# On functions $F\colon \mathbb{F}_{2^{2t}} \to \mathbb{F}_{2^{2t}}$ mapping cosets of $\mathbb{F}_{2^t}^*$ to cosets of $\mathbb{F}_{2^t}^*$

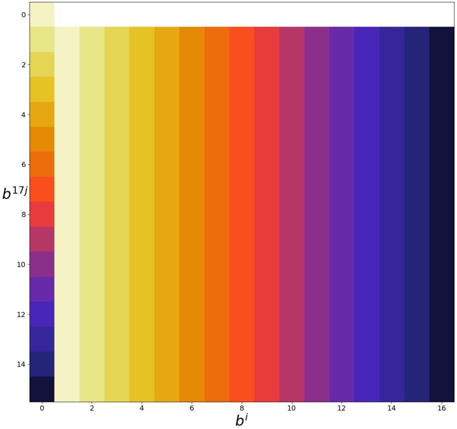
Jules Baudrin, Anne Canteaut & Léo Perrin

Inria, Paris, France

June 18th, 2024

Contact: jules.baudrin@inria.fr

# Alignment




The Sbox $\pi$ [GOST standards Streebog/Kuznyechik]

- $\pi : \mathbb{F}_2^8 \to \mathbb{F}_2^8$ bijection specified as a look-up table
- Reversed-engineered [BirPerUdo16,PerUdo16,Per19]
- Happens to be extremely aligned !

# In this talk

1a) The Sbox $\pi$

1b) Bijections mapping $\gamma\mathbb{F}_{2^t}^*$ onto $G(\gamma)+\mathbb{F}_{2^t}^*$ (and their linearity)

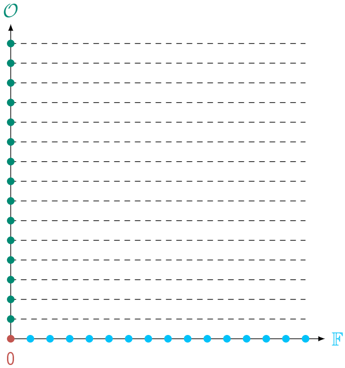
2a) The Kim mapping $\kappa$

2b) Functions mapping $\gamma\mathbb{F}_{2^t}^*$ onto $F(\gamma)\mathbb{F}_{2^t}^*$ (and their APN-ness)

# Partitions of $\mathbb{L}$ and $\mathbb{L}^*$

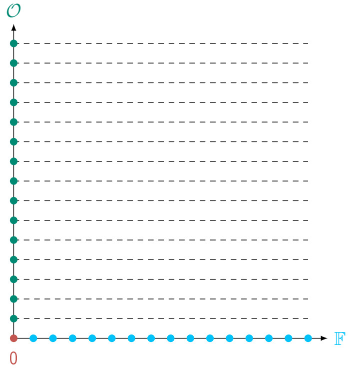
## Finite fields

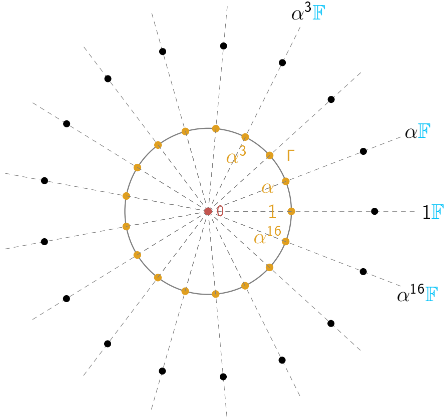
- $\mathbb{F} \subset \mathbb{L}$ finite fields of characteristic 2.
- $\mathbb{F}$ additive subgroup of $\mathbb{L} \implies \mathbb{L} = \bigsqcup_{x \in \mathcal{O}} x + \mathbb{F}$



## Finite fields

- $\mathbb{F} \subset \mathbb{L}$ finite fields of characteristic 2.
- $\mathbb{F}$ additive subgroup of $\mathbb{L} \implies \mathbb{L} = \bigsqcup_{x \in \mathcal{O}} x + \mathbb{F}$
- $\mathbb{F}^*$ multiplicative subgroup of $\mathbb{L}^* \implies \mathbb{L}^* = \bigsqcup_{\gamma \in \Gamma} \gamma\mathbb{F}^*$



# Decomposition of $\pi$

$\mathbb{F}_2^8 \simeq \mathbb{L} = \mathbb{F}_{256}, \quad \mathbb{F} = \mathbb{F}_{16}$ $\lambda \in \mathbb{L}, \gamma \in \Gamma, \varphi \in \mathbb{F}$

16 additive cosets $x + \mathbb{F}, x \in \mathcal{O}$, 17 multiplicative cosets $\gamma\mathbb{F}^*, \gamma \in \Gamma$

$\mathbb{F}_2^8 \simeq \mathbb{L} = \mathbb{F}_{256}$, $\mathbb{F} = \mathbb{F}_{16}$ $\lambda \in \mathbb{L}, \gamma \in \Gamma, \varphi \in \mathbb{F}$

16 additive cosets $x + \mathbb{F}, x \in \mathcal{O}$, 17 multiplicative cosets $\gamma\mathbb{F}^*, \gamma \in \Gamma$

## Multiplicative cosets to additive cosets

- For any $\gamma\mathbb{F}^* \neq \mathbb{F}^*$, $\pi(\gamma\mathbb{F}^*) = x_\gamma + \mathbb{F}^*$.

## Decomposition of $\pi$

$\mathbb{F}_2^8 \simeq \mathbb{L} = \mathbb{F}_{256}, \quad \mathbb{F} = \mathbb{F}_{16}$ $\quad \lambda \in \mathbb{L}, \gamma \in \Gamma, \varphi \in \mathbb{F}$

16 additive cosets $x + \mathbb{F}, x \in \mathcal{O}$, 17 multiplicative cosets $\gamma\mathbb{F}^*, \gamma \in \Gamma$

### Multiplicative cosets to additive cosets

- For any $\gamma\mathbb{F}^* \neq \mathbb{F}^*$, $\quad \pi(\gamma\mathbb{F}^*) = x_\gamma + \mathbb{F}^*$.
- $\pi(\mathbb{F}) = \{x_\gamma\} = \mathcal{O}$

# Decomposition of $\pi$

$\mathbb{F}_2^8 \simeq \mathbb{L} = \mathbb{F}_{256}, \quad \mathbb{F} = \mathbb{F}_{16}$ $\lambda \in \mathbb{L}, \gamma \in \Gamma, \varphi \in \mathbb{F}$

16 additive cosets $x + \mathbb{F}, x \in \mathcal{O}$, 17 multiplicative cosets $\gamma\mathbb{F}^*, \gamma \in \Gamma$

## Multiplicative cosets to additive cosets

- For any $\gamma\mathbb{F}^* \neq \mathbb{F}^*$, $\pi(\gamma\mathbb{F}^*) = x_\gamma + \mathbb{F}^*$.
- $\pi(\mathbb{F}) = \{x_\gamma\} = \mathcal{O}$
- $\gamma\mathbb{F}^* \rightsquigarrow x_\gamma + \mathbb{F}^*$ always the same.

