Evolving Boolean Functions Satisfying Multiple Criteria

John A. Clark[1], Jeremy L. Jacob[1], Susan Stepney[1],
Subhamoy Maitra[2], and William Millan[3]

[1] Department of Computer Science, University of York
York YO10 3EE, England
{jac,jeremy,susan.stepney}@cs.york.ac.uk
[2] Applied Statistics Unit, Indian Statistical Institute
203 B T Road, Calcutta 700 108, India
subho@isical.ac.in
[3] Information Security Research Center
Queensland University of Technology
GPO Box 2434, Brisbane, Queensland, Australia 4001
b.millan@qut.edu.au

Abstract. Many desirable properties have been identified for Boolean functions with cryptographic applications. Obtaining optimal tradeoffs among such properties is hard. In this paper we show how simulated annealing, a search technique inspired by the cooling processes of molten metals, can be used to derive functions with profiles of cryptographically-relevant properties as yet unachieved by any other technique.

Keywords: Heuristic Optimisation, Boolean Functions, Nonlinearity, Autocorrelation, Correlation Immunity.

1 Introduction

A variety of desirable criteria for functions with cryptographic application have been identified: balancedness, high nonlinearity, correlation immunity of reasonably high order, low autocorrelation, high algebraic degree etc. The tradeoffs between these criteria have received a lot of attention in Boolean function literature for some time (see [12] and the references therein). The more criteria that have to be taken into account, the more difficult it is to generate Boolean functions satisfying those properties purely by constructive algebraic means. Indeed, recent work has sought to blend construction with aspects of computer search. Many of the best functions on small numbers of variables (7–10) have been obtained in this way [12, 19, 16].

Some authors have attempted to use *guided* search techniques to evolve Boolean functions [13, 14, 15, 3]. Although such efforts have shown promise, they have not rivalled the best of alternative methods. In this paper, using modifications of the simulated annealing based in [3] we demonstrate how to evolve various functions with profiles of desirable properties unachieved by other means.

A. Menezes, P. Sarkar (Eds.): INDOCRYPT 2002, LNCS 2551, pp. 246–259, 2002.
© Springer-Verlag Berlin Heidelberg 2002

We shall also show how the capabilities of search-based techniques can be enhanced using well-established cryptology theory (and change of basis in particular). First, we provide the technical definitions needed to understand this paper together with a description of the simulated annealing algorithm used.

2 Preliminaries

Boolean Functions. This section provides definitions concerning Boolean functions with cryptographic application. We denote the binary truth table of a Boolean function by $f : Z_2^n \rightarrow Z_2$ mapping each combination of n binary values to some binary value. If the number of combinations mapping to 0 is the same as the number mapping to 1 then the function is said to be *balanced*.

The *polarity truth table* is a particularly useful representation for our purposes. It is defined by $\hat{f}(x) = (-1)^{f(x)}$. Two functions f and g are said to be uncorrelated when $\sum_{x \in Z_2^n} \hat{f}(x)\hat{g}(x) = 0$. If so, if one tries to approximate f by using g, he/she will be right half the time and wrong half the time. An area of particular importance for cryptanalysts is the ability to approximate a function f by a simple linear function. One of the cryptosystem designer's tasks is to make such approximation as difficult as possible (by making the function f suitably *nonlinear*). We make use of the following terms (these and further definitions can be found in [2] and [25]).

Linear Boolean Function. A linear Boolean function, determined by $\omega \in Z_2^n$, is denoted by $L_\omega(x) = \omega_1 x_1 \oplus \omega_2 x_2 \cdots \oplus \omega_n x_n$, where $w_i x_i$ denotes the bitwise AND of the i-th bits of ω and x, and $\oplus$ denotes bitwise XOR.

Affine Function. The set of affine functions is the set of linear functions and their complements $A_{\omega,c}(x) = L_\omega(x) \oplus c$, where $c \in Z_2$.

Walsh Hadamard Transform. For a function f, the Walsh Hadamard Transform $\hat{F}_f$ is defined by $\hat{F}_f(\omega) = \sum_{x \in Z_2^n} \hat{f}(x)\hat{L}_\omega(x)$. We denote the maximum absolute value by $WH_{max}(f) = \max_{\omega \in Z_2^n} \left| \hat{F}_f(\omega) \right|$. It is related to the nonlinearity of f.

Nonlinearity. The nonlinearity N_f of a Boolean function f is its minimum distance to any affine function. It is given by $N_f = \frac{1}{2}(2^n - WH_{max}(f))$.

Parseval's Theorem. This states that $\sum_{\omega \in Z_2^n} (\hat{F}_f(\omega))^2 = 2^{2n}$. A consequence of this result is that $WH_{max}(f) \geq 2^{\frac{n}{2}}$. This fact forms the starting point for the principal cost functions in this paper.

