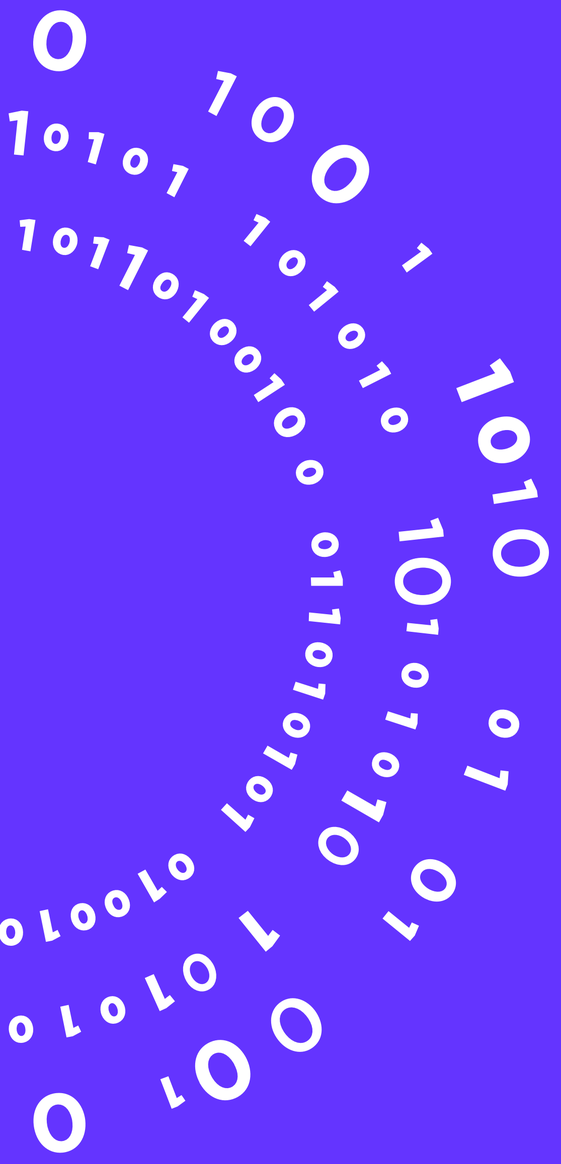


Cryptography Research Centre

Boosting Differential-Linear Cryptanalysis of ChaCha7 with MILP

Emanuele Bellini[1], David Gerault[1], Juan Grados[1], Rusydi H. Makarim[2], Thomas Peyrin[3]

1 Technology Innovation Institute, Abu Dhabi, UAE
2 Independent Researcher, Indonesia
3 Nanyang Technological University, Singapore

FSE 2024

TII Technology Innovation Institute

Outline

Cryptography Research Centre

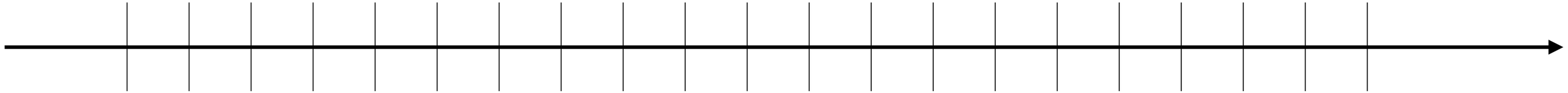
- Review of Cryptanalysis against ChaCha
- Contributions
  - Flipping 2-bit instead of 1
  - Crafting choosing intermediate states
  - MILP implementation of ChaCha
  - Distinguishers and Key-Recovery against ChaCha
- Conclusions

Related Works

Attacking ChaCha

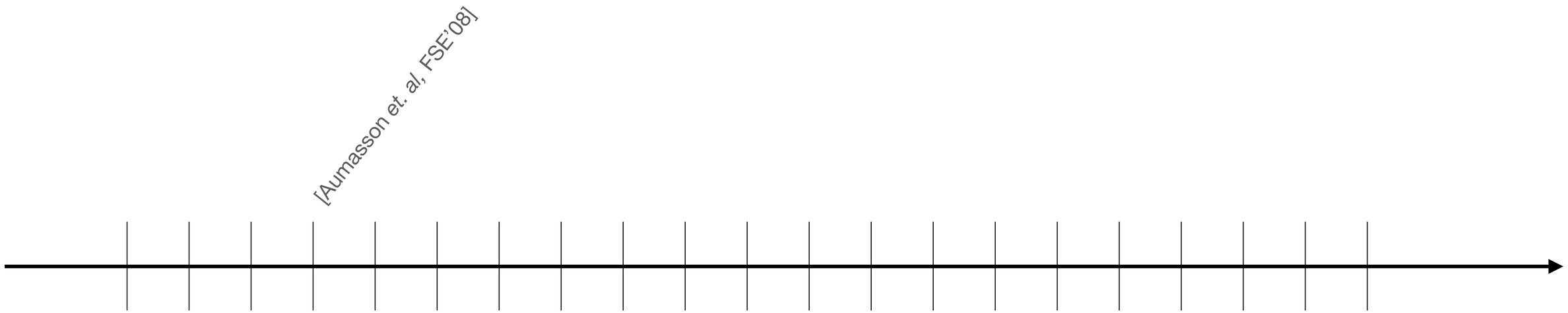
Related Works

Attacking ChaCha



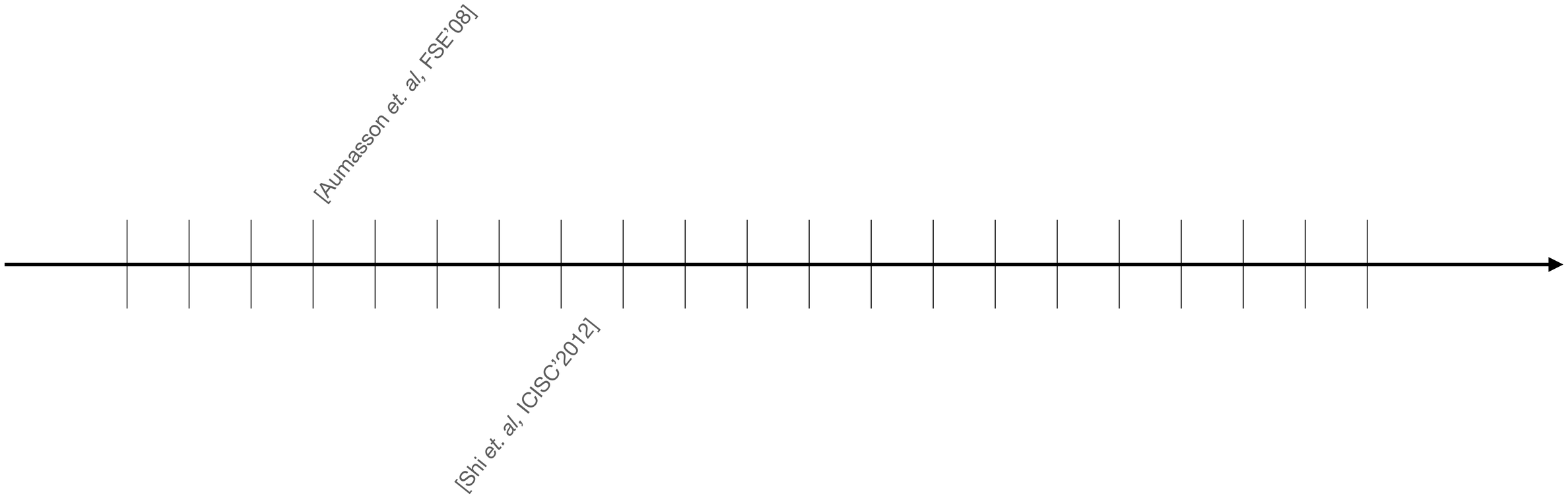
Related Works

Attacking ChaCha



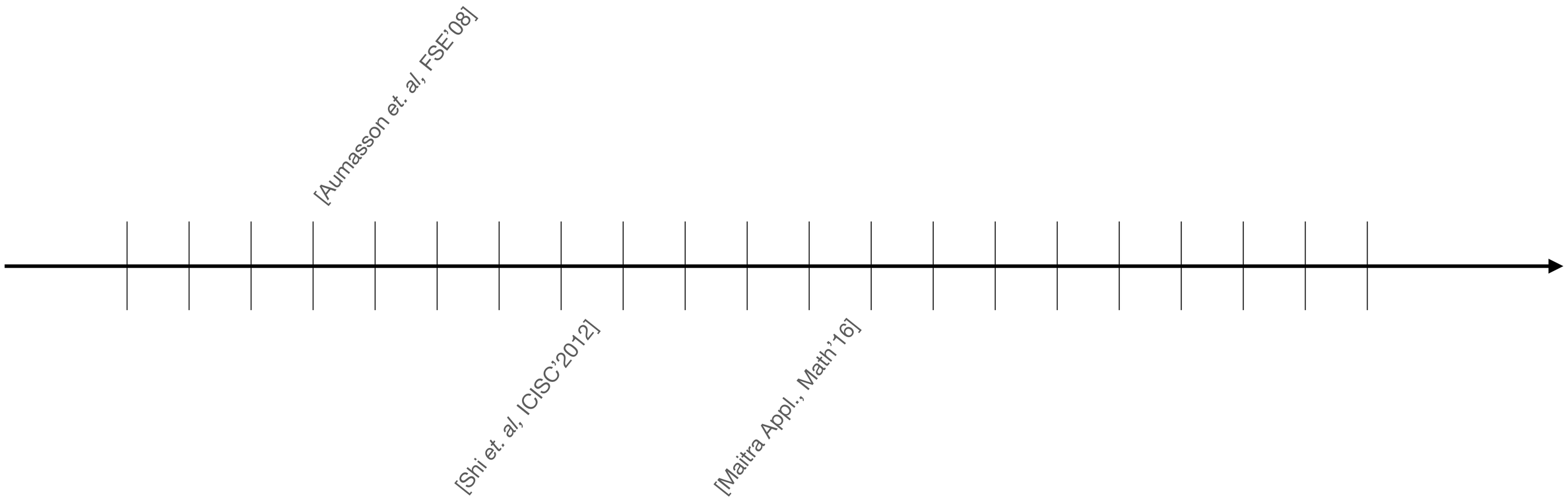
Related Works

Attacking ChaCha



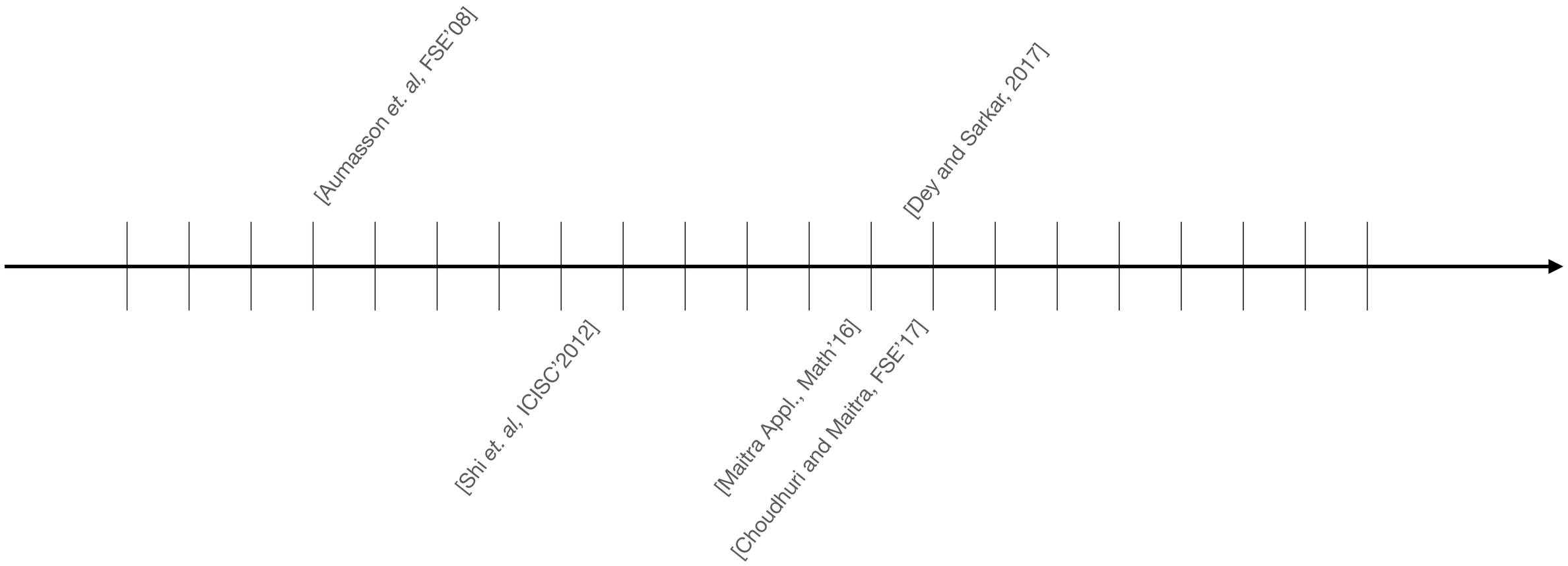
Related Works

Attacking ChaCha



Related Works

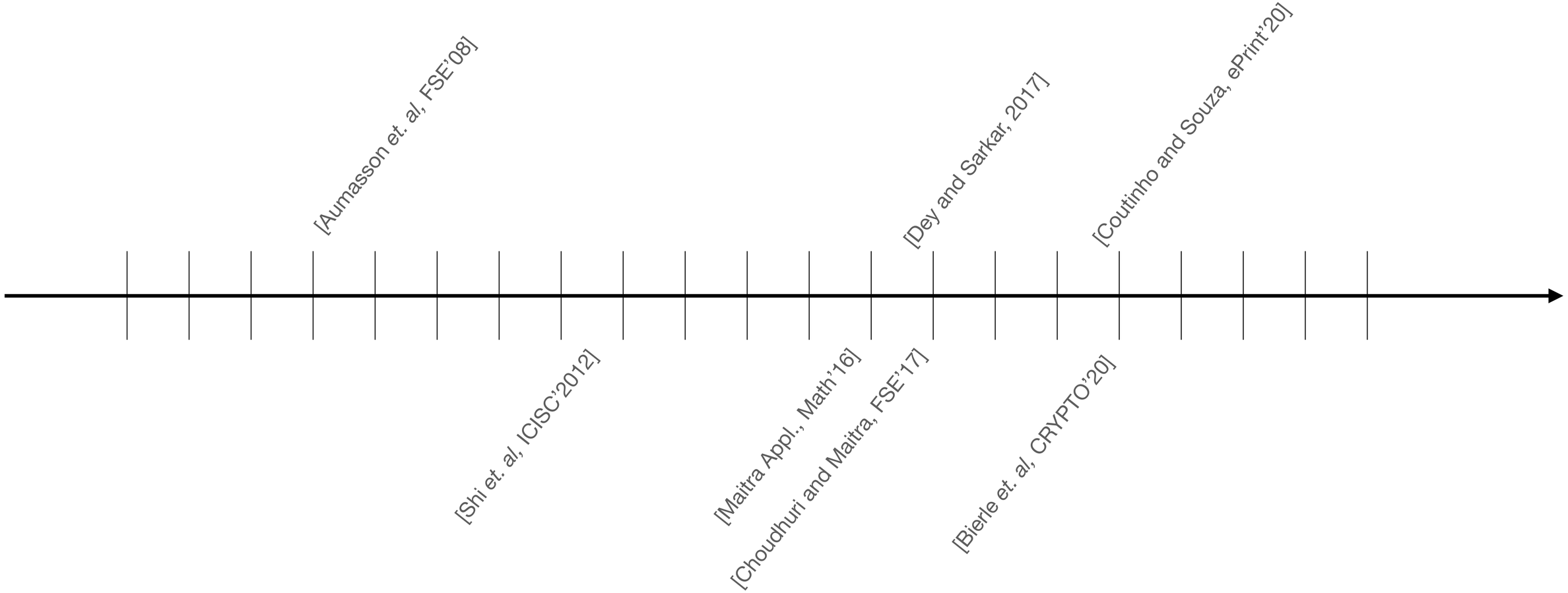
Attacking ChaCha



Cryptography Research Centre

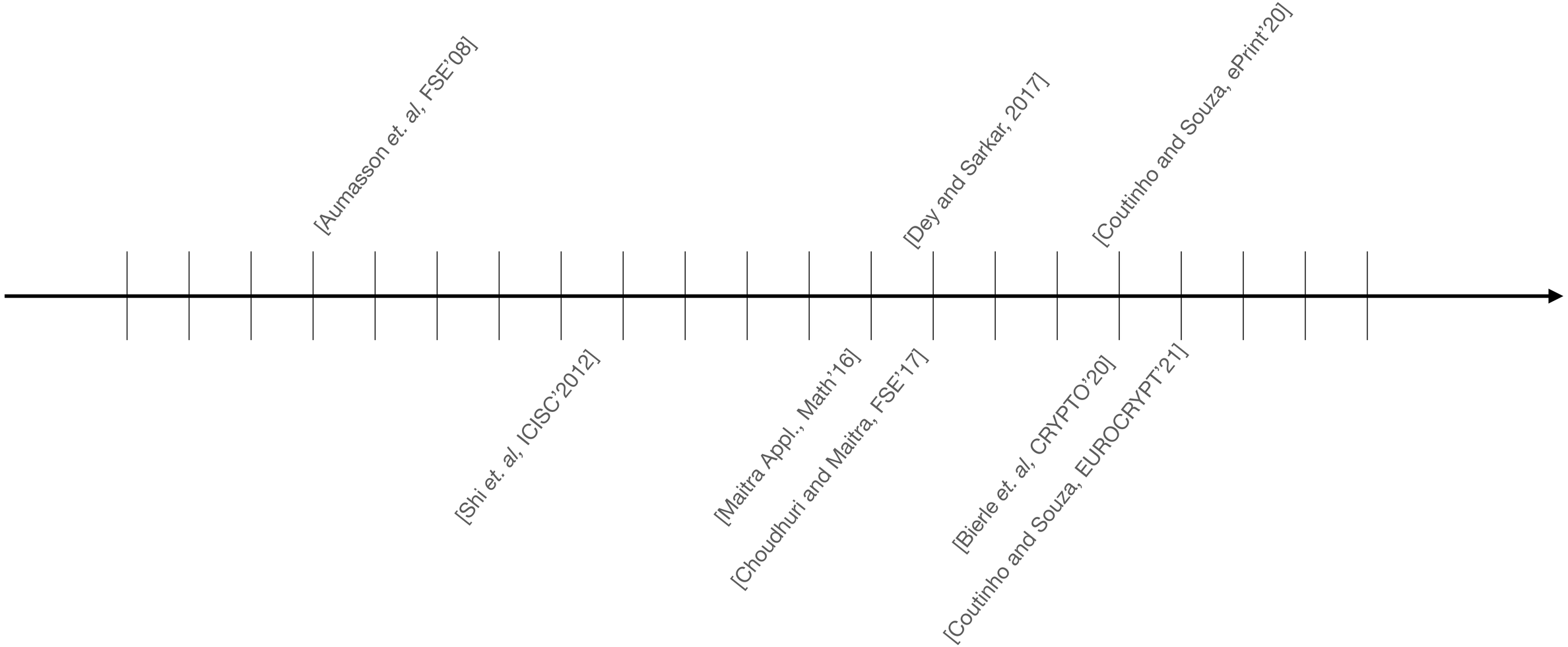
Related Works

Attacking ChaCha



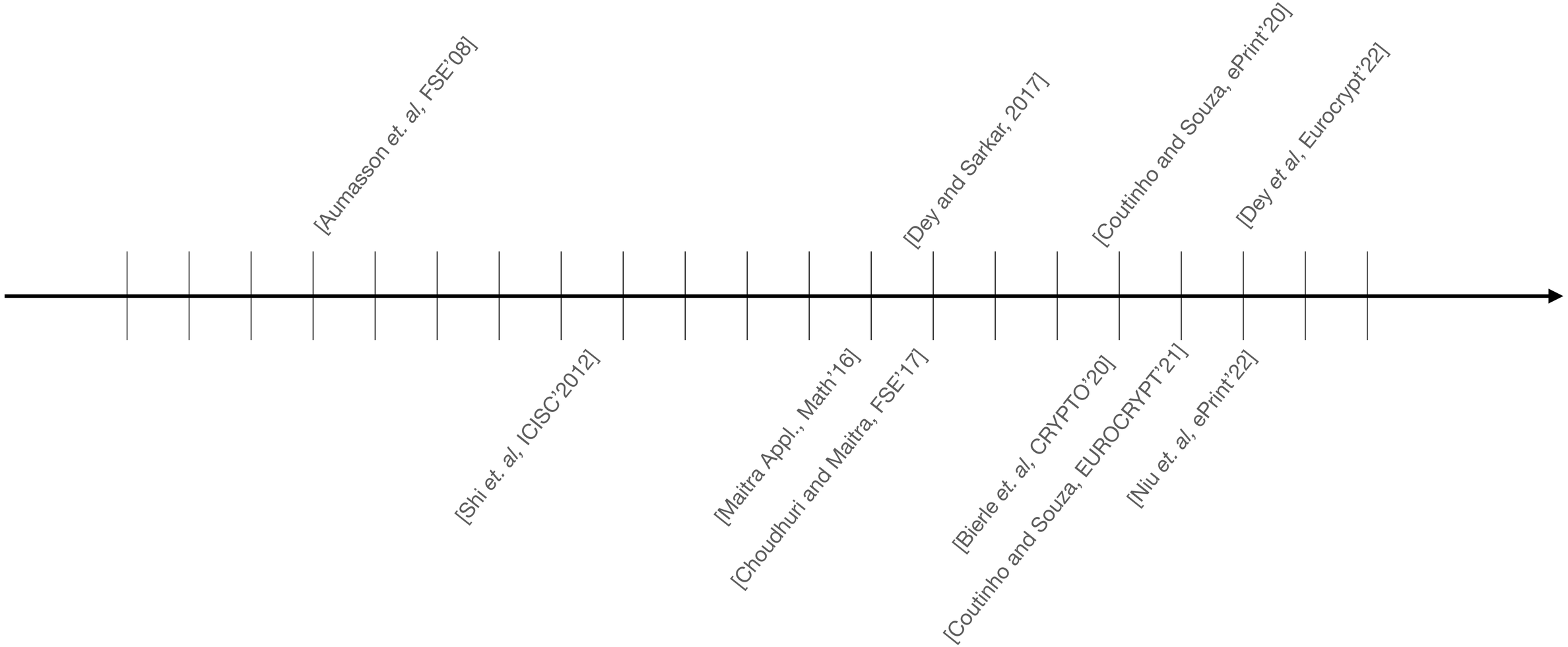
Related Works

Attacking ChaCha



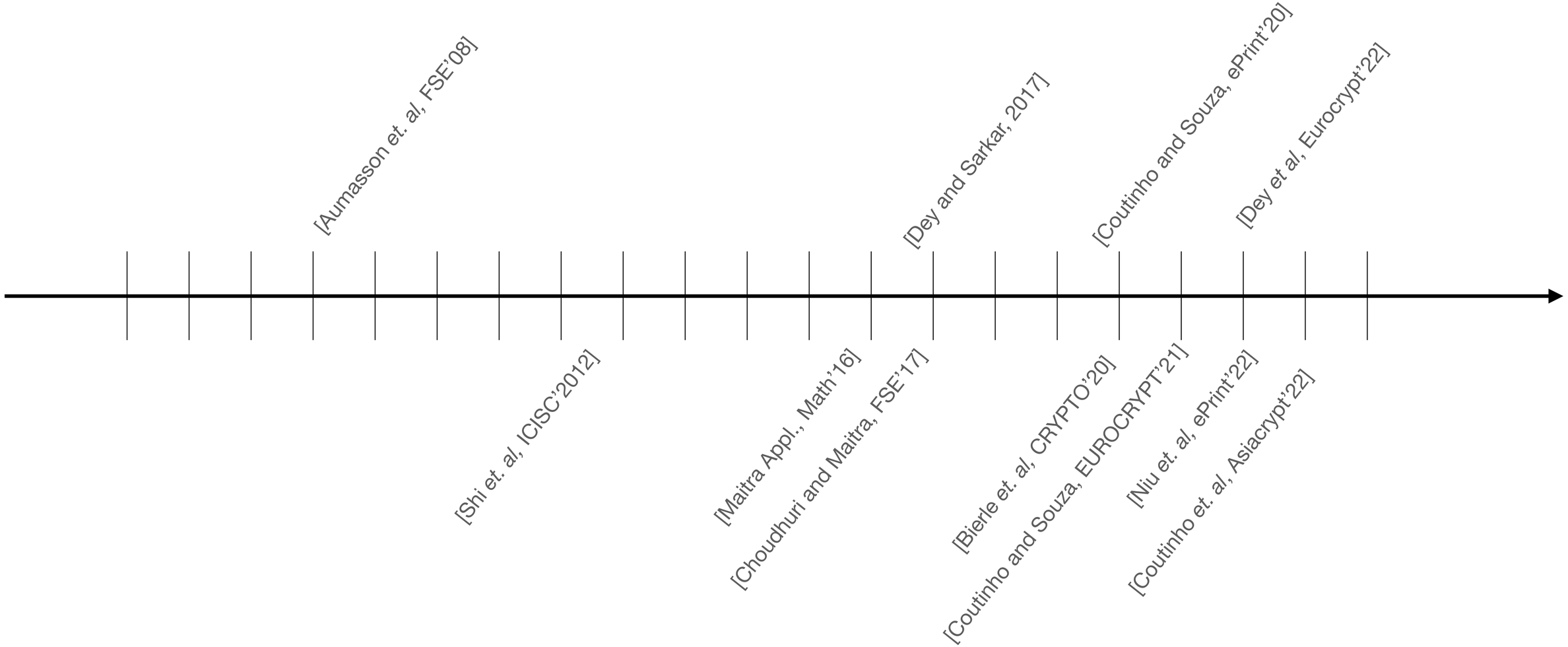
Related Works

Attacking ChaCha



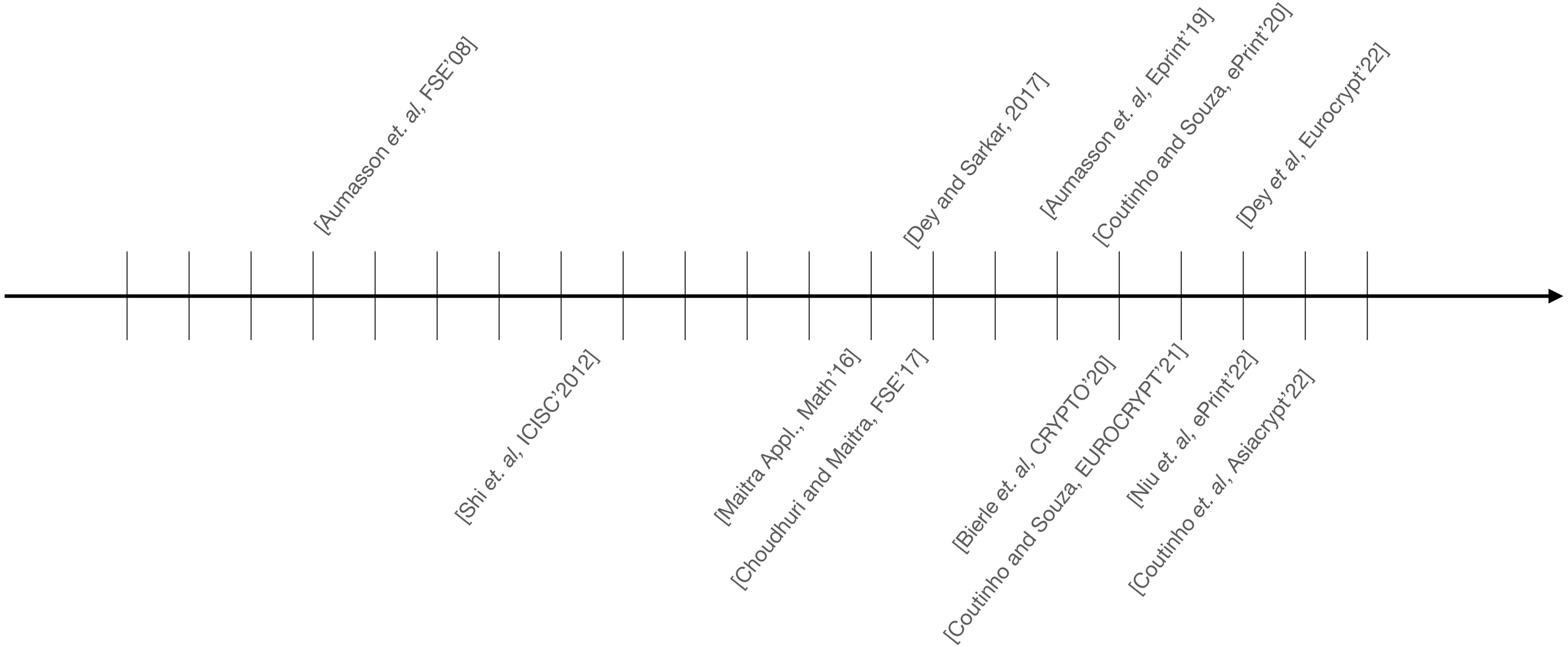
Related Works

Attacking ChaCha



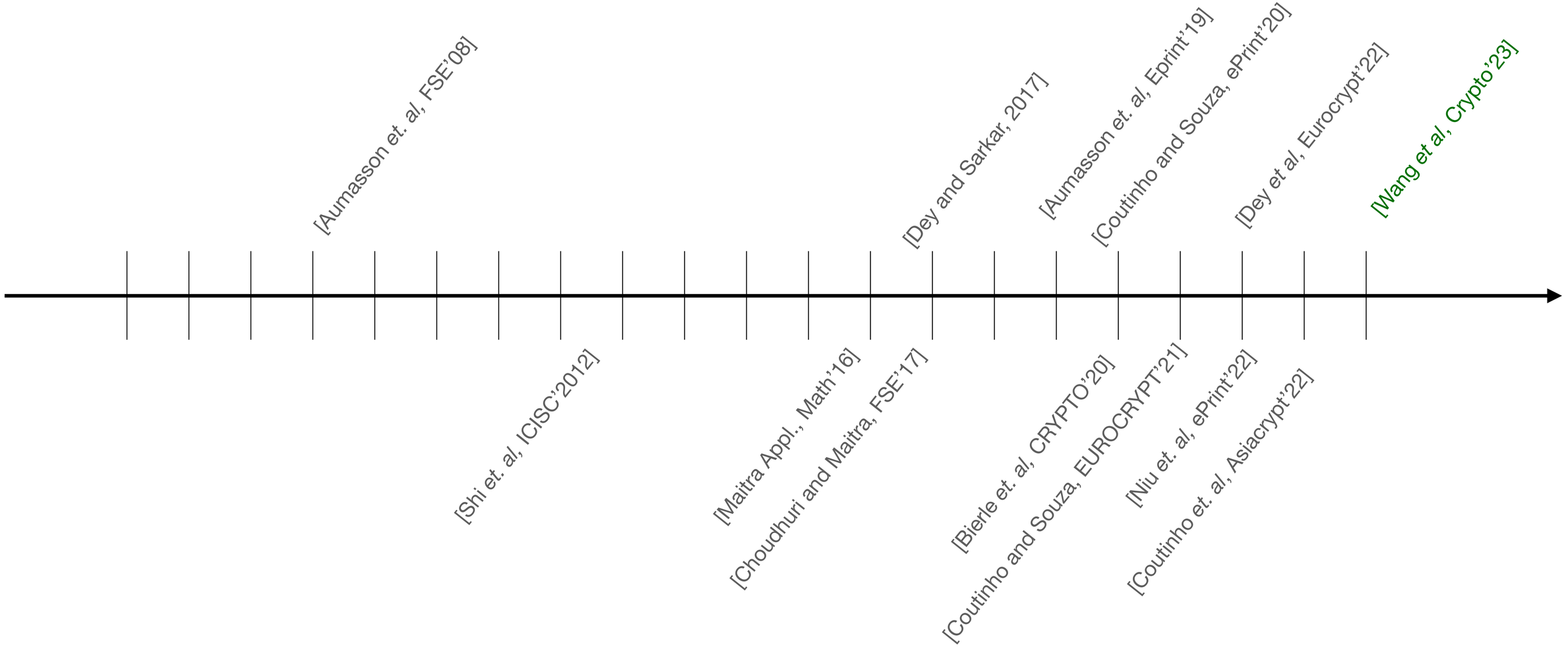
Related Works

Attacking ChaCha



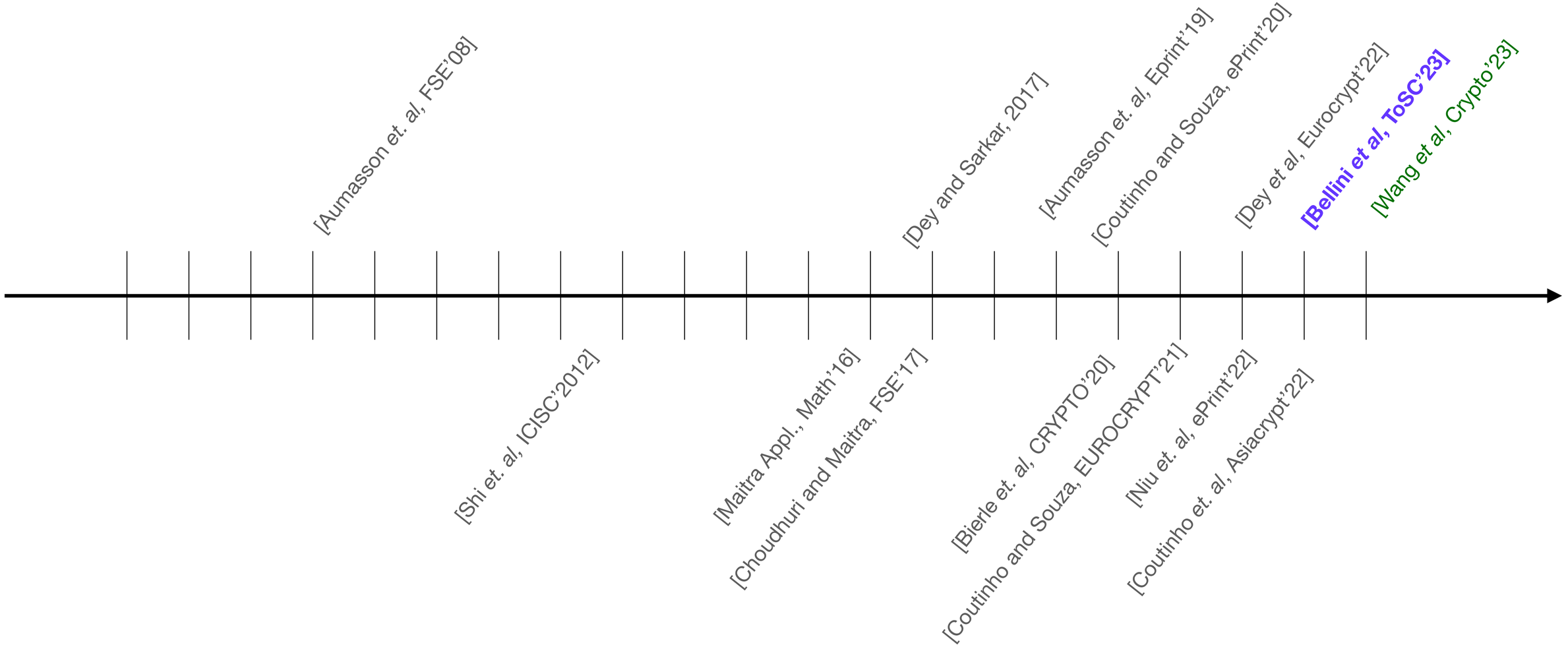
Related Works

Attacking ChaCha



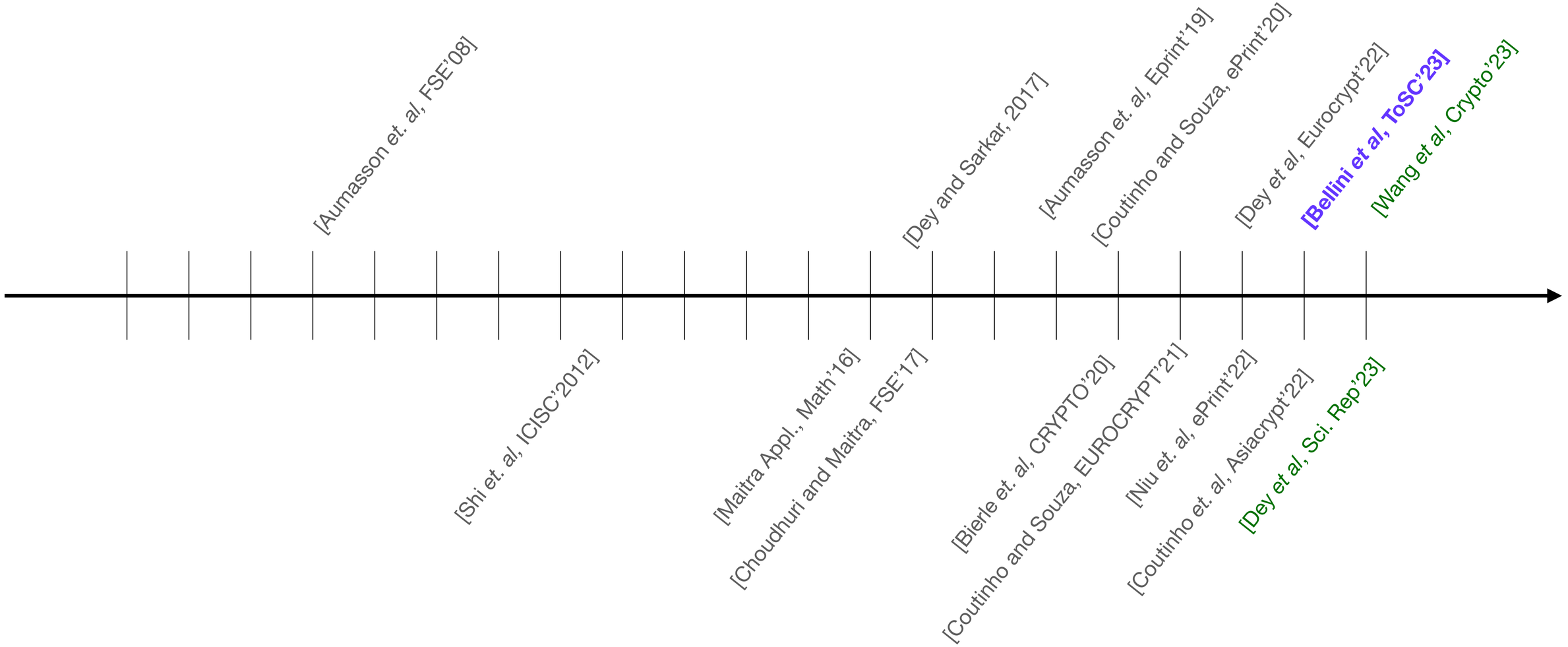
Related Works

Attacking ChaCha



Related Works

Attacking ChaCha



Background

ChaCha description

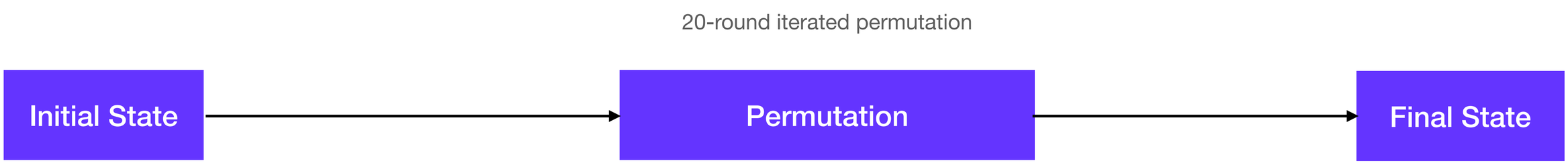
Cryptography Research Centre

- Stream cipher invented by Daniel J. Bernstein
- Fast in software environment
- Resistance against timing attacks and cache attacks
- Better Diffusion than Salsa
- Actually used in TLS v1.3
- There are some proposes to use ChaCha reduced to 8 rounds. Example: “Too Much Crypto” [Aumasson *et* al, 2019].

