Nonlinear Vector Resilient Functions

Jung Hee Cheon

International Research center for Information Security (IRIS)
Information and Communications University (ICU), Taejon, Republic of Korea
jhcheon@icu.ac.kr
http://vega.icu.ac.kr/~jhcheon

Abstract. An (n, m, k)-resilient function is a function $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m$ such that every possible output m-tuple is equally likely to occur when the values of k arbitrary inputs are fixed by an adversary and the remaining $n-k$ input bits are chosen independently at random. In this paper we propose a new method to generate a $(n+D+1, m, d-1)$-resilient function for any non-negative integer D whenever a $[n, m, d]$ linear code exists. This function has algebraic degree D and nonlinearity at least $2^{n+D} - 2^n\lfloor\sqrt{2^{n+D+1}}\rfloor + 2^{n-1}$. If we apply this method to the simplex code, we can get a $(t(2^m-1)+D+1, m, t2^{m-1}-1)$-resilient function with algebraic degree D for any positive integers m, t and D. Note that if we increase the input size by D in the proposed construction, we can get a resilient function with the same parameter except algebraic degree increased by D.

Keywords: Resilient functions, nonlinearity, correlation immunity, linearized polynomials

1 Introduction

An (n, m, k)-resilient function is a function $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m$ such that every possible output m-tuple is equally likely to occur when the values of k arbitrary inputs are fixed by an adversary and the remaining $n-k$ input bits are chosen independently at random. The concept was introduced by Chor *et al.* in [8] and independently by Bennett *et al.* in [1]. It was called just *a resilient function* in those references. We call it a vector resilient function when we need to distinguish it from a resilient function with $m = 1$ since the term 'a resilient function' was regarded as a balanced correlation immune function, i.e. a resilient function with $m = 1$ in recent references [17,21]. The application area of this function includes fault-tolerant distributed computing [8], privacy amplification [1,2] and a combining generator for stream ciphers. A resilient function is also closely related to the coloring problem [9] to find the smallest k such that $(2^m; n, k)$-coloring exists. *$(2^m; n, k)$-coloring is a coloring of the n-dimensional Boolean cube with 2^m colors such that in every k-dimensional subcube each color appears $2^k/2^m$ times.*

Almost all of works on resilient functions with few exceptions [5,20,23] deals with linear resilient functions or resilient functions with a single bit output. In

J. Kilian (Ed.): CRYPTO 2001, LNCS 2139, pp. 458–469, 2001.

[10,3], they focused on finding a bound on a resiliency of a vector Boolean function with algebraic degree one. In [6,7,16,17,18,21], they focused on constructing a resilient function with a single bit output having as high as nonlinearity as possible. In [23], Zhang and Zheng proposed a method to construct a nonlinear vector resilient function from a linear vector resilient function by permuting nonlinearly its output bits. This method gives an easy transformation from a linear resilient function to a nonlinear resilient function, but has a disadvantage that a resilient function with m bit output constructed by the method has algebraic degree at most m. In [20], Stinson and Massey proposed nonlinear resilient functions, which are the counterexamples of the conjecture: *If there exist a resilient function with certain parameters, then there exists a linear resilient function with the same parameters.* They proposed infinitely many functions, but it covers only special parameters.

In this paper, we propose a new method to construct nonlinear vector resilient functions using linearized polynomial. A linearized polynomial $R(x)$ is a polynomial over $\mathbb{F}_{2^n}$ such that every term of $R(x)$ has degree of a power of 2. An equivalent definition is that the set of roots of $R(x)$ in its splitting field forms a vector space over $\mathbb{F}_2$. Given positive integers n, m and D, let d to be the minimal distance of certain m-dimensional linear code with length n. If we take a linearized polynomial $R(x)$ whose roots forms a n-dimensional subspace of $\mathbb{F}_{2^{n+D+1}}$, then some projection of $R(x)^{-1}+x$ to $\mathbb{F}_{2^m}$ is a $(n+D+1, m, d-1)$-resilient function under the basis whose dual contains a subset generating the set of roots of $R(x)$. We can easily find such a projection using a $[n, m, d]$ linear code. Such a function has algebraic degree D and nonlinearity at least $2^{n+D} - 2^n \lfloor \sqrt{2^{n+D+1}} \rfloor + 2^{n-1}$. To sum up, we can construct a $(n+D+1, m, d-1)$-resilient function with algebraic degree D whenever a $[n, m, d]$ linear code exists. Observe that by increasing the input size by D we can construct a resilient function with the same parameter except algebraic degree increased by D.