Autocorrelation Transform. The autocorrelation transform of a function f is given by $\hat{r}_f(s) = \sum_x \hat{f}(x)\hat{f}(x \oplus s)$. We denote the maximum absolute value in the autocorrelation spectra of a function f by AC_f, i.e., $AC_f = \max_s \left| \sum_x \hat{f}(x)\hat{f}(x \oplus s) \right|$. Here x and s range over Z_2^n and so produces a result in Z_2^n.

Simulated Annealing. In 1983 Kirkpatrick et al. [8] proposed *simulated annealing*, a new search technique inspired by the cooling processes of molten metals. It merges hill-climbing with the probabilistic acceptance of non-improving moves. The basic algorithm is shown in Figure 1. The search starts at some initial state $S = S_0$. There is a control parameter T known as the temperature. This starts 'high' at T_0 and is gradually lowered. At each temperature, a number MIL (Moves in Inner Loop) of moves to new states are attempted. A candidate state Y is randomly selected from the neighborhood $N(S)$ of the current state. The change in value, δ, of f is calculated. If it improves the value of $f(S)$ (i.e., if $\delta < 0$ for a minimisation problem) then a move to that state is taken is taken ($S = Y$); if not, then it is taken with some probability. The worse a move is, the less likely it is to be accepted. The lower the temperature T, the less likely is a worsening move to be accepted. Probabilistic acceptance is determined by generating a random value U in the range (0..1) and performing the indicated comparison. Initially the temperature is high and virtually any move is accepted. As the temperature is lowered it becomes ever more difficult to accept worsening moves. Eventually, only improving moves are allowed and the process becomes 'frozen'. The algorithm terminates when the stopping criterion is met. Common stopping criteria, and the ones used for the work in this paper, are to stop the search after a fixed number $MaxIL$ of inner loops have been executed, or else when some maximum number MUL of consecutive unproductive inner loops have been executed (i.e., without a single move having been accepted). Generally the best state achieved so far is also recorded (since the search may actually move out of it and subsequently be unable to find a state of similar quality). At the end of each inner loop the temperature is lowered. The simplest way of lowering the temperature is to multiply by a constant cooling factor α in the range (0..1); this is known as *geometric cooling*. The basic simulated annealing algorithm has proven remarkably effective over a range of problems.

```
$S = S_0$
$T = T_0$
Repeat
{
        for(int $i = 0$; $i < MIL$; $i++$)
        {
                Select $Y \in N(S)$
                $\delta = f(Y) - f(S)$
                if ($\delta < 0$) then
                        $S = Y$
                else
                        Generate $U = U(0,1)$
                        if ($U < \exp(-\delta/T)$) then $S = Y$
        }
        $T = T \times \alpha$
}
Until stopping criterion is met
```

Fig. 1. Basic Simulated Annealing for Minimisation Problems

3 Nonlinearity, Autocorrelation and Algebraic Degree

3.1 Cost Functions and General Approach

We aim to derive excellent Boolean functions via optimisation of some cost function. The cost function used here is motivated by Parseval's theorem and the characteristics of Bent functions. Bent functions have maximal nonlinearity and zero autocoreation. For Bent functions $\hat{F}_f(\omega) = 2^{\frac{n}{2}}$ for all ω. For balanced Boolean functions this ideal bound cannot be achieved but it does suggest that a cost function that seeks to minimise the spread of the Walsh Handamard values is well-motivated. Accordingly a cost function of the following form is used:

$$cost(\hat{f}) = \sum_{\omega \in Z_2^n} \left| \left| \hat{F}_f(\omega) \right| - X \right|^R \tag{1}$$

The value R is positive and can be varied. In the experiments reported here we have mostly used $R = 3$. Values of X ranging from -16 to 30 have been used. (This was to investigate the effects of parametric variation. Here we present only summary results. Further results can be found in [4]).

A balanced function is represented using polar form, i.e., as a vector $\hat{f}$ in R^{2^n} with 2^{n-1} elements equal to 1 and 2^{n-1} elements equal to -1. A search starts with a balanced (but otherwise random) function in polar form. A valid move simply swaps two dissimilar vector elements and so preserves balance — the (equal) numbers of 1s and -1s are maintained. The approach is as follows:

1. Use an annealing-based search to minimise the value of the new cost function (suitably parametrised) given in Equation (1). Let the best solution produced during the search be f_{sa}.
2. Hill-climb from f_{sa} with respect to nonlinearity or autocorrelation (we shall term these the Non-Linearity Targeted (NLT)and Auto-Correlation Targeted (ACT) approaches respectively) to produce the final solution f_{sahc}
3. Measure the nonlinearity, autocorrelation and algebraic degree of f_{sahc}.

