

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

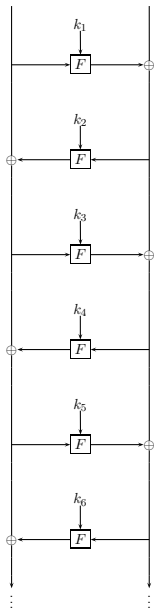
Daniel Loebenberger Michael Nüsken

Bonn-Aachen International Center for Information Technology

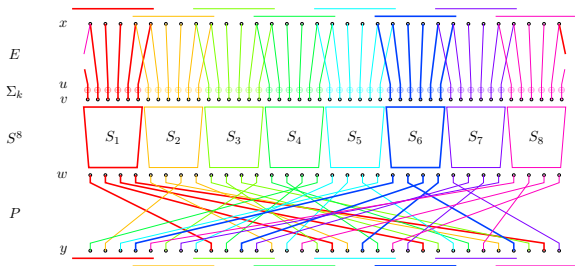
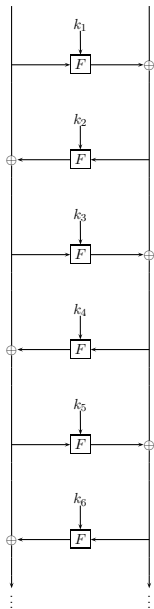
YACC 2014, 11 June 2014



From DES to DESL+

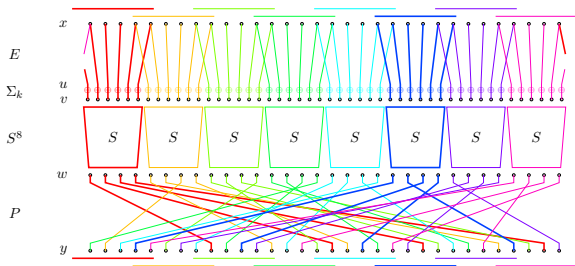
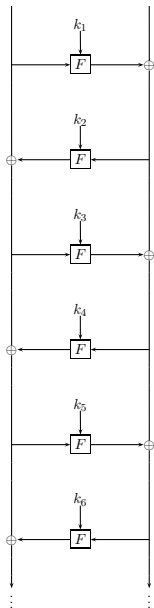


From DES to DESL+



DES round function

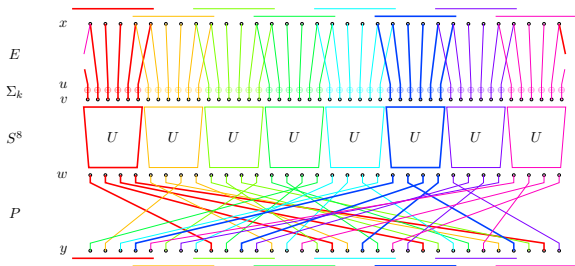
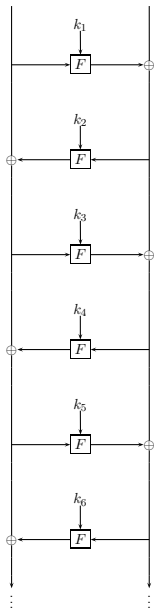
From DES to DESL+



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

Preliminaries

Properties

Applications to DESL

Summary

Preliminaries

Properties

Applications to DESL

Summary

S-boxes: Differential probabilities and bias

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

Definition (Differential probability)

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

Definition (Bias)

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

S-boxes: Differential probabilities and bias

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

Definition (Differential probability)

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

Definition (Bias)

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

S-boxes: Differential probabilities and bias

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

Definition (Differential probability)

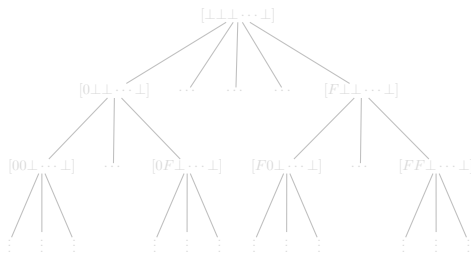
$$\begin{aligned} \text{diff}_S(\Delta x \rightarrow \Delta y) &= \text{prob}(S(X) \oplus S(X \oplus \Delta x) = \Delta y) \\ &= \frac{1}{2^k} \# \left\{ x \in \mathbb{F}_2^k \mid S(x) \oplus S(x \oplus \Delta x) = \Delta y \right\} \\ &\in [0, 1] \end{aligned}$$

Definition (Bias)

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

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!

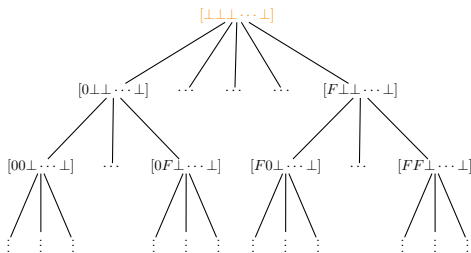
Split into manageable tasks, by cutting the tree at a certain level.
We used level 18, leading to 937 140 subtrees to consider.

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!

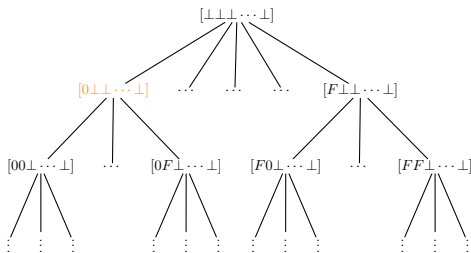
Split into manageable tasks, by cutting the tree at a certain level.
We used level 18, leading to 937 140 subtrees to consider.

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!

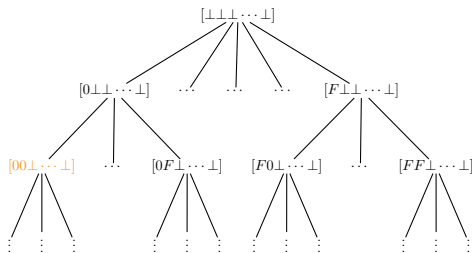
Split into manageable tasks, by cutting the tree at a certain level.
We used level 18, leading to 937 140 subtrees to consider.

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!

