A New Conditional Cube Attack on Reduced-Round Ascon-128a in Nonce-misuse Setting

Donghoon Chang, Jinkeon Kang, and Meltem Sönmez Turan

Computer Security Division, NIST

Fifth Lightweight Cryptography Workshop, 10 May 2022

Aim

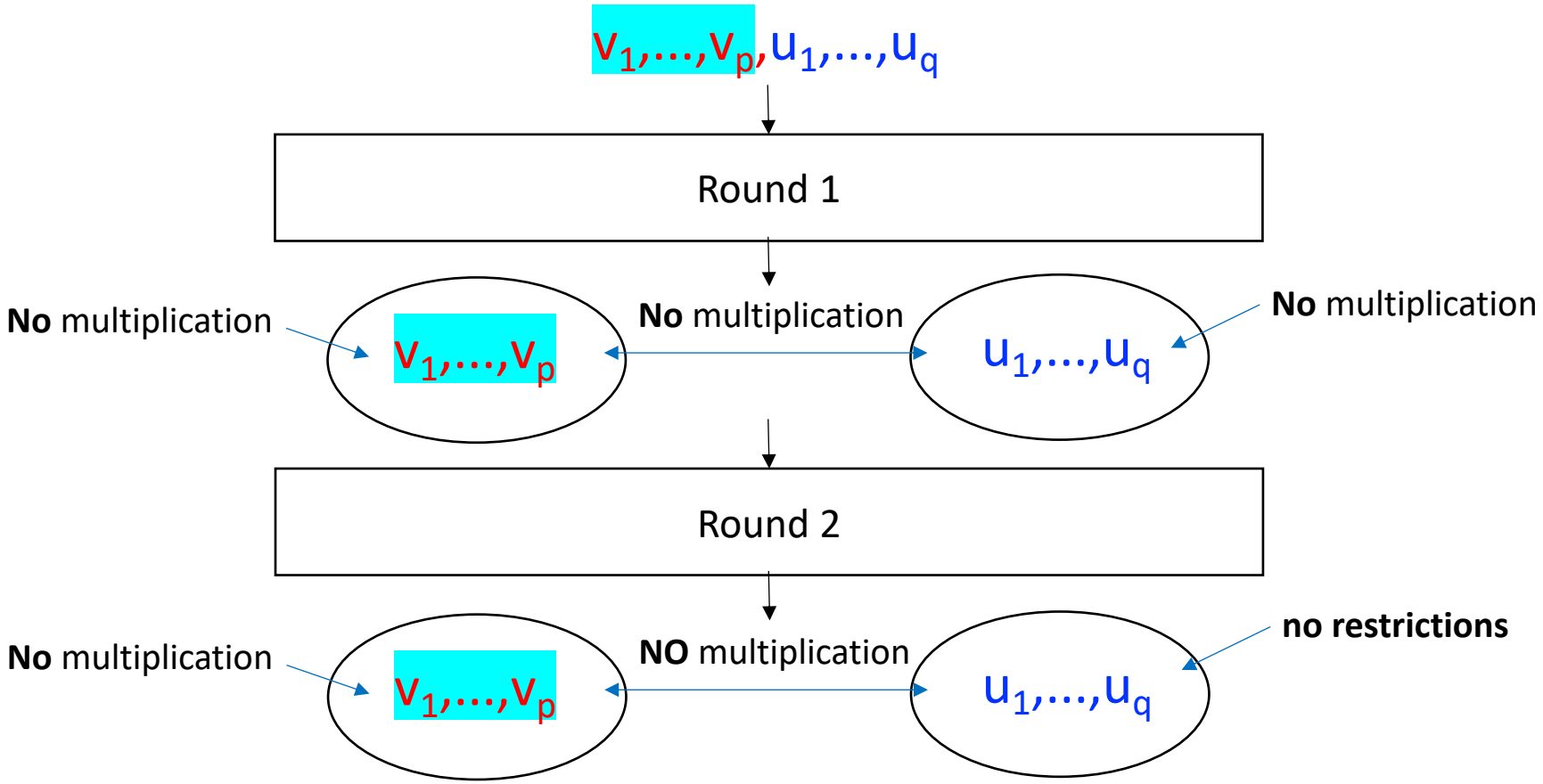
Evaluate Ascon-128a (non-primary) variant in nonce-misuse setting via conditional cube attacks

Table 1: Summary of cube attacks on ASCON-128a

Attack type	Method	Rounds [1] (12, 8, 12)	Data	Time	Memory	Nonce misuse	Ref.
Key recovery	Conditional cube	6,⋆,⋆	2^{40}	2^{40}	-	No	[LDW17]
	Cube	7,⋆,⋆	$2^{77.2}$	$2^{103.92}$	-	No	[LDW17]
	Cube	7,⋆,⋆	2^{64}	2^{123}	-	No	[RHSS21]
	Cube	7,5,⋆	2^{33}	2^{97}	-	Yes	[LZWW17]
	Conditional cube	⋆,7,⋆	2^{117}	2^{118}	2^{32}	Yes	this study
Forgery	Cube	⋆,⋆,5	2^{17}	2^{17}	-	Yes	[LZWW17]
	Cube	⋆,⋆,6	2^{33}	2^{33}	-	Yes	[LZWW17]
State-recovery	Conditional cube	⋆,7,⋆	2^{117}	2^{118}	-	Yes	this study

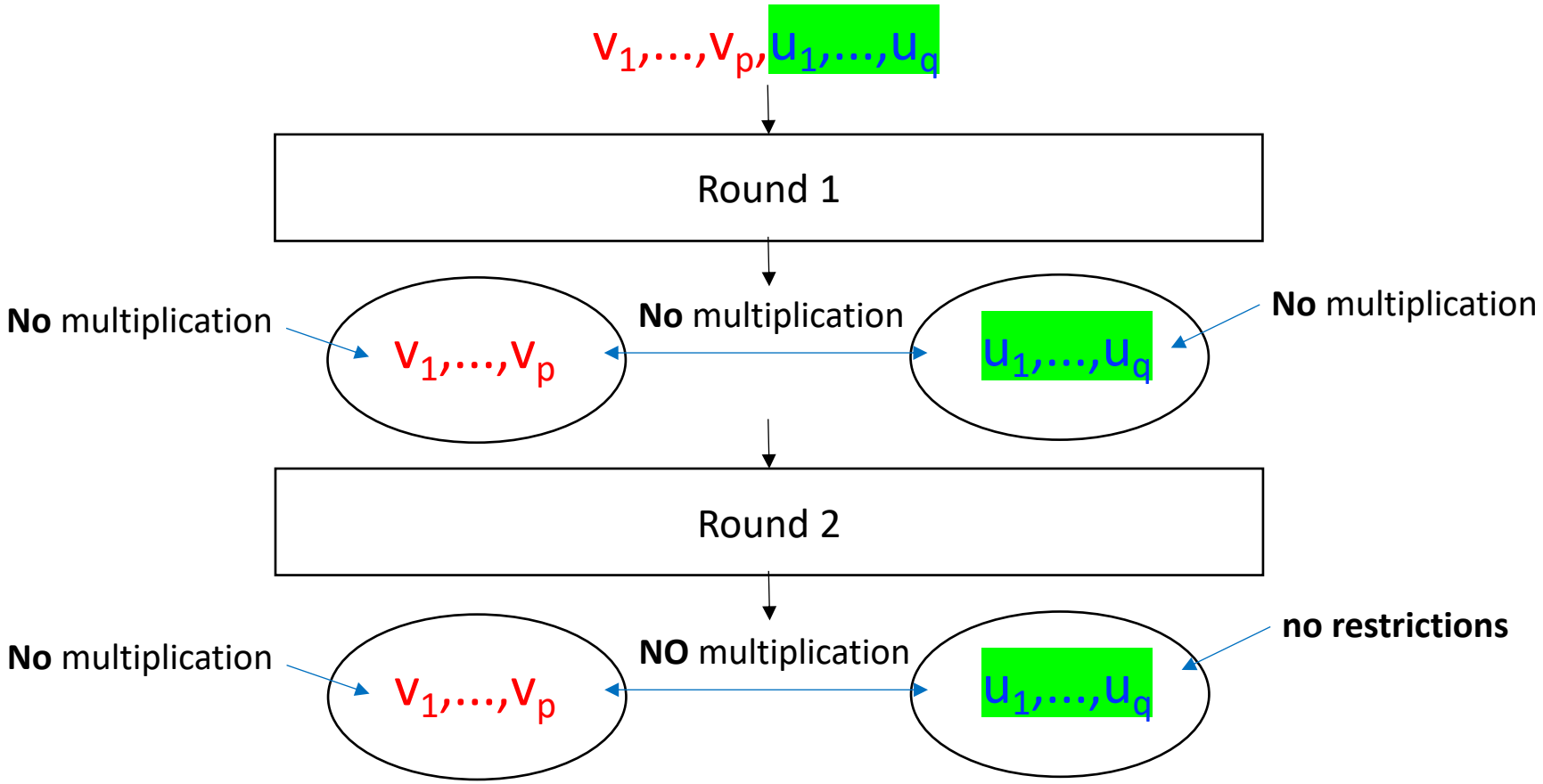
Conditional Cube Variables, Ordinary Cube Variables With True Conditions

- There are p+q cube variables, $v_1,\ldots,v_p,u_1,\ldots,u_q$.



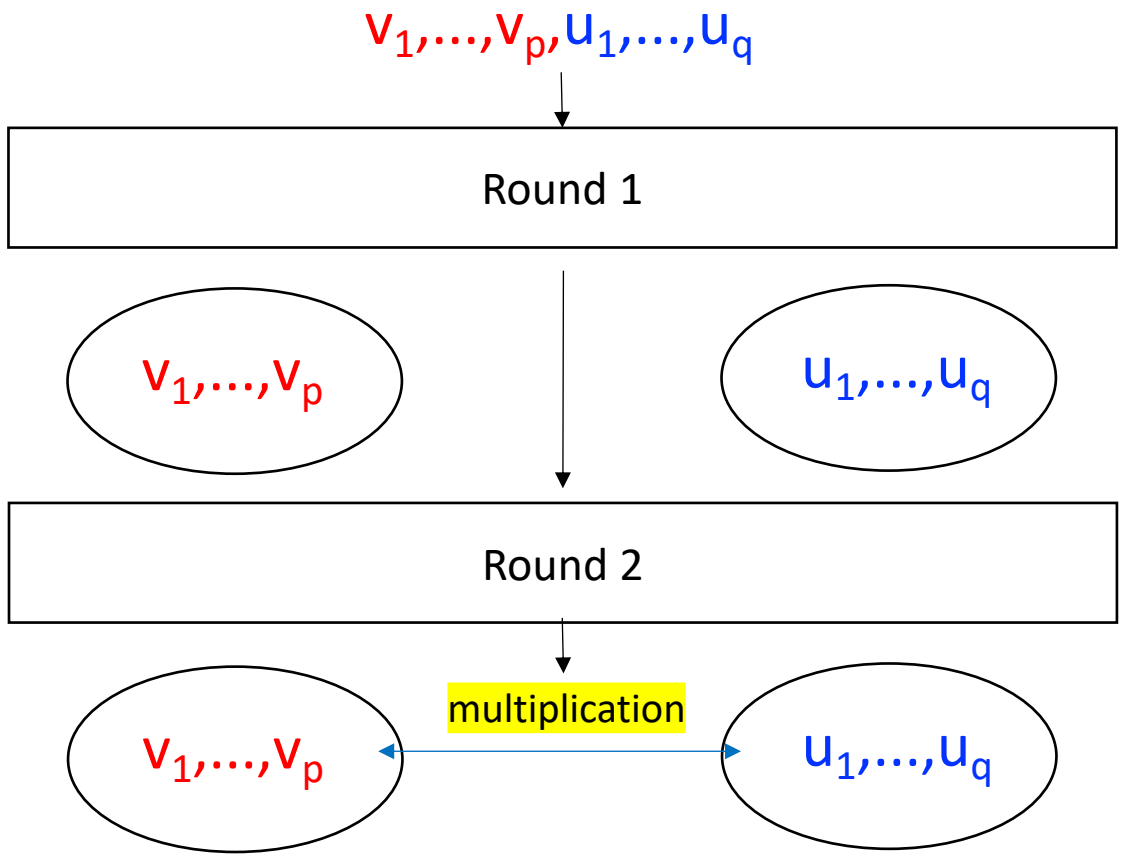
Conditional Cube Variables, Ordinary Cube Variables With True Conditions

- There are p+q cube variables, $v_1,\ldots,v_p,u_1,\ldots,u_q$.



Conditional Cube Variables, Ordinary Cube Variables With *False* Conditions

- There are p+q cube variables, $v_1,\ldots,v_p,u_1,\ldots,u_q$.



Theorem 2 – EUROCRYPT 2017*

- Assume that there are p conditional cube variables $v_1,\ldots,v_p$ and q ordinary cube variables $u_1,\ldots,u_q$, where

  (1) $p,q \geq 1$ and $q=2^{n+1}-2p+1$

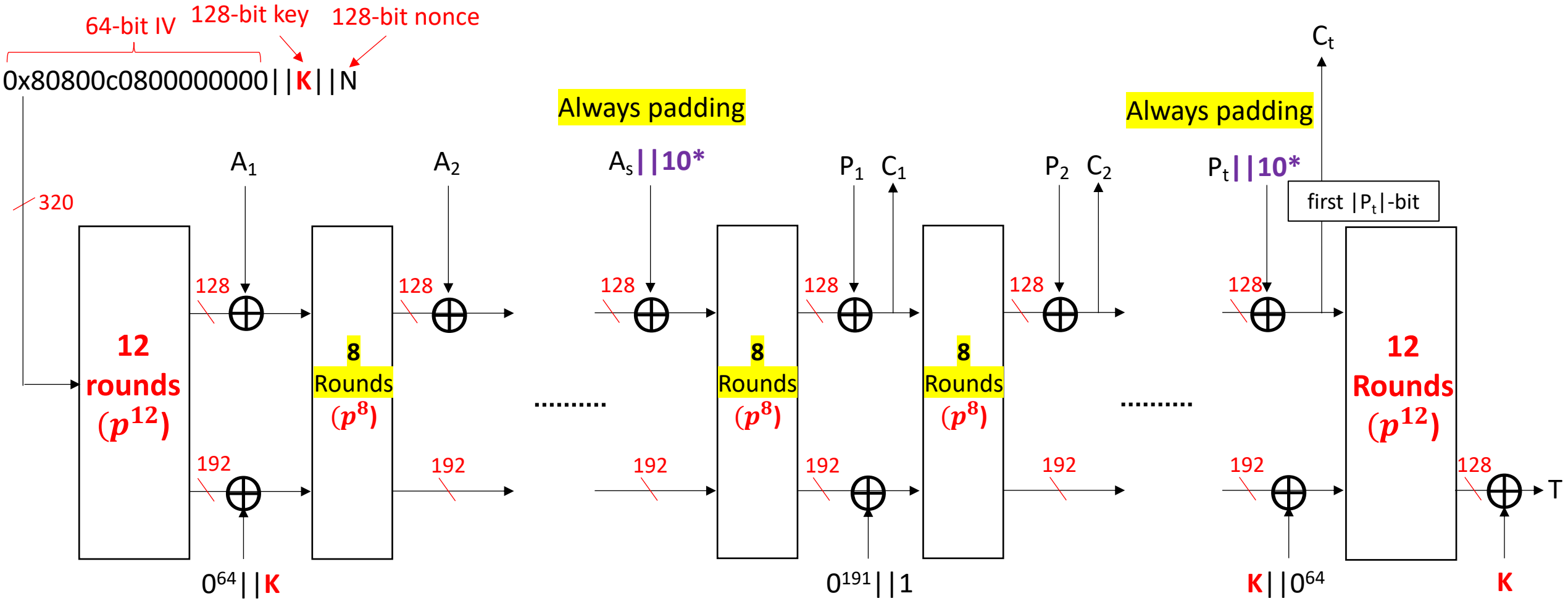
  or (2) $q=0$ and $p=2^n+1$

- If the conditions are true, then the term $v_1v_2\ldots v_pu_1u_2\ldots u_q$ will not appear in the output polynomials of **(n+2)**-round function, where the degree of each round is 2.

