Improved Cryptanalysis of GIFT-64

Patrick Derbez[1], Baptiste Germon[1], Bastien Michel[2], María Naya-Plasencia[2]

[1]Univ Rennes, Inria, CNRS, IRISA, France
[2]Inria, Paris

March 27, 2026

Overview

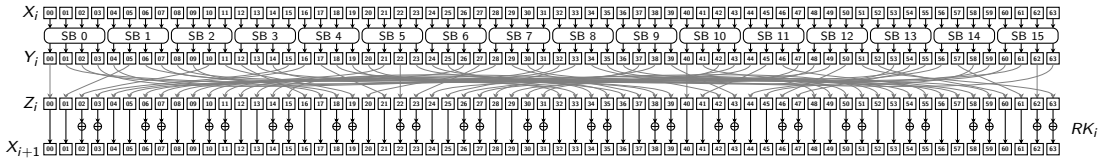
GIFT

Improving differential attacks with parallel matching

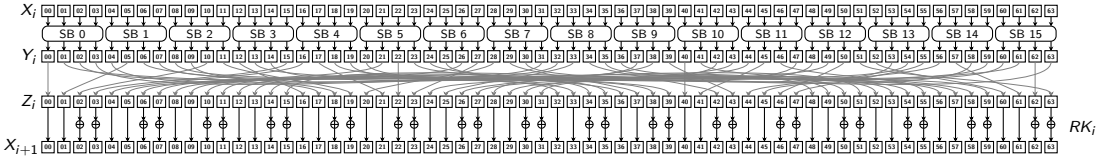
Differential meet-in-the-middle cryptanalysis

Conclusive results

The block cipher GIFT [BPP+17]



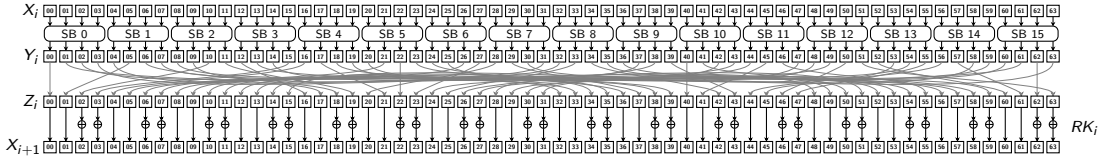
The block cipher GIFT [BPP+17]



$$MK = k_7||k_6||k_5||k_4||k_3||k_2||k_1||k_0$$

$$k_7||k_6||\dots||\underbrace{\boxed{k_1||k_0}}_{RK_i} \longleftarrow k_1 \ggg 2||k_0 \ggg 12||\dots||k_3||k_2$$

The block cipher GIFT [BPP+17]

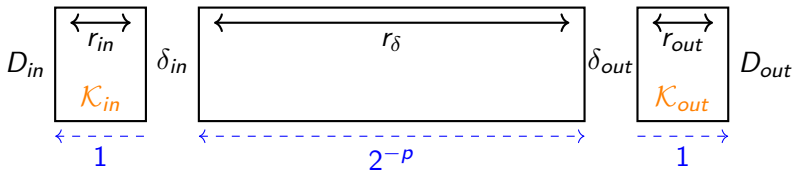


$$MK = k_7||k_6||k_5||k_4||k_3||k_2||k_1||k_0$$

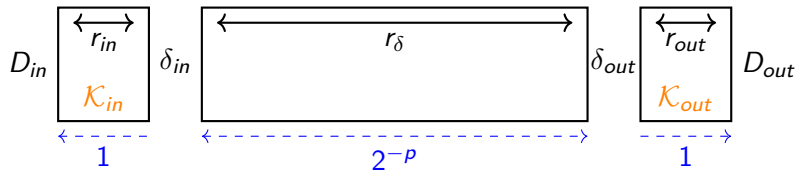
$$k_7||k_6||\dots||\underbrace{k_1||k_0}_{RK_i} \longleftarrow k_1 \ggg 2||k_0 \ggg 12||\dots||k_3||k_2$$

Cipher	Rounds	Setup	Key space size	Time	Data	Memory	Type of Attack	Source
GIFT-64	21	SK	2^{124}	$2^{117.42}$	2^{64}	2^{96}	Differential	[CWWH25]
	26	RK	2^{120}	$2^{120.44}$	$2^{60.96}$	$2^{25.22}$	Differential	[CN25]

A previous lower bound of differential attacks



A previous lower bound of differential attacks

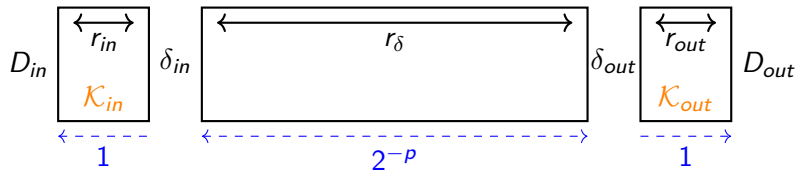


Acquiring data

$\mathcal{D}$

$\mathcal{T} = 2^{p+1} \cdot C_E$

A previous lower bound of differential attacks



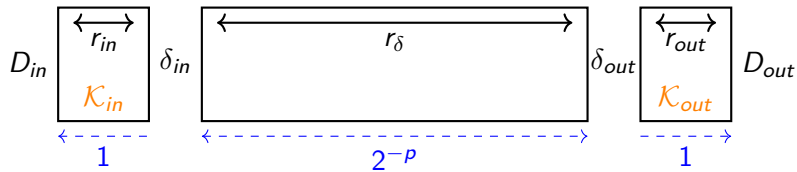
Acquiring data | Filtering and forming the pairs

$\mathcal{D} \longrightarrow \mathcal{N}$

Lin. equ.

$$\mathcal{T} = 2^{p+1} \cdot C_E + \quad 2^{p+d_{in}-n+d_{out}}$$

A previous lower bound of differential attacks

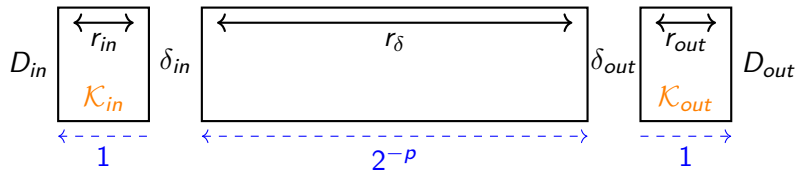


Acquiring data | Filtering and forming the pairs

$\mathcal{D}$ —Lin. equ.→ $\mathcal{N}$ —Non Lin. equ.→ $\mathcal{N}'$

$$\mathcal{T} = 2^{p+1} \cdot C_E + 2^{p+d_{in}-n+d_{out}} \cdot C_S$$

A previous lower bound of differential attacks

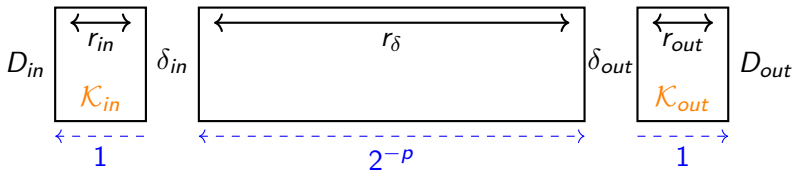


Acquiring data | Filtering and forming the pairs | Key recovery

$\mathcal{D} \xrightarrow{\text{Lin. equ.}} \mathcal{N} \xrightarrow{\text{Non Lin. equ.}} \mathcal{N}' \longrightarrow \mathcal{K}$

$$\mathcal{T} = 2^{p+1} \cdot C_E + 2^{p+d_{in}-n+d_{out}} \cdot C_S + N' \cdot C_{KR}$$

A previous lower bound of differential attacks

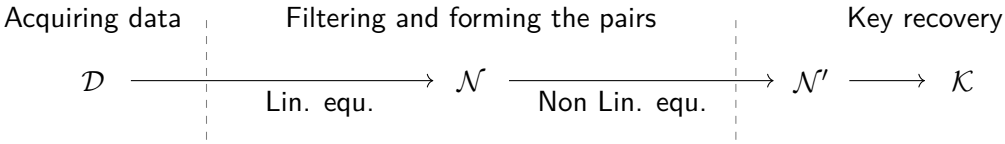


Acquiring data | Filtering and forming the pairs | Key recovery

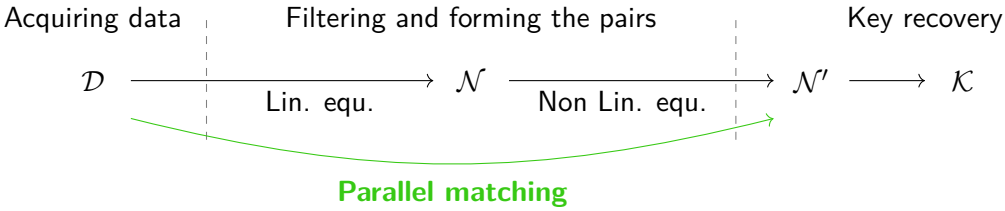
$\mathcal{D} \xrightarrow{\text{Lin. equ.}} \mathcal{N} \xrightarrow{\text{Non Lin. equ.}} \mathcal{N}' \longrightarrow \mathcal{K}$

$$\mathcal{T} = 2^{p+1} \cdot C_E + \underbrace{2^{p+d_{in}-n+d_{out}} \cdot C_S}_{\text{Lower bound}} + N' \cdot C_{KR}$$

