Journal of Computing and Security

Research Article, 2026, Volume 13, Number 2 (pp. 75–83)

http://www.jcomsec.org

Boomeyong Cryptanalysis of Reduced-Round mCrypton

Parsa Yousefpour [a], Atiyeh Mirzaie [b], Siavash Ahmadi [c,*] Mohammad Reza Aref [b]

[a] *Department of Electrical Engineering, Sharif University of Technology, Tehran, Iran.*

[b] *Information Systems and Security Lab (ISSL), Department of Electrical Engineering, Sharif University of Technology, Tehran, Iran.*

[c] *Electronics Research Institute, Sharif University of Technology, Tehran, Iran.*

ARTICLE INFO.

Article history:
Received: 06 December 2025
Revised: 28 June 2026
Accepted: 13 July 2026
Published Online: 22 September 2026

Keywords:
Boomerang, Yoyo, mCrypton, Distinguisher, Key Recovery.

ABSTRACT

Given the growing demand for secure yet lightweight encryption in constrained environments such as RFID tags and wireless sensor networks, resource-constrained devices are increasingly relying on lightweight block ciphers to protect sensitive data while meeting strict power, area, and latency requirements. In response to the challenge of designing such block ciphers, several lightweight block ciphers, such as mCrypton, have been proposed. However, a thorough security evaluation of such ciphers is crucial, since their vulnerabilities can threaten the entire security architecture of systems. In this paper, we present the first application of the boomeyong attack—a hybrid technique combining boomerang and yoyo frameworks—on the reduced-round mCrypton block cipher. We formulate a novel 5-round distinguisher and demonstrate a key recovery attack that improves upon all previously known results. By refining structural definitions and adapting the boomeyong framework to the SPN-based design of mCrypton, our attack achieves a data complexity of 2^{26}, a time complexity of $2^{23.02}$En. $+2^{25}$XOR, and a memory complexity of 2^{12} blocks.

1 Introduction

Boomerang cryptanalysis, introduced by Wagner in 1999 [1], is an effective method for analyzing block ciphers when high-probability differential characteristics are only available for a limited number of rounds. It leverages two short characteristics on subciphers instead of a single long one.

The original attack assumes statistical independence between the subciphers, a condition often violated in practice. To address this, Dunkelman et al. proposed the sandwich framework [2, 3], which models dependencies using a three-part cipher structure.

A key analytical tool in this context is the Boomerang Connectivity Table (BCT), introduced by Cid et al. in 2018 [4]. The BCT quantifies boomerang uniformity of S-boxes and has led to further studies on improved definitions [5], probabilistic modeling [6], and structural generalizations [7–9].

Automation has significantly advanced boomerang analysis. Delaune et al. [10] proposed the first automatic distinguisher construction using MILP and CP, removing the need to predefine internal layer bound-

* Corresponding author.

Email addresses: par.yousef123@sharif.ir (P. Yousefpour), atiyeh.mirzaie@ee.sharif.edu (A. Mirzaie), s.ahmadi@sharif.edu (S. Ahmadi), aref@sharif.edu (M. Aref)

https://dx.doi.org/10.22108/jcs.2026.147711.1189
ISSN: 2322-4460

aries. Later improvements included automated key recovery [11], refined BCT-based methods [12], and the hybrid "boomeyong" attack combining boomerang and yoyo techniques [13].

mCrypton is a lightweight block cipher designed specifically for resource-constrained environments such as RFID tags and wireless sensor networks [14]. Proposed by Lim and Korkishko in 2005, mCrypton is a variant of the original Crypton cipher, optimized for low-cost hardware implementations. It features a 64-bit block size and supports key sizes of 64, 96, or 128 bits. The cipher structure is based on a Substitution–Permutation Network (SPN). Due to its well-structured components, mCrypton has attracted attention for various cryptanalytic studies.

Our Contribution. In this paper, the following contributions are made:

- Proposing the revised boomeyong definitions and lemmas for mCrypton: Building a boomeyong distinguisher demands deriving lemmas corresponding to the cipher structure. To do so, we first updated the definitions to accommodate mCrypton Super-SBoxes and words (Definitions 3 and 4), and then derived Lemmas 1 to 3 to provide the probabilistic foundation of the 5-round mCrypton distinguisher. This development leads to the first application of the boomeyong framework on reduced-round mCrypton.
- Introducing a new 5-round key recovery attack superior to previous results of the same number of rounds: Building upon the proposed distinguisher, we introduce a key recovery procedure that achieves at least improved time and memory complexities relative to previously known results for the same number of rounds (Table 1). It is worth noting that while higher-round attacks already exist, providing a more efficient cryptanalysis is still inherently valuable because it enhances comprehension of the cipher's design and security margin. The source code for our implementation is also available at https://github.com/mirzaieatiyeh/mcrypton-boomeyong/.

The remainder of this paper is organized as follows. Section 2 introduces the necessary background on mCrypton, the boomerang attack, and the Yoyo framework. In Section 3, we describe the boomeyong attack comprehensively. Section 4 explains the construction of the 5-round distinguisher and key recovery attack. Finally, Section 5 concludes the paper.

2 Preliminaries

This section outlines the preliminaries for the paper. It begins with a concise overview of mCrypton, followed by brief explanations of the boomerang and yoyo attacks, along with key results.

