On CCZ-equivalence of Addition mod 2n

Ernst Schulte-Geers

On CCZ-equivalence of Addition mod 2^n

Ernst Schulte-Geers

Bundesamt für Sicherheit in der Informationstechnik (BSI)
ernst.schulte-geers(at)bsi.bund.de

Abstract. We show that addition mod 2^n is CCZ-equivalent to a quadratic vectorial Boolean function. We use this to reduce the solution of systems differential equations of addition to the solution of a system of linear equations and to derive a fully explicit formula for the correlation coefficients, which leads to new results about the Walsh transform of addition mod 2^n . The results have applications in the cryptanalysis of cyptographic primitives which use addition mod 2^n .

Keywords: CCZ-equivalence, addition, Walsh transform, differential eq. of addition

1 Introduction

Addition mod 2^n is frequently used as one source of Boolean nonlinearity in modern block ciphers and hash functions. It is e.g. used in the ciphers FEAL, IDEA, SAFER,RC5, MARS, Twofish and the current SHA-3 finalists Skein and BLAKE.

We revisit here the compatibility of addition mod 2^n ($\boxplus$) with XOR.

The different aspects of compatibility of XOR with modular additions have been the subject of extensive research, mostly along the following lines:

(1) The Markov chain of carries :
one way to treat the approximation of addition by XOR probabilistically is to consider the Markov chain generated by the carry bits ([9],[4],[8],[1]). In [1] Alquié gave an explicit formula for the bias of the i-th carry bit for any fixed number n of summands.

(2) Differential cryptanalysis (DC):
beginning with the DC of FEAL by Biham&Shamir [2] partial results begin to appear, but a complete (fully explicit) formula for the differential probabilities of addition mod 2^n was apparently only given in 2001 by Lipmaa&Moriai ([5]). These authors also give efficient algorithms to compute certain maximal differential probabilities.
Closely related to DC of addition are "differential equations of addition"(DEA), where a DEA is an equation of the form $(\mathbf{x} \boxplus \mathbf{y}) \oplus ((\mathbf{x} \oplus \mathbf{a}) \boxplus (\mathbf{y} \oplus \mathbf{b})) = \mathbf{c}$ (where $\mathbf{a}, \mathbf{b}, \mathbf{c}$ are given and $\mathbf{x}, \mathbf{y}$ are to be found). Paul&Preneel [7] studied the decision problem for systems of DEAs, showed that it is in $\mathcal{P}$, and moreover gave efficient

algorithms to solve such systems completely if solutions exists.

(3) Linear cryptanalysis (LC):
Wallén [10] gave a formula for the linear correlations of addition mod 2^n and undertook an in depth study of the algorithmic aspects of computing them. However, the formula is not explicit in the sense that one of its ingredients has to be computed recursively (for details, see the remark after Theorem 4 below). Another method for the computation of linear correlations of addition, applicable also in the case of more than two summands, was shown by Nyberg&Wallén in [6].

1.1 Our results

We observe that addition mod 2^n is CCZ-equivalent to a quadratic vectorial Boolean function and apply this to the circle of questions above.
DC: We show that the solution of systems of DEA can be reduced to the solution of systems of very simple linear equations.
In the course we give a simple re-derivation for the Lipmaa-Moriai explicit formula for the differential probabilities of addition.
LC: We give a completely explicit formula for the Walsh transform of addition. We use this formula to determine maximal correlations for the case where one or two input masks are fixed.
The simplicity of our results and the easiness of obtaining them indicate that CCZ-equivalence is the natural framework to treat these aspects of addition.

2 Prelimimaries

2.1 Notations and Conventions, Reminder

Bits and bit vectors, modular addition

Throughout n is a fixed natural number.

$\mathbb{F}_2$ denotes the field with the two elements $0, 1$ ("bits"), $\mathbb{F}_2^n$ denotes the $\mathbb{F}_2$-vector space of bit vectors of length n. We write the elements of $\mathbb{F}_2^n$ as rows (i.e. $1 \times n$ matrices) and denote them by small bold face letters. Subscripted indices denote coordinates. The left most coordinate of a bit vector $\mathbf{x}$ has the index 0 and corresponds to the least significant bit of $\overline{\mathbf{x}}$. Bit vectors are always written in the form $\mathbf{x} = (x_0, \ldots, x_{n-1})$,i.e. "little-endian".

$\oplus$ denotes binary addition (of bits as well as of bit vectors).

For $\mathbf{x} = (x_0, \ldots, x_{n-1}) \in \mathbb{F}_2^n$ we let $\overline{\mathbf{x}} := \sum_{i=0}^{n-1} x_i 2^i \in \mathbb{N}$ denote the natural number represented by $\mathbf{x}$. Identifying bit vectors with natural numbers in this way, the addition mod 2^n of elements $\overline{\mathbf{x}}, \overline{\mathbf{y}} \in \mathbb{Z}_{2^n}$ gives an operation on $\mathbb{F}_2^n$. We denote this "modular addition"by $\boxplus$ (i.e. $\mathbf{x} \boxplus \mathbf{y} \cong (\overline{\mathbf{x}} + \overline{\mathbf{y}}) \bmod 2^n$).

For bit vectors $\mathbf{x}, \mathbf{y} \in \mathbb{F}_2^n$ we denote their bitwise AND with $\mathbf{x} \star \mathbf{y}$ (i.e. $\mathbf{x} \star \mathbf{y} = (x_0 y_0, \ldots, x_{n-1} y_{n-1})$), and their bitwise OR with $\mathbf{x}|\mathbf{y}$ (i.e. $\mathbf{x}|\mathbf{y} = (x_0|y_0, \ldots, x_{n-1}|y_{n-1})$).

The all one vector is denoted by $\mathbf{e}$, the bitwise complement of $\mathbf{x}$ then is $\mathbf{x} \oplus \mathbf{e}$.

$\preceq$ denotes the partial order on $\mathbb{F}_2^n$ defined by $\mathbf{x} \preceq \mathbf{y} \Leftrightarrow x_i \leq y_i \ \forall i \in \{0, \ldots, n-1\}$

The Hammingweight (also called "length") of $\mathbf{x} \in \mathbb{F}_2^n$ is denoted by $|\mathbf{x}|$.

