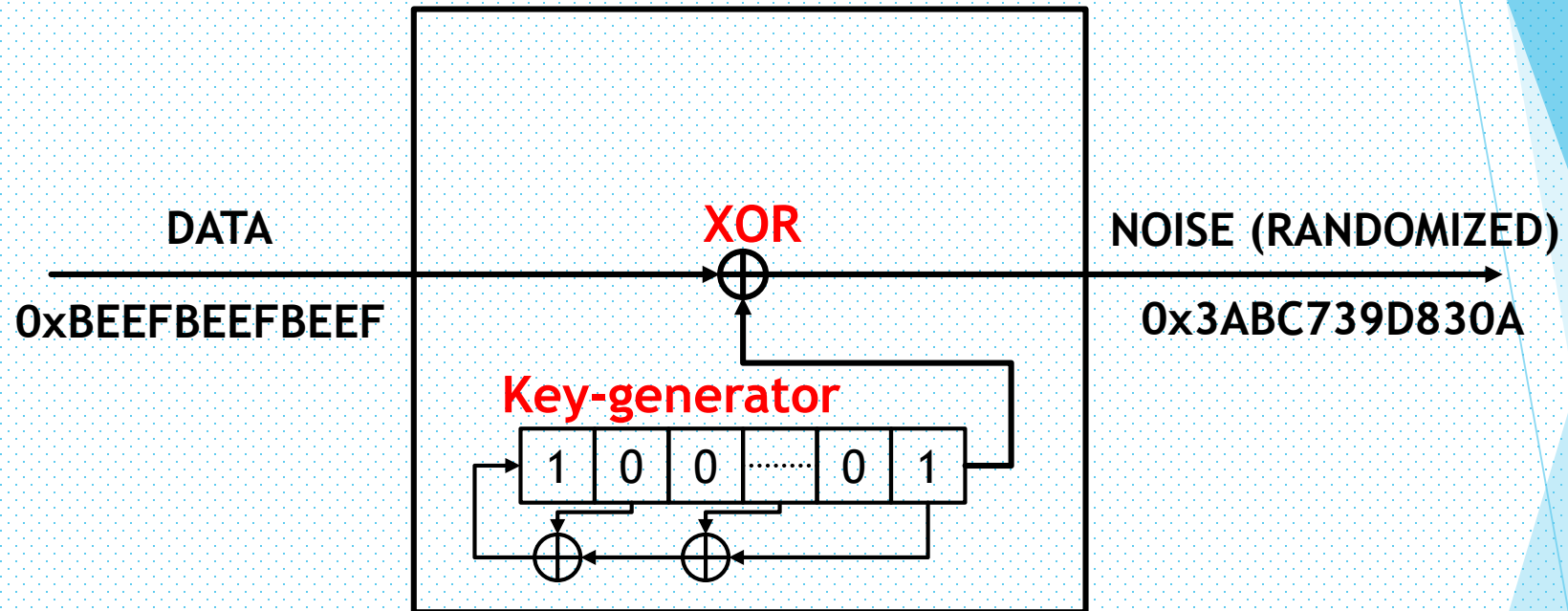


SPARE AREA XOR KEY EXTRACTION

Krzysztof (Chris) Przewoźnik- Rusolut

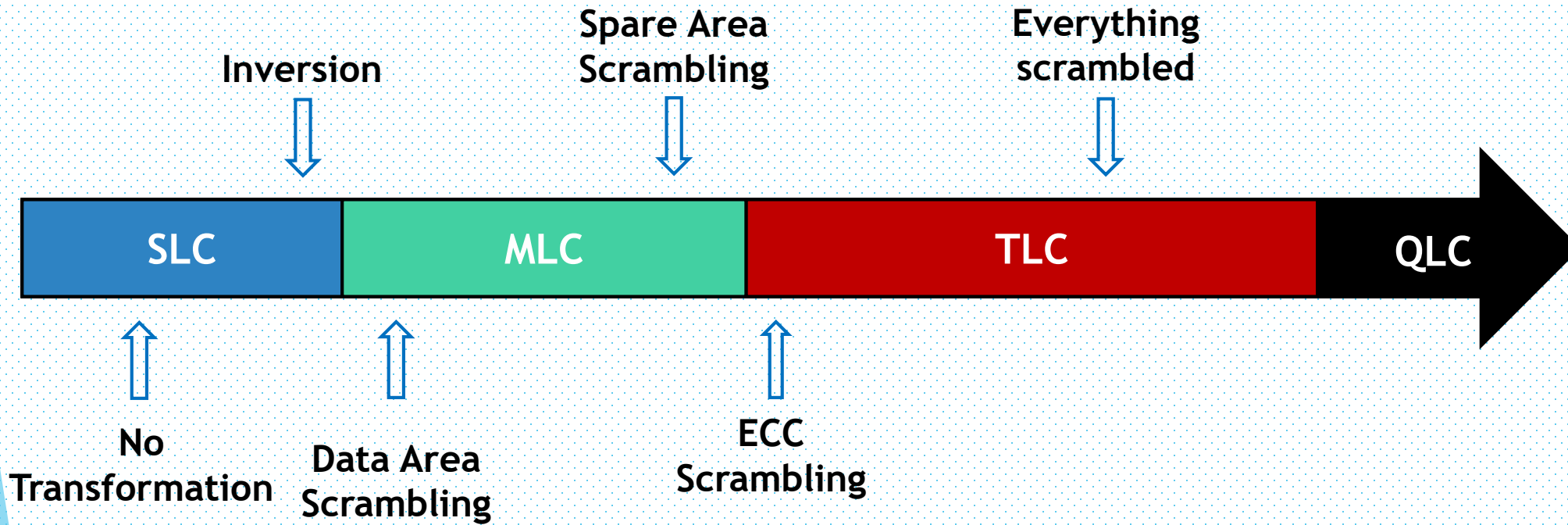
SCRAMBLING

CONTROLLER



Scrambling- cyclic data randomization algorithm protecting NAND memory from charges leaks.

