暨南大學
JINAN UNIVERSITY

Improving Differential-Neural Cryptanalysis for Large-State SPECK

Tianrong Huang, Yingying Li, Qinggan Fu, Yincen Chen, and Ling Song

Jinan University

Aug 26, 2024

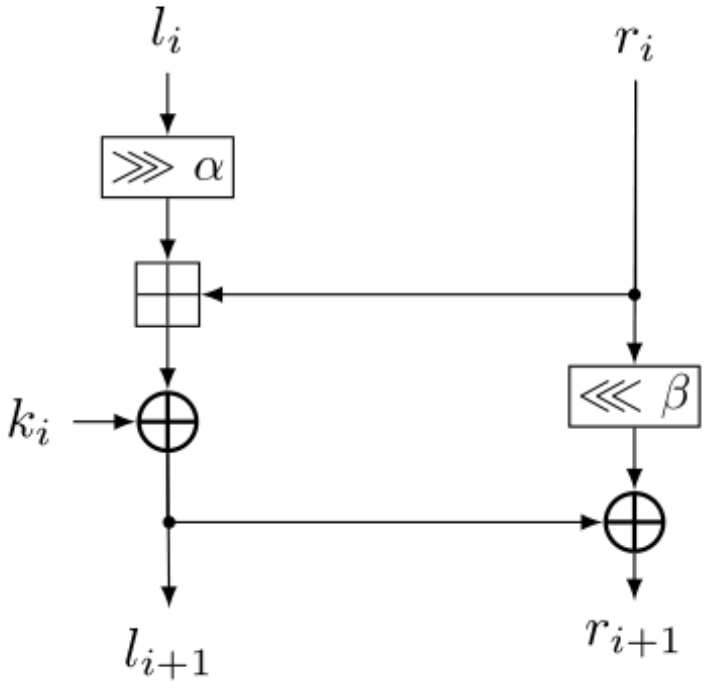
ICICS 2024

Table of Contents

Table of Contents

SPECK

SPECK is a set of lightweight block cipher algorithms designed by the National Security Agency (NSA) of the United States.



Based on **the block size and key size**, SPECK can be categorized into various versions, such as **SPECK32/64**.

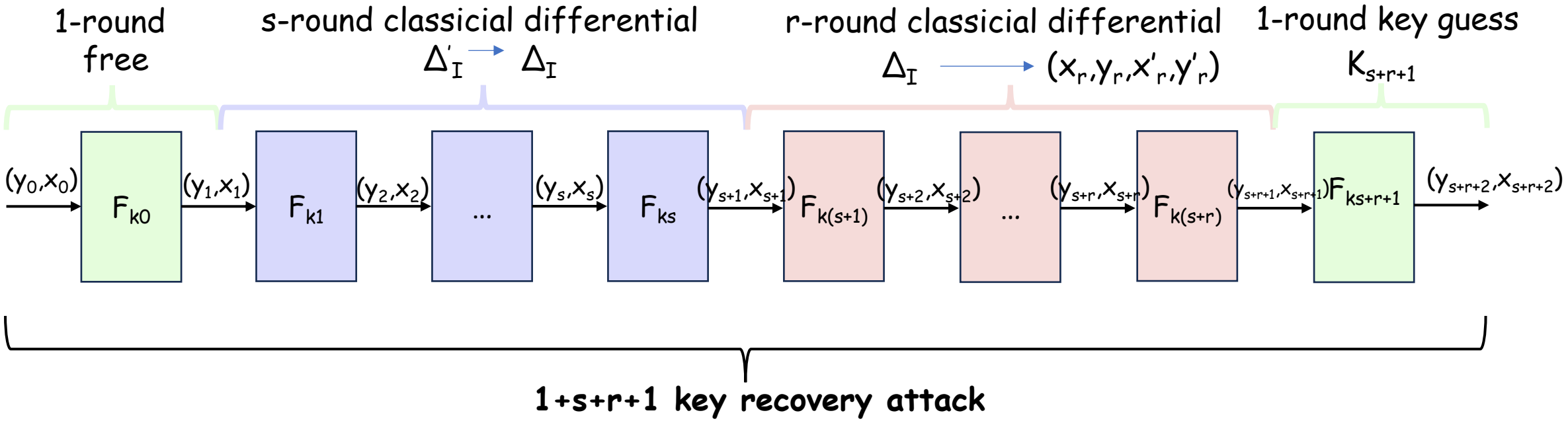
- **Differential-Neural Distinguishers**[Gohr in 2019]:

