On CCZ-Equivalence, Extended-Affine Equivalence and Function Twisting

Anne Canteaut, Léo Perrin

June 18, 2018
BFA'2018

informatics mathematics

Definition (CCZ-Equivalence)

$F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ and $G : \mathbb{F}_2^n \to \mathbb{F}_2^m$ are *C(arlet)-C(harpin)-Z(inoviev) equivalent* if

$$\Gamma_G = \left\{(x, G(x)), \forall x \in \mathbb{F}_2^n\right\} \;=\; L\left(\left\{(x, F(x)), \forall x \in \mathbb{F}_2^n\right\}\right) = L(\Gamma_F)\,,$$

where $L : \mathbb{F}_2^{n+m} \to \mathbb{F}_2^{n+m}$ is an affine permutation.

Definition (CCZ-Equivalence)

$F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ and $G : \mathbb{F}_2^n \to \mathbb{F}_2^m$ are *C(arlet)-C(harpin)-Z(inoviev) equivalent* if

$$\Gamma_G = \left\{(x, G(x)), \forall x \in \mathbb{F}_2^n\right\} \; = \; L\left(\left\{(x, F(x)), \forall x \in \mathbb{F}_2^n\right\}\right) = L(\Gamma_F) \, ,$$

where $L : \mathbb{F}_2^{n+m} \to \mathbb{F}_2^{n+m}$ is an affine permutation.

Definition (EA-Equivalence; EA-mapping)

F and G are *E(xtented) A(ffine) equivalent* if $G(x) = (B \circ F \circ A)(x) + C(x)$, where A, B, C are affine and A, B are permutations; so that

$$\left\{(x, G(x)), \forall x \in \mathbb{F}_2^n\right\} \; = \left[\begin{array}{cc} A^{-1} & 0 \\ CA^{-1} & B \end{array} \right] \left(\left\{(x, F(x)), \forall x \in \mathbb{F}_2^n\right\}\right) \; .$$

Definition (CCZ-Equivalence)

$F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ and $G : \mathbb{F}_2^n \to \mathbb{F}_2^m$ are *C(arlet)-C(harpin)-Z(inoviev) equivalent* if

$$\Gamma_G = \left\{ (x, G(x)), \forall x \in \mathbb{F}_2^n \right\} \; = \; L\left(\left\{ (x, F(x)), \forall x \in \mathbb{F}_2^n \right\} \right) = L(\Gamma_F) \, ,$$

where $L : \mathbb{F}_2^{n+m} \to \mathbb{F}_2^{n+m}$ is an affine permutation.

Definition (EA-Equivalence; EA-mapping)

F and G are *E(xtented) A(ffine) equivalent* if $G(x) = (B \circ F \circ A)(x) + C(x)$, where A, B, C are affine and A, B are permutations; so that

$$\left\{ (x, G(x)), \forall x \in \mathbb{F}_2^n \right\} \; = \left[\begin{array}{cc} A^{-1} & 0 \\ CA^{-1} & B \end{array} \right] \left(\left\{ (x, F(x)), \forall x \in \mathbb{F}_2^n \right\} \right) \; .$$

Affine permutations with such linear part are **EA-mappings**; their transposes are **TEA-mappings**

Definition (CCZ-Equivalence)

$F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ and $G : \mathbb{F}_2^n \to \mathbb{F}_2^m$ are *C(arlet)-C(harpin)-Z(inoviev) equivalent* if

$$\Gamma_G = \{(x, G(x)), \forall x \in \mathbb{F}_2^n\} = L\left(\{(x, F(x)), \forall x \in \mathbb{F}_2^n\}\right) = L(\Gamma_F),$$

where $L : \mathbb{F}_2^{n+m} \to \mathbb{F}_2^{n+m}$ is an affine permutation.

Definition (EA-Equivalence; EA-mapping)

F and G are *E(xtented) A(ffine) equivalent* if $G(x) = (B \circ F \circ A)(x) + C(x)$, where A, B, C are affine and A, B are permutations; so that

$$\{(x, G(x)), \forall x \in \mathbb{F}_2^n\} = \begin{bmatrix} A^{-1} & 0 \\ CA^{-1} & B \end{bmatrix} \left(\{(x, F(x)), \forall x \in \mathbb{F}_2^n\}\right) .$$

Affine permutations with such linear part are **EA-mappings**; their transposes are **TEA-mappings**

What is the relation between functions that are CCZ- but not EA-equivalent?

Admissible Mapping

For $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$, the affine permutation L is **admissible for F** if

$$L\left(\{(x, F(x)), \forall x \in \mathbb{F}_2^n\} \right) = \{(x, G(x)), \forall x \in \mathbb{F}_2^n\}$$

for a well defined function $G : \mathbb{F}_2^n \to \mathbb{F}_2^m$.

Admissible Mapping

For $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$, the affine permutation L is **admissible for F** if

$$L\left(\{(x, F(x)), \forall x \in \mathbb{F}_2^n\} \right) = \{(x, G(x)), \forall x \in \mathbb{F}_2^n\}$$

for a well defined function $G : \mathbb{F}_2^n \to \mathbb{F}_2^m$.

Definition (LAT/Walsh Spectrum)

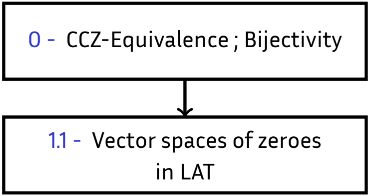
The L(inear) A(pproximation) T(able) of $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is

$$\mathcal{W}_F(\alpha, \beta) = \sum_{x \in \mathbb{F}_2^n} (-1)^{\alpha \cdot x + \beta \cdot F(x)} .$$

