SHIFT-INVARIANT FUNCTIONS AND ALMOST LIFTINGS

JAN KRISTIAN HAUGLAND AND TRON OMLAND

Abstract. We investigate shift-invariant vectorial Boolean functions on n bits that are lifted from Boolean functions on k bits, for $k \leq n$. We consider vectorial functions that are not necessarily permutations, but are, in some sense, almost bijective. In this context, we define an almost lifting as a Boolean function for which there is an upper bound on the number of collisions of its lifted functions that does not depend on n. We show that if a Boolean function with diameter k is an almost lifting, then the maximum number of collisions of its lifted functions is 2^{k-1} for any n.

Moreover, we search for functions in the class of almost liftings that have good cryptographic properties and for which the non-bijectivity does not cause major security weaknesses.

These functions generalize the well-known map χ used in the Keccak hash function.

Introduction

In symmetric cryptography, the ciphers often consist of linear and nonlinear operations in layers, where the nonlinear part is determined by a so-called S-box, short for "substitution box", which is a permutation on the set $\mathbb{F}_2^n$ of n-bit vectors. All the substitution-permutation networks are of this type, including the current block cipher standard, AES, and the S-boxes are fundamental in increasing confusion and diffusion to such ciphers. Moreover, lookup tables typically have large implementation costs, so good candidates for S-boxes are bijections with an easy description and good cryptographic properties. Shift-invariant bijections have shown to be useful in this context, e.g., in lightweight cryptography.

In this paper we relax the bijectivity condition on the nonlinear layer and are allowing some collisions. In particular, we look at "non-bijective S-boxes" that are "almost bijective" shift-invariant functions $\mathbb{F}_2^n \to \mathbb{F}_2^n$ induced from Boolean functions. To pursue this approach, we need to discuss what "almost bijective" should mean, e.g., one natural property to demand is that the ratio between the sizes of the image and codomain should be fairly high. Henceforth, we will use the term S-box also for functions $\mathbb{F}_2^n \to \mathbb{F}_2^n$ that are not necessarily bijective.

Let $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ be an S-box and s be the right shift, that is, $s(x_1, x_2, \ldots, x_n) = (x_n, x_1 \ldots, x_{n-1})$. Then F is shift-invariant (sometimes also called rotation-symmetric) if $F \circ s = s \circ F$, and F is then completely determined by a Boolean function $f\colon \mathbb{F}_2^n \to \mathbb{F}_2$. Therefore, shift-invariant S-boxes with sufficiently good cryptographic properties are candidates to be used as primitives in symmetric ciphers.

A Boolean function f on k bits determines a shift-invariant S-box F on n bits, for $n \geq k$, by

$$F(x_1, x_2, \ldots, x_n) = \big(f(x_1, x_2, \ldots, x_k), f(x_2, x_3, \ldots, x_{k+1}), \ldots, f(x_n, x_1, \ldots, x_{k-1})\big).$$

Date: July 16, 2024.

One motivating example is the function $\chi(x_1, x_2, x_3) = x_1 \oplus (1 \oplus x_2)x_3$, first studied in Daemen's thesis [4]. The function χ gives rise to bijections for all odd $n \geq 3$ with good cryptographic properties and is used in the hash function Keccak. It may also be interesting to look at the non-bijective case, for even n.

Examples of good cryptographic properties are: no differentials with high differential probability, no linear approximations with high linear potential. For implementation, we want low computational complexity and as much symmetry as we can get.

A low algebraic degree is good for protection against side-channel attacks by means of masking, while a high algebraic degree is good for protection against higher order differential attacks. A dense ANF protects better against integral attacks, but relatively sparse ANF can be compensated for by taking a linear layer with large diffusion. Moreover, some desirable properties for almost bijectivity could be:

(P1) (size of the image of F)/(size of the codomain of F) should be high,
(P2) the image $\mathrm{F}(\mathbb{F}_2^n)$ should be unstructured in $\mathbb{F}_2^n$,
(P3) $\max_y |F^{-1}(y)|$ should be low.

More concretely, we search for Boolean functions on up to five bits with simple descriptions that induce S-boxes with decent cryptographic properties. Our hope is that non-bijective shift-invariant S-boxes have useful applications, e.g., in modes of operation of a block cipher or vectorial function where we do not need the inverse (Grassi has discussed this over odd prime fields [5]), but then one needs to investigate whether collisions due to non-invertibility form a threat to security.

Shift-invariant S-boxes can also be viewed as cellular automata, which are certain dynamical systems on the space of infinite binary strings indexed by $\mathbb{Z}$, thought of as cells, where the the state of a cell at the next time step is determined by an update rule depending on a finite number of neighboring cells and uniformly applied to all cells at the same time, see e.g. [7, 8]. Cellular automata that are reversible correspond to bijective shift-invariant S-boxes, so what we consider in this paper correspond to "almost reversible" cellular automata. These are less studied, but still have applications in physics and biology, typically for simulation of microsystems that exhibit non-equilibrium behavior and history-dependent dynamics.

Even though shift-invariant S-boxes (or cellular automata) can be described by simple rules, finding the ones that are bijective is difficult, but previous works and computational data indicate that there are still a lot of examples (see e.g., [4, Appendix A] and [9]). In the almost bijective non-bijective case, it seems that not much is known.

In this paper we first consider what we call potential (k, n)-liftings in Section 1. The purpose of this is to reduce the search space, when looking for functions with desirable properties. We provide some tables in the appendix for the number of such functions, which is also helpful when trying to find (k, n)-liftings.

Further, in Section 2, we introduce almost liftings as Boolean functions for which there is an upper bound for the number of collisions of its lifted functions that does not depend on n. We then prove Theorem 2.6 stating that if a Boolean function with diameter k is an almost lifting, then the maximum number of collisions of its lifted functions is 2^{k-1} for any n. This means that all functions we consider will satisfy property (P3) in the above list, or at least that we have some control of the number of collisions.

Our Proposition 4.1 combined with computer experiments provide a conjecture for what the best possible values for (P1) are. The Boolean functions giving rise to these values will be called virtual liftings and we give a complete list of such functions for $k \leq 5$. Property (P2) may be hard to achieve, and in practice, it can be taken care of by carefully designing the linear layer.

In Section 6 we choose a selection of functions, that are potentially applicable in symmetric ciphers and compute various cryptographic properties for these functions. It is not clear that our selection is the best one, and there are probably other properties that come into play as well. In other words, there is more investigation left for future work.

1. Potential liftings

Let $f\colon \mathbb{F}_2^k \to \mathbb{F}_2$ be a Boolean function. The diameter of f is the length of the consecutive input sequence that the values of f depend on. If $1 \leq i \leq j \leq k$ are such that i and j is the smallest and largest number, respectively, such that f depends on x_i and x_j, then its diameter is $j - i + 1$. If f depends on both x_1 and x_k, then its diameter is k.

