Differential cryptanalysis of conjugate ciphers

Jules Baudrin

based on joint works with C. Beierle, P. Felke, G. Leander,
P. Neumann, L. Perrin & L. Stennes

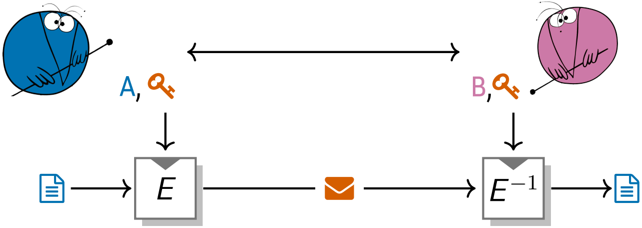
UCLouvain

Rennes cryptography seminar, February 7th, 2025

Symmetric encryption

Goal

Ensure confidentiality



Constraints

- Secure
- Easily implemented
- Arbitrary-long messages

Primitives

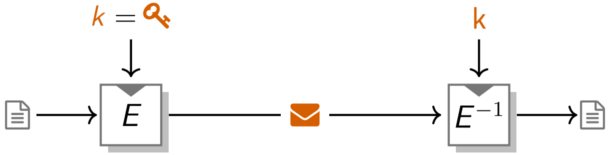
Definition (Primitive)

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

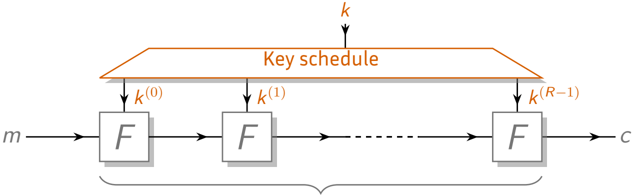


Building a block cipher

Recap (Block cipher)

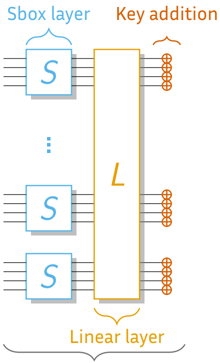
A family of bijections $\mathcal{E} = \left(E_k : \mathbb{F}_2^n \xrightarrow{\sim} \mathbb{F}_2^n\right)_{k \in \mathbb{F}_2^\kappa}$. Should be *efficient* and *secure*.

Iterated construction



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

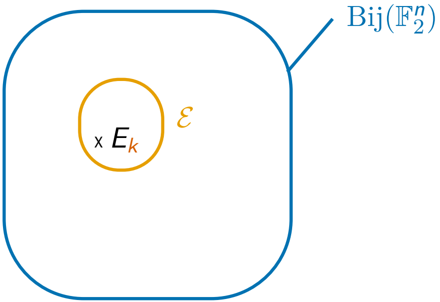
Substitution Permutation Network



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

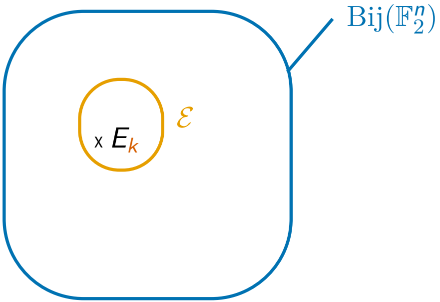
Recap (Block cipher)

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 $[\, F \xleftarrow{\$} \mathrm{Bij}(\mathbb{F}_2^n) \,]$.

Outline

II - Differential cryptanalysis

Differential distinguisher

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.

$$\begin{tikzcd} x \arrow[d, leftrightarrow, "\Delta^{\mathrm{in}}"] \\ y \end{tikzcd} \qquad\qquad \begin{tikzcd} E_k(x) \arrow[d, leftrightarrow, "\Delta^{\mathrm{out}}"] \\ E_k(y) \end{tikzcd}$$

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.

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

For a random bijection F

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

Recap

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

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

For a random bijection F

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

Differential distinguisher [BihSha91]

$\Delta^{\text{in}} \neq 0, \Delta^{\text{out}}$ s.t for many k, $E_k(x + \Delta^{\text{in}}) + E_k(x) = \Delta^{\text{out}}$ 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 $i \geq 0$.

