Aperiodic propagation criteria for Boolean functions

Lars Eirik Danielsen [a], T. Aaron Gulliver [b],
Matthew G. Parker [a,*]

[a] *The Selmer Center, Department of Informatics, University of Bergen, PB 7800, N-5020 Bergen, Norway.*

[b] *Dept. of Elec. & Computer Eng., University of Victoria, P.O. Box 3055 STN CSC, Victoria, B.C. Canada, V8W 3P6*

Abstract

We characterise the *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 the *Extended Propagation Criteria* (EPC) 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.

Key words: Propagation criteria; Differential cryptanalysis; Aperiodic autocorrelation; Quantum error-correcting codes; Boolean functions; Graph theory; Quantum entanglement

1 Introduction

Imagine the block cipher scenario where an attacker has knowledge of the values of a fixed subset, $\boldsymbol{\mu}$, of the plaintext bits and any subset of the ciphertext

* Corresponding author.
Email addresses: larsed@ii.uib.no (Lars Eirik Danielsen), agullive@ece.uvic.ca (T. Aaron Gulliver), matthew@ii.uib.no (Matthew G. Parker).
URLs: http://www.ii.uib.no/~larsed/ (Lars Eirik Danielsen), http://www.ece.uvic.ca/~agullive/ (T. Aaron Gulliver), http://www.ii.uib.no/~matthew/ (Matthew G. Parker).

bits, for multiple plaintext/ciphertext pairs. Moreover he is able to modify any of the plaintext bits from the set $\boldsymbol{\mu}$, in order to realise a differential attack on the cipher. For a given cipher, what is the smallest size of $\boldsymbol{\mu}$ 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 $\boldsymbol{\mu}$ 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, $\boldsymbol{\mu}$, of the plaintext bits, and he is able to modify any subset, $\boldsymbol{a}$, of the plaintext bits, but this time $\boldsymbol{a}$ is not necessarily a subset of $\boldsymbol{\mu}$. For a given cipher, and for a given size for $\boldsymbol{a}$, what is the smallest size for $\boldsymbol{\mu}$ such that a biased differential can be established across the cipher? Preneel et al. [33] 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 cannot be found if $\boldsymbol{\mu}$ is of size q or less given that $\boldsymbol{a}$ is of size l or less. To ease comparison with APC, we further propose *EPC distance* to be the minimum size of $\boldsymbol{\mu} \cup \boldsymbol{a}$ such that a biased differential can be found. EPC is also considered in [8, 26].

One purpose of this paper is 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. [33] 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 of m variables as a quantum state of m qubits, we also establish, rather surprisingly, that the APC distance of a quadratic Boolean function is equal to the minimum distance of an associated zero-dimensional *quantum error-correcting code* (QECC) which represents, in turn, a highly-entangled pure quantum state [23]. We apply recent results on quantum codes to the construction of quadratic Boolean functions with favourable APC. This suggests that the disciplines of *quantum entanglement* and cryptographic criteria for Boolean functions are closely related [32]. 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 *local complementation* (LC) operations on associated graphs [3, 18, 19, 42]. These graph operations encode the action of a special subset of the local

unitary transforms. Similarly, APC distance-invariant orbits of functions of algebraic degree greater than two can also be generated by application of the same set of local unitary transforms. Therefore, a second purpose of this paper is to re-cast the construction of QECCs as a problem of construction of Boolean functions. As a result, we are able to generalise the set of QECCs to Boolean functions of degree greater than two, whereas conventional QECCs only map to Boolean functions of degree two.

This paper is structured as follows. After establishing the notation, we characterise the 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 LC symmetry. Finally we consider the challenging problem of finding constructions for Boolean functions of algebraic degree greater than two with favourable APC, and we describe the generalisation of LC 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.

2 Preliminaries

Let $\mathcal{B}_m$ denote the set of all Boolean functions on m variables. For $\boldsymbol{a} = (a_0, a_1, \ldots, a_{m-1}) \in \mathbb{F}_2^m$, the *Hamming weight* of $\boldsymbol{a}$ is

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

We define the operators $\overline{\ } : \mathbb{F}_2^m \to \mathbb{F}_2^m$, and $\& : \mathbb{F}_2^m \times \mathbb{F}_2^m \to \mathbb{F}_2^m$ as bitwise negation and modular multiplication modulo 2, respectively. Let $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c} \in \mathbb{F}_2^m$, then

$$\boldsymbol{c} = \boldsymbol{a} \,\&\, \boldsymbol{b} \quad \Rightarrow \quad c_i = a_i b_i, \ \forall i, \ 0 \le i < m. \tag{2}$$

$$\boldsymbol{c} = \overline{\boldsymbol{a}} \quad \Rightarrow \quad c_i = a_i + 1, \ \forall i, \ 0 \le i < m. \tag{3}$$

Let $\boldsymbol{a}, \boldsymbol{b} \in \mathbb{F}_2^m$, then

$$\boldsymbol{b} \preceq \boldsymbol{a} \quad \Leftrightarrow \quad b_i \le a_i, \ \forall i, \ 0 \le i < m, \tag{4}$$

and we say that $\boldsymbol{a}$ *covers* $\boldsymbol{b}$.

The *dual*, $V^{\perp}$, of a subspace $V \subset \mathbb{F}_2^m$ can be described relative to the scalar product,

$$V^{\perp} = \{\boldsymbol{x} \in F_2^m \mid \boldsymbol{x} \cdot \boldsymbol{y} = 0,\ \boldsymbol{y} \in V\}. \tag{5}$$

In particular, for $\boldsymbol{r} \in \mathbb{F}_2^m$, we define $V_{\boldsymbol{r}}$ as

$$V_{\boldsymbol{r}} = \{\boldsymbol{x} \in \mathbb{F}_2^m \mid \boldsymbol{x} \preceq \boldsymbol{r}\}. \tag{6}$$

Moreover, for any $\boldsymbol{k} \in \mathbb{F}_2^m$, $\boldsymbol{k} + V$ defines a *coset* of V.

Let E be any subset of $\mathbb{F}_2^m$. For any $f \in \mathcal{B}_m$ we define $f\phi_E$ as the *restriction* of f to E such that $f\phi_E(\boldsymbol{x}) = 1$ iff $f(\boldsymbol{x}) = 1$ and $\boldsymbol{x} \in E$. If E is a k-dimensional linear subspace of $\mathbb{F}_2^m$ then, for any coset, $\boldsymbol{b} + E$, we identify $f\phi_{\boldsymbol{b}+E}$ with a Boolean function in $\mathcal{B}_k$, where the function obtained depends on $\boldsymbol{b}$.

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

$$\mathcal{F}(f) = \sum_{\boldsymbol{x} \in \mathbb{F}_2^m} (-1)^{f(\boldsymbol{x})}. \tag{7}$$

If E is a k-dimensional linear subspace of $\mathbb{F}_2^m$ then, for any coset $\boldsymbol{b} + E$,

$$\mathcal{F}(f\phi_{\boldsymbol{b}+E}) = \sum_{\boldsymbol{x} \in \boldsymbol{b}+E} (-1)^{f(\boldsymbol{x})}. \tag{8}$$

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

$$\{\mathcal{F}(f + \boldsymbol{\alpha} \cdot \boldsymbol{x}),\ \boldsymbol{\alpha} \in \mathbb{F}_2^m\}. \tag{9}$$

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 $\mathcal{F}(f + \boldsymbol{\alpha} \cdot \boldsymbol{x}) = 0$ for any $\boldsymbol{\alpha} \in \mathbb{F}_2^m$ such that $1 \leq \mathrm{wt}(\boldsymbol{\alpha}) \leq t$. Moreover, if such an f is also balanced, it is said to be t-*resilient*. A* balanced *function with no correlation-immunity is 0-resilient.*

For any $f \in \mathcal{B}_m$ and $\boldsymbol{a} \in \mathbb{F}_2^m$, the *first derivative* of f with respect to $\boldsymbol{a}$ is given by $\mathcal{D}_{\boldsymbol{a}} f \in \mathcal{B}_m$, where

$$\mathcal{D}_{\boldsymbol{a}} f = f(\boldsymbol{x}) + f(\boldsymbol{x} + \boldsymbol{a}). \tag{10}$$

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

For $\boldsymbol{a}, \boldsymbol{k}, \boldsymbol{\mu} \in \mathbb{F}_2^m$, $\boldsymbol{a} \preceq \overline{\boldsymbol{\mu}}$, $\boldsymbol{k} \preceq \boldsymbol{\mu}$, the *fixed-periodic autocorrelation* coefficients, $p_{\boldsymbol{a},\boldsymbol{k},\boldsymbol{\mu}}$, of f after fixing the subspace $V_{\boldsymbol{\mu}}$ to $\boldsymbol{k}$, can be defined by

$$p_{\boldsymbol{a},\boldsymbol{k},\boldsymbol{\mu}} = \mathcal{F}(\mathcal{D}_{\boldsymbol{a}} f \phi_{\boldsymbol{k}+V_{\overline{\boldsymbol{\mu}}}}),\ \boldsymbol{a} \preceq \overline{\boldsymbol{\mu}},\ \boldsymbol{k} \preceq \boldsymbol{\mu}. \tag{11}$$

When $\boldsymbol{\mu} = 0$ there is no subspace fixing, and (11) simplifies to the *periodic autocorrelation* of f, given by

$$p_{\boldsymbol{a}} = \mathcal{F}(\mathcal{D}_{\boldsymbol{a}} f). \tag{12}$$

Definition 2 ([33]) *Let $E \subset \mathbb{F}_2^m$. The function $f \in \mathcal{B}_m$ satisfies the (periodic)* Propagation Criteria *(PC) with respect to E if, for all $\boldsymbol{e} \in E$, $p_{\boldsymbol{e}} = 0$. The function f satisfies PC of degree l and order q (also denoted* PC(l) *of order q) for some positive integers l and q if $p_{\boldsymbol{a},\boldsymbol{k},\boldsymbol{\mu}} = 0$ for any $\boldsymbol{a}, \boldsymbol{k}, \boldsymbol{\mu} \in \mathbb{F}_2^m$ such that $\boldsymbol{a} \preceq \overline{\boldsymbol{\mu}}$, $\boldsymbol{k} \preceq \boldsymbol{\mu}$, $1 \leq \mathrm{wt}(\boldsymbol{a}) \leq l$ and $0 \leq \mathrm{wt}(\boldsymbol{\mu}) \leq q$. For $q = 0$ we abbreviate, saying that f satisfies* PC(l).

3 Aperiodic Autocorrelation of a Boolean Function

For $\boldsymbol{a}, \boldsymbol{k}, \boldsymbol{\mu} \in \mathbb{F}_2^m$, $\boldsymbol{a}, \boldsymbol{k} \preceq \boldsymbol{\mu}$, and $\boldsymbol{\theta} = \boldsymbol{\mu} + \boldsymbol{a}$, where $\boldsymbol{\theta}$ and $\boldsymbol{a}$ are disjoint, the *fixed-aperiodic autocorrelation* coefficients of f after fixing the subspace $V_{\boldsymbol{\theta}}$ to $\boldsymbol{k} \,\&\, \boldsymbol{\theta}$ are defined by

$$u_{\boldsymbol{a},\boldsymbol{k},\boldsymbol{\mu}} = \mathcal{F}(\mathcal{D}_{\boldsymbol{a}} f \phi_{\boldsymbol{k}+V_{\overline{\boldsymbol{\mu}}}}),\ \boldsymbol{a}, \boldsymbol{k} \preceq \boldsymbol{\mu}. \tag{13}$$

The only difference between (11) and (13) is that, for the fixed-periodic case, $\boldsymbol{a} \preceq \overline{\boldsymbol{\mu}}$ whereas, for the fixed-aperiodic case, $\boldsymbol{a} \preceq \boldsymbol{\mu}$. For (11), $(\mathcal{D}_{\boldsymbol{a}} f)\phi_{\boldsymbol{k}+V_{\overline{\boldsymbol{\mu}}}} = \mathcal{D}_{\boldsymbol{a}}(f\phi_{\boldsymbol{k}+V_{\overline{\boldsymbol{\mu}}}})$, but this is ill-defined for (13). Note that "knowledge of the values of a fixed subset, $\boldsymbol{\mu}$", as stated in Section 1, is here characterised by fixed values of $\boldsymbol{k}$, where $\boldsymbol{k}$ is covered by $\boldsymbol{\mu}$.

When $\boldsymbol{\mu} = \boldsymbol{a}$ there are no additional fixed values, and (13) simplifies to the *aperiodic autocorrelation* of f, given by

$$u_{\boldsymbol{a},\boldsymbol{k}} = \mathcal{F}(\mathcal{D}_{\boldsymbol{a}} f \phi_{\boldsymbol{k}+V_{\overline{\boldsymbol{a}}}}),\ \boldsymbol{k} \preceq \boldsymbol{a}. \tag{14}$$

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 $\sum_{\boldsymbol{a} \in \mathbb{F}_2^m} 2^{\mathrm{wt}(\boldsymbol{a})} = 3^m$ coefficients $u_{\boldsymbol{a},\boldsymbol{k}}$ and $\sum_{\boldsymbol{\mu} \in \mathbb{F}_2^m} 2^{2\,\mathrm{wt}(\boldsymbol{\mu})} = 5^m$ coefficients $u_{\boldsymbol{a},\boldsymbol{k},\boldsymbol{\mu}}$. In fact, for autocorrelations of real functions, $\mathbb{F}_2^m \to \mathbb{R}$, there are only a maximum of $\frac{3^m}{2}$ and $\frac{5^m}{2}$ different values for $u_{\boldsymbol{a},\boldsymbol{k}}$ and $u_{\boldsymbol{a},\boldsymbol{k},\boldsymbol{\mu}}$, 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. [33], and investigated by Carlet [8]. However, the aperiodic property is more accurately characterised by a criteria we define as *Aperiodic Propagation Criteria* (APC). We first explain why (13) is an aperiodic (non-modular) metric, and we later return to the definitions of both APC and EPC.