DATA OPTIMIZATION TIMELINE



PAGE STRUCTURE

Phison



Silicon Motion, Innostor



Sandisk

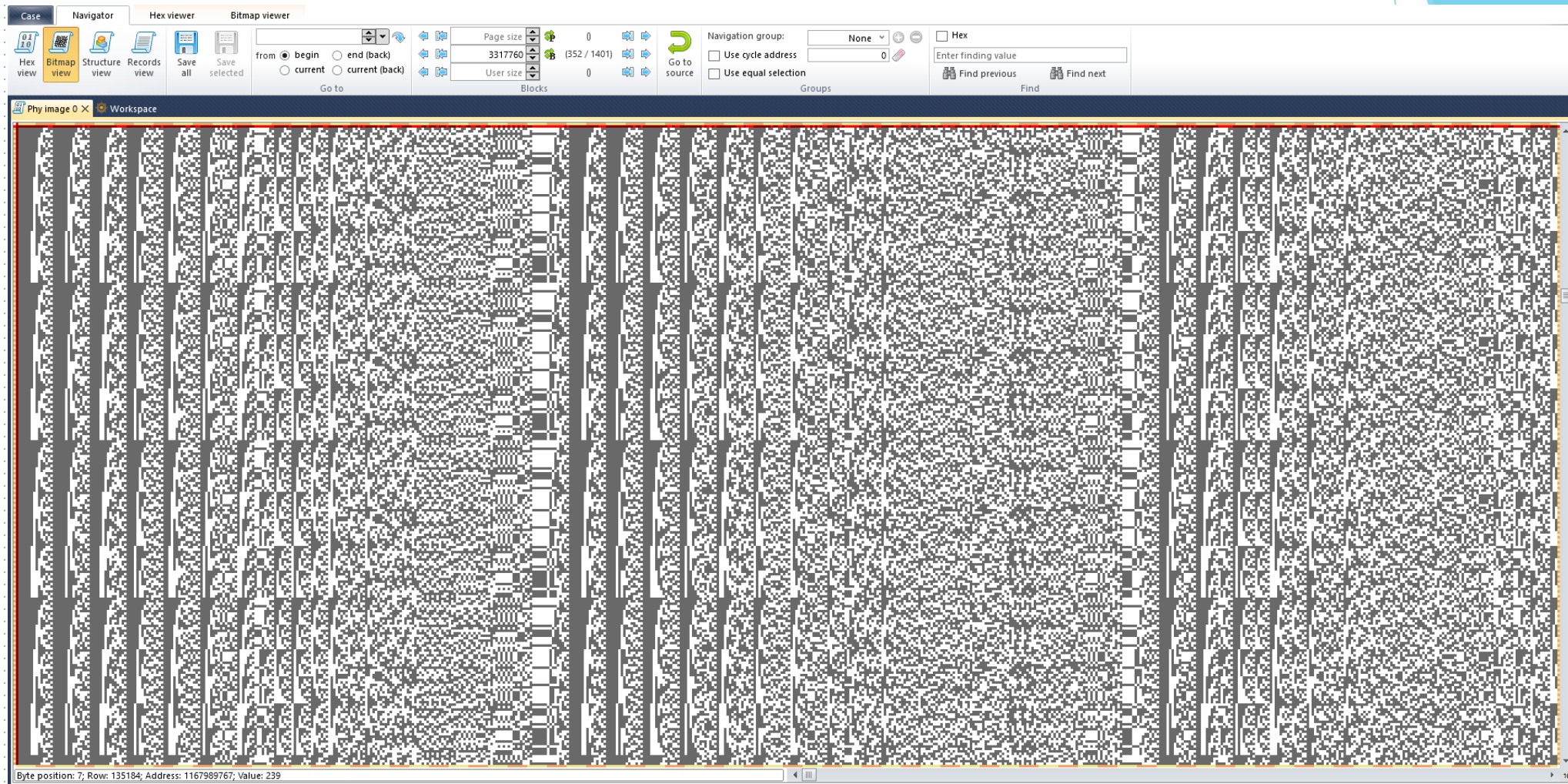


ATJ3115 (Voice Recorder)



