Non-Separable Cryptographic Functions

Yuliang Zheng[†] and Xian-Mo Zhang[‡]

[†]School of Network Computing
Monash University
Melbourne, VIC 3199, Australia
Email: yuliang.zheng@infotech.monash.edu.au

[‡] School of Info. Tech. & Comp. Sci.
University of Wollongong
Wollongong, NSW 2522, Australia
Email: xianmo@cs.uow.edu.au

Abstract

We study nonlinear Boolean functions that are used in cryptography, especially in block and stream ciphers. We point out possible cryptographic weaknesses of the so-called *separable functions*. A characteristic of these functions is that they can be transformed into ones that are composed of two "sub-functions" with *disjoint variables*. We then proceed to construct *non-separable functions* that exhibit additional useful cryptographic properties such as balance, high nonlinearity, correlation immunity, and good propagation characteristics.

1. Introduction

A functions on V_n is a mapping from V_n to $GF(2)$ where V_n is the vector space of n tuples of elements from $GF(2)$. We write a function f on V_n as $f(x)$, where $x = (x_1, \ldots, x_n)$ is the variable vector in V_n. The *truth table* of a function f on V_n is a $(0,1)$-sequence defined by $(f(\alpha_0),\ f(\alpha_1), \ldots, f(\alpha_{2^n-1}))$, and the *sequence* of f is a $(1,-1)$-sequence defined by $((-1)^{f(\alpha_0)}, (-1)^{f(\alpha_1)}, \ldots, (-1)^{f(\alpha_{2^n-1})})$.

f is said to be *balanced* if its truth table contains an equal number of ones and zeros. We point out that balance is one of the most basic requirements of Boolean functions used in cryptography.

An *affine* function f on V_n is a function that takes the form of $f(x_1, \ldots, x_n) = a_1x_1 \oplus \cdots \oplus a_nx_n \oplus c$, where $a_j, c \in GF(2)$, $j = 1, 2, \ldots, n$. Furthermore f is called a *linear* function if $c = 0$.

The *Hamming weight* of a $(0,1)$ sequence, denoted by $HW(\xi)$, is the number of ones in the sequence. Given two functions f and g on V_n, the *Hamming distance* $d(f,g)$ between them is defined as the Hamming weight of the truth table of $f(x) \oplus g(x)$.

The *nonlinearity* of a function f on V_n, denoted by N_f, is the minimal Hamming distance between f and all affine functions on V_n, i.e., $N_f = \min_{i=0,1,\ldots,2^{n+1}-1} d(f, \varphi_i)$, where $\varphi_0,\ \varphi_1,\ \ldots,\ \varphi_{2^{n+1}-1}$ are all the affine functions on V_n. N_f is upper bounded by $2^{n-1} - 2^{\frac{1}{2}n-1}$. We note that nonlinearity is an important cryptographic criterion, and a high nonlinearity is a prerequisite to resist linear cryptanalytic attacks.

We say that f satisfies the *propagation criterion with respect to* α if $f(x) \oplus f(x \oplus \alpha)$ is a balanced function. Furthermore f is said to satisfy the *propagation criterion of degree* k if it satisfies the propagation criterion with respect to every non-zero vector α whose Hamming weight is not larger than k (see [6]). The *strict avalanche criterion (SAC)* [9] is identical to the propagation criterion of degree one. As yet another important nonlinearity criterion, good propagation characteristics are used to resist differential cryptanalytic attacks.

The concept of correlation immune functions was introduced by Siegenthaler [8]. Xiao and Massey gave an equivalent definition [4]: a function f on V_n is called a *kth-order correlation immune function* if it satisfies the condition of $\sum_{x \in V_n} f(x)(-1)^{\langle \beta, x \rangle} = 0$ for all $\beta \in V_n$ with $1 \leq HW(\beta) \leq k$, where in the the sum, $f(x)$ and $\langle \beta, x \rangle$ are regarded as real-valued functions. Correlation immune functions are used in the design of running-key generators in stream ciphers that resist against correlation attacks. Let ξ denote the sequence of f. Then from Section 4.2 of [2], a function on V_n is kth-order correlation immune function if and only if $\langle \xi, \ell \rangle = 0$ for every ℓ, the sequence of a linear function $\varphi(x) = \langle \alpha, x \rangle$ on V_n constrained by $1 \leq HW(\alpha) \leq k$.

