Cryptographically Resilient Functions [*]

Xian-Mo Zhang
Department of Computer Science
University of Wollongong
Wollongong, NSW 2522, Australia
xianmo@cs.uow.edu.au

Yuliang Zheng
The Peninsula School of Computing and Information Technology
Monash University, Frankston
Melbourne, VIC 3199, Australia
yzheng@fcit.monash.edu.au

Abstract

This paper studies resilient functions which have applications in fault-tolerant distributed computing, quantum cryptographic key distribution and random sequence generation for stream ciphers. We present a number of methods for synthesizing resilient functions. An interesting aspect of these methods is that they are applicable both to linear and to nonlinear resilient functions. Our second major contribution is to show that every linear resilient function can be transformed into a large number of nonlinear resilient functions with the same parameters. As a result, we obtain resilient functions that are highly nonlinear and have a high algebraic degree.

1 Introduction

A (n, m, t)-resilient function is an n-input m-output function F with the property that it runs through every possible output m-tuple an equal number of times when t arbitrary inputs are fixed and the remaining $n-t$ inputs runs through all the 2^{n-t} input tuples once. The concept was introduced by Chor *et al* in [5] and independently, by Bennett *et al* in [1]. It turned out that (balanced) correlation immune functions introduced by Siegenthaler [20] is a special case of resilient functions. Areas where resilient functions find their applications include fault-tolerant distributed computing, quantum cryptographic key distribution and random sequence generation for stream ciphers.

Researchers have concentrated themselves on linear resilient functions, with only one exception being the work by Stinson and Massey [22]. The two researchers' aim was solely to disprove a conjecture that if there exists a nonlinear resilient function then there exists a linear resilient function with the same parameters which was posed in [5], rather than to explore cryptographic merits of nonlinear resilient functions. Recent advances in cryptanalysis, in particular the discovery of the linear cryptanalytic attack [12], have shown the vital importance of nonlinear functions in data encryption and one-way hashing algorithms. With the further revelation of the potential power of the linear attack, we might see its serious implications on the security of many other cryptographic routines, including those employing resilient functions. A relevant but earlier development is the best affine approximation (BAA) attack proposed by Ding, Xiao and Shan in [6]. It has been shown in their book that the BAA attack can successfully break a number of types of key stream generators that employ a combining or filtering function which, though correlation immune, has a *low* nonlinearity. Success

[*] To be presented at EUROCRYPT'95, May 1995, France

of these attacks clearly shows a need to investigate highly nonlinear resilient functions.

The rest of the paper is organized as follows: Section 2 introduces basic definitions. It also reviews important properties of resilient functions, as well as previous work in the area. Section 3 presents a number of methods for constructing new resilient functions from old. Some of them significantly generalize methods known previously. An exceptional feature of these methods is that they can be applied *both to linear and to nonlinear* resilient functions. Section 4 shows how to turn a known resilient function into a new one. As a result we can obtain a large number of highly nonlinear resilient functions from a linear one. Some miscellaneous results on resilient functions, including a discussion on algebraic degree, are included in Section 5, and the paper is closed by some concluding remarks in Section 6.

2 Preliminaries

The vector space of n tuples of elements from $GF(2)$ is denoted by V_n. These vectors, in ascending alphabetical order, are denoted by α_0, α_1, ..., α_{2^n-1}. As vectors in V_n and integers in $[0, 2^n - 1]$ have a natural one-to-one correspondence, it allows us to switch from a vector in V_n to its corresponding integer in $[0, 2^n - 1]$, and vice versa.

Let f be a (Boolean) function from V_n to $GF(2)$ (or simply, a function on V_n). The *sequence* of f is defined as $((-1)^{f(\alpha_0)}$, $(-1)^{f(\alpha_1)}$, ..., $(-1)^{f(\alpha_{2^n-1})})$, while the *truth table* of f is defined as $(f(\alpha_0)$, $f(\alpha_1)$, ..., $f(\alpha_{2^n-1}))$. f is said to be *balanced* if its truth table assumes an equal number of zeros and ones. We call $h(x) = a_1x_1 \oplus \cdots \oplus a_nx_n \oplus c$ an *affine function*, where $x = (x_1, \ldots, x_n)$ and $a_j, c \in GF(2)$. In particular, h will be called a *linear function* if $c = 0$. The sequence of an affine (linear) function will be called an *affine (linear) sequence*.

The algebraic degree $deg(f)$ of a function f is the size of the longest term in the algebraic normal form representation of the function. The *Hamming weight* of a vector v, denoted by $W(v)$, is the number of ones in v. Let f and g be functions on V_n. Then $d(f, g) = \sum_{f(x)\neq g(x)} 1$, where the addition is over the reals, is called the *Hamming distance* between f and g. Let $\varphi_0, \ldots, \varphi_{2^{n+1}-1}$ be the affine functions on V_n. Then $N_f = \min_{i=0,\ldots,2^{n+1}-1} d(f, \varphi_i)$ is called the *nonlinearity* of f. It is well-known that the nonlinearity of f on V_n satisfies $N_f \leqq 2^{n-1} - 2^{\frac{1}{2}n-1}$. An extensive investigation of highly nonlinear balanced functions has been carried out in [17].

Algebraic degree and nonlinearity can also be defined for mappings or tuples of Boolean functions. Let $F = (f_1, \ldots, f_m)$ be a function from V_n to V_m (where each f_i is a function on V_n). The algebraic degree of F, denoted by $deg(F)$, is defined as the minimum among the algebraic degrees of all nonzero linear combinations of the component functions of F, namely,

$$deg(F) = \min_g \{deg(g) | g = \bigoplus_{j=1}^{m} c_j f_j\}.$$

Similarly the nonlinearity of F, denoted by N_F, is defined as

$$N_F = \min_g \{N_g | g = \bigoplus_{j=1}^{m} c_j f_j\}.$$

This definition regarding N_F was first introduced by Nyberg in [13].

$F = (f_1, \ldots, f_m)$ is said to be linear if all its component functions are linear, and to be nonlinear otherwise. If F is linear, then $deg(F) = 1$ and $N_F = 0$. The converse, however, is not always true.