2.1 mCrypton overview

mCrypton [14] is a 64-bit lightweight block cipher designed for resource-constrained devices like RFID tags and sensors. It processes data as a 4×4 nibble array and operates through four key transformations per round.

2.1.1 Basic Building Blocks

The primary components of mCrypton are briefly described below:

- **Nonlinear Substitution (γ):**
  - Uses four 4-bit S-boxes (S_0 to S_3) with $S_2 = S_0^{-1}$ and $S_3 = S_1^{-1}$
  - Applies S-boxes cyclically to i-th row/column (a 4-nibble word $a = (a_0, a_1, a_2, a_3)$):

$$\gamma_i(a) = (S_i(a_0), S_{i+1}(a_1), S_{i+2}(a_2), S_{i+3}(a_3)) \quad (1)$$

- **Bit Permutation (π):**
  - Column-wise mixing using XOR operations. Each component column permutation π is defined for nibble columns $a = (a_0, a_1, a_2, a_3)$ and $b = (b_0, b_1, b_2, b_3)$ by

$$b = \pi_i(a) \Leftrightarrow b_j = \bigoplus_{k=0}^{3} (m_{i+j+k \ mod 4}.a_k), \quad (2)$$

  with mask nibbles:

$$m_0 = 1110_2, m_1 = 1101_2, m_2 = 1011_2, m_3 = 0111_2 \quad (3)$$

- **Column-to-Row Transposition (τ):**
  - It proposes a simple matrix transposition:

$$B = \tau(A) \Leftrightarrow b_{ij} = a_{ji} \quad (4)$$

  - It is self-inverse: $\tau^{-1} = \tau$
- **Key Addition (σ_K):**
  - XOR operation with round key $K = (K[0], K[1], K[2], K[3])$:

$$B = \sigma_K(A) \Leftrightarrow B_r[i] = A_r[i] \oplus K[i] \quad 0 \le i \le 3 \quad (5)$$

2.1.2 Round Structure

The encryption round ρ_K and decryption round ρ_K^{-1} functions are defined as:

Table 1. 5 round Cryptanalysis Results of mCrypton.

Approach	Method	Data	Time	Memory	Reference
Integral / Truncated diff	Generalised δ set distinguisher	2^4 (one δ set)	-	-	[15]
Meet in the Middle	MITM using 5 round δ set	2^{48}	$2^{54.5}$ En	$2^{53.5}$	[15]
Boomeyong	**Boomeyong key recovery attack**	$\mathbf{2^{26}}$	$\mathbf{2^{23.02}}$**En+**$\mathbf{2^{25}}$**XOR**	$\mathbf{2^{12}}$	**this paper**

Figure 1. 4 Parallel mCrypton Super-SBox.

$$\rho_K = \sigma_K \circ \tau \circ \pi \circ \gamma, \tag{6a}$$

$$\rho_K^{-1} = \gamma^{-1} \circ \pi \circ \tau \circ \sigma_K \tag{6b}$$

with full encryption involving 12 rounds and an output transformation $\phi = \tau \circ \pi \circ \tau$.

2.1.3 Super-SBox

Here we introduce the concept of Super-SBox in the mCrypton block cipher, which is illustrated in Figure 1. Consider a row from the input state (four orange-colored nibbles). After applying the specified functions in Figure 1, those four nibbles align to the same four nibbles (first row); in other words, these four nibbles of output are only dependent on those specified four nibbles of input through 1.5 rounds. This is conceptualized as a Super-SBox with 16-bit input and 16-bit output.

2.1.4 Key Schedule for 64-Bit Keys

mCrypton has three key sizes: 64 bits, 96 bits, and 128 bits. We review the key schedule for the 64-bit one here.

- Encryption round keys: The key register U is initially set to K, after which the encryption round keys for rounds $r = 0, 1, \ldots, 12$ are computed as follows:

$$T \leftarrow S(U[0]) \oplus C[r], \quad T_i \leftarrow T.M_i \quad (0 \le i \le 3), \tag{7}$$

$$K_e^r \leftarrow (U[1] \oplus T_0, U[2] \oplus T_1, U[3] \oplus T_2, U[0] \oplus T_3) \tag{8}$$

$$U \leftarrow (U[1], U[2], U[3], U[0]^{\lll 3}) \tag{9}$$

- Decryption round keys: The key register V is first initialized as

$$V \leftarrow (K[0]^{\lll 9}, K[1]^{\lll 9}, K[2]^{\lll 9}, K[3]^{\lll 9}). \tag{10}$$

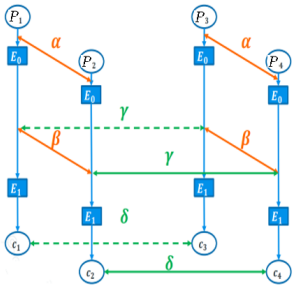


Figure 2. Conventional Boomerang Distinguisher [4].