$\mathbb{F}_2^8 \simeq \mathbb{L} = \mathbb{F}_{256}$, $\quad \mathbb{F} = \mathbb{F}_{16}$ $\qquad \lambda \in \mathbb{L}, \gamma \in \Gamma, \varphi \in \mathbb{F}$

16 additive cosets $x + \mathbb{F}, x \in \mathcal{O}$, $\qquad$ 17 multiplicative cosets $\gamma\mathbb{F}^*, \gamma \in \Gamma$

### Multiplicative cosets to additive cosets

- For any $\gamma\mathbb{F}^* \neq \mathbb{F}^*$, $\quad \pi(\gamma\mathbb{F}^*) = x_\gamma + \mathbb{F}^*$.
- $\pi(\mathbb{F}) = \{x_\gamma\} = \mathcal{O}$
- $\gamma\mathbb{F}^* \rightsquigarrow x_\gamma + \mathbb{F}^*$ always the same.

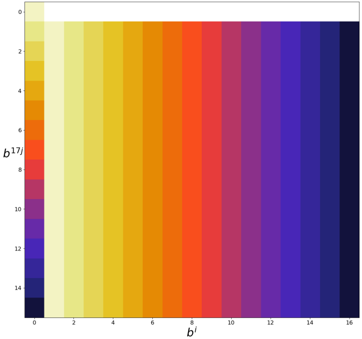
### Decomposition of $\pi$ [Perrin19]

With well-chosen $\mathbb{F}_2^8 \simeq \mathbb{L}$, $\Gamma$, $\mathcal{O}$, $\quad \pi$ can be expressed as:

$$\begin{aligned} \pi|_{\mathbb{L}\setminus\mathbb{F}} : \mathbb{L} \setminus \mathbb{F} &\to \mathbb{L} \\ \gamma\varphi &\mapsto G(\gamma) + F(\varphi) \end{aligned}$$

where $G : \Gamma \setminus \mathbb{F} \xrightarrow{\sim} \mathcal{O}$, $\quad F : \mathbb{F} \xrightarrow{\sim} \mathbb{F}$ $\quad$ with $F(0) = 0$ and $\pi(\mathbb{F}) = \mathcal{O}$.

$\pi(\gamma\varphi) = G(\gamma) + F(\varphi)$ when $\gamma \in \Gamma \setminus \mathbb{F}, \varphi \in \mathbb{F}^*$.

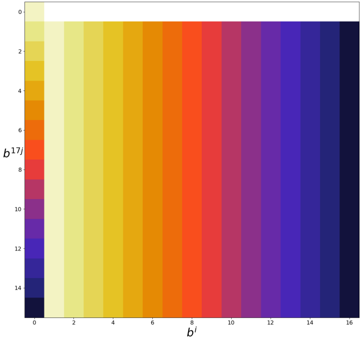



$\mathrm{Tr}_{\mathbb{L}/\mathbb{F}}(\pi(b^{i+17j}))$, where $\mathbb{L}^* = \langle b \rangle$

## A few novelties

- The choice of $\mathcal{O}$ is understood.
- $G$ is understood.
- $\pi|_{\mathbb{F}}$ and $G$ behaves in the “same way”.

$\pi(\gamma\varphi) = G(\gamma) + F(\varphi)$ when $\gamma \in \Gamma \setminus \mathbb{F}, \varphi \in \mathbb{F}^*$.




$\mathrm{Tr}_{\mathbb{L}/\mathbb{F}}(\pi(b^{i+17j}))$, where $\mathbb{L}^* = \langle b \rangle$

## A few novelties

- The choice of $\mathcal{O}$ is understood.
- $G$ is understood.
- $\pi|_{\mathbb{F}}$ and $G$ behaves in the "same way".

**Can we say more about this structure ?**

# Generalizing $\pi$

$\pi|_{\mathbb{L}\setminus\mathbb{F}}: \quad \gamma\varphi \mapsto G(\gamma) + F(\varphi)$ $\qquad$ $\Gamma, \mathcal{O}$, sys. of reps. $\qquad$ $\lambda \in \mathbb{L}, \gamma \in \Gamma, \varphi \in \mathbb{F}$

$\pi|_{\mathbb{L}\setminus\mathbb{F}}: \quad \gamma\varphi \mapsto G(\gamma) + F(\varphi)$ $\qquad \Gamma, \mathcal{O}$, sys. of reps. $\qquad \lambda \in \mathbb{L}, \gamma \in \Gamma, \varphi \in \mathbb{F}$

## Generalizing $\pi$

$[\mathbb{L} : \mathbb{F}] = 2 \qquad |\mathbb{L}^*| = 2^{2t} - 1 = (2^t - 1)(2^t + 1) \qquad |\Gamma| = 2^t + 1, \quad |\mathcal{O}| = |\mathbb{F}| = 2^t.$

$\pi|_{\mathbb{L}\setminus\mathbb{F}}: \quad \gamma\varphi \;\mapsto\; G(\gamma) + F(\varphi)$ $\qquad$ $\Gamma, \mathcal{O}$, sys. of reps. $\qquad$ $\lambda \in \mathbb{L}, \gamma \in \Gamma, \varphi \in \mathbb{F}$

## Generalizing $\pi$

$[\mathbb{L} : \mathbb{F}] = 2$ $\qquad$ $|\mathbb{L}^*| = 2^{2t} - 1 = (2^t - 1)(2^t + 1)$ $\qquad$ $|\Gamma| = 2^t + 1, \quad |\mathcal{O}| = |\mathbb{F}| = 2^t.$

$$\Pi|_{\mathbb{L}\setminus\mathbb{F}}: \quad \gamma\varphi \;\mapsto\; G(\gamma) + F(\varphi)$$

where $G : \Gamma \setminus \mathbb{F} \xrightarrow{\sim} \mathcal{O}$, $\quad F : \mathbb{F} \xrightarrow{\sim} \mathbb{F}$, with $F(0) = 0$ and $\Pi(\mathbb{F}) = \mathcal{O}$.

$\pi|_{\mathbb{L}\setminus\mathbb{F}}: \quad \gamma\varphi \mapsto G(\gamma) + F(\varphi)$ $\qquad \Gamma, \mathcal{O}$, sys. of reps. $\qquad \lambda \in \mathbb{L}, \gamma \in \Gamma, \varphi \in \mathbb{F}$

## Generalizing $\pi$

$[\mathbb{L} : \mathbb{F}] = 2 \qquad |\mathbb{L}^*| = 2^{2t} - 1 = (2^t - 1)(2^t + 1) \qquad |\Gamma| = 2^t + 1, \quad |\mathcal{O}| = |\mathbb{F}| = 2^t.$

$$\Pi|_{\mathbb{L}\setminus\mathbb{F}}: \quad \gamma\varphi \mapsto G(\gamma) + F(\varphi)$$

where $G : \Gamma \setminus \mathbb{F} \xrightarrow{\sim} \mathcal{O}$, $\quad F : \mathbb{F} \xrightarrow{\sim} \mathbb{F}$, with $F(0) = 0$ and $\Pi(\mathbb{F}) = \mathcal{O}$.

