Switching the Top Slice of the Sandwich with Extra Filling Yields a Stronger Boomerang for NLFSR-based Block Ciphers

Amit Jana[1], Mostafizar Rahman[2], Dhiman Saha[3], Goutam Paul[1]

[1]Cryptology and Security Research Unit (CSRU),
R. C. Bose Centre for Cryptology and Security,
Indian Statistical Institute Kolkata
janaamit001@gmail.com,goutam.paul@isical.ac.in
[2]University of Hyogo
mrahman454@gmail.com
[3]de.ci.phe.red LAB,
Department of Computer Science & Engineering,
Indian Institute of Technology Bhilai
dhiman@iitbhilai.ac.in

Abstract. The Boomerang attack was one of the first attempts to visualize a cipher (E) as a composition of two sub-ciphers ($E_0 \circ E_1$) to devise and exploit two high-probability (say p, q) shorter trails instead of relying on a single low probability (say s) longer trail for differential cryptanalysis. The attack generally works whenever $p^2 \cdot q^2 > s$. However, it was later succeeded by the so-called "sandwich attack" which essentially splits the cipher in three parts $E_0' \circ E_m \circ E_1'$ adding an additional *middle* layer (E_m) with distinguishing probability of $p^2 \cdot r \cdot q^2$. It is primarily the generalization of a body of research in this direction that investigate what is referred to as the *switching* activity and capture the dependencies and potential incompatibilities of the layers that the middle layer separates. This work revisits the philosophy of the sandwich attack over multiple rounds for NLFSR-based block ciphers and introduces a new method to find high probability boomerang distinguishers. The approach formalizes boomerang attacks using only ladder/And switches. The cipher is treated as $E = E_m \circ E_1$, a specialized form of a sandwich attack which we called as the "open-sandwich attack". The distinguishing probability for this attack configuration is $r \cdot q^2$.

Using this innovative approach, the study successfully identifies a deterministic boomerang distinguisher for the keyed permutation of the TinyJambu cipher over 320 rounds. Additionally, a 640-round boomerang with a probability of 2^{-22} is presented with 95% success rate. In the related-key setting, we unveil full-round boomerangs with probabilities of 2^{-19}, 2^{-18}, and 2^{-12} for all three variants, demonstrating a 99% success rate. Similarly, for KATAN32, a more effective related-key boomerang spanning 140 rounds with a probability of 2^{-15} is uncovered with 70% success rate. Further, in the single-key setting, a 84 round boomerang with probability 2^{-30} found with success rate of 60%. This research deepens the understanding of boomerang attacks, enhancing the toolkit for cryptanalysts to develop efficient and impactful attacks on NLFSR-based block ciphers.

Keywords: MILP · Boomerang · Sandwich · KATAN · TinyJAMBU · Symmetric-Key Cryptanalysis

1 Introduction

The introduction of the Boomerang attack by Wagner [22] was an important moment in the history of block cipher cryptanalysis. This was primarily because it allowed us to interpret a cipher as a composition of sub-ciphers showcasing the interaction of differential trails on orthogonal planes of the *Boomerang-Cube*. This demonstrated that shorter (and hence high probability) trails on orthogonal plane of the sub-ciphers were better than longer (and hence low probability) rails on a single plane of the full block cipher. Thus was born the *'Boomerang Quartet'* whose analysis spawned an entire body of research giving us further insight into *Boomerang-Cube* and its exploitation to deliver some of the best distinguishers on block ciphers reported in literature. In the classical boomerang attack, the cipher E is considered as a composition of two sub-ciphers E_0 and E_1, i.e., $E = E_1 \circ E_0$, where we suppose that the input difference Δ_0 is propagated to the difference Δ_1 by E_0 with probability p and the difference ∇_0 is propagated to ∇_1 by E_1 with probability q. This is described in Figure 1 while the expected probability of this attack is shown below. Equation 1 shows that by performing $\frac{1}{p^2 \cdot q^2}$ number of adaptively chosen plaintext/cipertext queries with the Δ_0 difference on the encryption queries and the ∇_1 difference on the decryption queries, the attacker can distinguish E from the ideal cipher. The most important part of this boomerang-style attacks is to select suitable differential characteristics for E_0 and E_1 so that the probability of obtaining a right quartet will be maximized. Also, in this type of attacks, the overall probability was calculated based on the assumption that the two sub-ciphers E_0 and E_1 are independent.

$$\Pr[E^{-1}(E(x) \oplus \nabla_1) \oplus E^{-1}(E(x \oplus \Delta_0) \oplus \nabla_1) = \Delta_0] = p^2 \cdot q^2. \tag{1}$$

One direction in boomerang research entailed improving the boomerang trails by the relaxing the assumptions at the edge of the sub-ciphers (like the Amplified Boomerang [17] attack) while another attempt was to convert the Boomerang attack to a chosen plaintext attack (Rectangle Attack [3]) with the penalty of an increased complexity. Yet another direction was inspired by Murphy's work [18] on the impossible Boomerang Quartet (showing incompatibilities between upper and lower trails due to incorrectness of the independence assumption). Research in this direction lead to many interesting contributions which let to the plane at the edge of the sub-ciphers in the Boomerang-Cube to be inflated to a cube in itself. This view allowed capture the various dependencies between the upper and lower trails and also resolved the problem of incompatible trails.

Research Exploiting Inter-trail Dependencies in the Boomerang-Cube One of the first exploitations of trail dependencies was due to Biryukov et al. in the middle round S-box trick [5]. Besides, many improvements taking advantages of the dependency between the two differential characteristics have been proposed, such as the ladder switch, S-box switch, and the Feistel switch in [6]. The basic idea is that the boundaries of E_0 and E_1 do not need to be defined on a state, instead, the state can be further divided into words, and some words can be in E_0 and others can be in E_1. Suppose, in a boomerang trail, half of the state is active in the upper trail E_0, the other half is active in the lower trail E_1, in between them only S-box layer is there. In this case, the probability on all the active S-boxes becomes 1. This technique is called ladder switch. Further, in the S-box switch, when both the characteristics for E_0 and E_1 activate the same S-box with an identical input difference and an identical output difference, the probability of this S-box to generate a quartet becomes p' instead of p'^2.

Later, in [12,13], Dunkelman et al. formalised the above observations, and captured in the framework of sandwich attack. In this attack, the target cipher E can be further decomposed into three parts, i.e., $E = E_1 \circ E_m \circ E_0$ where the middle part E_m consists of relatively short transformations (as depicted in Figure 2). Let (x_1, x_2, x_3, x_4) and (y_1, y_2, y_3, y_4) be the input and the output quartet values for E_m respectively such that $y_i = E_m(x_i)$. Thus, the probability of a valid boomerang quartet would be $p^2 \cdot q^2 \cdot r$, where r denotes the probability of E_m satisfying some differential propagation among four texts and is computed as follows.

$$r = \Pr[(x_3 \oplus x_4 = \Delta_1) | (x_1 \oplus x_2 = \Delta_1) \wedge (y_1 \oplus y_3 = \nabla_0) \wedge (y_2 \oplus y_4 = \nabla_0)]. \quad (2)$$

Therefore, the boomerang switching effects can be integrated as the dependency between the two characteristics of E_0 and E_1 which now lie in E_m. To calculate the probability r of E_m in a systematic way, as well as for finding the other switches to increase r, Cid et al. in [9] first proposed an efficient technique, called Boomerang Connectivity Table (BCT) to capture the boomerang switches of E_m. The BCT can capture both the incompatibility, indroduced by [18] and the observations by [6]. Moreover, BCT shows that the switching effect can be applied to increase the probability even when Δ_1 cannot be propagated to Δ_2 in the DDT. The drawbacks of BCT is that the incompatibility can be avoided by upto one round, but it cannot capture the incompatibility when multiple rounds of E_m are considered. In [23], Wang et al. proposed a modified tool, called Boomerang Difference Table (BDT) to improve the BCT when considering multiple rounds. Several other improvements on the middle layer for boomerang switch can be found in [21,26].

NLFSR-based Designs. Securing low-end devices like RFID tags is challenging due to their constrained environment. The ideal security solution must be compact, low-power, and fast enough for real-time protocols. In this context, NLFSR-based designs are a suitable choice. They offer several advantages such as low hardware cost, efficient parallel computation of rounds, and easy loading of stream input data into the state during state updates. These characteristics make NLFSR-based designs well-suited for compact, low-power, and real-time protocol requirements. Some well-known NLFSR-based designs include Grain, Trivium, KATAN, and TinyJambu. In we demonstrate the application of generalized boomerang switch techniques on the NLFSR-based block cipher KATAN, which is a highly efficient hardware-oriented cipher. Additionally, we explore the keyed permutation of TinyJambu, which was one of the ten finalists in the NIST lightweight authenticated encryption competition [2].

1.1 Our Contributions

Our contributions in this work can be summarized as follows:

- Comprehensive Analysis of Switching Techniques for NLFSR-based ciphers: We provide a comprehensive analysis of boomerang attacks, particularly in the context of NLFSR-based ciphers. By investigating the impact of different switch techniques, we deepen the understanding of how these attacks work and how the interdependencies between characteristics influence their success.
- Introducing the Open-Sandwich Attack: We introduce a novel approach to identify boomerang distinguishers by exclusively utilizing the path through ladder or And switches. This approach, called as the "open-sandwich attack", offers a new perspective on attack modeling and provides a new way to uncover vulnerabilities in ciphers.
- Best distinguishers on TinyJambu and KATAN32: Using our approach, we successfully identify better boomerang distinguishers for ciphers, like TinyJambu and KATAN32. A brief comparison of these attacks are presented in Table 1. These discoveries highlight the practical applicability of our methods and their potential to uncover weaknesses in real-world cryptographic systems.

1.2 Outline of the Paper

The structure of this paper is outlined as follows. In Section 2, we establish the foundational knowledge necessary for constructing a novel sandwich attack tailored for NLFSR-based block ciphers. Section 3 is dedicated to a comprehensive discussion on the development of a Mixed Integer Linear Programming (MILP) model, effectively dissecting the sandwich attack through the utilization of various switches. Section 4 presents empirical results derived from our innovative technique, applied to both the related-key and single-key settings for the TinyJambu cipher. Additionally, Section 5 extends our methodology to explore and discover optimal boomerangs for the KATAN32 cipher under both key settings. Subsequently, in Section 6, we engage in a discussion encompassing potential enhancements and future research challenges pertinent to our technique. Finally, Section 7 offers concluding remarks that summarize the key findings and implications of our work.

