Since $t \leq 1$, we have

$$\begin{aligned} u(s, t) &= \tfrac{1}{2}\left(1 + s^2 + 2st\right)^{1/2} \\ &\leq \tfrac{1}{2}(1 + s). \end{aligned}$$

Thus, since $D(x)$ is nondecreasing in x, we have

$$\begin{aligned} \Delta_r C(r, s, t) &\geq \tfrac{1}{2}(\log e)\left(D\left(\tfrac{1}{2}(1+s)r\right) - D\left(u(s,t)r\right)\right) \\ &\geq 0 \end{aligned}$$

which completes the proof of (3.3).

REFERENCES

[1] C. H. Bennett and P. W. Shor, "Quantum information theory," *IEEE Trans. Inform. Theory*, vol. 44, pp. 2724–2742, Oct. 1998.

[2] W. Evans and L. J. Schulman, "Signal propagation, with application to a lower bound on the depth of noisy formulas," in *Proc. IEEE Symp. Foundations of Computer Science*, vol. 34, 1993, pp. 594–603.

[3] ——, "Signal propagation and noisy circuits," *IEEE Trans. Inform. Theory*, vol. 45, pp. 2367–2373, Nov. 1999.

[4] A. S. Holevo, "Bounds for the quantity of information transmitted by a quantum communication channel," *Probl. Inform. Transm.*, vol. 9, pp. 177–183, 1973.

[5] J. von Neumann, "Thermodynamik quantenmechanischer Gesamtheiten," *Gött. Nachr.*, pp. 273–291, 1927.

[6] C. E. Shannon, "A mathematical theory of communication," *Bell Syst. Tech. J.*, vol. 27, pp. 379–423, 623–655, 1948.

Modifications of Patterson–Wiedemann Functions for Cryptographic Applications

Subhamoy Maitra and Palash Sarkar

***Abstract*—Three basic properties of Boolean functions to be useful for cryptographic purposes are balancedness, high algebraic degree, and high nonlinearity. In addition, strict avalanche criteria and propagation characteristics are required for design of S-boxes. In this correspondence, we introduce methods to modify the Patterson–Wiedemann and bent functions to achieve the above cryptographic properties. In the process, we are able to answer some open questions about Boolean functions.**

***Index Terms*—Algebraic degree, balancedness, Boolean function, nonlinearity, propagation characteristics, S-box, strict avalanche criteria.**

I. INTRODUCTION

Boolean functions are used as primitives in the design of block ciphers. Research over the last decade and a half has indicated that a Boolean function must possess certain properties to be suitable for block cipher applications. Perhaps the most important of these properties is nonlinearity, which is the distance of the function from the set of affine functions. This is also an important parameter from the coding theory point of view. It is well known that the maximum possible nonlinearity of an n-variable function is equal to the covering radius of first-order Reed–Muller code $\mathcal{R}(1, n)$. For even values of n, the maximum possible nonlinearity is known and functions achieving this nonlinearity are called bent [12]. For odd values of n, the maximum possible nonlinearity is known only for $n \leq 7$. However, it is possible to obtain high nonlinearity by concatenating two bent functions on $(n-1)$-variables. In an important paper, Patterson and Wiedemann [8] showed that for odd $n \geq 15$, it is possible to construct functions whose nonlinearity is greater than that obtained by concatenating two bent functions. However, for cryptographic purpose it is not sufficient to have only high nonlinearity. Among the other required criteria are balancedness, high algebraic degree, propagation criteria/strict avalanche characteristics. Here we introduce modifications of the Patterson–Wiedemann (PW) functions to achieve the above criteria while retaining nonlinearity higher than the bent concatenation value. The constructed Boolean functions are suited for block cipher applications. Also our results solve the following open problems.

- Seberry, Zhang, and Zheng [14] showed how to use the 15-variable PW functions to construct balanced functions with nonlinearity greater than the bent concatenation value for odd $n \geq 29$. Here we show that the same can be achieved for odd $n \geq 15$. Further, the constructed functions can have maximum algebraic degree $n - 1$. The technique that we employ is completely different from that of [14].
- For the first time we show that for odd $n \geq 15$, it is possible to construct PC (1) functions with nonlinearity greater than the bent concatenation value. Further, this is also true for balanced functions.
- For $k \leq \frac{n}{2} - 1$, we show how to construct balanced SAC (k), n-variable functions with degree $n - k - 1$. The construction of these functions were posed as open problems in [6], [11], [10]. Moreover, the functions we construct have the currently best nonlinearities, and they are obtained by modifying bent and PW functions.

II. PRELIMINARIES

In this section, we introduce a few basic concepts and notations. We denote the addition operator over GF (2) by $\oplus$. The following notations will be used later.

- For binary strings S_1, S_2 of the same length λ, we denote by $\#(S_1 = S_2)$ (respectively, $\#(S_1 \neq S_2)$), the number of places where S_1 and S_2 are equal (respectively, unequal).
- The Hamming distance between S_1, S_2 is denoted by $d(S_1, S_2)$, i.e., $d(S_1, S_2) = \#(S_1 \neq S_2)$.
- Also we define $wd(S_1, S_2) = \#(S_1 = S_2) - \#(S_1 \neq S_2)$. Note that, $wd(S_1, S_2) = \lambda - 2\,d(S_1, S_2)$.
- The Hamming weight or simply the weight of a binary string S is the number of ones in S. This is denoted by $\mathrm{wt}(S)$.
- Given a binary string S, by S^c we denote the string which is the bitwise complement of S.

By Ω_n we mean the set of all Boolean functions of n-variables. A Boolean function f of n-variables maps the elements of $\{0, 1\}^n$ to $\{0, 1\}$. One representation of n-variable Boolean function is by a binary string of length 2^n. Let $\sigma_0, \ldots, \sigma_{2^n-1}$ be an enumeration of the elements of $\{0, 1\}^n$, where σ_i is the n-bit binary representation of i.

Note that the enumeration of $\{0, 1\}^{n+1}$ can be described recursively as follows:

$$\{0, 1\}^1: 0, 1$$
$$\{0, 1\}^{n+1}: 0\sigma_0, \ldots, 0\sigma_{2^n-1}, 1\sigma_0, \ldots, 1\sigma_{2^n-1}. \quad (1)$$

Since a Boolean function f is a map from $\{0, 1\}^n$ to $\{0, 1\}$, it is completely specified by specifying the values of f for the elements σ_i. Thus, f is completely specified by the string

$$f(\sigma_0), \ldots, f(\sigma_{2^n-1}).$$

Conversely, we may consider any binary string of length 2^n to uniquely define a Boolean function with respect to the enumeration of $\{0, 1\}^n$ given above.

The algebraic degree is an important parameter of a Boolean function both from cryptographic and coding-theoretic points of view.

Definition 1: An n-variable Boolean function can be written in the form

$$f(X_n, \ldots, X_1) = a_0 \oplus \left(\bigoplus_{i=1}^{i=n} a_i X_i\right) \oplus \left(\bigoplus_{1\le i\ne j\le n} a_{ij} X_i X_j\right) \oplus \cdots \oplus a_{12\cdots n} X_1 X_2 \cdots X_n$$

where the coefficients $a_0, a_{ij}, \ldots, a_{12\cdots n} \in \{0, 1\}$. This representation of f is called the algebraic normal form (ANF) of f. The number of variables in a highest order product term with nonzero coefficient is called the algebraic degree, or simply degree of f.

