Algebraic properties of symmetric ciphers and of their non-linear components

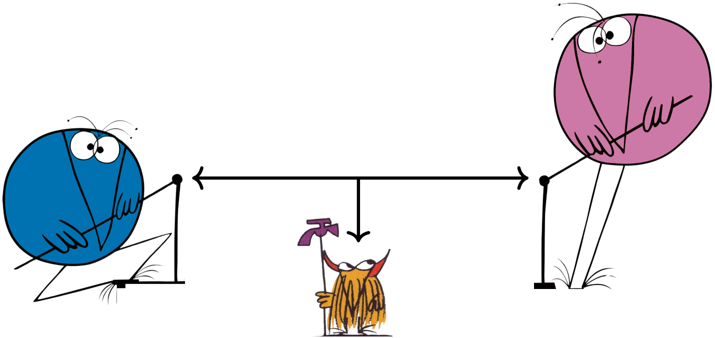
Jules Baudrin

PhD defense

December 6th, 2024

Assumption

Common secret shared beforehand.



A, E, $\varnothing$ B,

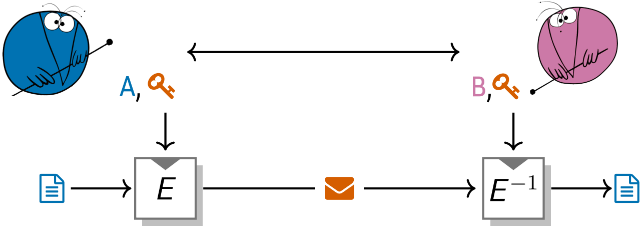
Goal

Ensure *confidentiality* and/or authenticity and/or integrity

Symmetric encryption

Goal

Ensure confidentiality



Constraints

- Secure
- Easily implemented
- Arbitrary-long messages

Primitives

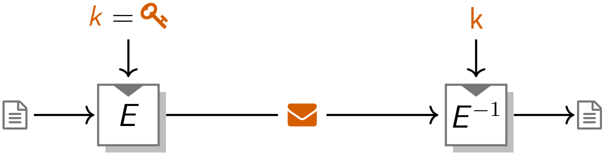
Definition (Primitive)

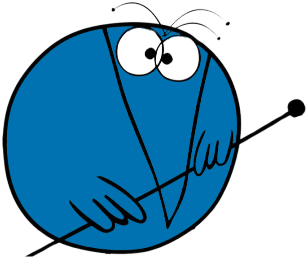
Low-level algorithm for ***very specific*** tasks

Example (Block cipher)

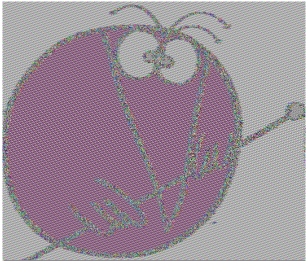
Encrypts ***fixed-size*** messages

$\rightsquigarrow$ A block cipher $\mathcal{E}$ is a family of bijections $\mathcal{E} = \left(E_k : \mathbb{F}_2^n \xrightarrow{\sim} \mathbb{F}_2^n\right)_{k \in \mathbb{F}_2^\kappa}$.





Each pixel is encrypted independently



Definition (Mode of operation)

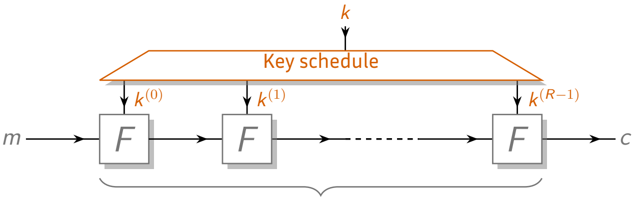
High-level algorithm *based on primitives* to provide *e.g.* confidentiality

Building a block cipher

Recap (Block cipher)

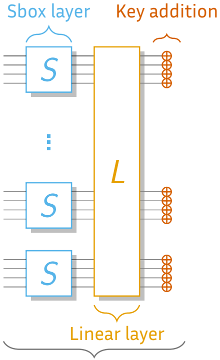
A family of bijections $\mathcal{E} = \left(E_k : \mathbb{F}_2^n \xrightarrow{\sim} \mathbb{F}_2^n\right)_{k \in \mathbb{F}_2^\kappa}$. Should be *efficient* and *secure*.

Iterated construction



$$E_k = F_{k^{(R-1)}} \circ \cdots \circ F_{k^{(1)}} \circ F_{k^{(0)}}$$

Substitution Permutation Network

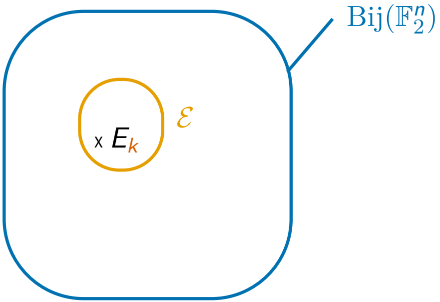


$$F_{k^{(i)}} = T_{k^{(i)}} \circ L \circ S$$

Recap (Block cipher)

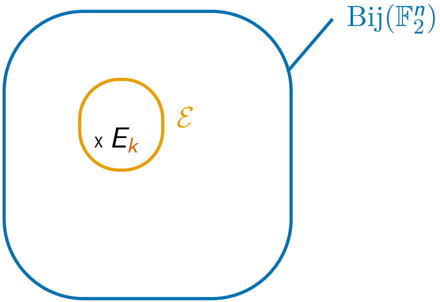
A family of bijections $\mathcal{E} = \left(E_k : \mathbb{F}_2^n \xrightarrow{\sim} \mathbb{F}_2^n\right)_{k \in \mathbb{F}_2^\kappa}$.

Should be *efficient* and *secure*.



Recap (Block cipher)

A family of bijections $\mathcal{E} = \left(E_k : \mathbb{F}_2^n \xrightarrow{\sim} \mathbb{F}_2^n\right)_{k \in \mathbb{F}_2^\kappa}$. Should be *efficient* and *secure*.



Definition (Indistinguishability)

$[\, E \xleftarrow{\$} \mathcal{E} \,]$ ***indistinguishable*** from $[\, F \xleftarrow{\$} \mathrm{Bij}(\mathbb{F}_2^n) \,]$.

Contributions

Cryptanalysis

- Higher-order differential attack against Ascon [B, Canteaut & Perrin, ToSC 2022]
- Commutative distinguishers for variants of Midori
  [B, Felke, Leander, Neumann, Perrin & Stennes, ToSC 2023]
- Links between commutative and differential cryptanalyses
  [B, Beierle, Felke, Leander, Neumann, Perrin & Stennes, submitted (2024)]

Optimal building blocks

- Links between linear self-equivalence and APN functions
  [B, Canteaut & Perrin, submitted (2024)]

Design

- Universal hash functions and MACs based on AES
  [Bariant, B, Leurent, Pernot, Perrin & Peyrin, ToSC 2024]
- Stream cipher over $\mathbb{F}_{17}$ for transciphering with TFHE
  [B, Belaïd, Bon, Boura, Canteaut, Leurent, Paillier, Perrin, Rivain, Rotella & Tap, submitted (2024)]

Contributions

Cryptanalysis

- Higher-order differential attack against Ascon [B, Canteaut & Perrin, ToSC 2022]
- Commutative distinguishers for variants of Midori

  [B, Felke, Leander, Neumann, Perrin & Stennes, ToSC 2023]
- Links between commutative and differential cryptanalyses

  [B, Beierle, Felke, Leander, Neumann, Perrin & Stennes, submitted (2024)]

Optimal building blocks

- Links between linear self-equivalence and APN functions

  [B, Canteaut & Perrin, submitted (2024)]

Design

- Universal hash functions and MACs based on AES

  [Bariant, B, Leurent, Pernot, Perrin & Peyrin, ToSC 2024]
- Stream cipher over $\mathbb{F}_{17}$ for transciphering in TFHE

  [B, Belaïd, Bon, Boura, Canteaut, Leurent, Paillier, Perrin, Rivain, Rotella & Tap, submitted (2024)]

Outline

I - Introduction

II - Differential cryptanalysis

III - Differential cryptanalysis of conjugate ciphers

[B, Felke, Leander, Neumann, Perrin & Stennes, ToSC 2023]

[B, Beierle, Felke, Leander, Neumann, Perrin & Stennes, submitted (2024)]

IV - Linear self-equivalences of APN functions

[B, Canteaut & Perrin, submitted (2024)]

II - Differential cryptanalysis

Recap

$\mathcal{E} = \left(E_k : \mathbb{F}_2^n \xrightarrow{\sim} \mathbb{F}_2^n\right)_{k \in \mathbb{F}_2^\kappa}$. $\quad [\, E \xleftarrow{\$} \mathcal{E} \,]$ or $[\, F \xleftarrow{\$} \mathrm{Bij}(\mathbb{F}_2^n) \,]$?

The difference Δ^{out} between two ciphertexts ***should be uniformly distributed***, even when the difference Δ^{in} between plaintexts is chosen.

$$\begin{array}{ccc} x & & E_k(x) \\ \updownarrow \Delta^{\mathrm{in}} & & \updownarrow \Delta^{\mathrm{out}} \\ y & & E_k(y) \end{array}$$

Recap

$\mathcal{E} = \left(E_k : \mathbb{F}_2^n \xrightarrow{\sim} \mathbb{F}_2^n\right)_{k \in \mathbb{F}_2^\kappa}$. $[\, E \xleftarrow{\$} \mathcal{E} \,]$ or $[\, F \xleftarrow{\$} \mathrm{Bij}(\mathbb{F}_2^n) \,]$?

The difference Δ^{out} between two ciphertexts ***should be uniformly distributed***, even when the difference Δ^{in} between plaintexts is chosen.

$$
\begin{array}{ccc}
x & & E_k(x) \\
\updownarrow \Delta^{\text{in}} & & \updownarrow \Delta^{\text{out}} \\
y & & E_k(y)
\end{array}
$$

For a random bijection F

$F(x + \Delta^{\text{in}}) + F(x) = \Delta^{\text{out}}$ has 1 solution x on average.

Recap

$\mathcal{E} = \left(E_k : \mathbb{F}_2^n \xrightarrow{\sim} \mathbb{F}_2^n\right)_{k \in \mathbb{F}_2^\kappa}$. $\qquad [\, E \xleftarrow{\$} \mathcal{E} \,]$ or $[\, F \xleftarrow{\$} \mathrm{Bij}(\mathbb{F}_2^n) \,]$?

The difference Δ^{out} between two ciphertexts ***should be uniformly distributed***, even when the difference Δ^{in} between plaintexts is chosen.

$$x \; \updownarrow \Delta^{\mathrm{in}} \; y \qquad\qquad E_k(x) \; \updownarrow \Delta^{\mathrm{out}} \; E_k(y)$$

For a random bijection F

$F(x + \Delta^{\mathrm{in}}) + F(x) = \Delta^{\mathrm{out}}$ has 1 solution x on average.

Differential distinguisher [BihSha91]

$\Delta^{\mathrm{in}} \neq 0, \Delta^{\mathrm{out}}$ s.t for many k, $\quad E_k(x + \Delta^{\mathrm{in}}) + E_k(x) = \Delta^{\mathrm{out}}$ has many solutions x.

Differential cryptanalysis

$$\begin{tikzcd}
x^{(0)} \arrow[r, "F_{k^{(0)}}"] \arrow[d, leftrightarrow, "\Delta^{\mathrm{in}}"] & x^{(1)} \arrow[r, dashed] \arrow[d, leftrightarrow, "\Delta^{(1)}"] & x^{(R-1)} \arrow[r, "F_{k^{(R-1)}}"] \arrow[d, leftrightarrow, "\Delta^{(R-1)}"] & E_k(x^{(0)}) \arrow[d, leftrightarrow, "\Delta^{\mathrm{out}}"] \\
y^{(0)} \arrow[r, "F_{k^{(0)}}"'] & y^{(1)} \arrow[r, dashed] & y^{(R-1)} \arrow[r, "F_{k^{(R-1)}}"'] & E_k(y^{(0)})
\end{tikzcd}$$

$F_{k^{(i)}} = F \circ T_{k^{(i)}}$ for $i \geq 0$.