We will consider the case that **p**=1 and **q**=63 and **n**=5.

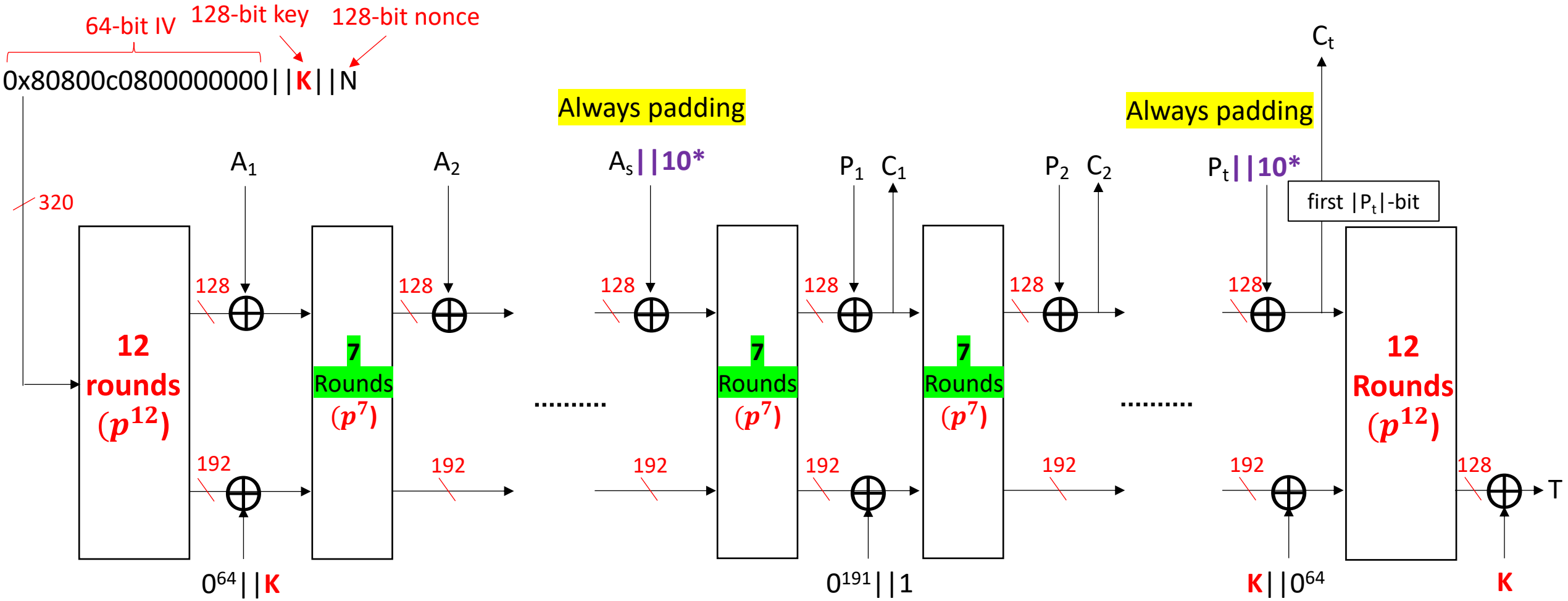
*Senyang Huang, Xiaoyun Wang, Guangwu Xu, Meiqin Wang, and Jingyuan Zhao, "Conditional cube attack on reduced-round keccak sponge function," EUROCRYPT 2017

ASCON-128a



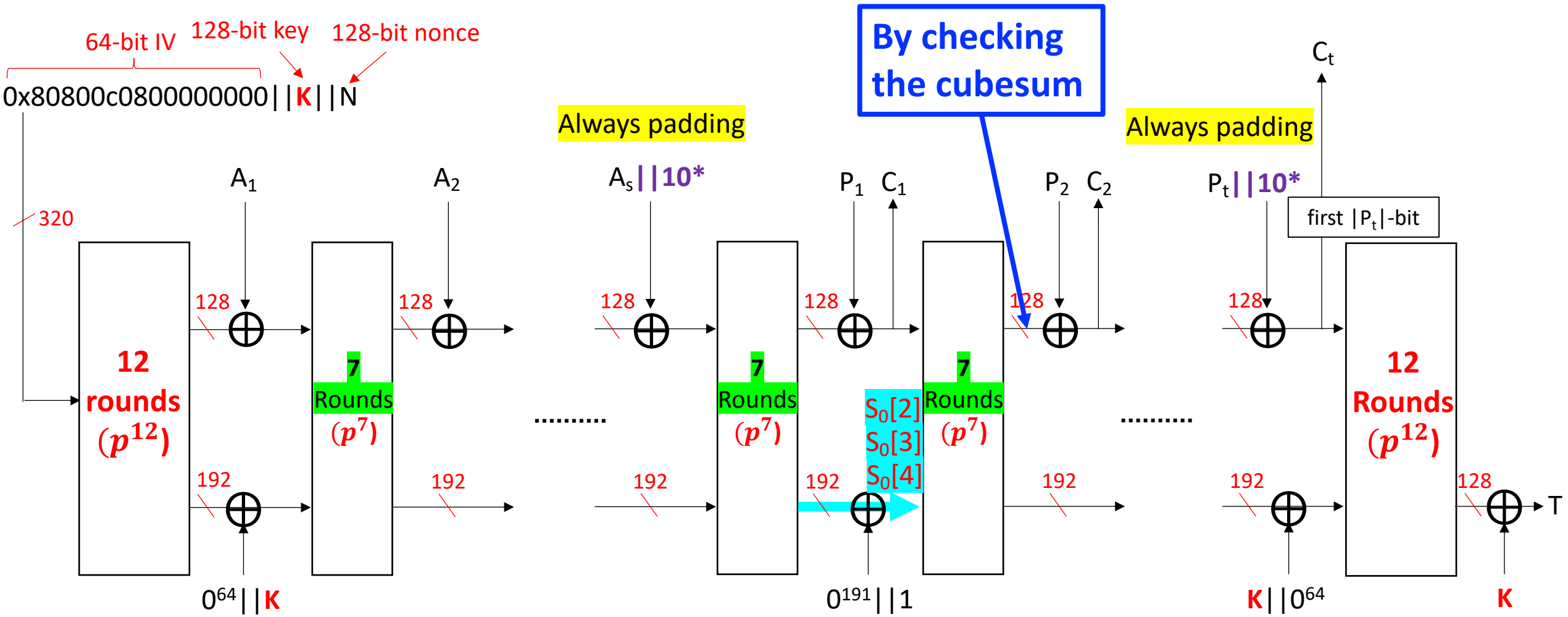
In case that $|A| \neq 0$

ASCON-128a with 7-Round Encryption



In case that $|A| \neq 0$

Our target is to recover 192-bit secret state ($S_0[2],S_0[3],S_0[4]$) ASCON-128a with 7-Round Encryption



In case that $|A| \neq 0$

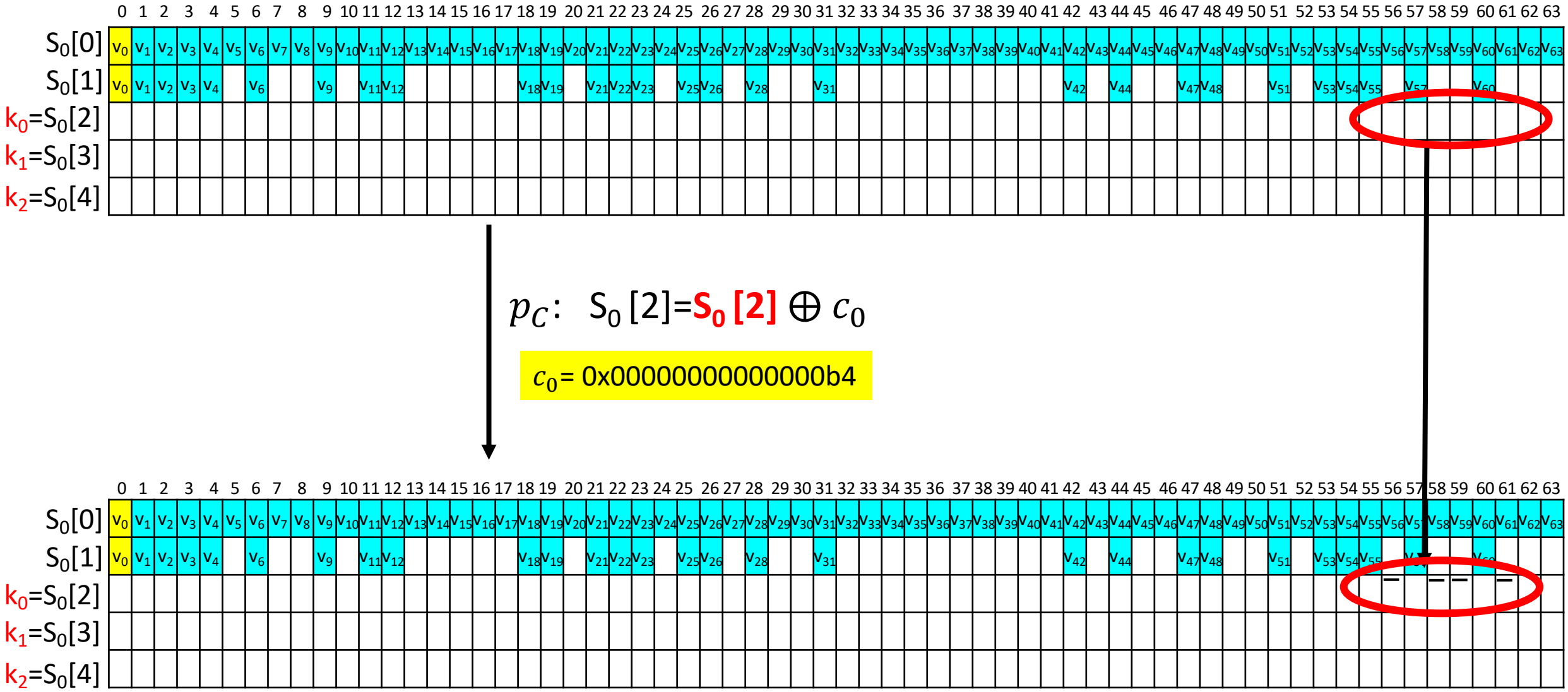
Selection of cube variables.

- Pattern-A: 64 cube variables (1 conditional, 63 ordinary) to recover 38 bits out of 192-bit secret state.
- Pattern-B: 64 cube variables (1 conditional, 63 ordinary) to recover 19 bits out of 192-bit secret state.

Pattern-A

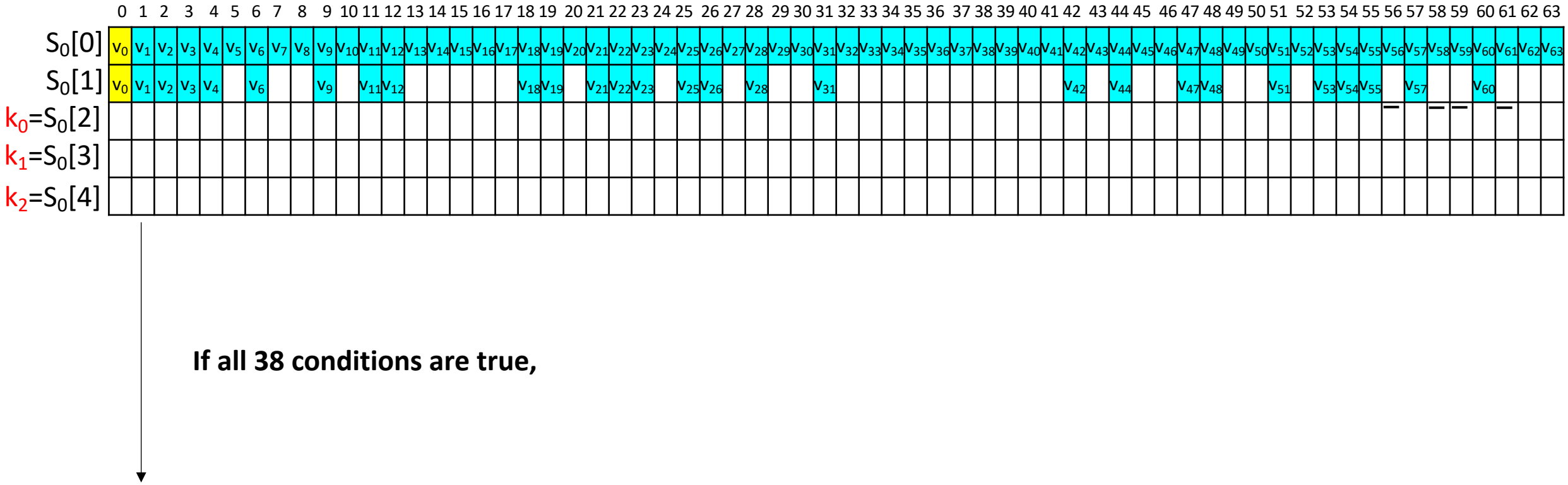
Pattern-A

Propagation of Cube Variables through Constant Addition (Round 0)



Pattern-A

Propagation of Cube Variables through S-box (Round 0)



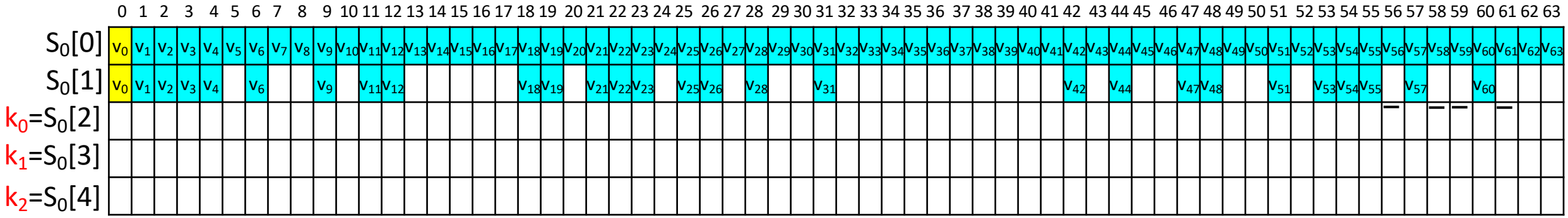
Pattern-A

38 conditions of Pattern-A

Column	Condition	Column	Condition	Column	Condition
0	$k_0[0] = k_1[0] = k_2[0] = 0$	19	$k_0[19] = k_1[19] = k_2[19] = 0$	47	$k_1[47] = k_2[47]$
1	$k_0[1] = k_1[1] = k_2[1]$	21	$k_2[21] = 0$	48	$k_1[48] = k_2[48]$
2	$k_1[2] = k_2[2]$	22	$k_0[22] = k_1[22]$	51	$k_2[51] = 0$
3	$k_0[3] = k_1[3]$	23	$k_2[23] = 0$	53	$k_0[53] = k_1[53] = k_2[53]$
4	$k_0[4] = k_1[4]$	25	$k_0[25] = k_1[25]$	54	$k_1[54] = k_2[54]$
6	$k_0[6] = k_1[6] = k_2[6]$	26	$k_0[26] = k_1[26]$	55	$k_1[55] = k_2[55]$
9	$k_0[9] = k_1[9] = k_2[9]$	28	$k_0[28] = k_1[28] = k_2[28] = 0$	57	$k_2[57] = 0$
11	$k_1[11] = k_2[11]$	31	$k_0[31] = k_1[31]$	60	$k_1[60] = k_2[60]$
12	$k_2[12] = 0$	42	$k_2[42] = 0$		
18	$k_1[18] = k_2[18]$	44	$k_0[44] = k_1[44]$		

Pattern-A

Propagation of Cube Variables through S-box (Round 0)



In total, 38 conditions.

