Is AEZ v4.1 Sufficiently Resilient Against Key-Recovery Attacks?

Colin Chaigneau[1] and Henri Gilbert[2]

26/04/2017 - Journées C2 - La Bresse, France

UVSQ[1], ANSSI[2], France

Outline

1. AEZ - Overview
2. AEZ - Cryptanalysis
3. Conclusion

AEZ - Overview

AEZ - Summary

- submitted by Hoang, Krovetz and Rogaway to the CAESAR competition in 2014
- encode-then-encipher, plaintext expanded before encryption
- high-resilience against nonce/decryption misuse
  - Robust Authenticated Encryption model
  - not attainable by online AE schemes
- versions submitted:
  - **AEZ v1-3** initial versions - 1st round
  - **AEZ v4.x** targeted version - 2nd (v4.0,v4.1) and 3rd (v4.2) round
  - **AEZ v5** last version - 3rd round

AEZ - Security Claims

Security property	Query complexity (block)	Time complexity
Confidentiality	2^{55}	2^{128}
Authenticity	2^{55}	2^{128}
Robust AE	2^{55}	2^{128}

Data limitation: up to 2^{44} blocks can be processed under the same key (safety margin as compared to 2^{55})

- **nonce and decryption misuse resistant**
- strongest security claims among CAESAR candidates
- no beyond-birthday bound security claim

How resilient is AEZ when approaching the birthday bound?

AEZ - Former Analysis Results / Our contribution

AEZ version	Data complexity (blocks)	Success prob.	Ref.
AEZ v3	$2^{66.6}$	1	[FLS15]
AEZ v3	2^{44}	$2^{-45.2}$	[FLS15]

- **AEZ v3.0**: key-recovery attack by Fuhr, Leurent and Suder [FLS15]
  - nonce-reuse scenario
  - birthday complexity

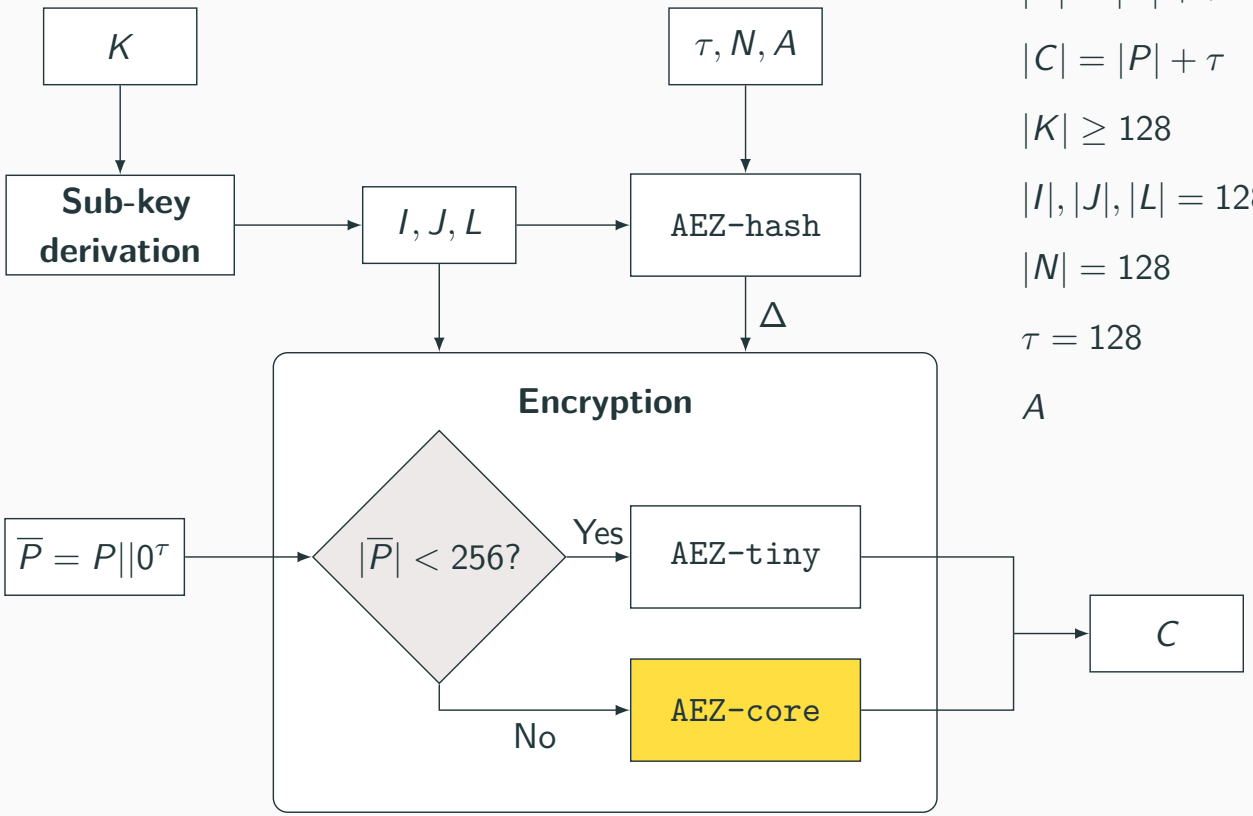
AEZ - Former Analysis Results / Our contribution

AEZ version	Data complexity (blocks)	Success prob.	Ref.
AEZ v3	$2^{66.6}$	1	[FLS15]
AEZ v3	2^{44}	$2^{-45.2}$	[FLS15]
AEZ v4.x	$2^{66.5}$	0.5	Our attack
AEZ v4.x	2^{44}	$2^{-45.7}$	Our attack

- **AEZ v4.x**: **key-recovery attack**
  - modifications between AEZ v3 and v4 aimed at thwarting the [FLS15] attack
  - same attack model and still of birthday complexity
  - targets another part of AEZ

Is AEZ v4.1 Sufficiently Resilient Against Key-Recovery Attacks?

