Commutative Cryptanalysis as a Generalization of Differential Cryptanalysis

WCC 2024, June 17 – 21, 2024

Christof Beierle

RUHR UNIVERSITÄT BOCHUM

Gefördert durch Deutsche Forschungsgemeinschaft

CASA — Cyber Security in the Age of Large-Scale Adversaries

Horst Görtz Institut

This talk

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

- J. Baudrin, P. Felke, G. Leander, P. Neumann, L. Perrin, L. Stennes. Commutative Cryptanalysis Made Practical. IACR Transactions on Symmetric Cryptology, 2023(4), 299–329, 2023
- J. Baudrin, C. Beierle, P. Felke, G. Leander, P. Neumann, L. Perrin, L. Stennes. On a Generalization of Differential Uniformity for Commutative Cryptanalysis (in preparation)

Preliminaries

- Throughout this talk, let $G = (G, +)$ be a finite abelian group
- For each $\gamma \in G$, the group structure allows to define the bijective mapping

$$T_\gamma \colon G \mapsto G, x \mapsto x + \gamma,$$

called translation by γ

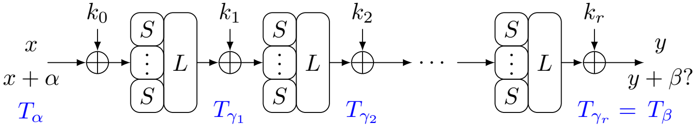
Differential Uniformity of S-boxes and Differential Cryptanalysis

Differential Uniformity [Nyberg, '93]

Let $S\colon G \to G$. The differential uniformity of S is

$$\delta_S := \max_{\substack{\alpha\in G\setminus\{0\}\\ \beta\in G}} |\{x \in G \mid S\circ T_\alpha(x) = T_\beta\circ S(x)\}| = \max_{\substack{\alpha\in G\setminus\{0\}\\ \beta\in G}} |\{x \in G \mid S(x+\alpha)-S(x) = \beta\}|.$$

- widely-studied notion, of mathematical interest (e.g., APN functions, planar functions)
- measures resistance against differential cryptanalysis of ciphers (originally $G = \mathbb{F}_2^n$).
- choose S-box S with small δ_S, argue resistance with wide-trail strategy [Daemen '95]



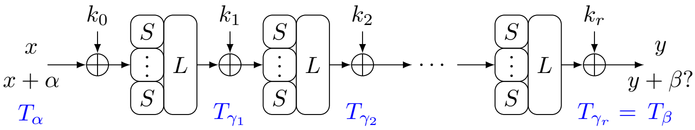
Differential Uniformity of S-boxes and Differential Cryptanalysis

Differential Uniformity [Nyberg, '93]

Let $S\colon G \to G$. The differential uniformity of S is

$$\delta_S := \max_{\substack{\alpha \in G\setminus\{0\}\\ \beta\in G}} |\{x \in G \mid S \circ T_\alpha(x) = T_\beta \circ S(x)\}| = \max_{\substack{\alpha \in G\setminus\{0\}\\ \beta\in G}} |\{x \in G \mid S(x+\alpha) - S(x) = \beta\}|.$$

- widely-studied notion, of mathematical interest (e.g., APN functions, planar functions)
- measures resistance against differential cryptanalysis of ciphers (originally $G = \mathbb{F}_2^n$).
- choose S-box S with small δ_S, argue resistance with wide-trail strategy [Daemen '95]



A Generalization of Differential Uniformity

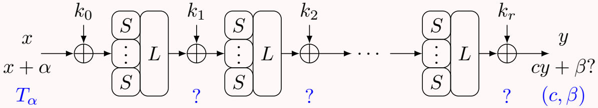
c-Differential Uniformity ($G = \mathbb{F}_{p^n}$) [Ellingsen, Felke, Riera, Stănică, Tkachenko]

Let $S\colon \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ and $c \in \mathbb{F}_{p^n}^*$. The c-differential uniformity of S is

$$ {}_c\delta_S := \max_{\alpha,\beta \in \mathbb{F}_{p^n}, \alpha \neq 0 \text{ if } c=1} \left|\{x \in \mathbb{F}_{p^n} \mid S(x+\alpha) - cS(x) = \beta\}\right| $$

- widely studied for S-boxes from a theoretic point of view

A cryptographic attack for $c \neq 1$ remains to be shown



CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

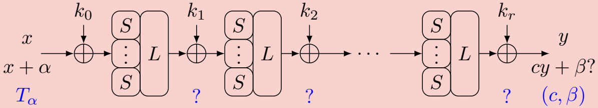
c-Differential Uniformity ($G = \mathbb{F}_{p^n}$) [Ellingsen, Felke, Riera, Stănică, Tkachenko]

Let $S\colon \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ and $c \in \mathbb{F}_{p^n}^*$. The c-differential uniformity of S is

$$_c\delta_S := \max_{\alpha,\beta\in\mathbb{F}_{p^n},\alpha\neq 0 \text{ if } c=1} |\{x \in \mathbb{F}_{p^n} \mid S(x+\alpha) - cS(x) = \beta\}|$$

- widely studied for S-boxes from a theoretic point of view

A cryptographic attack for $c \neq 1$ remains to be shown



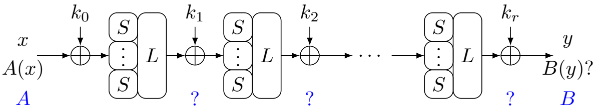
Commutative Cryptanalysis as a Unifying Framework

Commutative Distinguisher (Informal)

Let $(E_k)_{k \in \kappa}$ a finite family of permutations over G (i.e., a block cipher). A commutative distinguisher is a pair (A, B) with $A, B \colon G \to G$ s.t.

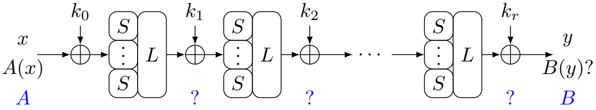
$$P(A \xrightarrow{E_k} B) := \mathrm{Pr}_{x \in G}[E_k(A(x)) = B(E_k(x))]$$

is high for many keys $k \in \kappa$.



- corresponds to notion of commutative diagram cryptanalysis [Wagner, 2004]
- advantage needs to be formalized (e.g., $A = B = \mathrm{id}$ is not meaningful)

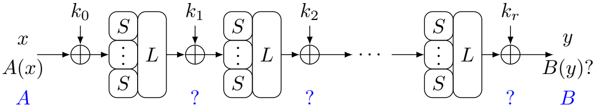
Commutative Cryptanalysis as a Unifying Framework (cont.)



- Differential cryptanalysis [Biham, Shamir, '91]: $A = T_\alpha := (x \mapsto x + \alpha)$ and $B = T_\beta := (x \mapsto x + \beta)$
- Rotational cryptanalysis [Khovratovich, Nikolić, 2010]: Let $G = \mathbb{F}_2^n$ and $\rho\colon (x_1, \ldots, x_n) \mapsto (x_2, \ldots, x_n, x_1)$. Then, $A = \rho^i$ and $B = \rho^j$
- Rotational differential cryptanalysis [Ashur, Liu, 2016]: Let $G = \mathbb{F}_2^n$. $A = \rho^i \circ T_\alpha$ and $B = T_\beta$
- c-differentials: finite field $G = \mathbb{F}_{p^n}$, $A = T_\alpha$ and $B\colon x \mapsto cx + \beta$ with $\alpha, \beta, c \in \mathbb{F}_{p^n}, c \neq 0$

Commutative Cryptanalysis as a Unifying Framework (cont.)

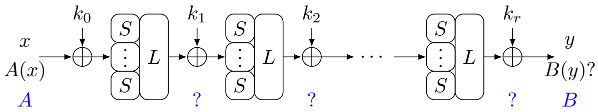
CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES



- Differential cryptanalysis [Biham, Shamir, '91]: $A = T_\alpha := (x \mapsto x + \alpha)$ and $B = T_\beta := (x \mapsto x + \beta)$
- Rotational cryptanalysis [Khovratovich, Nikolić, 2010]: Let $G = \mathbb{F}_2^n$ and $\rho\colon (x_1, \ldots, x_n) \mapsto (x_2, \ldots, x_n, x_1)$. Then, $A = \rho^i$ and $B = \rho^j$
- Rotational differential cryptanalysis [Ashur, Liu, 2016]: Let $G = \mathbb{F}_2^n$. $A = \rho^i \circ T_\alpha$ and $B = T_\beta$
- c-differentials: finite field $G = \mathbb{F}_{p^n}$, $A = T_\alpha$ and $B\colon x \mapsto cx + \beta$ with $\alpha, \beta, c \in \mathbb{F}_{p^n}, c \neq 0$

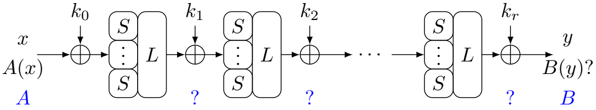
Commutative Cryptanalysis as a Unifying Framework (cont.)