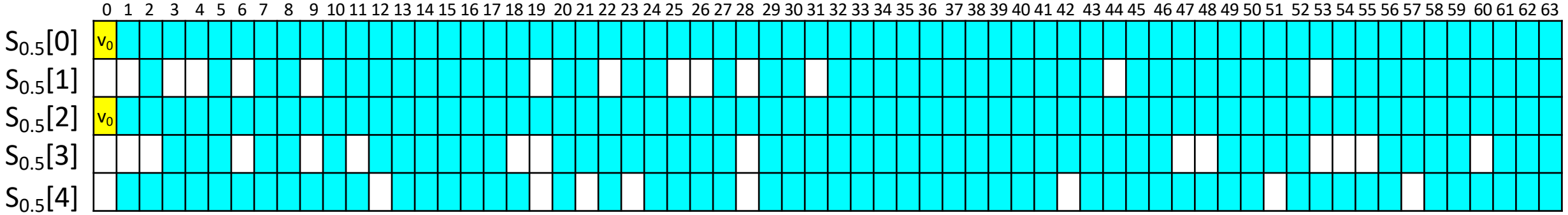
$$y_0 = x_4x_1 + x_3 + x_2x_1 + x_2 + x_1\ x_0 + x_1 + x_0$$

$$y_1 = x_4 + x_3x_2 + x_3x_1 + x_3 + x_2x_1 + x_2 + x_1 + x_0$$

$$y_2 = x_4x_3 + x_4 + x_2 + x_1 + 1$$

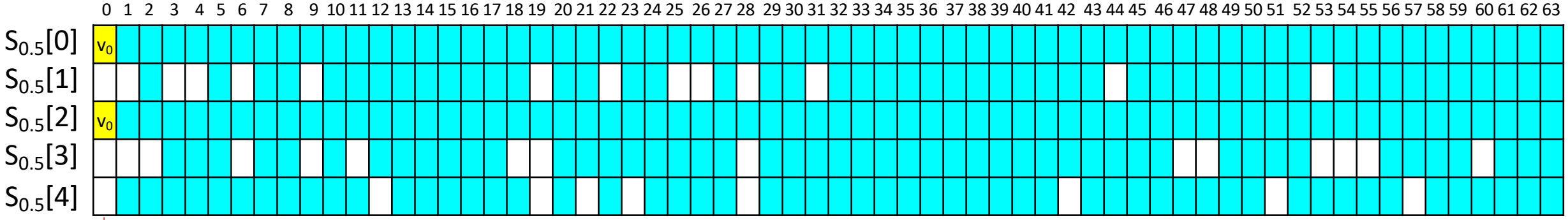
$$y_3 = x_4\ x_0 + x_4 + x_3\ x_0 + x_3 + x_2 + x_1 + x_0$$

$$y_4 = x_4x_1 + x_4 + x_3 + x_1x_0 + x_1$$

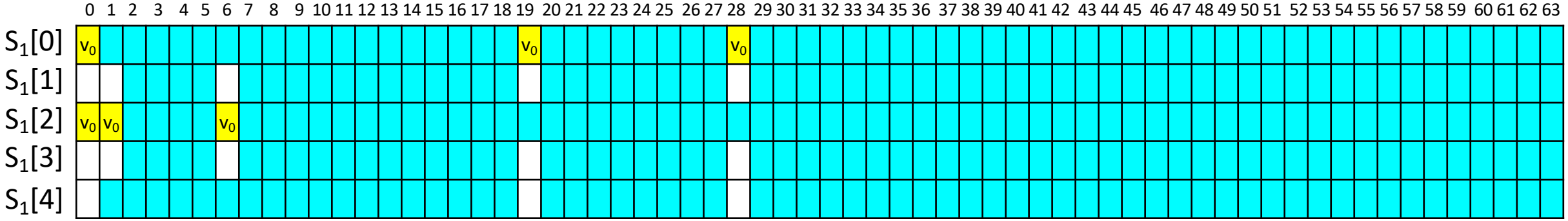


Pattern-A

Propagation of Cube Variables through Diffusion Layer (Round 0)

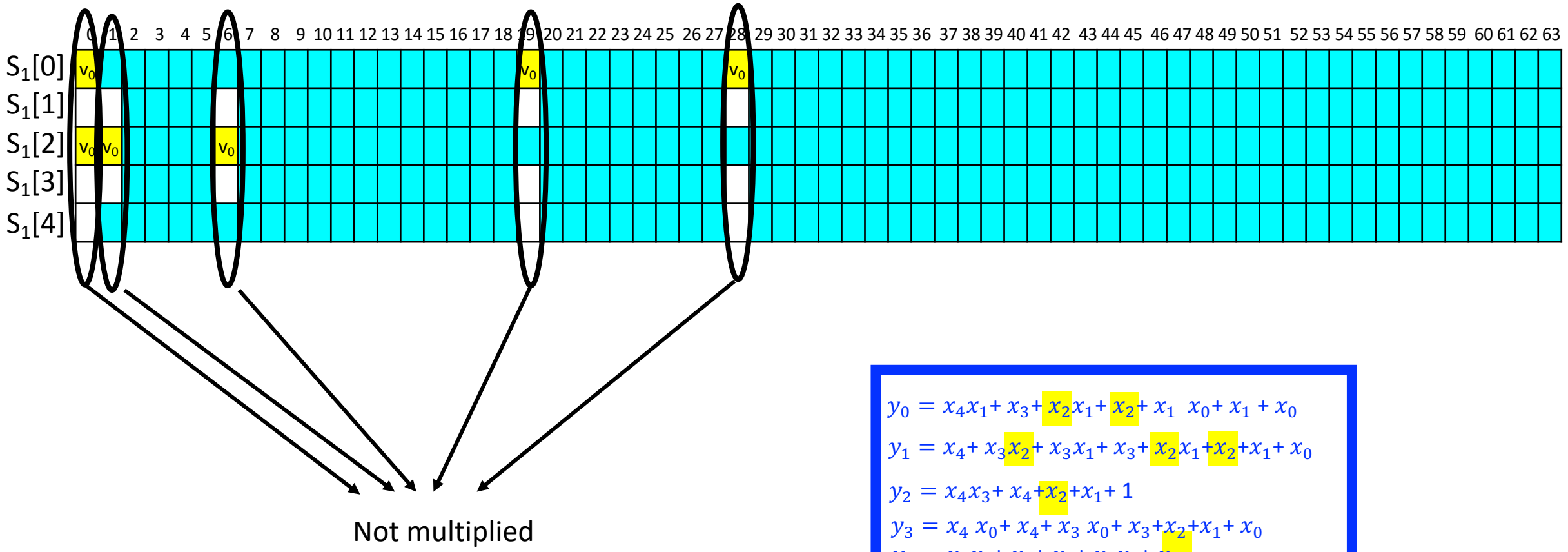


$$\Sigma_0(x_0) = x_0 \oplus (x_0 \ggg 19) \oplus (x_0 \ggg 28)$$
$$\Sigma_0(x_1) = x_1 \oplus (x_1 \ggg 61) \oplus (x_1 \ggg 39)$$
$$\Sigma_0(x_2) = x_2 \oplus (x_2 \ggg 1) \oplus (x_2 \ggg 6)$$
$$\Sigma_0(x_3) = x_3 \oplus (x_3 \ggg 10) \oplus (x_3 \ggg 17)$$
$$\Sigma_0(x_4) = x_4 \oplus (x_4 \ggg 7) \oplus (x_4 \ggg 41)$$



Pattern-A

Propagation of Cube Variables through Constant Addition and S-box (Round 1)



$$y_0 = x_4x_1 + x_3 + x_2x_1 + x_2 + x_1\ \ x_0 + x_1 + x_0$$

$$y_1 = x_4 + x_3x_2 + x_3x_1 + x_3 + x_2x_1 + x_2 + x_1 + x_0$$

$$y_2 = x_4x_3 + x_4 + x_2 + x_1 + 1$$

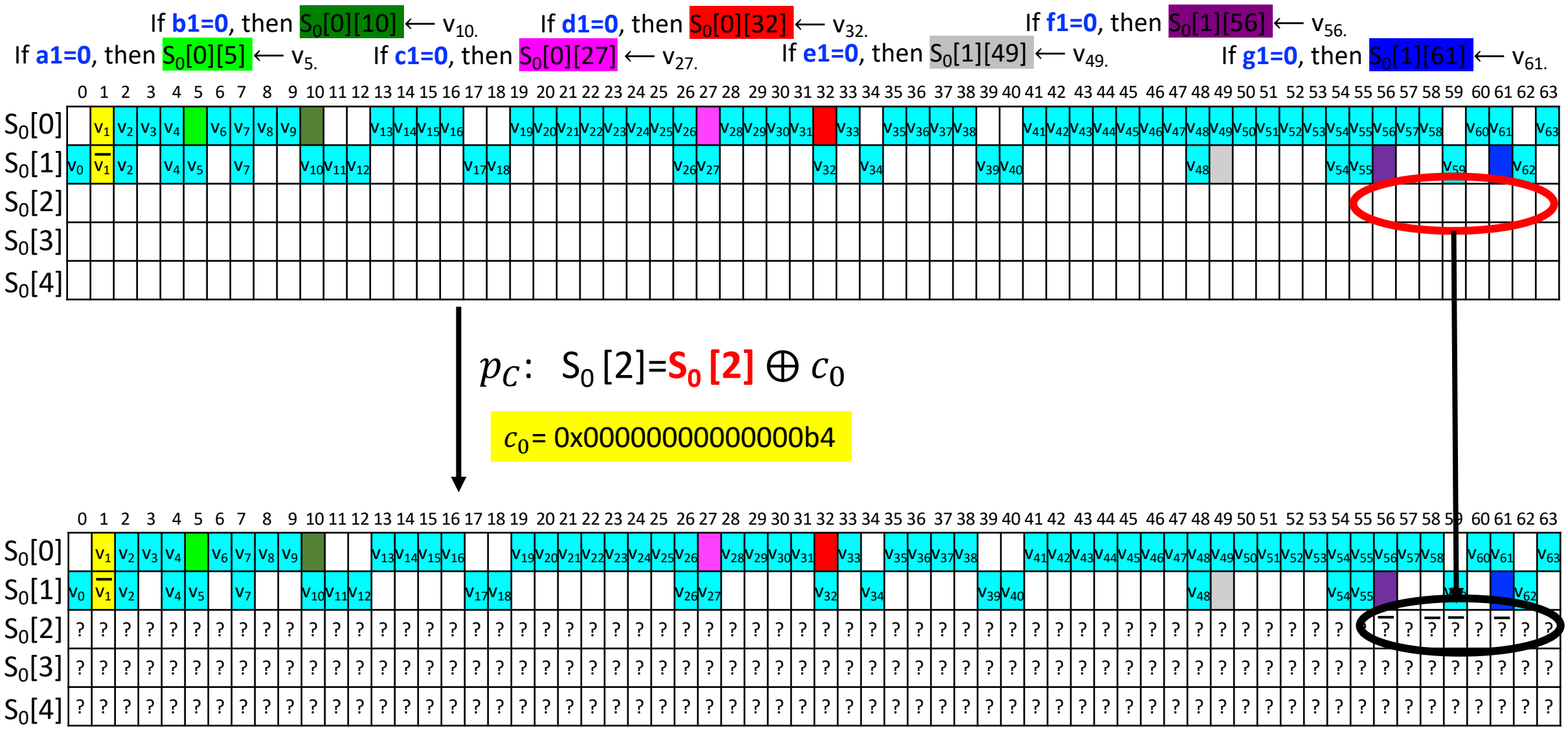
$$y_3 = x_4\ x_0 + x_4 + x_3\ x_0 + x_3 + x_2 + x_1 + x_0$$

$$y_4 = x_4x_1 + x_4 + x_3 + x_1x_0 + x_1$$

Pattern-B

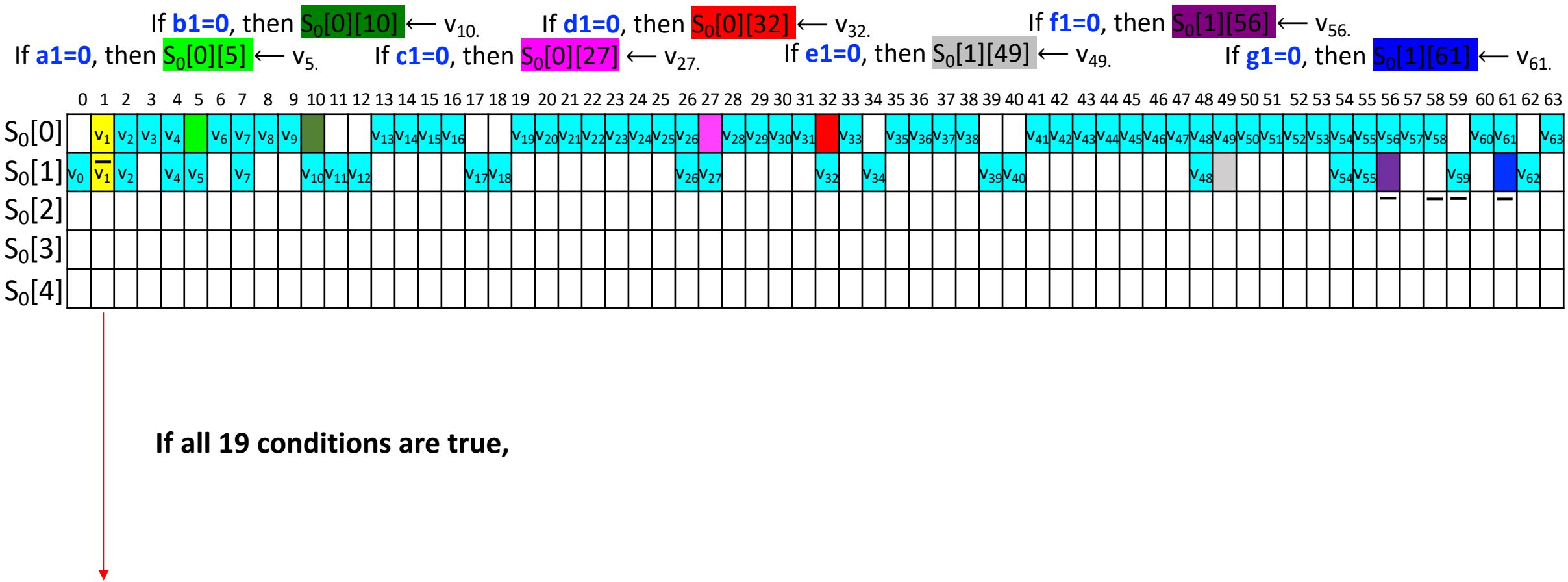
Pattern-B

Propagation of Cube Variables through Constant Addition (Round 0) – for any (a1,…,g1)



