The t-wise Independence of Substitution-Permutation Networks

Tianren Liu[1] Stefano Tessaro[1] Vinod Vaikuntanathan[2]

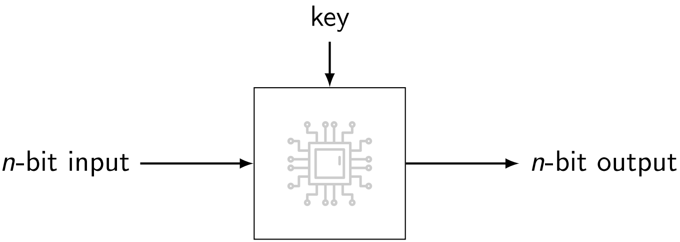
[1]University of Washington, Seattle

[2]MIT, Cambridge

CRYPTO 2021

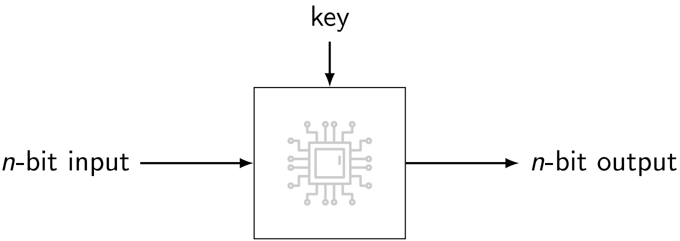
Random-looking Keyed Permutation

indistinguishable from a random permutation



Random-looking Keyed Permutation

indistinguishable from a random permutation



theory

Pseudorandom Permutation

Provable security
based on hardness assumptions

practice

Block Cipher

Heuristic security
resisting known attacks

theory

Pseudorandom Permutation

practice

Block Cipher

theory

Pseudorandom Permutation

practice

Block Cipher

provable security based on . . .

Feistel [LR88] plus
- one-way functions [GGM84]
- factoring [NR04,. . .]
- lattice problems [BPR12,. . .]

theory

Pseudorandom Permutation

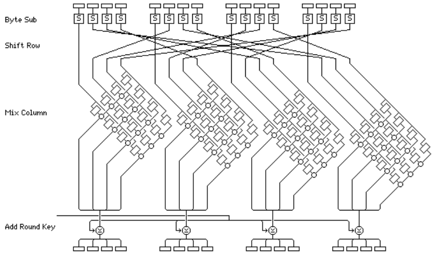
provable security based on . . .

Feistel [LR88] plus
- one-way functions [GGM84]
- factoring [NR04,. . .]
- lattice problems [BPR12,. . .]

practice

Block Cipher

very efficient ciphers (e.g. AES)



theory

Pseudorandom Permutation

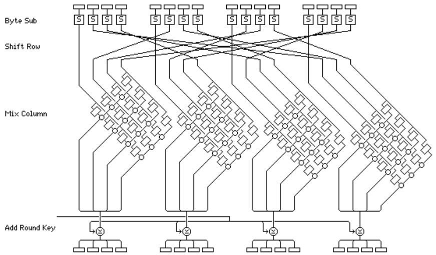
provable security based on . . .

Feistel [LR88] plus
- one-way functions [GGM84]
- factoring [NR04,. . .]
- lattice problems [BPR12,. . .]

practice

Block Cipher

very efficient ciphers (e.g. AES)



Is AES secure? Is AES secure?

theory

Pseudorandom Permutation

provable security based on . . .

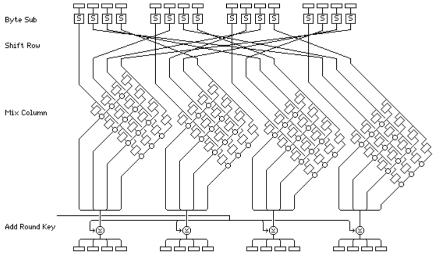
Feistel [LR88] plus
- one-way functions [GGM84]
- factoring [NR04,. . .]
- lattice problems [BPR12,. . .]

Base AES on assumptions?

practice

Block Cipher

very efficient ciphers (e.g. AES)



theory

Pseudorandom Permutation

provable security based on ...

Feistel [LR88] plus
- one-way functions [GGM84]
- factoring [NR04,...]
- lattice problems [BPR12,...]

Base AES on assumptions?

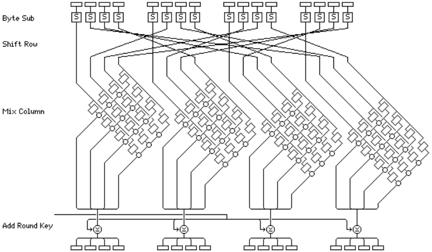
Idealized model

BKL+12, Ste12, ABD+13, LS14, CS14, CLL+14, HT16, DSSL16, GL15, DKS+17, CDK+18, CL18, WYCD20, etc

practice

Block Cipher

very efficient ciphers (e.g. AES)



theory

Pseudorandom Permutation

provable security based on . . .

Feistel [LR88] plus
- one-way functions [GGM84]
- factoring [NR04,. . .]
- lattice problems [BPR12,. . .]

Base AES on assumptions?

Idealized model

BKL+12, Ste12, ABD+13, LS14, CS14, CLL+14, HT16, DSSL16, GL15, DKS+17, CDK+18, CL18, WYCD20, etc

practice

Block Cipher

very efficient ciphers (e.g. AES)

Cryptanalysis

linear [MY92] and differential [BS91] cryptanalysis, higher-order [Lai94] and truncated [Knu94] differential attacks, impossible differential attacks [Knu98], algebraic attacks [JK97], integral cryptanalysis [KW02], biclique attacks [BKR11], etc

theory

Pseudorandom Permutation

provable security based on . . .

Feistel [LR88] plus
- one-way functions [GGM84]
- factoring [NR04,. . .]
- lattice problems [BPR12,. . .]

Base AES on assumptions?

Idealized model

BKL+12, Ste12, ABD+13, LS14, CS14, CLL+14, HT16, DSSL16, GL15, DKS+17, CDK+18, CL18, WYCD20, etc

practice

Block Cipher

very efficient ciphers (e.g. AES)

Cryptanalysis

linear [MY92] and differential [BS91] cryptanalysis, higher-order [Lai94] and truncated [Knu94] differential attacks, impossible differential attacks [Knu98], algebraic attacks [JK97], integral cryptanalysis [KW02], biclique attacks [BKR11], etc