For the sake of notational convenience, by f we will denote both the ANF and the string representations of f. The binary string representation of Boolean functions is going to be used in our search algorithms. The most frequently used operation will be the concatenation of two Boolean functions. Hence, we briefly explain this. Let f_0, f_1 be two n-variable functions, represented by bit strings of length 2^n. By $f = f_0 f_1$ we will denote the $(n+1)$-variable function f, defined by

$$f(0\sigma_i) = f_0(\sigma_i)$$
$$f(1\sigma_i) = f_1(\sigma_i). \quad (2)$$

The recursive enumeration in (1) and (2) suggests that the "new" variable X_{n+1} is "placed to the left" of the earlier variables $X_n, \ldots, X_1$. For this reason, we find it advantageous to our intuition to use the notation $f(X_{n+1}, X_n, \ldots, X_1)$ instead of the more usual notation $f(X_1, \ldots, X_n, X_{n+1})$, which is favored by most experts. However, this is a minor point and really depends on how comfortable one feels in thinking about Boolean function.

Algebraically, the concatenation operation corresponds to

$$f(X_{n+1}, X_n, \ldots, X_1) = (1 \oplus X_{n+1}) f_0(X_n, \ldots, X_1) \oplus X_{n+1} f_1(X_n, \ldots, X_1).$$

For a Boolean function f, the notation $\mathrm{wt}(f)$ denotes the number of 1's in the string representation of f. For cryptographic applications, it is usually desirable to use functions whose output column has an equal number of zeros and ones.

Definition 2: An n-variable function f is said to be balanced if its output column in the truth table contains equal number of 0's and 1's (i.e., $\mathrm{wt}(f) = 2^{n-1}$).

Functions of degree at most one are called affine functions. An affine function with the constant term equal to zero is called a linear function. The set of all n-variable affine (respectively, linear) functions is denoted by $A(n)$ (respectively, $L(n)$). The distance of a Boolean function from the set of affine functions is called its nonlinearity.

Definition 3: The nonlinearity of an n-variable function f is

$$\mathrm{nl}(f) = \min_{g\in A(n)} (d(f, g))$$

i.e., the distance of f from the set of all n-variable affine functions.

For even values of n, the maximum possible nonlinearity achievable is known and is equal to $2^{n-1} - 2^{\frac{n-2}{2}}$ [12]. Functions achieving this nonlinearity are called bent. Further, if f is an n-variable bent function and l is any linear function in $L(n)$, then $d(f, l)$ takes one of the values $2^{n-1} \pm 2^{\frac{n-2}{2}}$.

We next define propagation characteristic (PC) and strict avalanche criteria (SAC) which are important properties of Boolean functions to be used in S-boxes.

Definition 4: Let $\overline{X} = (X_n, \ldots, X_1)$ and $\overline{\alpha} \in \{0, 1\}^n$. A function $f \in \Omega_n$ is said to satisfy

1) SAC if $f(\overline{X}) \oplus f(\overline{X} \oplus \overline{\alpha})$ is balanced for any $\overline{\alpha}$ such that $\mathrm{wt}(\overline{\alpha}) = 1$;
2) SAC (k) if any function obtained from f by keeping any k input bits constant satisfies SAC.
3) PC (l) if $f(\overline{X}) \oplus f(\overline{X} \oplus \overline{\alpha})$ is balanced for any $\overline{\alpha}$ such that $1 \le \mathrm{wt}(\overline{\alpha}) \le l$;
4) PC (l) of order k if any function obtained from f by keeping any k input bits constant satisfies PC (l).

SAC was introduced by Webster and Tavares [15] and SAC (k) was introduced by Forré [4]. PC was introduced by Preneel *et al.* [11], [10]. Also Preneel *et al.* introduced the notion of extended propagation characteristics which has later been studied by Carlet [2]. In their original paper, Preneel *et al.* [11], [10] raised several questions on the construction of functions satisfying SAC. These were partially answered by Kurosawa and Satoh [6] who introduced a new construction of Boolean functions satisfying SAC and PC. This construction was later generalized by Carlet [2]. Here we use the original construction of Kurosawa and Satoh [6] along with new ideas to answer some of the questions raised in [11], [10] and not answered in [6]. We next state a few simple results which will be used later.

Proposition 1: Let $f \in \Omega_n$ and $f = f_1 f_2$, where $f_1, f_2 \in \Omega_{n-1}$. Then the algebraic degree of f is n iff $\mathrm{wt}(f)$ is odd. Moreover, if both $\mathrm{wt}(f_1)$ and $\mathrm{wt}(f_2)$ are odd then the algebraic degree of f is $n-1$.

Proposition 2: Given a balanced function $f \in \Omega_n$ with $\mathrm{nl}(f) = x$, one can construct balanced $f' \in \Omega_n$ with $\mathrm{nl}(f') \ge x - 2$ and $\deg(f') = n - 1$.

Proof: Let $f = f_1 f_2$ where $f_1, f_2 \in \Omega_{n-1}$. If $\mathrm{wt}(f_1)$ and $\mathrm{wt}(f_2)$ are both odd, then $\deg(f) = n - 1$ and take $f' = f$. If both $\mathrm{wt}(f_1)$ and $\mathrm{wt}(f_2)$ are even, change any one bit of f_1 from 0 to 1 to get f_1' and any one bit of f_2 from 1 to 0 to get f_2'. Then the function $f' = f_1' f_2'$ is in Ω_n and is balanced. Further, the degree of f' is $n-1$ since the weights of both f_1' and f_2' are odd (see Proposition 1). Also, $\mathrm{nl}(f') \ge \mathrm{nl}(f) - 2$, since the nonlinearity can fall by at most 2 for changing 2 bits. □

Also, we will need the following result which is available in [7].

Proposition 3: For odd $n \ge 3$, it is possible to construct a balanced Boolean function in Ω_n with nonlinearity $2^{n-1} - 2^{\frac{n-1}{2}}$ and algebraic degree $(n-1)$.

For odd $n \ge 15$, we provide a method to obtain higher nonlinearity than Proposition 3. We will only use Proposition 3 for odd n, such that $3 \le n \le 13$.

Next, we state a standard result on nonlinearity (see, for example, [8], [13]).

Proposition 4: Let us consider $h(X_n, \ldots, X_1) \in \Omega_n$ and $g(Y_m, \ldots, Y_1) \in \Omega_m$ with separate sets of input variables. Let

$$f(Y_m, \ldots, Y_1, X_n, \ldots, X_1) = g(Y_m, \ldots, Y_1) \oplus h(X_n, \ldots, X_1).$$

Then $\mathrm{nl}(f) = 2^n \mathrm{nl}(g) + 2^m \mathrm{nl}(h) - 2\,\mathrm{nl}(g)\,\mathrm{nl}(h)$.

