Latin Dances Reloaded: Improved Cryptanalysis against Salsa and ChaCha, and the proposal of Forró

Murilo Coutinho, Iago Passos, Juan Grados, Rafael T. de Sousa Jr, Fábio Borges

1 Electrical Engineering Department (ENE), Technology College, University of Brasilia, Brasilia, Brazil
2 Technology Innovation Institute, Abu Dhabi, UAE
3 National Laboratory for Scientific Computing, Petrópolis, Brazil

Cryptography Research Center

tii.ae

Agenda

- Review ChaCha and Salsa
- Review cryptanalysis against Chacha and Salsa
- Review best attack techniques against ChaCha and Salsa
- Our contributions
  - Cryptanalysis against Salsa and ChaCha
  - New cipher Forró
- Conclusions

Background

Salsa description

- Stream cipher Invented by Daniel J. Bernstein in 2005
- 20 rounds
- Fast in software
- Resistance against timing attacks and cache attacks
- You can generate 2^{64} streams

Background

ChaCha description

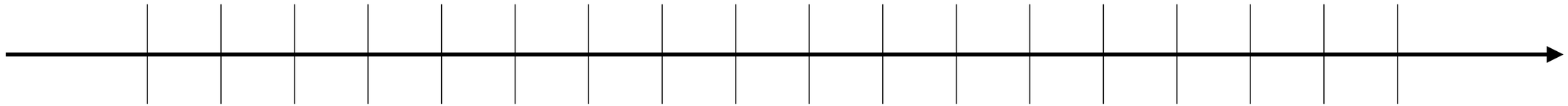
- Stream cipher invented by Daniel J. Bernstein
- Fast in software environment
- Resistance against timing attacks and cache attacks
- 20 rounds
- Better Diffusion than Salsa
- Actually used in TLS v1.3

