Correlation Power Analysis on Ascon with Multi-bit Selection Function

Viet-Sang Nguyen

joint work with Vincent Grosso and Pierre-Louis Cayrel

SECRYPT

Bilbao, 11 June, 2025

UNIVERSITÉ DE LYON

UNIVERSITÉ JEAN MONNET SAINT-ÉTIENNE

Laboratoire Hubert Curien
UMR ▪ CNRS ▪ 5516 ▪ Saint-Étienne

anr
PROPHY ANR-22-CE39-0008-01

NIST

2018  Lightweight cryptography competition

NIST

2018  Lightweight cryptography competition

2023  Selected Ascon

NIST

2018  Lightweight cryptography competition

2023  Selected Ascon

NIST

2018  Lightweight cryptography competition

2023  Selected Ascon

 Possible attacks

 Secure implementations

In this talk

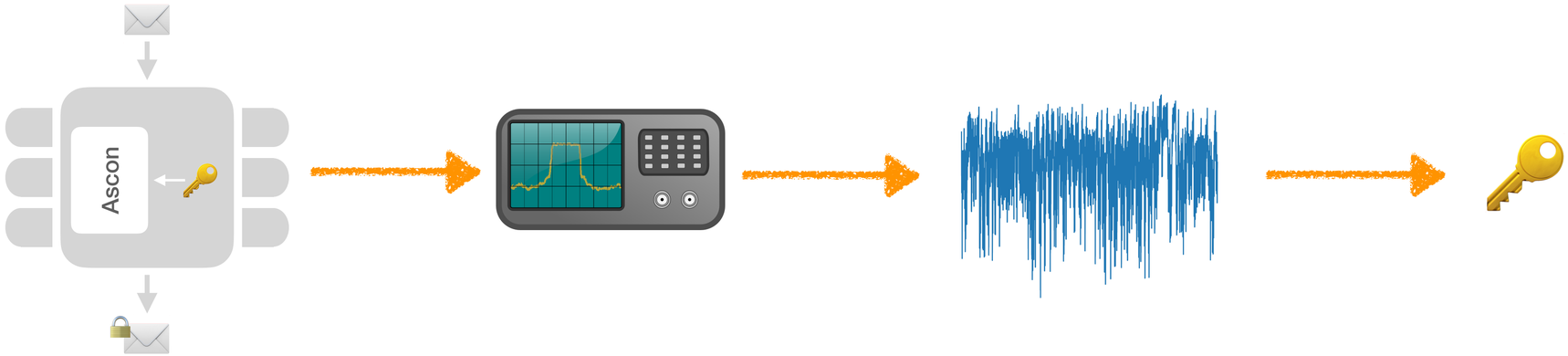
Possible attacks

In this talk

Possible attacks

Correlation Power Analysis (CPA) attack

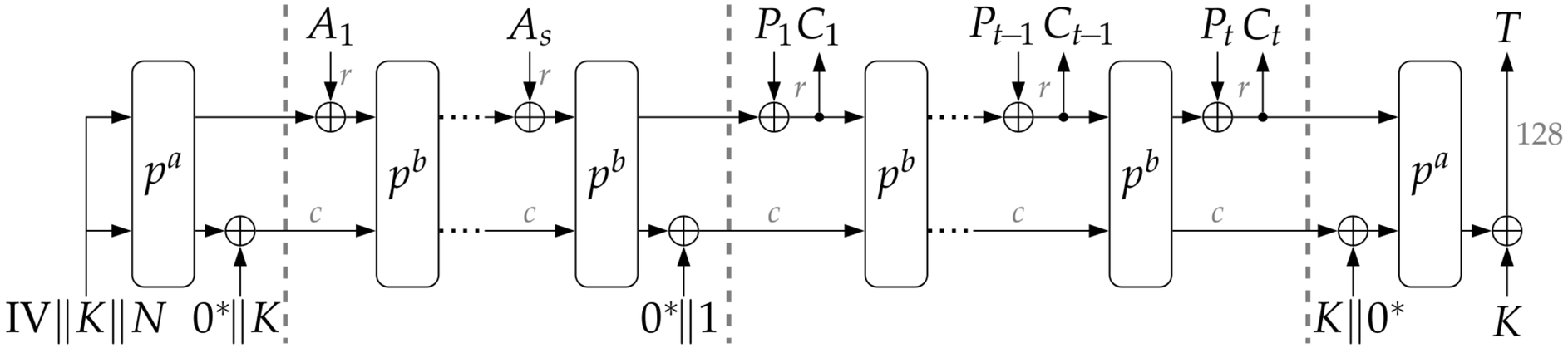
In this talk



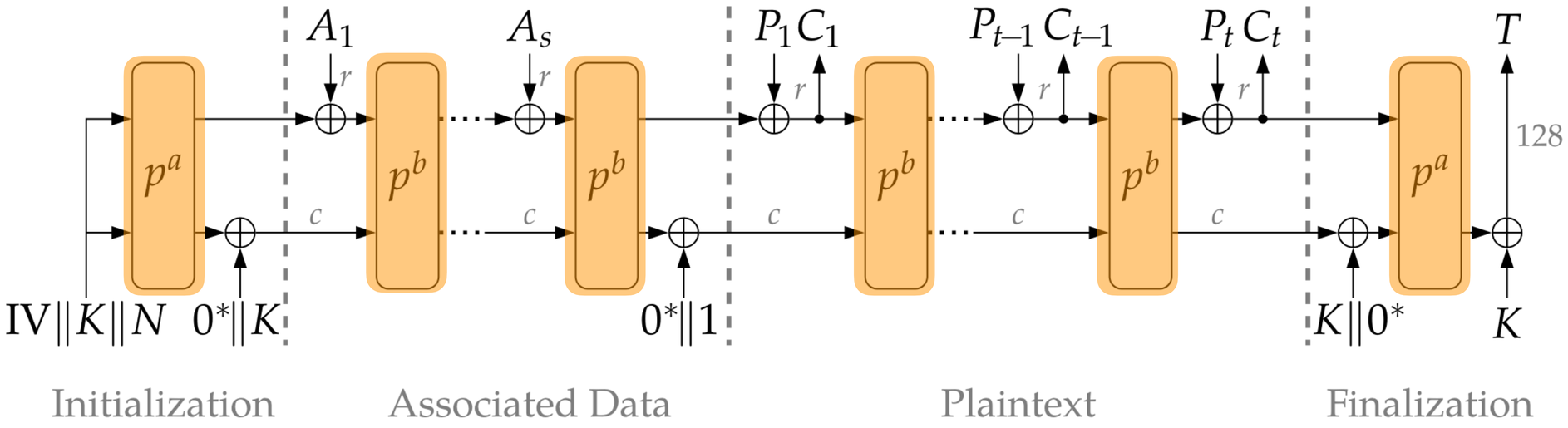
Possible attacks

Correlation Power Analysis (CPA) attack

Ascon

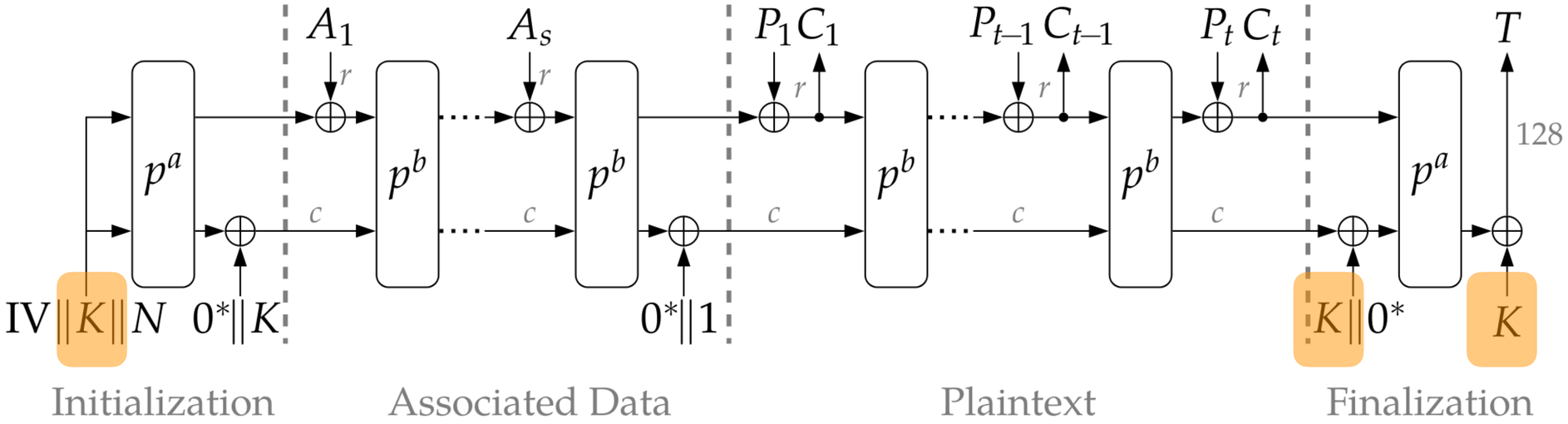

A_1
A_s
$P_1 C_1$
$P_{t-1} C_{t-1}$
$P_t C_t$
T
r
p^a
p^b
c
128
$\mathrm{IV} \| K \| N$
$0^* \| K$
$0^* \| 1$
$K \| 0^*$
K
Initialization
Associated Data
Plaintext
Finalization

Permutation blocks

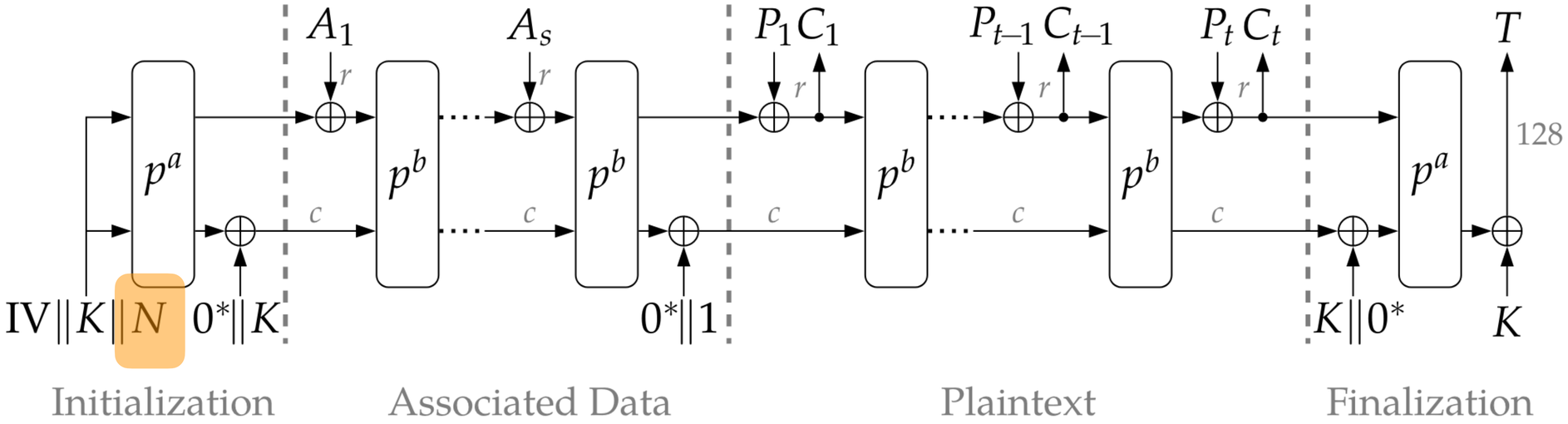


- p^a: 12 permutation rounds ($a = 12$)
- p^b: 8 permutation rounds ($b = 8$)

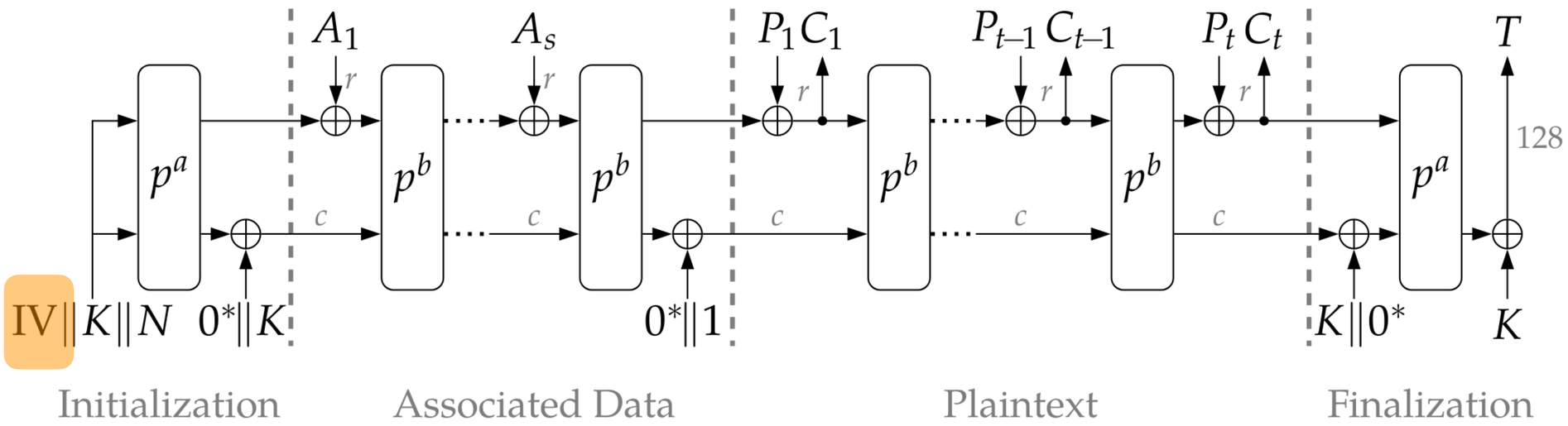
Key (128 bits)


A_1
A_s
$P_1 C_1$
$P_{t-1} C_{t-1}$
$P_t C_t$
T
r
c
p^a
p^b
128
IV ‖ K ‖ N
0^* ‖ K
0^* ‖ 1
K ‖ 0^*
K
Initialization
Associated Data
Plaintext
Finalization

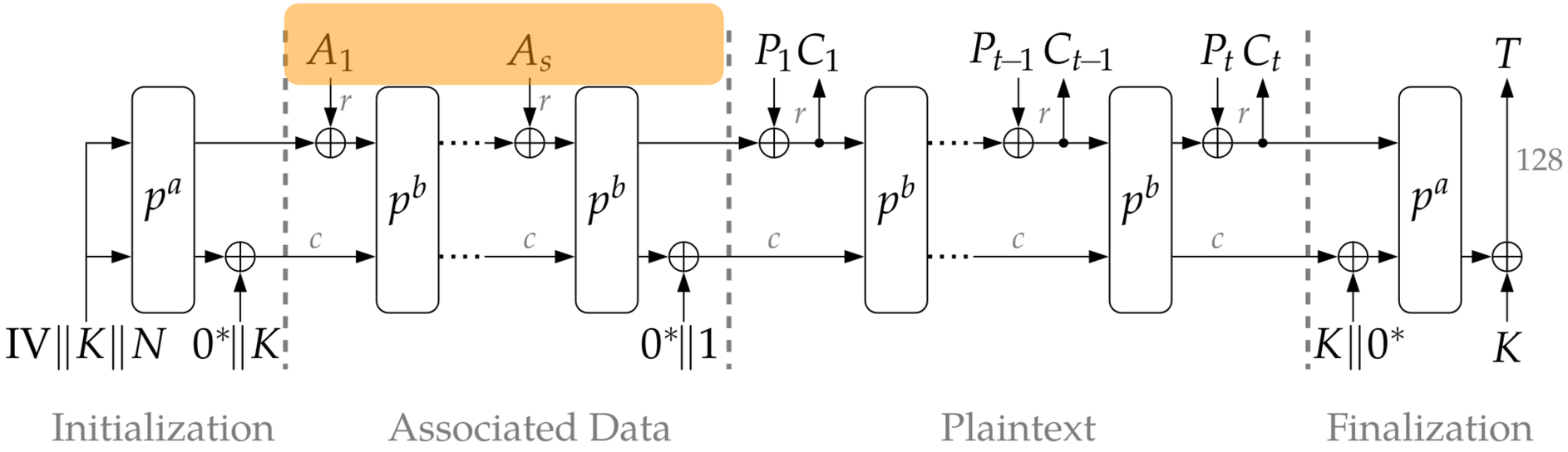
Nonce (128 bits)



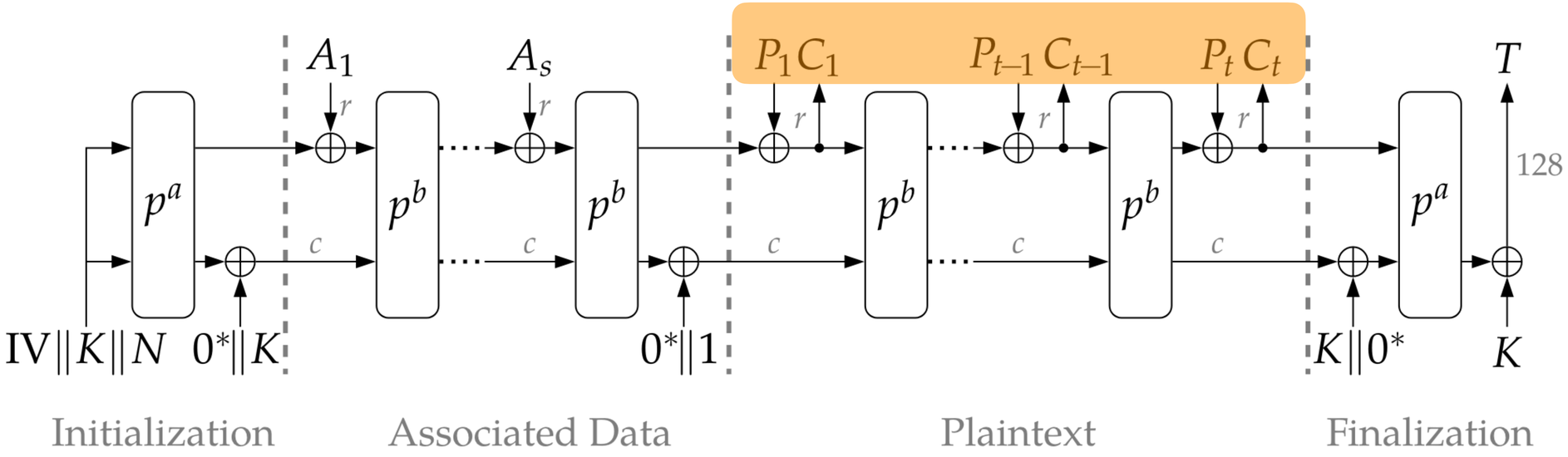
Initialization vector



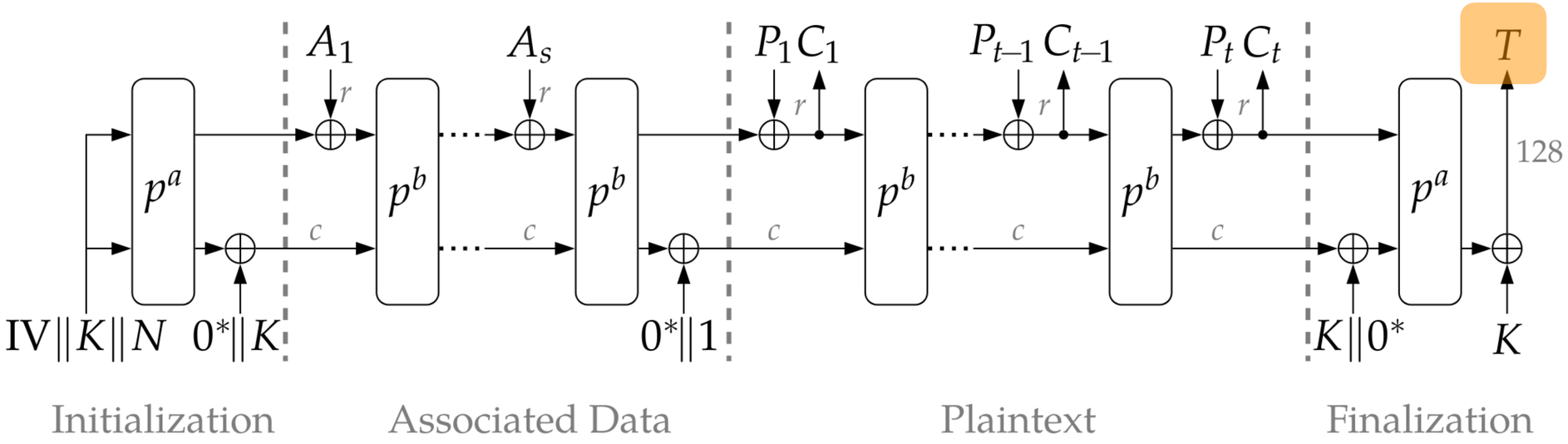
Associated data

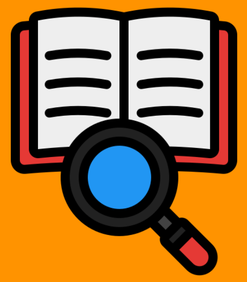


Plaintext / Ciphertext

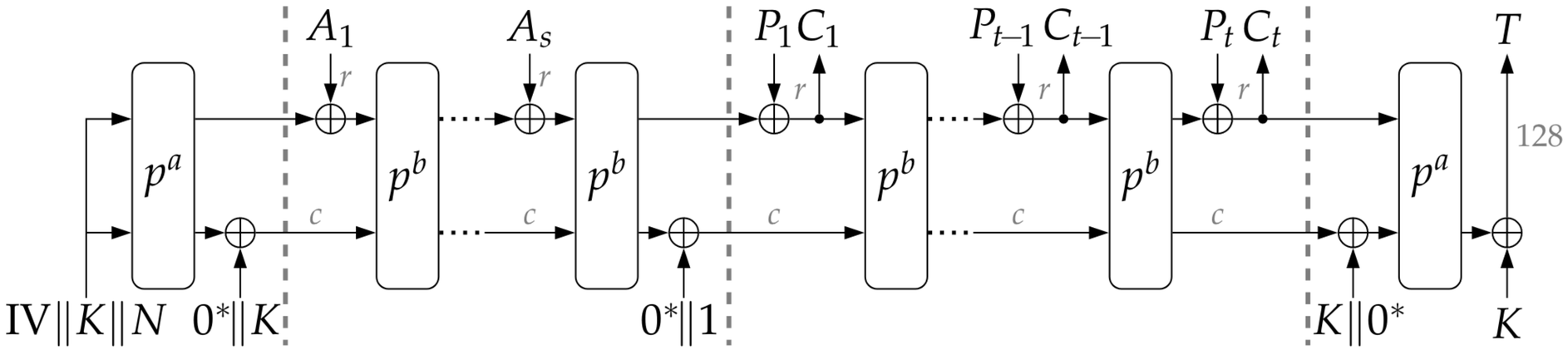


Verification Tag

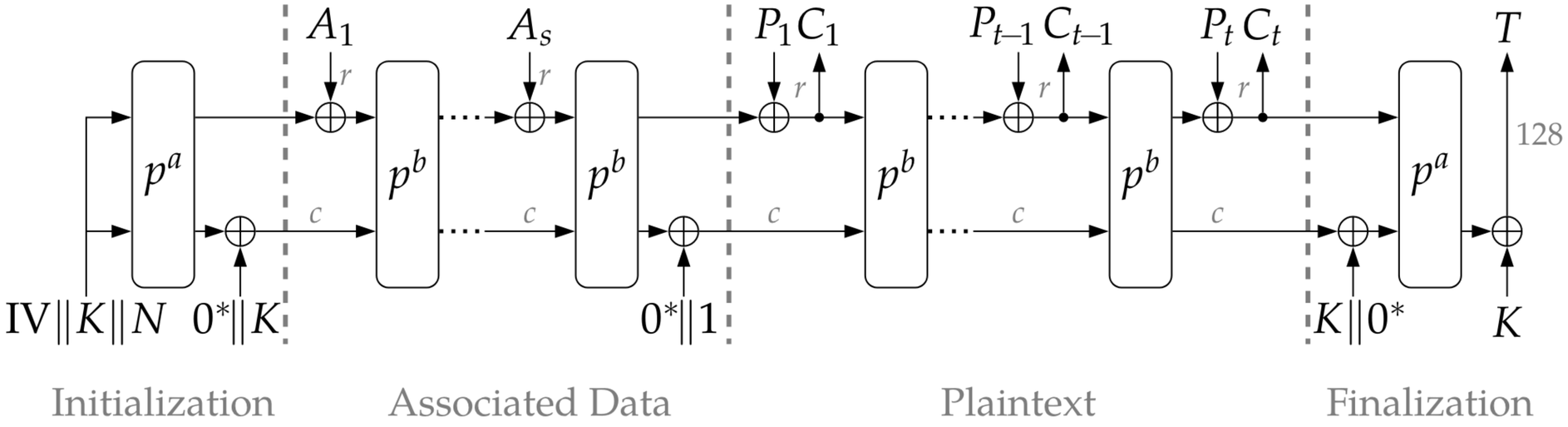




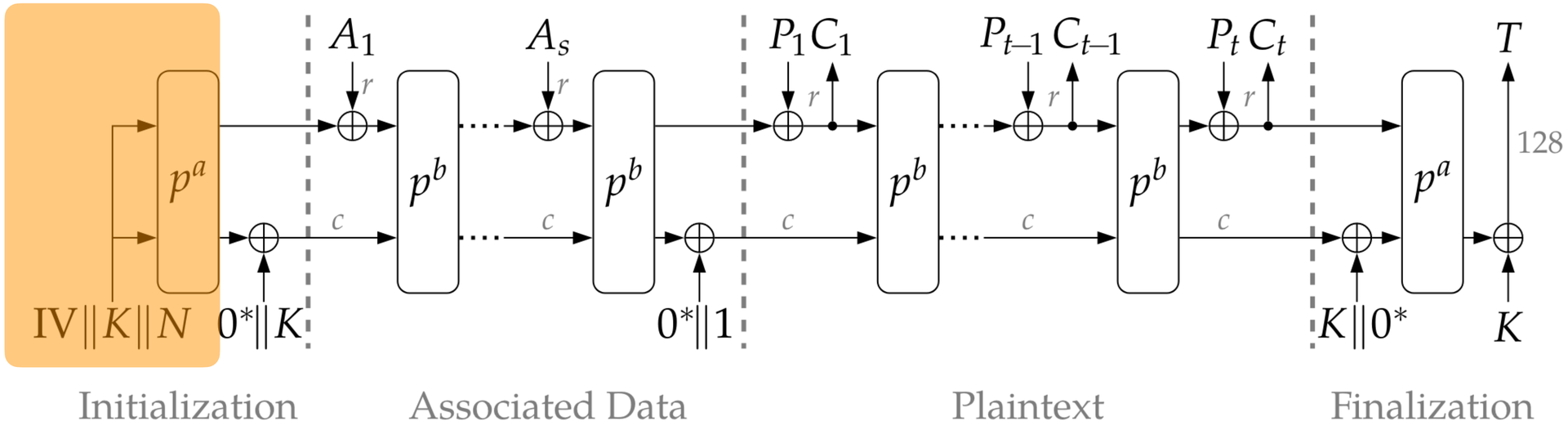
Correlation Power Analysis (CPA) on Ascon


A_1
A_s
$P_1 C_1$
$P_{t-1} C_{t-1}$
$P_t C_t$
T
r
c
p^a
p^b
128
$\mathrm{IV} \| K \| N$
$0^* \| K$
$0^* \| 1$
$K \| 0^*$
K
Initialization
Associated Data
Plaintext
Finalization