III. Nonlinearity of Balanced Functions

For odd n, one easy way to construct n-variable functions with high nonlinearity is to concatenate two bent functions of $(n-1)$-variables. The nonlinearity achieved is equal to $2^{n-1} - 2^{\frac{n-1}{2}}$ and is sometimes called the bent concatenation nonlinearity. It is a notoriously difficult problem to construct n-variable functions with nonlinearity higher than this value. In an important paper, Patterson and Wiedemann [8], [9] have shown how to construct 15-variable functions with nonlinearity 16276 . The achieved nonlinearity is higher than the corresponding bent concatenation nonlinearity of $2^{14} - 2^7 = 16256$. Also, the constructed functions have weight $16492 = 16384 + 108 = 2^{14} + 108$ and hence are not balanced. Patterson and Wiedemann [8] also pointed out how to use these functions to construct n-variable functions with nonlinearity equal to $2^{n-1} - 2^{\frac{n-1}{2}} + 20 \times 2^{\frac{n-15}{2}}$ for all odd $n \geq 15$. The importance of their result lies in the fact that these are the only known direct constructions of functions with nonlinearity greater than the bent concatenation value.

In later work, Seberry, Zhang, and Zheng [14] used PW functions to construct balanced functions with nonlinearity greater than $2^{n-1} - 2^{\frac{n-1}{2}}$ for odd $n \geq 29$. The question of obtaining balanced functions with nonlinearity greater than the bent concatenation value for odd n between 15 and 27 was left open. Also, [14] did not consider the degree of the constructed functions.

In this section, we introduce new ways of modifying the PW functions to achieve balancedness and maximum algebraic degree and still retain nonlinearity higher than the bent concatenation value for all odd $n \geq 15$.

We start by identifying an important result which is the first step in the construction of balanced 15-variable function with nonlinearity greater than 16256.

Proposition 5: It is possible to construct $f \in \Omega_{15}$ with nonlinearity $16276 = 2^{14} - 2^7 + 20$ and weight $16364 = 2^{14} - 20$.

Proof: Consider a PW function $f_1 \in \Omega_{15}$ with $\mathrm{nl}(f_1) = 16276$ and $\mathrm{wt}(f_1) = 16492$. From [9], we know that there are 3255 linear functions in $L(15)$ at a distance 16364 from f_1. Let l be one of these 3255 linear functions. Define $f = f_1 \oplus l$. Then $f \in \Omega_{15}$ and $\mathrm{nl}(f) = \mathrm{nl}(f_1) = 16276$ and $\mathrm{wt}(f) = \mathrm{wt}(f_1 \oplus l) = d(f_1, l) = 16364$. □

Next, we have the following randomized heuristic for constructing highly nonlinear balanced functions for odd $n \geq 15$.

Algorithm 1: RandBal(n)

1. Let f be a function constructed using Proposition 5. Let $n = 2k + 15$, $k \geq 0$ and let $F \in \Omega_n$ be defined as follows.
   - If $k = 0$, take $F = f$.
   - If $k > 0$, take
   $$F = f(X_1, \ldots, X_{15}) \oplus g(X_{16}, \ldots, X_n)$$
   where $g \in \Omega_{2k}$ is a bent function.
   Note that $\mathrm{nl}(F) = 2^{n-1} - 2^{\frac{n-1}{2}} + 20 \times 2^k$ (see Proposition 4) and $\mathrm{wt}(F) = 2^{n-1} - 20 \times 2^k$.
2. Divide the string F in Ω_n into 20×2^k equal contiguous substrings, with the last substring longer than the rest.
3. In each substring choose a position with 0 value uniformly at random and change that to 1. This generates a balanced function $F_b \in \Omega_n$.
4. If $\mathrm{nl}(F_b) > 2^{n-1} - 2^{\frac{n-1}{2}}$, then report. Go to Step 1 and continue.

We have run this experiment a number of times and succeeded in obtaining plenty of balanced functions with nonlinearities $2^{14} - 2^7 + 6$, $2^{16} - 2^8 + 18$, $2^{18} - 2^9 + 46$ and $2^{20} - 2^{10} + 104$, respectively, for 15, 17, 19, and 21 variables.

Remark 1: It is possible to distribute the 0's and 1's in the function in a manner (changing Steps 2 and 3 in Algorithm 1) such that the weights of the upper and lower halves of the function are odd. Using Proposition 1, this provides balanced functions with maximum algebraic degree $(n-1)$ and the same nonlinearity as before.

Note that, running Algorithm 1 for large n is time-consuming. This is because we need to check the nonlinearity which takes $O(n2^n)$ time for an n-variable Boolean function using fast Walsh transform algorithm. However, we can extend the experimental results in a way similar to that in [8]. Consider a bent function $g(Y_1, \ldots, Y_{2k}) \in \Omega_{2k}$ and $f(X_1, \ldots, X_{21})$ with nonlinearity $2^{20} - 2^{10} + 104$ as obtained from Algorithm RandBal(). Let $h \in \Omega_{21+2k}$ such that $h = g \oplus f$. Then, it follows that

$$\mathrm{nl}(h) = 2^{20+2k} - 2^{10+k} + 104 \times 2^k.$$

These functions can be modified to get algebraic degree $(n-1)$ as in Proposition 2. Thus we get the following result.

Theorem 1: One can construct balanced Boolean functions on $n = 15 + 2k$ $(k \geq 0)$ variables with nonlinearity greater than $2^{n-1} - 2^{\frac{n-1}{2}}$. Moreover, such functions can have algebraic degree $(n-1)$.

Dobbertin [3] provided a recursive procedure for modifying a general class of bent functions to obtain highly nonlinear balanced Boolean functions on an even number of variables. A special case of this procedure which modifies the Maiorana–McFarland class of bent functions was earlier described in [14]. For even n, it was conjectured in [3] that the maximum value of nonlinearity of balanced functions, which we denote by $\mathrm{nlbmax}(\,)$, satisfies the recurrence

$$\mathrm{nlbmax}(n) = 2^{n-1} - 2^{\frac{n}{2}} + \mathrm{nlbmax}\left(\frac{n}{2}\right).$$

We next provide a combined interlinked recursive algorithm to construct highly nonlinear balanced functions for both odd and even n. Note that for an even number of variables, Algorithm 2 uses a special case of the recursive construction in [3]. Further, we show how to obtain the maximum algebraic degree. The input to this algorithm is n and the output is balanced $f \in \Omega_n$ with the currently best known nonlinearity.

Algorithm 2: BalConstruct(n)

1. If n is odd
   a) if $3 \leq n \leq 13$ construct f with algebraic degree $(n-1)$ and nonlinearity $2^{n-1} - 2^{\frac{n-1}{2}}$ (see Proposition 3).
   b) if $15 \leq n \leq 21$ return f to be the best function constructed by RandBal(n).
   c) if $n \geq 23$
   i. Let $h_1 \in \Omega_{n-21}$ be bent and $g_1 \in \Omega_{21}$ be the best nonlinear function constructed by RandBal(n). Let $f_1 \in \Omega_n$ be such that $f_1 = h_1 \oplus g_1$.
   ii. Let h_2 = BalConstruct($n-15$) and $g_2 \in \Omega_{15}$ as in Proposition 5. Let $f_2 \in \Omega_n$ be such that $f_2 = h_2 \oplus g_2$.
   iii. If $\mathrm{nl}(f_1) \geq \mathrm{nl}(f_2)$ return f_1 else return f_2.
2. If n is even
   Let h = BalConstruct($\frac{n}{2}$). Let f be the concatenation of h followed by $2^{\frac{n}{2}} - 1$ distinct nonconstant linear functions on $\frac{n}{2}$-variables. Return f.

To obtain maximum algebraic degree in the above algorithm we need the following modifications.

