Related-key Differential Cryptanalysis of Full Round CRAFT

Muhammad ElSheikh and Amr M. Youssef

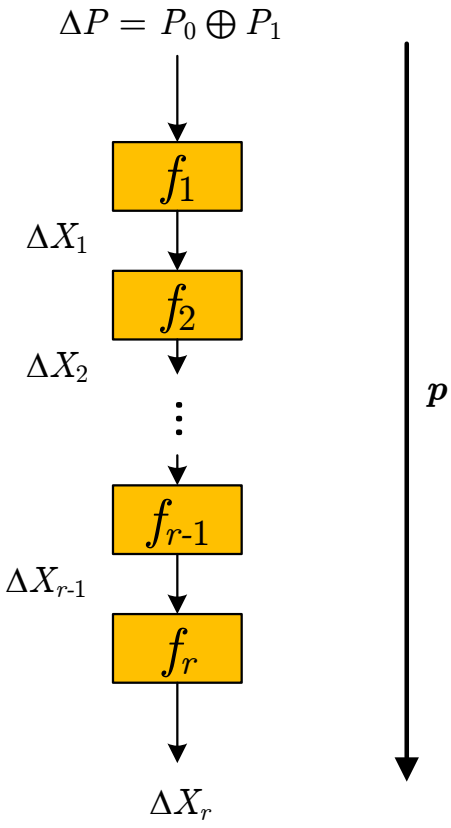
Concordia Institute for Information Systems Engineering,
Concordia University, Montréal, Québec, Canada

SPACE 2019
December 5-7, 2019
Gandhinagar, India

Outline

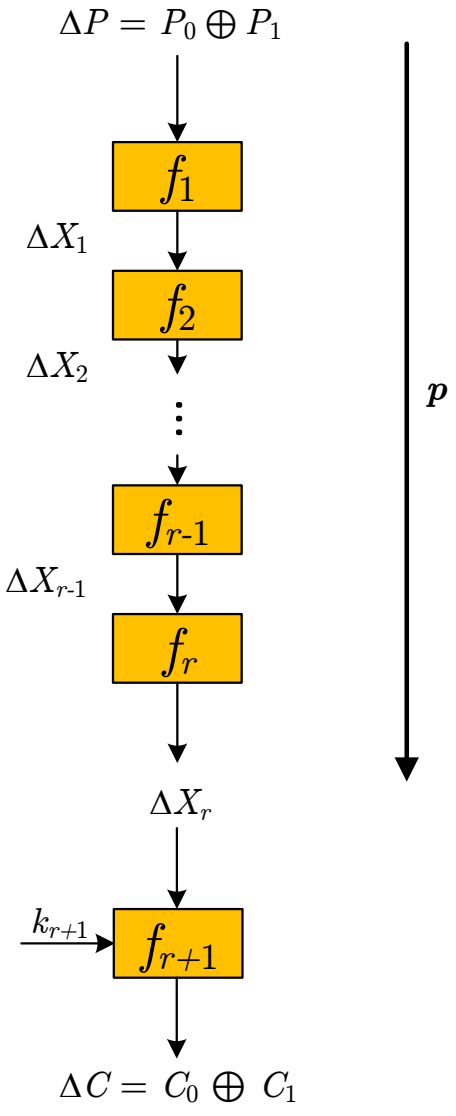
Outline

Differential Cryptanalysis



$$Pr(\Delta P \rightarrow \Delta X_r) = p > 2^{-n}$$

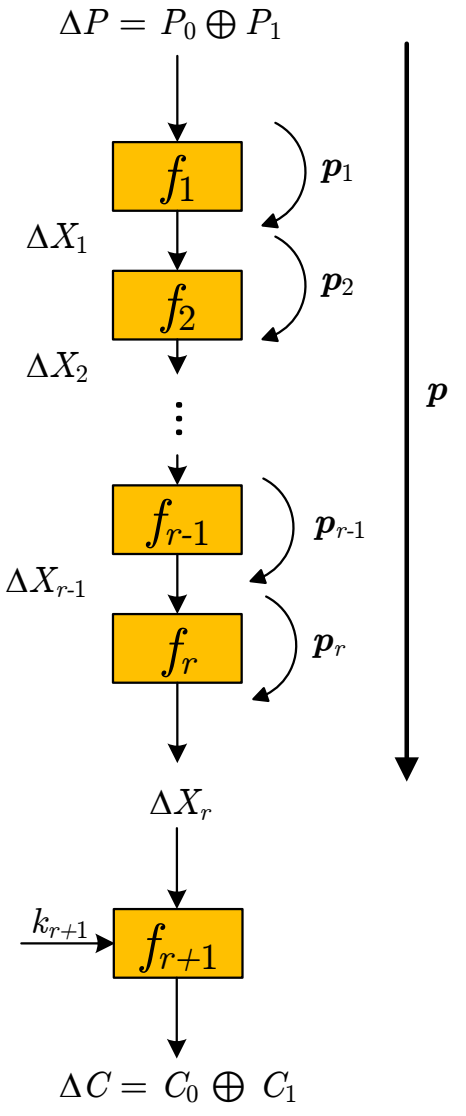
Differential Cryptanalysis



$$Pr(\Delta P \rightarrow \Delta X_r) = p > 2^{-n}$$

Append one more round and Guess k_{r+1}

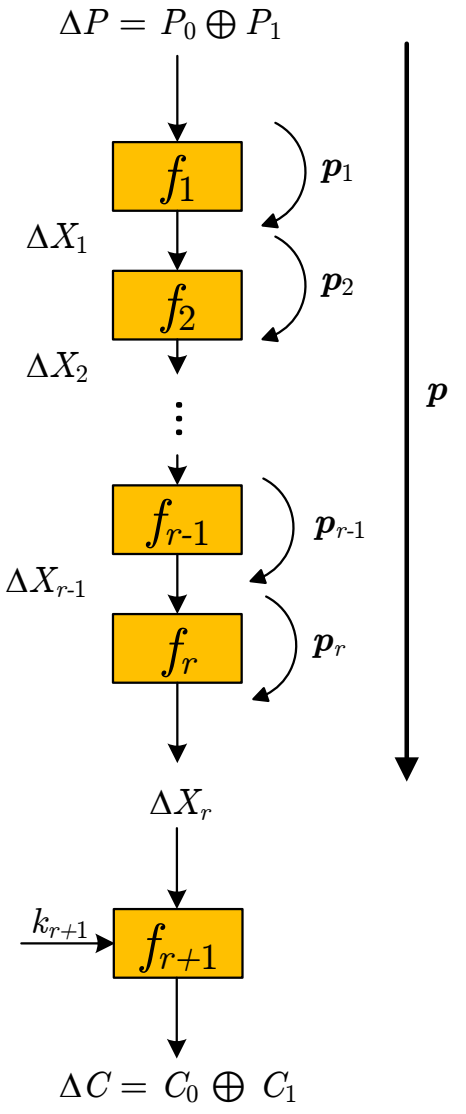
Differential Cryptanalysis



$$Pr(\Delta P \rightarrow \Delta X_r) = p > 2^{-n}$$

$$\Delta P \xrightarrow{p_1} \Delta X_1 \cdots \xrightarrow{p_r} \Delta X_r$$

Differential Cryptanalysis



$$Pr(\Delta P \rightarrow \Delta X_r) = p > 2^{-n}$$

$$\Delta P \xrightarrow{p_1} \Delta X_1 \cdots \xrightarrow{p_r} \Delta X_r$$

$$p = \prod_{i=1}^{r} p_i$$

Outline

Specifications of CRAFT

A lightweight tweakable block cipher

- Input:
  - a block size of 64 bits. It is represented as a 4×4 square array of nibbles.
  - a key (K) of 128 bits length split into two 64-bit subkeys K^0 and K^1, and each subkey is represented as a 4×4 square array of nibbles.
  - a tweak (T) of 64 bits. It is represented as a 4×4 square array of nibbles.
- Output: a block of 64 bits of ciphertext.

Tweakey Schedule

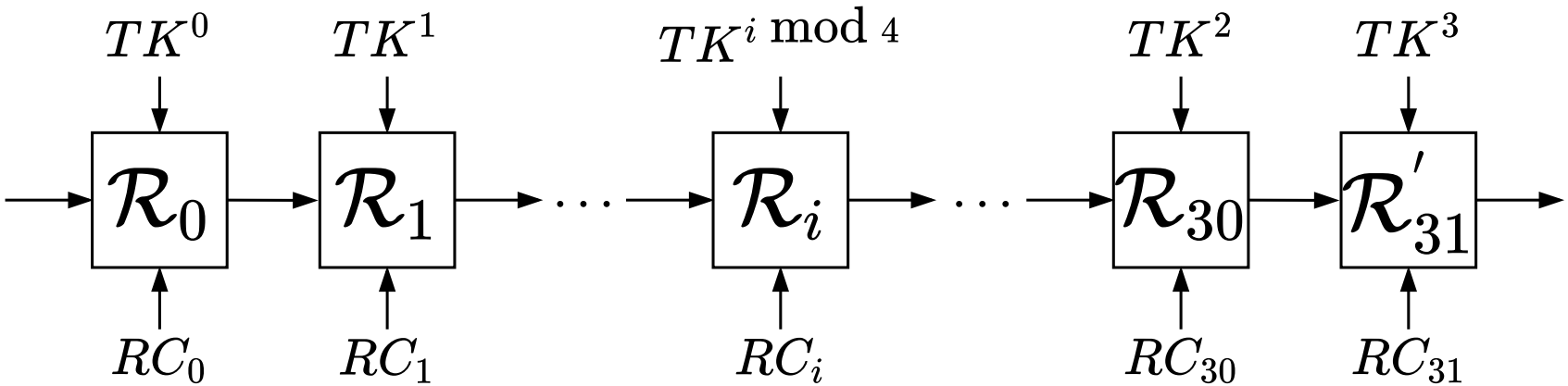
- Input: subkeys K^0 and K^1, and a tweak T.
- Output: four 64-bit tweakeys TK^0, TK^1, TK^2 and TK^3.
- Operation:

$$TK^0 = K^0 \oplus T$$
$$TK^1 = K^1 \oplus T$$
$$TK^2 = K^0 \oplus Q(T)$$
$$TK^3 = K^1 \oplus Q(T)$$

where $Q(T)$ is a permutation on the nibbles of the input tweak T.

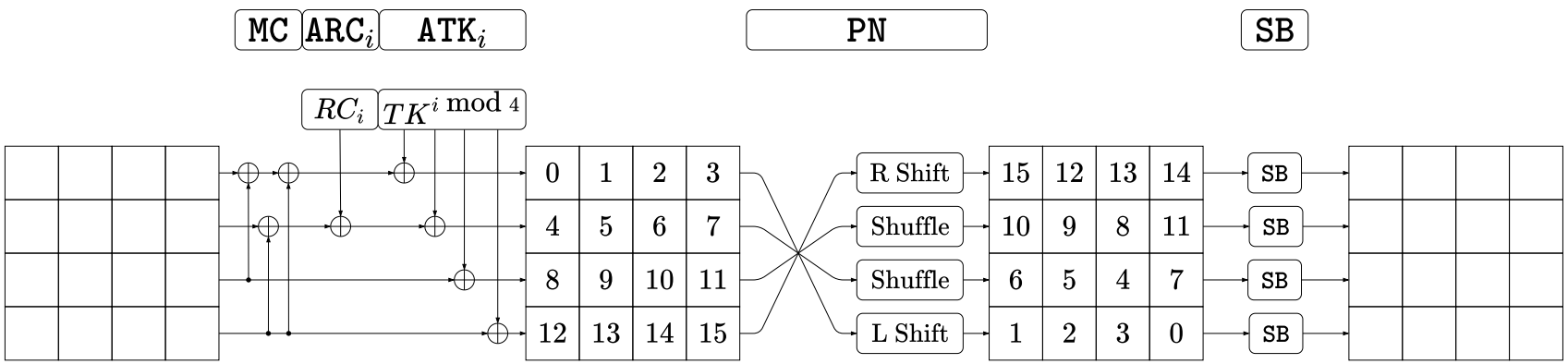
The encryption operation

- The plaintext $m = m_0||m_1||\cdots||m_{14}||m_{15}$ (where m_i is a 4-bit nibble) is loaded into the 4×4 square array internal state.
- The internal state is updated by applying the full round function of CRAFT 31 times ($\mathcal{R}_i$, $0 \leq i \leq 30$) using the tweakey $TK^{i \bmod 4}$.
- One more linear round($\mathcal{R}'_{31}$) is applied on the internal state using the tweakey TK^3 in order to compute the ciphertext.



