Improbable Differential Attacks on SERPENT using Undisturbed Bits

Cihangir TEZCAN[1,2], Halil Kemal TAŞKIN[1,3] and Murat DEMİRCİOĞLU[1,3]

[1]Institute of Applied Mathematics, Department of Cryptography
Middle East Technical University, Ankara, Turkey

[2]Department of Mathematics
Middle East Technical University, Ankara, Turkey

[3]Oran Technology
Ankara, Turkey

SIN 2014, Glasgow, Scotland
9 September 2014

Outline

Outline

A (Very) Short Introduction to Differential Cryptanalysis

- Differential Cryptanalysis
  - First public announcement by E. Biham and A. Shamir, early 1980s
  - Find a path (characteristic) so that when the input difference is α, output difference is β with high probability

A (Very) Short Introduction to Differential Cryptanalysis

- Differential Cryptanalysis
  - First public announcement by E. Biham and A. Shamir, early 1980s
  - Find a path (characteristic) so that when the input difference is α, output difference is β with high probability
- Truncated Differential Cryptanalysis
  - Discovered by L. Knudsen, 1994
  - Find a path (differential) so that when the input difference is α, output difference is β with high probability
  - Only parts of the differences α and β are specified

A (Very) Short Introduction to Differential Cryptanalysis

- Differential Cryptanalysis
  - First public announcement by E. Biham and A. Shamir, early 1980s
  - Find a path (characteristic) so that when the input difference is α, output difference is β with high probability
- Truncated Differential Cryptanalysis
  - Discovered by L. Knudsen, 1994
  - Find a path (differential) so that when the input difference is α, output difference is β with high probability
  - Only parts of the differences α and β are specified
- Impossible Differential Cryptanalysis
  - Discovered by E. Biham, A. Biryukov, A. Shamir, 1998
  - Find a path (impossible differential) so that when the input difference is α, the output difference is never β

A (Very) Short Introduction to Differential Cryptanalysis

- Differential Cryptanalysis
  - First public announcement by E. Biham and A. Shamir, early 1980s
  - Find a path (characteristic) so that when the input difference is α, output difference is β with high probability
- Truncated Differential Cryptanalysis
  - Discovered by L. Knudsen, 1994
  - Find a path (differential) so that when the input difference is α, output difference is β with high probability
  - Only parts of the differences α and β are specified
- Impossible Differential Cryptanalysis
  - Discovered by E. Biham, A. Biryukov, A. Shamir, 1998
  - Find a path (impossible differential) so that when the input difference is α, the output difference is never β
- And others (Higher-order Differential, Boomerang,...)

A (Very) Short Introduction to Differential Cryptanalysis

- Differential Cryptanalysis
  - First public announcement by E. Biham and A. Shamir, early 1980s
  - Find a path (characteristic) so that when the input difference is α, output difference is β with high probability
- Truncated Differential Cryptanalysis
  - Discovered by L. Knudsen, 1994
  - Find a path (differential) so that when the input difference is α, output difference is β with high probability
  - Only parts of the differences α and β are specified
- Impossible Differential Cryptanalysis
  - Discovered by E. Biham, A. Biryukov, A. Shamir, 1998
  - Find a path (impossible differential) so that when the input difference is α, the output difference is never β
- And others (Higher-order Differential, Boomerang,...)
- Improbable Differential Cryptanalysis
  - Discovered by C. Tezcan in 2008 (published in 2010)
  - Differentials are less probable for the correct key

Improbable Differential Cryptanalysis

Statistical Attacks

Statistical attacks on block ciphers make use of a property of the cipher so that an incident (characteristic, differential,...) occurs with different probabilities depending on whether the correct key is used or not.

Improbable Differential Cryptanalysis

Statistical Attacks

Statistical attacks on block ciphers make use of a property of the cipher so that an incident (characteristic, differential,...) occurs with different probabilities depending on whether the correct key is used or not.

Attack Type	Probability of the incident for a wrong key	probability of the incident for the correct key	Note
Statistical Attacks (Differential, Truncated,...)	p	p_0	$p_0 > p$

Improbable Differential Cryptanalysis

Statistical Attacks

Statistical attacks on block ciphers make use of a property of the cipher so that an incident (characteristic, differential,...) occurs with different probabilities depending on whether the correct key is used or not.

Attack Type	Probability of the incident for a wrong key	probability of the incident for the correct key	Note
Statistical Attacks (Differential, Truncated,...)	p	p_0	$p_0 > p$
Impossible Differential	p	0	$p_0 = 0$

Improbable Differential Cryptanalysis

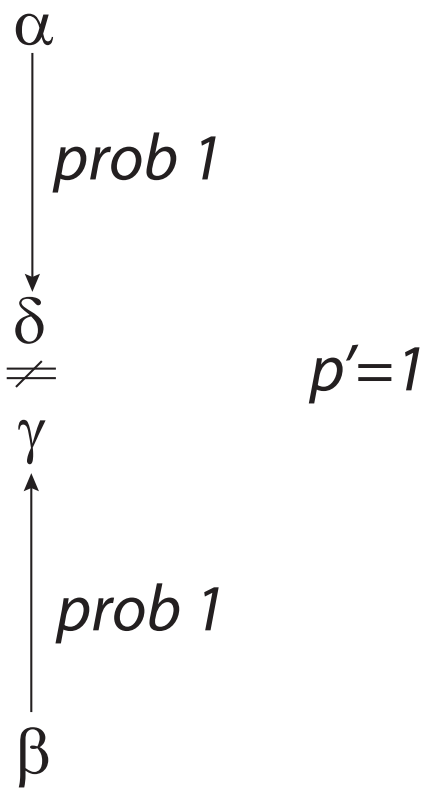
Statistical Attacks

Statistical attacks on block ciphers make use of a property of the cipher so that an incident (characteristic, differential,...) occurs with different probabilities depending on whether the correct key is used or not.

