On existence of a system of blocks for the translation group of a vector space V_m, which mapped by permutation with a non-trivial automorphism group to a system of blocks

Burov Dmitry, Karabeynikov Igor

Requirements for nonlinear cryptographic functions

1. low differential δ-uniformity $\delta(f)$,
2. high nonlinearity,
3. low differentially-linear characteristic,
4. low boomerang uniformity,
5. high algebraic degree,
6. high graph algebraic immunity,
7. non-existance of linear structures in linear combinations of coordinate functions, etc.

Question

What are the relationships between these characteristics?

Definition

A mapping $f: \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ is called differentially δ-uniform if the equation

$$f(x+a)+f(x)=b$$

has at most δ solutions for every $a \in \mathbb{F}_{2^m}^*$, $b \in \mathbb{F}_{2^m}$. Minimal δ with this property is called the differential uniformity of f and denoted by $\delta(f)$.

Definition

A nonlinearity of a mapping $f: \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ is called a value

$$nl(f) = 2^{m-1} - \frac{1}{2} \max_{u \in \mathbb{F}_{2^m}, v \in \mathbb{F}_{2^m}^*} |W_f(u,v)|,$$

where $W_f(u,v) = \sum_{x \in \mathbb{F}_{2^m}} (-1)^{tr_m(f(x)v+xu)}$.

Some well-known relations between characteristics

1. If f is an AB function, then f is an APN function.
2. If f is an APN function, then $nl(f) > 0$.
3. If f is a differentially δ-uniform power permutation, then $nl(f) > 2^{n-1} - 2^{\frac{3n-4}{4}} \sqrt[4]{\delta}$.
4. Low differential δ-uniformity and high nonlinearity don't provide a low differential-linear characteristic. For example, $x \mapsto x^3$ is AB function, but the differentially-linear characteristic is 1.
5. Low differential δ-uniformity and high nonlinearity don't provide a high algebraic degree. For example, $x \mapsto x^3$.
6. Low differential δ-uniformity and high nonlinearity don't provide high graph algebraic immunity. For example, $x \mapsto x^{-1}$.

Definition of block

Definition

Let G be a group acting on a set Ω. A nonempty subset Δ of Ω is called a block for G if for each $g \in G$ either $g(\Delta) = \Delta$ or $g(\Delta) \cap \Delta = \emptyset$.

Definition

We call set $\Sigma = \{\Gamma_i \mid \Gamma_i \subset \Omega\}$ the system of blocks for group G if each Γ_i is a block for G and $\bigcup_i \Gamma_i = \Omega$.

It is known that block for regular group is a coset of some subgroup.

Diffusion of systems of blocks

Let $V_m = \{0,1\}^m$, $W < V_m$. Denote by $(V_m : W)$ the set of cosets V_m by W. The partition $(V_m : W)$ is invariant with respect to the group

