Design Strategies for ARX with Provable Bounds: SPARX and LAX

Daniel Dinu[1], Léo Perrin[1], Aleksei Udovenko[1],
Vesselin Velichkov[1], Johann Großschädl[1], Alex Biryukov[1]

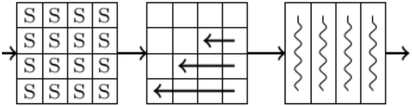
[1]SnT, University of Luxembourg

https://www.cryptolux.org

December 7, 2016
ASIACRYPT

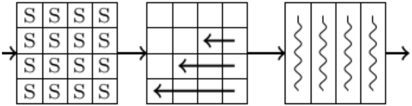
UNIVERSITÉ DU LUXEMBOURG

securityandtrust.lu



$$P_{\text{diff}} \leq \left(\frac{\Delta_S}{2^b}\right)^{\#\text{ active S-Boxes}}$$

Design of an S-Box based SPN
(wide-trail strategy)

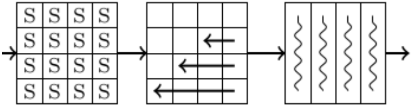


$$P_{\text{diff}} \leq \left(\frac{\Delta_S}{2^b}\right)^{\#\ \text{active S-Boxes}}$$

Design of an S-Box based SPN (wide-trail strategy)

Design of an ARX-cipher (allegory)

source: Wiki Commons



$$P_{\text{diff}} \leq \left(\frac{\Delta_S}{2^b}\right)^{\#\text{ active S-Boxes}}$$

Design of an S-Box based SPN (wide-trail strategy)

Design of an ARX-cipher (allegory)

source: Wiki Commons

Can we use ARX *and* have provable bounds?

Outline

Plan

The Wide Trail Strategy (WTS)

Wide Trail Argument

$$\mathrm{MEDCP}(F^r) \leq {p_S}^{\mathbf{a}(r)}$$

- $\mathrm{MEDCP}(F^r) = \max\left(P[\text{any trail covering } r \text{ rounds of } F]\right)$
- $P[S(x \oplus \mathbf{c}) \oplus S(x) = \mathbf{d}] \;\leq\; p_S$
- $\#\{\text{active S-Boxes on } r \text{ rounds}\} \geq \mathbf{a}(r)$

The Wide Trail Strategy (WTS)

Wide Trail Argument

$$\text{MEDCP}(F^r) \leq {p_S}^{\mathbf{a}(r)}$$

- $\text{MEDCP}(F^r) = \max\left(P[\text{any trail covering } r \text{ rounds of } F]\right)$
- $P[S(x \oplus \mathbf{c}) \oplus S(x) = \mathbf{d}] \leq p_S$
- $\#\{\text{active S-Boxes on } r \text{ rounds}\} \geq \mathbf{a}(r)$

Used to design the AES!

The Wide Trail Strategy (WTS)

Wide Trail Argument

$$\text{MEDCP}(F^r) \leq {p_S}^{\mathbf{a}(r)}$$

- $\text{MEDCP}(F^r) = \max\left(P[\text{any trail covering } r \text{ rounds of } F]\right)$
- $P[S(x \oplus \mathbf{c}) \oplus S(x) = \mathbf{d}] \leq p_S$
- $\#\{\text{active S-Boxes on } r \text{ rounds}\} \geq \mathbf{a}(r)$

Used to design the AES!

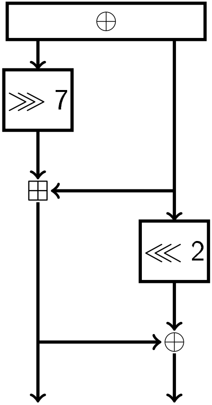
Application to ARX

Can we use this to build an ARX-based cipher?

ARX-Boxes (1/2)

SPECKEY

1. Start from SPECK-32
2. XOR key in full state (Markov assumption)
3. Find best trails



SPECKEY.

