More Brisés in Ballet: Extending Differential and Linear Cryptanalysis

Selected Areas in Cryptography (SAC26)

Emanuele Bellini[1] **Gabriele Bellini**[2] Alessandro De Piccoli[2]
Michela Gallone[2] David Gerault[1] Yun Ju Huang Paul Huynh[1]
Matteo Onger[2] Simone Pelizzola[2] Andrea Visconti[2]

27 Aug 2026, Ottawa

UNIVERSITÀ DEGLI STUDI DI MILANO

Joint work

our work is a collaboration between

Technology Innovation Institute
Cryptography Research Centre

UNIVERSITÀ DEGLI STUDI DI MILANO

[1] Technology Innovation Institute, UAE

[2] University of Milan, IT

Overview

1 Introduction

In this presentation, we will cover:

- an overview of the Ballet block cipher;
- our cryptanalysis of Ballet;
- our key-recovery results;
- our proposal for reducing the number of cipher rounds.

Slides: https://github.com/gabriele-bellini/SAC26/blob/main/slides.pdf

Introduction to the cipher

Ballet is a family of block ciphers **standardized in China**.

The Ballet family won the 2018 CARC (Chinese Association for Cryptologic Research) competition for symmetric ciphers in the software category.

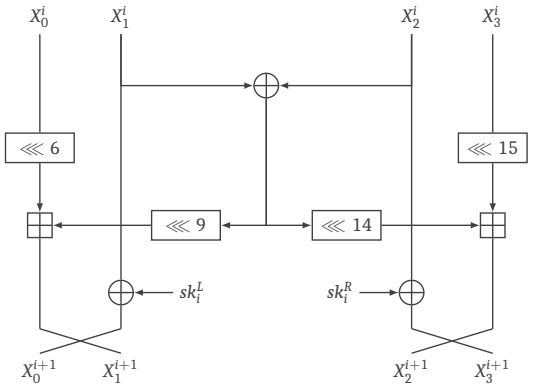
The cipher family has three variants with different block sizes, key sizes, and numbers of rounds.

Block size (bits)	Key size (bits)	Rounds
128	128	46
128	256	48
256	256	74

The Ballet Round Function

2 Ballet cipher structure

- Ballet is an **ARX** cipher: Addition, Rotation, and XOR.
- It uses a **Lai–Massey construction**.



Round function

The Ballet key schedule

The cipher uses a **linear key schedule**.

Algorithm 1: Key generation for Ballet n/n

$K = k_0 \,\|\, k_1$;
for $i = 0$ **to** $r - 1$ **do**
    output : $k_0 = sk_i^L \,\|\, sk_i^R$;
    $k_{temp} = k_1$;
    $k_1 = k_0 \oplus (k_1 \lll 3) \oplus (k_1 \lll 5) \oplus i$;
    $k_0 = k_{temp}$;
end

Algorithm 2: Key generation for Ballet $n/2n$

$K = k_0 \,\|\, k_1 \,\|\, t_0 \,\|\, t_1$;
for $i = 0$ **to** $r - 1$ **do**
    output : $k_0 = sk_i^L \,\|\, sk_i^R$;
    $t_{temp} = t_1, k_{temp} = k_1$;
    $t_1 = t_0 \oplus (t_1 \lll 7) \oplus (t_1 \lll 17)$;
    $k_1 = k_0 \oplus (k_1 \lll 3) \oplus (k_1 \lll 5)$;
    $t_0 = t_{temp}, k_0 = k_{temp}$;
    $k_1 = k_1 \oplus t_1 \oplus i$;
end

Our contributions

3 Contributions

- **Differential & linear cryptanalysis**
  - New optimal trails
  - Tighter security bounds for Ballet-128
  - Improved impossible-differential result (7 $\rightarrow$ 8 rounds)
- **Differential-linear cryptanalysis**
  - First trail
  - **First key-recovery attack**
- **CLAASP improvements**
  - Optimized SAT-based search
  - Time-based cutoff heuristic ($\rightarrow$ trails up to 20 rounds)

