A Known-Plaintext Attack with Minimal Data Complexity on 25-Round CRAFT

Eran Lambooij Patrick Neumann

FSE 2026

Inria, Paris, France

Inria

Comparison with Prior Attacks on Craft

Rounds	Time	Memory	Data	Attack	Setting	Reference
23	2^{125}	2^{101}	2^{60}	TD-MitM	CC	[AKMMN24]
	$2^{111.46}$	2^{120}	$2^{60.99}$	D	CP	[SYCHW24]
	2^{109}	2^{36}	2^{58}	TD-MitM	CC	[MNN25]
	2^{117}	2^{96}	2^{1}	MitM	KP	This Work
24	2^{110}	2^{34}	2^{60}	TD-MitM	CC	[MNN25]
	2^{121}	2^{104}	2^{1}	MitM	KP	This Work
25	$2^{117.58}$	2^{48}	2^{60}	TD-MitM	CC	[MNN25]
	2^{125}	2^{100}	2^{1}	MitM	KP	This Work
26	2^{118}	2^{34}	2^{64}	TD-MitM	CC	[MNN25]

D	Differential	MitM	Meet-in-the-Middle
ID	Impossible Differential	TD-MitM	Truncated-Differential MitM
CC	Chosen Ciphertext	CP	Chosen Plaintext
KP	Known Plaintext		

Comparison with Prior Attacks on Craft

Rounds	Time	Memory	Data	Attack	Setting	Reference
23	2^{125}	2^{101}	2^{60}	TD-MitM	CC	[AKMMN24]
	$2^{111.46}$	2^{120}	$2^{60.99}$	D	CP	[SYCHW24]
	2^{109}	2^{36}	2^{58}	TD-MitM	CC	[MNN25]
	2^{117}	2^{96}	2^{1}	MitM	KP	This Work
24	2^{110}	2^{34}	2^{60}	TD-MitM	CC	[MNN25]
	2^{121}	2^{104}	2^{1}	MitM	KP	This Work
25	$2^{117.58}$	2^{48}	2^{60}	TD-MitM	CC	[MNN25]
	2^{125}	2^{100}	2^{1}	MitM	KP	This Work
26	2^{118}	2^{34}	2^{64}	TD-MitM	CC	[MNN25]

D	Differential	MitM	Meet-in-the-Middle
ID	Impossible Differential	TD-MitM	Truncated-Differential MitM
CC	Chosen Ciphertext	CP	Chosen Plaintext
KP	Known Plaintext		

Comparison with Prior Attacks on Craft

Rounds	Time	Memory	Data	Attack	Setting	Reference
23	2^{125}	2^{101}	2^{60}	TD-MitM	CC	[AKMMN24]
	$2^{111.46}$	2^{120}	$2^{60.99}$	D	CP	[SYCHW24]
	2^{109}	2^{36}	2^{58}	TD-MitM	CC	[MNN25]
	2^{117}	2^{96}	2^{1}	MitM	KP	This Work
24	2^{110}	2^{34}	2^{60}	TD-MitM	CC	[MNN25]
	2^{121}	2^{104}	2^{1}	MitM	KP	This Work
25	$2^{117.58}$	2^{48}	2^{60}	TD-MitM	CC	[MNN25]
	2^{125}	2^{100}	2^{1}	MitM	KP	This Work
26	2^{118}	2^{34}	2^{64}	TD-MitM	CC	[MNN25]

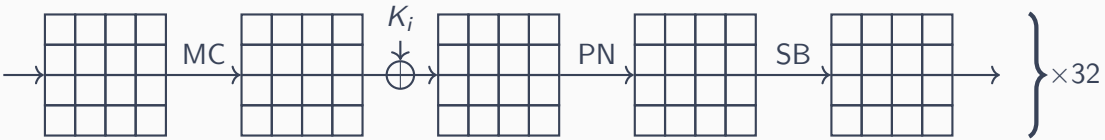
D	Differential	MitM	Meet-in-the-Middle
ID	Impossible Differential	TD-MitM	Truncated-Differential MitM
CC	Chosen Ciphertext	CP	Chosen Plaintext
KP	Known Plaintext		

Explanation of Craft [BLMR19] & Decomposition

- 64 bit state, represented as a 4×4 matrix, and 128 bit key (K_0, K_1)

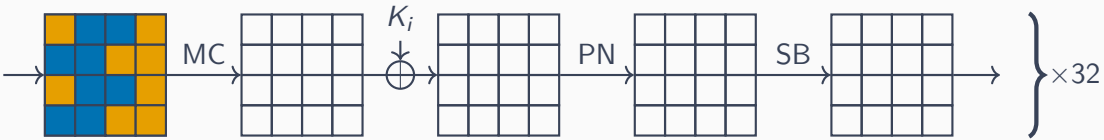
Explanation of Craft [BLMR19] & Decomposition

- 64 bit state, represented as a 4×4 matrix, and 128 bit key (K_0, K_1)



