The Independence of Linear Approximations in Symmetric Cryptology

Sean Murphy
Royal Holloway

Abstract

The basic form of the technique of *linear cryptanalysis* considers a block cipher which encrypts a binary plaintext vector $\mathbf{p}_i$ to ciphertext vector $\mathbf{c}_i$ under a key $\mathbf{k}$. A linear approximation of this block cipher is an expression of the form

$$\mathbf{a}^T \begin{pmatrix} \mathbf{p}_i \\ \mathbf{c}_i \end{pmatrix} = \mathbf{b}^T\mathbf{k} \text{ with probability } p = \frac{1}{2} + \epsilon,$$

where $\mathbf{a}$ and $\mathbf{b}$ are known as the *data mask* and *key mask* respectively, and ϵ is known as the *bias*. The simplest form of linear cryptanalysis uses this single linear approximation with many plaintext–ciphertext pairs to find the key bit $\mathbf{b}^T\mathbf{k}$. This talk considers the use of many such linear approximations with data masks $\mathbf{a}_0, \mathbf{a}_1, \ldots$ to find the key bit $\mathbf{b}^T\mathbf{k}$. Issues discussed include:

- whether using a third linearly dependent mask $\mathbf{a}_0 + \mathbf{a}_1$ can give more key information than using just the two masks $\mathbf{a}_0$ and $\mathbf{a}_1$;
- whether a mask $\mathbf{a}$ with bias $\epsilon = 0$ can give any key information.