Differential cryptanalysis

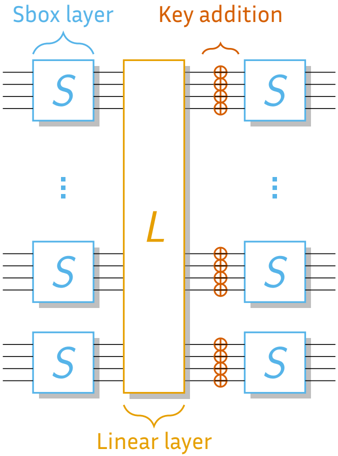
$$
\begin{tikzcd}
x^{(0)} \arrow[r, "F_{k^{(0)}}"] \arrow[d, leftrightarrow, "\Delta^{\mathrm{in}}"] & x^{(1)} \arrow[r, dashed] \arrow[d, leftrightarrow, "\Delta^{(1)}"] & x^{(R-1)} \arrow[r, "F_{k^{(R-1)}}"] \arrow[d, leftrightarrow, "\Delta^{(R-1)}"] & E_k(x^{(0)}) \arrow[d, leftrightarrow, "\Delta^{\mathrm{out}}"] \\
y^{(0)} \arrow[r, "F_{k^{(0)}}"'] & y^{(1)} \arrow[r, dashed] & y^{(R-1)} \arrow[r, "F_{k^{(R-1)}}"'] & E_k(y^{(0)})
\end{tikzcd}
$$

$F_{k^{(i)}} = F \circ T_{k^{(i)}}$ for $i \geq 0$.

On average over all key sequences [LaiMasMur91]

$$\mathbb{E}\left[\Delta^{(0)} \xrightarrow{\mathcal{E}} \Delta^{(r)}\right] \geq \mathbb{E}\left[\Delta^{(0)} \xrightarrow{F} \Delta^{(1)} \rightarrow \cdots \xrightarrow{F} \Delta^{(R)}\right] = \prod_{i=0}^{R-1} \mathbb{P}\left[\Delta^{(i)} \xrightarrow{F} \Delta^{(i+1)}\right]$$

Resisting differential cryptanalysis



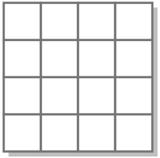
As a designer [DaeRij00]

- Low ***differential uniformity***: [Nyberg94]

$$\delta(S) = \max_{\Delta^{\text{in}} \neq 0, \Delta^{\text{out}}} \left| \left\{ x, S(x + \Delta^{\text{in}}) + S(x) = \Delta^{\text{out}} \right\} \right|$$

- Minimum number of active Sboxes determined by L

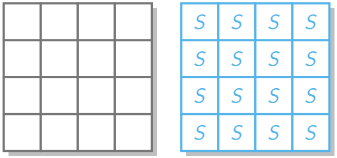
Advanced Encryption Standard (AES)



AES [DaeRij00]

- 4×4 matrix of bytes = 128-bit state

Advanced Encryption Standard (AES)

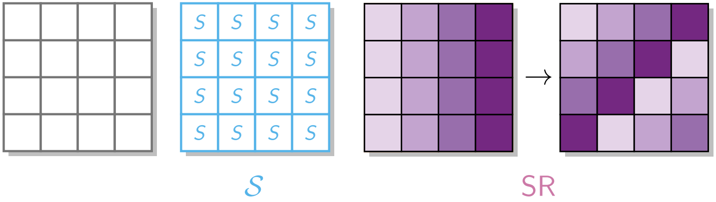


$\mathcal{S}$

AES [DaeRij00]

- 4×4 matrix of bytes = 128-bit state

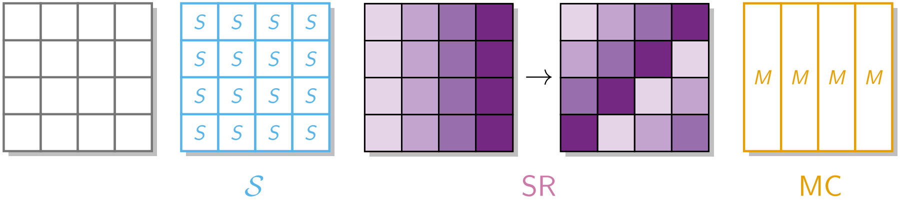
Advanced Encryption Standard (AES)



AES [DaeRij00]

- 4×4 matrix of bytes = 128-bit state

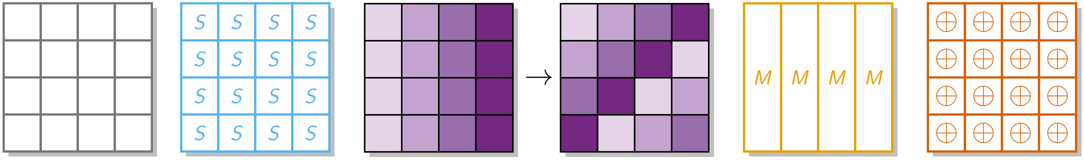
Advanced Encryption Standard (AES)



AES [DaeRij00]

- 4×4 matrix of bytes = 128-bit state

Advanced Encryption Standard (AES)

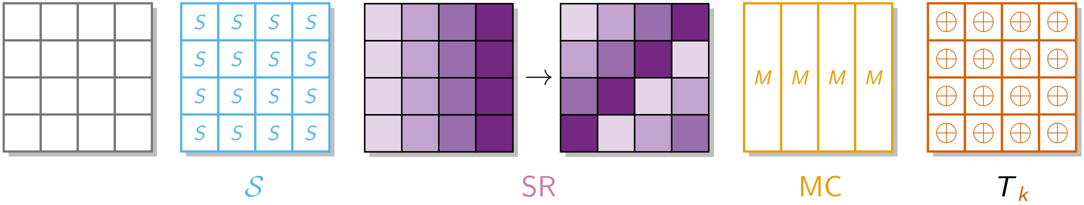


$\mathcal{S}$ SR MC T_k

AES [DaeRij00]

- 4×4 matrix of bytes = 128-bit state
- $F_{k^{(i)}} = T_{k^{(i)}} \circ \mathrm{MC} \circ \mathrm{SR} \circ \mathcal{S}$.
- Repeat 10 times.

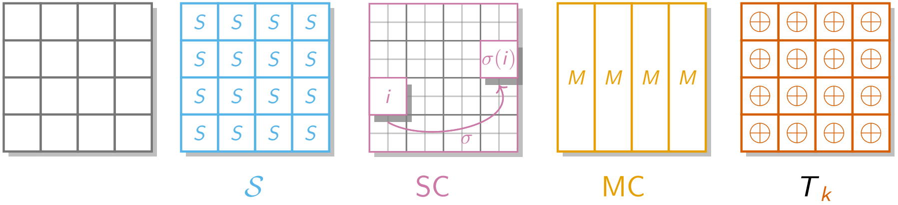
Advanced Encryption Standard (AES)

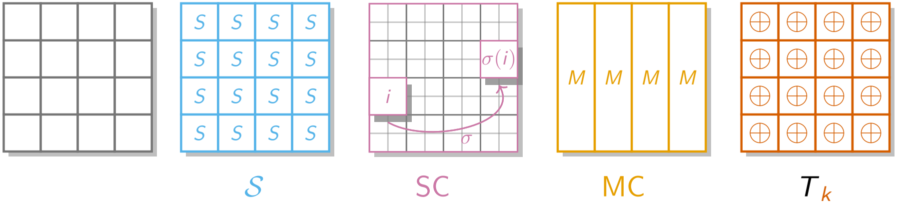


AES [DaeRij00]

- 4×4 matrix of bytes = 128-bit state
- $F_{k^{(i)}} = T_{k^{(i)}} \circ \mathsf{MC} \circ \mathsf{SR} \circ \mathcal{S}$.
- Repeat 10 times.
- $\delta(S) = 4$.
- Structured linear layer $\mathsf{MC} \circ \mathsf{SR}$: $\implies \mathbb{E}\left[\Delta^{(0)} \xrightarrow{F^{(0)}} \Delta^{(1)} \to \cdots \xrightarrow{F^{(3)}} \Delta^{(3)}\right] \leq 2^{-150}$.

Midori





Midori

[BBISHAR15]

- 4×4 matrix of ***nibbles*** = 64-bit state
- $F_{k^{(i)}} = T_{k^{(i)}} \circ \mathrm{MC} \circ \mathrm{SC} \circ \mathcal{S}$.
- Repeat 16 times.
- $\delta(S) = 4$.
- $\mathbb{E}\left[\Delta^{(0)} \xrightarrow{F^{(0)}} \Delta^{(1)} \rightarrow \cdots \xrightarrow{F^{(6)}} \Delta^{(7)}\right] \leq 2^{-70}$.

III - Differential cryptanalysis of conjugate ciphers

Changing our point of view

Chosen plaintext access = freedom of study

1) Encrypt $H(x)$ $\quad\rightsquigarrow E_k \circ H(x)$
2) Apply G $\quad\rightsquigarrow G \circ E_k \circ H(x)$
3) Study $G \circ E_k \circ H$

Changing our point of view

Chosen plaintext access = freedom of study

1) Encrypt $H(x)$ $\rightsquigarrow E_k \circ H(x)$
2) Apply G $\rightsquigarrow G \circ E_k \circ H(x)$
3) Study $G \circ E_k \circ H$

Conjugation

The conjugate of F relative to G is the function $G \circ F \circ G^{-1}$ denoted by F^G.

F^G is the ***same function*** as F, ***up to a change of variables***.

Chosen plaintext access = freedom of study

1) Encrypt $H(x)$ $\rightsquigarrow E_k \circ H(x)$
2) Apply G $\rightsquigarrow G \circ E_k \circ H(x)$
3) Study $G \circ E_k \circ H$

Conjugation

The conjugate of F relative to G is the function $G \circ F \circ G^{-1}$ denoted by F^G.

F^G is the ***same function*** as F, ***up to a change of variables***.

$$E_k = F_{k^{(R-1)}} \circ \ldots \circ F_{k^{(1)}} \circ F_{k^{(0)}}$$

Chosen plaintext access = freedom of study

1) Encrypt $H(x)$ $\rightsquigarrow E_k \circ H(x)$
2) Apply G $\rightsquigarrow G \circ E_k \circ H(x)$
3) Study $G \circ E_k \circ H$

Conjugation

The conjugate of F relative to G is the function $G \circ F \circ G^{-1}$ denoted by F^G.

F^G is the *same function* as F, *up to a change of variables*.

$$E_k = F_{k(R-1)} \circ \ldots \circ F_{k(1)} \circ F_{k(0)}$$

$$E_k^G = F_{k(R-1)}^G \circ \ldots \circ F_{k(1)}^G \circ F_{k(0)}^G$$

Proof left as exercice. $\square$ $(G^{-1} \circ G = \mathrm{Id})$

Chosen plaintext access = freedom of study

1) Encrypt $H(x)$ $\rightsquigarrow E_k \circ H(x)$
2) Apply G $\rightsquigarrow G \circ E_k \circ H(x)$
3) Study $G \circ E_k \circ H$

Conjugation

The conjugate of F relative to G is the function $G \circ F \circ G^{-1}$ denoted by F^G.

F^G is the ***same function*** as F, ***up to a change of variables***.

$$E_k = F_{k(R-1)} \circ \ldots \circ F_{k(1)} \circ F_{k(0)}$$

$$E_k^G = F^G_{k(R-1)} \circ \ldots \circ F^G_{k(1)} \circ F^G_{k(0)}$$

Proof left as exercice. $\square$ $(G^{-1} \circ G = \mathrm{Id})$

Is it simpler to attack E_k^G than E_k ?

Linear VS non-linear change of variables

Recap

$F^G := G \circ F \circ G^{-1}$

$$E_k^G = F^G_{k(R-1)} \circ \ldots \circ F^G_{k(1)} \circ F^G_{k(0)}$$

Linear VS non-linear change of variables

Recap

$F^G := G \circ F \circ G^{-1}$

$$E_k^G = F_{k(R-1)}^G \circ \ldots \circ F_{k(1)}^G \circ F_{k(0)}^G$$

Definition/Proposition (Affine equivalence)

Def: $F_1 \sim_{\mathrm{aff}} F_2$ if $\exists\, A, B$ bijective affine s.t. $A \circ F_1 \circ B = F_2$.

Prop: If $F_1 \sim_{\mathrm{aff}} F_2$, then $\delta(F_1) = \delta(F_2)$ and $\mathcal{L}(F_1) = \mathcal{L}(F_2)$

Linear VS non-linear change of variables

Recap

$F^G := G \circ F \circ G^{-1}$

$$E_k^G = F_{k(R-1)}^G \circ \ldots \circ F_{k(1)}^G \circ F_{k(0)}^G$$

Definition/Proposition (Affine equivalence)

Def: $F_1 \sim_{\text{aff}} F_2$ if $\exists\, A, B$ bijective affine s.t. $A \circ F_1 \circ B = F_2$.

Prop: If $F_1 \sim_{\text{aff}} F_2$, then $\delta(F_1) = \delta(F_2)$ and $\mathcal{L}(F_1) = \mathcal{L}(F_2)$

Corollary

- If G linear, $\delta(F) = \delta(F^G)$ and $\mathcal{L}(F) = \mathcal{L}(F^G)$

$\implies$ Fine-grained arguments are needed.