Related Works

Attacking Salsa

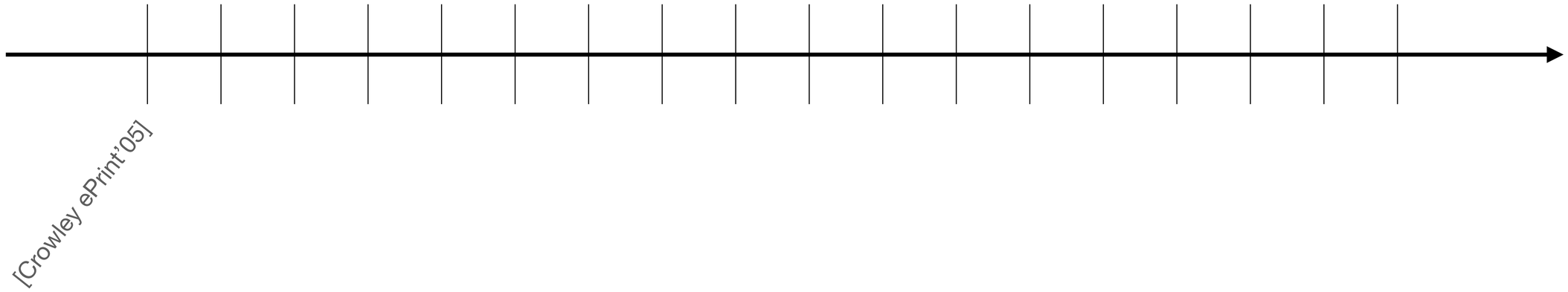
Related Works

Attacking Salsa



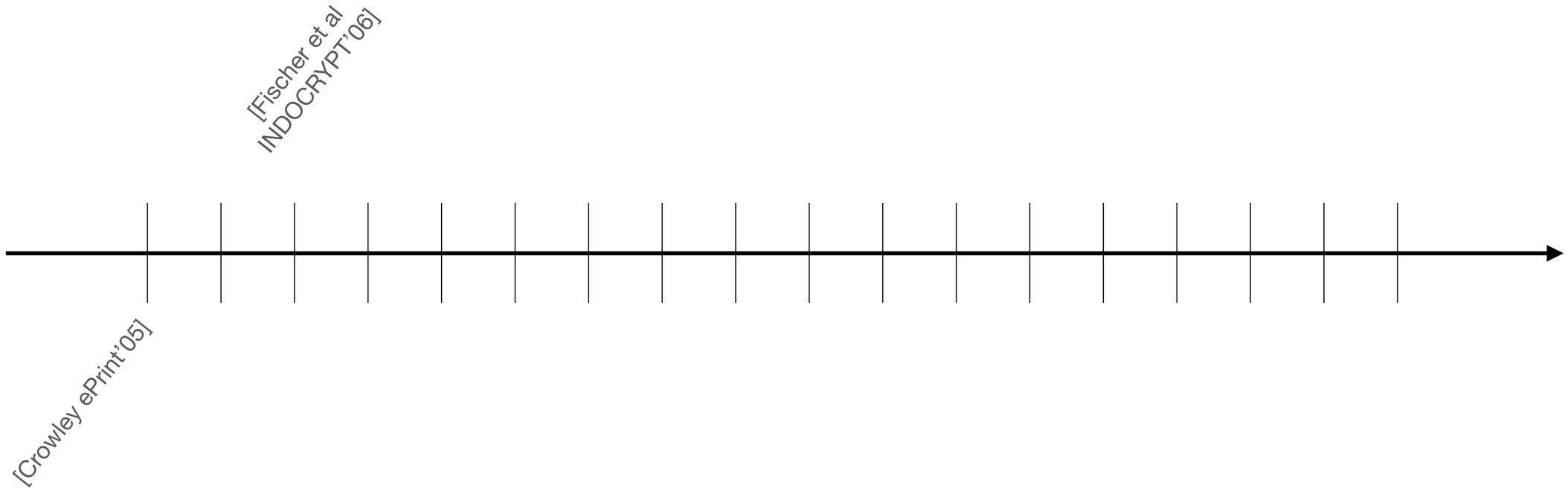
Related Works

Attacking Salsa



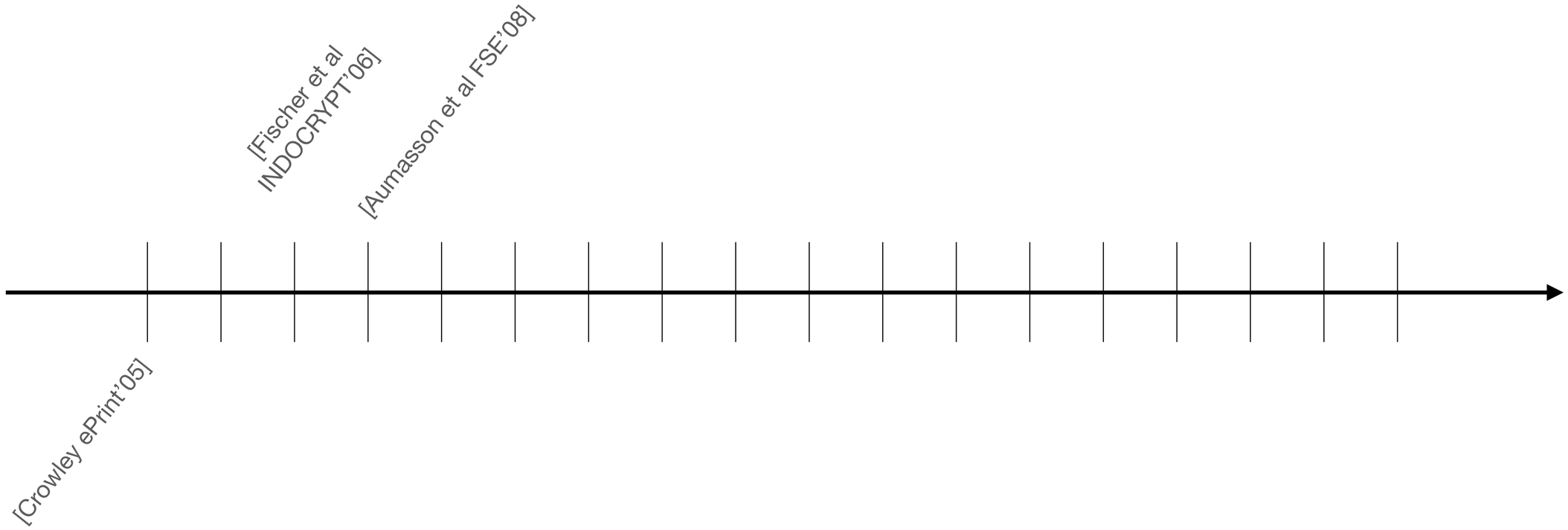
Related Works

Attacking Salsa



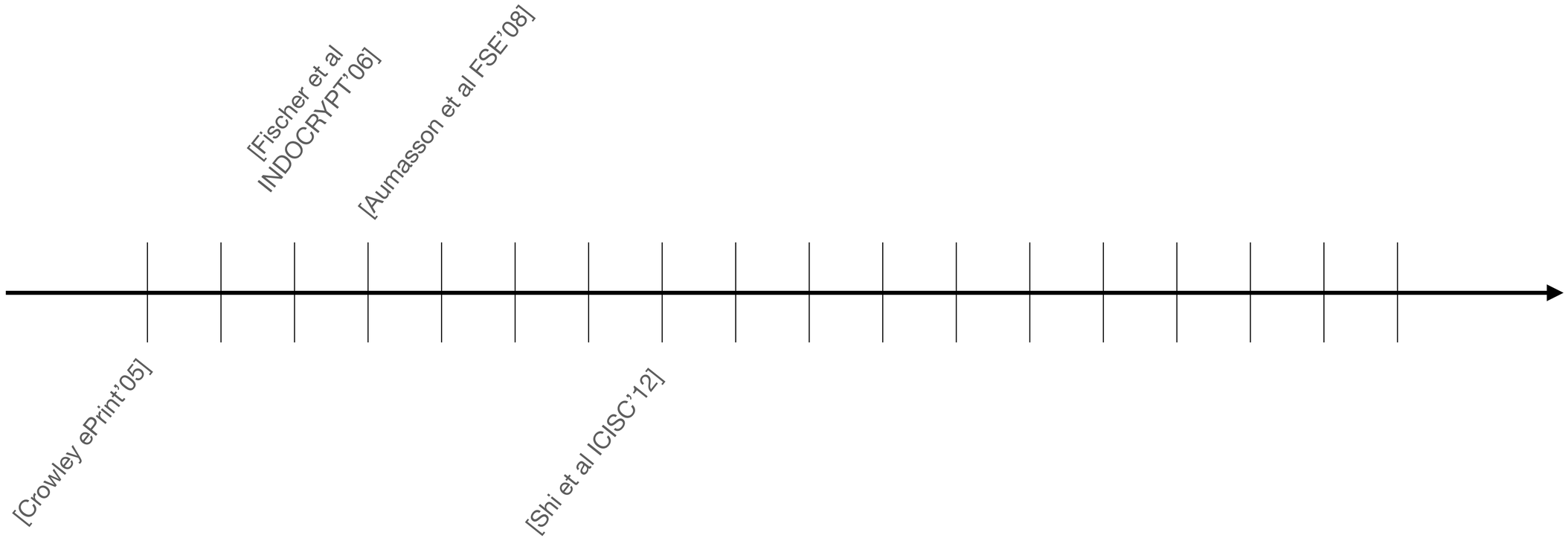
Related Works

Attacking Salsa



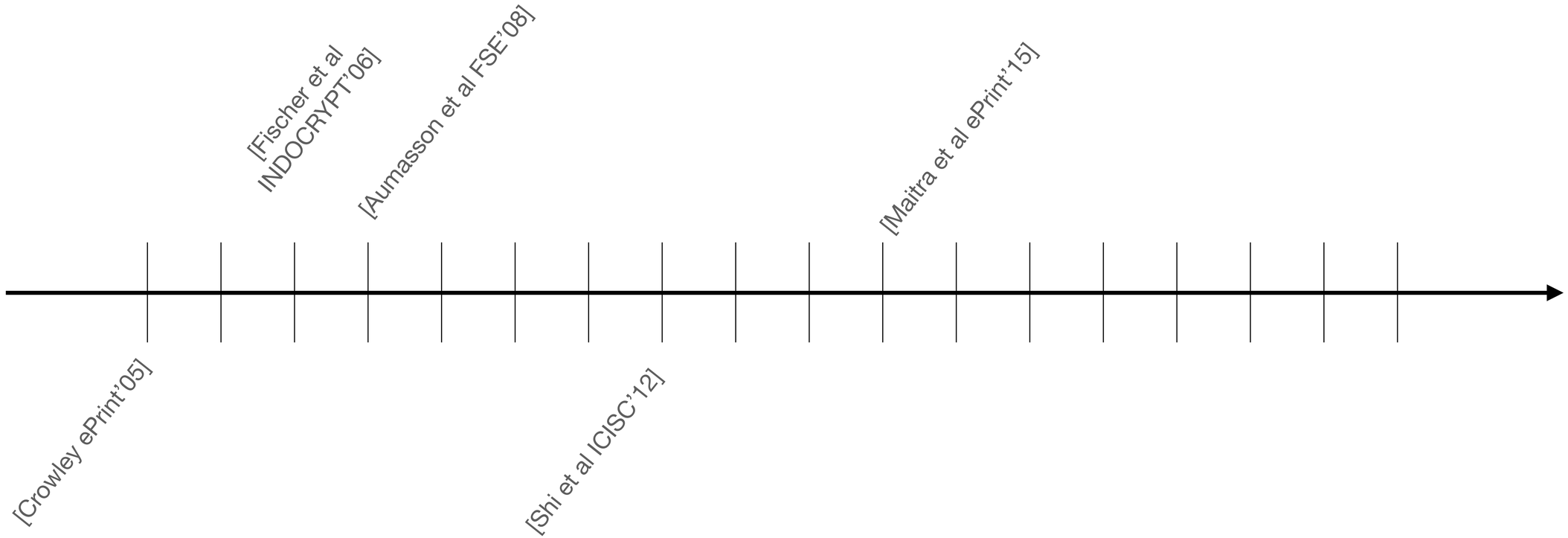
Related Works

Attacking Salsa



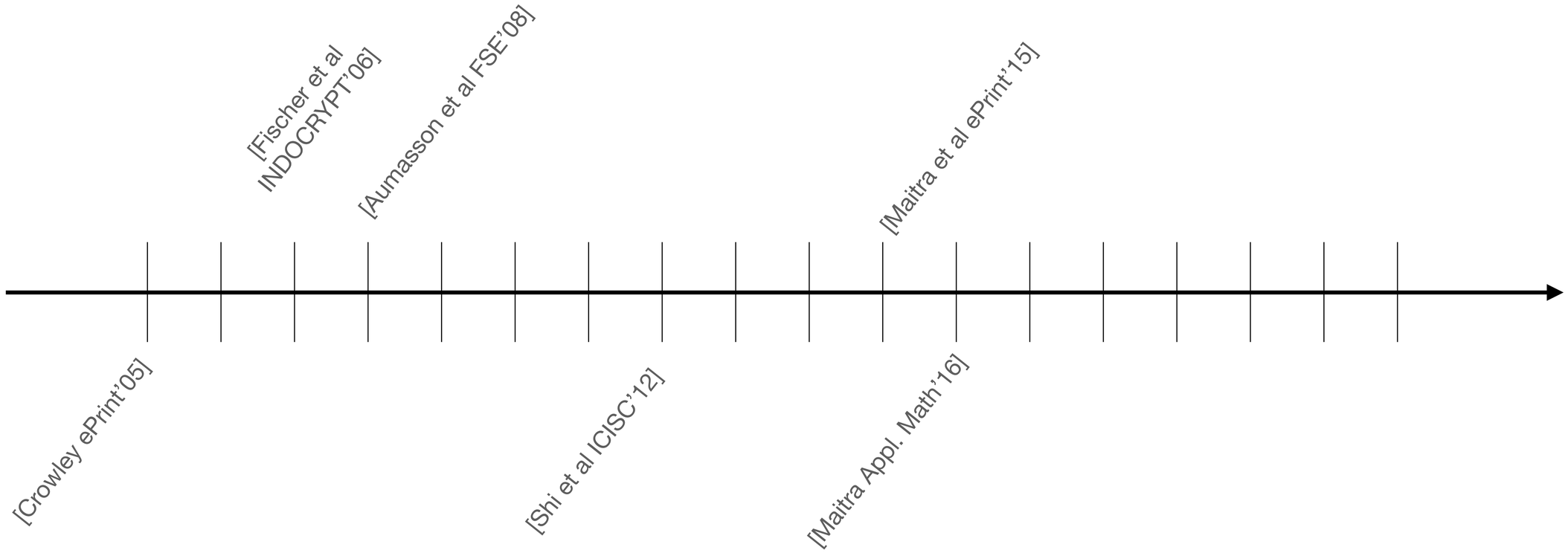
Related Works

Attacking Salsa



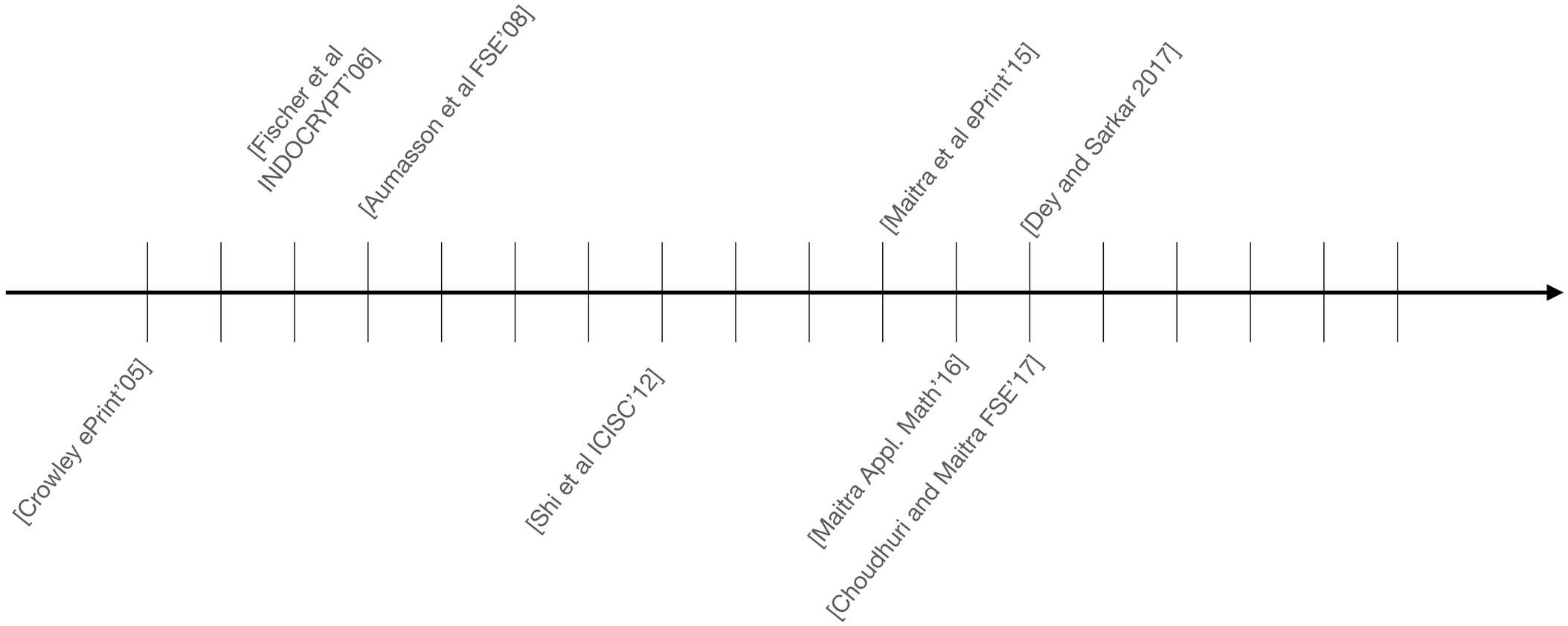
Related Works

Attacking Salsa



Related Works

Attacking Salsa

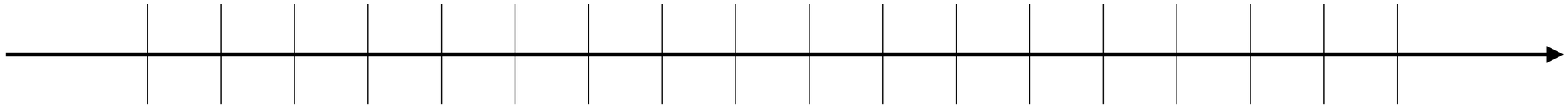


Related Works

Attacking ChaCha

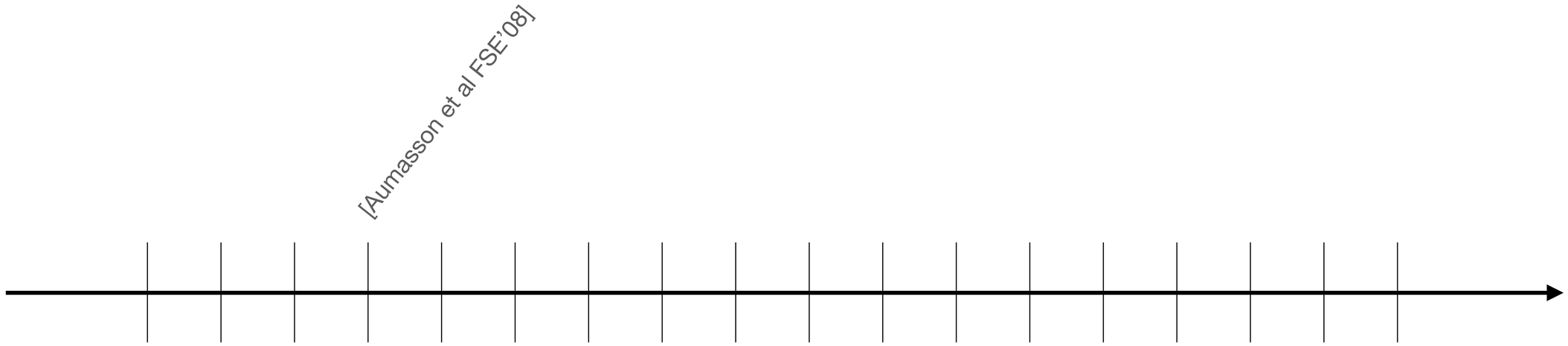
Related Works

Attacking ChaCha



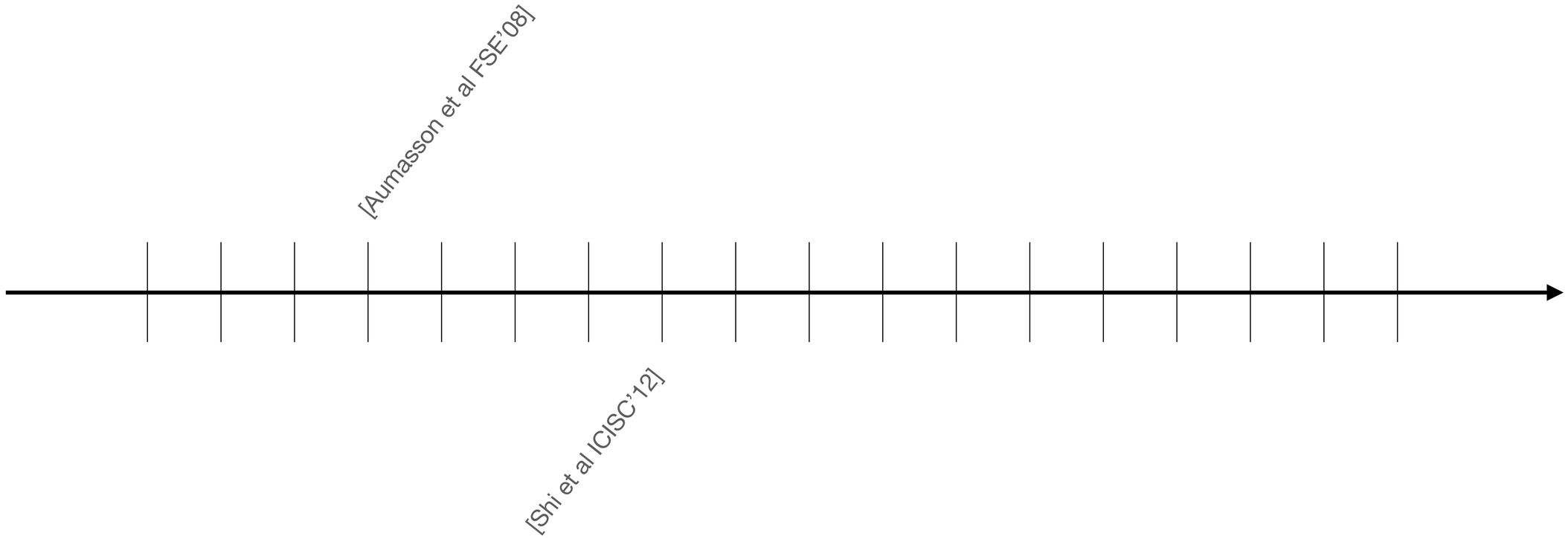
Related Works

Attacking ChaCha



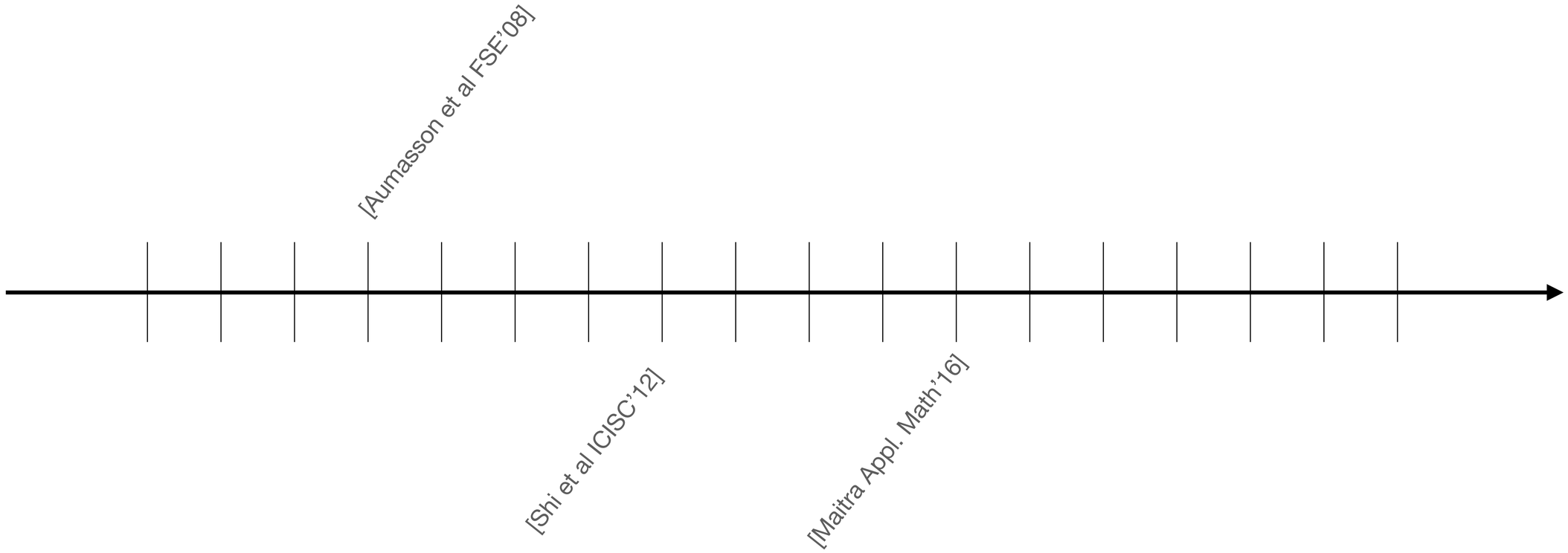
Related Works

Attacking ChaCha



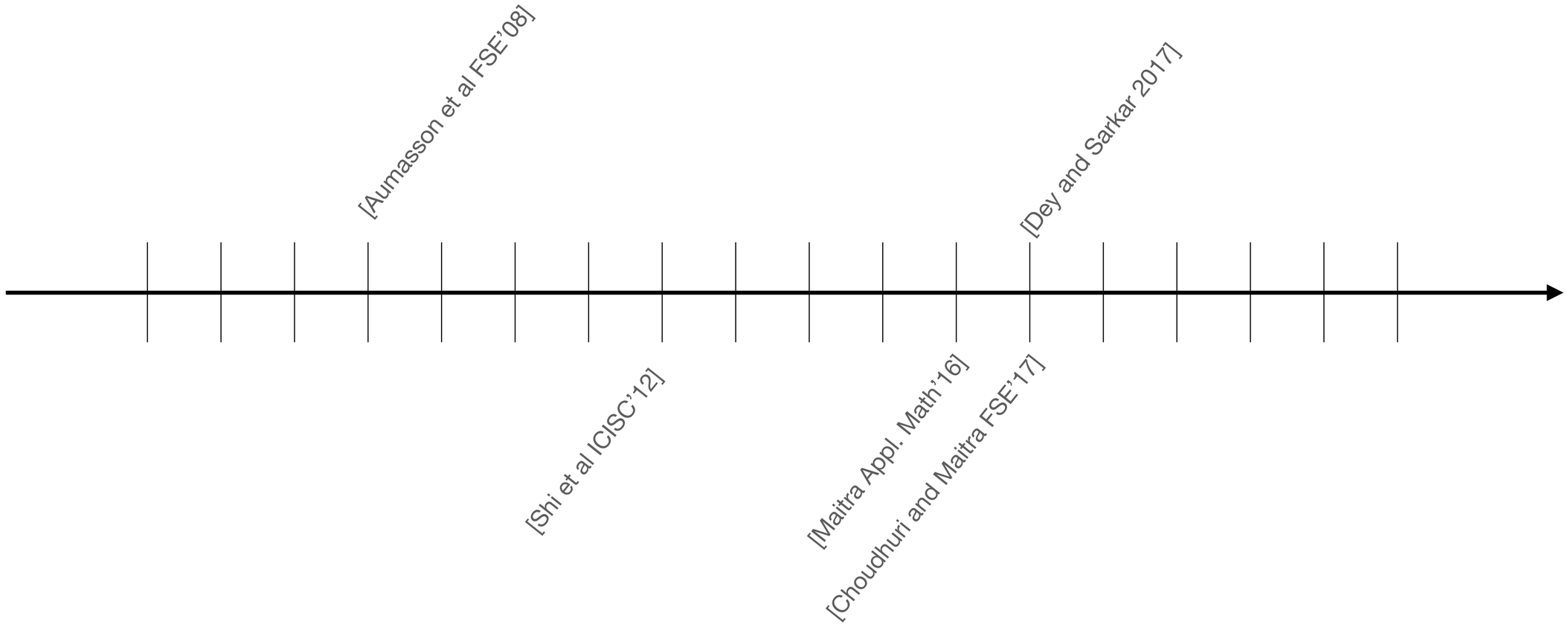
Related Works

Attacking ChaCha



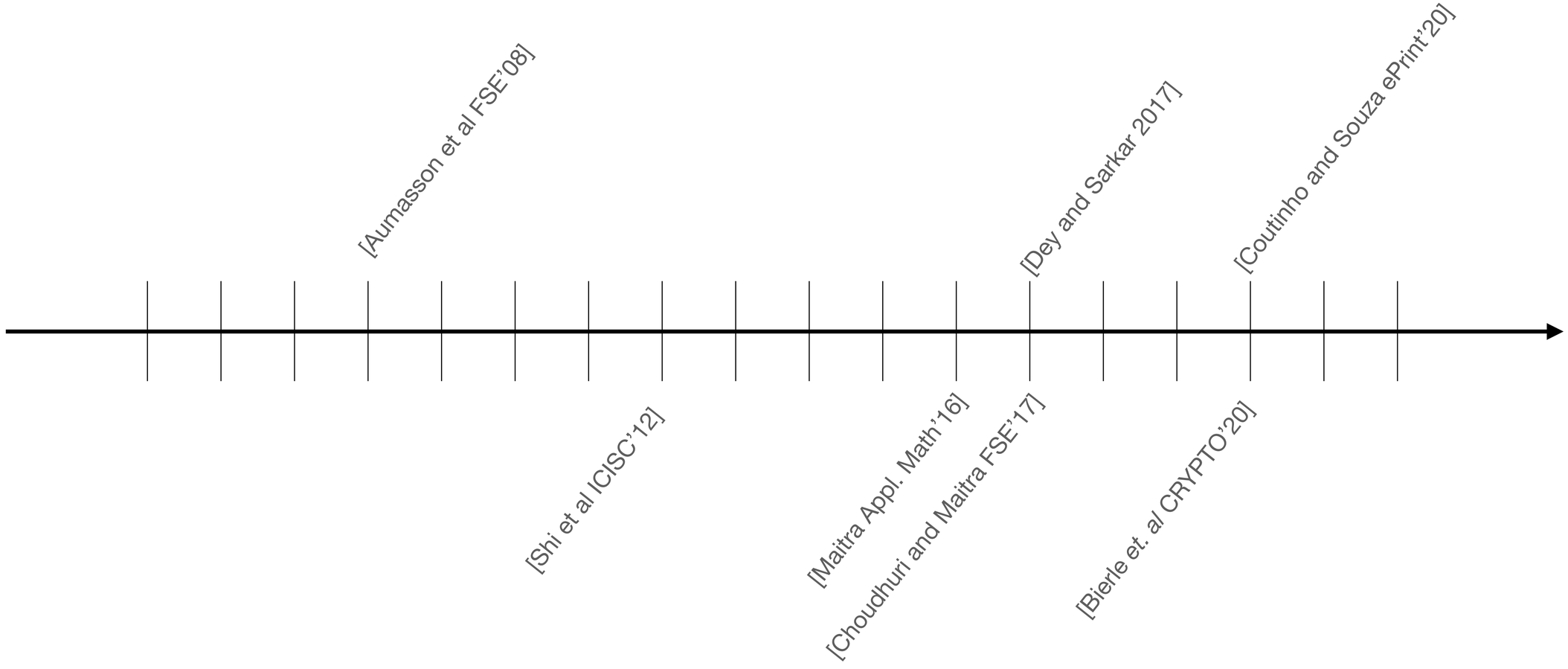
Related Works

Attacking ChaCha



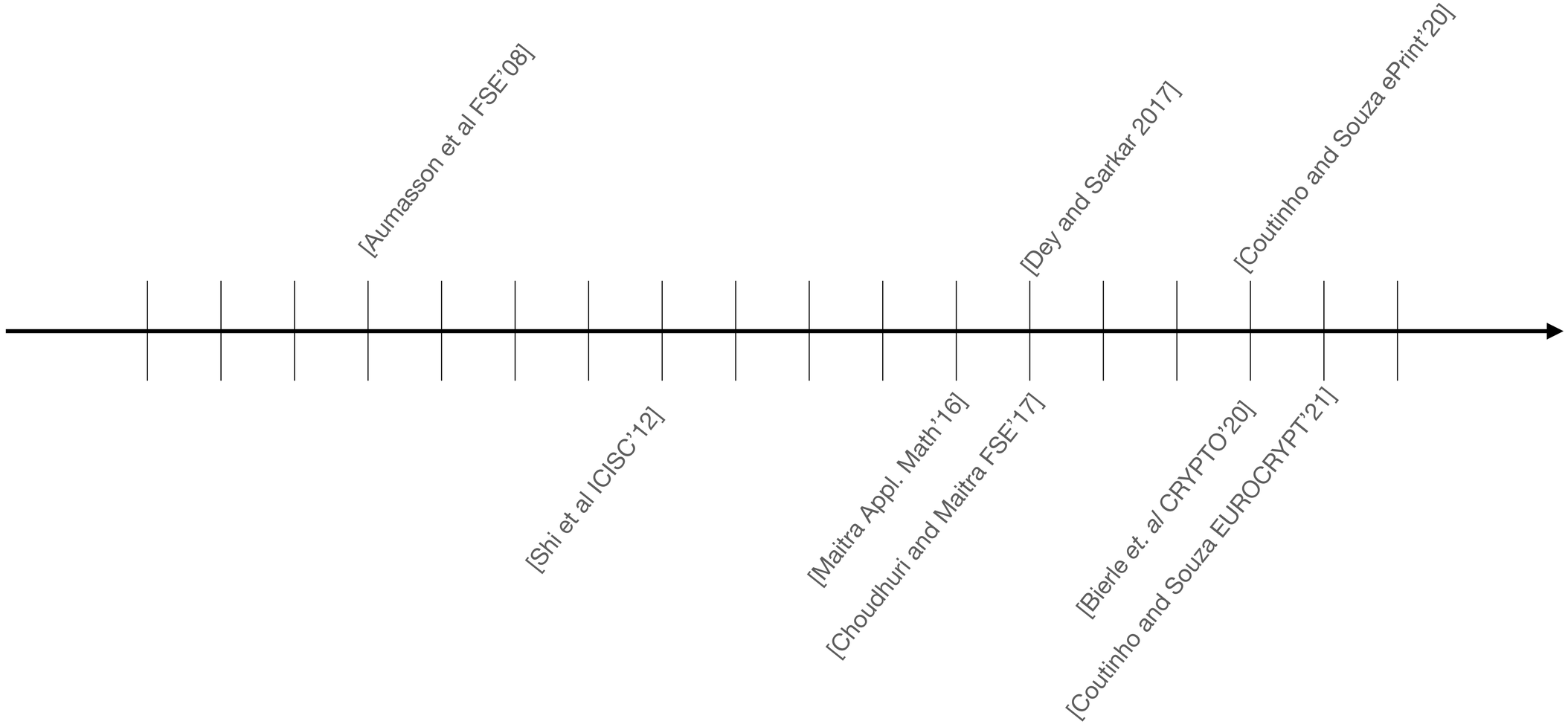
Related Works

Attacking ChaCha



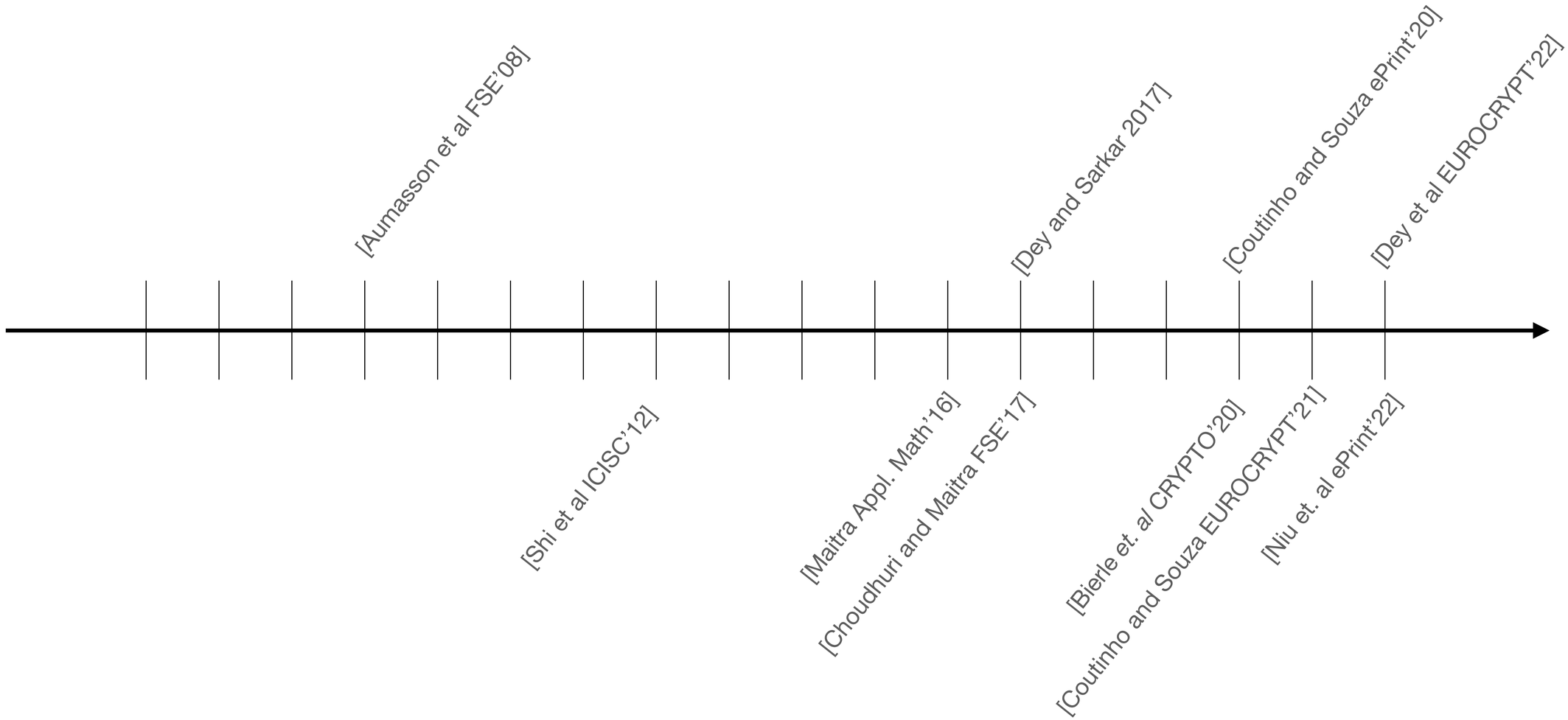
Related Works

Attacking ChaCha



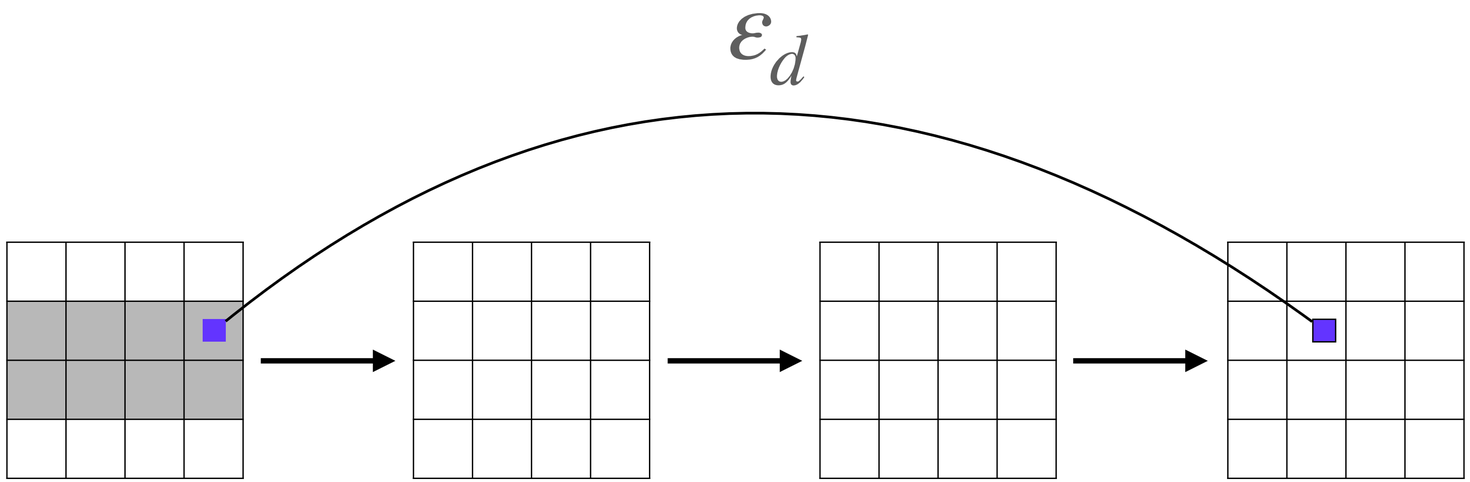
Related Works

Attacking ChaCha



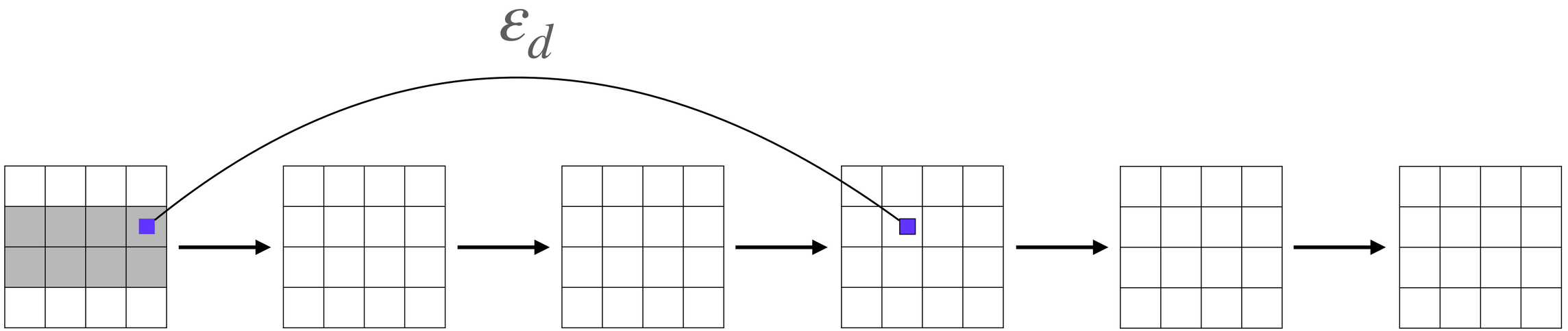
Background

Probabilistic Neutral Bits attack (PNB)



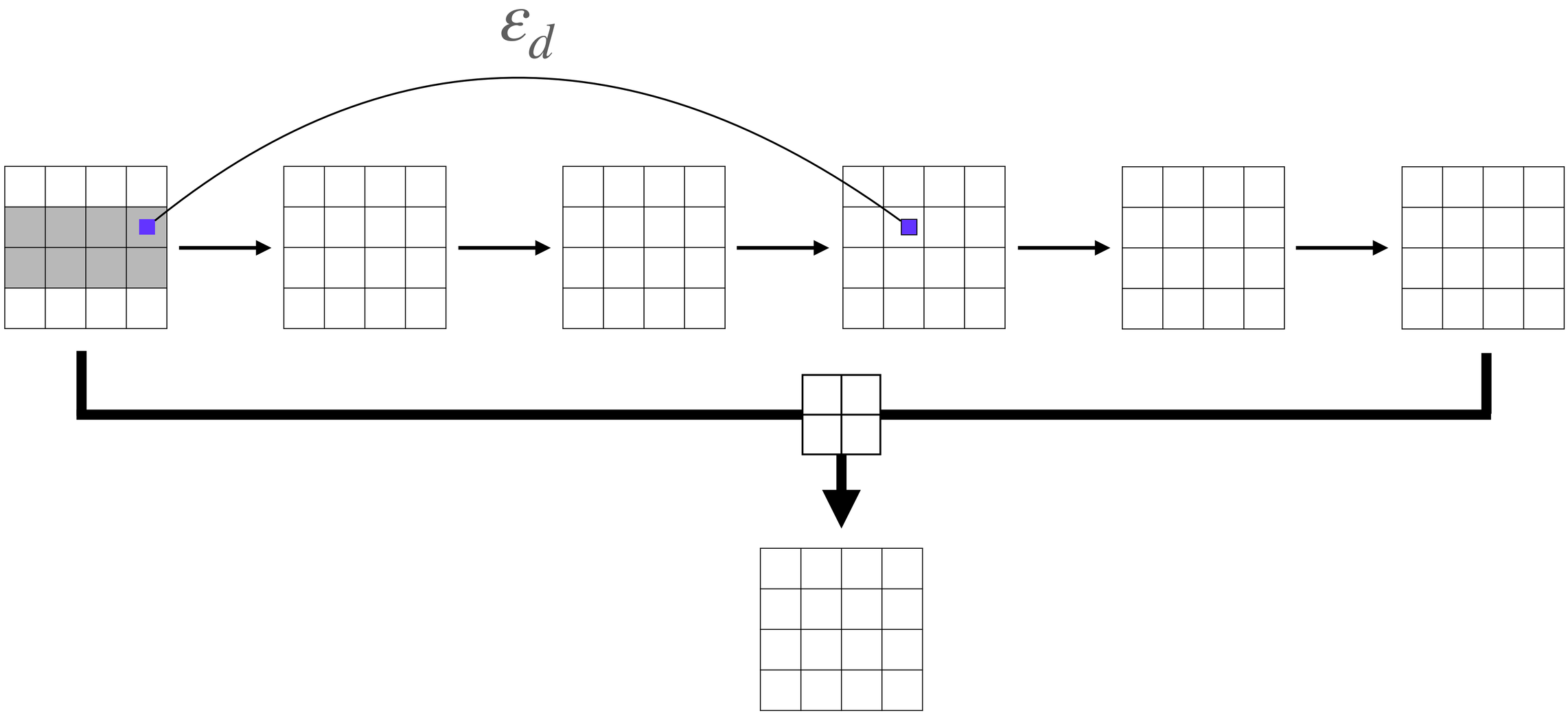
Background

Probabilistic Neutral Bits attack (PNB)



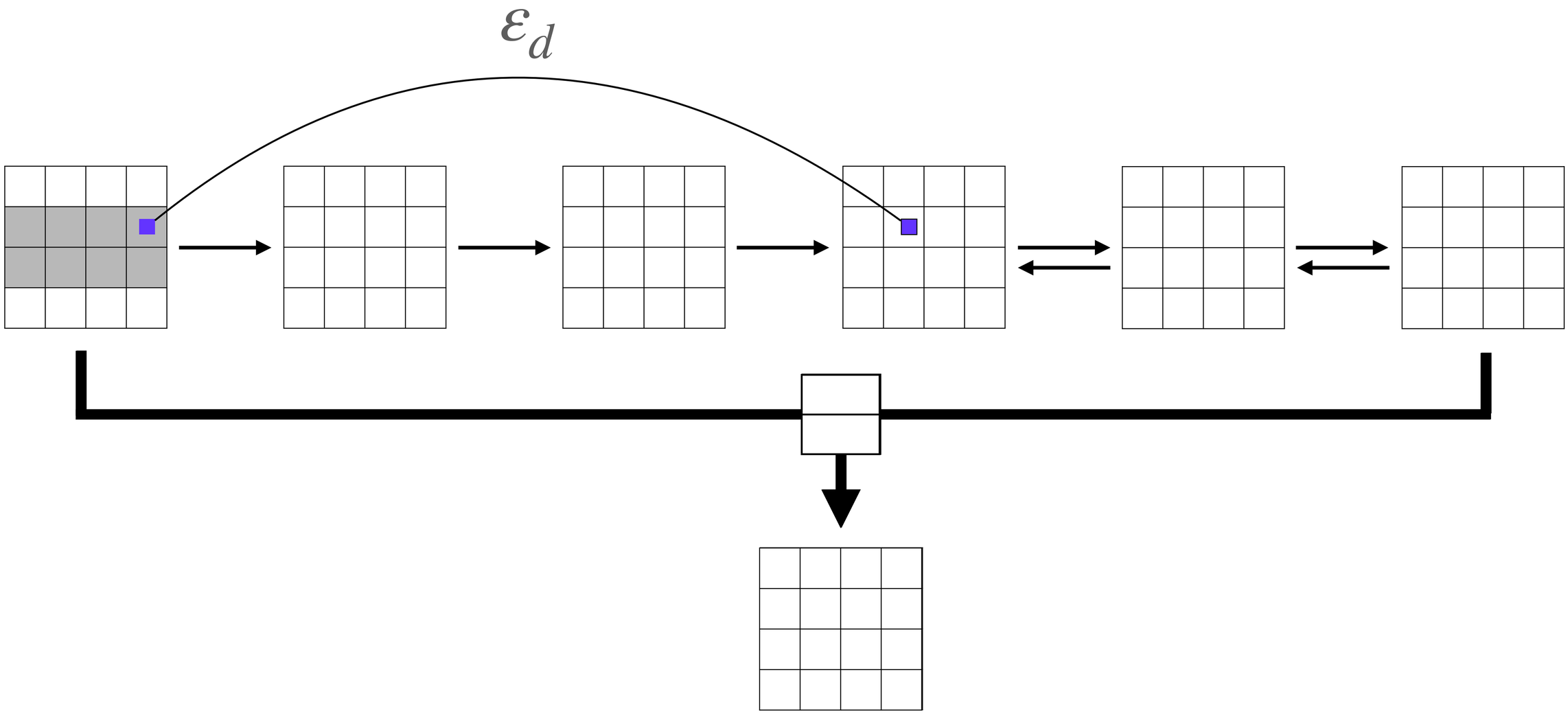
Background

Probabilistic Neutral Bits attack (PNB)



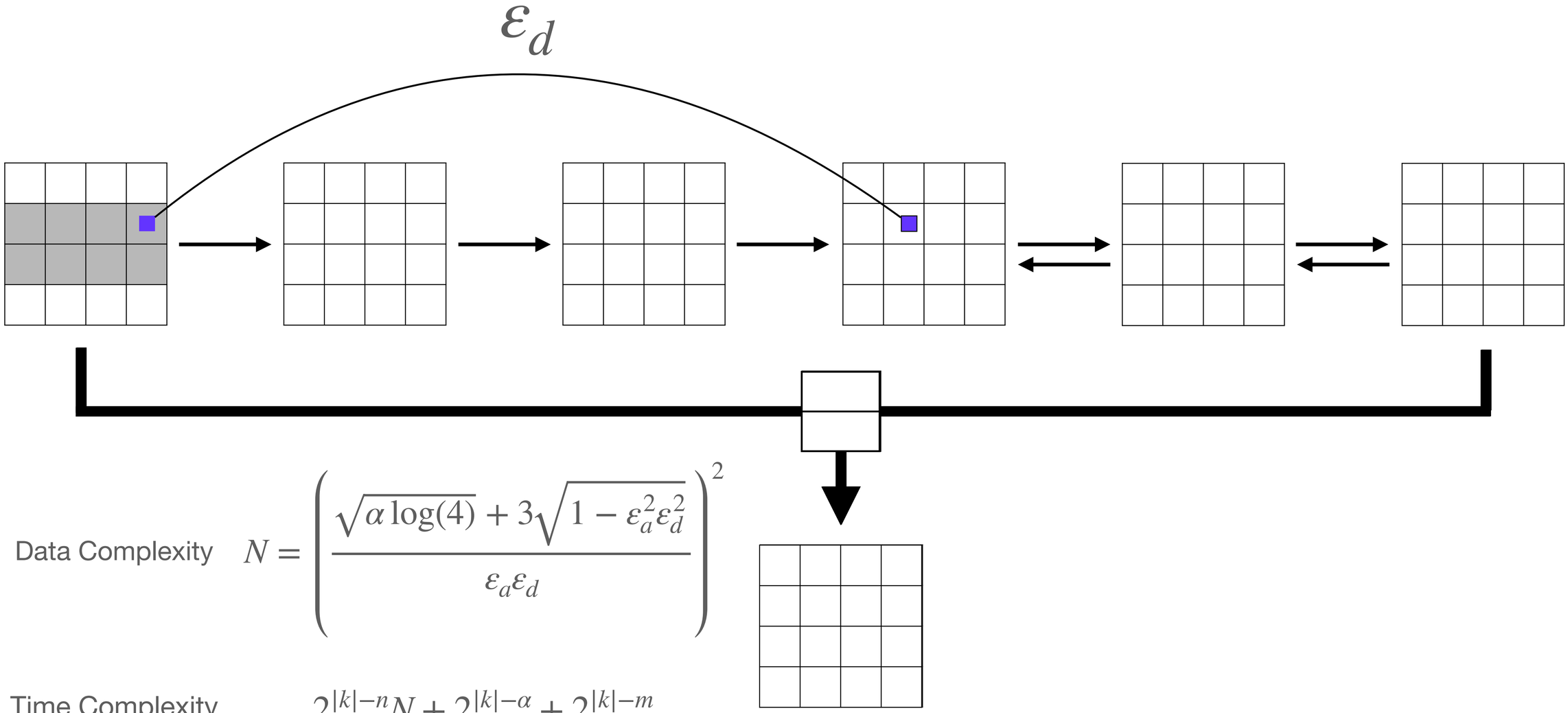
Background

Probabilistic Neutral Bits attack (PNB)



