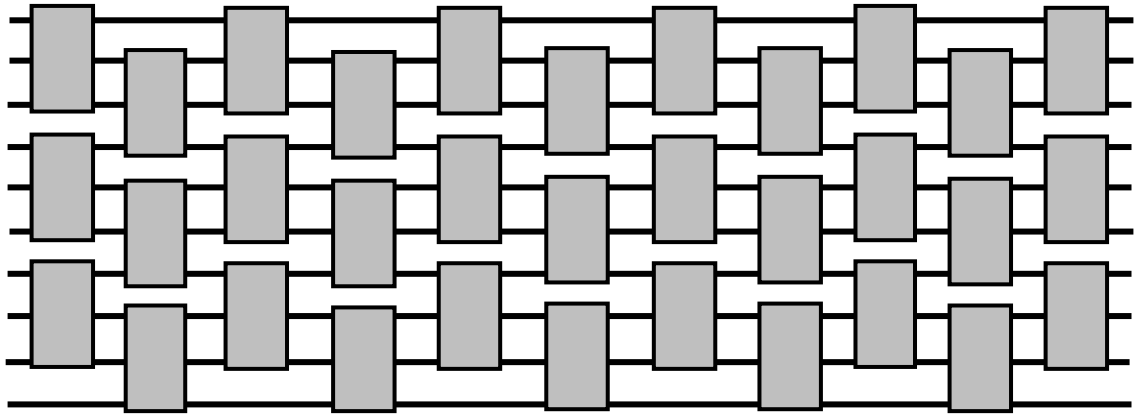
"cipher" if $P(s_1) + \cdots + P(s_5) = 0^n$,
"random" otherwise



Randomize non-special



Tool. Random reversible brickwork circuit



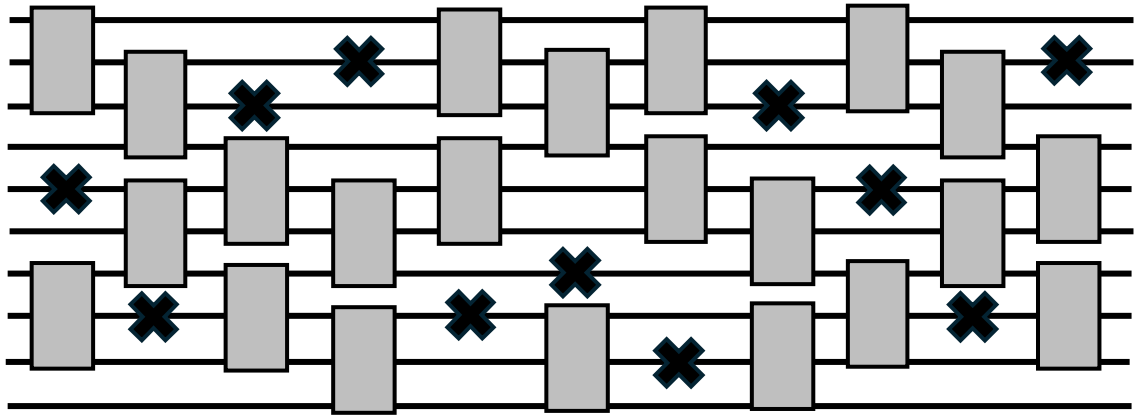
Each gate is
random permutation on Σ^3

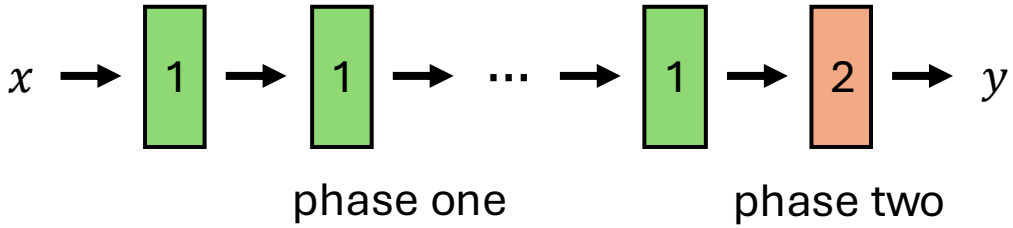
Converges to k-wise
independence rapidly
[CHH+25, GHKO25]

Caveat. Want to keep special $s_x = \uparrow\uparrow\cdots\uparrow x$ the same!