Complete Single Round

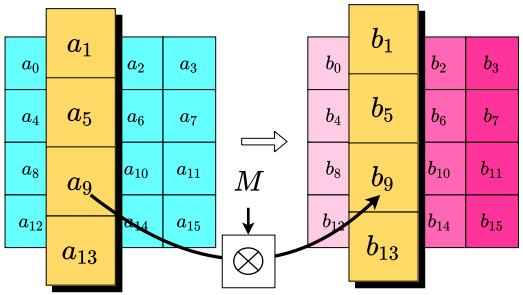
- The full round of CRAFT ($\mathcal{R}_i$) consists of the following five operations: MixColumn, $\texttt{AddConstant}_i$, $\texttt{AddTweakey}_i$, PermuteNibbles and SubBox.
- The last round ($\mathcal{R}'_{31}$) omits PermuteNibbles and SubBox operations from the full round.



a_0	a_1	a_2	a_3
a_4	a_5	a_6	a_7
a_8	a_9	a_{10}	a_{11}
a_{12}	a_{13}	a_{14}	a_{15}

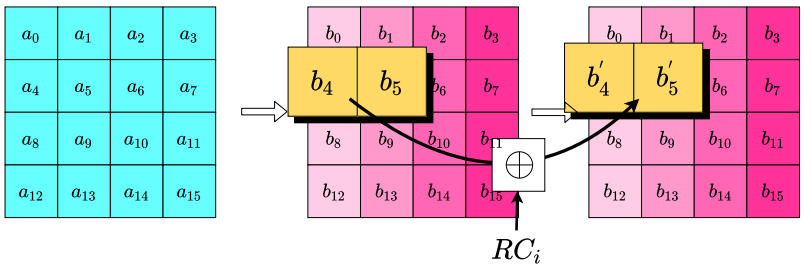
- The internal state of the cipher is represented as a row-wise 4×4 square array of nibbles or as a 16-nibble vector by concatenating the rows of the square array.
- The notation $I_{i,j}$ is used to denote the nibble located at row i and column j of the 4×4 array.
- The single subscript I_i denotes the nibble in the i-th position of 16-nibble vector, i.e., $I_{i,j} = I_{4i+j}$.

MixColumn (MC)



$$M = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} I_{0,j} \\ I_{1,j} \\ I_{2,j} \\ I_{3,j} \end{bmatrix} \mapsto \begin{bmatrix} I_{0,j} \oplus I_{2,j} \oplus I_{3,j} \\ I_{1,j} \oplus I_{3,j} \\ I_{2,j} \\ I_{3,j} \end{bmatrix}$$

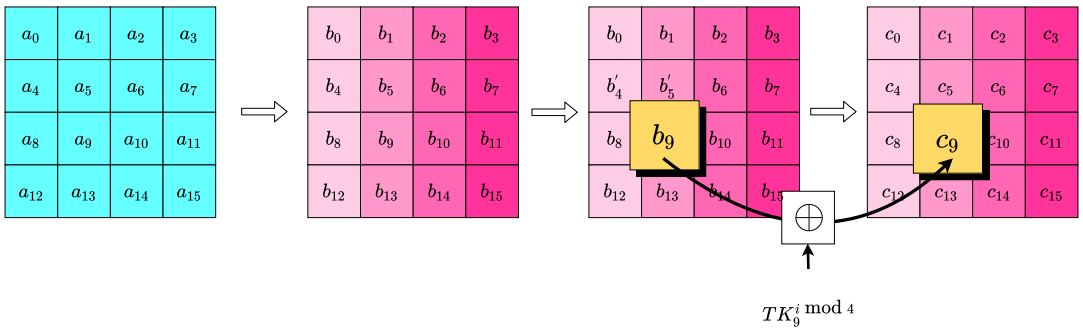
AddConstants$_i$ (ARC$_i$)



The internal state nibbles I_4 and I_5 are XOR-ed with the round constant RC_i.

$$(b'_4||b'_5) = (b_4||b_5) \oplus RC_i$$

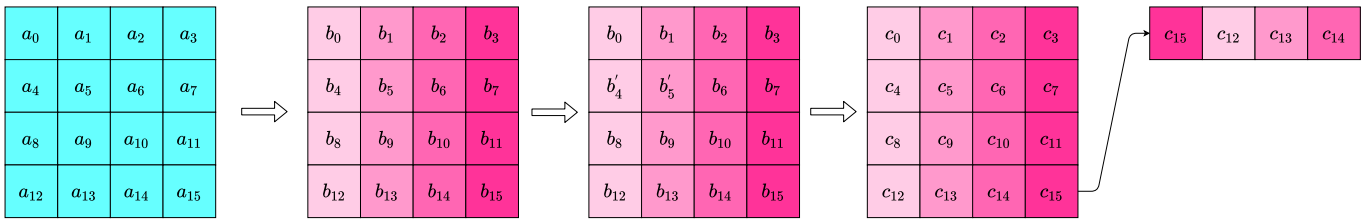
$\texttt{AddTweakey}_i$ $(\texttt{ATK}_i)$



Each nibble of the internal state is XOR-ed with the corresponding nibble of the tweakey $TK^{i \bmod 4}$.

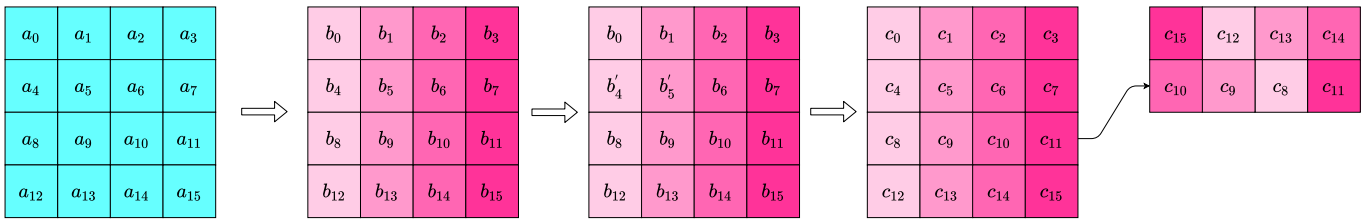
$$c_j = b_j \oplus TK_j^{i \bmod 4}$$

PermuteNibbles (PN)



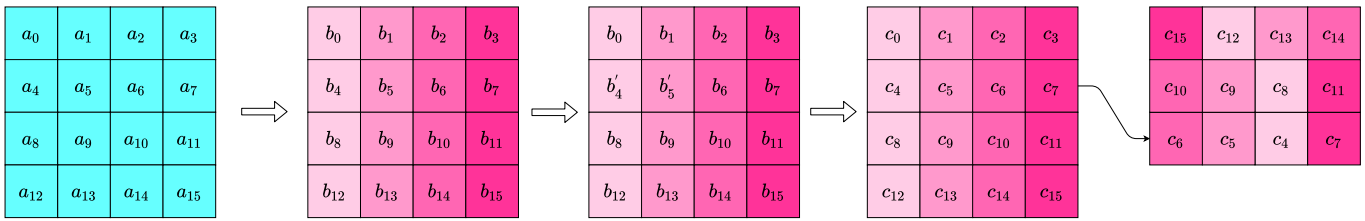
The first row of the new state is the last row of the current state shifted to right by one position.

PermuteNibbles (PN)



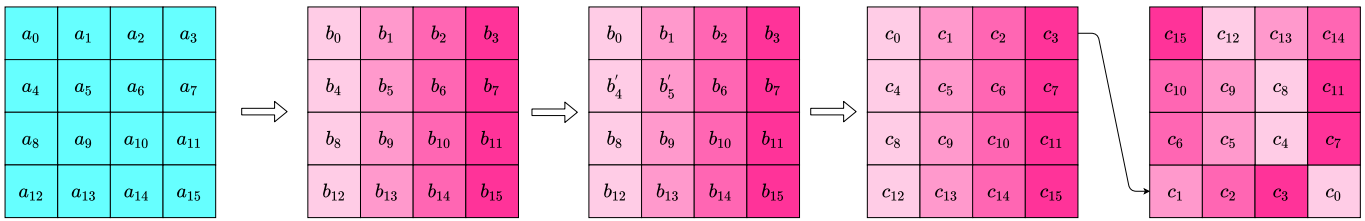
The second row of the new state is the third row of the current state after shuffling.

PermuteNibbles (PN)



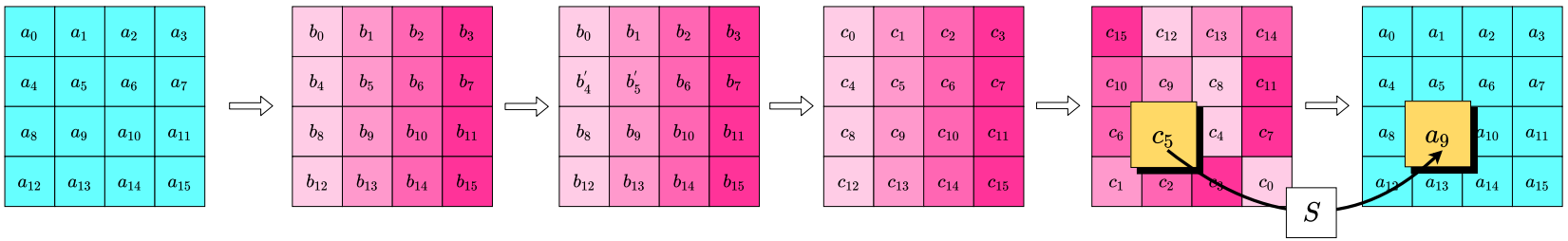
The third row of the new state is the row of the second current state after shuffling.

PermuteNibbles (PN)



The last row of the new state is the first row of the current state shifted to left by one position.