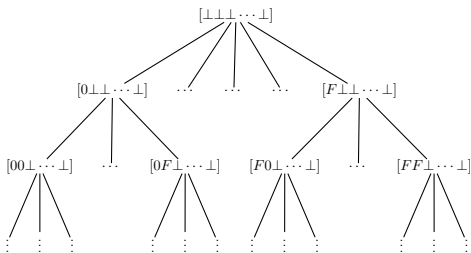
Split into manageable tasks, by cutting the tree at a certain level.
We used level 18, leading to 937 140 subtrees to consider.

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!

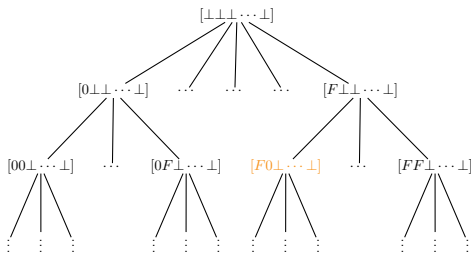
Split into manageable tasks, by cutting the tree at a certain level.
We used level 18, leading to 937 140 subtrees to consider.

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!

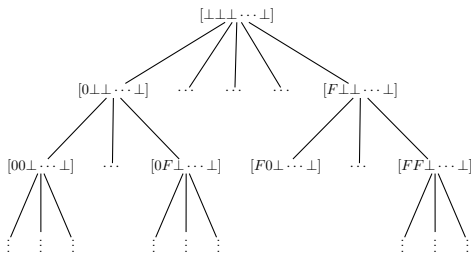
Split into manageable tasks, by cutting the tree at a certain level.
We used level 18, leading to 937 140 subtrees to consider.

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!

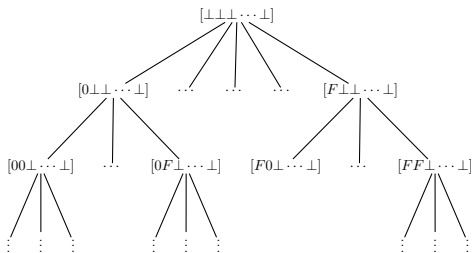
Split into manageable tasks, by cutting the tree at a certain level.
We used level 18, leading to 937 140 subtrees to consider.

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!

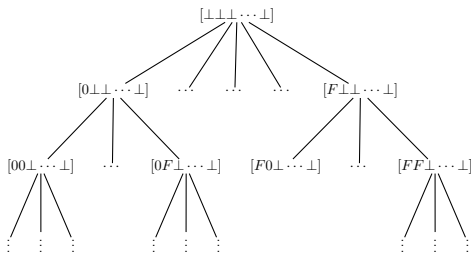
Split into manageable tasks, by cutting the tree at a certain level.
We used level 18, leading to 937 140 subtrees to consider.

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!

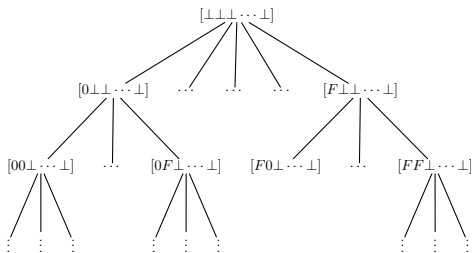
Split into manageable tasks, by cutting the tree at a certain level.
We used level 18, leading to 937 140 subtrees to consider.

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!

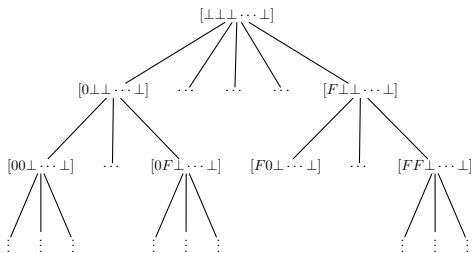
Split into manageable tasks, by cutting the tree at a certain level.
We used level 18, leading to 937 140 subtrees to consider.

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!

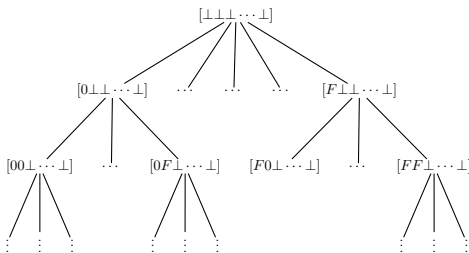
Split into manageable tasks, by cutting the tree at a certain level.
We used level 18, leading to 937 140 subtrees to consider.

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.