- For odd $n \leq 13$, the functions available from Proposition 3 guarantee degree $(n-1)$.
- For odd n, $15 \leq n \leq 21$, modification of algorithm RandBal() (see Remark 1) guarantees algebraic degree $(n-1)$ without dropping nonlinearity.

- For odd $n \geq 23$, using Proposition 2, degree $(n-1)$ can be achieved sacrificing nonlinearity by at most 2.
- For even n, recursively ensure that algebraic degree of h (in Step 2 of BalConstruct()) is $\frac{n}{2}-1$.

Let $\mathrm{nlb}\,(n)$ be the nonlinearity of an n-variable balanced Boolean function constructed by BalConstruct(n). Similarly, let $\mathrm{nla}\,(n)$ be the nonlinearity of an n-variable balanced function with degree $n-1$, constructed by Algorithm BalConstruct(n). We have the following performance guarantee on $\mathrm{nlb}\,(n)$ and $\mathrm{nla}\,(n)$.

Theorem 2: The Algorithm BalConstruct(n) constructs a balanced n-variable function having nonlinearity $\mathrm{nlb}\,(n)$, given by

$$\begin{aligned}\mathrm{nlb}\,(n) &= 2^{n-1} - 2^{\frac{n-1}{2}}, \qquad \text{for odd } n,\ 3 \leq n \leq 13 \quad (1)\\ &= \sigma_{15}+6,\ \sigma_{17}+18,\ \sigma_{19}+46,\ \sigma_{21}+104,\\ &\qquad\qquad \text{for } n = 15,\ 17,\ 19,\ 21 \quad (2)\\ &= \max(A,\ B), \qquad \text{for odd } n \geq 23 \quad (3)\\ &= 2^{n-1} - 2^{\frac{n}{2}} + \mathrm{nlb}\left(\frac{n}{2}\right), \quad \text{for even } n \quad (4)\end{aligned}$$

where $\sigma_n = 2^{n-1} - 2^{\frac{n-1}{2}}$

$$\begin{aligned}A &= 2^{n-1} - 2^{\frac{n-1}{2}} - 88 \times 2^k + 216 \times \mathrm{nlb}\,(k)\\ B &= 2^{n-1} - 2^{\frac{n-1}{2}} + 13 \times 2^k\end{aligned}$$

and $k = \frac{n-15}{2}$. For cases (1) and (2), $\mathrm{nla}\,(n) = \mathrm{nlb}\,(n)$. For case (3), $\mathrm{nla}\,(n) \geq \mathrm{nlb}\,(n) - 2$, and for case (4), $\mathrm{nla}\,(n) = 2^{n-1} - 2^{\frac{n}{2}} + \mathrm{nla}\,(\frac{n}{2})$.

It should be noted that, from Theorem 2, for even n, the nonlinearity measures $\mathrm{nla}\,(\,)$ and $\mathrm{nlb}\,(\,)$ satisfy the same recurrence of $\mathrm{nlbmax}(\,)$ as conjectured by Dobbertin [3]. Algorithm BalConstruct(n) provides currently best known nonlinear balanced functions for all n. In particular, we summarize the following points to highlight the performance of the algorithm.

1) Our method provides balanced functions with nonlinearity greater than $2^{n-1} - 2^{\frac{n-1}{2}}$ for odd n, $15 \leq n \leq 27$ which were not known earlier.
2) For even n, the nonlinearity obtained by our method is strictly greater than that mentioned in [14, Theorem 13] for all $n = 2^s(2t+1)$, $s \geq 1$, $t \geq 7$.
3) For odd n, the nonlinearity obtained by our method is strictly greater than that mentioned in [14] for all $n = 2^s(2t+1)+15$, $s \geq 1$, $t \geq 7$.
4) Apart from points 2) and 3) above, compared to [14] we also obtain strictly better nonlinearities for certain other values of n (for example, $n = 29,\ 31$).

In this section we have shown how to heuristically modify the PW functions to obtain balancedness while retaining nonlinearity higher than the bent concatenation value. However, the question of mathematically constructing such functions remains open. Also settling the conjecture in [3] is an important unsolved question.

IV. Autocorrelation Function

The autocorrelation function $C_f(\overline{\alpha})$ of a Boolean function f is defined as

$$C_f(\overline{\alpha}) = \sum_{\overline{X} \in \{0,\,1\}^n} (-1)^{f(\overline{X}) \oplus f(\overline{X} \oplus \overline{\alpha})}.$$

It is easy to see that the autocorrelation value at $\overline{0}$, i.e., $C_f(\overline{0})$, is equal to 2^n. Hence, in the following, we will only consider the values of the autocorrelation function at nonzero points. First we present the autocorrelation values for the 15-variable PW functions. It is interesting to note that these values are the same for both the functions in [9].

No. of $\overline{\alpha}$	3255	6727	9765	3255	3255	6510
$C_{f_1}(\overline{\alpha})$	160	64	0	-32	-64	-96

In [16], two measures were introduced based on the autocorrelation function and these were called the global avalanche characteristics. Here, we consider only the absolute indicator Δ_f, which is defined as

$$\Delta_f = \max_{\overline{\alpha} \neq 0} |C_f(\overline{\alpha})|.$$

In [16, Sec. 4], it has been conjectured that for $n = 2k+1$, the absolute indicator Δ_f for any n-variable balanced function f is greater than 2^{k+1}.

From the preceding table, the absolute indicator for the 15-variable PW functions is 160. We have also computed the absolute indicator for the balanced modifications of the PW functions. The minimum value obtained is 216 and in this case the autocorrelation function takes 54 distinct values, i.e., all the multiples of 8 between -216 and 216. Since 216 is less than $2^{7+1} = 256$, the conjecture of [16] is disproved for $n = 15$.

V. Propagation Characteristics

Here we use the PW functions for the construction of functions satisfying propagation characteristics.

Theorem 3: For odd $n \geq 15$, it is possible to construct n-variable, PC (1) functions with nonlinearity $2^{n-1} - 2^{\frac{n-1}{2}} + 20 \times 2^{\frac{n-15}{2}}$.

Proof: Let $\overline{X} = (X_n, \ldots, X_1)$ and $\overline{\alpha} \in \{0,\,1\}^n$. Let

$$S_f = \{\overline{\alpha} | f(\overline{X}) \oplus f(\overline{X} \oplus \overline{\alpha}) \text{ is balanced}\}.$$

The 15-variable PW functions have the property that there are 15 linearly independent vectors in S_f. Consider B_f to be a 15×15 nonsingular matrix whose rows are the following 15 linearly independent vectors. For each of these vectors $\overline{\alpha}$, we have $C_f(\overline{\alpha}) = 0$. The matrix B_f is as follows:

$$\begin{bmatrix}
0&0&0&0&0&0&0&0&0&0&1&1&0&0&0\\
0&0&0&0&0&0&0&0&0&1&0&0&0&0&0\\
0&0&0&0&0&0&0&0&1&0&0&1&0&0&0\\
0&0&0&0&0&0&0&1&0&0&0&1&0&0&0\\
0&0&0&0&0&0&1&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&1&0&1&0&0&0&0&0&0\\
0&0&0&0&0&1&0&0&0&0&0&0&0&0&0\\
0&0&0&0&1&0&0&0&0&0&0&0&0&0&0\\
0&0&0&1&0&0&0&0&0&0&0&0&0&0&1\\
0&0&0&1&0&0&0&0&1&0&0&0&0&0&0\\
0&0&1&0&0&0&0&0&0&1&0&0&0&0&0\\
0&1&0&0&0&0&0&0&0&0&0&0&1&0&0\\
1&0&0&0&0&0&0&0&0&0&0&1&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&1&0\\
0&0&0&0&0&0&0&0&0&0&0&0&1&0&0
\end{bmatrix}$$