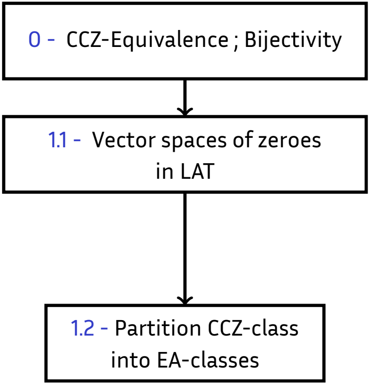
Structure of this talk

0 - CCZ-Equivalence ; Bijectivity

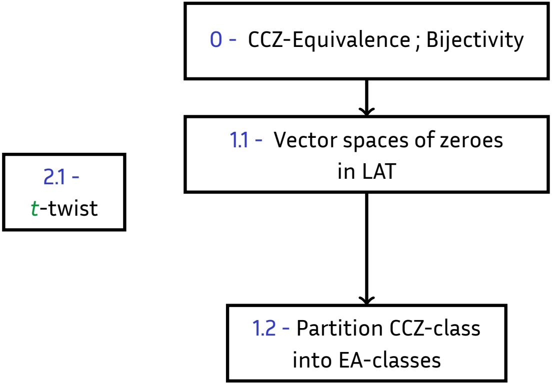
Structure of this talk



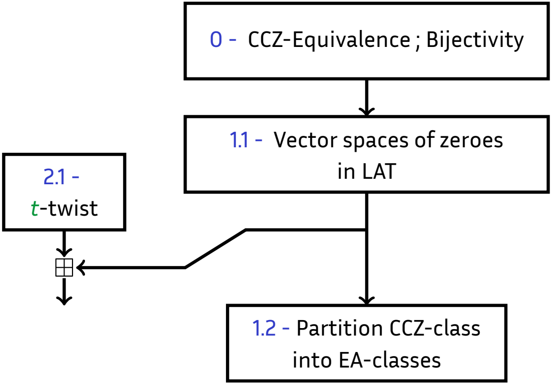
Structure of this talk



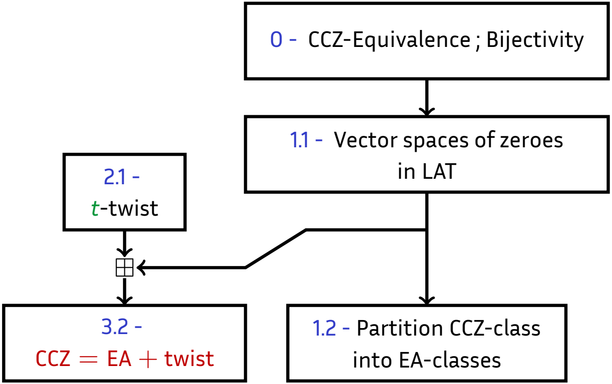
Structure of this talk



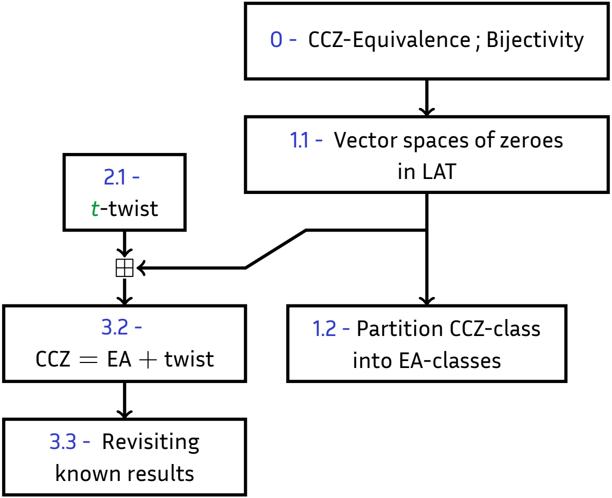
Structure of this talk



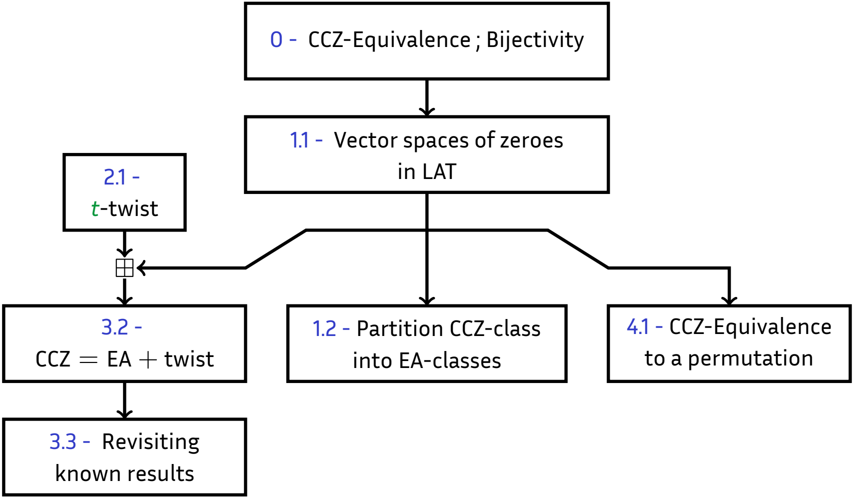
Structure of this talk



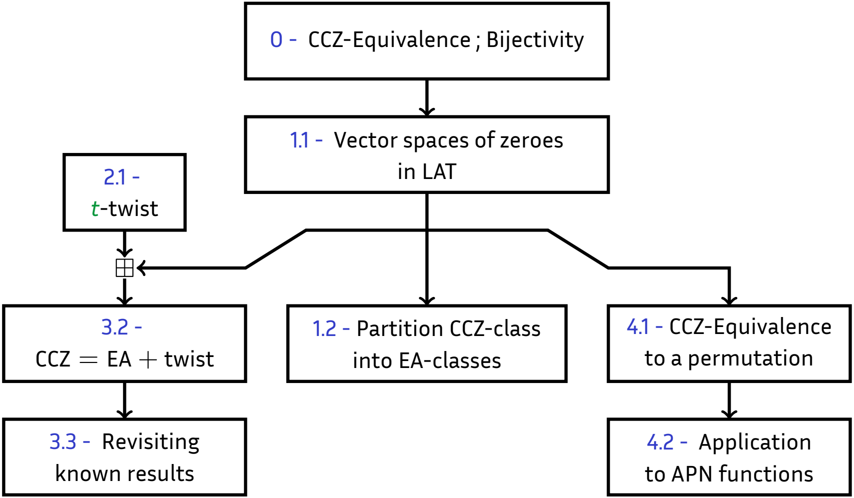
Structure of this talk



Structure of this talk



Structure of this talk



Outline

Plan of this Section

Walsh Zeroes

For all $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$, we have

$$\mathcal{W}_F(\alpha, 0) = \sum_{x \in \mathbb{F}_2^n} (-1)^{\alpha \cdot x + 0 \cdot F(x)} = 0.$$