## Walsh coefficients of $\Pi$

$$\widehat{\Pi}_\beta(\alpha) := \sum_{\lambda \in \mathbb{L}} (-1)^{\mathrm{Tr}_{\mathbb{L}/\mathbb{F}_2}(\alpha\lambda + \beta\Pi(\lambda))}$$

$\pi|_{\mathbb{L}\setminus\mathbb{F}}: \quad \gamma\varphi \;\mapsto\; G(\gamma) + F(\varphi)$ $\quad\Gamma, \mathcal{O}$, sys. of reps. $\quad \lambda \in \mathbb{L}, \gamma \in \Gamma, \varphi \in \mathbb{F}$

## Generalizing $\pi$

$[\mathbb{L} : \mathbb{F}] = 2 \qquad |\mathbb{L}^*| = 2^{2t} - 1 = (2^t - 1)(2^t + 1) \qquad |\Gamma| = 2^t + 1, \quad |\mathcal{O}| = |\mathbb{F}| = 2^t.$

$$\Pi|_{\mathbb{L}\setminus\mathbb{F}}: \quad \gamma\varphi \;\mapsto\; G(\gamma) + F(\varphi)$$

where $G : \Gamma \setminus \mathbb{F} \xrightarrow{\sim} \mathcal{O}$, $\quad F : \mathbb{F} \xrightarrow{\sim} \mathbb{F}$, with $F(0) = 0$ and $\Pi(\mathbb{F}) = \mathcal{O}$.

## Walsh coefficients of $\Pi$

$\widehat{\Pi}_\beta(\alpha) := \sum_{\lambda\in\mathbb{L}} (-1)^{\mathrm{Tr}_{\mathbb{L}/\mathbb{F}_2}(\alpha\lambda+\beta\Pi(\lambda))}$ $\qquad H : \mathbb{F} \to \mathbb{F},\; x \mapsto \mathrm{Tr}_{\mathbb{L}/\mathbb{F}}(\gamma_\beta \Pi(x))$

$$\widehat{\Pi}_\beta(\alpha) = \widehat{H}_{\varphi_\beta}(\mathrm{Tr}_{\mathbb{L}/\mathbb{F}}(\alpha)) - \widehat{H}_{\varphi_\beta}(0) + \sum_{\gamma\in\Gamma\setminus\mathbb{F}} (-1)^{\mathrm{Tr}_{\mathbb{L}/\mathbb{F}}(\beta G(\gamma))}\, \widehat{F}_{\mathrm{Tr}_{\mathbb{L}/\mathbb{F}}(\beta)}(\mathrm{Tr}_{\mathbb{L}/\mathbb{F}}(\alpha\gamma))$$

# Functions with low linearity

$\Pi|_{\mathbb{L}\setminus\mathbb{F}}: \quad \gamma\varphi \mapsto G(\gamma) + F(\varphi)$ $\qquad \Gamma, \mathcal{O}$, sys. of reps. $\qquad \lambda \in \mathbb{L}, \gamma \in \Gamma, \varphi \in \mathbb{F}$

$$\widehat{\Pi}_\beta(\alpha) := \sum_{\lambda\in\mathbb{L}} (-1)^{\mathrm{Tr}_{\mathbb{L}/\mathbb{F}_2}(\alpha\lambda+\beta\Pi(\lambda))}$$

# Functions with low linearity

$\Pi|_{\mathbb{L}\setminus\mathbb{F}}: \quad \gamma\varphi \mapsto G(\gamma) + F(\varphi) \qquad \Gamma, \mathcal{O}$, sys. of reps. $\qquad \lambda \in \mathbb{L}, \gamma \in \Gamma, \varphi \in \mathbb{F}$

$$\widehat{\Pi}_\beta(\alpha) := \sum_{\lambda\in\mathbb{L}} (-1)^{\mathrm{Tr}_{\mathbb{L}/\mathbb{F}_2}(\alpha\lambda+\beta\Pi(\lambda))}$$

### A specific choice for $\Gamma$

$[\mathbb{L} : \mathbb{F}] = 2 \quad \Longrightarrow \quad \Gamma$ can be the subgroup $\mathbb{G}$ of order $2^t + 1$.

$\Pi|_{\mathbb{L}\setminus\mathbb{F}}: \quad \gamma\varphi \mapsto G(\gamma) + F(\varphi)$ $\quad$ $\Gamma, \mathcal{O}$, sys. of reps. $\quad$ $\lambda \in \mathbb{L}, \gamma \in \Gamma, \varphi \in \mathbb{F}$

$$\widehat{\Pi}_\beta(\alpha) := \sum_{\lambda \in \mathbb{L}} (-1)^{\mathrm{Tr}_{\mathbb{L}/\mathbb{F}_2}(\alpha\lambda + \beta\Pi(\lambda))}$$

**A specific choice for $\Gamma$**

$[\mathbb{L} : \mathbb{F}] = 2 \implies \Gamma$ can be the subgroup $\mathbb{G}$ of order $2^t + 1$.

**Functions with low linearity**

$\Gamma = \mathbb{G}$, $F = \mathrm{Id}$.

$\Pi|_{\mathbb{L}\setminus\mathbb{F}}: \quad \gamma\varphi \mapsto G(\gamma) + F(\varphi)$ $\qquad \Gamma, \mathcal{O}$, sys. of reps. $\qquad \lambda \in \mathbb{L}, \gamma \in \Gamma, \varphi \in \mathbb{F}$

$$\widehat{\Pi}_\beta(\alpha) := \sum_{\lambda \in \mathbb{L}} (-1)^{\mathrm{Tr}_{\mathbb{L}/\mathbb{F}_2}(\alpha\lambda + \beta\Pi(\lambda))}$$

## A specific choice for $\Gamma$

$[\mathbb{L} : \mathbb{F}] = 2 \implies \Gamma$ can be the subgroup $\mathbb{G}$ of order $2^t + 1$.

## Functions with low linearity

$\Gamma = \mathbb{G}$, $F = \mathrm{Id}$. $\qquad$ For $\forall\ \alpha, \forall\ \beta \neq 0$, $\quad |\widehat{\Pi}_\beta(\alpha)| \leq 2^{t+2}$.