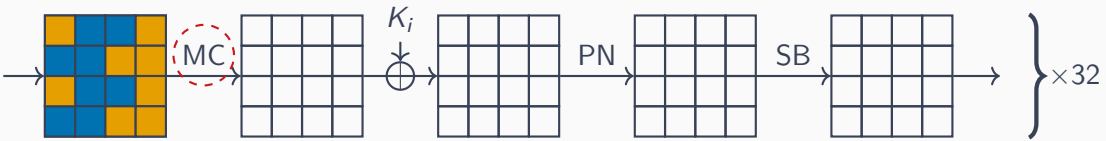
Explanation of Craft [BLMR19] & Decomposition

- 64 bit state, represented as a 4×4 matrix, and 128 bit key (K_0, K_1)



Explanation of Craft [BLMR19] & Decomposition

- 64 bit state, represented as a 4×4 matrix, and 128 bit key (K_0, K_1)

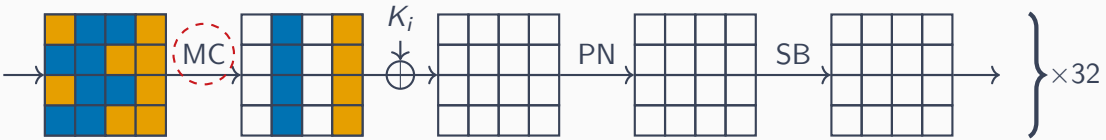


Mix Columns

$$\begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Explanation of Craft [BLMR19] & Decomposition

- 64 bit state, represented as a 4×4 matrix, and 128 bit key (K_0, K_1)

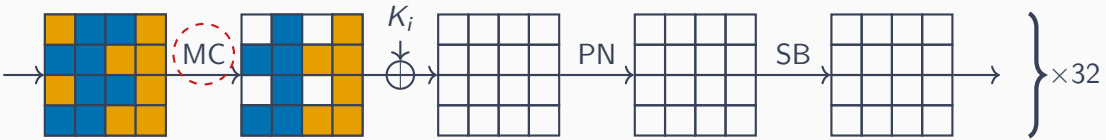


Mix Columns

$$\begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Explanation of Craft [BLMR19] & Decomposition

- 64 bit state, represented as a 4×4 matrix, and 128 bit key (K_0, K_1)

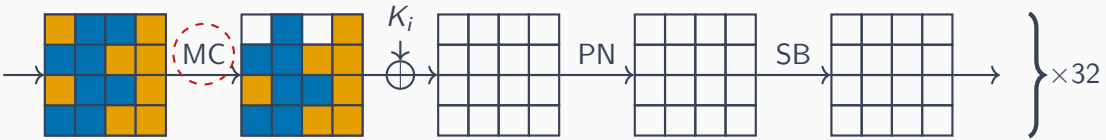


Mix Columns

$$\begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Explanation of Craft [BLMR19] & Decomposition

- 64 bit state, represented as a 4×4 matrix, and 128 bit key (K_0, K_1)

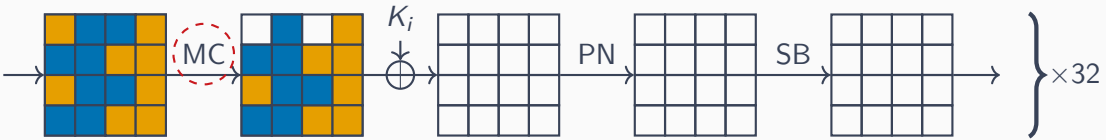


Mix Columns

$$\begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

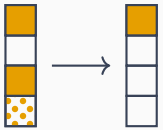
Explanation of Craft [BLMR19] & Decomposition

- 64 bit state, represented as a 4×4 matrix, and 128 bit key (K_0, K_1)



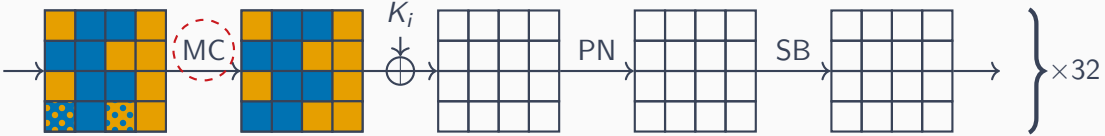
Mix Columns

$$\begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$



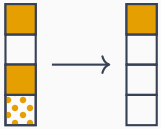
Explanation of Craft [BLMR19] & Decomposition

- 64 bit state, represented as a 4×4 matrix, and 128 bit key (K_0, K_1)



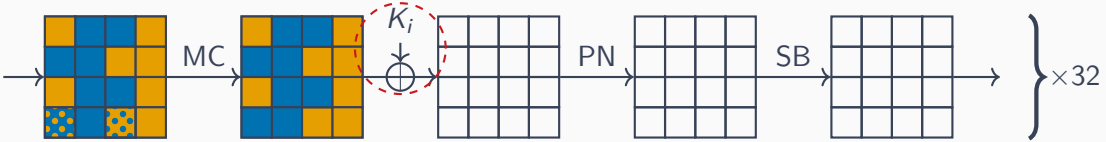
Mix Columns

$$\begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$



Explanation of Craft [BLMR19] & Decomposition

- 64 bit state, represented as a 4×4 matrix, and 128 bit key (K_0, K_1)



