What can we (not) prove about AES?

Gausta, Norway, April 2026

PAUL G. ALLEN SCHOOL
OF COMPUTER SCIENCE & ENGINEERING

Stefano Tessaro

tessaro@cs.washington.edu

A theorist's frustration?

AES secure $\Longrightarrow$ provable security extremely ineffective

Three reactions in theory community:

Denial

Critique

Curiosity

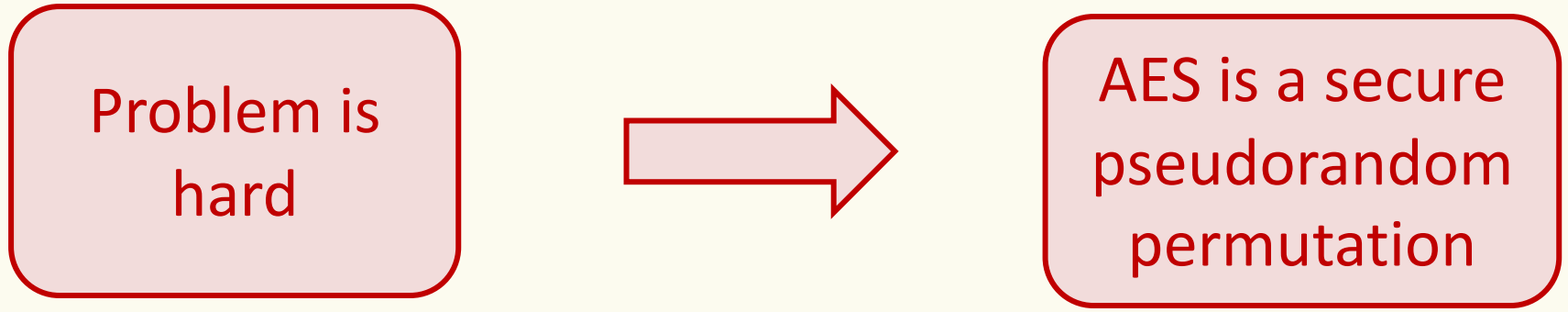
This talk

Security = AES is a Pseudorandom Permutation (PRP)

– E.g., every T-time attacker achieves distinguishing advantage at most $T/2^{120}$. *

* somewhat tricky to formalize

Theory of cryptography: Security = Reduction



However: No good choice for AES and other block ciphers!

Instead: Theoretical constructions of pseudorandom permutations based on well-established computational assumptions

Not fast enough for practice

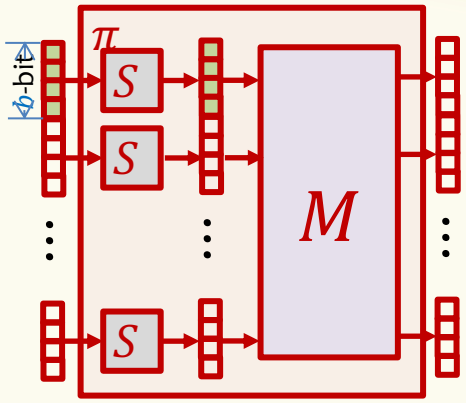
[Luby-Rackoff 88] + one-way functions [GGM84,HILL99] / factoring [NR04,…] / lattice problems [BPR12,…] / …

The bottom line

Individual **AES** *rounds are very weak …*

… with no measurable cryptographic security …

… yet, somehow, they become secure when iterated!



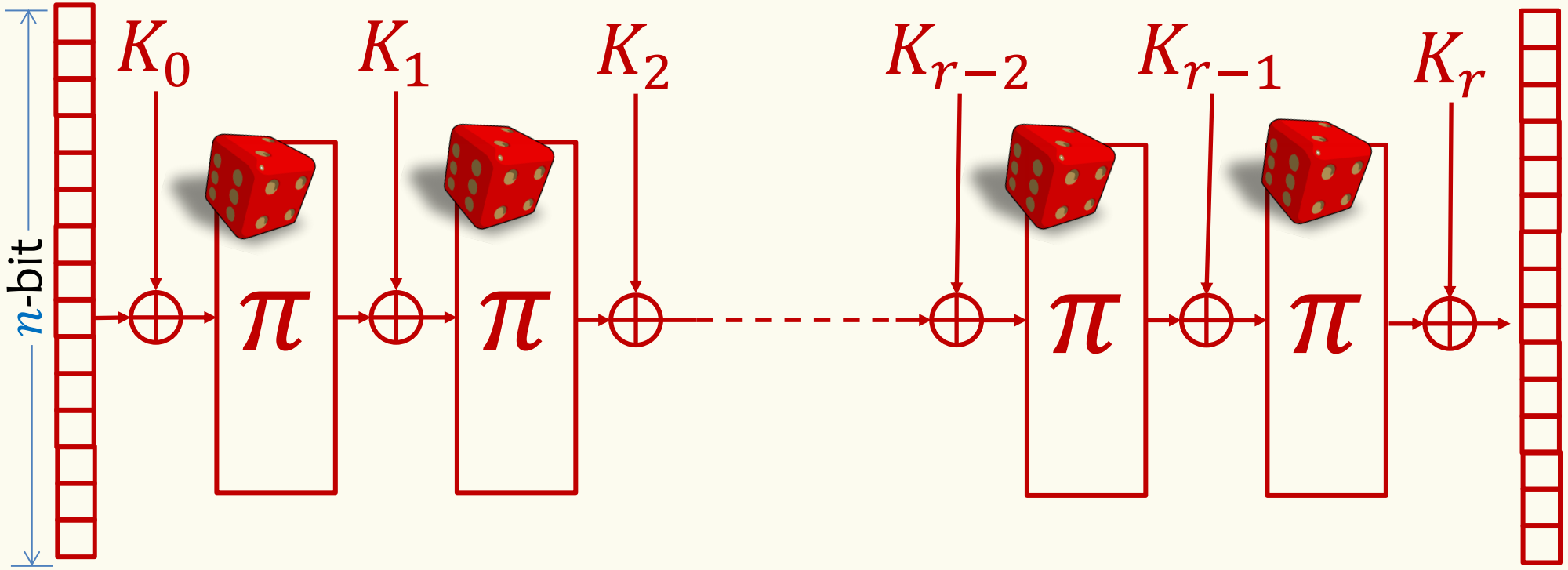
Absolutely no idea how to prove that this is true in the sense of provable security!