Methods Used in Our Analysis

3 Contributions

Differential, linear, and differential-linear cryptanalysis

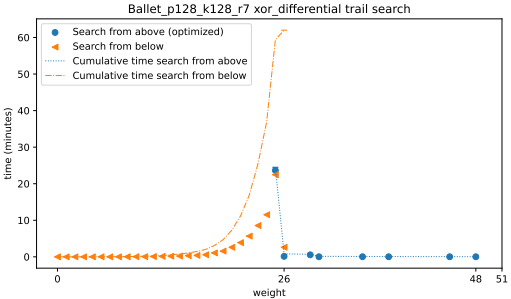
- SAT search (*from below*) to find **optimal trails**
  - + Heuristic: *splicing* — partially fixing trail values
- **Optimized SAT search** (*from above*)
  - + Heuristic: **time-based cutoff**

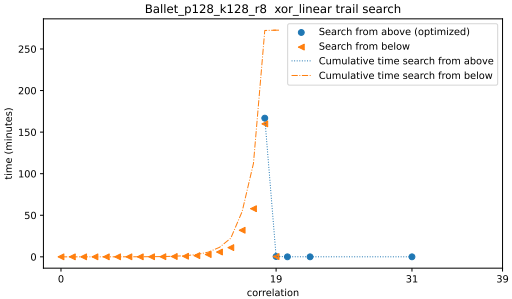
Impossible-differential trail search

- Fix the plaintext and ciphertext masks
- Check satisfiability via SAT solver

Optimized SAT search and time-based cutoff heuristic

3 Contributions





Differential distinguishers Ballet-128

4 Cryptanalysis

Cryptanalysis	Rounds	Probability	Parameters	Cores	Time ($\leq$)	Trail	Reference
differential distinguisher	**9**	$\leq \mathbf{2^{-43}}$	NA	NA	NA	✗	Ballet's paper
	9	$\mathbf{2^{-46}}$	NA	80	49 days	✓	our work
differential distinguisher via splicing	10	$\geq 2^{-63}$	**8 fixed rounds**	50	2 min	✓	our work
	11	$\geq 2^{-81}$		50	3 min	✓	our work
	12	$\geq 2^{-90}$		50	4 min	✓	our work
	13	$\geq 2^{-105}$		50	9 min	✓	our work
	14	$\geq \mathbf{2^{-116}}$		50	4 hours	✓	our work
differential distinguisher via optimized SAT and time-based cutoff heuristic	10	$\geq 2^{-57}$	time cutoff = 4d start = 127	8	4.6 days	✓	our work
	11	$\geq 2^{-64}$	time cutoff = 5d start = 127	8	5.3 days	✓	our work
	12	$\geq 2^{-75}$	time cutoff = 5d start = 127	8	5.5 days	✓	our work
	13	$\geq 2^{-84}$	time cutoff = 2d start = 127	8	5.4 days	✓	our work
	14	$\geq 2^{-91}$	time cutoff = 3d start = 108	30	12.6 days	✓	our work
	15	$\geq 2^{-100}$	time cutoff = 3.5d start = 123	50	12.8 days	✓	our work
	16	$\geq \mathbf{2^{-127}}$	time cutoff = 8d start = 127	50	9.9 days	✓	our work