Background

Probabilistic Neutral Bits attack (PNB)

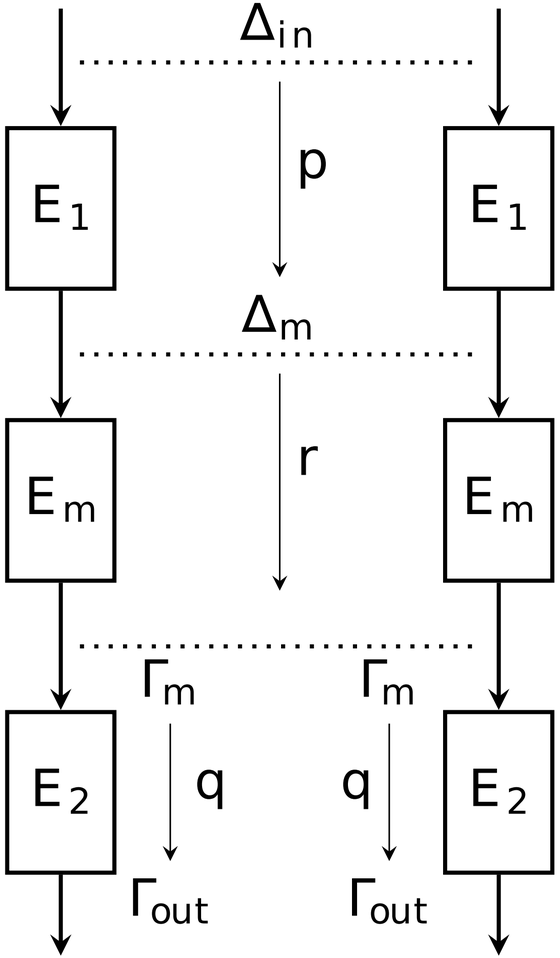


Data Complexity $N = \left(\frac{\sqrt{\alpha \log(4)} + 3\sqrt{1 - \varepsilon_a^2 \varepsilon_d^2}}{\varepsilon_a \varepsilon_d} \right)^2$

Time Complexity $2^{|k|-n}N + 2^{|k|-\alpha} + 2^{|k|-m}$

Background

Differential-Linear Attack

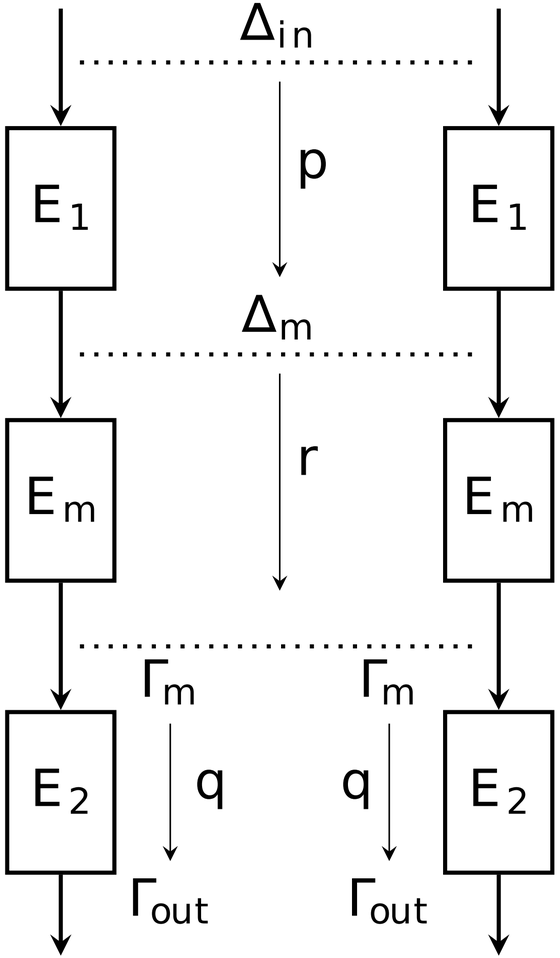


Correlation

$$prq^2$$

Background

Differential-Linear Attack



Correlation

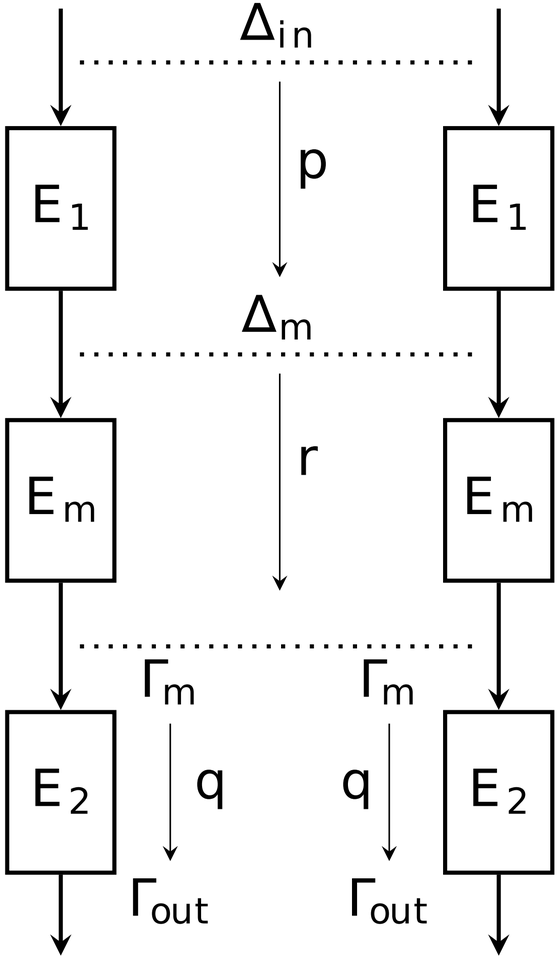
$$prq^2$$

Complexity

$$O\left(\frac{1}{p^2r^2q^4}\right)$$

Background

Differential-Linear Attack



Correlation

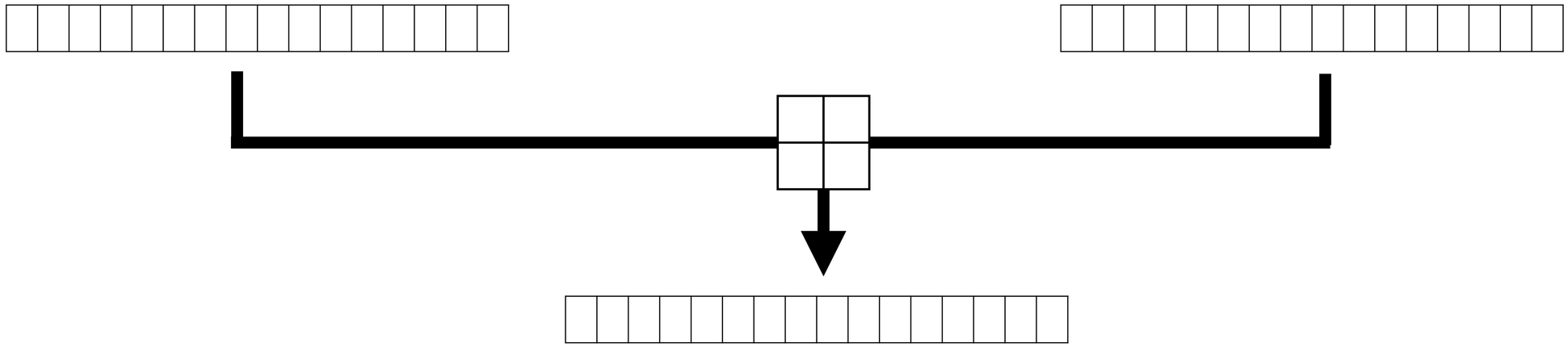
$$prq^2$$

Complexity

$$O\left(\frac{1}{p^2r^2q^4}\right)$$

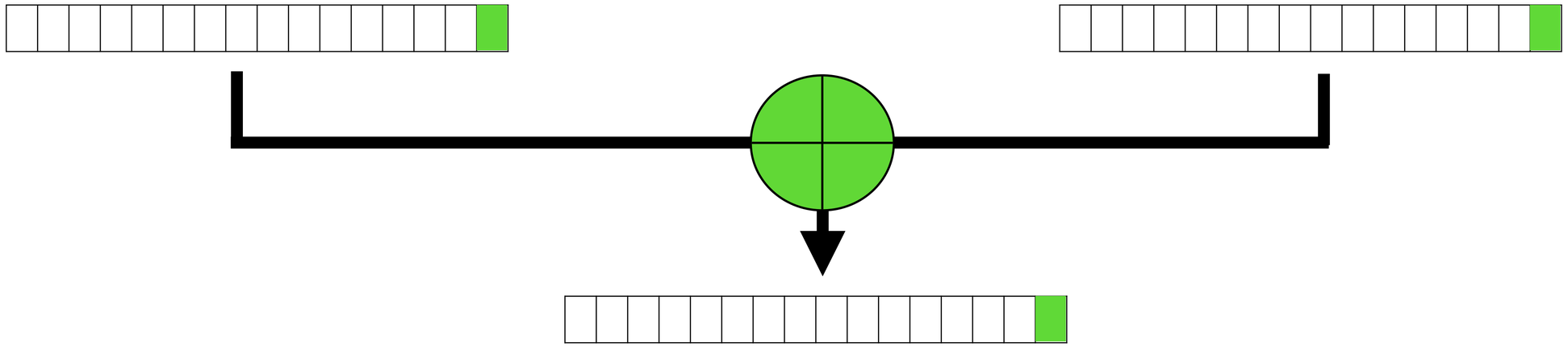
Background

Linear Approximations of Modular Addition



Background

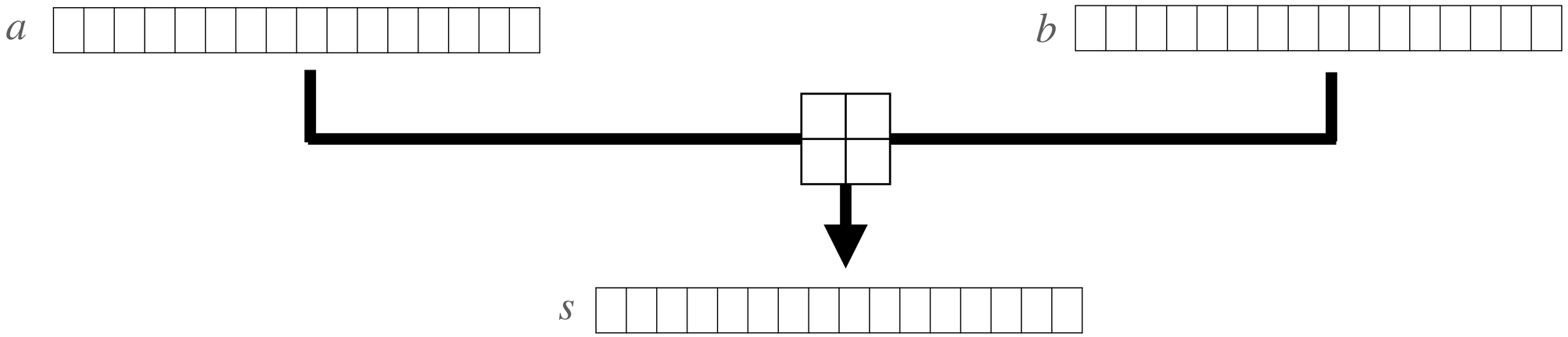
Linear Approximations of Modular Addition



$$s_0 = a_0 \oplus b_0$$

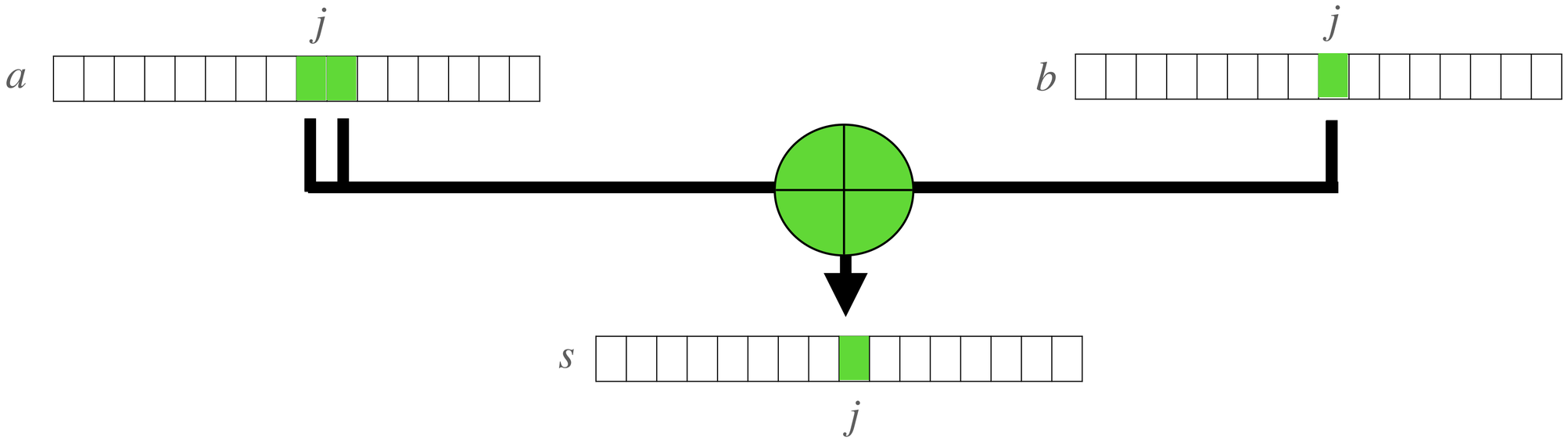
Background

Linear Approximations of Modular Addition



Background

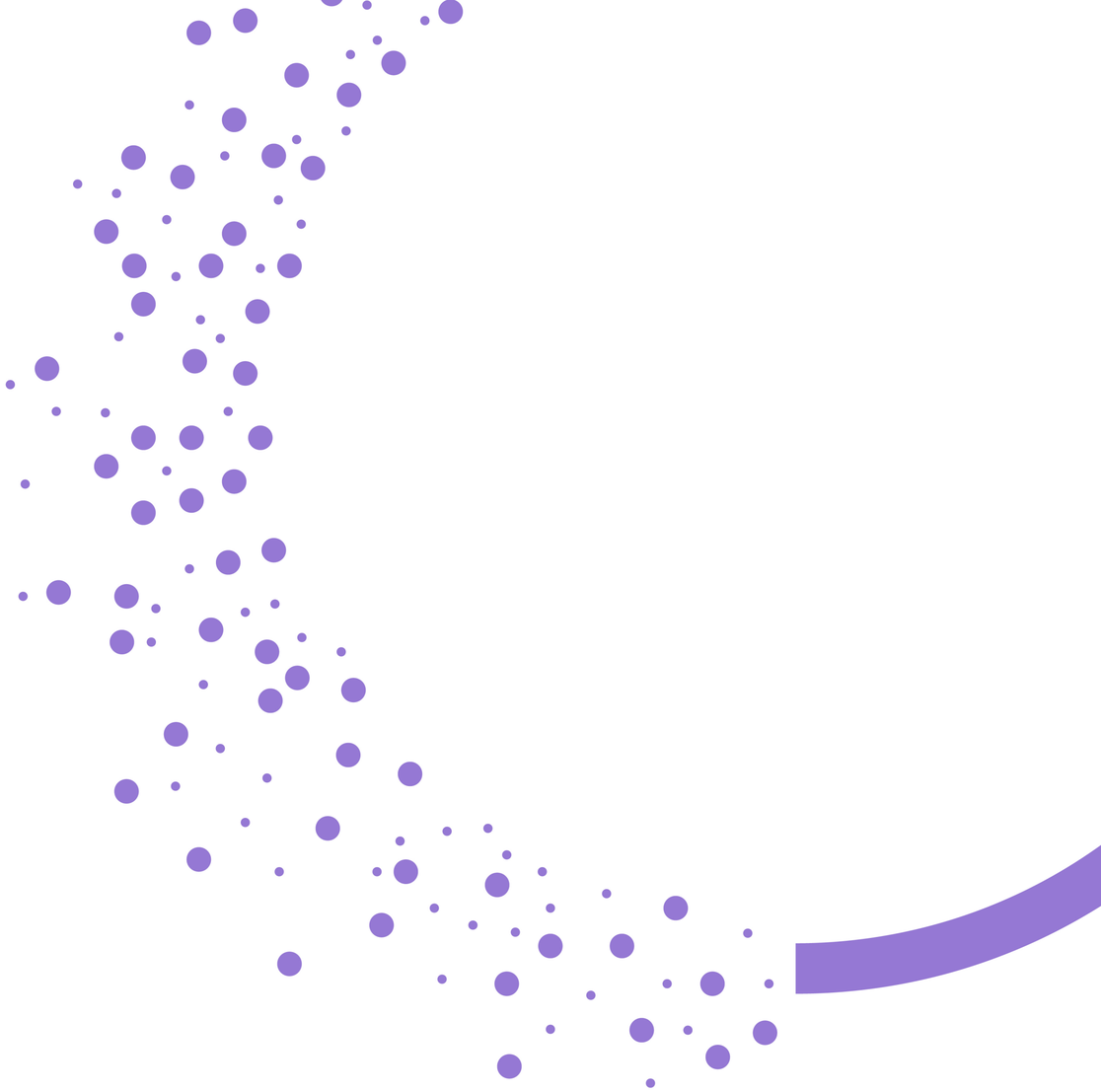
Linear Approximations of Modular Addition



$$s_j = a_j \oplus b_j \oplus a_{j-1} \text{ w.p. } \frac{3}{4}$$

Technology Innovation Institute

Our contributions
Cryptanalysis



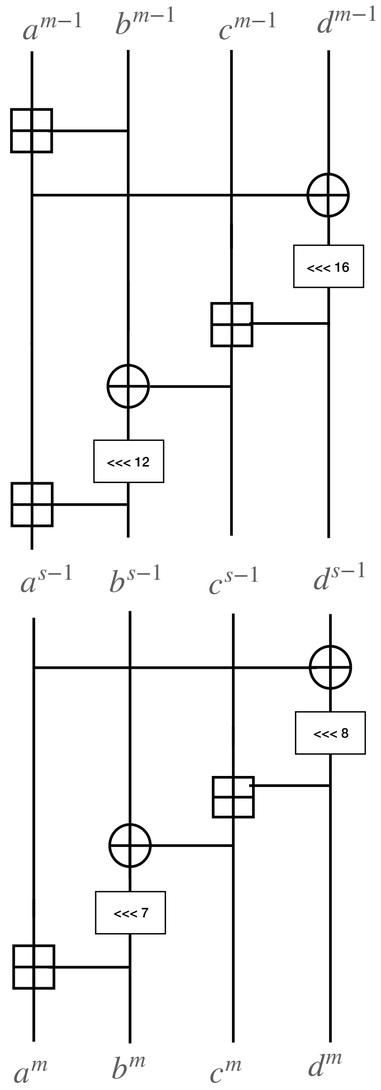
Cryptography Research Center

tii.ae

New Linear Approximations for ChaCha

Reducing the number of rules

- [Choudhuri and Maitra FSE'17]
  - 8 rules
- [Coutinho et al EUROCRYPT'21]
  - 18 rules
- This work
  - 3 rules

