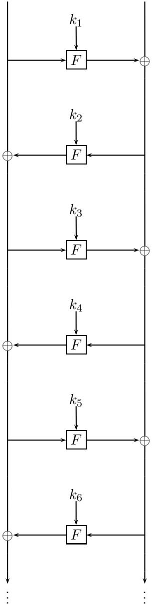
A family of 6-to-4-bit S-boxes with large linear branch number

Daniel Loebenberger Michael Nüsken

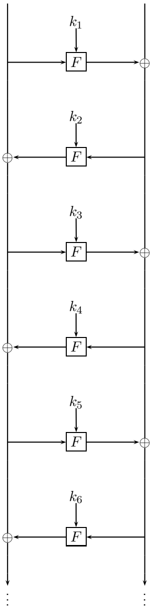
Bonn-Aachen International Center for Information Technology

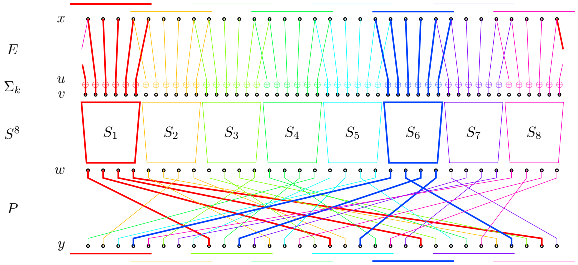
YACC 2014, 11 June 2014

From DES to DESL+

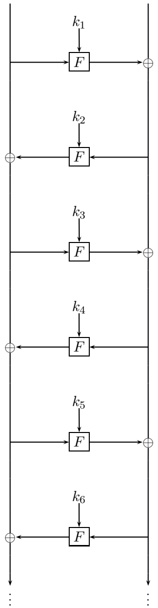


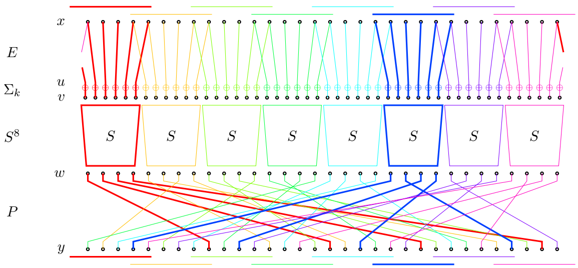
From DES to DESL+





DES round function

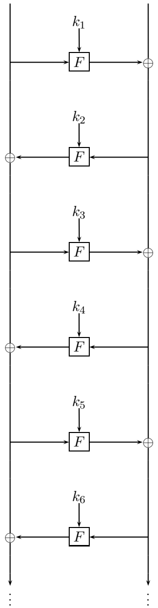


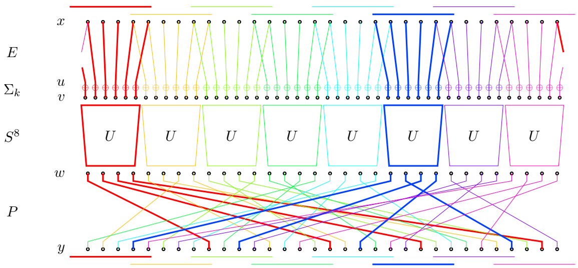


DESL round function

Leander, Paar, Poschmann & Schramm (2007)

From DES to DESL+





DESL+ round function

$efgh$	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$U(0efgh0)$	0	9	7	2	B	E	C	5	3	F	D	8	4	1	A	6
$U(0efgh1)$	B	6	8	F	2	1	5	C	D	A	E	3	7	4	0	9
$U(1efgh0)$	E	4	8	D	2	7	1	B	5	A	6	3	9	C	F	0
$U(1efgh1)$	1	D	4	2	F	8	A	7	6	0	9	5	C	B	3	E

Outline

Preliminaries

Properties

Applications to DESL

Summary

Outline

Preliminaries

Properties

Applications to DESL

Summary

S-boxes: Differential probabilities and bias

Consider an S-box $S\colon \mathbb{F}_2^k \to \mathbb{F}_2^\ell$.

Definition (Differential probability)

$$\begin{aligned}\mathsf{diff}_S(\Delta x \to \Delta y) &= \mathsf{prob}\left(S(X) \oplus S(X \oplus \Delta x) = \Delta y\right)\\ &= \frac{1}{2^k}\#\left\{x \in \mathbb{F}_2^k \,\middle|\, S(x) \oplus S(x \oplus \Delta x) = \Delta y\right\}\\ &\in [0,1]\end{aligned}$$

Definition (Bias)

$$\begin{aligned}\mathsf{bias}_S(a,b) &= \mathsf{prob}\left(\langle a \,|\, X\rangle = \langle b \,|\, S(X)\rangle\right) - \mathsf{prob}\left(\langle a \,|\, X\rangle \neq \langle b \,|\, S(X)\rangle\right)\\ &= \frac{1}{2^k}\sum_{x \in \mathbb{F}_2^k} (-1)^{\langle a \,|\, x\rangle}(-1)^{\langle b \,|\, S(x)\rangle}\\ &\in [-1,1]\end{aligned}$$

S-boxes: Differential probabilities and bias

Consider an S-box $S\colon \mathbb{F}_2^k \to \mathbb{F}_2^\ell$.

Definition (Differential probability)

$$\begin{aligned}\mathsf{diff}_S(\Delta x \to \Delta y) &= \mathsf{prob}\left(S(X) \oplus S(X \oplus \Delta x) = \Delta y\right)\\ &= \frac{1}{2^k} \# \left\{ x \in \mathbb{F}_2^k \,\middle|\, S(x) \oplus S(x \oplus \Delta x) = \Delta y \right\}\\ &\in [0,1]\end{aligned}$$

Definition (Bias)

$$\begin{aligned}\mathsf{bias}_S(a,b) &= \mathsf{prob}\left(\langle a \,|\, X\rangle = \langle b \,|\, S(X)\rangle\right) - \mathsf{prob}\left(\langle a \,|\, X\rangle \neq \langle b \,|\, S(X)\rangle\right)\\ &= \frac{1}{2^k} \sum_{x \in \mathbb{F}_2^k} (-1)^{\langle a \,|\, x\rangle} (-1)^{\langle b \,|\, S(x)\rangle}\\ &\in [-1,1]\end{aligned}$$

Consider an S-box $S\colon \mathbb{F}_2^k \to \mathbb{F}_2^\ell$.

Definition (Differential probability)

$$\begin{aligned}\mathsf{diff}_S(\Delta x \to \Delta y) &= \mathsf{prob}\left(S(X) \oplus S(X \oplus \Delta x) = \Delta y\right)\\ &= \frac{1}{2^k}\#\left\{x \in \mathbb{F}_2^k \,\middle|\, S(x) \oplus S(x \oplus \Delta x) = \Delta y\right\}\\ &\in [0,1]\end{aligned}$$

Definition (Bias)

$$\begin{aligned}\mathsf{bias}_S(a,b) &= \mathsf{prob}\left(\langle a \,|\, X\rangle = \langle b \,|\, S(X)\rangle\right) - \mathsf{prob}\left(\langle a \,|\, X\rangle \neq \langle b \,|\, S(X)\rangle\right)\\ &= \frac{1}{2^k}\sum_{x \in \mathbb{F}_2^k} (-1)^{\langle a \,|\, x\rangle}(-1)^{\langle b \,|\, S(x)\rangle}\\ &\in [-1,1]\end{aligned}$$

Differential and bias table

$\Delta x \setminus \Delta y$	0000	0001	0010	0100	1000	0011	0101	0110	1001	1010	1100	0111	1011	1101	1110	1111
000000	64	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
000001	.	.	.	.	.	6	6	2	8	4	6	2	6	4	4	16
000010	.	.	.	.	.	4	16	4	8	4	8	8	.	8	.	4
000100	.	.	.	.	.	8	8	4	8	.	4	12	4	4	4	8
001000	.	.	.	.	.	6	4	4	6	8	4	10	8	2	12	.
010000	.	.	.	.	.	8	8	8	4	4	4	4	8	4	8	4
100000	.	.	.	.	.	2	4	6	6	4	2	4	12	12	4	8
000011	8	4	6	.	4	8	4	10	4	10	4	.	.	.	2	.
000101	8	.	8	6	6	6	.	4	2	4	6	.	2	4	6	2
000110	.	.	12	8	4	8	.	4	8	.	4	.	4	.	12	.
001001	2	6	6	6	4	2	8	2	6	6	4	.	4	4	2	2
001010	.	.	10	4	2	8	.	6	8	4	6	4	4	4	4	.
001100	.	.	.	.	.	2	4	.	10	16	8	2	4	2	8	8
010001	2	6	4	6	6	2	6	4	4	4	8	6	.	2	2	2
010010	.	12	.	12	.	.	.	4	.	8	4	.	12	.	4	8
010100	.	4	8	4	16	.	8	4	.	.	4	8	.	8	.	.
011000	.	4	4	4	12	2	.	4	2	.	4	10	4	10	.	4
100001	10	2	6	8	10	2	4	6	4	2	.	2	.	2	2	4
100010	.	.	2	4	6	.	.	4	4	16	8	6	4	2	8	.
100100	.	2	8	10	8	4	4	4	4	8	4	.	2	.	2	4
101000	.	10	6	6	6	4	4	2	4	4	6	.	2	4	6	.
110000	.	8	6	.	2	4	8	8	.	8	4	2	4	6	4	.
000111	6	10	.	4	.	2	8	2	4	.	6	8	2	6	2	4
001011	2	2	.	2	8	4	2	6	6	4	2	6	6	4	4	6
001101	6	2	2	4	2	10	10	8	4	6	4	6	.	.	.	.
001110	.	.	2	4	2	4	16	2	8	8	6	4	.	4	.	4
010011	2	2	4	10	6	6	8	2	4	4	2	2	4	2	2	4
010101	6	10	.	.	8	2	.	2	2	4	.	8	8	6	8	.
010110	.	12	12	12	12	.	.	.	.	.	.	.	8	8	.	.
011001	.	4	10	8	6	2	.	4	2	2	2	8	6	2	4	4
011010	.	12	10	4	10	.	.	2	.	4	2	.	.	8	4	8
011100	.	8	4	8	4	6	.	8	2	4	4	2	4	2	.	8
100011	2	4	.	2	6	6	10	4	2	.	.	4	4	10	2	8
100101	.	2	.	4	4	6	2	6	8	6	.	4	14	4	.	4
100110	4	2	2	2	2	6	8	2	6	.	2	6	6	6	6	4
101001	.	10	4	6	2	8	4	6	4	4	2	2	.	4	4	4
101010	12	2	2	2	2	4	4	6	4	.	2	8	2	4	2	8
101100	.	12	10	8	2	6	4	4	2	.	4	4	.	.	4	4
110001	2	4	6	.	.	4	4	4	6	4	6	4	6	2	10	2
110010	8	4	.	4	.	6	.	2	2	4	6	12	8	4	.	4
110100	.	6	6	2	6	6	4	2	6	4	2	2	2	2	6	8
111000	.	6	8	10	4	2	4	4	6	4	4	2	6	2	2	.
001111	8	.	2	2	.	2	2	6	6	6	8	2	4	2	4	10
010111	.	.	6	6	6	4	.	2	.	2	4	10	10	4	6	4
011011	.	8	10	8	2	2	6	2	2	2	.	.	2	10	8	2
011101	8	4	2	2	.	2	2	6	4	2	2	2	6	10	6	6
011110	.	12	2	4	2	8	.	10	.	4	2	.	4	.	8	8
100111	4	4	6	6	.	2	.	8	2	8	8	2	2	4	8	.
101011	2	6	.	6	8	10	.	6	.	.	4	2	2	2	6	10
101101	2	6	2	2	8	4	2	2	.	12	6	4	2	6	2	4
101110	16	4	2	.	6	6	4	4	2	.	4	4	4	4	.	4
110011	6	2	6	2	4	6	2	4	4	.	6	.	8	2	8	4
110101	8	4	4	.	2	.	10	4	2	.	6	6	.	8	8	2
110110	8	2	4	2	4	4	.	4	4	.	4	4	2	4	10	8
111001	4	.	4	6	4	2	4	.	2	2	8	8	2	4	4	10
111010	8	2	4	2	.	2	8	4	6	4	4	6	2	6	2	4
111100	.	4	4	12	4	4	.	2	4	.	6	2	4	6	4	8
011111	6	6	4	.	6	4	2	2	6	4	6	4	4	4	4	2
101111	4	6	6	6	2	2	2	2	4	8	4	4	.	8	.	6
110111	8	2	8	2	2	2	8	.	8	4	2	6	6	4	2	.
111011	6	4	6	2	10	2	4	2	6	8	2	2	6	2	.	2
111101	6	4	6	6	2	6	2	4	6	2	4	2	8	2	2	2
111110	8	.	.	.	12	4	8	6	4	8	2	2	4	2	4	.
111111	.	4	.	6	.	2	6	6	6	4	6	12	4	.	6	2

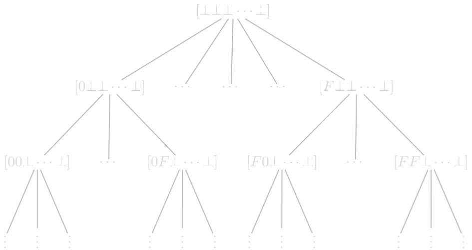
Table : $2^6 \cdot \mathsf{diff}_U(\Delta x \to \Delta y)$

