Correlation Power Analysis on Ascon with Multi-bit Selection Function

Viet-Sang Nguyen

joint work with Vincent Grosso and Pierre-Louis Cayrel

Bilbao, 11 June, 2025







SECRYPT



Viet-Sang Nguyen

viet.sang.nguyen@univ-st-etienne.fr









Viet-Sang Nguyen

viet.sang.nguyen@univ-st-etienne.fr

Lightweight cryptography competition

CPA on Ascon with Multi-bit Selection Function





2018





Viet-Sang Nguyen

viet.sang.nguyen@univ-st-etienne.fr

Lightweight cryptography competition



2023 Selected Ascon

CPA on Ascon with Multi-bit Selection Function







2018



2023

Viet-Sang Nguyen

viet.sang.nguyen@univ-st-etienne.fr

Lightweight cryptography competition



Selected Ascon

CPA on Ascon with Multi-bit Selection Function











Viet-Sang Nguyen

viet.sang.nguyen@univ-st-etienne.fr

2023



Lightweight cryptography competition



Selected Ascon

Possible attacks

Secure implementations

CPA on Ascon with Multi-bit Selection Function



In this talk



Viet-Sang Nguyen

viet.sang.nguyen@univ-st-etienne.fr

Possible attacks





In this talk



Viet-Sang Nguyen

viet.sang.nguyen@univ-st-etienne.fr

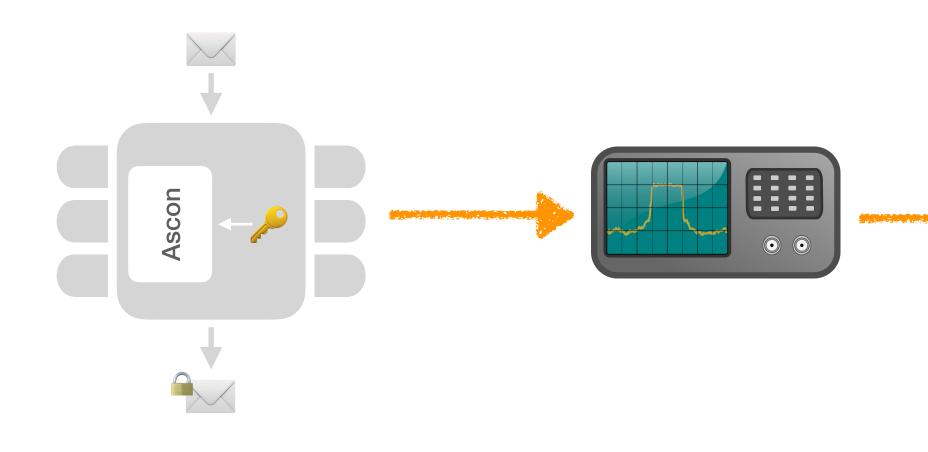
Possible attacks

Correlation Power Analysis (CPA) attack





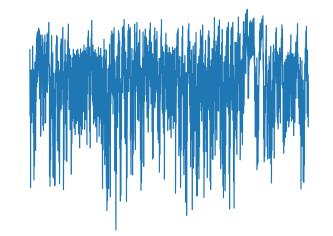
In this talk





Viet-Sang Nguyen

viet.sang.nguyen@univ-st-etienne.fr





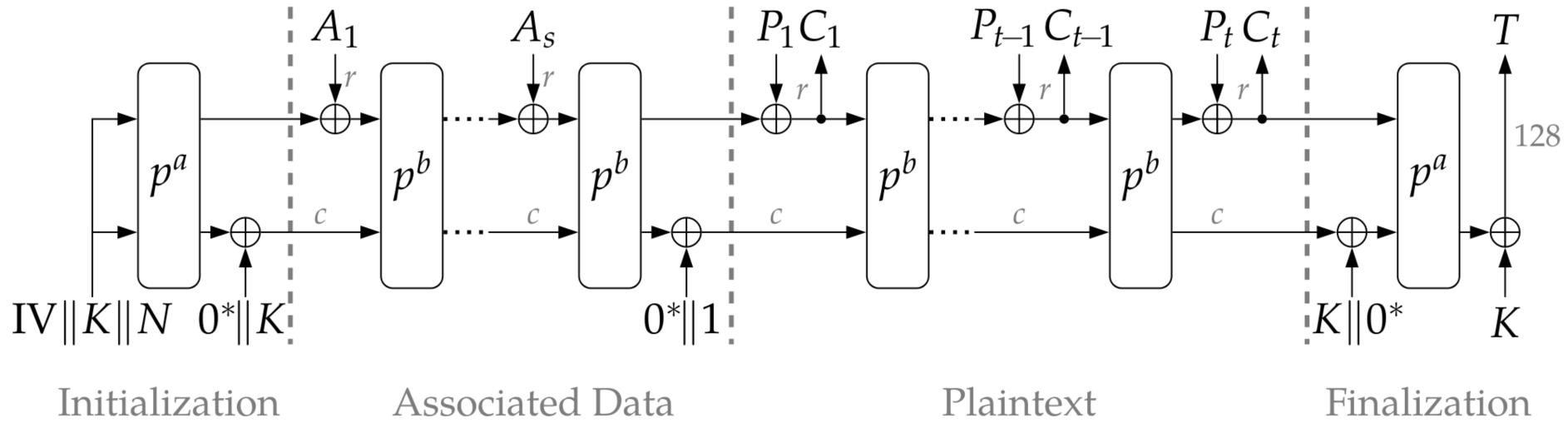
Possible attacks

Correlation Power Analysis (CPA) attack









Viet-Sang Nguyen

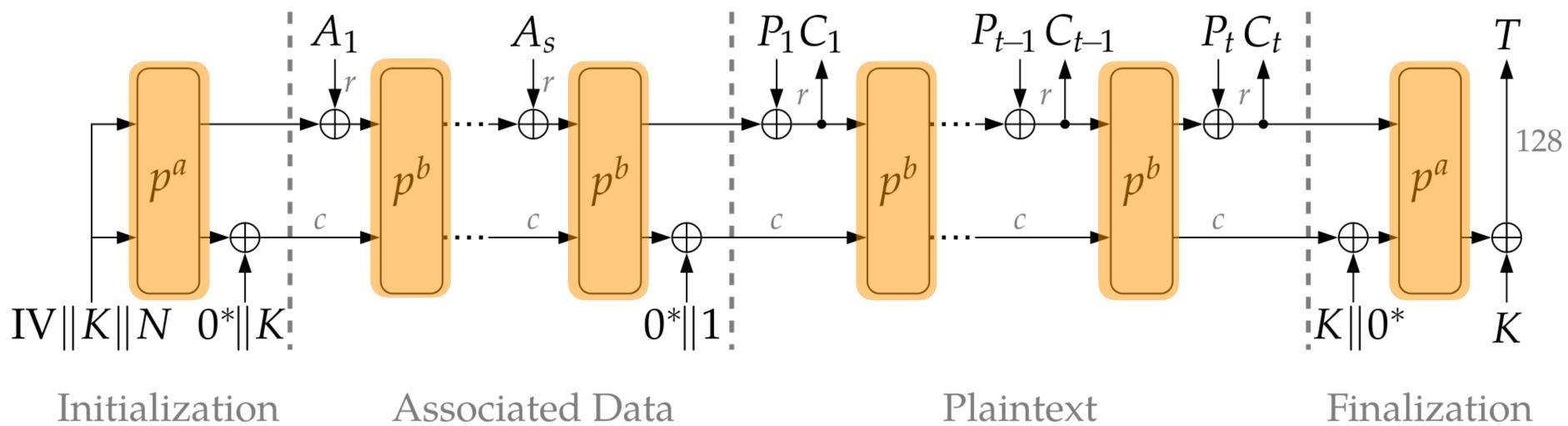
viet.sang.nguyen@univ-st-etienne.fr

Plaintext

Finalization



Permutation blocks



Viet-Sang Nguyen

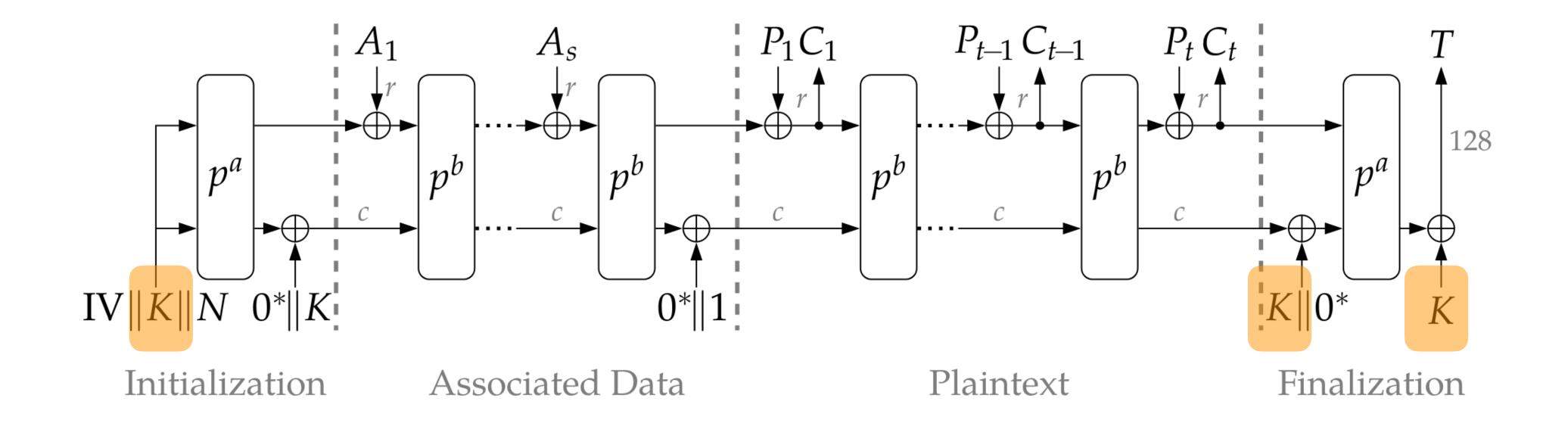
viet.sang.nguyen@univ-st-etienne.fr

▶ p^a : 12 permutation rounds (a = 12)

▶ p^b : 8 permutation rounds (b = 8)



Key (128 bits)

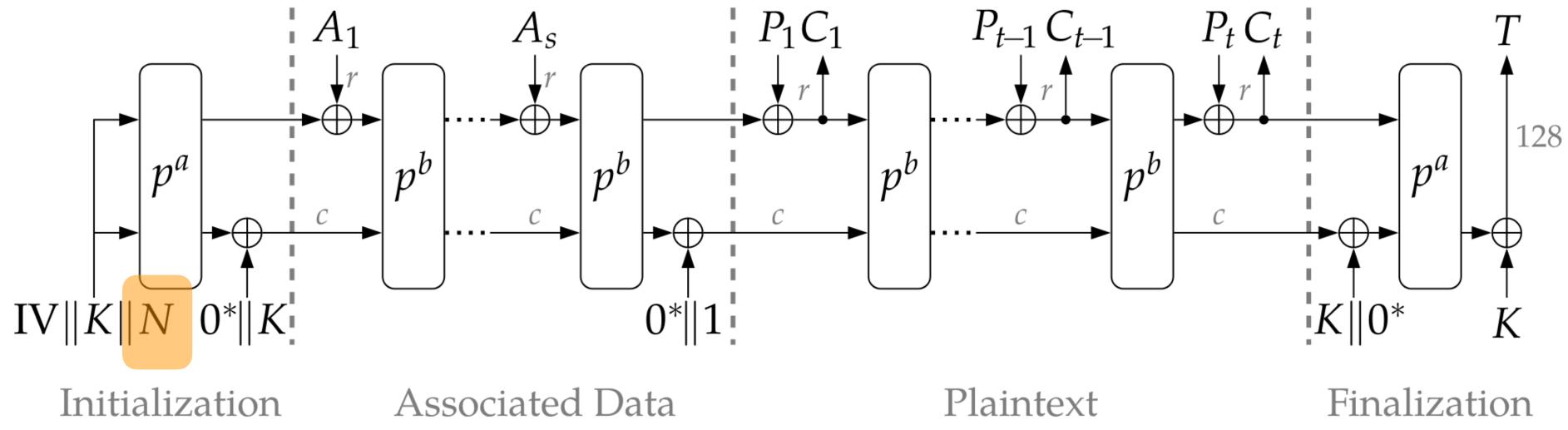




viet.sang.nguyen@univ-st-etienne.fr

CPA on Ascon with Multi-bit Selection Function

Nonce (128 bits)