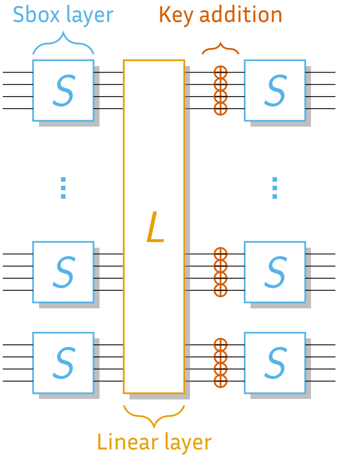
$$\begin{tikzcd} x^{(0)} \arrow[r, "F_{k^{(0)}}"] \arrow[d, leftrightarrow, "\Delta^{\text{in}}"] & x^{(1)} \arrow[r, dashed] \arrow[d, leftrightarrow, "\Delta^{(1)}"] & x^{(R-1)} \arrow[r, "F_{k^{(R-1)}}"] \arrow[d, leftrightarrow, "\Delta^{(R-1)}"] & E_k(x^{(0)}) \arrow[d, leftrightarrow, "\Delta^{\text{out}}"]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

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

On average over all key sequences [LaiMasMur91]

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

Resisting differential cryptanalysis



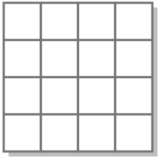
As a designer [DaeRij00]

- 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

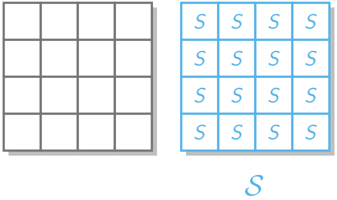
Advanced Encryption Standard (AES)



AES [DaeRij00]

- 4×4 matrix of bytes = 128-bit state

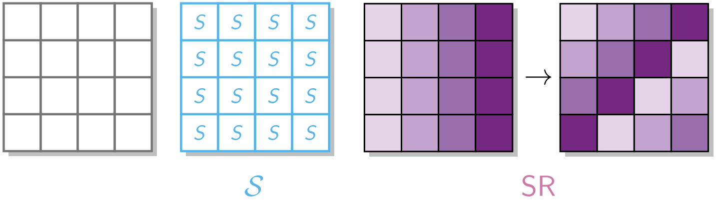
Advanced Encryption Standard (AES)



AES [DaeRij00]

- 4×4 matrix of bytes = 128-bit state

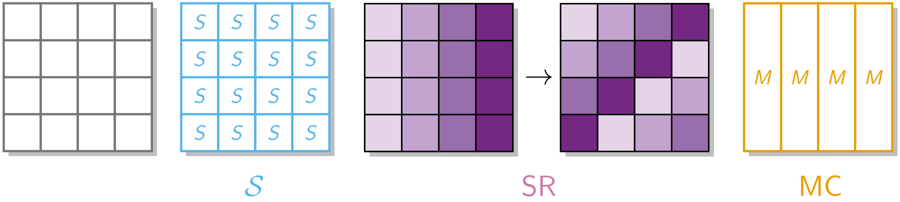
Advanced Encryption Standard (AES)



AES [DaeRij00]

- 4×4 matrix of bytes = 128-bit state

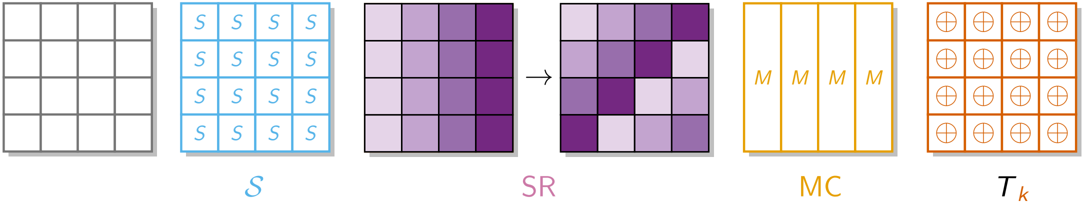
Advanced Encryption Standard (AES)



AES [DaeRij00]

- 4×4 matrix of bytes = 128-bit state

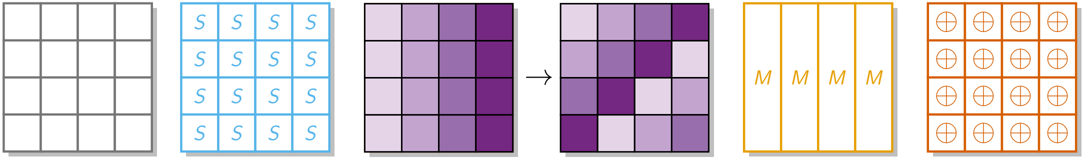
Advanced Encryption Standard (AES)