Attack Type	Probability of the incident for a wrong key	probability of the incident for the correct key	Note
Statistical Attacks (Differential, Truncated,...)	p	p_0	$p_0 > p$
Impossible Differential	p	0	$p_0 = 0$
Improbable Differential	p	p_0	$p_0 < p$

Miss-in-the-Middle Technique

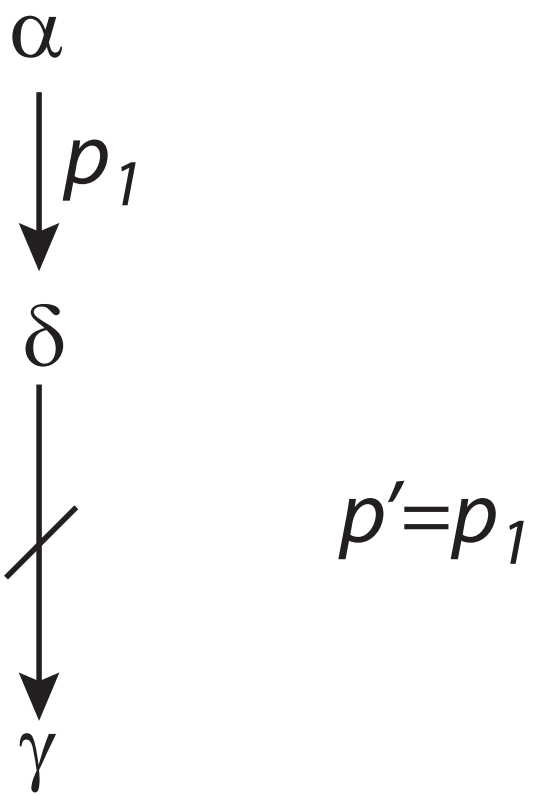
Figure : Miss-in-the-Middle Technique for obtaining Impossible Differentials



Improbable Differentials from Impossible Differentials

$p' = 1$

Improbable Differentials from Impossible Differentials



Improbable Differentials from Impossible Differentials

$p' = p_2$

Improbable Differential Attacks

Known Improbable Differential Attacks

- 13, 14, 15-round attacks on Clefia (best known attacks) [1,2]
- 13-round attack on Present [3]

References

1. C. Tezcan, The Improbable Differential Attacks: Cryptanalysis of Reduced Round Clefia. In G. Gong and K. C. Gupta (eds), INDOCRYPT, volume 6498 of LNCS, pages 197-209, Springer 2010
2. C. Tezcan and A. A. Selçuk, Improved Improbable Differential Attacks on ISO Standard Clefia: Expansion Technique Revisited (submitted to Information Processing Letters).
3. C. Tezcan, Improbable Differential Attacks on Present using Undisturbed Bits, Journal of Computational and Applied Mathematics, 259, Part B(0), pp. 503-511, 2014.

S-box Properties and Cryptanalysis

S-box Properties and Cryptanalysis

Confusion layer of cryptographic algorithms mostly consists of S-boxes.

1. Differential Uniformity => Differential Cryptanalysis
2. Non-linear Uniformity => Linear Cryptanalysis
3. Branch Number => Algebraic and Cube Attacks
4. Number of Shares => Side-Channel Attacks, DPA
5. Undisturbed Bits => Truncated, Impossible, Improbable Differential Cryptanalysis
6. Differential Factors => Differential Cryptanalysis and its variants

Undisturbed Bits

Definition

For a specific input difference of an S-box, if some bits of the output difference remain invariant, then we call such bits *undisturbed*.

Undisturbed Bits

Definition

For a specific input difference of an S-box, if some bits of the output difference remain invariant, then we call such bits *undisturbed*.

Example (SERPENT S_1)

1. Input Difference: 4_x => Output Difference: ?1??
2. Input Difference: 8_x => Output Difference: ?1??
3. Input Difference: C_x => Output Difference: ?0??
4. **Output Difference: $\mathbf{1_x}$ => Input Difference: 1???**
5. **Output Difference: $\mathbf{4_x}$ => Input Difference: 1???**
6. Output Difference: $\mathbf{5_x}$ => Input Difference: 0???