Task: distinguishing two types of ciphertext pairs

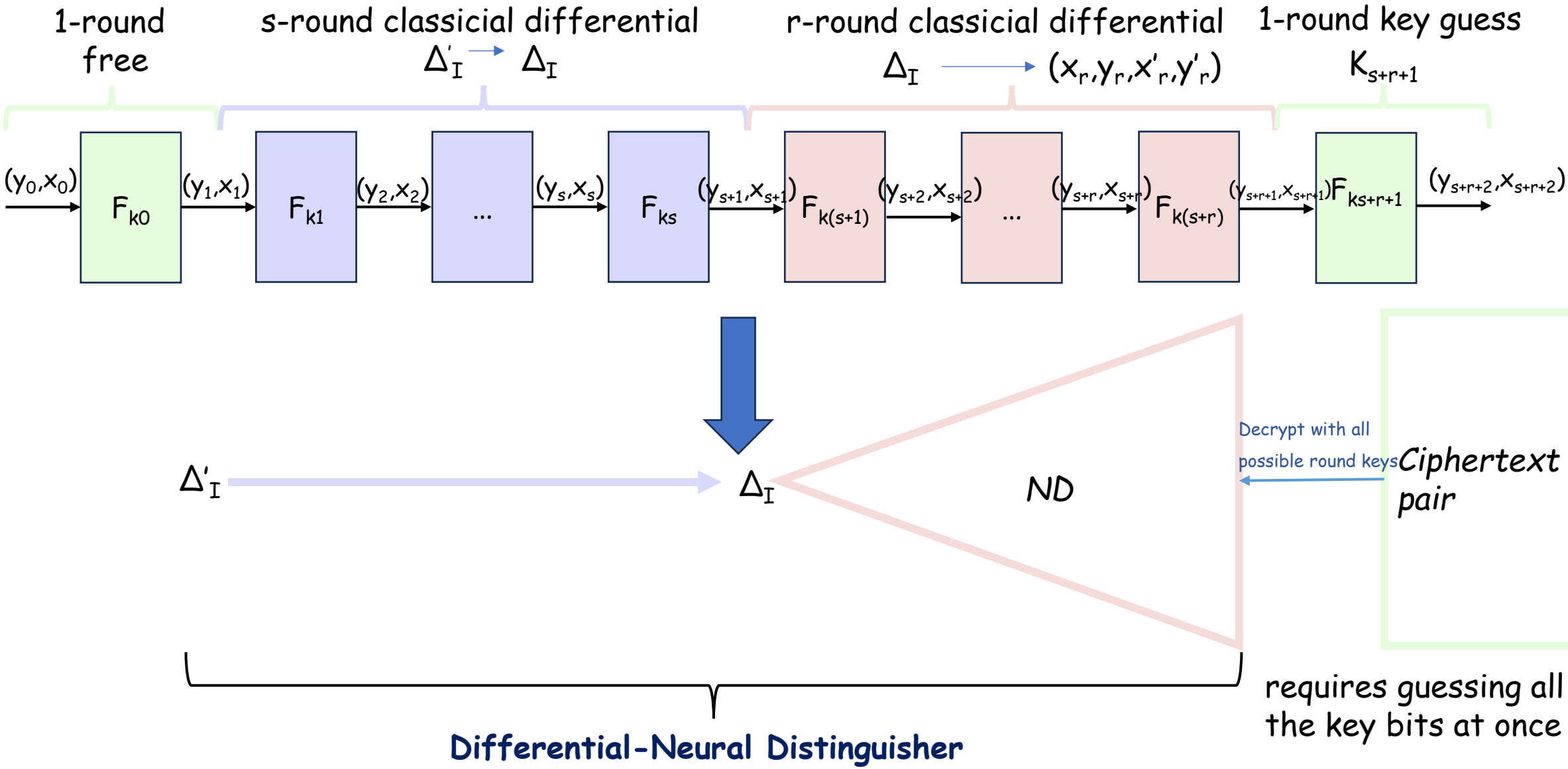
Positive $(C,C'),Y=1$, where $(C,C') \xleftarrow{Enc} ((P, P') \mid P = \$, P' = P \oplus \Delta_I)$

Negative $(C,C'),Y=0$, where $(C,C') \xleftarrow{Enc} ((P, P') \mid P = \$, P' = \$')$

➢ Key Recovery Attack [Gohr in 2019] :



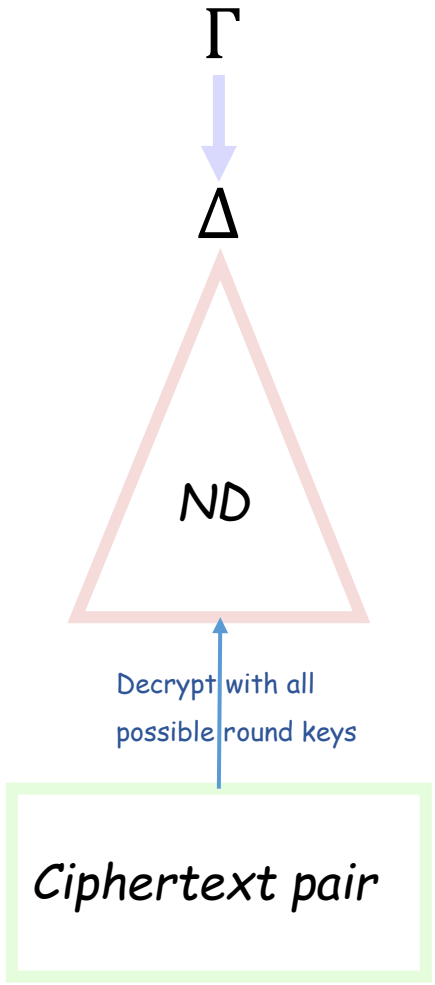
Gohr's Differential-Neural Cryptanalysis



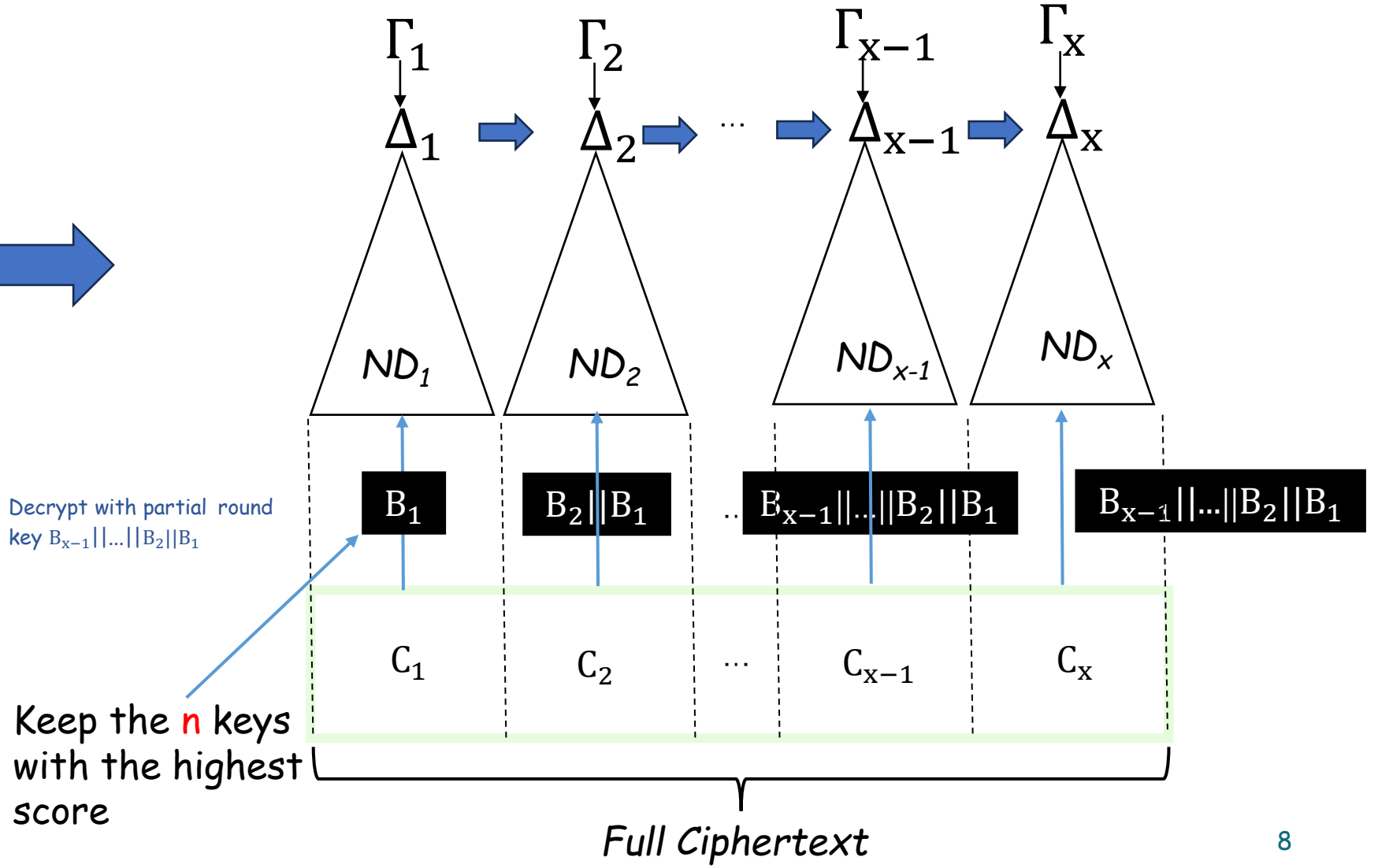
Cryptanalysis for Large-State Block Cipher

