情報保護學會論文誌
第17卷 第4號, 2007. 8

스트림 암호에서 높은 비선형도의 상관면역함수의 설계와 그의 안전성 분석

양 정 모*
중부대학교

The Security analysis and construction of correlation immune function with higher nonlinearity on stream cipher

Jeong-mo Yang*
Joongbu University

요 약

상관면역함수 f를 만드는 방법으로 Siegenthaler의 방법, Camion의 방법과 Seberry의 방법 등이 있다. 이 중에서 Seberry의 방법은 Hadamard 행렬이론을 이용하여 상관면역함수를 만드는 것으로, 임의의 상관면역도의 균형상관면역함수를 만드는 방법을 제공하였다.

본 논문에서는 저차원의 벡터공간에서 만들어진 여러 개의 상관면역함수를 조합하여 고차원 벡터공간위에서 상당히 비도가 높은 함수를 설계하는 Seberry의 방법들을 연구하였고, 그 함수들의 비선형도를 계산하였다. 즉, 두 개의 함수의 직합으로 설계된 새로운 상관면역함수와 네 개의 함수의 조합으로 설계된 새로운 상관면역함수의 비선형도가 각각의 이전 함수들과 비교하여 더 높은 비선형도를 갖는다는 것을 보였다. 또한 위의 방법을 응용하여 상대적으로 비도가 높은 상관공격으로부터 안전한 스트림암호에서 사용되는 함수들을 설계하였다.

ABSTRACT

There are various methods constructing correlation immune functions such as Siegenthaler's, Camion et al's and Seberry et al's. In particular, Seberry et al's is a method which directly constructs balanced correlation immune functions of any order using the theory of Hadamard matrices.

In this paper, we have studied Seberry et al's method for constructing a correlation immune function on a higher dimensional space by combining known correlation immune functions on a lower dimensional space. Futhermore, we calculated the nonlinearity of functions which are constructed by combining of several correlation immune functions. That is, we have shown that the direct sum of two correlation immune functions and a combination of four correlation immune functions have higher nonlinearity in comparison with each functions. This functions in stream cipher are safe against correlation attacks.

Keywords : *nonlinearity, correlation immune function*

접수일: 2007년 5월 11일; 채택일: 2007년 6월 11일
* 주저자, jmyang@joongbu.ac.kr

Ⅰ. 서 론

상관면역함수는 선형귀환축차생성기(LFSR)를 사용하여 열쇠이진수열 생성기 설계를 포함한 컴퓨터보안에서 많은 응용이 되고 있다. 실질적인 응용에 있어서, 상관공격으로부터 안전한 상관면역함수를 쉽게 설계할 수 있는 방법을 찾는 것은 스트림암호 체계에서 매우 중요하다.

균형상관면역함수를 설계한 첫 번째 방법은 Siegenthaler[9]에 의해 발표되었다. 그의 방법은 실질적인 응용을 하는 데 있어서 만족스럽지 못하였다. Camion[3] 등에 의해 설계된 상관면역함수는 대수적 부호이론의 관점에서 연구되어 왔고 상관면역도가 주어진 상관면역함수를 설계하는 방법으로 표현되었다. 그리고 Seberry[7] 등은 Hadamard 행렬이론을 이용하여 상관면역함수를 연구하였으며 이는 상관면역도가 주어진 균형상관면역함수의 직접적인 설계방법으로 표현되었다. 그들은 저차원공간의 상관면역함수를 결합하여 고차원의 상관면역함수를 설계하는 방법을 연구하였다.

본 논문에서는 저차원의 벡터공간에서 만들어진 여러 개의 상관면역함수를 조합하여 고차원 벡터공간위에서 상당히 비도가 높은 함수를 설계하는 Seberry의 방법들을 연구하였고, 그 함수들의 비선형도를 계산하였다. 즉, 두 개의 함수의 직합으로 설계된 새로운 상관면역함수와 네 개의 함수의 조합으로 설계된 새로운 상관면역함수의 비선형도가 각각의 이전 함수들과 비교하여 더 높은 비선형도를 갖는다는 것을 보였다. 또한 위의 방법을 응용하여 상대적으로 비도가 높은 상관공격으로부터 안전한 스트림 암호에서 사용되는 함수들을 설계하였다.

Ⅱ. 비선형도 계산을 위한 몇 가지 성질들

다음 몇 가지 성질들은 새로이 설계된 고차원의 상관면역함수의 비선형도를 계산하는데 필요한 성질들이다.

성질 2.1 g 를 V_m 상의 함수라 하고 η_g 를 그에 의해 생성된 수열이라 하자. 그러면 g 가 상관면역도가 k 인 상관면역함수일 필요충분조건은 임의의 η_h 에 대하여 $<\eta_g, \eta_h> = 0$ 이다. 여기서 η_h 는 $V_m (1 \leq W(\alpha) \leq k.)$ 상에서 $h(x) = <\alpha, x>$ 의 선형함수에 의해 생성된 수열이다.