SubBox (SB)



A nonlinear bijective mapping applied on every nibble of the internal state in parallel using the following Sbox:

x	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
$S(x)$	c	a	d	3	e	b	f	7	8	9	1	5	0	2	4	6

Outline

Notation

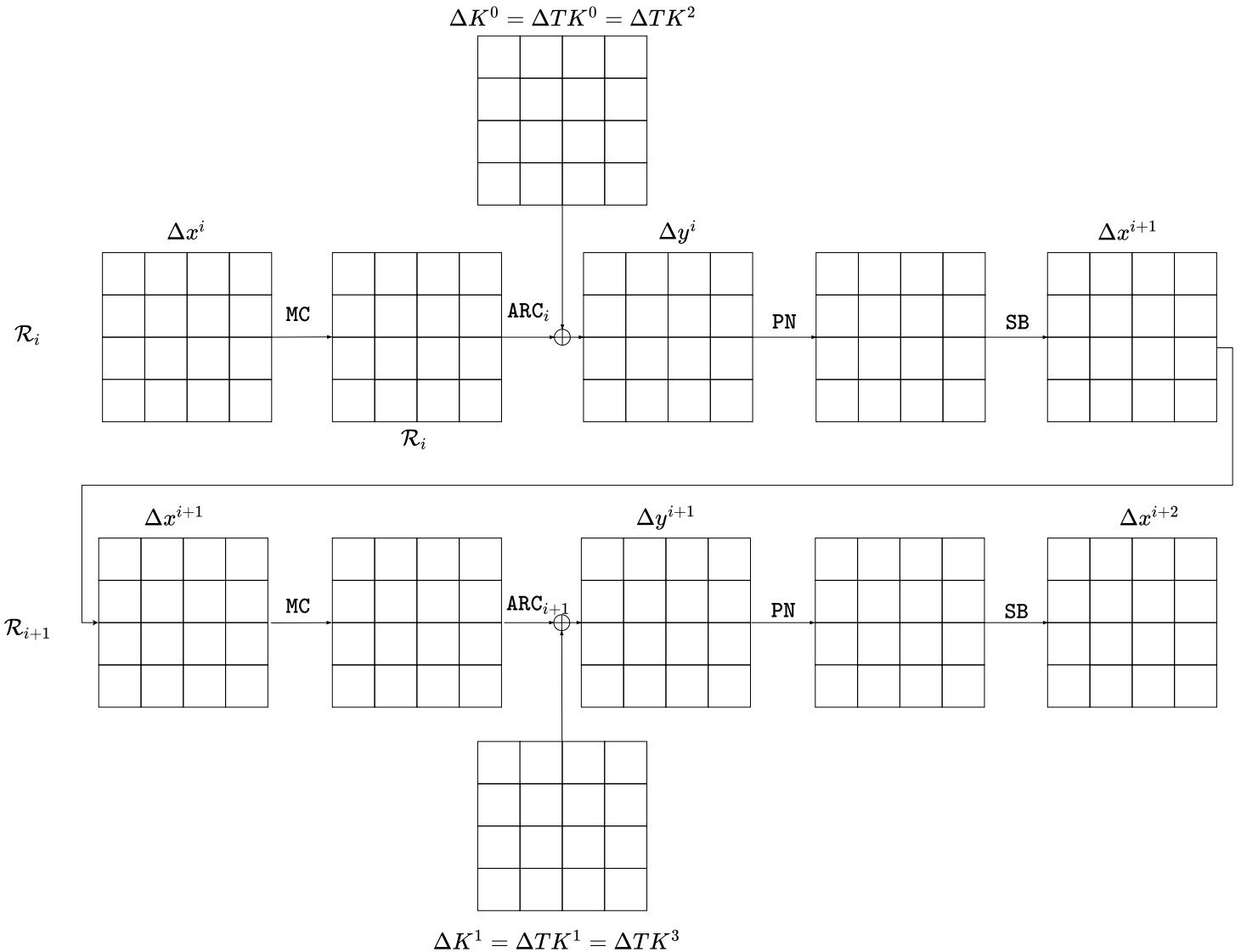
- Denote the state at the input and the output of round i of CRAFT by x^i and x^{i+1}
- Denote the state after MC, $\mathtt{ARC}_i$ and $\mathtt{ATK}_i$ operations by y^i

$$y^i = \mathtt{ATK}_i \circ \mathtt{ARC}_i \circ \mathtt{MC}(x^i)$$
$$x^{i+1} = \mathtt{SB} \circ \mathtt{PN}(y^i)$$

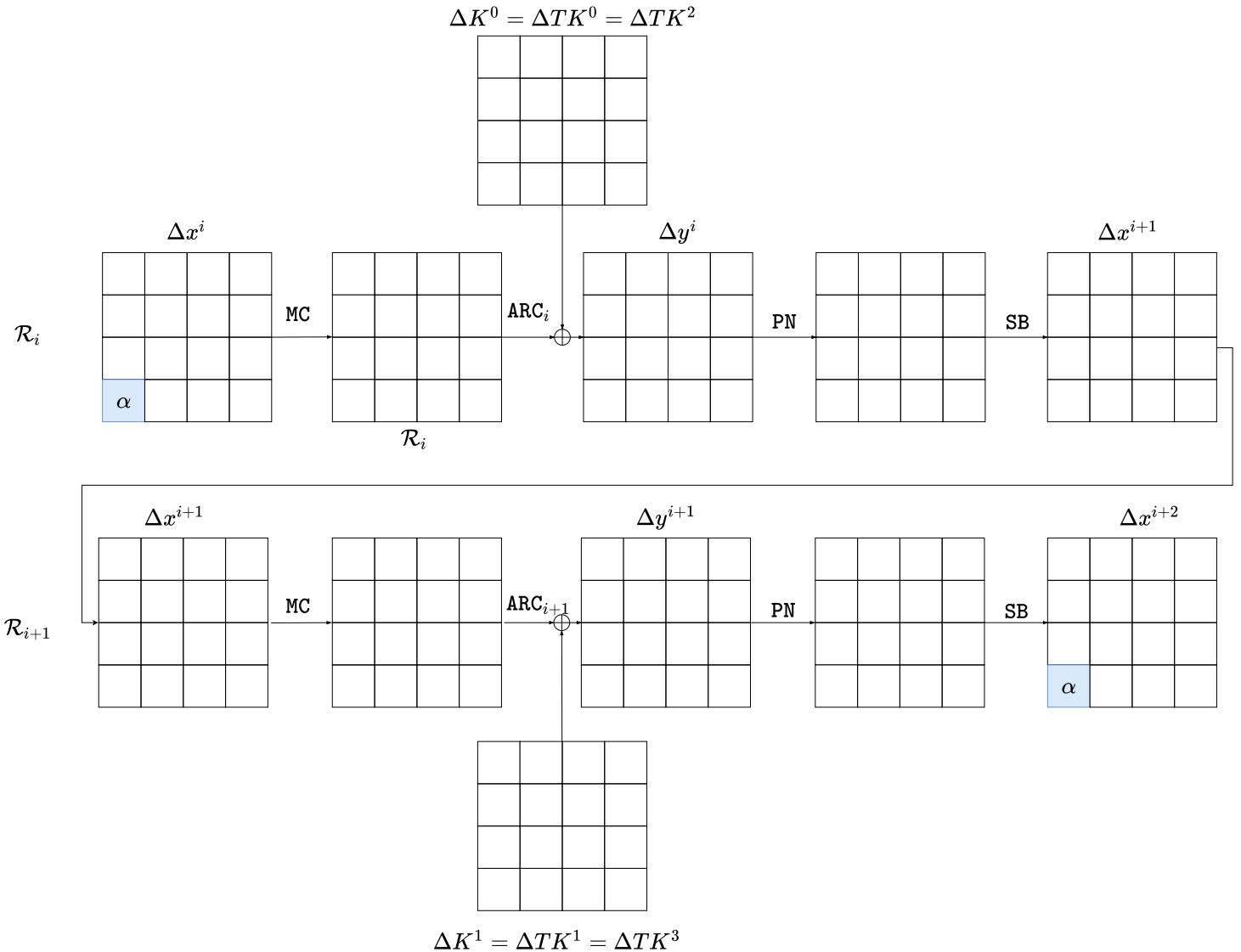
- In the related-key with a single tweak model of CRAFT, the tweak (T) has zero difference
- The subkeys (K^0, K^1) have the nonzero differences ΔK^0 and ΔK^1
- The four tweakeys have nonzero differences as follows:

$$\Delta TK^0 = \Delta TK^2 = \Delta K^0, \quad \Delta TK^1 = \Delta TK^3 = \Delta K^1$$

