T-79.5501 Cryptology
Homework 6
February 27, 2007

1. Consider the example linear attack in Stinson, section 3.3.3. In S_2^2 replace the random variable $\mathbf{T}_2$ by $\mathbf{U}_6^2 \oplus \mathbf{V}_8^2$. Then in the third round the random variable $\mathbf{T_3}$ is not needed. What is the final random variable corresponding to formula (3.3) (Stinson)) and what is its bias?

2. Consider the finite field $GF(2^3) = \mathbb{Z}_2[x]/(f(x))$ with polynomial $f(x) = x^3 + x + 1$ (see Stinson 6.4).

   (a) Compute the look-up table for the inversion function $g : z \mapsto z^{-1}$ in $GF(2^3)$, where we set $g(0) = 0$.

   (b) Compute the algebraic normal form of the Boolean function defined by the least significant bit of the inversion function.

3. The standard hash-function SHA-1 makes use of two non-linear combination functions. The first of them, G, the Geffe function is described in the handout on Boolean functions. The second one is the "threshold function" denoted by T and it is defined as follows. Let X_0, X_1, X_2 be three 32-bit words. Then

$$T(X_0, X_1, X_2) \quad = \quad (X_0 \wedge X_1) \vee (X_0 \wedge X_2) \vee (X_1 \wedge X_2)$$

   Let t denote the one-bit component of T.

   (a) Compute the values of $t(x)$ as x runs through all 3-bit strings. Show that it takes the value "1" exactly when at least two of the input-variables take the value "1".

   (b) Compute the ANF of t.

   (c) A *linear structure* of a Boolean function f of three variables is defined as a vector $w = (w_1, w_2, w_3) \neq (0, 0, 0)$ such that $f(x \oplus w) \oplus f(x)$ is constant. Show that t has exactly one linear structure.

4. Given three input bits (x_1, x_2, x_3) the output bits (y_1, y_2) an 3-to-2 S-box π_S are defined as follows:

$$\begin{aligned} y_1 &= x_1x_2 \oplus x_3 \\ y_2 &= x_1x_3 \oplus x_2 \end{aligned}$$

   Compute the linear approximation table of π_S.

5. Consider the finite field $\mathbb{F} = \mathbb{Z}_2[x]/(x^3 + x + 1)$ and let $f : \mathbb{F} \to \mathbb{F}$ be a function defined as

$$\begin{aligned} f(z) &= z^{-1}, \text{ for } z \neq 0, \\ f(0) &= 0. \end{aligned}$$

   Let a Feistel cipher be defined as follows

$$\begin{aligned} L_i &= R_{i-1} \\ R_i &= L_{i-1} \oplus f(R_{i-1} \oplus K_i), \end{aligned}$$

   where $L_i \in \mathbb{F}$, $R_i \in \mathbb{F}$ and the round keys are defined as $K_i = K^i$, for $i = 1, 2, 3$, where $K \in \mathbb{F}$ is the key. Assume that one known plaintext-ciphertext pair is given as follows: $L_0 = 100$, $R_0 = 001$, $L_3 = 110$ and $R_3 = 100$. Attempt to find the key K.

6. Let π_S be an m-bit to n-bit S-box. Let us derive a mathematical expression of $N_L(a,b)$ in the linear distribution table. Consider the sum

$$\sum_{x\in\{0,1\}^m} (-1)^{a\cdot x\oplus b\cdot\pi_S(x)},$$

computed over integers. It is easy to see that

$$\begin{aligned}
&\sum_{x\in\{0,1\}^m} (-1)^{a\cdot x\oplus b\cdot\pi_S(x)} \\
= \quad & \#\{x\in\{0,1\}^m \,|\, a\cdot x\oplus b\cdot\pi_S(x)=0\} - \#\{x\in\{0,1\}^m \,|\, a\cdot x\oplus b\cdot\pi_S(x)=1\} \\
= \quad & N_L(a,b) - (2^m - N_L(a,b)) = 2N_L(a,b) - 2^m.
\end{aligned}$$

Actually, this is nothing else but the Walsh-Hadamard transform of the Boolean function $b\cdot\pi_S(x)$, see the handout on Boolean functions. It follows that

$$N_L(a,b) = 2^{m-1} + \frac{1}{2}\sum_{x\in\{0,1\}^m} (-1)^{a\cdot x\oplus b\cdot\pi_S(x)}. \tag{1}$$

(a) Problem(Stinson)): Let π_S be an m-bit to n-bit S-box. Show that

$$\sum_{a=0}^{2^m-1} N_L(a,b) = 2^{2m-1} \pm 2^{m-1},$$

for all n-bit mask values b, where the sum is taken over all m-bit mask values a (enumerated from 0 to 2^m-1).

(b) Check the result in (a) for the linear approximation table computed in Problem 4.