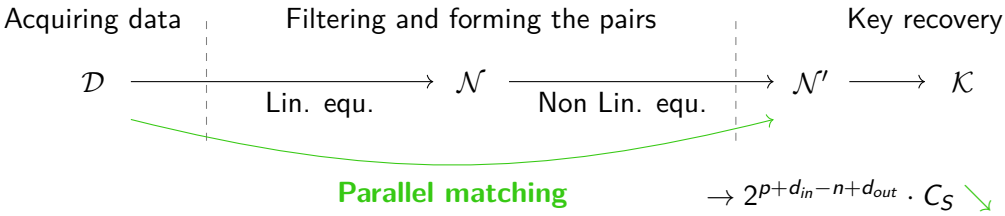
Improving the lower bound with parallel matching



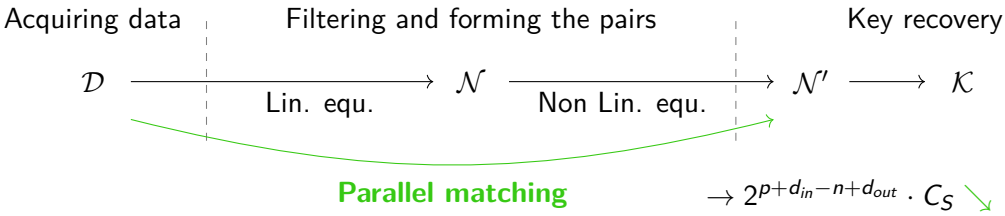
Improving the lower bound with parallel matching



Improving the lower bound with parallel matching

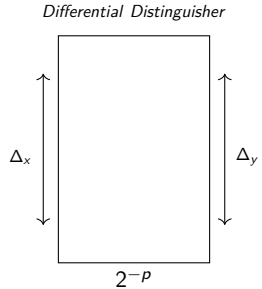


Improving the lower bound with parallel matching

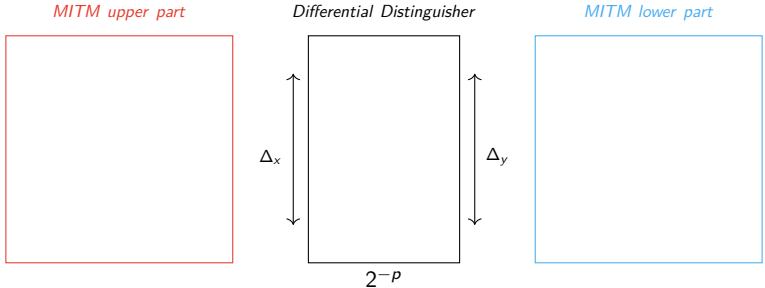


Cipher	Rounds	Setup	Key space size	Time	Data	Memory	Type of Attack	Source
	25	RK	2^{120}	2^{107}	2^{51}	2^{49}	Differential	[BDD+24]
GIFT-64	25	**RK**	$\mathbf{2^{120}}$	$\mathbf{2^{81.59}}$	$\mathbf{2^{51}}$	$\mathbf{2^{50.12}}$	**Differential**	**This Paper**
	26	RK	2^{120}	$2^{113.03}$	$2^{61.96}$	$2^{95.15}$	Differential	[CN25]

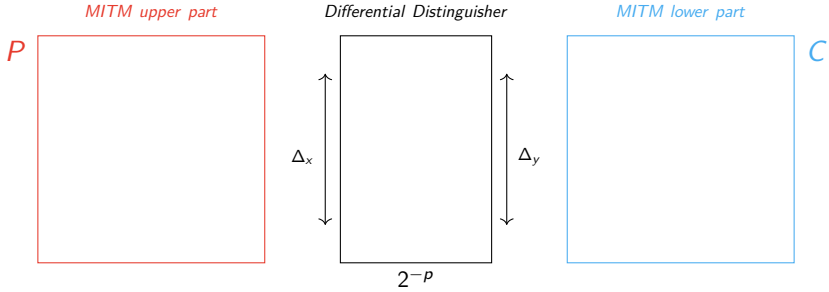
Differential Meet-in-the-middle Framework [BDD+23]



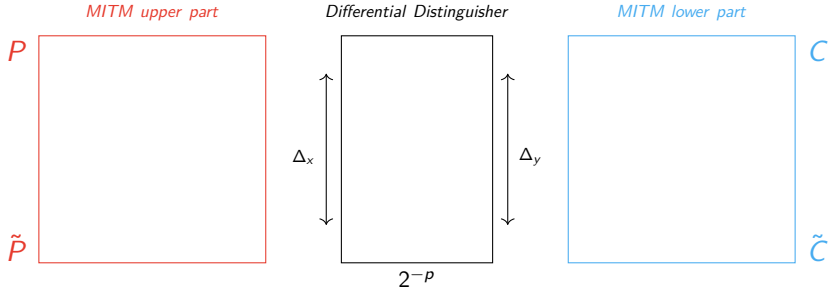
Differential Meet-in-the-middle Framework [BDD+23]



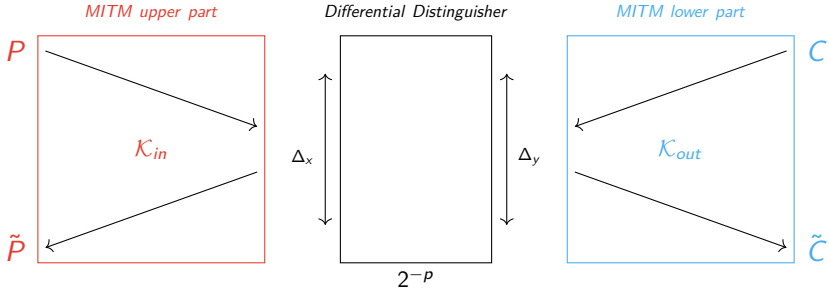
Differential Meet-in-the-middle Framework [BDD+23]



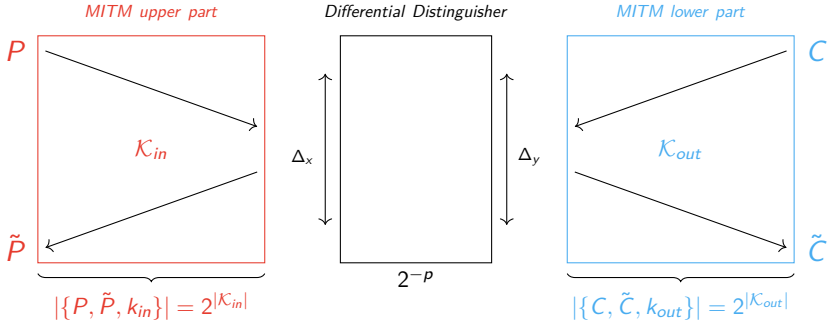
Differential Meet-in-the-middle Framework [BDD+23]



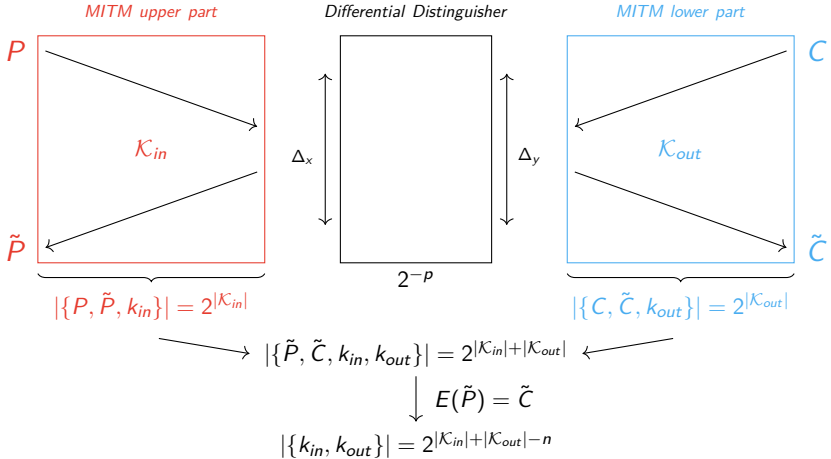
Differential Meet-in-the-middle Framework [BDD+23]