暨南大學 JINAN UNIVERSITY

Differential-Neural Distinguisher for SPECK32/64



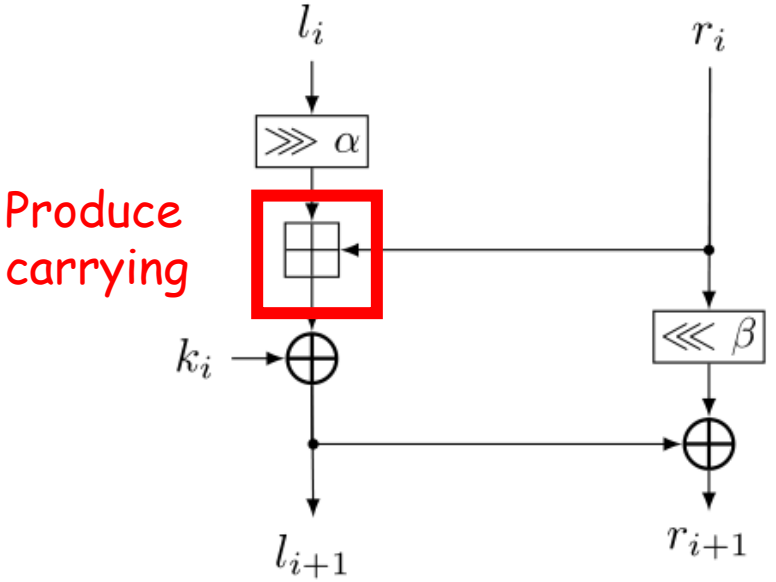
Key Recovery Framework for Large-State SPECK [Chen et al. in 2019]:



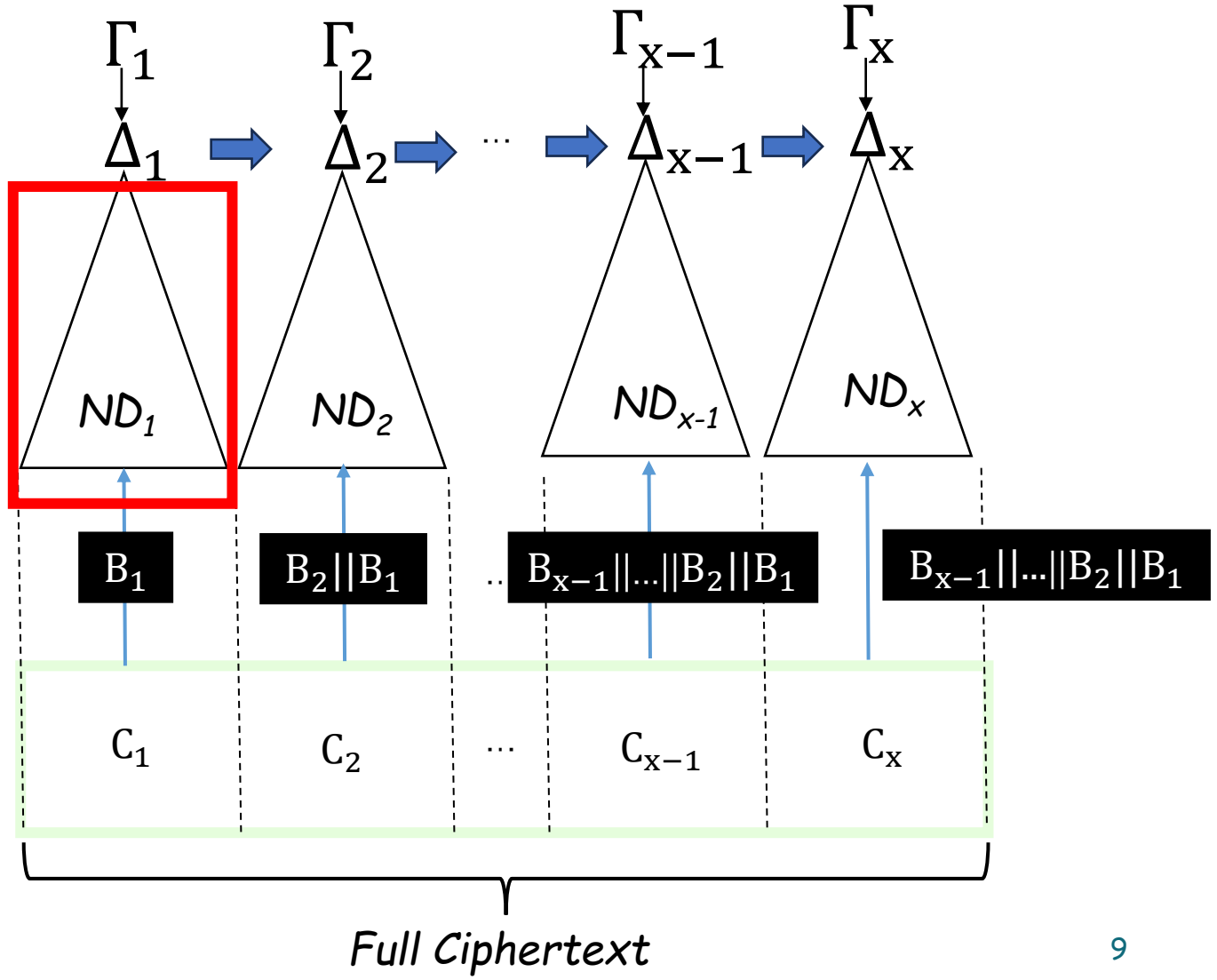
Cryptanalysis for Large-State Block Cipher