Pattern-B

Propagation of Cube Variables through S-box (Round 0) – for any (a1,…,g1)



If all 19 conditions are true,

Pattern-B

19 conditions of Pattern-B

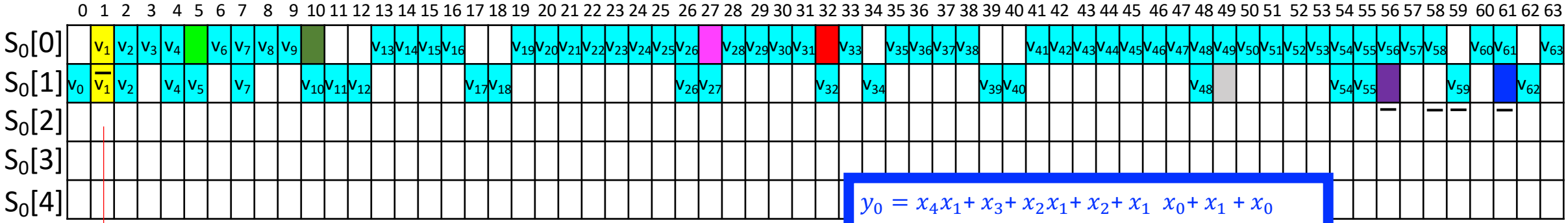
Column	Condition	Column	Condition
1	$k_0[1] = k_1[1] = k_2[1] = 1$	49	$k_1[49] = k_2[49]$ **+ e1**
2	$k_0[2] = k_1[2] = k_2[2]$	54	$k_1[54] = k_2[54]$
4	$k_0[4] = k_1[4]$	55	$k_1[55] = k_2[55]$
5	$k_0[5] = k_1[5]$ **+ a1**	56	$k_1[56] = k_2[56]$ **+ f1**
7	$k_0[7] = k_1[7] = k_2[7]$	63	$k_1[61] = k_2[61]$ **+ g1**
10	$k_0[10] = k_1[10]$ **+ b1**		
26	$k_0[26] = k_1[26]$		
27	$k_0[27] = k_1[27]$ **+ c1**		
32	$k_0[32] = k_1[32]$ **+ d1**		
48	$k_1[48] = k_2[48]$		

Pattern-B

Propagation of Cube Variables through S-box (Round 0) – for any (a1,…,g1)

If **b1=0**, then $S_0[0][10] \leftarrow v_{10}$. If **d1=0**, then $S_0[0][32] \leftarrow v_{32}$. If **f1=0**, then $S_0[1][56] \leftarrow v_{56}$.

If **a1=0**, then $S_0[0][5] \leftarrow v_5$. If **c1=0**, then $S_0[0][27] \leftarrow v_{27}$. If **e1=0**, then $S_0[1][49] \leftarrow v_{49}$. If **g1=0**, then $S_0[1][61] \leftarrow v_{61}$.



$$y_0 = x_4x_1 + x_3 + x_2x_1 + x_2 + x_1\ \ x_0 + x_1 + x_0$$

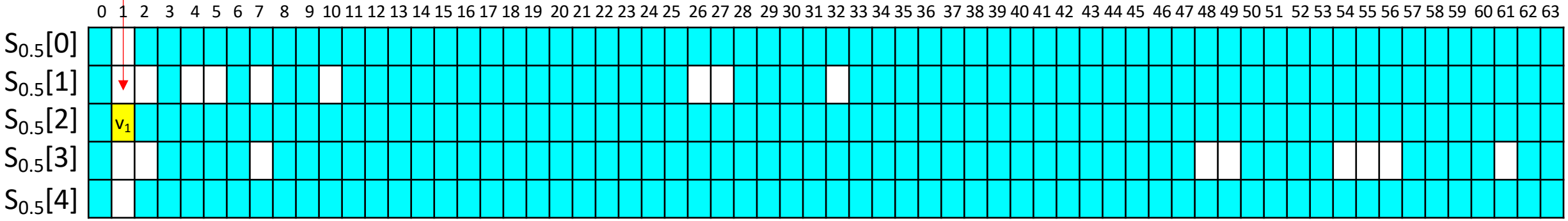
$$y_1 = x_4 + x_3x_2 + x_3x_1 + x_3 + x_2x_1 + x_2 + x_1 + x_0$$

$$y_2 = x_4x_3 + x_4 + x_2 + x_1 + 1$$

$$y_3 = x_4\ x_0 + x_4 + x_3\ x_0 + x_3 + x_2 + x_1 + x_0$$

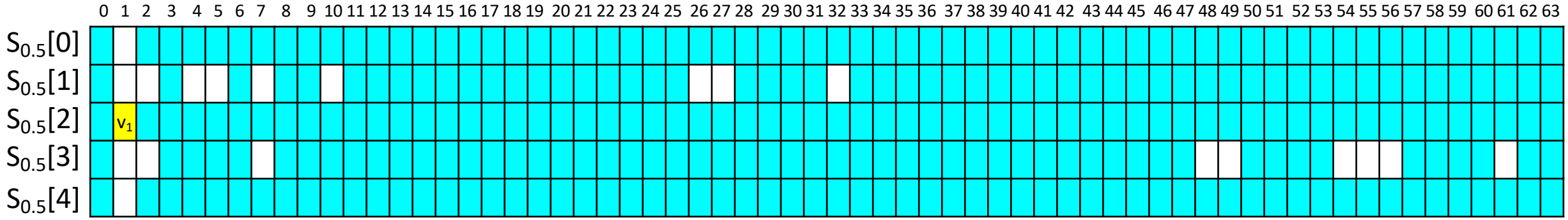
$$y_4 = x_4x_1 + x_4 + x_3 + x_1x_0 + x_1$$

If all 19 conditions are true,

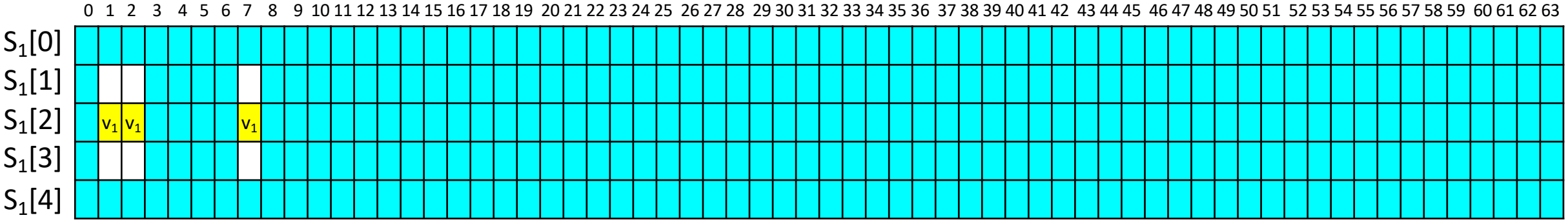


Pattern-B

Propagation of Cube Variables through Diffusion Layer (Round 0)

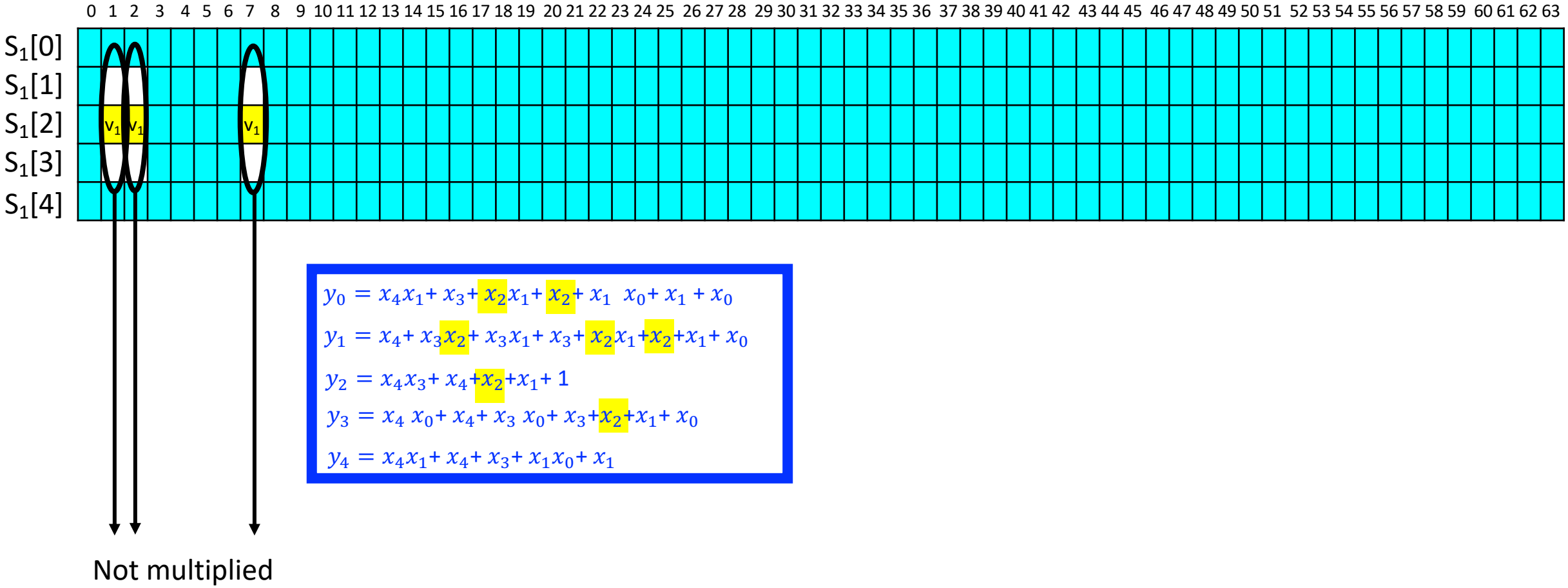


$$\Sigma_0(x_0) = x_0 \oplus (x_0 \ggg 19) \oplus (x_0 \ggg 28)$$
$$\Sigma_0(x_1) = x_1 \oplus (x_1 \ggg 61) \oplus (x_1 \ggg 39)$$
$$\Sigma_0(x_2) = x_2 \oplus (x_2 \ggg 1) \oplus (x_2 \ggg 6)$$
$$\Sigma_0(x_3) = x_3 \oplus (x_3 \ggg 10) \oplus (x_3 \ggg 17)$$
$$\Sigma_0(x_4) = x_4 \oplus (x_4 \ggg 7) \oplus (x_4 \ggg 41)$$



Pattern-B

Propagation of Cube Variables through Constant Addition and S-box (Round 1)



$$y_0 = x_4x_1 + x_3 + x_2x_1 + x_2 + x_1\ x_0 + x_1 + x_0$$

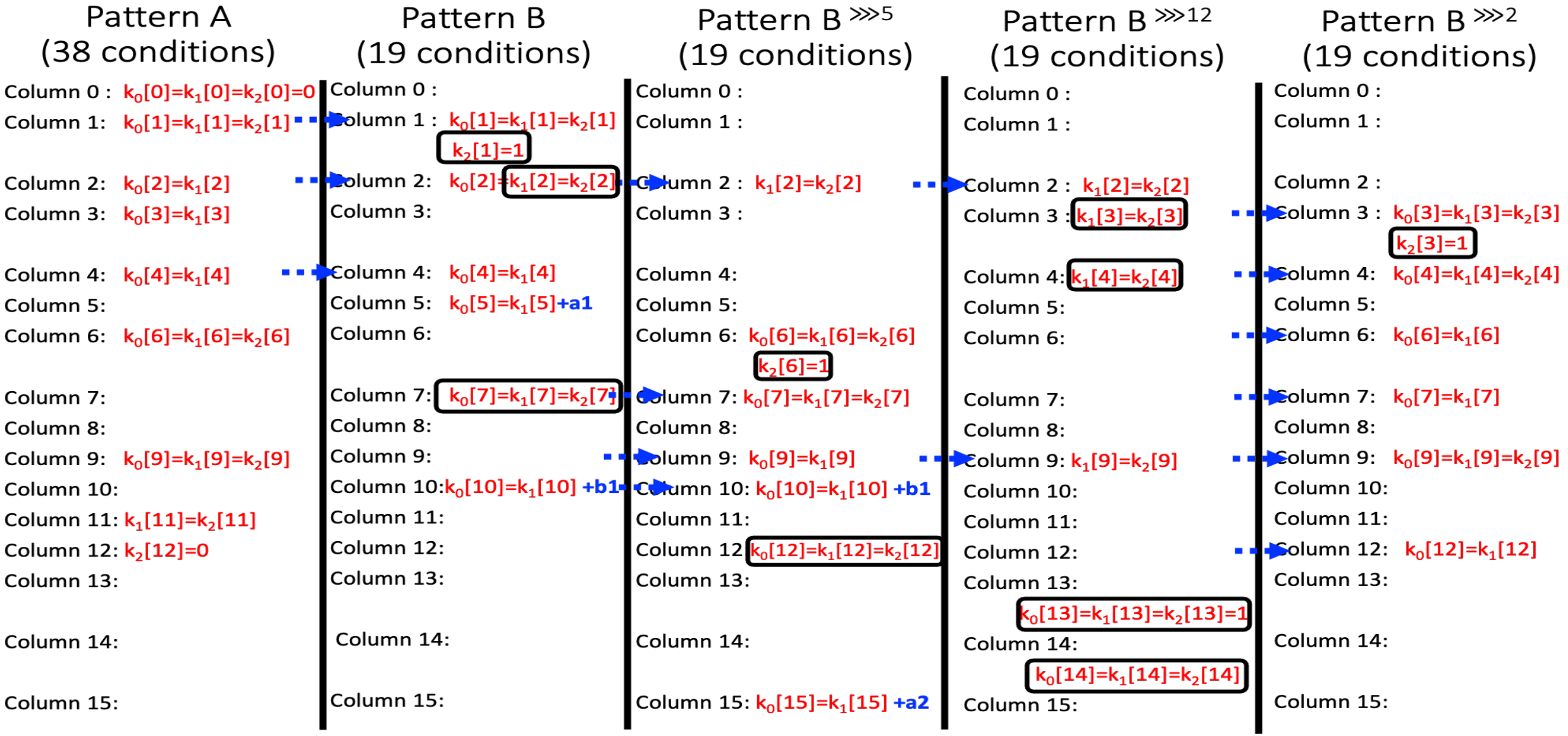
$$y_1 = x_4 + x_3x_2 + x_3x_1 + x_3 + x_2x_1 + x_2 + x_1 + x_0$$