성질 2.2. (1) $H_m = \begin{bmatrix} l_0 \\ l_1 \\ \vdots \\ l_{2^m-1} \end{bmatrix}$ 라 놓고 l_i 는 H_m 의 행이라 하자. 그러면 l_i 는 모든 $i = 0,1\cdots,2^m-1$ 에 대하여 선형함수 $h_i(x) = <\alpha_i, x>$ 에 의해 생성된 수열이다. 단, $x = (x_1, x_2, \cdots, x_m)$, $\alpha_i \in V_m$.

(2) 역으로 V_m 위에서 각각의 선형함수에 의해 생성된 수열은 H_m 의 행이다.

성질 2.3.(Seberry등의 설계) m, n을 $m > n$ 인 양의 정수라 하자.

$\Phi_{m,n} = \{\varphi_{\alpha_0}, \varphi_{\alpha_1}, \cdots, \varphi_{\alpha_{2^{m-n}-1}}\}$ 을 V_n 상에서 2^{m-n} 개의 선형함수를 포함하는 족(family)이라 가정하자. 여기서 $\Phi_{m,n}$ 는 선형함수가 $\Phi_{m,n}$ 안에서 한번 이상 나타날 수 있다는 측면에서 다중족(multi-family)이 될 수 있다.

$g(y,x) = \oplus_{\delta \in V_{m-n}} D_\delta(y)\varphi_\delta(x) \oplus r(y)$,로 놓자. 그리고 r 을 V_{m-n} 상에서 임의의 함수라 하자. 그러면 g 는 V_m 상에서 상관면역도가 k 인 균형상관면역함수이다. 여기서 $x = (x_1, x_2, \cdots, x_n)$, $y = (y_1, y_2, \cdots, y_{m-n})$ 이고, $k \leq \min\{W(\gamma_\delta) \mid \delta \in V_{m-n}\} - 1$, $\gamma_\delta \in V_n$, $\varphi_\delta(x) = <\gamma, x> \in \Phi_{m,n}$ 이다.

성질 2.4 η_f 와 η_g 를 V_m 상에서 각각 함수 f 와 g 에 의해 생성된 수열이라 하자. 그러면

$$d(f, g) = 2^{m-1} - \frac{1}{2}<\eta_f, \eta_g>$$

이다.

성질 2.5 g 를 성질 2.3에서 정의한 함수라 하자. 그러면

$$2^{m-1} - t\,2^{n-1} \leq N_g \leq \begin{cases} 2^{m-1} - 2^{\frac{m}{2}-1} - 2 & \text{if } m \text{ is even,} \\ [2^{m-1} - 2^{\frac{m}{2}-1}] & \text{if } m \text{ is odd,} \end{cases}$$

이다. 여기서, $t = \max t_\delta \mid \delta \in V_{m-n}$, $m > n > 2$ 인 $m, n \in Z$ 이고 t_δ 는 $\Phi_{m,n}$ 에 나타나는 선형함수 ϕ_δ 의 횟수이다.

Ⅲ. 고차원공간에서 설계된 상관면역함수의 선형도 분석

3.1. 이전 방법들

저차원공간에서 함수들을 결합한 고차원에서의 상관면역함수들을 설계하는 기존의 방법들을 소개하고 그들의 비선형도를 계산하는 법을 소개한다. 성질 2.3의 내용은 성질 3.1로 확장된다.

$m, n, k, s \in Z(m > n > k \geq 1)$라 하고, $w=(y,x,z)$를 V_{m+s}의 원소라 하자. 또, $y=(y_1,\cdots,y_{m-n})$, $x=(x_1,\cdots,x_n)$ 그리고 $z=(z_1,\cdots,z_s)$ 라 하자. 지금

$$\Phi_{m,n} = \{\varphi_0,\cdots,\varphi_{2^{m-n}-1}\}$$

을 선형함수들의 선택을 반복 허용하는 집합 $\Omega_{k,n}$으로부터 선택한 각각의 V_n 상에서 선형함수들의 집합족이라 하자. r_1을 V_{m-n} 상에서 임의의 함수라고 할 때

$$g_1(y,x) = D_{0\cdots0}(y)\varphi_0(x) \oplus \cdots \oplus D_{1\cdots1}(y)\varphi_{2^{m-n}-1}(x) \oplus r_1(y)$$

라 놓으면 성질 2.3에 의하여 g_1은 V_m상에서 상관면역도 k인 균형상관면역함수이다. 지금 $\{f_0,\cdots,f_{2^{m-n}-1}\}$를 V_s 상에서 위수 p의 상관면역함수족 들이라 하자. 이 함수족 안에 있는 함수들은 서로 다를 필요는 없다. r_2를 V_{m-n}상에서 임의의 함수라고 할 때

$$g_2(y,z) = D_{0\cdots0}(y)f_0(z) \oplus \cdots \oplus D_{1\cdots1}(y)f_{2^{m-n}-1}(z) \oplus r_2(y)$$

라 놓자.

