NMIX: AN IDEAL CANDIDATE FOR KEY MIXING

Jaydeb Bhaumik
G. S. Sanyal School of Telecommunications, Indian Institute of Technology, Kharagpur, India

Dipanwita Roy Chowdhury
Department of Computer Science and Engineering, Indian Institute of Technology, Kharagpur, India

Keywords: Boolean function, Nonlinearity, Reversibility.

Abstract: Boolean functions play an important role in cryptography. In this paper, a Boolean function '*Nmix*' has been proposed which is balanced, reversible and highly nonlinear in nature. It has been proved that the bias of each of the bits decrease exponentially with the bit position. Thus the Boolean function provides high resistance against linear cryptanalysis compared to addition modulo 2^n, the popularly known non-linear function used in cryptographic primitives. The cryptographic properties of *Nmix* are compared with similar cryptographic functions and the result justify to select it as as an ideal choice for key mixing.

1 INTRODUCTION

Boolean functions play a vital role in the design of cryptographic primitives. They have been employed as key mixing functions in block ciphers. In case of AES and DES, XOR function is used as a key mixing function. But XOR function does not provide any nonlinearity and it is provided by the substitution boxes (S-box) solely. Addition *mod* 2^n is another popular key mixing technique which is used in block ciphers like IDEA, MARS, FEAL, SEA. In these ciphers, addition *mod* 2^n provides extra nonlinearity besides the nonlinearity provided by S-boxes. However modular addition has the demerit that the bias (Matsui, 1993) of the XOR of consecutive output bit positions is held constant at $\frac{1}{4}$. Recently another nonlinear and reversible function modular *Slash* has been proposed in (Bhattacharya, 2007). The *Slash* function has a strong resistance against linear cryptanalysis. Also it has been shown that hardware implementation cost and time delay of *Slash* is less compared to addition *mod* 2^n. However like modular addition, *Slash* has the demerit that the bias of the XOR of consecutive output bit positions is held constant at $\frac{1}{4}$. Also recent findings shows that S-boxes make the block ciphers unsuitable for light weight cryptography (Koo, 2008). Highly nonlinear Boolean functions are well suited for application of light weight cryptography (Bhaumik, 2009). Thus it may be prudent at this point to look into Boolean circuits which provide high nonlinearity to light weight block ciphers.

In this work, a new Boolean function *Nmix* has been proposed which is nonlinear, balanced and also reversible in nature. It provides better resistance against linear cryptanalysis compared to addition and *Slash*. It has been shown that the bias of the XOR of consecutive bits position in the output also smaller than the value for addition modulo 2^n. The function *Nmix* can be used as a better key mixing function in block ciphers because it is nonlinear, reversible.

The rest of the work is organized as follows. Section 2 discusses some preliminaries required for this work. Our proposed function is elaborated in section 3. Performance of the proposed function has been discussed in section 4 and section 5 concludes the work.

2 PRELIMINARIES

In this section, some basic definitions and notations have been discussed.

Affine Function. An n variable Boolean function $\xi(x_1,x_2,...,x_n)$ is said to be an affine function if the ANF of ξ is of the form $\xi(x_1,x_2,...,x_n) = p_0 \oplus p_1x_1 \oplus p_2x_2 \oplus ... \oplus p_nx_n$, where $p_0,p_1,...p_n \in \{1,0\}$. If p_0 is 0 then the function is said to be linear.

Hamming Distance. The Hamming distance be-

Roy Chowdhury D. and Bhaumik J. (2009).
NMIX: AN IDEAL CANDIDATE FOR KEY MIXING.
In *Proceedings of the International Conference on Security and Cryptography*, pages 285-288
DOI: 10.5220/0002260702850288

tween two binary strings (say x and y) of equal length is measured by wt($x \oplus y$).

Nonlinearity. Nonlinearity of an n variable Boolean function ξ is defined as the minimum Hamming distance from the set of all affine function of n variables.