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES



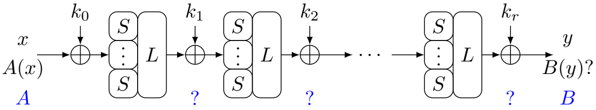
- Differential cryptanalysis [Biham, Shamir, '91]: $A = T_\alpha := (x \mapsto x + \alpha)$ and $B = T_\beta := (x \mapsto x + \beta)$
- Rotational cryptanalysis [Khovratovich, Nikolić, 2010]: Let $G = \mathbb{F}_2^n$ and $\rho\colon (x_1, \ldots, x_n) \mapsto (x_2, \ldots, x_n, x_1)$. Then, $A = \rho^i$ and $B = \rho^j$
- Rotational differential cryptanalysis [Ashur, Liu, 2016]: Let $G = \mathbb{F}_2^n$. $A = \rho^i \circ T_\alpha$ and $B = T_\beta$
- c-differentials: finite field $G = \mathbb{F}_{p^n}$, $A = T_\alpha$ and $B\colon x \mapsto cx + \beta$ with $\alpha, \beta, c \in \mathbb{F}_{p^n}, c \neq 0$

Commutative Cryptanalysis as a Unifying Framework (cont.)



- Differential cryptanalysis [Biham, Shamir, '91]: $A = T_\alpha := (x \mapsto x + \alpha)$ and $B = T_\beta := (x \mapsto x + \beta)$
- Rotational cryptanalysis [Khovratovich, Nikolić, 2010]: Let $G = \mathbb{F}_2^n$ and $\rho\colon (x_1, \ldots, x_n) \mapsto (x_2, \ldots, x_n, x_1)$. Then, $A = \rho^i$ and $B = \rho^j$
- Rotational differential cryptanalysis [Ashur, Liu, 2016]: Let $G = \mathbb{F}_2^n$. $A = \rho^i \circ T_\alpha$ and $B = T_\beta$
- c-differentials: finite field $G = \mathbb{F}_{p^n}$, $A = T_\alpha$ and $B\colon x \mapsto cx + \beta$ with $\alpha, \beta, c \in \mathbb{F}_{p^n}, c \neq 0$

Commutative Cryptanalysis as a Unifying Framework (cont.)



- [Baudrin et al., 2023] studied the case of $G = \mathbb{F}_2^n$ and A, B affine permutations

Question

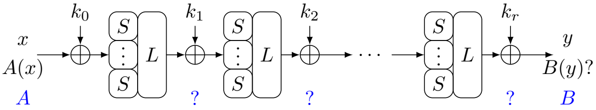
Can we study the resistance by studying an isolated property of S (as for differentials)?

Affine Uniformity [Baudrin et al., 2023]

Given an S-box $S\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ and $A, B \in \mathrm{AGL}(n, \mathbb{F}_2)$, define

$$\Gamma_S(A, B) = |\{x \in \mathbb{F}_2^n \mid S(A(x)) = B(S(x))\}|, \quad \Gamma_S := \max_{A,B,\mathrm{id} \notin \{A,B\}} \Gamma_S(A, B).$$

Commutative Cryptanalysis as a Unifying Framework (cont.)



- [Baudrin et al., 2023] studied the case of $G = \mathbb{F}_2^n$ and A, B affine permutations

Question

Can we study the resistance by studying an isolated property of S (as for differentials)?

Affine Uniformity [Baudrin et al., 2023]

Given an S-box $S\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ and $A, B \in \mathrm{AGL}(n, \mathbb{F}_2)$, define

$$\Gamma_S(A,B) = |\{x \in \mathbb{F}_2^n \mid S(A(x)) = B(S(x))\}|, \quad \Gamma_S := \max_{A,B,\mathrm{id} \notin \{A,B\}} \Gamma_S(A,B).$$

Outline

A Chosen-Plaintext Distinguisher

CASA
Cyber Security in the Age of Large-Scale Adversaries

Commutative Distinguisher (Informal)

Pair (A, B) with $A, B\colon G \to G$ such that $\Pr_x[E_k(A(x)) = B(E_k(x))]$ is high for many k.

The security model

Adversary $\mathcal{A}$ interacts with $\mathcal{O} = E_k\colon G \to G$ for an (unknown) uniformly chosen $k \in \kappa$ or with a uniformly random chosen permutation $\mathcal{O} = P\colon G \to G$ (such that $\Pr(\mathcal{O} = E_k) = \Pr(\mathcal{O} = P) = 0.5$). $\mathcal{A}$ tells whether $\mathcal{O} = E_k$ (return 1) or $\mathcal{O} = P$ (ret. 0).

How the commutative (chosen-plaintext) distinguisher works:

- $\mathcal{A}$ encrypts x_i and $A(x_i)$ for a random x_i and checks $\mathcal{O}(A(x_i)) \stackrel{?}{=} B(\mathcal{O}(x_i))$
- makes a guess for $\mathcal{O} \in \{E_k, P\}$ and returns 1 or 0

CASA
Cyber Security in the Age of Large-Scale Adversaries

Commutative Distinguisher (Informal)

Pair (A, B) with $A, B\colon G \to G$ such that $\Pr_x[E_k(A(x)) = B(E_k(x))]$ is high for many k.

The security model

Adversary $\mathcal{A}$ interacts with $\mathcal{O} = E_k\colon G \to G$ for an (unknown) uniformly chosen $k \in \kappa$ or with a uniformly random chosen permutation $\mathcal{O} = P\colon G \to G$ (such that $\Pr(\mathcal{O} = E_k) = \Pr(\mathcal{O} = P) = 0.5$). $\mathcal{A}$ tells whether $\mathcal{O} = E_k$ (return 1) or $\mathcal{O} = P$ (ret. 0).

How the commutative (chosen-plaintext) distinguisher works:

- $\mathcal{A}$ encrypts x_i and $A(x_i)$ for a random x_i and checks $\mathcal{O}(A(x_i)) \stackrel{?}{=} B(\mathcal{O}(x_i))$
- makes a guess for $\mathcal{O} \in \{E_k, P\}$ and returns 1 or 0

The Distinguishing Advantage

CASA
Cyber Security in the Age of Large-Scale Adversaries

For a permutation $P\colon G \to G$, we have

$$\Pr(A \xrightarrow{P} B) = \Pr_{x \in G}[P(A(x)) = B(P(x))] = \frac{\Gamma_P(A, B)}{|G|},$$

where $\Gamma_P(A, B) := |\{x \in G \mid P(A(x)) = B(P(x))\}|$. For $(E_k)_{k \in \kappa}$, define the expected commutative probability as

$$\mathrm{ECP}(A \xrightarrow{E} B) := \frac{1}{|\kappa|} \sum_{k \in \kappa} \Pr(A \xrightarrow{E_k} B).$$

Distinguishing Advantage of Commutative Distinguisher (A, B)

$$\mathrm{Adv}_{(A,B)} := |\mathrm{ECP}(A \xrightarrow{E} B) - \Pr_{P \in \mathrm{Perm}(G), x \in G}[P(A(x)) = B(P(x))]|,$$

where $\mathrm{Perm}(G)$ denotes the set of all permutations of G.

The Distinguishing Advantage

For a permutation $P\colon G \to G$, we have

$$\Pr(A \xrightarrow{P} B) = \Pr_{x \in G}[P(A(x)) = B(P(x))] = \frac{\Gamma_P(A, B)}{|G|},$$

where $\Gamma_P(A, B) := |\{x \in G \mid P(A(x)) = B(P(x))\}|$. For $(E_k)_{k \in \kappa}$, define the expected commutative probability as

$$\mathrm{ECP}(A \xrightarrow{E} B) := \frac{1}{|\kappa|} \sum_{k \in \kappa} \Pr(A \xrightarrow{E_k} B).$$

Distinguishing Advantage of Commutative Distinguisher (A, B)

$$\mathrm{Adv}_{(A,B)} := |\mathrm{ECP}(A \xrightarrow{E} B) - \Pr_{P \in \mathrm{Perm}(G), x \in G}[P(A(x)) = B(P(x))]|,$$

where $\mathrm{Perm}(G)$ denotes the set of all permutations of G.

The Distinguishing Advantage (cont.)

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

Distinguishing Advantage of Commutative Distinguisher (A, B)

$$\mathrm{Adv}_{(A,B)} := \left|\mathrm{ECP}(A \xrightarrow{E} B) - \mathrm{Pr}_{P \in \mathrm{Perm}(G), x \in G}[P(A(x)) = B(P(x))]\right|$$

Lemma

Let G be a finite set and $A, B \colon G \to G$. Then,

$$\mathrm{Pr}_{P \in \mathrm{Perm}(G), x \in G}[P \circ A(x) = B \circ P(x)] = \frac{|G| - |\mathrm{Fix}(A)| - |\mathrm{Fix}(B)| + |\mathrm{Fix}(A)| \cdot |\mathrm{Fix}(B)|}{|G| \cdot (|G| - 1)},$$

where $\mathrm{Fix}(\cdot)$ denotes the set of fixed points.

The Distinguishing Advantage (cont.)

CASA
Cyber Security in the Age of Large-Scale Adversaries

Distinguishing Advantage of Commutative Distinguisher (A, B)

$$\mathrm{Adv}_{(A,B)} := \left|\mathrm{ECP}(A \xrightarrow{E} B) - \frac{|G| - |\mathrm{Fix}(A)| - |\mathrm{Fix}(B)| + |\mathrm{Fix}(A)| \cdot |\mathrm{Fix}(B)|}{|G| \cdot (|G| - 1)}\right|$$

If $G = \mathbb{F}_p^n$, $C \in \mathrm{AGL}(n, \mathbb{F}_p)$ such that $C = L + c$ with L being linear, we have

$$|\mathrm{Fix}(C)| = \begin{cases} 0 & \text{if } c \notin \mathrm{Im}(\mathrm{id} - L) \\ p^{\dim \ker(\mathrm{id} - L)} & \text{otherwise (and } \mathrm{Fix}(C) \text{ is an affine subspace of } \mathbb{F}_p^n) \end{cases},$$

Be careful with the notion of affine uniformity!