Walsh Zeroes

For all $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m$, we have

$$\mathcal{W}_F(\alpha, 0) = \sum_{x \in \mathbb{F}_2^n} (-1)^{\alpha \cdot x + 0 \cdot F(x)} = 0.$$

Definition (Walsh Zeroes)

The *Walsh zeroes* of $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m$ is the set

$$\mathcal{Z}_F = \{u \in \mathbb{F}_2^n \times \mathbb{F}_2^m, \mathcal{W}_F(u) = 0\} \cup \{0\}.$$

With $\mathcal{V} = \{(x, 0), \forall x \in \mathbb{F}_2^n\} \subset \mathbb{F}_2^{n+m}$, we have $\mathcal{V} \subset \mathcal{Z}_F$.

Walsh Zeroes

For all $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$, we have

$$\mathcal{W}_F(\alpha, 0) = \sum_{x \in \mathbb{F}_2^n} (-1)^{\alpha \cdot x + 0 \cdot F(x)} = 0.$$

Definition (Walsh Zeroes)

The *Walsh zeroes* of $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is the set

$$\mathcal{Z}_F = \{u \in \mathbb{F}_2^n \times \mathbb{F}_2^m, \mathcal{W}_F(u) = 0\} \cup \{0\}.$$

With $\mathcal{V} = \{(x, 0), \forall x \in \mathbb{F}_2^n\} \subset \mathbb{F}_2^{n+m}$, we have $\mathcal{V} \subset \mathcal{Z}_F$.

Note that if $\Gamma_G = L(\Gamma_F)$, then $\mathcal{Z}_G = (L^T)^{-1}(\mathcal{Z}_F)$.

Admissibility for F

Lemma

Let $L : \mathbb{F}_2^{n+m} \to \mathbb{F}_2^{n+m}$ be a linear permutation. It is admissible for $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ if and only if

$$L^T(\mathcal{V}) \subseteq \mathcal{Z}_F$$

Admissibility of EA-mappings

EA-mappings are admissible for all $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$:

$$\begin{bmatrix} A & 0 \\ C & B \end{bmatrix}^T (\mathcal{V}) = \begin{bmatrix} A^T & C^T \\ 0 & B^T \end{bmatrix} \left(\left\{ \begin{bmatrix} x \\ 0 \end{bmatrix}, \forall x \in \mathbb{F}_2^n \right\} \right) = \mathcal{V} .$$

Admissibility of EA-mappings

EA-mappings are admissible for all $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m$:

$$\begin{bmatrix} A & 0 \\ C & B \end{bmatrix}^T (\mathcal{V}) = \begin{bmatrix} A^T & C^T \\ 0 & B^T \end{bmatrix} \left(\left\{ \begin{bmatrix} x \\ 0 \end{bmatrix}, \forall x \in \mathbb{F}_2^n \right\} \right) = \mathcal{V} .$$

Theorem (Budaghyan, Carlet (2011))

The CCZ-class of a bent function contains only its EA-class.

Admissibility of EA-mappings

EA-mappings are admissible for all $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$:

$$\begin{bmatrix} A & 0 \\ C & B \end{bmatrix}^T (\mathcal{V}) = \begin{bmatrix} A^T & C^T \\ 0 & B^T \end{bmatrix} \left(\left\{ \begin{bmatrix} x \\ 0 \end{bmatrix}, \forall x \in \mathbb{F}_2^n \right\} \right) = \mathcal{V} .$$

Theorem (Budaghyan, Carlet (2011))

The CCZ-class of a bent function contains only its EA-class.

Proof.

A function is bent

Admissibility of EA-mappings

EA-mappings are admissible for all $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$:

$$\begin{bmatrix} A & 0 \\ C & B \end{bmatrix}^T (\mathcal{V}) = \begin{bmatrix} A^T & C^T \\ 0 & B^T \end{bmatrix} \left(\left\{ \begin{bmatrix} x \\ 0 \end{bmatrix}, \forall x \in \mathbb{F}_2^n \right\} \right) = \mathcal{V} .$$

Theorem (Budaghyan, Carlet (2011))

The CCZ-class of a bent function contains only its EA-class.

Proof.

A function is bent

$\Longrightarrow$ no zeroes outside of $\mathcal{V}$

Admissibility of EA-mappings

EA-mappings are admissible for all $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$:

$$\begin{bmatrix} A & 0 \\ C & B \end{bmatrix}^T (\mathcal{V}) = \begin{bmatrix} A^T & C^T \\ 0 & B^T \end{bmatrix} \left(\left\{ \begin{bmatrix} x \\ 0 \end{bmatrix}, \forall x \in \mathbb{F}_2^n \right\} \right) = \mathcal{V} .$$

Theorem (Budaghyan, Carlet (2011))

The CCZ-class of a bent function contains only its EA-class.

Proof.

A function is bent

$\implies$ no zeroes outside of $\mathcal{V}$

$\implies$ no vector spaces of zeroes other than $\mathcal{V}$

Admissibility of EA-mappings

EA-mappings are admissible for all $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$:

$$\begin{bmatrix} A & 0 \\ C & B \end{bmatrix}^T (\mathcal{V}) = \begin{bmatrix} A^T & C^T \\ 0 & B^T \end{bmatrix} \left(\left\{ \begin{bmatrix} x \\ 0 \end{bmatrix}, \forall x \in \mathbb{F}_2^n \right\} \right) = \mathcal{V} .$$

Theorem (Budaghyan, Carlet (2011))

The CCZ-class of a bent function contains only its EA-class.

Proof.