2.1 Properties of Resilient Functions

In this sub-section we summarize a number of facts regarding resilient functions. Though most of these results are either previously known in, for instance, [1, 5, 3], or can be proven easily, they are collected here with the intention to help the reader in understanding our results to be presented in the coming sections. We start with a formal definition of a resilient function.

Definition 1 *Let $F = (f_1, \ldots, f_m)$ be a function from V_n to V_n, where $n \geqq m \geqq 1$, and let $x = (x_1, \ldots, x_n) \in V_n$.*

1. *F is said to be* unbiased *with respect to a fixed subset $T = \{j_1, \ldots, j_t\}$ of $\{1, \ldots, n\}$, if for every $(a_1, \ldots, a_t) \in V_t$*

$$(f_1(x), \ldots, f_m(x))|_{x_{j_1}=a_1,\ldots,x_{j_t}=a_t}$$

runs through all the vectors in V_m each 2^{n-m-t} times while $(x_{i_1}, \ldots, x_{i_{n-t}})$ runs through V_n once, where $t \geqq 0$, $\{i_1, \ldots, i_{n-t}\} = \{1, \ldots, n\} - \{j_1, \ldots, j_t\}$ and $i_1 < \cdots < i_{n-t}$.

2. *F is said to be a (n, m, t)-resilient function if F is unbiased with respect to every $T \subseteq V_n$ with $|T| = t$. The parameter t is called the* resiliency *of the function.*

Obviously, $n - m \geqq t$ holds for each (n, m, t)-resilient function.

Resilient functions are closely related to correlation immune functions introduced by Siegenthaler [20]. As was noticed by Stinson and coworkers, a $(n, 1, t)$-resilient function is the same as a *balanced* tth-order correlation immune Boolean function. We will come back to this issue shortly.

The following lemma is helpful in understanding the relationship between a resilient function and its component functions. It has been called *XOR Lemma* and expressed in terms of independence of random variables in [5, 1]. Here we follow the version described in [19].

Lemma 1 *A function $(f_1, \ldots, f_m)$, where each f_i is a function on V_n and $n \geqq m$, is unbiased, namely, it runs through all the vectors in V_m each 2^{n-m} times while x runs through V_n once, if and only if each nonzero linear combinations of $f_1, \ldots, f_m$ are balanced.*

Hence we have

Lemma 2 *Let $F = (f_1, \ldots, f_m)$ be a function from V_n to V_n, where n and m are integers with $n \geqq m \geqq 1$ and each f_j is a function on V_n. Then F is unbiased with respect to $T = \{j_1, \ldots, j_t\}$, a fixed subset of $\{1, \ldots, n\}$, if and only if every nonzero linear combination of $f_1, \ldots, f_m$, $f(x) = \bigoplus_{j=1}^m c_j f_j(x)$, is unbiased (i.e., balanced) with respect to $T = \{j_1, \ldots, j_t\}$, where $x = (x_1, \ldots, x_n) \in V_n$.*

As an immediate consequence, we have

Theorem 1 *Let $F = (f_1, \ldots, f_m)$ be a function from V_n to V_m, where n and m are integers with $n \geqq m \geqq 1$ and each f_j is a function on V_n. Then F is a (n, m, t)-resilient function if and only if every nonzero linear combination of $f_1, \ldots, f_m$, $f(x) = \bigoplus_{j=1}^m c_j f_j(x)$, is a $(n, 1, t)$-resilient function, where $x = (x_1, \ldots, x_n) \in V_n$.*

It follows from Theorem 1 that if $F = (f_1, \ldots, f_m)$ is a (n, m, t)-resilient function, then $G = (f_1, \ldots, f_s)$ is a (n, s, t)-resilient function for each integer $1 \leqq s \leqq m$.

Theorem 1 shows that each (n, m, t)-resilient function gives $2^m - 1$ distinct balanced tth-order correlation immune functions on V_n. It also indicates that we can study (n, m, t)-resilient functions, including their properties and constructions, through investigating the correlation immune characteristics of their component functions.

To facilitate our investigations, we introduce the following lemma.

Lemma 3 *A function f on V_n is unbiased with respect to $T = \{j_1, \ldots, j_t\}$, a fixed subset of $\{1, \ldots, n\}$, if and only if for each linear function $\varphi(x) = c_{j_1} x_{j_1} \oplus \cdots \oplus c_{j_t} x_{j_t}$ on V_n, where $x = (x_1, \ldots, x_n)$, $f(x) \oplus \varphi(x)$ is balanced.*

Proof. First we consider the simplest case where $T = \{1, \ldots, t\}$. Let $(a_1, \ldots, a_t)$ be an arbitrary but fixed vector in V_t. Then

$$\begin{aligned} &(f(x) \oplus \varphi(x))|_{x_1=a_1,\ldots,x_t=a_t} \\ &= f(a_1, \ldots, a_t, x_{t+1}, \ldots, x_n) \\ &\oplus \varphi(a_1, \ldots, a_t, x_{t+1}, \ldots, x_n). \end{aligned}$$

Now suppose that f is unbiased with respect to $T = \{1, \ldots, t\}$. Then

$$f(a_1, \ldots, a_t, x_{t+1}, \ldots, x_n)$$

is balanced. Note that

$$\varphi(a_1, \ldots, a_t, x_{t+1}, \ldots, x_n)$$

is a constant. Thus

$$(f(x) \oplus \varphi(x))|_{x_1=a_1,\ldots,x_t=a_t}$$

is balanced. As $(a_1, \ldots, a_t)$ is arbitrary, $f(x) \oplus \varphi(x)$ is a balanced function on V_n.

Conversely, suppose that $f(x) \oplus \varphi(x)$ is balanced for an arbitrary $\varphi(x) = c_1 x_1 \oplus \cdots \oplus c_t x_t$.

Let $\xi_{a_1\cdots a_t}$ be the sequence of

$$f(a_1,\ldots,a_t,x_{t+1},\ldots,x_n).$$

By Lemma 1 of [16],

$$\xi = \xi_{0\cdots0},\xi_{0\cdots1},\ldots,\xi_{1\cdots1}$$

is the sequence of $f(x_1,\ldots,x_n)$.