We <u>can</u> amplify weak PRP security [Maurer-**T** ‘09, **T** ’11] but too strong of a property already!

This talk – A theoretically grounded agenda

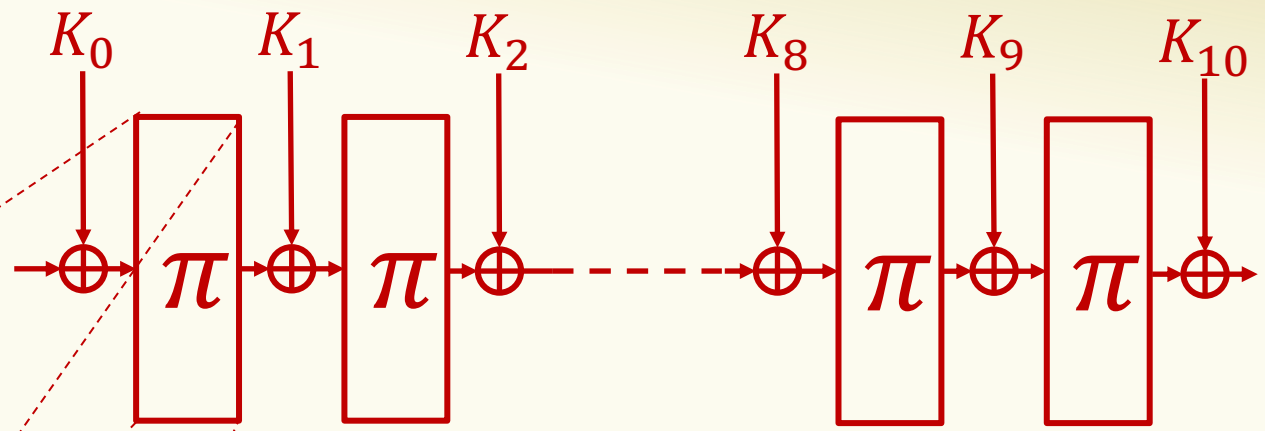
- Ideal-model analyses
- k-wise independence
- Disproving conjectures
- Other things we may be able to prove

Ideal-model analyses – Permutation level

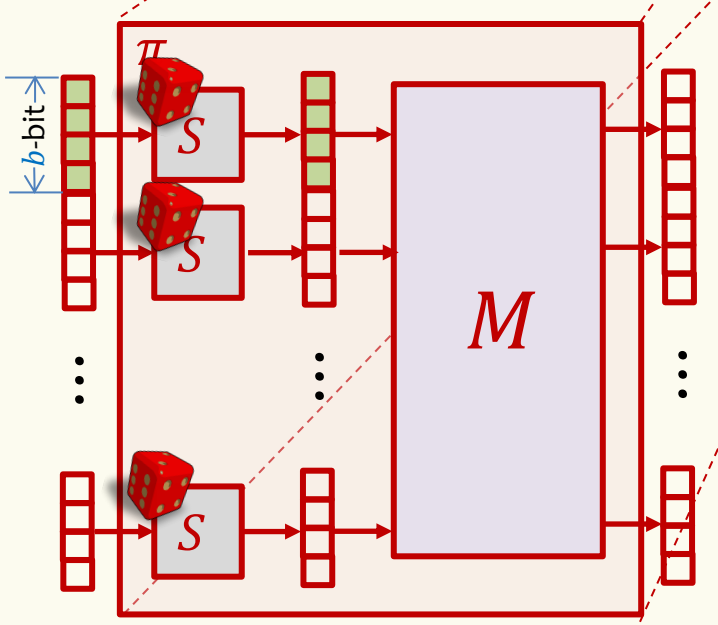


Idea: π / π^{-1} = random permutation oracle, bounded queries (up to 2^n)

[EM97, BKL+12, Ste12, ABD+13, LS14, CS14, CLL+14, HT16, DSST17, TZ21, …]



$n = k \times b$



Alternative: S / S^{-1} = random permutation oracle, bounded queries (up to 2^b) [MV12, CDKLSTZ18, …]

b needs to be large, but conjectures to extend to "small S-box regime" [DKW22]

Small S-box conjecture [Dodis-Karthikeyan-Wichs '22]

▶ **Conjecture 13** (Hardness Amplification; Informal). *Let T be the desired attacker time bound, and assume that r-rounds block cipher E of length wn utilizing idealized block f of size n is $(T, 2^{-\alpha n})$-secure,* as long as *$n > a \log T$ (for some constants $a > 1$ and $\alpha < 1$). Then,* provided *$n > a \log T$, cascading E for $c = O(w/\alpha)$ times will result in a $r' = O(wr/\alpha)$-round block cipher E' which is $(T, O(T/2^{\ell(n)} + 2^{-wn}))$-secure, where $\ell(n)$ is the key length of E' under to corresponding cascading step (equal to c times the key length of E when independent keys are used).*

▶ **Conjecture 14** (Big-to-Small Conjecture; Informal). *Assume a block cipher E' with key length $\ell(n)$ is $(T, \epsilon'(n))$-secure, where $\epsilon'(n) > T/2^{\ell(n)}$, when using ideal building component of length $n \geq a \log T$ (for some $a > 1$). Then, for some constant $n_0 = n_0(a)$, the "scaled down" version of E' using building block f of size $n \geq n_0$ is still $(T, O(\epsilon'(n))$-secure.*

Suggested agenda: Try to break the conjectures!

