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

Anne Canteaut, Léo Perrin

June 3, 2019
Fq14, Vancouver

Inria informatics mathematics

Setting up the background

Cryptographic properties $\rightarrow$ Equivalence classes $\rightarrow$ CCZ-equivalence

Cryptographic Properties

$F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ and $G : \mathbb{F}_2^n \to \mathbb{F}_2^m$ are functions (e.g. S-Boxes).

Definition (DDT/LAT)

The D(ifference) D(istribution) T(able) of $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is

$$\mathcal{D}_F(\alpha, \beta) \; = \; \# \{x, F(x \oplus \alpha) \oplus F(x) = \beta\}$$

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

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

Cryptographic Properties

$F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ and $G : \mathbb{F}_2^n \to \mathbb{F}_2^m$ are functions (e.g. S-Boxes).

Definition (DDT/LAT)

The D(ifference) D(istribution) T(able) of $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is

$$\mathcal{D}_F(\alpha, \beta) \ = \ \# \{x, F(x \oplus \alpha) \oplus F(x) = \beta\}$$

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

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

Big APN Problem

Is there an APN permutation on $2t$ bits such that $\max(\mathrm{DDT}) = 2$?

Equivalence Relations that $\approx$ Preserve DDT/LAT (1/2)

Definition (Affine-Equivalence)

F and G are *affine equivalent* if $G(x) = (B \circ F \circ A)(x)$, where A, B are affine permutations.

Equivalence Relations that $\approx$ Preserve DDT/LAT (1/2)

Definition (Affine-Equivalence)

F and G are *affine equivalent* if $G(x) = (B \circ F \circ A)(x)$, where A, B are affine permutations.

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

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

Equivalence Relations that ≈ Preserve DDT/LAT (1/2)

Definition (Affine-Equivalence)

F and G are *affine equivalent* if $G(x) = (B \circ F \circ A)(x)$, where A, B are affine permutations.

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**

Equivalence Relations that $\approx$ Preserve DDT/LAT (2/2)

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.

Equivalence Relations that $\approx$ Preserve DDT/LAT (2/2)

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.

CCZ-equivalence plays a crucial role in the investigation of the big APN problem.

Equivalence Relations that ≈ Preserve DDT/LAT (2/2)

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.

CCZ-equivalence plays a crucial role in the investigation of the big APN problem.

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

The Problem with CCZ-Equivalence

Admissible Mapping

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

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

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

The Problem with CCZ-Equivalence

Admissible Mapping

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

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

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

How can we list all admissible mappings for F?

Structure of this talk

1. CCZ-Equivalence and Vector Spaces of 0
2. Function Twisting
3. Necessary and Efficient Conditions for CCZ-Equivalence to a Permutation
4. Conclusion

Outline

Plan of this Section

Walsh Zeroes

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

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

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

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

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

Admissibility of EA-mappings

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

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

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 $L^T(\mathcal{V}) = L'^T(\mathcal{V})$, 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 $L^T(\mathcal{V}) = L'^T(\mathcal{V})$, 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 $L^T(\mathcal{V}) = L'^T(\mathcal{V})$, 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 $L^T(\mathcal{V}) = L'^T(\mathcal{V})$, 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.

Outline

Plan of this Section

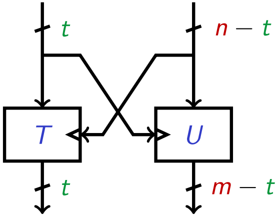
EA-equivalence is a simple sub-case of CCZ-Equivalence...

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

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

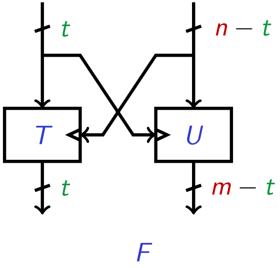
Definition of the Twist

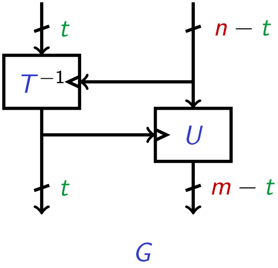
Any function $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ can be projected on $\mathbb{F}_2^t \times \mathbb{F}_2^{m-t}$:
$F(x, y) = \big(T_y(x), U_x(y)\big)$



Definition of the Twist

Any function $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ can be projected on $\mathbb{F}_2^t \times \mathbb{F}_2^{m-t}$:
$F(x, y) = \big(T_y(x), U_x(y)\big)$