Chen et al.'s Key Recovery Framework for Large-State SPECK

During training, the C_i part of the full ciphertext is used directly for training.



Produce carrying



Cryptanalysis for Large-State Block Cipher

暨南大學 JINAN UNIVERSITY

When recovering the high-level part of the key such as B_2, not only B_2 should be used to decrypt C_2, but also the carry effect of using B_1 to decrypt C_1 should be considered.

Chen et al.'s Key Recovery Framework for Large-State SPECK

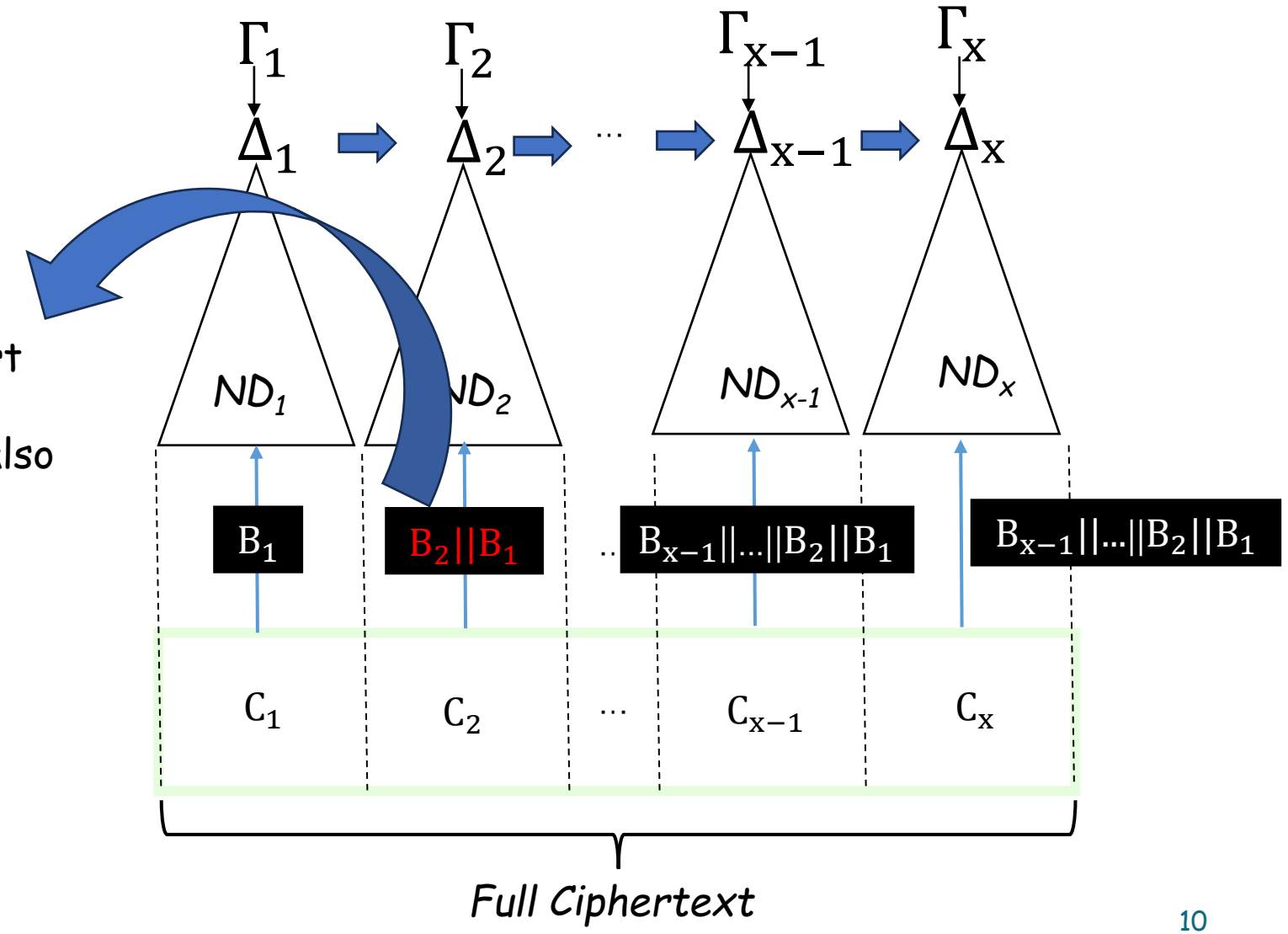
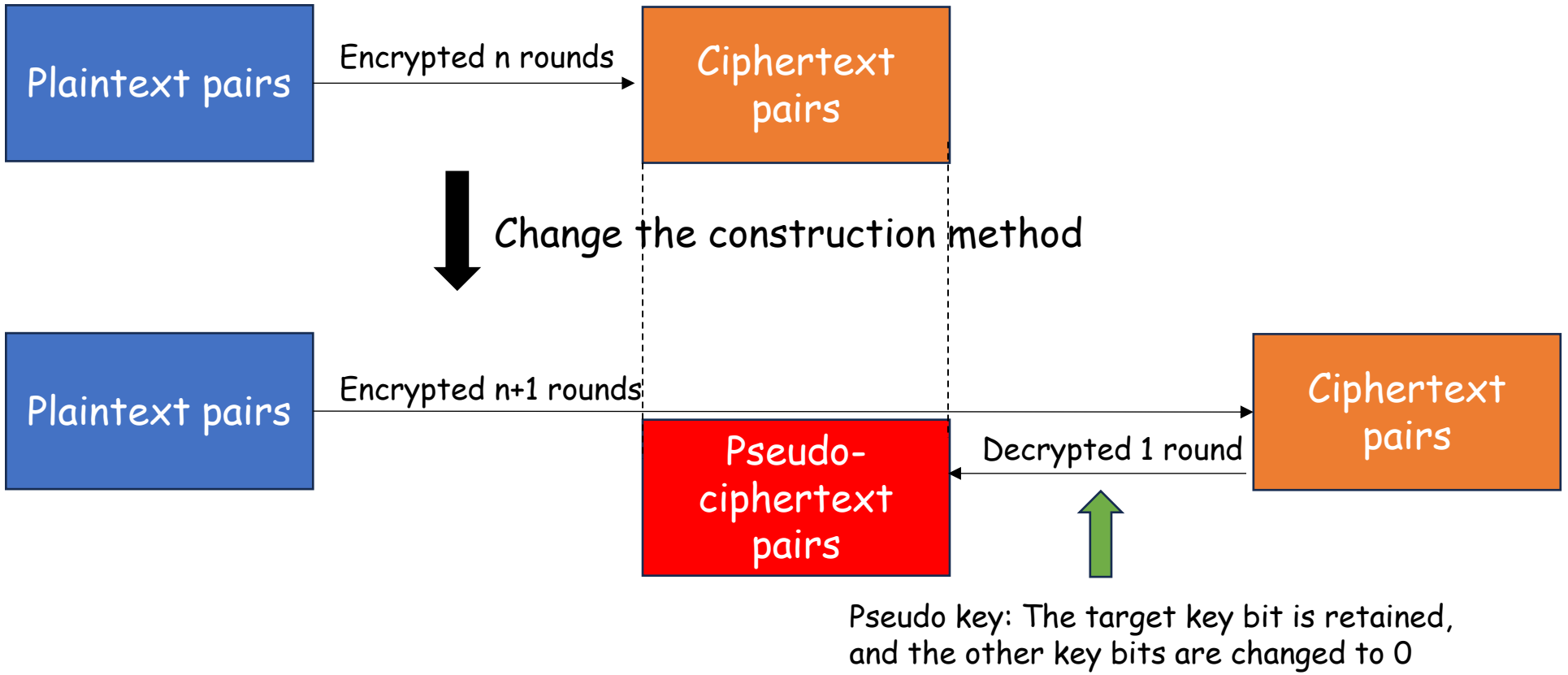