Recall that a $(1,-1)$-matrix H of order m is called a *Hadamard* matrix if $HH^t = mI_m$, where H^t is the transpose of H and I_m is the identity matrix of order m [15]. A Sylvester-Hadamard matrix of order 2^n, denoted by H_n, is generated by the following recursive relation

$$\begin{aligned} &H_0 = 1,\ H_n = \left[\begin{array}{cc} H_{n-1} & H_{n-1} \\ H_{n-1} & -H_{n-1} \end{array}\right], \\ &n = 1,\, 2, \ldots. \end{aligned} \qquad (1)$$

Now let L be the sequence of φ. Then L is a row of H_n. Since $H_n = H_t \times H_{n-t}$, where $\times$ denotes the Kronecker product, we have $L = \ell' \times \ell''$, where ℓ' is a row of H_t and ℓ'' is a row of H_{n-t}. Write $\ell' = (d_0,\ldots,d_{2^t-1})$. Then $L = (d_0\ell'',\ldots,d_{2^t-1}\ell'')$ and hence

$$\begin{aligned} &\langle \xi, L\rangle = d_0\langle \xi_{0\cdots0},\ell''\rangle + d_1\langle \xi_{0\cdots01},\ell''\rangle \\ &+\cdots + d_{2^t-1}\langle \xi_{1\cdots01},\ell''\rangle \end{aligned} \qquad (2)$$

Since $f(x)\oplus\varphi(x)$ is balanced, $\langle \xi, L\rangle = 0$. Note that $\ell' = (d_0,\ldots,d_{2^t-1})$, a row or column of H_t, is also the sequence of $\varphi'(x') = c_1x_1\oplus\cdots\oplus c_tx_t$. A fact with H_t is that the rows (columns) of H_t comprises all the linear sequences (see Lemma 2 of [16]). Then from (2),

$$\begin{aligned} (\langle\xi_{0\cdots0},\ \ \ell''\ \ \rangle, \langle\xi_{0\cdots01},\ell''\rangle, \cdots, \langle\xi_{1\cdots11},\ell''\rangle)H_t \\ = \ \ (0,0,\cdots,0). \end{aligned}$$

As H_t has inverse, we have

$$\langle\xi_{0\cdots0},\ell''\rangle = \langle\xi_{0\cdots01},\ell''\rangle = \cdots = \langle\xi_{1\cdots11},\ell''\rangle = 0.$$

Rewrite $\varphi(x) = \varphi(x')\oplus\varphi(x'')$, where $x'\in V_t$ and $x''\in V_{n-t}$. Now ℓ' is the sequence of φ' while ℓ'' is the sequence of ℓ''. Note that $\varphi'(x') = c_1x_1\oplus\cdots\oplus c_tx_t$. Thus $\varphi'' = 0$ and $\ell'' = (1,\ldots,1)$. As a result, $\langle\xi_{a_1\ldots a_t},\ell''\rangle = 0$, which implies that $\xi_{a_1\ldots a_t}$ is balanced and hence $f(a_1,\ldots,a_t,x_{t+1},\ldots,x_n)$ is balanced, where $(a_1,\ldots,a_t)$ is an arbitrary vector in V_t. This shows that f is unbiased with respect to $T = \{1,\ldots,t\}$.

For the more general case where $T = \{j_1,\ldots,j_t\}$, set

$$f(x_1,\ldots,x_n) = g(x_{j_1},\ldots,x_{j_t},x_{j_{t+1}},\ldots,x_{j_n}),$$

where $\{j_1,\ldots,j_t\} = T$ and

$$\{x_{j_t},x_{j_{t+1}},\ldots,x_{j_n}\} = \{1,\ldots,n\} - T.$$

Also set

$$x_{j_1} = y_1,\ldots,x_{j_n} = y_n. \qquad (3)$$

Thus

$$\begin{aligned} &g(x_{j_1},\ldots,x_{j_t},x_{j_{t+1}},\ldots,x_{j_n}) \\ &= g(y_1,\ldots,y_t,y_{t+1},\ldots,y_n). \end{aligned}$$

Now write $\psi(y) = \psi(y_1,\ldots,y_n) = c_1y_1\oplus\cdots\oplus c_ty_t$, where $y = (y_1,\ldots,y_n)$. Obviously $\psi(y_1,\ldots,y_n) = \varphi(x_1,\ldots,x_n)$. Hence $f(x)\oplus\varphi(x) = g(y)\oplus\psi(y)$. Clearly, f is unbiased with respect to $\{j_1,\ldots,j_t\}$ if and only if g is unbiased with respect to $\{1,\ldots,t\}$, and by the above discussions, if and only if $g(y)\oplus\psi(y) = f(x)\oplus\varphi(x)$ is balanced. □

A corollary of Lemma 3 is

Corollary 1 *f is a $(n,1,t)$-resilient function if and only if for each linear function $\varphi(x) = c_1x_1\oplus\cdots\oplus c_nx_n$ with $W(c_1,\ldots,c_n)\leqq t$, $f(x)\oplus\varphi(x)$ is balanced.*

From this corollary and Theorem 1 it follows

Corollary 2 *F is a (n,m,t)-resilient function if and only if it is a (n,m,s)-resilient function for each $0\leqq s\leqq t$.*

Now we go back to correlation immune functions. Work by Xiao and Massey provides us with an equivalent definition of the concept [10]:

Definition 2 *A function f on V_n is said to be tth-order correlation immune if for each linear function $\varphi(x) = c_1x_1\oplus\cdots\oplus c_nx_n$ with $1\leqq W(c_1,\ldots,c_n)\leqq t$, $f(x)\oplus\varphi(x)$ is balanced.*

As $W(c_1, \ldots, c_n) = 0$ is excluded, the definition covers both balanced and non-balanced correlation immune function, although stream ciphers prefer balanced to non-balanced functions.

Comparing the definition with Corollary 1, it becomes clear that a balanced tth-order correlation immune function is indeed identical to a $(n, 1, t)$-resilient function.

Having presented essential facts on resilient functions, next we consider transformations on the coordinates of a resilient function. Unlike nonlinearity and algebraic degree, the resiliency of functions is not invariant under a nonsingular linear transformation on the coordinates. This can be seen from the following example.