The decryption round keys are then computed sequentially for each round $r = 0, 1, \ldots, 12$ as follows:

$$T \leftarrow S(V[0]) \oplus C[12 - r], \quad T_i \leftarrow T.M_i \quad (0 \le i \le 3), \tag{11}$$

$$K_d^r \leftarrow (\phi_0(V[1] \oplus T_0), \phi_1(V[2] \oplus T_1), \phi_2(V[3] \oplus T_2), \phi_3(V[0] \oplus T_3)) \tag{12}$$

$$V \leftarrow (V[3]^{\lll 13}, V[0], V[1], V[2]) \tag{13}$$

2.2 Boomerang Attack

The boomerang attack, introduced by Wagner [1], is an extension of differential cryptanalysis. It constructs a distinguisher for a block cipher by combining two differential trails. The attack divides the cipher into two parts: an upper part E_0 and a lower part E_1, each with corresponding differential trails referred to as the *upper trail* and *lower trail*, respectively.

Consider a cipher E decomposed into $E = E_1 \circ E_0$. Let the probabilities of the differential trails be $\Pr[\alpha \xrightarrow{E_0} \beta] = p$ and $\Pr[\gamma \xrightarrow{E_1^{-1}} \delta] = q$. For simplicity, assume $p = q = 1$ initially. The boomerang attack proceeds as follows (Figure 2):

(1) Choose plaintexts P^1 and P^2 such that $P^1 \oplus P^2 = \alpha$.
(2) Encrypt them to obtain ciphertexts $C^1 = E(P^1)$ and $C^2 = E(P^2)$.
(3) Construct ciphertexts $C^3 = C^1 \oplus \delta$ and $C^4 = C^2 \oplus \delta$.
(4) Decrypt them to obtain $P^3 = E^{-1}(C^3)$ and $P^4 = E^{-1}(C^4)$.
(5) Check if $P^3 \oplus P^4 = \alpha$.

When $p = q = 1$, this holds deterministically because: $E_0(P^1) \oplus E_0(P^2) = \beta$ (upper trail), $E_1^{-1}(C^1) \oplus E_1^{-1}(C^3) = \gamma$ and $E_1^{-1}(C^2) \oplus E_1^{-1}(C^4) = \gamma$ (lower trail).

Let $Q^i = E_0(P^i) = E_1^{-1}(C^i)$. Then:

$$Q^1 \oplus Q^2 = \beta \tag{14a}$$

$$Q^1 \oplus Q^3 = Q^2 \oplus Q^4 = \gamma. \tag{14b}$$

By combining these differences:

$$Q^3 \oplus Q^4 = (Q^1 \oplus Q^2) \oplus (Q^1 \oplus Q^3) \oplus (Q^2 \oplus Q^4) = \beta, \tag{15}$$

which implies $P^3 \oplus P^4 = \alpha$ due to the upper trail. For arbitrary p and q, the probability of this event is p^2q^2, assuming independence between the trails.

Enhancements: S-box Switch and Ladder Switch

Biryukov and Khovratovich [16] improved the boomerang attack by introducing dependencies between the upper and lower trails via *s-box switch* and *ladder switch* techniques.

Assume the last substitution layer in E_0 partitions the state into t parts, such that $Q^i = Q_0^i \| Q_1^i \| \dots \| Q_{t-1}^i, \beta = \beta_0 \| \beta_1 \| \dots \| \beta_{t-1}$, and $\gamma = \gamma_0 \| \gamma_1 \| \dots \| \gamma_{t-1}$.

Let S denote the substitution layer, and let $S^{-1}(Q_k^1) \oplus S^{-1}(Q_k^2) = \phi_k$ for the k-th partition. The probability of $\phi_k \xrightarrow{S} \beta_k$ is q'_k.

Two special cases optimize the trail probability:

(1) **S-box Switch**: If $\gamma_k = \beta_k$, then:

$$Q_k^3 = Q_k^2 \quad \text{and} \quad Q_k^4 = Q_k^1. \tag{16}$$

This satisfies $S^{-1}(Q_k^3) \oplus S^{-1}(Q_k^4) = \phi_k$ deterministically, improving the probability by a factor of q'_k.

(2) **Ladder Switch**: If $\gamma_k = 0$, then:

$$Q_k^3 = Q_k^1 \quad \text{and} \quad Q_k^4 = Q_k^2. \tag{17}$$

Here, $S^{-1}(Q_k^3) \oplus S^{-1}(Q_k^4) = \phi_k$ always holds, improving the probability by $q_{k'}^2$.

2.3 Yoyo Attack

The yoyo game is a cryptanalytic technique first introduced by Biham et al. [17] to analyze the Skipjack cipher. This adaptive chosen-ciphertext/plaintext strategy identifies text pairs satisfying specific invariant properties. Ronjom et al. [18] later adapted this approach to construct deterministic distinguishers for generic 2-round Substitution-Permutation Networks (SPNs), which was subsequently applied to AES. We review the foundational definitions from [18]:

Definition 1 (Zero Difference Pattern (ZDP) [18]). For $\alpha \in \mathbb{F}_q^n$ where $q = 2^k$, define the zero indicator z_i as:

$$z_i = \begin{cases} 1 & \text{if } \alpha_i = 0, \\ 0 & \text{otherwise.} \end{cases} \tag{18}$$

The Zero Difference Pattern $\nu(\alpha) \in \mathbb{F}_2^n$ is:

$$\nu(\alpha) = (z_0, z_1, ..., z_{n-1}). \tag{19}$$

Definition 2 (Word Swapping [18]). Given $v \in \mathbb{F}_2^n$ and states $\alpha, \beta \in \mathbb{F}_q^n$, the swapped state $\rho^v(\alpha, \beta)$ is constructed as:

$$\rho^v(\alpha, \beta)_i = \begin{cases} \alpha_i & \text{if } v_i = 1, \\ \beta_i & \text{if } v_i = 0. \end{cases} \tag{20}$$

The Hamming weight $wt(v)$ determines the number of swapped words.