Cryptographic Algorithms with Undisturbed Bits

4×4 S-boxes with Undisturbed Bits (Previously known)

- We observed 69 out of 102 S-boxes contain 399 undisturbed bits
  1. CLEFIA
  2. DES
  3. GOST
  4. Hamsi
  5. Hummingbird-1
  6. Hummingbird-2
  7. LED
  8. LUCIFER
  9. Luffa
  10. NOEKEON
  11. LBLOCK
  12. PRESENT
  13. SERPENT
  14. Twofish

3×3 S-boxes with Undisturbed Bits

We proved that every bijective 3×3 S-box contains undisturbed bits

Undisturbed Bits and Cryptanalysis

Undisturbed Bits and Cryptanalysis

- Improbable differential attack on 13-round PRESENT by Tezcan [1]
- Differential-linear attack on 10, 11, 12-round SERPENT-128, SERPENT-192, SERPENT-256 by Tezcan and Özbudak [3] (with the help of differential factors)
- Improbable differential attack on 7-round SERPENT by Tezcan, Taşkın, Demircioğlu [2] (this talk)

References

1. C. Tezcan, Improbable Differential Attacks on PRESENT using Undisturbed Bits, Journal of Computational and Applied Mathematics, 259, Part B(0), pp. 503-511, 2014.
2. C. Tezcan, H. K. Taşkın, M. Demircioğlu, Improbable Differential Attacks on SERPENT using Undisturbed Bits, to appear at SIN'14, 10 September 2014.
3. C. Tezcan, F. Özbudak, Differential Factors: Improved Attacks on SERPENT, Lightsec 2014.

Cryptographic Algorithms with Undisturbed Bits

4×4 S-boxes with Undisturbed Bits (new results)

1. Piccolo
2. RECTANGLE
3. SPONGENT

Cryptographic Algorithms with Undisturbed Bits

4×4 S-boxes with Undisturbed Bits (new results)

1. Piccolo
2. RECTANGLE
3. SPONGENT

5×5 and 6×6 S-boxes with Undisturbed Bits (new results)

1. FIDES

Cryptographic Algorithms with Undisturbed Bits

4×4 S-boxes with Undisturbed Bits (new results)

1. Piccolo
2. RECTANGLE
3. SPONGENT

5×5 and 6×6 S-boxes with Undisturbed Bits (new results)

1. FIDES

9×9 S-boxes with Undisturbed Bits (new results)

1. KASUMI
2. MISTY

Cryptographic Algorithms with Undisturbed Bits

4×4 S-boxes with Undisturbed Bits (new results)

1. Piccolo
2. RECTANGLE
3. SPONGENT

5×5 and 6×6 S-boxes with Undisturbed Bits (new results)

1. FIDES

9×9 S-boxes with Undisturbed Bits (new results)

1. KASUMI
2. MISTY

Remark

Undisturbed bits can be observed in large S-boxes.

Undisturbed Bits for 3×3 S-boxes

3×3 S-boxes with Undisturbed Bits

- The previously obtained result that every 3×3 S-boxes contains undisturbed bits was correct but the proof overlooked some cases

Undisturbed Bits for 3×3 S-boxes

3×3 S-boxes with Undisturbed Bits

- The previously obtained result that every 3×3 S-boxes contains undisturbed bits was correct but the proof overlooked some cases
- We provided another proof for this theorem and exhaustively obtained that out of $8! = 40320$ bijective 3×3 S-boxes
  - 17088 of them have 6
  - 10368 of them have 30
  - 1344 of them have 42

  undisturbed bits.

Undisturbed Bits of Serpent

Serpent

- Serpent came second in the AES contest
- It is a substitution permutation network with 8 S-boxes
- Block size: 128 bits
- Key size: 128, 192, 256 bits
- 5 out of its 8 S-boxes have 27 undisturbed bits

Undisturbed Bits of SERPENT

Table : Undisturbed bits of SERPENT's S-boxes

S-box	Input Difference	Output Difference
S_0	2_x, 4_x	1???
S_0	6_x	0???
S_0^{-1}	4_x, 8_x	?1??
S_0^{-1}	C_x	?0??
S_1	4_x, 8_x	?1??
S_1	C_x	?0??
S_1^{-1}	1_x, 4_x	1???
S_1^{-1}	5_x	0???
S_2	2_x, 8_x	???1
S_2	A_x	???0
S_2^{-1}	1_x, C_x	???1
S_2^{-1}	D_x	???0
S_4, S_5	4_x, B_x	???1
S_4, S_5	F_x	???0
S_6	2_x, 4_x	??1?
S_6	6_x	??0?
S_6^{-1}	2_x, 8_x	??1?
S_6^{-1}	A_x	??0?

Improbable Differential Attacks on SERPENT

Table : A 5.5-Round Impossible Differential for SERPENT

Input	X_0:	0000	0000	0000	0000	0000	0000	0000	0000
	X_1:	0001	0000	0000	0000	0000	0000	0000	0000
	X_2:	0000	0010	0000	0000	0000	0000	0000	0000
	X_3:	0001	0000	0000	0000	0000	0000	0000	0000

Improbable Differential Attacks on SERPENT

Table : A 5.5-Round Impossible Differential for SERPENT

Input	X_0: 0000	0000	0000	0000	0000	0000	0000	0000
	X_1: 0001	0000	0000	0000	0000	0000	0000	0000
	X_2: 0000	0010	0000	0000	0000	0000	0000	0000
	X_3: 0001	0000	0000	0000	0000	0000	0000	0000
LT	X_0: 0000	0000	0000	0000	0000	0000	0000	0000
	X_1: 0000	0000	0000	0000	0000	0000	0000	0000
	X_2: 0000	0000	0000	0100	0000	0000	0000	0000
	X_3: 0000	0000	0000	0000	0000	0000	0000	0000