For every $n \geq k$ we say that f is a (k, n)-lifting if the diameter of f is k and $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ defined by

$$F(x_1, \dots, x_n) = \Big(f(x_1, x_2, \dots, x_k), f(x_2, x_3, \dots, x_{k+1}), \dots, f(x_n, x_1, \dots, x_{k-1})\Big)$$

is a bijection. Note the discrepancy between this definition and the one from [9], where it is not required that the diameter is equal to k. The reason for assuming full diameter is only a matter of presentation. All of the arguments hold also without this requirement.

For every $m \geq k$ define $F_{(m)}\colon \mathbb{F}_2^m \to \mathbb{F}_2^{m-k+1}$ by

$$F_{(m)}(x_1, \dots, x_m) = \Big(f(x_1, x_2, \dots, x_k), f(x_2, \dots, x_{k+1}), \dots, f(x_{m-k+1}, \dots, x_m)\Big).$$

We say that $F_{(m)}$ has uniform distribution if for all $y \in \mathbb{F}_2^{m-k+1}$

$$|F_{(m)}^{-1}(y)| = 2^{k-1}.$$

Lemma 1.1. *If f is a (k, n)-lifting then $F_{(m)}$ has uniform distribution whenever $k \leq m \leq n$.*

Proof. Let $m \geq k$, pick $y \in \mathbb{F}_2^{m-k+1}$, and set

$$Y = \{z \in \mathbb{F}_2^n : z = (y, y') \text{ for some } y' \in \mathbb{F}_2^{n-(m-k+1)}\}.$$

Then $F_{(m)}(x) = y$ if and only if $F(x, x') \in Y$ for every $x' \in \mathbb{F}_2^{n-m}$, so

$$|F_{(m)}^{-1}(y)| = \frac{|F^{-1}(Y)|}{2^{n-m}} = \frac{|Y|}{2^{n-m}} = \frac{2^{n-(m-k+1)}}{2^{n-m}} = 2^{k-1},$$

where the second equality follows by bijectivity of F. $\square$

Definition 1.2. A Boolean function $f\colon \mathbb{F}_2^k \to \mathbb{F}_2$ of diameter k is called a *potential (k, n)-lifting* if $F_{(m)}$ has uniform distribution for every m such that $k \leq m \leq n$.

Corollary 1.3. *If $k \leq n \leq n'$ and f is a potential (k, n')-lifting, then f is also a potential (k, n)-lifting.*

If $k \leq m \leq m'$ and $F_{(m')}$ has uniform distribution, then $F_{(m)}$ has uniform distribution.

Proof. The first statement follows directly from the definition. For the latter statement, let $k \leq m \leq m'$, pick $y \in \mathbb{F}_2^{m-k+1}$, and set

$$Y = \{z \in \mathbb{F}_2^{m'-k+1} : z = (y, y') \text{ for some } y' \in \mathbb{F}_2^{m'-m}\}.$$

Since $|F_{(m')}^{-1}(Y)| = 2^{m'-m}|F_{(m)}^{-1}(y)|$ and $F_{(m')}$ has uniform distribution, we get

$$|F_{(m)}^{-1}(y)| = \frac{|F_{(m')}^{-1}(Y)|}{2^{m'-m}} = \frac{2^{k-1}|Y|}{2^{m'-m}} = 2^{k-1}. \qquad \square$$

Remark 1.4. It is observed in [9] that f can only be a (k,n)-lifting if $f(0,0,\ldots,0) \neq f(1,1,\ldots,1)$, but this is not required for potential (k,n)-liftings. However, when searching for (k,n)-liftings, to reduce the space, it would still be natural to consider only the potential (k,n)-liftings satisfying $f(0,\ldots,0) = 0$ and $f(1,\ldots,1) = 1$.

Remark 1.5. It follows from the definition that all potential (k,n)-liftings must be balanced, and a balanced Boolean function in k variables cannot have algebraic degree k ([3], Theorem 2.5). Therefore, all potential (k,n)-liftings have degree at most $k-1$.

Let $S_{k,n}$ denote the set of all $f\colon \mathbb{F}_2^k \to \mathbb{F}_2$ such that f is a potential (k,n)-lifting and $f(0,0,\ldots,0) = 0$, and let $S_k = \{f\colon \mathbb{F}_2^k \to \mathbb{F}_2 \mid f \in S_{k,n} \text{ for all } n \geq k\}$. Data suggest that we have $|S_3| = 10$, $|S_4| = 264$, and $|S_5| = 70942$. Among these functions, 5, 132, and 35450, respectively, satisfy $f(1,\ldots,1) = 1$.

Lemma 1.6. *For any two Boolean functions $h, h' : \mathbb{F}_2^{k-1} \to \mathbb{F}_2$, where $h(x)$ depends on x_1 and $h'(x)$ depends on x_{k-1}, the functions $f, g\colon \mathbb{F}_2^k \to \mathbb{F}_2$ given by $f(x_1,\ldots,x_k) = h(x_1,\ldots,x_{k-1}) \oplus x_k$ and $g(x_1,\ldots,x_k) = x_1 \oplus h'(x_2,\ldots,x_k)$ are potential (k,n)-liftings for all $n \geq k$.*

Proof. Suppose f has this form, and take any $y \in \mathbb{F}_2^{m-k+1}$. The diameter of f is clearly k, and it suffices to prove that for any $z \in \mathbb{F}_2^{k-1}$, there is exactly one element of the form $x = (z,w) \in F_{(m)}^{-1}(y)$. Indeed, there are 2^{k-1} elements in $\mathbb{F}_2^{k-1}$, so this would give that $|F_{(m)}^{-1}(y)| = 2^{k-1}$. But given $x_1,\ldots,x_{k-1}$ for some element $x \in F_{(m)}^{-1}(y)$, and for $i = 0,1,\ldots,m-k$ in turn, we necessarily have $x_{k+i} = y_{i+1} \oplus h(x_{i+1},\ldots,x_{i+k-1})$. The corresponding argument for g is immediate by symmetry. $\square$

Corollary 1.7. $|S_k| \geq 2^{2^{k-1}} - 3 \cdot 2^{2^{k-2}-1}$.

Proof. The number of functions of the form $h(x_1,\ldots,x_{k-1}) \oplus x_k$ that depend on x_1 is $2^{2^{k-1}} - 2^{2^{k-2}}$, and similarly for functions of the form $x_1 \oplus h'(x_2,\ldots,x_k)$ that depend on x_k. There are $2^{2^{k-2}}$ functions in the intersection, i.e., of the form $x_1 \oplus h(x_2,\ldots,x_{k-1}) \oplus x_k$. This gives us $2 \cdot 2^{2^{k-1}} - 3 \cdot 2^{2^{k-2}}$ distinct functions, of which half satisfy $f(0,\ldots,0) = 0$. $\square$

The corollary gives us $|S_3| \geq 10$, $|S_4| \geq 232$ and $|S_5| \geq 65152$, which is not far from the actual values.