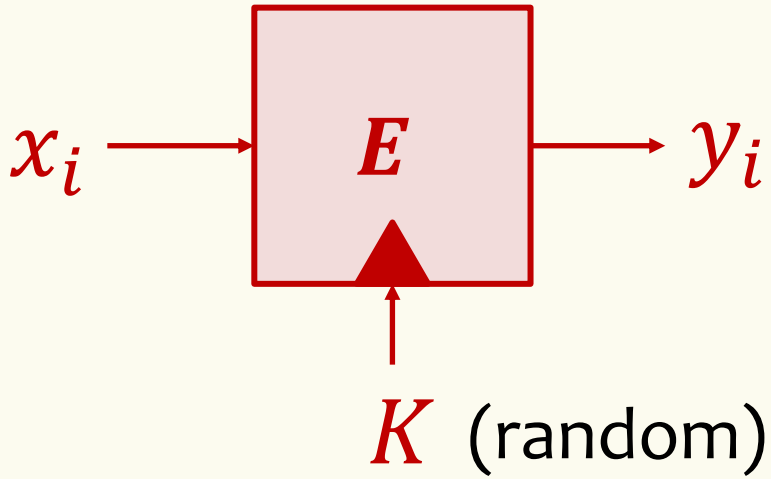
Next best thing: Provable security of non-idealized block ciphers against restricted attack classes

Bounds for differential & linear cryptanalysis [NK95, KMT01,PSC+02, PSLL03, Kel04, KS07, MV12,…]

Here: *t*-wise independence

t-wise independence

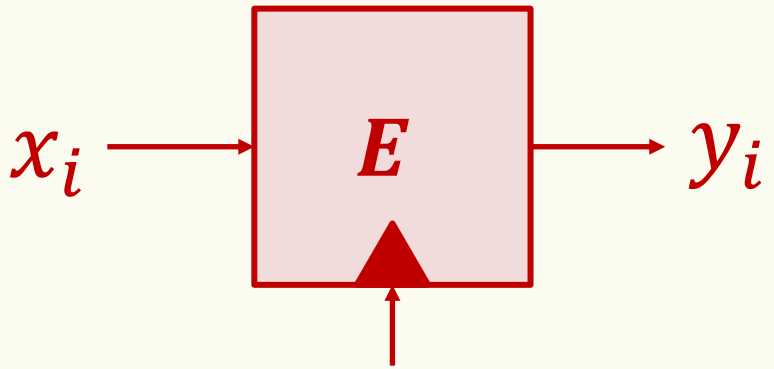
$\boldsymbol{E}: \mathcal{K} \times \{0,1\}^n \to \{0,1\}^n$



∀ inputs $x_1, \ldots, x_t$: outputs $y_1, \ldots, y_t$ are i.i.d. random

ϵ-close to t-wise independence

$\boldsymbol{E}: \mathcal{K} \times \{0,1\}^n \to \{0,1\}^n$



$$\forall\, x_1, \ldots, x_t: \Delta\big((y_1, \ldots, y_t), \mathrm{unif}\big) \leq \epsilon$$

$$\Delta(X, Y) = \frac{1}{2} \sum_x |\Pr[X = x] - \Pr[Y = x]|$$

Feasible when $|K| \geq t \cdot n$ (e.g., assume independent round keys)

- $t = 2 \Longrightarrow$ resistance to linear & differential attacks
- $t = 2^d \Longrightarrow$ resistance to order-d differential attacks
- More generally: resistance to statistical attacks involving t evaluations