Let $f(x) = x_1 \oplus x_2 \oplus \cdots \oplus x_n$, where $x = (x_1, \ldots, x_n)$. Then f is a $(n, 1, n-1)$-resilient function. Now let B be a matrix of order n over $GF(2)$ satisfying $(x_1, x_2, \ldots, x_{n-1}, x_n)B = (x_2, x_3, \ldots, x_{n-1}, \bigoplus_{j=1}^{n} x_j)$. Set $g(x) = f(xB^{-1})$. Then $g(x) = x_n$ whose resiliency is zero.

Another issue is in relation to the transformation of the component functions, namely output, of a resilient function. This will be discussed in detail in Section 4, where we show an important result regarding invariant properties of resilient functions under transformations of (output) component functions.

2.2 Related Work

The concept of a resilient function was introduced in [5, 1]. The equivalence between linear resilient functions and linear error correcting codes was established also in [5, 1], while the equivalence between resilient functions and large sets of orthogonal arrays was proved in [21]. Two upper bounds on resiliency which are the best known so far were derived in [7, 3]. In [22] Stinson and Massey disproved the conjecture that if there exists a nonlinear resilient function then there exists a linear resilient function with the same parameters. The nonlinear resilient functions they constructed were based on the (nonlinear) Kerdock and Preparata codes [11]. Some linear resilient functions achieving an upper bound on resiliency can be found in [7, 3]. Resilient functions which are symmetric were studied in [5, 8], while non-binary resilient functions were examined in [9].

Soon after the concept of a correlation immune function was introduced by Siegenthaler [20], Xiao and Massey gave an equivalent definition in [10]. These were followed by [4, 18] where various methods for constructing correlation immune functions were presented.

3 Constructing New Resilient Functions from Old

Constructing new resilient functions from old ones is an interesting problem that has many practical implications. There are two opposite directions in relation to this problem, these being constructing "large" ones from "small" ones and "small" ones from "large" ones. Due to the close relationship between resilient functions and error correcting codes, in particular the equivalence between linear codes and linear resilient functions as was revealed in [5, 1], numerous techniques can be borrowed from the theory of error correcting codes to construct new resilient functions from old. These techniques have been further enriched by Stinson's work on the equivalence between resilient functions and large sets of orthogonal arrays [21]. Some concrete examples on constructing new from old can be found in [3].

The main purpose of this section is to present a number of methods for directly synthesizing large resilient functions from small ones. A distinctive feature of these methods is that they are applicable both to linear and to nonlinear resilient functions.

We start with correlation immune functions. Let f_i be a $(n_i, 1, t_i)$-resilient function, $i = 1, 2$. Then $f_1(x) \oplus f_2(y)$ is a $(n_1 + n_2, 1, t_1 + t_2 + 1)$-resilient function, where $x \in V_{n_1}$ and $y \in V_{n_2}$. To show that this is correct, let φ be a linear function on $V_{n_1+n_2}$ defined by

$$\begin{aligned} \varphi(x, y) = c_1 x_1 \oplus \cdots \oplus c_{n_1} x_{n_1} \\ \oplus d_1 y_1 \oplus \cdots \oplus d_{n_2} y_{n_2}, \end{aligned}$$

where $x = (x_1, \ldots, x_{n_1})$, $y = (y_1, \ldots, y_{n_2})$, $c_j, d_i \in GF(2)$. Suppose that

$$W(c_1, \ldots, c_{n_1}, d_1, \ldots, d_{n_2}) \leqq t_1 + t_2 + 1.$$

Then either $W(c_1,\ldots,c_{n_1}) \leqq t_1$ or $W(d_1,\ldots,d_{n_2}) \leqq t_2$. By Corollary 1, either $f_1(x)\oplus\varphi_1(x)$ or $f_2(y)\oplus\varphi_2(y)$ is balanced, where $\varphi_1(x) = c_1x_1\oplus\cdots\oplus c_{n_1}x_{n_1}$ and $\varphi_2(y) = d_1y_1\oplus\cdots\oplus d_{n_2}y_{n_2}$. Note that the sum of two functions with disjoint variables is balanced if one of the two functions is balanced (for a simple proof see Lemma 9 of [16]). Hence $f_1(x)\oplus f_2(y)\oplus\varphi(x,y) = [f_1(x)\oplus\varphi_1(x)]\oplus[f_2(y)\oplus\varphi_2(y)]$ is balanced. Again by Corollary 1, $f_1(x)\oplus f_2(y)$ is a $(n_1+n_2, 1, t_1+t_2+1)$-resilient function.

By induction, we have the following result.

Lemma 4 *Let f_i be a $(n_i,1,t_i)$-resilient function, $i = 1,\ldots,s$. Then $f_1(x)\oplus\cdots\oplus f_s(y)$ is a $(\sum_{j=1}^s n_j, 1, s-1+\sum_{j=1}^s t_j)$-resilient function, where $x\in V_{n_1},\ldots,y\in V_{n_s}$.*

As an application of Lemma 4, we can combine known resilient functions to obtain a new one. First we show that *if $F = (f_1,\ldots,f_m)$ is a (n,m,t)-resilient function, then $G(x,y,z) = (F(x)\oplus F(y), F(y)\oplus F(z))$ is a $(3n,2m,2t+1)$-resilient function, where $x,y,z\in V_n$.*

To prove that G is a $(3n,2m,2t+1)$-resilient function, we first note that $f_1(x)\oplus f_1(y)$, …, $f_m(x)\oplus f_m(y)$, $f_1(y)\oplus f_1(z),\ldots, f_m(y)\oplus f_m(z)$ comprise all the $2m$ component functions of G. Consider a nonzero linear combination of these $2m$ component functions

$$\begin{aligned} f(x,y,z) &= \bigoplus_{j=1}^{m} c_j(f_j(x)\oplus f_j(y)) \\ &\oplus \bigoplus_{j=1}^{m} d_j(f_j(y)\oplus f_j(z)), \end{aligned}$$

where either $(c_1,\ldots,c_m) \neq (0,\ldots,0)$ or $(d_1,\ldots,d_m)\neq(0,\ldots,0)$.