Key Addition

Add $K_{i \bmod 2}$ in round i

Explanation of Craft [BLMR19] & Decomposition

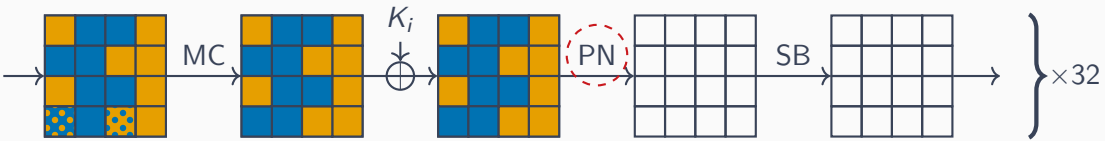
- 64 bit state, represented as a 4×4 matrix, and 128 bit key (K_0, K_1)

Key Addition

Add $K_{i \bmod 2}$ in round i

Explanation of Craft [BLMR19] & Decomposition

- 64 bit state, represented as a 4×4 matrix, and 128 bit key (K_0, K_1)



Permute Nibbles

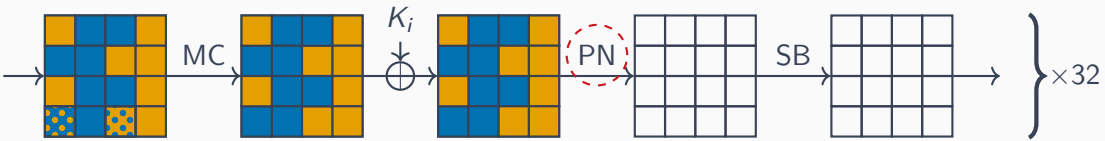
0	1	2	3
4	5	6	7
8	9	10	11
12	13	14	15

→

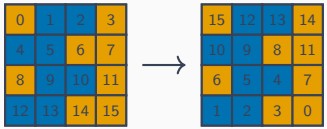
15	12	13	14
10	9	8	11
6	5	4	7
1	2	3	0

Explanation of Craft [BLMR19] & Decomposition

- 64 bit state, represented as a 4×4 matrix, and 128 bit key (K_0, K_1)



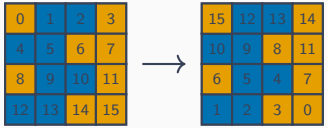
Permute Nibbles



Explanation of Craft [BLMR19] & Decomposition

- 64 bit state, represented as a 4×4 matrix, and 128 bit key (K_0, K_1)

Permute Nibbles



Explanation of Craft [BLMR19] & Decomposition

- 64 bit state, represented as a 4×4 matrix, and 128 bit key (K_0, K_1)

S-Box Layer

Apply s-box to all cells

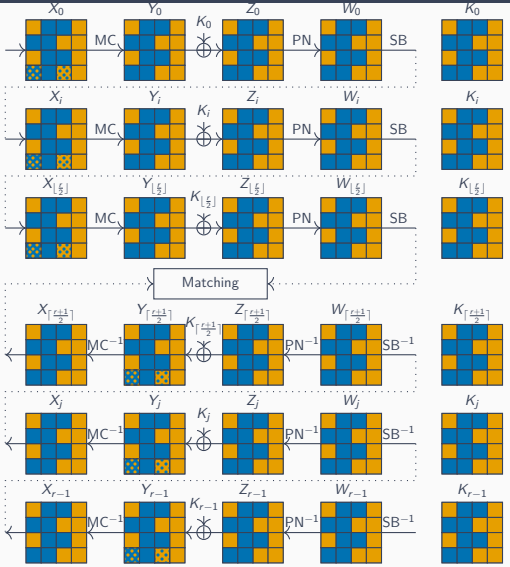
Explanation of Craft [BLMR19] & Decomposition

- 64 bit state, represented as a 4×4 matrix, and 128 bit key (K_0, K_1)

S-Box Layer

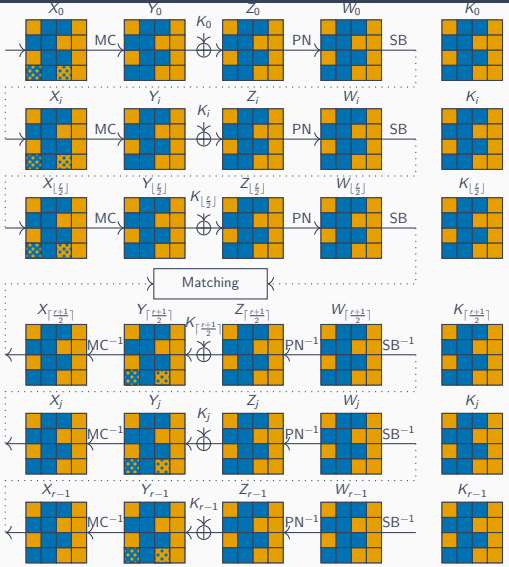
Apply s-box to all cells

Our Attack (Simplified)