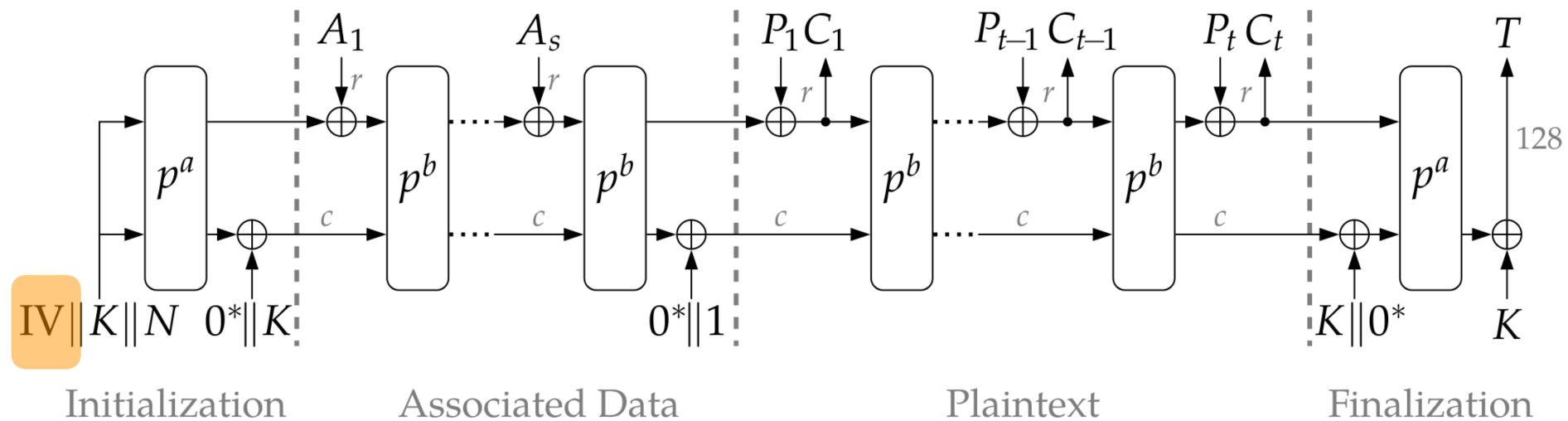


Viet-Sang Nguyen

viet.sang.nguyen@univ-st-etienne.fr



Initialization vector



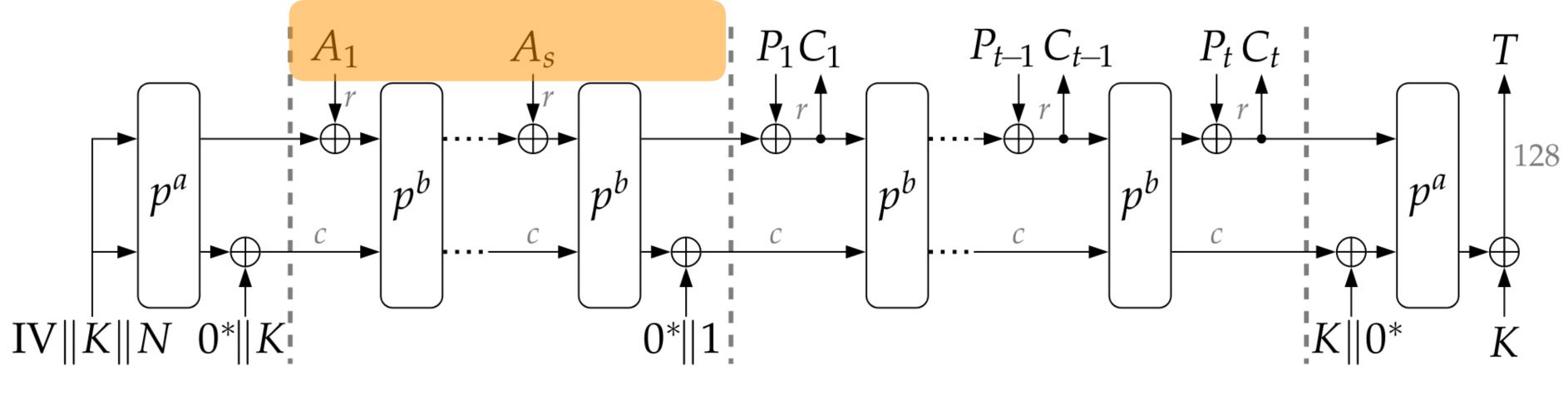
Viet-Sang Nguyen

viet.sang.nguyen@univ-st-etienne.fr

Finalization



Associated data



Initialization

Associated Data

Viet-Sang Nguyen

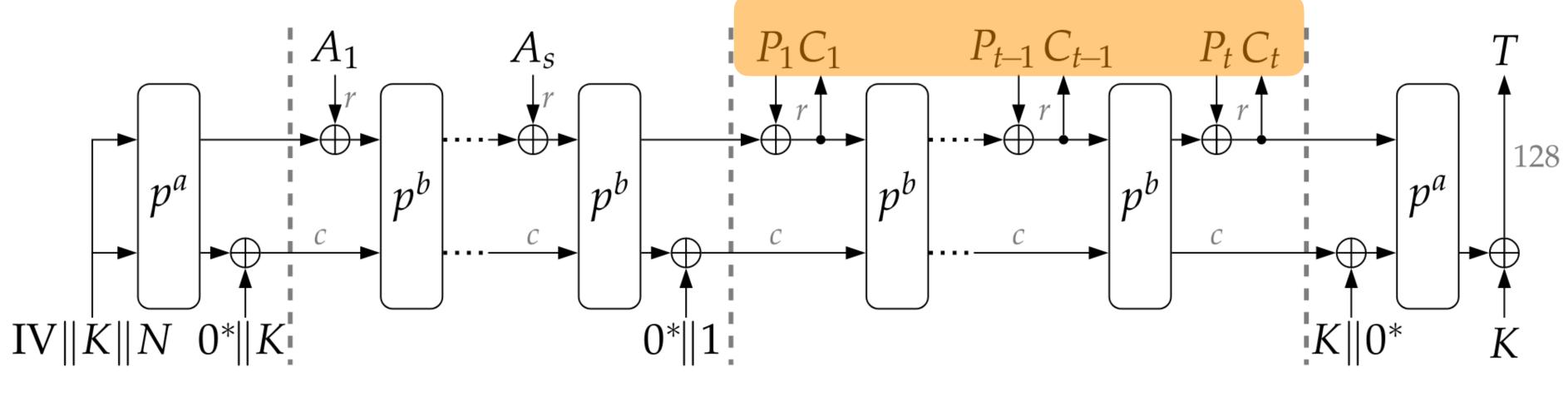
viet.sang.nguyen@univ-st-etienne.fr

Plaintext

Finalization



Plaintext / Ciphertext



Initialization

Associated Data

Viet-Sang Nguyen

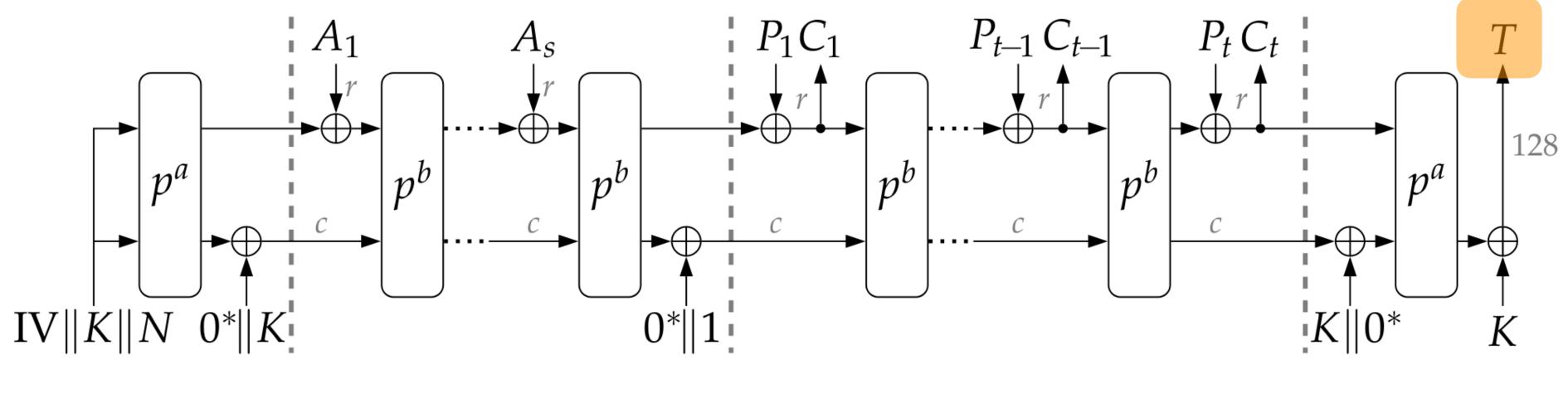
viet.sang.nguyen@univ-st-etienne.fr

Plaintext

Finalization

CPA on Ascon with Multi-bit Selection Function

Verification Tag



Initialization

Associated Data

Viet-Sang Nguyen

viet.sang.nguyen@univ-st-etienne.fr

Plaintext

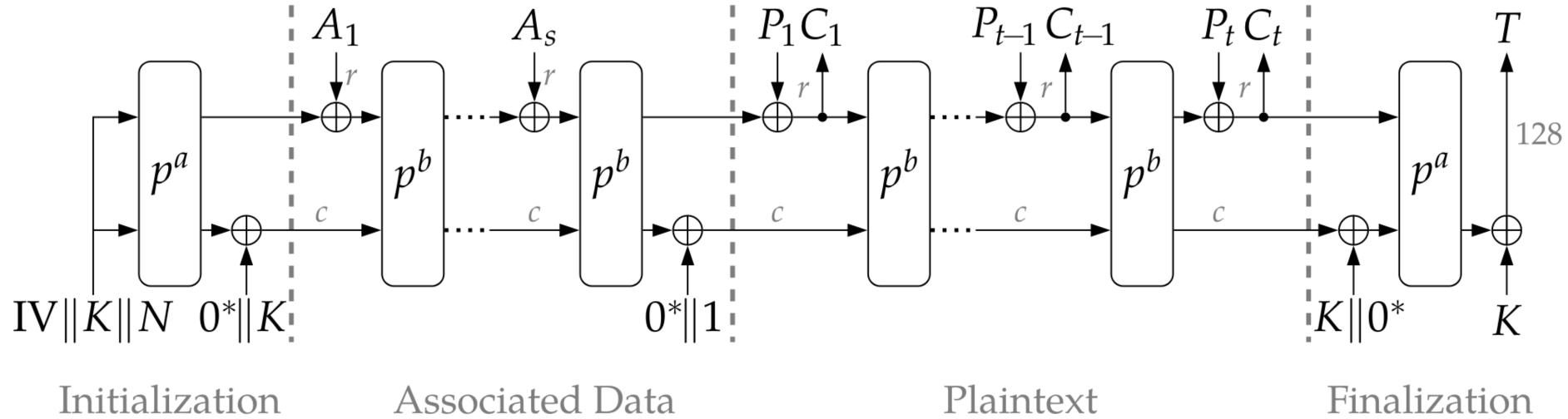
Finalization

CPA on Ascon with Multi-bit Selection Function



Correlation Power Analysis (CPA) on Ascon





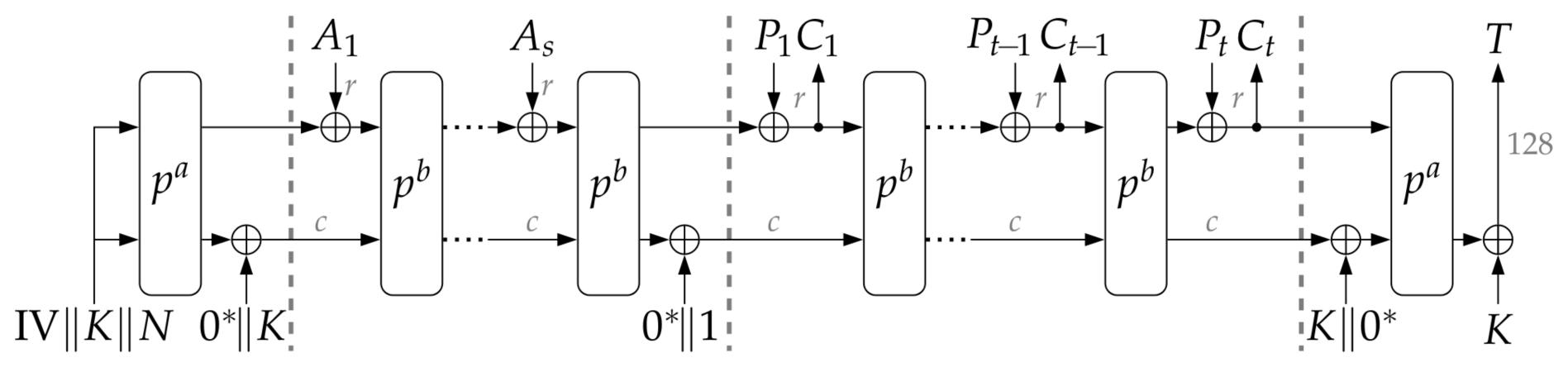
Viet-Sang Nguyen

viet.sang.nguyen@univ-st-etienne.fr

Plaintext

Finalization





Initialization

Associated Data

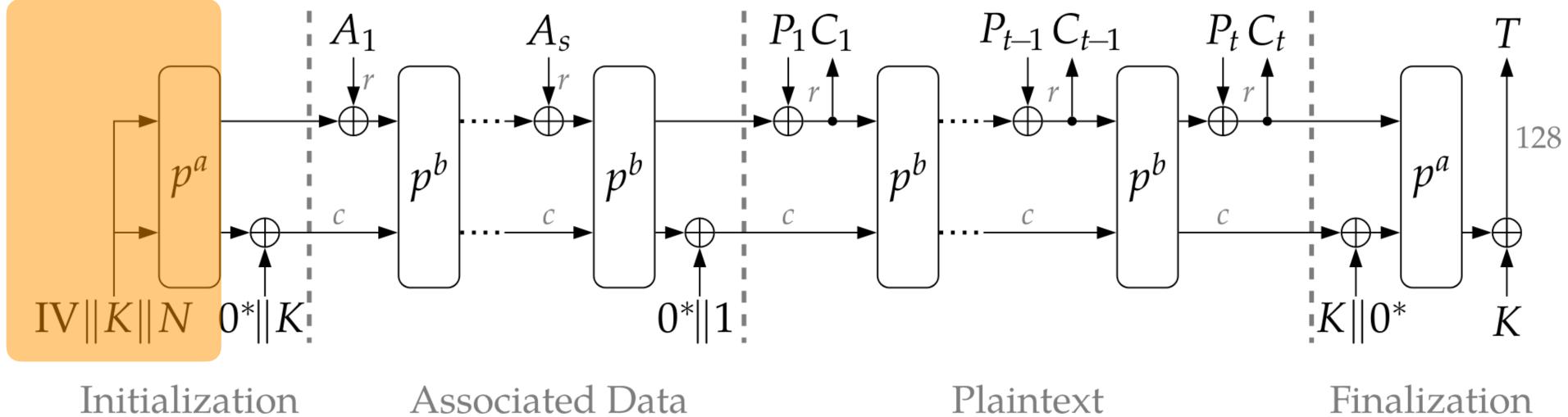
Viet-Sang Nguyen

viet.sang.nguyen@univ-st-etienne.fr

Plaintext

Finalization





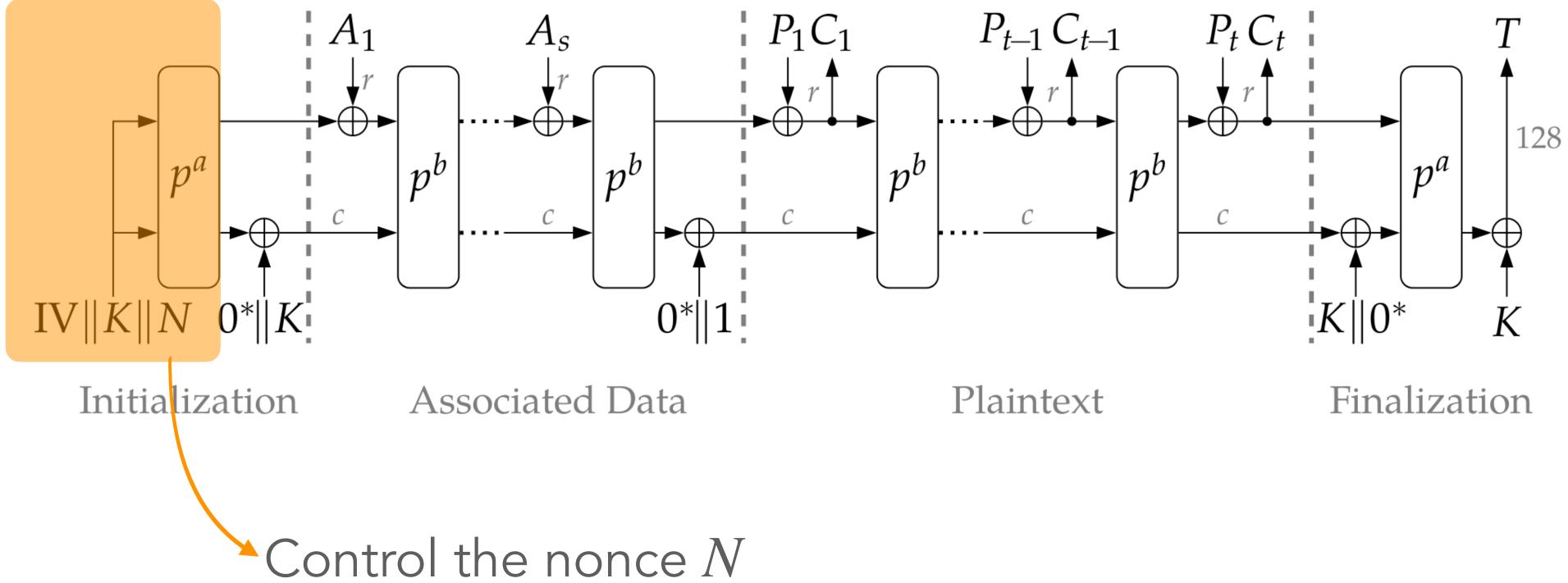
Viet-Sang Nguyen

viet.sang.nguyen@univ-st-etienne.fr

Plaintext

Finalization

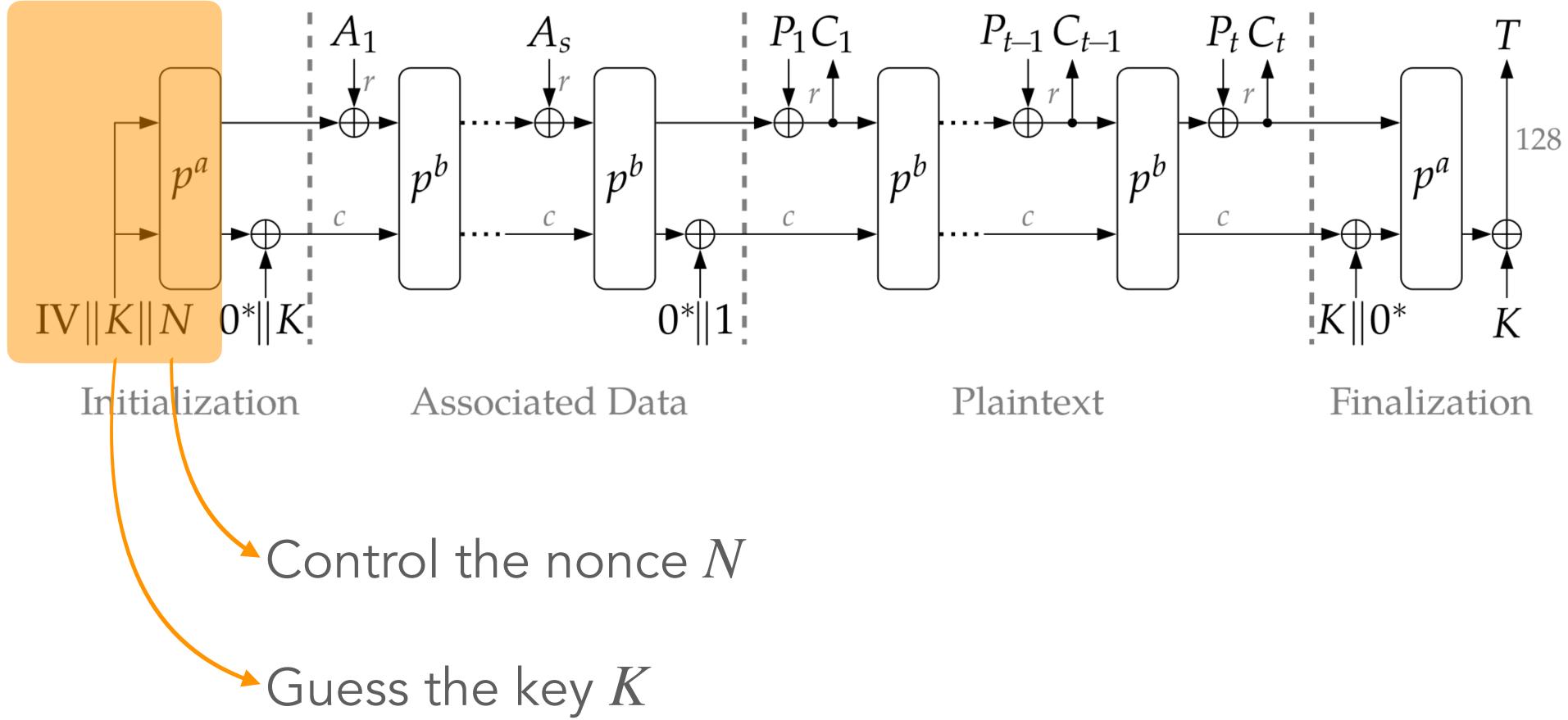




Viet-Sang Nguyen

viet.sang.nguyen@univ-st-etienne.fr





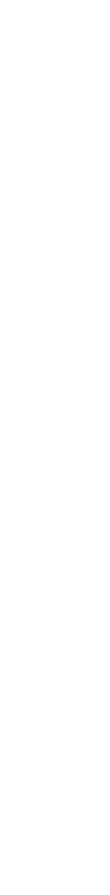
Viet-Sang Nguyen

viet.sang.nguyen@univ-st-etienne.fr



Viet-Sang Nguyen

viet.sang.nguyen@univ-st-etienne.fr

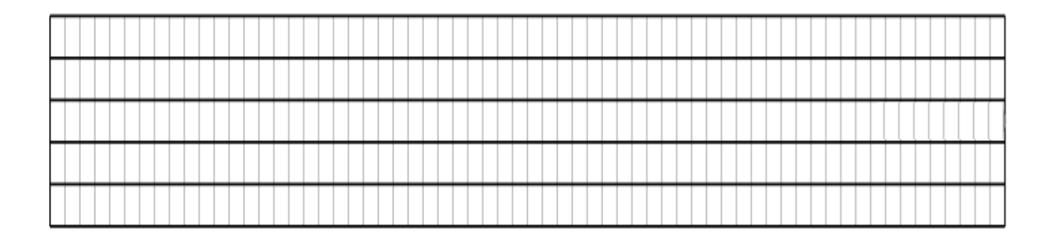


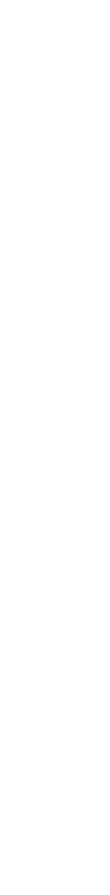


On 320-bit state = 5×64 -bit words

Viet-Sang Nguyen

viet.sang.nguyen@univ-st-etienne.fr





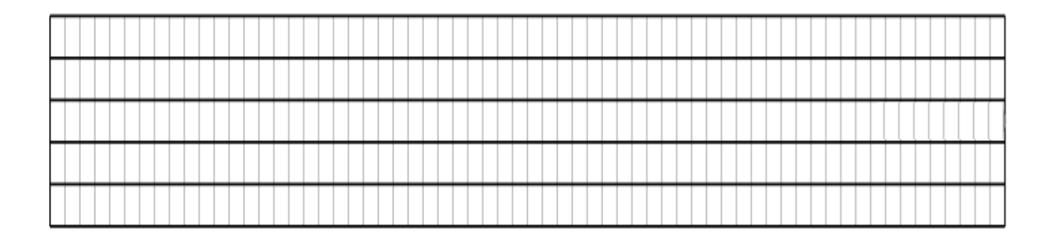


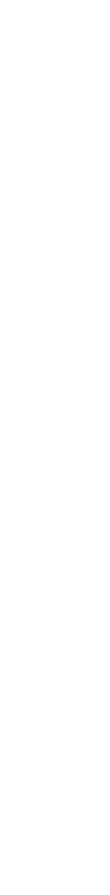
On 320-bit state = 5×64 -bit words

Input of the first round:



viet.sang.nguyen@univ-st-etienne.fr



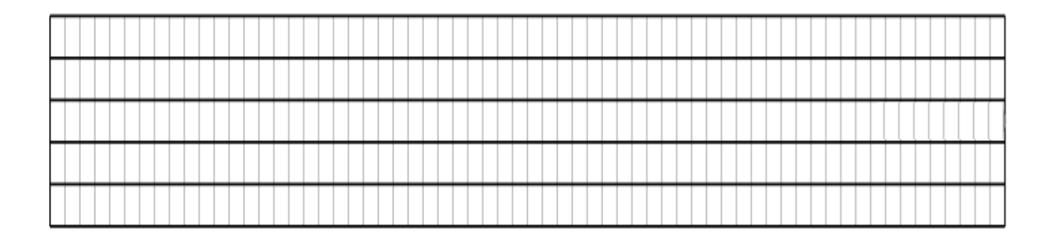


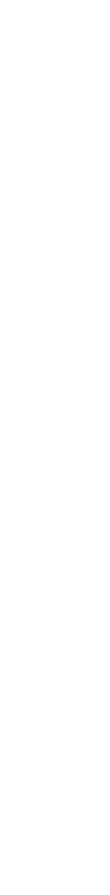


On 320-bit state = 5×64 -bit words

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



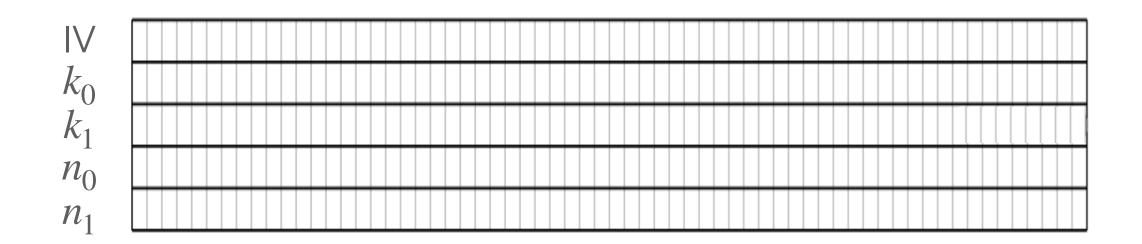


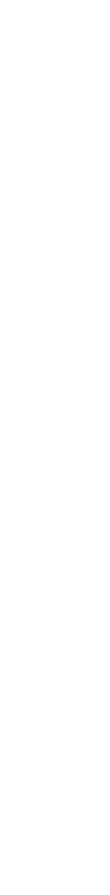


On 320-bit state = 5×64 -bit words

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



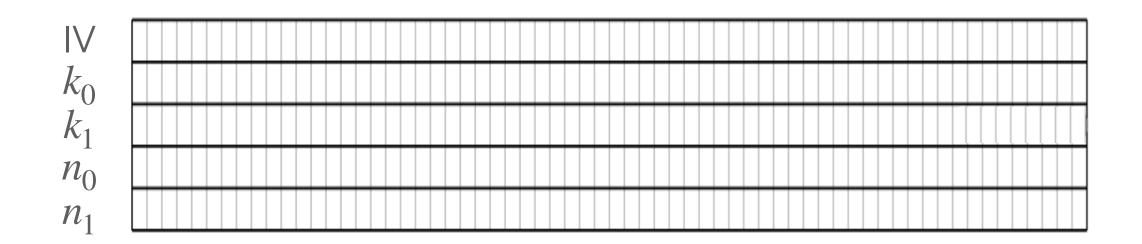


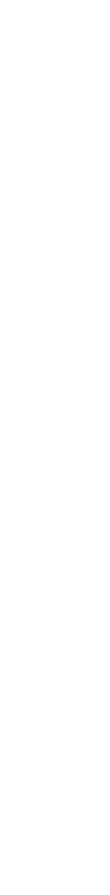


On 320-bit state = 5×64 -bit words

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



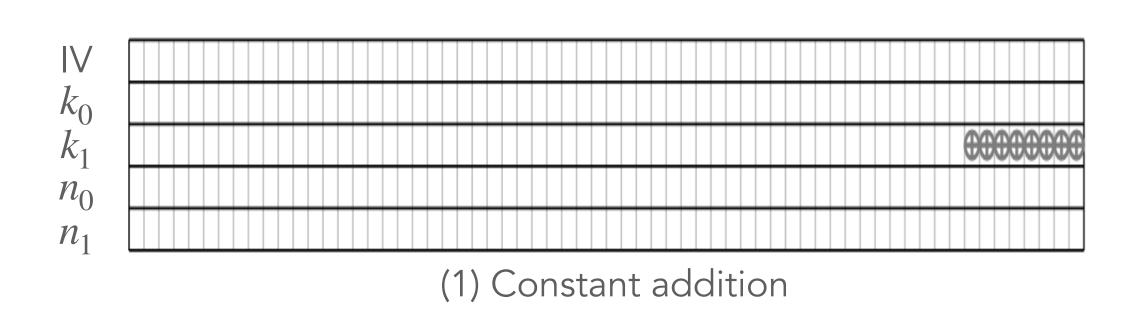




On 320-bit state = 5×64 -bit words

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

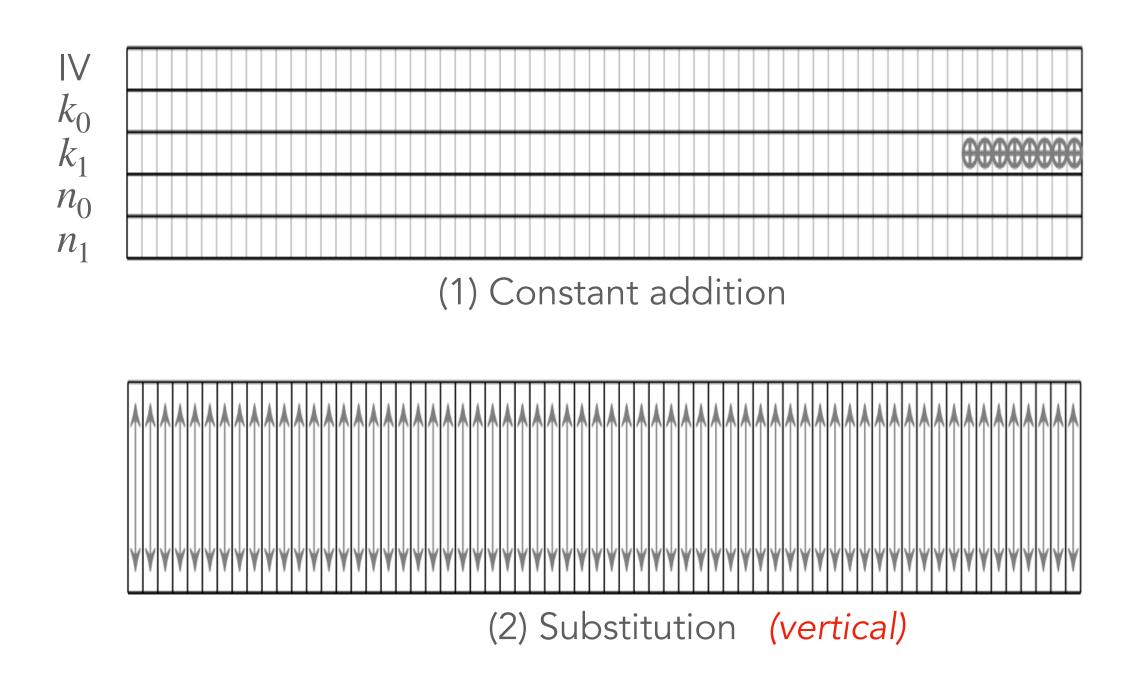




On 320-bit state = 5×64 -bit words

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

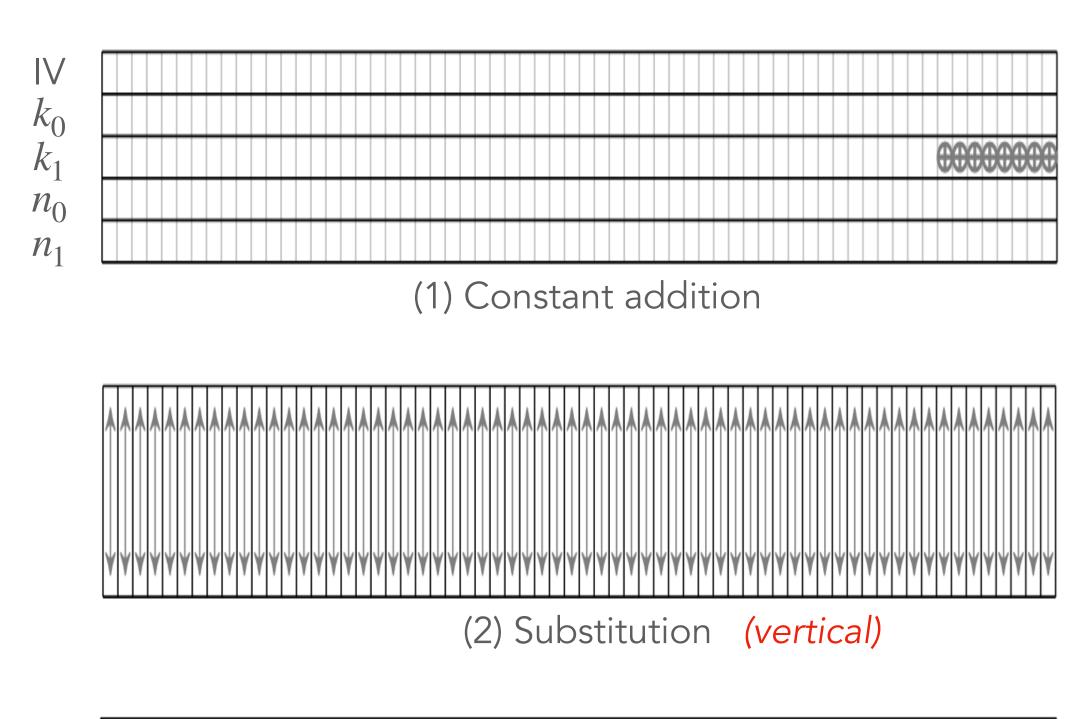


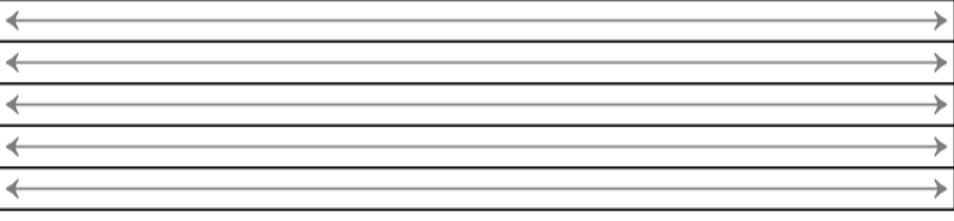


On 320-bit state = 5×64 -bit words

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





(3) Linear diffusion (horizontal)