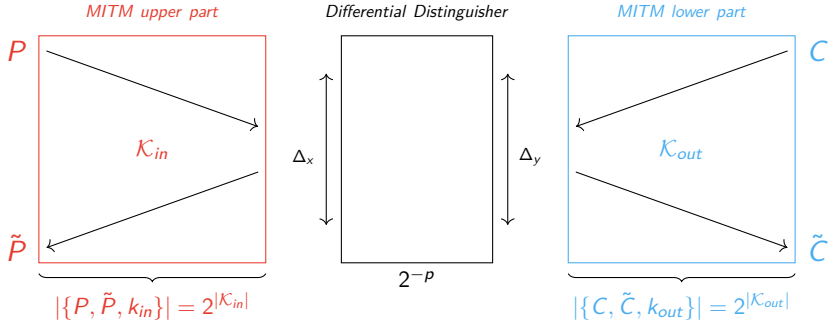
Differential Meet-in-the-middle Framework [BDD+23]



Differential Meet-in-the-middle Framework [BDD+23]



Differential Meet-in-the-middle Framework [BDD+23]



$\mathcal{T} = 2^p \left(2^{|\mathcal{K}_{in}|} + 2^{|\mathcal{K}_{out}|} + 2^{|\mathcal{K}_{in}|+|\mathcal{K}_{out}|-|\mathcal{K}_{in}\cap\mathcal{K}_{out}|-n}\right)$, $\mathcal{M} = 2^{min(|\mathcal{K}_{in}|,|\mathcal{K}_{out}|)}, \mathcal{D} = 2^{n-a}$ with $p + a < n - a$

A differential distinguisher of 13 rounds of GIFT 64 [CZD20], [CWWH25]

$$(0000\ 0000\ 0000\ 0202) \xrightarrow[13r]{2^{-57.82}} (0000\ 0005\ 0000\ 0005).$$

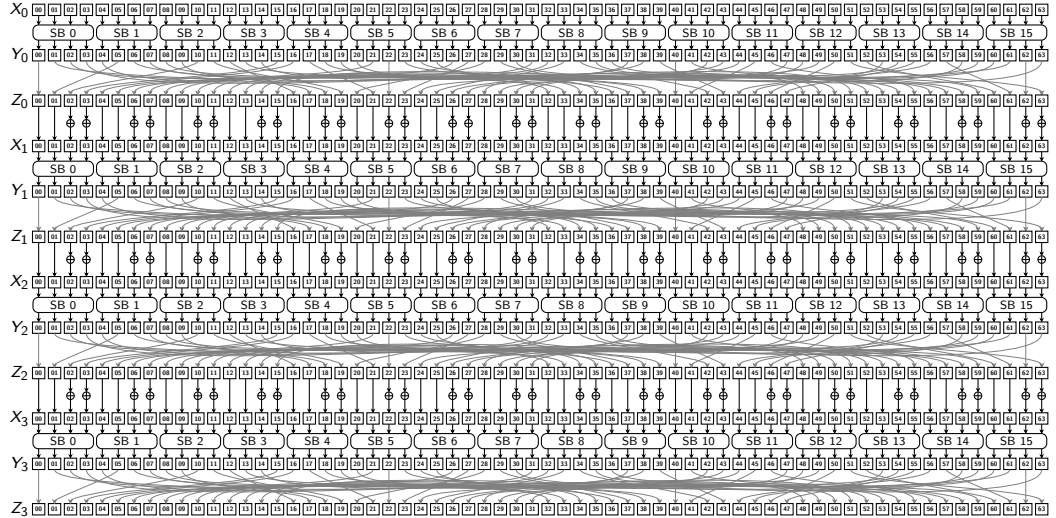
A differential distinguisher of 13 rounds of GIFT 64 [CZD20], [CWWH25]

$$(0000\ 0000\ 0000\ 0202) \xrightarrow[13r]{2^{-57.82}} (0000\ 0005\ 0000\ 0005).$$

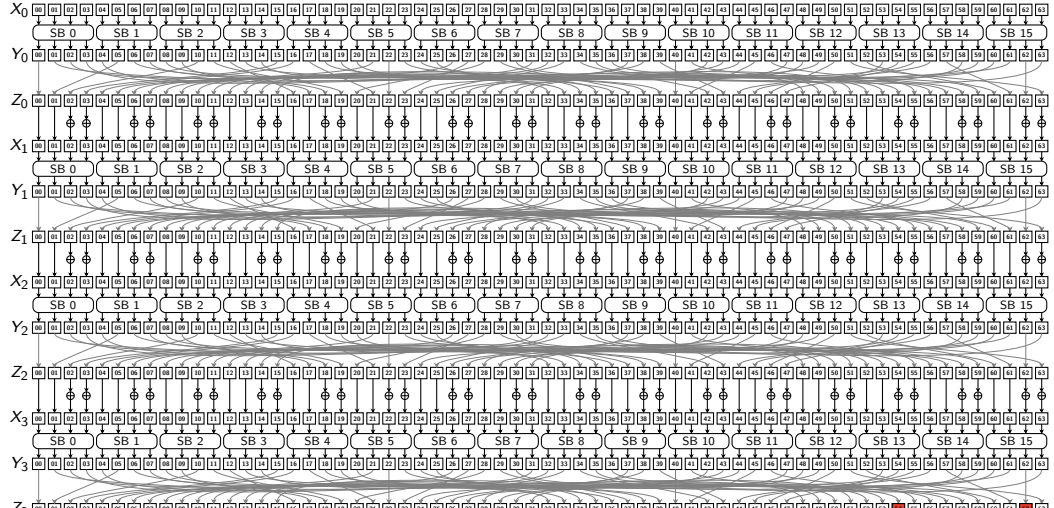
Weak key space : size 2^{124}

$$k_4[4] + k_4[12] = 0, k_4[0] + k_4[8] = 0,$$
$$k_0[5] + k_0[13] = 0, k_0[1] + k_0[9] = 0.$$

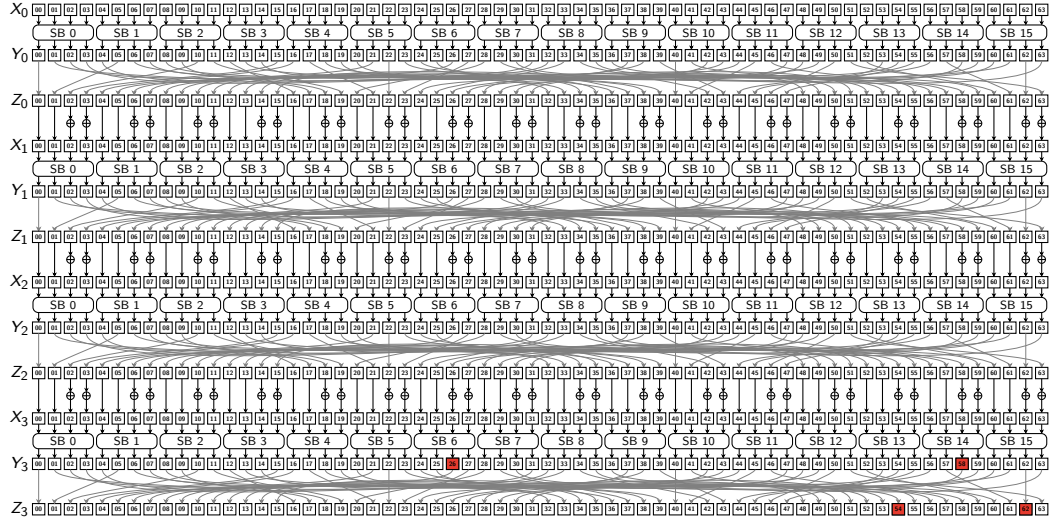
Upper extensions of the key recovery part