3.2 Experimental Results

A variety of runs have been carried out. Our interest is primarily in demonstrating the *profiles* of properties of the functions generated by the NCT and ACT methods. The best profiles are recorded in Table 1. (Further information on nonlinearity and autocorrelation in isolation is given in Tables 2 and 3.) The quadruplet entry (n, d, nl, ac) indicates that the technique was able to evolve a function on n inputs with algebraic degree d, nonlinearity nl and autocorrelation ac.

For n less than or equal to 7 the technique has generated functions with the highest achievable nonlinearity values (often within a few seconds). For $n = 8$ no function with nonlinearity of 118 has ever been demonstrated. The evolution of functions with profile $(8, 5, 112, 16)$ is of particular interest. The autocorrelation value of 16 is lower than the best achieved previously (and indeed lower

Table 1. Best Values (n , d , nl , ac) Obtained Using NLT (upper) and ACT (lower)

(5,3,12,8)	(6,5,26,16)	(7,6,56,16)	(8,7,116,24)
(5,4,12,16)			(8,5,112,16)
(9,8,238,40)	(10,9,486,72)	(11,9,984,96)	(12,10,1992,156)
	(10,9, 484, 64)	(11,10,982, 96)	(12,10,1990,144)
(5,3,12,8)	(6,5,26,16)	(7,6,56,16)	(8,7,116,24)
(5,4,12,16)			(8,5,112,16)
(9,8,238,40)	(10,9,484,56)	(11,10,982,88)	(12,11,1986,128)

Table 2. Comparing the Nonlinearity of Balanced Functions

	5	6	7	8	9	10	11	12
Lowest Upper Bound	12	26	56	118	244	494	1000	2014
Best Known Example [17, 7]	12	26	56	116	240	492	992	2010
Dobertin's Conjecture [5]		26		116		492		2010
Bent Concatenation	12	24	56	112	240	480	992	1984
Random	-	-	-	112	230	472	962	1954
Random Plus Hill-Climb	-	-	-	114	236	476	968	1960
Genetic Algorithms [14]	12	26	56	116	236	484	980	1976
NLT	12	26	56	116	238	486	984	1992
ACT	12	26	56	116	238	484	982	1986

Table 3. Conjectured Bounds and Attained Values for Autocorrelation of Balanced Functions

	5	6	7	8	9	10	11	12
Zhang and Zheng	8	16	16	24	32	48	64	96
Maitra Construction [10]	8	16	16	24	32	40	64	80
Maitra Conjecture [10]		16		24		40		80
NLT	8	16	16	16	40	64	96	144
ACT	8	16	16	16	40	56	88	128

Table 4. Sum of Squares Bounds and Results using Equation (2). 100 Runs. Annealing parameters of $\alpha = 0.95$, $MIL = 200$, $MaxIL = 400$ and $MUL = 50$

n	Son et al.	GAC-σ_f	Annealing + Hill-climbing			Average
	Bound	Bound	Minimum	Average	Maximum	Time (secs)
5	1280	2048	1664	1664	1664	0.4
6	4608	7168	6784	6784	6784	1.2
7	17408	32768	23936	24550.4	24704	1.25
8	67584	90112	86656	89931.5	101248	2.9
9	266240	524288	379904	389273.6	404864	13.5
10	1056768	1245184	1535488	1550272	1566592	137

than a recently conjectured bound). Table 3 summarises autocorrelation results. For $n = 5, 6, 7$ and 8 the autocorrelation must be bounded below by 8. Despite extensive computation, AC values of 8 have eluded discovery for $n = 6, 7$ and 8. Many functions found by the searches have best achieved values for nonlinearity, autocorrelation and algebraic degree simultaneously. (Note: for $n = 5$, the profiles shown have been found to be optimal by exhaustive search, i.e., $(5, 4, 12, 8)$ is unattainable.)

Zhang and Zheng [25] offered two Global Avalanche Criteria (GAC). One was what we have termed autocorrelation above; the other was the sum-of-squares measure σ_f (which treats all autocorrelation transform values $\hat{r}(s)$ equally):

$$\sigma_f = \sum_{s=0}^{2^n-1} \hat{r}^2(s) \tag{2}$$

Zhang and Zheng also offered constructions for even and odd n and claimed that the resulting sums of squares were optimal for balanced functions. This is in fact not the case. The authors have used simulated annealing with the sum-of-squares given in Equation (2) as a cost function to obtain functions with lower values. For 5–10 input variables 100 runs of the annealing algorithm were carried out followed by hill-climbing (with the same cost function). The results are given in Table 4. Lower bounds on GAC sum-of-squares values have recently been derived by Son *et al.* and are also shown in Table 4. Zhang and Zheng's conjectured bounds have frequently and easily been exceeded, often within a few seconds (running on a 1.4 GHz Pentium PC).