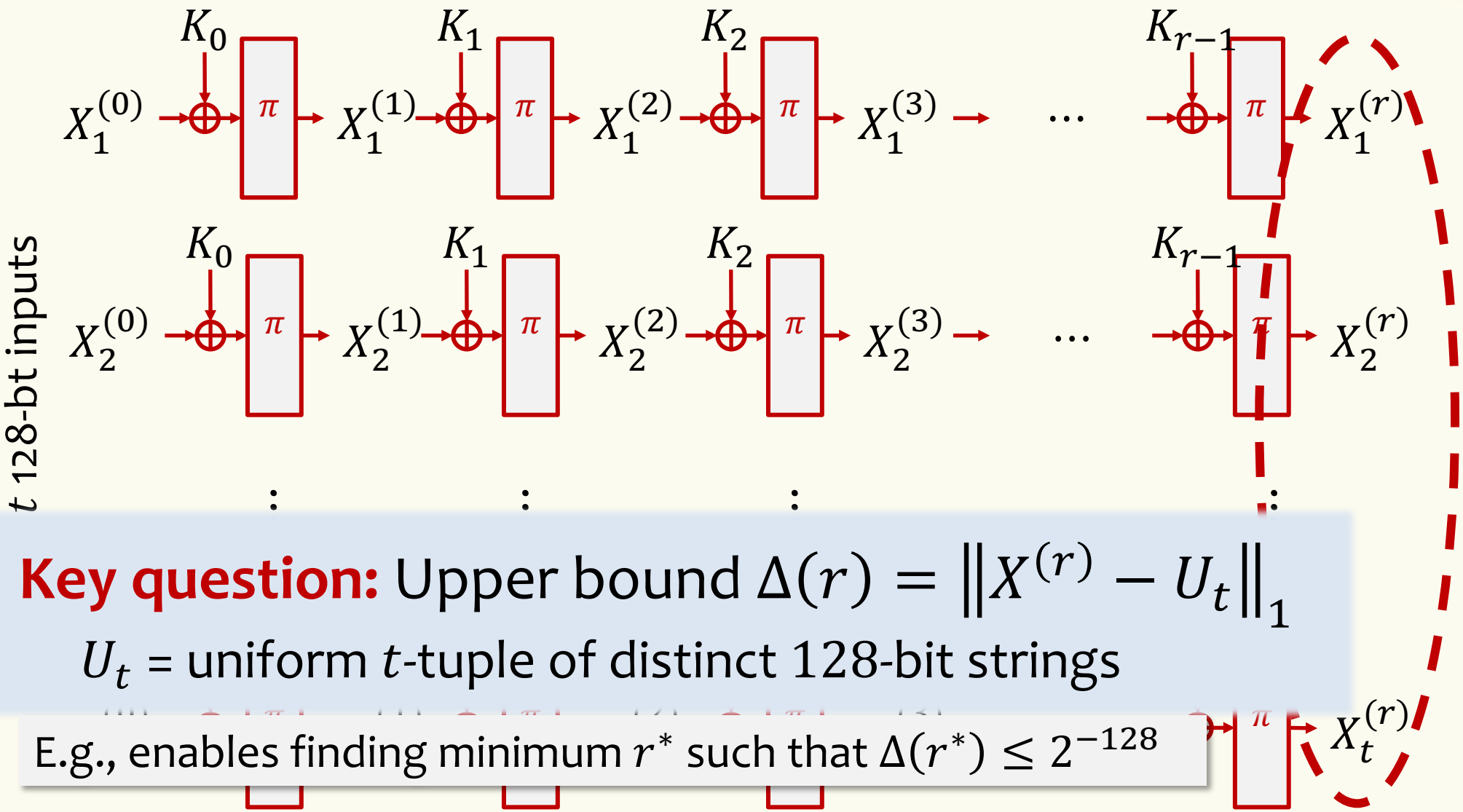
How to prove *t*-wise independence?

Key question: For a given t, how many rounds of AES are sufficient for t-wise independence?*

* With independent round keys

Random Walk Viewpoint

$K_0, K_1, \ldots, K_{r-1} \leftarrow \{0,1\}^{128}$



How close to uniform?

Key question: Upper bound $\Delta(r) = \left\| X^{(r)} - U_t \right\|_1$

U_t = uniform t-tuple of distinct 128-bit strings

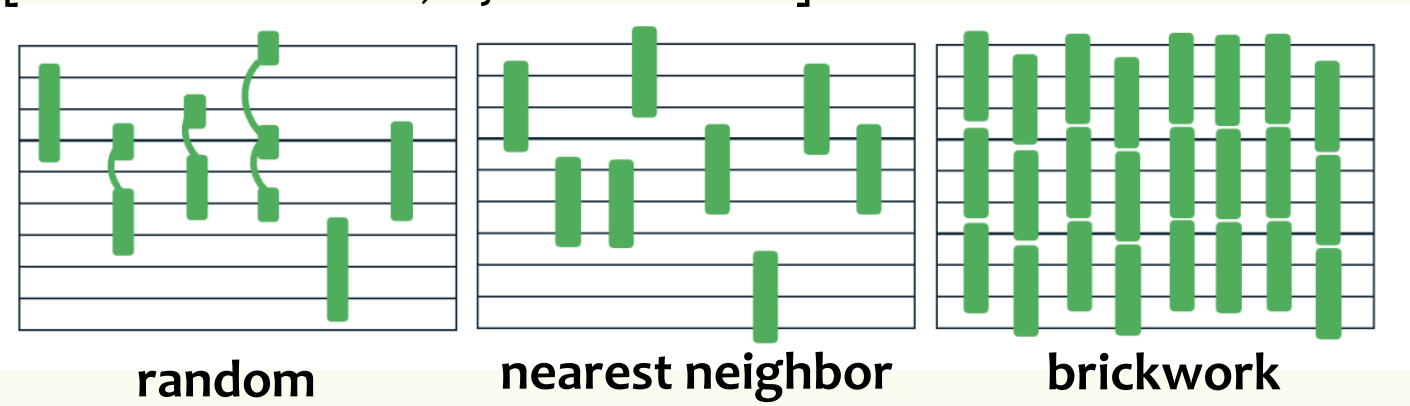
E.g., enables finding minimum r^* such that $\Delta(r^*) \leq 2^{-128}$

Related work – t-wise independence of random local circuits

[Gow89, HMMR05, BH08, HO'D24, GHP24, CHH+24]

Idea: Apply random reversible gate(s) to random constant subset of wires

[Credit: William He, Ryan O'Donnell]



State of the art (depth):

- Brickwork: $\left[nt + \log\left(\frac{1}{\epsilon}\right)\right] \cdot \tilde{O}(t)$ [He-O'Donnell, '24]
- Unrestricted: $\min\left\{nt \log\left(\frac{1}{\epsilon}\right), n\left(nt + \log\left(\frac{1}{\epsilon}\right)\right)\right\}$ [GHP24, CHH+24]