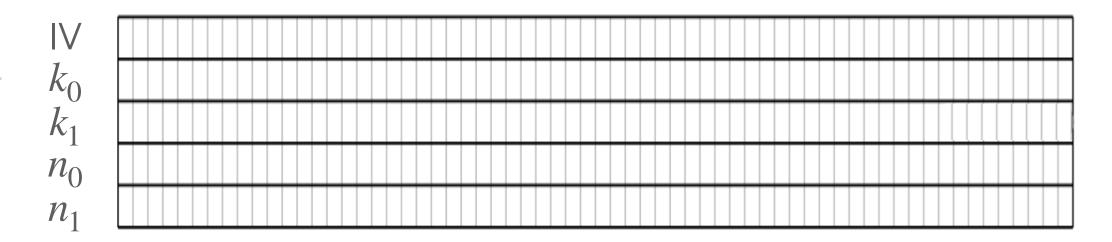


State changes in 1st round

Viet-Sang Nguyen

viet.sang.nguyen@univ-st-etienne.fr



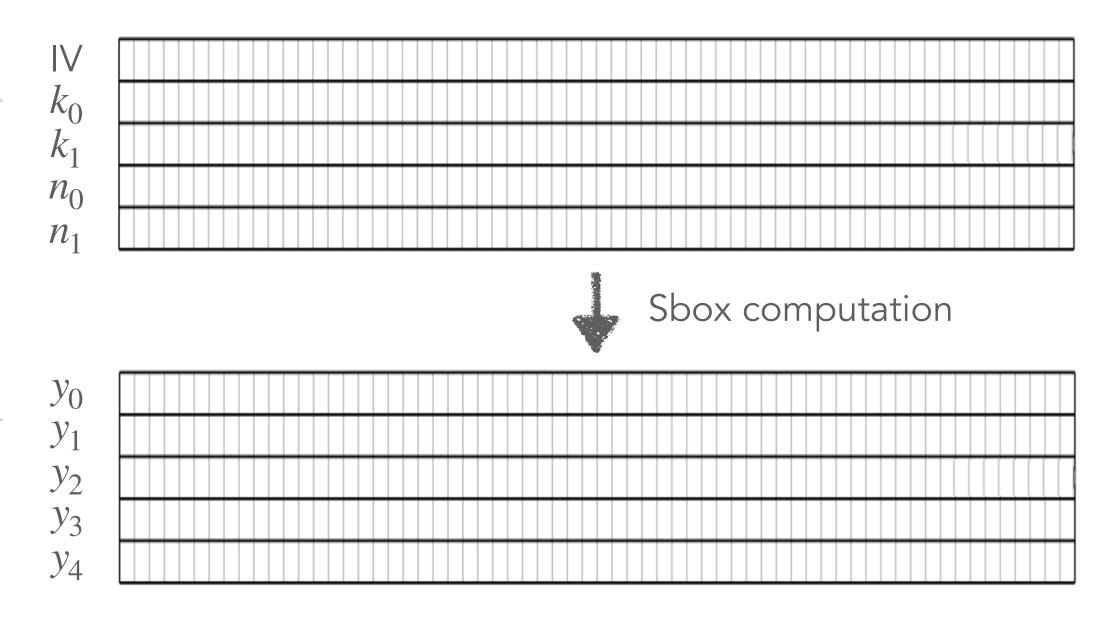


CPA on Ascon with Multi-bit Selection Function

State changes in 1st round

Viet-Sang Nguyen

viet.sang.nguyen@univ-st-etienne.fr

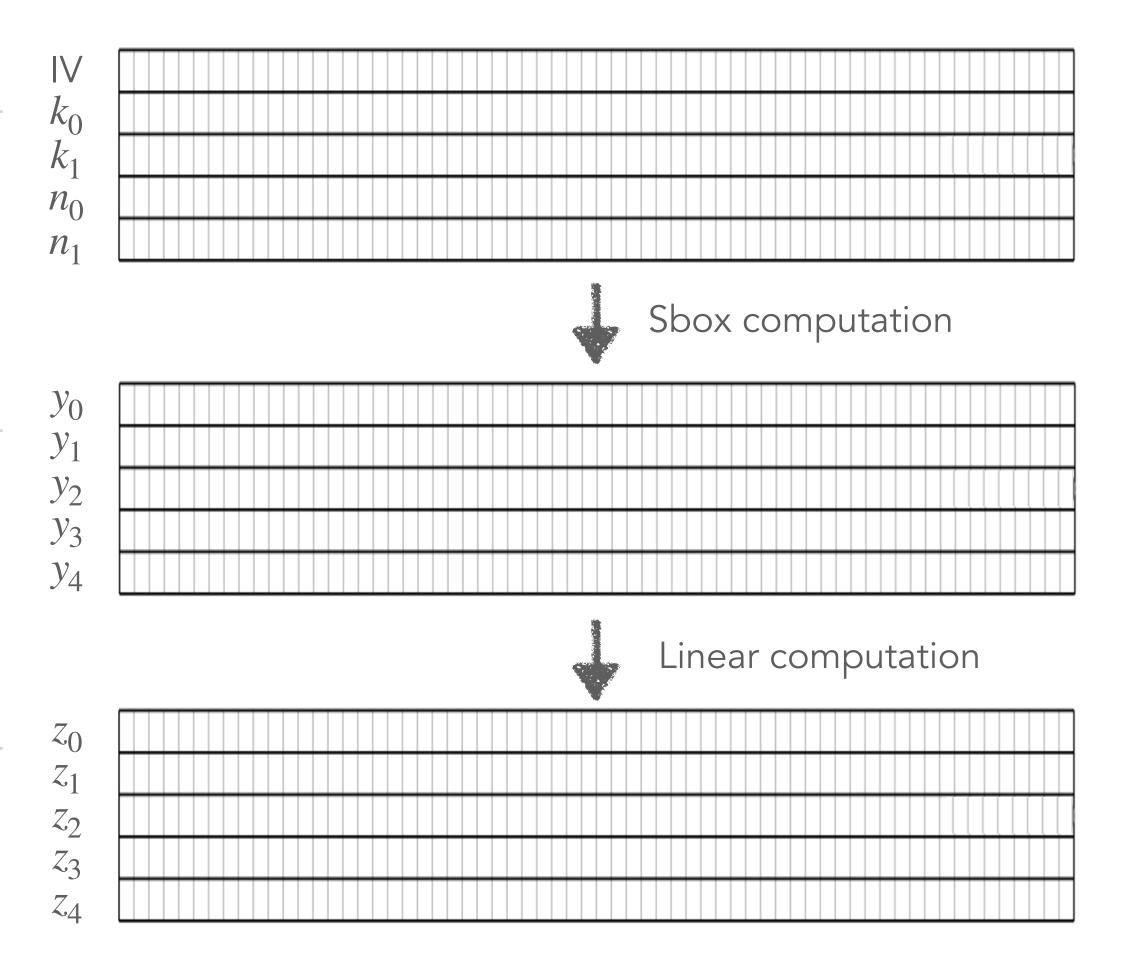


CPA on Ascon with Multi-bit Selection Function

State changes in 1st round

Viet-Sang Nguyen

viet.sang.nguyen@univ-st-etienne.fr

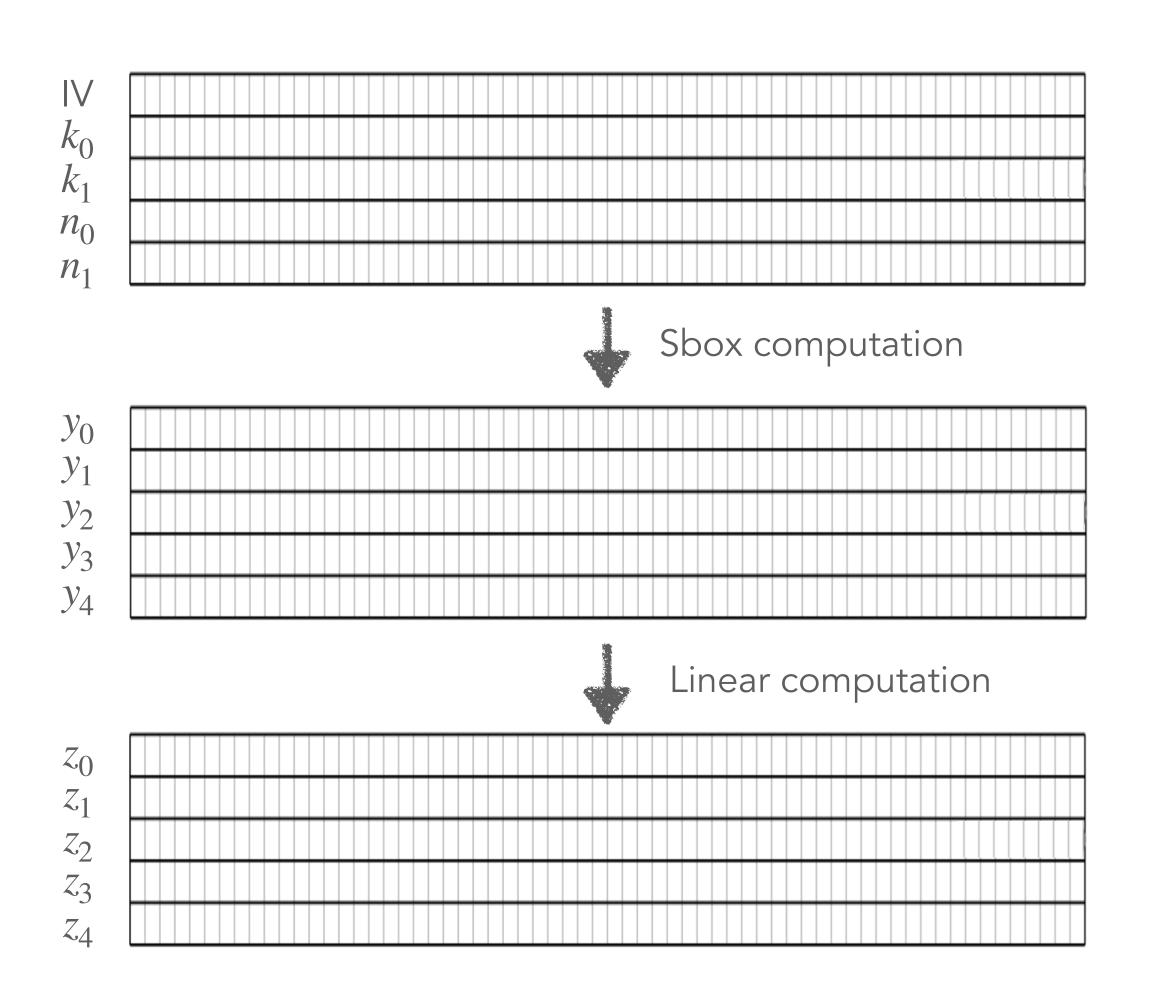


CPA on Ascon with Multi-bit Selection Function

Samwel and Daemen, 2018

Viet-Sang Nguyen

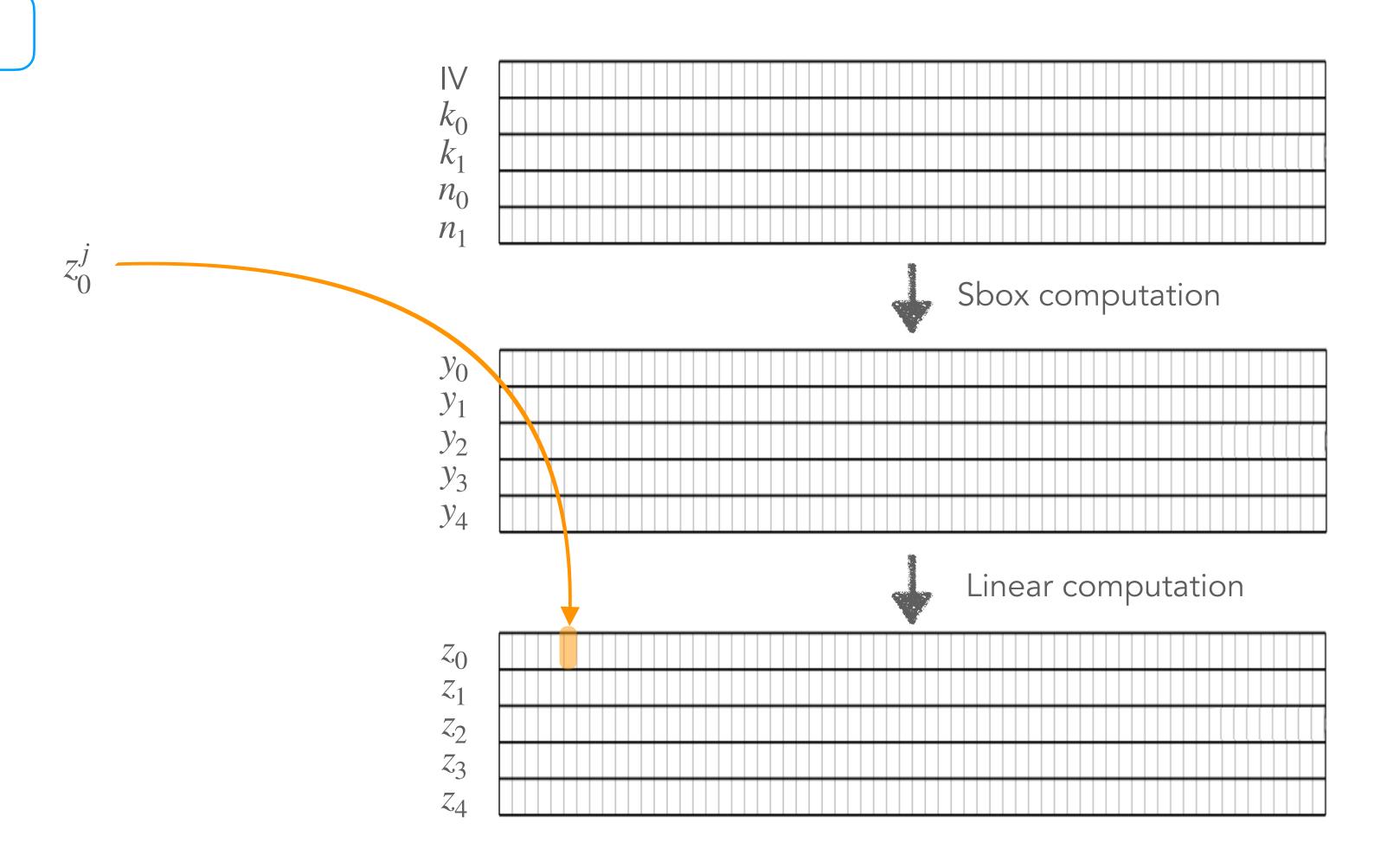
viet.sang.nguyen@univ-st-etienne.fr



CPA on Ascon with Multi-bit Selection Function



Samwel and Daemen, 2018



Viet-Sang Nguyen

viet.sang.nguyen@univ-st-etienne.fr

CPA on Ascon with Multi-bit Selection Function



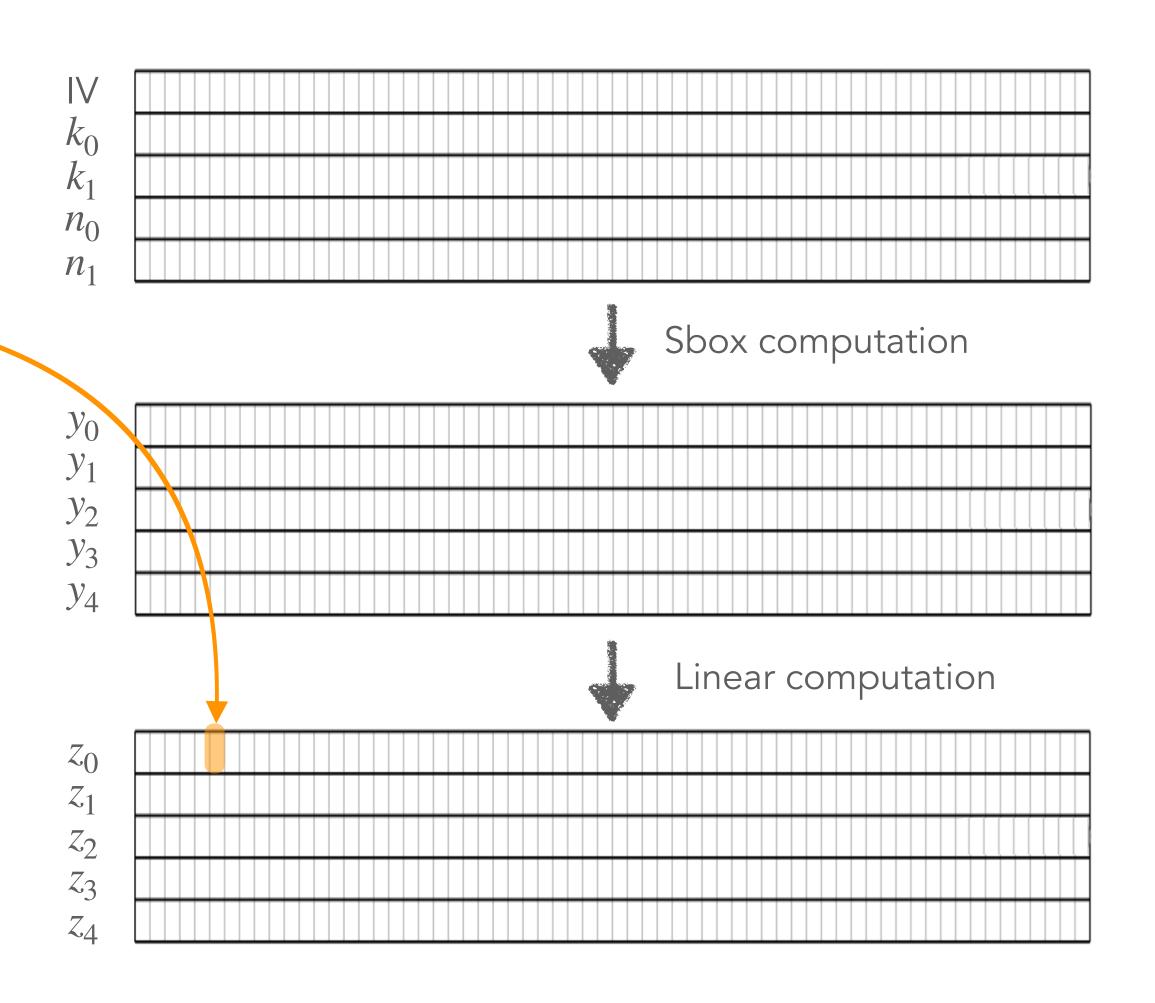
Samwel and Daemen, 2018

hypothetical power consumption

 7^{J} ~0

Viet-Sang Nguyen

viet.sang.nguyen@univ-st-etienne.fr



CPA on Ascon with Multi-bit Selection Function



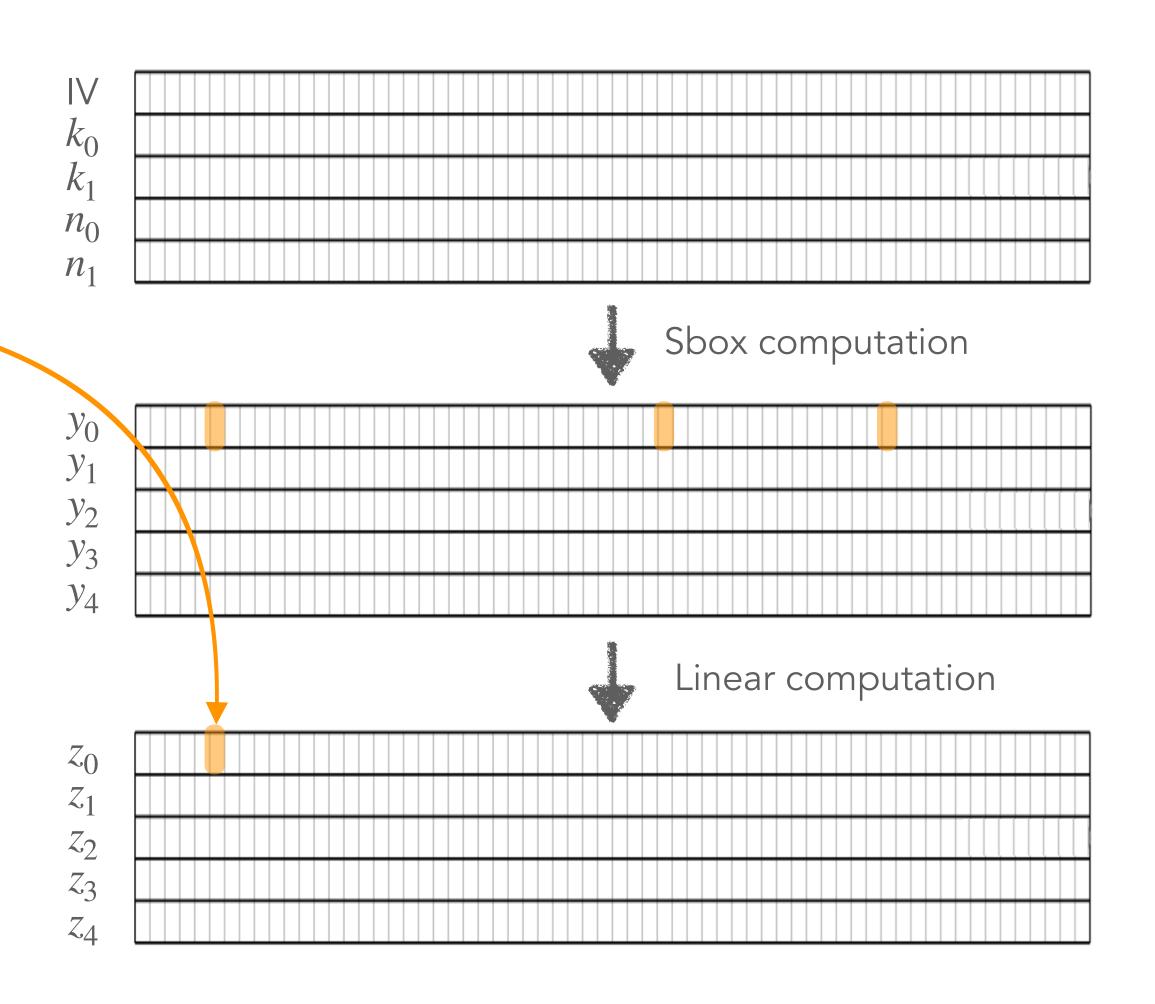
Samwel and Daemen, 2018

hypothetical power consumption

 7^{J} ~0

Viet-Sang Nguyen

viet.sang.nguyen@univ-st-etienne.fr



CPA on Ascon with Multi-bit Selection Function



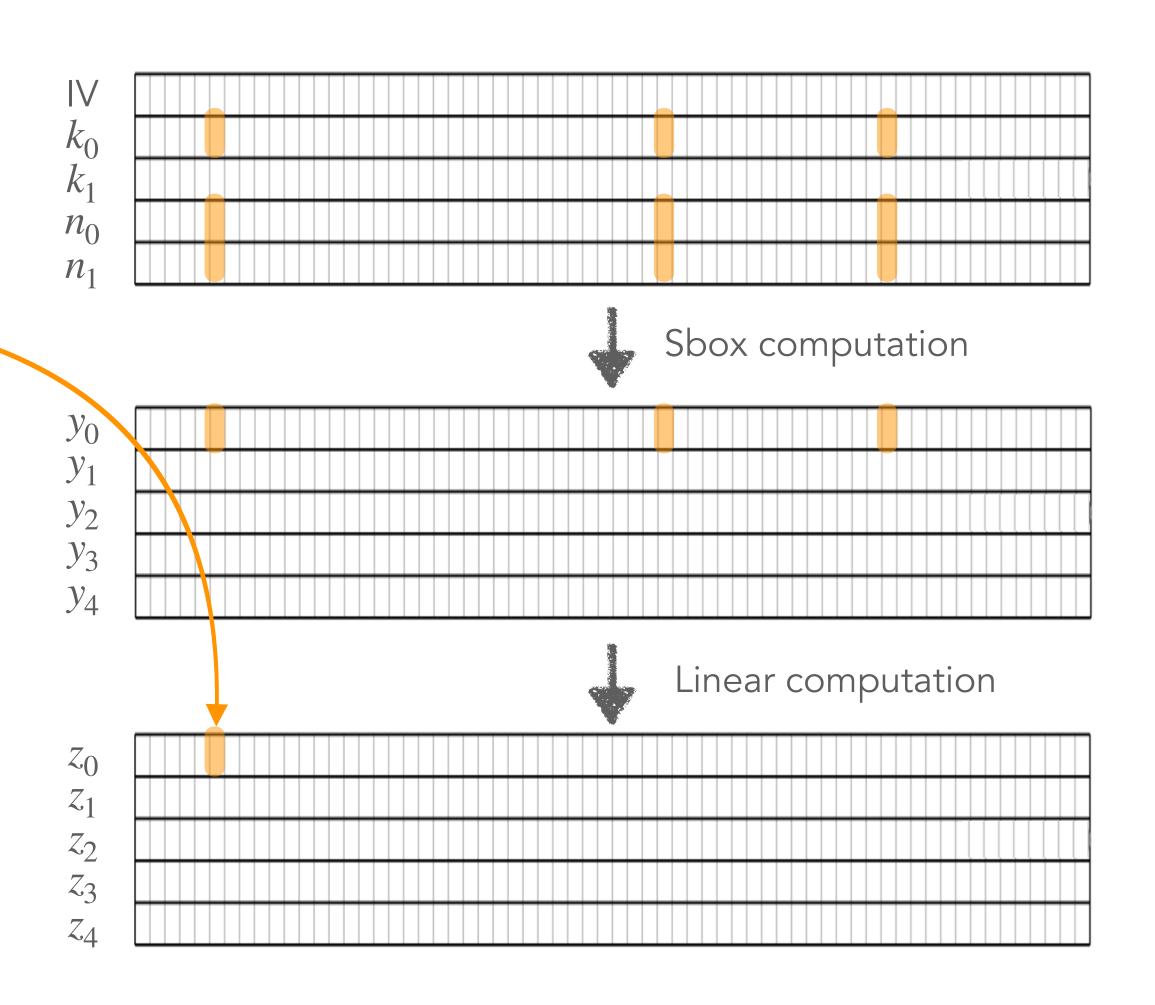
Samwel and Daemen, 2018

hypothetical power consumption

 7^{J} ~0

Viet-Sang Nguyen

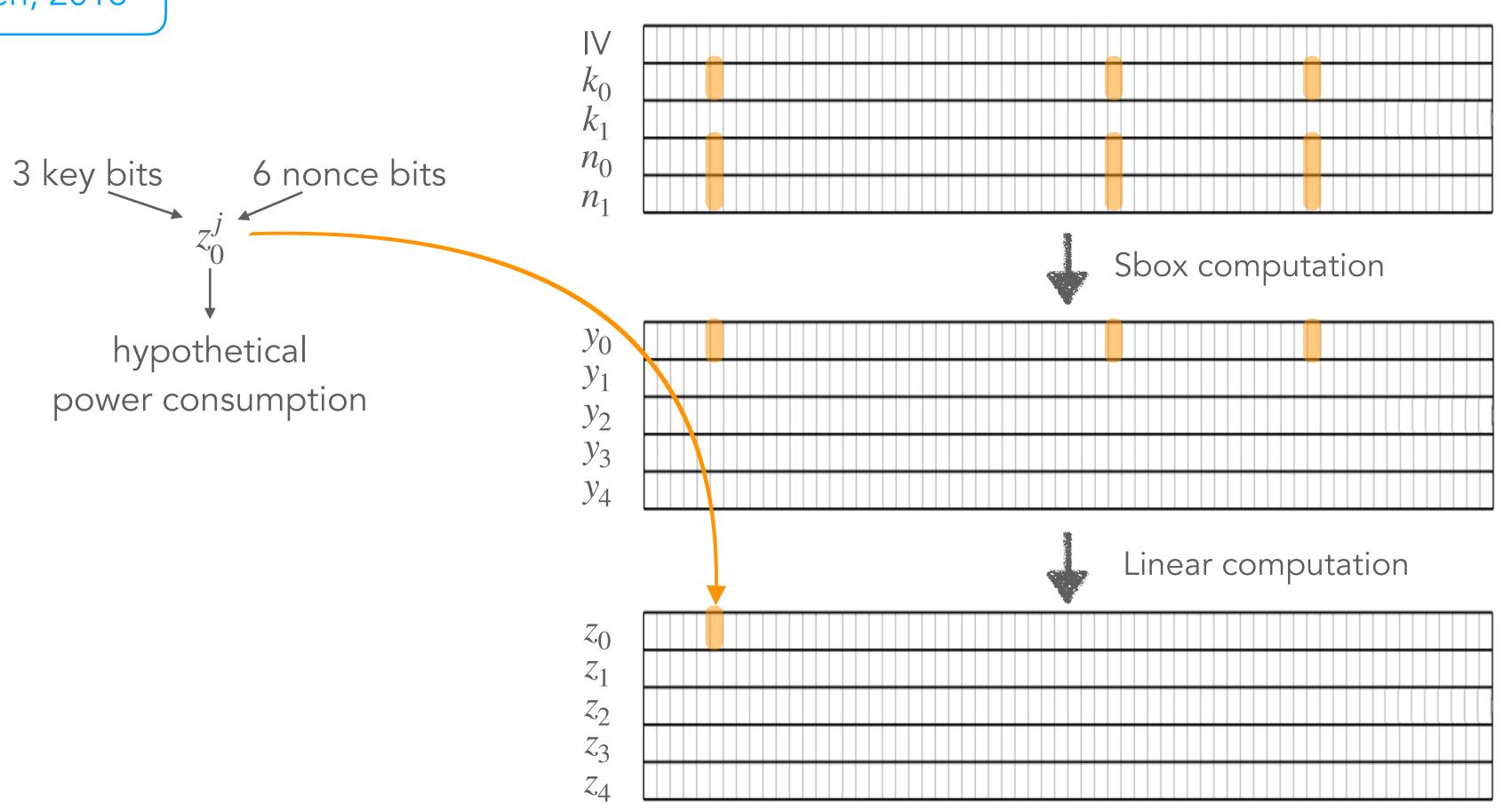
viet.sang.nguyen@univ-st-etienne.fr



CPA on Ascon with Multi-bit Selection Function



Samwel and Daemen, 2018

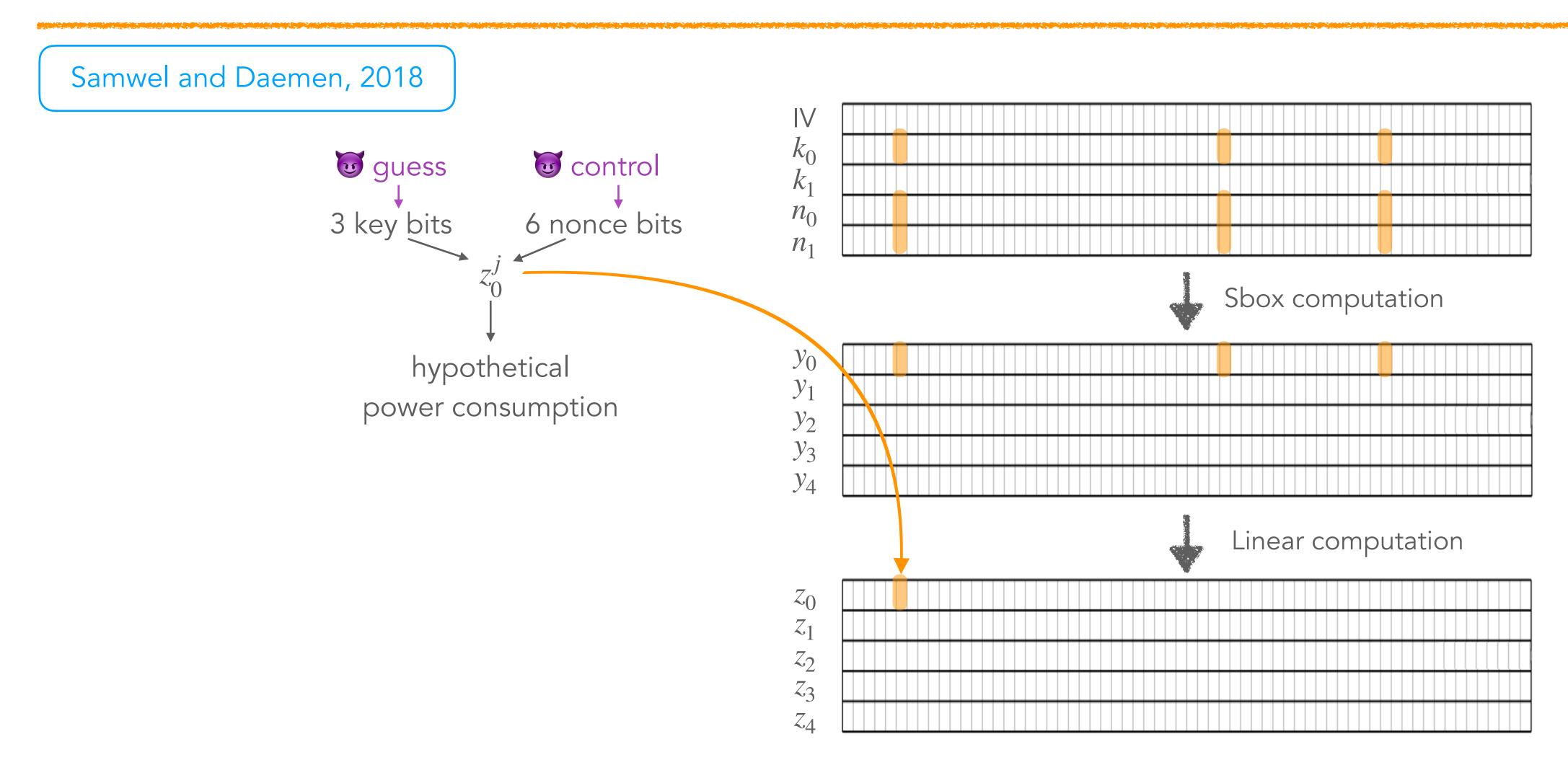


Viet-Sang Nguyen

