Shift-invariant functions and almost liftings (joint with Jan Kristian Haugland)

Dubrovnik, Croatia, September 2024
Tron Omland
Norwegian National Security Authority (NSM) and University of Oslo

Shift-invariant vectorial Boolean function

Let $S\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ denote the right shift, i.e.,

$$S(x_1, x_2, \ldots, x_n) = (x_n, x_1, \ldots, x_{n-1}).$$

A function $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ is called shift-invariant (or rotation-symmetric) if

$$F \circ S = S \circ F.$$

Shift-invariant vectorial Boolean function

NSM

Let $S\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ denote the right shift, i.e.,

$$S(x_1, x_2, \ldots, x_n) = (x_n, x_1, \ldots, x_{n-1}).$$

A function $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ is called shift-invariant (or rotation-symmetric) if

$$F \circ S = S \circ F.$$

Every shift-invariant function F is determined by a Boolean function $f\colon \mathbb{F}_2^n \to \mathbb{F}_2$ by setting $f(x) = F(x)_1$, so that

$$F(x) = \left(f(x), f \circ S^{-1}(x), \ldots, f \circ S^{-(n-1)}(x)\right).$$

Shift-invariant vectorial Boolean function

NSM

Let $S\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ denote the right shift, i.e.,

$$S(x_1, x_2, \ldots, x_n) = (x_n, x_1, \ldots, x_{n-1}).$$

A function $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ is called shift-invariant (or rotation-symmetric) if

$$F \circ S = S \circ F.$$

Every shift-invariant function F is determined by a Boolean function $f\colon \mathbb{F}_2^n \to \mathbb{F}_2$ by setting $f(x) = F(x)_1$, so that

$$F(x) = \big(f(x), f \circ S^{-1}(x), \ldots, f \circ S^{-(n-1)}(x)\big).$$

Moreover, every Boolean function $f\colon \mathbb{F}_2^k \to \mathbb{F}_2$ induces shift-invariant functions $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ for all $n \geq k$ in this way. We often say that F is a lifting of f.

For example, if $k = 3$ and $n = 5$, then

$$F(x_1, x_2, x_3, x_4, x_5) = \big(f(x_1, x_2, x_3), f(x_2, x_3, x_4), f(x_3, x_4, x_5), f(x_4, x_5, x_1), f(x_5, x_1, x_2)\big).$$

Motivation and applications of non-bijections

From a mathematical point of view, there are many hard problems about when the induced F is a bijection (=permutation), but we will not focus on these:

(i) Given $f\colon \mathbb{F}_2^k \to \mathbb{F}_2$ find the set $\{n \geq k \mid F\colon \mathbb{F}_2^n \to \mathbb{F}_2^n \text{ is bijective}\}$

(ii) Given a pair (k, n), find all $f\colon \mathbb{F}_2^k \to \mathbb{F}_2$ that induce bijections $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$.

(iii) Find all functions $f\colon \mathbb{F}_2^k \to \mathbb{F}_2$ that induce bijections $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ for every $n \geq k$.

Motivation and applications of non-bijections

NSM

From a mathematical point of view, there are many hard problems about when the induced F is a bijection (=permutation), but we will not focus on these:

(i) Given $f\colon \mathbb{F}_2^k \to \mathbb{F}_2$ find the set $\{n \geq k \mid F\colon \mathbb{F}_2^n \to \mathbb{F}_2^n \text{ is bijective}\}$

(ii) Given a pair (k, n), find all $f\colon \mathbb{F}_2^k \to \mathbb{F}_2$ that induce bijections $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$.

(iii) Find all functions $f\colon \mathbb{F}_2^k \to \mathbb{F}_2$ that induce bijections $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ for every $n \geq k$.

Our motivation and goal

- Using shift-invariant functions as S-boxes can be useful due to symmetry properties, low complexity, flexibility and adaptability, e.g., in lightweight cryptography.

Motivation and applications of non-bijections

NSM

From a mathematical point of view, there are many hard problems about when the induced F is a bijection (=permutation), but we will not focus on these:

(i) Given $f\colon \mathbb{F}_2^k \to \mathbb{F}_2$ find the set $\{n \geq k \mid F\colon \mathbb{F}_2^n \to \mathbb{F}_2^n \text{ is bijective}\}$

(ii) Given a pair (k, n), find all $f\colon \mathbb{F}_2^k \to \mathbb{F}_2$ that induce bijections $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$.