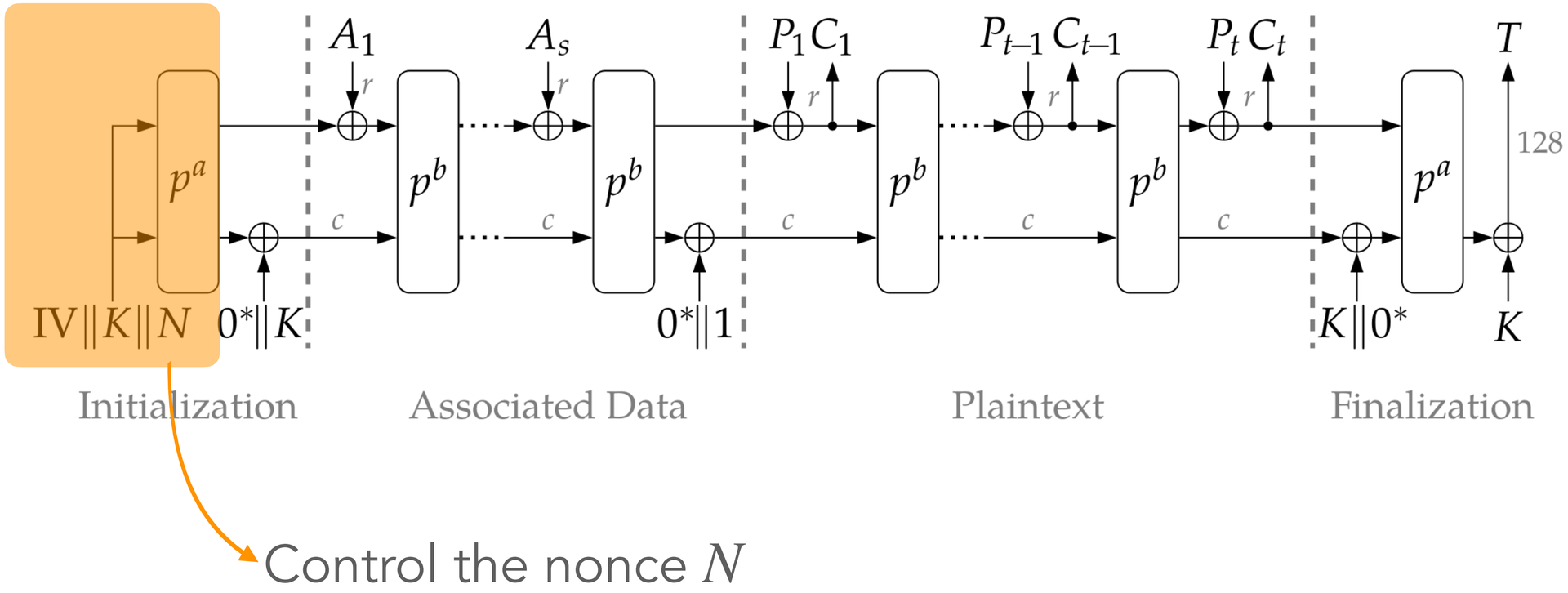
Focus on 1st round of initialization



Focus on 1st round of initialization

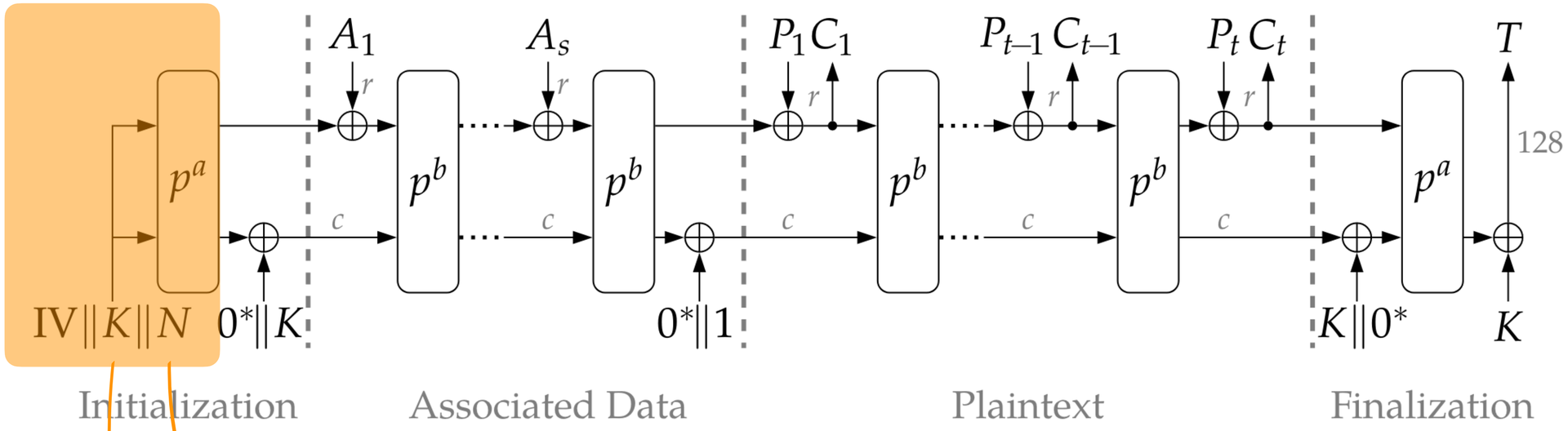


Focus on 1st round of initialization



Control the nonce N

Focus on 1st round of initialization



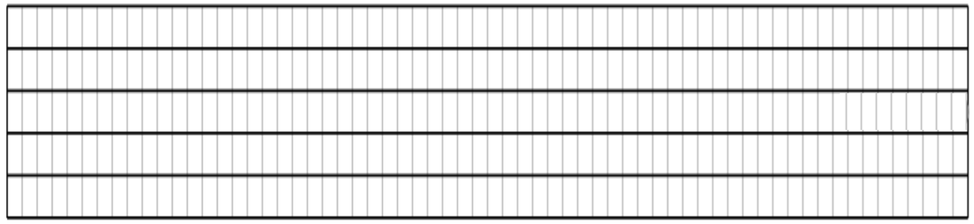
Control the nonce N

Guess the key K

1st round computation

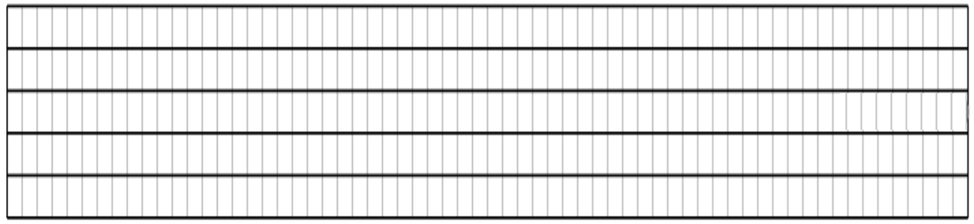
1st round computation

On 320-bit state = 5 x 64-bit words



1st round computation

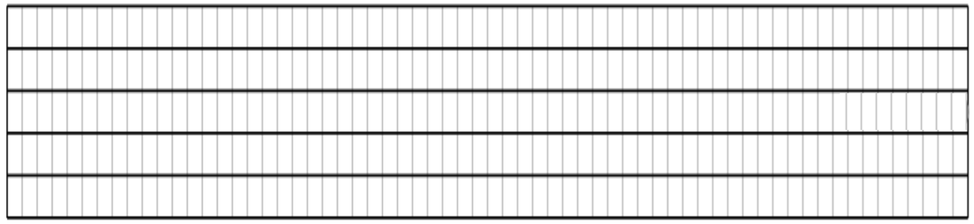
On 320-bit state = 5 x 64-bit words



Input of the first round:

1st round computation

On 320-bit state = 5 x 64-bit words

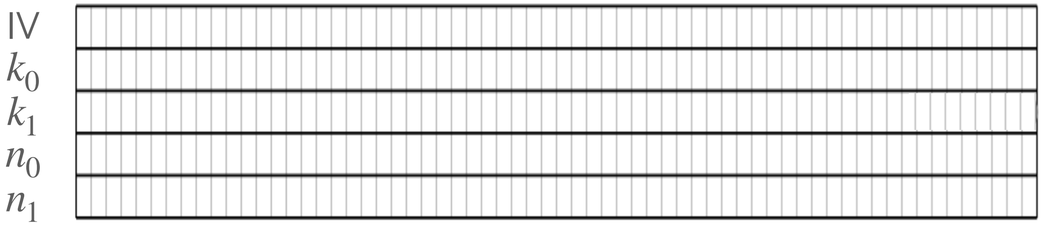


Input of the first round:

- 128-bit key : $K = (k_0, k_1)$
- 128-bit nonce : $N = (n_0, n_1)$
- 64-bit init. vector : IV

1st round computation

On 320-bit state = 5 x 64-bit words

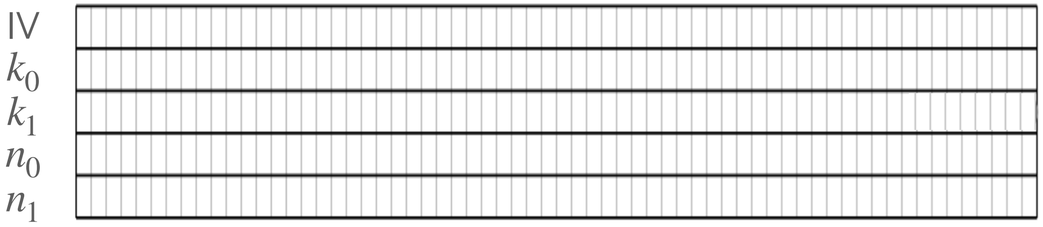


Input of the first round:

- 128-bit key : $K = (k_0, k_1)$
- 128-bit nonce : $N = (n_0, n_1)$
- 64-bit init. vector : IV

1st round computation

On 320-bit state = 5 x 64-bit words



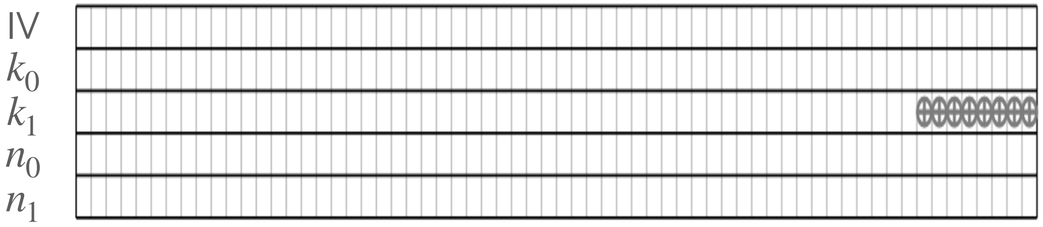
Input of the first round:

- 128-bit key : $K = (k_0, k_1)$
- 128-bit nonce : $N = (n_0, n_1)$
- 64-bit init. vector : IV

3 operations in a round

1st round computation

On 320-bit state = 5 x 64-bit words



(1) Constant addition

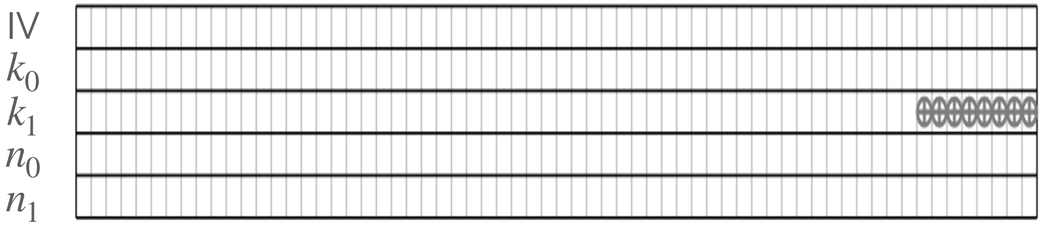
Input of the first round:

- 128-bit key : $K = (k_0, k_1)$
- 128-bit nonce : $N = (n_0, n_1)$
- 64-bit init. vector : IV

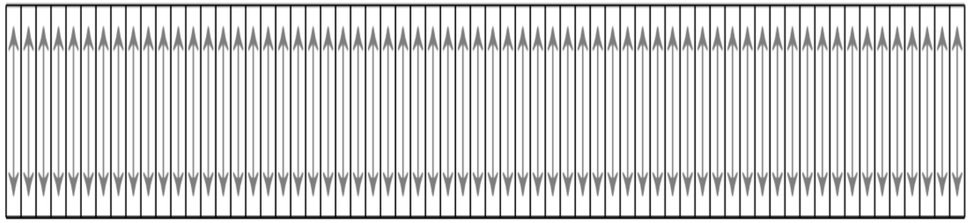
3 operations in a round

1st round computation

On 320-bit state = 5 x 64-bit words



(1) Constant addition



(2) Substitution *(vertical)*

Input of the first round:

- 128-bit key : $K = (k_0, k_1)$
- 128-bit nonce : $N = (n_0, n_1)$
- 64-bit init. vector : IV

3 operations in a round

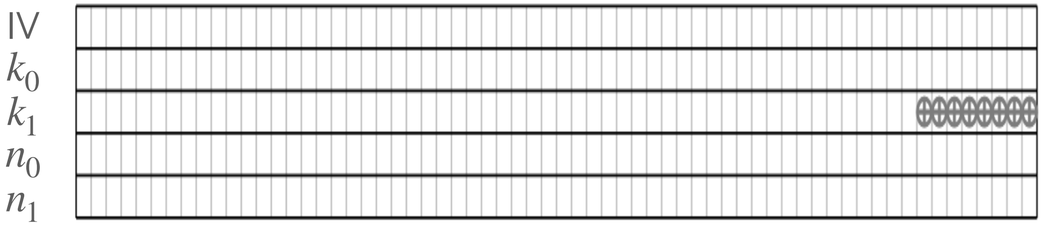
1st round computation

On 320-bit state = 5 x 64-bit words

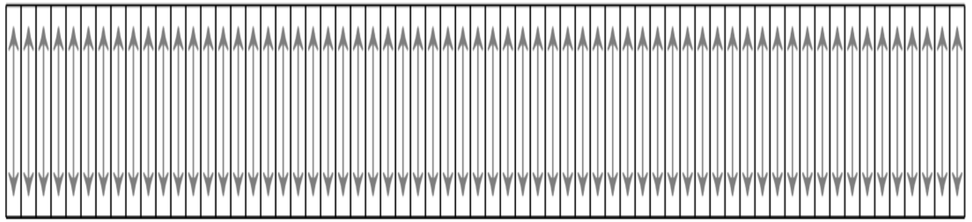
Input of the first round:

- 128-bit key : $K = (k_0, k_1)$
- 128-bit nonce : $N = (n_0, n_1)$
- 64-bit init. vector : IV

