Journal of Universal Computer Science, vol. 3, no. 6 (1997), 721-729
submitted: 9/12/96, accepted: 9/4/97, appeared: 28/6/97 © Springer Pub. Co.

Highly Nonlinear t-Resilient Functions

Kaoru Kurosawa
(Tokyo Institute of Technology, Japan
kurosawa@ss.titech.ac.jp)

Takashi Satoh
(Tokyo Institute of Technology, Japan
tsato@ss.titech.ac.jp)

Kentaro Yamamoto
(Tokyo Institute of Technology, Japan)

Abstract: High resilient and high nonlinear Boolean functions are desirable for secure key generators in stream ciphers, for example. This paper first shows that there exists a tradeoff between resiliency and nonlinearity. Then we show a new simple design method for high resilient and high nonlinear Boolean functions. Our method gives higher nonlinearity than [Zhang and Zheng 95] while their method gives larger resiliency than our method. Further, the proposed method provides a tradeoff between resiliency t and nonlinearity N_F by using an intermediate parameter l. If we choose a large l, then a small t and a large N_F are obtained. If we choose a small l, then a large t and a small N_F are obtained.
Key Words: cryptology, Boolean function, nonlinearity, resiliency
Category: E.3

1 Introduction

An n-input and m-output function $F(x_1, \ldots, x_n) = (f_1, \ldots, f_m)$ is called an (n, m, t)-resilient function if any function obtained from F by keeping any t input bits constant is uniformly distributed [Bennett et al. 88, Chor et al. 85, Stinson 93]. Resilient functions play important roles in cryptography such as key renewal [Bennett et al. 88, Chor et al. 85] and the design of running-key generators in stream ciphers against correlation attacks [Siegenthaler 84, Rueppel 86].

A common method for constructing key stream generators is to combine a set of linear shift registers with a nonlinear function. Some key stream generator can be broken by ciphertext-only correlation attacks on individual subsequences. The immunity against such attacks is quantified by the smallest number $t+1$ of subsequences that must be simultaneously considered in a correlation attack. [Siegenthaler 84] introduced a new class of combining functions called tth-order correlation functions, which provides immunity against such an attack. An (n, m, t)-resilient function is a balanced tth-order correlation-immune function.

On the other hand, linear approximation of Boolean functions is very useful in cryptanalysis on stream ciphers and block ciphers. Ding, Xiao and Shan [Ding, Xiao, Shan 91] showed the best affine approximation (BAA) attack on key stream generators with a low nonlinear correlation-immune function. This cryptanalysis shows that nonlinearity is also a crucial criterion for cryptographically strong combining functions. (Matsui showed the linear cryptanalysis on DES [Matsui 94] after BAA attack appeared.)

Therefore, it is a need to investigate highly nonlinear and high resilient functions. Recently, [Zhang and Zheng 95] showed how to transform linear (n, m, t)-resilient functions into nonlinear ones with the same parameters.

This paper first shows that there exists a tradeoff between resiliency and nonlinearity. Then we propose another simple approach for designing (n, m, t)-resilient functions with high nonlinearity. For the same n and m, our method gives higher nonlinearity than [Zhang and Zheng 95] while their method gives larger resiliency than our method. Further, the proposed method provides a tradeoff between resiliency t and nonlinearity N_F by using an intermediate parameter l.

2 Preliminaries

2.1 Balance

Let $x = (x_1, \ldots, x_n)$. Let f be a function: $\{0,1\}^n \to \{0,1\}$. Then $f(x)$ is balanced if

$$|\{x \mid f(x) = 0\}| = |\{x \mid f(x) = 1\}| = 2^{n-1} \ .$$

Let F be a function: $\{0,1\}^n \to \{0,1\}^m$. Then $F(x)$ is uniformly distributed if

$$|\{x \mid F(x) = \beta\}| = 2^{n-m}$$

for any $\beta \in \{0,1\}^m$.

Proposition 1. *[Lidl et al. 83] $F(x) = (f_1(x), \ldots, f_m(x))$ is uniformly distributed if and only if all nonzero linear combinations of $f_1, \ldots, f_m$ are balanced.*

2.2 Nonlinearity and Bent functions

For two functions $f(x)$ and $g(x)$, define

$$d(f, g) \stackrel{\triangle}{=} |\{x \mid f(x) \neq g(x)\}| \ .$$

Definition 2. [Pieprzyk et al. 88] The nonlinearity of f, denoted by N_f, is defined as

$$N_f \stackrel{\triangle}{=} \min_{(a_0,\ldots,a_n)\in\{0,1\}^{n+1}} d(f(x), a_0 \oplus a_1x_1 \oplus \cdots \oplus a_nx_n) \ .$$

$a_0 \oplus a_1x_1 \oplus \cdots \oplus a_nx_n$ is called an affine function. N_f denotes a distance between $f(x)$ and the set of affine functions.