$a \setminus b$	0000	0001	0010	0100	1000	0011	0101	0110	1001	1010	1100	0111	1011	1101	1110	1111
000000	64	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
000001	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
000010	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
000100	.	.	.	.	.	.	−8	.	8	8	.	−8	.	.	8	−8
001000	.	.	.	.	.	−8	8	.	8	−8	.	16	8	−16	−8	.
010000	.	.	.	.	.	.	8	.	.	.	.	−8	−16	8	.	−24
100000	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
000011	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
000101	.	.	.	.	.	.	−8	.	−8	8	.	−8	16	16	−24	8
000110	.	−8	−8	.	8	.	.	−8	8	−8	8	8	−8	16	−8	.
001001	.	.	.	.	.	8	8	.	−8	−8	.	.	8	.	−8	.
001010	.	.	8	−8	.	.	−16	16	−8	.	−8	16	.	8	8	−16
001100	.	.	.	.	.	−8	.	.	.	16	.	8	8	.	16	24
010001	.	.	.	.	.	.	−8	.	.	.	.	8	16	24	.	−8
010010	.	8	.	16	.	8	.	.	−8	16	.	.	−8	.	.	.
010100	.	.	−8	8	.	−8	−8	16	8	.	8	16	8	.	−8	.
011000	.	8	8	.	.	8	−8	8	16	.	.	−8	8	.	.	−8
100001	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
100010	.	.	.	.	.	16	16	−16	.	.	.	16	16	16	16	−16
100100	.	−8	−8	8	8	.	−8	.	8	8	.	.	8	−8	.	−8
101000	.	−8	−16	8	−16	16	8	8	.	−8	8	.	.	.	.	.
110000	.	.	.	.	.	.	−8	.	.	.	.	8	−16	24	.	24
000111	.	8	8	16	8	.	.	−8	8	8	−8	24	8	.	−8	.
001011	.	.	−8	−8	16	.	16	.	−8	.	8	16	.	8	8	16
001101	.	.	.	.	.	8	.	.	.	16	.	−8	−8	.	−16	8
001110	.	−8	.	8	8	.	.	−8	−16	8	16	8	−8	−8	.	.
010011	.	8	.	.	.	8	.	16	−8	−16	16	.	−8	.	16	.
010101	.	16	−8	−8	.	8	8	.	8	.	−8	.	8	.	8	.
010110	.	.	−16	8	−8	.	8	−8	16	16	16	−8	−8	8	8	.
011001	.	8	8	.	.	−8	8	8	.	.	.	−8	8	.	.	8
011010	.	.	.	8	.	24	8	8	−24	8	−8	.	8	.	.	.
011100	.	−8	16	−8	.	.	−24	−8	−8	.	−8	.	.	8	8	.
100011	.	.	.	.	.	16	−16	−16	.	.	.	−16	16	−16	16	16
100101	.	−8	8	8	−8	16	−8	16	8	8	16	16	−8	−8	.	8
100110	.	.	.	8	.	16	.	−8	8	−8	−8	.	.	−8	.	.
101001	.	−8	16	8	16	.	8	8	16	−8	8	−16	.	16	.	.
101010	.	−8	8	.	.	−8	.	−8	.	.	16	.	8	−8	.	.
101100	.	.	8	.	−8	.	.	−8	8	−16	−8	.	−8	8	.	24
110001	.	.	.	.	.	.	8	.	.	.	.	−8	16	8	.	8
110010	.	−8	.	.	.	8	.	.	8	−16	−16	.	−8	.	.	.
110100	.	8	.	16	−8	−8	−8	.	8	.	−8	8	.	8	16	.
111000	.	.	−8	8	16	.	8	16	8	.	−24	−8	.	.	8	8
001111	.	8	.	−8	−8	.	.	8	−16	−8	16	−8	8	8	.	.
010111	.	.	.	−8	−8	−16	8	−8	.	.	.	8	−8	−8	8	.
011011	.	.	−16	−8	−16	−8	8	8	8	8	−8	.	8	.	−16	.
011101	.	8	16	8	.	.	−8	8	8	.	8	.	.	−8	−8	.
011110	.	8	.	.	−8	−16	.	16	.	8	8	−8	8	8	8	.
100111	.	16	.	−8	16	.	.	8	−8	8	−8	.	−16	−8	.	.
101011	.	−8	−8	.	16	−8	.	8	.	.	.	.	8	−8	.	.
101101	.	.	−8	.	8	.	.	8	−8	−16	8	.	8	−8	.	8
101110	.	8	8	8	.	8	.	.	8	8	8	.	8	.	.	.
110011	.	−8	.	−16	.	8	.	16	8	16	.	.	−8	.	16	.
110101	.	−8	16	.	−24	−8	8	.	−8	.	−8	8	.	−8	.	.
110110	.	8	8	.	.	.	8	−8	.	16	.	.	.	.	.	.
111001	.	.	−8	8	16	−16	−8	−16	−8	.	8	−8	.	.	8	−8
111010	.	8	.	.	.	.	8	.	.	8	.	.	.	.	8	.
111100	.	8	8	−8	8	8	8	.	.	.	.	8	.	.	−8	.
011111	.	8	.	−16	8	.	.	.	16	−8	8	8	8	−8	8	.
101111	.	24	−8	24	.	−8	.	.	−8	−8	−8	.	−8	.	.	.
110111	.	−24	8	16	16	.	8	8	.	.	.	.	.	.	.	.
111011	.	8	16	−16	16	.	8	.	.	8	.	.	.	.	−8	.
111101	.	−8	24	8	−8	−8	24	.	.	.	.	−8	.	.	8	.
111110	.	−8	−8	−16	.	8	.	−8	8	8	.	.	−8	.	−8	.
111111	.	24	8	.	.	8	.	−8	8	−8	16	.	−8	.	−8	.

Table : $2^6 \cdot \mathsf{bias}_U(a, b)$

How to find an S-box

- There are $2^{4 \cdot 2^6} = 2^{256}$ S-boxes mapping 6 bits to 4 bits.
- Most of them are not suitable for cryptographic purposes.



Techniques:

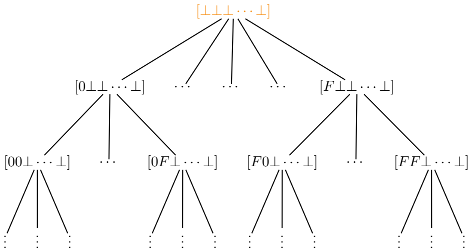
- Start with a void S-box.
- Add values depth first like.
- Incrementally compute differential and bias table (afap).
  - Diff: 0, $+1$ or $+2$. (few)
  - Bias: -1 or $+1$. (all)
- Purge subtree if node is too bad.
- Optional: sort children by penalty.
- Use isomorphisms: $49\,152$ members in the family.

Still, there are roughly $10^{14} \approx 2^{47}$ nodes to traverse!

Split into manageable tasks, by cutting the tree at a certain level.
We used level 18, leading to $937\,140$ subtrees to consider.

How to find an S-box

- There are $2^{4\cdot 2^6} = 2^{256}$ S-boxes mapping 6 bits to 4 bits.
- Most of them are not suitable for cryptographic purposes.



Techniques:

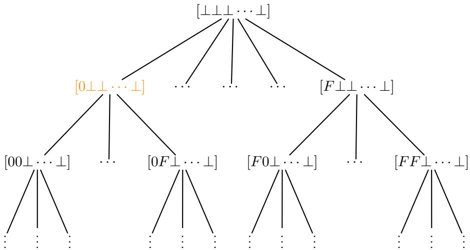
- Start with a void S-box.
- Add values depth first like.
- Incrementally compute differential and bias table (afap).
  - Diff: 0, $+1$ or $+2$. (few)
  - Bias: -1 or $+1$. (all)
- Purge subtree if node is too bad.
- Optional: sort children by penalty.
- Use isomorphisms: $49\,152$ members in the family.

Still, there are roughly $10^{14} \approx 2^{47}$ nodes to traverse!

Split into manageable tasks, by cutting the tree at a certain level.
We used level 18, leading to $937\,140$ subtrees to consider.

How to find an S-box

- There are $2^{4 \cdot 2^6} = 2^{256}$ S-boxes mapping 6 bits to 4 bits.
- Most of them are not suitable for cryptographic purposes.



Techniques:

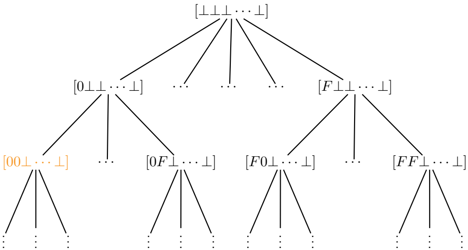
- Start with a void S-box.
- Add values depth first like.
- Incrementally compute differential and bias table (afap).
  - Diff: 0, $+1$ or $+2$. (few)
  - Bias: -1 or $+1$. (all)
- Purge subtree if node is too bad.
- Optional: sort children by penalty.
- Use isomorphisms: $49\,152$ members in the family.

Still, there are roughly $10^{14} \approx 2^{47}$ nodes to traverse!

Split into manageable tasks, by cutting the tree at a certain level.
We used level 18, leading to $937\,140$ subtrees to consider.

How to find an S-box

- There are $2^{4 \cdot 2^6} = 2^{256}$ S-boxes mapping 6 bits to 4 bits.
- Most of them are not suitable for cryptographic purposes.



Techniques:

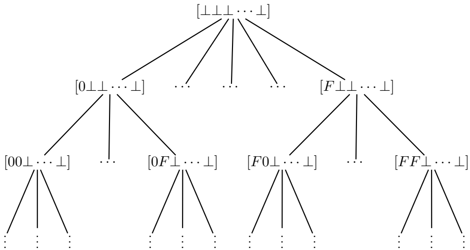
- Start with a void S-box.
- Add values depth first like.
- Incrementally compute differential and bias table (afap).
  - Diff: 0, $+1$ or $+2$. (few)
  - Bias: -1 or $+1$. (all)
- Purge subtree if node is too bad.
- Optional: sort children by penalty.
- Use isomorphisms: $49\,152$ members in the family.

Still, there are roughly $10^{14} \approx 2^{47}$ nodes to traverse!

Split into manageable tasks, by cutting the tree at a certain level.
We used level 18, leading to $937\,140$ subtrees to consider.

How to find an S-box

- There are $2^{4\cdot 2^6} = 2^{256}$ S-boxes mapping 6 bits to 4 bits.
- Most of them are not suitable for cryptographic purposes.



Techniques:

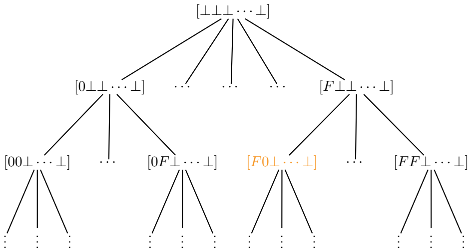
- Start with a void S-box.
- Add values depth first like.
- Incrementally compute differential and bias table (afap).
  - Diff: 0, $+1$ or $+2$. (few)
  - Bias: -1 or $+1$. (all)
- Purge subtree if node is too bad.
- Optional: sort children by penalty.
- Use isomorphisms: $49\,152$ members in the family.

Still, there are roughly $10^{14} \approx 2^{47}$ nodes to traverse!

Split into manageable tasks, by cutting the tree at a certain level.
We used level 18, leading to $937\,140$ subtrees to consider.

How to find an S-box

- There are $2^{4\cdot 2^6} = 2^{256}$ S-boxes mapping 6 bits to 4 bits.
- Most of them are not suitable for cryptographic purposes.



Techniques:

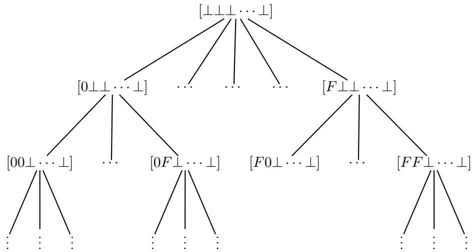
- Start with a void S-box.
- Add values depth first like.
- Incrementally compute differential and bias table (afap).
  - Diff: 0, $+1$ or $+2$. (few)
  - Bias: -1 or $+1$. (all)
- Purge subtree if node is too bad.
- Optional: sort children by penalty.
- Use isomorphisms: $49\,152$ members in the family.

Still, there are roughly $10^{14} \approx 2^{47}$ nodes to traverse!

Split into manageable tasks, by cutting the tree at a certain level.
We used level 18, leading to $937\,140$ subtrees to consider.

How to find an S-box

- There are $2^{4 \cdot 2^6} = 2^{256}$ S-boxes mapping 6 bits to 4 bits.
- Most of them are not suitable for cryptographic purposes.



Techniques:

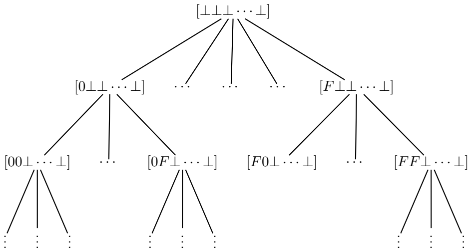
- Start with a void S-box.
- Add values depth first like.
- Incrementally compute differential and bias table (afap).
  - Diff: 0, $+1$ or $+2$. (few)
  - Bias: -1 or $+1$. (all)
- Purge subtree if node is too bad.
- Optional: sort children by penalty.
- Use isomorphisms: $49\,152$ members in the family.

Still, there are roughly $10^{14} \approx 2^{47}$ nodes to traverse!

Split into manageable tasks, by cutting the tree at a certain level.
We used level 18, leading to $937\,140$ subtrees to consider.

How to find an S-box

- There are $2^{4 \cdot 2^6} = 2^{256}$ S-boxes mapping 6 bits to 4 bits.
- Most of them are not suitable for cryptographic purposes.



Techniques:

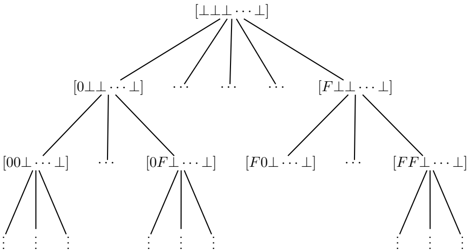
- Start with a void S-box.
- Add values depth first like.
- Incrementally compute differential and bias table (afap).
  - Diff: 0, $+1$ or $+2$. (few)
  - Bias: -1 or $+1$. (all)
- Purge subtree if node is too bad.
- Optional: sort children by penalty.
- Use isomorphisms: $49\,152$ members in the family.

Still, there are roughly $10^{14} \approx 2^{47}$ nodes to traverse!

Split into manageable tasks, by cutting the tree at a certain level.
We used level 18, leading to $937\,140$ subtrees to consider.

How to find an S-box

- There are $2^{4 \cdot 2^6} = 2^{256}$ S-boxes mapping 6 bits to 4 bits.
- Most of them are not suitable for cryptographic purposes.



Techniques:

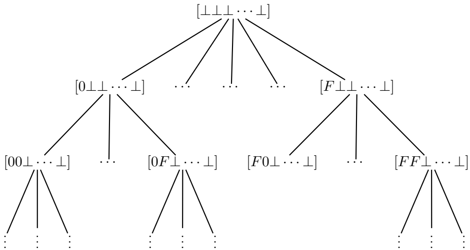
- Start with a void S-box.
- Add values depth first like.
- Incrementally compute differential and bias table (afap).
  - Diff: 0, $+1$ or $+2$. (few)
  - Bias: -1 or $+1$. (all)
- Purge subtree if node is too bad.
- Optional: sort children by penalty.
- Use isomorphisms: $49\,152$ members in the family.