Define $g(\overline{X}) = f(\overline{X}B_f)$. Then, g has the same nonlinearity as f and satisfies PC (1). We proceed inductively for odd numbers of input vari-

ables $n > 15$. Let $g(X_{n-2}, \ldots, X_1)$ be an $(n-2)$-variable, PC (1) function with nonlinearity $2^{n-3} - 2^{\frac{n-3}{2}} + 20 \times 2^{\frac{n-17}{2}}$. Let

$$h(X_n, X_{n-1}) = X_n X_{n-1}$$

be a two-variable bent function whose output column is of the form 0001. Define

$$G(X_n, X_{n-1}, X_{n-2}, \ldots, X_1) = h(X_n, X_{n-1}) \oplus g(X_{n-2}, \ldots, X_1).$$

Thus, G can be seen as a concatenation of the form $gggg^c$. Once again note that g^c is the bitwise complement of g. Take any n-length binary vector $\overline{\alpha} = (\alpha_n, \alpha_{n-1}, \ldots, \alpha_1)$ with $\mathrm{wt}(\overline{\alpha}) = 1$. Also, let

$$\overline{X} = (X_n, X_{n-1}, \ldots, X_1)$$

and

$$\overline{X}' = (X_{n-2}, \ldots, X_1).$$

Now three cases arise.

Case 1) $\overline{\alpha} = (\alpha_n = 0, \alpha_{n-1} = 0, \alpha_{n-2} \ldots, \alpha_1)$: Let $\overline{\alpha}' = (\alpha_{n-2}, \ldots, \alpha_1)$. Note that $\mathrm{wt}(\overline{\alpha}') = 1$. Thus,

$$\begin{aligned}\mathrm{wt}(G(\overline{X}) \oplus G(\overline{X} \oplus \overline{\alpha})) &= \mathrm{wt}(g(\overline{X}') \oplus g(\overline{X}' \oplus \overline{\alpha}')) \\ &\quad + \mathrm{wt}(g(\overline{X}') \oplus g(\overline{X}' \oplus \overline{\alpha}')) \\ &\quad + \mathrm{wt}(g(\overline{X}') \oplus g(\overline{X}' \oplus \overline{\alpha}')) \\ &\quad + \mathrm{wt}(g^c(\overline{X}') \oplus g^c(\overline{X}' \oplus \overline{\alpha}')) \\ &= 4 \times 2^{n-3} \text{ (from the induction hypothesis as } g \text{ is PC}(1)) \\ &= 2^{n-1}.\end{aligned}$$

Case 2) $\overline{\alpha} = (\alpha_n = 0, \alpha_{n-1} = 1, \ldots, \alpha_1 = 0)$: In this case

$$\begin{aligned}\mathrm{wt}(G(\overline{X}) \oplus G(\overline{X} \oplus \overline{\alpha})) &= \mathrm{wt}(g \oplus g) + \mathrm{wt}(g \oplus g) \\ &\quad + \mathrm{wt}(g \oplus g^c) + \mathrm{wt}(g^c \oplus g) \\ &= 2^{n-1}.\end{aligned}$$

Case 3) $\overline{\alpha} = (\alpha_n = 1, \alpha_{n-1} = 0, \ldots, \alpha_1 = 0)$: Again

$$\begin{aligned}\mathrm{wt}(G(\overline{X}) \oplus G(\overline{X} \oplus \overline{\alpha})) &= \mathrm{wt}(g \oplus g) + \mathrm{wt}(g \oplus g^c) \\ &\quad + \mathrm{wt}(g \oplus g) + \mathrm{wt}(g^c \oplus g) \\ &= 2^{n-1}.\end{aligned}$$

Hence, G is PC (1) and since $G = h \oplus g$, we get

$$\mathrm{nl}(G) = 2^{n-1} - 2^{\frac{n-1}{2}} + 20 \times 2^{\frac{n-15}{2}}. \qquad \square$$

A similar result can be proved on the nonlinearity of balanced PC(1) functions.

Theorem 4: For odd $n \geq 15$, it is possible to construct n-variable, balanced PC (1) functions with nonlinearity $2^{n-1} - 2^{\frac{n-1}{2}} + 6 \times 2^{\frac{n-15}{2}}$.

Proof: The proof is similar to the proof of Theorem 3. We start with a balanced 15-variable function with nonlinearity $2^{14} - 2^7 + 6$ as obtained by modifying a PW function using the randomized heuristic. As in Theorem 3, we obtain a 15×15 matrix B_f such that for each row α of B_f, the autocorrelation function at α is 0. The construction is similar to Theorem 3. $\square$

Our next results are based on a general construction of Boolean functions introduced by Kurosawa and Satoh [6]. The construction is

$$f(X_1, \ldots, X_s, Y_1, \ldots, Y_t) = [X_1, \ldots, X_s] Q [Y_1, \ldots, Y_t]^T \oplus g(X_1, \ldots, X_s)$$

where Q is an $s \times t$ binary matrix and $g(X_1, \ldots, X_s)$ is any function. Under certain conditions on Q, the function f satisfies PC (l) of order k (see [6]). Moreover, according to the proof of [6, Theorem 16], $\mathrm{nl}(f) = 2^t \mathrm{nl}(g)$ and $\deg(f) = \deg(g)$. It is possible to improve the results of [6] by using functions constructed by the methods of Section III.

Theorem 5: For odd s, it is possible to construct PC (l) of order k function f such that

a) $\deg(f) = s-1$ and $\mathrm{nl}(f) \geq 2^{t+s-1} - 2^{t+\frac{s-1}{2}}$ for $3 \leq s \leq 13$;
b) $\deg(f) = s$ and $\mathrm{nl}(f) > 2^{t+s-1} - 2^{t+\frac{s-1}{2}}$ for $s \geq 15$.

Proof: For $3 \leq s \leq 13$, s odd, we can consider $g \in \Omega_s$ as the function available from Proposition 3 with algebraic degree $s-1$ and nonlinearity $2^{s-1} - 2^{\frac{s-1}{2}}$. For $s \geq 15$, one can consider $g \in \Omega_s$ with nonlinearity $2^{s-1} - 2^{\frac{s-1}{2}} + 20 \times 2^{\frac{s-15}{2}} - 1$ and algebraic degree s. This can be obtained by considering a function on s variables with maximum known nonlinearity and then making $\mathrm{wt}(g)$ odd by complementing one bit. This will provide the full algebraic degree and decrease the nonlinearity by at most 1. $\square$

For odd s, the corresponding result in [6] is $\deg(f) = \frac{s-1}{2}$ and $\mathrm{nl}(f) \geq 2^{t+s-1} - 2^{t+\frac{s-1}{2}}$ which is clearly improved in Theorem 5.