The GAC sum-of-squares of functions derived by NLT and ACT methods earlier have also been measured. Some functions had sums-of-squares as low as the minima generated by the direct experiments in this section. Additionally, for $n = 9$ a function with sum-of-squares value of 376832 had been generated and for $n = 10$ one with value 1534720 had been produced. Each is lower than the results obtained by the direct use of sum-of-squares as a cost function (shown in Table 4). This suggests that the cost function given in Equation (1) is capable of generating very special functions indeed. As it happens, there are more surprises in store, as we show below.

4 Constructing Correlation Immune Functions

The relationship between the criteria balancedness, correlation immunity, nonlinearity and algebraic degree is now known [20, 19, 1, 24, 21]. At this point, by (n, m, d, x) function we denote an n-variable, m-resilient function with degree d and nonlinearity x following the notation in [19]. It is now clear that the nonlinearity and algebraic degree of such functions are maximised simultaneously and for balanced mth order correlation immune functions, the maximum algebraic degree is $n-m-1$ [20]. Let us now clarify the exact upper bounds on nonlinearity of resilient Boolean functions. In particular we consider $(n, m, n-m-1, x)$ functions. We use the term $nlmax(n)$ to denote the maximum nonlinearity of an n-variable Boolean function. It is known that for n even, $nlmax(n) = 2^{n-1} - 2^{\frac{n}{2}-1}$

Table 5. Upper Bounds on Achievable Properties (n, m, d, nl)

(5, 1, 3, 12)	(5, 2, 2, 8)	(5, 3, 1, 0)		
(6, 1, 4, 24)	(6, 2, 3, 24)	(6, 3, 2, 16)	(6, 4, 1, 0)	
(7, 1, 5, 56)	(7, 2, 4, 56)	(7, 3, 3, 48)	(7, 4, 2, 32)	(7, 5, 1, 0)
(8, 1, 6, 116)	(8, 2, 5, 112)	(8, 3, 4, 112)	(8, 4, 3, 96)	(8, 5, 2, 64)
(9, 1, 7, 244)*	(9, 2, 6, 240)*	(9, 3, 5, 240)*	(9, 4, 4, 224)	(9, 5, 3, 192)
(10, 1, 8, 492)*	(10, 2, 7, 488)*	(10, 3, 6, 480)	(10, 4, 5, 480)	(10, 5, 4, 448)

(bent functions). However, the problem remains open for odd n. It is clear that the bent functions cannot be correlation immune. For the n odd case, to write the upper bound on nonlinearity of resilient functions, we assume here that the functions attaining the maximum possible nonlinearity $nlmax(n)$ may have the correlation immunity property.

1. If n is even, and $m > \frac{n}{2} - 2$, then $x \leq 2^{n-1} - 2^{m+1}$.
2. If n is even, and $m \leq \frac{n}{2} - 2$, then $x \leq 2^{n-1} - 2^{\frac{n}{2}-1} - 2^{m+1}$.
3. If n is odd, and $nlmax(n) \geq 2^{n-1} - 2^{m+1}$, then $x \leq 2^{n-1} - 2^{m+1}$.
4. If n is odd, and $nlmax(n) < 2^{n-1} - 2^{m+1}$, then x is the highest multiple of 2^{m+1} which is $\leq nlmax(n)$.

Table 5 provides the best theoretical bounds known for optimal tradeoffs for balanced functions and is formed using information in [19, 21, 12, 16, 22, 23]. The mark '*' in the Table 5 highlights that the indicated bound has not yet been demonstrated by any method. Examples of $(7, 2, 4, 56)$ functions [16] and $(8, 1, 6, 116)$ functions [12] were found only very recently using search techniques which need considerable combinatorial argument to reduce the search space.

4.1 Motivation and Method – The First Pass

In [14] a genetic algorithm was used to derive correlation immune balanced functions with high nonlinearity. A cost function influenced by the notions of deviation from [14] but which draws more on the experience of the previous section is

$$cost(f) = \sum_{|\omega| \leq m} |\hat{F}_f(\omega)|^R + A \ \times \max_{\omega} |\hat{F}_f(\omega)|. \qquad (3)$$

Here A is a weighting constant for the nonlinearity component. This enables correlation immunity and nonlinearity to be taken into account. For correlation immunity, the values of all relevant $|\hat{F}_f(\omega)|$ rather than just the most extreme value are considered. The search will be restricted to balanced functions and so $\hat{F}_f(0) = 0$. Algebraic degree is ignored during the search; its value is simply recorded for the final function obtained.

Experiments were carried out for 5–10 input variables. The parameter of A in Equation (3) was 10 (except for the searches for (7,2,4,56) where a value of 100 proved successful). The parameter R varied from 2.0 to 3.0. The cooling parameter α was in the range 0.95–0.99. MIL was in the range 400–2000 and MUL was in the range 50–200. In heuristic search experimentation with cost function and annealing function parameters is pretty much universal.