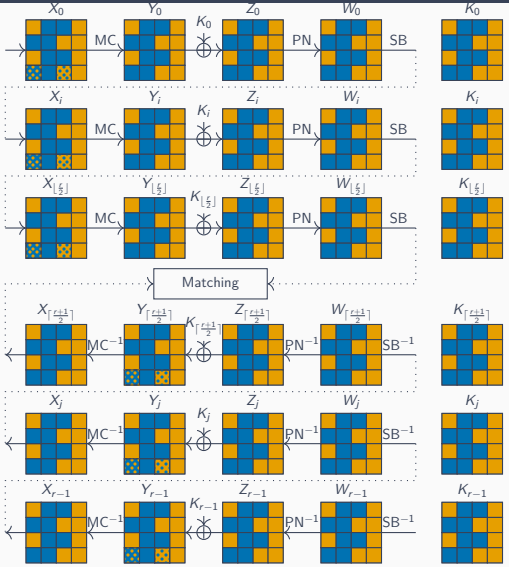
- Mount separate MitM attacks on *blue* and *orange* halves

Our Attack (Simplified)



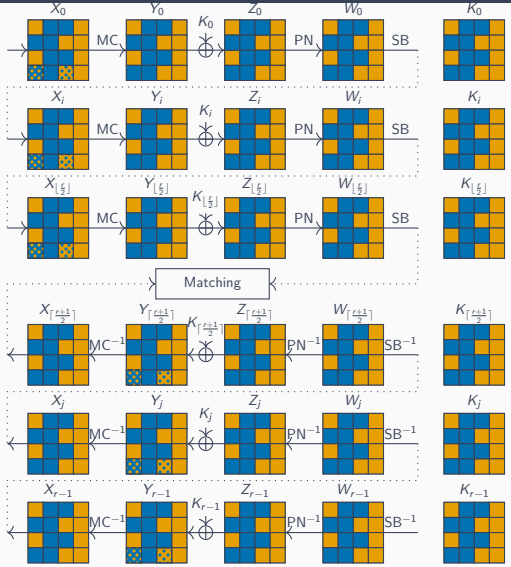
- Mount separate MitM attacks on *blue* and *orange* halves
- Merge by matching on the guessed values of the state

Our Attack (Simplified)



- Mount separate MitM attacks on *blue* and *orange* halves
- Merge by matching on the guessed values of the state
- Left with 2^{64} key candidates (using a single plaintext-ciphertext pair)

Our Attack (Simplified)



- Mount separate MitM attacks on *blue* and *orange* halves
- Merge by matching on the guessed values of the state
- Left with 2^{64} key candidates (using a single plaintext-ciphertext pair)
- Improve complexity by postponing state guesses to after key addition

Comparison with Prior Attacks on Craft

Rounds	Time	Memory	Data	Attack	Setting	Reference
23	2^{125}	2^{101}	2^{60}	TD-MitM	CC	[AKMMN24]
	$2^{111.46}$	2^{120}	$2^{60.99}$	D	CP	[SYCHW24]
	2^{109}	2^{36}	2^{58}	TD-MitM	CC	[MNN25]
	2^{117}	2^{96}	2^{1}	MitM	KP	This Work
24	2^{110}	2^{34}	2^{60}	TD-MitM	CC	[MNN25]
	2^{121}	2^{104}	2^{1}	MitM	KP	This Work
25	$2^{117.58}$	2^{48}	2^{60}	TD-MitM	CC	[MNN25]
	2^{125}	2^{100}	2^{1}	MitM	KP	This Work
26	2^{118}	2^{34}	2^{64}	TD-MitM	CC	[MNN25]

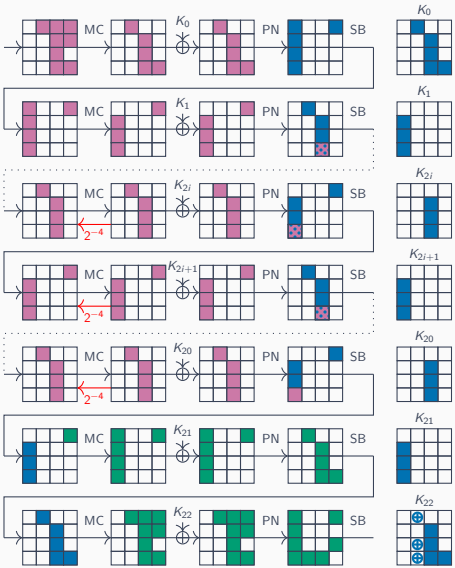
D	Differential	MitM	Meet-in-the-Middle
ID	Impossible Differential	TD-MitM	Truncated-Differential MitM
CC	Chosen Ciphertext	CP	Chosen Plaintext
KP	Known Plaintext		