For any $\mathbf{z} \in \mathbb{F}_2^n$ the set $U_{\mathbf{z}} := \{\mathbf{x} \in \mathbb{F}_2^n \ : \ \mathbf{x} \preceq \mathbf{z}\}$ is an $\mathbb{F}_2$-vectorspace of dimension $|\mathbf{z}|$.

The algebraic normal form (ANF) of a vectorial boolean function $\mathbf{f} : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^m$ is given by the 2^n coefficients $\mathbf{c_f}(\mathbf{z})$, $\mathbf{z} \in \mathbb{F}_2^n$ where $\mathbf{c_f}(\mathbf{z}) := \bigoplus_{\mathbf{x} \preceq \mathbf{z}} \mathbf{f}(\mathbf{x}) \in \mathbb{F}_2^m$.
The degree of a vectorial Boolean function is $\deg \mathbf{f} := \max\{|\mathbf{z}| \ : \ \mathbf{c_f}(\mathbf{z}) \neq \mathbf{0}\}$.
A vectorial Boolean function of degree 2 is called quadratic.

The $k-$th vector of the standard basis of $\mathbb{F}_2^n$ is denoted by $\mathbf{e}_k$, $0 \leq k \leq n-1$.

The superscript t indicates transposition of a matrix.

If $S \in \mathbb{F}_2^{m \times n}$ is a matrix and $\mathbf{x} \in \mathbb{F}_2^n$ we let $S(\mathbf{x}) := \mathbf{x}S^t \in \mathbb{F}_2^m$, i.e. we don't distinguish in notation between S and the linear mapping defined by S w.r. to the standard bases domain and codomain.

$L : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^n$ denotes the "left shift" $\mathbf{x} = (x_0, \ldots, x_{n-1}) \mapsto L(\mathbf{x}) = (x_1, \ldots, x_{n-1}, 0)$.

$R : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^n$ denotes the "right shift" $\mathbf{x} = (x_0, \ldots, x_{n-1}) \mapsto R(\mathbf{x}) = (0, x_0, \ldots, x_{n-2})$.

Finally $M : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^n$ denotes the (right shifted) "partial sums mapping"

$$\mathbf{x} = (x_0, \ldots, x_{n-1}) \mapsto M(\mathbf{x}) = (0, x_0, x_0 \oplus x_1, \ldots, x_0 \oplus \ldots \oplus x_{n-2})$$

I denotes the identity matrix. Clearly $M = R(I \oplus R)^{-1} = (I \oplus R)^{-1}R$ and $L = R^t$, $R = L^t$

Fourier transform

We use the Fourier transform on the abelian group $(\mathbb{F}_2^n, \oplus)$ in the following form:

We write the standard character χ of $(\mathbb{F}_2, \oplus)$ (i.e. $\chi(0) = 1$, $\chi(1) = -1$) in the suggestive form $\chi(x) = (-1)^x$.

For two binary vectors $\mathbf{x}, \mathbf{y} \in \mathbb{F}_2^n$ we let $\mathbf{x} \cdot \mathbf{y} := \mathbf{x}\mathbf{y}^t = \bigoplus_{i=0}^{n-1} x_i \, y_i$.

Each $\mathbf{y} \in \mathbb{F}_2^n$ defines a charakter $\chi_{\mathbf{y}}$ of $(\mathbb{F}_2^n, \oplus)$ by

$$\chi_{\mathbf{y}} : \mathbb{F}_2^n \longrightarrow \mathbb{C}, \ \ \chi_{\mathbf{y}}(x) := \chi(\mathbf{y} \cdot \mathbf{x}) = (-1)^{\mathbf{y} \cdot \mathbf{x}}.$$

We identify $\mathbb{F}_2^n$ with its character group via $\mathbf{y} \cong \chi_{\mathbf{y}}$.

For a real function $f : \mathbb{F}_2^n \longrightarrow \mathbb{R}$ and $\mathbf{u} \in \mathbb{F}_2^n$ we define the Fourier transform $\hat{f}$ by

$$\hat{f}(\mathbf{u}) := \sum_{\mathbf{x} \in \mathbb{F}_2^n} f(\mathbf{x})(-1)^{\mathbf{u} \cdot \mathbf{x}}$$

We a call a mapping $\mathbf{g} : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^m$ a vectorial Boolean function. For such a vectorial Boolean function and $\mathbf{t} \in \mathbb{F}_2^m, \mathbf{u} \in \mathbb{F}_2^n$ we define the Walsh transform $W_{\mathbf{g}}$ by

$$W_{\mathbf{g}}(\mathbf{t}, \mathbf{u}) := \sum_{\mathbf{x} \in \mathbb{F}_2^n} (-1)^{\mathbf{t} \cdot \mathbf{g}(\mathbf{x}) \oplus \mathbf{u} \cdot \mathbf{x}}.$$

We call the value $\phi_{\mathbf{g}}(\mathbf{t},\mathbf{u}) := \frac{W_{\mathbf{g}}(\mathbf{t},\mathbf{u})}{2^n}$ the "linear correlation" of $\mathbf{g}$ at $(\mathbf{t},\mathbf{u})$.
Clearly $W_{\mathbf{g}} = \hat{1}_{G_{\mathbf{g}}}$, that is, the Walsh transform of the vectorial Boolean function $\mathbf{g}$ is simply the ordinary Fourier transform of the indicator function $1_{G_{\mathbf{g}}}$ of the graph

$$G_{\mathbf{g}} := \{(\mathbf{g}(\mathbf{x}),\mathbf{x}) \,:\, \mathbf{x} \in \mathbb{F}_2^n \,\} \subset \mathbb{F}_2^{n+m} \quad .$$

CCZ-equivalence of vectorial boolean functions

Vectorial Boolean functions $\mathbf{h},\mathbf{g} : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^m$ are called CCZ-equivalent([3]) iff there is an affine-linear permutation A of $\mathbb{F}_2^{n+m}$ such that

$$G_{\mathbf{g}} = A(G_{\mathbf{h}})$$

that is, $\mathbf{h}$ and $\mathbf{g}$ are CCZ-equivalent iff the graph $G_{\mathbf{h}}$ of $\mathbf{h}$ can be affine-linearly transformed into the graph $G_{\mathbf{g}}$ of $\mathbf{g}$.