Still, there are roughly $10^{14} \approx 2^{47}$ nodes to traverse!

Split into manageable tasks, by cutting the tree at a certain level.
We used level 18, leading to $937\,140$ subtrees to consider.

How to find an S-box

- There are $2^{4 \cdot 2^6} = 2^{256}$ S-boxes mapping 6 bits to 4 bits.
- Most of them are not suitable for cryptographic purposes.



Techniques:

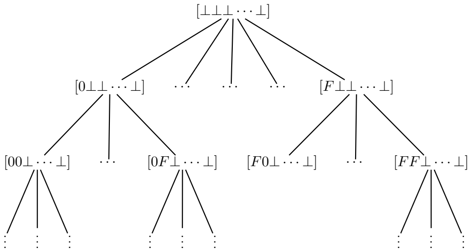
- Start with a void S-box.
- Add values depth first like.
- Incrementally compute differential and bias table (afap).
  - Diff: 0, $+1$ or $+2$. (few)
  - Bias: -1 or $+1$. (all)
- Purge subtree if node is too bad.
- Optional: sort children by penalty.
- Use isomorphisms: $49\,152$ members in the family.

Still, there are roughly $10^{14} \approx 2^{47}$ nodes to traverse!

Split into manageable tasks, by cutting the tree at a certain level.
We used level 18, leading to $937\,140$ subtrees to consider.

How to find an S-box

- There are $2^{4 \cdot 2^6} = 2^{256}$ S-boxes mapping 6 bits to 4 bits.
- Most of them are not suitable for cryptographic purposes.



Techniques:

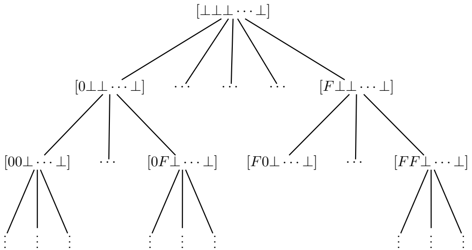
- Start with a void S-box.
- Add values depth first like.
- Incrementally compute differential and bias table (afap).
  - Diff: 0, $+1$ or $+2$. (few)
  - Bias: -1 or $+1$. (all)
- Purge subtree if node is too bad.
- Optional: sort children by penalty.
- Use isomorphisms: $49\,152$ members in the family.

Still, there are roughly $10^{14} \approx 2^{47}$ nodes to traverse!

Split into manageable tasks, by cutting the tree at a certain level.
We used level 18, leading to $937\,140$ subtrees to consider.

How to find an S-box

- There are $2^{4 \cdot 2^6} = 2^{256}$ S-boxes mapping 6 bits to 4 bits.
- Most of them are not suitable for cryptographic purposes.



Techniques:

- Start with a void S-box.
- Add values depth first like.
- Incrementally compute differential and bias table (afap).
  - Diff: 0, $+1$ or $+2$. (few)
  - Bias: -1 or $+1$. (all)
- Purge subtree if node is too bad.
- Optional: sort children by penalty.
- Use isomorphisms: $49\,152$ members in the family.

Still, there are roughly $10^{14} \approx 2^{47}$ nodes to traverse!

For purging,

- in early runs: properties (on diff and bias) by Leander, Paar, Poschmann & Schramm (2007) with some relaxations,
- in later runs: our own properties.

Outline

Preliminaries

Properties

Applications to DESL

Summary

Differential properties

$\Delta x \setminus \Delta y$	0000	0001	0010	0100	1000	0011	0101	0110	1001	1010	1100	0111	1011	1101	1110	1111
000000	64	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
000001	.	.	.	.	.	6	6	2	8	4	6	2	6	4	4	16
000010	.	.	.	.	.	4	16	4	8	4	8	8	.	8	.	4
000100	.	.	.	.	.	8	8	4	8	.	4	12	4	4	4	8
001000	.	.	.	.	.	6	4	4	6	8	4	10	8	2	12	.
010000	.	.	.	.	.	8	8	8	4	4	4	4	8	4	8	4
100000	.	.	.	.	.	2	4	6	6	4	2	4	12	12	4	8
000011	8	4	6	.	4	8	4	10	4	10	4	.	.	.	2	.
000101	8	.	8	6	6	6	.	4	2	4	6	.	2	4	6	2
000110	.	.	12	8	4	8	.	4	8	.	4	.	4	.	12	.
001001	2	6	6	6	4	2	8	2	6	6	4	.	4	4	2	2
001010	.	.	10	4	2	8	.	6	8	4	6	4	4	4	4	.
001100	.	.	.	.	.	2	4	.	10	16	8	2	4	2	8	8
010001	2	6	4	6	6	2	6	4	4	4	8	6	.	2	2	2
010010	.	12	.	12	.	.	.	4	.	8	4	.	12	.	4	8
010100	.	4	8	4	16	.	8	4	.	.	4	8	.	8	.	.
011000	.	4	4	4	12	2	.	4	2	.	4	10	4	10	.	4
100001	10	2	6	8	10	2	4	6	4	2	.	2	.	2	2	4
100010	.	.	2	4	6	.	.	4	4	16	8	6	4	2	8	.
100100	.	2	8	10	8	4	4	4	4	8	4	.	2	.	2	4
101000	.	10	6	6	6	4	4	2	4	4	6	.	2	4	6	.
110000	.	8	6	.	2	4	8	8	.	8	4	2	4	6	4	.
000111	6	10	.	4	.	2	8	2	4	.	6	8	2	6	2	4
001011	2	2	.	2	8	4	2	6	6	4	2	6	6	4	4	6
001101	6	2	2	4	2	10	10	8	4	6	4	6	.	.	.	.
001110	.	.	2	4	2	4	16	2	8	8	6	4	.	4	.	4
010011	2	2	4	10	6	6	8	2	4	4	2	2	4	2	2	4
010101	6	10	.	.	8	2	.	2	2	4	.	8	8	6	8	.
010110	.	12	12	12	12	.	.	.	.	.	.	.	8	8	.	.
011001	.	4	10	8	6	2	.	4	2	2	2	8	6	2	4	4
011010	.	12	10	4	10	.	.	2	.	4	2	.	.	8	4	8
011100	.	8	4	8	4	6	.	8	2	4	4	2	4	2	.	8
100011	2	4	.	2	6	6	10	4	2	.	.	4	4	10	2	8
100101	.	2	.	4	4	6	2	6	8	6	.	4	14	4	.	4
100110	4	2	2	2	2	6	8	2	6	.	2	6	6	6	6	4
101001	.	10	4	6	2	8	4	6	4	4	2	2	.	4	4	4
101010	12	2	2	2	2	4	4	6	4	.	2	8	2	4	2	8
101100	.	12	10	8	2	6	4	4	2	.	4	4	.	.	4	4
110001	2	4	6	.	.	4	4	4	6	4	6	4	6	2	10	2
110010	8	4	.	4	.	6	.	2	2	4	6	12	8	4	.	4
110100	.	6	6	2	6	6	4	2	6	4	2	2	2	2	6	8
111000	.	6	8	10	4	2	4	4	6	4	4	2	6	2	2	.
001111	8	.	2	2	.	2	2	6	6	6	8	2	4	2	4	10
010111	.	.	6	6	6	4	.	2	.	2	4	10	10	4	6	4
011011	.	8	10	8	2	2	6	2	2	2	.	.	2	10	8	2
011101	8	4	2	2	.	2	2	6	4	2	2	2	6	10	6	6
011110	.	12	2	4	2	8	.	10	.	4	2	.	4	.	8	8
100111	4	4	6	6	.	2	.	8	2	8	8	2	2	4	8	.
101011	2	6	.	6	8	10	.	6	.	.	4	2	2	2	6	10
101101	2	6	2	2	8	4	2	2	.	12	6	4	2	6	2	4
101110	16	4	2	.	6	6	4	4	2	.	4	4	4	4	.	4
110011	6	2	6	2	4	6	2	4	4	.	6	.	8	2	8	4
110101	8	4	4	.	2	.	10	4	2	.	6	6	.	8	8	2
110110	8	2	4	2	4	4	.	4	4	.	4	4	2	4	10	8
111001	4	.	4	6	4	2	4	.	2	2	8	8	2	4	4	10
111010	8	2	4	2	.	2	8	4	6	4	4	6	2	6	2	4
111100	.	4	4	12	4	4	.	2	4	.	6	2	4	6	4	8
011111	6	6	4	.	6	4	2	2	6	4	6	4	4	4	4	2
101111	4	6	6	6	2	2	2	2	4	8	4	4	.	8	.	6
110111	8	2	8	2	2	2	8	.	8	4	2	6	6	4	2	.
111011	6	4	6	2	10	2	4	2	6	8	2	2	6	2	.	2
111101	6	4	6	6	2	6	2	4	6	2	4	2	8	2	2	2
111110	8	.	.	.	12	4	8	6	4	8	2	2	4	2	4	.
111111	.	4	.	6	.	2	6	6	6	4	6	12	4	.	6	2

Table : $2^6 \cdot \mathsf{diff}_U(\Delta x \to \Delta y)$

Coppersmith, 1994:

S-1 $k = 6,\ \ell = 4.$

S-3 $\mathsf{diff}_S(0{*}{*}{*}{*}0 \to 0000) = 0.$

S-4 $\mathsf{diff}_S(\underline{\quad \text{wt } 1 \quad} \to \underline{\text{wt} \le 1}) = 0.$

S-5 $\mathsf{diff}_S(001100 \to \underline{\text{wt} \le 1}) = 0.$

S-7 $\mathsf{diff}_S(\Delta x \to \Delta y) \le \frac{16}{64}$ for $\Delta x \ne 0.$

Kim, Lee, Park & Lee, 1995:

Q1 $\mathsf{diff}_S(1{*}{*}{*}00 \to 0000) = 0$

$\Rightarrow$ Due to S-4, if $\mathsf{wt}(\Delta x) + \mathsf{wt}(\Delta y) < 2$ then $\mathsf{diff}_S(\Delta x \to \Delta y) = 0$, i.e. $\mathsf{diffbranch}(U) = 2.$

Differential properties

$\Delta x \setminus \Delta y$	0000	0001	0010	0100	1000	0011	0101	0110	1001	1010	1100	0111	1011	1101	1110	1111
000000	64	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
000001	.	.	.	.	.	6	6	2	8	4	6	2	6	4	4	16
000010	.	.	.	.	.	4	16	4	8	4	8	8	.	8	.	4
000100	.	.	.	.	.	8	8	4	8	.	4	12	4	4	4	8
001000	.	.	.	.	.	6	4	4	6	8	4	10	8	2	12	.
010000	.	.	.	.	.	8	8	8	4	4	4	4	8	4	8	4
100000	.	.	.	.	.	2	4	6	6	4	2	4	12	12	4	8
000011	8	4	6	.	4	8	4	10	4	10	4	.	.	.	2	.
000101	8	.	8	6	6	6	.	4	2	4	6	.	2	4	6	2
000110	.	.	12	8	4	8	.	4	8	.	4	.	4	.	12	.
001001	2	6	6	6	4	2	8	2	6	6	4	.	4	4	2	2
001010	.	.	10	4	2	8	.	6	8	4	6	4	4	4	4	.
001100	.	.	.	.	.	2	4	.	10	16	8	2	4	2	8	8
010001	2	6	4	6	6	2	6	4	4	4	8	6	.	2	2	2
010010	.	12	.	12	.	.	.	4	.	8	4	.	12	.	4	8
010100	.	4	8	4	16	.	8	4	.	.	4	8	.	8	.	.
011000	.	4	4	4	12	2	.	4	2	.	4	10	4	10	.	4
100001	10	2	6	8	10	2	4	6	4	2	.	2	.	2	2	4
100010	.	.	2	4	6	.	.	4	4	16	8	6	4	2	8	.
100100	.	2	8	10	8	4	4	4	4	8	4	.	2	.	2	4
101000	.	10	6	6	6	4	4	2	4	4	6	.	2	4	6	.
110000	.	8	6	.	2	4	8	8	.	8	4	2	4	6	4	.
000111	6	10	.	4	.	2	8	2	4	.	6	8	2	6	2	4
001011	2	2	.	2	8	4	2	6	6	4	2	6	6	4	4	6
001101	6	2	2	4	2	10	10	8	4	6	4	6	.	.	.	.
001110	.	.	2	4	2	4	16	2	8	8	6	4	.	4	.	4
010011	2	2	4	10	6	6	8	2	4	4	2	2	4	2	2	4
010101	6	10	.	.	8	2	.	2	2	4	.	8	8	6	8	.
010110	.	12	12	12	12	.	.	.	.	.	.	.	8	8	.	.
011001	.	4	10	8	6	2	.	4	2	2	2	8	6	2	4	4
011010	.	12	10	4	10	.	.	2	.	4	2	.	.	8	4	8
011100	.	8	4	8	4	6	.	8	2	4	4	2	4	2	.	8
100011	2	4	.	2	6	6	10	4	2	.	.	4	4	10	2	8
100101	.	2	.	4	4	6	2	6	8	6	.	4	14	4	.	4
100110	4	2	2	2	2	6	8	2	6	.	2	6	6	6	6	4
101001	.	10	4	6	2	8	4	6	4	4	2	2	.	4	4	4
101010	12	2	2	2	2	4	4	6	4	.	2	8	2	4	2	8
101100	.	12	10	8	2	6	4	4	2	.	4	4	.	.	4	4
110001	2	4	6	.	.	4	4	4	6	4	6	4	6	2	10	2
110010	8	4	.	4	.	6	.	2	2	4	6	12	8	4	.	4
110100	.	6	6	2	6	6	4	2	6	4	2	2	2	2	6	8
111000	.	6	8	10	4	2	4	4	6	4	4	2	6	2	2	.
001111	8	.	2	2	.	2	2	6	6	6	8	2	4	2	4	10
010111	.	.	6	6	6	4	.	2	.	2	4	10	10	4	6	4
011011	.	8	10	8	2	2	6	2	2	2	.	.	2	10	8	2
011101	8	4	2	2	.	2	2	6	4	2	2	2	6	10	6	6
011110	.	12	2	4	2	8	.	10	.	4	2	.	4	.	8	8
100111	4	4	6	6	.	2	.	8	2	8	8	2	2	4	8	.
101011	2	6	.	6	8	10	.	6	.	.	4	2	2	2	6	10
101101	2	6	2	2	8	4	2	2	.	12	6	4	2	6	2	4
101110	16	4	2	.	6	6	4	4	2	.	4	4	4	4	.	4
110011	6	2	6	2	4	6	2	4	4	.	6	.	8	2	8	4
110101	8	4	4	.	2	.	10	4	2	.	6	6	.	8	8	2
110110	8	2	4	2	4	4	.	4	4	.	4	4	2	4	10	8
111001	4	.	4	6	4	2	4	.	2	2	8	8	2	4	4	10
111010	8	2	4	2	.	2	8	4	6	4	4	6	2	6	2	4
111100	.	4	4	12	4	4	.	2	4	.	6	2	4	6	4	8
011111	6	6	4	.	6	4	2	2	6	4	6	4	4	4	4	2
101111	4	6	6	6	2	2	2	2	4	8	4	4	.	8	.	6
110111	8	2	8	2	2	2	8	.	8	4	2	6	6	4	2	.
111011	6	4	6	2	10	2	4	2	6	8	2	2	6	2	.	2
111101	6	4	6	6	2	6	2	4	6	2	4	2	8	2	2	2
111110	8	.	.	.	12	4	8	6	4	8	2	2	4	2	4	.
111111	.	4	.	6	.	2	6	6	6	4	6	12	4	.	6	2