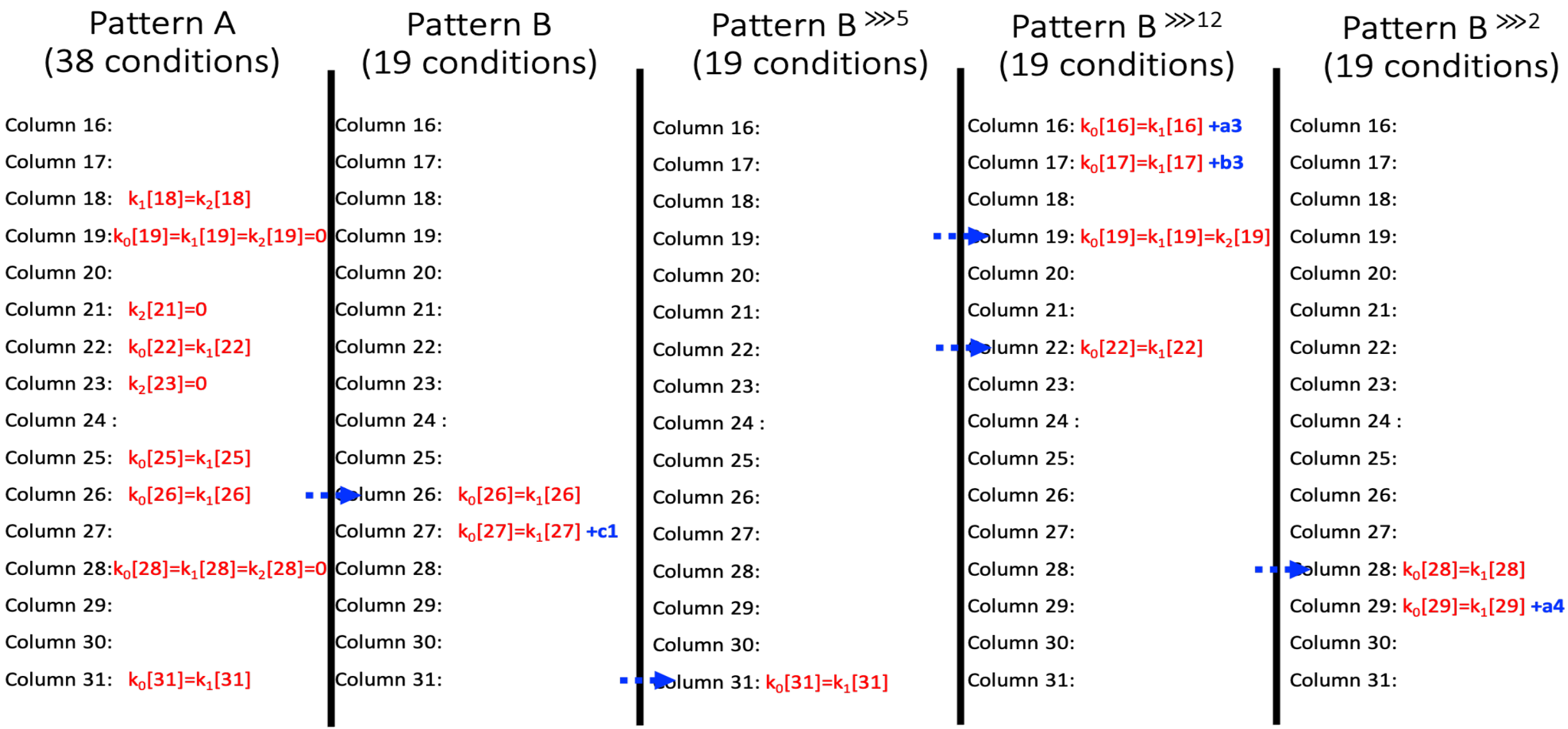
$$y_2 = x_4x_3 + x_4 + x_2 + x_1 + 1$$

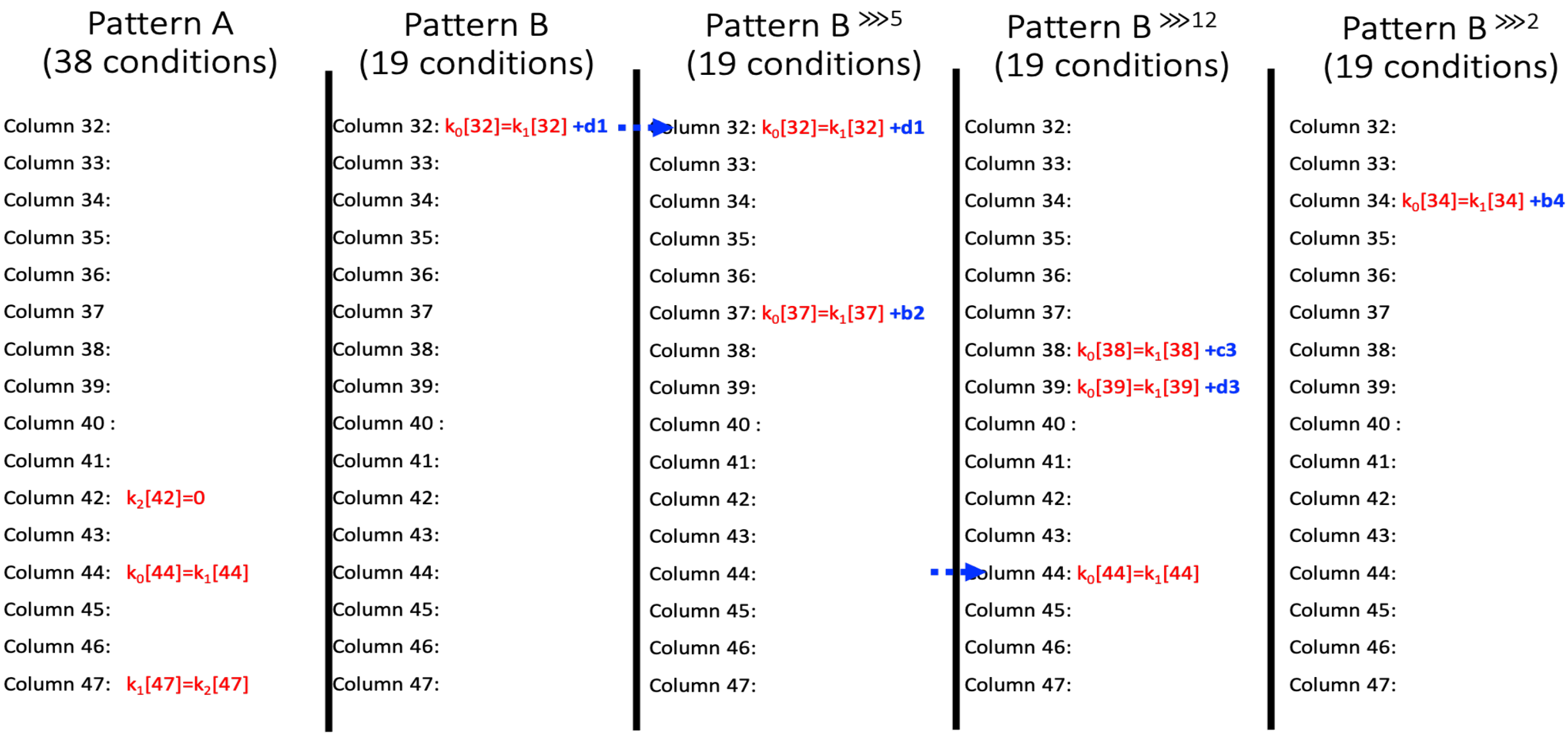
$$y_3 = x_4\ x_0 + x_4 + x_3\ x_0 + x_3 + x_2 + x_1 + x_0$$

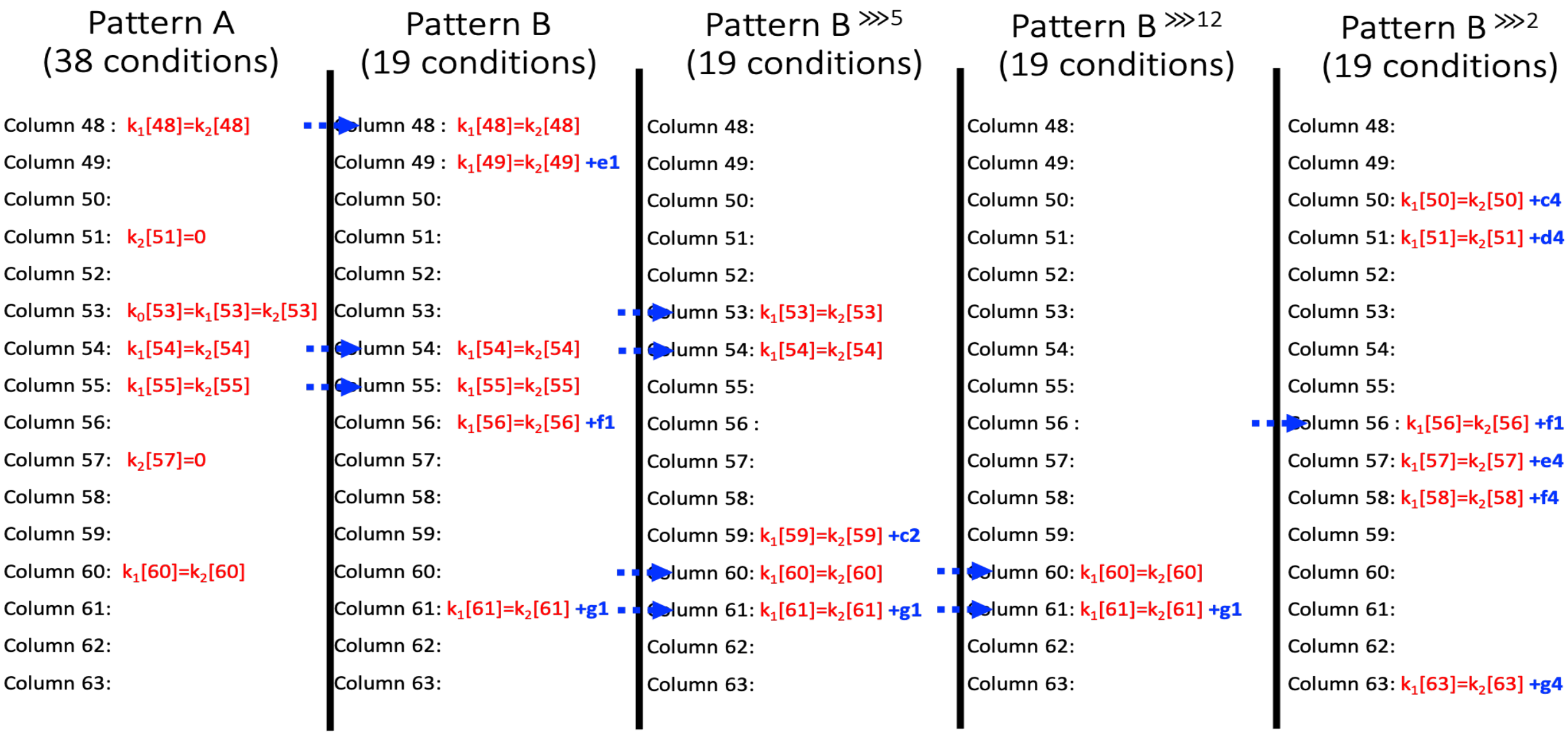
$$y_4 = x_4x_1 + x_4 + x_3 + x_1x_0 + x_1$$

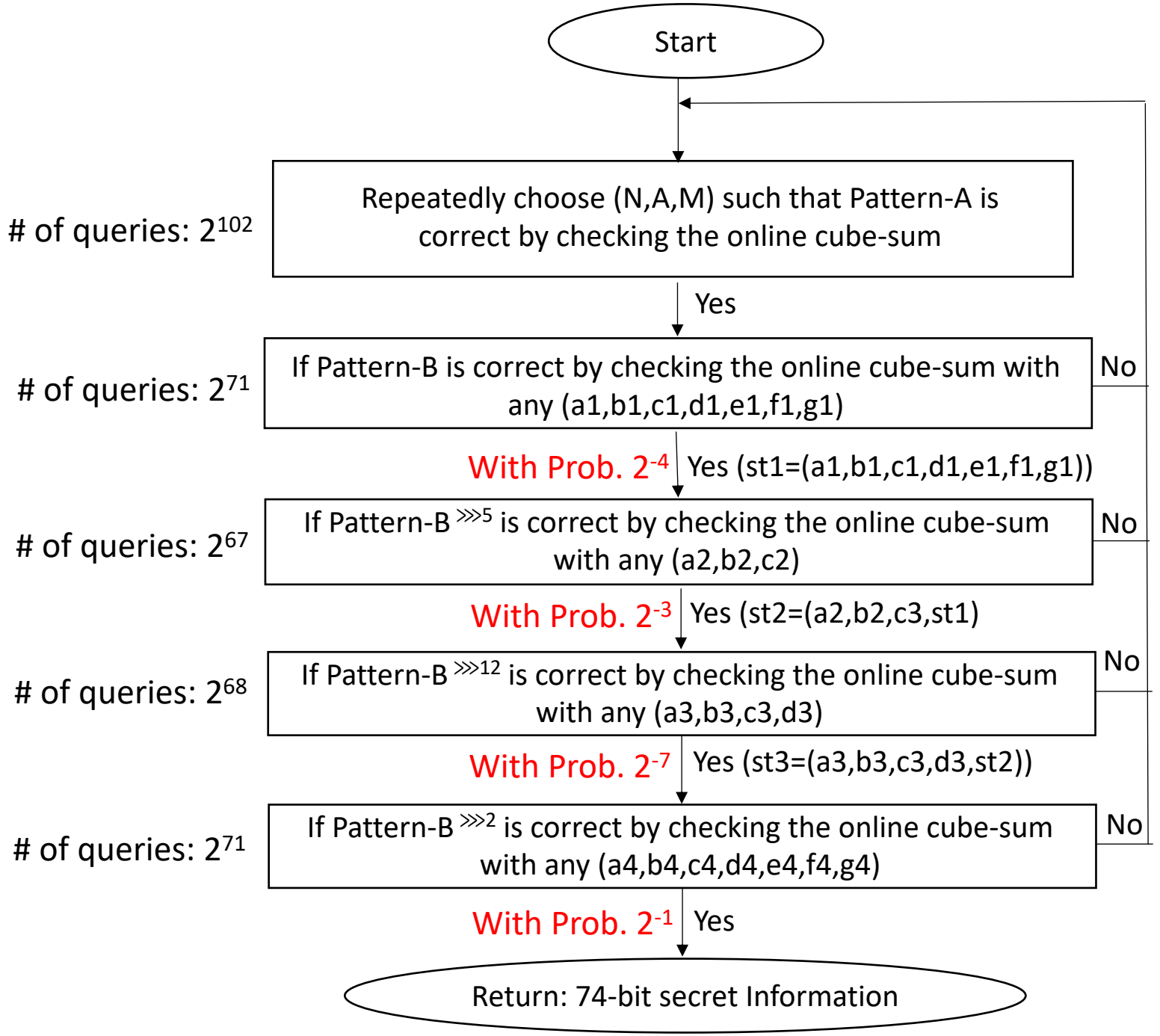
Pattern-A + Pattern-B
+ Shifts of Pattern-B