A simplex code is a $[2^m-1, m, 2^{m-1}]$ linear code, whose minimal distance is maximal. By concatenating each codeword t times, we get a $[t(2^m-1), m, t2^{m-1}]$ linear code. Using this code, we can construct a $(t(2^m-1)+D+1, m, t2^{m-1}-1)$-resilient function with algebraic degree D for any positive integers m, t and D. It has nonlinearity greater than or equal to

$$2^{t(2^m-1)+D} - 2^{t(2^m-1)} \lfloor \sqrt{2^{t(2^m-1)+D+1}} \rfloor + 2^{t(2^m-1)-1}.$$

In Section 2, we introduce some notation and definitions of cryptographic properties. In Section 3, we propose a new method to construct a resilient function from a linearized polynomial. In Section 4, we prove the algebraic degree of the proposed resilient function. In Section 5, we deal with nonlinearity. In Section 6, we generalize the method in Section 3 into a vector resilient function. In Section 7, we apply the proposed vector resilient function for a combining generator with multi-bit output, a kind of stream cipher. We conclude in Section 8.

2 Boolean Functions and Nonlinearity

Let E be a vector space of finite dimension n over the finite field $\mathbb{F}_2$. A function f from E into $\mathbb{F}_2$ is called *a Boolean function.* The cardinality of the set $\{x \in E | f(x) = 1\}$ is called the *weight* of f and denoted by $\mathrm{wt}(f)$. The degree of f, denoted by $\deg(f)$, is the maximal value of the degrees of the terms of f when expressed in the reduced form, called the *algebraic normal form.* A function with degree 1 is called an affine function. The *Hamming distance* between two function f and g is the weight of $f + g$. The minimal distance between f and any affine function from E into $\mathbb{F}_2$ is the *nonlinearity* of f, that is:

$$\mathcal{N}(f) = \min_{\phi \in \Gamma} \mathrm{wt}(f + \phi) \tag{1}$$

where Γ is the set of all affine functions over E.

A function $F : E \to \mathbb{F}_{2^m}$ is called *a vector Boolean function.* Note that if a basis of $\mathbb{F}_{2^m}$ over $\mathbb{F}_2$ is specified, there are the unique Boolean function f_i's such that $F = (f_1, f_2, \cdots, f_m)$. We denotes by $b \cdot F$ the Boolean function $b_1 f_1 + b_2 f_2 + \cdots + b_n f_n$ for $b = (b_1, b_2, \cdots, b_m) \in \mathbb{F}_{2^m}$. Using this notation, we can write Γ as follows:

$$\Gamma = \{a \cdot x + \delta | a \in E, \delta \in \mathbb{F}_2\}. \tag{2}$$

Definition 1. *The nonlinearity $\mathcal{N}(F)$ of a Boolean function $F : E \to \mathbb{F}_{2^m}$ is defined as*

$$\mathcal{N}(F) = \min_{b \in \mathbb{F}_{2^m}^*} N(b \cdot F) = \min_{b \in \mathbb{F}_{2^m}^*, \phi \in \Gamma} wt(b \cdot F + \phi) \tag{3}$$

where Γ is the set of all affine functions over E. Or equivalently,

$$\mathcal{N}(F) = \min_{a \in E, b \in \mathbb{F}_{2^m}^*, \delta \in \mathbb{F}_2} wt(b \cdot F + a \cdot x + \delta). \tag{4}$$

The Walsh-Hadamard transformation of a Boolean function f is defined as

$$W_f(a) = \sum_{x \in E} (-1)^{f(x) + a \cdot x}, \quad a \in E. \tag{5}$$

Since $W_f(a) = wt(f(x) + a \cdot x) - wt(f(x) + a \cdot x + 1)$, we have

$$\mathcal{N}(f) = 2^{n-1} - \frac{1}{2} \max_{a \in E} |W_f(a)|. \tag{6}$$

Definition 2. *A Boolean function $f : E \to \mathbb{F}_2$ is called a k-th order correlation immune function if $W_f(a) = 0$ for all $a \in E$ with $0 < wt(a) \leq k$. A k-th order correlation immune function is called a k-resilient function if it is balanced(i.e. $W_f(0) = 0$).*

Definition 3. *A vector Boolean function $F : E \to \mathbb{F}_{2^m}$ is called a k-resilient function or a (n, m, k)-resilient function for the dimension n of E if $b \cdot F$ is a k-resilient function for any $b \in \mathbb{F}_{2^m}^*$.*

3 Resiliency

Throughout this paper, let $q = 2^n$ for a positive integer n. A polynomial in $\mathbb{F}_q[x]$ is called a linearized polynomial if each of its terms has degree of a power of 2 [14]. Let $R(x) = \sum_{i=0}^{h} A_i x^{2^i}$ $(A_i \in \mathbb{F}_{2^n})$ be a linearized polynomial over $\mathbb{F}_{2^n}$ and $N_R(\mathbb{F}_q) = \{x \in \mathbb{F}_q | R(x) = 0\}$ be the set of zeros of $R(x)$ which forms a subspace of $\mathbb{F}_q$. From now on, we define the inversion function $R(x)^{-1}$ to be $R(x)^{2^n-2}$. Note that if we represent $a, b \in \mathbb{F}_q$ by a basis and its dual basis, respectively, we have $a \cdot b = Tr[ab]$ where $Tr[\cdot]$ is the trace function from $\mathbb{F}_q$ to $\mathbb{F}_2$.