Improbable Differential Attacks on SERPENT

Table : A 5.5-Round Impossible Differential for SERPENT

Input	X_0: 0000	0000	0000	0000	0000	0000	0000	0000
	X_1: 0001	0000	0000	0000	0000	0000	0000	0000
	X_2: 0000	0010	0000	0000	0000	0000	0000	0000
	X_3: 0001	0000	0000	0000	0000	0000	0000	0000
LT	X_0: 0000	0000	0000	0000	0000	0000	0000	0000
	X_1: 0000	0000	0000	0000	0000	0000	0000	0000
	X_2: 0000	0000	0000	0100	0000	0000	0000	0000
	X_3: 0000	0000	0000	0000	0000	0000	0000	0000
S_1	X_0: 0000	0000	0000	0?00	0000	0000	0000	0000
	X_1: 0000	0000	0000	0?00	0000	0000	0000	0000
	X_2: 0000	0000	0000	0100	0000	0000	0000	0000
	X_3: 0000	0000	0000	0?00	0000	0000	0000	0000

Improbable Differential Attacks on SERPENT

Table : A 5.5-Round Impossible Differential for SERPENT

Input	X_0: 0000	0000	0000	0000	0000	0000	0000	0000
	X_1: 0001	0000	0000	0000	0000	0000	0000	0000
	X_2: 0000	0010	0000	0000	0000	0000	0000	0000
	X_3: 0001	0000	0000	0000	0000	0000	0000	0000
LT	X_0: 0000	0000	0000	0000	0000	0000	0000	0000
	X_1: 0000	0000	0000	0000	0000	0000	0000	0000
	X_2: 0000	0000	0000	0100	0000	0000	0000	0000
	X_3: 0000	0000	0000	0000	0000	0000	0000	0000
S_1	X_0: 0000	0000	0000	0?00	0000	0000	0000	0000
	X_1: 0000	0000	0000	0?00	0000	0000	0000	0000
	X_2: 0000	0000	0000	0100	0000	0000	0000	0000
	X_3: 0000	0000	0000	0?00	0000	0000	0000	0000
LT	X_0: 0?00	100?	0000	0000	0000	0000	00??	0010
	X_1: 0000	0000	0100	?000	0000	0000	0000	000?
	X_2: 00?0	0000	0000	110?	?000	1000	0000	0000
	X_3: 0001	00?0	0000	0000	0000	0000	0000	0000

Improbable Differential Attacks on SERPENT

Table : A 5.5-Round Impossible Differential for SERPENT

Input	X_0: 0000	0000	0000	0000	0000	0000	0000	0000
	X_1: 0001	0000	0000	0000	0000	0000	0000	0000
	X_2: 0000	0010	0000	0000	0000	0000	0000	0000
	X_3: 0001	0000	0000	0000	0000	0000	0000	0000
LT	X_0: 0000	0000	0000	0000	0000	0000	0000	0000
	X_1: 0000	0000	0000	0000	0000	0000	0000	0000
	X_2: 0000	0000	0000	0100	0000	0000	0000	0000
	X_3: 0000	0000	0000	0000	0000	0000	0000	0000
S_1	X_0: 0000	0000	0000	0?00	0000	0000	0000	0000
	X_1: 0000	0000	0000	0?00	0000	0000	0000	0000
	X_2: 0000	0000	0000	0100	0000	0000	0000	0000
	X_3: 0000	0000	0000	0?00	0000	0000	0000	0000
LT	X_0: 0?00	100?	0000	0000	0000	0000	00??	0010
	X_1: 0000	0000	0100	?000	0000	0000	0000	000?
	X_2: 00?0	0000	0000	110?	?000	1000	0000	0000
	X_3: 0001	00?0	0000	0000	0000	0000	0000	0000
S_2	X_0: 0??1	?0??	0100	??0?	?000	?000	00??	00??
	X_1: 0???	?0??	0?00	??0?	?000	?000	00??	00??
	X_2: 0???	?0??	0?00	??0?	?000	?000	00??	00??
	X_3: 0???	?0??	0?00	??0?	?000	?000	00??	00??

Improbable Differential Attacks on SERPENT

Table : A 5.5-Round Impossible Differential for SERPENT

Input	X_0: 0000	0000	0000	0000	0000	0000	0000	0000
	X_1: 0001	0000	0000	0000	0000	0000	0000	0000
	X_2: 0000	0010	0000	0000	0000	0000	0000	0000
	X_3: 0001	0000	0000	0000	0000	0000	0000	0000
LT	X_0: 0000	0000	0000	0000	0000	0000	0000	0000
	X_1: 0000	0000	0000	0000	0000	0000	0000	0000
	X_2: 0000	0000	0000	0100	0000	0000	0000	0000
	X_3: 0000	0000	0000	0000	0000	0000	0000	0000
S_1	X_0: 0000	0000	0000	0?00	0000	0000	0000	0000
	X_1: 0000	0000	0000	0?00	0000	0000	0000	0000
	X_2: 0000	0000	0000	0100	0000	0000	0000	0000
	X_3: 0000	0000	0000	0?00	0000	0000	0000	0000
LT	X_0: 0?00	100?	0000	0000	0000	0000	00??	0010
	X_1: 0000	0000	0100	?000	0000	0000	0000	000?
	X_2: 00?0	0000	0000	110?	?000	1000	0000	0000
	X_3: 0001	00?0	0000	0000	0000	0000	0000	0000
S_2	X_0: 0??1	?0??	0100	??0?	?000	?000	00??	00??
	X_1: 0???	?0??	0?00	??0?	?000	?000	00??	00??
	X_2: 0???	?0??	0?00	??0?	?000	?000	00??	00??
	X_3: 0???	?0??	0?00	??0?	?000	?000	00??	00??
LT	X_0: ????	????	????	????	????	????	????	????
	X_1: ????	0??0	??0?	????	??0?	?1??	????	0???
	X_2: ????	????	????	????	????	????	1???	????
	X_3: ?0??	????	????	1?0?	??**1**?	??0?	????	??0?

