DEPARTAMENTO DE CIÊNCIA DA COMPUTAÇÃO

Relatório Técnico

RT-MAC-9708

An Augmented Family of Cryptographic Parity Circuits

Kenji Koyama
Routo Terada

setembro 97

An Augmented Family of Cryptographic Parity Circuits [1]

Kenji Koyama and Routo Terada
NTT C.S. Labs. Dept. of Computer Science
Kyoto, Japan Univ. of S. Paulo, Brazil
(rt@ime.usp.br)

ABSTRACT

A computationally inexpensive involution called *value-dependent swapping* is introduced. This involution is included in the non-linear cryptographic family of functions called Parity Circuits to increase its non-affineness and thus increase its strength against cryptanalysis. Our analysis shows that this augmented version of Parity Circuits still have fundamental cryptographic properties. The addition of this involution introduces a new type of randomization while preserving the invertibility of the functions being defined. We formulate affineness for a general function, and introduce a normalized non-affineness measure. We prove some non-affineness conditions for the augmented Parity Circuits, and evaluate their non-affineness. We suggest the value-dependent swapping can also be incorporated into DES-like cryptographic functions as well to make them stronger against cryptanalysis. □

1. Introduction

We introduce a random involution called *value-dependent swapping*, *VDS*. In the *VDS*, the left half and the right half of a sequence of bits are swapped if its weight is odd. *VDS* is included in the cryptographic family of functions called Parity Circuits $C(n,d)$ [KT90] to obtain an augmented version called $C_+(n,d)$, where n is the the plaintext input length, and d is the depth of the circuit. Cryptographic properties of $C_+(n,d)$ are analyzed. In particular, we prove that $C_+(n,d)$ for $n \geq 4$ is *not* affine. We also show the degree of the non-affineness of $C_+(n,d)$ increases as n or d increases.

This work is in response to a very recent short note by Youssef and Tavares [YT97] in which they show our original Parity Circuits [KT90] are affine and hence insecure.

In Section 2, we introduce *VDS*, and in Sections 3 and 4, we summarize the Parity Circuits $C(n,d)$ and define the augmented circuits $C_+(n,d)$. In Section 5, the swapping properties for $C_+(n,d)$ are clarified. In Section 6.1, we formulate affineness for a general function, and introduce a normalized non-affineness measure. In Section 6.2, we prove non-affineness conditions for $C_+(n,d)$. In Section 6.3, we evaluate the non-affineness measure for the circuits $C_+(n,d)$ when n or d increases. In Section 7 and 8, other cryptographic properties are briefly described.

2. Value-dependent swapping

[1] This work was presented to the 1997 Information Security Workshop (Japan Advanced Institute of Science and Technology, Kanazawa, September 17-19, 1997, Japan)

We propose a random involution called value-dependent swapping (VDS). A function called *value-dependent swapping* is generally defined as follows.

Definition 1 Let $x = L \parallel R$ be a sequence of $2k$ ($k > 0$) bits, where L stands for left half of x, and R stands for right, $length(L) = length(R) = k$. A *value-dependent swapping*, or $V(x)$, is defined to be

$$V(x) = \begin{cases} R \parallel L & \text{if } h(x) = 0, \\ L \parallel R & \text{if } h(x) = 1, \end{cases}$$

where $h(x) \in \{0,\ 1\}$. □

Notice that $V(x)$ is an involution: $V(V(x)) = x$ if $h(L \parallel R) = h(R \parallel L)$.
Among various candidates for $h(x)$ satisfying $h(L \parallel R) = h(R \parallel L)$, we can define a particular involutional value-dependent swapping called VDS.

Definition 2 (VDS) Let $x = L \parallel R$ be a sequence of $2k$ ($k > 0$) bits, where $length(L) = length(R) = k$. A VDS, which is an involutional *value-dependent swapping* based on the parity of the weight of x, is defined to be

$$V(x) = V(L \parallel R) = \begin{cases} R \parallel L & \textit{if } weight(x) \textit{ is odd}, \\ L \parallel R & \textit{otherwise}, \end{cases}$$

where $weight(x)$ is the number of 1's in the bit-sequence x. □

Notice that if $L = R$, then $weight(x)$ is even and no swapping occurs.

From now on in this paper, we will assume that n is even, unless otherwise noticed.

3. Summary of Parity Circuits C(n,d)

We summarize in this section the basic concepts defined in [KT90] which will be used later.

Definition 3 A *parity circuit layer with length* n, or simply an $L(n)$ circuit layer, is a Boolean device with an n-bit input and an n-bit output, characterized by a *key* that is a sequence of n symbols from $\{0, 1, +, -\}$. □

The symbols 0 and 1 are called *testers*, the symbol $+$ is called *even inverter*, and $-$ is called *odd inverter*.

Definition 4 A function $B = f(K, A)$ computed by an $L(n)$ circuit layer with key $K = k_1 k_2 \cdots k_n \in \{0, 1, +, -\}^n$ is the relation from an n-bit input sequence $A = a_1\ a_2\ \cdots\ a_n \in \{0,1\}^n$ to an n-bit output sequence $B = b_1 b_2 \cdots b_n \in \{0,1\}^n$ defined below. An $L(n)$ circuit layer computes first the variable T modulo 2 such that:

$$T = \textstyle\sum_{j=1}^{n} t_j \bmod 2 \quad \text{where } t_j = \begin{cases} 1 & \text{if } (k_j = 0 \text{ and } a_j = 0) \text{ or } (k_j = 1 \text{ and } a_j = 1) \\ 0 & \text{otherwise.} \end{cases}$$

Note that $T = 0$ if there are no testers in K. When $T = 0$ we will say an *even parity event* ocurred; otherwise, an *odd parity event* occurred.