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)

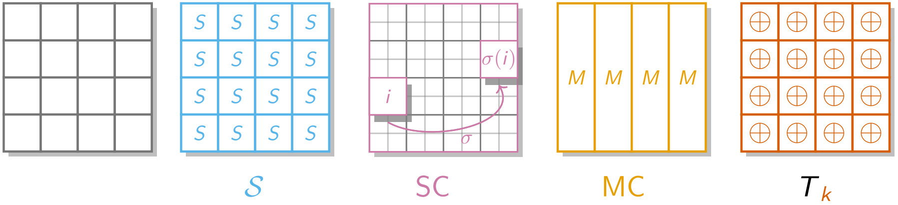


$\mathcal{S}$ SR MC T_k

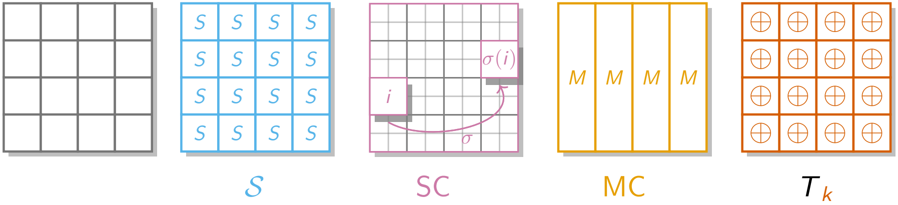
AES [DaeRij00]

- 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.
- $\delta(S) = 4$.
- Structured linear layer MC $\circ$ 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



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.
- $\delta(S) = 4$.
- $\mathbb{E}\left[\Delta^{(0)} \xrightarrow{F^{(0)}} \Delta^{(1)} \to \dots \xrightarrow{F^{(6)}} \Delta^{(7)}\right] \le 2^{-70}$.

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***.

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

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***.

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

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

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

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

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

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 $\mathcal{L}(F_1) = \mathcal{L}(F_2)$

Linear VS non-linear change of variables

Recap

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

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

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 $\mathcal{L}(F_1) = \mathcal{L}(F_2)$

Corollary

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

$\Longrightarrow$ Fine-grained arguments are needed.

- If G non-linear ?

$\Longrightarrow$ Linear attack cf. [BeiCanLea18]

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

Non-linear change of variables (1/3)

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

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

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 (1/3)

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

Main problem

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

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

The usual case

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

$$T_k(x + \Delta) = x + \Delta + k = T_k(x) + \Delta$$

Non-linear change of variables (1/3)

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

Main problem

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

The usual case

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

$$T_k(x + \Delta) = x + \Delta + k = T_k(x) + \Delta$$

A possible solution

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

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

Recap

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

Non-linear change of variables (2/3)

Recap

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

Weak-key space

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

$$\mathbb{P}\left[\Delta \xrightarrow{T_k^G} \Delta\right] = 1 \quad \iff \quad \forall\, x,\ T_k^G(x) + T_k^G(x+\Delta) = \Delta$$

Non-linear change of variables (2/3)

Recap

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

Weak-key space

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

$$\mathbb{P}\left[\Delta \xrightarrow{T_k^G} \Delta\right] = 1 \quad \Longleftrightarrow \quad \forall\, x,\ T_k^G(x) + T_k^G(x + \Delta) = \Delta$$

Definition (Derivative)

The function $D_\Delta F : x \mapsto F(x) + F(x + \Delta)$ is the *derivative* of F along the direction Δ.

Non-linear change of variables (2/3)

Recap

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

Weak-key space

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

$$\mathbb{P}\left[\Delta \xrightarrow{T_k^G} \Delta\right] = 1 \iff \forall\, x,\ T_k^G(x) + T_k^G(x+\Delta) = \Delta$$

Definition (Derivative)

The function $D_\Delta F : x \mapsto F(x) + F(x+\Delta)$ is the ***derivative*** of F along the direction Δ.

$$\mathbb{P}\left[\Delta \xrightarrow{T_k^G} \Delta\right] = 1 \iff D_\Delta T_k^G \text{ is constant}$$

Non-linear change of variables (3/3)

Intuition

T_k^G with constant derivatives $\rightsquigarrow$ $T_k^G = G \circ T_k \circ G^{-1}$ somehow close to be linear.