Pattern A
(38 conditions)
Column 0 : k0[0]=k1[0]=k2[0]=0
Column 1: k0[1]=k1[1]=k2[1]
Column 2: k0[2]=k1[2]
Column 3: k0[3]=k1[3]
Column 4: k0[4]=k1[4]
Column 5:
Column 6: k0[6]=k1[6]=k2[6]
Column 7:
Column 8:
Column 9: k0[9]=k1[9]=k2[9]
Column 10:
Column 11: k1[11]=k2[11]
Column 12: k2[12]=0
Column 13:
Column 14:
Column 15:
Pattern B
(19 conditions)
Column 0 :
Column 1 : k0[1]=k1[1]=k2[1]
k2[1]=1
Column 2: k0[2]=k1[2]=k2[2]
Column 3:
Column 4: k0[4]=k1[4]
Column 5: k0[5]=k1[5]+a1
Column 6:
Column 7: k0[7]=k1[7]=k2[7]
Column 8:
Column 9:
Column 10:k0[10]=k1[10] +b1
Column 11:
Column 12:
Column 13:
Column 14:
Column 15:
Pattern B ⋙5
(19 conditions)
Column 0 :
Column 1 :
Column 2 : k1[2]=k2[2]
Column 3 :
Column 4:
Column 5:
Column 6: k0[6]=k1[6]=k2[6]
k2[6]=1
Column 7: k0[7]=k1[7]=k2[7]
Column 8:
Column 9: k0[9]=k1[9]
Column 10: k0[10]=k1[10] +b1
Column 11:
Column 12 k0[12]=k1[12]=k2[12]
Column 13:
Column 14:
Column 15: k0[15]=k1[15] +a2
Pattern B ⋙12
(19 conditions)
Column 0 :
Column 1 :
Column 2 : k1[2]=k2[2]
Column 3 : k1[3]=k2[3]
Column 4: k1[4]=k2[4]
Column 5:
Column 6:
Column 7:
Column 8:
Column 9: k1[9]=k2[9]
Column 10:
Column 11:
Column 12:
Column 13:
k0[13]=k1[13]=k2[13]=1
Column 14:
k0[14]=k1[14]=k2[14]
Column 15:
Pattern B ⋙2
(19 conditions)
Column 0 :
Column 1 :
Column 2 :
Column 3 : k0[3]=k1[3]=k2[3]
k2[3]=1
Column 4: k0[4]=k1[4]=k2[4]
Column 5:
Column 6: k0[6]=k1[6]
Column 7: k0[7]=k1[7]
Column 8:
Column 9: k0[9]=k1[9]=k2[9]
Column 10:
Column 11:
Column 12: k0[12]=k1[12]
Column 13:
Column 14:
Column 15:


Pattern A
(38 conditions)
Column 16:
Column 17:
Column 18: k1[18]=k2[18]
Column 19:k0[19]=k1[19]=k2[19]=0
Column 20:
Column 21: k2[21]=0
Column 22: k0[22]=k1[22]
Column 23: k2[23]=0
Column 24 :
Column 25: k0[25]=k1[25]
Column 26: k0[26]=k1[26]
Column 27:
Column 28:k0[28]=k1[28]=k2[28]=0
Column 29:
Column 30:
Column 31: k0[31]=k1[31]
Pattern B
(19 conditions)
Column 16:
Column 17:
Column 18:
Column 19:
Column 20:
Column 21:
Column 22:
Column 23:
Column 24 :
Column 25:
Column 26: k0[26]=k1[26]
Column 27: k0[27]=k1[27] +c1
Column 28:
Column 29:
Column 30:
Column 31:
Pattern B »»5
(19 conditions)
Column 16:
Column 17:
Column 18:
Column 19:
Column 20:
Column 21:
Column 22:
Column 23:
Column 24 :
Column 25:
Column 26:
Column 27:
Column 28:
Column 29:
Column 30:
Column 31: k0[31]=k1[31]
Pattern B »»12
(19 conditions)
Column 16: k0[16]=k1[16] +a3
Column 17: k0[17]=k1[17] +b3
Column 18:
Column 19: k0[19]=k1[19]=k2[19]
Column 20:
Column 21:
Column 22: k0[22]=k1[22]
Column 23:
Column 24 :
Column 25:
Column 26:
Column 27:
Column 28:
Column 29:
Column 30:
Column 31:
Pattern B »»2
(19 conditions)
Column 16:
Column 17:
Column 18:
Column 19:
Column 20:
Column 21:
Column 22:
Column 23:
Column 24 :
Column 25:
Column 26:
Column 27:
Column 28: k0[28]=k1[28]
Column 29: k0[29]=k1[29] +a4
Column 30:
Column 31:


Pattern A
(38 conditions)
Column 32:
Column 33:
Column 34:
Column 35:
Column 36:
Column 37
Column 38:
Column 39:
Column 40 :
Column 41:
Column 42: k2[42]=0
Column 43:
Column 44: k0[44]=k1[44]
Column 45:
Column 46:
Column 47: k1[47]=k2[47]
Pattern B
(19 conditions)
Column 32: k0[32]=k1[32] +d1
Column 33:
Column 34:
Column 35:
Column 36:
Column 37
Column 38:
Column 39:
Column 40 :
Column 41:
Column 42:
Column 43:
Column 44:
Column 45:
Column 46:
Column 47:
Pattern B >>>5
(19 conditions)
Column 32: k0[32]=k1[32] +d1
Column 33:
Column 34:
Column 35:
Column 36:
Column 37: k0[37]=k1[37] +b2
Column 38:
Column 39:
Column 40 :
Column 41:
Column 42:
Column 43:
Column 44:
Column 45:
Column 46:
Column 47:
Pattern B >>>12
(19 conditions)
Column 32:
Column 33:
Column 34:
Column 35:
Column 36:
Column 37:
Column 38: k0[38]=k1[38] +c3
Column 39: k0[39]=k1[39] +d3
Column 40 :
Column 41:
Column 42:
Column 43:
Column 44: k0[44]=k1[44]
Column 45:
Column 46:
Column 47:
Pattern B >>>2
(19 conditions)
Column 32:
Column 33:
Column 34: k0[34]=k1[34] +b4
Column 35:
Column 36:
Column 37
Column 38:
Column 39:
Column 40 :
Column 41:
Column 42:
Column 43:
Column 44:
Column 45:
Column 46:
Column 47:


Pattern A
(38 conditions)
Column 48 : k1[48]=k2[48]
Column 49:
Column 50:
Column 51: k2[51]=0
Column 52:
Column 53: k0[53]=k1[53]=k2[53]
Column 54: k1[54]=k2[54]
Column 55: k1[55]=k2[55]
Column 56:
Column 57: k2[57]=0
Column 58:
Column 59:
Column 60: k1[60]=k2[60]
Column 61:
Column 62:
Column 63:
Pattern B
(19 conditions)
Column 48 : k1[48]=k2[48]
Column 49 : k1[49]=k2[49] +e1
Column 50:
Column 51:
Column 52:
Column 53:
Column 54: k1[54]=k2[54]
Column 55: k1[55]=k2[55]
Column 56: k1[56]=k2[56] +f1
Column 57:
Column 58:
Column 59:
Column 60:
Column 61: k1[61]=k2[61] +g1
Column 62:
Column 63:
Pattern B >>>5
(19 conditions)
Column 48:
Column 49:
Column 50:
Column 51:
Column 52:
Column 53: k1[53]=k2[53]
Column 54: k1[54]=k2[54]
Column 55:
Column 56 :
Column 57:
Column 58:
Column 59: k1[59]=k2[59] +c2
Column 60: k1[60]=k2[60]
Column 61: k1[61]=k2[61] +g1
Column 62:
Column 63:
Pattern B >>>12
(19 conditions)
Column 48:
Column 49:
Column 50:
Column 51:
Column 52:
Column 53:
Column 54:
Column 55:
Column 56 :
Column 57:
Column 58:
Column 59:
Column 60: k1[60]=k2[60]
Column 61: k1[61]=k2[61] +g1
Column 62:
Column 63:
Pattern B >>>2
(19 conditions)
Column 48:
Column 49:
Column 50: k1[50]=k2[50] +c4
Column 51: k1[51]=k2[51] +d4
Column 52:
Column 53:
Column 54:
Column 55:
Column 56 : k1[56]=k2[56] +f1
Column 57: k1[57]=k2[57] +e4
Column 58: k1[58]=k2[58] +f4
Column 59:
Column 60:
Column 61:
Column 62:
Column 63: k1[63]=k2[63] +g4

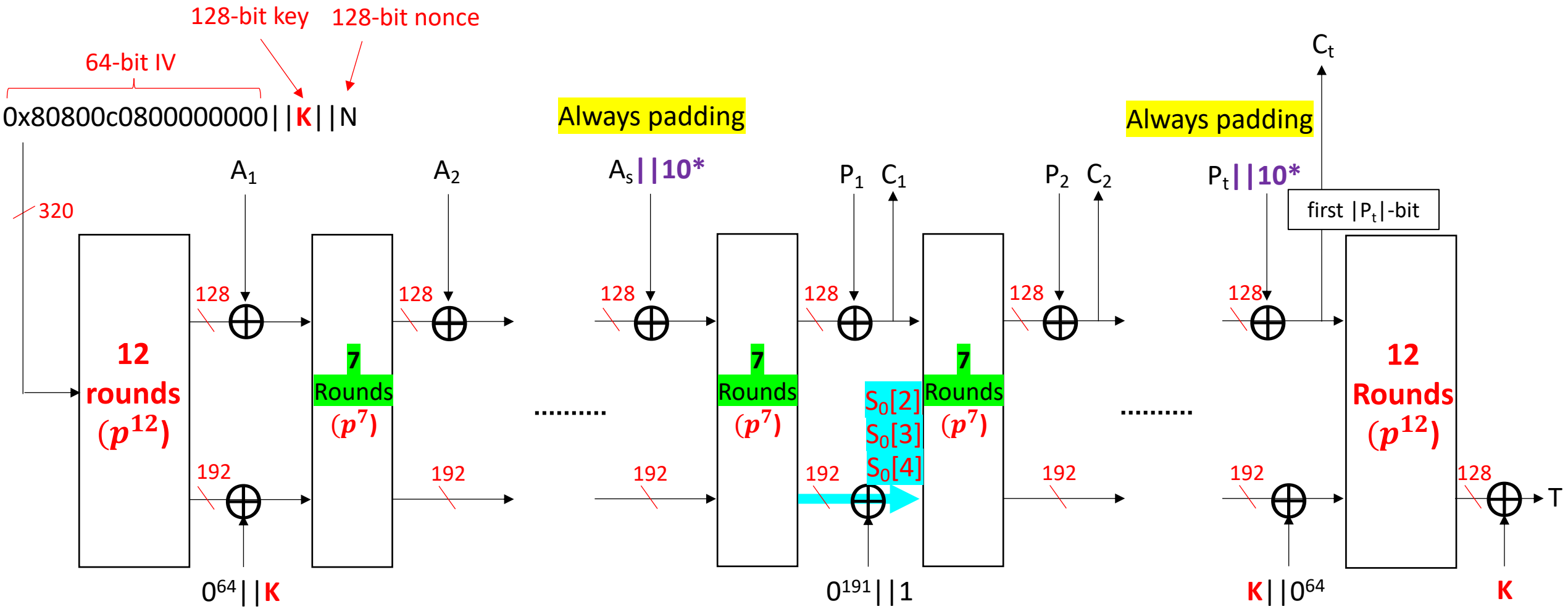


The total query-complexity is about 2^{117} to recover 74-bit secret information.

The remaining 118-bit can be found by the exhaustive search with time-complexity 2^{118}.

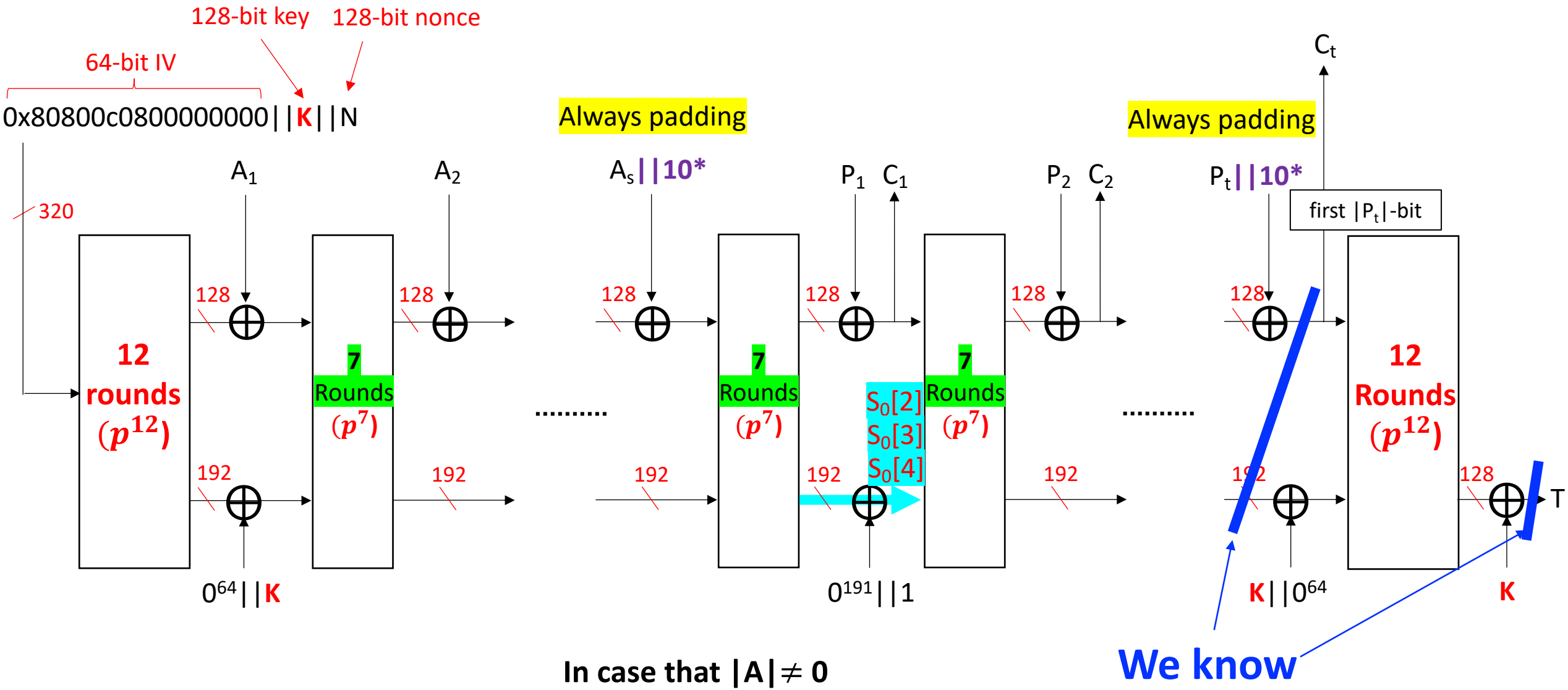
Key Recovery Attack

After recovering the 192-bit secret state ($S_0[2], S_0[3], S_0[4]$),



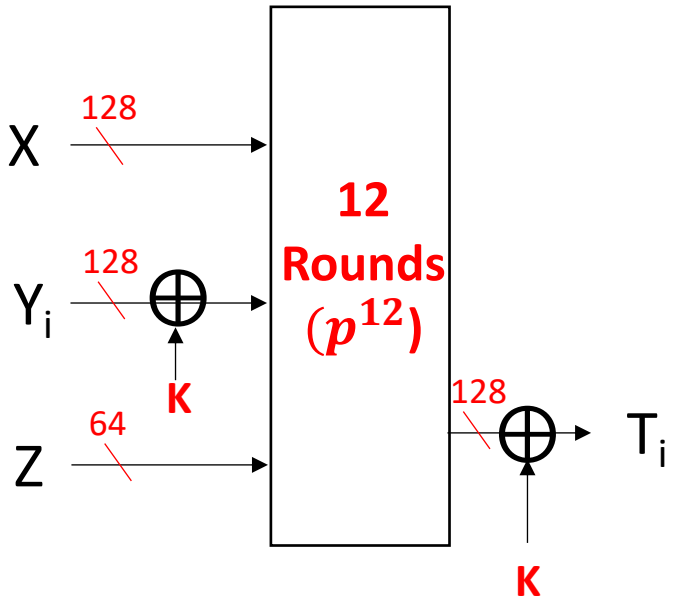
In case that $|A| \neq 0$

After recovering the 192-bit secret state ($S_0[2], S_0[3], S_0[4]$),



Due to 10* padding, not 96 but 97.