(iii) Find all functions $f\colon \mathbb{F}_2^k \to \mathbb{F}_2$ that induce bijections $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ for every $n \geq k$.

Our motivation and goal

- Using shift-invariant functions as S-boxes can be useful due to symmetry properties, low complexity, flexibility and adaptability, e.g., in lightweight cryptography.
- We will consider non-bijective shift-invariant S-boxes that are “almost bijective”.

Motivation and applications of non-bijections

NSM

From a mathematical point of view, there are many hard problems about when the induced F is a bijection (=permutation), but we will not focus on these:

(i) Given $f\colon \mathbb{F}_2^k \to \mathbb{F}_2$ find the set $\{n \geq k \mid F\colon \mathbb{F}_2^n \to \mathbb{F}_2^n \text{ is bijective}\}$

(ii) Given a pair (k, n), find all $f\colon \mathbb{F}_2^k \to \mathbb{F}_2$ that induce bijections $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$.

(iii) Find all functions $f\colon \mathbb{F}_2^k \to \mathbb{F}_2$ that induce bijections $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ for every $n \geq k$.

Our motivation and goal

- Using shift-invariant functions as S-boxes can be useful due to symmetry properties, low complexity, flexibility and adaptability, e.g., in lightweight cryptography.
- We will consider non-bijective shift-invariant S-boxes that are “almost bijective”.
- The goal is to find Boolean functions $f\colon \mathbb{F}_2^k \to \mathbb{F}_2$ such that the induced functions $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ are “almost bijective” S-boxes with good cryptographic properties for all $n \geq k$, and find applications in cryptography.

Desired properties and strategy

NSM

Desired properties (for every n)

(1) $\max_y |F^{-1}(y)|$ should be low,

(2) (size of the image of F)/(size of the codomain of F) should be high,

(3) the image $\mathrm{F}(\mathbb{F}_2^n)$ and its complement should be unstructured in $\mathbb{F}_2^n$,

(4) $\{x \in \mathbb{F}_2^n : F(x \oplus u) = F(x)\}$ should be small for all $u \neq 0$.

Desired properties and strategy

NSM

Desired properties (for every n)

(1) $\max_y |F^{-1}(y)|$ should be low,

(2) (size of the image of F)/(size of the codomain of F) should be high,

(3) the image $\mathrm{F}(\mathbb{F}_2^n)$ and its complement should be unstructured in $\mathbb{F}_2^n$,

(4) $\{x \in \mathbb{F}_2^n : F(x \oplus u) = F(x)\}$ should be small for all $u \neq 0$.

Our strategy

- It turns out that there is a fairly concrete and well-defined class satisfying (1).
- The strategy is reducing the search space to this class and find candidates there with good properties with respect to (2)-(4), differential and linear cryptanalysis, etc.

Almost liftings

Given $f\colon \mathbb{F}_2^k \to \mathbb{F}_2$ and define for $n \geq k$ the maximal collision number of $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ by

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

Almost liftings

Given $f\colon \mathbb{F}_2^k \to \mathbb{F}_2$ and define for $n \geq k$ the maximal collision number of $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ by

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

Definition

- A functon $f\colon \mathbb{F}_2^k \to \mathbb{F}_2$ is called a *proper lifting* if $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ is bijective for all $n \geq k$.
- A functon $f\colon \mathbb{F}_2^k \to \mathbb{F}_2$ is called an *almost lifting* if $\sup_{n \geq k} \ell_n(f) < \infty$.

Examples

NSM

Example

Let $\chi(x) = x_1 \oplus (x_2 \oplus 1)x_3$ be the function used in e.g., Keccak. Then $\ell_n(\chi) = 1$ for n odd and 3 for n even. In particular, $\sup_{n \geq k} \ell_n(\chi) = 3$ so χ is an almost lifting.

Examples

NSM

Example

Let $\chi(x) = x_1 \oplus (x_2 \oplus 1)x_3$ be the function used in e.g., Keccak. Then $\ell_n(\chi) = 1$ for n odd and 3 for n even. In particular, $\sup_{n \geq k} \ell_n(\chi) = 3$ so χ is an almost lifting.