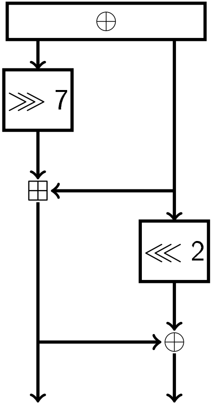
ARX-Boxes (1/2)

SPECKEY

1. Start from SPECK-32
2. XOR key in full state (Markov assumption)
3. Find best trails

Parameter Search

- Rotations 7, −2
- Second best crypto properties, lightest
- Indeed NSA design strategy (see DAC'15).



SPECKEY.

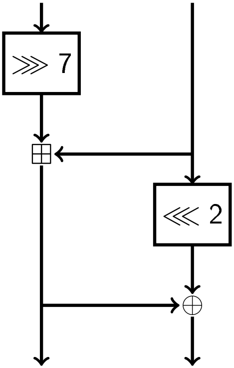
ARX-Boxes (2/2)

Differential/Linear bounds

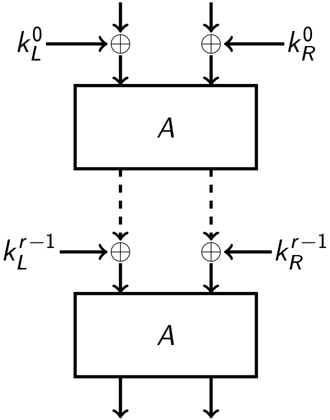
r	1	2	3	4	5	6	7	8	9	10
MEDCP(A^r)	−0	−1	−3	−5	−9	−13	−18	−24	−30	−34
MELCC(A^r)	−0	−0	−1	−3	−5	−7	−9	−12	−14	−17

Maximum expected differential characteristic probabilities (MEDCP) and maximum expected absolute linear characteristic correlations (MELCC) of SPECKEY ($\log_2$ scale); r is the number of rounds.

Notations



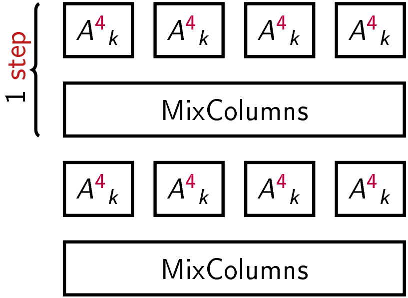
A.



A_k^r.

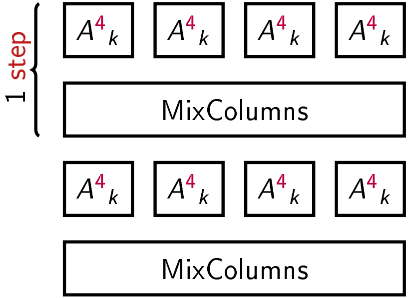
Naive Approach

S-Box: A^4 ; Linear layer: 128-bit MixColumns.



Naive Approach

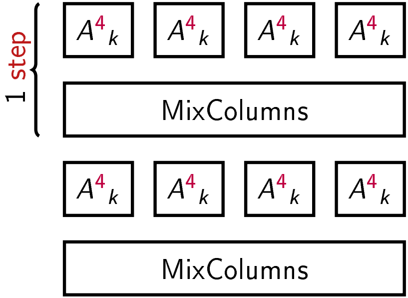
S-Box: A^4 ; Linear layer: 128-bit MixColumns.



- Active ARX-Boxes: $\mathbf{a}(2s) \geq 5s$,
- $\log_2 \left(\text{MEDCP}(A^4)\right) = -5$

Naive Approach

S-Box: A^4 ; Linear layer: 128-bit MixColumns.

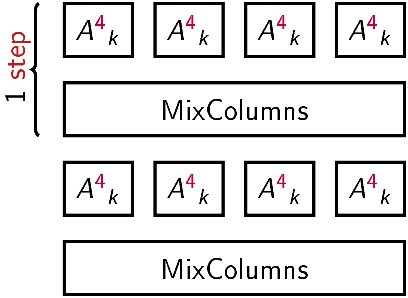


- Active ARX-Boxes: $\mathbf{a}(2s) \geq 5s$,
- $\log_2\left(\text{MEDCP}(A^4)\right) = -5$

$$\log_2(P[\text{diff. trail on } 2s \text{ steps}]) \leq 5s \times \text{MEDCP}(A^4)$$
$$\log_2(P[\text{diff. trail on } 2s \text{ steps}]) \leq -25s$$

Naive Approach

S-Box: A^4 ; Linear layer: 128-bit MixColumns.