Comparison with Prior Attacks on Craft

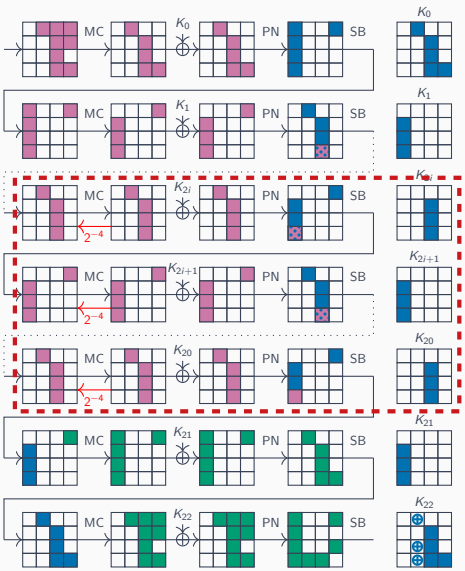
Rounds	Time	Memory	Data	Attack	Setting	Reference
23	2^{125}	2^{101}	2^{60}	TD-MitM	CC	[AKMMN24]
	$2^{111.46}$	2^{120}	$2^{60.99}$	D	CP	[SYCHW24]
	2^{109}	2^{36}	2^{58}	TD-MitM	CC	[MNN25]
	2^{117}	2^{96}	2^{1}	MitM	KP	This Work
24	2^{110}	2^{34}	2^{60}	TD-MitM	CC	[MNN25]
	2^{121}	2^{104}	2^{1}	MitM	KP	This Work
25	$2^{117.58}$	2^{48}	2^{60}	TD-MitM	CC	[MNN25]
	2^{125}	2^{100}	2^{1}	MitM	KP	This Work
26	2^{118}	2^{34}	2^{64}	TD-MitM	CC	[MNN25]

D	Differential	MitM	Meet-in-the-Middle
ID	Impossible Differential	TD-MitM	Truncated-Differential MitM
CC	Chosen Ciphertext	CP	Chosen Plaintext
KP	Known Plaintext		

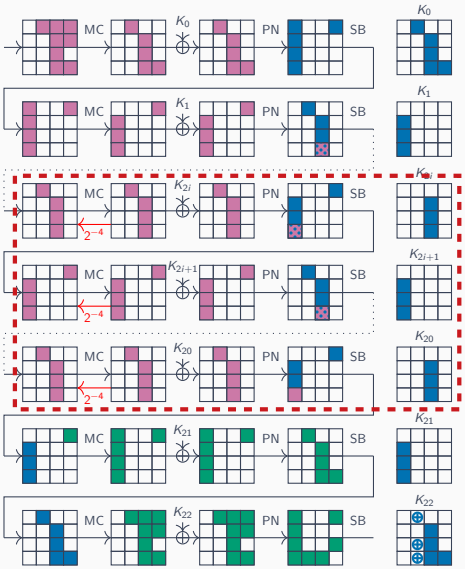
A Link to the Best Attack [MNN25]



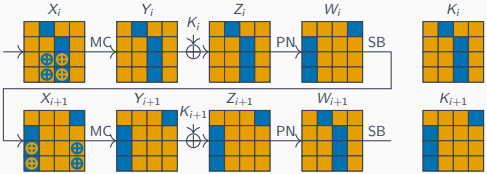
A Link to the Best Attack [MNN25]



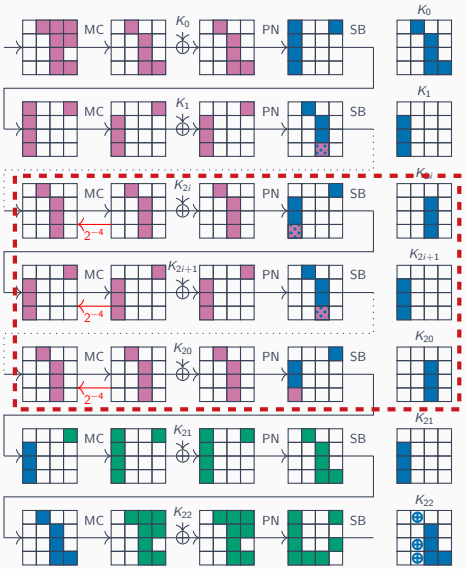
A Link to the Best Attack [MNN25]



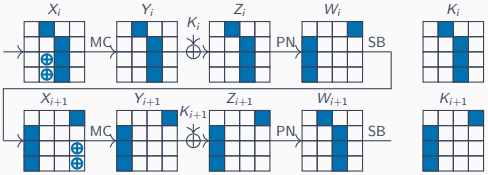
2-Round Iterative Decomposition



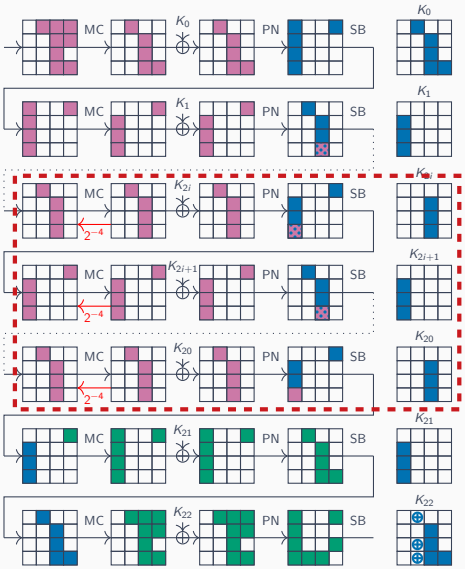
A Link to the Best Attack [MNN25]



