On Perfect Linear Approximations and Differentials over Two-Round SPNs

CRYPTO 2023, August 23, 2023

Christof Beierle, Patrick Felke, Gregor Leander, Patrick Neumann, Lukas Stennes

CASA
Cyber Security in the Age of Large-Scale Adversaries

Ruhr Universität Bochum RUB
University of Applied Sciences Hochschule Emden • Leer

Gefördert durch DFG Deutsche Forschungsgemeinschaft

Horst Görtz Institut

Arguments for Security

- Security of symmetric primitives based on resilience to existing attacks

Arguments for Security

- Security of symmetric primitives based on resilience to existing attacks
- Example: Block cipher E_k

Arguments for Security

- Security of symmetric primitives based on resilience to existing attacks
- Example: Block cipher E_k
- Desirable: resilience for (almost) all keys

Arguments for Security

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

- Security of symmetric primitives based on resilience to existing attacks
- Example: Block cipher E_k
- Desirable: resilience for (almost) all keys

Attack	Bound for (almost) all k
Linear	$\mathrm{C}[\gamma \xrightarrow{E_k} \zeta] := 2 \cdot \left(\mathrm{P}_x[\langle \gamma, x\rangle = \langle \zeta, E_k(x)\rangle] - \frac{1}{2}\right)$

Arguments for Security

- Security of symmetric primitives based on resilience to existing attacks
- Example: Block cipher E_k
- Desirable: resilience for (almost) all keys

Attack	Bound for (almost) all k
Linear	$\mathrm{C}[\gamma \xrightarrow{E_k} \zeta] := 2 \cdot \left(\mathrm{P}_{\mathrm{x}}[\langle \gamma, x \rangle = \langle \zeta, E_k(x) \rangle] - \frac{1}{2}\right)$
Differential	$\mathrm{P}[\alpha \xrightarrow{E_k} \beta] := \mathrm{P}_{\mathrm{x}}[E_k(x) \oplus E_k(x \oplus \alpha) = \beta]$

Arguments for Security

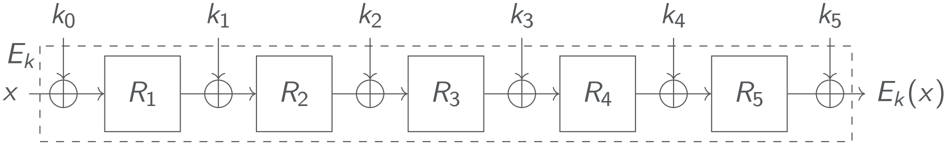
CASA
Cyber Security in the Age of Large-Scale Adversaries

- Security of symmetric primitives based on resilience to existing attacks
- Example: Block cipher E_k
- Desirable: resilience for (almost) all keys

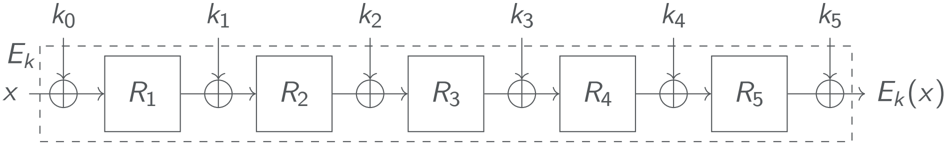
Attack	Bound for (almost) all k
Linear	$\mathrm{C}[\gamma \xrightarrow{E_k} \zeta] := 2 \cdot \left(\mathrm{P}_{\mathrm{x}}[\langle \gamma, x \rangle = \langle \zeta, E_k(x) \rangle] - \frac{1}{2}\right)$
Differential	$\mathrm{P}[\alpha \xrightarrow{E_k} \beta] := \mathrm{P}_{\mathrm{x}}[E_k(x) \oplus E_k(x \oplus \alpha) = \beta]$

- Only possible if E_k has structure

For Round-Based Primitives

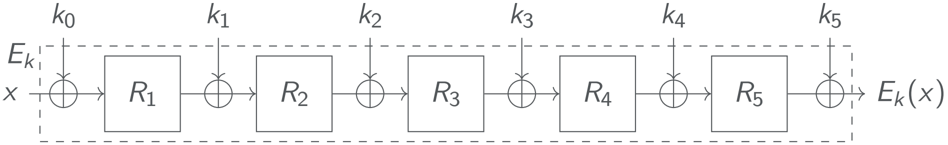


For Round-Based Primitives



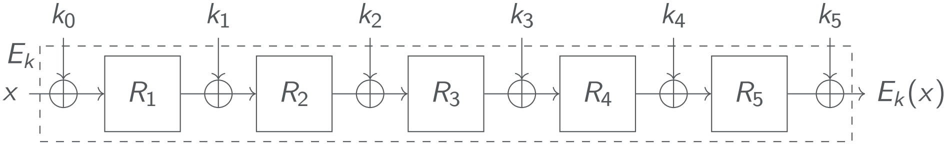
- Start with $\mathrm{C}[\gamma \xrightarrow{R_i} \zeta]$ and $\mathrm{P}[\alpha \xrightarrow{R_i} \beta]$

For Round-Based Primitives

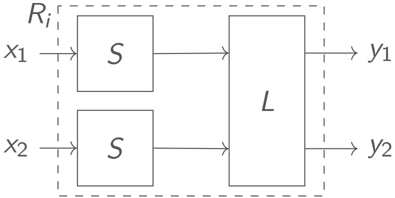


- Start with $C[\gamma \xrightarrow{R_i} \zeta]$ and $P[\alpha \xrightarrow{R_i} \beta]$
- Often only possible if R_i themselves have structure

For Round-Based Primitives

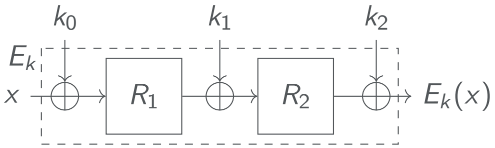


- Start with $C[\gamma \xrightarrow{R_i} \zeta]$ and $P[\alpha \xrightarrow{R_i} \beta]$
- Often only possible if R_i themselves have structure
- Here: focus on SPNs



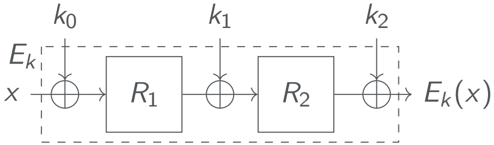
For Two Rounds

CASA
Cyber Security in the Age of Large-Scale Adversaries



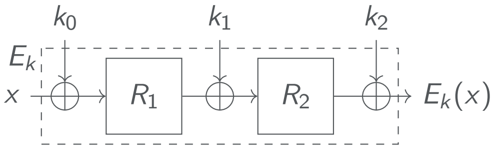
For Two Rounds

$$\mathrm{P}[\, \alpha \xrightarrow{E_k} \beta \,]$$



For Two Rounds

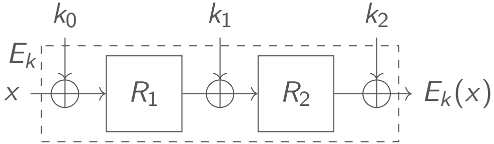
$$\mathrm{P}[\,\alpha \xrightarrow{\quad E_k \quad} \beta\,]$$



$$\mathrm{P}[\,\alpha \longrightarrow \delta \longrightarrow \beta\,]$$

For Two Rounds

$$\mathrm{P}[\,\alpha \xrightarrow{\quad E_k \quad} \beta\,]$$

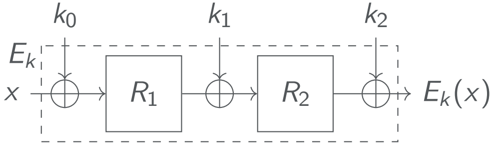


$$\mathrm{P}[\,\alpha \longrightarrow \delta \longrightarrow \beta\,]$$

$$= \quad \mathrm{P}[\alpha \xrightarrow{R_1} \delta] \cdot \mathrm{P}[\delta \xrightarrow{R_2} \beta]$$