Chacha stream cipher

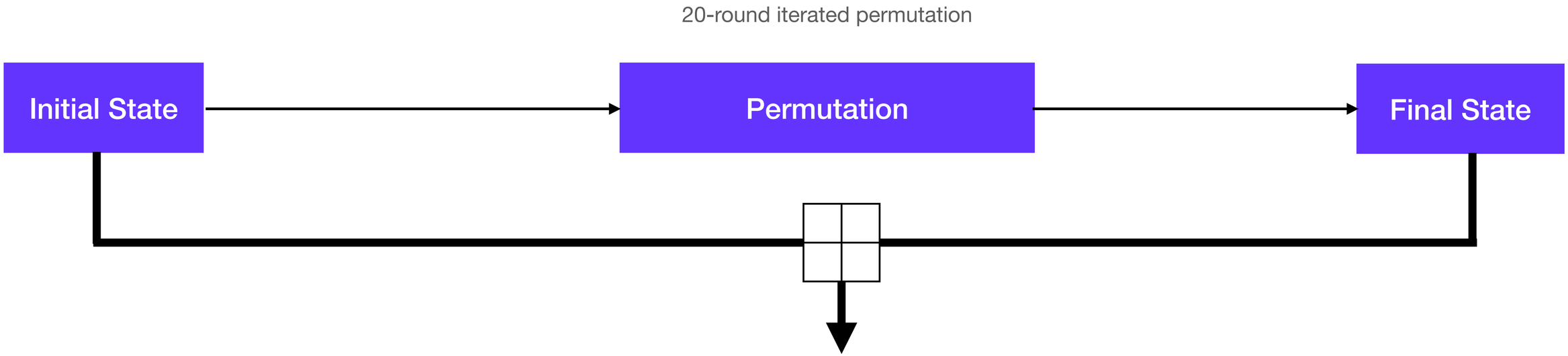
High Level Design

Cryptography Research Centre



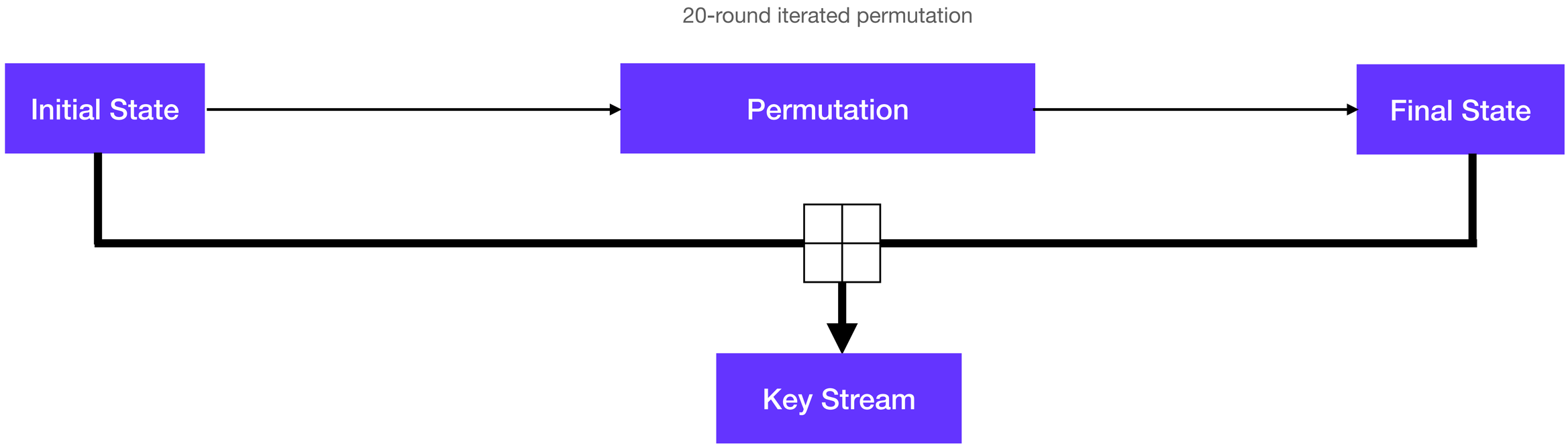
Chacha stream cipher

High Level Design



Chacha stream cipher

High Level Design



Background

ChaCha 2 rounds

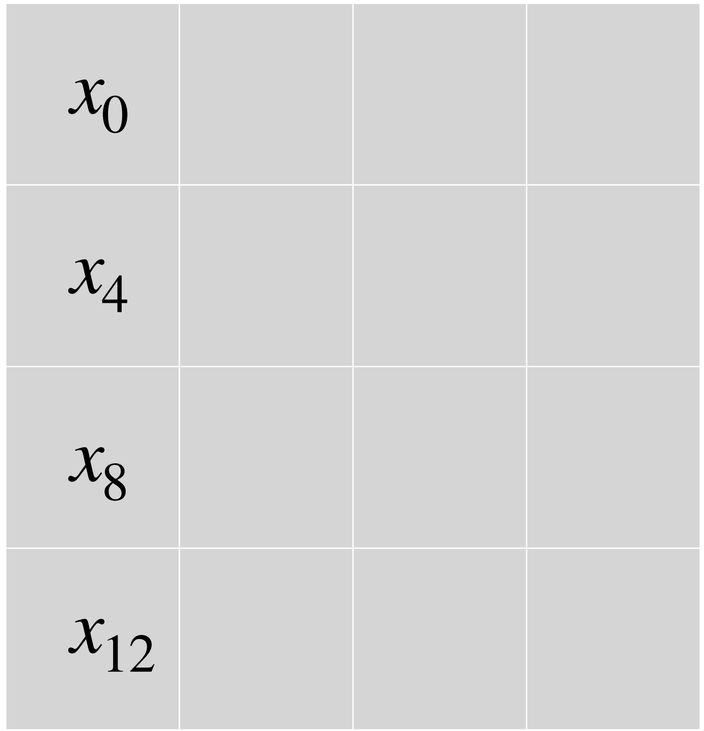
x_0 x_4 x_8 x_{12} x_1 x_5 x_9 x_{13} x_2 x_6 x_{10} x_{14} x_3 x_7 x_{11} x_{15}

x_0 x_4 x_8 x_{12} x_1 x_5 x_9 x_{13} x_2 x_6 x_{10} x_{14} x_3 x_7 x_{11} x_{15}

x_0 x_5 x_{10} x_{15} x_1 x_6 x_{11} x_{12} x_2 x_7 x_8 x_{13} x_3 x_4 x_9 x_{14}

Background

ChaCha 2 rounds



x_1 x_5 x_9 x_{13}

x_1 x_5 x_9 x_{13}

x_2 x_6 x_{10} x_{14}

x_2 x_6 x_{10} x_{14}

x_3 x_7 x_{11} x_{15}

x_3 x_7 x_{11} x_{15}

x_0 x_5 x_{10} x_{15}

x_1 x_6 x_{11} x_{12}

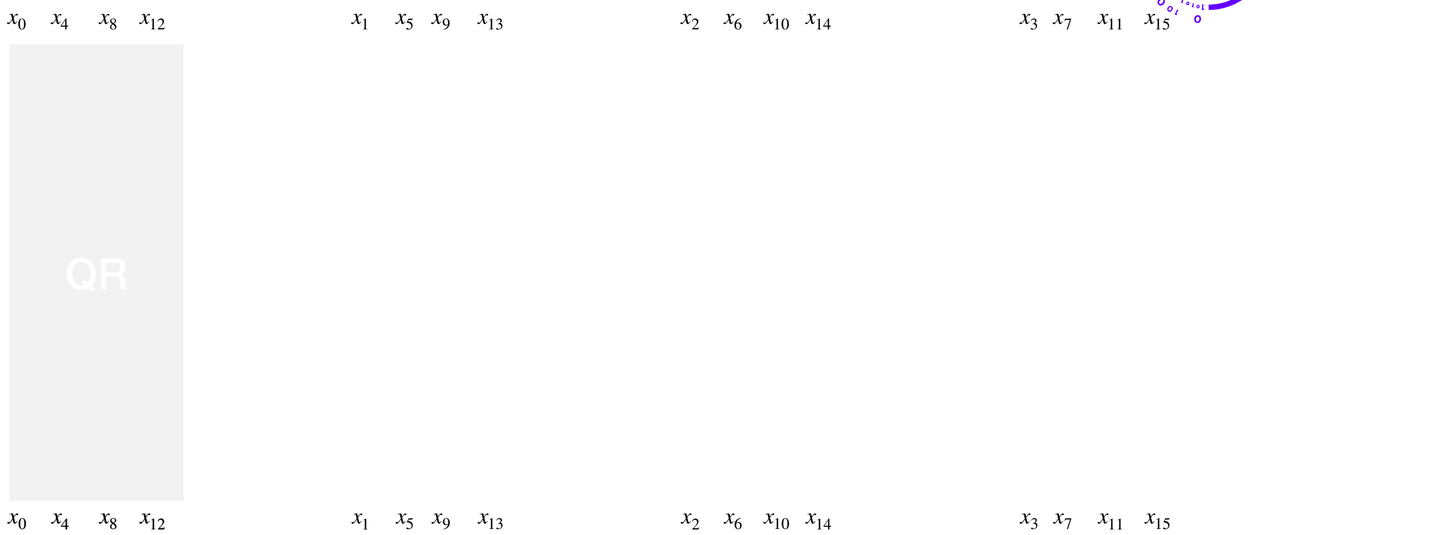
x_2 x_7 x_8 x_{13}

x_3 x_4 x_9 x_{14}

Background

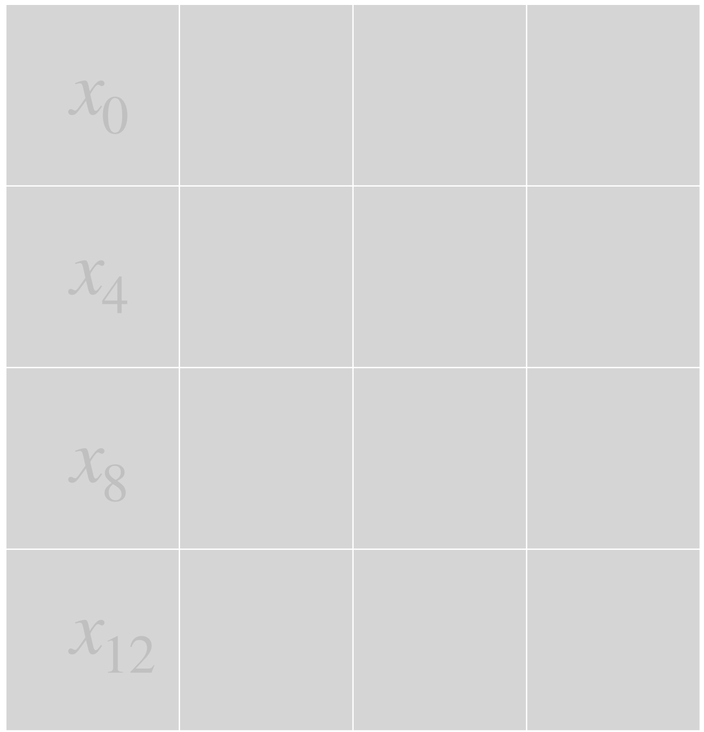
ChaCha 2 rounds

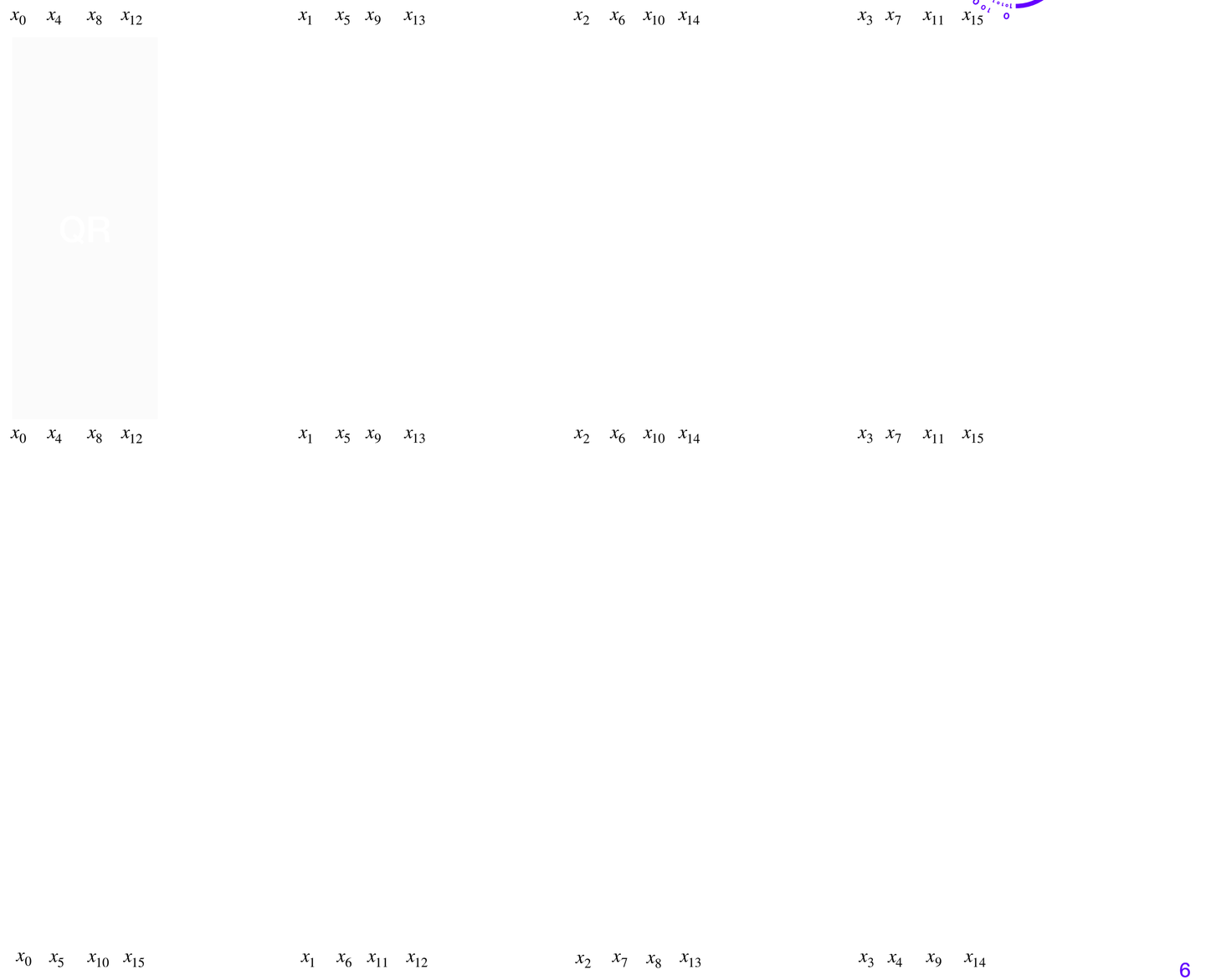
x_0			
x_4			
x_8			
x_{12}			



Background

ChaCha 2 rounds

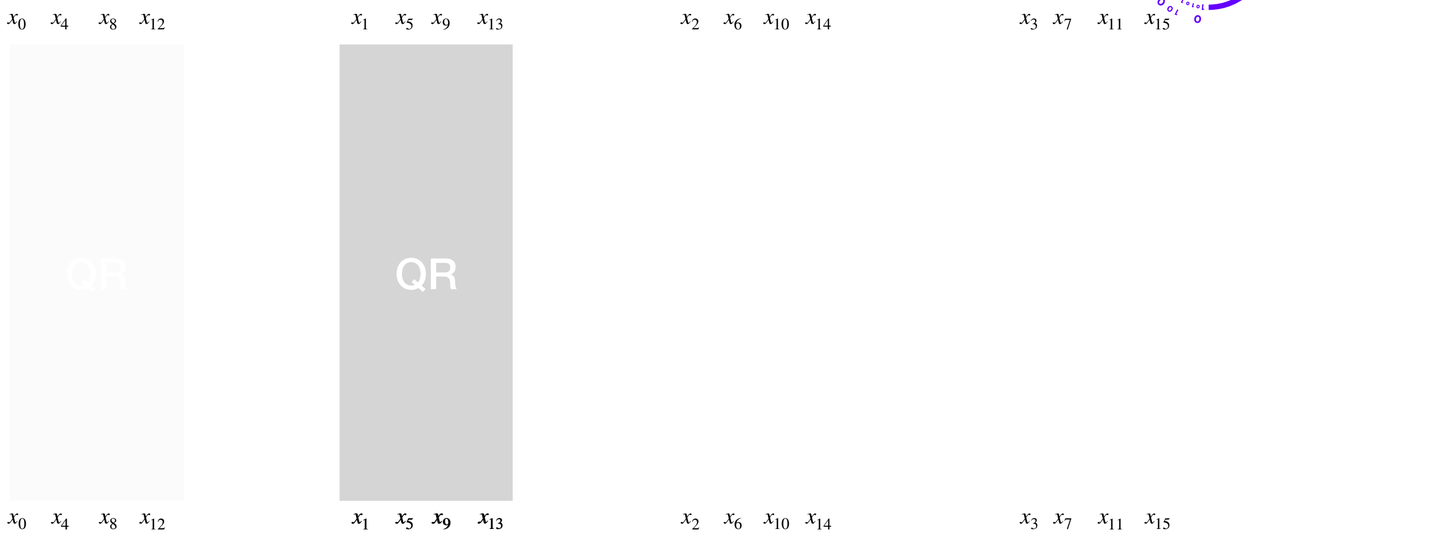




Background

ChaCha 2 rounds

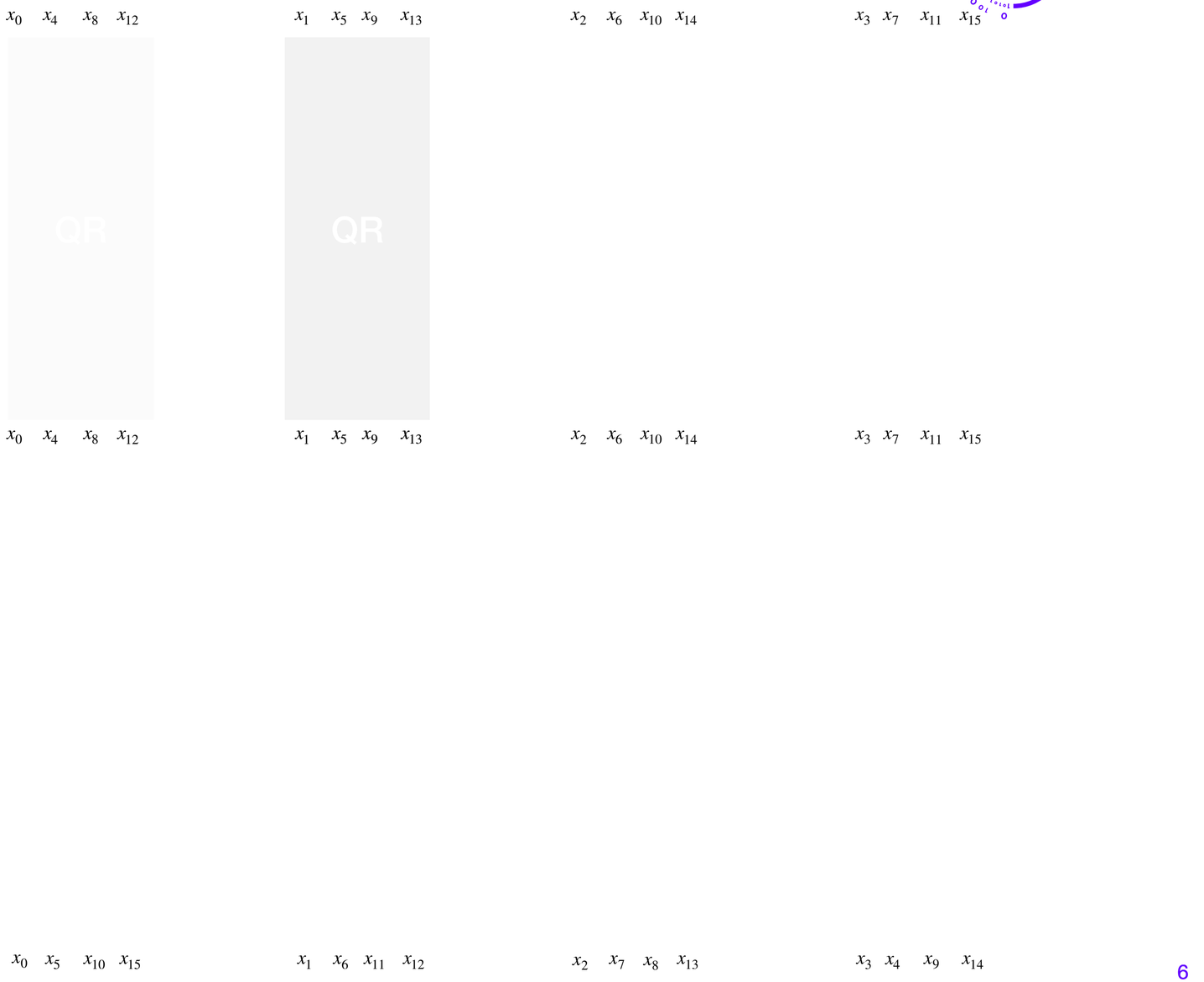
x_0	x_1		
x_4	x_5		
x_8	x_9		
x_{12}	x_{13}		



x_0 x_5 x_{10} x_{15} x_1 x_6 x_{11} x_{12} x_2 x_7 x_8 x_{13} x_3 x_4 x_9 x_{14}

Background

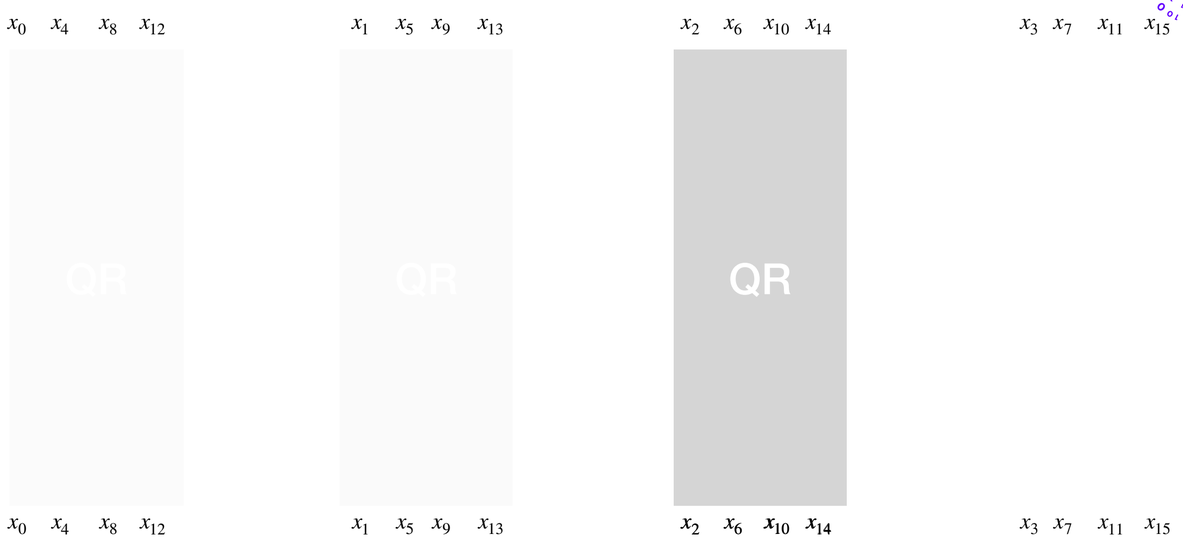
ChaCha 2 rounds



Background

ChaCha 2 rounds

x_0	x_1	x_2	
x_4	x_5	x_6	
x_8	x_9	x_{10}	
x_{12}	x_{13}	x_{14}	

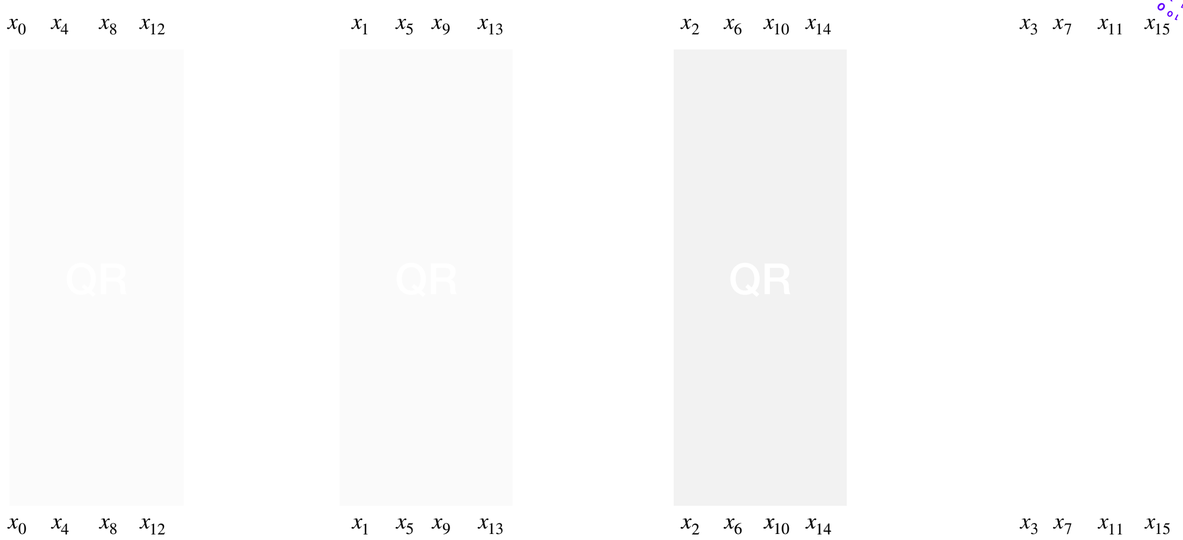


x_0 x_5 x_{10} x_{15} x_1 x_6 x_{11} x_{12} x_2 x_7 x_8 x_{13} x_3 x_4 x_9 x_{14}

Background

ChaCha 2 rounds

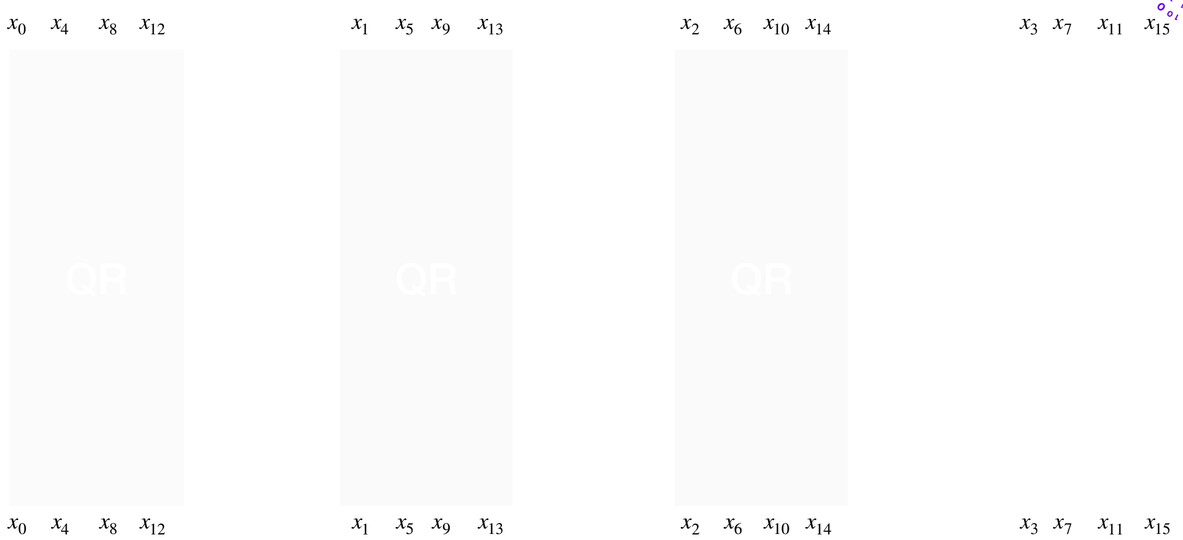
x_0	x_1	x_2	
x_4	x_5	x_6	
x_8	x_9	x_{10}	
x_{12}	x_{13}	x_{14}	



Background

ChaCha 2 rounds

x_0	x_1	x_2	
x_4	x_5	x_6	
x_8	x_9	x_{10}	
x_{12}	x_{13}	x_{14}	

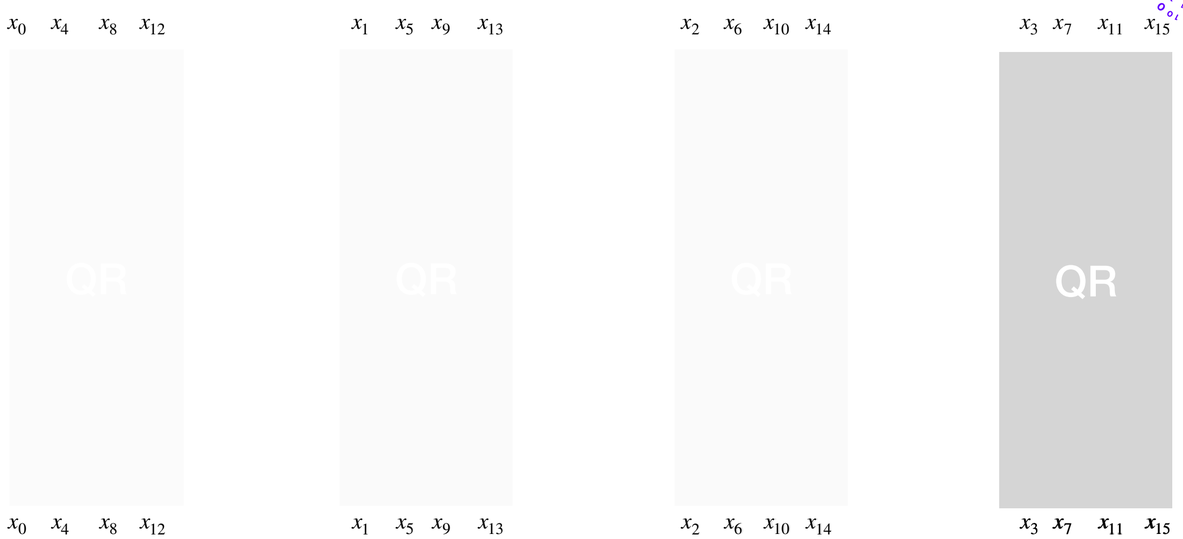


x_0 x_5 x_{10} x_{15} x_1 x_6 x_{11} x_{12} x_2 x_7 x_8 x_{13} x_3 x_4 x_9 x_{14}

Background

ChaCha 2 rounds

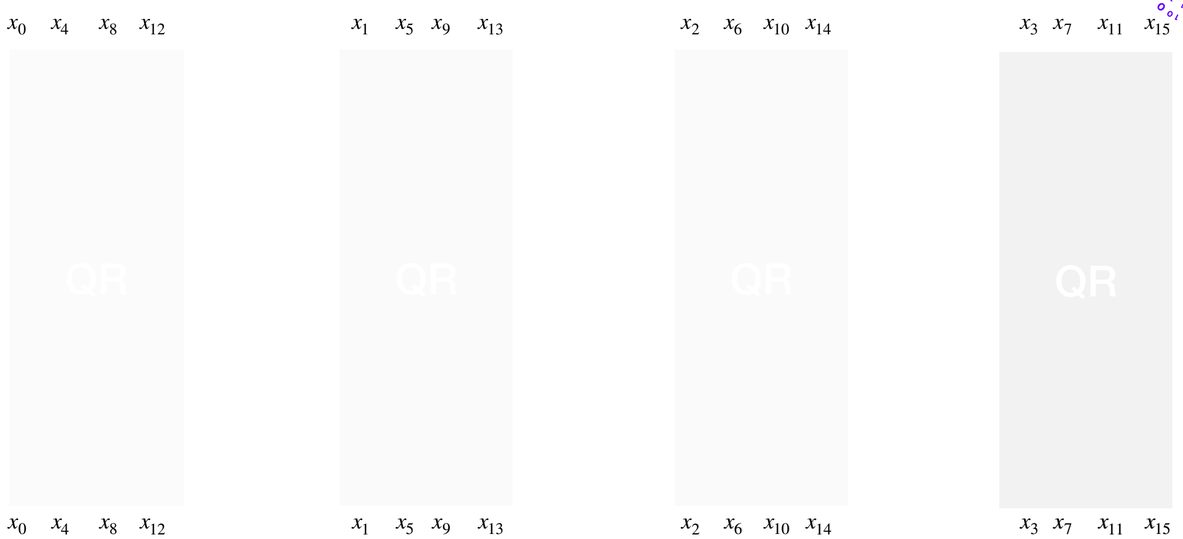
x_0	x_1	x_2	x_3
x_4	x_5	x_6	x_7
x_8	x_9	x_{10}	x_{11}
x_{12}	x_{13}	x_{14}	x_{15}