Example

Define the function $p(x) = x_2 \oplus x_1(x_3 \oplus 1)x_4$. This is, up to elementary equivalence, the only proper lifting for $k \leq 4$ (as observed by Patt), i.e., $\ell_n(p) = 1$ for all n.

Examples

NSM

Example

Let $\chi(x) = x_1 \oplus (x_2 \oplus 1)x_3$ be the function used in e.g., Keccak. Then $\ell_n(\chi) = 1$ for n odd and 3 for n even. In particular, $\sup_{n \geq k} \ell_n(\chi) = 3$ so χ is an almost lifting.

Example

Define the function $p(x) = x_2 \oplus x_1(x_3 \oplus 1)x_4$. This is, up to elementary equivalence, the only proper lifting for $k \leq 4$ (as observed by Patt), i.e., $\ell_n(p) = 1$ for all n.

Example

Define the function $f(x) = x_1 \oplus x_2(x_3 \oplus x_4 \oplus 1)$. Then $\ell_n(f)$ is an irregular sequence $4, 2, 4, 2, 4, 2, 3, 2, 4, 2, 3, 3, 4, 2, 4, 3, 4$ computed for $4 \leq n \leq 20$, and (it looks like) f is an almost lifting.

Elementary equivalence

NSM

Definition

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 *elementary 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.

Elementary equivalence

NSM

Definition

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 *elementary 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.

For every $n \geq k$, their induced versions then satisfy

$$G(x) \oplus (\ell, \ldots, \ell) = F(r^i \circ c^j(x))$$

and have identical cryptographic properties.

Bound for number of collisions

NSM

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

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

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

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

Bound for number of collisions

NSM

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

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

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

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

Theorem

The following are equivalent:

(i) $F_{(m)}$ *has uniform distribution for all* $m \geq k$

(ii) f *is an almost lifting (i.e.,* $\sup_{n \geq k} \ell_n(f) < \infty$*, where* $\ell_n(f) = \max_{y \in \mathbb{F}_2^n} |F^{-1}(y)|$*)*

(iii) $\ell_n(f) \leq 2^{k-1}$ *for every* $n \geq k$

Searching for almost liftings

NSM

Theorem

The following are equivalent:

(i) $F_{(m)}$ *has uniform distribution for all* $m \geq k$

(ii) f *is an almost lifting (i.e.,* $\sup_{n \geq k} \ell_n(f) < \infty$, *where* $\ell_n(f) = \max_{y \in \mathbb{F}_2^n} |F^{-1}(y)|$)

(iii) $\ell_n(f) \leq 2^{k-1}$ *for every* $n \geq k$

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

$$\{f \colon \mathbb{F}_2^k \to \mathbb{F}_2 : \ F_{(m')} \text{ has unif. dist.}\} \supseteq \{f \colon \mathbb{F}_2^k \to \mathbb{F}_2 : \ F_{(m)} \text{ has unif. dist.}\}$$

Searching for almost liftings

NSM

Theorem

The following are equivalent:

(i) $F_{(m)}$ *has uniform distribution for all* $m \geq k$

(ii) f *is an almost lifting (i.e.,* $\sup_{n \geq k} \ell_n(f) < \infty$*, where* $\ell_n(f) = \max_{y \in \mathbb{F}_2^n} |F^{-1}(y)|$*)*

(iii) $\ell_n(f) \leq 2^{k-1}$ *for every* $n \geq k$

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

$$\{f \colon \mathbb{F}_2^k \to \mathbb{F}_2 : \ F_{(m')} \text{ has unif. dist.}\} \supseteq \{f \colon \mathbb{F}_2^k \to \mathbb{F}_2 : \ F_{(m)} \text{ has unif. dist.}\}$$

and thus

$$\{f \colon \mathbb{F}_2^k \to \mathbb{F}_2 \text{ is an almost lifting}\} = \bigcap_m \{f \colon \mathbb{F}_2^k \to \mathbb{F}_2 : \ F_{(m)} \text{ has unif. dist.}\}$$