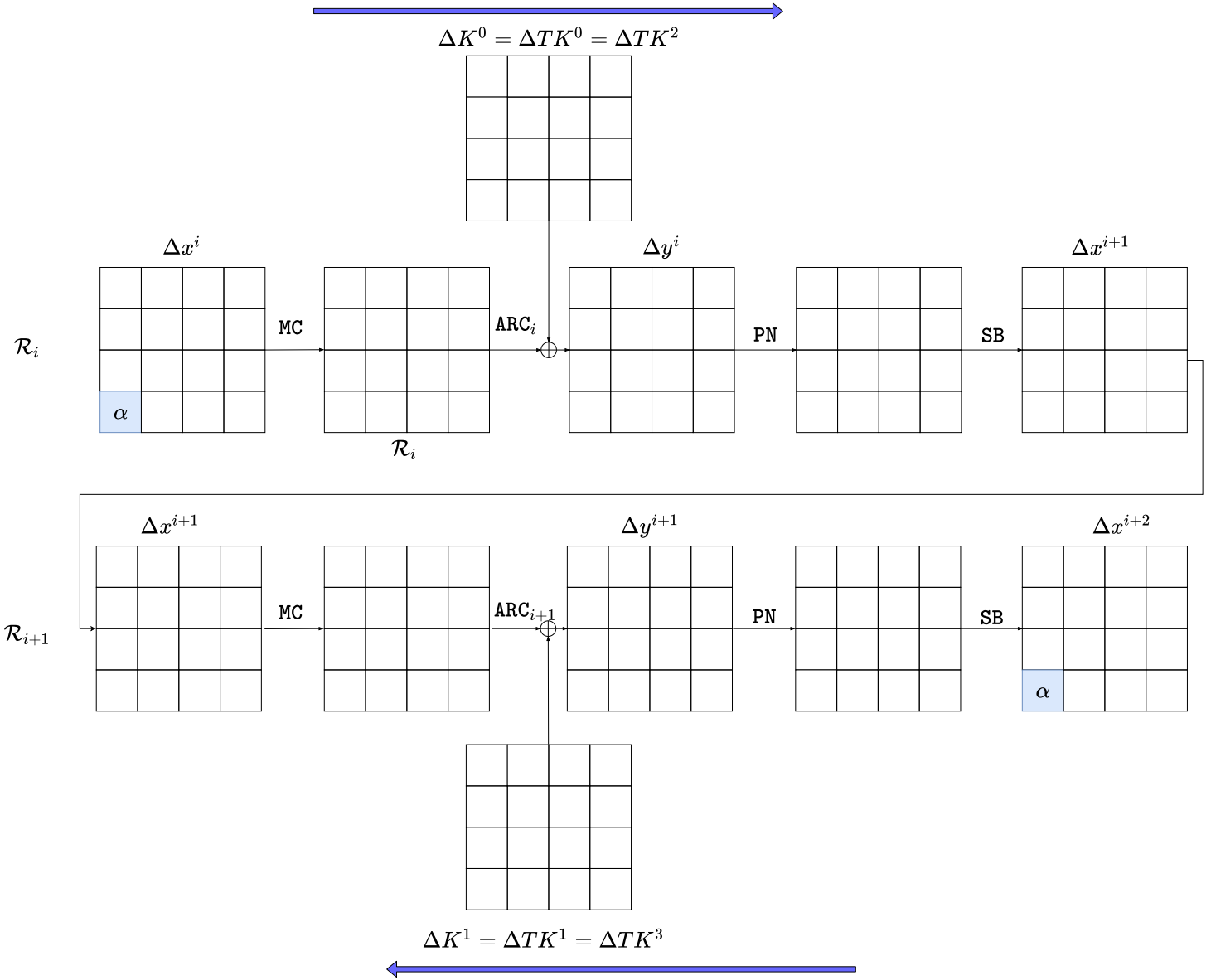
A 2-round Characteristic



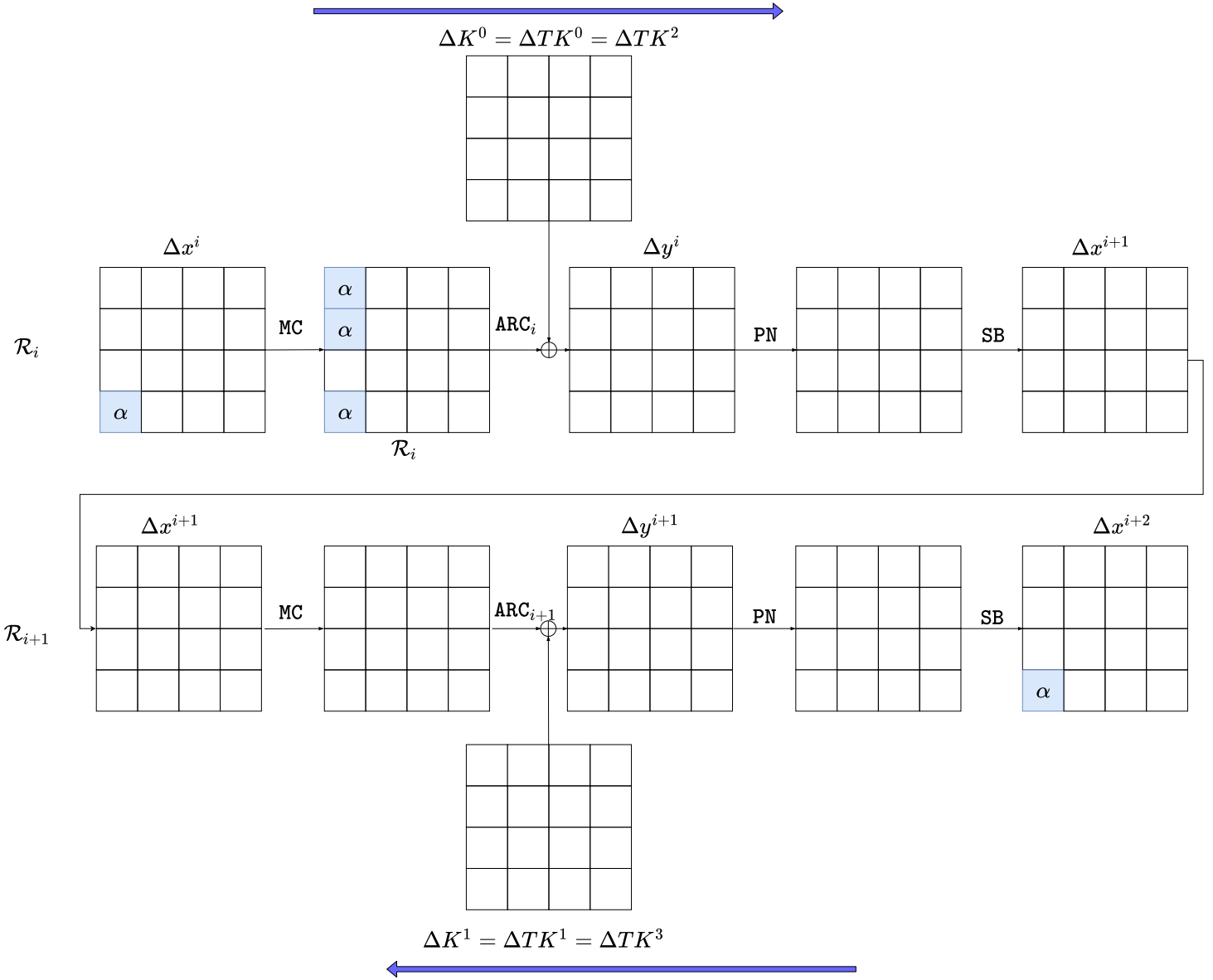
A 2-round Characteristic



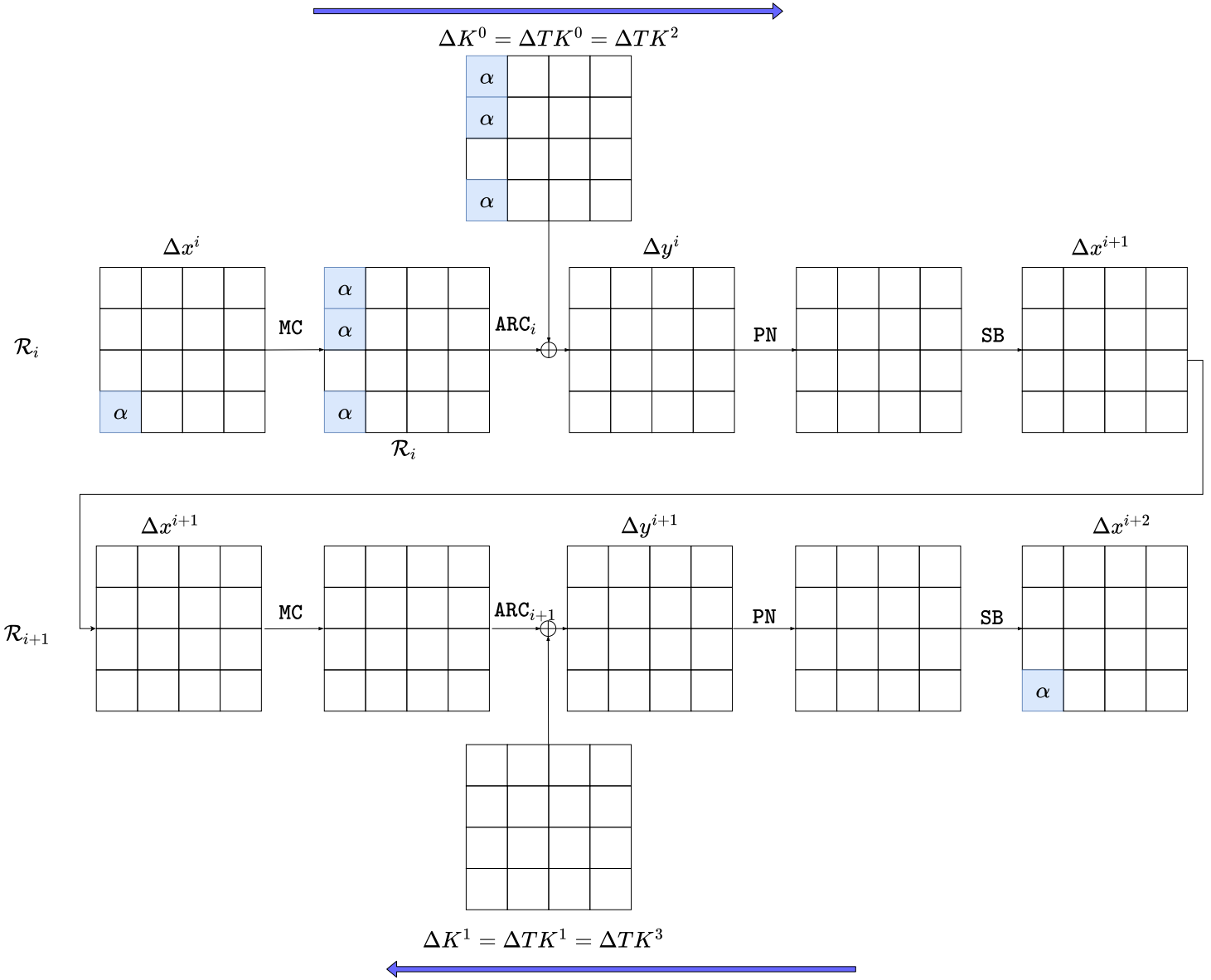
A 2-round Characteristic



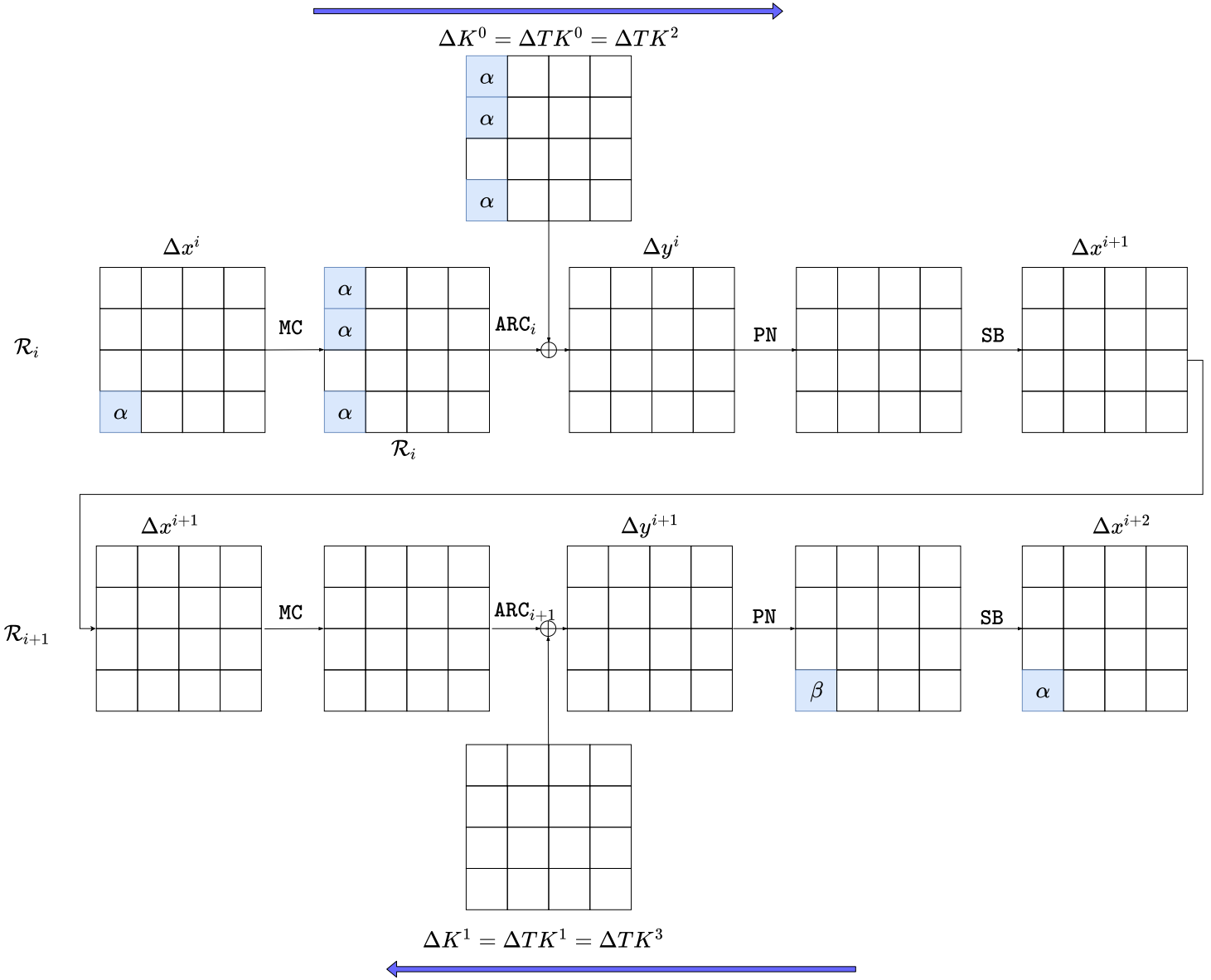
A 2-round Characteristic



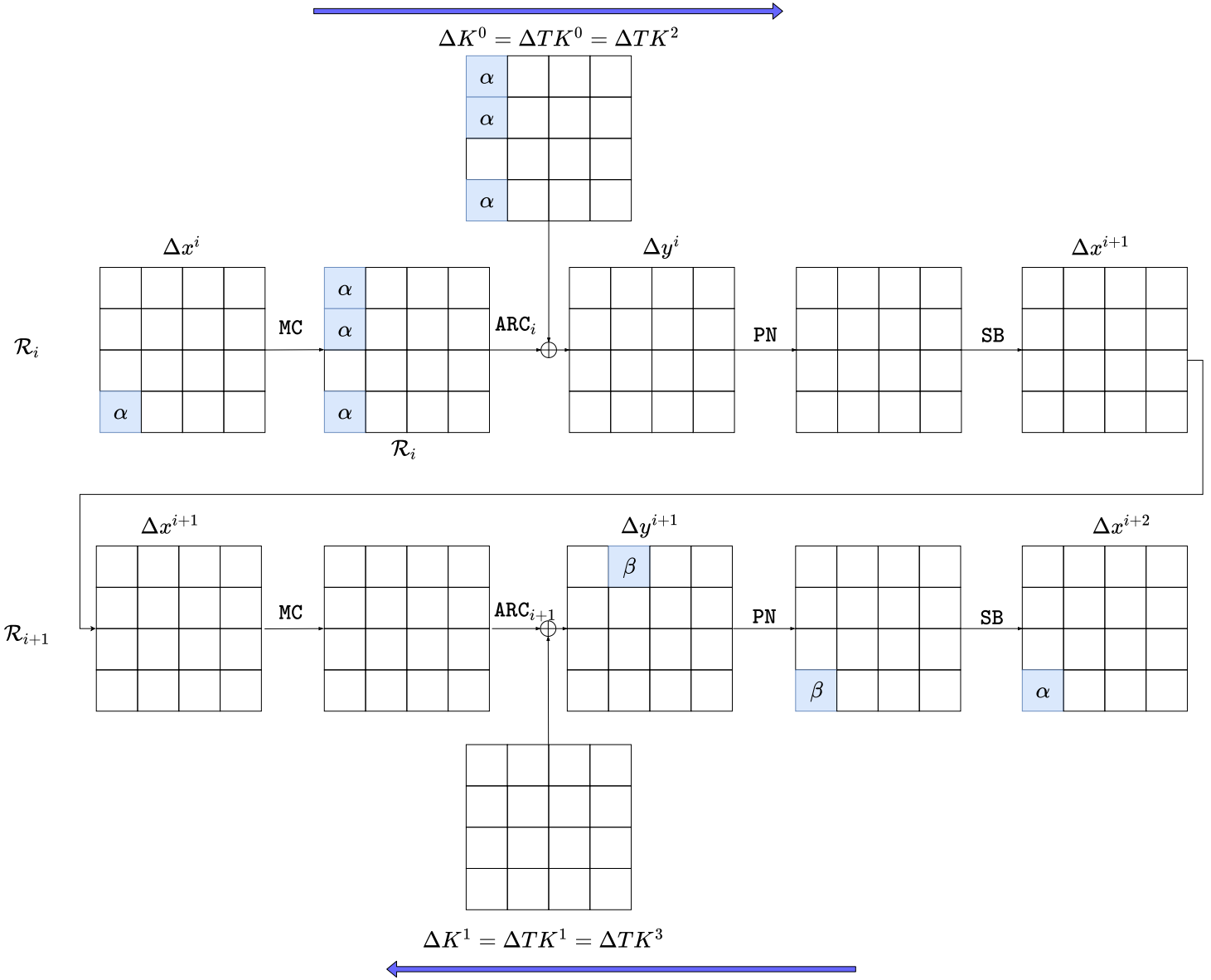
A 2-round Characteristic



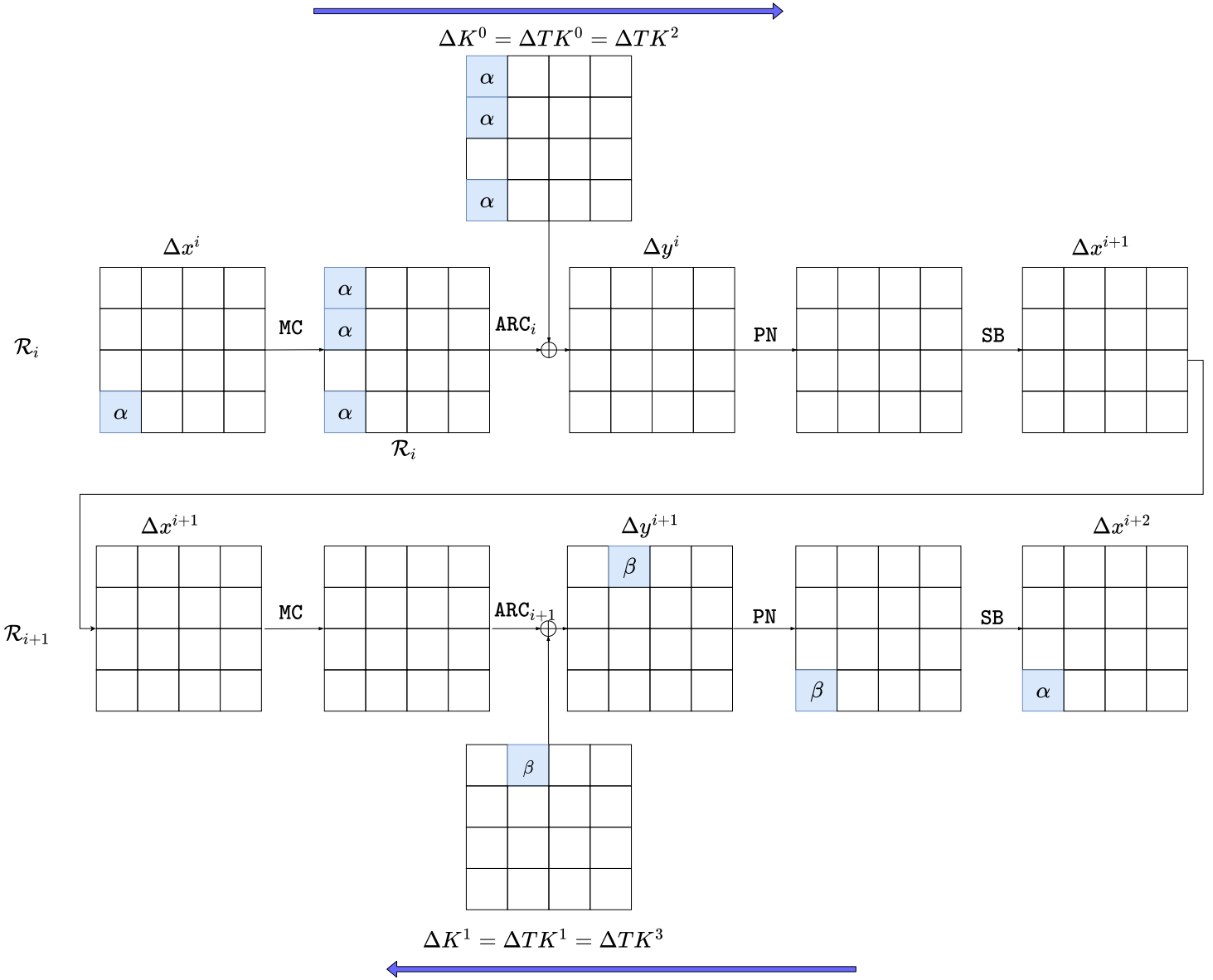
A 2-round Characteristic



A 2-round Characteristic



A 2-round Characteristic



Values of α and β

- $\Pr[\mathtt{SB}^{-1}(\alpha) \rightarrow \beta] = \Pr[\mathtt{SB}(\beta) \rightarrow \alpha] = p$
