The ISC Int'l Journal of Information Security
ISeCure

October 2025, Volume 17, Number 3 (pp. 1–9)
http://www.isecure-journal.org

Presented at the ISCISC'2025 in TEHRAN, Iran.

Integral Attack on CHILOW **

Akram Khalesi [1,*], and Zahra Ahmadian [2]
[1] Research Center for Development of Advanced Technologies, Tehran, Iran.
[2] Department of Electrical Engineering, Shahid Beheshti University, Tehran, Iran.

ARTICLE INFO.

Keywords:
CHILOW, Division Property, Integral attack

Type:

doi:

Abstract

CHILOW is a family of tweakable block ciphers introduced at Eurocrypt 2025, prioritizing decryption speed over encryption speed. This is achieved through a low-latency non-linear layer of degree two within the round function and a minimal number of rounds. As a result, CHILOW presents an appealing target for attacks that exploit its algebraic properties. These characteristics, along with the strict query limitations imposed by the designers, motivate our investigation into CHILOW's security against integral attacks leveraging the division property. We have identified several integral distinguishers, which vary in data complexity and the number of balanced output bits. Specifically, for CHILOW-(32+τ), we derived a 4-round distinguisher with 15 constant bits in the input, in which all the 32 output bits are balanced. However, the longest integral distinguisher that complies with query limitations extends up to 3 rounds. For CHILOW-40, integral distinguishers up to 5 rounds are detected; however, only those spanning three rounds meet the query constraints. Furthermore, we have explored the potential for extending these distinguishers to key-recovery attacks and analyzed their complexity. Using the 3-round distinguisher on CHILOW-(32+τ), we propose key recovery attack with a 32-bit advantage, data complexity of 2^{40} chosen ciphertexts and time complexity of 2^{40} decryptions, all within the query limits. Therefore, by performing an exhaustive search over the remaining key candidates, a single candidate for the master key can be recovered, resulting in an overall attack time complexity of 2^{96} decryptions. Additionally, we present an integral key-recovery attack on the 6-round version of CHILOW-(32+τ) with a data complexity of 2^8 chosen ciphertexts and a time complexity of $2^{102.6}$ encryptions. This attack only obtains information from the tweaks of the last three rounds, and using this information to recover the master key will be the subject of future research.

1 Introduction

Designing innovative cryptographic algorithms to meet the changing security demands is vital in cryptography. Although a wide variety of cryptographic algorithms already exist, researchers continue to propose new designs and structures to address emerging challenges or enhance existing methods. An example is the introduction of three constructions for Authenticated Code Encryption (ACE) and their implementation through a family of tweakable block ciphers called CHILOW, presented at Eurocrypt 2025 [1].

The newly developed primitives, CHILOW-(32+τ) and CHILOW-40, are particularly suitable for scenarios where decryption speed is more critical than encryption speed. For instance, in ACE, decryption often dominates because encrypted instructions are frequently decrypted for execution, while encryption occurs less frequently, such as during software updates. This is supported by the introduction of a new family of non-linear layer called CHICHI, which is based on the well-known non-linear function χ utilized in Keccak [2], Ascon [3] and Koala [4].

Integral attack is a powerful cryptanalysis technique used against block ciphers, where attackers seek to identify sets of inputs whose outputs sum to zero at specific positions. Initially, methods for detecting integral distinguishers relied on tracking the propagation of integral properties or estimating the algebraic degree. However, with the advent of the division property, these earlier techniques became outdated.

The division property [5], a robust tool for uncovering integral distinguishers, exists in two forms. The first, known as the two-subset division property [5], is less precise but simpler to implement in automated cryptanalysis. The second, the three-subset division property [6], offers higher accuracy while its automation is more challenging [7–9].

The first method, utilized by Todo for automated search for integral distinguishers based on the division property, is based on the breadth-first approach [5]. Afterward, Xiang et al. proposed an MILP model for the two-subset division property, which became the foundation of its future work [10].

In this paper, we analyze the security of CHILOW-(32+τ) and CHILOW-40 against integral attacks leveraging the division property. Specifically, we apply the MILP modeling approach for the two-subset division property, as introduced by Xiang et al. [10], within a single-tweak single-key framework, uncovering several integral distinguishers. The distinguishers identified for CHILOW-(32+τ) and CHILOW-40 cover up to 4 and 5 rounds, respectively; however, only the 3-round distinguishers satisfy the query constraints given by the designers, in both cases. Subsequently, we explore key recovery attacks based on these distinguishers and propose some 4-round attacks on CHILOW-(32+τ) that offer trade-offs between time and data complexities. To the best of our knowledge, these attacks surpass previously known results on CHILOW-(32+τ). Furthermore, we present an integral attack on 6 rounds of CHILOW-(32+τ); however, only the tweaks of the last three rounds are recovered, while the master key remains unrecovered. The results are summarized in Table 1.

The paper is organized as follows. Section 2 introduces the notations used throughout the paper, along with an overview of the integral attack and division property as a tool to find integral distinguishers. In Section 3, we provide a brief overview of the tweakable block cipher family CHILOW and present our findings on studying its resistance against integral attack using two-subset division properties. Finally, Section 4 offers our concluding remarks.

