Aperiodic Propagation Criteria for Boolean Functions

Lars Eirik Danielsen, T. Aaron Gulliver, and Matthew G. Parker

Abstract

We characterise aperiodic autocorrelation for a boolean function, f, and define the *Aperiodic Propagation Criteria* (APC) of degree l and order q. We establish the strong similarity between APC and *Extended Propagation Criteria* (EPC) of degree l and order q as defined by Preneel et al. in 1991, although the criteria are not identical. We also show how aperiodic autocorrelation can be related to the first derivative of f. We further propose the metric *APC Distance* and show that Quantum Error Correcting Codes (QECCs) are natural candidates for boolean functions with favourable APC Distance.

Keywords

Propagation Criteria, Differential Cryptanalysis, Aperiodic Autocorrelation, Quantum Error-Correcting Codes, Boolean Functions, GF(4)-additive Codes, Graph Theory, Quantum Entanglement.

I. Introduction

Imagine the block cipher scenario where an attacker has knowledge of the values of a fixed subset, μ, of the plaintext bits and any subset of the ciphertext bits, for multiple plaintext/ciphertext pairs. Moreover he is able to modify any of the plaintext bits from the set μ, in order to realise a differential attack on the cipher. For a given cipher, what is the smallest size of μ such that a biased differential can be established across the cipher? This scenario motivates us to define *Aperiodic Propagation Criteria* (APC) for a boolean function such that *APC Distance* is this minimum size for μ for a constituent boolean function of the cipher. We also define multivariate *aperiodic autocorrelation* of a boolean function, from which APC is derived.

Now imagine a similar scenario where the attacker has knowledge of the values of a fixed subset, μ, of the plaintext bits, and he is able to modify any subset, $\mathbf{a}$, of the plaintext bits, but this time $\mathbf{a}$ is not necessarily a subset of μ. For a given cipher, and for a given size for $\mathbf{a}$, what is the smallest size for μ such that a biased differential can be established across the cipher? Preneel et al. [30] have defined *Extended Propagation Criteria* (EPC) such that, for a constituent boolean function of the cipher, EPC(l) of order q means that a biased differential can not be found if μ is of size q or less given that $\mathbf{a}$ is of size l or less. To ease comparison with APC, we further propose *EPC Distance* to be the minimum size of $\mu \bigcup \mathbf{a}$ such that a biased differential can be found. EPC is also considered in [24] and [5].

It is the purpose of this paper to characterise aperiodic autocorrelation for a boolean function, to motivate its use for cryptanalysis, and to consider constructions for boolean functions with favourable aperiodic criteria, where favourable here means that the aperiodic coefficients are zero at low weight indices. Preneel et al. [30] propose (periodic) *Propagation Criteria* (PC) of degree l and order q which evaluates periodic properties of a boolean function when q of the input bits are kept constant. In the same way we propose *Aperiodic Propagation Criteria* (APC) of degree l and order q to evaluate aperiodic properties when q bits are kept constant. It is then natural to compare APC with EPC.

By interpreting our boolean function over m variables as a quantum state over m qubits, we also establish, rather surprisingly, that APC Distance of a quadratic boolean function is equal to the minimum distance of an associated zero-dimension *Quantum Error-Correcting Code* (QECC) which is, in turn, a highly-entangled pure quantum state [21]. We apply recent results on quantum codes to the construction of quadratic boolean

T.A. Gulliver is with the Dept. of Elec. & Computer Eng., University of Victoria, P.O.Box 3055, STN CSC, Victoria, B.C., Canada V8W 3P6 E-mail: `agullive@ece.uvic.ca`

L.E.Danielsen and M.G.Parker are with the Selmer Centre, Inst. for Informatikk, Høyteknologisenteret i Bergen, University of Bergen, Bergen 5020, Norway. E-mail: `matthew@ii.uib.no`. Web: `http://www.ii.uib.no/~matthew/`

functions with favourable APC. This suggests that the disciplines of *quantum entanglement* and cryptographic criteria for boolean functions are closely related [28]. The mapping of boolean functions into Hilbert space allows one to apply *Local Unitary Transforms* to establish orbits of boolean functions over which APC Distance is invariant. Orbits of quadratic functions can be generated by successive *Vertex-Neighbour-Complement* (VNC) operations [14] which encode the action of a special subset of Local Unitary Transforms. Similarly, APC Distance-invariant orbits of functions of algebraic degree > 2 can also be generated by application of the same set of Local Unitary Transforms.

This paper is structured as follows. After establishing the notation, we characterise aperiodic and fixed-aperiodic autocorrelation for a boolean function. We then define APC, elaborate on the similarities between APC and EPC, and define APC and EPC distance metrics. We consider constructions for quadratic boolean functions with favourable APC, using known results for QECCs. We also highlight the unusual VNC symmetry. Finally we consider the challenging problem of finding constructions for boolean functions of algebraic degree > 2 with favourable APC, and we describe the generalisation of VNC for such functions. We also show, in Appendix B, how to use aperiodic coefficients to compute the combined periodic/negaperiodic coefficients, and vice versa. Symmetries associated with aperiodic autocorrelation are described in Appendix C. Finally Appendix D presents the results of the (truncated) differential analysis of a few state-of-the-art S-boxes with respect to periodic, aperiodic, and fixed-aperiodic autocorrelation.

II. Preliminaries

Let $\mathcal{B}_m$ denote the set of all Boolean functions on m variables. For $a = (a_0, a_1, \ldots, a_{m-1}) \in F_2^m$, the *Hamming Weight* of a is

$$\mathrm{wt}(a) = \sum_{i=0}^{m-1} a_i.$$

We define the operators $\bar{\ }: F_2^m \rightarrow F_2^m$, and $\&: F_2^m \times F_2^m \rightarrow F_2^m$ as bitwise negation and modular multiplication mod 2, respectively. Let $a, b, c \in F_2^m$, then

$$\begin{array}{lcll} c = a\&b & \Rightarrow & c_i = a_i b_i & \forall i, 0 \leq i < m. \\ c = \bar{a} & \Rightarrow & c_i = a_i + 1 & \forall i, 0 \leq i < m. \end{array}$$

Let $a, b \in F_2^m$, then

$$b \preceq a \quad \Leftrightarrow \quad b_i \leq a_i \qquad \forall i, 0 \leq i < m,$$

and we say that a *covers* b.

The *dual*, $V^{\perp}$, of a subspace, $V \subset F_2^m$ can be described relative to the scalar product

$$V^{\perp} = \{x \in F_2^m | \forall y \in V, x \cdot y = 0\}.$$

In particular, for $r \in F_2^m$, we define V_r as follows

$$V_r = \{x \in F_2^m | x \preceq r\}.$$

Moreover, for any $k \in F_2^m$, $k + V$ defines a *coset* of V.

Let E be any subset of F_2^m. For any $f \in \mathcal{B}_m$ we define $f\phi_E$ as the *restriction* of f to E such that $f\phi_E(x) = 1$ iff $f(x) = 1$ and $x \in E$. If E is a k-dimensional linear subspace of F_2^m then, for any coset, $b + E$, we identify $f\phi_{b+E}$ with a boolean function in $\mathcal{B}_k$, where the function obtained depends on b.

For any $f \in \mathcal{B}_m$ we define $\mathcal{F}(f)$ as follows

$$\mathcal{F}(f) = \sum_{x \in F_2^m} (-1)^{f(x)}.$$

If E is a k-dimensional linear subspace of F_2^m then, for any coset, $b+E$

$$\mathcal{F}(f\phi_{b+E}) = \sum_{x \in b+E} (-1)^{f(x)}.$$

The (Walsh-Hadamard) *Fourier Spectrum* of $f \in \mathcal{B}_m$ is expressed as the multi-set

$$\{\mathcal{F}(f + \alpha \cdot x), \alpha \in F_2^m\}.$$

Definition 1: Let $f \in \mathcal{B}_m$ and let t be some positive integer. The function f is said to be *Correlation-Immune* of order t if and only if $\mathcal{F}(f + \alpha \cdot x) = 0$ for any $\alpha \in F_2^m$ such that $1 \leq \mathrm{wt}(\alpha) \leq t$. Moreover, when f is balanced, it is said to be *t-Resilient.* A *Balanced Function* is 0-Resilient.

For any $f \in \mathcal{B}_m$ and $a \in F_2^m$, the *first derivative* of f with respect to a is given by $\mathcal{D}_a f \in \mathcal{B}_m$, where

$$\mathcal{D}_a f = f(x) + f(x+a).$$

In the sequel we use expressions of the form $\mathcal{D}_a f \phi_E$ which should always be taken to mean $(\mathcal{D}_a f)\phi_E$, i.e. we omit brackets for clarity.

For $a, k, \mu \in F_2^m$, $a \preceq \bar{\mu}$, $k \preceq \mu$, the *fixed-periodic autocorrelation* coefficients, $p_{a,k,\mu}$, of f after fixing the subspace, V_μ, to k, can be defined by

$$p_{a,k,\mu} = \mathcal{F}(\mathcal{D}_a f \phi_{k+V_{\bar{\mu}}}), \qquad a \preceq \bar{\mu}, k \preceq \mu. \tag{1}$$

When $\mu = 0$ there is no subspace fixing, and (1) simplifies to the *periodic autocorrelation* of f, given by

$$p_a = \mathcal{F}(\mathcal{D}_a f). \tag{2}$$

Definition 2: [30] Let $E \subset F_2^m$. The function $f \in \mathcal{B}_m$ satisfies the (periodic) *Propagation Criteria* (PC) with respect to E if, for all $e \in E$, $p_e = 0$. The function f satisfies PC of degree l and order q (PC(l) of order q) for some positive integers l and q if $p_{a,k,\mu} = 0$ for any $a, k, \mu \in F_2^m$ such that $a \preceq \bar{\mu}$, $k \preceq \mu$, $1 \leq \mathrm{wt}(a) \leq l$ and $0 \leq \mathrm{wt}(\mu) \leq q$. For $q = 0$ we abbreviate, saying that f satisfies PC(l).

III. Aperiodic Autocorrelation of a Boolean Function

For $a, k, \mu \in F_2^m$, $a, k \preceq \mu$, and $\theta = \mu + a$, where θ and a are disjoint, the *fixed-aperiodic autocorrelation* coefficients of f after fixing the subspace, V_θ, to $k\&\theta$ are defined by

$$u_{a,k,\mu} = \mathcal{F}(\mathcal{D}_a f \phi_{k+V_{\bar{\mu}}}), \qquad a, k \preceq \mu. \tag{3}$$

The only difference between (1) and (3) is that, for the fixed-periodic case, $a \preceq \bar{\mu}$ whereas, for the fixed-aperiodic case, $a \preceq \mu$. For (1), $(\mathcal{D}_a f)\phi_{k+V_{\bar{\mu}}} = \mathcal{D}_a(f\phi_{k+V_{\bar{\mu}}})$, but this is ill-defined for (3). Note that "knowledge of the values of a fixed subset, μ", as stated in Section I, is here characterised by fixed values of k, where k is covered by μ.

When $\mu = a$ there are no additional fixed values, and (3) simplifies to the *aperiodic* autcorrelation of f, given by

$$u_{a,k} = \mathcal{F}(\mathcal{D}_a f \phi_{k+V_{\bar{a}}}), \qquad k \preceq a. \tag{4}$$

In other words, the aperiodic autocorrelation coefficients are given by a set of restrictions on the first derivatives of f. From the definitions there are $\sum_{a \in F_2^m} 2^{\mathrm{wt}(a)} = 3^m$ coefficients, $u_{a,k}$, and $\sum_{\mu \in F_2^m} 2^{2\mathrm{wt}(\mu)} = 5^m$ coefficients, $u_{a,k,\mu}$. In fact, for autocorrelations of real functions, $F_2^m \rightarrow \mathcal{R}$, there are only a maximum of $3^m/2$ and $5^m/2$ different values for $u_{a,k}$ and $u_{a,k,\mu}$, respectively.

The fixed-aperiodic autocorrelation of a boolean function over a subspace is related to the *Extended Propagation Criteria* (EPC) as defined by Preneel et al. in [30]. This was investigated by Carlet in [5]. However, the aperiodic property is more accurately characterised by a criteria we define as *Aperiodic Propagation Criteria* (APC). We first, therefore, explain why (3) is an aperiodic (non-modular) metric, and later we return to the definitions of both APC and EPC.

Proposition 1: The periodic autocorrelations of (1) and (2) can be expressed as modular (periodic) multivariate polynomial multiplications, and the aperiodic autocorrelations of (3) and (4) can be expressed as non-modular (aperiodic) multivariate polynomial multiplications.