Background

ChaCha 2 rounds

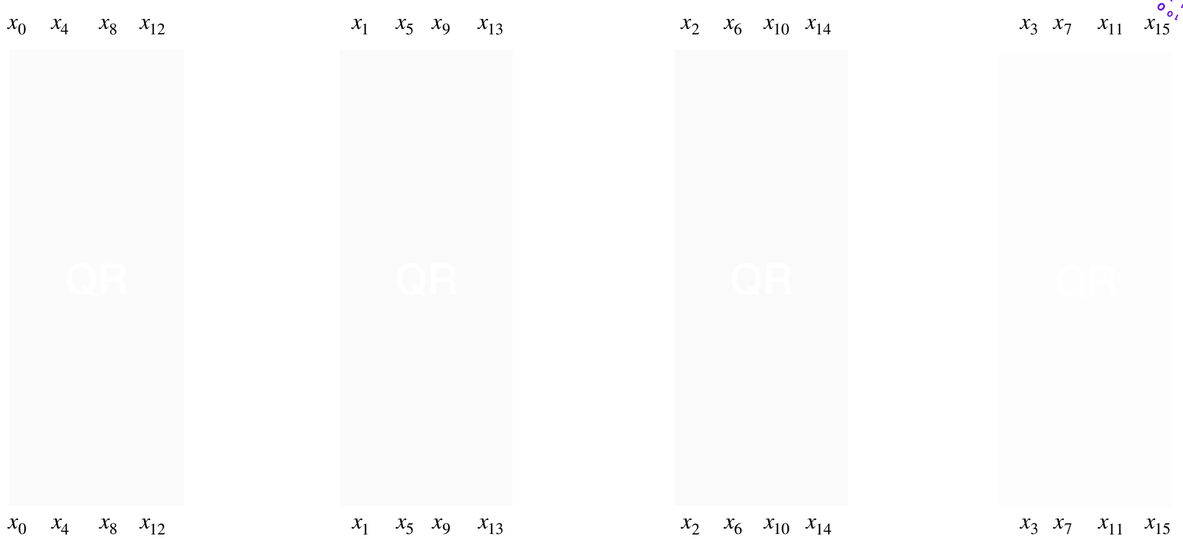
x_0	x_1	x_2	x_3
x_4	x_5	x_6	x_7
x_8	x_9	x_{10}	x_{11}
x_{12}	x_{13}	x_{14}	x_{15}



Background

ChaCha 2 rounds

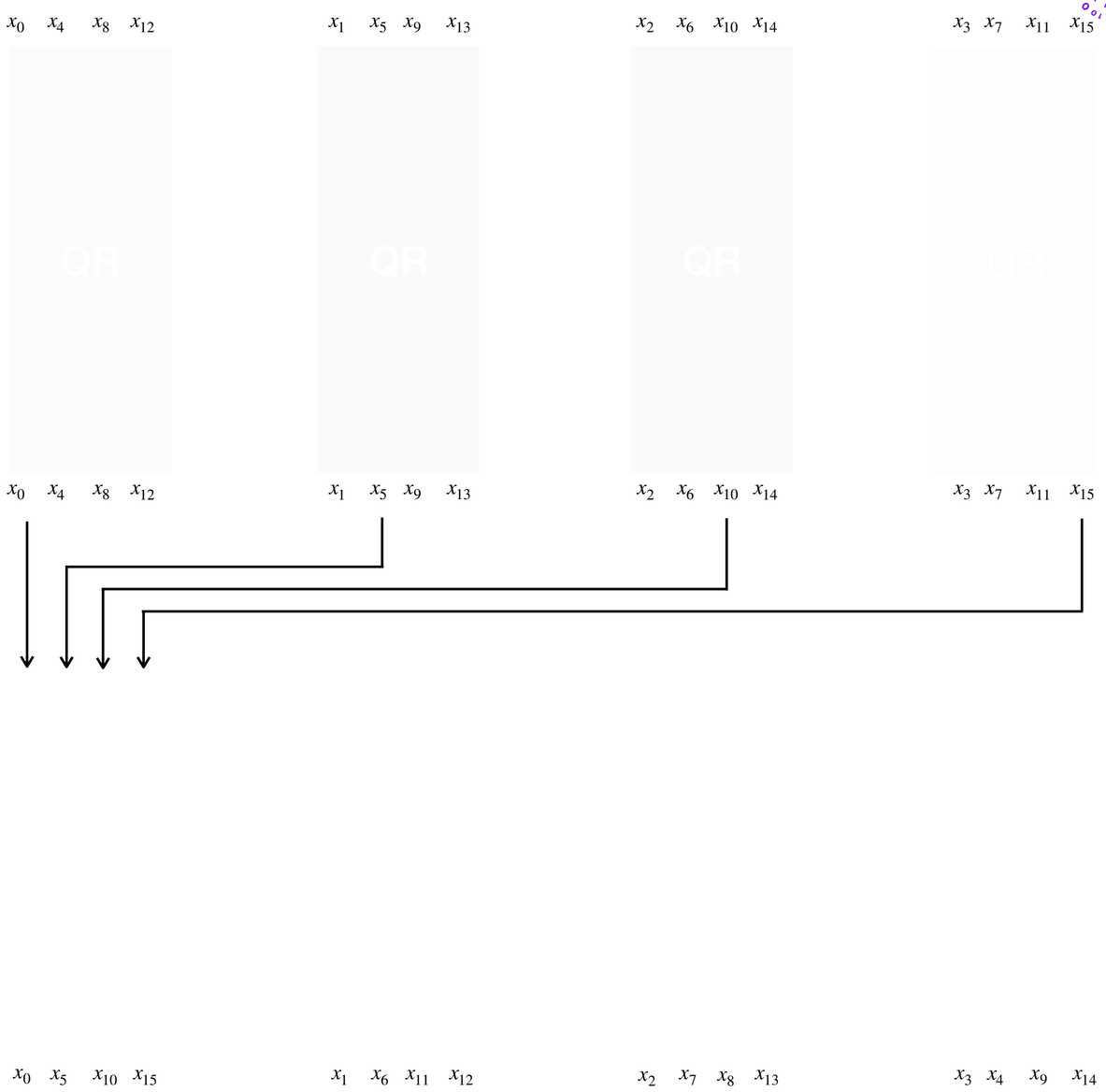
x_0	x_1	x_2	x_3
x_4	x_5	x_6	x_7
x_8	x_9	x_{10}	x_{11}
x_{12}	x_{13}	x_{14}	x_{15}



Background

ChaCha 2 rounds

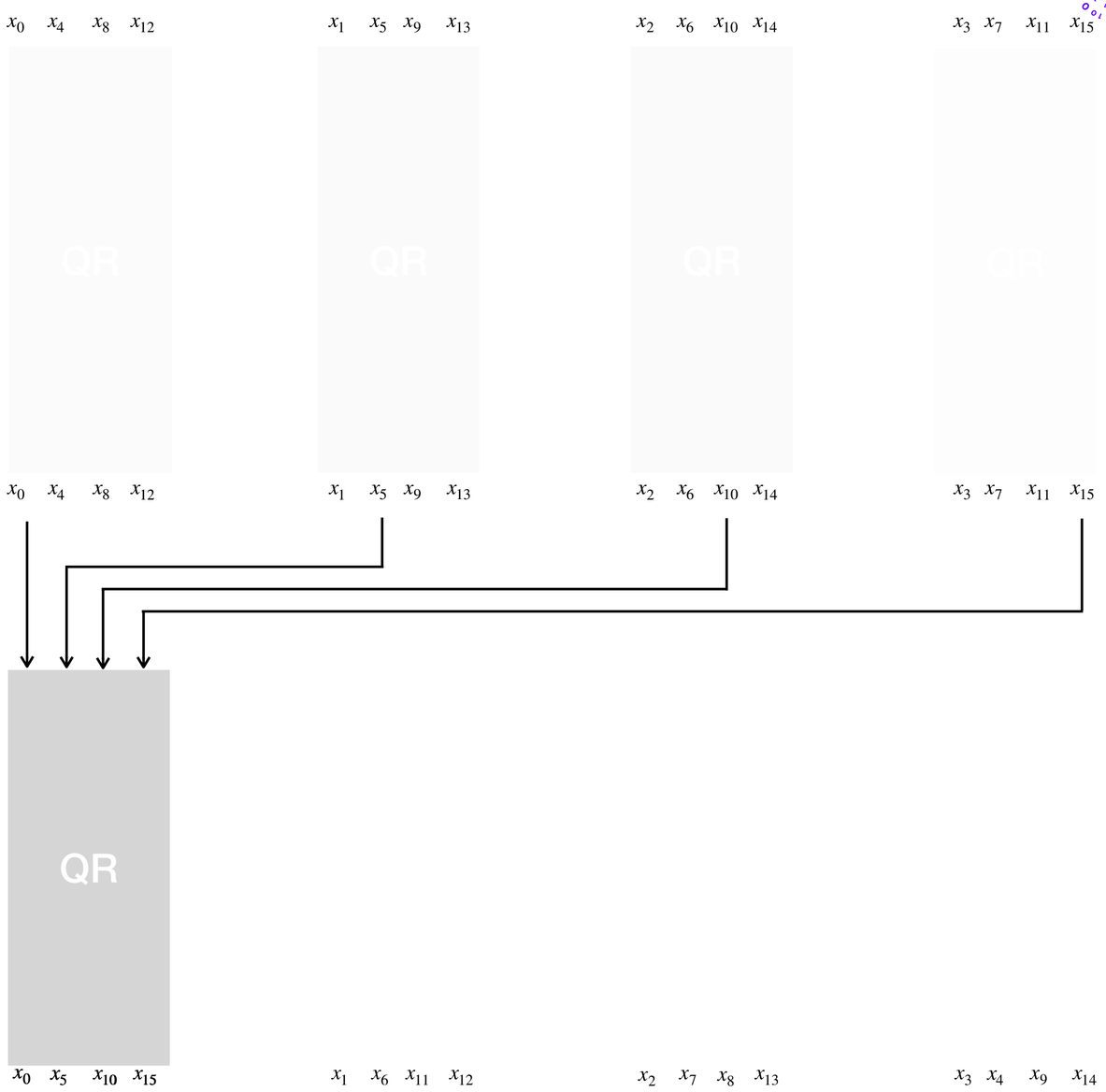
x_0	x_1	x_2	x_3
x_4	x_5	x_6	x_7
x_8	x_9	x_{10}	x_{11}
x_{12}	x_{13}	x_{14}	x_{15}



Background

ChaCha 2 rounds

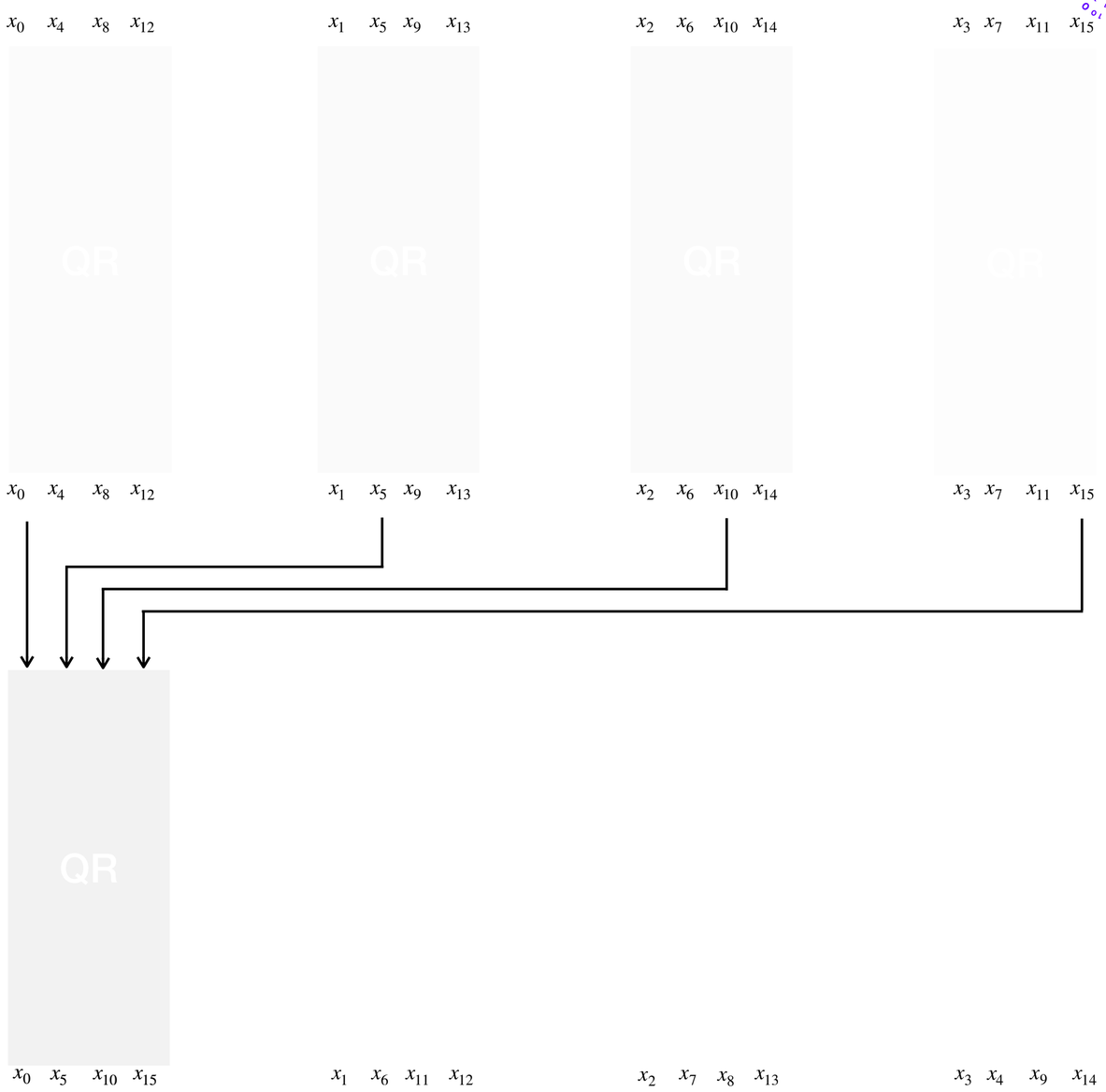
x_0	x_1	x_2	x_3
x_4	x_5	x_6	x_7
x_8	x_9	x_{10}	x_{11}
x_{12}	x_{13}	x_{14}	x_{15}



Background

ChaCha 2 rounds

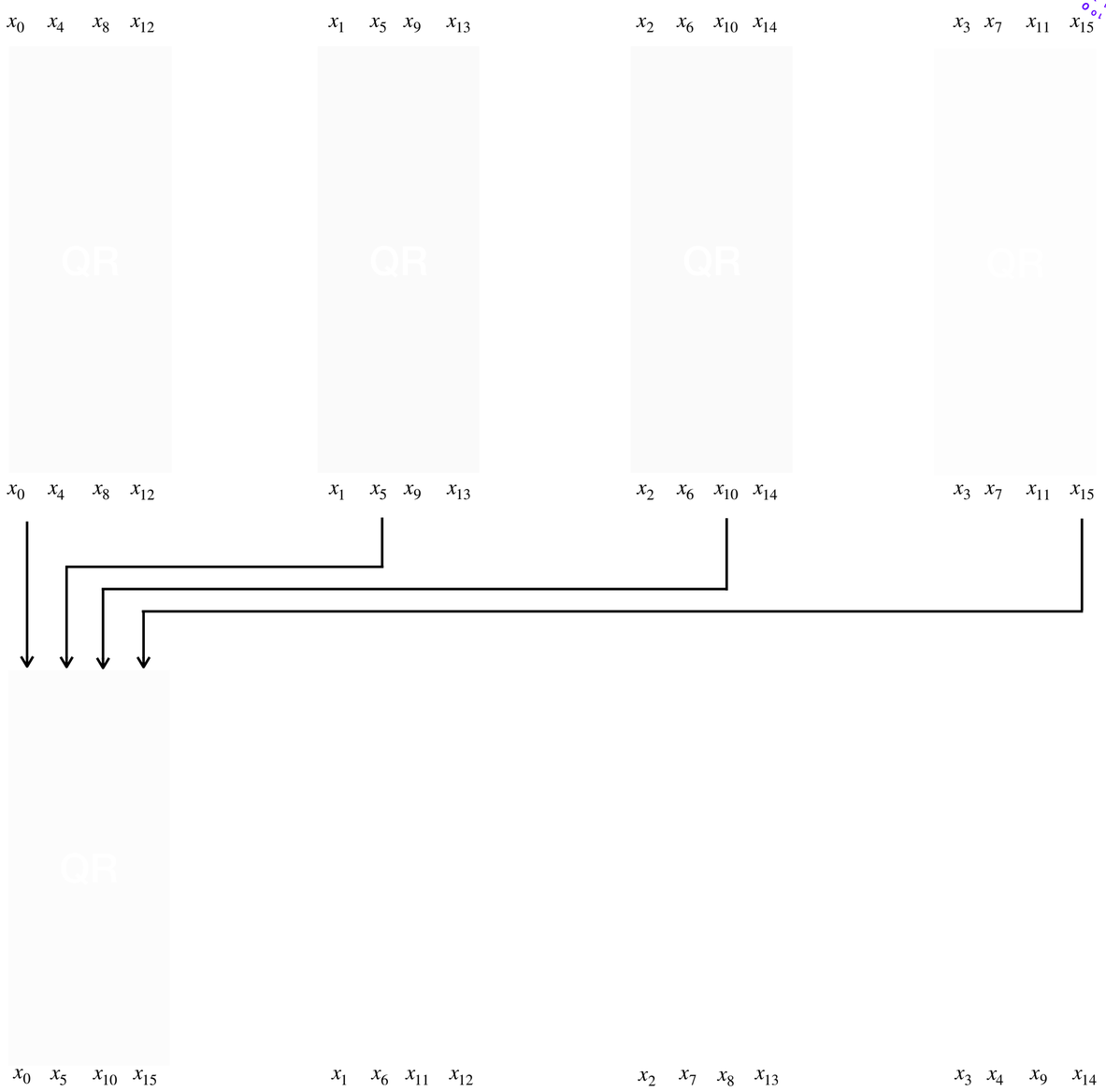
x_0	x_1	x_2	x_3
x_4	x_5	x_6	x_7
x_8	x_9	x_{10}	x_{11}
x_{12}	x_{13}	x_{14}	x_{15}



Background

ChaCha 2 rounds

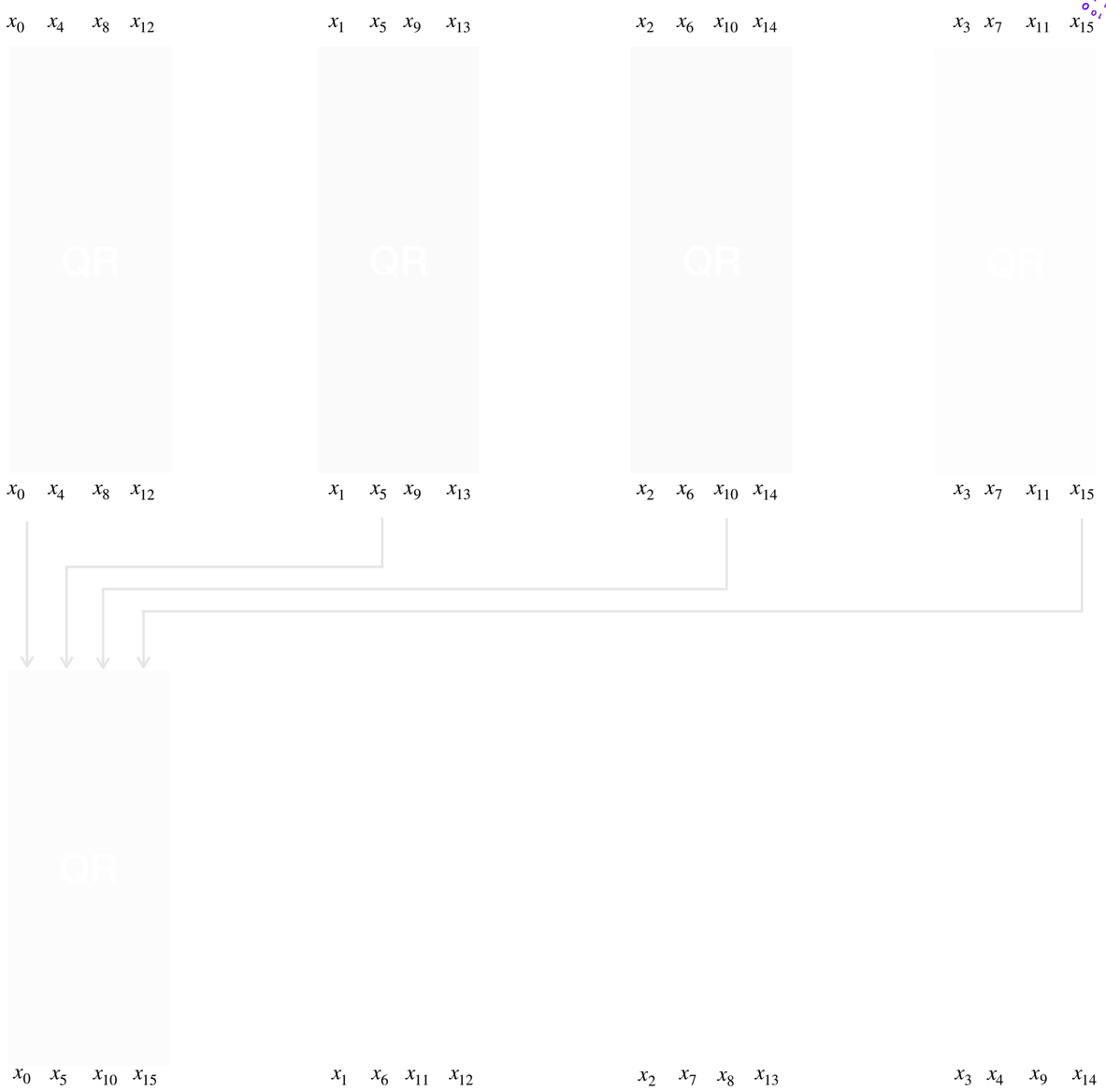
x_0	x_1	x_2	x_3
x_4	x_5	x_6	x_7
x_8	x_9	x_{10}	x_{11}
x_{12}	x_{13}	x_{14}	x_{15}



Background

ChaCha 2 rounds

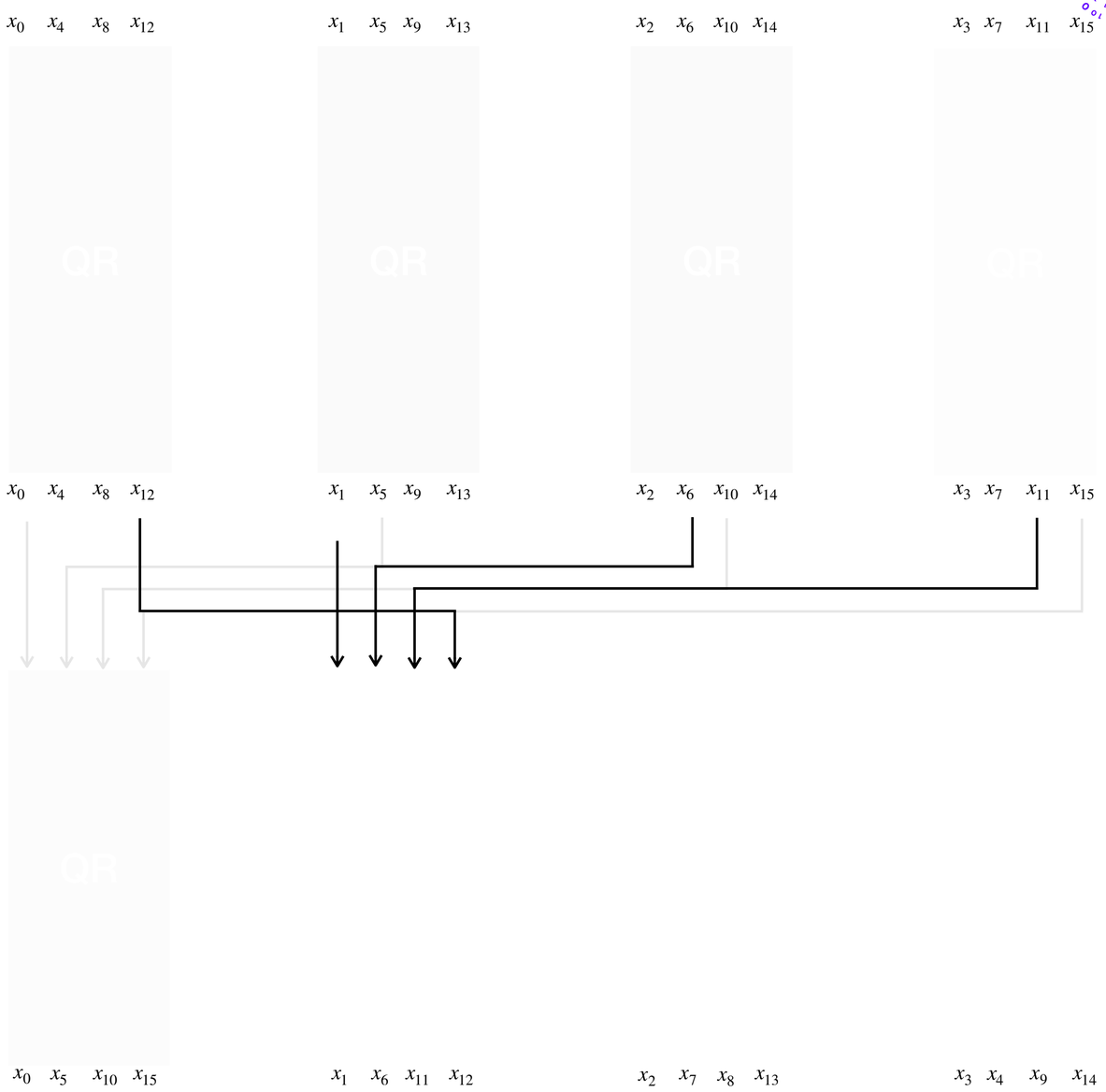
x_0	x_1	x_2	x_3
x_4	x_5	x_6	x_7
x_8	x_9	x_{10}	x_{11}
x_{12}	x_{13}	x_{14}	x_{15}



Background

ChaCha 2 rounds

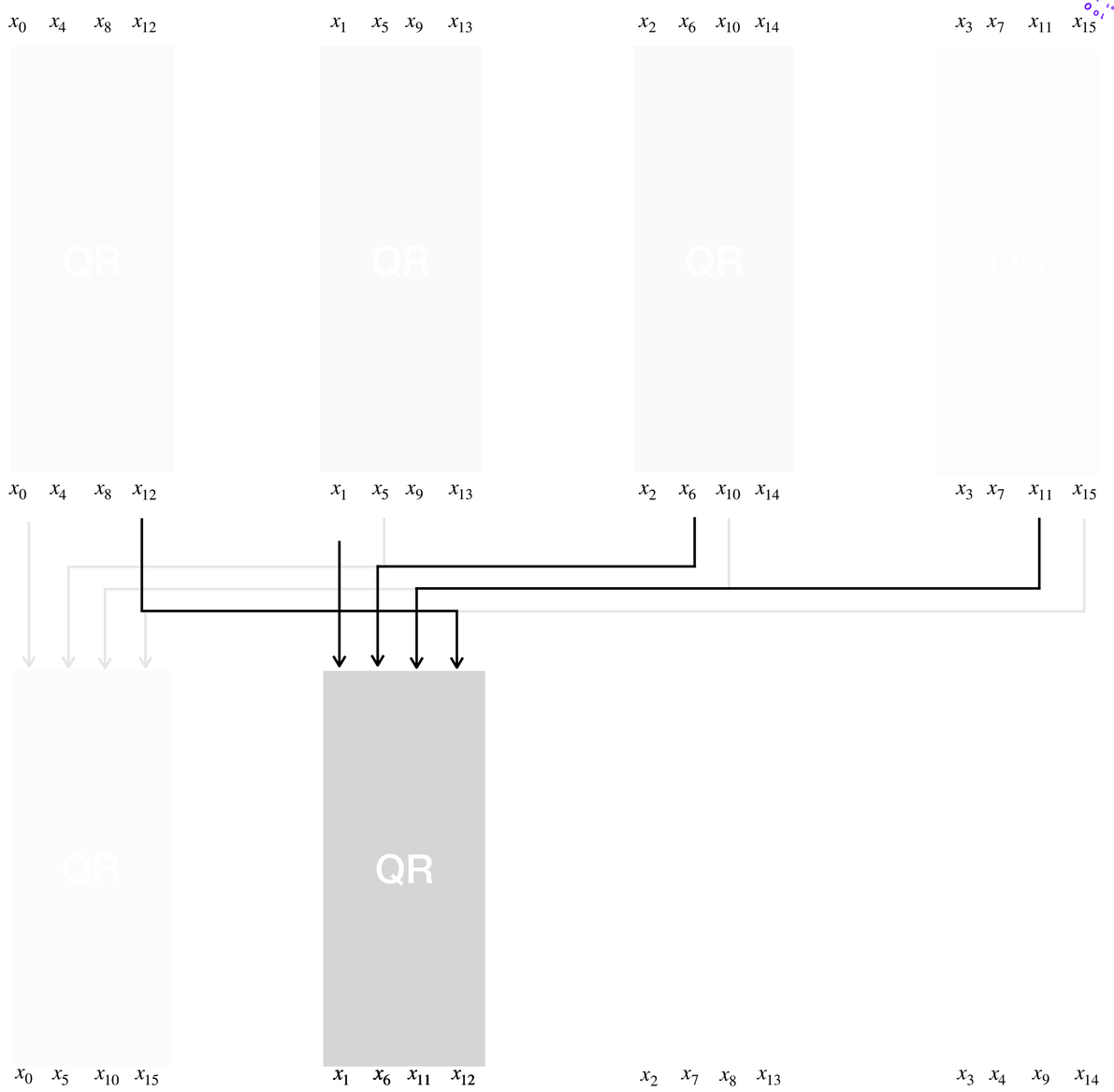
x_0	x_1	x_2	x_3
x_4	x_5	x_6	x_7
x_8	x_9	x_{10}	x_{11}
x_{12}	x_{13}	x_{14}	x_{15}



Background

ChaCha 2 rounds

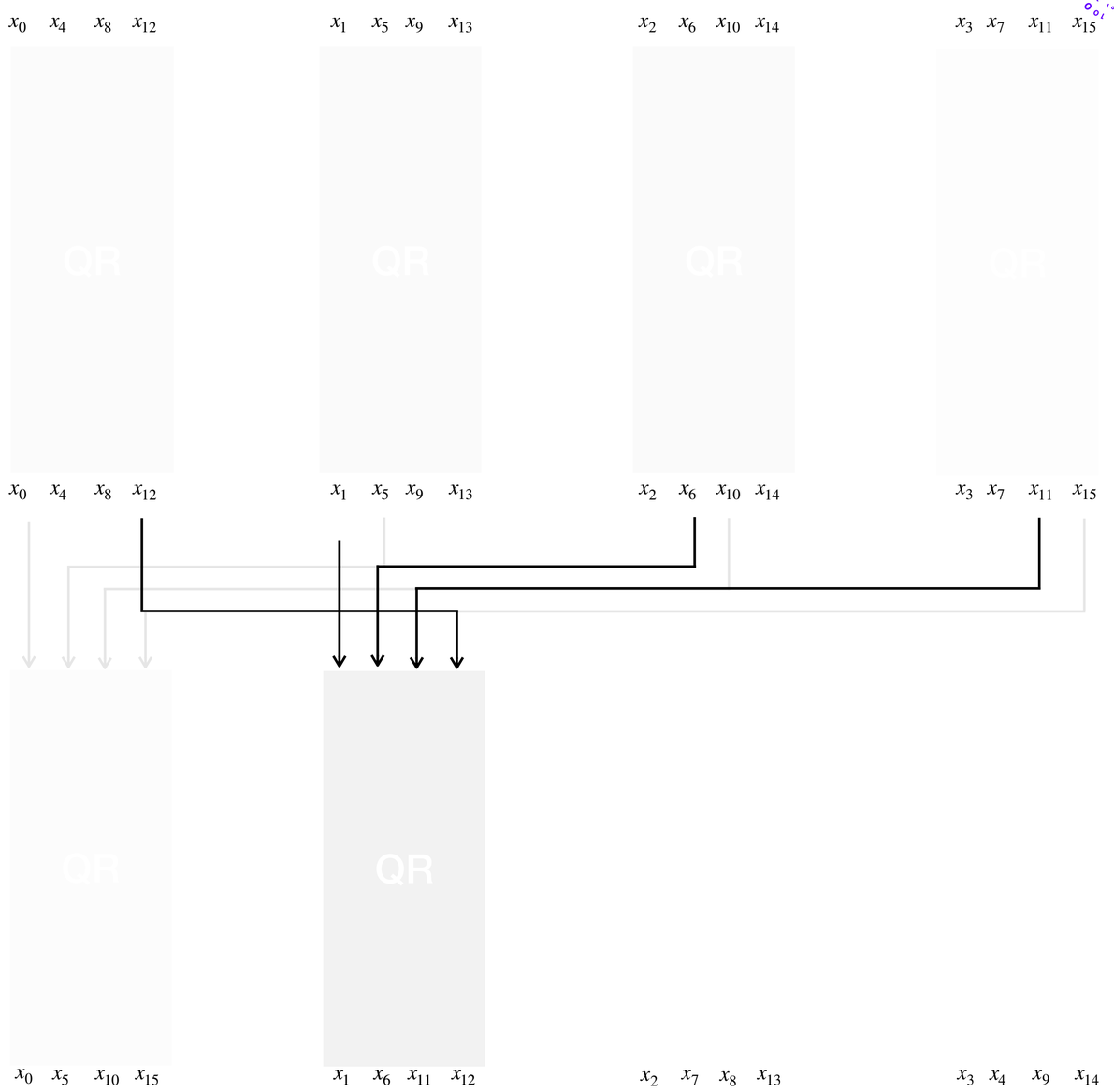
x_0	x_1	x_2	x_3
x_4	x_5	x_6	x_7
x_8	x_9	x_{10}	x_{11}
x_{12}	x_{13}	x_{14}	x_{15}



Background

ChaCha 2 rounds

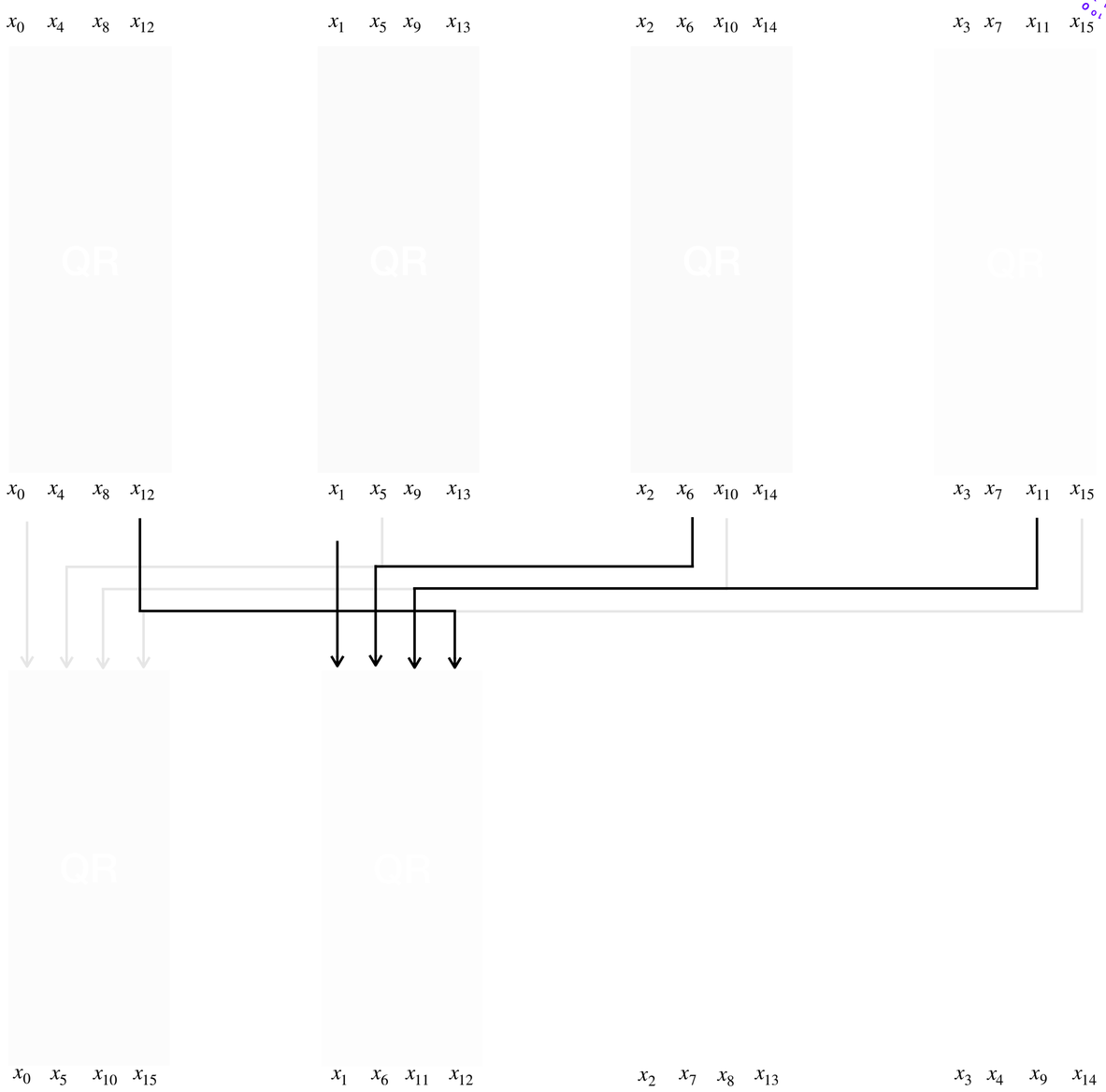
x_0	x_1	x_2	x_3
x_4	x_5	x_6	x_7
x_8	x_9	x_{10}	x_{11}
x_{12}	x_{13}	x_{14}	x_{15}