Upper extensions of the key recovery part

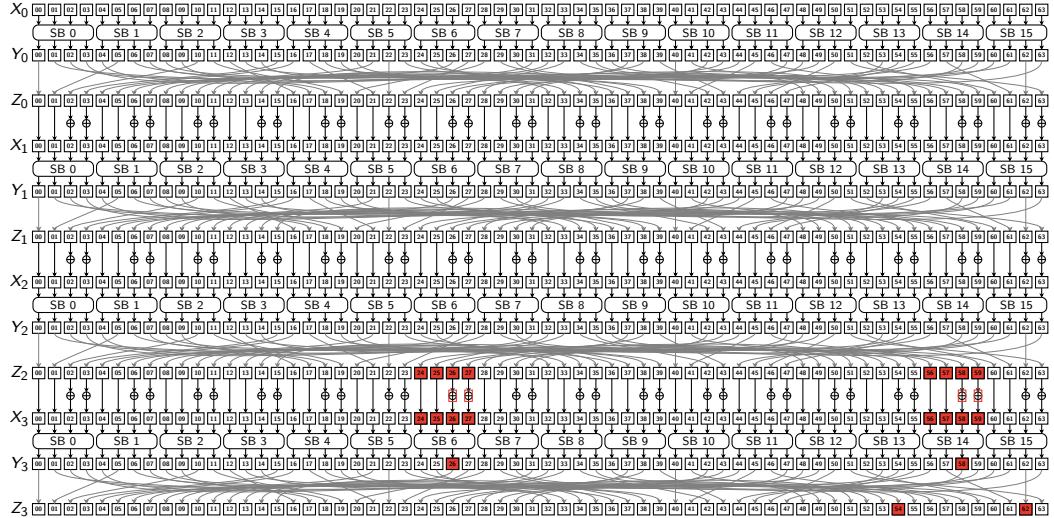


Upper extensions of the key recovery part

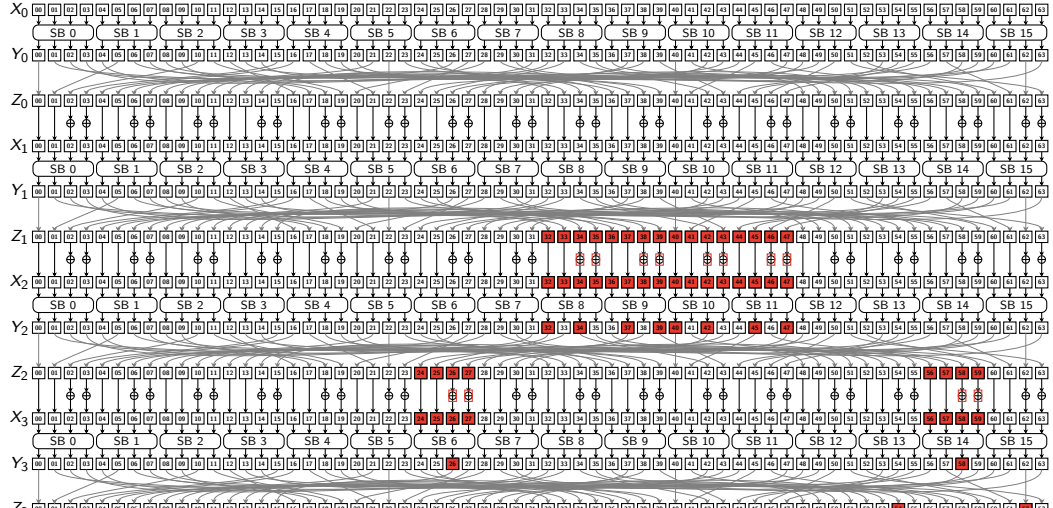


Upper extensions of the key recovery part

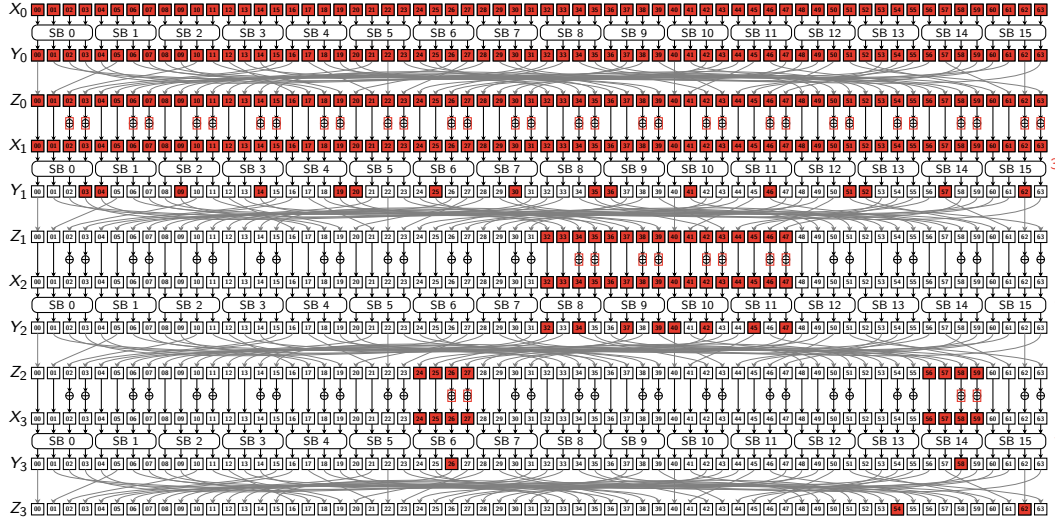
Upper extensions of the key recovery part



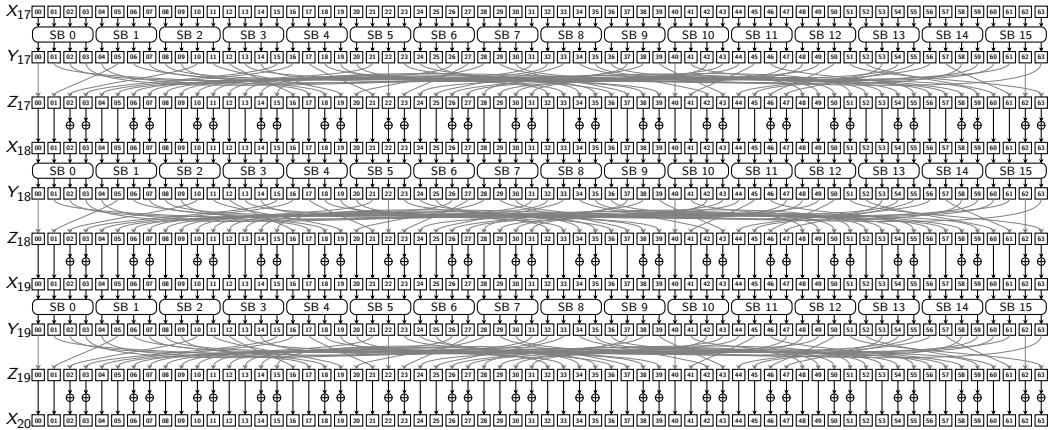
Upper extensions of the key recovery part



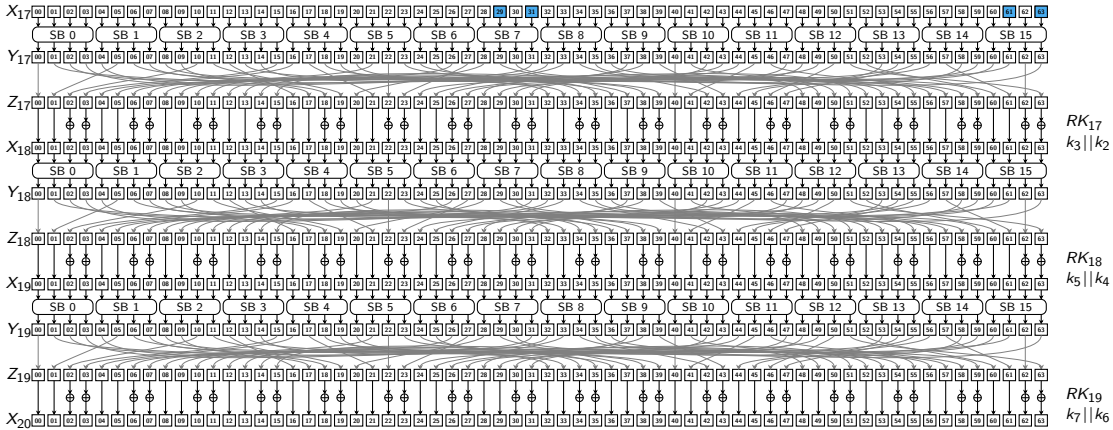
Upper extensions of the key recovery part



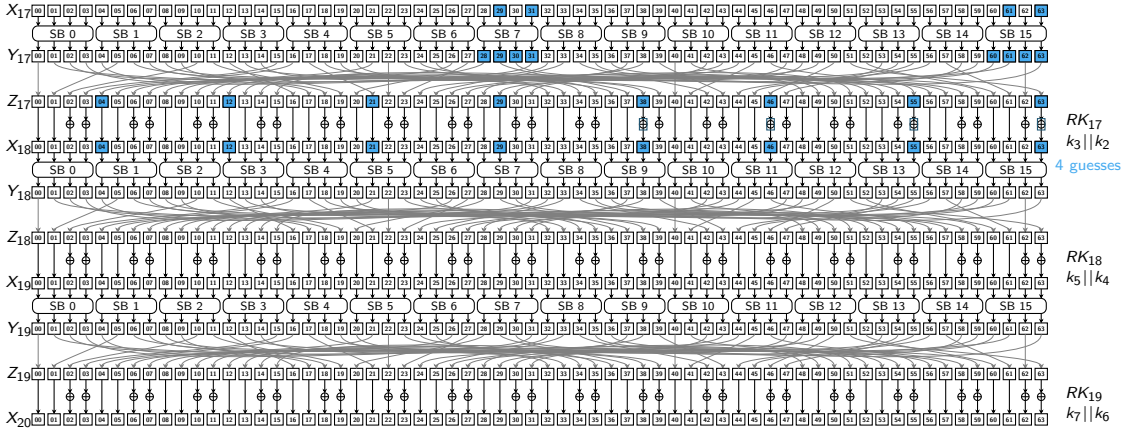
Lower extensions of the key recovery part