3 CCZ-equivalence

3.1 Recursive carry computation

The "grade school method" for adding integers $\overline{\mathbf{x}},\overline{\mathbf{y}}$ in the binary number system is well known (see e.g.[9]). Let $c_j = c_j(\mathbf{x},\mathbf{y})$ denote the carry-bit which is produced in position $j-1$ and added in position j and let $\mathbf{c} = \mathbf{c}(\mathbf{x},\mathbf{y})$ be the carry vector produced in the modular addition of $\mathbf{x}$ and $\mathbf{y}$. Then the grade school addition algorithm performs the following recursion: $c_0 = 0$ and $(\mathbf{x} \boxplus \mathbf{y})_j = x_j \oplus y_j \oplus c_j$ and $c_{j+1} = x_j y_j \oplus (x_j \oplus y_j)c_j$ (since a carry is produced at position j iff the majority of x_j, y_j, c_j is 1).
Clearly this also computes the carry for the addition mod 2^n if done up to $j = n-1$.

3.2 Linear equivalence of the modular addition graph

For cryptographic purposes one is interested in the Walsh spectrum and in the differential spectrum of modular addition. These are properties of the graph

$$G_{\boxplus} := \{(\mathbf{x} \boxplus \mathbf{y},\mathbf{x},\mathbf{y}) \,:\, \mathbf{x} \in \mathbb{F}_2^n \,, \mathbf{y} \in \mathbb{F}_2^n \,\} \subset \mathbb{F}_2^{3n} \quad .$$

In general, if for sets $A, B \subset \mathbb{F}_2^m$ and a linear permutation T the relation $A = T(B)$ holds, then the Walsh resp. differential properties are transformed by the relations

$$\hat{1}_A(\mathbf{u}) = \hat{1}_B(T^t(\mathbf{u}))$$

resp.

$$(1_A * 1_A)(\mathbf{x}) = (1_B * 1_B)(T^{-1}(\mathbf{x})) \quad \text{(here } * \text{ denotes convolution)}$$

It is therefore of great value to observe that the graph of modular addition can be linearly transformed into the graph of a much simpler vectorial Boolean function.

To describe this let $\mathbf{q} : \mathbb{F}_2^n \times \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^n$ the mapping $(\mathbf{x}, \mathbf{y}) \mapsto M(\mathbf{x} \star \mathbf{y})$, and let

$$G_{\mathbf{q}} := \{(\mathbf{q}(\mathbf{x}, \mathbf{y}), \mathbf{x}, \mathbf{y}) \, : \, \mathbf{x} \in \mathbb{F}_2^n \, , \, \mathbf{y} \in \mathbb{F}_2^n \, \}$$

be the graph of $\mathbf{q}$.
The following lemma is the basis for our results.

Lemma 1. *The mapping*

$$\beta : \mathbb{F}_2^n \times \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^n \times \mathbb{F}_2^n \, , \, (\mathbf{x}, \mathbf{y}) \mapsto (\mathbf{x} \oplus \mathbf{c}(\mathbf{x}, \mathbf{y}), \mathbf{y} \oplus \mathbf{c}(\mathbf{x}, \mathbf{y}))$$

is a bijection with inverse

$$\alpha : \mathbb{F}_2^n \times \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^n \times \mathbb{F}_2^n \, , \, (\mathbf{x}, \mathbf{y}) \mapsto (\mathbf{x} \oplus \mathbf{q}(\mathbf{x}, \mathbf{y}), \mathbf{y} \oplus \mathbf{q}(\mathbf{x}, \mathbf{y}))$$

Proof. Let $\mathbf{c} = \mathbf{c}(\mathbf{x}, \mathbf{y})$ be the carry vector produced in the modular addition of $\mathbf{x}$ and $\mathbf{y}$. By the grade school algorithm (see 3.1. above) we have $c_0 = 0$ and $c_{j+1} \oplus c_j = (x_j \oplus c_j) \cdot (y_j \oplus c_j)$ for $j = 0, \ldots, n-2$. Thus $(I \oplus R)(\mathbf{c}) = R((\mathbf{x} \oplus \mathbf{c}) \star (\mathbf{y} \oplus \mathbf{c}))$ and hence $\mathbf{c} = M((\mathbf{x} \oplus \mathbf{c}) \star (\mathbf{y} \oplus \mathbf{c})) = \mathbf{q}(\mathbf{x} \oplus \mathbf{c}, \mathbf{y} \oplus \mathbf{c})$.
Since $(\mathbf{x}, \mathbf{y}) = (\mathbf{x} \oplus \mathbf{c}, \mathbf{y} \oplus \mathbf{c}) \oplus (\mathbf{c}, \mathbf{c})$ and since $\mathbf{c}$ can be computed from $(\mathbf{x} \oplus \mathbf{c}), (\mathbf{y} \oplus \mathbf{c})$ the mapping $\mathbb{F}_2^{2n} \ni (\mathbf{x}, \mathbf{y}) \mapsto (\mathbf{x} \oplus \mathbf{c}(\mathbf{x}, \mathbf{y}), \mathbf{y} \oplus \mathbf{c}(\mathbf{x}, \mathbf{y})) \in \mathbb{F}_2^{2n}$ is injective (hence bijective). Since $\mathbf{c} = \mathbf{q}(\mathbf{x} \oplus \mathbf{c}, \mathbf{y} \oplus \mathbf{c})$ the inverse mapping is $(\mathbf{x}, \mathbf{y}) \mapsto (\mathbf{x} \oplus \mathbf{q}(\mathbf{x}, \mathbf{y}), \mathbf{y} \oplus \mathbf{q}(\mathbf{x}, \mathbf{y}))$ □

Theorem 1. *(CZZ-equivalence of $\boxplus$ and q)*
The linear mapping $T : (\mathbb{F}_2^n)^3 \longrightarrow (\mathbb{F}_2^n)^3, (\mathbf{x}, \mathbf{y}, \mathbf{z}) \mapsto T(\mathbf{x}, \mathbf{y}, \mathbf{z}) = (\mathbf{x} \oplus \mathbf{y} \oplus \mathbf{z}, \mathbf{x} \oplus \mathbf{y}, \mathbf{x} \oplus \mathbf{z})$ maps the graph of G_q bijectively onto the graph of $G_{\boxplus}$.