- Active ARX-Boxes: $\mathbf{a}(2s) \geq 5s$,
- $\log_2\left(\text{MEDCP}(A^4)\right) = -5$

$$\log_2(P[\text{diff. trail on } 2s \text{ steps}]) \leq 5s \times \text{MEDCP}(A^4)$$
$$\log_2(P[\text{diff. trail on } 2s \text{ steps}]) \leq -25s$$

Need $2\lceil 128/25 \rceil = 12$ steps, i.e. **48 ARX rounds!**

Drawbacks

The Wide Trail Strategy fails here

Two (bad) options:

1. design a very weak cipher, or
2. design a very slow cipher.

Drawbacks

The Wide Trail Strategy fails here

Two (bad) options:

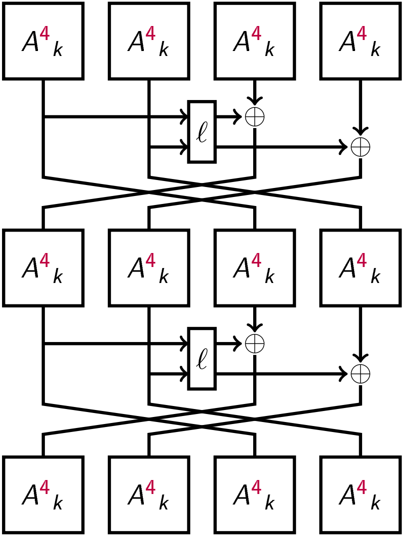
1. design a very weak cipher, or
2. design a very slow cipher.

A New Hope

- $\log_2\left(\text{MEDCP}(A^4)\right) = -5$
- $\log_2\left(\text{MEDCP}(A^8)\right) = -24 \ll -5 \times 2$

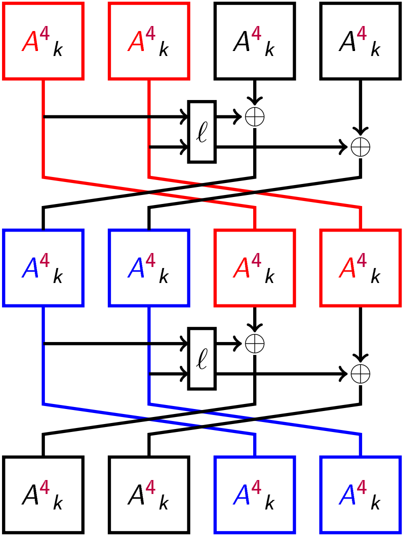
Better Approach

- New linear layer "chaining" ARX-Boxes.



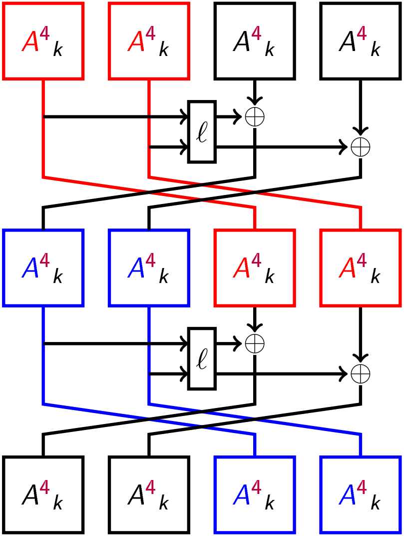
Better Approach

- New linear layer "chaining" ARX-Boxes.



