New Results in the Linear Cryptanalysis of DES

Igor Semaev

AG15
August 7, 2015
Outline

- Basics of linear cryptanalysis: approximations, Matsui’s algorithms
- Using multiple approximations
- New approach:
  - Reduction to solving a system of equations
- Success probability
Known plain-text attack

- Encryption equation
  \[ E_K(P_i) = C_i \]
  - Plain-text \( P_i \), cipher-text \( C_i \), key \( K \)
  - Given \( P_i, C_i, i = 1, \ldots, n \)
  - Find \( K \)
A priory Approximation

- $\Phi(P_i, C_i, K) = 0$
- with probability $p = 1/2 + \delta$
- $\delta \neq 0$
Linear Approximation

- $\Phi(P_i, C_i, K) = l_1(P_i, C_i) \oplus l_2(K) = 0$
- $l_1, l_2$ linear functions
- holds with probability $p$
- **Matsui’s Algorithm 1:**
  - find effective key bit $l_2(K)$ to fit the probability
  - brute force the rest of the key (search phase)
- Success probability by CLT
Approximation in Round Ciphers

- By eliminating last round,

\[ l_1(P_i, C_i) \oplus l_2(K) \oplus R'(C_i, \text{last round key}) = 0 \]

- more biased: \(|\delta|\) increases

- **Matsui’s Algorithm 2:**
- test

\[ l_2(K), \text{effective last round key-bits} \]

  to fit the probability

- (rank effective key-bit values)

- brute force the rest of the key(search phase)
Success Probability with one Approximation

- heuristic argument in Matsui’s
- theory-based by Selçuk, 2007
Approximation in Round Ciphers

- By eliminating first and last rounds

\[ l_1(P_i, C_i) \oplus l_2(K) \oplus R(P_i, \text{first round key}) \oplus R'(C_i, \text{last round key}) = 0 \]

- significantly more biased
- **Matsui’s Algorithm 2:**
  - test
    \[ l_2(K), \text{effective first and last round key-bits} \]
  to fit the probability
- brute force the rest of the key (search phase)
Multiple Approximations

- $\Phi_i(\text{Data}, K^i) = 0$ with probability $p_i = 1/2 + \delta_i$
- $i = 1, \ldots, N$
- Data - plain-text/cipher-text bits
- $K^i$ key-bits or linear combinations
Matsui’s Linear Cryptanalysis with 2 approximations

- $\Phi_i(\text{Data, } K^i) = 0, i = 1, 2$ with probability $1/2 - 1.19 \times 2^{21}$
- Rank separately $K^1 = k_1$ and $K^2 = k_2$
- Rank $(k_1, k_2)$ by an heuristic
- For $2^{13}$ highest rank pairs, solve
  \[
  \begin{pmatrix}
  K^1 \\
  K^2
  \end{pmatrix}
  = 
  \begin{pmatrix}
  k_1 \\
  k_2
  \end{pmatrix}
  \]
  in 26 effective key-bits
- Brute force the rest $30 = 56 - 26$
Matsui Linear Cryptanalysis with 2 approximations

- with $n = 2^{43}$ plain-text/cipher-text blocks
- Overall complexity $2^{43}$ DES encryptions
- Success probability is 0.85 by an heuristic argument
Linear Cryptanalysis with \( N > 2 \) approximations

- \( \Phi_i(\text{Data}, K^i) = 0 \) with probability \( p_i = 1/2 + \delta_i \)
- \( i = 1, \ldots, N \)
- Known solutions work for
  - \( K^1 = \ldots = K^N \) or \( K^1, \ldots, K^N \) are linearly independent
  - In practice, \( K^1, \ldots, K^N \) are different and linearly dependent
- How to merge data from different approximations efficiently?
- How to compute success probability, given the number of plain-texts and the number of trials in the search phase?
New Approach

- First, reject $K^i = k$ which are unlikely correct
- Technically: define $C(x_i)$, depends on a parameter $x_i$
- to test $K^i = k$
- Count $\nu = \# \{ \Phi_i(Data, k) = 0 \}$
- Decide $K^i \neq k$ if $\nu \in C(x_i)$
Construct and Solve MRHS equations

- Second, construct

\[ K^i \in \{ \text{accepted } k \} \]

- called MRHS equation in Raddum-Semaev, 2007

- \( i = 1, \ldots, N \). That is an equation system

- Third, get by Gluing

\[ \bar{K} \in \{ k_1, \ldots, k_s \} \]

- \( \bar{K} \) a new string of key-bits or linear combinations

- No additional memory. Average complexity is \( O(s) \), negligible

- Finally, for each \( k_j \), solve \( \bar{K} = k_j \)

- Brute force each solution
Complexity vs Success Probability

- For $i$-th approximation

  \[ K^i \in \{ \text{accepted} \quad k \} \]

- Incorrect $k$ appears with probability $1 - \alpha_i$

  \[ \alpha_i = \alpha(x_i, p_i) = \Pr(K^i \neq k | K^i \neq k) \]

- Correct $k$ appears with probability $1 - \beta_i$

  \[ \beta_i = \beta(x_i, p_i) = \Pr(K^i \neq k | K^i = k) \]
Complexity vs Success Probability

- In the final equation

\[ \bar{K} \in \{k_1, \ldots, k_s\} \]

- Most of incorrect \( k \) appear with probability

\[ \prod_{i=1}^{N} (1 - \alpha_i) \]

- Correct \( k \) appears with probability

\[ \prod_{i=1}^{N} (1 - \beta_i) \]
Construct equations

- Average number of sides in the final equation
  \[ s \approx 2^{\text{rank}(\tilde{K})} \prod_{i=1}^{N} (1 - \alpha_i) \]

- The number of trials in the search phase
  \[ 2^{|K|} \prod_{i=1}^{N} (1 - \alpha_i) \]

- Success probability
  \[ \prod_{i=1}^{N} (1 - \beta_i) \]

- both depend on \( x_1, \ldots, x_N \)
Optimisation problem

- We want $2^{K-t}$ trials on the average in the search phase and maximal success probability
- Find $x_i$ such that
  \[ \prod_{i=1}^{N} (1 - \alpha_i) = 2^{-t} \]
- to maximise
  \[ \prod_{i=1}^{N} (1 - \beta_i) \]
DES with 10 Approximations

- with $2^{43}$ plain-text/cipher-text blocks
- Overall complexity $2^{43}$ DES encryptions
- Success probability is 0.89 proved under natural assumptions
- Checked experimentally for 8-round DES
- To compare: 0.85 for 2 approximations by an heuristic argument
Conclusion

- New method for multiple approximations
- With predictable success probability
- Applicable to any cipher
- There is room for extensions