Instead. Conditional brickwork: Every round

1. Choose a random wire $i \in [n-1]$.
2. Apply brickwork only if $i-\text{th wire} \neq \uparrow$.





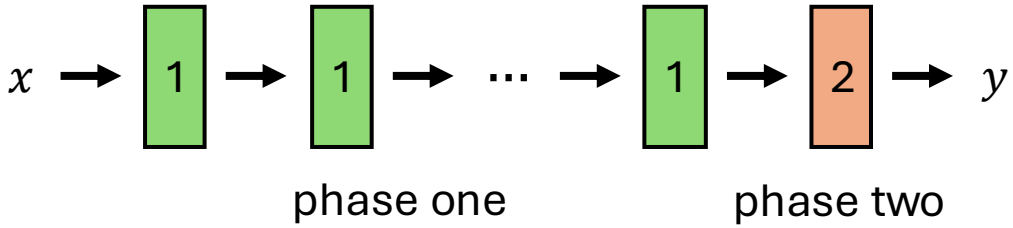
Special $s_x = \uparrow\uparrow\cdots\uparrow x$:
$i-\text{th wire} = \uparrow$, never apply brickwork

Non-special:
$\exists \text{wire} \neq \uparrow$, will apply brickwork

Theorem. After $n \log n$ rounds, non-special $\approx_{\text{negl}}$ 4-wise independent.

Technique: Markov chain comparison + [GHKO25] as a black box.

Phase two

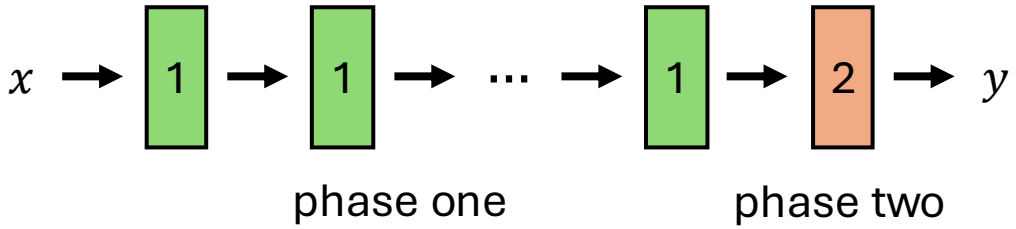


Goal.

1. Make special strings 4-wise independent.
2. Satisfy $P(s_1) + \cdots + P(s_5) = 0^n$.

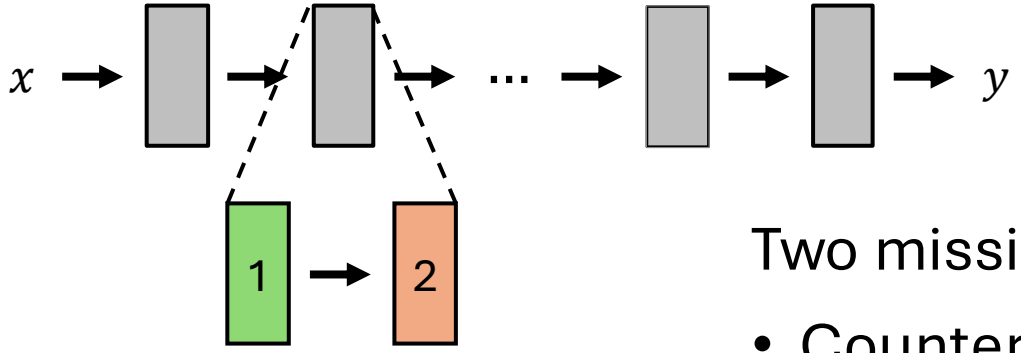
Can implement via simple rounds because 5 is constant.

Sketch of full construction



Rounds must be identically distributed.

Idea. Always try both actions, but only one succeeds.



Two missing ingredients:

- Counter to decide when to switch phases.
- Mixing step.

Discussion

This paper: Refutation of the HMMR conjecture.

Conjecture. Let P be a block cipher with simple rounds.
If $P^m \approx_{\text{negl}}$ 4-wise independent $\Rightarrow$ P^m is pseudorandom.

P^m: m rounds of P

Exact relation of

k-wise independence

and

pseudorandomness

remains unclear

These conjectures deepen our understanding.

Propose natural follow-up conjectures.

This paper: Refutation of the HMMR conjecture.

Conjecture. Let P be a block cipher with simple rounds.
If $P^m \approx_{\text{negl}}$ 4-wise independent $\Rightarrow$ P^m is pseudorandom.

P^m: m rounds of P

Open questions:

1. Logarithmic Independence

Conjecture. Let P be a block cipher with simple rounds.
If $P^m \approx_{\text{negl}}$ $\log n$-wise independent $\Rightarrow$ P^m is pseudorandom.

2. Increased Pseudorandomness Threshold

Conjecture. Let P be a block cipher with simple rounds.
If $P^m \approx_{\text{negl}}$ 4-wise independent $\Rightarrow$ $P^{f(m)}$ is pseudorandom.

f fixed polynomial

3. Refute HMMR conjecture using a Substitution-Permutation Network?

Thank you