The output $B = b_1 b_2 \cdots b_n$ of the circuit layer is then

$$b_j = \begin{cases} \overline{a}_j & \text{if} \begin{cases} k_j = + \text{ and } T = 0 \text{ (even event)} \\ \text{or} \\ k_j = - \text{ and } T = 1 \text{ (odd event)} \\ \text{or} \\ k_j = 1 \end{cases} \\ a_j & \text{otherwise. } \square \end{cases}$$

It is shown in [KT90] that every circuit layer $L(n)$ computing f has an inverse layer $L^{-1}(n)$ to compute f^{-1} *i.e.* , $f^{-1}(K, f(K, A)) = A$, for any n-bit input A and any key K.

Definition 5 A *parity circuit of width n and depth d*, or simply a *$C(n,d)$ circuit*, is a matrix of d $L(n)$ circuit layers with keys denoted by $\mathbf{K} = K_1 \parallel K_2 \parallel \cdots \parallel K_d$ for which the n output bits of the $(i-1)$-th circuit layer are the n input bits for the i-th circuit layer, for $2 \leq i \leq d$. The *key* for the $C(n,d)$ circuit is a $d \times n$ matrix with its d lines containing the circuit layer keys. $\square$

Let $F(.)$ be the function from $\{0,\ 1\}^n$ to $\{0,\ 1\}^n$ computed by a circuit $C(n,\ d)$ with key $K_1 \parallel K_2 \parallel \cdots \parallel K_d$. That is, $F(\mathbf{K}, A)$ is defined as

$$F(\mathbf{K}, A) = f(K_d, f(K_{d-1}, \cdots f(K_1, A) \cdots).$$

It is also shown in [KT90] the inverse function $F^{-1}(.)$ is computed by the "inverted" circuit $C^{-1}(n,d)$ with key $K_d \parallel K_{d-1} \parallel \cdots \parallel K_1$.

Table 1 shows the behavior of an example of $C(n,d)$ circuit [KT90] with width $n = 10$ and depth $d = 3$ that will be referred to as Example 1 with key $\mathbf{K}^*$ in the later sections.

Table 1. Example 1: $C(n,d)$ when $n = 10$ and $d = 3$

Input	1	0	1	1	0	0	1	0	0	1
K_1	−	0	1	−	+	+	1	1	−	+
Output	0	0	0	0	0	0	0	1	1	1
K_2	+	1	0	1	1	+	0	−	+	−
Output	1	1	0	1	1	1	0	1	0	1
K_3	−	0	1	+	+	0	−	+	+	−
Output	1	1	1	0	0	1	0	0	1	1

4. Augmented Non-affine Parity Circuits $C_+(n,d)$

Definition 6 A function $B = f_+(K, A)$ computed by an *augmented $L(n)$ circuit layer* with key K, or simply *$L_+(n)$ layer*, is the function $V(f(K, A))$, where V is the VDS function as in Defintion 2, and f is the function computed by an $L(n)$ circuit layer. $\square$

We will see next that $L_+(n)$ layer is still invertible: for invertion just compute $V(x)$ *before* computing the inverse of $L(n)$ (as pointed out, $V(x)$ is an involution).

Theorem 1 *Every function $B = f_+(K, A)$ computed by an $L_+(n)$ layer is invertible, i.e., for any n-bit input sequence A, and any key K, there is an inverse layer, $L_+^{-1}(n)$ layer, to compute f_+^{-1} so that $f_+^{-1}(K, f_+(K, A)) = A$.*

Proof First, we have from Lemma 1 in [KT90] that every function $f(K, A)$ computed by an $L(n)$ layer has an inverse f^{-1}. From the definition, we have $f_+ = V \circ f$ and $f_+^{-1} = f^{-1} \circ V$. Since V is an involution, we have

$$f_+^{-1} \circ f_+ = f^{-1} \circ V \circ V \circ f = identity \quad \square$$

$L_+(n)$ layers are composed as $L(n)$ layers are in Section 3:

Definition 7 An *augmented parity circuit of width n and depth d*, or simply a $C_+(n,d)$ *circuit*, is a matrix of d $L_+(n)$ layers with keys denoted by $\mathbf{K} = K_1 \parallel K_2 \parallel \cdots \parallel K_d$ for which the n output bits of the $(i-1)$-th circuit layer are the n input bits for the i-th circuit layer, for $2 \le i \le d$. The *key* for the $C_+(n,\ d)$ circuit is a $d \times n$ matrix with its d lines containing the circuit layer keys. A function $F_+(\mathbf{K}, A)$ is computed by a $C_+(n,d)$ circuit as:

$$F_+(\mathbf{K}, A) = f_+(K_d, f_+(K_{d-1}, \cdots, f_+(K_1, A)\cdots)$$

where each $f_+(K_i, .)$ is computed by a $L_+(n)$ circuit layer as defined before. $\square$

Since each function computed by $L_+(n)$ layers is invertible, as we have seen, the functions F_+ computed by $C_+(n,d)$ circuits are also invertible.

Table 2 shows the behavior of a $C_+(10,3)$ circuit with the same input and the same key $\mathbf{K}^*$ in Example 1.

Table 2. $C_+(n,d)$ when $n = 10$ and $d = 3$

Input	1	0	1	1	0	0	1	0	0	1	swap ?
K_1	−	0	1	−	+	+	1	1	−	+	
Output	0	0	1	1	1	0	0	0	0	0	yes
K_2	+	1	0	1	1	+	0	−	+	−	
Output	0	1	1	0	0	0	0	1	0	1	no
K_3	−	0	1	+	+	0	−	+	+	−	
Output	0	0	0	1	1	0	1	0	1	1	yes

5. Swapping Properties for C_+ Circuits

The swapping properties for C_+ are clarified in the following Theorems 2, 3 and 4.