Elementary equivalence classes for $k = 5$

NSM

n	# unif.dist.	# unif.dist. with $f(0) \neq f(1)$	# bijections, i.e., $\ell_n(f) = 1$
5	75165111	38800984	2815556
6			13316
7			462
8	36080	18072	31
9	18808	9369	52
10	17921	8953	34
11	17885	8940	78
12	17882	8937	8
13	17881	8936	78
14	17881	8936	33
15	17881	8936	43
16	17881	8936	27
17	17881	8936	75
18	17881	8936	14
19	17881	8936	74
20	17881	8936	25

Permutive functions

A Boolean function $f\colon \mathbb{F}_2^k \to \mathbb{F}_2$ is called permutive if there exists $h\colon \mathbb{F}_2^{k-1} \to \mathbb{F}_2$ such that $f(x_1, \ldots, x_k) = x_1 \oplus h(x_2, \ldots, x_k)$ (up to elementary equivalence).

Proposition

Every permutive function is an almost lifting.

Permutive functions

NSM

A Boolean function $f\colon \mathbb{F}_2^k \to \mathbb{F}_2$ is called permutive if there exists $h\colon \mathbb{F}_2^{k-1} \to \mathbb{F}_2$ such that $f(x_1, \ldots, x_k) = x_1 \oplus h(x_2, \ldots, x_k)$ (up to elementary equivalence).

Proposition

Every permutive function is an almost lifting.

Comparison between number of elementary equivalence classes:

k	# almost liftings	# permutive
3	4	4
4	73	65
5	17881	16416

Cellular automata

NSM

Given a Boolean function $f\colon \mathbb{F}_2^k \to \mathbb{F}_2$, consider the induced function on the bi-infinite bit-strings, i.e.,

$$F\colon \mathbb{F}_2^{\mathbb{Z}} \to \mathbb{F}_2^{\mathbb{Z}}$$

given by

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

It is known that F is bijective if and only if f is a proper lifting.

Cellular automata

NSM

Given a Boolean function $f\colon \mathbb{F}_2^k \to \mathbb{F}_2$, consider the induced function on the bi-infinite bit-strings, i.e.,

$$F\colon \mathbb{F}_2^{\mathbb{Z}} \to \mathbb{F}_2^{\mathbb{Z}}$$

given by

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

It is known that F is bijective if and only if f is a proper lifting.

Theorem

The following are equivalent:

(i) *f is an almost lifting,(i.e., $\sup_{n\geq k} \ell_n(f) < \infty$, where $\ell_n(f) = \max_{y\in\mathbb{F}_2^n} |F^{-1}(y)|$)*

(ii) *$F\colon \mathbb{F}_2^{\mathbb{Z}} \to \mathbb{F}_2^{\mathbb{Z}}$ is surjective*

(iii) $\sup_{y\in\mathbb{F}_2^{\mathbb{Z}}} |F^{-1}(y)| \leq 2^{k-1}$

(iv) *$F^{-1}(y)$ is finite for all $y \in \mathbb{F}_2^{\mathbb{Z}}$*

Virtual liftings

NSM

For every k there are functions $f\colon \mathbb{F}_2^k \to \mathbb{F}_2$ with $\deg(f) = d < k$ such that for all $n \geq k$

$$\left|\{y \in \mathbb{F}_2^n : y \text{ is not in the image of } F\}\right| = \begin{cases} d \cdot 2^{\frac{n}{d}-1} & \text{if } d|n, \\ 0 & \text{otherwise.} \end{cases}$$

These are the non-bijections that have largest image, and are bijective except when $n = dm$. Note that χ is such a function.

Virtual liftings

NSM

For every k there are functions $f\colon \mathbb{F}_2^k \to \mathbb{F}_2$ with $\deg(f) = d < k$ such that for all $n \geq k$

$$\left|\{y \in \mathbb{F}_2^n : y \text{ is not in the image of } F\}\right| = \begin{cases} d \cdot 2^{\frac{n}{d}-1} & \text{if } d|n, \\ 0 & \text{otherwise.} \end{cases}$$

These are the non-bijections that have largest image, and are bijective except when $n = dm$. Note that χ is such a function.

Question

If f induces bijections for infinitely many n, does it do so in a periodic way?