2 Preliminaries

In this section, we begin by providing a concise overview of the framework of boomerang attacks. Following that, we delve into the categorization of the generalized switching effects for a single AND-based non-linear feedback shift register

Table 1: Comparison of Attacks against KATAN32 and TinyJambu variants. Here SK, RK, KP, ACP represent Single-key, Related-key, Known Plaintext and Adaptive Chosen Plaintext respectively

Cipher	Techniques	Attack Model	Key Size	Rounds	Distinguishing Probability	References
TinyJambu	Differential	RK	128	1024	2^{-16}	[11]
					2^{-14}	[16]
			192	1152	2^{-12}	[11]
					2^{-10}	[16]
			256	1280	2^{-10}	[11]
					2^{-8}	[16]
		SK	128	384	2^{-19}	[19]
				384	2^{-14}	[16]
				640	2^{-42}	
				1024	2^{-108}	
	Slide	KP	128	∞	2^{-64}	[20]
		ACP	192	∞	2^{-65}	
		ACP	256	∞	$2^{-67.5}$	
	Boomerang	RK	128	1024	2^{-19}	**This Work** Section 5
			192	1152	2^{-18}	
			256	1280	2^{-12}	
		SK	128	640	2^{-22}	
KATAN32	Boomerang	RK	80	140	$2^{-27.2}$	[15]
					$2^{-26.58}$	[8]
					2^{-15}	**This Work** Section 6
		SK	80	83†	$2^{-21.78}$	[8]
				84	2^{-30}	**This Work** Section 6

†The given trail has probability much lower than 2^{-32}.

(NLFSR). This discussion aims to lay the foundation for a comprehensive understanding of boomerang attacks and their applicability in cryptographic analysis.

2.1 Differential Propagation through AND Gates

Differential cryptanalysis was first proposed by Biham and Shamir in the early 1990s in [4]. It is one of the most fundamental cryptanalytic approach to evaluate the security of block ciphers. For differential cryptanalysis, the basic idea is to find the higher probability differential trails by assuming that the state differences spreading through the rounds in a cipher are independent. This probability comes due to some active non-linear components through the rounds for iterated ciphers, and is inversely proportional to the number of rounds. Thus, the resistance against differential cryptanalysis for iterated ciphers (based on the non-linear components like S-box/Addition/AND operations) is highly dependent on the non-linearity features of these operations. For an n-bit S-box $S : \{0,1\}^n \rightarrow \{0,1\}^n$, the differential properties of S are typically represented by the $2^n \times 2^n$ Difference Distribution Table (DDT) T, where a row represents the input difference ($\varDelta_i$) and a clomun represents the output difference ($\varDelta_o$). The entries in T are defined by $T(\varDelta_i, \varDelta_o) = \#\{x : S(x) \oplus S(x \oplus \varDelta_i) = \varDelta_o\}$.

Thus, the probability for any given difference pair $(\varDelta_i, \varDelta_o)$, i.e., the input difference $\varDelta_i$ propagates to the output difference $\varDelta_o$ is $\frac{T(\varDelta_i, \varDelta_o)}{2^n}$. Also, for an AND gate, if $(\varDelta a, \varDelta b)$ denotes the input difference and $\varDelta z$ as its output difference, then we have,

$$\varDelta z = a \cdot b \oplus (a + \varDelta a) \cdot (b + \varDelta b) = a \cdot \varDelta b \oplus b \cdot \varDelta a \oplus \varDelta a \cdot \varDelta b. \quad (3)$$

The differential properties of AND gate can also be represented by 4×2 DDT table T, which is given in Table 2. The entries in the table T are defined by

$$T((\varDelta a, \varDelta b), \varDelta z) = \#\{(a, b) : a \cdot b \oplus (a \oplus \varDelta a) \cdot (b \oplus \varDelta b) = \varDelta z\}.$$

$(\varDelta a,\ \varDelta b)$	$\varDelta z = 0$	$\varDelta z = 1$
(0, 0)	4	0
(0, 1)	2	2
(1, 0)	2	2
(1, 1)	2	2

Table 2: Difference Distribution Table of AND Gate

Therefore, the probability for the input difference $(\varDelta a, \varDelta b)$ propagates to the output difference $\varDelta z$ will be $\frac{T((\varDelta a, \varDelta b), \varDelta z)}{4}$. According to the Table 2, the output difference $\varDelta z$ follows a uniform distribution for any given non-zero input difference $(\varDelta a, \varDelta b)$.

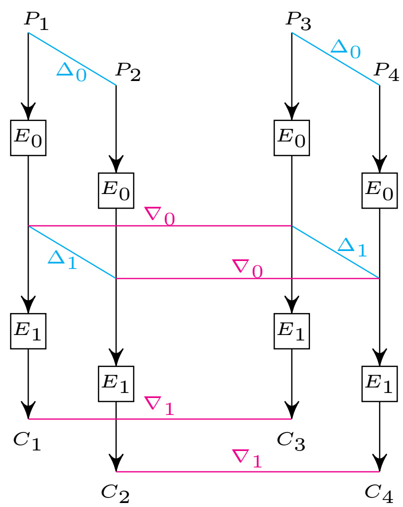

Fig. 1: Boomerang Attack

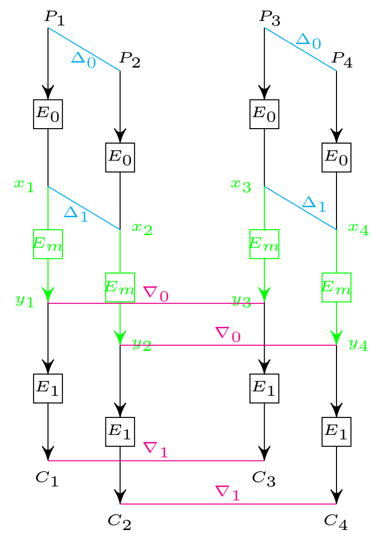

Fig. 2: Sandwich Attack

2.2 Boomerang Attack

Now, we give a brief overview of the boomerang attack. Let $E_K(P)$ and $E_K(C)$ denote the encryption of P and the decryption of C under a key K, respectively. Suppose ΔK, ∇K are the master key differences of the differentials. Then, the boomerang distinguisher is mounted as follows:

1. Ask for the ciphertexts $C_1 = E_K(P_1)$ and $C_2 = E_K(P_2)$, where $P_2 = P_1 \oplus \Delta_0$.
2. Ask for the plaintexts $P_3 = E_K^{-1}(C_3)$ and $P_4 = E_K^{-1}(C_4)$, where $C_3 = C_1 \oplus \nabla_1$ and $C_4 = C_2 \oplus \nabla_1$.
3. Check whether $P_3 \oplus P_4 = \Delta_0$.

Also, the boomerang framework in the related-key setting works as follows:

1. $K_1 \leftarrow K$, $K_2 \leftarrow K_1 \oplus \Delta K$, $K_3 \leftarrow K_1 \oplus \nabla K$, $K_4 \leftarrow K_1 \oplus \Delta K \oplus \nabla K$.
2. Ask for the ciphertexts $C_1 = E_{K_1}(P_1)$ and $C_2 = E_{K_2}(P_2)$, where $P_2 = P_1 \oplus \Delta_0$.
3. Ask for the plaintexts $P_3 = E_{K_3^{-1}}(C_3)$ and $P_4 = E_{K_4^{-1}}(C_4)$, where $C_3 = C_1 \oplus \nabla_1$ and $C_4 = C_2 \oplus \nabla_1$.
4. Check whether $P_3 \oplus P_4 = \Delta_0$.

Switching in Boomerang Attacks. Here, we give a brief overview of the switching techniques that are employed in the boomerang attacks tailored for Substitution-Permutation Network (SPN) based ciphers. Consider a cipher E

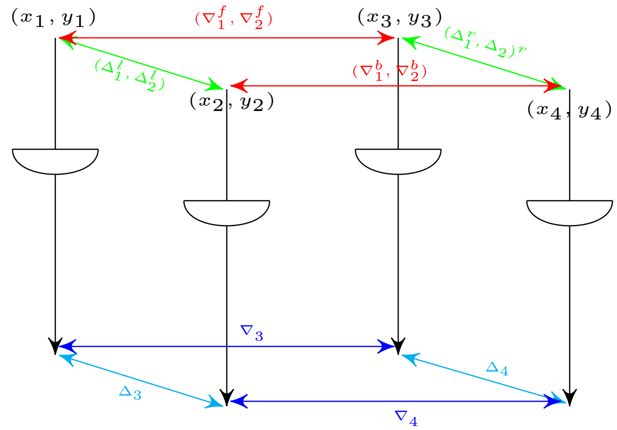

Fig. 3: A Valid Boomerang Quartet of E_m as One Round NLFSR

and its decomposition $E = E_1 \circ E_m \circ E_0$ (refer to Fig. 2) as formalised in [12,13]. Assume that the last substitution layer partitions x_1 into t words, i. e., $x_1 = x_1^0 || \cdots || x_1^{t-1}$. Similarly, x_i's $(2 \leq i \leq 4)$, y_j's $(1 \leq j \leq 4)$, Δ_1 and ∇_0 can be partitioned into t words (assume that the corresponding s-box is $\nu \times \nu$). Consider the following relation for the k-th word-

$$x_1^{k-1} \oplus x_2^{k-1} = \Delta_1^{k-1}$$

For satisfying the E_0 trail (in the return path of the boomerang), the following relation must hold for $1 \leq k \leq t$-

$$S^{-1}(S(x_1^{k-1}) \oplus \nabla_0^{k-1}) \oplus S^{-1}(S(x_2^{k-1}) \oplus \nabla_0^{k-1}) = \Delta_1^{k-1} \tag{4}$$

where S is the substitution operation applied on each word. Now consider the following two cases-

- **Case I:** When $x_1^{k-1} = x_2^{k-1}$, Eq. 4 holds with probability one. This particular case is designated as *ladder* switch.
- **Case II:** When $S(x_1^{k-1}) \oplus S(x_2^{k-1}) = \nabla_0^{k-1}$, Eq. 4 holds with probability $\frac{\mu}{2^\nu}$, where μ is entry in the difference distribution table (DDT) of S with Δ_1^{k-1} and ∇_0^{k-1} as the input and output differences, respectively. This particular case is designated as s-box switch.

Next, we introduce a notion similar to these switches when the non-linear layer of a cipher consists of AND operations.

