On the algebraic immunity of weightwise perfectly balanced functions

Agnese Gini, Pierrick Méaux

Luxembourg University, Luxembourg

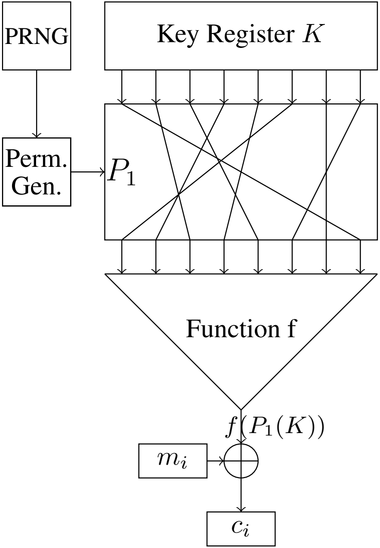
UNIVERSITÉ DU LUXEMBOURG

Quito — Ecuador
Thursday October 7^{th}

Summary

Filter Permutator and FLIP [MJSC16]

New stream cipher design adapted for homomorphic evaluation

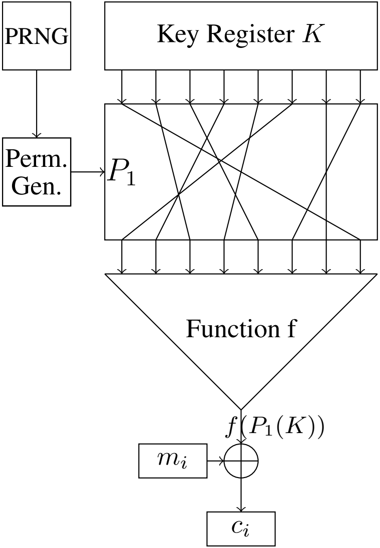


Components:

- Key register K,
- Public PRNG,
- Filtering function $f : \mathbb{F}_2^n \to \mathbb{F}_2$.

Filter Permutator and FLIP [MJSC16]

New stream cipher design adapted for homomorphic evaluation



Components:

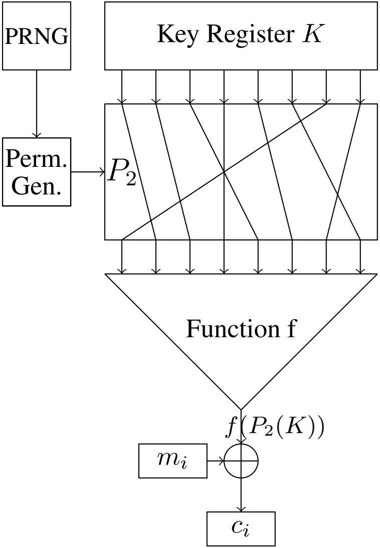
- Key register K,
- Public PRNG,
- Filtering function $f : \mathbb{F}_2^n \to \mathbb{F}_2$.

For each keystream bit:

- P_i is publicly derived,
- K is permuted,
- f is applied on $P_i(K)$,
- the result is XORed to m_i.

Filter Permutator and FLIP [MJSC16]

New stream cipher design adapted for homomorphic evaluation



Components:

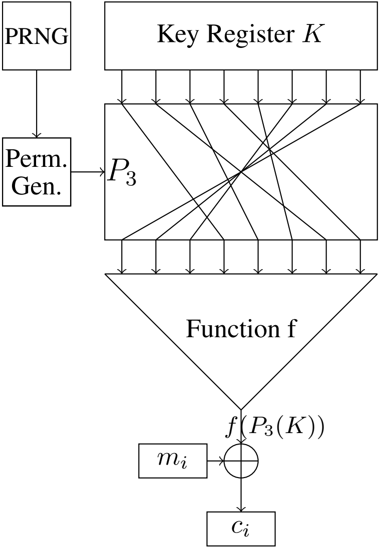
- Key register K,
- Public PRNG,
- Filtering function $f : \mathbb{F}_2^n \to \mathbb{F}_2$.

For each keystream bit:

- P_i is publicly derived,
- K is permuted,
- f is applied on $P_i(K)$,
- the result is XORed to m_i.