Preliminaries

Properties

Applications to DESL

Summary

Differential properties

$\Delta x \setminus \Delta y$	0000	0001	0010	0011	0100	0101	0110	1000	1001	1010	1011	1100	1101	1110	1111
000000	64	-	-	-	-	-	-	-	-	-	-	-	-	-	-
000001	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
000010	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
0000100	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
0010000	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
0100000	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
1000000	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
0000011	8	4	6	-	4	8	4	10	4	10	4	-	-	-	2
000010	8	-	8	6	6	6	6	-	4	2	4	6	-	-	4
0000100	-	-	12	8	8	8	8	-	-	-	-	-	-	-	4
0010001	2	6	6	6	4	2	8	2	6	6	4	-	-	-	4
0010010	-	-	10	4	2	8	-	6	8	4	6	4	4	4	4
0010000	-	-	-	-	-	-	-	-	10	16	16	8	2	4	8
0100001	2	6	4	6	6	2	6	4	4	4	8	6	-	-	2
010010	12	-	12	-	-	-	-	4	-	8	4	-	12	-	4
010100	4	8	4	16	-	8	4	-	-	-	4	8	-	8	-
0110000	4	4	4	12	2	-	4	2	-	4	10	4	10	4	2
1000001	10	2	6	8	10	2	4	6	4	2	2	2	-	-	2
1000100	-	-	2	4	6	-	-	4	16	8	6	4	2	8	8
1001000	-	-	2	8	10	8	4	4	4	4	8	4	-	-	2
1010000	-	-	10	6	6	4	4	2	4	4	6	6	2	4	6
1100000	-	-	8	6	-	2	4	8	8	-	8	4	2	4	6
000011	6	10	-	4	-	2	8	2	4	-	6	8	2	6	2
000101	2	2	-	2	8	4	2	6	6	4	2	6	6	4	4
000110	6	2	2	4	2	10	10	16	2	8	6	4	6	-	4
010011	2	2	4	10	6	6	8	2	4	4	2	2	4	2	2
010101	6	10	-	-	8	2	-	2	2	4	-	-	8	8	6
010110	-	-	12	12	12	12	-	-	-	-	-	-	-	-	8
011001	-	-	4	10	8	6	2	-	4	2	2	2	8	6	2
011010	-	-	12	10	4	10	-	-	2	-	4	2	-	8	4
011100	-	-	8	4	8	4	6	8	8	2	4	4	2	4	2
100011	2	4	-	2	4	10	4	10	4	2	4	2	4	4	10
100010	4	2	-	4	4	6	2	6	8	6	-	-	4	14	4
10010	4	2	2	2	2	2	6	8	2	6	-	-	2	6	6
101001	-	-	10	4	6	2	8	4	6	4	4	2	2	-	4
101010	12	2	2	2	2	2	8	4	6	4	2	2	8	4	2
101100	-	-	12	10	8	2	6	4	4	2	-	-	4	-	4
110001	2	4	6	-	-	4	4	4	6	4	6	4	6	2	10
110010	8	4	-	4	-	6	-	2	2	4	6	12	8	4	-
110100	-	-	6	6	2	8	6	2	6	4	2	2	2	2	6
111000	-	-	6	8	10	4	2	4	4	6	4	2	6	2	2
001111	8	-	2	2	2	2	2	2	6	6	6	8	2	4	2
010111	-	-	6	6	6	4	-	2	-	2	4	10	10	4	6
011011	-	-	8	10	8	2	2	6	2	2	2	2	2	10	8
011101	8	4	2	2	-	2	2	6	4	2	2	2	6	10	6
011110	-	-	12	2	4	2	8	-	10	-	4	2	-	4	-
100011	4	4	6	6	-	2	-	8	2	8	8	2	2	4	8
101011	2	6	6	2	8	10	6	6	-	6	-	4	2	2	6
10110	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
110101	8	4	6	2	10	2	6	2	2	-	6	6	6	6	8
110110	8	2	4	2	4	4	-	4	4	4	4	4	2	4	4
111001	4	-	4	6	4	2	4	-	2	2	8	8	2	4	10
111010	8	2	4	2	-	2	8	4	6	4	4	6	2	6	2
111100	-	-	4	4	12	4	2	2	4	6	2	4	2	6	4
011111	6	6	4	6	4	2	2	2	6	4	4	4	4	4	2
101111	4	6	6	2	2	2	2	4	8	4	4	4	-	8	-
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
111110	8	-	-	-	12	4	8	6	4	8	2	2	4	2	4
111111	-	-	4	-	6	-	2	6	6	6	4	6	12	4	-

Coppersmith, 1994:

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

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

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

S-5 $\text{diff}_S(0011100 \rightarrow \underline{\text{wt } \leq 1}) = 0$.

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

Kim, Lee, Park & Lee, 1995:

Q1 $\text{diff}_S(1***00 \rightarrow 0000) = 0$

\Rightarrow Due to S-4,

if $\text{wt}(\Delta x) + \text{wt}(\Delta y) < 2$
then $\text{diff}_S(\Delta x \rightarrow \Delta y) = 0$,
i.e. $\text{diffbranch}(U) = 2$.

Table: $2^6 \cdot \text{diff}_f(\Delta x \rightarrow \Delta y)$

Differential properties

$\Delta x \setminus \Delta y$	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
000000	04
000001
000010
0000100
0010000
0100000
1000000
0000011	8	4	6	.	4	8	4	10	4	10	4	2
0000101	8	.	8	6	6	6	.	4	2	4	6	2
0000110	.	.	12	4	8	8	12
0010001	2	6	6	6	4	2	8	2	6	6	4	2
0010010	.	.	10	4	2	8	.	6	8	4	6	4	4	4	4	2
0011000	10	16	16	8	2	4	2	8
0100001	2	6	4	6	6	2	6	4	4	4	8	6	.	.	.	2
0100100	.	12	.	12	4	.	8	4	.	12	.	4
0101000	.	4	8	4	16	.	8	4	.	.	4	8	.	8	.	.
1000001	10	2	6	8	10	2	4	6	4	2	2	2
1000100	.	.	2	4	6	.	.	.	4	16	8	6	4	2	8	8
1001000	.	2	8	10	8	4	4	4	4	8	4	2
1010000	.	10	6	6	6	4	4	2	4	4	6	8	2	4	2	8
1100000	.	8	6	.	2	4	8	8	.	8	4	2	4	6	4	.
0000111	6	10	.	4	.	2	8	2	4	.	6	8	2	6	2	4
0001011	2	2	.	2	8	4	2	6	6	4	2	6	6	4	4	6
0001101	6	2	2	4	2	10	10	8	4	6	4	6
0100111	2	2	4	10	6	6	8	2	4	4	2	2	4	2	2	4
0101011	6	10	.	.	8	2	.	2	2	4	.	8	8	6	8	.
0101101	.	12	12	12	12
0110001	4	10	8	6	2	.	4	2	2	2	.	8	6	2	4	4
0110101	.	12	10	4	10	.	.	2	.	4	2	.	8	4	8	.
0111000	.	8	4	8	4	6	8	2	4	4	2	4	4	2	.	8
1000111	2	4	.	2	6	10	4	2	6	10	4	4	4	10	.	8
1000101	2	2	.	4	4	6	2	6	8	6	6	.	14	4	.	4
1001010	4	2	2	2	2	6	8	2	6	.	2	6	6	6	6	4
1010001	.	10	4	6	2	8	4	6	4	4	2	2	.	4	4	4
1010101	12	2	2	2	2	6	2	6	4	2	2	8	4	2	8	4
1011000	.	12	10	8	2	6	4	4	2	.	4	4
1100001	2	4	6	.	4	4	4	6	4	6	4	6	2	10	2	2
1100101	8	4	.	4	.	6	.	2	2	4	6	12	8	4	.	4
1101000	.	6	6	2	8	6	2	6	4	2	2	6	4	2	2	6
1110000	.	6	8	10	4	2	4	4	6	4	4	2	6	2	2	2
0011111	8	.	2	2	.	2	2	6	6	6	8	2	4	2	4	10
0101111	.	6	6	6	4	.	2	.	2	4	10	10	4	6	4	.
0110111	.	10	8	8	2	2	6	2	2	2	2	2	10	8	2	.
0111011	8	4	2	2	.	2	2	6	4	2	2	2	6	10	6	6
0111101	.	12	2	4	2	8	.	10	.	4	2	.	4	.	8	8
1000111	4	4	6	6	.	2	.	8	2	8	8	2	2	4	8	8
1010111	2	6	2	2	8	10	6	8	10	6	8	6	8	2	6	10
1011011	16	4	2	.	6	6	4	4	2	4	2	.	4	4	4	4
1100111	6	2	6	2	4	6	2	4	4	.	6	.	8	2	8	4
1101011	8	4	4	.	2	10	2	2	2	.	6	6	6	8	2	8
1101101	8	2	4	2	4	4	.	4	4	4	4	4	2	4	10	8
1110001	4	.	4	6	4	2	4	.	2	2	8	8	2	4	4	10
1110101	8	2	4	2	.	2	8	4	6	4	4	6	2	6	2	4
1111000	.	4	4	12	.	4	4	2	4	2	4	2	4	2	4	8
0111111	6	6	4	.	6	4	.	2	2	6	4	6	4	4	4	2
1011111	4	6	6	6	2	2	2	2	4	8	4	4	.	8	.	6
1101111	8	2	8	2	2	2	8	.	8	4	2	6	6	4	2	.
1110111	6	4	6	2	10	2	4	2	6	8	2	2	6	8	2	2
1111011	6	4	6	6	2	6	2	4	6	2	4	2	8	2	2	2
1111101	8	.	.	.	12	4	8	6	4	8	2	2	4	2	4	.
1111111	.	4	.	6	.	2	6	6	6	4	6	12	4	.	6	2