3 Introducing Generalized Switching in NLFSR

Consider the middle layer E_m in a sandwich attack which is composed of a single round NLFSR-based cipher which has only one AND gate as the non-linear

(Δ_1,Δ_2) \ (∇_1,∇_2)	**(0,0)**	**(1,0)**	**(0,1)**	**(1,1)**
(0,0)	4	4	4	4
(1,0)	4	4	0	0
(0,1)	4	0	4	0
(1,1)	4	0	0	4

Table 3: Boomerang Connectivity Table of Single AND-based NLFSR

component, given in Figure 3. The target cipher is divided into three parts E_0, E_m, and E_1. Let $(x_1,y_1),(x_2,y_2),(x_3,y_3),(x_4,y_4) \in \{0,1\}^2$ are the inputs to the four AND gates of E_m such that $x_1 \oplus x_2 = x_3 \oplus x_4 = \Delta_1^l = \Delta_1^r = \Delta_1$ (say), $y_1 \oplus y_2 = y_3 \oplus y_4 = \Delta_2^l = \Delta_2^r = \Delta_2$, $x_1 \oplus x_3 = x_2 \oplus x_4 = \nabla_1^f = \nabla_1^r = \nabla_1$ and $y_1 \oplus y_3 = y_2 \oplus y_4 = \nabla_2^f = \nabla_2^r = \nabla_2$. Also, let $z_1, z_2, z_3, z_4 \in \{0,1\}$ are the corresonding output differences such that $z_1 \oplus z_2 = \Delta_3$ and $z_3 \oplus z_4 = \Delta_4$. For $(x,y) \in \{0,1\}^2$, the output difference of the AND operation in the left plane is given by

$$\Delta_3 = x \cdot y \oplus (x \oplus \Delta_1) \cdot (y \oplus \Delta_2).$$

Similarly,

$$\Delta_4 = (x \oplus \nabla_1) \cdot (y \oplus \nabla_2) \oplus (x \oplus \nabla_1 \oplus \Delta_1) \cdot (y \oplus \nabla_2 \oplus \Delta_2).$$

In order to obtain a right quartet, we can obtain a necessary condition similar to Equation 4 for such NLFSR-based ciphers-

$$\begin{aligned} &\Delta_3 = \Delta_4 \\ \Longrightarrow\ & x \cdot y \oplus (x \oplus \Delta_1) \cdot (y \oplus \Delta_2) = (x \oplus \nabla_1) \cdot (y \oplus \nabla_2) \oplus (x \oplus \nabla_1 \oplus \Delta_1) \cdot (y \oplus \nabla_2 \oplus \Delta_2) \end{aligned}$$

Then, the probability that the above condition holds is given by:

$$\begin{aligned} &Pr[\Delta_3 = \Delta_4] \\ =& \frac{\#\{(x,y) : (x \oplus \nabla_1) \cdot (y \oplus \nabla_2) \oplus (((x \oplus \Delta_1) \oplus \nabla_1) \cdot ((y \oplus \Delta_2) \oplus \nabla_2)) = (x \cdot y) \oplus ((x \oplus \Delta_1) \cdot (y \oplus \Delta_2))\}}{2^2}. \end{aligned} \tag{5}$$

The evaluation of Equation 5 is illustrated in Figure 2. This is exactly the r in Equation 2, when E_m is a single AND layer. Similar to the DDT, we evaluate the Boomerang Connectivity Table (BCT) using Equation 5 for all pairs of (Δ_1, Δ_2) and (∇_1, ∇_2) as shown in Table 3. Further, according to Figure 3 different generalized switching techniques are introduced here.

Trivial switch:

$$\left\{ \Delta_3 = \Delta_4 = \nabla_3 = \nabla_4 = 0 \qquad \text{if } (\Delta_1^l, \Delta_2^l) = (\Delta_1^r, \Delta_2^r) = (\nabla_1^f, \nabla_2^f) = (\nabla_1^b, \nabla_2^b) = (0,0). \right.$$

Ladder switch:

$$\begin{cases} \Delta_3 = \Delta_4 = 0, \nabla_3 = \nabla_4 & \text{if } (\Delta_1^l, \Delta_2^l) = (\Delta_1^r, \Delta_2^r) = (0,0), (\nabla_1^f, \nabla_2^f) = (\nabla_1^b, \nabla_2^b) \neq (0,0), \\ \Delta_3 = \Delta_4, \nabla_3 = \nabla_4 = 0 & \text{if } (\Delta_1^l, \Delta_2^l) = (\Delta_1^r, \Delta_2^r) \neq (0,0), (\nabla_1^f, \nabla_2^f) = (\nabla_1^b, \nabla_2^b) = (0,0). \end{cases}$$

AND Switch:

$$\begin{cases} \Delta_3 = \Delta_4 = \nabla_3 = \nabla_4 & \text{if } (\Delta_1^l, \Delta_2^l) = (\Delta_1^r, \Delta_2^r) = (\nabla_1^f, \nabla_2^f) = (\nabla_1^b, \nabla_2^b) \neq (0,0). \end{cases}$$

Trail Switch:

$$\begin{cases} {}^{1}\Delta_3 \neq \Delta_4, \nabla_3 \neq \nabla_4 & \text{if } (\Delta_1^l, \Delta_2^l) = (\Delta_1^r, \Delta_2^r) \neq (0,0), \\ & \quad (\nabla_1^f, \nabla_2^f) = (\nabla_1^b, \nabla_2^b) \neq (0,0), (\Delta_1^l, \Delta_2^l) \neq (\nabla_1^f, \nabla_2^f), \\ \Delta_3 = \Delta_4, \nabla_3 \neq \nabla_4 & \text{if } (\Delta_1^l, \Delta_2^l) = (\Delta_1^r, \Delta_2^r), (\nabla_1^f, \nabla_2^f) \neq (\nabla_1^b, \nabla_2^b), \\ \Delta_3 \neq \Delta_4, \nabla_3 = \nabla_4 & \text{if } (\Delta_1^l, \Delta_2^l) \neq (\Delta_1^r, \Delta_2^r), (\nabla_1^f, \nabla_2^f) = (\nabla_1^b, \nabla_2^b), \\ \Delta_3 \neq \Delta_4, \nabla_3 \neq \nabla_4 & \text{if } \begin{cases} (\Delta_1^l, \Delta_2^l) \neq (\Delta_1^r, \Delta_2^r), (\nabla_1^f, \nabla_2^f) \neq (\nabla_1^b, \nabla_2^b), \\ (\Delta_1^l, \Delta_2^l) = (\Delta_1^r, \Delta_2^r) \neq (\nabla_1^f, \nabla_2^f) = (\nabla_1^b, \nabla_2^b). \end{cases} \end{cases}$$

In the context of distinguishing probability, the various switches play a significant role within the framework of the boomerang attack. The objective in forming a boomerang quartet is to maintain equal parallel plane (state) differences in both the segments. Considering a one-round operation denoted as E_m (refer to Figure 3), and omitting the shifting operation within the state, taking a special case where $\Delta_1^l = \Delta_1^r$, $\Delta_2^l = \Delta_2^r$, $\nabla_1^f = \nabla_1^b$, and $\nabla_2^f = \nabla_2^b$, the probabilities for the corresponding output differences that will be the same under these switches are summarized in Figure 4.

4 Slicing the Sandwich Attack

In the context of the sandwich attack, the cipher E is conceptualized as the composition of three subciphers: E_0, E_m, and E_1, represented as $E = E_0 \circ E_m \circ E_1$. The intermediary component E_m is utilized to incorporate a small number of rounds via various switch techniques, directly enhancing the probability of the boomerang distinguisher. For ciphers based on Sbox, when only ladder switches occur in E_m, the value of r becomes 1. Consequently, the distinguishing probability simplifies to $p^2 \cdot q^2 \cdot r = p^2 \cdot q^2$. Furthermore, the Sbox or other new switches within E_m can also contribute to improving the value of r, although not significantly compared to the ladder switch. Thus, for the sandwich attack (as illustrated in Figure 2), constructing single or very few rounds of E_m using Sbox or other new switches is relatively straightforward. However, employing switch techniques for a large number of rounds in E_m can introduce compatibility challenges. To address this, several systematic techniques [21,23,14] are introduced to effectively resolve these incompatibility issues as the number of rounds increases.

[1] This sub-case of the Trail Switch category covers all switches except Trivial, Ladder, and AND when we require two opposite plane differences to be equal (refer to Table 4). The remaining sub-cases within the Trail Switch category occur when no specific conditions are imposed on opposite plane differences.

Δ_1	Δ_2	∇_1	∇_2	Switch	$Pr[\Delta_3 = \Delta_4, \nabla_3 = \nabla_4]$
0	0	0	0	-	1
0	0	0	1	Ladder	1
0	0	1	0	Ladder	1
0	0	1	1	Ladder	1
0	1	0	0	Ladder	1
0	1	0	1	And	1
0	1	1	0	Trail	0
0	1	1	1	Trail	0
1	0	0	0	Ladder	1
1	0	0	1	Trail	0
1	0	1	0	And	1
1	0	1	1	Trail	0
1	1	0	0	Ladder	1
1	1	0	1	Trail	0
1	1	1	0	Trail	0
1	1	1	1	And	1

Table 4: Different Switching Probabilities to Maintain Equal Plane Differences in E_m.

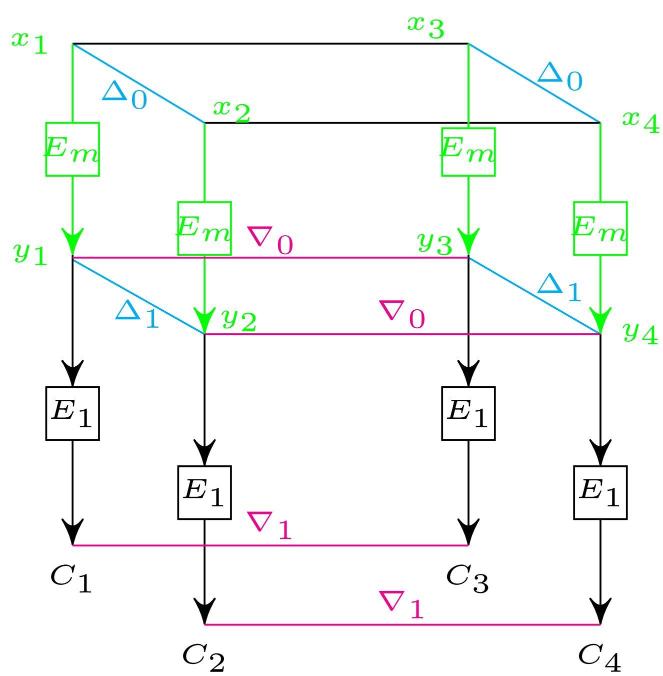

Fig. 4: Open-Sandwich Attack

For NLFSR-based block ciphers, it is important to highlight that only ladder or And switches have the potential to enhance the value of r in E_m and simultaneously maintain equality in their opposite plane (state) differences. In contrast, other switch cases result in unequal opposite plane differences. While employing other switch techniques might allow the attacker to obtain the input difference Δ_0 through boomerang-style attacks, the resulting distinguishing probability is notably lower compared to the scenarios where only ladder or And switches are used.

In this study, our primary focus is to delve into the discussion of boomerang attacks exclusively through the utilization of ladder or And switches. Within the scope of this work, we particularly concentrate on exploring and analyzing these switches. It is worth noting that in the pursuit of identifying the optimal boomerang for NLFSR-based block ciphers, a useful approach is to conceptualize the cipher E as the composition of E_m and E_1, expressed as $E = E_m \circ E_1$. This framework essentially constitutes a special case of a sandwich attack, with E_0 being omitted. We refer to this technique as the "open-face sandwich attack". The distinguishing probability of this attack will be $r \cdot q^2$. This attack is demonstrated in Figure 4.