- If G non-linear ?

$\implies$ Linear attack cf. [BeiCanLea18]

$\implies$ Differential attack cf. [BFLNPS23,BBFLNPS24]

Non-linear change of variables (1/2)

$$F_{k(i)} = T_{k(i)} \circ \mathrm{MC} \circ \mathrm{SC} \circ \mathcal{S} \quad \rightsquigarrow \quad F^G_{k(i)} = T^G_{k(i)} \circ \mathrm{MC}^G \circ \mathrm{SC}^G \circ \mathcal{S}^G$$

Non-linear change of variables (1/2)

$$F_{k(i)} = T_{k(i)} \circ \mathrm{MC} \circ \mathrm{SC} \circ \mathcal{S} \quad \rightsquigarrow \quad F^G_{k(i)} = T^G_{k(i)} \circ \mathrm{MC}^G \circ \mathrm{SC}^G \circ \mathcal{S}^G$$

Main problem

If F is *linear*, F^G is a priori not.

$\implies$ T^G_k *non-linear dependency* in the key bits.

Non-linear change of variables (1/2)

$$F_{k(i)} = T_{k(i)} \circ \mathrm{MC} \circ \mathrm{SC} \circ \mathcal{S} \quad \rightsquigarrow \quad F^G_{k(i)} = T^G_{k(i)} \circ \mathrm{MC}^G \circ \mathrm{SC}^G \circ \mathcal{S}^G$$

Main problem

If F is *linear*, F^G is a priori not.
$\Longrightarrow$ T^G_k *non-linear dependency* in the key bits.

A possible solution

General case For all Δ and all k: $\mathbb{P}\left[\Delta \xrightarrow{T_k} \Delta\right] = 1$

Conjugated case For *some* Δ and *some* k: $\mathbb{P}\left[\Delta \xrightarrow{T^G_k} \Delta\right] = 1$

$\Longrightarrow$ ***Weak-key attacks***!

Non-linear change of variables (1/2)

$$F_{k^{(i)}} = T_{k^{(i)}} \circ \mathrm{MC} \circ \mathrm{SC} \circ \mathcal{S} \quad \rightsquigarrow \quad F^G_{k^{(i)}} = T^G_{k^{(i)}} \circ \mathrm{MC}^G \circ \mathrm{SC}^G \circ \mathcal{S}^G$$

Main problem

If F is *linear*, F^G is a priori not.

$\implies$ T^G_k *non-linear dependency* in the key bits.

A possible solution

General case For all Δ and all k: $\mathbb{P}\left[\Delta \xrightarrow{T_k} \Delta\right] = 1$

Conjugated case For *some* Δ and *some* k: $\mathbb{P}\left[\Delta \xrightarrow{T^G_k} \Delta\right] = 1$

$\implies$ ***Weak-key attacks***!

Weak-key space

$$W(\Delta) = \left\{k,\ \mathbb{P}\left[\Delta \xrightarrow{T^G_k} \Delta\right] = 1\right\}$$

Non-linear change of variables (1/2)

$$F_{k^{(i)}} = T_{k^{(i)}} \circ \mathrm{MC} \circ \mathrm{SC} \circ \mathcal{S} \quad \rightsquigarrow \quad F^G_{k^{(i)}} = T^G_{k^{(i)}} \circ \mathrm{MC}^G \circ \mathrm{SC}^G \circ \mathcal{S}^G$$

Main problem

If F is *linear*, F^G is a priori not.

$\implies$ T_k^G *non-linear dependency* in the key bits.

A possible solution

General case For all Δ and all k: $\mathbb{P}\left[\Delta \xrightarrow{T_k} \Delta\right] = 1$

Conjugated case For *some* Δ and *some* k: $\mathbb{P}\left[\Delta \xrightarrow{T_k^G} \Delta\right] = 1$

$\implies$ *Weak-key attacks*!

Weak-key space

$$W(\Delta) = \left\{k,\ \mathbb{P}\left[\Delta \xrightarrow{T_k^G} \Delta\right] = 1\right\} = \{k,\ D_\Delta T_k^G \text{ constant and equal to } \Delta\}$$

$\implies$ *linear structure*

Non-linear change of variables (2/2)

Recap

T_k^G with linear structures $\rightsquigarrow$ G should be sparse

Non-linear change of variables (2/2)

Recap

T_k^G with linear structures $\rightsquigarrow$ G should be sparse

Our explored space

$\mathcal{G}$ Sbox layer based on $G : \mathbb{F}_2^4 \to \mathbb{F}_2^4$ with

$$G\,(x_0,\ x_1,\ x_2,\ x_3) = (x_0 + g(x_1, x_2, x_3),\ x_1,\ x_2,\ x_3)$$

$(G = G^{-1})$

Non-linear change of variables (2/2)

Recap

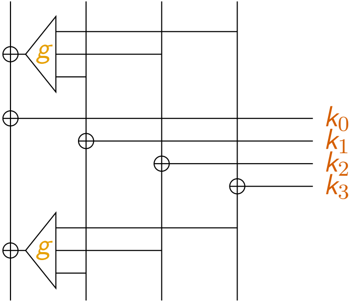
T_k^G with linear structures $\rightsquigarrow$ G should be sparse

Our explored space

$\mathcal{G}$ Sbox layer based on $G : \mathbb{F}_2^4 \to \mathbb{F}_2^4$ with

$$G(x_0,\ x_1,\ x_2,\ x_3) = (x_0 + g(x_1, x_2, x_3),\ x_1,\ x_2,\ x_3)$$

$(G = G^{-1})$



$$T_k^G(x_0,\ x_1,\ x_2,\ x_3) = \begin{pmatrix} x_0 + k_0 + D_{\tilde{k}} g(x_1, x_2, x_3) \\ x_1 + k_1 \\ x_2 + k_2 \\ x_3 + k_3 \end{pmatrix}$$

Non-linear change of variables (2/2)

Recap

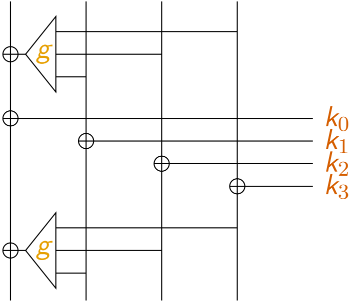
T_k^G with linear structures $\rightsquigarrow$ G should be sparse

Our explored space

$\mathcal{G}$ Sbox layer based on $G : \mathbb{F}_2^4 \to \mathbb{F}_2^4$ with

$$G(x_0,\ x_1,\ x_2,\ x_3) = (x_0 + g(x_1, x_2, x_3),\ x_1,\ x_2,\ x_3)$$

$(G = G^{-1})$



$$T_k^G(x_0,\ x_1,\ x_2,\ x_3) = \begin{pmatrix} x_0 + k_0 + D_{\tilde{k}}g(x_1, x_2, x_3) \\ x_1 + k_1 \\ x_2 + k_2 \\ x_3 + k_3 \end{pmatrix}$$

g quadratic $\implies$ T_k^G linear $\implies$ constant derivatives $D_\triangle T_k^G$

Sbox

By computer search, there exist G and Δ s.t $\mathbb{P}\left[\Delta \xrightarrow{S^G} \Delta\right] = 1$ $\mathbb{P}\left[\nabla \xrightarrow{\mathcal{S}^G} \nabla\right] = 1.$
$\nabla = (\Delta, \ldots, \Delta)$.

The case of Midori

Sbox

By computer search, there exist G and Δ s.t $\mathbb{P}\left[\Delta \xrightarrow{S^G} \Delta\right] = 1$ $\mathbb{P}\left[\nabla \xrightarrow{\mathcal{S}^G} \nabla\right] = 1.$

$\nabla = (\Delta, \ldots, \Delta).$

Linear layer

$$M = \begin{pmatrix} 0 & \mathrm{Id} & \mathrm{Id} & \mathrm{Id} \\ \mathrm{Id} & 0 & \mathrm{Id} & \mathrm{Id} \\ \mathrm{Id} & \mathrm{Id} & 0 & \mathrm{Id} \\ \mathrm{Id} & \mathrm{Id} & \mathrm{Id} & 0 \end{pmatrix}$$

$$\mathbb{P}\left[\nabla \xrightarrow{\mathsf{MC}^G} \nabla\right] = 1$$

Sbox

By computer search, there exist G and Δ s.t $\mathbb{P}\left[\Delta \xrightarrow{S^G} \Delta\right] = 1$

$\nabla = (\Delta, \dots, \Delta)$.

$$\mathbb{P}\left[\nabla \xrightarrow{S^G} \nabla\right] = 1.$$

Linear layer

$$M = \begin{pmatrix} 0 & \mathrm{Id} & \mathrm{Id} & \mathrm{Id} \\ \mathrm{Id} & 0 & \mathrm{Id} & \mathrm{Id} \\ \mathrm{Id} & \mathrm{Id} & 0 & \mathrm{Id} \\ \mathrm{Id} & \mathrm{Id} & \mathrm{Id} & 0 \end{pmatrix}$$

$$\mathbb{P}\left[\nabla \xrightarrow{\mathsf{MC}^G} \nabla\right] = 1$$

Probability-1 distinguisher for infinitely many rounds★

$$\mathbb{P}\left[\nabla \xrightarrow{S^G} \nabla \xrightarrow{(MC\circ \mathsf{SC})^G} \nabla \xrightarrow{T^G_{k(0)}} \nabla \xrightarrow{S^G} \nabla \xrightarrow{(MC\circ \mathsf{SC})^G} \nabla \xrightarrow{T^G_{k(1)}} \nabla \xrightarrow{S^G} \nabla \xrightarrow{(MC\circ \mathsf{SC})^G} \nabla \xrightarrow{T^G_{k(0)}} \cdots\right] = 1$$

★ If the two round keys are weak. $\frac{|W(\nabla)|}{2^{64}} = 2^{-16} \implies 2^{96}$ weak-keys for variants of Midori

Equivalent points of view

$$\mathbb{P}[\Delta^{\text{in}} \xrightarrow{F^G} \Delta^{\text{out}}] = 1 \iff \forall\, x, F^G(x + \Delta^{\text{in}}) + F^G(x) = \Delta^{\text{out}}$$

Equivalent points of view

$$\mathbb{P}[\Delta^{\mathrm{in}} \xrightarrow{F^G} \Delta^{\mathrm{out}}] = 1 \iff \forall\, x, F^G(x + \Delta^{\mathrm{in}}) + F^G(x) = \Delta^{\mathrm{out}}$$

$$\iff G \circ F \circ G^{-1} \circ T_{\Delta^{\mathrm{in}}} = T_{\Delta^{\mathrm{out}}} \circ G \circ F \circ G^{-1}$$

Equivalent points of view

$$\mathbb{P}[\Delta^{\text{in}} \xrightarrow{F^G} \Delta^{\text{out}}] = 1 \iff \forall\, x, F^G(x + \Delta^{\text{in}}) + F^G(x) = \Delta^{\text{out}}$$

$$\iff G \circ F \circ G^{-1} \circ T_{\Delta^{\text{in}}} = T_{\Delta^{\text{out}}} \circ G \circ F \circ G^{-1}$$

$$\iff F \circ \underbrace{(G^{-1} \circ T_{\Delta^{\text{in}}} \circ G)}_{A} = \underbrace{(G^{-1} \circ T_{\Delta^{\text{out}}} \circ G)}_{B} \circ F$$

Equivalent points of view

$$\mathbb{P}[\Delta^{\mathrm{in}} \xrightarrow{F^G} \Delta^{\mathrm{out}}] = 1 \iff \forall x, F^G(x + \Delta^{\mathrm{in}}) + F^G(x) = \Delta^{\mathrm{out}}$$

$$\iff G \circ F \circ G^{-1} \circ T_{\Delta^{\mathrm{in}}} = T_{\Delta^{\mathrm{out}}} \circ G \circ F \circ G^{-1}$$

$$\iff F \circ \underbrace{(G^{-1} \circ T_{\Delta^{\mathrm{in}}} \circ G)}_{A} = \underbrace{(G^{-1} \circ T_{\Delta^{\mathrm{out}}} \circ G)}_{B} \circ F$$

Equivalent points of view

- "Commutation" $F \circ A = B \circ F$ [BFLNPS23]

Equivalent points of view

$$\mathbb{P}[\Delta^{\text{in}} \xrightarrow{F^G} \Delta^{\text{out}}] = 1 \iff \forall x, F^G(x + \Delta^{\text{in}}) + F^G(x) = \Delta^{\text{out}}$$

$$\iff G \circ F \circ G^{-1} \circ T_{\Delta^{\text{in}}} = T_{\Delta^{\text{out}}} \circ G \circ F \circ G^{-1}$$

$$\iff F \circ \underbrace{\left(G^{-1} \circ T_{\Delta^{\text{in}}} \circ G\right)}_{A} = \underbrace{\left(G^{-1} \circ T_{\Delta^{\text{out}}} \circ G\right)}_{B} \circ F$$