Best known bijections achieve $\leq 2^{t+1}$

# In this talk

1a) The Sbox $\pi$ ☑

1b) Bijections mapping $\gamma\mathbb{F}_{2^t}^*$ onto $G(\gamma)+\mathbb{F}_{2^t}^*$ (and their linearity) ☑

2a) The Kim mapping $\kappa$

2b) Functions mapping $\gamma\mathbb{F}_{2^t}^*$ onto $F(\gamma)\mathbb{F}_{2^t}^*$ (and their APN-ness)

# The enigmatic Kim function

**Kim mapping** [BDMW10]

$$\begin{aligned} \kappa : \quad \mathbb{F}_{64} &\to \mathbb{F}_{64} \\ x &\mapsto x^3 + x^{10} + ux^{24}; \end{aligned}$$

where $u$ is a specific root of $x^6 + x^4 + x^3 + x + 1$.

**Kim mapping** [BDMW10]

$$\begin{aligned}\kappa: \quad \mathbb{F}_{64} &\to \mathbb{F}_{64} \\ x &\mapsto x^3 + x^{10} + ux^{24};\end{aligned}$$

where $u$ is a specific root of $x^6 + x^4 + x^3 + x + 1$.

**The reason of the fame**

- Optimal resistance against differential cryptanalysis (APN)
- Even number of variables and CCZ-equivalent to a bijection

$F \sim G \iff \exists\ \mathcal{A}$ affine, bijective, $\quad \mathcal{A}(\{(x, F(x)), x \in \mathbb{L}\}) = \{(x, G(x)), x \in \mathbb{L}\}$

## Kim mapping [BDMW10]

$$\kappa: \mathbb{F}_{64} \rightarrow \mathbb{F}_{64}$$
$$x \mapsto x^3 + x^{10} + ux^{24};$$

where $u$ is a specific root of $x^6 + x^4 + x^3 + x + 1$.

## The reason of the fame

- Optimal resistance against differential cryptanalysis (APN)
- Even number of variables and CCZ-equivalent to a bijection

$F \sim G \iff \exists\, \mathcal{A}$ affine, bijective, $\mathcal{A}(\{(x, F(x)), x \in \mathbb{L}\}) = \{(x, G(x)), x \in \mathbb{L}\}$

## Big APN problem

Up to CCZ-equivalence, does there exist any other APN permutation in even dimension ?

# The subspace property

A "special" property [BDMW10]

*"$\kappa$ maps the subspace $\lambda\mathbb{F}_8$ to the subspace $\kappa(\lambda)\mathbb{F}_8$ for all $\lambda \in \mathbb{F}_{64}$"*

## A "special" property [BDMW10]

*"$\kappa$ maps the subspace $\lambda\mathbb{F}_8$ to the subspace $\kappa(\lambda)\mathbb{F}_8$ for all $\lambda \in \mathbb{F}_{64}$"*

## Subspace property

$\mathbb{F} \subset \mathbb{L}$ two finite fields. $F : \mathbb{L} \to \mathbb{L}$ satisfies the subspace property if:

$$\forall\ \lambda \in \mathbb{L}, \quad F(\lambda\mathbb{F}) = F(\lambda)\mathbb{F}.$$

**A "special" property** [BDMW10]

*"$\kappa$ maps the subspace $\lambda\mathbb{F}_8$ to the subspace $\kappa(\lambda)\mathbb{F}_8$ for all $\lambda \in \mathbb{F}_{64}$"*

**Subspace property**

$\mathbb{F} \subset \mathbb{L}$ two finite fields. $F : \mathbb{L} \to \mathbb{L}$ satisfies the subspace property if:

$$\forall\ \lambda \in \mathbb{L}, \quad F(\lambda\mathbb{F}) = F(\lambda)\mathbb{F}.$$

**Mapping cosets onto cosets**

$\mathbb{F} \subset \mathbb{L}$ two finite fields. $F : \mathbb{L} \to \mathbb{L}$ satisfies the subspace property iff:

$$\forall\lambda \in \mathbb{L},\ \exists\ G_\lambda : \mathbb{F} \to \mathbb{F} \text{ bijective s.t: } \quad \forall\varphi \in \mathbb{F}, \quad F(\lambda\varphi) = F(\lambda)G_\lambda(\varphi).$$

If $F(\lambda) \neq 0$, $G_\lambda$ unique

# Properties of the Kim mapping (1/2)

$\kappa(x) = x^3 + x^{10} + ux^{24}$

# Properties of the Kim mapping (1/2)

$\kappa(x) = x^3 + x^{10} + ux^{24}$

**Observation** [BDMW10]

$$\forall\ \varphi \in \mathbb{F}, \lambda \in \mathbb{L}, \quad \kappa(\varphi\lambda) = \varphi^3 \kappa(\lambda)$$

Proof: As $|\mathbb{F}^*| = 7$, we get $\varphi^3 = \varphi^{10} = \varphi^{24}$.

# Properties of the Kim mapping (1/2)

$\kappa(x) = x^3 + x^{10} + ux^{24}$

**Observation** [BDMW10]

$$\forall\ \varphi \in \mathbb{F}, \lambda \in \mathbb{L}, \quad \kappa(\varphi\lambda) = \varphi^3 \kappa(\lambda)$$

Proof: As $|\mathbb{F}^*| = 7$, we get $\varphi^3 = \varphi^{10} = \varphi^{24}$.

**Cyclotomic mapping** [Wang07]

$\mathbb{G} \subset \mathbb{L}^*$ a subgroup. $F : \mathbb{L} \to \mathbb{L}$ is a cyclotomic mapping of order $d$ over $\mathbb{G}$ if:

$$\forall\ \lambda \in \mathbb{L}, \forall\ \varphi \in \mathbb{G}, \quad F(\varphi\lambda) = \varphi^d F(\lambda) \quad \Longleftrightarrow \quad F = x^d P(x^{|G|})$$

Here: $\mathbb{G} = \mathbb{F}^*$

# Properties of the Kim mapping (1/2)

$\kappa(x) = x^3 + x^{10} + ux^{24}$

**Observation** [BDMW10]

$$\forall\ \varphi \in \mathbb{F}, \lambda \in \mathbb{L}, \quad \kappa(\varphi\lambda) = \varphi^3 \kappa(\lambda)$$

Proof: As $|\mathbb{F}^*| = 7$, we get $\varphi^3 = \varphi^{10} = \varphi^{24}$.