- The overall probability of this characteristic depends on the values of α and β.
- We select the value of the tuple (α, β) so that p is equal to the maximum differential probability for an active Sbox which is 2^{-2}
- Based on the differential distribution table (DDT) of the CRAFT's Sbox, the unordered tuples (α, β) can take one of the values from the following set:

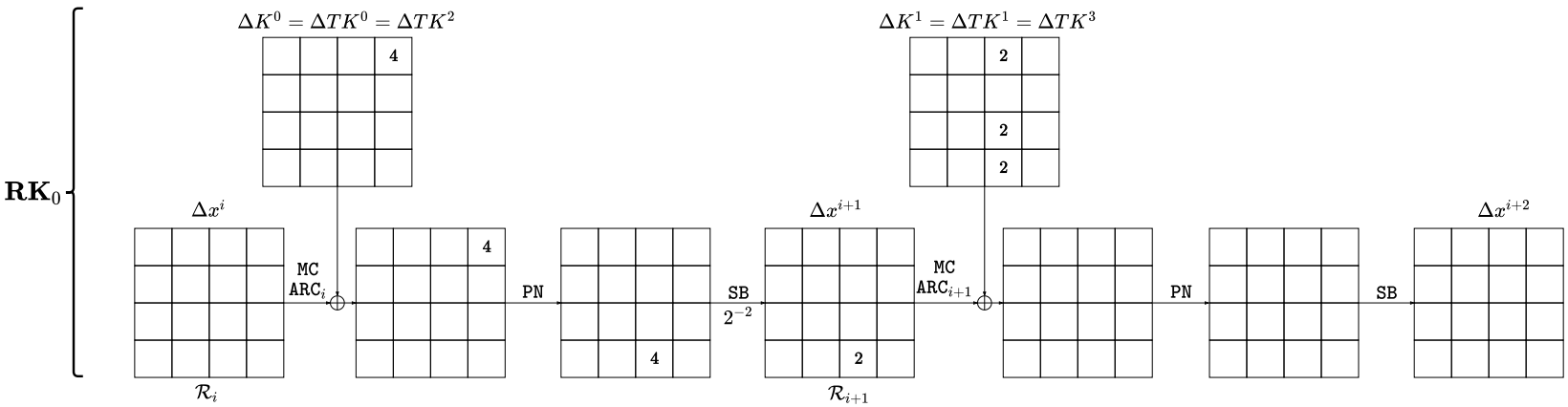
$$(\alpha, \beta) \text{ or } (\beta, \alpha) \in \{(1,2),(2,4),(2,9),(2,c),(3,6),(5,7),(5,a),(7,d),(a,a),(a,d),(a,f),(b,b),(e,e),(f,f)\}.$$