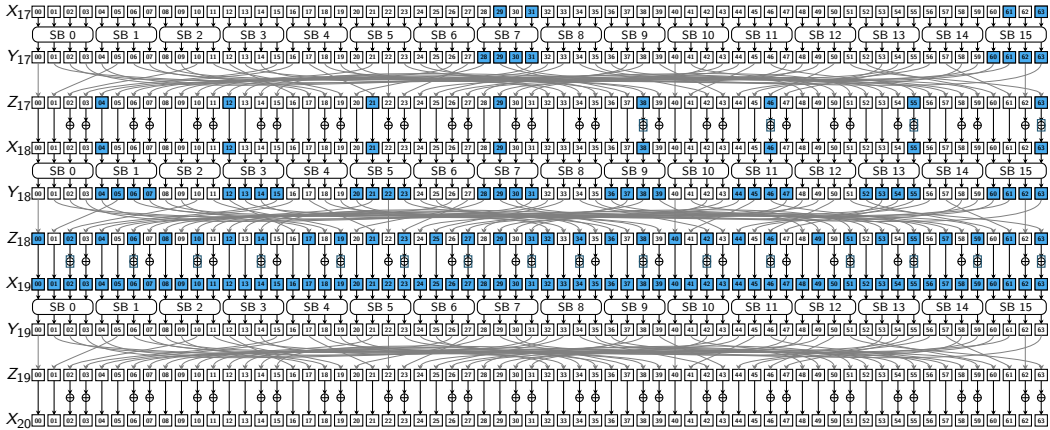
Lower extensions of the key recovery part



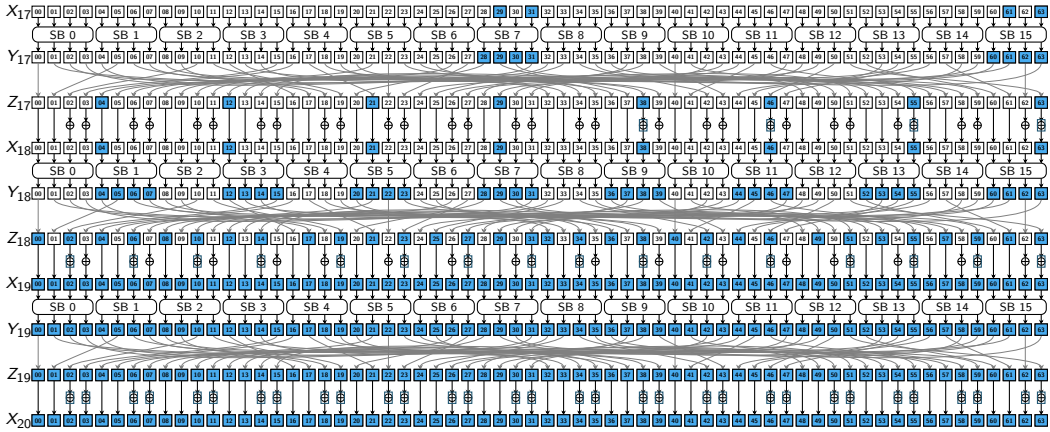
Lower extensions of the key recovery part



Lower extensions of the key recovery part



Lower extensions of the key recovery part



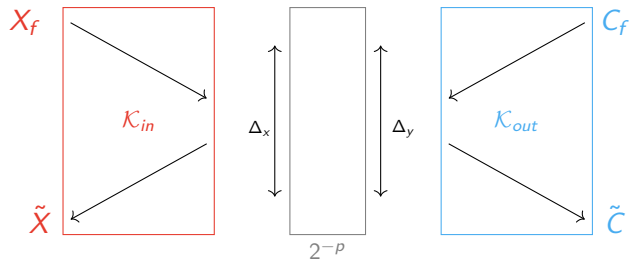
Complexities of Diff MITM attacks

- $\mathcal{R} = 4 + 13 + 3 = 20$.
- $|\mathcal{K}_{in}| = 44$, $|\mathcal{K}_{out}| = 52$, $|\mathcal{K}_{in} \cap \mathcal{K}_{out}| = 4$.

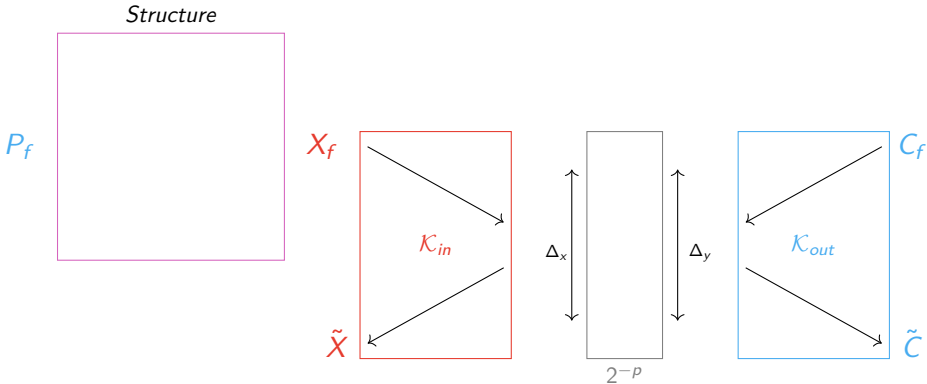
Complexities of Diff MITM attacks

- $\mathcal{R} = 4 + 13 + 3 = 20$.
- $|\mathcal{K}_{in}| = 44$, $|\mathcal{K}_{out}| = 52$, $|\mathcal{K}_{in} \cap \mathcal{K}_{out}| = 4$.
- $\mathcal{T} = 2^{p}(2^{|\mathcal{K}_{in}|} + 2^{|\mathcal{K}_{out}|} + 2^{|\mathcal{K}_{in}|+|\mathcal{K}_{out}|-n}) = 2^{57.82}(2^{44} + 2^{52} + 2^{44+52-64}) = 2^{109.82}$.
- $\mathcal{M} = 2^{min(|\mathcal{K}_{in}|-|\mathcal{K}_{in}\cap\mathcal{K}_{out}|,|\mathcal{K}_{out}|-|\mathcal{K}_{in}\cap\mathcal{K}_{out}|)} = 2^{40}$.
- $\mathcal{D} = 2^{n-a} = 2^{61}, a = 3, p = 57.82$.

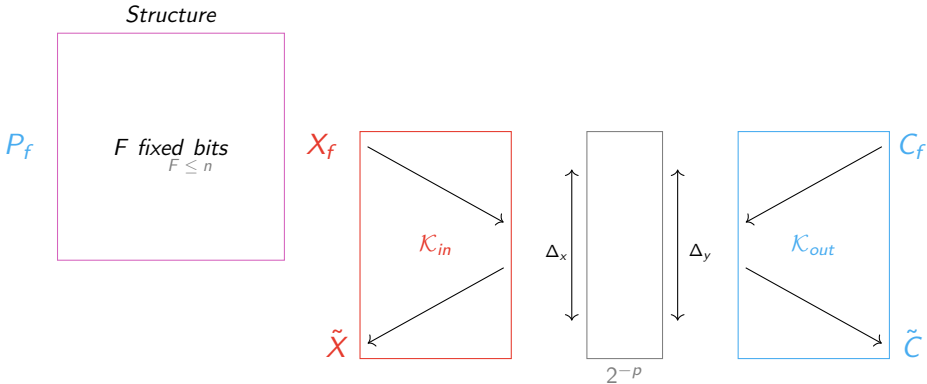
Diff MITM framework with structures [BBD+23], [AKM+24]



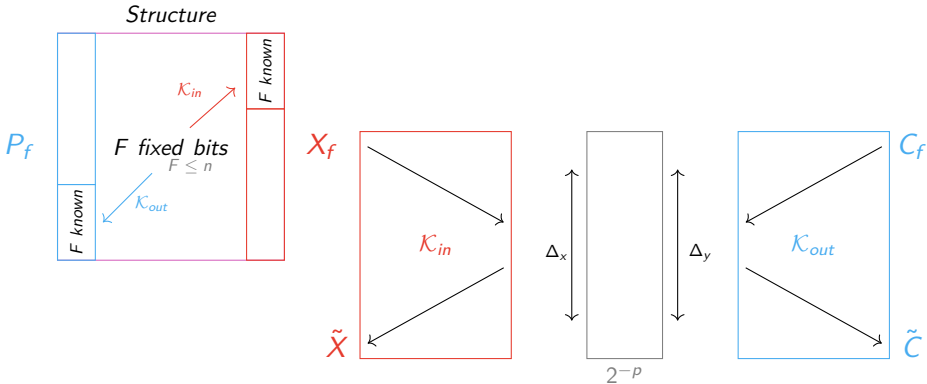
Diff MITM framework with structures [BBD+23], [AKM+24]