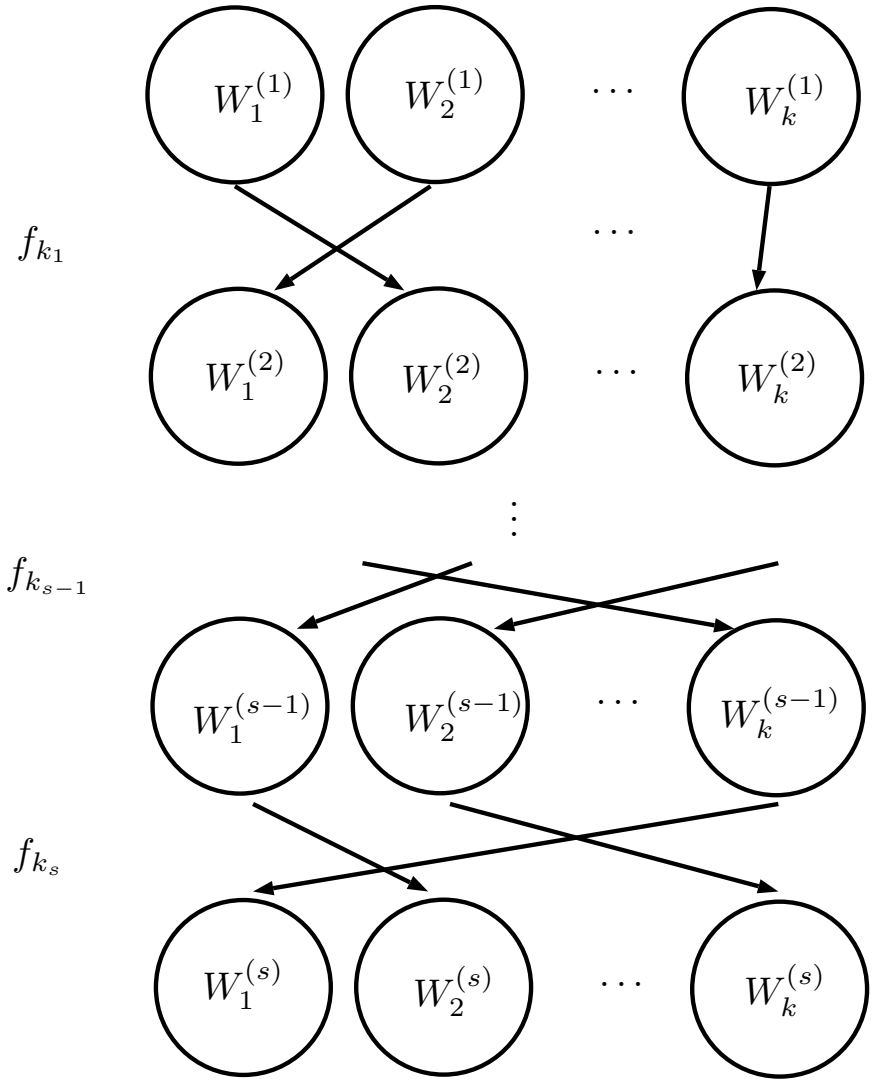
$$V_m^+ = \left\{\alpha^+ : x \mapsto x + \alpha \,|\alpha \in V_m\right\}.$$

The existence of $W, U < V_m$ such that

$$f(V_m : W) = (V_m : U)$$

can be used in the the partition-based attack. There are examples of block ciphers that are resistant to the differential and linear methods, but not to the partition-based attack (Bannier A., 2016).

Trapdoor based on a system of blocks



The relationship cryptographic characteristics of diffusion of the system of blocks

Let $W, U < V_m$, $\dim W = \dim U = d$. If

$$f(V_m : W) = (V_m : U),$$

then (Bannier A., 2016)

$$\delta(f) \geq \frac{2^m}{2^d - 1}.$$

It follows that differentially 2-uniform permutation does not map the partition $(V_m : W)$ into the partition $(V_m : U)$ for any $W, U < V_m$. However, differentially 4-uniform permutation can map the partition $(V_m : W)$ into partition $(V_m : U)$ for some W, U.

Question

How to relax the requirements for $\delta(f)$ in some permutation classes?

Detecting systems of blocks

Most of used S-boxes act on spaces of small dimension ($m \leq 8$), so iterate over all subspaces and check

$$f(V_m : W) = (V_m : U).$$

However, recently, in connection with homomorphic encryption, block ciphers (Chaghri, MiMC) have been proposed, the round function of which has the form

$$f_k : x \mapsto f(x + k),$$

where f is the permutation of high-dimensional field $\mathbb{F}_{2^m}$. For example, in Chaghri: $f : x \mapsto x^{2^{32}+1}$, $x \in \mathbb{F}_{2^{63}}$, in MiMC: $f : x \mapsto x^3$, $x \in \mathbb{F}_{2^{63}}$. In this case, it is impossible to iterate through all subspaces. Consequently, cipher design requires a theoretical proof of the non-existance of such subspaces.