Tables for $k = 3,4,5$ (no constant term and $f(1,\ldots,1) = 1$) are given in Appendix C.

Question 1.8. Here we list some problems:

(i) Given k, how large is the set

$$\{f\colon \mathbb{F}_2^k \to \mathbb{F}_2 \mid f \text{ is a } (k,n)\text{-lifting for some } n \geq k\}?$$

Moreover, does there exist some $\tau(k)$, depending only on k, such that this set coincides with

$$\{f\colon \mathbb{F}_2^k \to \mathbb{F}_2 \mid f \text{ is a } (k,n)\text{-lifting for some } k \leq n \leq \tau(k)\}?$$

(ii) It seems like the number of (k,n)-liftings is only large for fairly small n. How large is the set

$$\{f\colon \mathbb{F}_2^k \to \mathbb{F}_2 \mid f \text{ is a } (k,n)\text{-lifting for infinitely many } n \geq k\}?$$

Moreover, does there exist some $\sigma(k)$, depending only on k, such that this set coincides with

$$\{f\colon \mathbb{F}_2^k \to \mathbb{F}_2 \mid f \text{ is a } (k,n)\text{-lifting for some } n \geq \sigma(k)\}?$$

2. Almost liftings

Let $f\colon \mathbb{F}_2^k \to \mathbb{F}_2$ be a Boolean function and for every $n \geq k$ we define $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ by

$$F(x_1,\ldots,x_n) = \Big(f(x_1,x_2,\ldots,x_k), f(x_2,x_3,\ldots,x_{k+1}),\ldots,f(x_{n-k+1},x_{n-k+2},\ldots,x_n)\Big),$$

and set

$$\ell_n(f) = \max_{y\in\mathbb{F}_2^n} |F^{-1}(y)|,$$
$$\ell(f) = \sup_{n\geq k} \ell_n(f).$$

Definition 2.1. Let $f\colon \mathbb{F}_2^k \to \mathbb{F}_2$ be a Boolean function of diameter k. If $\ell(f) < \infty$, we say that f is an *almost lifting.*

Moreover, let $l > 1$ and assume that the diameter of f is k. Then f is called a *potential l-almost (k,n)-lifting* if $|F_{(m)}^{-1}(y)| \leq l \cdot 2^{k-1}$ for any $y \in \mathbb{F}_2^{m-k+1}$ for every m such that $k \leq m \leq n$.

Lemma 2.2. *If f is an almost lifting, then f is a potential $\ell(f)$-almost (k,n)-lifting for all $n \geq k$.*

Proof. If $\ell(f) < \infty$, then $|f^{-1}(y)| \leq \ell(f)$ for all $y \in \mathbb{F}_2^n$, so $|f^{-1}(Y)| \leq \ell(f)|Y|$ for any $Y \subseteq \mathbb{F}_2^n$. Let $k \leq m \leq n$, pick $y \in \mathbb{F}_2^{m-k+1}$ and define Y as in the proof of Lemma 1.1, then

$$|F_{(m)}^{-1}(y)| = \frac{|F^{-1}(Y)|}{2^{n-m}} \leq \frac{\ell(f)|Y|}{2^{n-m}} = \frac{\ell(f)2^{n-(m-k+1)}}{2^{n-m}} = \ell(f)2^{k-1}.$$

□

Lemma 2.3. *Fix some $l > 1$ and let $m \geq k$. If $F_{(m)}$ does not have uniform distribution, then for any sufficiently large r, there exists $z \in \mathbb{F}_2^{rm-k+1}$ such that $|F_{(rm)}^{-1}(z)| > l \cdot 2^{k-1}$.*

Proof. If $F_{(m)}$ does not have uniform distribution, there exist $y \in \mathbb{F}_2^{m-k+1}$ and a rational number $c > 1$ such that $|F_{(m)}^{-1}(y)| = c \cdot 2^{k-1}$. Let $X = \{x \in \mathbb{F}_2^m \colon F_{(m)}(x) = y\}$ and choose a natural number r so such that $c^r > l$. Then $F_{(rm)}$ maps any element of the form $(x_1,\ldots,x_r)$ with $x_i \in X$ to an element of the form $(y, y_1, y, y_2, \ldots, y_{r-1}, y)$ with $y_i \in \mathbb{F}_2^{k-1}$ for $1 \leq i \leq r-1$. Let

$$X^r = \{(x_1,\ldots,x_r) \in \mathbb{F}_2^{rm} : x_i \in X\},$$
$$Z = \{(y, y_1, y, y_2, \ldots, y_{r-1}, y) \in \mathbb{F}_2^{rm-k+1} : y_i \in \mathbb{F}_2^{k-1}\}.$$

Then $F_{(rm)}$ maps X^r onto Z. We see that $|X^r| = c^r 2^{r(k-1)}$ and $|Z| = 2^{(r-1)(k-1)}$, and it follows that there exists one element $z \in Z$ such that the size of its inverse image is at least $c^r 2^{k-1}$. □

Corollary 2.4. *Let $l > 1$. Assume that f is a potential l-almost (k,n)-lifting for all $n \geq k$. Then f is a potential (k,n)-lifting for all $n \geq k$.*

Proof. Assume that there is some n such that f is not a potential (k,n)-lifting. Then there exists m with $k \leq m \leq n$ such that $F_{(m)}$ is not uniformly distributed, and by the above lemma, there exists m' and $z \in \mathbb{F}_2^{m'-k+1}$ such that $|F_{(m')}^{-1}(z)| > l \cdot 2^{k-1}$. For $n' \geq m'$, it follows that f is not a potential l-almost (k,n')-lifting. □

Remark 2.5. Pick some $l > 1$. Let $S_{k,n,l}$ denote the set of all Boolean $f\colon \mathbb{F}_2^k \to \mathbb{F}_2$ such that f is a potential l-almost (k,n)-lifting and $f(0,0,\ldots,0) = 0$, and let $S_{k,l} = \{f\colon \mathbb{F}_2^k \to \mathbb{F}_2 \mid f \in S_{k,n,l} \text{ for all } n \geq k\}$. Then, we have

$$|S_{k,l}| = \lim_{n\to\infty} |S_{k,n,l}| = \lim_{n\to\infty} |S_{k,n,1}| = |S_k|.$$

Note that the limits exists since the number of potential (k,n)-liftings is bounded from above by 2^{2^k} and decreases with growing n.

Theorem 2.6. *Let $f\colon \mathbb{F}_2^k \to \mathbb{F}_2$. Then f is a potential (k,n)-lifting for all $n \geq k$ if and only if f is an almost lifting.*

Moreover, if f is an almost lifting, then $\ell(f) \leq 2^{k-1}$.