Table : $2^6 \cdot \text{diff}_f(\Delta x \rightarrow \Delta y)$

Coppersmith, 1994:

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

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

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

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

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

Kim, Lee, Park & Lee, 1995:

Q1 $\text{diff}_S(1***00 \rightarrow 0000) = 0$

\Rightarrow Due to S-4,

if $\text{wt}(\Delta x) + \text{wt}(\Delta y) < 2$

then $\text{diff}_S(\Delta x \rightarrow \Delta y) = 0,$

i.e. $\text{diffbranch}(U) = 2.$

Differential properties

$\Delta x \setminus \Delta y$	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
000000	04
000001
000010
0000100
0010000
0100000
1000000
0000011	8	4	6	.	4	8	4	10	4	10	4	2
0000101	8	.	8	6	6	6	.	4	2	4	6	2
0000110	.	.	12	4	8	8	2
0010001	2	6	6	6	4	2	8	2	6	6	4	2
0010100	.	.	10	4	2	8	.	6	8	4	6	2
0011000	10	16	16	2
0100001	2	6	4	6	6	2	6	4	4	4	8	6	.	.	.	2
0100100	.	12	.	12	4	.	8	4	.	.	.	4
0101000	.	4	8	4	16	.	8	4	.	.	4	8	.	.	.	8
0110000	4	4	4	12	2	.	4	2	.	.	4	10	4	.	.	2
1000001	10	2	6	8	10	2	4	6	4	2	2	2
1000100	.	.	2	4	6	.	.	.	4	16	8	6	4	.	.	2
1001000	.	2	8	10	8	4	4	4	4	8	4	2
1010000	10	6	6	6	4	4	2	4	4	6	2
1100000	.	8	6	.	2	4	8	8	.	8	4	2
0000111	6	10	.	4	.	2	8	2	4	.	6	8	2	6	2	4
0001011	2	2	.	2	8	4	2	6	6	4	2	6	6	4	4	6
0001101	6	2	2	4	2	10	10	8	4	6	4	6	.	.	.	4
0001110	.	2	4	2	4	16	2	8	8	8	4	4	.	.	.	4
0100111	2	2	4	10	6	6	8	2	4	4	2	2	4	2	2	4
0100101	6	10	.	.	8	2	.	2	2	4	8
0100110	.	12	12	12	12	8
0110001	4	10	8	6	2	.	4	2	2	2	4
0110100	.	12	10	4	10	.	.	2	.	4	2	8
0111000	8	4	8	4	6	8	2	2	4	4	8
1000011	2	4	.	2	6	10	4
1000101	2	2	4	4	6	2	6	8	6	4
1000110	4	2	2	2	2	6	8	2	6	6
1010001	.	10	4	2	2	8	4	6	4	4	2	2	.	.	.	4
1010100	12	2	2	2	2	6	2	6	4	2	2
1011000	12	10	8	2	6	4	4	2	4
1100001	2	4	6	.	.	4	4	4	6	4	6	4	.	.	.	2
1100010	8	4	.	4	.	6	.	2	2	4	6	12	8	4	.	4
1100100	2	6	6	2	6	6	2	6	4	2	2
1110000	.	6	8	10	4	2	4	4	6	4	2
0011111	8	.	2	2	.	2	2	6	6	6	8	2	4	2	4	10
0101111	.	6	6	6	4	.	2	.	2	4	10	10	4	6	4	6
0110111	.	10	8	2	2	6	2	2	2	2	2	10	8	2	6	2
0111011	8	4	2	2	.	2	2	6	4	2	2	2	6	10	6	6
0111101	.	12	2	4	2	8	.	10	.	4	2	.	4	.	.	8
1000111	4	4	6	6	.	2	.	8	2	8	8	2	2	4	8	8
1010111	2	6	6	2	6	10	6	8	10	6	10
1011011	2	6	2	2	8	4	2	2	.	12	6	4	2	6	2	4
1011101	16	4	2	.	6	6	4	4	2	.	4	4	4	4	.	4
1100111	6	2	6	2	4	6	2	4	4	.	6	.	8	2	8	4
1100101	8	4	4	.	2	10	.	2	.	2	.	.	6	6	8	2
1101011	8	2	4	2	4	4	.	4	4	4	.	.	4	2	4	8
1110001	4	.	4	6	4	2	4	.	2	2	8	8	2	4	10	8
1110100	8	2	4	2	.	2	8	4	6	4	4	6	2	6	2	4
1111000	4	4	4	12	.	4	4	2	4	2	8
0111111	6	6	4	.	6	4	.	2	2	6	4	6	4	4	4	2
1011111	4	6	6	6	2	2	2	2	4	8	4	4	.	8	.	6
1101111	8	2	8	2	2	2	8	.	8	4	2	6	6	4	2	.
1110111	6	4	6	2	10	2	4	2	6	8	2	2	6	2	2	2
1111011	6	4	6	6	2	6	2	4	6	2	4	2	8	2	2	2
1111101	8	.	.	.	12	4	8	6	4	8	2	2	4	2	4	.
1111111	.	4	.	6	.	2	6	6	6	4	6	12	4	.	6	2

Table: $2^6 \cdot \text{diff}_f(\Delta x \rightarrow \Delta y)$

Coppersmith, 1994:

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

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

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

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

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

Kim, Lee, Park & Lee, 1995:

Q1 $\text{diff}_S(1***00 \rightarrow 0000) = 0$

\Rightarrow Due to S-4,

if $\text{wt}(\Delta x) + \text{wt}(\Delta y) < 2$
then $\text{diff}_S(\Delta x \rightarrow \Delta y) = 0$,
i.e. $\text{diffbranch}(U) = 2$.