For Two Rounds

$$\mathrm{P}[\,\alpha \xrightarrow{\qquad E_k \qquad} \beta\,]$$

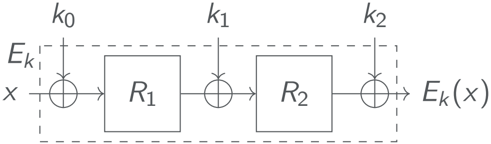


$$\sum_\delta \mathrm{P}[\,\alpha \longrightarrow \delta \longrightarrow \beta\,]$$

$$= \sum_\delta \mathrm{P}[\alpha \xrightarrow{R_1} \delta] \cdot \mathrm{P}[\delta \xrightarrow{R_2} \beta]$$

For Two Rounds

$$\mathrm{P}[\,\alpha \xrightarrow{\qquad\qquad E_k \qquad\qquad} \beta\,]$$



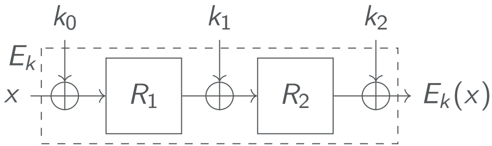
$$\sum_\delta \mathrm{P}[\,\alpha \xrightarrow{\qquad\qquad} \delta \xrightarrow{\qquad\qquad} \beta\,]$$

$$= \sum_\delta \quad \mathrm{P}[\alpha \xrightarrow{R_1} \delta] \;\cdot\; \mathrm{P}[\delta \xrightarrow{R_2} \beta]$$

- Gives only average $\mathrm{P}[\alpha \xrightarrow{E_k} \beta]$ (over the key)

For Two Rounds

$$\mathrm{P}[\,\alpha \xrightarrow{\qquad\qquad E_k \qquad\qquad} \beta\,]$$



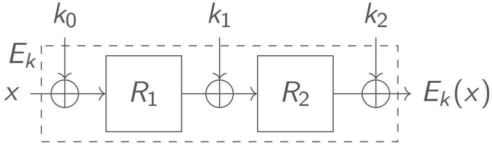
$$\sum_\delta \mathrm{P}[\,\alpha \xrightarrow{\qquad\qquad} \delta \xrightarrow{\qquad\qquad} \beta\,]$$

$$= \sum_\delta \mathrm{P}[\alpha \xrightarrow{R_1} \delta] \cdot \mathrm{P}[\delta \xrightarrow{R_2} \beta]$$

- Gives only average $\mathrm{P}[\alpha \xrightarrow{E_k} \beta]$ (over the key)
- Similarly: get only average $\mathrm{C}[\gamma \xrightarrow{E_k} \zeta]^2$ (over the key)

For Two Rounds

$$\mathrm{P}[\alpha \xrightarrow{\quad E_k \quad} \beta]$$

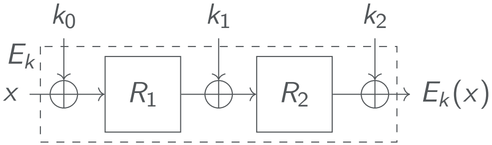


$$\sum_\delta \mathrm{P}[\alpha \longrightarrow \delta \longrightarrow \beta]$$

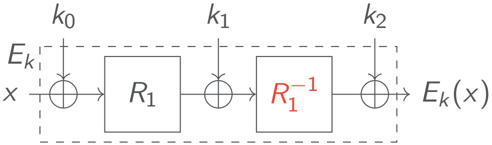
$$= \sum_\delta \mathrm{P}[\alpha \xrightarrow{R_1} \delta] \cdot \mathrm{P}[\delta \xrightarrow{R_2} \beta]$$

- Gives only average $\mathrm{P}[\alpha \xrightarrow{E_k} \beta]$ (over the key)
- Similarly: get only average $\mathrm{C}[\gamma \xrightarrow{E_k} \zeta]^2$ (over the key)
- Can we do better?

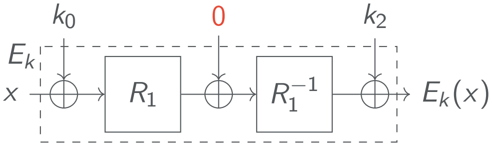
For Two Rounds and all keys



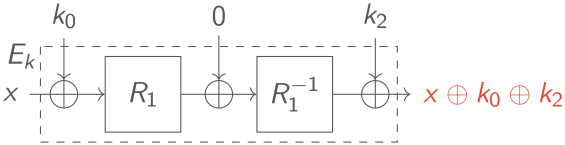
For Two Rounds and all keys



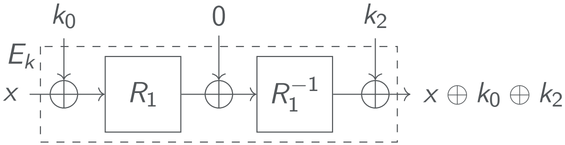
For Two Rounds and all keys



For Two Rounds and all keys

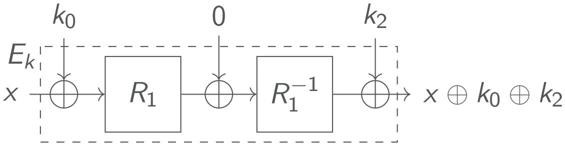


For Two Rounds and all keys



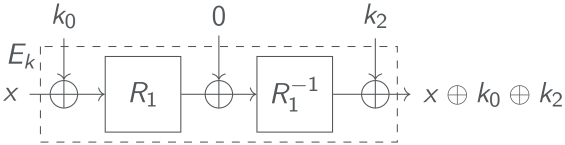
- $\left|\mathrm{C}[\gamma \xrightarrow{E_k} \gamma]\right| = 1$ and $\mathrm{P}[\alpha \xrightarrow{E_k} \alpha] = 1$, even if R_1 is resilient

For Two Rounds and all keys



- $\left|\mathrm{C}[\gamma \xrightarrow{E_k} \gamma]\right| = 1$ and $\mathrm{P}[\alpha \xrightarrow{E_k} \alpha] = 1$, even if R_1 is resilient
- Seeing rounds as independent cannot work!

For Two Rounds and all keys



- $\left|C[\gamma \xrightarrow{E_k} \gamma]\right| = 1$ and $P[\alpha \xrightarrow{E_k} \alpha] = 1$, even if R_1 is resilient
- Seeing rounds as independent cannot work!

As a First Step

Answer existence of k such that

- $\left|C[\gamma \xrightarrow{E_k} \zeta]\right| = 1$ (perfect linear approximation), or
- $P[\alpha \xrightarrow{E_k} \beta] = 1$ (perfect differential)

for two-round SPNs

Existence of Perfect Linear Approximations

- Perfect linear approximation: there exist $\gamma, \zeta \neq 0$ s.t.

$$\left|\mathrm{cor}(\gamma \xrightarrow{E_k} \zeta)\right| = 1 \iff \exists c : \quad \langle \gamma, x \rangle = \langle \zeta, E_k(x) \rangle \oplus c \quad \forall x$$

Existence of Perfect Linear Approximations

CASA
Cyber Security in the Age of Large-Scale Adversaries

- Perfect linear approximation: there exist $\gamma, \zeta \neq 0$ s.t.

$$\left|\mathrm{cor}(\gamma \xrightarrow{E_k} \zeta)\right| = 1 \quad \iff \quad \exists c : \quad \langle \gamma, x \rangle = \langle \zeta, E_k(x) \rangle \oplus c \quad \forall x$$

- For fixed k: easy to find all perfect linear approximations

Existence of Perfect Linear Approximations

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

- Perfect linear approximation: there exist $\gamma, \zeta \neq 0$ s.t.

$$\left|\mathrm{cor}(\gamma \xrightarrow{E_k} \zeta)\right| = 1 \quad \iff \quad \exists c : \quad \langle \gamma, x \rangle = \langle \zeta, E_k(x) \rangle \oplus c \quad \forall x$$

- For fixed k: easy to find all perfect linear approximations
  - For each x we get a linear equation in γ, ζ and c

Existence of Perfect Linear Approximations

CASA
Cyber Security in the Age of Large-Scale Adversaries

- Perfect linear approximation: there exist $\gamma, \zeta \neq 0$ s.t.

$$\left|\mathrm{cor}(\gamma \xrightarrow{E_k} \zeta)\right| = 1 \quad \iff \quad \exists c : \quad \langle \gamma, x \rangle = \langle \zeta, E_k(x) \rangle \oplus c \quad \forall x$$

- For fixed k: easy to find all perfect linear approximations
  - For each x we get a linear equation in γ, ζ and c
  - Solving the system leads to all perfect linear approximations

Existence of Perfect Linear Approximations

- Perfect linear approximation: there exist $\gamma, \zeta \neq 0$ s.t.

$$\left|\mathrm{cor}(\gamma \xrightarrow{E_k} \zeta)\right| = 1 \quad \Longleftrightarrow \quad \exists c : \quad \langle \gamma, x \rangle = \langle \zeta, E_k(x) \rangle \oplus c \quad \forall x$$

- For fixed k: easy to find all perfect linear approximations
  - For each x we get a linear equation in γ, ζ and c
  - Solving the system leads to all perfect linear approximations
- Question: Do some k lead to perfect linear approximations?