These definitions enable a deterministic distinguisher for 2-round SPNs (G_2):

Proposition 1 (Yoyo Distinguisher [18]). *Let $p^0, p^1 \in \mathbb{F}_q^n$ encrypt to $c^0 = G_2(p^0)$, $c^1 = G_2(p^1)$. For any $v \in \mathbb{F}_2^n$, construct:*

$$c'^0 = \rho^v(c^0, c^1), \quad c'^1 = \rho^v(c^1, c^0). \tag{21}$$

Then decryption preserves the ZDP:

$$\nu(G_2^{-1}(c'^0) \oplus G_2^{-1}(c'^1)) = \nu(p^0 \oplus p^1). \tag{22}$$

3 Boomeyong Attack

Rahman et al. [13] introduced a novel cryptanalytic technique combining boomerang and yoyo attacks, where a yoyo trail is embedded within a boomerang distinguisher. The core idea leverages the deterministic properties of yoyo games in the upper trail while using specially crafted differential trails in the lower half.

Let $E : \mathbb{F}_{2^k}^n \to \mathbb{F}_{2^k}^n$ be a block cipher partitioned into two segments: the upper trail E_0 and the lower trail E_1. The upper trail E_0 consists of the initial sequence of layers $S \circ L \circ S$, while the remainder of the cipher is denoted by E_1. Suppose we have four plaintexts P^1, P^2, P^3, P^4, encrypted under E to produce ciphertexts C^1, C^2, C^3, C^4, respectively. Let $Q^i = E_0(P^i)$ for $i = 1, 2, 3, 4$, representing the intermediate states at the output of E_0. The objective is to simulate the yoyo game on E_0.

If P^1 and P^2 form an input pair, then due to the yoyo principle, we have $\nu(P^1 \oplus P^2) = \nu(P^3 \oplus P^4)$. This implies that Q^3 and Q^4 can be generated by swapping certain words between Q^1 and Q^2, leading

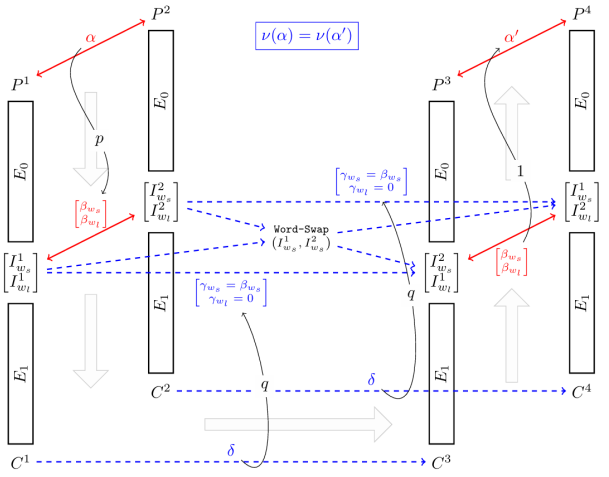


Figure 3. Boomeyong Distinguisher [13].

to the equality:

$$Q^1 \oplus Q^2 = Q^3 \oplus Q^4 = \beta.$$

Let $\alpha = P^1 \oplus P^2$ and $\alpha' = P^3 \oplus P^4$. The distinguishing factor between the classic boomerang attack and the approach presented here lies in their constraints: boomerang requires $\alpha = \alpha'$, whereas in this method, equality of Hamming weights suffices, i.e., $\nu(\alpha) = \nu(\alpha')$, though $\alpha \neq \alpha'$ may hold.

The construction of the lower trail is similar to that in boomerang attacks. Define $Q^1 \oplus Q^3 = \gamma$, which implies $Q^2 \oplus Q^4 = \gamma$ as well. To complete the trail in the lower part, we must construct a differential path satisfying $\delta \xrightarrow{E_1^{-1}} \gamma$. Importantly, to enable the word swapping at the boundary between E_0 and E_1, a specific relation must be established between β and γ.

Theorem 1 ([13]). Let $Q^1, Q^2, \gamma \in \mathbb{F}_{2^k}^n$ and $Q^1 \oplus Q^2 = \beta$. Consider, $Q^i = Q^i_1 || Q^i_2 || \cdots || Q^i_n$, $\beta = \beta_1 || \cdots || \beta_n$ and $\gamma = \gamma_1 || \cdots || \gamma_n$. If $J \subset \{1, \cdots, n\}$, $J \neq \emptyset$ and for all $j \in J$, $\gamma_j = \beta_j$; otherwise, $\gamma_j = 0$, then, $Q^1 \oplus \gamma$, $Q^2 \oplus \gamma$ can be formed by swapping words between Q^1, Q^2.