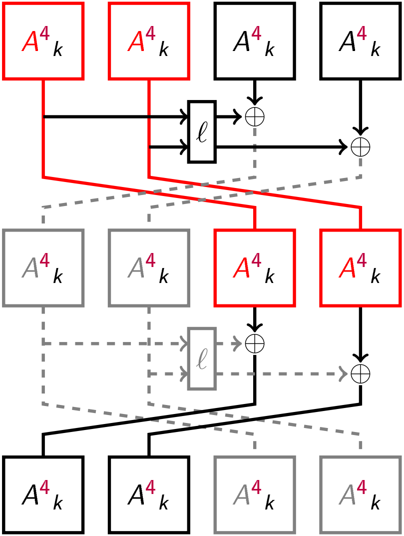
Better Approach

- New linear layer "chaining" ARX-Boxes.
- We can use MEDCP(A^8) instead of $(\text{MEDCP}(A^4))^2$.



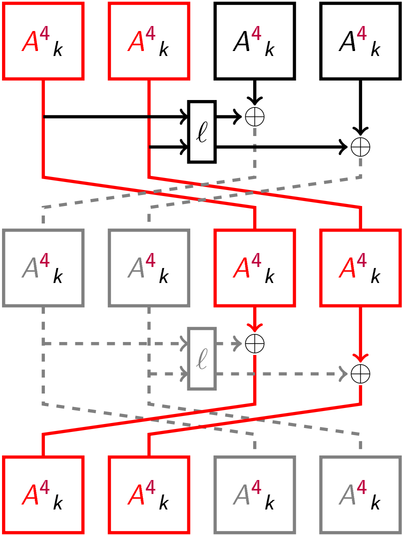
Better Approach

- New linear layer "chaining" ARX-Boxes.
- We can use MEDCP(A^8) instead of $(\text{MEDCP}(A^4))^2$.
- If left half has zero differences,



Better Approach

- New linear layer "chaining" ARX-Boxes.
- We can use MEDCP(A^8) instead of $(\text{MEDCP}(A^4))^2$.
- If left half has zero differences, we can use MEDCP(A^{12}) instead of $(\text{MEDCP}(A^4))^3$.



The Long Trail Argument (1/2)

Definition (Long Trail)

A Long Trail (LT) is a trail covering several ARX-Boxes without receiving any outside difference. Can be *static* (probability = 1) or *dynamic* (depends on the trail).

The Long Trail Argument (1/2)

Definition (Long Trail)

A Long Trail (LT) is a trail covering several ARX-Boxes without receiving any outside difference. Can be *static* (probability $= 1$) or *dynamic* (depends on the trail).

Definition (Truncated Trail)

A sequence of values in $\{0, 1\}^4$: 1 if ARX-Box i is active, else 0.

The Long Trail Argument (2/2)

Bounding Differential Probability

For all truncated trails covering r rounds:

1. check if it is coherent with the linear layer,
2. decompose it into long trails (static and dynamic),
3. bound the probability of all trails following the truncated trail.

The Long Trail Argument (2/2)

Bounding Differential Probability

For all truncated trails covering r rounds:

1. check if it is coherent with the linear layer,
2. decompose it into long trails (static and dynamic),
3. bound the probability of all trails following the truncated trail.

$\Longrightarrow$ Deduce a bound on the probability of all trails.

The Long Trail Argument (2/2)

Bounding Differential Probability

For all truncated trails covering r rounds:

1. check if it is coherent with the linear layer,
2. decompose it into long trails (static and dynamic),
3. bound the probability of all trails following the truncated trail.

$\implies$ Deduce a bound on the probability of all trails.

Example of a LT bound

After 5 steps, the best trail for four 4-round ARX-Boxes + Feistel linear layer is $< 2^{-128}$.

$5 \ll 12$ steps

The Long Trail Strategy (LTS)

Definition (Design Principle)

When using large, weak S-Boxes, it is better to foster Long Trails than diffusion. Thus, the linear layer must be small.

The Long Trail Strategy (LTS)

Definition (Design Principle)

When using large, weak S-Boxes, it is better to foster Long Trails than diffusion. Thus, the linear layer must be small.