Table : $2^6 \cdot \mathsf{diff}_U(\Delta x \to \Delta y)$

Coppersmith, 1994:

S-1 $k = 6,\ \ell = 4.$

S-3 $\mathsf{diff}_S(0{*}{*}{*}{*}0 \to 0000) = 0.$

S-4 $\mathsf{diff}_S(\underline{\quad \text{wt } 1 \quad} \to \underline{\text{wt} \leq 1}) = 0.$

S-5 $\mathsf{diff}_S(001100 \to \underline{\text{wt} \leq 1}) = 0.$

S-7 $\mathsf{diff}_S(\Delta x \to \Delta y) \leq \frac{16}{64}$ for $\Delta x \neq 0.$

Kim, Lee, Park & Lee, 1995:

Q1 $\mathsf{diff}_S(1{*}{*}{*}00 \to 0000) = 0$

$\Rightarrow$ Due to S-4, if $\text{wt}(\Delta x) + \text{wt}(\Delta y) < 2$ then $\mathsf{diff}_S(\Delta x \to \Delta y) = 0$, i.e. $\mathsf{diffbranch}(U) = 2.$

Differential properties

$\Delta x \setminus \Delta y$	0000	0001	0010	0100	1000	0011	0101	0110	1001	1010	1100	0111	1011	1101	1110	1111
000000	64	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
000001	.	.	.	.	.	6	6	2	8	4	6	2	6	4	4	16
000010	.	.	.	.	.	4	16	4	8	4	8	8	.	8	.	4
000100	.	.	.	.	.	8	8	4	8	.	4	12	4	4	4	8
001000	.	.	.	.	.	6	4	4	6	8	4	10	8	2	12	.
010000	.	.	.	.	.	8	8	8	4	4	4	4	8	4	8	4
100000	.	.	.	.	.	2	4	6	6	4	2	4	12	12	4	8
000011	8	4	6	.	4	8	4	10	4	10	4	.	.	.	2	.
000101	8	.	8	6	6	6	.	4	2	4	6	.	2	4	6	2
000110	.	.	12	8	4	8	.	4	8	.	4	.	4	.	12	.
001001	2	6	6	6	4	2	8	2	6	6	4	.	4	4	2	2
001010	.	.	10	4	2	8	.	6	8	4	6	4	4	4	4	.
001100	.	.	.	.	.	2	4	.	10	16	8	2	4	2	8	8
010001	2	6	4	6	6	2	6	4	4	4	8	6	.	2	2	2
010010	.	12	.	12	.	.	.	4	.	8	4	.	12	.	4	8
010100	.	4	8	4	16	.	8	4	.	.	4	8	.	8	.	.
011000	.	4	4	4	12	2	.	4	2	.	4	10	4	10	.	4
100001	10	2	6	8	10	2	4	6	4	2	.	2	.	2	2	4
100010	.	.	2	4	6	.	.	4	4	16	8	6	4	2	8	.
100100	.	2	8	10	8	4	4	4	4	8	4	.	2	.	2	4
101000	.	10	6	6	6	4	4	2	4	4	6	.	2	4	6	.
110000	.	8	6	.	2	4	8	8	.	8	4	2	4	6	4	.
000111	6	10	.	4	.	2	8	2	4	.	6	8	2	6	2	4
001011	2	2	.	2	8	4	2	6	6	4	2	6	6	4	4	6
001101	6	2	2	4	2	10	10	8	4	6	4	6	.	.	.	.
001110	.	.	2	4	2	4	16	2	8	8	6	4	.	4	.	4
010011	2	2	4	10	6	6	8	2	4	4	2	2	4	2	2	4
010101	6	10	.	.	8	2	.	2	2	4	.	8	8	6	8	.
010110	.	12	12	12	12	.	.	.	.	.	.	.	8	8	.	.
011001	.	4	10	8	6	2	.	4	2	2	2	8	6	2	4	4
011010	.	12	10	4	10	.	.	2	.	4	2	.	.	8	4	8
011100	.	8	4	8	4	6	.	8	2	4	4	2	4	2	.	8
100011	2	4	.	2	6	6	10	4	2	.	.	4	4	10	2	8
100101	.	2	.	4	4	6	2	6	8	6	.	4	14	4	.	4
100110	4	2	2	2	2	6	8	2	6	.	2	6	6	6	6	4
101001	.	10	4	6	2	8	4	6	4	4	2	2	.	4	4	4
101010	12	2	2	2	2	4	4	6	4	.	2	8	2	4	2	8
101100	.	12	10	8	2	6	4	4	2	.	4	4	.	.	4	4
110001	2	4	6	.	.	4	4	4	6	4	6	4	6	2	10	2
110010	8	4	.	4	.	6	.	2	2	4	6	12	8	4	.	4
110100	.	6	6	2	6	6	4	2	6	4	2	2	2	2	6	8
111000	.	6	8	10	4	2	4	4	6	4	4	2	6	2	2	.
001111	8	.	2	2	.	2	2	6	6	6	8	2	4	2	4	10
010111	.	.	6	6	6	4	.	2	.	2	4	10	10	4	6	4
011011	.	8	10	8	2	2	6	2	2	2	.	.	2	10	8	2
011101	8	4	2	2	.	2	2	6	4	2	2	2	6	10	6	6
011110	.	12	2	4	2	8	.	10	.	4	2	.	4	.	8	8
100111	4	4	6	6	.	2	.	8	2	8	8	2	2	4	8	.
101011	2	6	.	6	8	10	.	6	.	.	4	2	2	2	6	10
101101	2	6	2	2	8	4	2	2	.	12	6	4	2	6	2	4
101110	16	4	2	.	6	6	4	4	2	.	4	4	4	4	.	4
110011	6	2	6	2	4	6	2	4	4	.	6	.	8	2	8	4
110101	8	4	4	.	2	.	10	4	2	.	6	6	.	8	8	2
110110	8	2	4	2	4	4	.	4	4	.	4	4	2	4	10	8
111001	4	.	4	6	4	2	4	.	2	2	8	8	2	4	4	10
111010	8	2	4	2	.	2	8	4	6	4	4	6	2	6	2	4
111100	.	4	4	12	4	4	.	2	4	.	6	2	4	6	4	8
011111	6	6	4	.	6	4	2	2	6	4	6	4	4	4	4	2
101111	4	6	6	6	2	2	2	2	4	8	4	4	.	8	.	6
110111	8	2	8	2	2	2	8	.	8	4	2	6	6	4	2	.
111011	6	4	6	2	10	2	4	2	6	8	2	2	6	2	.	2
111101	6	4	6	6	2	6	2	4	6	2	4	2	8	2	2	2
111110	8	.	.	.	12	4	8	6	4	8	2	2	4	2	4	.
111111	.	4	.	6	.	2	6	6	6	4	6	12	4	.	6	2

Table : $2^6 \cdot \mathrm{diff}_U(\Delta x \to \Delta y)$

Coppersmith, 1994:

S-1 $k = 6$, $\ell = 4$.

S-3 $\mathrm{diff}_S(0{*}{*}{*}{*}0 \to 0000) = 0$.

S-4 $\mathrm{diff}_S(\underline{\text{wt } 1} \to \underline{\text{wt} \leq 1}) = 0$.

S-5 $\mathrm{diff}_S(001100 \to \underline{\text{wt} \leq 1}) = 0$.

S-7 $\mathrm{diff}_S(\Delta x \to \Delta y) \leq \frac{16}{64}$ for $\Delta x \neq 0$.

Kim, Lee, Park & Lee, 1995:

Q1 $\mathrm{diff}_S(1{*}{*}{*}00 \to 0000) = 0$

$\Rightarrow$ Due to S-4,
if $\mathrm{wt}(\Delta x) + \mathrm{wt}(\Delta y) < 2$
then $\mathrm{diff}_S(\Delta x \to \Delta y) = 0$,
i.e. $\mathrm{diffbranch}(U) = 2$.

Differential properties

$\Delta x \setminus \Delta y$	0000	0001	0010	0100	1000	0011	0101	0110	1001	1010	1100	0111	1011	1101	1110	1111
000000	64	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
000001	.	.	.	.	.	6	6	2	8	4	6	2	6	4	4	16
000010	.	.	.	.	.	4	16	4	8	4	8	8	.	8	.	4
000100	.	.	.	.	.	8	8	4	8	.	4	12	4	4	4	8
001000	.	.	.	.	.	6	4	4	6	8	4	10	8	2	12	.
010000	.	.	.	.	.	8	8	8	4	4	4	4	8	4	8	4
100000	.	.	.	.	.	2	4	6	6	4	2	4	12	12	4	8
000011	8	4	6	.	4	8	4	10	4	10	4	.	.	.	2	.
000101	8	.	8	6	6	6	.	4	2	4	6	.	2	4	6	2
000110	.	.	12	8	4	8	.	4	8	.	4	.	4	.	12	.
001001	2	6	6	6	4	2	8	2	6	6	4	.	4	4	2	2
001010	.	.	10	4	2	8	.	6	8	4	6	4	4	4	4	.
001100	.	.	.	.	.	2	4	.	10	16	8	2	4	2	8	8
010001	2	6	4	6	6	2	6	4	4	4	8	6	.	2	2	2
010010	.	12	.	12	.	.	.	4	.	8	4	.	12	.	4	8
010100	.	4	8	4	16	.	8	4	.	.	4	8	.	8	.	.
011000	.	4	4	4	12	2	.	4	2	.	4	10	4	10	.	4
100001	10	2	6	8	10	2	4	6	4	2	.	2	.	2	2	4
100010	.	.	2	4	6	.	.	4	4	16	8	6	4	2	8	.
100100	.	2	8	10	8	4	4	4	4	8	4	.	2	.	2	4
101000	.	10	6	6	6	4	4	2	4	4	6	.	2	4	6	.
110000	.	8	6	.	2	4	8	8	.	8	4	2	4	6	4	.
000111	6	10	.	4	.	2	8	2	4	.	6	8	2	6	2	4
001011	2	2	.	2	8	4	2	6	6	4	2	6	6	4	4	6
001101	6	2	2	4	2	10	10	8	4	6	4	6	.	.	.	.
001110	.	.	2	4	2	4	16	2	8	8	6	4	.	4	.	4
010011	2	2	4	10	6	6	8	2	4	4	2	2	4	2	2	4
010101	6	10	.	.	8	2	.	2	2	4	.	8	8	6	8	.
010110	.	12	12	12	12	.	.	.	.	.	.	.	8	8	.	.
011001	.	4	10	8	6	2	.	4	2	2	2	8	6	2	4	4
011010	.	12	10	4	10	.	.	2	.	4	2	.	.	8	4	8
011100	.	8	4	8	4	6	.	8	2	4	4	2	4	2	.	8
100011	2	4	.	2	6	6	10	4	2	.	.	4	4	10	2	8
100101	.	2	.	4	4	6	2	6	8	6	.	4	14	4	.	4
100110	4	2	2	2	2	6	8	2	6	.	2	6	6	6	6	4
101001	.	10	4	6	2	8	4	6	4	4	2	2	.	4	4	4
101010	12	2	2	2	2	4	4	6	4	.	2	8	2	4	2	8
101100	.	12	10	8	2	6	4	4	2	.	4	4	.	.	4	4
110001	2	4	6	.	.	4	4	4	6	4	6	4	6	2	10	2
110010	8	4	.	4	.	6	.	2	2	4	6	12	8	4	.	4
110100	.	6	6	2	6	6	4	2	6	4	2	2	2	2	6	8
111000	.	6	8	10	4	2	4	4	6	4	4	2	6	2	2	.
001111	8	.	2	2	.	2	2	6	6	6	8	2	4	2	4	10
010111	.	.	6	6	6	4	.	2	.	2	4	10	10	4	6	4
011011	.	8	10	8	2	2	6	2	2	2	.	.	2	10	8	2
011101	8	4	2	2	.	2	2	6	4	2	2	2	6	10	6	6
011110	.	12	2	4	2	8	.	10	.	4	2	.	4	.	8	8
100111	4	4	6	6	.	2	.	8	2	8	8	2	2	4	8	.
101011	2	6	.	6	8	10	.	6	.	.	4	2	2	2	6	10
101101	2	6	2	2	8	4	2	2	.	12	6	4	2	6	2	4
101110	16	4	2	.	6	6	4	4	2	.	4	4	4	4	.	4
110011	6	2	6	2	4	6	2	4	4	.	6	.	8	2	8	4
110101	8	4	4	.	2	.	10	4	2	.	6	6	.	8	8	2
110110	8	2	4	2	4	4	.	4	4	.	4	4	2	4	10	8
111001	4	.	4	6	4	2	4	.	2	2	8	8	2	4	4	10
111010	8	2	4	2	.	2	8	4	6	4	4	6	2	6	2	4
111100	.	4	4	12	4	4	.	2	4	.	6	2	4	6	4	8
011111	6	6	4	.	6	4	2	2	6	4	6	4	4	4	4	2
101111	4	6	6	6	2	2	2	2	4	8	4	4	.	8	.	6
110111	8	2	8	2	2	2	8	.	8	4	2	6	6	4	2	.
111011	6	4	6	2	10	2	4	2	6	8	2	2	6	2	.	2
111101	6	4	6	6	2	6	2	4	6	2	4	2	8	2	2	2
111110	8	.	.	.	12	4	8	6	4	8	2	2	4	2	4	.
111111	.	4	.	6	.	2	6	6	6	4	6	12	4	.	6	2

Table : $2^6 \cdot \mathrm{diff}_U(\Delta x \to \Delta y)$

Coppersmith, 1994:

S-1 $k = 6,\ \ell = 4.$

S-3 $\mathrm{diff}_S(0{*}{*}{*}{*}0 \to 0000) = 0.$

S-4 $\mathrm{diff}_S(\underline{\text{wt } 1} \to \underline{\text{wt} \leq 1}) = 0.$

S-5 $\mathrm{diff}_S(001100 \to \underline{\text{wt} \leq 1}) = 0.$

S-7 $\mathrm{diff}_S(\Delta x \to \Delta y) \leq \frac{16}{64}$ for $\Delta x \neq 0.$

Kim, Lee, Park & Lee, 1995:

Q1 $\mathrm{diff}_S(1{*}{*}{*}00 \to 0000) = 0$

$\Rightarrow$ Due to S-4,
if $\mathrm{wt}(\Delta x) + \mathrm{wt}(\Delta y) < 2$
then $\mathrm{diff}_S(\Delta x \to \Delta y) = 0$,
i.e. $\mathrm{diffbranch}(U) = 2.$

Linear properties

Q2$^+$ $|\mathsf{bias}_S(a,b)| \leq \frac{24}{64}$ for $a \neq 0$.