According to Theorem 1, each word in γ must either be zero or match the corresponding word in β. This condition guarantees that a word-swapping has occurred at the interface between the upper and lower parts of the cipher, allowing the yoyo game to proceed within the E_0 layer. The Boomeyong distinguisher is illustrated in Figure 3.

In the upper trail E_0, the exact value of α is not predetermined; rather, its Hamming weight $\nu(\alpha)$ is fixed. Let the probability that a difference with weight t maps through E_0 to β be denoted by $\Pr[\{\alpha \mid \nu(\alpha) = t\} \xrightarrow{E_0} \beta] = p$, and the likelihood of reaching γ through the inverse of the lower trail be $\Pr[\delta \xrightarrow{E_1^{-1}} \gamma] = q$.

Consequently, with probability pq^2, the intermediate values Q^3 and Q^4 can be obtained by permuting certain words between Q^1 and Q^2, preserving the condition $\nu(P^3 \oplus P^4) = \nu(P^1 \oplus P^2)$. Denote this fixed weight by $t = wt(\nu(P^1 \oplus P^2))$. If E behaves like a uniform random permutation, then the probability of such an event occurring is 2^{-tk}. Therefore, when incorporating the yoyo strategy into a boomerang distinguisher, it is essential to select upper and lower trails such that the condition $pq^2 > 2^{-tk}$ holds.

3.1 Attack Idea

The following steps outline the construction of a distinguisher by embedding the yoyo principle within a boomerang. Assume access to an oracle $\mathbf{O}$, which is either the cipher E or a uniformly random permutation. The goal is to determine the nature of $\mathbf{O}$.

(1) Select two plaintexts P^1 and P^2 such that $wt(\nu(P^1 \oplus P^2))$, equals a predefined value t. Query the oracle $\mathbf{O}$ to obtain the corresponding ciphertexts C^1 and C^2.
(2) Construct ciphertexts $C^3 = C^1 \oplus \delta$ and $C^4 = C^2 \oplus \delta$, then decrypt them via oracle $\mathbf{O}$ to retrieve the corresponding plaintexts P^3 and P^4.
(3) Check if $\nu(P^3 \oplus P^4) = \nu(P^1 \oplus P^2)$.
(4) If the equality holds, identify $\mathbf{O}$ as the cipher E. If not, repeat steps 1–3 up to $\frac{1}{pq^2}$ times. If no such quartet (P^1, P^2, P^3, P^4) is found after all repetitions, conclude that $\mathbf{O}$ is a random permutation.

4 Boomeyong Attack on mCrypton

The Boomeyong cryptanalysis is applied to reduced-round mCrypton in this section; so we update the definitions and lemmas in [13] to match the mCrypton structure.

A key limitation of incorporating a yoyo structure beneath a boomerang trail is the loss of deterministic word swapping between ciphertexts. To address this, a probabilistic variant of the yoyo game is introduced. Before proceeding, we define some structural components of mCrypton states — namely, columns and rows. The notation $\subset_\phi$ denotes a non-empty proper subset and $S = \{0, 1, 2, 3\}$.

Definition 3. For a set $I \subset_\phi \{0, 1, 2, 3\}$, define the column positions as $\mathcal{C}_I = \{(i, j) : i \in S, j \in I\}$. For an mCrypton state X, the corresponding nibbles are denoted $\mathcal{C}_I(X)$.

Definition 4. For a set $I \subset_\phi \{0, 1, 2, 3\}$, define the row positions as $\mathcal{R}_I = \{(i, j) : i \in I, j \in S\}$. For an mCrypton state X, the corresponding nibbles are

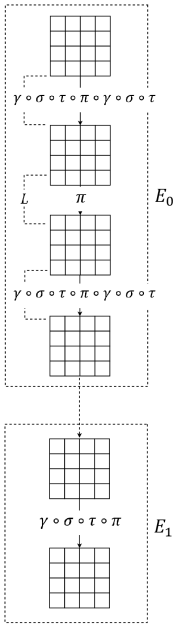


Figure 4. Partitioning 5-round mCrypton in E_0 and E_1.

denoted $\mathcal{R}_I(X)$.

The following two lemmas provide the probabilistic foundation for swapping rows under certain column differences — a technique used to extend the attack across additional mCrypton rounds. For further details and proofs refer to [13].

Lemma 1. Let $I, J \subset_\phi \{0,1,2,3\}$, and $p^1, p^2 \in \mathbb{F}_{2^4}^{4\times 4}$. The probability that rows in J are swapped between p^1 and p^2, given that columns in I are swapped, is

$$P_{ID}(|I|,|J|) = 2^{-4\cdot(4(|I|+|J|)-2|I||J|)}.$$

Lemma 2. Let $p^1, p^2 \in \mathbb{F}_{2^4}^{4\times 4}$ and $c^1 = f(p^1)$, $c^2 = f(p^2)$, where $f = \gamma \circ \sigma \circ \tau \circ \pi$. The probability that swapping rows in c^1, c^2 corresponds to swapping those in p^1, p^2 is given by

$$P_{swap}(|I|) = \sum_{j=1}^{3} \binom{4}{j} P_{ID}(|I|, j).$$

The maximum value of $P_{\text{swap}}(|I|)$ occurs when $|I| = 1$, yielding approximately 2^{-23}.