Equivalent points of view

- "Commutation" $F \circ A = B \circ F$ [BFLNPS23]
- Self-equivalence $B^{-1} \circ F \circ A = F$ [BFLNPS23]

Equivalent points of view

$$\mathbb{P}[\Delta^{\text{in}} \xrightarrow{F^G} \Delta^{\text{out}}] = 1 \iff \forall x, F^G(x + \Delta^{\text{in}}) + F^G(x) = \Delta^{\text{out}}$$
$$\iff G \circ F \circ G^{-1} \circ T_{\Delta^{\text{in}}} = T_{\Delta^{\text{out}}} \circ G \circ F \circ G^{-1}$$
$$\iff F \circ \underbrace{\left(G^{-1} \circ T_{\Delta^{\text{in}}} \circ G\right)}_{A} = \underbrace{\left(G^{-1} \circ T_{\Delta^{\text{out}}} \circ G\right)}_{B} \circ F$$

Equivalent points of view

- "Commutation" $F \circ A = B \circ F$ [BFLNPS23]
- Self-equivalence $B^{-1} \circ F \circ A = F$ [BFLNPS23]
- Differential eq. for ***another group law*** $F \circ \left(G^{-1} \circ T_{\Delta^{\text{in}}} \circ G\right) = \left(G^{-1} \circ T_{\Delta^{\text{out}}} \circ G\right) \circ F$
  $G^{-1} T_{\Delta} G$ is an addition, up to a change of variables. [CivBloSal19, CalCivInv24]

Equivalent points of view

$$\mathbb{P}[\Delta^{\mathrm{in}} \xrightarrow{F^G} \Delta^{\mathrm{out}}] = 1 \iff \forall x, F^G(x + \Delta^{\mathrm{in}}) + F^G(x) = \Delta^{\mathrm{out}}$$
$$\iff G \circ F \circ G^{-1} \circ T_{\Delta^{\mathrm{in}}} = T_{\Delta^{\mathrm{out}}} \circ G \circ F \circ G^{-1}$$
$$\iff F \circ \underbrace{(G^{-1} \circ T_{\Delta^{\mathrm{in}}} \circ G)}_{A} = \underbrace{(G^{-1} \circ T_{\Delta^{\mathrm{out}}} \circ G)}_{B} \circ F$$

Equivalent points of view

- "Commutation" $F \circ A = B \circ F$ [BFLNPS23]
- Self-equivalence $B^{-1} \circ F \circ A = F$ [BFLNPS23]
- Differential eq. for ***another group law*** $F \circ (G^{-1} \circ T_{\Delta^{\mathrm{in}}} \circ G) = (G^{-1} \circ T_{\Delta^{\mathrm{out}}} \circ G) \circ F$
  $G^{-1} T_{\Delta} G$ is an addition, up to a change of variables. [CivBloSal19, CalCivInv24]

The case of Midori

- $A = B \implies$ "commutation" makes sense
- A and B are affine $\implies$ Self-equivalence makes sense

Benefits from each point of view

$$\mathbb{P}[\Delta^{\text{in}} \xrightarrow{F^G} \Delta^{\text{out}}] = 1 \iff F \circ (G^{-1} \circ T_{\Delta^{\text{in}}} \circ G) = (G^{-1} \circ T_{\Delta^{\text{out}}} \circ G) \circ F$$
$$\iff F \circ A = B \circ F$$
$$\iff B^{-1} \circ F \circ A = F$$

Self affine-equivalence for the Sbox

Efficient search for affine bijections A, B s.t. $B^{-1} \circ F \circ A = F$ [BDBP03][Dinur18]

Benefits from each point of view

$$\mathbb{P}[\Delta^{\text{in}} \xrightarrow{F^G} \Delta^{\text{out}}] = 1 \iff F \circ (G^{-1} \circ T_{\Delta^{\text{in}}} \circ G) = (G^{-1} \circ T_{\Delta^{\text{out}}} \circ G) \circ F$$
$$\iff F \circ A = B \circ F$$
$$\iff B^{-1} \circ F \circ A = F$$

Self affine-equivalence for the Sbox

Efficient search for affine bijections A, B s.t. $B^{-1} \circ F \circ A = F$ [BDBP03][Dinur18]

Commutation for linear layer

For Midori, A affine and $A = B$.

$$\begin{pmatrix} 0 & \mathrm{Id} & \mathrm{Id} & \mathrm{Id} \\ \mathrm{Id} & 0 & \mathrm{Id} & \mathrm{Id} \\ \mathrm{Id} & \mathrm{Id} & 0 & \mathrm{Id} \\ \mathrm{Id} & \mathrm{Id} & \mathrm{Id} & 0 \end{pmatrix} \begin{pmatrix} A & 0 & 0 & 0 \\ 0 & A & 0 & 0 \\ 0 & 0 & A & 0 \\ 0 & 0 & 0 & A \end{pmatrix} = \begin{pmatrix} A & 0 & 0 & 0 \\ 0 & A & 0 & 0 \\ 0 & 0 & A & 0 \\ 0 & 0 & 0 & A \end{pmatrix} \begin{pmatrix} 0 & \mathrm{Id} & \mathrm{Id} & \mathrm{Id} \\ \mathrm{Id} & 0 & \mathrm{Id} & \mathrm{Id} \\ \mathrm{Id} & \mathrm{Id} & 0 & \mathrm{Id} \\ \mathrm{Id} & \mathrm{Id} & \mathrm{Id} & 0 \end{pmatrix}$$

Benefits from each point of view

$$\mathbb{P}[\Delta^{\text{in}} \xrightarrow{F^G} \Delta^{\text{out}}] = 1 \iff F \circ (G^{-1} \circ T_{\Delta^{\text{in}}} \circ G) = (G^{-1} \circ T_{\Delta^{\text{out}}} \circ G) \circ F$$
$$\iff F \circ A = B \circ F$$
$$\iff B^{-1} \circ F \circ A = F$$

Self affine-equivalence for the Sbox

Efficient search for affine bijections A, B s.t. $B^{-1} \circ F \circ A = F$ [BDBP03][Dinur18]

Commutation for linear layer

For Midori, A affine and $A = B$.

$$\begin{pmatrix} 0 & \mathrm{Id} & \mathrm{Id} & \mathrm{Id} \\ \mathrm{Id} & 0 & \mathrm{Id} & \mathrm{Id} \\ \mathrm{Id} & \mathrm{Id} & 0 & \mathrm{Id} \\ \mathrm{Id} & \mathrm{Id} & \mathrm{Id} & 0 \end{pmatrix} \begin{pmatrix} A & 0 & 0 & 0 \\ 0 & A & 0 & 0 \\ 0 & 0 & A & 0 \\ 0 & 0 & 0 & A \end{pmatrix} = \begin{pmatrix} A & 0 & 0 & 0 \\ 0 & A & 0 & 0 \\ 0 & 0 & A & 0 \\ 0 & 0 & 0 & A \end{pmatrix} \begin{pmatrix} 0 & \mathrm{Id} & \mathrm{Id} & \mathrm{Id} \\ \mathrm{Id} & 0 & \mathrm{Id} & \mathrm{Id} \\ \mathrm{Id} & \mathrm{Id} & 0 & \mathrm{Id} \\ \mathrm{Id} & \mathrm{Id} & \mathrm{Id} & 0 \end{pmatrix}$$

Alternative group law for key addition layer

Bounds on the dimension of $W(\Delta)$. [CivBloSal19]

Take away

Theorem (Relationships between cryptanalysis techniques)

Commutative $\supset$ Affine commutative $\approx$ Differential for conjugates = Differential w.r.t $(\mathbb{F}_2^n, \diamond)$

Sum up

- Conjugates of ciphers do *play a role in cryptanalysis*
- ⚠ $B \circ S \circ A = S$ with sparse linear layer and sparse key-schedule

Open questions

- Efficient ways of finding “good’ G?
- *Probabilistic* cryptanalysis
- Associated *security criteria* ?

IV - Self-linear equivalences among known infinite APN families

Almost perfect non-linear (APN) functions

$$F(x + \Delta^{\text{in}}) + F(x) = \Delta^{\text{out}}$$

APN function [NybKnu92]

F is APN if: $\forall\, \Delta^{\text{in}} \neq 0, \Delta^{\text{out}}$, $\quad F(x + \Delta^{\text{in}}) + F(x) = \Delta^{\text{out}}$ has at most 2 solutions x.

Almost perfect non-linear (APN) functions

$$F(x + \Delta^{\text{in}}) + F(x) = \Delta^{\text{out}}$$

APN function [NybKnu92]

F is APN if: $\forall\, \Delta^{\text{in}} \neq 0, \Delta^{\text{out}}$, $\quad F(x + \Delta^{\text{in}}) + F(x) = \Delta^{\text{out}}$ has at most 2 solutions x.

A classification problem

- Easy to define
- Hard to build new instances
- Hard to classify

Almost perfect non-linear (APN) functions

$$F(x + \Delta^{\text{in}}) + F(x) = \Delta^{\text{out}}$$

APN function [NybKnu92]

F is APN if: $\forall\ \Delta^{\text{in}} \neq 0, \Delta^{\text{out}}$, $\quad F(x + \Delta^{\text{in}}) + F(x) = \Delta^{\text{out}}$ has at most 2 solutions x.

A classification problem

- Easy to define
- Hard to build new instances
- Hard to classify

Even harder with more constraints

1) $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$, n ***even***, F APN & ***bijective*** ? [Big APN problem, BDMW10]
2) F ***equivalent*** to neither a power function nor a quadratic function ?

For both, a ***single*** example is known (for now ?) [BDMW10] & [BriLea08,EdePot09]

Tool #1: Equivalence relations

Recap (Affine equivalence)

$F_1 \sim_{\text{aff}} F_2$ if $\quad \exists\, A, B$, bijective affine s.t. $\quad A \circ F_1 \circ B = F_2$.

Prop: If $F_1 \sim_{\text{aff}} F_2$, then $\delta(F_1) = \delta(F_2)$. $\quad F_1$ APN $\iff$ F_2 APN.

Tool #1: Equivalence relations

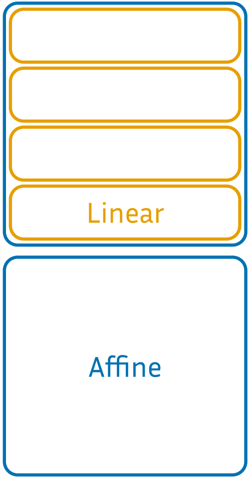
Recap (Affine equivalence)

$F_1 \sim_{\text{aff}} F_2$ if $\exists\, A, B$, bijective affine s.t. $A \circ F_1 \circ B = F_2$.

Prop: If $F_1 \sim_{\text{aff}} F_2$, then $\delta(F_1) = \delta(F_2)$. F_1 APN $\iff$ F_2 APN.

Subcase (Linear equivalence)

$F_1 \sim_{\text{lin}} F_2$ if $\exists\, A, B$, bijective *linear* s.t. $A \circ F_1 \circ B = F_2$.



Recap (Affine equivalence)

$F_1 \sim_{\text{aff}} F_2$ if $\exists\ A, B$, bijective affine s.t. $A \circ F_1 \circ B = F_2$.

Prop: If $F_1 \sim_{\text{aff}} F_2$, then $\delta(F_1) = \delta(F_2)$. F_1 APN $\iff$ F_2 APN.

Subcase (Linear equivalence)

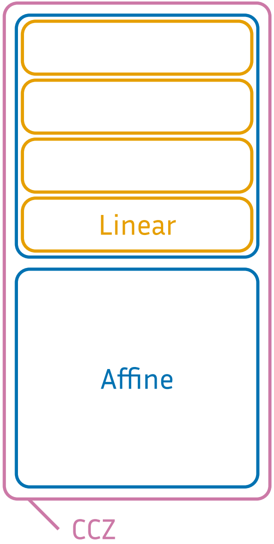
$F_1 \sim_{\text{lin}} F_2$ if $\exists\ A, B$, bijective *linear* s.t. $A \circ F_1 \circ B = F_2$.

More general case (CCZ equivalence) [CCZ98]

$F_1, F_2 : \mathbb{F}_2^n \to \mathbb{F}_2^n$ CCZ-equivalent if: $\exists\ \mathcal{A} : \mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{F}_2^n \times \mathbb{F}_2^n$ bijective *affine* s.t.

$$\mathcal{A}\left(\{(x,\ F_1(x)), x \in \mathbb{F}_2^n\}\right) = \{(x,\ F_2(x)), x \in \mathbb{F}_2^n\}$$

Prop: If $F_1 \sim_{\text{CCZ}} F_2$, then F_1 APN $\iff$ F_2 APN.



