Cryptographic properties of substitutions

Oleksandr Kazymyrov

University of Bergen
Norway

Autumn 2012

Outline

- Definitions
- Cryptographic properties
  - Boolean functions
  - Substitutions
- Relations between cryptographic properties
- Examples
- Open questions

Definitions

- The Hemming weight:

$$hw(f) = \sum_{x \in F_2^n} f(x)$$

- The Hamming distance between two functions:

$$hd(f, g) = \sum_{x \in F_2^n} f(x) \oplus g(x)$$

- Function $f(x)$ of n-variable is called balanced if

$$hw(f) = 2^{n-1}$$

Definitions

- The algebraic normal form (ANF):

$$f(x_0, x_1, \ldots, x_{n-1}) = \sum_{j=(j_0,j_1,\ldots,j_{n-1}) \in F_2^n} a_j x_0^{j_0} x_1^{j_1} \cdots x_{n-1}^{j_{n-1}}$$

- The algebraic degree ($deg(f)$) of $f(x)$ is defined to be the maximal $hw(j)$ such that $a_j \neq 0$.
- The Walsh Hadamard transform (WHT):

$$W(\omega) = \sum_{x \in F_2^n} (-1)^{f(x) \oplus l_\omega(x)}$$

where $l_\omega(x) = \omega \cdot x = \bigoplus_{i=0}^{n-1} \omega_i x_i$.

Criteria of Boolean functions

- Balance
- Algebraic degree
- Nonlinearity
- Autocorrelation
- Correlation Immunity
- Propagation criteria
- Algebraic Immunity

Nonlinearity

- The nonlinearity ($NL(f)$):

$$NL(f) = \frac{1}{2}\left(2^n - |W_{max}|\right)$$

$$NL(f) \leq \begin{cases} 2^{n-1} - 2^{\frac{n}{2}-1}, \text{for even n} \\ 2^{n-1} - 2^{\frac{n-1}{2}}, \text{ for odd n} \end{cases}$$

- Bent functions:

$$NL(f) = \begin{cases} 2^{n-1} - 2^{\frac{n}{2}-1}, \text{for even n} \\ 2^{n-1} - 2^{\frac{n-1}{2}}, \text{ for odd n} \end{cases}$$

Avalanche

- The autocorrelation:

$$r_f(\alpha) = \sum_{x \in F_2^n} (-1)^{f(x) \oplus f(x \oplus \alpha)}$$

- The maximum absolute autocorrelation value:

$$|AC(f)|_{max} = max_{\alpha} |r_f(\alpha)|$$

- Sum of square indicator:

$$\sigma = \sum_{\alpha \in F_2^n} r_f^2(\alpha)$$

Correlation immunity

- m^{th}-order correlation immunity:

$$\begin{cases} 1 \leq hw(\omega) & \leq & m, \\ W(\omega) & = & 0. \end{cases}$$

- An N-variable boolean function, $f(x)$, which is both balanced and has m^{th}-order correlation immunity, is known as an m-resilient boolean function.

Propagation criteria

Propagation criterion of degree k:

$$\begin{cases} 1 \leq hw(\alpha) & \leq & k \\ \sum_{x \in F_2^n} f(x) \oplus f(x \oplus \alpha) & = & 2^{n-1} \end{cases}$$

Satisfy strict avalanche criterion (SAC):

$$\begin{cases} hw(\alpha) & = & 1 \\ \sum_{x \in F_2^n} f(x) \oplus f(x \oplus \alpha) & = & 2^{n-1} \end{cases}$$

Algebraic Immunity

The lowest degree of function g for which $f \cdot g = 0$ or $(f \oplus 1) \cdot g = 0$ is called the algebraic immunity (AI) of f. The function g for which $f \cdot g = 0$ is called annihilator of f.

Criteria of substitutions

- Balance
- Nonlinearity
- Algebraic degree
- Autocorrelation
- Correlation Immunity
- Propagation criteria

Criteria of Sbox

Let $S = (f_1, f_2, \ldots, f_M)$ be an NxM substitution, where f_i are N-variable boolean functions.
Let g be the set of linear combinations of f_i.
Then criteria can be expressed as follow:

- S is balanced iff all g_j are balanced
- nonlinearity of S:

$$NL(S) = min_g\{NL(g_j)\}$$

- algebraic degree of S:

$$deg(S) = min_g\{deg(g_j)\}$$

Criteria of Sbox

- The maximum absolute autocorrelation value of S:

$$|AC(S)|_{max} = max_g|AC(g)_{max}|$$

- S is a t^{th}-order correlation immunity S-box iff every g_j is t^{th}-order correlation immunity boolean function.
- S satisfies propagation criteria of order k iff every g_j satisfies $PC(k)$.