Proof. First, suppose there is some $l > 1$ such that f is an l-almost potential (k,n)-lifting for all $n \geq k$. Pick any $n \geq k$ and consider the map

$$F_{(n+k-1)}\colon \mathbb{F}_2^{n+k-1} \to \mathbb{F}_2^n.$$

For every $y \in \mathbb{F}_2^n$, we then have that

$$|F^{-1}(y)| \leq |F_{(n+k-1)}^{-1}(y)| \leq l \cdot 2^{k-1}.$$

Thus, f is an almost lifting.

On the other hand, Lemma 2.2 in combination with Corollary 2.4 implies that an almost lifting is a potential (k,n)-lifting for all $n \geq k$.

For the second statement, we note that $S_k = S_{k,1}$, and if f is a potential (k,n)-lifting for all $n \geq k$, then $\ell(f) = 2^{k-1}$. □

3. Surjective cellular automata

Let P_n be the set of n-periodic doubly infinite (i.e., indexed by $\mathbb{Z}$) bit strings and let P be the set of all periodic doubly infinite bit strings, i.e., $P = \cup_{n\geq 1} P_n$.

A function $F\colon \mathbb{F}_2^{\mathbb{Z}} \to \mathbb{F}_2^{\mathbb{Z}}$ is called a cellular automaton if it is continuous and shift-invariant. Clearly, a cellular automaton F restricts to a shift-invariant map $P_n \to P_n$ for all $n \geq 1$, and to a shift-invariant continuous map $P \to P$. Moreover, F is called reversible if there exists a cellular automata G such that $FG = GF = I$. It is known that a cellular automaton is reversible if and only if it is bijective [6].

Let f be Boolean function of diameter k, $w \in \mathbb{Z}$, and let $F\colon \mathbb{F}_2^{\mathbb{Z}} \to \mathbb{F}_2^{\mathbb{Z}}$ be the map defined by

$$F(x)_{i+w} = f(x_i, x_{i+1}, \ldots, x_{i+k-1}),$$

that is, cell $i+w$ of the state after F is applied depends on the k-cells $i, i+1, \ldots, i+k-1$ of the previous state. Then F is a cellular automaton and every cellular automaton F is defined by such a local rule f. If w is nonzero, we can replace F by Fs^w, so it suffices to study the case $w = 0$.

Theorem 3.1. *Let $f\colon \mathbb{F}_2^k \to \mathbb{F}_2$ be a Boolean function of diameter k. Then the following are equivalent:*

(i) *$F\colon P \to P$ is surjective,*
(ii) *$F\colon \mathbb{F}_2^{\mathbb{Z}} \to \mathbb{F}_2^{\mathbb{Z}}$ is surjective,*
(iii) *$F_{(m)}\colon \mathbb{F}_2^m \to \mathbb{F}_2^{m-k+1}$ is surjective for all $m \geq k$,*
(iv) *f is an almost lifting.*

Proof. By Theorem 2.6, f is an almost lifting if and only if f is a potential (k,n)-lifting for any $n \geq k$, which is equivalent to $F_{(m)}$ having uniform distribution for any m, $m \geq k$.

(i) $\Longrightarrow$ (ii): Since $\mathbb{F}_2^{\mathbb{Z}}$ is compact and P is dense in $\mathbb{F}_2^{\mathbb{Z}}$, if $F(\mathbb{F}_2^{\mathbb{Z}})$ contains P it must contain all of $\mathbb{F}_2^{\mathbb{Z}}$ (this is also explained in [10, Theorem 5 and 6]).

(ii) $\Longrightarrow$ (iii): Pick $y \in \mathbb{F}_2^{m-k+1}$, and expand it to an element of $y' \in \mathbb{F}_2^{\mathbb{Z}}$ by setting $y'_i = y_j$ for $i \equiv j (\operatorname{mod} m-k+1)$. Find $x' \in \mathbb{F}_2^{\mathbb{Z}}$ such that $F(x') = y'$, and define $x \in \mathbb{F}_2^m$ by $x_i = x'_i$. Then $F_{(m)}(x) = y$.

(iii) $\Longrightarrow$ (iv): Suppose that f is not an almost lifting. Then there exists some m, $m \geq k$ such that $F_{(m)}$ does not have uniform distribution. It follows that there exists some bitstring y of length $m-k+1$ such that $|F_{(m)}^{-1}(y)| \leq 2^{k-1}-1$. For a positive integer r, let S_r denote the set of bitstrings y' of length $rm-k+1$ consisting of y, then any $k-1$ bits, then y, then any $k-1$ bits, and so on. There are $2^{(r-1)(k-1)}$ elements in S_r, but at most $\left(2^{k-1}-1\right)^r$ elements in $|F_{(rm)}^{-1}(S_r)|$. Thus, if r is large enough that $\left(1-\frac{1}{2^{k-1}}\right)^r < \frac{1}{2^{k-1}}$, then $F_{(rm)}$ is not surjective.

(iv) $\Longrightarrow$ (i): Suppose f is an almost lifting. Let y be any finite bitstring of some length $n \geq k$, and let $m = 2^k n + k - 1$. Since $F_{(m)}$ has uniform distribution, it is surjective, so there exists $x \in \mathbb{F}_2^m$ such that $F_{(m)}(x) = yy\ldots y$. Note that y is determined by a substring of x of length $n+k-1$. Because there are only 2^k distinct strings of length k, there must exist $i, j \in \{0, n, \ldots, 2^k n\}$ such that $i < j$ and $x_i = x_j, x_{i+1} = x_{j+1}, \ldots, x_{i+k-1} = x_{j+k-1}$. Let $x' \in P$ of period $j-i$ be given by $x'_l = x_l$ for $i \leq l \leq j-1$. Then we have $F(x') = \ldots yy\ldots$. Thus, $F: P \to P$ is surjective. $\square$

Remark that some of the above could also be deduced from [6, Section 5].

4. Desirable properties for almost bijectivity

We would like to find non-bijective shift-invariant function with preferably these properties for all n:

(P1) (size of the image of F)/(size of the codomain of F) should be high,
(P2) F($\mathbb{F}_2^n$) and its complement should be unstructured in $\mathbb{F}_2^n$
(P3) $\max_y |F^{-1}(y)|$ should be low

Moreover, to have applications in cryptography, almost bijective functions should otherwise have good properties when it comes to differential uniformity, nonlinearity, algebraic degree, etc., that will be discussed in the next section.

First, regarding (P3), we already know from the previous section that if f is an almost lifting, then $\ell_n(f) \leq 2^{k-1}$ for all $n \geq k$. Moreover, computer experiments suggest that the collision number pattern, that is, the sequences $\left(\ell_n(f)\right)_{n\geq k}$ are sometimes periodic and sometimes irregular, and often take values a bit lower than 2^{k-1}.