Proof: Let p_a and $u_{a,k}$ be as defined in (2) and (4), respectively. Let $z \in \mathcal{C}_2^m$. Define $v(z)$, $P(z)$, and $A(z)$ as follows

$$\begin{array}{l} v(z) = \sum_{x \in F_2^m} (-1)^{f(x)} \prod_{i \in \mathcal{Z}_m} z_i^{x_i} \\ P(z) = \sum_{a \in F_2^m} p_a \prod_{i \in \mathcal{Z}_m} z_i^{a_i} \\ A(z) = \sum_{k,a \in F_2^m, k \preceq a} u_{a,k} \prod_{i \in \mathcal{Z}_m} z_i^{a_i(-1)^{k_i}} \end{array}$$

Then an expansion verifies the following modular and non-modular relationships for $P(z)$ and $A(z)$

$$\begin{array}{ll} P(z) = v(z)v(z^{-1}) & \pmod{\prod_{i \in \mathcal{Z}_m}(z_i^2 - 1)} \\ A(z) = v(z)v(z^{-1}), & \end{array}$$

respectively. The above argument carries over simply to (1) (resp. (3)) by first fixing a subspace V_μ (resp. V_θ), then computing a modular (resp. non-modular) polynomial multiplication over the remaining subspace. ■

For $a, c \in F_2^m$, define $G_{a,c}$ as the Fourier Spectrum of $\mathcal{D}_a f$, so that

$$G_{a,c} = \mathcal{F}(\mathcal{D}_a f + c \cdot x). \tag{5}$$

The fixed-aperiodic autocorrelation of f after fixing a subspace, V_θ, is equivalent to a subspace Fourier Transform of the Fourier Transform of the first derivatives of f, as in the following proposition.

Proposition 2:

$$u_{a,k,\mu} = 2^{-\mathrm{wt}(\mu)} \sum_{c \preceq \mu} G_{a,c}(-1)^{k \cdot c}, \qquad a, k \preceq \mu,$$

and

$$G_{a,c} = \sum_{k \preceq \mu} u_{a,k,\mu}(-1)^{c \cdot k}, \qquad a, c \preceq \mu,$$

where, as before, the simplification to no additional fixed values is given by assigning $\mu = a$ above.

Proof: See Appendix A. ■

The relationship between aperiodic autocorrelation and its constituent periodic and negaperiodic autocorrelations is described in subsection VIII-A of Appendix B, and relationships to the second derivative are described in subsection VIII-B of the same Appendix.

We can establish power relationships between fixed-aperiodic coefficients and Fourier spectra of the first derivative of f, as follows

$$\sum_{k \preceq \mu} |u_{a,k,\mu}|^2 = 2^{-\mathrm{wt}(\mu)} \sum_{c \preceq \mu} |G_{a,c}|^2. \tag{6}$$

We define the *fixed-aperiodic sum-of-squares with respect to a* after fixing a subspace V_θ, referred to as $\sigma_{a,\mu}$, as follows

$$\sigma_{a,\mu} = \sum_{k \preceq \mu} |u_{a,k,\mu}|^2. \tag{7}$$

By summing over all $a, \mu \in F_2^m$ where $a \preceq \mu$, we arrive at an expression for the *complete fixed-aperiodic sum-of-squares*, Φ, for f

$$\Phi = \sum_{\mu \in F_2^m} \sum_{a \preceq \mu} \sigma_{a,\mu} = \sum_{\mu \in F_2^m} \sum_{a,k \preceq \mu} |u_{a,k,\mu}|^2. \tag{8}$$

When $a = \mu$, the above expression simplifies to the *aperiodic sum-of-squares*

$$\sigma = \sum_{a \in F_2^m} \sigma_a = \sum_{a \in F_2^m} \sum_{k \preceq a} |u_{a,k}|^2. \tag{9}$$

The aperiodic sum-of-squares has been investigated in [19] where recursions in σ have been established for certain infinite quadratic boolean constructions. Of significant interest in this paper are the choices for a and μ such that $\sigma_{a,\mu} = 0$, in particular for the cases where $\mathrm{wt}(\mu)$ is small. To this end we define *Aperiodic Propagation Criteria* as follows.

Definition 3: The function $f \in \mathcal{B}_m$ satisfies the *Aperiodic Propagation Criteria* (APC) of degree l and order q (APC(l) of order q), for some positive integers l and q if $u_{a,k,\mu} = 0$ for any $a, k, \mu \in F_2^m$ such that $a, k \preceq \mu$, $\mu = a + \theta$, $1 \le \mathrm{wt}(a) \le l$ and $0 \le \mathrm{wt}(\theta) \le q$, where a and θ are disjoint. For $q = 0$ we abbreviate, saying that f satisfies APC(l).
An intuitive reason for the usefulness of APC in a classical cryptographic context is as follows. Let $\mathbf{x}$ be the complete set of input bits $\{x_i\}$, let $\mathbf{x}_\mu, \mathbf{x_a} \subset \mathbf{x}$ be such that $\mathbf{x_a} \subset \mathbf{x}_\mu$, $|\mathbf{x}_\mu| \le q + |\mathbf{x_a}|$, and $|\mathbf{x_a}| \le l$. Then a boolean function, f, satisfies APC(l) of order q if, for every possible $\mathbf{x}_\mu, \mathbf{x_a}$ pair, knowledge of the bits in $\mathbf{x}_\mu$ gives no information as to the values of the function $\mathcal{D}_a f$, where $a_i = 1$ iff $x_i \in \mathbf{x_a}$. This definition is very similar but not identical to the *Extended Propagation Criteria* (EPC) originally defined by Preneel et al. [30]. In order to define EPC, we first define *extended autocorrelation.*

For $a, k, \mu \in F_2^m$, $k \preceq \mu$, and $\theta \preceq \mu$, the *extended autocorrelation* coefficients of f after fixing the subspace, V_θ, to $k\&\theta$, are defined by

$$v_{a,k,\mu} = \mathcal{F}(\mathcal{D}_a f \phi_{k+V_{\bar{\mu}}}), \qquad k \preceq \mu. \tag{10}$$

When $\mu \preceq a$, (10) simplifies to the extended autocorrelation of f, given by

$$v_{a,k} = \mathcal{F}(\mathcal{D}_a f \phi_{k+V_{\bar{\mu}}}), \qquad k \preceq a. \tag{11}$$

Note that

$$u_{a,k,\mu} = v_{a,k,\mu}, a \preceq \mu, \qquad \text{and} \qquad u_{a,k} = v_{a,k}, a = \mu, \tag{12}$$

so the fixed-aperiodic autocorrelation coefficients are a subset of the extended autocorrelation coefficient spectra. EPC is defined as follows.

Definition 4: [30] The function $f \in \mathcal{B}_m$ satisfies the *Extended Propagation Criteria* (EPC) of degree l and order q (EPC(l) of order q) for some positive integers l and q if $v_{a,k,\mu} = 0$ for any $a, k, \mu \in F_2^m$, such that $k \preceq \mu$, $1 \le \mathrm{wt}(a) \le l$ and $0 \le \mathrm{wt}(\mu) \le q$. For $q = 0$ we abbreviate, saying that f satisfies EPC(l).
An intuitive reason for the usefulness of EPC in a classical cryptographic context is as follows [30], [5]. Let $\mathbf{x}$ be the complete set of input bits $\{x_i\}$, let $\mathbf{x}_\mu, \mathbf{x_a} \subset \mathbf{x}$ be such that $|\mathbf{x}_\mu| \le q$, and $|\mathbf{x_a}| \le l$. Then a boolean function, f, satisfies EPC(l) of order q if, for every possible $\mathbf{x}_\mu, \mathbf{x_a}$ pair, knowledge of the bits in $\mathbf{x}_\mu$ gives no information as to the values of the function $\mathcal{D}_a f$, where $a_i = 1$ iff $x_i \in \mathbf{x_a}$.

The essential difference between APC and EPC is that, for APC the bits in the set $\mathbf{x_a}$ are assumed to be known. This is not necessarily the case for EPC. In practice this means that APC envisages a scenario where the ability to modify input bits from the set $\mathbf{x_a}$ also means that the attacker has 'free' knowledge of the values of these same bits. In other words, 'Modify' and 'Read' are not distinguished for APC, whereas they are distinguished for EPC.

It is useful to define both APC and EPC in terms of one parameter, namely *APC Distance* and *EPC Distance*, respectively.

Definition 5: The function $f \in \mathcal{B}_m$ has *APC Distance* d if it satisfies the APC(l) of order q for all positive integers, l, q, such that $d > l + q$.

Definition 6: The function $f \in \mathcal{B}_m$ has *EPC Distance* d if it satisfies the EPC(l) of order q for all positive integers, l, q, such that $d > l + q$.

The following is easily verified from (12)

$$\text{APC Distance}(f) \leq \text{EPC Distance}(f). \tag{13}$$

Computational results suggest that, for most boolean functions, the two distances are equal. A counterexample is the clique function, namely, $f = \sum_{i<j} x_i x_j$. For $m \geq 4$, we have EPC Distance $= 4$ but APC Distance $= 2$.

The APC has been defined above in terms of fixed-aperiodic coefficients, $u_{a,k,\mu}$, but can also be defined in terms of $G_{a,c}$. From (6) we have the following two-way implication, where $a \preceq \mu$

$$u_{a,k,\mu} = 0, \forall k \preceq \mu \qquad \Leftrightarrow \qquad G_{a,c} = 0, \forall c \preceq \mu. \tag{14}$$

Preneel et al. [30] and Carlet [5] have given spectral characterizations of the EPC in terms of the Fourier Transform of $\mathcal{D}_a f$. We now re-express this characterization in terms of EPC distance and Resilience of $\mathcal{D}_a f$.

Corollary 1:

$$f \text{ has EPC Distance } d \qquad \Leftrightarrow \qquad \mathcal{D}_a f \text{ is } (d - \mathrm{wt}(a) - 1)\text{-Resilient}, \qquad \forall a, \mathrm{wt}(a) < d.$$

Using (13) we obtain the following corollary.

Corollary 2:

$$f \text{ has APC Distance } d \qquad \Rightarrow \qquad \mathcal{D}_a f \text{ is } (d - \mathrm{wt}(a) - 1)\text{-Resilient}, \qquad \forall a, \mathrm{wt}(a) < d.$$

If $\mathcal{D}_a f$ is $(d - \mathrm{wt}(a) - 1)$-Resilient, then f may have APC distance less than d (e.g. the clique function $f = \sum_{i<j} x_i x_j$ for $m \geq 3$).

APC is slightly stricter than EPC[1] and a much stricter criteria than PC. For example, it is easily verified that the hyper-bent function

$$\begin{aligned} f \;=\; & x_0x_1x_2 + x_0x_1x_5 + x_0x_2x_3 + x_0x_4x_5 + x_1x_2x_3 + x_1x_2x_4 + x_1x_2x_5 + x_1x_3x_4 \\ & + x_1x_3x_5 + x_1x_4x_5 + x_2x_4x_5 + x_0x_3 + x_0x_5 + x_1x_4 + x_2x_3 + x_3x_4 \end{aligned}$$

has PC(6), but only APC(1), and further has APC Distance and EPC Distance of 2. In fact, PC acts as an upper-bound on EPC which, in turn, acts as an upper bound on APC, giving the following lemma.

Lemma 1: Let f satisfy

$$\text{PC}(l) \text{ of order } q, \qquad \text{EPC}(l') \text{ of order } q, \qquad \text{APC}(l'') \text{ of order } q\ .$$

Then $l'' \leq l' \leq l$.

Fig 1. shows the scope of μ and a for EPC, APC and PC. Although EPC is more general then APC (because a is not necessarily a subset of μ), the "spectral region" examined by EPC is no bigger than for APC. In other words, for EPC, the part of a not covered by μ is, in a sense, superfluous, as it refers only to the periodic

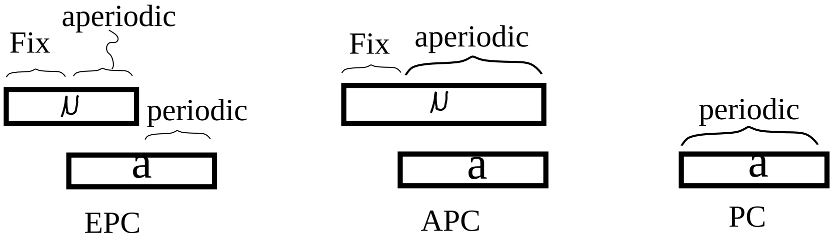

Fig. 1
RELATIVE SCOPE OF μ AND a FOR EXTENDED, APERIODIC, AND PERIODIC AUTOCORRELATIONS

autocorrelation, which is a spectral subset of the aperiodic autocorrelation [2]. APC, on the other hand, has no purely periodic part.