Summary(?)

proper lifting $\iff$ cellular automata is bijective
virtual lifting $\iff$ CA surjective + induce bijections (periodically) for infintely many n
almost lifting $\iff$ CA surjective

Selected candidates of almost liftings

NSM

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

(A) $f(x) = x_1 \oplus x_2(x_3 \oplus 1)$

(B1) $f(x) = x_1 \oplus x_2(x_3 \oplus x_4)$

(B2) $f(x) = x_1 \oplus x_2(1 \oplus x_3 \oplus x_4)$

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

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

(F) $f(x) = x_5 \oplus x_1x_3 \oplus x_4(x_1 \oplus x_2 \oplus x_3)$

(G) $f(x)$ = long expression, degree 4

Differential and linear uniformity

The differential probability uniformity of F is defined by

$$\mathrm{DU}(F) = \frac{1}{2^n} \max_{a,b \in \mathbb{F}_2^n,\, a \neq 0} |\{x \in \mathbb{F}_2^n : F(x \oplus a) \oplus F(x) = b\}|.$$

Differential and linear uniformity

The differential probability uniformity of F is defined by

$$\mathrm{DU}(F) = \frac{1}{2^n} \max_{a,b \in \mathbb{F}_2^n,\, a \neq 0} |\{x \in \mathbb{F}_2^n : F(x \oplus a) \oplus F(x) = b\}|.$$

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

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

The linear potential uniformity

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

Differential and linear uniformity

The differential probability uniformity of F is defined by

$$\mathrm{DU}(F) = \frac{1}{2^n} \max_{a,b \in \mathbb{F}_2^n,\, a \neq 0} |\{x \in \mathbb{F}_2^n : F(x \oplus a) \oplus F(x) = b\}|.$$

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

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

The linear potential uniformity

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

We want both DU and LU to be small.

Properties

NSM

	k	deg	DU	LU	size of image $n = 10$	type
(A)	3	2	1/4 = 16/64	1/4 = 16/64	.97	χ, virtual
(B1)	4	2	1/8 = 8/64	1/4 = 16/64	.84	
(B2)	4	2	1/8 = 8/64	1/4 = 16/64	.86	
(B3)	4	2	1/8 = 8/64	1/4 = 16/64	.83	
(C1)	4	3	5/16 = 20/64	9/16 = 36/64	.90	
(C2)	4	3	5/16 = 20/64	9/16 = 36/64	.71	
(D1)	5	3	7/32 = 14/64	1/4 = 16/64	.95	virtual
(D2)	5	3	9/32 = 18/64	9/16 = 36/64	.95	virtual
(E)	5	4	1/4 = 16/64	25/64	1	pure
(F)	5	2	1/16 = 4/64	1/4 = 16/64	.76	
(G)	5	4	5/64	9/64	.90	

Collisions of differences: $\max_{u \neq 0}\{x \in \mathbb{F}_2^n : F(x \oplus u) = F(x)\}$ is $2^{-n/2}$ for A when n is even, and for the three B functions it is approximately $2^{-2n/3}$ for all n.

Sumary and further work

NSM

Summary: we have described a class of Boolean function called almost liftings.

Sumary and further work

NSM

Summary: we have described a class of Boolean function called almost liftings.

Further work

Do a more comprehensive search for almost liftings that induce non-bijective S-boxes with good cryptographic properties, and find applications in “almost-permutation-based cryptography”.

(it could also be interesting to get theoretical proofs of various desired properties for families of almost liftings)

Sumary and further work

NSM

Summary: we have described a class of Boolean function called almost liftings.

Further work

Do a more comprehensive search for almost liftings that induce non-bijective S-boxes with good cryptographic properties, and find applications in “almost-permutation-based cryptography”.

(it could also be interesting to get theoretical proofs of various desired properties for families of almost liftings)

Expand to nonbinary fields

The concept of almost liftings, and the equivalence with surjective CA, can be extended to $\mathbb{F}_p^k \to \mathbb{F}_p$ for all fields of characteristic $p > 2$, i.e., $\sup_n \ell_n(f) \leq p^{k-1}$ or infinite
(actually to all functions $\{0, 1, \ldots, p-1\}^k \to \{0, 1, \ldots, p-1\}$ for any integer $p > 2$)

Tron Omland

Tlf: 67 86 40 00
nsm.no