Optimizing Cryptographic Strength of Substitution Layers in Symmetric-Key Cryptographic Algorithms

Christopher A. Wood

May 9, 2012

Agenda

Avalanche effect

A function $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$ exhibits the *avalanche effect* if and only if

$$\sum_{x \in \mathbb{F}_2^n} \mathrm{wt}(f(x) \oplus f(x \oplus c_i^n)) = n2^{n-1}, *$$

for all $i(1 \leq i \leq n)$, where $c_i^n = [0, 0, \ldots, 1, \ldots, 0]$ (where a 1 is in the nth position of the vector of cardinality n).

*wt indicates the Hamming Weight function

Branch number

The *branch number* of an $n \times n$-bit S-Box is

$$BN = \min_{a,b \neq a}(\mathrm{wt}(a \oplus b) + \mathrm{wt}(S(a) \oplus S(b))),$$

where $a, b \in \mathbb{F}_2^n$.

S-box specific nonlinear measurements

The nonlinearity of an $n \times n$-bit S-Box from $\mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$ can be measured by

$$P_S = \max_{0 \neq a,b} |\{x \in \mathbb{F}_2^n : S(x+a) - S(x) = b\}|$$

where $a, b \in \mathbb{F}_2^n$.