Wide Trail Strategy

Long Trail Strategy

The Long Trail Strategy (LTS)

Definition (Design Principle)

When using large, weak S-Boxes, it is better to foster Long Trails than diffusion. Thus, the linear layer must be small.

Wide Trail Strategy

S-Box	Small, cheap.
Lin. Layer	Expensive, complex.

Long Trail Strategy

S-Box	Large, expensive.
Lin. Layer	Cheap, simple.

Plan

1 The Long-Trail Strategy

2 The SPARX Family of LW-BC
- High Level View
- Security Analysis
- Implementation
  - Methodology
  - Results

3 The LAX Approach

4 Conclusion

High Level View

SPARX family of block ciphers

- Designed using a long trail strategy.
- SPARX-n/k: n-bit block, k-bit key ($k \geq 128$).
- Only need 16-bit operations: $\lll i$, $\oplus$, $\boxplus$.

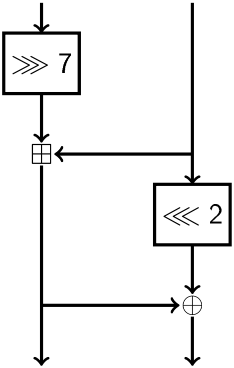
High Level View

SPARX family of block ciphers

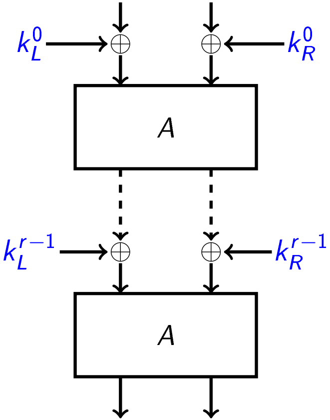
- Designed using a long trail strategy.
- SPARX-n/k: n-bit block, k-bit key ($k \geq 128$).
- Only need 16-bit operations: $\lll i$, $\oplus$, $\boxplus$.

n/k	64/128	128/128	128/256
# Rounds/Step	3	4	4
# Steps	8	8	10
Best Attack (# rounds)	15/24	22/32	24/40

Notations (reminder)

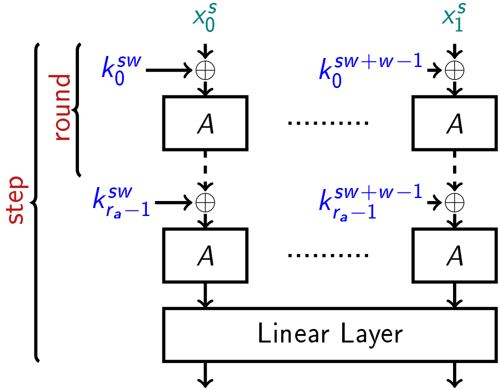


A.

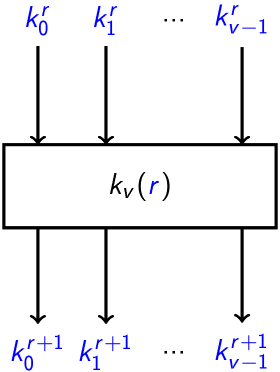


A_k^r.

High level view

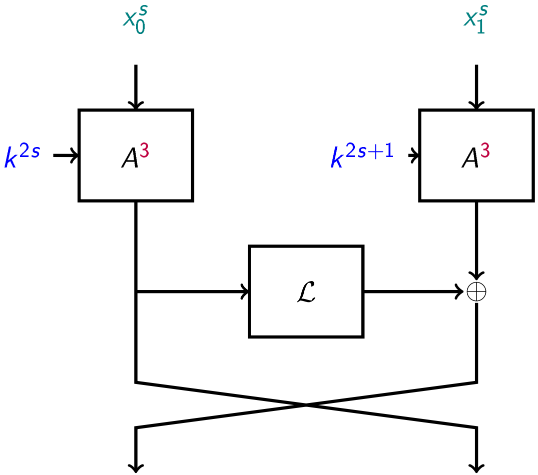


Round function of SPARX.