Existence of Perfect Linear Approximations

- Perfect linear approximation: there exist $\gamma, \zeta \neq 0$ s.t.

$$\left|\mathrm{cor}(\gamma \xrightarrow{E_k} \zeta)\right| = 1 \quad \Longleftrightarrow \quad \exists c : \quad \langle \gamma, x \rangle = \langle \zeta, E_k(x) \rangle \oplus c \quad \forall x$$

- For fixed k: easy to find all perfect linear approximations
  - For each x we get a linear equation in γ, ζ and c
  - Solving the system leads to all perfect linear approximations
- Question: Do some k lead to perfect linear approximations?
  - Problem: often infeasible to try all k

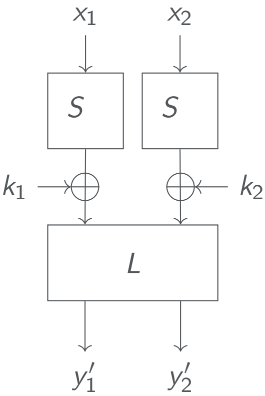
Existence of Perfect Linear Approximations

- Perfect linear approximation: there exist $\gamma, \zeta \neq 0$ s.t.

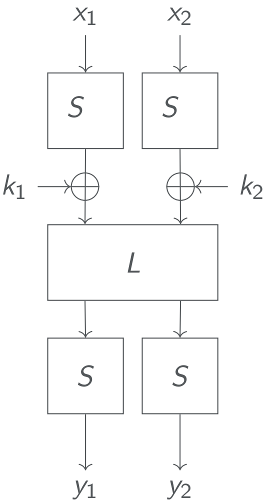
$$\left|\operatorname{cor}(\gamma \xrightarrow{E_k} \zeta)\right| = 1 \quad \iff \quad \exists c : \quad \langle \gamma, x \rangle = \langle \zeta, E_k(x) \rangle \oplus c \quad \forall x$$

- For fixed k: easy to find all perfect linear approximations
  - For each x we get a linear equation in γ, ζ and c
  - Solving the system leads to all perfect linear approximations
- Question: Do some k lead to perfect linear approximations?
  - Problem: often infeasible to try all k
  - For two-round SPNs: can be (efficiently) answered

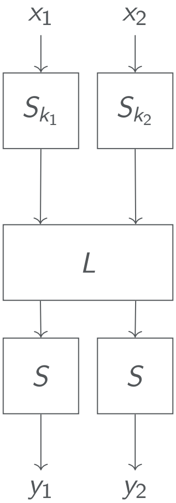
Existence of Perfect Linear Approximations over Two-Round SPNs



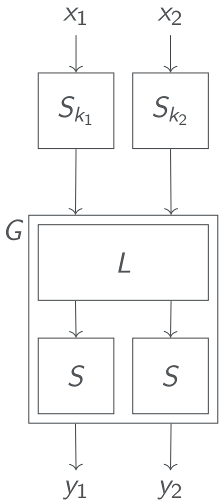
Existence of Perfect Linear Approximations over Two-Round SPNs



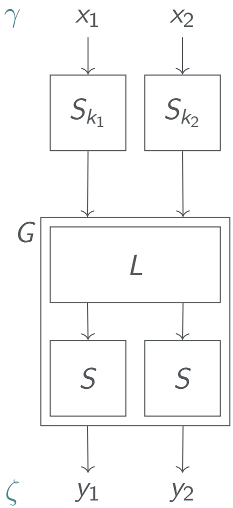
Existence of Perfect Linear Approximations over Two-Round SPNs



Existence of Perfect Linear Approximations over Two-Round SPNs

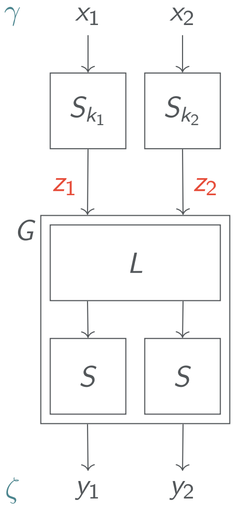


Existence of Perfect Linear Approximations over Two-Round SPNs



$$\left\langle \gamma, \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \right\rangle = \left\langle \zeta, \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \right\rangle \oplus c$$

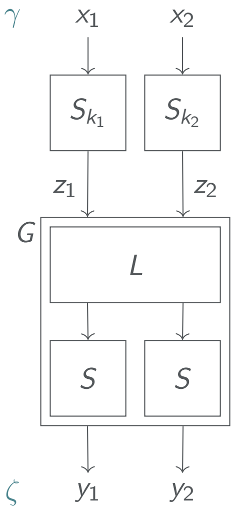
Existence of Perfect Linear Approximations over Two-Round SPNs



$$\langle \gamma, \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \rangle = \langle \zeta, \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \rangle \oplus c$$

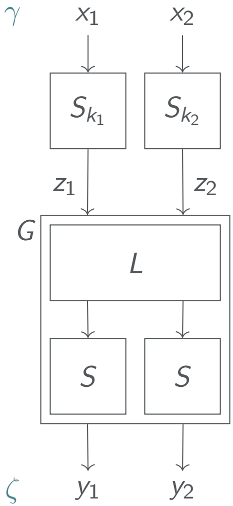
Existence of Perfect Linear Approximations over Two-Round SPNs

CASA
Cyber Security in the Age of Large-Scale Adversaries



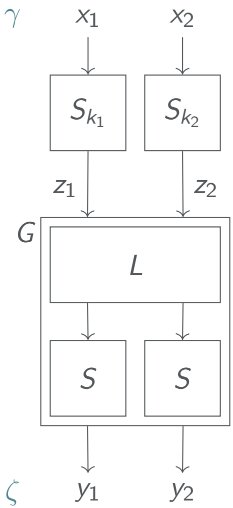
$$\left\langle \gamma, \begin{pmatrix} S_{k_1}^{-1}(z_1) \\ S_{k_2}^{-1}(z_2) \end{pmatrix} \right\rangle = \left\langle \gamma, \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \right\rangle = \left\langle \zeta, \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \right\rangle \oplus c$$

Existence of Perfect Linear Approximations over Two-Round SPNs



$$\left\langle \gamma, \begin{pmatrix} S_{k_1}^{-1}(z_1) \\ S_{k_2}^{-1}(z_2) \end{pmatrix} \right\rangle = \left\langle \gamma, \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \right\rangle = \left\langle \zeta, \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \right\rangle \oplus c = \left\langle \zeta, G \begin{pmatrix} z_1 \\ z_2 \end{pmatrix} \right\rangle \oplus c$$

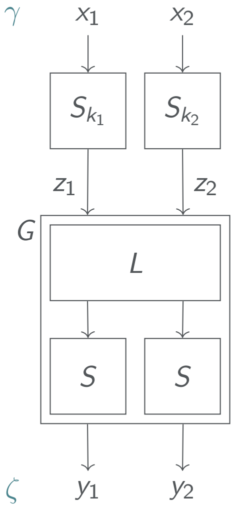
Existence of Perfect Linear Approximations over Two-Round SPNs



$$\left\langle \gamma, \begin{pmatrix} S_{k_1}^{-1}(z_1) \\ S_{k_2}^{-1}(z_2) \end{pmatrix} \right\rangle = \left\langle \gamma, \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \right\rangle = \left\langle \zeta, \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \right\rangle \oplus c = \left\langle \zeta, G \begin{pmatrix} z_1 \\ z_2 \end{pmatrix} \right\rangle \oplus c$$

$$\begin{pmatrix} S_{k_1}^{-1}(z_1') \\ S_{k_2}^{-1}(z_2') \end{pmatrix} \oplus \begin{pmatrix} S_{k_1}^{-1}(z_1') \\ S_{k_2}^{-1}(0) \end{pmatrix} = \begin{pmatrix} S_{k_1}^{-1}(0) \\ S_{k_2}^{-1}(z_2') \end{pmatrix} \oplus \begin{pmatrix} S_{k_1}^{-1}(0) \\ S_{k_2}^{-1}(0) \end{pmatrix}$$