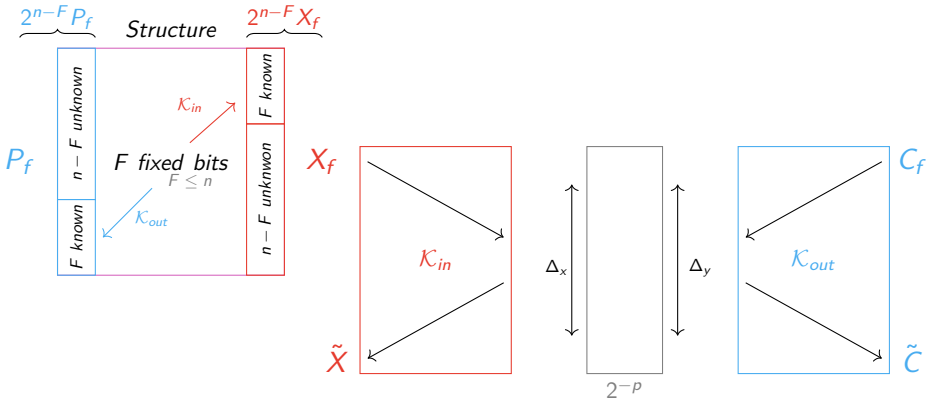
Diff MITM framework with structures [BBD+23], [AKM+24]



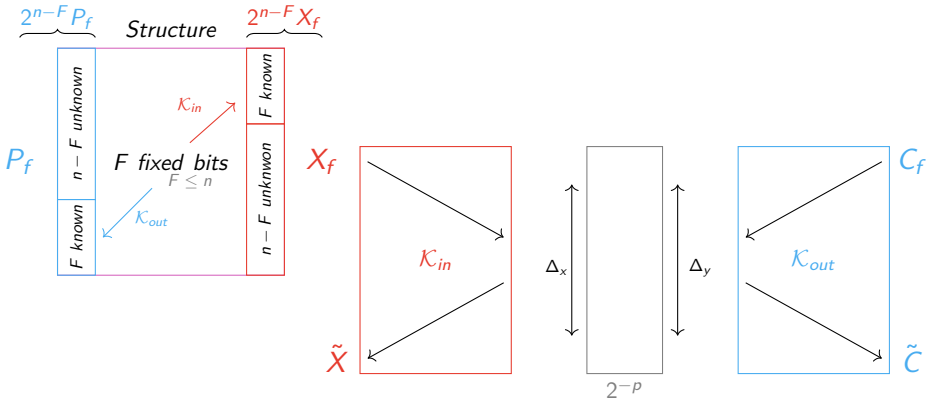
Diff MITM framework with structures [BBD+23], [AKM+24]



Diff MITM framework with structures [BBD+23], [AKM+24]

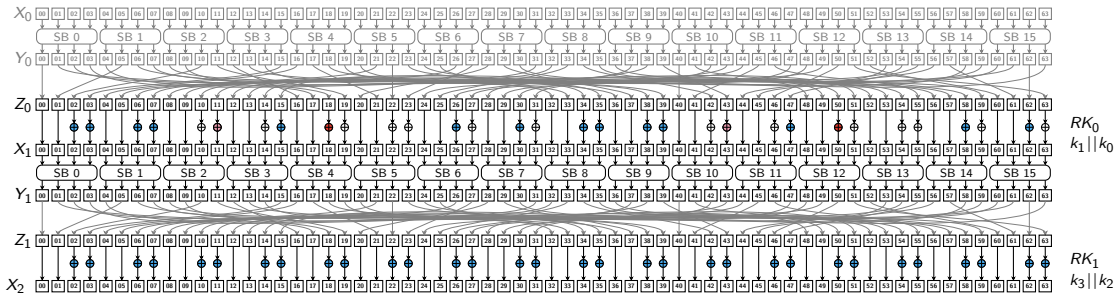


Diff MITM framework with structures [BBD+23], [AKM+24]



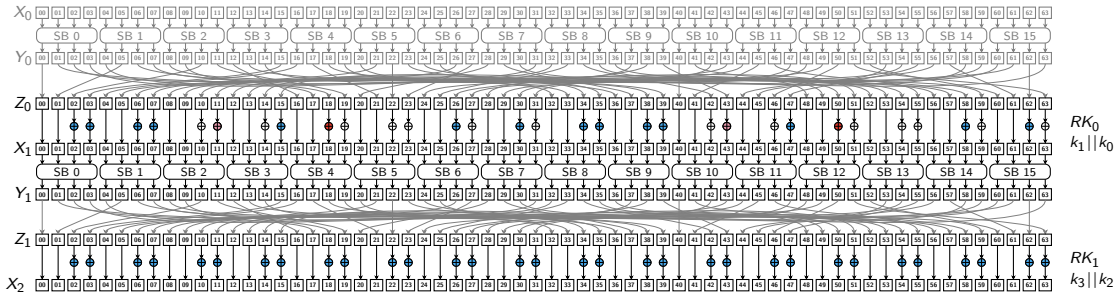
$$\mathcal{T} = 2^{p-(n-F)}\left(2^{n-F}2^{|\mathcal{K}_{in}|} + 2^{n-F}2^{|\mathcal{K}_{out}|} + 2^{2(n-F)+|\mathcal{K}_{in}|+|\mathcal{K}_{out}|-|\mathcal{K}_{in}\cap\mathcal{K}_{out}|-F-F_{add}}\right), \mathcal{M} = 2^{n-F}2^{min(\mathcal{K}_{in},\mathcal{K}_{out})}$$

Building a 2 rounds structure



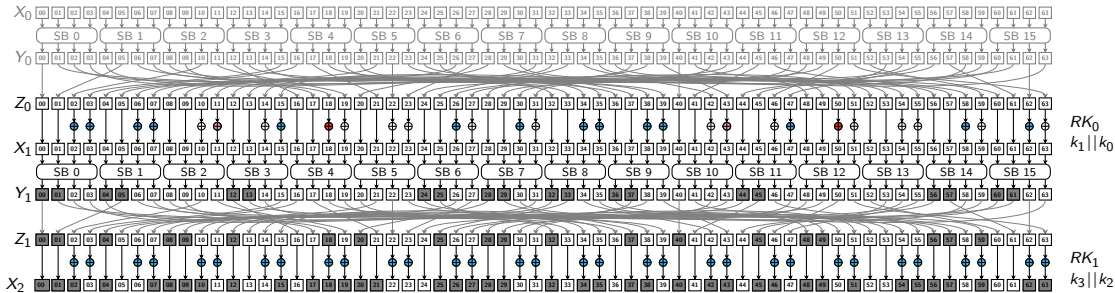
Building a 2 rounds structure

$|\mathcal{K}_{in}| = 44$ $|\mathcal{K}_{out}| = 52$ $|\mathcal{K}_{in} \cap \mathcal{K}_{out}| = 2$



Building a 2 rounds structure

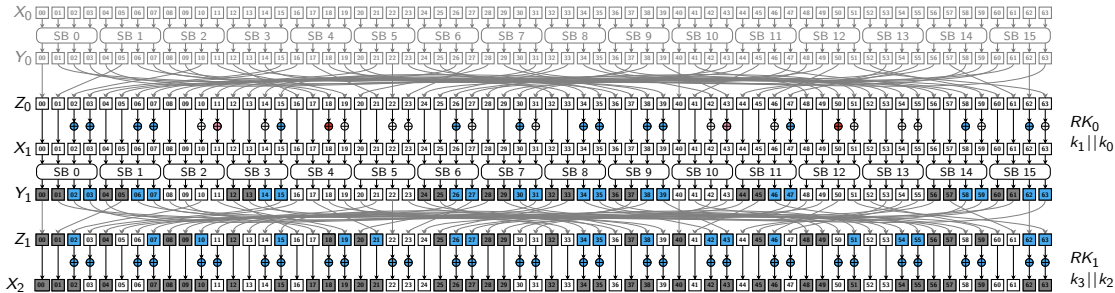
$|\mathcal{K}_{in}| = 44$ $|\mathcal{K}_{out}| = 52$ $|\mathcal{K}_{in} \cap \mathcal{K}_{out}| = 2$



$F_{X_2} = 40$

Building a 2 rounds structure

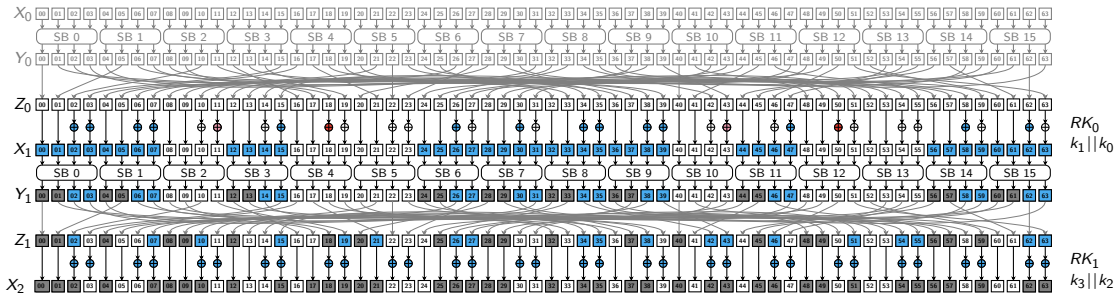
$|\mathcal{K}_{in}| = 44$ $|\mathcal{K}_{out}| = 52$ $|\mathcal{K}_{in} \cap \mathcal{K}_{out}| = 2$