Lemma 1. *[11] Let $a, b \in \mathbb{F}_q$, $R(x)$ a linearized polynomial and $F(x) = 1/R(x)$. If $Tr[ax]$ does not vanish identically on $N_R(\mathbb{F}_q)$, then*

$$W_{Tr[bF(x)]}(a) = 0.$$

Proof. Suppose $x_0 \in \mathbb{F}_q \setminus N_R(\mathbb{F}_q)$. For $x = x_0 + x'$ with $x' \in N_R(\mathbb{F}_q)$, we have $Tr[ax + \frac{b}{R(x)}] = Tr[ax_0 + \frac{b}{R(x_0)}] + Tr[ax']$ and this is zero for $\# N_R(\mathbb{F}_q)/2$ elements x'. Since a half of elements of each coset of $N_R(\mathbb{F}_q)$ satisfies $Tr[ax + \frac{b}{R(x)}] = 0$, we have $W_{Tr[bF]}(a) = 0$.

Using this, we can derive the following.

Theorem 1. *Let $R(x)$ be a linearized polynomial such that $N_R(\mathbb{F}_q)$ is generated by $\{\xi_1, \xi_2, \cdots, \xi_w\}$ for some $w > 0$, and let $F(x) = 1/R(x) + cx$ for $c \in \mathbb{F}_q$. Suppose $\mathcal{B} = \{\xi_1, \xi_2, \cdots, \xi_n\}$ is a basis of $\mathbb{F}_q$ and $\hat{\mathcal{B}} = \{\widehat{\xi_1}, \widehat{\xi_2}, \cdots, \widehat{\xi_n}\}$ its dual basis. Then $Tr[bF]$ is a $(t-1)$-resilient function under the basis $\mathcal{B}$ if the projection of bc on $\langle \widehat{\xi_1}, \widehat{\xi_2}, \cdots, \widehat{\xi_w} \rangle$ has weight t.*

Observe that the maximum of t is w.

Proof. Let $a = \sum_{i=0}^{n} a_i \hat{\xi_i}$ and $bc = \sum_{i=1}^{n} b_i \hat{\xi_i}$. If we write $f(x) = Tr[b(1/R(x) + cx)]$, we have

$$\begin{aligned} W_f(a) \neq 0 &\Leftrightarrow Tr[(a + bc)x] = 0 \quad \text{on } N_R(\mathbb{F}_q) \\ &\Leftrightarrow Tr[(a + bc)\xi_i] = 0 \quad \text{for } 1 \leq i \leq w \\ &\Leftrightarrow a_i = b_i \quad \text{for } 1 \leq i \leq w \end{aligned}$$

Since t elements of b_i for $1 \leq i \leq w$ is equal to one, we have $W_f(a) = 0$ for all a with $0 \leq wt(a) < t$, which proves the $(t-1)$-resiliency of $Tr[bF]$.

Example 1. Let $q = 2^8$ and $V = \{\xi_1, \xi_2, \xi_3, \xi_4\}$ a set of linearly independent elements of $\mathbb{F}_q$, and let $R(x) = \prod(x - \xi)$ where ξ ranges over all linear combinations of elements of V. Suppose $\mathcal{B} = \{\xi_1, \xi_2, \cdots, \xi_8\}$ is a basis of $\mathbb{F}_q$ and $\hat{\mathcal{B}} = \{\widehat{\xi_1}, \widehat{\xi_2}, \cdots, \widehat{\xi_8}\}$ its dual basis. Then $f(x) = Tr[(\widehat{\xi_1} + \widehat{\xi_2} + \widehat{\xi_3} + \widehat{\xi_4})(\frac{1}{R(x)} + x)]$ is a 3-resilient function under the basis $\hat{\mathcal{B}}$.

4 Algebraic Degree

Theorem 2. *Let $w \geq 0$. Consider a linearized polynomial $R(x) = \prod(x - \xi)$ where ξ ranges over all elements of a w-dimensional subspace V of $\mathbb{F}_q$. Then $F(x) = \frac{1}{R(x)}$ has the algebraic degree $n - 1 - w$.*

Proof. First, we claim that $F(x)$ has the algebraic degree $\leq n - 1 - w$. We use the induction on w. For $w = 0$, it is trivial since $F(x) = 1/x$ has the algebraic degree $n - 1$. Assume that the claim holds for all dimension less than w. Let W be a $(w - 1)$-dimensional subspace of V, $\alpha \in V \setminus W$ and $S(x) = \prod_{\zeta \in W}(x - \zeta)$. Then we have

$$\frac{1}{R(x)} = \frac{1}{S(x)S(x+\alpha)} = \frac{1}{S(x) + S(x+\alpha)} \left(\frac{1}{S(x)} + \frac{1}{S(x+\alpha)} \right). \tag{7}$$

Note that $f(x) + f(x + a)$ has algebraic degree less than that of f for any Boolean function f and $a \in \mathbb{F}_q$. Since $S(x)$ is a linearized polynomial and so has the algebraic degree 1, $S(x) + S(x + \alpha)$ is a nonzero constant for $\alpha \in W$. By the induction hypothesis, $\frac{1}{S(x)}$ has algebraic degree $\leq n - 1 - (w - 1) = n - w$. Hence $F(x)$ has algebraic degree less than $n - w$ which proves the claim.