Proposition 3. *[Meier and Staffelbach 90] $N_f \leq 2^{n-1} - 2^{n/2-1}$.*

For $f(x)$, define its Walsh transform as

$$\mathcal{F}(\omega_1, \ldots, \omega_n) \stackrel{\triangle}{=} \sum_x (-1)^{f(x)}(-1)^{\omega_1x_1+\cdots+\omega_nx_n} \ .$$

Proposition 4. *[Meier and Staffelbach 90]*

$$N_f = 2^{n-1} - \frac{1}{2} \max_{(\omega_1,\ldots,\omega_n)} |\mathcal{F}(\omega_1,\ldots,\omega_n)| \ .$$

Definition 5. [Rothaus 76] $f(x)$ is a bent function if

$$|\mathcal{F}(\omega_1,\ldots,\omega_n)| = 2^{n/2} \tag{1}$$

for any $(\omega_1,\ldots,\omega_n)$.

Corollary 6. *The equality of Proposition 3 is satisfied if and only if f is a bent function.*

Definition 7. [Nyberg 93] The nonlinearity of $F(x) = (f_1(x),\ldots,f_m(x))$, denoted by N_F, is defined as the minimum among the nonlinearities of all nonzero linear combinations of the component functions of F:

$$N_F \stackrel{\triangle}{=} \min_g \{N_g \mid g = \bigoplus_{j=1}^{m} c_j f_j, c_j \in \{0,1\}, (c_1,\ldots,c_m) \neq (0,\ldots,0)\}$$

Definition 8. $F(x_1,\ldots,x_n) = (f_1,\ldots,f_m)$ is an (n,m)-bent function if all nonzero linear combinations of $f_1,\ldots,f_m$ are bent functions.

Proposition 9. *[Nyberg 91] There exists an (n,m)-bent function if and only if $n \geq 2m$ and $n =$even.*

2.3 Resilient function

Definition 10. $F(x_1,\ldots,x_n) = (f_1,\ldots,f_m)$ is an (n,m,t)-resilient function if any function obtained from F by keeping any t input bits constant is uniformly distributed.

From Proposition 1, we obtain the following corollary.

Corollary 11. *$F(x_1,\ldots,x_n) = (f_1,\ldots,f_m)$ is an (n,m,t)-resilient function if and only if all nonzero linear combinations of $f_1,\ldots,f_m$ are $(n,1,t)$-resilient functions.*

Proposition 12. *[Xiao and Massey 88] $f(x)$ is an $(n,1,t)$-resilient function if and only if its Walsh transform satisfies*

$$\mathcal{F}(\omega) = 0 \quad \textit{for } 0 \leq W(\omega) \leq t \ ,$$

where $W(\omega)$ denotes the Hamming weight of $\omega = (\omega_1,\ldots,\omega_n)$.

3 Tradeoff between resiliency and nonlinearity

In this section, we show that there exists a tradeoff between resiliency and nonlinearity.

Theorem 13. *In an $(n,1,t)$-resilient function f,*

$$N_f \le 2^{n-1} - \frac{1}{2}\frac{2^n}{\sqrt{2^n - \sum_{k=0}^{t}\binom{n}{k}}} \quad .$$

Proof. Suppose that $f(x)$ is an $(n,1,t)$-resilient function. From Parseval's theorem,

$$\sum_{\omega} F(\omega)^2 = 2^n \sum_{x}((-1)^{f(x)})^2 = 2^{2n}.$$

From Proposition 12

$$\sum_{\omega \text{ s.t. } W(\omega)>t} F(\omega)^2 = 2^{2n}.$$

Then from Proposition 4

$$N_f = 2^{n-1} - \frac{1}{2}\max_{\omega}|F(\omega)| \le 2^{n-1} - \frac{1}{2}\frac{2^n}{\sqrt{2^n - \sum_{k=0}^{t}\binom{n}{k}}} \quad .$$

□

From Theorem 13, we see that if t is large, then N_f must be small. This shows a trade-off between resiliency and nonlinearity. The above theorem is generalized to $m \ge 2$ easily.