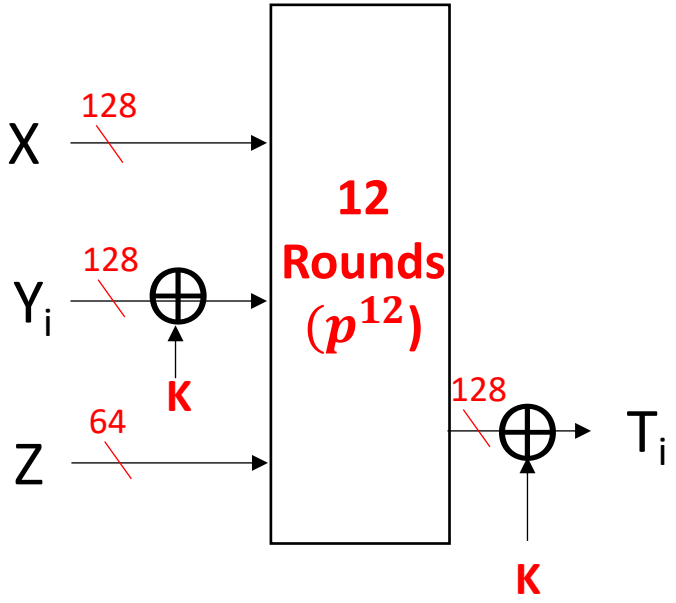
Through 2^{32} queries and 2^{97} time,
store (Y_i,T_i)'s with fixed X and Z,
where $1 \leq i \leq 2^{32}$.



(ONLINE PHASE)

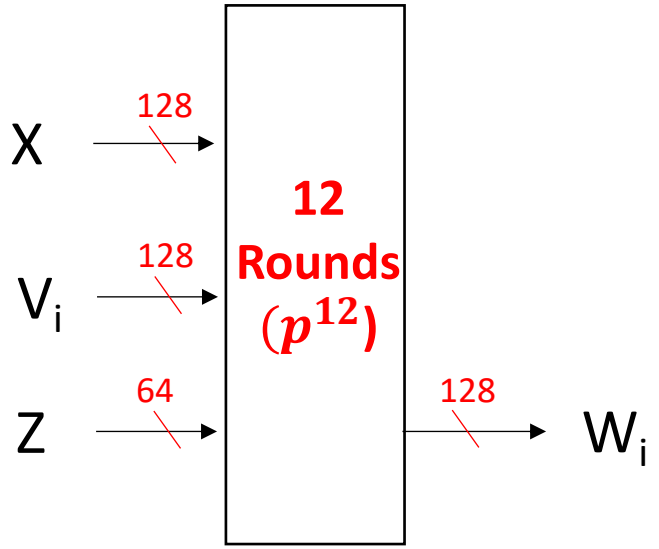
Due to 10* padding, not 96 but 97.

Through 2^{32} queries and 2^{97} time, store (Y_i,T_i)'s with fixed X and Z, where $1 \leq i \leq 2^{32}$.



(ONLINE PHASE)

Find i and j such that $Y_i \oplus T_i = V_j \oplus W_j$ with about time 2^{96}. **Then, K will be $Y_i \oplus V_j$.**



(OFFLINE PHASE)

Conclusion

- In a nonce-misuse scenario, we showed how to recover a secret state and secret key with data complexity 2^{117} and time complexity 2^{118} when only one round is reduced during the encryption phase.

- The attack does not violate any of the designers' claims. Still of interest to see the resistance of Ascon-128a against nonce-misuse attacks.

Table 1: Summary of cube attacks on ASCON-128a

Attack type	Method	Rounds [1] (12, 8, 12)	Data	Time	Memory	Nonce misuse	Ref.
Key recovery	Conditional cube	6,⋆,⋆	2^{40}	2^{40}	-	No	[LDW17]
	Cube	7,⋆,⋆	$2^{77.2}$	$2^{103.92}$	-	No	[LDW17]
	Cube	7,⋆,⋆	2^{64}	2^{123}	-	No	[RHSS21]
	Cube	7,5,⋆	2^{33}	2^{97}	-	Yes	[LZWW17]
	Conditional cube	⋆,7,⋆	2^{117}	2^{118}	2^{32}	Yes	this study
Forgery	Cube	⋆,⋆,5	2^{17}	2^{17}	-	Yes	[LZWW17]
	Cube	⋆,⋆,6	2^{33}	2^{33}	-	Yes	[LZWW17]
State-recovery	Conditional cube	⋆,7,⋆	2^{117}	2^{118}	-	Yes	this study

Pattern-A

We can show that

- Case 1) one of the column-0 conditions are not true.

  - There is a multiplication between v_0 and v_i for some i ($1 \leq i \leq 63$) after 2 rounds.

- Case 2) All of the column-0 conditions are true.

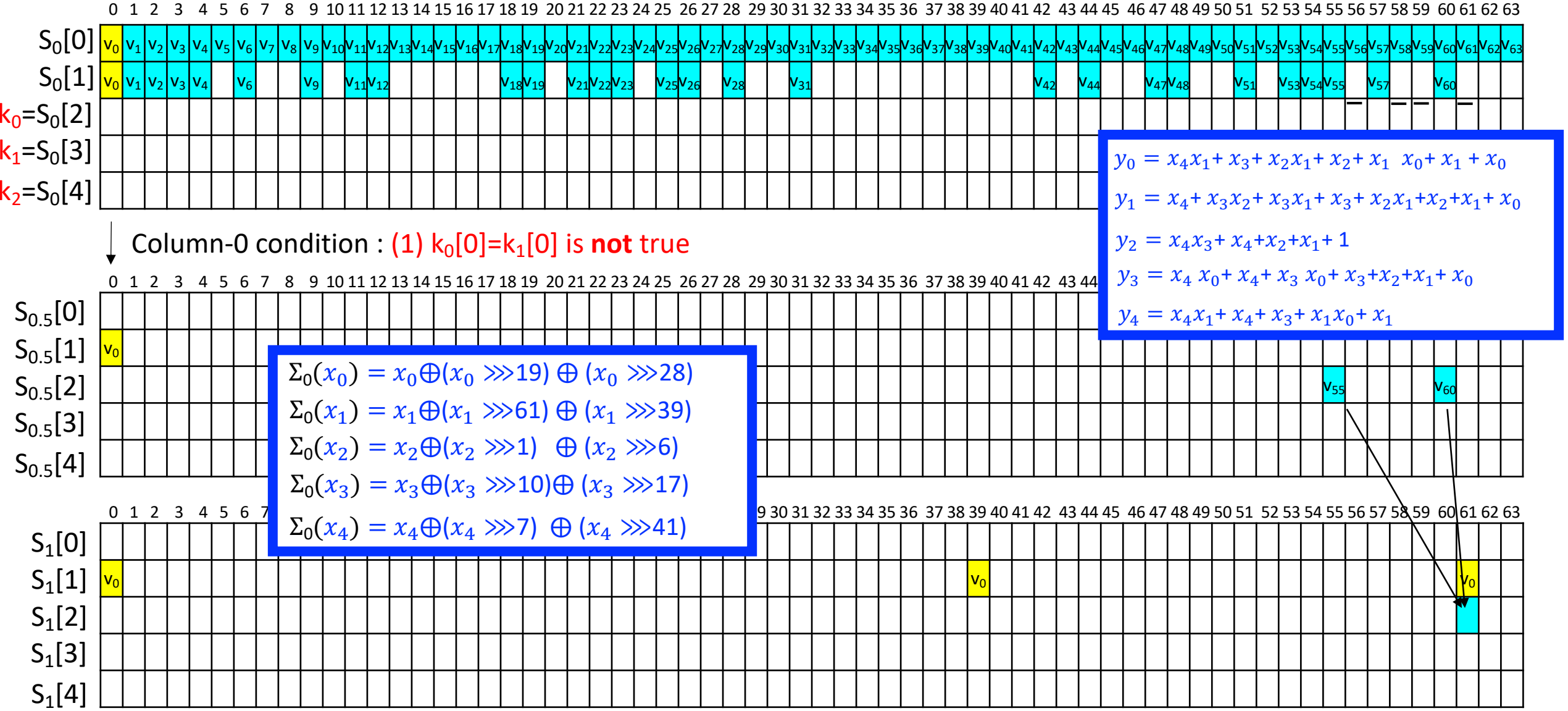
  - If any of the column-i conditions ($1 \leq i \leq 63$) is not true, then there is a multiplication between v_0 and v_i after 2 rounds.

⇨ These means that If any of the column-i conditions ($0 \leq i \leq 63$) is not true, then there is a multiplication between v_0 and v_j for some j ($1 \leq j \leq 63$) after 2 rounds.

⇨ v_0 is the conditional cube variable and v_j's ($1 \leq j \leq 63$) are ordinary cube variables.

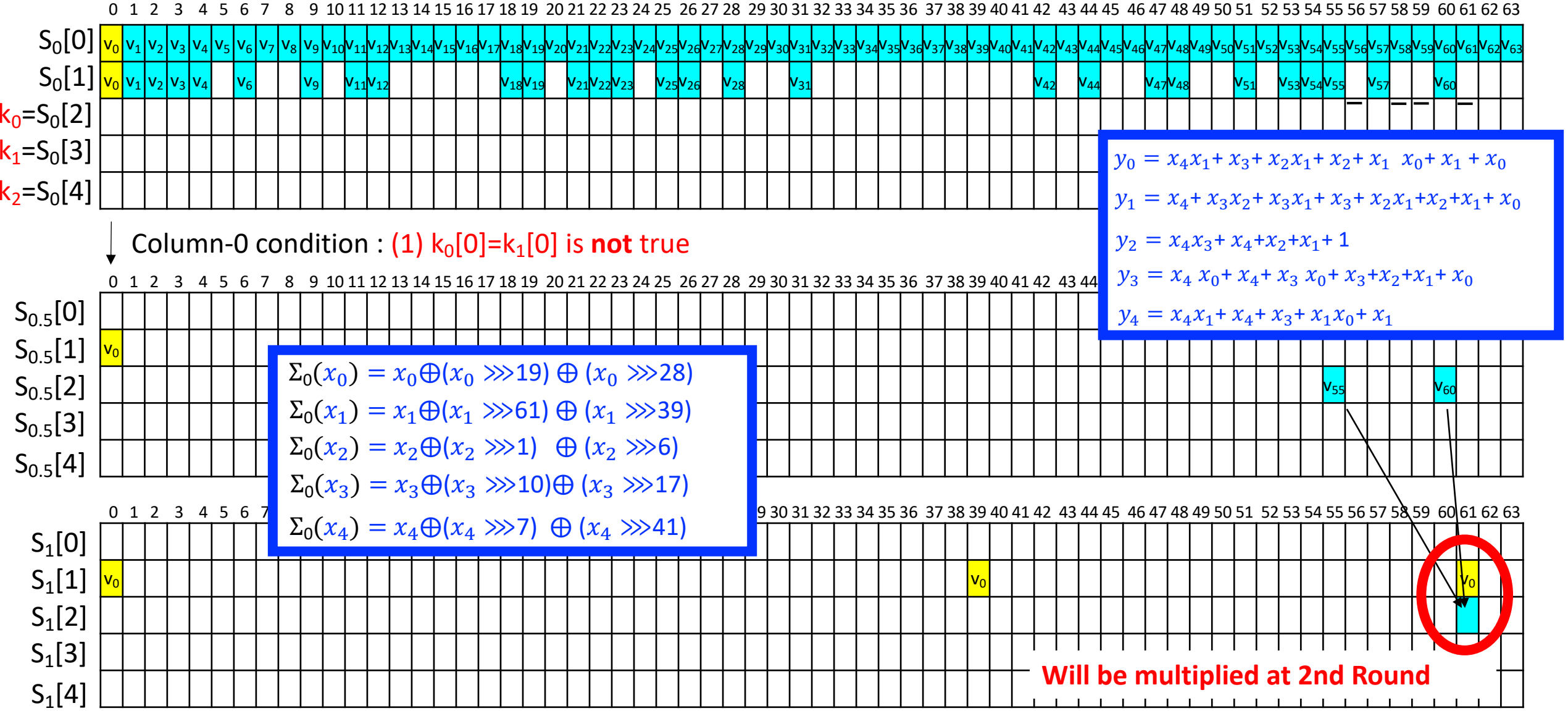
Pattern-A

Case 1) one of the column-0 conditions are not true.