Proposition 3 *The periodic autocorrelations of* (11) *and* (12) *can be expressed as modular (periodic) multivariate polynomial multiplications, and the aperiodic autocorrelations of* (13) *and* (14) *can be expressed as non-modular (aperiodic) multivariate polynomial multiplications.*

PROOF. Let $p_{\boldsymbol{a}}$ and $u_{\boldsymbol{a},\boldsymbol{k}}$ be as defined in (12) and (14), respectively. Let $\boldsymbol{z} \in \mathbb{C}^m$. Define $v(\boldsymbol{z})$, $P(\boldsymbol{z})$, and $A(\boldsymbol{z})$ as

$$v(\boldsymbol{z}) = \sum_{\boldsymbol{x} \in \mathbb{F}_2^m} (-1)^{f(\boldsymbol{x})} \prod_{i \in \mathbb{Z}_m} z_i^{x_i}, \tag{15}$$

$$P(\boldsymbol{z}) = \sum_{\boldsymbol{a} \in \mathbb{F}_2^m} p_{\boldsymbol{a}} \prod_{i \in \mathbb{Z}_m} z_i^{a_i}, \tag{16}$$

$$A(\boldsymbol{z}) = \sum_{\boldsymbol{k},\boldsymbol{a} \in \mathbb{F}_2^m, \boldsymbol{k} \preceq \boldsymbol{a}} u_{\boldsymbol{a},\boldsymbol{k}} \prod_{i \in \mathbb{Z}_m} z_i^{a_i (-1)^{k_i}}. \tag{17}$$

Let $\boldsymbol{z}^{-1} = (z_0^{-1}, z_1^{-1}, \ldots, z_{m-1}^{-1})$. Then an expansion verifies the following modular and non-modular relationships for $P(\boldsymbol{z})$ and $A(\boldsymbol{z})$.

$$P(\boldsymbol{z}) = v(\boldsymbol{z}) v(\boldsymbol{z}^{-1}) \pmod{\prod_{i \in \mathbb{Z}_m} (z_i^2 - 1)}, \tag{18}$$

$$A(\boldsymbol{z}) = v(\boldsymbol{z}) v(\boldsymbol{z}^{-1}). \tag{19}$$

The above argument carries over simply to (11) (resp. (13)) by first fixing a subspace $V_{\boldsymbol{\mu}}$ (resp. $V_{\boldsymbol{\theta}}$), then computing a modular (resp. non-modular) polynomial multiplication over the remaining subspace. □

For $\boldsymbol{a}, \boldsymbol{c} \in \mathbb{F}_2^m$, define $G_{\boldsymbol{a},\boldsymbol{c}}$ as the Fourier spectrum of $\mathcal{D}_{\boldsymbol{a}} f$, so that

$$G_{\boldsymbol{a},\boldsymbol{c}} = \mathcal{F}(\mathcal{D}_{\boldsymbol{a}} f + \boldsymbol{c} \cdot \boldsymbol{x}). \tag{20}$$

The fixed-aperiodic autocorrelation of f after fixing a subspace, $V_{\boldsymbol{\theta}}$, is equivalent to a subspace Fourier transform of the Fourier transform of the first derivatives of f, as in the following proposition.

Proposition 4

$$u_{\boldsymbol{a},\boldsymbol{k},\boldsymbol{\mu}} = 2^{-\operatorname{wt}(\boldsymbol{\mu})} \sum_{\boldsymbol{c} \preceq \boldsymbol{\mu}} G_{\boldsymbol{a},\boldsymbol{c}} (-1)^{\boldsymbol{k} \cdot \boldsymbol{c}}, \ \boldsymbol{a}, \boldsymbol{k} \preceq \boldsymbol{\mu}, \tag{21}$$

$$G_{\boldsymbol{a},\boldsymbol{c}} = \sum_{\boldsymbol{k} \preceq \boldsymbol{\mu}} u_{\boldsymbol{a},\boldsymbol{k},\boldsymbol{\mu}} (-1)^{\boldsymbol{c} \cdot \boldsymbol{k}}, \ \boldsymbol{a}, \boldsymbol{c} \preceq \boldsymbol{\mu}, \tag{22}$$

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

PROOF. See Appendix A. □

The relationship between aperiodic autocorrelation and its constituent periodic and negaperiodic autocorrelations is described in subsection B.1 of Appendix B, and the relationships to the second derivative are described in subsection B.2 of the same appendix.

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

$$\sum_{\boldsymbol{k} \preceq \boldsymbol{\mu}} |u_{\boldsymbol{a},\boldsymbol{k},\boldsymbol{\mu}}|^2 = 2^{-\operatorname{wt}(\boldsymbol{\mu})} \sum_{\boldsymbol{c} \preceq \boldsymbol{\mu}} |G_{\boldsymbol{a},\boldsymbol{c}}|^2 \tag{23}$$

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

$$\sigma_{\boldsymbol{a},\boldsymbol{\mu}} = \sum_{\boldsymbol{k} \preceq \boldsymbol{\mu}} |u_{\boldsymbol{a},\boldsymbol{k},\boldsymbol{\mu}}|^2. \tag{24}$$

By summing over all $\boldsymbol{a}, \boldsymbol{\mu} \in \mathbb{F}_2^m$ where $\boldsymbol{a} \preceq \boldsymbol{\mu}$, we arrive at an expression for the *complete fixed-aperiodic sum-of-squares*, $\mathcal{E}$, for f, where

$$2\mathcal{E} + 6^n = \sum_{\boldsymbol{\mu} \in \mathbb{F}_2^m} \sum_{\boldsymbol{a} \preceq \boldsymbol{\mu}} \sigma_{\boldsymbol{a},\boldsymbol{\mu}} = \sum_{\boldsymbol{\mu} \in \mathbb{F}_2^m} \sum_{\boldsymbol{a},\boldsymbol{k} \preceq \boldsymbol{\mu}} |u_{\boldsymbol{a},\boldsymbol{k},\boldsymbol{\mu}}|^2 \tag{25}$$

When $\boldsymbol{a} = \boldsymbol{\mu}$, the above expression simplifies to the *aperiodic sum-of-squares*, σ, where

$$2\sigma + 4^n = \sum_{\boldsymbol{a} \in \mathbb{F}_2^m} \sigma_{\boldsymbol{a}} = \sum_{\boldsymbol{a} \in \mathbb{F}_2^m} \sum_{\boldsymbol{k} \preceq \boldsymbol{a}} |u_{\boldsymbol{a},\boldsymbol{k}}|^2. \tag{26}$$

The aperiodic sum-of-squares, and the complete fixed-aperiodic sum-of-squares, have been investigated in [22] and [31], resp., where recursions in σ and $\mathcal{E}$, resp., have been established for certain infinite quadratic Boolean constructions [1]. Of significant interest in this paper are the choices for $\boldsymbol{a}$ and $\boldsymbol{\mu}$ such that $\sigma_{\boldsymbol{a},\boldsymbol{\mu}} = 0$, in particular for the cases where $\operatorname{wt}(\boldsymbol{\mu})$ is small. To this end we define the *Aperiodic Propagation Criteria* as follows.

Definition 5 *The function $f \in \mathcal{B}_m$ satisfies the* Aperiodic Propagation Criteria *(APC) of degree l and order q (also denoted* APC(l) *of order q), for some positive integers l and q if $u_{\boldsymbol{a},\boldsymbol{k},\boldsymbol{\mu}} = 0$ for any $\boldsymbol{a}, \boldsymbol{k}, \boldsymbol{\mu} \in \mathbb{F}_2^m$ such that $\boldsymbol{a}, \boldsymbol{k} \preceq \boldsymbol{\mu}$, $\boldsymbol{\mu} = \boldsymbol{a} + \boldsymbol{\theta}$, $1 \leq \operatorname{wt}(\boldsymbol{a}) \leq l$ and $0 \leq \operatorname{wt}(\boldsymbol{\theta}) \leq q$, where $\boldsymbol{a}$ and $\boldsymbol{\theta}$ 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 $\boldsymbol{x} = \{x_i\}$ be the complete set of input bits. let $\boldsymbol{x}_{\boldsymbol{\mu}}, \boldsymbol{x}_{\boldsymbol{a}} \subseteq \boldsymbol{x}$ be such that $\boldsymbol{x}_{\boldsymbol{a}} \subseteq \boldsymbol{x}_{\boldsymbol{\mu}}$, $|\boldsymbol{x}_{\boldsymbol{\mu}}| \leq q + |\boldsymbol{x}_{\boldsymbol{a}}|$, and $|\boldsymbol{x}_{\boldsymbol{a}}| \leq l$. Then a Boolean function, f, satisfies APC(l) of order q if, for every possible $\boldsymbol{x}_{\boldsymbol{\mu}}, \boldsymbol{x}_{\boldsymbol{a}}$ pair, knowledge

[1] The factor of 2 on the left-hand sides of (25) and (26) reflects the fact that, for real functions, $\mathbb{F}_2^m \to \mathbb{R}$, we have $u_{\boldsymbol{a},\boldsymbol{k},\boldsymbol{\mu}} = u_{\boldsymbol{a},\bar{\boldsymbol{k}},\boldsymbol{\mu}}$ and $u_{\boldsymbol{a},\boldsymbol{k}} = u_{\boldsymbol{a},\bar{\boldsymbol{k}}}$, respectively. Moreover, 6^n and 4^n represent the zero-shift contributions.

of the bits in $\boldsymbol{x}_{\boldsymbol{\mu}}$ gives no information as to the values of the function $\mathcal{D}_{\boldsymbol{a}}f$, where $a_i = 1$ iff $x_i \in \boldsymbol{x}_{\boldsymbol{a}}$. This definition is very similar but not identical to the *Extended Propagation Criteria* (EPC) originally defined by Preneel et al. [33]. In order to define EPC, we first define *extended autocorrelation*.

For $\boldsymbol{a}, \boldsymbol{k}, \boldsymbol{\mu} \in \mathbb{F}_2^m$, $\boldsymbol{k} \preceq \boldsymbol{\mu}$, and $\boldsymbol{\theta} \preceq \boldsymbol{\mu}$, the *fixed-extended autocorrelation* coefficients of f after fixing the subspace, $V_{\boldsymbol{\theta}}$, to $\boldsymbol{k} \,\&\, \boldsymbol{\theta}$, are defined by

$$v_{\boldsymbol{a},\boldsymbol{k},\boldsymbol{\mu}} = \mathcal{F}(\mathcal{D}_{\boldsymbol{a}} f \phi_{\boldsymbol{k}+V_{\overline{\boldsymbol{\mu}}}}),\ \boldsymbol{k} \preceq \boldsymbol{\mu}. \tag{27}$$

When $\boldsymbol{\mu} \preceq \boldsymbol{a}$, (27) simplifies to the *extended autocorrelation* of f, given by

$$v_{\boldsymbol{a},\boldsymbol{k}} = \mathcal{F}(\mathcal{D}_{\boldsymbol{a}} f \phi_{\boldsymbol{k}+V_{\overline{\boldsymbol{\mu}}}}),\ \boldsymbol{k} \preceq \boldsymbol{a}. \tag{28}$$

Note that

$$u_{\boldsymbol{a},\boldsymbol{k},\boldsymbol{\mu}} = v_{\boldsymbol{a},\boldsymbol{k},\boldsymbol{\mu}},\ \boldsymbol{a} \preceq \boldsymbol{\mu}, \tag{29}$$

$$u_{\boldsymbol{a},\boldsymbol{k}} = v_{\boldsymbol{a},\boldsymbol{k}},\ \boldsymbol{a} = \boldsymbol{\mu}, \tag{30}$$

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

Definition 6 ([33]) *The function $f \in \mathcal{B}_m$ satisfies the* Extended Propagation Criteria *(EPC) of degree l and order q (also denoted* EPC(l) *of order q) for some positive integers l and q if $v_{\boldsymbol{a},\boldsymbol{k},\boldsymbol{\mu}} = 0$ for any $\boldsymbol{a}, \boldsymbol{k}, \boldsymbol{\mu} \in \mathbb{F}_2^m$, such that $\boldsymbol{k} \preceq \boldsymbol{\mu}$, $1 \le \mathrm{wt}(\boldsymbol{a}) \le l$ and $0 \le \mathrm{wt}(\boldsymbol{\mu}) \le q$. For $q = 0$ we abbreviate, saying that f satisfies* EPC(l). [2]

An intuitive reason for the usefulness of EPC in a classical cryptographic context is as follows [8,33]. Let $\boldsymbol{x} = \{x_i\}$ be the complete set of input bits. Let $\boldsymbol{x}_{\boldsymbol{\mu}}, \boldsymbol{x}_{\boldsymbol{a}} \subseteq \boldsymbol{x}$ be such that $|\boldsymbol{x}_{\boldsymbol{\mu}}| \le q$, and $|\boldsymbol{x}_{\boldsymbol{a}}| \le l$. Then a Boolean function, f, satisfies EPC(l) of order q if, for every possible $\boldsymbol{x}_{\boldsymbol{\mu}}, \boldsymbol{x}_{\boldsymbol{a}}$ pair, knowledge of the bits in $\boldsymbol{x}_{\boldsymbol{\mu}}$ gives no information as to the values of the function $\mathcal{D}_{\boldsymbol{a}}f$, where $a_i = 1$ iff $x_i \in \boldsymbol{x}_{\boldsymbol{a}}$.

The essential difference between APC and EPC is that, for APC the bits in the set $\boldsymbol{x}_{\boldsymbol{a}}$ 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 $\boldsymbol{x}_{\boldsymbol{a}}$ 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.

[2] There appears to be some disagreement in the literature regarding the distinction between PC and EPC, and the reader should be aware that some papers (e.g. [26]) refer to EPC(l) of order k as PC(l) of order k.

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

Definition 7 *The function $f \in \mathcal{B}_m$ has* APC distance d *if it satisfies* APC(l) *of order q for all positive integers, l, q, such that $d > l + q$.*

Definition 8 *The function $f \in \mathcal{B}_m$ has* EPC distance d *if it satisfies* EPC(l) *of order q for all positive integers, l, q, such that $d > l + q$.*

The following is easily verified from (29).

$$\text{APC distance}(f) \leq \text{EPC distance}(f) \tag{31}$$

Computational results suggest that, for most Boolean functions of a small number of variables, the two distances are equal. A counterexample is the *clique function*, $f = \sum_{i<j} x_i x_j$. 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, $u_{\boldsymbol{a},\boldsymbol{k},\boldsymbol{\mu}}$, but can also be defined in terms of $G_{\boldsymbol{a},\boldsymbol{c}}$. From (23) we have the following two-way implication, where $\boldsymbol{a} \preceq \boldsymbol{\mu}$.

$$u_{\boldsymbol{a},\boldsymbol{k},\boldsymbol{\mu}} = 0, \ \forall \boldsymbol{k} \preceq \boldsymbol{\mu} \quad \Leftrightarrow \quad G_{\boldsymbol{a},\boldsymbol{c}} = 0, \ \forall \boldsymbol{c} \preceq \boldsymbol{\mu}. \tag{32}$$

Preneel et al. [33] and Carlet [8] have given spectral characterisations of the EPC in terms of the Fourier transform of $\mathcal{D}_{\boldsymbol{a}} f$. We now re-express this characterisation in terms of the EPC distance and resilience of $\mathcal{D}_{\boldsymbol{a}} f$.