4.1 Our Observations

Consider a straightforward boomerang structure $E = E_0 \circ E_1$ (as depicted in Figure 1), which corresponds to optimal differentials $\Delta_0 \to \Delta_1$ of E_0 with a probability of p, and $\nabla_0 \to \nabla_1$ of E_1 with a probability of q. In this context, the probability of success for this boomerang distinguisher can be approximately evaluated using the formula $p^2 \cdot q^2$. Now, for the simple boomerang within NLFSR-based block ciphers, let p represent the count of active AND gates for the differential $\Delta_0 \to \Delta_1$ in one of the two opposing upper planes within E_0. Likewise, let q denote the count of active AND gates for the differential $\nabla_0 \to \nabla_1$ in one of the two opposing lower planes within E_1. However, it is important to note that in this scenario, the actual probability of satisfying this boomerang tends to be notably higher than the theoretical probability $p^2 \cdot q^2$. This discrepancy between theoretical and actual probabilities sparked our curiosity to further explore the behavior of such boomerang attacks within NLFSR-based ciphers and to accurately estimate the theoretical probability.

In NLFSR-based block ciphers, AND gates constitute the sole non-linear operations utilized within the cipher structure. When examining a boomerang scenario (as illustrated in Figure 4), consider the differential $\Delta_0 \to \Delta_1$ pertaining to E_m and the differential $\nabla_0 \to \nabla_1$ associated with E_1. Within the boomerang quartet, the plane differences in each round align with the category of distinct switches mentioned earlier.

Boomerangs involving trail switches cause the opposite plane differences to become unequal, simultaneously compelling the increase of trail switches across rounds. Consequently, these trail switch-based boomerangs lead to a significant reduction in the overall probability. As a result, the quest for an improved boomerang distinguisher involves seeking a promising differential boomerang path that traverses through various switches while excluding the other switches. Upon discovering such an optimal boomerang path, characterized by the right number of ladder or And switches, the probability can be precisely computed using the formula $r \cdot q^2$.

4.2 Searching of Good Boomerang Trails

In our pursuit of identifying effective boomerang trails for the cipher, our strategy revolves around optimizing the number of ladder or And switches necessary to create a boomerang effect. To accomplish this, we have developed a straightforward model that employs mixed-integer linear programming (MILP) to search for the optimal boomerang trails.

In this MILP model, a pragmatic approach is taken: we maintain four state differences and focus on optimizing the plane differences by assigning appropriate weights to the ladder or And switches. Specifically, when dealing with rounds of E_m, we assign a weight of 1 to the ladder or And switches. Conversely, for the lower part (E_1), we assign a weight of 2 to the ladder or And switches. Within the framework of the optimal boomerang trail, let us denote w_1 and w_2 as the cumulative weights of E_m and E_1, respectively. Consequently, the probability associated with the boomerang trail can be expressed as $r \cdot q^2 = 2^{-w_1 - w_2}$. This formulation allows us to effectively determine and optimize the probability of the boomerang trail.

It is important to note that this probability accurately represents the boomerang's success when both differences Δ_1 and ∇_1 are predetermined. However, if Δ_1 and ∇_1 are arbitrary differences, the calculated probability can potentially experience a notable enhancement due to the existence of multiple paths within the boomerang or due to the inclusion of trail switches. In such scenarios, the actual probability of obtaining a right boomerang quartet could be higher than the calculated value due to the increased flexibility introduced by these variations.

5 Attacks on TinyJambu

The TinyJambu [25] is an authentication scheme that is chosen as one of the finalists in the NIST lightweight cryptography (LWC) competition. It employs an NLFSR-based keyed permutation as its internal structure, without a key schedule function. TinyJambu provides three versions with key sizes of 128, 192, and 256 bits respectively. During initialization, the initial version of TinyJambu [24] utilizes 384 rounds to process the nonce and associated data, while for processing the message, it employs 1024/1152/1280 rounds depending on the key size of 128/192/256 bits. However, in 2020, Saha et al. [19] demonstrated a forgery attack on the full-round TinyJambu scheme with a probability close to $2^{-70.64}$, indicating a security level near 64 bits. In response, the designers increased the number of rounds from 384 to 640 to enhance the scheme's security. For a more comprehensive understanding of TinyJambu's specifications, please refer to [25]. Regarding the keyed permutation of TinyJambu in the secret key setting, further research has revealed certain vulnerabilities. In the work [20], key-recovery attacks on all variant sizes were presented, achieving results close to the birthday bound of 2^{64}.

Dunkelman et al. [10] demonstrated a zero-sum distinguisher for 544 rounds out of the 1024-round TinyJambu keyed permutation, achieving this with a complexity of 2^{23}. Furthermore, in their work [11], the authors revealed related-key forgery attacks targeting various TinyJambu variants. These attacks exhibited differential probabilities of 2^{-16}, 2^{-12} and 2^{-10} for 128, 192, and 256-bit keys, respectively, emphasizing potential security concerns.

In another development, Jana et al. [16] identified a full-round differential trail within the 1024-round TinyJambu keyed permutation. This trail displayed an exceptionally low probability of 2^{-108}, revealing non-random properties within the keyed permutation. Additionally, in this attack, the authors demonstrated improved related-key differential probabilities of 2^{-14}, 2^{-10} and 2^{-8} for 128, 192, and 256-bit keys, respectively, highlighting potential vulnerabilities in TinyJambu's security characteristics.

In this section, our focus is on the TinyJambu keyed permutation, where we investigate the application of different switch techniques to explore boomerang properties. By employing these techniques, we achieve significant advancements in the analysis of TinyJambu with 640 rounds in the secret-key settings, surpassing the success rates of previous attacks. Furthermore, we present the related-key boomerang attacks for all the TinyJambu variants.

5.1 Specification

TinyJambu is an authenticated encryption with associated data (AEAD) scheme, featuring a 128-bit non-linear feedback shift register (NLFSR)-based keyed permutation with a 128-bit state size and 32-bit message block size. It was selected as one of the top ten finalists in the NIST Lightweight Cryptography (LWC) competition, competing among 56 submissions. The 128-bit keyed permutation, represented as P_l^K, comprises l rounds, with the secret key K belonging to $\mathbb{F}_2^{|K|}$, where K is defined as $(k_{|K|-1}, k_{|K|-2}, \cdots, k_1, k_0)$. This permutation offers support for three key sizes: 128 bits, 192 bits, and 256 bits. In this work, we denote an l-round keyed permutation of TinyJambu as $\mathcal{P}_\mathsf{l}$. Each round of the permutation, $P_l^K : \mathbb{F}_2^{128} \to \mathbb{F}_2^{128}$, transforms an initial state $(s_{127}, s_{126}, \cdots, s_1, s_0)$ into a final state $(s_f, s_{127}, s_{126}, \cdots, s_2, s_1)$, where s_f is calculated as $s_0 \oplus s_{47} \oplus \overline{s_{70}s_{85}} \oplus s_{91} \oplus k_{i \mod |K|}$. Figure 5 refers to a visual representation of this permutation.

TinyJambu offers three variants, denoted as TinyJambu-128, TinyJambu-192, and TinyJambu-256, each defined by specific parameters listed in Table 5. The encryption process in TinyJambu involves four main phases: Initialization, Associated Data Processing, Encryption, and Finalization. We refer to Figure 6 for an overview of the TinyJambu mode's overall structure. Detailed specifications for the permutations P_l and $\hat{P}_l$ can be found in Table 5. The complete details of this scheme can be found in [25].

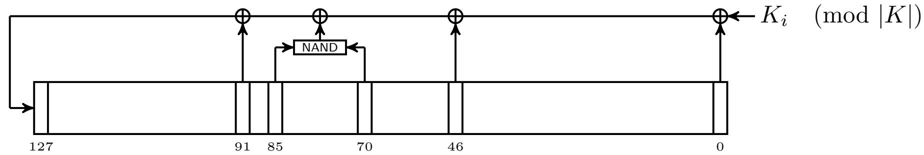

Fig. 5: The Permutation P^{k_i}

Table 5: TinyJambu Variants

AEAD Variants of TinyJambu Mode	Size in bits				Number of Rounds in	
	State	Key	Nonce	Tag	P_l	$\hat{P}_l$
TinyJambu-128	128	128	96	64	640	1024
TinyJambu-192	128	192	96	64	640	1152
TinyJambu-256	128	256	96	64	640	1280

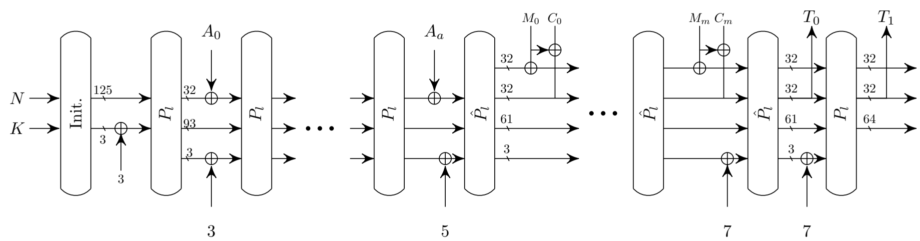

Fig. 6: The Description of TinyJambu Mode

5.2 MILP Modelling

When employing MILP modeling for a boomerang attack on TinyJambu, there are several approaches to consider.

One approach involves utilizing MILP modeling to discover optimal differential trails for both the upper part (E_0) and the lower part (E_1) of the TinyJambu cipher. This optimization of differential trails can significantly enhance the effectiveness of the attack. Another approach entails partitioning the TinyJambu cipher into four separate planes, each corresponding to an individual TinyJambu function. In this setup, the MILP model is responsible for determining the minimum count of active AND gates in E_m and E_1. However, it is worth noting that as the number of variables and constraints increases, this model might experience a notable slowdown in computational speed.

To enhance the computational efficiency of the MILP model and reduce the required computational time, it is possible to implement the attack by focusing on two planes rather than four. By minimizing the ladder/And switches, an efficient and effective boomerang distinguisher can be developed while maintaining a reasonable level of modeling speed. In essence, the objective of implementing the boomerang attack using MILP modeling for TinyJambu is to treat the Tiny-

Jambu cipher as $E_m \circ E_1$, with a focus on minimizing the ladder/And switches to create a potent boomerang distinguisher that is both efficient and effective.