Now we prove the equality. Suppose that there is a w-dimensional subspace V such that $\frac{1}{R(x)}$ has algebraic degree less than $n - w - 1$. Take a basis $B = \langle \xi_1, \xi_2, \cdots, \xi_n \rangle$ of $\mathbb{F}_q$ where $\xi_1, \xi_2, \cdots, \xi_w$ generates V. Take $R_w(x) = R(x)$ and $R_{i+1}(x) = R_i(x)R_i(x + \xi_i)$ for $w \leq i < n - 1$. By the same deduction with (7), $1/R_{i+1}(x)$ has algebraic degree less than $1/R_i(x)$ for $w \leq i < n - 1$. Thus, $1/R_{n-1}(x)$ has algebraic degree less than $(n - 1) - (n - 1) = 0$. That is, $1/R_{n-1}(x) = 0$ should be zero for all $x \in \mathbb{F}_q$ which implies $R_{n-1}(x) = 0$ for all $x \in \mathbb{F}_q$. This is a contradiction because R_{n-1} has only 2^{n-1} roots. Therefore we have the theorem.

Observe that if V has the dimension w, we can derive a $(w - 1)$-resilient function with the algebraic degree $n - w - 1$ from $F(x) = 1/R(x)$. From the Siegenthaler's inequality [19], we have $\deg f \leq n - 1 - (w - 1) = n - w$ for every component function f of $1/R(x)$. Thus, our resilient function has one less algebraic degree than the maximal degree achieved by $(w - 1)$-resilient functions in $\mathbb{F}_q$.

5 Nonlinearity

Consider a non-singular complete curve given by $y^2 + y = ax + \frac{b}{R(x)}$ for $a, b \in \mathbb{F}_q$. By Hurwitz-Zeuthen formula, it has the genus $g = 2^h - \delta_{a,0}$ where h is the degree of $R(x)$ and the Kronecker delta $\delta_{a,0}$ is one if and only if $a = 0$. Using the Hasse-Weil bound on the number of points of an algebraic curve, we can get the following lemma.

Lemma 2. *Let $R(x)$ be a linearized polynomial such that $N_R(\mathbb{F}_q)$ is generated by $\{\xi_1, \xi_2, \cdots, \xi_w\}$ for some $0 < w < n$. Let $a, b \in \mathbb{F}_q$ and $b \neq 0$. Let C be a complete non-singular curve over $\mathbb{F}_q$ given by $y^2 + y = ax + \frac{b}{R(x)}$. Then we have*

$$|\#C(\mathbb{F}_q) - q - 1| \leq 2g\sqrt{q},$$

where $g = 2^w - \delta_{a,0}$ is the genus of the curve C.

Theorem 3. *Let $R(x)$ be a linearized polynomial such that $N_R(\mathbb{F}_q)$ is generated by $\{\xi_1, \xi_2, \cdots, \xi_w\}$ for some $0 < w < n$. Then we have*

$$\mathcal{N}(\frac{1}{R(x)}) \geq 2^{n-1} - 2^w \lfloor \sqrt{2^n} \rfloor + 2^{w-1}.$$

Proof. Let $F(x) = 1/R(x)$ and $b \in \mathbb{F}_q^*$.

Assume $a \neq 0$. The complete non-singular curve C given by $y^2 + y = ax + b/R(x)$ has a point at the infinity and a point on each of roots of $R(x)$. Otherwise, it has 2 points whenever $Tr[ax + b/R(x)] = 0$. Hence we have

$$\#C(\mathbb{F}_q) = 2\#\{x \in \mathbb{F}_q | Tr[ax + \frac{b}{R(x)}] = 0\} + 2^w + 1. \tag{8}$$

Assume $a = 0$. The complete non-singular curve C given by $y^2 + y = b/R(x)$ has two points at the infinity and a point on each of roots of $R(x)$. Otherwise, it has 2 points whenever $Tr[ax + b/R(x)] = 0$. Hence we have

$$\#C(\mathbb{F}_q) = 2\#\{x \in \mathbb{F}_q | Tr[ax + \frac{b}{R(x)}] = 0\} + 2^w + 2. \tag{9}$$

Observe that $\#C(\mathbb{F}_q) - 1 - \delta_{a,0}$ is divisible by 2^{w+1} from Corollary (1.5) in [11]. Since $W_{b \cdot F}(a) = 2\#\{x \in \mathbb{F}_q | Tr[ax + \frac{b}{R(x)}] = 0\} - q = \#C(\mathbb{F}_q) - 1 - \delta_{a,0} - 2^w - q$, we can write $W_{Tr[bF]}(a) = s \cdot 2^{w+1} - 2^w$ for some integer s.