Background

ChaCha 2 rounds

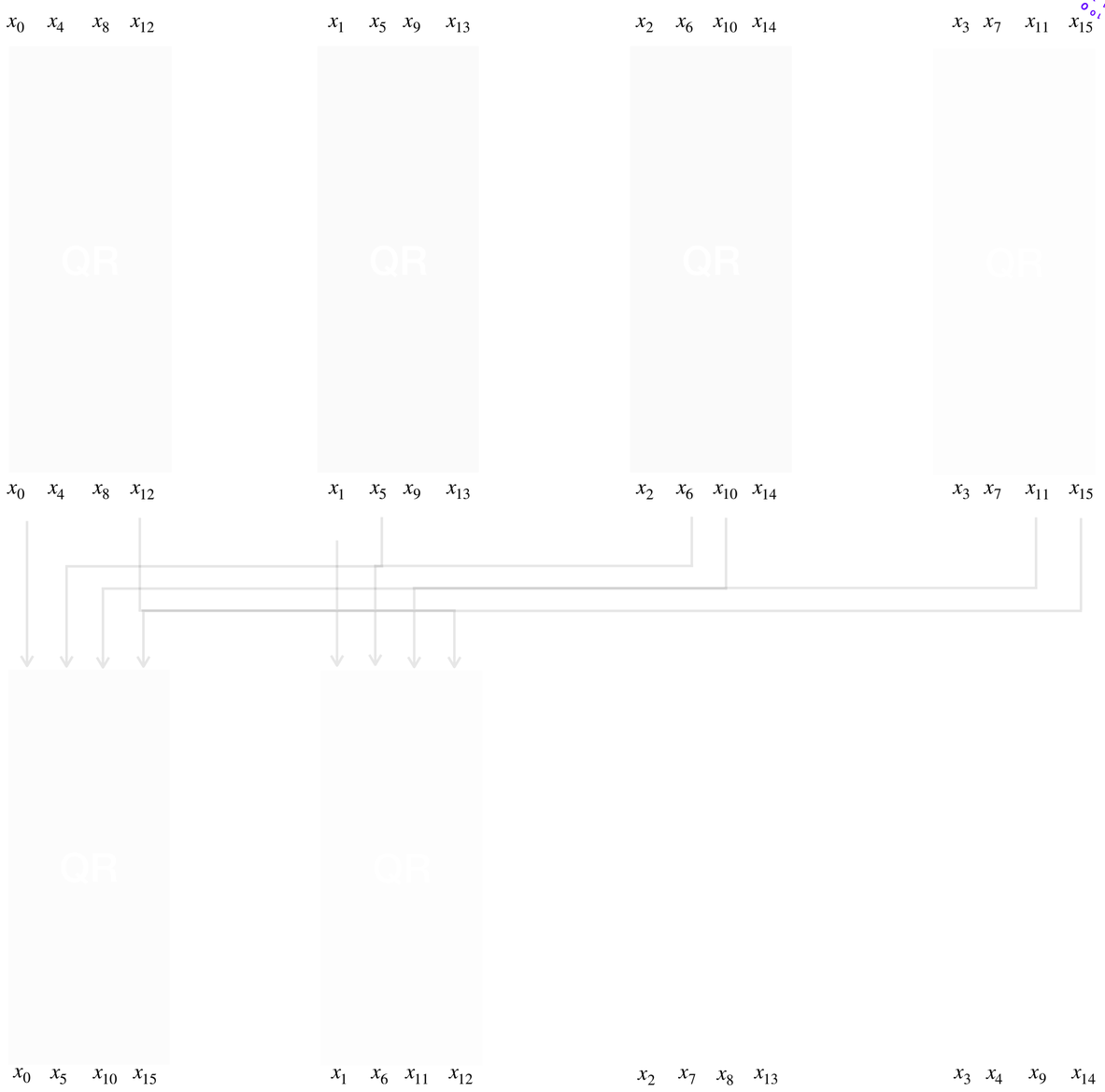
x_0	x_1	x_2	x_3
x_4	x_5	x_6	x_7
x_8	x_9	x_{10}	x_{11}
x_{12}	x_{13}	x_{14}	x_{15}



Background

ChaCha 2 rounds

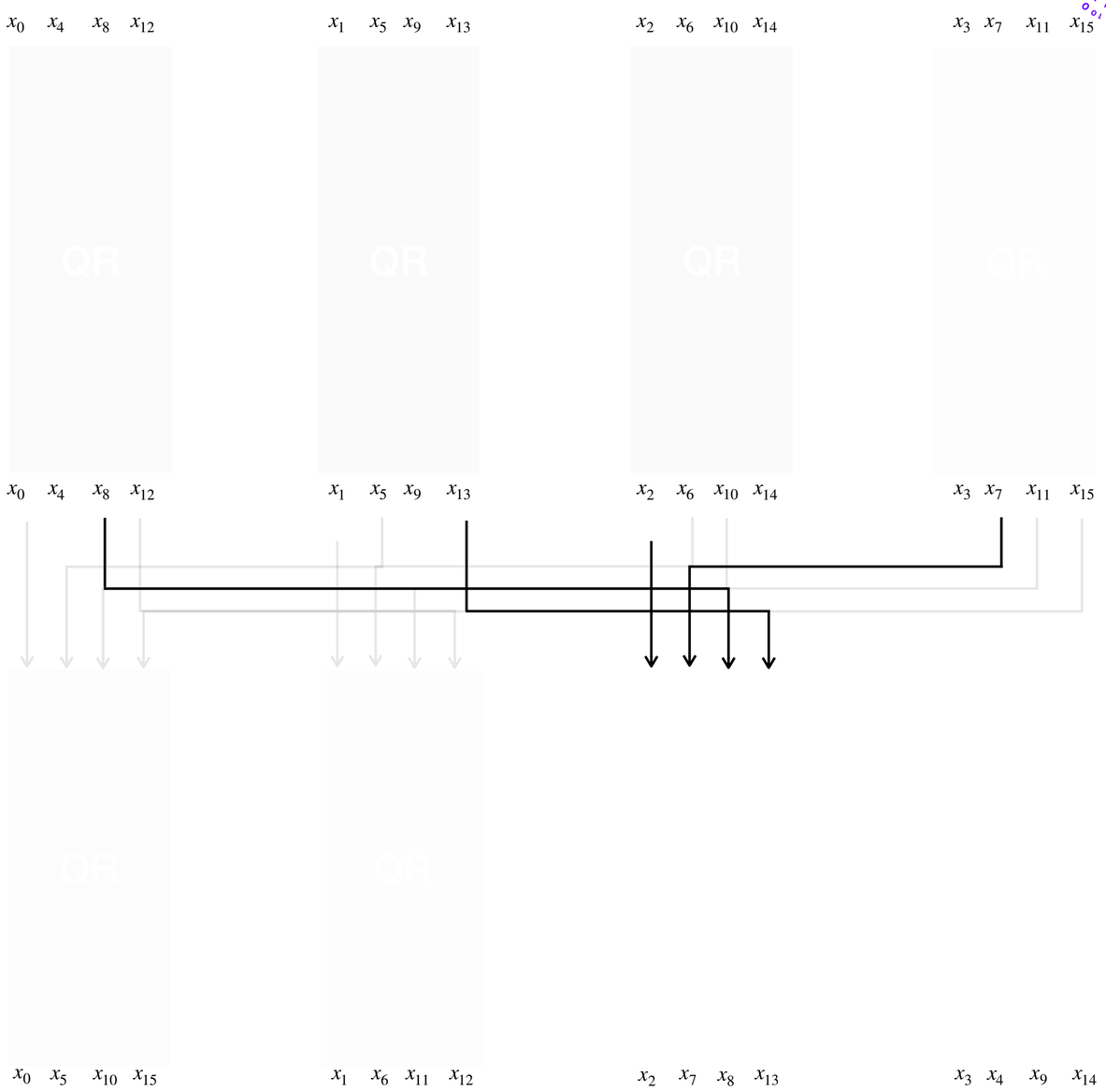
x_0	x_1	x_2	x_3
x_4	x_5	x_6	x_7
x_8	x_9	x_{10}	x_{11}
x_{12}	x_{13}	x_{14}	x_{15}



Background

ChaCha 2 rounds

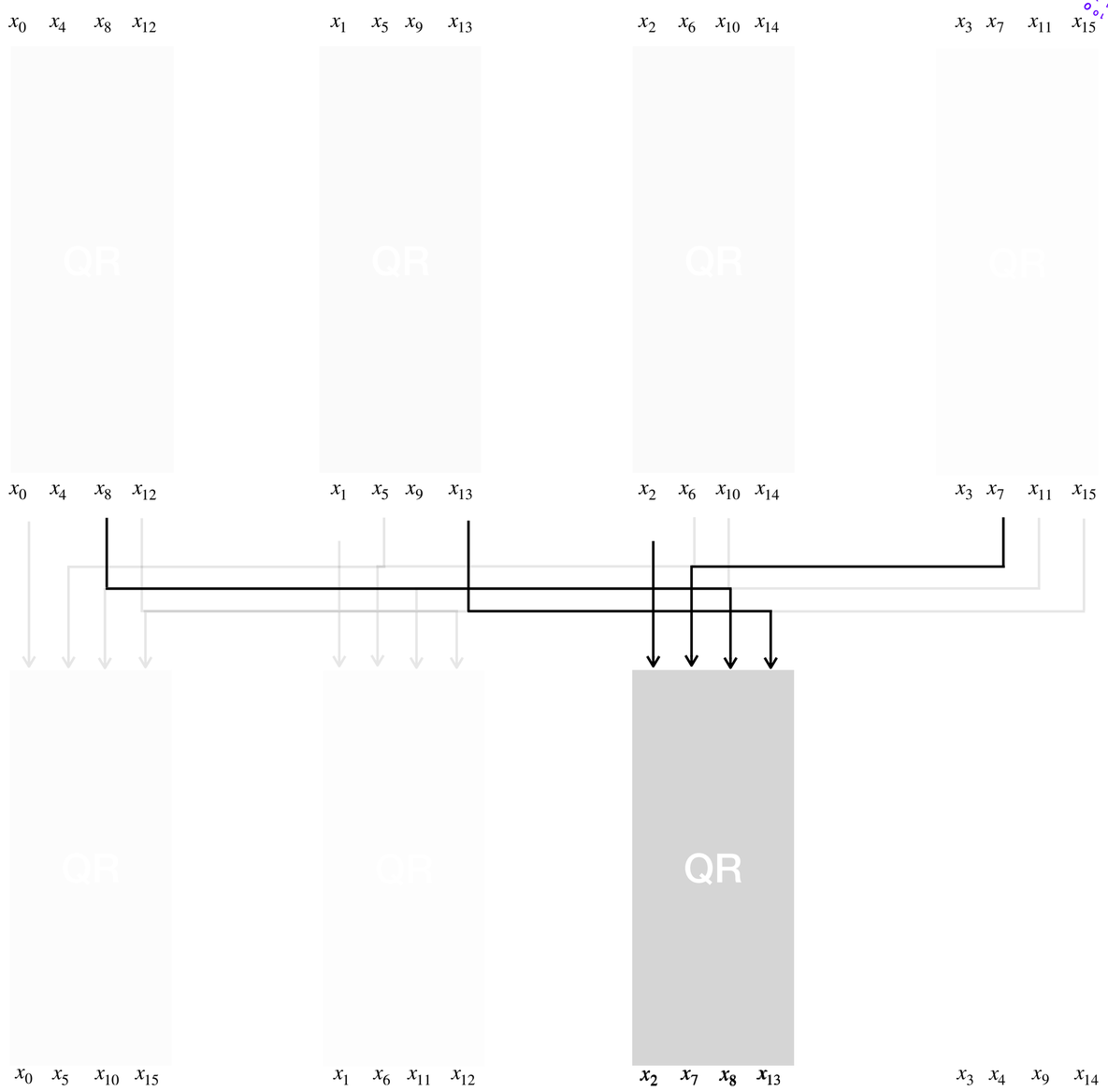
x_0	x_1	x_2	x_3
x_4	x_5	x_6	x_7
x_8	x_9	x_{10}	x_{11}
x_{12}	x_{13}	x_{14}	x_{15}



Background

ChaCha 2 rounds

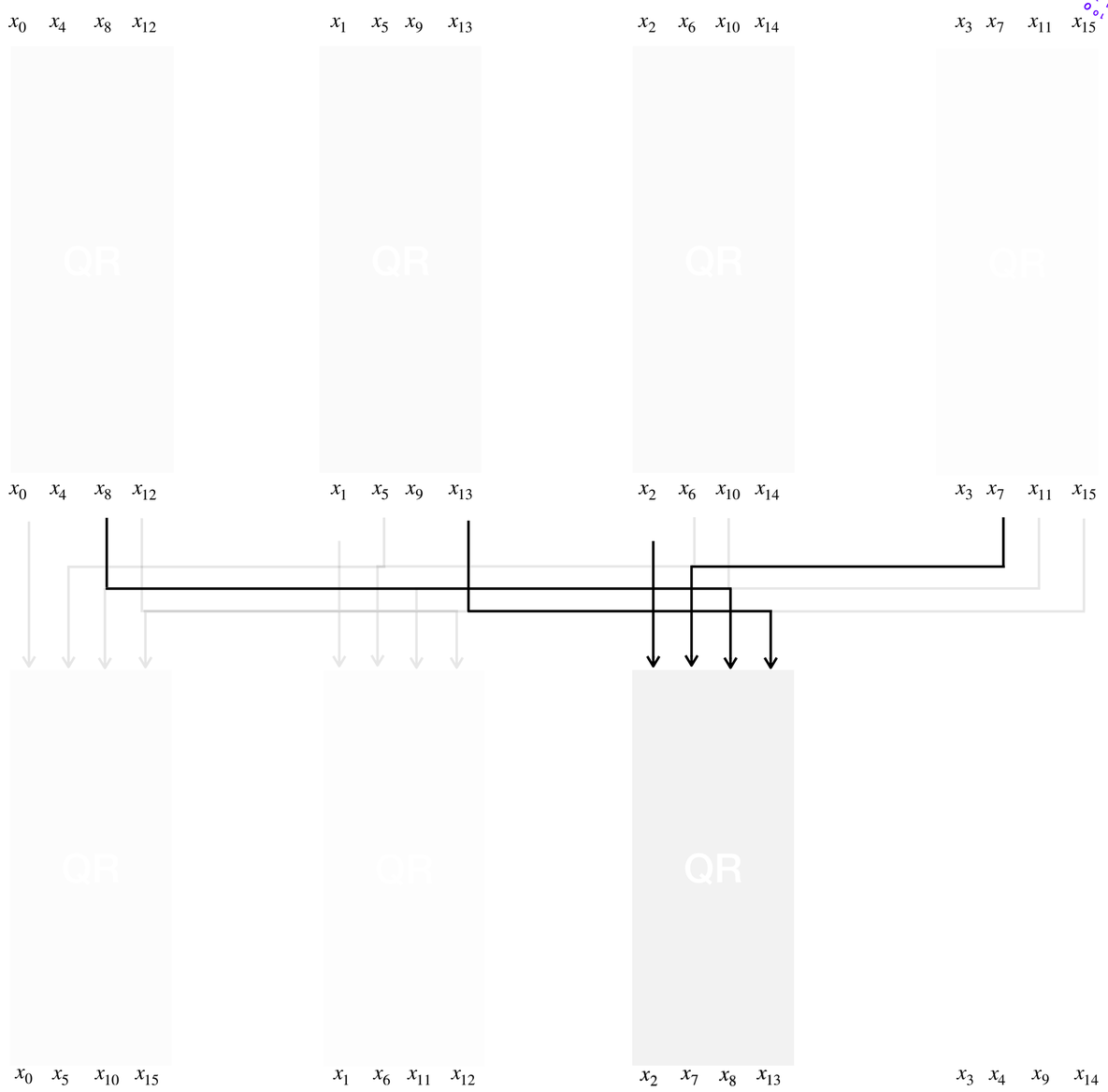
x_0	x_1	x_2	x_3
x_4	x_5	x_6	x_7
x_8	x_9	x_{10}	x_{11}
x_{12}	x_{13}	x_{14}	x_{15}



Background

ChaCha 2 rounds

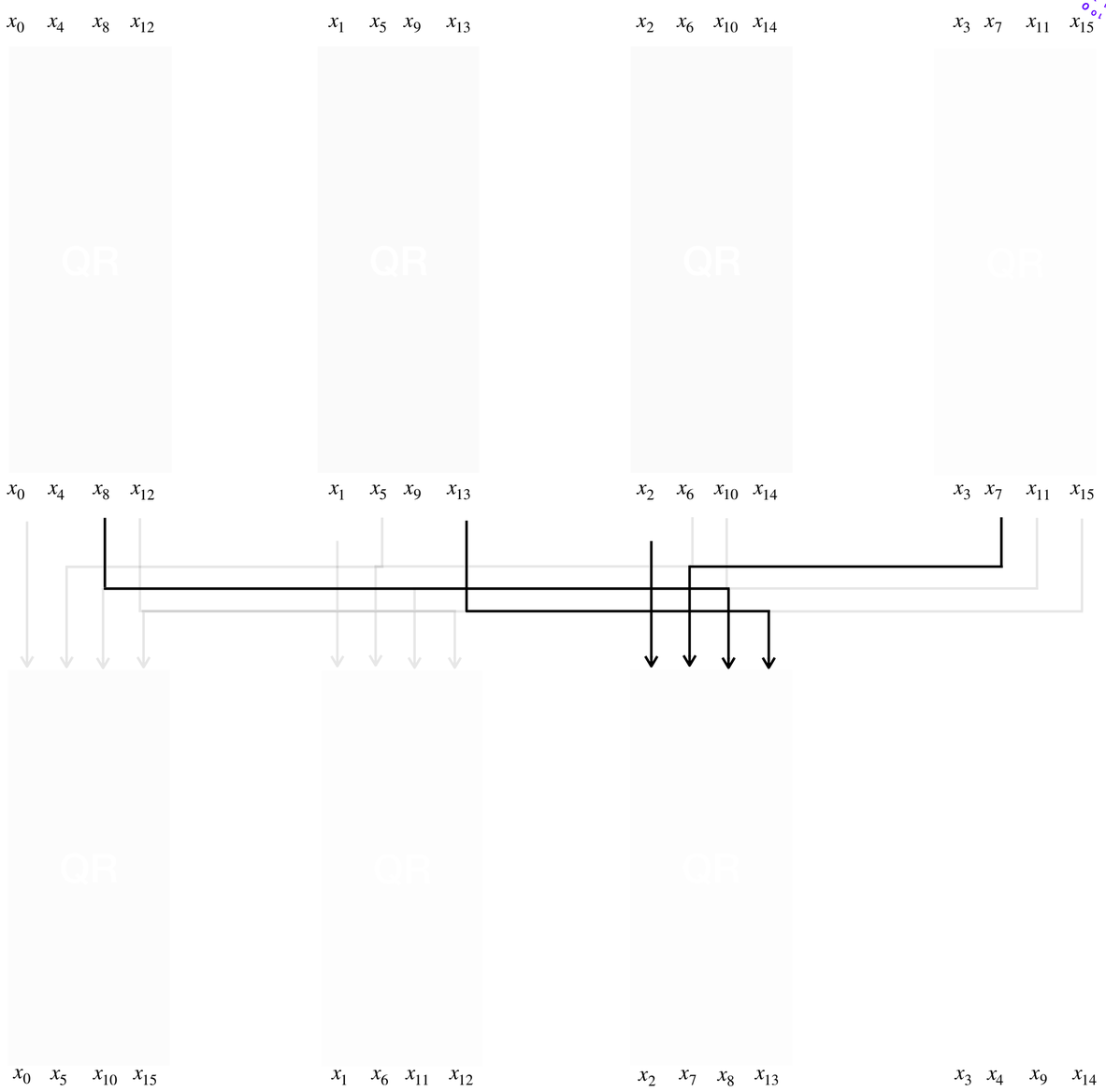
x_0	x_1	x_2	x_3
x_4	x_5	x_6	x_7
x_8	x_9	x_{10}	x_{11}
x_{12}	x_{13}	x_{14}	x_{15}



Background

ChaCha 2 rounds

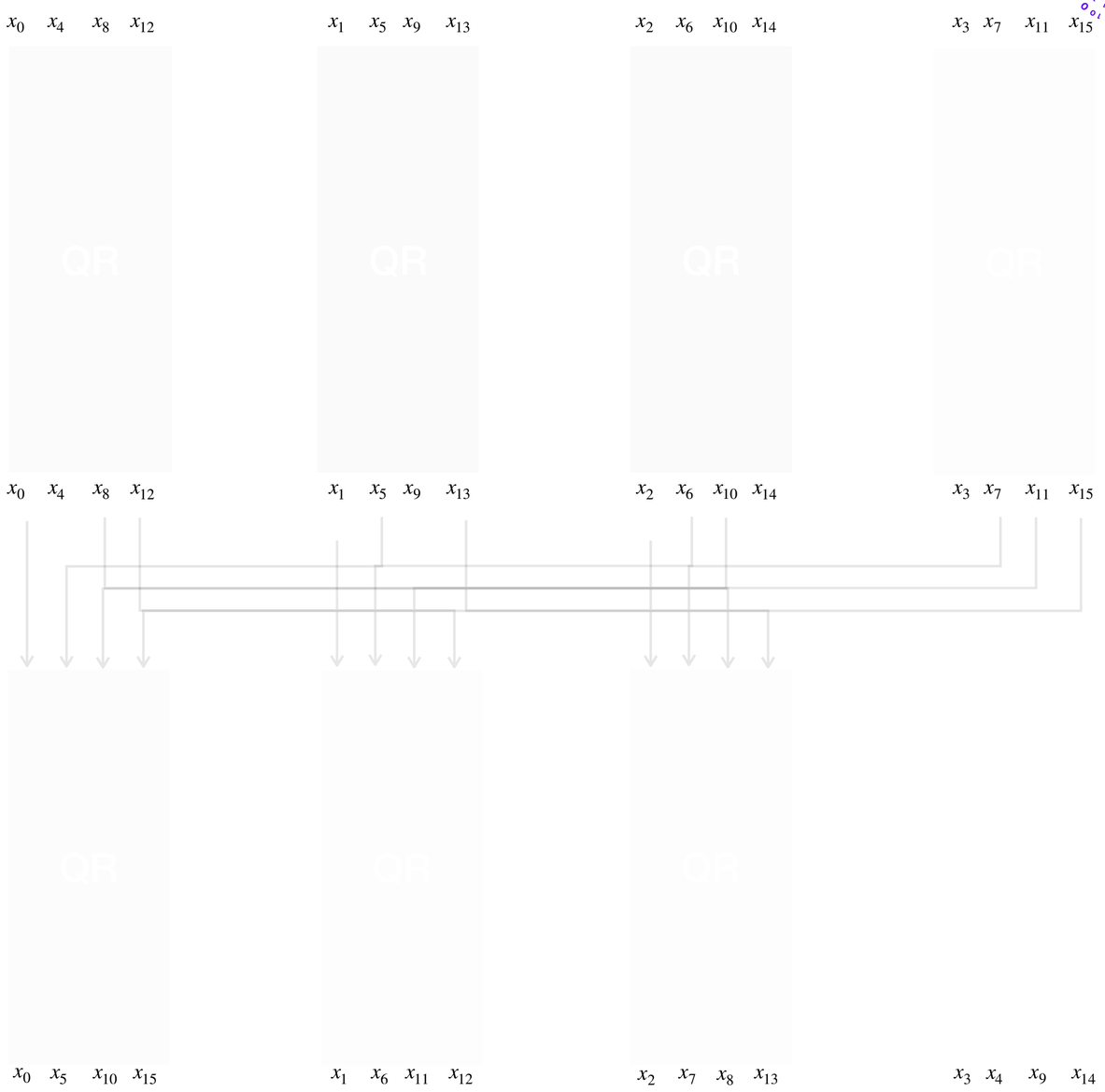
x_0	x_1	x_2	x_3
x_4	x_5	x_6	x_7
x_8	x_9	x_{10}	x_{11}
x_{12}	x_{13}	x_{14}	x_{15}



Background

ChaCha 2 rounds

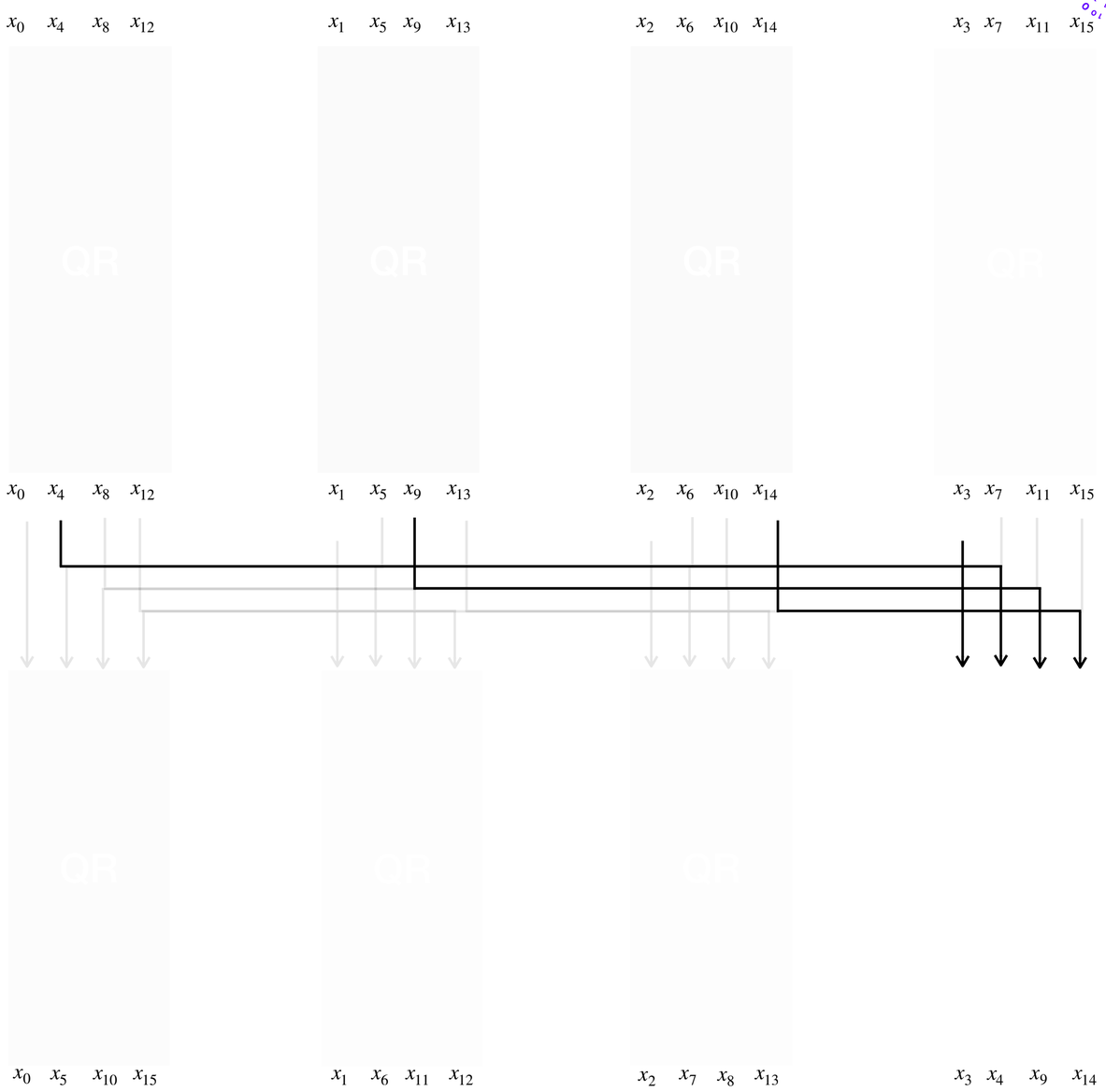
x_0	x_1	x_2	x_3
x_4	x_5	x_6	x_7
x_8	x_9	x_{10}	x_{11}
x_{12}	x_{13}	x_{14}	x_{15}



Background

ChaCha 2 rounds

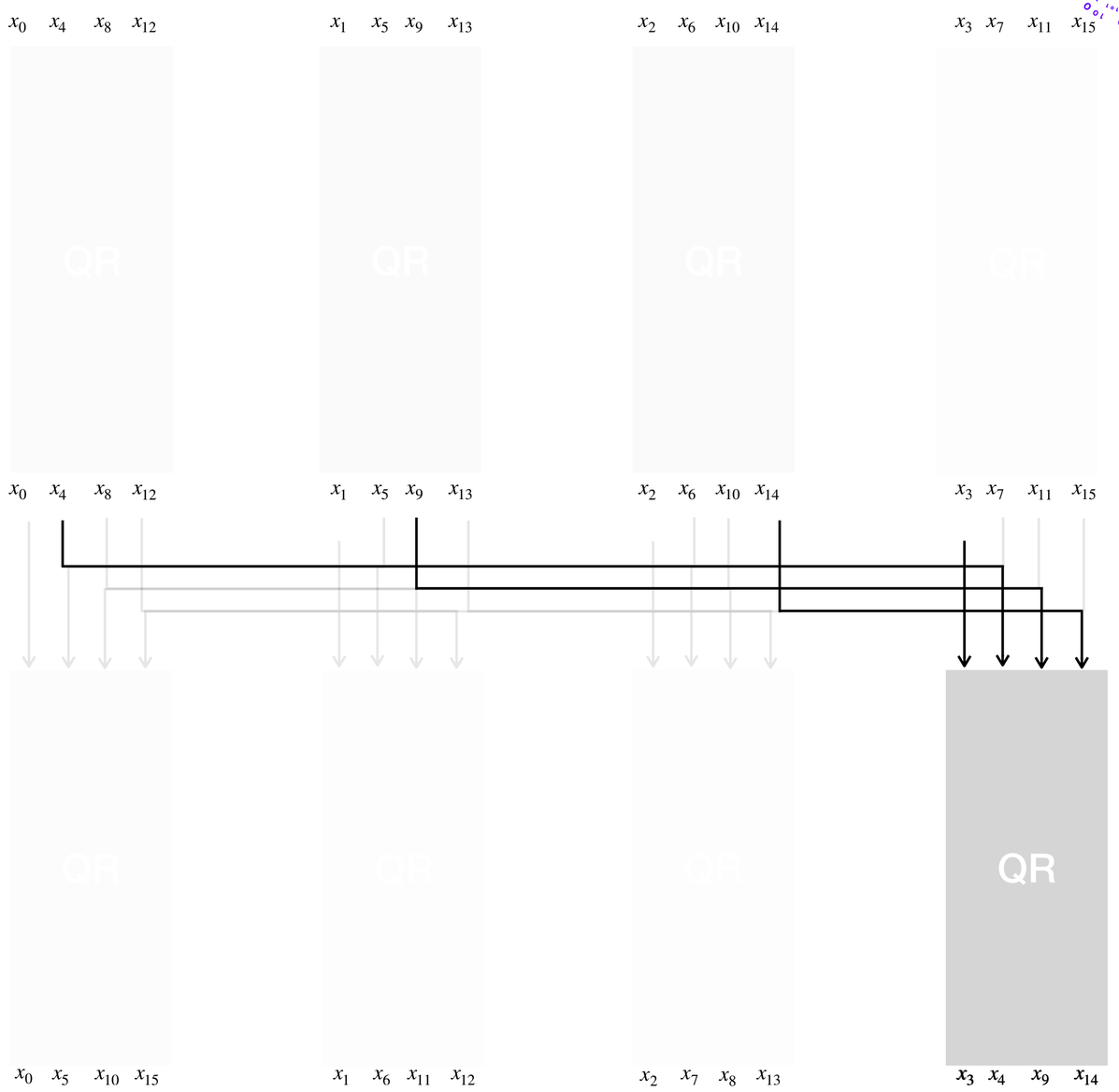
x_0	x_1	x_2	x_3
x_4	x_5	x_6	x_7
x_8	x_9	x_{10}	x_{11}
x_{12}	x_{13}	x_{14}	x_{15}



Background

ChaCha 2 rounds

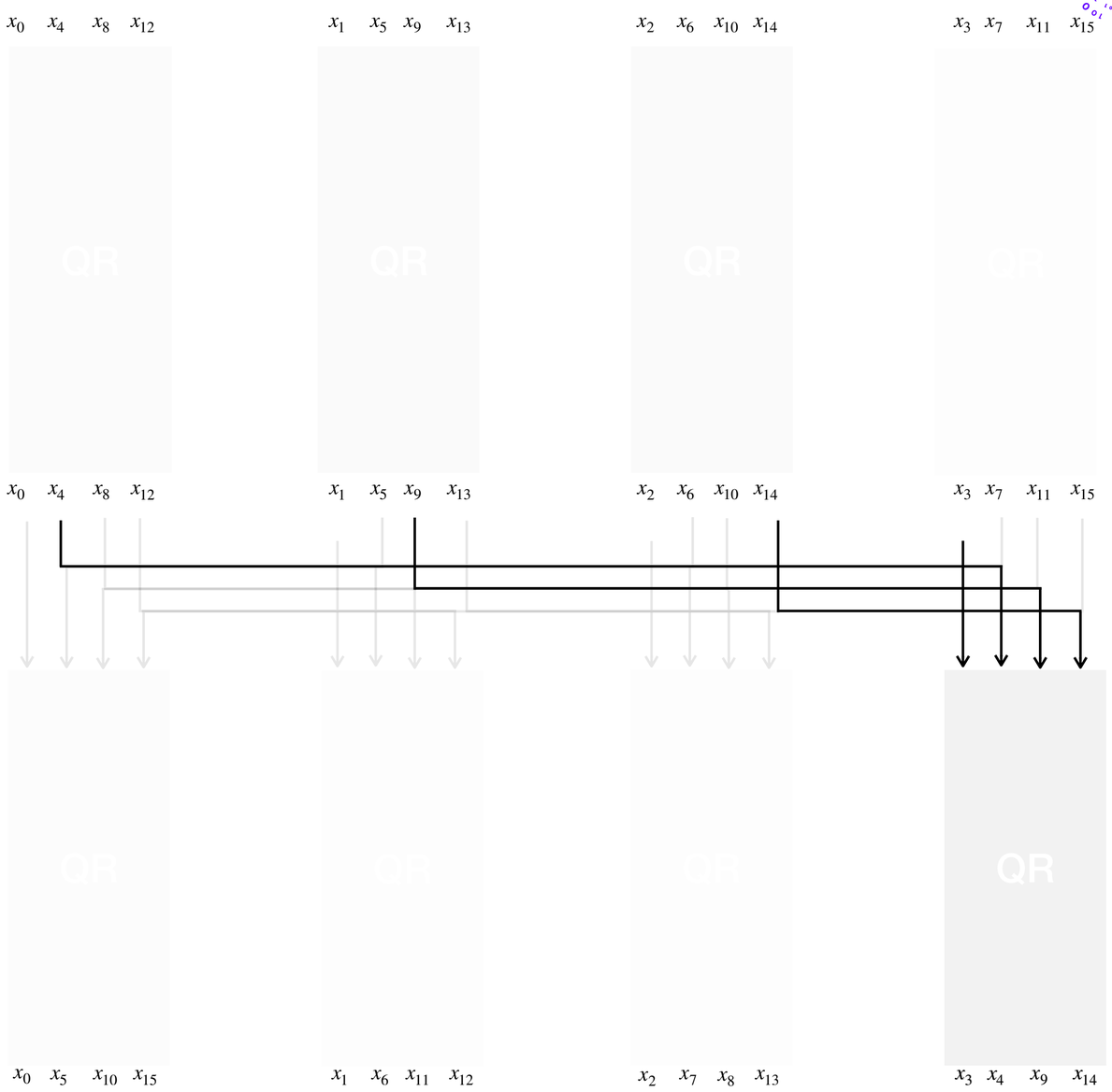
x_0	x_1	x_2	x_3
x_4	x_5	x_6	x_7
x_8	x_9	x_{10}	x_{11}
x_{12}	x_{13}	x_{14}	x_{15}