Improbable Differential Attacks on SERPENT

Table : A 5.5-Round Impossible Differential for SERPENT

LT	X_0:	0000	0000	0000	0000	0000	0000	0001	0000
	X_1:	1000	0000	0000	0000	0000	0000	0000	0000
	X_2:	0000	0000	0000	0000	0000	0000	0000	0000
	X_3:	0000	0000	0000	0000	0000	0000	0000	0000

Improbable Differential Attacks on SERPENT

Table : A 5.5-Round Impossible Differential for SERPENT

S_5	X_0: 0000	0000	0000	0000	0000	0000	0000	0000
	X_1: 0100	0000	0000	0000	0000	0000	0000	0000
	X_2: 0000	0000	0000	0000	0000	0000	0000	0000
	X_3: 0000	0000	0000	0000	0000	0000	0000	0000
LT	X_0: 0000	0000	0000	0000	0000	0000	0001	0000
	X_1: 1000	0000	0000	0000	0000	0000	0000	0000
	X_2: 0000	0000	0000	0000	0000	0000	0000	0000
	X_3: 0000	0000	0000	0000	0000	0000	0000	0000

Improbable Differential Attacks on SERPENT

Table : A 5.5-Round Impossible Differential for SERPENT

LT	X_0: 0?00	0000	0000	0000	0000	0000	0000	0000
	X_1: 0?00	0000	0000	0000	0000	0000	0000	0000
	X_2: 0?00	0000	0000	0000	0000	0000	0000	0000
	X_3: 0?00	0000	0000	0000	0000	0000	0000	0000
S_5	X_0: 0000	0000	0000	0000	0000	0000	0000	0000
	X_1: 0100	0000	0000	0000	0000	0000	0000	0000
	X_2: 0000	0000	0000	0000	0000	0000	0000	0000
	X_3: 0000	0000	0000	0000	0000	0000	0000	0000
LT	X_0: 0000	0000	0000	0000	0000	0000	0001	0000
	X_1: 1000	0000	0000	0000	0000	0000	0000	0000
	X_2: 0000	0000	0000	0000	0000	0000	0000	0000
	X_3: 0000	0000	0000	0000	0000	0000	0000	0000

Improbable Differential Attacks on SERPENT

Table : A 5.5-Round Impossible Differential for SERPENT

S_4	X_0: 0000	0000	0000	00?0	000?	0000	0000	0000
	X_1: 0??0	00?0	0000	0000	0000	000?	0000	0000
	X_2: 0000	?000	0000	0000	0000	0000	00?0	0000
	X_3: 0?0?	0000	?000	0000	0000	000?	0000	0000
LT	X_0: 0?00	0000	0000	0000	0000	0000	0000	0000
	X_1: 0?00	0000	0000	0000	0000	0000	0000	0000
	X_2: 0?00	0000	0000	0000	0000	0000	0000	0000
	X_3: 0?00	0000	0000	0000	0000	0000	0000	0000
S_5	X_0: 0000	0000	0000	0000	0000	0000	0000	0000
	X_1: 0100	0000	0000	0000	0000	0000	0000	0000
	X_2: 0000	0000	0000	0000	0000	0000	0000	0000
	X_3: 0000	0000	0000	0000	0000	0000	0000	0000
LT	X_0: 0000	0000	0000	0000	0000	0000	0001	0000
	X_1: 1000	0000	0000	0000	0000	0000	0000	0000
	X_2: 0000	0000	0000	0000	0000	0000	0000	0000
	X_3: 0000	0000	0000	0000	0000	0000	0000	0000

Improbable Differential Attacks on SERPENT

Table : A 5.5-Round Impossible Differential for SERPENT

LT	X_0: 0???	?0?0	?000	00?0	000?	000?	00?0	0000
	X_1: 0???	?0?0	?000	00?0	000?	000?	00?0	0000
	X_2: 0???	?0?0	?000	00?0	000?	000?	00?0	0000
	X_3: 0???	?0?0	?000	00?0	000?	000?	00?0	0000
S_4	X_0: 0000	0000	0000	00?0	000?	0000	0000	0000
	X_1: 0??0	00?0	0000	0000	0000	000?	0000	0000
	X_2: 0000	?000	0000	0000	0000	0000	00?0	0000
	X_3: 0?0?	0000	?000	0000	0000	000?	0000	0000
LT	X_0: 0?00	0000	0000	0000	0000	0000	0000	0000
	X_1: 0?00	0000	0000	0000	0000	0000	0000	0000
	X_2: 0?00	0000	0000	0000	0000	0000	0000	0000
	X_3: 0?00	0000	0000	0000	0000	0000	0000	0000
S_5	X_0: 0000	0000	0000	0000	0000	0000	0000	0000
	X_1: 0100	0000	0000	0000	0000	0000	0000	0000
	X_2: 0000	0000	0000	0000	0000	0000	0000	0000
	X_3: 0000	0000	0000	0000	0000	0000	0000	0000
LT	X_0: 0000	0000	0000	0000	0000	0000	0001	0000
	X_1: 1000	0000	0000	0000	0000	0000	0000	0000
	X_2: 0000	0000	0000	0000	0000	0000	0000	0000
	X_3: 0000	0000	0000	0000	0000	0000	0000	0000