A vector α in V_n is called a *linear structure* of a function f on V_n if $f(x) \oplus f(x \oplus \alpha)$ is a constant. It is easy to verify that the set of all linear structures of a function f form a linear subspace of V_n, whose dimension is called the *linearity of* f. We note that non-zero linear structures are considered cryptographically undesirable.

2. Separable and Non-Separable Functions

Definition 1 *A function* f *on* V_n *is said to be* separable *if there exist an $n \times n$ nonsingular matrix B over $GF(2)$ and an integer p with $1 \leq p \leq n-1$ such that $f(xB) = g(y) \oplus h(z)$ where $x = (y, z)$, $y \in V_p$, $z \in V_{n-p}$, g is a function on V_p and h is a function on V_{n-p}. Otherwise the function is said to be non-separable.*

In particular, if g or h is an affine function, then f, undesirably, must have non-zero linear structures. One also notices that for $n > 2$, all quadratic functions on V_n are separable.

Write $y = (y_1, \ldots, y_p)$ and $z = (z_{p+1}, \ldots, z_n)$. We can see that with a separable function f, y_i and z_j, where $1 \leq i \leq p$ and $p+1 \leq j \leq n$, do not appear in the same term in the algebraic normal form of the function $f(xB)$. The function f is regarded cryptographically weak, in light of the following observation which indicates that the function remains constant with respect to "double" difference. The "double" difference is closely related to differential attacks on block ciphers discovered by Biham and Shamir [1].

Theorem 1 *A function f on V_n is separable if and only if there exists an integer p with $1 \leq p \leq n-1$, a p-dimensional linear subspace W of V_n and a complementary subspace U in V_n such that for every non-zero vector $\alpha \in W$ and every non-zero vector $\alpha' \in U$, we have $f(x) \oplus f(x \oplus \alpha) \oplus f(x \oplus \alpha') \oplus f(x \oplus \alpha \oplus \alpha') = 0$.*

From these discussions, it becomes obvious that a non-separable function will never have a non-zero linear structure. We further observe that the separability of a function is invariant under any nonsingular linear transformation on the variables.

Consider a function f on V_n whose algebraic degree is n. As the algebraic degree of a function is invariant under a nonsingular linear transformation on the variables, from Definition 1, we can see that f is non-separable. Next we consider the case where f has an algebraic degree of smaller than n. Set $g(x_1, \ldots, x_n) = f(x_1, \ldots, x_n) \oplus x_1 \cdots x_n$. Then resultant new function g is a degree n function. Following the discussions above, g is non-separable. Note that

$$g(\alpha) = \begin{cases} f(\alpha) & \text{if } \alpha \neq (1, \ldots, 1) \\ 1 \oplus f(\alpha) & \text{if } \alpha = (1, \ldots, 1) \end{cases}$$

Thus we have $d(g, f) = 1$. Let ψ be an affine function on V_n. Then we have $d(g, \psi) + d(g, f) \geq d(f, \psi)$. Hence $d(g, \psi) + d(g, f) \geq N_f$. Since ψ is arbitrary, we have shown that $N_g \geq N_f - 1$.

While the above discussions show that constructing highly nonlinear non-separable functions from an existing highly nonlinear, not necessarily non-separable, function is easy, we encounter a problem with the balance of the resultant function g. Since g is a function on V_n whose algebraic degree is n, we have the term $x_1 \cdots x_n$ appearing in the algebraic normal form of g. Thus $\bigoplus_{\alpha \in V_n} g(\alpha) = 1$ (see p. 372 of [5]). This means that g is unbalanced, which renders the function useless in many cryptographic applications. Furthermore we should point out that a very high algebraic degree may contradict other cryptographic requirements, such as correlation immunity. These considerations motivate us to investigate methods for systematically constructing non-separable functions that satisfy various other cryptographic requirements such as balance, high nonlinearity, good propagation characteristics and high correlation immunity. This problem is addressed in the next section.