Non-linear change of variables (3/3)

Intuition

T_k^G with constant derivatives $\rightsquigarrow$ $T_k^G = G \circ T_k \circ G^{-1}$ somehow close to be linear.

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 (3/3)

Intuition

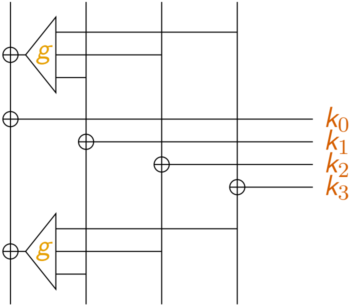
T_k^G with constant derivatives $\rightsquigarrow$ $T_k^G = G \circ T_k \circ G^{-1}$ somehow close to be linear.

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 (3/3)

Intuition

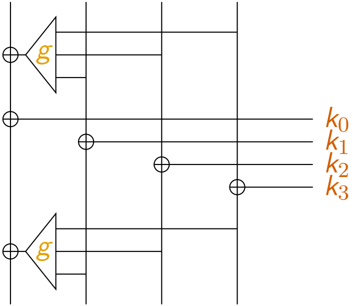
T_k^G with constant derivatives $\rightsquigarrow$ $T_k^G = G \circ T_k \circ G^{-1}$ somehow close to be linear.

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 $\mathbb{P}\left[\Delta \xrightarrow{S^G} \Delta\right] = 1$ $\mathbb{P}\left[\nabla \xrightarrow{\mathcal{S}^{\mathcal{G}}} \nabla\right] = 1.$
$\nabla = (\Delta, \ldots, \Delta)$.

Sbox

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

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

Linear layer

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

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

The case of Midori

Sbox

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

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

Linear layer

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

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

Probability-1 distinguisher for infinitely many rounds*

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

$\star$ 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

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

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

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

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

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

Equivalent points of view

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

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

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

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

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

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*** $F \circ \left(G^{-1} \circ T_{\Delta^{\mathrm{in}}} \circ G\right) = \left(G^{-1} \circ T_{\Delta^{\mathrm{out}}} \circ G\right) \circ F$
  $G^{-1} T_{\Delta} G$ is an addition, up to a change of variables. [CivBloSal19, CalCivInv24]

Benefits from each point of view

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

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

Differential cryptanalysis of conjugates *makes sense*

Theorem (Many fruitful points of view)

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

Open questions

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

IV - Relationship with standard differential cryptanalysis

Recap (Commutative interpretation for "almost"-Midori)

Under weak-key hypothesis, there exists an affine bijective mapping $\mathcal{A}$ such that:

$$\mathcal{A} \circ F = F \circ \mathcal{A} \quad \text{for every layer } F.$$

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

From commutative cryptanalysis back to differential cryptanalysis

Recap (Commutative interpretation for “almost”-Midori)

Under weak-key hypothesis, there exists an affine bijective mapping $\mathcal{A}$ such that:

$$\mathcal{A} \circ F = F \circ \mathcal{A} \quad \text{for every layer } F.$$

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

Differential cryptanalysis

Commutative cryptanalysis restricted to $\mathcal{A}(x) = \mathrm{Id}(x) + \Delta$

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

Differential interpretation of a commutative distinguisher

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

$$\Delta^{(i)} := x^{(i)} \oplus y^{(i)} = x^{(i)} \oplus \mathcal{A}(x^{(i)})$$

Differential interpretation of a commutative distinguisher

$$\begin{array}{ccccccc}
x^{(0)} & \xrightarrow{F_{k^{(0)}}} & x^{(1)} & \dashrightarrow & x^{(R-1)} & \xrightarrow{F_{k^{(R-1)}}} & E_k(x^{(0)}) \\
\Delta^{(0)} \big\downarrow \mathcal{A} & & \Delta^{(1)} \big\downarrow \mathcal{A} & & \Delta^{(R-1)} \big\downarrow \mathcal{A} & & \Delta^{(R)} \big\downarrow \mathcal{A} \\
y^{(0)} & \xrightarrow[F_{k^{(0)}}]{} & y^{(1)} & \dashrightarrow & y^{(R-1)} & \xrightarrow[F_{k^{(R-1)}}]{} & E_k(y^{(0)})
\end{array}$$

$$\Delta^{(i)} := x^{(i)} \oplus y^{(i)} = x^{(i)} \oplus \mathcal{A}(x^{(i)})$$

Observation

Let $C : x \mapsto x \oplus A(x)$. Then $C(\mathbb{F}_2^4) = \{\delta, \delta'\}$ where $\delta \neq \delta'$.