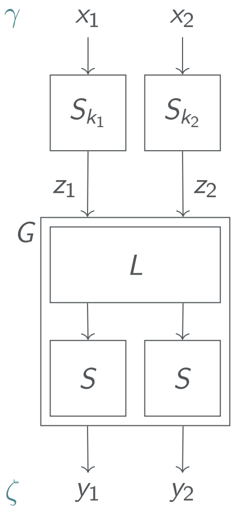
Existence of Perfect Linear Approximations over Two-Round SPNs



$$\left\langle \gamma, \begin{pmatrix} S_{k_1}^{-1}(z_1) \\ S_{k_2}^{-1}(z_2) \end{pmatrix} \right\rangle = \left\langle \gamma, \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \right\rangle = \left\langle \zeta, \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \right\rangle \oplus c = \left\langle \zeta, G \begin{pmatrix} z_1 \\ z_2 \end{pmatrix} \right\rangle \oplus c$$

$$\left\langle \gamma, \begin{pmatrix} S_{k_1}^{-1}(z_1') \\ S_{k_2}^{-1}(z_2') \end{pmatrix} \right\rangle \oplus \left\langle \gamma, \begin{pmatrix} S_{k_1}^{-1}(z_1') \\ S_{k_2}^{-1}(0) \end{pmatrix} \right\rangle = \left\langle \gamma, \begin{pmatrix} S_{k_1}^{-1}(0) \\ S_{k_2}^{-1}(z_2') \end{pmatrix} \right\rangle \oplus \left\langle \gamma, \begin{pmatrix} S_{k_1}^{-1}(0) \\ S_{k_2}^{-1}(0) \end{pmatrix} \right\rangle$$

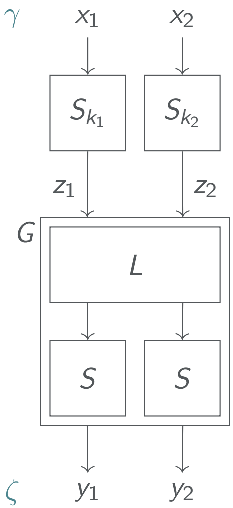
Existence of Perfect Linear Approximations over Two-Round SPNs



$$\left\langle \gamma, \begin{pmatrix} S_{k_1}^{-1}(z_1) \\ S_{k_2}^{-1}(z_2) \end{pmatrix} \right\rangle = \left\langle \gamma, \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \right\rangle = \left\langle \zeta, \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \right\rangle \oplus c = \left\langle \zeta, G \begin{pmatrix} z_1 \\ z_2 \end{pmatrix} \right\rangle \oplus c$$

$$\underbrace{\left\langle \gamma, \begin{pmatrix} S_{k_1}^{-1}(z_1') \\ S_{k_2}^{-1}(z_2') \end{pmatrix} \right\rangle}_{\left\langle \zeta, G \begin{pmatrix} z_1' \\ z_2' \end{pmatrix} \right\rangle \oplus c} \oplus \underbrace{\left\langle \gamma, \begin{pmatrix} S_{k_1}^{-1}(z_1') \\ S_{k_2}^{-1}(0) \end{pmatrix} \right\rangle}_{\left\langle \zeta, G \begin{pmatrix} z_1' \\ 0 \end{pmatrix} \right\rangle \oplus c} = \underbrace{\left\langle \gamma, \begin{pmatrix} S_{k_1}^{-1}(0) \\ S_{k_2}^{-1}(z_2') \end{pmatrix} \right\rangle}_{\left\langle \zeta, G \begin{pmatrix} 0 \\ z_2' \end{pmatrix} \right\rangle \oplus c} \oplus \underbrace{\left\langle \gamma, \begin{pmatrix} S_{k_1}^{-1}(0) \\ S_{k_2}^{-1}(0) \end{pmatrix} \right\rangle}_{\left\langle \zeta, G \begin{pmatrix} 0 \\ 0 \end{pmatrix} \right\rangle \oplus c}$$

Existence of Perfect Linear Approximations over Two-Round SPNs



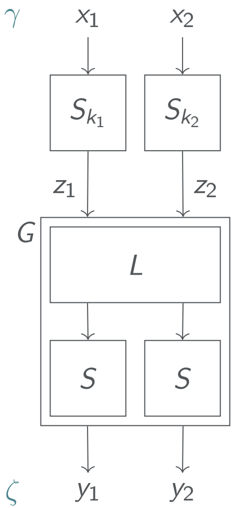
$$\left\langle \gamma, \begin{pmatrix} S_{k_1}^{-1}(z_1) \\ S_{k_2}^{-1}(z_2) \end{pmatrix} \right\rangle = \left\langle \gamma, \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \right\rangle = \left\langle \zeta, \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \right\rangle \oplus c = \left\langle \zeta, G \begin{pmatrix} z_1 \\ z_2 \end{pmatrix} \right\rangle \oplus c$$

$$\underbrace{\left\langle \gamma, \begin{pmatrix} S_{k_1}^{-1}(z_1') \\ S_{k_2}^{-1}(z_2') \end{pmatrix} \right\rangle}_{\langle \zeta, G \begin{pmatrix} z_1' \\ z_2' \end{pmatrix} \rangle \oplus c} \oplus \underbrace{\left\langle \gamma, \begin{pmatrix} S_{k_1}^{-1}(z_1') \\ S_{k_2}^{-1}(0) \end{pmatrix} \right\rangle}_{\langle \zeta, G \begin{pmatrix} z_1' \\ 0 \end{pmatrix} \rangle \oplus c} = \underbrace{\left\langle \gamma, \begin{pmatrix} S_{k_1}^{-1}(0) \\ S_{k_2}^{-1}(z_2') \end{pmatrix} \right\rangle}_{\langle \zeta, G \begin{pmatrix} 0 \\ z_2' \end{pmatrix} \rangle \oplus c} \oplus \underbrace{\left\langle \gamma, \begin{pmatrix} S_{k_1}^{-1}(0) \\ S_{k_2}^{-1}(0) \end{pmatrix} \right\rangle}_{\langle \zeta, G \begin{pmatrix} 0 \\ 0 \end{pmatrix} \rangle \oplus c}$$

$$\Longrightarrow \quad \left\langle \zeta, G \begin{pmatrix} z_1' \\ z_2' \end{pmatrix} \oplus G \begin{pmatrix} z_1' \\ 0 \end{pmatrix} \oplus G \begin{pmatrix} 0 \\ z_2' \end{pmatrix} \oplus G \begin{pmatrix} 0 \\ 0 \end{pmatrix} \right\rangle = 0$$

