Narrow Sense Linear Cryptanalysis of a Family of Modified DES Ciphers with Even Weight S-boxes

Robert Tsenkov
Institute of Mathematics and Informatics, Bulgarian Academy of Sciences

Joint work with Yuri Borissov

ACCT 2016 – Albena, Bulgaria, June 18-24, 2016

Motivation

LINEAR CRYPTANALYSIS exploits LINEARITY.

S-BOX presumes NONLINEARITY.

EVEN WEIGHT CODE presumes LINEARITY.

However, an S-box of this kind possesses single error-detection capability and therefore it is immune (to a certain extent) against fault-injection attacks during the execution time of the algorithm. In addition, such S-box satisfies automatically the criteria concerning spectrum of Hamming distances between its outputs, relevant in case of differential cryptanalysis.

The question: Can we say something additional about

EVEN WEIGHT S-BOXES ?

Contents

- Notations and Definitions.
- Our (General) Experiment.
- Previous Results.
- Some references.
- Current experiment.
- Analysis for Small Number of Rounds.
- Results for Many Rounds.
- Conclusions.

Notations and Definitions (1)

- Linear Cryptanalysis:

$$\mathbf{P}[I_P] + \mathbf{C}[I_C] = \mathbf{K}[I_K]$$

  $\mathbf{P}, \mathbf{C}$, $\mathbf{K}$ – Plaintext, Ciphertext, Key;
  $\mathbf{B}[I_B] = B_{b_1} \oplus B_{b_2} \oplus \cdots \oplus B_{b_m}$, $I_B = \{b_1, b_2, \ldots, b_m\}$.

- $(I_X(j), I_F(j))$ – *1-round linear characteristic* for round j;
  X, F – the round input and output.

- $((I_X(1), I_F(1)), \ldots, (I_X(n), I_F(n)))$ – *n-round linear characteristic*.

- Every characteristic is associated with the probability of coincidence of the sums of the input bits and the output bits, determined by the characteristic.

Notations and Definitions (2)

- For given $m \times n$ S-box S_k regarded as mapping $S_k : \mathbf{F_2}^m \mapsto \mathbf{F_2}^n$, and given integers α and β, such that $0 \leq \alpha \leq 2^m - 1$ and $0 \leq \beta \leq 2^n - 1$, let $NS_k(\alpha, \beta)$ be the number of times when the XOR-sum of the input bits masked by α coincides with the XOR-sum of the output bits masked by β. The table, where the vertical and the horizontal axes indicate α and β respectively, and each entry contains the "centered" value

$$\mathcal{L}S_k(\alpha, \beta) = NS_k(\alpha, \beta) - 2^{m-1}$$

is referred to as *Linear Approximation Table* (*LAT*) for the S-box S_k.

Notations and Definitions (3)

- If a linear approximation holds with probability $p \neq 1/2$ for randomly given plaintext P and the corresponding ciphertext C, the absolute value of the *bias* $p - 1/2$ represents the *effectiveness* of that approximation.

- A linear characteristic is called *best characteristic* when the effectiveness of corresponding linear approximation is maximal.

Our (General) Experiment

- Use of Data Encryption Standart (DES) cipher as base cipher.
- Precoding of the output of each S-box of the DES into an even-weight code of length 4 by embedding a parity bit.
- Use of classical technics (Matsui 1993,1994) for linear cryptanalysis.
- Study of the best characteristics, based on at most one active S-box per round ("narrow sense" linear cryptanalysis) for different number of rounds (up to 20).
- Comparison of the results obtained to that for the original cipher.

Additional notations: $\mathcal{L}S_k(\pi;\alpha,\beta)$ – the deviations, when parity bit mask π is applied to S_k.

Previous Results (1)

The first experimental cryptanalytic attack on DES (Matsui, 1994)

- Based on linear approximations, derived from the best 14-round characteristics, based on at most one active S-box per round. (the type, we examine!)
- The result: DES is breakable with complexity 2^{43} at success rate of 85% if 2^{43} known plaintexts are available.
- The complexity of such kind of attacks practically depends only on the effectiveness e of the approximations used and the participating output bits from the first and the last rounds.
- The number of the necessary plaintext/ciphertext pairs is proportional to e^{-2}.