Table 6 records the best values attained. The values marked with an asterisk are known to be suboptimal (from Table 5). The symbol $\Longleftarrow$ indicates that direct attempts failed but the values have been inherited from a higher order success (e.g., the technique successfully evolved a (9,5,3,192) function and since any $CI(5)$ function is also $CI(4)$, a (9,4,3,192) function has been demonstrated too.)

Table 6. Best Results (n, m, d, nl) obtained by the Direct Method

(5, 1, 3, 12)	(5, 2, 2, 8)			
(6, 1, 4, 24)	(6, 2, 3, 24)	(6, 3, 2, 16)		
(7, 1, 5, 52)*	(7, 2, 4, 56)	(7, 3, 3, 48)	(7, 4, 2, 32)	
(8, 1, 6, 112)*	(8, 2, 5, 112)	(8, 3, 3, 96, 256)*	(8, 4, 3, 96)	(8, 5, 2, 64)
(9, 1, 7, 232)*	(9, 2, 6, 232)	$\Longleftarrow$*	$\Longleftarrow$*	(9,5,3,192)
(10, 1, 8, 476)*				

The direct technique would appear to have achieved a fair amount of success. In addition it has proved capable of deriving a (7,2,4,56) (demonstrated only very recently citex2000-Pasalic-Maitra-Johansson-Sarkar).

4.2 Change of Basis

We now revisit the functions generated previously by the NLT and ACT approaches and investigate whether they can be transformed under change of basis to give first order correlation immune functions. This technique has previously been used by Maitra and Pasalic [12]. Consider functions f on n input variables. Now consider the set of Walsh zeroes

$$WZ_f = \{\omega : \hat{F}_f(\omega) = 0\} \tag{4}$$

If there exist n linearly independent vectors in WZ_f, then one can construct a nonsingular $n \times n$ matrix B_f whose rows are linearly independent vectors from WZ_f. Let $C_f = B_f^{-1}$. Now if we construct a function $f'(x) = f(C_f x)$, then both f', f *have the same nonlinearity and algebraic degree*. Moreover, $\hat{F}_{f'}(\omega) = 0$ for $wt(\omega) = 1$, where $\hat{F}_{f'}$ is the Walsh Hadamard transform of f'. This ensures that f' is 1st order correlation immune. Also if f is balanced then f' is balanced.

In Section 3, we have considered optimization both in terms of nonlinearity and autocorrelation values. Now we consider these functions obtain correlation immune functions of order 1 using linear transformation. Using this technique we get the functions (5, 1, 3, 12, 8), (6, 1, 4, 24, 16), (7, 1, 5, 56, 16), (8, 1, 6, 116, 24), (9, 1, 7, 236, 40), (10, 1, 8, 484, 64), (11, 1, 9, 984, 96) and (12, 1, 10, 1992, 160). Here we consider the function parameters in the form (n, m, d, nl, AC_f). The value of the parameter X in Equation 1 may have significant effect. For example, for $n = 8$ and $X = -14$, 82 out of 100 runs produced functions with Walsh zeroes of rank 8. With $X = 0$ none were produced. The reader is referred to [4] for details. Here we present only summary results.

Comparison to Previous Works for 1st Order Correlation Immunity Note that the function $(5, 1, 3, 12, 8)$ has been reported in [11]. The $(6, 1, 4, 24)$ and $(7, 1, 5, 56)$ functions have been reported in [18]. However, the construction proposed in [18] has not considered the AC_f value. A construction by Maitra [18] provides $(6, 1, 4, 24, 64)$ and $(7, 1, 5, 56, 64)$ functions in comparison to $(6, 1, 4, 24, 16)$ and $(7, 1, 5, 56, 16)$ functions in our method. We have also used an $(8, 0, 6, 116, 24)$ function with the support

$$a53a20176ca6cbd897f5a8743035cda47fc5ace26bc8ef4e4030ad66929c0ebb$$

and transform it to get $(8, 1, 6, 116, 24)$ function with the following support :

$$c7d185111af4adfdc36666da964280f9c93ab2558d28cd621fd63a0b6a8fb531$$

This function has much better autocorrelation property than the $(8, 1, 6, 116, 80)$ function described in [12].

In [12], (10, 1, 8, 488, 320) function has been constructed and (10, 1, 8, 484, 192) function has been constructed in [18]. The autocorrelation values have not been reported in the respective papers, which we check here. In our method, the (10, 1, 8, 484, 64) function has been found using linear transformation from a (10, 0, 8, 484, 64) function.