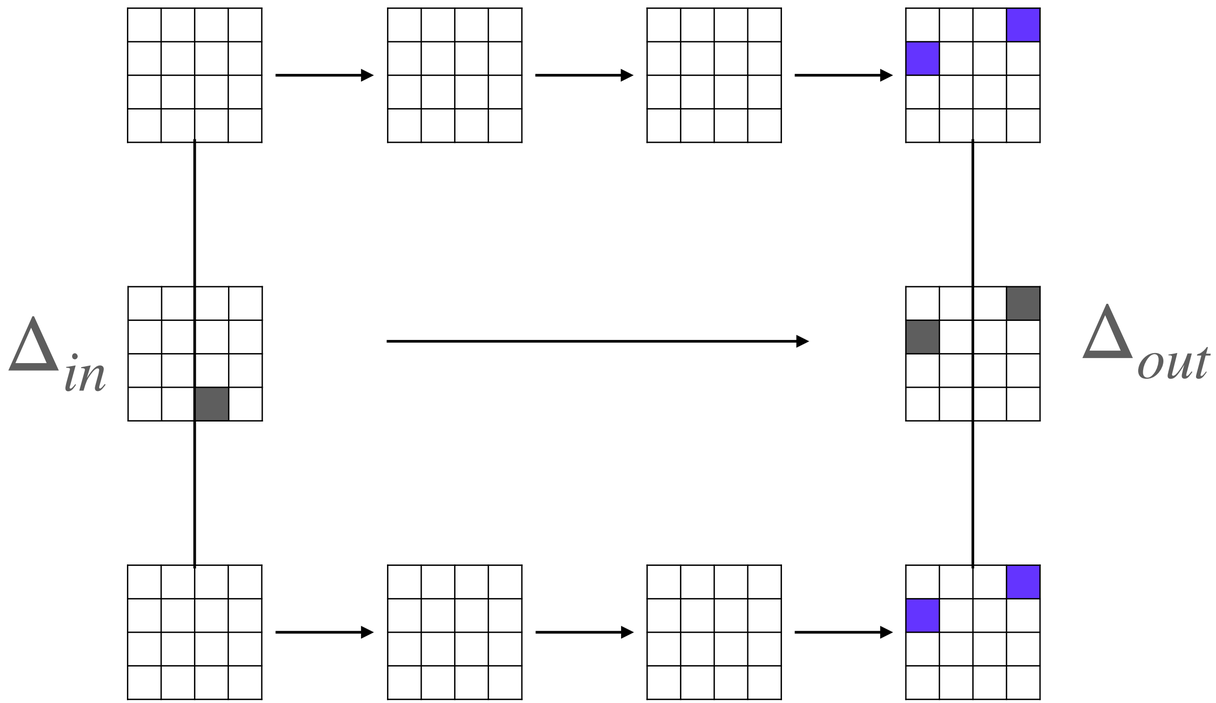


Attacking 7 rounds ChaCha

Differential-Linear distinguisher ChaCha

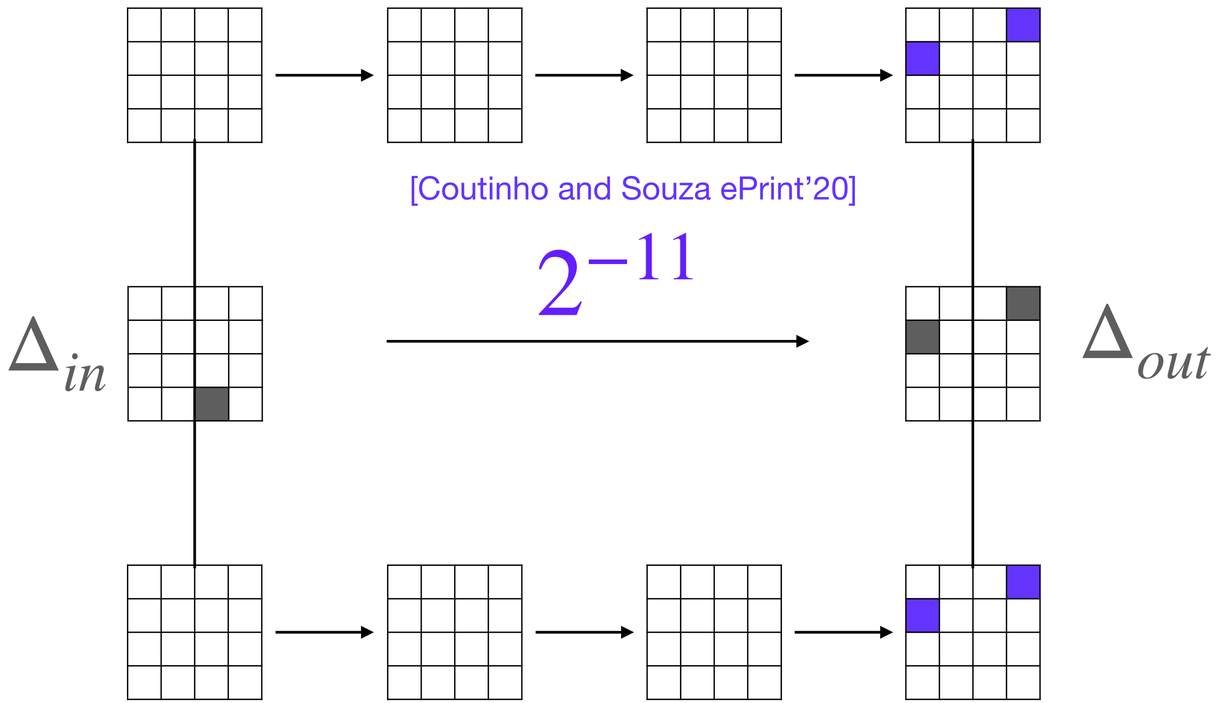
Attacking 7 rounds ChaCha

Differential-Linear distinguisher ChaCha



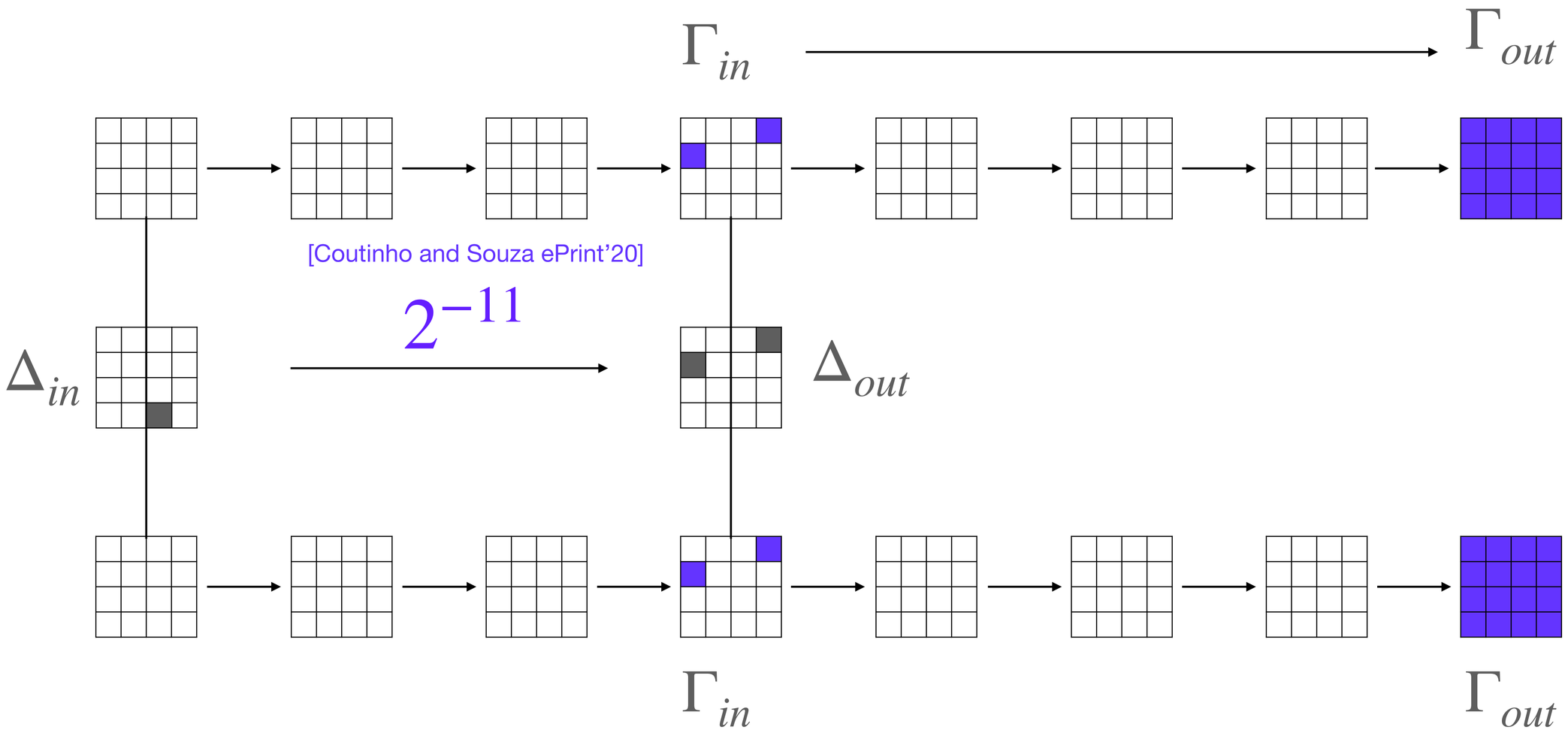
Attacking 7 rounds ChaCha

Differential-Linear distinguisher ChaCha



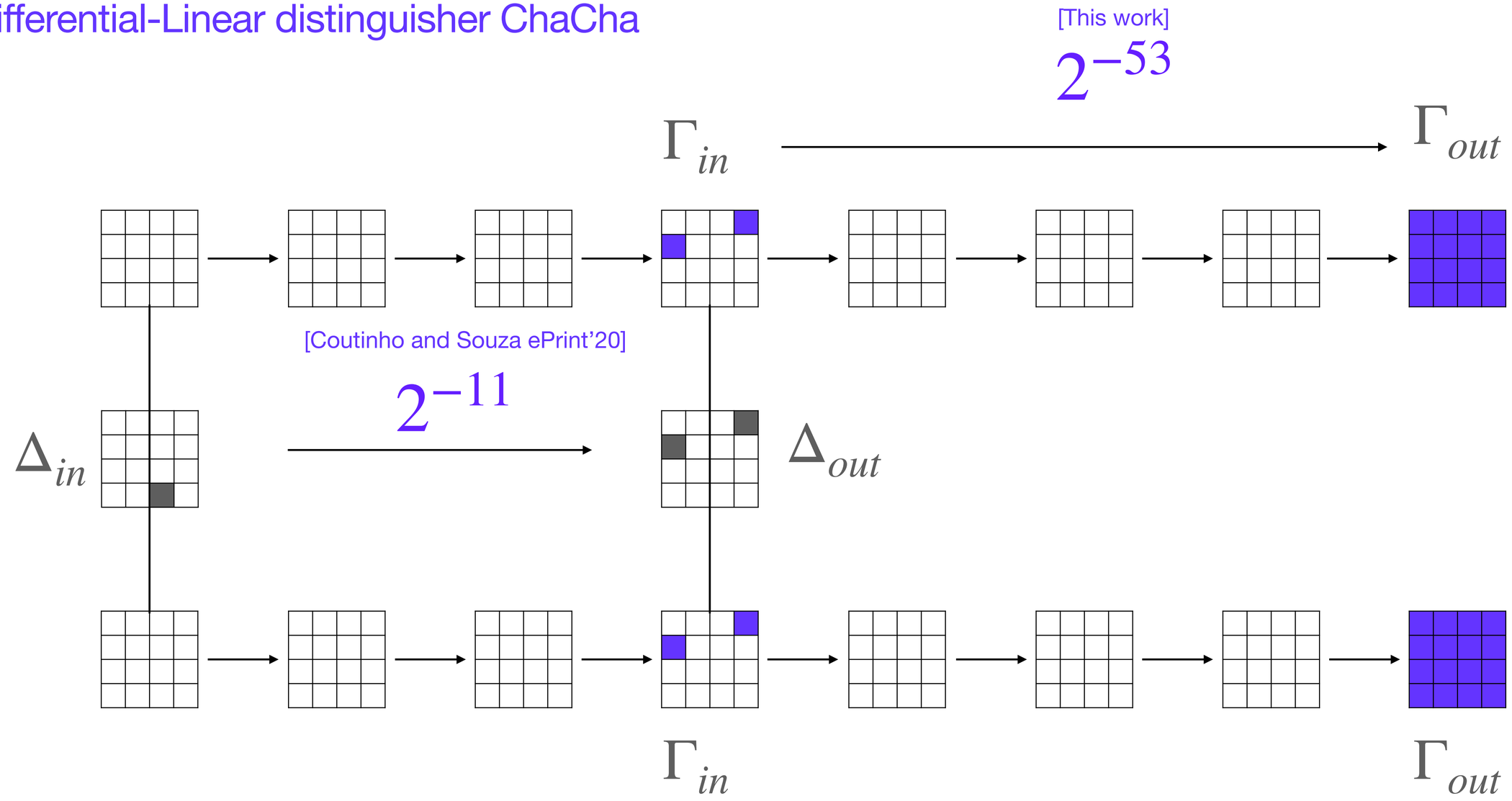
Attacking 7 rounds ChaCha

Differential-Linear distinguisher ChaCha



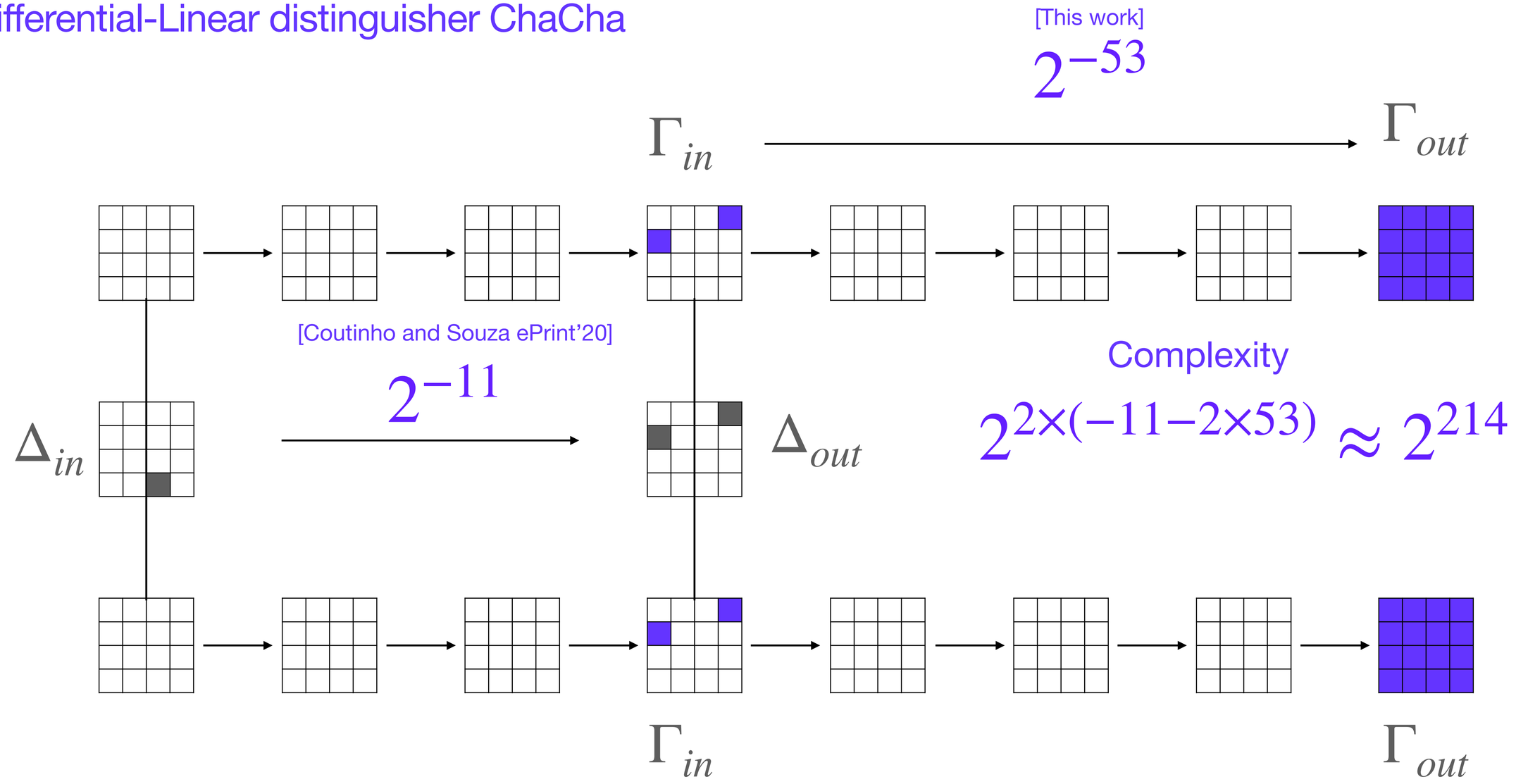
Attacking 7 rounds ChaCha

Differential-Linear distinguisher ChaCha



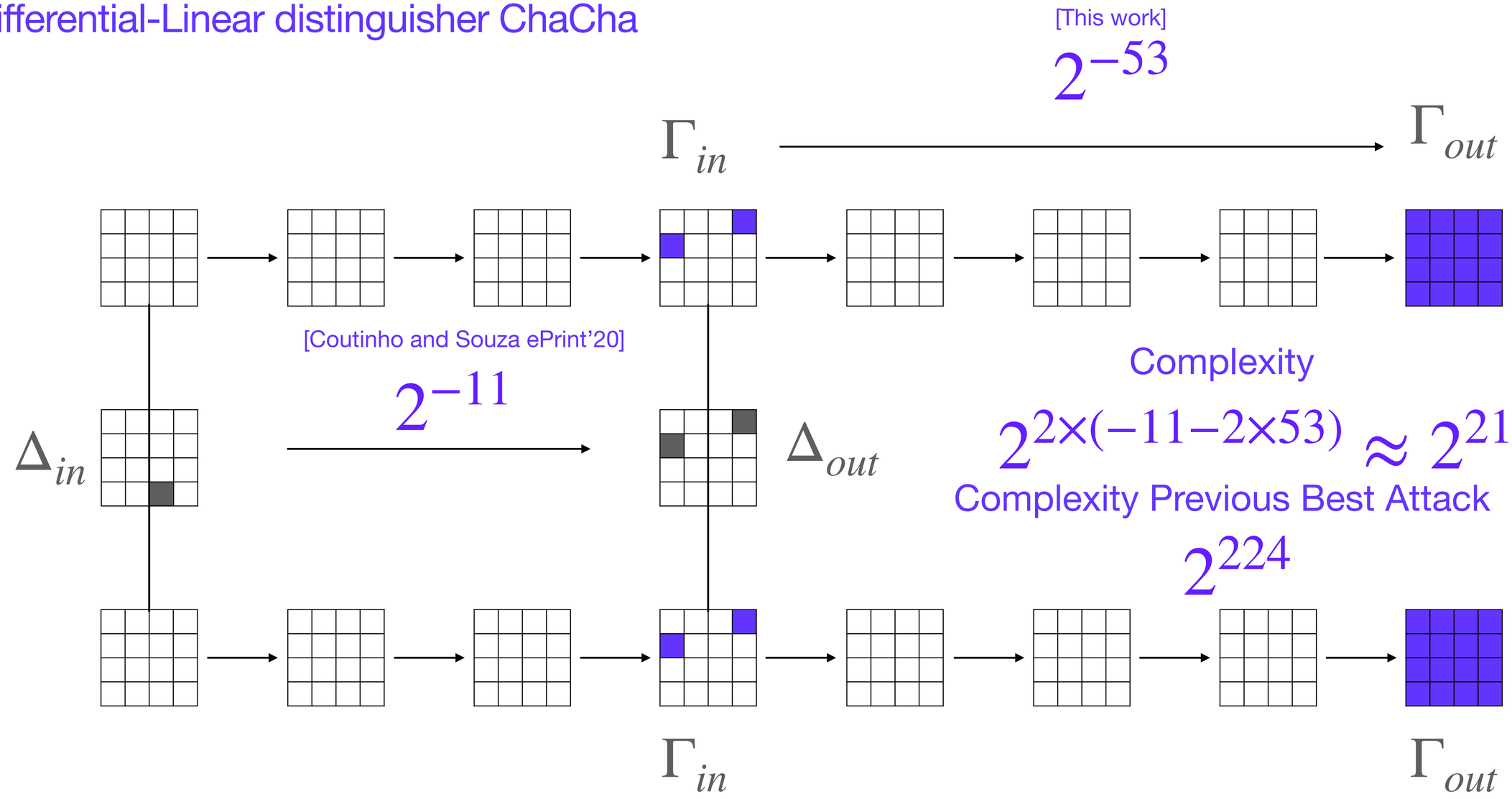
Attacking 7 rounds ChaCha

Differential-Linear distinguisher ChaCha



Attacking 7 rounds ChaCha

Differential-Linear distinguisher ChaCha



Complexity

$2^{2\times(-11-2\times53)} \approx 2^{214}$

Complexity Previous Best Attack

2^{224}

Attacking 8 rounds of Salsa

Bidirectional Linear Expansion (BLE)

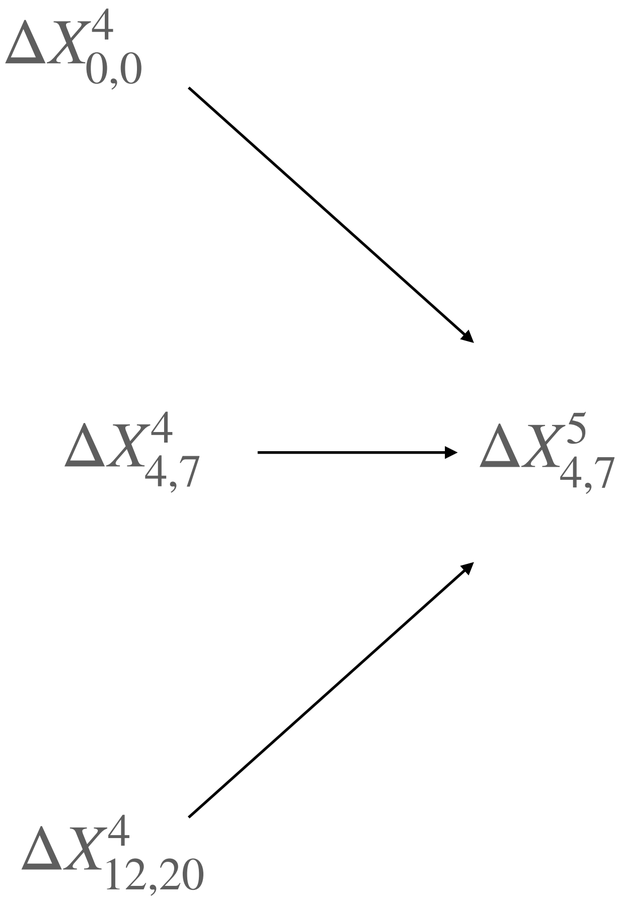
Attacking 8 rounds of Salsa

Bidirectional Linear Expansion (BLE)

$$\Delta X^5_{4,7}$$

Attacking 8 rounds of Salsa

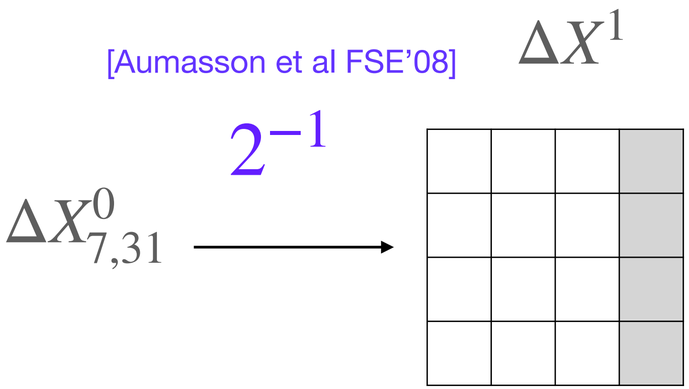
Bidirectional Linear Expansion (BLE)

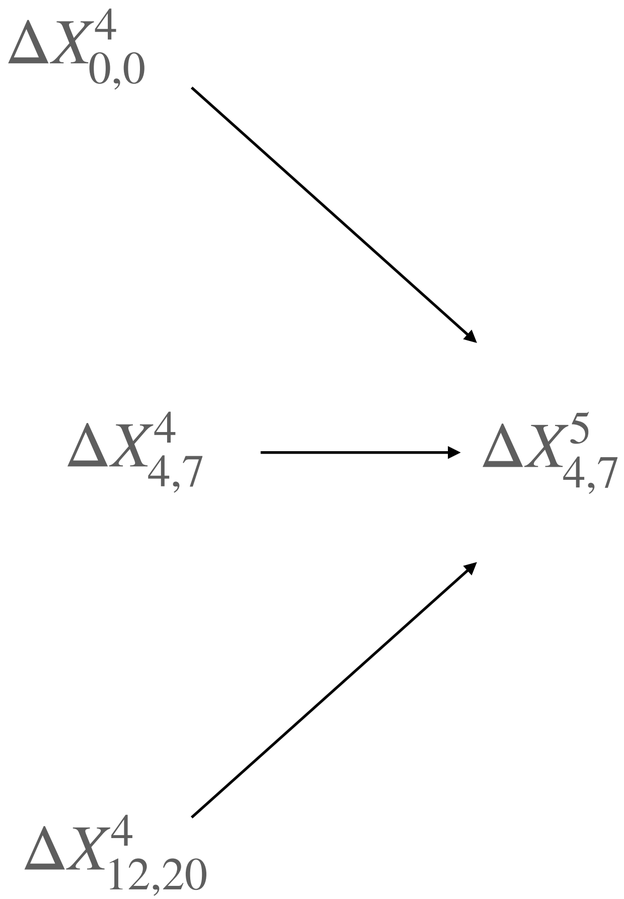


Attacking 8 rounds of Salsa

Bidirectional Linear Expansion (BLE)

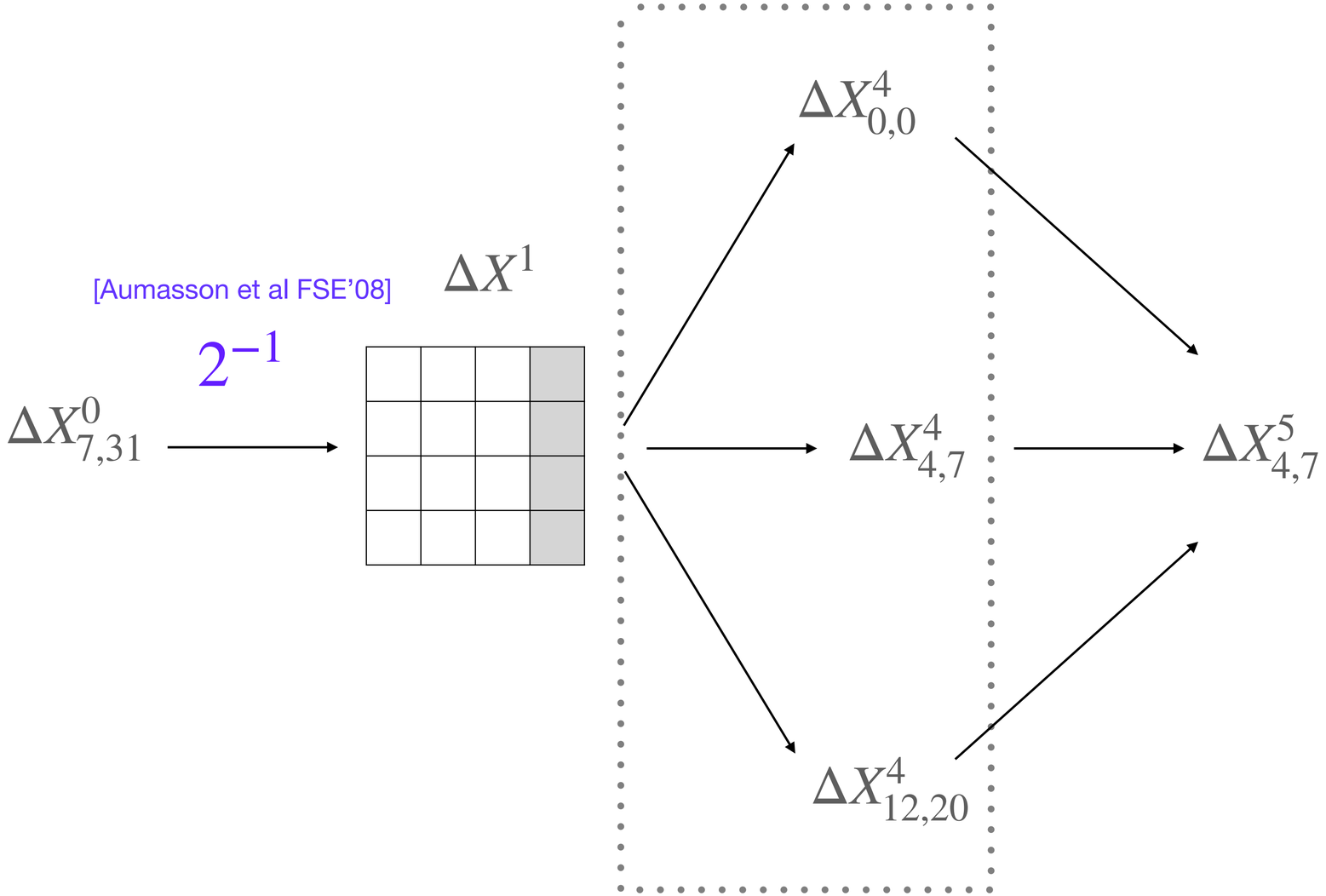
[Aumasson et al FSE'08]





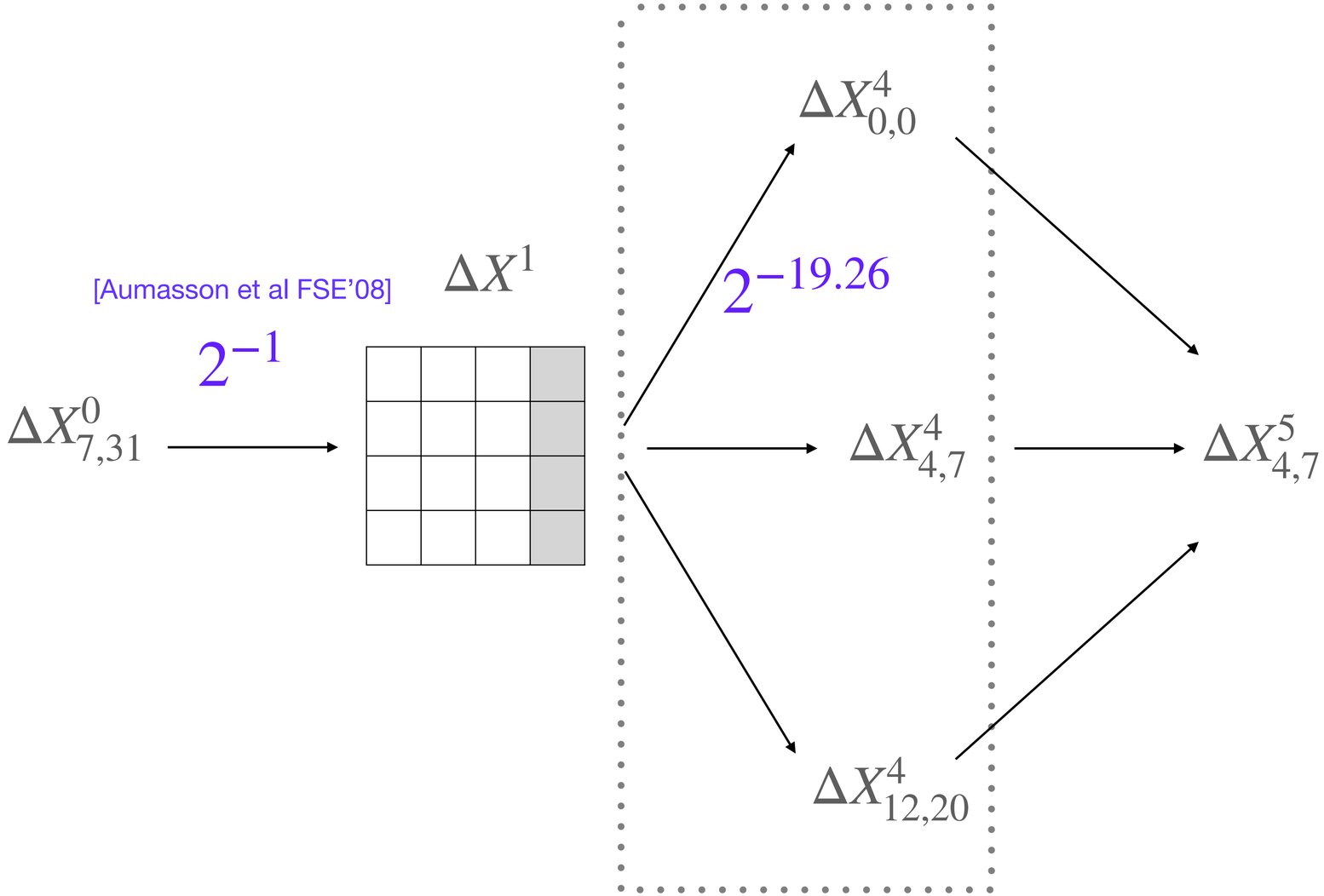
Attacking 8 rounds of Salsa

Bidirectional Linear Expansion (BLE)



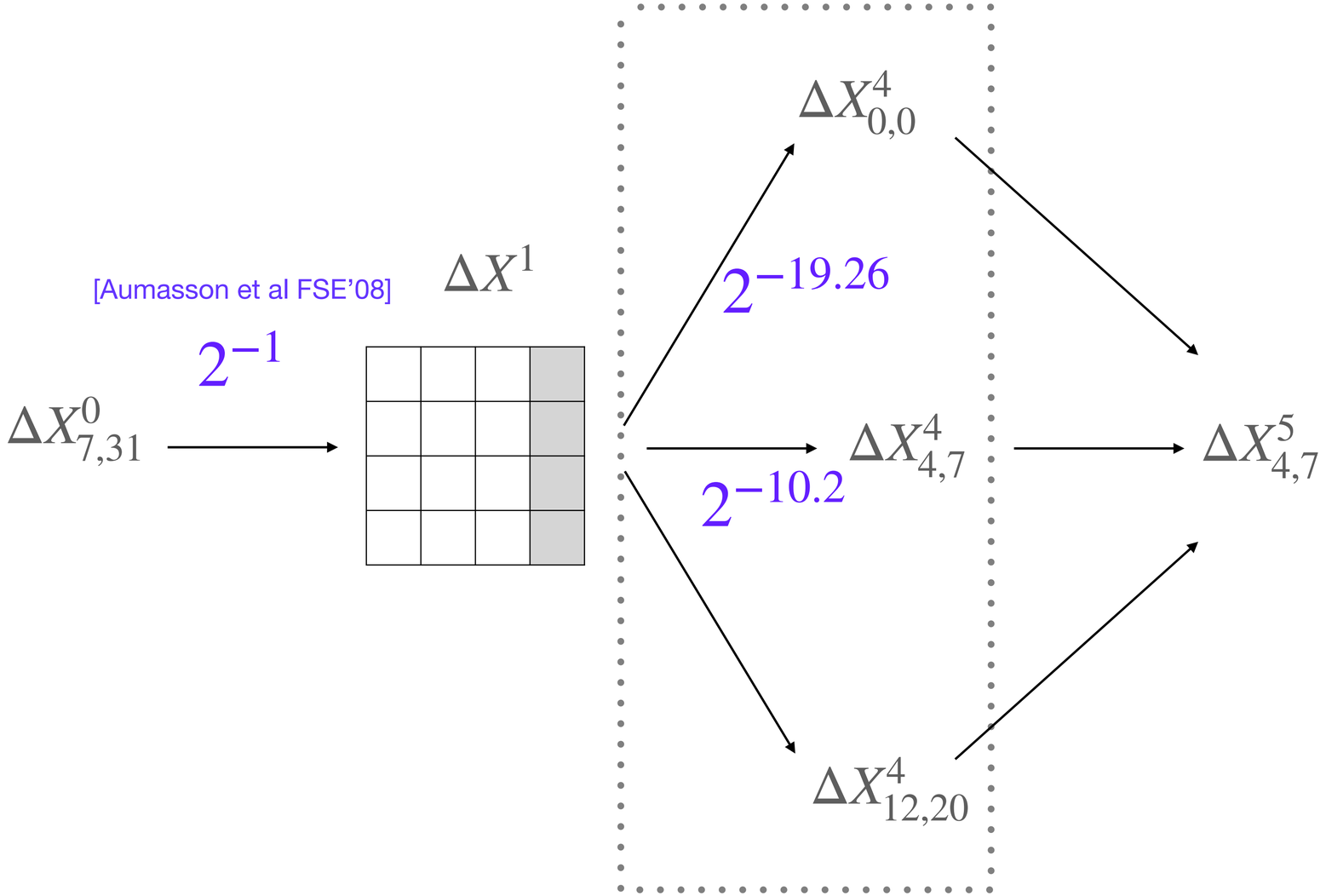
Attacking 8 rounds of Salsa

Bidirectional Linear Expansion (BLE)