Theorem 2 *Let n be a positive integer ($n \ge 1$), let $A = a_1\ a_2\ \cdots\ a_n \in \{0,1\}^n$ be an n-bit input sequence to a circuit $C(n,d)$ with key $\mathbf{K}$ and let $B = b_1 b_2 \cdots b_n \in \{0,1\}^n$ be the n-bit output sequence. If A is uniformly generated, then*

$$Prob\{weight(B)\ is\ odd\} = \frac{1}{2}, \quad Prob\{weight(B)\ is\ even\} = \frac{1}{2}.$$

Proof By hypothesis, $Prob\{a_j = 0\} = 1/2$ and $Prob\{a_j = 1\} = 1/2$, for $1 \le j \le n$. Let $p = Prob\{a_j\ is\ complemented\ by\ \mathbf{K}\}$. Then:

$$\begin{aligned} Prob\{b_j = 0\} &= Prob\{a_j = 1\} \cdot p + Prob\{a_j = 0\} \cdot (1-p) \\ &= (1/2)p + (1/2)(1-p) = 1/2. \end{aligned}$$

Similarly, one can show $Prob\{b_j = 1\} = 1/2$, for $1 \le j \le n$.

By mathematical induction, we show $Prob\{weight(B)\ is\ odd\} = 1/2$ for any positive integer n. When $n = 1$, we have $Prob\{weight(B)\ is\ odd\} = 1/2$. Let $B \in \{0,\ 1\}^k$ and $B^+ = (B \parallel b_{k+1}) \in \{0,\ 1\}^{k+1}$. If $Prob\{weight(B)\ is\ odd\} = 1/2$, then we have

$$\begin{aligned} Prob\{weight(B^+) \text{ is odd}\} &= Prob\{weight(B) \text{ is odd}\} \cdot Prob\{b_{k+1} = 0\} \\ &\quad + Prob\{weight(B) \text{ is even}\} \cdot Prob\{b_{k+1} = 1\} \\ &= (1/2) \cdot (1/2) + (1/2) \cdot (1/2) \\ &= 1/2. \quad \square \end{aligned}$$

From Theorem 2, a swapping occurs in an $L_+(n)$ layer with probability $1/2$. If A is uniformly generated, then we have the following formulas from well known results of binomial distribution,

$$Prob\{\textit{one or more swappings occur in } C_+(n,d) \textit{ circuit}\} = 1 - \left(\frac{1}{2}\right)^d.$$

$$\textit{The average of the number of swappings in } C_+(n,d) \textit{ circuit is : } \frac{d}{2}.$$

$$\textit{The variance of the number of swappings in } C_+(n,d) \textit{ circuit is : } \frac{d}{4}.$$

Let p be the probability that the swapping occurs in one layer. Considering now d layers, we have: the first formula is derived from the equation:

$$Prob\{\text{one or more swappings occur in } d \text{ layers}\}$$

$$= 1 - Prob\{\text{no swappings occur in } d \text{ layers}\}$$

The average and the variance are derived from well known results of binomial distribution: the average of the number of swappings in d layers is dp, and its variance is $dp(1-p)$. Since $p = 1/2$, we have the above formulas.

By randomization through VDS, the output of $F_+(\mathbf{K}, A)$ coincides with the output of $F(\mathbf{K}, A)$ with the following probability.

Theorem 3 *Let $P(n,d) = Prob\{F_+(\mathbf{K}, A) = F(\mathbf{K}, A)\}$ for a common set of input A and key $\mathbf{K}$, where $F_+(\mathbf{K}, A)$ is computed by $C_+(n,d)$, and $F(\mathbf{K}, A)$ is computed by $C(n,d)$. If A and $\mathbf{K}$ are uniformly generated, then*

$$P(n,1) = \frac{1}{2},$$

$$P(n,d) = \left(\frac{1}{4} - \frac{1}{2^{n+1}} - \frac{1}{2^{n-1}+1}\right)\left(\frac{1}{2} - \frac{1}{2^n}\right)^{d-2} + \frac{1}{2^{n-1}+1} \quad \text{if } d \geq 2.$$

Proof

Case 1 ($d = 1$): If the weight of $f(K, A)$ is odd, then $L \neq R$ and $f_+(K, A) = V \circ f(K, A) \neq f(K, A)$. Since $Prob\{f_+(K, A) \neq f(K, A)\} = 1/2$, we have $P(n, 1) = 1/2$.

Case 2 ($d \geq 2$): Let $\mathbf{K_d}$ be the key of d layers. If $d = 2$, $f_+(K_1, A) = f(K_1, A)$ $(= A')$ and $f_+(K_2, A') \neq f(K_2, A')$, then $F_+(\mathbf{K_2}, A) \neq F(\mathbf{K_2}, A)$ with probability 1. If $f_+(K_1, A) \neq f(K_1, A)$, then $F_+(\mathbf{K_2}, A) = F(\mathbf{K_2}, A)$ with probability $1/2^n$. Thus, when $d = 2$, we have

$$\begin{aligned} & P(n,2) \\ = \; & Prob\{F_+(\mathbf{K_2}, A) = F(\mathbf{K_2}, A)\} \\ = \; & Prob\{f_+(K_2, f_+(K_1, A)) = f(K_2, f(K_1, A))\} \\ = \; & Prob\{f_+(K_1, A) = f(K_1, A)\ (= A')\} \cdot Prob\{f_+(K_2, A') = f(K_2, A')\} \\ & + Prob\{f_+(K_1, A) \neq f(K_1, A)\} \cdot \tfrac{1}{2^n} \\ = \; & \tfrac{1}{4} + \tfrac{1}{2}\tfrac{1}{2^n} \end{aligned}$$