viet.sang.nguyen@univ-st-etienne.fr

CPA on Ascon with Multi-bit Selection Function



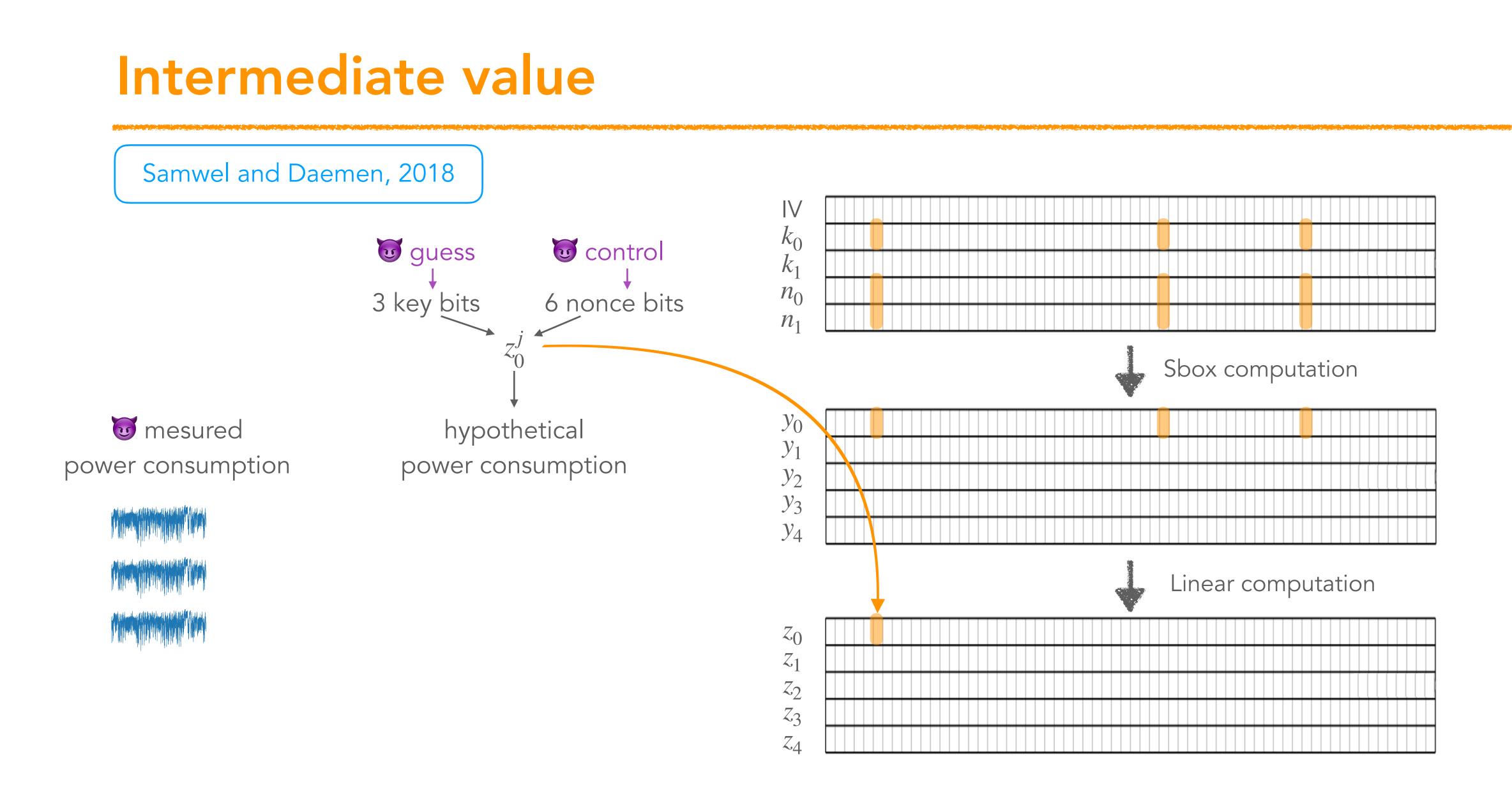


Viet-Sang Nguyen

viet.sang.nguyen@univ-st-etienne.fr

CPA on Ascon with Multi-bit Selection Function

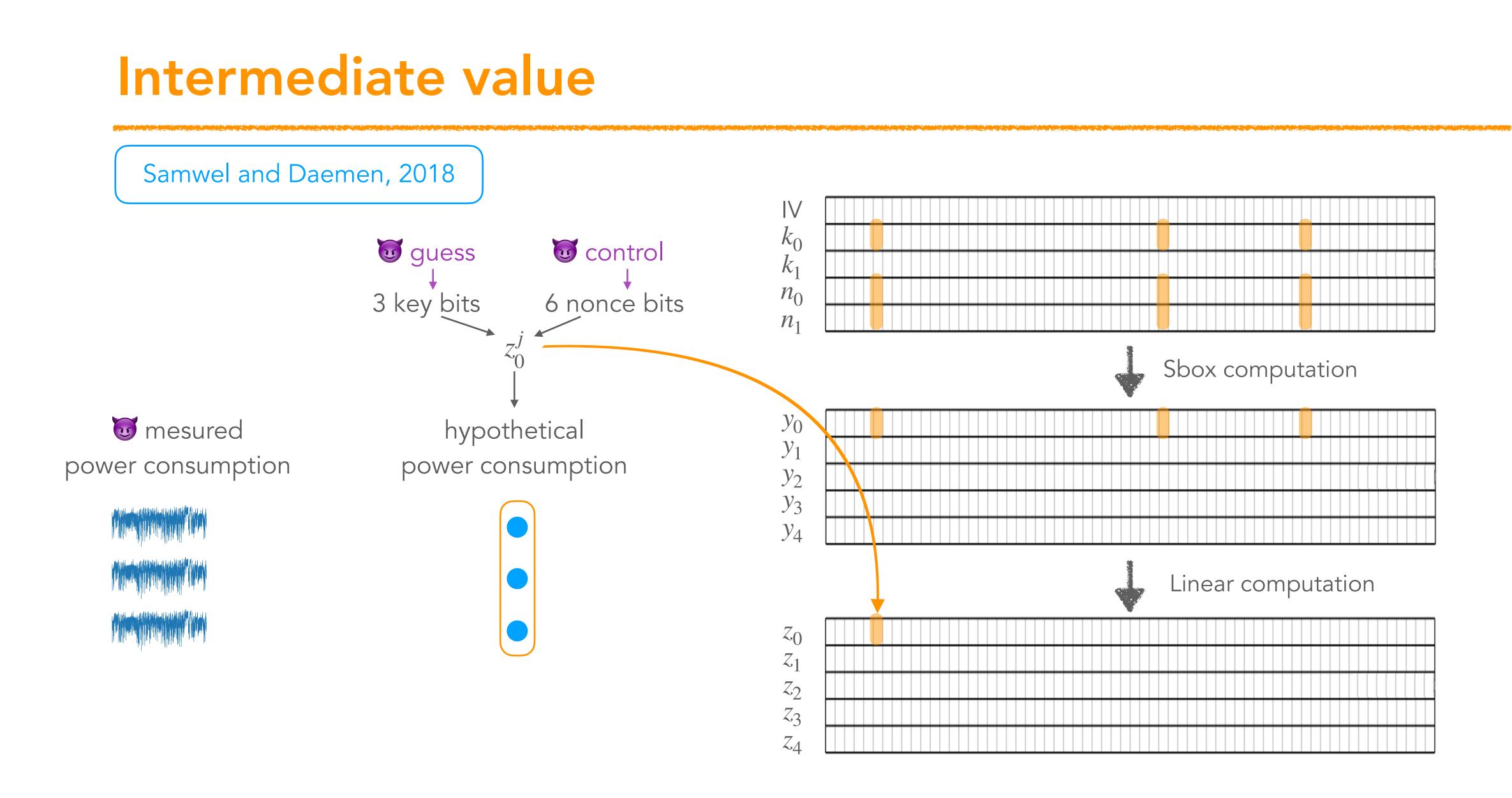




viet.sang.nguyen@univ-st-etienne.fr

CPA on Ascon with Multi-bit Selection Function

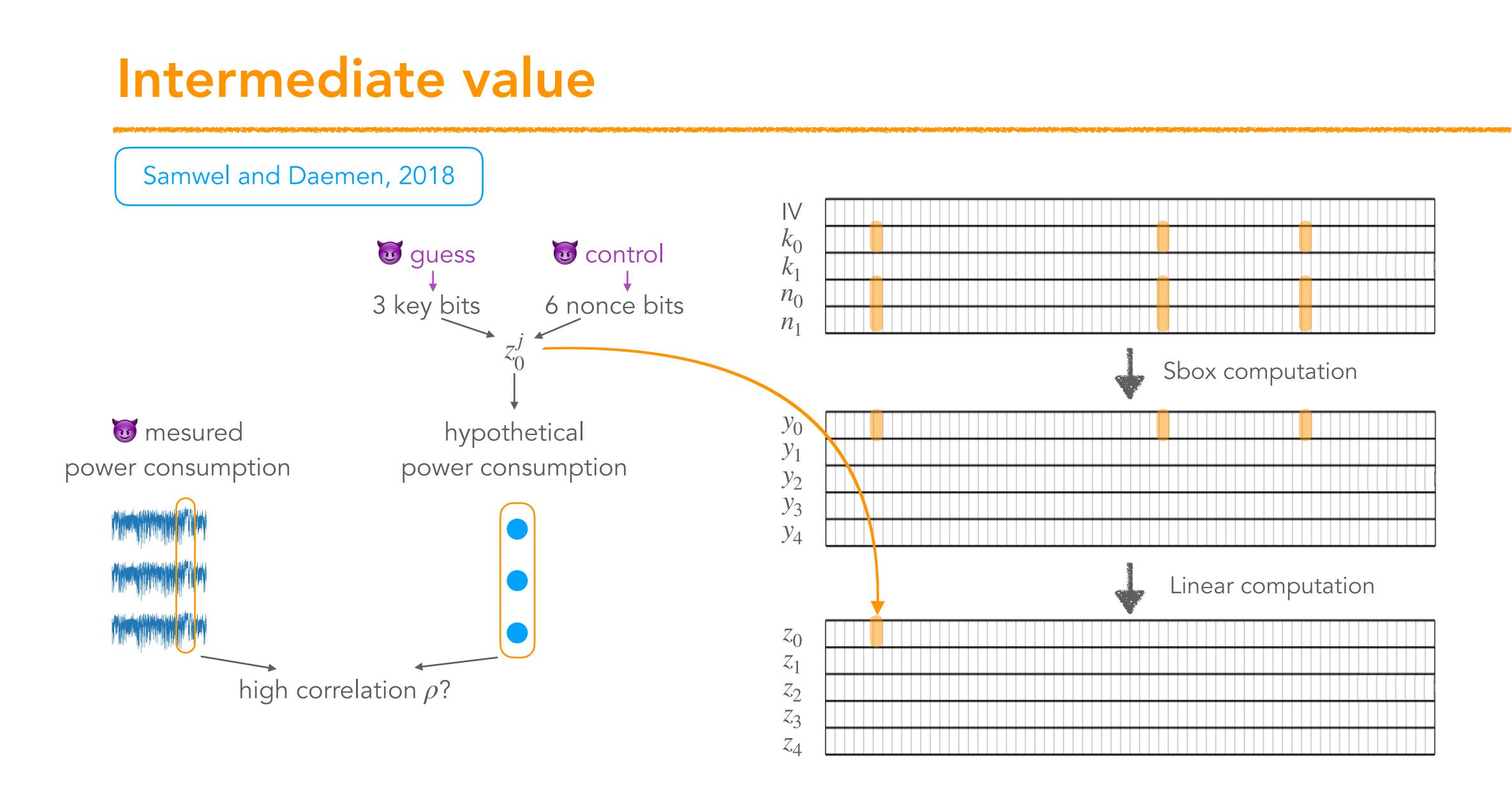




viet.sang.nguyen@univ-st-etienne.fr

CPA on Ascon with Multi-bit Selection Function

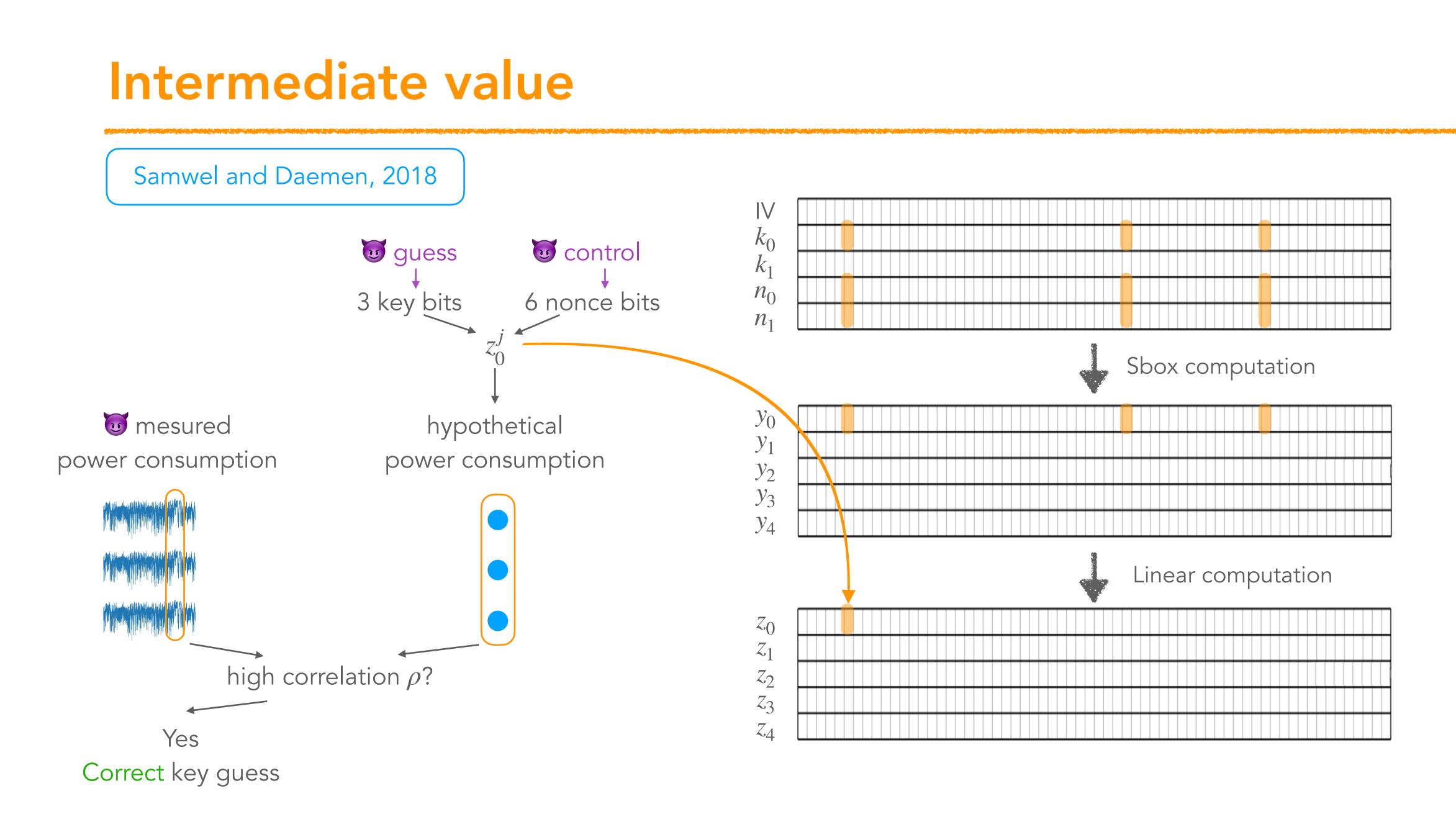




viet.sang.nguyen@univ-st-etienne.fr

CPA on Ascon with Multi-bit Selection Function

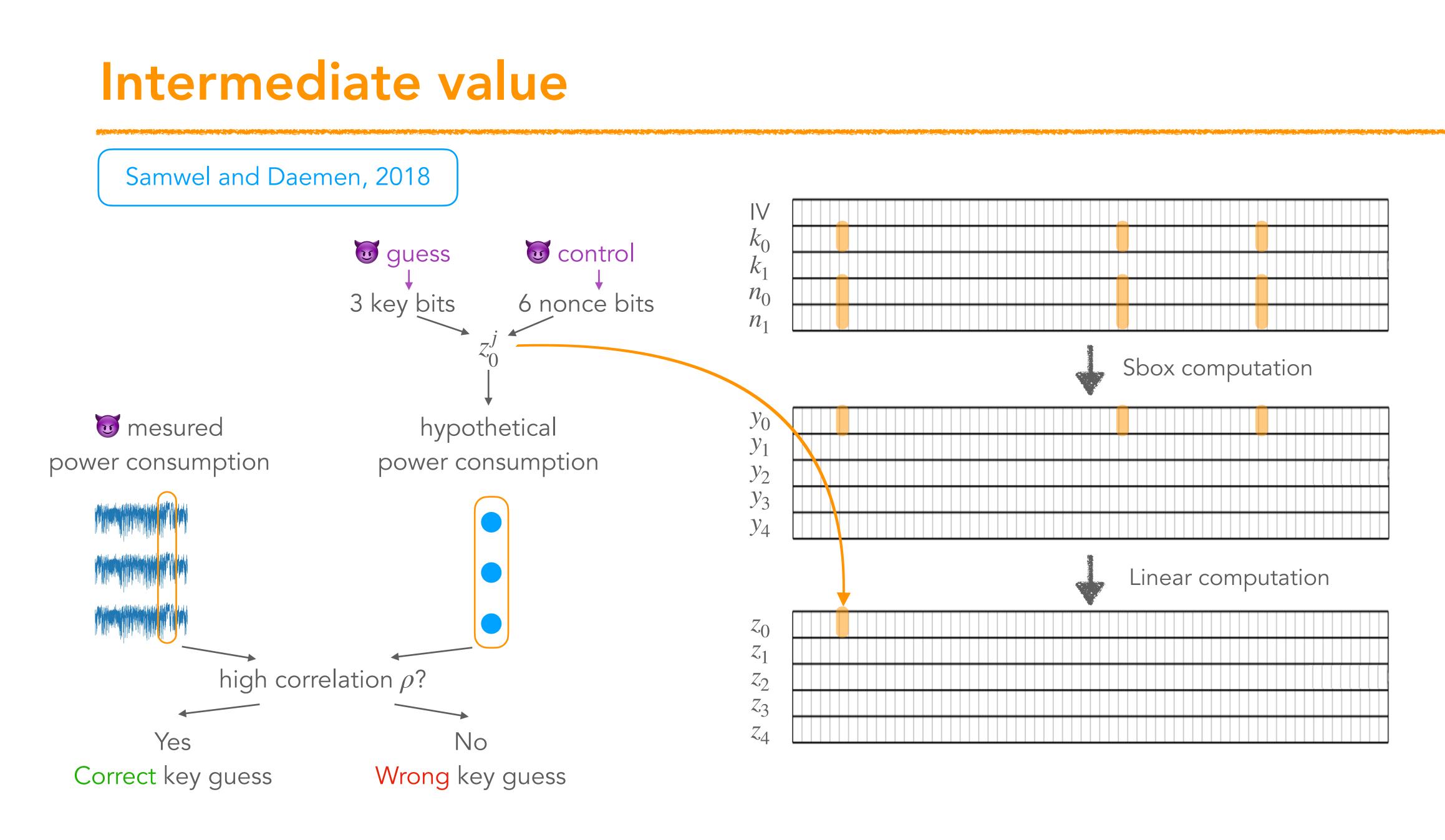




viet.sang.nguyen@univ-st-etienne.fr

CPA on Ascon with Multi-bit Selection Function





viet.sang.nguyen@univ-st-etienne.fr

CPA on Ascon with Multi-bit Selection Function





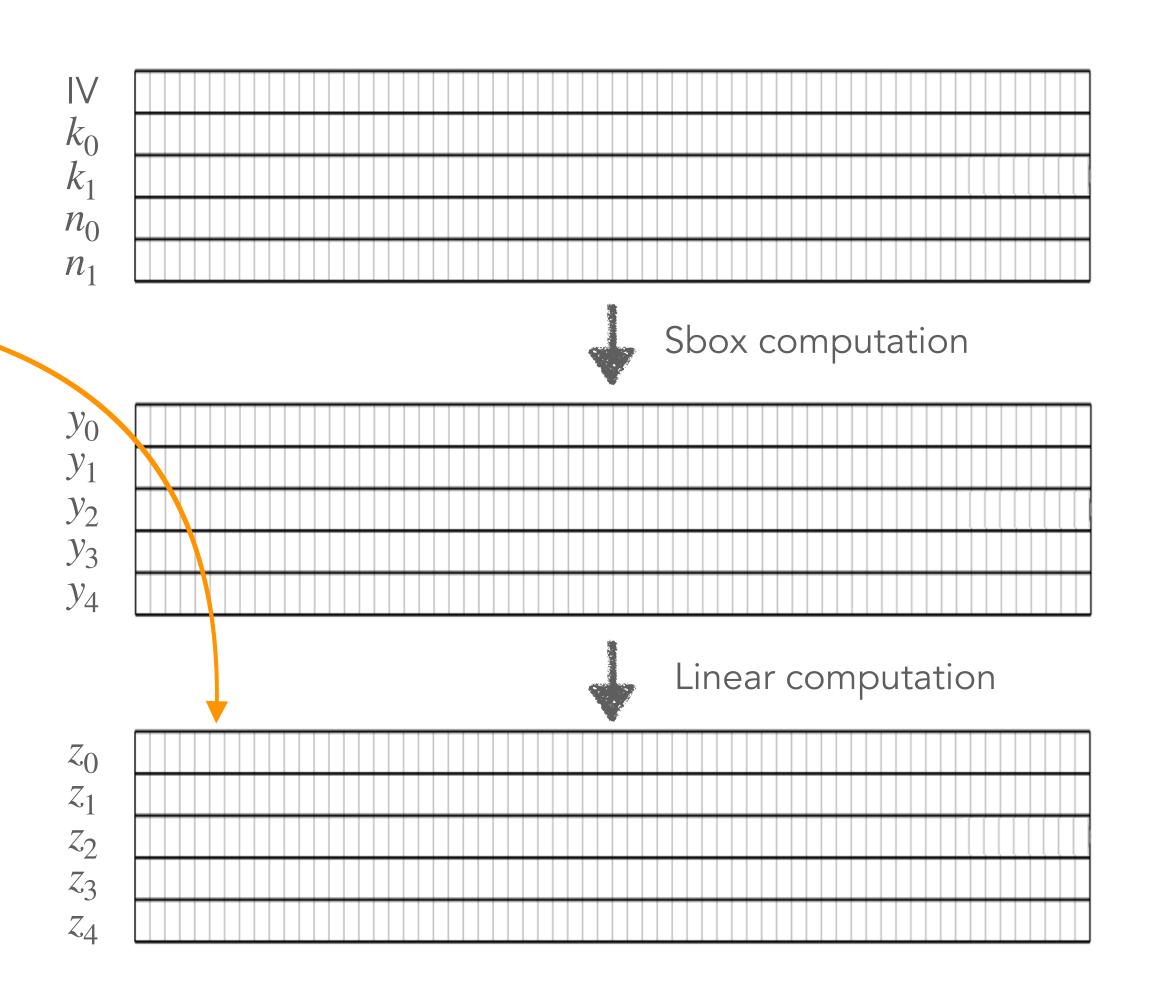
Main idea

~0 hypothetical power consumption

 7^{J}

Viet-Sang Nguyen

viet.sang.nguyen@univ-st-etienne.fr



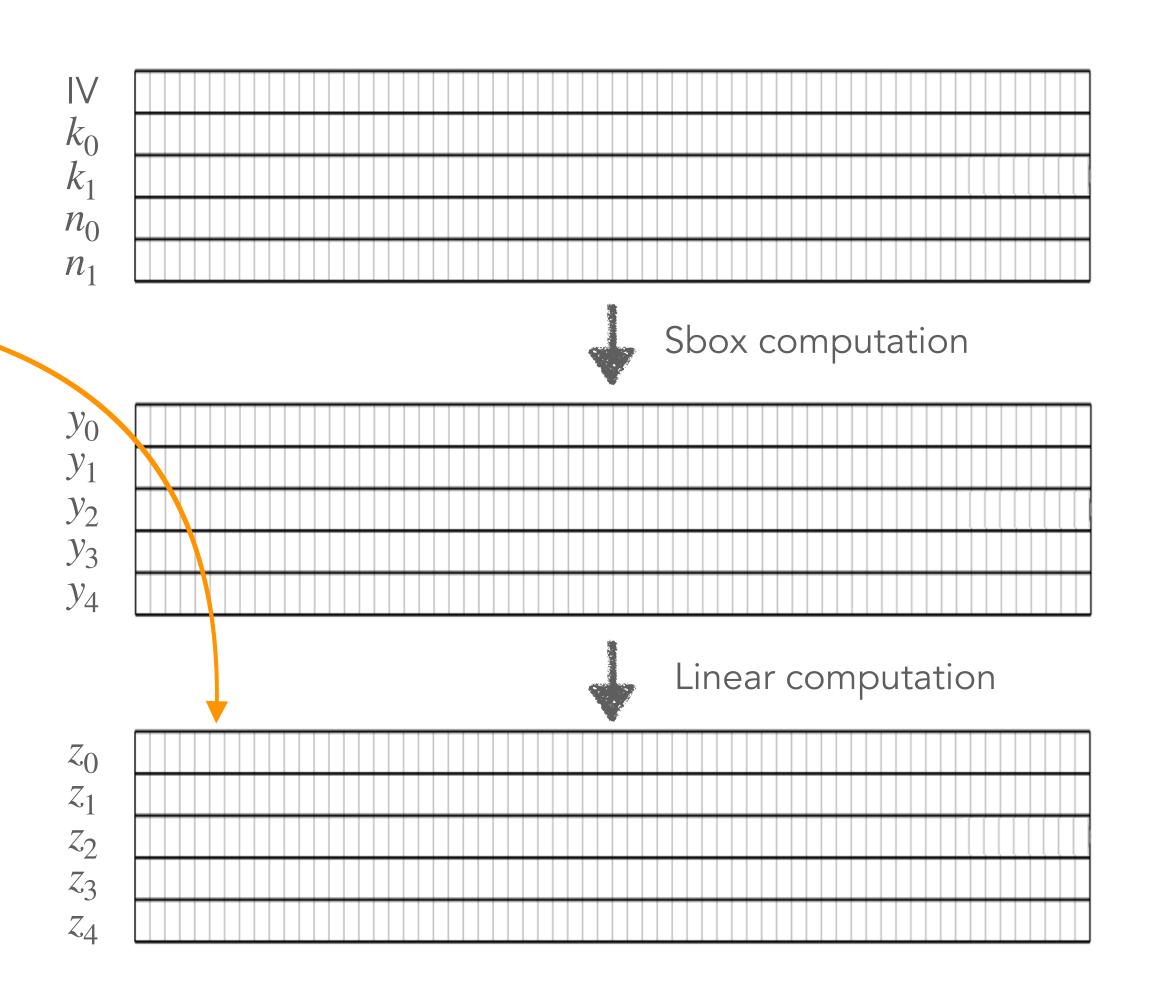


hypothetical power consumption (modeled on 1 bit)

 7^{J} ~0

Viet-Sang Nguyen

viet.sang.nguyen@univ-st-etienne.fr





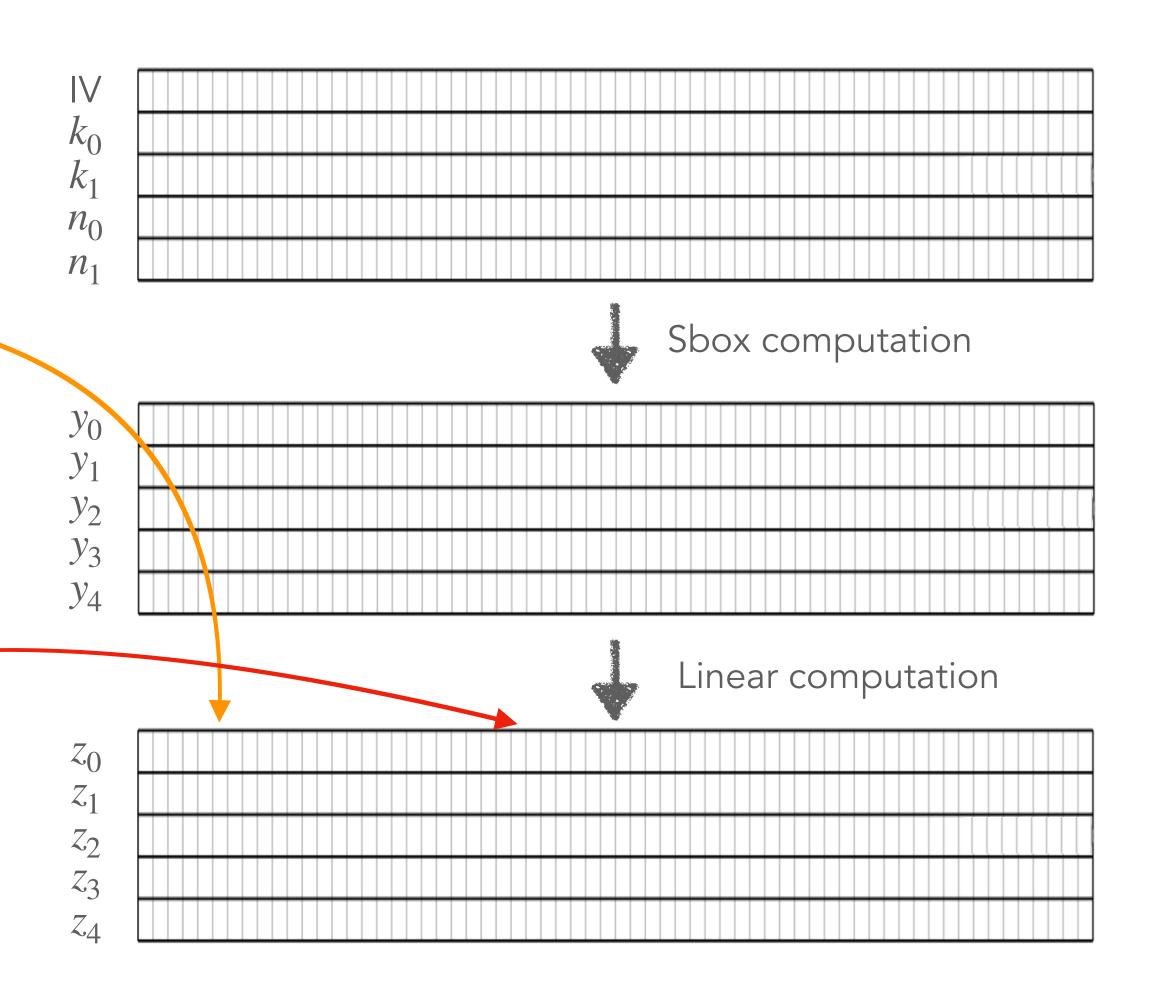
hypothetical power consumption (modeled on 1 bit)

 Z_0^J

actual power consumption depends on entire *m*-bit machine word

viet.sang.nguyen@univ-st-etienne.fr

Viet-Sang Nguyen



CPA on Ascon with Multi-bit Selection Function



partial correlation when considering d out of m bits

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

Brier et al., 2004

hypothetical power consumption

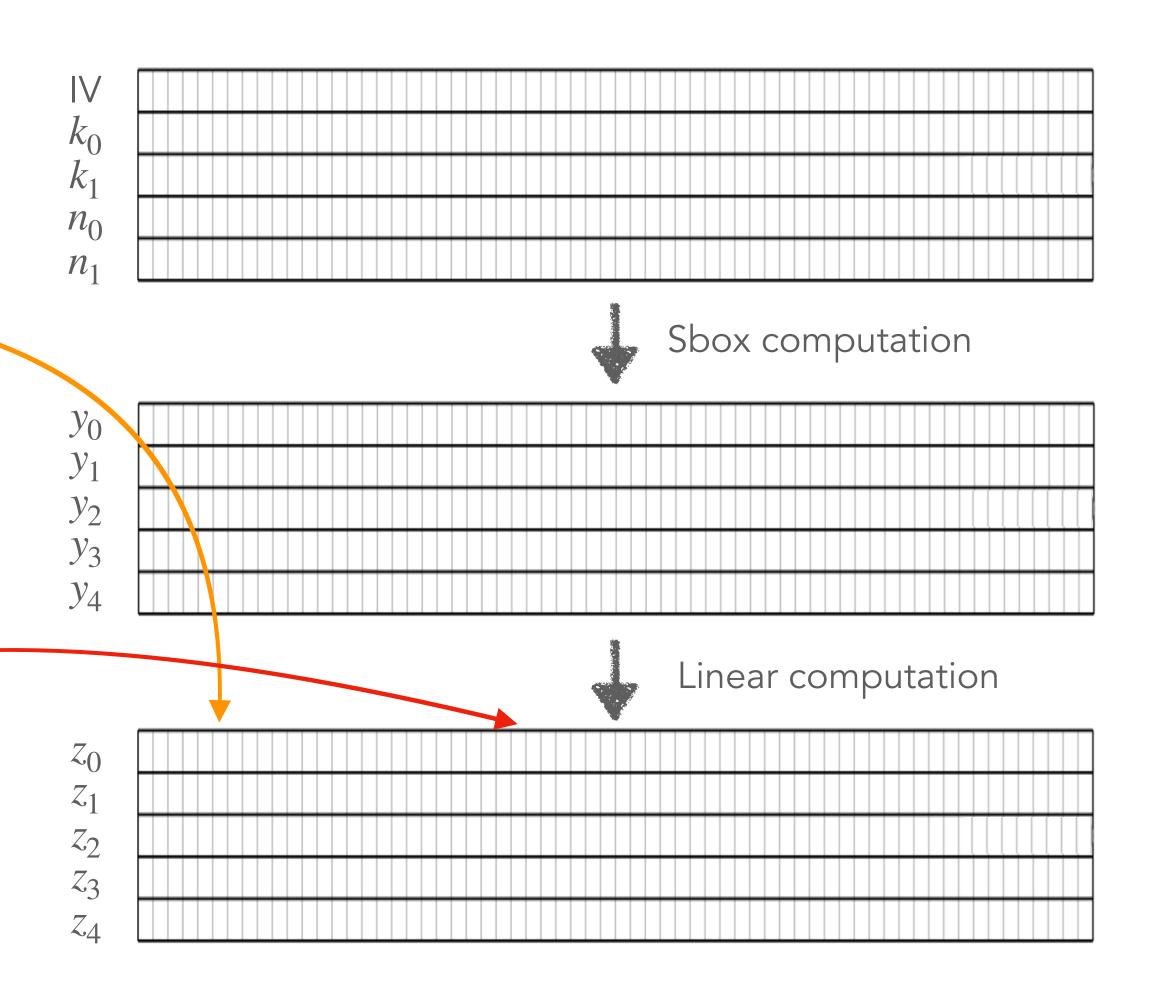
 z_0^J

(modeled on 1 bit)