2 Preliminaries

2.1 Notations

In this paper, binary values are denoted by lowercase letters like x, vectors by boldface like $\boldsymbol{x}$ or just uppercase letters like X, and (multi-) sets by blackboard bold uppercase letters like $\mathbb{X}$. Let $\mathbb{F}_2$ denote the binary finite field and $\boldsymbol{a} = (a_0, a_1, ..., a_{n-1}) \in \mathrm{F}_2^n$ be an n-bit vector, where a_i denotes the i-th bit of $\boldsymbol{a}$, and $\overline{a_i} = a_i \oplus 1$. The vector $\boldsymbol{e}_i$ is the unit vector whose i-th element is 1. For any $\boldsymbol{k} \in \mathrm{F}_2^n$ and $\boldsymbol{k'} \in \mathrm{F}_2^n$, we define $\boldsymbol{k} \succeq \boldsymbol{k'}$ if $k_i \geq k'_i$ for all $i = 0, 1, ..., n-1$. By the symbol $\leftarrow$, we mean adding a member to a (multi) set. Finally, by $X_{i...j}$ we mean a chunk of X from i-th to j-th bit.

2.2 Integral Cryptanalysis

The core concept in higher-order differential [11] and integral [12, 13] attacks is the same, where the attackers attempt to find a collection of inputs for which the resulting outputs sum up to zero in specific positions. The old methods for finding integral distinguishers rely on propagation of the integral properties [13] or estimation of the algebraic degree[11]. However, recent methods are based on the division property proposed by Todo in [5].

* Corresponding author.
**The ISCISC'2025 program committee effort is highly acknowledged for reviewing this paper.
Email addresses: khalesi@rcdat.ac.ir, z_ahmadian@sbu.ac.ir
ISSN: 2008-2045

Table 1. Summary of the key recovery attacks on CHILOW-(32+τ)

#rounds	Dist. #rounds	Data	Time	Memory	Model	Attack	Target	Ref.
3	-	4 KC	2^{106} Dec.	2^{103}	STSK	MITM	Key recovery	[1]
4	-	4 KC	2^{126} Dec.	2^{126}	STSK	MITM	Key recovery	[1]
4	**3**	**2^{37}CC**	**2^{105} Dec.**	**Negligible**	**RTSK(i)**	**Integral**	**Key recovery**	**Sec. 3.3**
4	**3**	**2^{40} CC**	**2^{96} Dec.**	**Negligible**	**RTSK(i)**	**Integral**	**Key recovery**	**Sec. 3.3**
6	**3**	**2^{8} CC**	**$2^{102.6}$ Enc.**	**Negligible**	**RTSK(i)**	**Integral**	**Key recovery(ii)**	**Sec. 3.3**

KC, CC, STSK, RTSK and MITM denote known ciphertext, chosen ciphertext, single-tweak single-key, related-tweak single-key, and meet-in-the-middle, respectively.
(i) The attack needs multiple tweaks; however, it employs single-tweak single-key distinguisher.
(ii) Only the tweaks of the last three rounds are recovered.

2.3 Integral Distinguishers Based on Division Property

The division property comes in two variants: the two-subset division property, also known as the conventional division property, and the three-subset division property. In the first variant, the input set sums to zero (the balanced property) or an unknown value. In contrast, the second variant allows the sum of the input set to have three possible states: zero, one, and unknown.

Definition 1 (two-subset division property[5]). The multiset $\mathbb{X}$ with elements from F_2^n has division property $\mathrm{D}_{\mathbb{K}}^{1^n}$ if

$$\bigoplus_{x\in\mathbb{X}} \boldsymbol{x^u} = \begin{cases} \textit{unknown}, & \textit{if there exists } \boldsymbol{k}\in\mathbb{K} \textit{ s.t. } \boldsymbol{u}\succeq\boldsymbol{k}, \\ 0, & \textit{otherwise} \end{cases}.$$

where $\mathbb{K}$ denotes a set of n-dimensional binary vectors.

Definition 2 (three-subset division property[6]). The multiset $\mathbb{X}$ with elements from F_2^n has division property $\mathrm{D}_{\mathbb{K},\mathbb{L}}^{1^n}$ if

$$\bigoplus_{x\in\mathbb{X}} \boldsymbol{x^u} = \begin{cases} \textit{unknown}, & \textit{if there exists } \boldsymbol{k}\in\mathbb{K} \textit{ s.t. } \boldsymbol{u}\succeq\boldsymbol{k}, \\ 1, & \textit{if there exists } \boldsymbol{l}\in\mathbb{L} \textit{ s.t. } \boldsymbol{u}=\boldsymbol{l}, \\ 0, & \textit{otherwise.} \end{cases}$$

where $\mathbb{K}$ and $\mathbb{L}$ are sets of n-dimensional binary vectors.

The propagation rules of the division property through basic components are provided in [5, 6]. Here, we summarize the propagation rules for the two-subset version, since our investigations are based on it.