The notion of affine uniformity is only meaningful if we restrict to sets $\mathcal{A} \subseteq \mathrm{AGL}(n, \mathbb{F}_p)^2$ such that $(A_1, B_1), (A_2, B_2) \in \mathcal{A}$ implies $|\mathrm{Fix}(A_1)| = |\mathrm{Fix}(A_2)|$ and $|\mathrm{Fix}(B_1)| = |\mathrm{Fix}(B_2)|$.

The Distinguishing Advantage (cont.)

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

Distinguishing Advantage of Commutative Distinguisher (A, B)

$$\mathrm{Adv}_{(A,B)} := \left|\mathrm{ECP}(A \xrightarrow{E} B) - \frac{|G| - |\mathrm{Fix}(A)| - |\mathrm{Fix}(B)| + |\mathrm{Fix}(A)| \cdot |\mathrm{Fix}(B)|}{|G| \cdot (|G| - 1)}\right|$$

If $G = \mathbb{F}_p^n$, $C \in \mathrm{AGL}(n, \mathbb{F}_p)$ such that $C = L + c$ with L being linear, we have

$$|\mathrm{Fix}(C)| = \begin{cases} 0 & \text{if } c \notin \mathrm{Im}(\mathrm{id} - L) \\ p^{\dim\ker(\mathrm{id}-L)} & \text{otherwise (and } \mathrm{Fix}(C) \text{ is an affine subspace of } \mathbb{F}_p^n) \end{cases},$$

Be careful with the notion of affine uniformity!

The notion of affine uniformity is only meaningful if we restrict to sets $\mathcal{A} \subseteq \mathrm{AGL}(n, \mathbb{F}_p)^2$ such that $(A_1, B_1), (A_2, B_2) \in \mathcal{A}$ implies $|\mathrm{Fix}(A_1)| = |\mathrm{Fix}(A_2)|$ and $|\mathrm{Fix}(B_1)| = |\mathrm{Fix}(B_2)|$.

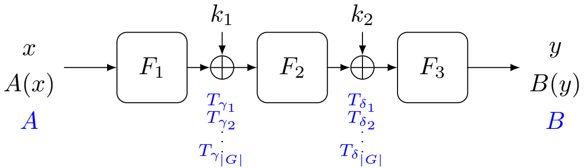
Expressing $\mathrm{ECP}(A \xrightarrow{E} B)$ using Commutative Trails

CASA
Cyber Security in the Age of Large-Scale Adversaries

Commutative Trail Formula for Iterated Ciphers (over independent round keys)

Let $(E_k)_{k \in G \times G}$ be the family of permutations defined by $E_{(k_1,k_2)} = F_3 \circ T_{k_2} \circ F_2 \circ T_{k_1} \circ F_1$ for permutations $F_1, F_2, F_3 \colon G \to G$ and let $A, B \colon G \to G$. We have

$$\mathrm{ECP}(A \xrightarrow{E} B) = \sum_{\gamma \in G} \sum_{\delta \in G} \mathrm{Pr}(A \xrightarrow{F_1} T_\gamma) \cdot \mathrm{Pr}(T_\gamma \xrightarrow{F_2} T_\delta) \cdot \mathrm{Pr}(T_\delta \xrightarrow{F_3} B).$$



- Generalization of the case where A, B are translations [Lai, Massey, Murphy, '91]

Expressing $\mathrm{ECP}(A \xrightarrow{E} B)$ using Commutative Trails (cont.)

CASA
Cyber Security in the Age of Large-Scale Adversaries

Commutative Trail Formula for Iterated Ciphers

Let $(E_k)_{k \in G \times G}$ be the family of permutations defined by $E_{(k_1,k_2)} = F_3 \circ T_{k_2} \circ F_2 \circ T_{k_1} \circ F_1$ for permutations $F_1, F_2, F_3 \colon G \to G$ and let $A, B \colon G \to G$. We have

$$\mathrm{ECP}(A \xrightarrow{E} B) = \sum_{\gamma \in G} \sum_{\delta \in G} \Pr(A \xrightarrow{F_1} T_\gamma) \cdot \Pr(T_\gamma \xrightarrow{F_2} T_\delta) \cdot \Pr(T_\delta \xrightarrow{F_3} B).$$

Application to Even-Mansour Cipher (Setting $F_1 = F_3 = \mathrm{id}, F_2 = R$)

$$\mathrm{ECP}(A \xrightarrow{E} B) \leq \frac{\delta_R}{|G|} \cdot \frac{(|G| - |\mathrm{Fix}(A)|)(|G| - |\mathrm{Fix}(B)|)}{|G|^2} + \frac{|\mathrm{Fix}(A)| \cdot |\mathrm{Fix}(B)|}{|G|^2}.$$

If one of $A - \mathrm{id}$ or $B - \mathrm{id}$ is bijective, we have $\mathrm{ECP}(A \xrightarrow{E} B) = \frac{1}{|G|}$.

Putting All Together

Distinguishing Advantage over Cipher with Independent Whitening Keys

$$\mathrm{Adv}_{(A,B)} \leq \max_{\gamma,\delta \in G, \gamma \neq 0} \mathrm{ECP}(T_\gamma \xrightarrow{E} T_\delta) + \frac{2}{|G|-1}.$$

If one of $A - \mathrm{id}$ or $B - \mathrm{id}$ is invertible, then $\mathrm{Adv}_{(A,B)} = 0$.

- When there are independent whitening keys, we cannot do better than a differential attack (already shown in [Liu, Tessaro, Vaikuntanathan, 2021])
- c-differentials ($c \neq 1$) yield advantage 0, as $x \mapsto cx + \beta - x$ is invertible

Weak-Key Model

A commutative (non-differential) attack only works in the weak-key model, or exploits properties of the key schedule!

Putting All Together

CASA — Cyber Security in the Age of Large-Scale Adversaries

Distinguishing Advantage over Cipher with Independent Whitening Keys

$$\mathrm{Adv}_{(A,B)} \leq \max_{\gamma,\delta\in G,\gamma\neq 0} \mathrm{ECP}(T_\gamma \xrightarrow{E} T_\delta) + \frac{2}{|G|-1}.$$

If one of $A - \mathrm{id}$ or $B - \mathrm{id}$ is invertible, then $\mathrm{Adv}_{(A,B)} = 0$.

- When there are independent whitening keys, we cannot do better than a differential attack (already shown in [Liu, Tessaro, Vaikuntanathan, 2021])
- c-differentials ($c \neq 1$) yield advantage 0, as $x \mapsto cx + \beta - x$ is invertible

Weak-Key Model

A commutative (non-differential) attack only works in the weak-key model, or exploits properties of the key schedule!

Putting All Together

CASA — Cyber Security in the Age of Large-Scale Adversaries

Distinguishing Advantage over Cipher with Independent Whitening Keys

$$\mathrm{Adv}_{(A,B)} \leq \max_{\gamma,\delta \in G, \gamma \neq 0} \mathrm{ECP}(T_\gamma \xrightarrow{E} T_\delta) + \frac{2}{|G|-1}.$$

If one of $A - \mathrm{id}$ or $B - \mathrm{id}$ is invertible, then $\mathrm{Adv}_{(A,B)} = 0$.

- When there are independent whitening keys, we cannot do better than a differential attack (already shown in [Liu, Tessaro, Vaikuntanathan, 2021])
- c-differentials ($c \neq 1$) yield advantage 0, as $x \mapsto cx + \beta - x$ is invertible

Weak-Key Model

A commutative (non-differential) attack only works in the weak-key model, or exploits properties of the key schedule!

Outline

Commutative Trails of Probability 1

CASA
Cyber Security in the Age of Large-Scale Adversaries

In the following, let $G = \mathbb{F}_p^n$.

Deterministic Commutative Trail

Let $F = F_r \circ \cdots \circ F_2 \circ F_1$ be an iterated permutation, $F_i \colon \mathbb{F}_p^n \to \mathbb{F}_p^n$ permutations.
Let $C_0, \ldots, C_r \in \mathrm{AGL}(n, \mathbb{F}_p)$ such that $F_i \circ C_{i-1} = C_i \circ F_i$ for all i, then $F \circ A = B \circ F$ with $A = C_0, B = C_r$ (i.e., $\Gamma_F(A, B) = p^n$).

Idea (as studied in [Baudrin et al., 2023]):

- Separate the block cipher (SPN) into the S-box layer ($\mathcal{S}$), linear layer (L), and key addition (T_k)
- for all $X \in \{\mathcal{S}, L\} \cup \{T_k \mid k \in \mathrm{WeakKeys}\}$ find $C, C' \in \mathrm{AGL}(n, \mathbb{F}_p)$ with $X \circ C = C' \circ X$ (i.e., $\Gamma_X(C, C') = p^n$)

Commutative Trails of Probability 1

In the following, let $G = \mathbb{F}_p^n$.