Table 6: Boomerang Distinguishers of TinyJambu through MILP Search

Rounds	Ladder Switch	And Switch	Distinguishing Probability	Input Difference (Upper Plane)	Output Difference (Lower Plane)	Success Probability
320	6	0	2^{-9}	$\Delta_0 =$ 0x00000120 00000000 02000000 00000400	$\nabla_0 =$ 0x00000001 20000000 00020000 00000004	99.9%
				$\Delta_1 =$ 0x00000000 00000000 00000400 00000020	$\nabla_1 =$ 0x00000000 00000000 00000004 00000000	
	7	0	2^{-10}	$\Delta_0 =$ 0x00004000 00000000 80000000 00000000	$\nabla_0 =$ 0x00000001 20000000 00020000 00000004	99.9%
				$\Delta_1 =$ 0x00000000 80000000 04000020 00204000	$\nabla_1 =$ 0x00000000 00000000 00000004 00000000	
384	8	0	2^{-12}	$\Delta_0 =$ 0x00000241 00020000 04000000 00000800	$\nabla_0 =$ 0x00020010 00000004 80000000 00080000	99.9%
				$\Delta_1 =$ 0x00000000 00000800 00000040 00020002	$\nabla_1 =$ 0x00000000 00000000 00000010 00000000	
	4	4	2^{-12}	$\Delta_0 =$ 0x00020010 00000004 80000000 00080000	$\nabla_0 =$ 0x00200100 00000048 00000000 00800000	100%
				$\Delta_1 =$ 0x00000000 00000000 00000010 00000000	$\nabla_1 =$ 0x00000000 00000000 00000100 00000008	
640[1]	24	2	2^{-39}	$\Delta_0 =$ 0x00001000 80000000 24000000 00004000	$\nabla_0 =$ 0x00008004 00000001 20000000 00020000	–
				$\Delta_1 =$ 0x04000000 00204000 00010000 80000810	$\nabla_1 =$ 0x20000000 01020000 00080004 00004081	

Table 7: Amplified Boomerang Distinguishers of TinyJambu

Rounds	Distinguishing Probability	Input Difference (Upper Plane)	Output Difference (Lower Plane)	Success Probability
288	1	$\Delta_0 =$ 0x00004000 00000000 80000000 00000000	$\nabla_1 =$ 0x00000000 00000000 00000400 00000020	100%
320	1	$\Delta_0 =$ 0x00001000 00000000 20000000 00000000	$\nabla_1 =$ 0x00000000 00000000 00000040 00000002	100%
		$\Delta_0 =$ 0x00004000 00000000 80000000 00000000	$\nabla_1 =$ 0x00000000 00000000 00000004 00000000	100%
	2^{-4}	$\Delta_0 =$ 0x00000120 00000000 02000000 00000400	$\nabla_1 =$ 0x00000000 00000000 00000004 00000000	99.8%
384	2^{-4}	$\Delta_0 =$ 0x00000241 00020000 04000000 00000800	$\nabla_1 =$ 0x00000000 00000000 00000010 00000000	98%
	2^{-4}	$\Delta_0 =$ 0x00020010 00000004 80000000 00080000	$\nabla_1 =$ 0x00000000 00000000 00000100 00000008	97.6%
640	2^{-22}	$\Delta_0 =$ 0x00048200 04000008 00000000 00100000	$\nabla_1 =$ 0x00000000 00000000 20000000 01000000	95%
	2^{-24}	$\Delta_0 =$ 0x00001000 80000000 24000000 00004000	$\nabla_1 =$ 0x20000000 01020000 00080004 00004081	95%

5.3 Results on TinyJambu

Single-key Boomerang Attacks By employing our proposed MILP modeling, we have successfully identified a boomerang distinguisher for TinyJambu spanning up to 320 rounds. Our optimal solution involves 6 ladder switches occurring at specific rounds: 0, 32, 47, 168, 200, and 215. Additionally, the second best solution consists of 7 ladder switches at rounds 107, 122, 144, 159, 168, 200, and 215. These boomerang trails are detailed in Table 6.

[2] Sub-optimal solution due to MILP solver limitations.

Our search approach treats E as two equal subciphers: E_m and E_1. For the optimal solution, we find three ladder switches in each of E_m and E_1. This results in $r = 2^{-3}$ and $q = 2^{-3}$, yielding a distinguishing probability of $r \cdot q^2 = 2^{-9}$. Similarly, for the second best solution, we have $r = 2^{-4}$, $q = 2^{-3}$, and a probability of 2^{-10}.

Alternatively, if we consider the boomerang trail as two distinct differentials of 160 rounds each, denoted as $E = E_0 \circ E_1$, the distinguishing probability becomes $p^2 \cdot q^2$, where $p = \Pr(\varDelta_0 \to \varDelta_1)$ and $q = \Pr(\nabla_0 \to \nabla_1)$. For the first 320-round boomerang distinguisher in Table 6, we have $p = 2^{-3}$ and $q = 2^{-3}$, resulting in a probability of 2^{-12}. Similarly, for the second distinguisher of 320 rounds, with $p = 2^{-4}$ and $q = 2^{-3}$, the probability is 2^{-14}.

In our comprehensive investigation, we have delved into the intricacies of boomerang paths, particularly focusing on larger rounds, namely 384 rounds and 640 rounds. For the 384-round scenario, our diligent analysis led to the discovery of an optimal boomerang path, meticulously comprising 8 ladder switches strategically activated at specific rounds: 31, 46, 159, 174, 215, 230, 262, and 277. When considering fixed values for $\varDelta_1$ and ∇_0, this carefully designed boomerang path yields a probability for the boomerang distinguisher, precisely calculated as $r \cdot q^2 = 2^{-4} \cdot 2^{-8} = 2^{-12}$. This finding underscores that even with a substantial number of cipher rounds, the likelihood of success for this boomerang attack remains relatively low.

In a more extensive scenario involving 640 rounds, our investigation led to the identification of an intricate boomerang trail. This path involves the activation of 26 ladder/And switches, consisting of 24 ladder switches and 2 And switches, thoughtfully positioned throughout the rounds. The resulting distinguishing probability for this extensive boomerang path is significantly lower, quantified as 2^{-41}. This difference emphasizes the escalating difficulty and diminishing success rate associated with boomerang attacks as the number of rounds in the cipher increases. Our approach to identifying these optimal boomerang trails through various switches effectively captures the probability distribution, shedding light on the challenging landscape of NLFSR-based cryptographic cipher analysis.

Moreover, we have explored the concept of amplified boomerangs in this context to enhance the overall probability of boomerang distinguishers. Our approach involves deliberately seeking suboptimal solutions from our MILP search. The goal is to create a boomerang with the input difference $\varDelta_0$ and the output difference ∇_1 that possesses numerous alternate paths. This strategic manipulation has led to notably improved probabilities for these rounds of TinyJambu, which are detailed in Table 7.

Related-key Boomerang Attacks In a similar manner, we applied the MILP model to investigate related-key boomerang trails for the TinyJambu-128 cipher. For a 384-round cipher, we identified an optimal solution that resulted in a deterministic boomerang trail, requiring no ladder or And switches.

Table 8: Related-key Boomerang Distinguishers of TinyJambu Variants through MILP Search

Variants	Rounds	Ladder Switch	And Switch	Distinguishing Probability	Upper Trail Difference	Lower Trail Difference	Upper Key Difference Lower Key Difference	Success Probability
TinyJambu128	384	0	0	1	$\Delta_0 =$ 0x00102400 00000020 40000000 00000000 $\Delta_1 =$ 0x00000000 00000000 00000400 00000000	$\nabla_0 =$ 0x00000008 00000000 00100000 00000000 $\nabla_1 =$ 0x00000000 00000000 00000200 00000010	0x00000400 00000020 40000000 00000000 0x04000000 00000000 00000200 00000000	100%
	512[1]	4	0	2^{-6}	$\Delta_0 =$ 0x00090000 00000010 00000000 00200000 $\Delta_1 =$ 0x00000000 00000000 00000000 00200000	$\nabla_0 =$ 0x00000008 00000000 00100000 00000000 $\nabla_1 =$ 0x00000000 00000000 00100000 00008000	0x00000000 00000000 00000000 00200000 0x00000000 00000000 00100000 00000000	92%
	640[2]	5	0	2^{-7}	$\Delta_0 =$ 0x40000000 12000000 00002000 00000000 $\Delta_1 =$ 0x00000000 00000000 00000000 02000000	$\nabla_0 =$ 0x00001200 00000000 20000000 00000000 $\nabla_1 =$ 0x00000000 00000000 00000200 00000010	0x40000000 02000000 00002000 00000000 0x20000000 00004000 00000200 00000000	22%
	1024[1]	16	0	2^{-24}	$\Delta_0 =$ 0x00000000 00000000 00000800 00000000 $\Delta_1 =$ 0x00000000 00000000 00000800 00000000	$\nabla_0 =$ 0x00000000 00000000 00000800 00000000 $\nabla_1 =$ 0x00000000 00000000 00000800 00000000	0x00000000 04000000 00000000 00000040 0x00000000 04000000 00000000 00000040	100%
TinyJambu192	512	0	0	1	$\Delta_0 =$ 0x40902201 80008120 4c000000 00000000 $\Delta_1 =$ 0x00000000 00000000 00000401 80008100	$\nabla_0 =$ 0x00000000 00000000 08000000 00000000 $\nabla_1 =$ 0x00000000 00000000 00000400 00000020	0x00000401 80008120 4c000000 00000000 00000000 00000000 0x00000000 00000000 00000400 00000000 08000000 00000000	100%
	640[1]	4	0	2^{-6}	$\Delta_0 =$ 0x12000000 00002000 00000000 40000000 $\Delta_1 =$ 0x00000000 00000000 00000000 00040000	$\nabla_0 =$ 0x00000000 00000200 00000000 00000000 $\nabla_1 =$ 0x00000000 00000000 00040000 00002000	0x00000000 00000000 00000000 40000000 00000000 00000000 0x00040000 00000000 00000000 00000000 00000000 00000000	72%
	1152[1]	12	0	2^{-18}	$\Delta_0 =$ 0x00000000 00000000 00000000 00040000 $\Delta_1 =$ 0x00000000 00000000 00000000 00040000	$\nabla_0 =$ 0x00000000 00000200 00000000 00000000 $\nabla_1 =$ 0x00000000 00000200 00000000 00000000	0x00002000 00000002 00000000 00040000 00000000 00040000 0x01000000 00000200 00000000 00000200 00000010 00000000	84%
TinyJambu256	640	0	0	1	$\Delta_0 =$ 0x40180400 22008030 08000000 00000000 $\Delta_1 =$ 0x00000000 00000000 00000000 22008030	$\nabla_0 =$ 0x0010400d 26c00020 80000000 00000000 $\nabla_1 =$ 0x00000000 00000000 0000000d 26c00020	0x00000000 22008030 08000000 00000000 00000000 00000000 00000000 00000000 0x00000000 00000000 0000000d 26c00020 80000000 00000000 00000000 00000000	100%
	1280[1]	8	0	2^{-12}	$\Delta_0 =$ 0x00000000 00000000 40000000 00000000 $\Delta_1 =$ 0x00000000 00000000 00000000 00000000	$\nabla_0 =$ 0x01000000 00000000 00000000 00000000 $\nabla_1 =$ 0x00000000 00000000 00000000 00000000	0x00002000 00000000 40000000 00000000 00000000 00000000 40000000 02000000 0x01000000 00080000 00000080 00000000 01000000 00000000 00000000 00000000	91%

In the case of a 512-round cipher, our analysis yielded an optimal solution involving four ladder switches positioned at 21, 36, 261, and 502. In this specific path, two switches were activated during the initial 256 rounds, while the other two switches became active during the final 256 rounds. This configuration led to a boomerang distinguisher with a probability of $2^{-2} \cdot 2^{-4} = 2^{-6}$.