On the other hand, by Lemma 2, for all a we have

$$|\#C(\mathbb{F}_q) - q - 1| = |s \cdot 2^{w+1} + \delta_{a,0}| \leq 2(2^w - \delta_{a,0})\sqrt{q}.$$

That is, we have $|s| \leq \lfloor \sqrt{q} \rfloor$.

Combining them, we find that the maximum of $|W_{Tr[bF]}(a)|$ is bounded by $2^{w+1}\lfloor \sqrt{q} \rfloor - 2^w$. From 6, we get the theorem.

Observe that this bound of nonlinearity is very tight for small w, but not so good for large w.

6 Vector Resilient Functions

We begin with some basic terminology of coding theory [13]. A *linear code C* is a linear subspace of $\mathbb{F}_2^n$. An element of C is called a *codeword.* The *minimum* *distance* of C is defined as the minimum of weights of all nonzero codewords in C. A $[n, m, d]$ *code* is a m-dimensional linear code of length n with minimum distance d.

Suppose W is a vector space generated by $\{e_1, e_2, e_3\}$. Then $V = \langle e_1+e_2+e_3\rangle$ is a $[3, 1, 3]$ linear code since V has one nonzero element $e_1 + e_2 + e_3$ with weight 3. If we define $V = \langle e_1 + e_2, e_2 + e_3\rangle$, it is a $(3, 2, 2)$ linear code since every nonzero element of V has weight 2.

Theorem 4. *Let $R(x)$ be a linearized polynomial such that $N_R(\mathbb{F}_q)$ is generated by $\{\xi_1, \xi_2, \cdots, \xi_w\}$ for some $w > 0$, and $F(x) = 1/R(x) + x$. Suppose $\mathcal{B} = \{\xi_1, \xi_2, \cdots, \xi_n\}$ is a basis of $\mathbb{F}_q$ and $\hat{\mathcal{B}} = \{\widehat{\xi_1}, \widehat{\xi_2}, \cdots, \widehat{\xi_n}\}$ its dual basis. For $1 \le m \le w$, let $B_1, B_2, \cdots, B_m$ be elements of the vector space $\mathbb{F}_q$ with the basis $\hat{\mathcal{B}}$ whose projection on $\langle\widehat{\xi_1}, \widehat{\xi_2}, \cdots, \widehat{\xi_w}\rangle$ forms a $[w, m, d]$ linear code. Then $(Tr[B_1F], Tr[B_2F], \cdots, Tr[B_mF])$ is a $(d-1)$-resilient function under the basis $\mathcal{B}$.*

Proof. Any component function of $(Tr[B_1F], Tr[B_2F], \cdots, Tr[B_mF])$ is written as $Tr[BF]$ for $B = \sum_{i=0}^{m} b_iB_i$ with $b_i \in \mathbb{F}_2$. Observe that the projection of such B on $\langle\widehat{\xi_1}, \widehat{\xi_2}, \cdots, \widehat{\xi_w}\}\rangle$ has weight greater than or equal to d. Hence $B \cdot F$ is a $(d-1)$-resilient function by Theorem 1. Since every component function is a $(d-1)$-resilient function, so does $(Tr[B_1F], Tr[B_2F], \cdots, Tr[B_mF])$.

Using Theorem 4, we can construct a (n, m, k)-resilient function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ when $k = d(w, m) - 1$ for some w with $0 < m \le w < n$ as Algorithm 1.

Algorithm 1 (Construct a vector resilient function)

1. **Input n, m and k such that $k = d(w, m) - 1$ for some w with $0 < m \le w < n$.**
2. **Take a set $V = \{\xi_1, \xi_2, \cdots, \xi_w\}$ of w linearly independent elements of $\mathbb{F}_{2^n}$. Let $\mathcal{B} = \{\xi_1, \xi_2, \cdots, \xi_n\}$ is a basis of $\mathbb{F}_{2^n}$ and $\hat{\mathcal{B}} = \{\widehat{\xi_1}, \widehat{\xi_2}, \cdots, \widehat{\xi_n}\}$ its dual basis.**
3. **Assume a $[w, m, d]$ linear code is generated by $\{c_i, c_2, \cdots, c_m\}$ where $c_i = [c_{i1}, c_{i2}, \cdots, c_{iw}]$ and $c_{iw} \in \mathbb{F}_2$. Compute $B_i = \sum_{j=1}^{m} c_{ij}\widehat{\xi_i}$.**
4. **Let $F(x) = 1/R(x) + x$ for $R(x) = \prod_\zeta(x - \zeta)$ where ζ ranges over all elements of the subspace generated by V. Compute $Tr[B_iF(x)]$ for $1 \le i \le m$.**
5. **Output a k-resilient function**

$$S(x) = (Tr[B_1F(x)], Tr[B_2F(x)], \cdots, Tr[B_mF])$$

from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ by taking the basis $\mathcal{B}$ for $\mathbb{F}_{2^n}$.

The following is an example of Algorithm 1.