Connections with t-designs & black holes 😉

AES/SPNs – Very Partial Results

Construction	t	r^*
AES [Liu-**T**-Vaikuntanathan '21]	2	≈ 9000
AES [Dinur '26]	2	38
AES [Beyne-Leander-Schütt '21]	2	20
AES* [Liu-Pelecanos-**T**-Vaikuntanathan '23]	2	7

AES* = AES with <u>random</u> S-box

For $t > 2$, all results are for: **SPN*** [Liu-Pelecanos-**T**-Vaikuntanathan '23] or "censored" version of **SPN** [Jain-Liu-Mizgerd-Pelecanos-**T**-Vaikuntanathan '25]

Only meaningful for general SPNs, asymptotic results

SPN* Results

Maximum branch number

r rounds = (r + 1 S-box) + (r mixing) layers

Theorem. r rounds of SPN* suffice to reach ε-close to c-wise independence

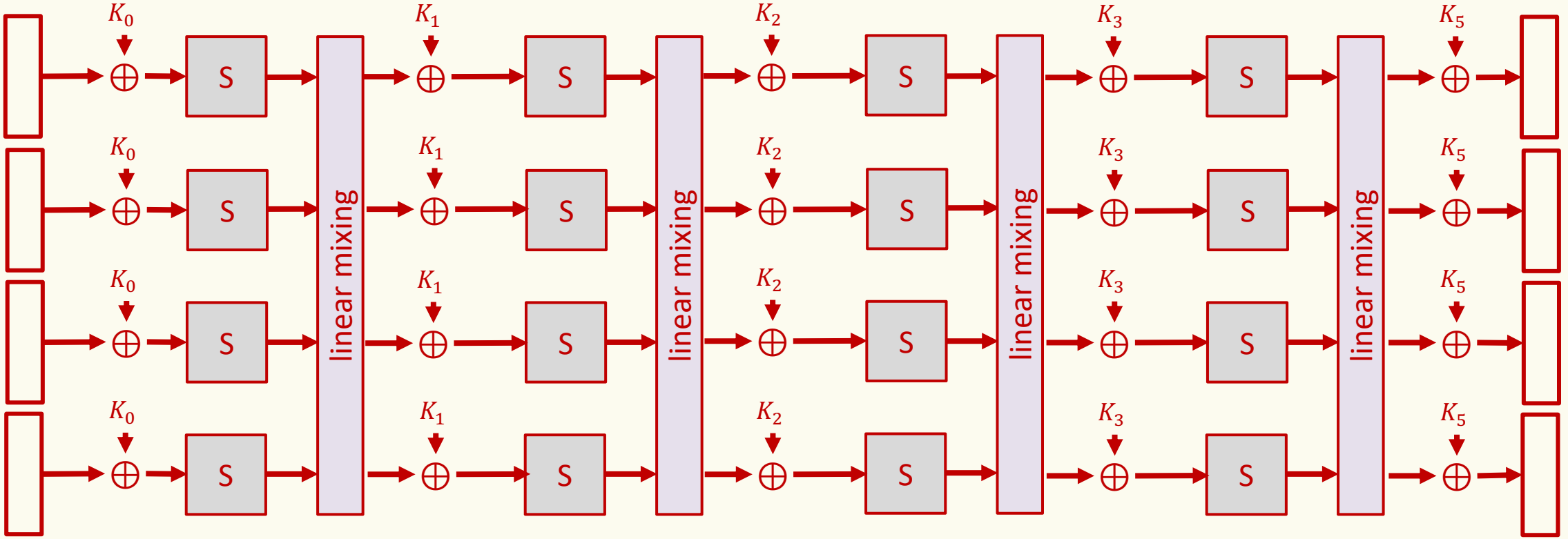
[Liu-Pelecanos-**T**-Vaikuntanathan '23]

Rounds r	ε-Closeness	t
2	$2^{-\Omega(kb)}$	$O(1)$
2	2^{-b}	$2^{\left(0.499-\frac{1}{4k}\right)b}$
$O(k)$	$2^{-\Omega(kb)}$	$2^{\left(0.499-\frac{1}{4k}\right)b}$
$O(\log t)$	$2^{-\Omega(kb)}$	$2^{0.499b}$