AEZ - Overview



$\lvert\overline{P}\rvert = \lvert P\rvert + \tau$	plaintext (expansion)
$\lvert C\rvert = \lvert P\rvert + \tau$	ciphertext
$\lvert K\rvert \geq 128$	key (default value 384)
$\lvert I\rvert, \lvert J\rvert, \lvert L\rvert = 128$	sub-key
$\lvert N\rvert = 128$	nonce
$\tau = 128$	plaintext expansion
A	associated data

Encode-then-encipher: no tag, zeros appended to P, ciphertext larger than P

AEZ - Tweakable Block Cipher

AEZ uses an AES-based TBC $E_K^{j,i}$

- based on **XE** or **XEX** construction
- given a tweak value (j, i), $E_K^{j,i}(X)$ is defined as follows:

$$E_K^{j,i}(X) = \overbrace{\underbrace{\texttt{AES4}(X \oplus O_{in}^{j,i})}_{\textbf{XEX}} \oplus O_{out}^{j,i}}^{\textbf{XE}} \quad \boxed{j, i}$$

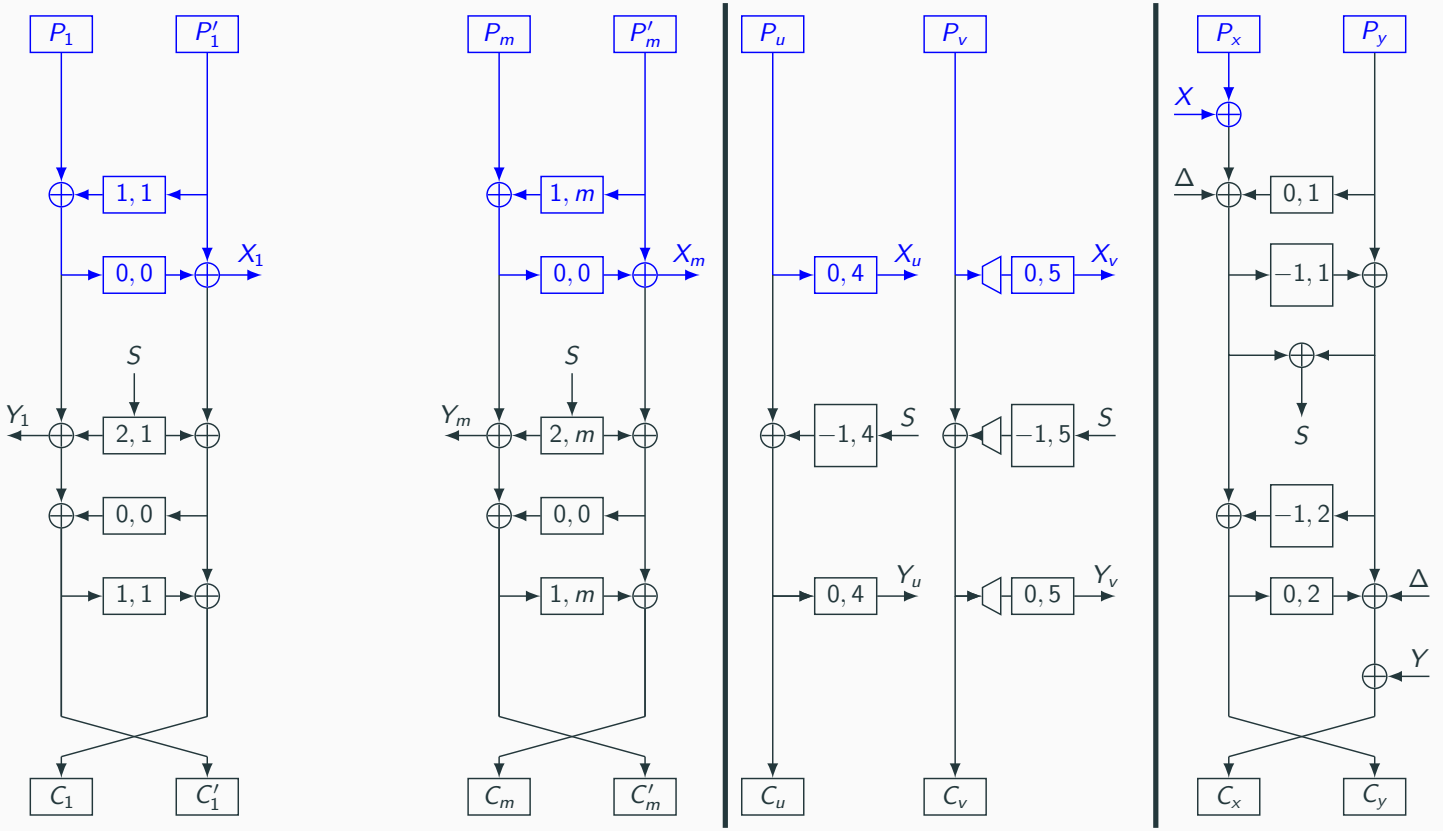
$O_\bullet^{i,j}$ depend linearly on I, J and L

AES4: 4-round AES, good differential and linear security bounds for independent sub-keys.

AEZ-core

$$\overline{P} = P||0^{\tau}$$

$$\overline{P} = P_1 P_1' \;||\; \ldots \;||\; P_m P_m' \;||\; P_u[P_v] \;||\; P_x P_y$$