Example 2. Let $q = 2^8$ and $V = \{\xi_1, \xi_2, \xi_3\}$ a set of linearly independent elements of $\mathbb{F}_q$, and let $R(x) = \prod(x-\xi)$ where ξ ranges over all linear combinations of elements of V. Let $\mathcal{B} = \{\xi_1, \xi_2, \cdots, \xi_n\}$ is a basis of $\mathbb{F}_q$ and $\hat{\mathcal{B}} = \{\widehat{\xi_1}, \widehat{\xi_2}, \cdots, \widehat{\xi_n}\}$

its dual basis. Then (f_1, f_2) is a (8,2,1)-resilient function under the basis $\mathcal{B}$ where $f_1 = Tr[(\widehat{\xi_1} + \widehat{\xi_2})(\frac{1}{R(x)} + x)]$ and $f_2 = Tr[(\widehat{\xi_2} + \widehat{\xi_3})(\frac{1}{R(x)} + x)]$.

If we combine Theorem 2, 3 and 4, we can get the following Theorem.

Theorem 5. *Assume* $0 < m \leq n$ *and a* $[n, m, d]$ *linear code exists. For any nonnegative integer* D*, there exists a* $(n + D + 1, m, d - 1)$*-resilient function with algebraic degree* D*, whose nonlinearity is greater than or equal to* $2^{n+D} - 2^n \lfloor \sqrt{2^{n+D+1}} \rfloor + 2^{n-1}$.

Note that for any positive integer there exists a $[2^m - 1, m, 2^{m-1}]$ code, so called a simplex code, which has the maximal value of minimal distances for m-dimensional linear codes with length $2^m - 1$. Concatenating each codeword t times gives a $[t(2^m - 1), m, t2^{m-1}]$ linear code. If we apply this code to Theorem 5, we get the following result.

Corollary 1. *For any positive integers* m, t *and* D*, there is a* $(t(2^m - 1) + D + 1, m, t2^{m-1} - 1)$*-resilient function with algebraic degree* D *and nonlinearity greater than or equal to*

$$2^{t(2^m-1)+D} - 2^{t(2^m-1)} \lfloor \sqrt{2^{t(2^m-1)+D+1}} \rfloor + 2^{t(2^m-1)-1}.$$

Given positive integers n and m, we define the maximal resiliency $\kappa(n, m)$ to be the maximal value of resiliency k such that a (n, m, k)-resilient function exists. Chor *et al.* [8] showed that $\kappa(n, 2) = \lfloor \frac{2n}{3} \rfloor - 1$. For general m, Friedman [10] showed that given positive integers n and m the maximal resiliency $\kappa(n, m)$ satisfies

$$\kappa(n, m) \leq n - 1 - \frac{n(2^m - 2)}{2(2^m - 1)}. \tag{10}$$

Bierbrauer *et al.* [3] showed that a $[n, m, d]$ linear code can be used to construct a $(n, m, d - 1)$-resilient function. Combining this with (10), we find that $\kappa(t(2^m - 1), m) = t2^{m-1} - 1$. On the other hand, if we consider linear resilient functions, i.e. $D = 1$, in Corollary 1, the proposed construction gives $(t(2^m - 1) + 2, m, t2^{m-1} - 1)$-resilient function which has 2 bit larger input length with the same output size and resiliency. By this construction, however, for any positive integer D we can construct a resilient function of algebraic degree D with the same parameter by increasing the input size by D bits.

In [23], authors proposed a method to construct a nonlinear vector resilient function from a linear vector resilient function by permuting nonlinearly its output bits. That is,

Let F *be a linear* (n, m, k)*-resilient function and* G *a permutation on* $\mathbb{F}_2^m$ *whose nonlinearity is* $\mathcal{N}_G$*. Then* $P = G \cdot F$ *is a* (n, m, k)*-resilient function such that*

1. *the nonlinearity* $\mathcal{N}_P$ *of* P *satisfies* $\mathcal{N}_P = 2^{n-m}\mathcal{N}_G$ *and*
2. *the algebraic degree of* P *is the same as that of* G.

A vector Boolean function with m bit output generated by this method has an algebraic degree less than m while our method can generate a resilient function with algebraic degree up to $n-2-m$. The largest nonlinearity achieved by a permutation on $\mathbb{F}_2^m$ is $2^{m-1}-2^{(m-1)/2}$ [15]. Thus, such (n,m,k)-resilient function has nonlinearity $\leq 2^{n-1}-2^{n-(m+1)/2}$. Hence resilient functions constructed by the proposed method have larger bound of nonlinearity for small m than the previous method. Another obstacle of the previous method is to find a nonlinear permutation, which is not easy for even m except x^{-1}.

Generally, it is not easy to obtain the maximum value of m given n and d or the maximal value of d given n and m. For small n,m, however, there is a table [4] for the maximum value $d(n,m)$ of d such that a $[n,m,d]$ linear code exists. Refer to the appendix for $1 \leq n \leq 15$ and $1 \leq m \leq 6$. These maximum values of the minimum distances gives the maximal resiliency k of (n,m,k)-resilient functions with the algebraic degree D constructed by Algorithm 1. In Table 1, 0-resiliency means balancedness.

