Differential Factors: Improved Attacks on Serpent

Cihangir TEZCAN and Ferruh Özbudak

Department of Mathematics
Middle East Technical University

Institute of Applied Mathematics
Department of Cryptography
Middle East Technical University

LightSEC 2014
İstanbul, Turkey

Outline

S-box Properties and Cryptanalysis

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

S-box Properties and Cryptanalysis

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

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

Undisturbed Bits and Cryptanalysis

Undisturbed Bits and Cryptanalysis

- Improbable differential attack on 13-round PRESENT by Tezcan [1]
- Improbable differential attack on 7-round SERPENT by Tezcan, Taşkın, Demircioğlu [2]
- Differential-linear attack on 11, 12, 13-round SERPENT-128, SERPENT-192, SERPENT-256 [3] (this talk)

Undisturbed Bits and Cryptanalysis

Undisturbed Bits and Cryptanalysis

- Improbable differential attack on 13-round PRESENT by Tezcan [1]
- Improbable differential attack on 7-round SERPENT by Tezcan, Taşkın, Demircioğlu [2]
- Differential-linear attack on 11, 12, 13-round SERPENT-128, SERPENT-192, SERPENT-256 [3] (this talk)
- For more information on undisturbed bits see tomorrow's talk [4].

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.
4. R. H. Makarim, C. Tezcan, Relating Undisturbed Bits to Other Properties of Substitution Boxes, Lightsec 2014.

Linear Factors

Definition (Linear Factor)

A block cipher is said to have a *linear factor* if, for all plaintexts and keys, there is a fixed non-empty set of key bits whose simultaneous complementation leaves the XOR sum of a fixed non-empty set of ciphertext bits unchanged.

Linear Factors

Definition (Linear Factor)

A block cipher is said to have a *linear factor* if, for all plaintexts and keys, there is a fixed non-empty set of key bits whose simultaneous complementation leaves the XOR sum of a fixed non-empty set of ciphertext bits unchanged.

Alternative Definition

A function $F : \mathbb{F}_2^{\not\times} \to \mathbb{F}_2^m$ is said to have a *linear factor*, if for all $x \in \mathbb{F}_2^n$, there exists a nonzero $\alpha \in \mathbb{F}_2^n$ and a nonzero $b \in \mathbb{F}_2^m$ such that

$$b \cdot F(x \oplus \alpha) = \epsilon$$

for a fixed $\epsilon \in \mathbb{F}_2$.

Linear Factors

Definition (Linear Factor)

A block cipher is said to have a *linear factor* if, for all plaintexts and keys, there is a fixed non-empty set of key bits whose simultaneous complementation leaves the XOR sum of a fixed non-empty set of ciphertext bits unchanged.

Alternative Definition

A function $F : \mathbb{F}_2^{\not\times} \to \mathbb{F}_2^m$ is said to have a *linear factor*, if for all $x \in \mathbb{F}_2^n$, there exists a nonzero $\alpha \in \mathbb{F}_2^n$ and a nonzero $b \in \mathbb{F}_2^m$ such that

$$b \cdot F(x \oplus \alpha) = \epsilon$$

for a fixed $\epsilon \in \mathbb{F}_2$.

Note

An S-box does not have linear factors.

Differential Factors

Definition (Differential Factor)

Let S be a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$. For all $x, y \in \mathbb{F}_2^n$ that satisfy $S(x) \oplus S(y) = \mu$, if we also have $S(x \oplus \lambda) \oplus S(y \oplus \lambda) = \mu$, then we say that the S-box has a *differential factor* λ for the output difference μ. (i.e. μ remains invariant for λ).

Differential Factors

Definition (Differential Factor)

Let S be a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$. For all $x, y \in \mathbb{F}_2^n$ that satisfy $S(x) \oplus S(y) = \mu$, if we also have $S(x \oplus \lambda) \oplus S(y \oplus \lambda) = \mu$, then we say that the S-box has a *differential factor* λ for the output difference μ. (i.e. μ remains invariant for λ).

Example (SERPENT's S_1)

$(\lambda = F, \mu = E)$

x	5	A	8	0	2	1	E	D	F	7	6	9	C	B	3	4
S(x)	0	E	1	F	2	C	3	D	4	A	5	B	6	8	7	9

Differential Factors

Theorem 1

If a bijective S-box S has a differential factor λ for an output difference μ, then S^{-1} has a differential factor μ for the output difference λ.

Differential Factors

Theorem 1

If a bijective S-box S has a differential factor λ for an output difference μ, then S^{-1} has a differential factor μ for the output difference λ.