Further, maximum algebraic degree can be obtained in this construction at the cost of small drop in nonlinearity. For odd s between 3 and 13, $\deg(g)$ can be made s by changing one bit of g. This decreases $\mathrm{nl}(g)$ by one. The corresponding parameters of f are $\deg(f) = s$ and $\mathrm{nl}(f) \geq 2^{t+s-1} - 2^{t+\frac{s-1}{2}} - 2^t$. For even s, the result in [6] is $\deg(f) = \frac{s}{2}$ and $\mathrm{nl}(f) \geq 2^{t+s-1} - 2^{t+\frac{s}{2}-1}$. As before, by changing one bit of g we can ensure $\deg(f) = s$ and $\mathrm{nl}(f) \geq 2^{t+s-1} - 2^{t+\frac{s}{2}-1} - 2^t$.

A Boolean function f is said to be resilient if it is balanced and for any variable X_i, the function $X_i \oplus f$ is also balanced (see [5] for a more general definition of resiliency). Resiliency is an important property of a Boolean function to be used in stream cipher systems. We present an interesting result combining resiliency and propagation characteristics.

Theorem 6: For even n, it is possible to construct resilient functions in Ω_n, with nonlinearity $2^{n-1} - 2^{\frac{n}{2}}$, algebraic degree $\frac{n}{2} - 1$, and satisfying PC$(\frac{n}{2} - 1)$.

Proof: Let $f \in \Omega_{n-2}$ be a bent function, n even. Then

$$F(X_1, \ldots, X_{n-1}) = (1 \oplus X_{n-1}) f(X_1, \ldots, X_{n-2}) \oplus X_{n-1}(1 \oplus f(X_1 \oplus \alpha_1, \ldots, X_{n-2} \oplus \alpha_{n-2}))$$

is balanced and satisfies propagation criterion with respect to all nonzero vectors except $(\alpha_1, \ldots, \alpha_{n-2}, 1)$. Also $\mathrm{nl}(F) = 2^{n-2} - 2^{\frac{n-2}{2}}$.

Let

$$G(X_1, \ldots, X_n) = (1 \oplus X_n) F(X_1, \ldots, X_{n-1}) \oplus X_n (F(X_1 \oplus \beta_1, \ldots, X_{n-1} \oplus \beta_{n-1})).$$

Then G is balanced and satisfies the propagation criterion with respect to all nonzero vectors except

$$\overline{\alpha} = (\alpha_1, \ldots, \alpha_{n-2}, \alpha_{n-1} = 1, \alpha_n = 0)$$

and

$$\overline{\beta} = (\beta_1, \ldots, \beta_{n-1}, \beta_n = 1)$$

and $\overline{\alpha} \oplus \overline{\beta}$. Also G is balanced and $\mathrm{nl}(G) = 2^{n-1} - 2^{\frac{n}{2}}$.

Choose $(\alpha_1, \alpha_2, \ldots, \alpha_{n-2})$ with $\mathrm{wt}(\alpha_1, \alpha_2, \ldots, \alpha_{n-2}) = \frac{n}{2} - 1$. Now consider

$$\overline{\alpha} = (\alpha_1, \ldots, \alpha_{n-2}, \alpha_{n-1} = 1, \alpha_n = 0)$$
$$\overline{\beta} = (\beta_1 = 1, \ldots, \beta_{n-1} = 1, \beta_n = 1).$$

Since $\mathrm{wt}\,(\overline{\alpha}) = \frac{n}{2} - 1 + 1$ and $\mathrm{wt}\,(\overline{\beta}) = n$ we get, $\mathrm{wt}\,(\overline{\alpha} \oplus \overline{\beta}) = \frac{n}{2}$. Note that G satisfies the propagation criterion with respect to all the nonzero vectors except $\overline{\alpha}$, $\overline{\beta}$, $\overline{\alpha} \oplus \overline{\beta}$ and hence G satisfies PC $(\frac{n}{2} - 1)$.

Note that since we choose

$$(\beta_1 = 1, \ldots, \beta_{n-1} = 1)$$

$G(X_1, \ldots, X_n)$ is 1-resilient [1], [7].

Since $f \in \Omega_{n-2}$ is bent, it is possible to construct f with algebraic degree $\frac{n}{2} - 1$ and $\deg(G) = \deg(f)$. □

VI. Strict Avalanche Criteria

Next we turn to the study of SAC (k) combined with the properties of balancedness, degree and nonlinearity. In [6], the construction

$$f(X_1, \ldots, X_s, Y_1, \ldots, Y_t) = [X_1, \ldots, X_s]Q[Y_1, \ldots, Y_t]^T \oplus g(X_1, \ldots, X_s)$$

has been used for the construction of SAC (k) function by setting $s = n - k - 1, t = k + 1$, and Q to be the $(n - k - 1) \times (k + 1)$ matrix whose elements are all 1. Under these conditions, the function f takes the form

$$f(X_1, \ldots, X_n) = (X_1 \oplus \cdots \oplus X_{n-k-1})(X_{n-k} \oplus \cdots \oplus X_n) \oplus g(X_1, \ldots, X_{n-k-1}).$$

Moreover, it was shown that f is balanced if

$$\left|\{\overline{X} | g(\overline{X}) = 0, \overline{X}Q = \overline{0}\}\right| = \left|\{\overline{X} \,|g(\overline{X}) = 1, \overline{X}Q = \overline{0}\}\right|$$

where $\overline{X} = (X_1, \ldots, X_{n-k-1})$. It is important to interpret this idea with respect to the truth table of g. Since all entries of Q are ones, the vector $\overline{X}Q$ is either the all-zero or the all-one vector. Further, it is the all-zero vector iff $\mathrm{wt}\,(\overline{X})$ is even. This means that f is balanced if

$$\#\{\overline{X} | g(\overline{X}) = 0, \mathrm{wt}\,(\overline{X}) = \text{even}\} = \#\{\overline{X} | g(\overline{X}) = 1, \mathrm{wt}\,(\overline{X}) = \text{even}\}.$$

Thus, in the truth table we have to check for balancedness of g restricted to the rows where the weight of the input string is even. In half of such places g must be 0 and in the other half g must be 1. Motivated by this discussion we make the following definition of *brEven* (restricted balancedness with respect to inputs with even weight) and *brOdd* (restricted balancedness with respect to inputs with odd weight).

Definition 5: Let $g \in \Omega_p$ and $\overline{X} = (X_1, \ldots, X_p)$. Then g is called brEven (respectively brOdd) if $\#\{g(\overline{X}) = 0 | \mathrm{wt}\,(\overline{X}) = \text{even}\} = \#\{g(\overline{X}) = 1 | \mathrm{wt}\,(\overline{X}) = \text{even}\} = 2^{p-2}$ (respectively, $\#\{g(\overline{X}) = 0 | \mathrm{wt}\,(\overline{X}) = \text{odd}\} = \#\{g(\overline{X}) = 1 | \mathrm{wt}\,(\overline{X}) = \text{odd}\} = 2^{p-2}$).

We show that PW functions can be modified to make them brEven. This in turn provides balanced n-variable, SAC (k) functions with degree $n - k - 1$ and very high nonlinearity. The construction of such functions were posed as open problems in [11], [10].

Proposition 6: For p odd, it is possible to construct $g \in \Omega_p$ with nonlinearity i) $2^{p-1} - 2^{\frac{p-1}{2}}$ for $p \leq 13$ and ii) $2^{p-1} - 2^{\frac{p-1}{2}} + 20 \times 2^{\frac{p-15}{2}}$ for $p \geq 15$ which is brEven.