Existence of Perfect Linear Approximations over Two-Round SPNs

CASA
Cyber Security in the Age of Large-Scale Adversaries



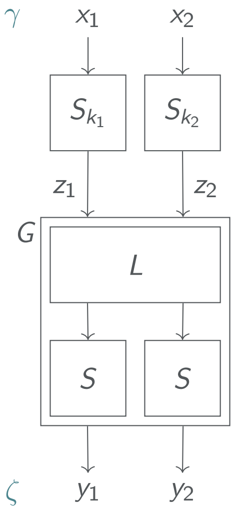
$$\left\langle \gamma, \begin{pmatrix} S_{k_1}^{-1}(z_1) \\ S_{k_2}^{-1}(z_2) \end{pmatrix} \right\rangle = \left\langle \gamma, \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \right\rangle = \left\langle \zeta, \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \right\rangle \oplus c = \left\langle \zeta, G \begin{pmatrix} z_1 \\ z_2 \end{pmatrix} \right\rangle \oplus c$$

$$\underbrace{\left\langle \gamma, \begin{pmatrix} S_{k_1}^{-1}(z_1') \\ S_{k_2}^{-1}(z_2') \end{pmatrix} \right\rangle}_{\left\langle \zeta, G \begin{pmatrix} z_1' \\ z_2' \end{pmatrix} \right\rangle \oplus c} \oplus \underbrace{\left\langle \gamma, \begin{pmatrix} S_{k_1}^{-1}(z_1') \\ S_{k_2}^{-1}(0) \end{pmatrix} \right\rangle}_{\left\langle \zeta, G \begin{pmatrix} z_1' \\ 0 \end{pmatrix} \right\rangle \oplus c} = \underbrace{\left\langle \gamma, \begin{pmatrix} S_{k_1}^{-1}(0) \\ S_{k_2}^{-1}(z_2') \end{pmatrix} \right\rangle}_{\left\langle \zeta, G \begin{pmatrix} 0 \\ z_2' \end{pmatrix} \right\rangle \oplus c} \oplus \underbrace{\left\langle \gamma, \begin{pmatrix} S_{k_1}^{-1}(0) \\ S_{k_2}^{-1}(0) \end{pmatrix} \right\rangle}_{\left\langle \zeta, G \begin{pmatrix} 0 \\ 0 \end{pmatrix} \right\rangle \oplus c}$$

$$\Longrightarrow \quad \left\langle \zeta, G \begin{pmatrix} z_1' \\ z_2' \end{pmatrix} \oplus G \begin{pmatrix} z_1' \\ 0 \end{pmatrix} \oplus G \begin{pmatrix} 0 \\ z_2' \end{pmatrix} \oplus G \begin{pmatrix} 0 \\ 0 \end{pmatrix} \right\rangle = 0$$

For every z': linear equation in ζ

Existence of Perfect Linear Approximations over Two-Round SPNs



$$\langle \gamma, \begin{pmatrix} S_{k_1}^{-1}(z_1) \\ S_{k_2}^{-1}(z_2) \end{pmatrix} \rangle = \langle \gamma, \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \rangle = \langle \zeta, \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \rangle \oplus c = \langle \zeta, G \begin{pmatrix} z_1 \\ z_2 \end{pmatrix} \rangle \oplus c$$

$$\underbrace{\langle \gamma, \begin{pmatrix} S_{k_1}^{-1}(z_1') \\ S_{k_2}^{-1}(z_2') \end{pmatrix} \rangle}_{\langle \zeta, G \begin{pmatrix} z_1' \\ z_2' \end{pmatrix} \rangle \oplus c} \oplus \underbrace{\langle \gamma, \begin{pmatrix} S_{k_1}^{-1}(z_1') \\ S_{k_2}^{-1}(0) \end{pmatrix} \rangle}_{\langle \zeta, G \begin{pmatrix} z_1' \\ 0 \end{pmatrix} \rangle \oplus c} = \underbrace{\langle \gamma, \begin{pmatrix} S_{k_1}^{-1}(0) \\ S_{k_2}^{-1}(z_2') \end{pmatrix} \rangle}_{\langle \zeta, G \begin{pmatrix} 0 \\ z_2' \end{pmatrix} \rangle \oplus c} \oplus \underbrace{\langle \gamma, \begin{pmatrix} S_{k_1}^{-1}(0) \\ S_{k_2}^{-1}(0) \end{pmatrix} \rangle}_{\langle \zeta, G \begin{pmatrix} 0 \\ 0 \end{pmatrix} \rangle \oplus c}$$

$$\Longrightarrow \quad \langle \zeta, G \begin{pmatrix} z_1' \\ z_2' \end{pmatrix} \oplus G \begin{pmatrix} z_1' \\ 0 \end{pmatrix} \oplus G \begin{pmatrix} 0 \\ z_2' \end{pmatrix} \oplus G \begin{pmatrix} 0 \\ 0 \end{pmatrix} \rangle = 0$$

For every z': linear equation in ζ independent of key!

Existence of Perfect Linear Approximations over Two-Round SPNs

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

Cipher	Linear
	$r = 2$
Boomslang	
CRAFT	
MANTIS	
Midori64	
SKINNY-64	
SKINNY-128	
AES	✓
GIFT-64/128	✓
LED	✓
PRESENT	✓
PRINCE	✓
Streebog	✓
Ascon	✓
iSCREAM	✓
Keccak-100	✓
Kuznechik	✓
PRIDE	✓
RECTANGLE	✓

✓	Non-existence
✗	Existence
$\perp$	Abort
–	Not tested

Existence of Perfect Linear Approximations over Two-Round SPNs

Cipher	Linear $r = 2$
Boomslang	✗
CRAFT	
MANTIS	
Midori64	
SKINNY-64	
SKINNY-128	
AES	✓
GIFT-64/128	✓
LED	✓
PRESENT	✓
PRINCE	✓
Streebog	✓
Ascon	✓
iSCREAM	✓
Keccak-100	✓
Kuznechik	✓
PRIDE	✓
RECTANGLE	✓

✓	Non-existence
✗	Existence
$\perp$	Abort
–	Not tested

Existence of Perfect Linear Approximations over Two-Round SPNs

Cipher	Linear
	$r = 2$
Boomslang	✗
CRAFT	✗
MANTIS	
Midori64	
SKINNY-64	
SKINNY-128	
AES	✓
GIFT-64/128	✓
LED	✓
PRESENT	✓
PRINCE	✓
Streebog	✓
Ascon	✓
iSCREAM	✓
Keccak-100	✓
Kuznechik	✓
PRIDE	✓
RECTANGLE	✓

✓ Non-existence
✗ Existence
$\perp$ Abort
– Not tested

Existence of Perfect Linear Approximations over Two-Round SPNs

Cipher	Linear $r = 2$
Boomslang	✗
CRAFT	✗
MANTIS	✗
Midori64	✗
SKINNY-64	
SKINNY-128	
AES	✓
GIFT-64/128	✓
LED	✓
PRESENT	✓
PRINCE	✓
Streebog	✓
Ascon	✓
iSCREAM	✓
Keccak-100	✓
Kuznechik	✓
PRIDE	✓
RECTANGLE	✓

✓ Non-existence
✗ Existence
$\perp$ Abort
– Not tested

Existence of Perfect Linear Approximations over Two-Round SPNs

Cipher	Linear
	$r = 2$
Boomslang	✗
CRAFT	✗
MANTIS	✗
Midori64	✗
SKINNY-64	✗
SKINNY-128	✗
AES	✓
GIFT-64/128	✓
LED	✓
PRESENT	✓
PRINCE	✓
Streebog	✓
Ascon	✓
iSCREAM	✓
Keccak-100	✓
Kuznechik	✓
PRIDE	✓
RECTANGLE	✓

✓ Non-existence
✗ Existence
$\perp$ Abort
– Not tested

Existence of Perfect Linear Approximations over Two-Round SPNs

CASA
Cyber Security in the Age of Large-Scale Adversaries

Cipher	Linear $r = 2$	Linear $r = 3$
Boomslang	✗	✓
CRAFT	✗	✓
MANTIS	✗	✓
Midori64	✗	✓
SKINNY-64	✗	✓
SKINNY-128	✗	$\perp$
AES	✓	✓
GIFT-64/128	✓	✓
LED	✓	✓
PRESENT	✓	✓
PRINCE	✓	✓
Streebog	✓	✓
Ascon	✓	✓
iSCREAM	✓	$\perp$
Keccak-100	✓	✓
Kuznechik	✓	$\perp$
PRIDE	✓	✓
RECTANGLE	✓	✓

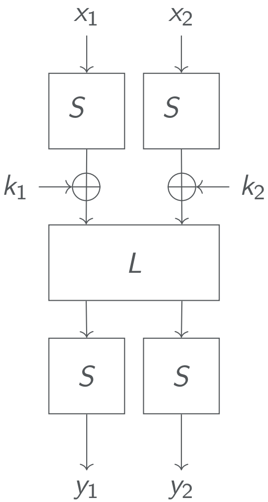
✓ Non-existence
✗ Existence
$\perp$ Abort
– Not tested