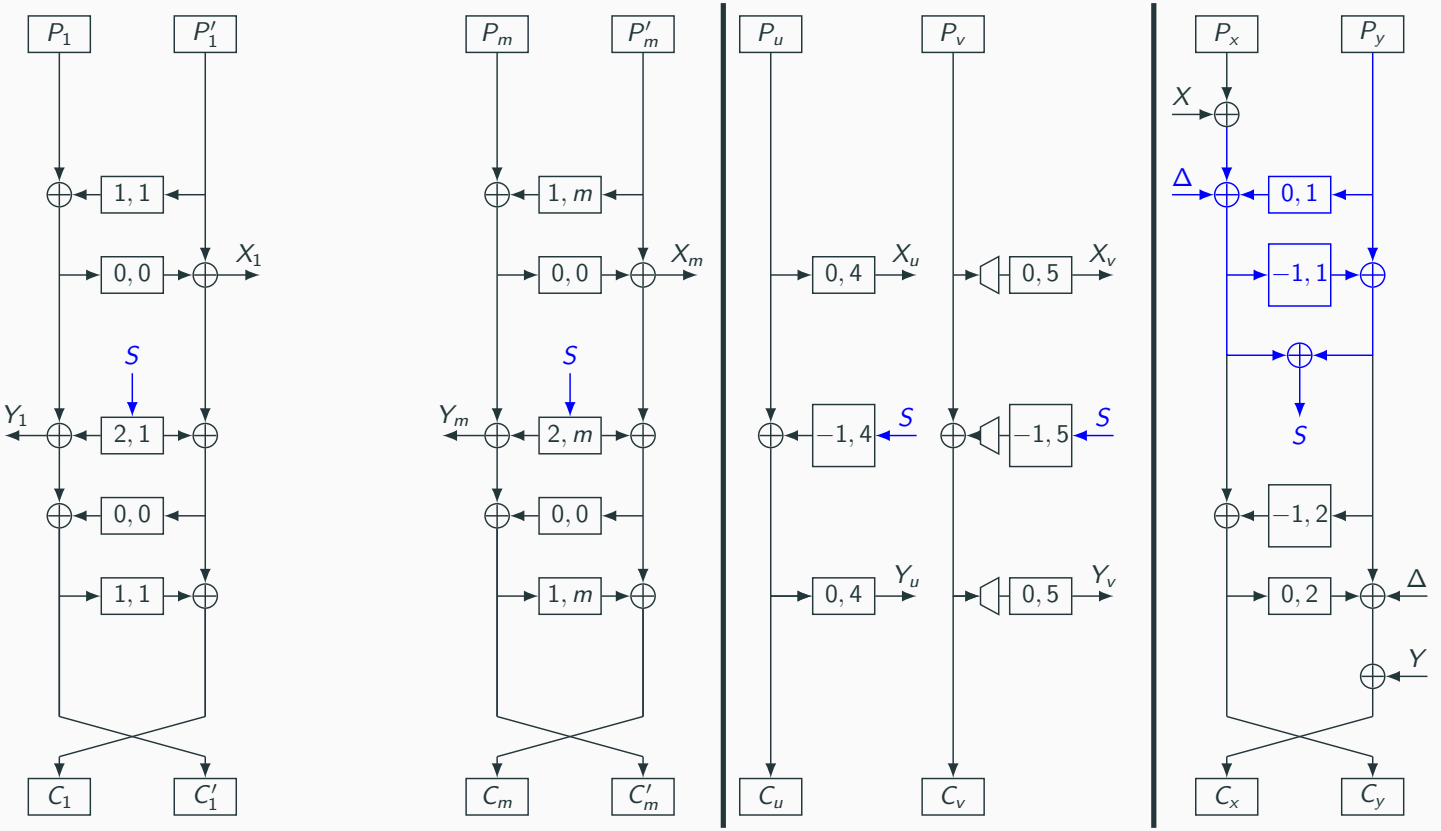


Note: $X = X_1 \oplus \ldots \oplus X_m \oplus X_u \oplus X_v$

AEZ-core

$$\overline{P} = P||0^{\tau}$$

$$\overline{P} = P_1 P_1' \;||\; \ldots \;||\; P_m P_m' \;||\; P_u[P_v] \;||\; P_x P_y$$

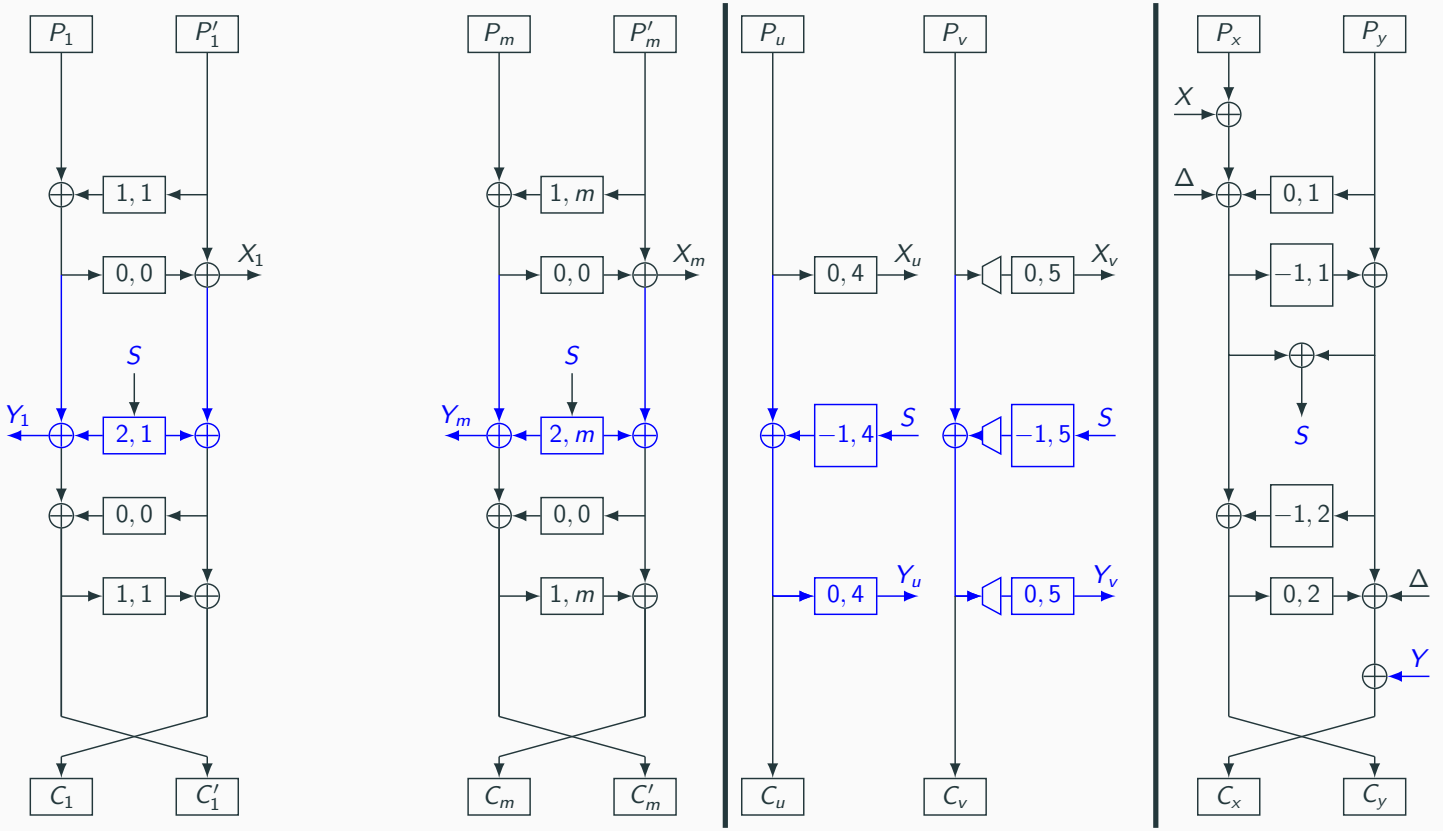


Note: $\Delta = \texttt{AEZ-hash}(K, T, \tau)$

AEZ-core

$$\overline{P} = P||0^{\tau}$$

$$\overline{P} = P_1 P_1' \;||\; \ldots \;||\; P_m P_m' \;||\; P_u[P_v] \;||\; P_x P_y$$