Proof

Let us assume that S has a differential factor λ for an output difference μ. If $S^{-1}(c_1) \oplus S^{-1}(c_2) = \lambda$ for some c_1 and c_2, then we need to show that $S^{-1}(c_1 \oplus \mu) \oplus S^{-1}(c_2 \oplus \mu) = \lambda$. Let $c_1 \oplus \mu = S(p_1)$ for some p_1, then we have $S(S^{-1}(c_1) \oplus \lambda) \oplus S(p_1 \oplus \lambda) = \mu$ since λ is a differential factor of S for μ. Thus, we have

$$\begin{aligned} S^{-1}(c_1 \oplus \mu) \oplus S^{-1}(c_2 \oplus \mu) &= S^{-1}(S(p_1)) \oplus S^{-1}(S(S^{-1}(c_1) \oplus \lambda) \oplus \mu) \\ &= p_1 \oplus S^{-1}(S(p_1 \oplus \lambda)) \\ &= p_1 \oplus p_1 \oplus \lambda \\ &= \lambda \end{aligned}$$

□

Differential Factors

Definition (Advantage)

If an attack on an m-bit key gets the correct value ranked among the top r out of 2^m possible candidates, we say the attack obtained an $(m - log(r))$-bit *advantage* over exhaustive search.

Differential Factors

Definition (Advantage)

If an attack on an m-bit key gets the correct value ranked among the top r out of 2^m possible candidates, we say the attack obtained an $(m - log(r))$-bit *advantage* over exhaustive search.

Theorem 2

If an input pair provides the output difference μ under a partial subkey k, then the same output difference is observed under the partial subkey $k \oplus \lambda$. Therefore, during a differential attack involving the guess of a partial subkey corresponding to the output difference μ, the advantage of the cryptanalyst reduced by 1 bit and the time complexity of this key guess step is halved.

Differential Factors

Theorem 3

If λ_1 and λ_2 are differential factors for an output difference μ, then $\lambda_1 \oplus \lambda_2$ is also differential factor for the output difference μ. i.e. All differential factors λ_i for μ forms a vector space.

Differential Factors

Theorem 3

If λ_1 and λ_2 are differential factors for an output difference μ, then $\lambda_1 \oplus \lambda_2$ is also differential factor for the output difference μ. i.e. All differential factors λ_i for μ forms a vector space.

Corollary

During a differential attack involving the guess of a partial subkey corresponding to the output difference μ of an S-box that has a vector space of differential factors of dimension r for μ, then advantage of the cryptanalyst is reduced by r bits and the time complexity of the key guess step is reduced by a factor of 2^r.

Cryptographic Algorithms with Differential Factors

4×4 S-boxes with Differential Factors

- We observed 40 out of 102 S-boxes contain 74 differential factors
  1. DES
  2. GOST
  3. Hamsi
  4. LED
  5. LBLOCK
  6. LUFFA
  7. NOEKEON
  8. Piccolo
  9. PRESENT
  10. RECTANGLE
  11. SARMAL
  12. SERPENT
  13. SPONGENT
  14. Twofish

Cryptographic Algorithms with Differential Factors

3×3 S-boxes with Differential Factors

Among the $2^3! = 40320$ different bijective 3×3 S-boxes, 29568 of them contains differential factors (73.3%).

- 1344 of them contain 49
- 9408 of them contain 25
- 18816 of them contain 9

Cryptographic Algorithms with Differential Factors

3×3 S-boxes with Differential Factors

Among the $2^3! = 40320$ different bijective 3×3 S-boxes, 29568 of them contains differential factors (73.3%).

- 1344 of them contain 49
- 9408 of them contain 25
- 18816 of them contain 9

8×8 S-boxes with Differential Factors

1. CRYPTON (old version)

Cryptographic Algorithms with Differential Factors

3×3 S-boxes with Differential Factors

Among the $2^3! = 40320$ different bijective 3×3 S-boxes, 29568 of them contains differential factors (73.3%).

- 1344 of them contain 49
- 9408 of them contain 25
- 18816 of them contain 9

8×8 S-boxes with Differential Factors

1. CRYPTON (old version)

Differential-Linear Attacks on SERPENT

Differential-linear attacks of Dunkelman at al. on 10, 11, and 12-round SERPENT overlook the differential factors of S_0 and S_1 of SERPENT. We reduced the time complexities of these attacks by a factor of 2, 2, and 4, respectively.

Differential-Linear Attacks on SERPENT

Differential-Linear Cryptanalysis

- Langford and Hellman combined differential and linear cryptanalysis in 1994
- Biham-Dunkelman-Keller enhanced this technique in 2002 by showing that the differential does not need to hold with probability 1

Differential-Linear Attacks on SERPENT

Differential-Linear Cryptanalysis

- Langford and Hellman combined differential and linear cryptanalysis in 1994
- Biham-Dunkelman-Keller enhanced this technique in 2002 by showing that the differential does not need to hold with probability 1

Differential-Linear Attacks on SERPENT

Biham, Dunkelman and Keller attacked 11-round SERPENT-192 and SERPENT-256 by combining the 3-round differential

$$\Delta : 00000000000000000000000040050000 \rightarrow 0??00?000?00000000?00?0??0??0?0$$

that has a probability of $p = 2^{-7}$ with the 6-round linear approximation

$$\Lambda : 20060040000001001000000000000000 \rightarrow 00001000000000005000010000100001$$

that has bias $q = 2^{-27}$.

Differential-Linear Attacks on SERPENT

Differential-Linear Attacks on SERPENT

- The first attack on 10-round SERPENT-128 is also presented by Biham, Dunkelman and Keller by removing the last round of the linear approximation.