More generally, when $d \geq 2$, we have

$$\begin{aligned} & P(n,d) \\ = \; & Prob\{F_+(\mathbf{K}_d, A) = F(\mathbf{K}_d, A)\} \\ = \; & Prob\{F_+(\mathbf{K}_{d-1}, A) = F(\mathbf{K}_{d-1}, A)\ (= A'')\} \cdot Prob\{f_+(K_d, A'') = f(K_d, A'')\} \\ & + Prob\{F_+(\mathbf{K}_{d-1}, A) \neq F(\mathbf{K}_{d-1}, A)\} \cdot \tfrac{1}{2^n} \\ = \; & P(n,d-1)\tfrac{1}{2} + (1 - P(n,d-1))\tfrac{1}{2^n} \\ = \; & P(n,d-1) \cdot (\tfrac{1}{2} - \tfrac{1}{2^n}) + \tfrac{1}{2^n}. \end{aligned}$$

By obtaining a finite geometric sum, we have the above formula. □

6. Non-affineness

6.1 Non-affineness Measure

In general, a cryptographic function $\mathcal{F}$ is affine if and only if the following equation holds for any input $A = (a_1, a_2, \cdots, a_n)$, $a_i \in \{0,1\}$ and any key $\mathbf{K}$.

$$\mathcal{F}(\mathbf{K}, A) = \mathcal{F}(\mathbf{K}, \mathbf{0}) \oplus a_1 \mathcal{D}(\tilde{A}_n) \oplus a_2 \mathcal{D}(\tilde{A}_{n-1}) \oplus \cdots \oplus a_n \mathcal{D}(\tilde{A}_1), \tag{1}$$

where $\mathcal{D}(\tilde{A}_i) = \mathcal{F}(\mathbf{K}, \tilde{A}_i) \oplus \mathcal{F}(\mathbf{K}, \mathbf{0})$, and $\tilde{A}_i$ $(1 \leq i \leq n)$ denotes an input with only the i-th bit equal to 1, and $\oplus$ denotes the exclusive-or operation.

If there is a nonempty set of inputs A and a nonempty set of keys $\mathbf{K}$ for which equation (1) does not hold, then $\mathcal{F}$ is *non-affine*. A measure of non-affineness can be defined by the number of pairs (A, K) for which equation (1) does not hold. It is similar to a measure of non-linearity which is often defined by the order of the Boolean canonical form of the nonlinear function [R86]. Thus, we introduce a normalized non-affineness measure as follows.

Definition 8 Let $\mathcal{A}$ be the input set, and $|\mathcal{A}|$ be the number of elements in $\mathcal{A}$. Let H be the number of elements in $\mathcal{A}$ for which equation (1) does not hold. *A key-dependent non-affineness measure* $N_{\mathbf{K}}$ for a cryptographic function $\mathcal{F}$ with key $\mathbf{K}$ is defined by

$$N_{\mathbf{K}} = \frac{H}{|\mathcal{A}|}.$$

Let $\mathcal{K}$ be the key set, and $|\mathcal{K}|$ be the number of elements in $\mathcal{K}$. *A non-affineness measure* N is defined by an average of $N_{\mathbf{K}}$ over the key set $\mathcal{K}$ as

$$N = \frac{\sum_{\mathcal{K}} N_{\mathbf{K}}}{|\mathcal{K}|}. \quad \square$$

Note that $\mathcal{F}$ is affine if and only if $N = 0$. Even if $\mathcal{F}$ is non-affine, there may exist keys implying $N_{\mathbf{K}} = 0$. If $\mathcal{F}$ is $F_+(\mathbf{K}, A)$ computed by $C_+(n,d)$, then N is evaluated by all of the combinations of 2^n inputs and 4^{nd} keys. In general the bounds for N are evaluated as follows.

Theorem 4 *Let $\mathcal{F}$ be a bijection from $\{0,1\}^n$ to $\{0,1\}^n$. A non-affineness measure N is bounded as*

$$0 \leq N \leq 1 - \frac{n+1}{2^n}.$$

Proof For any cryptographic function $\mathcal{F}$ and any key $\mathbf{K}$, equation (1) holds for the inputs $\tilde{A}_i$ $(1 \le i \le n)$ and the input equal to zero. That is, $n+1$ inputs always satisfy equation (1). Thus, we have $H \le 2^n - (n+1)$. Consequently, we have the above inequality. □

Theorem 5 *Let $\mathcal{F}$ be a bijection from $\{0,1\}^n$ to $\{0,1\}^n$. If $n = 2$, then $\mathcal{F}$ is affine.*

Proof If $\mathcal{F}$ is a bijection from $\{0,1\}^2$ to $\{0,1\}^2$, then the function $\mathcal{F}$ has four outputs such as $B_1 = (0,0)$, $B_2 = (0,1)$, $B_3 = (1,0)$ and $B_4 = (1,1)$. Since $B_i = B_j \oplus B_k \oplus B_\ell$ for any combination of distinct subscripts (i,j,k,ℓ), equation (1) always holds. □

6.2 Non-affineness for $\mathbf{C_+}$ Circuits

The non-affine conditions for $L_+(n)$ and $C_+(n,d)$ will be shown in Theorems 6 and 7.