$F_{X_2} = 40$

Building a 2 rounds structure

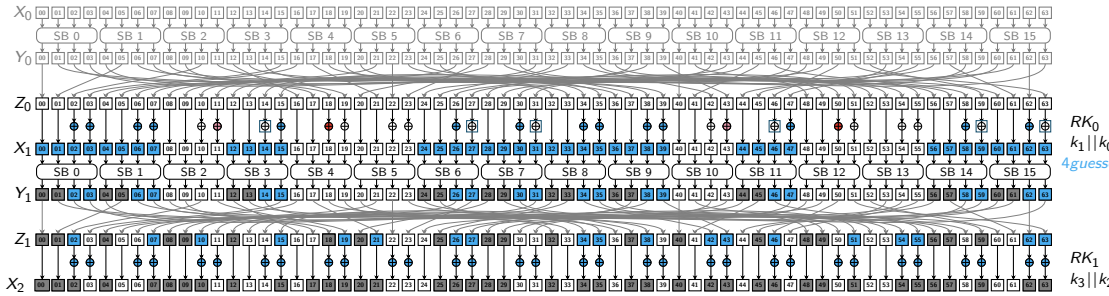
$|\mathcal{K}_{in}| = 44$ $|\mathcal{K}_{out}| = 52$ $|\mathcal{K}_{in} \cap \mathcal{K}_{out}| = 2$



$F_{X_2} = 40$

Building a 2 rounds structure

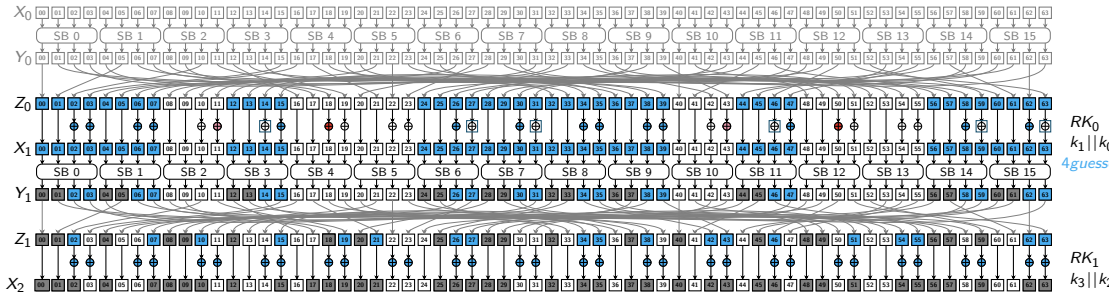
$|\mathcal{K}_{in}| = 44$ $|\mathcal{K}_{out}| = 52 + 4$ $|\mathcal{K}_{in} \cap \mathcal{K}_{out}| = 2$



$F_{X_2} = 40$

Building a 2 rounds structure

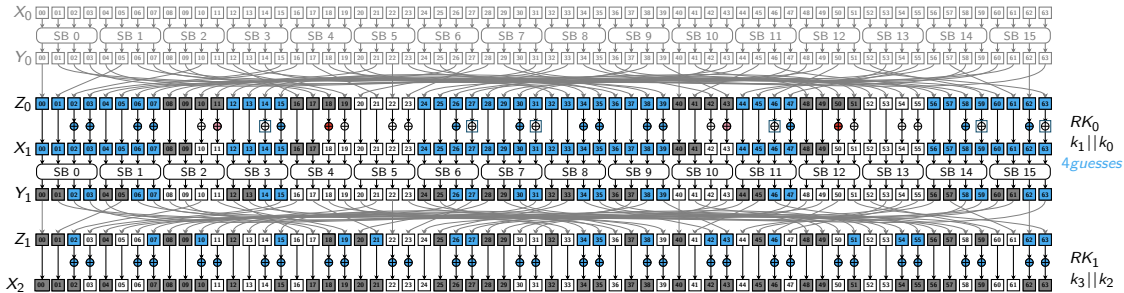
$|\mathcal{K}_{in}| = 44$ $|\mathcal{K}_{out}| = 52 + 4$ $|\mathcal{K}_{in} \cap \mathcal{K}_{out}| = 2$



$F_{X_2} = 40$

Building a 2 rounds structure

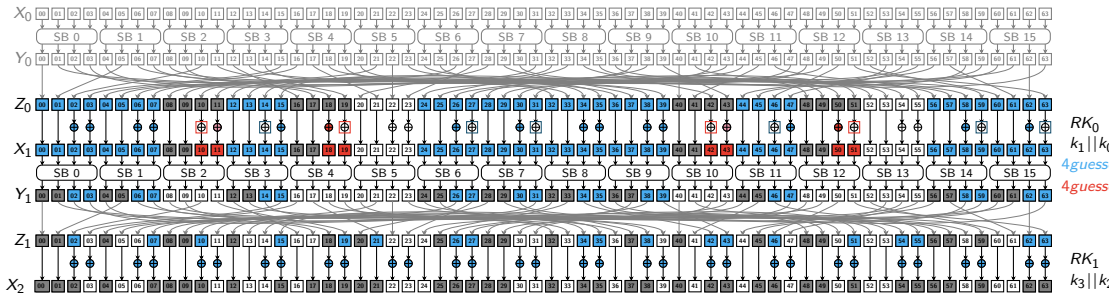
$|\mathcal{K}_{in}| = 44$ $|\mathcal{K}_{out}| = 52 + 4$ $|\mathcal{K}_{in} \cap \mathcal{K}_{out}| = 2$



$F_{X_2} = 40$ $F_{Z_0} = 16$

Building a 2 rounds structure

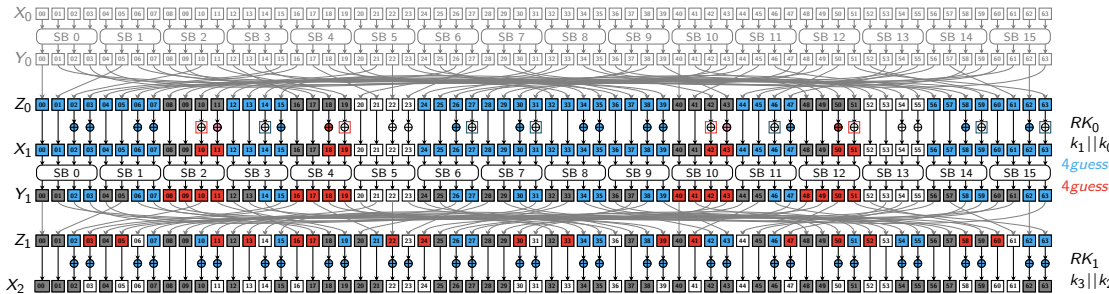
$|\mathcal{K}_{in}| = 44 + 4$ $|\mathcal{K}_{out}| = 52 + 4$ $|\mathcal{K}_{in} \cap \mathcal{K}_{out}| = 2$



$F_{X_2} = 40$ $F_{Z_0} = 16$

Building a 2 rounds structure

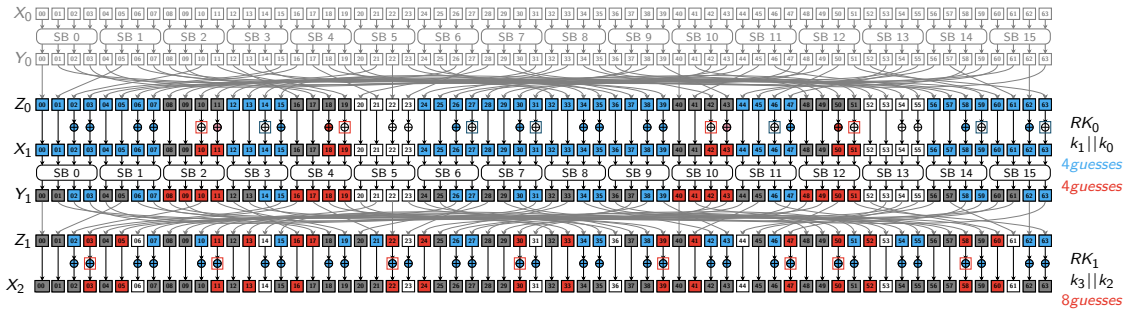
$|\mathcal{K}_{in}| = 44 + 4$ $|\mathcal{K}_{out}| = 52 + 4$ $|\mathcal{K}_{in} \cap \mathcal{K}_{out}| = 2$