Filter Permutator and FLIP [MJSC16]

New stream cipher design adapted for homomorphic evaluation



Components:

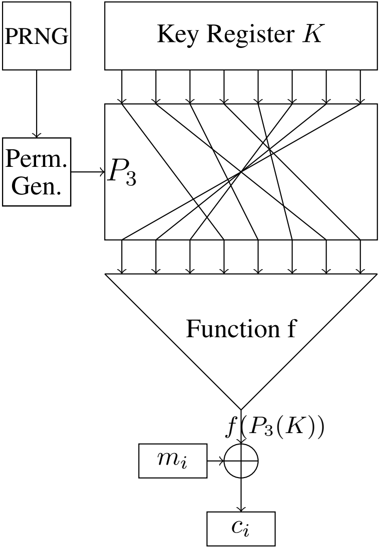
- Key register K,
- Public PRNG,
- Filtering function $f : \mathbb{F}_2^n \to \mathbb{F}_2$.

For each keystream bit:

- P_i is publicly derived,
- K is permuted,
- f is applied on $P_i(K)$,
- the result is XORed to m_i.

Filter Permutator and FLIP [MJSC16]

New stream cipher design adapted for homomorphic evaluation



Components:

- Key register K,
- Public PRNG,
- Filtering function $f : \mathbb{F}_2^n \to \mathbb{F}_2$.

For each keystream bit:

- P_i is publicly derived,
- K is permuted,
- f is applied on $P_i(K)$,
- the result is XORed to m_i.

Particularity:

$$\mathsf{w_H}(P_i(K)) = \mathsf{w_H}(P_j(K)).$$

invariant Hamming weight

Boolean functions on restricted inputs [CMR17]

Study the properties of Boolean functions applied only on a subset S of $\mathbb{F}_2^n$.

Global cryptographic criteria:

- balancedness,
- nonlinearity,
- degree,
- algebraic immunity (AI).

Restricted cryptographic criteria:

- restricted balancedness,
- restricted nonlinearity,
- restricted degree,
- restricted algebraic immunity.

Boolean functions on restricted inputs [CMR17]

Study the properties of Boolean functions applied only on a subset S of $\mathbb{F}_2^n$.

Global cryptographic criteria:

- balancedness,
- nonlinearity,
- degree,
- algebraic immunity (AI).

Restricted cryptographic criteria:

- restricted balancedness,
- restricted nonlinearity,
- restricted degree,
- restricted algebraic immunity.

For FLIP, properties on the slices: $\mathsf{E}_{k,n} = \{x \in \mathbb{F}_2^n \,|\, \mathsf{w_H}(x) = k\}$

Boolean functions on restricted inputs [CMR17]

Study the properties of Boolean functions applied only on a subset S of $\mathbb{F}_2^n$.

Global cryptographic criteria:

- balancedness,
- nonlinearity,
- degree,
- algebraic immunity (AI).

Restricted cryptographic criteria:

- restricted balancedness,
- restricted nonlinearity,
- restricted degree,
- restricted algebraic immunity.

For FLIP, properties on the slices: $\mathsf{E}_{k,n} = \{x \in \mathbb{F}_2^n \,|\, \mathsf{w_H}(x) = k\}$
Question: How to build Boolean functions with good properties on all slices?

Boolean functions on restricted inputs [CMR17]

Study the properties of Boolean functions applied only on a subset S of $\mathbb{F}_2^n$.

Global cryptographic criteria:

- balancedness,
- nonlinearity,
- degree,
- algebraic immunity (AI).

Restricted cryptographic criteria:

- restricted balancedness,
- restricted nonlinearity,
- restricted degree,
- restricted algebraic immunity.

For FLIP, properties on the slices: $\mathsf{E}_{k,n} = \{x \in \mathbb{F}_2^n \,|\, \mathsf{w_H}(x) = k\}$
Question: How to build Boolean functions with good properties on all slices?

Weightwise Perfectly Balanced function ($n = 2^m$)

For all $k \in [1, n-1]$:

$$|\mathsf{supp}_k(f)| = |\mathsf{E}_{k,n}|/2,$$

$f(0_n) = 0$ and $f(1_n) = 1$.
$\mathcal{WPB}_m$ denotes the set of 2^m-variable WPB functions.

WPB functions and cryptographic properties

Many constructions: CMR17, LM19, TL19, LS20, MS21, MSL21, ZS21, GM22a, GS22, MCL22, MPJDL22, ZS22, GM22b, MKL22, MSLZ22, GM23a, ZJZQ23, DM23, ...