actual power consumption depends on entire *m*-bit machine word

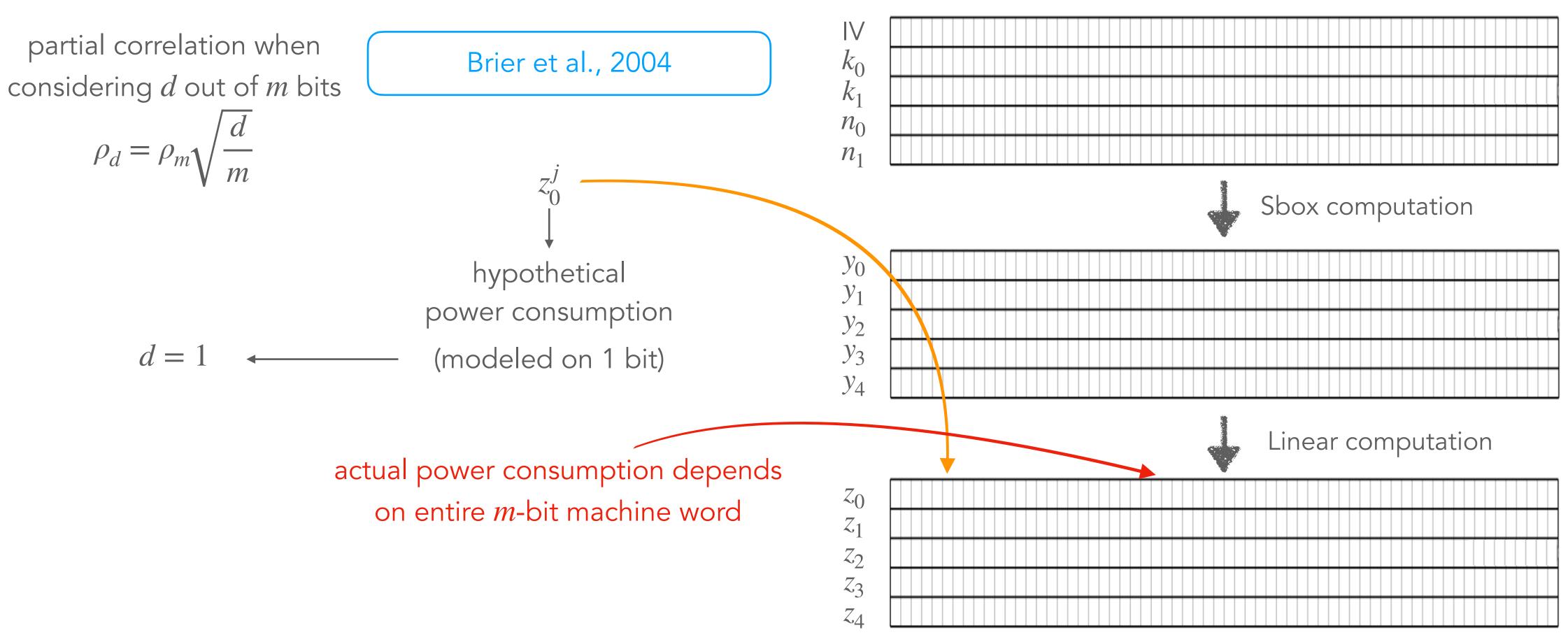
Viet-Sang Nguyen

viet.sang.nguyen@univ-st-etienne.fr







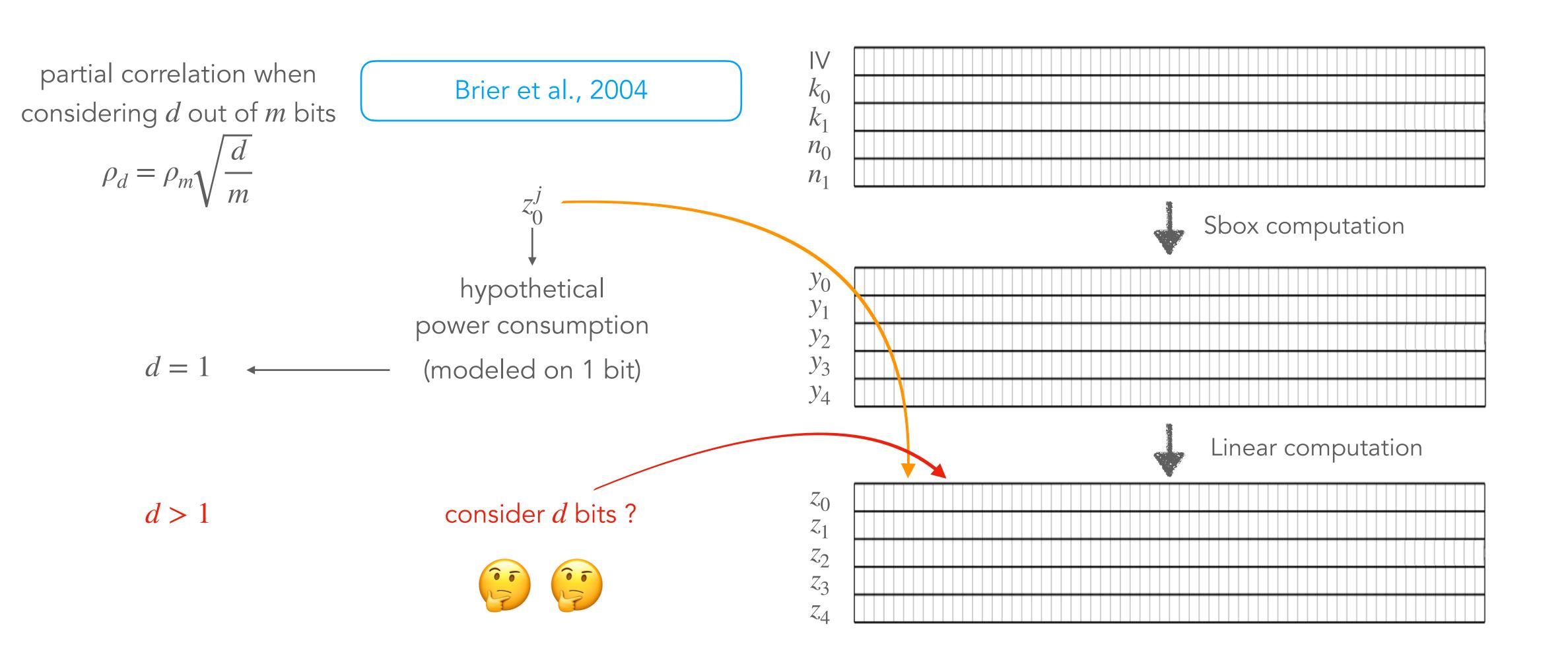


Viet-Sang Nguyen

viet.sang.nguyen@univ-st-etienne.fr





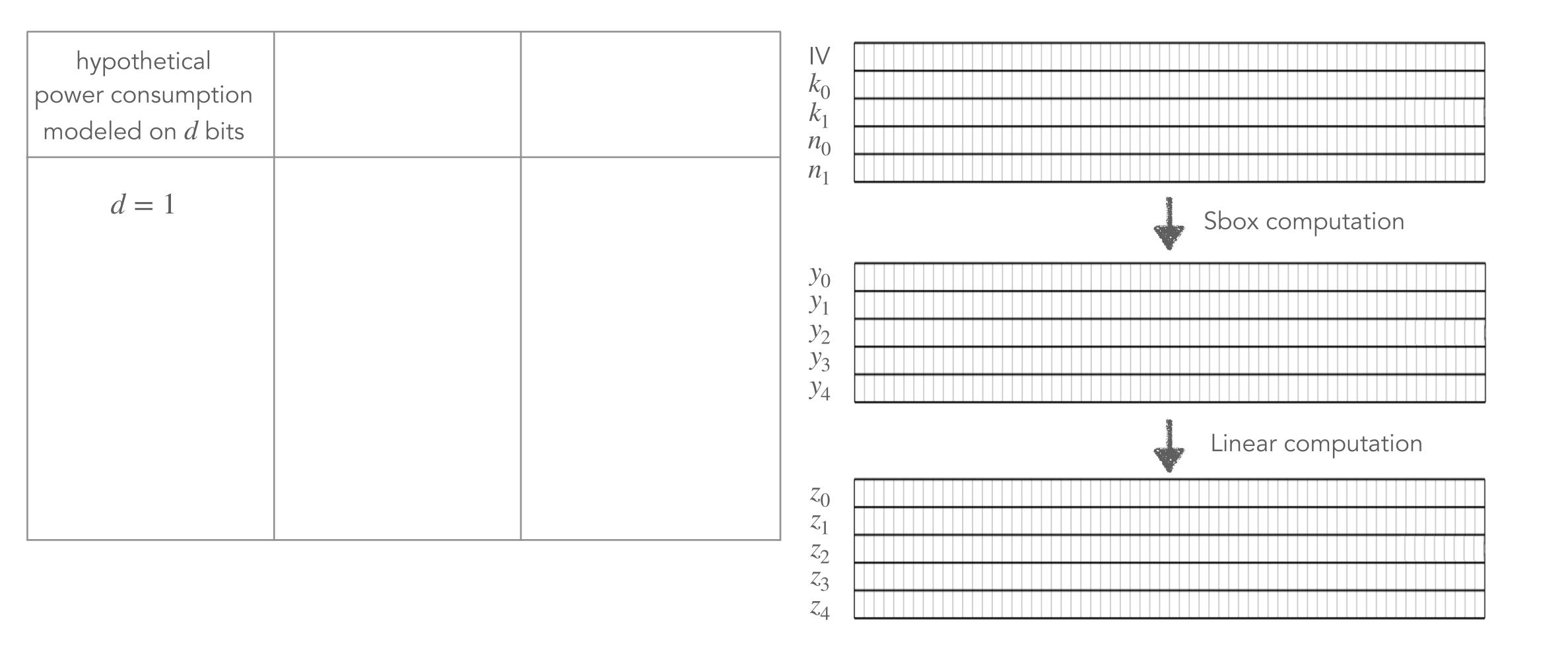


Viet-Sang Nguyen

viet.sang.nguyen@univ-st-etienne.fr





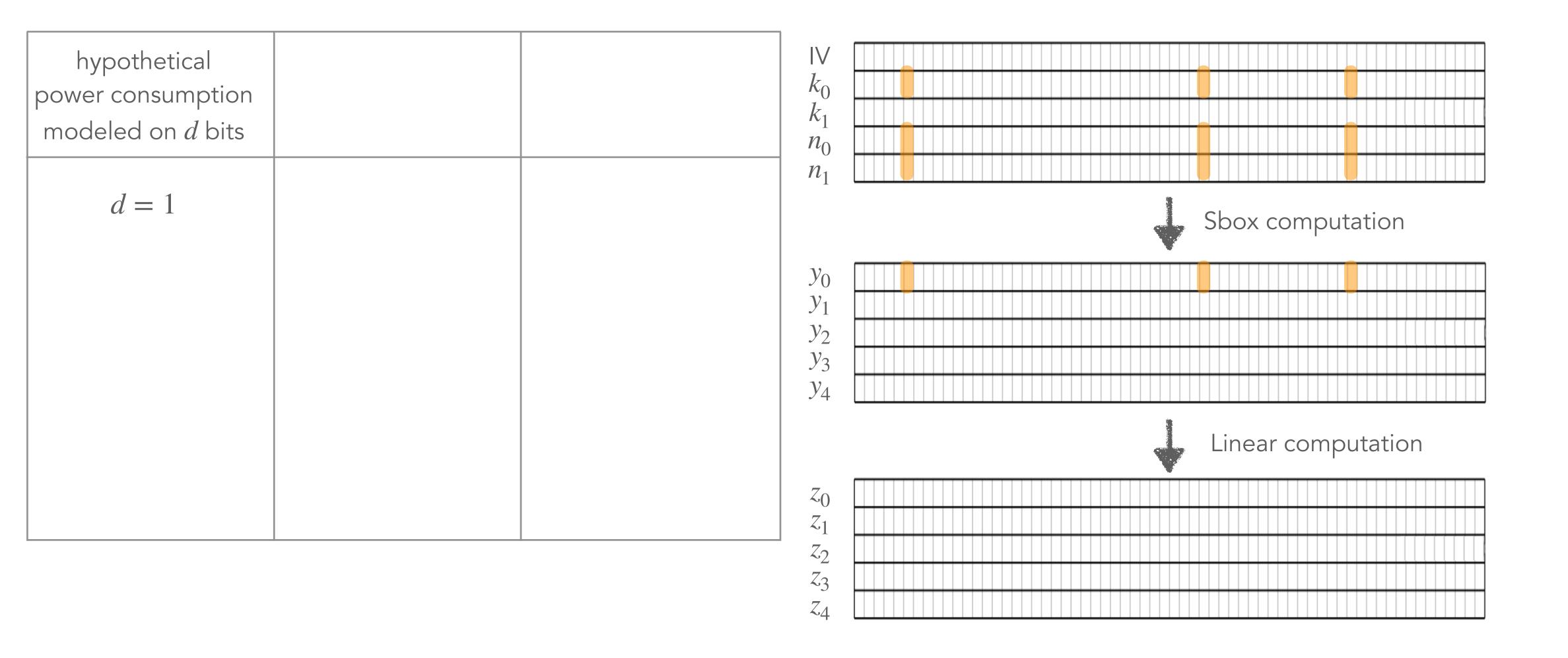


Viet-Sang Nguyen

viet.sang.nguyen@univ-st-etienne.fr







Viet-Sang Nguyen

viet.sang.nguyen@univ-st-etienne.fr

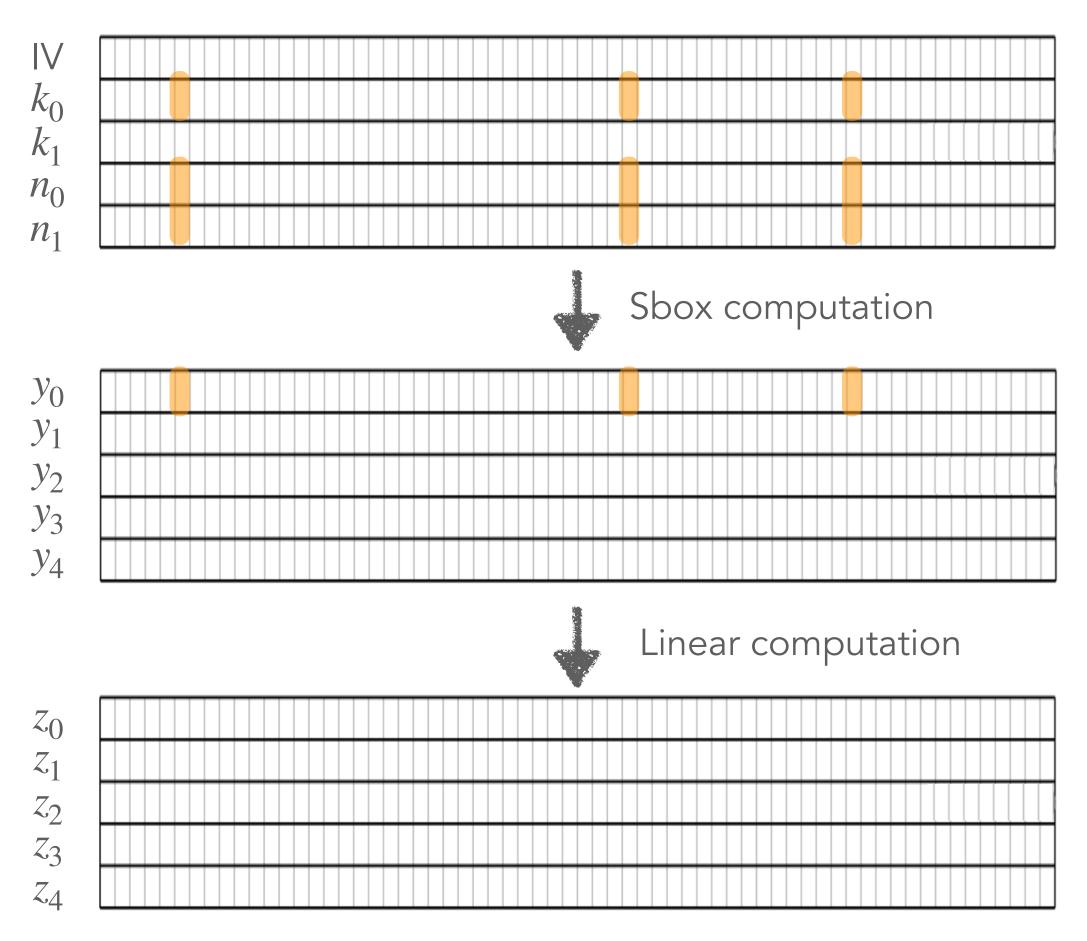




hypothetical power consumption modeled on <i>d</i> bits	# recovered key bits in 1 CPA run	
d = 1	3	

Viet-Sang Nguyen

viet.sang.nguyen@univ-st-etienne.fr



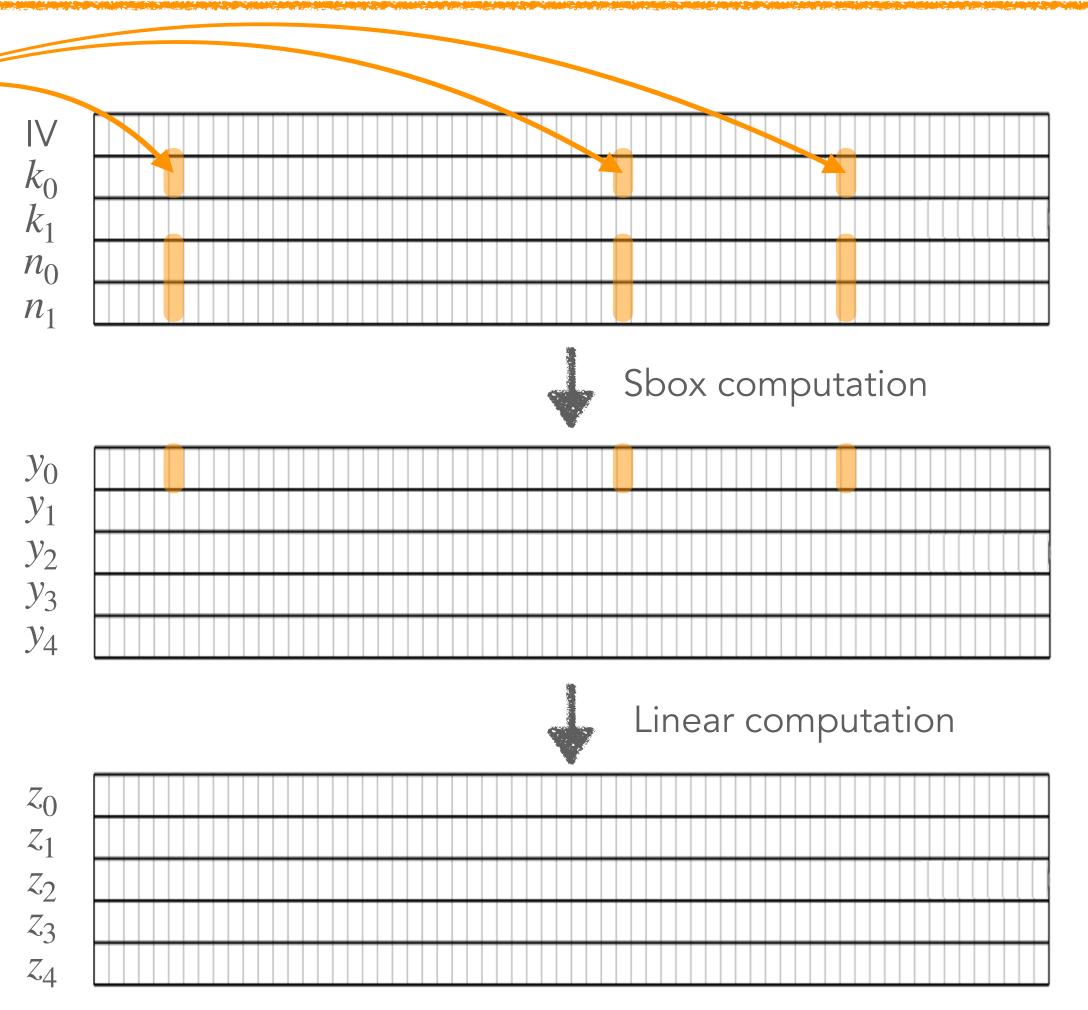




# recovered key bits in 1 CPA run	
3	

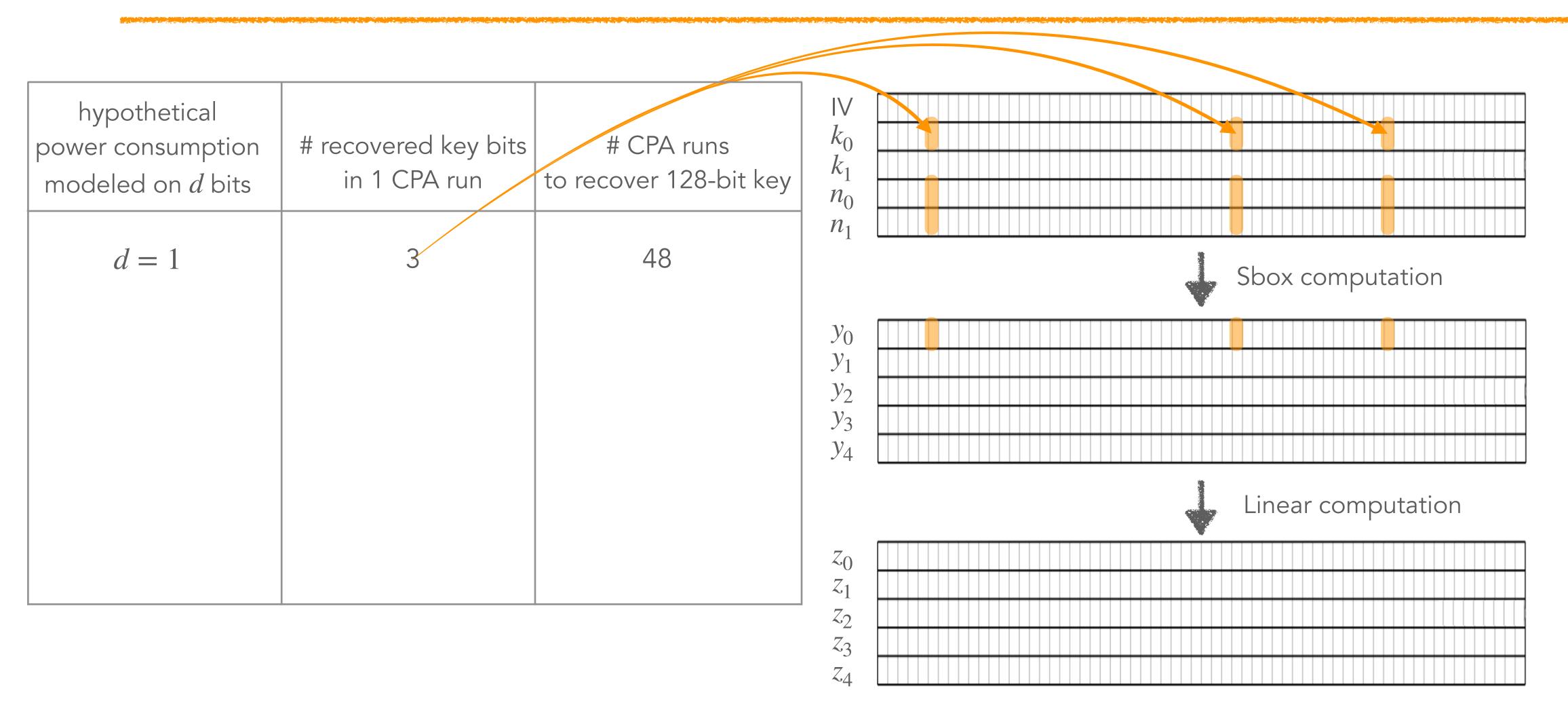
Viet-Sang Nguyen

viet.sang.nguyen@univ-st-etienne.fr









Viet-Sang Nguyen

viet.sang.nguyen@univ-st-etienne.fr

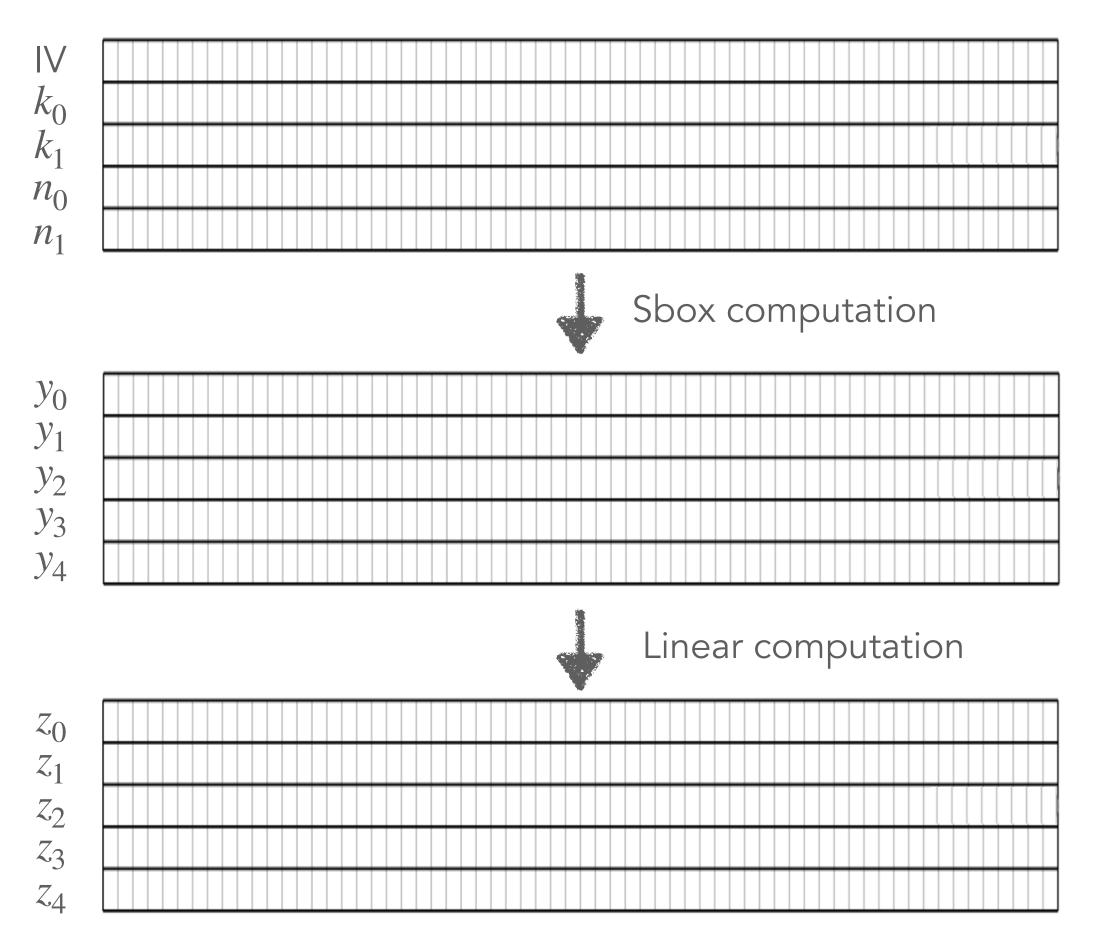




hypothetical power consumption modeled on <i>d</i> bits	# recovered key bits in 1 CPA run	# CPA runs to recover 128-bit key
d = 1	3	48

Viet-Sang Nguyen

viet.sang.nguyen@univ-st-etienne.fr



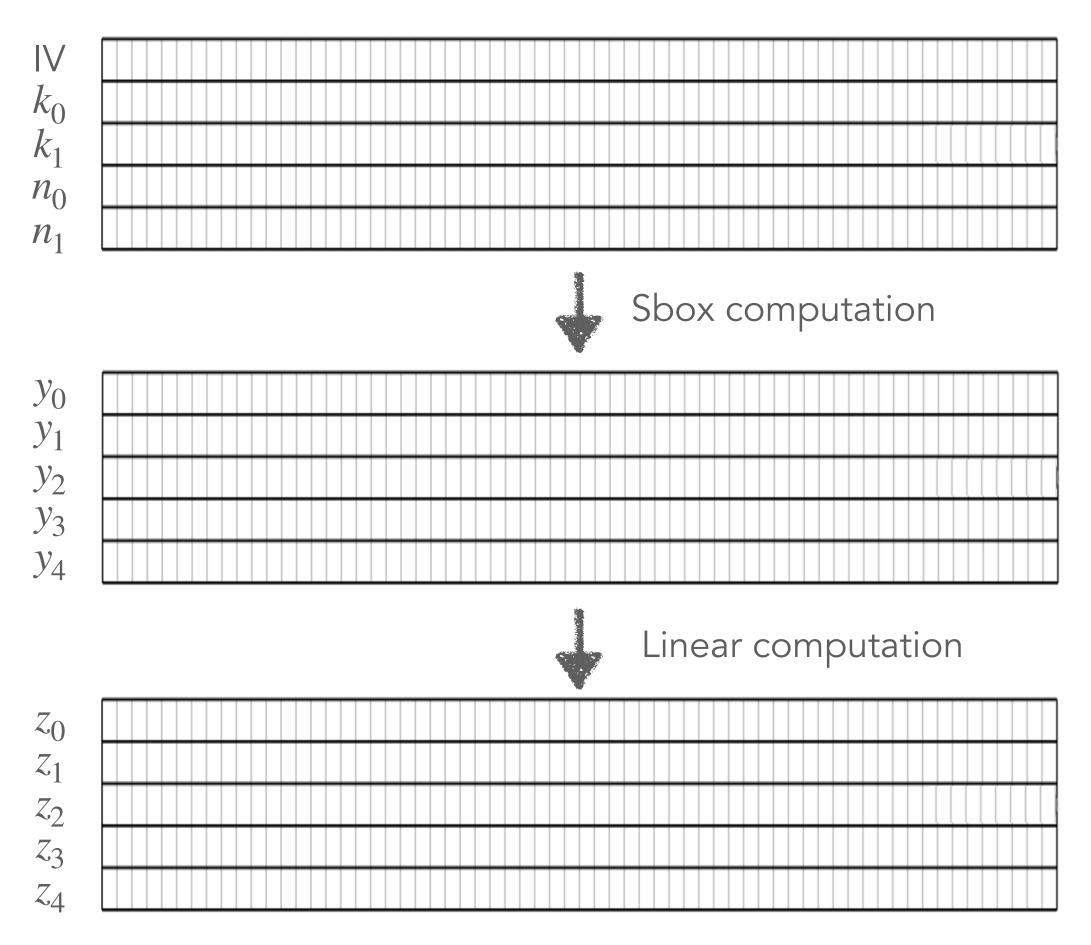




hypothetical power consumption modeled on <i>d</i> bits	# recovered key bits in 1 CPA run	# CPA runs to recover 128-bit key
d = 1	3	48
d = 2		



viet.sang.nguyen@univ-st-etienne.fr

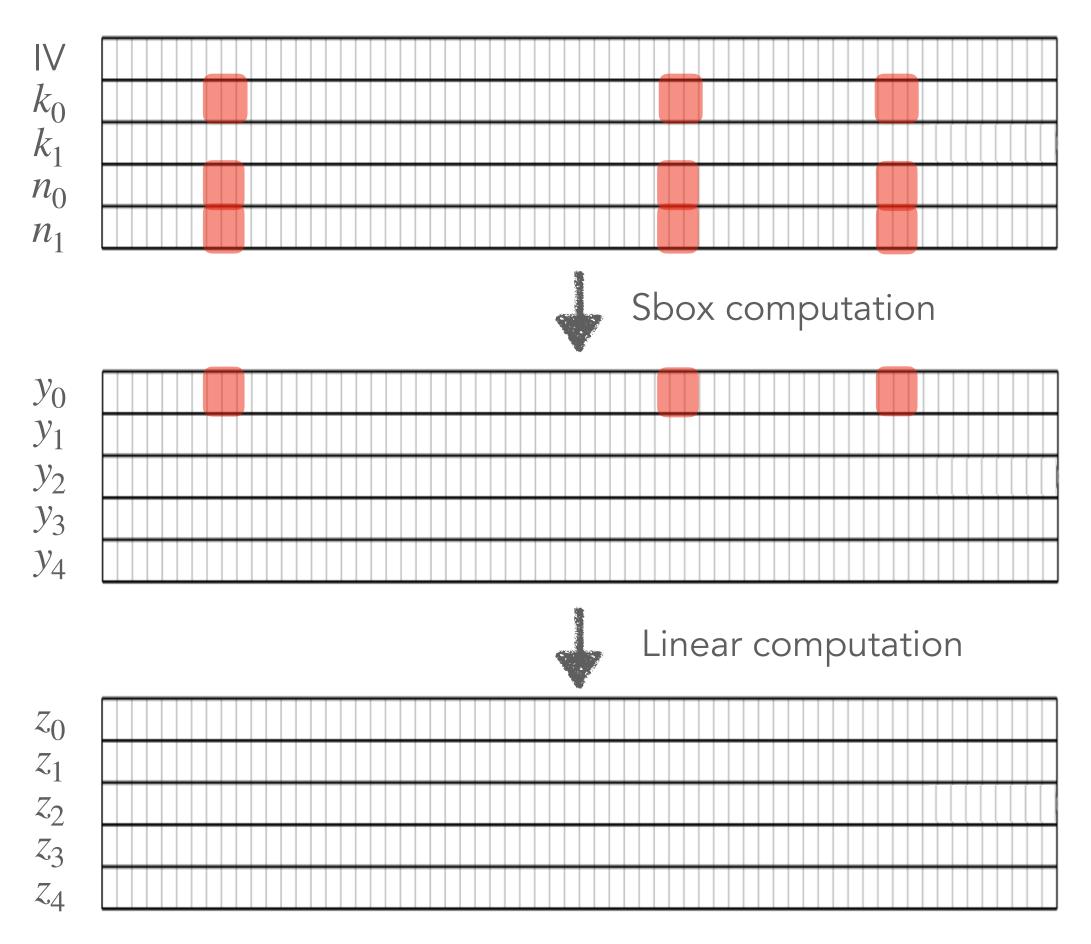




hypothetical power consumption modeled on <i>d</i> bits	# recovered key bits in 1 CPA run	# CPA runs to recover 128-bit key
d = 1	3	48
d = 2		



viet.sang.nguyen@univ-st-etienne.fr

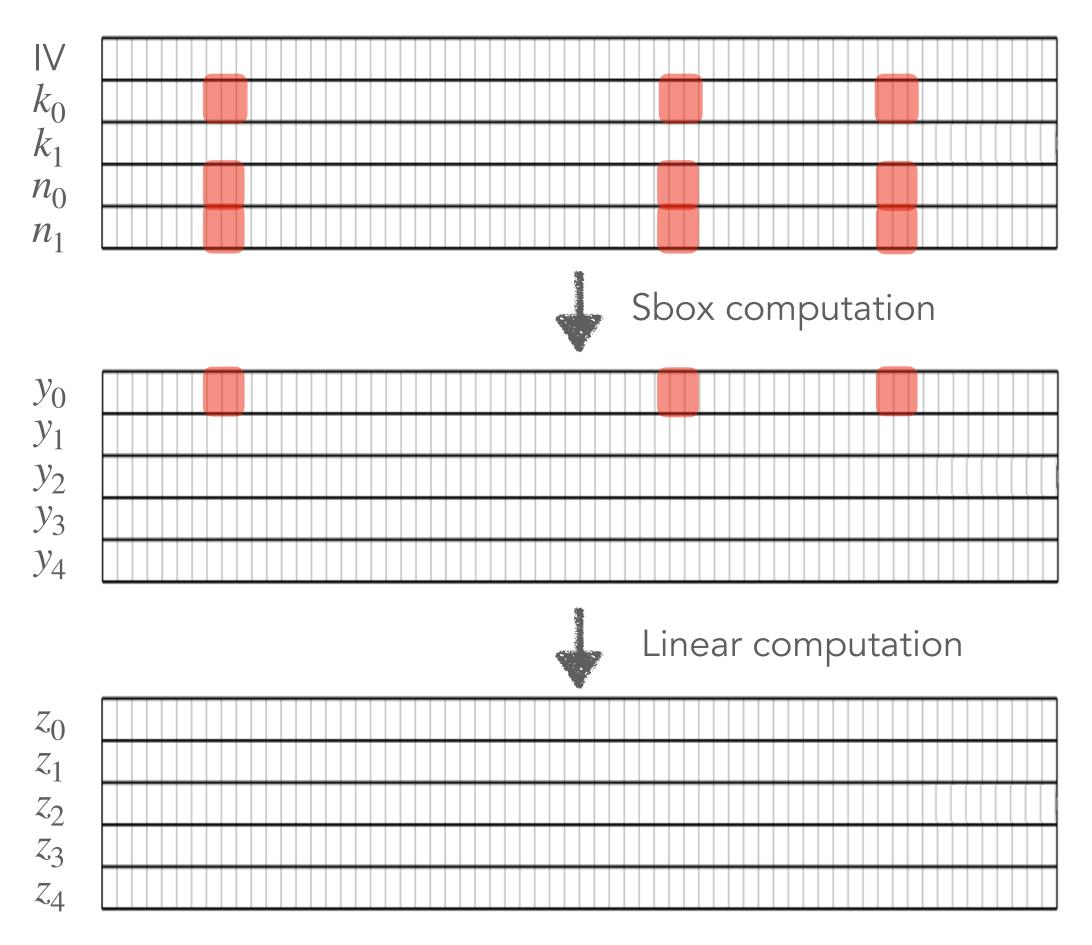




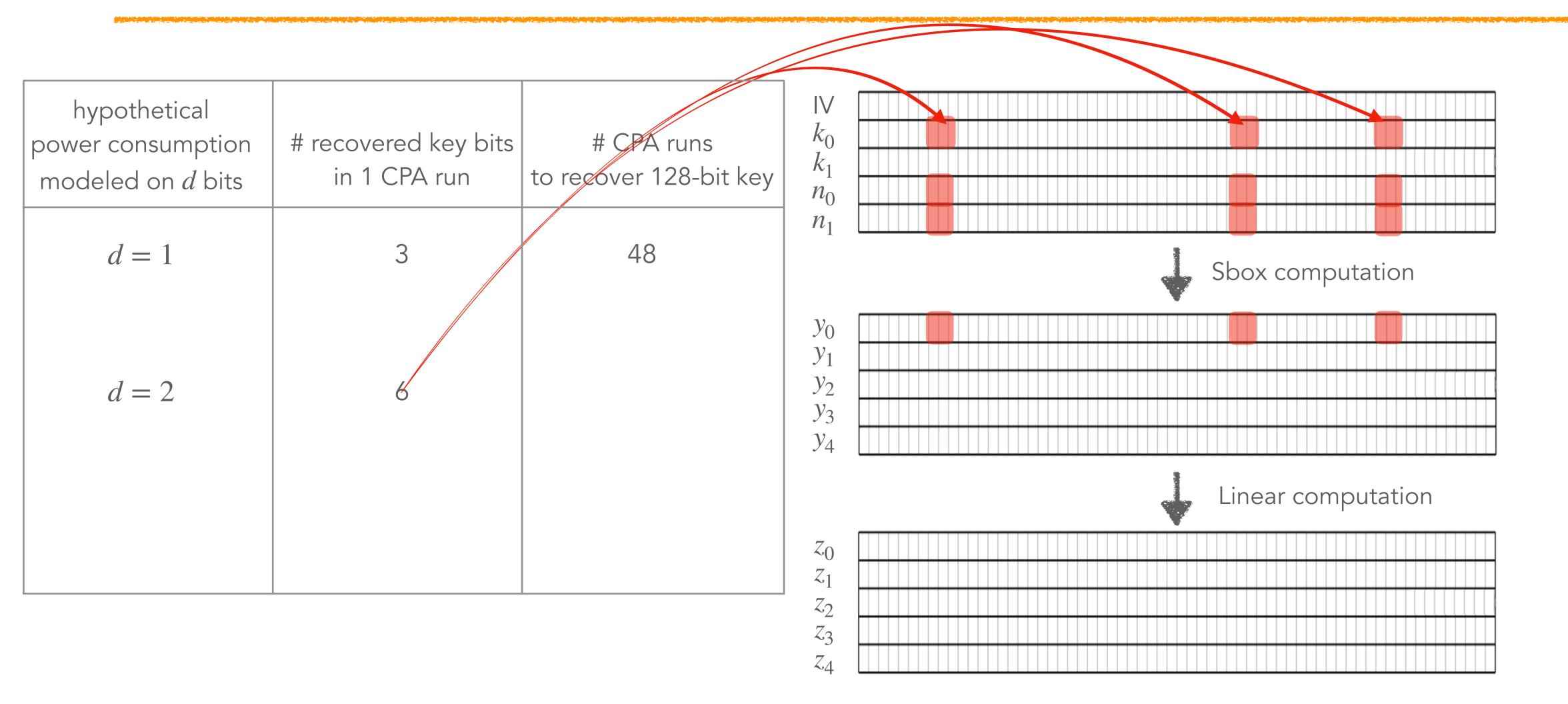
hypothetical power consumption modeled on <i>d</i> bits	# recovered key bits in 1 CPA run	# CPA runs to recover 128-bit key
d = 1	3	48
d = 2	6	