4.1 Distinguishing Attack on 5-Round mCrypton

The proposed method is now applied to develop a distinguisher for 5-round mCrypton, which is further extended into a key recovery attack. The cipher is divided into two parts. Here, E_0 consists of an $S \circ L \circ S$ structure, where S is an mCrypton Super-Sbox and L represents the π. Figure 4 illustrates this partitioning.

By combining Proposition 1 and Lemma 2, a probabilistic yoyo distinguisher is constructed for 5-round mCrypton, embedding the yoyo technique within a boomerang framework.

Definition 5. Given a state $\alpha \in \mathbb{F}_{2^4}^{4\times 4}$ and a binary vector $v \in \mathbb{F}_2^4$, define $\tau^v(\alpha) \in \mathbb{F}_{2^4}^{4\times 4}$ such that for $0 \le i \le 3$,

$$\mathcal{R}_{\{i\}}(\tau^v(\alpha)) = \begin{cases} \mathcal{R}_{\{i\}}(\alpha), & \text{if } v_i = 0; \\ 0, & \text{otherwise.} \end{cases}$$

Lemma 3. *Let $p^1, p^2 \in \mathbb{F}_{2^4}^{4\times 4}$, and let $c^1 = R_5(p^1)$, $c^2 = R_5(p^2)$, where $R_5 = E_1 \circ E_0$ represents 5-round mCrypton. For any $v \in \mathbb{F}_2^4$ with $1 \le wt(v) \le 3$, define:*

$$c'^1 = c^1 \oplus \tau^v(c^1 \oplus c^2), \quad c'^2 = c^2 \oplus \tau^v(c^2 \oplus c^1),$$
$$p'^1 = R_5^{-1}(c'^1), \quad p'^2 = R_5^{-1}(c'^2).$$

Then, the equality $\nu(p^1 \oplus p^2) = \nu(p'^1 \oplus p'^2)$ holds with probability $P_{swap}(4 - wt(v))$.

Note that $P_{\text{swap}}(4 - wt(v))$ is maximized at approximately 2^{-23} when $wt(v) = 3$. This lemma is used to construct both the upper and lower trails of the distinguisher.

4.1.1 Upper Trail Construction

Plaintext pairs p^1, p^2 are selected such that $wt(\nu(p^1 \oplus p^2)) = 1$, i.e., only one active row. In the output difference β, six nibbles within the set $(\mathcal{C}_{\{3\}} \cup \mathcal{R}_{\{3\}}) \setminus (\mathcal{C}_{\{3\}} \cap \mathcal{R}_{\{3\}})$ remain inactive, which occurs with probability 2^{-24}. By considering single-element sets $J = \{0\}, \{1\}, \{2\}$, the overall success probability increases to 2^{-23}. Configurations with $|J| > 1$ are disregarded due to their negligible impact on the overall attack probability.

4.1.2 Lower Trail Construction

In the 5-round mCrypton structure, the lower trail partially relies on the outcome of the upper trail. Specifically, at least one word of γ must match the corresponding word in β. $\beta_3 = \gamma_3$, and the other words of γ are zero. To produce such a γ, the construction of δ must depend on the ciphertexts obtained from the upper trail:

$$\delta_i = \begin{cases} c_3^1 \oplus c_3^2, & \text{if } i = 3; \\ 0, & \text{otherwise.} \end{cases}$$

According to Definition 5, this matches the form $\delta = \tau^v(c^1 \oplus c^2)$. While $\delta \xrightarrow{E_1^{-1}} \gamma$ appears probabilistic in isolation, it becomes deterministic once β is fixed. Thus, the total probability of the attack remains 2^{-22}.

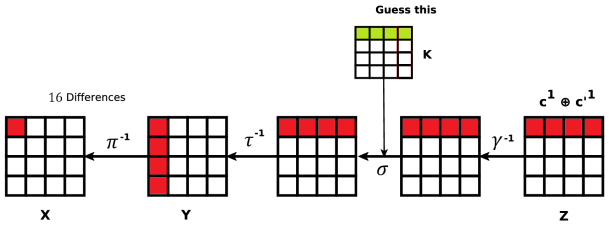


Figure 5. Key Recovery Attack on 5-round mCrypton.

4.1.3 Attack Procedure

(1) Construct a set of 2^{12} plaintexts $\{p^i\}$ such that all nibbles are constant except those on the first row, which vary across the set.
(2) For each i, query the encryption oracle with p^i to obtain the corresponding ciphertext c^i.
(3) For all pairs (i, j) with $0 \leq i < j < 2^{12}$, perform the following:
   (a) Construct the difference:
$$\delta_m = \begin{cases} c_3^i \oplus c_3^j, & m = 3; \\ 0, & \text{o.w.}, \end{cases} \text{ for } 0 \leq m \leq 3.$$
   (b) Compute modified ciphertexts:
$$c'^i = c^i \oplus \delta, \quad c'^j = c^j \oplus \delta.$$
   (c) Query the decryption oracle on c'^i, c'^j to obtain p'^i, p'^j.
   (d) Check if:
$$\nu(p^i \oplus p^j) = \nu(p'^i \oplus p'^j).$$
   If the condition holds, identify a valid quartet and conclude that the oracle behaves as a 5-round mCrypton.
(4) If no matching quartet is found after all comparisons, classify the oracle as a random permutation.