Bias of Linear Approximation. It is defined as $p_i - \frac{1}{2}$, where p_i is the probability of linear approximation.

Piling-up Lemma. (Stinson, 1995) Let the biases of k of independent random variables X_{i_1}, . . . , X_{i_k} be denoted by ε_{i_1}, . . ., ε_{i_k} and $\varepsilon_{i_1,i_2,\ldots i_k}$ denote the bias of the random variable $X_{i_1} \oplus \ldots \oplus X_{i_k}$. Then $\varepsilon_{i_1,i_2,\ldots i_k} = 2^{k-1}\prod_{j=1}^{k}\varepsilon_{i_j}$

Bent Function. (Rothaus, 1976) A Boolean function $\xi(x)$ of n variable, where n is even, is called a Bent function if it has a nonlinearity value $2^{n-1} - 2^{n/2-1}$. This is the highest possible nonlinearity for an n variable Boolean function if n is even.

Theorem 1. (Sarker, 2004) The nonlinearity of Boolean function $f(x_n,\ldots,x_1) \oplus g(y_m,\ldots,y_1)$ is $2^n nl(g) + 2^m nl(f) - 2nl(f)nl(g)$, where $f(x_n,\ldots,x_1)$ and $g(y_m,\ldots,y_1)$ are the two boolean function of n and m variables respectively, $\{x_n,\ldots,x_1\} \cap \{y_m,\ldots,y_1\} = \phi$ and $nl(f)$, $nl(g)$ denote the nonlinearity of f and g respectively.

3 PROPOSED NONLINEAR FUNCTION

In this section, a new nonlinear mixing function called '*Nmix*' and inverse mixing function '*I-Nmix*' is introduced.

Forward Nonlinear mixing (*Nmix*). *Nmix* function operates on two $n-$bit variables $X = (x_{n-1}\, x_{n-2} \ldots x_0)$, $K = (k_{n-1}\, k_{n-2} \ldots k_0)$ and produces a $n-$bit output variable $Y = (y_{n-1}\, y_{n-2} \ldots y_0)$, where each output bit is related to the input bits by the following relationship

$$\begin{aligned} y_i &= x_i \oplus k_i \oplus c_{i-1} \\ c_i &= \bigoplus_{j=0}^{i} x_j \cdot k_j \oplus x_{i-1}x_i \oplus k_{i-1}k_i \end{aligned} \quad (1)$$

where $0 \le i < n$, $c_{-1} = 0$, $x_{-1} = 0$, $k_{-1} = 0$ and c_i is the carry term propagating from i^{th} bit position to $(i+1)^{th}$ bit position. The end carry c_{n-1} is neglected. Each output bit y_i is balanced for all $0 \le i < n$. We will use the notation $Y = (X \dagger K)\ mod\ 2^n = F(X,K)$ in the rest of the paper, where $\dagger$ is the *Nmix* operator.

Inverse Nonlinear Mixing (*I-Nmix*). In inverse mixing, the mixer takes two n-bit variables $Y = (y_{n-1}\, y_{n-2} \ldots y_0)$, $K = (k_{n-1}\, k_{n-2} \ldots k_0)$ as inputs and produces an $n-$bit output $X = (x_{n-1}\, x_{n-2} \ldots x_0)$. Inverse mixing operation can be defined as

$$\begin{aligned} x_i &= y_i \oplus k_i \oplus d_{i-1} \\ d_i &= \bigoplus_{j=0}^{i} x_j \cdot k_j \oplus x_{i-1}x_i \oplus k_{i-1}k_i \end{aligned} \quad (2)$$

where $0 \le i < n$, $d_{-1} = 0$, $x_{-1} = 0$, $k_{-1} = 0$, and d_i is the carry term propagating from i^{th} bit position to $(i+1)^{th}$ bit position. The end carry d_{n-1} is neglected. In the rest of the paper we will use the notation $X = (Y * K)\ mod\ 2^n = G(Y,K)$, where $*$ is the *I-Nmix* operator. Function G is the inverse function of F. The following section discusses the performance of the proposed nonlinear function, *Nmix* against linear and differential cryptanalysis.