Repeatable 2-round related-key differential

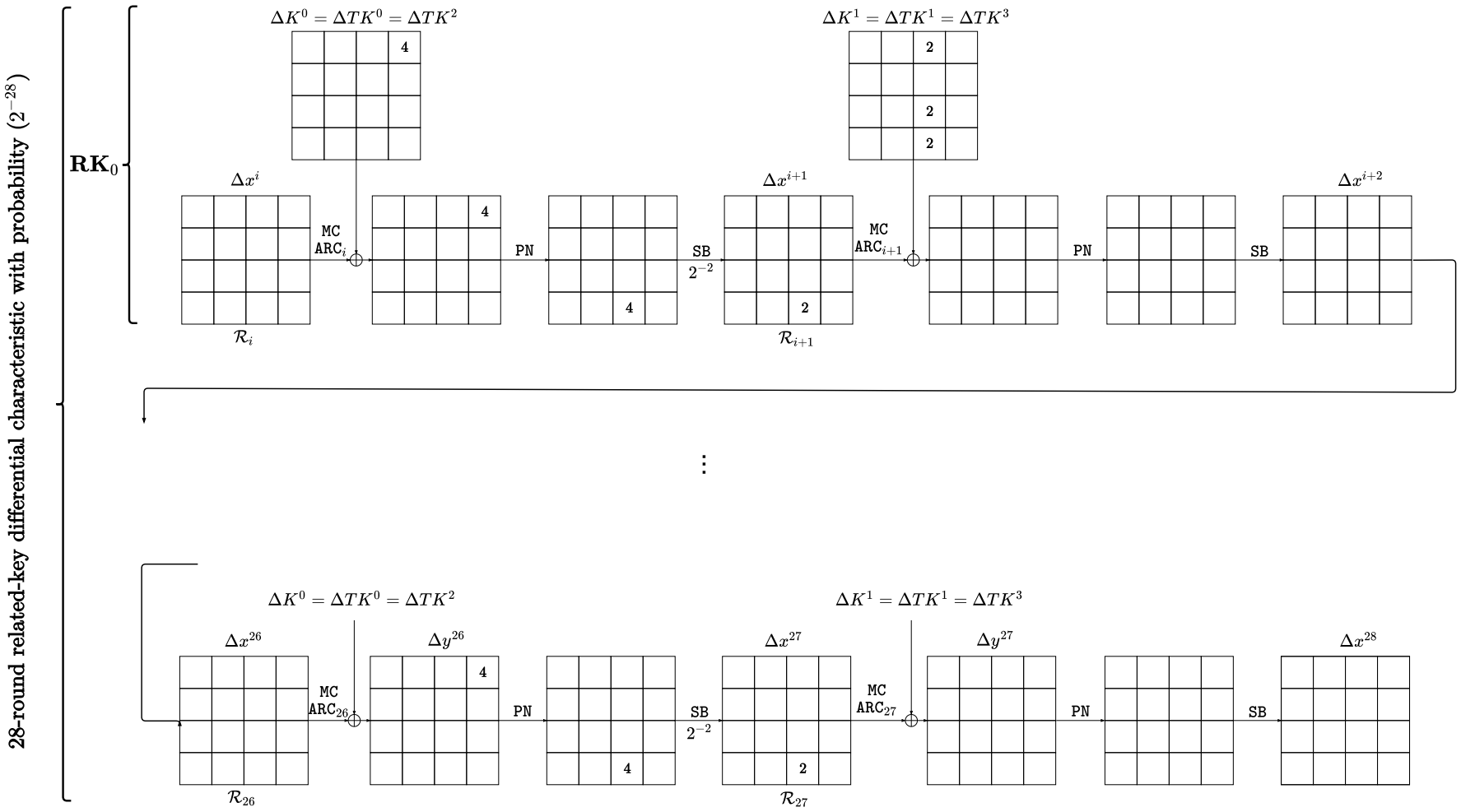
	$\Delta K^0 = \Delta TK^0 = \Delta TK^2$	$\Delta K^1 = \Delta TK^1 = \Delta TK^3$	$\Delta x^i = \Delta x^{i+2}$
$\mathbf{RK}_0$	$(0,0,0,\alpha,0,0,0,0,0,0,0,0,0,0,0,0)$	$(0,0,\beta,0,0,0,\beta,0,0,0,0,0,0,0,\beta,0)$	$(0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0)$
$\mathbf{RK}_1$	$(\alpha,0,0,0,\alpha,0,0,0,0,0,0,0,\alpha,0,0,0)$	$(0,\beta,0,0,0,0,0,0,0,0,0,0,0,0,0,0)$	$(0,0,0,0,0,0,0,0,0,0,0,0,\alpha,0,0,0)$
$\mathbf{RK}_2$	$(0,\alpha,0,0,0,\alpha,0,0,0,0,0,0,0,\alpha,0,0)$	$(0,0,\beta,0,0,0,0,0,0,0,0,0,0,0,0,0)$	$(0,0,0,0,0,0,0,0,0,0,0,0,0,\alpha,0,0)$
$\mathbf{RK}_3$	$(0,0,\alpha,0,0,0,\alpha,0,0,0,0,0,0,0,\alpha,0)$	$(0,0,0,\beta,0,0,0,0,0,0,0,0,0,0,0,0)$	$(0,0,0,0,0,0,0,0,0,0,0,0,0,0,\alpha,0)$
$\mathbf{RK}_4$	$(0,0,0,\alpha,0,0,0,\alpha,0,0,0,0,0,0,0,\alpha)$	$(\beta,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0)$	$(0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,\alpha)$
$\mathbf{RK}_5$	$(\alpha,0,0,0,0,0,0,0,\alpha,0,0,0,0,0,0,0)$	$(0,0,0,0,0,0,\beta,0,0,0,0,0,0,0,0,0)$	$(0,0,0,0,0,0,0,0,\alpha,0,0,0,0,0,0,0)$
$\mathbf{RK}_6$	$(0,\alpha,0,0,0,0,0,0,0,\alpha,0,0,0,0,0,0)$	$(0,0,0,0,0,\beta,0,0,0,0,0,0,0,0,0,0)$	$(0,0,0,0,0,0,0,0,0,\alpha,0,0,0,0,0,0)$
$\mathbf{RK}_7$	$(0,0,\alpha,0,0,0,0,0,0,0,\alpha,0,0,0,0,0)$	$(0,0,0,0,\beta,0,0,0,0,0,0,0,0,0,0,0)$	$(0,0,0,0,0,0,0,0,0,0,\alpha,0,0,0,0,0)$
$\mathbf{RK}_8$	$(0,0,0,\alpha,0,0,0,0,0,0,0,\alpha,0,0,0,0)$	$(0,0,0,0,0,0,0,\beta,0,0,0,0,0,0,0,0)$	$(0,0,0,0,0,0,0,0,0,0,0,\alpha,0,0,0,0)$
$\mathbf{RK}_9$	$(0,0,0,0,\alpha,0,0,0,0,0,0,0,0,0,0,0)$	$(0,0,0,0,0,0,0,0,0,0,\beta,0,0,0,0,0)$	$(0,0,0,0,\alpha,0,0,0,0,0,0,0,0,0,0,0)$
$\mathbf{RK}_{10}$	$(0,0,0,0,0,\alpha,0,0,0,0,0,0,0,0,0,0)$	$(0,0,0,0,0,0,0,0,0,\beta,0,0,0,0,0,0)$	$(0,0,0,0,0,\alpha,0,0,0,0,0,0,0,0,0,0)$
$\mathbf{RK}_{11}$	$(0,0,0,0,0,0,\alpha,0,0,0,0,0,0,0,0,0)$	$(0,0,0,0,0,0,0,0,\beta,0,0,0,0,0,0,0)$	$(0,0,0,0,0,0,\alpha,0,0,0,0,0,0,0,0,0)$
$\mathbf{RK}_{12}$	$(0,0,0,0,0,0,0,\alpha,0,0,0,0,0,0,0,0)$	$(0,0,0,0,0,0,0,0,0,0,0,\beta,0,0,0,0)$	$(0,0,0,0,0,0,0,\alpha,0,0,0,0,0,0,0,0)$
$\mathbf{RK}_{13}$	$(\alpha,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0)$	$(0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,\beta)$	$(\alpha,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0)$
$\mathbf{RK}_{14}$	$(0,\alpha,0,0,0,0,0,0,0,0,0,0,0,0,0,0)$	$(0,0,0,0,0,0,0,0,0,0,0,0,\beta,0,0,0)$	$(0,\alpha,0,0,0,0,0,0,0,0,0,0,0,0,0,0)$
$\mathbf{RK}_{15}$	$(0,0,\alpha,0,0,0,0,0,0,0,0,0,0,0,0,0)$	$(0,0,0,0,0,0,0,0,0,0,0,0,0,\beta,0,0)$	$(0,0,\alpha,0,0,0,0,0,0,0,0,0,0,0,0,0)$
$\mathbf{RK}_{16}$	$(0,0,0,\alpha,0,0,0,0,0,0,0,0,0,0,0,0)$	$(0,0,0,0,0,0,0,0,0,0,0,0,0,0,\beta,0)$	$(0,0,0,\alpha,0,0,0,0,0,0,0,0,0,0,0,0)$

Outline

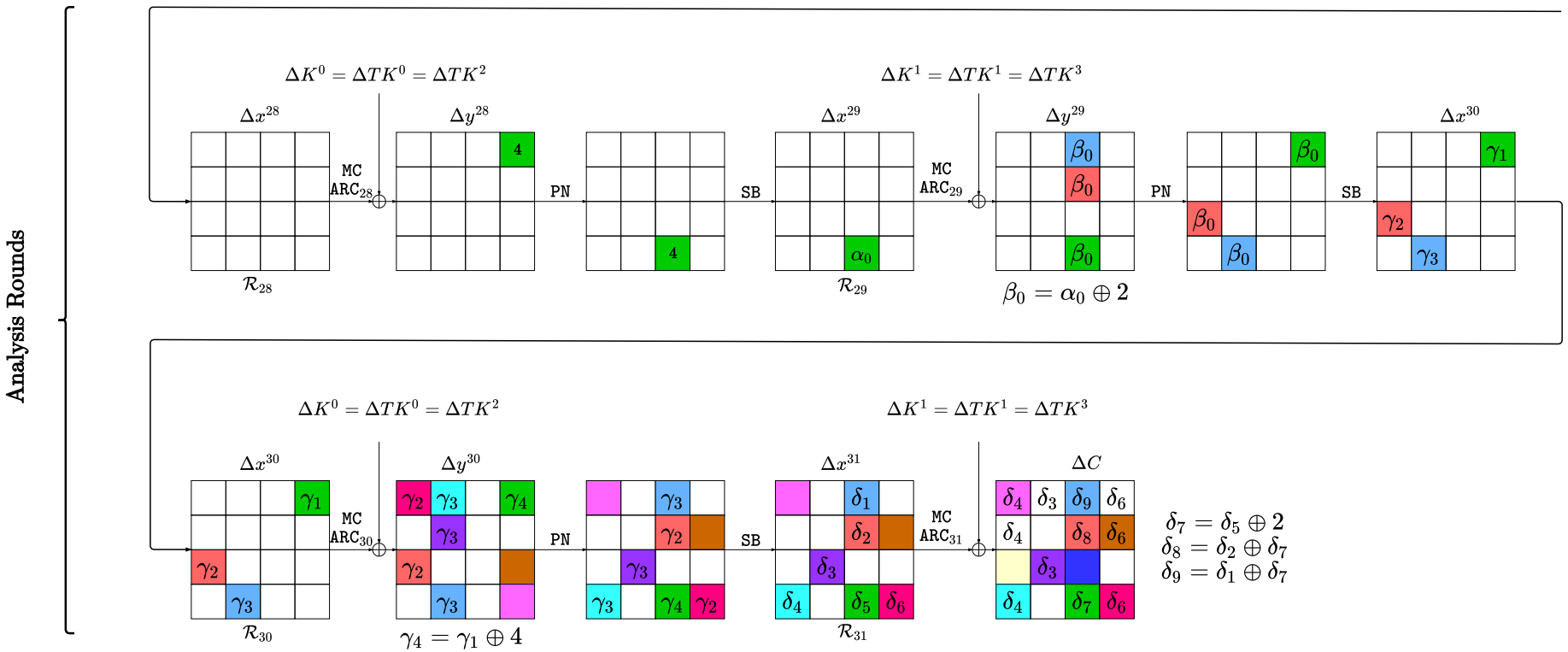
28-round Related-key Differential Characteristic



28-round Related-key Differential Characteristic



4-round Analysis



$$\Delta C = (\delta_4, \delta_3, \delta_9, \delta_6, \delta_4, 0, \delta_8, \delta_6, 0, \delta_3, 0, 0, \delta_4, 0, \delta_7, \delta_6).$$

Attack Details

- Data Collection:
  - Collect $2^m = 4 \times p^{-1} = 4 \times 2^{28} = 2^{30}$ pairs of plaintexts/ciphertexts using 2^{31} plaintext.
  - Filter out the pairs that do not satisfy the conditions on the differences of the ciphertext.
  - The probability of satisfying these conditions is 2^{-40}. This means that the right pairs only pass this filtration.