Corollary 14. *In an (n,m,t)-resilient function F,*

$$N_F \le 2^{n-1} - \frac{1}{2}\frac{2^n}{\sqrt{2^n - \sum_{k=0}^{t}\binom{n}{k}}}.$$

Proof. For any nonzero vector $(c_1,\ldots,c_m)$, let

$$g \triangleq \bigoplus_{j=1}^{m} c_j f_j \quad .$$

Then

$$N_g \le 2^{n-1} - \frac{1}{2}\frac{2^n}{\sqrt{2^n - \sum_{k=0}^{t}\binom{n}{k}}}$$

from Theorem 13. Now from Definition 7, we obtain this corollary. □

Again, we see a tradeoff between t and N_F.

4 Highly Nonlinear t-Resilient Functions

Let φ be a function: $\{0,1\}^k \to \{0,1\}$ and ψ be a function: $\{0,1\}^l \to \{0,1\}$. Let $x = (x_1, \ldots, x_k)$ and $y = (y_1, \ldots, y_l)$. Define

$$f(x,y) \stackrel{\triangle}{=} \varphi(x) \oplus \psi(y) \ .$$

Proposition 15. *[Seberry et al. 94] The nonlinearity of $f(x,y)$ satisfies*

$$N_f \geq N_\varphi 2^l + N_\psi 2^k - 2N_\varphi N_\psi \ .$$

Corollary 16. *Suppose that $\psi(y)$ is not an affine function. Then the nonlinearity of $f(x,y)$ satisfies*

$$N_f > 2^l N_\varphi \ .$$

Proof. From Proposition 3,

$$2^k - 2N_\varphi \geq 2^{k/2} > 0 \ .$$

Since $\psi(y)$ is not an affine function,

$$N_\psi > 0 \ .$$

Therefore, from Proposition 15,

$$N_f \geq N_\varphi 2^l + N_\psi(2^k - 2N_\varphi) > 2^l N_\varphi \ .$$

□

Lemma 17. *If $\varphi(x)$ is a $(k,1,t)$-resilient function, then $f(x,y)$ is a $(k+l,1,t)$-resilient function.*

Proof. Fix t-bits among $(x_1, \ldots, x_n, y_1, \ldots, y_l)$ arbitrarily. For simplicity, suppose that the fixed bits are

$$x_1 = b_1, \ldots, x_h = b_h, y_1 = b_{h+1}, \ldots, y_{t-h} = b_t.$$

First,

$$\varphi(b_1, \ldots, b_h, x_{h+1}, \ldots, x_k)$$

is balanced because $\varphi(x)$ is t-resilient and $h \leq t$. Therefore, for any fixed values $c_1, \ldots, c_{l-t+h}$,

$$\varphi(b_1, \ldots, b_h, x_{h+1}, \ldots, x_k) \oplus \psi(b_{h+1}, \ldots, b_t, c_1, \ldots, c_{l-t+h})$$

is balanced. Hence,

$$\varphi(b_1, \ldots, b_h, x_{h+1}, \ldots, x_k) \oplus \psi(b_{h+1}, \ldots, b_t, y_{t+1}, \ldots, y_l)$$

is balanced. This means that $\varphi(x) \oplus \psi(y)$ is t-resilient. □

Theorem 18. *For any even l such that $l \geq 2m$, if there exists an $(n-l,m,t)$-resilient function $\Phi(x)$, then there exists an (n,m,t)-resilient function $F(x,y)$ whose nonlinearity satisfies $N_F > 2^{n-1} - 2^{n-l/2-1}$.*

Proof. Let the $(n-l, m, t)$-resilient function be

$$\Phi(x) = \{\varphi_1(x), \ldots, \varphi_m(x)\} \ .$$

On the other hand, from Proposition 9, there exists a (l, m)-bent function

$$\Psi(y) = \{\psi_1(y), \ldots, \psi_m(y)\}$$

for our (l, m). Define

$$F(x, y) \stackrel{\triangle}{=} \{\varphi_1(x) \oplus \psi_1(y), \ldots, \varphi_m(x) \oplus \psi_m(y)\} \ .$$

Now for any $(c_1, \ldots, c_m) \neq (0, \ldots, 0)$, let

$$\begin{aligned} f(x, y) &\stackrel{\triangle}{=} c_1(\varphi_1(x) \oplus \psi_1(y)) \oplus \cdots \oplus c_m(\varphi_m(x) \oplus \psi_m(y)) \\ &= (c_1\varphi_1(x) \oplus \cdots \oplus c_m\varphi_m(x)) \oplus (c_1\psi_1(x) \oplus \cdots \oplus c_m\psi_m(x)) \ . \end{aligned}$$