Tool #2: Different representations of the same object

Recap (Linear change of variables)

$$\delta_F(\Delta^{\text{in}}, \Delta^{\text{out}}) := \left|\left\{x, F(x + \Delta^{\text{in}}) + F(x) = \Delta^{\text{out}}\right\}\right|$$

$F : \mathbb{F}_2^n \to \mathbb{F}_2^n$, $G : \mathbb{F}_2^n \to \mathbb{F}_2^n$ linear bijection. Then:

$$\forall\, \Delta^{\text{in}}, \Delta^{\text{out}} \quad \delta_{GFG^{-1}}(\Delta^{\text{in}}, \Delta^{\text{out}}) = \delta_F(G^{-1}(\Delta^{\text{in}}), G^{-1}(\Delta^{\text{out}}))$$

Tool #2: Different representations of the same object

Recap (Linear change of variables)

$$\delta_F(\Delta^{\mathrm{in}}, \Delta^{\mathrm{out}}) := \left|\{x, F(x + \Delta^{\mathrm{in}}) + F(x) = \Delta^{\mathrm{out}}\}\right|$$

$F : \mathbb{F}_2^n \to \mathbb{F}_2^n$, $G : \mathbb{F}_2^n \to \mathbb{F}_2^n$ linear bijection. Then:

$$\forall\, \Delta^{\mathrm{in}}, \Delta^{\mathrm{out}} \quad \delta_{GFG^{-1}}(\Delta^{\mathrm{in}}, \Delta^{\mathrm{out}}) = \delta_F(G^{-1}(\Delta^{\mathrm{in}}), G^{-1}(\Delta^{\mathrm{out}}))$$

$$\begin{tikzcd}
(\mathbb{F}_2^n, +) \arrow[r, "F"] & (\mathbb{F}_2^n, +) \arrow[d, "G"] \\
(\mathbb{F}_2^n, +) \arrow[u, "G^{-1}"] \arrow[r, dashed, "F^G"] & (\mathbb{F}_2^n, +)
\end{tikzcd}$$

Recap (Linear change of variables)

$$\delta_F(\Delta^{\mathrm{in}}, \Delta^{\mathrm{out}}) := \left|\left\{x, F(x + \Delta^{\mathrm{in}}) + F(x) = \Delta^{\mathrm{out}}\right\}\right|$$

$F : \mathbb{F}_2^n \to \mathbb{F}_2^n$, $G : \mathbb{F}_2^n \to \mathbb{F}_2^n$ linear bijection. Then:

$$\forall\, \Delta^{\mathrm{in}}, \Delta^{\mathrm{out}} \quad \delta_{GFG^{-1}}(\Delta^{\mathrm{in}}, \Delta^{\mathrm{out}}) = \delta_F(G^{-1}(\Delta^{\mathrm{in}}), G^{-1}(\Delta^{\mathrm{out}}))$$

$$\begin{tikzcd}
(\mathbb{F}_2^n, +) \arrow[r, "F"] & (\mathbb{F}_2^n, +) \arrow[d, "G"] \\
(V, \diamond) \arrow[u, "G^{-1}"] \arrow[r, dashed, "F^G"] & (V, \diamond)
\end{tikzcd}$$

$G : (\mathbb{F}_2^n, +) \to (V, \diamond)$, group *isomorphism*.

Recap (Linear change of variables)

$$\delta_F(\Delta^{\mathrm{in}}, \Delta^{\mathrm{out}}) := \left|\left\{x, F(x + \Delta^{\mathrm{in}}) + F(x) = \Delta^{\mathrm{out}}\right\}\right|$$

$F : \mathbb{F}_2^n \to \mathbb{F}_2^n$, $G : \mathbb{F}_2^n \to \mathbb{F}_2^n$ linear bijection. Then:

$$\forall\ \Delta^{\mathrm{in}}, \Delta^{\mathrm{out}} \quad \delta_{GFG^{-1}}(\Delta^{\mathrm{in}}, \Delta^{\mathrm{out}}) = \delta_F(G^{-1}(\Delta^{\mathrm{in}}), G^{-1}(\Delta^{\mathrm{out}}))$$

$$\begin{tikzcd}
(\mathbb{F}_2^n, +) \arrow[r, "F"] & (\mathbb{F}_2^n, +) \arrow[d, "G"] \\
(V, \diamond) \arrow[u, "G^{-1}"] \arrow[r, dashed, "F^G"] & (V, \diamond)
\end{tikzcd}$$

$G : (\mathbb{F}_2^n, +) \to (V, \diamond)$, group ***isomorphism***.

Freedom of representation

$$F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n} \quad \simeq \quad F : \mathbb{F}_2^n \to \mathbb{F}_2^n \quad \simeq \quad F : (\mathbb{F}_{2^k})^\ell \to (\mathbb{F}_{2^k})^\ell,\ n = \ell k$$

Zoo of APN functions

Univariate
$x^{2^s+1} + ax^{2^{(3-i)k+s}+2^{ik}}$
$x^{2^s+1} + ax^{2^{(4-i)k+s}+2^{ik}}$
$ax^{2^k+1} + x^{2^s+1} + x^{2^{s+k}+2^k} + bx^{2^{k+s}+1} + b^{2^k}x^{2^s+2^k}$
$x^3 + a^{-1}\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}(a^3x^9)$
$x^3 + a^{-1}\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^3}}(a^3x^9 + a^6x^{18})$
$x^3 + a^{-1}\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^3}}(a^6x^{18} + a^{12}x^{36})$
$ax^{2^s+1} + a^{2^k}x^{2^{2k}+2^{k+s}} + bx^{2^{2k}+1} + ca^{2^k+1}x^{2^s+2^{k+s}}$
$a^2x^{2^{2k+1}+1} + b^2x^{2^{k+1}+1} + ax^{2^{2k}+2} + bx^{2^k+2} + dx^3$
$x^3 + ax^{2^{s+i}+2^i} + a^2x^{2^{k+1}+2^k} + x^{2^{s+i+k}+2^{i+k}}$
$a\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^k}}(bx^{2^i+1}) + a^{2^k}\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^k}}(cx^{2^s+1})$
$L(x)^{2^k+1} + bx^{2^k+1}$

Multivariate
$(x,y) \mapsto \begin{pmatrix} x^{2^s+1} + ay^{(2^s+1)2^i} \\ xy \end{pmatrix}$
$(x,y) \mapsto \begin{pmatrix} x^{2^{2s}+2^{3s}} + ax^{2^{2s}}y^{2^s} + by^{2^s+1} \\ xy \end{pmatrix}$
$(x,y) \mapsto \begin{pmatrix} x^{2^s+1} + x^{2^{s+k/2}}y^{2^{k/2}} + axy^{2^s} + by^{2^s+1} \\ xy \end{pmatrix}$
$(x,y) \mapsto \begin{pmatrix} x^{2^s+1} + xy^{2^s} + y^{2^s+1} \\ x^{2^{2s}+1} + x^{2^{2s}}y + y^{2^{2s}+1} \end{pmatrix}$
$(x,y) \mapsto \begin{pmatrix} x^{2^s+1} + xy^{2^s} + y^{2^s+1} \\ x^{2^{3s}}y + xy^{2^{3s}} \end{pmatrix}$
$(x,y) \mapsto \begin{pmatrix} x^{2^s+1} + by^{2^s+1} \\ x^{2^{s+k/2}}y + \frac{a}{b}xy^{2^{s+k/2}} \end{pmatrix}$
$(x,y) \mapsto \begin{pmatrix} x^{2^s+1} + xy^{2^s} + ay^{2^s+1} \\ x^{2^{2s}+1} + ax^{2^{2s}}y + (1+a)^{2^s}xy^{2^{2s}} + ay^{2^{2s}+1} \end{pmatrix}$
$(x,y,z) \mapsto \begin{pmatrix} x^{2^s+1} + x^{2^s}z + yz^{2^s} \\ x^{2^s}z + y^{2^s+1} \\ xy^{2^s} + y^{2^s}z + z^{2^s+1} \end{pmatrix}$
$(x,y,z) \mapsto \begin{pmatrix} x^{2^s+1} + xy^{2^s} + yz^{2^s} \\ xy^{2^s} + z^{2^s+1} \\ x^{2^s}z + y^{2^s+1} + y^{2^s}z \end{pmatrix}$

Zoo of APN functions

Univariate
$x^{2^s+1} + ax^{2^{(3-i)k+s}+2^{ik}}$
$x^{2^s+1} + ax^{2^{(4-i)k+s}+2^{ik}}$
$ax^{2^k+1} + x^{2^s+1} + x^{2^{s+k}+2^k} + bx^{2^{k+s}+1} + b^{2^k}x^{2^s+2^k}$
$x^3 + a^{-1}\mathrm{Tr}_{\mathbb{F}_2}$ …
$x^3 + a^{-1}\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^3}}$ …
$x^3 + a^{-1}\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^3}}(a^6x^{18} + a^{12}x^{36})$
$ax^{2^s+1} + a^{2^k}x^{2^{2k}+2^{k+s}} + bx^{2^{2k}+1} + ca^{2^k+1}x^{2^s+2^{k+s}}$
$a^2x^{2^{2k+1}+1} + b^2x^{2^{k+1}+1} + ax^{2^{2k}+2} + bx^{2^k+2} + dx^3$
$x^3 + ax^{2^{s+i}+2^i} + a^2x^{2^{k+1}+2^k} + x^{2^{s+i+k}+2^{i+k}}$
$a\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^k}}(bx^{2^i+1}) + a^{2^k}\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^k}}(cx^{2^s+1})$
$L(x)^{2^k+1} + bx^{2^k+1}$

Multivariate
$(x,y) \mapsto \begin{pmatrix} x^{2^s+1} + ay^{(2^s+1)2^i} \\ xy \end{pmatrix}$
$(x,y) \mapsto \begin{pmatrix} x^{2^{2s}+2^{3s}} + ax^{2^{2s}}y^{2^s} + by^{2^s+1} \\ xy \end{pmatrix}$
$(x,y) \mapsto \begin{pmatrix} x^{2^s+1} + x^{2^{s+k/2}}y^{2^{k/2}} + axy^{2^s} + by^{2^s+1} \\ xy \end{pmatrix}$
… $xy^{2^s} + y^{2^s+1}$ … $^{2^{2s}}y + y^{2^{2s}+1}$
… $xy^{2^s} + y^{2^s+1}$ … $+ xy^{2^{3s}}$
$(x,y) \mapsto \begin{pmatrix} x^{2^s+1} + by^{2^s+1} \\ x^{2^{s+k/2}}y + \frac{a}{b}xy^{2^{s+k/2}} \end{pmatrix}$
$(x,y) \mapsto \begin{pmatrix} x^{2^s+1} + xy^{2^s} + ay^{2^s+1} \\ x^{2^{2s}+1} + ax^{2^{2s}}y + (1+a)^{2^s}xy^{2^{2s}} + ay^{2^{2s}+1} \end{pmatrix}$
$(x,y,z) \mapsto \begin{pmatrix} x^{2^s+1} + x^{2^s}z + yz^{2^s} \\ x^{2^s}z + y^{2^s+1} \\ xy^{2^s} + y^{2^s}z + z^{2^s+1} \end{pmatrix}$
$(x,y,z) \mapsto \begin{pmatrix} x^{2^s+1} + xy^{2^s} + yz^{2^s} \\ xy^{2^s} + z^{2^s+1} \\ x^{2^s}z + y^{2^s+1} + y^{2^s}z \end{pmatrix}$

Are they related ? equivalent ?