3. Constructing Non-Separable Functions

First we give a sufficient condition for non-separable functions.

Theorem 2 *Let f be a function on V_n, and W be a p-dimensional linear subspace of V_n, where $p > \frac{n}{2}$. If for every two non-zero vectors $\alpha \in W$ and $\alpha' \notin W$, we have $f(x) \oplus f(x \oplus \alpha) \oplus f(x \oplus \alpha') \oplus f(x \oplus \alpha \oplus \alpha') \neq 0$, then f is non-separable.*

Proof. We prove the theorem by contradiction. For the sake of convenience, we write $\lambda_{\alpha,\alpha'}(x) = f(x) \oplus f(x \oplus \alpha) \oplus f(x \oplus \alpha') \oplus f(x \oplus \alpha \oplus \alpha')$. Assume for contradiction that f satisfying the property in the theorem is separable. From Theorem 1, there exist a q-dimensional linear subspace W^* of V^n, where $1 \leq q \leq n-1$, and a complementary subspace U^* of W^* in V_n, such that for every non-zero vector $\beta^* \in W^*$ and every non-zero vector $\gamma^* \in U^*$, we have $\lambda_{\beta^*,\gamma^*}(x) = 0$. Since W^* and U^* are complementary to each other, the dimension of U^* is $n - q$. Note that either $q \geq \frac{1}{2}n$ or $n - q \geq \frac{1}{2}n$. Without loss of generality, we assume that $q \geq \frac{n}{2}$. Since W and W^* have different properties, we have $W^* \neq W$. Hence there exists a vector β^{**} such that $\beta^{**} \in W^*$ but $\beta^{**} \notin W$. Furthermore, there must exist a non-zero vector $\beta^{***} \in W \cap W^*$. Two cases should be considered: $U^* \not\subseteq W$ and $U^* \subseteq W$.

With the case of $U^* \not\subseteq W$, there exists a non-zero vector $\gamma^{**} \in U^*$ but $\gamma^{**} \notin W$. From the property of W, we have $\lambda_{\beta^{***},\gamma^{**}}(x) \neq 0$. But, from the property of W^*, we should have $\lambda_{\beta^{***},\gamma^{**}}(x) = 0$ instead. Thus we have a contradiction.

With the case of $U^* \subseteq W$, there must exist a non-zero vector $\alpha^{**} \in U^* \subseteq W$. Similarly to the previous case, we also a contradiction, namely $\lambda_{\alpha^{**},\beta^{**}}(x) \neq 0$ according to W, but $\lambda_{\alpha^{**},\beta^{**}}(x) = 0$ according to W^*. Hence we have proved that f is indeed non-separable.

The following result will be useful in constructing non-separable functions.

Theorem 3 *Let g and h be two functions on V_{n-1} satisfying*

(i) g has no non-zero linear structures,

(ii) for any $\beta, \beta' \in V_{n-1}$, if $g(x) \oplus g(x \oplus \beta) \oplus g(x \oplus \beta') \oplus g(x \oplus \beta \oplus \beta') = 0$, then $h(x) \oplus h(x \oplus \beta) \oplus h(x \oplus \beta') \oplus h(x \oplus \beta \oplus \beta') = c$, where c is a constant.

Then $f(x) = x_1 g(y) \oplus h(y)$, where $x = (x_1, \ldots, x_n)$ and $y = (x_2, \ldots, x_n)$, is a non-separable function on V_n.

Proof. Let $W = \{(0, a_2, \ldots, a_n) | (0, a_2, \ldots, a_n) \in V_n\}$. Note that W is an $(n-1)$-dimensional subspace of V_n For any non-zero $\alpha \in W$ and any $\alpha' \notin W$, we can write $\alpha = (0, \beta)$ and $\alpha' = (1, \beta')$, where $\beta, \beta' \in V_{n-1}$ and $\beta \neq 0$. We now show that with W thus defined, f satisfies the condition in Theorem 2. We notice that $f(x) \oplus f(x \oplus \alpha) \oplus f(x \oplus \alpha') \oplus f(x \oplus \alpha' \oplus \alpha) = x_1(g(y) \oplus g(y \oplus \beta) \oplus g(y \oplus \beta') \oplus g(y \oplus \beta' \oplus \beta)) \oplus g(y \oplus \beta') \oplus g(y \oplus \beta' \oplus \beta) \oplus h(y) \oplus h(y \oplus \beta) \oplus h(y \oplus \beta') \oplus h(y \oplus \beta' \oplus \beta)$.