4 PERFORMANCE OF *NMIX*

4.1 Linear Cryptanalysis

Linear cryptanalysis (LC) tries to take advantage of high probability of occurrences of linear expressions involving input bits, key bits and output bits. Following theorem explains the strength of *Nmix* against LC.

Theorem 2. The bias for best linear approximation of output bit y_i of *Nmix* is 2^{-i}, where $2 \le i < n$

Proof. Assume *Nmix* function operates on two $n-$bit variables $X = (x_{n-1} \ldots x_0)$, $K = (k_{n-1} \ldots k_0)$ and generates an n-bit variable $Y = (y_{n-1} \ldots y_0)$ such that $Y = F(X,K)$. From the definition of F, it is evident that in the output $y_i = x_i \oplus k_i \oplus c_{i-1}$, where c_{i-1} is the carry input into the i^{th} bit position and c_{i-1} for $2 \le i < n$ can be expressed as

$$c_{i-1} = x_0k_0 \oplus \ldots \oplus x_{i-1}k_{i-1} \oplus k_{i-1}k_{i-2} \oplus x_{i-1}x_{i-2} \quad (3)$$

After simplification c_{i-1} can be expressed as

$$c_{i-1} = x_0k_0 \oplus \ldots \oplus x_{i-3}k_{i-3} \oplus (x_{i-1} \oplus k_{i-2})(k_{i-1} \oplus x_{i-2}) \quad (4)$$

Let $f(x_0,k_0,\ldots,x_{i-3},k_{i-3}) = x_0k_0 \oplus \ldots \oplus x_{i-3}k_{i-3}$ and $g(x_{i-1},k_{i-1},x_{i-2},k_{i-2}) = (x_{i-1} \oplus k_{i-2})(k_{i-1} \oplus x_{i-2})$. Since f is a function of $2(i-2)$ variables and it is in the form of bent function. Therefore, non-linearity of f is $2^{2i-5} - 2^{i-3}$, where $2 \le i < n$. Also it is found that nonlinearity of the four variable function g is 4. The nonlinearity of $c_{i-1} = f \oplus g$ is computed using Theorem 1 in section 2. The nonlinearity of c_{i-1} is $2^{2i-4}.4 + (2^{2i-5} - 2^{i-3}).2^4 - 2.4.(2^{2i-5} - 2^{i-3}) = 2^{2i-1} - 2^i$. Therefore the nonlinearity of y_i is $2^2(2^{2i-1} - 2^i) = 2^{2i+1} - 2^{i+2}$ (using Theorem 1). So, number of matches in the best linear approximation is $2^{2i+2} - 2^{2i+1} + 2^{i+2} = 2^{2i+1} + 2^{i+2}$ and hence probability of matches is $\frac{1}{2} + 2^{-i}$. Therefore, bias of best

linear approximation is 2^{-i}, where $2 \leq i < n$. Since, $y_0 = x_0 \oplus k_0$, so bias of best linear approximation is $\frac{1}{2}$. For $y_1 = x_1 \oplus k_1 \oplus x_0 k_0$, the bias is $\frac{1}{4}$. Therefore, except the first two bits *Nmix* posses high nonlinearity at all other bits.