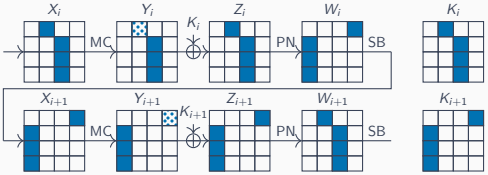
2-Round Iterative Decomposition



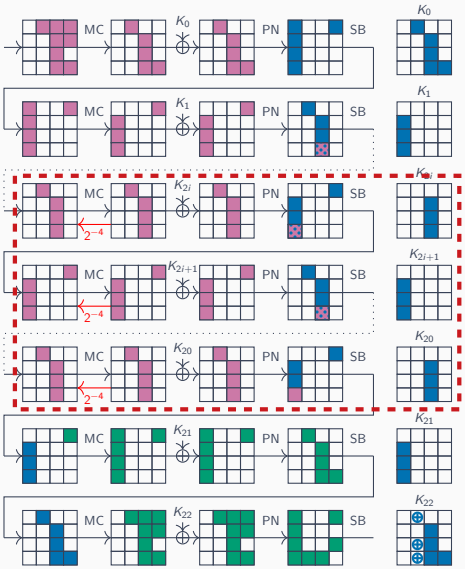
A Link to the Best Attack [MNN25]



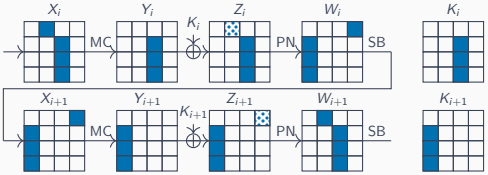
2-Round Iterative Decomposition



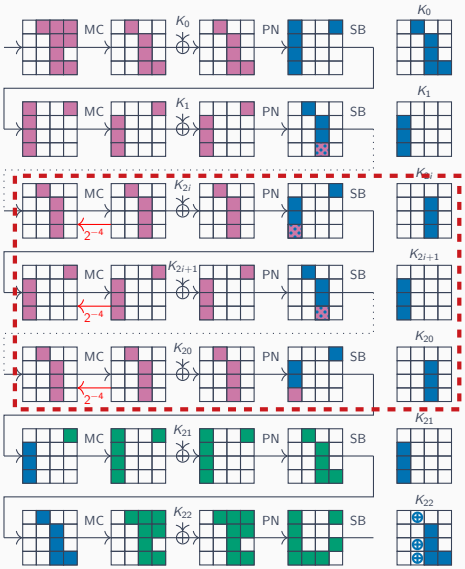
A Link to the Best Attack [MNN25]



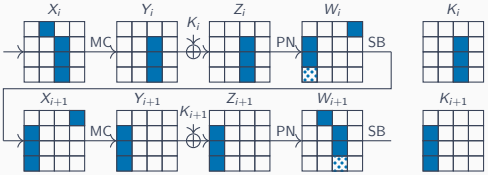
2-Round Iterative Decomposition



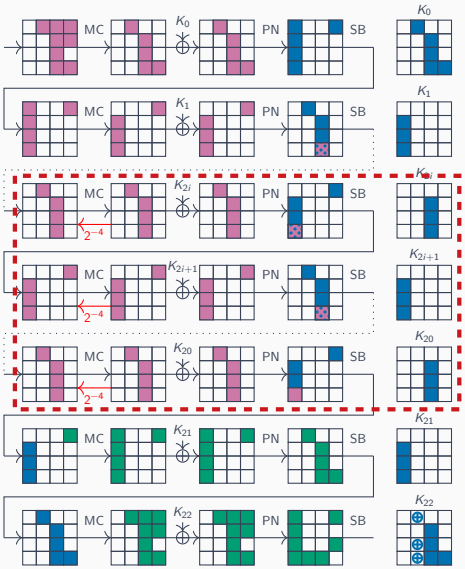
A Link to the Best Attack [MNN25]



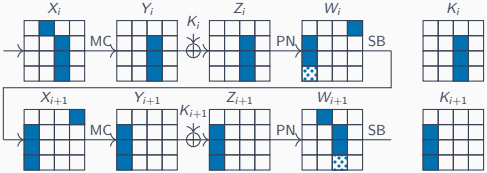
2-Round Iterative Decomposition



A Link to the Best Attack [MNN25]