Table 7. Best Achieved Properties (n, m, d, nl, AC_f) by Any Optimisation Method

(5,1,3,12,8)	(5,2,2,8,32)	(5,3,1,0,32)		
(6,1,4,24,16)	(6,2,3,24,32)	(6,3,2,16,64)	(6,4,1,0,64)	
(7,1,5,56,16)	(7,2,4,56,24)	(7,3,3,48,128)	(7,4,2,32,128)	(7,5,1,0,128)
(8,1,6,116,24)	(8,2,5,112,56)	(8,3,3,96,256)	(8,4,3,96,256)	(8,5,2,64,256)
(9,1,7,236,40)	(9,2,6,232,88)	(9,3,3,192,512)	(9,4,3,192,512)	(9,5,3,192,512)
(10,1,8,484,64)				
(11,1,9,984,96)				
(12,1,10,1992,160)				

4.3 Transformation for Higher Order Correlation Immunity

Linear change of basis has proved to be an effective way of transforming functions to obtain first order correlation immunity. Can a similar transformation be found to produce higher order correlation immunity? Once again consider set of Walsh zeroes WZ_f (defined in Equation 4). Consider there exists a subset SWZ_f of WZ_f with the following property. For any k elements $\omega_{i_1}, \dots, \omega_{i_k}$, $1 \leq k \leq m$,

$$\hat{F}_f(\bigoplus_{j=1}^{k} \omega_{i_j}) = 0.$$

Now construct a nonsingular $n \times n$ matrix B_f whose rows are vectors from SWZ_f. Let, $C_f = B_f^{-1}$. Now if we construct a function $f'(x) = f(C_f x)$, then both f', f *have the same nonlinearity and algebraic degree*. Moreover, $\hat{F}_{f'}(\omega) = 0$ for $1 \leq wt(\omega) \leq m$, where $\hat{F}_{f'}$ is the Walsh Hadamard transform of f'. This ensures that f' is mth order correlation immune. Also if f is balanced then f' is balanced.

Obtaining a linearly independent subset is an easily solvable problem of linear algebra (start with an empty set and add to the set only vectors that increase the dimension of the space spanned). There would appear to be no known *efficient* method for obtaining a basis with the indicated mth order characteristics. The problem is hard but is of relevance. It can also be couched as a nonlinear search problem. Let

$$pwz = \langle \omega_1, \dots, \omega_r \rangle \tag{5}$$

be a permutation of the Walsh zeroes WZ_f. For each such permutation, let the first n elements form a candidate basis. Thus,

$$candBasis(pwz) = \{\omega_1, \dots, \omega_n\}. \tag{6}$$

To be a suitable basis the set $\{\omega_1, \dots, \omega_n\}$ must have rank n and the kth order combinations $\bigoplus_{j=1}^{k} \omega_{i_j}$ of its elements ($1 \leq k \leq m$) must also be in the set WZ_f. A permutation not meeting these requirements should be punished. As example, for $m = 2$, for a candidate basis *candBasis*(*pwz*) define the number of misses as the number of xor combinations of two dissimilar candidate basis elements that are themselves not in WZ_f.

$$misses(candBasis(pwz)) = \#\{i, j : 1..n \cdot i < j \wedge w_i \oplus w_j \notin WZ_f\} \tag{7}$$

A cost function that seeks to punish deviation from required properties is given by:

$$cost(pwz) = K * (n - rank(candBasis(pwz))) + misses(candBasis(pwz)) \tag{8}$$

In attempting to obtain (7, 2, 4, 56) functions the authors also obtained many which were (7, 0, 4, 56) but for which the Walsh zeroes had rank seven. With $K = 20$, this cost function was used as part of an annealing search over the sets of Walsh zeroes with dimension 7. Of 23 such functions the annealing-based search for bases giving second order immunity was successful in the case of 4 of these functions. A search for second order characteristics usually takes less than a minute in comparison to half an hour reported in [16].

4.4 Linear Transformation for Propagation Characteristics

For a Boolean function f consider $ACZ_f = \{s \mid \hat{r}_f(s) = 0\}$. Suppose that there are n linearly independent vectors in ACZ_f. Consider B_f to be a $n \times n$ matrix whose rows are the n linearly independent vectors. Thus, it is clear that $f(xB_f)$ has the same nonlinearity and algebraic degree as $f(x)$ and satisfies PC(1).

The (8,0,6,116,24) function can similarly be transformed to the $PC(1)$ balanced function.

$$9215f91fa524ff81ab12337e5b7d328dbba8c1b2e02419689e6cf8e1372742c5$$

Obtaining higher order properties using this directed search method is novel. We also use the same technique as in Subsection 4.3 to search for a linear change of basis giving rise to $PC(2)$ functions. In the same way as before, if all pairwise combinations $w_i \oplus w_j$ from the basis subset are also in ACZ_f then the function transformed function is $PC(2)$. Very little experimentation has been carried out but this has already provided new information. Prior to 1997 the highest algebraic degree exhibited for a $PC(2)$ function was $\frac{n}{2}$ (for bent functions, which are actually $PC(n)$ — they have zero autocorrelation). Honda et al. [6] showed how this bound was very weak and demonstrated how to construct functions on $n = l + 2^l - 1$ input bits with algebraic degree $n - l - 1$ and showed also how to construct similar balanced functions. They noted that the degree of their constructed functions is 'much larger than the best degree so far'. This is true. They also comment

> Now suppose $f(x_1, \ldots, x_n)$ satisfies $PC(2)$. Then since f satisfies SAC [Strict Avalanche Criterion] we obtain a trivial upper bound on $deg(f)$ such that $deg(f) \leq n - 1$.