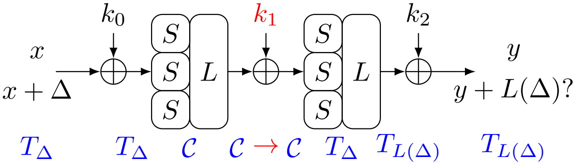
Deterministic Commutative Trail

Let $F = F_r \circ \cdots \circ F_2 \circ F_1$ be an iterated permutation, $F_i \colon \mathbb{F}_p^n \to \mathbb{F}_p^n$ permutations.
Let $C_0, \ldots, C_r \in \mathrm{AGL}(n, \mathbb{F}_p)$ such that $F_i \circ C_{i-1} = C_i \circ F_i$ for all i, then $F \circ A = B \circ F$ with $A = C_0, B = C_r$ (i.e., $\Gamma_F(A, B) = p^n$).

Idea (as studied in [Baudrin et al., 2023]):

- Separate the block cipher (SPN) into the S-box layer ($\mathcal{S}$), linear layer (L), and key addition (T_k)
- for all $X \in \{\mathcal{S}, L\} \cup \{T_k \mid k \in \mathrm{WeakKeys}\}$ find $C, C' \in \mathrm{AGL}(n, \mathbb{F}_p)$ with $X \circ C = C' \circ X$ (i.e., $\Gamma_X(C, C') = p^n$)

Example 1 (Two-Round Cipher [B., Felke, Leander, Neumann, Stennes])

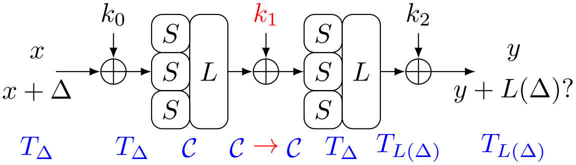


- S-box layer $\mathcal{S}$ applies three 5-bit S-boxes in parallel, i.e., $\mathcal{S} = (S, S, S)$
- Linear layer L defined by a special 15×15 matrix over $\mathbb{F}_2$
- The two-round cipher defined as $E_{k_0,k_1,k_2} := T_{k_2} \circ L \circ \mathcal{S} \circ T_{k_1} \circ L \circ \mathcal{S} \circ T_{k_0}$

Special properties of S and L (we see later how such S, L can be constructed)

- $\exists \delta \in \mathbb{F}_2^5 \setminus \{0\}$ and $C \in \mathrm{AGL}(5, \mathbb{F}_2)$ such that $S \circ T_\delta = C \circ S$ and $S \circ C = T_\delta \circ S$. Then, $\mathcal{S} \circ T_\Delta = \mathcal{C} \circ \mathcal{S}$ and $\mathcal{S} \circ \mathcal{C} = T_\Delta \circ \mathcal{S}$ where $\Delta = (\delta, \delta, \delta), \mathcal{C} = \mathrm{Diag}(C, C, C)$
- S has non-trivial differential uniformity and non-trivial linearity (here $\delta_S = 20$).
- $\mathcal{C}$ commutes with L, i.e., $L \circ \mathcal{C} = \mathcal{C} \circ L$

Example 1 (Two-Round Cipher [B., Felke, Leander, Neumann, Stennes])



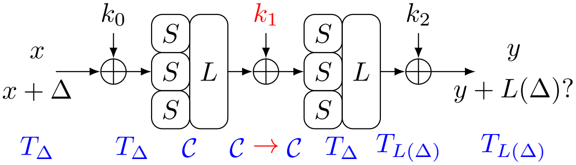
- S-box layer $\mathcal{S}$ applies three 5-bit S-boxes in parallel, i.e., $\mathcal{S} = (S, S, S)$
- Linear layer L defined by a special 15×15 matrix over $\mathbb{F}_2$
- The two-round cipher defined as $E_{k_0,k_1,k_2} := T_{k_2} \circ L \circ \mathcal{S} \circ T_{k_1} \circ L \circ \mathcal{S} \circ T_{k_0}$

Special properties of S and L (we see later how such S, L can be constructed)

- $\exists \delta \in \mathbb{F}_2^5 \setminus \{0\}$ and $C \in \mathrm{AGL}(5, \mathbb{F}_2)$ such that $S \circ T_\delta = C \circ S$ and $S \circ C = T_\delta \circ S$. Then, $\mathcal{S} \circ T_\Delta = \mathcal{C} \circ \mathcal{S}$ and $\mathcal{S} \circ \mathcal{C} = T_\Delta \circ \mathcal{S}$ where $\Delta = (\delta, \delta, \delta), \mathcal{C} = \mathrm{Diag}(C, C, C)$
- S has non-trivial differential uniformity and non-trivial linearity (here $\delta_S = 20$).
- $\mathcal{C}$ commutes with L, i.e., $L \circ \mathcal{C} = \mathcal{C} \circ L$

Example 1 (Two-Round Cipher [B., Felke, Leander, Neumann, Stennes])

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

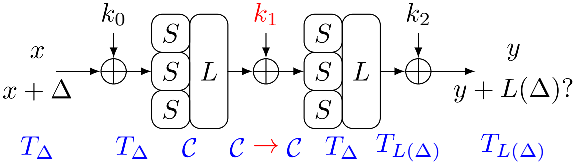


- S-box layer $\mathcal{S}$ applies three 5-bit S-boxes in parallel, i.e., $\mathcal{S} = (S, S, S)$
- Linear layer L defined by a special 15×15 matrix over $\mathbb{F}_2$
- The two-round cipher defined as $E_{k_0,k_1,k_2} := T_{k_2} \circ L \circ \mathcal{S} \circ T_{k_1} \circ L \circ \mathcal{S} \circ T_{k_0}$

Special properties of S and L (we see later how such S, L can be constructed)

- $\exists \delta \in \mathbb{F}_2^5 \setminus \{0\}$ and $C \in \mathrm{AGL}(5, \mathbb{F}_2)$ such that $S \circ T_\delta = C \circ S$ and $S \circ C = T_\delta \circ S$. Then, $\mathcal{S} \circ T_\Delta = \mathcal{C} \circ \mathcal{S}$ and $\mathcal{S} \circ \mathcal{C} = T_\Delta \circ \mathcal{S}$ where $\Delta = (\delta, \delta, \delta), \mathcal{C} = \mathrm{Diag}(C, C, C)$
- S has non-trivial differential uniformity and non-trivial linearity (here $\delta_S = 20$).
- $\mathcal{C}$ commutes with L, i.e., $L \circ \mathcal{C} = \mathcal{C} \circ L$

Example 1 (Two-Round Cipher [B., Felke, Leander, Neumann, Stennes])



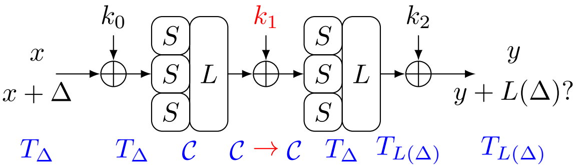
- S-box layer $\mathcal{S}$ applies three 5-bit S-boxes in parallel, i.e., $\mathcal{S} = (S, S, S)$
- Linear layer L defined by a special 15×15 matrix over $\mathbb{F}_2$
- The two-round cipher defined as $E_{k_0,k_1,k_2} := T_{k_2} \circ L \circ \mathcal{S} \circ T_{k_1} \circ L \circ \mathcal{S} \circ T_{k_0}$

Special properties of S and L (we see later how such S, L can be constructed)

- $\exists \delta \in \mathbb{F}_2^5 \setminus \{0\}$ and $C \in \mathrm{AGL}(5, \mathbb{F}_2)$ such that $S \circ T_\delta = C \circ S$ and $S \circ C = T_\delta \circ S$. Then, $\mathcal{S} \circ T_\Delta = \mathcal{C} \circ \mathcal{S}$ and $\mathcal{S} \circ \mathcal{C} = T_\Delta \circ \mathcal{S}$ where $\Delta = (\delta, \delta, \delta), \mathcal{C} = \mathrm{Diag}(C, C, C)$
- S has non-trivial differential uniformity and non-trivial linearity (here $\delta_S = 20$).
- $\mathcal{C}$ commutes with L, i.e., $L \circ \mathcal{C} = \mathcal{C} \circ L$

Example 1 (cont.)

CASA
Cyber Security in the Age of Large-Scale Adversaries



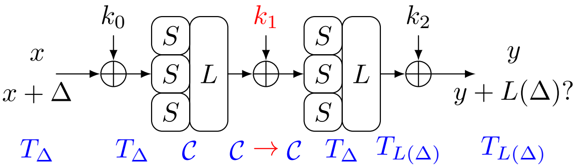
- If k_1 is a weak key (in the sense that $T_{k_1} \circ \mathcal{C} = \mathcal{C} \circ T_{k_1}$), we have $E_{k_0,k_1,k_2}(x + \Delta) = E_{k_0,k_1,k_2}(x) + L(\Delta)$, i.e., a probability-1 differential
- There are no probability-1 differentials over a single round (since $\delta_S < 2^5$)

What are the weak keys?

In this example, the weak keys form a 12-dimensional subspace of $\mathbb{F}_2^{15}$.

Example 1 (cont.)

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES



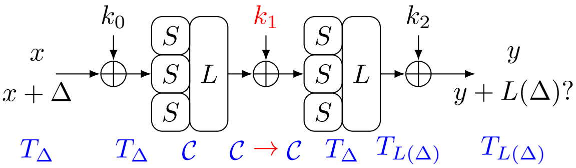
- If k_1 is a weak key (in the sense that $T_{k_1} \circ \mathcal{C} = \mathcal{C} \circ T_{k_1}$), we have $E_{k_0,k_1,k_2}(x + \Delta) = E_{k_0,k_1,k_2}(x) + L(\Delta)$, i.e., a probability-1 differential
- There are no probability-1 differentials over a single round (since $\delta_S < 2^5$)

What are the weak keys?