There exist two cases to be considered: $g(y) \oplus g(y \oplus \beta) \oplus g(y \oplus \beta') \oplus g(y \oplus \beta' \oplus \beta) \neq 0$ and $g(y) \oplus g(y \oplus \beta) \oplus g(y \oplus \beta') \oplus g(y \oplus \beta' \oplus \beta) = 0$.

In the first case, it is obvious that $f(x) \oplus f(x \oplus \alpha) \oplus f(x \oplus \alpha') \oplus f(x \oplus \alpha' \oplus \alpha) \neq 0$.

In the other case, considering the second condition in the theorem, we have $h(y) \oplus h(y \oplus \beta) \oplus h(y \oplus \beta') \oplus h(y \oplus \beta' \oplus \beta) = c$, where c is constant. Hence $f(x) \oplus f(x \oplus \alpha) \oplus f(x \oplus \alpha') \oplus f(x \oplus \alpha' \oplus \alpha) = g(y \oplus \beta') \oplus g(y \oplus \beta' \oplus \beta) \oplus c$. Since g has no non-zero linear structures and $\beta \neq 0$, $g(y \oplus \beta') \oplus g(y \oplus \beta \oplus \beta')$ cannot be a constant. This proves that $f(x) \oplus f(x \oplus \alpha) \oplus f(x \oplus \alpha') \oplus f(x \oplus \alpha' \oplus \alpha) \neq 0$. Noticing that the dimension of W is $n - 1 > \frac{1}{2}n$, we have proved that f does satisfy the condition in Theorem 2. This proves the theorem.

Next we introduce an auxiliary tool to be used in the description of methods for constructing non-separable functions.

Lemma 1 *Let $\chi(\mathbf{x}) = \mathbf{x}^p \oplus a_{p-1}\mathbf{x}^{p-1} \oplus \cdots \oplus a_1\mathbf{x} \oplus a_0$ be a primitive polynomial of degree p over $GF(2)$. From χ, we define a $p \times p$ matrix Γ over $GF(2)$ as follows:*

$$\Gamma = \begin{bmatrix} 0 & 0 & 0 & \cdots & 0 & a_0 \\ 1 & 0 & 0 & \cdots & 0 & a_1 \\ 0 & 1 & 0 & \cdots & 0 & a_2 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & a_{p-1} \end{bmatrix}$$

Then we have

(i) $\Gamma^{2^p-1} = I$, where I denotes the $p \times p$ identity matrix, and $\Gamma^k \neq I$, for all k with $0 \leq k \leq 2^p - 2$,

(ii) each Γ^k is a non-zero linear combination of $\Gamma^0, \Gamma^1, \ldots, \Gamma^{p-1}$, where $\Gamma^0 = I$, and each non-zero linear combination of $\Gamma^0, \Gamma^1, \ldots, \Gamma^{p-1}$ is identified with a Γ^k, $0 \leq k \leq 2^p - 2$.

Let τ_0 be an arbitrary non-zero vector in V_p. Define vector τ_k as $\tau_k = \tau_0 \tau^k$, $k = 0, 1, 2 \ldots$ The following theorem demonstrates how to construct highly nonlinear, balanced, non-separable functions that also exhibit a good propagation characteristic.

Theorem 4 *Let p and s be integers with $0 < s < p$, and P be a mapping from V_s to V_p defined by $P(\delta) = \tau_k$, where $\delta \in V_s$ is the binary representation of an integer k, $k = 0, 1, \ldots, 2^s - 1$. Define a function f on V_{s+p} as follows: $f(x) = f(y, z) = P(y)z^T$, where $x = (y, z)$, $y \in V_s$ and $z \in V_p$. Then f satisfies the following properties:*

(i) f is non-separable,

(ii) f is balanced,

(iii) the nonlinearity of f satisfies $N_f = 2^{s+p-1} - 2^{p-1}$,

(iv) there exists an $n \times n$ nonsingular matrix B over $GF(2)$ such that $g(x) = f(xB)$ satisfies the SAC.