$$\forall\, \Delta \in \{\delta, \delta'\}^{16},\ \mathbb{P}_{x \xleftarrow{\$} \mathbb{F}_2^{64}} (x + \mathcal{A}(x) = \Delta) = 2^{-16}$$

Differential interpretation of a commutative distinguisher

$$\begin{array}{ccccccc}
x^{(0)} & \xrightarrow{F_{k^{(0)}}} & x^{(1)} & \dashrightarrow & x^{(R-1)} & \xrightarrow{F_{k^{(R-1)}}} & E_k(x^{(0)}) \\
\Delta^{(0)} \Big\downarrow \mathcal{A} & & \Delta^{(1)} \Big\downarrow \mathcal{A} & & \Delta^{(R-1)} \Big\downarrow \mathcal{A} & & \Delta^{(R)} \Big\downarrow \mathcal{A} \\
y^{(0)} & \xrightarrow[F_{k^{(0)}}]{} & y^{(1)} & \dashrightarrow & y^{(R-1)} & \xrightarrow[F_{k^{(R-1)}}]{} & E_k(y^{(0)})
\end{array}$$

$$\Delta^{(i)} := x^{(i)} \oplus y^{(i)} = x^{(i)} \oplus \mathcal{A}(x^{(i)})$$

Observation

Let $C : x \mapsto x \oplus \mathcal{A}(x)$. Then $C(\mathbb{F}_2^4) = \{\delta, \delta'\}$ where $\delta \neq \delta'$.

$$\forall\, \Delta \in \{\delta, \delta'\}^{16},\ \mathbb{P}_{x \xleftarrow{\$} \mathbb{F}_2^{64}} (x + \mathcal{A}(x) = \Delta) = 2^{-16}$$

Surprising differential interpretation

A differential pair $(x, x + \Delta)$ coincides with a commutative pair $(x, \mathcal{A}(x))$ with proba 2^{-16}

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

Weak-key differential interpretation

Recap

Under weak-key hypothesis:

- $\mathbb{P}_{x \xleftarrow{\$} X}\left(\Delta \to \{\delta, \delta'\}^{16}\right) \geq 2^{-16}$ for any $\Delta \in \{\delta, \delta'\}^{16}$.
- If output differences are uniformly distributed, then: $\mathbb{P}_{x \xleftarrow{\$} X}(\Delta \to \Delta') \approx 2^{-32}$ for any $\Delta, \Delta' \in \{\delta, \delta'\}^{16}$
- Holds for *infinitely many rounds* !

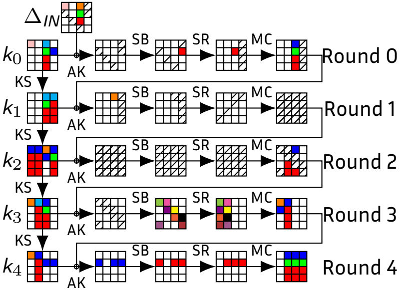
Weak-key differential interpretation

Recap

Under weak-key hypothesis:

- $\mathbb{P}_{x \xleftarrow{\$} X}\left(\Delta \to \{\delta, \delta'\}^{16}\right) \geq 2^{-16}$ for any $\Delta \in \{\delta, \delta'\}^{16}$.
- If output differences are uniformly distributed, then: $\mathbb{P}_{x \xleftarrow{\$} X}(\Delta \to \Delta') \approx 2^{-32}$ for any $\Delta, \Delta' \in \{\delta, \delta'\}^{16}$
- Holds for *infinitely many rounds* !

