Cryptanalysis of Block Ciphers via Decoding of Long Reed-Muller Codes

Ilya Dumer, Rafaël Fourquet and Cédric Tavernier

Univ. of California, Riverside, USA

Univ. Paris 8, France

Emirates Advanced Investment, U.A.E

ACCT 2010

Introduction

Reconstruction of the key

Decoding of RM codes with repeated symbols

Introduction

- Linear Cryptanalysis: powerful tool in the analysis of block ciphers (Matsui, 1993)
- *Step 1:* finding **linear relations** involving **key**, **plaintext** and **ciphertext** bits with probability $1/2 + \varepsilon$
- *Step 2:* using these relations and a sample of plaintext-ciphertext pairs to recover some key bits.
- *data complexity*: $\mathcal{O}(1/\varepsilon^2)$
- reducing this data-complexity:
  - multiple linear relations: Kaliski-Robshaw (1994), Biryukov-De Cannière-Quisquater (2004), Gérard-Tillich (2007), Fourquet-Loidreau-Tavernier (2009)
  - non-linear relations: Knudsen-Robshaw (1996), Shimoyama-Kaneko (1998), Tokareva (2008)

Proposed Algorithm: given non-linear (low order) relations between plaintext, ciphertext and key bits, reconstruct the key bits (Step 2).

- this reconstruction is translated to a soft decoding problem in the Reed-Muller (RM) codes, with *repeated symbols* .
- these codes can be decoded with quasi-linear complexity
- it is a general purpose algorithm
- it is hard to find non-linear approximations satisfying the error-probability threshold allowed by this algorithm.
- any decoding algorithm may be used (e.g. in RM codes of order 2)

Block Ciphers

- A block cipher is a vectorial Boolean function:

$$\begin{array}{rcccccc} E: & \mathbb{F}_2^u & \times & \mathbb{F}_2^v & \longrightarrow & \mathbb{F}_2^w \\ & (X & , & K) & \longmapsto & Y = E(X,K) \end{array}$$

  $X = (X_1, \ldots, X_u)$: plaintext
  $K = (K_1, \ldots, K_v)$: key
  $Y = (Y_1, \ldots, Y_w)$: ciphertext

- A relation between X, K and $Y = E(X,K)$ with bias $0 < \varepsilon \leq 1/2$ is given by a Boolean function $F : \mathbb{F}_2^{u+v+w} \to \mathbb{F}_2$ such that:

$$F(X,K,Y) = 0 \text{ with probability } 1/2 + \varepsilon$$

- *Linear* cryptanalysis: F is a linear function
- for clarity, we consider $F : \mathbb{F}_2^{u+v} \to \mathbb{F}_2$ and $G : \mathbb{F}_2^w \to \mathbb{F}_2$ such that

$$F(X,K) = G(E(X,K)) \text{ with probability } 1/2 + \varepsilon$$

Reconstruction of the key

Notation: for $i = (i_1, \ldots, i_u) \in \mathbb{F}_2^u$ and $j = (j_1, \ldots, j_v) \in \mathbb{F}_2^v$:

$$X^i := X_1^{i_1} X_2^{i_2} \cdots X_u^{i_u} \quad \text{and} \quad K^j := K_1^{j_1} K_2^{j_2} \cdots K_v^{j_v}$$

Let F have the following polynomial representation:

$$\begin{aligned} F(X, K) &= \sum_{i,j} a_{i,j} X^i K^j \in \mathbb{F}_2[X, K] \\ F_K(X) &= \sum_i (\sum_j a_{i,j} K^j) X^i \in \mathbb{F}_2[X] \quad \text{when K is fixed} \end{aligned}$$

with $a_{i,j} \in \mathbb{F}_2$.

Using a sample of plaintext-ciphertext pairs associated with a fixed key $\bar{K}$, we will reconstruct the polynomial $F_{\bar{K}}(X) = F(X, \bar{K})$

$\longrightarrow$ this gives the coefficients of the form $\sum_j a_{i,j} K^j$.