4.2 Bias for XOR of Consecutive Output Bits

From the definition of F, it is found that $y_0 \oplus y_1 = x_1 \oplus k_1 \oplus x_0 \oplus k_0 \oplus x_0 k_0$. Let $f(x_0, k_0) = x_0 \oplus k_0 \oplus x_0 k_0$. Since f is OR function so it has nonlinearity 1. Therefore $y_0 \oplus y_1$ has nonlinearity $= 2^2.1 = 4$ and bias 0.25. Similarly expression of $y_1 \oplus y_2$ is $y_1 \oplus y_2 = x_2 \oplus k_2 \oplus x_1 \oplus k_1 \oplus x_1 k_1 \oplus x_0 x_1 \oplus k_0 k_1 = x_2 \oplus k_2 \oplus x_1(1 \oplus k_1 \oplus x_0) \oplus k_1(1 \oplus k_0) = x_2 \oplus k_2 \oplus x_1 p_1 \oplus k_1 q_1$, where $p_1 = 1 \oplus k_1 \oplus x_0$ and $q_1 = 1 \oplus k_0$. The nonlinearity of $y_1 \oplus y_2$ is $2^2.6 = 24$ and bias is 0.125. For $2 \leq i < n$, $y_i \oplus y_{i+1}$ can be exressed as

$$y_i \oplus y_{i+1} = x_{i+1} \oplus k_{i+1} \oplus x_i \oplus k_i \oplus x_i k_i \oplus x_{i-1}(x_i \oplus x_{i-2}) \oplus k_{i-1}(k_i \oplus k_{i-2}) \quad (5)$$

If we assume $a_i = x_i \oplus x_{i-2}$ and $b_i = k_i \oplus k_{i-2}$, then $y_i \oplus y_{i+1} = x_{i+1} \oplus k_{i+1} \oplus x_i \oplus k_i \oplus x_i k_i \oplus x_{i-1} a_i \oplus k_{i-1} b_i = f \oplus g$, where $f = x_{i+1} \oplus k_{i+1} \oplus x_i \oplus k_i \oplus x_i k_i$ and $x_{i-1} a_i \oplus k_{i-1} b_i$. It is observed that f has nonlinearity 4 and g is in the form of four variable bent function, so it has nonlinearity 6. Therefore nonlinearity of $y_i \oplus y_{i+1}$ is $2^4.6 + 2^4.4 - 2.4.6 = 112$ and bias of best linear approximation for $y_i \oplus y_{i+1}$ is 0.0625, where $2 \leq i < n$. In case of addition and *Slash* modulo 2^n the bias for best linear approximation of $y_i \oplus y_{i+1} = 0.025$ for $0 \leq i < n$. Therefore, *Nmix* is cryptographically stronger than other two functions.

4.3 Enhancing Nonlinearity of *Nmix*

It has been observed that bias for best linear approximation of the first (starting from y_0) four/five output bits of *Nmix* are not negligible. Therefore linear cryptanalysis could be applied to recover at least few key (K) bits. But twice application of Nmix : 1st right to left and then from left to right using different sequences, increases the overall nonlinearity hence bias decreases drastically to a low value which makes linear cryptanalysis difficult. As the number of bits in a word increases the bias decreases more. Assume $Y = F_{l \leftarrow r}(X, R)$, where $F_{l \leftarrow r}$ is the *Nmix* function operates from right to left and $X = (x_{n-1} \ldots x_1\ x_0)$, $Y = (y_{n-1} \ldots y_1\ y_0)$, $R = (r_{n-1} \ldots r_1\ r_0)$ are three n-bit variables. The bitwise expression of Y as follows

$$\begin{aligned}
y_0 &= x_0 \oplus r_0 \\
y_1 &= x_1 \oplus r_1 \oplus x_0 r_0 \\
y_2 &= x_2 \oplus r_2 \oplus x_0 r_0 \oplus x_1 r_1 \oplus x_0 x_1 \oplus r_0 r_1 \\
&\ \ \vdots \\
y_{n-1} &= x_{n-1} \oplus r_{n-1} \oplus x_0 r_0 \oplus x_1 r_1 \oplus \ \ldots\ \oplus \\
&\qquad x_{n-2} r_{n-2} \oplus x_{n-3} x_{n-2} \oplus r_{n-3} r_{n-2}
\end{aligned} \quad (6)$$