Existence of Perfect Linear Approximations over Two-Round SPNs

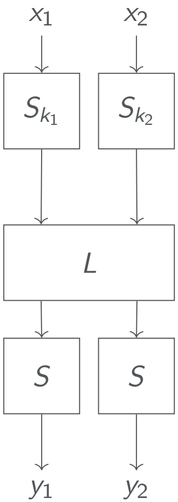
Cipher	Linear		
	$r = 2$	$r = 3$	$r = 4$
Boomslang	✗	✓	✗
CRAFT	✗	✓	✓
MANTIS	✗	✓	✗
Midori64	✗	✓	✗
SKINNY-64	✗	✓	✓
SKINNY-128	✗	$\perp$	$\perp$
AES	✓	✓	$\perp$
GIFT-64/128	✓	✓	✓
LED	✓	✓	✓
PRESENT	✓	✓	✓
PRINCE	✓	✓	✓
Streebog	✓	✓	$\perp$
Ascon	✓	✓	–
iSCREAM	✓	$\perp$	–
Keccak-100	✓	✓	–
Kuznechik	✓	$\perp$	–
PRIDE	✓	✓	–
RECTANGLE	✓	✓	–

✓ Non-existence
✗ Existence
$\perp$ Abort
– Not tested

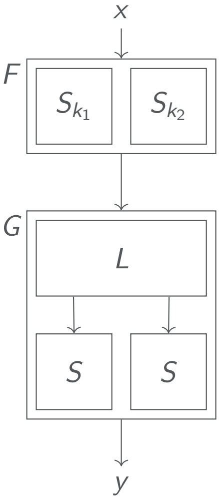
Existence of Perfect Differentials over Two-Round SPNs



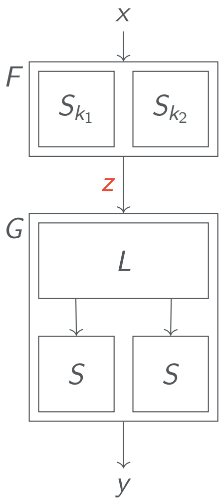
Existence of Perfect Differentials over Two-Round SPNs



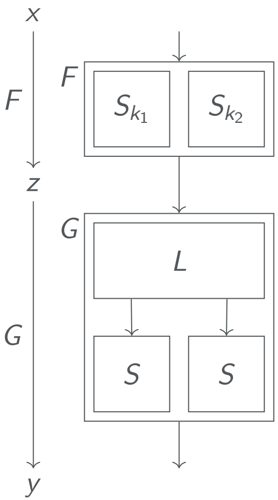
Existence of Perfect Differentials over Two-Round SPNs



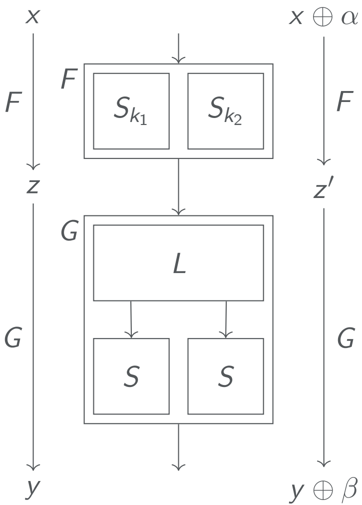
Existence of Perfect Differentials over Two-Round SPNs



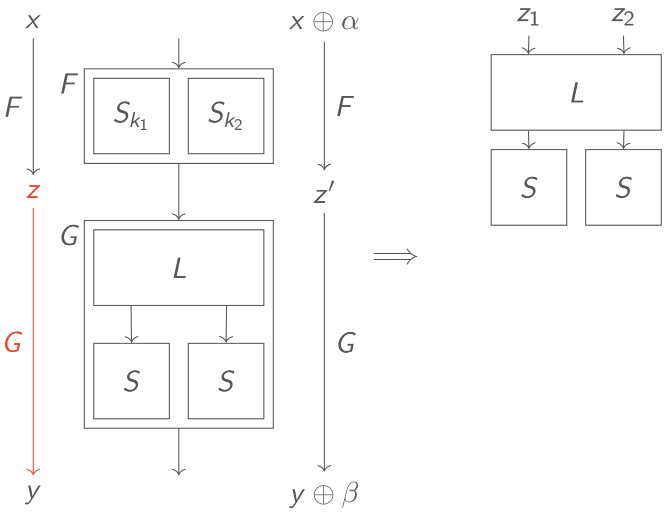
Existence of Perfect Differentials over Two-Round SPNs



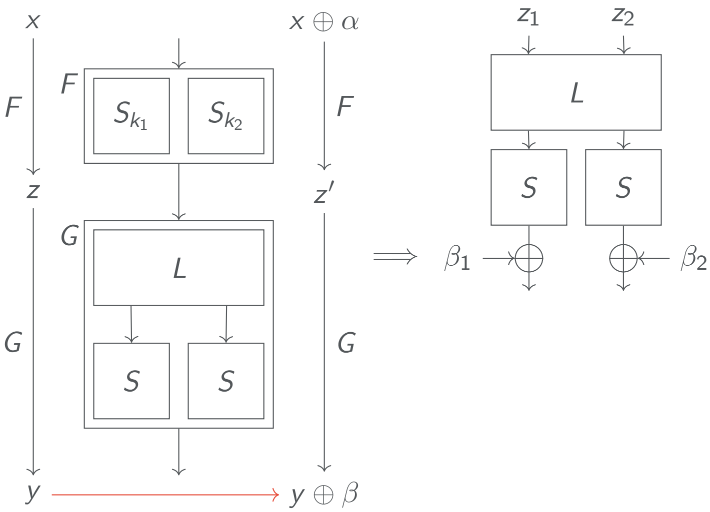
Existence of Perfect Differentials over Two-Round SPNs



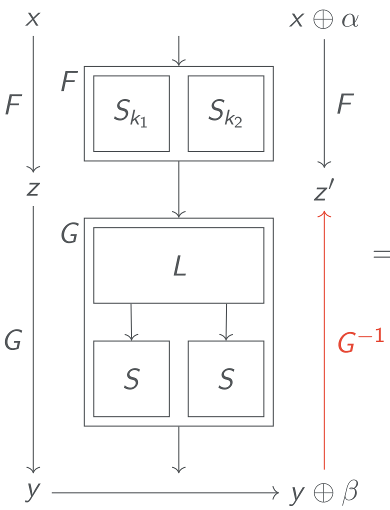
Existence of Perfect Differentials over Two-Round SPNs



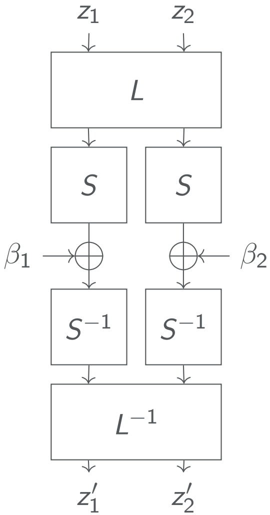
Existence of Perfect Differentials over Two-Round SPNs



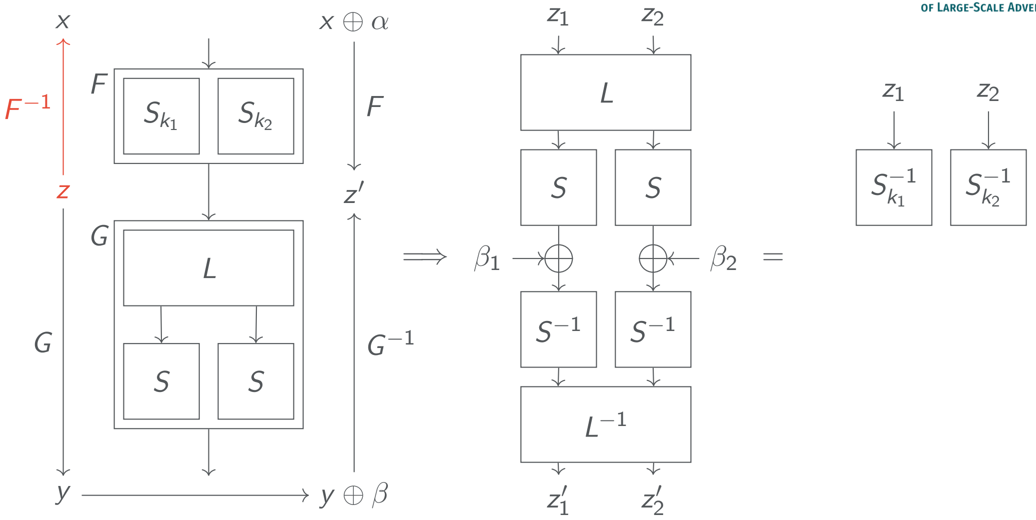
Existence of Perfect Differentials over Two-Round SPNs