A function is bent

$\Longrightarrow$ no zeroes outside of $\mathcal{V}$

$\Longrightarrow$ no vector spaces of zeroes other than $\mathcal{V}$

$\Longrightarrow$ only 1 EA-class

□

Permutations

We define

$$\mathcal{V}^{\perp} = \{(0, y), \forall y \in \mathbb{F}_2^m\} \subset \mathbb{F}_2^{n+m}.$$

Lemma

$F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is a permutation if and only if

$$\mathcal{V}^{\perp} \subset \mathcal{Z}_F .$$

EA-classes imply vector spaces

Lemma

*let F, G and G' be such that $\Gamma_G = L(\Gamma_F)$ and $\Gamma_{G'} = L'(\Gamma_F)$.
If $L(\mathcal{V}) = L'(\mathcal{V})$, then G and G' are EA-equivalent.*

EA-classes imply vector spaces

Lemma

let F, G and G' be such that $\Gamma_G = L(\Gamma_F)$ and $\Gamma_{G'} = L'(\Gamma_F)$.
If $L(\mathcal{V}) = L'(\mathcal{V})$, then G and G' are EA-equivalent.

Can we use this knowledge to partition a CCZ-class into its EA-classes?

EA-classes imply vector spaces

Lemma

*let F, G and G' be such that $\Gamma_G = L(\Gamma_F)$ and $\Gamma_{G'} = L'(\Gamma_F)$.
If $L(\mathcal{V}) = L'(\mathcal{V})$, then G and G' are EA-equivalent.*

Can we use this knowledge to partition a CCZ-class into its EA-classes?

The Lemma gives us hope!

1 EA-class $\implies$ 1 vector space of zeroes of dimension n in $\mathcal{Z}_n$

EA-classes imply vector spaces

Lemma

*let F, G and G' be such that $\Gamma_G = L(\Gamma_F)$ and $\Gamma_{G'} = L'(\Gamma_F)$.
If $L(\mathcal{V}) = L'(\mathcal{V})$, then G and G' are EA-equivalent.*

Can we use this knowledge to partition a CCZ-class into its EA-classes?

The Lemma gives us hope!

1 EA-class $\implies$ 1 vector space of zeroes of dimension n in $\mathcal{Z}_n$

Reality takes it back...

The converse of the lemma is wrong.

Counter-example

Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a permutation and let

$$M_n = \begin{bmatrix} 0 & I_n \\ I_n & 0 \end{bmatrix} .$$

It holds that

$$\begin{aligned} \Gamma_{F^{-1}} &= \{ (x, F(x)) , \forall x \in \mathbb{F}_2^n \} \\ &= \{ \left(F^{-1}(y), (F \circ F^{-1})(y)\right) , \forall y \in \mathbb{F}_2^n \} \\ &= \{ \left(F^{-1}(y), y\right) , \forall y \in \mathbb{F}_2^n \} \\ &= M_n(\Gamma_F) . \end{aligned}$$

Counter-example

Let $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$ be a permutation and let

$$M_n = \begin{bmatrix} 0 & I_n \\ I_n & 0 \end{bmatrix} .$$

It holds that

$$\begin{aligned}
\Gamma_{F^{-1}} &= \{ (x, F(x)) , \forall x \in \mathbb{F}_2^n \} \\
&= \{ \left(F^{-1}(y), (F \circ F^{-1})(y)\right) , \forall y \in \mathbb{F}_2^n \} \\
&= \{ \left(F^{-1}(y), y\right) , \forall y \in \mathbb{F}_2^n \} \\
&= M_n(\Gamma_F) .
\end{aligned}$$

The contradiction

If F is an involution then $\Gamma_F = \Gamma_{F^{-1}} = M_n(\Gamma_F)$

Counter-example

Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a permutation and let

$$M_n = \begin{bmatrix} 0 & I_n \\ I_n & 0 \end{bmatrix} .$$

It holds that

$$\begin{aligned} \Gamma_{F^{-1}} &= \left\{ (x, F(x)) , \forall x \in \mathbb{F}_2^n \right\} \\ &= \left\{ \left(F^{-1}(y), (F \circ F^{-1})(y)\right) , \forall y \in \mathbb{F}_2^n \right\} \\ &= \left\{ \left(F^{-1}(y), y\right) , \forall y \in \mathbb{F}_2^n \right\} \\ &= M_n(\Gamma_F) . \end{aligned}$$

The contradiction

If F is an involution then $\Gamma_F = \Gamma_{F^{-1}} = M_n(\Gamma_F)$

$\implies M_n(\mathcal{V}) = \mathcal{V}^\perp \neq I_n(\mathcal{V})$

Counter-example

Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a permutation and let

$$M_n = \begin{bmatrix} 0 & I_n \\ I_n & 0 \end{bmatrix} .$$

It holds that

$$\begin{aligned}
\Gamma_{F^{-1}} &= \left\{ (x, F(x)) , \forall x \in \mathbb{F}_2^n \right\} \\
&= \left\{ \left(F^{-1}(y), (F \circ F^{-1})(y)\right) , \forall y \in \mathbb{F}_2^n \right\} \\
&= \left\{ \left(F^{-1}(y), y\right) , \forall y \in \mathbb{F}_2^n \right\} \\
&= M_n(\Gamma_F) .
\end{aligned}$$

The contradiction

If F is an involution then $\Gamma_F = \Gamma_{F^{-1}} = M_n(\Gamma_F)$

$\Longrightarrow$ $M_n(\mathcal{V}) = \mathcal{V}^\perp \neq I_n(\mathcal{V})$

... but M_n and I_n send Γ_F in the same EA-class (namely that of F).

Making the converse work (1/2)

Definition (CCZ-invariants)

The CCZ-invariants of $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$ are the affine permutations L of $\mathbb{F}_2^{n+n}$ such that

$$L(\Gamma_F) = \Gamma_F .$$

Making the converse work (1/2)

Definition (CCZ-invariants)

The CCZ-invariants of $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ are the affine permutations L of $\mathbb{F}_2^{n+n}$ such that

$$L(\Gamma_F) = \Gamma_F .$$

Examples

- For an involution, M_n is a CCZ-invariant.
- For a quadratic function q, there are CCZ-invariants with the following linear parts:

$$\begin{bmatrix} I_n & 0 \\ \Delta_\alpha q & I_n \end{bmatrix} .$$

Making the converse work (2/2)

Theorem (Number of EA-classes)

For $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m$, *let:*

- s_F *be the number of vector spaces of dimension* n *in* $\mathcal{Z}_F$
- c_F *be the number of CCZ-invariants of* F
- e_F *be the number of EA-classes in the CCZ-class of* F.