Proof. Let $(\mathbf{x}', \mathbf{y}') := \beta(\mathbf{x}, \mathbf{y}) = (\mathbf{x} \oplus \mathbf{c}(\mathbf{x}, \mathbf{y}), \mathbf{y} \oplus \mathbf{c}(\mathbf{x}, \mathbf{y}))$ We have

$$\begin{aligned} G_{\boxplus} &= \{(\mathbf{c}(\mathbf{x}, \mathbf{y}) \oplus \mathbf{x} \oplus \mathbf{y}, \mathbf{x}, \mathbf{y}) \, : \, \mathbf{x} \in \mathbb{F}_2^n \, , \mathbf{y} \in \mathbb{F}_2^n \, \} \\ &= \{(\mathbf{c}(\mathbf{x}, \mathbf{y}) \oplus \mathbf{x} \oplus \mathbf{y}, \mathbf{x} \oplus \mathbf{c}(\mathbf{x}, \mathbf{y}) \oplus \mathbf{c}(\mathbf{x}, \mathbf{y}), \mathbf{y} \oplus \mathbf{c}(\mathbf{x}, \mathbf{y}) \oplus \mathbf{c}(\mathbf{x}, \mathbf{y})) \, : \, \mathbf{x} \in \mathbb{F}_2^n \, , \\ &\qquad \mathbf{y} \in \mathbb{F}_2^n \, \} \\ &= \{(\mathbf{q}(\mathbf{x}', \mathbf{y}') \oplus \mathbf{x}' \oplus \mathbf{y}', \mathbf{q}(\mathbf{x}', \mathbf{y}') \oplus \mathbf{x}', \mathbf{q}(\mathbf{x}', \mathbf{y}') \oplus \mathbf{y}') \, : \, \mathbf{x}' \in \mathbb{F}_2^n \, , \mathbf{y}' \in \mathbb{F}_2^n \, \} \end{aligned}$$

where the final equality follows from lemma 1. The result is now obvious. □

Some remarks:

1. Thus for each $n \geq 1$ the mappings $(\mathbf{x}, \mathbf{y}) \mapsto \mathbf{x} \boxplus \mathbf{y}$ and $(\mathbf{x}, \mathbf{y}) \mapsto \mathbf{q}(\mathbf{x}, \mathbf{y})$ give an example of a pair of vectorial Boolean functions $F, G : \mathbb{F}_2^{2n} \longrightarrow \mathbb{F}_2^n$ which are CCZ-equivalent.
2. Written in coordinates , $\mathbf{q}$ is the vectorial Boolean function

   $$(\mathbf{x}, \mathbf{y}) \mapsto (0, x_0 y_0, x_0 y_0 \oplus x_1 y_1, \ldots, x_0 y_0 \oplus \ldots \oplus x_{n-2} y_{n-2})$$

   For $j \geq 1$ the ANF of the coordinate function $q_j(x, y)$ is of degree 2 in the variables $x_0, \ldots, x_{n-1}, y_0, \ldots, y_{n-1}$. On the other hand it is easy to see that the ANF of the coordinate function $(\mathbf{x}, \mathbf{y}) \mapsto (\mathbf{x} \boxplus \mathbf{y})_j$ is of degree $j + 1$ in these variables. For $n \geq 3$ therefore $\boxplus$ and $\mathbf{q}$ can not possibly be (extended) affine equivalent.

3. Of course, addition mod 2^n is e.g also CCZ-equivalent to the vectorial Boolean function
$$(\mathbf{x}, \mathbf{y}) \mapsto (x_0 y_0, x_1 y_1, \ldots, x_{n-2} y_{n-2}, 0)$$
and others. Since such standard linear equivalences of $\mathbf{q}$ do not add anything substantially new to the picture, we do not consider them here.
4. The recursion for the carries is also the starting point of all other published investigations of the boolean properties of addition mod 2^n . New in the approach here is the use of the bijections α, β to exploit CCZ-equivalence.
5. The graph of addition mod 2^n is thus "only" the graph of a quadratic vectorial function. From this perspective addition mod 2^n is a very simple boolean operation. Here we use this fact only to revisit the linear and differential properties of addition mod 2^n , but it should be clear that it can potentially also be useful for algebraic attacks.

4 Differential properties

The differential properties of quadratic vectorial Boolean functions are easy to describe, since their difference functions are affine-linear. To take advantage of this fact here, we observe:

Theorem 2. *Let* $\mathbf{a}, \mathbf{b}, \mathbf{d} \in \mathbb{F}_2^n$ *and for* $\mathbf{x}, \mathbf{y} \in \mathbb{F}_2^n$ *let* $(\mathbf{x}', \mathbf{y}') := \alpha(\mathbf{x}, \mathbf{y}) = (\mathbf{x} \oplus \mathbf{q}(\mathbf{x}, \mathbf{y}), \mathbf{y} \oplus \mathbf{q}(\mathbf{x}, \mathbf{y}))$. *Then* $\mathbf{q}(\mathbf{x} \oplus \mathbf{a}, \mathbf{y} \oplus \mathbf{b}) = \mathbf{q}(\mathbf{x}, \mathbf{y}) \oplus \mathbf{d} \Leftrightarrow$
$$(\mathbf{x}' \boxplus \mathbf{y}') \oplus ((\mathbf{x}' \oplus \mathbf{a} \oplus \mathbf{d}) \boxplus (\mathbf{y}' \oplus \mathbf{b} \oplus \mathbf{d})) = \mathbf{a} \oplus \mathbf{b} \oplus \mathbf{d}$$

Equivalently

$$\mathbf{q}(\mathbf{x} \oplus \mathbf{b} \oplus \mathbf{d}, \mathbf{y} \oplus \mathbf{a} \oplus \mathbf{d}) = \mathbf{q}(\mathbf{x}, \mathbf{y}) \oplus \mathbf{a} \oplus \mathbf{b} \oplus \mathbf{d} \;\Leftrightarrow\; (\mathbf{x}' \boxplus \mathbf{y}') \oplus ((\mathbf{x}' \oplus \mathbf{a}) \boxplus (\mathbf{y}' \oplus \mathbf{b})) = \mathbf{d}$$