Here is a well-known quadratic construction [11] for $f \in \mathcal{B}_m$ which has APC($\lfloor \frac{m}{2} \rfloor$).

Theorem 1: Define $f \in \mathcal{B}_m$, $e \in F_2^m$, and $d \in F_2$ such that

$$f(x) = \sum_{i=0}^{m-2} x_{\pi(i)} x_{\pi(i+1)} + e \cdot x + d,$$

where π is any permutation from $\mathbb{Z}_m$ to $\mathbb{Z}_m$. Then f has APC($\lfloor \frac{m}{2} \rfloor$).

Proof: See Appendix A ■

Unfortunately the construction of Theorem 1 only gives APC Distance 2. This is because fixing variables can comprise the strength of the residual subspace function. For instance, for π the identity, $\mu = 1100\ldots$, and $a = 100\ldots$ we find that $u_{a,k,\mu} \neq 0$ and $\text{wt}(\mu) = 2$.

IV. CONSTRUCTIONS FOR BOOLEAN FUNCTIONS WITH FAVOURABLE APC

A. *Qubits and Local Unitary Transforms*

A 'quantum bit' or *qubit* is an idealisation of a 2-dimensional quantum object. It is described by the vector (q_0, q_1), such that the probablity of measuring the qubit in state 0 or state 1 is $|q_0|^2$ or $|q_1|^2$, respectively, with $|q_0|^2 + |q_1|^2 = 1$. Similarly, m qubits comprise a 2^m-dimensional object or pure [3] *quantum state*, $|\psi>$, as described by the vector $s = (s_{00\ldots0}, s_{00\ldots1}, \ldots, s_{11\ldots1})$ such that the probability of a joint measurement on the m qubits of $|\psi>$ yielding state i is $|s_i|^2$, where $i \in \mathbb{Z}_2^m$, and $||s||_2^2 = \sum_{i=00\ldots0}^{11\ldots1} |s_i|^2 = 1$, where $||s||_p$ is the L_p-norm of s. We say that s is normalised if $||s||_2^2 = 1$. A local change of basis on the measurement axes is realised by evaluating $s' = Us$, where U is a $2^m \times 2^m$ tensor-decomposable, unitary matrix. U is unitary if $UU^\dagger = I$, where I is the identity and $\dagger$ means 'transpose-conjugate', and U is tensor-decomposable if it can be written as $U = u_0 \otimes u_1 \otimes \ldots \otimes u_{m-1}$, where the u_j are 2×2 unitary matrices. If U is of this form then it is referred to as a *Local Unitary Transform*. The transform is *local* because it is fully tensor-decomposed. We define s and s' to be *locally equivalent* if $s' = Us$ for U a Local Unitary Transform. In such a case s and s' are considered to be equivalent quantum states. It is this notion of equivalence that is exploited later in this section in the context of boolean functions. As in [28], we will use a bijective mapping from a boolean

[1] Although the fixed-aperiodic autocorrelation coefficients are a subset of the extended autocorrelation coefficients (see (12)), the interpretation of the weight of the coefficient indices as a distance measure means that APC is stricter than EPC.

[2] By "spectral region" we mean that the $u_{a,k,\mu}$ and $v_{a,k,\mu}$ of f can both be computed from the $\{I, H, N\}^m$ set of transforms, where $\{I, H, N\}^m$ is as defined in section IV-F. More specifically, aperiodic autocorrelation ($u_{a,k}$) can be computed from the set of $\{H, N\}^m$ transform coefficients, whereas periodic autocorrelation (p_a) can be computed from the $\{H\}^m$ (Walsh-Hadamard) coefficients, which are a subset of the $\{H, N\}^m$ transform coefficients.

[3] We only deal with 'pure' states in this paper.

function, $f \in \mathcal{B}_m$, to a quantum state of m qubits, $|\psi>$, as represented by s

$$|\psi> \equiv s = 2^{-\frac{m}{2}}(-1)^{f(x)} \tag{15}$$

with $s_i = 2^{-\frac{m}{2}}(-1)^{f(x=i)}$. Consequently we refer to qubit i as x_i. This mapping allows us to view the fixed-aperiodic autocorrelation of a boolean function in a quantum context. In particular we will see that the typical error model used to define a QECC can be related precisely to the operations associated with the fixed-aperiodic autocorrelation of a boolean function. As the QECC error set is invariant to local basis change, this means that, if $s = 2^{-\frac{m}{2}}(-1)^{f(x)}$ and $s' = 2^{-\frac{m}{2}}(-1)^{f'(x)}$ are locally equivalent, then f and f' have the same fixed-aperiodic autocorrelation profile.

B. Quantum Error Correcting Codes (QECCs)

Stabilizer QECCs [16], [33], [17], [18], [20] make excellent candidates for boolean functions with favourable APC. An $[[m,k,d]]$ QECC is a code over m qubits of dimension k and distance d, where each of the 2^k codewords can be thought of as a length 2^m normalised complex vector. The typical error-model for such a code assumes the occurence of *no error*, *bit-flip*, *phase-flip*, or *combined phase-flip then bit-flip* error on each qubit, independently, (errors I, X, Z, and Y, respectively). We introduce the *Pauli Matrices*, $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, $Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$ which form a linear basis for all 2×2 complex unitary matrices. Let a quantum code of m qubits be subject to an error, $\mathcal{E} = (\mathcal{E}_0, \mathcal{E}_1, \ldots, \mathcal{E}_{m-1})$, such that $\mathcal{E}_j \in \{I, X, Z, Y = iXZ\}$ acts on qubit j, where $i^2 = -1$. An error from $\mathcal{E}$ can be described by the Local Unitary Transform $U_\mathcal{E} = \mathcal{E}_0 \otimes \mathcal{E}_1 \ldots \otimes \mathcal{E}_{m-1}$ such that $s' = U_\mathcal{E} s$ takes s to the error state s'. The weight of the error vector, $\mathcal{E}$, is given by $\mathrm{wt}(\mathcal{E}) = |\{\mathcal{E}_j | \mathcal{E}_j \neq I\}|$, and an $[[m,k,d]]$ QECC can, by definition, detect any error vector of weight less than d. Any *Stabilizer* QECC can be represented by a graph over m vertices [33], [14], [37], [18], [15]. Quantum states with a graphical representation which have a direct interpretation as quadratic boolean functions were also investigated in [28]. These turn out to be QECCs of dimension $k = 0$, and therefore correspond to the *graph states* recently proposed in [21], [38]. These QECCs also correspond to *additive self-dual codes over* $GF(4)$ [3], [20]. The mapping from an additive self-dual code over GF(4) to a graph can be understood by converting the code generator matrix over GF(4) to an equivalent form, G, such that $G = \Gamma + \omega I$, where Γ is a symmetric $m \times m$ matrix in GF(2) with zeroes on the diagonal, and $\omega \in$ GF(4) such that $\omega^2 + \omega + 1 = 0$. This conversion is always possible if the code is self-orthogonal. Γ is then, simultaneously, the adjacency matrix for a simple graph that represents the graph state. In this paper we also intepret this graph state as a quadratic boolean function, $f = \sum_{j>i} \Gamma_{i,j} x_i x_j$, where the $\Gamma_{i,j}$ are entries of G. In other words, we exploit the equivalence of $[[m,0,d]]$ Stabilizer QECCs [17] to quadratic boolean functions via their interpretation as simple graphs. Conversely, we interpret a quadratic boolean function as a graph state which, in turn is a Stabilizer QECC of zero dimension, using the mapping (15). The QECC literature often refers to stabilizer states more abstractly as eigenvectors of a subset of error operators [4] but, w.l.o.g., we can associate these eigenvectors with specific states. When the dimension of the QECC is $k = 0$ the code coincides with a single quantum state which we interpret in this paper by a quadratic boolean function and, if the distance, d, of the code is high, the state is relatively robust to errors, implying that the state is highly *entangled* [28], [21]. Later in this section we also use the mapping (15) to find non-stabilizer QECCS via non-quadratic boolean functions. A pure m-partite quantum state is un-entangled if its associated state vector can be fully decomposed as a tensor product. Otherwise the quantum state is considered to be entangled. There are an infinite number of metrics to describe the entanglement of an m-partite quantum state just as there are an infinite number of metrics to describe the properties of an error-correcting code [28], (and, for large enough m,

[4] The QECC is defined by finding a subset of error operators such that any codeword in the QECC is a joint eigenvector of all operators in the subset, i.e. the codeword is 'stabilized' by this subset of error operators. The minimum distance of the QECC is then given by the minimum-weight error operator in the subset.

most of them are intractable). Therefore any single metric is, inevitably, a partial measure. However, in this paper, we focus on the fixed-aperiodic properties of the state as giving a good indication of the entanglement of the state - certainly much more useful than just the periodic properties - with high APC Distance indicating high entanglement.

For $|\psi>$ described by f above, and $a \in F_2^m$, $a = (a_0, a_1, \ldots, a_{m-1})$, the set of bit-flips, X_a, on $|\psi>$ on qubits x_j, $j \in \{k | a_k = 1, 0 \leq k < m\}$ can be described in terms of f as follows

$$|\psi> \rightarrow X_a(|\psi>) \qquad \Leftrightarrow \qquad f(x) \rightarrow f(x+a).$$

Similarly, for $c \in F_2^m$, $c = (c_0, c_1, \ldots, c_{m-1})$, the set of phase-flips, Z_c, on $|\psi>$ on qubits x_j, $j \in \{k | c_k = 1, 0 \leq k < m\}$ can be described in terms of f as follows

$$|\psi> \rightarrow Z_c(|\psi>) \qquad \Leftrightarrow \qquad f(x) \rightarrow f(x) + c \cdot x.$$

Therefore any combination of phase-flips followed by bit-flips on $|\psi>$ can be described in terms of f as follows

$$|\psi> \rightarrow X_a Z_c(|\psi>) \qquad \Leftrightarrow \qquad f(x) \rightarrow f(x+a) + c \cdot x + c \cdot a,$$

with a combined phase-flip then bit-flip occuring at the indices covered by $a \& c$. $Z_c X_a(|\psi>) = -X_a Z_c(|\psi>)$ but to simplify the discussion in this paper we ignore post-multiplication by -1 and assume phase-flips are always performed before bit-flips.

The error-vector, $\mathcal{E}$, describing $X_a Z_c(|\psi>)$, has weight $\mathrm{wt}(\mu)$, where $\mu = a + \bar{a} \& c$ (i.e. $\mu = a$ OR c). To ensure that the QECC can detect all errors of weight $< d$ it is necessary and sufficient that, for $\mathrm{wt}(\mu) < d$, all error states, $X_a Z_c(|\psi>)$, are orthogonal to $|\psi>$ with respect to the normal scalar product of vectors. If this is true then the QECC is an $[[m, 0, d]]$ code.

Theorem 2: For $f \in \mathcal{B}_m$, let $|\psi>$ be a $[[m, 0, d]]$ QECC, described by $s = 2^{-\frac{m}{2}}(-1)^{f(x)}$. Then f has APC Distance d. Conversely, if f has APC Distance d then s represents an $[[m, 0, d]]$ QECC, $|\psi>$.

Proof: See Appendix A ■

Remark: Theorem 2 holds for f of any algebraic degree, but when f has degree 2 we are considering stabilizer QECCs. In this case, the error-subset which forms the stabilizer can be identified with the subset of fixed-aperiodic (as opposed to periodic) propagations that identify all *linear structures* [13], [7].

As stated earlier, a particularly convenient way to construct QECCs is via additive codes over GF(4). In this paper we focus on those codes of zero dimension as these relate to single boolean functions. (Higher dimension codes relate to sets of functions which will be dealt with in future work). Upper-bounds on the minimum distance of a stabilizer QECC can, for instance, be ascertained from [20]. These bounds depend on whether the underlying additive self-dual code over GF(4) is of Type I or Type II. For Type I codes, the minimum distance, d_I, for $m > 1$, satisfies

$$d_I \leq \begin{cases} 2\lfloor \frac{m}{6} \rfloor + 1, & \text{if } m \equiv 0 (\bmod 6) \\ 2\lfloor \frac{m}{6} \rfloor + 3, & \text{if } m \equiv 5 (\bmod 6) \\ 2\lfloor \frac{m}{6} \rfloor + 2, & \text{otherwise.} \end{cases}$$

For Type II codes, the minimum distance, d_{II}, for $m > 1$, satisfies

$$d_{II} \leq 2\lfloor \frac{m}{6} \rfloor + 2.$$

These upper-bounds translate directly into upper-bounds on the APC Distance for quadratic boolean functions on m variables.