Improbable Differential Attacks on SERPENT

Table : A 5.5-Round Impossible Differential for SERPENT

S_3	X_0: ?000	??0?	0?00	?0??	??0?	???0	?0??	0000
	X_1: 0???	????	??0?	????	?00?	?00?	????	?0??
	X_2: 0?00	????	0???	?00?	??0?	00?0	00??	??0?
	X_3: ????	????	????	????	?00?	??0?	???0	?0?0
LT	X_0: 0???	?0?0	?000	00?0	000?	000?	00?0	0000
	X_1: 0???	?0?0	?000	00?0	000?	000?	00?0	0000
	X_2: 0???	?0?0	?000	00?0	000?	000?	00?0	0000
	X_3: 0???	?0?0	?000	00?0	000?	000?	00?0	0000
S_4	X_0: 0000	0000	0000	00?0	000?	0000	0000	0000
	X_1: 0??0	00?0	0000	0000	0000	000?	0000	0000
	X_2: 0000	?000	0000	0000	0000	0000	00?0	0000
	X_3: 0?0?	0000	?000	0000	0000	000?	0000	0000
LT	X_0: 0?00	0000	0000	0000	0000	0000	0000	0000
	X_1: 0?00	0000	0000	0000	0000	0000	0000	0000
	X_2: 0?00	0000	0000	0000	0000	0000	0000	0000
	X_3: 0?00	0000	0000	0000	0000	0000	0000	0000
S_5	X_0: 0000	0000	0000	0000	0000	0000	0000	0000
	X_1: 0100	0000	0000	0000	0000	0000	0000	0000
	X_2: 0000	0000	0000	0000	0000	0000	0000	0000
	X_3: 0000	0000	0000	0000	0000	0000	0000	0000
LT	X_0: 0000	0000	0000	0000	0000	0000	0001	0000
	X_1: 1000	0000	0000	0000	0000	0000	0000	0000
	X_2: 0000	0000	0000	0000	0000	0000	0000	0000
	X_3: 0000	0000	0000	0000	0000	0000	0000	0000

Improbable Differential Attacks on SERPENT

Table : A 5.5-Round Impossible Differential for SERPENT

LT	X_0: ????	????	????	????	??0?	????	????	????
	X_1: ????	????	????	????	??0?	????	????	????
	X_2: ????	????	????	????	??0?	????	????	????
	X_3: ????	????	????	????	??**0**?	????	????	????
S_3	X_0: ?000	??0?	0?00	?0??	??0?	???0	?0??	0000
	X_1: 0???	????	??0?	????	?00?	?00?	????	?0??
	X_2: 0?00	????	0???	?00?	??0?	00?0	00??	??0?
	X_3: ????	????	????	????	?00?	??0?	???0	?0?0
LT	X_0: 0???	?0?0	?000	00?0	000?	000?	00?0	0000
	X_1: 0???	?0?0	?000	00?0	000?	000?	00?0	0000
	X_2: 0???	?0?0	?000	00?0	000?	000?	00?0	0000
	X_3: 0???	?0?0	?000	00?0	000?	000?	00?0	0000
S_4	X_0: 0000	0000	0000	00?0	000?	0000	0000	0000
	X_1: 0??0	00?0	0000	0000	0000	000?	0000	0000
	X_2: 0000	?000	0000	0000	0000	0000	00?0	0000
	X_3: 0?0?	0000	?000	0000	0000	000?	0000	0000
LT	X_0: 0?00	0000	0000	0000	0000	0000	0000	0000
	X_1: 0?00	0000	0000	0000	0000	0000	0000	0000
	X_2: 0?00	0000	0000	0000	0000	0000	0000	0000
	X_3: 0?00	0000	0000	0000	0000	0000	0000	0000
S_5	X_0: 0000	0000	0000	0000	0000	0000	0000	0000
	X_1: 0100	0000	0000	0000	0000	0000	0000	0000
	X_2: 0000	0000	0000	0000	0000	0000	0000	0000
	X_3: 0000	0000	0000	0000	0000	0000	0000	0000
LT	X_0: 0000	0000	0000	0000	0000	0000	0001	0000
	X_1: 1000	0000	0000	0000	0000	0000	0000	0000
	X_2: 0000	0000	0000	0000	0000	0000	0000	0000
	X_3: 0000	0000	0000	0000	0000	0000	0000	0000