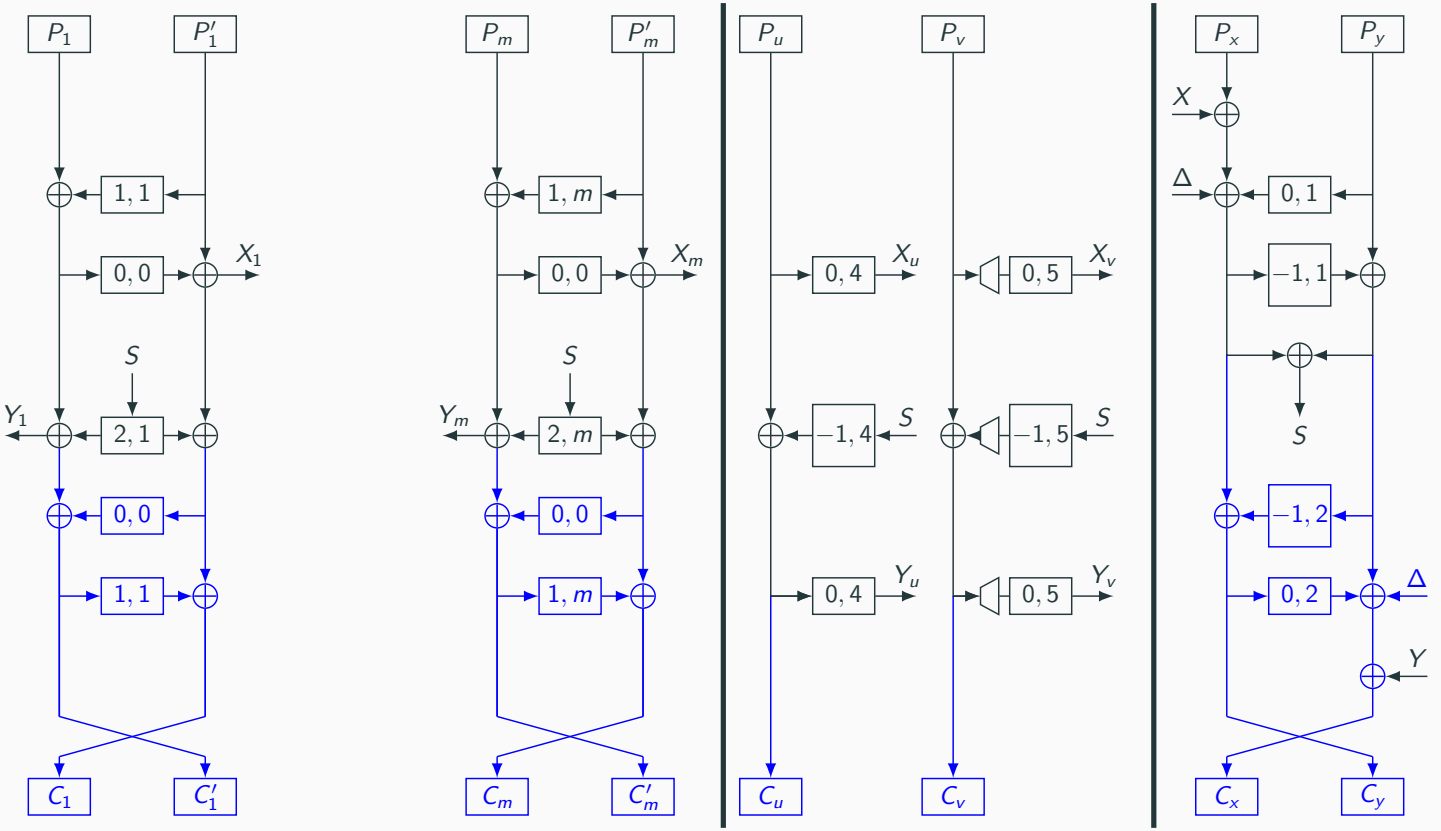


Note: $Y = Y_1 \oplus \ldots \oplus Y_m \oplus Y_u \oplus Y_v$

AEZ-core

$$\overline{P} = P||0^{\tau}$$

$$\overline{P} = P_1 P_1' \;||\; \ldots \;||\; P_m P_m' \;||\; P_u[P_v] \;||\; P_x P_y$$



Note: $\Delta = \texttt{AEZ-hash}(K, T, \tau)$

AEZ - Cryptanalysis

Our attack - Overall Structure

Attack	Data complexity (blocks)	Success prob.
Phase 1	2^{44} $2^{66.5}$	$2^{-45.6}$ 0.5
Phase 2	$2^{34.6}$	1

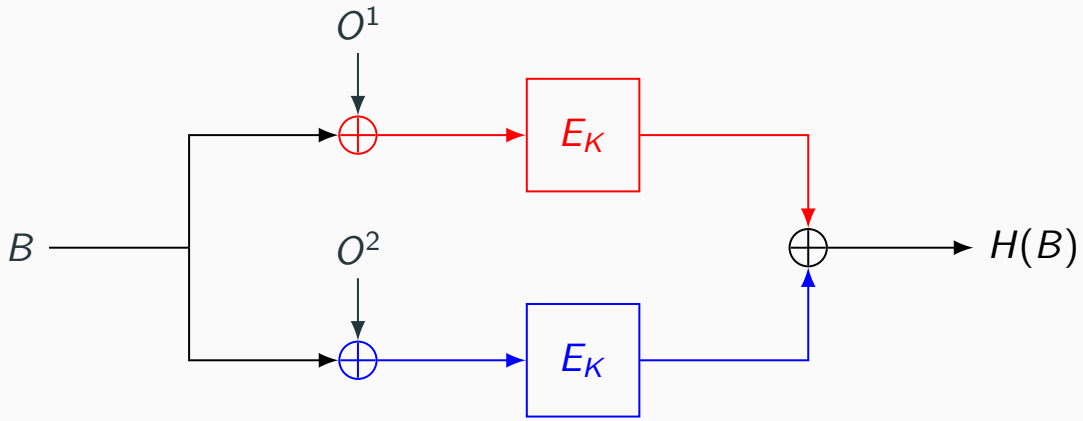
Full secret material (namely I, J, L) can be retrieved with a 2-phase nonce-reuse attack

- **Phase 1:** birthday-bound attack to recover sub-key I
- **Phase 2:** differential attack on an appropriate `AES4` instance to recover full secret material