Now we consider (P1) and define the distribution of the sizes of preimages by letting $c_{j,n}$, for $j = 0, 1, 2, \dots$ and $n \geq k$, be given by

$$c_{j,n} = \Big| \{ y \in \mathbb{F}_2^n : |F^{-1}(y)| = j \} \Big|.$$

E.g., one would typically say the distribution is good if $c_{0,n}$ is small and $c_{1,n}$ is large, relative to 2^n, which again should mean that all $c_{j,n}$ for $j \geq 2$ are small.

Moreover, note that we have

$$\frac{2^n}{2^n - c_{0,n}} \leq \ell_n(f) \leq c_{0,n} + 1 \quad \text{ and } \quad \ell_n(f) - 1 \leq c_{0,n} \leq 2^n \left(1 - \frac{1}{\ell_n(f)} \right).$$

These are derived from considering the extreme cases with either only one instance or $2^n - c_{0,n}$ instances of $|F^{-1}(y)| = \ell_n(f)$, and $c_{0,n}$ instances of $|F^{-1}(y)| = 0$ and $|F^{-1}(y)| = 1$ otherwise.

Given f, let $\iota(n) = \Big| \{ y \in \mathbb{F}_2^n : |F^{-1}(y)| = 0 \} \Big| = c_{0,n}$. Clearly, if f is a (k, n)-lifting, then $\iota(n) = 0$. We are interested in functions f for which $\iota(n)$ is not identically 0, but is bounded by some slowly growing function.

Proposition 4.1. *Given a positive integer d, let $f \colon \mathbb{F}_2^{d+1} \to \mathbb{F}_2$ be the function of algebraic degree d, given by $f(x_1, \dots, x_{d+1}) = x_1 \oplus x_2 \cdots x_d(x_{d+1} \oplus 1)$. Then, for $n > d$,*

$$\iota(n) = \begin{cases} d \cdot 2^{\frac{n}{d} - 1} & \text{if } d | n, \\ 0 & \text{otherwise} \end{cases} \tag{1}$$

Proof. Take any $y \in \mathbb{F}_2^n$ and set $Y = \{ i : y_i = 0 \} = \{ \beta_1 < \beta_2 < \cdots < \beta_{|Y|} \}$. If $\beta_{i+1} - \beta_i \equiv 0 \bmod d$ for all $1 \leq i \leq |Y|$, where $\beta_{|Y|+1} := n + \beta_1$, then we say that y satisfies $(*)$. In particular, we note that if y satisfies $(*)$, then d must divide n.

Suppose $1 \leq \alpha_1 < \ldots < \alpha_j \leq n$ are integers such that conditions (i)-(iv) are satisfied. The indices are considered modulo j such that α_{j+1} is α_1, and the set $\{ \alpha_i + 1, \dots, \alpha_{i+1} - 1 \}$ for $i = j$ should be read as $\{ \alpha_j + 1, \dots, n \} \cup \{ 1, \dots, \alpha_1 - 1 \}$.

(i) $y_{\alpha_i} = 0$ for all i.
(ii) For each i, there is at most one element $l \in \{ \alpha_i + 1, \dots, \alpha_{i+1} - 1 \}$ such that $y_l = 0$.
(iii) If $\alpha_i \equiv \alpha_{i+1} \bmod d$, then it is required that such an element l exists.
(iv) If there is indeed such an element l, then it is required that $l \equiv \alpha_{i+1} \bmod d$.

Then there exists $x \in \mathbb{F}_2^n$ such that $F(x) = y$. Indeed, we can start with $x = y$ and make the following modifications for each $i \in \{ 1, \dots, j \}$. If there is no $l \in \{ \alpha_i + 1, \dots, \alpha_{i+1} - 1 \}$ such that $y_l = 0$, shift the values of $x_{\alpha_{i+1} - d}, x_{\alpha_{i+1} - 2d}, \dots$ until the end of the interval (α_i, α_{i+1}) is reached. If there is such an l, stop at that index. Note that $y_{\alpha_i} = f(x_{\alpha_i}, \dots, x_{\alpha_i + d}) = x_{\alpha_i} = 0$ for all i.

Suppose first that y does not satisfy $(*)$. If $m \geq 1$, there exists an i such that d does not divide $\beta_{i+1} - \beta_i$. We will let β_i be one of the α's. Now traverse the β's backwards (i.e., consider $\beta_{i-1}, \beta_{i-2}, \dots$ in turn) in search of new α's. Whenever the current β is not congruent to the last added α, add it. Otherwise, skip it and add the next β regardless. Because of the starting condition, there will not be a conflict when we come back to where we started. An example: $n = 10$, $d = 3$, $y = (0, 1, 1, 0, 1, 0, 0, 1, 0)$. We have $\{ \beta_i \} = \{ 1, 4, 6, 7, 9 \}$. Since 6 and 7 are not congruent mod 3, we can let 6 be an α. Going backwards, we add 4, since 4 and 6 are not congruent. Now we skip 1 because 1 and 4 are congruent modulo 3 and get 9, and then 7. So $\{\alpha_i\} = \{4, 6, 7, 9\}$.

Assume next that y satisfies $(*)$ and $|Y|$ is odd. Then $\beta_{i+1} - \beta_i \equiv 0 \bmod d$ for each i, so by condition (iii) it follows that every other β_i is an α_i, i.e., exactly half of the β_i's is an α_i, but this is not possible if $|Y|$ is odd. The number of such elements y is equal to d (the number of residue classes) times the number of subsets of $\{1, \ldots, \frac{n}{d}\}$ with an odd number of elements, which is $2^{\frac{n}{d}-1}$, and this is now an upper bound for $\iota(n)$ when $d|n$, while $\iota(n)$ must be 0 otherwise.

Finally, we suppose that y satisfies $(*)$ and $|Y|$ is even. The indices i such that $y_i = 0$ are congruent modulo d, and we usually get two distinct possibilities for x using the same method: If $y_i = 0$ for $i \in \{\beta_1, \ldots, \beta_{2j}\}$, then we can take either $\alpha_i = \beta_{2i-1}$ for all i or $\alpha_i = \beta_{2i}$ for all i. The exception is $y = (1, \ldots, 1)$, for which x can either be equal to y, or $x_i = 0$ for all i in any given residue class modulo d and $x_i = 1$ otherwise. Since every additional inverse in this case removes an inverse from the previous case, it follows that $\iota(n)$ is at least $d(2^{\frac{n}{d}-1} - 1) + d = d \cdot 2^{\frac{n}{d}-1}$. □

Definition 4.2. Consider the maps $c, r\colon \mathbb{F}_2^k \to \mathbb{F}_2^k$ given by complementing and reflecting, that commute, and are defined by

$$c(x_1, x_2, \ldots, x_k) = (\overline{x_1}, \overline{x_2}, \ldots, \overline{x_k}) \quad \text{and} \quad r(x_1, x_2, \ldots, x_k) = (x_k, \ldots, x_2, x_1).$$

We say that two Boolean functions $f, g\colon \mathbb{F}_2^k \to \mathbb{F}_2$ are equivalent if there are $i, j, \ell \in \{0, 1\}$ such that

$$g(x) \oplus \ell = f \circ r^i \circ c^j(x).$$

There are at most eight functions in such an equivalence class, and they have identical cryptographic properties.