Attack Details

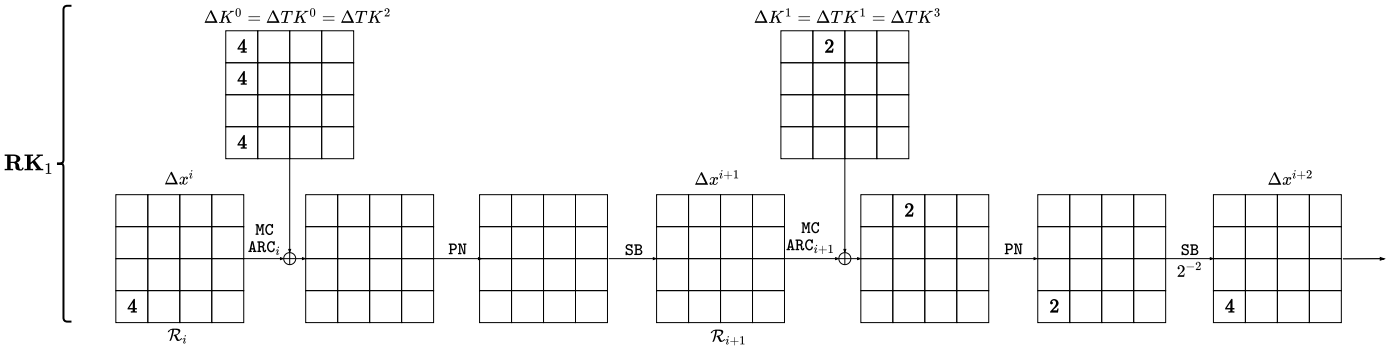
- Data Collection:
  - Collect $2^m = 4 \times p^{-1} = 4 \times 2^{28} = 2^{30}$ pairs of plaintexts/ciphertexts using 2^{31} plaintext.
  - Filter out the pairs that do not satisfy the conditions on the differences of the ciphertext.
  - The probability of satisfying these conditions is 2^{-40}. This means that the right pairs only pass this filtration.
- Key Recovery:
  - Since there are 44 bits of the key involved in the analysis, we recover only 44 bits using this distingusiher.
  - We perform the exhaustive search over the remaining 2^{84} keys using 2 plaintext/ciphertext pairs.

Outline

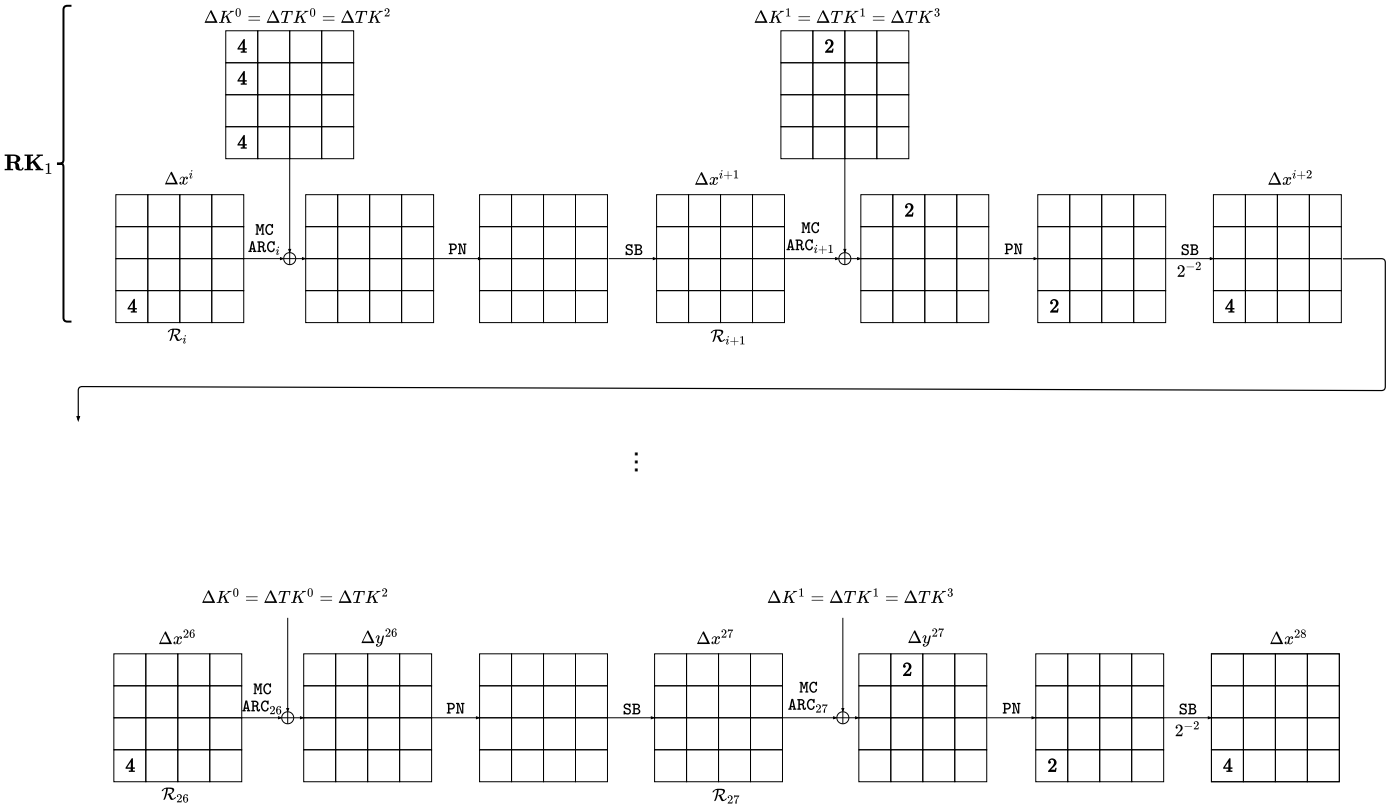
30-round Related-key Differential Characteristics

- We employ the repeatable 2-round characteristics ($\mathbf{RK}_1$ – $\mathbf{RK}_8$) with the tuple $(\alpha, \beta) = (4, 2)$ in order to build eight 30-round characteristics as follows.
- First, we repeat each $\mathbf{RK}_i$ $(1 \leq i \leq 8)$ 14 times to build a 28-round characteristic with probability $(2^{-2})^{14} = 2^{-28}$.
- Then, we append another 2 rounds with probability of (2^{-2}). Thus, we are able to construct a 30-round characteristic with total probability (p) of 2^{-30}.
- We use these characteristics one by one to collect 8 datasets $(\mathcal{D}_i, 1 \leq i \leq 8)$ and then apply a partial-key recovery process to determine a part of the master secret key.

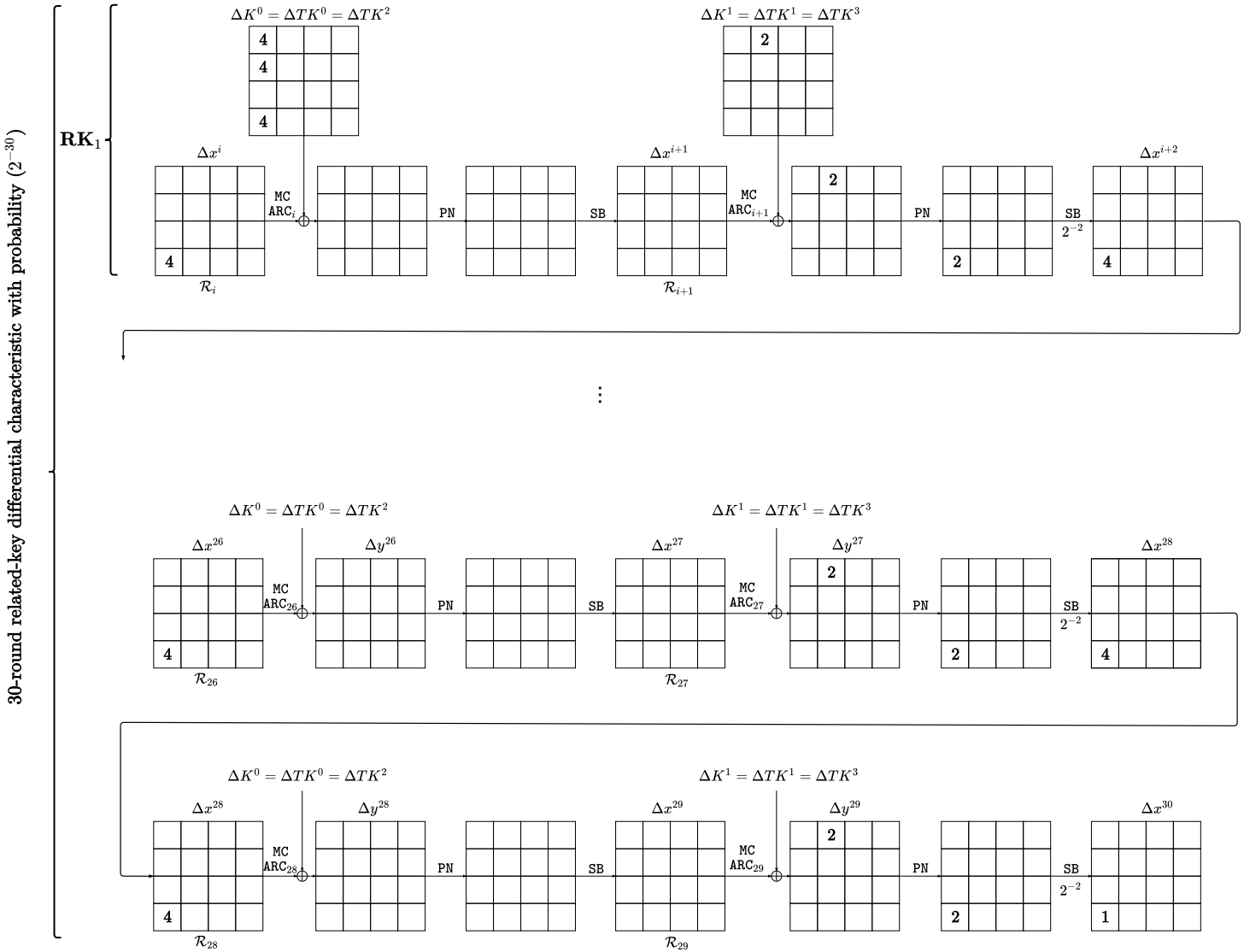
30-round Characteristic using $\mathbf{RK}_1$ ($\mathcal{D}_1$)



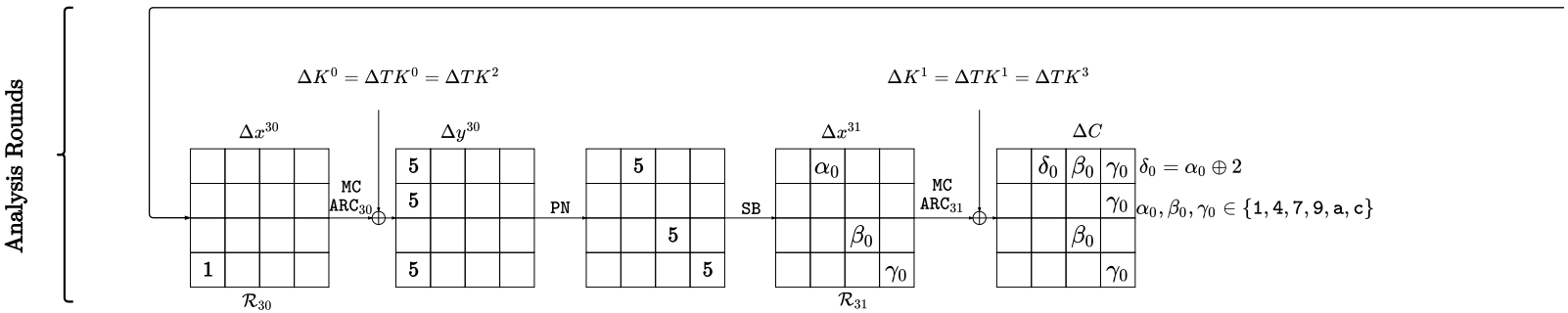
30-round Characteristic using $\mathbf{RK}_1$ ($\mathcal{D}_1$)



30-round Characteristic using $\mathbf{RK}_1$ ($\mathcal{D}_1$)