Table 1. The maximum resiliency k of proposed (n,m,k)-resilient functions with the algebraic degree D.

$m \setminus n$	$2+D$	$3+D$	$4+D$	$5+D$	$6+D$	$7+D$	$8+D$	$9+D$	$10+D$	$11+D$	$12+D$	$13+D$	$14+D$
1	0	1	2	3	4	5	6	7	8	9	10	11	12
2		0	1	1	2	3	3	4	5	5	6	7	7
3			0	1	1	2	3	3	3	4	5	5	6
4				0	1	1	2	3	3	3	4	5	5
5					0	1	1	1	2	3	3	3	4
6						0	1	1	1	2	3	3	3

7 Stream Ciphers

One of the most widely used design for stream cipher is a combination generator. A combination generator consists of several linear feedback shift registers(LFSRs) whose output sequences are combined by a nonlinear Boolean function, called a combining function. To resist against the well-known correlation attack, a combining function should be resilient. Fig. 1 is an example of a stream cipher with multi-bit output where KGSs are key stream generators and F is a combining function.

To get a high linear complexity, we use feedback shift registers with carry operation (FCSRs) [12] as KSGs instead of LFSRs in a combining generator. Let n be the number of FCSRs with k registers and m the number of output bits. By Theorem 5, we can construct a $(w+D+1,m,d-1)$-resilient function for any non-negative integer D whenever a $[w,m,d]$ linear code exists. The function has algebraic degree D and nonlinearity at least $2^{w+D}-2^{w}\lfloor\sqrt{2^{w+D+1}}\rfloor+2^{w-1}$. We use this vector resilient function as a combining function.

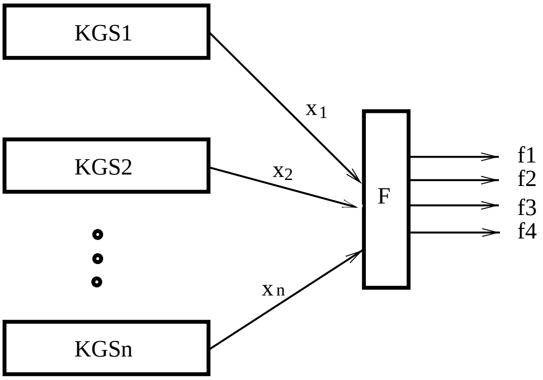

Fig. 1. A stream cipher with multi-bit output

Note that correlation attack has complexity $O(2^{kd})$ when the combining function is $(d-1)$-resilient. On the other hand, linear complexity attack has complexity $O(M^3)$ for a cipher with linear complexity M. Since every FCSR has linear complexity 2^k and the combining function has algebraic degree $n-w-1$, we have $M = 2^{k(n-w-1)}$. Hence when $d(w,m) \approx 3(n-w-1)$, two complexities are similar.

For example, if we let $n-w-1 = 2$ and $d = 5$, the complexity becomes $O(2^{3k})$. In that case, we have $w = 9$ for $m = 2$ and $w = m+8$ for $m \geq 3$. That is, if $k = 20$, we can design ciphers with the following feature. Here the complexity is against the linear complexity attack and the correlation attack for a linear combination of output bits.

However, if we consider a correlation attack using a nonlinear combination of output bits, the complexity might be different. In that case, the maximum correlation coefficient [22] should be considered. Currently, we don't know the maximum correlation of the proposed vector resilient functions. It would be interesting problem to compute them.

Table 2. Input v.s. Output with the fixed Resiliency

Input(n)	Output(m)	Dim(w)	Alg. Deg.(D)	Resiliency(k)	Complexity
12	2	9	2	5	2^{120}
14	3	11	2	5	2^{120}
15	4	12	2	5	2^{120}
17	5	14	2	5	2^{120}
18	6	15	2	5	2^{120}
19	7	16	2	5	2^{120}
21	9	18	2	5	2^{120}

8 Conclusion

In this paper we proposed a method to construct a $(n+D+1, m, d-1)$-resilient function with algebraic degree D for arbitrary positive integer D using a linearized polynomial and a $[n, m, d]$ linear code. Since its nonlinearity is related with the number of rational points of associated algebraic curves, we can find a bound of its nonlinearity using Hasse-Weil bound of algebraic curves. Applying this method to the well-known simplex code gives a $(t(2^m-1)+D+1, m, t2^{m-1}-1)$-resilient function with algebraic degree D for any positive integers m, t and D. Note that if we increase the input size by D in the proposed construction, we can get a resilient function with the same parameter except algebraic degree increased by D. In author's knowledge, this method is the first one to generate a nonlinear vector resilient function with larger algebraic degree than the output size.

Acknowledgements. The author would like to thank Dr. Seongtaek Chee, Prof. Joseph Silverman, and Prof. Kyeongcheol Yang for helpful discussion and comments. This work was supported by postdoctoral fellowship program from Korea Science and Engineering Foundation (KOSEF).