Improbable Differential Attacks on SERPENT

Table : A 5.5-Round Impossible Differential for SERPENT

Input	X_0:	0000	0000	0000	0000	0000	0000	0000	0000
	X_1:	0001	0000	0000	0000	0000	0000	0000	0000
	X_2:	0000	0010	0000	0000	0000	0000	0000	0000
	X_3:	0001	0000	0000	0000	0000	0000	0000	0000
LT	X_0:	0000	0000	0000	0000	0000	0000	0000	0000
	X_1:	0000	0000	0000	0000	0000	0000	0000	0000
	X_2:	0000	0000	0000	0100	0000	0000	0000	0000
	X_3:	0000	0000	0000	0000	0000	0000	0000	0000
S_1	X_0:	0000	0000	0000	0?00	0000	0000	0000	0000
	X_1:	0000	0000	0000	0?00	0000	0000	0000	0000
	X_2:	0000	0000	0000	0100	0000	0000	0000	0000
	X_3:	0000	0000	0000	0?00	0000	0000	0000	0000
LT	X_0:	0?00	100?	0000	0000	0000	0000	00??	0010
	X_1:	0000	0000	0100	?000	0000	0000	0000	000?
	X_2:	00?0	0000	0000	110?	?000	1000	0000	0000
	X_3:	0001	00?0	0000	0000	0000	0000	0000	0000
S_2	X_0:	0??1	?0??	0100	??0?	?000	?000	00??	00??
	X_1:	0???	?0??	0?00	??0?	?000	?000	00??	00??
	X_2:	0???	?0??	0?00	??0?	?000	?000	00??	00??
	X_3:	0???	?0??	0?00	??0?	?000	?000	00??	00??
LT	X_0:	????	????	????	????	????	????	????	????
	X_1:	????	0??0	??0?	????	??0?	?1??	????	0???
	X_2:	????	????	????	????	????	????	1???	????
	X_3:	?0??	????	????	1?0?	??**1**?	??0?	????	??0?
					Impossible				
LT	X_0:	????	????	????	????	??0?	????	????	????
	X_1:	????	????	????	????	??0?	????	????	????
	X_2:	????	????	????	????	??0?	????	????	????
	X_3:	????	????	????	????	??**0**?	????	????	????
S_3	X_0:	?000	??0?	0?00	?0??	??0?	???0	?0??	0000
	X_1:	0???	????	??0?	????	?00?	?00?	????	?0??
	X_2:	0?00	????	0???	?00?	??0?	00?0	00??	??0?
	X_3:	????	????	????	????	?00?	??0?	???0	?0?0
LT	X_0:	0???	?0?0	?000	00?0	000?	000?	00?0	0000
	X_1:	0???	?0?0	?000	00?0	000?	000?	00?0	0000
	X_2:	0???	?0?0	?000	00?0	000?	000?	00?0	0000
	X_3:	0???	?0?0	?000	00?0	000?	000?	00?0	0000
S_4	X_0:	0000	0000	0000	00?0	000?	0000	0000	0000
	X_1:	0??0	00?0	0000	0000	0000	000?	0000	0000
	X_2:	0000	?000	0000	0000	0000	0000	00?0	0000
	X_3:	0?0?	0000	?000	0000	0000	000?	0000	0000
LT	X_0:	0?00	0000	0000	0000	0000	0000	0000	0000
	X_1:	0?00	0000	0000	0000	0000	0000	0000	0000
	X_2:	0?00	0000	0000	0000	0000	0000	0000	0000
	X_3:	0?00	0000	0000	0000	0000	0000	0000	0000
S_5	X_0:	0000	0000	0000	0000	0000	0000	0000	0000
	X_1:	0100	0000	0000	0000	0000	0000	0000	0000
	X_2:	0000	0000	0000	0000	0000	0000	0000	0000
	X_3:	0000	0000	0000	0000	0000	0000	0000	0000
LT	X_0:	0000	0000	0000	0000	0000	0000	0001	0000
	X_1:	1000	0000	0000	0000	0000	0000	0000	0000
	X_2:	0000	0000	0000	0000	0000	0000	0000	0000
	X_3:	0000	0000	0000	0000	0000	0000	0000	0000

Improbable Differential Attacks on SERPENT

Table : A 7-Round Improbable Differential Attack

Input	X_0:	0000	0000	?00?	0000	0000	0000	??00	?00?
	X_1:	0000	0000	?00?	0000	0000	0000	??00	?00?
	X_2:	0000	0000	?00?	0000	0000	0000	??00	?00?
	X_3:	0000	0000	?00?	0000	0000	0000	??00	?00?
S_7	X_0:	0000	0000	0000	0000	0000	0000	1000	0000
	X_1:	0000	0000	0001	0000	0000	0000	0100	1000
	X_2:	0000	0000	0000	0000	0000	0000	0000	1001
	X_3:	0000	0000	1000	0000	0000	0000	0100	1000
LT	X_0:	0000	0010	0000	0000	0000	0000	0000	0000
	X_1:	0000	0000	0000	0000	0000	0000	0000	0000
	X_2:	0001	0010	0000	0000	0000	0000	0000	0000
	X_3:	0000	0000	0000	0000	0000	0000	0000	0000
S_0	X_0:	0000	0000	0000	0000	0000	0000	0000	0000
	X_1:	0001	0000	0000	0000	0000	0000	0000	0000
	X_2:	0000	0010	0000	0000	0000	0000	0000	0000
	X_3:	0001	0000	0000	0000	0000	0000	0000	0000
4.5-Round Impossible Differential									
LT	X_0:	0??0	0?00	0000	0000	00?0	0??0	?000	?000
	X_1:	0?00	00?0	0000	0000	0000	0000	0000	0000
	X_2:	0??0	??00	??0?	0??0	??0?	0000	0000	00?0
	X_3:	0?00	000?	0000	0000	0000	000?	00??	0000
S_5	X_0:	0??0	????	??0?	0??0	????	0???	?0??	?0?0
	X_1:	0??0	????	??0?	0??0	????	0???	?0??	?0?0
	X_2:	0??0	????	??0?	0??0	????	0???	?0??	?0?0
	X_3:	0??0	????	??0?	0??0	????	0???	?0??	?0?0