Corollary 9 *f has EPC distance d if and only if $\mathcal{D}_{\boldsymbol{a}} f$ is $(d - \text{wt}(\boldsymbol{a}) - 1)$-resilient for all $\boldsymbol{a}$ where $\text{wt}(\boldsymbol{a}) < d$.*

Using (31) we obtain the following corollary.

Corollary 10 *If f has APC distance d, then $\mathcal{D}_{\boldsymbol{a}} f$ is $(d - \text{wt}(\boldsymbol{a}) - 1)$-resilient for all $\boldsymbol{a}$ where $\text{wt}(\boldsymbol{a}) < d$.*

If $\mathcal{D}_{\boldsymbol{a}} f$ is $(d - \text{wt}(\boldsymbol{a}) - 1)$-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 distance is slightly stricter than EPC distance[3] and both are much stricter criteria than PC. For example, it is easily verified that the *hyper-bent* function $f = x_0x_1x_2 + x_0x_1x_5 + x_0x_2x_3 + x_0x_4x_5 + x_1x_2x_3 + x_1x_2x_4 +$

[3] Although the fixed-aperiodic autocorrelation coefficients are a subset of the extended autocorrelation coefficients (see (29)), the interpretation of the weight of the coefficient indices as a distance measure means that APC is stricter than EPC. More informally, EPC distance is weaker than APC distance because EPC double-counts (does not identify) the overlap between $\boldsymbol{\mu}$ and $\boldsymbol{a}$.

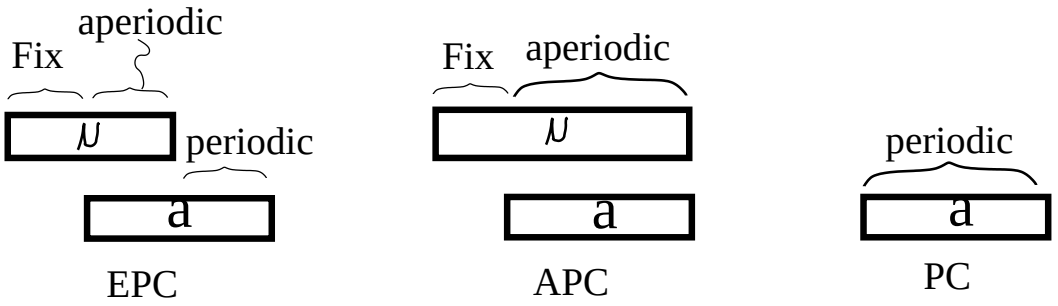

Fig. 1. Relative Scope of $\boldsymbol{\mu}$ and $\boldsymbol{a}$ for Extended, Aperiodic, and Periodic Autocorrelations

$x_1x_2x_5 + x_1x_3x_4 + x_1x_3x_5 + x_1x_4x_5 + x_2x_4x_5 + x_0x_3 + x_0x_5 + x_1x_4 + x_2x_3 + x_3x_4$ satisfies PC(6), but only APC(1), and further has both APC distance and EPC distance equal to 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 11 *Let f satisfy* PC(l) *of order q,* EPC(l') *of order q, and* APC(l'') *of order q. Then $l'' \leq l' \leq l$.*

Fig. 1 shows the scope of $\boldsymbol{\mu}$ and $\boldsymbol{a}$ for EPC, APC, and PC. Although EPC is more general then APC (because $\boldsymbol{a}$ is not necessarily a subset of $\boldsymbol{\mu}$), the "spectral region" examined by EPC is no bigger than for APC. In other words, for EPC, the part of $\boldsymbol{a}$ not covered by $\boldsymbol{\mu}$ is, in a sense, superfluous, as it refers only to the periodic autocorrelation, which is a spectral subset of the aperiodic autocorrelation [4]. APC, on the other hand, has no purely periodic part.

Here is a well-known quadratic construction [15] for $f \in \mathcal{B}_m$ which satisfies APC($\lfloor \frac{m}{2} \rfloor$).

Theorem 12 *Define $f \in \mathcal{B}_m$, $\boldsymbol{e} \in \mathbb{F}_2^m$, and $d \in \mathbb{F}_2$ such that*

$$f(\boldsymbol{x}) = \sum_{i=0}^{m-2} x_{\pi(i)}x_{\pi(i+1)} + \boldsymbol{e} \cdot \boldsymbol{x} + d, \tag{33}$$

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

PROOF. See Appendix A. □

[4] By "spectral region" we mean that the $u_{\boldsymbol{a},\boldsymbol{k},\boldsymbol{\mu}}$ and $v_{\boldsymbol{a},\boldsymbol{k},\boldsymbol{\mu}}$ 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 4.6. More specifically, aperiodic autocorrelation ($u_{\boldsymbol{a},\boldsymbol{k}}$) can be computed from the set of $\{H, N\}^m$ transform coefficients, whereas periodic autocorrelation ($p_{\boldsymbol{a}}$) can be computed from the $\{H\}^m$ (Walsh-Hadamard) coefficients, which are a subset of the $\{H, N\}^m$ transform coefficients.

Unfortunately the construction of Theorem 12 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, $\boldsymbol{\mu} = 1100\ldots$, and $\boldsymbol{a} = 100\ldots$ we find that $u_{\boldsymbol{a},\boldsymbol{k},\boldsymbol{\mu}} \neq 0$ and $\mathrm{wt}(\boldsymbol{\mu}) = 2$.

4 Constructions for Boolean Functions with Favourable APC

4.1 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 probability 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* [5] *quantum state*, $|\psi\rangle$, as described by the vector $\boldsymbol{s} = (s_{00\ldots0}, s_{00\ldots1}, \ldots, s_{11\ldots1})$ such that the probability of a joint measurement on the m qubits of $|\psi\rangle$ yielding state i is $|s_i|^2$, where $i \in \mathbb{Z}_2^m$, and $||\boldsymbol{s}||_2^2 = \sum_{i=00\ldots0}^{11\ldots1} |s_i|^2 = 1$, where $||\boldsymbol{s}||_p$ is the L_p-norm of $\boldsymbol{s}$. We say that $\boldsymbol{s}$ is normalised if $||\boldsymbol{s}||_2^2 = 1$. A local change of basis on the measurement axes is realised by evaluating $\boldsymbol{s}' = U\boldsymbol{s}$, 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*. 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 $\boldsymbol{s}$ and $\boldsymbol{s}'$ to be *locally equivalent* if $\boldsymbol{s}' = U\boldsymbol{s}$ for U a local unitary transform. In such a case, $\boldsymbol{s}$ and $\boldsymbol{s}'$ 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 [32], we will use a bijective mapping from a Boolean function, $f \in \mathcal{B}_m$, to a quantum state of m qubits, $|\psi\rangle$, as represented by $\boldsymbol{s}$.

$$|\psi\rangle \equiv \boldsymbol{s} = 2^{-\frac{m}{2}}(-1)^{f(\boldsymbol{x})}, \tag{34}$$

with $s_i = 2^{-\frac{m}{2}}(-1)^{f(i)}$. 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 a local basis change, this means that, if $\boldsymbol{s} = 2^{-\frac{m}{2}}(-1)^{f(\boldsymbol{x})}$ and $\boldsymbol{s}' = 2^{-\frac{m}{2}}(-1)^{f'(\boldsymbol{x})}$ are locally equivalent, then f and f' have the same fixed-aperiodic autocorrelation profile.

[5] Only pure states are considered in this paper.

Stabilizer QECCs [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 minimum 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 occurrence of *no error*, *bit-flip*, *phase-flip*, or *combined phase-flip then bit-flip* error on each qubit independently. These errors are denoted I, X, Z, and Y, respectively. We introduce the *Pauli matrices*

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} = iXZ, \tag{35}$$

where $i^2 = -1$. The Pauli matrices 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 $\mathcal{E}_j \in \{I, X, Z, Y\}$ acts on qubit j. 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 $\boldsymbol{s}' = U_\mathcal{E} \boldsymbol{s}$ takes $\boldsymbol{s}$ to the errored state $\boldsymbol{s}'$. The weight of the error vector is given by $\mathrm{wt}(\mathcal{E}) = |\{\mathcal{E}_j \mid \mathcal{E}_j \neq I\}|$, and an $[[m, k, d]]$ QECC can, by definition, detect any error vector of weight less than d.

It has been shown that any stabilizer QECC can be represented by a graph on m vertices [3,18,19,21,35,37,41,42]. Quantum states with a graphical representation which have a direct interpretation as quadratic Boolean functions were also investigated in [32]. These turn out to be QECCs of dimension $k = 0$, and therefore correspond to the *graph states* recently proposed in [23,42] as a consequence of the work of [4,34]. These QECCs also correspond to *additive self-dual codes over* GF(4) [5,19]. The mapping from an additive self-dual code over GF(4) to a graph can be understood by converting the 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 over GF(2) with zero diagonal, and ω is a primitive element of GF(4). This conversion is always possible if the code is self-dual. Γ is then, simultaneously, the adjacency matrix for a simple graph that represents the graph state. In this paper we also interpret this graph state as a quadratic Boolean function

$$f(\boldsymbol{x}) = \sum_{j>i} \Gamma_{i,j} x_i x_j, \tag{36}$$

where the $\Gamma_{i,j}$ are entries of Γ. In other words, we exploit the equivalence of $[[m, 0, d]]$ stabilizer QECCs 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 dimension zero, using the mapping (34). The QECC literature often refers to stabilizer states more

abstractly as eigenvectors of a subset of error operators [6], but, without loss of generality, 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* [23, 32]. Later in this section we also use the mapping (34) to find non-stabilizer QECCs via non-quadratic Boolean functions. A pure m-partite quantum state is unentangled if its associated state vector can be fully decomposed as a tensor product. Otherwise the quantum state is considered to be entangled. There are many metrics to describe the entanglement of an m-partite quantum state just as there are many metrics to describe the properties of an error-correcting code [32], (and, for large enough m, most of them are intractable to compute). For $m > 2$ any single metric is, inevitably, insufficient to describe the properties of the state or code. 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. [7]

Let $|\psi\rangle$ be described by f, and $\boldsymbol{a} \in \mathbb{F}_2^m$ define the set of bit-flips $X_{\boldsymbol{a}}$, such that qubit x_j is bit-flipped if $j \in \{k \mid a_k = 1\}$. These bit-flips can also be described in terms of f,

$$|\psi\rangle \to X_{\boldsymbol{a}}(|\psi\rangle) \quad \Leftrightarrow \quad f(\boldsymbol{x}) \to f(\boldsymbol{x} + \boldsymbol{a}). \tag{37}$$

Similarly, for $\boldsymbol{c} \in \mathbb{F}_2^m$, the set of phase-flips $Z_{\boldsymbol{c}}$, where qubit x_j is phase-flipped if $j \in \{k \mid c_k = 1\}$, can be described in terms of f as

$$|\psi\rangle \to Z_{\boldsymbol{c}}(|\psi\rangle) \quad \Leftrightarrow \quad f(\boldsymbol{x}) \to f(\boldsymbol{x}) + \boldsymbol{c} \cdot \boldsymbol{x}. \tag{38}$$

Any combination of phase-flips followed by bit-flips on $|\psi\rangle$ can be described in terms of f as

$$|\psi\rangle \to X_{\boldsymbol{a}} Z_{\boldsymbol{c}}(|\psi\rangle) \quad \Leftrightarrow \quad f(\boldsymbol{x}) \to f(\boldsymbol{x} + \boldsymbol{a}) + \boldsymbol{c} \cdot \boldsymbol{x} + \boldsymbol{c} \cdot \boldsymbol{a}, \tag{39}$$

with a combined phase-flip then bit-flip occurring at the indices covered by

[6] 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 "stabilised" by this subset of error operators. The minimum distance of the QECC is then given by the minimum-weight error operator in the subset.

[7] In the physics literature there is an important subset of entanglement metrics, namely *entanglement monotones* [1]. We will not discuss these metrics in this paper but, instead, consider the weaker, more general notion of *entanglement criteria*. APC are certainly the latter but are also closely related to the former. The sum-of-squares metric, $\mathcal{E}$, of (25) will be shown in a future paper to be an entanglement monotone to within a trivial re-formulation.

$\boldsymbol{a} \,\&\, \boldsymbol{c}$. Note that $Z_{\boldsymbol{c}} X_{\boldsymbol{a}}(|\psi\rangle) = -X_{\boldsymbol{a}} Z_{\boldsymbol{c}}(|\psi\rangle)$, 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 $X_{\boldsymbol{a}} Z_{\boldsymbol{c}}(|\psi\rangle)$, has weight $\mathrm{wt}(\boldsymbol{\mu})$, where $\boldsymbol{\mu} = \boldsymbol{a} + \overline{\boldsymbol{a}} \,\&\, \boldsymbol{c}$ (i.e. $\boldsymbol{\mu} = \boldsymbol{a} \,\mathrm{OR}\, \boldsymbol{c}$). To ensure that the QECC can detect all errors of weight less than d it is necessary and sufficient that, for $\mathrm{wt}(\boldsymbol{\mu}) < d$, all error states, $X_{\boldsymbol{a}} Z_{\boldsymbol{c}}(|\psi\rangle)$, are orthogonal to $|\psi\rangle$ with respect to the normal scalar product of vectors. If this is true then the QECC is an $[[m, 0, d]]$ code.

Theorem 13 *For $f \in \mathcal{B}_m$, let $|\psi\rangle$ be a $[[m, 0, d]]$ QECC, described by $\boldsymbol{s} = 2^{-\frac{m}{2}}(-1)^{f(\boldsymbol{x})}$. Then f has APC distance d. Conversely, if f has APC distance d, then $\boldsymbol{s}$ represents an $[[m, 0, d]]$ QECC, $|\psi\rangle$.*

PROOF. See Appendix A. □

Remark 14 *Theorem 13 holds for f of any algebraic degree, but when f has degree two 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 *[10,17].*

In this paper we focus on QECCs of dimension zero as these relate to single Boolean functions. (Codes of higher dimension relate to sets of functions which will be dealt with in future work). An $[[m, 0, d]]$ QECC corresponds to an $(m, 2^m, d)$ self-dual additive code over GF(4). We distinguish between two types of self-dual additive code over GF(4). A code is of *type II* if all codewords have even weight, otherwise it is of *type I*. Bounds on the minimum distance of self-dual codes were given by Rains and Sloane [5]. Let d_I be the minimum distance of a type I code of length m. Then d_I is upper-bounded by

$$d_I \leq \begin{cases} 2\left\lfloor \frac{m}{6} \right\rfloor + 1, & \text{if } m \equiv 0 \pmod 6 \\ 2\left\lfloor \frac{m}{6} \right\rfloor + 3, & \text{if } m \equiv 5 \pmod 6 \\ 2\left\lfloor \frac{m}{6} \right\rfloor + 2, & \text{otherwise.} \end{cases} \tag{40}$$

There is a similar bound on d_{II}, the minimum distance of a type II code of length m,

$$d_{II} \leq 2\left\lfloor \frac{m}{6} \right\rfloor + 2. \tag{41}$$

A code that meets the appropriate bound is called *extremal*. These upper-bounds translate directly into upper-bounds on the APC distance for quadratic Boolean functions of m variables.