Note that

$$f(x,y,z) = \bigoplus_{j=1}^{m} c_jf_j(x)$$
$$\oplus\bigoplus_{j=1}^{m}(c_j\oplus d_j)f_j(y)\oplus\bigoplus_{j=1}^{m} d_jf_j(z).$$

By Theorem 1, $\bigoplus_{j=1}^m c_jf_j(x)$ is a $(n,1,t)$-resilient function when $(c_1,\ldots,c_m)\neq(0,\ldots,0)$. Similarly, $\bigoplus_{j=1}^m d_jf_j(z)$ is a $(n,1,t)$-resilient function when $(d_1,\ldots,d_m)\neq(0,\ldots,0)$, and $\bigoplus_{j=1}^m(c_j\oplus d_j)f_j(y)$ is a $(n,1,t)$-resilient function when $(c_1\oplus d_1,\ldots,c_m\oplus d_m)\neq(0,\ldots,0)$.

Since either $(c_1,\ldots,c_m)\neq(0,\ldots,0)$ or $(d_1,\ldots,d_m)\neq(0,\ldots,0)$, at least two hold among $(c_1,\ldots,c_m)\neq(0,\ldots,0)$, $(d_1,\ldots,d_m)\neq(0,\ldots,0)$ and $(c_1\oplus d_1,\ldots,c_m\oplus d_m)\neq(0,\ldots,0)$. By Lemma 4, when two hold $f(x,y,z)$ is a $(3n,1,2t+1)$-resilient function, while when three hold it is a $(3n,1,3t+2)$-resilient function. By Theorem 1, $G(x,y,z)$ is indeed a $(3n,2m,2t+1)$-resilient function.

It was first observed in [5] that $g(x_1,\ldots,x_{3h}) = (x_1\oplus\cdots\oplus x_{2h}, x_{h+1}\oplus\cdots\oplus x_{3h})$ is a linear $(3h,2,2h-1)$-resilient function. We can view this function as being obtained from $f(x_1,\ldots,x_h) = x_1\oplus\cdots\oplus x_h$, which is a $(h,1,h-1)$-resilient function, by using the technique described above. Conversely we can also regard our technique as a significant generalization of the idea underling the construction of $g(x_1,\ldots,x_{3h}) = (x_1\oplus\cdots\oplus x_{2h}, x_{h+1}\oplus\cdots\oplus x_{3h})$.

Now applying the same technique to the resulting function G itself, we obtain a $(3^2n, 2^2m, 2^2(1+t)-1)$-resilient function. In general repeating the technique for k times, $k = 1,2,\ldots$, we obtain a $(3^kn, 2^km, 2^k(1+t)-1)$-resilient function from a (n,m,t)-resilient function.

The technique can also be generalized in other directions. In particular, it is easy to prove that if $F = (f_1,\ldots,f_m)$ is a (n,m,t)-resilient function, then $G(x,y,z,u) = (F(x)\oplus F(y), F(y)\oplus F(z), F(z)\oplus F(u))$ is a $(4n,3m,2t+1)$-resilient function, where $x,y,z,u\in V_n$. Again by iterating the technique, we can construct from a (n,m,t)-resilient function a $(4^kn, 3^km, 2^k(1+t)-1)$-resilient function for all $k = 1,2,\ldots$.

To summarize the discussions, we have

Lemma 5 *Given a (n,m,t)-resilient function, there is an iterative method to construct a $((h+1)^kn, h^km, 2^k(1+t)-1)$-resilient function for all $h = 2,3,\ldots$ and $k = 1,2,\ldots$.*

As another application of Lemma 4, we give the following result.

Corollary 3 *Let $F = (f_1,\ldots,f_m)$ be a (n_1,m,t_1)-resilient function and $G = (g_1,\ldots,g_m)$ a*

(n_2, m, t_2)-resilient function. Then $P(z) = F(x) \oplus G(y) = (f_1(x) \oplus g_1(y), \ldots, f_m(x) \oplus g_m(y))$ is a $(n_1 + n_2, m, t_1 + t_2 + 1)$-resilient function, where $z = (x, y)$, $x \in V_{n_1}$ and $y \in V_{n_2}$.

Proof. Consider an arbitrary nonzero linear combination of the component functions of $P(z)$, say

$$\begin{aligned} p(z) &= \bigoplus_{j=1}^{m} c_j[f_j(x) \oplus g_j(y)] \\ &= \bigoplus_{j=1}^{m} c_j f_j(x) \oplus \bigoplus_{j=1}^{m} c_j g_j(y). \end{aligned}$$

By Theorem 1, $\bigoplus_{j=1}^{m} c_j f_j(x)$ is a t_1-resilient function, while $\bigoplus_{j=1}^{m} c_j g_j(y)$ is a t_2-resilient function. Hence by Lemma 4, $p(z)$ is a $t_1 + t_2 + 1$-resilient function. As $p(z)$ is arbitrary, again by Theorem 1, $P(z)$ is a $(n_1 + n_2, m, t_1 + t_2 + 1)$-resilient function. □

A special case of the technique indicated in Corollary 3, namely when both F and G are linear, has been employed by Bierbrauer, Gopalakrishnan and Stinson in proving their Theorem 7 in [3].

The following result is concerned with placing resilient functions in parallel.

Corollary 4 *Let $F = (f_1, \ldots, f_{m_1})$ be a (n_1, m_1, t_1)-resilient function and $G = (g_1, \ldots, g_{m_2})$ be a (n_2, m_2, t_2)-resilient function. Then*

$$P(z) = (f_1(x), \ldots, f_{m_1}(x), g_1(y), \ldots, g_{m_2}(y))$$

is a $(n_1 + n_2, m_1 + m_2, \rho)$-resilient function, where $z = (x, y)$, $x \in V_{n_1}$, $y \in V_{n_2}$, and $\rho = \min\{t_1, t_2\}$.