Proof. First we define a subspace W of V_{s+p} by $W = \{(0, \ldots, 0, b_1, \ldots, b_p) | (0, \ldots, 0, b_1, \ldots, b_p) \in V_{s+p}\}$, where each $b_j \in GF(2)$. Let $\alpha \in W$ and $\alpha' \notin W$ be two non-zero vectors. Write $\alpha = (0, \gamma)$ and $\alpha' = (\beta', \gamma')$, where 0 denotes the zero vector in V_s, $\gamma, \gamma' \in V_p$, $\beta' \in V_s$, $\gamma \neq 0$ and $\beta' \neq 0$. We notice that $f(x) \oplus f(x \oplus \alpha) \oplus f(x \oplus \alpha') \oplus f(x \oplus \alpha' \oplus \alpha) = (P(y) \oplus P(y \oplus \beta'))\gamma^T$. Since $\beta' \neq 0$, from Lemma 1, we have $P(y) \neq P(y \oplus \beta')$, as well as the fact that $P(y) \oplus P(y \oplus \beta')$ is nonsingular. As $\gamma \neq 0$, we conclude that $f(x) \oplus f(x \oplus \alpha) \oplus f(x \oplus \alpha') \oplus f(x \oplus \alpha' \oplus \alpha) = (P(y) \oplus P(y \oplus \beta'))\gamma^T \neq 0$. Considering the dimension p of W satisfying $p > \frac{1}{2}(s+p)$, and Theorem 2, we have proved (i).

For a fixed $\delta \in V_s$, since $P(\delta) \neq 0$, $f(\delta, z) = P(\delta)z^T$ is a non-zero linear function on V_p and hence it is balanced. We have now proved (ii).

(iii) follows from Theorem 5 of [3].

Finally, let $\alpha = (\beta, \gamma)$ where $\beta \in V_s$, $\gamma \in V_p$ and $\beta \neq 0$. Notice that $f(x) \oplus f(x \oplus \alpha) = P(y)z^T \oplus P(y \oplus \beta)(z \oplus \gamma)^T = (P(y) \oplus P(y \oplus \beta))z^T \oplus P(y \oplus \beta)\gamma^T$. For each fixed $\delta \in V_s$, since $P(\delta) \oplus P(\delta \oplus \beta) \neq 0$, $(P(\delta) \oplus P(\delta \oplus \beta))z^T$ is a non-zero linear function on V_p, and hence it is balanced. This shows that $f(x) \oplus f(x \oplus \alpha)$ is balanced when

$\alpha = (\beta, \gamma)$ satisfies $\beta \in V_s$, $\gamma \in V_p$ and $\beta \neq 0$. Note that there exist $2^{s+p} - 2^p$ such vectors as $\alpha = (\beta, \gamma)$ satisfying $\beta \in V_s$, $\gamma \in V_p$ and $\beta \neq 0$. This implies that there are at least $2^{s+p} - 2^p$ non-zero vectors α such that $f(x) \oplus f(x \oplus \alpha)$ is balanced. Since $2^{s+p} - 2^p > 2^{s+p-1}$, by using Theorem 7 of [7], we have proved (iv).

Next we present a method for constructing non-separable functions that are highly nonlinear, balanced and correlation immune.

Theorem 5 *Let p, s and r be integers with $0 < s, r < p$. Set $\mu(p, r) = \binom{p}{1} + \binom{p}{2} + \cdots + \binom{p}{r}$. If $2^{p-s} > 1 + \mu(p, r)$, then we can find an integer k_0 with $0 < k_0 < 2^p - 2^s$, that allows us to define a mapping Q from V_s to V_p such that $Q(\delta) = \tau_{k+k_0}$, where $\delta \in V_s$ and δ is the binary representation of an integer k, $k = 0, 1, \ldots, 2^s - 1$. Based on Q, we can then construct a function $f(x) = f(y, z) = Q(y)z^T$ on V_{s+p}, where $x = (y, z)$, $y \in V_s$ and $z \in V_p$, such that f has the following useful properties:*

(i) f is non-separable,

(ii) f is balanced,

(iii) the nonlinearity of f satisfies $N_f = 2^{s+p-1} - 2^{p-1}$, and

(iv) f is an rth-order correlation immune function.