Q3$^+$ $\mathsf{bias}_S(\underline{\quad \mathsf{wt}\ 1 \quad}, \underline{\quad \mathsf{wt}\ 1 \quad}) = 0$.

Q4$^+$ $|\mathsf{bias}_S(\underline{\quad \mathsf{wt}\ k \quad}, \underline{\quad \mathsf{wt}\ \ell \quad})| \leq \frac{16}{64}$ when $0 < k + \ell \leq 4$.

Q5$^-$ $|\mathsf{bias}_S(a, b_1) \cdot \mathsf{bias}_S(a, b_2)| \leq \frac{384}{64^2}$ for all $a \in \mathbb{F}_2^6$, $b_1, b_2 \in \mathbb{F}_2^4$ with $\mathsf{wt}(b_1 + b_2) = 1$.

$\Rightarrow$ Due to Q3$^+$, if $\mathsf{wt}(a) + \mathsf{wt}(b) < 3$ then $\mathsf{bias}_S(a,b) = 0$, i.e. $\mathsf{linbranch}(U) = 3$.

$a \setminus b$	0000	0001	0010	0100	1000	0011	0101	0110	1001	1010	1100	0111	1011	1101	1110	1111
000000	64	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
000001	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
000010	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
000100	.	.	.	.	.	.	−8	.	8	8	.	−8	.	.	8	−8
001000	.	.	.	.	.	−8	8	.	8	−8	.	16	8	−16	−8	.
010000	.	.	.	.	.	.	8	.	.	.	.	−8	−16	8	.	−24
100000	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
000011	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
000101	.	.	.	.	.	.	−8	.	−8	8	.	−8	16	16	−24	8
000110	.	−8	−8	.	8	.	.	−8	8	−8	8	8	−8	16	−8	.
001001	.	.	.	.	.	8	8	.	−8	−8	.	.	8	.	−8	.
001010	.	.	8	−8	.	.	−16	16	−8	.	−8	16	.	8	8	−16
001100	.	.	.	.	.	−8	.	.	.	16	.	8	8	.	16	24
010001	.	.	.	.	.	.	−8	.	.	.	.	8	16	24	.	−8
010010	.	8	.	16	.	8	.	.	−8	16	.	.	−8	.	.	.
010100	.	.	−8	8	.	−8	−8	16	8	.	8	16	8	.	−8	.
011000	.	8	8	.	.	8	−8	8	16	.	.	−8	8	.	.	−8
100001	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
100010	.	.	.	.	.	16	16	−16	.	.	.	16	16	16	16	−16
100100	.	−8	−8	8	8	.	−8	.	8	8	.	.	8	−8	.	−8
101000	.	−8	−16	8	−16	16	8	8	.	−8	8	.	.	.	.	.
110000	.	.	.	.	.	.	−8	.	.	.	.	8	−16	24	.	24
000111	.	8	8	16	8	.	.	−8	8	8	−8	24	8	.	−8	.
001011	.	.	−8	−8	16	.	16	.	−8	.	8	16	.	8	8	16
001101	.	.	.	.	.	8	.	.	.	16	.	−8	−8	.	−16	8
001110	.	−8	.	8	8	.	.	−8	−16	8	16	8	−8	−8	.	.
010011	.	8	.	.	.	8	.	16	−8	−16	16	.	−8	.	16	.
010101	.	16	−8	−8	.	8	8	.	8	.	−8	.	8	.	8	.
010110	.	.	−16	8	−8	.	8	−8	16	16	16	−8	−8	8	8	.
011001	.	8	8	.	.	−8	8	8	.	.	.	−8	8	.	.	8
011010	.	.	.	8	.	24	8	8	−24	8	−8	.	8	.	.	.
011100	.	−8	16	−8	.	.	−24	−8	−8	.	−8	.	.	8	8	.
100011	.	.	.	.	.	16	−16	−16	.	.	.	−16	16	−16	16	16
100101	.	−8	8	8	−8	16	−8	16	8	8	16	16	−8	−8	.	8
100110	.	.	.	8	.	16	.	−8	8	−8	−8	.	.	−8	.	.
101001	.	−8	16	8	16	.	8	8	16	−8	8	−16	.	16	.	.
101010	.	−8	8	.	.	−8	.	−8	.	.	16	.	8	−8	.	.
101100	.	.	8	.	−8	.	.	−8	8	−16	−8	.	−8	8	.	24
110001	.	.	.	.	.	.	8	.	.	.	.	−8	16	8	.	8
110010	.	−8	.	.	.	8	.	.	8	−16	−16	.	−8	.	.	.
110100	.	8	.	16	−8	−8	−8	.	8	.	−8	8	.	8	16	.
111000	.	.	−8	8	16	.	8	16	8	.	−24	−8	.	.	8	8
001111	.	8	.	−8	−8	.	.	8	−16	−8	16	−8	8	8	.	.
010111	.	.	.	−8	−8	−16	8	−8	.	.	.	8	−8	−8	8	.
011011	.	.	−16	−8	−16	−8	8	8	8	8	−8	.	8	.	−16	.
011101	.	8	16	8	.	.	−8	8	8	.	8	.	.	−8	−8	.
011110	.	8	.	.	−8	−16	.	16	.	8	8	−8	8	8	8	.
100111	.	16	.	−8	16	.	.	8	−8	8	−8	.	−16	−8	.	.
101011	.	−8	−8	.	16	−8	.	8	.	.	.	.	8	−8	.	.
101101	.	.	−8	.	8	.	.	8	−8	−16	8	.	8	−8	.	8
101110	.	8	8	8	.	8	.	.	8	8	8	.	8	.	.	.
110011	.	−8	.	−16	.	8	.	16	8	16	.	.	−8	.	16	.
110101	.	−8	16	.	−24	−8	8	.	−8	.	−8	8	.	−8	.	.
110110	.	8	8	.	.	.	8	−8	.	16	.	.	.	.	.	.
111001	.	.	−8	8	16	−16	−8	−16	−8	.	8	−8	.	.	8	−8
111010	.	8	.	.	.	.	8	.	.	8	.	.	.	.	8	.
111100	.	8	8	−8	8	8	8	.	.	.	.	8	.	.	−8	.
011111	.	8	.	−16	8	.	.	.	16	−8	8	8	8	−8	8	.
101111	.	24	−8	24	.	−8	.	.	−8	−8	−8	.	−8	.	.	.
110111	.	−24	8	16	16	.	8	8	.	.	.	.	.	.	.	.
111011	.	8	16	−16	16	.	8	.	.	8	.	.	.	.	−8	.
111101	.	−8	24	8	−8	−8	24	.	.	.	.	−8	.	.	8	.
111110	.	−8	−8	−16	.	8	.	−8	8	8	.	.	−8	.	−8	.
111111	.	24	8	.	.	8	.	−8	8	−8	16	.	−8	.	−8	.

Table : $2^6 \cdot \mathsf{bias}_U(a,b)$

Linear properties

Q2$^+$ $|\text{bias}_S(a,b)| \le \frac{24}{64}$ for $a \neq 0$.

Q3$^+$ $\text{bias}_S(\underline{\quad\text{wt } 1\quad}, \underline{\quad\text{wt } 1\quad}) = 0.$

Q4$^+$ $|\text{bias}_S(\underline{\quad\text{wt } k\quad}, \underline{\quad\text{wt } \ell\quad})| \le \frac{16}{64}$ when $0 < k + \ell \le 4$.

Q5$^-$ $|\text{bias}_S(a, b_1) \cdot \text{bias}_S(a, b_2)| \le \frac{384}{64^2}$ for all $a \in \mathbb{F}_2^6$, $b_1, b_2 \in \mathbb{F}_2^4$ with $\text{wt}(b_1 + b_2) = 1$.

$\Rightarrow$ Due to Q3$^+$,
if $\text{wt}(a) + \text{wt}(b) < 3$
then $\text{bias}_S(a,b) = 0$,
i.e. $\text{linbranch}(U) = 3$.

$a \setminus b$	0000	0001	0010	0100	1000	0011	0101	0110	1001	1010	1100	0111	1011	1101	1110	1111
000000	64	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
000001	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
000010	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
000100	.	.	.	.	.	.	−8	.	8	8	.	−8	.	.	8	−8
001000	.	.	.	.	.	−8	8	.	8	−8	.	16	8	−16	−8	.
010000	.	.	.	.	.	.	8	.	.	.	.	−8	−16	8	.	−24
100000	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
000011	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
000101	.	.	.	.	.	.	−8	.	−8	8	.	−8	16	16	−24	8
000110	.	−8	−8	.	8	.	.	−8	8	−8	8	8	−8	16	−8	.
001001	.	.	.	.	.	8	8	.	−8	−8	.	.	8	.	−8	.
001010	.	.	8	−8	.	.	−16	16	−8	.	−8	16	.	8	8	−16
001100	.	.	.	.	.	−8	.	.	.	16	.	8	8	.	16	24
010001	.	.	.	.	.	.	−8	.	.	.	.	8	16	24	.	−8
010010	.	8	.	16	.	8	.	.	−8	16	.	.	−8	.	.	.
010100	.	.	−8	8	.	−8	−8	16	8	.	8	16	8	.	−8	.
011000	.	8	8	.	.	8	−8	8	16	.	.	−8	8	.	.	−8
100001	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
100010	.	.	.	.	.	16	16	−16	.	.	.	16	16	16	16	−16
100100	.	−8	−8	8	8	.	−8	.	8	8	.	.	8	−8	.	−8
101000	.	−8	−16	8	−16	16	8	8	.	−8	8	.	.	.	.	.
110000	.	.	.	.	.	.	−8	.	.	.	.	8	−16	24	.	24
000111	.	8	8	16	8	.	.	−8	8	8	−8	24	8	.	−8	.
001011	.	.	−8	−8	16	.	16	.	−8	.	8	16	.	8	8	16
001101	.	.	.	.	.	8	.	.	.	16	.	−8	−8	.	−16	8
001110	.	−8	.	8	8	.	.	−8	−16	8	16	8	−8	−8	.	.
010011	.	8	.	.	.	8	.	16	−8	−16	16	.	−8	.	16	.
010101	.	16	−8	−8	.	8	8	.	8	.	−8	.	8	.	8	.
010110	.	.	−16	8	−8	.	8	−8	16	16	16	−8	−8	8	8	.
011001	.	8	8	.	.	−8	8	8	.	.	.	−8	8	.	.	8
011010	.	.	.	8	.	24	8	8	−24	8	−8	.	8	.	.	.
011100	.	−8	16	−8	.	.	−24	−8	−8	.	−8	.	.	8	8	.
100011	.	.	.	.	.	16	−16	−16	.	.	.	−16	16	−16	16	16
100101	.	−8	8	8	−8	16	−8	16	8	8	16	16	−8	−8	.	8
100110	.	.	.	8	.	16	.	−8	8	−8	−8	.	.	−8	.	.
101001	.	−8	16	8	16	.	8	8	16	−8	8	−16	.	16	.	.
101010	.	−8	8	.	.	−8	.	−8	.	.	16	.	8	−8	.	.
101100	.	.	8	.	−8	.	.	−8	8	−16	−8	.	−8	8	.	24
110001	.	.	.	.	.	.	8	.	.	.	.	−8	16	8	.	8
110010	.	−8	.	.	.	8	.	.	8	−16	−16	.	−8	.	.	.
110100	.	8	.	16	−8	−8	−8	.	8	.	−8	8	.	8	16	.
111000	.	.	−8	8	16	.	8	16	8	.	−24	−8	.	.	8	8
001111	.	8	.	−8	−8	.	.	8	−16	−8	16	−8	8	8	.	.
010111	.	.	.	−8	−8	−16	8	−8	.	.	.	8	−8	−8	8	.
011011	.	.	−16	−8	−16	−8	8	8	8	8	−8	.	8	.	−16	.
011101	.	8	16	8	.	.	−8	8	8	.	8	.	.	−8	−8	.
011110	.	8	.	.	−8	−16	.	16	.	8	8	−8	8	8	8	.
100111	.	16	.	−8	16	.	.	8	−8	8	−8	.	−16	−8	.	.
101011	.	−8	−8	.	16	−8	.	8	.	.	.	.	8	−8	.	.
101101	.	.	−8	.	8	.	.	8	−8	−16	8	.	8	−8	.	8
101110	.	8	8	8	.	8	.	.	8	8	8	.	8	.	.	.
110011	.	−8	.	−16	.	8	.	16	8	16	.	.	−8	.	16	.
110101	.	−8	16	.	−24	−8	8	.	−8	.	−8	8	.	−8	.	.
110110	.	8	8	.	.	.	8	−8	.	16	.	.	.	.	.	.
111001	.	.	−8	8	16	−16	−8	−16	−8	.	8	−8	.	.	8	−8
111010	.	8	.	.	.	.	8	.	.	8	.	.	.	.	8	.
111100	.	8	8	−8	8	8	8	.	.	.	.	8	.	.	−8	.
011111	.	8	.	−16	8	.	.	.	16	−8	8	8	8	−8	8	.
101111	.	24	−8	24	.	−8	.	.	−8	−8	−8	.	−8	.	.	.
110111	.	−24	8	16	16	.	8	8	.	.	.	.	.	.	.	.
111011	.	8	16	−16	16	.	8	.	.	8	.	.	.	.	−8	.
111101	.	−8	24	8	−8	−8	24	.	.	.	.	−8	.	.	8	.
111110	.	−8	−8	−16	.	8	.	−8	8	8	.	.	−8	.	−8	.
111111	.	24	8	.	.	8	.	−8	8	−8	16	.	−8	.	−8	.