Differential properties

$\Delta x \setminus \Delta y$	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
000000	04
000001
000010
0000100
0010000
0100000
1000000
0000011	8	4	6	.	4	8	4	10	4	10	4
0000101	8	.	8	6	6	6	6	.	4	2	4	6
0000110	.	.	12	4	8	8	8
0010001	2	6	6	6	4	2	8	2	6	6	4
0010010	.	.	10	4	2	8	.	6	8	4	6	4	4	4	4	4
0011000	.	.	6	6	4	2	4	10	16	16	6	2	4	2	8	8
0100001	2	6	4	6	6	2	6	4	4	4	8	6
0100100	.	12	.	12	4	.	8	4	.	12	.	4
0101000	.	4	8	4	16	.	8	4	.	.	4	8	.	8	.	.
1000001	10	2	6	8	10	2	4	6	4	2	2
1000100	.	.	2	4	6	.	.	.	4	16	8	6	4	2	8	8
1001000	.	2	8	10	8	4	4	4	4	8	4
1010000	10	6	6	6	4	4	2	4	4	6	6	2	4	2	8	8
1100000	.	8	6	.	2	4	8	8	.	8	4	2	4	6	4	.
0000111	6	10	.	4	.	2	8	2	4	.	6	8	2	6	2	4
0001011	2	2	.	2	8	4	2	6	6	4	2	6	6	4	4	6
0001101	6	2	4	2	4	8	10	10	8	4	6	4	6	.	.	.
0001110	.	2	4	2	4	16	2	8	8	8	4	4	4	.	.	.
0100111	2	2	4	10	6	6	8	2	4	4	2	2	4	2	2	4
0101011	6	10	.	.	8	2	.	2	2	4	.	8	8	6	8	.
0101100	.	12	12	12	12
0110001	4	10	8	6	2	.	4	2	2	2	.	8	6	2	4	4
0110100	.	12	10	4	10	.	.	.	2	.	4	2	.	8	4	8
0111000	.	8	4	8	4	6	8	2	4	4	2	4	4	2	.	.
1000011	2	4	.	2	4	6	10	4	2	.	4	4	10	.	.	.
1000101	2	2	4	4	6	2	6	8	6	6	.	4	14	4	.	.
1000110	4	2	2	2	2	6	8	2	6	.	2	6	6	6	6	4
1010001	.	10	4	2	2	8	4	6	4	4	2	2	.	4	4	4
1010100	12	2	2	2	2	4	6	2	6	4	2	2	8	4	2	8
1011000	12	10	8	2	6	4	4	2	.	4	.	4
1100001	2	4	6	.	4	4	4	6	4	6	4	6	2	10	2	2
1100010	8	4	.	.	6	.	2	2	4	6	12	8	4	.	.	.
1101000	2	6	6	2	6	6	2	6	4	2	2	2	2	2	2	6
1110000	.	6	8	10	4	2	4	4	6	4	4	2	6	2	2	2
0011111	8	.	2	2	.	2	2	6	6	6	8	2	4	2	4	10
0101111	.	6	6	6	4	.	2	.	2	4	10	10	4	6	4	.
0110111	.	10	8	8	.	2	6	2	2	2	2	10	8	2	.	.
0111011	8	4	2	2	.	2	2	6	4	2	2	2	6	10	6	6
0111100	.	12	2	4	2	8	.	10	.	4	2	.	4	.	8	8
1000111	4	4	6	6	.	2	.	8	2	8	8	2	2	4	8	2
1010111	2	6	6	2	6	8	10	6	8	6	8	6	2	2	6	10
1011011	2	6	2	2	8	4	2	2	.	12	6	4	2	6	2	4
1011100	16	4	2	.	6	6	4	4	2	.	4	4	4	4	.	4
1100011	6	2	6	2	4	6	2	4	4	.	6	.	8	2	8	4
1100101	8	4	6	.	2	10	.	2	2	.	6	.	6	8	8	2
1100110	8	2	4	2	4	4	.	4	4	4	4	4	2	4	10	8
1110001	4	.	4	6	4	2	4	.	2	2	8	8	2	4	4	10
1110010	8	2	4	2	.	2	8	4	6	4	4	6	2	6	2	4
1111000	2	4	4	12	.	4	4	2	4	4	2	4	2	4	4	8
0111111	6	6	4	.	6	4	2	2	6	4	6	4	4	4	4	2
1011111	4	6	6	6	2	2	2	2	4	8	4	4	.	8	.	6
1101111	8	2	8	2	2	2	8	.	8	4	2	6	6	4	2	.
1110111	6	4	6	2	10	2	4	2	6	8	2	2	6	8	2	2
1111011	6	4	6	6	2	6	2	4	6	2	4	2	8	2	2	2
1111100	8	.	.	.	12	4	8	6	4	8	2	2	4	2	4	.
1111111	.	4	.	6	.	2	6	6	6	4	6	12	4	.	6	2

Table : $2^6 \cdot \text{diff}_f(\Delta x \rightarrow \Delta y)$

Coppersmith, 1994:

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

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

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

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

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

Kim, Lee, Park & Lee, 1995:

Q1 $\text{diff}_S(1***00 \rightarrow 0000) = 0$

\Rightarrow Due to S-4,

if $\text{wt}(\Delta x) + \text{wt}(\Delta y) < 2$

then $\text{diff}_S(\Delta x \rightarrow \Delta y) = 0$,

i.e. $\text{diffbranch}(U) = 2$.