4.1.4 Complexity Analysis

The attack requires 2^{12} encryption queries and approximately 2^{24} decryption queries (due to $\binom{2^{12}}{2} \approx 2^{23}$ pairwise comparisons). Thus, the total data complexity is dominated by decryption queries. The time complexity is 2^{23} XOR operations, and memory usage is 2^{12} mCrypton states to store all ciphertexts.

4.2 Key Recovery Attack on 5-Round mCrypton

This attack extends the previously described distinguishing attack to extract key bits. Refer to Figure 5 for the key recovery attack. Assume a valid quartet (p^1, p^2, p'^1, p'^2) and their corresponding ciphertexts (c^1, c^2, c'^1, c'^2) have been identified by the distinguisher. Focus on the difference $Z = c^1 \oplus c'^1$, particularly the active nibbles. After applying γ^{-1}, the active nibbles are mapped into the first row. The attacker then guesses the first row of the round key K, and applies τ^{-1} to the affected nibbles.

Next, compute the difference in the intermediate state Y, and apply π^{-1}. The resulting difference is inspected in state X. If the difference in X is confined to a single nibble, the key guess is considered valid.

Since an active nibble in X can take 16 possible non-zero values, each row leads to approximately 2^4 candidate keys. Repeating this process for all four rows yields 2^{16} key candidates in total. Finally, an exhaustive search is performed over these 2^{16} possibilities to recover the correct round key.

The source code for our implementation is also available at https://github.com/mirzaieatiyeh/mcrypton-boomeyong/.

4.2.1 Complexity Analysis

Each row guess requires four valid quartets. Thus, the data and memory complexity are $4 \times 2^{24} = 2^{26}$ (adaptive chosen plaintext-ciphertext pairs) and 2^{12}(mCrypton states), respectively. Once a correct quartet is identified, one can generate 2^4 candidate keys for a single row using about $2^{16} \times 2$ one-round mCrypton encryptions. For all four columns:

$$2^{17} \text{ one-round mCrypton operations.}$$

Since each 5-round mCrypton encryption is equivalent to five one-round operations, this translates to:

$$\frac{2^{17}}{5} = 2^{14.5} \text{ full mCrypton encryptions.}$$

Step 3 of attack procedure needs $\binom{2^{12}}{2} \approx 2^{23}$ decryption queries. Also, an additional exhaustive search over the 2^{16} key candidates results in:

$$2^{16} \text{ mCrypton encryptions.}$$

Thus, the total time complexity is approximately:

$$2^{14.5} + 2^{23} + 2^{16} \approx 2^{23.02} \text{ mCrypton encryptions.}$$

Additionally, around 2^{25} XOR operations are needed, computed as:

$$4 \times 2^{23} = 2^{25}.$$

5 Conclusions

In this work, we presented the first application of the hybrid Boomeyong attack on reduced-round mCrypton. By refining the boomerang and yoyo frameworks and adapting them to the SPN-based structure of mCrypton, we were able to construct a new 5-round distinguisher and a key recovery attack. Our approach leverages updated structural definitions tailored to

mCrypton, resulting in significantly improved complexities compared to all previous cryptanalytic results on the same round-reduced version. The attack achieves a data complexity of 2^{26}, a time complexity of $2^{23.02}$ encryption calls plus 2^{25} XOR operations, and a memory complexity of 2^{12} blocks.

References

[1] David Wagner. The boomerang attack. In *International Workshop on Fast Software Encryption*, pages 156–170. Springer, 1999. doi:10.1007/3-540-48519-8_12.

[2] Orr Dunkelman, Nathan Keller, and Adi Shamir. A practical-time related-key attack on the kasumi cryptosystem used in gsm and 3g telephony. In *Annual cryptology conference*, pages 393–410. Springer, 2010. doi:10.1007/978-3-642-14623-7_22.

[3] Orr Dunkelman, Nathan Keller, and Adi Shamir. A practical-time related-key attack on the kasumi cryptosystem used in gsm and 3g telephony. *Journal of cryptology*, 27(4):824–849, 2014. doi:10.1007/s00145-013-9154-9.

[4] Claude Cid, Yosuke Huang, Thomas Peyrin, Yu Sasaki, and Ling Song. Boomerang connectivity table: A new cryptanalysis tool. In *EUROCRYPT*, pages 683–714, 2018. doi:10.1007/978-3-319-78375-8_22.

[5] Christina Boura and Anne Canteaut. On the boomerang uniformity of cryptographic sboxes. *IACR Transactions on Symmetric Cryptology*, pages 290–310, 2018. doi:10.13154/tosc.v2018.i3.290-310.

[6] Lei Hu, Ling Song, and Xianrui Qin. Boomerang connectivity table revisited. application to skinny and aes. *IACR Transactions on Symmetric Cryptology*, pages 118–141, 2019. doi:10.13154/tosc.v2019.i1.118-141.

[7] Haoyang Wang and Thomas Peyrin. Boomerang switch in multiple rounds. application to aes variants and deoxys. *IACR Transactions on Symmetric Cryptology*, pages 142–169, 2019. doi:10.13154/tosc.v2019.i1.142-169.