Previous Results (2)

LAT Properties

- *(Matsui, 1993)*

  (i) $\mathcal{L}S_k(\alpha, \beta)$ is even.

  (ii) If $\alpha = 1, 32$ or 33, then $\mathcal{L}S_k(\alpha, \beta) = 32$ for all S_k and β.

- *(Borissov, Boyvalenkov, Tsenkov, 2016)*

  Let parity bit with mask π is embedded in the S-box S_k.
  If $\alpha, \beta \neq 0$ and '$\&$' denotes tuple-wise AND operator, then:

  (iii) $\mathcal{L}S_k(\pi; \alpha, \beta) = \mathcal{L}S_k(\alpha, \beta)$ for all α and β such that $\beta \& \pi = 0$;

  (iv) $\mathcal{L}S_k(\pi; \alpha, \beta) = \mathcal{L}S_k(\alpha, 15 - \beta)$ for all α and $\beta < 15$ such that $\beta \& \pi \neq 0$;

  (v) $\mathcal{L}S_k(\pi; \alpha, 15) = 0$ for all α.

Previous Results (3)

Borissov, Boyvalenkov, Tsenkov, 2016

- Under the assumption $\pi_1 = \pi_2 = \ldots = \pi_8 = \pi$, i.e. the same parity mask is applied to all S-boxes (restrictive conditions!).
- **Theorem 1.** Every parity mask applied to the S-boxes of the DES leads to a reduction of the maximal effectiveness for the 1-round and 3-round versions of that cipher.
- **In the general multi-round case:** LC against the modified ciphers has varying magnitude of complexity depending on the parity position chosen. The complexity of successful linear attacks mainly increases, but also diminishes in a few cases, comparing to the original cipher.

Previous Results (4)

Borissov, Boyvalenkov, Tsenkov, 2016

- Use of our own algorithm for construction of "valid" multi-round linear characteristics, optimized and adapted to work with the modified ciphers, too. Implemented in C++.
- Basic Search Algorithm (BSA):
  Phase I: Initialization.
  Input: Empty sequence.
  Output: Completely constructed $I_F(1)$, $I_X(1)$ and $I_F(2)$ and partially constructed $I_X(2)$.
  Phase II: Round chaining. (one step; executed for $j = 2, 3, \ldots, n-1$)
  Input: Completely constructed $I_F(j-1)$ and $I_F(j)$ and partially constructed $I_X(j)$.
  Output: Completely constructed $I_X(j)$ and $I_F(j+1)$, partially constructed $I_X(j+1)$ if $j+1 < n$ and completely constructed $I_X(j+1)$ if $j+1 = n$.

Some references

- M. Hellman, R. Merkle, R. Schroeppel, L. Washington, W. Diffie, S. Pohlig, P. Schweitzer: *Results of an initial attempt to cryptanalyze the NBS Data Encryption Standard,* SEL 76-042, Sept. 9, 1976.
- K. Nyberg, *On the construction of highly nonlinear permutation,* EUROCRYPT'92: Springer LNCS 658, pp. 92-98, 1993.
- M. Matsui: *Linear cryptanalysis of DES cipher (I), version 1.03.* Available from http://www.cs.bilkent.edu.tr/~selcuk/teaching/cs519/Matsui-LC.pdf.
- D. Coppersmith: *The Data Encryption Standard (DES) and its strength against attacks,* IBM Journal of Research and Development 38(3), pp. 243-250 (1994).
- A.G. Konheim: *Computer Security and Cryptography.* John Wiley & Sons Inc., New Jersey, 2007.
- [BorBoyTse'2016] Y. Borissov, P. Boyvalenkov, R. Tsenkov: *Linear cryptanalysis and modified DES with parity check in the S-boxes,* Second Conference on Cryptography and Information Security in the Balkans: Springer LNCS 9540, pp. 60 - 78, 2016.