Open questions:
Unbounded t

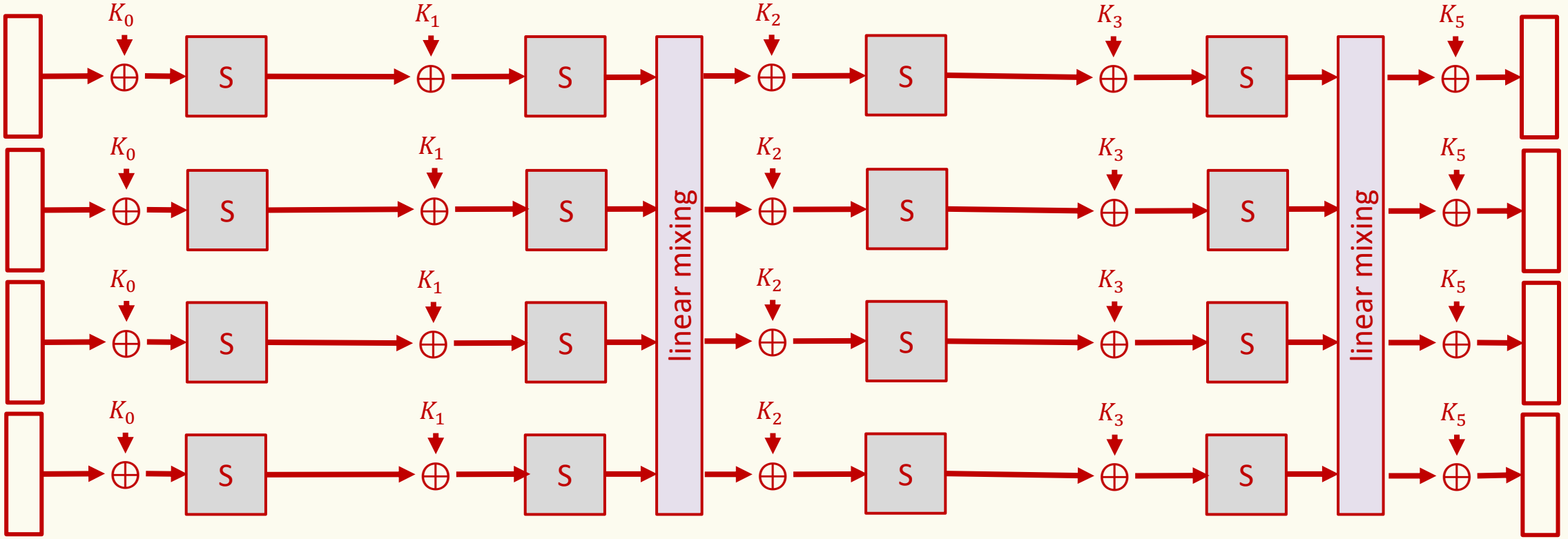
Limitation
t only goes up to $\approx \sqrt{2^b}$

Censored AES



Censored AES

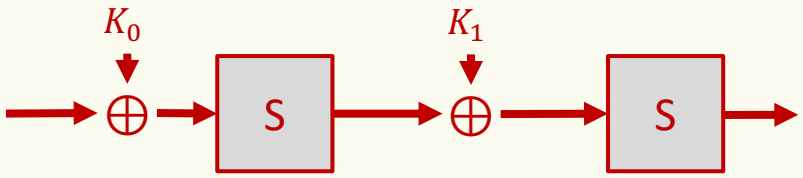
Remove some mixing layers ..



Censored AES conjecture

Conjecture. r-round AES at least as secure as r-round censored AES

Why care?



Behaves like a random permutation after $O(b2^b)$ rounds
[Jain-Liu-Mizgerd-Pelecanos-**T**-Vaikuntanathan, '25]

r-round AES* analysis $\Longrightarrow$ $O(b2^b r)$-round censored AES analysis

What we are and what we are not saying …

Obviously: t-wise independence $\ll$ PRP

– However: implies resistance to some statistical attacks

Conservative interpretation

Resistance to (some) classical cryptanalysis + sanity check

Optimistic interpretation

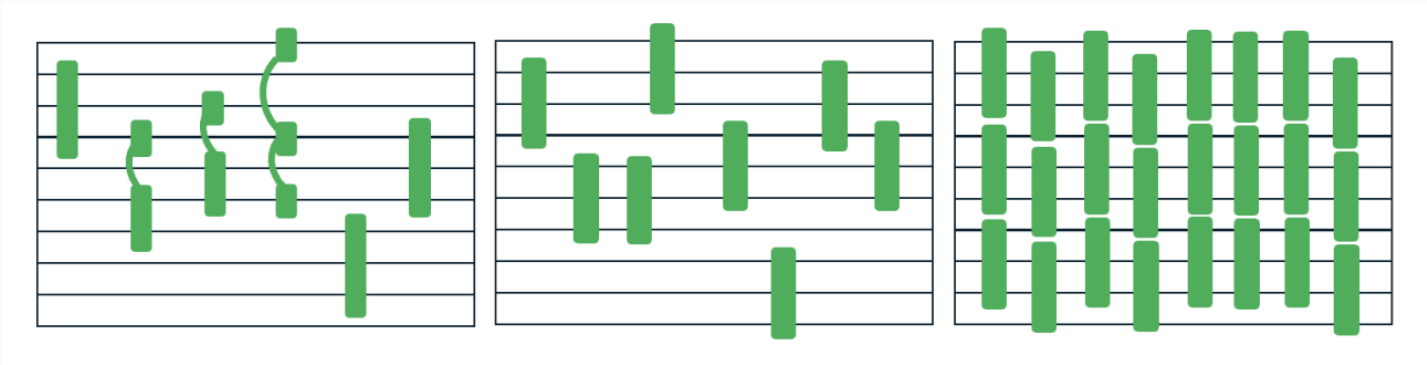
Conjecture: t-wise independence + "nice structure" $\Longrightarrow$ PRP

Caution with Optimism

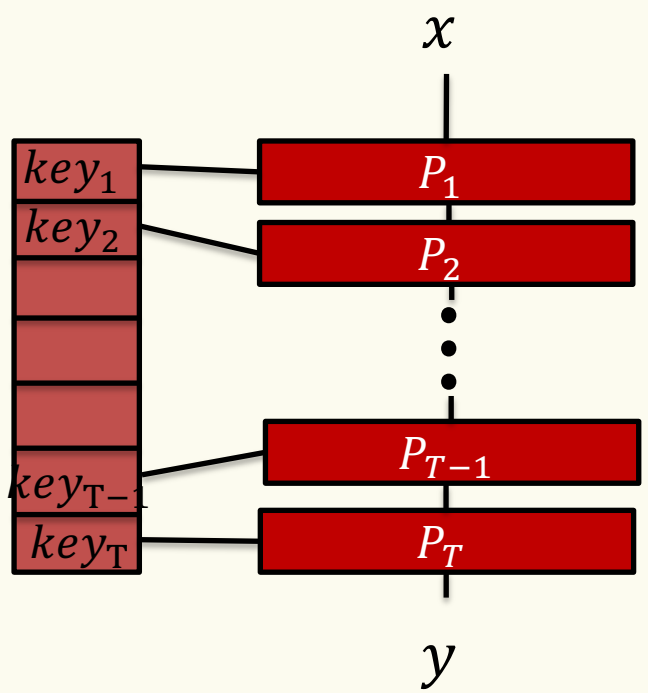
Optimistic interpretation
Conjecture that t-wise independence + "nice structure" $\Longrightarrow$ PRP

Does not apply to AES
[Hoory-Magen-Myers-Rackoff, '04]
$t = 4$ & nice structure = local rounds
("Rackoff conjecture")

Theorem. [Dujmovic-Pelecanos-**T** '26] Rackoff's conjecture is false.