Provable bounds

on the advantage of known attacks

NK95, KMT01, PSC+02, PSLL03, Kel04, KS07, etc

Prove bounds against an attack class

integral cryptanalysis

algebraic attacks

truncated higher-order differential attacks

biclique attacks

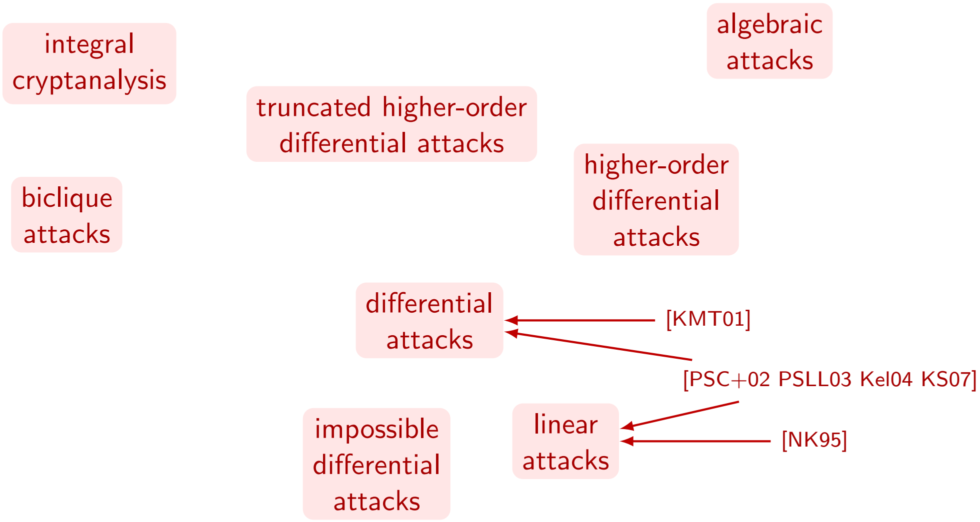
higher-order differential attacks

differential attacks

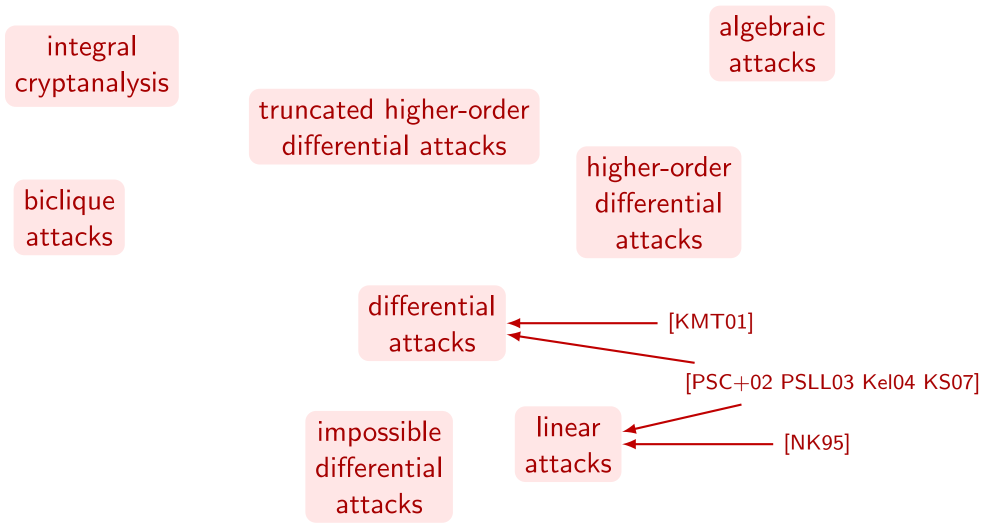
impossible differential attacks

linear attacks

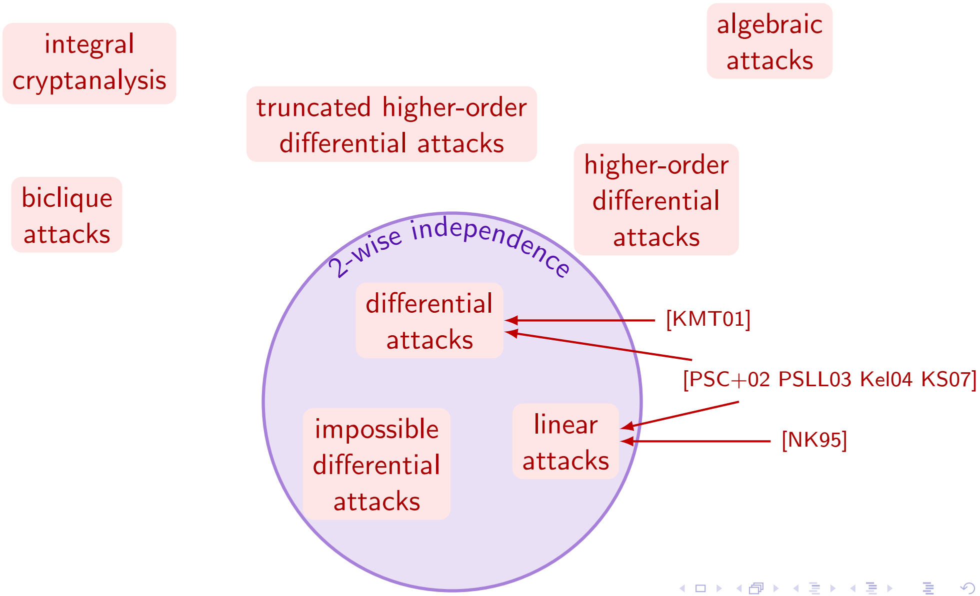
Prove bounds against an attack class



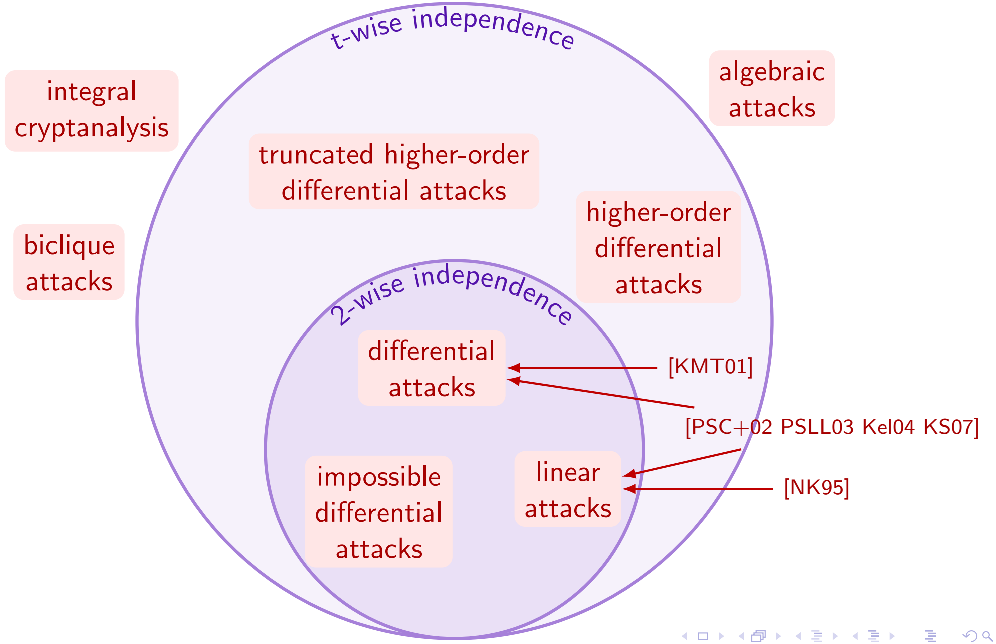
This paper: t-wise independence

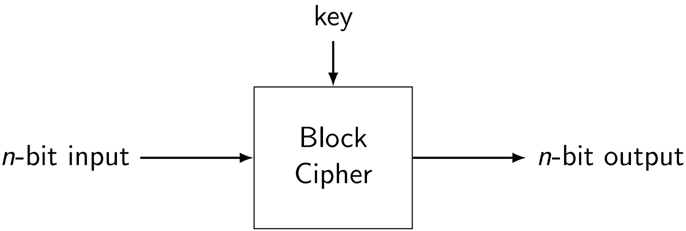


This paper: t-wise independence



This paper: t-wise independence



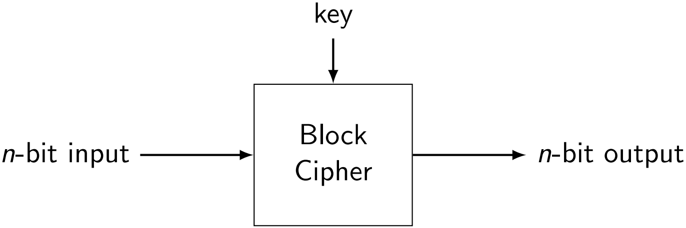


t-wise Independence

$\forall \mathrm{input}_1, \ldots, \mathrm{input}_t$

$\mathrm{output}_1, \ldots, \mathrm{output}_t$ are i.i.d. uniform

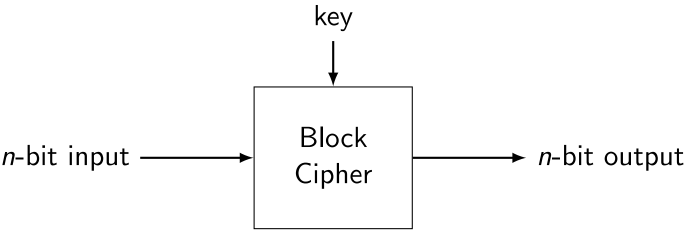
used in [HMMR05, KNR05, BH08, AL13]



ε-close to t-wise Independence

$$\forall \text{input}_1, \ldots, \text{input}_t$$
$$\text{StatisticalDistance}((\text{output}_1, \ldots, \text{output}_t), \text{uniform}) \leq \varepsilon$$

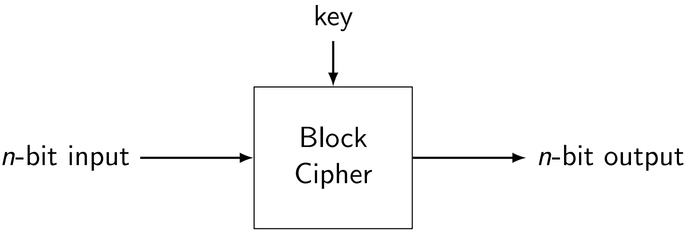
used in [HMMR05, KNR05, BH08, AL13]



ε-close to t-wise Independence

$$\forall \mathrm{input}_1, \ldots, \mathrm{input}_t$$
$$\mathrm{StatisticalDistance}((\mathrm{output}_1, \ldots, \mathrm{output}_t), \mathrm{uniform}) \leq \varepsilon$$

Feasible when $|\mathrm{key}| \geq t \cdot n$

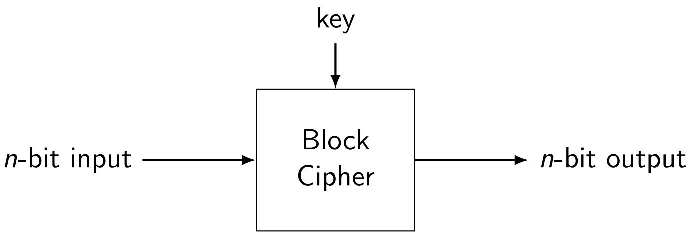


ε-close to t-wise Independence

$\forall \text{input}_1, \ldots, \text{input}_t$

$\text{StatisticalDistance}((\text{output}_1, \ldots, \text{output}_t), \text{uniform}) \leq \varepsilon$

Feasible when $|\text{key}| \geq t \cdot n$ e.g. assume independent round keys

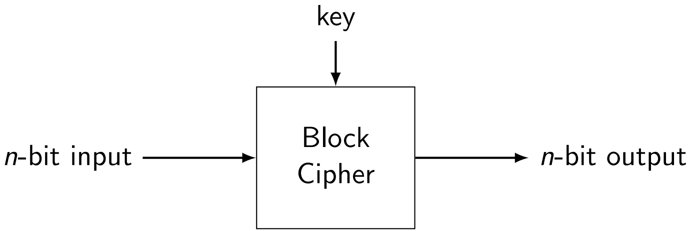


ε-close to t-wise Independence

$$\forall \text{input}_1, \ldots, \text{input}_t$$
$$\text{StatisticalDistance}((\text{output}_1, \ldots, \text{output}_t), \text{uniform}) \leq \varepsilon$$

Feasible when $|\text{key}| \geq t \cdot n$ e.g. assume independent round keys

Statistically indistinguishable with t non-adaptive queries



ε-close to t-wise Independence

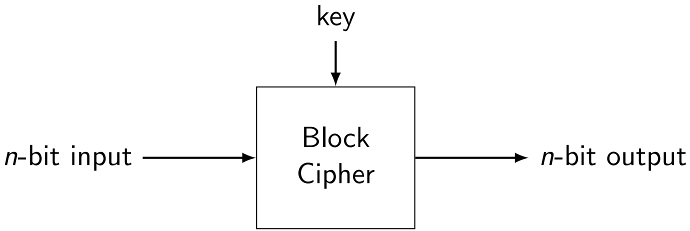
$\forall \text{input}_1, \ldots, \text{input}_t$

$\text{StatisticalDistance}((\text{output}_1, \ldots, \text{output}_t), \text{uniform}) \leq \varepsilon$

Feasible when $|\text{key}| \geq t \cdot n$ e.g. assume independent round keys

Statistically indistinguishable with t non-adaptive queries

- 2 non-adaptive queries **linear & differential attacks**



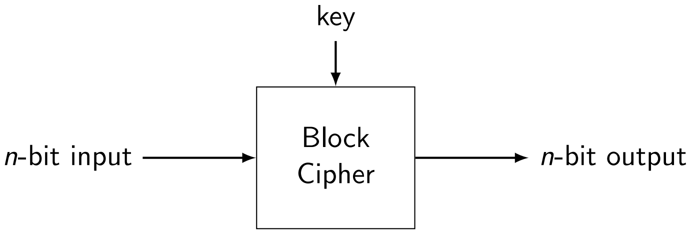
ε-close to t-wise Independence

$$\forall \text{input}_1, \ldots, \text{input}_t$$
$$\text{StatisticalDistance}((\text{output}_1, \ldots, \text{output}_t), \text{uniform}) \leq \varepsilon$$

Feasible when $|\text{key}| \geq t \cdot n$ e.g. assume independent round keys

Statistically indistinguishable with t non-adaptive queries

- 2 non-adaptive queries **linear & differential attacks**
- 2^d non-adaptive queries **order-d differential attacks**



ε-close to t-wise Independence

$$\forall \text{input}_1, \ldots, \text{input}_t$$
$$\text{StatisticalDistance}((\text{output}_1, \ldots, \text{output}_t), \text{uniform}) \leq \varepsilon$$

Feasible when $|\text{key}| \geq t \cdot n$ e.g. assume independent round keys

Statistically indistinguishable with t non-adaptive queries

$$\varepsilon\text{-close to 2-wise indp} \implies \begin{cases} \text{MEDP} \leq \varepsilon + \frac{1}{2^n - 1} & \text{(differential attack)} \\ \text{CORR} \leq 8\varepsilon + \frac{4}{2^n} & \text{(linear attack)} \end{cases}$$

Key-Alternating Cipher (KAC)

Substitution-Permutation Network (SPN)

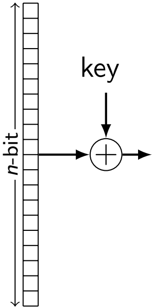
Advanced Encryption Standard (AES)

Key-Alternating Cipher (KAC)

Substitution-Permutation Network (SPN)

Advanced Encryption Standard (AES)

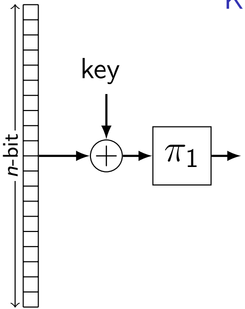
Key-Alternating Cipher (KAC)



Substitution-Permutation Network (SPN)

Advanced Encryption Standard (AES)

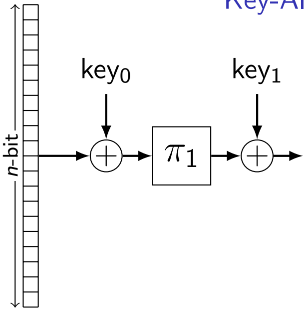
Key-Alternating Cipher (KAC)



Substitution-Permutation Network (SPN)

Advanced Encryption Standard (AES)

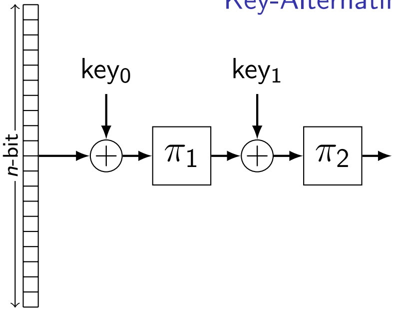
Key-Alternating Cipher (KAC)



Substitution-Permutation Network (SPN)

Advanced Encryption Standard (AES)

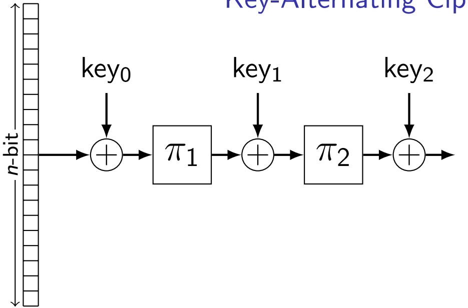
Key-Alternating Cipher (KAC)



Substitution-Permutation Network (SPN)

Advanced Encryption Standard (AES)

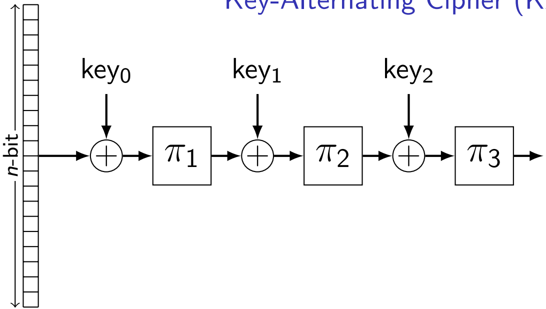
Key-Alternating Cipher (KAC)



Substitution-Permutation Network (SPN)

Advanced Encryption Standard (AES)

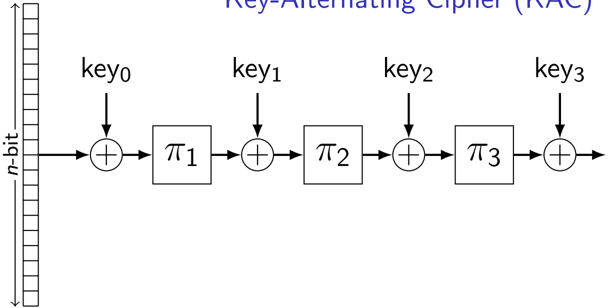
Key-Alternating Cipher (KAC)



Substitution-Permutation Network (SPN)

Advanced Encryption Standard (AES)

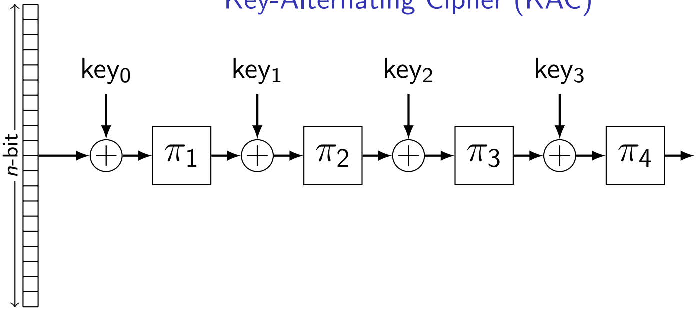
Key-Alternating Cipher (KAC)