Rule 1 (Copy). Let $\boldsymbol{y}=f(\boldsymbol{x})$ be the Copy function with $\boldsymbol{x}=(x_0,x_1,...,x_{n-1})\in\mathrm{F}_2^n$ as the input, and $\boldsymbol{y}=(x_0,x_0,x_1,...,x_{n-1})\in\mathrm{F}_2^{n+1}$ as the output. If the input multiset $\mathbb{X}$ has $\mathrm{D}_{\mathbb{K}}^{1^n}$, then the output multiset $\mathbb{Y}$ has $\mathrm{D}_{\mathbb{K}'}^{1^{n+1}}$, where $\mathbb{K}'$ is computed from all $\boldsymbol{k}\in\mathbb{K}$ as

$$\mathbb{K}' \leftarrow \begin{cases} (0,0,k_1,...,k_{n-1}), & \textit{if } k_0=0 \\ (1,0,k_1,...,k_{n-1}),(0,1,k_1,...,k_{n-1}), & \textit{if } k_0=1 \end{cases},$$

where $\mathbb{K}'\leftarrow\boldsymbol{k}$ denotes that $\boldsymbol{k}$ is inserted into $\mathbb{K}'$.

Rule 2 (And). Let $\boldsymbol{y}=f(\boldsymbol{x})$ be the And function with $\boldsymbol{x}=(x_0,x_1,...,x_{n-1})\in\mathrm{F}_2^n$ as the input, and $\boldsymbol{y}=(x_0\wedge x_1,...,x_{n-1})\in\mathrm{F}_2^{n-1}$ as the output. If the input multiset $\mathbb{X}$ has $\mathrm{D}_{\mathbb{K}}^{1^n}$, then the output multiset $\mathbb{Y}$ has $\mathrm{D}_{\mathbb{K}'}^{1^{n-1}}$, where $\mathbb{K}'$ is computed from all $\boldsymbol{k}\in\mathbb{K}$ as

$$\mathbb{K}'\leftarrow(\lceil\frac{k_0+k_1}{2}\rceil,k_2,...,k_{n-1}).$$

Rule 3 (Xor). Let $\boldsymbol{y}=f(\boldsymbol{x})$ be the Xor function with $\boldsymbol{x}=(x_0,x_1,...,x_{n-1})\in\mathrm{F}_2^n$ as the input, and $\boldsymbol{y}=(x_0\oplus x_1,...,x_{n-1})\in\mathrm{F}_2^{n-1}$ as the output. If the input multiset $\mathbb{X}$ has $\mathrm{D}_{\mathbb{K}}^{1^n}$, then the output multiset $\mathbb{Y}$ has $\mathrm{D}_{\mathbb{K}'}^{1^{n-1}}$, where $\mathbb{K}'$ is computed from all $\boldsymbol{k}\in\mathbb{K}$ s.t. $(k_0,k_1)=(0,0),(1,0)$, or $(0,1)$ as

$$\mathbb{K}'\leftarrow(k_0+k_1,k_2,...,k_{n-1}).$$

2.4 MILP modeling of the division property

In the first papers on division property [5, 6], serching for integral distinguishers was based on breadth-first approach. Later in Asiacrypt 2016, Xiang et al. proposed an MILP modeling for the two-subset division property [10]. They defined *division trail* as follows.

Definition 3 (Division Trail). Let $D_{\mathbb{K}_i}$ be the division property of the input for the i-th round function. Consider the propagation of the conventional bit-based division property $\{\boldsymbol{k_I}\}\overset{def}{=}\mathbb{K}_0\xrightarrow{f}\mathbb{K}_1\xrightarrow{f}\cdots\xrightarrow{f}\mathbb{K}_r$. For any vector $\boldsymbol{k_{i+1}}\in\mathbb{K}_{i+1}$, there must exist a vector $\boldsymbol{k_i}\in\mathbb{K}_i$ such that $\boldsymbol{k_i}$ can propagate to $\boldsymbol{k_{i+1}}$ according to the propagation rules. Beside, for $(\boldsymbol{k_0},\boldsymbol{k_1},\ldots,\boldsymbol{k_r})\in\mathbb{K}_0\times\mathbb{K}_1\times...\times\mathbb{K}_r$, we call $\boldsymbol{k_0}\xrightarrow{f}\boldsymbol{k_1}\xrightarrow{f}\cdots\xrightarrow{f}\boldsymbol{k_r}$ an r-round two-subset bit-based division property trail if $\boldsymbol{k_i}$ can propagate to $\boldsymbol{k_{i+1}}$ for all $i\in\{0,1,\ldots,r-1\}$.

Their method is based on the fact that if there is no division trail $\boldsymbol{k_0}\xrightarrow{E_k}\boldsymbol{e_i}$ for the r-round cipher E_k, the i-th bit of the ciphertext is balanced. The constraints

for propagation of division property through round function are included in the MILP model, and the solver checks the feasibility of the division trail $\boldsymbol{k_o} \xrightarrow{E_k} \boldsymbol{e_i}$, where $\boldsymbol{k_o}$ is determined according to the active bits in the input. If such a division trail is not feasible, the output bit is balanced.