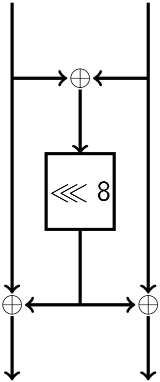


Key schedule.

SPARX-64/128

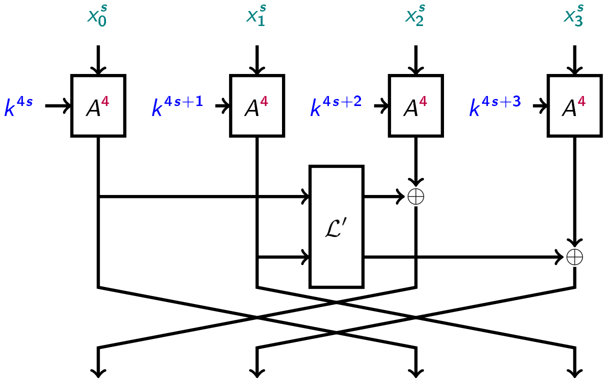


Step Function.

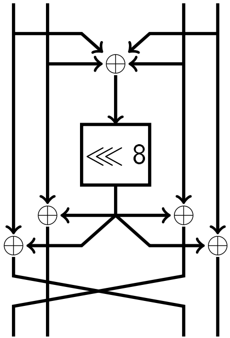


$\mathcal{L}$.

SPARX-128/128 and SPARX-128/256



Step Function.



$\mathcal{L}'$.

Security

Long Trail Argument

$$P[\text{any diff. trail covering at least 5 steps}] < 2^{-n}$$

Security

Long Trail Argument

$$P[\text{any diff. trail covering at least 5 steps}] < 2^{-n}$$

Integral Attacks

- Todo's division property: 4-5 steps for n =64-128,
- properties of modular addition: +1 round,
- best distinguishers cover 13-21 rounds for n =64-128.

Security

Long Trail Argument

$$P[\text{any diff. trail covering at least 5 steps}] < 2^{-n}$$

Integral Attacks

- Todo's division property: 4-5 steps for n =64-128,
- properties of modular addition: +1 round,
- best distinguishers cover 13-21 rounds for n =64-128.

n/k	64/128	128/128	128/256
rounds attacked/total	15/24	22/32	24/40
security margin	38 %	31 %	40 %

Benchmarking

https://www.cryptolux.org/index.php/FELICS

- **F**air **E**valuation of **L**ightweight **C**ryptographic **S**ystems
- 8-bit ATMEL AVR ; 16-bit TI MSP ; 32-bit ARM Cortex-M3
- Usage scenarios (e.g. CBC encryption of 128 bytes)
- Extracts RAM usage, ROM usage, # CPU cycles.

Benchmarking

https://www.cryptolux.org/index.php/FELICS

- **F**air **E**valuation of **L**ightweight **C**ryptographic **S**ystems
- 8-bit ATMEL AVR ; 16-bit TI MSP ; 32-bit ARM Cortex-M3
- Usage scenarios (e.g. CBC encryption of 128 bytes)
- Extracts RAM usage, ROM usage, # CPU cycles.
- Figure Of Merit aggregates: all metrics accross all platforms for the best implementations of one algorithm.

Efficiency of the SPARX Ciphers

Rank	Cipher	Block size	Key size	Scenario 1 FOM	Security margin
1	Speck	64	128	5.0	27 %
2	Chaskey-LTS	128	128	5.0	42 %
3	Simon	64	128	6.9	32 %
4	RECTANGLE	64	128	7.8	28 %
5	LEA	128	128	8.0	33 %
6	**Sparx**	**64**	**128**	**8.6**	**38 %**
7	**Sparx**	**128**	**128**	**12.9**	**31 %**
8	HIGHT	64	128	14.1	19 %
9	AES	128	128	15.3	30 %
10	Fantomas	128	128	17.2	?? %

Efficiency of the SPARX Ciphers

Rank	Cipher	Block size	Key size	Scenario 1 FOM	Security margin
–	Speck	64	128	5.0	27 %
–	Chaskey-LTS	128	128	5.0	42 %
–	Simon	64	128	6.9	32 %
1	RECTANGLE	64	128	7.8	28 %
–	LEA	128	128	8.0	33 %
2	**Sparx**	**64**	**128**	**8.6**	**38 %**
3	**Sparx**	**128**	**128**	**12.9**	**31 %**
–	HIGHT	64	128	14.1	19 %
4	AES	128	128	15.3	30 %
5	Fantomas	128	128	17.2	?? %

Gray: designers did not provide differential/linear bounds.

