Separable Statistics in Linear Cryptanalysis

S. Fauskanger and I. Semaev

August 8, 2017

Let $\mathtt{x}$ be a vectorial random variable. In a cryptanalysis based on generalisations of Matsui's Algorithm 2 the variable $\mathtt{x}$ incorporates some bits of the encryption first round output and some bits of the last round input. As $\mathtt{x}$ depends on the cipher key, there is a huge variety of possible distributions to $\mathtt{x}$. So one can only compute an approximation to the distribution of $\mathtt{x}$. It may depend on a relatively low number of the key-bits(linear combination of the key-bits) denoted $\mathtt{key}$. On the other hand, the observation on $\mathtt{x}$ depends on the available plain-text/cipher-text blocks and a number of the key-bits from the first and the last round keys. Let's denote those key-bits by $\mathtt{Key}$. In theory, one can apply a multivariate variation of Matsui's linear cryptanalysis developed by Baign et al., Hermelin et al. by using LLR (logarithmic likelihood ratio) statistic, which depends on both a priori distribution and observation, and therefore on $\bar{K} = \mathtt{key}, \mathtt{Key}$. That may not be efficient if the size(rank) of $\bar{K}$ is large. The latter always happens due to the diffusion in the first and the last rounds if the size of $\mathtt{x}$ is large enough. One is to run over $2^{rank(\bar{K})}$ values of the statistic to range the values of $\bar{K}$ and to get $\bar{K}$-candidates to be brute forced.

The distribution of the projections(functions) $h_i(\mathtt{x})$ and observations on them may depend on a much lower number of the key-bits $\bar{K}_i = \mathtt{key}_i, \mathtt{Key}_i$. At least that holds for DES. The sub-keys $\bar{K}_i$ which affect the distributions and the observations for the projections h_i may partly coincide or be linearly dependent. In this talk we first show how to compute an approximate a priori distribution of multivariate random variables $\mathtt{x}$ constructed with internal bits of DES-type encryption. Second, we demonstrate how by observing the values of several projections $h_i(\mathtt{x})$ reconstruct a set of $\bar{K}$-candidates which contains the correct value with a prescribed success probability. We will answer what the size of that set is. That defines the complexity of the attack.

Let the observation $x = (x_1, \dots, x_m)$ on m projections $h_i(\mathtt{x})$ be available, where x_i is a vector of realisations of $h_i(\mathtt{x})$, So that x_i is a function in available plain-text/cipher-text and $\bar{K}_i$. A statistic $S(x)$ is called separable if $S(x) = \sum_{i=1}^{m} S_i(x_i)$. One decides the value of $\bar{K}$ is correct if $S(x) > z$ for some z. If a priori distribution of $\mathtt{x}$ is close to be uniform, it looks that the best possible statistic to distinguish it from the uniform distribution by observing $h_i(\mathtt{x})$ is approximately separable. In that case $S_i(x_i)$ are weighted LLR statistics for separate $h_i(\mathtt{x})$. That allows an efficient algorithm to construct $\bar{K}$-values from $\bar{K}_i$-values. We apply this new technique to 16-round DES with success.