성질 3.1 $g(y,x,z) = g_1(y,x) \oplus g_2(y,z)$으로 설계하면 g는 V_{m+s} 상에서 상관면역도가 $(k+p+1)$인 균형상관면역함수이고 g의 비선형도는 다음을 만족한다.

$$N_g \geq 2^{m+s-1} - t\,2^n\,(2^{s-1}-N)$$

이때, $t = \max\{t_i \mid i=0,1,\cdots,2^{m-n}-1\}$이고 t_i는 φ_i가 $\Phi_{m,n}$ 안에 나타나는 회수를 나타낸다. 그리고

$$N = \min\{\{N_{f_i} \mid i=0,1,\cdots,2^{m-n}-1\}\}$$

이다.

성질 3.2 (두 개의 상관면역함수의 직합) f를 V_m 상에 상관면역도가 k_1인 상관면역함수라 하고 g를 V_n 상에 상관면역도가 k_2인 상관면역함수라 하자. 그러면 $h(x,y)=f(x)\oplus g(y)$는 V_{m+n}상에서 상관면역도가 (k_1+k_2+1)인 상관면역삼수이고 h의 비선형도 N_h는 다음을 만족한다.

$$N_h \geq d_1\,2^n + d_2\,2^m - 2\,d_1\,d_2\,.$$

여기서 $N_f = d_1$이고 $N_g = d_2$이다.

성질 3.3 (4 개의 상관면역함수의 조합) f_1과 f_2를 V_m상에서 상관면역도가 k_1인 상관면역함수라 하고 g_1과 g_2는 V_n상에서 상관면역도가 k_2인 상관면역함수라 하자. 또, $\eta_{f_1}, \eta_{f_2}, \eta_{g_1}$ 과 η_{g_2}를 각각 f_1, f_2, g_1 과 g_2에 의해 생성되는 수열이라 하자. η_h는 다음과 같이 정의되는 (1,-1)-수열이라 하면 η_h에 대응되는 함수 h는 V_{m+n}상에서 상관면역도가 (k_1+k_2+1)인 상관면역함수이다.

$$\eta_h = \frac{1}{2}(\eta_{f_1}+\eta_{f_2}) \otimes \eta_{g_1} + \frac{1}{2}(\eta_{f_1}-\eta_{f_2}) \otimes \eta_{g_2}$$

여기서+ 는 원소끼리의 덧셈이고 ⊗는 Kronecker 곱이다.

3.2. 비선형도 계산의 새로운 접근 설계 제안

성질 2.3에서 소개한 방법에 의해 설계된 V_m상에서의 상관면역도가 k인 상관면역함수 g의 대수적 차수는 $m-n+1$ 임을 보였다. 이제 상관면역도가 k이고 대수적 차수가 d인 함수 g의 비선형도를 계산하는 방법을 제안하고자 한다.

정리 3.4 성질 2.5에서 $n=k+2$라면 성질 2.3의 방법에 의해 설계된 V_m상의 상관면역도 k인 균형상관면역함수 g의 최대 대수적 차수는 $m-k-1$이고 g의 비선형도 N_g는 다음과 같다.

$$2^k(2^d-2) \leq N_g\,.$$

증명. 다음 집합들의 원소의 개수는 다음과 같다. 즉,

$\#(\Omega_{k,n}) = 2^n - \sum_{r=0}^{k} {}_nC_r$ 이고 $\#(\Phi_{m,n}) = 2^{m-n}$.

만약 $\#(\Omega_{k,n}) \geq \#(\Phi_{m,n})$이라면,

$$2^n - \sum_{r=0}^{k} {}_n C_r \geq 2^{m-n} .$$

일반적으로, $1 \leq k < n < m$ 인 어떤 고정된 n에 대하여 $2^n(2^n - \sum_{r=0}^{k} {}_n C_r) \geq 2^m$ 을 만족하는 회수로 $t=1$ 을 선택할 수 있다. 왜냐하면 N_g가 $t=1$ 일 때 가장 높은 비선형도를 갖기 때문이다. 또한 $n=k+2$ 라면 g의 최대 대수적 차수는 $m-k-1$ 이고 $d+k \leq m-1$ 이다. 이 경우, $2^{d+k} = 2^{m-1}$ 이고 $2^{d+k} - t\,2^{n-1} = 2^{m-1} - t\,2^{n-1} \leq 2^{d+k} - 2^{n-1} \leq N_g$ 이다. 따라서,

$$2^{d+k} - 2^{n-1} = 2^{d+k} - 2^{k+1} \leq N_g .$$

즉, 어떤 고정된 n 에 대하여 $d+k=m-1$ 이고 $t=1$ 이라면 N_g 의 최소값은 $2^{d+k} - 2^{k+1}$ 이다. 따라서 $2^k(2^d - 2) \leq N_g$.