In this example, the weak keys form a 12-dimensional subspace of $\mathbb{F}_2^{15}$.

Example 1 (cont.)

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES



- If k_1 is a weak key (in the sense that $T_{k_1} \circ \mathcal{C} = \mathcal{C} \circ T_{k_1}$), we have $E_{k_0,k_1,k_2}(x + \Delta) = E_{k_0,k_1,k_2}(x) + L(\Delta)$, i.e., a probability-1 differential
- There are no probability-1 differentials over a single round (since $\delta_S < 2^5$)

What are the weak keys?

In this example, the weak keys form a 12-dimensional subspace of $\mathbb{F}_2^{15}$.

Example 2 (Midori) and Example 3 (Scream)

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

- Midori [Banik et al., 2015] is a 64-bit block cipher (SPN) using a 128-bit key
- Scream [Grosso et al., 2015] is a 128-bit tweakable block cipher using a 128-bit key

Results shown in [Baudrin et al., 2023]

- Midori: If the round constants are slightly modified, there exists a probability-1 commutative trail covering an arbitrary number of rounds for 2^{96} keys
- Scream: There is a probability-1 commutative trail for 2^{80} keys

Question

What are the properties of the S-box, key addition and linear layer to make such attacks possible?

Example 2 (Midori) and Example 3 (Scream)

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

- Midori [Banik et al., 2015] is a 64-bit block cipher (SPN) using a 128-bit key
- Scream [Grosso et al., 2015] is a 128-bit tweakable block cipher using a 128-bit key

Results shown in [Baudrin et al., 2023]

- Midori: If the round constants are slightly modified, there exists a probability-1 commutative trail covering an arbitrary number of rounds for 2^{96} keys
- Scream: There is a probability-1 commutative trail for 2^{80} keys

Question

What are the properties of the S-box, key addition and linear layer to make such attacks possible?

Outline

Characterizing Weak Keys

Let $A, B \in \mathrm{AGL}(n, \mathbb{F}_p)$ with $A = L_A + c_A$, $B = L_B + c_B$ for L_A, L_B linear and $k \in \kappa$. For $x \in \mathbb{F}_p^n$, we have

$$T_k \circ A(x) = B \circ T_k(x) \quad \Leftrightarrow \quad (L_A - L_B)(x) = (L_B - \mathrm{id})(k) + c_B - c_A$$

Examples

- Differentials ($A = T_\alpha = \mathrm{id} + \alpha, B = T_\beta = \mathrm{id} + \beta$): Commutation is equivalent to $0 = \beta - \alpha$, hence $\Gamma_{T_k}(T_\alpha, T_\alpha) = p^n$ (independently of x and k)
- c-Differentials ($A = T_\alpha, B = c \cdot \mathrm{id} + \beta$): For $c \neq 1$, commutation is equivalent to

$$x = \frac{c-1}{1-c} \cdot k + \frac{\beta - \alpha}{1-c}.$$

Hence, for each k, we have $\Gamma_{T_k}(A, B) = 1$.

Characterizing Weak Keys

CASA
Cyber Security in the Age of Large-Scale Adversaries

Let $A, B \in \mathrm{AGL}(n, \mathbb{F}_p)$ with $A = L_A + c_A$, $B = L_B + c_B$ for L_A, L_B linear and $k \in \kappa$. For $x \in \mathbb{F}_p^n$, we have

$$T_k \circ A(x) = B \circ T_k(x) \quad \Leftrightarrow \quad (L_A - L_B)(x) = (L_B - \mathrm{id})(k) + c_B - c_A$$

Examples

- Differentials ($A = T_\alpha = \mathrm{id} + \alpha, B = T_\beta = \mathrm{id} + \beta$): Commutation is equivalent to $0 = \beta - \alpha$, hence $\Gamma_{T_k}(T_\alpha, T_\alpha) = p^n$ (independently of x and k)
- c-Differentials ($A = T_\alpha, B = c \cdot \mathrm{id} + \beta$): For $c \neq 1$, commutation is equivalent to

$$x = \frac{c-1}{1-c} \cdot k + \frac{\beta - \alpha}{1-c}.$$

Hence, for each k, we have $\Gamma_{T_k}(A, B) = 1$.

Characterizing Weak Keys

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

Let $A, B \in \mathrm{AGL}(n, \mathbb{F}_p)$ with $A = L_A + c_A, B = L_B + c_B$ for L_A, L_B linear and $k \in \kappa$. For $x \in \mathbb{F}_p^n$, we have

$$T_k \circ A(x) = B \circ T_k(x) \quad \Leftrightarrow \quad (L_A - L_B)(x) = (L_B - \mathrm{id})(k) + c_B - c_A$$

Examples

- Differentials ($A = T_\alpha = \mathrm{id} + \alpha, B = T_\beta = \mathrm{id} + \beta$): Commutation is equivalent to $0 = \beta - \alpha$, hence $\Gamma_{T_k}(T_\alpha, T_\alpha) = p^n$ (independently of x and k)
- c-Differentials ($A = T_\alpha, B = c \cdot \mathrm{id} + \beta$): For $c \neq 1$, commutation is equivalent to

$$x = \frac{c-1}{1-c} \cdot k + \frac{\beta - \alpha}{1-c}.$$

Hence, for each k, we have $\Gamma_{T_k}(A, B) = 1$.

Characterizing Weak Keys (cont.)

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

$$T_k \circ A(x) = B \circ T_k(x) \quad \Leftrightarrow \quad (L_A - L_B)(x) = (L_B - \mathrm{id})(k) + c_B - c_A$$

More general requirement

An attacker would like to have many solutions $(x, k) \in (\mathbb{F}_p^n)^2$ of $T_k \circ A(x) = B \circ T_k(x)$, i.e., $\mathrm{rank}(M_{A,B})$, where

$$M_{A,B} := [L_A - L_B \mid \mathrm{id} - L_B],$$

should be as low as possible.

- Attacker's best case ($\mathrm{rank}(M_{A,B}) = 0$): Commutation holds independently of x and k. This is if and only if $L_A = L_B = \mathrm{id}$ (differential attack)
- Attacker's worst case ($\mathrm{rank}(M_{A,B}) = n$): For example if $L_A = \mathrm{id}, L_B = c \cdot \mathrm{id}, c \neq 1$, i.e., the case of c-differentials

Characterizing Weak Keys (cont.)

CASA
Cyber Security in the Age of Large-Scale Adversaries

$$T_k \circ A(x) = B \circ T_k(x) \quad \Leftrightarrow \quad (L_A - L_B)(x) = (L_B - \mathrm{id})(k) + c_B - c_A$$

More general requirement

An attacker would like to have many solutions $(x, k) \in (\mathbb{F}_p^n)^2$ of $T_k \circ A(x) = B \circ T_k(x)$, i.e., $\mathrm{rank}(M_{A,B})$, where

$$M_{A,B} := [L_A - L_B \mid \mathrm{id} - L_B],$$

should be as low as possible.

- Attacker's best case ($\mathrm{rank}(M_{A,B}) = 0$): Commutation holds independently of x and k. This is if and only if $L_A = L_B = \mathrm{id}$ (differential attack)
- Attacker's worst case ($\mathrm{rank}(M_{A,B}) = n$): For example if $L_A = \mathrm{id}, L_B = c \cdot \mathrm{id}, c \neq 1$, i.e., the case of c-differentials

Characterizing Weak Keys (cont.)

$$T_k \circ A(x) = B \circ T_k(x) \quad \Leftrightarrow \quad (L_A - L_B)(x) = (L_B - \mathrm{id})(k) + c_B - c_A$$

More general requirement

An attacker would like to have many solutions $(x, k) \in (\mathbb{F}_p^n)^2$ of $T_k \circ A(x) = B \circ T_k(x)$, i.e., $\mathrm{rank}(M_{A,B})$, where

$$M_{A,B} := [L_A - L_B \mid \mathrm{id} - L_B],$$

should be as low as possible.

- Attacker's best case ($\mathrm{rank}(M_{A,B}) = 0$): Commutation holds independently of x and k. This is if and only if $L_A = L_B = \mathrm{id}$ (differential attack)
- Attacker's worst case ($\mathrm{rank}(M_{A,B}) = n$): For example if $L_A = \mathrm{id}, L_B = c \cdot \mathrm{id}, c \neq 1$, i.e., the case of c-differentials

Characterizing Weak Keys (cont.)