Theorem 6 *A function $f_+(.)$ based on $L_+(n)$ is not affine if $n \ge 4$.*

Proof: We prove that there is a key K so that $f_+(K,A)$ is not affine. Consider four input sets A_0, A_1, A_2, A_3 and their outputs such that

$$B_i = (b_{i,1}, b_{i,2}, ..., b_{i,n}) = f_+(K, A_i) = f_+(K, (a_{i,1}, a_{i,2}, ..., a_{i,n})), \quad (0 \le i \le 3,\ n \ge 4).$$

$$\begin{array}{lcll} A_0 & = & (0,0,0,...,0), & (a_{0,j} = 0 \ \ (1 \le j \le n)), \\ A_1 & = & (1,0,0,...,0), & (a_{1,1} = 1,\ a_{1,j} = 0 \ \ (j \ne 1)), \\ A_2 & = & (0,1,0,...,0), & (a_{2,2} = 1,\ a_{2,j} = 0 \ \ (j \ne 2)), \\ A_3 & = & (1,1,0,...,0), & (a_{3,1} = a_{3,2} = 1,\ a_{3,j} = 0 \ \ (j \ne 1,2)). \end{array}$$

If the function $f_+(.)$ is affine, then the following equation must hold for any key.

$$B_3 = B_0 \oplus B_1 \oplus B_2.$$

However, when the key K is all zero, we have

$$\begin{array}{lcll} B_0 & = & (0,0,0,...,0,0,...,0), & (b_{0,j} = 0 \ \ (1 \le j \le n)), \\ B_1 & = & (0,0,0,...,1,0,...,0), & (b_{1,n/2+1} = 1,\ b_{1,j} = 0 \ \ (j \ne n/2+1)), \\ B_2 & = & (0,0,0,...,0,1,...,0), & (b_{2,n/2+2} = 1,\ b_{2,j} = 0 \ \ (j \ne n/2+2)), \\ B_3 & = & (1,1,0,...,0,0,...,0), & (b_{3,1} = b_{3,2} = 1,\ b_{3,j} = 0 \ \ (j \ne 1,2)), \end{array}$$

and

$$B_3 \ne B_0 \oplus B_1 \oplus B_2.$$

Thus, the function $f_+(.)$ is not affine if $n \ge 4$. □

Theorem 7 *A function $F_+(.)$ based on $C_+(n,d)$ is not affine if $n \ge 4$.*

Proof: Without loss of generality, we show the case when $n = 4$. We prove that we can construct keys $\mathbf{K} = K_1 \parallel K_2 \parallel \cdots \parallel K_d$ so that $F_+(\mathbf{K}, A)$ is not affine. To check non-affineness simply consider the four input sets A_0, A_1, A_2 and A_3 such that

$$A_0 = (0,0,0,0), \quad A_1 = (1,0,0,0), \quad A_2 = (0,1,0,0), \quad A_3 = (1,1,0,0)$$

Let B_i^ℓ be the output of the ℓ-th circuit layer $L_+(4)$ for input A_i.

$$B_i^\ell = f_+(K_\ell, f_+(K_{\ell-1}, \cdots f_+(K_1, (a_{i,1}, a_{i,2}, a_{i,3}, a_{i,4})), \quad (0 \le i \le 3).$$

If the function $F_+(.)$ is affine, then the following equation must hold for any key.

$$B_3^d = B_0^d \oplus B_1^d \oplus B_2^d.$$

However, we can choose key $\mathbf{K}$ so that this equation does not hold.
(1) If d is odd, each layer key is chosen as

$$K_\ell = (0,0,0,0) \quad (1 \le \ell \le d).$$

Thus, we have

$$B_0^{d-1} = (0,0,0,0), \quad B_1^{d-1} = (1,0,0,0), \quad B_2^{d-1} = (0,1,0,0), \quad B_3^{d-1} = (1,1,0,0),$$

$$B_0^d = (0,0,0,0), \quad B_1^d = (0,0,1,0), \quad B_2^d = (0,0,0,1), \quad B_3^d = (1,1,0,0).$$

Consequently,

$$B_3^d \neq B_0^d \oplus B_1^d \oplus B_2^d.$$

(2) If d is even, each layer key is chosen as

$$K_\ell = (0,0,0,0), \quad (1 \le \ell \le d-2), \quad K_{d-1} = (+,-,0,0), \quad K_d = (+,0,0,0).$$

Thus, we have

$$B_0^{d-2} = (0,0,0,0), \quad B_1^{d-2} = (1,0,0,0), \quad B_2^{d-2} = (0,1,0,0), \quad B_3^{d-2} = (1,1,0,0),$$

$$B_0^{d-1} = (0,0,1,0), \quad B_1^{d-1} = (0,0,0,0), \quad B_2^{d-1} = (1,1,0,0), \quad B_3^{d-1} = (0,0,0,1),$$

$$B_0^d = (1,0,1,0), \quad B_1^d = (0,0,0,0), \quad B_2^d = (0,0,0,1), \quad B_3^d = (1,0,0,1).$$

Consequently,

$$B_3^d \neq B_0^d \oplus B_1^d \oplus B_2^d.$$

From cases (1) and (2), we conclude that function $F_+(.)$ is not affine when $n = 4$. The general case when $n \ge 6$ is similarly formalized as in the proof of Theorem 6. □

6.3 Evaluation of Non-affineness Measure for C_+ Circuits

6.3.1 Example

We use here the same key $\mathbf{K}^*$ used in $C(10,3)$ of Example 1 in Section 3 for comparison reasons.

Putting $\mathcal{F} = F_+$ and $D(\tilde{A}_i) = F_+(\mathbf{K}^*, \mathbf{0}) \oplus F_+(\mathbf{K}^*, \tilde{A}_i)$, we have checked whether or not equation (1) holds for all of 1024 inputs. There are only 64 inputs satisfying the affine equation (1) as shown in Table 3. Therefore, the function computed by this $C_+(n,d)$ circuit is *not affine*.