정리 3.5 f_1 과 f_2 를 V_m 상에서 상관면역도가 k_1 인 상관면역함수라 하고 g_1 과 g_2 는 V_n 상에서 상관면역도가 k_2 인 상관면역함수라 하자. 또, η_{f_1}, η_{f_2}, η_{g_1} 과 η_{g_2} 를 각각 f_1, f_2, g_1 과 g_2 에 의해 생성되는 수열이라 하자. η_h 는

$$\eta_h = \frac{1}{2}(\eta_{f_1} + \eta_{f_2}) \otimes \eta_{g_1} + \frac{1}{2}(\eta_{f_1} - \eta_{f_2}) \otimes \eta_{g_2}$$

같이 정의되는 (1,-1)-수열이라 하면

$$N_h \geq 2^m(d_3+d_4) + 2^n(d_1+d_2) - (d_1+d_2)(d_3+d_4) - 2^{m+n-1}$$

여기서 + 는 원소끼리의 덧셈, $\otimes$는 Kronecker 곱이고 $N_{f_1} = d_1$, $N_{f_2} = d_2$, $N_{g_1} = d_3$ 이고 $N_{g_2} = d_4$ 이다.

증명 $\gamma, z \in V_{m+n}$ 에 대하여 $\varphi(z) = <\gamma, z>$ 을 V_{m+n} 상에서 선형함수라 하자. 단, 여기서 $z=(u,v)$, $u \in V_m$, $v \in V_n$. 그리고 L을 φ의 수열이라 하자. 그러면 L은 H_{m+n} 의 행 이다. 사실, 성질 3.2에 의하여

$$\varphi(z) = <\gamma, z> = <\alpha, u> \oplus <\beta, v>,$$

이다. 단, 여기서 $\gamma=(\alpha,\beta)$, $\alpha \in V_m$, $\beta \in V_n$. l_1은 H_m 의 행이고 l_2는 H_m 의 행 일 때 $H_{m+n} = H_m \otimes H_n$ 이기 때문에 $L = l_1 \otimes l_2$ 이다. l_1 , l_2는 성질 3.2에 의하여 각각 $<\alpha,u>$ 과 $<\beta,v>$의 수열이다. 성질 2.4에 의하여,

$$d_1 = N_{f_1} \leq d(f_1,\varphi_1) = 2^{m-1} - \frac{1}{2} < \eta_{f_1}, l_1 >,$$

$$d_2 = N_{f_2} \leq d(f_2,\varphi_1) = 2^{m-1} - \frac{1}{2} < \eta_{f_2}, l_1 >,$$

$$d_3 = N_{g_1} \leq d(g_1,\varphi_2) = 2^{n-1} - \frac{1}{2} < \eta_{g_1}, l_2 >,$$

$$d_4 = N_{g_2} \leq d(g_2,\varphi_2) = 2^{n-1} - \frac{1}{2} < \eta_{g_2}, l_2 >,$$

단, $\alpha, u \in V_m$, $\beta, v \in V_n$ 에 대하여 $\varphi_1(u) = <\alpha,u>$ 과 $\varphi_2(v) = <\beta,v>$ 은 아핀 함수이다. 그러면 $<\eta_{f_1}, l_1> \leq 2^m - 2d_1$ 이고 $d_2 \leq d(f_2,\varphi_1) \leq 2^m - d_2$ 이기 때문에

$$2d_2 - 2^m \leq <\eta_{f_2}, l_1> \leq 2^m - 2d_2 .$$

역시, $<\eta_{g_1}, l_2> \leq 2^n - 2d_3$ 이고 $<\eta_{g_2}, l_2> \leq 2^n - 2d_4$ 이다. 따라서,