Making the converse work (2/2)

Theorem (Number of EA-classes)

For $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m$, let:

- *s_F be the number of vector spaces of dimension n in $\mathcal{Z}_F$*
- *c_F be the number of CCZ-invariants of F*
- *e_F be the number of EA-classes in the CCZ-class of F.*

Then

$$\frac{s_F}{c_F} \leq e_F \leq s_F .$$

Making the converse work (2/2)

Theorem (Number of EA-classes)

For $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m$, let:

- *s_F be the number of vector spaces of dimension n in $\mathcal{Z}_F$*
- *c_F be the number of CCZ-invariants of F*
- *e_F be the number of EA-classes in the CCZ-class of F.*

Then

$$\frac{s_F}{c_F} \leq e_F \leq s_F \ .$$

Corollary

If $c_F = 1$, then we do have a bijection between EA-classes and vector spaces of 0 of dimension n in $\mathcal{Z}_F$.

Outline

Plan of this Section

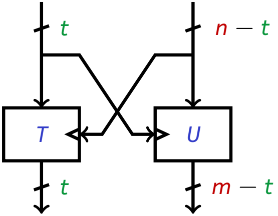
EA-equivalence is a simple sub-case of CCZ-Equivalence...

EA-equivalence is a simple sub-case of CCZ-Equivalence...

What must we add to EA-equivalence to fully describe CCZ-Equivalence?

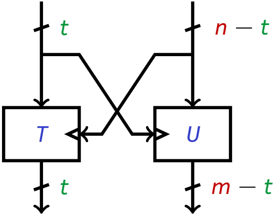
Definition of the Twist

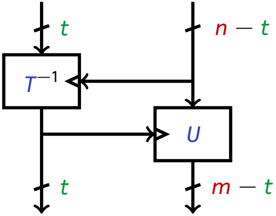
Any function $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m$ can be projected on $\mathbb{F}_2^t \times \mathbb{F}_2^{m-t}$.



Definition of the Twist

Any function $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m$ can be projected on $\mathbb{F}_2^t \times \mathbb{F}_2^{m-t}$.





If T is a permutation for all secondary inputs, then we define the t-twist equivalent of F as G, where

$$G(x, y) = \left(T_y^{-1}(x), U_{T_y^{-1}(x)}(y)\right)$$

for all $(x, y) \in \mathbb{F}_2^t \times \mathbb{F}_2^{n-t}$.

Examples of Twisting

- Inversion is an n-twist.

Examples of Twisting

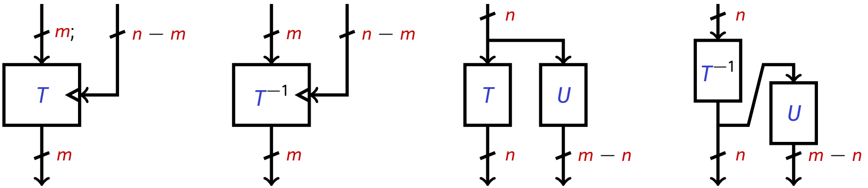
- Inversion is an n-twist.
- Open and closed butterflies operating on n bits are obtained from another with an $(n/2)$-twist.

Examples of Twisting

- Inversion is an n-twist.
- Open and closed butterflies operating on n bits are obtained from another with an $(n/2)$-twist.
- Some degenerate cases exist for $t = m$ and $n = n$.

Examples of Twisting

- Inversion is an n-twist.
- Open and closed butterflies operating on n bits are obtained from another with an $(n/2)$-twist.
- Some degenerate cases exist for $t = m$ and $n = n$.



$t = m$ (start) $t = m$ (end) $t = n$ (start) $t = n$ (end)

Swap Matrices

The swap matrix permuting $\mathbb{F}_2^{n+m}$ is defined for $t \leq \min(n, m)$ as

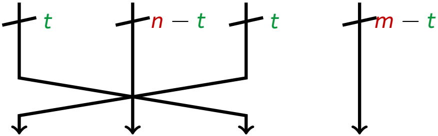
$$M_t = \begin{bmatrix} 0 & 0 & I_t & 0 \\ 0 & I_{n-t} & 0 & 0 \\ I_t & 0 & 0 & 0 \\ 0 & 0 & 0 & I_{m-t} \end{bmatrix} .$$

Swap Matrices

The swap matrix permuting $\mathbb{F}_2^{n+m}$ is defined for $t \leq \min(n, m)$ as

$$M_t = \begin{bmatrix} 0 & 0 & I_t & 0 \\ 0 & I_{n-t} & 0 & 0 \\ I_t & 0 & 0 & 0 \\ 0 & 0 & 0 & I_{m-t} \end{bmatrix} .$$

It has a simple interpretation:

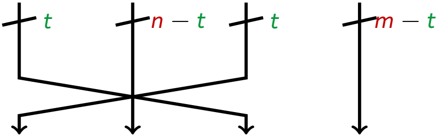


Swap Matrices

The swap matrix permuting $\mathbb{F}_2^{n+m}$ is defined for $t \leq \min(n, m)$ as

$$M_t = \begin{bmatrix} 0 & 0 & I_t & 0 \\ 0 & I_{n-t} & 0 & 0 \\ I_t & 0 & 0 & 0 \\ 0 & 0 & 0 & I_{m-t} \end{bmatrix} .$$

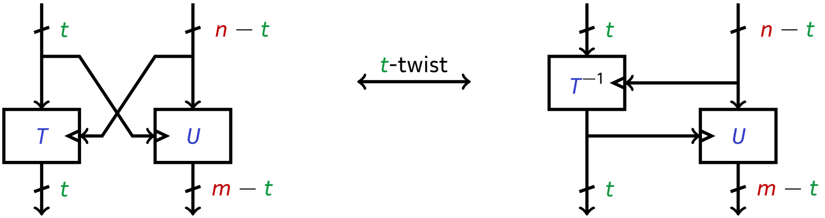
It has a simple interpretation:



For all $t \leq \min(n, m)$, M_t is an **orthogonal** and **symmetric involution**.