$p' = 2^{-4}$

Summary of Attacks on SERPENT

Table : Summary of Attacks on SERPENT

#Rounds	Attack Type	Key	Data	Time	Memory	Advantage	Success	Reference
6	Meet-in-the-middle	256	512 KP	2^{247} En	2^{246} B	-	-	Kohno et al.
6	Differential	All	2^{83} CP	2^{90} En	2^{40} B	-	-	Kohno et al.
6	Differential	All	2^{71} CP	2^{103} En	2^{75} B	-	-	Kohno et al.
6	Differential	192	2^{41} CP	2^{163} En	2^{45} B	124	-	Kohno et al.
7	Differential	256	2^{122} CP	2^{248} En	2^{126} B	128	-	Kohno et al.
7	**Improbable**	**All**	$\mathbf{2^{116.85}}$ **CP**	$\mathbf{2^{117.57}}$ **En**	$\mathbf{2^{113}}$ **B**	**112**	**99.9%**	**SIN'14**
7	Differential	All	2^{84} CP	2^{85} MA	2^{56} B	-	-	Biham et al.
10	Rectangle	192	$2^{126.3}$ CP	$2^{173.8}$ MA	$2^{131.8}$ B	80	-	Biham et al.
10	Boomerang	192	$2^{126.3}$ AC	$2^{173.8}$ MA	2^{89} B	80	-	Biham et al.
10	Differential-Linear	All	$2^{101.2}$ CP	$2^{115.2}$ En	2^{40} B	40	84%	Dunkelman et al.
10	**Differential-Linear**	**All**	$\mathbf{2^{101.2}}$ **CP**	$\mathbf{2^{113.2}}$ **En**	$\mathbf{2^{40}}$ **B**	**38**	**84%**	**LightSEC'14**
10	**Differential-Linear**	**All**	$\mathbf{2^{100.55}}$ **CP**	$\mathbf{2^{116.55}}$ **En**	$\mathbf{2^{40}}$ **B**	**42**	**84%**	**LightSEC'14**
11	Linear	256	2^{118} KP	2^{214} MA	2^{85} B	140	78.5%	Biham et al.
11	Multidimensional Linear	All	$2^{125.81}$ KP	$2^{114.13}$ MA	2^{108} B	48	78.5%	Nguyen et al.
11	Multidimensional Linear	All	$2^{127.78}$ KP	$2^{110.10}$ MA	2^{104} B	44	78.5%	Nguyen et al.
11	Nonlinear	192	$2^{120.36}$ KP	$2^{139.63}$ MA	$2^{133.17}$ B	118	78.5%	McLaughlin et al.
11	Filtered Nonlinear	192	$2^{114.55}$ KP	$2^{155.76}$ MA	$2^{146.59}$ B	132	78.5%	McLaughlin et al.
11	Differential-Linear	192	$2^{121.8}$ CP	$2^{135.7}$ MA	2^{76} B	48	84%	Dunkelman et al.
11	**Differential-Linear**	**192**	$\mathbf{2^{121.8}}$ **CP**	$\mathbf{2^{133.7}}$ **MA**	$\mathbf{2^{76}}$ **B**	**46**	**84%**	**LightSEC'14**
11	**Differential-Linear**	**192**	$\mathbf{2^{121.15}}$ **CP**	$\mathbf{2^{137.05}}$ **MA**	$\mathbf{2^{76}}$ **B**	**50**	**84%**	**LightSEC'14**
12	Multidimensional Linear	256	$\geq 2^{125.81}$ KP	$2^{242.13}$ MA	2^{125} B	174	78.5%	Nguyen et al.
12	Differential-Linear	256	$2^{123.5}$ CP	$2^{249.4}$ En	$2^{128.5}$ B	160	84%	Dunkelman et al.
12	**Differential-Linear**	**256**	$\mathbf{2^{123.5}}$ **CP**	$\mathbf{2^{246.4}}$ **En**	$\mathbf{2^{128.5}}$ **B**	**157**	**84%**	**LightSEC'14**

Summary

Summary

1. Introduced undisturbed bits for new ciphers with 4×4 S-boxes

Summary

Summary

1. Introduced undisturbed bits for new ciphers with 4×4 S-boxes
2. Showed that undisturbed bits are possible for large S-boxes (namely 5×5 and 6×6 S-boxes of FIDES and 9×9 S-boxes of KASUMI and MISTY)

Summary

Summary

1. Introduced undisturbed bits for new ciphers with 4×4 S-boxes
2. Showed that undisturbed bits are possible for large S-boxes (namely 5×5 and 6×6 S-boxes of FIDES and 9×9 S-boxes of KASUMI and MISTY)
3. Provided the first impossible and improbable differential attacks on SERPENT using undisturbed bits. The cipher looks secure against these kind of attacks.

Thanks

Thank You for Your Attention