3 Integral Cryptanalysis of CHILOW

3.1 Specification of CHILOW

In [1], three constructions have been introduced for authenticated code encryption. The encryption algorithms for these constructions are illustrated in Figure 1, where f is a stream cipher, F is a "tweakable" PRF, and E is a tweakable block cipher. Additionally, `A`, `N`, `M`, and `C` denote the address (to retrieve the code fragment from), auxiliary information (such as a software version number), instruction, and encrypted instruction, respectively. The address and auxiliary information together can be viewed as a nonce or tweak, while the instruction serves as the plaintext. In the ACE1 and ACE2 constructions, `C` consists of the encrypted instruction concatenated with an authentication tag. In ACE3, `C` is the encryption of the instruction padded with τ zero bits. To instantiate the ACE2 and ACE3 constructions, primitives CHILOW-(32+τ) and CHILOW-40 are proposed, respectively.

For CHILOW-(32+τ), tweakable block ciphers $D_{32}(K, X, T)$ and $D'_{32}(K, X, T)$ are introduced, where K, T, and X are 128-bit key, 64-bit tweak, and 32-bit input, respectively. In ACE2, D_{32} represents E^{-1} and it is used to decrypt the 32-bit encrypted instruction. The output of D'_{32} will be truncated to its first τ bits to derive an authentication tag for an encrypted instruction.

For CHILOW-40, only the tweakable block cipher $D_{40}(K, X, T)$ is introduced, where K, T, and X are 128-bit key, 64-bit tweak, and 40-bit input, respectively. It returns a 40-bit block as the output. In ACE3, D_{40}^{-1} represents E and is used to encrypt a 32-bit instruction code concatenated by 8 bits of zeros. The zero-bits are padded for authentication such that the last 8 bits of the output of D_{40} should be equal to zero.

The total number of queries for CHILOW-(32+τ) and CHILOW-40 is limited to 2^{40} overall and 2^8 per tweak. Despite the presence of a 2-degree non-linear layer and a minimal number of rounds, this restriction poses a significant challenge for cryptanalysis.

3.1.1 CHILOW-(32+τ)

The block ciphers D_{32} and D'_{32}, utilized for CHILOW-(32+τ) in ACE2 construction, take the encrypted instruction code as the 32-bit input block X. The inputs to the first rounds are initialized by whitening the input block as $X^{(0)} = X \oplus K_{64\ldots95}$ for D_{32} and $X'^{(0)} = X \oplus K_{96\ldots127}$ for D'_{32}. The intermediate states $X^{(i+1)}$ and $X'^{(i+1)}$ for $i \leq rnd - 2$ are computed as

$$X^{(i+1)} = L_{32}(\mathbb{X}_{32}(X^{(i)})) \oplus T^{(i+1)}_{0\ldots31},$$
$$X'^{(i+1)} = L'_{32}(\mathbb{X}_{32}(X'^{(i)})) \oplus T^{(i+1)}_{32\ldots63};$$

where rnd is the number of rounds in the block ciphers D_{32} and D'_{32} which is 8. The linear functions $L_{32}(x)$ and $L'_{32}(x)$, as well as the non-linear function $\mathbb{X}_{32}(x)$ are introduced in Section 3.1.3 and Section 3.1.4, respectively.

The last round functions in D_{32} and D'_{32} just consist of the non-linear function $\mathbb{X}_{32}$, so

$$X^{(rnd)} = \mathbb{X}_{32}(X^{(rnd-1)}) \oplus T^{(rnd)}_{0\ldots31},$$
$$X'^{(rnd)} = \mathbb{X}_{32}(X'^{(rnd-1)}) \oplus T^{(rnd)}_{32\ldots63}.$$

The output of the decryption algorithm in CHILOW-(32+τ) consists of the output of D_{32}, namely $X^{(rnd)}$, and the truncation of the output of D'_{32} to its first τ bits, i.e., $X'^{(rnd)}_{0\ldots\tau-1}$, as depicted in Figure 2.

In the round functions, the parameters $T^{(i)}_j$ are the j^{th}-bit of $T^{(i)}$, computed by the tweak and key schedules as

$$T^{(i+1)} = L_{64}(\mathbb{X}_{64}(T^{(i)})) \oplus K^{(i+1)}_{0\ldots63}, \text{for } i \leq rnd - 2,$$
$$T^{(rnd)} = L_{64}(T^{(i)}),$$
$$K^{(i+1)} = L_{128}(\mathbb{X}_{128}(K^{(i)}) \oplus \boldsymbol{c^{(i)}}), \text{for } i \leq rnd - 2.$$

The input to the tweak schedule is the 64-bit tweak whitened with 64 bits of the master key as $T^{(0)} = T \oplus K_{0\ldots63}$. The input to the key schedule is the 128-bit master key as $K^{(0)} = K$. As illustrated in Figure 2, the 64-bit tweak and the 128-bit master key are each treated as a concatenation of 32-bit words, specifically defined as $T = T_0 \,\|\, T_1$ and $K = K_0 \,\|\, K_1 \,\|\, K_2 \,\|\, K_3$. The round constants $c^{(i)}$ for $i \leq rnd - 2$, affect bits 96 to 127 and are computed as

$$\boldsymbol{c}^{(i)}_{96\ldots127} = i \oplus (1 \ll (i+4)) \oplus (b \ll 31),$$
$$c^{(i)}_j = 0, j = 0\ldots95;$$

where $\ll$ represents a shift to the left, and $b \in \{0, 1\}$ is set to 1 only for CHILOW-40. The linear function $L_j(x)$ and the non-linear function $\mathbb{X}_j(x)$ are introduced in Section 3.1.3 and Section 3.1.4, respectively. One can refer to [1] for more details.