The functions given in Proposition 4.1 generalize the χ function (up to equivalence). Computer experiments indicate that the values for $c_{0,n}$ given in (1) are lowest possible for almost liftings that do not lift to a bijection for all n. We have checked all functions up to $k = 5$ and also some classes for $k = 6$, for $n \leq 20$, and Proposition 4.1 shows that such functions exist for all these k's. We therefore conjecture that this bound is indeed optimal, and make the following definition.

Definition 4.3. A nonlinear function f of diameter k and $\deg(f) = d < k$ is called a *virtual lifting* if it satisfies condition (1) for all $n \geq k$.

A complete list of almost liftings for $k \leq 5$ satisfying (1) for all $n \leq 20$ is given in Appendix B. We believe they are all virtual liftings. Moreover, a complete list of Boolean functions for $k \leq 5$ that induce bijections for all n is given in Appendix C (the proof will be given in a forthcoming paper). We call such functions proper liftings.

Definition 4.4. Given any function $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^m$, one defines for $0 \neq v \in \mathbb{F}_2^m$ its component functions $f_v\colon \mathbb{F}_2^n \to \mathbb{F}_2$ by $f_v(x) = v \cdot F(x)$ (inner product). If $v = e_i$ these functions are called the coordinate functions of f and denoted f_i.

Furthermore, for (P2) and structuredness of the image, one can look at properties such as as balancedness and strict avalanche. Balancedness for a given n is defined by

$$\max_{v \neq 0} \Big| \sum_{x \in \mathbb{F}_2^n} (-1)^{v \cdot F(x)} \Big|,$$

and is 0 if F is bijective, and otherwise says something about how the outputs may accumulate around certain vectors. The strict avalanche criterion (the effect of changing one input; the best is if it flips half of the outputs) is given for each $v \neq 0$ and $1 \leq i \leq n$ by setting $(v \cdot F)_i(x) = (v \cdot F)(x) \oplus (v \cdot F)(x \oplus e_i)$ and then compute

$$\max_{1 \leq i \leq n,\, v \neq 0} \Big| \sum_{x \in \mathbb{F}_2^n} (-1)^{(v \cdot F)_i(x)} \Big|.$$

The strict avalanche criterion may also be defined for F (although we are not sure if we have seen this being considered elsewhere), that is, for $1 \leq n$, set $F_i(x) = F(x) \oplus F(x \oplus e_i)$

$$\max_{1 \leq i \leq n,\, y \in \mathbb{F}_2^n} |F_i^{-1}(y)|.$$

We think that balancedness and strict avalanche could play a role for non-bijective functions, since we would like unbalancedness to be "spread out" as most as possible.

5. Desirable cryptographic properties for non-bijections

Good cryptographic properties generally include aspects such as algebraic degree, nonlinearity, differential uniformity, and differential branch number. It is also desirable that the Boolean function has a fairly simple polynomial expression, to achieve low computational complexity.

Of course, it is not really a clear distinction between cryptographic properties and the properties for almost bijectivity discussed in the previous section.

First, the differential probability of F is defined for $a, b \in \mathbb{F}_2^n$ by

$$\mathrm{DP}(a, b) = \frac{1}{2^n} |\{x \in \mathbb{F}_2^n : F(x + a) + F(x) = b\}|.$$

The differential probability uniformity (DU) is then $\max\{\mathrm{DP}(a, b) : a, b \in \mathbb{F}_2^n,\, a \neq 0\}$ and we want this to be low.

Remark 5.1. We have verified with computer assistance that among the almost liftings of diameter $k = 3, 4, 5$, the best possible differential probability uniformity appears to be 2^{1-k} for all $n \geq k$. In general, if $F \colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ is a shift-invariant function defined by a Boolean function of diameter k, it is an open question whether the lowest possible differential uniformity for F is 2^{n-k+1}. Recall that a vectorial Boolean function $F \colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ is called almost perfect nonlinear (APN) if the differential uniformity of F is 2. In light of the above, we say that a Boolean function f is an *APN lifting* if for every $n \geq k$, the lifted version of f to $F \colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ has differential uniformity 2^{n-k+1} (in particular, F is an APN function for $n = k$). Our computer experiments show that for $k = 3, 4, 5$ there are 2, 8, and 64 equivalence classes, respectively, of almost liftings that are APN liftings. All of them are of algebraic degree 2 (for more on shift-invariant APN functions, see [2, Section 4.2]).

We have also searched through all almost liftings of degree 2 for $k = 6$, and in this case there are 32 equivalence classes. Among all the APN almost liftings that were found, none of them contain the term $x_1 x_k$ in the ANF. For $k = 6$, there are none that contain $x_1 x_{k-1}$ or $x_2 x_k$ either, whereas all of them contain $x_2 x_{k-1}$ and $x_3 x_{k-2}$.

The nonlinearity of a Boolean function f is the minimum Hamming distance between f and affine functions. We shall denote it by $\mathrm{nl}(f)$. To protect against certain linear attack, the nonlinearity of F is given by $\mathrm{NL}(F) = \min_{v\neq 0} \mathrm{nl}(v \cdot F)$, and we have (see [1, Definition 29])

$$2\,\mathrm{NL}(F) = 2^n - \max_{a,b,b\neq 0} \Big| \sum_{x\in\mathbb{F}_2^n} (-1)^{a\cdot x + b\cdot F(x)} \Big|.$$

Define the correlation for $a, b \in \mathbb{F}_2^n$ by

$$\mathrm{C}(a,b) = \frac{1}{2^n} \sum_{x\in\mathbb{F}_2^n} (-1)^{a\cdot x+b\cdot F(x)}$$

and the linear potential of a linear approximation (a, b) by $\mathrm{LP}(a, b) = \mathrm{C}(a, b)^2$. The relationship between correlation and nonlinearity is therefore

$$2\,\mathrm{NL}(F) + 2^n \max_{b\neq 0} \sqrt{\mathrm{LP}(a,b)} = 2^n.$$

The linear potential uniformity, or just linear uniformity (LU), is then

$$\max\{\mathrm{LP}(a,b) : a,b \in \mathbb{F}_2^n,\, b \neq 0\} = \left(1 - \frac{\mathrm{NL}(F)}{2^{n-1}}\right)^2.$$

Further, the algebraic degree of F is given by $\deg(F) = \max_{v\neq 0} \deg(v \cdot F)$. When F is shift-invariant, this is the same as the algebraic degree of f_1. Indeed, for all $1 \leq i \leq n$ we clearly have $\deg(f_1) = \deg(f_i)$ and $\deg(F) \geq \deg(f_1) = \deg(f_i)$. Moreover, since $v \cdot F$ are sums of the f_i's we must have $\deg(F) \leq \deg(f_i)$.