Note: J and L can also be recovered with a birthday attack

Phase 1 - Birthday-Bound Attack

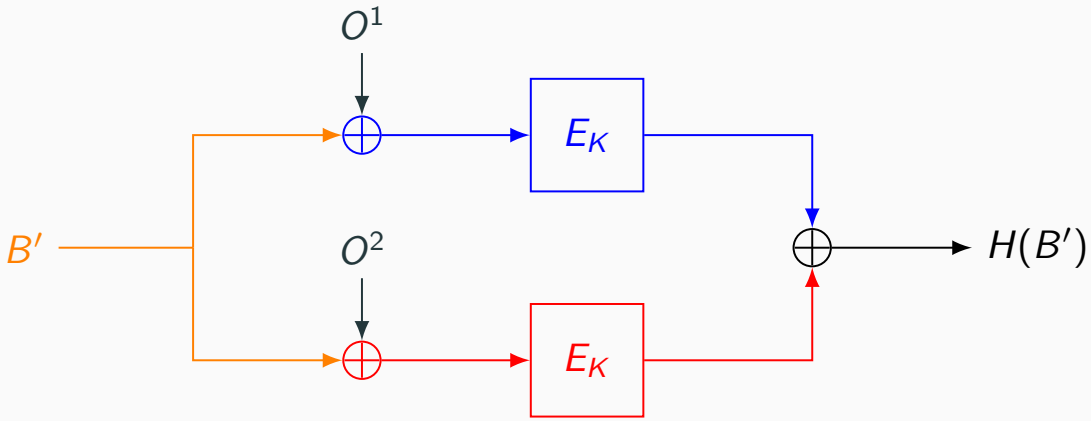
Let $H(B) = E_K(B \oplus O^1) \oplus E_K(B \oplus O^2)$



If $B' = B \oplus O^1 \oplus O^2$ we remark that $H(B) = H(B')$, birthday complexity to recover $O^1 \oplus O^2$

Phase 1 - Birthday-Bound Attack

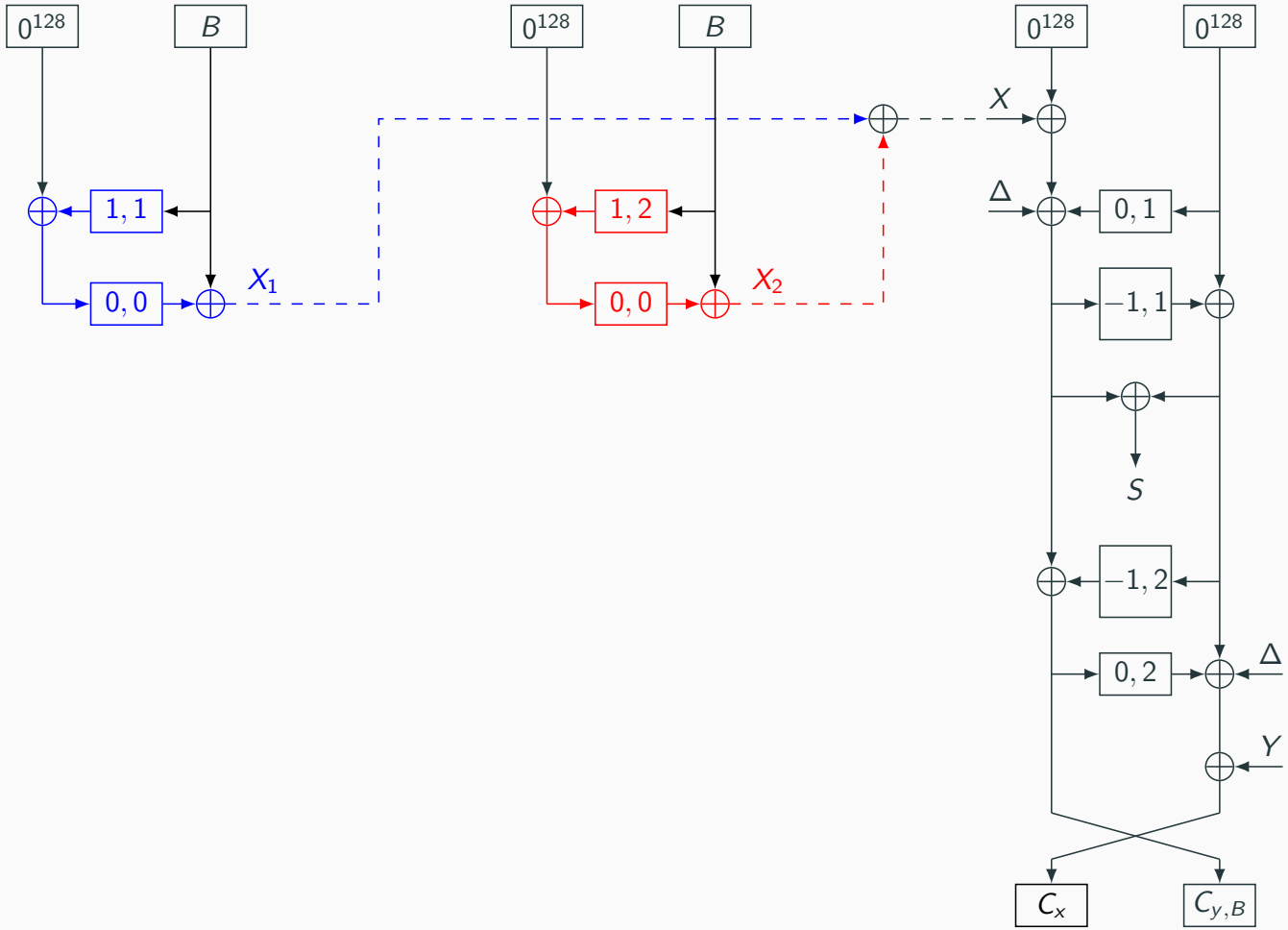
Let $H(B) = E_K(B \oplus O^1) \oplus E_K(B \oplus O^2)$



If $B' = B \oplus O^1 \oplus O^2$ we remark that $H(B) = H(B')$, birthday complexity to recover $O^1 \oplus O^2$