Differential cluster effect of Ballet

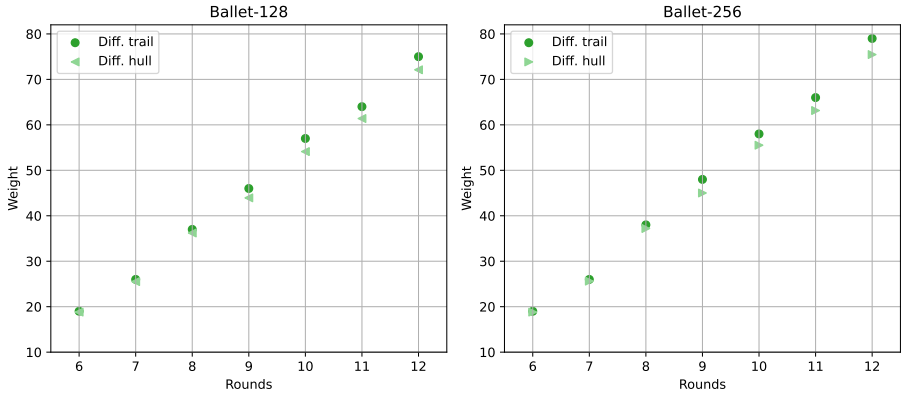
4 Cryptanalysis

Table: For each round, the table reports the trail weight of the best found single trail and the corresponding differential weight.

# Round	Ballet-128		Ballet-256	
	Trail weight	Differential weight	Trail weight	Differential weight
6	19	18.81	19	18.81
7	26	25.52	26	25.62
8	37	36.21	38	37.20
9	46	43.94	48	45.01
10	57	54.12	58	55.52
11	64	61.39	66	63.15
12	75	72.11	79	75.46

Differential cluster effect of Ballet

4 Cryptanalysis



Impossible differential distinguishers

4 Cryptanalysis

Table: Ballet-128

Cryptanalysis	Rounds	Parameters	Cores	Time (≤)	Trail	Reference
impossible differential distinguisher	7	hw pt=1, ct=1	NA	NA	✗	Ballet's paper
	7	hw pt=1, ct=1	1	6 hours	✓	our work
	8	**hw pt=2, ct=1**	100	45 min	✓	our work
	7	hw pt=1, ct=2	100	45 min	✓	our work
	7	hw pt=2, ct=2	64	3 days	✓	our work

Table: Ballet-256

Cryptanalysis	Rounds	Parameters	Cores	Time (≤)	Trail	Reference
impossible differential distinguisher	7	hw pt=1 ct=1	NA	NA	✗	Ballet paper
	7	hw pt=1 ct=1	1	1 day	✓	our work
	8	**hw pt=2 ct=1**	100	11 hours	✓	our work
	7	hw pt=1 ct=2	100	12 hours	✓	our work

Linear distinguishers Ballet-128

4 Cryptanalysis

Cryptanalysis	Rounds	Probability	Parameters	Cores	Time ($\leq$)	Report trail	Reference
linear distinguisher (correlation)	**9**	$\mathbf{2^{-23}}$	NA	NA	NA	✗	Ballet's paper
	9	2^{-23}	NA	100	7 hours	✓	our work
	10	2^{-26}	NA	80	4 days	✓	our work
	11	$\mathbf{2^{-30}}$	NA	80	16 days	✓	our work
linear distinguisher via optimized SAT and time-based cutoff heuristic	10	$\geq 2^{-26}$	time cutoff = 2h start = 80	40	15 hours	✓	our work
	11	$\geq 2^{-30}$		40	3 days	✓	our work
	12	$\geq 2^{-36}$		40	2 days	✓	our work
	13	$\geq 2^{-43}$		40	2 days	✓	our work
	14	$\geq 2^{-49}$		40	6 days	✓	our work
	15	$\geq 2^{-56}$		40	10 days	✓	our work
	16	$\geq \mathbf{2^{-63}}$	time cutoff = 36h start = 68	50	4 days	✓	our work

Differential-linear distinguishers Ballet-128

4 Cryptanalysis

Cryptanalysis	Rounds	Probability	Parameters	Cores	Time ($\leq$)	Trail	Reference
differential-linear distinguisher	9	2^{-12}	4-1-4	4	2 min	✓	our work
	10	2^{-16}	4-1-5	4	5 min	✓	our work
	11	2^{-22}	5-1-5	4	54 min	✓	our work
	12	2^{-30}	5-1-6	4	7 hours	✓	our work
	13	2^{-40}	6-1-6	50	2 hours	✓	our work
	14	$\mathbf{2^{-52}}$	7-1-6 and 6-1-7	50	3 days	✓	our work