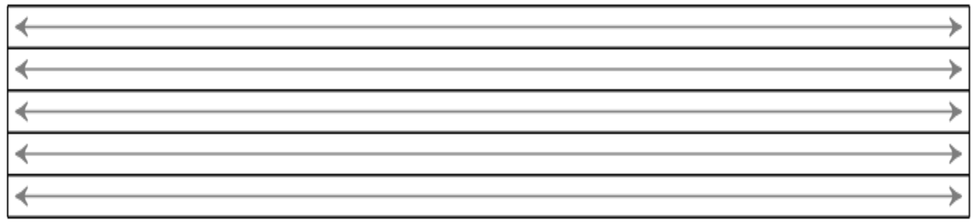
3 operations in a round



(1) Constant addition

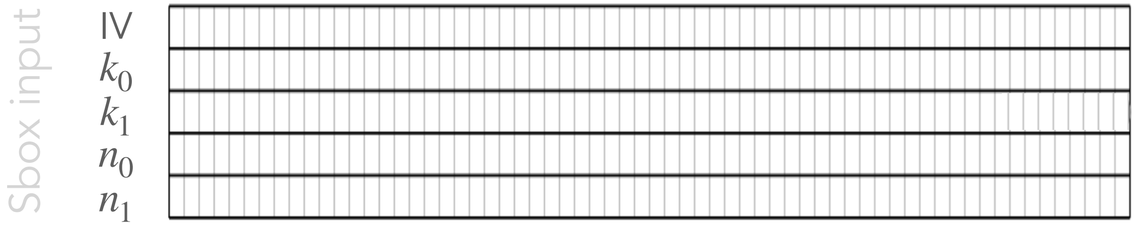


(2) Substitution *(vertical)*

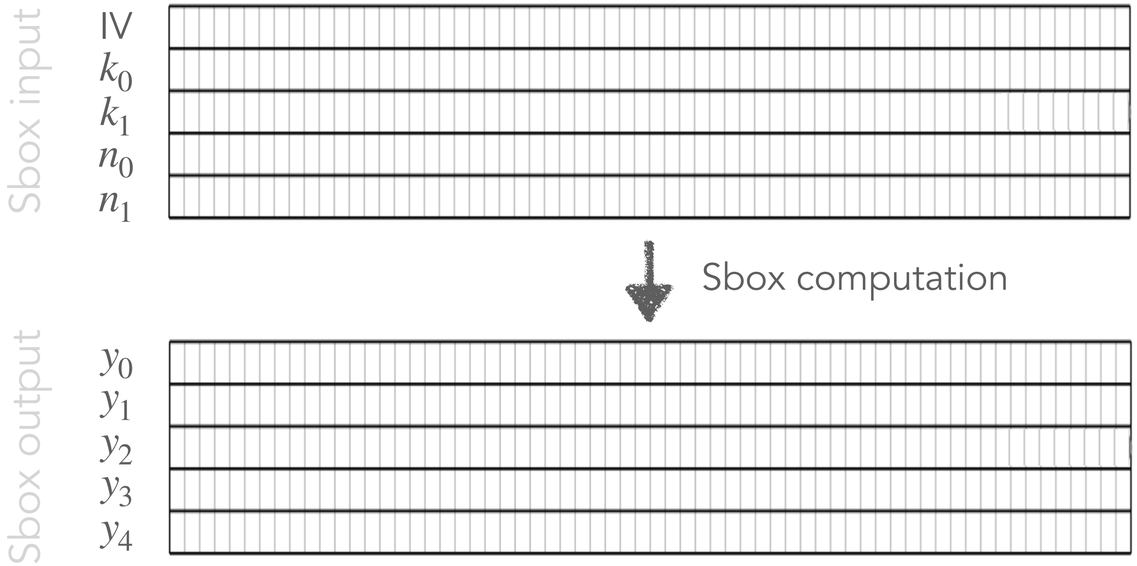


(3) Linear diffusion *(horizontal)*

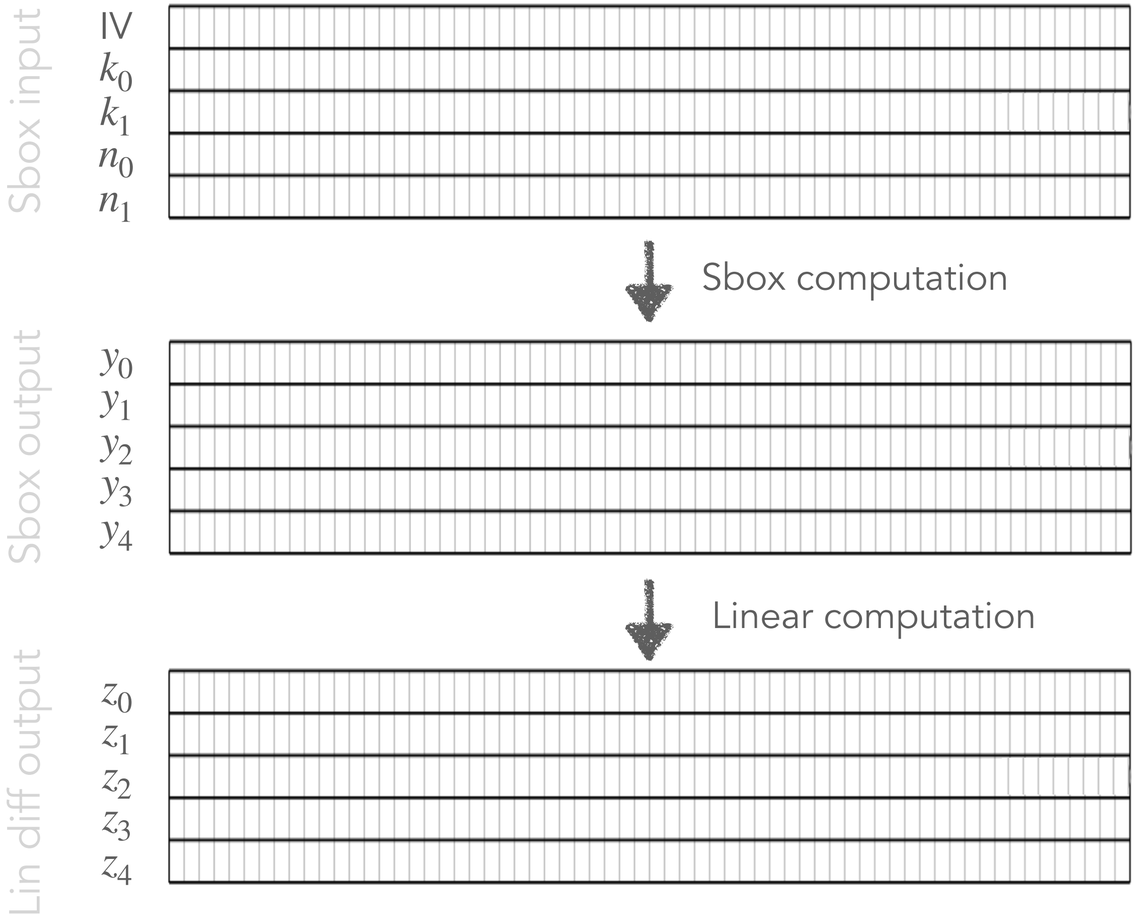
State changes in 1st round



State changes in 1st round

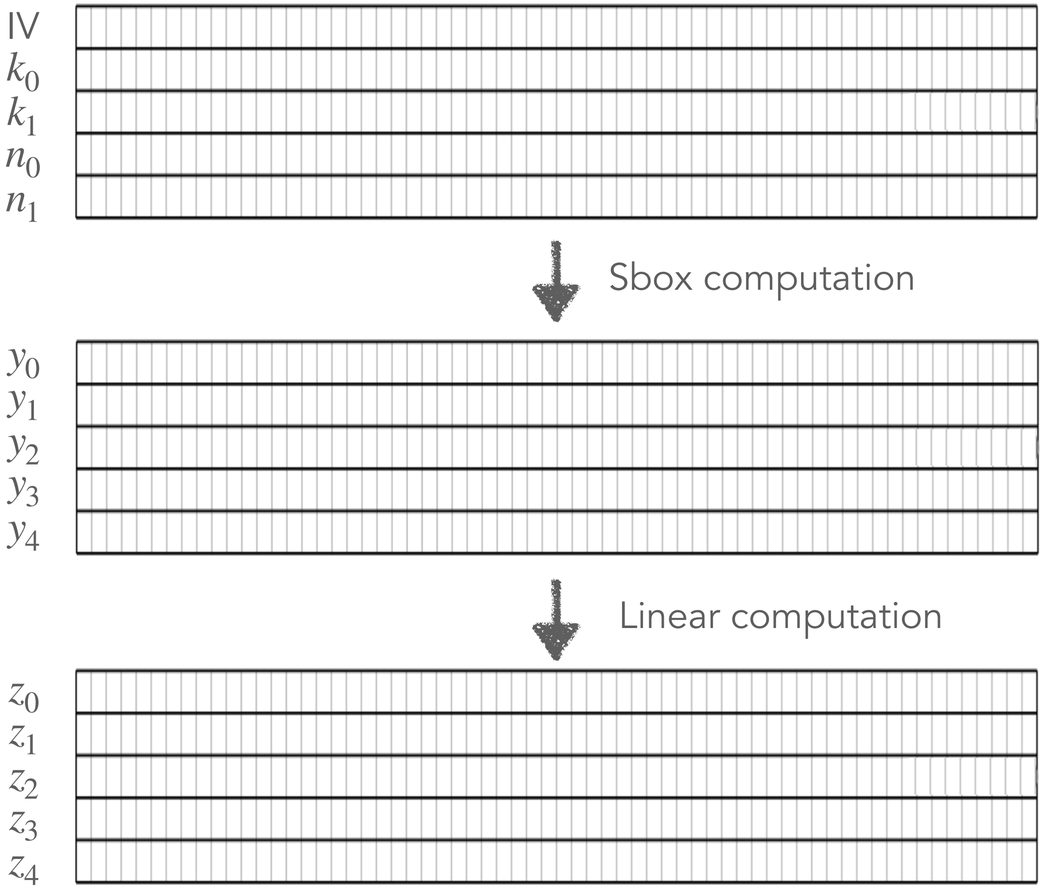


State changes in 1st round



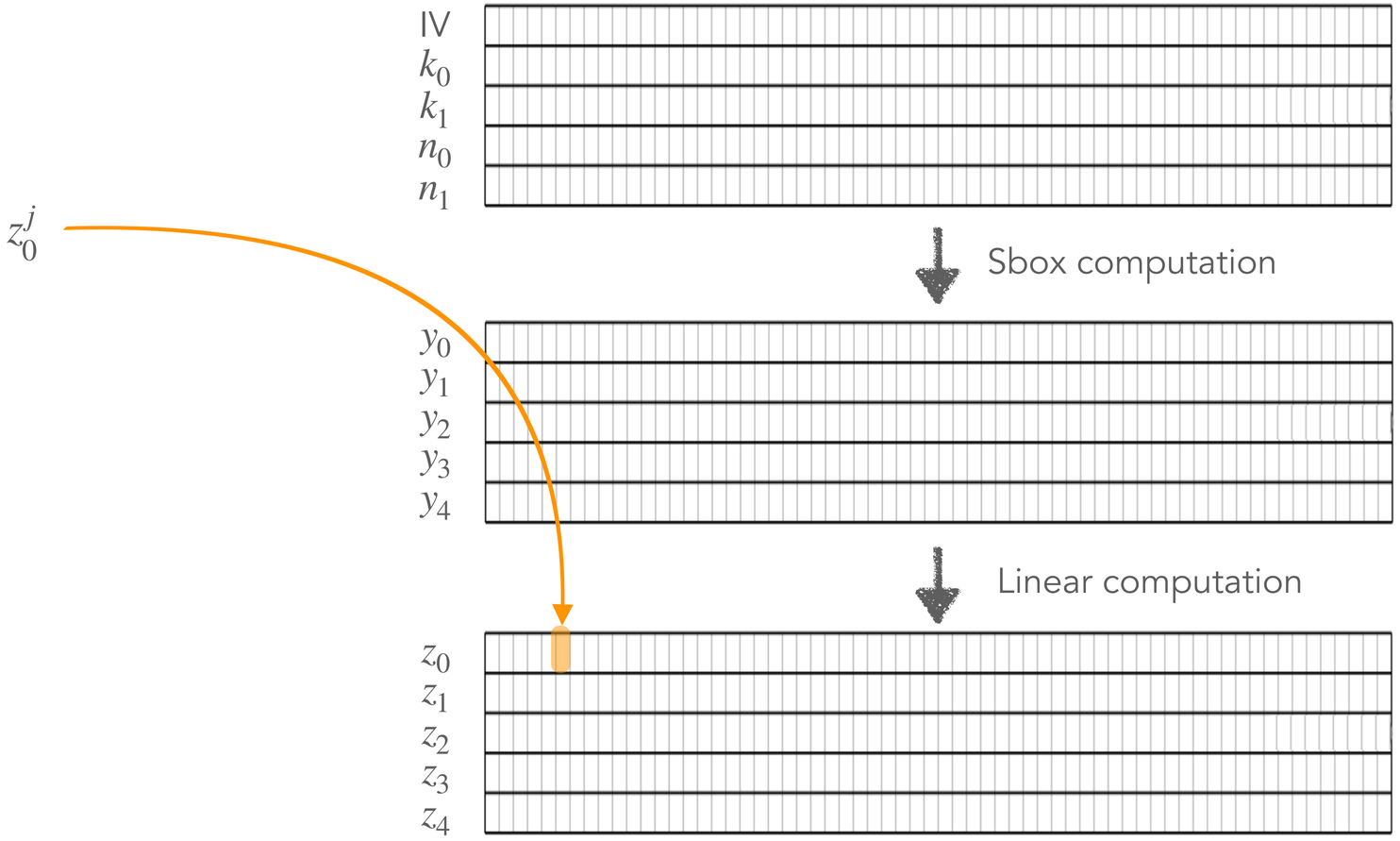
Intermediate value

Samwel and Daemen, 2018



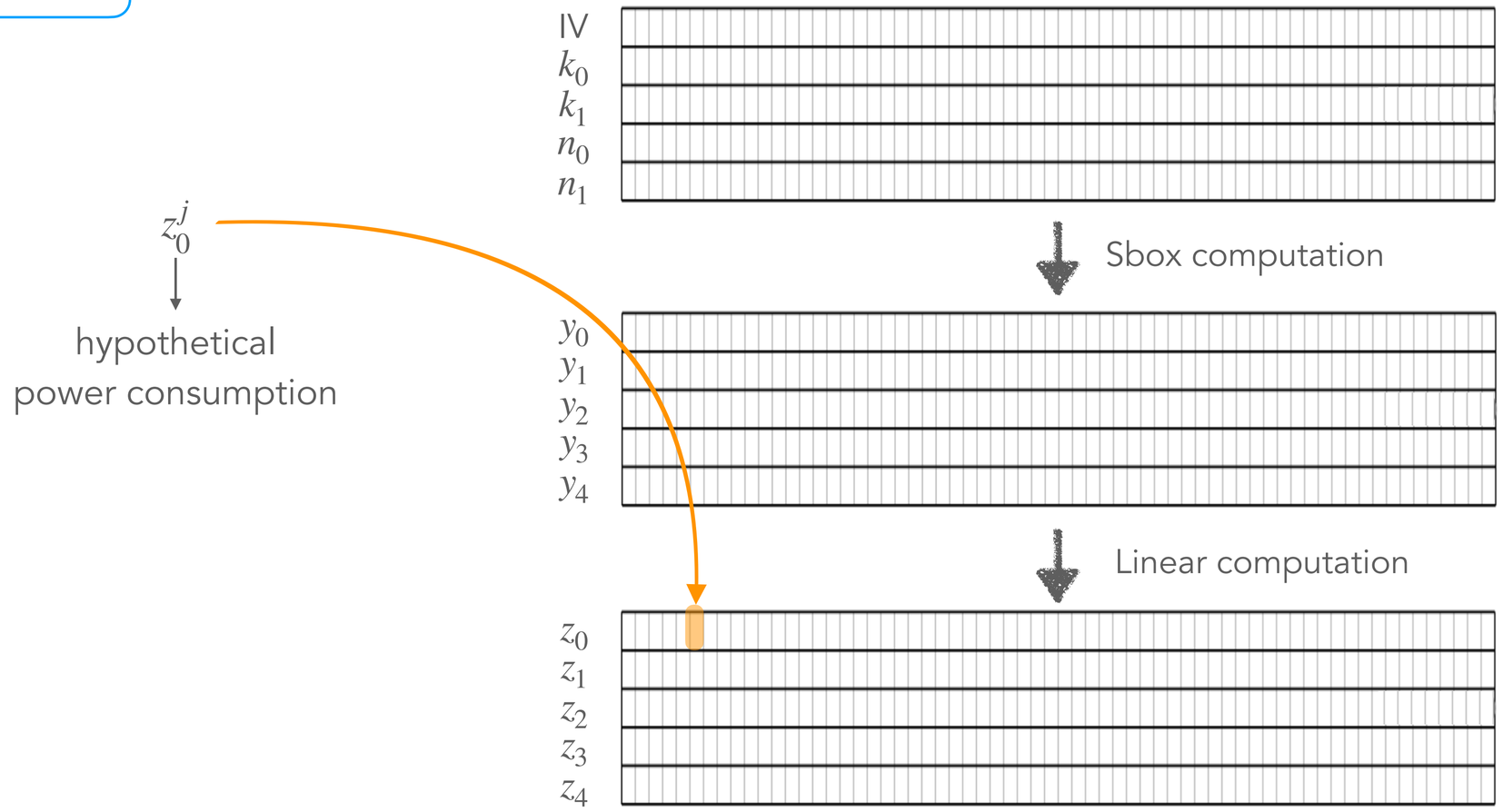
Intermediate value

Samwel and Daemen, 2018



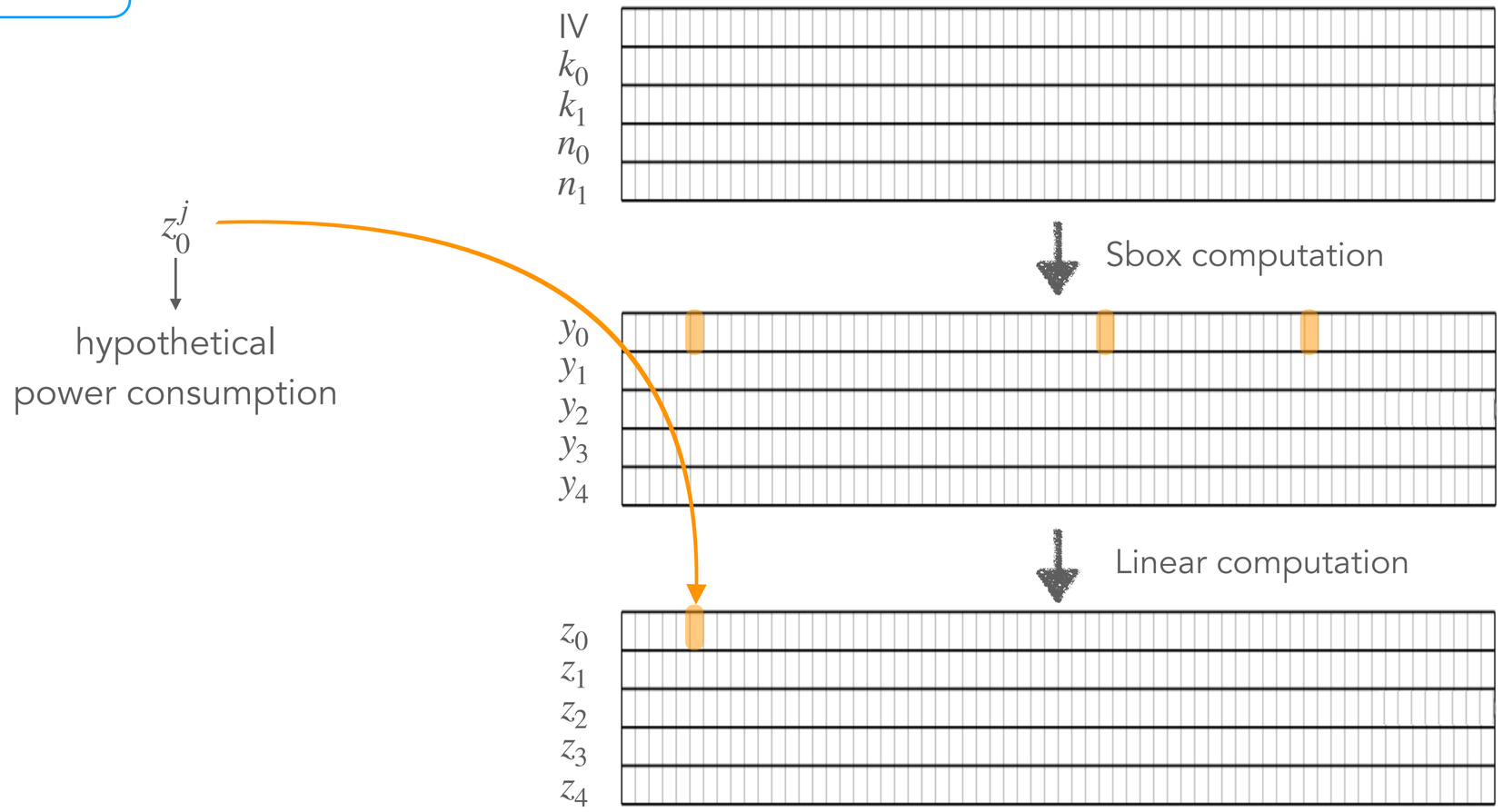
Intermediate value

Samwel and Daemen, 2018



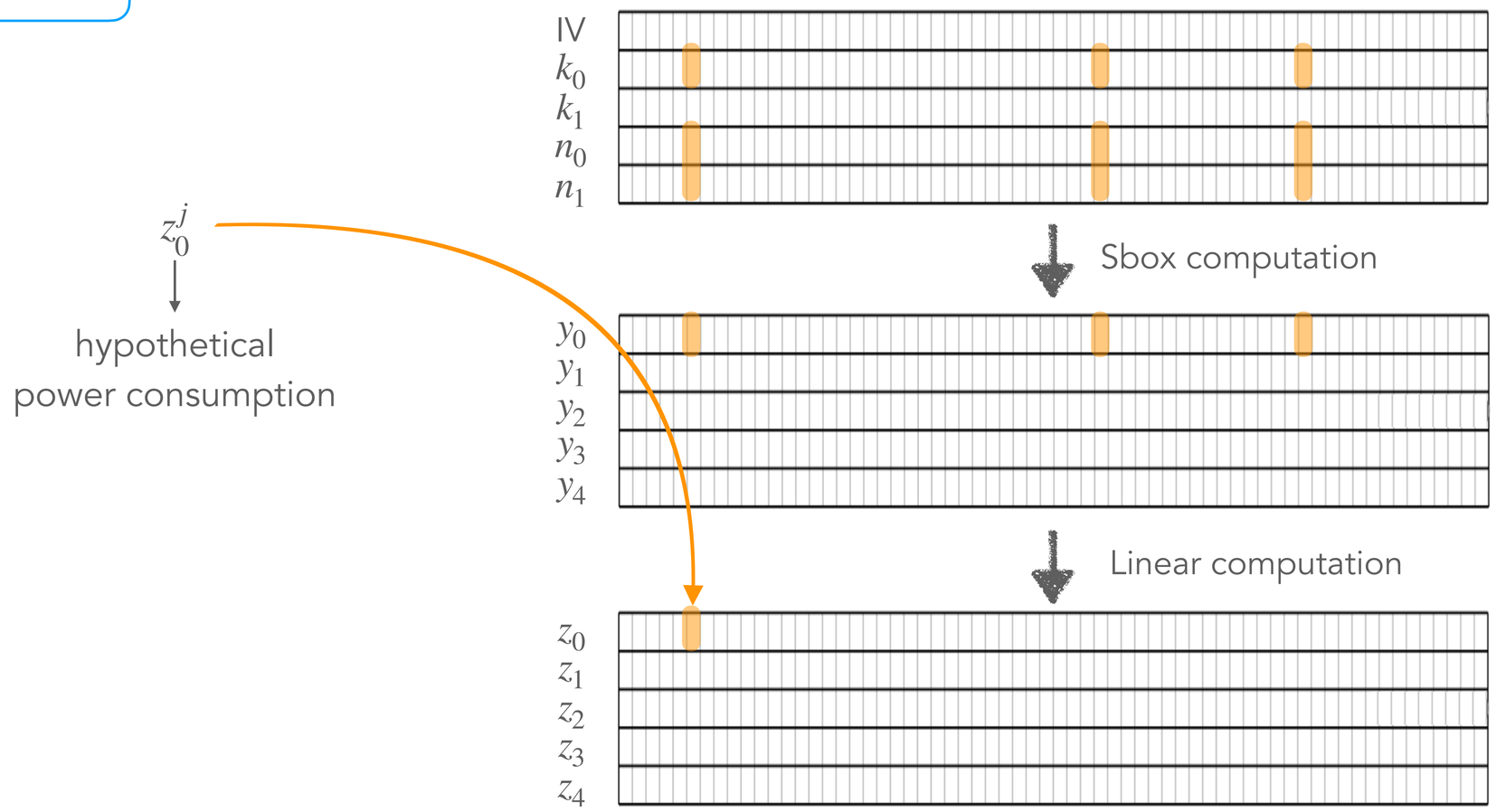
Intermediate value

Samwel and Daemen, 2018



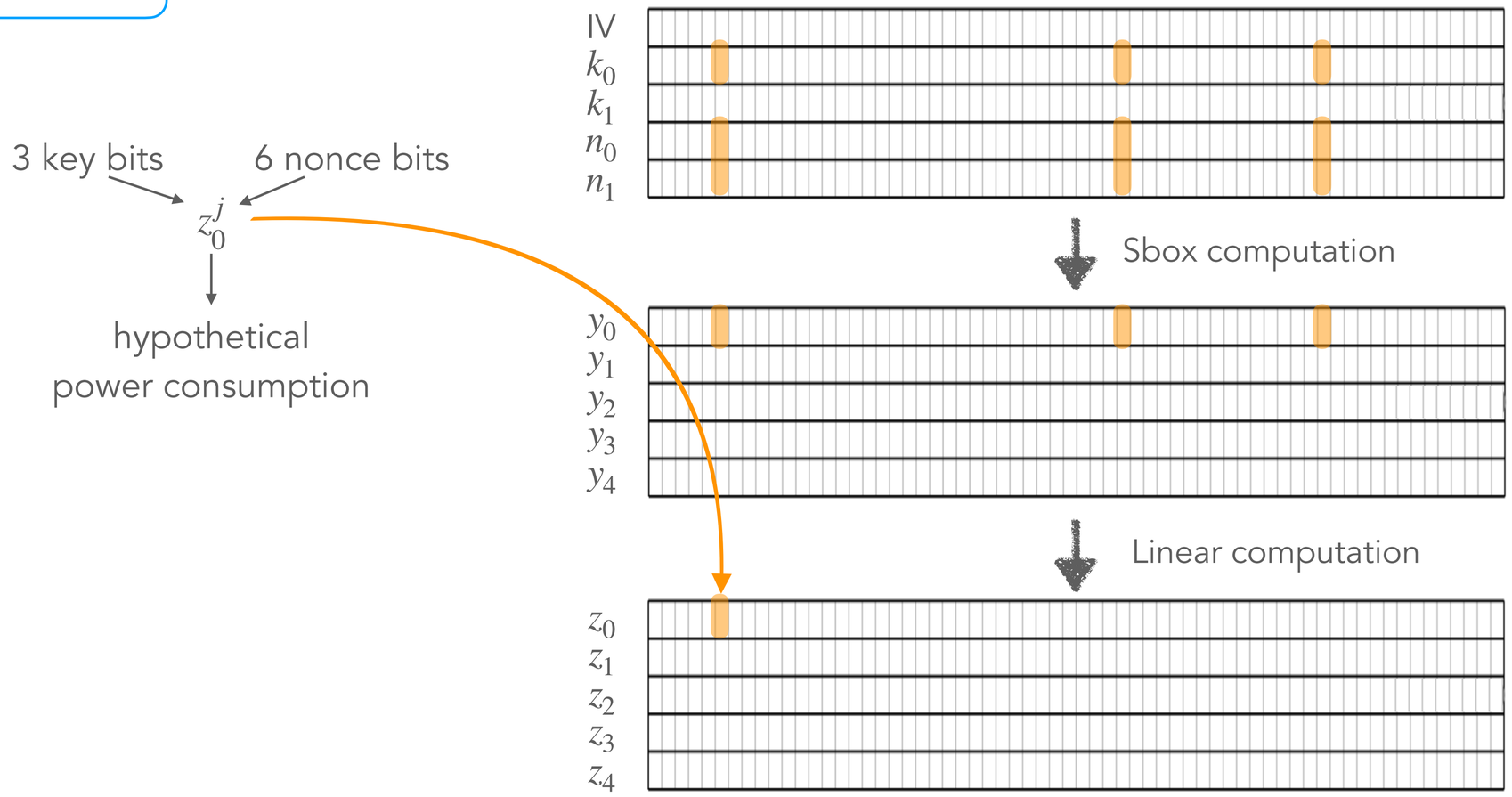
Intermediate value

Samwel and Daemen, 2018



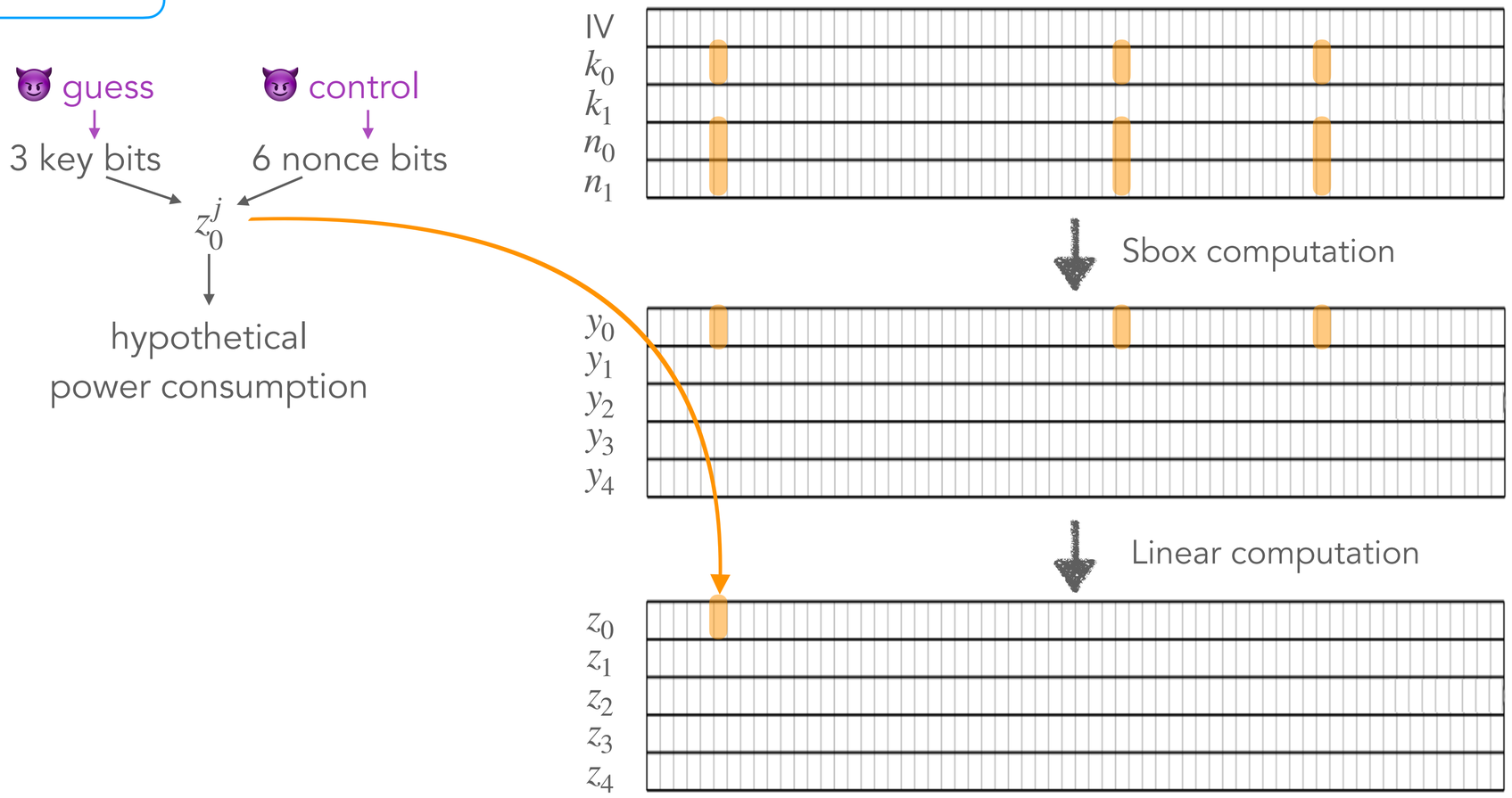
Intermediate value

Samwel and Daemen, 2018



Intermediate value

Samwel and Daemen, 2018



Intermediate value

Samwel and Daemen, 2018

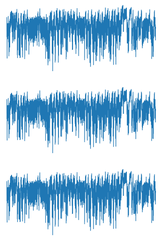
😈 guess → 3 key bits

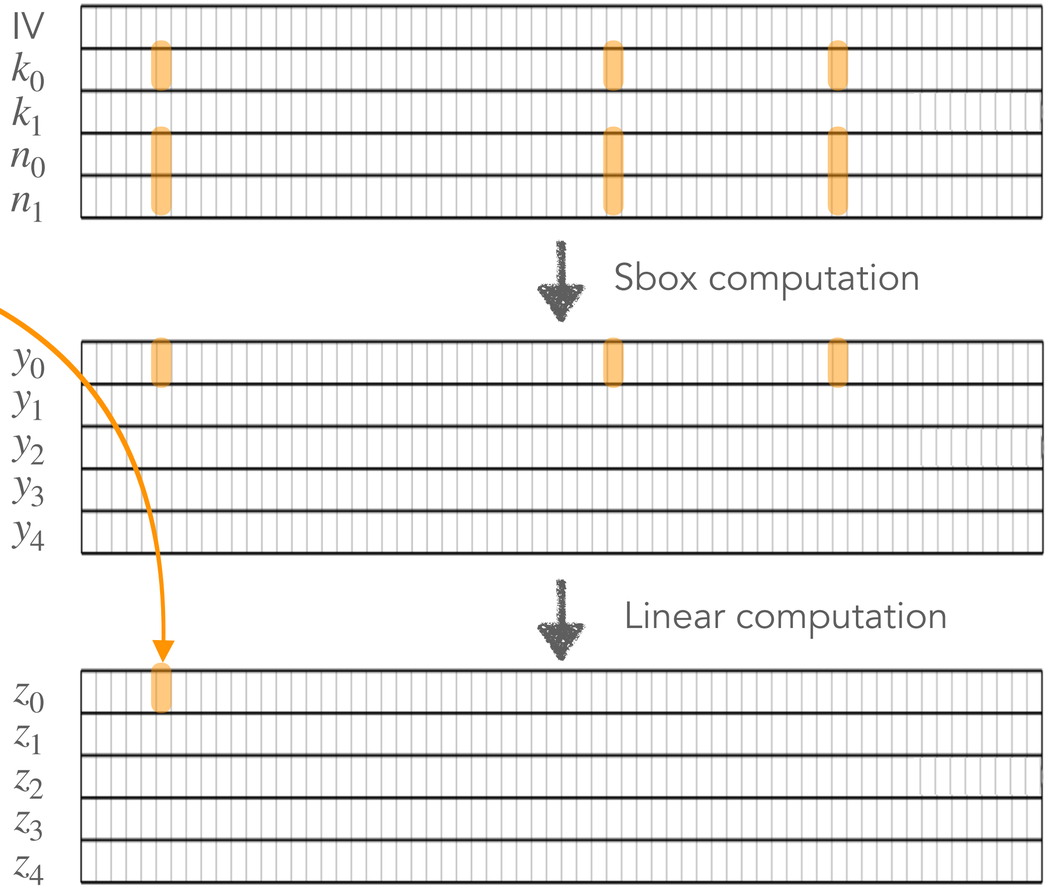
😈 control → 6 nonce bits

z_0^j

😈 mesured power consumption

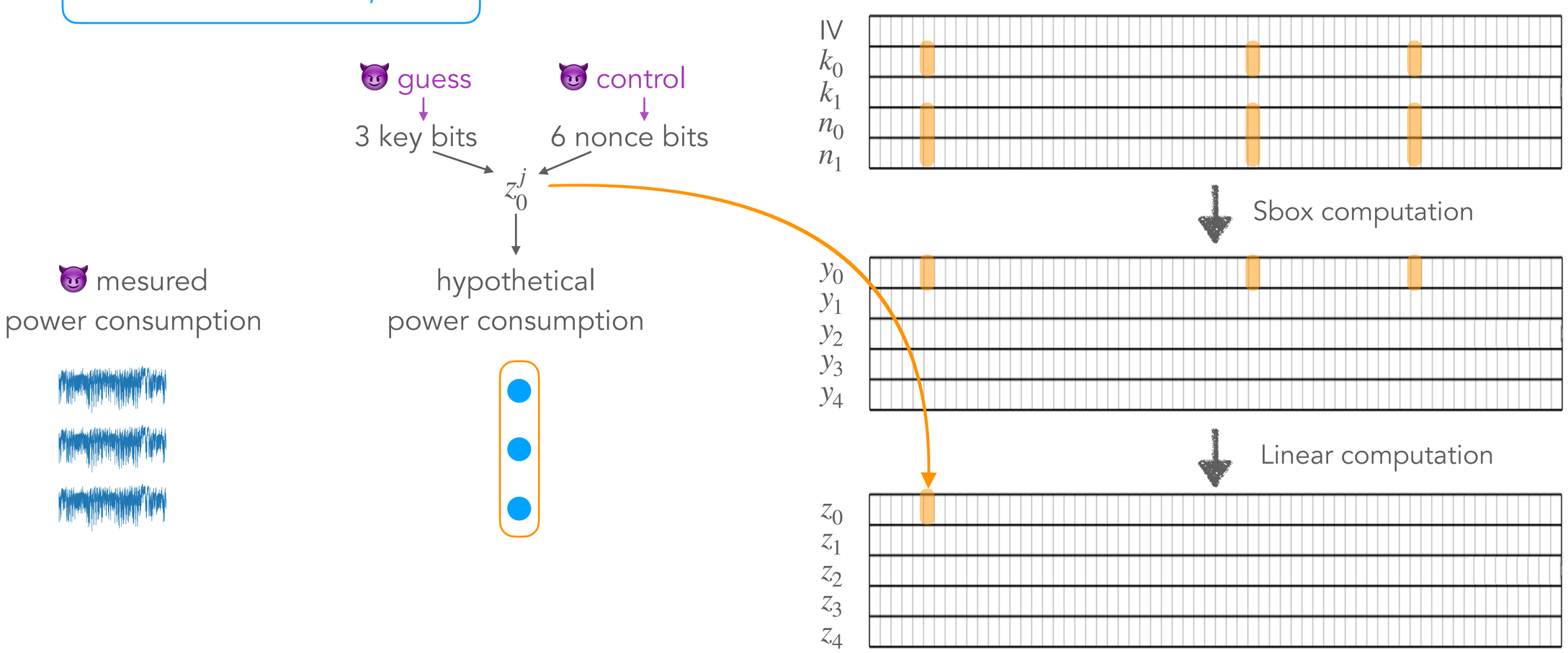
hypothetical power consumption





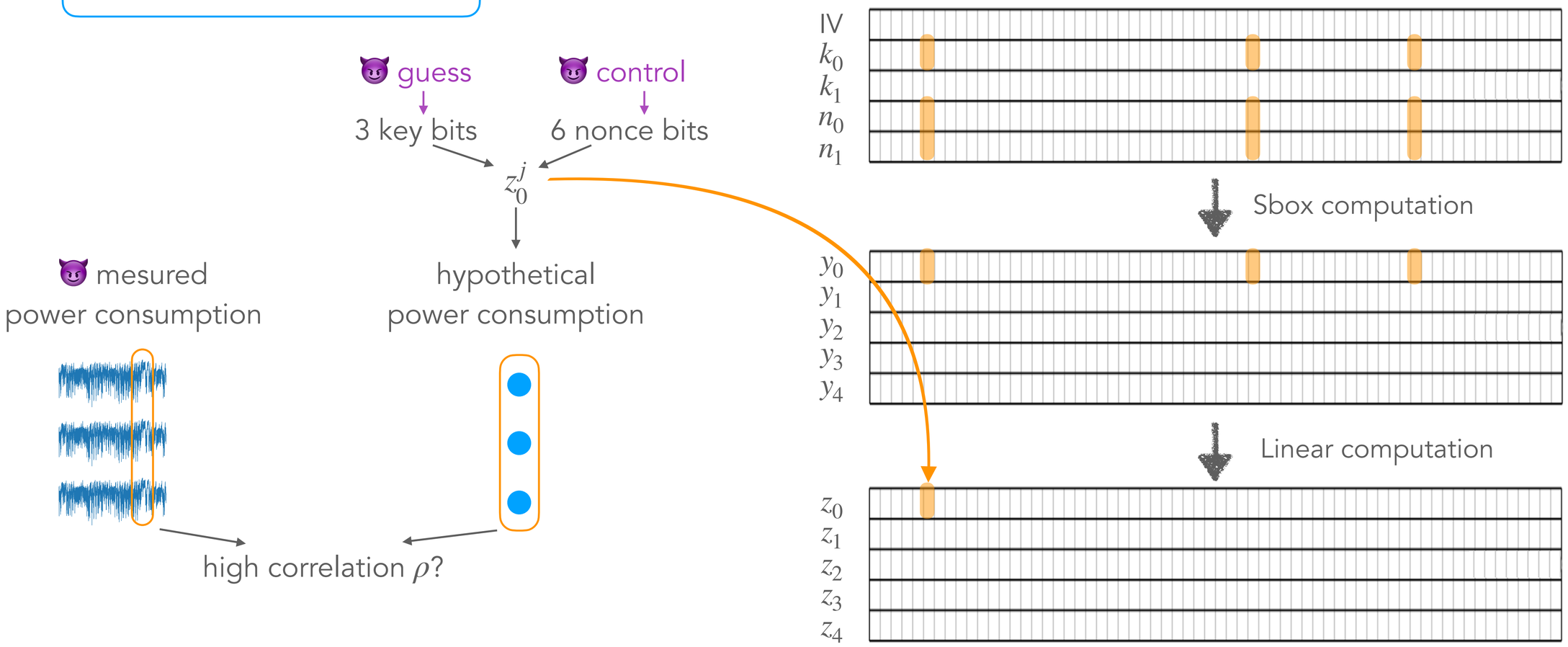
Intermediate value

Samwel and Daemen, 2018



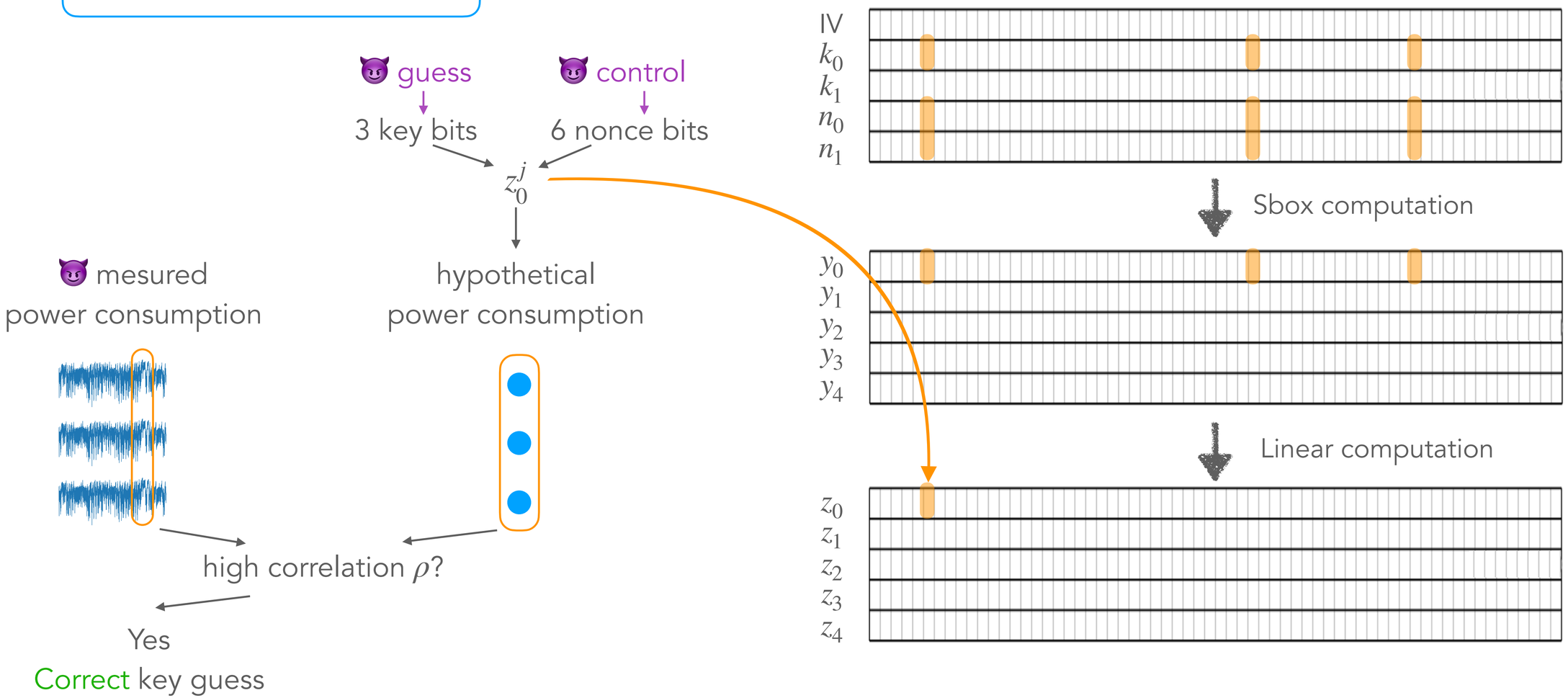
Intermediate value

Samwel and Daemen, 2018



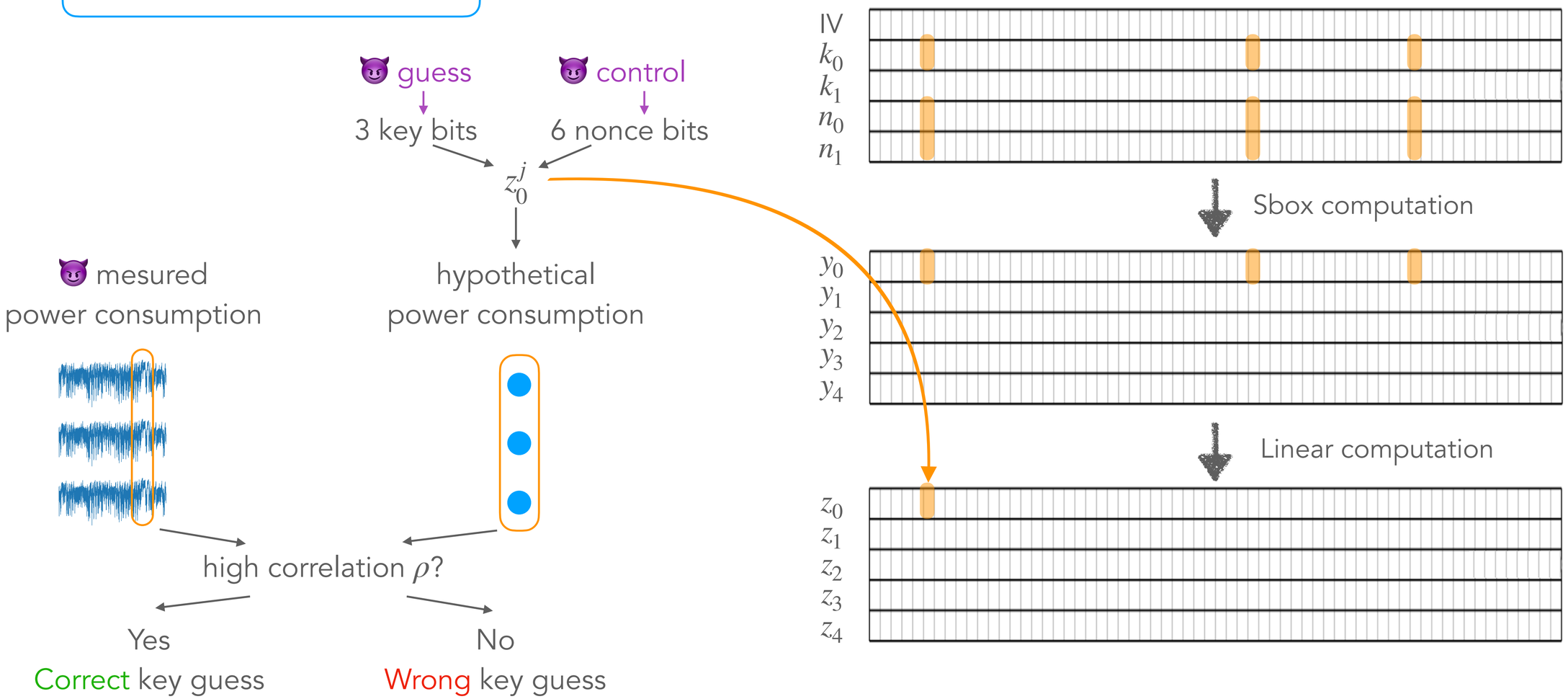