Parker and Rijmen [32] observed that quantum states represented by the clique function, $f(\boldsymbol{x}) = \sum_{i<j} x_i x_j$, and the star function, $f(\boldsymbol{x}) = \sum_{i=1}^{m-1} x_0 x_i$, 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 4.6, where the transform equivalence is described in more detail [8].

We focus here on the quadratic equivalence which has been formulated as a graph symmetry by Glynn [18,19], where the symmetry operation is referred to as *vertex-neighbour-complement* (VNC). It was also described independently by Hein et al. [23] and Van Den Nest et al. [42]. In [35] this operation is explicitly described via repeated actions of the so-called $\{I, H, N\}^m$ transform set. The same operation also has a history in graph theory, where it is referred to as *local complementation* (LC) by Bouchet [3], who identified *isotropic systems* as being equivalent with respect to local complementation. LC also translates into the natural equivalence between self-dual additive codes over GF(4). Not surprisingly, isotropic systems and self-dual additive codes over GF(4) are very similar structures (if not identical). The LC symmetry rule can be described as follows.

Definition 15 *If the quadratic monomial $x_i x_j$ occurs in the algebraic normal form of the quadratic Boolean function $f \in \mathcal{B}_m$, 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* LC orbit *if*

$$f'(\boldsymbol{x}) = f(\boldsymbol{x}) + \sum_{\substack{j,k \in \mathcal{N}_a \\ j \neq k}} x_j x_k \pmod 2, \tag{42}$$

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 [16], so the members of an LC-orbit

[8] Note, however, that Boolean functions of degree greater than two 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 states and, for large d, the quantum state is highly-entangled.

represent flat spectra with respect to a certain set of local unitary transforms as described in Subsection 4.6 [35]. Exploiting this generalised duality, one can show the following.

Theorem 16 *Let $f, f' \in \mathcal{B}_m$ such that f and f' are quadratic and in the same LC orbit. Then f and f' have the same APC distance.*

For example, the quadratic functions $f_h(\boldsymbol{x}) = x_0x_1+x_0x_3+x_0x_4+x_1x_2+x_1x_5+x_2x_3+x_2x_5+x_3x_4+x_4x_5$ and $f'_h(\boldsymbol{x}) = x_0(x_1+x_2+x_3+x_4+x_5)+x_1x_2+x_2x_3+x_3x_4+x_4x_5+x_5x_1$ are in the same orbit and therefore have the same APC distance (of 4). They are the two representations of the $[[6,0,4]]$ *hexacode* up to graph isomorphism. The graphs associated with these two functions both have a maximum *independent set* of 2, but the maximum independent sets of the clique and star graph, which are two members of another LC orbit, are 1 and $m-1$ respectively. In general, quadratic Boolean functions with high APC distance correspond to LC orbits that only comprise graphs with small maximum independent sets [12, 14].

To illustrate the interpretation of the graph as a self-dual additive code over GF(4), consider the hexacode as represented by the Boolean function f_h defined above. According to (36), this function corresponds to the graph with adjacency matrix

$$\Gamma = \begin{pmatrix} 0&1&0&1&1&0\\ 1&0&1&0&0&1\\ 0&1&0&1&0&1\\ 1&0&1&0&1&0\\ 1&0&0&1&0&1\\ 0&1&1&0&1&0 \end{pmatrix}.$$

A generator matrix for the $(6, 2^6, 4)$ additive code over GF(4) can then be written as

$$\Gamma + \omega I = \begin{pmatrix} \omega&1&0&1&1&0\\ 1&\omega&1&0&0&1\\ 0&1&\omega&1&0&1\\ 1&0&1&\omega&1&0\\ 1&0&0&1&\omega&1\\ 0&1&1&0&1&\omega \end{pmatrix},$$

where ω is a primitive element in GF(4).

All self-dual additive codes over GF(4) of length m, i.e., the LC orbits of quadratic Boolean functions, have been classified, up to equivalence, by Calderbank et al. [5] for $m \leq 5$, by Höhn [24] for $m \leq 7$, by Hein et al. [23] for $m \leq 7$, by Glynn et al. [19] for $m \leq 9$, and by two of the authors of this paper [12, 13] for $m \leq 12$. The number of LC orbits up to isomorphism is given in Table 1, where i_m denotes the number of LC orbits of *connected* graphs on m vertices, and t_m denotes the total number of LC orbits. The values of i_m and t_m can also

Table 1
Number of LC Orbits of Graphs on m Vertices

	m											
	1	2	3	4	5	6	7	8	9	10	11	12
i_m	1	1	1	2	4	11	26	101	440	3,132	40,457	1,274,068
t_m	1	2	3	6	11	26	59	182	675	3,990	45,144	1,323,363

be found as sequences A090899 and A094927 in *The On-Line Encyclopedia of Integer Sequences* [39]. A database of orbit representatives up to $m = 12$ can be obtained from `http://www.ii.uib.no/~larsed/vncorbits/`.

4.4 Examples

Consider the following construction, known as the *quadratic residue construction*. Let p be a prime of the form $4k+1$. Assign $a_{ij} = 1$ iff $j - i$ is a quadratic residue modulo p, and $a_{ij} = 0$ otherwise. (n is a quadratic residue modulo p iff there exists an m such that $m^2 \equiv n \pmod{p}$.) Let $f \in \mathcal{B}_p$ be a quadratic Boolean function defined by

$$f(\boldsymbol{x}) = \sum_{i<j} a_{ij} x_i x_j. \tag{43}$$

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 a *Paley graph* which is well-known in the graph-theoretic literature.

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

$$g(\boldsymbol{x}) = f(\boldsymbol{x}) + x_p \sum_{i=0}^{p-1} x_i. \tag{44}$$

Then g has favourable APC distance.

As an example, for $p = 5$, $f(\boldsymbol{x}) = x_0x_1 + x_1x_2 + x_2x_3 + x_3x_4 + x_4x_0$, and $g(\boldsymbol{x}) = f(\boldsymbol{x}) + x_5(x_0 + x_1 + x_2 + x_3 + x_4)$. f has APC distance 3 and g has APC distance 4. The function g is unique over the 6-variable quadratics in achieving an optimal APC distance of 4, and corresponds to the unique $[[6, 0, 4]]$ QECC, known as the hexacode. This function has been identified as being a highly entangled 6-qubit quantum state [32]. As another example, when $p = 29$, f has an APC distance of 11 and g has an APC distance of 12.

For $m = 12$ the QECC with optimal distance is the *dodecacode* which maps to a function with APC distance 6. Its LC orbit can be represented by the Boolean function $f(\boldsymbol{x}) = x_0x_3 + x_0x_7 + x_0x_8 + x_0x_9 + x_0x_{11} + x_1x_4 + x_1x_6 +$

$x_1x_8 + x_1x_9 + x_1x_{10} + x_2x_5 + x_2x_6 + x_2x_7 + x_2x_{10} + x_2x_{11} + x_3x_6 + x_3x_8 + x_3x_{10} + x_3x_{11} + x_4x_6 + x_4x_7 + x_4x_9 + x_4x_{11} + x_5x_7 + x_5x_8 + x_5x_9 + x_5x_{10} + x_6x_9 + x_7x_{10} + x_8x_{11}$. It is interesting to note that both the hexacode and dodecacode can be represented by regular graphs with minimal vertex degree for every vertex, namely 3 and 5, these being one less than their respective distances. These minimal representations appear to be possible for many optimal QECCs although not all [12]. In particular, a partial (but significant) search did not reveal a regular graph with vertex degree 11 in the LC orbit of the graph corresponding to the $[[30, 0, 12]]$ QECC. It remains an open problem as to whether a minimal representation exists for this graph.

We are also able to use the LC orbit to improve the resiliency of quadratic functions, combined with the addition of a suitable affine function. The addition of linear terms does not change the APC. The LC 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 representations of the hexacode up to 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 [10].

4.5 Aperiodic Properties of Nonquadratic Boolean Functions

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. Cryptographically, 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 rises. We now consider the APC distance of such functions. These functions can also be referred to as *hypergraph states*. Note that both Kurosawa and Satoh [26], and Carlet [8], have proposed non-quadratic Boolean functions with favourable EPC properties based on binary linear codes, and binary Kerdock and Preparata nonlinear codes, respectively.

An exhaustive computer search [12], making use of the program *nauty* [28], reveals that no Boolean function of 4 or 5 variables and of degree greater than 2 has an APC distance greater than 2. However, there are 24 cubic functions of 6 variables which satisfy an APC distance of 3. These 24 functions are

inequivalent with respect to the symmetries discussed in Appendix C. If we also consider the symmetry described in Subsection 4.6, there are only 11 inequivalent such functions. For example, $f(\boldsymbol{x}) = x_1x_3x_5 + x_1x_2x_5 + x_3x_4x_5 + x_2x_4x_5 + x_0x_1x_3 + x_0x_1x_2 + x_0x_3x_4 + x_0x_2x_4 + x_0x_4 + x_0x_5 + x_1x_2 + x_1x_4 + x_2x_3 + x_2x_5 + x_3x_4 + x_3x_5 + x_4x_5$ has APC and EPC distances of 3. It was also found that no cubic functions of 6 variables can 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, $f(\boldsymbol{x}) = x_1x_3x_5 + x_0x_1 + x_0x_2 + x_1x_6 + x_2x_5 + x_3x_4 + x_3x_6 + x_4x_5 + x_5x_6$ and $f(\boldsymbol{x}) = x_0x_1x_2x_3 + x_0x_4 + x_0x_5 + x_1x_4 + x_1x_6 + x_2x_5 + x_2x_6 + x_3x_4 + x_3x_5 + x_3x_6$ 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* [16] is as follows.

$$f(\boldsymbol{y}, \boldsymbol{z}) = \boldsymbol{y} \cdot \lambda(\boldsymbol{z}) + g(\boldsymbol{z}), \tag{45}$$

where $f \in \mathcal{B}_{r+s}$, $\boldsymbol{y} \in \mathbb{F}_2^r$, $\boldsymbol{z} \in \mathbb{F}_2^s$, $g \in \mathcal{B}_s$, and λ maps $\mathbb{F}_2^s$ to $\mathbb{F}_2^r$. Following [26], the above examples of 7-variable and 8-variable functions can both be described using (45) with λ a linear map and $g(\boldsymbol{z})$ the non-quadratic part. We have found, as shown above, functions of this kind with favourable APC but, as pointed out by Carlet [8], the reliance on $g(\boldsymbol{z})$ to make the function non-quadratic may lead to cryptanalytic attacks. A more interesting set of functions is obtained by changing λ to a non-linear mapping. Carlet constructs such functions with favourable EPC [8], based on nonlinear Kerdock/Preparata mappings. We can, trivially, use Lemma 11 to state that, for these Kerdock/Preparata-based constructions, 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 (31), both the EPC and APC distances for such functions are upper-bounded by $2^{m-1} - 2^{m/2-1} + 5$. From (45), the Maiorana-McFarland construction is bipartite, and the size of the maximum independent set of its associated hypergraph is at least r. Typically one chooses $r = s$, but LC orbits of the graphs corresponding to the best QECCs maintain a small maximum independent set for every member of the orbit, i.e., $r \ll s$, with $g(\boldsymbol{z})$ an APC-favourable sub-graph. We expect, similarly, that constructions for Boolean functions of algebraic degree greater than two (hypergraphs) with favourable APC should also have a small independent set for their quadratic part, with $g(\boldsymbol{z})$ constructed recursively in the same way. Over 32 variables, the Maiorana-McFarland constructions of Carlet [8] 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 4.4 has APC distance 12, and the graph describing this quadratic function has a maximum independent set of only 6. Moreover a partial search of about 10 million functions from within the (huge) LC orbit of this 30-variable function did not reveal a maximum independent set of size greater than 7.

4.6 Orbits of Boolean Functions with respect to $\{I, H, N\}^m$

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 taken from a set of transforms called the $\{I, H, N\}^m$ set (using and refining the terminology introduced in [30]). The APC distance is invariant over this orbit.

For $\boldsymbol{a}, \boldsymbol{b} \in \mathbb{F}_2^m$, we define $\boldsymbol{a} \tilde{+} \boldsymbol{b}$ such that $0 \tilde{+} 0 = 0$, $1 \tilde{+} 0 = 0 \tilde{+} 1 = 1$, and $1 \tilde{+} 1 = 2$. Moreover, for $h \in \mathbb{F}_2$ and $c \in \mathbb{Z}$, we define ch to be in $\{0, c\}$.