Substitution-Permutation Network (SPN)

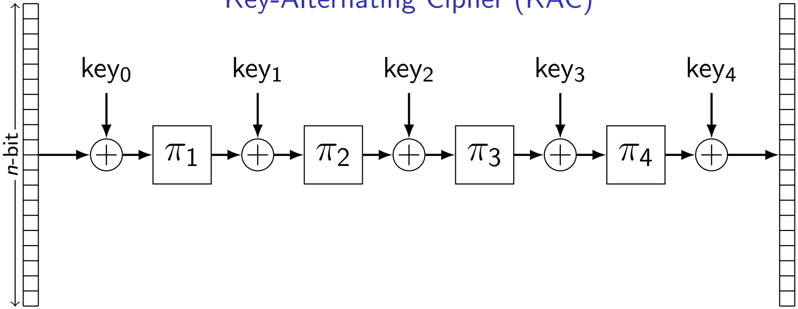
Advanced Encryption Standard (AES)

Key-Alternating Cipher (KAC)



Substitution-Permutation Network (SPN)   Advanced Encryption Standard (AES)

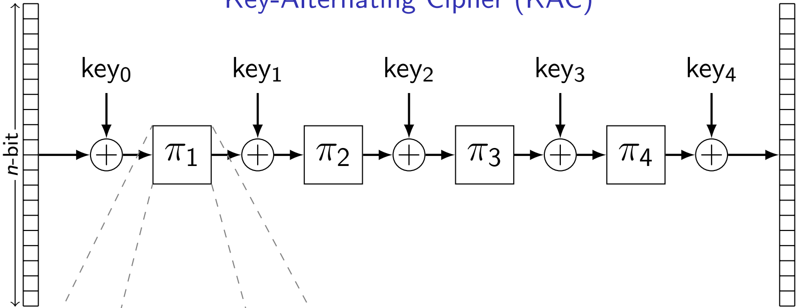
Key-Alternating Cipher (KAC)



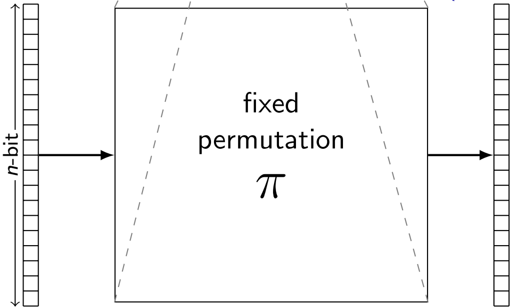
Substitution-Permutation Network (SPN)

Advanced Encryption Standard (AES)

Key-Alternating Cipher (KAC)

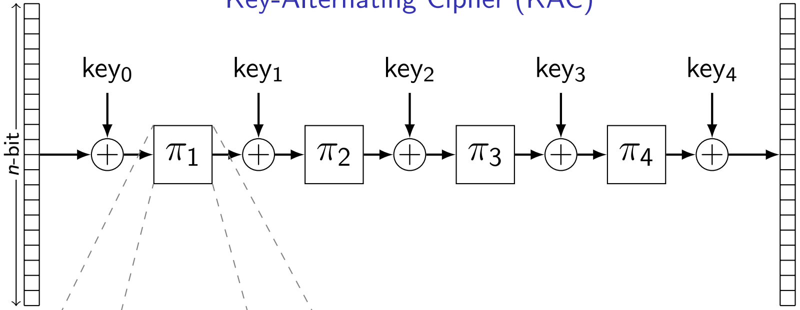


Substitution-Permutation Network (SPN)

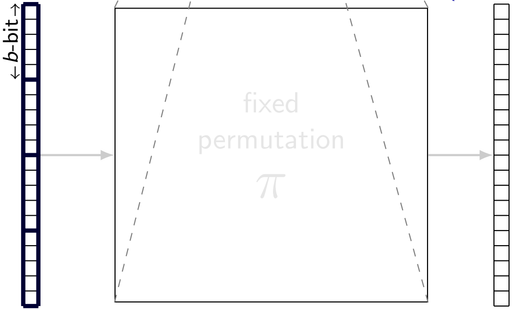


Advanced Encryption Standard (AES)

Key-Alternating Cipher (KAC)

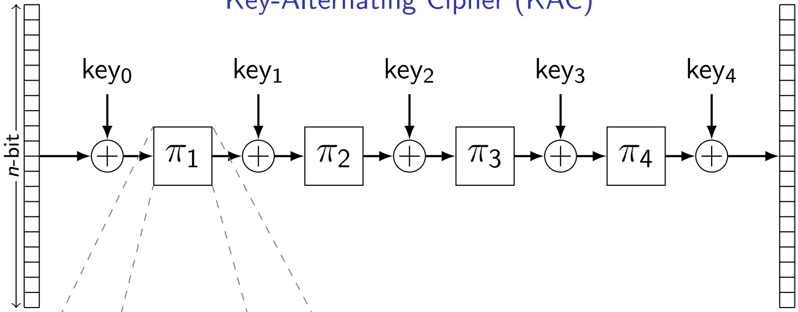


Substitution-Permutation Network (SPN)

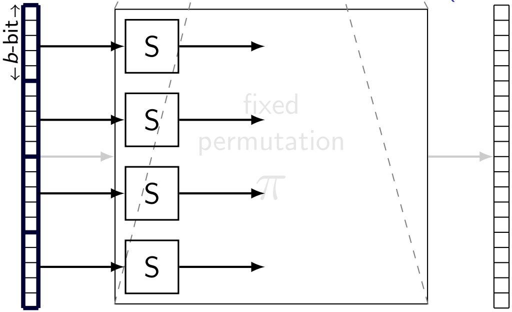


Advanced Encryption Standard (AES)

Key-Alternating Cipher (KAC)

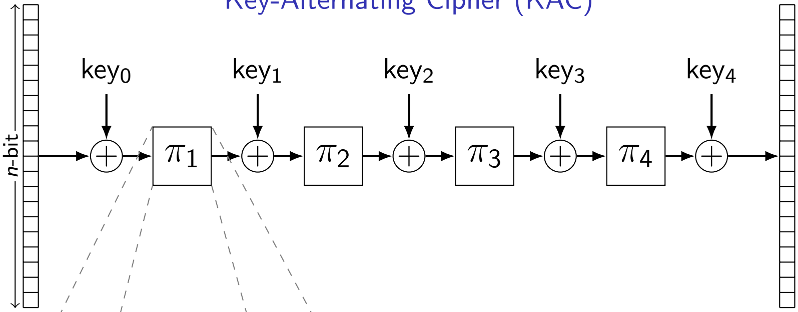


Substitution-Permutation Network (SPN)

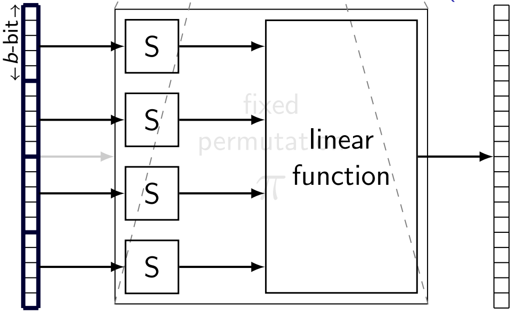


Advanced Encryption Standard (AES)

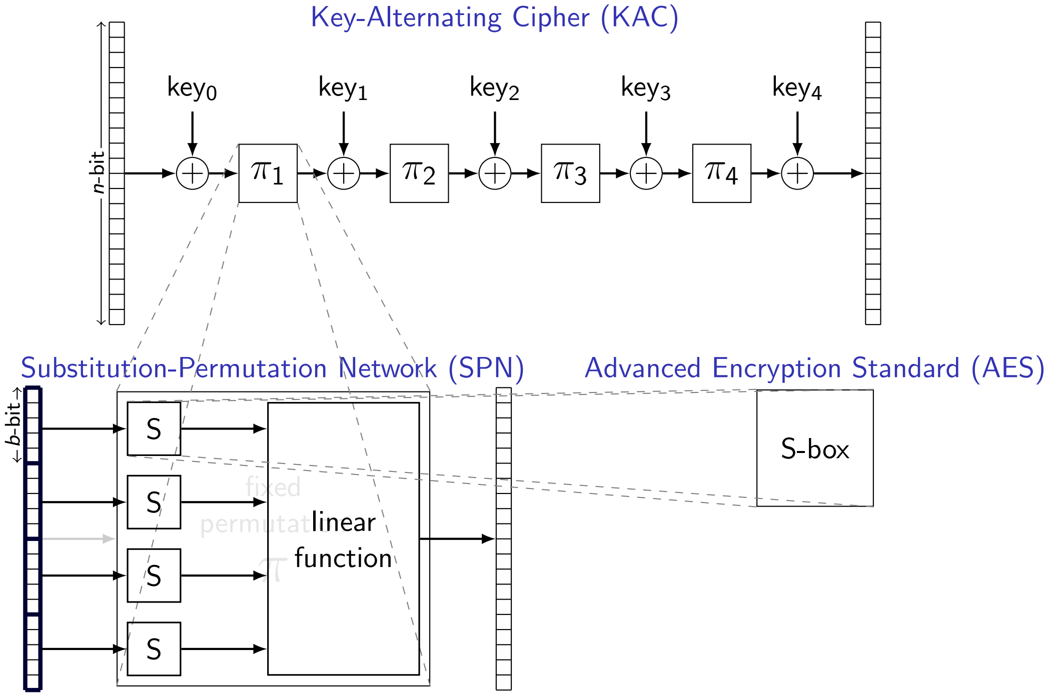
Key-Alternating Cipher (KAC)

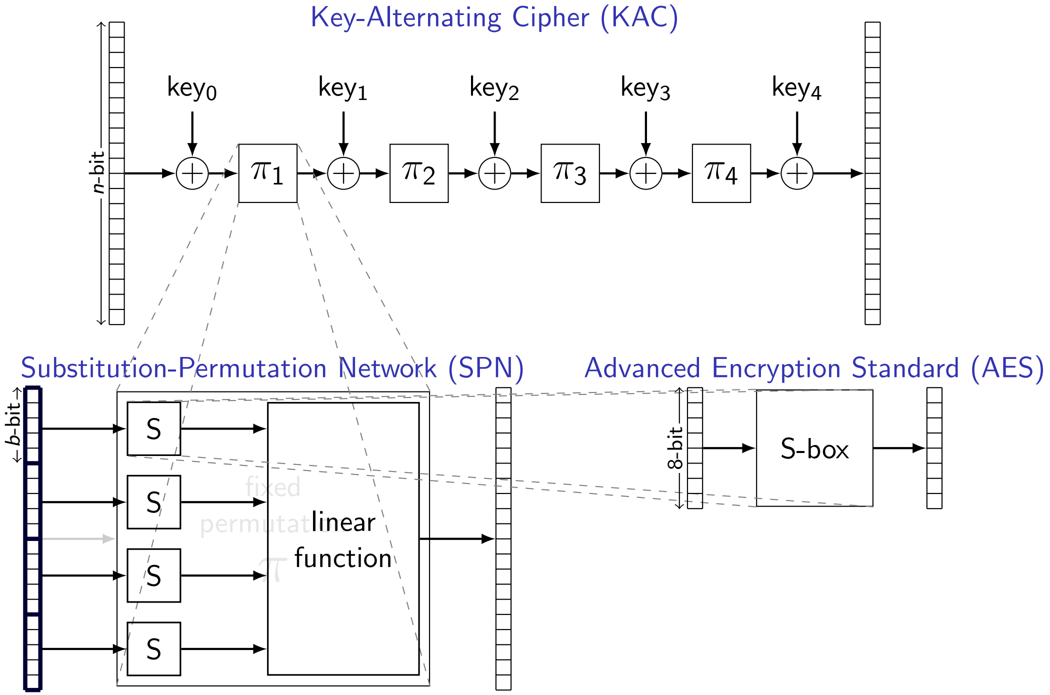


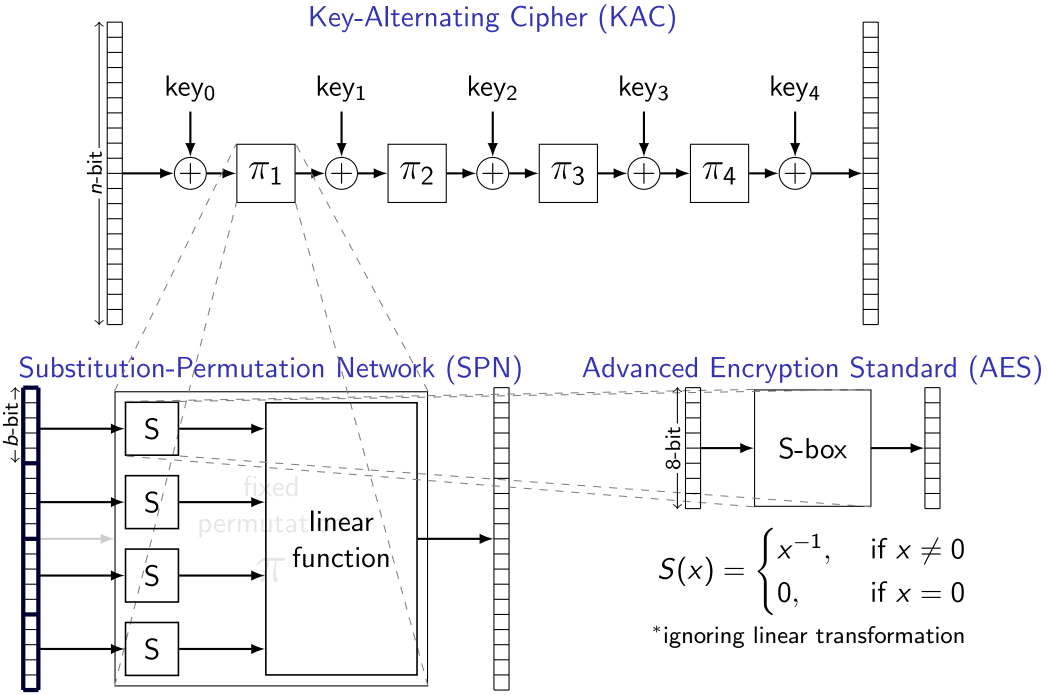
Substitution-Permutation Network (SPN)