Intermediate value

Samwel and Daemen, 2018



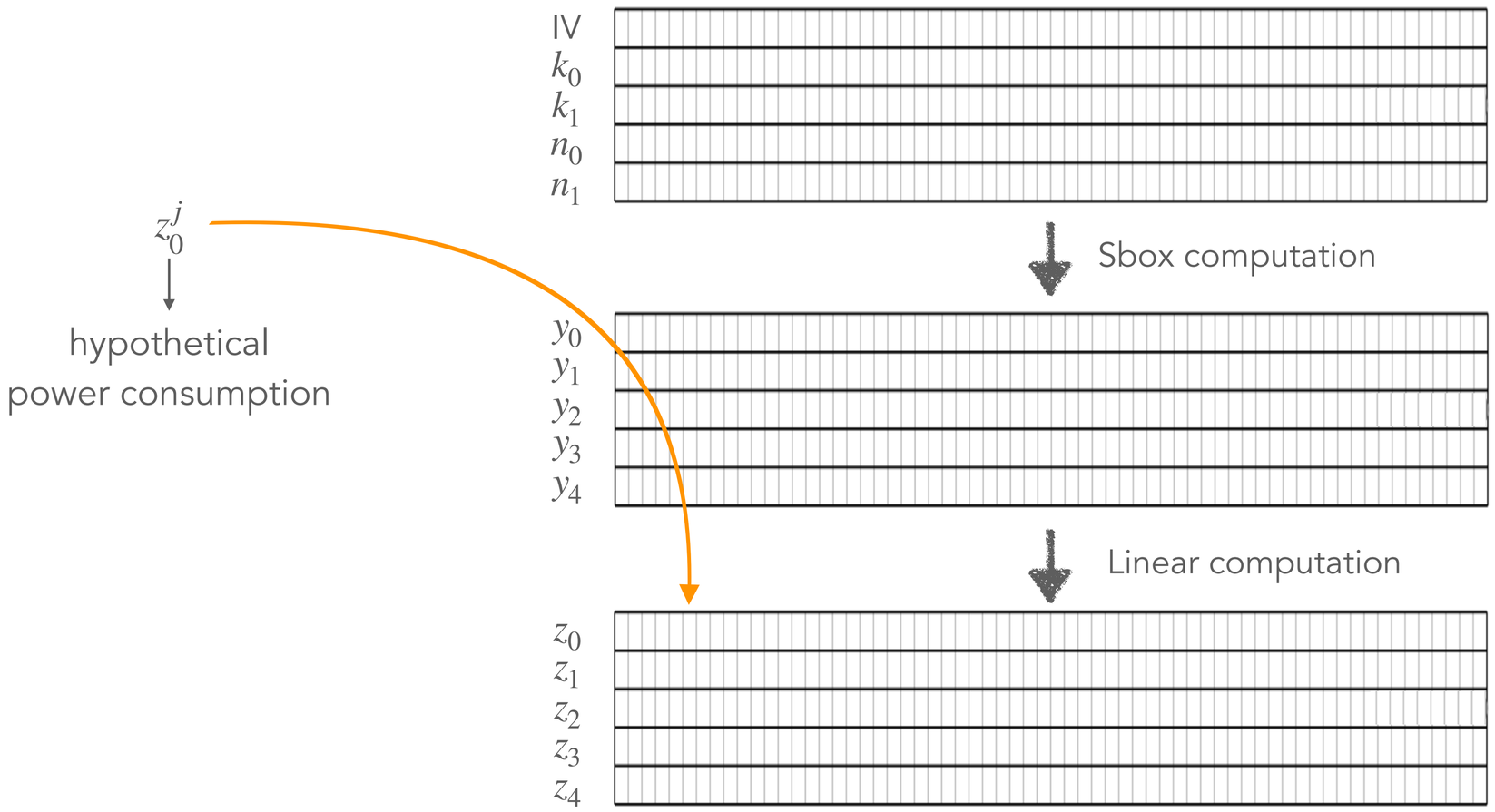
Intermediate value

Samwel and Daemen, 2018

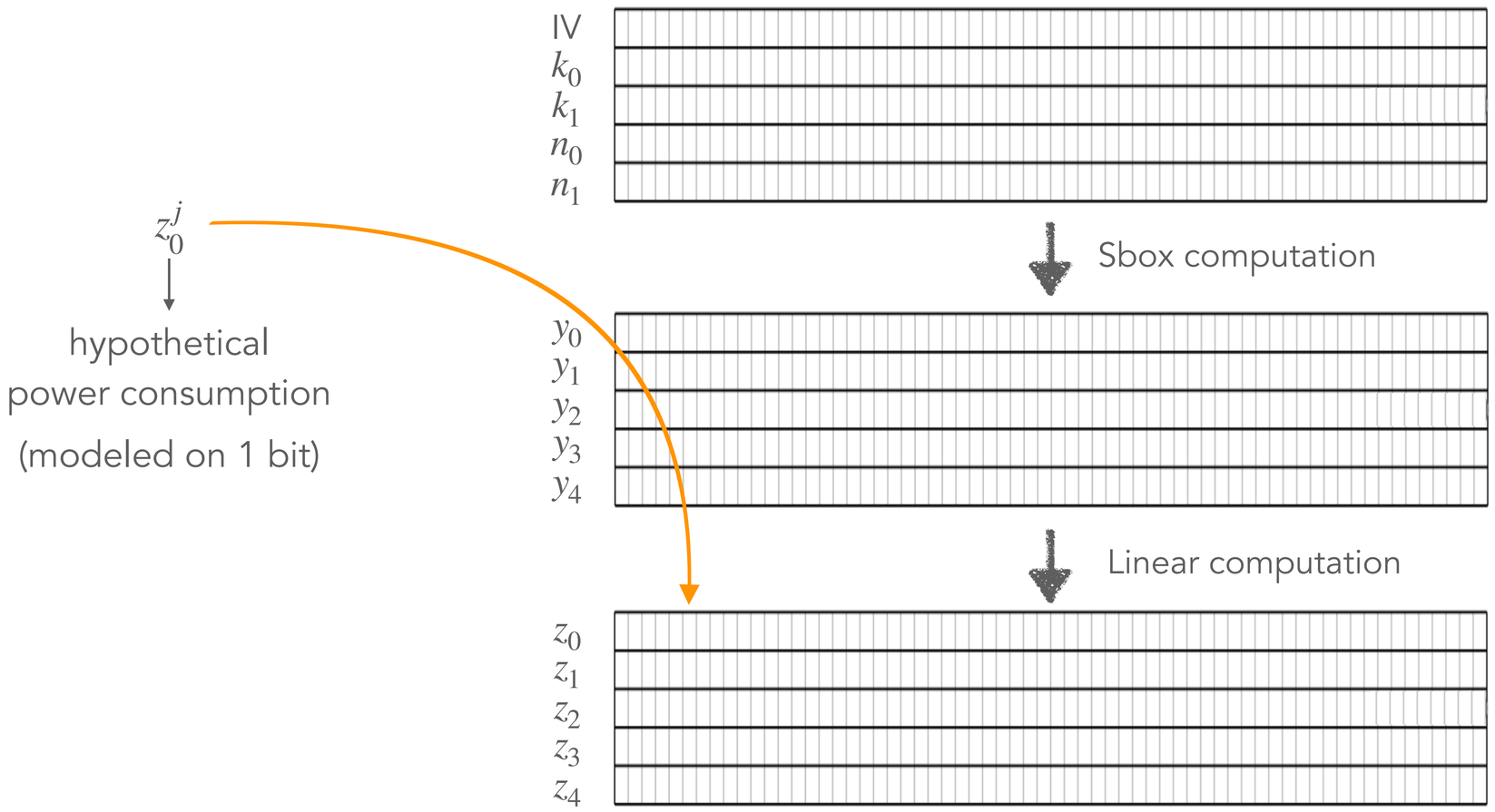


Main idea

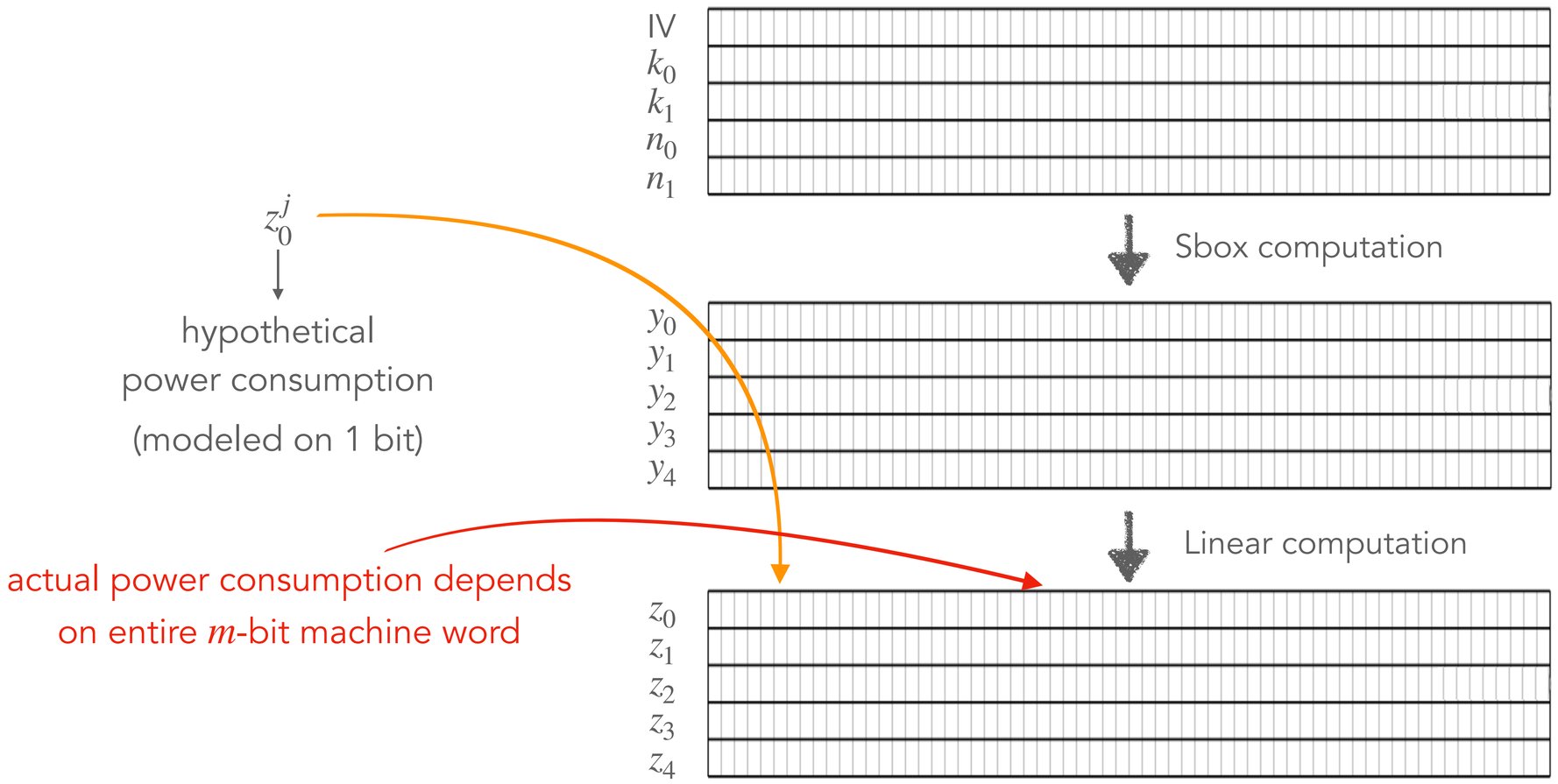
Observation



Observation



Observation

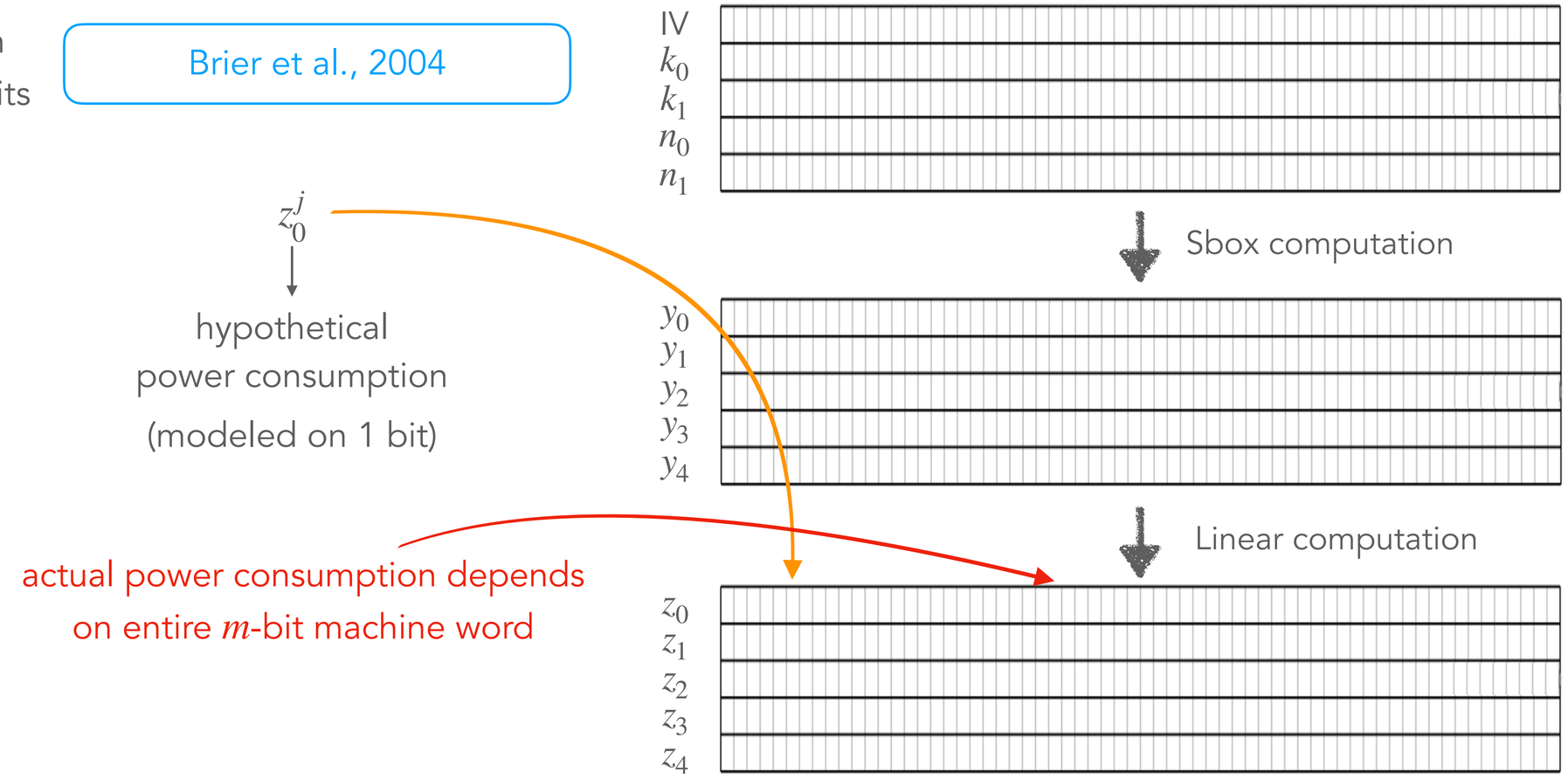


Observation

partial correlation when considering d out of m bits

$$\rho_d = \rho_m \sqrt{\frac{d}{m}}$$

Brier et al., 2004



Observation

partial correlation when considering d out of m bits

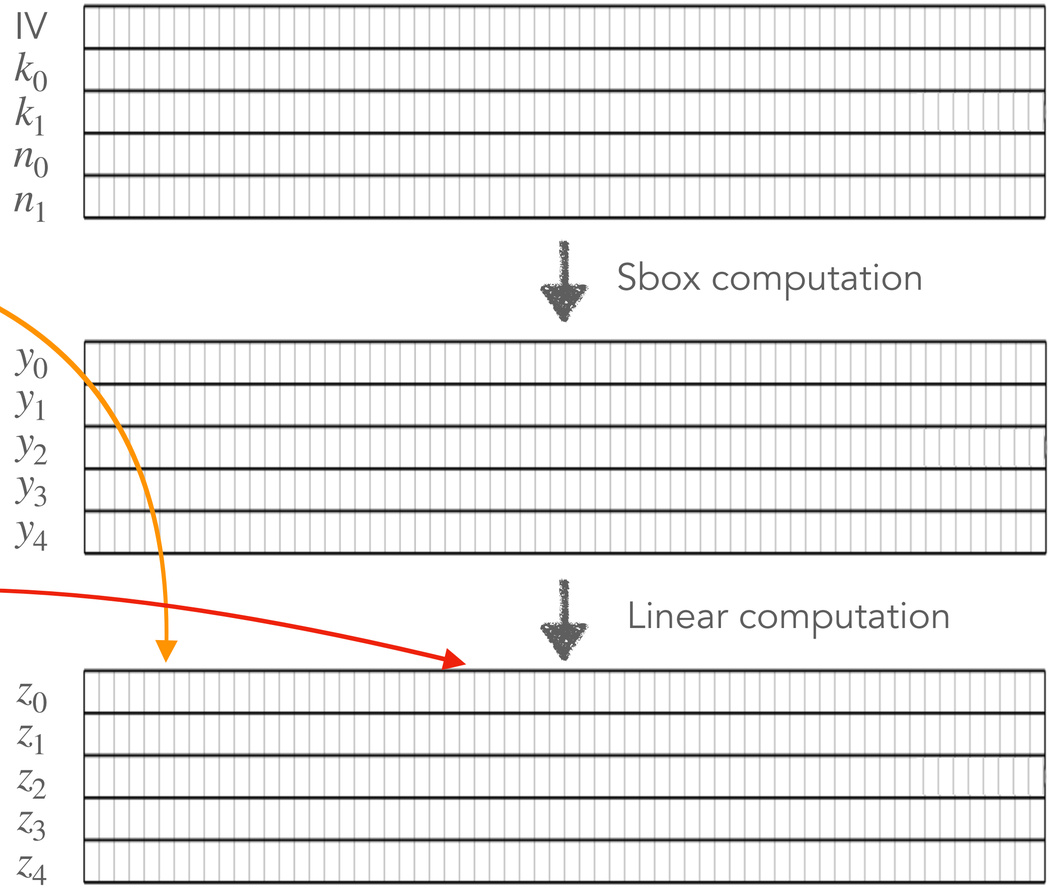
$$\rho_d = \rho_m \sqrt{\frac{d}{m}}$$

Brier et al., 2004

z_0^j

hypothetical power consumption (modeled on 1 bit)

$d = 1$



actual power consumption depends on entire m-bit machine word

Observation

partial correlation when considering d out of m bits

$$\rho_d = \rho_m \sqrt{\frac{d}{m}}$$

Brier et al., 2004

z_0^j

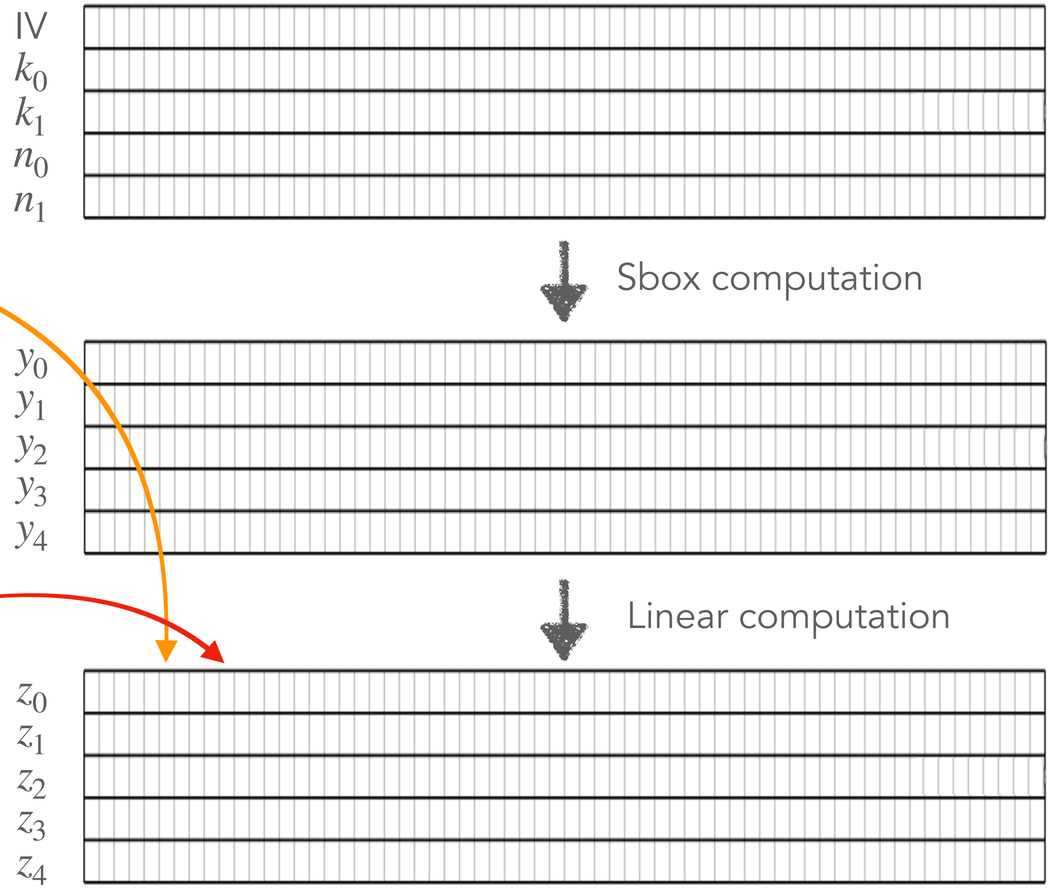
hypothetical power consumption (modeled on 1 bit)

$d = 1$

$d > 1$

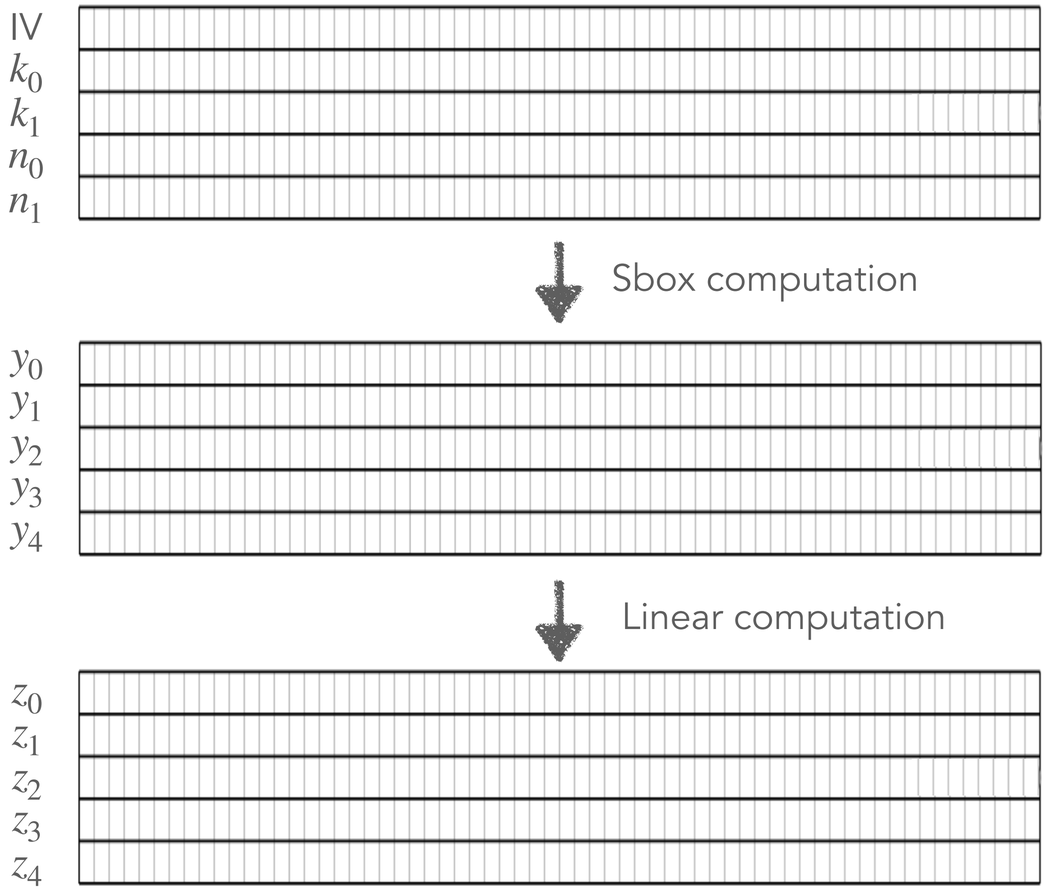
consider d bits ?

🤔 🤔



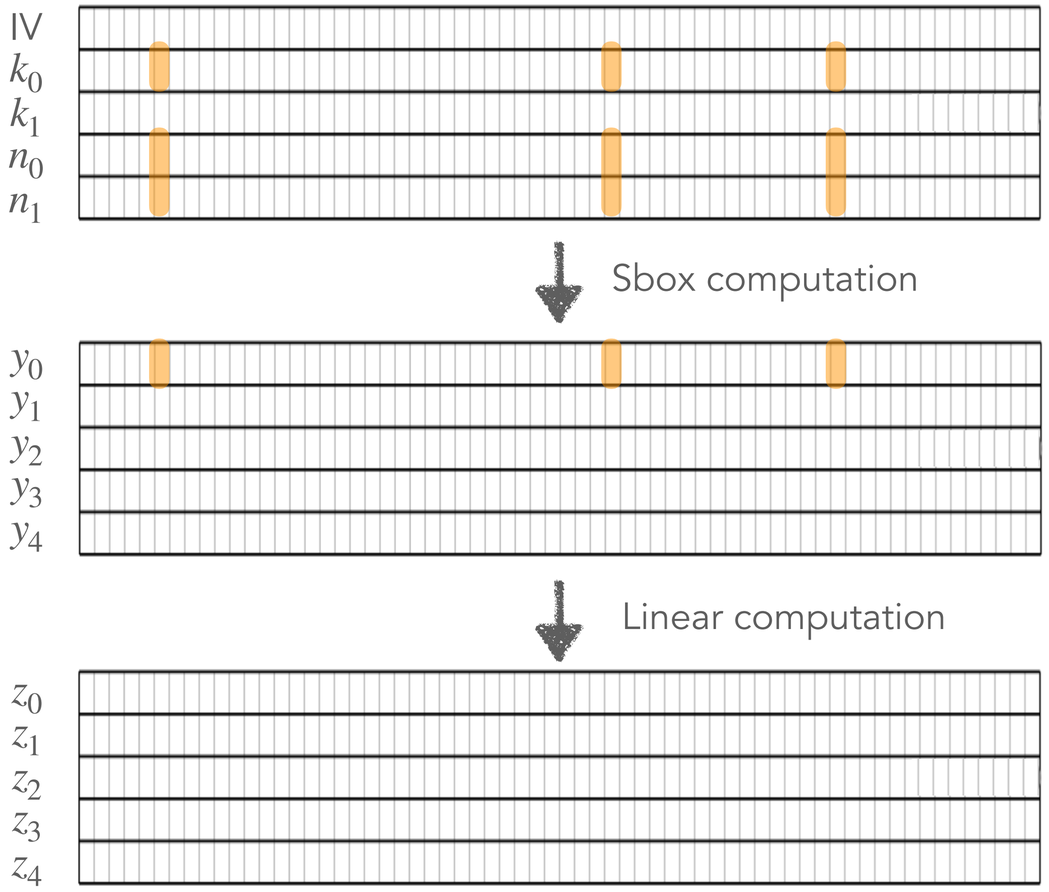
Advantage in number of CPA runs

hypothetical power consumption modeled on d bits		
$d = 1$		



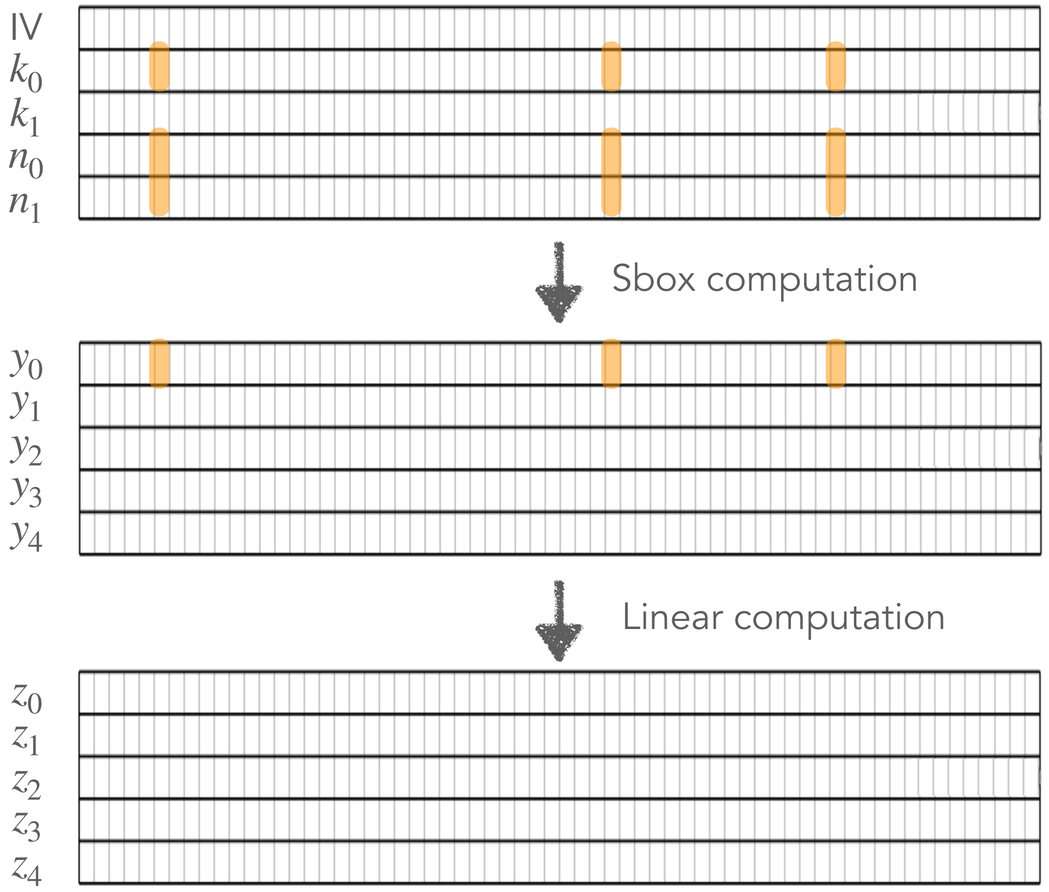
Advantage in number of CPA runs

hypothetical power consumption modeled on d bits		
$d = 1$		



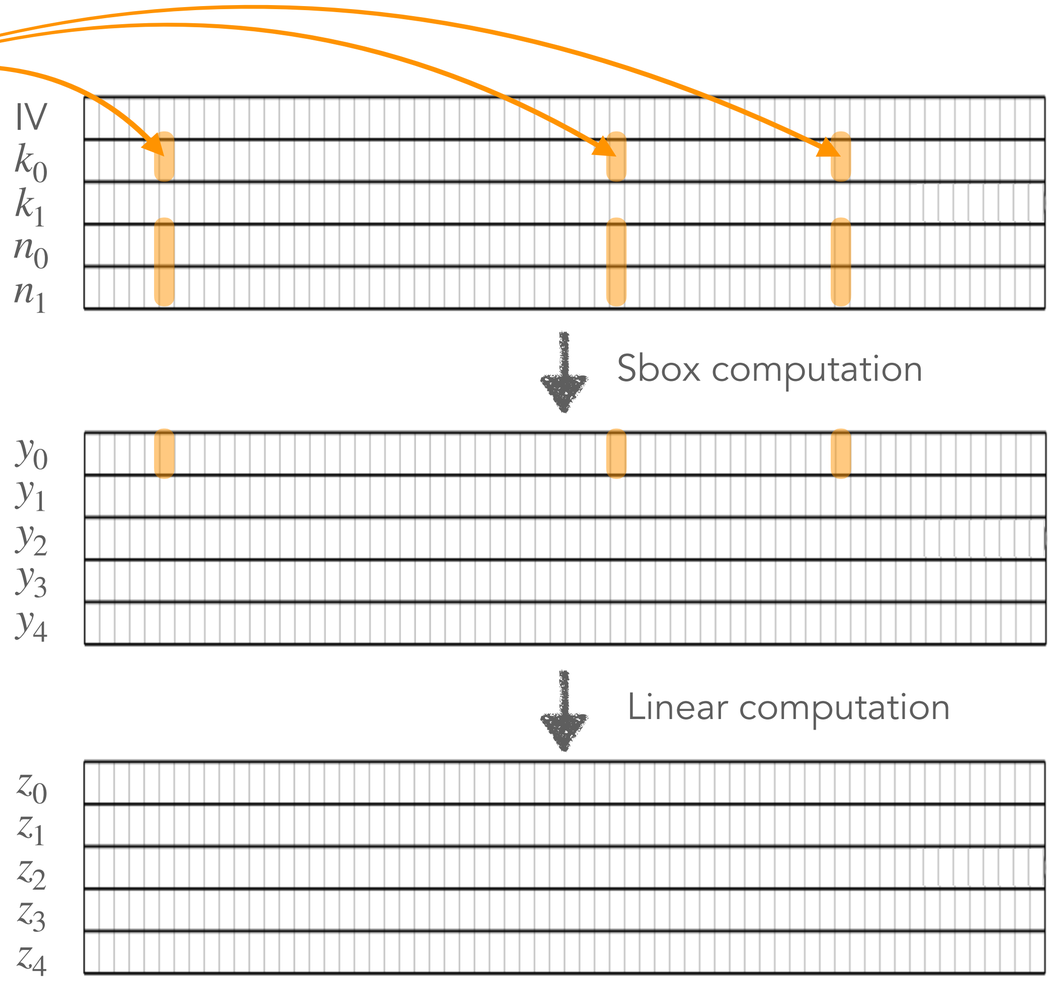
Advantage in number of CPA runs

hypothetical power consumption modeled on d bits	# recovered key bits in 1 CPA run	
$d = 1$	3	