3.1.2 CHILOW-40

The block cipher D_{40} is proposed for decryption in CHILOW-40. The input to the first round, namely $X^{(0)}$, is the 40-bit ciphertext X xored with $K_{64\ldots103}$,

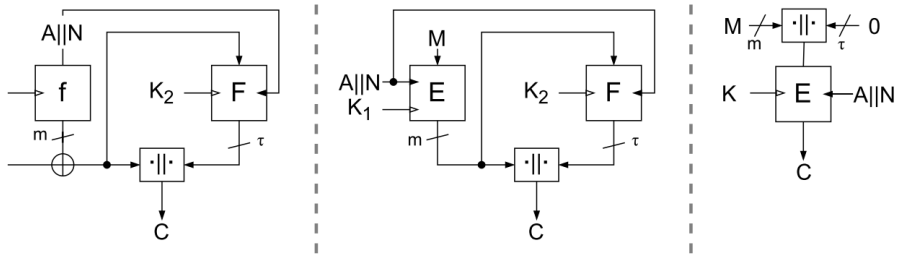

Figure 1. ACE constructions ACE1, ACE2 and ACE3 (from left to right)[1].

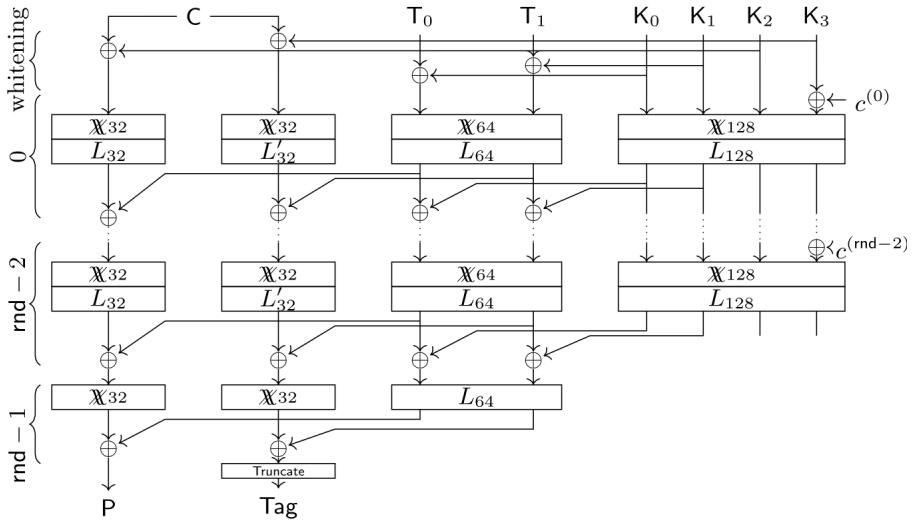

Figure 2. CHILOW-(32+τ) decryption and tag computation[1].

i.e., $X^{(0)} = X \oplus K_{64\ldots103}$. Similar to D_{32} and D'_{32}, the internal states $X^{(i+1)}$ for $i \leq rnd-2$ are computed as

$$X^{(i+1)} = L_{40}(\mathbb{X}_{40}(X^{(i)})) \oplus T^{(i+1)}_{0\ldots39}.$$

The output $X^{(rnd)}$ is computed as

$$X^{(rnd)} = \mathbb{X}_{40}(X^{(rnd-1)}) \oplus T^{(rnd)}_{0\ldots39},$$

and it is expected to contain the 32-bit instruction code followed by 8 bits of zeros. The round number rnd for D_{40} is 8 as in D_{32} and D'_{32}.

3.1.3 Linear Functions

The Linear functions $\boldsymbol{y} = L_j(\boldsymbol{x})$ for $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{F}_2^j$ and $j \in \{32, 40, 64, 128\}$ as well as $\boldsymbol{y} = L'_{32}(\boldsymbol{x})$ for $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{F}_2^{32}$ are computed as

$$y_i = x_{\alpha i+\beta_0} \oplus x_{\alpha i+\beta_1} \oplus x_{\alpha i+\beta_2},$$

where the indices are computed modulo j for $y = L_j(x)$ and modulo 32 for $y = L'_{32}(x)$. The values of α and β_ks are provided in Table 2.

3.1.4 Non-Linear Functions

The non-linear function $\boldsymbol{y} = \mathbb{X}_n(\boldsymbol{x})$ for $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{F}_2^n$ and $n \in \{32, 40, 64, 128\}$, where $n = 2m$ is defined as

Table 2. Offsets for the linear functions

Linear Map	α	β_0	β_1	β_2
L_{32}	11	5	9	12
L'_{32}	11	1	26	30
L_{40}	17	1	9	30
L_{64}	3	1	26	50
L_{128}	17	7	11	14

$$y_i = \begin{cases} x_i \oplus \overline{x}_{i+1}x_{i+2} & i < m-3 \text{ or } m < i < n-2 \\ x_m \oplus \overline{x}_{m-2}x_0 & i = m-3 \\ x_{m-1} \oplus \overline{x}_0 x_1 & i = m-2 \\ \overline{x}_{m-3} \oplus \overline{x}_m \overline{x}_{m+1} & i = m-1 \\ x_{m-2} \oplus \overline{x}_{m+1}x_{m+2} & i = m \\ x_{n-2} \oplus \overline{x}_{n-1}x_{m-1} & i = n-2 \\ x_{n-1} \oplus \overline{x}_{m-1}x_m & i = n-1. \end{cases}$$