$$\begin{aligned}
<\eta_h, L> &= <\frac{1}{2}(\eta_{f_1}+\eta_{f_2}) \otimes \eta_{g_1} + \frac{1}{2}(\eta_{f_1}-\eta_{f_2}) \otimes \eta_{g_2}, \\
&\quad l_1 \otimes l_2> \\
&= \frac{1}{2} <(\eta_{f_1}+\eta_{f_2}) \otimes \eta_{g_1}, l_1 \otimes l_2> \\
&\quad + \frac{1}{2} <(\eta_{f_1}-\eta_{f_2}) \otimes \eta_{g_2}, l_1 \otimes l_2> \\
&= \frac{1}{2} <(\eta_{f_1}+\eta_{f_2}), l_1><\eta_{g_1}, l_2> \\
&\quad + \frac{1}{2} <(\eta_{f_1}-\eta_{f_2}), l_1><\eta_{g_2}, l_2> \\
&= \frac{1}{2}(<\eta_{f_1}, l_1> + <\eta_{f_2}, l_1>)<\eta_{g_1}, l_2> \\
&\quad + \frac{1}{2}(<\eta_{f_1}, l_1> - <\eta_{f_2}, l_1>)<\eta_{g_2}, l_2> \\
&\leq \frac{1}{2}\{(2^m - 2d_1) + (2^m - 2d_2)\}(2^n - 2d_3) \\
&\quad + \frac{1}{2}\{(2^m - 2d_1) - (2d_2 - 2^m)\}(2^n - 2d_4) \\
&= \frac{1}{2}\{(2^{m+1} - 2(d_1+d_2)\}(2^n - 2d_3) \\
&\quad + \frac{1}{2}\{(2^{m+1} - 2(d_1+d_2)\}(2^n - 2d_4) \\
&= (2^m - (d_1+d_2))(2^n - 2d_3) \\
&\quad + (2^m - (d_1+d_2))(2^n - 2d_4) \\
&= \{2^m - (d_1+d_2)\}(2^n - 2d_3 + 2^n - 2d_4) \\
&= \{2^m - (d_1+d_2)\}\{2^{n+1} - 2(d_3+d_4)\} \\
&= 2^{m+n+1} - 2^{m+1}(d_3+d_4)
\end{aligned}$$

$$-2^{n+1}(d_1+d_2)+2(d_1+d_2)(d_3+d_4).$$

따라서, $<\eta_h, L>$ 은

$2^{m+n+1}-2^{m+1}(d_3+d_4)-2^{n+1}(d_1+d_2)+2(d_1+d_2)(d_3+d_4)$ 보다 크지 않다.

성질 2.4에 의하여, $d(h,\varphi)=2^{m+n-1}-\frac{1}{2}<\eta_h, L>$ 은

$2^m(d_3+d_4)+2^n(d_1+d_2)-(d_1+d_2)(d_3+d_4)-2^{m+n-1}$ 보다 작지 않다. h 는 η_h 에 대응되는 함수이고 φ 은 임의의 아핀 함수이기 때문에

$$N_h \geq 2^m(d_3+d_4)+2^n(d_1+d_2)-(d_1+d_2)(d_3+d_4)-2^{m+n-1}$$

이다.

예제 3.1. 성질 3.1에서 $m=9, n=5, k=1, s=4$ 그리고 $r=3$ 라 놓으면 $\#(\Phi_{9,5})=16$, $\#(\Omega_{1,5})=26$, $\#(\Phi_{4,3})=2$, $\#(\Omega_{1,3})=4$.

여기서 $y=(y_1, y_2, y_3, y_4)$, $x=(x_1, x_2, x_3, x_4, x_5)$, $w=(y, x, z)$, 그리고 $z=(z_1, z_2, z_3, z_4)$이다. 그리고 $\Phi_{9,5}=\{\varphi_0, \varphi_1, \cdots, \varphi_{15}\}$를 V_5 상에서 $\Omega_{1,5}$로부터 선택된 각각에 대한 선형 함수들의 집합이라 하자. 이제

$\varphi_0=x_1\oplus x_2$, $\varphi_1=x_1\oplus x_3$ $\varphi_2=x_1\oplus x_4$,

$\varphi_3=x_1\oplus x_5$, $\varphi_4=x_4\oplus x_5$, $\varphi_5=x_1\oplus x_2\oplus x_3$,
$\varphi_6=x_1\oplus x_2\oplus x_4$, $\varphi_7=x_1\oplus x_3\oplus x_4$,
$\varphi_8=x_1\oplus x_4\oplus x_5$, $\varphi_9=x_2\oplus x_3\oplus x_4$,
$\varphi_{10}=x_2\oplus x_4\oplus x_5$, $\varphi_{11}=x_3\oplus x_4\oplus x_5$,
$\varphi_{12}=x_1\oplus x_2\oplus x_3\oplus x_4$, $\varphi_{13}=x_1\oplus x_2\oplus x_3\oplus x_5$,
$\varphi_{14}=x_1\oplus x_3\oplus x_4\oplus x_5\varphi_{15}=x_1\oplus x_2\oplus x_3\oplus x_4\oplus x_5$