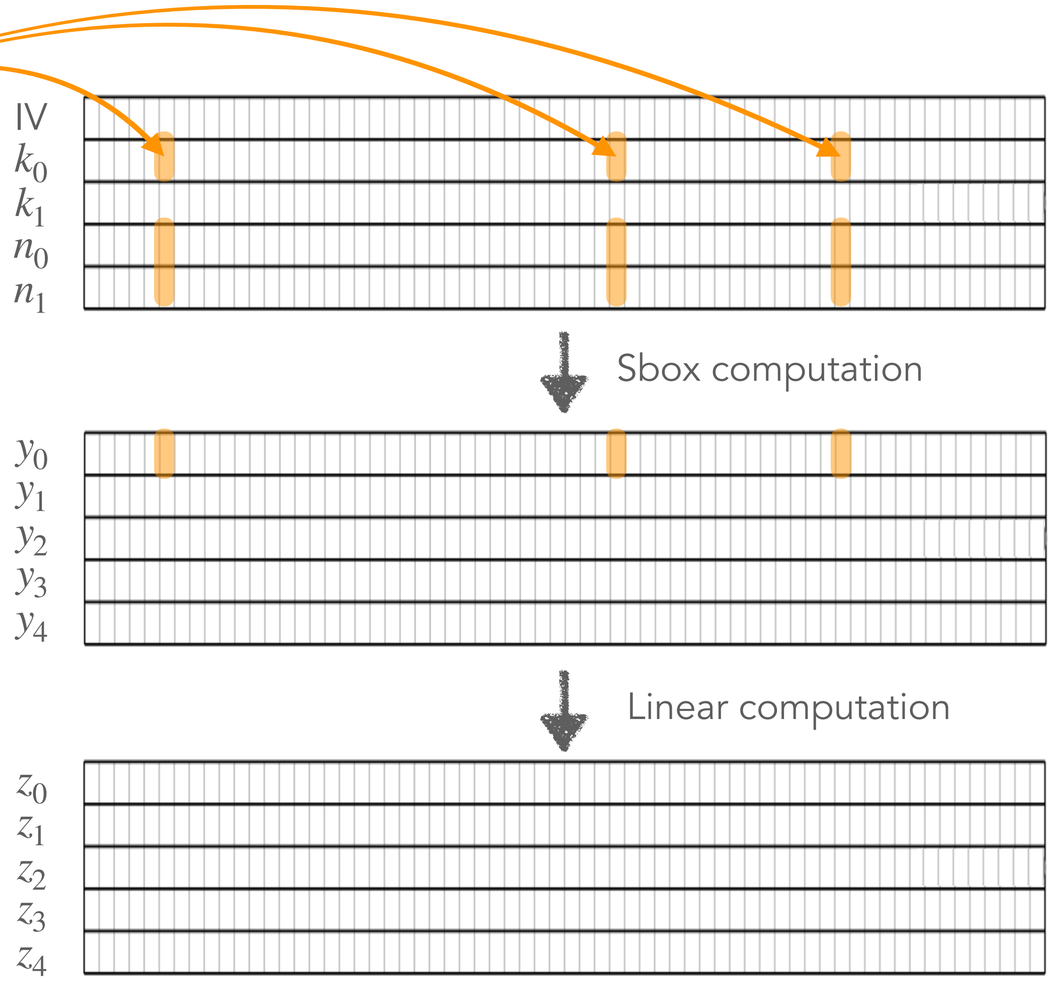
Advantage in number of CPA runs

hypothetical power consumption modeled on d bits	# recovered key bits in 1 CPA run	
$d = 1$	3	



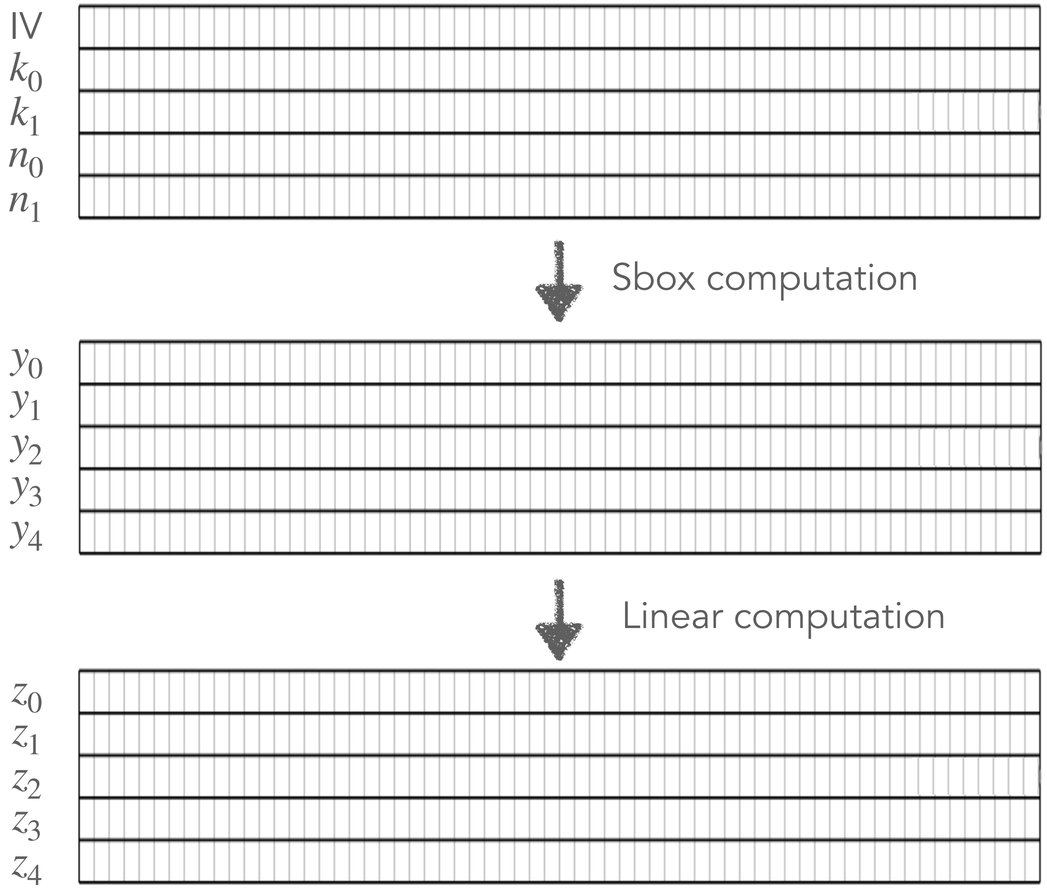
Advantage in number of CPA runs

hypothetical power consumption modeled on d bits	# recovered key bits in 1 CPA run	# CPA runs to recover 128-bit key
$d = 1$	3	48



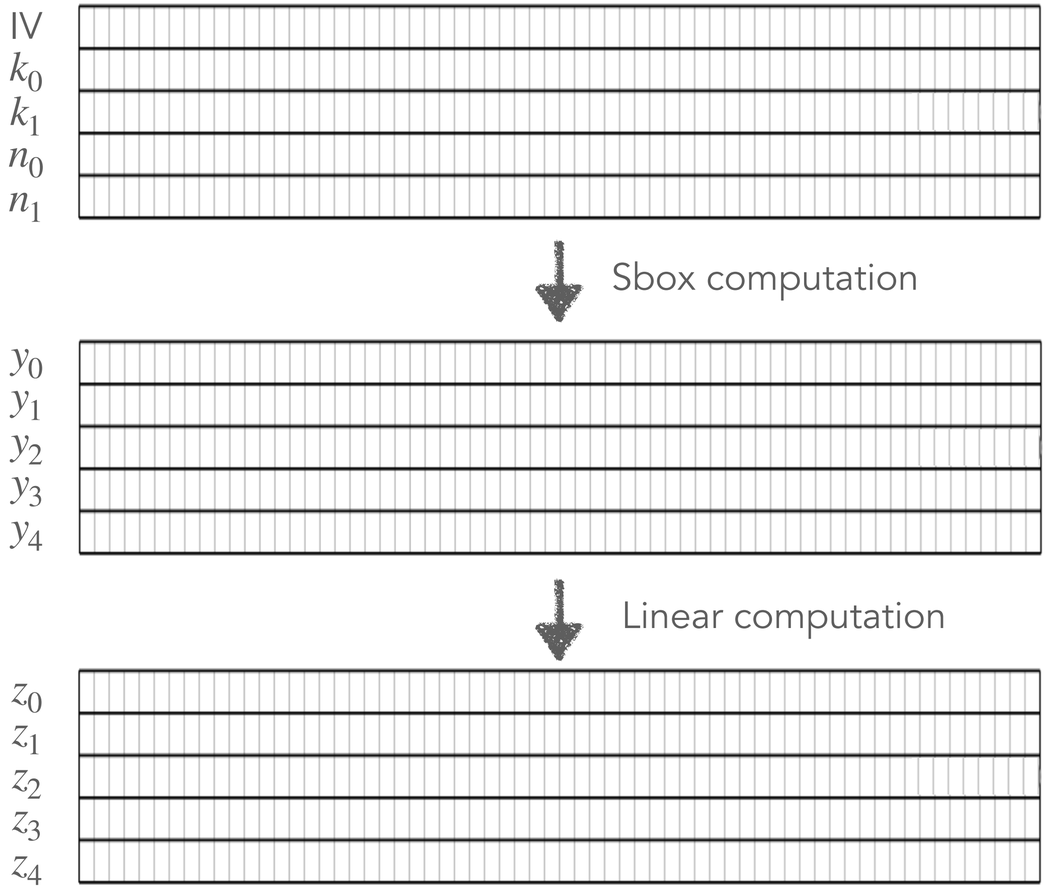
Advantage in number of CPA runs

hypothetical power consumption modeled on d bits	# recovered key bits in 1 CPA run	# CPA runs to recover 128-bit key
$d = 1$	3	48



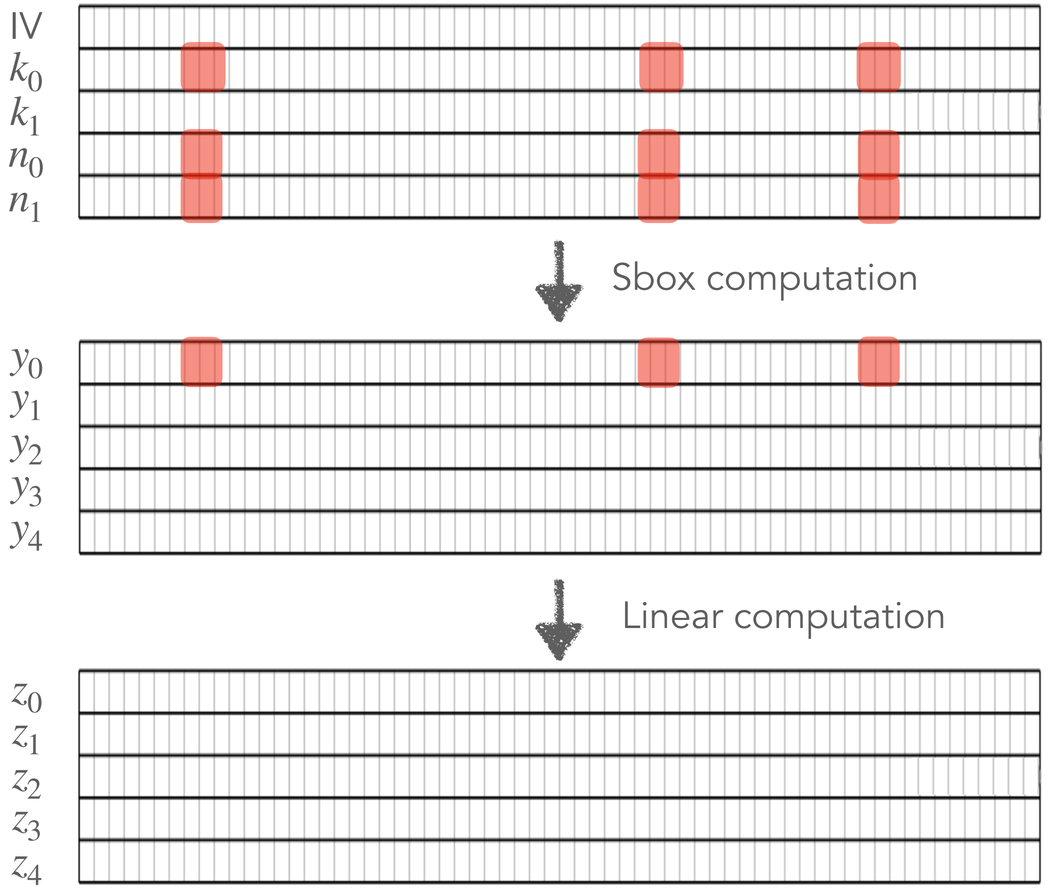
Advantage in number of CPA runs

hypothetical power consumption modeled on d bits	# recovered key bits in 1 CPA run	# CPA runs to recover 128-bit key
$d = 1$	3	48
$d = 2$		



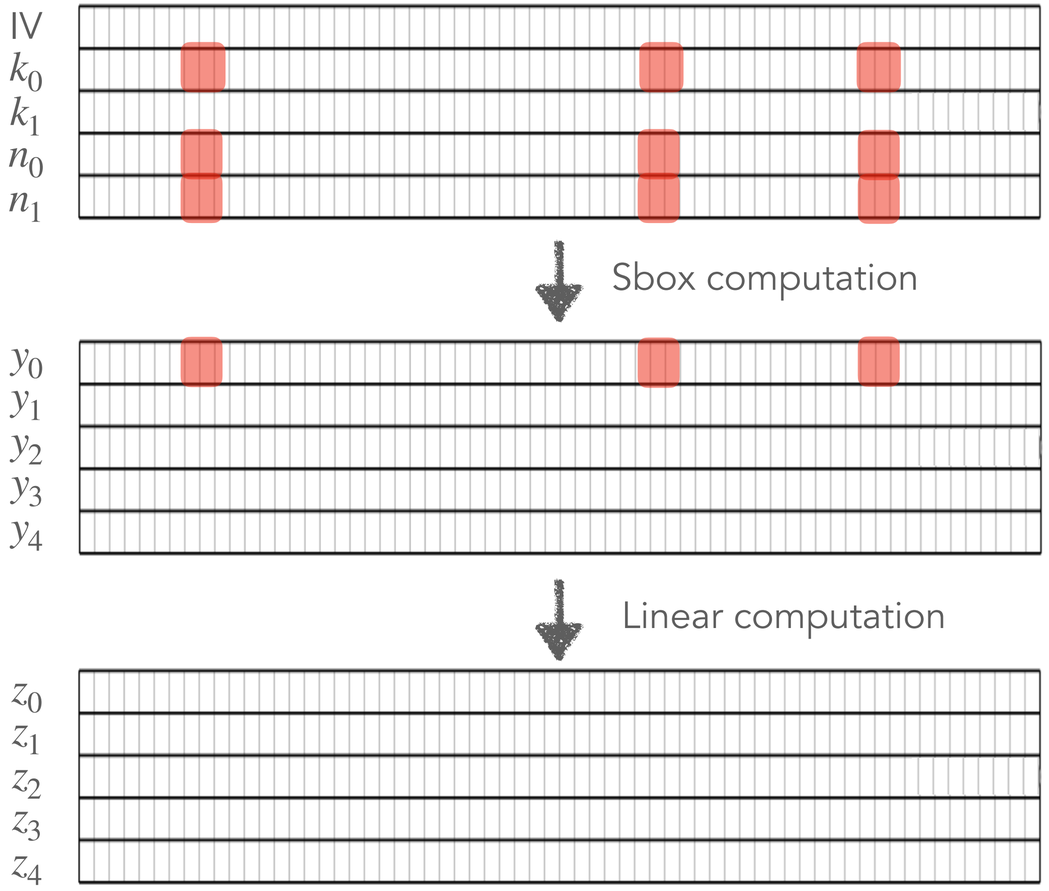
Advantage in number of CPA runs

hypothetical power consumption modeled on d bits	# recovered key bits in 1 CPA run	# CPA runs to recover 128-bit key
$d = 1$	3	48
$d = 2$		



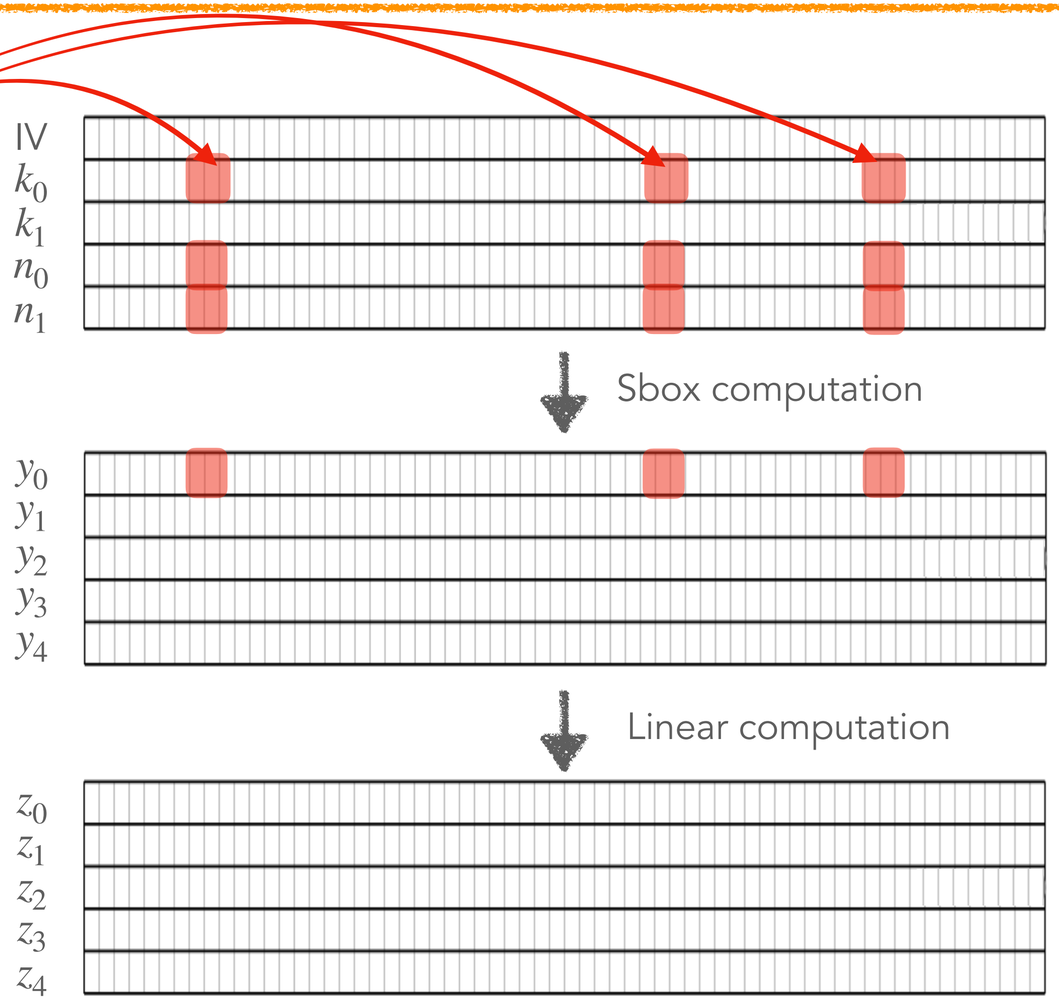
Advantage in number of CPA runs

hypothetical power consumption modeled on d bits	# recovered key bits in 1 CPA run	# CPA runs to recover 128-bit key
$d = 1$	3	48
$d = 2$	6	



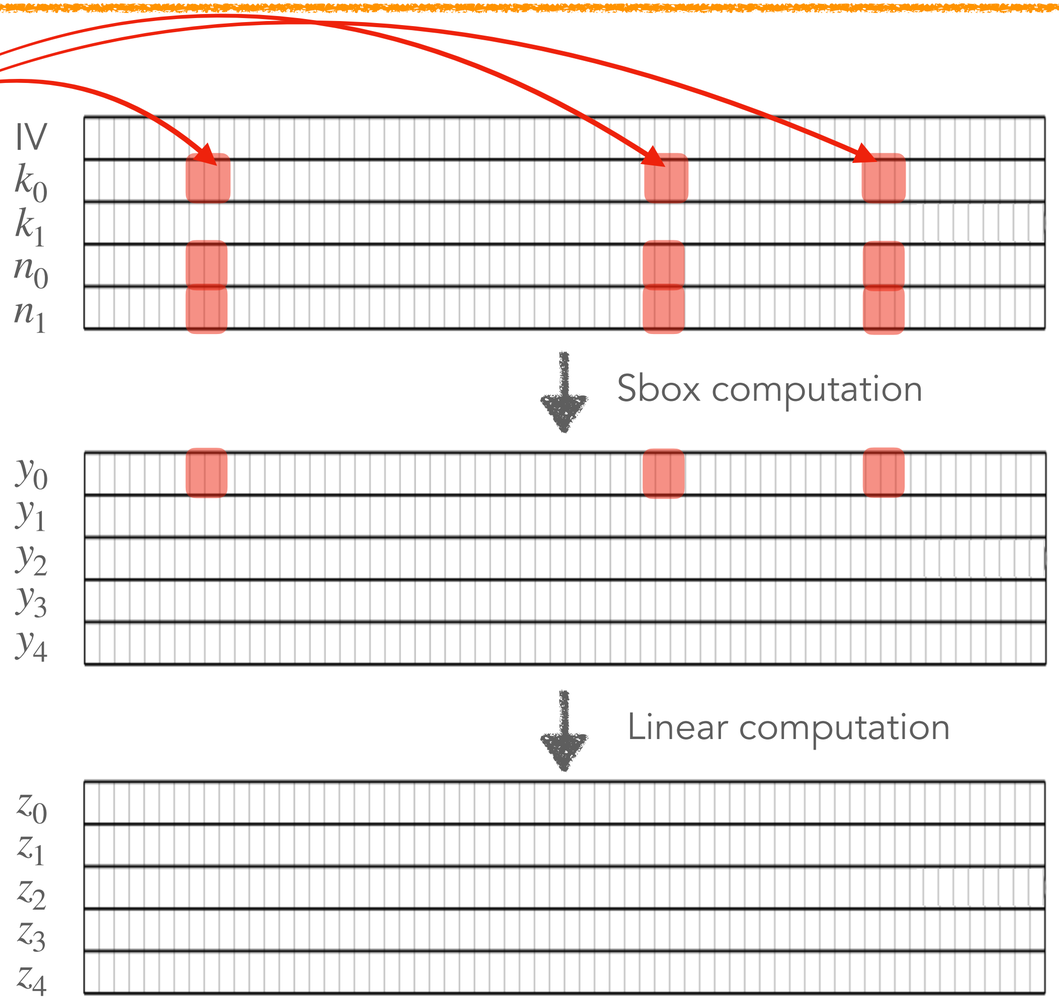
Advantage in number of CPA runs

hypothetical power consumption modeled on d bits	# recovered key bits in 1 CPA run	# CPA runs to recover 128-bit key
$d = 1$	3	48
$d = 2$	6	



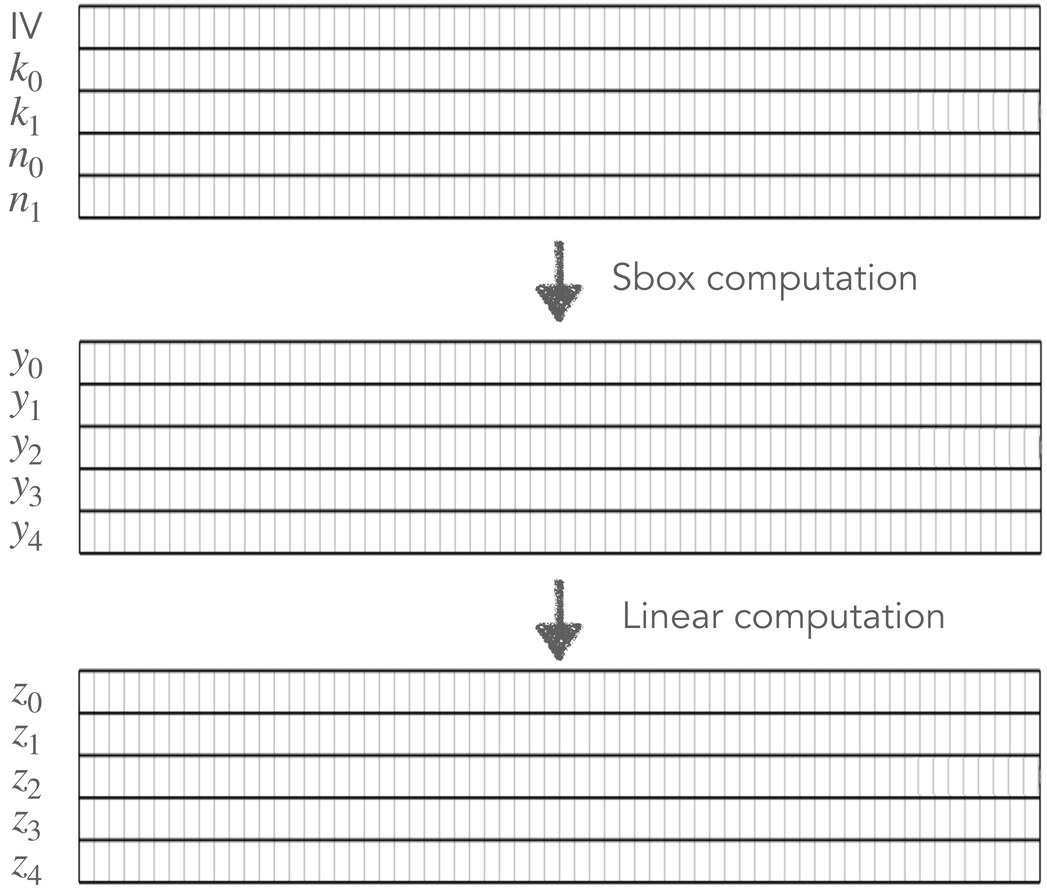
Advantage in number of CPA runs

hypothetical power consumption modeled on d bits	# recovered key bits in 1 CPA run	# CPA runs to recover 128-bit key
$d = 1$	3	48
$d = 2$	6	26



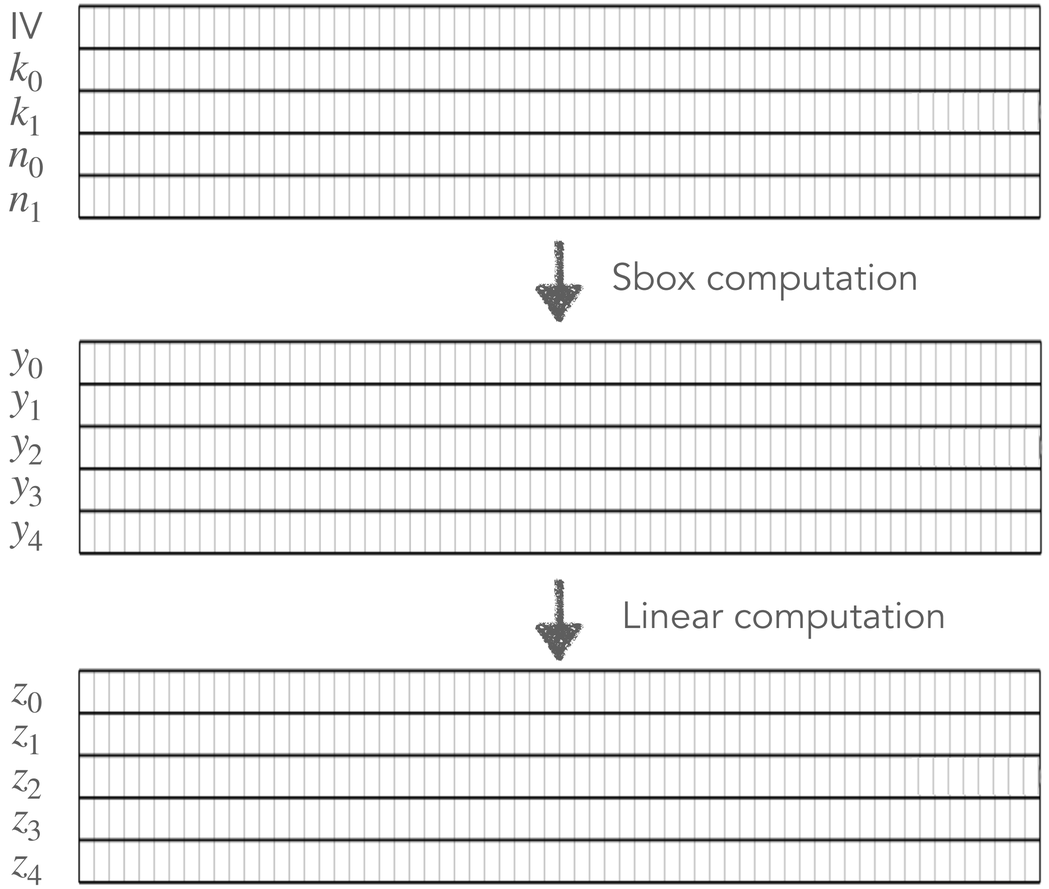
Advantage in number of CPA runs

hypothetical power consumption modeled on d bits	# recovered key bits in 1 CPA run	# CPA runs to recover 128-bit key
$d = 1$	3	48
$d = 2$	6	26