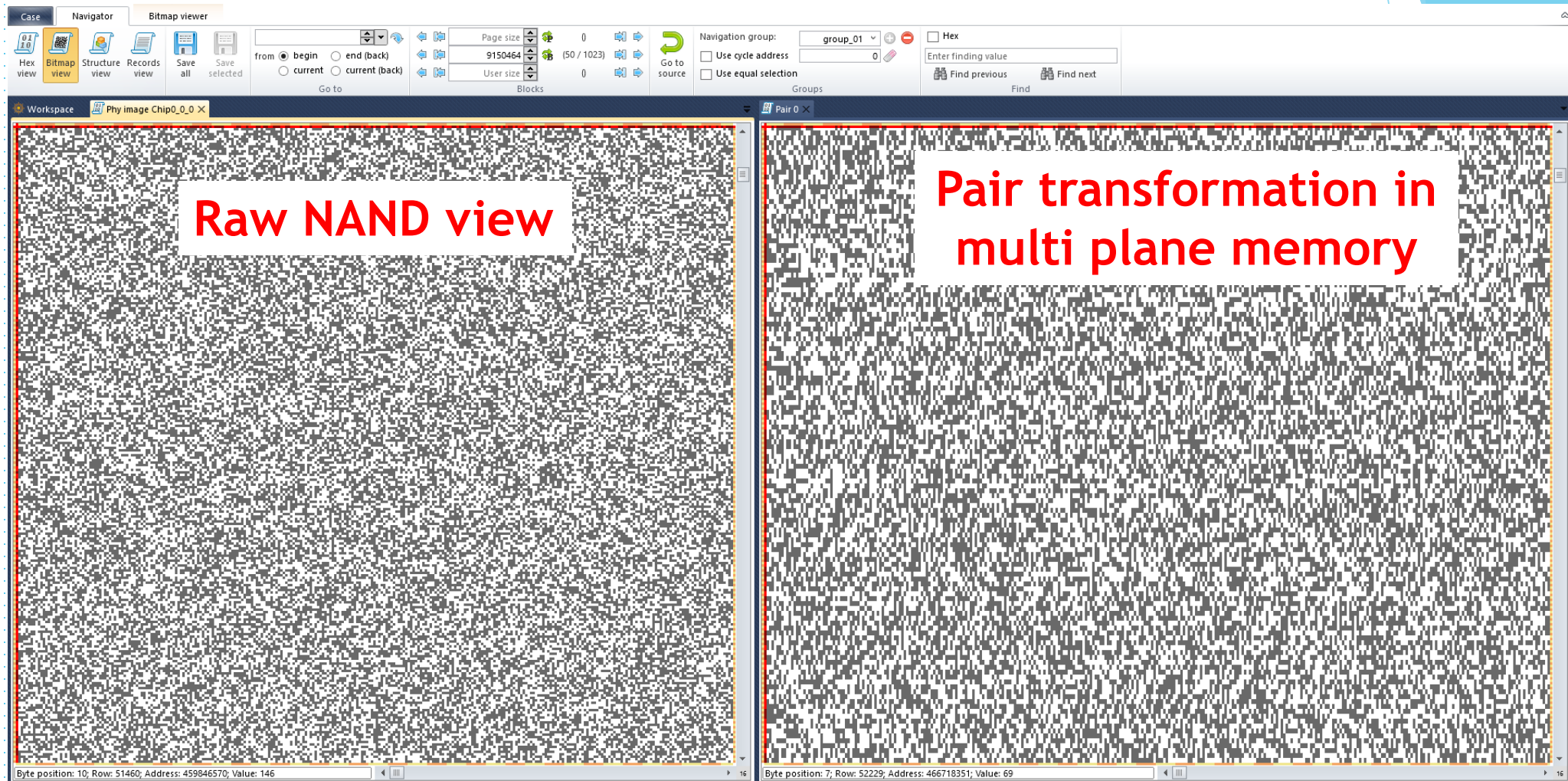
XOR KEY RECOGNITION

Pattern XOR key



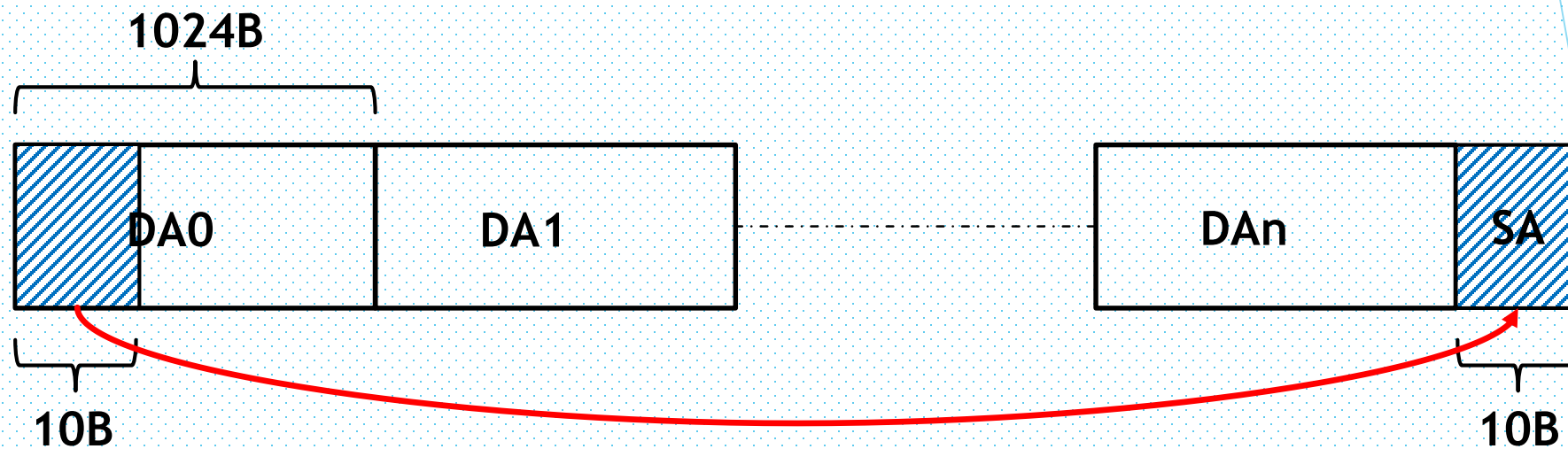
XOR KEY RECOGNITION

„Noise-like” XOR key



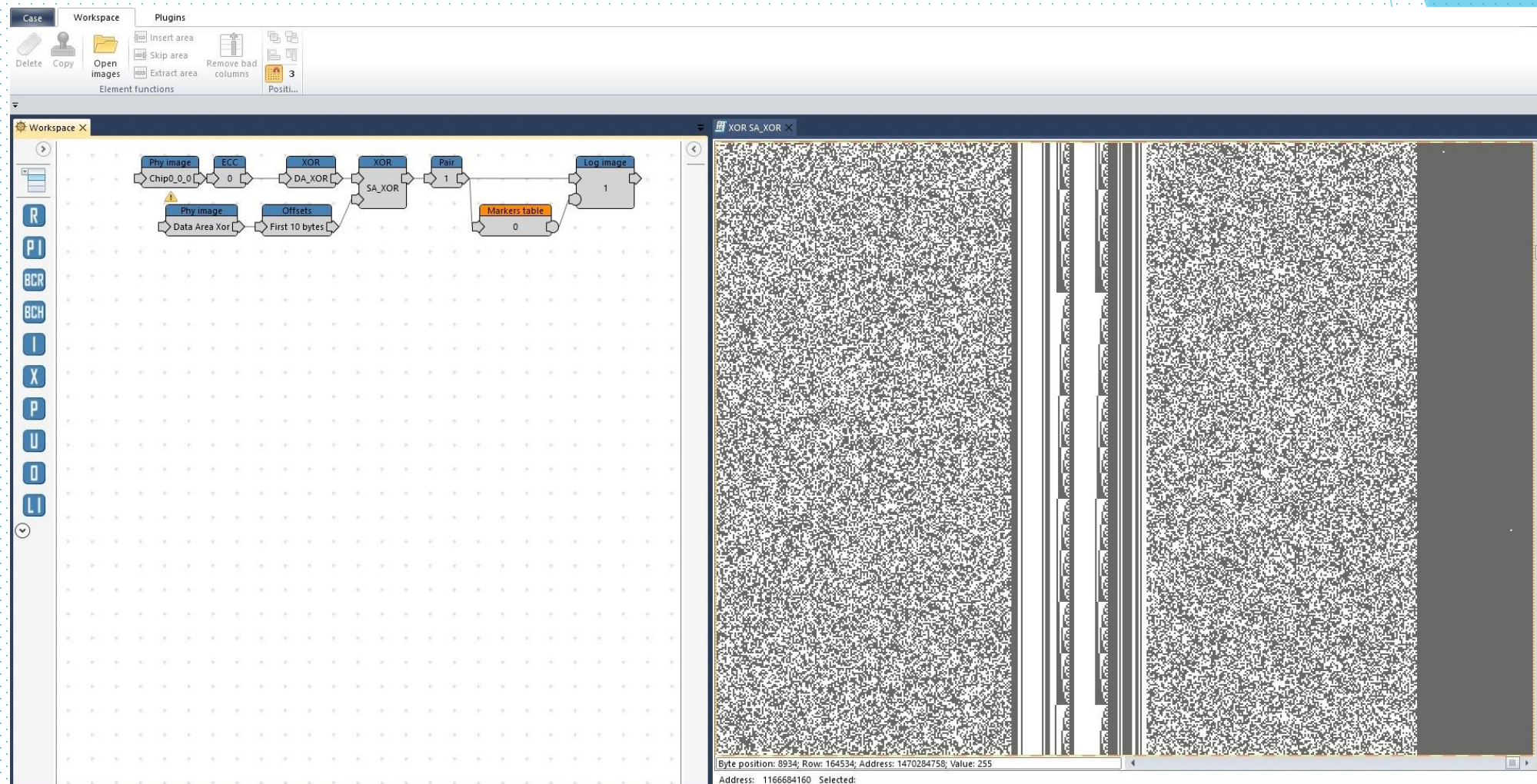