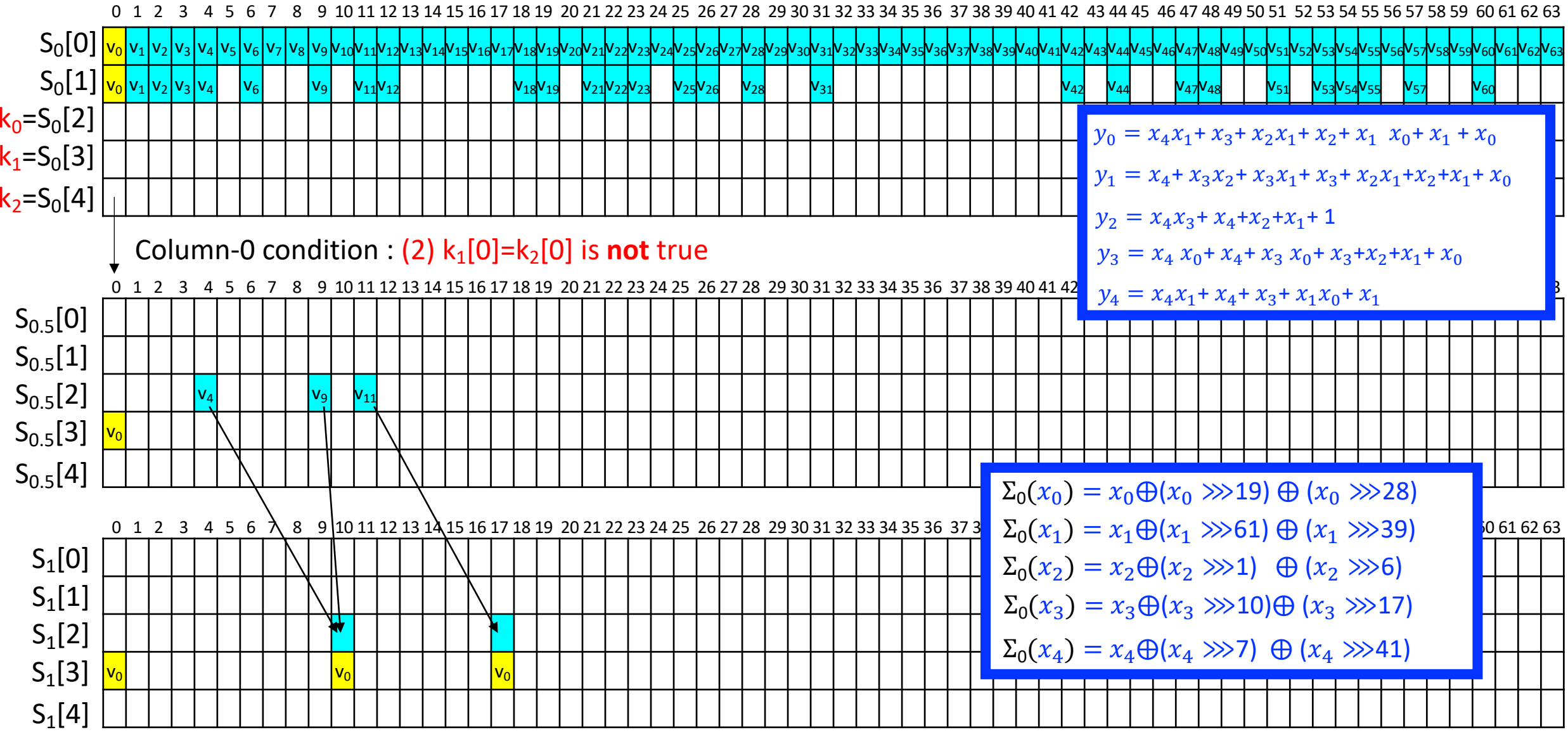
Pattern-A

Case 1) one of the column-0 conditions are not true.



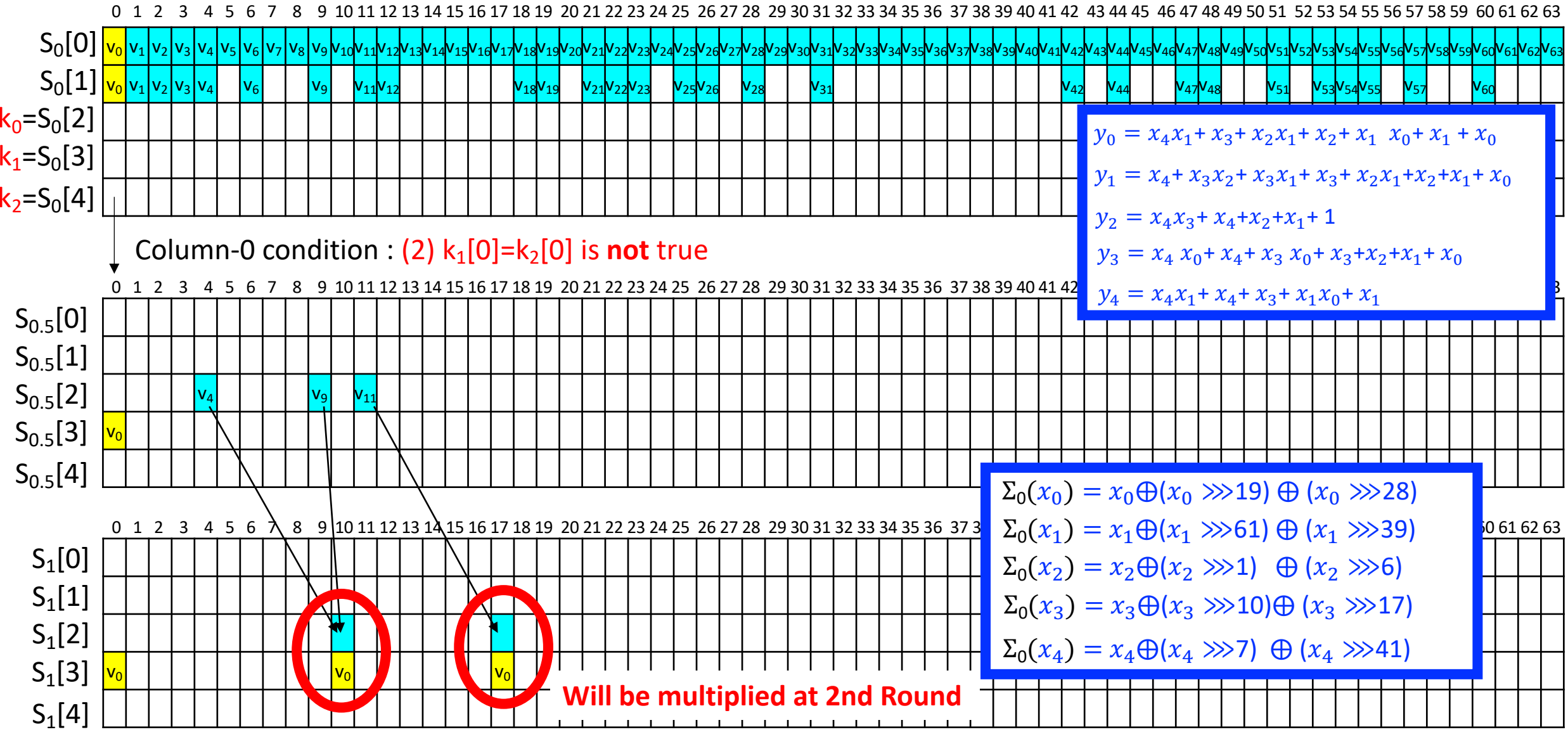
Pattern-A

Case 1) one of the column-0 conditions are not true.



Pattern-A

Case 1) one of the column-0 conditions are not true.



$$y_0 = x_4x_1 + x_3 + x_2x_1 + x_2 + x_1\ \ x_0 + x_1 + x_0$$
$$y_1 = x_4 + x_3x_2 + x_3x_1 + x_3 + x_2x_1 + x_2 + x_1 + x_0$$
$$y_2 = x_4x_3 + x_4 + x_2 + x_1 + 1$$
$$y_3 = x_4\ x_0 + x_4 + x_3\ x_0 + x_3 + x_2 + x_1 + x_0$$
$$y_4 = x_4x_1 + x_4 + x_3 + x_1x_0 + x_1$$

$$\Sigma_0(x_0) = x_0 \oplus (x_0 \ggg 19) \oplus (x_0 \ggg 28)$$
$$\Sigma_0(x_1) = x_1 \oplus (x_1 \ggg 61) \oplus (x_1 \ggg 39)$$
$$\Sigma_0(x_2) = x_2 \oplus (x_2 \ggg 1) \oplus (x_2 \ggg 6)$$
$$\Sigma_0(x_3) = x_3 \oplus (x_3 \ggg 10) \oplus (x_3 \ggg 17)$$
$$\Sigma_0(x_4) = x_4 \oplus (x_4 \ggg 7) \oplus (x_4 \ggg 41)$$

Pattern-B

We can show that

- Case 1) one of the column-1 conditions are not true.

  - There is a multiplication between v_1 and v_i for some i ($0 \leq i \leq 63$, $i \neq 1$) after 2 rounds.

- Case 2) All of the column-1 conditions are true.

  - If any of the column-i conditions ($0 \leq i \leq 63$, $i \neq 1$) is not true, then there is a multiplication between v_1 and v_i after 2 rounds.

⇨ These means that If any of the column-i conditions ($0 \leq i \leq 63$) is not true, then there is a multiplication between v_1 and v_j for some j ($0 \leq j \leq 63$, ,$j \neq 1$) after 2 rounds.

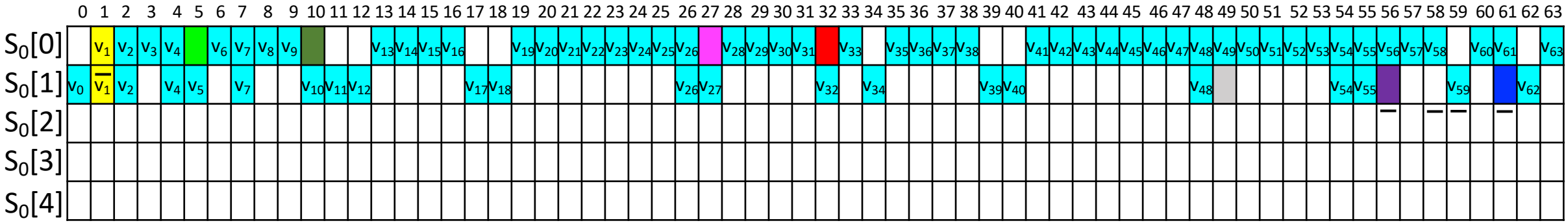
⇨ v_1 is the conditional cube variable and v_j's ($0 \leq j \leq 63$, ,$j \neq 1$) are ordinary cube variables.

Pattern-B

Case 1) one of the column-1 conditions are not true.

If **b1=0**, then $S_0[0][10] \leftarrow v_{10}$. If **d1=0**, then $S_0[0][32] \leftarrow v_{32}$. If **f1=0**, then $S_0[1][56] \leftarrow v_{56}$.

If **a1=0**, then $S_0[0][5] \leftarrow v_5$. If **c1=0**, then $S_0[0][27] \leftarrow v_{27}$. If **e1=0**, then $S_0[1][49] \leftarrow v_{49}$. If **g1=0**, then $S_0[1][61] \leftarrow v_{61}$.



Three conditions :

(1) $k_0[1]=k_1[1]$ is **not** true or

(2) $k_1[1]=k_2[1]$ is **not** true or

(3) $k_2[1]=1$ is **not** true.

$$y_0 = x_4x_1 + x_3 + x_2x_1 + x_2 + x_1\ \ x_0 + x_1 + x_0$$

$$y_1 = x_4 + x_3x_2 + x_3x_1 + x_3 + x_2x_1 + x_2 + x_1 + x_0$$

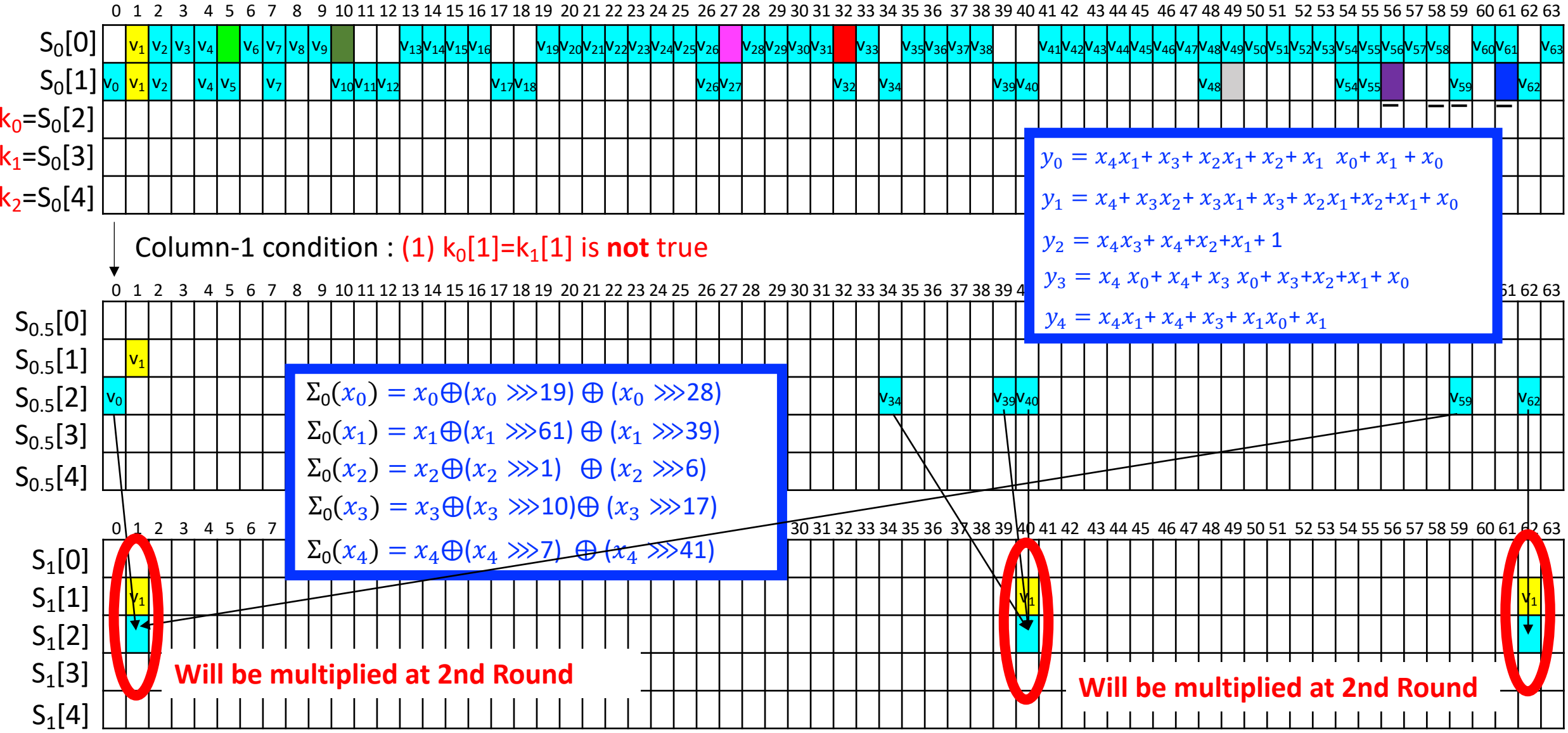
$$y_2 = x_4x_3 + x_4 + x_2 + x_1 + 1$$

$$y_3 = x_4\ x_0 + x_4 + x_3\ x_0 + x_3 + x_2 + x_1 + x_0$$

$$y_4 = x_4x_1 + x_4 + x_3 + x_1x_0 + x_1$$

Pattern-B

Case 1) one of the column-1 conditions are not true.



Pattern-B

Case 1) one of the column-1 conditions are not true.