Viet-Sang Nguyen

viet.sang.nguyen@univ-st-etienne.fr



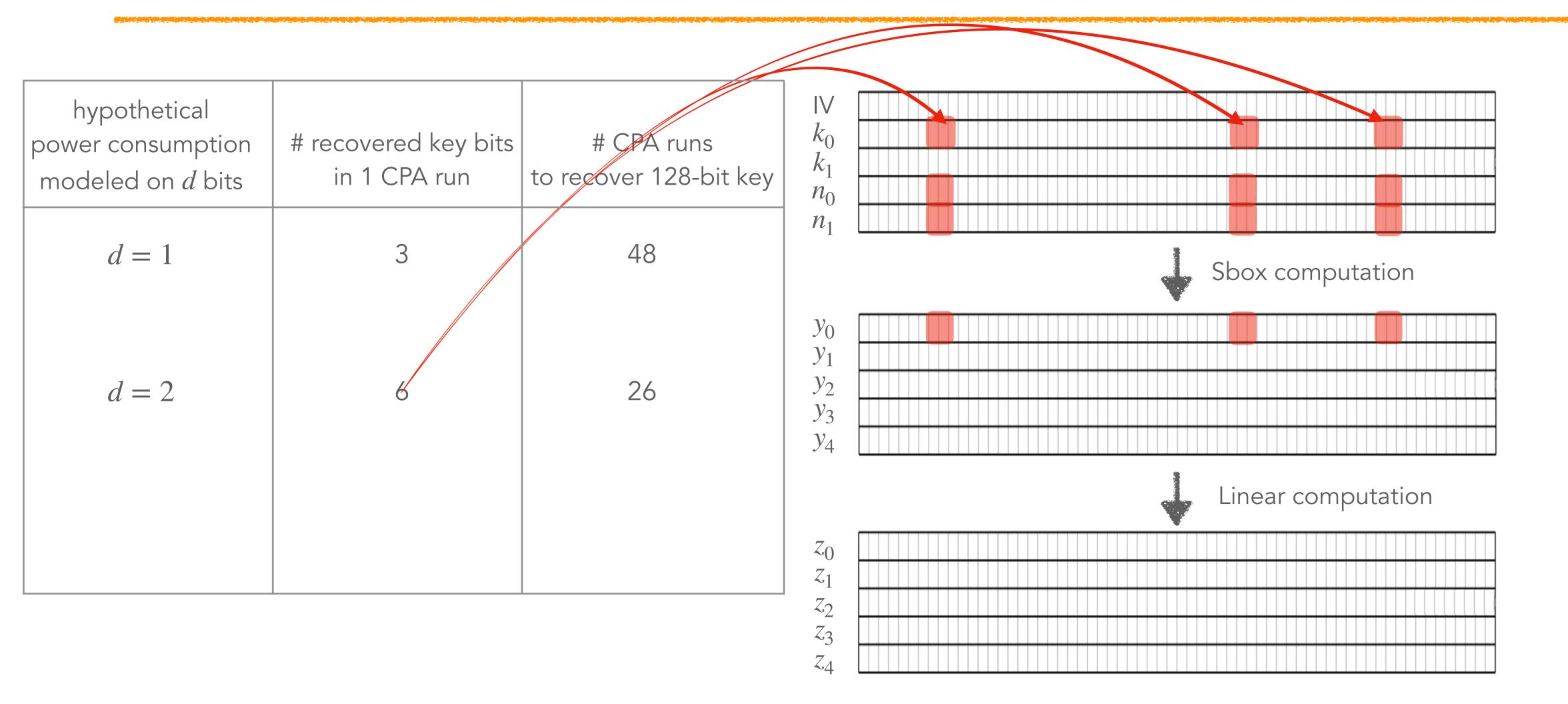




Viet-Sang Nguyen

viet.sang.nguyen@univ-st-etienne.fr





Viet-Sang Nguyen

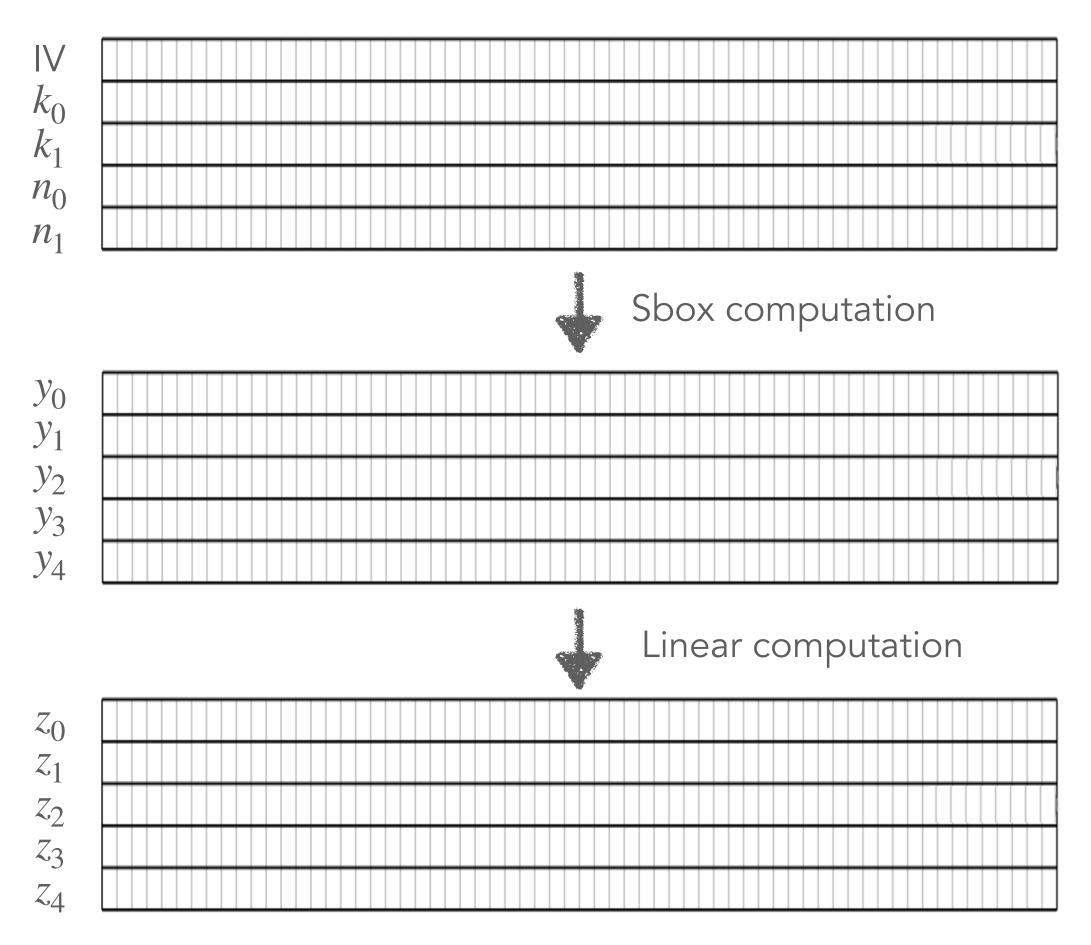
viet.sang.nguyen@univ-st-etienne.fr



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

Viet-Sang Nguyen

viet.sang.nguyen@univ-st-etienne.fr

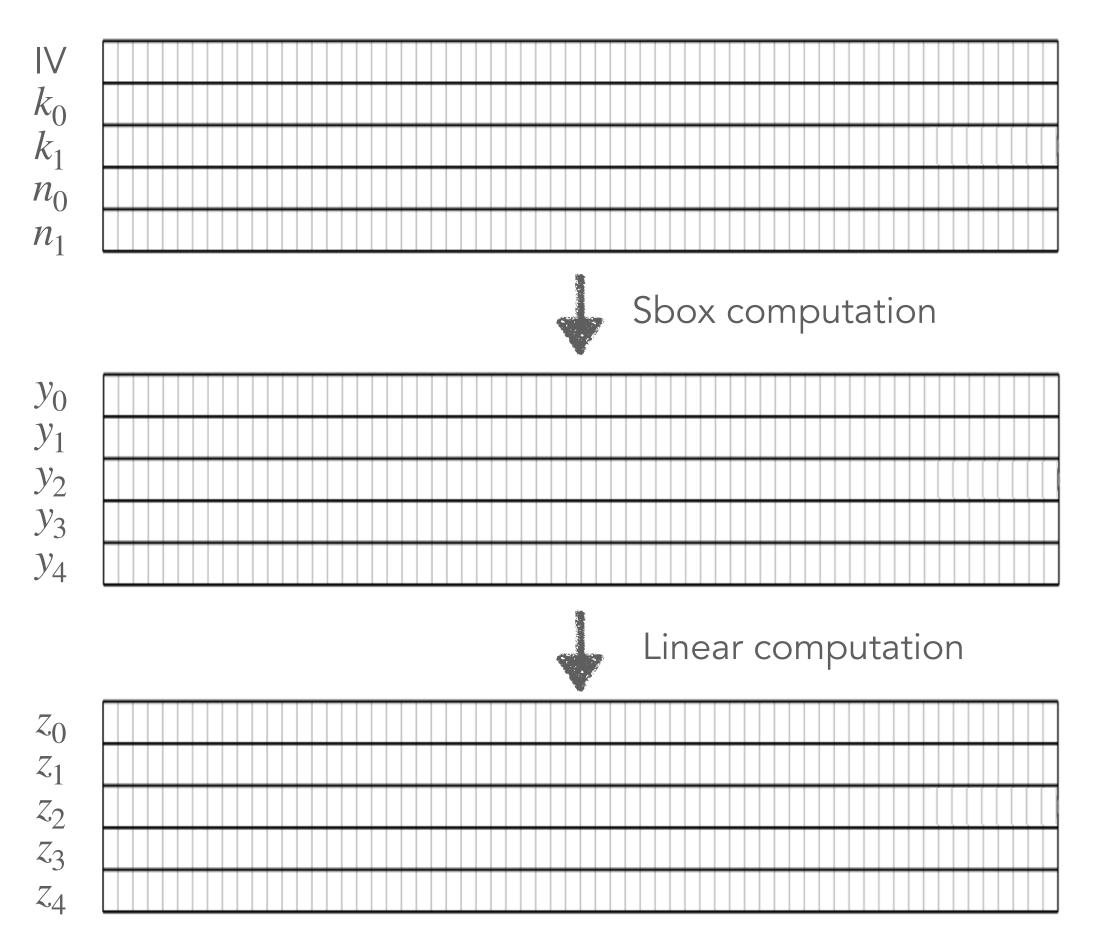


CPA on Ascon with Multi-bit Selection Function

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

Viet-Sang Nguyen

viet.sang.nguyen@univ-st-etienne.fr



CPA on Ascon with Multi-bit Selection Function

Results of full key recovery

Viet-Sang Nguyen

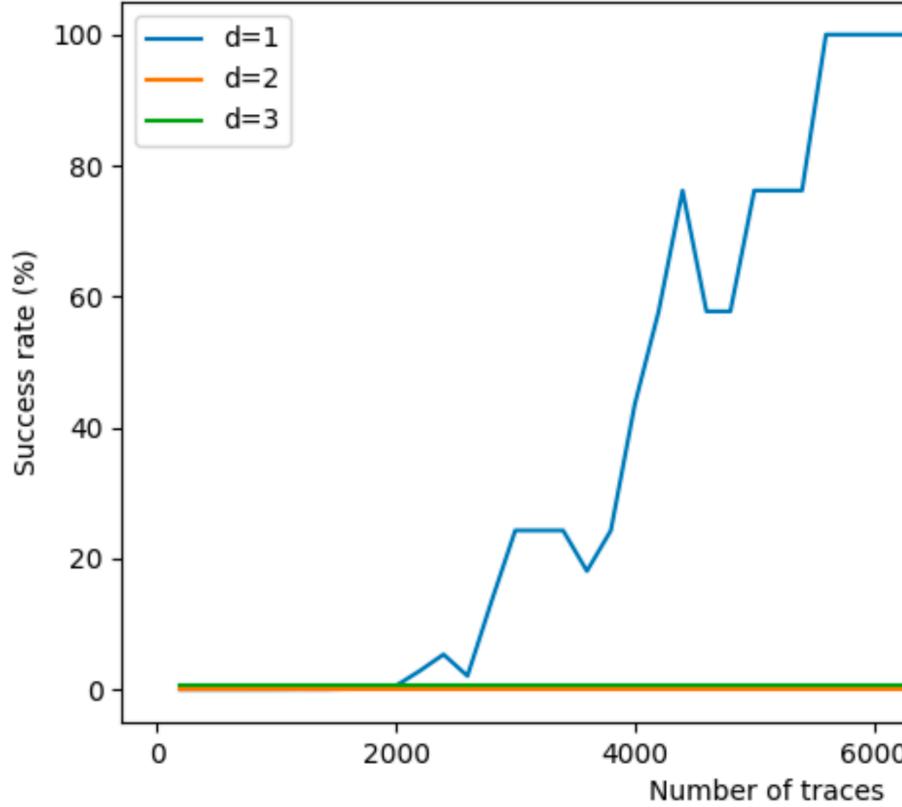
viet.sang.nguyen@univ-st-etienne.fr







Results of full key recovery



Viet-Sang Nguyen

viet.sang.nguyen@univ-st-etienne.fr

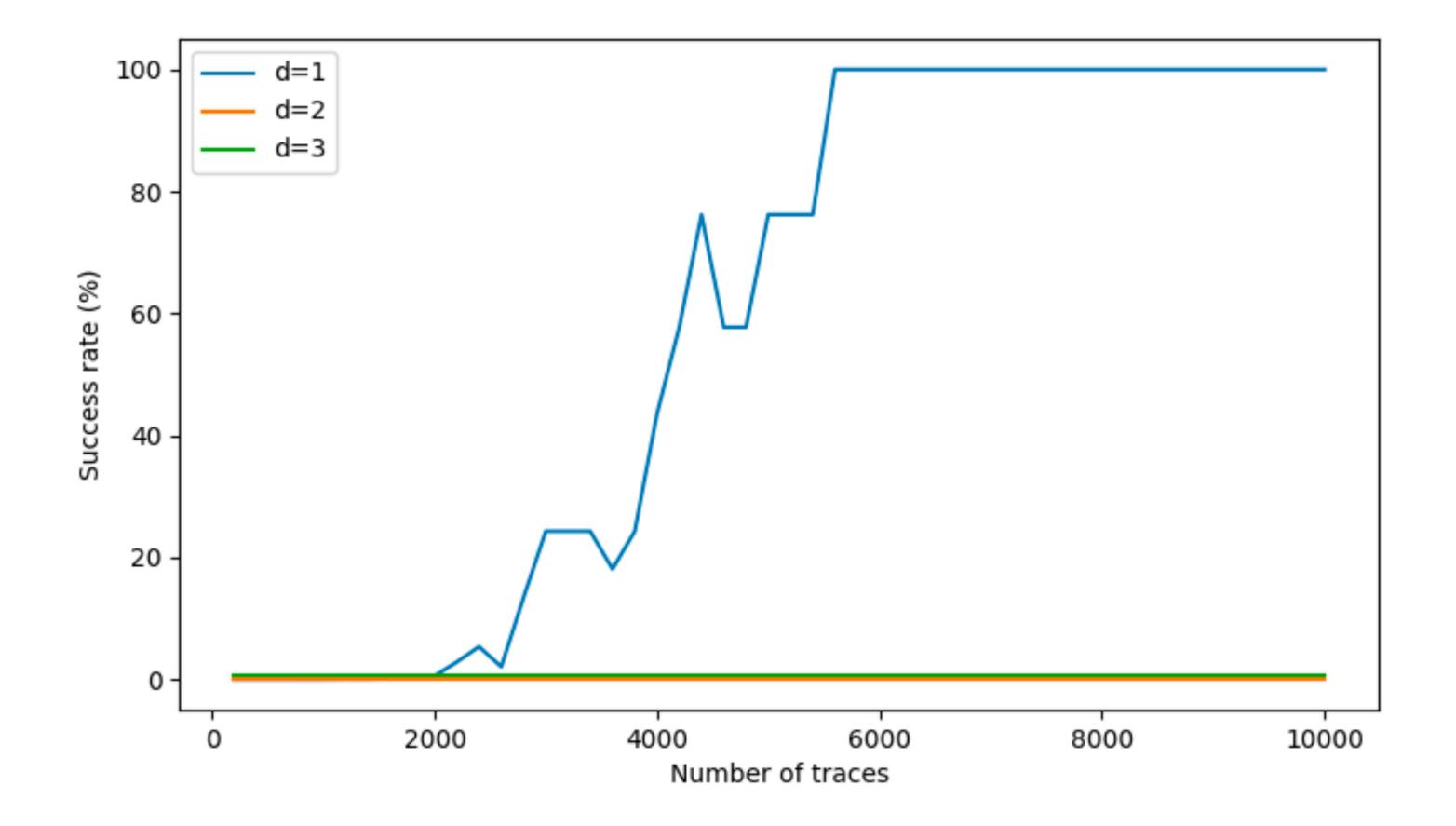


)	8000	10000





Results of full key recovery



Viet-Sang Nguyen

viet.sang.nguyen@univ-st-etienne.fr





CPA on Ascon with Multi-bit Selection Function

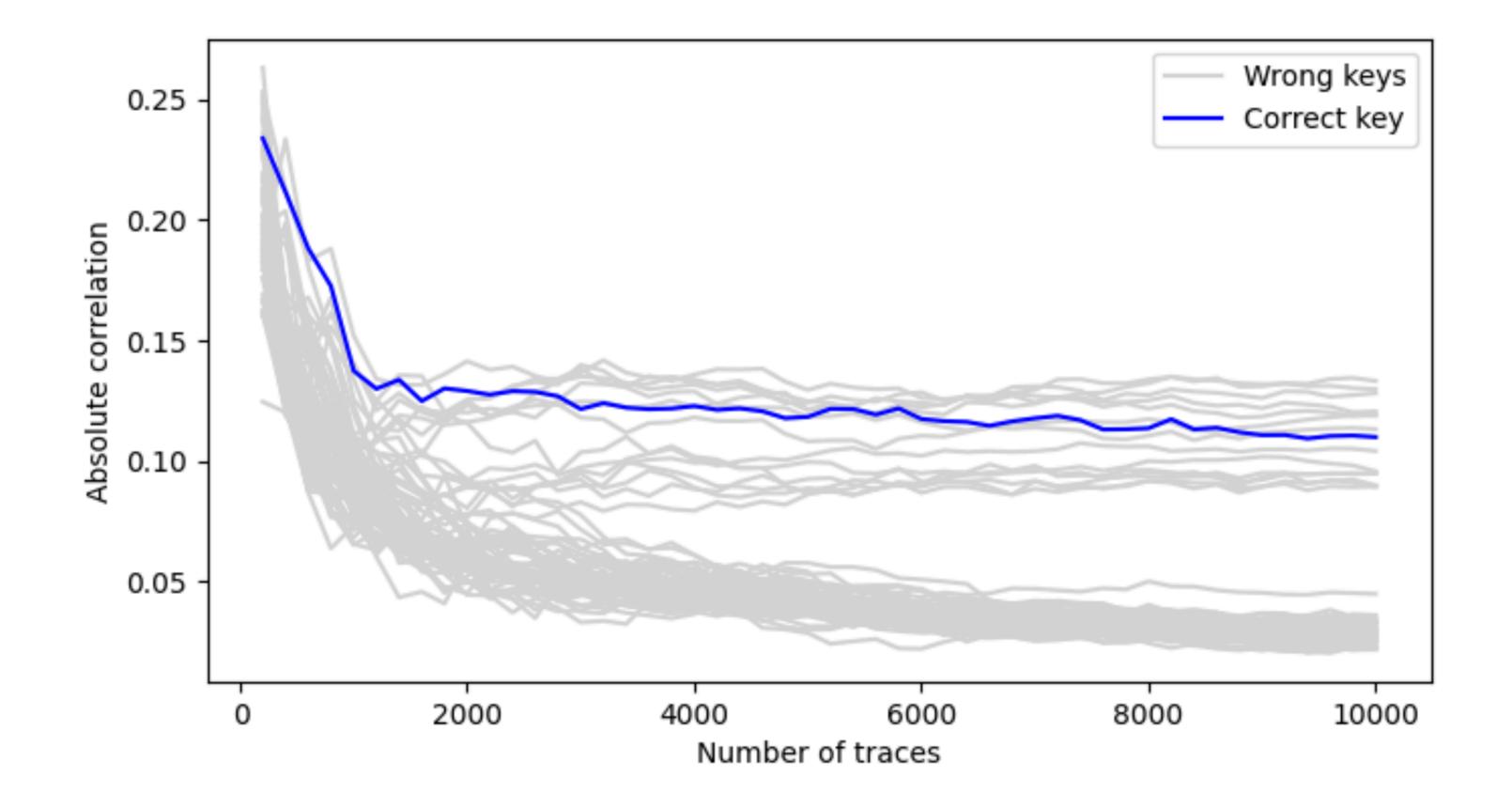




viet.sang.nguyen@univ-st-etienne.fr

CPA on Ascon with Multi-bit Selection Function



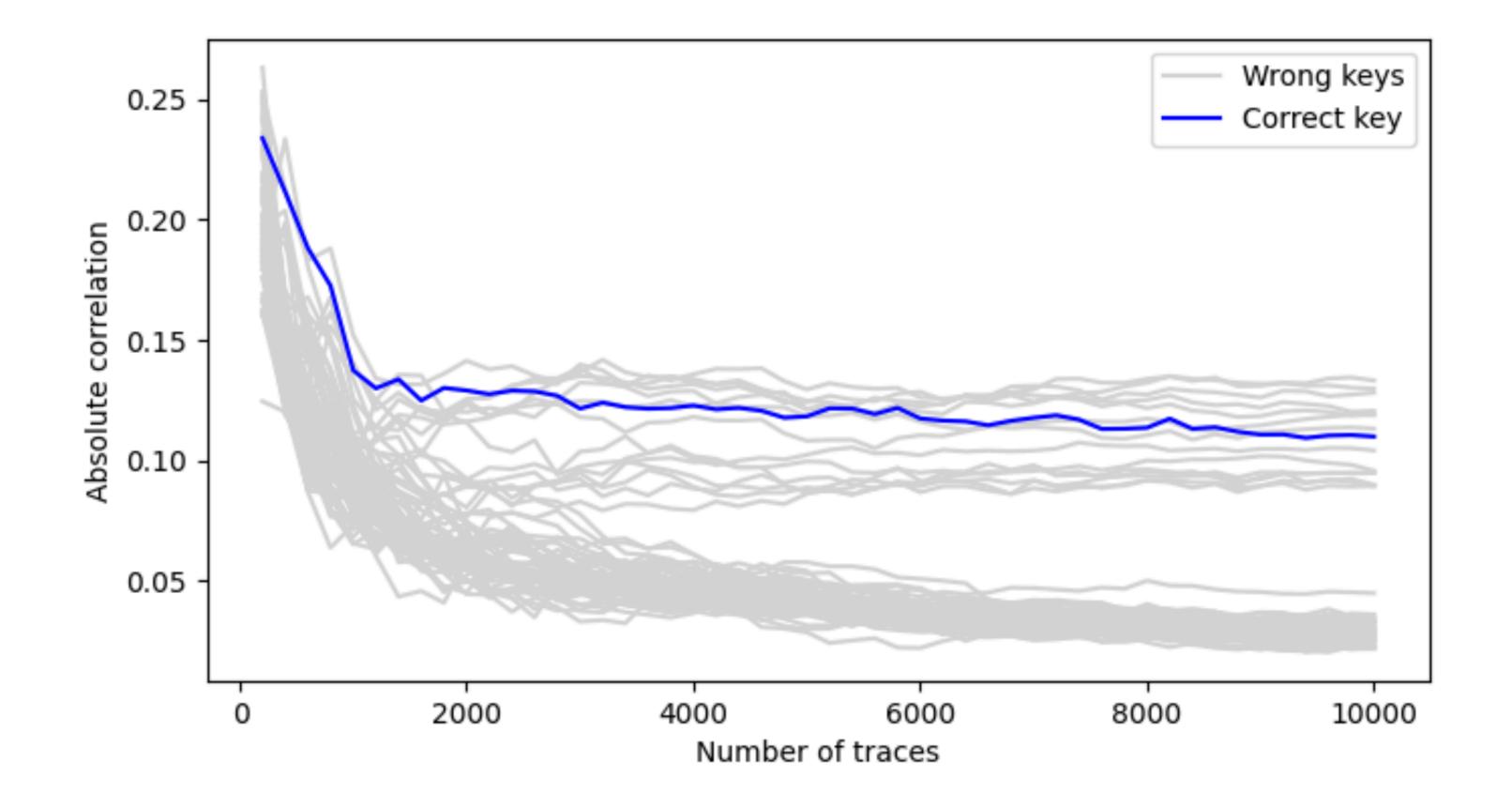


Viet-Sang Nguyen

viet.sang.nguyen@univ-st-etienne.fr

CPA on Ascon with Multi-bit Selection Function





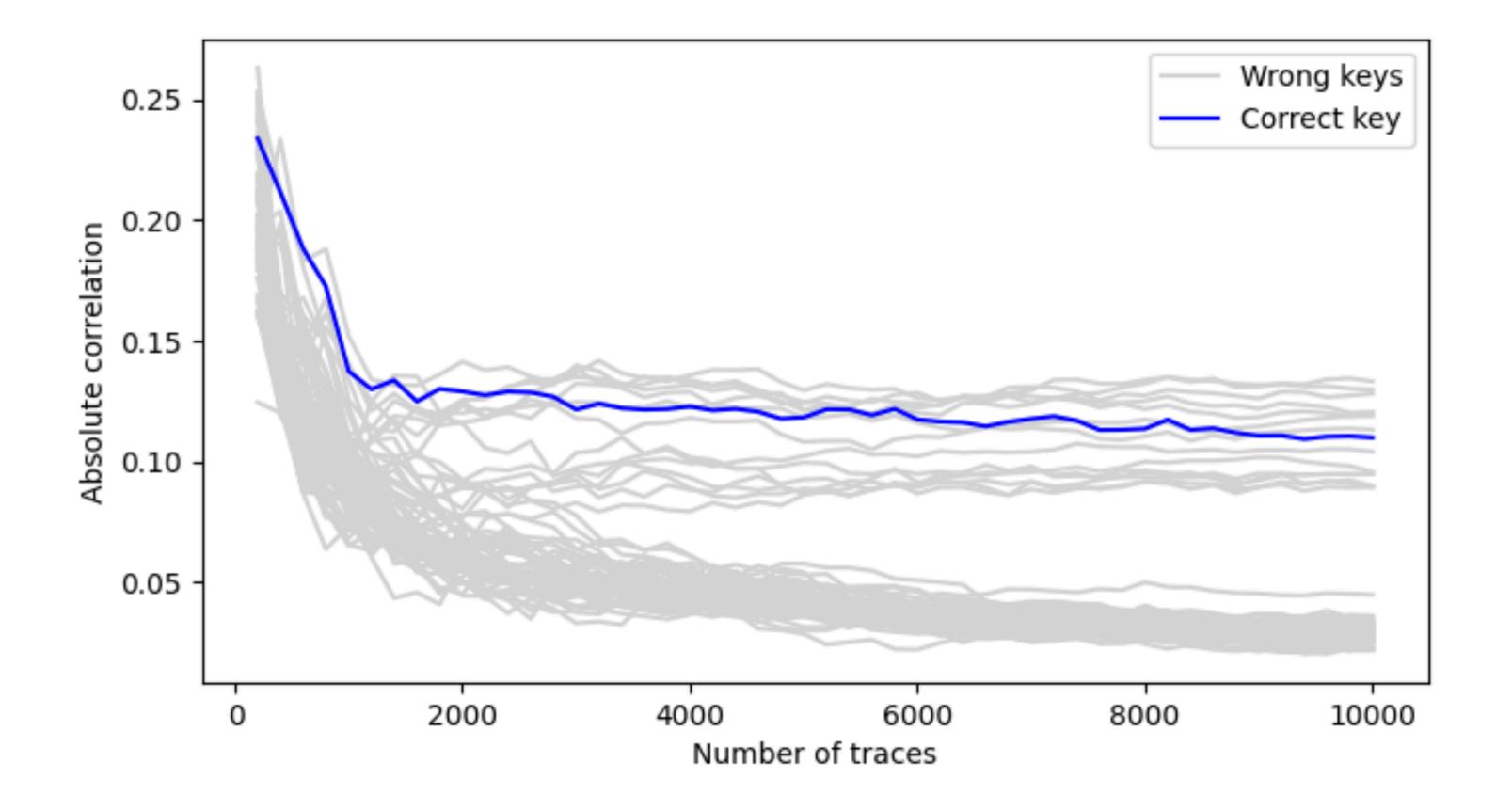
Viet-Sang Nguyen

viet.sang.nguyen@univ-st-etienne.fr

Expected: correct key is distinguished

CPA on Ascon with Multi-bit Selection Function





Viet-Sang Nguyen

viet.sang.nguyen@univ-st-etienne.fr

Expected: correct key is distinguished

Observed: a group of keys is distinguished

CPA on Ascon with Multi-bit Selection Function



viet.sang.nguyen@univ-st-etienne.fr

Expected: correct key is distinguished

Observed: a group of keys is distinguished



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

Viet-Sang Nguyen

viet.sang.nguyen@univ-st-etienne.fr

Expected: correct key is distinguished