Table 3. Inputs satisfying the affine equation for $C_+(10,3)$ with $\mathbf{K}^*$

000	008	023	062	070	0e3	117	174	19f	200	24c	284	2eb	31f	397	3f4
001	010	040	063	073	0ef	11b	178	1f0	20c	24f	288	2ef	370	399	3f8
002	013	043	067	080	100	160	193	1f4	22c	263	28c	313	378	39a	3f9
004	020	061	06b	08c	103	163	197	1fc	22f	26f	2ee	31b	37c	39b	3fc

Since $|A| = 1024$ and $H = 960$ $(= 1024 - 64)$, we have $N_{\mathbf{K}^*} = 960/1024 = 0.9375$. Note that equation (1) holds for the inputs $\tilde{A}_i$ with only the i-th bit equal to 1 $(1 \leq i \leq 10)$, as shown in underlined numbers in Table 3.

6.3.2 Total Properties of Non-affineness

By computer simulation, we have estimated the non-affineness measure N for $C_+(n,d)$ when $2 \leq n \leq 16$ and $1 \leq d \leq 10$. Table 4 shows the range of the values of $N_{\mathbf{K}}$, which have been exhaustively computed for all keys. For example, if $n = 4$ and $d = 1$, then $N_{\mathbf{K}} = N = 1/4 = 0.250$ for any key among all of $256(= 4^4)$ keys. From Table 4, we can observe that circuits $C_+(n,d)$ may imply $N_{\mathbf{K}} = 0$ for some keys if $n = 4$, $1 \leq d \leq 2$. However, $N_{\mathbf{K}} \neq 0$ otherwise. Table 5 shows the values of N obtained by an extensive computer simulation. From Table 5, we can observe that the degree of non-affineness N for $C_+(n,d)$ increases as n or d increases.

Table 4. Key-dependent non-affineness measure $N_{\mathbf{K}}$

n	d	Range of $N_{\mathbf{K}}$	No. of tested keys	Comments
4	1	$N_{\mathbf{K}} = 0.250$	$256(= 4^4)$	
4	2	$0.000 \leq N_{\mathbf{K}} \leq 0.500$	$65536(= 4^8)$	$N_{\mathbf{K}} = 0$ for 25.00% keys
4	3	$0.000 \leq N_{\mathbf{K}} \leq 0.625$	$16777216(= 4^{12})$	$N_{\mathbf{K}} = 0$ for 3.125% keys
6	1	$0.375 \leq N_{\mathbf{K}} \leq 0.750$	$4096(= 4^6)$	
8	1	$0.438 \leq N_{\mathbf{K}} \leq 0.813$	$65536(= 4^8)$	

Table 5. Non-affineness measure N (*: results of exhaustive tests)

	$n=2$	$n=4$	$n=6$	$n=8$	$n=10$	$n=16$
$d=1$	0.00	0.250*	0.445*	0.566*	0.605	0.999
$d=2$	0.00	0.266*	0.548	0.823	0.913	0.999
$d=3$	0.00	0.350*	0.683	0.886	0.946	0.999
$d=4$	0.00	0.405	0.740	0.901	0.969	0.999
$d=6$	0.00	0.440	0.810	0.921	0.980	0.999
$d=8$	0.00	0.492	0.853	0.939	0.983	0.999
$d=10$	0.00	0.527	0.866	0.952	0.986	0.999

7. Other Cryptographic Properties for C_+ Circuits

Besides involution and non-affineness, other cryptographic properties such as nonlinearity, the probability of bit complementation, avalanche effect for $C_+(n,d)$ circuits can be clarified. These properties (except non-affineness) are similar to those for $C(n,d)$ circuits, which were described in [KT90]. For $C_+(n,d)$ circuits, the n and d values can be increased as necessary to properly secure a cryptosystem.

8. Conclusions

We have proposed a family of augmented non-affine parity circuits $C_+(n,d)$ by introducing a random involution called value-dependent swapping (VDS).

We also incorporated *VDS* into DES to make it stronger against differential [BS90] and linear cryptanalysis [KKT94,NKKT96].

References

[BS90] Biham, E. and A. Shamir: "Differential Cryptanalysis of DES-like Cryptosystems", presented at CRYPTO'90 (Aug.), 1990.

[KKT94] Kaneko, T., Koyama, K. and R. Terada: "Dynamic swapping schemes and Differential Cryptanalysis", IEICE Transactions on Fundamentals, vol. E77-A, pp 1328-1336, 1994.

[KT90] Koyama, K. and R. Terada: 'Nonlinear Parity Circuits and Their Cryptographic Applications", Proceedings of CRYPTO'90, 1990.

[NKKT96] Nakao, Y., Kaneko, T., Koyama, K. and R. Terada: "The security of an RDES cryptosystem against Linear Cryptanalysis", IEICE Transactions on Fundamentals, vol. E79-A, pp 12-19, 1996.

[R86] Rueppel, R.A.:"Analysis and Design of Stream Ciphers", Springer-Verlag, Berlin, 1986.

[YT97] Youssef, A.M., and S.E. Tavares:"Cryptanalysis of 'nonlinear- parity circuits' ", Electronic Letters, vol. 33 (7), pp. 585-586, 1997.

RELATÓRIOS TÉCNICOS

DEPARTAMENTO DE CIÊNCIA DA COMPUTAÇÃO

Instituto de Matemática e Estatística da USP

A listagem contendo os relatórios técnicos anteriores a 1994 poderá ser consultada ou solicitada à Secretaria do Departamento, pessoalmente, por carta ou e-mail(mac@ime.usp.br).

Flavio S. Corrêa da Silva
AN ALGEBRAIC VIEW OF COMBINATION RULES
RT-MAC-9401, Janeiro de 1994, 10 pp.

Flavio S. Corrêa da Silva e Junior Barrera
AUTOMATING THE GENERATION OF PROCEDURES TO ANALYSE BINARY IMAGES
RT-MAC-9402, Janeiro de 1994, 13 pp.

Junior Barrera, Gerald Jean Francis Banon e Roberto de Alencar Lotufo
A MATHEMATICAL MORPHOLOGY TOOLBOX FOR THE KHOROS SYSTEM
RT-MAC-9403, Janeiro de 1994, 28 pp.