Proof: First note that if any function $f(\overline{X})$ is brEven, then $f(\overline{X} \oplus \overline{\alpha})$ is brOdd whenever $\mathrm{wt}\,(\overline{\alpha})$ is odd and *vice versa*. Also, $\mathrm{nl}\,(f(\overline{X})) = \mathrm{nl}\,(f(\overline{X} \oplus \overline{\alpha}))$.

For odd $p \leq 13$, choose $f_3 \in \Omega_{p-1}$, a brEven bent function, as given in Proposition 7 (see later). Then construct $f_2 \in \Omega_{p-1}$, such that $f_2 = f_3(\overline{X} \oplus \overline{\alpha})$ where $\mathrm{wt}\,(\overline{\alpha})$ is odd. Thus, f_2 is a brOdd function. Now construct a function $F \in \Omega_p$, where F is concatenation of f_3 and f_2, i.e., $F = (1 \oplus X_p)f_3 \oplus X_p f_2$. Then F is brEven and $\mathrm{nl}\,(F) = 2^{p-1} - 2^{\frac{p-1}{2}}$.

For $p \geq 15$, we use a recursive construction. Let $f_1 \in \Omega_{15}$ be a 15-variable PW function. Note that $\mathrm{nl}\,(f_1) = 2^{14} - 2^7 + 20$. Now consider the 32 768 functions of the form $f_1 \oplus l$, where $l \in L(15)$. We have found functions among these which are brOdd (but none of which are brEven). Let $f_2(X_1, \ldots, X_{15})$ be such a brOdd function. Then $f_3(X_1, \ldots, X_{15}) = f_2(X_1 \oplus \alpha_1, \ldots, X_{15} \oplus \alpha_{15})$ is brEven when $\mathrm{wt}\,(\alpha_1, \ldots, \alpha_{15})$ is odd. Note that $\mathrm{nl}\,(f_2) = \mathrm{nl}\,(f_3) = \mathrm{nl}\,(f_1)$. This settles the base case.

Consider that for all odd p, $15 \leq p \leq m$, (m odd), there exists a brEven function $f \in \Omega_p$ with

$$\mathrm{nl}\,(f) = 2^{p-1} - 2^{\frac{p-1}{2}} + 20 \times 2^{\frac{p-15}{2}}.$$

Let us take $f_3 \in \Omega_m$ be a brEven function with

$$\mathrm{nl}\,(f_3) = 2^{m-1} - 2^{\frac{m-1}{2}} + 20 \times 2^{\frac{m-15}{2}}.$$

Then we can construct brOdd function

$$f_2(X_1, \ldots, X_m) = f_3(X_1 \oplus \alpha_1, \ldots, X_p \oplus \alpha_m)$$

where $\mathrm{wt}\,(\alpha_1, \ldots, \alpha_m)$ is odd. Construct $F \in \Omega_{m+2}$ where $F = f_3 f_2 f_2 f_3^c$. Then it can be shown that F is also brEven. Now, any linear function on $(m + 2)$ variables is of one of the following forms $llll$, $ll^c l^c$, $lll^c l^c$, $ll^c l^c l$, for some $l \in L(m)$. Thus, considering the distance of $F = f_3 f_2 f_2 f_3^c$ to the linear functions of the above forms, it is possible to show

$$\mathrm{nl}\,(F) = 2^{m+2-1} - 2^{\frac{m+2-1}{2}} + 20 \times 2^{\frac{m+2-15}{2}}.$$

This proves the inductive step. □

The construction in the above theorem can also be seen in the following way. Consider a brOdd function f_2 and a brEven function f_3 on 15 variables with $\mathrm{nl}\,(f_2) = \mathrm{nl}\,(f_3) = 2^{14} - 2^7 + 20 \times 2^0$. Now we show the construction of a brEven function on $15 + 2k$ variables. Let $g(Y_1, \ldots, Y_{2k})$ be a bent function on $2k$ variables. Define $F \in \Omega_{15+2k}$ as follows:

$$F = (Y_1 \oplus \cdots \oplus Y_{2k})(g \oplus f_2) \oplus (1 \oplus Y_1 \oplus \cdots \oplus Y_{2k})(g \oplus f_3).$$

Then F is brEven and $\mathrm{nl}\,(F) = 2^{14+2k} - 2^{7+k} + 20 \times 2^k$.

Theorem 7: Let $(n - k - 1) \geq (k + 1)$, i.e., $k \leq \frac{n}{2} - 1$ and $n - k - 1 =$ odd. Then it is possible to construct balanced SAC (k) function $f \in \Omega_n$ such that $\deg(f) = n - k - 1$. Moreover, for $3 \leq n - k - 1 \leq 13$

$$\mathrm{nl}(f) = 2^{n-1} - 2^{\frac{n+k}{2}} - 2^{k+1}$$

and for $n - k - 1 \geq 15$

$$\mathrm{nl}\,(f) = 2^{n-1} - 2^{\frac{n+k}{2}} + 20 \times 2^{\frac{n+k-14}{2}} - 2^{k+1}.$$

Proof: We start with an $(n - k - 1)$-variable brEven function g constructed using Proposition 6. Note that $\mathrm{wt}\,(g)$ is even. Choose an input $\overline{\alpha} = (\alpha_{n-k-1}, \ldots, \alpha_1)$ of g such that $\mathrm{wt}\,(\overline{\alpha})$ is odd. Construct a function g' as follows:

$$g'(\overline{X}) = g(\overline{X}), \quad \text{if } \overline{X} \neq \overline{\alpha},$$
$$= g(\overline{X}) \oplus 1, \quad \text{if } \overline{X} = \overline{\alpha}.$$

Clearly, $\mathrm{wt}\,(g') = \mathrm{wt}\,(g) \pm 1 =$ odd and hence, using Proposition 3, the degree of g' is odd. Since $\mathrm{wt}\,(\overline{\alpha})$ is odd the function g' retains the brEven property. The nonlinearity of g' is exactly one less than the nonlinearity of g. We use this g' in the construction [6]

$$f(X_1, \ldots, X_s, Y_1, \ldots, Y_t) = [X_1, \ldots, X_s]Q[Y_1, \ldots, Y_t]^T \oplus g(X_1, \ldots, X_s)$$

to get the desired results. □

The next result is important as it shows that certain types of bent functions can be brEven. This allows us to obtain balanced n-variable,

SAC (k) functions with degree $n-k-1$ and very high nonlinearity which could not be obtained in [6].

Proposition 7: For p even, it is possible to construct bent functions $g \in \Omega_p$ which are brEven.

Proof: First note that g is brEven iff g^c is brEven. Let $q = \frac{p}{2}$. For $0 \le i \le q-1$, let $l_i \in L(q)$ be the linear function $a_q X_q \oplus \cdots \oplus a_1 X_1$, where $a_q \cdots a_1$ is the q-bit binary expansion of i. We provide construction of bent functions $g(X_1, \ldots, X_p)$ which are brEven. Let $\overline{X} = (X_1, \ldots, X_p)$.