Proof. Consider an arbitrary nonzero linear combination of the component functions of $P(z)$

$$p(z) = \bigoplus_{j=1}^{m_1} c_j f_j(x) \oplus \bigoplus_{j=1}^{m_2} d_j g_j(y).$$

As $(c_1, \ldots, c_{m_1}, d_1, \ldots, d_{m_2})$ is a nonzero vector, without loss of generality, we can assume that $(c_1, \ldots, c_{m_1}) \neq (0, \ldots, 0)$. For any λ_1-subset $\{j_1, \ldots, j_{\lambda_1}\} \subseteq \{1, \ldots, n_1\}$ and any λ_2-subset $\{i_1, \ldots, i_{\lambda_2}\} \subseteq \{1, \ldots, n_2\}$, where $\lambda_1 + \lambda_2 = \rho$, and any $a_1, \ldots, a_{\lambda_1}$, $b_1, \ldots, b_{\lambda_2} \in GF(2)$, by Theorem 1, and the fact that the sum of two functions with disjoint variables is balanced if one of the two functions is balanced (Lemma 9 of [16]), $\bigoplus_{j=1}^{m_1} c_j f_j(x)|_{x_{j_1}=a_1,\ldots,x_{j_{\lambda_1}}=a_{\lambda_1}}$ is balanced. Thus

$$\begin{aligned} &\bigoplus_{j=1}^{m_1} c_j f_j(x)|_{x_{j_1}=a_1,\ldots,x_{j_{\lambda_1}}=a_{\lambda_1}} \\ &\oplus \bigoplus_{j=1}^{m_2} d_j g_j(y)|_{y_{i_1}=b_1,\ldots,b_{i_{\lambda_2}}=b_{\lambda_2}} \end{aligned}$$

is balanced. It follows from Theorem 1 that

$$P(z) = (f_1(x), \ldots, f_{m_1}(x), g_1(y), \ldots, g_{m_2}(y))$$

is a $(n_1 + n_2, m_1 + m_2, \rho)$-resilient function. □

4 Transforming Linear Resilient Functions to Nonlinear Ones

Recall that a resilient function is said to be *linear* if its component functions are all linear, and said to be *nonlinear* otherwise. When the concept of resilient functions was introduced, it was conjectured that if there exists a *nonlinear* resilient function with certain parameters, then there exists a *linear* resilient function with the same parameters [5, 1]. This conjecture was disproved by Stinson and Massey [22]. In particular, they showed that there exists an infinite class of nonlinear resilient functions for which there do not exist linear resilient functions with the same parameters. They used nonlinear error correcting codes in their proof. In this section we investigate this topic in a slightly different direction. In particular we show that by permuting the output m-tuples (i.e., all 2^m vectors in V_m), instead of only re-ordering the m component functions of a (n, m, t)-resilient function, we can obtain $2^m!$ distinct (n, m, t)-resilient functions. A consequence of this result is that the *converse* of the conjecture in [5, 1] is true, namely if there exists a *linear* resilient function with certain parameters, then there exists a *nonlinear* resilient function with the same parameters.

Here is the main result in this section.

Theorem 2 *Let F be a (n,m,t)-resilient function and G be a permutation on V_m. Then $P = G \circ F$, namely $P(x) = G(F(x))$, is also a (n,m,t)-resilient function.*

Proof. Since F is a (n,m,t)-resilient function, for each $\{j_1,\dots,j_t\} \subseteq \{1,\dots,n\}$ and $a_1,\dots,a_t \in GF(2)$,

$$F(x)|_{x_{j_1}=a_1,\dots,x_{j_t}=a_t}$$

runs through all the vectors in V_m each 2^{n-m-t} times while $(x_{i_1},\dots,x_{i_{n-t}})$ runs through V_n once, where $\{i_1,\dots,i_{n-t}\} = \{1,\dots,n\} - \{j_1,\dots,j_t\}$ and $i_1 < \cdots < i_{n-t}$. As G is a permutation on V_m,

$$\begin{aligned}&P(x)|_{x_{j_1}=a_1,\dots,x_{j_t}=a_t}\\ &= G(F(x))|_{x_{j_1}=a_1,\dots,x_{j_t}=a_t}\end{aligned}$$

runs through all the vectors in V_m each 2^{n-m-t} times while $(x_{i_1},\dots,x_{i_{n-t}})$ runs through V_n once. It immediately follows that P is a (n,m,t)-resilient function. □

Note that the total number of different permutations on V_m is $2^m!$ which is far larger than $m!$. The latter is the number of ways to re-order the m component functions. New resilient functions generated using these permutations are all different. To prove this, let G_1 and G_2 be two different permutations on V_m. We want to prove that $G_1 \circ F \neq G_2 \circ F$. Suppose for contradiction that $G_1 \circ F = G_2 \circ F$. Then $F = G_1^{-1} \circ G_2 \circ F$. As F is unbiased, for each $\beta \in V_m$, there exist 2^{n-m} different vectors $\alpha \in V_n$ such that $F(\alpha) = \beta$. This causes $\beta = G_1^{-1} \circ G_2(\beta)$. As β is arbitrary, $G_1^{-1} \circ G_2$ must be the identity permutation on V_m, which contradicts the fact that $G_1 \neq G_2$. Thus we have proved the following:

Corollary 5 *Given a (n,m,t)-resilient function, Theorem 2 produces $2^m!$ distinct (n,m,t)-resilient function.*

Now we describe an example to show applications of Theorem 2. It is easy to verify that

$$\begin{aligned}&F(x_1,x_2,x_3,x_4,x_5,x_6)\\ &= (x_1 \oplus x_2 \oplus x_3,\ \ x_3 \oplus x_4 \oplus x_5,\\ &x_5 \oplus x_6 \oplus x_1)\end{aligned}$$

is a linear $(6,3,2)$-resilient function. Consider a permutation G on V_3 defined by

$$\begin{aligned}&G(u_1,u_2,u_3)\\ &= (u_1 \oplus u_3 \oplus u_2u_3,\ \ u_1 \oplus u_2 \oplus u_1u_3,\\ &u_2 \oplus u_3 \oplus u_1u_2).\end{aligned}$$

By Theorem 2, $P = G \circ F$ is also a $(6,3,2)$-resilient function.

Note that all component functions of the resulting resilient function P are quadratic. The rest of this section is devoted to this direction, namely converting linear resilient functions to nonlinear ones. We also show how to calculate the nonlinearity of a resulting nonlinear resilient function. The following lemma will be used in the discussions.

Lemma 6 *Let g be a function on V_m whose nonlinearity is N_g. Let $n \geqq m$ and B be an $n \times m$ matrix over $GF(2)$ whose rank is m. Set $h(x_1,\dots,x_n) = g((x_1,\dots,x_n)B)$. Then the nonlinearity N_h of h, a function on V_n, satisfies $N_h = 2^{n-m}N_g$, and the algebraic degree of h is the same as that of g.*

Proof. First we note that this lemma is a generalization of the following result: *Let $h(x_1,\dots,x_n) = g(x_1,\dots,x_k)$. Then h, a function on V_n, satisfies $N_h = 2^{n-m}N_g$.* A proof for this special case can be found in, for instance, [18].