2-round Analysis using $\mathbf{RK}_1$ ($\mathcal{D}_1$)



$$\Delta C = (0, \delta_0, \beta_0, \gamma_0, 0, 0, 0, \gamma_0, 0, 0, \beta_0, 0, 0, 0, 0, \gamma_0).$$

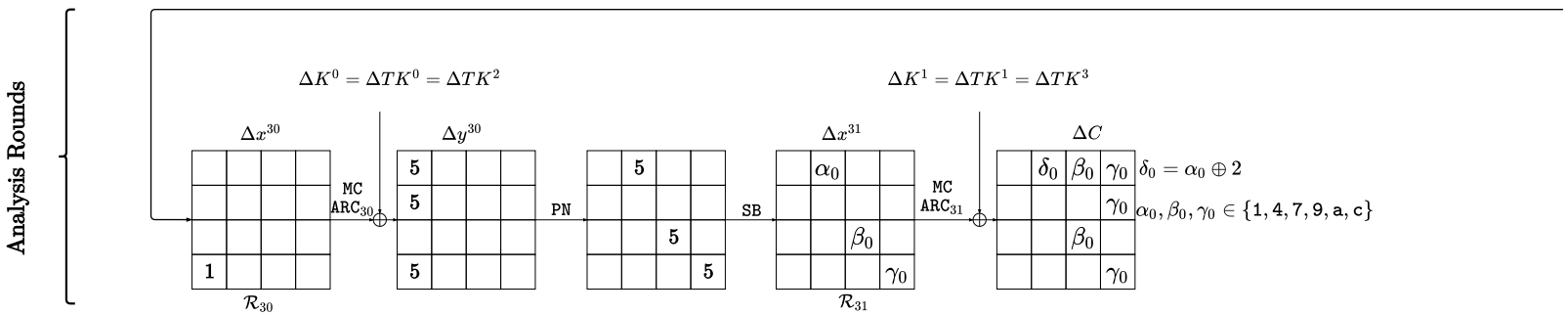
where $\delta_0 = \alpha_0 \oplus 2$ and based on the DDT of CRAFT Sbox, $\alpha_0, \beta_0, \gamma_0 \in \{0, 4, 7, 9, a, c\}$.

$$\Delta C_i = 0, \ i \in \{0, 4, 5, 6, 8, 9, 11, 12, 13, 14\}, \quad \Delta C_1 = \delta_0,$$
$$\Delta C_2 = \Delta C_{10} = \beta_0, \qquad \Delta C_3 = \Delta C_7 = \Delta C_{15} = \gamma_0.$$

Key Recovery-First Stage

Goal: Recover $K^1_8, K^1_9, K^1_{10}, K^1_{11}, K^1_{12}, K^1_{13}, K^1_{14}, K^1_{15}$.

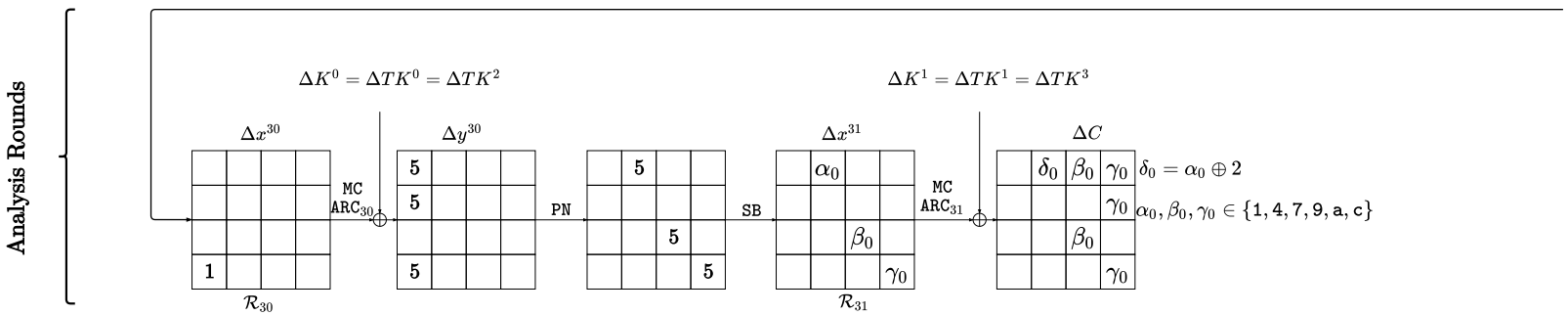
Example: Determine the right value of K^1_{11} and K^1_{15} using $\mathcal{D}_1$.



Key Recovery-Second Stage

Goal: Recover $K_0^1, K_1^1, K_2^1, K_3^1, K_{12}^0, K_{13}^0, K_{14}^0, K_{15}^0$.

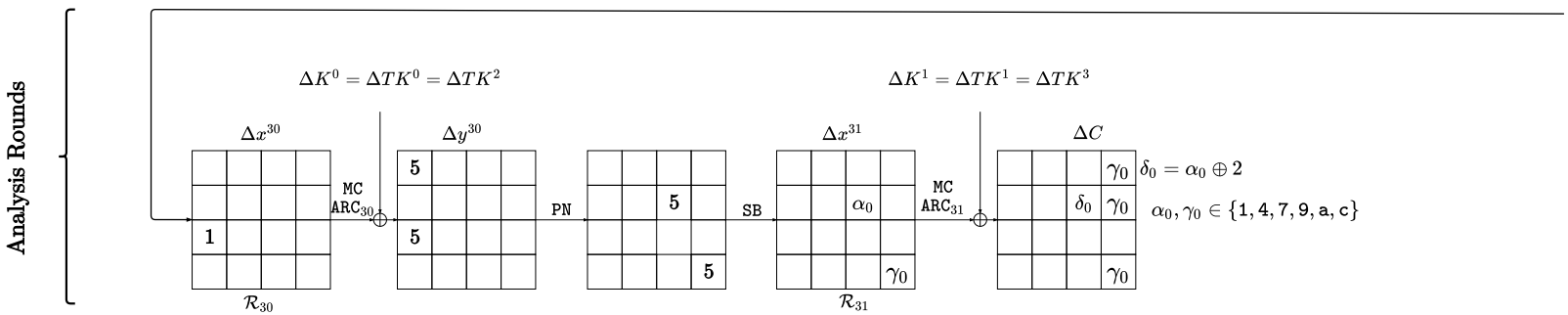
Example: Determine the right value of K_1^1 and K_{12}^0 using $\mathcal{D}_1$.



Key Recovery-Third Stage

Goal: Recover $K_4^1, K_5^1, K_6^1, K_7^1, K_8^0, K_9^0, K_{10}^0, K_{11}^0$.

Example: Determine the right value of K_6^1 and K_8^0 using $\mathcal{D}_5$.



Key Recovery

- First Stage(8 nibbles): $K_8^1, K_9^1, K_{10}^1, K_{11}^1, K_{12}^1, K_{13}^1, K_{14}^1, K_{15}^1$.
- Second Stage(8nibbles): $K_0^1, K_1^1, K_2^1, K_3^1, K_{12}^0, K_{13}^0, K_{14}^0, K_{15}^0$.
- Third Stage (8 nibbles): $K_4^1, K_5^1, K_6^1, K_7^1, K_8^0, K_9^0, K_{10}^0, K_{11}^0$.
- Run exhaustive search over the remaining 2^{32} keys using 2 plaintext/ciphertext pairs.

Omitting the Exhaustive Search Step

Goal: Recover $K_0^0, K_1^0, K_2^0, K_3^0, K_4^0, K_5^0, K_6^0, K_7^0$.

- We utilize the repeatable 2-round characteristics $\mathbf{RK}_9$ – $\mathbf{RK}_{16}$ to build another 8 30-round characteristics and collect another 8 datasets $(\mathcal{D}_i, 9 \leq i \leq 16)$.
- We use the same technique as in the second and the third stages.

Outline

Conclusion I

1. 2-round characteristics

Conclusion I

1. 2-round characteristics
   - We have presented a systematic method of how to construct a repeatable 2-round characteristic (the input difference is the same as the output difference) with only one active Sbox and holds with probability equals to the maximum differential probability of an active Sbox of CRAFT (2^{-2}).

Conclusion I

1. 2-round characteristics
   - We have presented a systematic method of how to construct a repeatable 2-round characteristic (the input difference is the same as the output difference) with only one active Sbox and holds with probability equals to the maximum differential probability of an active Sbox of CRAFT (2^{-2}).
   - To illustrate the effectiveness of this method, we have presented 17 repeatable 2-round characteristics.

Conclusion I

1. 2-round characteristics
   - We have presented a systematic method of how to construct a repeatable 2-round characteristic (the input difference is the same as the output difference) with only one active Sbox and holds with probability equals to the maximum differential probability of an active Sbox of CRAFT (2^{-2}).
   - To illustrate the effectiveness of this method, we have presented 17 repeatable 2-round characteristics.
2. Related-key Differential Attack using single difference

Conclusion I

1. 2-round characteristics
   - We have presented a systematic method of how to construct a repeatable 2-round characteristic (the input difference is the same as the output difference) with only one active Sbox and holds with probability equals to the maximum differential probability of an active Sbox of CRAFT (2^{-2}).
   - To illustrate the effectiveness of this method, we have presented 17 repeatable 2-round characteristics.
2. Related-key Differential Attack using single difference
   - We have extended one of these characteristics to a 28-round related-key differential characteristic with probability 2^{-28}.

Conclusion I

1. 2-round characteristics
   - We have presented a systematic method of how to construct a repeatable 2-round characteristic (the input difference is the same as the output difference) with only one active Sbox and holds with probability equals to the maximum differential probability of an active Sbox of CRAFT (2^{-2}).
   - To illustrate the effectiveness of this method, we have presented 17 repeatable 2-round characteristics.
2. Related-key Differential Attack using single difference
   - We have extended one of these characteristics to a 28-round related-key differential characteristic with probability 2^{-28}.
   - After that, we have employed it to mount a key recovery attack on full-round CRAFT using 2^{31} queries to the encryption oracle and 2^{86} encryptions.

Conclusion II

3. Related-key Differential Attack using multiple differences

Conclusion II

3. Related-key Differential Attack using multiple differences
   - We have speed up the key recovery attack against the full-round CRAFT using $2^{35.17}$ queries to the encryption oracle and 2^{32} full-round encryptions.

Conclusion II

3. Related-key Differential Attack using multiple differences
   - We have speed up the key recovery attack against the full-round CRAFT using $2^{35.17}$ queries to the encryption oracle and 2^{32} full-round encryptions.
   - To this end, we manage to use 8 different related-key differential characteristics (with 8 related-key differences).

Conclusion II

3. Related-key Differential Attack using multiple differences
   - We have speed up the key recovery attack against the full-round CRAFT using $2^{35.17}$ queries to the encryption oracle and 2^{32} full-round encryptions.
   - To this end, we manage to use 8 different related-key differential characteristics (with 8 related-key differences).
   - Furthermore, we can perform the previous attack without the exhaustive search step and recover the whole master key with $2^{36.09}$ queries to the encryption oracle and only 11 full-round encryptions (instead of 2^{32} in the above attack) using 16 different related-key differential characteristics (with 16 related-key differences).

Conclusion II

3. Related-key Differential Attack using multiple differences
   - We have speed up the key recovery attack against the full-round CRAFT using $2^{35.17}$ queries to the encryption oracle and 2^{32} full-round encryptions.
   - To this end, we manage to use 8 different related-key differential characteristics (with 8 related-key differences).
   - Furthermore, we can perform the previous attack without the exhaustive search step and recover the whole master key with $2^{36.09}$ queries to the encryption oracle and only 11 full-round encryptions (instead of 2^{32} in the above attack) using 16 different related-key differential characteristics (with 16 related-key differences).
   - This attack has been verified experimentally.

Thank You

For Questions: m_elshei@encs.concordia.ca