ویژگی‌های رمزنگاری جمع پیمانه‌ای به پیمانه‌ی توانی از 2

سید مجتبی دهنوی
اکبر محمودی ریشکانی
حمیدرضا میمنی

$$\varphi : F_2{}^n \to Z_{2^n}$$

$$x = (x_{n-1},\ldots,x_0) \mapsto \varphi(x) = \sum_{i=0}^{n-1} x_i 2^i$$

$$x = (x_{n-1},\ldots,x_0) \quad \text{و} \quad u = (u_{n-1},\ldots,u_0)$$

$$x^u = x_0^{u_0}\ldots x_{n-1}^{u_{n-1}}$$

$$f(x) = \bigoplus_{u \in Z_{2^n}} h_u x^u, \quad h_u \in F_2$$

$$h_u = \bigoplus_{x \prec u} f(x)$$

$$f_a(x) = \begin{cases} 0 & f(x) = a.x \\ 1 & f(x) \neq a.x \end{cases}$$

$$\underset{\substack{a \in F_2^m \\ a \neq 0}}{Max}\left(4\left(\frac{|f^{-1}(0)| - 2^{m-1}}{2^m}\right)^2\right)$$

$$f^a(x) = \begin{cases} 0 & f(x) = f(x \oplus a) \\ 1 & f(x) \neq f(x \oplus a) \end{cases}$$

$$\underset{\substack{a \in F_2^m \\ a \neq 0}}{Max} \frac{|\{x \mid f^a(x) = 0\}|}{2^m}$$

$$P_{f,g} = \frac{|\{x \in F_2^m \mid f(x) = g(x)\}|}{2^m}$$

$$E_{f,g} = n - \frac{\sum_{x \in F_2^m} d(f(x), g(x))}{2^m} = \frac{\sum_{i=0}^{n-1} |\{x \in F_2^m \mid f_i(x) = g_i(x)\}|}{2^m}$$

$$z = (z_{n-1},\ldots, z_0) \quad y = (y_{n-1},\ldots, y_0) \quad x = (x_{n-1},\ldots, x_0)$$

$$f : F_2^{2n} \to F_2^n$$

$$f(x, y) = z \qquad z = x + y \mod 2^n$$

$$z_0 = x_0 \oplus y_0 \oplus c_0, \quad c_0 = 0$$
$$z_i = x_i \oplus y_i \oplus c_i, \quad c_i = x_{i-1} y_{i-1} \oplus c_{i-1}(x_{i-1} \oplus y_{i-1})$$

$$x + y = (x \oplus y) + 2(x \wedge y) \bmod 2^n$$

$$P_{f,g} = \left(\frac{3}{4}\right)^{n-1}$$

$$P(c_i = 0) = \frac{1}{2} + \frac{1}{2^{i+1}}$$

$$P(c_i = 0) = P(x_{i-1}y_{i-1} \oplus c_{i-1}(x_{i-1} \oplus y_{i-1}) = 0)$$
$$= P(c_{i-1} = 0)P(x_{i-1}y_{i-1} = 0) +$$
$$P(c_{i-1} = 1)P(x_{i-1} \oplus y_{i-1} \oplus x_{i-1}y_{i-1} = 0)$$
$$= \frac{3}{4}(\frac{1}{2} + \frac{1}{2^i}) + \frac{1}{4}(\frac{1}{2} - \frac{1}{2^i})$$
$$= \frac{1}{2} + \frac{1}{2^{i+1}}$$

$$(a_{n-1}, \ldots, a_0) \in F_2^n$$

$$P(c_{n-1} = a_{n-1}, \ldots, c_0 = a_0) = \begin{cases} (\frac{3}{4})^{n-1} 3^{-w(b)} & a_0 = 0 \\ 0 & a_0 \neq 0 \end{cases}$$

$$b = (b_{n-1}, \ldots, b_0)$$
$$= (a_{n-1} \oplus a_{n-2}, \ldots, a_1 \oplus a_0, 0)$$

$$P(c_i = a_i \mid c_{i-1} = a_{i-1}, \ldots, c_0 = a_0)$$
$$= P(c_i = a_i \mid c_{i-1} = a_{i-1})$$

$$P(c_{n-1} = a_{n-1}, \ldots, c_0 = 0)$$
$$= P(c_0 = 0) \times P(c_1 = a_1 \mid c_0 = 0)$$
$$\times \ldots \times P(c_{n-1} = a_{n-1} \mid c_{n-2} = a_{n-2})$$

$$P(c_i = 0 \mid c_{i-1} = 0) = P(c_i = 1 \mid c_{i-1} = 1) = \frac{3}{4}$$

$$P(c_i = 1 \mid c_{i-1} = 0) = P(c_i = 0 \mid c_{i-1} = 1) = \frac{1}{4}$$

$$P(c_i = a \mid c_{i-j} = b) = \frac{1}{2} + \frac{(-1)^{a+b}}{2^{j+1}}$$

$$2 \le r \le n \qquad a \in F_2^r \qquad a = (a_{r-1}, \ldots, a_0)$$

$$0 < j_0 < j_1 < \ldots < j_{r-1} < n$$

$$P(c_{j_{r-1}} = a_{r-1}, \ldots, c_{j_0} = a_0) = \prod_{k=0}^{r-1} \left(\frac{1}{2} + \frac{(-1)^{a_k + a_{k-1}}}{2^{j_k - j_{k-1}+1}}\right)$$

$$j_{-1} = a_{-1} = 0$$

$$c_i^n = c_i^m, \ 0 \le i < n, \ m > n$$

$$d_i^n = 1, \quad 0 \le i < n$$

$$a = (1, \overbrace{0,\ldots,0}^{n-1}, 1, \overbrace{0,\ldots,0}^{n-1})$$

0.00006, 0.00024, 0.00098, 0.00391, 0.01563, 0.625, 0.25