CASA
Cyber Security in the Age of Large-Scale Adversaries

$$T_k \circ A(x) = B \circ T_k(x) \quad \Leftrightarrow \quad (L_A - L_B)(x) = (L_B - \mathrm{id})(k) + c_B - c_A$$

Condition on deterministic commutation

If $T_k \circ A = B \circ T_k$, we must have $L_A = L_B$ and then, $(L_A - \mathrm{id})(k) = c_A - c_B$. Hence,

$$|\mathrm{WeakKeys}| = \begin{cases} p^{n-\mathrm{rank}(L_A-\mathrm{id})} & \text{if } c_A - c_B \in \mathrm{Im}(L_A - \mathrm{id}) \\ 0 & \text{else} \end{cases}.$$

- In Example 1, $\mathrm{rank}(\mathcal{C} - \mathrm{id}) = 3$, so there are 2^{12} weak keys out of 2^{15} choices for k_1

To summarize

For commutation over S and L, we will mainly be interested in those A, B with $d_A := \mathrm{rank}(L_A - \mathrm{id})$ and $d_B := \mathrm{rank}(L_B - \mathrm{id})$ as low as possible (or at least one of them)

Characterizing Weak Keys (cont.)

$$T_k \circ A(x) = B \circ T_k(x) \quad \Leftrightarrow \quad (L_A - L_B)(x) = (L_B - \mathrm{id})(k) + c_B - c_A$$

Condition on deterministic commutation

If $T_k \circ A = B \circ T_k$, we must have $L_A = L_B$ and then, $(L_A - \mathrm{id})(k) = c_A - c_B$. Hence,

$$|\mathrm{WeakKeys}| = \begin{cases} p^{n-\mathrm{rank}(L_A - \mathrm{id})} & \text{if } c_A - c_B \in \mathrm{Im}(L_A - \mathrm{id}) \\ 0 & \text{else} \end{cases}.$$

- In Example 1, $\mathrm{rank}(\mathcal{C} - \mathrm{id}) = 3$, so there are 2^{12} weak keys out of 2^{15} choices for k_1

To summarize

For commutation over S and L, we will mainly be interested in those A, B with $d_A := \mathrm{rank}(L_A - \mathrm{id})$ and $d_B := \mathrm{rank}(L_B - \mathrm{id})$ as low as possible (or at least one of them)

Outline

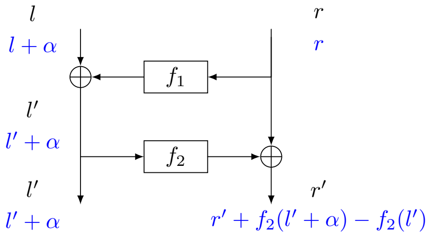
Coming Back to Example 1

- S was a 5-bit S-Box $S\colon \mathbb{F}_2^5 \to \mathbb{F}_2^5$
- $\exists \delta \in \mathbb{F}_2^5 \setminus \{0\}, C \in \mathrm{AGL}(5, \mathbb{F}_2)$ such that $S \circ T_\delta = C \circ S$ and $S \circ C = T_\delta \circ S$
- S was chosen ad-hoc by computer search to allow many weak keys
- In fact, $\mathrm{rank}(L_C - \mathrm{id}) = 1$

Question

How can we construct such S-boxes (with non-trivial differential uniformity)?

A Possible Construction (Two-Round Feistel)



- $S\colon \mathbb{F}_2^{2m} \to \mathbb{F}_2^{2m}, (\ell, r) \mapsto (\ell', r')$ with $\ell' = \ell + f_1(r)$, $r' = r + f_2(\ell')$
- Fulfills $S \circ T_{(\alpha,0)} = B \circ S$ with $B(x,y) = (x+\alpha, y + f_2(x+\alpha) - f_2(x))$
- If f_2 has alg. degree at most 2, then $B \in \mathrm{AGL}(n, \mathbb{F}_2)$
- $\delta_S = 2^m \cdot \max\{\delta_{f_1}, \delta_{f_2}\}$

Example

$f_1 = f_2\colon x \mapsto x^3 (\in \mathbb{F}_{2^n})$. Then $\mathrm{rank}(L_B - \mathrm{id}) = \mathrm{rank}(\alpha x^2 + \alpha^2 x) = m-1$ and $\delta_S = 2^{m+1}$

Relation to Differential Uniformity

- This construction allows trade-offs between differential uniformity and $\mathrm{rank}(L_B - \mathrm{id})$ (corresponding to number of weak keys)
- For instance, choose f_2 with $\delta_{f_2} = 2^{m-1}$. Then, $\delta_S = 2^{n-1}$, but $\mathrm{rank}(L_B - \mathrm{id}) = 1$

Question

How does $\Gamma_S(A, B)$ relate to the differential uniformity δ_S in general (not assuming a specific construction)?

Recall: $\Gamma_S(A, B) := |\{x \mid S \circ A(x) = B \circ S(x)\}|$.

Relation to Differential Uniformity

CASA
Cyber Security in the Age of Large-Scale Adversaries

- This construction allows trade-offs between differential uniformity and $\mathrm{rank}(L_B - \mathrm{id})$ (corresponding to number of weak keys)
- For instance, choose f_2 with $\delta_{f_2} = 2^{m-1}$. Then, $\delta_S = 2^{n-1}$, but $\mathrm{rank}(L_B - \mathrm{id}) = 1$

Question

How does $\Gamma_S(A, B)$ relate to the differential uniformity δ_S in general (not assuming a specific construction)?

Recall: $\Gamma_S(A, B) := |\{x \mid S \circ A(x) = B \circ S(x)\}|$.

Bounds

An upper bound $\Gamma_S(A, B)$ based on the differential uniformity

Let $S, A, B \colon G \to G$. Then,

$$\Gamma_S(A,B) \leq \begin{cases} |\mathrm{Im}(A - \mathrm{id})| \cdot |\mathrm{Im}(B - \mathrm{id})| \cdot \delta_S & \text{if } |\mathrm{Fix}(A)| = \emptyset \\ (|\mathrm{Im}(A - \mathrm{id})| - 1) \cdot |\mathrm{Im}(B - \mathrm{id})| \cdot \delta_S + \min\{|\mathrm{Fix}(A)|, |\mathrm{Fix}(B)|\} & \text{else} \end{cases}.$$

Corollary for $G = \mathbb{F}_p^n$ and $A, B \in \mathrm{AGL}(n, \mathbb{F}_p)$

Let $A = L_A + a, B = L_B + b$ with L_A, L_B linear, $d_A := \mathrm{rank}(L_A - \mathrm{id}), d_B := \mathrm{rank}(L_B - \mathrm{id})$.

$$\Gamma_S(A,B) \leq \begin{cases} p^{d_A + d_B} \cdot \delta_S & \text{if } a \notin \mathrm{Im}(\mathrm{id} - L_A) \\ (p^{d_A} - 1) \cdot p^{d_B} \cdot \delta_S + \min\{p^{n-d_A}, p^{n-d_B}\} & \text{else} \end{cases}.$$

CASA
Cyber Security in the Age of Large-Scale Adversaries

An upper bound $\Gamma_S(A, B)$ based on the differential uniformity

Let $S, A, B\colon G \to G$. Then,

$$\Gamma_S(A,B) \le \begin{cases} |\mathrm{Im}(A-\mathrm{id})| \cdot |\mathrm{Im}(B-\mathrm{id})| \cdot \delta_S & \text{if } |\mathrm{Fix}(A)| = \emptyset \\ (|\mathrm{Im}(A-\mathrm{id})| - 1) \cdot |\mathrm{Im}(B-\mathrm{id})| \cdot \delta_S + \min\{|\mathrm{Fix}(A)|, |\mathrm{Fix}(B)|\} & \text{else} \end{cases}.$$

Corollary for $G = \mathbb{F}_p^n$ and $A, B \in \mathrm{AGL}(n, \mathbb{F}_p)$

Let $A = L_A + a, B = L_B + b$ with L_A, L_B linear, $d_A := \mathrm{rank}(L_A - \mathrm{id}), d_B := \mathrm{rank}(L_B - \mathrm{id})$.

$$\Gamma_S(A,B) \le \begin{cases} p^{d_A+d_B} \cdot \delta_S & \text{if } a \notin \mathrm{Im}(\mathrm{id} - L_A) \\ (p^{d_A} - 1) \cdot p^{d_B} \cdot \delta_S + \min\{p^{n-d_A}, p^{n-d_B}\} & \text{else} \end{cases}.$$

Bounds (cont.)

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

Corollary for $G = \mathbb{F}_p^n$ and $A, B \in \mathrm{AGL}(n, \mathbb{F}_p)$

Let $A = L_A + a, B = L_B + b$ with L_A, L_B linear, $d_A := \mathrm{rank}(L_A - \mathrm{id}), d_B := \mathrm{rank}(L_B - \mathrm{id})$.

$$\Gamma_S(A,B) \leq \begin{cases} p^{d_A+d_B} \cdot \delta_S & \text{if } a \notin \mathrm{Im}(\mathrm{id} - L_A) \\ (p^{d_A} - 1) \cdot p^{d_B} \cdot \delta_S + \min\{p^{n-d_A}, p^{n-d_B}\} & \text{else} \end{cases}.$$

- For low d_A, d_B, the differential uniformity must be high if we want $\Gamma_S(A,B) = p^n$.
- Suppose $\Gamma_S(A,B) = p^n$ for $A = T_\alpha$ $(\alpha \neq 0)$. Then, $\delta_S \geq p^{n-d_B}$.
- The two-round Feistel construction ($p = 2$) given before meets this bound exactly
- If S is bijective and $\Gamma_S(A,B) = p^n$ for $A = T_\alpha$ $(\alpha \neq 0)$, we can further show $d_B \leq \frac{n(p-1)}{p}$, thus, $\delta_S \geq \max\{p^{\frac{n}{p}}, p^{n-d_B}\}$

Bounds (cont.)