Table of Contents

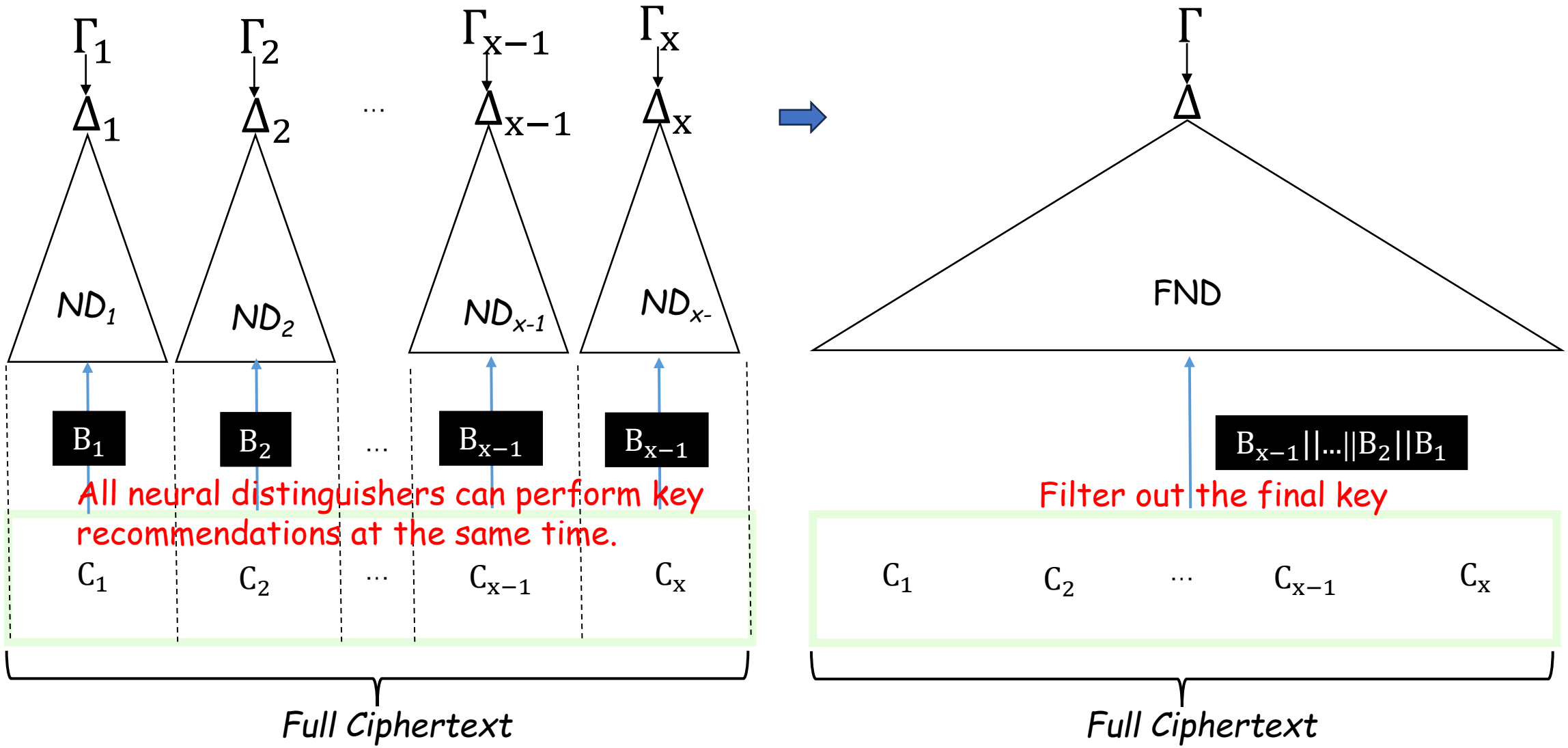
New Training Strategy for Neural Distinguishers