If $Z = F_{l \rightarrow r}(Y, K)$, where $F_{l \rightarrow r}$ is the *Nmix* function operates from left to right and Y = (y_{n-1} ... y_1 y_0), $K = (k_{n-1} \ldots k_1\ k_0)$, $Z = (z_{n-1} \ldots z_1\ z_0)$ are three n-bit variables then bitwise expression of Z is

$$\begin{aligned}
z_{n-1} &= y_{n-1} \oplus k_{n-1} \\
z_{n-2} &= y_{n-2} \oplus k_{n-2} \oplus y_{n-1} k_{n-1} \\
z_{n-3} &= y_{n-3} \oplus k_{n-3} \oplus \ \ldots\ \oplus y_{n-1} y_{n-2} \oplus k_{n-1} k_{n-2} \\
&\ \ \vdots \\
z_0 &= y_0 \oplus k_0 \oplus y_{n-1} k_{n-1} \oplus y_{n-2} k_{n-2} \oplus \ \ldots\ \oplus \\
&\qquad y_2 k_2 \oplus y_1 k_1 \oplus y_1 y_2 \oplus k_1 k_2
\end{aligned} \quad (7)$$

Using pilling-up lemma we compute bias for best linear approximation of z_i for $0 \leq i < n$.
Bias of z_0 is $2 \times 2^{-1} \times 2^{-(n-1)} = 2^{-(n-1)}$
Bias of z_1 is $2 \times 2^{-2} \times 2^{-(n-2)} = 2^{-(n-1)}$
Bias of z_2 is $2 \times 2^{-2} \times 2^{-(n-3)} = 2^{-(n-2)}$

Bias of z_{n-1} is $2 \times 2^{-1} \times 2^{-(n-1)} = 2^{-(n-1)}$
Therefore after twice application of *Nmix*, the bias for best linear approximation of z_i depends on word size n and maximum value of bias is $\frac{1}{2^{n-2}}$. Even for 8-bit word the maximum bias is $\frac{1}{64}$ which makes linear cryptanalysis more difficult.

4.4 Differential Cryptanalysis

Key mixing using nonlinear function *Nmix* offers differential resistance. But the key mixing which is done by XOR operator, does not provide any differential resistance as always $\Delta y = \Delta x$, which is independent of the key. Assume $X = (x_{n-1}\ x_{n-2} \ldots x_0)$, $K = (k_{n-1}\ k_{n-2} \ldots k_0)$ are two n-bit inputs of *Nmix* function and corresponding output is $Y = (y_{n-1}\ y_{n-2} \ldots y_0)$, where $Y = F(X, K)$ and c_i represents the carry from the i^{th} level. Let $X' = (x'_{n-1}\ x'_{n-2} \ldots x'_0)$ be another n-bit input for same $K = (k_{n-1}\ k_{n-2} \ldots k_0)$ and the output is $Y' = (y'_{n-1}\ y'_{n-2} \ldots y'_0)$, where $Y' = F(X', K)$ and c'_i represents the carry from the i^{th} level. Then $\Delta y_i = (y_i \ \oplus \ y'_i) = \Delta x_i \oplus \Delta c_{i-1}$, where $\Delta x_i = x_i \oplus x'_i$ and $\Delta c_{i-1} = c_{i-1} \oplus c'_{i-1}$ From equation (1) it can be shown that

$$\Delta y_i = \Delta x_i \oplus x_{i-2} x_{i-1} \oplus x'_{i-2} x'_{i-1} \bigoplus_{j=0}^{i-1} k_j \Delta x_j \quad (8)$$

Table 1: Comparison of Over all Performance.