In addition to our findings for various round counts, we encountered intriguing results when exploring boomerang distinguishers in a 640-round cipher. The optimal solution in this scenario featured five ladder switches strategically positioned at rounds 12, 172, 187, 476, and 491. Within this trail, three of these switches were actively involved during the initial 320 rounds, while the remaining two switches occured in the final 320 rounds. As a result, this arrangement gave rise to a boomerang distinguisher with a probability calculated as $2^{-3} \cdot 2^{-4} = 2^{-7}$.

For a cipher spanning 1024 rounds, we uncovered a sub-optimal boomerang path characterized by the presence of sixteen ladder switches. Eight of these switches were active during the initial 512 rounds, and the remaining eight switches came into play during the subsequent 512 rounds. This specific configuration led to a boomerang distinguisher with a probability of $2^{-8} \cdot 2^{16} = 2^{-24}$.

Table 9: Related-key Amplified Boomerang Distinguishers of TinyJambu Variants

Variants	Rounds	Distinguishing Probability	Upper trail Input Difference Lower Trail Output Difference	Upper Key Difference Lower Key Difference	Success Probability
TinyJambu128	384	1	Δ_0 = 0x00102400000000204000000000000000 ∇_1 = 0x00000000000000000000002000000010	0x00004000000000204000000000000000 0x04000000000000000000002000000000	100%
	512	2^{-6}	Δ_0 = 0x00090000000000010000000000200000 ∇_1 = 0x00000000000000000001000000008000	0x00000000000000000000000000200000 0x00000000000000000001000000000000	99%
	640	2^{-7}	Δ_0 = 0x40000000120000000000200000000000 ∇_1 = 0x00000000000000000000002000000010	0x40000000020000000000200000000000 0x20000000000040000000020000000000	62%
	1024	2^{-19}	Δ_0 = 0x00000000000000000000080000000000 ∇_1 = 0x00000000000000000000080000000000	0x00000000400000000000000000000040 0x00000000400000000000000000000040	99%
TinyJambu192	512	1	Δ_0 = 0x40902201800081204c00000000000000 ∇_1 = 0x00000000000000000000040000000020	0x00000401800081204c000000000000000000000000000000 0x000000000000000000000400000000000800000000000000	100%
	640	2^{-6}	Δ_0 = 0x12000000000002000000000040000000 ∇_1 = 0x00000000000000000004000000002000	0x000000000000000000000000400000000000000000000000 0x000400000000000000000000000000000000000000000000	99%
	1152	2^{-18}	Δ_0 = 0x00000000000000000000000000040000 ∇_1 = 0x00000000000002000000000000000000	0x000020000000000020000000000040000000000000040000 0x010000000000020000000000000020000000010000000000	99%
TinyJambu256	640	1	Δ_0 = 0x40180400220080300800000000000000 ∇_1 = 0x00000000000000000000000d26c00020	0x0000000022008030080000000000000000000000000000000000000000000000 0x00000000000000000000000d26c0002080000000000000000000000000000000	100%
	1280	2^{-12}	Δ_0 = 0x00000000000000004000000000000000 ∇_1 = 0x00000000000000000000000000000000	0x0000200000000000400000000000000000000000000000000000400000002000000 0x0100000000800000000080000000001000000000000000000000000000000000	99%

Furthermore, our exploration extended to related-key boomerang distinguishers, where we successfully identified deterministic distinguishers spanning 512 and 640 rounds for TinyJambu-192 and TinyJambu-256, respectively. In the case of full rounds for TinyJambu-192, we discovered a sub-optimal boomerang path featuring twelve ladder switches, resulting in a distinguishing probability of 2^{-18}. Similarly, for the complete rounds of TinyJambu-1280, we encountered a sub-optimal solution characterized by eight ladder switches, resulting in a probability of 2^{-18}.

We have summarized these discovered trails and their respective characteristics in Table 8. Furthermore, our exploration extended to finding amplified boomerang trails by considering sub-optimal solutions, thereby increasing the overall probability of these distinguishers. Detailed information about these amplified boomerang trails and their success probabilities can also be found in Table 9.

Experimental Results Under both single-key and related-key settings, we have rigorously conducted practical verifications for all the boomerang paths of TinyJambu presented in Tables 6,8. These paths were discovered using the MILP (Mixed-Integer Linear Programming) search method. This meticulous validation process ensures the reliability and practical applicability of our reported boomerang paths. Furthermore, we have subjected our findings related to the best amplified boomerang attacks on TinyJambu, as outlined in Tables 7,9, to thorough validation across scenarios involving both single-key and related-key settings. For a comprehensive understanding of our verification process, as well as access to detailed results and supporting information, we refer to [1]. These verifications constitute substantial evidence that our reported boomerang paths, success rates, and findings have undergone rigorous real-world testing and analysis, affirming their reliability and practical utility.

6 Attacks on KATAN

The KATAN cipher, as described in [7], is a family of NLFSR-based block ciphers with three variants corresponding to block sizes of 32, 48, and 64 bits. The state of the KATAN cipher consists of two registers, namely L_1 and L_2, which have different sizes based on their state sizes. All variants of KATAN employ 254 rounds and use an 80-bit key to derive 508 subkey bits through a linear feedback shift register (LFSR) in the key schedule function. In the round function of KATAN, both registers, L_1 and L_2, function as NLFSRs. The feedback bit of L_1 is fed into the least significant bit (LSB) of L_2, and vice versa. Additionally, the state bits are shifted by one position from the least significant bit (LSB) to the most significant bit (MSB) in each round. For the KATAN48 and KATAN64 variants, the round function is repeated 2 and 3 times respectively, using the same subkeys. For more detailed information about the KATAN cipher, please refer to [7].

In previous research, Isobe et al.[15] introduced a related-key boomerang distinguisher for KATAN32 consisting of 140 rounds, achieving a distinguisher probability of $2^{-27.2}$. Building upon their work, Chen et al.[8] further enhanced the boomerang distinguisher by employing the branch-and-bound method, resulting in an improved probability of $2^{-26.58}$. These advancements demonstrated the vulnerability of KATAN32 to related-key boomerang attacks.

In a distinct research direction, a recent work by Jana et al. [16] introduced the DEEPAND model, specifically designed for analyzing the impact of multiple AND gates within NLFSR-based ciphers like KATAN. This model capitalizes on exploiting correlations among these AND gates to enhance the probability of differential trails. Through this technique, the researchers successfully elevated the efficiency of a differential trail. Leveraging the capabilities of the DEEPAND model, the authors achieved significant advancements. They managed to identify and establish highly effective differential trails, encompassing a remarkable 70 rounds. This achievement resulted in the development of a notably potent related-key boomerang distinguisher. By employing this innovative approach, a deeper understanding of the cipher's vulnerabilities was obtained, and this, in turn, facilitated the creation of more powerful and effective attack strategies.

6.1 Specification

The KATAN family is an efficient hardware-oriented block cipher, featuring three variants: KATAN32, KATAN48, and KATAN64, designed for 32-bit, 48-bit, and 64-bit block sizes, respectively. All variants employ 254 rounds and utilize the non-linear functions $\mathcal{NF}1$ and $\mathcal{NF}2$. They share a common LFSR-based key schedule that takes an 80-bit key as input. The fundamental structure of the KATAN cipher involves loading plaintext into two registers, L_1 and L_2. During each round, several bits from these registers are processed by the non-linear functions $\mathcal{NF}1$ and $\mathcal{NF}2$, and the results are loaded into the least significant bits of the registers. The key schedule function expands the 80-bit user-provided key k_i $(0 \leq i < 80)$ into a 508-bit subkey sk_i $(0 \leq i < 508)$ using specific linear operations.

$$sk_i = \begin{cases} k_i, & 0 \leq i < 80 \\ k_{i-80} \oplus k_{i-61} \oplus k_{i-50} \oplus k_{i-13}, & 80 \leq x < 508. \end{cases}$$

Also, the two non-linear functions are defined as follows:

$$\mathcal{NF}_1(L_1) = L_1[x_1] \oplus L_1[x_2] \oplus (L_1[x_3] \cdot L_1[x_4]) \oplus (L_1[x_5] \cdot IR) \oplus k_a$$

$$\mathcal{NF}_2(L_2) = L_2[y_1] \oplus L_2[y_2] \oplus (L_2[y_3] \cdot L_2[y_4]) \oplus (L_2[y_5] \cdot L_2[y_6])) \oplus k_b,$$

The KATAN cipher employs a predefined round constant known as IR (details provided in [**?**]), along with two subkey bits, k_a and k_b, in its operations. The selection of specific bits, denoted as x_i for $1 \leq i \leq 5$ and y_i for $1 \leq i \leq 6$, is variant-specific and outlined in Table 10. In the case of KATAN32, the i-th round function, illustrated in Figure 7, assigns k_a the value of k_{2i} and k_b the

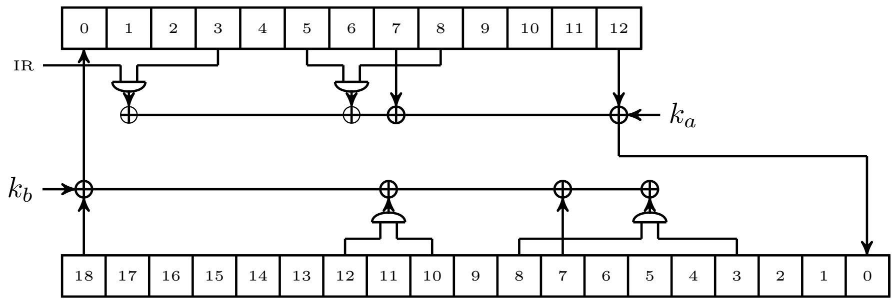

Fig. 7: Round Function of KATAN [32]

value of k_{2i+1}. After 254 rounds, the values contained in the registers are output as ciphertext. In KATAN48, a unique feature is the application of the non-linear functions $\mathcal{NF}_1$ and $\mathcal{NF}_2$ twice within a single round. Initially, the first pair of $\mathcal{NF}_1$ and $\mathcal{NF}_2$ is applied, and following the update of the registers, they are reapplied using the same subkeys. Likewise, in the KATAN64 variant, each round involves three consecutive applications of $\mathcal{NF}_1$ and $\mathcal{NF}_2$ with the same key bits. More details regarding the specifications of the KATAN family of ciphers can be found in [7].

Table 10: Parameters of KATAN Variants

KATAN Variants	$\mid L_1 \mid$	$\mid L_2 \mid$	x_1	x_2	x_3	x_4	x_5	y_1	y_2	y_3	y_4	y_5	y_6
KATAN [32]	13	19	12	7	8	5	3	18	7	12	10	8	3
KATAN [48]	19	29	18	12	15	7	6	28	19	21	13	15	6
KATAN [64]	25	39	24	15	20	11	9	38	25	33	21	14	9

6.2 MILP Modelling

In our approach to attacking KATAN, we have chosen to simplify things by narrowing our focus from four planes to just two. This decision aims to make the attack more efficient in terms of both computation and time. When it comes to using MILP modeling for attacking KATAN, we follow a straightforward strategy. We treat the KATAN cipher as if it is the middle part, denoted as E_m, in the model. The main goal is to reduce the use of ladder/And switches as much as possible. This emphasis on minimizing these specific switches helps us create a powerful boomerang distinguisher that is not only efficient but also highly effective in exploiting the cipher's vulnerabilities.