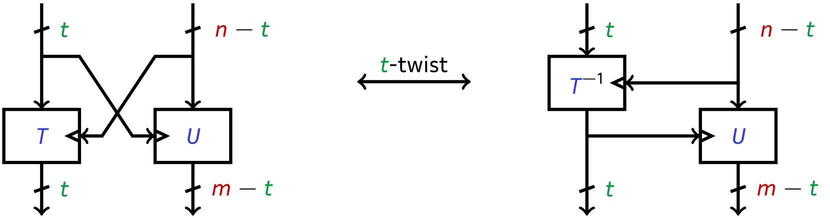
Swap Matrices and Twisting

$\mathbf{F} : \mathbb{F}_2^n \to \mathbb{F}_2^m$ $\qquad$ $\mathbf{G} : \mathbb{F}_2^n \to \mathbb{F}_2^m$



Swap Matrices and Twisting

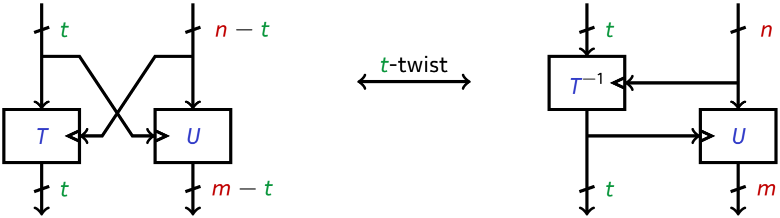
$F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ $\quad$ $G : \mathbb{F}_2^n \to \mathbb{F}_2^m$



$$\Gamma_F = \{ (x, F(x)), \forall x \in \mathbb{F}_2^n \} \quad \overset{M_t}{\longleftrightarrow} \quad \Gamma_G = \{ (x, G(x)), \forall x \in \mathbb{F}_2^n \}$$

Swap Matrices and Twisting

$\mathbf{F} : \mathbb{F}_2^n \to \mathbb{F}_2^m$ $\quad\quad$ $\mathbf{G} : \mathbb{F}_2^n \to \mathbb{F}_2^m$



$$\Gamma_F = \left\{ (x, F(x)), \forall x \in \mathbb{F}_2^n \right\} \quad \xleftrightarrow{M_t} \quad \Gamma_G = \left\{ (x, G(x)), \forall x \in \mathbb{F}_2^n \right\}$$

$$\mathcal{W}_F(u) = \mathcal{W}_G(M_t(u))$$

Twisting and CCZ-Class

Lemma

Twisting preserves the CCZ-equivalence class.

Twisting and CCZ-Class

Lemma

Twisting preserves the CCZ-equivalence class.

Main Result

Theorem

If $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ and $G : \mathbb{F}_2^n \to \mathbb{F}_2^m$ are CCZ-equivalent, then

$$\Gamma_G = (B \times M_t \times A)(\Gamma_F) ,$$

where A and B are EA-mappings and where

$$t = \dim \left(proj_{\mathcal{V}^\perp} \left((A^T \times M_t \times B^T)(\mathcal{V}) \right) \right) .$$

In other words, EA-equivalence and twists are sufficient to fully describe CCZ-equivalence!

Main Result

Theorem

If $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m$ and $G : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m$ are CCZ-equivalent, then

$$\Gamma_G = (B \times M_t \times A)(\Gamma_F) ,$$

where A and B are EA-mappings and where

$$t = \dim \left(proj_{\mathcal{V}^\perp} \left((A^T \times M_t \times B^T)(\mathcal{V}) \right) \right) .$$

In other words, EA-equivalence and twists are sufficient to fully describe CCZ-equivalence!

Corollary

If a function is CCZ-equivalent but not EA-equivalent to another function, then they have to be EA-equivalent to functions for which a t-twist is possible.

Proof sketch

1. As F is CCZ-equivalent to G, there is a linear permutation $L : \mathbb{F}_2^{n+m} \rightarrow \mathbb{F}_2^{n+m}$ such that
$$\Gamma_G = L(\Gamma_F) \text{ and } L^T(\mathcal{V}) \subset \mathcal{Z}_F \ .$$

Proof sketch

1. As F is CCZ-equivalent to G, there is a linear permutation $L : \mathbb{F}_2^{n+m} \rightarrow \mathbb{F}_2^{n+m}$ such that
$$\Gamma_G = L(\Gamma_F) \text{ and } L^T(\mathcal{V}) \subset \mathcal{Z}_F \ .$$
2. Any vector space V of dimension n such that $\dim(\text{proj}_{\mathcal{V}^\perp}(V)) = t$ can be written as
$$V \ = \ (A^T \times M_t)(\mathcal{V}) \ ,$$
where A is an EA-mapping.

Proof sketch

1. As F is CCZ-equivalent to G, there is a linear permutation $L : \mathbb{F}_2^{n+m} \to \mathbb{F}_2^{n+m}$ such that
$$\Gamma_G = L(\Gamma_F) \text{ and } L^T(\mathcal{V}) \subset \mathcal{Z}_F \ .$$
2. Any vector space V of dimension n such that $\dim(\text{proj}_{\mathcal{V}^\perp}(V)) = t$ can be written as
$$V = (A^T \times M_t)(\mathcal{V}) \ ,$$
where A is an EA-mapping.

1+2. We deduce that $L^T(\mathcal{V}) = (A^T \times M_t)(\mathcal{V}) \subset \mathcal{Z}_F$.

Proof sketch

1. As F is CCZ-equivalent to G, there is a linear permutation $L : \mathbb{F}_2^{n+m} \to \mathbb{F}_2^{n+m}$ such that
$$\Gamma_G = L(\Gamma_F) \text{ and } L^T(\mathcal{V}) \subset \mathcal{Z}_F .$$
2. Any vector space V of dimension n such that $\dim(\text{proj}_{\mathcal{V}^\perp}(V)) = t$ can be written as
$$V = (A^T \times M_t)(\mathcal{V}) ,$$
where A is an EA-mapping.