We revisited the batches of functions generated in Section 3.2. For functions of six input variables, application of annealing based searches for second order characteristics enabled balanced $PC(2)$ functions of algebraic degree 5 to be found. No balanced $PC(2)$ function has previously been demonstrated at the trivial bound of $n - 1$ (balanced functions can have degree at most $n - 1$). An example function obtained is given below

$$c65b4d405ceb91f1.$$

For low numbers of input variables optimisation is able to generate examples with optimal properties that have hitherto escaped theoretical construction. Honda et al. make no claim to optimality, merely that the previous best bound can be surpassed. Whether or not $PC(2)$ functions exist with degree $n - 1$ for $n > 6$ is left as an open question (though preliminary experimentation has come very close — for $n = 7$ and 8 change of bases have been found that give rise to $PC(1)$ functions with only a single element $w_i \oplus w_j$ not being in the set of AC zeroes). Thorough investigation of the application of the optimisation techniques to propagation characteristics (and other propagation criteria) is left as future work. The generation of a single example meeting the 'trivial' bound shows once again that optimisation techniques have some potential to check conjectures or to attack current bounds for relationships between the various criteria.

Table 8. Supports for Functions with CI and PI Together

n	PC(k)CI(m)	Support	NL	AC
6	PC(1)CI(1)	6CB405778EA9BD30	24	32
6	PC(1)CI(2)	5C721BCAAC27B1C5	16	64
7	PC(1)CI(1)	3BD8254D458FB41D	52	32
		CDA8F192662334FA		
8	PC(1)CI(1)	54FFAAC5467F9703B1AC48E3C016DB82	112	48
		98621FE54A386A60163247E1F7C7BD8D		

4.5 CI and PC Together

Optimisation-based approaches can easily be extended to incorporate multiple criteria. Correlation immunity CI(m) and propagation criteria PC(k) can be targeted together using a cost function of the form:

$$\mathit{cost}(f) = A \times \sum_{1 \leq |s| \leq k} |\hat{r}_f(s)|^R + B \times \sum_{|\omega| \leq m} |\hat{F}_f(\omega)|^R + C \times \max_{\omega} |\hat{F}_f(\omega)|. \quad (9)$$

At present only small scale experiments have been performed but these have already produced interesting results. Table 8 records the support of some functions evolved so far.

5 Conclusions

Using heuristic approaches we have attained functions with profiles unattained by other techniques. The range of properties addressed shows that heuristic search is a flexible framework for Boolean function investigation. The change of basis transformations show that a little theory can complement heuristic approaches to good effect. Adopting further elements of cryptological theory into the search process may prove a fruitful avenue for future research. Heuristic search is little exploited in modern-day cryptology. We encourage other researchers to consider it.

References

[1] C. Carlet. On the coset weight divisibility and nonlinearity of resilient and correlation immune functions. In *Sequences and Their Applications - SETA 2001*, Discrete Mathematics and Theoretical Computer Science, pages 131–144. Springer Verlag, 2001. 251

[2] C. Ding, G. Xiao, and W. Shan. *The Stability of Stream Ciphers*, Lecture Notes in Computer Science, Volume 561. Springer-Verlag, 1991. 247

[3] J. A. Clark and J. L. Jacob. Two-Stage Optimisation in the Design of Boolean Functions. In *5th Australasian Conference on Information, Security and Privacy – ACISP 2000*, Lecture Notes in Computer Science, Volume 1841, pages 242–254. Springer-Verlag, 2000. 246

[4] J. A. Clark. Metaheuristic Search as a Cryptological Tool. DPhil Thesis. YCST-2002-07. Deptartment of Computer Science. University of York, York UK. December 2001. Available at http://www.cs.york.ac.uk/ftpdir/reports/ 249, 254

[5] H. Dobbertin. Construction of bent functions and balanced functions with high nonlinearity. In *Fast Software Encryption, 1994 Leuven Workshop*, Lecture Notes in Computer Science, Volume 1008, pages 61–74, Berlin, 1994. Springer-Verlag. 250

[6] T. Honda, T. Satoh, T. Iwata and K. Kurosawa. Balanced Boolean functions satisfying pc(2) and very large degree. Selected Areas in Cryptography (SAC) 1997. Available from http://adonis.ee.queensu.ca:8000/sac/sac97/papers.html 256

[7] X.-D. Hou. On the Norm and Covering Radius of First-Order Reed-Muller Codes. *IEEE Transactions on Information Theory*, 43(3):1025–1027, May 1997. 250

[8] S. Kirkpatrick, Jr. C. D. Gelatt, and M. P. Vecchi. Optimization by simulated annealing. *Science*, 220(4598):671–680, May 1983. 247

[9] S. Maitra and P. Sarkar. Modifications of Patterson-Wiedemann functions for cryptographic applications. *IEEE Transactions on Information Theory*, 48(1):278–284, January 2002.