Let $f \in \mathcal{B}_m$ and $\boldsymbol{\theta}, \boldsymbol{r}, \boldsymbol{\alpha}, \boldsymbol{e} \in \mathbb{F}_2^m$ such that $\boldsymbol{r} \preceq \boldsymbol{\theta}$ and $\boldsymbol{\alpha}, \boldsymbol{e} \preceq \overline{\boldsymbol{\theta}}$. Then each pair of values of $\boldsymbol{e}$ and $\boldsymbol{\theta}$ describes one of 3^m possible local unitary transforms taken from the $\{I, H, N\}^m$ set.

$$s_{\boldsymbol{e},\boldsymbol{\theta}}(\boldsymbol{z}) = 2^{\frac{\mathrm{wt}(\boldsymbol{\theta})}{2}} \sum_{\boldsymbol{x} \in \boldsymbol{r} + V_{\overline{\boldsymbol{\theta}}}} i^{2(f(\boldsymbol{x}) + \boldsymbol{\alpha}) \tilde{+} \boldsymbol{e}}, \tag{46}$$

where $\boldsymbol{z} = \boldsymbol{\alpha} + \boldsymbol{r}$, $i^2 = -1$, and $s_{\boldsymbol{e},\boldsymbol{\theta}} \in \mathbb{C}^{2^m}$. In related papers [30, 32, 35] 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, defined as

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad N = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix}, \tag{47}$$

where $i^2 = -1$. In this paper we largely avoid the matrix terminology but retain the name $\{I, H, N\}^m$. [9]

If, for a fixed $\boldsymbol{e}$ and $\boldsymbol{\theta}$, $s_{\boldsymbol{e},\boldsymbol{\theta}}$ is a flat spectrum, i.e., if $|s_{\boldsymbol{e},\boldsymbol{\theta}}(\boldsymbol{z})| = |s_{\boldsymbol{e},\boldsymbol{\theta}}(\boldsymbol{z}')|$ for all $\boldsymbol{z}, \boldsymbol{z}' \in \mathbb{F}_2^m$, then we can write

$$s_{\boldsymbol{e},\boldsymbol{\theta}}(\boldsymbol{z}) = 2^{\frac{m}{2}} w^{g_{\boldsymbol{e},\boldsymbol{\theta}}(\boldsymbol{z})}, \tag{48}$$

where $g_{\boldsymbol{e},\boldsymbol{\theta}}(\boldsymbol{z})$ is a function from $\mathbb{F}_2^m$ to $\mathbb{Z}_8^m$ and $w = e^{\frac{2\pi i}{8}}$, $w \in \mathbb{C}$.

[9] However, to clarify (46) in terms of $\{I, H, N\}^m$, note that the one positions in $\boldsymbol{\theta}$ and $\boldsymbol{e}$ identify the tensor positions where I and N are applied, respectively, with H applied to all other tensor positions.

Definition 17 *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 $\boldsymbol{e}$ and $\boldsymbol{\theta}$, $s_{\boldsymbol{e},\boldsymbol{\theta}}$ is a flat spectrum and $g_{\boldsymbol{e},\boldsymbol{\theta}}$ can further be written as $g_{\boldsymbol{e},\boldsymbol{\theta}}(\boldsymbol{z}) = 4f'(\boldsymbol{z}) + \boldsymbol{c} \cdot \boldsymbol{z} + d \pmod 8$, where $\boldsymbol{c} \in \mathbb{Z}_8^m$, and $d \in \mathbb{Z}_8$.*

The following theorem has previously been proven for f quadratic but not for general f, which is proven here. The LC symmetry discussed in subsection 4.3 is a translation of the quadratic case of this theorem into graphical operations.

Theorem 18 *Let $f, f' \in \mathcal{B}_m$. If f and f' are both in the same $\{I, H, N\}^m$ orbit, then f and f' have the same APC distance.*

PROOF. The proof relies on two critical observations that we express as lemmas.

Lemma 19 *Let $\boldsymbol{a}, \boldsymbol{b} \in \mathbb{C}^N$ be two complex vectors of length N. Let U be an $N \times N$ complex unitary matrix such that $\boldsymbol{a}' = U\boldsymbol{a}$ and $\boldsymbol{b}' = U\boldsymbol{b}$. Define orthogonality of vectors $\boldsymbol{a}$ and $\boldsymbol{b}$ with respect to the scalar product, $\langle \boldsymbol{a}, \boldsymbol{b} \rangle = \boldsymbol{a} \cdot \boldsymbol{b} = 0$. Then $\langle \boldsymbol{a}, \boldsymbol{b} \rangle = 0$ if and only if $\langle \boldsymbol{a}', \boldsymbol{b}' \rangle = 0$.*

Let $\mathcal{E} \in \{I, X, Y, Z\}$, as defined in Section 4, be the error acting on a single qubit. 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 generates the *local Clifford group* which is defined as the group of local unitary matrices that keeps the Pauli matrices over a single complex variable invariant with respect to conjugation [25] (to within a global constant). Explicitly, for $T \in \{I, H, N\}$, $\mathcal{E}' = T\mathcal{E}T^{-1}$ satisfies, $\mathcal{E}' \in \{I, X, Y, Z\}$ [10]. It follows immediately that the $\{I, H, N\}^m$ transform set, as defined in (46), 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 20 *Let $T_{\boldsymbol{e},\boldsymbol{\theta}} \in \{I, H, N\}^m$ and $\mathcal{E} \in \{I, X, Y, Z\}^m$. Then*

$$\mathcal{E}' = T_{\boldsymbol{e},\boldsymbol{\theta}} \mathcal{E} T_{\boldsymbol{e},\boldsymbol{\theta}}^{-1} \quad \Rightarrow \quad \mathcal{E}' \in \{I, X, Y, Z\}^m \quad \Rightarrow \quad \mathrm{wt}(\mathcal{E}') = \mathrm{wt}(\mathcal{E}). \tag{49}$$

Let a quantum state of m qubits, $|\psi\rangle$, be represented by a length 2^m vector $\boldsymbol{s} \in \mathbb{C}^{2^m}$, where $\boldsymbol{s} = 2^{-\frac{m}{2}}(-1)^{f(\boldsymbol{x})}$. We can then re-express Theorem 13 as follows.

$$\text{APC distance}(f) = d \quad \Rightarrow \quad \langle \mathcal{E}\boldsymbol{s}, \boldsymbol{s} \rangle = 0, \ \forall \mathcal{E}, \ 0 < \mathrm{wt}(\mathcal{E}) < d, \tag{50}$$

[10] 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.

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

$$\text{APC distance}(f) = d \quad \Rightarrow \quad \langle \mathcal{E}'\boldsymbol{s}', \boldsymbol{s}' \rangle = 0, \ \forall \mathcal{E}', \ 0 < \text{wt}(\mathcal{E}') < d, \tag{51}$$

where $\mathcal{E}' \in \{I, X, Y, Z\}^m$, and $\boldsymbol{s}'$ 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 $\boldsymbol{s} = T_{\boldsymbol{e},\boldsymbol{\theta}}\boldsymbol{s}'$ for some $T_{\boldsymbol{e},\boldsymbol{\theta}} \in \{I, H, N\}^m$. We now use Lemma 20 to conjugate $\mathcal{E}$ acting on $\boldsymbol{s}$ to $\mathcal{E}'$ acting on $\boldsymbol{s}'$. Now we can write $\langle \mathcal{E}\boldsymbol{s}, \boldsymbol{s} \rangle = 0$ as $\left\langle T^{-1}_{\boldsymbol{e},\boldsymbol{\theta}}\mathcal{E}'T_{\boldsymbol{e},\boldsymbol{\theta}}\boldsymbol{s}, T^{-1}_{\boldsymbol{e},\boldsymbol{\theta}}T_{\boldsymbol{e},\boldsymbol{\theta}}\boldsymbol{s} \right\rangle = 0$. It follows from Lemmas 19 and 20 that $\langle \mathcal{E}'T_{\boldsymbol{e},\boldsymbol{\theta}}\boldsymbol{s}, T_{\boldsymbol{e},\boldsymbol{\theta}}\boldsymbol{s} \rangle = 0, \ \forall \mathcal{E}', \ 0 < \text{wt}(\mathcal{E}') < d$. The theorem follows. □

Remark 21 *Note that we have proved the invariance of the APC distance for any $\boldsymbol{s}$ and $\boldsymbol{s}'$ in the same orbit with respect to the $\{I, H, N\}^m$ transform set. So the proof not only holds for Boolean functions, but also more generally for functions from $\mathbb{F}_2^m$ to $\mathbb{Z}_8$. More generally still, the proof holds for any $\boldsymbol{s}$ and $\boldsymbol{s}'$, even when $\boldsymbol{s}$ and $\boldsymbol{s}'$ represent non-flat spectra.*

We next provide an example of this spectral symmetry for non-quadratic Boolean functions, which generalises LC and uses the flat spectra of a Boolean function with respect to the $\{I, H, N\}^n$ transform set to 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 3 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 $\boldsymbol{\theta} = 110110$ and $\boldsymbol{e} = 001000$. Note, however, that no linear offset of a member of this orbit is balanced, so resiliency cannot be satisfied.

5 Conclusions

We have motivated and characterised aperiodic autocorrelation and the Aperiodic Propagation Criteria (APC) for a Boolean function. In particular we have equated, for quadratic Boolean functions, APC distance with the minimum distance of an associated zero-dimensional quantum error-correcting code. It follows that, for quantum states which have an interpretation as Boolean functions, the APC of the function are also quantum entanglement criteria for the associated state. We highlighted the importance of local complementation (LC) symmetry for APC analysis of quadratic Boolean functions, and also gave a generalisation of LC to Boolean functions of algebraic degree greater than

two. We presented some results for the APC distance of functions of degree greater than two and discussed possible forms other Boolean constructions might take to improve APC distance.

We also showed that fixed-aperiodic autocorrelation is a subset of extended autocorrelation. We further defined the metrics of APC and EPC distance and demonstrated that APC distance is a slightly stricter criteria than EPC distance. Although extended autocorrelation considers a slightly more general set of cryptographic scenarios than fixed-aperiodic autocorrelation, the APC, in some sense, highlights the most important parts of EPC, and this motivates the use of APC for cryptography.

APC is also a potential attack scenario. Just as generalised linear cryptanalysis [30] finds substantially higher biases over state-of-the-art S-boxes, the differential "dual", as covered in this paper, finds substantially higher differential biases where, by "differential" we here refer to an input differential $\Delta \boldsymbol{x} \in \mathbb{F}_2^m$, and an output binary (truncated) differential $\Delta y \in \mathbb{F}_2$. Appendix D gives results of 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 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 [11]. 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 [30, 40]. 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.

[11] However, see [7]

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 $\mathbb{F}_2^m$ to $\mathbb{F}_2^n$ 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 D.2 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 $\mathbb{F}_2^n$, $n > 1$, 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 [30] and [35], e.g., with respect to $\{I, H, N\}^m$. This can be explained by considering a generalisation of the results of [9] to larger transform sets.

Acknowledgements

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

A Proofs

PROOF. [Proposition 4] Proposition 1 of [6] states

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

where k is the dimension of V. Applying (A.1) to (20) gives

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

It is further stated in [6] that

$$\sum_{\boldsymbol{v}\in V^\perp} \mathcal{F}(f + \boldsymbol{x}\cdot\boldsymbol{v})(-1)^{\boldsymbol{k}\cdot\boldsymbol{v}} = 2^{m-k}\mathcal{F}(f\phi_{\boldsymbol{k}+V}). \tag{A.3}$$

Applying (A.3) to (13), (20), and (A.2) gives the result. □

PROOF. [Theorem 12] First we compute the values of $u_{\boldsymbol{a},\boldsymbol{k}}$ for $\boldsymbol{k} = \boldsymbol{0} = 000\ldots$ with π the identity permutation. Let $u_{\boldsymbol{a},\boldsymbol{k}}[m]$ denote the values of $u_{\boldsymbol{a},\boldsymbol{k}}$ for f over m variables. Below are tabulated the values of $u_{\boldsymbol{a},\boldsymbol{0}}[m]$ and the associated upper bound on the l of APC(l) inferred from these $u_{\boldsymbol{a},\boldsymbol{0}}[m]$, for all possible assignments to the three least significant bits (lsbs) of $\boldsymbol{a}$, where * means "don't care".

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

We are interested in the lowest value of l that we can achieve by suitable assignments to $\boldsymbol{a}$. 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 $\boldsymbol{a}$ according to this last row (e.g. for the second iteration we have $\boldsymbol{a} = 10101\ldots$ and $l \leq m-2$). By induction one concludes that $l = \lfloor \frac{m}{2} \rfloor$. As f is a quadratic function we can invoke the symmetry of Lemma 23 in Appendix C to extend the result from $u_{\boldsymbol{a},\boldsymbol{0}}[m]$ to all $u_{\boldsymbol{a},\boldsymbol{k}}[m]$. We further invoke the permutation symmetry of Lemma 24 to extend the result to all functions f where π is not necessarily the identity permutation. □

PROOF. [Theorem 13] Consider all bit-flip and phase-flip errors on $|\psi\rangle$ of weight less than d, described by $\boldsymbol{a}$ and $\boldsymbol{c}$ such that $\mathrm{wt}(\boldsymbol{\mu}) = \mathrm{wt}(\boldsymbol{a}) + \mathrm{wt}(\boldsymbol{\theta}) < d$, as discussed previously, where $\boldsymbol{\mu} = \boldsymbol{a} + \overline{\boldsymbol{a}} \,\&\, \boldsymbol{c}$ and $\boldsymbol{\theta} = \overline{\boldsymbol{a}} \,\&\, \boldsymbol{c}$. We know that $X_{\boldsymbol{a}} Z_{\boldsymbol{c}} |\psi\rangle$, is orthogonal to $|\psi\rangle$ and this can be interpreted in terms of f by asserting that $\mathcal{D}_{\boldsymbol{a}} f + \boldsymbol{c} \cdot \boldsymbol{x}$ is balanced for all $\boldsymbol{a}, \boldsymbol{c}$ that satisfy $\mathrm{wt}(\boldsymbol{\mu}) < d$. In other words, from (20), (32), and Definition 6, $G_{\boldsymbol{a},\boldsymbol{c}} = 0$ for all $\boldsymbol{a}, \boldsymbol{c} \preceq \boldsymbol{\mu}$. The first part of the theorem follows from Definition 7. The converse is easily proven. □

B Further Spectral Identities

B.1 Periodic/Negaperiodic Autocorrelation

We here define the *periodic/negaperiodic autocorrelation* of f, and show how its coefficients are derived from the Fourier spectra of $\mathcal{D}_{\boldsymbol{a}} f$, thus allowing us to relate the periodic/negaperiodic autocorrelation with the aperiodic autocorrelation. The reason we refer to the autocorrelations as "periodic/negape-

riodic" will be explained in Proposition 22. Define the *periodic/negaperiodic autocorrelation coefficients* of f after fixing the subspace $V_{\boldsymbol{\theta}}$ as $U_{\boldsymbol{a},\boldsymbol{e},\boldsymbol{r},\boldsymbol{\mu}}$, where $\boldsymbol{a},\boldsymbol{r},\boldsymbol{\mu} \in \mathbb{F}_2^m$, $\boldsymbol{e} \preceq \boldsymbol{a} \preceq \boldsymbol{\mu}$, $\boldsymbol{r} \preceq \boldsymbol{\theta}$, and $\boldsymbol{\theta} = \boldsymbol{\mu} + \boldsymbol{a}$, and $\boldsymbol{\theta}$ and $\boldsymbol{a}$ are disjoint. Then

$$\begin{aligned} U_{\boldsymbol{a},\boldsymbol{e},\boldsymbol{r},\boldsymbol{\mu}} &= 2^{-\operatorname{wt}(\boldsymbol{\theta})} \sum_{\boldsymbol{c} \in \boldsymbol{e}+V_{\boldsymbol{\theta}}} \mathcal{F}(\mathcal{D}_{\boldsymbol{a}} f + \boldsymbol{c}\cdot\boldsymbol{x} + \operatorname{wt}(\boldsymbol{c}))(-1)^{\boldsymbol{r}\cdot\boldsymbol{c}} \\ &= 2^{-\operatorname{wt}(\boldsymbol{\theta})} \sum_{\boldsymbol{c} \in \boldsymbol{e}+V_{\boldsymbol{\theta}}} \mathcal{F}(\mathcal{D}_{\boldsymbol{a}} f + \boldsymbol{c}\cdot\boldsymbol{x})(-1)^{\overline{\boldsymbol{r}}\cdot\boldsymbol{c}}. \end{aligned} \tag{B.1}$$