Advanced Encryption Standard (AES)


Key-Alternating Cipher (KAC)
n-bit
key0
key1
key2
key3
key4
π1
π2
π3
π4
Substitution-Permutation Network (SPN)
Advanced Encryption Standard (AES)
b-bit
S
S
S
S
fixed
permutation
π
linear
function
S-box

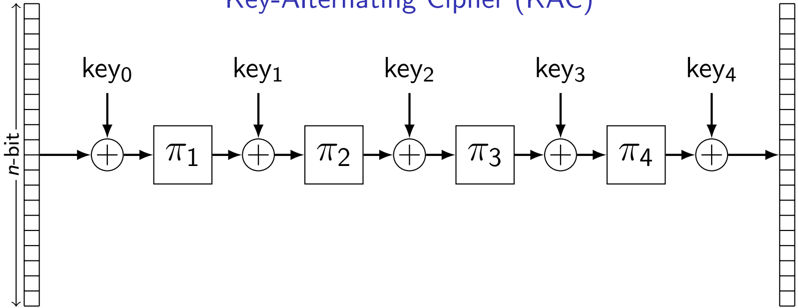

Key-Alternating Cipher (KAC)
n-bit
key0
key1
key2
key3
key4
π1
π2
π3
π4
Substitution-Permutation Network (SPN)
Advanced Encryption Standard (AES)
b-bit
S
S
S
S
fixed
permutation
π
linear
function
8-bit
S-box



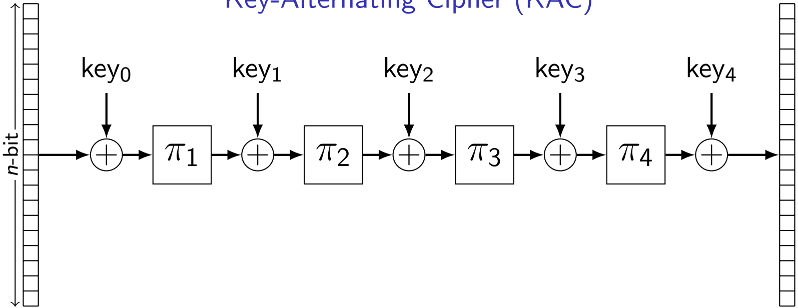
$$S(x) = \begin{cases} x^{-1}, & \text{if } x \neq 0 \\ 0, & \text{if } x = 0 \end{cases}$$

*ignoring linear transformation

Key-Alternating Cipher (KAC)

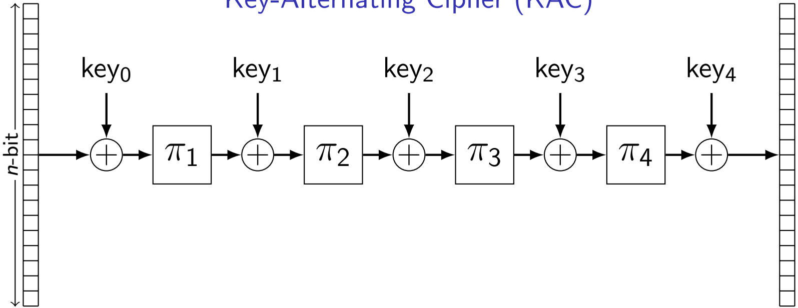


Key-Alternating Cipher (KAC)



r-round $\mathrm{KAC}(\pi_1, \ldots, \pi_r)$ is not $(r+2)$-wise independent

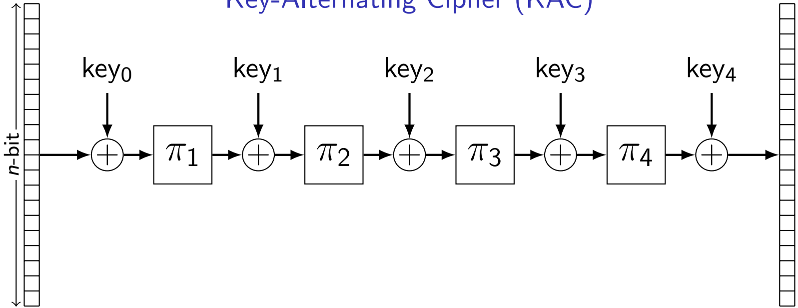
Key-Alternating Cipher (KAC)



Our Results (KAC)

r-round KAC$(\pi_1, \ldots, \pi_r)$ is close to $(r - o(r))$-wise independent for most $\pi_1, \ldots, \pi_r$

Key-Alternating Cipher (KAC)

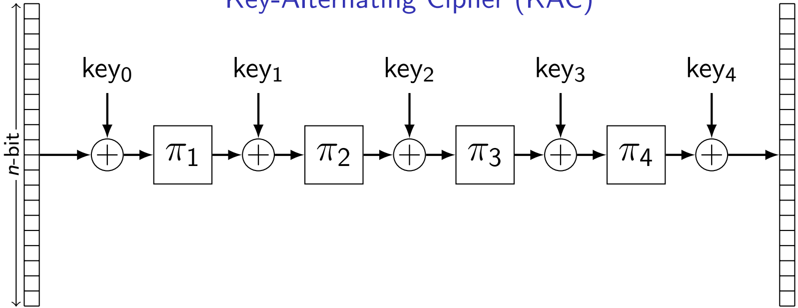


Our Results (KAC)

r-round KAC$(\pi_1, \ldots, \pi_r)$ is close to
$(r - o(r))$-wise independent
for most $\pi_1, \ldots, \pi_r$

*existential result & probabilistic method

Key-Alternating Cipher (KAC)

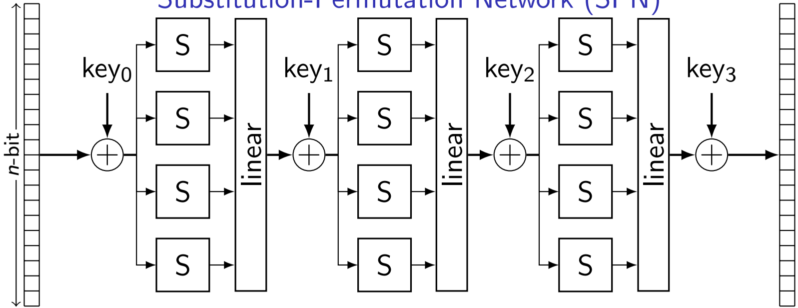


Our Results (KAC)

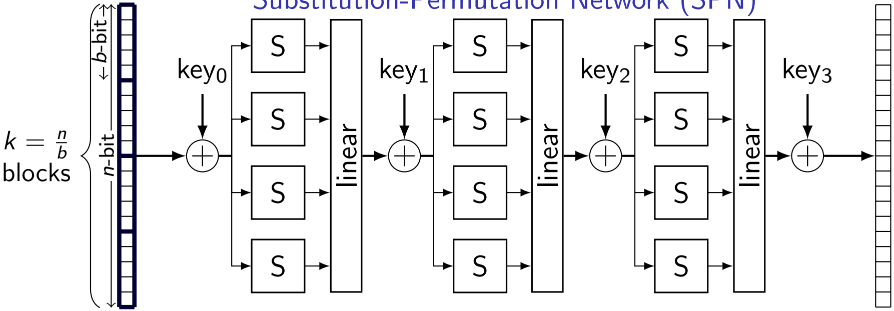
r-round KAC$(\pi_1, \ldots, \pi_r)$ is close to
$(r - o(r))$-wise independent
for most $\pi_1, \ldots, \pi_r$

*existential result & probabilistic method
*unlike ideal model results, $\pi_1, \ldots, \pi_r$ are completely known to adv

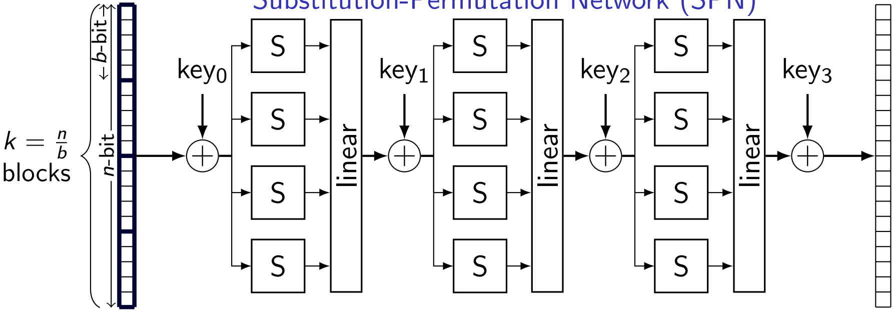
Substitution-Permutation Network (SPN)



Substitution-Permutation Network (SPN)

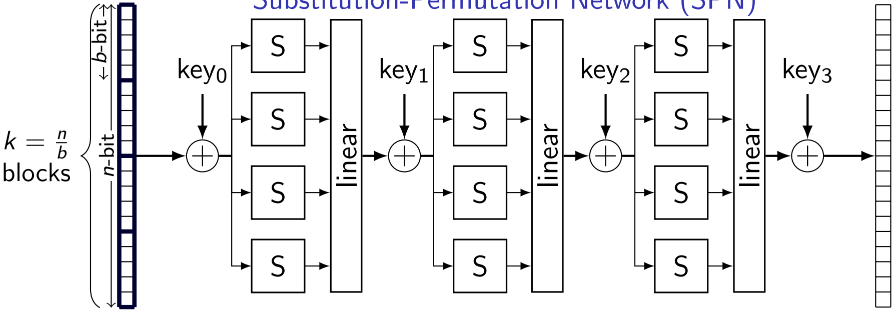


Substitution-Permutation Network (SPN)



$S(x) = x^{-1}$ (used by AES) *or* $S(x) = x^3$ (used by MiMC)

Substitution-Permutation Network (SPN)

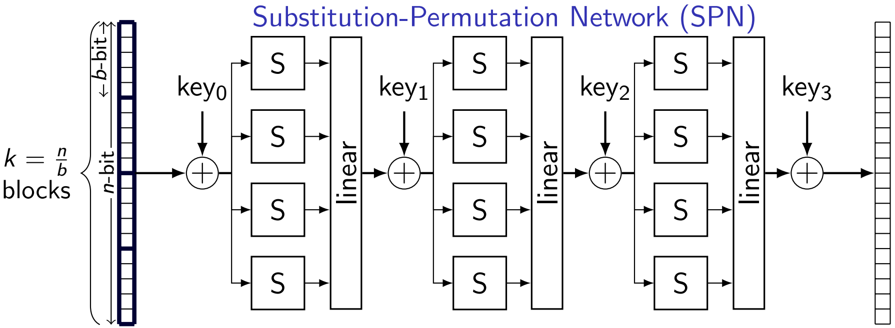


$S(x) = x^{-1}$ (used by AES) *or* $S(x) = x^3$ (used by MiMC)

Our Results

2-round SPN is $(\frac{4k}{2^b} + \sqrt{\frac{2^k}{2^b}})$-close to 2-wise independent.

3-round SPN is $(\frac{8k}{2^b} + \sqrt{\frac{k}{2^b}})$-close to 2-wise independent.



$S(x) = x^{-1}$ (used by AES) *or* $S(x) = x^3$ (used by MiMC)

Our Results

2-round SPN is $(\frac{4k}{2^b} + \sqrt{\frac{2^k}{2^b}})$-close to 2-wise independent.