Background

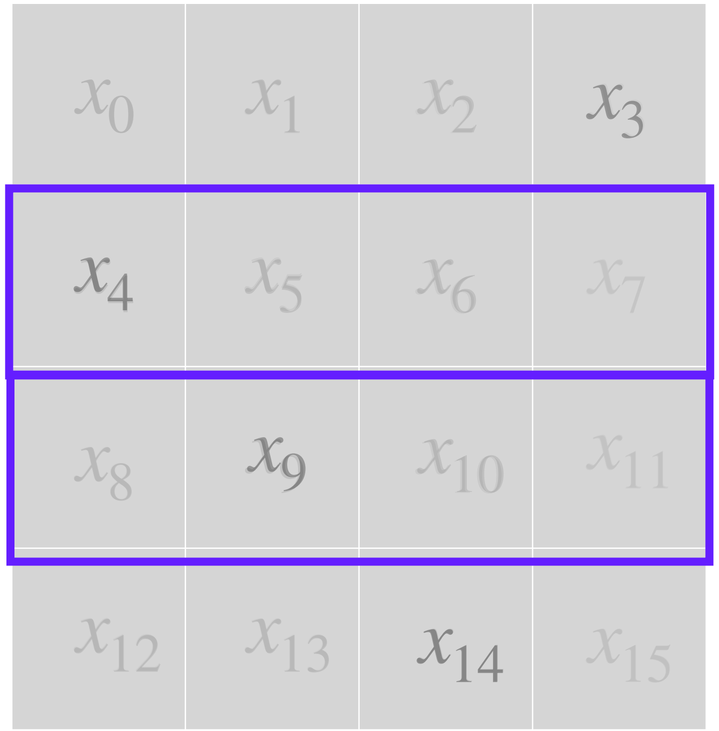
ChaCha 2 rounds

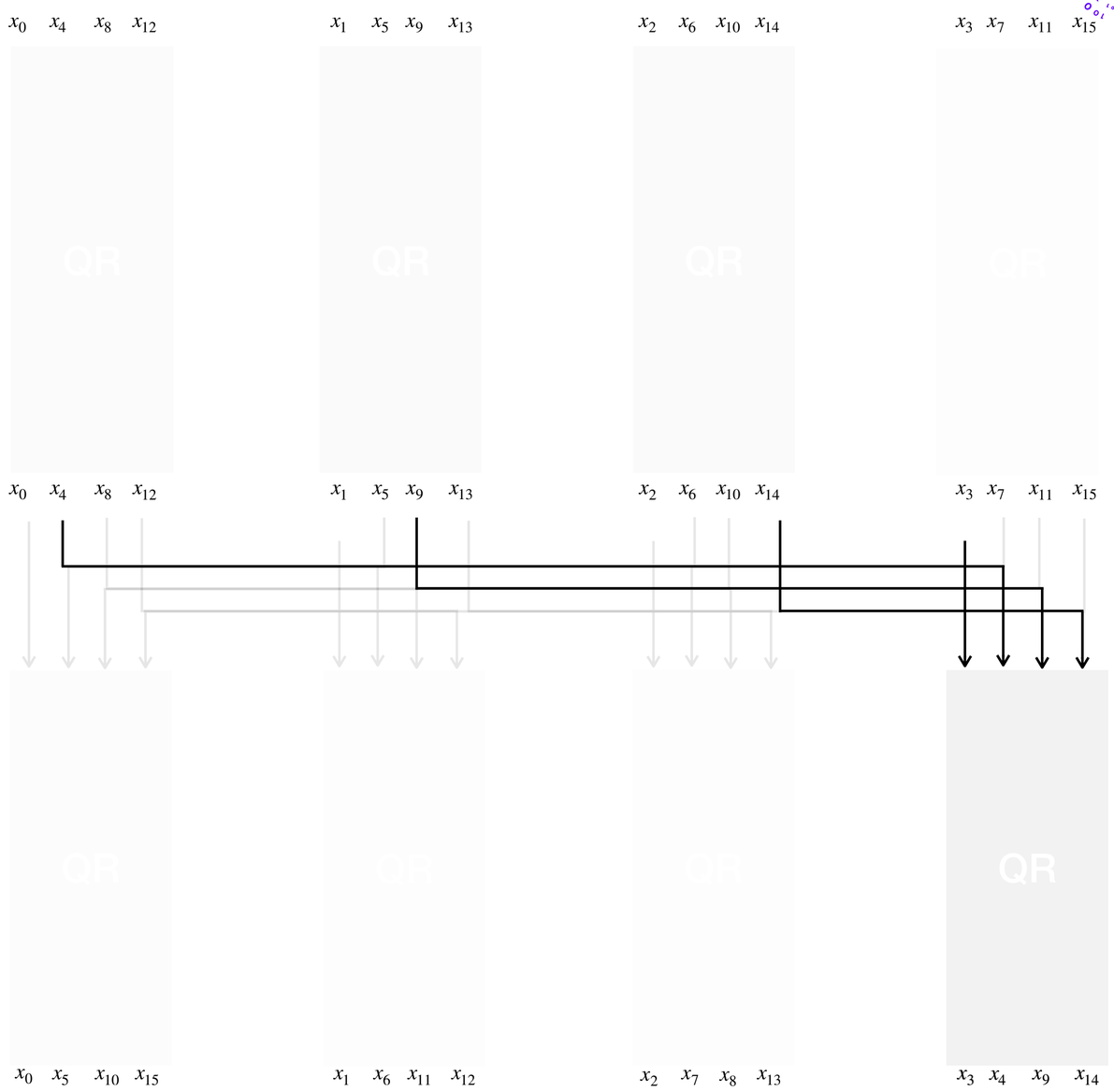
x_0	x_1	x_2	x_3
x_4	x_5	x_6	x_7
x_8	x_9	x_{10}	x_{11}
x_{12}	x_{13}	x_{14}	x_{15}



Background

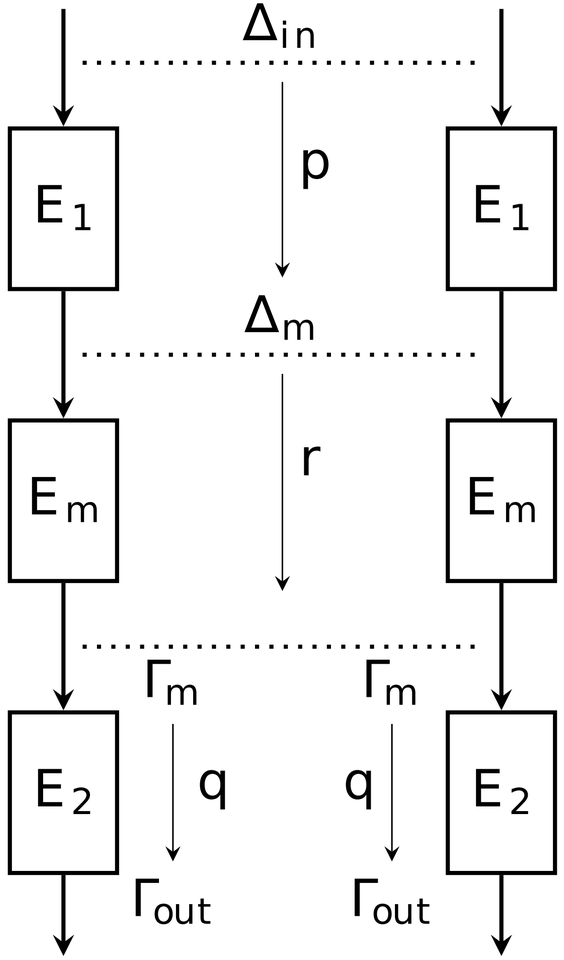
ChaCha 2 rounds





Background

Differential-Linear Attack

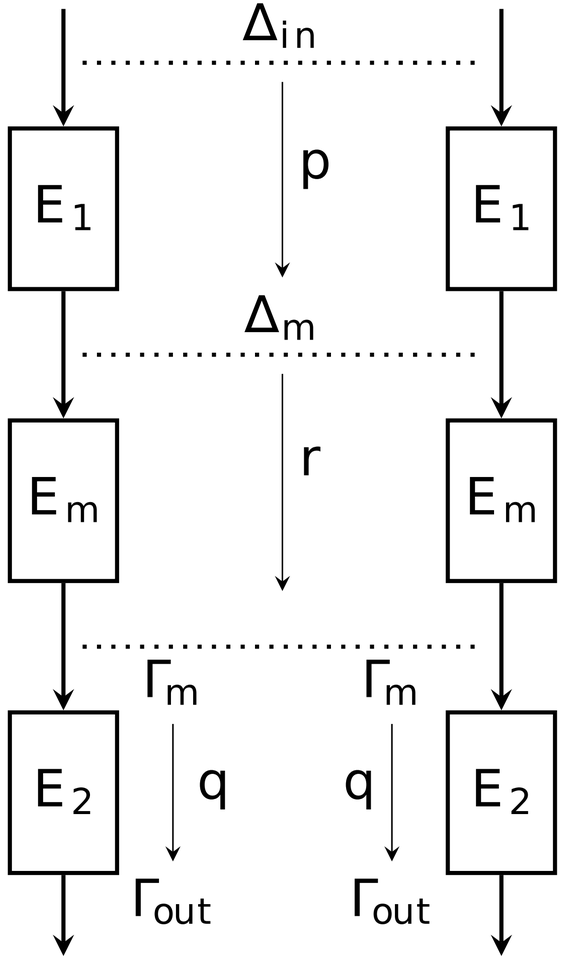


Correlation

$$prq^2$$

Background

Differential-Linear Attack



Correlation

$$prq^2$$

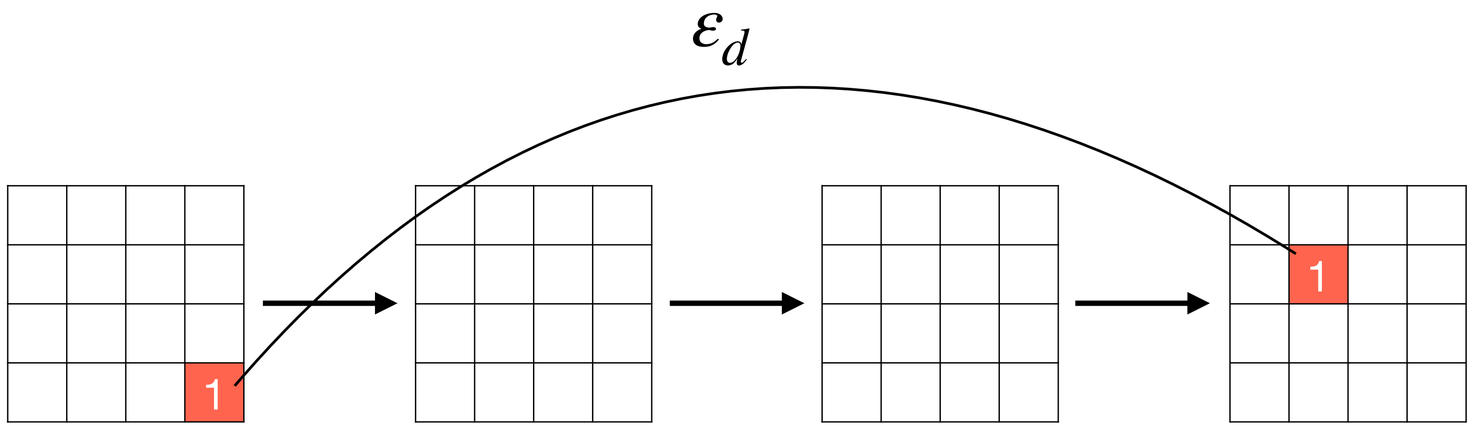
Complexity

$$O(p^{-2}r^{-2}q^{-4})$$

Background: Probabilistic Neutral Bits Attack (PNB)

Cryptography Research Centre

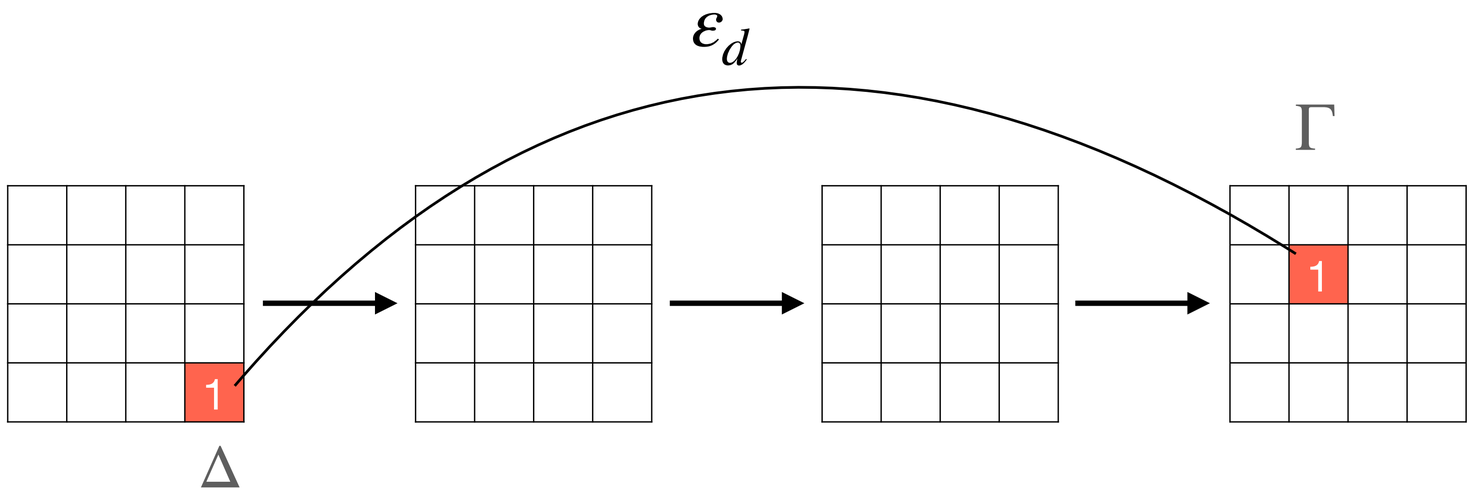
Step 1: Finding a distinguisher



Background: Probabilistic Neutral Bits Attack (PNB)

Cryptography Research Centre

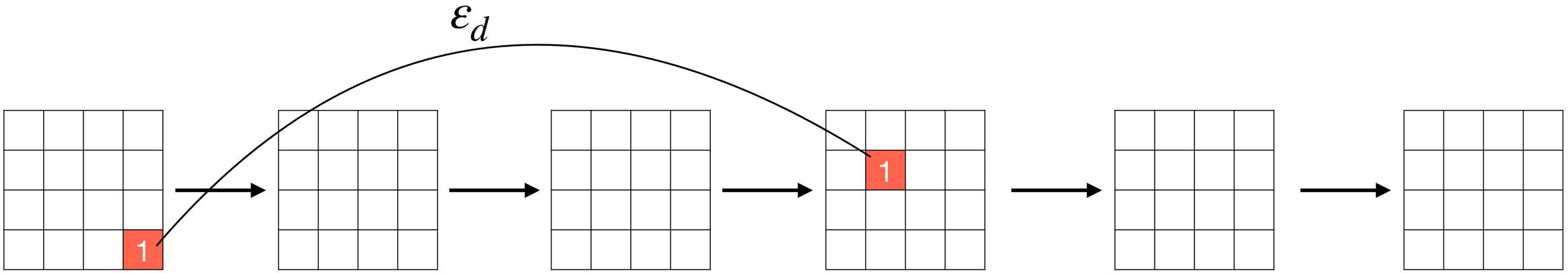
Step 1: Finding a distinguisher



Background: Probabilistic Neutral Bits Attack (PNB)

Cryptography Research Centre

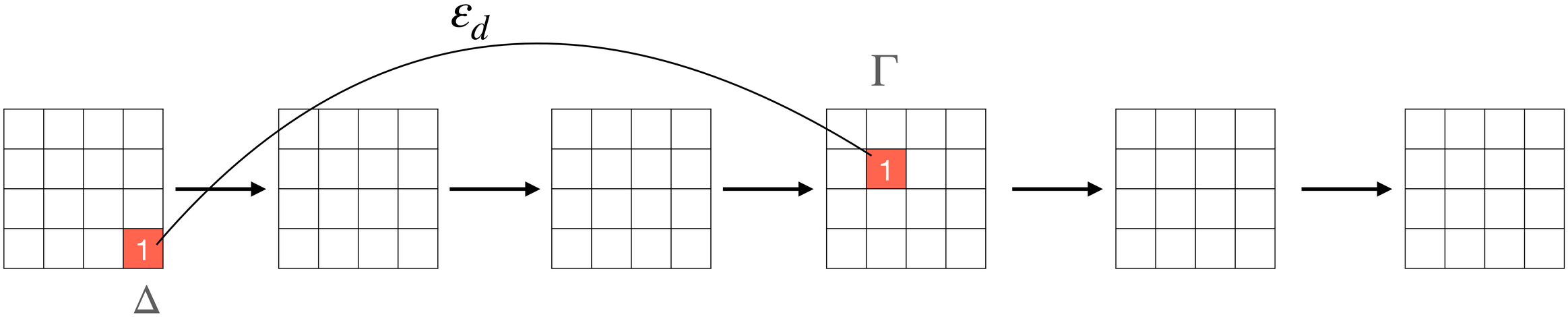
Step 1: Finding a distinguisher



Background: Probabilistic Neutral Bits Attack (PNB)

Cryptography Research Centre

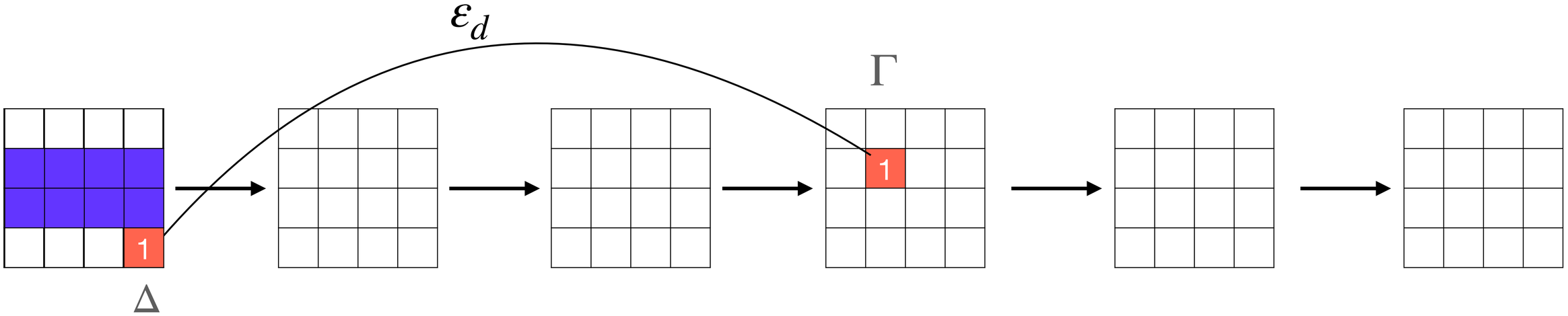
Step 1: Finding a distinguisher



Background: Probabilistic Neutral Bits Attack (PNB)

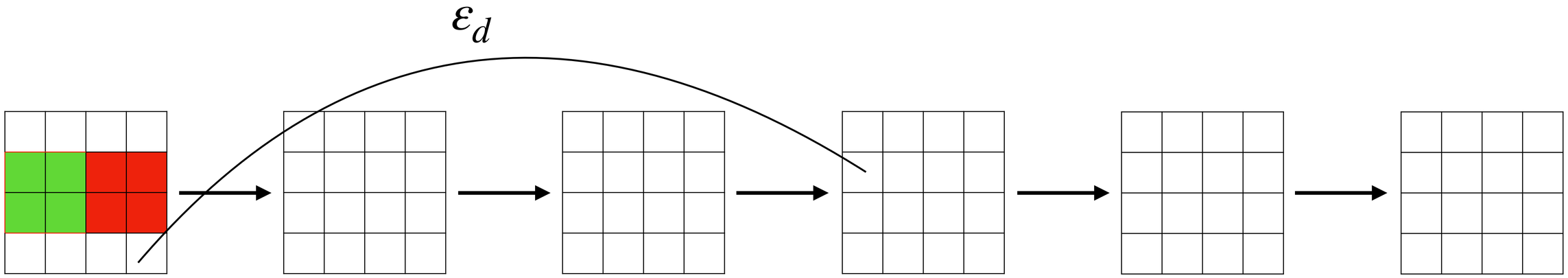
Cryptography Research Centre

Step 1: Finding a distinguisher



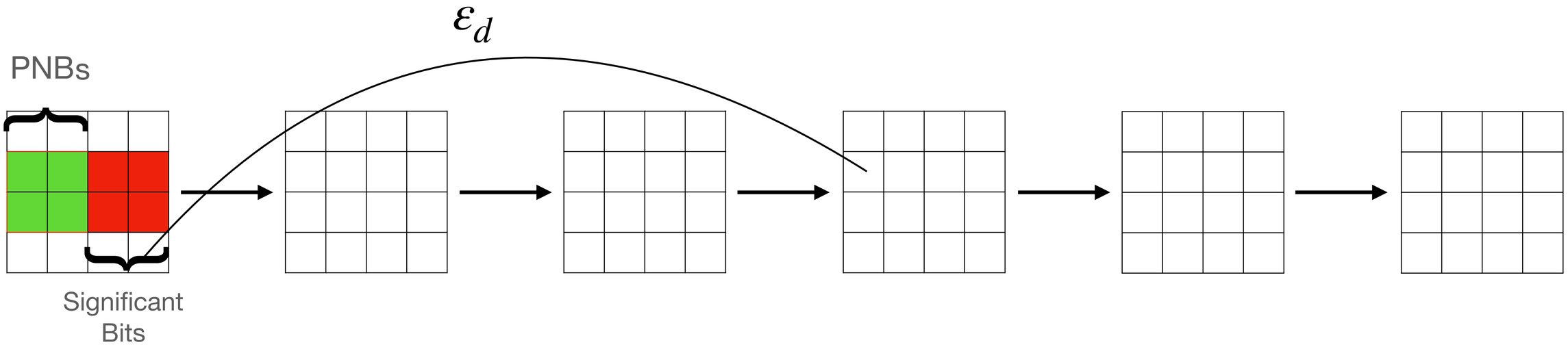
Background

Step 2 : Using the remaining bits to perform the attack



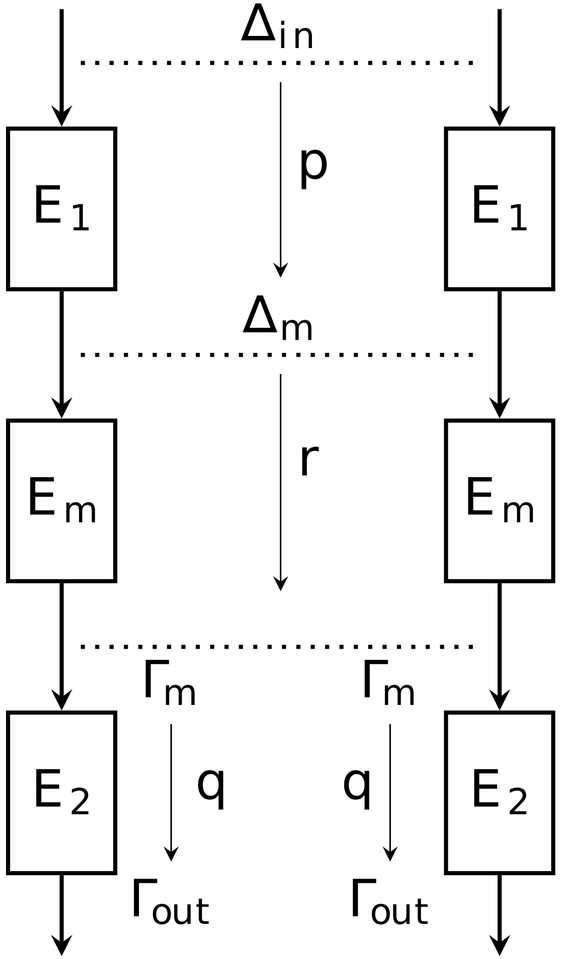
Background

Step 2 : Using the remaining bits to perform the attack



Contributions

How to improve the correlation of the distinguisher?



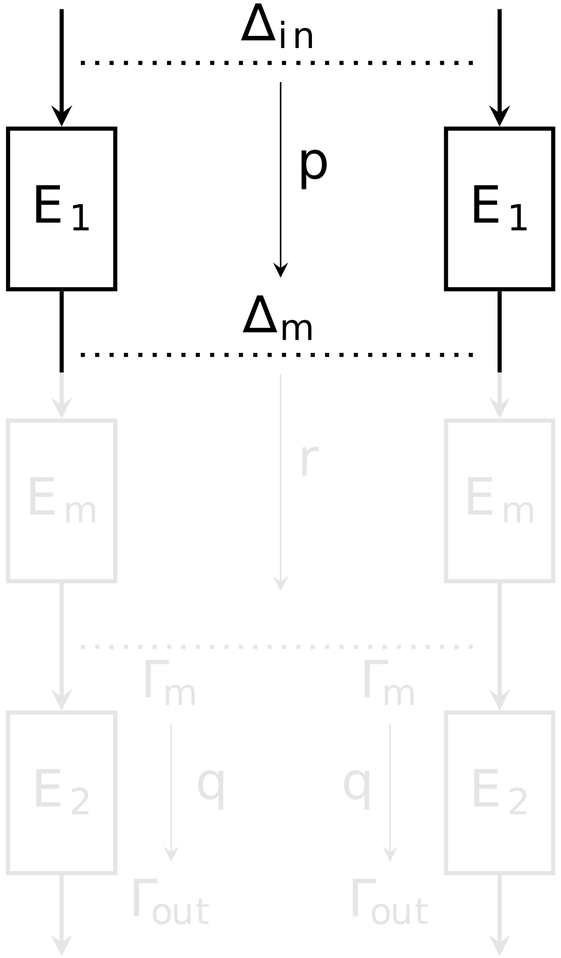
Different from previous works, we explore input differences with 2 active bits

We use the power of GPUs to find “very-low” correlation differential-linear distinguishers

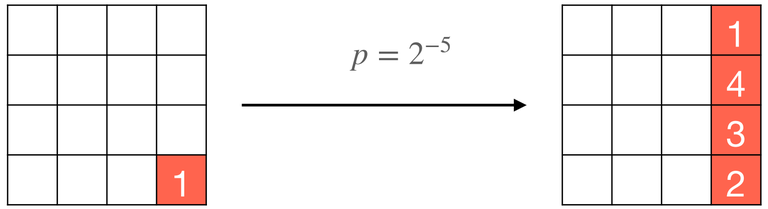
Different from previous works, we use MILP techniques to automate the search for linear approximations

Exploring 2-active-bit input differences

Top part

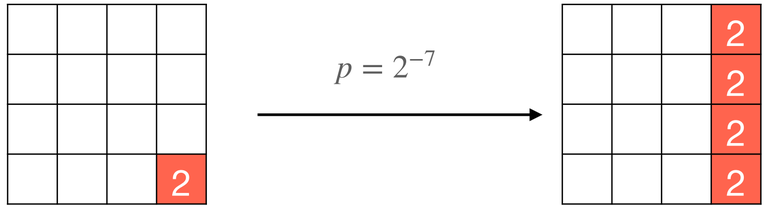


Previous works starting with hamming weight (hw)1: (Crypto 2020, Eurocrypt 2022)



10 active differences

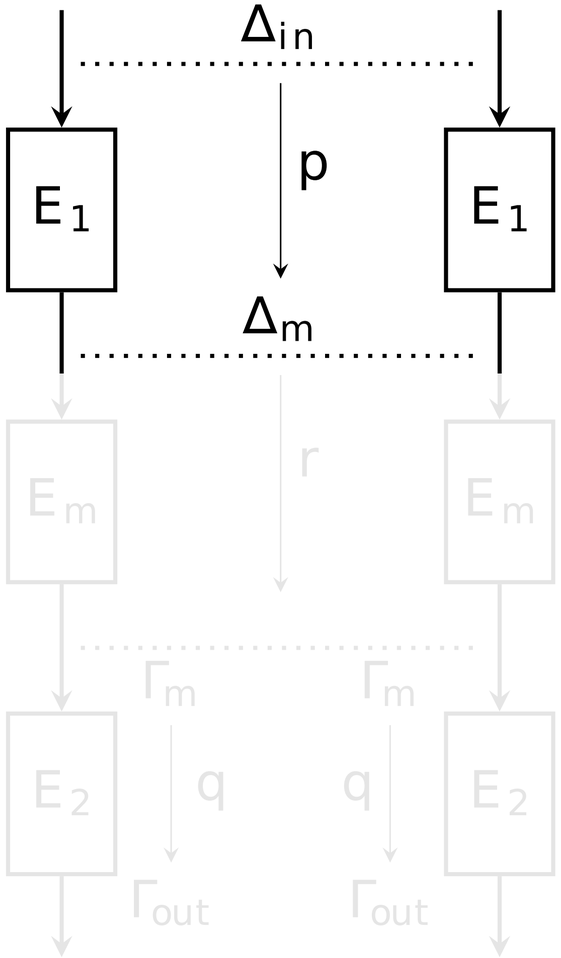
This paper starts with hamming weight (hw) 2:



8 active differences

Exploring 2-active-bit input differences

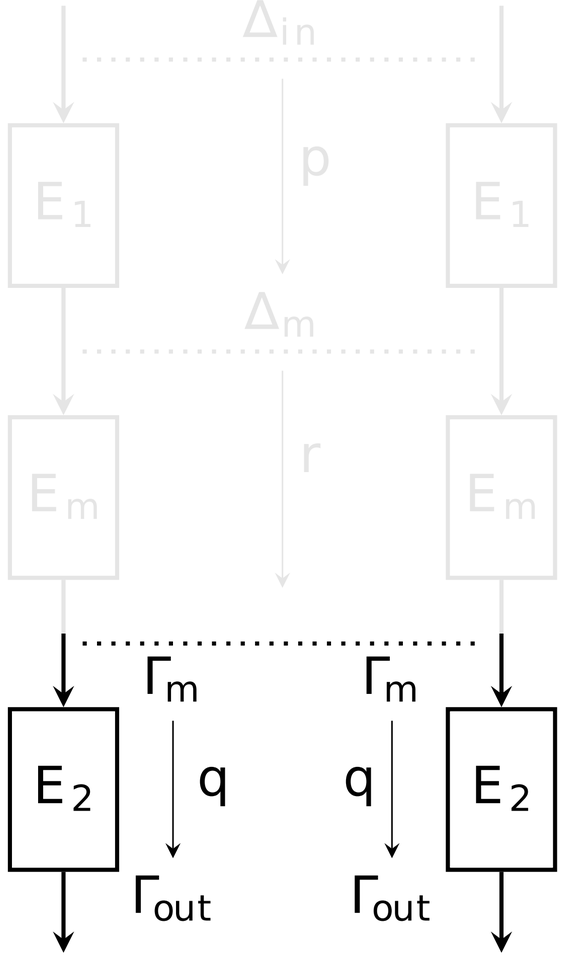
Top part

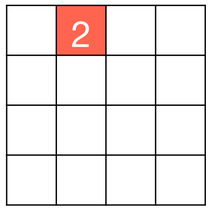


- We use MILP techniques from [FWG+16]
- We explore 1-round trail with 3 active differences in the input, without success
- We explore 2-round trails, without success.