Linear properties

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

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

$$Q4^+ \quad \left| \text{bias}_S\left(\frac{\text{wt } k}{\text{wt } k}, \frac{\text{wt } \ell}{\text{wt } \ell}\right) \right| \leq \frac{16}{64}$$

when $0 < k + \ell \leq 4$.

$$Q5^- \quad |\text{bias}_S(a, b_1) \cdot \text{bias}_S(a, b_2)| \leq \frac{384}{64^2}$$

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 \ b	0000	0001	0010	0100	1000	0011	0101	0110	1001	1010	1100	0111	1011	1101	1110	1111
00000	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
00001	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
00010	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
00100	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
01000	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10000	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
00011	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
00101	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
01010	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10100	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
00111	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
01101	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10110	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
11010	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
11001	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10011	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10101	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10111	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
11011	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
11101	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
11110	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
11111	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

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

Linear properties

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

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

$$Q4^+ \quad \left| \text{bias}_S\left(\frac{\text{wt } k}{\text{wt } k}, \frac{\text{wt } \ell}{\text{wt } \ell}\right) \right| \leq \frac{16}{64}$$

when $0 < k + \ell \leq 4$.

$$Q5^- \quad |\text{bias}_S(a, b_1) \cdot \text{bias}_S(a, b_2)| \leq \frac{384}{64^2}$$

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 \ b	0000	0001	0010	0100	1000	0011	0101	0110	1001	1010	1100	0111	1011	1101	1110	1111
000000	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
000001	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
000010	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
000100	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
010000	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
100000	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
000011	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
000110	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
010010	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
001010	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
001100	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
010001	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
010010	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
010100	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
100001	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
100010	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
101000	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
110000	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
000111	8	8	16	8	0	0	-8	8	8	-8	0	24	8	0	-8	16
001011	0	-8	-8	16	0	16	-8	-8	0	8	16	0	8	8	8	16
001110	-8	0	8	8	0	8	-8	-16	8	16	-8	-8	-8	-16	8	0
010011	8	0	0	0	0	8	16	-8	-16	16	0	-8	0	-16	0	0
010101	16	-8	-8	-8	0	8	8	8	0	-8	0	8	8	8	8	16
010110	0	-16	8	-8	0	8	-8	-16	16	16	0	-8	8	8	8	0
011001	8	8	0	0	0	-24	8	8	-24	8	-8	-8	8	0	0	8
011010	-8	16	-8	0	0	-24	-8	-8	0	-8	0	-8	8	8	8	16
100011	0	0	0	0	0	16	-16	-16	0	0	-16	16	-16	16	16	16
100101	-8	8	8	-8	0	16	-8	16	8	8	16	16	-8	-8	8	0
100110	0	0	0	0	0	16	-8	-8	-8	-8	0	0	-8	0	0	0
101001	-8	16	8	16	0	8	8	16	-8	8	-16	-8	8	8	8	16
101010	-8	8	8	0	0	-8	8	-8	8	16	8	-8	8	-8	8	0
101100	0	0	0	-8	0	0	-8	8	-16	-8	0	-8	8	8	24	8
110001	0	0	0	0	0	8	0	0	0	0	0	-8	16	8	0	8
110010	-8	0	0	0	0	8	0	8	-16	-16	0	-8	0	8	16	0
110100	8	8	16	-8	0	-8	-8	8	0	-8	0	8	8	8	16	0
111000	0	-8	8	16	0	8	16	8	-24	-24	-8	-8	8	8	8	8
001111	8	0	-8	-8	0	0	8	-16	-8	8	-8	8	8	8	0	0
010111	0	-16	-8	-8	0	-16	8	-8	0	8	-8	8	-8	8	8	0
011011	8	16	8	0	0	-8	8	8	8	8	0	0	-8	-8	-8	0
011110	8	0	0	-8	0	-16	16	0	8	8	-8	8	8	8	8	0
000111	16	0	-8	16	0	0	8	-8	8	-8	0	-16	-8	0	0	0
001011	-8	-8	-8	16	0	-8	8	-8	-16	8	0	8	-8	-8	0	0
001101	0	-8	8	8	0	0	-8	-8	-16	8	0	8	-8	-8	8	8
010110	8	8	8	0	0	8	0	8	8	8	8	8	8	0	0	0
010011	-8	8	-16	8	0	8	16	8	16	0	0	-8	0	-16	0	0
010101	-8	16	0	-24	0	-8	8	8	8	8	-8	8	8	-8	0	0
010110	8	8	0	0	0	8	-8	-8	-16	8	0	-8	0	0	0	0
110001	0	-8	8	16	0	-16	-8	-16	-8	8	0	-8	0	8	-8	0
110010	8	0	0	0	0	8	0	0	8	0	0	0	0	0	0	0
110100	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8
111000	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8
011111	8	0	-16	8	0	-8	0	-16	-8	8	8	8	-8	8	0	0
101111	24	-8	24	0	0	-8	0	-8	-8	-8	0	-8	0	0	0	0
110111	-24	8	16	16	0	8	8	0	0	0	0	0	0	0	0	0
111011	8	16	-16	16	0	8	8	8	8	8	8	8	8	-8	-8	0
111101	-8	24	8	-8	0	-8	24	0	0	0	-8	0	0	0	0	0
111110	-8	-8	-16	0	0	8	0	-8	8	8	0	-8	0	-8	0	0
111111	24	8	0	0	0	8	0	-8	8	-8	16	-8	0	-8	0	0

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

Linear properties

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

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

$$Q4^+ \quad \left| \text{bias}_S\left(\frac{\text{wt } k}{\text{wt } k}, \frac{\text{wt } \ell}{\text{wt } \ell}\right) \right| \leq \frac{16}{64}$$

when $0 < k + \ell \leq 4$.

$$Q5^- \quad |\text{bias}_S(a, b_1) \cdot \text{bias}_S(a, b_2)| \leq \frac{384}{64^2}$$