C. Spectral Equivalence and the Vertex-Neighbour-Complement (VNC) Operation

Parker and Rijmen [28] observed that quantum states represented by the clique function, $f(x) = \sum_{i<j} x_i x_j$, and the star function, $f(x) = \sum_{i=1}^{m-1} x_0 x_i$, are equivalent with respect to Local Unitary Transforms (and further equivalent to the generalised GHZ (Greenberger-Horne-Zeilinger) state). It turns out that, for a special subset of Local Unitary Transforms, for any pair of boolean functions which are equivalent with respect to this transform set, the APC Distance remains invariant. This invariance is already known in the context of QECCs, (i.e. for quadratic boolean functions), but the proof is extended to all boolean functions in subsection IV-F, where the transform equivalence is described in more detail. [5]

We focus here on the quadratic equivalence which has been re-formulated as a graph symmetry by Glynn [14], [15], where the symmetry operation is referred to as *Vertex-Neighbour-Complement* (VNC). It was also described independently by Hein et al. [21] and Van Den Nest et al. [38]. In [31] VNC is explicitly described via repeated actions of the so-called $\{I, H, N\}^m$ transform set. VNC also has a history in graph theory, where it is referred to as *Local Complementation* by Bouchet [2], who identified *isotropic systems* as being equivalent with respect to Local Complementation. VNC also translates into the natural equivalence between additive codes over GF(4) which preserves the weight distribution, and this is the context in which it is presented by Calderbank et al. [3]. Not surprisingly, isotropic systems and GF(4) additive codes are very similar structures. The VNC symmetry rule can be described as follows.

Definition 7: If the quadratic monomial $x_i x_j$ occurs in the algebraic normal form of the quadratic boolean function f, then x_i and x_j are mutual neighbours in the graph represented by f, as described by the $m \times m$ symmetric adjacency matrix, Γ, where $\Gamma_{i,j} = \Gamma_{j,i} = 1$ iff $x_i x_j$ occurs in f, and $\Gamma_{i,j} = 0$ otherwise. For quadratic $f, f' \in \mathcal{B}_m$, f and f' are in the same *VNC orbit* if

$$f'(x) = f(x) + \sum_{j,k \in \mathcal{N}_a, j \neq k} x_j x_k \pmod 2, \tag{16}$$

where $\mathcal{N}_a$ comprises the neighbours of x_a in the graphical representation of f.
In the same way that a Bent function f and its dual, $\tilde{f}$, are equivalent with respect to a Walsh-Hadamard Transform [12], so the members of a VNC-orbit represent flat spectra with respect to a certain set of Local Unitary Transforms as described in subsection IV-F. [31]. Exploiting this generalised Fourier duality, one can show the following.

Theorem 3: [14], [15] Let $f, f' \in \mathcal{B}_m$ such that f and f' are quadratic and in the same VNC orbit. Then

$$\text{APC Distance}(f) = \text{APC Distance}(f').$$

For example, the quadratic functions

$$f_h = x_0x_1 + x_0x_3 + x_0x_4 + x_1x_2 + x_1x_5 + x_2x_3 + x_2x_5 + x_3x_4 + x_4x_5,$$

and

$$f'_h = x_0(x_1 + x_2 + x_3 + x_4 + x_5) + x_1x_2 + x_2x_3 + x_3x_4 + x_4x_5 + x_5x_1,$$

are in the same orbit and therefore have the same APC distance (of 4). They are the two forms of the $[[6, 0, 4]]$ *hexacode* up to graph isomorphism. The graphs associated with these two functions both satisfy a maximum Independent Set of 2, but the maximum Independent Sets of the clique and star graph, which are two members

[5] Note, however, that boolean functions of degree > 2 with APC Distance d do not map to stabilizer QECCs as these functions no longer map to joint eigenvectors of the error-set. However, one can still interpret the functions as $[[m, 0, d]]$ QECCs, as all errored-states of error-weight less than d are orthogonal to the unerrored state and, for large d, the quantum state is highly-entangled.

of another VNC orbit, are 1 and $m-1$ respectively. In general, VNC orbits which only comprise graphs with low maximum Independent Sets represent quadratic boolean functions with high APC Distance [9], [10].

To illustrate the interpretation of the graph as a GF(4) additive code, consider the hexacode as represented by the boolean function, f_h, above. Then an associated generator matrix for the $[6, 2^6, 4]$ additive code over GF(4) can immediately be written as

$$\begin{array}{c} w10110 \\ 1w1001 \\ 01w101 \\ 101w10 \\ 1001w1 \\ 01101w \end{array},$$

where $w \in$ GF(4), $\quad w^2 + w + 1 = 0$.

It has been shown by Calderbank et al. (up to $m = 5$) [3], by Hohn (up to $m = 7$) [22], by Glynn et al. (up to $m = 9$) [15], by Hein et al. (up to $m = 7$) [21], and by Danielsen (up to $m = 12$) [10] that, up to graph isomorphism, the number of VNC-orbits for quadratic boolean functions that represent connected graphs is

m	1	2	3	4	5	6	7	8	9	10	11	12
#orbits	1	1	1	2	4	11	26	101	440	3132	40457	1274068

This sequence exists as sequence A090899 in *The On-Line Encyclopedia of Integer Sequences* [35]. A database of orbit representatives up to $m = 12$ can be obtained from http://www.ii.uib.no/~larsed/vncorbits/.

D. Examples

Consider the following important construction. Let p be a prime integer of the form $4k+1$. Assign $a_{ij} = 1$ iff $j - i$ is a quadratic residue, mod p, and $a_{ij} = 0$ otherwise. Let $f \in \mathcal{B}_p$ be a quadratic boolean function defined by

$$f(x) = \sum_{i<j} a_{ij} x_i x_j.$$

Then f has favourable APC distance. The $m \times m$ symmetric adjacency matrix, Γ, where $\Gamma_{i,j} = \Gamma_{j,i} = 1$ iff $a_{i,j} = 1$, represents the *Paley Graph* which is well-known in the graph-theoretic literature.

We extend the above construction by 'bordering' the function, as follows. With f as defined above, let $g \in \mathcal{B}_{p+1}$ be a quadratic boolean function defined by

$$g(x) = f(x) + x_p \sum_{i=0}^{p-1} x_i.$$

Then g has favourable APC distance.

As an example, for $p = 5$, $f(x) = x_0x_1 + x_1x_2 + x_2x_3 + x_3x_4 + x_4x_0$, and $g(x) = f(x) + x_5(x_0 + x_1 + x_2 + x_3 + x_4)$. f has APC distance 3 and g has APC Distance 4. g is unique over the 6-variable quadratics in achieving an optimal APC Distance of 4. g is the hexacode over GF(4) (a code which is both linear and additive over GF(4)). g was identified as being a highly-entangled 6-qubit quantum state in [28]. Another example with $p = 29$, f has an APC Distance of 11 and g has an APC Distance of 12.

For $m = 12$ variables the QECC with optimal distance is the *dodecacode* which maps to a function with APC Distance 6. Its VNC orbit can be represented by the boolean function

$$f = 03, 07, 08, 09, 0B, 14, 16, 18, 19, 1A, 25, 26, 27, 2A, 2B, 36, 38, 3A, 3B, 46, 47, 49, 4B, 57, 58, 59, 5A, 69, 7A, 8B,$$

where ij, kl denotes $x_ix_j + x_kx_l, \ldots,$, etc. It is interesting to note that both the hexacode and dodecode can be represented by graphs which have minimal node degree for every node, namely 3 and 5, these being one less than their respective distances, d. These minimal representations appear to be possible for many optimal QECCs although not all. In particular, a partial (but significant) search did not reveal a graph with node degree 11 in the VNC orbit of the graph of the $[[30, 0, 12]]$ QECC.

We are also able to use the VNC orbit to improve the resiliency of our function combined with the addition of a suitable linear function to the quadratic function identified. This addition of a linear term does not change the APC. The VNC orbit is particularly useful in this context as the maximum resiliency achievable can change over the orbit. For example, as discussed previously, there are two versions of the hexacode to within graph isomorphism - namely f_h and f'_h. One of these functions, f'_h, is Bent (i.e. satisfies PC(n)), and so cannot be resilient for any linear offset. The other function is correlation-immune of order 1 and the maximum achievable resiliency is 0 by choosing, say, the balanced function, $f_h + x_0$. Typically the maximum achievable resiliency for functions with favourable APC will be low [7].

E. Aperiodic Properties of Boolean Functions of Algebraic Degree > 2

To the best of our knowledge, QECCs represented by boolean functions of degree greater than two have not been examined in the literature. These will, in general, be non-stabilizer QECCs, as the boolean functions no longer map to eigenvectors of the error set, so one must be careful how to use these QECCs. However APC remains well-defined for such functions. We are particularly interested in boolean functions of high degree so as to avoid potential algebraic attacks. From a quantum standpoint, in general, one may expect the QECC minimum distance to decrease as algebraic degree rise. We now consider the APC Distance of such functions. These functions can also be referred to as *hypergraph states.* Note that Carlet [5] has proposed non-quadratic boolean functions with favourable EPC properties based on Kerdock and Preparata codes.

An exhaustive computer search, making use of *nauty* [26], reveals that no boolean function of $m = 4$ or 5 variables and of degree > 2 satisfies an APC Distance greater than 2. However, there are 24 cubic functions of $m = 6$ variables which satisfy an APC Distance of 3. These 24 functions are inequivalent with respect to symmetries discussed in subsections IX-B and IX-C of Appendix C. For example $f = x_1x_3x_5 + x_1x_2x_5 + x_3x_4x_5 + x_2x_4x_5 + x_0x_1x_3 + x_0x_1x_2 + x_0x_3x_4 + x_0x_2x_4 + x_0x_4 + x_0x_5 + x_1x_2 + x_1x_4 + x_2x_3 + x_2x_5 + x_3x_4 + x_3x_5 + x_4x_5$ satisfies has APC and EPC Distances of 3. By incorporating *nauty* [26] into a computer search, it was found that no cubic functions of 6 variables achieve an APC Distance greater than 3. By searching all inequivalent boolean functions with just one non-quadratic term we found 7-variable and 8-variable functions with APC Distances 3 and 4, respectively. For example $f = x_1x_3x_5 + x_0x_1 + x_0x_2 + x_1x_6 + x_2x_5 + x_3x_4 + x_3x_6 + x_4x_5 + x_5x_6$ and $f = x_0x_1x_2x_3 + x_0x_4 + x_0x_5 + x_1x_4 + x_1x_6 + x_2x_5 + x_2x_6 + x_3x_4 + x_3x_5 + x_3x_6$ have APC and EPC Distances of 3, and $f = x_0x_1x_2 + x_0x_4 + x_0x_5 + x_0x_7 + x_1x_4 + x_1x_6 + x_1x_7 + x_2x_5 + x_2x_6 + x_2x_7 + x_3x_4 + x_3x_5 + x_3x_6$ and $f = x_0x_1x_2x_3 + x_0x_4 + x_0x_5 + x_0x_6 + x_1x_4 + x_1x_5 + x_1x_7 + x_2x_4 + x_2x_6 + x_2x_7 + x_3x_5 + x_3x_6 + x_3x_7$ have APC and EPC Distances of 4. These results equal the best distances achievable using quadratic functions.

The Maiorana-McFarland construction [12] is as follows.

$$f(y, z) = y \cdot \lambda(z) + g(z), \tag{17}$$

where $f \in \mathcal{B}_{r+s}$, $y \in F_2^r$, $z \in F_2^s$, $g(z) \in \mathcal{B}_s$, and λ maps F_2^s to F_2^r. Following [5], the above examples of 7-variable and 8-variable functions can both be described using (17) with λ a linear map and $g(z)$ the non-quadratic part. We have found, as shown above, functions of this kind with favourable APC but, as pointed out by Carlet [5], the reliance on $g(z)$ to make the function non-quadratic may lead to cryptanalytic attack. A more interesting set of functions is obtained by changing λ to a non-linear mapping. Carlet constructs such functions with favourable EPC in [5], based on nonlinear Kerdock/Preparata mappings. We can, trivially, use Lemma 1 to state that, for the Kerdock/Preparata-based constructions of [5], the resultant 2^{m+1}-variable functions satisfy APC(l) of order $2^{m-1} - 2^{m/2-1} - 1$, with maximum possible $l \leq 5$, or APC(l) of order 5 with maximum possible $l \leq 2^{m-1} - 2^{m/2-1} - 1$. Moreover, using (13), both the EPC and APC Distances for such functions are upper-bounded by $2^{m-1} - 2^{m/2-1} + 5$. From (17), the Maiorana-McFarland construction is bipartite with a maximum *Independent Set* of its associated hypergraph being $\geq r$. Typically one chooses $r = s$, but VNC-orbits for the graphs of the best QECCs maintain a small maximum Independent Set for every member of the orbit, i.e. $r \ll s$, with $g(z)$ an APC-favourable sub-graph. We expect, similarly, that constructions for boolean functions of algebraic degree > 2 (hypergraphs) with favourable APC should also have a small Independent Set for their quadratic part, with $g(z)$ constructed recursively in the same way. Over 32 variables the Maiorana-McFarland constructions of Carlet [5] satisfy an APC Distance upper-bounded by 11 and the maximum Independent Set of the quadratic part of the functions is 16. In contrast the 30-variable function of subsection IV-D satisfies APC Distance 12, and the graph describing this quadratic function has a maximum Independent Set of only 6. Moreover a partial search of 9779546 functions from within the (huge) VNC orbit of this 30-variable function did not reveal a maximum Independent Set greater than 7.