When $\boldsymbol{\mu} = \boldsymbol{a}$ then $\boldsymbol{\theta} = \boldsymbol{0}$ and there is no subspace fixing, so that (B.1) simplifies to the computation of the periodic/negaperiodic autocorrelation coefficients of f, namely $U_{\boldsymbol{a},\boldsymbol{c}}$, where $\boldsymbol{c} \preceq \boldsymbol{a}$.

$$U_{\boldsymbol{a},\boldsymbol{c}} = (-1)^{\operatorname{wt}(\boldsymbol{c})} \mathcal{F}(\mathcal{D}_{\boldsymbol{a}} f + \boldsymbol{c}\cdot\boldsymbol{x}),\ \boldsymbol{c} \preceq \boldsymbol{a}. \tag{B.2}$$

There are 3^m coefficients, $U_{\boldsymbol{a},\boldsymbol{c}}$, where $\boldsymbol{c} \preceq \boldsymbol{a}$, and these can be used to construct 2^m complete autocorrelation profiles, one for each value of $\boldsymbol{c}$. Depending on the value of $\boldsymbol{a}$, each of the 3^m coefficients is represented $2^{\operatorname{wt}(\overline{\boldsymbol{a}})}$ times to realise a complete set of 2^{2m} autocorrelation coefficients. Combining (20) with (B.1) and (B.2) yields

$$U_{\boldsymbol{a},\boldsymbol{e},\boldsymbol{r},\boldsymbol{\mu}} = 2^{-\operatorname{wt}(\boldsymbol{\theta})} \sum_{\boldsymbol{c} \in \boldsymbol{e}+V_{\boldsymbol{\theta}}} G_{\boldsymbol{a},\boldsymbol{c}} (-1)^{\overline{\boldsymbol{r}}\cdot\boldsymbol{c}},\ \boldsymbol{e} \preceq \boldsymbol{a} \preceq \boldsymbol{\mu},\ \boldsymbol{r} \preceq \boldsymbol{\theta}, \tag{B.3}$$

and

$$U_{\boldsymbol{a},\boldsymbol{c}} = (-1)^{\operatorname{wt}(\boldsymbol{c})} G_{\boldsymbol{a},\boldsymbol{c}},\ \boldsymbol{c} \preceq \boldsymbol{a}. \tag{B.4}$$

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

By combining Proposition 4 with (B.3) and (B.4) we can now express the fixed-aperiodic (non-modular) autocorrelation coefficients in terms of the periodic/negaperiodic autocorrelation coefficients, and vice versa, where $\boldsymbol{e} \preceq \boldsymbol{a} \preceq \boldsymbol{\mu}$, $\boldsymbol{k} \preceq \boldsymbol{\mu}$, $\boldsymbol{\theta} = \boldsymbol{a} + \boldsymbol{\mu}$, and $\boldsymbol{r} = \boldsymbol{k} \,\&\, \boldsymbol{\theta}$

$$u_{\boldsymbol{a},\boldsymbol{k},\boldsymbol{\mu}} = 2^{-\operatorname{wt}(\boldsymbol{a})} \sum_{\boldsymbol{e} \preceq \boldsymbol{a}} U_{\boldsymbol{a},\boldsymbol{e},\boldsymbol{r},\boldsymbol{\mu}} (-1)^{\overline{\boldsymbol{k}}\cdot\boldsymbol{e}},\ \boldsymbol{k} \preceq \boldsymbol{\mu} \tag{B.5}$$

$$U_{\boldsymbol{a},\boldsymbol{e},\boldsymbol{r},\boldsymbol{\mu}} = \sum_{\boldsymbol{k} \preceq \boldsymbol{r}+V_{\boldsymbol{a}}} u_{\boldsymbol{a},\boldsymbol{k},\boldsymbol{\mu}} (-1)^{\boldsymbol{e}\cdot\overline{\boldsymbol{k}}},\ \boldsymbol{e} \preceq \boldsymbol{a} \tag{B.6}$$

$$u_{\boldsymbol{a},\boldsymbol{k}} = 2^{-\operatorname{wt}(\boldsymbol{a})} \sum_{\boldsymbol{c} \preceq \boldsymbol{a}} U_{\boldsymbol{a},\boldsymbol{c}} (-1)^{\overline{\boldsymbol{k}}\cdot\boldsymbol{c}},\ \boldsymbol{k} \preceq \boldsymbol{a} \tag{B.7}$$

$$U_{\boldsymbol{a},\boldsymbol{c}} = \sum_{\boldsymbol{k} \preceq \boldsymbol{a}} u_{\boldsymbol{a},\boldsymbol{k}} (-1)^{\boldsymbol{c}\cdot\overline{\boldsymbol{k}}},\ \boldsymbol{c} \preceq \boldsymbol{a}. \tag{B.8}$$

We now explain why (B.1) and (B.2) can be viewed as periodic/negaperiodic (modular) metrics.

Proposition 22 *Each periodic/negaperiodic autocorrelation of* (B.1) *and* (B.2) *is specified after fixing a subspace (resp. without fixing) by the parameters* $\boldsymbol{a}, \boldsymbol{e}, \boldsymbol{r}, \boldsymbol{\mu}$ *(resp.* $\boldsymbol{a}, \boldsymbol{c}$*). For each setting of the parameters, the coefficients can be calculated using multivariate polynomial multiplications which are periodically modular for the variables identified by the "1" positions of* $\boldsymbol{a} \,\&\, \overline{\boldsymbol{e}}$ *(resp.* $\boldsymbol{a} \,\&\, \overline{\boldsymbol{c}}$*), and negaperiodically modular for the variables identified by the "1" positions of* $\boldsymbol{e}$ *(resp.* $\boldsymbol{c}$*).*

PROOF. Let $U_{\boldsymbol{a},\boldsymbol{c}}$ be as defined in (B.2), and let $\boldsymbol{z} \in \mathbb{C}^m$. Define $v(\boldsymbol{z})$, and $Q_{\boldsymbol{c}}(\boldsymbol{z})$ as follows

$$v(\boldsymbol{z}) = \sum_{\boldsymbol{x} \in \mathbb{F}_2^m} (-1)^{f(\boldsymbol{x})} \prod_{i \in \mathbb{Z}_m} z_i^{x_i} \tag{B.9}$$

$$Q_{\boldsymbol{c}}(\boldsymbol{z}) = \sum_{\boldsymbol{a} \in \mathbb{F}_2^m} U_{\boldsymbol{a},\boldsymbol{c}} \prod_{i \in \mathbb{Z}_m} z_i^{a_i}. \tag{B.10}$$

Then an expansion verifies the following modular relationship for $Q_{\boldsymbol{c}}(\boldsymbol{z})$

$$Q_{\boldsymbol{c}}(\boldsymbol{z}) = v(\boldsymbol{z}) v(\boldsymbol{z}^{-1}) \pmod{\prod_{i \in \mathbb{Z}_m} (z_i^2 - (-1)^{c_i})}. \tag{B.11}$$

$Q_{\boldsymbol{c}}(\boldsymbol{z})$ 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 (B.1) by first fixing the subspace $V_{\boldsymbol{\theta}}$, then computing all possible periodic/negaperiodic multivariate polynomial multiplications over the remaining unfixed subspace. □

We can recover the (non-modular) polynomial $A(\boldsymbol{z})$ of Proposition 3 by applying the *Chinese remainder theorem* (CRT) to the residue polynomials $Q_{\boldsymbol{c}}(\boldsymbol{z})$. In summary,

$$A(\boldsymbol{z}) = v(\boldsymbol{z}) v(\boldsymbol{z}^{-1}) = v(\boldsymbol{z}) v(\boldsymbol{z}^{-1}) \pmod{\prod_{i \in \mathbb{Z}_m} (z_i^4 - 1)} = \mathrm{CRT}(\{Q_{\boldsymbol{c}}(\boldsymbol{z})\}). \tag{B.12}$$

In this way, we obtain an alternative derivation of (B.8). A similar argument can be used with respect to a fixed subspace, $V_{\boldsymbol{\theta}}$, so as to rederive (B.6).

B.2 Relationships to the Second Derivative

As $G_{\boldsymbol{a},\boldsymbol{c}}$ is the Fourier spectrum of the first derivative of f, there is a natural relationship between the Fourier power spectra of $G_{\boldsymbol{a},\boldsymbol{c}}$ and the *second*

derivative of f, $\mathcal{D}_{\boldsymbol{b}}\mathcal{D}_{\boldsymbol{a}}f$, where $\boldsymbol{a}, \boldsymbol{c}, \boldsymbol{b} \in \mathbb{F}_2^m$.

$$\sum_{\boldsymbol{c} \preceq \boldsymbol{\mu}} |G_{\boldsymbol{a},\boldsymbol{c}}|^2 (-1)^{\boldsymbol{c}\cdot\boldsymbol{k}} = 2^{\mathrm{wt}(\boldsymbol{\mu})} \sum_{\boldsymbol{b} \in \boldsymbol{k} + V_{\overline{\boldsymbol{\mu}}}} \mathcal{F}(\mathcal{D}_{\boldsymbol{b}}\mathcal{D}_{\boldsymbol{a}}f),\ \boldsymbol{k} \preceq \boldsymbol{\mu}. \tag{B.13}$$

Moreover we can use Parseval's theorem to establish the following.

$$\sum_{\boldsymbol{c} \preceq \boldsymbol{\mu}} |G_{\boldsymbol{a},\boldsymbol{c}}|^4 = 2^{\mathrm{wt}(\boldsymbol{\mu})} \sum_{\boldsymbol{k} \preceq \boldsymbol{\mu}} \left(\sum_{\boldsymbol{b} \in \boldsymbol{k} + V_{\overline{\boldsymbol{\mu}}}} \mathcal{F}(\mathcal{D}_{\boldsymbol{b}}\mathcal{D}_{\boldsymbol{a}}f) \right)^2. \tag{B.14}$$

Combining the above relationship with (23), we can establish the following upper bound on the *fixed-aperiodic sum-of-squares* with respect to $\boldsymbol{a}$ after fixing a subspace $V_{\boldsymbol{\theta}}$, referred to as $\sigma_{\boldsymbol{a},\boldsymbol{\mu}}$, and defined in (24), in terms of the second derivative of f.

$$\sigma_{\boldsymbol{a},\boldsymbol{\mu}} \leq 2^{-2\,\mathrm{wt}(\boldsymbol{\mu})} \sum_{\boldsymbol{k} \preceq \boldsymbol{\mu}} \left(\sum_{\boldsymbol{b} \in \boldsymbol{k} + V_{\overline{\boldsymbol{\mu}}}} \mathcal{F}(\mathcal{D}_{\boldsymbol{b}}\mathcal{D}_{\boldsymbol{a}}f) \right)^2. \tag{B.15}$$

B.3 A Generalised Definition of APC

Using the results of this Appendix and Appendix C we are able to generalise (32) as follows.

$$\begin{aligned} u_{\boldsymbol{a},\boldsymbol{k},\boldsymbol{\mu}} = 0,\ \forall \boldsymbol{k} \preceq \boldsymbol{\mu} \quad &\Leftrightarrow \quad U_{\boldsymbol{a},\boldsymbol{e},\boldsymbol{r},\boldsymbol{\mu}} = 0,\ \forall \boldsymbol{e} \preceq \boldsymbol{a},\ \forall \boldsymbol{r} \preceq \boldsymbol{\theta} \\ &\Leftrightarrow \quad G_{\boldsymbol{a},\boldsymbol{c}} = 0,\ \forall \boldsymbol{c} \preceq \boldsymbol{\mu} \\ &\Leftrightarrow \quad \sum_{\boldsymbol{b} \in \boldsymbol{k} + V_{\overline{\boldsymbol{\mu}}}} \mathcal{F}(\mathcal{D}_{\boldsymbol{b}}\mathcal{D}_{\boldsymbol{a}}f) = 0,\ \forall \boldsymbol{k} \preceq \boldsymbol{\mu}, \end{aligned} \tag{B.16}$$

where $\boldsymbol{a} \preceq \boldsymbol{\mu}$.

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.

C.1 Quadratic Simplification

When the degree of f is two, a substantial simplification of the fixed-aperiodic autocorrelation profile can be obtained as follows.

Lemma 23 *Let $f \in \mathcal{B}_m$ be a quadratic function, and let $u_{\boldsymbol{a},\boldsymbol{k},\boldsymbol{\mu}}$ be as defined in* (13)*. Then, for any $\boldsymbol{k}' \preceq \boldsymbol{\mu}$, $u_{\boldsymbol{a},\boldsymbol{k},\boldsymbol{\mu}} = \pm u_{\boldsymbol{a},\boldsymbol{k}',\boldsymbol{\mu}}$.*

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 4 the APC distance is equivalent to the distance measure for zero-dimensional QECCs. Such QECCs map to quadratic Boolean functions. As QECCs of the stabilizer type are conveniently described by self-dual additive codes over GF(4), quadratic Boolean functions with favourable APC can conversely be constructed with relative ease from self-dual additive codes over GF(4). This simplification implicitly exploits the symmetry of Lemma 23.