From Corollary 11,

$$c_1\varphi_1(x) \oplus \cdots \oplus c_m\varphi_m(x)$$

is t-resilient. From Definition 8,

$$c_1\psi_1(x) \oplus \cdots \oplus c_m\psi_m(x)$$

is a bent function. Then from Lemma 17 and Corollary 16, $f(x, y)$ is t-resilient and

$$N_f > 2^{n-l}(2^{l-1} - 2^{l/2-1}).$$

Therefore, $F(x, y)$ is an (n, m, t)-resilient function and $N_F > 2^{n-1} - 2^{n-l/2-1}$. □

In Theorem 18, we can choose even l arbitrarily in $2m \leq l \leq n - m$. If l is large, then we obtain small t and large N_F. If l is small, then we obtain large t and small N_F.

5 Comparison

Zhang and Zheng showed how to transform linear resilient functions into nonlinear resilient functions [Zhang and Zheng 95].

Proposition 19. *Let F be a linear (n, m, t)-resilient function and G be a permutation on $\{0, 1\}^m$ whose nonlinearity is N_G. Then $\hat{F} = G \circ F$ is an (n, m, t)-resilient function whose nonlinearity satisfies $N_{\hat{F}} = 2^{n-m} N_G$.*

This section shows that for the same n and m,

- Theorem 18 gives higher nonlinearity than Proposition 19.
- Proposition 19 gives larger resiliency than Theorem 18.

Suppose that we obtain an (n, m, t)-resilient function F with nonlinearity N_F from Theorem 18 and an $(n, m, \hat{t})$-resilient function $\hat{F}$ with nonlinearity $N_{\hat{F}}$ from Proposition 19.

5.1 On resiliency

Theorem 18 requires the existence of an $(n-l, m, t)$-resilient function such that $l \geq 2m$. Proposition 19 requires the existence of a linear $(n, m, \hat{t})$-resilient function. Therefore, if we ignore "linear", then $\hat{t} \geq t$.

5.2 On nonlinearity

In Proposition 19,

$$N_G \leq 2^{m-1} - 2^{m/2-1} \quad .$$

from Proposition 3 and Definition 7. Therefore,

$$N_{\hat{F}} \leq 2^{n-1} - 2^{n-m/2-1} \quad . \tag{2}$$

On the other hand, from Theorem 18,

$$N_F > 2^{n-1} - 2^{n-l/2-1} \geq 2^{n-1} - 2^{n-m-1}$$

since $l \geq 2m$. Hence,

$$N_{\hat{F}} \leq 2^{n-1} - 2^{n-m/2-1} < 2^{n-1} - 2^{n-m-1} < N_F \quad .$$

6 Examples

6.1 Comparison with Zhang and Zheng

It is known that there exists a linear (n, m, t)-resilient function if and only if there exists a linear $[n, m, t+1]$-code. Suppose that we want a $(36, 8, t)$ resilient function with high nonlinearity N_F.

Proposed method

From [Verhoeff 87], there exists a linear $[18, 8, 6]$-code. So there exists a linear $(18, 8, 5)$-resilient function. In Theorem 18, let $l = 18$. Then we obtain a linear $(36, 8, 5)$-resilient function with nonlinearity

$$N_F > 2^{35} - 2^{26} \quad .$$

Zhang and Zheng method

On the other hand, there exists a linear $[36, 8, 16]$-code from [Brouwer]. So there exists a linear $(36, 8, 15)$-resilient function. Then from Proposition 19 and eq.(2), we obtain a linear $(36, 8, 15)$-resilient function with nonlinearity

$$N_{\hat{F}} \geq 2^{35} - 2^{31} \quad .$$

We summarize the above results in [Tab. 1]. From this table, we see that our method gives higher nonlinearity N_F than Zhang and Zheng method while Zhang and Zheng method gives larger resiliency t than our method.