Table : $2^6 \cdot \text{bias}_U(a,b)$

Linear properties

Q2$^+$ $|\mathsf{bias}_S(a,b)| \leq \frac{24}{64}$ for $a \neq 0$.

Q3$^+$ $\mathsf{bias}_S(\underline{\quad \text{wt } 1 \quad}, \underline{\quad \text{wt } 1 \quad}) = 0$.

Q4$^+$ $|\mathsf{bias}_S(\underline{\quad \text{wt } k \quad}, \underline{\quad \text{wt } \ell \quad})| \leq \frac{16}{64}$ when $0 < k + \ell \leq 4$.

Q5$^-$ $|\mathsf{bias}_S(a, b_1) \cdot \mathsf{bias}_S(a, b_2)| \leq \frac{384}{64^2}$ for all $a \in \mathbb{F}_2^6$, $b_1, b_2 \in \mathbb{F}_2^4$ with $\mathrm{wt}(b_1 + b_2) = 1$.

$\Rightarrow$ Due to Q3$^+$, if $\mathrm{wt}(a) + \mathrm{wt}(b) < 3$ then $\mathsf{bias}_S(a,b) = 0$, i.e. $\mathrm{linbranch}(U) = 3$.

$a \setminus b$	0000	0001	0010	0100	1000	0011	0101	0110	1001	1010	1100	0111	1011	1101	1110	1111
000000	64	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
000001	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
000010	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
000100	.	.	.	.	.	.	−8	.	8	8	.	−8	.	.	8	−8
001000	.	.	.	.	.	−8	8	.	8	−8	.	16	8	−16	−8	.
010000	.	.	.	.	.	.	8	.	.	.	.	−8	−16	8	.	−24
100000	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
000011	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
000101	.	.	.	.	.	.	−8	.	−8	8	.	−8	16	16	−24	8
000110	.	−8	−8	.	8	.	.	−8	8	−8	8	8	−8	16	−8	.
001001	.	.	.	.	.	8	8	.	−8	−8	.	.	8	.	−8	.
001010	.	.	8	−8	.	.	−16	16	−8	.	−8	16	.	8	8	−16
001100	.	.	.	.	.	−8	.	.	.	16	.	8	8	.	16	24
010001	.	.	.	.	.	.	−8	.	.	.	.	8	16	24	.	−8
010010	.	8	.	16	.	8	.	.	−8	16	.	.	−8	.	.	.
010100	.	.	−8	8	.	−8	−8	16	8	.	8	16	8	.	−8	.
011000	.	8	8	.	.	8	−8	8	16	.	.	−8	8	.	.	−8
100001	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
100010	.	.	.	.	.	16	16	−16	.	.	.	16	16	16	16	−16
100100	.	−8	−8	8	8	.	−8	.	8	8	.	.	8	−8	.	−8
101000	.	−8	−16	8	−16	16	8	8	.	−8	8	.	.	.	.	.
110000	.	.	.	.	.	.	−8	.	.	.	.	8	−16	24	.	24
000111	.	8	8	16	8	.	.	−8	8	8	−8	24	8	.	−8	.
001011	.	.	−8	−8	16	.	16	.	−8	.	8	16	.	8	8	16
001101	.	.	.	.	.	8	.	.	.	16	.	−8	−8	.	−16	8
001110	.	−8	.	8	8	.	.	−8	−16	8	16	8	−8	−8	.	.
010011	.	8	.	.	.	8	.	16	−8	−16	16	.	−8	.	16	.
010101	.	16	−8	−8	.	8	8	.	8	.	−8	.	8	.	8	.
010110	.	.	−16	8	−8	.	8	−8	16	16	16	−8	−8	8	8	.
011001	.	8	8	.	.	−8	8	8	.	.	.	−8	8	.	.	8
011010	.	.	.	8	.	24	8	8	−24	8	−8	.	8	.	.	.
011100	.	−8	16	−8	.	.	−24	−8	−8	.	−8	.	.	8	8	.
100011	.	.	.	.	.	16	−16	−16	.	.	.	−16	16	−16	16	16
100101	.	−8	8	8	−8	16	−8	16	8	8	16	16	−8	−8	.	8
100110	.	.	.	8	.	16	.	−8	8	−8	−8	.	.	−8	.	.
101001	.	−8	16	8	16	.	8	8	16	−8	8	−16	.	16	.	.
101010	.	−8	8	.	.	−8	.	−8	.	.	16	.	8	−8	.	.
101100	.	.	8	.	−8	.	.	−8	8	−16	−8	.	−8	8	.	24
110001	.	.	.	.	.	.	8	.	.	.	.	−8	16	8	.	8
110010	.	−8	.	.	.	8	.	.	8	−16	−16	.	−8	.	.	.
110100	.	8	.	16	−8	−8	−8	.	8	.	−8	8	.	8	16	.
111000	.	.	−8	8	16	.	8	16	8	.	−24	−8	.	.	8	8
001111	.	8	.	−8	−8	.	.	8	−16	−8	16	−8	8	8	.	.
010111	.	.	.	−8	−8	−16	8	−8	.	.	.	8	−8	−8	8	.
011011	.	.	−16	−8	−16	−8	8	8	8	8	−8	.	8	.	−16	.
011101	.	8	16	8	.	.	−8	8	8	.	8	.	.	−8	−8	.
011110	.	8	.	.	−8	−16	.	16	.	8	8	−8	8	8	8	.
100111	.	16	.	−8	16	.	.	8	−8	8	−8	.	−16	−8	.	.
101011	.	−8	−8	.	16	−8	.	8	.	.	.	.	8	−8	.	.
101101	.	.	−8	.	8	.	.	8	−8	−16	8	.	8	−8	.	8
101110	.	8	8	8	.	8	.	.	8	8	8	.	8	.	.	.
110011	.	−8	.	−16	.	8	.	16	8	16	.	.	−8	.	16	.
110101	.	−8	16	.	−24	−8	8	.	−8	.	−8	8	.	−8	.	.
110110	.	8	8	.	.	.	8	−8	.	16	.	.	.	.	.	.
111001	.	.	−8	8	16	−16	−8	−16	−8	.	8	−8	.	.	8	−8
111010	.	8	.	.	.	.	8	.	.	8	.	.	.	.	8	.
111100	.	8	8	−8	8	8	8	.	.	.	.	8	.	.	−8	.
011111	.	8	.	−16	8	.	.	.	16	−8	8	8	8	−8	8	.
101111	.	24	−8	24	.	−8	.	.	−8	−8	−8	.	−8	.	.	.
110111	.	−24	8	16	16	.	8	8	.	.	.	.	.	.	.	.
111011	.	8	16	−16	16	.	8	.	.	8	.	.	.	.	−8	.
111101	.	−8	24	8	−8	−8	24	.	.	.	.	−8	.	.	8	.
111110	.	−8	−8	−16	.	8	.	−8	8	8	.	.	−8	.	−8	.
111111	.	24	8	.	.	8	.	−8	8	−8	16	.	−8	.	−8	.

Table : $2^6 \cdot \mathsf{bias}_U(a,b)$

Linear properties

Q2$^+$ $|\mathsf{bias}_S(a,b)| \le \frac{24}{64}$ for $a \neq 0$.

Q3$^+$ $\mathsf{bias}_S(\underline{\quad \text{wt } 1 \quad}, \underline{\quad \text{wt } 1 \quad}) = 0$.

Q4$^+$ $|\mathsf{bias}_S(\underline{\quad \text{wt } k \quad}, \underline{\quad \text{wt } \ell \quad})| \le \frac{16}{64}$ when $0 < k + \ell \le 4$.

Q5$^-$ $|\mathsf{bias}_S(a,b_1) \cdot \mathsf{bias}_S(a,b_2)| \le \frac{384}{64^2}$ for all $a \in \mathbb{F}_2^6$, $b_1, b_2 \in \mathbb{F}_2^4$ with $\mathrm{wt}(b_1 + b_2) = 1$.

$\Rightarrow$ Due to Q3$^+$, if $\mathrm{wt}(a) + \mathrm{wt}(b) < 3$ then $\mathsf{bias}_S(a,b) = 0$, i.e. $\mathrm{linbranch}(U) = 3$.

$a \setminus b$	0000	0001	0010	0100	1000	0011	0101	0110	1001	1010	1100	0111	1011	1101	1110	1111
000000	64	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
000001	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
000010	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
000100	.	.	.	.	.	.	−8	.	8	8	.	−8	.	.	8	−8
001000	.	.	.	.	.	−8	8	.	8	−8	.	16	8	−16	−8	.
010000	.	.	.	.	.	.	8	.	.	.	.	−8	−16	8	.	−24
100000	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
000011	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
000101	.	.	.	.	.	.	−8	.	−8	8	.	−8	16	16	−24	8
000110	.	−8	−8	.	8	.	.	−8	8	−8	8	8	−8	16	−8	.
001001	.	.	.	.	.	8	8	.	−8	−8	.	.	8	.	−8	.
001010	.	.	8	−8	.	.	−16	16	−8	.	−8	16	.	8	8	−16
001100	.	.	.	.	.	−8	.	.	.	16	.	8	8	.	16	24
010001	.	.	.	.	.	.	−8	.	.	.	.	8	16	24	.	−8
010010	.	8	.	16	.	8	.	.	−8	16	.	.	−8	.	.	.
010100	.	.	−8	8	.	−8	−8	16	8	.	8	16	8	.	−8	.
011000	.	8	8	.	.	8	−8	8	16	.	.	−8	8	.	.	−8
100001	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
100010	.	.	.	.	.	16	16	−16	.	.	.	16	16	16	16	−16
100100	.	−8	−8	8	8	.	−8	.	8	8	.	.	8	−8	.	−8
101000	.	−8	−16	8	−16	16	8	8	.	−8	8	.	.	.	.	.
110000	.	.	.	.	.	.	−8	.	.	.	.	8	−16	24	.	24
000111	.	8	8	16	8	.	.	−8	8	8	−8	24	8	.	−8	.
001011	.	.	−8	−8	16	.	16	.	−8	.	8	16	.	8	8	16
001101	.	.	.	.	.	8	.	.	.	16	.	−8	−8	.	−16	8
001110	.	−8	.	8	8	.	.	−8	−16	8	16	8	−8	−8	.	.
010011	.	8	.	.	.	8	.	16	−8	−16	16	.	−8	.	16	.
010101	.	16	−8	−8	.	8	8	.	8	.	−8	.	8	.	8	.
010110	.	.	−16	8	−8	.	8	−8	16	16	16	−8	−8	8	8	.
011001	.	8	8	.	.	−8	8	8	.	.	.	−8	8	.	.	8
011010	.	.	.	8	.	24	8	8	−24	8	−8	.	8	.	.	.
011100	.	−8	16	−8	.	.	−24	−8	−8	.	−8	.	.	8	8	.
100011	.	.	.	.	.	16	−16	−16	.	.	.	−16	16	−16	16	16
100101	.	−8	8	8	−8	16	−8	16	8	8	16	16	−8	−8	.	8
100110	.	.	.	8	.	16	.	−8	8	−8	−8	.	.	−8	.	.
101001	.	−8	16	8	16	.	8	8	16	−8	8	−16	.	16	.	.
101010	.	−8	8	.	.	−8	.	−8	.	.	16	.	8	−8	.	.
101100	.	.	8	.	−8	.	.	−8	8	−16	−8	.	−8	8	.	24
110001	.	.	.	.	.	.	8	.	.	.	.	−8	16	8	.	8
110010	.	−8	.	.	.	8	.	.	8	−16	−16	.	−8	.	.	.
110100	.	8	.	16	−8	−8	−8	.	8	.	−8	8	.	8	16	.
111000	.	.	−8	8	16	.	8	16	8	.	−24	−8	.	.	8	8
001111	.	8	.	−8	−8	.	.	8	−16	−8	16	−8	8	8	.	.
010111	.	.	.	−8	−8	−16	8	−8	.	.	.	8	−8	−8	8	.
011011	.	.	−16	−8	−16	−8	8	8	8	8	−8	.	8	.	−16	.
011101	.	8	16	8	.	.	−8	8	8	.	8	.	.	−8	−8	.
011110	.	8	.	.	−8	−16	.	16	.	8	8	−8	8	8	8	.
100111	.	16	.	−8	16	.	.	8	−8	8	−8	.	−16	−8	.	.
101011	.	−8	−8	.	16	−8	.	8	.	.	.	.	8	−8	.	.
101101	.	.	−8	.	8	.	.	8	−8	−16	8	.	8	−8	.	8
101110	.	8	8	8	.	8	.	.	8	8	8	.	8	.	.	.
110011	.	−8	.	−16	.	8	.	16	8	16	.	.	−8	.	16	.
110101	.	−8	16	.	−24	−8	8	.	−8	.	−8	8	.	−8	.	.
110110	.	8	8	.	.	.	8	−8	.	16	.	.	.	.	.	.
111001	.	.	−8	8	16	−16	−8	−16	−8	.	8	−8	.	.	8	−8
111010	.	8	.	.	.	.	8	.	.	8	.	.	.	.	8	.
111100	.	8	8	−8	8	8	8	.	.	.	.	8	.	.	−8	.
011111	.	8	.	−16	8	.	.	.	16	−8	8	8	8	−8	8	.
101111	.	24	−8	24	.	−8	.	.	−8	−8	−8	.	−8	.	.	.
110111	.	−24	8	16	16	.	8	8	.	.	.	.	.	.	.	.
111011	.	8	16	−16	16	.	8	.	.	8	.	.	.	.	−8	.
111101	.	−8	24	8	−8	−8	24	.	.	.	.	−8	.	.	8	.
111110	.	−8	−8	−16	.	8	.	−8	8	8	.	.	−8	.	−8	.
111111	.	24	8	.	.	8	.	−8	8	−8	16	.	−8	.	−8	.

Table : $2^6 \cdot \mathsf{bias}_U(a,b)$

Linear properties

Q2$^+$ $|\text{bias}_S(a,b)| \leq \frac{24}{64}$ for $a \neq 0$.

Q3$^+$ $\text{bias}_S(\underline{\text{wt } 1}, \underline{\text{wt } 1}) = 0$.

Q4$^+$ $|\text{bias}_S(\underline{\text{wt } k}, \underline{\text{wt } \ell})| \leq \frac{16}{64}$ when $0 < k + \ell \leq 4$.