CASA — CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

Corollary for $G = \mathbb{F}_p^n$ and $A, B \in \mathrm{AGL}(n, \mathbb{F}_p)$

Let $A = L_A + a, B = L_B + b$ with L_A, L_B linear, $d_A := \mathrm{rank}(L_A - \mathrm{id}), d_B := \mathrm{rank}(L_B - \mathrm{id})$.

$$\Gamma_S(A, B) \leq \begin{cases} p^{d_A + d_B} \cdot \delta_S & \text{if } a \notin \mathrm{Im}(\mathrm{id} - L_A) \\ (p^{d_A} - 1) \cdot p^{d_B} \cdot \delta_S + \min\{p^{n-d_A}, p^{n-d_B}\} & \text{else} \end{cases}.$$

- For low d_A, d_B, the differential uniformity must be high if we want $\Gamma_S(A, B) = p^n$.
- Suppose $\Gamma_S(A, B) = p^n$ for $A = T_\alpha$ $(\alpha \neq 0)$. Then, $\delta_S \geq p^{n-d_B}$.
- The two-round Feistel construction ($p = 2$) given before meets this bound exactly
- If S is bijective and $\Gamma_S(A, B) = p^n$ for $A = T_\alpha$ $(\alpha \neq 0)$, we can further show $d_B \leq \frac{n(p-1)}{p}$, thus, $\delta_S \geq \max\{p^{\frac{n}{p}}, p^{n-d_B}\}$

Bounds (cont.)

CASA
Cyber Security in the Age of Large-Scale Adversaries

Corollary for $G = \mathbb{F}_p^n$ and $A, B \in \mathrm{AGL}(n, \mathbb{F}_p)$

Let $A = L_A + a, B = L_B + b$ with L_A, L_B linear, $d_A := \mathrm{rank}(L_A - \mathrm{id}), d_B := \mathrm{rank}(L_B - \mathrm{id})$.

$$\Gamma_S(A, B) \leq \begin{cases} p^{d_A + d_B} \cdot \delta_S & \text{if } a \notin \mathrm{Im}(\mathrm{id} - L_A) \\ (p^{d_A} - 1) \cdot p^{d_B} \cdot \delta_S + \min\{p^{n-d_A}, p^{n-d_B}\} & \text{else} \end{cases}.$$

- For low d_A, d_B, the differential uniformity must be high if we want $\Gamma_S(A, B) = p^n$.
- Suppose $\Gamma_S(A, B) = p^n$ for $A = T_\alpha$ $(\alpha \neq 0)$. Then, $\delta_S \geq p^{n-d_B}$.
- The two-round Feistel construction $(p = 2)$ given before meets this bound exactly
- If S is bijective and $\Gamma_S(A, B) = p^n$ for $A = T_\alpha$ $(\alpha \neq 0)$, we can further show $d_B \leq \frac{n(p-1)}{p}$, thus, $\delta_S \geq \max\{p^{\frac{n}{p}}, p^{n-d_B}\}$

Bounds (cont.)

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

Corollary for $G = \mathbb{F}_p^n$ and $A, B \in \mathrm{AGL}(n, \mathbb{F}_p)$

Let $A = L_A + a, B = L_B + b$ with L_A, L_B linear, $d_A := \mathrm{rank}(L_A - \mathrm{id}), d_B := \mathrm{rank}(L_B - \mathrm{id})$.

$$\Gamma_S(A,B) \leq \begin{cases} p^{d_A + d_B} \cdot \delta_S & \text{if } a \notin \mathrm{Im}(\mathrm{id} - L_A) \\ (p^{d_A} - 1) \cdot p^{d_B} \cdot \delta_S + \min\{p^{n-d_A}, p^{n-d_B}\} & \text{else} \end{cases}.$$

- For low d_A, d_B, the differential uniformity must be high if we want $\Gamma_S(A,B) = p^n$.
- Suppose $\Gamma_S(A,B) = p^n$ for $A = T_\alpha$ $(\alpha \neq 0)$. Then, $\delta_S \geq p^{n-d_B}$.
- The two-round Feistel construction $(p = 2)$ given before meets this bound exactly
- If S is bijective and $\Gamma_S(A,B) = p^n$ for $A = T_\alpha$ $(\alpha \neq 0)$, we can further show $d_B \leq \frac{n(p-1)}{p}$, thus, $\delta_S \geq \max\{p^{\frac{n}{p}}, p^{n-d_B}\}$

Bounds (cont.)

Corollary for $G = \mathbb{F}_p^n$ and $A, B \in \mathrm{AGL}(n, \mathbb{F}_p)$

Let $A = L_A + a, B = L_B + b$ with L_A, L_B linear, $d_A := \mathrm{rank}(L_A - \mathrm{id}), d_B := \mathrm{rank}(L_B - \mathrm{id})$.

$$\Gamma_S(A, B) \leq \begin{cases} p^{d_A + d_B} \cdot \delta_S & \text{if } a \notin \mathrm{Im}(\mathrm{id} - L_A) \\ (p^{d_A} - 1) \cdot p^{d_B} \cdot \delta_S + \min\{p^{n-d_A}, p^{n-d_B}\} & \text{else} \end{cases}.$$

- For low d_A, d_B, the differential uniformity must be high if we want $\Gamma_S(A, B) = p^n$.
- Suppose $\Gamma_S(A, B) = p^n$ for $A = T_\alpha$ $(\alpha \neq 0)$. Then, $\delta_S \geq p^{n-d_B}$.
- The two-round Feistel construction $(p = 2)$ given before meets this bound exactly
- If S is bijective and $\Gamma_S(A, B) = p^n$ for $A = T_\alpha$ $(\alpha \neq 0)$, we can further show $d_B \leq \frac{n(p-1)}{p}$, thus, $\delta_S \geq \max\{p^{\frac{n}{p}}, p^{n-d_B}\}$

Link to APN Functions with Self-Equivalences

CASA — Cyber Security in the Age of Large-Scale Adversaries

Corollary for $G = \mathbb{F}_p^n$ and $A, B \in \mathrm{AGL}(n, \mathbb{F}_p)$

Let $A = L_A + a, B = L_B + b$ with L_A, L_B linear, $d_A := \mathrm{rank}(L_A - \mathrm{id}), d_B := \mathrm{rank}(L_B - \mathrm{id})$.

$$\Gamma_S(A,B) \leq \begin{cases} p^{d_A+d_B} \cdot \delta_S & \text{if } a \notin \mathrm{Im}(\mathrm{id} - L_A) \\ (p^{d_A}-1) \cdot p^{d_B} \cdot \delta_S + \min\{p^{n-d_A}, p^{n-d_B}\} & \text{else} \end{cases}.$$

- If $\Gamma_S(A,B) = p^n$, then $S = B^{-1} \circ S \circ A$ (i.e., (A,B) defines an affine self-equivalence)
- Suppose $\Gamma_S(A,B) = p^n$ (no further restriction on A now). Then, $\delta_S > p^{n-(d_A+d_B)-1}$.
- If we want $\Gamma_S(A,B) = p^n$ and $\delta_S \leq p$, we obtain $d_A + d_B > n - 2$
- APN case: If $S \colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ is APN with affine self-equivalence $S = B^{-1} \circ S \circ A$, then $d_A + d_B > n - 2$

Link to APN Functions with Self-Equivalences

CASA
Cyber Security in the Age of Large-Scale Adversaries

Corollary for $G = \mathbb{F}_p^n$ and $A, B \in \mathrm{AGL}(n, \mathbb{F}_p)$

Let $A = L_A + a, B = L_B + b$ with L_A, L_B linear, $d_A := \mathrm{rank}(L_A - \mathrm{id}), d_B := \mathrm{rank}(L_B - \mathrm{id})$.

$$\Gamma_S(A, B) \leq \begin{cases} p^{d_A + d_B} \cdot \delta_S & \text{if } a \notin \mathrm{Im}(\mathrm{id} - L_A) \\ (p^{d_A} - 1) \cdot p^{d_B} \cdot \delta_S + \min\{p^{n-d_A}, p^{n-d_B}\} & \text{else} \end{cases}.$$

- If $\Gamma_S(A, B) = p^n$, then $S = B^{-1} \circ S \circ A$ (i.e., (A, B) defines an affine self-equivalence)
- Suppose $\Gamma_S(A, B) = p^n$ (no further restriction on A now). Then, $\delta_S > p^{n-(d_A+d_B)-1}$.
- If we want $\Gamma_S(A, B) = p^n$ and $\delta_S \leq p$, we obtain $d_A + d_B > n - 2$
- APN case: If $S \colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ is APN with affine self-equivalence $S = B^{-1} \circ S \circ A$, then $d_A + d_B > n - 2$

Link to APN Functions with Self-Equivalences

CASA
Cyber Security in the Age of Large-Scale Adversaries

Corollary for $G = \mathbb{F}_p^n$ and $A, B \in \mathrm{AGL}(n, \mathbb{F}_p)$

Let $A = L_A + a, B = L_B + b$ with L_A, L_B linear, $d_A := \mathrm{rank}(L_A - \mathrm{id}), d_B := \mathrm{rank}(L_B - \mathrm{id})$.

$$\Gamma_S(A, B) \leq \begin{cases} p^{d_A + d_B} \cdot \delta_S & \text{if } a \notin \mathrm{Im}(\mathrm{id} - L_A) \\ (p^{d_A} - 1) \cdot p^{d_B} \cdot \delta_S + \min\{p^{n-d_A}, p^{n-d_B}\} & \text{else} \end{cases}.$$

- If $\Gamma_S(A, B) = p^n$, then $S = B^{-1} \circ S \circ A$ (i.e., (A, B) defines an affine self-equivalence)
- Suppose $\Gamma_S(A, B) = p^n$ (no further restriction on A now). Then, $\delta_S > p^{n-(d_A+d_B)-1}$.
- If we want $\Gamma_S(A, B) = p^n$ and $\delta_S \leq p$, we obtain $d_A + d_B > n - 2$
- APN case: If $S \colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ is APN with affine self-equivalence $S = B^{-1} \circ S \circ A$, then $d_A + d_B > n - 2$