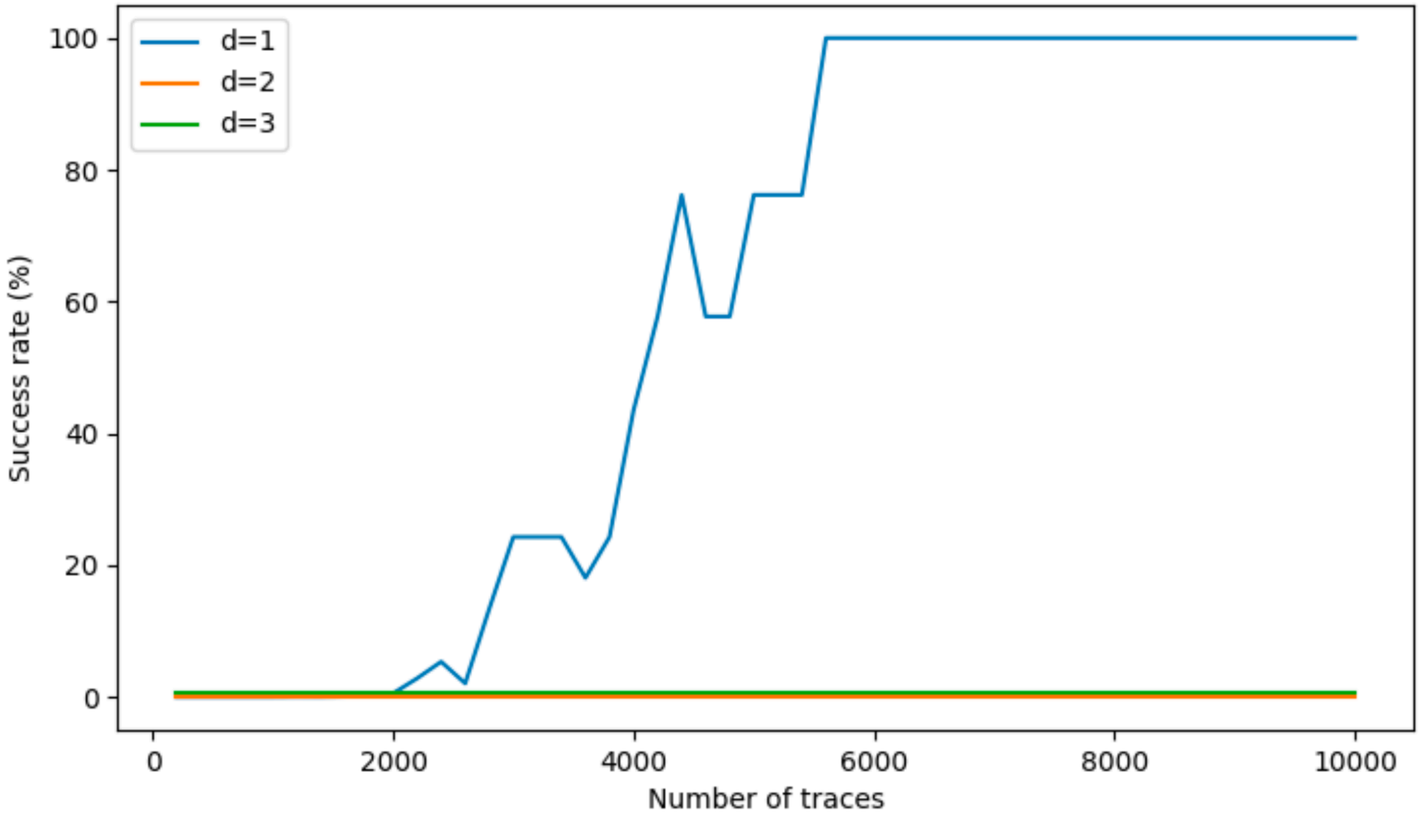
Advantage in number of CPA runs

hypothetical power consumption modeled on d bits	# recovered key bits in 1 CPA run	# CPA runs to recover 128-bit key
$d = 1$	3	48
$d = 2$	6	26
$d = 3$	9	19

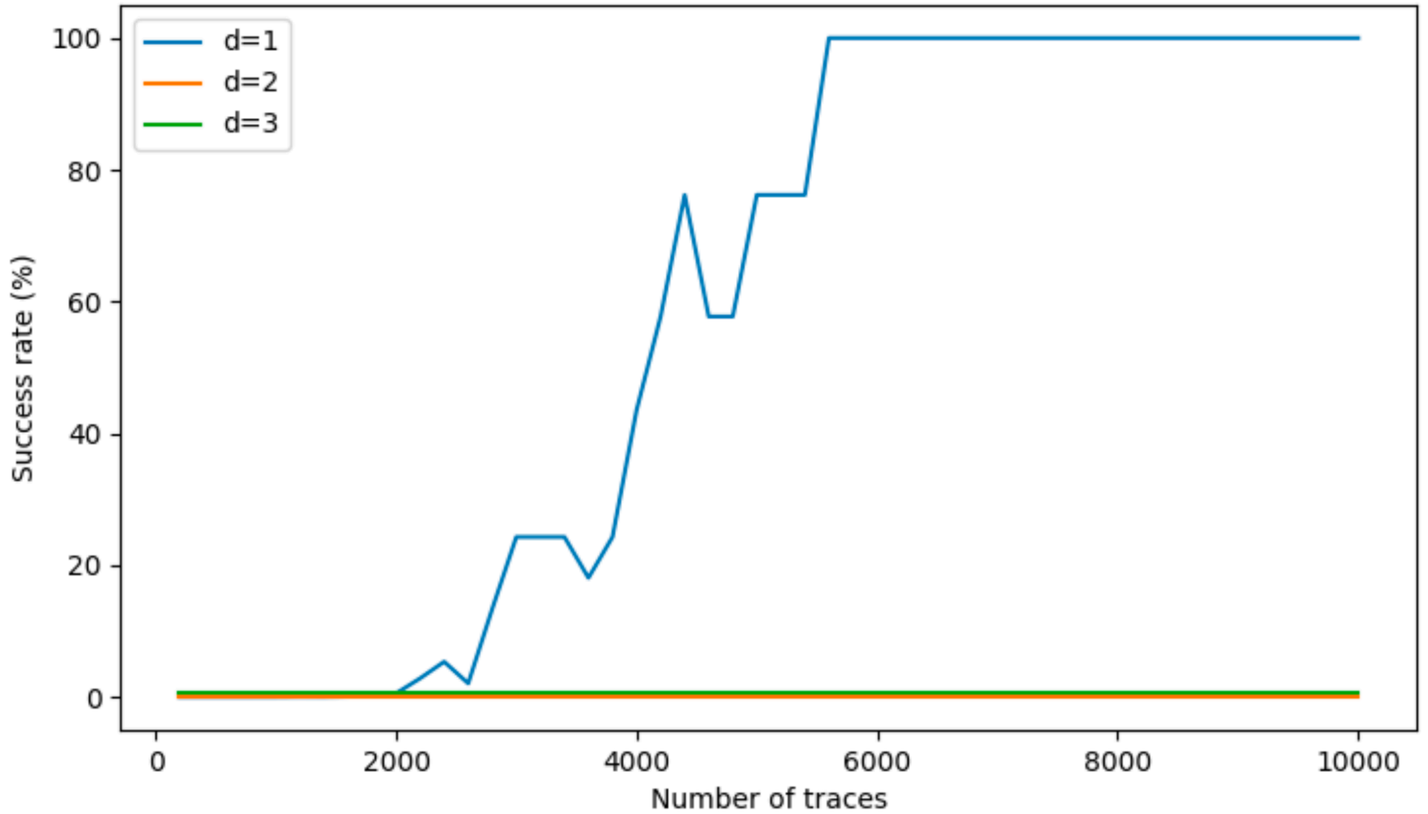


Results of full key recovery

Results of full key recovery



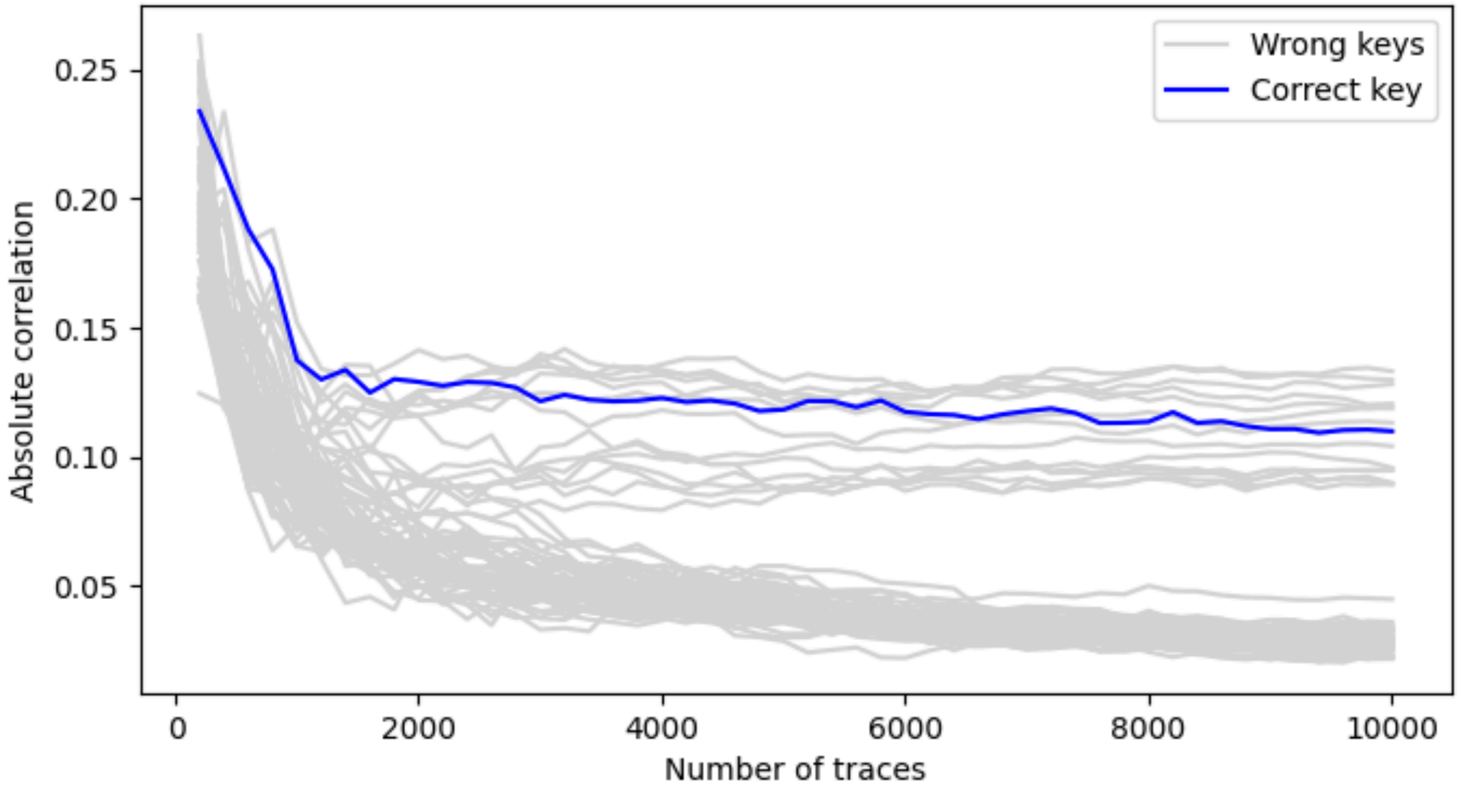
Results of full key recovery



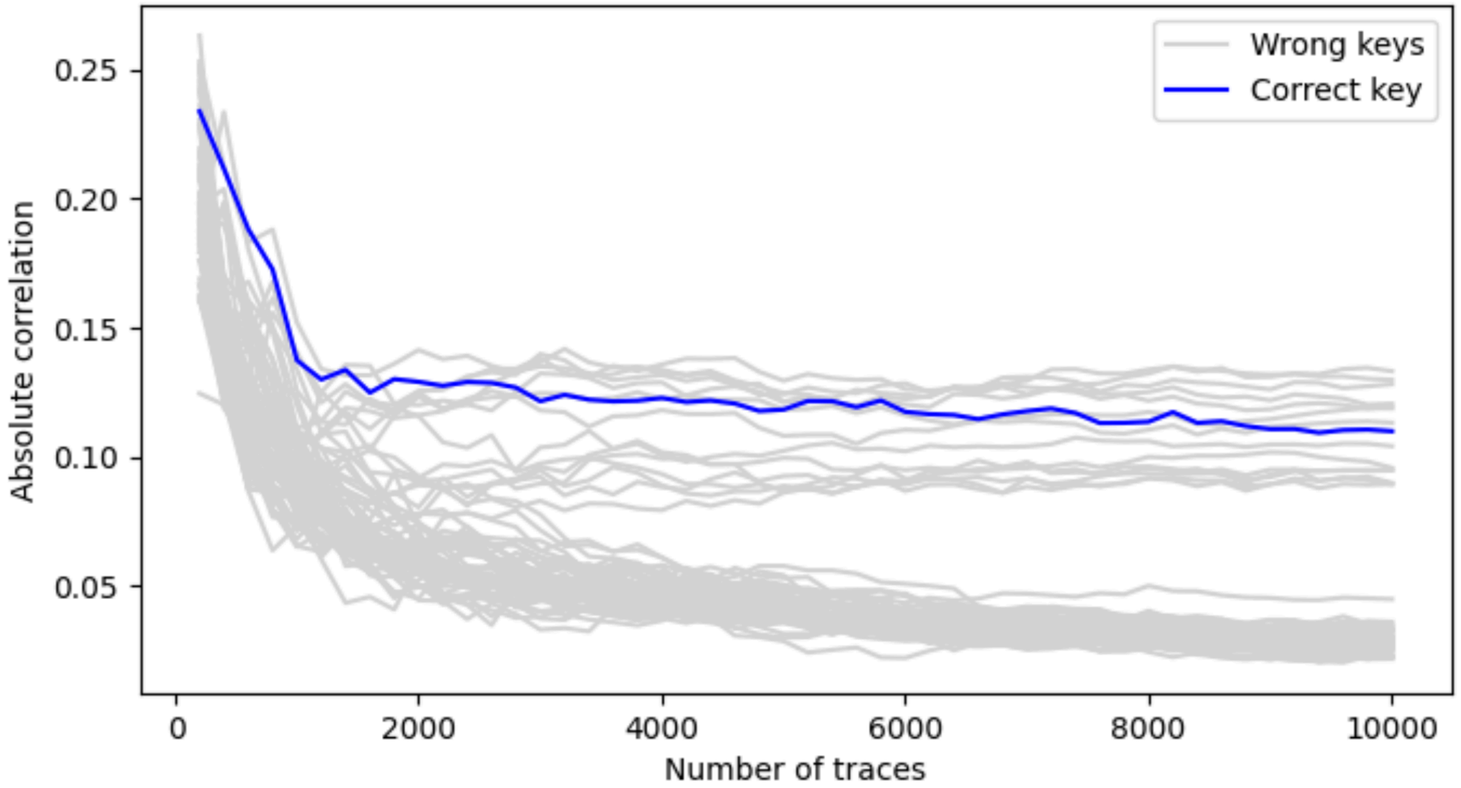
Why ? 🤔

Correlations

Correlations

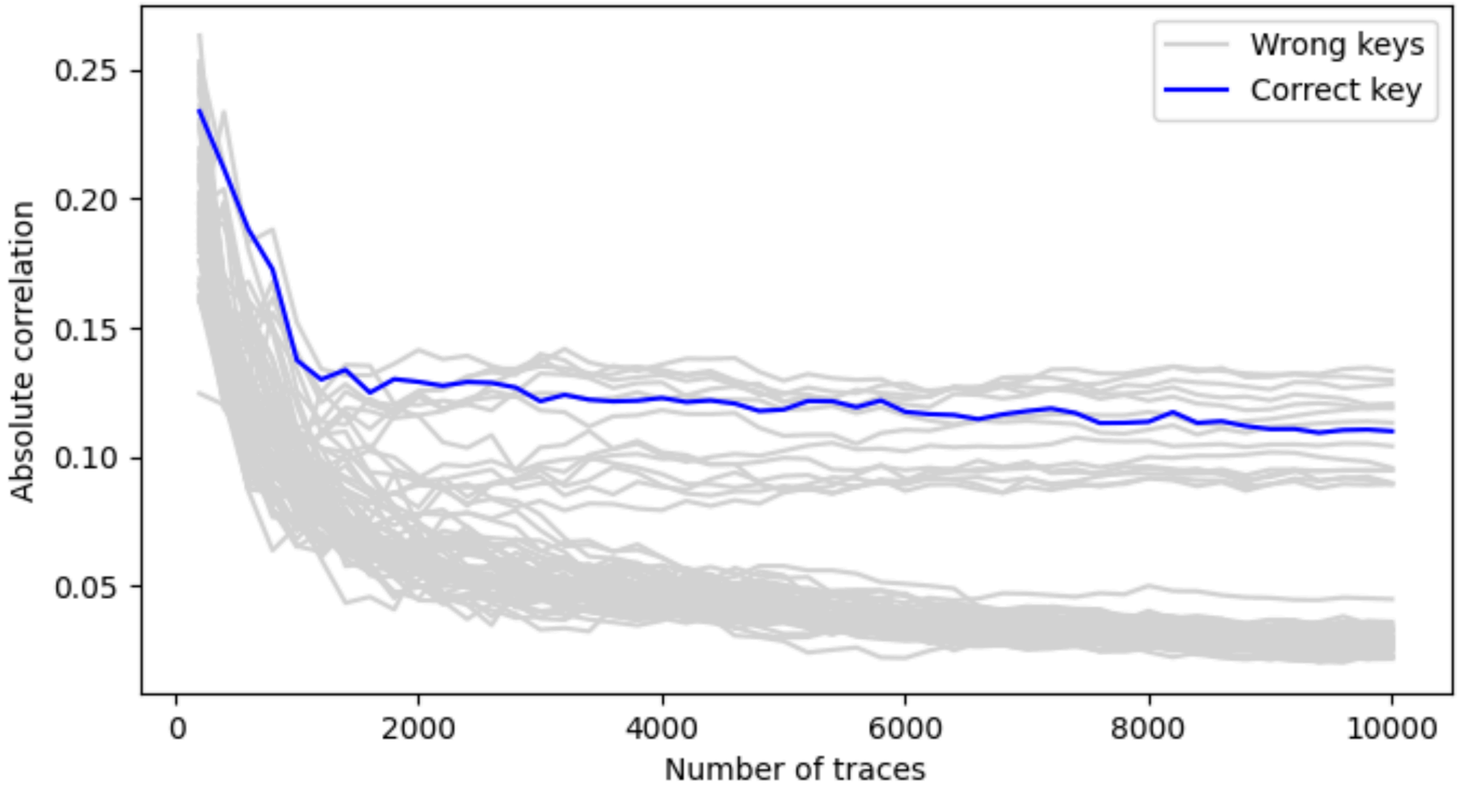


Correlations



Expected: correct key is distinguished

Correlations



Expected: correct key is distinguished

Observed: a group of keys is distinguished

Correlations

Expected: correct key is distinguished

Observed: a group of keys is distinguished

Correlations

Rank	Key	Corr.	Rank	Key	Corr.
1	10	0.133	33	6	0.030
2	32	0.130	34	26	0.030
3	2	0.128	35	27	0.030
4	42	0.121	36	35	0.029
5	40	0.119	37	53	0.029
6	8	0.119	38	55	0.029
7	34	0.113	39	44	0.028
8	0	0.110	40	3	0.028
9	1	0.104	41	57	0.028
10	5	0.096	42	50	0.028
11	4	0.095	43	45	0.028
12	17	0.095	44	37	0.027
13	16	0.090	45	41	0.027
14	21	0.089	46	12	0.026
15	20	0.089	47	46	0.026
16	31	0.045	48	49	0.026
17	60	0.036	49	33	0.026
18	61	0.035	50	54	0.026
19	15	0.035	51	47	0.026
20	23	0.034	52	58	0.026
21	11	0.033	53	48	0.026
22	19	0.033	54	62	0.026
23	22	0.033	55	13	0.025
24	39	0.033	56	28	0.025
25	7	0.033	57	24	0.025
26	43	0.032	58	25	0.023
27	18	0.032	59	59	0.023
28	56	0.031	60	51	0.023
29	14	0.030	61	38	0.023
30	30	0.030	62	63	0.022
31	36	0.030	63	9	0.022
32	52	0.030	64	29	0.022

Expected: correct key is distinguished

Observed: a group of keys is distinguished

Correlations

Rank	Key	Corr.	Rank	Key	Corr.
1	10	0.133	33	6	0.030
2	32	0.130	34	26	0.030
3	2	0.128	35	27	0.030
4	42	0.121	36	35	0.029
5	40	0.119	37	53	0.029
6	8	0.119	38	55	0.029
7	34	0.113	39	44	0.028
8	0	0.110	40	3	0.028
9	1	0.104	41	57	0.028
10	5	0.096	42	50	0.028
11	4	0.095	43	45	0.028
12	17	0.095	44	37	0.027
13	16	0.090	45	41	0.027
14	21	0.089	46	12	0.026
15	20	0.089	47	46	0.026
16	31	0.045	48	49	0.026
17	60	0.036	49	33	0.026
18	61	0.035	50	54	0.026
19	15	0.035	51	47	0.026
20	23	0.034	52	58	0.026
21	11	0.033	53	48	0.026
22	19	0.033	54	62	0.026
23	22	0.033	55	13	0.025
24	39	0.033	56	28	0.025
25	7	0.033	57	24	0.025
26	43	0.032	58	25	0.023
27	18	0.032	59	59	0.023
28	56	0.031	60	51	0.023
29	14	0.030	61	38	0.023
30	30	0.030	62	63	0.022
31	36	0.030	63	9	0.022
32	52	0.030	64	29	0.022

Expected: correct key is distinguished

Observed: a group of keys is distinguished

Correlations

Rank	Key	Corr.	Rank	Key	Corr.
1	10	0.133	33	6	0.030
2	32	0.130	34	26	0.030
3	2	0.128	35	27	0.030
4	42	0.121	36	35	0.029
5	40	0.119	37	53	0.029
6	8	0.119	38	55	0.029
7	34	0.113	39	44	0.028
8	0	0.110	40	3	0.028
9	1	0.104	41	57	0.028
10	5	0.096	42	50	0.028
11	4	0.095	43	45	0.028
12	17	0.095	44	37	0.027
13	16	0.090	45	41	0.027
14	21	0.089	46	12	0.026
15	20	0.089	47	46	0.026
16	31	0.045	48	49	0.026
17	60	0.036	49	33	0.026
18	61	0.035	50	54	0.026
19	15	0.035	51	47	0.026
20	23	0.034	52	58	0.026
21	11	0.033	53	48	0.026
22	19	0.033	54	62	0.026
23	22	0.033	55	13	0.025
24	39	0.033	56	28	0.025
25	7	0.033	57	24	0.025
26	43	0.032	58	25	0.023
27	18	0.032	59	59	0.023
28	56	0.031	60	51	0.023
29	14	0.030	61	38	0.023
30	30	0.030	62	63	0.022
31	36	0.030	63	9	0.022
32	52	0.030	64	29	0.022

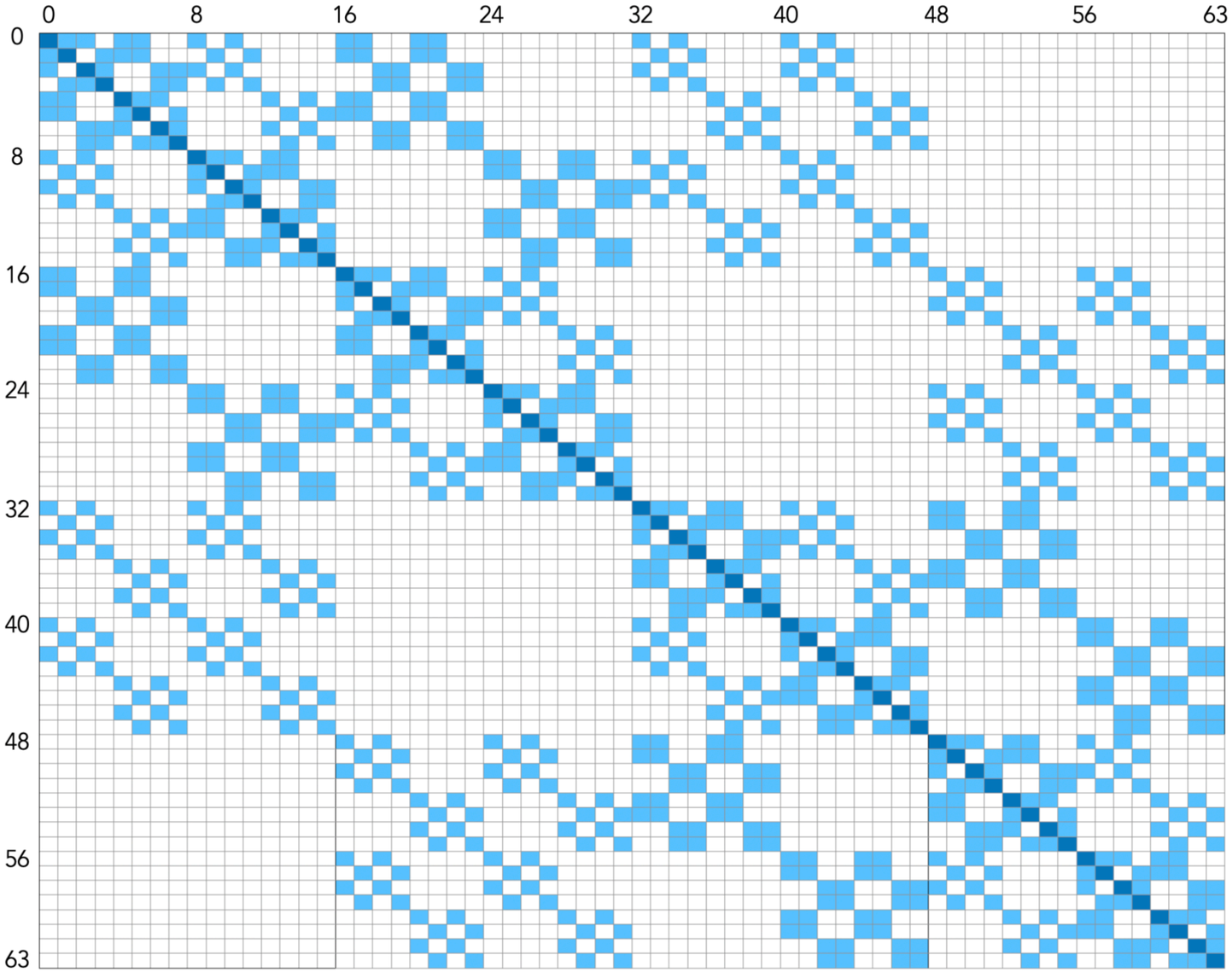
Expected: correct key is distinguished

Observed: a group of keys is distinguished

Suspected: distributions associated to some keys are partially correlated !? 🤔

Correlations between distributions of all key pairs

Correlations between distributions of all key pairs

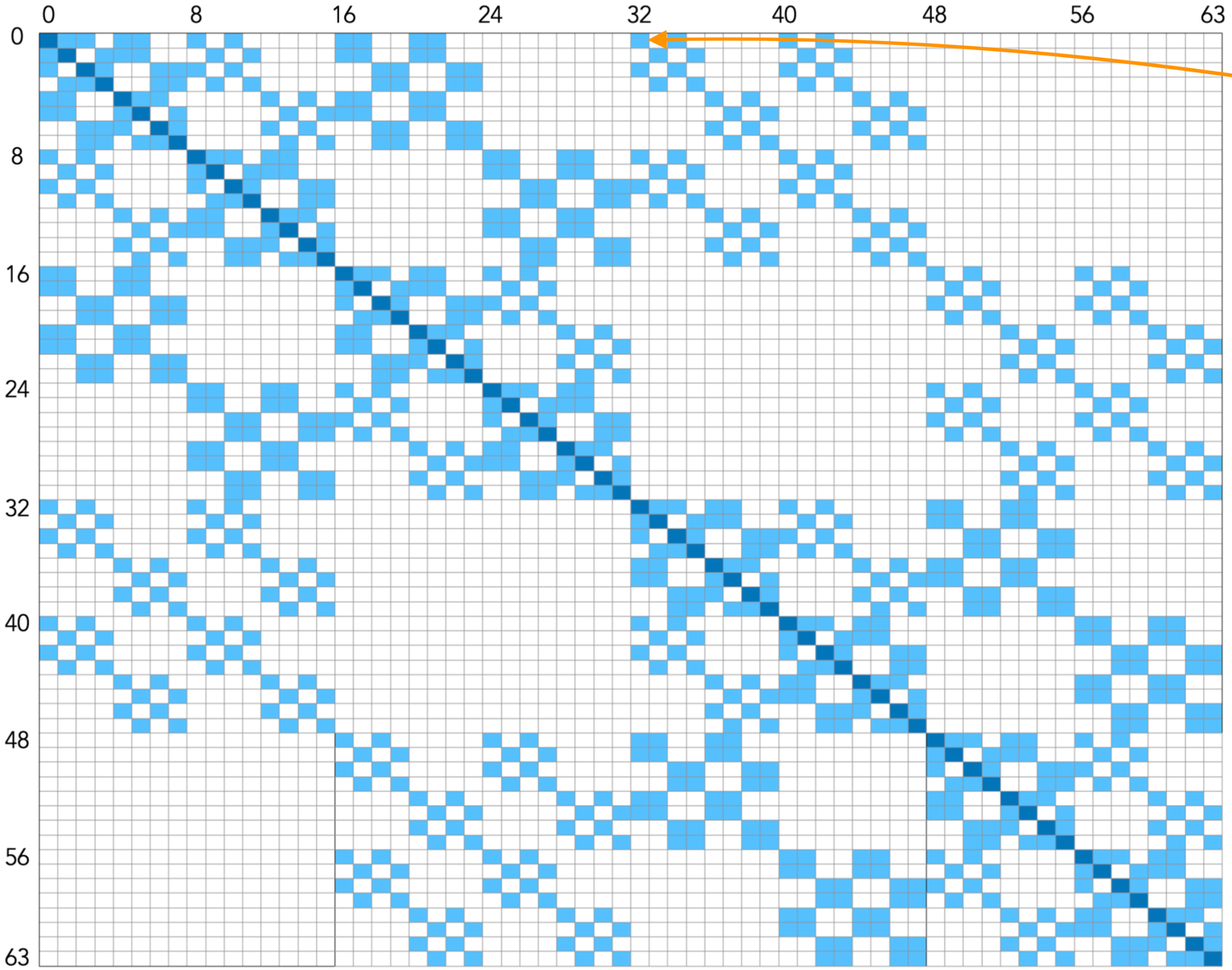


correlation of 1

correlation of 0.5

correlation of 0

Correlations between distributions of all key pairs



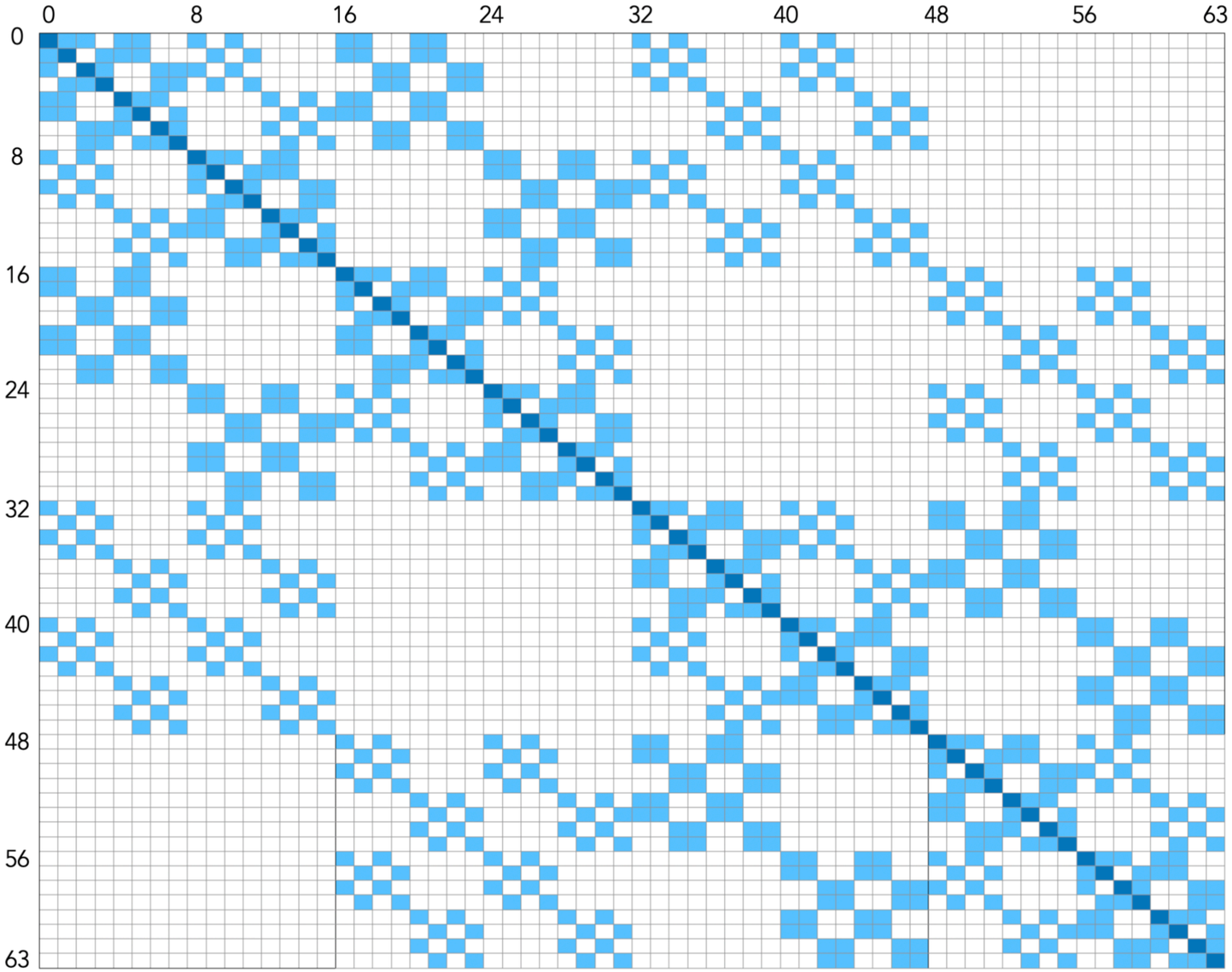
distributions corresponding to key pair (0,32) are correlated with coefficient of 0.5