Q5$^-$ $|\text{bias}_S(a,b_1) \cdot \text{bias}_S(a,b_2)| \leq \frac{384}{64^2}$ for all $a \in \mathbb{F}_2^6$, $b_1, b_2 \in \mathbb{F}_2^4$ with $\text{wt}(b_1 + b_2) = 1$.

$\Rightarrow$ Due to Q3$^+$, if $\text{wt}(a) + \text{wt}(b) < 3$ then $\text{bias}_S(a,b) = 0$, i.e. $\text{linbranch}(U) = 3$.

$a \setminus b$	0000	0001	0010	0100	1000	0011	0101	0110	1001	1010	1100	0111	1011	1101	1110	1111
000000	64	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
000001	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
000010	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
000100	.	.	.	.	.	.	−8	.	8	8	.	−8	.	.	8	−8
001000	.	.	.	.	.	−8	8	.	8	−8	.	16	8	−16	−8	.
010000	.	.	.	.	.	.	8	.	.	.	.	−8	−16	8	.	−24
100000	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
000011	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
000101	.	.	.	.	.	.	−8	.	−8	8	.	−8	16	16	−24	8
000110	.	−8	−8	.	8	.	.	−8	8	−8	8	8	−8	16	−8	.
001001	.	.	.	.	.	8	8	.	−8	−8	.	.	8	.	−8	.
001010	.	.	8	−8	.	.	−16	16	−8	.	−8	16	.	8	8	−16
001100	.	.	.	.	.	−8	.	.	.	16	.	8	8	.	16	24
010001	.	.	.	.	.	.	−8	.	.	.	.	8	16	24	.	−8
010010	.	8	.	16	.	8	.	.	−8	16	.	.	−8	.	.	.
010100	.	.	−8	8	.	−8	−8	16	8	.	8	16	8	.	−8	.
011000	.	8	8	.	.	8	−8	8	16	.	.	−8	8	.	.	−8
100001	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
100010	.	.	.	.	.	16	16	−16	.	.	.	16	16	16	16	−16
100100	.	−8	−8	8	8	.	−8	.	8	8	.	.	8	−8	.	−8
101000	.	−8	−16	8	−16	16	8	8	.	−8	8	.	.	.	.	.
110000	.	.	.	.	.	.	−8	.	.	.	.	8	−16	24	.	24
000111	.	8	8	16	8	.	.	−8	8	8	−8	24	8	.	−8	.
001011	.	.	−8	−8	16	.	16	.	−8	.	8	16	.	8	8	16
001101	.	.	.	.	.	8	.	.	.	16	.	−8	−8	.	−16	8
001110	.	−8	.	8	8	.	.	−8	−16	8	16	8	−8	−8	.	.
010011	.	8	.	.	.	8	.	16	−8	−16	16	.	−8	.	16	.
010101	.	16	−8	−8	.	8	8	.	8	.	−8	.	8	.	8	.
010110	.	.	−16	8	−8	.	8	−8	16	16	16	−8	−8	8	8	.
011001	.	8	8	.	.	−8	8	8	.	.	.	−8	8	.	.	8
011010	.	.	.	8	.	24	8	8	−24	8	−8	.	8	.	.	.
011100	.	−8	16	−8	.	.	−24	−8	−8	.	−8	.	.	8	8	.
100011	.	.	.	.	.	16	−16	−16	.	.	.	−16	16	−16	16	16
100101	.	−8	8	8	−8	16	−8	16	8	8	16	16	−8	−8	.	8
100110	.	.	.	8	.	16	.	−8	8	−8	−8	.	.	−8	.	.
101001	.	−8	16	8	16	.	8	8	16	−8	8	−16	.	16	.	.
101010	.	−8	8	.	.	−8	.	−8	.	.	16	.	8	−8	.	.
101100	.	.	8	.	−8	.	.	−8	8	−16	−8	.	−8	8	.	24
110001	.	.	.	.	.	.	8	.	.	.	.	−8	16	8	.	8
110010	.	−8	.	.	.	8	.	.	8	−16	−16	.	−8	.	.	.
110100	.	8	.	16	−8	−8	−8	.	8	.	−8	8	.	8	16	.
111000	.	.	−8	8	16	.	8	16	8	.	−24	−8	.	.	8	8
001111	.	8	.	−8	−8	.	.	8	−16	−8	16	−8	8	8	.	.
010111	.	.	.	−8	−8	−16	8	−8	.	.	.	8	−8	−8	8	.
011011	.	.	−16	−8	−16	−8	8	8	8	8	−8	.	8	.	−16	.
011101	.	8	16	8	.	.	−8	8	8	.	8	.	.	−8	−8	.
011110	.	8	.	.	−8	−16	.	16	.	8	8	−8	8	8	8	.
100111	.	16	.	−8	16	.	.	8	−8	8	−8	.	−16	−8	.	.
101011	.	−8	−8	.	16	−8	.	8	.	.	.	.	8	−8	.	.
101101	.	.	−8	.	8	.	.	8	−8	−16	8	.	8	−8	.	8
101110	.	8	8	8	.	8	.	.	8	8	8	.	8	.	.	.
110011	.	−8	.	−16	.	8	.	16	8	16	.	.	−8	.	16	.
110101	.	−8	16	.	−24	−8	8	.	−8	.	−8	8	.	−8	.	.
110110	.	8	8	.	.	.	8	−8	.	16	.	.	.	.	.	.
111001	.	.	−8	8	16	−16	−8	−16	−8	.	8	−8	.	.	8	−8
111010	.	8	.	.	.	.	8	.	.	8	.	.	.	.	8	.
111100	.	8	8	−8	8	8	8	.	.	.	.	8	.	.	−8	.
011111	.	8	.	−16	8	.	.	.	16	−8	8	8	8	−8	8	.
101111	.	24	−8	24	.	−8	.	.	−8	−8	−8	.	−8	.	.	.
110111	.	−24	8	16	16	.	8	8	.	.	.	.	.	.	.	.
111011	.	8	16	−16	16	.	8	.	.	8	.	.	.	.	−8	.
111101	.	−8	24	8	−8	−8	24	.	.	.	.	−8	.	.	8	.
111110	.	−8	−8	−16	.	8	.	−8	8	8	.	.	−8	.	−8	.
111111	.	24	8	.	.	8	.	−8	8	−8	16	.	−8	.	−8	.

Table : $2^6 \cdot \text{bias}_U(a,b)$

Q2$^+$ $|\mathsf{bias}_S(a,b)| \le \frac{24}{64}$ for $a \neq 0$.

Q3$^+$ $\mathsf{bias}_S(\underline{\quad \text{wt } 1 \quad}, \underline{\quad \text{wt } 1 \quad}) = 0$.

Q4$^+$ $|\mathsf{bias}_S(\underline{\quad \text{wt } k \quad}, \underline{\quad \text{wt } \ell \quad})| \le \frac{16}{64}$ when $0 < k + \ell \le 4$.

Q5$^-$ $|\mathsf{bias}_S(a,b_1) \cdot \mathsf{bias}_S(a,b_2)| \le \frac{384}{64^2}$ for all $a \in \mathbb{F}_2^6$, $b_1, b_2 \in \mathbb{F}_2^4$ with $\mathrm{wt}(b_1 + b_2) = 1$.

$\Rightarrow$ Due to Q3$^+$,
if $\mathrm{wt}(a) + \mathrm{wt}(b) < 3$
then $\mathsf{bias}_S(a,b) = 0$,
i.e. $\mathrm{linbranch}(U) = 3$.

$a \setminus b$	0000	0001	0010	0100	1000	0011	0101	0110	1001	1010	1100	0111	1011	1101	1110	1111
000000	64	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
000001	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
000010	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
000100	.	.	.	.	.	.	−8	.	8	8	.	−8	.	.	8	−8
001000	.	.	.	.	.	−8	8	.	8	−8	.	16	8	−16	−8	.
010000	.	.	.	.	.	.	8	.	.	.	.	−8	−16	8	.	−24
100000	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
000011	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
000101	.	.	.	.	.	.	−8	.	−8	8	.	−8	16	16	−24	8
000110	.	−8	−8	.	8	.	.	−8	8	−8	8	8	−8	16	−8	.
001001	.	.	.	.	.	8	8	.	−8	−8	.	.	8	.	−8	.
001010	.	.	8	−8	.	.	−16	16	−8	.	−8	16	.	8	8	−16
001100	.	.	.	.	.	−8	.	.	.	16	.	8	8	.	16	24
010001	.	.	.	.	.	.	−8	.	.	.	.	8	16	24	.	−8
010010	.	8	.	16	.	8	.	.	−8	16	.	.	−8	.	.	.
010100	.	.	−8	8	.	−8	−8	16	8	.	8	16	8	.	−8	.
011000	.	8	8	.	.	8	−8	8	16	.	.	−8	8	.	.	−8
100001	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
100010	.	.	.	.	.	16	16	−16	.	.	.	16	16	16	16	−16
100100	.	−8	−8	8	8	.	−8	.	8	8	.	.	8	−8	.	−8
101000	.	−8	−16	8	−16	16	8	8	.	−8	8	.	.	.	.	.
110000	.	.	.	.	.	.	−8	.	.	.	.	8	−16	24	.	24
000111	.	8	8	16	8	.	.	−8	8	8	−8	24	8	.	−8	.
001011	.	.	−8	−8	16	.	16	.	−8	.	8	16	.	8	8	16
001101	.	.	.	.	.	8	.	.	.	16	.	−8	−8	.	−16	8
001110	.	−8	.	8	8	.	.	−8	−16	8	16	8	−8	−8	.	.
010011	.	8	.	.	.	8	.	16	−8	−16	16	.	−8	.	16	.
010101	.	16	−8	−8	.	8	8	.	8	.	−8	.	8	.	8	.
010110	.	.	−16	8	−8	.	8	−8	16	16	16	−8	−8	8	8	.
011001	.	8	8	.	.	−8	8	8	.	.	.	−8	8	.	.	8
011010	.	.	.	8	.	24	8	8	−24	8	−8	.	8	.	.	.
011100	.	−8	16	−8	.	.	−24	−8	−8	.	−8	.	.	8	8	.
100011	.	.	.	.	.	16	−16	−16	.	.	.	−16	16	−16	16	16
100101	.	−8	8	8	−8	16	−8	16	8	8	16	16	−8	−8	.	8
100110	.	.	.	8	.	16	.	−8	8	−8	−8	.	.	−8	.	.
101001	.	−8	16	8	16	.	8	8	16	−8	8	−16	.	16	.	.
101010	.	−8	8	.	.	−8	.	−8	.	.	16	.	8	−8	.	.
101100	.	.	8	.	−8	.	.	−8	8	−16	−8	.	−8	8	.	24
110001	.	.	.	.	.	.	8	.	.	.	.	−8	16	8	.	8
110010	.	−8	.	.	.	8	.	.	8	−16	−16	.	−8	.	.	.
110100	.	8	.	16	−8	−8	−8	.	8	.	−8	8	.	8	16	.
111000	.	.	−8	8	16	.	8	16	8	.	−24	−8	.	.	8	8
001111	.	8	.	−8	−8	.	.	8	−16	−8	16	−8	8	8	.	.
010111	.	.	.	−8	−8	−16	8	−8	.	.	.	8	−8	−8	8	.
011011	.	.	−16	−8	−16	−8	8	8	8	8	−8	.	8	.	−16	.
011101	.	8	16	8	.	.	−8	8	8	.	8	.	.	−8	−8	.
011110	.	8	.	.	−8	−16	.	16	.	8	8	−8	8	8	8	.
100111	.	16	.	−8	16	.	.	8	−8	8	−8	.	−16	−8	.	.
101011	.	−8	−8	.	16	−8	.	8	.	.	.	.	8	−8	.	.
101101	.	.	−8	.	8	.	.	8	−8	−16	8	.	8	−8	.	8
101110	.	8	8	8	.	8	.	.	8	8	8	.	8	.	.	.
110011	.	−8	.	−16	.	8	.	16	8	16	.	.	−8	.	16	.
110101	.	−8	16	.	−24	−8	8	.	−8	.	−8	8	.	−8	.	.
110110	.	8	8	.	.	.	8	−8	.	16	.	.	.	.	.	.
111001	.	.	−8	8	16	−16	−8	−16	−8	.	8	−8	.	.	8	−8
111010	.	8	.	.	.	.	8	.	.	8	.	.	.	.	8	.
111100	.	8	8	−8	8	8	8	.	.	.	.	8	.	.	−8	.
011111	.	8	.	−16	8	.	.	.	16	−8	8	8	8	−8	8	.
101111	.	24	−8	24	.	−8	.	.	−8	−8	−8	.	−8	.	.	.
110111	.	−24	8	16	16	.	8	8	.	.	.	.	.	.	.	.
111011	.	8	16	−16	16	.	8	.	.	8	.	.	.	.	−8	.
111101	.	−8	24	8	−8	−8	24	.	.	.	.	−8	.	.	8	.
111110	.	−8	−8	−16	.	8	.	−8	8	8	.	.	−8	.	−8	.
111111	.	24	8	.	.	8	.	−8	8	−8	16	.	−8	.	−8	.

Table : $2^6 \cdot \mathsf{bias}_U(a,b)$

Linear properties

Q2$^+$ $|\mathsf{bias}_S(a,b)| \le \frac{24}{64}$ for $a \neq 0$.

Q3$^+$ $\mathsf{bias}_S(\underline{\quad\mathsf{wt}\ 1\quad}, \underline{\quad\mathsf{wt}\ 1\quad}) = 0$.

Q4$^+$ $|\mathsf{bias}_S(\underline{\quad\mathsf{wt}\ k\quad}, \underline{\quad\mathsf{wt}\ \ell\quad})| \le \frac{16}{64}$ when $0 < k + \ell \le 4$.

Q5$^-$ $|\mathsf{bias}_S(a,b_1) \cdot \mathsf{bias}_S(a,b_2)| \le \frac{384}{64^2}$ for all $a \in \mathbb{F}_2^6$, $b_1, b_2 \in \mathbb{F}_2^4$ with $\mathsf{wt}(b_1 + b_2) = 1$.

$\Rightarrow$ Due to Q3$^+$,
if $\mathsf{wt}(a) + \mathsf{wt}(b) < 3$
then $\mathsf{bias}_S(a,b) = 0$,
i.e. $\mathsf{linbranch}(U) = 3$.