But the left equation is the same as

$$R(\mathbf{x} \star (\mathbf{a} \oplus \mathbf{d})) \oplus R(\mathbf{y} \star (\mathbf{b} \oplus \mathbf{d})) = R((\mathbf{a} \oplus \mathbf{d}) \star (\mathbf{b} \oplus \mathbf{d})) \oplus (I \oplus R)(\mathbf{a} \oplus \mathbf{b} \oplus \mathbf{d}) \quad (**),$$

i.e. a (very simple) system of linear equations.
Thus the set of solutions of a DEA is simply an affine linear subspace of $(\mathbb{F}_2^n)^2$, "deformed" by α. This observation reduces the question of solvability resp. the computation of all solutions of a system of DEAs to linear algebra: just solve the equivalent linear system first, and then compute the image of the solution set under α. We remark that single equations of this type can easily be solved explicitly:

Lemma 2. *Let* $\mathbf{a}, \mathbf{b}, \mathbf{d} \in \mathbb{F}_2^n$ *and consider the equation*
$$(\mathbf{a} \star \mathbf{x}) \oplus (\mathbf{b} \star \mathbf{y}) = \mathbf{d} \quad (*)$$
Then $(*)$ *has a solution iff* $\mathbf{d} \preceq \mathbf{a}|\mathbf{b}$. *In this case* $(\mathbf{x}_0, \mathbf{y}_0) := (\mathbf{a} \star \mathbf{d}, (\mathbf{b} \oplus \mathbf{a} \star \mathbf{b}) \star \mathbf{d})$ *is a solution. All other solutions can be obtained from* $(\mathbf{x}_0, \mathbf{y}_0)$ *by modifying* $\mathbf{y}_0$ *arbitrarily at positions* i *were* $a_i = 1, b_i = 0$, *modifying* $\mathbf{x}_0$ *arbitrarily at the positions where* $a_i = 0, b_i = 1$, *modifying* $\mathbf{x}_0, \mathbf{y}_0$ *in the same way (i.e. leaving* $x_i \oplus y_i$ *unchanged) where* $a_i = b_i = 1$ *and choosing* x_i, y_i *arbitrarily if* $a_i = b_i = 0$. *Thus there are* $2^{2n - |\mathbf{a}|\mathbf{b}|}$ *solutions, if solutions exist.*

This leads immediately to the solutions of $(**)$.

Corollary 1. $(\mathbf{x}' \boxplus \mathbf{y}') \oplus ((\mathbf{x}' \oplus \mathbf{a}) \boxplus (\mathbf{y}' \oplus \mathbf{b})) = \mathbf{d}$ *(or equivalently* $(**)$ *) has solutions iff*

$$(I \oplus R)(\mathbf{a} \oplus \mathbf{b} \oplus \mathbf{d}) \preceq R(\mathbf{a} \oplus \mathbf{d}) | R(\mathbf{b} \oplus \mathbf{d})$$

In this case, with $\hat{\mathbf{d}} := R((\mathbf{a} \oplus \mathbf{d}) * (\mathbf{b} \oplus \mathbf{d})) \oplus (I \oplus R)(\mathbf{a} \oplus \mathbf{b} \oplus \mathbf{d})$, $\hat{\mathbf{a}} := R(\mathbf{a} \oplus \mathbf{d})$, $\hat{\mathbf{b}} := R(\mathbf{b} \oplus \mathbf{d})$ *a special solution is given by* $(\mathbf{x}_0, \mathbf{y}_0) := (L(\hat{\mathbf{a}} \star \hat{\mathbf{d}}), L((\hat{\mathbf{b}} \oplus \hat{\mathbf{a}} \star \hat{\mathbf{b}}) \star \hat{\mathbf{d}}))$ *. Since* $\mathbf{x}_0 \star \mathbf{y}_0 = \mathbf{0}$ *for this special solution* $\mathbf{x}'_0 = \mathbf{x}_0$, $\mathbf{y}'_0 = \mathbf{y}_0$.

Combining the two preceding results we find:

Theorem 3. *(Lipmaa-Moriai) Let* (X, Y) *be uniformly distributed on* $\mathbb{F}_2^n \times \mathbb{F}_2^n$ *. Then*

$$P\left((X \boxplus Y) \oplus ((X \oplus \mathbf{a}) \boxplus (Y \oplus \mathbf{b})) = \mathbf{d}\right) = 1_{\{(I \oplus R)(\mathbf{a} \oplus \mathbf{b} \oplus \mathbf{d}) \preceq R((\mathbf{a} \oplus \mathbf{d}) | (\mathbf{b} \oplus \mathbf{d}))\}} 2^{-|(R((\mathbf{a} \oplus \mathbf{d}) | (\mathbf{b} \oplus \mathbf{d}))|}$$

This is theorem 1 from [5] (up to notation), where it forms the basis of an extensive discussion of the differential spectrum of addition mod 2^n .

Finally we note that solving systems of DEAs is much easier than solving general linear equations. In fact, by theorem 2 a system of k DEAs is equivalent to a system of equations of the form

$$(\mathbf{a}_i \star \mathbf{x}) \oplus (\mathbf{b}_i \star \mathbf{y}) = \mathbf{d}_i \quad i = 1, \ldots, k$$

(plus trivial equations for the least significant bits). The linear equations on the lhs of each such equation are described by a coefficient matrix $\begin{pmatrix} A_i & B_i \end{pmatrix}$ where A_i, B_i are diagonal matrices. Therefore such a system of equations can be solved extremely efficiently.

5 Linear correlations of addition mod 2^n

In this section we revisit linear correlations of addition. We show that CCZ-equivalence leads to a simple explicit formula for the correlation coefficients and use this formula to extend the results of [10].
Let $\mathbf{u} := (u_0, \ldots, u_{n-1})$, $\mathbf{v} := (v_0, \ldots, v_{n-1})$, $\mathbf{w} := (w_0, \ldots, w_{n-1}) \in \mathbb{F}_2^n$
($\mathbf{u}$ is the "output mask", and $\mathbf{v}, \mathbf{w}$ are the "input masks"), and let $\mathbf{z} = M^t(\mathbf{u})$.