TYPES OF XOR KEY FOR SA

SA XOR key extacted from Data Area



TYPES OF XOR KEY FOR SA

SA XOR key extacted from Data Area



TYPES OF XOR KEY FOR SA

SA XOR key extacted from Data Area

Pros

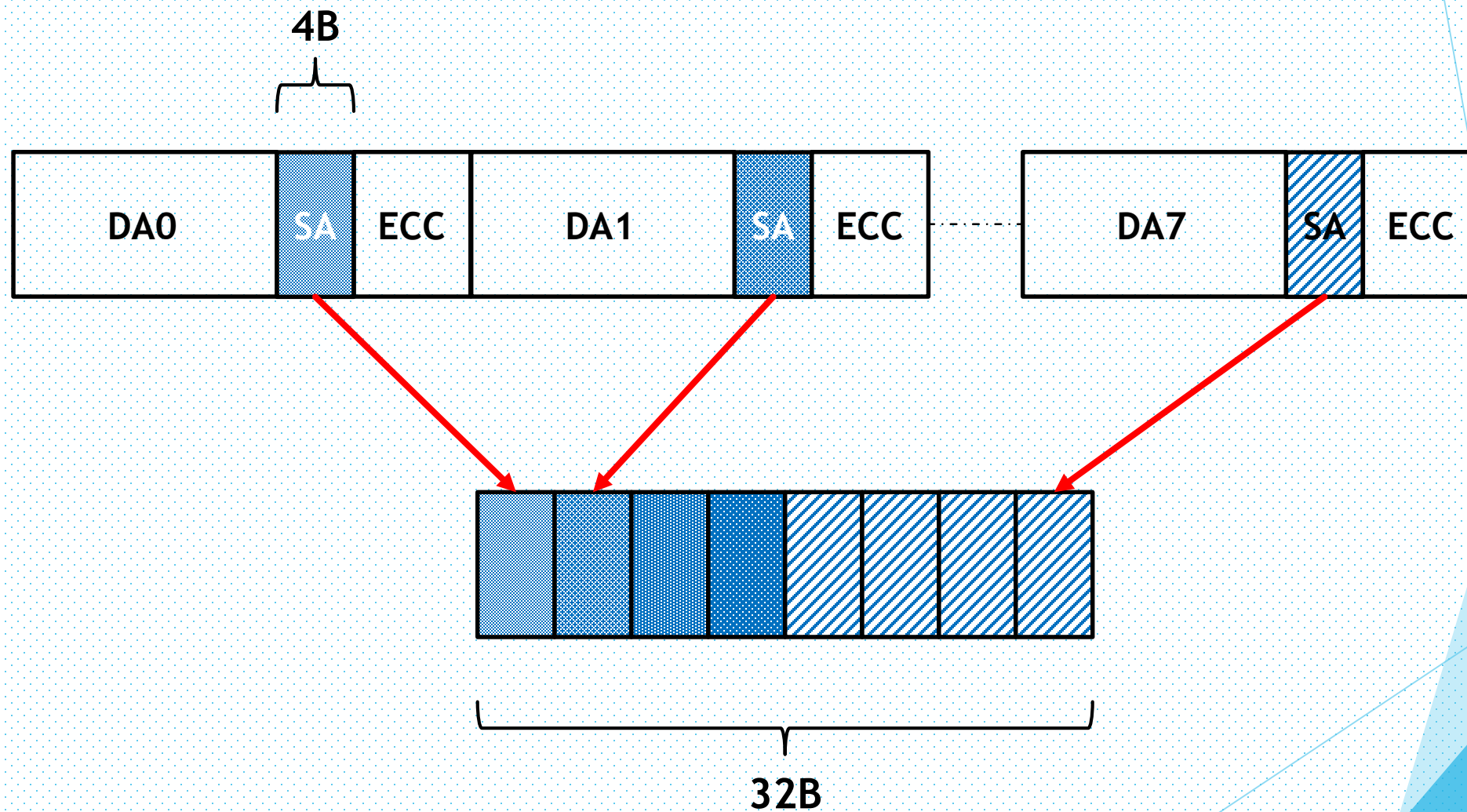
- ▶ 100% pure SA xor key
- ▶ SA is not distorted
- ▶ „Hot data” blocks can be used in structure build
- ▶ Easy extraction