correlation of 1

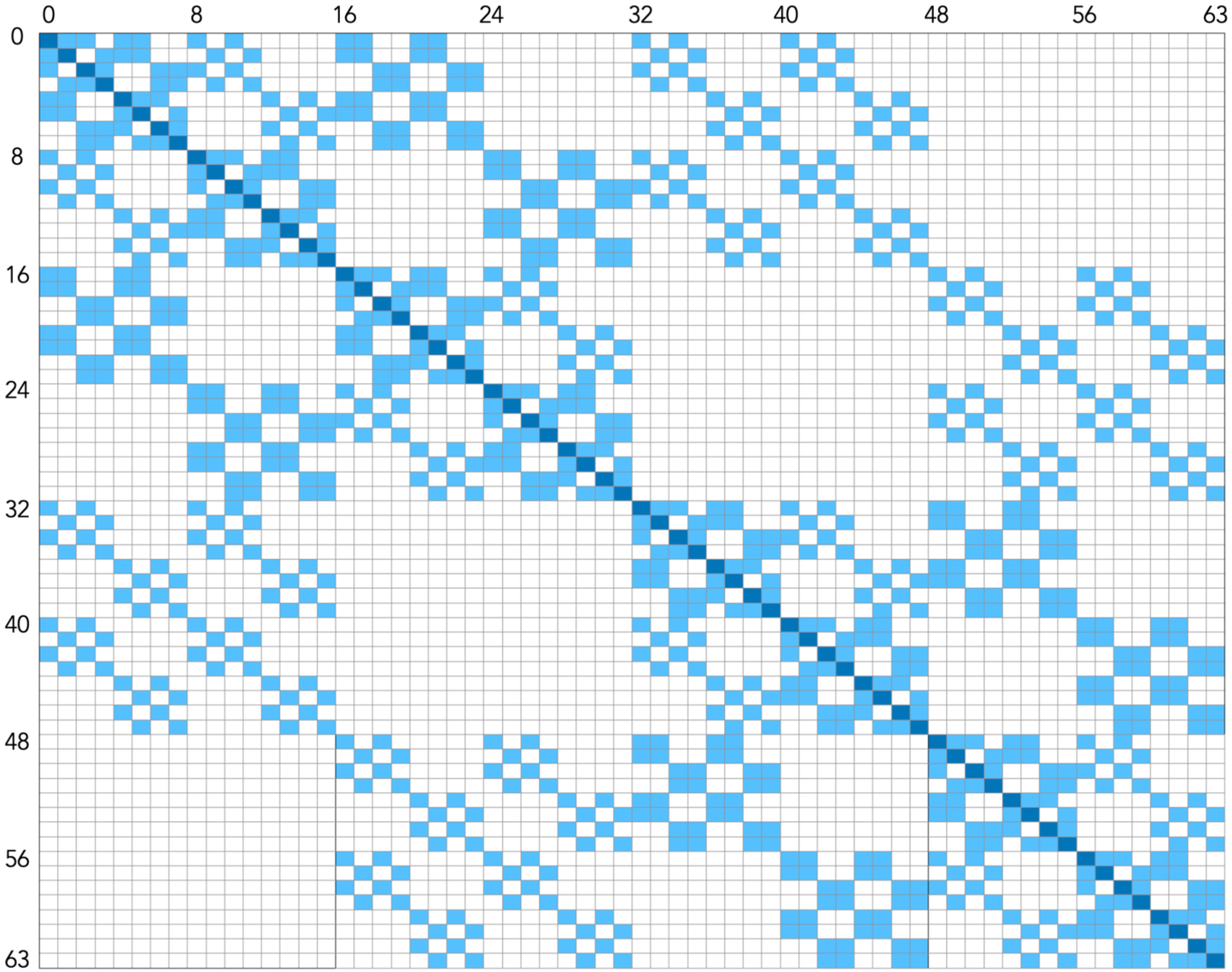
correlation of 0.5

correlation of 0

Verify the prediction

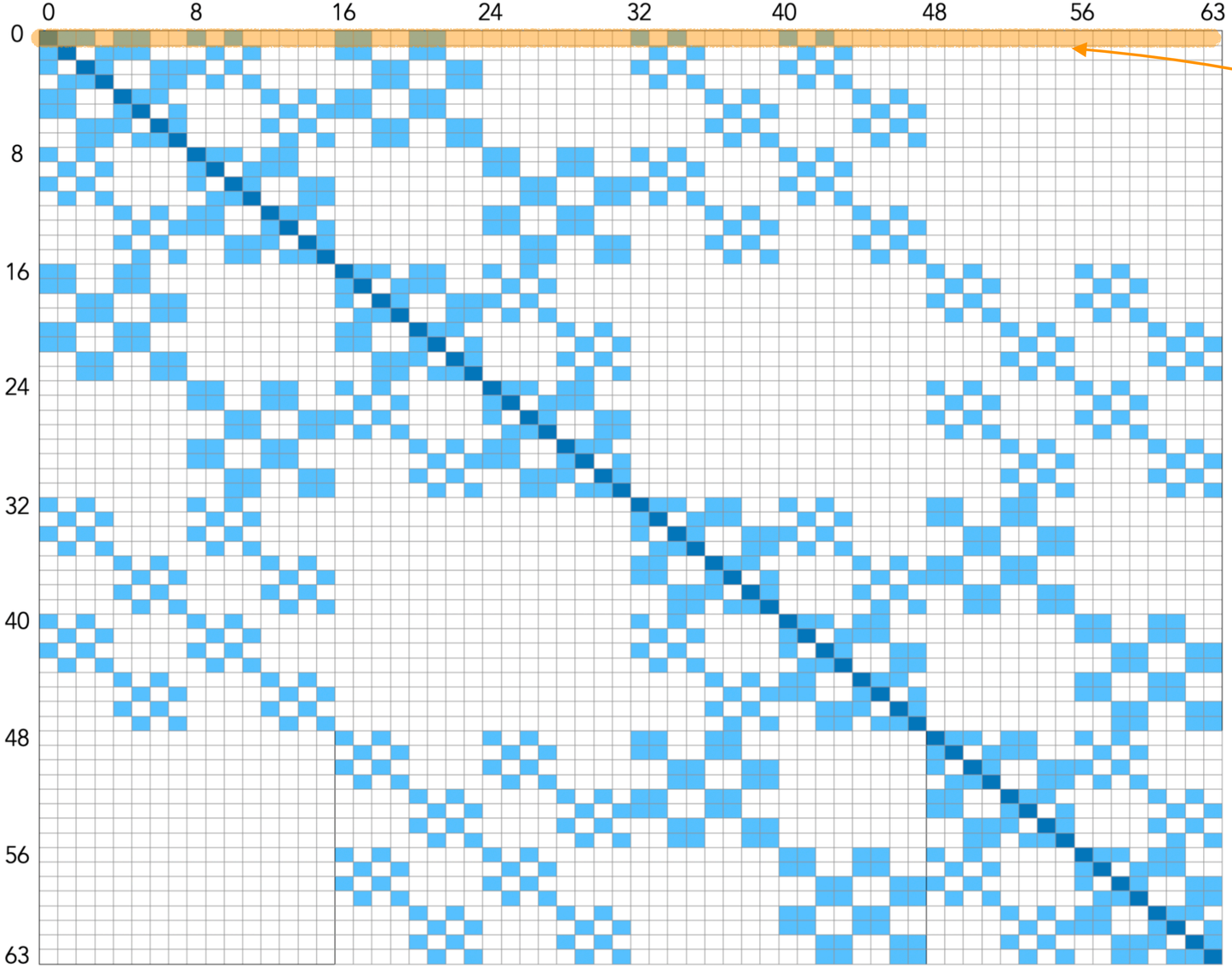


Verify the prediction



Rank	Key	Corr.	Rank	Key	Corr.
1	10	0.133	33	6	0.030
2	32	0.130	34	26	0.030
3	2	0.128	35	27	0.030
4	42	0.121	36	35	0.029
5	40	0.119	37	53	0.029
6	8	0.119	38	55	0.029
7	34	0.113	39	44	0.028
8	0	0.110	40	3	0.028
9	1	0.104	41	57	0.028
10	5	0.096	42	50	0.028
11	4	0.095	43	45	0.028
12	17	0.095	44	37	0.027
13	16	0.090	45	41	0.027
14	21	0.089	46	12	0.026
15	20	0.089	47	46	0.026
16	31	0.045	48	49	0.026
17	60	0.036	49	33	0.026
18	61	0.035	50	54	0.026
19	15	0.035	51	47	0.026
20	23	0.034	52	58	0.026
21	11	0.033	53	48	0.026
22	19	0.033	54	62	0.026
23	22	0.033	55	13	0.025
24	39	0.033	56	28	0.025
25	7	0.033	57	24	0.025
26	43	0.032	58	25	0.023
27	18	0.032	59	59	0.023
28	56	0.031	60	51	0.023
29	14	0.030	61	38	0.023
30	30	0.030	62	63	0.022
31	36	0.030	63	9	0.022
32	52	0.030	64	29	0.022

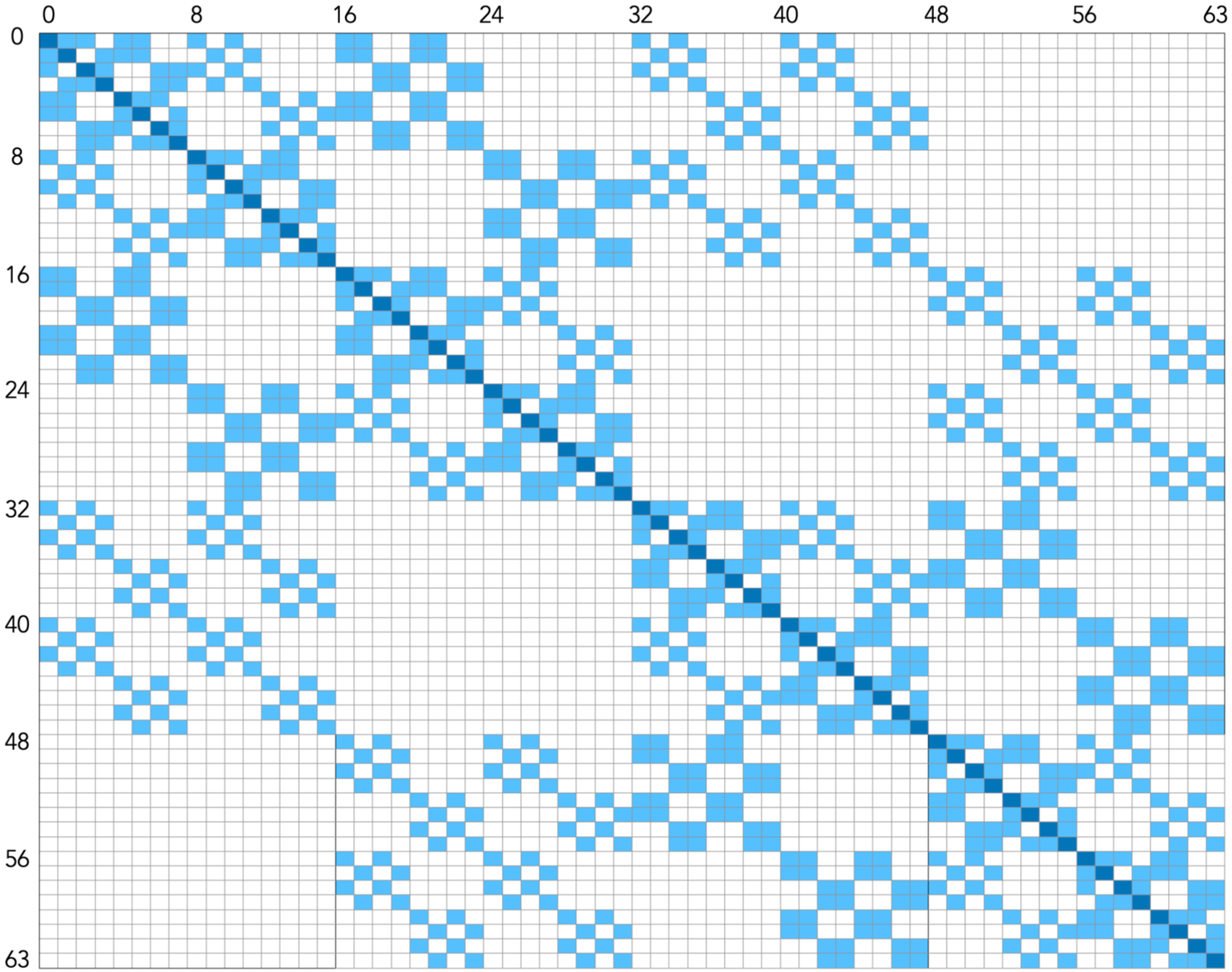
Verify the prediction



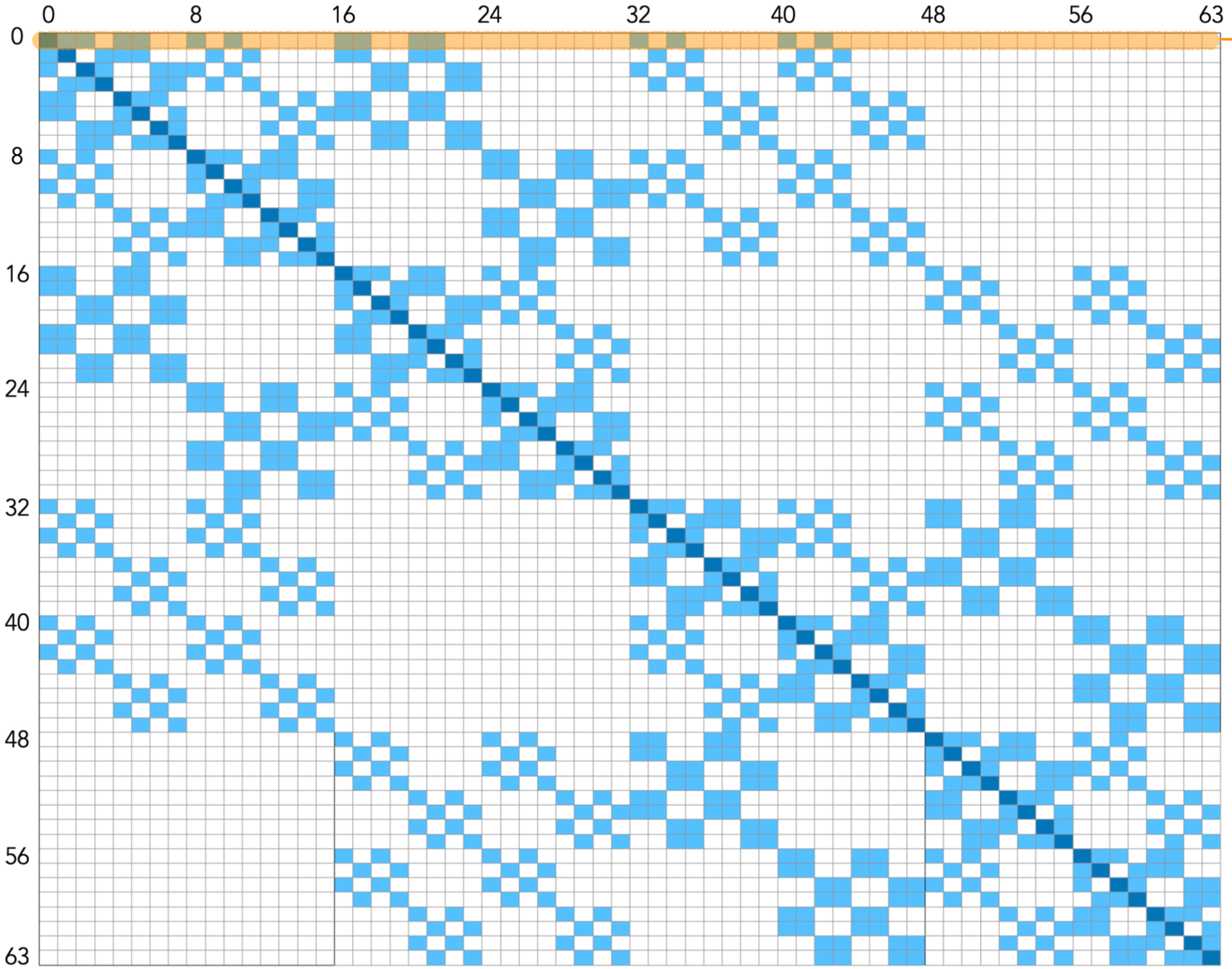
Rank	Key	Corr.	Rank	Key	Corr.
1	10	0.133	33	6	0.030
2	32	0.130	34	26	0.030
3	2	0.128	35	27	0.030
4	42	0.121	36	35	0.029
5	40	0.119	37	53	0.029
6	8	0.119	38	55	0.029
7	34	0.113	39	44	0.028
8	0	0.110	40	3	0.028
9	1	0.104	41	57	0.028
10	5	0.096	42	50	0.028
11	4	0.095	43	45	0.028
12	17	0.095	44	37	0.027
13	16	0.090	45	41	0.027
14	21	0.089	46	12	0.026
15	20	0.089	47	46	0.026
16	31	0.045	48	49	0.026
17	60	0.036	49	33	0.026
18	61	0.035	50	54	0.026
19	15	0.035	51	47	0.026
20	23	0.034	52	58	0.026
21	11	0.033	53	48	0.026
22	19	0.033	54	62	0.026
23	22	0.033	55	13	0.025
24	39	0.033	56	28	0.025
25	7	0.033	57	24	0.025
26	43	0.032	58	25	0.023
27	18	0.032	59	59	0.023
28	56	0.031	60	51	0.023
29	14	0.030	61	38	0.023
30	30	0.030	62	63	0.022
31	36	0.030	63	9	0.022
32	52	0.030	64	29	0.022

How to recover the key ?

Each key has an associated group

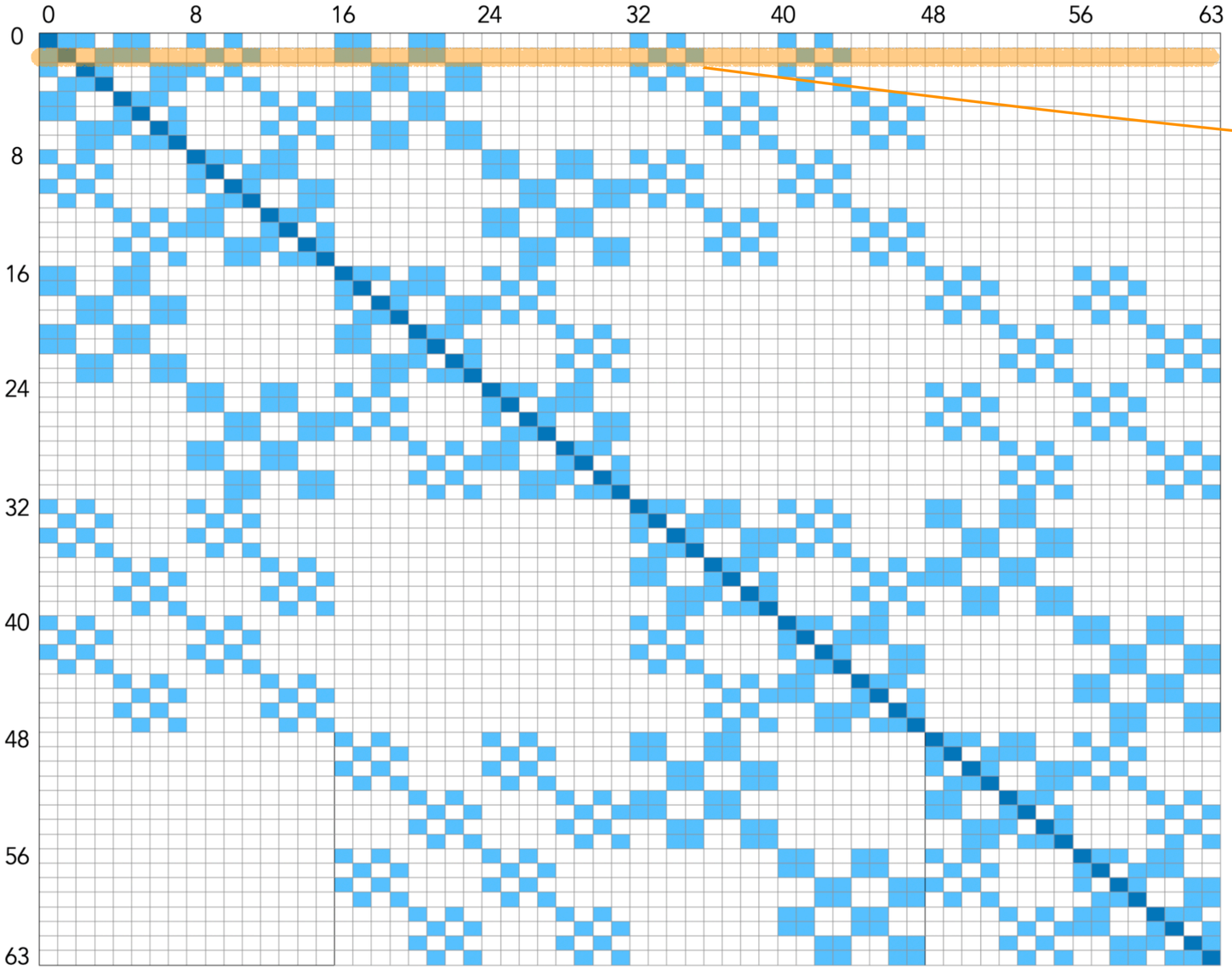


Each key has an associated group



$\mathcal{G}[0] = [0,1,2,4,5,8,10,16,17,20,21,32,34,40,42]$

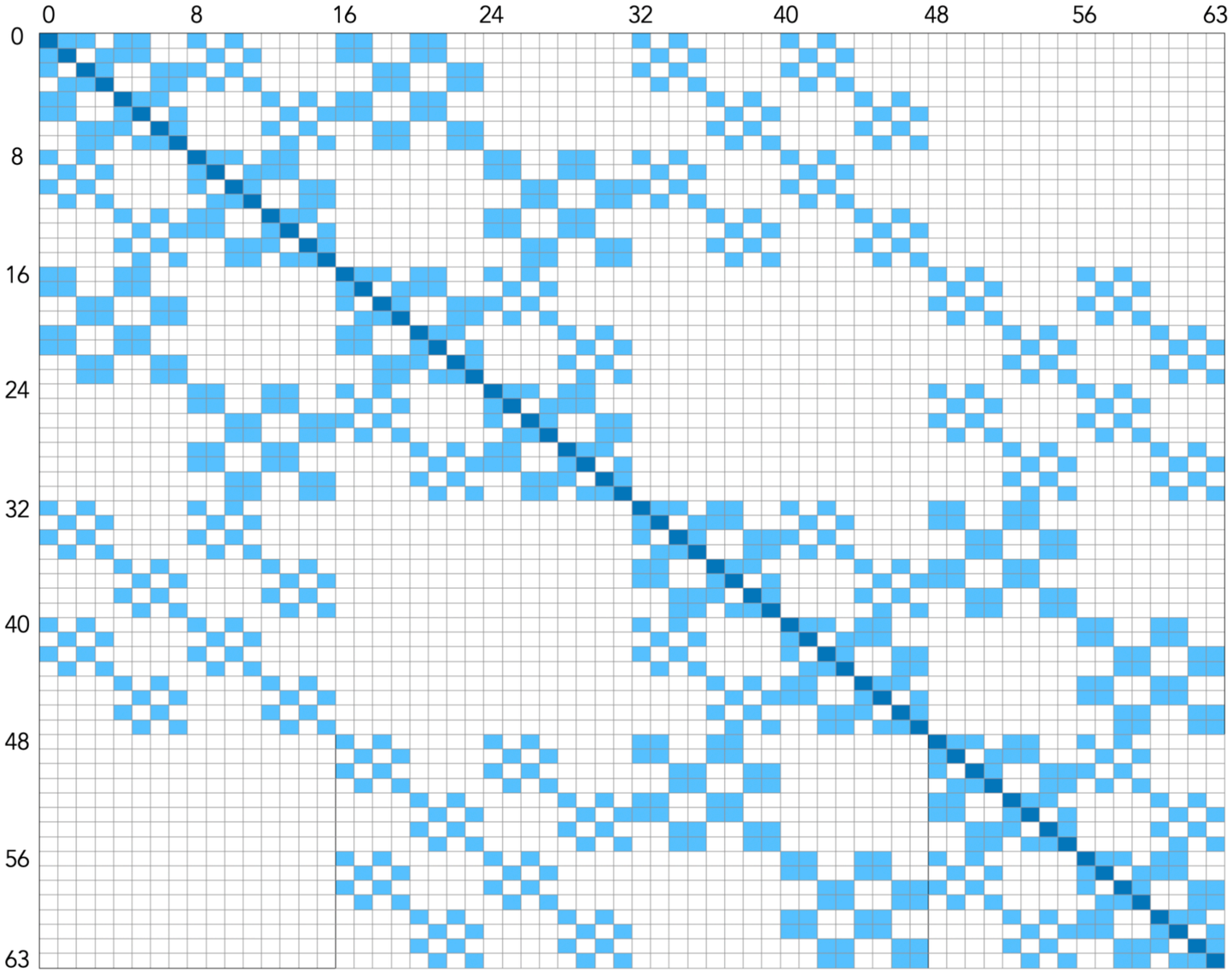
Each key has an associated group



$\mathcal{G}[0] = [0,1,2,4,5,8,10,16,17,20,21,32,34,40,42]$

$\mathcal{G}[1] = [0,1,3,4,5,9,11,16,17,20,21,33,35,41,43]$

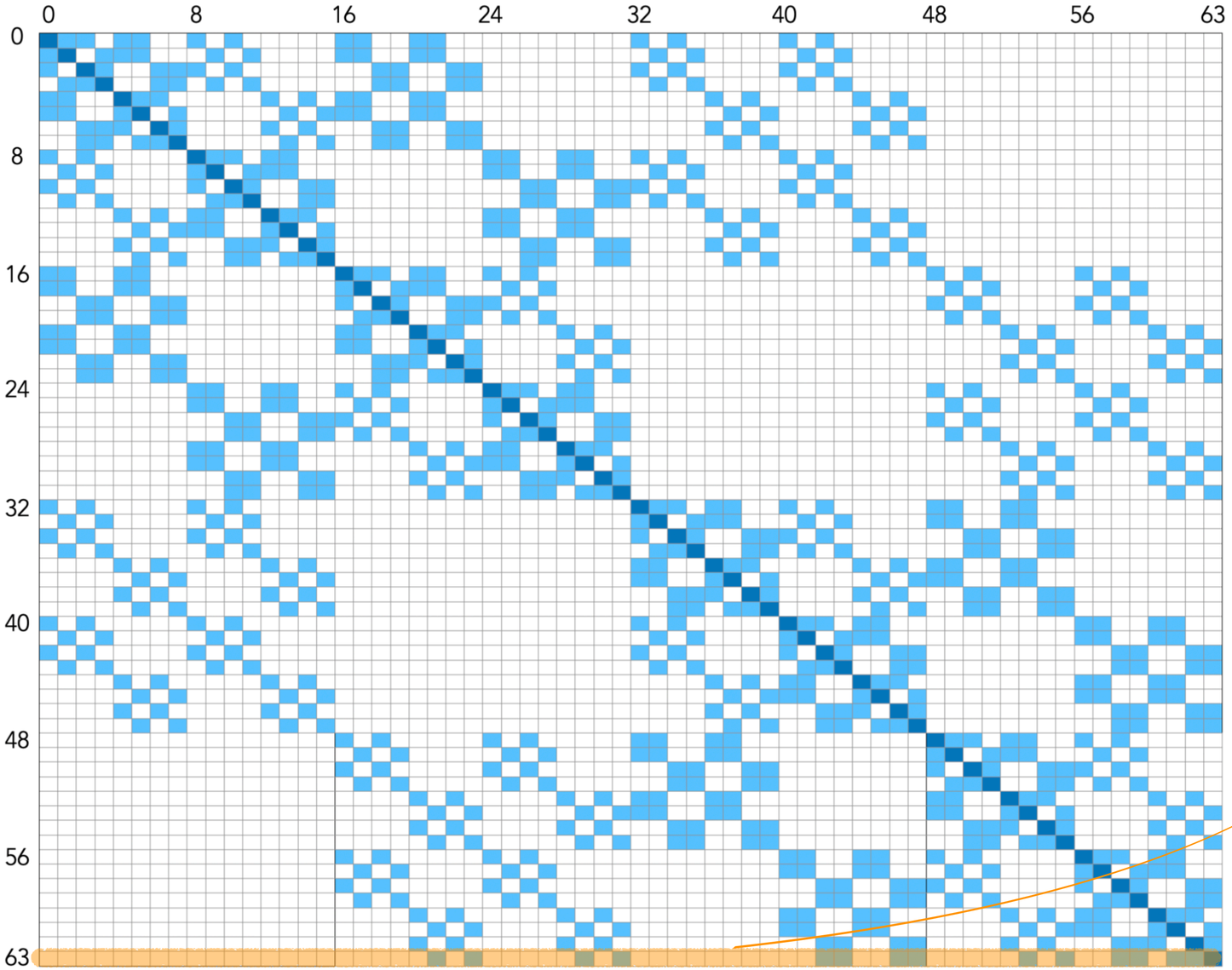
Each key has an associated group



$\mathcal{G}[0] = [0,1,2,4,5,8,10,16,17,20,21,32,34,40,42]$

$\mathcal{G}[1] = [0,1,3,4,5,9,11,16,17,20,21,33,35,41,43]$

Each key has an associated group



$\mathcal{G}[0] = [0,1,2,4,5,8,10,16,17,20,21,32,34,40,42]$

$\mathcal{G}[1] = [0,1,3,4,5,9,11,16,17,20,21,33,35,41,43]$

$\ldots$

$\mathcal{G}[63] = [\ldots]$

Verify the prediction

Rank	Key	Corr.	Rank	Key	Corr.
1	10	0.133	33	6	0.030
2	32	0.130	34	26	0.030
3	2	0.128	35	27	0.030
4	42	0.121	36	35	0.029
5	40	0.119	37	53	0.029
6	8	0.119	38	55	0.029
7	34	0.113	39	44	0.028
8	0	0.110	40	3	0.028
9	1	0.104	41	57	0.028
10	5	0.096	42	50	0.028
11	4	0.095	43	45	0.028
12	17	0.095	44	37	0.027
13	16	0.090	45	41	0.027
14	21	0.089	46	12	0.026
15	20	0.089	47	46	0.026
16	31	0.045	48	49	0.026
17	60	0.036	49	33	0.026
18	61	0.035	50	54	0.026
19	15	0.035	51	47	0.026
20	23	0.034	52	58	0.026
21	11	0.033	53	48	0.026
22	19	0.033	54	62	0.026
23	22	0.033	55	13	0.025
24	39	0.033	56	28	0.025
25	7	0.033	57	24	0.025
26	43	0.032	58	25	0.023
27	18	0.032	59	59	0.023
28	56	0.031	60	51	0.023
29	14	0.030	61	38	0.023
30	30	0.030	62	63	0.022
31	36	0.030	63	9	0.022
32	52	0.030	64	29	0.022

Verify the prediction

Which group does these key candidates correspond to ?