F. Orbits of Boolean Functions with respect to the $\{I,H,N\}^m$ Transform Set

We describe how an orbit of boolean functions can be generated such that any two members of the orbit are spectral 'duals' with respect to a certain Local Unitary Transform (LUT) taken from a set of transforms called the $\{I,H,N\}^m$ *set* (using and refining the terminology introduced by Parker in [29]). The APC Distance is invariant over this orbit.

For $a, b \in F_2^m$, define $a\tilde{+}b$ such that $0\tilde{+}0 = 0$, $1\tilde{+}0 = 0\tilde{+}1 = 1$, and $1\tilde{+}1 = 2$. Moreover, for $h \in F_2$ and $c \in \mathcal{Z}$, define ch to be in $\{0, c\}$.

Let $f \in \mathcal{B}_m$ and $\theta, r, \alpha, e \in F_2^m$ such that $r \preceq \theta$ and $\alpha, e \preceq \bar{\theta}$. Then each pair of values of e and θ describe one of 3^m possible Local Unitary Transforms taken from the so-called $\{I,H,N\}^m$ *set*, as follows

$$s_{e,\theta}(z) = 2^{\frac{\mathrm{wt}(\theta)}{2}} \sum_{x \in r + V_{\bar{\theta}}} i^{2(f(x)+\alpha)\tilde{+}e}, \tag{18}$$

where $z = \alpha + r$, $i^2 = -1$, and $s_{e,\theta} \in \mathcal{C}^{2^m}$. In related papers [28], [29], [31] the $\{I,H,N\}^m$ transform set is described as the set of 3^m Local Unitary Transform matrices of size $2^m \times 2^m$, constructed from any possible tensor product combination of the 2×2 unitary matrices I, H, and N, where $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$, and $N = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix}$, with $i^2 = -1$. In this paper we largely avoid the matrix terminology but retain the name "$\{I,H,N\}^m$".

If, for a fixed e and θ, $s_{e,\theta}$ is a flat spectrum, i.e. if $|s_{e,\theta}(z)| = |s_{e,\theta}(z')|$ $\forall z \neq z'$, then we can write

$$s_{e,\theta}(z) = 2^{\frac{m}{2}} w^{g_{e,\theta}(z)},$$

where $g_{e,\theta}(z)$ is a function from F_2^m to $\mathcal{Z}_8^m$ and $w^8 = 1$, $w \in \mathcal{C}$.

Definition 8: Let $f, f' \in \mathcal{B}_m$. Then f and f' are in the same $\{I,H,N\}^m$ orbit iff, for some choice of e and θ, $s_{e,\theta}$ is a flat spectrum and $g_{e,\theta}$ can further be written as

$$g_{e,\theta}(z) = 4f'(z) + c \cdot z + d \qquad \mod 8,$$

where $c \in \mathcal{Z}_8^m$, and $d \in \mathcal{Z}_8$.

The following Theorem has previously been proven for f quadratic but not for general f, which is proven here. The VNC Symmetry discussed in subsection IV-C is a translation of the quadratic case of this theorem into graphical operations.

Theorem 4: Let $f, f' \in \mathcal{B}_m$. If f and f' are both in the same $\{I,H,N\}^m$ orbit, then

$$\text{APC Distance}(f') = \text{APC Distance}(f).$$

Proof: The proof relies on two critical observations that we express as Lemmas.

Lemma 2: Let $a, b \in \mathcal{C}^N$ be two length N complex vectors. Let U be an $N \times N$ complex unitary (i.e. invertible) matrix such that $a' = Ua$ and $b' = Ub$. Define orthogonality of vectors a and b with respect to the scalar product by the statement $< a, b >= 0$. Then

$$< a, b >= 0 \qquad \Rightarrow \qquad < a', b' >= 0.$$

Let $\mathcal{E} \in \{I, X, Y, Z\}$, as defined in Section IV, be the error vector acting on a 1-qubit quantum state. Then it can be shown that any transform, T, taken from the $\{I, H, N\}$ set for $m = 1$, takes the error set, $\{I, X, Y, Z\}$ to itself under conjugation. This is because the $\{I, H, N\}$ set specifies the *Local Clifford Group* which is defined as the group of local unitary matrices that keeps the Pauli set of matrices over a single complex variable invariant with respect to conjugation [23] (to within a global constant). Explicitly, for $T \in \{I, H, N\}$, $\mathcal{E}' = T\mathcal{E}T^{-1}$ satisfies, $\mathcal{E}' \in \{I, X, Y, Z\}$ [6]. It follows immediately that the $\{I, H, N\}^m$ transform set, as defined in (18), keeps $\mathcal{E}$ within the Pauli set for any fixed m, and keeps the weight of $\mathcal{E}$ invariant. We then arrive at the following Lemma.

Lemma 3: Let $T_{e,\theta} \in \{I, H, N\}^m$ and $\mathcal{E} \in \{I, X, Y, Z\}^m$. Then

$$\begin{aligned} \mathcal{E}' = T_{e,\theta}\mathcal{E}T_{e,\theta}^{-1} \quad &\Rightarrow \quad \mathcal{E}' \in \{I, X, Y, Z\}^m \\ &\Rightarrow \quad \mathrm{wt}(\mathcal{E}') = \mathrm{wt}(\mathcal{E}) \end{aligned}$$

Let a quantum state of m qubits, $|\psi >$, be represented by a length 2^m vector $s \in \mathcal{C}^{2^m}$, where $s = 2^{-\frac{m}{2}}(-1)^{f(x)}$. We can then re-express Theorem 2 as follows

$$\text{APC Distance}(f) = d \qquad \Rightarrow \qquad < \mathcal{E}s, s >= 0, \qquad \forall \mathcal{E} | 0 < \mathrm{wt}(\mathcal{E}) < d,$$

where $\mathcal{E} \in \{I, X, Y, Z\}^m$. We wish to show that

$$\text{APC Distance}(f) = d \qquad \Rightarrow \qquad < \mathcal{E}'s', s' >= 0, \qquad \forall \mathcal{E}' | 0 < \mathrm{wt}(\mathcal{E}') < d,$$

where $\mathcal{E}' \in \{I, X, Y, Z\}^m$, and s' is any vector that occurs as a spectral output with respect to any transform taken from the $\{I, H, N\}^m$ set. To do this we note that $s = T_{e,\theta}s'$ for some $T_{e,\theta} \in \{I, H, N\}^m$. We now use Lemma 3 to conjugate $\mathcal{E}$ acting on s to $\mathcal{E}'$ acting on s'. Now we can write $< \mathcal{E}s, s >= 0$ as

$$< T_{e,\theta}^{-1}\mathcal{E}'T_{e,\theta}s, T_{e,\theta}^{-1}T_{e,\theta}s >= 0$$

It follows from Lemmas 2 and 3 that

$$< \mathcal{E}'T_{e,\theta}s, T_{e,\theta}s >= 0, \qquad \forall \mathcal{E}' | 0 < \mathrm{wt}(\mathcal{E}') < d$$

The theorem follows. ■

Remark: Note that we have proved the invariance of 'APC Distance' for any s and s' in the same orbit with respect to the $\{I, H, N\}^m$ transform set. So the proof not only holds for boolean functions, f and f', but also more generally for f and f' functions from F_2^m to $\mathcal{Z}_8$. More generally still, the proof holds for any s and s', even when s and s' represent non-flat spectra.

We next provide an example of this spectral symmetry for non-quadratic boolean functions, which generalises VNC and uses the flat spectra of a boolean function with respect to the $\{I, H, N\}^n$ transform set to

[6] Note that conjugation by H takes X to Z, Z to X, and Y to $-Y$. Conjugation by N takes X to $-iY$, Z to X, and Y to $-Z$. Conjugation by I takes X to X, Z to Z, and Y to Y.

generate an orbit of boolean functions with the same APC Distance, as described above. Consider the cubic boolean function $x_0x_1x_2 + x_0x_1x_3 + x_0x_1x_4 + x_0x_2x_3 + x_0x_2x_4 + x_0x_5 + x_1x_3 + x_1x_5 + x_2x_4 + x_2x_5 + x_3x_4$ which has APC Distance 3. Applying the transform technique described above, we obtain 144 flat spectra of which 20 map to boolean functions. Of these 20, only 3 are inequivalent. These 3 functions are cubic and have APC Distance and EPC Distance 3. For instance, $x_0x_1x_5 + x_0x_3x_5 + x_0x_4x_5 + x_0x_1 + x_0x_2 + x_0x_3 + x_0x_5 + x_1x_2 + x_1x_3 + x_1x_4 + x_1x_5 + x_2x_5 + x_3x_4 + x_4x_5$ is in the same orbit and is obtained via the transform obtained by setting $\theta = 110110$ and $e = 001000$. Note, however, that no linear offset of a member of this orbit is balanced, so resiliency cannot be satisfied.

V. Conclusions

We have motivated and characterised aperiodic autocorrelation and APC for a boolean function. In particular we have equated, for quadratic boolean functions, Aperiodic Propagation Criteria (APC) Distance with the minimum distance of an associated zero-dimension Quantum Error-Correcting Code. It follows that, for quantum states which have an interpretation as boolean functions, the quantum entanglement of the state is partially described by the APC of the function. We highlighted the importance of Vertex-Neighbour-Complement (VNC) symmetry for APC analysis of quadratic boolean functions, and also gave a generalisation of VNC to boolean functions of algebraic degree > 2. We presented some results for the APC Distance of functions of degree > 2 variables and discussed possible forms future boolean constructions might take to improve APC Distance.

APC as introduced in this paper is also a potential attack scenario. Just as the generalised linear cryptanalysis of [29] finds substantially higher biases over state-of-the-art S-boxes, the differential 'dual', as covered by this paper, finds substantially higher differential biases where, by 'differential' we here refer to an input differential $\Delta x \in F_2^m$, and an output binary (truncated) differential $\Delta y \in F_2$. Appendix D gives results for an exhaustive search for the worst-case differential biases of given input differential weight, taken over the linear space of selected state-of-the-art S-boxes. It is evident that significantly higher biases can be obtained by using aperiodic as opposed to periodic differentials. One should remember that the context in which the S-Box is used will determine whether a high-bias differential constitutes a weakness for the cipher. For instance, the 9×9 Misty1 S-Box, because it is a quadratic S-box, has a linear space with periodic differential biases that occur with probability 1.0 for all weights, (i.e. it has linear structures for all weights), but these do not necessarily constitute a weakness as the S-Box is used in a Feistel structure, and in conjunction with a 7×7 cubic S-Box. Still, the 7×7 S-Box exhibits significantly higher aperiodic and fixed-aperiodic biases compared to periodic biases. These biases may lead to a practical block cipher attack. However, for the typical block cipher which inputs the key via XOR, one cannot exploit these higher biases by using the standard technique of piecing together differential trails through successive cipher rounds, as the 'route' of the trail will be key-dependent [29], [36]. In other words, although aperiodic and fixed-aperiodic differentials establish much higher biases across constituent S-Boxes and, by implication, across complete block ciphers, than periodic differentials, the location of these biases across multiple rounds is strongly key-dependent. So it may be difficult to exploit these high biases. Even so, the results of this paper provide an extended theoretical framework for a boolean function, which suggests a technique where one finds a function with favourable fixed-aperiodic criteria, then one traverses, either exactly or approximately, through the orbit generated by a set of Local Unitary Transforms, so as to optimise the function with respect to the Walsh-Hadamard spectral criteria. The problem of designing an S-box (or block cipher) so that all constituent boolean functions have high APC Distance is also an interesting challenge, but the stipulation that an S-box is a balanced function from F_2^m to F_2^n may limit the achievable APC distance. Note that all S-boxes examined in Appendix D achieve only APC Distance 1 over the complete linear space of the S-box (in fact most S-boxes are not even designed to achieve PC(1)). At the end of Table I we have included the worst-case biases for the single quadratic boolean function that represents the $[[6,0,4]]$ hexacode. By definition, the biases are all 0.5 up to weight 4. However it is much more constraining - and remains an open problem - to construct a function (S-Box) with output in F_2^n, $n > 1$, such that the low-weight biases of the linear space of the S-Box are all near to 0.5. Finally, functions with favourable APC Distance automatically have high generalised nonlinearity with respect to the generalised transform sets discussed by [29] and [31], e.g. with respect to $\{I, H, N\}^m$. This can be explained by considering a generalisation of the results of [6] to larger transform sets.