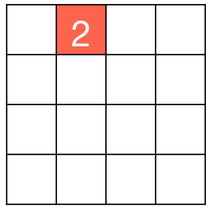
Analyzing Quarter Round Formulas

Linear Part

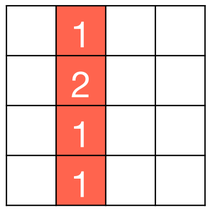




Round 4

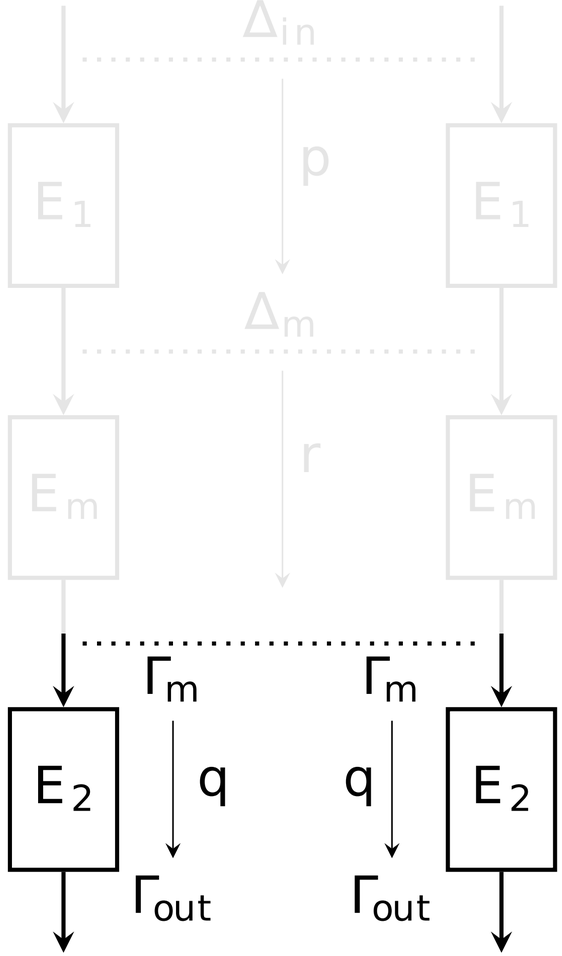


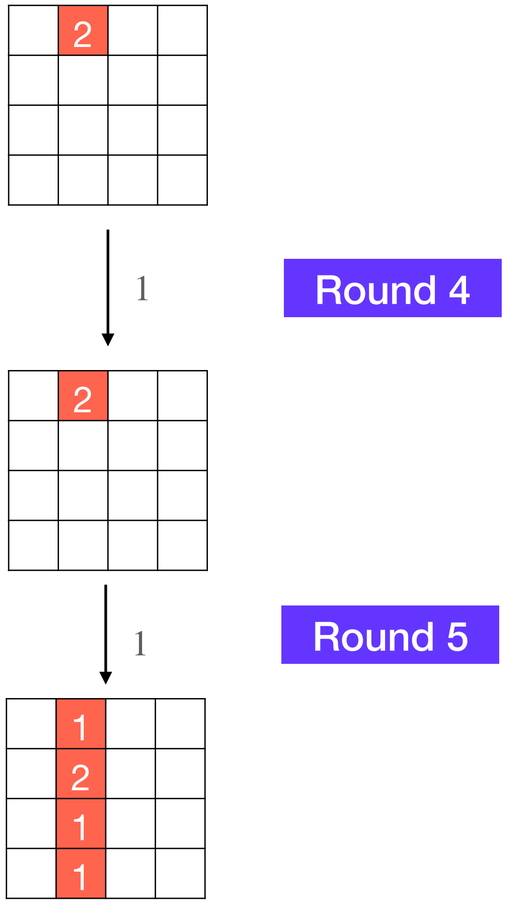
Round 5



Analyzing Quarter Round Formulas

Linear Part





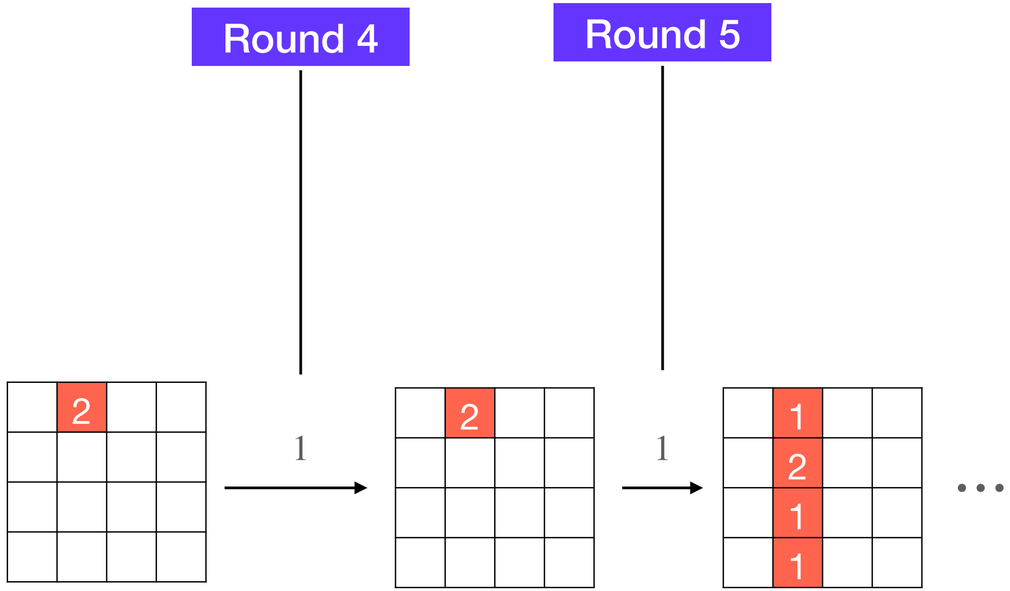
Round 4

Round 5

Computing the Correlation for the Middle Part

Cryptography Research Centre

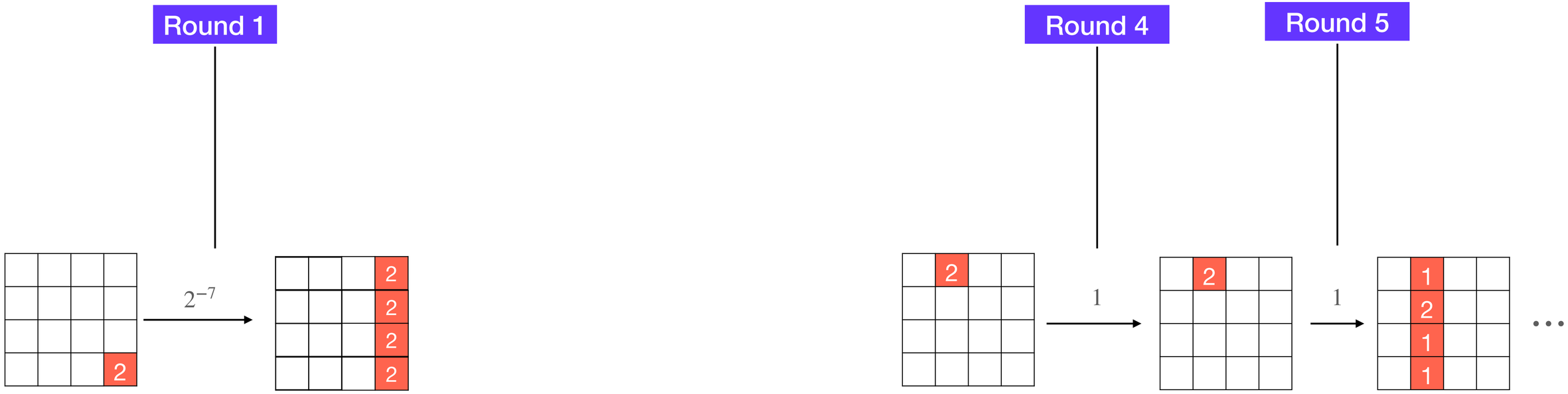
Middle Part



Computing the Correlation for the Middle Part

Cryptography Research Centre

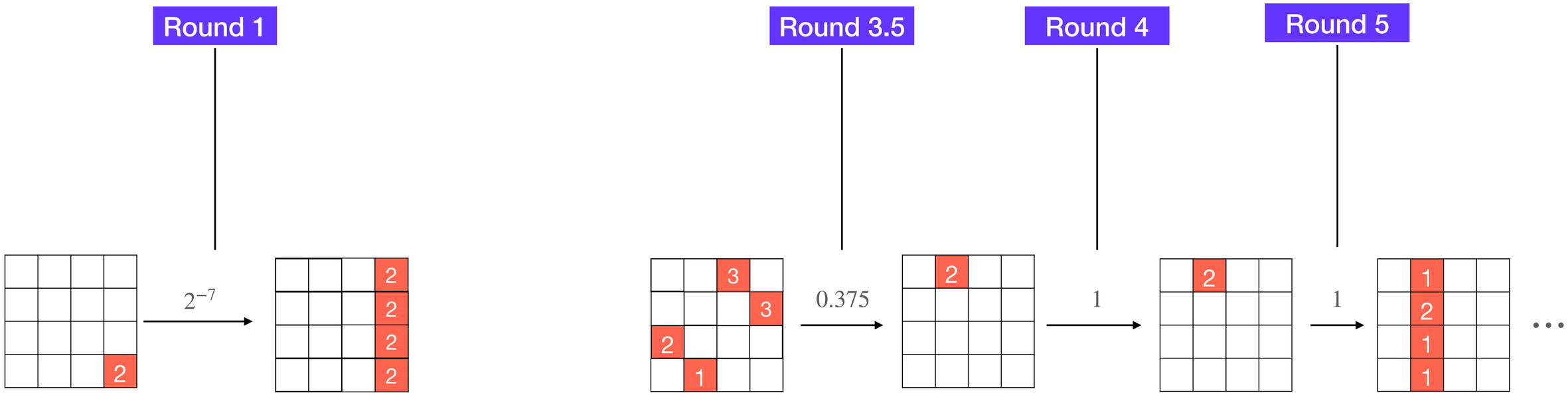
Middle Part



Computing the Correlation for the Middle Part

Cryptography Research Centre

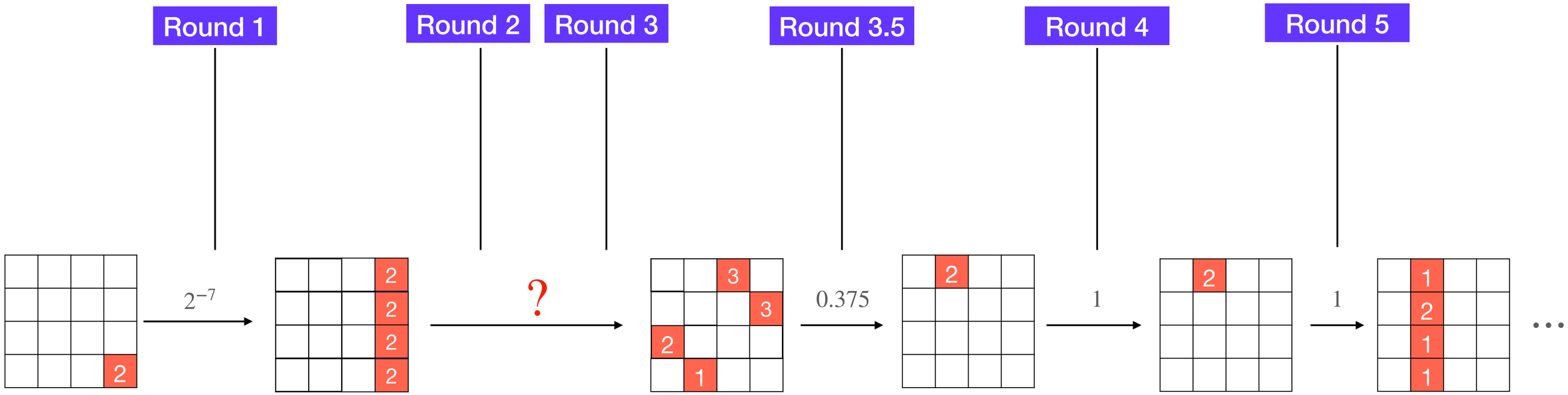
Middle Part



Computing the Correlation for the Middle Part

Cryptography Research Centre

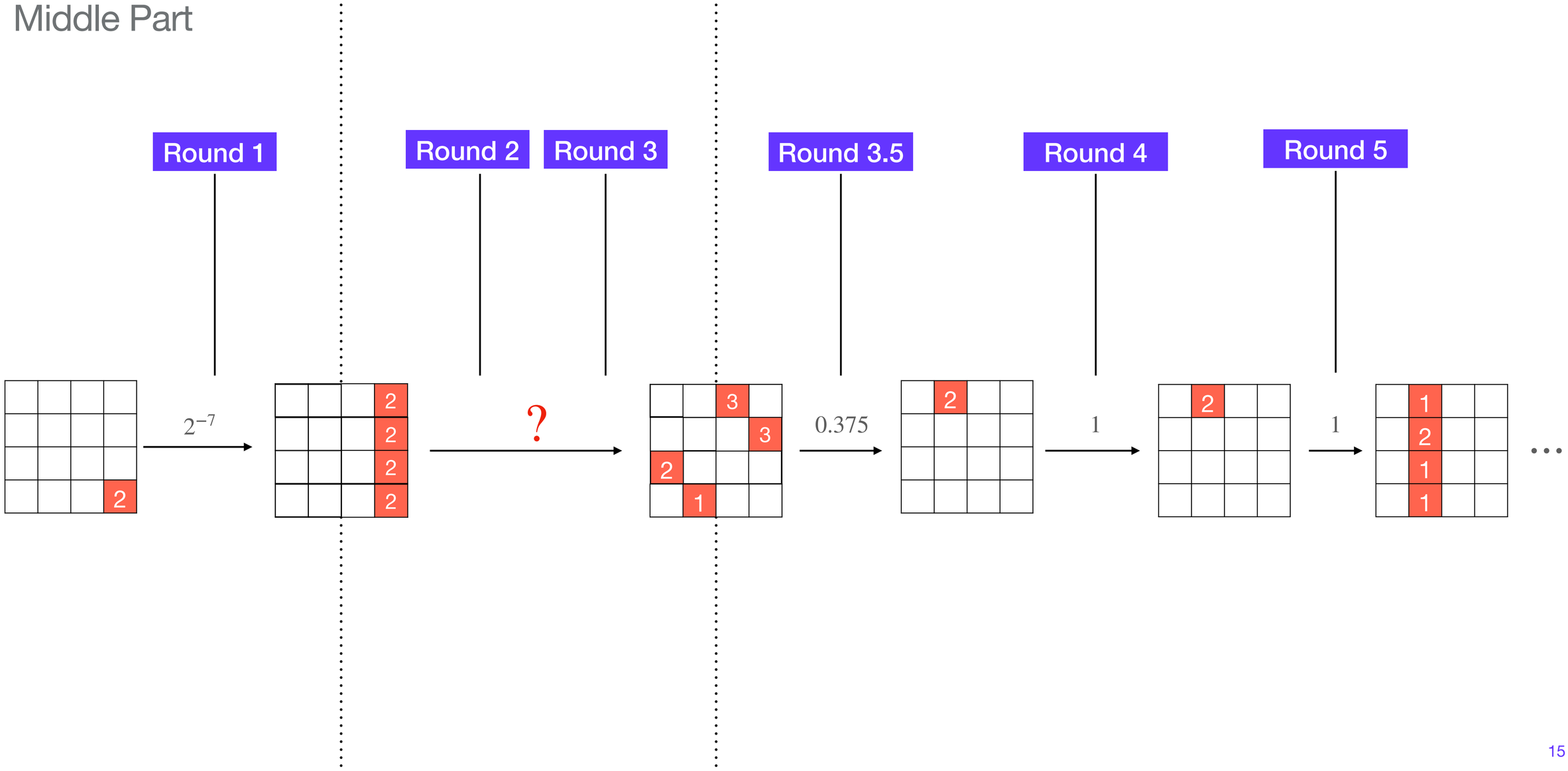
Middle Part



Computing the Correlation for the Middle Part

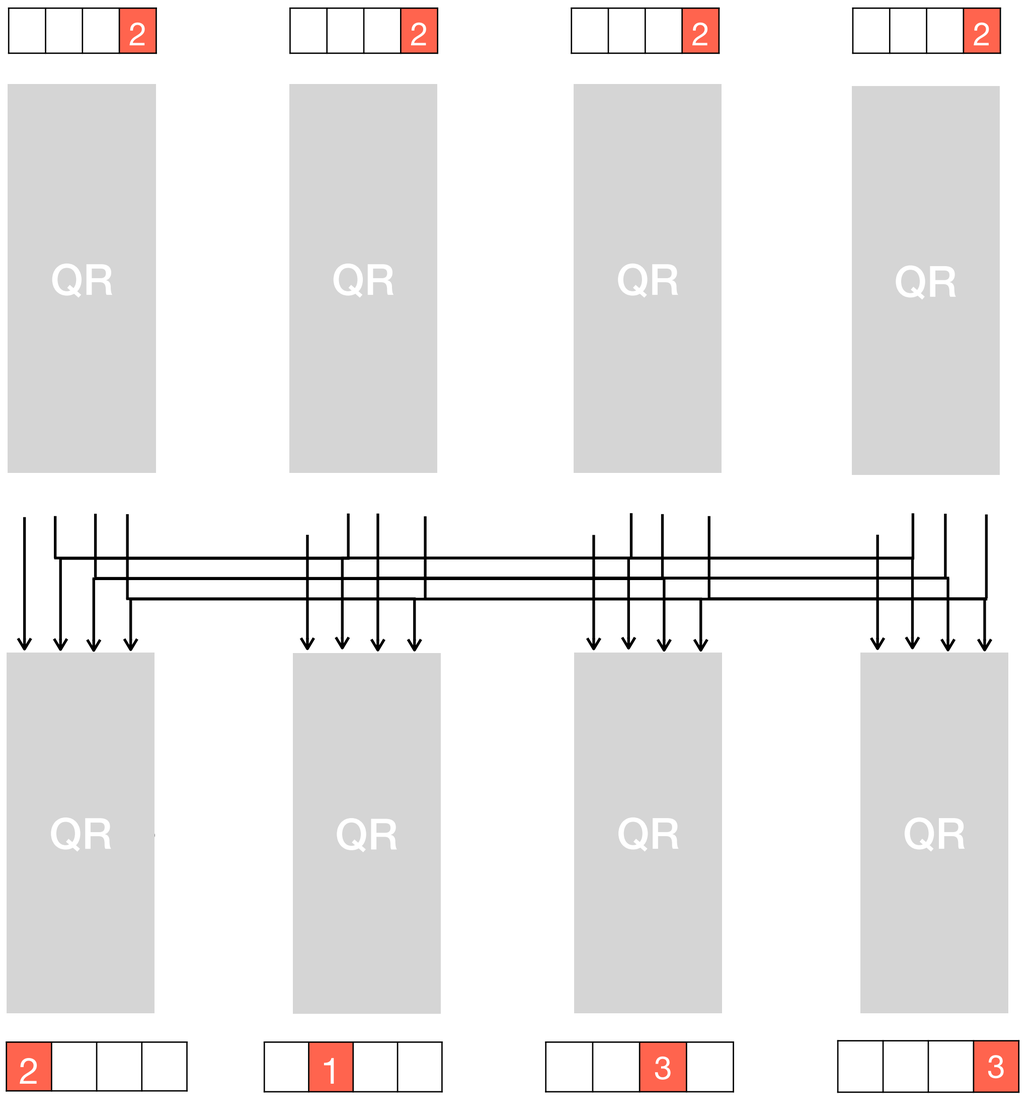
Cryptography Research Centre

Middle Part



Computing the Correlation for the Middle Part

Middle Part



Round 2

Round 3

Computing the Correlation for the Middle Part

Cryptography Research Centre

Middle Part

Round 2

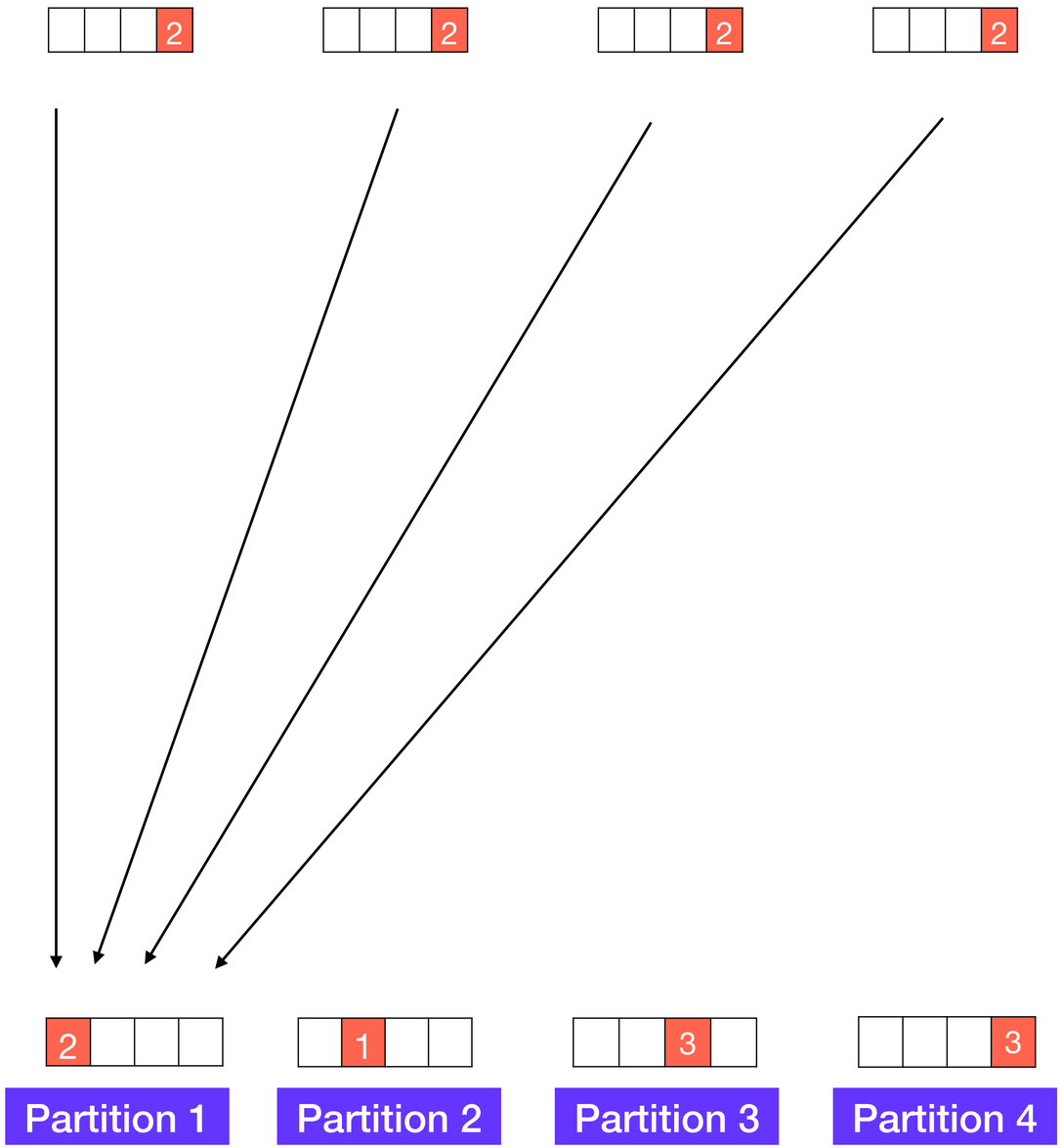
Round 3

Partition 1 | Partition 2 | Partition 3 | Partition 4

Computing the Correlation for the Middle Part

Cryptography Research Centre

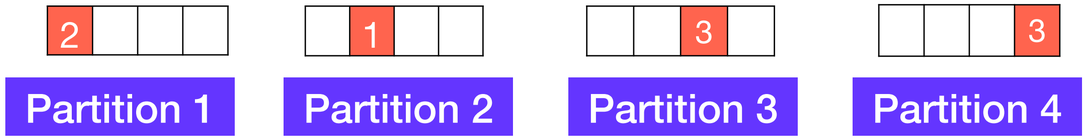
Middle Part



Computing the Correlation for the Middle Part

Cryptography Research Centre

Middle Part



Computing the Correlation for the Middle Part

Cryptography Research Centre

Middle Part

Round 2

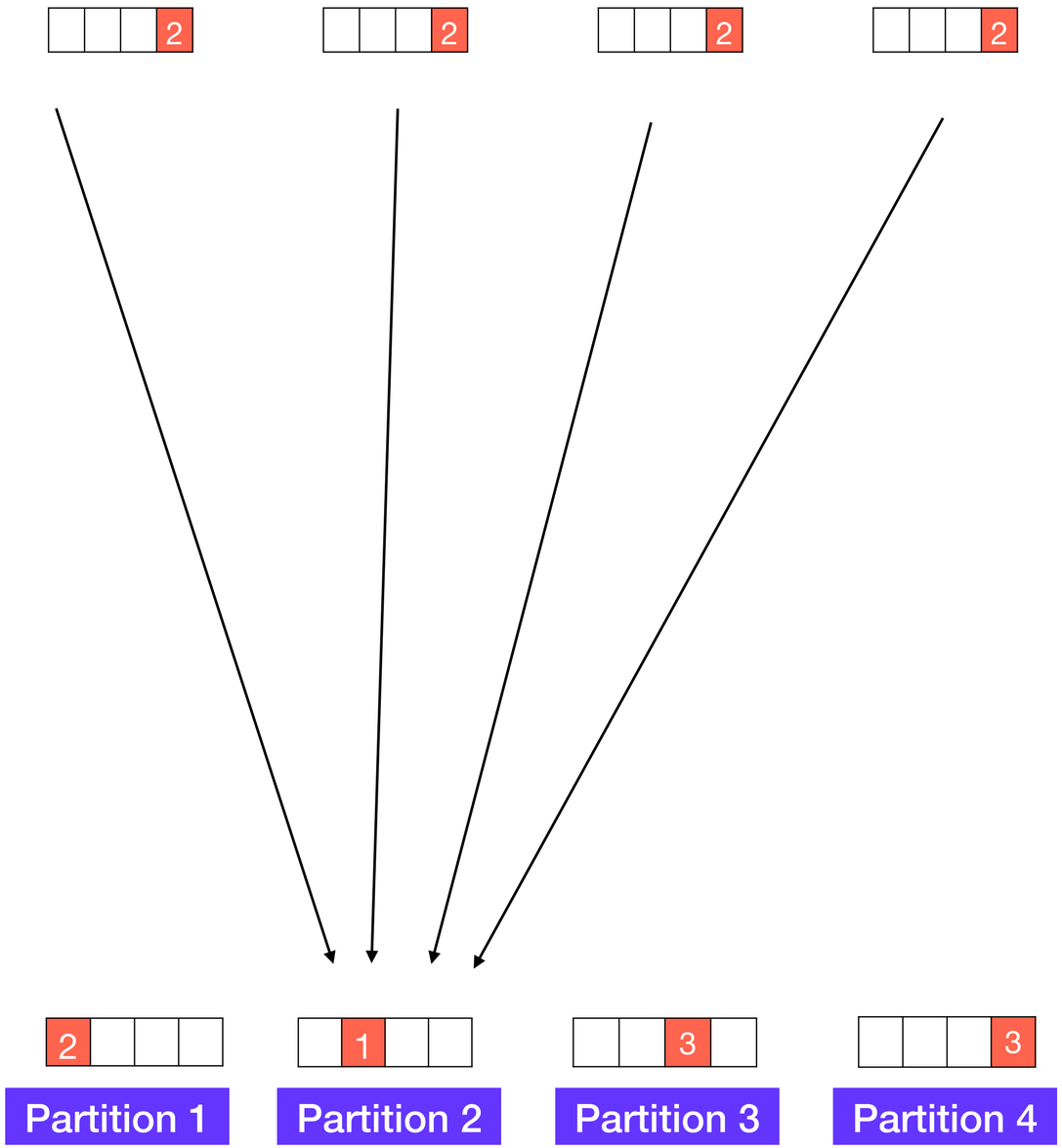
Round 3

Partition 1 | Partition 2 | Partition 3 | Partition 4

Computing the Correlation for the Middle Part

Cryptography Research Centre

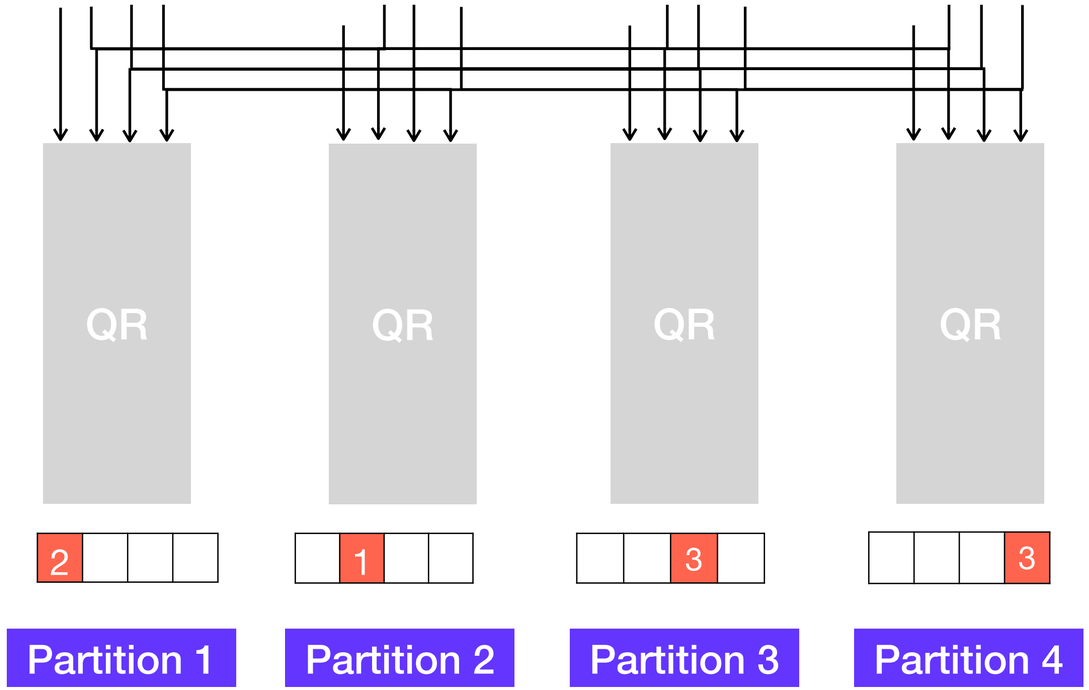
Middle Part



Computing the Correlation for the Middle Part

Cryptography Research Centre

Middle Part



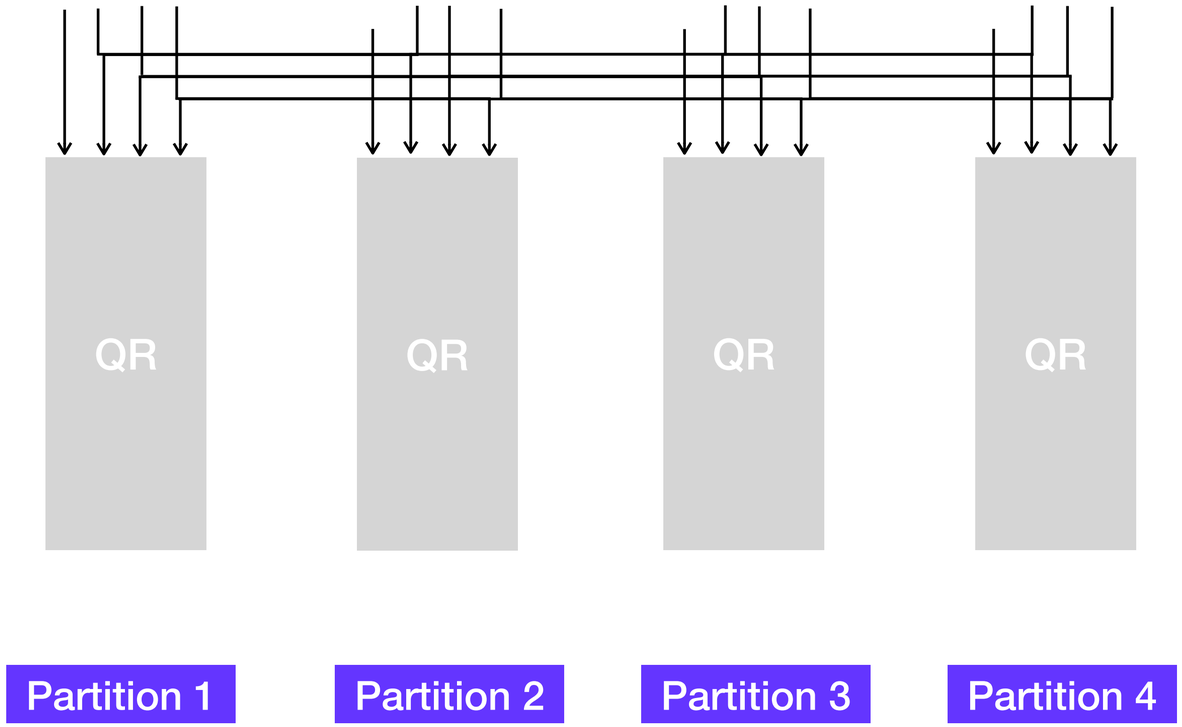
Round 3

Piling-Up Lemma

Experimental Verification with GPUs

Cryptography Research Centre

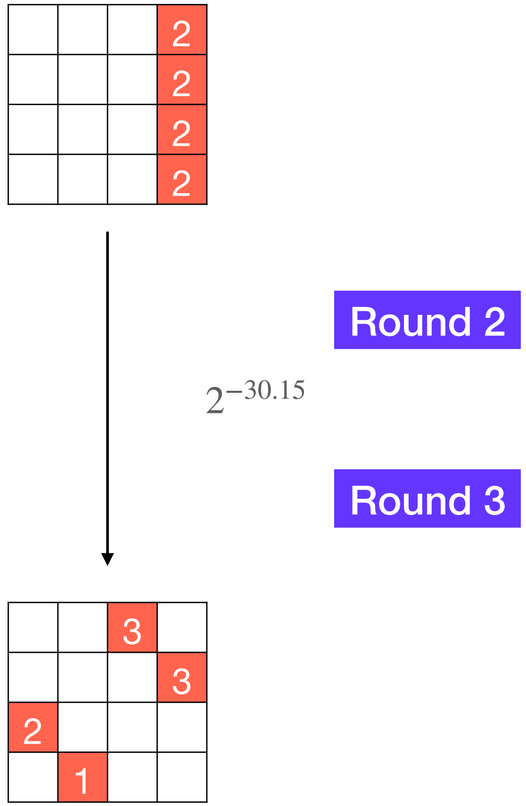
Middle Part



Partitions	Experimental	Piling-Up
1 and 2	-9.56	-10.15
1 and 3	-10.3	-12.21
1 and 4	-22.59	-24.6
2 and 4	-7.62	-8.44
2 and 4	-20.48	-20.83
3 and 4	-21.76	-22.89
1, 2 and 3	-12.75	-15.4
2, 3 and 4	-24.36	-26.08
1, 3 and 4	Too costly	Too costly
1, 2 and 4	-24.9	-27.79