We are interested in the linear correlations coefficients of addition mod 2^n

$$\phi_2(\mathbf{u}, \mathbf{v}, \mathbf{w}) := E(-1)^{\mathbf{u} \cdot (X \boxplus Y) \oplus \mathbf{v} \cdot X \oplus \mathbf{w} \cdot Y} = \frac{1}{2^{2n}} \hat{1}_{G_\boxplus}(\mathbf{u}, \mathbf{v}, \mathbf{w})$$

(where X, Y are independent and uniformly distributed on $\{0,1\}^n$) .
By the above we need only compute the Walsh transform of $\mathbf{q}$, as (by theorem 1) the relation

$$\phi_2(\mathbf{u}, \mathbf{v}, \mathbf{w}) = \phi_q(\mathbf{u} \oplus \mathbf{v} \oplus \mathbf{w}, \mathbf{u} \oplus \mathbf{v}, \mathbf{u} \oplus \mathbf{w}) \quad (*)$$

holds. But $\phi_{\mathbf{q}}(\mathbf{u}, \mathbf{vw})$ is easy to compute:

$$\begin{aligned}\phi_{\mathbf{q}}(\mathbf{u}, \mathbf{vw}) &= E(-1)^{M^t(\mathbf{u})\cdot(X\star Y)\oplus \mathbf{v}\cdot X\oplus \mathbf{w}\cdot Y} \\ &= \delta_{0,v_{n-1}}\delta_{0,w_{n-1}}\prod_{i=1}^{n-1} E(-1)^{z_iX_iY_i+v_iX_i+w_iY_i} \\ &= 1_{\{\mathbf{v}\preceq\mathbf{z}\}}1_{\{\mathbf{w}\preceq\mathbf{z}\}}(-1)^{\mathbf{v}\cdot\mathbf{w}}2^{-|\mathbf{z}|}\end{aligned}$$

(Here we have used the fact that for bits a, b, c and independent uniform random bits X, Y the relation $E(-1)^{aXY\oplus bX\oplus cY} = 1_{\{b\preceq a\}}1_{\{c\preceq a\}}(-1)^{bc}2^{-a}$ holds.) We thus have:

Theorem 4. *(Walsh transform of addition* mod 2^n *))*
Let $\mathbf{z} := M^t(\mathbf{u}\oplus\mathbf{v}\oplus\mathbf{w})$. *Then*

$$\phi_2(\mathbf{u}, \mathbf{v}, \mathbf{w}) = 1_{\{\mathbf{u}\oplus\mathbf{v}\preceq\mathbf{z}\}}1_{\{\mathbf{u}\oplus\mathbf{w}\preceq\mathbf{z}\}}(-1)^{(\mathbf{u}\oplus\mathbf{w})\cdot(\mathbf{u}\oplus\mathbf{v})}2^{-|\mathbf{z}|} \quad (*) \quad \textit{resp.}$$

$$\phi_2(\mathbf{u}, \mathbf{u}\oplus\mathbf{v}, \mathbf{u}\oplus\mathbf{w}) = 1_{\{\mathbf{v}\preceq\mathbf{z}\}}1_{\{\mathbf{w}\preceq\mathbf{z}\}}(-1)^{\mathbf{v}\cdot\mathbf{w}}2^{-|\mathbf{z}|}$$

Some remarks

1. This theorem is equivalent to Theorem 1 of [10], however, there the simple explicit description of $\mathbf{z}$ was not obtained. Instead $\mathbf{z}$ had to be computed recursively from the vectors $\mathbf{u}$ and $\mathbf{v}\oplus\mathbf{w}\oplus\mathbf{e}$. It is this explicit description of $\mathbf{z}$ as $\mathbf{z} = M^t(\mathbf{u}\oplus\mathbf{v}\oplus\mathbf{w})$ which gives additional insight into the Walsh spectrum of addition.
2. If the absolute value of $\phi_2(\mathbf{u}, \mathbf{v}, \mathbf{w})$ is non-zero it e.g. only depends on the Hamming weight of the binary vector $M^t(\mathbf{u}\oplus\mathbf{v}\oplus\mathbf{w})$. With $\mathbf{s} := \mathbf{u}\oplus\mathbf{v}\oplus\mathbf{w}$ we have $\mathbf{z} = (s_1\oplus\ldots s_{n-1}, s_2\oplus\ldots\oplus s_{n-1}, \ldots, s_{n-2}\oplus s_{n-1}, s_{n-1}, 0)$.
3. By the above we have the following "pencil and paper" method to compute $\phi_2(\mathbf{u}, \mathbf{v}, \mathbf{w})$:
   (a) compute $\mathbf{s} := \mathbf{u}\oplus\mathbf{v}\oplus\mathbf{w}$.
   (b) compute recursively $z_{n-1} = 0$, $z_{i-1} = z_i \oplus s_i$ for $i \geq 1$.
   (c) $\phi_2(\mathbf{u}, \mathbf{v}, \mathbf{w})$ is non-zero, iff for all i with $z_i = 0$ the equality $u_i = v_i = w_i$ holds.
   In this case the absolute value of $\phi_2(\mathbf{u}, \mathbf{v}, \mathbf{w})$ is $2^{-|\mathbf{z}|}$ and the sign is -1 iff the Hamming weight $|(\mathbf{u}\oplus\mathbf{v})\star(\mathbf{u}\oplus\mathbf{w})|$ is odd.

We collect some properties of the correlation matrix:

Corollary 2. *(symmetry properties)*

1. $\phi_2(\mathbf{u}, \mathbf{v}, \mathbf{w}) = (-1)^{(\mathbf{u}\oplus\mathbf{v})\cdot(\mathbf{u}\oplus\mathbf{v})}\phi_2(\mathbf{v}, \mathbf{u}, \mathbf{w}) = (-1)^{(\mathbf{u}\oplus\mathbf{w})\cdot(\mathbf{u}\oplus\mathbf{w})}\phi_2(\mathbf{w}, \mathbf{v}, \mathbf{u})$
2. $\phi_2(\mathbf{u}, \mathbf{v}, \mathbf{w}) = \phi_2(\mathbf{u}, \mathbf{w}, \mathbf{v})$

Corollary 3. *(values of some special linear correlations)*

1. $\phi_2(\mathbf{u}, \mathbf{u}, \mathbf{u}) = 2^{-|M^t(\mathbf{u})|}$
2. $\phi_2(\mathbf{u}, \mathbf{u}\oplus L(\mathbf{u}), \mathbf{u}) = 2^{-|L(\mathbf{u})|}$

3. *If* $\mathbf{e}_k \preceq M^t(\mathbf{u})$ *for a standard basis vector* $\mathbf{e}_k$ *then* $\phi_2(\mathbf{u}, \mathbf{u} \oplus \mathbf{e}_k, \mathbf{u}) \neq 0$. *The corresponding vector* $\mathbf{z} = M^t(\mathbf{u} \oplus \mathbf{e}_k) = M^t(\mathbf{u}) \oplus \bigoplus_{i=0}^{k-1} \mathbf{e}_i$, *i.e. it is computed from the corresponding* $z = M^t(\mathbf{u})$ *for* $(\mathbf{u}, \mathbf{u}, \mathbf{u})$ *by complementation below* k.