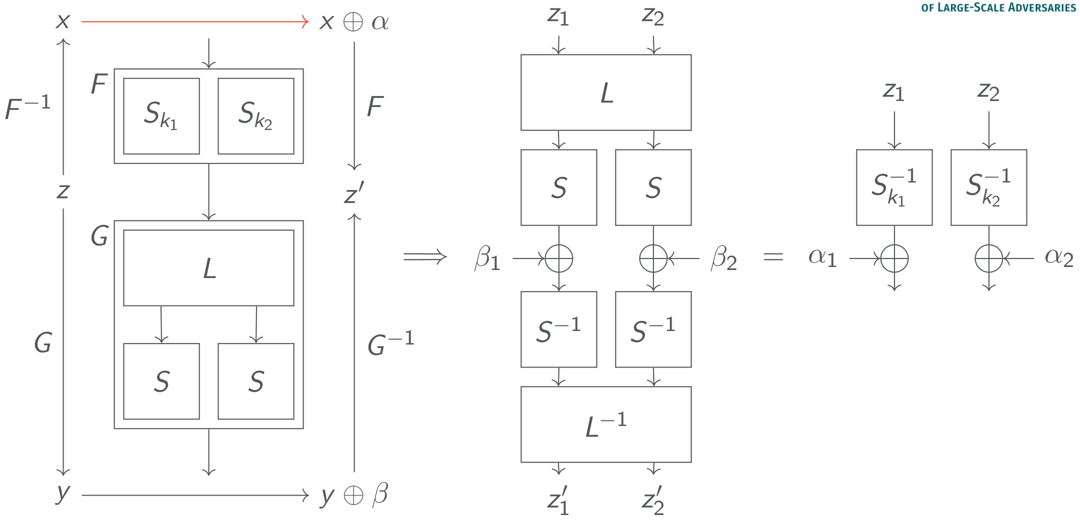
$\Longrightarrow$



Existence of Perfect Differentials over Two-Round SPNs

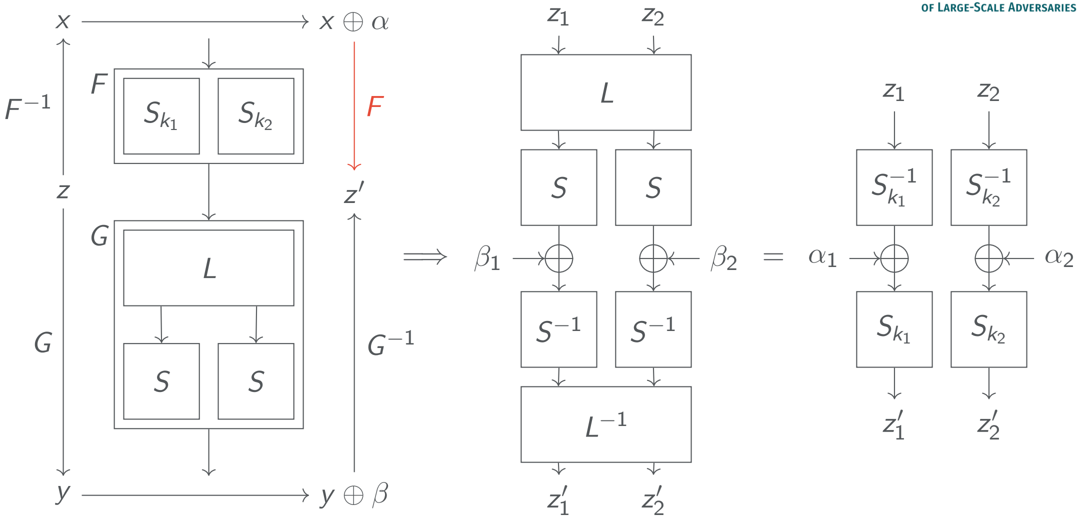


Existence of Perfect Differentials over Two-Round SPNs

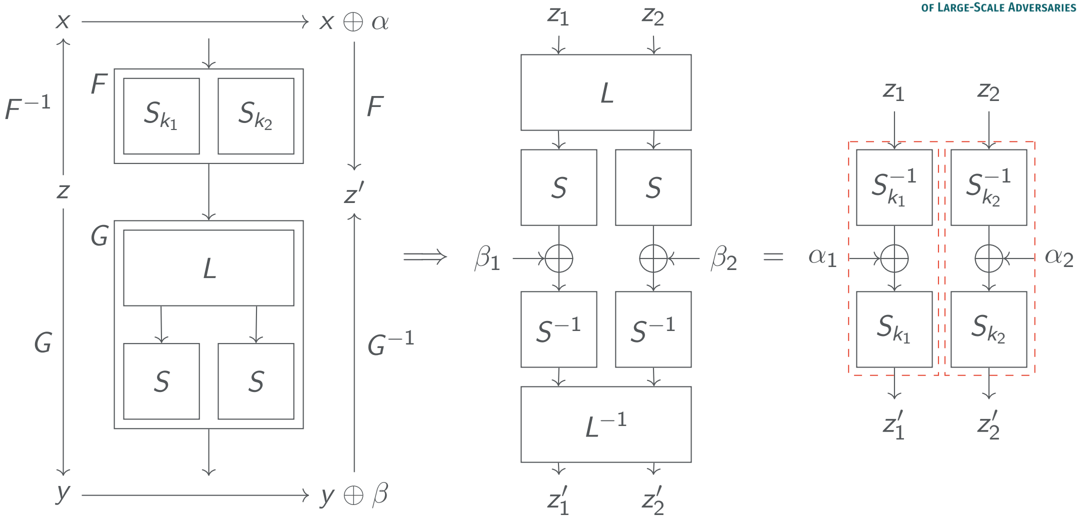


Existence of Perfect Differentials over Two-Round SPNs

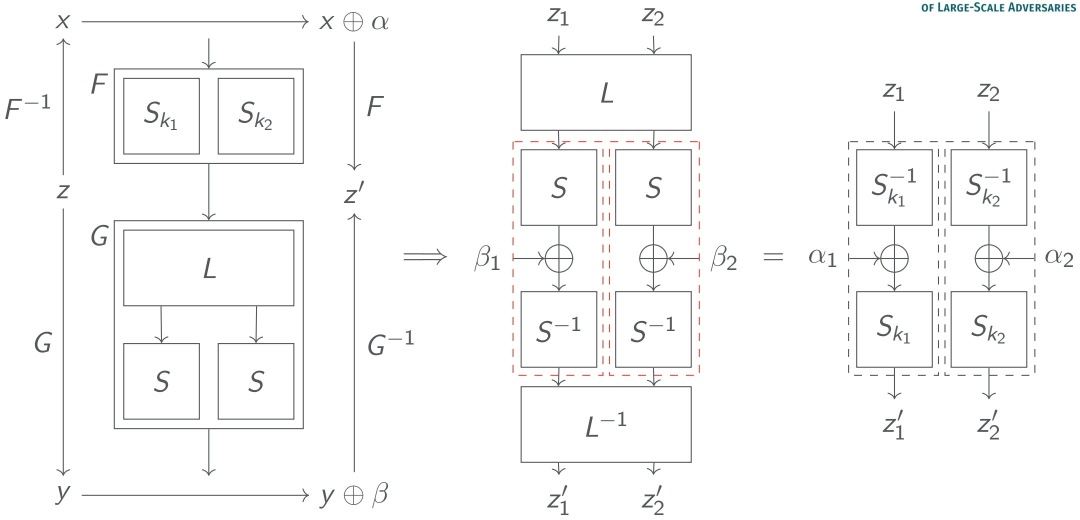
CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES



Existence of Perfect Differentials over Two-Round SPNs



Existence of Perfect Differentials over Two-Round SPNs



Existence of Perfect Differentials over Two-Round SPNs

Theorem 1 ([Lambin, Leander and N., EC'23], informal)

If an SPN-round-function has two essentially different decompositions then there exist a perfect linear approximation and a perfect differential over (at least) one of its s-boxes.