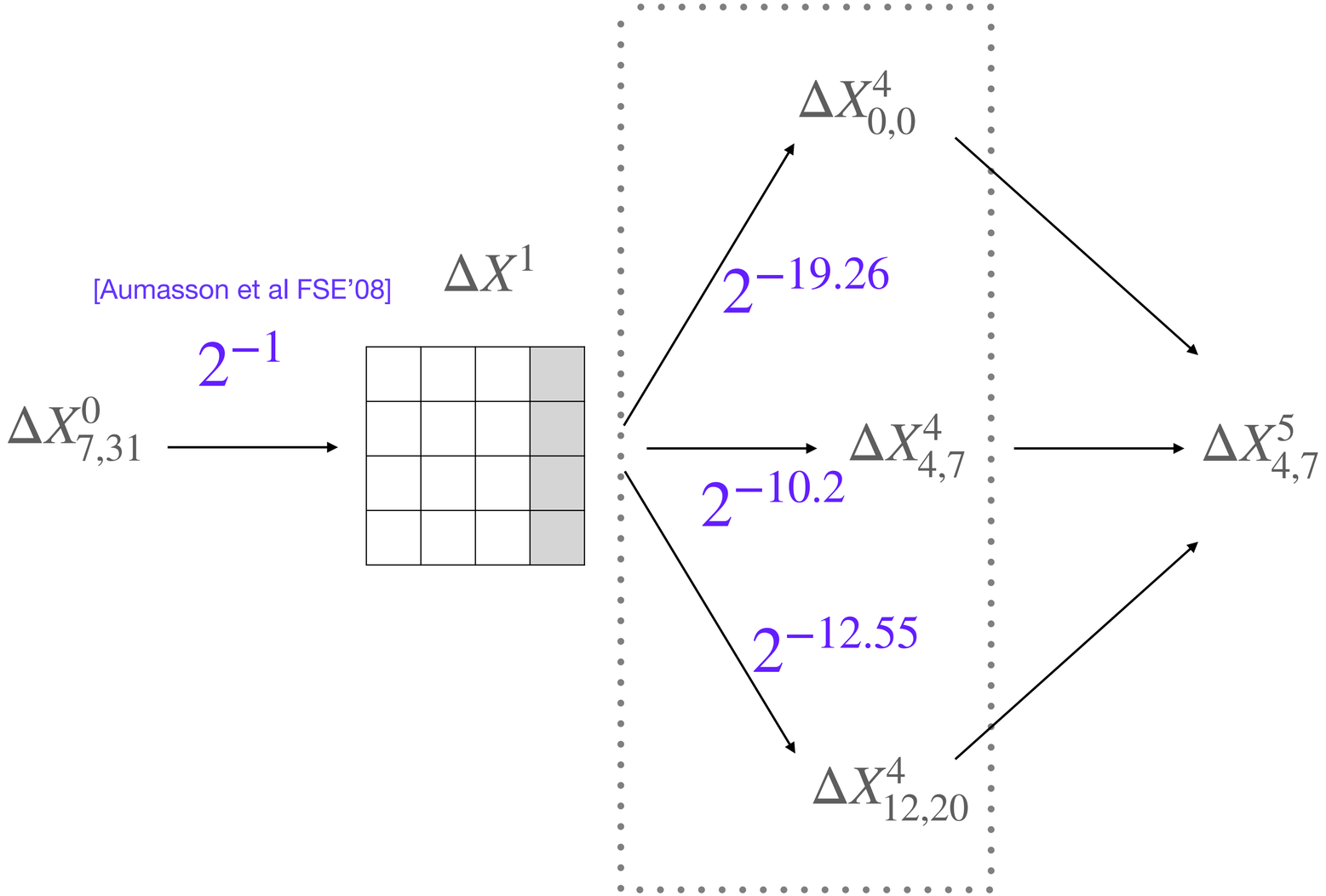
Attacking 8 rounds of Salsa

Bidirectional Linear Expansion (BLE)



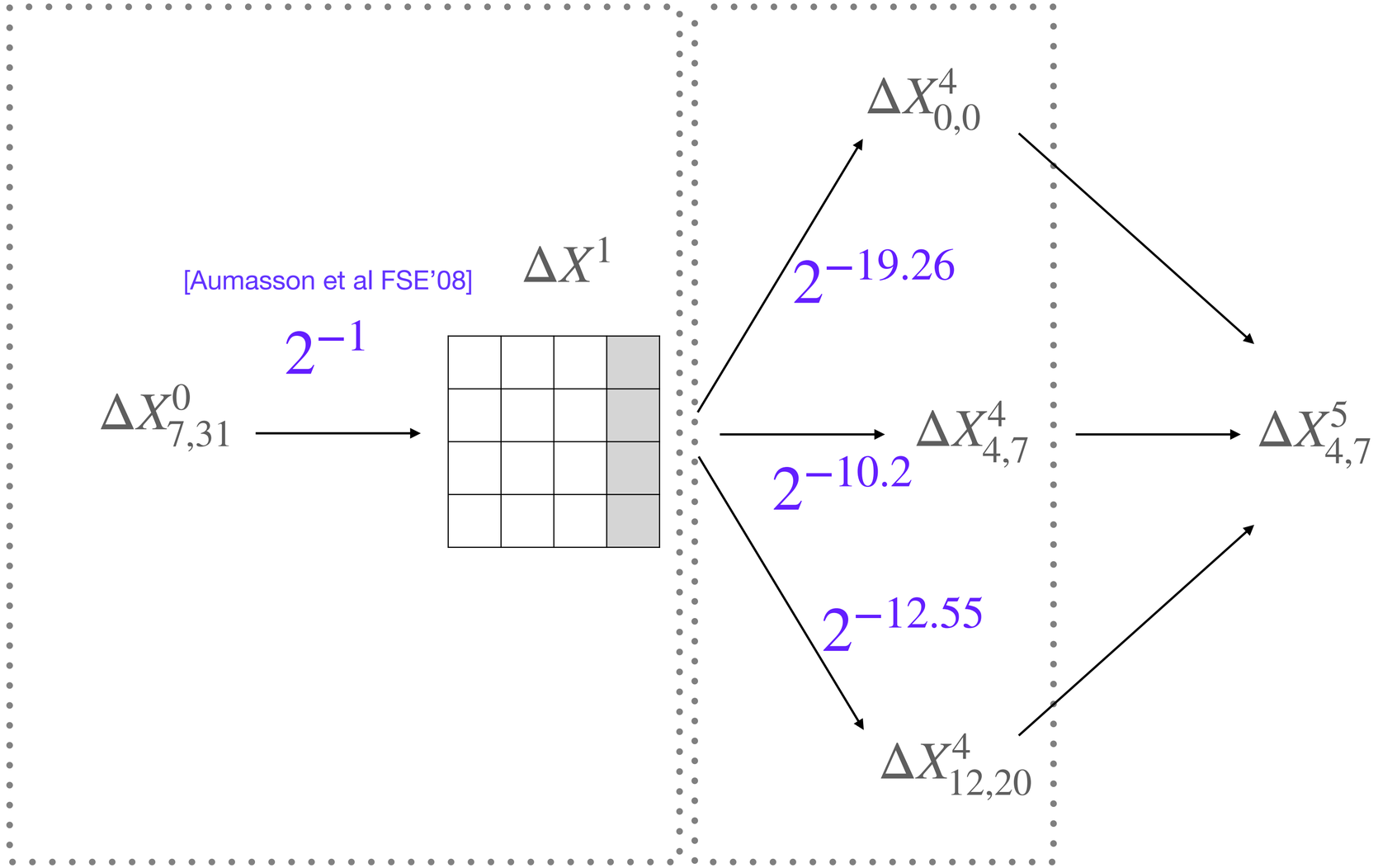
Attacking 8 rounds of Salsa

Bidirectional Linear Expansion (BLE)



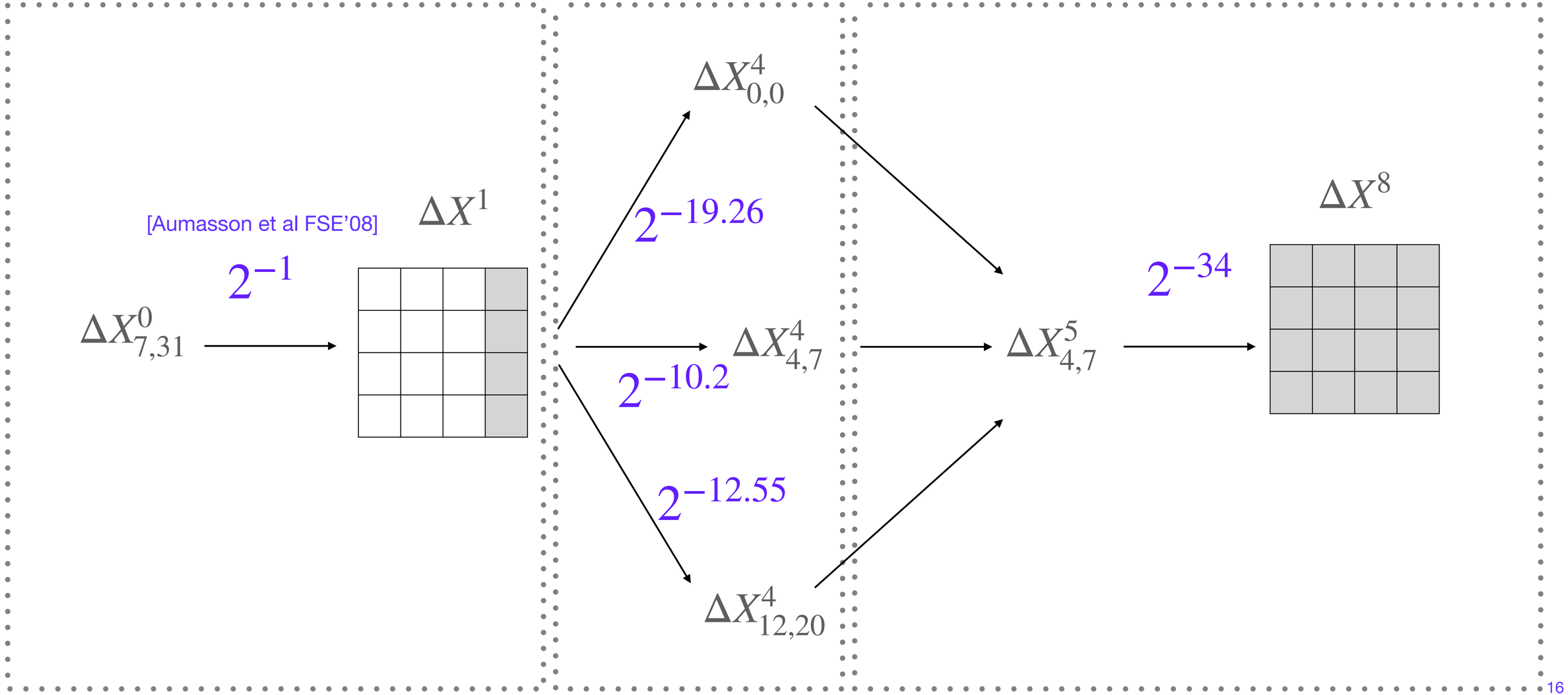
Attacking 8 rounds of Salsa

Bidirectional Linear Expansion (BLE)



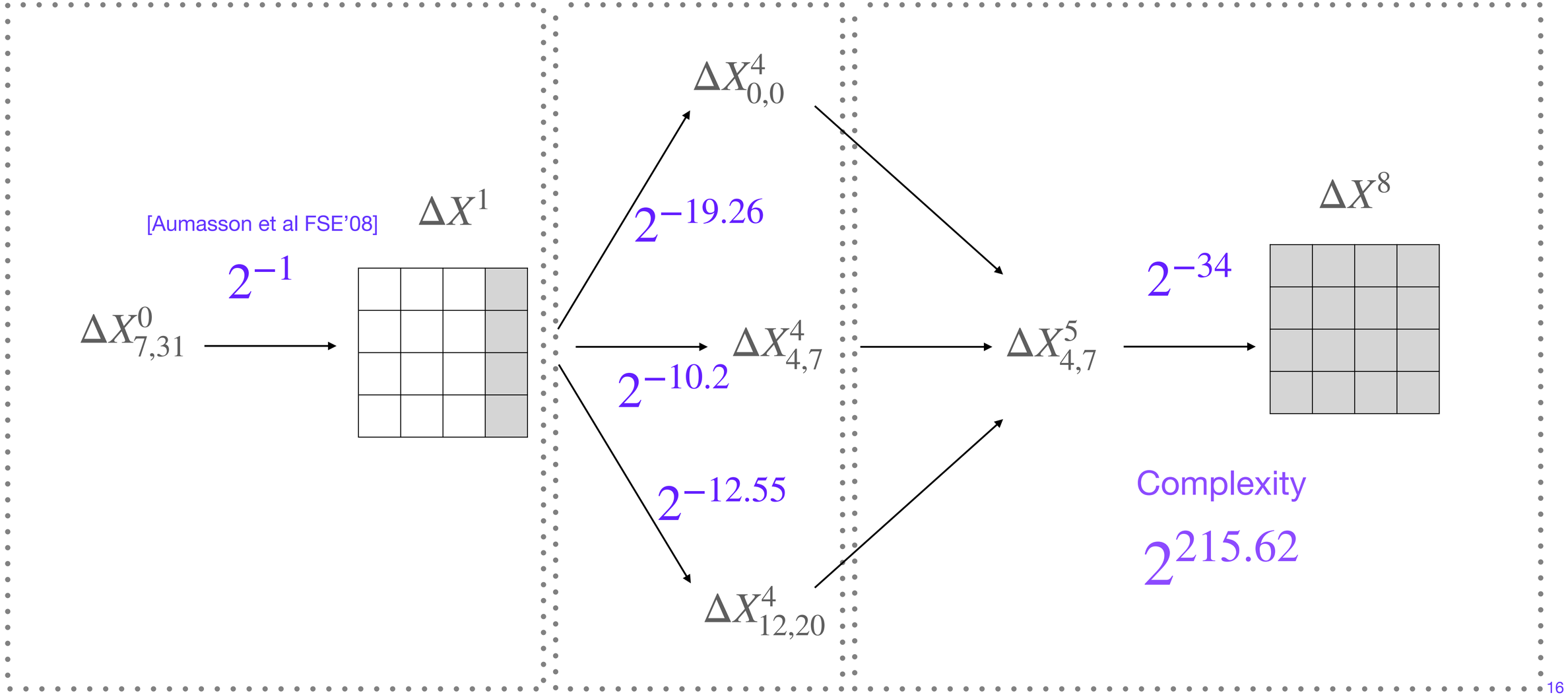
Attacking 8 rounds of Salsa

Bidirectional Linear Expansion (BLE)



Attacking 8 rounds of Salsa

Bidirectional Linear Expansion (BLE)