In cryptanalysis one is mainly interested in correlations of high absolute value. In the sequel we deal with the problem of determining "best" approximations when one or two of the masks are fixed.

5.1 A combinatorial problem

Consider the following problem: given $\mathbf{u} \in \mathbb{F}_2^n$, let

$$\mathcal{A}_L(\mathbf{u}) := \{\mathbf{x} \in \mathbb{F}_2^n \ : \mathbf{x} \oplus \mathbf{u} \preceq L(\mathbf{x})\}$$

Problem: find a $L-$minimal vector for $\mathbf{u}$, i.e. find a vector $\mathbf{a} = \mathbf{a}(\mathbf{u}) \in \mathcal{A}_L(\mathbf{u})$ s.th. the Hamming weight $|L(\mathbf{a})|$ is minimal.
It is clear that $\mathcal{A}_L(\mathbf{u}) \neq \emptyset$, since clearly $\mathbf{u} \in \mathcal{A}_L(\mathbf{u})$. Thus there exist solutions.

We need the following assertion (the proof is deferred to appendix A):

Theorem 5. (= Theorem A.3) *Let* $\mathbf{u} \in \mathbb{F}_2^n$.
Let $\mathbf{a}_L(\mathbf{u}) := \mathbf{u} \oplus (\mathbf{u} \star L(\mathbf{u})) \oplus \ldots \oplus (\mathbf{u} \star L(\mathbf{u}) \star L^2(\mathbf{u}) \star \cdots \star L^{n-1}(\mathbf{u}))$.
Then $\mathbf{a}_L(\mathbf{u})$ *is a L-minimal vector for* $\mathbf{u}$.

The function $\mathbf{a}_L(\mathbf{u})$ was introduced in [5] under the name of "all one parity".

5.2 Maximal correlations

We return to the problem of determining maximal correlations of addition mod 2^n .
In order to have a convenient way to formulate the results we call the elements $\phi_2(\mathbf{u}, ., .)$ the "row" $\mathbf{u}$ of the correlation matrix, and the elements $\phi_2(., \mathbf{v}, \mathbf{w})$ the "column" $(\mathbf{v}, \mathbf{w})$ of the correlation matrix. (By the the symmetry properties (lemma 3) only these cases need to be considered.) We first treat the row case.

Row maxima

Theorem 6. *(row maxima) Let* $\mathbf{u} \in \mathbb{F}_2^n$ *and* $\mathbf{b}(u) := (I \oplus L)(\mathbf{a}_L(\mathbf{u}))$

1. *In row* $\mathbf{u}$ *of* ϕ_2 *the element* $\phi_2(\mathbf{u}, \mathbf{b}(\mathbf{u}), \mathbf{u})$ *is an element of maximal modulus*
2. $\phi_2(\mathbf{u}, \mathbf{b}(\mathbf{u}), \mathbf{u}) = 2^{-d(\mathbf{u})}$
3. $d(\mathbf{u}) := |L(\mathbf{a}_L(\mathbf{u}))| = \sum_{\{B \,:\, B \text{ One-block in } L\mathbf{u}\}} \lceil |B|/2 \rceil$

By theorem 6.3 the structure and number of ones in $L(\mathbf{u})$ determine the linear approximability of $\mathbf{u} \cdot (\mathbf{x} \boxplus \mathbf{y})$ in a simple way: the less ones, and the better the subdivision in blocks of even length, the higher is the linear approximability.

Example 1.
Let $n = 13$ and let $\mathbf{u} = (1110\,1101\,0011\,1) = (7351)_2$ (little-endian!). Then $L(\mathbf{u}) = (1101\,1010\,0111\,0)$ has 1 one-block of length 1, 2 one-blocks of length 2, and one one-block of length 3. Thus $d(\mathbf{u}) = 1 + 2 + 2 = 5$. Further $a_L(u) = (1010\,0101\,0010\,1) = (5285)_2$ and $\mathbf{b}(\mathbf{u}) = (1110\,1111\,0111\,1) = (7927)_2$. Hence in row 7351 of the correlation matrix the element $\phi_2(7351, 7927, 7351) = 2^{-5}$ is maximal.

Column maxima
Similarly a correlation of maximal modulus can be found when two masks, say $\mathbf{v}$ and $\mathbf{w}$, are fixed. We have to determine $\mathbf{s} = \mathbf{u} \oplus \mathbf{v} \oplus \mathbf{w}$ s.th. $M^t(\mathbf{s})$ has minimal Hamming weight under the side conditions

$$\mathbf{s} \oplus \mathbf{w} = \mathbf{u} \oplus \mathbf{v} \preceq M^t(\mathbf{s}) \quad \text{and} \quad \mathbf{s} \oplus \mathbf{v} = \mathbf{u} \oplus \mathbf{w} \preceq M^t(\mathbf{s}) \; .$$

With $\mathbf{s} = \mathbf{a} \oplus L(\mathbf{a})$ the task then is to determine $\mathbf{a}$ s.th. $L(\mathbf{a})$ has minimal weight under the side conditions

$$\mathbf{a} \oplus \mathbf{v} \preceq L(\mathbf{a}), \;\; \mathbf{a} \oplus \mathbf{w} \preceq L(\mathbf{a}) \quad (*).$$

Especially each solution $\mathbf{a}$ of $(*)$ must fulfil : $\mathbf{v} \oplus \mathbf{w} \preceq L(\mathbf{a})$; i.e. $R(\mathbf{v} \oplus \mathbf{w}) \preceq \mathbf{a}$. Additionally we must have: if $v_i = w_i = 0$ and $a_i = 1$ then it must be that $a_{i+1} = 1$. If a section 10^k in $\mathbf{v}|\mathbf{w}$ corresponds to a section 0^{k+1} in $\mathbf{w} \star \mathbf{v}$, then the corresponding section in $L(\mathbf{a})$ must (for each solution $\mathbf{a}$ of $(*)$) be 1^{k+1}. Let $\mathbf{m}(\mathbf{v}, \mathbf{w})$ denote the the vector which is constructed by these modifications starting from $R(\mathbf{v} \oplus \mathbf{w})$.