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



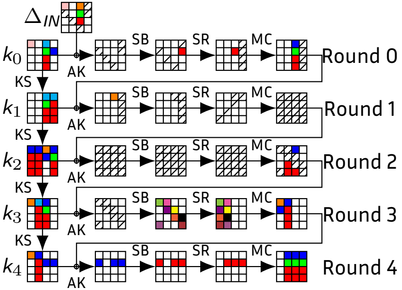
Weak-key differential interpretation

Recap

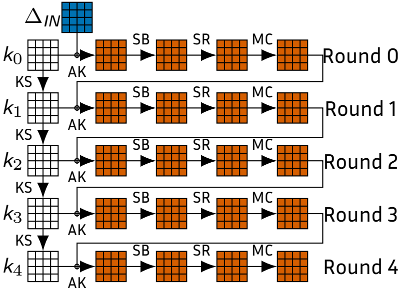
Under weak-key hypothesis:

- $\mathbb{P}_{x \xleftarrow{\$} X}\left(\Delta \rightarrow \{\delta, \delta'\}^{16}\right) \geq 2^{-16}$ for any $\Delta \in \{\delta, \delta'\}^{16}$.
- If output differences are uniformly distributed, then: $\mathbb{P}_{x \xleftarrow{\$} X}\left(\Delta \rightarrow \Delta'\right) \approx 2^{-32}$ for any $\Delta, \Delta' \in \{\delta, \delta'\}^{16}$
- Holds for *infinitely many rounds* !

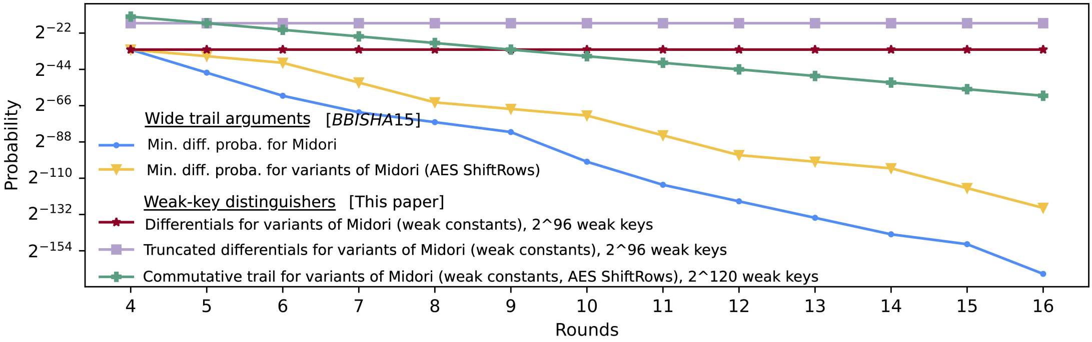
Standard case : *quite low* $\mathbb{P}_{k,x}$



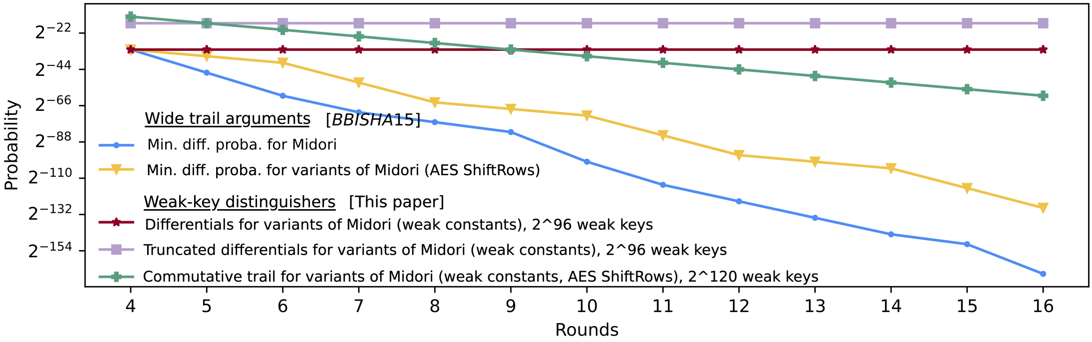
This work: *high* $\mathbb{P}_x$ for *some* k



Weak-key Differential interpretation, part 2



Weak-key Differential interpretation, part 2



Caution

- *Same observations* for the CAESAR candidate SCREAM.
- *Same idea* can be used to *hide* probability-1 differential trails. [C:BFLNS23]

Good news

Probability-1 commutative trails can be *automatically* detected !

Take away

Differential cryptanalysis

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

Systematization of change of variables in cryptanalysis?

- Linear using non-linear G [BeiCanLea18]
- Differential using non-linear G [BFLNPS23,BBFLNPS24]
- Integral using linear G [DerFou20,DerFouLam20,HebLamLeaTod21]

Change of variables in design?

Classification of known optimal functions w.r.t differential cryptanalysis [BCanPer24]