$a \setminus b$	0000	0001	0010	0100	1000	0011	0101	0110	1001	1010	1100	0111	1011	1101	1110	1111
000000	64	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
000001	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
000010	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
000100	.	.	.	.	.	.	−8	.	8	8	.	−8	.	.	8	−8
001000	.	.	.	.	.	−8	8	.	8	−8	.	16	8	−16	−8	.
010000	.	.	.	.	.	.	8	.	.	.	.	−8	−16	8	.	−24
100000	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
000011	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
000101	.	.	.	.	.	.	−8	.	−8	8	.	−8	16	16	−24	8
000110	.	−8	−8	.	8	.	.	−8	8	−8	8	8	−8	16	−8	.
001001	.	.	.	.	.	8	8	.	−8	−8	.	.	8	.	−8	.
001010	.	.	8	−8	.	.	−16	16	−8	.	−8	16	.	8	8	−16
001100	.	.	.	.	.	−8	.	.	.	16	.	8	8	.	16	24
010001	.	.	.	.	.	.	−8	.	.	.	.	8	16	24	.	−8
010010	.	8	.	16	.	8	.	.	−8	16	.	.	−8	.	.	.
010100	.	.	−8	8	.	−8	−8	16	8	.	8	16	8	.	−8	.
011000	.	8	8	.	.	8	−8	8	16	.	.	−8	8	.	.	−8
100001	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
100010	.	.	.	.	.	16	16	−16	.	.	.	16	16	16	16	−16
100100	.	−8	−8	8	8	.	−8	.	8	8	.	.	8	−8	.	−8
101000	.	−8	−16	8	−16	16	8	8	.	−8	8	.	.	.	.	.
110000	.	.	.	.	.	.	−8	.	.	.	.	8	−16	24	.	24
000111	.	8	8	16	8	.	.	−8	8	8	−8	24	8	.	−8	.
001011	.	.	−8	−8	16	.	16	.	−8	.	8	16	.	8	8	16
001101	.	.	.	.	.	8	.	.	.	16	.	−8	−8	.	−16	8
001110	.	−8	.	8	8	.	.	−8	−16	8	16	8	−8	−8	.	.
010011	.	8	.	.	.	8	.	16	−8	−16	16	.	−8	.	16	.
010101	.	16	−8	−8	.	8	8	.	8	.	−8	.	8	.	8	.
010110	.	.	−16	8	−8	.	8	−8	16	16	16	−8	−8	8	8	.
011001	.	8	8	.	.	−8	8	8	.	.	.	−8	8	.	.	8
011010	.	.	.	8	.	24	8	8	−24	8	−8	.	8	.	.	.
011100	.	−8	16	−8	.	.	−24	−8	−8	.	−8	.	.	8	8	.
100011	.	.	.	.	.	16	−16	−16	.	.	.	−16	16	−16	16	16
100101	.	−8	8	8	−8	16	−8	16	8	8	16	16	−8	−8	.	8
100110	.	.	.	8	.	16	.	−8	8	−8	−8	.	.	−8	.	.
101001	.	−8	16	8	16	.	8	8	16	−8	8	−16	.	16	.	.
101010	.	−8	8	.	.	−8	.	−8	.	.	16	.	8	−8	.	.
101100	.	.	8	.	−8	.	.	−8	8	−16	−8	.	−8	8	.	24
110001	.	.	.	.	.	.	8	.	.	.	.	−8	16	8	.	8
110010	.	−8	.	.	.	8	.	.	8	−16	−16	.	−8	.	.	.
110100	.	8	.	16	−8	−8	−8	.	8	.	−8	8	.	8	16	.
111000	.	.	−8	8	16	.	8	16	8	.	−24	−8	.	.	8	8
001111	.	8	.	−8	−8	.	.	8	−16	−8	16	−8	8	8	.	.
010111	.	.	.	−8	−8	−16	8	−8	.	.	.	8	−8	−8	8	.
011011	.	.	−16	−8	−16	−8	8	8	8	8	−8	.	8	.	−16	.
011101	.	8	16	8	.	.	−8	8	8	.	8	.	.	−8	−8	.
011110	.	8	.	.	−8	−16	.	16	.	8	8	−8	8	8	8	.
100111	.	16	.	−8	16	.	.	8	−8	8	−8	.	−16	−8	.	.
101011	.	−8	−8	.	16	−8	.	8	.	.	.	.	8	−8	.	.
101101	.	.	−8	.	8	.	.	8	−8	−16	8	.	8	−8	.	8
101110	.	8	8	8	.	8	.	.	8	8	8	.	8	.	.	.
110011	.	−8	.	−16	.	8	.	16	8	16	.	.	−8	.	16	.
110101	.	−8	16	.	−24	−8	8	.	−8	.	−8	8	.	−8	.	.
110110	.	8	8	.	.	.	8	−8	.	16	.	.	.	.	.	.
111001	.	.	−8	8	16	−16	−8	−16	−8	.	8	−8	.	.	8	−8
111010	.	8	.	.	.	.	8	.	.	8	.	.	.	.	8	.
111100	.	8	8	−8	8	8	8	.	.	.	.	8	.	.	−8	.
011111	.	8	.	−16	8	.	.	.	16	−8	8	8	8	−8	8	.
101111	.	24	−8	24	.	−8	.	.	−8	−8	−8	.	−8	.	.	.
110111	.	−24	8	16	16	.	8	8	.	.	.	.	.	.	.	.
111011	.	8	16	−16	16	.	8	.	.	8	.	.	.	.	−8	.
111101	.	−8	24	8	−8	−8	24	.	.	.	.	−8	.	.	8	.
111110	.	−8	−8	−16	.	8	.	−8	8	8	.	.	−8	.	−8	.
111111	.	24	8	.	.	8	.	−8	8	−8	16	.	−8	.	−8	.

Table : $2^6 \cdot \mathsf{bias}_U(a,b)$

Algebraic properties

Definition

An *algebraic relation* is a polynomial $p \in \mathbb{F}_2[x, y] \setminus \{0\}$ such that $p(x, S(x)) = 0$ for all $x \in \mathbb{F}_2^k$.

- Minimal number of independent algebraic relations:

$$\text{dimrel}(U) = [0, 0, 0, 112, 322, \dots].$$

- Thus, optimal graph algebraic immunity

$$AI_{\text{graph}}(U) = 3.$$

- Due to Siegenthaler's inequality optimal multivariate degree

$$AI_{\text{comp}}(U) = 4.$$

Algebraic properties

Definition

An *algebraic relation* is a polynomial $p \in \mathbb{F}_2[x, y] \setminus \{0\}$ such that $p(x, S(x)) = 0$ for all $x \in \mathbb{F}_2^k$.

- Minimal number of independent algebraic relations:

$$\mathsf{dimrel}(U) = [0, 0, 0, 112, 322, \dots].$$

- Thus, optimal graph algebraic immunity

$$AI_{\mathsf{graph}}(U) = 3.$$

- Due to Siegenthaler's inequality optimal multivariate degree

$$AI_{\mathsf{comp}}(U) = 4.$$

Algebraic properties

Definition

An *algebraic relation* is a polynomial $p \in \mathbb{F}_2[x,y] \setminus \{0\}$ such that $p(x, S(x)) = 0$ for all $x \in \mathbb{F}_2^k$.

- Minimal number of independent algebraic relations:

$$\mathsf{dimrel}(U) = [0, 0, 0, 112, 322, \dots].$$

- Thus, optimal graph algebraic immunity

$$AI_{\mathsf{graph}}(U) = 3.$$

- Due to Siegenthaler's inequality optimal multivariate degree

$$AI_{\mathsf{comp}}(U) = 4.$$

Definition

An *algebraic relation* is a polynomial $p \in \mathbb{F}_2[x, y] \setminus \{0\}$ such that $p(x, S(x)) = 0$ for all $x \in \mathbb{F}_2^k$.

- Minimal number of independent algebraic relations:

$$\mathsf{dimrel}(U) = [0, 0, 0, 112, 322, \ldots].$$

- Thus, optimal graph algebraic immunity

$$AI_{\mathsf{graph}}(U) = 3.$$

- Due to Siegenthaler's inequality optimal multivariate degree

$$AI_{\mathsf{comp}}(U) = 4.$$

Comparison

Property	Optimal	U	DESL	DES1	DES2	DES3	DES4	DES5	DES6	DES7	DES8
diffbranch	2?	2	2	2	2	2	2	2	2	2	2
linbranch	3?	3	2	2	2	2	2	2	2	2	2
AI_{graph}	3	3	2	2	3	3	2	2	3	3	3
AI_{comp}	5	4	4	4	4	4	3	4	5	5	4

Outline

Preliminaries

Properties

Applications to DESL

Summary

Independence assumption

Assumption

Round-keys and thus the bias of different rounds are independent.

$\Rightarrow$ No assumption on independence of the bias of adjacent S-boxes!

Approximations of the DES(L) round function

Lemma

Given $E\colon \mathbb{F}_2^{\ell_1} \to \mathbb{F}_2^{\ell_2}$ *injective, linear;* $F\colon \mathbb{F}_2^{\ell_2} \to \mathbb{F}_2^{\ell_3}$ *arbitrary. Then*

$$\mathsf{bias}_{F\circ E}(a,b) = \sum_{E^\vee d = a} \mathsf{bias}_F(d,b).$$

Corollary

For the DES round function $F_k = P \circ S^8 \circ \Sigma_k \circ E$ *we have*

$$\mathsf{bias}_{F_k}(a,b) = \sum_{E^\vee d = a} (-1)^{\langle d \,|\, k\rangle} \prod_i \mathsf{bias}_{S_i}(d_i, (P^{-1}b)_i).$$

Lemma (Patching)

Assume that there are 2^ℓ *selectors* d *with* $E^\vee d = a$ *and assume* $|\mathsf{bias}_{S_i}(d_i, b_i)| \le \varepsilon_i$. *Then* $|\mathsf{bias}_{F_k}(a,b)| \le 2^\ell \prod_i \varepsilon_i$.

Approximations of the DES(L) round function

Lemma

Given $E\colon \mathbb{F}_2^{\ell_1} \to \mathbb{F}_2^{\ell_2}$ *injective, linear;* $F\colon \mathbb{F}_2^{\ell_2} \to \mathbb{F}_2^{\ell_3}$ *arbitrary. Then*

$$\mathsf{bias}_{F \circ E}(a, b) = \sum_{E^\vee d = a} \mathsf{bias}_F(d, b).$$

Corollary

For the DES round function $F_k = P \circ S^8 \circ \Sigma_k \circ E$ *we have*

$$\mathsf{bias}_{F_k}(a, b) = \sum_{E^\vee d = a} (-1)^{\langle d \,|\, k \rangle} \prod_i \mathsf{bias}_{S_i}(d_i, (P^{-1} b)_i).$$

Lemma (Patching)

Assume that there are 2^ℓ *selectors* d *with* $E^\vee d = a$ *and assume* $|\mathsf{bias}_{S_i}(d_i, b_i)| \leq \varepsilon_i$. *Then* $|\mathsf{bias}_{F_k}(a, b)| \leq 2^\ell \prod_i \varepsilon_i$.

Approximations of the DES(L) round function

Lemma

Given $E\colon \mathbb{F}_2^{\ell_1} \to \mathbb{F}_2^{\ell_2}$ *injective, linear;* $F\colon \mathbb{F}_2^{\ell_2} \to \mathbb{F}_2^{\ell_3}$ *arbitrary. Then*

$$\mathsf{bias}_{F \circ E}(a, b) = \sum_{E^\vee d = a} \mathsf{bias}_F(d, b).$$

Corollary

For the DES round function $F_k = P \circ S^8 \circ \Sigma_k \circ E$ *we have*

$$\mathsf{bias}_{F_k}(a, b) = \sum_{E^\vee d = a} (-1)^{\langle d \,|\, k \rangle} \prod_i \mathsf{bias}_{S_i}(d_i, (P^{-1} b)_i).$$

Lemma (Patching)

Assume that there are 2^ℓ *selectors* d *with* $E^\vee d = a$ *and assume* $|\mathsf{bias}_{S_i}(d_i, b_i)| \leq \varepsilon_i$. *Then* $|\mathsf{bias}_{F_k}(a, b)| \leq 2^\ell \prod_i \varepsilon_i$.

Consequences

Conjecture

With S-box U, there is no relevant linear approximation.

Theorem

With S-box U, there is no relevant iterative approximation with at most ten active S-boxes.

- Problem: Bounds from the patching lemma are too weak.
- Complete proof: run a dedicated computer program.
  (111 CPU days / Intel(R) Xeon(TM) CPU 3.00GHz.)

Consequences

Conjecture

With S-box U, there is no relevant linear approximation.

Theorem

With S-box U, there is no relevant iterative approximation with at most ten active S-boxes.

- Problem: Bounds from the patching lemma are too weak.
- Complete proof: run a dedicated computer program.
  (111 CPU days / Intel(R) Xeon(TM) CPU 3.00GHz.)

Consequences

Conjecture

With S-box U, there is no relevant linear approximation.

Theorem

With S-box U, there is no relevant iterative approximation with at most ten active S-boxes.

- Problem: Bounds from the patching lemma are too weak.
- Complete proof: run a dedicated computer program.
  (111 CPU days / Intel(R) Xeon(TM) CPU 3.00GHz.)

Consequences

Conjecture

With S-box U, there is no relevant linear approximation.

Theorem

With S-box U, there is no relevant iterative approximation with at most ten active S-boxes.

- Problem: Bounds from the patching lemma are too weak.
- Complete proof: run a dedicated computer program.
  (111 CPU days / Intel(R) Xeon(TM) CPU 3.00GHz.)

Outline

Preliminaries

Properties

Applications to DESL

Summary

Summary

New S-box U and family:

- Considerable improvement of the linear properties.
- Algebraic properties better than before.
- Good differential properties as before.

Applications to DESL:

- No iterative linear approximations with ≤ 10 active S-boxes.
- Still many open questions.

Summary

New S-box U and family:

- Considerable improvement of the linear properties.
- Algebraic properties better than before.
- Good differential properties as before.

Applications to DESL:

- No iterative linear approximations with ≤ 10 active S-boxes.
- Still many open questions.

Thank you!

$efgh$	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$U(0efgh0)$	0	9	7	2	B	E	C	5	3	F	D	8	4	1	A	6
$U(0efgh1)$	B	6	8	F	2	1	5	C	D	A	E	3	7	4	0	9
$U(1efgh0)$	E	4	8	D	2	7	1	B	5	A	6	3	9	C	F	0
$U(1efgh1)$	1	D	4	2	F	8	A	7	6	0	9	5	C	B	3	E