First examples of APN functions

$n = 12 = 3 \times 4 = 2 \times 6$

Power function

[Gold68, Nyberg94]

$$F : \mathbb{F}_{2^{12}} \to \mathbb{F}_{2^{12}} \quad x \mapsto x^3$$

First examples of APN functions

$n = 12 = 3 \times 4 = 2 \times 6$

Power function

[Gold68, Nyberg94]

$$F : \mathbb{F}_{2^{12}} \to \mathbb{F}_{2^{12}} \quad x \mapsto x^3$$

One of the first non-power functions

[BudCarLea08]

$$F(x) = x^3 + \alpha x^{528} = x^3 P(x^{15}) \qquad P = 1 + x^{35}$$

First examples of APN functions

$n = 12 = 3 \times 4 = 2 \times 6$

Power function [Gold68, Nyberg94]

$$F : \mathbb{F}_{2^{12}} \to \mathbb{F}_{2^{12}} \quad x \mapsto x^3$$

One of the first non-power functions [BudCarLea08]

$$F(x) = x^3 + \alpha x^{528} = x^3 P(x^{15}) \qquad P = 1 + x^{35}$$

$\lambda \in \mathbb{F}_{2^4}^*$ (i.e. $\lambda^{15} = 1$). $\qquad F(\lambda) = \lambda^3 P(\lambda^{15}) = \lambda^3 P(1)$

First examples of APN functions

$n = 12 = 3 \times 4 = 2 \times 6$

Power function [Gold68, Nyberg94]

$$F : \mathbb{F}_{2^{12}} \to \mathbb{F}_{2^{12}} \quad x \mapsto x^3$$

One of the first non-power functions [BudCarLea08]

$$F(x) = x^3 + \alpha x^{528} = x^3 P(x^{15}) \qquad P = 1 + x^{35}$$

$\lambda \in \mathbb{F}_{2^4}^*$ (i.e. $\lambda^{15} = 1$). $\quad F(\lambda) = \lambda^3 P(\lambda^{15}) = \lambda^3 P(1)$

- F behaves as $x \mapsto x^3$ on each coset $\gamma \mathbb{F}_{2^4}$

First examples of APN functions

$n = 12 = 3 \times 4 = 2 \times 6$

Power function [Gold68, Nyberg94]

$$F : \mathbb{F}_{2^{12}} \to \mathbb{F}_{2^{12}} \quad x \mapsto x^3$$

One of the first non-power functions [BudCarLea08]

$$F(x) = x^3 + \alpha x^{528} = x^3 P(x^{15}) \qquad P = 1 + x^{35}$$

$\lambda \in \mathbb{F}_{2^4}^*$ (i.e. $\lambda^{15} = 1$). $\quad F(\lambda) = \lambda^3 P(\lambda^{15}) = \lambda^3 P(1)$

- F behaves as $x \mapsto x^3$ on each coset $\gamma \mathbb{F}_{2^4}$
- Multivariate point of view $\quad \widetilde{F} : (\mathbb{F}_{2^4})^3 \to (\mathbb{F}_{2^4})^3 \; (v_1, v_2, v_3) \mapsto \left(\widetilde{F_1}(v), \widetilde{F_2}(v), \widetilde{F_3}(v)\right)$

First examples of APN functions

$n = 12 = 3 \times 4 = 2 \times 6$

Power function [Gold68, Nyberg94]

$$F : \mathbb{F}_{2^{12}} \to \mathbb{F}_{2^{12}} \quad x \mapsto x^3$$

One of the first non-power functions [BudCarLea08]

$$F(x) = x^3 + \alpha x^{528} = x^3 P(x^{15}) \qquad P = 1 + x^{35}$$

$\lambda \in \mathbb{F}_{2^4}^*$ (i.e. $\lambda^{15} = 1$). $\quad F(\lambda) = \lambda^3 P(\lambda^{15}) = \lambda^3 P(1)$

- F behaves as $x \mapsto x^3$ on each coset $\gamma\mathbb{F}_{2^4}$
- Multivariate point of view $\quad \widetilde{F} : (\mathbb{F}_{2^4})^3 \to (\mathbb{F}_{2^4})^3 \; (v_1, v_2, v_3) \mapsto \left(\widetilde{F_1}(v), \widetilde{F_2}(v), \widetilde{F_3}(v)\right)$

$$\widetilde{F}_1(v) = ?v_1^2 v_2 + ?v_1 v_2^2 + ?v_2^3 + ?v_1^2 v_3 + ?v_2^2 v_3 + ?v_1 v_3^2 + ?v_2 v_3^2 + ?v_3^3 \qquad (1 + 2 = 3)$$

All coordinates $\widetilde{F}_i$ are ***homogeneous*** of the ***same*** order 3

First examples of APN functions

$n = 12 = 3 \times 4 = 2 \times 6$

Power function [Gold68, Nyberg94]

$$F : \mathbb{F}_{2^{12}} \to \mathbb{F}_{2^{12}} \quad x \mapsto x^3$$

One of the first non-power functions [BudCarLea08]

$$F(x) = x^3 + \alpha x^{528} = x^3 P(x^{15}) \qquad P = 1 + x^{35}$$

$\lambda \in \mathbb{F}_{2^4}^*$ (i.e. $\lambda^{15} = 1$). $\quad F(\lambda) = \lambda^3 P(\lambda^{15}) = \lambda^3 P(1)$

- F behaves as $x \mapsto x^3$ on each coset $\gamma \mathbb{F}_{2^4}$
- Multivariate point of view $\quad \widetilde{F} : (\mathbb{F}_{2^4})^3 \to (\mathbb{F}_{2^4})^3 \ (v_1, v_2, v_3) \mapsto \left(\widetilde{F_1}(v), \widetilde{F_2}(v), \widetilde{F_3}(v)\right)$

$$\widetilde{F}_1(v) = ?v_1^2 v_2 + ?v_1 v_2^2 + ?v_2^3 + ?v_1^2 v_3 + ?v_2^2 v_3 + ?v_1 v_3^2 + ?v_2 v_3^2 + ?v_3^3 \qquad (1 + 2 = 3)$$

All coordinates $\widetilde{F}_i$ are *homogeneous* of the *same* order 3

One of the first bivariate functions [ZhoPot13]

$$F : \mathbb{F}_{64}^2 \to \mathbb{F}_{64}^2, (x, y) \mapsto (xy, x^3 + ay^3)$$

Power mapping

$$F(x) = x^e$$

$A \circ F \circ B = F$ with $B(x) = \lambda x$, $A(x) = \lambda^{-e} x$ for any $\lambda \in \mathbb{F}_{2^n}^*$

Linear self-equivalence

Power mapping

$$F(x) = x^e$$

$A \circ F \circ B = F$ with $B(x) = \lambda x$, $A(x) = \lambda^{-e} x$ for any $\lambda \in \mathbb{F}_{2^n}^*$

Cyclotomic mapping w.r.t a subfield [Wang07]

$$F(x) = x^e P\left(x^{2^k - 1}\right), n = \ell k$$

$A \circ F \circ B = F$ with $B(x) = \lambda x$, $A(x) = \lambda^{-e} x$ for any $\lambda \in \mathbb{F}_{2^k}^*$

$\widetilde{A} \circ \widetilde{F} \circ \widetilde{B} = \widetilde{F}$ with $\widetilde{B}(v) = (\lambda v_1, \ldots, \lambda v_\ell)$, $\widetilde{A}(v) = (\lambda^{-e} v_1, \ldots, \lambda^{-e} v_\ell)$

Linear self-equivalence

Power mapping

$$F(x) = x^e$$

$A \circ F \circ B = F$ with $B(x) = \lambda x$, $A(x) = \lambda^{-e} x$ for any $\lambda \in \mathbb{F}_{2^n}^*$

Cyclotomic mapping w.r.t a subfield [Wang07]

$$F(x) = x^e P\left(x^{2^k - 1}\right), n = \ell k$$

$A \circ F \circ B = F$ with $B(x) = \lambda x$, $A(x) = \lambda^{-e} x$ for any $\lambda \in \mathbb{F}_{2^k}^*$

$\widetilde{A} \circ \widetilde{F} \circ \widetilde{B} = \widetilde{F}$ with $\widetilde{B}(v) = (\lambda v_1, \ldots, \lambda v_\ell)$, $\widetilde{A}(v) = (\lambda^{-e} v_1, \ldots, \lambda^{-e} v_\ell)$

ℓ-projective mapping [BCP24,Göloğlu22]

$$F \colon \mathbb{F}_{2^k}^\ell \to \mathbb{F}_{2^k}^\ell \ (v_1, \ldots, v_\ell) \mapsto (F_1(v), \ldots, F_\ell(v)),$$

$\forall\, i$, F_i is homogeneous of order e_i.

$A \circ \widetilde{F} \circ B = \widetilde{F}$ with $B(v) = (\lambda v_1, \ldots, \lambda v_\ell)$, $A(v) = (\lambda^{-e_1} v_1, \ldots, \lambda^{-e_\ell} v_\ell)$

Our main result (1/2)

Among the 22 known infinite APN families, 19 consist entirely of *cyclotomic* or *ℓ-projective* mappings, *up to linear equivalence*.

Univariate
$x^{2^s+1} + ax^{2^{(3-i)k+s}+2^{ik}}$
$x^{2^s+1} + ax^{2^{(4-i)k+s}+2^{ik}}$
$ax^{2^k+1} + x^{2^s+1} + x^{2^{s+k}+2^k} + bx^{2^{k+s}+1} + b^{2^k}x^{2^s+2^k}$
$x^3 + a^{-1}\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}(a^3x^9)$
$x^3 + a^{-1}\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^3}}(a^3x^9 + a^6x^{18})$
$x^3 + a^{-1}\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^3}}(a^6x^{18} + a^{12}x^{36})$
$ax^{2^s+1} + a^{2^k}x^{2^{2k}+2^{k+s}} + bx^{2^{2k}+1} + ca^{2^k+1}x^{2^s+2^{k+s}}$
$a^2x^{2^{2k+1}+1} + b^2x^{2^{k+1}+1} + ax^{2^{2k}+2} + bx^{2^k+2} + dx^3$
$x^3 + ax^{2^{s+i}+2^i} + a^2x^{2^{k+1}+2^k} + x^{2^{s+i+k}+2^{i+k}}$
$a\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^k}}(bx^{2^i+1}) + a^{2^k}\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^k}}(cx^{2^s+1})$
$L(x)^{2^k+1} + bx^{2^k+1}$

Our main result (1/2)

Among the 22 known infinite APN families, 19 consist entirely of *cyclotomic* or *ℓ-projective* mappings, *up to linear equivalence*.

Univariate	Observations
$x^{2^s+1} + ax^{2^{(3-i)k+s}+2^{ik}}$	cyclotomic
$x^{2^s+1} + ax^{2^{(4-i)k+s}+2^{ik}}$	cyclotomic
$ax^{2^k+1} + x^{2^s+1} + x^{2^{s+k}+2^k} + bx^{2^{k+s}+1} + b^{2^k}x^{2^s+2^k}$	$\sim_{\mathrm{lin}}$ biprojective
$x^3 + a^{-1}\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}(a^3x^9)$	cyclotomic/($\sim_{\mathrm{lin}}$) frob.
$x^3 + a^{-1}\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^3}}(a^3x^9 + a^6x^{18})$	cyclotomic/($\sim_{\mathrm{lin}}$) frob.
$x^3 + a^{-1}\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^3}}(a^6x^{18} + a^{12}x^{36})$	cyclotomic/($\sim_{\mathrm{lin}}$) frob.
$ax^{2^s+1} + a^{2^k}x^{2^{2k}+2^{k+s}} + bx^{2^{2k}+1} + ca^{2^k+1}x^{2^s+2^{k+s}}$	cyclotomic
$a^2x^{2^{2k+1}+1} + b^2x^{2^{k+1}+1} + ax^{2^{2k}+2} + bx^{2^k+2} + dx^3$	cyclotomic
$x^3 + ax^{2^{s+i}+2^i} + a^2x^{2^{k+1}+2^k} + x^{2^{s+i+k}+2^{i+k}}$	$\sim_{\mathrm{lin}}$ biprojective
$a\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^k}}(bx^{2^i+1}) + a^{2^k}\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^k}}(cx^{2^s+1})$	$\sim_{\mathrm{lin}}$ biprojective
$L(x)^{2^k+1} + bx^{2^k+1}$	?

Among the 22 known infinite APN families, 19 consist entirely of *cyclotomic* or *ℓ-projective* mappings, *up to linear equivalence*.