라 놓자. 그러면 $t=1$. 지금

$$\begin{aligned}g_1(y,x)&=D_{\alpha_0}(y)\varphi_0(x)\oplus\cdots\oplus D_{\alpha_{15}}(y)\varphi_{15}(x)\\&=(y_1\oplus y_3\oplus y_4\oplus y_3y_4\oplus y_1y_2y_3\oplus y_1y_2y_4\oplus y_1y_2y_3y)x_1\\&\oplus(1\oplus y_1\oplus y_2\oplus y_3\oplus y_4\oplus y_3y_4\oplus y_1y_2y_4\oplus y_1y_3y_4\\&\oplus y_2y_3y_4)x_2\oplus(1\oplus y_1\oplus y_2\oplus y_3\oplus y_1y_3\oplus y_2y_3\\&\oplus y_1y_4\oplus y_2y_4\oplus y_1y_2y_3)x_3\oplus(y_1\oplus y_2\oplus y_3\oplus y_1y_2\\&\oplus y_1y_3\oplus y_2y_3\oplus y_2y_4\oplus y_3y_4\oplus y_1y_2y_3\oplus y_1y_3y_4\\&\oplus y_1y_2y_3y_4)x_4\oplus(y_1\oplus y_2\oplus y_1y_4\oplus y_2y_3\oplus y_2y_4\\&\oplus y_3y_4\oplus y_1y_2y_4)x_5\end{aligned}$$

이라 놓으면 g_1 은 V_9상에서 위수 1인 균형상관면역함수이고 정리 성질 2.5에 의하여

$$240\leq N_{g_1}\leq 244.$$

지금, $\{f_0, f_1, \cdots, f_{15}\}$을 V_4 상에서 위수 1인 상관면역

〔표 1〕 위수 1인 상관면역함수와 비선형도 범위

i	$\psi_0(v)$	$\psi_1(v)$	f_i	위수	비선형도
0	$z_2\oplus z_3$	$z_2\oplus z_4$	$z_2\oplus z_3\oplus z_1z_3\oplus z_1z_4$	1	$4\leq N_{f_0}\leq 4$
1	$z_2\oplus z_3\oplus z_4$	$z_3\oplus z_4$	$z_1\oplus z_3\oplus z_4\oplus z_1z_2$	1	$4\leq N_{f_1}\leq 4$
2	$z_2\oplus z_3$	$z_3\oplus z_4$	$z_2\oplus z_3\oplus z_1z_2\oplus z_1z_4$	1	$4\leq N_{f_2}\leq 4$
3	$z_2\oplus z_3\oplus z_4$	$z_2\oplus z_4$	$z_2\oplus z_3\oplus z_4\oplus z_1z_3$	1	$4\leq N_{f_3}\leq 4$

함수의 집합이라 하자.

$$g_2(y,z)=D_{\alpha_0}(y)f_0(z)\oplus\cdots\oplus D_{\alpha_{15}}(y)f_{15}(z),$$

$$\Phi_{4,3}=\{\psi_0, \psi_1\},$$

$$\Omega_{1,3}=\{\psi \mid \psi(v)=<\alpha, v>, \alpha\in V_3, W(\alpha)\geq 2\}$$

$$=\{z_2\oplus z_3, z_2\oplus z_4, z_3\oplus z_4, z_2\oplus z_3\oplus z_4\}$$

라 놓자. 단, 여기서

$u=(z_1)$, $v=(z_2, z_3, z_4)$, $z=(u,v)=(z_1, z_2, z_3, z_4)$이다. 이제 다음과 같은 〔표 1〕에서 처럼 V_4상에서 위수 1인 상관면역함수 $f_0, f_1, \cdots, f_{15}$ 를 설계한다.

$f_0=f_4=f_8=f_{12}$, $f_1=f_5=f_9=f_{13}$,
$f_2=f_6=f_{10}=f_{14}$, $f_3=f_7=f_{11}=f_{15}$ 라 놓자.