1+2. We deduce that $L^T(\mathcal{V}) = (A^T \times M_t)(\mathcal{V}) \subset \mathcal{Z}_F$.

1+2+lem. As $L^T(\mathcal{V}) = (A^T \times M_t)(\mathcal{V})$, the functions G and G' such that $\Gamma_G = L(\Gamma_F)$ and $\Gamma_{G'} = (A^T \times M_t)(\Gamma_F)$ are EA-equivalent.
We conclude that
$$\Gamma_G = (B \times M_t \times A)(\Gamma_F) .$$

Usage?

What can we do with this knowledge?

Boolean Functions

Theorem (Budaghyan, Carlet (2011))

The CCZ-class of $F : \mathbb{F}_2^n \to \mathbb{F}_2$ *is limited to its EA-class.*

Boolean Functions

Theorem (Budaghyan, Carlet (2011))

The CCZ-class of $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$ is limited to its EA-class.

Proof.

F is CCZ- but not EA-equivalent to some G

Boolean Functions

Theorem (Budaghyan, Carlet (2011))

The CCZ-class of $F : \mathbb{F}_2^n \to \mathbb{F}_2$ is limited to its EA-class.

Proof.

F is CCZ- but not EA-equivalent to some G

$\Longrightarrow$ $F(x||y) = T_y(x), \forall (x,y) \in \mathbb{F}_2 \times \mathbb{F}_2^{n-1}$, where T_y is always a permutation of $\mathbb{F}_2$

Boolean Functions

Theorem (Budaghyan, Carlet (2011))

The CCZ-class of $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$ is limited to its EA-class.

Proof.

F is CCZ- but not EA-equivalent to some G

$\Longrightarrow$ $F(x||y) = T_y(x), \forall (x, y) \in \mathbb{F}_2 \times \mathbb{F}_2^{n-1}$, where T_y is always a permutation of $\mathbb{F}_2$

$\Longrightarrow$ $F(x||y) = x \oplus f(y), \forall (x, y) \in \mathbb{F}_2 \times \mathbb{F}_2^{n-1}$,

$\Longrightarrow$ 1-twisting F does not change the EA-class

$\Longrightarrow$ it is impossible to leave the EA-class of F

□

Modular Addition (1/2)

Theorem (Schulte-Geers'13)

Addition modulo 2^m *is CCZ-equivalent to*

$$q(x,y) = (0, x_0y_0, x_0y_0 + x_1y_1, ..., x_0y_0 + ... + x_{n2}y_{n2}) ,$$

where $\Gamma_{\boxplus} = L(\Gamma_q)$ *with*

$$L = \begin{bmatrix} I_m & 0 & I_m \\ 0 & I_m & I_m \\ I_m & I_m & I_m \end{bmatrix} .$$

Modular Addition (1/2)

Theorem (Schulte-Geers'13)

Addition modulo 2^m is CCZ-equivalent to

$$q(x,y) = (0, x_0 y_0, x_0 y_0 + x_1 y_1, \ldots, x_0 y_0 + \ldots + x_{n2} y_{n2}) ,$$

where $\Gamma_{\boxplus} = L(\Gamma_q)$ with

$$L = \begin{bmatrix} I_m & 0 & I_m \\ 0 & I_m & I_m \\ I_m & I_m & I_m \end{bmatrix} .$$

It holds that

$$L^{-1} = \underbrace{\begin{bmatrix} I_m & 0 & 0 \\ I_m & I_m & 0 \\ I_m & 0 & I_m \end{bmatrix}}_{A_1} \times \underbrace{\begin{bmatrix} 0 & 0 & I_m \\ 0 & I_m & 0 \\ I_m & 0 & 0 \end{bmatrix}}_{M_m} \times \underbrace{\begin{bmatrix} I_m & 0 & 0 \\ I_m & I_m & 0 \\ 0 & I_m & I_m \end{bmatrix}}_{A_2} .$$

Modular Addition (2/2)

Lemma

Let $T_z^{\boxplus} : \mathbb{F}_2^m \to \mathbb{F}_2^m$ *be defined by*

$$T_z^{\boxplus}(x) = \left(x \boxplus (x \oplus z)\right) \oplus (x \oplus z) .$$

Modular Addition (2/2)

Lemma

Let $T_z^{\boxplus} : \mathbb{F}_2^m \to \mathbb{F}_2^m$ *be defined by*

$$T_z^{\boxplus}(x) = \big(x \boxplus (x \oplus z)\big) \oplus (x \oplus z)\,.$$

- $T_z^{\boxplus}$ *is a permutation for all* z*;*
- *it is EA-equivalent to* $(x, y) \mapsto x \boxplus y$*;*

Modular Addition (2/2)

Lemma

Let $T_z^{\boxplus} : \mathbb{F}_2^m \to \mathbb{F}_2^m$ *be defined by*

$$T_z^{\boxplus}(x) = \left(x \boxplus (x \oplus z)\right) \oplus (x \oplus z) \,.$$

- $T_z^{\boxplus}$ *is a permutation for all* z*;*
- *it is EA-equivalent to* $(x, y) \mapsto x \boxplus y$*;*
- $(x, z) \mapsto T_z^{\boxplus}(x)$ *has algebraic degree* m*;*
- $(x, z) \mapsto (T_z^{\boxplus})^{-1}(x)$ ***is quadratic!***

Modular Addition (2/2)

Lemma

Let $T_z^{\boxplus} : \mathbb{F}_2^m \to \mathbb{F}_2^m$ be defined by

$$T_z^{\boxplus}(x) = \big(x \boxplus (x \oplus z)\big) \oplus (x \oplus z) .$$

- *$T_z^{\boxplus}$ is a permutation for all z;*
- *it is EA-equivalent to $(x, y) \mapsto x \boxplus y$;*
- *$(x, z) \mapsto T_z^{\boxplus}(x)$ has algebraic degree m;*
- *$(x, z) \mapsto (T_z^{\boxplus})^{-1}(x)$* ***is quadratic!***

Let $v = T_z^{\boxplus}(x)$. Then:

$$\begin{cases} v_0 & = x_0 \\ v_{i+1} & = x_i + x_{i+1} + v_i z_i \end{cases} \text{and, convertly,} \begin{cases} x_0 & = v_0 \\ x_{i+1} & = x_i + v_{i+1} + v_i z_i \end{cases} .$$

Outline

Plan of this Section

Another Problem

How do we know if a function is CCZ-equivalent to a permutation?