Theorem 7. *(column maxima)*
Let $\mathbf{v}, \mathbf{w} \in \mathbb{F}_2^n$ *be given s.th.* $v_{n-1} = w_{n-1} = 1$, *let* $\mathbf{a}(\mathbf{v}, \mathbf{w}) := \mathbf{a}_L(\mathbf{v} \star \mathbf{w}) | \mathbf{m}(\mathbf{v}, \mathbf{w})$ *and let* $\mathbf{u}(\mathbf{v}, \mathbf{w}) := (\mathbf{v} \oplus \mathbf{w}) \oplus (I \oplus L)(\mathbf{a}(\mathbf{v}, \mathbf{w}))$. *Then*

1. $\mathbf{a}(\mathbf{v}, \mathbf{w})$ *is a solution of* $(*)$ *with minimal length and minimal* $|L(\mathbf{a})|$
2. $|\phi_2(\mathbf{u}(\mathbf{v}, \mathbf{w}), \mathbf{v}, \mathbf{w})| = \max\{|\phi_2(\mathbf{u}, \mathbf{v}, \mathbf{w})| \, : \, \mathbf{u} \in \mathbb{F}_2^n \, \}$

Example 2.
Let $n = 11$ and $\mathbf{v} = (1101\,0001\,011) = (1675)_2$, $\mathbf{w} = (0100\,0101\,111) = (1954)_2$, (little-endian!). Then $R(\mathbf{v} \oplus \mathbf{w}) = (0100\,1010\,010)$, $\mathbf{m}(\mathbf{v}, \mathbf{w}) = (0100\,1111\,010)$ and $\mathbf{a}_L(\mathbf{v} \star \mathbf{w}) = (0100\,0001\,001)$. Finally $\mathbf{a}(\mathbf{v}, \mathbf{w}) = (0100\,1111\,011)$, $\mathbf{u}(\mathbf{v}, \mathbf{w}) = (0100\,0101\,001) = (1186)_2$ (little-endian) and the weight of $(\mathbf{u}(\mathbf{v}, \mathbf{w}) \oplus \mathbf{w}) \star (\mathbf{u}(\mathbf{v}, \mathbf{w}) \oplus \mathbf{v})$ is odd. Hence in column $(1675, 1954)$ of the correlation matrix the element $\phi_2(1186, 1675, 1954) = -2^{-7}$ is of maximal absolute value.

One focus of [10],[5] were "efficient" algorithms (where an "efficient" algorithm is one that uses order $\log(wordsize)$ operations on words). In appendix B we show that each of $\mathbf{z}, \mathbf{a}_L(\mathbf{u}), \mathbf{m}(\mathbf{v}, \mathbf{w})$ can be computed efficiently in this sense.

6 Summary

Addition mod 2^n is CCZ-equivalent to a quadratic vectorial Boolean function. This is theoretically interesting and it also leads to practical results: it makes the solution of differential equations of addition extremely easy (Section 4, improving on [7]), and it leads to advanced results on the Walsh transform of addition mod 2^n (identifying for the first time "row"- resp. "column"-maxima and making the formula of [10] explicit). The results are helpful for the analysis of cryptographic primitives which use addition mod 2^n . (E.g. since the correlation matrix F_r of the $MIX(r)$ operation in Threefish is $F_r(\mathbf{t}_1, \mathbf{t}_2; \mathbf{u}_1, \mathbf{u}_2) = \phi_2(\mathbf{t}_1 \oplus \mathbf{t}_2; \mathbf{u}_1, \mathbf{u}_2 \oplus (\mathbf{t}_2 \ggg r))$ the results of section 5 can be applied almost directly in the LC of Threefish). The results show that (in the sense of CCZ-equivalence) addition mod 2^n is a very simple vectorial Boolean function.

References

1. Alquié, D. Approximating addition by xor: How to go all the way. Technical Report 072/2010, Cryptology ePrint Archive, 2010. Available at http://eprint.iacr.org/2010/072.
2. Biham, E. and Shamir, A. Differential cryptanalysis of feal and n-hash. In *Advances in Cryptology - EUROCRYPT 1991*, number 547 in Lecture Notes in Computer Science, pages 1–16, Berlin, 1991. Springer.
3. Carlet, C, Charpin, P. and Zinoviev, V. Codes, bent functions and permutations suitable for des-like crypto systems. *Designs, Codes and Cryptography*, 15(2):125–156, 1998.
4. J. Holte. Carries, combinatorics and an amazing matrix. *American Mathematical Monthly*, 104(2):138–149, 1997.
5. Lipmaa, H. and Moriai, S. Efficient algorithms for computing differential properties of addition. In *Fast Software Encryption 2001*, number 2355 in Lecture Notes in Computer Science, pages 336–350, Berlin, 2002. Springer.
6. Nyberg, C. and Wallén, J. Improved linear distingusihers for snow 2.0. In *Fast Software Encryption 2006*, number 4047 in Lecture Notes in Computer Science, pages 336–350, Berlin, 2006. Springer.
7. Paul, S. and Preneel, B. Solving systems of differntial equations of addition. In *ACISP 2005*, number 3574 in Lecture Notes in Computer Science, pages 75–88, Berlin, 2006. Springer. Extended Version available as Technical Report 294/2004 at http://eprint.iacr.org/2004/294.
8. Sarkar,P. On approximating addition by exclusive or. Technical Report 047/2009, Cryptology ePrint Archive, 2009. Available at http://eprint.iacr.org/2009/047.
9. Staffelbach,0. and Meier, W. Cryptograpic significance of the carry for ciphers base on integer addition. In *Advances in Cryptology - CRYPT0 1990*, number 537 in Lecture Notes in Computer Science, pages 601–614, Berlin, 1990. Springer.
10. Wallén, J. Linear approximations of addition mod 2^n. In *Fast Software Encryption 2003*, number 2887 in Lecture Notes in Computer Science, pages 261–273, Berlin, 2003. Springer.

Note: due to space restrictions many details, proofs as well as the appendices had to be omitted from this extended abstract. These will appear in the full version of this paper.