Plan

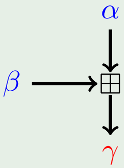
An Alternative Strategy for Provable ARX

The Wallén Challenge

[...] design a simple and efficient cipher that uses only addition modulo 2^n and F_2-affine functions, and that is provably resistant against basic DC and LC.

–Johan Wallén [Master Thesis, 2003]

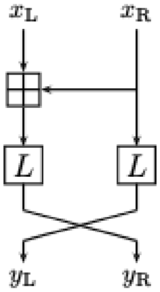
Rationale



- DP and LC drop exponentially with $\mathrm{hw}(\alpha \oplus \beta)$
- Affine part should maximize $\mathrm{hw}(\alpha \oplus \beta)$!

DP = differential probability; LC = linear correlation

The LAX Construction



$(y_L, y_R) =$
$(Lx_R,\ L(x_L \boxplus x_R))$

LAX-2n

- $2n$-bit block, $n \in \{8, 16\}$
- L is $n \times n$ binary matrix that
  1. is invertible,
  2. has branch number $d > 2$,
- $[I\ L]$ is a $[2n, n, d]$ lin. code:
  - LAX-16: [16, 8, 5]
  - LAX-32: [32, 16, 8]

Linear transform, Addition, XOR $\implies$ **LAX**

Differential Bound on 3 Rounds

Theorem

The maximum DP of any trail on 3 rounds of LAX-2n *is* $2^{-(d-2)}$, *where* d *is the branch number of* L.

$2n$	# Rounds	1	2	3	4	5	6	7	8	9	10	11	12
16	p_{best}	+0	−2	−4	−7	−8	−11	−13	−16	−18	−20	−23	−25
	p_{bound}			−3			−6			−9			−12
32	p_{best}	+0	−2	−6	−9	−11	−16	−18	−20	−24	−28	−29	−34
	p_{bound}			−6			−12			−18			−24

Differential Bound on 3 Rounds

Theorem

The maximum DP of any trail on 3 rounds of LAX-2n *is* $2^{-(d-2)}$*, where* d *is the branch number of* L*.*

$2n$	# Rounds	1	2	3	4	5	6	7	8	9	10	11	12
16	p_{best}	+0	−2	−4	−7	−8	−11	−13	−16	−18	−20	−23	−25
	p_{bound}			−3			−6			−9			−12
32	p_{best}	+0	−2	−6	−9	−11	−16	−18	−20	−24	−28	−29	−34
	p_{bound}			−6			−12			−18			−24

Open Problem

The bound does not hold for the linear case.

Plan

Conclusion

source: Wiki Commons

Conclusion

source: Wiki Commons

Long-Trail Strategy

- Dual of the Wide-trail strategy
- Differential *and* linear bounds
- `https://www.cryptolux.org/index.php/SPARX`

Conclusion

source: Wiki Commons

Long-Trail Strategy

- Dual of the Wide-trail strategy
- Differential *and* linear bounds
- `https://www.cryptolux.org/index.php/SPARX`

LAX

- Branching number $\Longrightarrow$ diff. bound
- Open problem: *LAX for linear bound?*

Conclusion

source: Wiki Commons

Long-Trail Strategy

- Dual of the Wide-trail strategy
- Differential *and* linear bounds
- `https://www.cryptolux.org/index.php/SPARX`

LAX

- Branching number $\Longrightarrow$ diff. bound
- Open problem: *LAX for linear bound?*

Thank you!