3.2 Integral Distinguishers for CHILOW

As pointed out by the designers, CHILOW utilizes a degree-2 non-linear layer while the number of rounds is only 8. This makes CHILOW an appealing target for cryptanalysis methods that exploit algebraic prop-

erties, such as higher-order differential attacks or integral attacks based on the division property. However, the security claims by the designers are based on the assumption that the total number of queries to the decryption oracle is limited to 2^{40} with no more than 2^8 queries per tweak for both CHILOW-(32+τ) and CHILOW-40. These limitations significantly hinder the feasibility of such attacks. Within this context, we examine the resilience of CHILOW against integral attacks while considering these imposed query limitations.

3.2.1 results on CHILOW-(32+τ)

In the single-key single-tweak setting, designers have experimentally verified that if we write the i-th coordinate of $D_{32}(K,T,X)$ as $p_{\boldsymbol{u},i}(K,T,X)X^{\boldsymbol{u}} \oplus q_{\boldsymbol{u},i}(K,T,X)$ for $\boldsymbol{u}$ of hamming weight 31 where $p_{\boldsymbol{u},i}$ and $q_{\boldsymbol{u},i}$ both are polynomials -along with the condition that $X^{\boldsymbol{u}}$ does not divide any monomial of $q_{\boldsymbol{u},i}$- then all the $32 \times 32 = 256$ polynomials $p_{\boldsymbol{u},i}$ are non-zero and linearly independent after 6 rounds. Based on this, it was concluded that there are no integral distinguishers on more than 5 rounds.

In this research, we explored the existence of integral distinguishers based on the two-subset division property, utilizing the method developed by Xiang *et al.*[10]. We modeled the cipher in the single-tweak single-key setting and identified some 4-round distinguishers for $D_{32}(K,T,X)$ such as

$$(1_{17}0_{15}) \xrightarrow{4-round} (0_{32}),$$

where 0_i and 1_j represent i bits of zeros and j bits of ones, respectively. Additionally, zeros and ones in the input (and output) denote constant and active (or balanced and unknown) bits, respectively. It is important to note that neither of the identified 4-round distinguishers satisfies the limitations on the number of queries in our investigations. However, we detected several 3-round integral distinguishers that can be easily extended to key-recovery attacks that outperform the existing ones. Some of the identified 3-round distinguishers are

$$(1_80_{24}) \xrightarrow{3-round} (0_{32}),$$

$$(1_70_{25}) \xrightarrow{3-round} (0_31_10_81_10_11_11_07),$$

and

$$(1_50_{27}) \xrightarrow{3-round} (1_10_11_30_11_40_11_20_21_20_11_40_11_20_11_20_11_3).$$

It is worth noting that we have experimentally verified several of the recovered distinguishers, including those used in key recovery attacks. Additionally, an r-round distinguisher includes the linear layer of the final round. For further investigation, our implementation's source code is publicly available at https://github.com/khalesiakram/CHILOW.

3.2.2 Results on CHILOW-40

There are no reported assessments by the designers regarding the security of CHILOW-40 against integral attacks. In our analysis, we explored this aspect by modeling a two-subset division property within the single-tweak single-key framework, using the same methodology applied to CHILOW-(32+τ). Our results suggest that integral distinguishers are possible up to 5 rounds of $D_{40}(K,T,X)$, with no distinguishers found beyond that point. However, neither the 5-round nor the 4-round distinguishers meet the query constraint. Some of the notable identified distinguishers are as follows:

$$(1_{32}0_8) \xrightarrow{5-round} (0_{40})$$

$$(1_{20}0_{20}) \xrightarrow{4-round} (0_{40})$$

$$(1_80_{32}) \xrightarrow{3-round} (0_{40})$$

3.3 Integral Key Recovery Attacks on CHILOW-(32+τ)

Algorithm 1 illustrates an integral key-recovery attack targeting the reduced 4-round version of CHILOW-(32+τ). The attack is based on the 3-round integral distinguisher $(1_80_{24}) \xrightarrow{3-round} (0_{32})$ of $D_{32}(K,T,X)$, while the linear layer of the last round is removed. Note that all of the 32 bits in the output of $\mathbb{X}_{32}$ from the last round are balanced. This distinguisher is extended by one round at the input for key recovery attack, as depicted in Figure 3. In this attack, for each combination of 2^{32} values of $K_{64,\ldots,95}$ and 2^8 values of $X^{(1)} \oplus T^{(1)}_{0,\ldots,31}$, where the first 8 bits are active and the remaining 24 bits are constant, we compute the set of 2^8 X as outlined in line 9 of Algorithm 1. We then query the decryption oracle with X and evaluate the parity across each set of 2^8 corresponding plaintexts. Any value of $K_{64,\ldots,95}$ with a parity of zero is a potential candidate for 32 bits of the master key.