[8] Orr Dunkelman, Nathan Keller, Eyal Ronen, and Adi Shamir. The retracing boomerang attack. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 280–309. Springer, 2020. doi:10.1007/978-3-030-45721-1_11.

[9] Hamid Boukerrou, Paul Huynh, Virginie Lallemand, Bimal Mandal, and Marine Minier. On the feistel counterpart of the boomerang connectivity table. *IACR Transactions on Symmetric Cryptology*, 2020(1):331–362, 2020. doi:10.13154/tosc.v2020.i1.331-362.

[10] Stéphanie Delaune, Patrick Derbez, and Mathieu Vavrille. Catching the fastest boomerangs: Application to skinny. *IACR Transactions on Symmetric Cryptology*, pages 104–129, 2020. doi:10.46586/tosc.v2020.i4.104-129.

[11] Lingyue Qin, Xiaoyang Dong, Xiaoyun Wang, Keting Jia, and Yunwen Liu. Automated search oriented to key recovery on ciphers with linear key schedule: applications to boomerangs in skinny and forkskinny. *IACR Transactions on Symmetric Cryptology*, 2021(2):249–291, 2021. doi:10.46586/tosc.v2021.i2.249-291.

[12] Hosein Hadipour, Nasour Bagheri, and Ling Song. Improved rectangle attacks on skinny and craft. *IACR Transactions on Symmetric Cryptology*, pages 140–198, 2021. doi:10.46586/tosc.v2021.i2.140-198.

[13] Mostafizar Rahman, Dhiman Saha, and Goutam Paul. Boomeyong: Embedding yoyo within boomerang and its applications to key recovery attacks on aes and pholkos. *IACR Transactions on Symmetric Cryptology*, pages 137–169, 2021. doi:10.46586/tosc.v2021.i3.137-169.

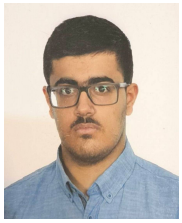
[14] Chae Hoon Lim and Tymur Korkishko. mcrypton–a lightweight block cipher for security of low-cost rfid tags and sensors. In *International workshop on information security applications*, pages 243–258. Springer, 2005. doi:10.1007/11604938_19.

[15] Bin Li, Jianhua Lu, Yingjiu Wang, and Amr M. Youssef. Improved meet-in-the-middle attacks on crypton and mcrypton. *IET Information Security*, 11(1):23–31, 2017. doi:10.1049/iet-ifs.2015.0335.

[16] Alex Biryukov, Dmitry Khovratovich, and Ivica Nikolić. Distinguisher and related-key attack on the full aes-256. In *Annual International Cryptology Conference*, pages 231–249. Springer, 2009. doi:10.1007/978-3-642-03356-8_14.

[17] Eli Biham, Alex Biryukov, Orr Dunkelman, Eran Richardson, and Adi Shamir. Initial observations on skipjack: Cryptanalysis of skipjack-3xor. In *International Workshop on Selected Areas in Cryptography*, pages 362–375. Springer, 1998. doi:10.1007/3-540-48892-8_27.

[18] Sondre Rønjom, Navid Ghaedi Bardeh, and Tor Helleseth. Yoyo tricks with aes. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 217–243. Springer, 2017. doi:10.1007/978-3-319-70694-8_8.



Parsa Yousefpoor received the B.Sc. degree in electrical engineering from Sharif University of Technology, Tehran, Iran, in 2025, and is currently pursuing the M.Sc. degree in electrical engineering at the same university. His research interests include cryptography and secure communication, with a current focus on lightweight block ciphers and symmetric-key cryptanalysis.

Atiyeh Mirzaie received the B.Sc. and M.Sc. degrees in electrical engineering from Sharif University of Technology, Tehran, Iran, in 2021 and 2023, respectively. She is currently a Ph.D. candidate in electrical engineering-communication systems and networks at Sharif University of Technology. Her main areas of research interest cover cryptography and secure communication with an emphasis on symmetric key cryptanalysis, automated attacks on block ciphers, and IoT security.

Siavash Ahmadi received the B.Sc., M.Sc., and Ph.D. degrees in electrical engineering from Sharif University of Technology, Tehran, Iran, in 2012, 2014, and 2020, respectively. He is currently an assistant professor at the Electronics Research Center at the Sharif University of Technology. His particular fields of interest include cryptology, wireless, cellular networks, the Internet of things, and artificial intelligence, with an emphasis on security.

Mohammad Reza Aref received the B.Sc. degree from the University of Tehran, Iran, in 1975, and the M.Sc. and Ph.D. degrees from Stanford University, Stanford, CA, USA, in 1976 and 1980, respectively, all in electrical engineering. He returned to Iran in 1980 and was actively engaged in academic affairs. From 1982 to 1995, he was a Faculty Member at the Isfahan University of Technology. He has been a professor of electrical engineering at the Sharif University of Technology, Tehran, since 1995 and a distinguished professor since 2013. He has published over 400 technical articles in communication, information theory, and cryptography in international journals and conferences. His current research interests include communication theory, information theory, cryptography, and statistical signal processing.