Flavio S. Corrêa da Silva
ON THE RELATIONS BETWEEN INCIDENCE CALCULUS AND FAGIN-HALPERN STRUCTURES
RT-MAC-9404, abril de 1994, 11 pp.

Junior Barrera; Flávio Soares Corrêa da Silva e Gerald Jean Francis Banon
AUTOMATIC PROGRAMMING OF BINARY MORPHOLOGICAL MACHINES
RT-MAC-9405, abril de 1994, 15 pp.

Valdemar W. Setzer; Cristina G. Fernandes; Wania Gomes Pedrosa e Flavio Hirata
UM GERADOR DE ANALISADORES SINTÁTICOS PARA GRAFOS SINTÁTICOS SIMPLES
RT-MAC-9406, abril de 1994, 16 pp.

Siang W. Song
TOWARDS A SIMPLE CONSTRUCTION METHOD FOR HAMILTONIAN DECOMPOSITION OF THE HYPERCUBE
RT-MAC-9407, maio de 1994, 13 pp.

Julio M. Stern
MODELOS MATEMATICOS PARA FORMAÇÃO DE PORTFÓLIOS
RT-MAC-9408, maio de 1994, 50 pp.

Imre Simon
STRING MATCHING ALGORITHMS AND AUTOMATA
RT-MAC-9409, maio de 1994, 14 pp.

Valdemar W. Setzer e Andrea Zisman
*CONCURRENCY CONTROL FOR ACCESSING AND COMPACTING B-TREES**
RT-MAC-9410, junho de 1994, 21 pp.

Renata Wassermann e Flávio S. Corrêa da Silva
TOWARDS EFFICIENT MODELLING OF DISTRIBUTED KNOWLEDGE USING EQUATIONAL AND ORDER-SORTED LOGIC
RT-MAC-9411, junho de 1994, 15 pp.

Jair M. Abe, Flávio S. Corrêa da Silva e Marcio Rillo
PARACONSISTENT LOGICS IN ARTIFICIAL INTELLIGENCE AND ROBOTICS.
RT-MAC-9412, junho de 1994, 14 pp.

Flávio S. Corrêa da Silva, Daniela V. Carbogim
A SYSTEM FOR REASONING WITH FUZZY PREDICATES
RT-MAC-9413, junho de 1994, 22 pp.

Flávio S. Corrêa da Silva, Jair M. Abe, Marcio Rillo
MODELING PARACONSISTENT KNOWLEDGE IN DISTRIBUTED SYSTEMS
RT-MAC-9414, julho de 1994, 12 pp.

Nami Kobayashi
THE CLOSURE UNDER DIVISION AND A CHARACTERIZATION OF THE RECOGNIZABLE Z-SUBSETS
RT-MAC-9415, julho de 1994, 29pp.

Flávio K. Miyazawa e Yoshiko Wakabayashi
AN ALGORITHM FOR THE THREE-DIMENSIONAL PACKING PROBLEM WITH ASYMPTOTIC PERFORMANCE ANALYSIS
RT-MAC-9416, novembro de 1994, 30 pp.

Thomaz I. Seidman e Carlos Humes Jr.
SOME KANBAN-CONTROLLED MANUFACTURING SYSTEMS: A FIRST STABILITY ANALYSIS
RT-MAC-9501, janeiro de 1995, 19 pp.

C.Humes Jr. and A.F.P.C. Humes
STABILIZATION IN FMS BY QUASI- PERIODIC POLICIES
RT-MAC-9502, março de 1995, 31 pp.

Fabio Kon e Arnaldo Mandel
SODA: A LEASE-BASED CONSISTENT DISTRIBUTED FILE SYSTEM
RT-MAC-9503, março de 1995, 18 pp.

Junior Barrera, Nina Sumiko Tomita, Flávio Soares C. Silva, Routo Terada
AUTOMATIC PROGRAMMING OF BINARY MORPHOLOGICAL MACHINES BY PAC LEARNING
RT-MAC-9504, abril de 1995,16 pp.

Flávio S. Corrêa da Silva e Fabio Kon
CATEGORIAL GRAMMAR AND HARMONIC ANALYSIS
RT-MAC-9505, junho de 1995,17 pp.

Henrique Mongelli e Routo Terada
ALGORITMOS PARALELOS PARA SOLUÇÃO DE SISTEMAS LINEARES
RT-MAC-9506, junho de 1995, 158 pp.

Kunio Okuda
PARALELIZAÇÃO DE LAÇOS UNIFORMES POR REDUÇÃO DE DEPENDÊNCIA
RT-MAC-9507, julho de 1995, 27 pp.

Valdemar W. Setzer e Lowell Monke
COMPUTERS IN EDUCATION: WHY, WHEN, HOW
RT-MAC-9508, julho de 1995, 21 pp.

Flávio S. Corrêa da Silva
REASONING WITH LOCAL AND GLOBAL INCONSISTENCIES
RT-MAC-9509, julho de 1995, 16 pp.

Julio M. Stern
MODELOS MATEMÁTICOS PARA FORMAÇÃO DE PORTFÓLIOS
RT-MAC-9510, julho de 1995, 43 pp.

Fernando Iazzetta e Fabio Kon
A DETAILED DESCRIPTION OF MAXANNEALING
RT-MAC-9511, agosto de 1995, 22 pp.

Flávio Keidi Miyazawa e Yoshiko Wakabayashi
POLYNOMIAL APPROXIMATION ALGORITHMS FOR THE ORTHOGONAL Z-ORIENTED 3-D PACKING PROBLEM
RT-MAC-9512, agosto de 1995, pp.