Proof. Set $\Omega = \{\gamma | \gamma \in V_p,\ 0 < HW(\gamma) \leq r\}$. Thus $\#\Omega = \mu(p, r)$, where $\#X$ denotes the number of elements in a set X. Since $2^{p-s} > 1 + \mu(p, r)$, one can verify that there exists an integer k_0 with $0 < k_0 < 2^p - 2^s$, satisfying

$$\{\tau_{k_0}, \tau_{k_0+1}, \ldots, \tau_{k_0+2^s-1}\} \cap \Omega = \emptyset \qquad (1)$$

where $\emptyset$ denotes the empty set. Define a mapping Q from V_s to V_p as $Q(\delta) = \tau_{k+k_0}$, where $\delta \in V_s$ and δ is the binary representation of an integer k, $k = 0, 1, \ldots, 2^s - 1$, and construct a function $f(x) = f(y, z) = Q(y)z^T$ on V_{s+p}, where $x = (y, z)$, $y \in V_s$ and $z \in V_p$.

Let L be the sequence of a linear function ψ on V_{s+p}, defined by $\psi(x) = \langle \alpha, x \rangle$ where $\alpha = (\beta, \gamma)$ and $x = (y, z)$, $y, \beta \in V_s$ and $z, \gamma \in V_p$. Hence $\psi(x) = \langle \beta, y \rangle \oplus \langle \gamma, z \rangle$, from which we have $\langle \xi, L \rangle = \sum_{y \in V_s, z \in V_p} (-1)^{Q(y)z^T \oplus \langle \beta, y \rangle \oplus \langle \gamma, z \rangle} = \sum_{y \in V_s} (-1)^{\langle \beta, y \rangle} \sum_{z \in V_p} (-1)^{(Q(y) \oplus \gamma) z^T}$.
Note that if $Q^{-1}(\gamma)$ does not exist, then we have $\sum_{z \in V_p} (-1)^{(Q(y) \oplus \gamma) z^T} = 0$ and hence $\langle \xi, L \rangle = 0$. We now consider L with $HW(\alpha) \leq r$. Obviously we have $HW(\gamma) \leq r$. Due to (1), $Q^{-1}(\gamma)$ does not exist. So we must have $\langle \xi, L \rangle = 0$. This proves (iv).

Detailed proofs for Lemma 1 and Theorems 1, together with some other results, will appear in the full version of the paper.

Acknowledgments

The second author was supported by a Queen Elizabeth II Fellowship (227 231002).

References

[1] E. Biham and A. Shamir, differential cryptanalysis of DES-like cryptosystems, *Journal of Cryptology*, 4(3):3-72, 1991.

[2] P. Camion, C. Carlet, P. Charpin and N. Sendrier, On Correlation-immune functions, In *Advances in Cryptology - CRYPTO'91*, Vol.576, LNCS, pp.87-100, Springer-Verlag, 1991.

[3] Seongtaek Chee and Sangjin Lee and Daiki Lee and Soo Hak Sung, On the Correlation Immune Functions and Their Nonlinearity, Advances in Cryptology - ASIACRYPT'96, Vol.1163, LNCS, pp.232-243, Springer-Verlag,

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

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

[6] B. Preneel and W. V. Leekwijck, L. V. Linden, R. Govaerts and J. Vandewalle, Propagation Characteristics of Boolean Functions, In *Advances in Cryptology - EUROCRYPT'90*, Vol.437, LNCS, pp.155-165, Springer-Verlag, 1991.

[7] J. Seberry, X. M. Zhang and Y. Zheng, Improving the Strict Avalanche Characteristics of Cryptographic Functions, *Information Processing Letters*, Vol.50, pp.37-41, 1994.

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

[9] A. F. Webster and S. E. Tavares, On the Design of S-Boxes, *Advances in Cryptology - CRYPTO'85*, Vol.219, LNCS, pp.523-534, Springer-Verlag, 1986.