Multivariate	Observations
$(x,y) \mapsto \begin{pmatrix} x^{2^s+1} + ay^{(2^s+1)2^i} \\ xy \end{pmatrix}$	$\sim_{\text{lin}}$ biprojective
$(x,y) \mapsto \begin{pmatrix} x^{2^{2s}+2^{3s}} + ax^{2^{2s}}y^{2^s} + by^{2^s+1} \\ xy \end{pmatrix}$	$\sim_{\text{lin}}$ biprojective
$(x,y) \mapsto \begin{pmatrix} x^{2^s+1} + x^{2^{s+k/2}}y^{2^{k/2}} + axy^{2^s} + by^{2^s+1} \\ xy \end{pmatrix}$	$\sim_{\text{lin}}$ 4-projective
$(x,y) \mapsto \begin{pmatrix} x^{2^s+1} + xy^{2^s} + y^{2^s+1} \\ x^{2^{2s}+1} + x^{2^{2s}}y + y^{2^{2s}+1} \end{pmatrix}$	biprojective
$(x,y) \mapsto \begin{pmatrix} x^{2^s+1} + xy^{2^s} + y^{2^s+1} \\ x^{2^{3s}}y + xy^{2^{3s}} \end{pmatrix}$	biprojective
$(x,y) \mapsto \begin{pmatrix} x^{2^s+1} + by^{2^s+1} \\ x^{2^{s+k/2}}y + \frac{a}{b}xy^{2^{s+k/2}} \end{pmatrix}$	biprojective
$(x,y) \mapsto \begin{pmatrix} x^{2^s+1} + xy^{2^s} + ay^{2^s+1} \\ x^{2^{2s}+1} + ax^{2^{2s}}y + (1+a)^{2^s}xy^{2^{2s}} + ay^{2^{2s}+1} \end{pmatrix}$	biprojective
$(x,y,z) \mapsto \begin{pmatrix} x^{2^s+1} + x^{2^s}z + yz^{2^s} \\ x^{2^s}z + y^{2^s+1} \\ xy^{2^s} + y^{2^s}z + z^{2^s+1} \end{pmatrix}$	3-projective $\sim_{\text{lin}}$ cyclotomic
$(x,y,z) \mapsto \begin{pmatrix} x^{2^s+1} + xy^{2^s} + yz^{2^s} \\ xy^{2^s} + z^{2^s+1} \\ x^{2^s}z + y^{2^s+1} + y^{2^s}z \end{pmatrix}$	3-projective $\sim_{\text{lin}}$ cyclotomic

Sketch of proof

Recap (Conjugacy, again)

The conjugate of a composition is the composition of the conjugates.

$$F = F_3 \circ F_2 \circ F_1 \quad \iff \quad F^G = F_3^G \circ F_2^G \circ F_1^G$$

Recap (Conjugacy, again)

The conjugate of a composition is the composition of the conjugates.

$$F = F_3 \circ F_2 \circ F_1 \iff F^G = F_3^G \circ F_2^G \circ F_1^G$$

Linear self-equivalence & conjugacy

For any G bijective:

$$F = A \circ F \circ B \iff F^G = A^G \circ F^G \circ B^G$$

Recap (Conjugacy, again)

The conjugate of a composition is the composition of the conjugates.

$$F = F_3 \circ F_2 \circ F_1 \iff F^G = F_3^G \circ F_2^G \circ F_1^G$$

Linear self-equivalence & conjugacy

For any G bijective:

$$F = A \circ F \circ B \iff F^G = A^G \circ F^G \circ B^G$$

If G is linear, A and $G \circ A \circ G^{-1}$ are *similar* and share the same *elementary divisors*

Recap (Conjugacy, again)

The conjugate of a composition is the composition of the conjugates.

$$F = F_3 \circ F_2 \circ F_1 \quad \Longleftrightarrow \quad F^G = F_3^G \circ F_2^G \circ F_1^G$$

Linear self-equivalence & conjugacy

For any G bijective:

$$F = A \circ F \circ B \quad \Longleftrightarrow \quad F^G = A^G \circ F^G \circ B^G$$

If G is linear, A and $G \circ A \circ G^{-1}$ are ***similar*** and share the same ***elementary divisors***

Recap (Cyclotomic mapping)

$$F(x) = x^e P\left(x^{2^k-1}\right), n = \ell k$$

Univariate: $A \circ F \circ B = F$ with $B(x) = \lambda x$, $A(x) = \lambda^{-e} x$ for any $\lambda \in \mathbb{F}_{2^k}^*$

Multivariate: $\widetilde{A} \circ \widetilde{F} \circ \widetilde{B} = \widetilde{F}$ with $\widetilde{B}(v) = (\lambda v_1, \ldots, \lambda v_\ell)$, $\widetilde{A}(v) = (\lambda^{-e} v_1, \ldots, \lambda^{-e} v_\ell)$

Take away

Theorem

Among the 22 known infinite APN families, 19 consist entirely of *cyclotomic* or *ℓ-projective* mappings, *up to linear equivalence*.

Sum up

- Characterization of *very specific* self-equivalences
- Unify most of the approaches
- Linearly self-equivalent APN functions from *computer searches* are generally *less structured*. [BeiBriLea21,BeiLea22]

Take away

Theorem

Among the 22 known infinite APN families, 19 consist entirely of *cyclotomic* or *ℓ-projective* mappings, *up to linear equivalence*.

Sum up

- Characterization of *very specific* self-equivalences
- Unify most of the approaches
- Linearly self-equivalent APN functions from *computer searches* are generally *less structured*. [BeiBriLea21,BeiLea22]

Open questions

- Link between self-equivalence and APN-ness [BeiBriLea21, Conjecture 1]
- Cyclotomic mappings outside the known classes? (from *non-quadratic* APN monomial)
- Projective mappings outside the known classes? (with *more* coordinates)

Conclusion: alternative representations in symmetric cryptography

$$E_k = F_{k(R-1)} \circ \ldots \circ F_{k(1)} \circ F_{k(0)} \quad \Longleftrightarrow \quad E_k^G = F^G_{k(R-1)} \circ \ldots \circ F^G_{k(1)} \circ F^G_{k(0)}$$

In cryptanalysis

- New vector of attacks
- New security criteria are needed

$$F = A \circ F \circ B \quad \Longleftrightarrow \quad F^G = A^G \circ F^G \circ B^G$$

In design

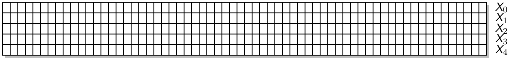
- Better understanding of optimal objects
- New directions to find new instances ?

V - Appendix

The permutation

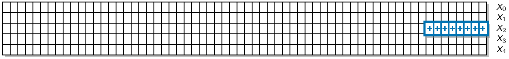
A confusion/diffusion structure...

The state

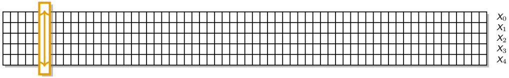


$$p = p_L \circ p_S \circ p_C$$

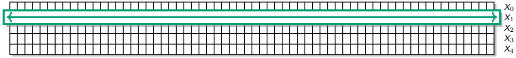
The constant addition p_C



The substitution layer p_S



The linear layer p_L



...studied algebraically

$$
\begin{aligned}
y_0 &= x_4x_1 + x_3 + x_2x_1 + x_2 + x_1x_0 + x_1 + x_0 \\
y_1 &= x_4 + x_3x_2 + x_3x_1 + x_3 + x_2x_1 + x_2 + x_1 + x_0 \\
y_2 &= x_4x_3 + x_4 + x_2 + x_1 + 1 \\
y_3 &= x_4x_0 + x_4 + x_3x_0 + x_3 + x_2 + x_1 + x_0 \\
y_4 &= x_4x_1 + x_4 + x_3 + x_1x_0 + x_1
\end{aligned}
$$

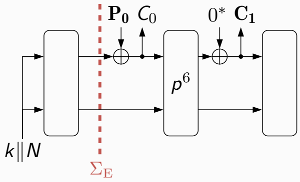
Algebraic Normal Form (ANF) of the S-box

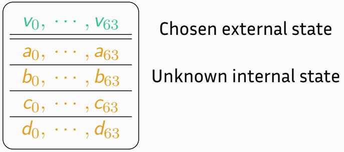
$$
\begin{aligned}
X_0 &= X_0 \oplus (X_0 \ggg 19) \oplus (X_0 \ggg 28) \\
X_1 &= X_1 \oplus (X_1 \ggg 61) \oplus (X_1 \ggg 39) \\
X_2 &= X_2 \oplus (X_2 \ggg 1) \oplus (X_2 \ggg 6) \\
X_3 &= X_3 \oplus (X_3 \ggg 10) \oplus (X_3 \ggg 17) \\
X_4 &= X_4 \oplus (X_4 \ggg 7) \oplus (X_4 \ggg 41)
\end{aligned}
$$

ANF of the linear layer p_L

The nonce-misuse scenario

Simplified setting of Ascon-128



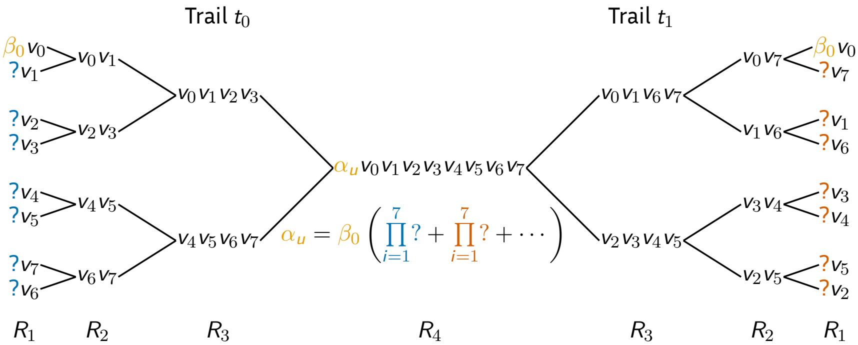


Σ_E State before encryption

- Many reuse of the same (k, N) pair.
- State recovery = compromised confidentiality without interaction.
- No trivial key-recovery nor forgery in that case.
- Different from the generic attack [ACNS:VauViz18].

Conditional cube

- We look for α_u with a simple divisor: β_0.
- α_u mostly unknown, but we still get: $\alpha_u = 1 \implies \beta_0 = 1$.
- If β_0 is linear, we get a linear system.



Choosing conditional cubes by forcing linear divisors

1st round

$$\begin{array}{c} v_0 \\ \hline a_0 \\ b_0 \\ c_0 \\ d_0 \end{array} \xrightarrow[S_1]{} \begin{array}{c} (a_0+1)v_0+\cdots \\ \hline v_0+\cdots \\ \hline \cdots \\ \hline (c_0+d_0+1)v_0+\cdots \\ \hline a_0 v_0+\cdots \end{array} \quad \begin{array}{l} \longleftarrow \beta_0 := a_0+1 \\ \\ \\ \longleftarrow \gamma_0 := c_0+d_0+1 \\ \\ \end{array}$$

Choosing conditional cubes by forcing linear divisors

1st round

$$\begin{array}{c} v_0 \\ \hline a_0 \\ b_0 \\ c_0 \\ d_0 \end{array} \xrightarrow{S_1} \begin{array}{c} (a_0+1)v_0+\cdots \\ \hline v_0+\cdots \\ \hline \cdots \\ \hline (c_0+d_0+1)v_0+\cdots \\ \hline a_0 v_0+\cdots \end{array}$$

$\longleftarrow \beta_0 := a_0 + 1$

$\longleftarrow \gamma_0 := c_0 + d_0 + 1$

2nd round

- For any $v_0 v_i$, $i \neq 0$: $\beta_0 P + 1Q + \gamma_0 R + (\beta_0 + 1)S$.
- But for some i: $\beta_0 P$ or $\gamma_0 R$.

Choosing conditional cubes by forcing linear divisors

6th round

- With chosen u, $\alpha_{u,\,j} = \beta_0(\dots) + \gamma_0(\dots)$, for all output coordinates.