Definitions and notations

1. $\mathbb{F}_{2^m}^+$ — right regular representation of the group $(\mathbb{F}_{2^m}, +)$.
2. $\mathbb{F}_{2^m}^*$ — right regular representation of the group $(\mathbb{F}_{2^m}^\times, \cdot)$, where $\mathbb{F}_{2^m}^\times = \mathbb{F}_{2^m} \setminus \{0\}$.
3. Denote W^+, H^* as a regular representation of $W < (\mathbb{F}_{2^m}, +)$, $H < (\mathbb{F}_{2^m}^*, \cdot)$ in $\mathbb{F}_{2^m}^+$, $\mathbb{F}_{2^m}^*$, respectively.
4. By $\preccurlyeq$ we denote a partial ordering relation on set $\{0, \ldots, 2^m - 1\}$: for $a = \sum\limits_{i=0}^{m-1} a_i 2^i$, $b = \sum\limits_{i=0}^{m-1} b_i 2^i \in \{0, \ldots, 2^m - 1\}$, $a_0, \ldots, a_{m-1}, b_0, \ldots, b_{m-1} \in \{0, 1\}$

$$a \preccurlyeq b \iff \forall i \in \{0, \ldots, m-1\}\ a_i \leq b_i.$$

The relation $a \prec b$ holds if and only if $a \preccurlyeq b$ and $a \neq b$.

Definition

Let $H < (\mathbb{F}_{2^m}^{\times}, \cdot)$ and $\mathbb{F}_{2^m}^{\times} = \bigcup_{i=0}^{r_H - 1} H_i$, H_i — cosets of H, $r_H = |\mathbb{F}_{2^m}^{\times} : H|$. A mapping $f : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ is called k-piecewise-monomial on $H < \mathbb{F}_{2^m}^{*}$ if the following properties hold:

1. $f(0) = 0$,
2. there are $A_0, A_1, \ldots, A_{r_H - 1} \in \mathbb{F}_{2^m}$ such that for every $x \in H_i$ the equality $f(x) = x^k A_i, i \in \{0, \ldots, r_H - 1\}$, holds.

Definition

Group

$$\mathrm{Aut}(f) = \{\varphi \in AGL_{2m}(2) \,|\varphi(\Gamma_f) = \Gamma_f\},$$

where is

$$\Gamma_f = \{(x, f(x)) \mid x \in V_m\},$$

is called the automorphism group of the function $f\colon V_m \to V_m$.

1. The group $\mathrm{Aut}(f)$ is non-trivial for the known APN permutations f, (Beierle C., Brinkmann M., Leander G., "Linearly self-equivalent APN permutations in small dimension", 2021).
2. The non-triviality of the group $\mathrm{Aut}(f)$ was used to construct 4-uniform permutations with graph algebraic immunity 3 (Burov D.A., Kostarev S.V., Menyachikhin A.V., 2023).

Definition

The subgroup $\mathrm{Aut}_{LE}(f)$ of the group $\mathrm{Aut}(f)$ is defined as:

$$\mathrm{Aut}_{LE}(f) = \left\{ \varphi \in \mathrm{Aut}(f) \mid \varphi = \begin{pmatrix} \varphi_1 & 0 \\ 0 & \varphi_2 \end{pmatrix}, \varphi_1, \varphi_2 \in GL_m(2) \right\}.$$

Define the projections of the $\mathrm{Aut}_{LE}(f)$ as

$$\mathrm{Aut}_{LE}(f)_1 = \left\{ \varphi_1 \in GL_m(2) \mid \exists \varphi_2 \in GL_m(2) : \begin{pmatrix} \varphi_1 & 0 \\ 0 & \varphi_2 \end{pmatrix} \in \mathrm{Aut}_{LE}(f) \right\}.$$

$$\mathrm{Aut}_{LE}(f)_2 = \left\{ \varphi_2 \in GL_m(2) \mid \exists \varphi_1 \in GL_m(2) : \begin{pmatrix} \varphi_1 & 0 \\ 0 & \varphi_2 \end{pmatrix} \in \mathrm{Aut}_{LE}(f) \right\}.$$

Systems of blocks for permutations with a non-trivial automorphism group

Theorem

Let f be a permutation over vector space V_m. Suppose that

$$f(V_m : W) = (V_m : U)$$

for some proper subspaces $W, U < V_m$. Then one of the following holds:

1. *for some subspaces $K < W, L < U$, $\dim K, \dim L \geq 2$ we have*

$$f(V_m : K) = (V_m : L),$$

   and $K^\times$ is a block for $Aut_{LE}(f)_1$, $L^\times$ is a block for $Aut_{LE}(f)_2$;
2. $\delta(f) = 2^m$.