	Proposed	Zhang and Zheng
t	5	15
N_F	$> 2^{35} - 2^{26}$	$\leq 2^{35} - 2^{31}$

Table 1: *Comparison of Theorem 18 and Proposition 19 on* $(36, 8, t)$*-resilient functions*

t	7	5	4	3	2	1	0
N_F	$2^{35} - 2^{27}$	$2^{35} - 2^{26}$	$2^{35} - 2^{25}$	$2^{35} - 2^{24}$	$2^{35} - 2^{23}$	$2^{35} - 2^{22}$	$2^{35} - 2^{21}$
l	16	18	20	22	24	26	28

Table 2: *Tradeoff between t and lower bounds of N_F on* $(36, 8, t)$*-resilient functions*

6.2 Tradeoff

The proposed method provides a tradeoff between resiliency t and nonlinearity N_F by using an intermediate parameter l. In Theorem 18, if l is large, then we obtain small t and large N_F. If l is small, then we obtain large t and small N_F. This tradeoff is illustrated in [Tab. 2] for $n = 36$ and $m = 8$.

References

[Bennett et al. 88] Bennett, B. I., Brassard, G. and Robert, J. M.: "Privacy amplification by public discussion"; SIAM Journal on Computing, 17 (1988) 210-229.

[Brouwer] Brouwer, A. E.: "Bounds on the minimum distance of binary linear codes"; `http://www.win.tue.nl/win/math/dw/voorlincod.html`.

[Chor et al. 85] Chor, B., Goldreich, O., Håstad, J., Friedman, J., Rudich, S. and Smolensky, R.: "The bit extraction problem or t-resilient functions"; Proc. of the 26th IEEE Symposium on Foundations of Computer Science (1985) 396-407.

[Ding, Xiao, Shan 91] Ding, C., Xiao, G. and Shan, W.: "The stability theory of stream ciphers"; Lecture Notes in Computer Science 561, Springer-Verlag, 1991.

[Lidl et al. 83] Lidl, S., Niederreiter, H.: "Finite Fields"; Encyclopedia of Mathematics and Its Applications 20, Corollary 7.39. Cambridge University Press, 1983.

[Matsui 94] Matsui, M.: Linear cryptanalysis method for DES cipher; Advances in Cryptology - EUROCRYPT '93 Proceedings, Lecture Notes in Computer Science 765, Springer-Verlag (1994), 386-397.

[Meier and Staffelbach 90] Meier, W. and Staffelbach, O.: "Nonlinearity criteria for cryptographic functions"; Advances in Cryptology - EUROCRYPT '89 Proceedings, Lecture Notes in Computer Science 434, Springer-Verlag, (1990) 549-562.

[Nyberg 91] Nyberg, K.: "Perfect nonlinear S-boxes"; Advances in Cryptology - EUROCRYPT '91 Proceedings, Lecture Notes in Computer Science 547, Springer-Verlag (1991), 378-386.

[Nyberg 93] Nyberg, K.: "On the construction of highly nonlinear permutations"; Advances in Cryptology - EUROCRYPT '92 Proceedings, Lecture Notes in Computer Science 658, Springer-Verlag (1993), 92-98.

[Pieprzyk et al. 88] Pieprzyk, J. and Finkelstein, G.: "Towards effective nonlinear cryptosystem design"; IEE Proceedings Part E, 35, 6 (1988), 325-335.

[Rothaus 76] Rothaus, O. S.: "On bent functions"; Journal of Combinatorial Theory (A), 20 (1976) 300-305.

[Rueppel 86] Rueppel, R. A.: "Analysis and design of stream ciphers"; Springer-Verlag (1986).

[Seberry et al. 94] Seberry, J., Zhang, X. M. and Zheng, Y.: "On constructions and nonlinearity of correlation immune functions"; Advances in Cryptology - EUROCRYPT '93 Proceedings, Lecture Notes in Computer Science 765, Springer-Verlag (1994), 181-199.

[Siegenthaler 84] Siegenthaler, T.: "Correlation-immunity of nonlinear combining functions for cryptographic applications"; IEEE Trans. Inform. Theory, IT-30, 5 (1984), 776-780.

[Stinson 93] Stinson, D. R.: "Resilient functions and large sets of orthogonal arrays"; Congressus Numerantium, 92 (1993), 105-110.

[Verhoeff 87] Verhoeff, T.: "An updated table of minimum-distance bounds for binary linear codes"; IEEE Trans. Inform. Theory, IT-33, 5 (1987), 665-680.

[Xiao and Massey 88] Xiao, G. and Massey J.L.: "A spectral characterization of correlation-immune combining function"; IEEE Trans. Inform. Theory, IT-34, 3 (1988), 569-571.

[Zhang and Zheng 95] Zhang, X. M. and Zheng, Y.: "On nonlinear resilient functions"; Advances in Cryptology - EUROCRYPT '95 Proceedings, Lecture Notes in Computer Science 921, Springer-Verlag (1995), 274-288.