For each possible value of $K_{64,\ldots,95}$, we use a distinct tweak T to query the decryption oracle with 2^8 different values of $X^{(1)} \oplus T^{(1)}_{0,\ldots,31}$, to adhere to the query limit per tweak. This results in 2^8 decryption queries for each of the 2^{32} possible values of $K_{64,\ldots,95}$, culminating in a total data complexity of 2^{40} chosen ciphertexts, which respects the overall query constraint. The time complexity is primarily driven by these 2^{40} decryption oracle queries. Thanks to the 32-bit parity condition, we expect, on average, a single candidate for $K_{64,\ldots,95}$, corresponding to the 32-bit advantage. Therefore, by performing an exhaustive search over possible values for 96 bits $K_{0,\ldots,63,96,\ldots,127}$, a single value for the 128-bit master key is expected

Algorithm 1 Integral Key-Recovery Attack on 4-round CHILOW(32+τ)

Input: The decryption oracle.
Output: A set of candidates $\mathcal{K}$ for $K_{64,\ldots,95}$
begin
  $\mathcal{K} = \emptyset$
  $T = 0$ ▷ Initialize T with zero (or any arbitrary 64-bit value)
  for all $K_{64,\ldots,95}$ **do**
    $parity = 0$
    for all $X^{(1)} \oplus T^{(1)}_{0,\ldots,31}$ s.t. $X^{(1)}_{0,\ldots,23} \oplus T^{(1)}_{0,\ldots,23} = const$ **do**
      $X = \mathbb{X}_{32}^{-1}(L_{32}^{-1}(X^{(1)} \oplus T^{(1)}_{0,\ldots,31})) \oplus K_{64,\ldots,95}$
      $P = D_{32}(K, T, X)$ ▷ Query the decryption oracle for X
      $parity = parity \oplus P$
    end for
    if $parity = 0$ **then**
      $\mathcal{K} = \mathcal{K} \cup \{K_{64,\ldots,95}\}$
    end if
    $T = T + 1$ ▷ or any alternative modification to T to prevent repetition
  end for
  return $\mathcal{K}$
end

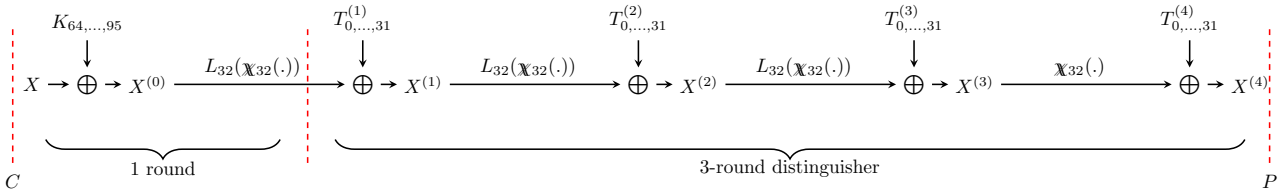

Figure 3. Key recovery attack on 4 rounds of CHILOW-(32+τ).

on average, resulting in an overall attack time complexity of 2^{96} decryptions.

It is worth noting that there are trade-offs between data and time complexities of the attack. For instance, we could employ a 3-round distinguisher with 5 active bits in the input, represented as $(1_5 0_{27})$, and 9 balanced bits in the output. Removing the linear layer from the last round, this distinguisher changes to $(1_5 0_{27}) \xrightarrow{2.5-round} (0_9 1_2 0_6 1_5 0_7 1_2 0_1)$. This adjustment would reduce the data complexity of the attack to 2^{37}. Consequently, we would expect 2^9 candidates for $K_{64,\ldots,95}$ on average, due to the 23-bit condition on the parity, which corresponds to the 23-bit advantage. By exhaustively searching through the remaining key candidates, the correct master key can be identified, yielding a total attack time complexity of 2^{105} decryptions.

As another example for a key-recovery attack on CHILOW-(32+τ), the 3-round distinguisher $(1_8 0_{24}) \xrightarrow{3-round} (0_{32})$ can be extended by adding three additional rounds at the output. This requires a set of ciphertexts of size 2^8, which is active in the first 8 bits and remains constant in the other positions. We then query the ciphertexts of this input set and guess 96 bits related to the tweaks of the last three rounds to perform partial encryption. By computing the parities of the output of the distinguisher, the guesses where these parities match the distinguisher's output are considered as candidates for the tweaks at those rounds. Consequently, with a data complexity of 2^8 chosen ciphertexts and an approximate time complexity of $2^{102.6}$ encryptions (calculated as $2^8 \times 2^{96} \times \frac{3}{8}$), it becomes possible to recover the tweaks of the last three rounds in the 6-round version. It should be noted that the recovered tweaks of the last three rounds have a complex relationship with the master key. This is mostly due to the nested tweak-key schedule, as depicted in Figure 2. As denoted by the designers, in the nested approach, the key schedule updates the key state to generate round keys. These round keys are then used to modify the tweak state, which subsequently modifies the cipher state. As a result, the tweaks for later rounds are effectively strong encryptions of the tweak using the master key. Therefore, even if an attacker manages to recover these round tweaks during an attack, it does not provide an easy way to deduce information about the master key or round tweaks corresponding to other tweak values. So,

leveraging the retrieved later round tweaks to recover the master key remains an open problem.