Automorphism groups for some classes of permutations

1. If $f : x \mapsto x^r$, $x \in \mathbb{F}_{2^m}^*$ is a power permutation, then

$$\mathbb{F}_{2^m}^* < \mathrm{Aut}_{LE}(f)_1, \mathbb{F}_{2^m}^* < \mathrm{Aut}_{LE}(f)_2.$$

   Since $\mathbb{F}_{2^m}^*$ is a regular, the blocks for $\mathbb{F}_{2^m}^*$ is a cosets of $(\mathbb{F}_{2^m}^{\times}, \cdot)$.
2. If f is a piecewise-monomial permutation on $H < (\mathbb{F}_{2^m}, \cdot)$, then

$$H^* < \mathrm{Aut}_{LE}(f)_1, H^* < \mathrm{Aut}_{LE}(f)_2.$$

   Since H^* is a semi-regular group, we need description of blocks for semi-regular groups.

Blocks for subgroups of the group $\mathbb{F}_{2^m}^*$

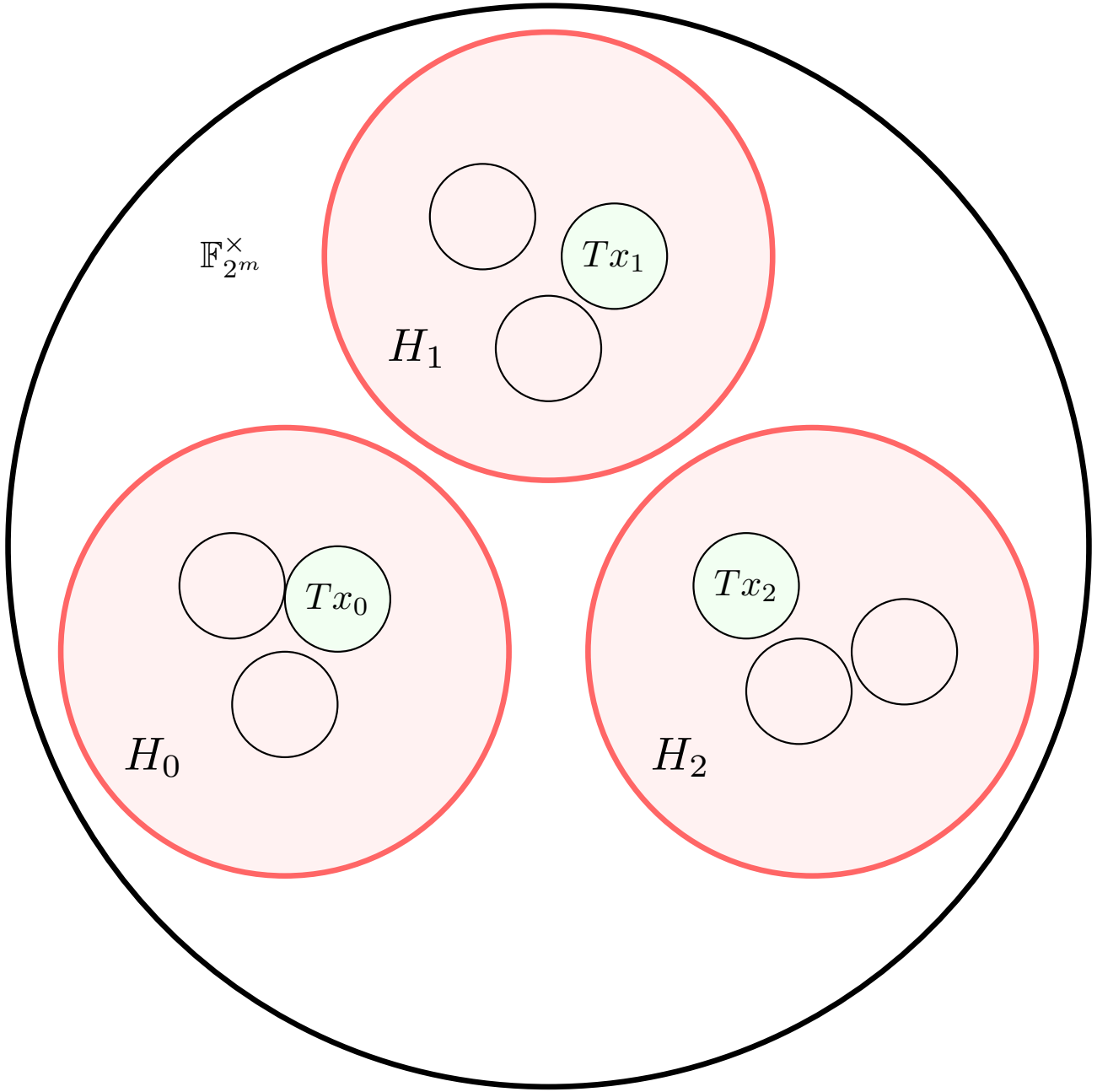
Lemma

Let $H < (\mathbb{F}_{2^m}^\times, \cdot)$, $\mathbb{F}_{2^m}^\times = \bigcup_{i=0}^{r-1} H_i$ *be the partition of* $(\mathbb{F}_{2^m}^\times, \cdot)$ *into cosets of* H, $r = |\mathbb{F}_{2^m}^\times : H|$. *Then subset* $\Delta \subseteq \mathbb{F}_{2^m}^\times$ *is a block for group* H^* *if and only if there exist*

1. *subgroup* $T < H$,
2. *subset of* $I \subseteq \{0, \ldots, r-1\}$,
3. *elements* $x_i \in H_i$, $i \in I$

such that

$$\Delta = \bigcup_{i \in I} T x_i.$$


$\mathbb{F}_{2^m}^{\times}$
Tx_1
H_1
Tx_0
H_0
Tx_2
H_2

Blocks for subgroups of the group $\mathbb{F}_{2^m}^*$ of index 3

Proposition

Let m be an even number, H be a subgroup of the group $(\mathbb{F}_{2^m}^\times, \cdot)$ of index 3, W be a subgroup of the group $(\mathbb{F}_{2^m}, +)$ such that $W^\times$ is a block for H^*. Then one of the following holds:

1. $W = q\mathbb{F}_{2^k}$ *for some* $k \mid m, q \in \mathbb{F}_{2^m}^\times$;
2. W *has dimension* $k \in \{1, 2\}$ *for* $3 \mid m$, *and* $k = 1$ *for* $3 \nmid m$.

Blocks for subgroups of $\mathbb{F}_{2^m}^*$ of index 5

Proposition

Let $4 \mid m$, H be a subgroup of $(\mathbb{F}_{2^m}^\times, \cdot)$ of index 5, W be a subgroup of the group $(\mathbb{F}_{2^m}, +)$ such that $W^\times$ is a block for H^*. Then one of the following conditions holds:

1. $W = q\mathbb{F}_{2^k}$ *for some* $q \in \mathbb{F}_{2^m}^\times$, $k \mid m$;
2. W *has dimension* $k \in \{1, 2, 4\}$ *for* $5 \mid m$, *and* $k \in \{1, 2\}$ *for* $5 \nmid m$.

Systems of blocks for monomial permutations

Theorem

Let $f : x \mapsto x^k$ *be the monomial permutation on* $\mathbb{F}_{2^m}$, $gcd(k, 2^m - 1) = 1$. *Then the following conditions are equivalent:*

1. k *equals* 2^i *for some* $i \in \{0, \ldots, m-1\}$;
2. *there are proper subgroups* $W, U < (\mathbb{F}_{2^m}, +)$ *such that*

$$f\left(\mathbb{F}_{2^m} : W\right) = \left(\mathbb{F}_{2^m} : U\right).$$

Systems of blocks for piecewise-monomial permutations on subgroup of index 3

Theorem

Let f be k-piecewise-monomial on H permutation of $\mathbb{F}_{2^m}$, H have index 3 in $(\mathbb{F}_{2^m}^{\times}, \cdot)$, $m \geq 8$ be an even number, and one of the following holds:

1. $3 \nmid m$ *and* $f(x) \neq x^{2^i}$, $i \in \{0, \ldots, m-1\}$;
2. $3 \mid m$ *and* $\delta(f) < \frac{2^m}{3}$.