Observed: a group of keys is distinguished



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

Viet-Sang Nguyen

viet.sang.nguyen@univ-st-etienne.fr

Expected: correct key is distinguished

Observed: a group of keys is distinguished



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

Viet-Sang Nguyen

viet.sang.nguyen@univ-st-etienne.fr

Expected: correct key is distinguished

Observed: a group of keys is distinguished

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





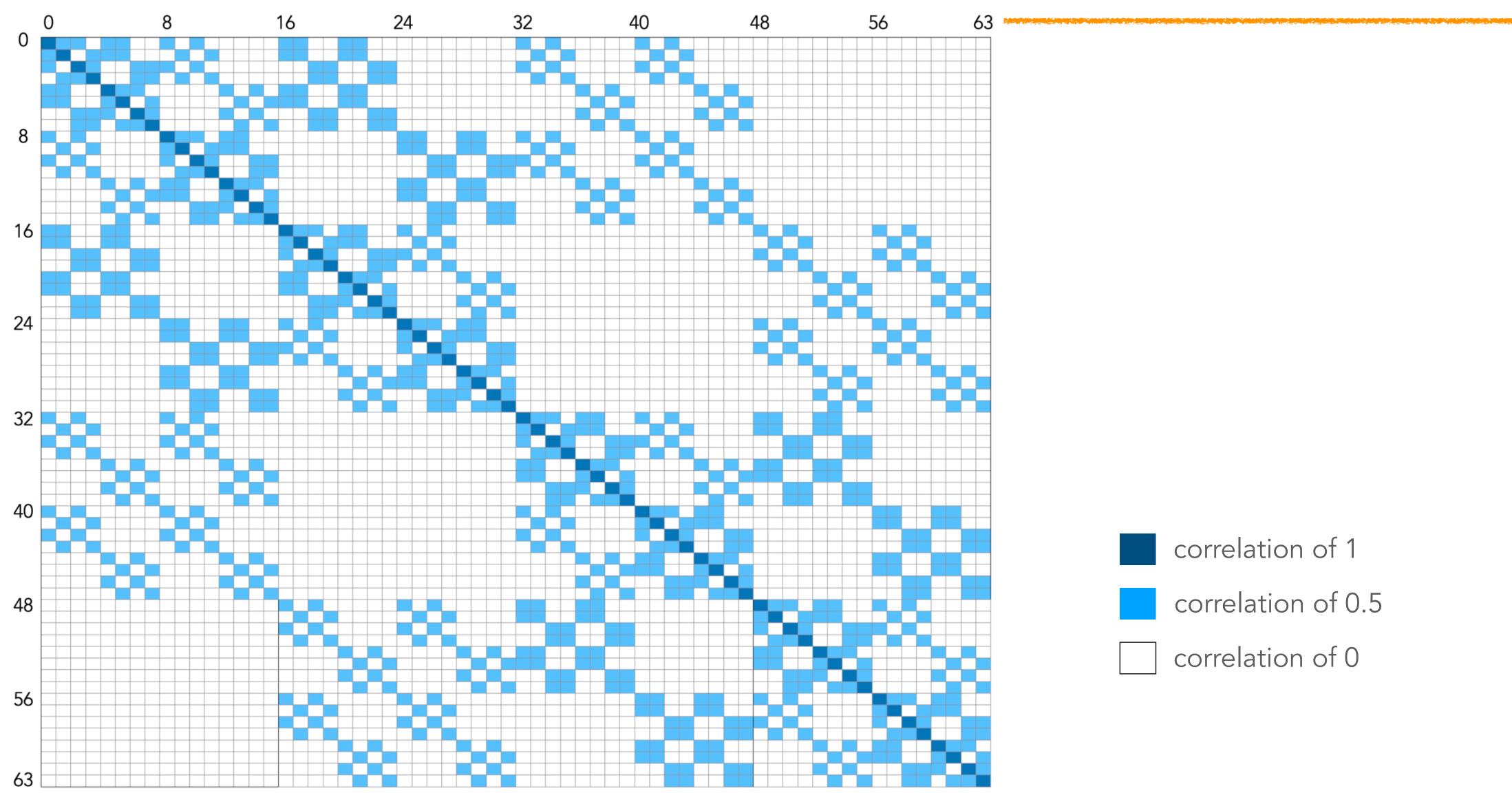
Correlations between distributions of all key pairs

Viet-Sang Nguyen

viet.sang.nguyen@univ-st-etienne.fr



Correlations between distributions of all key pairs

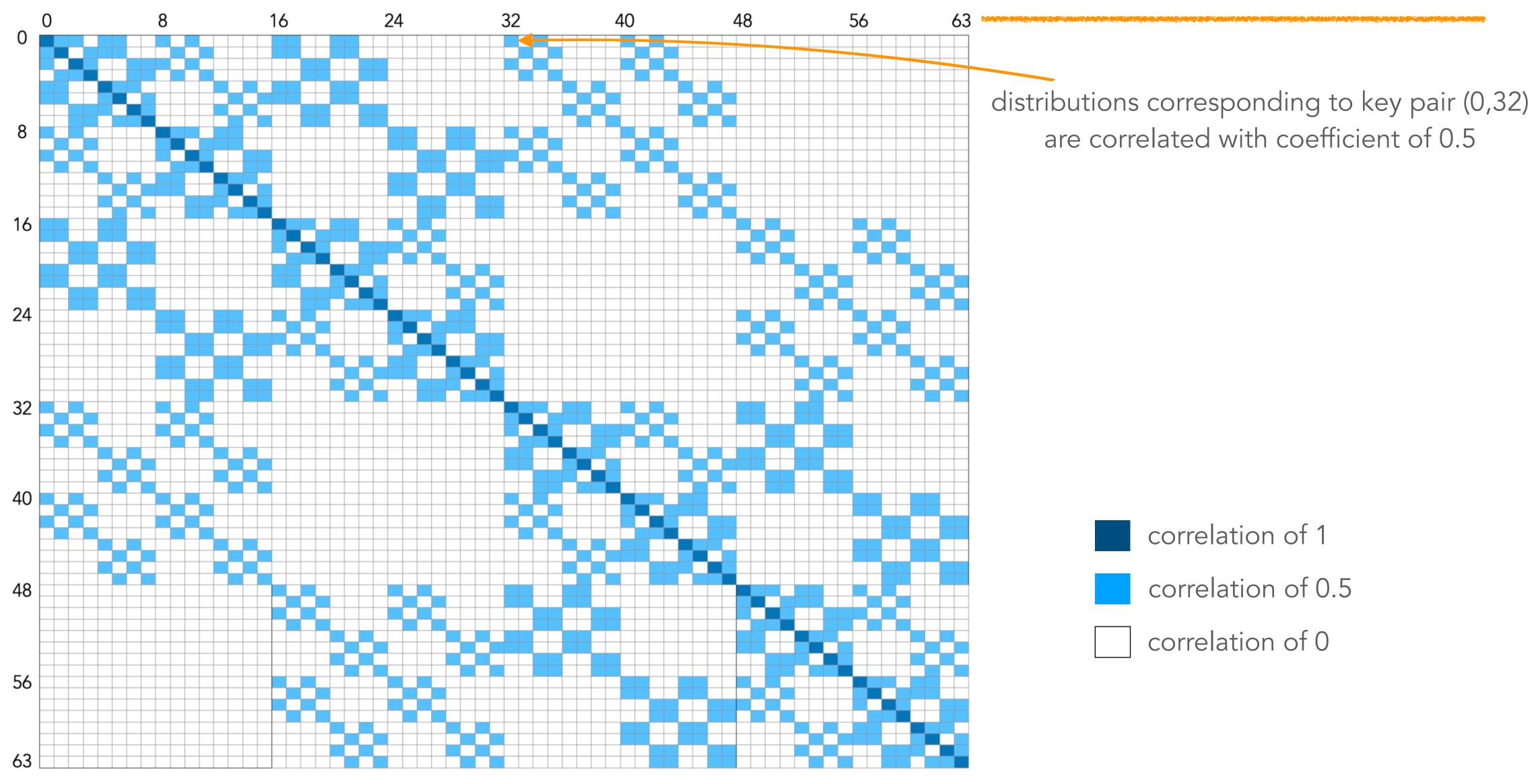


Viet-Sang Nguyen

viet.sang.nguyen@univ-st-etienne.fr



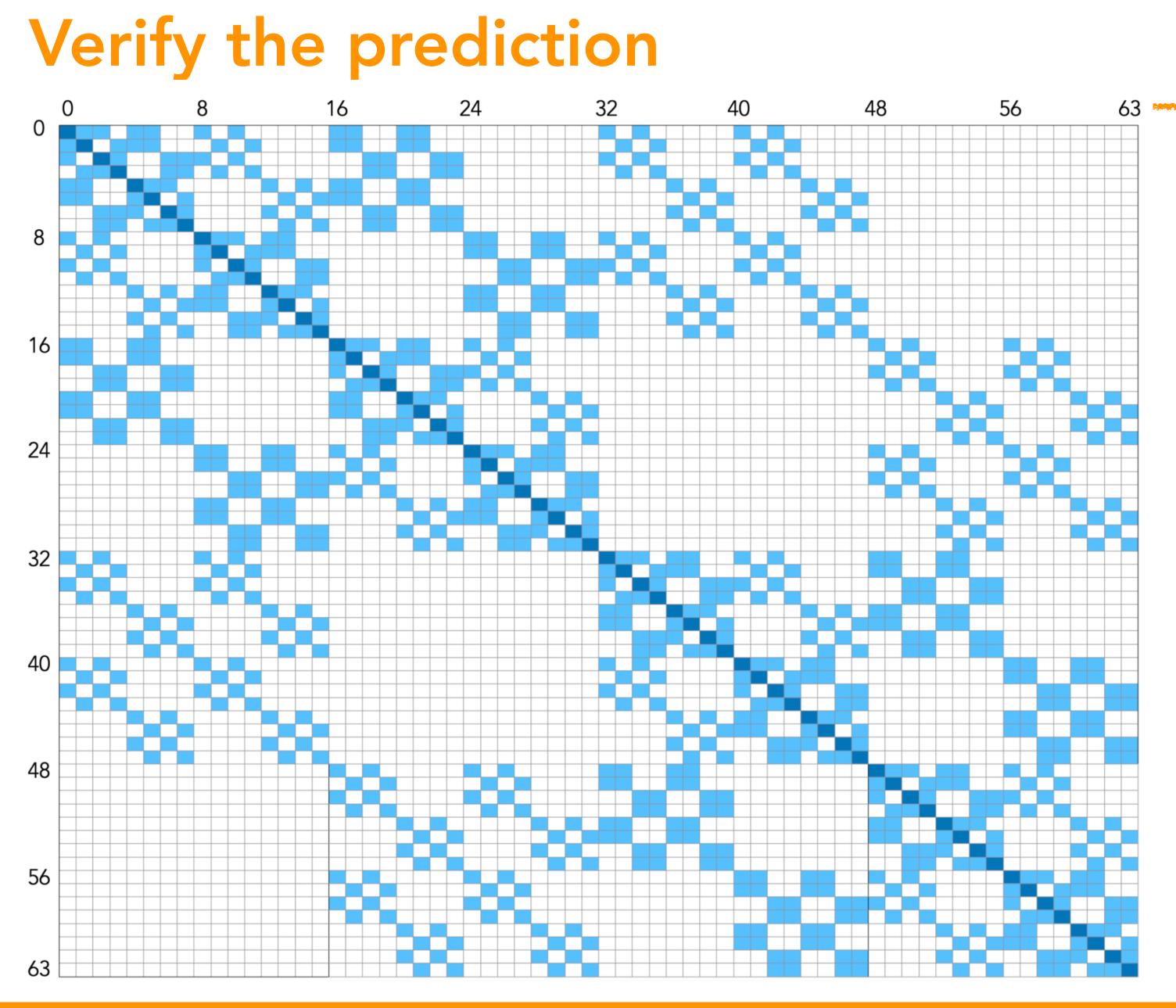
Correlations between distributions of all key pairs



Viet-Sang Nguyen

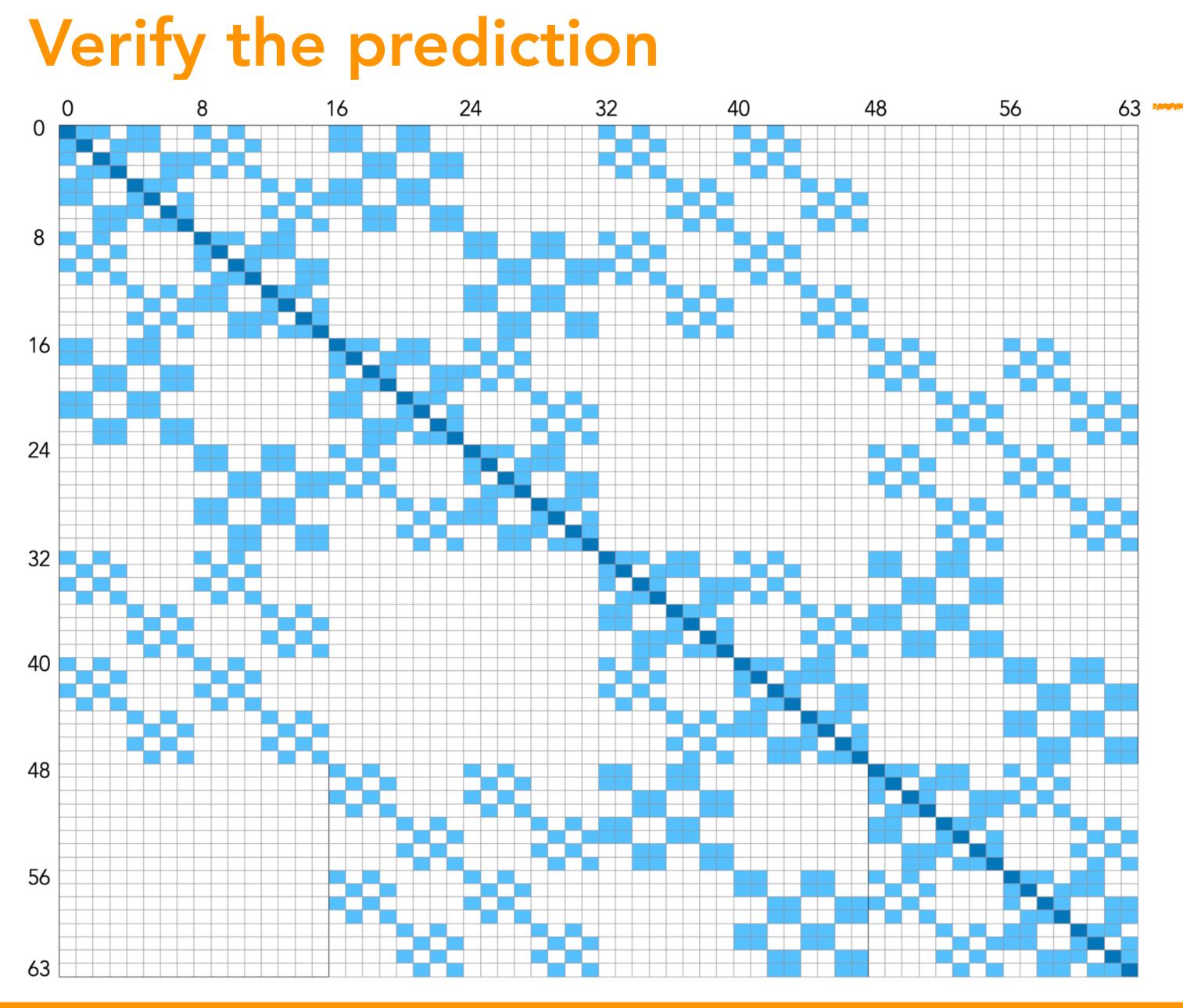
viet.sang.nguyen@univ-st-etienne.fr

CPA on Ascon with Multi-bit Selection Function



viet.sang.nguyen@univ-st-etienne.fr

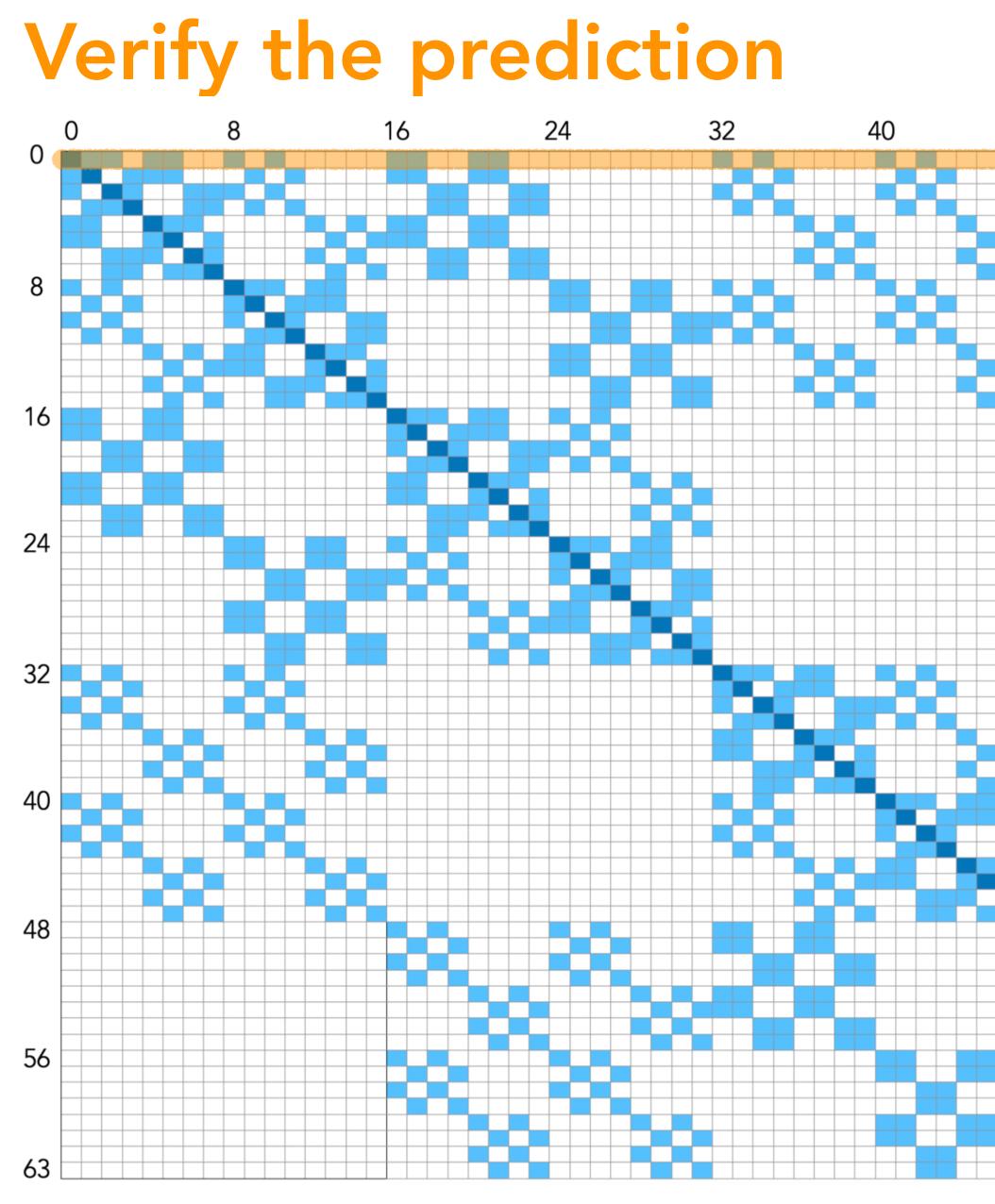




viet.sang.nguyen@univ-st-etienne.fr

Rank	Key	Corr.	Rank	Key	Corr.
1	10	0.133	33	<u>6</u>	0.030
2	32	0.133	33	26	0.030
3	2	0.130	35	20	0.030
3 4	42	0.128	36	35	0.030
4 5	42 40	0.121	30	53	0.029
5 6	40 8	0.119	37	55 55	0.029
0 7	-	0.119		33 44	
8	34 0	0.113	39 40	44 3	0.028 0.028
o 9	1	0.104	40	57	
9 10	5				0.028
10	3 4	0.096 0.095	42 43	50 45	0.028 0.028
11	4 17	0.095	43	43 37	0.028
12	16	0.093	44	41	0.027
13	21	0.090	43	12	0.027
14	$\frac{21}{20}$	0.089	40	46	0.020
15	31	0.089	48	40	0.020
10	60	0.045	40	33	0.020
17	61	0.035	50	55	0.020
19	15	0.035	51	47	0.026
20	23	0.033	52	58	0.026
20	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





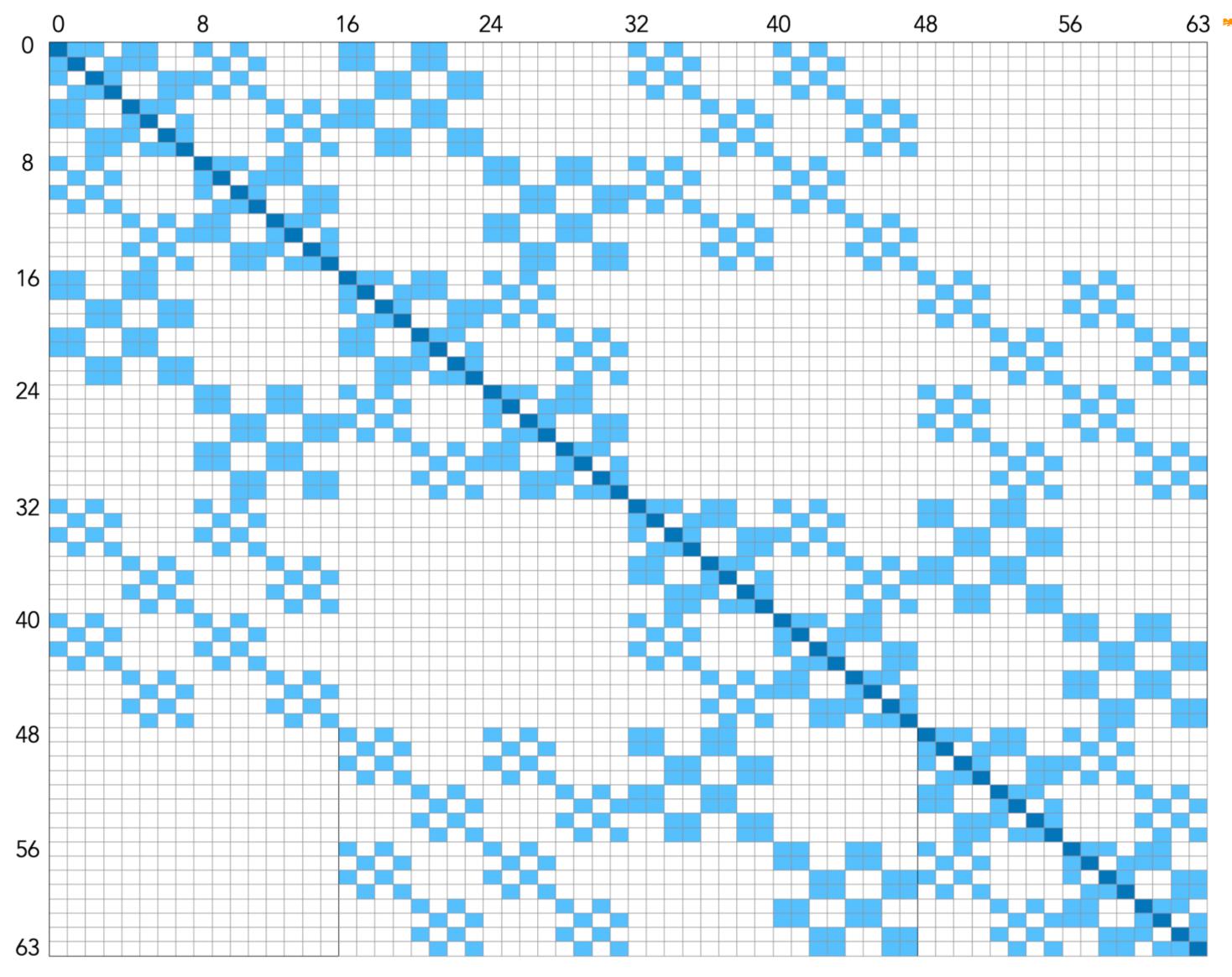
viet.sang.nguyen@univ-st-etienne.fr

48	56	63	lieters have a little of			ookeen oo tokuda		
			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 ?