그러면 $N=\min N_{f_i}=4$ 이고 V_8상에서

$$\begin{aligned}g_2(y,z)&=D_{\alpha_0}(y)f_0(z)\oplus\cdots\oplus D_{\alpha_{15}}(y)f_{15}(z)\\&=(1\oplus y_1\oplus y_2\oplus y_3\oplus y_1y_2\oplus y_1y_3\oplus y_1y_4\oplus y_2y_3\\&\oplus y_2y_4\oplus y_1y_2y_3\oplus y_1y_2y_4\oplus y_1y_3y_4\oplus y_2y_3y_4\\&\oplus y_1y_2y_3y_4)z_1\oplus(1\oplus y_4\oplus y_3y_4)z_2\\&\oplus(y_1\oplus y_2\oplus y_3\oplus y_4\oplus y_1y_2\oplus y_1y_3\oplus y_1y_4\oplus y_2y_3\oplus y_2y_4\\&\oplus y_3y_4\oplus y_1y_2y_3\oplus y_1y_2y_4\oplus y_1y_3y_4\oplus y_2y_3y_4\oplus\\&y_1y_2y_3y_4)z_3\oplus(1\oplus y_1\oplus y_2\oplus y_3\oplus y_1y_2\oplus y_1y_3\\&\oplus y_1y_4\oplus y_2y_3\oplus y_2y_4\oplus y_3y_4\oplus y_1y_2y_3\oplus y_1y_2y_4\\&\oplus y_1y_3y_4\oplus y_2y_3y_4\oplus y_1y_2y_3y_4)z_4\\&\oplus(1\oplus y_1\oplus y_2\oplus y_1y_2\oplus y_1y_3\oplus y_1y_4\oplus y_2y_3\oplus y_2y_4\oplus y_3y_4\\&\oplus y_1y_2y_3\oplus y_1y_2y_4\oplus y_1y_3y_4\oplus y_2y_3y_4)z_1z_2\\&\oplus(1\oplus y_3\oplus y_4)z_1z_3\oplus(1\oplus y_4)z_1z_4\end{aligned}$$

이다. 따라서, $g(y,x,z)$는 V_{13} 상에서

$$\begin{aligned}g(y,x,z)&=g_1(y,x)\oplus g_2(y,z)\\&=(y_1\oplus y_3\oplus y_4\oplus y_3y_4\oplus y_1y_2y_3\oplus y_1y_2y_4\\&\oplus y_1y_2y_3y_4)x_1\oplus(1\oplus y_1\oplus y_2\oplus y_3\oplus y_4\oplus y_3y_4\end{aligned}$$

$$\oplus y_1y_2y_4\oplus y_1y_3y_4\oplus y_2y_3y_4)x_2\oplus(1\oplus y_1\oplus y_2$$
$$\oplus y_3\oplus y_1y_3\oplus y_2y_3\oplus y_1y_4\oplus y_2y_4\oplus y_1y_2y_3)x_3$$
$$\oplus(y_1\oplus y_2\oplus y_3\oplus y_1y_2\oplus y_1y_3\oplus y_2y_3\oplus y_2y_4$$
$$\oplus y_3y_4\oplus y_1y_2y_3\oplus y_1y_3y_4\oplus y_1y_2y_3y_4)x_4\oplus(y_1$$
$$\oplus y_2\oplus y_1y_4\oplus y_2y_3\oplus y_2y_4\oplus y_3y_4\oplus y_1y_2y_4)x_5$$
$$\oplus(1\oplus y_1\oplus y_2\oplus y_3\oplus y_1y_2\oplus y_1y_3\oplus y_1y_4\oplus y_2y_3$$
$$\oplus y_2y_4\oplus y_1y_2y_3\oplus y_1y_2y_4\oplus y_1y_3y_4\oplus y_2y_3y_4$$
$$\oplus y_1y_2y_3y_4)z_1\oplus(1\oplus y_4\oplus y_3y_4)z_2\oplus(y_1\oplus y_2$$
$$\oplus y_3\oplus y_4\oplus y_1y_2\oplus y_1y_3\oplus y_1y_4\oplus y_2y_3\oplus y_2y_4$$
$$\oplus y_3y_4\oplus y_1y_2y_3\oplus y_1y_2y_4\oplus y_1y_3y_4\oplus y_2y_3y_4$$
$$\oplus y_1y_2y_3y_4)z_3\oplus(1\oplus y_1\oplus y_2\oplus y_3\oplus y_1y_2$$
$$\oplus y_1y_3\oplus y_1y_4\oplus y_2y_3\oplus y_2y_4\oplus y_3y_4\oplus y_1y_2y_3$$
$$\oplus y_1y_2y_4\oplus y_1y_3y_4\oplus y_2y_3y_4\oplus y_1y_2y_3y_4)z_4$$
$$\oplus(1\oplus y_1\oplus y_2\oplus y_1y_2\oplus y_1y_3\oplus y_1y_4\oplus y_2y_3$$
$$\oplus y_2y_4\oplus y_3y_4\oplus y_1y_2y_3\oplus y_1y_2y_4\oplus y_1y_3y_4$$
$$\oplus y_2y_3y_4)z_1z_2\oplus(1\oplus y_3\oplus y_4)z_1z_3$$
$$\oplus(1\oplus y_4)z_1z_4.$$

$t=4$ 에 대하여 $N_{g_2}\geq 2^{8-1}-4\cdot 2^{4-1}=96$ 임을 기억하자.