To prove this lemma, we append to B an $n \times (n-m)$ matrix C so that $A = [B, C]$ is a nonsingular matrix of order n over $GF(2)$. Set $(u_1,\dots,u_n) = (x_1,\dots,x_n)A$. Now define a function on V_n, say g^*, as follows

$$g^*(u_1,\dots,u_n) = g(u_1,\dots,u_m).$$

Then $N_{g^*} = 2^{n-m}N_g$, and g^* and g share the same algebraic degree. On the other hand, from the construction of h,

$$\begin{aligned}&h(x_1,\dots,x_n) = g((x_1,\dots,x_n)B)\\ &= g^*((x_1,\dots,x_n)A).\end{aligned}$$

By noting the fact that the nonlinearity and algebraic degree of a function are invariant under a nonsingular linear transformation on coordinates, we have $N_h = N_{g^*} = 2^{n-m}N_g$, and that h has the same algebraic degree as that of g^*, which is the same as that of g. □

Now we prove a significant result on constructing new resilient functions from old, linear ones.

Theorem 3 *Let F be a linear (n,m,t)-resilient function and G be a permutation on V_m whose nonlinearity is N_G. Then $P = G \circ F$ is a (n,m,t)-resilient function and*

(i) the nonlinearity N_P of P satisfies $N_P = 2^{n-m}N_G$,

(ii) the algebraic degree of P is the same as that of G.

Proof. As F is a linear resilient function, it can be written as $F(x_1,\dots,x_n) = (x_1,\dots,x_n)B$ where B is an $n \times m$ matrix of rank m over $GF(2)$ and $(x_1,\dots,x_n) \in V_n$. The theorem follows immediately from Lemma 6. □

We turn our attention back to the nonlinear $(6,3,2)$-resilient function constructed above. It is easy to verify that the nonlinearity of each nonzero linear combination of the component functions of G is 2. By Theorem 3, the nonlinearity of P is 16, and as we have seen, the algebraic degree of P is indeed 2.

Theorem 3 implies that highly nonlinear resilient functions can be constructed from linear resilient functions by applying highly nonlinear permutations in the transforming process. A number of highly nonlinear permutations which are based on polynomials on a finite field have been shown in [14, 2]. In particular, it is shown in [14] that the nonlinearity of a permutation G based on the inverse function on $GF(2^m)$ satisfies $N_G \geqq 2^{m-1} - 2^{\frac{1}{2}m}$ and the algebraic degree of G is $m-1$. Hence the following is proved:

Corollary 6 *If there exists a linear (n,m,t)-resilient function, then there exists a nonlinear (n,m,t)-resilient function P whose nonlinearity satisfies $N_P \geqq 2^{n-1} - 2^{n-\frac{1}{2}m}$ and whose algebraic degree is $m-1$.*

Another important implication of Theorem 3 is that from each linear resilient function, we can derive a large number nonlinear resilient functions with the same parameters. This, together with the result by Stinson and Massey [22], shows that it is more affluent in nonlinear resilient functions than in linear resilient functions, in terms of either the numbers or the parameters.

5 Remarks on Algebraic Degree

In his pioneering work [20], Siegenthaler showed, by a lengthy argument, that the algebraic degree of a balanced correlation immune function, i.e., a $(n,1,t)$-resilient function, is at most $n-t-1$, except for the case when $t = n-1$. Here we show that the proof can substantially shortened by employing Theorem 1 on Page 372 of [11].

Let f be a $(n,1,t)$-resilient function. As f is a function on V_n, by Theorem 1 on Page 372 of [11], it can be expressed in the algebraic normal form, namely

$$\begin{aligned} & f(x_1,\dots,x_n) \\ &= \bigoplus_{a_1,\dots,a_n \in GF(2)} g(a_1,\dots,a_n)x_1^{a_1}\cdots x_n^{a_n}, \end{aligned}$$

where

$$\begin{aligned} & g(a_1,\dots,a_n) \\ &= \bigoplus_{(b_1,\dots,b_n)\subset(a_1,\dots,a_n)} f(b_1,\dots,b_n), \end{aligned}$$

and by $(b_1,\dots,b_n) \subset (a_1,\dots,a_n)$ we mean that if $b_j = 1$ then $a_j = 1$.

Consider the coefficient of the term $x_1 \cdots x_{n-t}$, that is

$$\bigoplus_{b_1,\dots,b_{n-t} \in GF(2)} f(b_1,\dots,b_{n-t},0,\dots,0). \tag{4}$$

Since f is a $(n,1,t)$-resilient function, (4) becomes zero, except for $n-t = 1$ in which case (4) becomes one. By the same reasoning, we can see that the coefficient of every term of algebraic degree $n-t$ is zero. This proves that the algebraic degree of f is at most $n-t-1$.

By noting our Theorem 1, we have

Corollary 7 *The algebraic degree of a (n,m,t)-resilient function is at most $n-t-1$, except for the case when $t = n-1$.*

Recall that it is easy to construct linear $(n, n-1, 1)$-resilient functions from linear error correcting codes. Using Corollaries 5 and 6, we obtain $2^{n-1}!$ distinct $(n, n-1, 1)$-resilient functions, a large number of which have a nonlinearity of at least $2^{n-1} - 2^{\frac{n+1}{2}}$ and whose algebraic degree is $n-2$.

It should be noted, however, that due to Corollary 7, applying Theorem 3 to a *nonlinear* $(n, n-1, 1)$-resilient function does not always yield a function that has a higher algebraic degree.

In [7] Friedman proved that the resiliency t of a (n, m, t)-resilient function is bounded from above by

$$B_1 = \lfloor \frac{2^{m-1}n}{2^m - 1} \rfloor - 1.$$

Theorem 3 of [3] gives another upper bound

$$B_2 = 2\lfloor \frac{2^{m-2}(n+1)}{2^m - 1} \rfloor - 1. \qquad (5)$$

As shown in [3] a linear $(2^m - 1, m, 2^{m-1} - 1)$-resilient function can be obtained from a simplex code. This function achieves the upper bound on resiliency (5). Applying Corollaries 5 and 6 to this resilient function, we obtain $2^m!$ distinct $(2^m - 1, m, 2^{m-1} - 1)$ resilient functions, some of which have a nonlinearity of at least $2^{2^m - 2} - 2^{2^m - 1 - \frac{1}{2}m}$ and whose algebraic degree is $m-1$. All the resulting functions achieve the upper bound on resiliency indicated in (5).