VI. Acknowledgements

The authors would like to thank Prof. Alexander Pott for reading early versions of this paper and for helpful suggestions, and Prof. Patrick Sole for helpful advice and for pointing out numerous connections with other work in the literature.

VII. Appendix A

Proof: (Proposition 2): Proposition 1 of [4] states

$$\sum_{v \in V^\perp} \mathcal{F}(f + x \cdot v) = 2^{m-k} \mathcal{F}(f \phi_V), \tag{19}$$

where k is the dimension of V. Applying (19) to (5) gives

$$\sum_{c \preceq \mu} G_{a,c} = \sum_{c \preceq \mu} \mathcal{F}(\mathcal{D}_a f + c \cdot x) = 2^{\mathrm{wt}(\mu)} \mathcal{F}(\mathcal{D}_a f \phi_{V_{\bar{\mu}}}). \tag{20}$$

It is further stated in [4] that

$$\sum_{v \in V^\perp} \mathcal{F}(f + x \cdot v)(-1)^{k \cdot v} = 2^{m-k} \mathcal{F}(f \phi_{k+V}). \tag{21}$$

Applying (21) to (3), (5) and (20) gives the result. ■

Proof: (Theorem 1): First we compute the values of $u_{a,k}$ for $k = 0$ with π the identity permutation. Let $u_{a,k}[m]$ denote the values of $u_{a,k}$ for f over m variables. Below are tabulated the values of $u_{a,0}[m]$ and the associated upper bound on the l of APC(l) inferred from these $u_{a,0}[m]$, for all possible assignments to the three least significant bits (lsbs) of a, where $*$ means 'don't care.

a(lsb on the left)	$u_{a,0}[m]$	upper bound on l
$100\ldots$	0	$\le m$
$01*\ldots$	0	$\le m$
$11*\ldots$	$u_{a,0}[m-1]$	$\le (m-1)+1 = m$
$001\ldots$	0	$\le m$
$101\ldots$	$u_{a,0}[m-2]$	$\le (m-2)+1 = m-1$

We are interested in the lowest value of l that we can achieve by suitable assignments to a. From the above table, the only case where the upper bound on l is lower than m is in the last row of the table. We recursively assign the lsbs of a according to this last row (e.g. for the second iteration we have $a = 10101\ldots$ and $l \le m-2$). By induction one concludes that $l = \lfloor \frac{m}{2} \rfloor$. As f is a quadratic function we can invoke the symmetry of Lemma 4 in Appendix C to extend the result from $u_{a,0}[m]$ to all $u_{a,k}[m]$. We further invoke the permutation symmetry of Lemma 5 to extend the result to all functions f where π is not necessarily the identity permutation. ■

Proof: (Theorem 2): Consider all bit-flip and phase-flip errors on $|\psi>$ of weight $< d$, described by a and c such that $\mathrm{wt}(\mu) = \mathrm{wt}(a) + \mathrm{wt}(\theta) < d$, as discussed previously, where $\mu = a + \bar{a}\&c$ and $\theta = \bar{a}\&c$. We know that $X_a Z_c(|\psi>)$, is orthogonal to $|\psi>$ and this can be interpreted in terms of f by asserting that $\mathcal{D}_a f + c \cdot x$ is balanced, $\forall a, c$ such that $\mathrm{wt}(\mu) < d$. In other words, from (5), (14), and Definition 4, $G_{a,c} = 0$ $\forall a, c \preceq \mu$. The first part of the theorem follows from Definition 5. The converse is easily proven. ∎

VIII. Appendix B - Further Spectral Identities

A. Periodic/Negaperiodic Autocorrelation

We here define the *periodic/negaperiodic autocorrelation* of f, and show how its coefficients are derived from the Fourier Spectra of $\mathcal{D}_a f$, thus allowing us to relate the periodic/negaperiodic autocorrelation with the aperiodic autocorrelation. The reason we refer to the autocorrelations as 'periodic/negaperiodic' will be explained in Proposition 3. Define the *periodic/negaperiodic autocorrelation coefficients* of f after fixing the subspace, V_θ, as $U_{a,e,r,\mu}$, where $a, r, \mu \in F_2^m$, $e \preceq a \preceq \mu$, $r \preceq \theta$, and $\theta = \mu + a$, and θ and a are disjoint. Then

$$\begin{array}{ll} U_{a,e,r,\mu} & = 2^{-\mathrm{wt}(\theta)} \sum_{c \in e + V_\theta} \mathcal{F}(\mathcal{D}_a f + c \cdot x + \mathrm{wt}(c))(-1)^{r \cdot c} \\ & = 2^{-\mathrm{wt}(\theta)} \sum_{c \in e + V_\theta} \mathcal{F}(\mathcal{D}_a f + c \cdot x)(-1)^{\bar{r} \cdot c} \end{array} . \tag{22}$$

When $\mu = a$ then $\theta = 0$ and there is no subspace fixing, so that (22) simplifies to the computation of the periodic/negaperiodic autocorrelation coefficients of f, namely $U_{a,c}$, where $c \preceq a$

$$U_{a,c} = (-1)^{\mathrm{wt}(c)} \mathcal{F}(\mathcal{D}_a f + c \cdot x) \qquad c \preceq a. \tag{23}$$

There are 3^m coefficients, $U_{a,c}$, $c \preceq a$, but only 2^m complete autocorrelation profiles that we can obtain from $U_{a,c}$ as each value, $U_{a,c}$, is represented $2^{\mathrm{wt}(\bar{a})}$ times to realise a complete set of 2^{2m} autocorrelation coefficients. Combining (5) with (22) and (23) yields

$$U_{a,e,r,\mu} = 2^{-\mathrm{wt}(\theta)} \sum_{c \in e + V_\theta} G_{a,c} (-1)^{\bar{r} \cdot c} \qquad e \preceq a \preceq \mu, r \preceq \theta, \tag{24}$$

and

$$U_{a,c} = (-1)^{\mathrm{wt}(c)} G_{a,c} \qquad c \preceq a. \tag{25}$$

Note that the factor of $(-1)^{\mathrm{wt}(c)}$ is of no significance in this paper, but we retain it for completeness.

By combining Proposition 2 with (24) and (25) we can now express the fixed-aperiodic (non-modular) autocorrelation coefficients in terms of the periodic/negaperiodic autocorrelation coefficients, and vice versa, where $e \preceq a \preceq \mu$, $k \preceq \mu$, $\theta = a + \mu$, and $r = k \& \theta$

$$\begin{array}{lll} u_{a,k,\mu} = 2^{-\mathrm{wt}(a)} \sum_{e \preceq a} U_{a,e,r,\mu} (-1)^{\bar{k} \cdot e}, & & k \preceq \mu \\ U_{a,e,r,\mu} = \sum_{k \preceq r + V_a} u_{a,k,\mu} (-1)^{e \cdot \bar{k}}, & & e \preceq a \end{array} \tag{26}$$

$$\begin{array}{lll} u_{a,k} = 2^{-\mathrm{wt}(a)} \sum_{c \preceq a} U_{a,c} (-1)^{\bar{k} \cdot c}, & & k \preceq a \\ U_{a,c} = \sum_{k \preceq a} u_{a,k} (-1)^{c \cdot \bar{k}}, & & c \preceq a. \end{array} \tag{27}$$

We now explain why (22) and (23) can be viewed as periodic/negaperiodic (modular) metrics.

Proposition 3: Each periodic/negaperiodic autocorrelation of (22) and (23) is specified after fixing a subspace (without fixing) by the parameters a, e, r, μ (resp. a, c). For each setting of the parameters, the coefficients can be calculated using multivariate polynomial multiplications which are periodially modular for the variables identified by the '1' positions of $a \& \bar{e}$ (resp. $a \& \bar{c}$), and negaperiodically modular for the variables identified by the '1' positions of e (resp. c).

Proof: Let $U_{a,c}$ be as defined in (23), and let $z \in \mathcal{C}_2^m$. Define $v(z)$, and $Q_c(z)$ as follows

$$\begin{array}{l} v(z) = \sum_{x \in F_2^m} (-1)^{f(x)} \prod_{i \in \mathcal{Z}_m} z_i^{x_i} \\ Q_c(z) = \sum_{a \in F_2^m} U_{a,c} \prod_{i \in \mathcal{Z}_m} z_i^{a_i}. \end{array}$$

Then an expansion verifies the following modular relationship for $Q_c(z)$

$$Q_c(z) = v(z)v(z^{-1}) \qquad (\bmod \prod_{i \in \mathcal{Z}_m} (z_i^2 - (-1)^{c_i})).$$

$Q_c(z)$ is the evaluation of a periodic (negaperiodic) multiplication for variable i if $c_i = 0$, (resp. $c_i = 1$). The above argument then carries over to (22) by first fixing the subspace V_θ, then computing all possible periodic/negaperiodic multivariate polynomial multiplications over the remaining unfixed subspace. ■

We can recover the (non-modular) polynomial $A(z)$ of Proposition 1 by applying the Chinese Remainder Theorem (CRT) to the residue polynomials $Q_c(z)$. In summary

$$A(z) = v(z)v(z^{-1}) = v(z)v(z^{-1})(\bmod \prod_{i \in \mathcal{Z}_m} (z_i^4 - 1)) = \text{CRT}(\{Q_c(z)\}).$$

In this way, we obtain an alternative derivation of (27). A similar argument can be used with respect to a fixed subspace, V_θ, so as to rederive (26).

B. Relationships to the Second Derivative

As $G_{a,c}$ is the Fourier Spectrum of the first derivative of f, there is a natural relationship between the Fourier Power Spectra of $G_{a,c}$ and the *second derivative* of f, $\mathcal{D}_b\mathcal{D}_a f$, where $a, c, b \in F_2^m$

$$\sum_{c \preceq \mu} |G_{a,c}|^2 (-1)^{c \cdot k} = 2^{\text{wt}(\mu)} \sum_{b \in k + V_{\bar{\mu}}} \mathcal{F}(\mathcal{D}_b\mathcal{D}_a f), \qquad k \preceq \mu.$$

Moreover we can use Parseval's Theorem to establish the following

$$\sum_{c \preceq \mu} |G_{a,c}|^4 = 2^{\text{wt}(\mu)} \sum_{k \preceq \mu} \left(\sum_{b \in k + V_{\bar{\mu}}} \mathcal{F}(\mathcal{D}_b\mathcal{D}_a f) \right)^2$$

Combining the above relationship with (6), we can establish the following upper bound on the *fixed-aperiodic sum-of-squares* with respect to a after fixing a subspace V_θ, referred to as $\sigma_{a,\mu}$, and defined in (7), in terms of the second derivative of f

$$\sigma_{a,\mu} \leq 2^{-2\text{wt}(\mu)} \sum_{k \preceq \mu} \left(\sum_{b \in k + V_{\bar{\mu}}} \mathcal{F}(\mathcal{D}_b\mathcal{D}_a f) \right)^2.$$

C. A Generalised Definition of APC

Using the results of this Appendix and Appendix C we are able to generalise (14) as follows

$$\begin{array}{lllll} & u_{a,k,\mu} = 0, \forall k \preceq \mu & \Leftrightarrow & U_{a,e,r,\mu} = 0, \forall e \preceq a, \forall r \preceq \theta \\ \Leftrightarrow & G_{a,c} = 0, \forall c \preceq \mu & \Leftrightarrow & \sum_{b \in k + V_{\bar{\mu}}} \mathcal{F}(\mathcal{D}_b\mathcal{D}_a f) = 0, \forall k \preceq \mu, \end{array} \tag{28}$$

where $a \preceq \mu$.