To protect against summing attacks, we first set

$$X_F = \{\varnothing \neq A \subseteq \mathbb{F}_2^n : \sum_{a\in A} F(a + x) = 0 \text{ for all } x \in \mathbb{F}_2^n\}$$

and then define

$$\sigma(F) = \min\{|A| : A \in X_F\}.$$

We have not yet computed this value for our functions, but that is a task for future work.

Finally, two other properties one may consider are boomerang uniformity and differential branch number. The latter is given by

$$\min_{x\neq y}\{\mathrm{wt}(x + y) + \mathrm{wt}(F(x) + F(y))\}$$

and we have computed this for some classes of functions.

6. Selected candidates

After some searching, we now consider a few candidates more closely:

(A1) $f(x) = x_1 \oplus x_2(x_3 \oplus 1)$
(A2) $f(x) = x_1 \oplus x_2x_3$
(B1) $f(x) = x_1 \oplus x_2(x_3 \oplus x_4)$
(B2) $f(x) = x_1 \oplus x_2(x_1 \oplus x_3 \oplus x_4)$
(B3) $f(x) = x_1 \oplus x_4(x_2 \oplus x_3 \oplus 1)$
(C1) $f(x) = x_2 \oplus x_3 \oplus x_4(x_1 \oplus x_2)(x_3 \oplus 1)$
(C2) $f(x) = x_1 \oplus x_4 \oplus x_3(x_2 \oplus x_4 \oplus x_2x_4)$
(D1) $f(x) = x_2 \oplus x_3((x_1 \oplus x_2)(x_4 \oplus 1) \oplus x_4x_5 \oplus 1)$
(D2) $f(x) = x_2 \oplus x_3(x_1 \oplus 1) \oplus x_4((x_2 \oplus 1)(x_5 \oplus 1) \oplus x_3(x_1 \oplus x_5))$
(D3) $f(x) = x_2 \oplus x_4(x_5 \oplus 1)(x_1 \oplus x_3)$

(E1) $f(x) = x_2 \oplus x_1(x_4(x_3 \oplus 1) \oplus (x_4 \oplus 1)x_5(x_2 \oplus x_3 \oplus 1))$

The functions (A1), (A2) have diameter $k = 3$ and $\deg = 2$; for (B1), (B2), and (B3) we have $k = 4$ and $\deg = 2$; for (C1), (C2) we have $k = 4$ and $\deg = 3$ functions; (D1), (D2), (D3) are virtual liftings with $k = 5$ and $\deg = 3$; finally, (E1) is a proper lifting, i.e., it lifts to a permutation for all n, with $k = 5$ and $\deg = 4$.

There are actually eight functions (up to equivalences) in the B class, six of them having irregular collision number pattern, and we have picked three functions in the B class, where (B2) and (B3) have an irregular pattern. The only other of the above functions with irregular collision number pattern is (C2).

For (A1) and (A2) the differential probability uniformity is $\frac{1}{4}$ for every n that we checked, while for (B1), (B2), and (B3), the differential probability uniformity is $\frac{1}{8}$ for every n that we checked.

For all the first five functions, $\mathrm{NL}(F) = 2^{n-2}$, so the linear potential uniformity of F is independent of n, and equal to

$$\left(1 - \frac{\mathrm{NL}(F)}{2^{n-1}}\right)^2 = \frac{1}{4}.$$

Here is a summary of our computations – be aware that our values for DU and LU are not completely exact and only checked for $n \leq 9$ or 10. For some functions the value is indeed constant for each $n \leq 9$, while for some other function, there are minor fluctuation around the values given in the table. It also looks like the (P1) values stabilize when n grows for the B and C functions. For the A, D, and E functions the values are sometimes (periodically) the ones given, and otherwise 1.

	k	deg	DU	LU	(P1) for $n = 10$
(A1)	3	2	1/4	1/4	.97
(A2)	3	2	1/4	1/4	
(B1)	4	2	1/8	1/4	.84
(B2)	4	2	1/8	1/4	.86
(B3)	4	2	1/8	1/4	.83
(C1)	4	3	5/16	9/16	.90
(C2)	4	3	5/16	9/16	.71
(D1)	5	3	7/32	1/4	.95
(D2)	5	3	7/32	1/4	.95
(D3)	5	3	9/32	9/16	.95
(E1)	5	4	1/4	25/64	1

Moreover, the values for balancedness and strong avalanche seem to be $2^{n/2+1}$ and 2^{n-3}, respectively, for both (A1) and the three B functions, when n grows and is even. All the above functions have differential branch number 2, except (C2), that has 3.

Moreover, the balancedness of (A1) is $2^{n/2+1}$ when n is even, and for (A2) and the three B functions it also seems to be approximately $2^{n/2+1}$ for all n. For the (D) functions we get $3 \cdot 2^{n/3}$ when n is a multiple of 3. Very rough estimates for (C1) and (C2) are $2^{0.8n}$ and $2^{0.6n}$, respectively.

One final property that we will consider is that $\max_{a \neq 0} \mathrm{DP}(a, 0)$ shall be small, so the probability of differentials that imply a collision is small. For (A1) this is $2^{-n/2}$ when n is even, and for (A2) and the three B functions it is approximately $2^{-2n/3}$ for all n.

Appendix A. Counting the number of liftings

Tables for $k = 3, 4, 5$ (no constant term and $f(1, \dots, 1) = 1$; note that there are no balanced Boolean functions in k variables of degree k when $k \geq 2$ and thus no liftings of degree k, cf. [9, Theorem 6.1]).

$k = 3$

n	# potential	# liftings	deg = 1	deg = 2
3	17	15	0	15
4	7	1	1	0
5	5	5	1	4
6	5	0	0	0
7	5	5	1	4
8	5	1	1	0
9	5	4	0	4
10	5	1	1	0
11	5	5	1	4
12	5	0	0	0
13	5	5	1	4
14	5	1	1	0
15	5	4	0	4
16	5	1	1	0
17	5	5	1	4
18	5	0	0	0
19	5	5	1	4

$k = 4$

n	# potential	# liftings	deg = 1	deg = 2	deg = 3
4	3394	762	2	24	736
5	1070	222	2	24	196
6	236	18	2	8	8
7	144	16	0	0	16
8	132	14	2	0	12
9	132	10	2	0	8
10	132	14	2	0	12
11	132	18	2	0	16
12	132	6	2	0	4
13	132	18	2	0	16
14	132	12	0	0	12
15	132	10	2	0	8
16	132	14	2	0	12
17	132	18	2	0	16
18	132	6	2	0	4
19	132	18	2	0	16
20	132	14	2	0	12
21	132	8	0	0	8
22	132	14	2	0	12
23	132	18	2	0	16

$k = 5$

n	# potential	# liftings	deg = 1	deg = 2	deg = 3	deg = 4
5	155110676	11249536	3	1815	354718	10893000
6		52487	3	308	2628	49548
7		1627	4	65	298	1260
8	71508	106	4	0	36	66
9	37114	192	3	9	66	114
10	35508	125	3	4	40	78
11	35460	298	4	12	108	174
12	35452	25	3	0	0	22
13	35450	298	4	12	104	178
14	35450	118	4	4	36	74
15	35450	168	0	4	62	102
16	35450	94	4	0	32	58
17	35450	286	4	12	100	170
18	35450	49	3	4	4	38
19		282	4	12	100	166
20		89	3	0	32	54

Appendix B. List of virtual liftings

In both tables the given differentials are 2^n DU for $n = k, k+1, \ldots, k+4$.