Simpler case: Round-dependent HMMR Conjecture

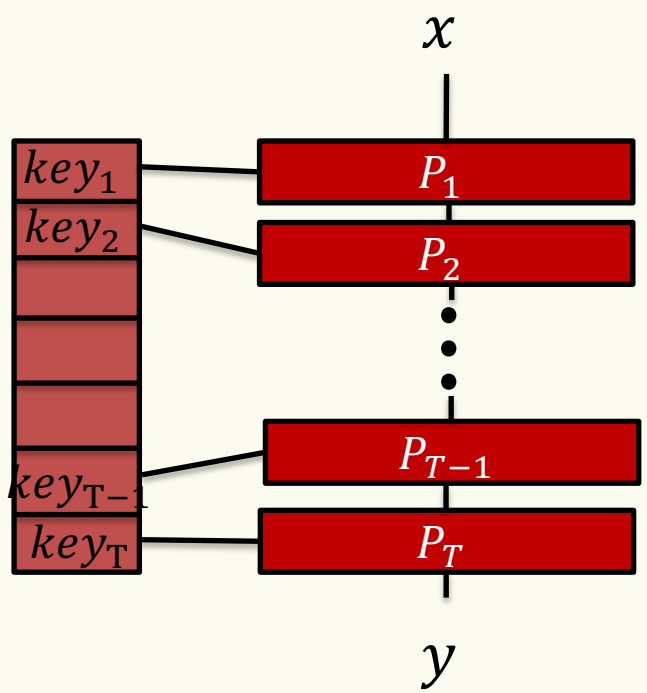


$P_1, \ldots, P_T$ = keyed permutations with constant locality.

We want to show:

1. $P_1 \circ \cdots \circ P_T$ is a 4-wise independent permutation,
2. $P_1 \circ \cdots \circ P_T$ is not a pseudorandom permutation.

Approach = “Special set”

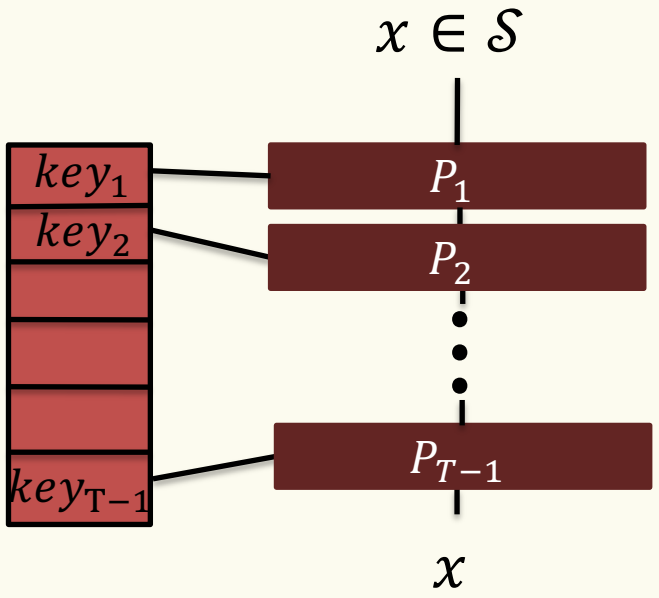


$P_1, \ldots, P_T$ = keyed permutations with constant locality.

Constant size alphabet Σ={♡, 1, 2, 3, 4, 5, …}

Special set $\mathcal{S} = \{♡♡\ldots♡\,1, ♡♡\ldots♡\,2, ♡♡\ldots♡\,3, ♡♡\ldots♡\,4, ♡♡\ldots♡\,5\}$

Special Strings



$P_1, \ldots, P_T$ = keyed permutations with constant locality.

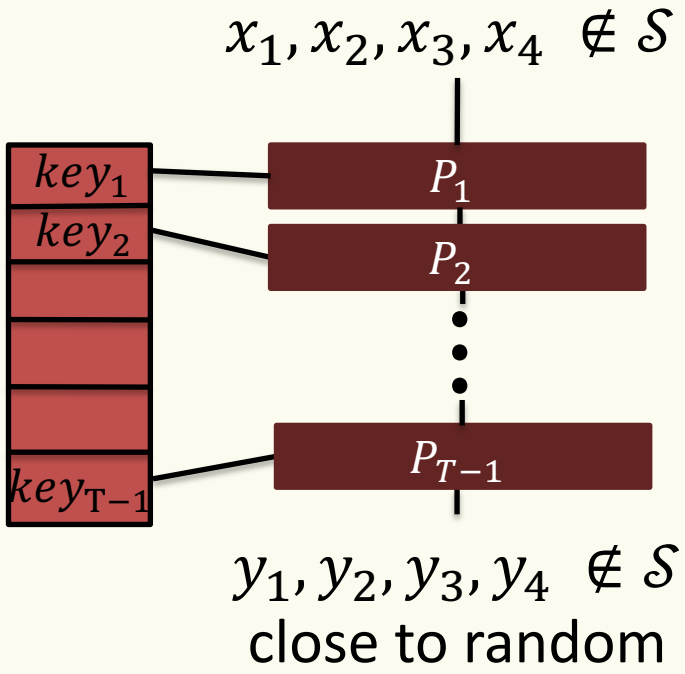
Constant size alphabet Σ={♡, 1, 2, 3, 4, 5, ...}