IX. Appendix C - Symmetries of Aperiodic Autocorrelation

We summarise some important conditions for simplification of the fixed-aperiodic autocorrelation profile and and/or symmetry operations that operate on a boolean function and that keep the multiset of fixed-aperiodic autocorrelation coefficients unchanged to within a multiplicative phase offset and to within a permutation of the coefficient positions within the autocorrelation profile.

A. Quadratic Simplification

When $\deg(f) = 2$, a substantial simplification of the fixed-aperiodic autocorrelation profile can be obtained as follows.

Lemma 4: Define $f \in \mathcal{B}_m$ where $\deg(f) = 2$. For $u_{a,k,\mu}$ as defined in (3) then, for any $k' \preceq \mu$,

$$u_{a,k,\mu} = \pm u_{a,k',\mu}$$

Proof: The proof is straightforward. ■

The simplification described by this Lemma significantly reduces the APC analysis for quadratic boolean functions as we can set $k = 0$. From Section IV the APC Distance is equivalent to the distance measure for zero-dimension Quantum Error-Correcting Codes (QECCs). Such QECCs map to quadratic boolean functions. As QECCs of the stabilizer type are conveniently described by additive codes over GF(4) [3], [33], [18], [20] then, conversely, quadratic boolean functions with favourable APC can be constructed with relative ease via additive codes over GF(4). This simplification implicitly exploits the symmetry of Lemma 4.

B. Index Permutation Symmetry (Hypergraph Isomorphism)

Lemma 5: Define $f \in \mathcal{B}_m$. Let π be a permutation from $\mathcal{Z}_m$ to $\mathcal{Z}_m$. Let γ be a permutation from F_2^m to F_2^m such that, for $r \in F_2^m$, $\gamma(r)$ takes r_i to $r_{\pi(i)}$. For $f = f(x_0, x_1, \ldots, x_{m-1})$, let $f' = f(x_{\pi(0)}, x_{\pi(1)}, \ldots, x_{\pi(m-1)})$. Then

$$u_{a,k,\mu}(f') = u_{\gamma(a),\gamma(k),\gamma(\mu)}(f),$$

so that both f and f' achieve APC(l) of order q.

C. Periodic and Negaperiodic Symmetries

The fixed-aperiodic autocorrelation coefficient magnitudes of a function $f \in \mathcal{B}_m$ remain unchanged to within a linear permutation of the indices after periodic and/or negaperiodic shift of the input variables of f. With $\gamma \in F_2^m$ define f' as a periodic shift of f, where

$$f'(x) = f(x + \gamma).$$

Proposition 4: With $a, k, \gamma, \mu \in F_2^m$ and f' as defined above, and fixed-aperiodic autocorrelation coefficients as defined in (3)

$$u_{a,k,\mu}(f) = u_{a,(k+\gamma)\&\mu,\mu}(f'), \qquad k \preceq \mu. \tag{29}$$

Proof: Using (3)

$$\begin{aligned} u_{a,k,\mu}(f') &= \mathcal{F}(\mathcal{D}_a f' \phi_{k+V_{\bar{\mu}}}), \qquad k \preceq \mu \\ &= \mathcal{F}(\mathcal{D}_a f \phi_{\gamma+k+V_{\bar{\mu}}}), \qquad k \preceq \mu. \end{aligned}$$

With $k \preceq \mu$

$$\gamma + k + V_{\bar{\mu}} = (\gamma\&\mu + k) + \gamma\&\bar{\mu} + V_{\bar{\mu}} = (\gamma + k)\&\mu + (\gamma\&\bar{\mu} + V_{\bar{\mu}}) = (\gamma + k)\&\mu + V_{\bar{\mu}}.$$

Therefore, after a change of variable $k \rightarrow (k + \gamma)\&\mu$, we obtain

$$u_{a,(k+\gamma)\&\mu,\mu}(f') = \mathcal{F}(\mathcal{D} f \phi_{k+V_{\bar{\mu}}}) = u_{a,k,\mu}(f), \qquad k \preceq \mu.$$

■

Similarly, with $\lambda \in F_2^m$ we define f'' as a negaperiodic shift of f, where

$$f''(x) = f(x+\lambda) + \lambda \cdot x + \mathrm{wt}(\lambda).$$

Proposition 5: With $a, k, \lambda, \mu \in F_2^m$, and f'' as defined above, and fixed-aperiodic autocorrelation coefficients as defined in (3)

$$u_{a,k,\mu}(f) = (-1)^{\lambda \cdot a} u_{a,(k+\lambda)\&\mu,\mu}(f''), \qquad k \preceq \mu. \tag{30}$$

Proof: Remembering that f' is a periodic shift of f, observe that

$$\mathcal{D}_a f'' = f(x+\lambda) + f(x+\lambda+a) + \lambda \cdot a = \mathcal{D}_a f' + \lambda \cdot a.$$

Therefore

$$\begin{aligned} u_{a,k,\mu}(f'') &= \mathcal{F}(\mathcal{D}_a f'' \phi_{k+V_{\bar{\mu}}}), \qquad k \preceq \mu \\ &= \mathcal{F}(\mathcal{D}_a f' \phi_{k+V_{\bar{\mu}}} + \lambda \cdot a), \qquad k \preceq \mu \\ &= (-1)^{\lambda \cdot a} \mathcal{F}(\mathcal{D}_a f' \phi_{\lambda+k+V_{\bar{\mu}}}), \qquad k \preceq \mu. \end{aligned}$$

Substituting k with $(k+\lambda)\&\mu$ gives

$$u_{a,(k+\lambda)\&\mu,\mu}(f'') = (-1)^{\lambda \cdot a} u_{a,k,\mu}(f), \qquad k \preceq \mu,$$

and the proposition follows. ∎

We can combine the above results for periodic and negaperiodic shift (Propositions 4 and 5) as follows. With $\gamma, \lambda \in F_2^m$ we define f_{pn} as a periodic/negaperiodic shift of f, where

$$f_{pn}(x) = f(x+\gamma) + \lambda \cdot x + \mathrm{wt}(\lambda), \qquad \lambda \preceq \gamma.$$

Proposition 6: With $a, k, \gamma, \lambda, \mu \in F_2^m$ and f_{pn} as defined above, and fixed-aperiodic autocorrelation coefficients as defined in (3)

$$u_{a,k,\mu}(f) = (-1)^{\lambda \cdot a} u_{a,(k+\gamma)\&\mu,\mu}(f_{pn}), \qquad k \preceq \mu, \lambda \preceq \gamma. \tag{31}$$

Proof: Combine Propositions 4 and 5. ∎

Corollary 3: For the special case with $\gamma \preceq \bar{\mu}$ and f_{pn} defined as above

$$u_{a,k,\mu}(f) = u_{a,k,\mu}(f_{pn}), \qquad k \preceq \mu \in F_2^m.$$

Proof: $\gamma \& \mu = 0$. ∎

Therefore a periodic shift (resp. negaperiodic shift) of f after fixing a subspace V_θ does not change the values (resp. magnitudes) of the fixed-aperiodic autocorrelation coefficients of f, but may permute them.

Given f_{pn} as defined above, (3) and Proposition 2, we obtain the identities for the periodic/negaperiodic autocorrelation coefficients given in Lemma 32.

Lemma 6:

$$\begin{array}{ll} G_{a,c}(f) = (-1)^{\lambda \cdot a + \gamma \cdot c} G_{a,c}(f_{pn}), & \lambda \preceq \gamma, c \preceq \mu \\ U_{a,c}(f) = (-1)^{\lambda \cdot a + \gamma \cdot c} U_{a,c}(f_{pn}), & \lambda \preceq \gamma, c \preceq a \\ U_{a,e,r,\mu}(f) = (-1)^{\lambda \cdot a + \gamma \cdot e} U_{a,e,(r+\gamma\&\theta),\mu}(f_{pn}), & \lambda \preceq \gamma, e \preceq a, r \preceq \theta \end{array} . \tag{32}$$

Proof: For $k \preceq \mu$ and $\lambda \preceq \gamma$, and noting that, for $c \preceq \mu$, $\gamma \& \mu \cdot c = \gamma \cdot c$,

$$(-1)^{\lambda \cdot a} u_{a,(k+\gamma)\&\mu,\mu} = 2^{-\mathrm{wt}(\mu)}(-1)^{\lambda \cdot a} \sum_{c \preceq \mu} G_{a,c}(-1)^{(k+\gamma)\& \cdot c} = 2^{-\mathrm{wt}(\mu)}(-1)^{\lambda \cdot a} \sum_{c \preceq \mu} ((-1)^{\gamma \cdot c} G_{a,c})(-1)^{k \cdot c}$$

The results for $U_{a,c}$ and $U_{a,e,r,\mu}$ follow in a similar way. ■

Therefore the magnitudes of the periodic/negaperiodic autocorrelation coefficients are unchanged by a periodic and/or negaperiodic shift of f to within a linear permutation of the indices.

As the magnitudes of $u_{a,k,\mu}(f)$, $U_{a,c}(f)$, and $U_{a,e,r,\mu}$ are invariant to a periodic and/or negaperiodic shift of f to within a linear permutation, it follows, from (9), Definition 4, and (14) that $\sigma_{a,\theta}(f)$, $\Phi(f)$, $\sigma(f)$, and the APC of f are invariant to periodic and/or negaperiodic shifts of f. We summarise these observations in the following Corollary.

Corollary 4: For $f \in \mathcal{B}_m$, and $\mu \in F_2^m$, $a \preceq \mu$, let f_{pn} be a periodic and/or negaperiodic shift of f. Then

$$\sigma_{a,\mu}(f_{pn}) = \sigma_{a,\mu}(f), \qquad \Phi(f_{pn}) = \Phi(f), \qquad \sigma(f_{pn}) = \sigma(f),$$
$$\mathrm{APC}(f_{pn}) \text{ of order } q = \mathrm{APC}(f) \text{ of order } q$$
$$\text{APC Distance}(f_{pn}) = \text{APC Distance}(f).$$

X. Appendix D - Generalised Differential Biases of State-of-the-Art S-Boxes

In this section we examine the worst-case (truncated) differential bias for a given input differential weight, with respect to periodic, aperiodic, and fixed-aperiodic autocorrelation, for selected state-of-the-art S-boxes. More precisely, we consider a function f (S-Box) mapping F_2^m to F_2^n, and comprising n m-variable functions, $f_i \in \mathcal{B}_m$, $0 \leq i < n$. Then we define the linear space of the S-Box to be the set of functions, $\{g_c \mid \forall c \in F_2^n\}$, such that $g_c = c \cdot f$. We then compute, for a given S-Box, the maximum bias over all functions in the set $\{g_c\}$. The periodic bias at weight $|a|$ is given by $\frac{2^m+|p_a|}{2^{m+1}}$, the aperiodic bias at weight $|a|$ is given by $\frac{2^{m-|a|}+|u_{a,k}|}{2^{m-|a|+1}}$, and the fixed-aperiodic bias at weight μ is given by $\frac{2^{m-|\mu|}+|u_{a,k,\mu}|}{2^{m-|\mu|+1}}$, where, for a given differential weight, periodic bias $\leq$ aperiodic bias $\leq$ fixed-aperiodic bias always holds. Table I shows the results. For example, an exhaustive search of all 256 8-variable boolean functions constructed by linear combinations of the 8 constituent boolean functions of the AES S-Box reveals that a weight-4 differential can be found with bias 0.56, 0.94, and 1.00, for periodic, aperiodic, and fixed-aperiodic differentials, respectively.

References

[1] P.S.L.M. Barreto and V. Rijmen, "The WHIRLPOOL Hashing Function", *NESSIE Workshop, Leuven*, Nov. 2000.

[2] A. Bouchet, "Recognizing Locally Equivalent Graphs," *Discrete Math.*, **114**, pp. 75–86, 1993.

[3] A.R. Calderbank, E.M. Rains, P.W. Shor and N.J.A. Sloane, "Quantum Error Correction Via Codes Over GF(4)," *IEEE Trans. Inform. Theory*, **44**, pp. 1369–1387, 1998,

[4] A. Canteaut and P. Charpin, "Decomposing Bent Functions," *IEEE Trans. Inform. Theory*, **49**, pp. 2004–2019, 2003.

[5] C. Carlet, "On Cryptographic Propagation Criteria for Boolean Functions," *Inform. and Computation.*, **151**, pp. 32–56, 1999.

[6] F. Chabaud and S. Vaudenay, "Links Between Differential and Linear Cryptanalysis", *Advances in Cryptology - EUROCRYPT '94, Lecture Notes in Computer Science, Springer-Verlag*, **950**, pp. 356–365, 1995.

[7] P. Charpin and E. Pasalic, "On Propagation Characteristics of Resilient Functions", *SAC, Selected Areas in Cryptography, Lecture Notes in Computer Science, Springer-Verlag*, **2595**, pp. 175–195, 2003.