In the $\ell_n(f)$ column of the first table, a, b means that $\ell_n(f) = a$ if $n \in b\mathbb{Z}$ and is $\ell_n(f) = 1$ otherwise.

The twelve virtual liftings (up to equivalence) for $k \leq 5$:

k	Boolean function	$\ell_n(f)$	deg	LU	differentials
3	$x_1 \oplus x_2(x_3 \oplus 1)$	3, 2	2	1/4	$2, 4, 8, 16, 32$
4	$x_1 \oplus x_2x_3(x_4 \oplus 1)$	4, 3	3	9/16	$6, 14, 28, 56, 112$
4	$x_1 \oplus x_2(x_3 \oplus 1)(x_4 \oplus 1)$	2, 3	3	9/16	$6, 14, 28, 56, 112$
5	$x_2 \oplus x_1(x_3x_4 \oplus x_5(x_3 \oplus x_4 \oplus 1))$	4, 3	3	9/16	$10, 24, 42, 80, 162$
5	$x_2 \oplus x_3((x_1 \oplus x_2)(x_4 \oplus 1) \oplus x_4x_5 \oplus 1)$	4, 3	3	1/4	$8, 14, 28, 56, 112$
5	$x_2 \oplus x_3(x_1 \oplus 1) \oplus x_4((x_2 \oplus 1)(x_5 \oplus 1) \oplus x_3(x_1 \oplus x_5))$	4, 3	3	1/4	$8, 14, 28, 56, 112$
5	$x_3 \oplus x_4(x_5(x_2 \oplus x_3 \oplus 1) \oplus 1) \oplus (x_4 \oplus 1)(x_2 \oplus x_3(x_1 \oplus x_2))$	4, 3	3	1	$10, 18, 44, 84, 168$
5	$x_2 \oplus x_4(x_5 \oplus 1)(x_1 \oplus x_3)$	2, 3	3	9/16	$12, 24, 34, 72, 144$
5	$x_1 \oplus x_2x_3x_4(x_5 \oplus 1)$	5, 4	4	49/64	$18, 38, 78, 156, 312$
5	$x_1 \oplus x_2x_3(x_4 \oplus 1)(x_5 \oplus 1)$	2, 4	4	49/64	$22, 36, 74, 148, 296$
5	$x_1 \oplus x_2(x_3 \oplus 1)(x_4 \oplus 1)(x_5 \oplus 1)$	2, 4	4	49/64	$18, 38, 78, 156, 312$
5	$x_1 \oplus x_2(x_3 \oplus 1)(x_4(x_5 \oplus 1) \oplus 1)$	3, 4	4	25/64	$14, 24, 48, 96, 192$

Appendix C. List of proper liftings

The six nonlinear Boolean functions of degree ≥ 2 with $k \leq 5$ that are (k, n)-liftings for all $n \geq k$, up to equivalence (there are at least 120 equivalence classes for $k = 6$):

k	Boolean function	deg	LU	differentials
4	$x_2 \oplus x_1(x_3 \oplus 1)x_4$	3	9/16	$6, 14, 30, 54, 108$
5	$x_2 \oplus x_1x_3(x_4 \oplus 1)(x_5 \oplus 1)$	4	49/64	$16, 34, 72, 148, 304$
5	$x_2 \oplus x_1(x_3 \oplus 1)(x_4 \oplus 1)x_5$	4	49/64	$22, 34, 72, 146, 286$
5	$x_2 \oplus x_1(x_4(x_3 \oplus 1) \oplus (x_4 \oplus 1)x_5(x_2 \oplus x_3 \oplus 1))$	4	25/64	$8, 18, 36, 68, 132$
5	$x_3 \oplus x_1x_2(x_4 \oplus 1)x_5$	4	49/64	$18, 40, 78, 152, 300$
5	$x_3 \oplus x_1(x_2 \oplus 1)x_4(x_5 \oplus 1)$	4	49/64	$22, 50, 74, 148, 304$

References

[1] Claude Carlet. *Boolean functions for cryptography and coding theory.* Cambridge University Press, New York, 2020.

[2] Claude Carlet. On the APN-ness and differential uniformity of some classes of (n, n)-functions over $\mathbb{F}_2^n$. *Adv. Math. Commun.*, 18(2):283–303, 2023.

[3] Thomas W. Cusick and Younhwan Cheon . Counting balanced Boolean functions in n variables with bounded degree. *Experimental Math.*, 16(1):101–105, 2007.

[4] Joan Daemen. Cipher and hash function design strategies based on linear and differential cryptanalysis. PhD thesis, KU Leuven, 1995.

[5] Lorenzo Grassi. Bounded surjective quadratic functions over $\mathbb{F}_p^n$ for MPC-/ZK-/FHE-friendly symmetric primitives. *IACR Transactions on Symmetric Cryptology*, 2023(2):94–131, 2023.

[6] Gustav A. Hedlund. Endomorphisms and automorphisms of the shift dynamical system. *Math. Systems Theory*, 3:320–375, 1969.

[7] Luca Mariot, Stjepan Picek, Domagoj Jakobovic, and Alberto Leporati. Evolutionary algorithms for designing reversible cellular automata. *Genetic Programming and Evolvable Machines*, 22(4):429–461, 2021.

[8] Luca Mariot, Stjepan Picek, Alberto Leporati, and Domagoj Jakobovic. Cellular automata based S-boxes. *Cryptography and Communications*, 11(1):41–62, Jan 2019.

[9] Tron Omland and Pantelimon Stanica. Permutation rotation-symmetric s-boxes, liftings and affine equivalence. Cryptology ePrint Archive, `https://eprint.iacr.org/2022/279`.

[10] Jan Schoone and Joan Daemen. The state diagram of χ. *Des. Codes Cryptogr.* 92, 1393–1421, 2024.

Norwegian National Security Authority (NSM), Norway
Email address: `admin@neutreeko.net`

Norwegian National Security Authority (NSM) and Department of Mathematics, University of Oslo, Norway
Email address: `tron.omland@gmail.com`