**Cyclotomic mapping** [Wang07]

$\mathbb{G} \subset \mathbb{L}^*$ a subgroup. $F : \mathbb{L} \to \mathbb{L}$ is a cyclotomic mapping of order $d$ over $\mathbb{G}$ if:

$$\forall\ \lambda \in \mathbb{L}, \forall\ \varphi \in \mathbb{G}, \quad F(\varphi\lambda) = \varphi^d F(\lambda) \quad \Longleftrightarrow \quad F = x^d P(x^{|G|})$$

Here: $\mathbb{G} = \mathbb{F}^*$

- Also known as Wan Lidl polynomials [WanLidl91]
- Studies about graphs or permutations, [AkbWan07, BorPanWan23, Laigle-Chapuy07]
- only a few about cryptographic properties [ChenCoulter23, Gologlu23, BeiBriLea21]

*Subspace prop*: $\forall\ \lambda,\qquad F(\lambda\mathbb{F}) = F(\lambda)\mathbb{F}$

*Cyclotomic*: $\exists\ d, \forall\ \lambda, \forall\ \varphi,\quad F(\varphi\lambda) = \varphi^d F(\lambda)$

*Subspace prop*: $\forall\ \lambda,\qquad F(\lambda\mathbb{F}) = F(\lambda)\mathbb{F}$

*Cyclotomic*: $\exists\ d, \forall\ \lambda, \forall\ \varphi,\quad F(\varphi\lambda) = \varphi^d F(\lambda)$

## Trivial relations

- Cyclotomic $\implies \forall\ \lambda,\quad F(\lambda\mathbb{F}) \subset F(\lambda)\mathbb{F}$.
- Cyclotomic mapping satisfies the subspace property $\iff$ $x \mapsto x^d$ bijective over $\mathbb{F}$

# Subspace property and Cyclotomy

*Subspace prop*: $\forall\ \lambda, \qquad F(\lambda\mathbb{F}) = F(\lambda)\mathbb{F}$

*Cyclotomic*: $\exists\ d, \forall\ \lambda, \forall\ \varphi, \quad F(\varphi\lambda) = \varphi^d F(\lambda)$

## Trivial relations

- Cyclotomic $\implies \forall\ \lambda, \quad F(\lambda\mathbb{F}) \subset F(\lambda)\mathbb{F}$.
- Cyclotomic mapping satisfies the subspace property $\iff x \mapsto x^d$ bijective over $\mathbb{F}$

## Generalized cyclotomic mapping [BorsWang22]

$\mathbb{G} \subset \mathbb{L}^*$ a subgroup. $F : \mathbb{L} \to \mathbb{L}$ is a generalized cyclotomic mapping over $\mathbb{G}$ if:

$$\forall\ \lambda \in \mathbb{L}, \exists\ d_\lambda, \forall\ \varphi \in \mathbb{G}, \quad F(\varphi\lambda) = \varphi^{d_\lambda} F(\lambda)$$

*Subspace prop*: $\forall\ \lambda,\qquad F(\lambda\mathbb{F}) = F(\lambda)\mathbb{F}$
*Cyclotomic*: $\exists\ d, \forall\ \lambda, \forall\ \varphi,\quad F(\varphi\lambda) = \varphi^d F(\lambda)$

## Trivial relations

- Cyclotomic $\implies \forall\ \lambda,\quad F(\lambda\mathbb{F}) \subset F(\lambda)\mathbb{F}$.
- Cyclotomic mapping satisfies the subspace property $\iff$ $x \mapsto x^d$ bijective over $\mathbb{F}$

## Generalized cyclotomic mapping [BorsWang22]

$\mathbb{G} \subset \mathbb{L}^*$ a subgroup. $F : \mathbb{L} \to \mathbb{L}$ is a generalized cyclotomic mapping over $\mathbb{G}$ if:

$$\forall\ \lambda \in \mathbb{L}, \exists\ d_\lambda, \forall\ \varphi \in \mathbb{G},\quad F(\varphi\lambda) = \varphi^{d_\lambda} F(\lambda)$$

## More trivial relations

- Gen. cyclotomic $\implies \forall\ \lambda,\quad F(\lambda\mathbb{F}) \subset F(\lambda)\mathbb{F}$.
- Gen. cyclotomic mapping satisfies the subspace property $\iff$ $\forall\ \lambda, \gcd(d_\lambda, |\mathbb{F}^*|) = 1$

# Spectral point of view (1/2)

*Subspace prop*: $\forall\ \lambda, \quad F(\lambda\mathbb{F}) = F(\lambda)\mathbb{F}.$ $\quad F(\lambda\varphi) = F(\lambda)G_\lambda(\varphi)$, with $G_\lambda : \mathbb{F} \xrightarrow{\sim} \mathbb{F}$

$$\widehat{F}_\beta(\alpha) := \sum_{\lambda\in\mathbb{L}} (-1)^{\mathrm{Tr}_{\mathbb{L}/\mathbb{F}_2}(\alpha\lambda+\beta F(\lambda))}$$

$\mathbb{L} = \mathbb{F}_{2^{2t}}$, $\mathbb{F} = \mathbb{F}_{2^t}$

*Subspace prop*: $\forall\ \lambda, \quad F(\lambda\mathbb{F}) = F(\lambda)\mathbb{F}$. $\qquad F(\lambda\varphi) = F(\lambda)G_\lambda(\varphi)$, with $G_\lambda : \mathbb{F} \xrightarrow{\sim} \mathbb{F}$

$\widehat{F}_\beta(\alpha) := \sum_{\lambda\in\mathbb{L}} (-1)^{\mathrm{Tr}_{\mathbb{L}/\mathbb{F}_2}(\alpha\lambda+\beta F(\lambda))}$ $\qquad \mathbb{L} = \mathbb{F}_{2^{2t}}$, $\mathbb{F} = \mathbb{F}_{2^t}$

## Decomposition of Walsh coefficients

$\Gamma$ system of representatives, $\alpha, \beta \in \mathbb{L}$. $F : \mathbb{L} \to \mathbb{L}$ satisfying the subspace property. Then:

$$\widehat{F}_\beta(\alpha) = -2^t + \sum_{\gamma\in\Gamma} \widehat{G_\lambda}_{\mathrm{Tr}_{\mathbb{L}/\mathbb{F}}(\beta F(\gamma))}(\mathrm{Tr}_{\mathbb{L}/\mathbb{F}}(\alpha\gamma)).$$

*Subspace prop*: $\forall\ \lambda, \quad F(\lambda\mathbb{F}) = F(\lambda)\mathbb{F}.$ $\quad F(\lambda\varphi) = F(\lambda)G_\lambda(\varphi)$, with $G_\lambda : \mathbb{F} \xrightarrow{\sim} \mathbb{F}$

$$\widehat{F}_\beta(\alpha) := \sum_{\lambda\in\mathbb{L}} (-1)^{\mathrm{Tr}_{\mathbb{L}/\mathbb{F}_2}(\alpha\lambda+\beta F(\lambda))}$$

$\mathbb{L} = \mathbb{F}_{2^{2t}}$, $\mathbb{F} = \mathbb{F}_{2^t}$

## Decomposition of Walsh coefficients

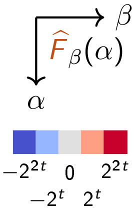
$\Gamma$ system of representatives, $\alpha, \beta \in \mathbb{L}$. $F : \mathbb{L} \to \mathbb{L}$ satisfying the subspace property. Then:

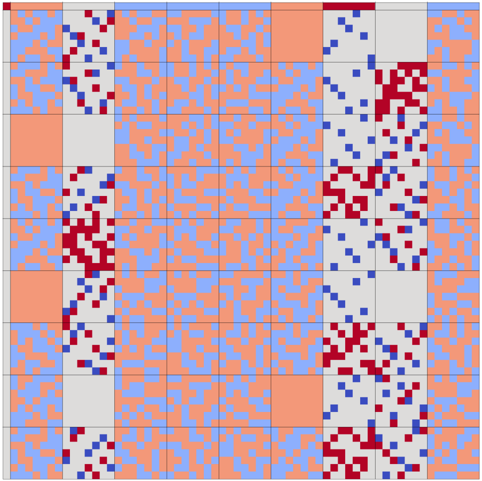
$$\widehat{F}_\beta(\alpha) = -2^t + \sum_{\gamma\in\Gamma} \widehat{G_\lambda}_{\mathrm{Tr}_{\mathbb{L}/\mathbb{F}}(\beta F(\gamma))}(\mathrm{Tr}_{\mathbb{L}/\mathbb{F}}(\alpha\gamma)).$$

## Symmetries of Walsh coefficients

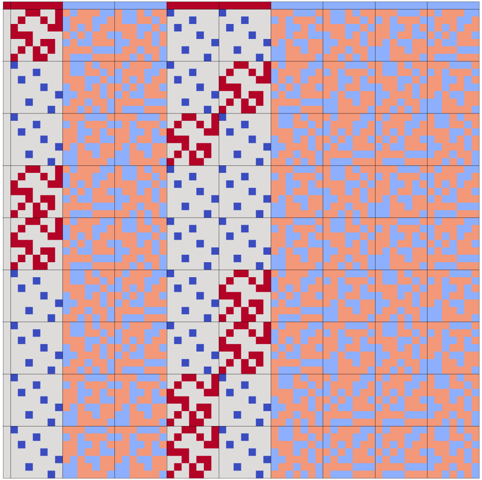
Let $G : \mathbb{F} \to \mathbb{F}$. $F$ satisfies the subspace property with $G_\lambda = G\ \forall\ \lambda$ if and only if:

$$\forall \alpha, \beta \in \mathbb{L},\ \forall \varphi \in \mathbb{F}^*, \quad \widehat{F}_{\beta G(\varphi)}(\alpha) = \widehat{F}_\beta(\alpha\varphi^{-1}).$$

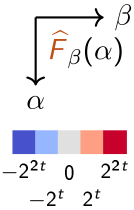


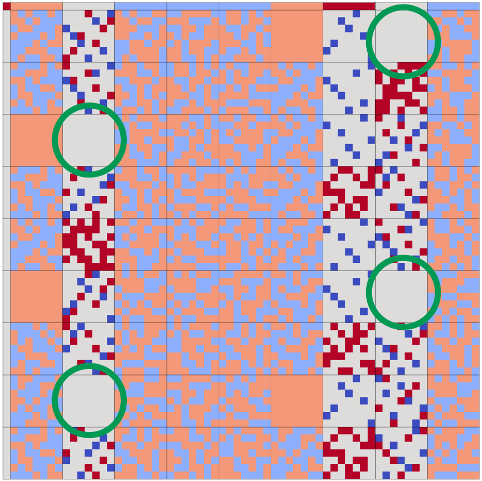



Kim mapping $\kappa: x \mapsto x^3 + x^{10} + ux^{24}$

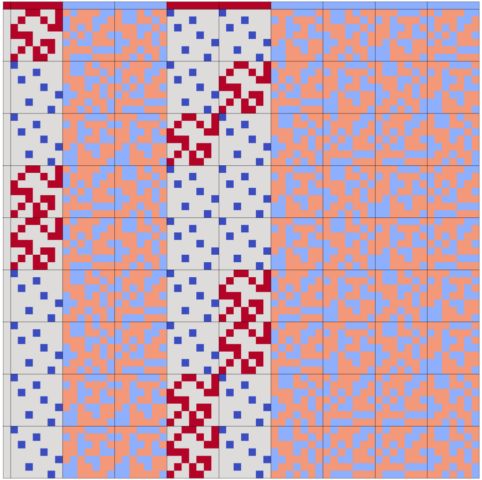


Cube over $\mathbb{F}_{64}$ $x \mapsto x^3$

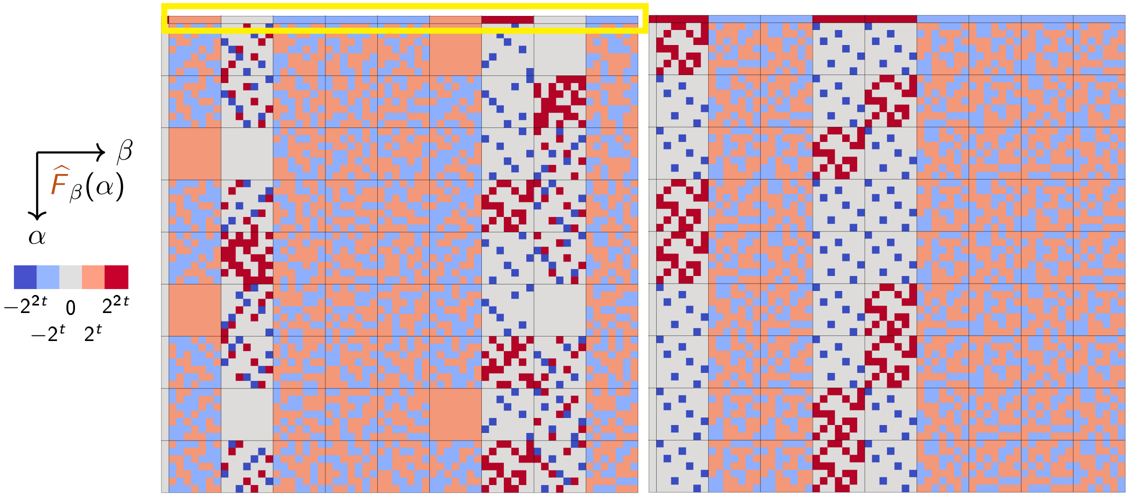


Kim mapping $\kappa\colon x \mapsto x^3 + x^{10} + ux^{24}$



Cube over $\mathbb{F}_{64}$ $x \mapsto x^3$




Kim mapping $\kappa\colon x \mapsto x^3 + x^{10} + ux^{24}$

Cube over $\mathbb{F}_{64}$ $x \mapsto x^3$

# Walsh coefficients $\widehat{F}_\beta(0)$

*Subspace prop*: $\forall\ \lambda,\quad F(\lambda\mathbb{F}) = F(\lambda)\mathbb{F}.\qquad F(\lambda\varphi) = F(\lambda)G_\lambda(\varphi)$, with $G_\lambda : \mathbb{F} \xrightarrow{\sim} \mathbb{F}$

$$\widehat{F}_\beta(\alpha) := \sum_{\lambda\in\mathbb{L}} (-1)^{\mathrm{Tr}_{\mathbb{L}/\mathbb{F}_2}(\alpha\lambda+\beta F(\lambda))} \qquad N_\lambda := \frac{\left|F^{-1}(\lambda\mathbb{F})\right|}{|\mathbb{F}|}$$