Link to APN Functions with Self-Equivalences

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

Corollary for $G = \mathbb{F}_p^n$ and $A, B \in \mathrm{AGL}(n, \mathbb{F}_p)$

Let $A = L_A + a, B = L_B + b$ with L_A, L_B linear, $d_A := \mathrm{rank}(L_A - \mathrm{id}), d_B := \mathrm{rank}(L_B - \mathrm{id})$.

$$\Gamma_S(A, B) \leq \begin{cases} p^{d_A+d_B} \cdot \delta_S & \text{if } a \notin \mathrm{Im}(\mathrm{id} - L_A) \\ (p^{d_A} - 1) \cdot p^{d_B} \cdot \delta_S + \min\{p^{n-d_A}, p^{n-d_B}\} & \text{else} \end{cases}.$$

- If $\Gamma_S(A, B) = p^n$, then $S = B^{-1} \circ S \circ A$ (i.e., (A, B) defines an affine self-equivalence)
- Suppose $\Gamma_S(A, B) = p^n$ (no further restriction on A now). Then, $\delta_S > p^{n-(d_A+d_B)-1}$.
- If we want $\Gamma_S(A, B) = p^n$ and $\delta_S \leq p$, we obtain $d_A + d_B > n - 2$
- APN case: If $S\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ is APN with affine self-equivalence $S = B^{-1} \circ S \circ A$, then $d_A + d_B > n - 2$

Link to APN Functions with Self-Equivalences

CASA — Cyber Security in the Age of Large-Scale Adversaries

Corollary for $G = \mathbb{F}_p^n$ and $A, B \in \mathrm{AGL}(n, \mathbb{F}_p)$

Let $A = L_A + a, B = L_B + b$ with L_A, L_B linear, $d_A := \mathrm{rank}(L_A - \mathrm{id}), d_B := \mathrm{rank}(L_B - \mathrm{id})$.

$$\Gamma_S(A, B) \leq \begin{cases} p^{d_A + d_B} \cdot \delta_S & \text{if } a \notin \mathrm{Im}(\mathrm{id} - L_A) \\ (p^{d_A} - 1) \cdot p^{d_B} \cdot \delta_S + \min\{p^{n-d_A}, p^{n-d_B}\} & \text{else} \end{cases}.$$

- If $\Gamma_S(A, B) = p^n$, then $S = B^{-1} \circ S \circ A$ (i.e., (A, B) defines an affine self-equivalence)
- Suppose $\Gamma_S(A, B) = p^n$ (no further restriction on A now). Then, $\delta_S > p^{n-(d_A+d_B)-1}$.
- If we want $\Gamma_S(A, B) = p^n$ and $\delta_S \leq p$, we obtain $d_A + d_B > n - 2$
- APN case: If $S \colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ is APN with affine self-equivalence $S = B^{-1} \circ S \circ A$, then $d_A + d_B > n - 2$

Link to APN Functions with Self-Equivalences

CASA
Cyber Security in the Age of Large-Scale Adversaries

Theorem [B., Brinkmann, Leander, 2021]

Suppose $F\colon \mathbb{F}_2^8 \to \mathbb{F}_2^8$ is an APN permutation with non-trivial linear self-equivalence. Then, F is CCZ-equivalent to a permutation G for which $G \circ A = B \circ G$ with

1. $B = A = \mathrm{Comp}(X^4 + X^3 + X^2 + X + 1) \oplus \mathrm{Comp}(X^4 + X^3 + X^2 + X + 1)$ or
2. $B = A = I_2 \oplus \mathrm{Comp}(X^2 + 1) \oplus \mathrm{Comp}(X^2 + 1) \oplus \mathrm{Comp}(X^2 + 1)$.

- With our bound, it follows that Class 2 is impossible!

Outline

CASA
Cyber Security in the Age of Large-Scale Adversaries

Commutation over Linear Layer [Baudrin et al., 2023]

Let $A = L_A + c_A, B = L_B + c_B \in \mathrm{AGL}(n, \mathbb{F}_p)$ with L_A, L_B linear.

$$L \circ A(x) = B \circ L(x) \quad \Leftrightarrow \quad (L \circ L_A - L_B \circ L)(x) = c_B - L(c_A)$$

Corollary

$$\Gamma_L(A, B) = \begin{cases} 0 & \text{if } c_B - L(c_A) \notin \mathrm{Im}(L \circ L_A - L_B \circ L) \\ 2^{\dim \ker(L \circ L_A - L_B \circ L)} & \text{otherwise} \end{cases} .$$

Further, $\Gamma_L(A, B) = p^n$ if and only if $L \circ L_A = L_B \circ L$ and $c_B = L(c_A)$.

- We are mainly interested in the case where L_A and L_B are block-diagonal matrices (aligned with the size of the S-box)

CASA Cyber Security in the Age of Large-Scale Adversaries

Commutation over Linear Layer [Baudrin et al., 2023]

Let $A = L_A + c_A, B = L_B + c_B \in \mathrm{AGL}(n, \mathbb{F}_p)$ with L_A, L_B linear.

$$L \circ A(x) = B \circ L(x) \quad \Leftrightarrow \quad (L \circ L_A - L_B \circ L)(x) = c_B - L(c_A)$$

Corollary

$$\Gamma_L(A,B) = \begin{cases} 0 & \text{if } c_B - L(c_A) \notin \mathrm{Im}(L \circ L_A - L_B \circ L) \\ 2^{\dim\ker(L \circ L_A - L_B \circ L)} & \text{otherwise} \end{cases}.$$

Further, $\Gamma_L(A,B) = p^n$ if and only if $L \circ L_A = L_B \circ L$ and $c_B = L(c_A)$.

- We are mainly interested in the case where L_A and L_B are block-diagonal matrices (aligned with the size of the S-box)

Commutation over Linear Layer [Baudrin et al., 2023]

CASA
Cyber Security in the Age of Large-Scale Adversaries

Let $A = L_A + c_A, B = L_B + c_B \in \mathrm{AGL}(n, \mathbb{F}_p)$ with L_A, L_B linear.

$$L \circ A(x) = B \circ L(x) \quad \Leftrightarrow \quad (L \circ L_A - L_B \circ L)(x) = c_B - L(c_A)$$

Corollary

$$\Gamma_L(A, B) = \begin{cases} 0 & \text{if } c_B - L(c_A) \notin \mathrm{Im}(L \circ L_A - L_B \circ L) \\ 2^{\dim \ker(L \circ L_A - L_B \circ L)} & \text{otherwise} \end{cases} .$$

Further, $\Gamma_L(A, B) = p^n$ if and only if $L \circ L_A = L_B \circ L$ and $c_B = L(c_A)$.

- We are mainly interested in the case where L_A and L_B are block-diagonal matrices (aligned with the size of the S-box)

Commutation over Linear Layer (cont.)

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

Commutation for Block-Diagonal Matrices

Let $L_A = \mathrm{Diag}(L_A^{(1)}, \ldots, L_A^{(m)})$ and $L_B = \mathrm{Diag}(L_B^{(1)}, \ldots, L_B^{(m)})$. Then, $L \circ L_A = L_B \circ L$ if and only if $L_{ij} \circ L_A^{(j)} = L_B^{(i)} \circ L_{ij}$ for all i, j, where L_{ij} are the blocks of L.

- Given L_A, L_B, such L can be constructed using linear algebra (solving equations with coefficients of L as unknowns)

Conclusion

- In the commutative cryptanalysis framework, differentials have the best potential for an attack
- A commutative attack cannot be better than a differential attack, unless in the weak-key model and/or if properties of the key-schedule are exploited
- c-differentials belong to those cases with the least potential to mount attacks
- Still, the study of S-boxes with respect to more general notions than differential uniformity can be interesting from a mathematical point of view (e.g., understanding probability-1 differentials over multiple rounds, example of APNs with fixed points)

Conclusion

- In the commutative cryptanalysis framework, differentials have the best potential for an attack
- A commutative attack cannot be better than a differential attack, unless in the weak-key model and/or if properties of the key-schedule are exploited
- c-differentials belong to those cases with the least potential to mount attacks
- Still, the study of S-boxes with respect to more general notions than differential uniformity can be interesting from a mathematical point of view (e.g., understanding probability-1 differentials over multiple rounds, example of APNs with fixed points)

Conclusion

- In the commutative cryptanalysis framework, differentials have the best potential for an attack
- A commutative attack cannot be better than a differential attack, unless in the weak-key model and/or if properties of the key-schedule are exploited
- c-differentials belong to those cases with the least potential to mount attacks
- Still, the study of S-boxes with respect to more general notions than differential uniformity can be interesting from a mathematical point of view (e.g., understanding probability-1 differentials over multiple rounds, example of APNs with fixed points)

Conclusion

- In the commutative cryptanalysis framework, differentials have the best potential for an attack
- A commutative attack cannot be better than a differential attack, unless in the weak-key model and/or if properties of the key-schedule are exploited
- c-differentials belong to those cases with the least potential to mount attacks
- Still, the study of S-boxes with respect to more general notions than differential uniformity can be interesting from a mathematical point of view (e.g., understanding probability-1 differentials over multiple rounds, example of APNs with fixed points)