6 Conclusion

Main results of this paper are related to the construction of nonlinear resilient functions. Of particular importance to practical applications is the method for transforming linear resilient functions into nonlinear ones. Currently we are in the process of extending in various directions the results reported in this paper.

Acknowledgment

We would like thank G. Stinson for kindly providing us with his papers. This project was supported in part by the Australian Research Council (ARC) under the reference number A49232172 and by the Australian Telecommunications and Electronics Research Board (ATERB) under the reference numbers C010/058 and N069/412.

This work was done while the second author was with the University of Wollongong.

References

[1] Bennett, C. H., Brassard, G., and Robert, J. M. Privacy amplification by public discussion. *SIAM J. Computing 17* (1988), 210–229.

[2] Beth, T., and Ding, C. On permutations against differential cryptanalysis. In *Advances in Cryptology - EUROCRYPT'93* (1994), vol. 765, Lecture Notes in Computer Science, Springer-Verlag, Berlin, Heidelberg, New York, pp. 65–76.

[3] Bierbrauer, J., Gopalakrishnan, K., and Stinson, D. R. Bounds on resilient functions and orthogonal arrays. In *Advances in Cryptology - CRYPTO'94* (1994), vol. 839, Lecture Notes in Computer Science, Springer-Verlag, Berlin, Heidelberg, New York, pp. 247–256.

[4] Camion, P., Carlet, C., Charpin, P., and Sendrier, N. On correlation-immune functions. In *Advances in Cryptology - CRYPTO'91* (1991), vol. 576, Lecture Notes in Computer Science, Springer-Verlag, Berlin, Heidelberg, New York, pp. 87–100.

[5] Chor, B., Goldreich, O., Håstad, J., Friedman, J., Rudich, S., and Smolensky, R. The bit extraction problem or t-resilient functions. *IEEE Symposium on Foundations of Computer Science 26* (1985), 396–407.

[6] Ding, C., Xiao, G., and Shan, W. *The Stability Theory of Stream Ciphers*, vol. 561 of *Lecture Notes in Computer Science*. Springer-Verlag, Berlin, Heidelberg, New York, 1991.

[7] Friedman, J. On the bit extraction problem. *Proc. 33rd IEEE Symp. on Foundations of Computer Science* (1992), 314–319.

[8] Gopalakrishnan, K., Hoffman, D. G., and Stinson, D. R. A note on a conjecture concerning symmetric resilient functions. *Information Processing Letters 47* (1993), 139–143.

[9] Gopalakrishnan, K., and Stinson, D. R. Three characterizations of non-binary correlation-immune and resilient functions. *Designs, Codes and Cryptography 5* (1995), 241–251.

[10] Guo-Zhen, X., and Massey, J. L. A spectral characterization of correlation-immune combining functions. *IEEE Transactions on Information Theory 34*, 3 (1988), 569–571.

[11] MacWilliams, F. J., and Sloane, N. J. A. *The Theory of Error-Correcting Codes.* North-Holland, Amsterdam, New York, Oxford, 1978.

[12] Matsui, M. Linear cryptanalysis method for DES cipher. In *Advances in Cryptology - EUROCRYPT'93* (1994), vol. 765, Lecture Notes in Computer Science, Springer-Verlag, Berlin, Heidelberg, New York, pp. 386–397.

[13] Nyberg, K. On the construction of highly nonlinear permutations. In *Advances in Cryptology - EUROCRYPT'92* (1993), vol. 658, Lecture Notes in Computer Science, Springer-Verlag, Berlin, Heidelberg, New York, pp. 92–98.

[14] Nyberg, K. Differentially uniform mappings for cryptography. In *Advances in Cryptology - EUROCRYPT'93* (1994), vol. 765, Lecture Notes in Computer Science, Springer-Verlag, Berlin, Heidelberg, New York, pp. 55–65.

[15] Seberry, J., and Yamada, M. Hadamard matrices, sequences, and block designs. In *Contemporary Design Theory: A Collection of Surveys*, J. H. Dinitz and D. R. Stinson, Eds. John Wiley & Sons, Inc, 1992, ch. 11, pp. 431–559.

[16] Seberry, J., Zhang, X. M., and Zheng, Y. Highly nonlinear 0-1 balanced functions satisfying strict avalanche criterion. In *Advances in Cryptology - AUSCRYPT'92* (1993), vol. 718, Lecture Notes in Computer Science, Springer-Verlag, Berlin, Heidelberg, New York, pp. 145–155.

[17] Seberry, J., Zhang, X. M., and Zheng, Y. Nonlinearly balanced boolean functions and their propagation characteristics. In *Advances in Cryptology - CRYPTO'93* (1994), vol. 773, Lecture Notes in Computer Science, Springer-Verlag, Berlin, Heidelberg, New York, pp. 49–60.

[18] Seberry, J., Zhang, X. M., and Zheng, Y. On constructions and nonlinearity of correlation immune functions. In *Advances in Cryptology - EUROCRYPT'93* (1994), vol. 765, Lecture Notes in Computer Science, Springer-Verlag, Berlin, Heidelberg, New York, pp. 181–199.

[19] Seberry, J., Zhang, X. M., and Zheng, Y. Relationships among nonlinearity criteria. In *Advances in Cryptology - EUROCRYPT'94* (1995), vol. 950, Lecture Notes in Computer Science, Springer-Verlag, Berlin, Heidelberg, New York, pp. 376–388.

[20] Siegenthaler, T. Correlation-immunity of nonlinear combining functions for cryptographic applications. *IEEE Transactions on Information Theory IT-30 No. 5* (1984), 776–779.

[21] Stinson, D. R. Resilient functions and large sets of orthogonal arrays. *Congressus Numerantium 92* (1993), 105–110.

[22] Stinson, D. R., and Massey, J. L. An infinite class of counterexamples to a conjecture concerning non-linear resilient functions. *Journal of Cryptology 8*, 3 (1995), 167–173.