References

1. C. Bennett, G. Brassard, and J. Robert, "Privacy Amplification by Public Discassion," SIAM J. Computing, Vol. 17, pp.210-229, 1988.
2. C. Bennett, G. Brassard, C. Crépeau, and U. Maurer, "Generalized Privacy Amplification," IEEE Trans. on Information Theory, Vol. 41, No. 6, pp. 1915-1923, 1995.
3. J. Bierbrauer, K. Gopalakrishnan, and D. Stinson, "Bounds on Resilient Functions and Orthogonal Arrays, " Proc. of Crypto'94, pp.247-256, Springer-Verlag, 1994.
4. A. Brouwer and T. Verhoeff, "An Updated Table of Mimimum-Distance Bounds for Binary Linear Codes," IEEE Trans. on Infomation Theory, Vol. 39, No. 2, pp.662-677, 1993.
5. J. Cheon and S. Chee, "Elliptic Curves and Resilient Functions," Proc. of ICISC'00, pp.64-72, 2000.
6. P. Camion, C. Carlet, P. Charpin, and N. Sendrier, "On Correlation Immune Functions," Proc. of Crypto'91, pp.86-100, Springer-Verlag, 1992.
7. S. Chee, S. Lee, D. Lee, and S. Sung, "On the Correlation Immune Functions and their Nonlinearity," Proc. of Asiacrypt'96, pp.232-243, Springer-Verlag, 1996.
8. B. Chor, O. Goldreich, J. Hastad, J. Friedman, S. Rudich, and R. Smolensky, "The Bit Extraction Problem or t-Resilient Functions," IEEE Symposium on Foundations of Computer Science, Vol. 26, pp. 396-407, 1985.
9. K. Friedl and S.C. Tsai, "Two Results on the Bit Extraction Problem", Discrete Applied Mathematics, Vol 99, pp. 443–454, 2000
10. J. Friedman, "On the Bit Extraction Problem," Proc. of 33rd IEEE Symposium on Foundations of Computer Science, pp.314-319, 1992.
11. G. van der Geer and M. van der Vlugt, "Trace Codes and Families of Algebraic Curves," Math. Z., Vol. 209, pp.307-315, Springer-Verlag, 1992.

12. A. Klapper and M. Goresky, "Feedback Shift Registers, Combiners with Memory, and 2-adic Span," Journal of Cryptology, Vol. 10, Springer-Verlag, pp. 111-147, 1997.
13. J.H. van Lint, *Intoroduction to Coding Theory*, Springer-Verlag, 1992.
14. R. Lidl and H. Niederreiter, *Finite Fields*, Cambridge University Press, 1997.
15. K. Nyberg, "S-Boxes and Round Functions with Controllable Linearity and Differential Uniformity," Proc. of the Second Fast Software Encryption, pp. 111 – 130, Springer-Verlag, 1994.
16. E. Pasalic and T. Johansson, "Further Results on the Relation Between Nonlinearity and Resiliency for Boolean Functions," Proc. of IMA Conference on Cryptography and Coding, pp. 35-44, LNCS 1746, Springer-Verlag, 1999.
17. P. Sarkar and S. Maitra, "Nonlinearity Bounds and Constructions of Resilient Boolean Functions," Proc. of Crypto'00, pp. 515-532, Springer-Verlag, 2000.
18. J. Seberry, X. Zhang and Y. Zheng, "On Constructions and Nonlinearity of Correlation Immune Boolean Functions," Eurocrypt'93, pp. 181-199, Springer-Verlag, 1993.
19. T. Siegenthaler, "Correlation-Immunity of Nonlinear Combining Functions for Cryptographic Applications," IEEE Transactions on Information Theory, IT-30(5), pp.776-780, 1984.
20. D. Stinson and J. Massey, "An Infinite Class of Counterexamples to a Conjecture Concerning Nonlinear Resilient Functions," Journal of Cryptology, Vol 8, No. 3, pp.167-173, Springer-Verlag, 1995.
21. Y. Tarannikov, "On Resilient Boolean Functions with Maximum Possible Nonlinearity," Proc. of Indocrypt'00, pp.19-30, Springer-Verlag, 2000.
22. M. Zhang and A. Chan, "Maximum Correlation Analysis of Nonlinear S-boxes in Stream Ciphers," Proc. of Crypto2000, pp. 501-514, Springer-Verlag, 2000.
23. X. Zhang and Y. Zheng, "Cryptographically Resilient Functions," IEEE Trans. Inform. Theory, Vol 43, No 5, pp. 1740-1747, 1997.

Appendix: Minimum Distance of Linear Codes

For given $n, m \leq 127$, there is a table [4] for the maximum value of d such that a $[n, m, d]$ linear code exists. Some of them are as below:

Table 3. The maximum d such that a $[n, m, d]$ linear code exists.

$m \setminus n$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
2		1	2	2	3	4	4	5	6	6	7	8	8	9	10
3			1	2	2	3	4	4	4	5	6	6	7	8	8
4				1	2	2	3	4	4	4	5	6	6	7	8
5					1	2	2	2	3	4	4	4	5	6	7
6						1	2	2	2	3	4	4	4	5	6