Remainder

Recall that F is a permutation if and only if $\mathcal{V} \subset \mathcal{Z}_F$ and $\mathcal{V}^{\perp} \subset \mathcal{Z}_F$.

Remainder

Recall that F is a permutation if and only if $\mathcal{V} \subset \mathcal{Z}_F$ and $\mathcal{V}^{\perp} \subset \mathcal{Z}_F$.

Lemma

G is CCZ-equivalent to a permutation if and only if

$$V = L(\mathcal{V}) \subset \mathcal{Z}_G \text{ and } V' = L(\mathcal{V}^{\perp}) \subset \mathcal{Z}_G$$

for some linear permutation L. Note that

$$span\left(V \cup V'\right) = \mathbb{F}_2^n \times \mathbb{F}_2^m .$$

3-Spaces Criteria

3-space criteria

Let $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m$, not be a permutation. If it is CCZ-equivalent to a permutation then $\mathcal{Z}_F$ must contain at least 3 vector spaces of zeroes of dimension n.

Projected Spaces Criteria

Key observation

The projections

$$p : (x, y) \mapsto x \text{ and } p' : (x, y) \mapsto y$$

mapping $\mathbb{F}_2^n \times \mathbb{F}_2^m$ to $\mathbb{F}_2^n$ and $\mathbb{F}_2^m$ respectively are **linear**.

Projected Spaces Criteria

Key observation

The projections

$$p : (x, y) \mapsto x \text{ and } p' : (x, y) \mapsto y$$

mapping $\mathbb{F}_2^n \times \mathbb{F}_2^m$ to $\mathbb{F}_2^n$ and $\mathbb{F}_2^m$ respectively are **linear**.

Thus, If G is CCZ-equivalent to a permutation then $p(V)$ and $p(V')$ are subspaces of $\mathbb{F}_2^n$ whose span is $\mathbb{F}_2^n$.

Projected Spaces Criteria

Key observation

The projections

$$p : (x, y) \mapsto x \text{ and } p' : (x, y) \mapsto y$$

mapping $\mathbb{F}_2^n \times \mathbb{F}_2^m$ to $\mathbb{F}_2^n$ and $\mathbb{F}_2^m$ respectively are **linear**.

Thus, If G is CCZ-equivalent to a permutation then $p(V)$ and $p(V')$ are subspaces of $\mathbb{F}_2^n$ whose span is $\mathbb{F}_2^n$.

We deduce that $\dim(p(V)) + \dim(p(V')) \geq n$

Projected Spaces Criteria

Key observation

The projections

$$p : (x, y) \mapsto x \text{ and } p' : (x, y) \mapsto y$$

mapping $\mathbb{F}_2^n \times \mathbb{F}_2^m$ to $\mathbb{F}_2^n$ and $\mathbb{F}_2^m$ respectively are **linear**.

Thus, If G is CCZ-equivalent to a permutation then $p(V)$ and $p(V')$ are subspaces of $\mathbb{F}_2^n$ whose span is $\mathbb{F}_2^n$.

We deduce that $\dim(p(V)) + \dim(p(V')) \geq n$

Projected Spaces Criteria

If $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is CCZ-equivalent to a permutation, then there are at least two subspaces of dimension $n/2$ in $p(\mathcal{Z}_F)$ and in $p'(\mathcal{Z}_F)$.

QAM

Yu et al. (DCC'14) generated 8180 8-APN quadratic functions from "*QAM*" (matrices).

QAM

Yu et al. (DCC'14) generated 8180 8-APN quadratic functions from "*QAM*" (matrices).

None of them are CCZ-equivalent to a permutation

Göloğlu's Candidates (1/2)

Göloğlu's introduced APN functions

$$f_k : x \mapsto x^{2^k+1} + \left(x + x^{2^{n/2}}\right)^{2^k+1}$$

for $n = 4t$. They have the *subspace property* of the Kim mapping.

Göloğlu's Candidates (1/2)

Göloğlu's introduced APN functions

$$f_k : x \mapsto x^{2^k+1} + (x + x^{2^{n/2}})^{2^k+1}$$

for $n = 4t$. They have the *subspace property* of the Kim mapping.

> *Unfortunately, f_k are not equivalent to permutations on $n = 4, 8$ and does not* ***seem*** *to be equivalent to one on $n = 12$ (we say "it does not seem to be equivalent to a permutation" since checking the existence of CCZ-equivalent permutations* ***requires huge amount of computing*** *and is infeasible on $n = 12$; our program was still running at the time of writing).*

Göloğlu's Candidates (2/2)

n	cardinal proj.	time proj. (s)	time `BasesExtraction` (s)
12	1365	0.066	0.0012
16	21845	16.79	0.084
20	349525	10096.00	37.48

Time needed to show that f_k is **not** CCZ-equivalent to a permutation.

Outline

Plan of this Section

Conclusion

- CCZ $=$ EA $+$ Twist, both of which have a simple interpretation.

Conclusion

- CCZ $=$ EA $+$ Twist, both of which have a simple interpretation.
- Efficient criteria to know if a function is CCZ-equivalent to a permutation...
- ... implemented using a very efficient vector space extraction algorithm (not presented)

The Fourier transform solves everything!

Open Problems

EA-equivalence

How can we efficiently check the EA-equivalence of two functions?

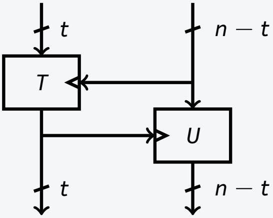
Open Problems

EA-equivalence

How can we efficiently check the EA-equivalence of two functions?

Conjecture

If the CCZ-class of a permutation P is not reduced to the EA-classes of P and P^{-1}, then P has the following decomposition



where both T and U are keyed permutations.