# Walsh coefficients $\widehat{F}_\beta(0)$

*Subspace prop*: $\forall\ \lambda, \quad F(\lambda\mathbb{F}) = F(\lambda)\mathbb{F}. \qquad F(\lambda\varphi) = F(\lambda)G_\lambda(\varphi)$, with $G_\lambda : \mathbb{F} \xrightarrow{\sim} \mathbb{F}$

$$\widehat{F}_\beta(\alpha) := \sum_{\lambda\in\mathbb{L}} (-1)^{\mathrm{Tr}_{\mathbb{L}/\mathbb{F}_2}(\alpha\lambda+\beta F(\lambda))} \qquad N_\lambda := \frac{\left|F^{-1}(\lambda\mathbb{F})\right|}{|\mathbb{F}|}$$

## Walsh coefficients in zero

$F$ satisfying the subspace property. $[\mathbb{L} : \mathbb{F}] = 2$. Then

$$\forall\ \beta \in \mathbb{L}^*, \quad \widehat{F}_\beta(0) = 2^t(N_{\beta^{-1}} - 1)$$

*Subspace prop*: $\forall\ \lambda, \quad F(\lambda\mathbb{F}) = F(\lambda)\mathbb{F}. \qquad F(\lambda\varphi) = F(\lambda)G_\lambda(\varphi)$, with $G_\lambda : \mathbb{F} \xrightarrow{\sim} \mathbb{F}$

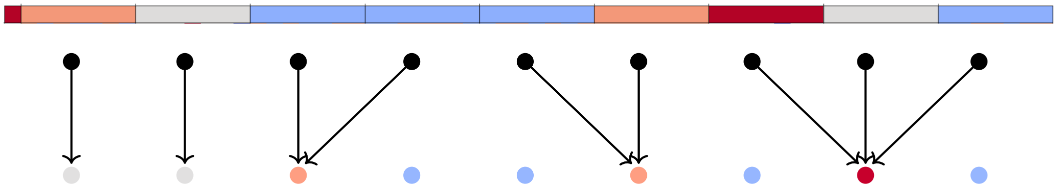
$$\widehat{F}_\beta(\alpha) := \sum_{\lambda\in\mathbb{L}} (-1)^{\mathrm{Tr}_{\mathbb{L}/\mathbb{F}_2}(\alpha\lambda+\beta F(\lambda))} \qquad N_\lambda := \frac{|F^{-1}(\lambda\mathbb{F})|}{|\mathbb{F}|}$$

**Walsh coefficients in zero**

$F$ satisfying the subspace property. $[\mathbb{L} : \mathbb{F}] = 2$. Then

$$\forall\ \beta \in \mathbb{L}^*, \quad \widehat{F}_\beta(0) = 2^t(N_{\beta^{-1}} - 1)$$

Kim mapping



# Walsh coefficients $\widehat{F}_\beta(0)$

*Subspace prop*: $\forall\ \lambda,\quad F(\lambda\mathbb{F}) = F(\lambda)\mathbb{F}$. $\qquad F(\lambda\varphi) = F(\lambda)G_\lambda(\varphi)$, with $G_\lambda : \mathbb{F} \xrightarrow{\sim} \mathbb{F}$

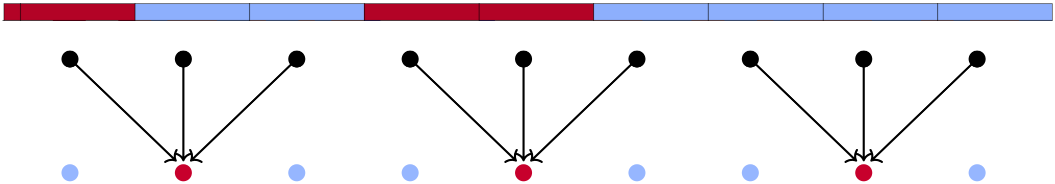
$$\widehat{F}_\beta(\alpha) := \sum_{\lambda\in\mathbb{L}} (-1)^{\mathrm{Tr}_{\mathbb{L}/\mathbb{F}_2}(\alpha\lambda+\beta F(\lambda))} \qquad N_\lambda := \frac{\left|F^{-1}(\lambda\mathbb{F})\right|}{|\mathbb{F}|}$$

## Walsh coefficients in zero

$F$ satisfying the subspace property. $[\mathbb{L} : \mathbb{F}] = 2$. Then

$$\forall\ \beta \in \mathbb{L}^*,\quad \widehat{F}_\beta(0) = 2^t(N_{\beta^{-1}} - 1)$$

Cube



# Subspace property and APNness

*Subspace prop*: $\forall\ \lambda,\quad F(\lambda\mathbb{F}) = F(\lambda)\mathbb{F}.\qquad F(\lambda\varphi) = F(\lambda)G_\lambda(\varphi)$, with $G_\lambda : \mathbb{F} \xrightarrow{\sim} \mathbb{F}$

$N_\lambda := \frac{|F^{-1}(\lambda\mathbb{F})|}{|\mathbb{F}|} \qquad \mathcal{N}_i := \{\gamma \in \Gamma, N_\gamma = i\}$

Subspace prop. when $[\mathbb{L} : \mathbb{F}] = 2 \implies \widehat{F}_\beta(0) = 2^t(N_{\beta^{-1}} - 1)$

*Subspace prop*: $\forall\ \lambda,\quad F(\lambda\mathbb{F}) = F(\lambda)\mathbb{F}.\qquad F(\lambda\varphi) = F(\lambda)G_\lambda(\varphi)$, with $G_\lambda : \mathbb{F} \xrightarrow{\sim} \mathbb{F}$

$N_\lambda := \frac{|F^{-1}(\lambda\mathbb{F})|}{|\mathbb{F}|} \qquad \mathcal{N}_i := \{\gamma \in \Gamma, N_\gamma = i\}$

Subspace prop. when $[\mathbb{L} : \mathbb{F}] = 2 \implies \quad \widehat{F}_\beta(0) = 2^t(N_{\beta^{-1}} - 1)$

## Necessary condition to be APN

$F$ quadratic satisfying the subspace property. $[\mathbb{L} : \mathbb{F}] = 2$.

- If $F$ is APN then $\mathcal{N}_0 + \mathcal{N}_2 \geq \frac{2(2^t+1)}{3}$
- If $\mathcal{L}(F) = 2^{t+1}$ and $\mathcal{N}_0 + \mathcal{N}_2 \geq \frac{2(2^t+1)}{3}$ then $F$ is APN.