Criteria of substitutions

- Bijection
- Fixed points
- Maximum of differential table
- Maximum of linear table
- Algebraic Immunity

Bijection and fixed point

- Substitution is bijective iff $\forall x$

$$S^{-1}(S(x)) = x$$

- S-box has n fixed points if $\exists X : X = \{x_0, x_1, \ldots, x_{n-1}\}$

$$S(x_j) = x_j$$

Maximum of differential table

Let S be an NxM S-box. Let δ be the largest value of the differential distribution table of the S-box (not taking into account first row and column). Then

$$\delta = \max_{\alpha \in F_2^N, \alpha \neq 0, \beta \in F_2^M} \max \#\{x | S(x) \oplus S(x \oplus \alpha) = \beta\}$$

Maximum of linear table

Let S be an NxM S-box. Let λ be the largest value of the linear distribution table of the S-box (not taking into account first row and column). Then

$$\lambda = \max_{\alpha \in F_2^N, \alpha \neq 0, \beta \in F_2^M} \left| \#\{x | \left(\bigoplus_{s=0}^{N} (x[s] \cdot \alpha[s]) \right) = \left(\bigoplus_{t=0}^{M} (S(x)[t] \cdot \beta[t]) \right) \} \right|.$$

where $\xi[s]$ is a s^{th} bit of ξ.

Algebraic Immunity

Suppose A is a matrix, which contains all combinations of input and output bits up to degree d.

$$A \cdot X = \bar{0}$$
$$X = NullSpace(A)$$

Let r be the number of equations of a system, which describes an NxM S-box. Then:

$$r = \sum_{x=0}^{d} \binom{N+M}{d} - Rank\,(A)$$

Relations between properties

Suppose f is m^{th}-order correlation immune.
Siegenthaler's Inequality:

$$n \geq m + deg(f) + \epsilon \text{ where } \epsilon = \begin{cases} 0 & \text{if function is balanced,} \\ 1 & \text{if function is unbalanced.} \end{cases}$$

Relation between MLT and nonlinearity of Boolean functions:

$$\lambda = 2^{n-1} - NL(S)$$

Relations between properties

Suppose H is Hadamard matrix, AC_v is autocorrelation set of f, AC_m is matrix consists of all function f shifted by α. Then

$$AC_v = AC_m \cdot f$$
$$NL_v = H \cdot f$$
$$H \cdot H^T = 2^n I$$
$$f = \frac{1}{2^n} H \cdot NL_v$$
$$AC_v = \frac{1}{2^n} AC_m \cdot H \cdot NL_v$$

Equivalence classes of substitutions

Suppose round function (F-function) in block cipher is described as follow:

$$F = K \circ L \circ S$$

where L - linear layer, S - nonlinear layer, K - key layer.
For example AES's F-function can be described as:

$$F = K \circ L_2 \circ L_1 \circ S$$

L_2 - MixColumns, L_1 - ShiftRows, S - SubBytes, K - AddRoundKey.

Equivalence classes of substitutions

General nonlinear layer:

$$S(x) = S1(x_1)||S2(x_2)||\ldots||SK(x_k)$$

Affine equivalence:

$$S2(x) = A \cdot S1(B \cdot x \oplus c) \oplus d$$

General nonlinear layer:

$$S(x) = L \circ S1(x_1)||S1(x_2)||\ldots||S1(x_k)$$

Important properties for block ciphers

Substitution must satisfy the following properties:

- Bijection
- Absence fixed points
- Minimum of MDT
- Minimum of MLT
- Maximum of AI
- Different equivalence classes*

S-box characteristics

	AES	Cam.	Lab.	R0	R1	R2	R3	R4
Balance of BF	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
NL	112	112	112	96	98	96	96	96
AC	32	32	32	88	88	88	104	96
SSI	133120	133120	133120	244480	252928	259456	291712	251392
PC	0	0	0	0	0	0	0	0
CI	0	0	0	0	0	0	0	0
Resilient	0	0	0	0	0	0	0	0
Degree	7	7	7	7	7	6	7	7
Number of eq.	39	39	39	441	441	441	441	441
Degree of eq.	2	2	2	3	3	3	3	3
MDT	4	4	4	8	8	8	8	8
MLT	16	16	16	32	30	32	32	32
Bijective	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Open questions

- Are there other relations between cryptographic properties?
- What are the most important properties for block ciphers (stream ciphers)?
- Question of finding faster algorithms for getting cryptographic properties is still opened.
- Problem of finding equivalence classes of substitution for $n > 4$.