Experimental Verification with GPUs

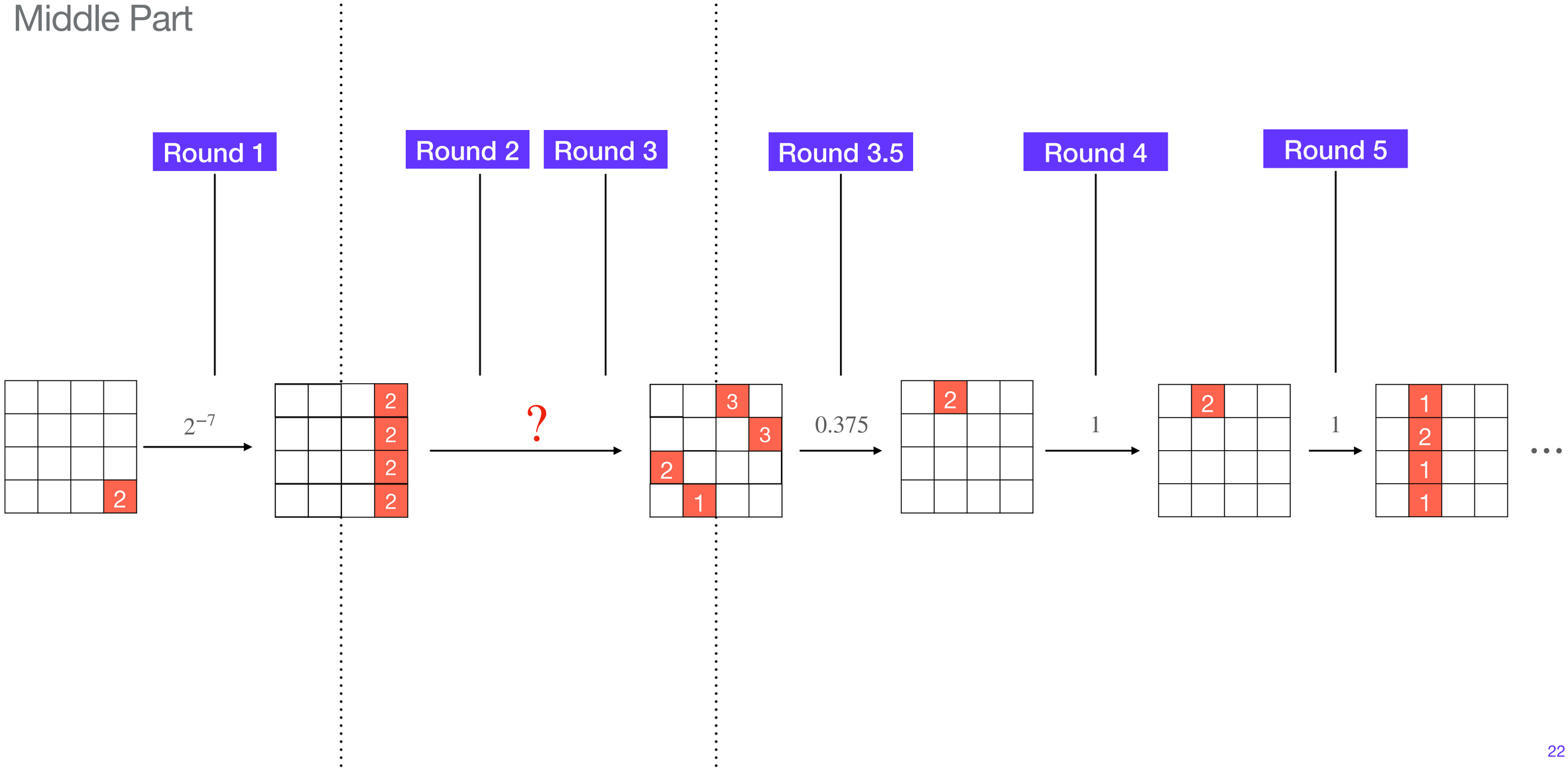
Middle Part



5-round differential-linear distinguisher

Cryptography Research Centre

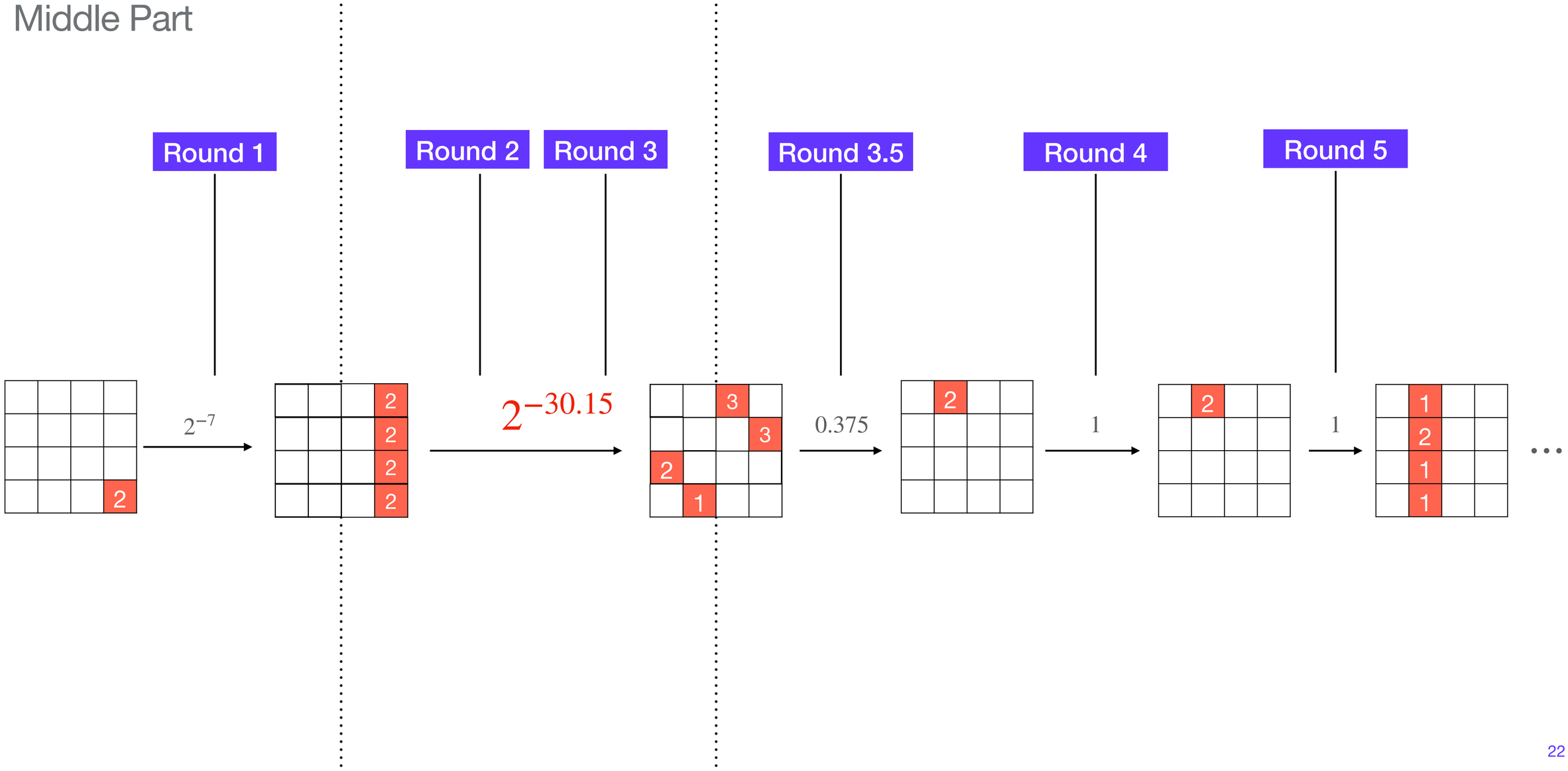
Middle Part



5-round differential-linear distinguisher

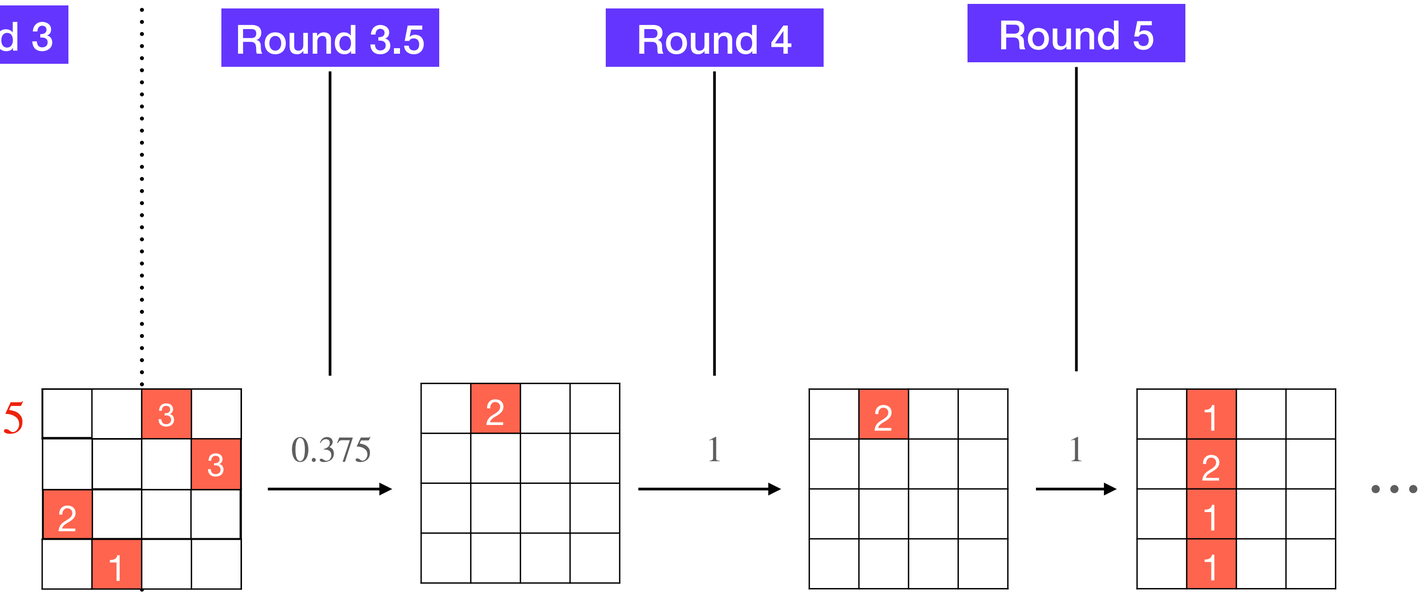
Cryptography Research Centre

Middle Part



Extending middle part to Linear Part

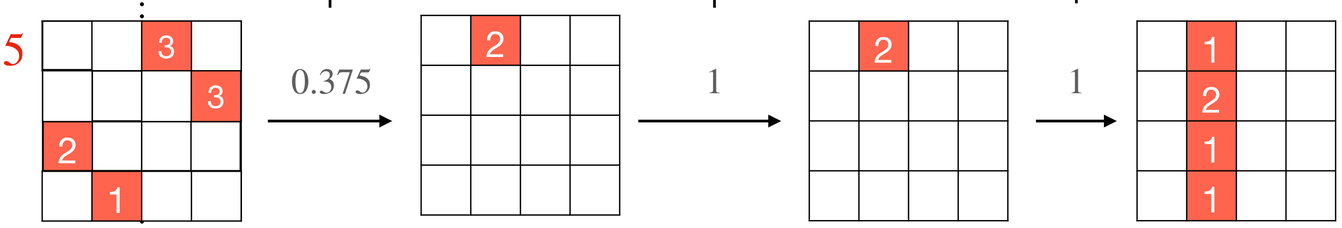
Middle Part



Linear Part

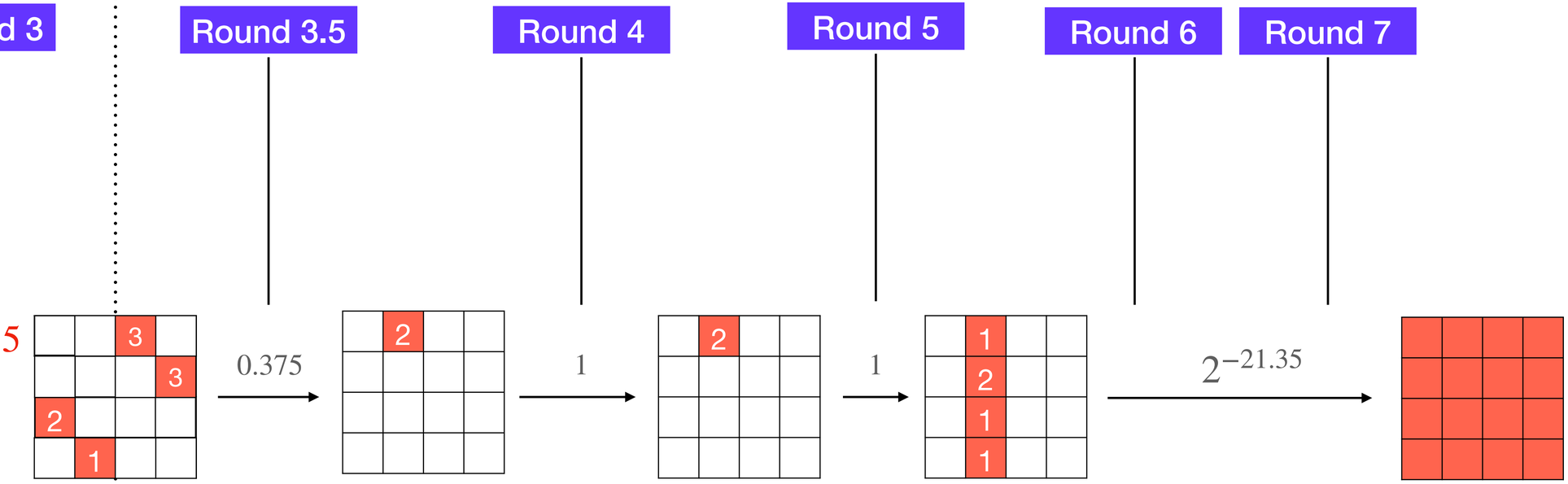
Middle Part

Round 3.5 | Round 4 | Round 5 | Round 6 | Round 7

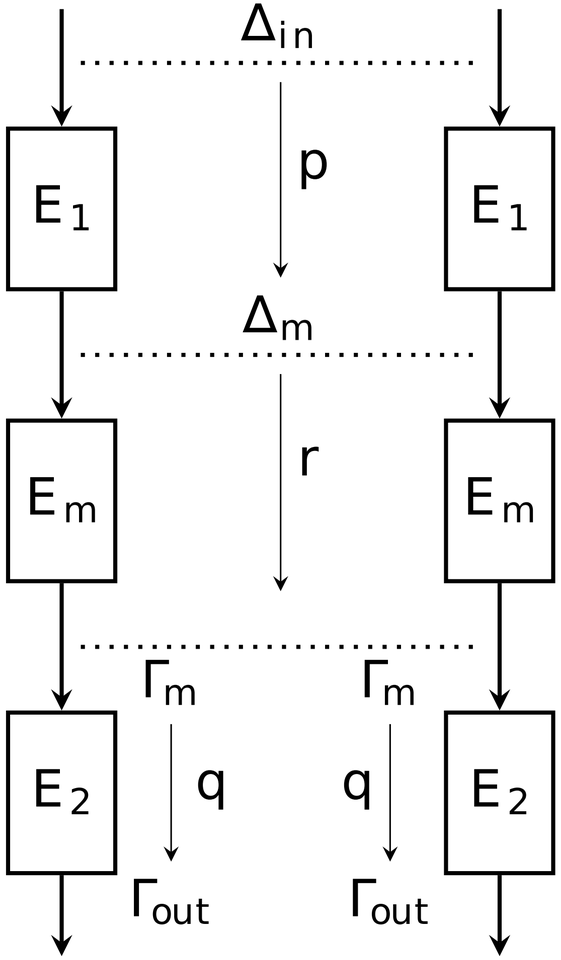


Linear Part

Middle Part



7-round DL Distinguisher



1 round $p = 2^{-7}$

2 rounds $r = 2^{-30.15}$

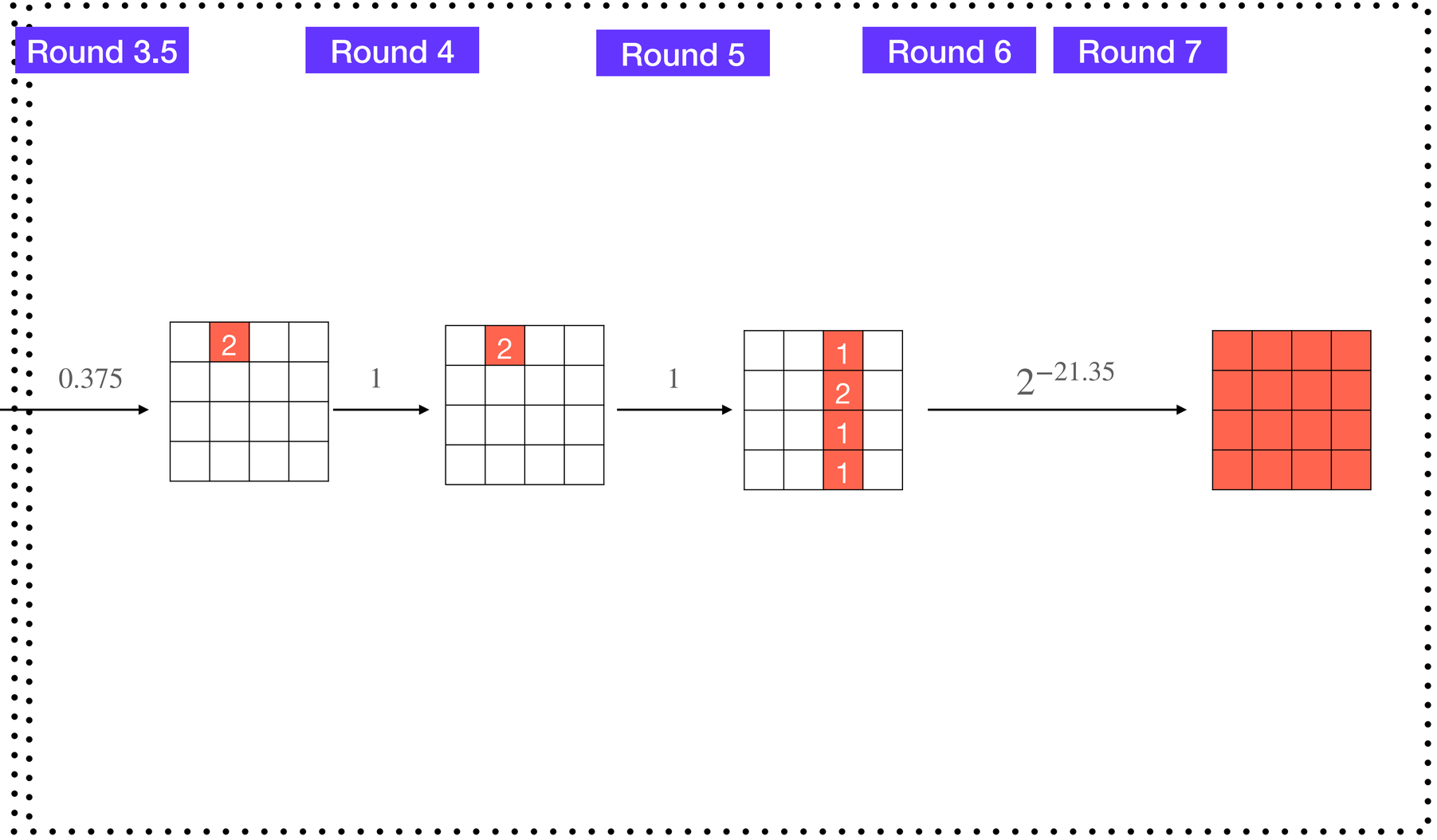
4 rounds $q = 2^{-23.15}$

Data complexity

$$p^{-2}r^{-2}q^{-4} = 2^{166.89}$$

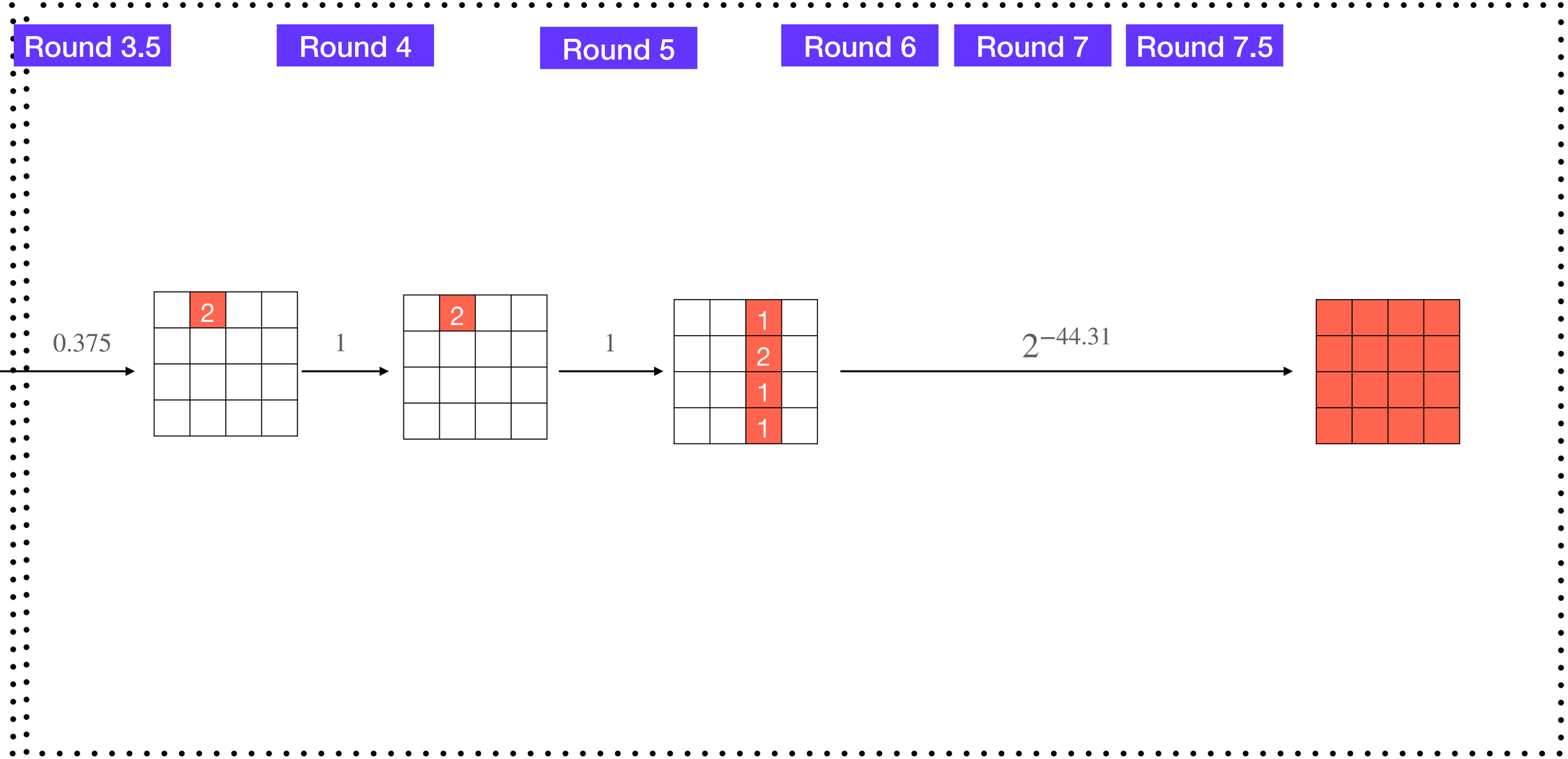
Extending from 7 to 7.5 rounds

Bottom part

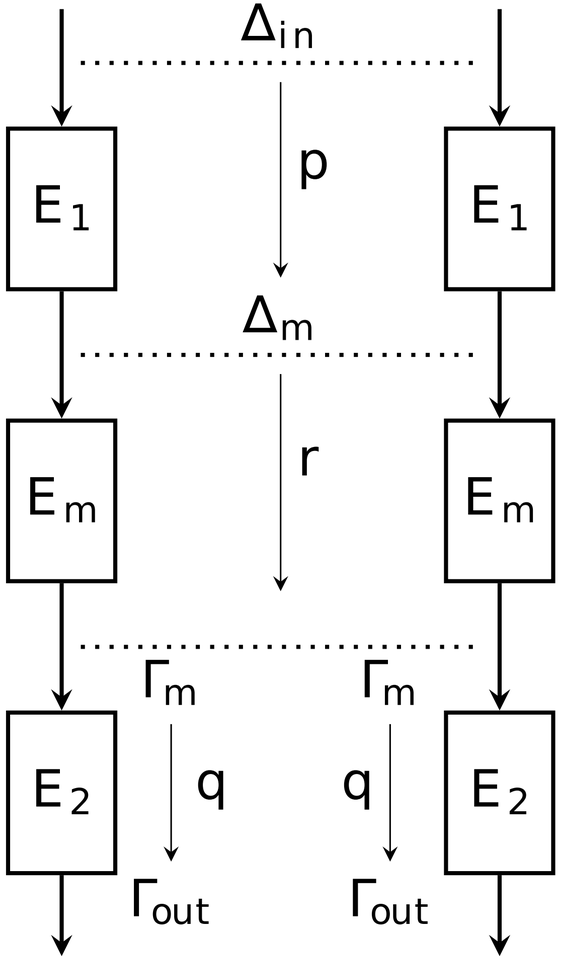


Extending from 7 to 7.5 rounds

Bottom part



7.5-round DL Distinguisher



1 round $p = 2^{-7}$

2 rounds $r = 2^{-30.15}$

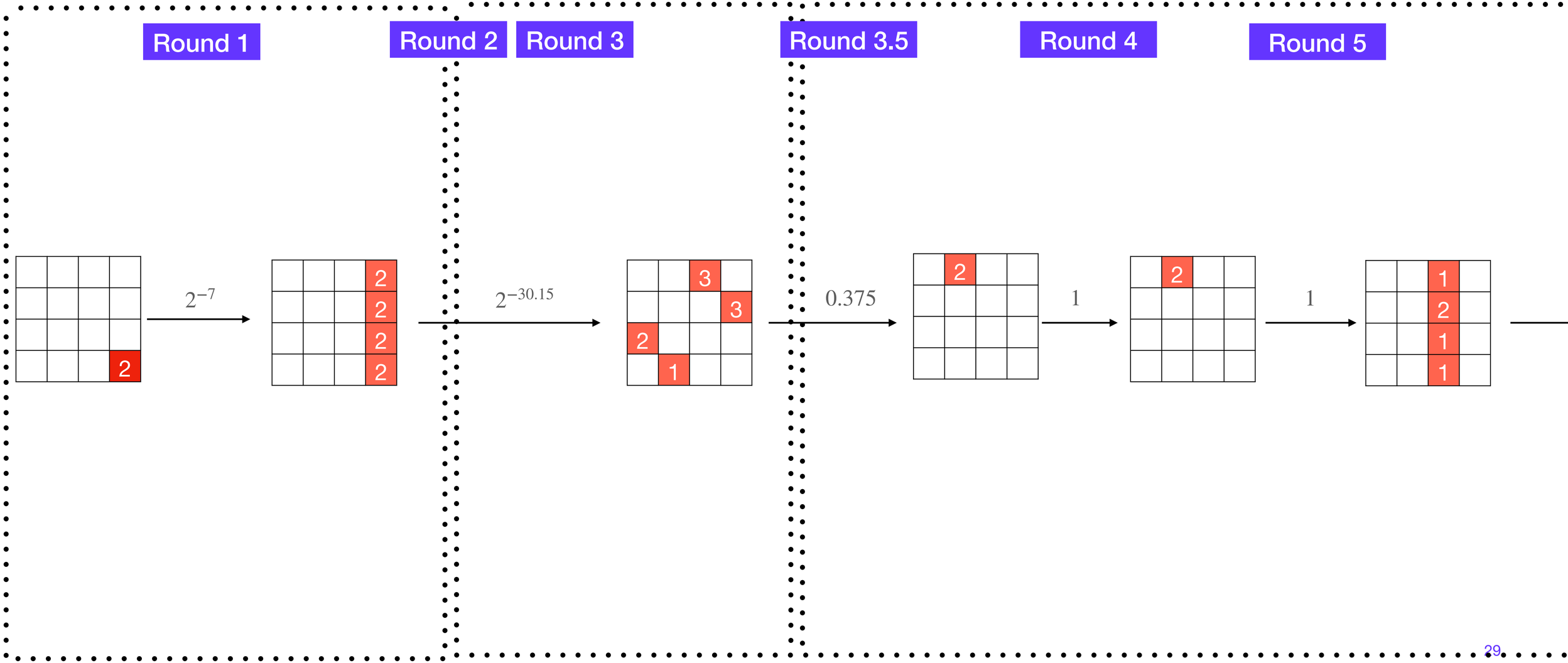
4 rounds $q = 2^{-44.31}$

Data complexity

$$p^{-2}r^{-2}q^{-4} = 2^{251.54}$$

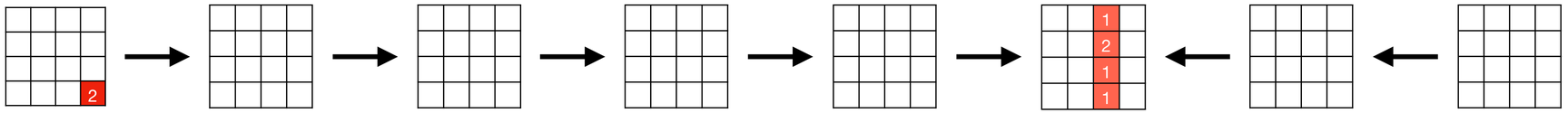
Remembering for key-recovery

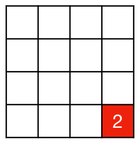
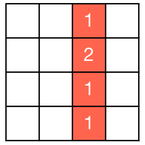
5-round Differential-Linear Distinguisher



7-round Key Recovery Attack

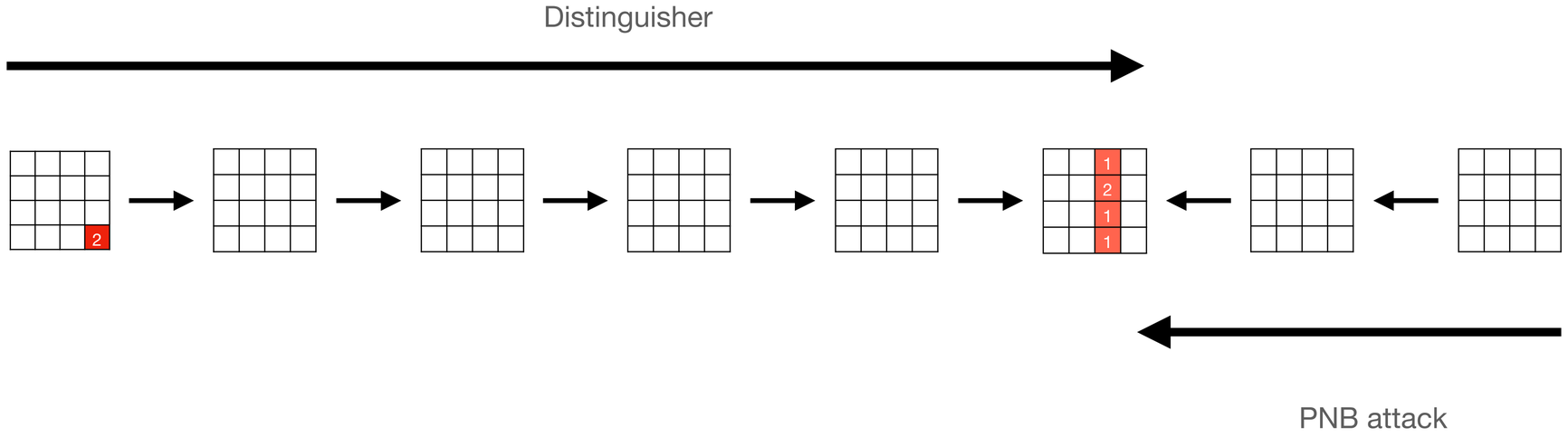
Using 5-round differential-linear distinguisher

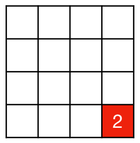
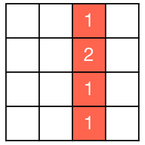


ID	OD	Corr abs(log2(x))	PNBs	Data Complexity log2	Time Complexity log2
 Hw 1	 Hw 5	−34.15	160	110.8	206.8

7-round Key Recovery Attack

Using 5-round differential-linear distinguisher

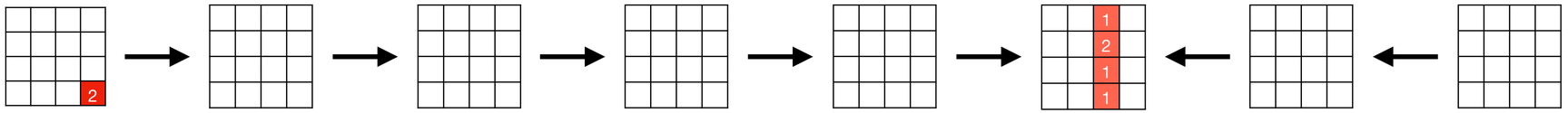


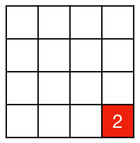
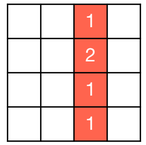
ID	OD	Corr abs(log2(x))	PNBs	Data Complexity log2	Time Complexity log2
 Hw 1	 Hw 5	−34.15	160	110.8	206.8

7-round Key Recovery Attack

Cryptography Research Centre

Using 5-round differential-linear distinguisher

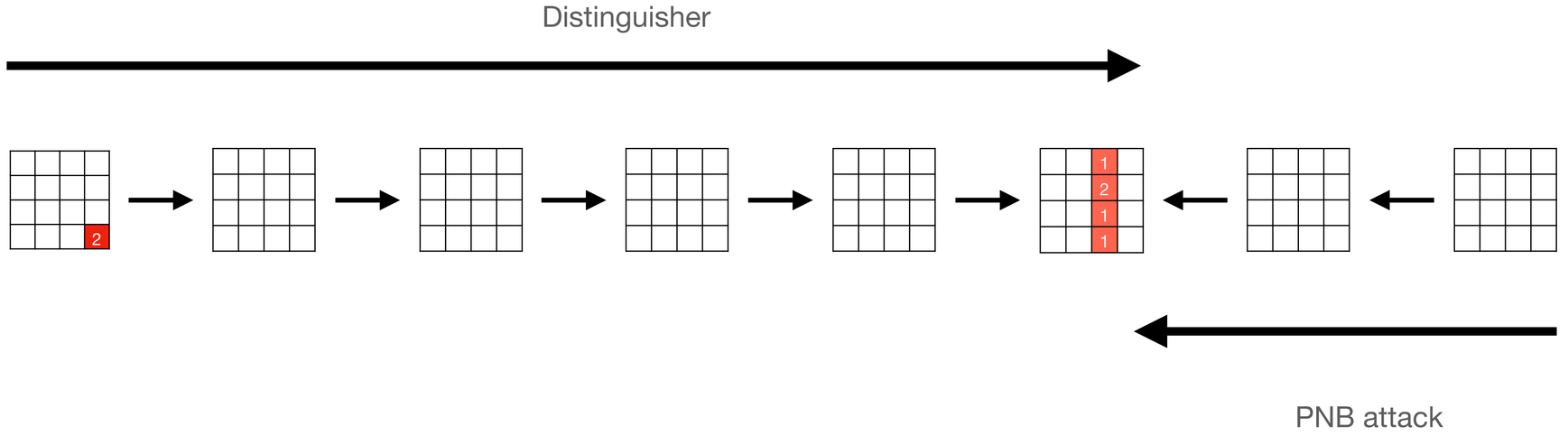


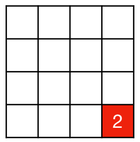
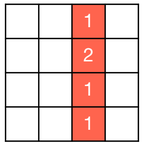
ID	OD	Corr abs(log2(x))	PNBs	Data Complexity log2	Time Complexity log2
 Hw 2	 Hw 5	−34.15	160	~~110.8~~ 111.27	~~206.8~~ 207.27

Thanks to researcher Shichang from State Key Laboratory of Information Security, Institute of Information - China

7-round Key Recovery Attack

Using 5-round differential-linear distinguisher

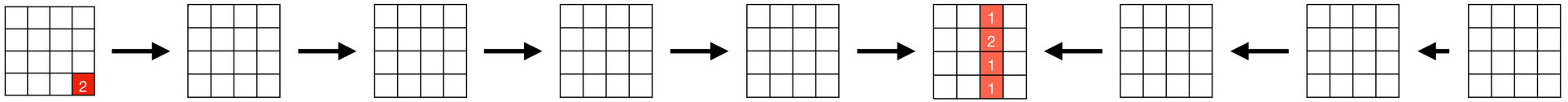


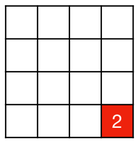
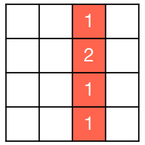
ID	OD	Corr abs(log2(x))	PNBs	Data Complexity log2	Time Complexity log2
 Hw 2	 Hw 5	−34.15	160	~~110.8~~ 111.27	~~206.8~~ 207.27

Thanks to researcher Shichang from State Key Laboratory of Information Security, Institute of Information - China

7.25-round Key Recovery Attack

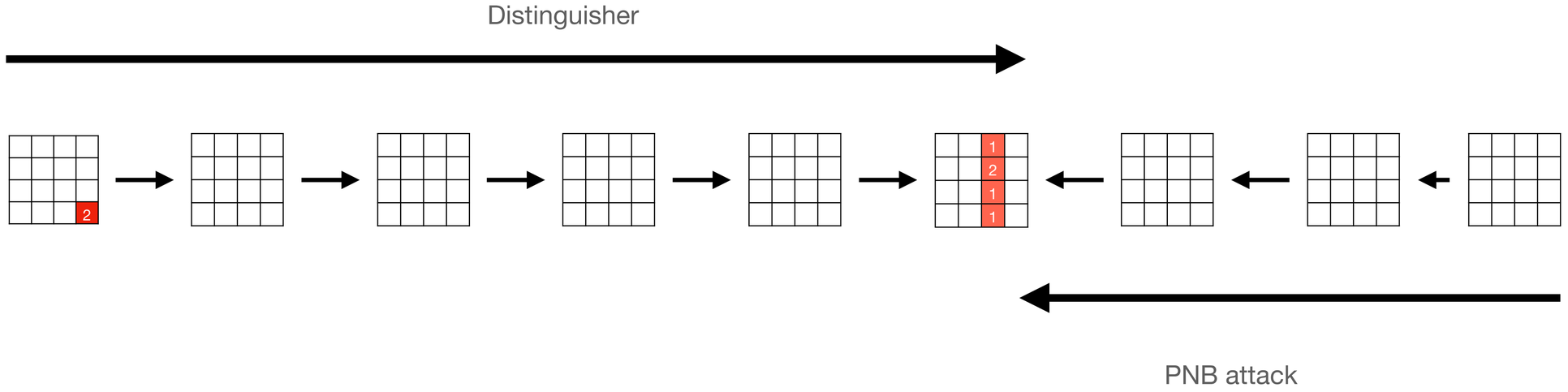
Using 5-round differential-linear distinguisher



ID	OD	Corr abs(log2(x))	PNBs	Data Complexity log2	Time Complexity log2
 Hw 2	 Hw 5	−34.15	133	122.34	238.34

7.25-round Key Recovery Attack

Using 5-round differential-linear distinguisher

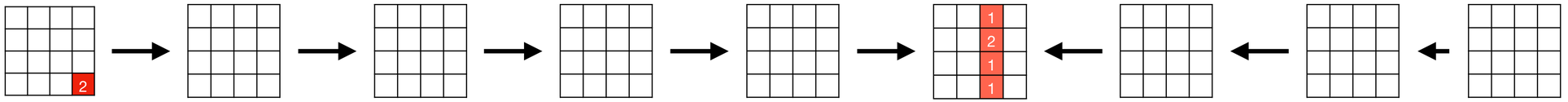


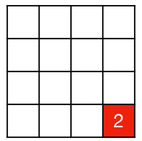
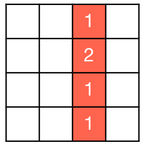
ID	OD	Corr abs(log2(x))	PNBs	Data Complexity log2	Time Complexity log2
Hw 2	Hw 5	−34.15	133	122.34	238.34

7.25-round Key Recovery Attack

Cryptography Research Centre

Using 5-round differential-linear distinguisher

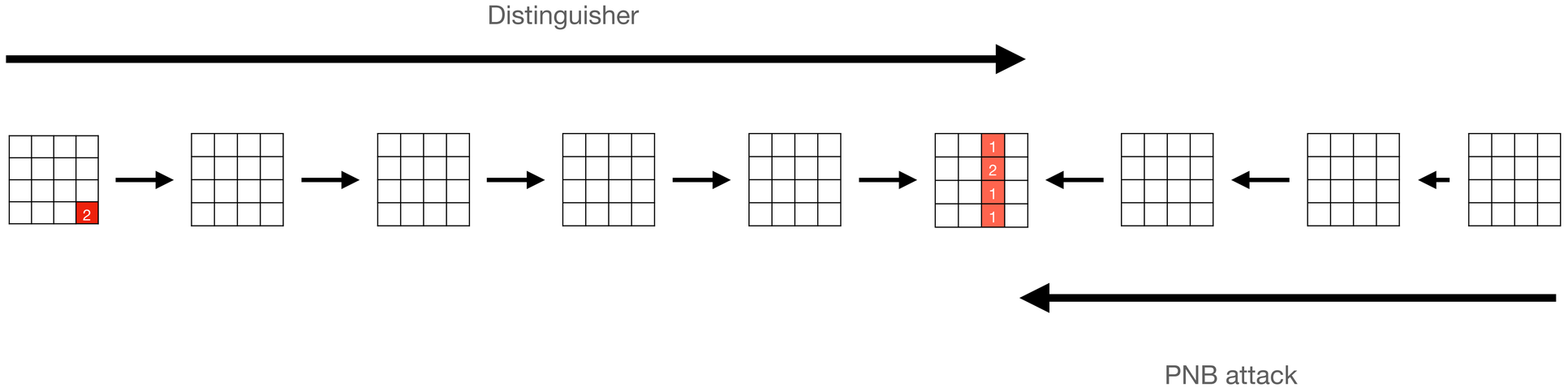


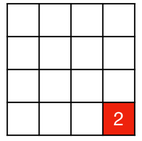
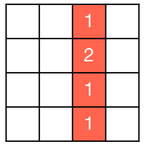
ID	OD	Corr abs(log2(x))	PNBs	Data Complexity log2	Time Complexity log2
 Hw 2	 Hw 5	−34.15	133	~~122.34~~ 124.34	~~238.34~~ 240.34

Thanks to researcher Shichang from State Key Laboratory of Information Security, Institute of Information - China

7.25-round Key Recovery Attack

Using 5-round differential-linear distinguisher



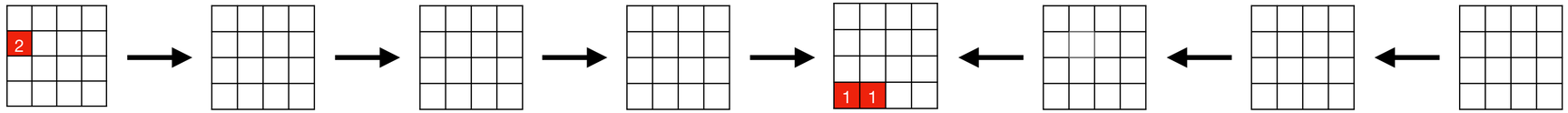
ID	OD	Corr abs(log2(x))	PNBs	Data Complexity log2	Time Complexity log2
 Hw 2	 Hw 5	−34.15	133	~~122.34~~ 124.34	~~238.34~~ 240.34

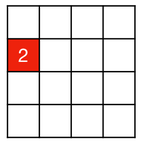
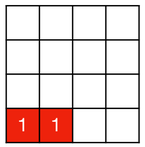
Thanks to researcher Shichang from State Key Laboratory of Information Security, Institute of Information - China

Another distinguisher and key-recovery attack

Cryptography Research Centre

- Distinguisher
  - 4-round with from round 1 to 4 with correlation $2^{-18.75}$ better than previous works due our MILP implementation in the linear part

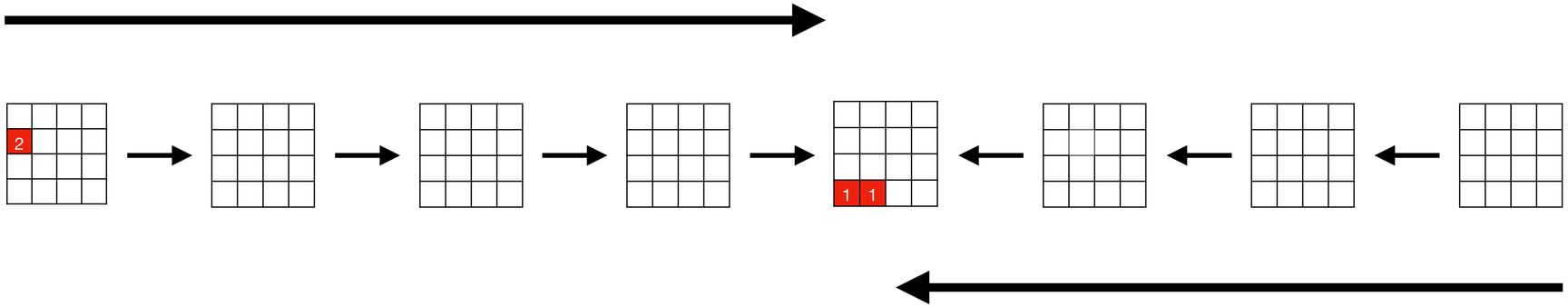


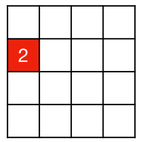
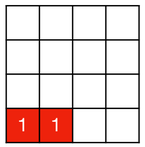
ID	OD	Corr abs(log2(x))	PNBs	Data Complexity log2	Time Complexity log2
 Hw 2	 Hw 2	-18.75	126	95.07	226.03

Another distinguisher and key-recovery attack

Cryptography Research Centre

- Distinguisher
  - 4-round with from round 1 to 4 with correlation $2^{-18.75}$ better than previous works due our MILP implementation in the linear part



ID	OD	Corr abs(log2(x))	PNBs	Data Complexity log2	Time Complexity log2
 Hw 2	 Hw 2	-18.75	126	95.07	226.03

Distinguisher Comparison

Cryptography Research Centre

Time complexity of Chacha reduced to 7-round and 7.5 distinguishers and with 256-bit key.