4 Conclusion

In this paper, we explored the security of CHILOW family of tweakable block ciphers against integral attack based on two-subset division property. We identified integral distinguishers up to 4 rounds for CHILOW-(32+τ) and 5 rounds for CHILOW-40; however, only the 3-round distinguishers in each case comply with the query limitations imposed by the designers.

Additionally, we investigated key-recovery attacks exploiting these distinguishers and proposed some 4-round attacks on CHILOW-(32+τ), each presenting different trade-offs between data and time complexities. For instance, one attack yields a 32-bit advantage with data and time complexities of 2^{40} chosen ciphertexts and decryptions, leading to an overall time complexity 2^{96}. In contrast, another attack achieves a 23-bit advantage with both data and time complexities reduced to 2^{37}, corresponding to overall time complexity 2^{105}. These attacks surpass the previously reported longest key recovery attack—a meet-in-the-middle approach on 4-round CHILOW-(32+τ)- which achieves only a 2-bit advantage and has a time complexity of 2^{126}.

Furthermore, we explored a key-recovery attack on 6-round CHILOW-(32+τ) to recover the tweaks of the last three rounds with a data complexity of 2^8 ciphertexts and a time complexity of $2^{102.6}$ encryptions. Using this information to recover the master key remains a task for future work.

References

[1] Yanis Belkheyar, Patrick Derbez, Shibam Ghosh, Gregor Leander, Silvia Mella, Léo Perrin, Shahram Rasoolzadeh, Lukas Stennes, Siwei Sun, Gilles Van Assche, et al. Chilow and chichi: new constructions for code encryption. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 212–243. Springer, 2025.

[2] Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche. Keccak. In *Annual international conference on the theory and applications of cryptographic techniques*, pages 313–314. Springer, 2013.

[3] Christoph Dobraunig, Maria Eichlseder, Florian Mendel, and Martin Schläffer. Ascon v1. 2: Lightweight authenticated encryption and hashing. *Journal of Cryptology*, 34(3):33, 2021.

[4] Parisa Amiri Eliasi, Yanis Belkheyar, Joan Daemen, Santosh Ghosh, Daniël Kuijsters, Alireza Mehrdad, Silvia Mella, Shahram Rasoolzadeh, and Gilles Van Assche. Koala: a low-latency pseudorandom function. In *International Conference on Selected Areas in Cryptography*, pages 239–266. Springer, 2024.

[5] Yosuke Todo. Structural evaluation by generalized integral property. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 287–314. Springer, 2015.

[6] Yosuke Todo and Masakatu Morii. Bit-based division property and application to simon family. In *International Conference on Fast Software Encryption*, pages 357–377. Springer, 2016.

[7] Yonglin Hao, Gregor Leander, Willi Meier, Yosuke Todo, and Qingju Wang. Modeling for three-subset division property without unknown subset: improved cube attacks against trivium and grain-128aead. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 466–495. Springer, 2020.

[8] Senpeng Wang, Bin Hu, Jie Guan, Kai Zhang, and Tairong Shi. Milp-aided method of searching division property using three subsets and applications. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 398–427. Springer, 2019.

[9] Jiahui He, Kai Hu, Hao Lei, and Meiqin Wang. Massive superpoly recovery with a meet-in-the-middle framework: Improved cube attacks on trivium and kreyvium. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 368–397. Springer, 2024.

[10] Zejun Xiang, Wentao Zhang, Zhenzhen Bao, and Dongdai Lin. Applying milp method to searching integral distinguishers based on division property for 6 lightweight block ciphers. In *International conference on the theory and application of cryptology and information security*, pages 648–678. Springer, 2016.

[11] Xuejia Lai. Higher order derivatives and differential cryptanalysis. In *Communications and Cryptography: Two Sides of One Tapestry*, pages 227–233. Springer, 1994.

[12] Joan Daemen, Lars Knudsen, and Vincent Rijmen. The block cipher square. In *International Workshop on Fast Software Encryption*, pages 149–165. Springer, 1997.

[13] Lars Knudsen and David Wagner. Integral cryptanalysis. In *International Workshop on Fast Software Encryption*, pages 112–127. Springer, 2002.

Akram Khalesi received her B.Sc. degree from Kashan University, Isfahan, Iran, in 2011, her M.Sc. degree from Malek-Ashtar University, Tehran, Iran, in 2014, and her Ph.D. degree from Shahid Beheshti University, Tehran, Iran, in 2024 all in Electrical Engineering. She is currently a researcher at the Research Center for Development of Advanced Technologies, Tehran, Iran. Her research area includes cryptology with an emphasis on symmetric designs and applied cryptography.

Zahra Ahmadian received her B.Sc. degree in Electrical Engineering (Communications and Electronics) from Amirkabir University of Technology, Tehran, Iran, in 2006, and the M.Sc. degree in Electrical Engineering (Secure Communications) and Ph.D. degree in Electrical Engineering (Communication Systems) both from Sharif University of Technology, Tehran, in 2008 and 2014 respectively. Since 2014, she has been with the Electrical Engineering Department of Shahid Beheshti University, Tehran, Iran, as a faculty member. Her special fields of interest include Wireless Security and Cryptology with an emphasis on Cryptanalysis.