Case 1: $q \equiv 1 \bmod 2$. Let $g = l_0 f_1 \cdots f_{q-2} l_{q-1}$, where

$$f_1, \ldots, f_{q-2} \in \{l_1, \ldots, l_{q-2}, l_1^c \ldots, l_{q-2}^c\}$$

and for $i \neq j$, $f_i \neq f_j$ and $f_i \neq f_j^c$. It is well known that such a g is bent [12]. We require the following three results whose proofs are straightforward though a bit tedious.

a) $\#\{l_0(X_1, \ldots, X_q) = 0 | \mathrm{wt}(X_1, \ldots, X_q) = \text{even}\} = 2^{q-1}$ and $\#\{l_0(X_1, \ldots, X_q) = 1 | \mathrm{wt}(X_1, \ldots, X_q) = \text{even}\} = 0$.

b) Since the f_i's are degenerate affine functions in $L(q)$, it is possible to show that individually they are both brEven and brOdd.

c) Using the fact that q is odd and $l_{q-1} = X_1 \oplus \cdots \oplus X_q$, it is possible to show

$$\#\{l_{q-1}(X_1, \ldots, X_q) = 0 | \mathrm{wt}(X_1, \ldots, X_q) = \text{even}\} = 0$$

and

$$\#\{l_{q-1}(X_1, \ldots, X_q) = 1 | \mathrm{wt}(X_1, \ldots, X_q) = \text{even}\} = 2^{q-1}.$$

As $\mathrm{wt}(X_1, \ldots, X_p) = \mathrm{wt}(X_1, \ldots, X_q) + \mathrm{wt}(X_{q+1}, \ldots, X_p)$ and g is the concatenation of $l_0, f_1, \ldots, f_{q-2}, l_{q-1}$, it is possible to show that g is brEven.

Case 2: For $q \equiv 0 \bmod 2$, the result is true for bent functions of the form $g = l_0^c f_1 \ldots f_{q-2} l_{q-1}$. □

In [6, Theorem 32], it has been stated that for even $n-k-1$, there exists balanced SAC (k) functions such that $\deg(f) = n-k-2$. The question whether such functions with algebraic degree $n-k-1$ exists has been left as an open question. The next result shows the existence of such functions which proves that the bound on algebraic degree provided in [11] is indeed tight for $k \le \frac{n}{2} - 1$.

Theorem 8: Let $(n-k-1) \ge (k+1)$, i.e., $k \le \frac{n}{2} - 1$ and $n-k-1 =$ even. Then it is possible to construct balanced SAC (k) function $f \in \Omega_n$ such that $\deg(f) = n-k-1$. Moreover, $\mathrm{nl}(f) = 2^{n-1} - 2^{\frac{n+k-1}{2}} - 2^{k+1}$.

Proof: Use a bent function $g \in \Omega_{n-k-1}$ which is brEven. Out of the 2^{n-k-1} bit positions in g (in the output column of the truth table), there are 2^{n-k-2} positions where $wt(X_1, \ldots, X_{n-k-1}) =$ odd and the value of g at these positions can be complemented without disturbing the brEven property. Since g is bent, $\mathrm{wt}(g)$ is even. Thus, we choose a row j in the truth table where $\mathrm{wt}(X_1, \ldots, X_{n-k-1})$ is odd and construct g' by complementing the output bit. Thus, $\mathrm{wt}(g') = \mathrm{wt}(g) \pm 1 =$ odd. Hence by Proposition 3, $\deg(g') = n-k-1$. Thus,

$$f(X_1, \ldots, X_n) = (X_1 \oplus \cdots \oplus X_{n-k-1})(X_{n-k} \oplus \cdots \oplus X_n) \oplus g'(X_1, \ldots, X_{n-k-1})$$

is balanced SAC (k) with algebraic degree $n-k-1$. Also,

$$\mathrm{nl}(g') = \mathrm{nl}(g) - 1 = 2^{n-k-2} - 2^{\frac{n-k-1}{2}-1} - 1$$

Thus,

$$\mathrm{nl}(f) = 2^{k+1} \times \mathrm{nl}(g') = 2^{n-1} - 2^{\frac{n+k-1}{2}} - 2^{k+1} \qquad \square$$

VII. Conclusion

In this correspondence, we have shown how to modify the famous PW functions to make them balanced and still retain nonlinearity higher than the bent concatenation value. Also, the modified n-variable functions can have the maximum algebraic degree $(n-1)$. Further, we have used a different type of modification of PW and bent functions along with a construction by Kurosawa and Satoh to construct functions satisfying SAC and PC which were not known earlier.

References

[1] P. Camion, C. Carlet, P. Charpin, and N. Sendrier, "On correlation immune functions," in *Advances in Cryptology—CRYPTO'91 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 1992, pp. 86–100.

[2] C. Carlet, "On cryptographic propagation criteria for Boolean functions," *Inform. Comput.*, vol. 151, pp. 32–56, 1999.

[3] H. Dobbertin, "Construction of bent functions and balanced Boolean functions with high nonlinearity," in *Fast Software Encryption (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 1994, vol. 1008, pp. 61–74.

[4] R. Forré, "The strict avalanche criterion: Spectral properties of Boolean functions and an extended definition," in *Advances in Cryptology—CRYPTO'88 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 1990, pp. 450–468.

[5] X. Guo-Zhen and J. Massey, "A spectral characterization of correlation immune combining functions," *IEEE Trans. Inform. Theory*, vol. 34, pp. 569–571, May 1988.

[6] K. Kurosawa and T. Satoh, "Design of SAC/PC(l) of order k Boolean functions and three other cryptographic criteria," in *Advances in Cryptology—EUROCRYPT'97 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 1997, pp. 434–449.

[7] S. Maitra and P. Sarkar, "Cryptographically significant Boolean functions with five valued Walsh spectra," *Theor. Comput. Sci.*, 2002, to be published.

[8] N. J. Patterson and D. H. Wiedemann, "The covering radius of the $(2^{15}, 16)$ Reed–Muller code is at least 16276," *IEEE Trans. Inform. Theory*, vol. IT-29, pp. 354–356, May 1983.

[9] ——, "Correction to—The covering radius of the $(2^{15}, 16)$ Reed–Muller code is at least 16276," *IEEE Trans. Inform. Theory*, vol. 36, p. 443, Mar. 1990.

[10] B. Preneel, R. Govaerts, and J. Vandewalle, "Boolean functions satisfying higher order propagation criteria," in *Advances in Cryptology—EUROCRYPT'91 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 1991, pp. 141–152.

[11] B. Preneel, W. Van Leekwijck, L. Van Linden, R. Govaerts, and J. Vandewalle, "Propagation characteristics of Boolean functions," in *Advances in Cryptology—EUROCRYPT'90 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 1991, pp. 161–173.

[12] O. S. Rothaus, "On bent functions," *J. Combin. Theory*, ser. A, vol. 20, pp. 300–305, 1976.

[13] P. Sarkar and S. Maitra, "Construction of nonlinear Boolean functions with important cryptographic properties," in *Advances in Cryptology—EUROCRYPT 2000 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 2000, vol. 1807, pp. 485–506.

[14] J. Seberry, X. M. Zhang, and Y. Zheng, "Nonlinearly balanced Boolean functions and their propagation characteristics," in *Advances in Cryptology—CRYPTO'93 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 1994, pp. 49–60.

[15] A. F. Webster and S. E. Tavares, "On the design of S-boxes," in *Advances in Cryptology—CRYPTO'85 (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 1986, pp. 523–534.

[16] X. M. Zhang and Y. Zheng, "GAC—The criterion for global avalanche characteristics of cryptographic functions," *J. Universal Comput. Sci.*, vol. 1, no. 5, pp. 316–333, 1995.