Special set $\mathcal{S} = \{♡♡...♡\ 1, ♡♡...♡\ 2, ♡♡...♡\ 3, ♡♡...♡\ 4, ♡♡...♡\ 5\}$

For $P_1, \ldots, P_{T-1}$:

- If input $x \in \mathcal{S}$ then $P_i(x) = x$

Non-Special Strings



$P_1, \ldots, P_T$ = keyed permutations with constant locality.

Constant size alphabet Σ={♡, 1, 2, 3, 4, 5, ...}

Special set $\mathcal{S} = \{♡♡...♡\ 1, ♡♡...♡\ 2, ♡♡...♡\ 3, ♡♡...♡\ 4, ♡♡...♡\ 5\}$

For $P_1, \ldots, P_{T-1}$:

- If input $x \in \mathcal{S}$ then $P_i(x) = x$
- If $x_1, x_2, x_3, x_4 \notin \mathcal{S}$ then $y_i = P_1 \circ \cdots \circ P_{T-1}(x_i)$

  y_1, y_2, y_3, y_4 is close to uniformly random.

Special Strings

Special set $\mathcal{S} =$
$\{\heartsuit\heartsuit\ldots\heartsuit\ 1, \heartsuit\heartsuit\ldots\heartsuit\ 2, \heartsuit\heartsuit\ldots\heartsuit\ 3, \heartsuit\heartsuit\ldots\heartsuit\ 4, \heartsuit\heartsuit\ldots\heartsuit\ 5\}$

For P_T:

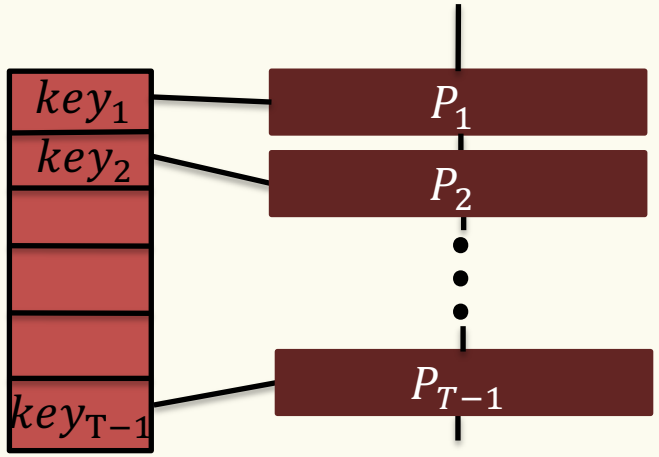
- $\mathrm{w}_i = P_T(\heartsuit\heartsuit\ldots\heartsuit\ i)$

$\mathrm{w}_1, \mathrm{w}_2, \mathrm{w}_3, \mathrm{w}_4, \mathrm{w}_5$ uniform s.t $\mathrm{w}_1 + \mathrm{w}_2 + \mathrm{w}_3 + \mathrm{w}_4 = \mathrm{w}_5$

Combination

Challenges: Implement this locally + round independent

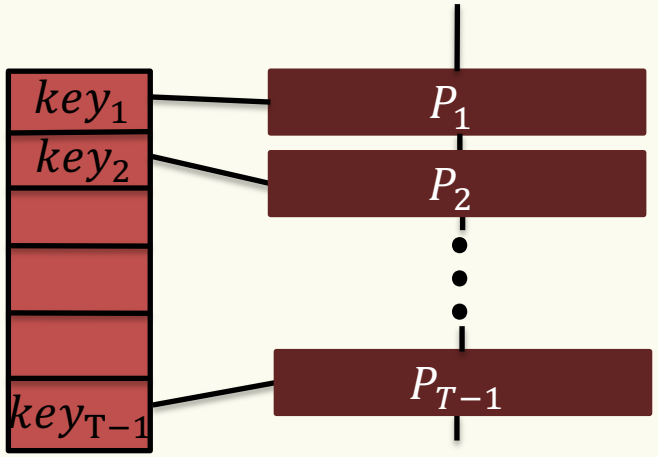
♡♡…♡ 1 ♡♡…♡ 2 ♡♡…♡ 3 ♡♡…♡ 4 ♡♡…♡ 5



♡♡…♡ 1 ♡♡…♡ 2 ♡♡…♡ 3 ♡♡…♡ 4 ♡♡…♡ 5

w_1 w_2 w_3 w_4 $w_1+w_2+w_3+w_4$

1♡♡♡1 2♡♡♡1 ♡♡♡♡♡ 1♡23♡♡



54221♡ 2♡2142 5♡5221 455114

5♡221♡ 2♡2125 5♡5225 455115

Analogous SPN Conjectures?

Can we instantiate an SPN so that:

- It is t-wise independent for a small $t = O(1)$
- Is robust to algebraic attack (in some well understood sense)

But: it is not a pseudorandom permutation!

What else can we hope to prove?

- Tighter bounds for pairwise independence?
- True bounds for $t \geq 3$?
- Algebraic attacks?
- ϵ-biasedness?
- Identify cryptographic hardness in AES structure?

Thank you!