3-round SPN is $(\frac{8k}{2^b} + \sqrt{\frac{k}{2^b}})$-close to 2-wise independent.

6-round AES is 0.472-close to 2-wise independent.

Our Results (SPN & AES)

2-round SPN is $(\frac{4k}{2^b} + \sqrt{\frac{2^k}{2^b}})$-close to 2-wise independent.

3-round SPN is $(\frac{8k}{2^b} + \sqrt{\frac{k}{2^b}})$-close to 2-wise independent.

6-round AES is 0.472-close to 2-wise independent.

Our Results (SPN & AES)

2-round SPN is $(\frac{4k}{2^b} + \sqrt{\frac{2^k}{2^b}})$-close to 2-wise independent.

3-round SPN is $(\frac{8k}{2^b} + \sqrt{\frac{k}{2^b}})$-close to 2-wise independent.

6-round AES is 0.472-close to 2-wise independent.

State of the art [Park-Sung-Lee-Lim 03]

4-round AES is pointwise 2^{17}-close to 2-wise independent.

Our Results (SPN & AES)

2-round SPN is $(\frac{4k}{2^b} + \sqrt{\frac{2^k}{2^b}})$-close to 2-wise independent.

3-round SPN is $(\frac{8k}{2^b} + \sqrt{\frac{k}{2^b}})$-close to 2-wise independent.

6-round AES is 0.472-close to 2-wise independent.

State of the art [Park-Sung-Lee-Lim 03]

4-round AES is pointwise 2^{17}-close to 2-wise independent.

def pointwise ε-close to uniform

$$1 - \varepsilon \leq \frac{\Pr[X \leftarrow \text{distribution}; X = v]}{\Pr[X \leftarrow \text{uniform}; X = v]} \leq 1 + \varepsilon$$

Our Results (SPN & AES)

2-round SPN is $(\frac{4k}{2^b} + \sqrt{\frac{2^k}{2^b}})$-close to 2-wise independent.

3-round SPN is $(\frac{8k}{2^b} + \sqrt{\frac{k}{2^b}})$-close to 2-wise independent.

6-round AES is 0.472-close to 2-wise independent.

MPR Amplification Lemma [Maurer-Pietrzak-Renner 07]

$$\left.\begin{array}{l}\mathcal{F} \text{ is } \varepsilon\text{-close to 2-wise indp.} \\ \mathcal{G} \text{ is } \delta\text{-close to 2-wise indp.}\end{array}\right\} \implies \mathcal{F} \circ \mathcal{G} \text{ is } 2\varepsilon\delta\text{-close to 2-wise indp.}$$

Our Results (SPN & AES)

2-round SPN is $(\frac{4k}{2^b} + \sqrt{\frac{2^k}{2^b}})$-close to 2-wise independent.

3-round SPN is $(\frac{8k}{2^b} + \sqrt{\frac{k}{2^b}})$-close to 2-wise independent.

6-round AES is 0.472-close to 2-wise independent.

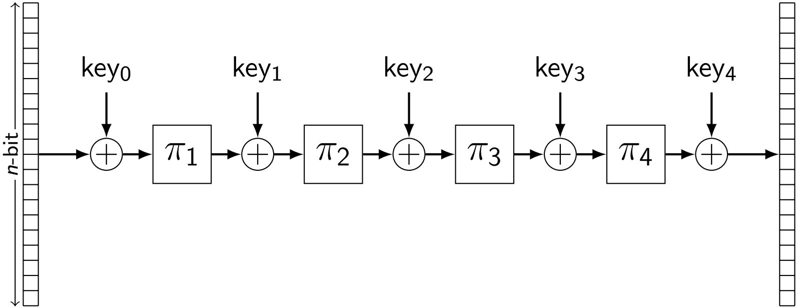
MPR Amplification Lemma [Maurer-Pietrzak-Renner 07]

$$\left.\begin{array}{l}\mathcal{F} \text{ is } \varepsilon\text{-close to 2-wise indp.} \\ \mathcal{G} \text{ is } \delta\text{-close to 2-wise indp.}\end{array}\right\} \implies \mathcal{F} \circ \mathcal{G} \text{ is } 2\varepsilon\delta\text{-close to 2-wise indp.}$$

Amplifying Our Results

$6r$-round AES is $(2^{r-1}0.472^r)$-close to 2-wise independent.

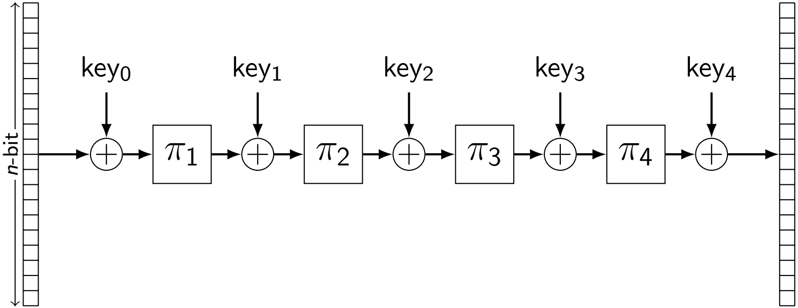
Proof Overview (KAC)



Our Results (KAC)

r-round KAC$(\pi_1, \ldots, \pi_r)$ is close to
$(r - o(r))$-wise independent
for most $\pi_1, \ldots, \pi_r$

Proof Overview (KAC)



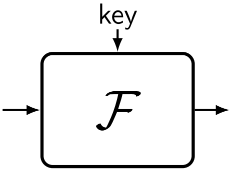
Our Results (KAC)

r-round KAC$(\pi_1, \ldots, \pi_r)$ is close to $(r - o(r))$-wise independent for most $\pi_1, \ldots, \pi_r$

Prove by induction

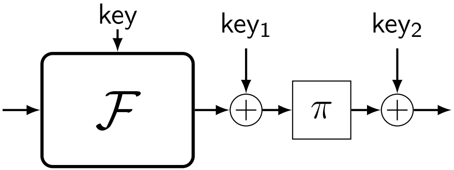
Proof Overview (KAC)

$\mathcal{F}$ is t-wise indp.



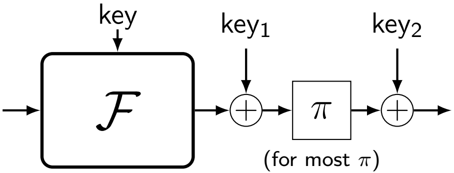
Proof Overview (KAC)

$\mathcal{F}$ is t-wise indp.



Proof Overview (KAC)

$\mathcal{F}$ is t-wise indp. $\implies$

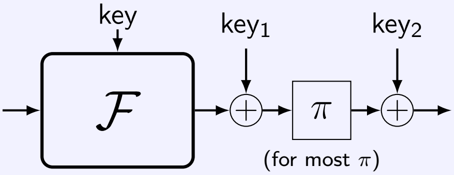


is pointwise $O(t^2 n)$-close to $(t+1)$-wise indp.

Proof Overview (KAC)

Independence Amplification Lemma

$\mathcal{F}$ is t-wise indp. $\Longrightarrow$



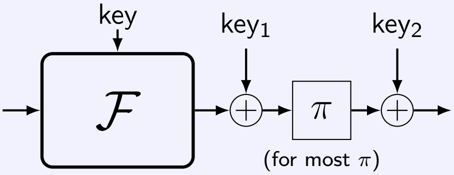
is pointwise $O(t^2 n)$-close to $(t+1)$-wise indp.

*existential result & probabilistic method on π

Proof Overview (KAC)

Independence Amplification Lemma

$\mathcal{F}$ is t-wise indp. $\Longrightarrow$



is pointwise $O(t^2 n)$-close to $(t+1)$-wise indp.

pointwise ε-close to t-wise independence

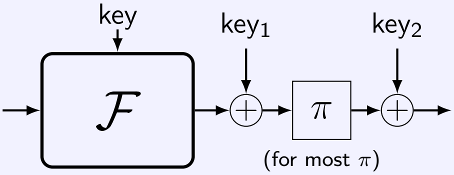
$\forall \text{input}_1, \ldots, \text{input}_t, \text{output}_1, \ldots, \text{output}_t$

$$\frac{1-\varepsilon}{2^{tn}} \leq \Pr[\text{output}_1, \ldots, \text{output}_t] \leq \frac{1+\varepsilon}{2^{tn}}$$

Proof Overview (KAC)

Independence Amplification Lemma

$\mathcal{F}$ is t-wise indp. $\implies$



is pointwise $O(t^2 n)$-close to $(t+1)$-wise indp.

pointwise ε-close to t-wise independence

$\forall \text{input}_1, \ldots, \text{input}_t, \text{output}_1, \ldots, \text{output}_t$

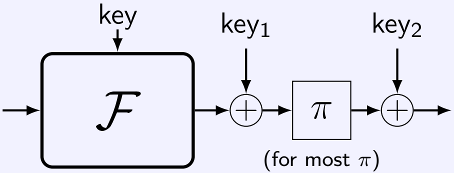
$$\frac{1-\varepsilon}{2^{tn}} \leq \Pr[\text{output}_1, \ldots, \text{output}_t] \leq \frac{1+\varepsilon}{2^{tn}}$$

*meaningful even if $\varepsilon \gg 1$

Proof Overview (KAC)

Independence Amplification Lemma

$\mathcal{F}$ is pointwise ε-close to t-wise indp. $\implies$



is pointwise $O((1+\varepsilon)t^2 n)$-close to $(t+1)$-wise indp.

pointwise ε-close to t-wise independence

$\forall \text{input}_1, \ldots, \text{input}_t, \text{output}_1, \ldots, \text{output}_t$

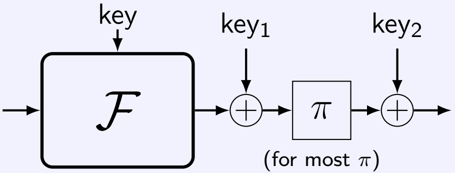
$$\frac{1-\varepsilon}{2^{tn}} \leq \Pr[\text{output}_1, \ldots, \text{output}_t] \leq \frac{1+\varepsilon}{2^{tn}}$$

*meaningful even if $\varepsilon \gg 1$

Proof Overview (KAC)

Independence Amplification Lemma

$\mathcal{F}$ is pointwise
ε-close to t-wise indp. $\Longrightarrow$



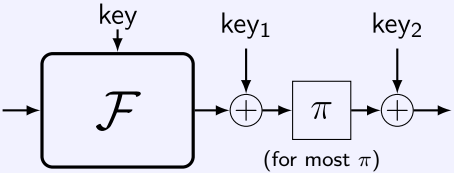
is pointwise $O((1+\varepsilon)t^2 n)$-close to $(t+1)$-wise indp.

0-round KAC (=one-time pad) is 1-wise indp.

Proof Overview (KAC)

Independence Amplification Lemma

$\mathcal{F}$ is pointwise ε-close to t-wise indp. $\Longrightarrow$



is pointwise $O((1+\varepsilon)t^2 n)$-close to $(t+1)$-wise indp.

0-round KAC (=one-time pad) is 1-wise indp.

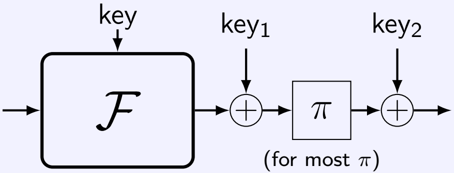
$\Downarrow$

1-round KAC is pointwise $O(n)$-close to 2-wise indp.

Proof Overview (KAC)

Independence Amplification Lemma

$\mathcal{F}$ is pointwise ε-close to t-wise indp. $\Longrightarrow$



is pointwise $O((1+\varepsilon)t^2 n)$-close to $(t+1)$-wise indp.

0-round KAC (=one-time pad) is 1-wise indp.

$\Downarrow$

1-round KAC is pointwise $O(n)$-close to 2-wise indp.

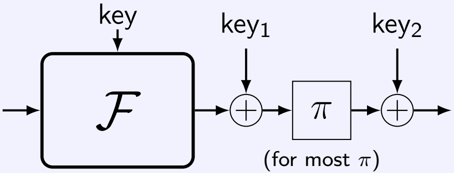
$\Downarrow$

2-round KAC is pointwise $O(n^2)$-close to 3-wise indp.

Proof Overview (KAC)

Independence Amplification Lemma

$\mathcal{F}$ is pointwise ε-close to t-wise indp. $\Longrightarrow$



is pointwise $O((1+\varepsilon)t^2 n)$-close to $(t+1)$-wise indp.

0-round KAC (=one-time pad) is 1-wise indp.

$\Downarrow$

1-round KAC is pointwise $O(n)$-close to 2-wise indp.

$\Downarrow$

2-round KAC is pointwise $O(n^2)$-close to 3-wise indp.

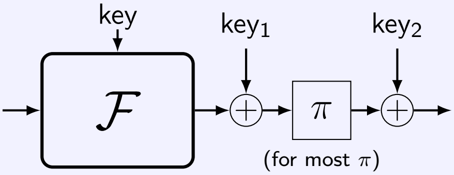
$\Downarrow$

r-round KAC is pointwise $n^r r^{O(r)}$-close to $(r+1)$-wise indp.