Junior Barrera e Guillermo Pablo Salas
SET OPERATIONS ON COLLECTIONS OF CLOSED INTERVALS AND THEIR APPLICATIONS TO THE AUTOMATIC PROGRAMMINIG OF MORPHOLOGICAL MACHINES
RT-MAC-9513, agosto de 1995, 84 pp.

Marco Dimas Gubitoso e Jörg Cordsen
PERFORMANCE CONSIDERATIONS IN VOTE FOR PEACE
RT-MAC-9514, novembro de 1995, 18pp.

Carlos Eduardo Ferreira e Yoshiko Wakabayashi
ANAIS DA I OFICINA NACIONAL EM PROBLEMAS COMBINATÓRIOS: TEORIA, ALGORITMOS E APLICAÇÕES
RT-MAC-9515, novembro de 1995, 45 pp.

Markus Endler and Anil D'Souza
SUPPORTING DISTRIBUTED APPLICATION MANAGEMENT IN SAMPA
RT-MAC-9516, novembro de 1995, 22 pp.

Junior Barrera, Routo Terada,
Flávio Corrêa da Silva and Nina Sumiko Tomita
*AUTOMATIC PROGRAMMING OF MMACH'S FOR OCR**
RT-MAC-9517, dezembro de 1995, 14 pp.

Junior Barrera, Guillermo Pablo Salas and Ronaldo Fumio Hashimoto
SET OPERATIONS ON CLOSED INTERVALS AND THEIR APPLICATIONS TO THE AUTOMATIC PROGRAMMING OF MMACH'S
RT-MAC-9518, dezembro de 1995, 14 pp.

Daniela V. Carbogim and Flávio S. Corrêa da Silva
FACTS, ANNOTATIONS, ARGUMENTS AND REASONING
RT-MAC-9601, janeiro de 1996, 22 pp.

Kunio Okuda
REDUÇÃO DE DEPENDÊNCIA PARCIAL E REDUÇÃO DE DEPENDÊNCIA GENERALIZADA
RT-MAC-9602, fevereiro de 1996, 20 pp.

Junior Barrera, Edward R. Dougherty and Nina Sumiko Tomita
AUTOMATIC PROGRAMMING OF BINARY MORPHOLOGICAL MACHINES BY DESIGN OF STATISTICALLY OPTIMAL OPERATORS IN THE CONTEXT OF COMPUTATIONAL LEARNING THEORY.
RT-MAC-9603, abril de 1996, 48 pp.

Junior Barrera e Guillermo Pablo Salas
SET OPERATIONS ON CLOSED INTERVALS AND THEIR APPLICATIONS TO THE AUTOMATIC PROGRAMMINIG OF MMACH'S
RT-MAC-9604, abril de 1995, 66 pp.

Kunio Okuda
CYCLE SHRINKING BY DEPENDENCE REDUCTION
RT-MAC-9605, maio de 1996, 25 pp.

Julio Stern, Fabio Nakano e Marcelo Lauretto
REAL: REAL ATTRIBUTE LEARNING FOR STRATEGIC MARKET OPERATION
RT-MAC-9606, agosto de 1996, 16 pp.

Markus Endler
SISTEMAS OPERACIONAIS DISTRIBUÍDOS: CONCEITOS, EXEMPLOS E TENDÊNCIAS
RT-MAC-9607, agosto de 1996, 120 pp.

Hae Yong Kim
CONSTRUÇÃO RÁPIDA E AUTOMÁTICA DE OPERADORES MORFOLÓGICOS E EFICIENTES PELA APRENDIZAGEM COMPUTACIONAL
RT-MAC-9608, outubro de 1996, 19 pp.

Marcelo Finger
NOTES ON COMPLEX COMBINATORS AND STRUCTURALLY-FREE THEOREM PROVING
RT-MAC-9609, dezembro 1996, 28 pp.

Carlos Eduardo Ferreira, Flávio Keidi Miyazawa e Yoshiko Wakabayashi (eds)
ANAIS DA I OFICINA NACIONAL EM PROBLEMAS DE CORTE E EMPACOTAMENTO
RT-MAC-9610, dezembro de 1996, 65 pp.

Carlos Eduardo Ferreira, C. C. de Souza e Yoshiko Wakabayashi
REARRANGEMENT OF DNA FRAGMENTS: A BRANCH-AND-CUT ALGORITHM
RT-MAC-9701, janeiro de 1997, 24 pp.

Marcelo Finger
NOTES ON THE LOGICAL RECONSTRUCTION OF TEMPORAL DATABASES
RT-MAC-9702, março de 1997, 36 pp.

Flávio S. Corrêa da Silva, Wamberto W. Vasconcelos e David Robertson
COOPERATION BETWEEN KNOWLEDGE BASED SYSTEMS
RT-MAC-9703, abril de 1997, 18 pp.

Junior Barrera, Gerald Jean Francis Banon, Roberto de Alencar Lotufo, Roberto Hirata Junior
MMACH: A MATHEMATICAL MORPHOLOGY TOOLBOX FOR THE KHOROS SYSTEM
RT-MAC-9704, maio de 1997, 67 pp.

Julio Michael Stern e Cibele Dunder
PORTFÓLIOS EFICIENTES INCLUINDO OPÇÕES
RT-MAC-9705, maio de 1997, 29 pp.

Junior Barrera e Ronaldo Fumio Hashimoto
COMPACT REPRESENTATION OF W-OPERATORS
RT-MAC-9706, julho de 1997, 13 pp.

Dilma M. Silva e Markus Endler
CONFIGURAÇÃO DINÂMICA DE SISTEMAS
RT-MAC-9707, agosto de 1997, 35 pp

Kenji Koyama e Routo Terada
AN AUGMENTED FAMILY OF CRYPTOGRAPHIC PARITY-CIRCUITS
RT-MAC-9708, setembro de 1997, 15 pp