Then there are no proper subgroups $W, U < (\mathbb{F}_{2^m}, +)$ such that

$$f\left(\mathbb{F}_{2^m} : W\right) = \left(\mathbb{F}_{2^m} : U\right).$$

Systems of blocks for piecewise-monomial permutations on subgroup of index 5

Theorem

Let f be k-piecewise-monomial on H permutation of $\mathbb{F}_{2^m}$, H have index 5 in $(\mathbb{F}_{2^m}^{\times}, \cdot)$, $m \geq 8$, and one of the following holds:

1. $5 \nmid m$ *and* $\delta(f) < \frac{2^m}{3}$;
2. $5 \mid m$ *and* $\delta(f) < \frac{2^m}{15}$.

Then there are no proper subgroups $W, U < (\mathbb{F}_{2^m}, +)$ such that

$$f\left(\mathbb{F}_{2^m} : W\right) = \left(\mathbb{F}_{2^m} : U\right).$$

Definition

$a \in V_m^{\times}$ is called a linear structure of function $f : V_m \to \{0, 1\}$ if

$$f(x + a) + f(x) = c \text{ for all } x, \text{ where } c \in \{0, 1\}.$$

Lemma

Let $f = (f_{m-1}, \ldots, f_0) : V_m \to V_m$ *and*

$$f(\mathbb{F}_{2^m} : W) = (\mathbb{F}_{2^m} : U)$$

for some proper subgroups $W, U < (\mathbb{F}_{2^m}, +)$. *Then there is a vector* $b = (b_{m-1}, \ldots, b_0) \in V_m^{\times}$ *such that the linear combination* $b \circ f = \sum_{i=0}^{m-1} b_i f_i$ *has a linear structure.*

Polynomial representation of piecewise-monomial permutations

Proposition (Charpin P., 2022)

Let F be a polynomial over $\mathbb{F}_{2^m}$, $F(x) = \sum_{\ell=1}^{2^m-2} a_\ell x^\ell$. If there is an exponent ℓ, and k in the range $\{1, \ldots, 2^n - 2\}$, such that $2^i k \neq \ell'$ for all exponent ℓ' and for any i, unless $i = 0$ and $\ell' = \ell$, then, no linear combination of the coordinate functions f has linear structures.

Proposition

A mapping $f : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ is k-piecewise–monomial on $H < \mathbb{F}_{2^m}^*$, $|H| = l$, if and only if f admits a representation $F(x)$ as a univariate polynomial over $\mathbb{F}_{2^m}$ of the form

$$F(x) = x^k G(x^l)$$

where $G(x) \in \mathbb{F}_{2^m}[x]$, $\deg G(x) \leq r_H - 1$.

Proposition

Let f be a k-piecewise-monomial permutation on $H < (\mathbb{F}_{2^m}^{\times}, \cdot)$, $f(x) \neq x^{2^i}$, $i \in \{0, \ldots, m-1\}$ that satisfies one of the following conditions:

1. $k = 1, \left|\mathbb{F}_{2^m}^{\times} : H\right| = 3$, $m \geq 6$ — *even number;*
2. $k = 1, \left|\mathbb{F}_{2^m}^{\times} : H\right| = 5$, $m \geq 12$ — *multiple of 4;*
3. $k = 2^d + 1, \left|\mathbb{F}_{2^m}^{\times} : H\right| = 3$, $m \geq 12$ — *even number;*
4. $k = 2^d + 1, \left|\mathbb{F}_{2^m}^{\times} : H\right| = 5$, $m \geq 16$ — *multiple of 4;*

Then there are no proper subgroups $W, U < (\mathbb{F}_{2^m}, +)$ such that

$$f\left(\mathbb{F}_{2^m} : W\right) = \left(\mathbb{F}_{2^m} : U\right).$$

Thanks for attention.