Good parameters?

WPB functions and cryptographic properties

Many constructions: CMR17, LM19, TL19, LS20, MS21, MSL21, ZS21, GM22a, GS22, MCL22, MPJDL22, ZS22, GM22b, MKL22, MSLZ22, GM23a, ZJZQ23, DM23, ...

Good parameters?

Generic studies on: nonlinearity, weightwise nonlinearity, and degree.

WPB functions and cryptographic properties

Many constructions: CMR17, LM19, TL19, LS20, MS21, MSL21, ZS21, GM22a, GS22, MCL22, MPJDL22, ZS22, GM22b, MKL22, MSLZ22, GM23a, ZJZQ23, DM23, ...

Good parameters?

Generic studies on: nonlinearity, weightwise nonlinearity, and degree.

Algebraic Immunity

$$\mathsf{AI}(f) = \min_{g \neq 0}\{\mathsf{deg}(g) \mid f \cdot g = 0 \text{ or } (f+1) \cdot g = 0\}.$$

WPB functions and cryptographic properties

Many constructions: CMR17, LM19, TL19, LS20, MS21, MSL21, ZS21, GM22a, GS22, MCL22, MPJDL22, ZS22, GM22b, MKL22, MSLZ22, GM23a, ZJZQ23, DM23, ...

Good parameters?

Generic studies on: nonlinearity, weightwise nonlinearity, and degree.

Algebraic Immunity

$$\mathsf{AI}(f) = \min_{g \neq 0} \{\mathsf{deg}(g) \mid f \cdot g = 0 \text{ or } (f+1) \cdot g = 0\}.$$

Algebraic Attack, Courtois Meier 2003, adapted

- keystream bit $s_i = f(P_i(K))$,
- g such that $f \cdot g = 0$,
- $s_i = 1 \Rightarrow g(P_i(K)) = 0$, an equation of degree $\mathsf{deg}(g)$ in the key variables,
- solving an algebraic system of degree $\mathsf{AI}(f)$ gives the key.

Table of Contents

Summary

WPB functions and AI distribution

Former results:

- few examples in 4, 8 and 16 variables,
- constructions with optimal AI, Tang Liu 19, MSL21, MSLZ22.

WPB functions and AI distribution

Former results:

- few examples in 4, 8 and 16 variables,
- constructions with optimal AI, Tang Liu 19, MSL21, MSLZ22.

Distribution in 8 variables:

x	3	4
$\tilde{p}_{\mathsf{AI}}(x)\%$	0.004	99.996
$\#$	353	8427167

WPB functions and AI distribution

Former results:

- few examples in 4, 8 and 16 variables,
- constructions with optimal AI, Tang Liu 19, MSL21, MSLZ22.

Distribution in 8 variables:

x	3	4
$\tilde{p}_{\mathsf{AI}}(x)\%$	0.004	99.996
#	353	8427167

Bounds on a known construction (CMR17):

$$f(x_1, x_2, \ldots, x_{2^m}) = \sum_{a=1}^{m} \sum_{i=1}^{2^{m-a}} \prod_{j=0}^{2^{a-1}-1} x_{i+j2^{m-a+1}}.$$

Proposition

$$\mathsf{AI}(f_{2^m}) \geq m, \quad \text{and for } m > 3, \quad \mathsf{AI}(f_{2^m}) \leq 2^{m-2}.$$

WPB functions and AI distribution

Former results:

- few examples in 4, 8 and 16 variables,
- constructions with optimal AI, Tang Liu 19, MSL21, MSLZ22.

Distribution in 8 variables:

x	3	4
$\tilde{p}_{\mathsf{AI}}(x)\%$	0.004	99.996
#	353	8427167

Bounds on a known construction (CMR17):

$$f(x_1, x_2, \ldots, x_{2^m}) = \sum_{a=1}^{m} \sum_{i=1}^{2^{m-a}} \prod_{j=0}^{2^{a-1}-1} x_{i+j2^{m-a+1}}.$$

Proposition

$$\mathsf{AI}(f_{2^m}) \geq m, \quad \text{and for } m > 3, \quad \mathsf{AI}(f_{2^m}) \leq 2^{m-2}.$$

$\rightarrow$ AI always at least $\mathcal{O}(\log n)$?