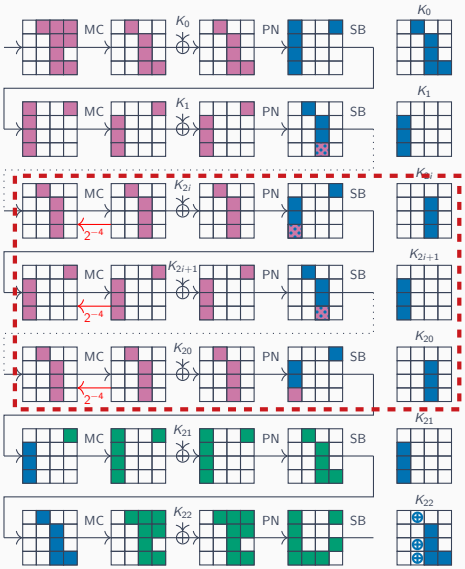


2-Round Iterative Decomposition

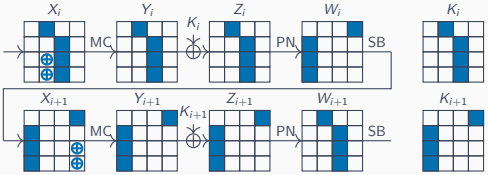


Difference stays within the *blue* part

A Link to the Best Attack [MNN25]

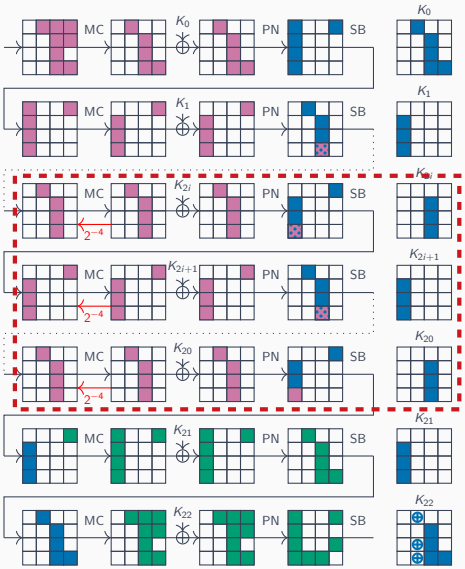


2-Round Iterative Decomposition

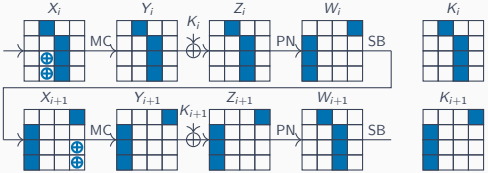


Difference stays within the *blue* part

A Link to the Best Attack [MNN25]



2-Round Iterative Decomposition

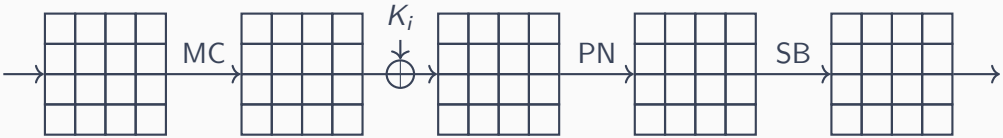


Difference stays within the *blue* part

Guessed part of the state stays constant

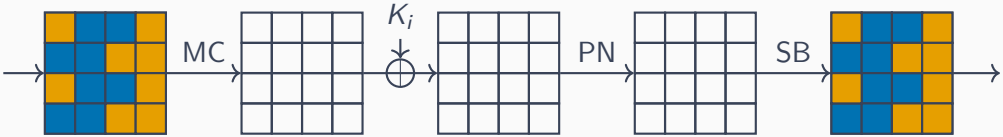
How to Find Decompositions

- For AES-like ciphers & cell-aligned decompositions



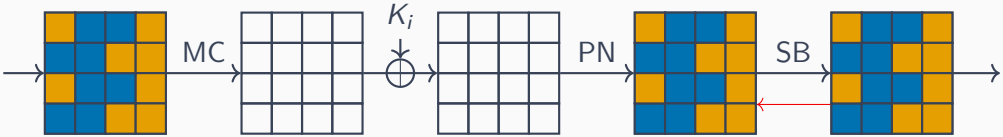
How to Find Decompositions

- For AES-like ciphers & cell-aligned decompositions
  - Given a decomposition of the input and the output



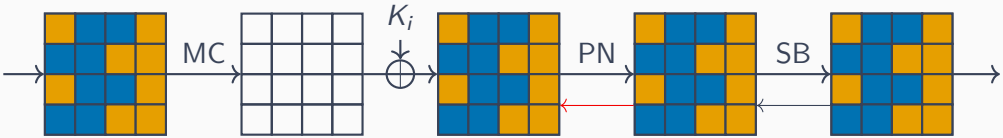
How to Find Decompositions

- For AES-like ciphers & cell-aligned decompositions
  - Given a decomposition of the input and the output



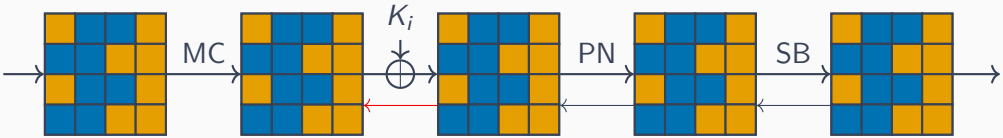
How to Find Decompositions

- For AES-like ciphers & cell-aligned decompositions
  - Given a decomposition of the input and the output