$F_{X_2} = 40$ $F_{Z_0} = 16$

Building a 2 rounds structure

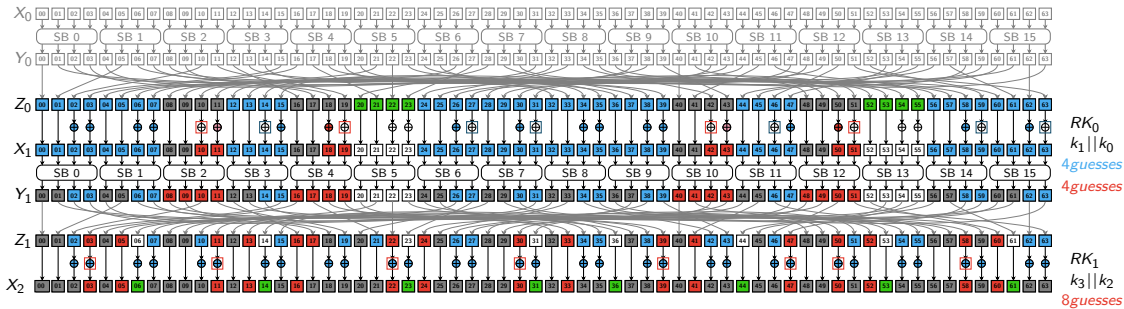
$|\mathcal{K}_{in}| = 44 + 4 + 8$ $|\mathcal{K}_{out}| = 52 + 4$ $|\mathcal{K}_{in} \cap \mathcal{K}_{out}| = 2 + 8$



$F_{X_2} = 40$ $F_{Z_0} = 16$

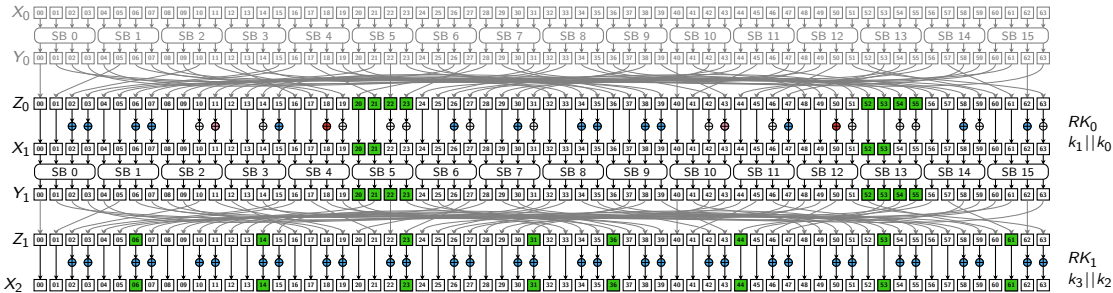
Building a 2 rounds structure

$|\mathcal{K}_{in}| = 44 + 4 + 8$ $|\mathcal{K}_{out}| = 52 + 4$ $|\mathcal{K}_{in} \cap \mathcal{K}_{out}| = 2 + 8$

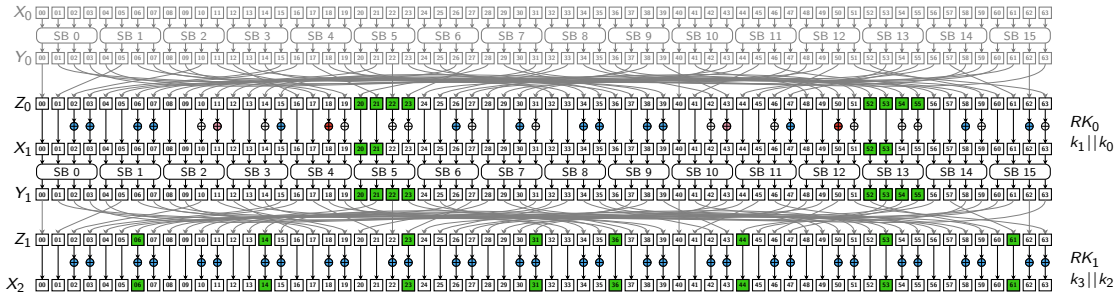


$F_{X_2} = 40$ $F_{Z_0} = 16$

Building a 2 rounds structure

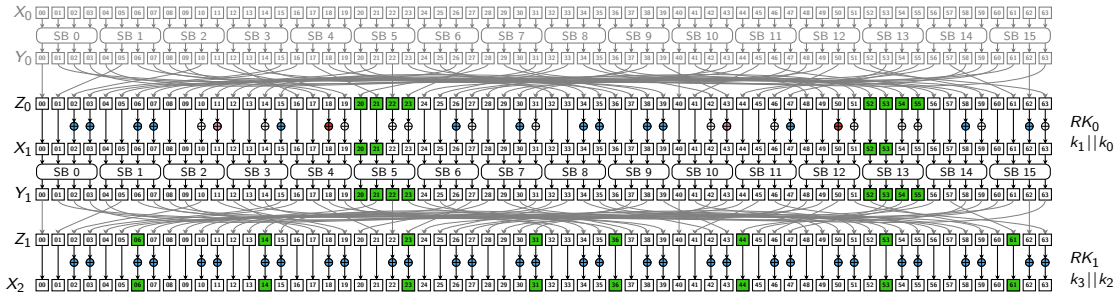


Building a 2 rounds structure



$$f_{add} = 2 \cdot 6$$

Building a 2 rounds structure



$$f_{add} = 2 \cdot 6 \qquad K_{info} = 4$$

Complexities with a structure

- $\mathcal{R} = 2 + 4 + 13 + 3 = 22$
- $|\mathcal{K}_{in}| = 56 - 2$, $|\mathcal{K}_{out}| = 58 - 1$, $|\mathcal{K}_{in} \cap \mathcal{K}_{out}| = 10$
- $F = 56$, $f_{add} = 12$

Complexities with a structure

- $\mathcal{R} = 2 + 4 + 13 + 3 = 22$
- $|\mathcal{K}_{in}| = 56 - 2$, $|\mathcal{K}_{out}| = 58 - 1$, $|\mathcal{K}_{in} \cap \mathcal{K}_{out}| = 10$
- $F = 56$, $f_{add} = 12$
- $\mathcal{T} = 2^{p}(2^{|\mathcal{K}_{in}|} + 2^{|\mathcal{K}_{out}|} + 2^{|\mathcal{K}_{in}|+|\mathcal{K}_{out}|+n-2*F-f_{add}})$
  $= 2^{57.82}(2^{56-2} + 2^{58-1} + 2^{54+57-10+64-2*56-12}) = 2^{114.82}$

$\rightarrow$ We recovered $54 + 57 - 10 + 4 = 105$ bits of the Master Key.

Complexities with a structure

- $\mathcal{R} = 2 + 4 + 13 + 3 = 22$
- $|\mathcal{K}_{in}| = 56 - 2$, $|\mathcal{K}_{out}| = 58 - 1$, $|\mathcal{K}_{in} \cap \mathcal{K}_{out}| = 10$
- $F = 56$, $f_{add} = 12$
- $\mathcal{T} = 2^{p}(2^{|\mathcal{K}_{in}|} + 2^{|\mathcal{K}_{out}|} + 2^{|\mathcal{K}_{in}|+|\mathcal{K}_{out}|+n-2*F-f_{add}})$
  $= 2^{57.82}(2^{56-2} + 2^{58-1} + 2^{54+57-10+64-2*56-12}) = 2^{114.82}$

$\rightarrow$ We recovered $54 + 57 - 10 + 4 = 105$ bits of the Master Key. To recover the full master key, we test the $2^{98.82}$ remaining pairs on extra data; final complexities are :

$$\mathcal{T} = 2^{98.82+19} = 2^{117.82},\ \mathcal{M} = 2^{8+56-10} = 2^{54},\ \mathcal{D} = 2^{61}$$

More trade-offs...

Results

Cipher	Rounds	Setup	Key space size	Time	Data	Memory	Type of Attack	Source
GIFT-64	21	SK	2^{124}	$2^{117.42}$	2^{64}	2^{96}	Differential	[CWWH25]
	22	**SK**	$\mathbf{2^{124}}$	$\mathbf{2^{117.82}}$	$\mathbf{2^{61}}$	$\mathbf{2^{99}}$	**Diff MITM**	**This Paper**
	25	RK	2^{120}	2^{107}	2^{51}	2^{49}	Differential	[BDD+24]
	25	**RK**	$\mathbf{2^{120}}$	$\mathbf{2^{81.59}}$	$\mathbf{2^{51}}$	$\mathbf{2^{50.12}}$	**Differential**	**This Paper**
	26	RK	2^{120}	$2^{113.03}$	$2^{61.96}$	$2^{95.15}$	Differential	[CN25]

Results

Cipher	Rounds	Setup	Key space size	Time	Data	Memory	Type of Attack	Source
GIFT-64	21	SK	2^{124}	$2^{117.42}$	2^{64}	2^{96}	Differential	[CWWH25]
	22	**SK**	$\mathbf{2^{124}}$	$\mathbf{2^{117.82}}$	$\mathbf{2^{61}}$	$\mathbf{2^{99}}$	**Diff MITM**	**This Paper**
	25	RK	2^{120}	2^{107}	2^{51}	2^{49}	Differential	[BDD+24]
	25	**RK**	$\mathbf{2^{120}}$	$\mathbf{2^{81.59}}$	$\mathbf{2^{51}}$	$\mathbf{2^{50.12}}$	**Differential**	**This Paper**
	26	RK	2^{120}	$2^{113.03}$	$2^{61.96}$	$2^{95.15}$	Differential	[CN25]

Thank you for your attention