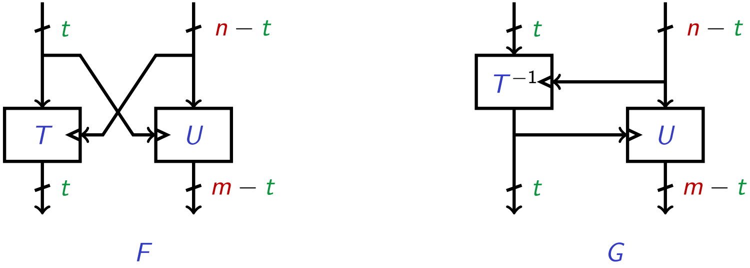


If T_y is a permutation for all y, then we define the t-twist equivalent of F as G such that, for all $(x, y) \in \mathbb{F}_2^t \times \mathbb{F}_2^{n-t}$:

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

Definition of the Twist

Any function $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ can be projected on $\mathbb{F}_2^t \times \mathbb{F}_2^{m-t}$:
$F(x, y) = \big(T_y(x), U_x(y)\big)$



If T_y is a permutation for all y, then we define the t-twist equivalent of F as G such that, for all $(x, y) \in \mathbb{F}_2^t \times \mathbb{F}_2^{n-t}$:

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

The identiy is a 0-twist, functional inversion is an n-twist.

Swap Matrices

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

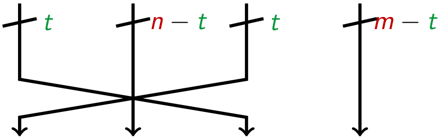
$$M_t = \begin{bmatrix} 0 & 0 & I_t & 0 \\ 0 & I_{n-t} & 0 & 0 \\ I_t & 0 & 0 & 0 \\ 0 & 0 & 0 & I_{m-t} \end{bmatrix} .$$

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:

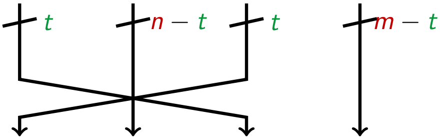


Swap Matrices

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

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

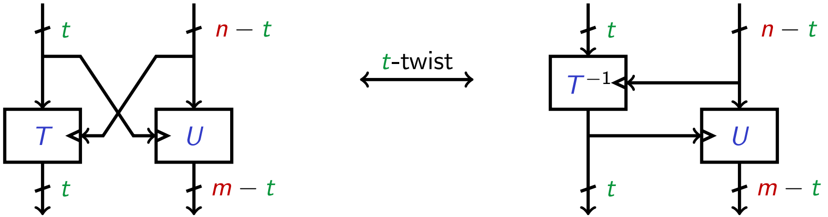
It has a simple interpretation:



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

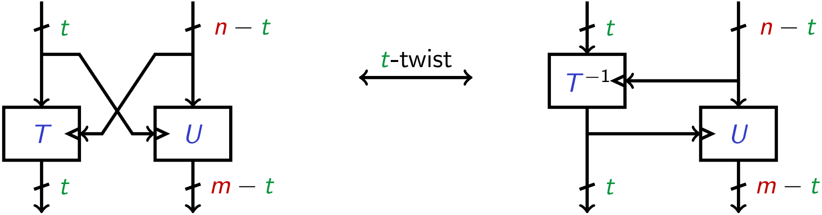
Swap Matrices and Twisting

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



Swap Matrices and Twisting

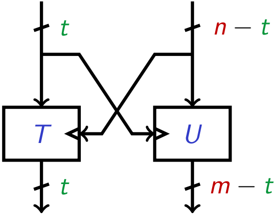
$\mathbf{F} : \mathbb{F}_2^{\mathbf{n}} \rightarrow \mathbb{F}_2^{\mathbf{m}}$ $\qquad$ $\mathbf{G} : \mathbb{F}_2^{\mathbf{n}} \rightarrow \mathbb{F}_2^{\mathbf{m}}$



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

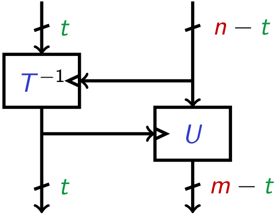
Swap Matrices and Twisting

$\mathbf{F} : \mathbb{F}_2^{\mathbf{n}} \rightarrow \mathbb{F}_2^{\mathbf{m}}$



t-twist ⟷

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



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

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

Twisting and CCZ-Class

Lemma

Twisting preserves the CCZ-equivalence class.

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!

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!

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.

Outline

Plan of this Section

Another Problem

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

Reminder

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

Reminder

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

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

Projected Spaces Criterion

Key observation

The projections

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

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 Criterion

Key observation

The projections

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

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 Criterion

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 Criterion

Key observation

The projections

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

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 Criterion

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

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

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)

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)
- It also explains why Dillon et al.'s technique for finding a 6-bit APN permutation yielded a butterfly!

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)
- It also explains why Dillon et al.'s technique for finding a 6-bit APN permutation yielded a butterfly!

The Fourier transform solves everything!

Open Problems

EA-equivalence

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

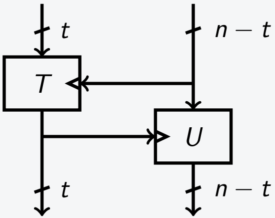
Open Problems

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.