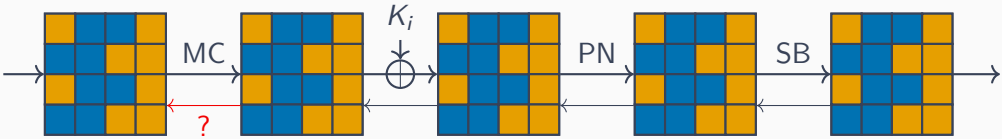
How to Find Decompositions

- For AES-like ciphers & cell-aligned decompositions
  - Given a decomposition of the input and the output



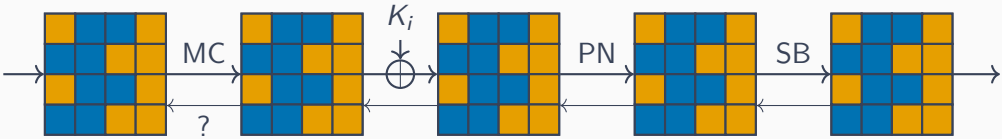
How to Find Decompositions

- For AES-like ciphers & cell-aligned decompositions
  - Given a decomposition of the input and the output
  - Can be broken down to transitions over Mix-Columns



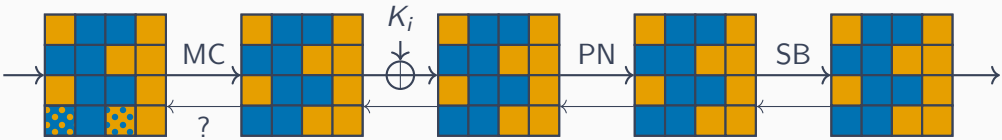
How to Find Decompositions

- For AES-like ciphers & cell-aligned decompositions
  - Given a decomposition of the input and the output
  - Can be broken down to transitions over Mix-Columns
  - Derive cost of transition as the number of bits that need to be guessed



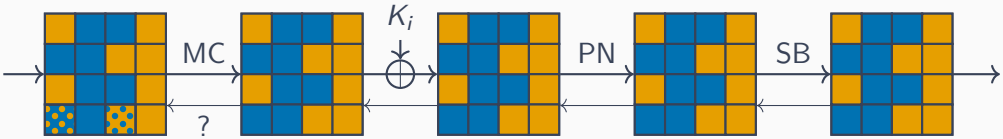
How to Find Decompositions

- For AES-like ciphers & cell-aligned decompositions
  - Given a decomposition of the input and the output
  - Can be broken down to transitions over Mix-Columns
  - Derive cost of transition as the number of bits that need to be guessed



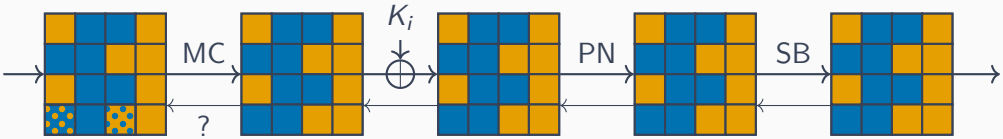
How to Find Decompositions

- For AES-like ciphers & cell-aligned decompositions
  - Given a decomposition of the input and the output
  - Can be broken down to transitions over Mix-Columns
  - Derive cost of transition as the number of bits that need to be guessed
  - Model similar to s-box transition (in the differential or linear setting)



How to Find Decompositions

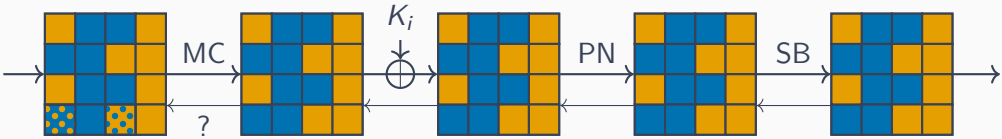
- For AES-like ciphers & cell-aligned decompositions
  - Given a decomposition of the input and the output
  - Can be broken down to transitions over Mix-Columns
  - Derive cost of transition as the number of bits that need to be guessed
  - Model similar to s-box transition (in the differential or linear setting)



- Applied to SKINNY and MANTIS/MIDORI/QARMA

How to Find Decompositions

- For AES-like ciphers & cell-aligned decompositions
  - Given a decomposition of the input and the output
  - Can be broken down to transitions over Mix-Columns
  - Derive cost of transition as the number of bits that need to be guessed
  - Model similar to s-box transition (in the differential or linear setting)



- Applied to SKINNY and MANTIS/MIDORI/QARMA
- Found no promising decomposition

Final Remarks

- Key schedule needs to be aligned with decomposition for this type of attack

Final Remarks

- Key schedule needs to be aligned with decomposition for this type of attack
- Our attacks on CRAFT could be prevented by adding a nibble permutation to the key schedule

Final Remarks

- Key schedule needs to be aligned with decomposition for this type of attack
- Our attacks on CRAFT could be prevented by adding a nibble permutation to the key schedule
- Open questions: applicability to unaligned primitives & primitives without key schedule

Final Remarks

- Key schedule needs to be aligned with decomposition for this type of attack
- Our attacks on CRAFT could be prevented by adding a nibble permutation to the key schedule
- Open questions: applicability to unaligned primitives & primitives without key schedule

Thank you for your attention!