➢ Change the training data of the partial neural distinguisher



When the neural distinguisher trained by this kind of data does key recovery, it only needs to pay attention to the target key bit, and the other positions are set to 0

Parallelizable Key Recovery Framework

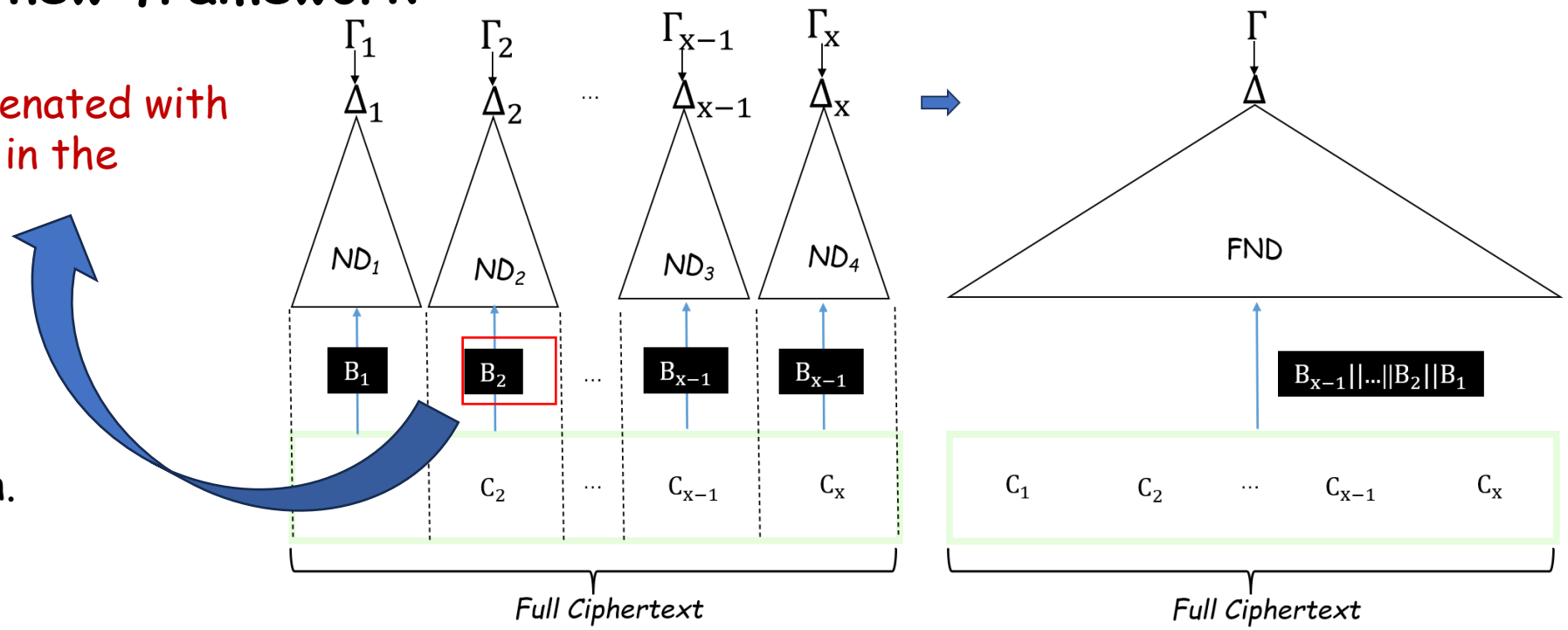


Parallelizable Key Recovery Framework

➢ Advantages of the new framework:

Do not need to be concatenated with the n keys recommended in the previous step.

The time is reduced to 1/n.



Under the condition of multiple GPUs, all distinguisher perform key recovery at the same time

The time is reduced to 1/x

Parallelizable Key Recovery Framework

暨南大學 JINAN UNIVERSITY

➢ Application to SPECK64/96 and SPECK96/96 :

Target	Round	Avg. Time[1]	hw(kg, rk)[2]	Conffgure	Reference
SPECK64/96	9	66s	1.93	$1 + 1r_{CD} + 6r_{ND}$	Chen et al.
		29s	0.80	$1 + 1r_{CD} + 6r_{ND}$	This paper
SPECK96/96	10	303s	1	$1 + 1r_{CD} + 7r_{ND}$	Chen et al.
		163s	0.44	$1 + 1r_{CD} + 7r_{ND}$	This paper

[1] Avg. Time refers to the average time required to perform a single attack on a computer equipped with an NVIDIA 3060 graphics card.

[2] hw(kg, rk) refers to the average Hamming distance between the guessed key and the actual key

Table of Contents

Improved Partial Neural Distinguisher for Ciphertext

- The longest-round traditional analysis results for SPECK64/96 and SPECK96/96[Song et al. in 2016]

Target	Rounds attacked/Total rounds	Reference
SPECK64/96	**19/26**	**Song et al.**
SPECK96/96	**20/28**	

- The Differential-Neural Cryptanalysis results for SPECK64/96 and SPECK96/96

Target	Round	Conffgure	Reference
SPECK64/96	9	$1 + 1r_{CD} + 6r_{ND}$	Chen et al.
		$1 + 1r_{CD} + 6r_{ND}$	**This paper**
SPECK96/96	**10**	$1 + 1r_{CD} + 7r_{ND}$	Chen et al.
		$1 + 1r_{CD} + 7r_{ND}$	**This paper**