Phase 1 - Recovery of Sub-key I

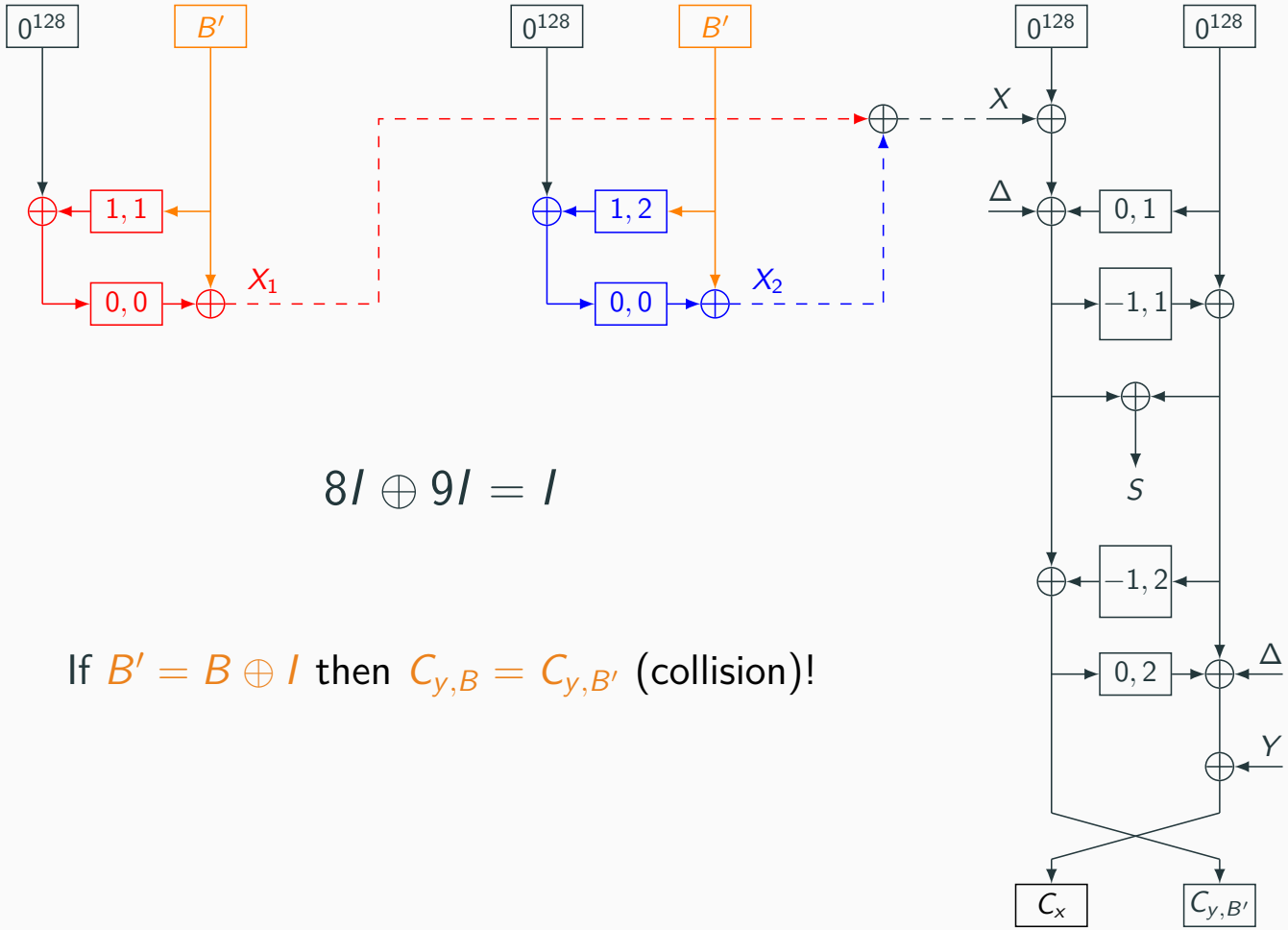
Encryption associated with B



Note: $\boxed{1,1} = \mathtt{AES4}_K(B \oplus 8I)$ $\boxed{1,2} = \mathtt{AES4}_K(B \oplus 9I)$

Phase 1 - Recovery of Sub-key I

Encryption associated with $B' = B \oplus I$



$$8I \oplus 9I = I$$

If $B' = B \oplus I$ then $C_{y,B} = C_{y,B'}$ (collision)!

Note: $\boxed{1,1} = \texttt{AES4}_K(B \oplus 8I)$ $\boxed{1,2} = \texttt{AES4}_K(B \oplus 9I)$

Phase 1 - Recovery of Sub-key I

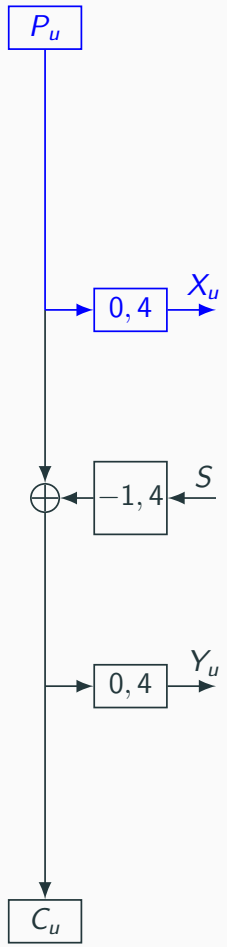
Recovery of Sub-key I

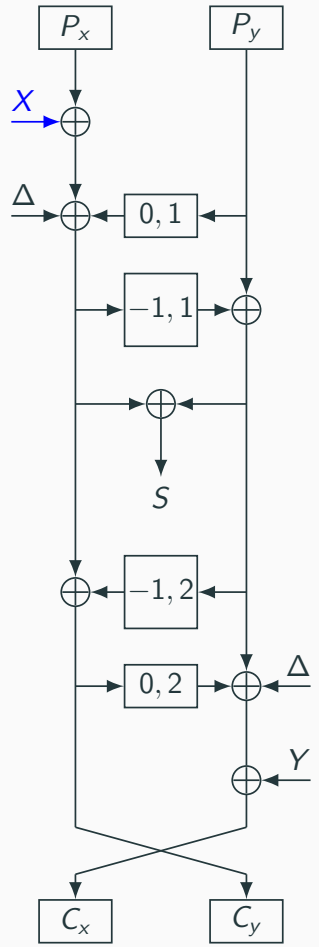
1. For MANY values of B, collect the corresponding values $C_{y,B}$
2. If a collision occurs, i.e. $C_{y,B} = C_{y,B'}$, this suggests $I = B \oplus B'$ (false alarms can be easily discarded)

Success probability	**MANY (block)**
0.5	$2^{66.5}$
$2^{-45.6}$	2^{44}

Phase 2 - From Sub-key I to Sub-keys J and L

- **Phase 1:** sub-key I recovery
- **Phase 2 (NOW):** leverage the knowledge of I to recover sub-keys J and L
- **Targeted part:** AES4 on the P_u part