WPB and minimum AI (1)

Minimum degree of annihilators of WPB functions

$$\mathsf{d}_m^{\varepsilon} = \min\{\mathsf{AN}(f + \varepsilon) \mid f \in \mathcal{WPB}_m\}.$$

WPB and minimum AI (1)

Minimum degree of annihilators of WPB functions

$$\mathsf{d}_m^\varepsilon = \min\{\mathsf{AN}(f+\varepsilon) \mid f \in \mathcal{WPB}_m\}.$$

Restricted Walsh transform

f a Boolean function, S a subset of $\mathbb{F}_2^n$, a an element of $\mathbb{F}_2^n$:

$$\mathcal{W}_{f,S}(a) := \sum_{x \in S} (-1)^{f(x)+ax}.$$

For $S = \mathsf{E}_{k,n}$ we denote $\mathcal{W}_{f,\mathsf{E}_{k,n}}(a)$ by $\mathcal{W}_{f,k}(a)$.

WPB and minimum AI (1)

Minimum degree of annihilators of WPB functions

$$\mathsf{d}_m^{\varepsilon} = \min\{\mathsf{AN}(f+\varepsilon) \mid f \in \mathcal{WPB}_m\}.$$

Restricted Walsh transform to the slices

$$\mathcal{W}_{f,k}(0) := \sum_{x \in \mathsf{E}_{k,n}} (-1)^{f(x)}.$$

Lemma: $g \in \mathcal{B}_n^*$ with positive $\mathcal{W}_{g,k}(0)$ on all* slices
$\implies \exists f \in \mathcal{WPB}_m$ such that $f \cdot g = 0$ or $(f+1) \cdot g = 0$.

WPB and minimum AI (1)

Minimum degree of annihilators of WPB functions

$$\mathsf{d}_m^\varepsilon = \min\{\mathsf{AN}(f+\varepsilon) \mid f \in \mathcal{WPB}_m\}.$$

Restricted Walsh transform to the slices

$$\mathcal{W}_{f,k}(0) := \sum_{x \in \mathsf{E}_{k,n}} (-1)^{f(x)}.$$

Lemma: $g \in \mathcal{B}_n^*$ with positive $\mathcal{W}_{g,k}(0)$ on all* slices
$\implies \exists f \in \mathcal{WPB}_m$ such that $f \cdot g = 0$ or $(f+1) \cdot g = 0$.

Proposition: Equivalent characterization of d_m^ε

$$\mathsf{d}_m^\varepsilon = \min\{\mathsf{deg}(g), g \in \mathcal{B}_n^* \mid \forall k \in [1-\varepsilon, 2^m-\varepsilon], \mathcal{W}_{g,k}(0) \geq 0\}.$$

WPB and minimum AI (2)

First result:

$$\mathsf{d}_1^{\varepsilon} = 1 \quad \text{and} \quad \text{for } m > 1,\ \mathsf{d}_m^{\varepsilon} > 1.$$

WPB and minimum AI (2)

First result:

$$\mathsf{d}_1^{\varepsilon} = 1 \quad \text{and} \quad \text{for } m > 1,\, \mathsf{d}_m^{\varepsilon} > 1.$$

Theorem

$$\min\left\{\mathsf{AI}(f) \colon f \in \mathcal{WPB}_m\right\} = 2, \text{ for } m \geq 2$$

WPB and minimum AI (2)

First result:

$$\mathsf{d}_1^{\varepsilon} = 1 \quad \text{and} \quad \text{for } m > 1,\, \mathsf{d}_m^{\varepsilon} > 1.$$

Theorem

$$\min\left\{\mathsf{AI}(f) \colon f \in \mathcal{WPB}_m\right\} = 2, \text{ for } m \geq 2$$

Constructive proof, with an explicit function: $x_i \cdot (x_j + x_k)$

WPB and minimum AI (2)

First result:

$$\mathsf{d}_1^{\varepsilon} = 1 \quad \text{and} \quad \text{for } m > 1,\, \mathsf{d}_m^{\varepsilon} > 1.$$

Theorem

$$\min\left\{\mathsf{AI}(f) \colon f \in \mathcal{WPB}_m\right\} = 2, \ \text{for } m \geq 2$$

Constructive proof, with an explicit function: $x_i \cdot (x_j + x_k)$

Corollary:

$$f \in \mathcal{WPB}_2 \Rightarrow \mathsf{AI}(f) = 2.$$

Summary

Construction from GM23a

Input: $g \in \mathcal{B}_{2^m}$.
Output: $h \in \mathcal{WPB}_m$.