Table 11: Related-key Boomerang Distinguishers of KATAN32 through MILP Search

Rounds	Ladder Switch	And Switch	Distinguishing Probability	Upper Trail Differences	Upper Trail Differences	Key Difference (Upper Trail)	Key Difference (Lower Trail)	Success Probability
120	5	2	2^{-11}	$\varDelta_0 =$ 0x00042000 $\varDelta_1 =$ 0x08000002	$\nabla_0 =$ 0x8400c010 $\nabla_1 =$ 0x01000002	0x40110020000000000802	0x026008401808a041a660	86.6%
	5	2	2^{-11}	$\varDelta_0 =$ 0x00004000 $\varDelta_1 =$ 0x00f80084	$\nabla_0 =$ 0x20058400 $\nabla_1 =$ 0x01000000	0x00010044008000000200	0x241157c289ba4c354b3b	86.5%
140[1]	14	0	2^{-21}	$\varDelta_0 =$ 0x00062000 $\varDelta_1 =$ 0x00400801	$\nabla_0 =$ 0xa4024010 $\nabla_1 =$ 0x00b80084	0x4051 00200000 0000080a	0x63c4 cf451630 862a0c25	97%
	10	4	2^{-21}	$\varDelta_0 =$ 0x80031000 $\varDelta_1 =$ 0x01200400	$\nabla_0 =$ 0xa4024010 $\nabla_1 =$ 0x00b80084	0x0140 00800000 00002029	0x63c4 cf451630 762a0c25	25%

6.3 Results on KATAN

Related-key Boomerang Attacks Through the application of our MILP model to KATAN32, we have successfully uncovered a related-key boomerang distinguisher spanning up to 120 rounds. Our optimal solution entails the activation of two And switches at positions 32 and 35, as well as five ladder switches at positions 57, 61, 64, 66, and 68. Additionally, we have identified another optimal solution with the same configuration: two And switches at positions 95 and 98, and five ladder switches at positions 25, 28, 56, 60, and 62. Notably, in both cases, three switches are engaged in the first 60 rounds, while four switches are triggered in the subsequent 60 rounds. Consequently, the probability of the boomerang distinguisher is determined to be $r \cdot q^2 = 2^{-3} \cdot 2^{-8} = 2^{-11}$.

In our pursuit of effective boomerang trails spanning 140 rounds, we have uncovered multiple optimal solutions using our MILP search. Among these, one solution stands out prominently. This particular solution involves the activation of fourteen ladder switches at distinct positions: 32, 35, 57, 60, 62, 69, 71, 74, 76, 78, 105, 108, and 136. This boomerang boasts a probability of $r \cdot q^2 = 2^{-7} \cdot 2^{-14} = 2^{-21}$. Another noteworthy solution we have identified features four And switches at positions 1, 58, 61, and 136, accompanied by ten ladder switches at positions 33, 36, 63, 68, 71, 74, 76, 78, 105, and 108. These intricate details of the optimal boomerang trails for 140 rounds are meticulously documented in Table 11.

Table 12: Related-key Amplified Boomerang Distinguishers of KATAN32

Rounds	Distinguishing Probability	Input Difference (Upper Trail)	Output Difference (Lower Trail)	Key Difference (Upper Trail)	Key Difference (Lower Trail)	Success Probability
120	2^{-7}	$\varDelta_0 = 0x00042000$	$\nabla_1 = 0x01000002$	$0x4011\ 00200000\ 00000802$	$0x0260\ 08401808\ a041a660$	64%
140	2^{-15}	$\varDelta_0 = 0x00062000$	$\nabla_1 = 0x00b80084$	$0x4051\ 00200000\ 0000080a$	$0x63c4\ cf451630\ 862a0c25$	70%

Table 13: Single-key Boomerang Distinguishers of KATAN32 through MILP Search

Rounds	Ladder Switch	And Switch	Distinguishing Probability	Upper Trail Differences	Lower Trail Differences	Success Probability
60	9	4	2^{-19}	$\Delta_0 =$ 0x00020040 $\Delta_1 =$ 0x00100210	$\nabla_0 =$ 0x0001a020 $\nabla_1 =$ 0x00080108	71%
	8	5	2^{-19}	$\Delta_0 =$ 0x00034040 $\Delta_1 =$ 0x00100210	$\nabla_0 =$ 0x00018020 $\nabla_1 =$ 0x00080108	70%
72	13	9	2^{-31}	$\Delta_0 =$ 0x00020040 $\Delta_1 =$ 0x0420840a	$\nabla_0 =$ 0x8004c600 $\nabla_1 =$ 0x00080108	−−
84	14	10	2^{-34}	$\Delta_0 =$ 0x10042080 $\Delta_1 =$ 0x00400840	$\nabla_0 =$ 0x10068080 $\nabla_1 =$ 0x00400840	−−

Our dedicated efforts are directed towards identifying efficient and potent boomerang distinguishers within the domain of cryptographic ciphers. Additionally, we have explored amplified boomerang trials through suboptimal solutions, further enhancing the overall probability of these distinguishers. A comprehensive list of these trails, along with their amplified probabilities, is provided in Table 12.

Single-key Boomerang Attacks In the context of single-key settings, we employed an MILP model to successfully identify a boomerang distinguisher for various numbers of rounds. Here are the details of our findings:

For a 60-round cipher, we discovered two optimal solutions for the boomerang distinguisher. In the first solution, the boomerang path involved nine ladder

Table 14: Amplified Boomerang Distinguishers of KATAN32

Rounds	Distinguishing Probability	Input Difference (Upper Trail)	Output Difference (Lower Trail)	Success Probability
60	2^{-14}	$\Delta_0 =$ 0x00020040	$\nabla_1 =$ 0x00080108	72%
	2^{-14}	$\Delta_0 =$ 0x00034040	$\nabla_1 =$ 0x00080108	70%
72	2^{-24}	$\Delta_0 =$ 0x00020040	$\nabla_1 =$ 0x00080108	65%
84	2^{-30}	$\Delta_0 =$ 0x10042080	$\nabla_1 =$ 0x00400840	60%

switches occurring at positions 18, 21, 24, 29, 33, 35, 37, 49, and 52, along with four AND switches at positions 2, 4, 6, and 55. In the second solution, the path consisted of eight ladder switches at positions 18, 21, 24, 29, 33, 35, 37, and 49, along with five AND switches at positions 2, 4, 6, 52, and 55. In both cases, seven switches were active during the initial 60 rounds, and six switches were active during the latter 60 rounds. As a result, the probability of the distinguisher was computed as $r \cdot q^2 = 2^{-7} \cdot 2^{-12} = 2^{-19}$.

Similarly, for a 72-round cipher, we identified a boomerang path comprising a total of twenty-two ladder and AND switches. Thirteen switches were active during the first 36 rounds, and nine switches were active during the last 36 rounds. This yielded a probability of $2^{-13} \cdot 2^{-18} = 2^{-31}$ for the distinguisher's success.

Finally, in the case of an 84-round cipher, our investigation led to the discovery of a boomerang path involving thirty-four ladder and AND switches. Fourteen switches were active during the upper 42 rounds, and ten switches were active during the lower 42 rounds. Consequently, the probability of this boomerang distinguisher was calculated as $2^{-14} \cdot 2^{-20} = 2^{-34}$.

We also delved into the exploration of amplified boomerang trails through optimal solutions to enhance the overall probability of these distinguishers. The details of these trails and their amplified probabilities are given in Table 14.

Experimental Results We have meticulously conducted practical validations for all the boomerang paths associated with KATAN32, as presented in Tables 13 and 11. These paths were discovered using the MILP (Mixed-Integer Linear Programming) search method, and we rigorously assessed their validity under both single-key and related-key settings. This comprehensive validation process ensures the dependability and practical applicability of the reported boomerang paths. Furthermore, our investigations into the best amplified boomerang attacks on KATAN32, which are detailed in Tables 14 and 12, have undergone extensive verification across various scenarios, encompassing both single-key and related-key settings. For a more comprehensive understanding of our validation process, detailed results, and supporting information, we refer to [1]. These rigorous validations provide robust evidence that our reported boomerang paths, success rates, and discoveries have been subjected to stringent real-world testing and analysis, affirming their practical relevance and reliability.

7 Discussion

The findings presented in this work represent a significant leap forward in the field of cryptanalysis, specifically in the domain of boomerang attacks on non-linear feedback shift register (NLFSR)-based block ciphers such as TinyJambu and KATAN32. The successful identification of enhanced boomerang distinguishers through our proposed methodology underscores its effectiveness. This discussion will delve into the implications of these discoveries, their broader relevance within the cryptographic landscape, and potential areas for future research.

Our approach employs a two-plane method in the Mixed Integer Linear Programming (MILP) search, a strategy aimed at optimizing efficiency and expanding the scope of coverage across rounds. However, it is worth noting that in certain instances, the success rate of the boomerang path identified through the MILP search may be relatively low. One possible reason behind this phenomenon is that, for the upper part (i.e., the E_m part) of the cipher, a ladder or And switch at a specific round may transform into Trail switch due to the differential propagation through the lower part (E_1). To present a more accurate model, assumptions considering equal differences in the opposite planes can be relaxed which can leverage on the Trail switches. This presents an intriguing open problem: how can constraints be integrated into the MILP model to effectively bypass these paths and discover the optimal boomerang path? Additionally, there is room for improving the MILP model's efficiency to facilitate the exploration of a larger number of rounds.

Another avenue for future research lies in the exploration of unequal round allocations between E_m and E_1. Currently, our approach assumes an equal number of rounds for both components. Investigating whether an uneven distribution of rounds can lead to the discovery of superior boomerang paths is an intriguing question that merits further investigation.

The practical implications of the improved boomerang distinguishers are substantial. They empower cryptanalysts with more potent tools to assess the security of cryptographic algorithms, potentially revealing vulnerabilities that may have remained hidden using conventional boomerang methods. Addressing the challenge of the vast number of variables in the MILP approach, we intend to explore the utilization of four planes within the MILP to refine the search for optimal boomerang paths through various switches, including other switches. Additionally, our future work will focus on systematically calculating the overall probability for amplified boomerangs, further enhancing our ability to analyze and assess the security of cryptographic systems.

Finally, this research demonstrates the evolving landscape of cryptanalysis and underscores the need for continued innovation in the quest for robust cryptographic solutions. The challenges identified here offer exciting opportunities for future investigations, ultimately contributing to the advancement of cryptographic theory and practice.

8 Conclusion

To sum up, our study focused on a technique called boomerang attacks, which are used to break block ciphers. Specifically, we were interested in ciphers that use a particular structure known as NLFSR. We investigated different ways to make these attacks more effective, with a special focus on a type of operation called ladder or And switches.

In our exploration, we made an interesting discovery. The usual method to calculate the likelihood of success in these attacks might not always give us the right answer. We came up with a new way to estimate this probability, which turned out to be different from what was commonly thought. This finding has implications for how well these attacks can work in practice.