Cons

- ▶ absent

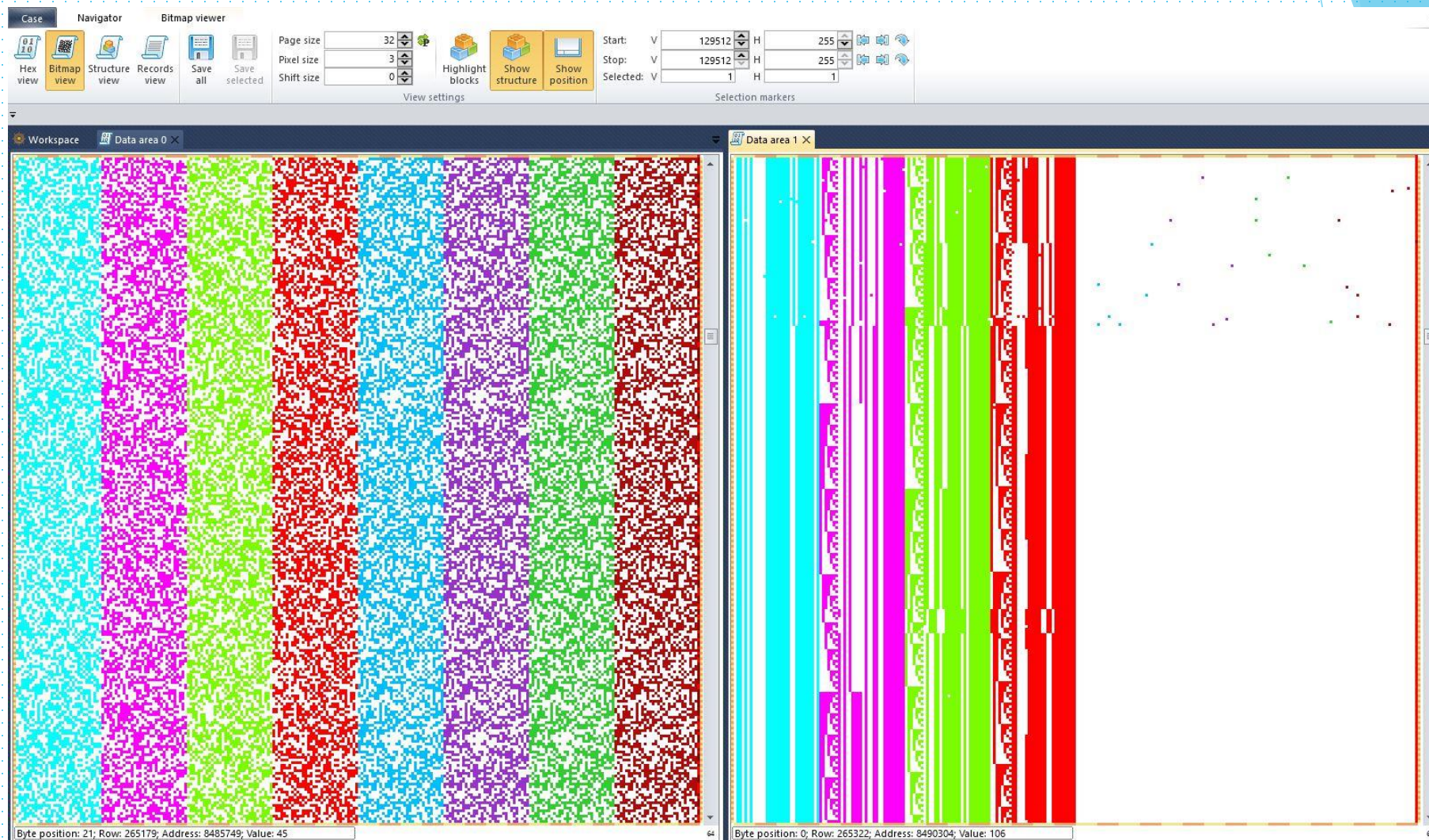
TYPES OF XOR KEY FOR SA

SA XOR key extacted from empty SA part



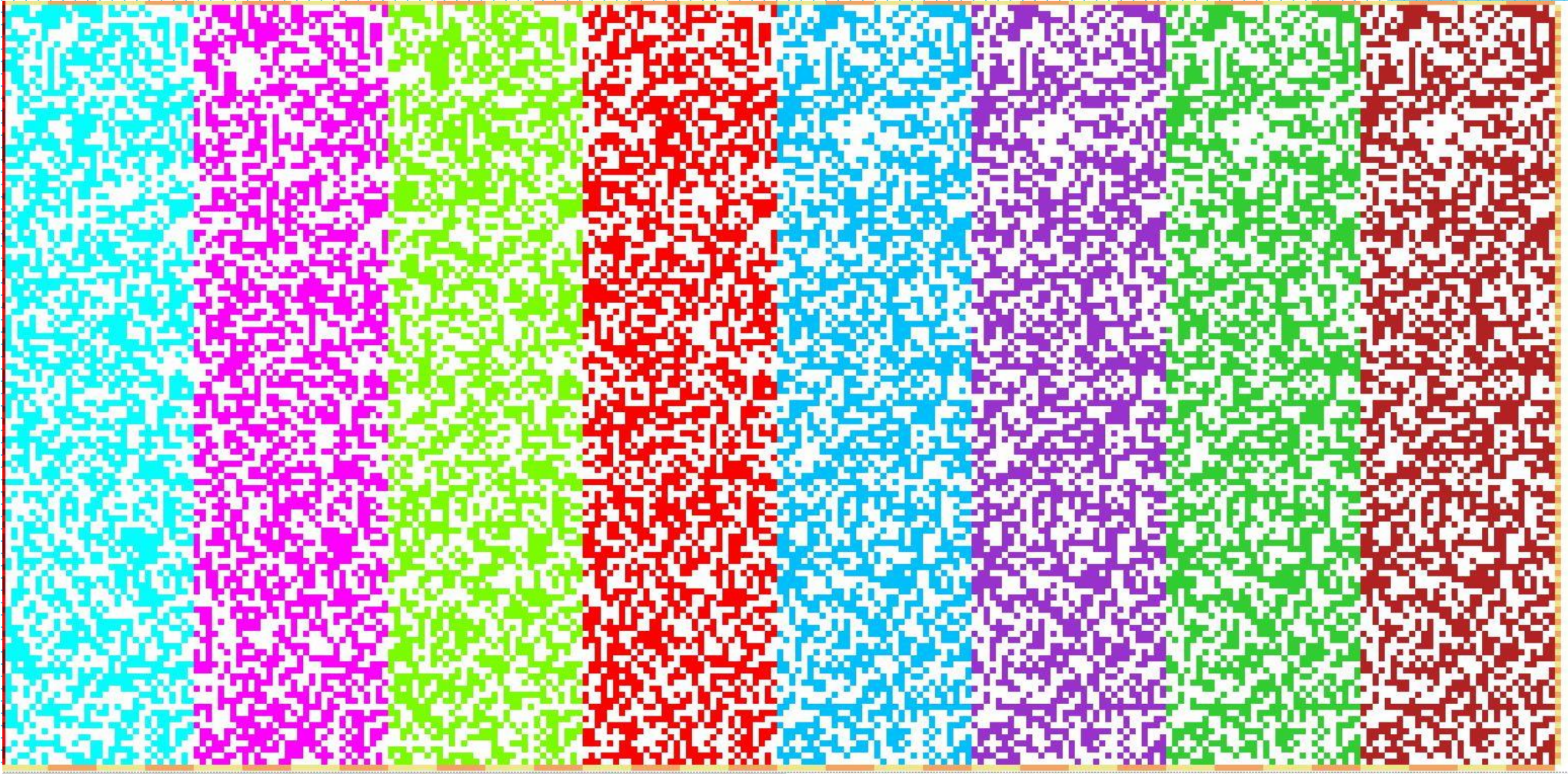
TYPES OF XOR KEY FOR SA

SA XOR key extacted from empty SA part



TYPES OF XOR KEY FOR SA

SA XOR key extacted from empty SA part



TYPES OF XOR KEY FOR SA

SA XOR key extacted from empty SA part

Pros

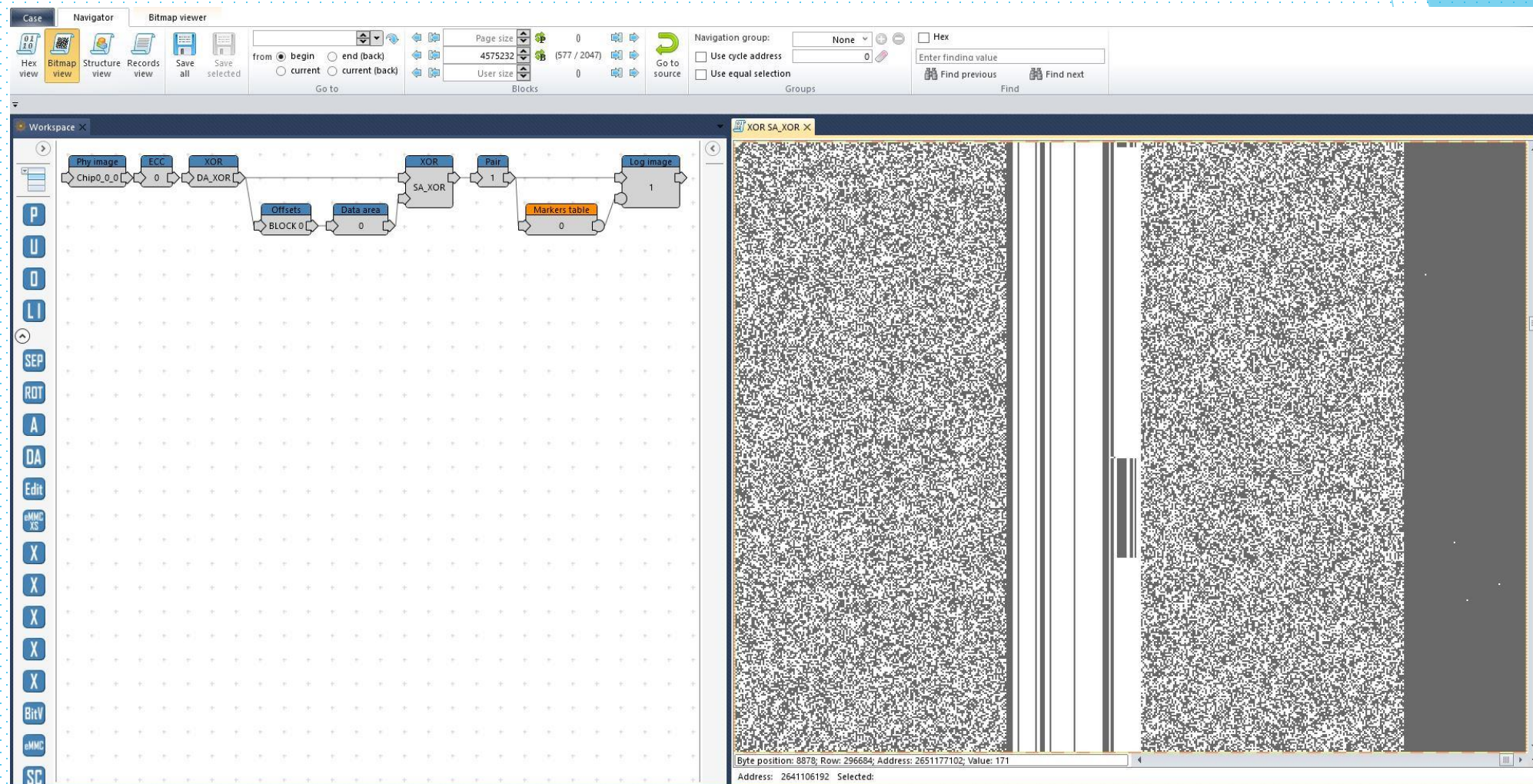
- ▶ 100% pure SA xor key
- ▶ LPN not distorted
- ▶ „Hot data” blocks can be used in recovery
- ▶ Quite easy extraction

Cons

- ▶ Works only when every SA part in block use same scrambling pattern
- ▶ Sometimes has to be inverted (When correct data in empty SA are FF instead of 00)
- ▶ Require at least one empty SA part

TYPES OF XOR KEY FOR SA

SA XOR key extacted from „Block 0”



TYPES OF XOR KEY FOR SA

SA XOR key extracted from „Block 0”

Pros

- ▶ Allow for restore block order
- ▶ Easy extraction

Cons

- ▶ SA is scrambled except LBN
- ▶ „Hot data” blocks can't be used in structure rebuild
- ▶ Sometimes require to use external data carver