Proof Overview (KAC)

Independence Amplification Lemma

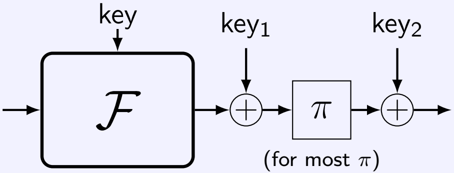
$\mathcal{F}$ is pointwise ε-close to t-wise indp. $\Longrightarrow$



is pointwise $O((1+\varepsilon)t^2 n)$-close to $(t+1)$-wise indp.

Distance Amplification Lemma

$\mathcal{F}$ is pointwise **very** close to t-wise indp. & pointwise **somewhat** close to $(t+1)$-wise indp. $\Longrightarrow$

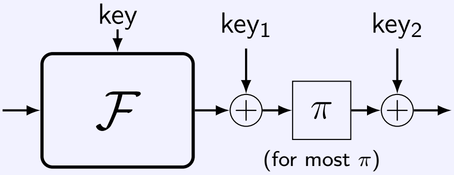


is pointwise **very** close to $(t+1)$-wise indp.

Proof Overview (KAC)

Independence Amplification Lemma

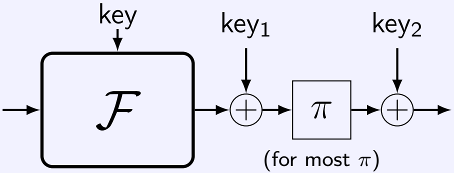
$\mathcal{F}$ is pointwise ε-close to t-wise indp. $\implies$



is pointwise $O((1+\varepsilon)t^2 n)$-close to $(t+1)$-wise indp.

Distance Amplification Lemma

$\mathcal{F}$ is pointwise ε-close to t-wise indp. & pointwise ε'-close to $(t+1)$-wise indp. $\implies$



is pointwise $(\varepsilon + \frac{O(\varepsilon' t)}{2^{n/3}})$-close to $(t+1)$-wise indp.

Proof Overview (KAC)

number of rounds	0-round	1-round	2-round	3-round	4-round
closeness to 1-wise indp.					
closeness to 2-wise indp.					
closeness to 3-wise indp.					
closeness to 4-wise indp.					
closeness to 5-wise indp.					

Proof Overview (KAC)

number of rounds	0-round	1-round	2-round	3-round	4-round
closeness to 1-wise indp.	0	0	0	0	0
closeness to 2-wise indp.					
closeness to 3-wise indp.					
closeness to 4-wise indp.					
closeness to 5-wise indp.					

Proof Overview (KAC)

number of rounds	0-round	1-round	2-round	3-round	4-round
closeness to 1-wise indp.	0	0	0	0	0
closeness to 2-wise indp.		$O(n)$			
closeness to 3-wise indp.			$O(n^2)$		
closeness to 4-wise indp.				$O(n^3)$	
closeness to 5-wise indp.					$O(n^4)$

Independence Amplification

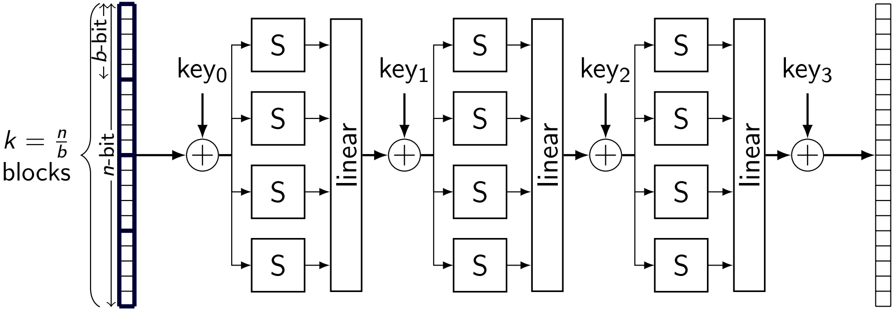
Proof Overview (KAC)

number of rounds	0-round	1-round	2-round	3-round	4-round
closeness to 1-wise indp.	0	0	0	0	0
closeness to 2-wise indp.		$O(n)$	$O(\frac{n}{2^{n/3}})$	$O(\frac{n}{2^{2n/3}})$	$O(\frac{n}{2^n})$
closeness to 3-wise indp.			$O(n^2)$	$O(\frac{n^2}{2^{n/3}})$	$O(\frac{n^2}{2^{2n/3}})$
closeness to 4-wise indp.				$O(n^3)$	$O(\frac{n^3}{2^{n/3}})$
closeness to 5-wise indp.					$O(n^4)$

Independence Amplification

Distance Amplification

Proof Overview (SPN & AES)



Our Results (SPN & AES)

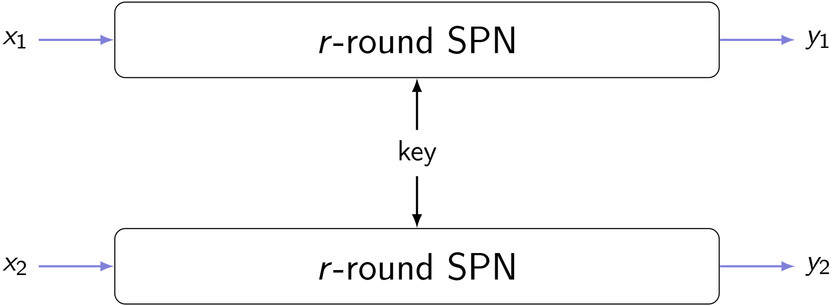
2-round SPN is $(\frac{4k}{2^b} + \sqrt{\frac{2^k}{2^b}})$-close to 2-wise independent.

3-round SPN is $(\frac{8k}{2^b} + \sqrt{\frac{k}{2^b}})$-close to 2-wise independent.

6-round AES is 0.472-close to 2-wise independent.

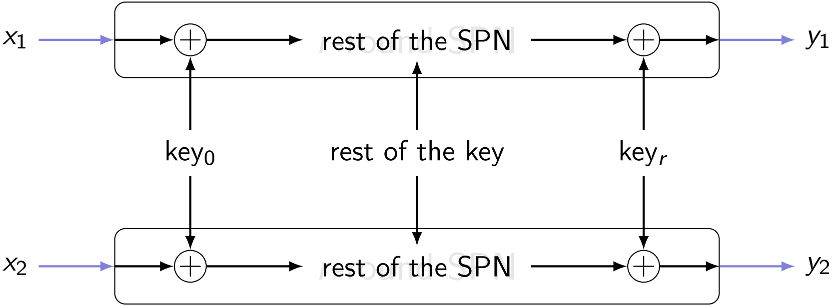
Proof Overview (SPN & AES)

Only the difference matters



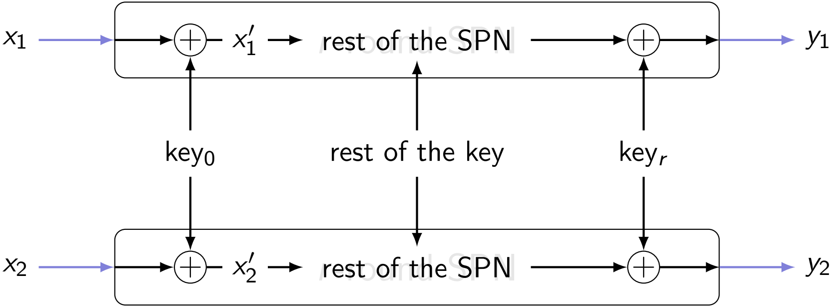
Proof Overview (SPN & AES)

Only the difference matters



Proof Overview (SPN & AES)

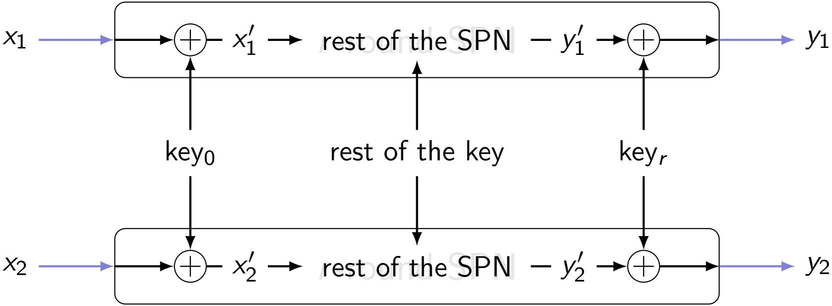
Only the difference matters



(x_1', x_2') is random conditioning on $x_1' - x_2' = x_1 - x_2$

Proof Overview (SPN & AES)

Only the difference matters

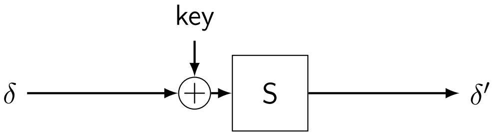


(x'_1, x'_2) is random conditioning on $x'_1 - x'_2 = x_1 - x_2$

$$\mathrm{SD}((y_1, y_2), \mathrm{uniform}) = \mathrm{SD}(y'_1 - y'_2, \mathrm{uniform})$$

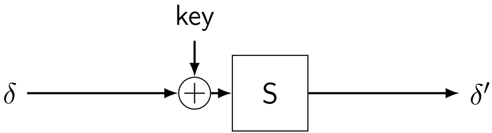
Proof Overview (SPN & AES)

S-box: input difference $\delta \quad \mapsto \quad$ output difference δ'



Proof Overview (SPN & AES)

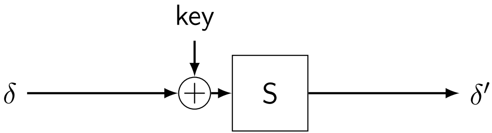
S-box: input difference $\delta \quad \mapsto \quad$ output difference δ'



given inputs x_1, x_2 s.t. $x_1 \oplus x_2 = \delta$,
what is the distribution of $\delta' = S(x_1 \oplus \text{key}) \oplus S(x_2 \oplus \text{key})$?

Proof Overview (SPN & AES)

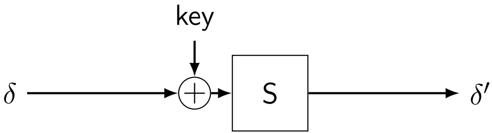
S-box: input difference $\delta \quad \mapsto \quad$ output difference δ'



$$S(x) = x^{-1} \quad or \quad S(x) = x^3 \quad \text{over } \mathbb{F}_{2^b}$$

Proof Overview (SPN & AES)

S-box: input difference $\delta \quad \mapsto \quad$ output difference δ'



$$S(x) = x^{-1} \quad or \quad S(x) = x^3 \quad \text{over } \mathbb{F}_{2^b}$$

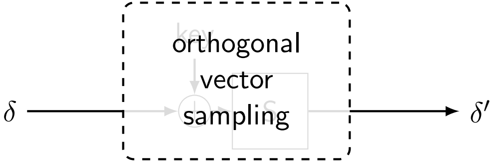
Subspace Sampling Lemma

View δ, δ' as dimension-n vectors in $\mathbb{F}_2^b$

δ' is a random vector orthogonal to δ!

Proof Overview (SPN & AES)

S-box: input difference $\delta \quad \mapsto \quad$ output difference δ'



$$S(x) = x^{-1} \quad \textit{or} \quad S(x) = x^3 \quad \text{over } \mathbb{F}_{2^b}$$

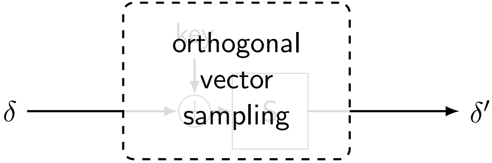
Subspace Sampling Lemma

View δ, δ' as dimension-n vectors in $\mathbb{F}_2^b$

δ' is a random vector orthogonal to δ!

Proof Overview (SPN & AES)

S-box: input difference $\delta \quad \mapsto \quad$ output difference δ'



$$S(x) = x^{-1} \quad \textit{or} \quad S(x) = x^3 \quad \text{over } \mathbb{F}_{2^b}$$

Subspace Sampling Lemma

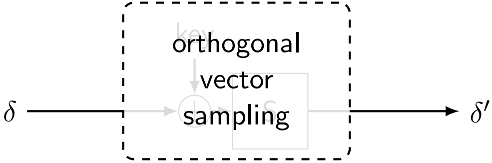
View δ, δ' as dimension-n vectors in $\mathbb{F}_2^b$

δ' is a random vector orthogonal to δ!

Not really true. Actually ...