Parameters	Bitwise XOR	Addition	Slash	Nmix
Nonlinearity of output bit y_i	0	2^{2i}	$2^{2i+1}-2^{i+1}$	$2^{2i+1}-2^{i+2}$
Bias for best linear approx. of output bit y_i	0.5	0.25	$2^{-(i+1)}$	2^{-i}
Bias for best linear approx. of $y_i \oplus y_{i+1}$	0.5	0.25	0.25	0.0625
Provide differential resistance	No	Yes	No	Yes
Algebraic degree of output bit y_i	1	$i+1$	2	2
Number of gates to implement n-bit function (froward transformation)	n XOR 0 AND 0 OR	$2n+1$ XOR $2n-4$ AND $n-2$ OR	$3n-3$ XOR $n-1$ AND 0 OR	$5n-7$ XOR $3n-5$ AND 0 OR
Time Complexity	O(1)	O(n)	O(n)	O(n)

So it is observed that the probability of a particular output difference ΔY occurs given a particular input difference ΔX is function of all x_i's and x_i''s for a fixed K. In other words *Nmix* has the property that a given XOR difference does not necessarily yield a fixed output difference. Therefore the proposed function provides differential resistance.

4.5 Comparison

In this section, we discuss cryptographic properties, hardware and time complexity of our proposed function as well as exiting modular addition and *Slash*. Table 1 shows a comparison of the proposed function with the similar existing key mixing functions. From table 1, it is observed that XOR provides no nonlinearity, modulo *Slash* has maximum nonlinearity and *Nmix* has nonlinearity greater than modulo addition but less compared to *Slash*. The bias for best linear approximation of y_i decreases exponentially with bit position in case of *Nmix* and *Slash* but remains constant both in modulo addition and bitwise XOR. Also the proposed function has lowest value for bias of best linear approximation of $y_i \oplus y_{i+1}$ compared to other three functions. Similar to modulo addition, *Nmix* provides differential resistance but bitwise XOR and *Slash* does not provide any differential resistance. Addition has higher algebraic degree compared to both *Slash* and *Nmix*. To implement a n-bit key mixing layer bitwise XOR requires minimum number of logic gates. Proposed function needs $5n-7$ XOR gates and $3n-5$ AND gates to implement a n-bit mixing layer. Bitwise XOR requires minimum computation time, whereas other three nonlinear mixing functions have $O(n)$ time complexity. Therefore *Nmix* is an ideal key mixing function for cryptographic primitives.

5 CONCLUSIONS

In this work, a highly nonlinear, balanced and reversible Boolean function *Nmix* has been proposed which can be used as nonlinear key mixing function in block ciphers. It has been shown that the proposed function provides higher nonlinearity compared to modular addition. Therefore *Nmix* gives better resistance against linear cryptanalysis. Also *Nmix* provides resistance against differential attack.

REFERENCES

Bhaumik, J., Roy Chowdhury, D. (2009). An Integrated ECC-MAC Based on RS code, In Transcations on Computational Science, vol. 4, LNCS. 5430

Koo, W. K., Lee, H., Kim, Y. H. and Lee, D. H. (2008). Implementation and Analysis of New Lightweight Cryptographic Algorithm Suitable for Wireless Sensor Networks, In ISA 2008, IEEE Computer Socity.

Bhattacharya, D., Mukhopadhyay, D., Saha, D. and Roy Chowdhury, D. (2007). Strengthening NLS against Crossword Puzzle Attack, In ACISP-2007, LNCS, vol. 4586.

Sarkar, P. and Mitra, S. 2004. Construction of Nonlinear Resilient Boolean Functions Using "Small" Affine functions, In IEEE Transactions on Information Theory, vol. 50, no. 9.

Stinson, D. R. (1995). Cryptography Theory and Practice, CRC Press, 1^{st} edition.

Matsui, M. (1993). Linear cryptoanalysis method for DES ciphers, In Eurocrypt 1993, LNCS, vol. 765.

Rothaus, O. S. (1976). On "Bent" Functions, In Journal of Combinatorial Theory, vol. 20(A).