Rounds	Rounds split	Complexity (log2)	Reference
7	1+2.5+3.5	224	[CN21a]
	3+4	214	[CPV+22]
	1+2+4	166.89	This work
7.5	1+2+4.5	251.4	This work

Key-recovery attack comparison

Summary of the best key-recovery attacks to ChaCha reduced to 7 round

	Distinguisher	Key recovery		
Reference	Split	#PNBs	Time (log2)	Data (log2)
[AFK+08]	3+0+0	35	248	27
[SZW12]	3+0+0	35, 34, 32, 28	246.5	27
[Mai16]	3+0+0	41	238.94	96
[CM16b]	4.5+0+1.5	50	237.65	96
[DS17]	4.5+0+1.5	53	235.22	-
[BLT20]	1+2.5+1.5	74	230.86	48.53
[CS21]	3.5+0+0	74	231.63	49.58
[CN21b]	1+2.5+1.5	108	228.51	80.51
[DGSS22]	1+2.5+0.5	79	221.95	90.20
Our work	1+2+2	160	207.27	111.27

Conclusions

Cryptography Research Centre

- We improved the best 7-round attacks presented in the literature on this primitive (both distinguisher and key-recovery).
- We present the first distinguisher against ChaCha reduced to 7.5 rounds (at the time of publication of this paper).
- These results were possible thanks to several new strategies:
  - We explored DL distinguishers with 2 bits flipped at the beginning of the differential part
  - We implemented a MILP model to automate the search for more effective linear masks in the linear part.
  - For the middle part, we studied and optimised the CUDA implementation presented in [Cou22] to verify our results.
  - Also, we can explore the three-stage strategy presented in [DGSS22] to increase the number of PNBs and thus reduce the key-recovery attack complexities even more.

Cryptography
Research
Centre

Thanks

Background

Identifying PNBs

Background

Identifying PNBs

Cryptography Research Centre

P_1

Background

Identifying PNBs

Background

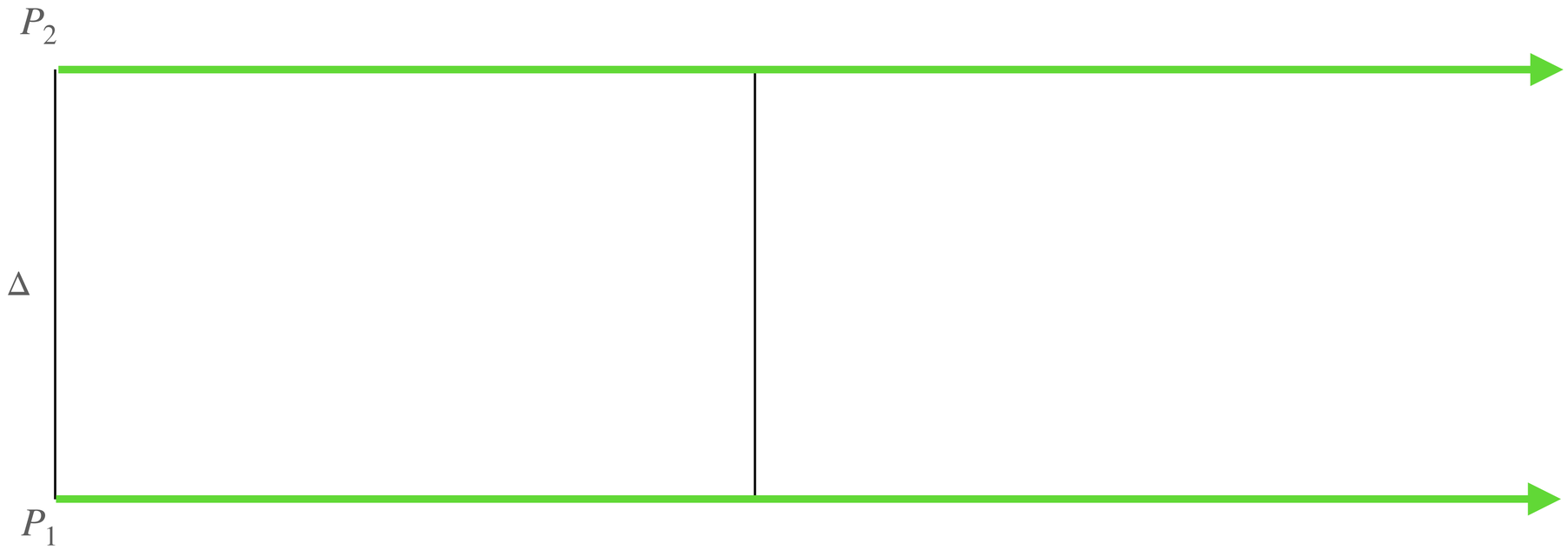
Identifying PNBs

Background

Identifying PNBs

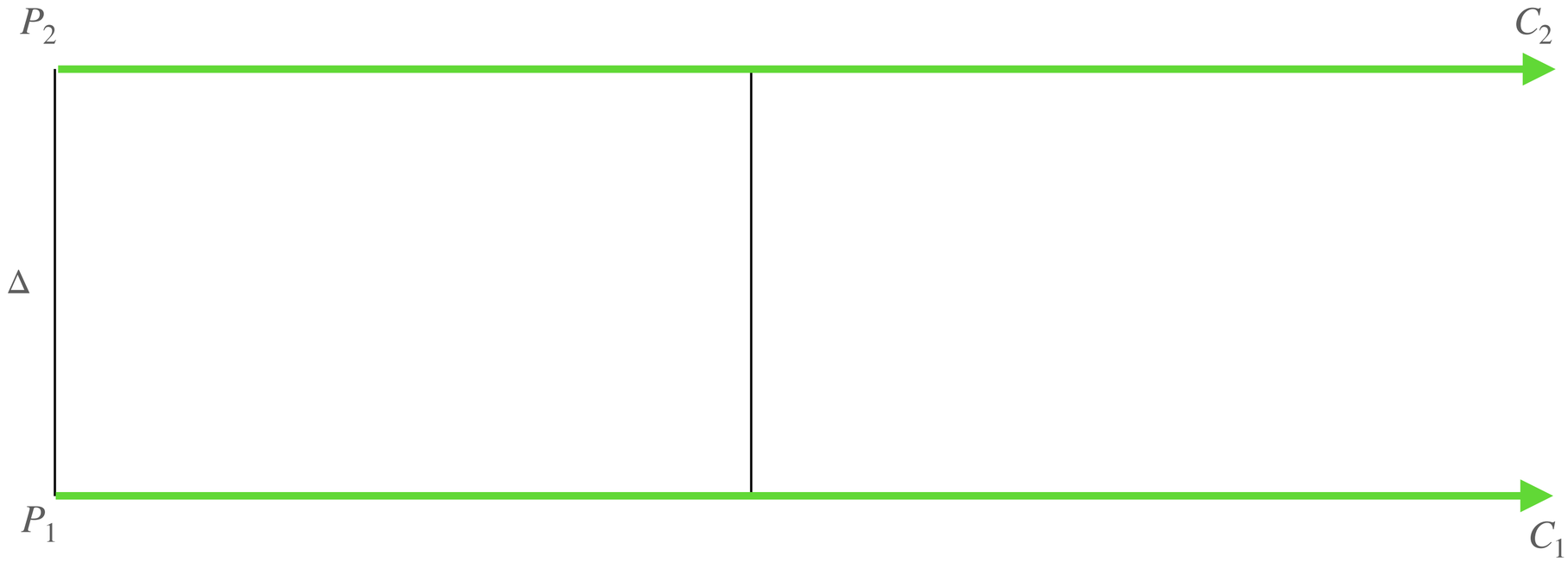
Background

Identifying PNBs



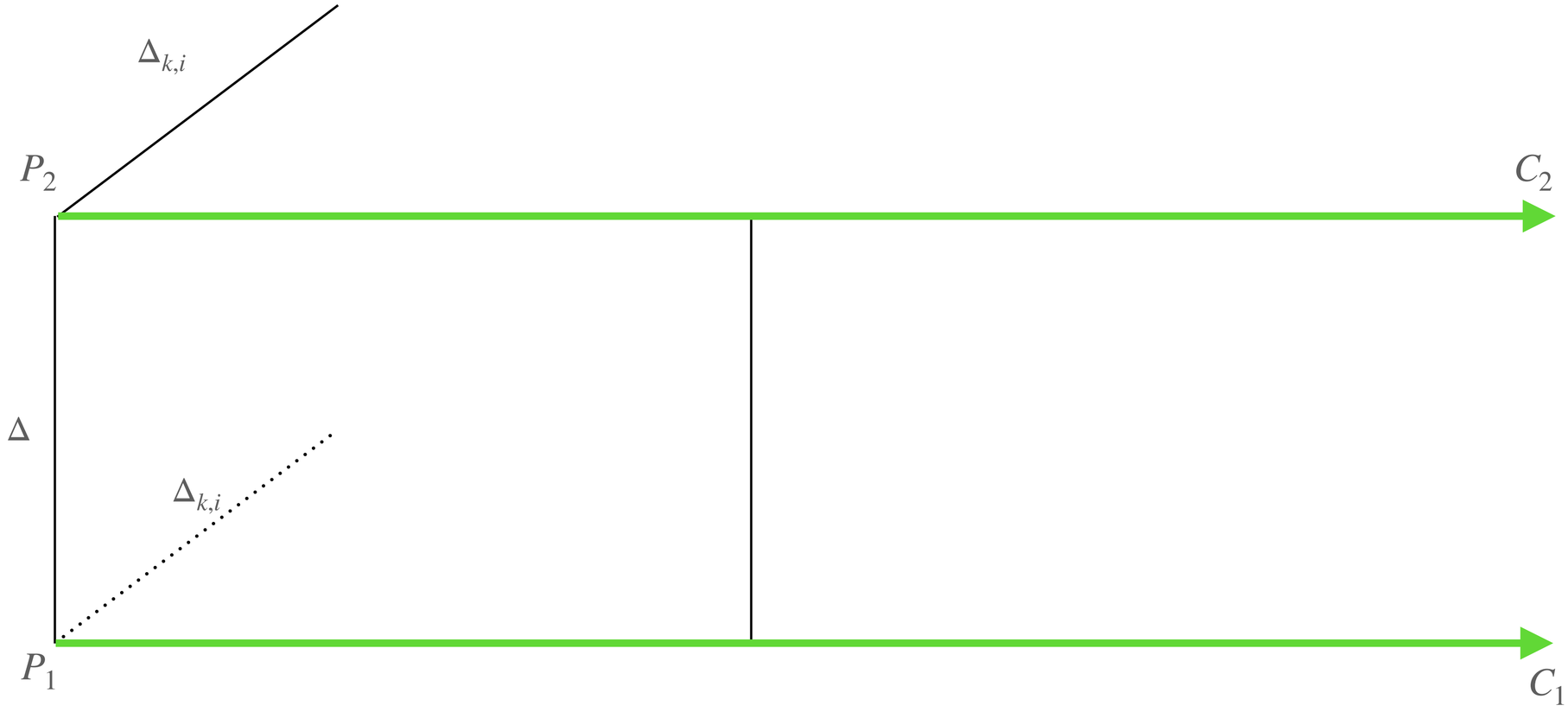
Background

Identifying PNBs



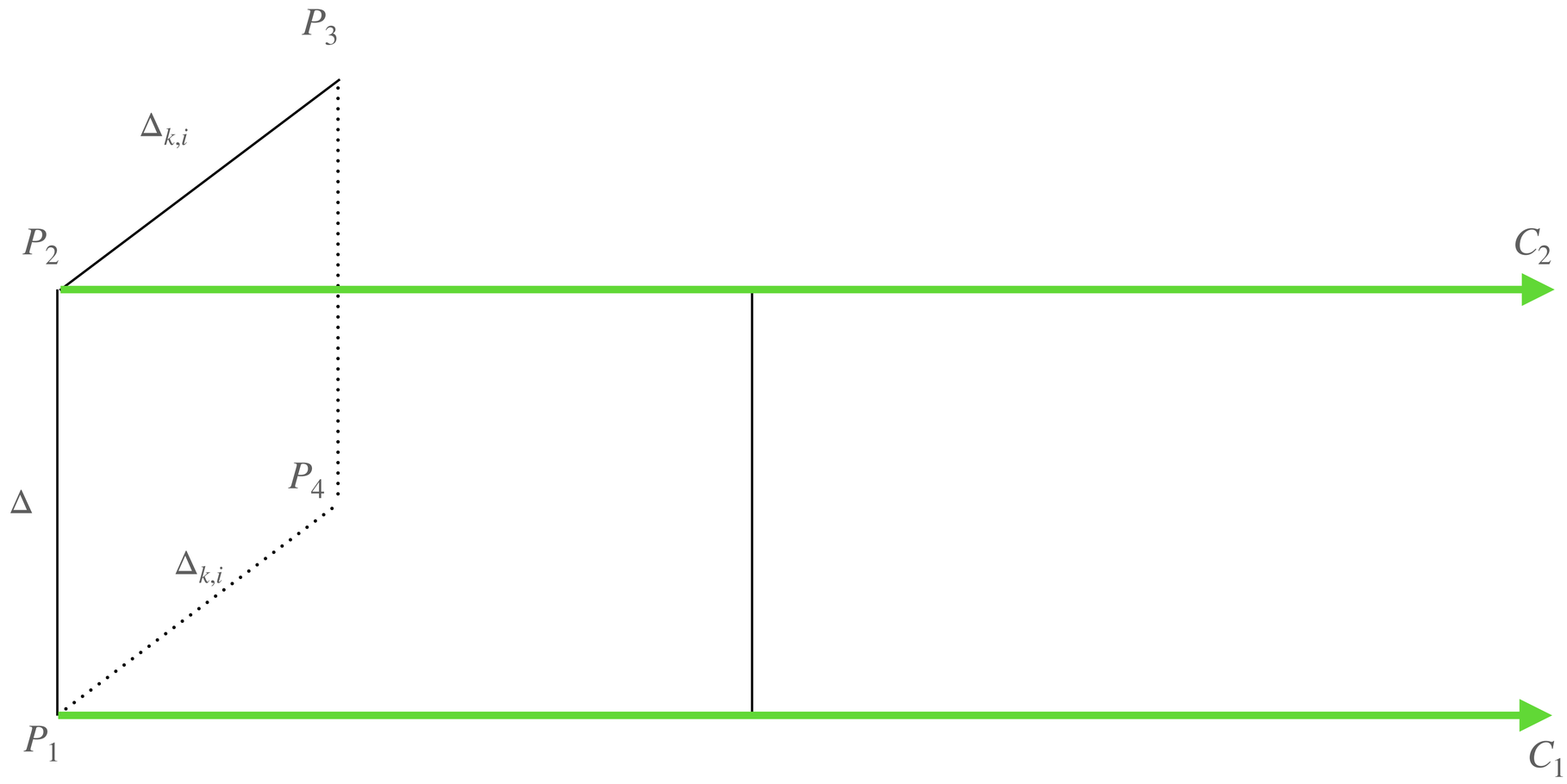
Background

Identifying PNBs



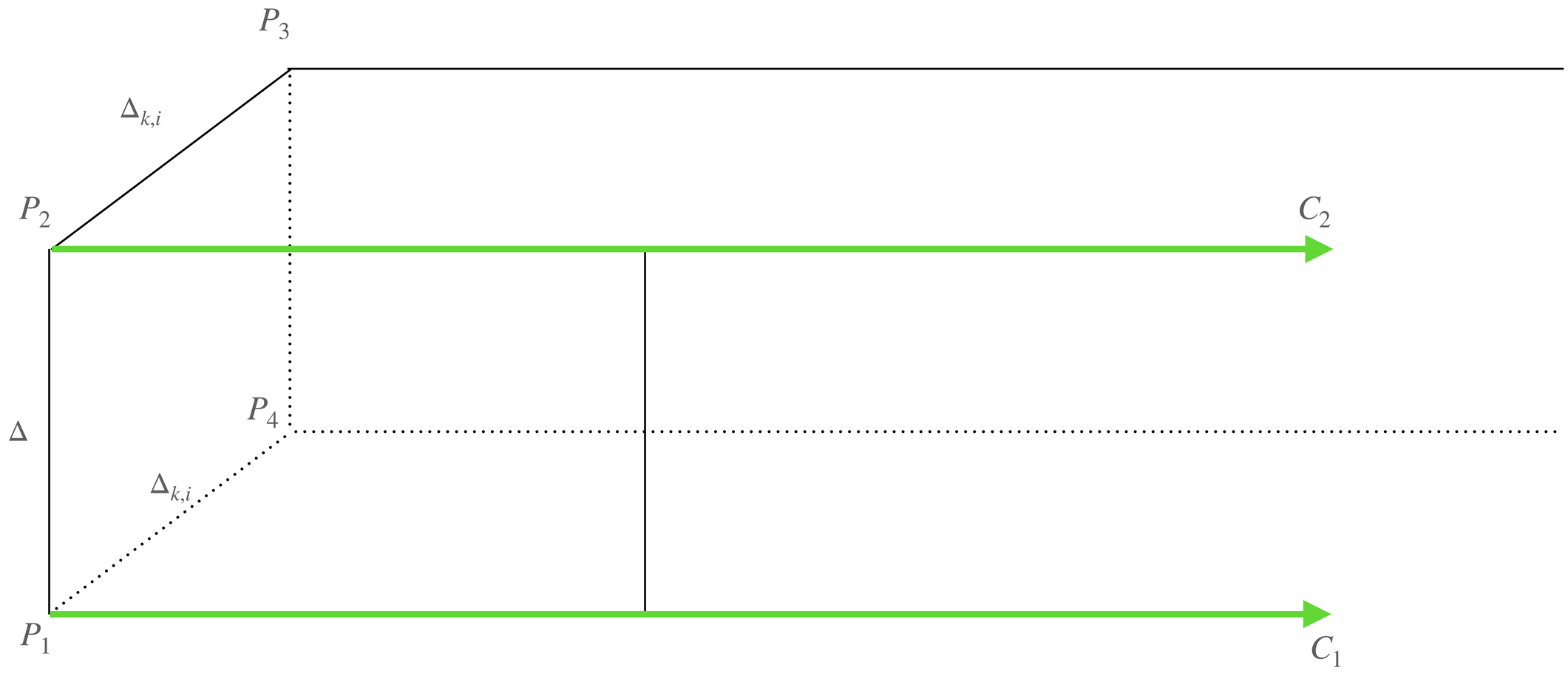
Background

Identifying PNBs



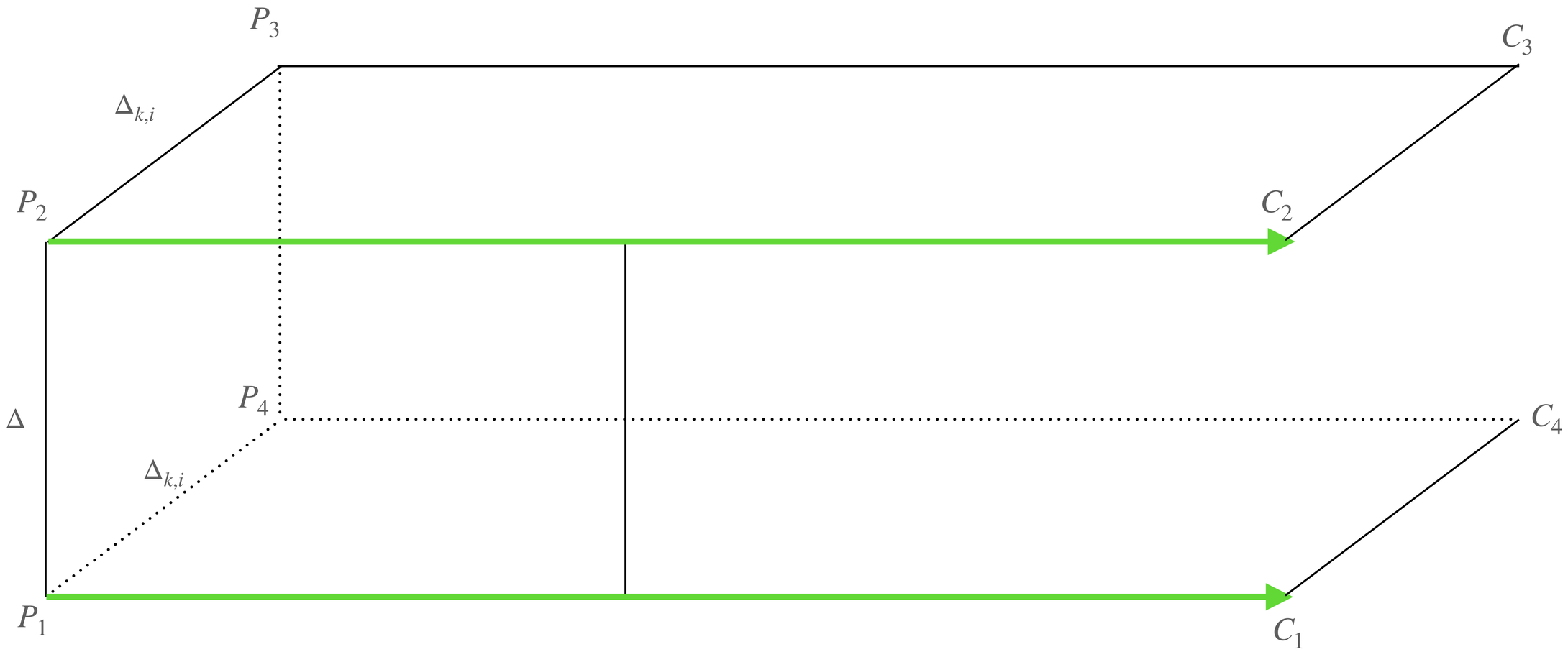
Background

Identifying PNBs



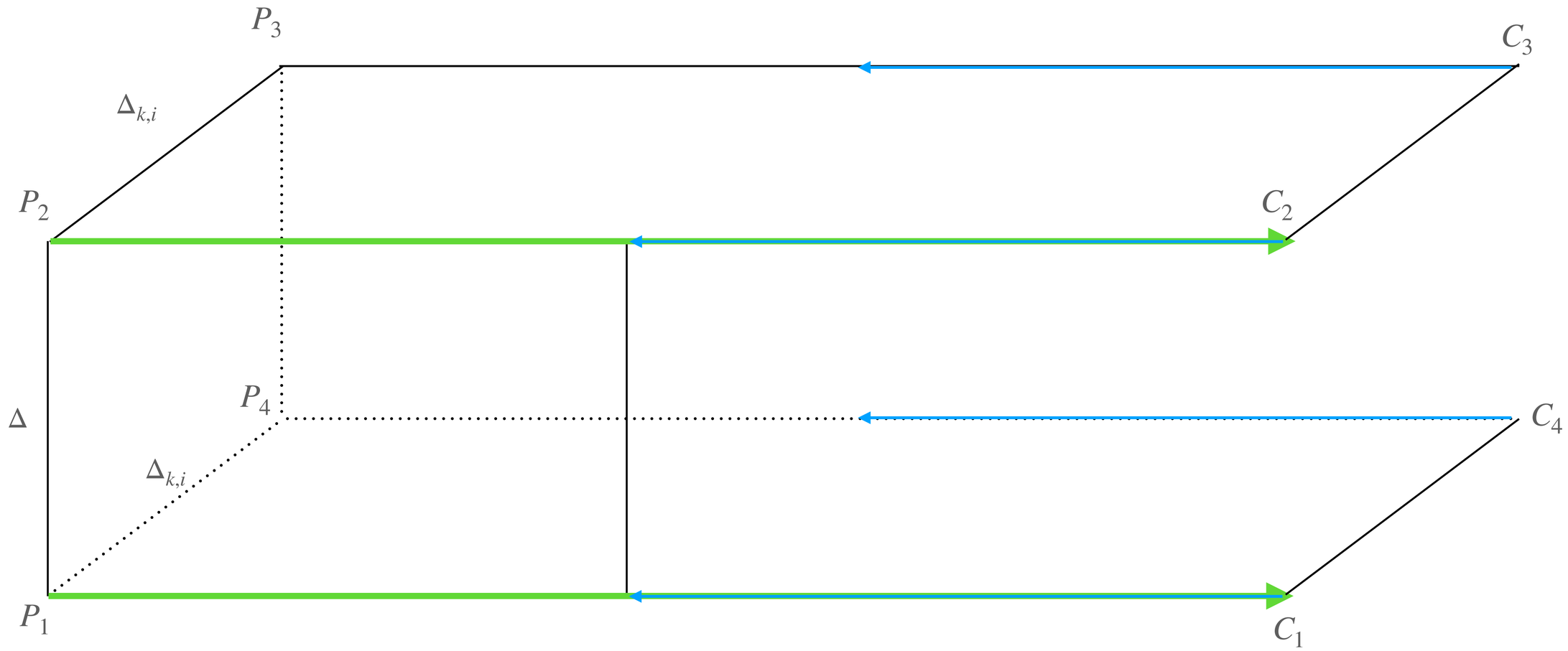
Background

Identifying PNBs



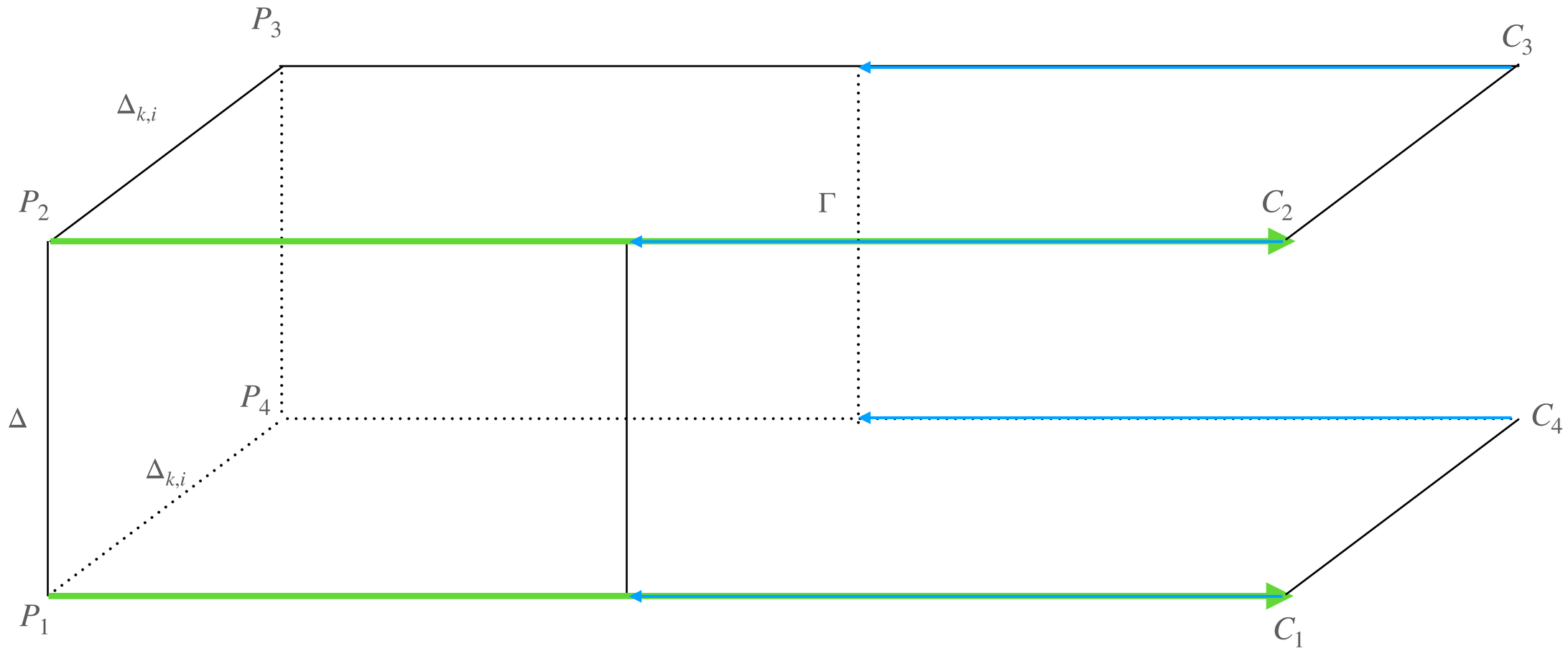
Background

Identifying PNBs



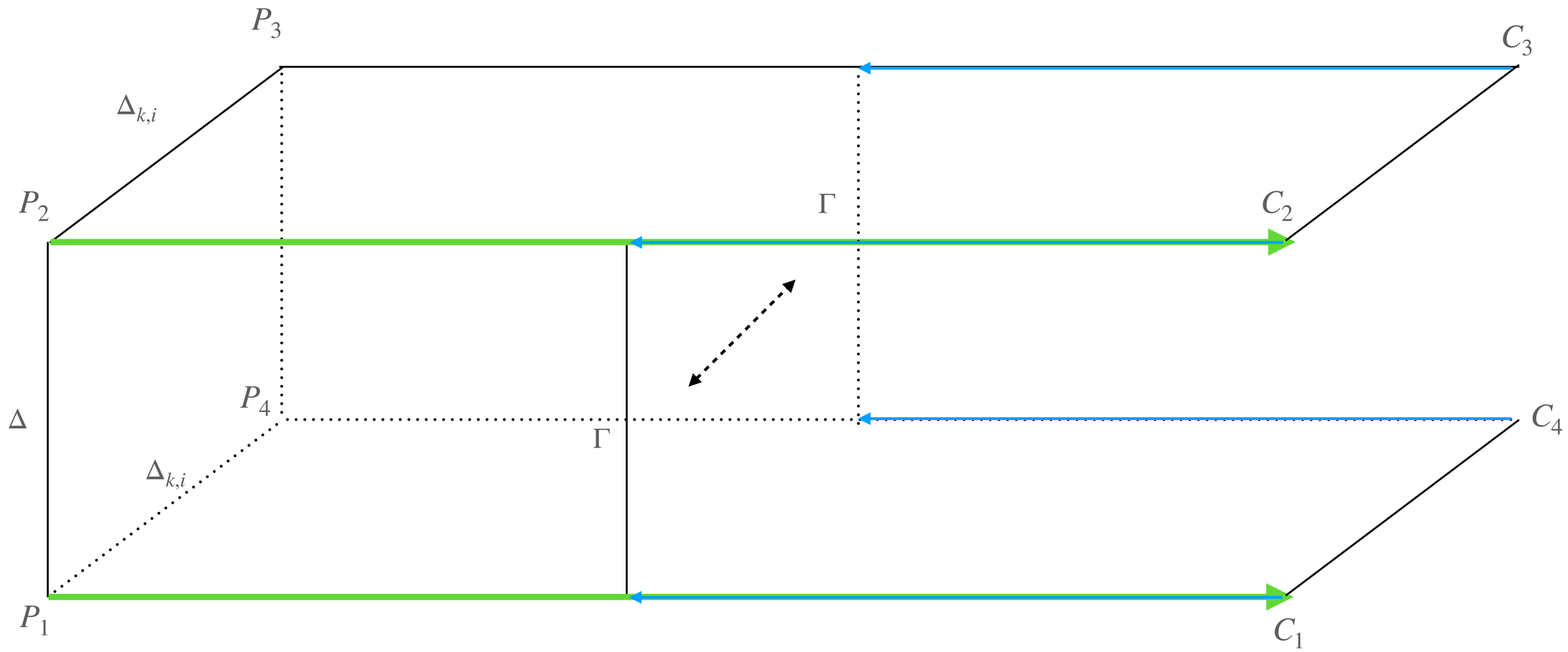
Background

Identifying PNBs



Background

Identifying PNBs



Background

Identifying PNBs