Rank	Key	Corr.	Rank	Key	Corr.
1	10	0.133	33	6	0.030
2	32	0.130	34	26	0.030
3	2	0.128	35	27	0.030
4	42	0.121	36	35	0.029
5	40	0.119	37	53	0.029
6	8	0.119	38	55	0.029
7	34	0.113	39	44	0.028
8	0	0.110	40	3	0.028
9	1	0.104	41	57	0.028
10	5	0.096	42	50	0.028
11	4	0.095	43	45	0.028
12	17	0.095	44	37	0.027
13	16	0.090	45	41	0.027
14	21	0.089	46	12	0.026
15	20	0.089	47	46	0.026
16	31	0.045	48	49	0.026
17	60	0.036	49	33	0.026
18	61	0.035	50	54	0.026
19	15	0.035	51	47	0.026
20	23	0.034	52	58	0.026
21	11	0.033	53	48	0.026
22	19	0.033	54	62	0.026
23	22	0.033	55	13	0.025
24	39	0.033	56	28	0.025
25	7	0.033	57	24	0.025
26	43	0.032	58	25	0.023
27	18	0.032	59	59	0.023
28	56	0.031	60	51	0.023
29	14	0.030	61	38	0.023
30	30	0.030	62	63	0.022
31	36	0.030	63	9	0.022
32	52	0.030	64	29	0.022

Verify the prediction

Which group does these key candidates correspond to ?

$\mathcal{G}[1]$

Rank	Key	Corr.	Rank	Key	Corr.
1	10	0.133	33	6	0.030
2	32	0.130	34	26	0.030
3	2	0.128	35	27	0.030
4	42	0.121	36	35	0.029
5	40	0.119	37	53	0.029
6	8	0.119	38	55	0.029
7	34	0.113	39	44	0.028
8	0	0.110	40	3	0.028
9	1	0.104	41	57	0.028
10	5	0.096	42	50	0.028
11	4	0.095	43	45	0.028
12	17	0.095	44	37	0.027
13	16	0.090	45	41	0.027
14	21	0.089	46	12	0.026
15	20	0.089	47	46	0.026
16	31	0.045	48	49	0.026
17	60	0.036	49	33	0.026
18	61	0.035	50	54	0.026
19	15	0.035	51	47	0.026
20	23	0.034	52	58	0.026
21	11	0.033	53	48	0.026
22	19	0.033	54	62	0.026
23	22	0.033	55	13	0.025
24	39	0.033	56	28	0.025
25	7	0.033	57	24	0.025
26	43	0.032	58	25	0.023
27	18	0.032	59	59	0.023
28	56	0.031	60	51	0.023
29	14	0.030	61	38	0.023
30	30	0.030	62	63	0.022
31	36	0.030	63	9	0.022
32	52	0.030	64	29	0.022

Verify the prediction

Which group does these key candidates correspond to ?

$\mathcal{G}[1]$ ✗

Rank	Key	Corr.	Rank	Key	Corr.
1	10	0.133	33	6	0.030
2	32	0.130	34	26	0.030
3	2	0.128	35	27	0.030
4	42	0.121	36	35	0.029
5	40	0.119	37	53	0.029
6	8	0.119	38	55	0.029
7	34	0.113	39	44	0.028
8	0	0.110	40	3	0.028
9	1	0.104	41	57	0.028
10	5	0.096	42	50	0.028
11	4	0.095	43	45	0.028
12	17	0.095	44	37	0.027
13	16	0.090	45	41	0.027
14	21	0.089	46	12	0.026
15	20	0.089	47	46	0.026
16	31	0.045	48	49	0.026
17	60	0.036	49	33	0.026
18	61	0.035	50	54	0.026
19	15	0.035	51	47	0.026
20	23	0.034	52	58	0.026
21	11	0.033	53	48	0.026
22	19	0.033	54	62	0.026
23	22	0.033	55	13	0.025
24	39	0.033	56	28	0.025
25	7	0.033	57	24	0.025
26	43	0.032	58	25	0.023
27	18	0.032	59	59	0.023
28	56	0.031	60	51	0.023
29	14	0.030	61	38	0.023
30	30	0.030	62	63	0.022
31	36	0.030	63	9	0.022
32	52	0.030	64	29	0.022

Verify the prediction

Which group does these key candidates correspond to ?

$\mathcal{G}[1]$ ✗

$\mathcal{G}[2]$

Rank	Key	Corr.	Rank	Key	Corr.
1	10	0.133	33	6	0.030
2	32	0.130	34	26	0.030
3	2	0.128	35	27	0.030
4	42	0.121	36	35	0.029
5	40	0.119	37	53	0.029
6	8	0.119	38	55	0.029
7	34	0.113	39	44	0.028
8	0	0.110	40	3	0.028
9	1	0.104	41	57	0.028
10	5	0.096	42	50	0.028
11	4	0.095	43	45	0.028
12	17	0.095	44	37	0.027
13	16	0.090	45	41	0.027
14	21	0.089	46	12	0.026
15	20	0.089	47	46	0.026
16	31	0.045	48	49	0.026
17	60	0.036	49	33	0.026
18	61	0.035	50	54	0.026
19	15	0.035	51	47	0.026
20	23	0.034	52	58	0.026
21	11	0.033	53	48	0.026
22	19	0.033	54	62	0.026
23	22	0.033	55	13	0.025
24	39	0.033	56	28	0.025
25	7	0.033	57	24	0.025
26	43	0.032	58	25	0.023
27	18	0.032	59	59	0.023
28	56	0.031	60	51	0.023
29	14	0.030	61	38	0.023
30	30	0.030	62	63	0.022
31	36	0.030	63	9	0.022
32	52	0.030	64	29	0.022

Verify the prediction

Which group does these key candidates correspond to ?

$\mathcal{G}[1]$ ✗

$\mathcal{G}[2]$ ✗

Rank	Key	Corr.	Rank	Key	Corr.
1	10	0.133	33	6	0.030
2	32	0.130	34	26	0.030
3	2	0.128	35	27	0.030
4	42	0.121	36	35	0.029
5	40	0.119	37	53	0.029
6	8	0.119	38	55	0.029
7	34	0.113	39	44	0.028
8	0	0.110	40	3	0.028
9	1	0.104	41	57	0.028
10	5	0.096	42	50	0.028
11	4	0.095	43	45	0.028
12	17	0.095	44	37	0.027
13	16	0.090	45	41	0.027
14	21	0.089	46	12	0.026
15	20	0.089	47	46	0.026
16	31	0.045	48	49	0.026
17	60	0.036	49	33	0.026
18	61	0.035	50	54	0.026
19	15	0.035	51	47	0.026
20	23	0.034	52	58	0.026
21	11	0.033	53	48	0.026
22	19	0.033	54	62	0.026
23	22	0.033	55	13	0.025
24	39	0.033	56	28	0.025
25	7	0.033	57	24	0.025
26	43	0.032	58	25	0.023
27	18	0.032	59	59	0.023
28	56	0.031	60	51	0.023
29	14	0.030	61	38	0.023
30	30	0.030	62	63	0.022
31	36	0.030	63	9	0.022
32	52	0.030	64	29	0.022

Verify the prediction

Which group does these key candidates correspond to ?

$\mathcal{G}[1]$ ✗

$\mathcal{G}[2]$ ✗

...

$\mathcal{G}[63]$ ✗

Rank	Key	Corr.	Rank	Key	Corr.
1	10	0.133	33	6	0.030
2	32	0.130	34	26	0.030
3	2	0.128	35	27	0.030
4	42	0.121	36	35	0.029
5	40	0.119	37	53	0.029
6	8	0.119	38	55	0.029
7	34	0.113	39	44	0.028
8	0	0.110	40	3	0.028
9	1	0.104	41	57	0.028
10	5	0.096	42	50	0.028
11	4	0.095	43	45	0.028
12	17	0.095	44	37	0.027
13	16	0.090	45	41	0.027
14	21	0.089	46	12	0.026
15	20	0.089	47	46	0.026
16	31	0.045	48	49	0.026
17	60	0.036	49	33	0.026
18	61	0.035	50	54	0.026
19	15	0.035	51	47	0.026
20	23	0.034	52	58	0.026
21	11	0.033	53	48	0.026
22	19	0.033	54	62	0.026
23	22	0.033	55	13	0.025
24	39	0.033	56	28	0.025
25	7	0.033	57	24	0.025
26	43	0.032	58	25	0.023
27	18	0.032	59	59	0.023
28	56	0.031	60	51	0.023
29	14	0.030	61	38	0.023
30	30	0.030	62	63	0.022
31	36	0.030	63	9	0.022
32	52	0.030	64	29	0.022

Verify the prediction

Which group does these key candidates correspond to ?

$\mathcal{G}[0]$

$\mathcal{G}[1]$ ✗

$\mathcal{G}[2]$ ✗

...

$\mathcal{G}[63]$ ✗

Rank	Key	Corr.	Rank	Key	Corr.
1	10	0.133	33	6	0.030
2	32	0.130	34	26	0.030
3	2	0.128	35	27	0.030
4	42	0.121	36	35	0.029
5	40	0.119	37	53	0.029
6	8	0.119	38	55	0.029
7	34	0.113	39	44	0.028
8	0	0.110	40	3	0.028
9	1	0.104	41	57	0.028
10	5	0.096	42	50	0.028
11	4	0.095	43	45	0.028
12	17	0.095	44	37	0.027
13	16	0.090	45	41	0.027
14	21	0.089	46	12	0.026
15	20	0.089	47	46	0.026
16	31	0.045	48	49	0.026
17	60	0.036	49	33	0.026
18	61	0.035	50	54	0.026
19	15	0.035	51	47	0.026
20	23	0.034	52	58	0.026
21	11	0.033	53	48	0.026
22	19	0.033	54	62	0.026
23	22	0.033	55	13	0.025
24	39	0.033	56	28	0.025
25	7	0.033	57	24	0.025
26	43	0.032	58	25	0.023
27	18	0.032	59	59	0.023
28	56	0.031	60	51	0.023
29	14	0.030	61	38	0.023
30	30	0.030	62	63	0.022
31	36	0.030	63	9	0.022
32	52	0.030	64	29	0.022

Verify the prediction

Which group does these key candidates correspond to ?

$\mathcal{G}[0]$ ✅

$\mathcal{G}[1]$ ❌

$\mathcal{G}[2]$ ❌

...

$\mathcal{G}[63]$ ❌

Rank	Key	Corr.	Rank	Key	Corr.
1	10	0.133	33	6	0.030
2	32	0.130	34	26	0.030
3	2	0.128	35	27	0.030
4	42	0.121	36	35	0.029
5	40	0.119	37	53	0.029
6	8	0.119	38	55	0.029
7	34	0.113	39	44	0.028
8	0	0.110	40	3	0.028
9	1	0.104	41	57	0.028
10	5	0.096	42	50	0.028
11	4	0.095	43	45	0.028
12	17	0.095	44	37	0.027
13	16	0.090	45	41	0.027
14	21	0.089	46	12	0.026
15	20	0.089	47	46	0.026
16	31	0.045	48	49	0.026
17	60	0.036	49	33	0.026
18	61	0.035	50	54	0.026
19	15	0.035	51	47	0.026
20	23	0.034	52	58	0.026
21	11	0.033	53	48	0.026
22	19	0.033	54	62	0.026
23	22	0.033	55	13	0.025
24	39	0.033	56	28	0.025
25	7	0.033	57	24	0.025
26	43	0.032	58	25	0.023
27	18	0.032	59	59	0.023
28	56	0.031	60	51	0.023
29	14	0.030	61	38	0.023
30	30	0.030	62	63	0.022
31	36	0.030	63	9	0.022
32	52	0.030	64	29	0.022

Verify the prediction

Which group does these key candidates correspond to ?

$\mathcal{G}[0]$ ✅ → correct key is 0

$\mathcal{G}[1]$ ❌

$\mathcal{G}[2]$ ❌

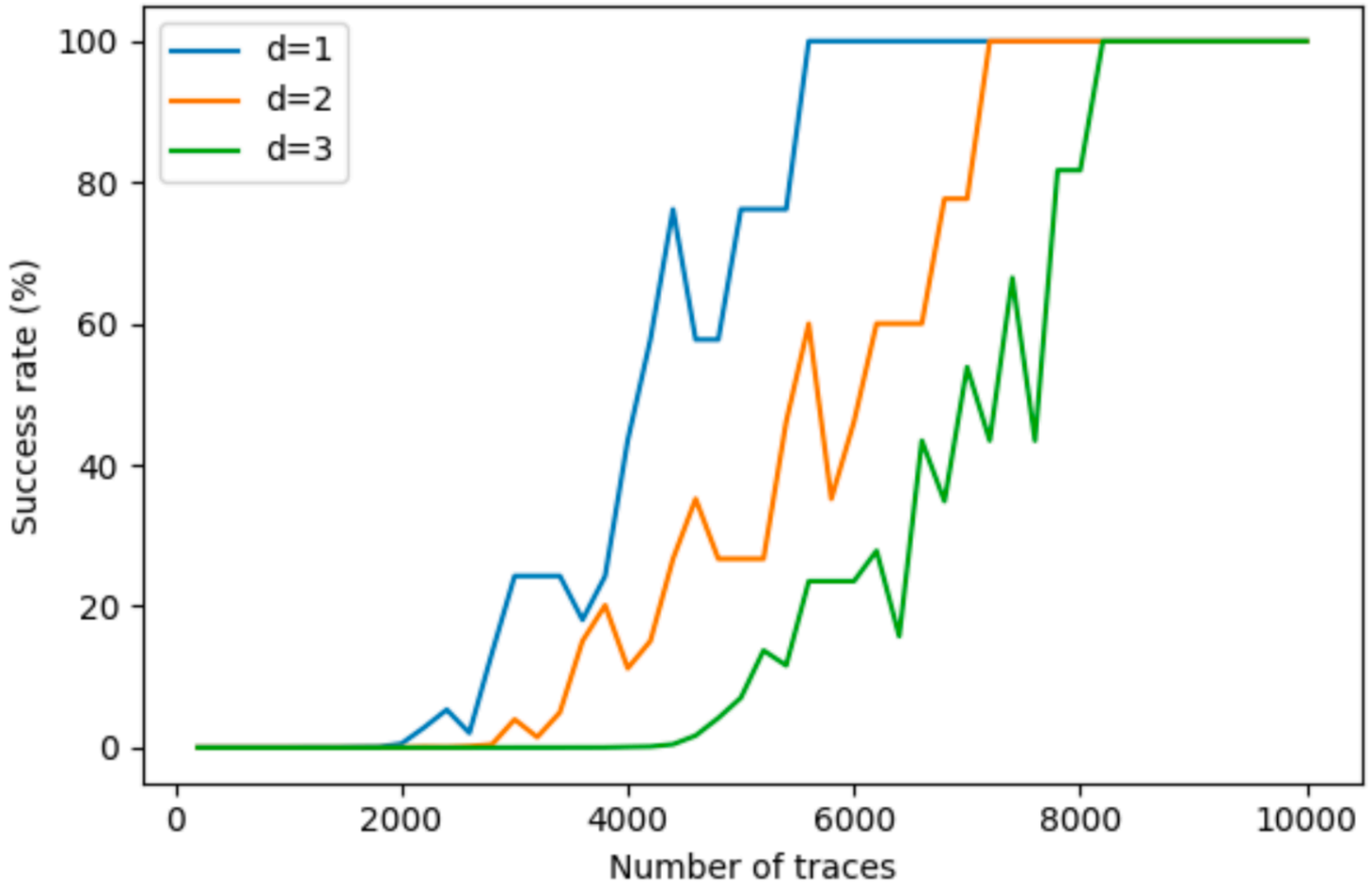
...

$\mathcal{G}[63]$ ❌

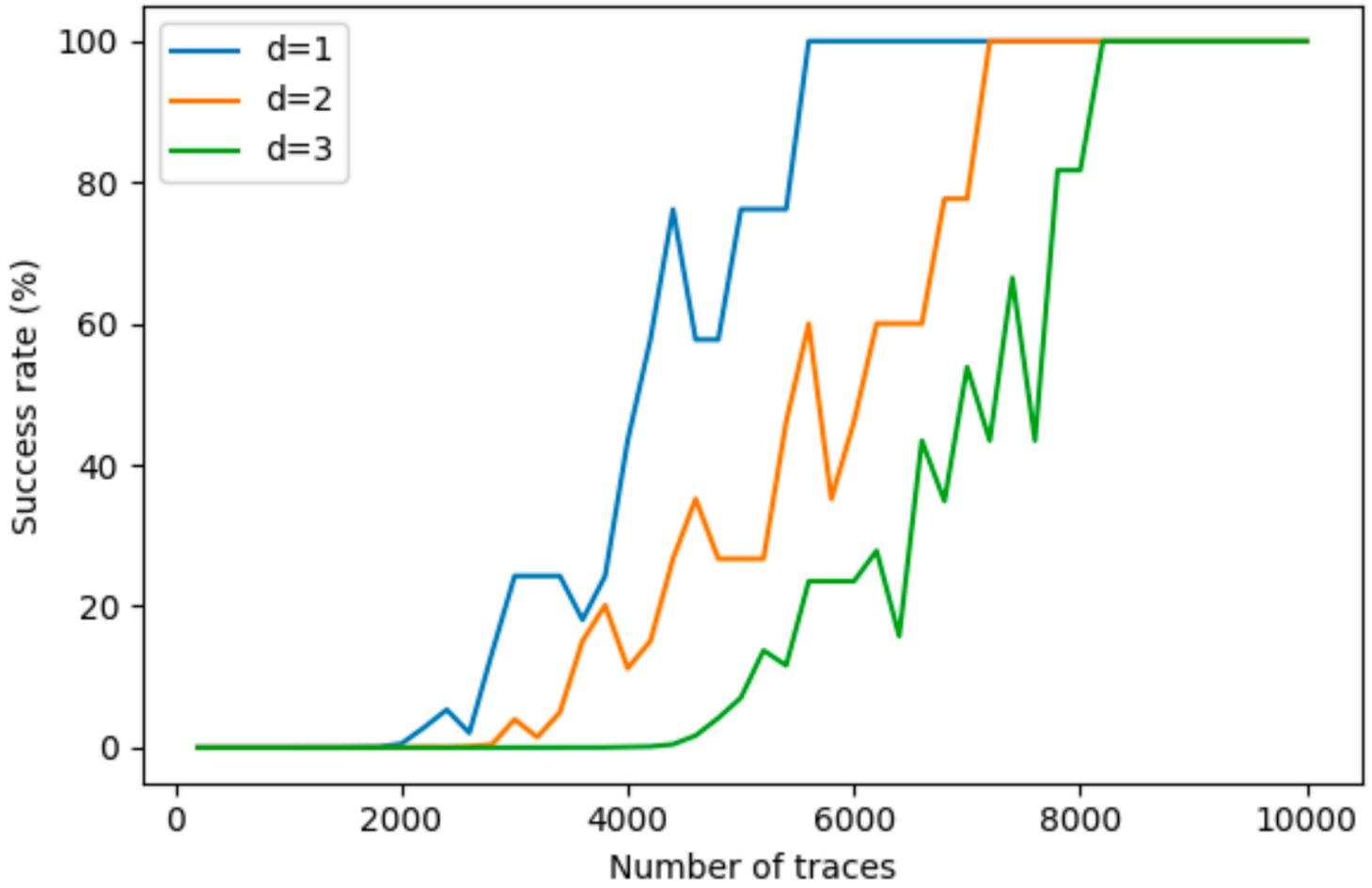
Rank	Key	Corr.	Rank	Key	Corr.
1	10	0.133	33	6	0.030
2	32	0.130	34	26	0.030
3	2	0.128	35	27	0.030
4	42	0.121	36	35	0.029
5	40	0.119	37	53	0.029
6	8	0.119	38	55	0.029
7	34	0.113	39	44	0.028
8	0	0.110	40	3	0.028
9	1	0.104	41	57	0.028
10	5	0.096	42	50	0.028
11	4	0.095	43	45	0.028
12	17	0.095	44	37	0.027
13	16	0.090	45	41	0.027
14	21	0.089	46	12	0.026
15	20	0.089	47	46	0.026
16	31	0.045	48	49	0.026
17	60	0.036	49	33	0.026
18	61	0.035	50	54	0.026
19	15	0.035	51	47	0.026
20	23	0.034	52	58	0.026
21	11	0.033	53	48	0.026
22	19	0.033	54	62	0.026
23	22	0.033	55	13	0.025
24	39	0.033	56	28	0.025
25	7	0.033	57	24	0.025
26	43	0.032	58	25	0.023
27	18	0.032	59	59	0.023
28	56	0.031	60	51	0.023
29	14	0.030	61	38	0.023
30	30	0.030	62	63	0.022
31	36	0.030	63	9	0.022
32	52	0.030	64	29	0.022

Results of full key recovery

Results of full key recovery

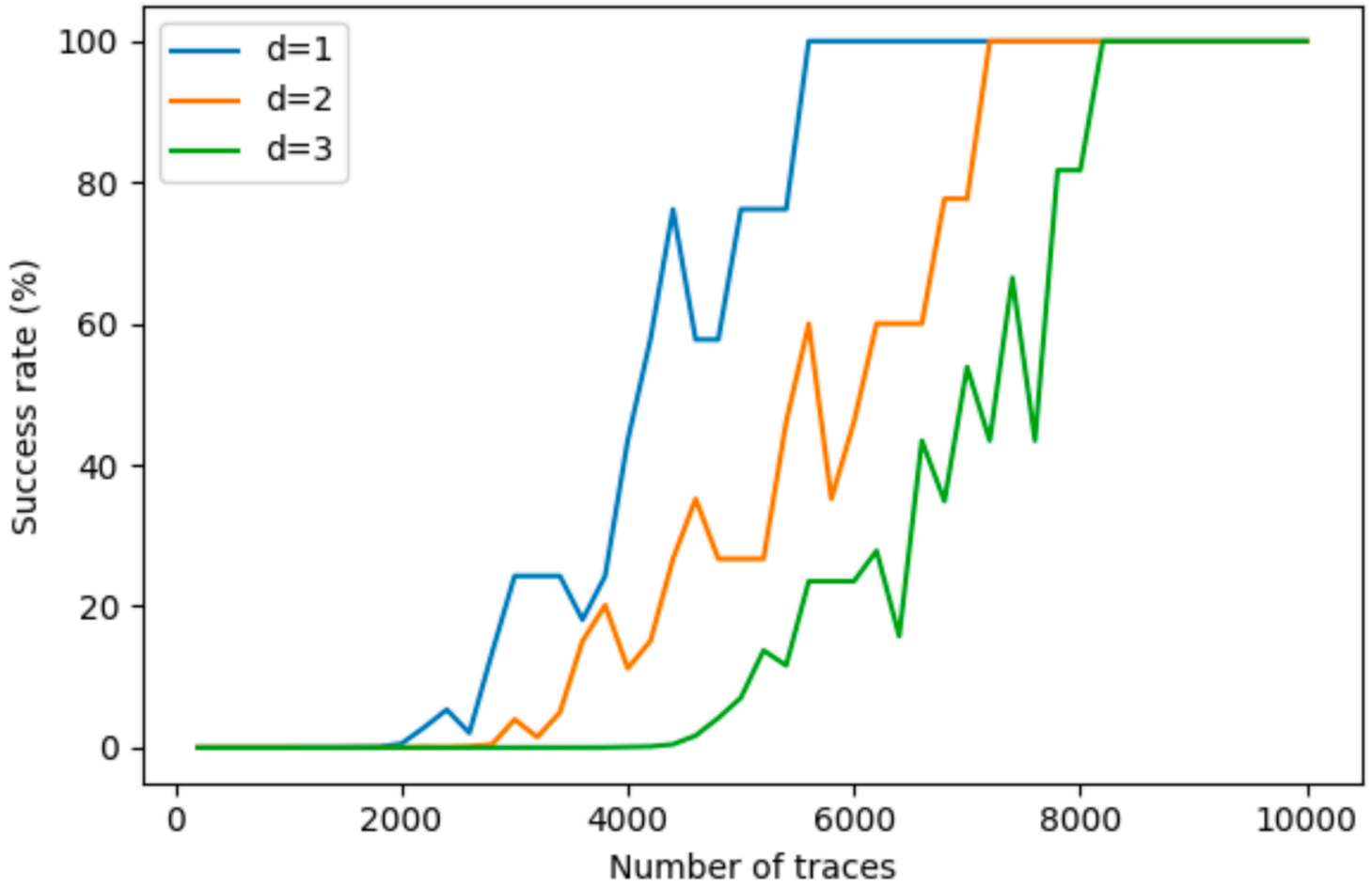


Results of full key recovery



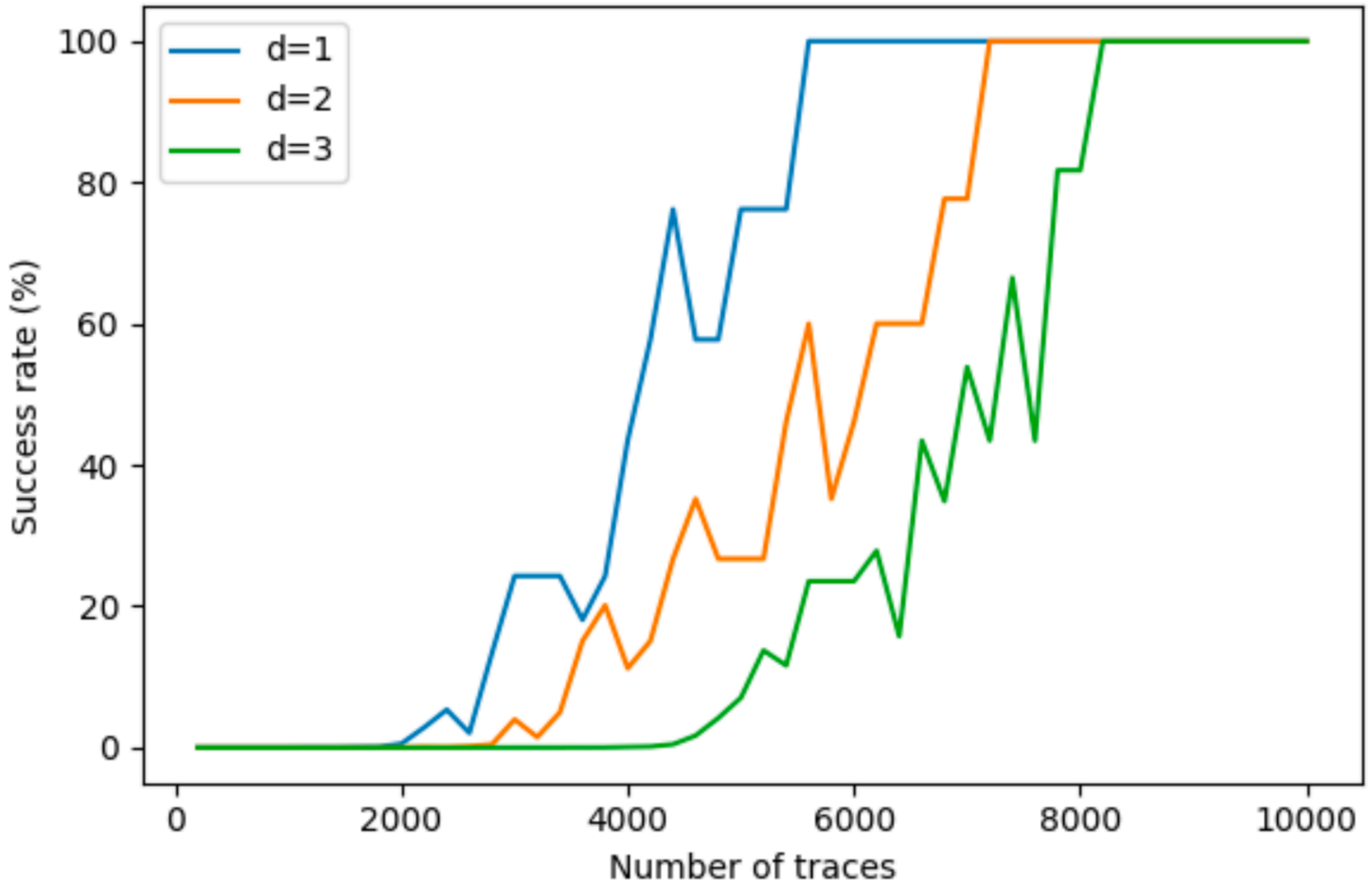
- Looks better

Results of full key recovery



- Looks better
- But still not as efficient as 1 bit

Results of full key recovery



- Looks better
- But still not as efficient as 1 bit
  → future work

Summary

CPA attack on Ascon

CPA attack on Ascon

- Extend hypothetical power consumption to multi-bit scenario

CPA attack on Ascon

- Extend hypothetical power consumption to multi-bit scenario
- Found the root cause of poor performance

CPA attack on Ascon

- Extend hypothetical power consumption to multi-bit scenario
- Found the root cause of poor performance
- Proposed approach for key recovery

Correlation Power Analysis on Ascon with Multi-bit Selection Function

Viet-Sang Nguyen

joint work with Vincent Grosso and Pierre-Louis Cayrel

SECRYPT

Bilbao, 11 June, 2025

UNIVERSITÉ DE LYON

UNIVERSITÉ JEAN MONNET SAINT-ÉTIENNE

Laboratoire Hubert Curien
UMR ▪ CNRS ▪ 5516 ▪ Saint-Étienne

anr
PROPHY ANR-22-CE39-0008-01