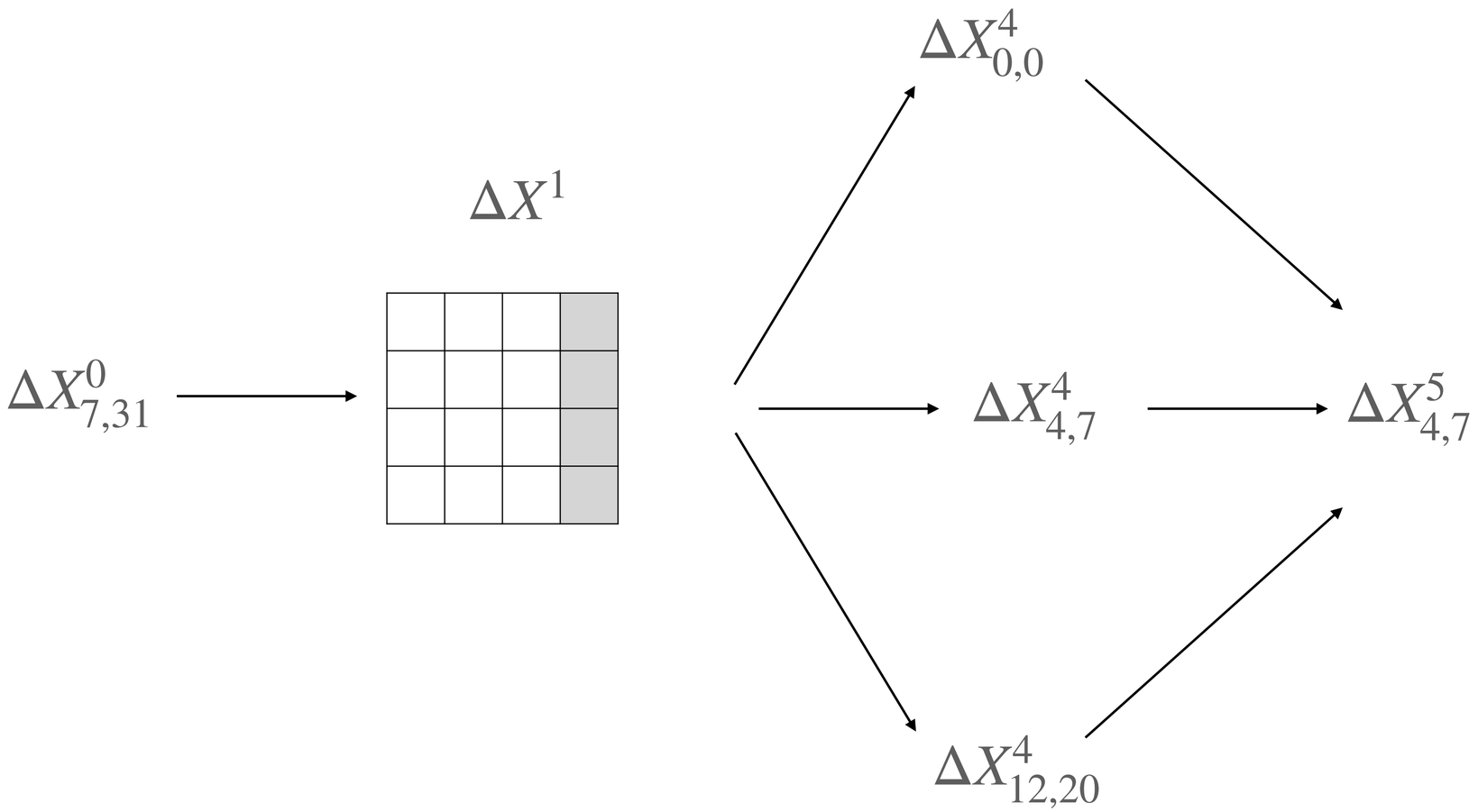


Attacking Salsa

Differential-Linear distinguisher Salsa

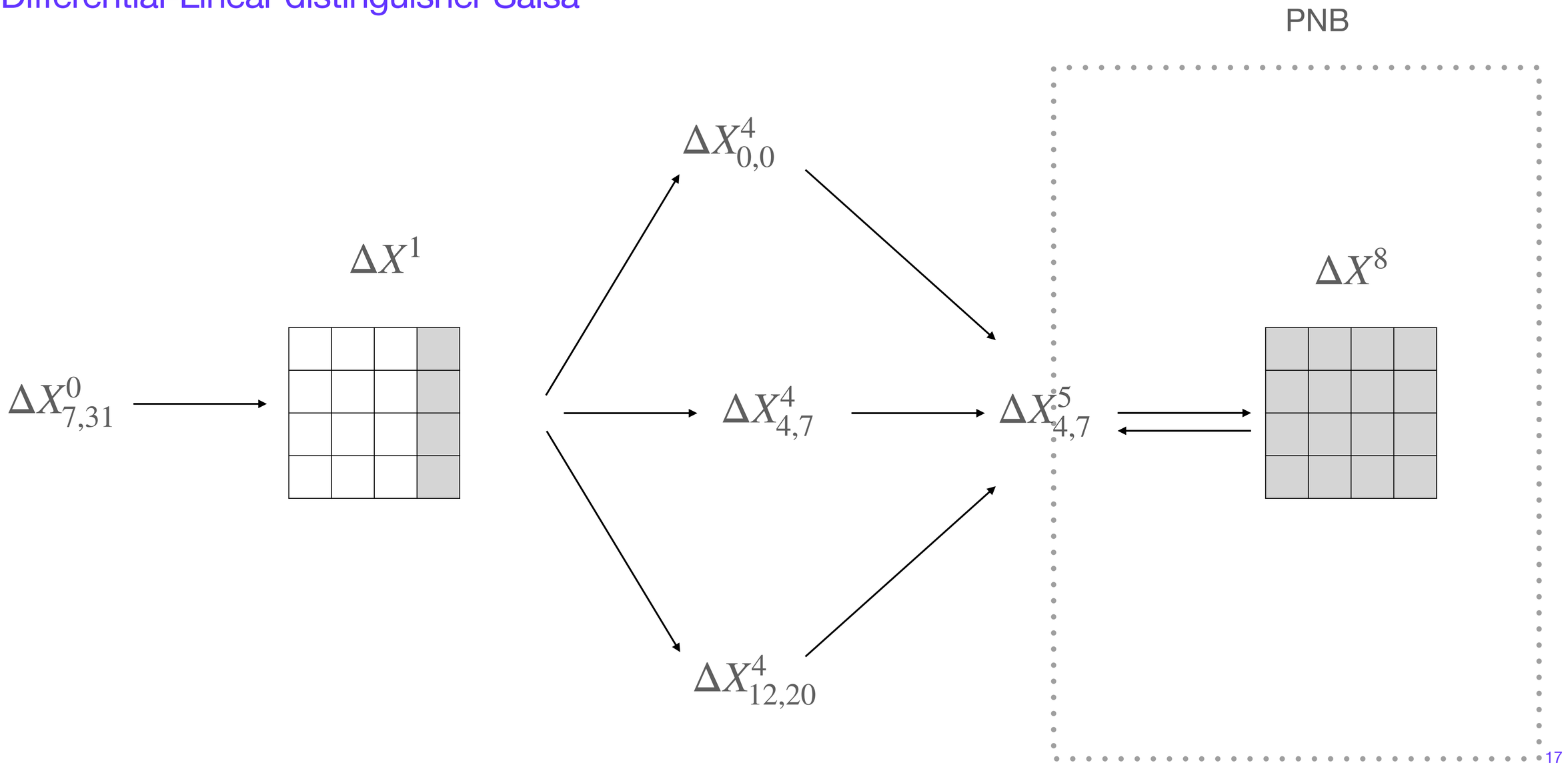
Attacking Salsa

Differential-Linear distinguisher Salsa



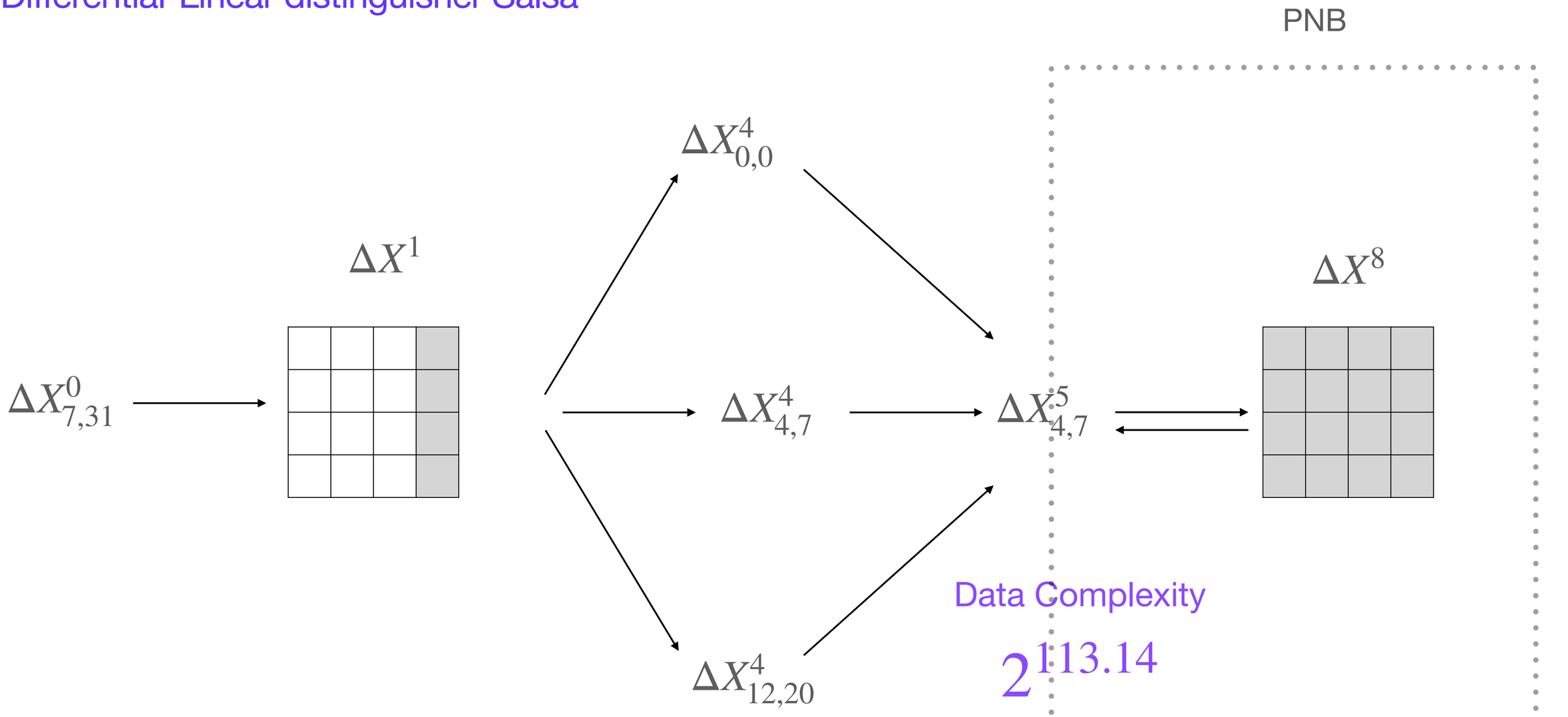
Attacking Salsa

Differential-Linear distinguisher Salsa



Attacking Salsa

Differential-Linear distinguisher Salsa

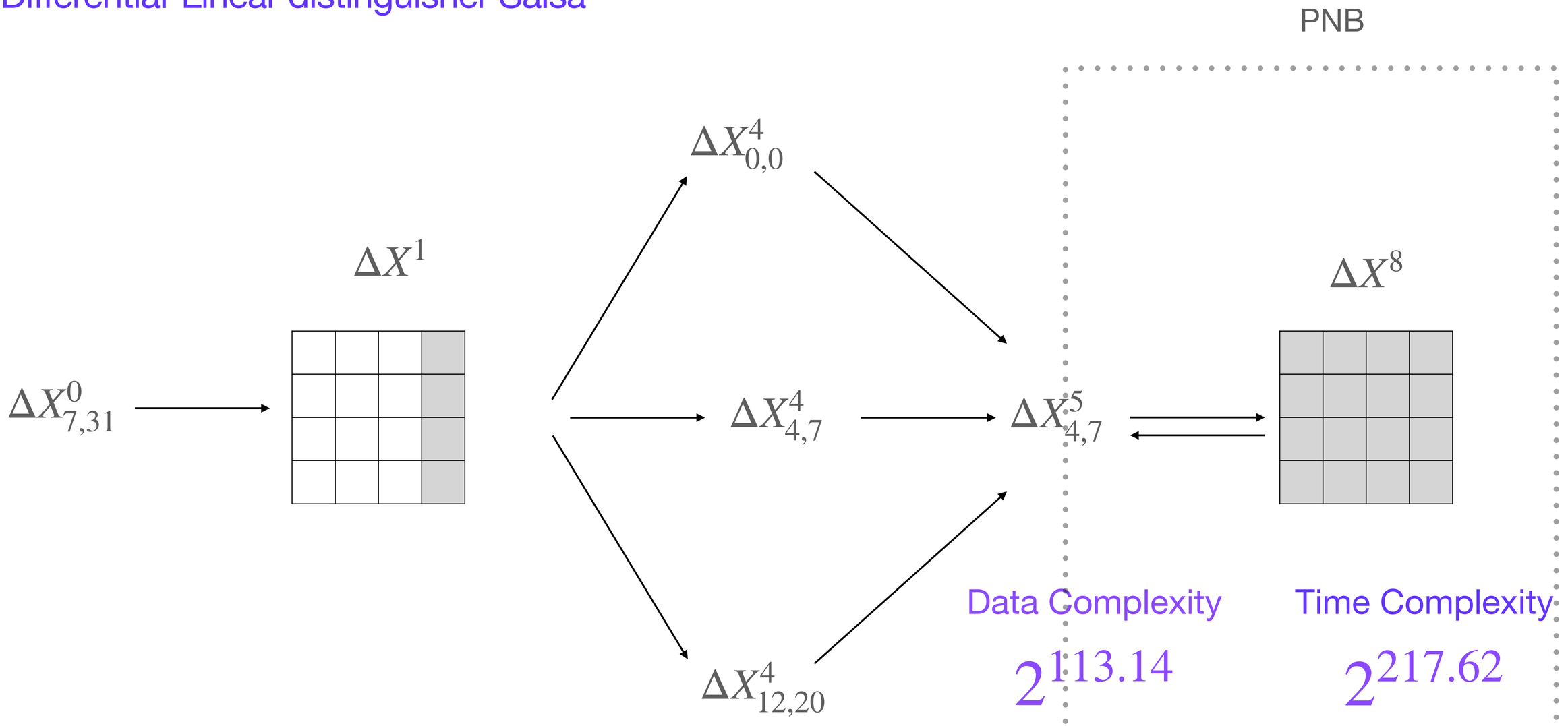


Data Complexity

$2^{113.14}$

Attacking Salsa

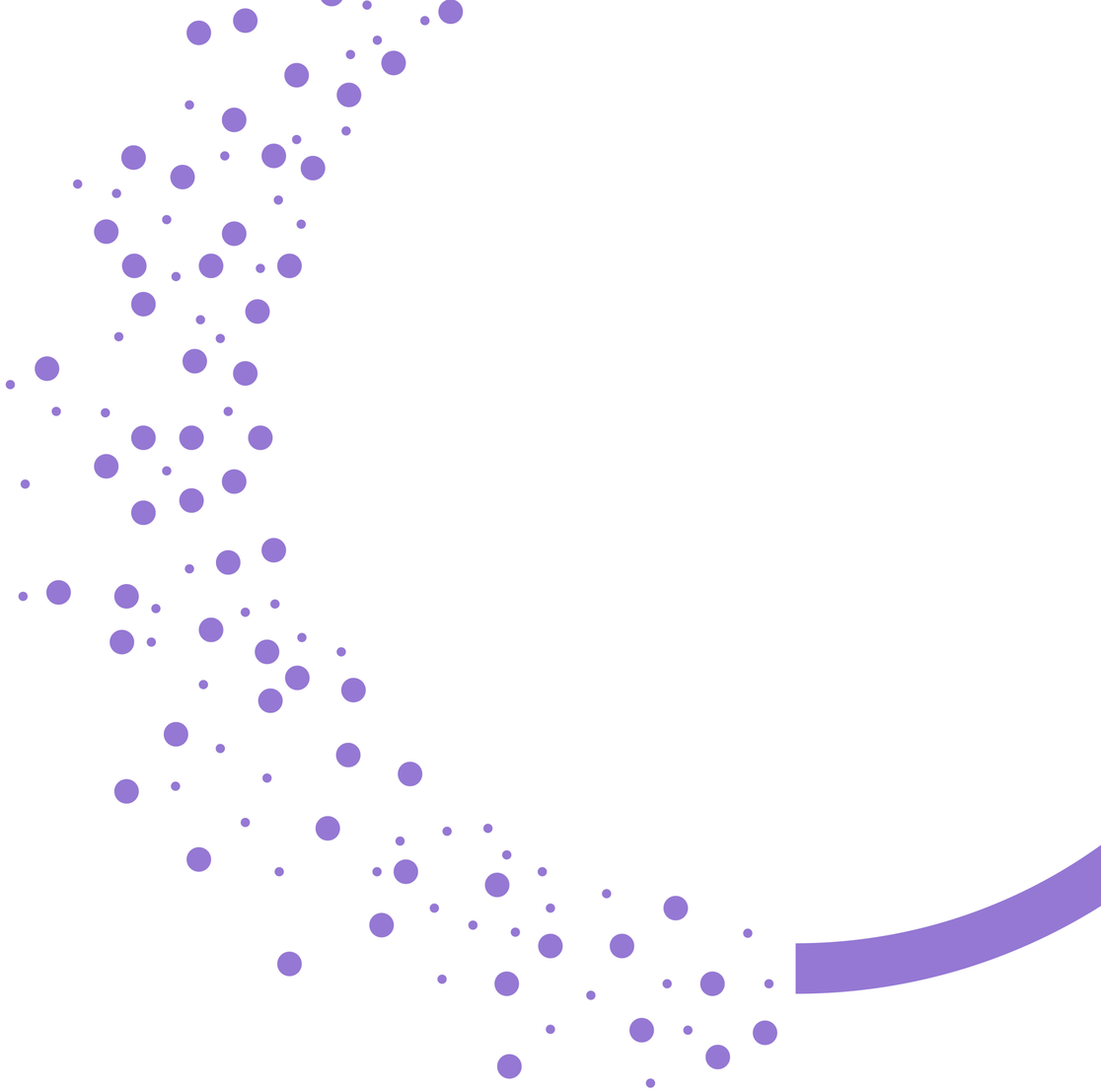
Differential-Linear distinguisher Salsa



Technology Innovation Institute

Our contributions

New cipher Forró

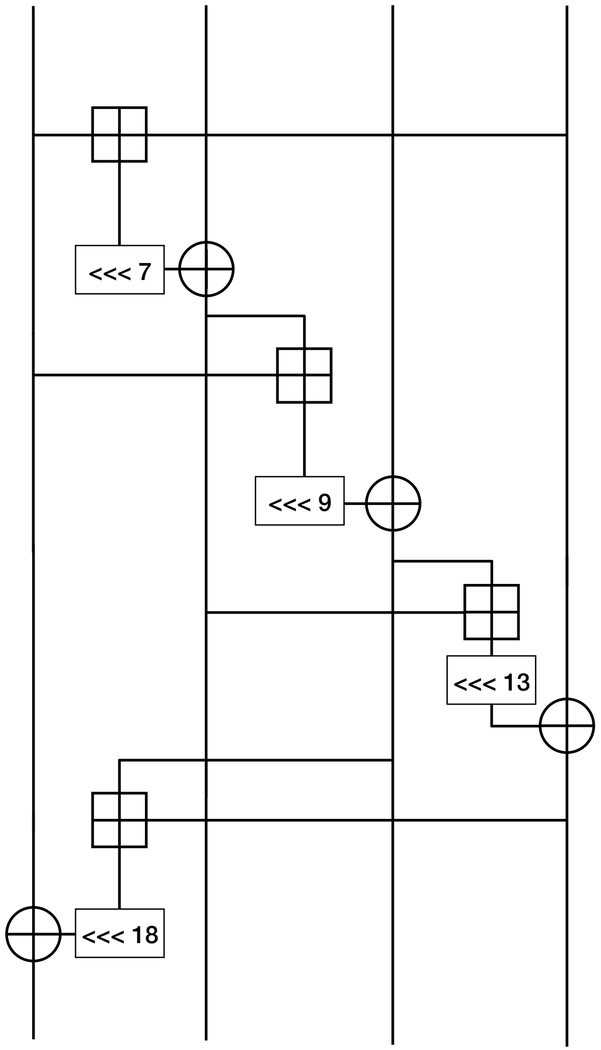


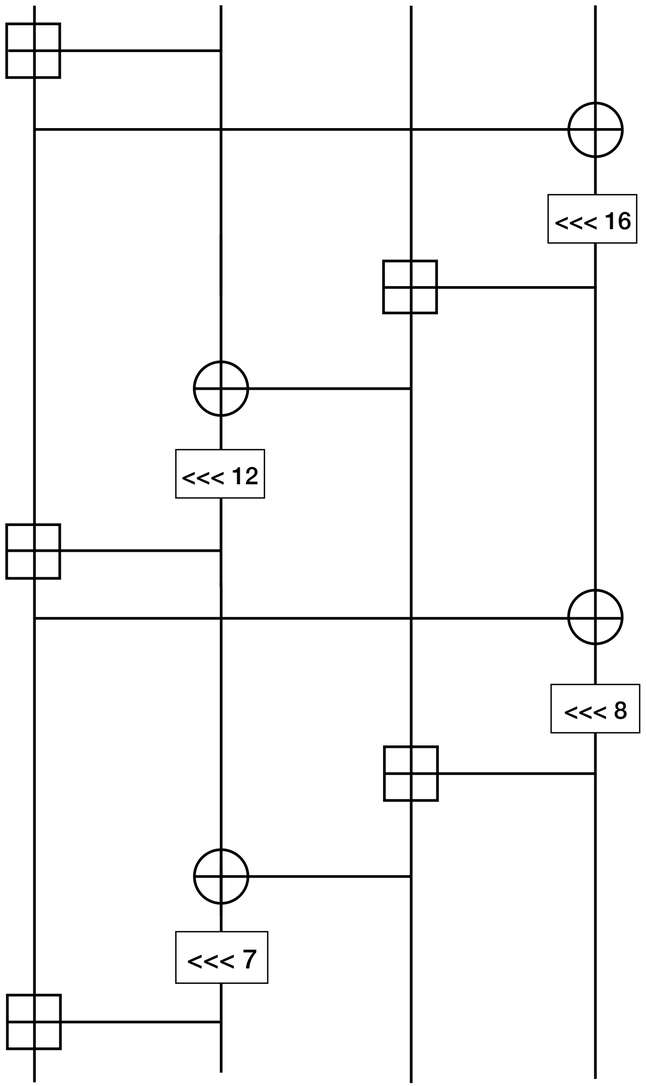
Cryptography Research Center

tii.ae

Salsa and ChaCha

Quarter Rounds

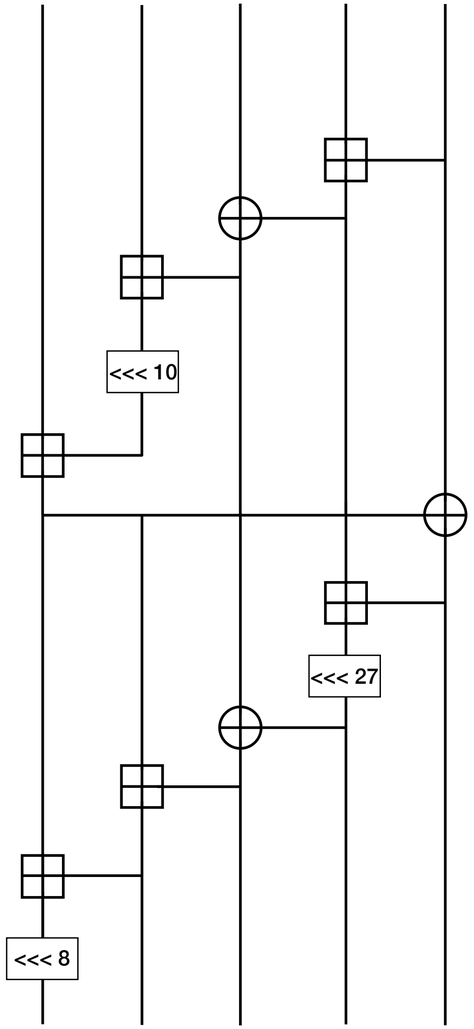




Forró

Description

- 256 key bits
- Same number of components as ChaCha and Salsa (12 components)
- Daniel J. Bernstein advice [Bernstein, D.J.’08] -> “Replacing some of the rotations with a comparable number of additions might achieve comparable diffusion in less time.”
- Better Diffusion than ChaCha -> Less rounds -> 14 rounds



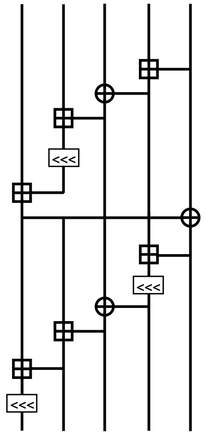
Forró

Design

Forró

Design

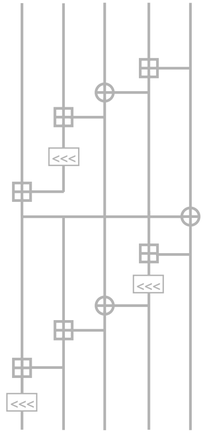
x_0			x_3
x_4			
x_8			
x_{12}			



Forró

Design

x_0			x_3
x_4			
x_8			
x_{12}			



Forró

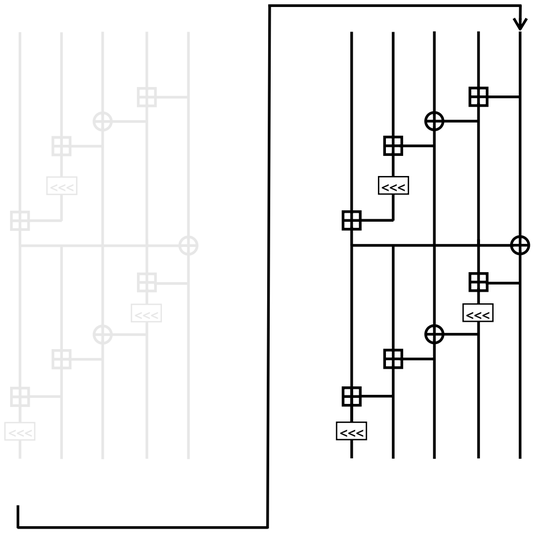
Design

x_0			x_3
x_4			
x_8			
x_{12}			

Forró

Design

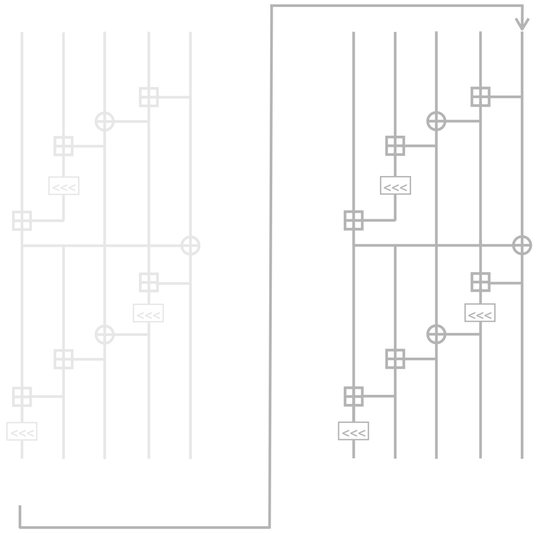
x_0	x_1		x_3
x_4	x_5		
x_8	x_9		
x_{12}	x_{13}		



Forró

Design

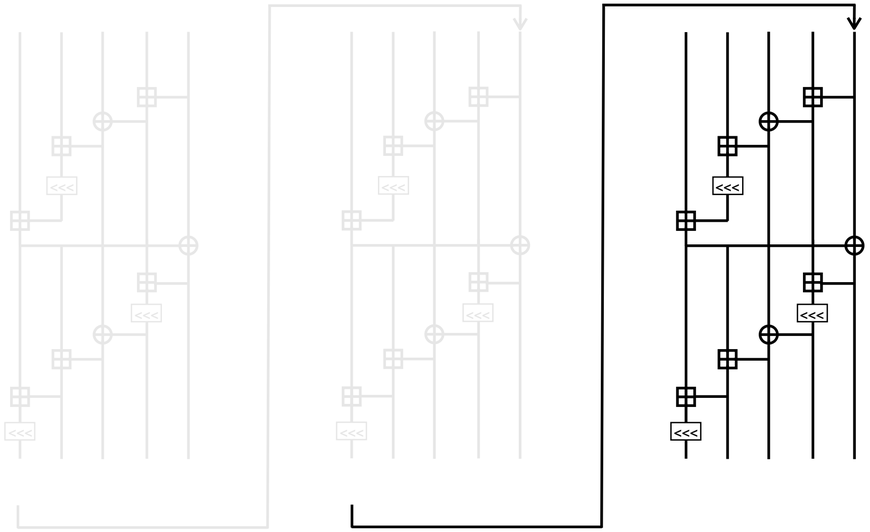
x_0	x_1		x_3
x_4	x_5		
x_8	x_9		
x_{12}	x_{13}		



Forró

Design

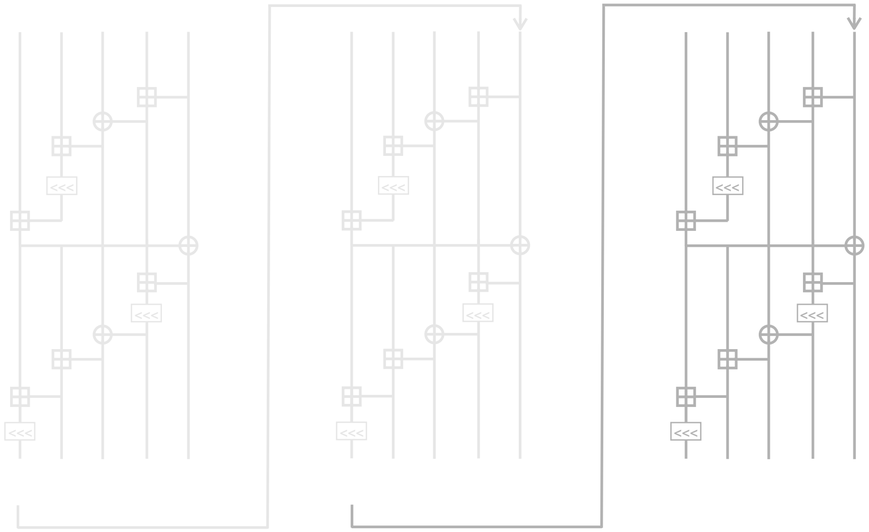
x_0	x_1	x_2	x_3
x_4	x_5	x_6	
x_8	x_9	x_{10}	
x_{12}	x_{13}	x_{14}	



Forró

Design

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



Forró

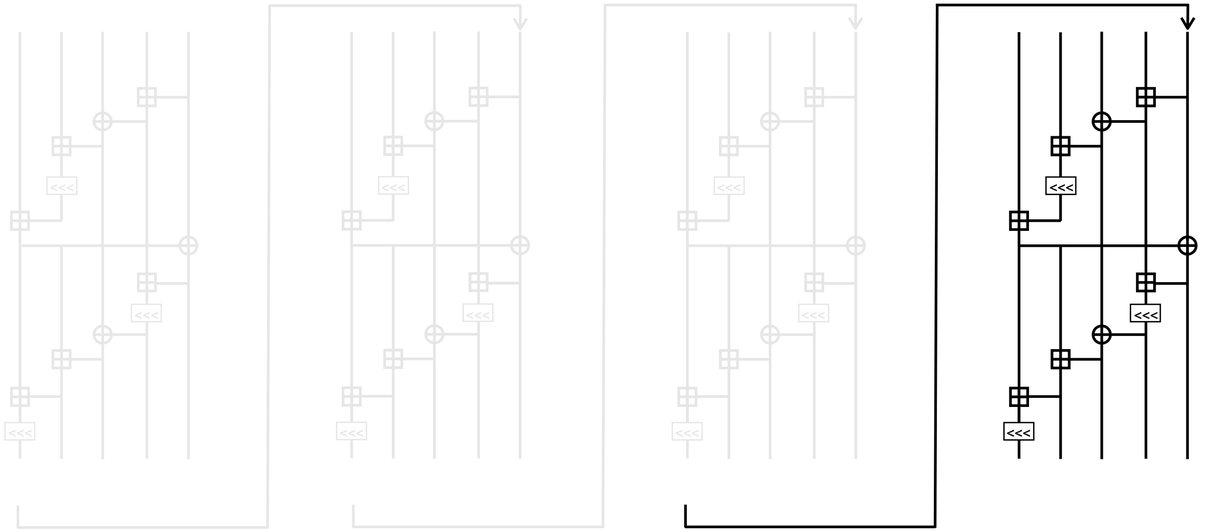
Design

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

Forró

Design

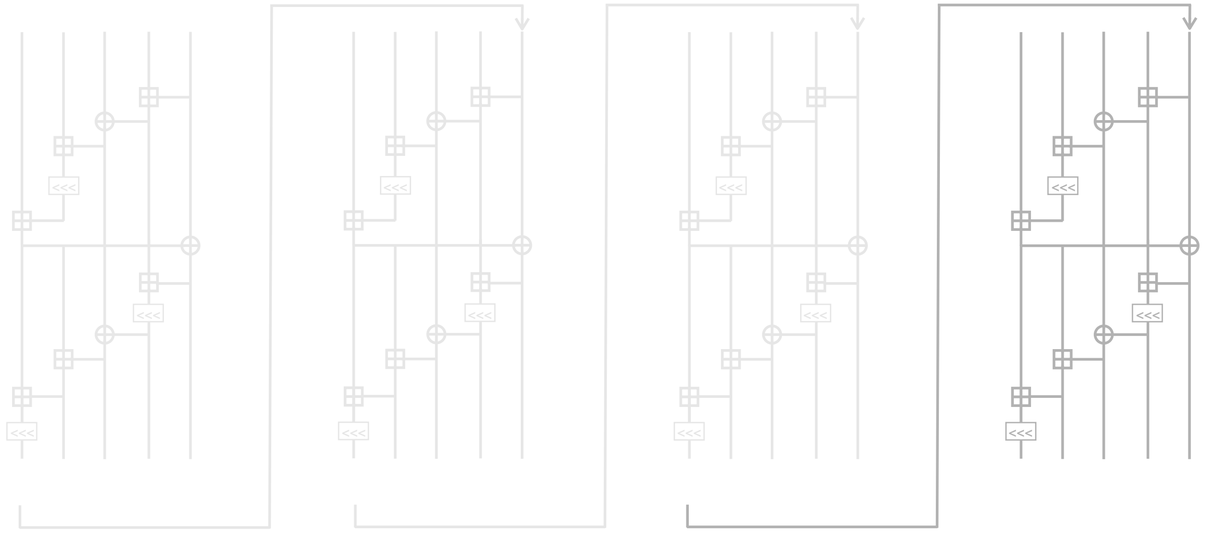
x_0	x_1	x_2	x_3
x_4	x_5	x_6	x_7
x_8	x_9	x_{10}	x_{11}
x_{12}	x_{13}	x_{14}	x_{15}



Forró

Design

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}



Forró

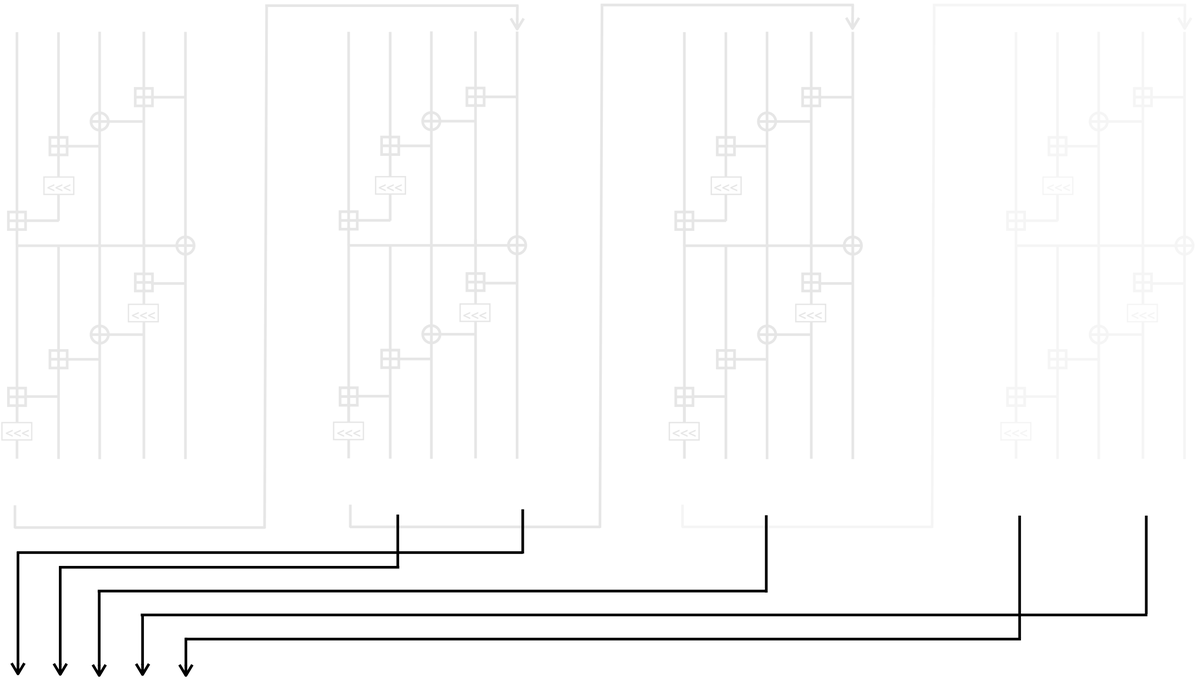
Design

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}

Forró

Design

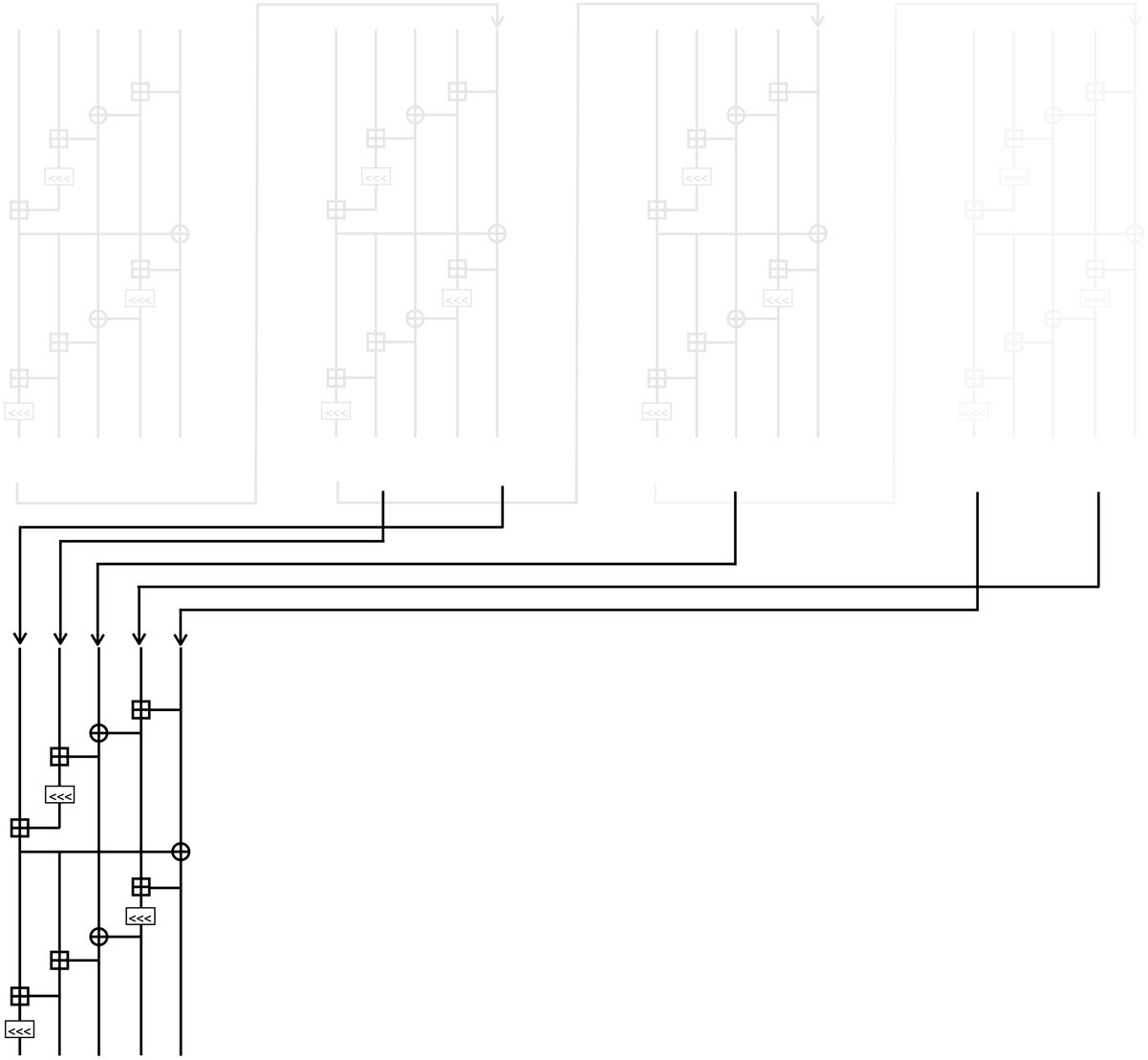
x_0	x_1	x_2	x_3
x_4	x_5	x_6	x_7
x_8	x_9	x_{10}	x_{11}
x_{12}	x_{13}	x_{14}	x_{15}