Choosing conditional cubes by forcing linear divisors

6th round

- With chosen u, $\alpha_{u,\,j} = \beta_0(\ldots) + \gamma_0(\ldots)$, for all output coordinates.
- $(\alpha_{u,0}, \cdots, \alpha_{u,63}) \neq (0, \cdots, 0) \implies \beta_0 = 1$ or $\gamma_0 = 1$

6th round

- With chosen u, $\alpha_{u,j} = \beta_0(\ldots) + \gamma_0(\ldots)$, for all output coordinates.
- $(\alpha_{u,0}, \cdots, \alpha_{u,63}) \neq (0, \cdots, 0) \implies \beta_0 = 1$ or $\gamma_0 = 1$
- In practice, reciprocal also true! $[\alpha_{u,j} = 0, \forall j] \implies \beta_0 = 0$ and $\gamma_0 = 0$

$$\begin{tikzcd}
x_0 \arrow[r, "R_0"] \arrow[d, "\Delta_0"', "\mathcal{A}^\star"] & x_1 \arrow[r, dashed] \arrow[d, "\Delta_1"', "\mathcal{A}^\star"] & x_{r-1} \arrow[r, "R_{r-1}"] \arrow[d, "\Delta_{r-1}"', "\mathcal{A}^\star"] & E(x_0) \arrow[d, "\Delta_r"', "\mathcal{A}^\star"] \\
z_0 \arrow[r, "R_0"'] & z_1 \arrow[r, dashed] & z_{r-1} \arrow[r, "R_{r-1}"'] & E(z_0)
\end{tikzcd}$$

$$\Delta_i := x_i \oplus z_i = x_i \oplus \mathcal{A}^\star(x_i)$$

Surprising differential interpretation

$\delta = \texttt{0xf}, \quad \delta' = \texttt{0xa}.$

$$\forall\, \Delta \in \{\delta, \delta'\}^{16},\ \mathbb{P}_{x \xleftarrow{\$} X}(x + \mathcal{A}^\star(x) = \Delta) = 2^{-16} \iff (x, x + \Delta) = (x, \mathcal{A}^\star(x)) \text{ with proba } 2^{-16}$$

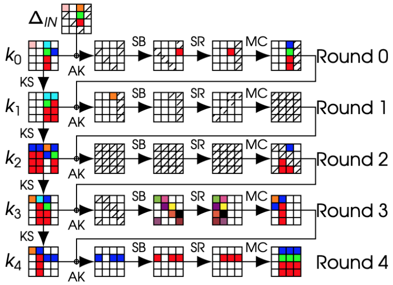
$$\Delta \xrightarrow{2^{-16}} \mathcal{A}^\star \xrightarrow{1} \cdots \xrightarrow{1} \mathcal{A}^\star \xrightarrow{2^{-16}} \Delta$$

Recap

If k is **weak**:

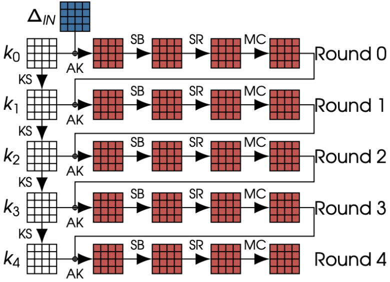
- $\mathbb{P}_{x \xleftarrow{\$} X}(\Delta \to \Delta') = 2^{-32}$ for any $\Delta, \Delta' \in \{\delta, \delta'\}^{16}$.
- $\mathbb{P}_{x \xleftarrow{\$} X}(\Delta \to \{\delta, \delta'\}^{16}) = 2^{-16}$ for any $\Delta \in \{\delta, \delta'\}^{16}$.
- For any number of rounds, activate all S-boxes.

Standard case : quite low $\mathbb{P}_{k,x}$



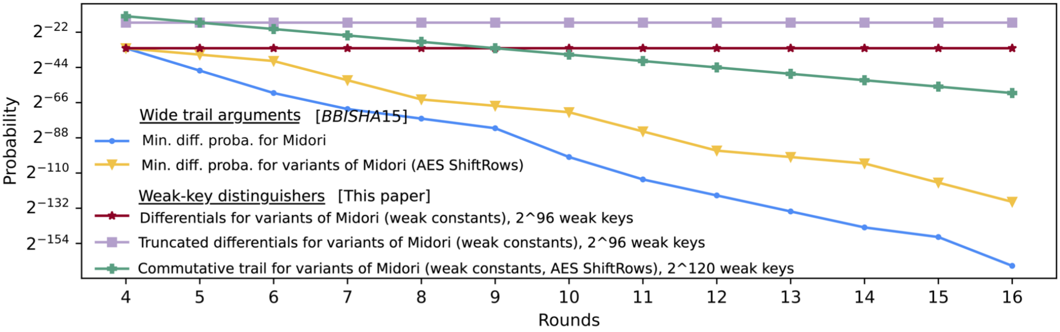
Part of 9-round chosen-key distinguisher for AES-128.

This work: high $\mathbb{P}_x$ for some k



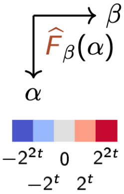
0xf

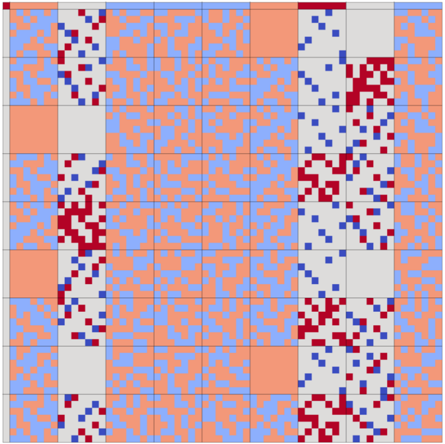
Midori



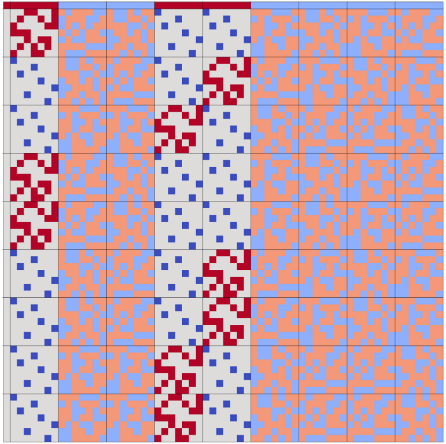
Probability
2^{-22}
2^{-44}
2^{-66}
2^{-88}
2^{-110}
2^{-132}
2^{-154}
Wide trail arguments [BBISHA15]
Min. diff. proba. for Midori
Min. diff. proba. for variants of Midori (AES ShiftRows)
Weak-key distinguishers [This paper]
Differentials for variants of Midori (weak constants), 2^96 weak keys
Truncated differentials for variants of Midori (weak constants), 2^96 weak keys
Commutative trail for variants of Midori (weak constants, AES ShiftRows), 2^120 weak keys
4 5 6 7 8 9 10 11 12 13 14 15 16
Rounds

Walsh spectrum of cyclotomic mappings





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



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

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

Generalizing π

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

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

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 Π

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

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

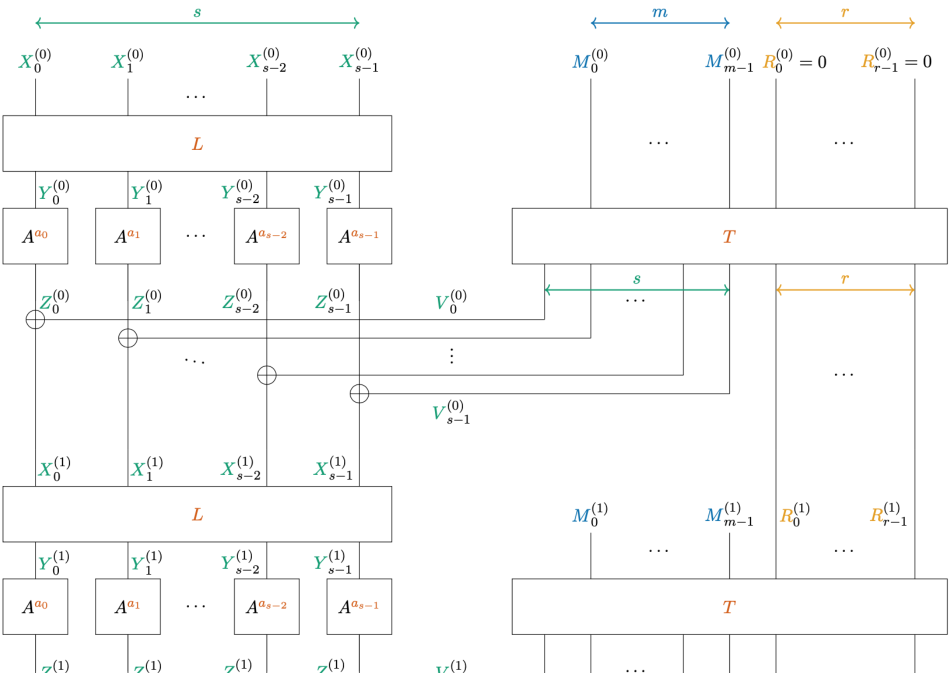
ID	Functions	Obs.	Ref.
(CLV22b)	$(x,y) \mapsto \begin{pmatrix} x^3+xy+xy^2+ay^3 \\ x^5+xy+ax^2y^2+ax^4y+(1+a)^2xy^4+ay^5 \end{pmatrix}$	?	[CLV22]
(LZLQ22b)	$(x,y) \mapsto \begin{pmatrix} x^3+xy^2+y^3+xy \\ x^5+x^4y+y^5+xy+x^2y^2 \end{pmatrix}$	?	[Li+22]
(LZLQ22a)	$L(x)^{2^k+1}+bx^{2^k+1}$	?	[Li+22]

Table 6.4: Remaining infinite families to classify.

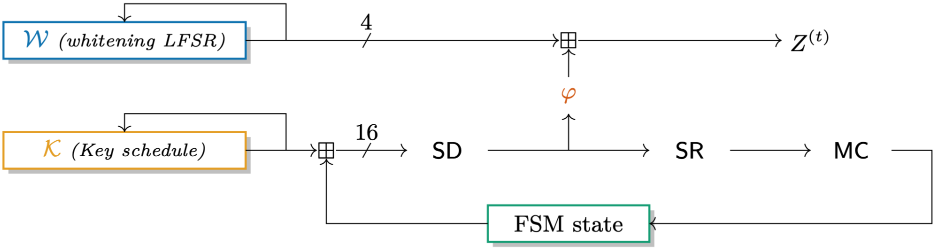
ID	GCD for Walsh spectrum of F	GCDs for Walsh and differential spectra of the ortho-derivative π_F	Number of mappings
BL-1	340	(1, 3)	8667
BL-2	2	(1, 3)	3206
BL-3	340	(1, 6)	403
BL-4	4	(1, 3)	311
BL-5	340	(1, 1)	204
BL-6	2	(1, 1)	45
BL-7	340	(1, 12)	26
BL-8	4	(1, 6)	11
BL-9	4	(1, 1)	11
BL-10	340	(1, 15)	10
BL-11	340	(1, 2)	7
BL-12	1	(1, 3)	4
BL-13	340	(1, 24)	3
BL-14	2	(1, 15)	3
BL-15	2	(1, 6)	3
BL-16	340	(1, 5)	2
BL-17	340	(1, 30)	2
BL-18	340	(5, 15)	2

QAM-1	340	(1, 1)	12201
QAM-2	2	(1, 1)	796
QAM-3	340	(1, 2)	359
QAM-4	340	(1, 3)	160
QAM-5	340	(1, 4)	17
QAM-6	2	(1, 3)	14
QAM-7	4	(1, 1)	14
QAM-8	340	(1, 6)	8
QAM-9	340	(1, 5)	8
QAM-10	340	(1, 12)	3
QAM-11	4	(1, 3)	2
QAM-12	340	(1, 10)	2
QAM-13	340	(85, 510)	1
QAM-14	340	(85, 1020)	1
QAM-15	340	(5, 60)	1
QAM-16	340	(2, 2)	1
QAM-17	340	(1, 24)	1
QAM-18	340	(1, 8)	1
QAM-19	2	(1, 2)	1

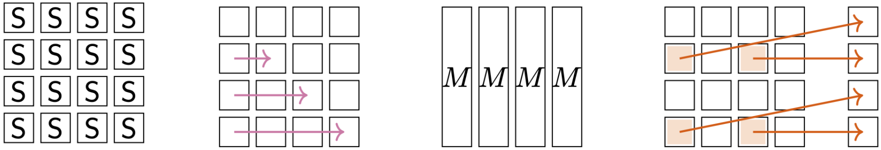
- 7 non-trivial automorphisms
- Elementary divisors for $\mathcal{L}$: $(X+1)$multiplicity 2, $(X+1)^2$ multiplicity 5
- If $\mathcal{L} \sim \mathrm{diag}(A, B)$ then $(X+1)^2$ is among the elementary divisors of $A \implies \min(A) = (X+1)^2$ not irreducible.
- Cannot be cyclotomic mappings nor ℓ-projective mappings.



s
m
r
$X_0^{(0)}$
$X_1^{(0)}$
$X_{s-2}^{(0)}$
$X_{s-1}^{(0)}$
$M_0^{(0)}$
$M_{m-1}^{(0)}$
$R_0^{(0)} = 0$
$R_{r-1}^{(0)} = 0$
L
$Y_0^{(0)}$
$Y_1^{(0)}$
$Y_{s-2}^{(0)}$
$Y_{s-1}^{(0)}$
A^{a_0}
A^{a_1}
$A^{a_{s-2}}$
$A^{a_{s-1}}$
T
$Z_0^{(0)}$
$Z_1^{(0)}$
$Z_{s-2}^{(0)}$
$Z_{s-1}^{(0)}$
$V_0^{(0)}$
$V_{s-1}^{(0)}$
$X_0^{(1)}$
$X_1^{(1)}$
$X_{s-2}^{(1)}$
$X_{s-1}^{(1)}$
$M_0^{(1)}$
$M_{m-1}^{(1)}$
$R_0^{(1)}$
$R_{r-1}^{(1)}$
$Y_0^{(1)}$
$Y_1^{(1)}$
$Y_{s-2}^{(1)}$
$Y_{s-1}^{(1)}$



(a) General structure (rectangles correspond to registers).



(b) SD. (c) SR. (d) MC. (e) φ.

Figure 7.3: A high level view of `Transistor`.