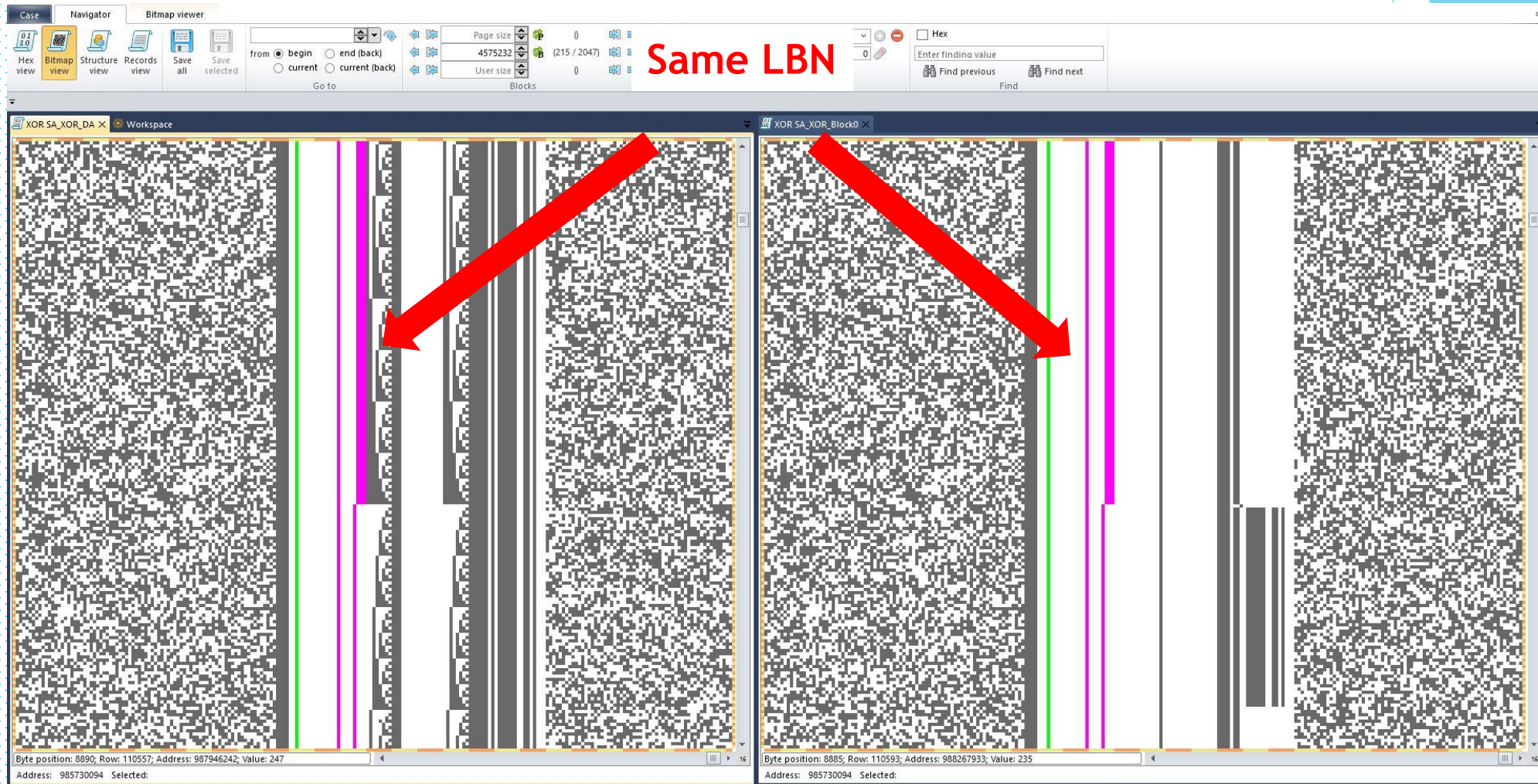
TYPES OF XOR KEY FOR SA

SA XOR key extracted from

DA

vs

Block 0



TYPES OF XOR KEY FOR SA

Markers Table Comparison

Header Misalignment

Missing LPN

The screenshot displays the Markers Table Comparison tool interface. It features a toolbar at the top with various icons for editing, filtering, and sorting. Below the toolbar, there are two main panels: 'Markers table DA' and 'Markers table Block0'. Each panel contains a table with columns for 'Use', 'Bank', 'LBN', 'Header', 'Test 1', 'Test 2', 'Address', 'LB', and 'RB'. The 'Markers table DA' panel shows a list of markers starting from LPN 00, while the 'Markers table Block0' panel shows a list of markers starting from LPN 00. Red arrows point to the 'Header' and 'LPN' columns, indicating misalignment and missing LPN values.

Use	Bank	LBN	Header	Test 1	Test 2	Address	LB	RB
☒	00	0000	30	55AA	E2	01FAAFA000		
☒	00	0001	30	55AA	E9	01FB3B4000		
☐	00	0001	40	0300	EA	01FD23F000		
☐	00	0001	40	55AA	EA	01FEC6D000		
☐	00	0001	E7	0000	37	01FA240000		
☒	00	0002	30	0000	E9	00188B2000		
☐	00	0002	40	0000	EA	0206F53000		
☐	00	0002	40	0000	EA	02073B0000		
☒	00	0003	20	0000	E7	001E8B0000		
☒	00	0004	20	0000	E7	001BD0E000		
☒	00	0005	30	0000	E7	01FC528000		
☐	00	0005	E7	0000	36	01F9986000		
☒	00	0006	20	0000	E6	00165CA000		
☐	00	0006	40	0000	E4	020D3AE000		
☒	00	0007	20	0000	E6	0220979000		
☒	00	0008	20	0000	E9	0220DD6000		
☒	00	0009	20	0000	E4	00068B8000		
☒	00	000A	20	59AF	E4	000A5CE000		
☒	00	000B	20	88C2	E4	001F16A000		
☒	00	000C	20	8876	E4	001E453000		
☒	00	000D	20	FAF6	E4	0021452000		
☒	00	000E	20	D56B	E4	00082E6000		
☒	00	000F	20	9D97	E4	0013E85000		
☒	00	0010	20	40A4	E5	0012D11000		
☒	00	0011	20	0606	E4	0008FFD000		
☒	00	0012	20	EA68	E5	0014B9C000		

Use	Bank	LBN	Header	Test 1	Test 2	Address	LB	RB
☒	00	0000	00	55AA	00	01FAAFA000		
☒	00	0001	00	55AA	0B	01FB3B4000		
☐	00	0001	70	0300	08	01FD23F000		
☐	00	0001	70	55AA	08	01FEC6D000		
☐	00	0001	D7	0000	D5	01FA240000		
☒	00	0002	00	0000	0B	00188B2000		
☐	00	0002	70	0000	08	0206F53000		
☐	00	0002	70	0000	08	02073B0000		
☒	00	0003	10	0000	05	001E8B0000		
☒	00	0004	10	0000	05	001BD0E000		
☒	00	0005	00	0000	05	01FC528000		
☐	00	0005	D7	0000	D4	01F9986000		
☒	00	0006	10	0000	04	00165CA000		
☐	00	0006	70	0000	06	020D3AE000		
☒	00	0007	10	0000	04	0220979000		
☒	00	0008	10	0000	0B	0220DD6000		
☒	00	0009	10	0000	06	00068B8000		
☒	00	000A	10	59AF	06	000A5CE000		
☒	00	000B	10	88C2	06	001F16A000		
☒	00	000C	10	8876	06	001E453000		
☒	00	000D	10	FAF6	06	0021452000		
☒	00	000E	10	D56B	06	00082E6000		
☒	00	000F	10	9D97	06	0013E85000		
☒	00	0010	10	40A4	07	0012D11000		
☒	00	0011	10	0606	06	0008FFD000		
☒	00	0012	10	EA68	07	0014B9C000		

CONTROLLERS EXAMPLES WITH SCRAMBLED SPARE AREA

▶ Silicon Motion:

- SM2685
- SM2703 Family
- SM2702
- SM3257 (optional)

▶ Innostor:

- IS817
- IS902
- IS903
- IS916
- IS917

▶ Allwinner: (Low cost tablets SoC)

- A10
- A13
- A15

▶ Rockchip: (Low cost tablets SoC)

- RK3066

▶ Actions (ATJ):(Voice Recorders SoC)

- ATJ2117
- AT3315

CASE SAMPLE

Silicon Motion SM2703