Forró

Design

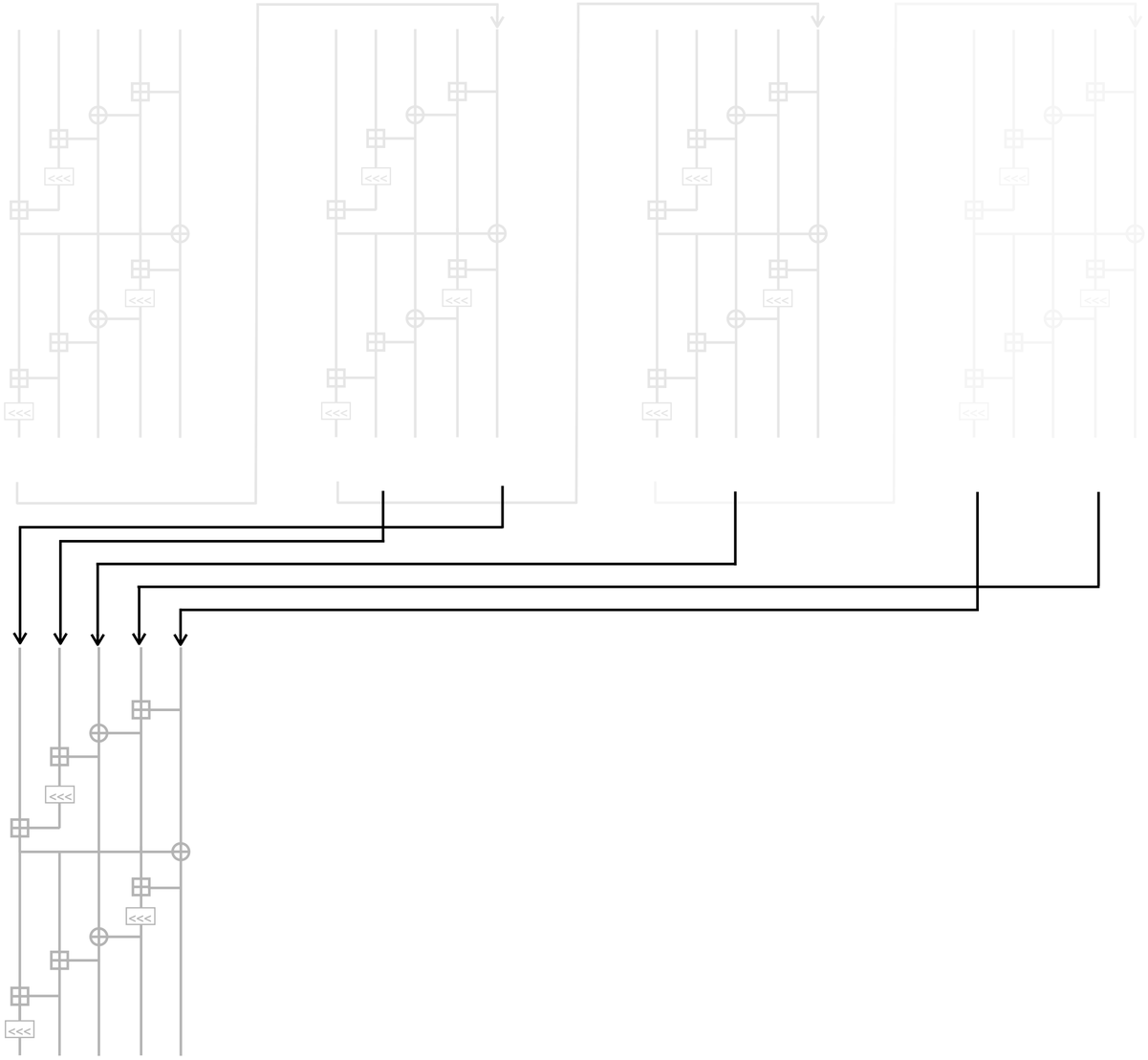
x_0	x_1	x_2	x_3
x_4	x_5	x_6	x_7
x_8	x_9	x_{10}	x_{11}
x_{12}	x_{13}	x_{14}	x_{15}



Forró

Design

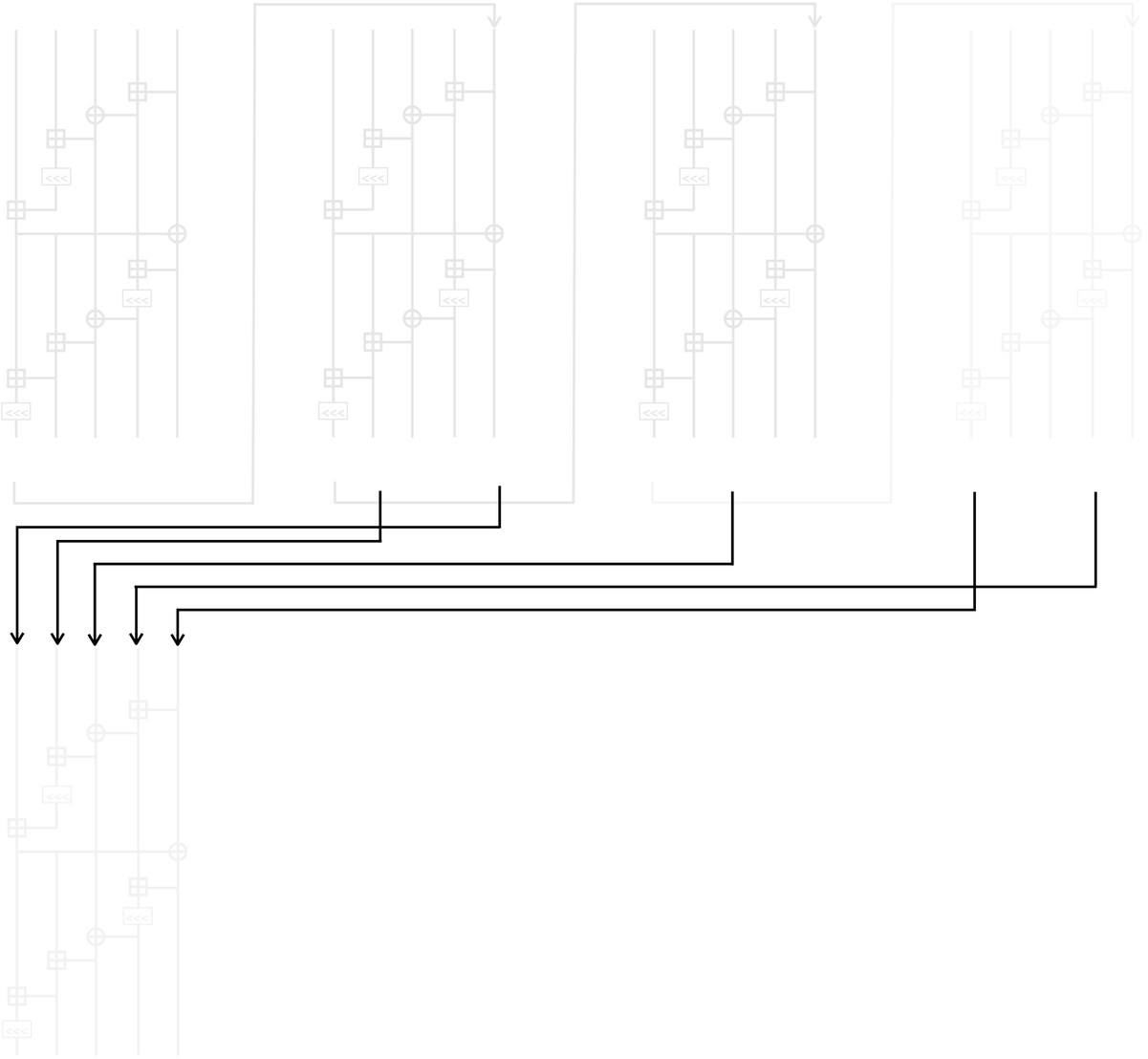
x_0	x_1	x_2	x_3
x_4	x_5	x_6	x_7
x_8	x_9	x_{10}	x_{11}
x_{12}	x_{13}	x_{14}	x_{15}



Forró

Design

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}



Forró

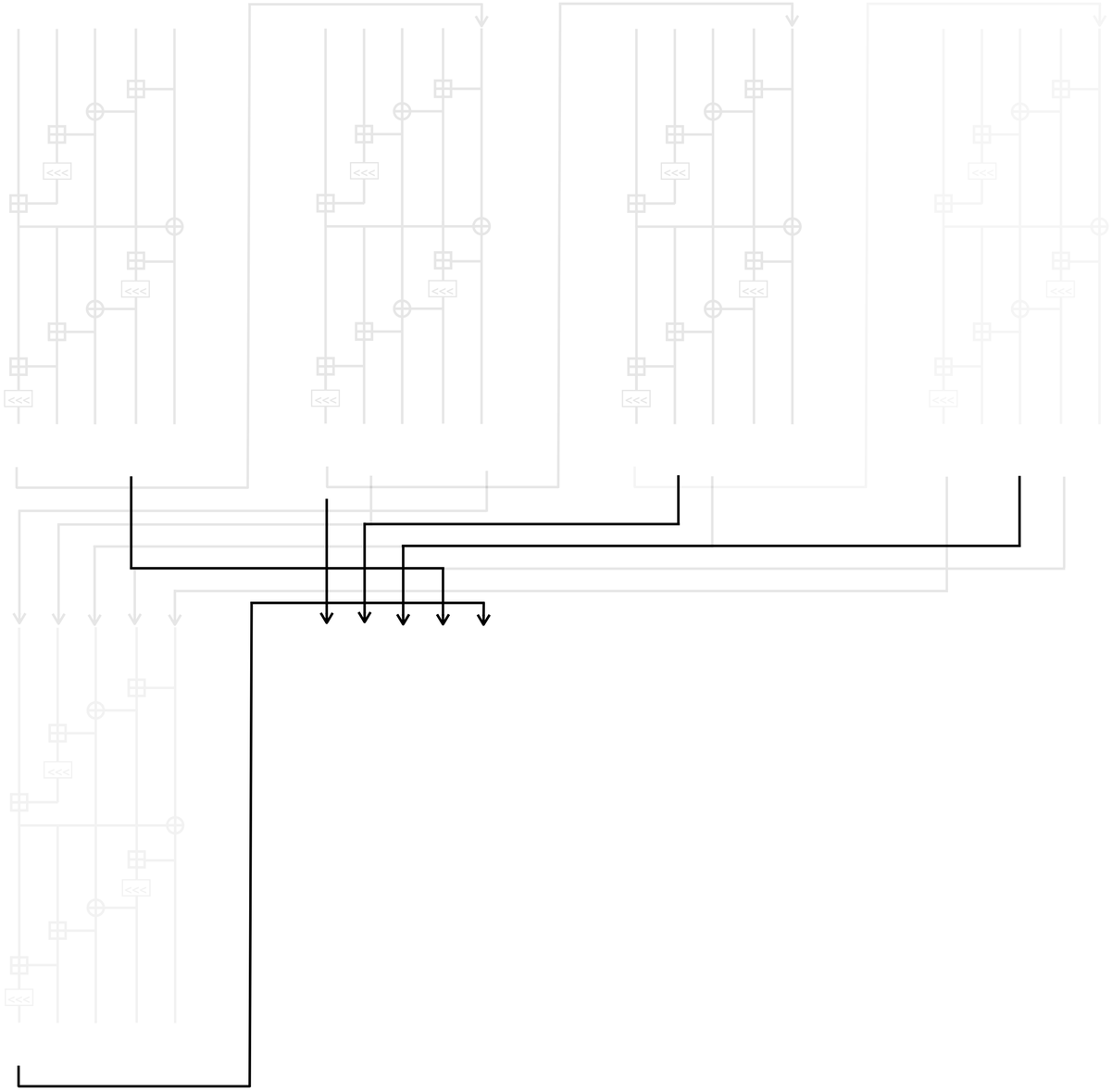
Design

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}

Forró

Design

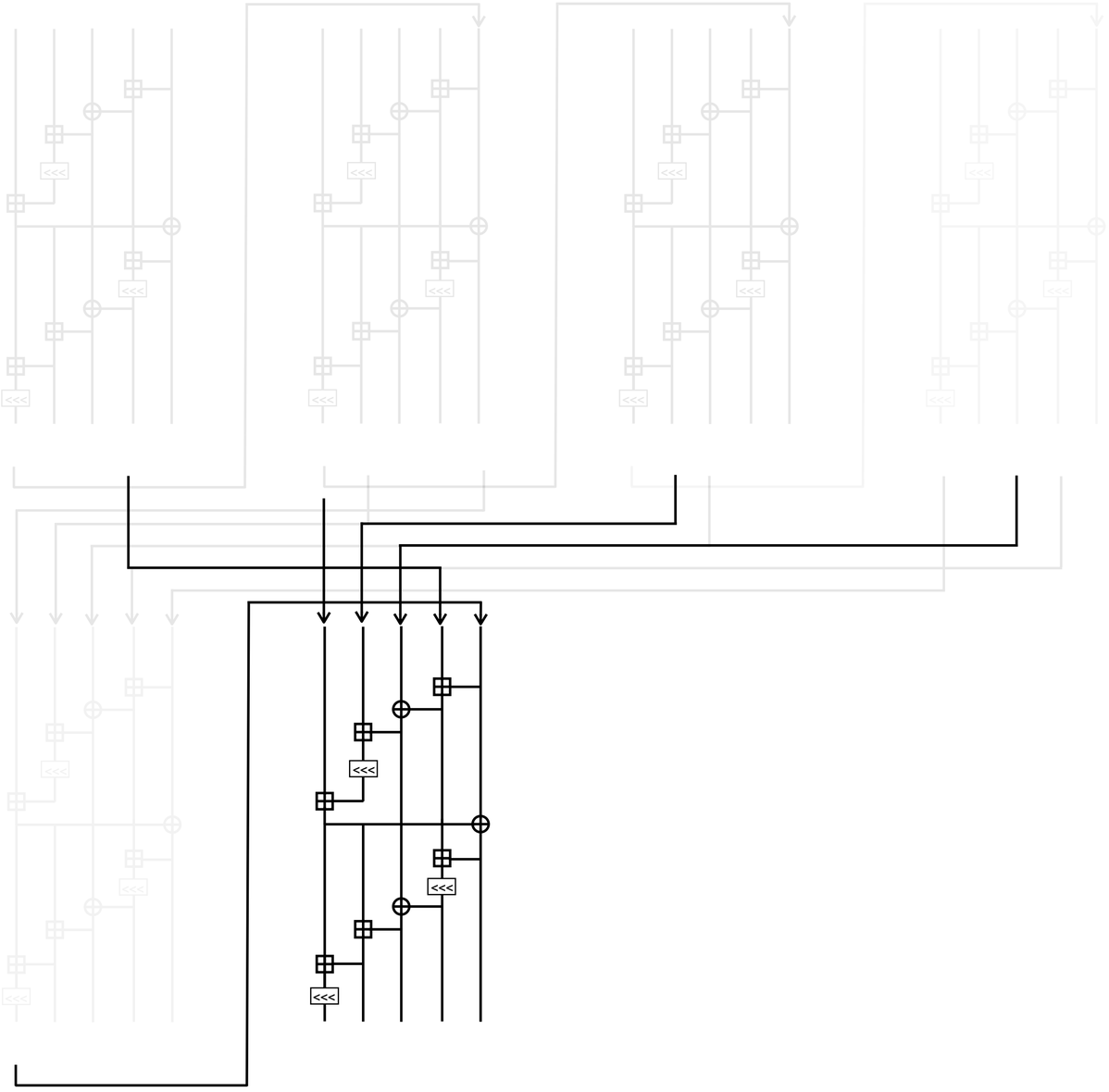
x_0	x_1	x_2	x_3
x_4	x_5	x_6	x_7
x_8	x_9	x_{10}	x_{11}
x_{12}	x_{13}	x_{14}	x_{15}



Forró

Design

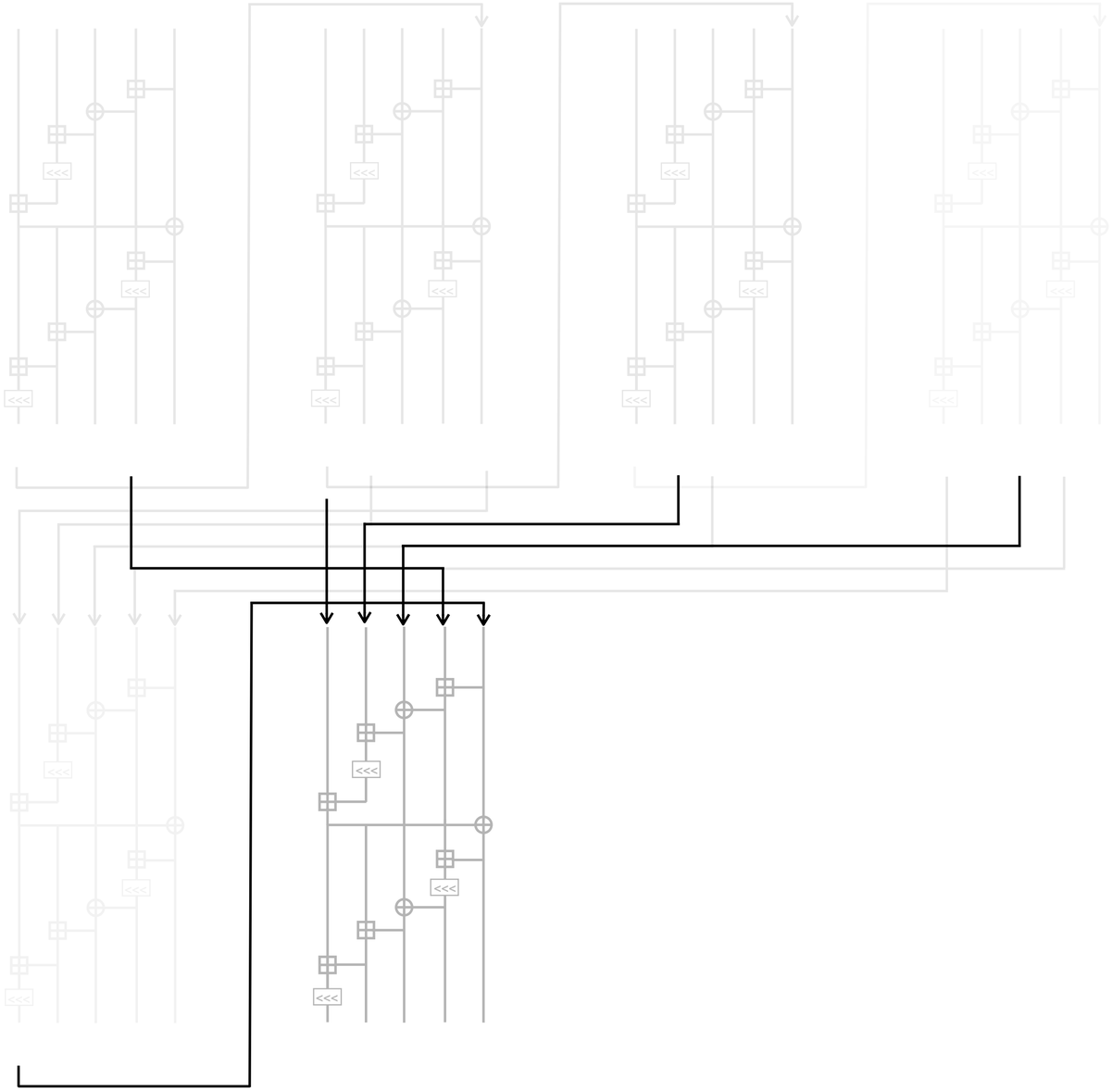
x_0	x_1	x_2	x_3
x_4	x_5	x_6	x_7
x_8	x_9	x_{10}	x_{11}
x_{12}	x_{13}	x_{14}	x_{15}



Forró

Design

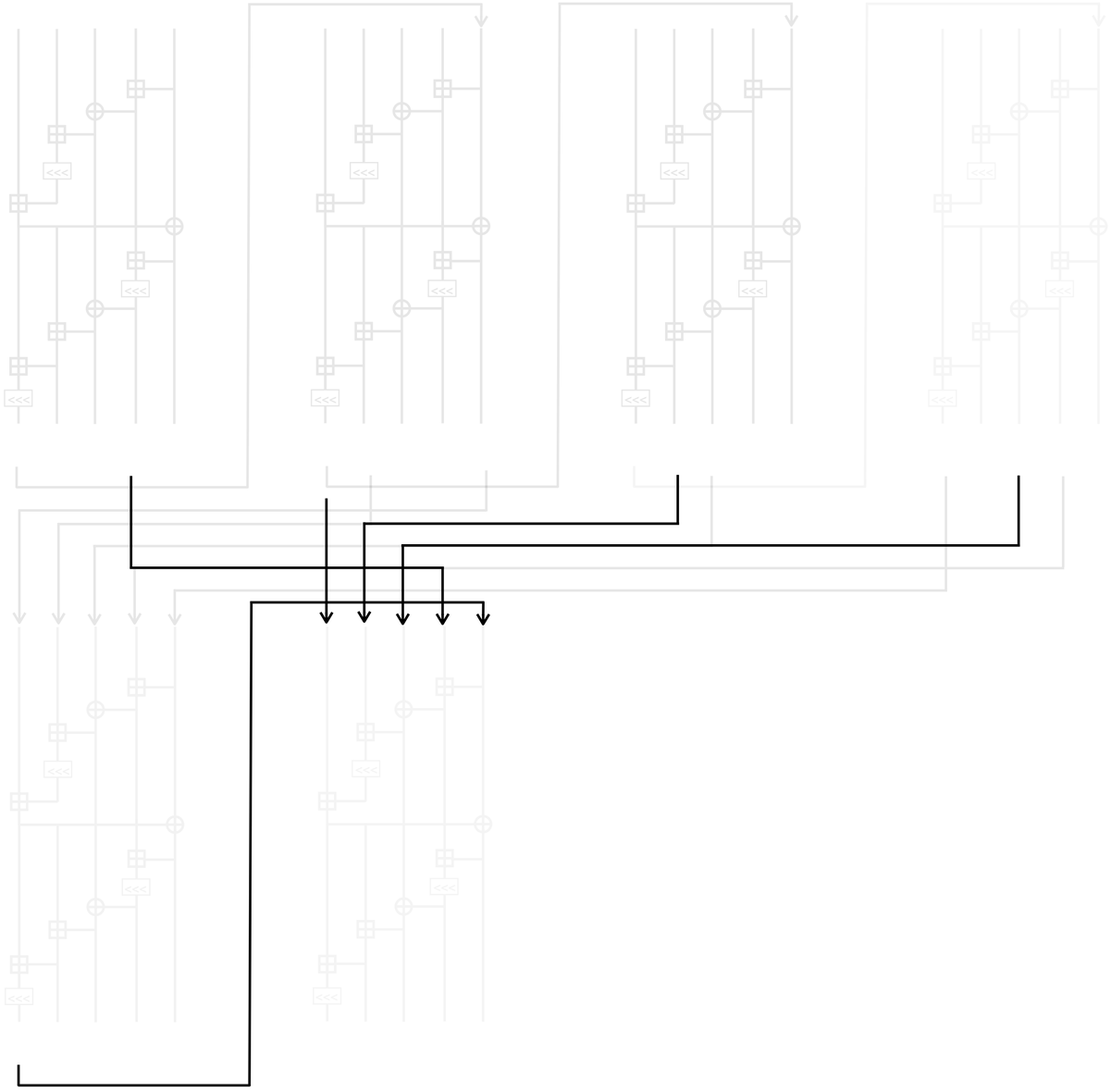
x_0	x_1	x_2	x_3
x_4	x_5	x_6	x_7
x_8	x_9	x_{10}	x_{11}
x_{12}	x_{13}	x_{14}	x_{15}