RM codes with repeated symbols

For complexity reasons, we will assume that:

- $F_K(X)$ depends on a small number $u' \ll u$ of variables, say $X_1, \ldots, X_{u'}$.
  For $X \in \mathbb{F}_2^u$, let $X' = (X_1, \ldots, X_{u'})$.
- The degree h of $F_K(X)$ is small.

$$F_K(X) = F_K(X') \in \mathrm{RM}(h, u').$$

Moreover, we assume that, when K is fixed, the relation between $F_K(X)$ and $E_K(X) = E(X, K)$ still holds:

$$\Pr_X[G(E_K(X)) = F_K(X')] = \frac{1}{2} + \varepsilon$$

$$\Pr_X[G(E_K(X)) = F_K(X')] = \frac{1}{2} + \varepsilon$$

Let S be a sample of size L of plaintext-ciphertext pairs $(X, Y = E_K(X))$ associated with the key K.

For $x \in \mathbb{F}_2^{u'}$, let

$$S_x = \{(X, Y) \in S | X' = x\},$$

of size L_x ($\sum_{x \in \mathbb{F}_2^{u'}} L_x = L$).

- *$F_K(X') \in \mathrm{RM}(h, u')$ is transmitted L_x times at position $x \in \mathbb{F}_2^{u'}$ over a channel with error probability $1/2 - \varepsilon$,*

with received symbols $(G(Y))_{(X,Y) \in S_x}$:

$$\text{position } x \text{ of } F_K(X') \overset{p=1/2-\varepsilon}{\longrightarrow} (G(Y))_{(X,Y) \in S_x}$$

Recovering the key bits

Let s_x be the Hamming weight of $(G(Y))_{(X,Y)\in S_x}$. We form the vector:

$$(s_1, s_2, \ldots, s_{2^{u'}})$$

We construct the received vector y of length $2^{u'}$ with "hard decoding": at position x, we set

$$y_x = \begin{cases} 0 & \text{if } s_x < L_x/2 \\ 1 & \text{otherwise} \end{cases}$$

Then, the vector y is decoded into the codeword $F_K(X') \in \mathrm{RM}(h, u')$ $\longrightarrow$ we obtain the coefficients $\sum_j a_{i,j} K^j$.

An example

Let

$$F(X,K) = X_1K_2 + X_2K_4 + X_3K_1K_5 + K_1$$

be an approximation of $G(E(X,K))$, with $X, K, Y = E(X,Y) \in \mathbb{F}_2^{64}$.
Here $u' = 3$, $X' = (X1, X2, X3)$, $\deg(F_K(X)) = 1 \Rightarrow F_K(X) \in \mathrm{RM}(1,3)$.
Using a sample S of plaintext-ciphertext pairs, we construct the "received" vector y as above:

$$y = (y_1, \ldots, y_8)$$

To reconstruct $F_K(X)$, we decode y into the nearest affine function

$$A(X') = a_0 + a_1X_1 + a_2X_2 + a_3X_3 \in RM(1,3)$$

which maximizes the quantity $\sum_x (-1)^{y(x)+A(x)}$ (FFT).
Then we obtain:

$$K_1 = a_0, K_2 = a_1, K_4 = a_2 \text{ and } K_1K_5 = a_3.$$

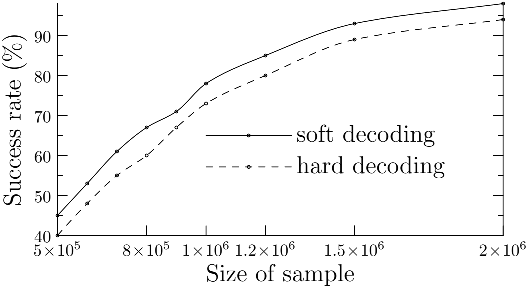
Example of the DES

The DES is a block-cipher with plaintext, ciphertext and key of size 64 bits. We found 20 quadratic approximations of the 8-round DES, with biases $\varepsilon \approx 0.001$. They all imply 6 bits of the key, and are of the form:

$K_9 + K_4K_{13} + K_{15} + K_4K_{15} + K_{13}K_{30} + K_{31} + K_{33} + K_{41} + K_{44} + K_4K_{47} + K_{30}K_{47} + K_{52} + K_{54} + K_{15}K_{54} + K_{47}K_{54} + X_{47} + X_0 + K_{15}X_0 + K_{47}X_0 + X_7 + X_{18} + X_{24} + K_4X_{27} + K_{30}X_{27} + K_{54}X_{27} + X_0X_{27} + X_{28} + K_4X_{28} + K_{54}X_{28} + X_0X_{28} + X_{29} + K_{13}X_{29} + K_{15}X_{29} + K_{47}X_{29} + X_{27}X_{29} + X_{28}X_{29} + K_{13}X_{30} + K_{47}X_{30} + X_{27}X_{30} + K_4X_{31} + K_{30}X_{31} + X_{29}X_{31} + X_{30}X_{31} = Y_{12} + Y_{16} + Y_{39} + Y_{50} + Y_{56}$.

$\longrightarrow$ results similar to using multiple linear relations.

Success rate (all 6 key bits are recovered) of the cryptanalysis:



Introduction

Reconstruction of the key

Decoding of RM codes with repeated symbols

Decoding of RM codes with repeated symbols

Recall the results of I. Dumer ("Soft decision decoding of Reed-Muller codes: a simplified algorithm", *IEEE* 2006):

Theorem

Consider long codes $\mathrm{RM}(r,m)$ *such that* $\frac{(m-r)}{\ln m} \to \infty$ *as* $m \to \infty$. *Then these codes can be decoded on a* BSC_p *with complexity of order* $(3n\log_2 n)/2$, *and have a vanishing output block error probability if* $p \leq 1/2 - \varepsilon_1$, *where*

$$\varepsilon_1 = 2\left(\frac{4m}{d}\right)^{1/2^r}. \tag{1}$$

Now, every codeword is transmitted L times over the same binary symmetric channel BSC_p with an error probability $p = 1/2 - \varepsilon$.
In the case of hard decoding, the above theorem gives the following improved threshold:

$$\varepsilon_L = 2\sqrt{\frac{2}{L}}\left(\frac{4m}{d}\right)^{1/2^r}. \tag{2}$$

A soft-decision version

Instead of the hard decoding, we use a soft version approach. Each symbol c_x of a code $\mathrm{RM}(r, m)$ is transmitted L times and is received as some vector g_x of length L and Hamming weight s_x.
For all s, we have:

$$Q(s) := \Pr[s_x = s | c_x = 0] = \binom{L}{s} p^s q^{L-s},$$
$$P(s) := \Pr[s_x = s | c_x = 1] = \binom{L}{s} q^s p^{L-s},$$

Then using the Bayes formula:

$$\Pr[c_x = 0 | s_x] = \frac{Q(s_x)}{P(s_x) + Q(s_x)}$$
$$\Pr[c_x = 1 | s_x] = \frac{P(s_x)}{P(s_x) + Q(s_x)}$$

The received soft-vector $y \in \mathbb{R}^{2^{u'}}$ will be constructed at position x as follows:

$$y_x = \Pr[c_x = 0|s_x] - \Pr[c_x = 1|s_x] = \frac{Q(s_x) - P(s_x)}{P(s_x) + Q(s_x)}$$

With this setting, the decoding threshold is further improved:

Theorem

Consider long codes $\mathrm{RM}(r, m)$ *such that* $\frac{(m-r)}{\ln m} \to \infty$ *as* $m \to \infty$*. Then an* L*-repeated RM code can be decoded on a* BSC_p *with a vanishing output error probability if* $p \leq 1/2 - \varepsilon_L$*, where*

$$\varepsilon_L = \frac{2}{\sqrt{L}} \left(\frac{4m}{d}\right)^{1/2^r} = \frac{\varepsilon_1}{\sqrt{L}}. \tag{3}$$