[10] S. Maitra. Highly nonlinear balanced Boolean functions with very good autocorrelation property. In *Workshop on Coding and Cryptography - WCC 2001*, Paris, January 8–12, 2001. Electronic Notes in Discrete Mathematics, Volume 6, Elsevier Science, 2001. 250

[11] S. Maitra. Autocorrelation properties of correlation immune Boolean functions. INDOCRYPT 2001, Lecture Notes in Computer Science Volume 2247, pages 242–253. Springer Verlag, December 2001. 254

[12] S. Maitra and E. Pasalic. Further constructions of resilient Boolean functions with very high nonlinearity. *IEEE Transactions on Information Theory*, 48(7):1825–1834, July 2002. 246, 252, 253, 254

[13] W. Millan, A. Clark and E. Dawson. An effective genetic algorithm for finding highly nonlinear Boolean functions. In *First International Conference on Information and Communications Security*, Lecture Notes in Computer Science, Volume 1334, pages 149–158. Springer Verlag, 1997. 246

[14] W. Millan, A. Clark and E. Dawson. Heuristic Design of Cryptographically Strong Balanced Boolean Functions. In *Advances in Cryptology EUROCRYPT'98*, Lecture Notes in Computer Science, Volume 1403, pages 489–499. Springer Verlag. 1998. 246, 250, 252

[15] W. Millan, A. Clark and E. Dawson. Boolean function design using hill climbing methods. In *4th Australasian Conference on Information, Security and Privacy*, Lecture Notes in Computer Science, Volume 1587, pages 1–11. Springer Verlag, April 1999. 246

[16] E. Pasalic, S. Maitra, T. Johansson and P. Sarkar. New constructions of resilient and correlation immune Boolean functions achieving upper bound on nonlinearity. In *Workshop on Coding and Cryptography - WCC 2001*, Paris, January 8–12, 2001. Electronic Notes in Discrete Mathematics, Volume 6, Elsevier Science, 2001. 246, 252, 255

[17] N. J. Patterson and D. H. Wiedemann. The covering radius of the $(2^{15}, 16)$ Reed-Muller code is at least 16276. *IEEE Transactions on Information Theory*, IT-29(3):354–356, 1983 (see correction IT-36(2):443, 1990). 250

[18] 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, Volume 1807, pages 485–506. Springer Verlag, May 2000. 254

[19] P. Sarkar and S. Maitra. Nonlinearity bounds and constuction of resilient Boolean functions. In Mihir Bellare, editor, *Advances in Cryptology - Crypto 2000*, Lecture Notes in Computer Science, Volume 1880, pages 515–532, Berlin, 2000. Springer-Verlag. 246, 251, 252

[20] T. Siegenthaler. Correlation immunity of nonlinear combining functions for cryptographic applications. *IEEE Transactions on Information Theory*, IT-30(5):776–780, September 1984. 251

[21] Y. Tarannikov. On resilient Boolean fnctions with maximal possible nonlinearity. In *Progress in Cryptology - INDOCRYPT 2000*, Lecture Notes in Computer Science, Volume 1977, pages 19–30. Springer Verlag, 2000. 251, 252

[22] Y. V. Tarannikov. New constructions of resilient Boolean functions with maximal nonlinearity. In *Fast Software Encryption - FSE 2001*, Lecture Notes in Computer Science, Volume 2355, pages 70–81. Springer Verlag, 2001. 252

[23] M. Fedorova and Y. V. Tarannikov. On the constructing of highly nonlinear resilient Boolean functions by means of special matrices. In *Progress in Cryptology - INDOCRYPT 2001*, Lecture Notes in Computer Science, Volume 2247, pages 254–266. Springer Verlag, 2001. 252

[24] Y. Zheng and X. M. Zhang. Improved upper bound on the nonlinearity of high order correlation immune functions. In *Selected Areas in Cryptography - SAC 2000*, Lecture Notes in Computer Science, Volume 2012, pages 264–274. Springer Verlag, 2000. 251

[25] X-M. Zhang and Y. Zheng. GAC – the criterion for global avalanche characteristics of cryptographic functions. *Journal of Universal Computer Science*, 1(5):316–333, 1995. 247, 251