Forró

Design

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}



Forró

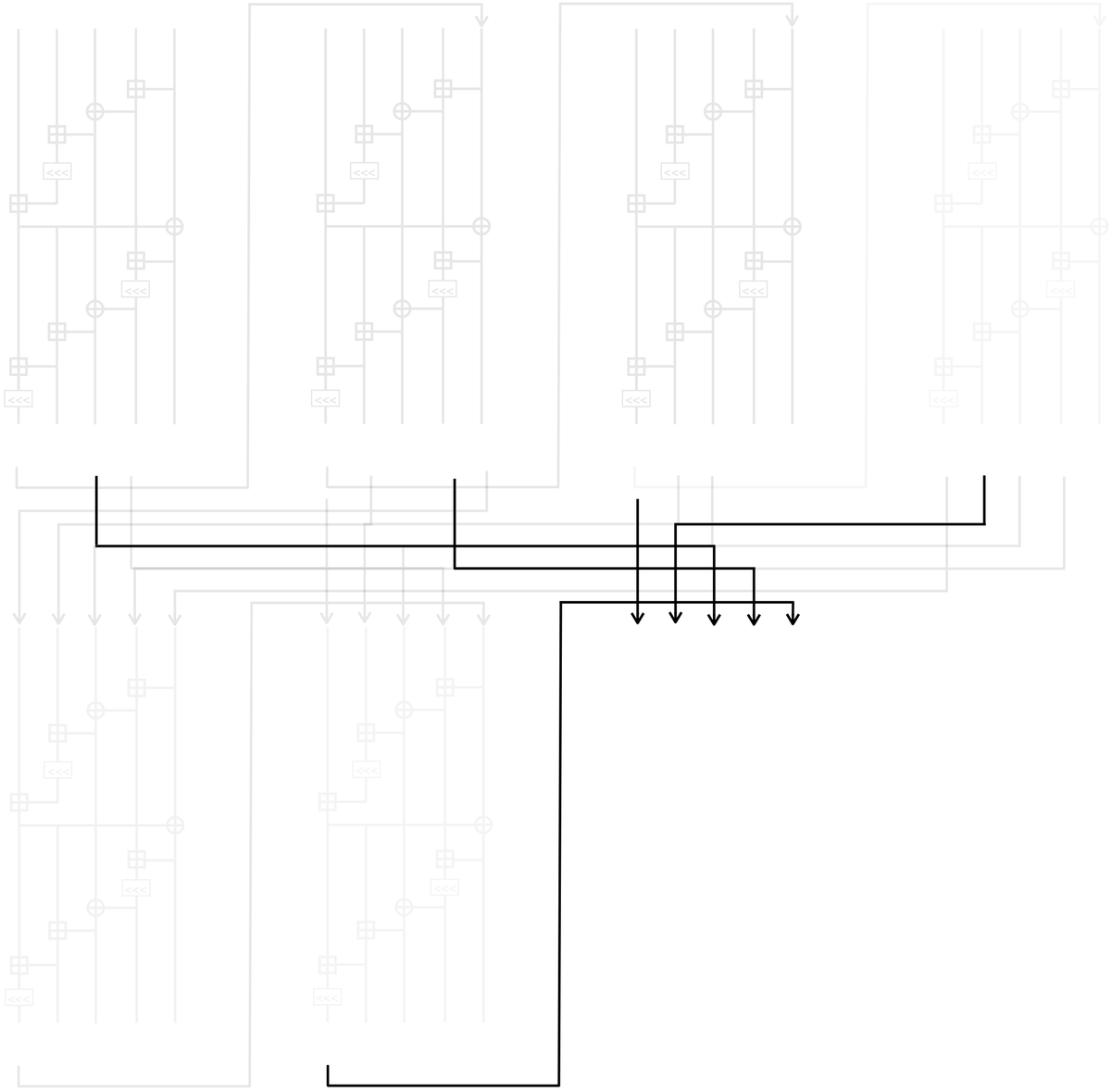
Design

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}

Forró

Design

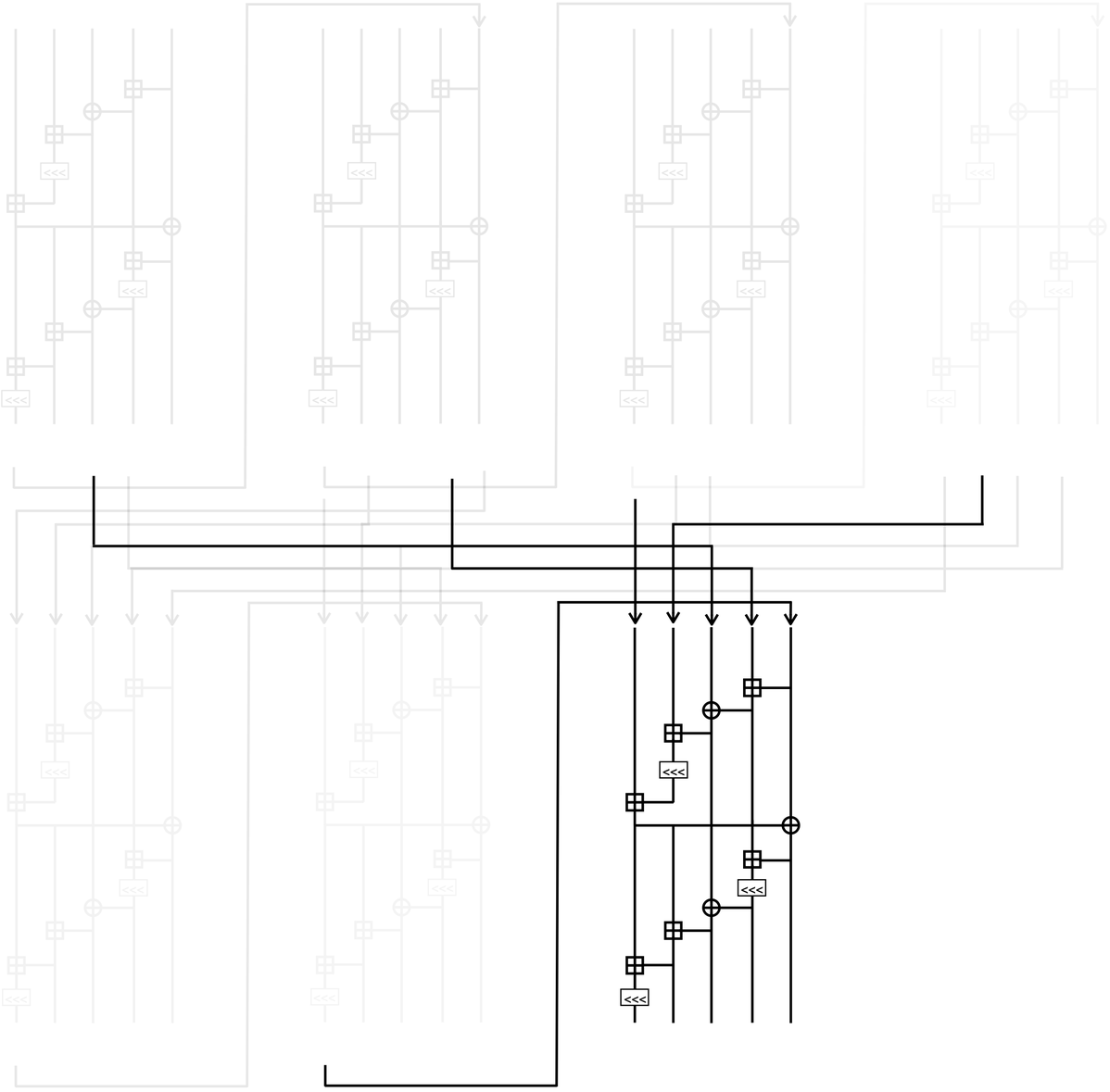
x_0	x_1	x_2	x_3
x_4	x_5	x_6	x_7
x_8	x_9	x_{10}	x_{11}
x_{12}	x_{13}	x_{14}	x_{15}



Forró

Design

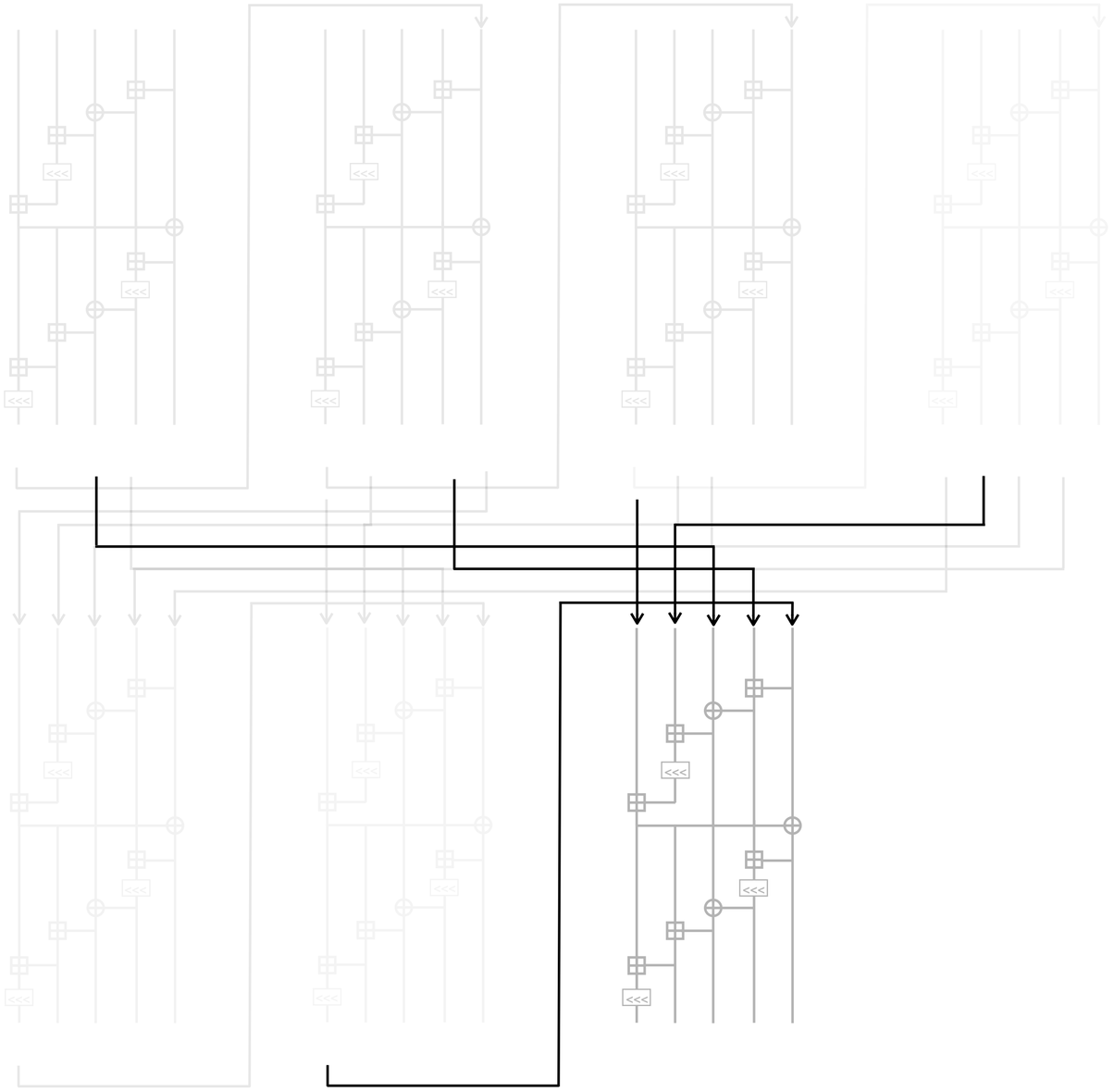
x_0	x_1	x_2	x_3
x_4	x_5	x_6	x_7
x_8	x_9	x_{10}	x_{11}
x_{12}	x_{13}	x_{14}	x_{15}



Forró

Design

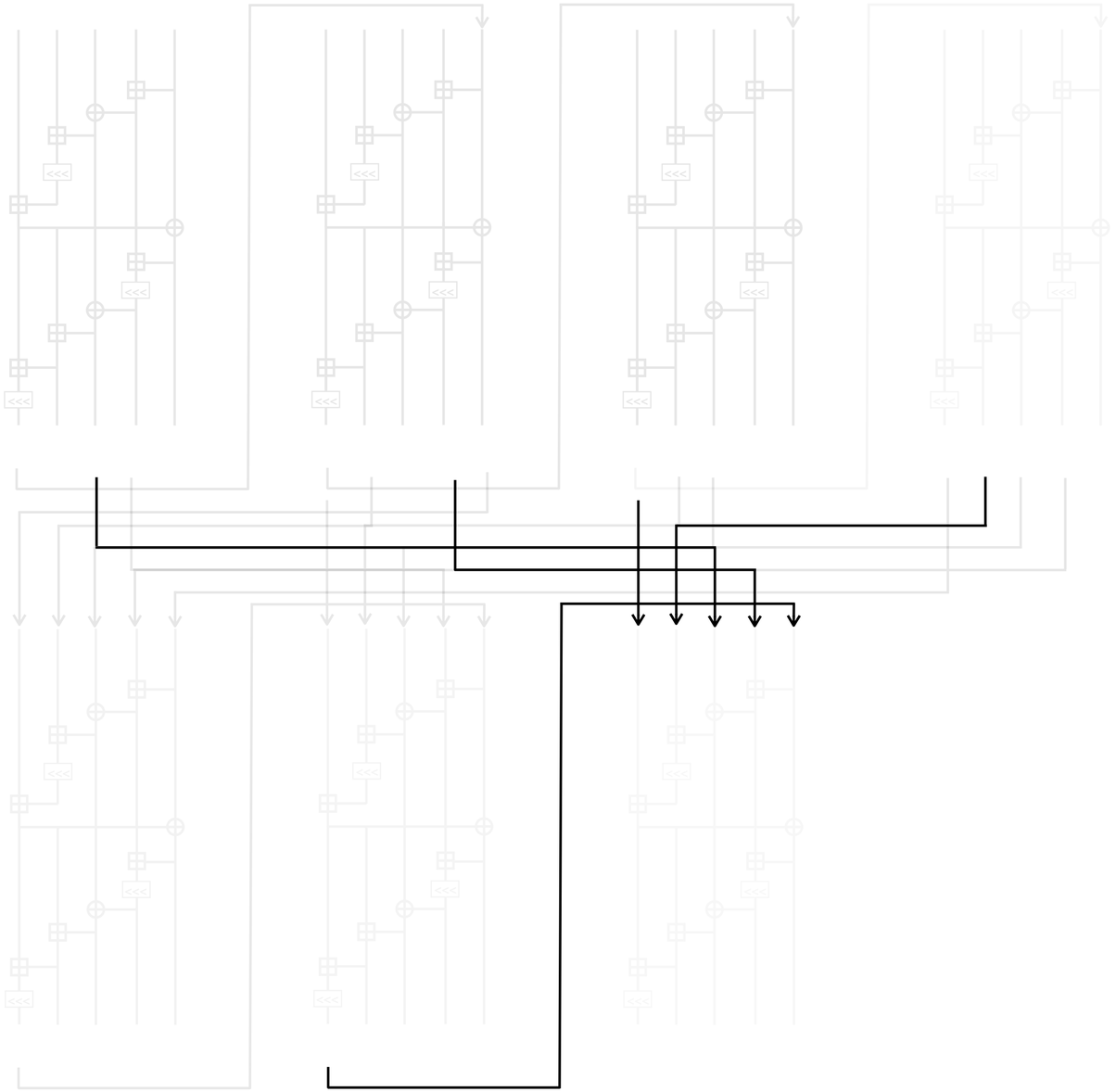
x_0	x_1	x_2	x_3
x_4	x_5	x_6	x_7
x_8	x_9	x_{10}	x_{11}
x_{12}	x_{13}	x_{14}	x_{15}



Forró

Design

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}



Forró

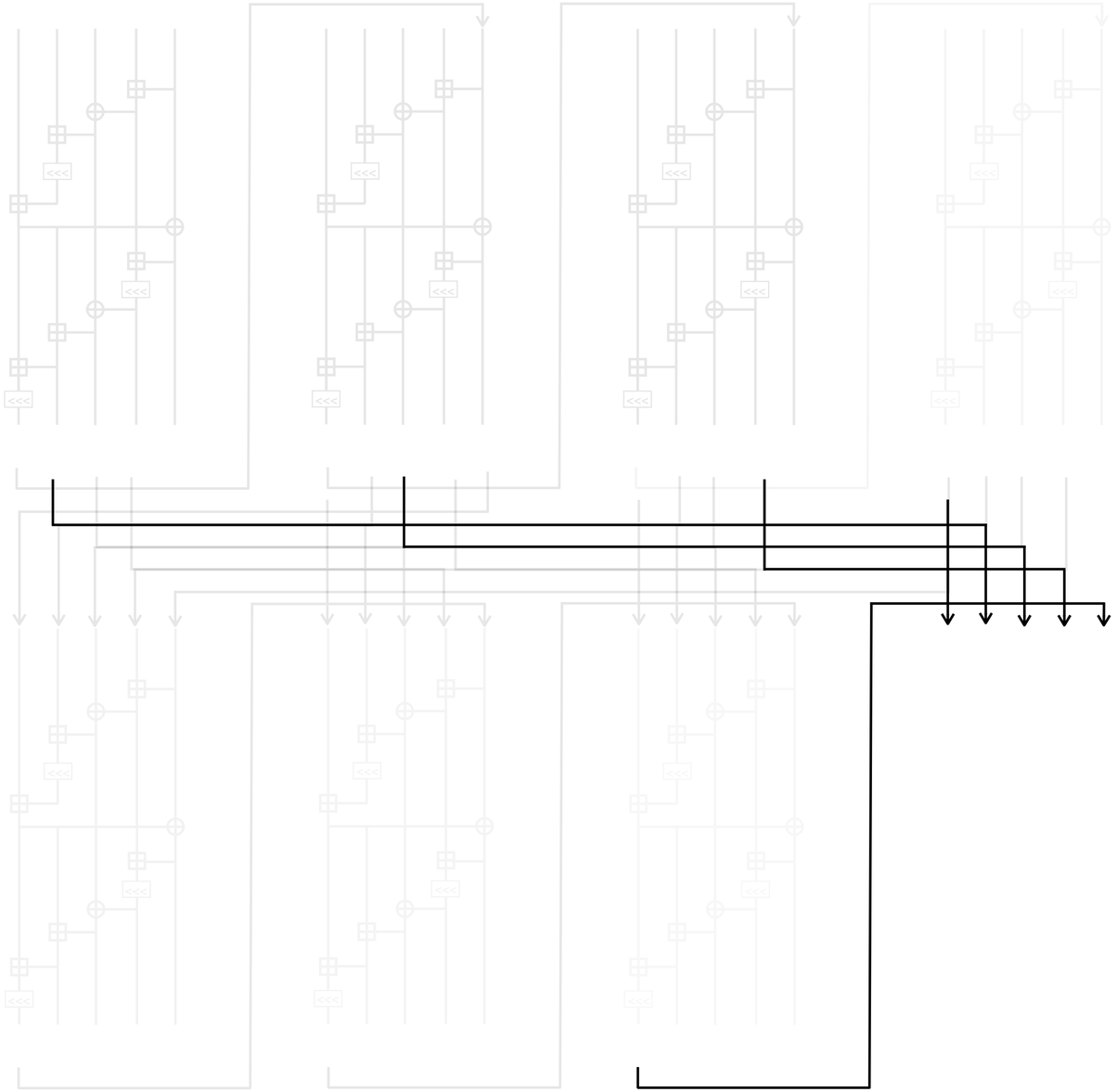
Design

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}

Forró

Design

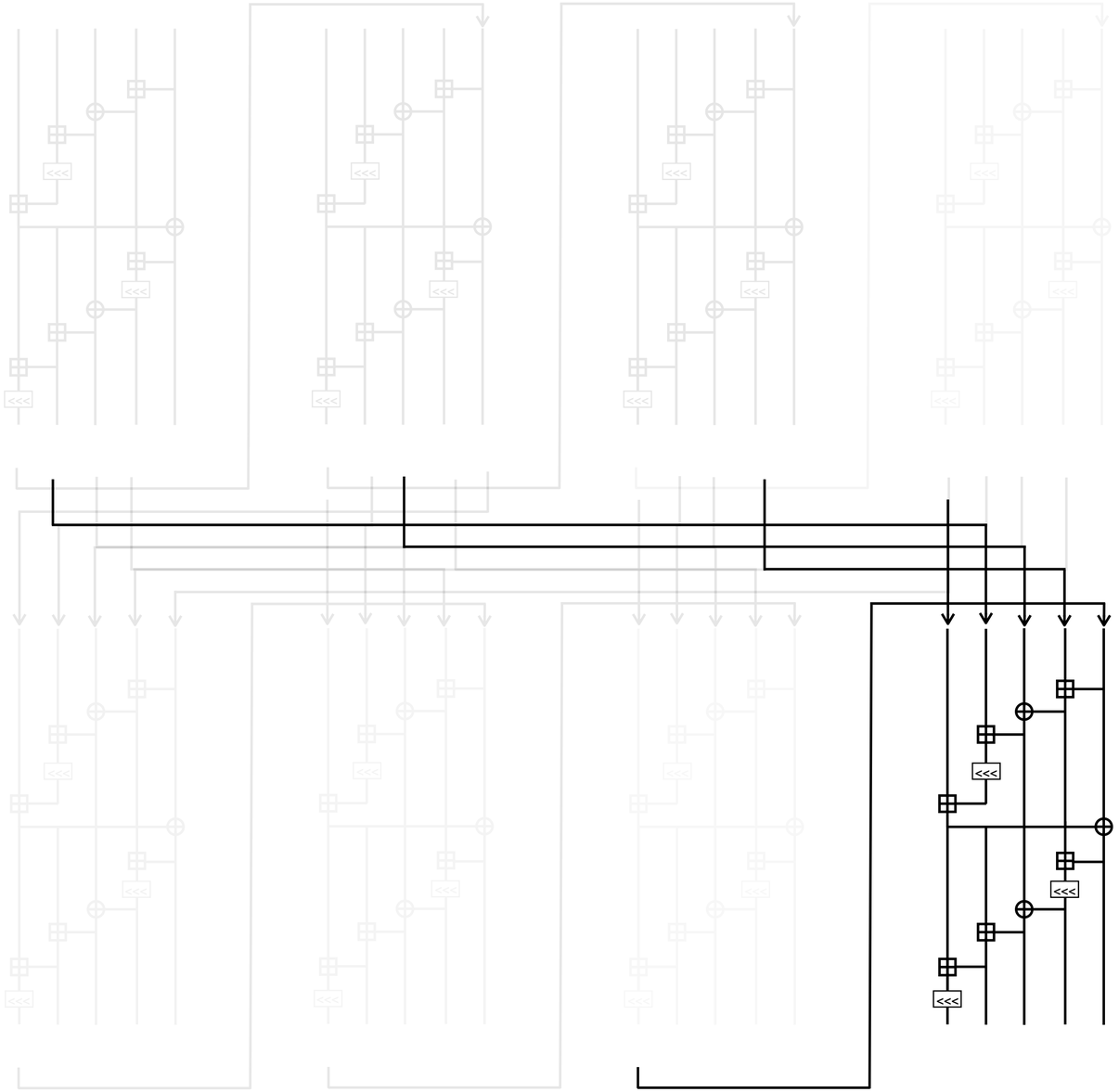
x_0	x_1	x_2	x_3
x_4	x_5	x_6	x_7
x_8	x_9	x_{10}	x_{11}
x_{12}	x_{13}	x_{14}	x_{15}



Forró

Design

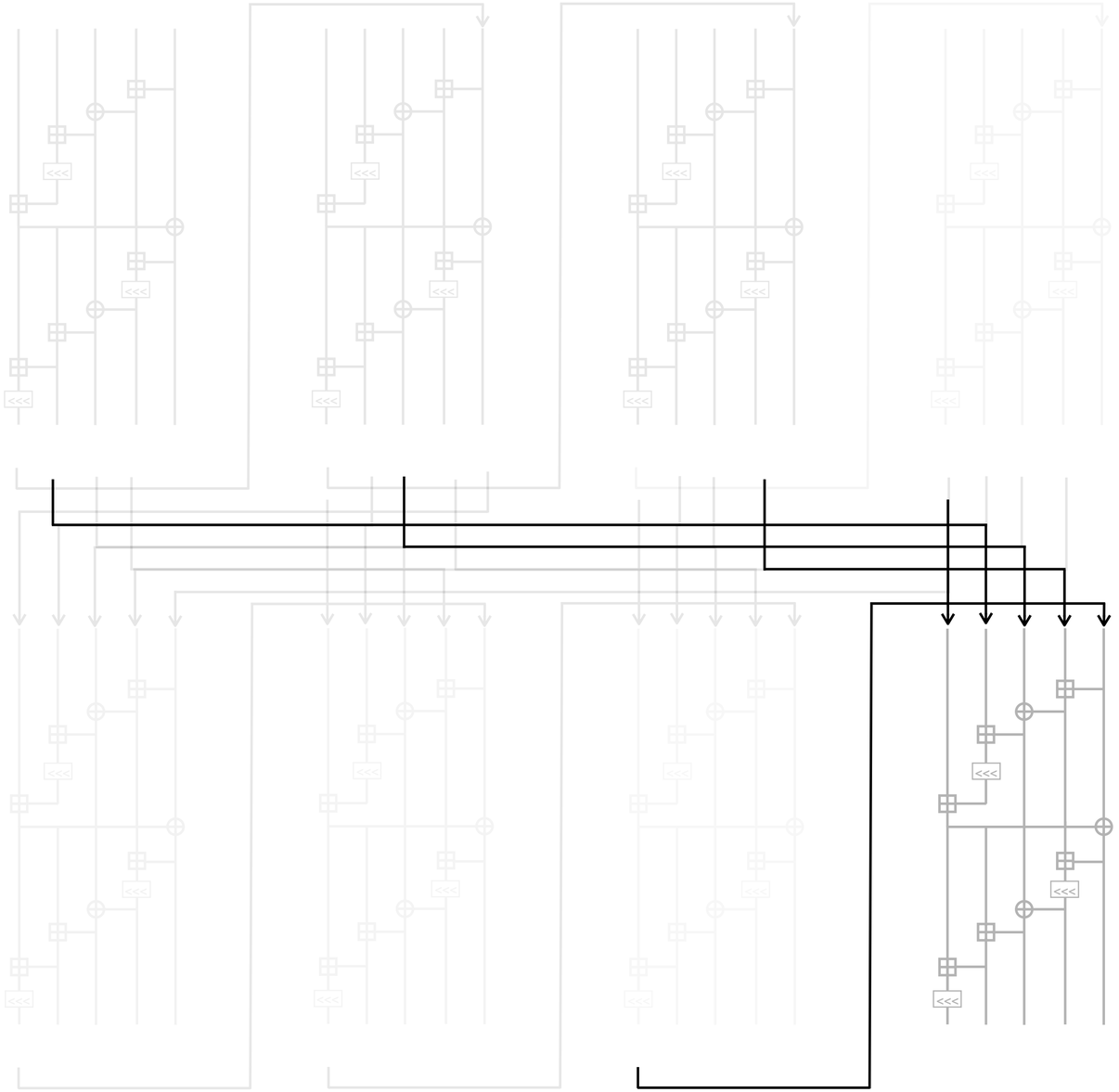
x_0	x_1	x_2	x_3
x_4	x_5	x_6	x_7
x_8	x_9	x_{10}	x_{11}
x_{12}	x_{13}	x_{14}	x_{15}



Forró

Design

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}



Forró

Security and Performance

- We reach up to 5 and 5.25 rounds against Forró by using the state of the art attacks against Salsa and ChaCha
- We attack 5 rounds of Forró in the key-recovery setting why using PNBs
- We implemented Forró in several hardware architectures and we conclude that Forró has slightly better performance than ChaCha and Salsa in hardware using some contained architectures (for example ARMv7).
- In some Intel architectures Forró has a comparable performance to ChaCha and Salsa

Conclusion

- New technique to attack Salsa
  - First time ever reaching 8-round using a “pure” differential-linear distinguisher
  - Our key-recovery attack against 8-round improve previous by a factor of 2^32
- Less rules to derive linear approximations in ChaCha
  - Our attack is 2^10 times faster
- Looking forward to apply in other ciphers
- New cipher with better diffusion called Forró
- New tool https://github.com/MurCoutinho/forro_cipher