그러므로, 성질 3.1에 의하여 g 는 V_{13}상에서 위수 3인 상관면역함수이고

$$N_g\geq 2^{9+4-1}-1\cdot 2^5(2^{4-1}-4)=3{,}712.$$

Ⅳ. 결 론

위의 예제에서 보듯이 저차원의 벡터공간에서 만들어진 여러 개의 상관면역함수를 조합하여 고차원 벡터공간위에서 함수를 설계하면 비선형도가 상당히 높이 증가하는 것을 볼 수 있었다. 즉, 두 개의 함수의 직합으로 설계된 새로운 상관면역함수와 네 개의 함수의 조합으로 설계된 새로운 상관면역함수의 비선형도가 각각의 이전 함수들과 비교하여 더 높은 비선형도를 갖는다는 것을 보였다. 또한 위의 방법을 응용하면 상대적으로 비도가 높은 상관공격으로부터 안전한 스트림 암호에서 사용되는 새로운 함수들을 설계할 수 있다.

논문에 쓰인 기호들

〔1〕 $d(f,g)$: $f(\alpha_i)\oplus g(\alpha_i)=1$ 인 벡터 α_i 의 개수

〔2〕 $N_f=\min_{i=0,1,\cdots,2^{m+1}-1} d(f,\varphi_i)$: V_m 위에서의 f 의 비선형도, $\varphi_0,\varphi_1,\cdots,\varphi_{2^{m+1}-1}$ 은 V_m 상에서 모든 아핀 함수들이다..

〔3〕 $D_\delta(y)=(y_1\oplus\overline{i_1})(y_2\oplus\overline{i_2})\cdots(y_n\oplus\overline{i_n})$: V_n 의 임의의 벡터 $y=(y_1,y_2,\cdots,y_n)$와 $\delta=(i_1,i_2,\cdots,i_n)$ 상에서의 함수. 여기서 $\overline{i}=1\oplus i$ 임.

〔4〕 $W(\alpha)$: 벡터 α의 영이 아닌 성분의 개수

〔5〕 $\Omega_{k,n}=\{\varphi\mid\varphi(x)=<\beta,x>,\beta\in V_n, W(\beta)\geq k+1\}$ 여기서$0\leq k<n$인 $k,n\in Z, x=(x_1,\cdots,x_n)$.

참고문헌

〔1〕 이만영, 원동호, 이민섭, 송주석, 임종인, 박춘식. "현대암호학및 응용", *홍릉출판사*, pp.90-94 (2002).

〔2〕 이민섭. "현대암호학", *교우사*, pp.196-258 (2002).

〔3〕 Camion, P., Carlet, C., Charpin, P. and Sendrier, N., On correlation immune functions, *In Advances in Cryptology:Crypto'91 Proceeding, Lecture Notes in Computer Science*, v.576, pp.87-100, Springer-Verlag, Berlin-Heidelberg-New York, 1991.

〔4〕 Zhen, X. G. and Massey, J. L., A spectral characterization of correlation immune combining functions, *IEEE Transactions on Information Theory*, 1988.

〔5〕 Meier, W. and Staffelbach, O., Nonlinearity criteria for crypto-graphic functions, *In Advances in Cryptology EUROCRYPT'89, Lecture Notes in Computer Science*, v.434, pp.549-562, Springer-Verlag, 1990.

〔6〕 Seberry, J. and Zhang, X. M., Highly nonlinear 0-1 balanced functions satisfying *SAC. In Advances in Cryptology AUSCRYPT'92, Lecture Notes in Computer Science*, v.718, pp.145-155, Springer-Verlag, 1992.

〔7〕 Seberry, J., Zhang, X. M. and Zheng, Y., On constructions and Nonlinearity of correlation-immune functions, *In Advances in Cryptology-EUROCRYPT'93, Lecture Notes in Computer Science*, v.765, pp.181-199, Springer-Verlag, Berlin, Heidelberg, New

York, 1994.

〔8〕 Seberry, J. and Zhang, X. M., Relating Nonlinearity to Propagation characteristics, *Cryptography, Lecture Notes in Computer Science*, v.1029, pp.283-297, Springer-Verlag, AUSTRALIA,1995.

〔9〕 Siegenthaler, T., Correlation-immunity of non-linear combining functions for cryptographic applications, IEEE Transactions on Information Theory, IT-30, No. 5: pp.776-779, 1984.

〈著者紹介〉

양 정 모 (Jeong-mo Yang) 종신회원

1984년 2월 : 동국대학교 사범대학 수학과 (이학사)
1989년 2월 : 동국대학교 사범대학 수학과 (이학 석사)
1997년 2월 : 단국대학교 대학원 수학과 (이학 박사)
1995년 ~현재 : 중부대학교 공과대학 정보보호학과 부교수
한국정보보호학회 교육이사, 대한수학회 정회원
<관심분야> 암호학, 부호이론