Proof Overview (SPN & AES)

S-box: input difference $\delta \quad \mapsto \quad$ output difference δ'



$$S(x) = x^{-1} \quad \textit{or} \quad S(x) = x^3 \quad \text{over } \mathbb{F}_{2^b}$$

Subspace Sampling Lemma

View δ, δ' as dimension-n vectors in $\mathbb{F}_2^b$

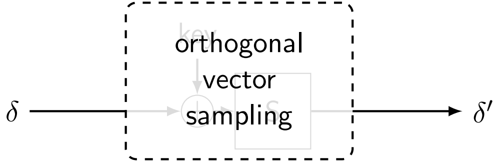
δ' is a random vector orthogonal to δ!

Not really true. Actually . . .

- $\delta = 0 \implies \delta' = 0$

Proof Overview (SPN & AES)

S-box: input difference $\delta \quad \mapsto \quad$ output difference δ'



$$S(x) = x^{-1} \quad \textit{or} \quad S(x) = x^3 \quad \text{over } \mathbb{F}_{2^b}$$

Subspace Sampling Lemma

View δ, δ' as dimension-n vectors in $\mathbb{F}_2^b$

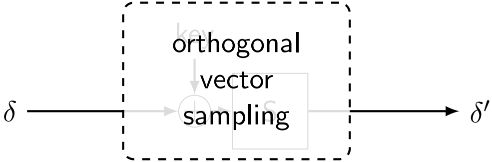
δ' is a random vector orthogonal to δ!

Not really true. Actually . . .

- $\delta = 0 \implies \delta' = 0$
- $\exists \pi, \pi'$ s.t. $\pi(\delta')$ is a random vector orthogonal to $\pi'(\delta)$

Proof Overview (SPN & AES)

S-box: input difference δ $\mapsto$ output difference δ'



$$S(x) = x^{-1} \quad \textit{or} \quad S(x) = x^3 \quad \text{over } \mathbb{F}_{2^b}$$

Subspace Sampling Lemma

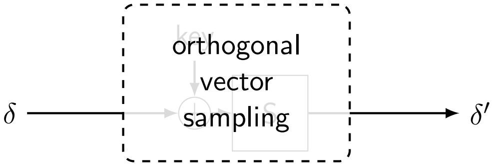
View δ, δ' as dimension-n vectors in $\mathbb{F}_2^b$

δ' is a random vector orthogonal to δ!

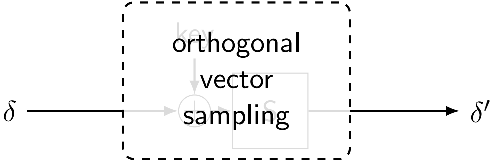
Not really true. Actually ...

- $\delta = 0 \implies \delta' = 0$
- $\exists \pi, \pi'$ s.t. $\pi(\delta')$ is a random vector orthogonal to $\pi'(\delta)$

Proof Overview (SPN & AES)

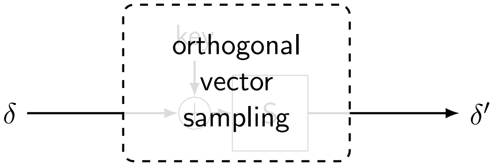


Proof Overview (SPN & AES)



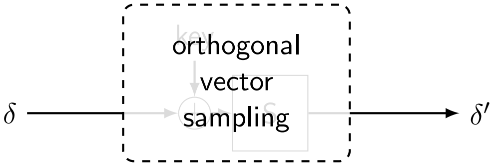
fixed $\delta \neq 0$ $\implies$ $H_\infty(\delta') = b - 1$

Proof Overview (SPN & AES)



$$H_\infty(\delta) \geq b - 1 \qquad \Longrightarrow \qquad ???$$

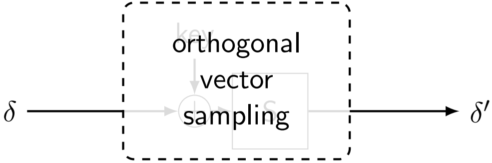
Proof Overview (SPN & AES)



Extraction Lemma

$H_\infty(\delta) \geq b - 1 \quad \Longrightarrow \quad \delta'$ close to uniform

Proof Overview (SPN & AES)

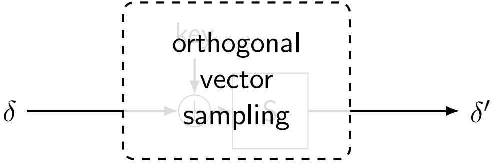


Extraction Lemma

$$\mathsf{H}_\infty(\delta) \geq b - 1 \quad \Longrightarrow \quad \delta' \text{ close to uniform}$$

Proved by Fourier analysis

Proof Overview (SPN & AES)



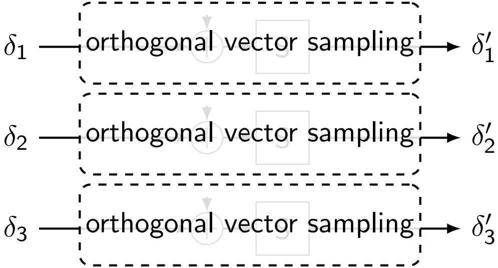
Extraction Lemma

$\mathsf{H}_\infty(\delta) \geq b - 1 \quad \Longrightarrow \quad \delta'$ close to uniform

Proved by Fourier analysis

(full version) Proved by collision probability

Proof Overview (SPN & AES)



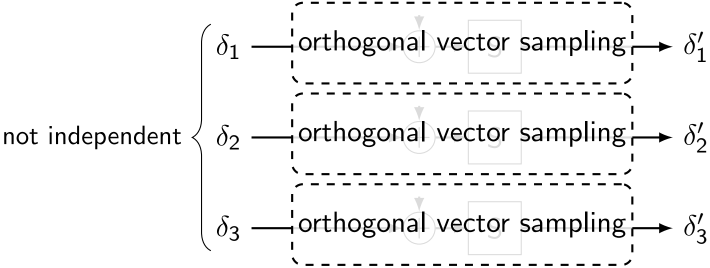
Extraction Lemma

$\forall i\ \mathrm{H}_\infty(\delta_i) \geq b - 1 \quad \Longrightarrow \quad (\delta'_1, \ldots, \delta'_k)$ close to uniform

Proved by Fourier analysis

(full version) Proved by collision probability

Proof Overview (SPN & AES)



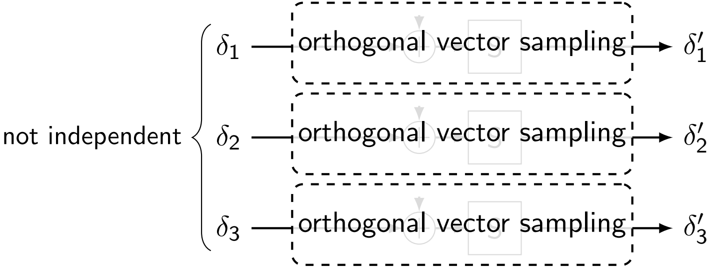
Extraction Lemma

$\forall i \; \mathrm{H}_\infty(\delta_i) \geq b - 1 \quad \Longrightarrow \quad (\delta'_1, \ldots, \delta'_k)$ close to uniform

Proved by Fourier analysis

(full version) Proved by collision probability

Proof Overview (SPN & AES)



Extraction Lemma

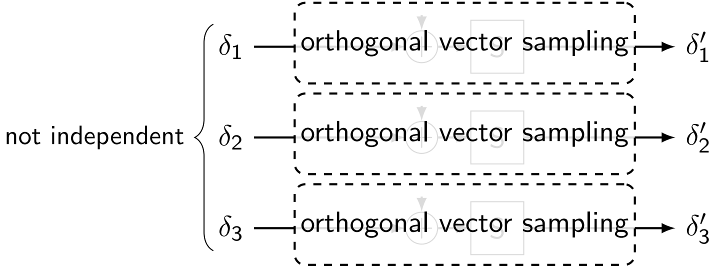
$\forall i\ \mathrm{H}_\infty(\delta_i) \geq b - 1 \implies (\delta'_1, \ldots, \delta'_k)$ close to uniform

$\mathrm{H}_\infty(\{\delta_i\}_{i \in S}) \geq (b-1) \cdot |S|$ for any subset $S \subseteq [k]$ $\implies (\delta'_1, \ldots, \delta'_k)$ very close to uniform

Proved by Fourier analysis

(full version) Proved by collision probability

Proof Overview (SPN & AES)



Extraction Lemma

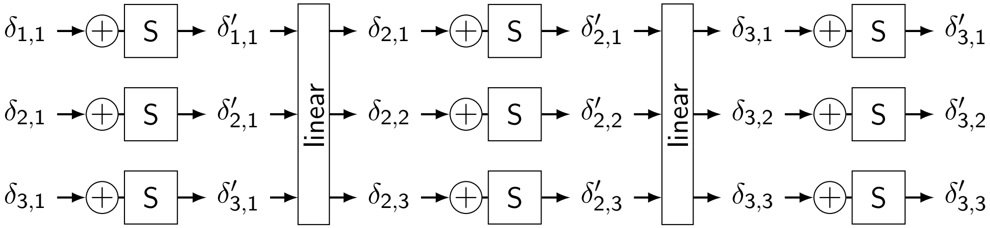
$$\forall i \; H_\infty(\delta_i) \geq b - 1 \implies \mathrm{SD}((\delta'_1, \ldots, \delta'_k), \text{uniform}) \leq \sqrt{\frac{2^k - 1}{2^b}}$$

$$H_\infty(\{\delta_i\}_{i \in S}) \geq (b-1) \cdot |S| \text{ for any subset } S \subseteq [k] \implies \mathrm{SD}((\delta'_1, \ldots, \delta'_k), \text{uniform}) \leq \sqrt{\frac{k}{2^b}}$$

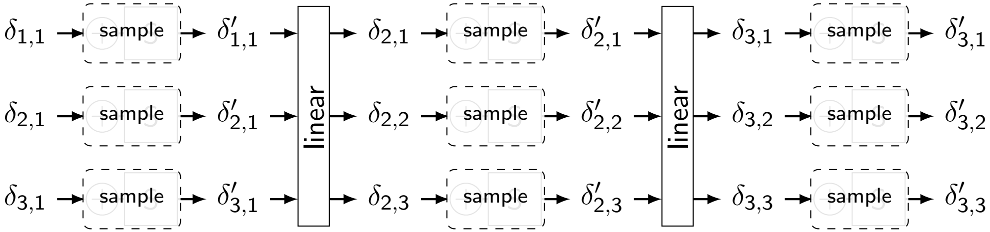
Proved by Fourier analysis

(full version) Proved by collision probability

Proof Overview (SPN & AES)



Proof Overview (SPN & AES)



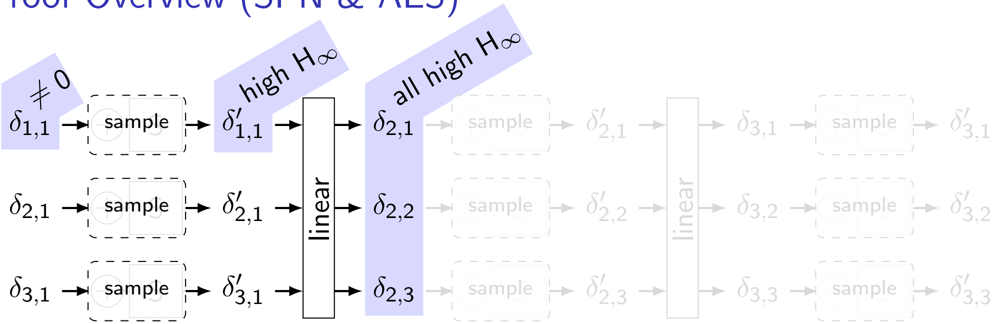
Proof Overview (SPN & AES)

$\xrightarrow{\text{w.l.o.g.}}$ $\delta_{1,1} \neq 0$

Proof Overview (SPN & AES)

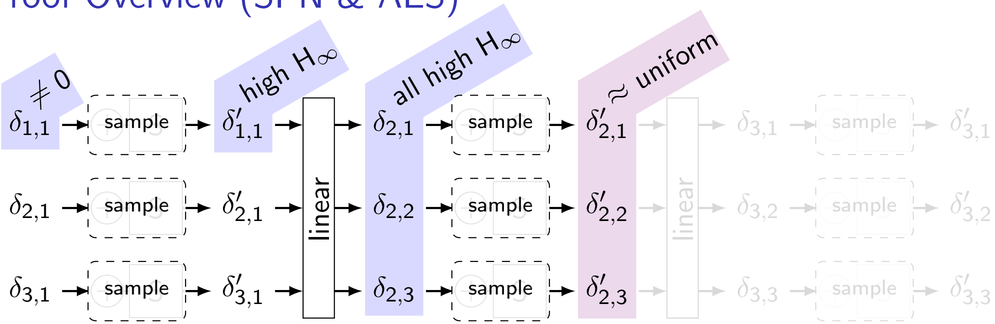
$\overset{\text{w.l.o.g.}}{\Longrightarrow}$ $\delta_{1,1} \neq 0 \Longrightarrow H_\infty(\delta'_{1,1}) = b - 1$