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 \ b	0000	0001	0010	0100	1000	0011	0101	0110	1001	1010	1100	0111	1011	1101	1110	1111
000000	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
000001	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
000010	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
000100	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
001000	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
010000	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
100000	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
000011	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
000101	-8	-8	8	8	8	-8	-8	8	8	8	8	-8	-8	8	8	8
001001	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
001010	0	8	-8	-8	-8	8	8	-8	-8	-8	-8	8	8	-8	-8	-8
001100	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
010001	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
010010	8	-8	8	8	8	-8	-8	8	8	8	8	-8	-8	8	8	8
011000	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
100001	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
100010	-8	-8	8	8	8	8	-8	-8	8	8	8	-8	-8	8	8	8
101000	-8	-16	8	-16	-16	8	8	-8	-8	-8	-8	8	-16	8	-16	8
110000	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
000111	8	8	16	8	8	-8	-8	8	8	-8	-8	24	8	-8	-8	8
001011	-8	-8	-8	-16	-16	8	8	-8	-8	8	8	16	-8	8	8	16
001110	-8	-8	8	8	8	8	-8	-16	8	16	8	-8	-8	-8	-16	8
010011	8	8	0	0	0	8	8	16	-8	-16	16	-8	-8	-8	8	8
010101	16	-8	-8	-8	-8	8	8	8	8	-8	-8	-8	8	-8	-8	8
010110	-16	8	8	-8	-8	-8	-8	-16	16	16	16	-8	-8	8	8	8
011001	8	8	0	0	0	-24	8	8	-24	8	-8	-8	8	-8	8	8
011010	-8	16	-8	-8	-8	-24	-8	-8	-8	-8	-8	-8	8	8	8	8
100011	-8	8	8	-8	-8	16	-16	-16	-16	-16	-16	-16	16	-16	-16	16
100101	-8	8	8	-8	-8	16	-8	16	8	8	16	16	-8	-8	-8	16
100110	-8	8	8	-8	-8	16	-8	-8	-8	-8	-8	-8	-8	-8	-8	8
101001	-8	16	8	16	16	8	8	16	-8	-8	8	-16	-8	16	-8	8
101010	-8	8	8	-8	-8	-8	-8	-8	-8	16	16	-8	-8	-8	-8	8
101100	8	8	0	0	0	-8	8	8	-16	-8	-8	-8	8	-8	24	8
110001	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
110010	-8	-8	8	8	8	8	-8	-8	-8	-8	-8	-8	-8	8	8	8
110100	8	8	16	-8	-8	-8	-8	8	8	-16	-16	-8	-8	8	16	8
111000	-8	-8	8	16	16	8	16	8	-24	-24	-24	-8	-8	8	16	8
001111	8	-8	-8	-8	-8	-8	-8	-16	-8	16	-8	-8	8	8	-8	8
010111	-16	-16	-8	-8	-8	-16	-8	-8	-8	-8	-8	-8	-8	-8	-8	8
011011	8	16	8	-16	-16	-8	8	8	8	8	8	-8	-8	-8	-8	8
011110	8	-8	-8	-8	-8	-16	16	8	8	8	8	-8	8	8	8	8
100111	16	-8	-8	16	16	-8	-8	-8	-8	-8	-8	-16	-8	-8	-8	8
101011	-8	-8	8	8	8	-8	-8	8	8	-16	8	8	-8	-8	-8	8
101101	8	8	8	8	8	8	-8	-8	-8	8	8	-8	-8	-8	-8	8
110011	-8	-8	-16	-16	-16	8	16	8	16	8	8	-8	-8	-8	-16	8
110101	-8	16	-24	-24	-24	-8	-8	-8	-8	-8	-8	8	-8	-8	-8	8
110110	8	8	0	0	0	-8	8	8	-16	-8	-8	-8	8	-8	-8	8
111001	-8	-8	8	16	16	-16	-8	-16	-8	-8	8	-8	-8	-8	-8	-8
111010	8	-8	8	8	8	8	8	-8	-8	-8	-8	-8	-8	-8	-8	8
111100	8	8	8	-8	-8	8	8	-8	-8	-8	-8	-8	-8	-8	-8	8
001111	8	-8	-16	8	8	-8	-8	-16	-8	8	8	8	8	-8	8	8
010111	-24	-8	24	-8	-8	-8	-8	-8	-8	-8	-8	-8	-8	-8	-8	8
110111	-24	8	16	16	16	8	8	-8	-8	-8	-8	-8	-8	-8	-8	8
111011	8	16	-16	16	16	-8	8	8	8	8	8	-8	-8	-8	-8	8
111101	-8	24	8	-8	-8	-8	24	-8	-8	-8	-8	-8	-8	-8	-8	8
111110	-8	-8	-16	-16	-16	8	-8	-8	8	8	8	-8	-8	-8	-8	8
111111	24	8	-8	-8	-8	8	-8	-8	8	-8	16	-8	-8	-8	-8	8

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

Linear properties

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

$$Q3^+ \quad \text{bias}_S\left(\frac{\text{wt } 1}{16}, \frac{\text{wt } 1}{16}\right) = 0.$$

$$Q4^+ \quad \left| \text{bias}_S\left(\frac{\text{wt } k}{16}, \frac{\text{wt } \ell}{16}\right) \right| \leq \frac{16}{64}$$

when $0 < k + \ell \leq 4$.

$$Q5^- \quad |\text{bias}_S(a, b_1) \cdot \text{bias}_S(a, b_2)| \leq \frac{384}{64^2}$$