Differential-Linear Attacks on SERPENT

Differential-Linear Attacks on SERPENT

- The first attack on 10-round SERPENT-128 is also presented by Biham, Dunkelman and Keller by removing the last round of the linear approximation.
- These attacks are further improved by Dunkelman, Indesteege and Keller by using the following improvements:
  1. Better analysis of the bias of the differential-linear approximation
  2. Better analysis of the success probability
  3. Changing the output mask
- These reduced complexities are also used to extend the 11-round attack and provide the first 12-round attack on SERPENT-256.

Differential-Linear Attacks on SERPENT

Differential-Linear Attacks on SERPENT

- The first attack on 10-round SERPENT-128 is also presented by Biham, Dunkelman and Keller by removing the last round of the linear approximation.
- These attacks are further improved by Dunkelman, Indesteege and Keller by using the following improvements:
  1. Better analysis of the bias of the differential-linear approximation
  2. Better analysis of the success probability
  3. Changing the output mask
- These reduced complexities are also used to extend the 11-round attack and provide the first 12-round attack on SERPENT-256.

Warning

Advantages and time complexities of these attacks are incorrect due to differential factors.

Differential Factors of SERPENT

Table : Differential Factors of SERPENT

S-box	λ	μ
SERPENT S_0	4_x	4_x
SERPENT S_0	D_x	F_x
SERPENT S_1	4_x	4_x
SERPENT S_1	F_x	E_x
SERPENT S_2	2_x	1_x
SERPENT S_2	4_x	D_x
SERPENT S_6	6_x	2_x
SERPENT S_6	F_x	F_x

Improved Attacks on SERPENT

Table : 12-round differential-linear attack of Dunkelman et al. Output differences μ that contain differential factors, which are 4_x and E_x for S_1 and 4_x for S_0, are shown in bold. Undisturbed bits are shown in italic.

Input	X_0:	????	????	0???	0???	????	????	????	00??
	X_1:	????	????	0???	0???	????	????	????	00??
	X_2:	????	????	0???	0???	????	???*1*	????	00??
	X_3:	????	????	0???	0???	????	????	????	00??
S_0	X_0:	??0?	00?0	0000	0?00	00?0	000**0**	00??	00??
	X_1:	??0?	????	00?0	0???	0???	???**0**	0?00	0000
	X_2:	000?	00??	0??0	0?00	??00	?00**1**	0?00	0000
	X_3:	?0??	?0??	00??	0???	??0?	0??**0**	?001	0000
LT	X_0:	?000	0000	0000	0??0	0?00	?000	0000	0000
	X_1:	?000	0000	0000	0??0	0?00	?000	0000	0000
	X_2:	?000	0000	0000	0??0	0?00	?000	0000	0000
	X_3:	?000	0000	0000	0*1*?0	0?00	*1*000	0000	0000
S_1	X_0:	0000	0000	0000	0100	0**0**00	**0**000	0000	0000
	X_1:	1000	0000	0000	0010	0**1**00	**0**000	0000	0000
	X_2:	0000	0000	0000	0000	0**1**00	**1**000	0000	0000
	X_3:	0000	0000	0000	0010	0**1**00	**0**000	0000	0000
LT	X_0:	0000	0000	0000	0000	0000	0000	0001	0000
	X_1:	0000	0000	0000	0000	0000	0000	0000	0000
	X_2:	0000	0000	0000	0000	0000	0000	1001	0000
	X_3:	0000	0000	0000	0000	0000	0000	0000	0000
9-Round Differential-Linear Characteristic $\Delta \circ \Lambda$									
Last Round									

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%**	**Tezcan et al.**
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	48	84%	Dunkelman et al.
10	**Differential-Linear**	**All**	$\mathbf{2^{101.2}}$ **CP**	$\mathbf{2^{114.2}}$ **En**	$\mathbf{2^{40}}$ **B**	**47**	**84%**	**LightSEC'14**
10	**Differential-Linear**	**All**	$\mathbf{2^{100.55}}$ **CP**	$\mathbf{2^{117.55}}$ **En**	$\mathbf{2^{40}}$ **B**	**51**	**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**	$\mathbf{2^{134.7}}$ **MA**	$\mathbf{2^{76}}$ **B**	**47**	**84%**	**LightSEC'14**
11	**Differential-Linear**	**192**	$\mathbf{2^{121.15}}$ **CP**	$\mathbf{2^{138.05}}$ **MA**	$\mathbf{2^{76}}$ **B**	**51**	**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**	$\mathbf{2^{247.4}}$ **En**	$\mathbf{2^{128.5}}$ **B**	**158**	**84%**	**LightSEC'14**

Summary

Summary

1. Introduced a new S-box evaluation criteria: *Differential Factors* (mostly observed in small S-boxes like 3×3 and 4×4)
2. Corrected and improved the best differential-linear attacks on SERPENT

Note

Time complexities and advantages of the previous differential attacks on ciphers with differential factors may be wrong

Thanks

Thank You for Your Attention