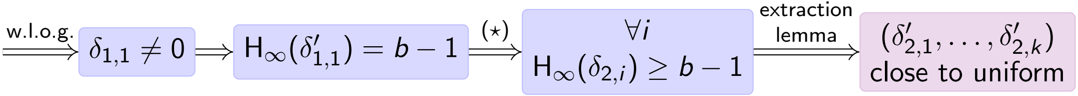
Proof Overview (SPN & AES)



$\xRightarrow{\text{w.l.o.g.}}$ $\delta_{1,1} \neq 0$ $\Longrightarrow$ $H_\infty(\delta'_{1,1}) = b - 1$ $\xRightarrow{(\star)}$ $\forall i$ $H_\infty(\delta_{2,i}) \geq b - 1$

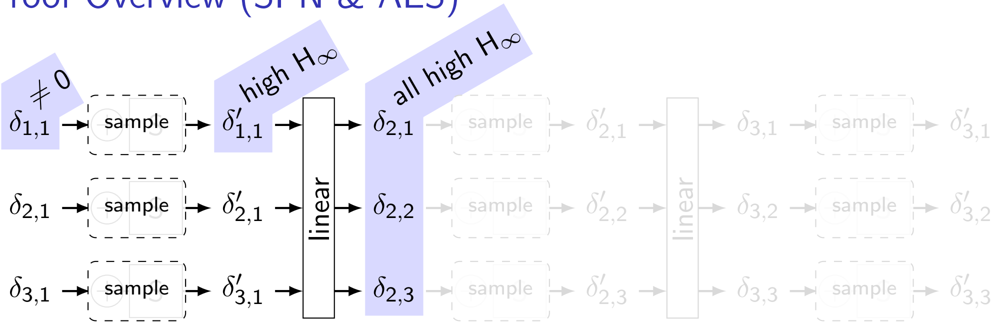
Proof Overview (SPN & AES)





$$SD = \sqrt{\frac{2^k}{2^b}} + O\left(\frac{k}{2^b}\right)$$

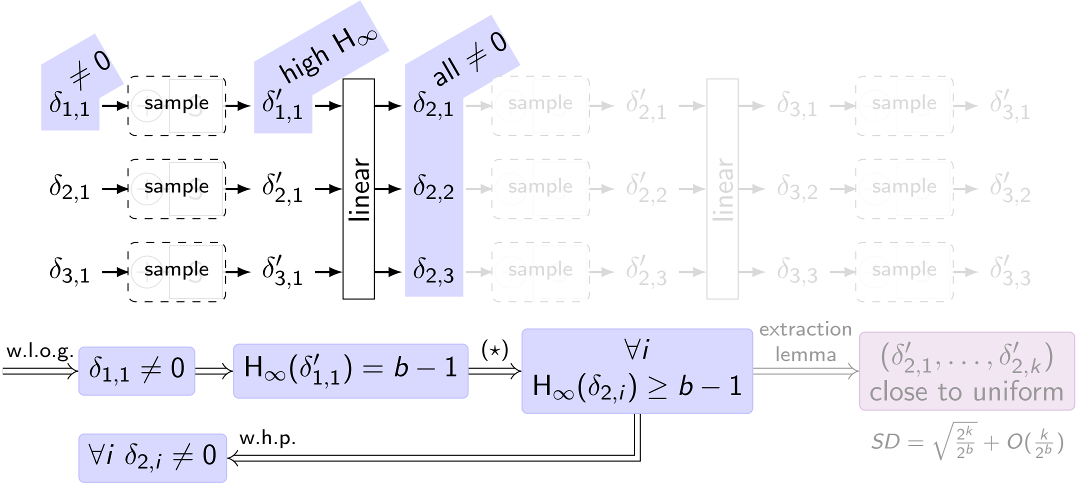
Proof Overview (SPN & AES)



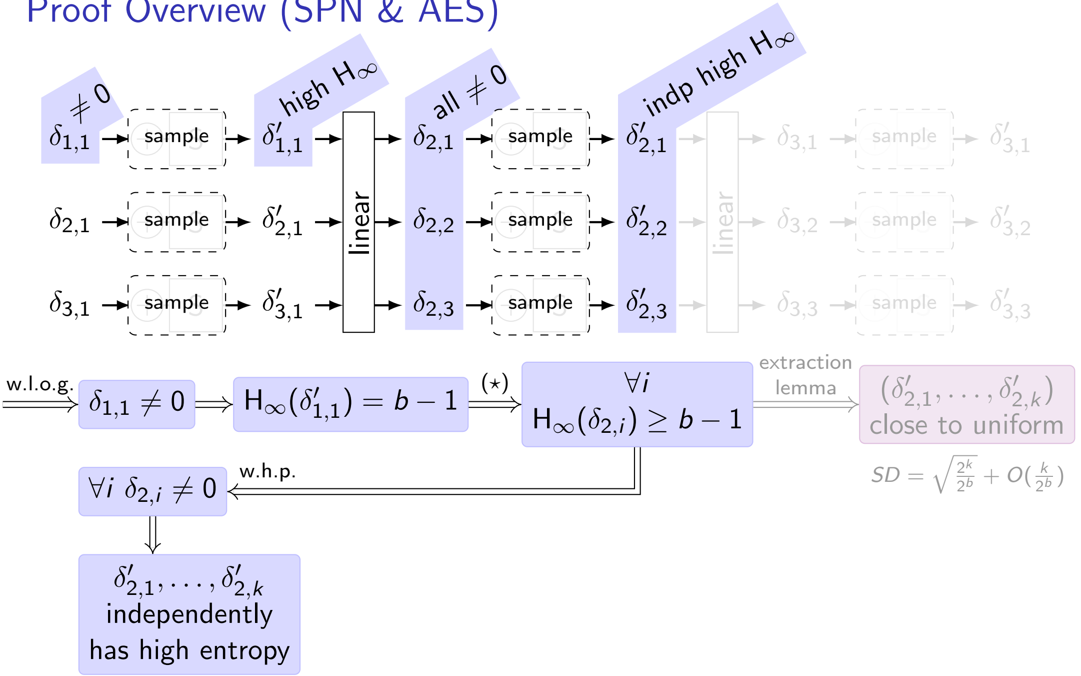
w.l.o.g. $\Longrightarrow$ $\delta_{1,1} \neq 0$ $\Longrightarrow$ $H_\infty(\delta'_{1,1}) = b-1$ $\overset{(\star)}{\Longrightarrow}$ $\forall i$ $H_\infty(\delta_{2,i}) \geq b-1$ $\overset{\text{extraction lemma}}{\Longrightarrow}$ $(\delta'_{2,1}, \ldots, \delta'_{2,k})$ close to uniform

$SD = \sqrt{\frac{2^k}{2^b}} + O(\frac{k}{2^b})$

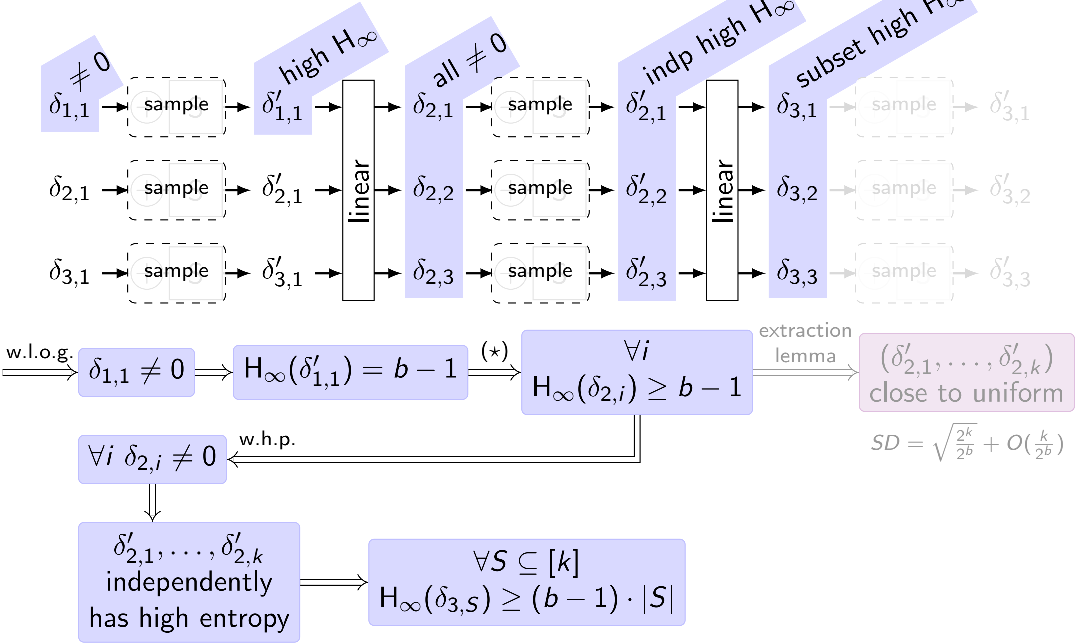
Proof Overview (SPN & AES)



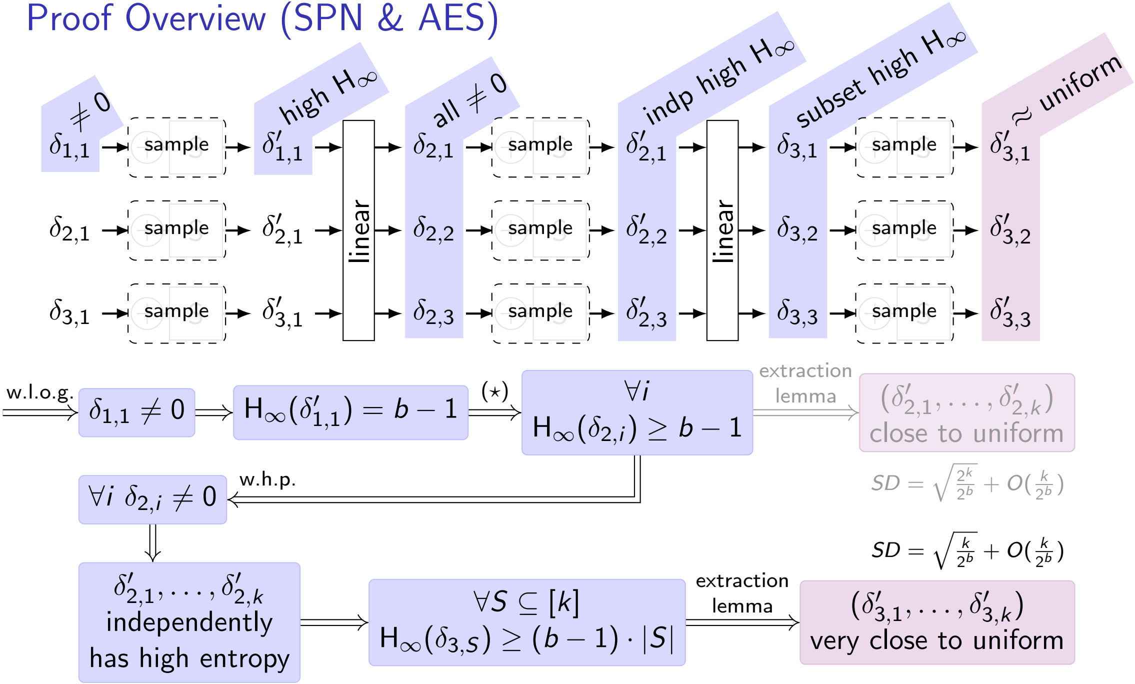
Proof Overview (SPN & AES)



Proof Overview (SPN & AES)



Proof Overview (SPN & AES)



Our Results (SPN & AES)

2-round SPN is $(\frac{4k}{2^b} + \sqrt{\frac{2^k}{2^b}})$-close to 2-wise independent.

3-round SPN is $(\frac{8k}{2^b} + \sqrt{\frac{k}{2^b}})$-close to 2-wise independent.

Our Results (SPN & AES)

2-round SPN is $(\frac{4k}{2^b} + \sqrt{\frac{2^k}{2^b}})$-close to 2-wise independent.

3-round SPN is $(\frac{8k}{2^b} + \sqrt{\frac{k}{2^b}})$-close to 2-wise independent.

6-round AES is 0.472-close to 2-wise independent.

Our Results (KAC)

r-round KAC$(\pi_1, \ldots, \pi_r)$ is close to $(r - o(r))$-wise indp for most $\pi_1, \ldots, \pi_r$

Our Results (SPN & AES)

2-round SPN is $(\frac{4k}{2^b} + \sqrt{\frac{2^k}{2^b}})$-close to 2-wise independent.

3-round SPN is $(\frac{8k}{2^b} + \sqrt{\frac{k}{2^b}})$-close to 2-wise independent.

6-round AES is 0.472-close to 2-wise independent.

t-**wise independence** has a really rich body of problems . . .

- Amplify independence like what we did in KAC
  - 3-wise independence of a concrete cipher
- The role of key scheduling
- Analysis of other concrete cipher design
  - e.g. add–rotate–xor (ARX) cipher
- The relationship between t-wise independent and other class(es) of attack