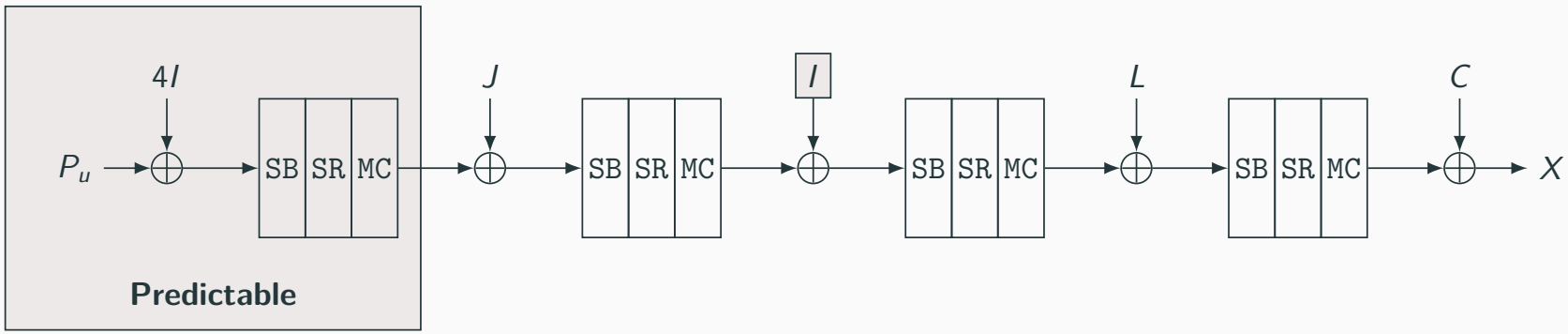


Phase 2 - Appropriate AES4 instance

Let $\overline{P} = \underbrace{P_u \,||\, 0^{128}}_{P_u, P_v} \,||\, \underbrace{P_x \,||\, 0^{\tau}}_{P_x, P_y}$, we have

$$X = \mathtt{AES4}_K(P_u \oplus 4I) \oplus C, \; C \text{ constant}$$

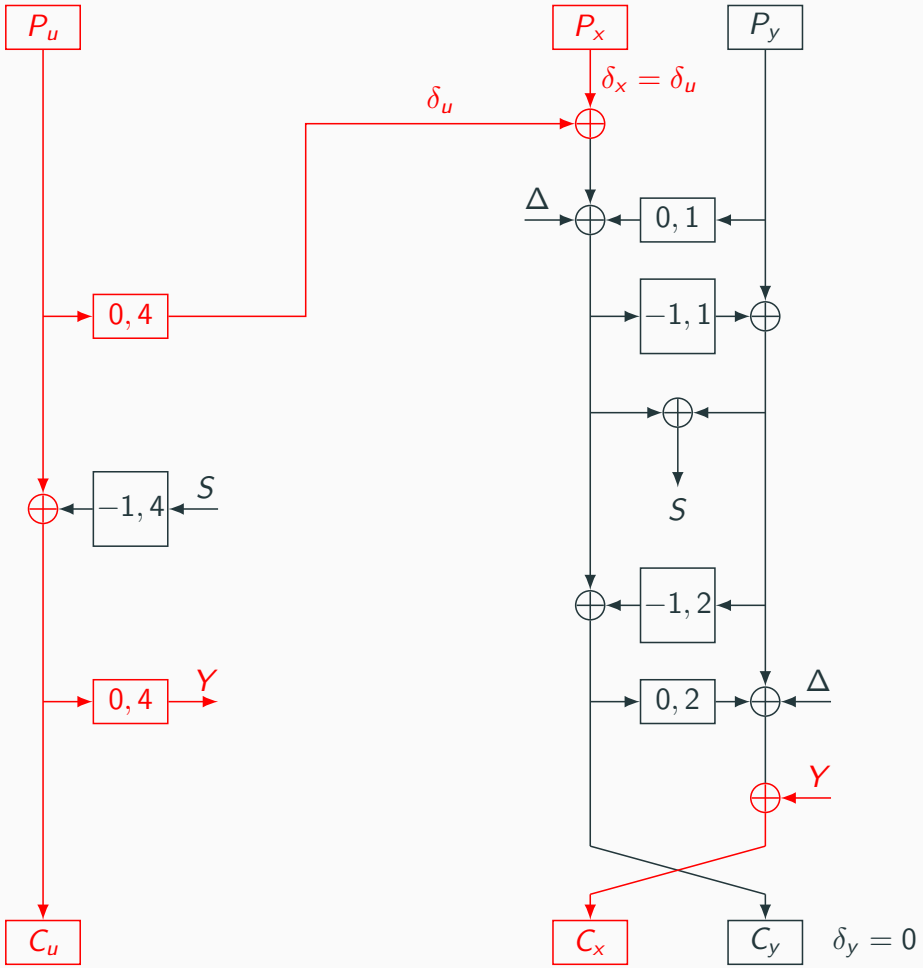
Since the sub-key I is known from the Phase 1 we have



Differential attack on a 3-round AES4

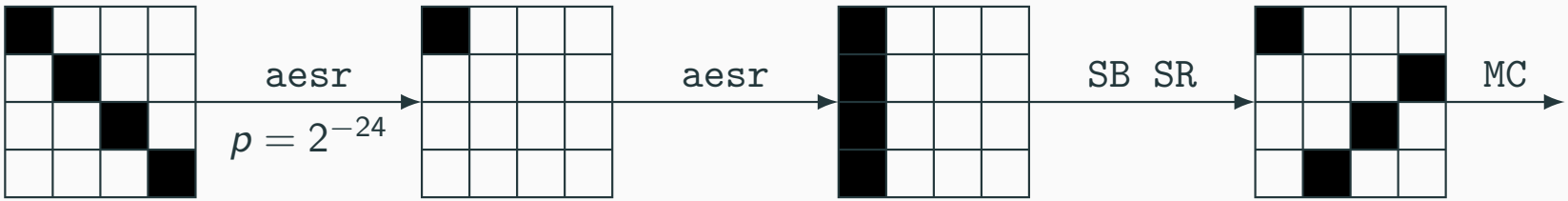
Phase 2 - AES4 Attack - Difference Propagation

Inject differences on P_u and P_x

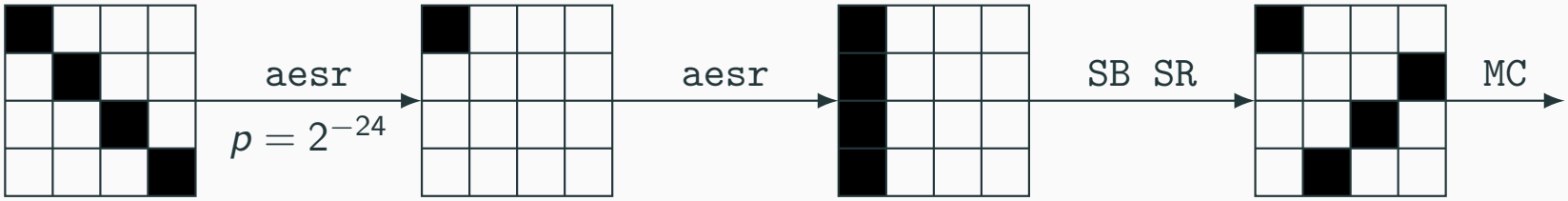


if $\delta_u = \delta_x$ then $\delta_y = 0$

Phase 2 - AES4 Attack - 4-1-4 Differential Pattern



Phase 2 - AES4 Attack - Use Of Structures



PROBLEM: $2^{32} \times 2^{32} = 2^{64}$ tests, too much!