Differential-linear distinguishers Ballet-128

4 Cryptanalysis

Cryptanalysis	Rounds	Probability	Parameters	Cores	Time ($\leq$)	Trail	Reference
differential-linear distinguisher with splicing	15	$\geq 2^{-64}$	7-1-4+3	16	2 min	✓	our work
	16	$\geq 2^{-78}$	7-1-4+4	16	3 min	✓	our work
	17	$\geq 2^{-96}$	5+0-1-4+f7	1	39 sec	✓	our work
	18	$\geq 2^{-106}$	6-1-4+7	32	5 hours	✓	our work
	19	$\geq 2^{-112}$	6-1-4+8	32	15 hours	✓	our work
	20	$\geq \mathbf{2^{-124}}$	7-1-4+8	16	14 hours	✓	our work
differential-linear distinguisher via optimized SAT and time-based cutoff heuristic	15	$\geq 2^{-61}$	time cutoff = 10d start = 63	4	14.4 days	✓	our work
	16	$\geq 2^{-75}$	time cutoff = 4d start = 77	20	4.4 days	✓	our work
	17	$\geq 2^{-84}$	time cutoff = 22d start = 87	1	30 days	✓	our work
	18	$\geq 2^{-94}$	time cutoff = 7d start = 98	40	11.2 days	✓	our work
	19	$\geq 2^{-106}$	time cutoff = 7d start = 110	40	10.9 days	✓	our work
	20	$\geq \mathbf{2^{-118}}$	time cutoff = 7d start = 120	100	15.9 days	✓	our work

Ballet Key recovery

4 Cryptanalysis

Cryptanalysis	Ballet version	Number of rounds	Time complexity	Data complexity
differential-linear	128/128	16	$2^{104.46}$	$2^{72.46}$
differential-linear	128/128	16	$2^{124.26}$	$2^{117.60}$
differential-linear	128/256	17	$2^{192.00}$	$2^{111.46}$
differential-linear	256/256	22	$2^{242.06}$	$2^{178.06}$

Ballet round reductions

4 Cryptanalysis

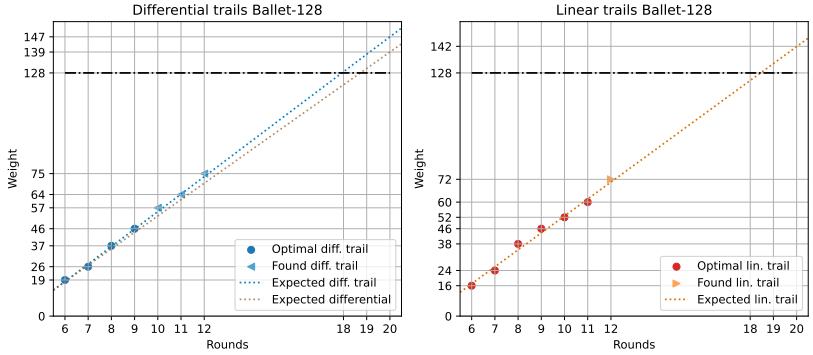
Table: Summary of bounds, attacks, and round reduction estimates for Ballet

Scheme	Rounds	Attack diff-lin. r	Proven bounds (conservative) No differential ≥ r	Proven bounds (conservative) No linear ≥ r	Trail growth estimates No diff./linear ≥ r	Trail growth estimates **Recommended r (≥30% sec.)**
Ballet-128/128	46	16	26	26	20	**27**
Ballet-128/256	48	17	26	26	20	**27**
Ballet-256/256	74	22	54	52	40	**54**

Ballet round reductions

4 Cryptanalysis

Figure: Differential (left) and linear (right) trail weights for Ballet-128 across rounds, including proven optimal trails, best-known trails, and expected growth trends.



More Brisés in Ballet: Extending Differential and Linear Cryptanalysis

Thanks for your attention!
Any questions?