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 \ b	0000	0001	0010	0100	1000	0011	0101	0110	1001	1010	1100	0011	0101	1101	1100	1110	1111
000000	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
000001	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
000010	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
000100	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
001000	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
010000	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
100000	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
000011	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
000110	-8	-8	8	8	8	8	8	8	8	8	8	-8	-8	-8	-8	8	8
001001	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
001010	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
001100	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
010001	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
010010	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
010100	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
100001	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
100010	-8	-8	8	8	8	8	8	8	8	8	8	-8	-8	-8	-8	8	8
101000	-8	-8	8	8	8	8	8	8	8	8	8	-8	-8	-8	-8	8	8
110000	-8	-8	8	8	8	8	8	8	8	8	8	-8	-8	-8	-8	8	8
000111	8	8	16	8	8	8	8	8	8	8	8	24	8	8	8	8	8
001011	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
001110	-8	-8	8	8	8	8	8	8	8	8	8	-8	-8	-8	-8	8	8
010011	8	8	16	8	8	8	8	8	8	8	8	24	8	8	8	8	8
010101	16	-8	-8	8	8	8	8	8	8	8	8	-8	-8	-8	8	8	8
010110	-16	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8
011001	8	8	16	8	8	8	8	8	8	8	8	-8	-8	-8	8	8	8
011010	-8	-8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8
011100	-8	-8	8	8	8	8	8	8	8	8	8	-8	-8	-8	8	8	8
100011	-8	-8	8	8	8	8	8	8	8	8	8	-8	-8	-8	8	8	8
100101	-8	-8	8	8	8	8	8	8	8	8	8	-8	-8	-8	8	8	8
100110	-8	-8	8	8	8	8	8	8	8	8	8	-8	-8	-8	8	8	8
101001	-8	-8	8	8	8	8	8	8	8	8	8	-8	-8	-8	8	8	8
101010	-8	-8	8	8	8	8	8	8	8	8	8	-8	-8	-8	8	8	8
101100	-8	-8	8	8	8	8	8	8	8	8	8	-8	-8	-8	8	8	8
110001	-8	-8	8	8	8	8	8	8	8	8	8	-8	-8	-8	8	8	8
110010	-8	-8	8	8	8	8	8	8	8	8	8	-8	-8	-8	8	8	8
110100	-8	-8	8	8	8	8	8	8	8	8	8	-8	-8	-8	8	8	8
111000	-8	-8	8	8	8	8	8	8	8	8	8	-8	-8	-8	8	8	8
001111	8	8	16	8	8	8	8	8	8	8	8	24	8	8	8	8	8
010111	-8	-8	8	8	8	8	8	8	8	8	8	-8	-8	-8	8	8	8
011011	8	8	16	8	8	8	8	8	8	8	8	24	8	8	8	8	8
011110	8	8	16	8	8	8	8	8	8	8	8	-8	-8	-8	8	8	8
100111	16	-8	-8	8	8	8	8	8	8	8	8	-8	-8	-8	8	8	8
101011	-8	-8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8
101101	-8	-8	8	8	8	8	8	8	8	8	8	-8	-8	-8	8	8	8
101110	-8	-8	8	8	8	8	8	8	8	8	8	-8	-8	-8	8	8	8
110011	-8	-8	8	8	8	8	8	8	8	8	8	-8	-8	-8	8	8	8
110101	-8	-8	8	8	8	8	8	8	8	8	8	-8	-8	-8	8	8	8
110110	8	8	16	8	8	8	8	8	8	8	8	24	8	8	8	8	8
111001	-8	-8	8	8	8	8	8	8	8	8	8	-8	-8	-8	8	8	8
111010	8	8	16	8	8	8	8	8	8	8	8	-8	-8	-8	8	8	8
111000	8	8	16	8	8	8	8	8	8	8	8	-8	-8	-8	8	8	8
111111	24	8	8	8	8	8	8	8	8	8	8	-8	-8	-8	8	8	8

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

Linear properties

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

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

$$Q4^+ \quad \left| \text{bias}_S\left(\frac{\text{wt } k}{\text{wt } k}, \frac{\text{wt } \ell}{\text{wt } \ell}\right) \right| \leq \frac{16}{64}$$

when $0 < k + \ell \leq 4$.

$$Q5^- \quad |\text{bias}_S(a, b_1) \cdot \text{bias}_S(a, b_2)| \leq \frac{384}{64^2}$$

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 \ b	0000	0001	0010	0100	1000	0011	0101	0110	1001	1010	1100	0111	1011	1101	1110	1111
000000	64															
000001																
000010																
000100																
001000																
010000																
100000																
000011																
000110																
001100																
010100																
011000																
100100																
101000																
110000																
000111																
001101																
001110																
010101																
010110																
011001																
011010																
100101																
100110																
101001																
101010																
101100																
110001																
110010																
110100																
111000																
001111																
010111																
011011																
011101																
011110																
100111																
101011																
101101																
101110																
110011																
110101																
110110																
111001																
111010																
111011																
111100																
011111																
101111																
110111																
111011																
111101																
111110																
111111																

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

Linear properties

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

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

$$Q4^+ \quad \left| \text{bias}_S\left(\frac{\text{wt } k}{}, \frac{\text{wt } \ell}{}\right) \right| \leq \frac{16}{64}$$

when $0 < k + \ell \leq 4$.

$$Q5^- \quad |\text{bias}_S(a, b_1) \cdot \text{bias}_S(a, b_2)| \leq \frac{384}{64^2}$$

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

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

Linear properties

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

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

$$Q4^+ \quad \left| \text{bias}_S\left(\frac{\text{wt } k}{}, \frac{\text{wt } \ell}{}\right) \right| \leq \frac{16}{64}$$

when $0 < k + \ell \leq 4$.

$$Q5^- \quad |\text{bias}_S(a, b_1) \cdot \text{bias}_S(a, b_2)| \leq \frac{384}{64^2}$$

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 \ b	0000	0001	0010	0100	1000	0011	0101	0110	1001	1010	1100	0011	1011	1101	1110	1111
000000	64															
000001																
000010																
000100																
001000																
010000																
100000																
000011																
000110																
001010																
001100																
010100																
011000																
100100																
101000																
110000																
000111																
000110																
001011																
001101																
010101																
010110																
011001																
011010																
100101																
100110																
101001																
101010																
101100																
110001																
110010																
110100																
111000																
001111																
010111																
011011																
011101																
011110																
100111																
101011																
101101																
101110																
110011																
110101																
110110																
111001																
111010																
111100																
011111																
110111																
111011																
111101																
111110																
111111																

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

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:

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

- ▶ Thus, optimal graph algebraic immunity

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

- ▶ Due to Siegenthaler's inequality optimal multivariate degree

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

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:

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

- ▶ Thus, optimal graph algebraic immunity

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

- ▶ Due to Siegenthaler's inequality optimal multivariate degree

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

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:

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

- ▶ Thus, optimal graph algebraic immunity

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

- ▶ Due to Siegenthaler's inequality optimal multivariate degree

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

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:

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

- ▶ Thus, optimal graph algebraic immunity

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

- ▶ Due to Siegenthaler's inequality optimal multivariate degree

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

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

Preliminaries

Properties

Applications to DESL

Summary

Assumption

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

⇒ No assumption on independence of the bias of adjacent S-boxes!

Lemma

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

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

Corollary

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

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

Lemma (Patching)

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

Lemma

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

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

Corollary

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

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

Lemma (Patching)

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

Lemma

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

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

Corollary

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

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

Lemma (Patching)

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

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.)

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.)

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.)

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.)

Preliminaries

Properties

Applications to DESL

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.

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!

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