C.2 Index Permutation Symmetry (Hypergraph Isomorphism)

Lemma 24 *Define $f \in \mathcal{B}_m$. Let π be a permutation from $\mathbb{Z}_m$ to $\mathbb{Z}_m$. Let γ be a permutation from $\mathbb{F}_2^m$ to $\mathbb{F}_2^m$ such that, for $\boldsymbol{r} \in \mathbb{F}_2^m$, $\gamma(\boldsymbol{r})$ 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 $u_{\boldsymbol{a},\boldsymbol{k},\boldsymbol{\mu}}(f') = u_{\gamma(\boldsymbol{a}),\gamma(\boldsymbol{k}),\gamma(\boldsymbol{\mu})}(f)$, so that both f and f' satisfy* APC(l) *of order q.*

C.3 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 $\boldsymbol{\gamma} \in \mathbb{F}_2^m$ define f' as a periodic shift of f, where $f'(\boldsymbol{x}) = f(\boldsymbol{x} + \boldsymbol{\gamma})$.

Proposition 25 *With $\boldsymbol{a}, \boldsymbol{k}, \boldsymbol{\gamma}, \boldsymbol{\mu} \in \mathbb{F}_2^m$, f' as defined above, and fixed-aperiodic autocorrelation coefficients as defined in* (13)*, $u_{\boldsymbol{a},\boldsymbol{k},\boldsymbol{\mu}}(f) = u_{\boldsymbol{a},(\boldsymbol{k}+\boldsymbol{\gamma})\,\&\,\boldsymbol{\mu},\boldsymbol{\mu}}(f')$, where $\boldsymbol{k} \preceq \boldsymbol{\mu}$.*

PROOF. Using (13), $u_{\boldsymbol{a},\boldsymbol{k},\boldsymbol{\mu}}(f') = \mathcal{F}(\mathcal{D}_{\boldsymbol{a}} f' \phi_{\boldsymbol{k}+V_{\overline{\boldsymbol{\mu}}}}) = \mathcal{F}(\mathcal{D}_{\boldsymbol{a}} f \phi_{\boldsymbol{\gamma}+\boldsymbol{k}+V_{\overline{\boldsymbol{\mu}}}})$, where $\boldsymbol{k} \preceq \boldsymbol{\mu}$.

$$\begin{aligned}\boldsymbol{\gamma} + \boldsymbol{k} + V_{\overline{\boldsymbol{\mu}}} &= (\boldsymbol{\gamma} \,\&\, \boldsymbol{\mu} + \boldsymbol{k}) + \boldsymbol{\gamma} \,\&\, \overline{\boldsymbol{\mu}} + V_{\overline{\boldsymbol{\mu}}} \\ &= (\boldsymbol{\gamma} + \boldsymbol{k}) \,\&\, \boldsymbol{\mu} + (\boldsymbol{\gamma} \,\&\, \overline{\boldsymbol{\mu}} + V_{\overline{\boldsymbol{\mu}}}) \\ &= (\boldsymbol{\gamma} + \boldsymbol{k}) \,\&\, \boldsymbol{\mu} + V_{\overline{\boldsymbol{\mu}}},\ \boldsymbol{k} \preceq \boldsymbol{\mu}.\end{aligned}$$

After the change of variable $\boldsymbol{k}$ to $(\boldsymbol{k} + \boldsymbol{\gamma}) \,\&\, \boldsymbol{\mu}$, we obtain

$$u_{\boldsymbol{a},(\boldsymbol{k}+\boldsymbol{\gamma})\,\&\,\boldsymbol{\mu},\boldsymbol{\mu}}(f') = \mathcal{F}(\mathcal{D} f \phi_{\boldsymbol{k}+V_{\overline{\boldsymbol{\mu}}}}) = u_{\boldsymbol{a},\boldsymbol{k},\boldsymbol{\mu}}(f),\ \boldsymbol{k} \preceq \boldsymbol{\mu}. \qquad \square \tag{C.1}$$

Similarly, with $\boldsymbol{\lambda} \in \mathbb{F}_2^m$ we define f'' as a negaperiodic shift of f, where $f''(\boldsymbol{x}) = f(\boldsymbol{x} + \boldsymbol{\lambda}) + \boldsymbol{\lambda} \cdot \boldsymbol{x} + \mathrm{wt}(\boldsymbol{\lambda})$.

Proposition 26 *With $\boldsymbol{a}, \boldsymbol{k}, \boldsymbol{\lambda}, \boldsymbol{\mu} \in \mathbb{F}_2^m$, f'' as defined above, and fixed-aperiodic autocorrelation coefficients as defined in* (13)

$$u_{\boldsymbol{a},\boldsymbol{k},\boldsymbol{\mu}}(f) = (-1)^{\boldsymbol{\lambda}\cdot\boldsymbol{a}} u_{\boldsymbol{a},(\boldsymbol{k}+\boldsymbol{\lambda})\,\&\,\boldsymbol{\mu},\boldsymbol{\mu}}(f''), \tag{C.2}$$

where $\boldsymbol{k} \preceq \boldsymbol{\mu}$.

PROOF. Remembering that f' is a periodic shift of f, observe that $\mathcal{D}_{\boldsymbol{a}} f'' = f(\boldsymbol{x} + \boldsymbol{\lambda}) + f(\boldsymbol{x} + \boldsymbol{\lambda} + \boldsymbol{a}) + \boldsymbol{\lambda} \cdot \boldsymbol{a} = \mathcal{D}_{\boldsymbol{a}} f' + \boldsymbol{\lambda} \cdot \boldsymbol{a}$. Therefore

$$\begin{aligned}u_{\boldsymbol{a},\boldsymbol{k},\boldsymbol{\mu}}(f'') &= \mathcal{F}(\mathcal{D}_{\boldsymbol{a}} f'' \phi_{\boldsymbol{k}+V_{\overline{\boldsymbol{\mu}}}}) \\ &= \mathcal{F}(\mathcal{D}_{\boldsymbol{a}} f' \phi_{\boldsymbol{k}+V_{\overline{\boldsymbol{\mu}}}} + \boldsymbol{\lambda} \cdot \boldsymbol{a}) \\ &= (-1)^{\boldsymbol{\lambda}\cdot\boldsymbol{a}} \mathcal{F}(\mathcal{D}_{\boldsymbol{a}} f' \phi_{\boldsymbol{\lambda}+\boldsymbol{k}+V_{\overline{\boldsymbol{\mu}}}}),\end{aligned}$$

where $\boldsymbol{k} \preceq \boldsymbol{\mu}$. Substituting $\boldsymbol{k}$ with $(\boldsymbol{k} + \boldsymbol{\lambda}) \,\&\, \boldsymbol{\mu}$ gives $u_{\boldsymbol{a},(\boldsymbol{k}+\boldsymbol{\lambda})\,\&\,\boldsymbol{\mu},\boldsymbol{\mu}}(f'') = (-1)^{\boldsymbol{\lambda}\cdot\boldsymbol{a}} u_{\boldsymbol{a},\boldsymbol{k},\boldsymbol{\mu}}(f)$, and the proposition follows. $\square$

We can combine the above results for periodic/negaperiodic shift (Propositions 25 and 26) as follows. With $\boldsymbol{\gamma}, \boldsymbol{\lambda} \in \mathbb{F}_2^m$ we define f_{pn} as a periodic/negaperiodic shift of f.

$$f_{pn}(\boldsymbol{x}) = f(\boldsymbol{x} + \boldsymbol{\gamma}) + \boldsymbol{\lambda} \cdot \boldsymbol{x} + \mathrm{wt}(\boldsymbol{\lambda}), \tag{C.3}$$

where $\boldsymbol{\lambda} \preceq \boldsymbol{\gamma}$.

Proposition 27 *With $\boldsymbol{a}, \boldsymbol{k}, \boldsymbol{\gamma}, \boldsymbol{\lambda}, \boldsymbol{\mu} \in \mathbb{F}_2^m$, f_{pn} as defined above, and fixed-aperiodic autocorrelation coefficients as defined in* (13)

$$u_{\boldsymbol{a},\boldsymbol{k},\boldsymbol{\mu}}(f) = (-1)^{\boldsymbol{\lambda}\cdot\boldsymbol{a}} u_{\boldsymbol{a},(\boldsymbol{k}+\boldsymbol{\gamma})\,\&\,\boldsymbol{\mu},\boldsymbol{\mu}}(f_{pn}), \tag{C.4}$$

where $\boldsymbol{k} \preceq \boldsymbol{\mu}$ and $\boldsymbol{\lambda} \preceq \boldsymbol{\gamma}$.

PROOF. Combine Propositions 25 and 26. □

Corollary 28 *For the special case with* $\boldsymbol{\gamma} \preceq \overline{\boldsymbol{\mu}}$ *and* f_{pn} *defined as above,* $u_{\boldsymbol{a},\boldsymbol{k},\boldsymbol{\mu}}(f) = u_{\boldsymbol{a},\boldsymbol{k},\boldsymbol{\mu}}(f_{pn})$*, where* $\boldsymbol{k} \preceq \boldsymbol{\mu}$*.*

PROOF. $\boldsymbol{\gamma} \,\&\, \boldsymbol{\mu} = 0$. □

It follows that a periodic shift (resp. negaperiodic shift) of f after fixing a subspace $V_{\boldsymbol{\theta}}$ 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, (13), and Proposition 4, we obtain the following identities for the periodic/negaperiodic autocorrelation coefficients.

Lemma 29

$$G_{\boldsymbol{a},\boldsymbol{c}}(f) = (-1)^{\boldsymbol{\lambda}\cdot\boldsymbol{a}+\boldsymbol{\gamma}\cdot\boldsymbol{c}} G_{\boldsymbol{a},\boldsymbol{c}}(f_{pn}),\ \boldsymbol{\lambda} \preceq \boldsymbol{\gamma},\ \boldsymbol{c} \preceq \boldsymbol{\mu}, \tag{C.5}$$

$$U_{\boldsymbol{a},\boldsymbol{c}}(f) = (-1)^{\boldsymbol{\lambda}\cdot\boldsymbol{a}+\boldsymbol{\gamma}\cdot\boldsymbol{c}} U_{\boldsymbol{a},\boldsymbol{c}}(f_{pn}),\ \boldsymbol{\lambda} \preceq \boldsymbol{\gamma},\ \boldsymbol{c} \preceq \boldsymbol{a}, \tag{C.6}$$

$$U_{\boldsymbol{a},\boldsymbol{e},\boldsymbol{r},\boldsymbol{\mu}}(f) = (-1)^{\boldsymbol{\lambda}\cdot\boldsymbol{a}+\boldsymbol{\gamma}\cdot\boldsymbol{e}} U_{\boldsymbol{a},\boldsymbol{e},(\boldsymbol{r}+\boldsymbol{\gamma}\,\&\,\boldsymbol{\theta}),\boldsymbol{\mu}}(f_{pn}),\ \boldsymbol{\lambda} \preceq \boldsymbol{\gamma},\ \boldsymbol{e} \preceq \boldsymbol{a},\ \boldsymbol{r} \preceq \boldsymbol{\theta}. \tag{C.7}$$

PROOF. For $\boldsymbol{k} \preceq \boldsymbol{\mu}$ and $\boldsymbol{\lambda} \preceq \boldsymbol{\gamma}$, and noting that, for $\boldsymbol{c} \preceq \boldsymbol{\mu}$, $\boldsymbol{\gamma} \,\&\, \boldsymbol{\mu} \cdot \boldsymbol{c} = \boldsymbol{\gamma} \cdot \boldsymbol{c}$,

$$\begin{aligned}(-1)^{\boldsymbol{\lambda}\cdot\boldsymbol{a}} u_{\boldsymbol{a},(\boldsymbol{k}+\boldsymbol{\gamma})\,\&\,\boldsymbol{\mu},\boldsymbol{\mu}} &= 2^{-\operatorname{wt}(\boldsymbol{\mu})}(-1)^{\boldsymbol{\lambda}\cdot\boldsymbol{a}} \sum_{\boldsymbol{c}\preceq\boldsymbol{\mu}} G_{\boldsymbol{a},\boldsymbol{c}}(-1)^{(\boldsymbol{k}+\boldsymbol{\gamma})\cdot\boldsymbol{c}} \\ &= 2^{-\operatorname{wt}(\boldsymbol{\mu})}(-1)^{\boldsymbol{\lambda}\cdot\boldsymbol{a}} \sum_{\boldsymbol{c}\preceq\boldsymbol{\mu}} ((-1)^{\boldsymbol{\gamma}\cdot\boldsymbol{c}} G_{\boldsymbol{a},\boldsymbol{c}})(-1)^{\boldsymbol{k}\cdot\boldsymbol{c}}.\end{aligned}$$

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

It follows that 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 $u_{\boldsymbol{a},\boldsymbol{k},\boldsymbol{\mu}}(f)$, $U_{\boldsymbol{a},\boldsymbol{c}}(f)$, and $U_{\boldsymbol{a},\boldsymbol{e},\boldsymbol{r},\boldsymbol{\mu}}$ are invariant to a periodic and/or negaperiodic shift of f to within a linear permutation, it follows, from (26), Definition 6, and (32) that $\sigma_{\boldsymbol{a},\boldsymbol{\theta}}(f)$, $\mathcal{E}(f)$, $\sigma(f)$, and the APC of f are invariant to periodic and/or negaperiodic shifts of f. We summarise these observations in the following corollary.

Corollary 30 *For* $f \in \mathcal{B}_m$*,* $\boldsymbol{\mu} \in \mathbb{F}_2^m$*, and* $\boldsymbol{a} \preceq \boldsymbol{\mu}$*, let* f_{pn} *be a periodic and/or negaperiodic shift of* f*. Then* $\sigma_{\boldsymbol{a},\boldsymbol{\mu}}(f_{pn}) = \sigma_{\boldsymbol{a},\boldsymbol{\mu}}(f)$*,* $\mathcal{E}(f_{pn}) = \mathcal{E}(f)$*, and* $\sigma(f_{pn}) = \sigma(f)$*. The functions* f *and* f_{pn} *will also satisfy APC of order* q *of the same degree, and have the same APC distance.*

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 $\mathbb{F}_2^m$ to $\mathbb{F}_2^n$, 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, $\{g_{\boldsymbol{c}} \mid \boldsymbol{c} \in \mathbb{F}_2^n\}$, such that $g_{\boldsymbol{c}} = \boldsymbol{c} \cdot f$. We then compute, for a given S-box, the maximum bias over all functions in the set $\{g_{\boldsymbol{c}}\}$. The periodic bias at $\boldsymbol{a}$ is given by $\frac{2^m + |p_{\boldsymbol{a}}|}{2^{m+1}}$, the aperiodic bias at $\boldsymbol{a}$ is given by $\frac{2^{m-|\boldsymbol{a}|} + |u_{\boldsymbol{a},\boldsymbol{k}}|}{2^{m-|\boldsymbol{a}|+1}}$, and the fixed-aperiodic bias at $\boldsymbol{\mu}$ is given by $\frac{2^{m-|\boldsymbol{\mu}|} + |u_{\boldsymbol{a},\boldsymbol{k},\boldsymbol{\mu}}|}{2^{m-|\boldsymbol{\mu}|+1}}$, where, for a given differential weight, it always holds that the periodic bias is less than the aperiodic bias, which again is less than the fixed-aperiodic bias. Tables D.1 and D.2 show 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 the periodic, aperiodic, and fixed-aperiodic differentials, respectively.