Initiate the support of h to $\mathsf{supp}(g)$.
If $0_n \in \mathsf{supp}(g)$ remove 0_n from $\mathsf{supp}(h)$.
If $1_n \notin \mathsf{supp}(g)$ add 1_n to $\mathsf{supp}(h)$.
for $k \leftarrow 1$ to $n-1$ **do**
    Compute $C_{k,n} = \mathcal{W}_{g,k}(0)/2$,
    if $C_{k,n} < 0$ **then**
        remove $|C_{k,n}|$ elements from $\mathsf{supp}_k(h)$,
    else
        if $C_{k,n} > 0$ **then**
            add $C_{k,n}$ new elements to $\mathsf{supp}_k(h)$,
        end if
    end if
end for
return h

Construction from GM23a

Input: $g \in \mathcal{B}_{2^m}$.
Output: $h \in \mathcal{WPB}_m$.

Initiate the support of h to $\mathsf{supp}(g)$.
If $0_n \in \mathsf{supp}(g)$ remove 0_n from $\mathsf{supp}(h)$.
If $1_n \notin \mathsf{supp}(g)$ add 1_n to $\mathsf{supp}(h)$.
for $k \leftarrow 1$ to $n-1$ **do**
    Compute $C_{k,n} = \mathcal{W}_{g,k}(0)/2$,
    if $C_{k,n} < 0$ **then**
        remove $|C_{k,n}|$ elements from $\mathsf{supp}_k(h)$,
    else
        if $C_{k,n} > 0$ **then**
            add $C_{k,n}$ new elements to $\mathsf{supp}_k(h)$,
        end if
    end if
end for
return h

Non Perfect Balancedness (NPB)

$$\mathsf{NPB}(f) = \min_{g \in \mathcal{WPB}_m} \mathsf{d_H}(f, g).$$

Construction from GM23a

Input: $g \in \mathcal{B}_{2^m}$.
Output: $h \in \mathcal{WPB}_m$.

Initiate the support of h to $\mathsf{supp}(g)$.
If $0_n \in \mathsf{supp}(g)$ remove 0_n from $\mathsf{supp}(h)$.
If $1_n \notin \mathsf{supp}(g)$ add 1_n to $\mathsf{supp}(h)$.
for $k \leftarrow 1$ to $n-1$ **do**
  Compute $C_{k,n} = \mathcal{W}_{g,k}(0)/2$,
  if $C_{k,n} < 0$ **then**
    remove $|C_{k,n}|$ elements from $\mathsf{supp}_k(h)$,
  else
    if $C_{k,n} > 0$ **then**
      add $C_{k,n}$ new elements to $\mathsf{supp}_k(h)$,
    end if
  end if
end for
return h

Non Perfect Balancedness (NPB)

$$\mathsf{NPB}(f) = \min_{g \in \mathcal{WPB}_m} \mathsf{d_H}(f, g).$$

g — small NPB, high NL $\xrightarrow{\text{Construction 1}}$ h — WPB, high NL

WPB constructions with upper bounded AI

Proposition (GM23a): h is WPB and $\mathsf{NL}(h) \geq \mathsf{NL}(g) - \mathsf{NPB}(g)$.

WPB constructions with upper bounded AI

Proposition (GM23a): h is WPB and $\mathsf{NL}(h) \geq \mathsf{NL}(g) - \mathsf{NPB}(g)$.

Theorem

$1+g$	Construction 1 $\longrightarrow$	h
$\mathcal{W}_{g,k} \geq 0$ for $k \in [1, n]$		$\mathsf{AI}(h) \leq \mathsf{deg}(g)$

Proof intuition:

- $\mathsf{supp}(h) \subseteq \mathsf{supp}(1+g)$,
- $1+g$ annihilates g so $h \cdot g = 0$,
- g is non null.

WPB constructions with upper bounded AI

Proposition (GM23a): h is WPB and $\mathsf{NL}(h) \geq \mathsf{NL}(g) - \mathsf{NPB}(g)$.