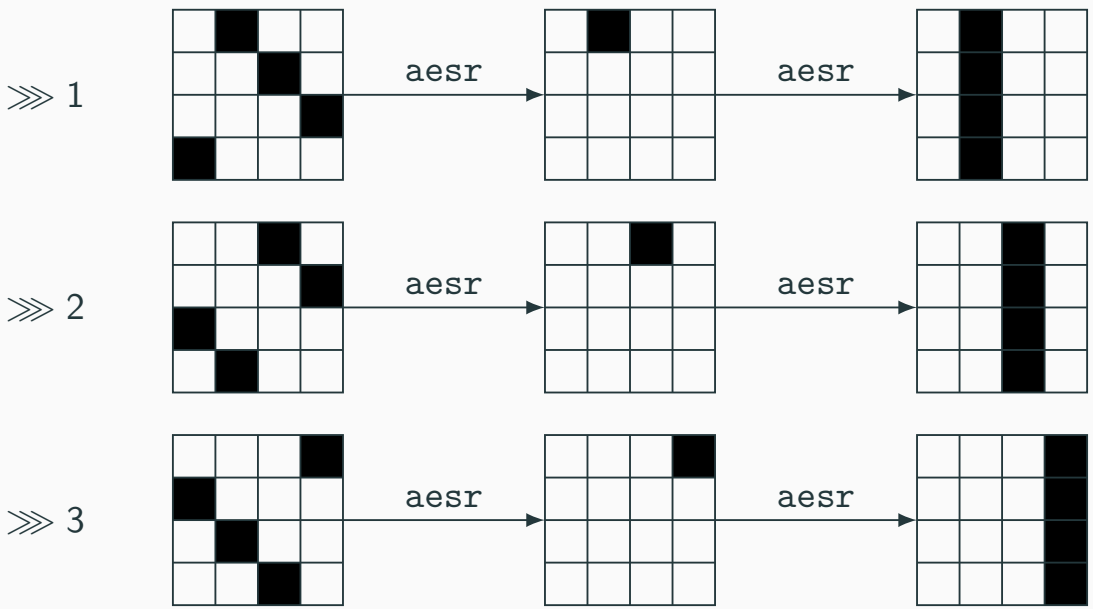
SOLUTION: use $(P_u, P_x) \in \mathcal{U} \times (\mathcal{X} \cup \mathcal{X}')$ where $\mathcal{U}, \mathcal{X}$ and $\mathcal{X}'$ are small structures

- reduces the number of input values P_u to 2^{13}
- due to the MixColumns linearity, the number of output values P_x can be reduced to 2×2^{16} values

RESULT: only $2 \times 2^{13} \times 2^{16} = 2^{30}$ tests to find a good pair of differences!

Phase 2 - AES4 Attack - 4-1-4 patterns

- a good pair of differences reduce the number of possible values for 4 bytes of J and L
- rotating the columns of the 4-1-4 pattern allows to target the other parts of J and L



Summary - Attack Complexity

Attack	Data complexity (blocks)	Success prob.
Phase 1	2^{44}	$2^{-45.6}$
	$2^{66.5}$	0.5
Phase 2	$2^{34.6}$	1

- Key search: time complexity $2^{44} \Rightarrow$ success probability 2^{-84}

Data complexity (block)	Success probability
2^{44}	$2^{-45.6}$
$2^{66.5}$	0.5

Conclusion

Conclusion - AEZ v4.x security

Our attack highlights some security limitations of AEZ v4.1

- modifications made to AEZ v3 to thwart the key-recovery attack [FLS15] were inefficient

Conclusion - AEZ v4.x security

Our attack highlights some security limitations of AEZ v4.1

- modifications made to AEZ v3 to thwart the key-recovery attack [FLS15] were inefficient
- each sub-key can be recovered by a birthday-bound attack

Conclusion - AEZ v4.x security

Our attack highlights some security limitations of AEZ v4.1

- modifications made to AEZ v3 to thwart the key-recovery attack [FLS15] were inefficient
- each sub-key can be recovered by a birthday-bound attack
- the three sub-keys can be recovered with the knowledge of only one

Conclusion - AEZ v4.x security

Our attack highlights some security limitations of AEZ v4.1

- modifications made to AEZ v3 to thwart the key-recovery attack [FLS15] were inefficient
- each sub-key can be recovered by a birthday-bound attack
- the three sub-keys can be recovered with the knowledge of only one
- does not contradict the designers' security claims for AEZ ...

Conclusion - AEZ v4.x security

Our attack highlights some security limitations of AEZ v4.1

- modifications made to AEZ v3 to thwart the key-recovery attack [FLS15] were inefficient
- each sub-key can be recovered by a birthday-bound attack
- the three sub-keys can be recovered with the knowledge of only one
- does not contradict the designers' security claims for AEZ ...
- ... but it raises some doubts about the resilience of AEZ against key-recovery attacks with birthday complexity

Conclusion - AEZ v4.x security

Our attack highlights some security limitations of AEZ v4.1

- modifications made to AEZ v3 to thwart the key-recovery attack [FLS15] were inefficient
- each sub-key can be recovered by a birthday-bound attack
- the three sub-keys can be recovered with the knowledge of only one
- does not contradict the designers' security claims for AEZ ...
- ... but it raises some doubts about the resilience of AEZ against key-recovery attacks with birthday complexity

So

Is AEZ v4.1 Sufficiently Resilient Against Key-Recovery Attacks?

Conclusion - What about AEZ v5?

- **Main modification (March 2017):** the offsets of the tweakable block cipher were modified and simplified

$$E_K^{j,i}(X) = \texttt{AES4}_K(X \oplus j \cdot J \oplus 2^{\lceil i/8 \rceil} \cdot I \oplus (i \bmod 8) \cdot L)$$

  in order to thwart attacks resulting from a recently spotted colliding offsets issue by Bonnetain et al. [BDDJLMS17]

Our attack has to be tweaked but still works:

- **Phase 1:** birthday-bound attack on `AEZ-prf` to obtain the value $3I \oplus 6L$, then compute $2I \oplus 4L$
- **Phase 2:** differential attack, knowledge of $2I \oplus 4L$ cancels one turn of `AES4`, recovery of I, J and L

Conclusion - What about AEZ v5?

Complexities are marginally increased (but success probability still abnormally high!)

Version	Data complexity (block)	Success probability
AEZ v4.x	2^{44} $2^{66.5}$	$2^{-45.6}$ 0.5
AEZ v5	2^{44} $2^{68.2}$	2^{-49} 0.5

Thanks for your attention ☻