Proof: [BerCanChaLai06]

# Subspace property and APNness

*Subspace prop*: $\forall\ \lambda,\quad F(\lambda\mathbb{F}) = F(\lambda)\mathbb{F}.\qquad F(\lambda\varphi) = F(\lambda)G_\lambda(\varphi)$, with $G_\lambda : \mathbb{F} \xrightarrow{\sim} \mathbb{F}$

$N_\lambda := \frac{|F^{-1}(\lambda\mathbb{F})|}{|\mathbb{F}|}\qquad \mathcal{N}_i := \{\gamma \in \Gamma, N_\gamma = i\}$

Subspace prop. when $[\mathbb{L} : \mathbb{F}] = 2 \implies \widehat{F}_\beta(0) = 2^t(N_{\beta^{-1}} - 1)$

## Necessary condition to be APN

$F$ quadratic satisfying the subspace property. $[\mathbb{L} : \mathbb{F}] = 2$.

- If $F$ is APN then $\mathcal{N}_0 + \mathcal{N}_2 \geq \frac{2(2^t+1)}{3}$
- If $\mathcal{L}(F) = 2^{t+1}$ and $\mathcal{N}_0 + \mathcal{N}_2 \geq \frac{2(2^t+1)}{3}$ then $F$ is APN.

Proof: [BerCanChaLai06]

## One already-solved case [Gologlu2023, ChaLis21]

$F$ quadratic cyclotomic when $[\mathbb{L} : \mathbb{F}] = 2$.

- If $t \neq 3$: $F$ APN $\iff$ $F \sim_{\text{CCZ}}$ Gold power
- If $t = 3$: $F$ APN $\iff$ $F \sim_{\text{CCZ}}$ Gold power or $F \sim_{\text{CCZ}} \kappa$.

# Squares of zeros

*Cyclotomic*: $\exists\ d, \forall\ \lambda, \forall\ \varphi, \quad F(\varphi\lambda) = \varphi^d F(\lambda)$ $\quad \mathbb{L} = \mathbb{F}_{2^{2t}}, \mathbb{F} = \mathbb{F}_{2^t}$

$$\widehat{F}_\beta(\alpha) := \sum_{\lambda \in \mathbb{L}} (-1)^{\mathrm{Tr}_{\mathbb{L}/\mathbb{F}_2}(\alpha\lambda + \beta F(\lambda))} \qquad Z_F := \left\{(\alpha, \beta), \widehat{F}_\beta(\alpha) = 0\right\} \cup \{(0,0)\}$$

# Squares of zeros

*Cyclotomic*: $\exists\, d, \forall\, \lambda, \forall\, \varphi, \quad F(\varphi\lambda) = \varphi^d F(\lambda)$ $\mathbb{L} = \mathbb{F}_{2^{2t}}, \mathbb{F} = \mathbb{F}_{2^t}$

$$\widehat{F}_\beta(\alpha) := \sum_{\lambda \in \mathbb{L}} (-1)^{\mathrm{Tr}_{\mathbb{L}/\mathbb{F}_2}(\alpha\lambda + \beta F(\lambda))} \qquad Z_F := \left\{(\alpha, \beta), \widehat{F}_\beta(\alpha) = 0\right\} \cup \{(0,0)\}$$

## Walsh zeroes

$F$ CCZ-equiv. to a bijection iff $\exists, U, V \subset Z_F$ subspaces of dim. $n$, $U \cap V = \{0\}$.

For $\kappa$, $U = u_1\mathbb{F} \times u_2\mathbb{F}$, $V = v_1\mathbb{F} \times v_2\mathbb{F}$.

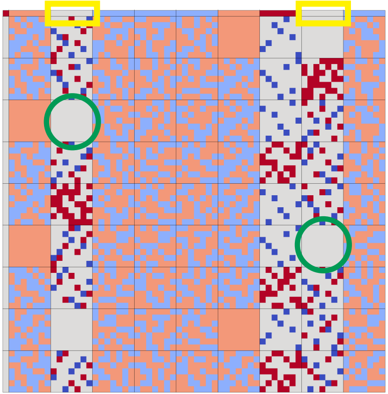
*Cyclotomic*: $\exists\, d, \forall\, \lambda, \forall\, \varphi, \quad F(\varphi\lambda) = \varphi^d F(\lambda)$ $\qquad \mathbb{L} = \mathbb{F}_{2^{2t}},\ \mathbb{F} = \mathbb{F}_{2^t}$

$$\widehat{F}_\beta(\alpha) := \sum_{\lambda \in \mathbb{L}} (-1)^{\mathrm{Tr}_{\mathbb{L}/\mathbb{F}_2}(\alpha\lambda + \beta F(\lambda))} \qquad Z_F := \left\{(\alpha,\beta), \widehat{F}_\beta(\alpha) = 0\right\} \cup \{(0,0)\}$$

## Walsh zeroes

$F$ CCZ-equiv. to a bijection iff $\quad \exists, U, V \subset Z_F$ subspaces of dim. $n$, $U \cap V = \{0\}$.

For $\kappa$, $U = u_1\mathbb{F} \times u_2\mathbb{F}$, $V = v_1\mathbb{F} \times v_2\mathbb{F}$.



## Characterization of $\alpha\mathbb{F}^* \times \beta\mathbb{F}^* \subset Z_F$

For cyclotomic mappings of order $d$ over $\mathbb{F}$, $[\mathbb{L} : \mathbb{F}] = 2$

- $F(\mathbb{L}) = c\mathbb{F} \quad \implies \quad \forall\, \alpha,\ \alpha\mathbb{F}^* \times c\mathbb{F}^* \subset Z_F$
- Otherwise*, can only happened if $\widehat{F}_\beta(0) = 0$.

* Full characterization in the abstract

# Conclusion

## Generalizations of $\pi$ and linearity

Can we go below $\mathcal{L}(\Pi) \leq 2^{t+2}$ with other $\Gamma, \mathcal{O}, F, G$ ? constructions close to this one ?

## Subspace property / Cyclotomic mapping APNness

- Study of non-bijective cyclotomic mapping
- Still hope : non-quadratic or $[\mathbb{L} : \mathbb{F}] \neq 2 \ldots$
- Computer search

## CCZ-equivalence and bijectivity

Is the characterization of Walsh-zeros "square" sporadic or not ?

## Thanks ! ☺

# Subspace property and Cyclotomy

*Subspace prop*: $\forall\ \lambda$, $\quad F(\lambda\mathbb{F}) = F(\lambda)\mathbb{F}$

*Cyclotomic*: $\exists\ d, \forall\ \lambda, \forall\ \varphi$, $\quad F(\varphi\lambda) = \varphi^{d} F(\lambda)$

*Gen. cyclotomic*: $\forall\ \lambda, \exists\ d_\lambda, \forall\ \varphi$, $\quad F(\varphi\lambda) = \varphi^{d_\lambda} F(\lambda)$