Theorem

g		h
$\mathcal{W}_{g,k} \geq 0$ for $k \in [0, n-1]$	$\xrightarrow{\text{Construction 1}}$	$\mathsf{AI}(h) \leq \mathsf{deg}(g)$

Proof intuition:

- $\mathsf{supp}(1+h) \subseteq \mathsf{supp}(1+g)$,
- g annihilates $1+g$ so $(1+h) \cdot g = 0$,
- g is non null.

WPB constructions with upper bounded AI

Proposition (GM23a): h is WPB and $\mathsf{NL}(h) \geq \mathsf{NL}(g) - \mathsf{NPB}(g)$.

Theorem

g — $\mathcal{W}_{g,k} \geq 0$ for $k \in [0, n-1]$ $\xrightarrow{\text{Construction 1}}$ h — $\mathsf{AI}(h) \leq \mathsf{deg}(g)$

Examples:

◇ Porcelain functions

$\kappa_n = x_i \cdot (x_j + x_k)$

$\mathsf{NPB} = \mathsf{NL} = 2^{n-2}$ $\xrightarrow{\text{Construction 1}}$ h — $\mathsf{AI} = 2$

Cardinal (in the article): $\mathfrak{F}_8(\kappa_8) > 2^{152}$ and $\mathfrak{F}_{16}(\kappa_{16}) > 2^{44521}$.

WPB constructions with upper bounded AI

Proposition (GM23a): h is WPB and $\mathsf{NL}(h) \geq \mathsf{NL}(g) - \mathsf{NPB}(g)$.

Theorem

g		h
$\mathcal{W}_{g,k} \geq 0$ for $k \in [0, n-1]$	$\xrightarrow{\text{Construction 1}}$	$\mathsf{AI}(h) \leq \mathsf{deg}(g)$

Examples:

◇ Porcelain functions

$\kappa_n = x_i \cdot (x_j + x_k)$	$\xrightarrow{\text{Construction 1}}$	h
$\mathsf{NPB} = \mathsf{NL} = 2^{n-2}$		$\mathsf{AI} = 2$

◇ Functions from GM23a

$\sigma_{2,n} + x_1 + \cdots + x_{n/2}$	$\xrightarrow{\text{Construction 1}}$	h
bent		$\mathsf{NL} \geq 2^{n-1} - 2^{n/2-2}$, $\mathsf{AI} = 2$

WPB constructions with lower bounded AI

Mesnager Tang 21: small support modification $\Rightarrow$ small AI modification

WPB constructions with lower bounded AI

Mesnager Tang 21: small support modification $\Rightarrow$ small AI modification

Theorem

$$\begin{array}{c} g \\ \mathsf{NPB}(g) < 2^{n/2} \end{array} \xrightarrow{\text{Cons. } 1} \begin{array}{c} h \\ \mathsf{AI}(h) \geq \mathsf{AI}(g) - \lfloor \log(\mathsf{NPB}(g) + 1) \rfloor \end{array}$$

WPB constructions with lower bounded AI

Theorem

$$\begin{array}{ccc} g & & h \\ \mathsf{NPB}(g) < 2^{n/2} & \xrightarrow{\text{Cons. 1}} & \mathsf{AI}(h) \geq \mathsf{AI}(g) - \lfloor \log(\mathsf{NPB}(g)+1) \rfloor \end{array}$$

Proposition:

$$\begin{array}{ccc} g + \sigma_{n/2,n} & & h \\ \mathsf{NPB}(g) < 2^{n/2}, \mathsf{deg}(g) < \frac{n}{2} & \xrightarrow{\text{Cons. 1}} & \mathsf{AI} \geq \frac{n}{2} - \mathsf{deg}(g) - \lfloor \log(\mathsf{NPB}(g)+1) \rfloor \end{array}$$

WPB constructions with lower bounded AI

Theorem

$$g \qquad \xrightarrow{\text{Cons. 1}} \qquad h$$

$$\mathsf{NPB}(g) < 2^{n/2} \qquad \longrightarrow \qquad \mathsf{AI}(h) \geq \mathsf{AI}(g) - \lfloor \log(\mathsf{NPB}(g)+1) \rfloor$$