Improved Partial Neural Distinguisher for Ciphertext

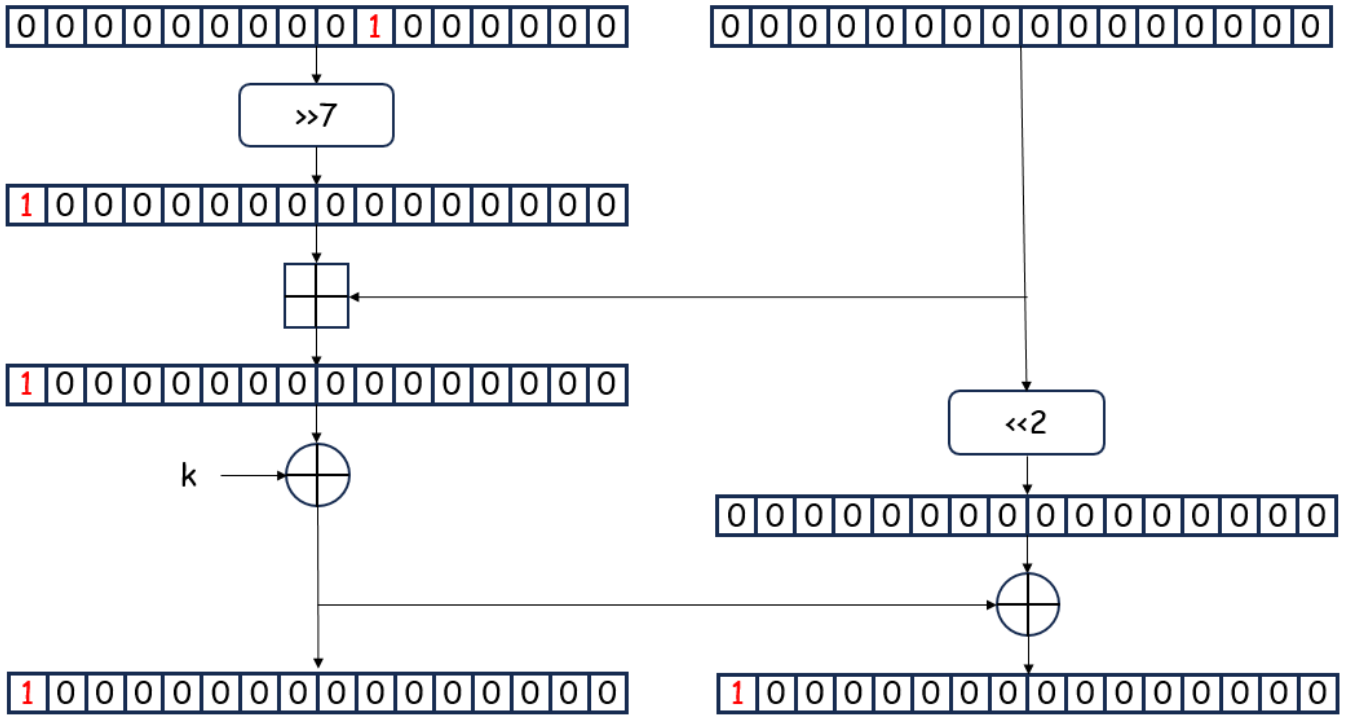
- Selection of Input Differences

Gohr choose 0x0040/0000 as the input difference

The carry effect produced by the first round of modular addition is eliminated.

0x0040/0000 $\xrightarrow{1}$ 0x8000/8000

Making the difference distribution more concentrated is beneffcial to the neural network in learning ciphertext knowledge.



Improved Partial Neural Distinguisher for Ciphertext

- Selection of Input Differences

Gohr choose 0x0040/0000 as the input difference

The carry effect produced by the first round of modular addition is eliminated.

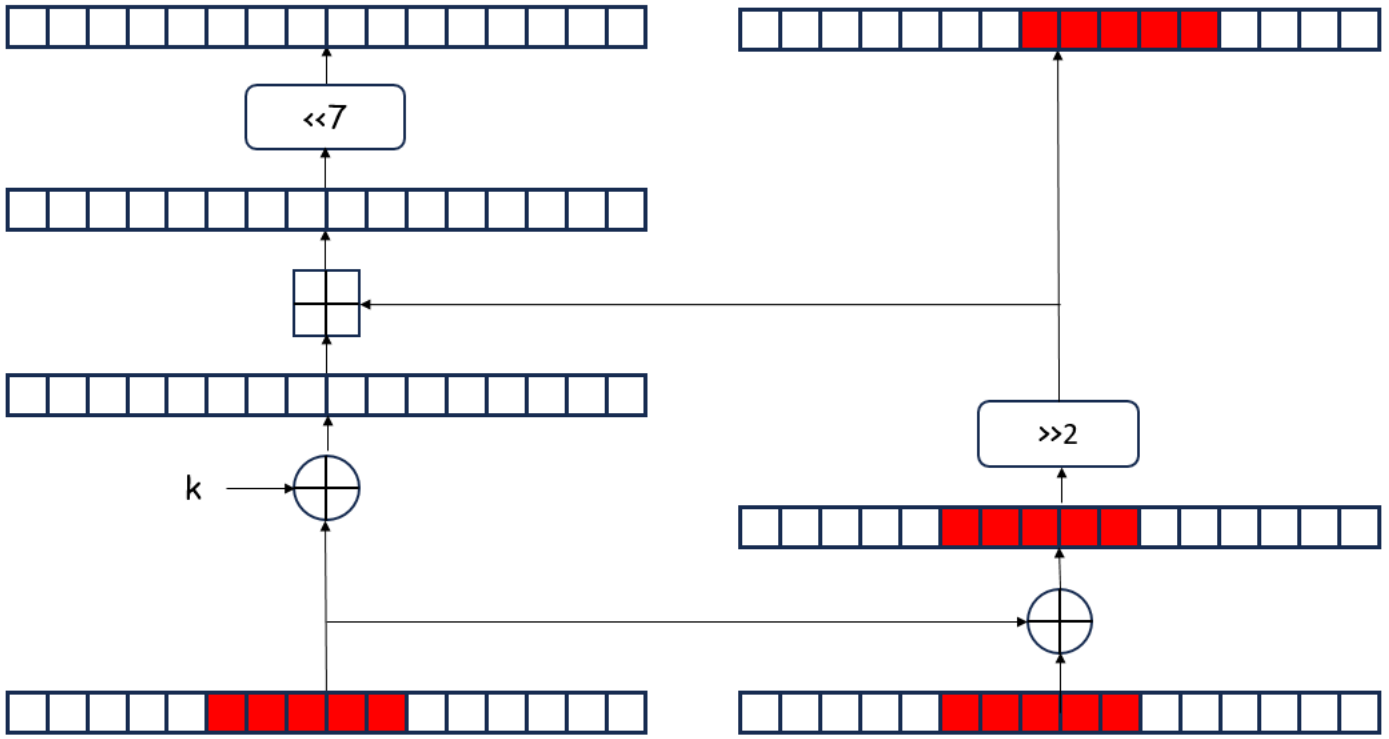
0x0040/0000 $\xrightarrow{1}$ 0x8000/8000

Making the difference distribution more concentrated is beneffcial to the neural network in learning ciphertext knowledge.