Table D.1
Periodic (P), Aperiodic (A), and Fixed-Aperiodic (F) Autocorrelation Biases for Selected S-Boxes

		Differential Weight								
S-box		1	2	3	4	5	6	7	8	9
AES [11]	P	0.56	0.56	0.56	0.56	0.56	0.56	0.56	0.56	
(8×8)	A	0.56	0.66	0.81	0.94	1.00	1.00	1.00	1.00	
	F	0.56	0.66	0.81	1.00	1.00	1.00	1.00	1.00	
Khazad [36]	P	0.67	0.67	0.69	0.70	0.67	0.67	0.66	0.63	
(8×8)	A	0.67	0.77	0.94	1.00	1.00	1.00	1.00	1.00	
	F	0.67	0.77	0.94	1.00	1.00	1.00	1.00	1.00	
Whirlpool [2]	P	0.66	0.69	0.67	0.69	0.66	0.67	0.66	0.64	
(8×8)	A	0.66	0.75	0.84	1.00	1.00	1.00	1.00	1.00	
	F	0.66	0.78	0.91	1.00	1.00	1.00	1.00	1.00	
Misty1 [27]	P	0.56	0.56	0.56	0.56	0.56	0.56	0.56		
(7×7)	A	0.56	0.75	0.75	1.00	1.00	1.00	1.00		
	F	0.56	0.75	1.00	1.00	1.00	1.00	1.00		
Misty1	P	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
(9×9)	A	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
	F	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
DES-1 [29]	P	0.88	0.81	0.81	0.81	0.75	0.69			
(6×4)	A	0.88	0.94	1.00	1.00	1.00	1.00			
	F	0.88	1.00	1.00	1.00	1.00	1.00			
DES-2	P	0.94	0.81	0.81	0.81	0.88	0.75			
(6×4)	A	0.94	0.94	1.00	1.00	1.00	1.00			
	F	0.94	1.00	1.00	1.00	1.00	1.00			
DES-3	P	0.88	0.75	0.81	0.81	0.75	0.69			
(6×4)	A	0.88	0.88	1.00	1.00	1.00	1.00			
	F	0.88	1.00	1.00	1.00	1.00	1.00			
DES-4	P	1.00	0.75	0.75	1.00	1.00	0.75			
(6×4)	A	1.00	1.00	1.00	1.00	1.00	1.00			
	F	1.00	1.00	1.00	1.00	1.00	1.00			
DES-5	P	0.81	0.81	0.81	0.81	0.75	0.63			
(6×4)	A	0.81	0.94	1.00	1.00	1.00	1.00			
	F	0.81	1.00	1.00	1.00	1.00	1.00			
DES-6	P	0.81	0.88	0.81	0.81	0.81	0.69			
(6×4)	A	0.81	0.94	1.00	1.00	1.00	1.00			
	F	0.81	1.00	1.00	1.00	1.00	1.00			
DES-7	P	0.88	0.88	0.81	0.81	0.81	0.69			
(6×4)	A	0.88	1.00	1.00	1.00	1.00	1.00			
	F	0.88	1.00	1.00	1.00	1.00	1.00			
DES-8	P	0.88	0.88	0.81	0.81	0.75	0.75			
(6×4)	A	0.88	0.94	1.00	1.00	1.00	1.00			
	F	0.88	1.00	1.00	1.00	1.00	1.00			

Table D.2
Periodic (P), Aperiodic (A), and Fixed-Aperiodic (F) Autocorrelation Biases for Selected S-Boxes

S-box		Differential Weight					
		1	2	3	4	5	6
FDE-1 [38]	P	0.69	0.88	0.88	0.88	0.75	0.63
(6×4)	A	0.69	1.00	1.00	1.00	1.00	1.00
	F	0.69	1.00	1.00	1.00	1.00	1.00
FDE-2	P	0.69	0.69	0.75	0.75	0.75	0.63
(6×4)	A	0.69	0.81	1.00	1.00	1.00	1.00
	F	0.69	0.88	1.00	1.00	1.00	1.00
FDE-3	P	0.75	0.75	0.75	0.69	0.69	0.75
(6×4)	A	0.75	0.88	1.00	1.00	1.00	1.00
	F	0.75	0.88	1.00	1.00	1.00	1.00
FDE-4	P	0.81	0.75	0.81	0.81	0.75	0.63
(6×4)	A	0.81	0.88	1.00	1.00	1.00	1.00
	F	0.81	1.00	1.00	1.00	1.00	1.00
FDE-5	P	0.75	0.69	0.75	0.75	0.69	0.69
(6×4)	A	0.75	0.94	1.00	1.00	1.00	1.00
	F	0.75	0.94	1.00	1.00	1.00	1.00
FDE-6	P	0.75	0.75	0.75	0.75	0.75	0.63
(6×4)	A	0.75	0.81	1.00	1.00	1.00	1.00
	F	0.75	0.88	1.00	1.00	1.00	1.00
FDE-7	P	0.75	0.75	0.75	0.75	0.69	0.69
(6×4)	A	0.75	0.88	1.00	1.00	1.00	1.00
	F	0.75	0.88	1.00	1.00	1.00	1.00
FDE-8	P	0.69	0.75	0.75	0.81	0.75	0.63
(6×4)	A	0.69	0.88	1.00	1.00	1.00	1.00
	F	0.69	0.88	1.00	1.00	1.00	1.00
$[[6, 0, 4]]$ hexacode	P	0.50	0.50	0.50	1.00	0.50	0.50
(single function)	A	0.50	0.50	0.50	1.00	0.50	1.00
	F	0.50	0.50	0.50	1.00	1.00	1.00

References

[1] H. Barnum, N. Linden, Monotones and invariants for multi-particle quantum states, J. Phys. A 34 (35) (2001) 6787–6805, arXiv:quant-ph/0103155.

[2] P. S. L. M. Barreto, V. Rijmen, The WHIRLPOOL hashing function, in: First open NESSIE workshop, Leuven, 2000.

[3] A. Bouchet, Graphic presentations of isotropic systems, J. Combin. Theory Ser. B 45 (1) (1988) 58–76.

[4] H. J. Briegel, R. Raussendorf, Persistent entanglement in arrays of interacting particles, Phys. Rev. Lett. 86 (5) (2001) 910–913, arXiv:quant-ph/0004051.

[5] A. R. Calderbank, E. M. Rains, P. M. Shor, N. J. A. Sloane, Quantum error correction via codes over GF(4), IEEE Trans. Inform. Theory 44 (4) (1998) 1369–1387, arXiv:quant-ph/9608006.

[6] A. Canteaut, P. Charpin, Decomposing bent functions, IEEE Trans. Inform. Theory 49 (8) (2003) 2004–2019.

[7] A. Canteaut, M. Videau, Degree of Composition of Highly Nonlinear Functions and Applications to Higher Order Differential Cryptanalysis, in: Advances in Cryptology – EUROCRYPT 2002, vol. 2332 of Lecture Notes in Comput. Sci., Springer-Verlag, Berlin, 2002, pp. 518–533.

[8] C. Carlet, On cryptographic propagation criteria for Boolean functions, Inform. and Comput. 151 (1–2) (1999) 32–56.

[9] F. Chabaud, S. Vaudenay, Links between differential and linear cryptanalysis, in: Advances in Cryptology – EUROCRYPT '94, vol. 950 of Lecture Notes in Comput. Sci., Springer-Verlag, Berlin, 1995, pp. 356–365.

[10] P. Charpin, E. Pasalic, On propagation characteristics of resilient functions, in: Selected Areas in Cryptography, vol. 2595 of Lecture Notes in Comput. Sci., Springer-Verlag, Berlin, 2003, pp. 175–195.

[11] J. Daemen, V. Rijmen, The block cipher Rijndael, NIST AES homepage, http://www.nist.gov/aes/, February 2003.

[12] L. E. Danielsen, On Self-Dual Quantum Codes, Graphs, and Boolean Functions, Master's thesis, Dept. of Informatics, Univ. of Bergen, Norway, arXiv:quant-ph/0503236, March 2005.

[13] L. E. Danielsen, M. G. Parker, On the classification of all self-dual additive codes over GF(4) of length up to 12, in: Fourth International Workshop on Optimal Codes and Related Topics, Institute of Mathematics and Informatics, Bulgarian Academy of Sciences, Sofia, 2005, pp. 47–52, arXiv:math.CO/0504522.

[14] L. E. Danielsen, M. G. Parker, Spectral orbits and peak-to-average power ratio of Boolean functions with respect to the $\{I, H, N\}^n$ transform,

in: Sequences and Their Applications – SETA 2004, vol. 3486 of Lecture Notes in Comput. Sci., Springer-Verlag, Berlin, 2005, pp. 373–388, arXiv:cs.IT/0504102.

[15] J. A. Davis, J. Jedwab, Peak-to-mean power control in OFDM, Golay complementary sequences and Reed-Muller codes, IEEE Trans. Inform. Theory 45 (7) (1999) 2397–2417.

[16] J. F. Dillon, Elementary Hadamard Difference Sets, Ph.D. thesis, Univ. of Maryland, 1974.

[17] J.-H. Evertse, Linear structures in block ciphers, in: Advances in Cryptology – EUROCRYPT '87, vol. 304 of Lecture Notes in Comput. Sci., Springer-Verlag, Berlin, 1987, pp. 249–266.

[18] D. G. Glynn, On self-dual quantum codes and graphs, submitted to Electron. J. Combin., 2002.

[19] D. G. Glynn, T. A. Gulliver, J. G. Maks, M. K. Gupta, The geometry of additive quantum codes, submitted to Springer-Verlag, 2005.

[20] D. Gottesman, Stabilizer Codes and Quantum Error Correction, Ph.D. thesis, California Institute of Technology, Pasadena, CA, arXiv:quant-ph/9705052, May 1997.

[21] M. Grassl, A. Klappenecker, M. Rötteler, Graphs, quadratic forms, and quantum codes, in: Proc. IEEE Int. Symp. Inform. Theory – ISIT 2002, 2002, p. 45.

[22] T. A. Gulliver, M. G. Parker, The multivariate merit factor of a Boolean function, in: Proc. IEEE Information Theory Workshop on Coding and Complexity – ITW 2005, 2005, pp. 58–62.

[23] M. Hein, J. Eisert, H. J. Briegel, Multi-party entanglement in graph states, Phys. Rev. A 69 (6) (2004) 062311, arXiv:quant-ph/0307130.

[24] G. Höhn, Self-dual codes over the Kleinian four group, Math. Ann. 327 (2) (2003) 227–255, arXiv:math.CO/0005266.

[25] A. Klappenecker, M. Rötteler, Clifford codes, in: Mathematics of quantum computation, Comput. Math. Ser., Chapman & Hall/CRC Press, Boca Raton, FL, 2002, pp. 253–273.

[26] K. Kurosawa, T. Satoh, Design of SAC/PC(l) of order k Boolean functions and three other cryptographic criteria, in: Advances in Cryptology – EUROCRYPT '97, vol. 1233 of Lecture Notes in Comput. Sci., Springer-Verlag, Berlin, 1997, pp. 434–449.

[27] M. Matsui, New block encryption algorithm MISTY, in: Fast Software Encryption – FSE '97, vol. 1267 of Lecture Notes in Comput. Sci., Springer-Verlag, Berlin, 1997, pp. 54–68.

[28] B. D. McKay, nauty User's Guide, http://cs.anu.edu.au/~bdm/nauty/, 2003.

[29] Data encryption standard, FIPS Publication 46, National Bureau of Standards, U.S. Dept. of Commerce, 1977.

[30] M. G. Parker, Generalised S-box nonlinearity, Public Document NES/DOC/UIB/WP5/020/A, NESSIE, 2003.

[31] M. G. Parker, Univariate and multivariate merit factors, in: Sequences and Their Applications – SETA 2004, vol. 3486 of Lecture Notes in Comput. Sci., Springer-Verlag, Berlin, 2005, pp. 72–100.

[32] M. G. Parker, V. Rijmen, The quantum entanglement of binary and bipolar sequences, in: Sequences and Their Applications – SETA '01, Discrete Math. Theor. Comput. Sci., Springer-Verlag, London, 2002, pp. 296–309, arXiv:quant-ph/0107106.

[33] B. Preneel, W. Van Leekwijck, L. Van Linden, R. Govaerts, J. Vandewalle, Propagation characteristics of Boolean functions, in: Advances in Cryptology – EUROCRYPT '90, vol. 473 of Lecture Notes in Comput. Sci., Springer-Verlag, Berlin, 1991, pp. 161–173.

[34] R. Raussendorf, D. E. Browne, H. J. Briegel, Measurement-based quantum computation with cluster states, Phys. Rev. A 68 (2) (2003) 022312, arXiv:quant-ph/0301052.

[35] C. Riera, M. G. Parker, Generalised bent criteria for Boolean functions (I), to appear in IEEE Trans. Inform. Theory, arXiv:cs.IT/0502049, 2005.

[36] V. Rijmen, P. S. L. M. Barreto, The KHAZAD legacy-level block cipher, in: First open NESSIE Workshop, Leuven, 2000.

[37] D. Schlingemann, R. F. Werner, Quantum error-correcting codes associated with graphs, Phys. Rev. A 65 (1) (2002) 012308, arXiv:quant-ph/0012111.

[38] A. Shafieinezhad, F. Hendessi, T. A. Gulliver, A structure for fast data encryption, preprint, 2004.

[39] N. J. A. Sloane, The On-Line Encyclopedia of Integer Sequences, http://www.research.att.com/~njas/sequences/.

[40] F.-X. Standaert, G. Rouvroy, G. Piret, J.-J. Quisquater, J.-D. Legat, Key-dependent approximations in cryptanalysis, in: Proc. 24th Symp. on Inform. Theory in the Benelux, 2003.

[41] V. D. Tonchev, Error-correcting codes from graphs, Discrete Math. 257 (2–3) (2002) 549–557.

[42] M. Van den Nest, J. Dehaene, B. De Moor, Graphical description of the action of local Clifford transformations on graph states, Phys. Rev. A 69 (2) (2004) 022316, arXiv:quant-ph/0308151.