Current Experiment

- Relaxing the conditions: parity position for each individual S-box is chosen independently at random $\rightarrow$ extending the family of ciphers.
- Search for optimality (optimal parity masks configurations).
- Two directions of optimality:
  (i) better conditions for attacking;
  (ii) higher resistance against linear attacks.

Analysis for Small Number of Rounds (1)

- Distinguishing of a special kind of elements.

  Definition. The entry $\mathcal{L}S_k(\alpha, \beta)$, $1 \leq \alpha \leq 63$, $1 \leq \beta \leq 14$, from the LAT of an S_k of the DES is called *invariant when applying parity check* (or simply *invariant*) if

  $$|\mathcal{L}S_k(\alpha, \beta)| = |\mathcal{L}S_k(\pi; \alpha, \beta)|$$

  for each parity mask π.

- **Proposition.** Let I be the set of all invariant entries from LATs, $M_I := \max_{\mathcal{L} \in I} |\mathcal{L}|$ and π_k be a parity mask applied to S_k of the DES, $1 \leq k \leq 8$. Then

  $$\max_{k,\alpha,\beta} \left\{ |\mathcal{L}S_k(\pi_k; \alpha, \beta)| \right\} \geq M_I.$$

Analysis for Small Number of Rounds (2)

- **Theorem 2.** Let π_7 be the parity mask applied to the S-box S_7 of the DES. Then:

  (i) The maximal possible effectiveness of the best 1-round characteristics for modified DES cipher is obtained iff $\pi_7 \neq 4$. There are exactly two elements of the LATs in this case possessing the highest magnitude 18.

  (ii) If $\pi_7 = 4$ then the effectiveness of the best 1-round characteristics for such a DES-like cipher is of minimal possible value equal to 0.25.

  (iii) The corresponding extremal effectiveness of the best 3-round characteristics is achieved at the same assumptions. These effectiveness are $2(18/64)^2 \approx 0.1582$ and 0.1250, respectively.

- **Note.** Every parity masks combination is optimal in one of the two directions!

Results for Many Rounds (1)

- Optimisation tasks:

$$\max_{\overline{\pi}} \max_{l} \{e(l)\} \qquad \min_{\overline{\pi}} \max_{l} \{e(l)\}$$

  where $e(l)$ denotes the effectiveness of the linear characteristic l and $\overline{\pi} = (\pi_1, \pi_2, \ldots, \pi_8)$.

- An exhaustive search has been made by computer.

- Our own algorithm for construction of "valid" characteristics from [BorBoyTse'2016] is used.

Results for Many Rounds (2)

Summary of the results:

- For small number of rounds (3 rounds): agreement with Theorem 2.
- Comparing to DES:

  (i) The common tendency is the modified ciphers to have better resistance towards narrow sense LC. A few exceptions exist only in some cases for 5,14,17 and 18-round versions.

  (ii) By independent choice of parity positions we can construct ciphers with better resistance towards linear attacks for any number of rounds.
- Comparing to [BorBoyTse'2016]:

  (i) Ciphers providing favorable opportunities for linear attacks exist for 4, 5 and 6-round versions only.

  (ii) By independent choice of parity positions we can construct ciphers with better resistance for most of the cases, except for 3,7,13,14,17 and 20-round versions, where the best maximal effectiveness coincides.

Conclusions

- Presumably, by their construction the examined ciphers are suspected to be more vulnerable in linear attacks. It turns out that this is not true and their vulnerability strongly depends on the parity bit positions. Moreover, in most cases (regarding the DES) they possess even better resistance than the original cipher.
- Due to the invariant property, the resistance against LC for small number of rounds can be analysed without computer assistance.
- However, before final recommendation, the resistance of these ciphers against other known forms of linear cryptanalysis should be investigated.

THANK YOU FOR YOUR ATTENTION !