We then introduced a new approach to these attacks. We concentrated on using ladder or And switches exclusively. This approach is somewhat similar to crafting a unique type of sandwich attack. By doing this, we were able to uncover vulnerabilities in NLFSR-based ciphers like TinyJambu and KATAN32.

In conclusion, Our study does not just provide new insights into these boomerang attacks; it equips experts with improved strategies for making attacks more successful. In the future, these findings will play a vital role in enhancing the security of NLFSR-based block ciphers.

References

1. Boomerang Verification of TinyJambu and KATAN32. https://drive.google.com/drive/u/4/folders/1l6VIrCZdIchHpPmh3vdVkHTcaBzI0gCK?hl=en
2. National Institute of Standards and Technology (NIST): Lightweight cryptography standardization process (2019). https://csrc.nist.gov/projects/lightweight-cryptography
3. Biham, E., Dunkelman, O., Keller, N.: The rectangle attack - rectangling the serpent. In: Pfitzmann, B. (ed.) Advances in Cryptology - EUROCRYPT 2001, International Conference on the Theory and Application of Cryptographic Techniques, Innsbruck, Austria, May 6-10, 2001, Proceeding. Lecture Notes in Computer Science, vol. 2045, pp. 340–357. Springer (2001). https://doi.org/10.1007/3-540-44987-6_21, https://doi.org/10.1007/3-540-44987-6_21
4. Biham, E., Shamir, A.: Differential Cryptanalysis of the Data Encryption Standard. Springer (1993). https://doi.org/10.1007/978-1-4613-9314-6, https://doi.org/10.1007/978-1-4613-9314-6
5. Biryukov, A., Cannière, C.D., Dellkrantz, G.: Cryptanalysis of SAFER++. In: Boneh, D. (ed.) Advances in Cryptology - CRYPTO 2003, 23rd Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 2003, Proceedings. Lecture Notes in Computer Science, vol. 2729, pp. 195–211. Springer (2003). https://doi.org/10.1007/978-3-540-45146-4_12, https://doi.org/10.1007/978-3-540-45146-4_12
6. Biryukov, A., Khovratovich, D.: Related-key cryptanalysis of the full AES-192 and AES-256. In: Matsui, M. (ed.) Advances in Cryptology - ASIACRYPT 2009, 15th International Conference on the Theory and Application of Cryptology and Information Security, Tokyo, Japan, December 6-10, 2009. Proceedings. Lecture Notes in Computer Science, vol. 5912, pp. 1–18. Springer (2009). https://doi.org/10.1007/978-3-642-10366-7_1, https://doi.org/10.1007/978-3-642-10366-7_1
7. Cannière, C.D., Dunkelman, O., Knezevic, M.: KATAN and KTANTAN - A family of small and efficient hardware-oriented block ciphers. In: Clavier, C., Gaj, K. (eds.) Cryptographic Hardware and Embedded Systems - CHES 2009, 11th International Workshop, Lausanne, Switzerland, September 6-9, 2009, Proceedings. Lecture Notes in Computer Science, vol. 5747, pp. 272–288. Springer (2009). https://doi.org/10.1007/978-3-642-04138-9_20, https://doi.org/10.1007/978-3-642-04138-9_20

8. Chen, J., Teh, J., Su, C., Samsudin, A., Fang, J.: Improved (related-key) attacks on round-reduced KATAN-32/48/64 based on the extended boomerang framework. In: Liu, J.K., Steinfeld, R. (eds.) Information Security and Privacy - 21st Australasian Conference, ACISP 2016, Melbourne, VIC, Australia, July 4-6, 2016, Proceedings, Part II. Lecture Notes in Computer Science, vol. 9723, pp. 333–346. Springer (2016). https://doi.org/10.1007/978-3-319-40367-0_21, https://doi.org/10.1007/978-3-319-40367-0_21
9. Cid, C., Huang, T., Peyrin, T., Sasaki, Y., Song, L.: Boomerang connectivity table: A new cryptanalysis tool. In: Nielsen, J.B., Rijmen, V. (eds.) Advances in Cryptology - EUROCRYPT 2018 - 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tel Aviv, Israel, April 29 - May 3, 2018 Proceedings, Part II. Lecture Notes in Computer Science, vol. 10821, pp. 683–714. Springer (2018). https://doi.org/10.1007/978-3-319-78375-8_22, https://doi.org/10.1007/978-3-319-78375-8_22
10. Dunkelman, O., Ghosh, S., Lambooij, E.: Full round zero-sum distinguishers on tinyjambu-128 and tinyjambu-192 keyed-permutation in the known-key setting. In: Isobe, T., Sarkar, S. (eds.) Progress in Cryptology - INDOCRYPT 2022 - 23rd International Conference on Cryptology in India, Kolkata, India, December 11-14, 2022, Proceedings. Lecture Notes in Computer Science, vol. 13774, pp. 349–372. Springer (2022). https://doi.org/10.1007/978-3-031-22912-1_16, https://doi.org/10.1007/978-3-031-22912-1_16
11. Dunkelman, O., Ghosh, S., Lambooij, E.: Practical related-key forgery attacks on full-round tinyjambu-192/256. IACR Trans. Symmetric Cryptol. **2023**(2), 176–188 (2023). https://doi.org/10.46586/tosc.v2023.i2.176-188, https://doi.org/10.46586/tosc.v2023.i2.176-188
12. Dunkelman, O., Keller, N., Shamir, A.: A practical-time related-key attack on the KASUMI cryptosystem used in GSM and 3g telephony. In: Rabin, T. (ed.) Advances in Cryptology - CRYPTO 2010, 30th Annual Cryptology Conference, Santa Barbara, CA, USA, August 15-19, 2010. Proceedings. Lecture Notes in Computer Science, vol. 6223, pp. 393–410. Springer (2010). https://doi.org/10.1007/978-3-642-14623-7_21, https://doi.org/10.1007/978-3-642-14623-7_21
13. Dunkelman, O., Keller, N., Shamir, A.: A practical-time related-key attack on the KASUMI cryptosystem used in GSM and 3g telephony. J. Cryptol. **27**(4), 824–849 (2014). https://doi.org/10.1007/s00145-013-9154-9, https://doi.org/10.1007/s00145-013-9154-9
14. Hadipour, H., Bagheri, N., Song, L.: Improved rectangle attacks on SKINNY and CRAFT. IACR Trans. Symmetric Cryptol. **2021**(2), 140–198 (2021). https://doi.org/10.46586/tosc.v2021.i2.140-198, https://doi.org/10.46586/tosc.v2021.i2.140-198
15. Isobe, T., Sasaki, Y., Chen, J.: Related-key boomerang attacks on KATAN32/48/64. In: Boyd, C., Simpson, L. (eds.) Information Security and Privacy - 18th Australasian Conference, ACISP 2013, Brisbane, Australia, July 1-3, 2013. Proceedings. Lecture Notes in Computer Science, vol. 7959, pp. 268–285. Springer (2013). https://doi.org/10.1007/978-3-642-39059-3_19, https://doi.org/10.1007/978-3-642-39059-3_19
16. Jana, A., Rahman, M., Saha, D.: DEEPAND: in-depth modeling of correlated AND gates for nlfsr-based lightweight block ciphers. IACR Cryptol. ePrint Arch. p. 1123 (2022), https://eprint.iacr.org/2022/1123
17. Kelsey, J., Kohno, T., Schneier, B.: Amplified boomerang attacks against reduced-round MARS and serpent. In: Schneier, B. (ed.) Fast Software Encryption,

7th International Workshop, FSE 2000, New York, NY, USA, April 10-12, 2000, Proceedings. Lecture Notes in Computer Science, vol. 1978, pp. 75–93. Springer (2000). https://doi.org/10.1007/3-540-44706-7_6, https://doi.org/10.1007/3-540-44706-7_6
18. Murphy, S.: The return of the cryptographic boomerang. IEEE Trans. Inf. Theory **57**(4), 2517–2521 (2011). https://doi.org/10.1109/TIT.2011.2111091, https://doi.org/10.1109/TIT.2011.2111091
19. Saha, D., Sasaki, Y., Shi, D., Sibleyras, F., Sun, S., Zhang, Y.: On the security margin of tinyjambu with refined differential and linear cryptanalysis. IACR Trans. Symmetric Cryptol. **2020**(3), 152–174 (2020). https://doi.org/10.13154/tosc.v2020.i3.152-174, https://doi.org/10.13154/tosc.v2020.i3.152-174
20. Sibleyras, F., Sasaki, Y., Todo, Y., Hosoyamada, A., Yasuda, K.: Birthday-bound slide attacks on tinyjambu's keyed-permutations for all key sizes. In: Cheng, C., Akiyama, M. (eds.) Advances in Information and Computer Security - 17th International Workshop on Security, IWSEC 2022, Tokyo, Japan, August 31 - September 2, 2022, Proceedings. Lecture Notes in Computer Science, vol. 13504, pp. 107–127. Springer (2022). https://doi.org/10.1007/978-3-031-15255-9_6, https://doi.org/10.1007/978-3-031-15255-9_6
21. Song, L., Qin, X., Hu, L.: Boomerang connectivity table revisited. application to SKINNY and AES. IACR Trans. Symmetric Cryptol. **2019**(1), 118–141 (2019). https://doi.org/10.13154/tosc.v2019.i1.118-141, https://doi.org/10.13154/tosc.v2019.i1.118-141
22. Wagner, D.A.: The boomerang attack. In: Knudsen, L.R. (ed.) Fast Software Encryption, 6th International Workshop, FSE '99, Rome, Italy, March 24-26, 1999, Proceedings. Lecture Notes in Computer Science, vol. 1636, pp. 156–170. Springer (1999). https://doi.org/10.1007/3-540-48519-8_12, https://doi.org/10.1007/3-540-48519-8_12
23. Wang, H., Peyrin, T.: Boomerang switch in multiple rounds. application to AES variants and deoxys. IACR Trans. Symmetric Cryptol. **2019**(1), 142–169 (2019). https://doi.org/10.13154/tosc.v2019.i1.142-169, https://doi.org/10.13154/tosc.v2019.i1.142-169
24. Wu, H., Huang, T.: TinyJAMBU: A Family of Lightweight Authenticated Encryption Algorithms, https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/spec-doc/TinyJAMBU-spec.pdf, nIST LWC Round 1 Candidate, 2019
25. Wu, H., Huang, T.: TinyJAMBU: A Family of Lightweight Authenticated Encryption Algorithms (Version 2), https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptography/documents/finalist-round/updated-spec-doc/tinyjambu-spec-final.pdf, nIST LWC Finalist, 2021
26. Yang, Q., Song, L., Sun, S., Shi, D., Hu, L.: New properties of the double boomerang connectivity table. IACR Trans. Symmetric Cryptol. **2022**(4), 208–242 (2022). https://doi.org/10.46586/tosc.v2022.i4.208-242, https://doi.org/10.46586/tosc.v2022.i4.208-242