[8] J. Daemen and V. Rijmen, "The Block Cipher Rijndael," NIST AES homepage, http://www.nist.gov/aes/

[9] L.E. Danielsen and M.G. Parker, "Spectral Orbits and Peak-to-Average Power Ratio of Boolean Functions with respect to the $\{I,H,N\}^n$ Transform", *SETA'04, Sequences and their Applications, Seoul*, October, 2004

[10] L.E. Danielsen, *Master's Thesis - In Preparation*, Selmer Centre, Inst. for Informatics, University of Bergen, Bergen, Norway, 2004.

[11] J.A. Davis and J. Jedwab, "Peak-to-mean Power Control in OFDM, Golay Complementary Sequences and Reed-Muller Codes," *IEEE Trans. Inform. Theory*, **45**, pp. 2397–2417, 1999.
[12] J. Dillon, "Elementary Hadamard Difference Sets",, *Ph.D. Dissertation*, Univ. Maryland, College Park, 1974.
[13] J.H.Evertse, "Linear Structures in Block Ciphers", *Advances in Cryptology - EUROCRYPT'87, Lecture Notes in Computer Science, Springer-Verlag*, **304**, pp. 249–266, 1987.
[14] D.G. Glynn, "On Self-Dual Quantum Codes and Graphs," submitted to *Elect. J. Combinatorics*, preprint at: http://homepage.mac.com/dglynn/quantum_files/Personal3.html, Apr. 2002.
[15] D.G. Glynn, T.A. Gulliver, J.G. Maks and M.K. Gupta, *The Geometry of Additive Quantum Codes - Connections with Finite Geometry,* Springer-Verlag, 2004.
[16] D. Gottesman, "Stabilizer Codes and Quantum Error Correction," *Ph.D. Thesis, Calif. Ins. Tech.*, http://xxx.soton.ac.uk/abs/quant-ph/?9705052, 1997.
[17] M. Grassl, "Bounds on dmin for additive $[[n,k,d]]$ QECC,", http://iaks-www.ira.uka.de/home/grassl/QECC/TableIII.html, Feb. 2003.
[18] M. Grassl, A. Klappenecker and M. Rotteler, "Graphs, Quadratic Forms, and Quantum Codes," Proc. *IEEE Int. Symp. Inform. Theory*, July 2002.
[19] T.A. Gulliver, R. Kristiansen and M.G. Parker, "The Multi-Dimensional Aperiodic Merit Factor of Binary Sequences," (preprint), 2003.
[20] T.A. Gulliver and J-L. Kim, "Circulant Based Extremal Additive Self-Dual Codes over GF(4)", *IEEE Trans. Inform. Theory*, **50**, pp. 359–366, Feb. 2004.
[21] M. Hein, J. Eisert and H.J. Briegel, "Multi-Party Entanglement in Graph States", *Phys. Rev. A*, **69**, 6, 2004. Preprint: http://xxx.soton.ac.uk/abs/quant-ph/0307130.
[22] G. Hohn, "Self-Dual Codes over the Kleinian Four Group," Mathematische Annalen, **327**, pp. 227–255, 2003.
[23] A. Klappenecker and M. Rötteler, "Clifford Codes", Chapter 10 in *Mathematics of Quantum Computing*, R. Brylinski and G. Chen (eds.), Chapman & Hall/CRC Press, pp. 253–273, 2002.
[24] K. Kurosawa and T. Satoh, "Design of SAC/PC(l) of Order k Boolean Functions and Three Other Cryptographic Criteria", Proc. *EUROCRYPT'97, Lecture Notes in Computer Science, Springer-Verlag*, **1233**, pp. 434–449, 1997.
[25] M. Matsui, "New Block Encryption Algorithm MISTY", *Fast Software Encryption Workshop*, Jan. 1997.
[26] B. McKay, "nauty", http://cs.anu.edu.au/ bdm/nauty/, 1994–2003.
[27] National Bureau of Standards, "Data Encryption Standards", *FIPS Publication 46*, U.S. Dept. of Commerce, 1977.
[28] M.G. Parker and V. Rijmen, "The Quantum Entanglement of Binary and Bipolar Sequences," short version in *Sequences and Their Applications*, Discrete Mathematics and Theoretical Computer Science Series, Springer-Verlag, 2001, long version at http://xxx.soton.ac.uk/abs/quant-ph/?0107106 or http://www.ii.uib.no/~matthew/BergDM2.ps, June 2001.
[29] M.G. Parker, "Generalised S-Box Nonlinearity", *NESSIE Public Document - NES/DOC/UIB/WP5/020/A*, https://www.cosic.esat.kuleuven.ac.be/nessie/reports/phase2/SBoxLin.pdf 2003.
[30] B. Preneel, W. Van Leekwijck, L. Van Linden, R. Govaerts and J. Vandewalle, "Propagation Characteristics of Boolean Functions," Proc. *EUROCRYPT'90, Lecture Notes in Computer Science*, **473**, pp. 161–173, 1991.
[31] C. Riera, G. Petrides, and M.G. Parker, "Generalised Bent Criteria for Quadratic Boolean Functions", (in preparation), 2004.
[32] V. Rijmen and P.S.L.M. Barreto, "The KHAZAD Block Cipher," *The Perl Journal*, 2003.
[33] D. Schlingemann and R.F. Werner, "Quantum error-correcting codes associated with graphs", *Phys. Rev. A*, **65**, 2002, http://xxx.soton.ac.uk/abs/quant-ph/?0012111, Dec. 2000.
[34] A. Shafieinezhad, F. Hendessi and T.A. Gulliver, "A Structure for Fast Data Encryption", *Preprint*, 2004
[35] N.J.A. Sloane, "The On-Line Encyclopedia of Integer Sequences", http://www.research.att.com/~njas/sequences/.
[36] F.X. Standaert, G. Rouvroy, G. Piret, J.J. Quisquater and J.D. Legat, "Key-Dependent Approximations in Cryptanalysis", *Proc. Symp. on Inform. Theory in the Benelux, Veldhoven, Netherlands* May 2003.
[37] V.D. Tonchev, "Error-Correcting Codes from Graphs", *Discrete Math.*, **257**, pp. 549–557, 2002.
[38] M. Van den Nest, J. Dehaene and B. De Moor, "Graphical description of the action of local Clifford transformations on graph states,", *Phys. Rev. A*, **69**, 2, 2004. Preprint: http://xxx.soton.ac.uk/abs/quant-ph/?0308151.

linear space of SBox	autocorrelation	Differential Weight 1	2	3	4	5	6	7	8	9
AES [8]	periodic	0.56	0.56	0.56	0.56	0.56	0.56	0.56	0.56	
(8×8)	aperiodic	0.56	0.66	0.81	0.94	1.00	1.00	1.00	1.00	
	fixed-aperiodic	0.56	0.66	0.81	1.00	1.00	1.00	1.00	1.00	
Khazad [32]	periodic	0.67	0.67	0.69	0.70	0.67	0.67	0.66	0.63	
(8×8)	aperiodic	0.67	0.77	0.94	1.00	1.00	1.00	1.00	1.00	
	fixed-aperiodic	0.67	0.77	0.94	1.00	1.00	1.00	1.00	1.00	
Whirlpool [1]	periodic	0.66	0.69	0.67	0.69	0.66	0.67	0.66	0.64	
(8×8)	aperiodic	0.66	0.75	0.84	1.00	1.00	1.00	1.00	1.00	
	fixed-aperiodic	0.66	0.78	0.91	1.00	1.00	1.00	1.00	1.00	
Misty1 [25]	periodic	0.56	0.56	0.56	0.56	0.56	0.56	0.56		
(7×7)	aperiodic	0.56	0.75	0.75	1.00	1.00	1.00	1.00		
	fixed-aperiodic	0.56	0.75	1.00	1.00	1.00	1.00	1.00		
Misty1	periodic	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
(9×9)	aperiodic	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
	fixed-aperiodic	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
DES-1 [27]	periodic	0.88	0.81	0.81	0.81	0.75	0.69			
(6×4)	aperiodic	0.88	0.94	1.00	1.00	1.00	1.00			
	fixed-aperiodic	0.88	1.00	1.00	1.00	1.00	1.00			
DES-2	periodic	0.94	0.81	0.81	0.81	0.88	0.75			
(6×4)	aperiodic	0.94	0.94	1.00	1.00	1.00	1.00			
	fixed-aperiodic	0.94	1.00	1.00	1.00	1.00	1.00			
DES-3	periodic	0.88	0.75	0.81	0.81	0.75	0.69			
(6×4)	aperiodic	0.88	0.88	1.00	1.00	1.00	1.00			
	fixed-aperiodic	0.88	1.00	1.00	1.00	1.00	1.00			
DES-4	periodic	1.00	0.75	0.75	1.00	1.00	0.75			
(6×4)	aperiodic	1.00	1.00	1.00	1.00	1.00	1.00			
	fixed-aperiodic	1.00	1.00	1.00	1.00	1.00	1.00			
DES-5	periodic	0.81	0.81	0.81	0.81	0.75	0.63			
(6×4)	aperiodic	0.81	0.94	1.00	1.00	1.00	1.00			
	fixed-aperiodic	0.81	1.00	1.00	1.00	1.00	1.00			
DES-6	periodic	0.81	0.88	0.81	0.81	0.81	0.69			
(6×4)	aperiodic	0.81	0.94	1.00	1.00	1.00	1.00			
	fixed-aperiodic	0.81	1.00	1.00	1.00	1.00	1.00			
DES-7	periodic	0.88	0.88	0.81	0.81	0.81	0.69			
(6×4)	aperiodic	0.88	1.00	1.00	1.00	1.00	1.00			
	fixed-aperiodic	0.88	1.00	1.00	1.00	1.00	1.00			
DES-8	periodic	0.88	0.88	0.81	0.81	0.75	0.75			
(6×4)	aperiodic	0.88	0.94	1.00	1.00	1.00	1.00			
	fixed-aperiodic	0.88	1.00	1.00	1.00	1.00	1.00			
FDE-1 [34]	periodic	0.69	0.88	0.88	0.88	0.75	0.63			
(6×4)	aperiodic	0.69	1.00	1.00	1.00	1.00	1.00			
	fixed-aperiodic	0.69	1.00	1.00	1.00	1.00	1.00			
FDE-2	periodic	0.69	0.69	0.75	0.75	0.75	0.63			
(6×4)	aperiodic	0.69	0.81	1.00	1.00	1.00	1.00			
	fixed-aperiodic	0.69	0.88	1.00	1.00	1.00	1.00			
FDE-3	periodic	0.75	0.75	0.75	0.69	0.69	0.75			
(6×4)	aperiodic	0.75	0.88	1.00	1.00	1.00	1.00			
	fixed-aperiodic	0.75	0.88	1.00	1.00	1.00	1.00			
FDE-4	periodic	0.81	0.75	0.81	0.81	0.75	0.63			
(6×4)	aperiodic	0.81	0.88	1.00	1.00	1.00	1.00			
	fixed-aperiodic	0.81	1.00	1.00	1.00	1.00	1.00			
FDE-5	periodic	0.75	0.69	0.75	0.75	0.69	0.69			
(6×4)	aperiodic	0.75	0.94	1.00	1.00	1.00	1.00			
	fixed-aperiodic	0.75	0.94	1.00	1.00	1.00	1.00			
FDE-6	periodic	0.75	0.75	0.75	0.75	0.75	0.63			
(6×4)	aperiodic	0.75	0.81	1.00	1.00	1.00	1.00			
	fixed-aperiodic	0.75	0.88	1.00	1.00	1.00	1.00			
FDE-7	periodic	0.75	0.75	0.75	0.75	0.69	0.69			
(6×4)	aperiodic	0.75	0.88	1.00	1.00	1.00	1.00			
	fixed-aperiodic	0.75	0.88	1.00	1.00	1.00	1.00			
FDE-8	periodic	0.69	0.75	0.75	0.81	0.75	0.63			
(6×4)	aperiodic	0.69	0.88	1.00	1.00	1.00	1.00			
	fixed-aperiodic	0.69	0.88	1.00	1.00	1.00	1.00			
[[6,0,4]]	periodic	0.50	0.50	0.50	1.00	0.50	0.50			
hexacode	aperiodic	0.50	0.50	0.50	1.00	0.50	1.00			
(single function)	fixed-aperiodic	0.50	0.50	0.50	1.00	1.00	1.00			

TABLE I

Periodic, Aperiodic, and Fixed-Aperiodic Autocorrelation Biases for Selected S-Boxes