We choose (0x80, 0), (0x8000, 0), and (0x800000, 0) as the input differences for the neural network of SEPCK64/96.

Improved Partial Neural Distinguisher for Ciphertext

- Including information from the penultimate round and multiple pairs.

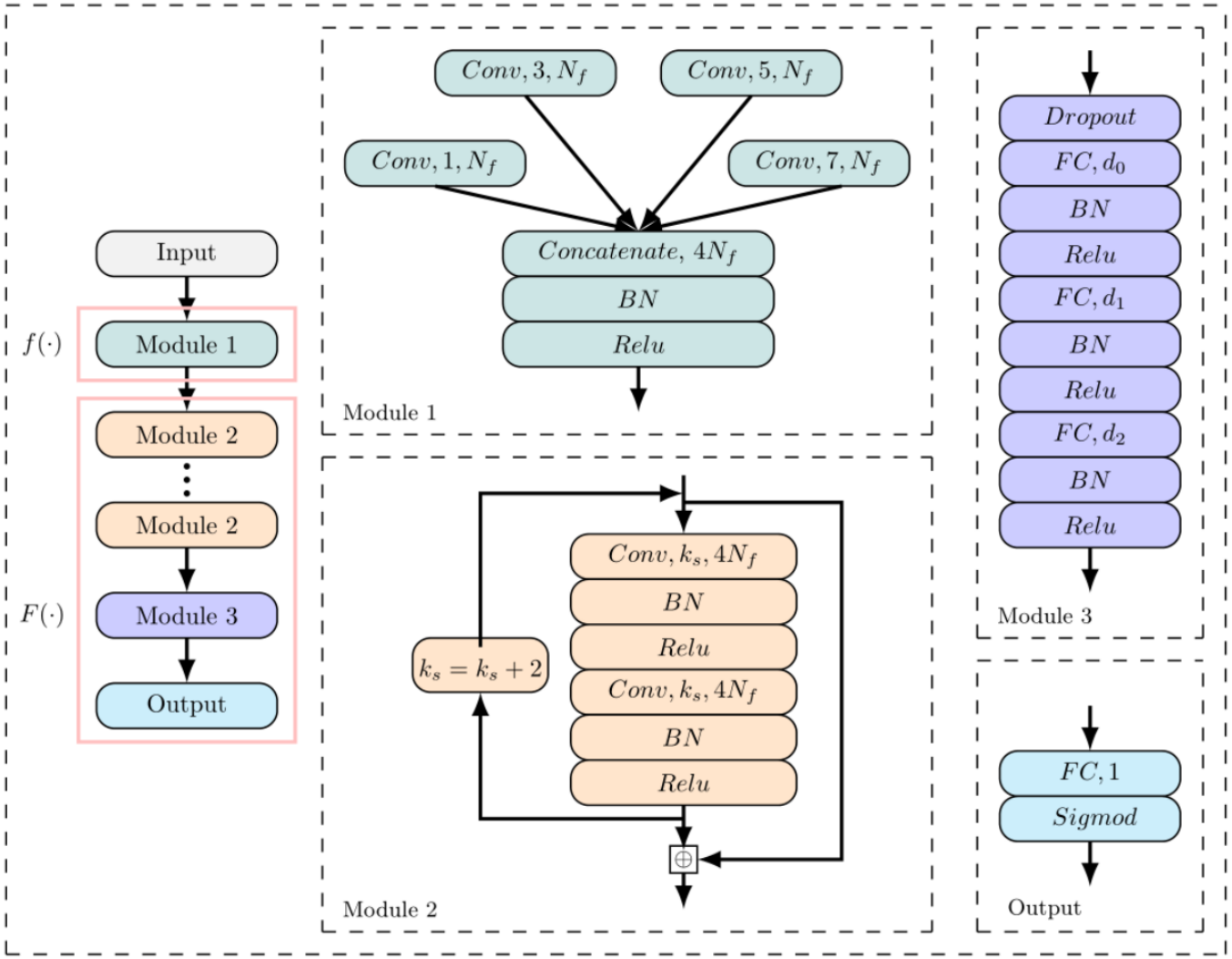


With ciphertext fragments, we can calculate the ciphertext fragments of the right half of the penultimate round without knowing the key. Add them to traing data.

At the same time, we include ciphertext information from multiple different ciphertext pairs in one training sample.

Improved Partial Neural Distinguisher for Ciphertext

- Network Architecture



Using the network structure proposed by Zhang et al. and use a staged training method.

Improved Partial Neural Distinguisher for Ciphertext

- Neural distinguishers against 7-round SPECK64

Distinguisher	Input difference	Ciphertext bits	Accuracy
ND_1	(0x8000, 0),	{17 ~ 8}	0.613
ND_2	(0x80, 0)	{29 ~ 18}	0.662
ND_3	(0x800000, 0),	{31, 30, 7 ~ 0}	0.620

Improved Partial Neural Distinguisher for Ciphertext

➢ Result of Key Recovery Attack for 10-Round SPECK64/96

Target	Round	Avg. Time[1]	hw(kg, rk)[2]	Conffgure	Reference
SPECK64/96	9	66s	1.93	$1 + 1r_{CD} + 6r_{ND}$	Chen et al.
		29s	0.80	$1 + 1r_{CD} + 6r_{ND}$	This paper
	10	424s	1.89	$1 + 1r_{CD} + 7r_{ND}$	This paper
SPECK96/96	10	303s	1	$1 + 1r_{CD} + 7r_{ND}$	Chen et al.
		163s	0.44	$1 + 1r_{CD} + 7r_{ND}$	This paper

Table of Contents

Summary

- A parallelizable multi-stage key recovery framework based on neural distinguishers, accelerating the key recovery attack on largestate block ciphers.
- Enhance the ability of the distinguisher in the multi-stage recovery framework.

Thank you!

Q & A