Existence of Perfect Differentials over Two-Round SPNs

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

Theorem 1 ([Lambin, Leander and N., EC'23], informal)

If an SPN-round-function has two essentially different decompositions then there exist a perfect linear approximation and a perfect differential over (at least) one of its s-boxes.

- Here: $\hat{S}\colon x \mapsto S^{-1}(S(x) \oplus \beta_i)$ are the s-boxes

Existence of Perfect Differentials over Two-Round SPNs

CASA
Cyber Security in the Age of Large-Scale Adversaries

Theorem 1 ([Lambin, Leander and N., EC'23], informal)

If an SPN-round-function has two essentially different decompositions then there exist a perfect linear approximation and a perfect differential over (at least) one of its s-boxes.

- Here: $\hat{S} : x \mapsto S^{-1}(S(x) \oplus \beta_i)$ are the s-boxes
- Perfect differential over $\hat{S}$ would imply

$$\exists \delta \neq 0, \delta' : \qquad S^{-1}(S(x) \oplus \beta_i) \oplus S^{-1}(S(x \oplus \delta) \oplus \beta_i) \qquad = \delta' \qquad \forall x$$

Existence of Perfect Differentials over Two-Round SPNs

CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

Theorem 1 ([Lambin, Leander and N., EC'23], informal)

If an SPN-round-function has two essentially different decompositions then there exist a perfect linear approximation and a perfect differential over (at least) one of its s-boxes.

- Here: $\hat{S}\colon x \mapsto S^{-1}(S(x) \oplus \beta_i)$ are the s-boxes
- Perfect differential over $\hat{S}$ would imply

$$\begin{aligned} \exists \delta \neq 0, \delta' : \quad & S^{-1}(S(x) \oplus \beta_i) \oplus S^{-1}(S(x \oplus \delta) \oplus \beta_i) &= \delta' \quad & \forall x \\ \Longrightarrow \quad & S^{-1}(S(x) \oplus \beta_i) \oplus S^{-1}(S(x \oplus \delta') \oplus \beta_i) &= \delta \quad & \forall x \end{aligned}$$

Existence of Perfect Differentials over Two-Round SPNs

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

Theorem 1 ([Lambin, Leander and N., EC'23], informal)

If an SPN-round-function has two essentially different decompositions then there exist a perfect linear approximation and a perfect differential over (at least) one of its s-boxes.

- Here: $\hat{S}\colon x \mapsto S^{-1}(S(x) \oplus \beta_i)$ are the s-boxes
- Perfect differential over $\hat{S}$ would imply

$$
\begin{aligned}
\exists \delta \neq 0, \delta' : \quad & S^{-1}(S(x) \oplus \beta_i) \oplus S^{-1}(S(x \oplus \delta) \oplus \beta_i) &&= \delta' && \forall x \\
\Longrightarrow \quad & S^{-1}(S(x) \oplus \beta_i) \oplus S^{-1}(S(x \oplus \delta') \oplus \beta_i) &&= \delta && \forall x \\
\Longrightarrow \quad & S^{-1}(S(x) \oplus \beta_i) \oplus S^{-1}(S(x \oplus \delta \oplus \delta') \oplus \beta_i) &&= \delta \oplus \delta' && \forall x
\end{aligned}
$$

Existence of Perfect Differentials over Two-Round SPNs

CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

Theorem 1 ([Lambin, Leander and N., EC'23], informal)

If an SPN-round-function has two essentially different decompositions then there exist a perfect linear approximation and a perfect differential over (at least) one of its s-boxes.

- Here: $\hat{S} \colon x \mapsto S^{-1}(S(x) \oplus \beta_i)$ are the s-boxes
- Perfect differential over $\hat{S}$ would imply

$$\begin{aligned}
\exists \delta \neq 0, \delta' : \quad & S^{-1}(S(x) \oplus \beta_i) \oplus S^{-1}(S(x \oplus \delta) \oplus \beta_i) &&= \delta' && \forall x \\
\Longrightarrow \quad & S^{-1}(S(x) \oplus \beta_i) \oplus S^{-1}(S(x \oplus \delta') \oplus \beta_i) &&= \delta && \forall x \\
\Longrightarrow \quad & S^{-1}(S(x) \oplus \beta_i) \oplus S^{-1}(S(x \oplus \delta \oplus \delta') \oplus \beta_i) &&= \delta \oplus \delta' && \forall x
\end{aligned}$$

- I.e. S would have maximal boomerang uniformity [Boura and Canteaut, ToSC'18]

Existence of Perfect Differentials over Two-Round SPNs

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

Theorem 1 ([Lambin, Leander and N., EC'23], informal)

If an SPN-round-function has two essentially different decompositions then there exist a perfect linear approximation and a perfect differential over (at least) one of its s-boxes.

- Here: $\hat{S}: x \mapsto S^{-1}(S(x) \oplus \beta_i)$ are the s-boxes
- Perfect differential over $\hat{S}$ would imply

$$\begin{aligned}
\exists \delta \neq 0, \delta' : \quad & S^{-1}(S(x) \oplus \beta_i) \oplus S^{-1}(S(x \oplus \delta) \oplus \beta_i) && = \delta' && \forall x \\
\implies \quad & S^{-1}(S(x) \oplus \beta_i) \oplus S^{-1}(S(x \oplus \delta') \oplus \beta_i) && = \delta && \forall x \\
\implies \quad & S^{-1}(S(x) \oplus \beta_i) \oplus S^{-1}(S(x \oplus \delta \oplus \delta') \oplus \beta_i) && = \delta \oplus \delta' && \forall x
\end{aligned}$$

- I.e. S would have maximal boomerang uniformity [Boura and Canteaut, ToSC'18]

Existence of Perfect Differentials over Two-Round SPNs

- Use theory from [Lambin, Leander and N., EC'23]

Existence of Perfect Differentials over Two-Round SPNs

- Use theory from [Lambin, Leander and N., EC'23]
- Exemplary implication

Corollary 2

If L has differential branch number of at least 3 and if S does not have

1. *maximal boomerang uniformity, or*
2. *linear structures*

then there cannot exist any perfect differential over two rounds.

Existence of Perfect Linear Approximations and Differentials over Two-Round SPNs

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

Cipher	Linear $r=2$	Linear $r=3$	Linear $r=4$	Differential $r=2$
Boomslang	✗	✓	✗	✓
CRAFT	✗	✓	✓	✓
MANTIS	✗	✓	✗	✓
Midori64	✗	✓	✗	✓
SKINNY-64	✗	✓	✓	✓
SKINNY-128	✗	$\perp$	$\perp$	✓
AES	✓	✓	$\perp$	✓
GIFT-64/128	✓	✓	✓	✓
LED	✓	✓	✓	✓
PRESENT	✓	✓	✓	✓
PRINCE	✓	✓	✓	✓
Streebog	✓	✓	$\perp$	✓
Ascon	✓	✓	–	✓
iSCREAM	✓	$\perp$	–	✓
Keccak-100	✓	✓	–	✓
Kuznechik	✓	$\perp$	–	✓
PRIDE	✓	✓	–	✓
RECTANGLE	✓	✓	–	✓

✓ Non-existence
✗ Existence
$\perp$ Abort
– Not tested

Existence of Perfect Linear Approximations and Differentials over Two-Round SPNs

CASA
Cyber Security in the Age of Large-Scale Adversaries

Cipher	Linear $r=2$	Linear $r=3$	Linear $r=4$	Differential $r=2$
Boomslang	✗	✓	✗	✓
CRAFT	✗	✓	✓	✓
MANTIS	✗	✓	✗	✓
Midori64	✗	✓	✗	✓
SKINNY-64	✗	✓	✓	✓
SKINNY-128	✗	⊥	⊥	✓
AES	✓	✓	⊥	✓
GIFT-64/128	✓	✓	✓	✓
LED	✓	✓	✓	✓
PRESENT	✓	✓	✓	✓
PRINCE	✓	✓	✓	✓
Streebog	✓	✓	⊥	✓
Ascon	✓	✓	–	✓
iSCREAM	✓	⊥	–	✓
Keccak-100	✓	✓	–	✓
Kuznechik	✓	⊥	–	✓
PRIDE	✓	✓	–	✓
RECTANGLE	✓	✓	–	✓

✓ Non-existence
✗ Existence
⊥ Abort
– Not tested

Thank you for your attention!