Proposition:

$$g + \sigma_{n/2,n} \qquad \xrightarrow{\text{Cons. 1}} \qquad h$$

$$\mathsf{NPB}(g) < 2^{n/2}, \mathsf{deg}(g) < \frac{n}{2} \qquad \longrightarrow \qquad \mathsf{AI} \geq \frac{n}{2} - \mathsf{deg}(g) - \lfloor \log(\mathsf{NPB}(g)+1) \rfloor$$

Truncated CMR: $$f_{d,m}(x_1, x_2, \ldots, x_{2^m}) = \sum_{a=1}^{d} \sum_{i=1}^{2^{m-a}} \prod_{j=0}^{2^{a-1}-1} x_{i+j2^{m-a+1}}.$$

$$f_{d,m} + \sigma_{n/2,n} \qquad \xrightarrow{\text{Cons. 1}} \qquad h$$

$$\mathsf{AI} \geq \frac{n}{2} - 2^{d-1} - m + d + 1$$

WPB constructions with lower bounded AI

Theorem

$$\begin{array}{ccc} g & & h \\ \mathsf{NPB}(g) < 2^{n/2} & \xrightarrow{\text{Cons. 1}} & \mathsf{AI}(h) \geq \mathsf{AI}(g) - \lfloor \log(\mathsf{NPB}(g)+1) \rfloor \end{array}$$

Proposition:

$$\begin{array}{ccc} g + \sigma_{n/2,n} & & h \\ \mathsf{NPB}(g) < 2^{n/2}, \deg(g) < \frac{n}{2} & \xrightarrow{\text{Cons. 1}} & \mathsf{AI} \geq \frac{n}{2} - \deg(g) - \lfloor \log(\mathsf{NPB}(g)+1) \rfloor \end{array}$$

Truncated CMR: $$f_{d,m}(x_1, x_2, \ldots, x_{2^m}) = \sum_{a=1}^{d} \sum_{i=1}^{2^{m-a}} \prod_{j=0}^{2^{a-1}-1} x_{i+j2^{m-a+1}}.$$

$$\begin{array}{ccc} f_{d,m} + \sigma_{n/2,n} & & h \\ & \xrightarrow{\text{Cons. 1}} & \mathsf{AI} \geq \frac{n}{2} - 2^{d-1} - m + d + 1 \end{array}$$

Example: $d = 1 \Rightarrow \mathsf{AI}(h) \geq 2^{m-1} - m + 1$.

Summary

Conclusion and open questions

First study of the AI of WPB functions:

◇ Extreme values and distribution:

- Estimated distribution in 4, 8 and 16 variables.
- Bound on secondary constructions.
- Characterization minimum AI for all m.

◇ Constructions with bounded AI:

- bounds on GM23a's Construction.
- Upper bounded AI, many functions of AI exactly 2.
- Lower bounded AI, a family with AI at least $n/2 - \log(n) + 1$.

Conclusion and open questions

First study of the AI of WPB functions:

◇ Extreme values and distribution:
- Estimated distribution in 4, 8 and 16 variables.
- Bound on secondary constructions.
- Characterization minimum AI for all m.

◇ Constructions with bounded AI:
- bounds on GM23a's Construction.
- Upper bounded AI, many functions of AI exactly 2.
- Lower bounded AI, a family with AI at least $n/2 - \log(n) + 1$.

Open questions:

◇ Functions with high NL and AI from GM23a's construction?

◇ Impact of adding symmetric functions to the different cryptographic parameters?
$\rightarrow$ First study in ePrint 2023/1101.

◇ Distribution of the algebraic immunity restricted to the slices?

Conclusion and open questions

First study of the AI of WPB functions:

◇ Extreme values and distribution:
- Estimated distribution in 4, 8 and 16 variables.
- Bound on secondary constructions.
- Characterization minimum AI for all m.

◇ Constructions with bounded AI:
- bounds on GM23a's Construction.
- Upper bounded AI, many functions of AI exactly 2.
- Lower bounded AI, a family with AI at least $n/2 - \log(n) + 1$.

Open questions:

◇ Functions with high NL and AI from GM23a's construction?

◇ Impact of adding symmetric functions to the different cryptographic parameters?
$\rightarrow$ First study in ePrint 2023/1101.

◇ Distribution of the algebraic immunity restricted to the slices?

Thank you!