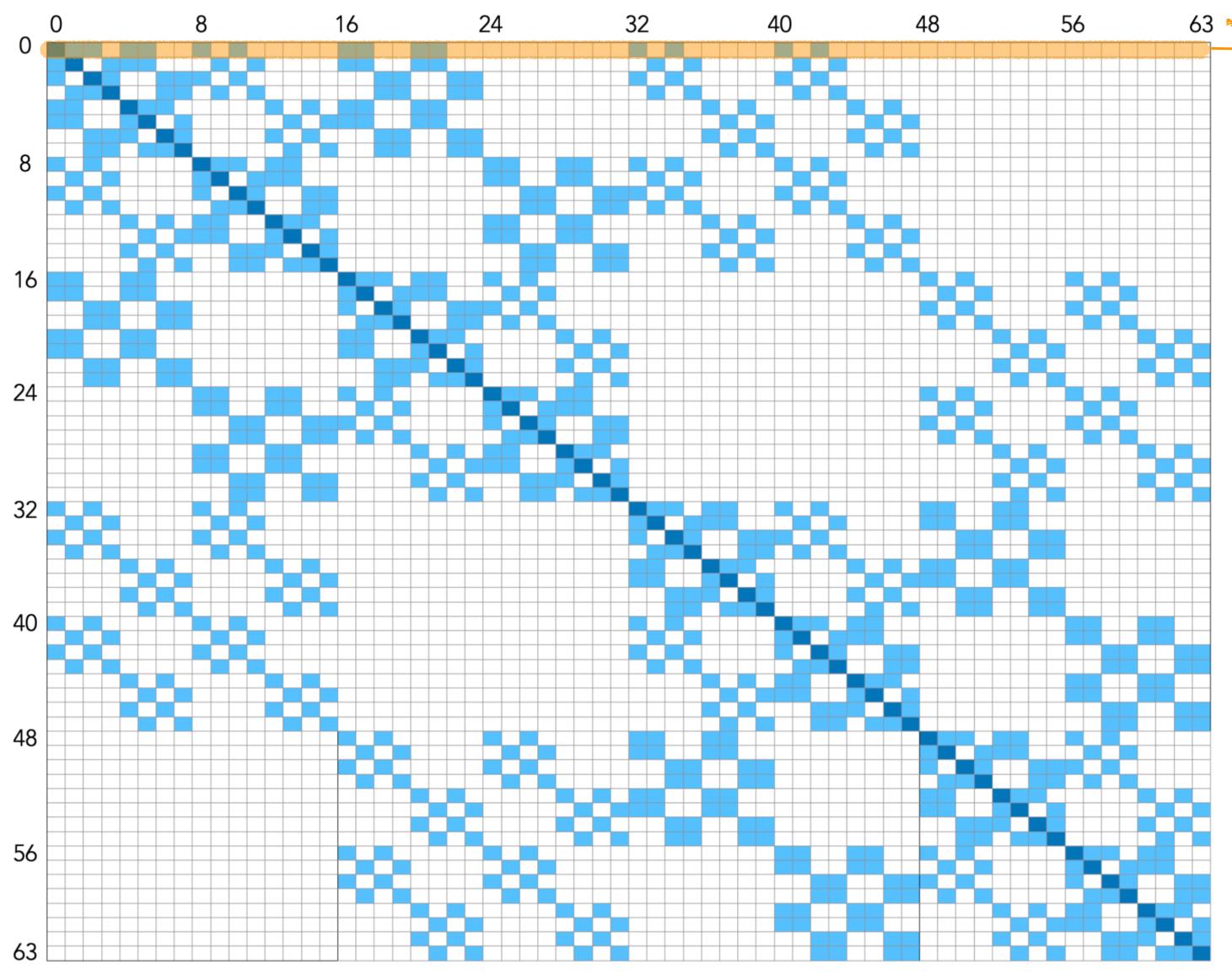


Viet-Sang Nguyen

viet.sang.nguyen@univ-st-etienne.fr







Viet-Sang Nguyen

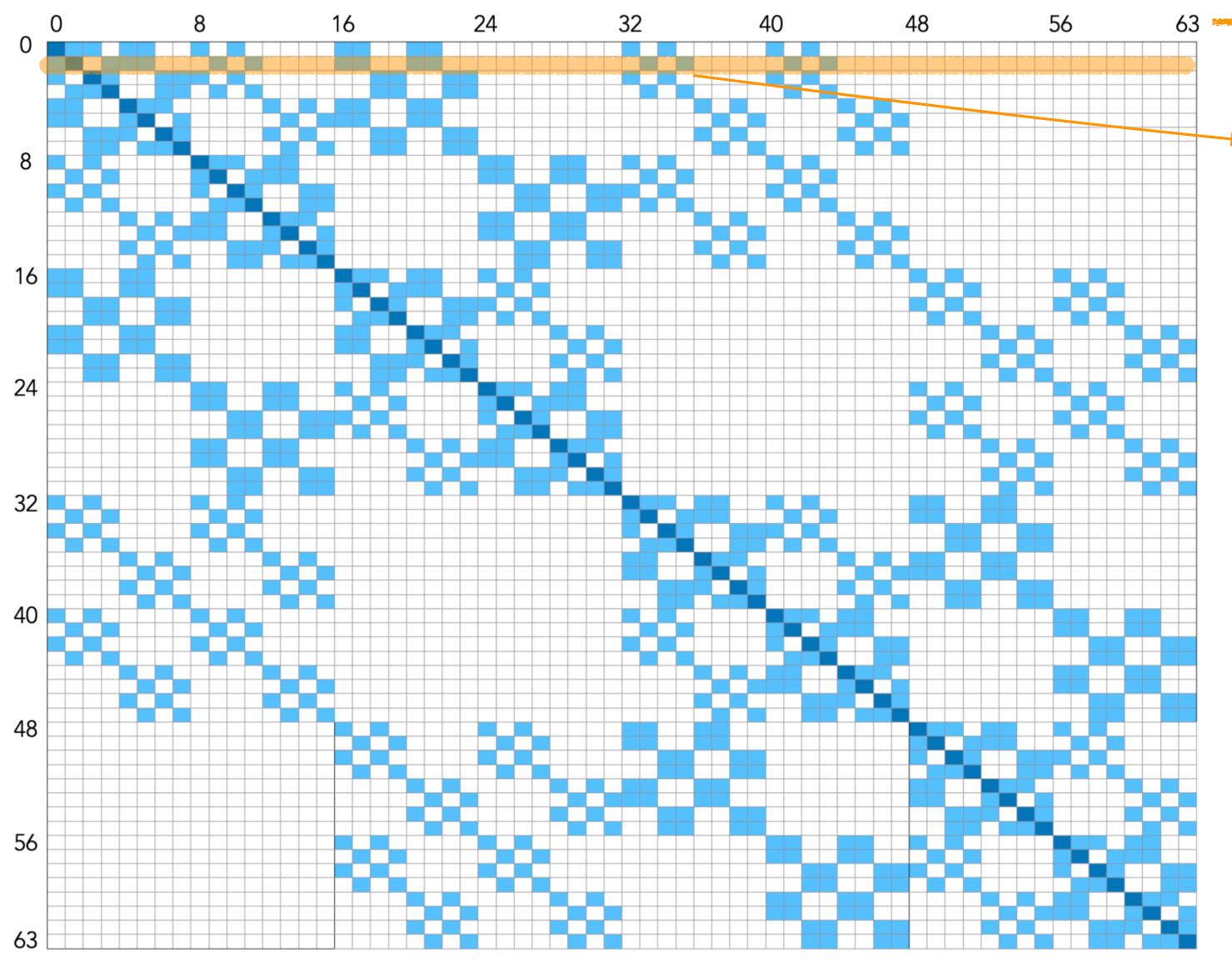
viet.sang.nguyen@univ-st-etienne.fr



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





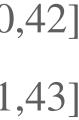


Viet-Sang Nguyen

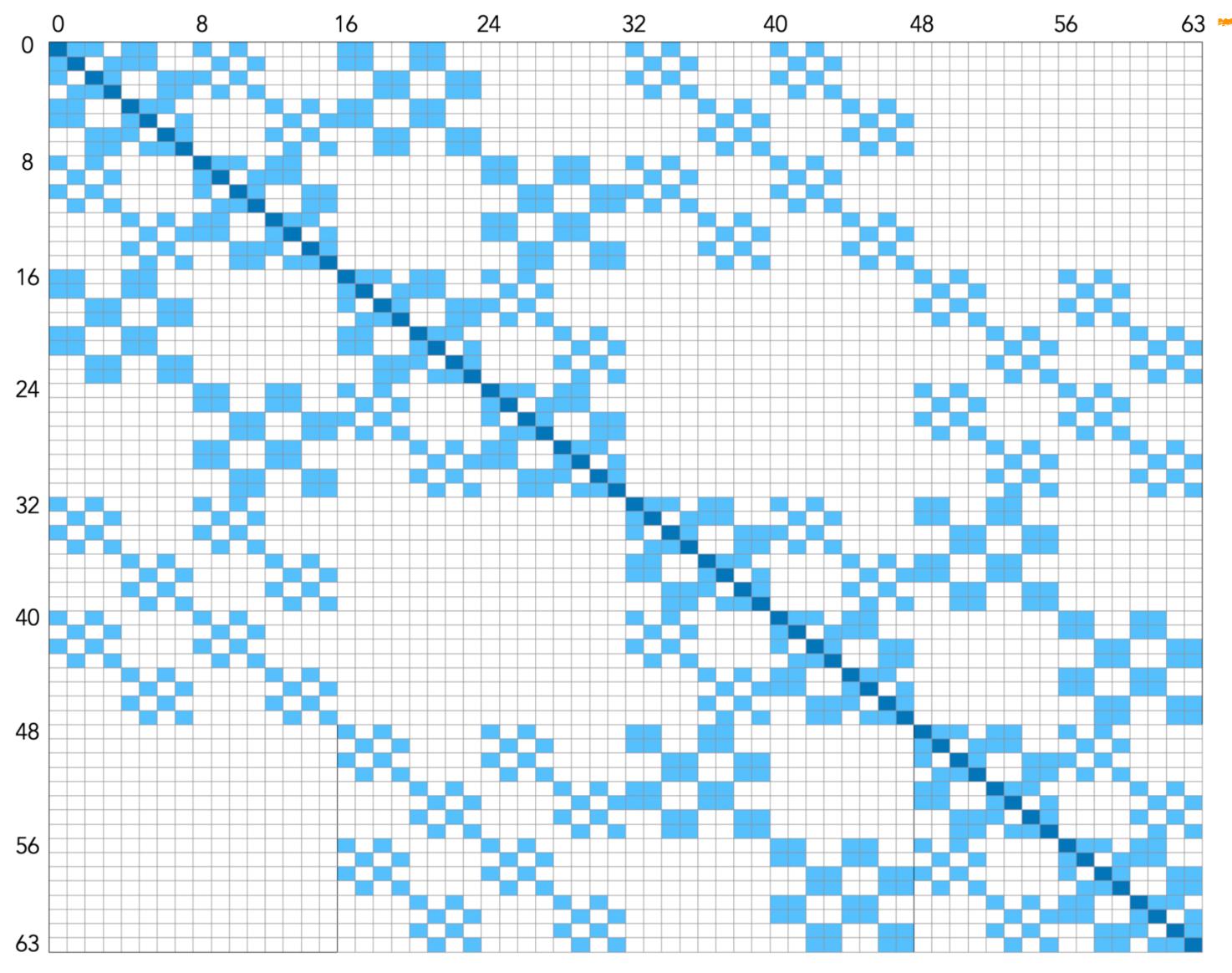
viet.sang.nguyen@univ-st-etienne.fr



$\mathscr{G}[0] = [0,1,2,4,5,8,10,16,17,20,21,32,34,40,42]$ $\mathscr{G}[1] = [0,1,3,4,5,9,11,16,17,20,21,33,35,41,43]$





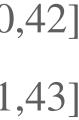


Viet-Sang Nguyen

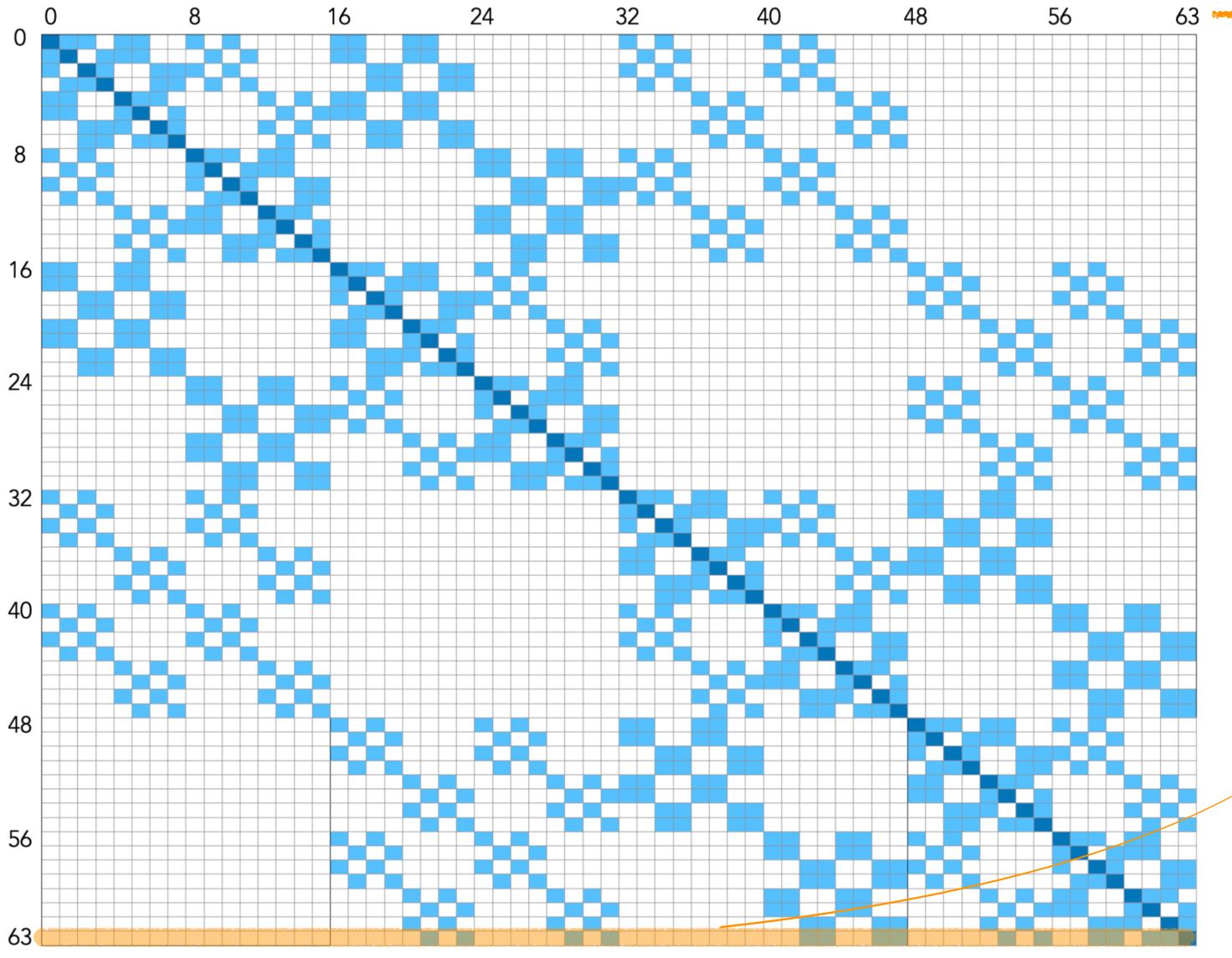
viet.sang.nguyen@univ-st-etienne.fr



$\mathscr{G}[0] = [0,1,2,4,5,8,10,16,17,20,21,32,34,40,42]$ $\mathscr{G}[1] = [0,1,3,4,5,9,11,16,17,20,21,33,35,41,43]$







Viet-Sang Nguyen

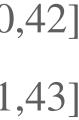
viet.sang.nguyen@univ-st-etienne.fr



 $\mathscr{G}[0] = [0,1,2,4,5,8,10,16,17,20,21,32,34,40,42]$ $\mathscr{G}[1] = [0,1,3,4,5,9,11,16,17,20,21,33,35,41,43]$

 $\mathscr{G}[63] = [\dots]$

• • •





Viet-Sang Nguyen

viet.sang.nguyen@univ-st-etienne.fr

alation and a sure of the second	Low The South	A CONTRACTOR OF A CONTRACT	malie and and the second	Georgeo de Care	a part and the second of the
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

CPA on Ascon with Multi-bit Selection Function



Which group does these key candid correspond to ?

Viet-Sang Nguyen

viet.sang.nguyen@univ-st-etienne.fr

₩₿₺ġ₿₽₽₩₩₽₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩	dielen ander siderer		en anter a la contra de la contra	redeenen anterio de la	Severation de Fritze	an ann an an airte an Anna an A
	Rank	Key	Corr.	Rank	Key	Corr.
idataa	1	10	0.133	33	6	0.030
idates	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

CPA on Ascon with Multi-bit Selection Function



Which group does these key candid correspond to ?

 $\mathscr{G}[1]$

Viet-Sang Nguyen

viet.sang.nguyen@univ-st-etienne.fr

	Rank	Key	Corr.	Rank	Key	Corr.
dataa	1	10	0.133	33	6	0.030
dates	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

CPA on Ascon with Multi-bit Selection Function



Which group does these key candid correspond to ?

$\mathscr{G}[1]$

Viet-Sang Nguyen

viet.sang.nguyen@univ-st-etienne.fr

	Rank	Key	Corr.	Rank	Key	Corr.
dataa	1	10	0.133	33	6	0.030
dates	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

CPA on Ascon with Multi-bit Selection Function



Which group does these key candid correspond to ?



Viet-Sang Nguyen

viet.sang.nguyen@univ-st-etienne.fr

	Rank	Key	Corr.	Rank	Key	Corr.
dataa	1	10	0.133	33	6	0.030
dates	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

CPA on Ascon with Multi-bit Selection Function



Which group does these key candid correspond to ?



Viet-Sang Nguyen

viet.sang.nguyen@univ-st-etienne.fr

	Rank	Key	Corr.	Rank	Key	Corr.
dataa	1	10	0.133	33	6	0.030
dates	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

CPA on Ascon with Multi-bit Selection Function



Which group does these key candid correspond to ?



Viet-Sang Nguyen

viet.sang.nguyen@univ-st-etienne.fr

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 0.119 37 53 0.029 5 40 0.119 37 53 0.029 6 8 0.110 38 55 0.029 7 34 0.113 39 44 0.028 9 1 0.104 41 57 0.028 10 5 0.096 42 50 0.028 11 4 0.095 44 37 0.027 13 16 0.090 45 41 0.026 12 17 0.095 44 37 0.026 15 20 0.089 47 46 0.026 1		diet		en de la compañía de	esterence atomiciati	-	an prins a star and a s
Clates 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 6 8 0.113 39 44 0.028 8 0 0.110 40 3 0.028 9 1 0.104 41 57 0.028 10 5 0.095 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 17 60 0.035 50 54 0.026 19 15 0.035 51 47 0.026 20 23 0.034 52 58 0.026 21		Rank	Key		Rank	Key	
$\begin{array}{c ccccccccccccccccccccccccccccccccccc$	idator				33	6	
$ \begin{array}{c ccccccccccccccccccccccccccccccccccc$	Idates		32	0.130	34	26	
$ \begin{array}{cccccccccccccccccccccccccccccccccccc$		3	2	0.128	35	27	0.030
$ \begin{array}{cccccccccccccccccccccccccccccccccccc$			42	0.121	36	35	0.029
$\begin{array}{cccccccccccccccccccccccccccccccccccc$		5	40	0.119	37	53	0.029
$\begin{array}{c ccccccccccccccccccccccccccccccccccc$			8	0.119	38	55	0.029
$\begin{array}{c ccccccccccccccccccccccccccccccccccc$			34	0.113	39	44	
$ \begin{array}{c ccccccccccccccccccccccccccccccccccc$		8	0	0.110	40	3	0.028
$ \begin{array}{cccccccccccccccccccccccccccccccccccc$		9			41	57	
$\begin{array}{c ccccccccccccccccccccccccccccccccccc$		10	5		42	50	
$ \begin{array}{cccccccccccccccccccccccccccccccccccc$							
$ \begin{array}{c ccccccccccccccccccccccccccccccccccc$			17			37	
$ \begin{array}{c ccccccccccccccccccccccccccccccccccc$					45		
$ \begin{array}{cccccccccccccccccccccccccccccccccccc$						12	
$ \begin{array}{cccccccccccccccccccccccccccccccccccc$							
$\begin{array}{c ccccccccccccccccccccccccccccccccccc$		16	31			49	
$\begin{array}{cccccccccccccccccccccccccccccccccccc$				I		33	
$\begin{array}{c ccccccccccccccccccccccccccccccccccc$		18	61		50	54	
$\begin{array}{c ccccccccccccccccccccccccccccccccccc$		19	15	I	51	47	
$\begin{array}{c ccccccccccccccccccccccccccccccccccc$		20	23	I	52	58	
$\begin{array}{cccccccccccccccccccccccccccccccccccc$		21	11		53	48	
$\begin{array}{c ccccccccccccccccccccccccccccccccccc$		22	19	0.033	54	62	0.026
$\begin{array}{cccccccccccccccccccccccccccccccccccc$		23	22	0.033	55	13	0.025
$\begin{array}{cccccccccccccccccccccccccccccccccccc$		24	39	0.033	56	28	0.025
$\begin{array}{cccccccccccccccccccccccccccccccccccc$		25	7	0.033	57	24	0.025
$\begin{array}{cccccccccccccccccccccccccccccccccccc$		26	43	0.032	58	25	0.023
29140.03061380.02330300.03062630.02231360.0306390.022		27	18	0.032	59	59	0.023
30300.03062630.02231360.0306390.022		28	56	0.031	60	51	0.023
31 36 0.030 63 9 0.022		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 32 0.030 OT 29 0.022		32	52	0.030	64	29	0.022

CPA on Ascon with Multi-bit Selection Function



Which group does these key candid correspond to ?



Viet-Sang Nguyen

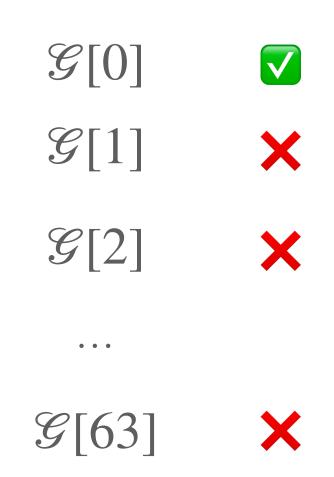
viet.sang.nguyen@univ-st-etienne.fr

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 0.119 37 53 0.029 5 40 0.119 37 53 0.029 6 8 0.110 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 44 45 0.026 12 17 0.095 44 45 0.026 15 20 0.089 47 46 0.026 16 </th <th></th> <th>diet</th> <th></th> <th>en de la compañía de</th> <th>esterence atomiciati</th> <th>B. C. Tomaticates</th> <th>an prins a star and a s</th>		diet		en de la compañía de	esterence atomiciati	B. C. Tomaticates	an prins a star and a s
Clates 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 6 8 0.113 39 44 0.028 8 0 0.110 40 3 0.028 9 1 0.104 41 57 0.028 10 5 0.095 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 17 60 0.035 50 54 0.026 19 15 0.035 51 47 0.026 20 23 0.034 52 58 0.026 21		Rank	Key		Rank	Key	
$\begin{array}{c ccccccccccccccccccccccccccccccccccc$	idator				33	6	
$ \begin{array}{c ccccccccccccccccccccccccccccccccccc$	Idates		32	0.130	34	26	
$ \begin{array}{cccccccccccccccccccccccccccccccccccc$		3	2	0.128	35	27	0.030
$ \begin{array}{cccccccccccccccccccccccccccccccccccc$			42	0.121	36	35	0.029
$\begin{array}{cccccccccccccccccccccccccccccccccccc$		5	40	0.119	37	53	0.029
$\begin{array}{c ccccccccccccccccccccccccccccccccccc$			8	0.119	38	55	0.029
$\begin{array}{c ccccccccccccccccccccccccccccccccccc$			34	0.113	39	44	
$ \begin{array}{c ccccccccccccccccccccccccccccccccccc$		8	0	0.110	40	3	0.028
$ \begin{array}{cccccccccccccccccccccccccccccccccccc$		9			41	57	
$\begin{array}{c ccccccccccccccccccccccccccccccccccc$		10	5		42	50	
$ \begin{array}{cccccccccccccccccccccccccccccccccccc$							
$ \begin{array}{c ccccccccccccccccccccccccccccccccccc$			17			37	
$ \begin{array}{c ccccccccccccccccccccccccccccccccccc$					45		
$ \begin{array}{cccccccccccccccccccccccccccccccccccc$						12	
$ \begin{array}{cccccccccccccccccccccccccccccccccccc$							
$\begin{array}{c ccccccccccccccccccccccccccccccccccc$		16	31			49	
$\begin{array}{cccccccccccccccccccccccccccccccccccc$				I		33	
$\begin{array}{c ccccccccccccccccccccccccccccccccccc$		18	61		50	54	
$\begin{array}{c ccccccccccccccccccccccccccccccccccc$		19	15	I	51	47	
$\begin{array}{c ccccccccccccccccccccccccccccccccccc$		20	23	I	52	58	
$\begin{array}{cccccccccccccccccccccccccccccccccccc$		21	11	I	53	48	
$\begin{array}{c ccccccccccccccccccccccccccccccccccc$		22	19	0.033	54	62	0.026
$\begin{array}{cccccccccccccccccccccccccccccccccccc$		23	22	0.033	55	13	0.025
$\begin{array}{cccccccccccccccccccccccccccccccccccc$		24	39	0.033	56	28	0.025
$\begin{array}{cccccccccccccccccccccccccccccccccccc$		25	7	0.033	57	24	0.025
$\begin{array}{cccccccccccccccccccccccccccccccccccc$		26	43	0.032	58	25	0.023
29140.03061380.02330300.03062630.02231360.0306390.022		27	18	0.032	59	59	0.023
30300.03062630.02231360.0306390.022		28	56	0.031	60	51	0.023
31 36 0.030 63 9 0.022		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 32 0.030 OT 29 0.022		32	52	0.030	64	29	0.022

CPA on Ascon with Multi-bit Selection Function



Which group does these key candid correspond to ?



Viet-Sang Nguyen

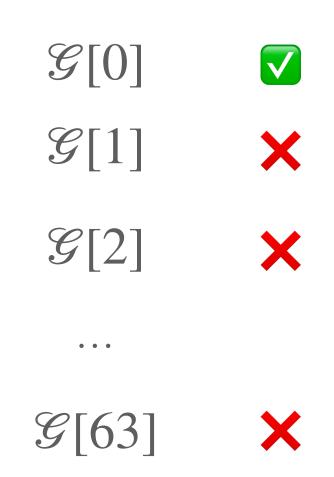
viet.sang.nguyen@univ-st-etienne.fr

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 0.119 37 53 0.029 5 40 0.119 37 53 0.029 6 8 0.110 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 44 45 0.026 12 17 0.095 44 45 0.026 15 20 0.089 47 46 0.026 16 </th <th></th> <th>diet</th> <th></th> <th>en de la compañía de</th> <th>esterence atomiciati</th> <th>B. C. Tomaticates</th> <th>an prins a star and a s</th>		diet		en de la compañía de	esterence atomiciati	B. C. Tomaticates	an prins a star and a s
Clates 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 6 8 0.113 39 44 0.028 8 0 0.110 40 3 0.028 9 1 0.104 41 57 0.028 10 5 0.095 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 17 60 0.035 50 54 0.026 19 15 0.035 51 47 0.026 20 23 0.034 52 58 0.026 21		Rank	Key		Rank	Key	
$\begin{array}{c ccccccccccccccccccccccccccccccccccc$	idator				33	6	
$ \begin{array}{c ccccccccccccccccccccccccccccccccccc$	Idates		32	0.130	34	26	
$ \begin{array}{cccccccccccccccccccccccccccccccccccc$		3	2	0.128	35	27	0.030
$ \begin{array}{cccccccccccccccccccccccccccccccccccc$			42	0.121	36	35	0.029
$\begin{array}{cccccccccccccccccccccccccccccccccccc$		5	40	0.119	37	53	0.029
$\begin{array}{c ccccccccccccccccccccccccccccccccccc$			8	0.119	38	55	0.029
$\begin{array}{c ccccccccccccccccccccccccccccccccccc$			34	0.113	39	44	
$ \begin{array}{c ccccccccccccccccccccccccccccccccccc$		8	0	0.110	40	3	0.028
$ \begin{array}{cccccccccccccccccccccccccccccccccccc$		9			41	57	
$\begin{array}{c ccccccccccccccccccccccccccccccccccc$		10	5		42	50	
$ \begin{array}{cccccccccccccccccccccccccccccccccccc$							
$ \begin{array}{c ccccccccccccccccccccccccccccccccccc$			17			37	
$ \begin{array}{c ccccccccccccccccccccccccccccccccccc$					45		
$ \begin{array}{cccccccccccccccccccccccccccccccccccc$						12	
$ \begin{array}{cccccccccccccccccccccccccccccccccccc$							
$\begin{array}{c ccccccccccccccccccccccccccccccccccc$		16	31			49	
$\begin{array}{cccccccccccccccccccccccccccccccccccc$				I		33	
$\begin{array}{c ccccccccccccccccccccccccccccccccccc$		18	61		50	54	
$\begin{array}{c ccccccccccccccccccccccccccccccccccc$		19	15	I	51	47	
$\begin{array}{c ccccccccccccccccccccccccccccccccccc$		20	23	I	52	58	
$\begin{array}{cccccccccccccccccccccccccccccccccccc$		21	11		53	48	
$\begin{array}{c ccccccccccccccccccccccccccccccccccc$		22	19	0.033	54	62	0.026
$\begin{array}{cccccccccccccccccccccccccccccccccccc$		23	22	0.033	55	13	0.025
$\begin{array}{cccccccccccccccccccccccccccccccccccc$		24	39	0.033	56	28	0.025
$\begin{array}{cccccccccccccccccccccccccccccccccccc$		25	7	0.033	57	24	0.025
$\begin{array}{cccccccccccccccccccccccccccccccccccc$		26	43	0.032	58	25	0.023
29140.03061380.02330300.03062630.02231360.0306390.022		27	18	0.032	59	59	0.023
30300.03062630.02231360.0306390.022		28	56	0.031	60	51	0.023
31 36 0.030 63 9 0.022		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 32 0.030 OT 29 0.022		32	52	0.030	64	29	0.022

CPA on Ascon with Multi-bit Selection Function



Which group does these key candid correspond to ?



Viet-Sang Nguyen

viet.sang.nguyen@univ-st-etienne.fr

	Rank	Key	Corr.	Rank	Key	Corr.
idates	1	10	0.133	33	6	0.030
IUALES	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
→ correct key is 0	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

CPA on Ascon with Multi-bit Selection Function

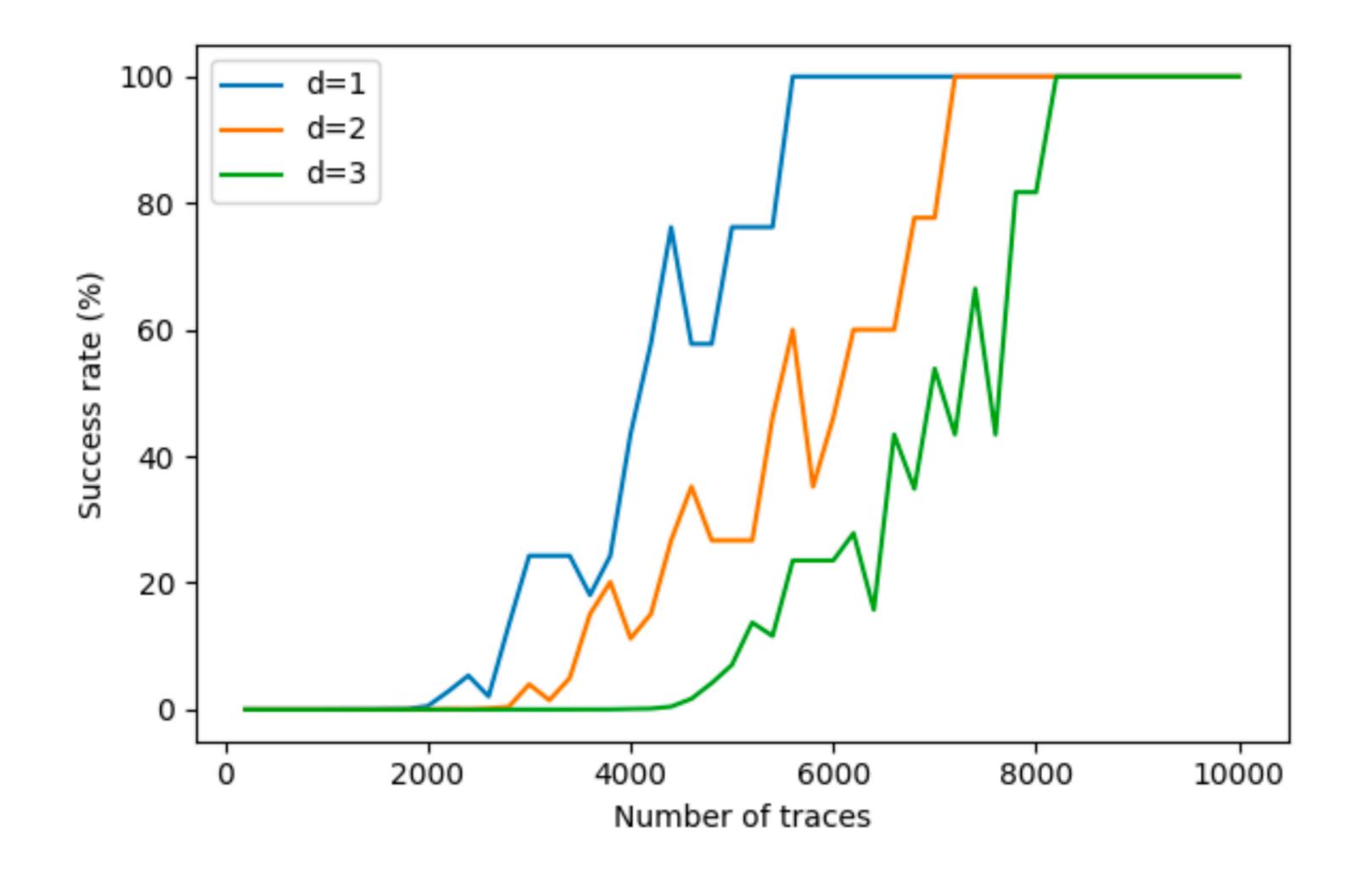


Viet-Sang Nguyen

viet.sang.nguyen@univ-st-etienne.fr





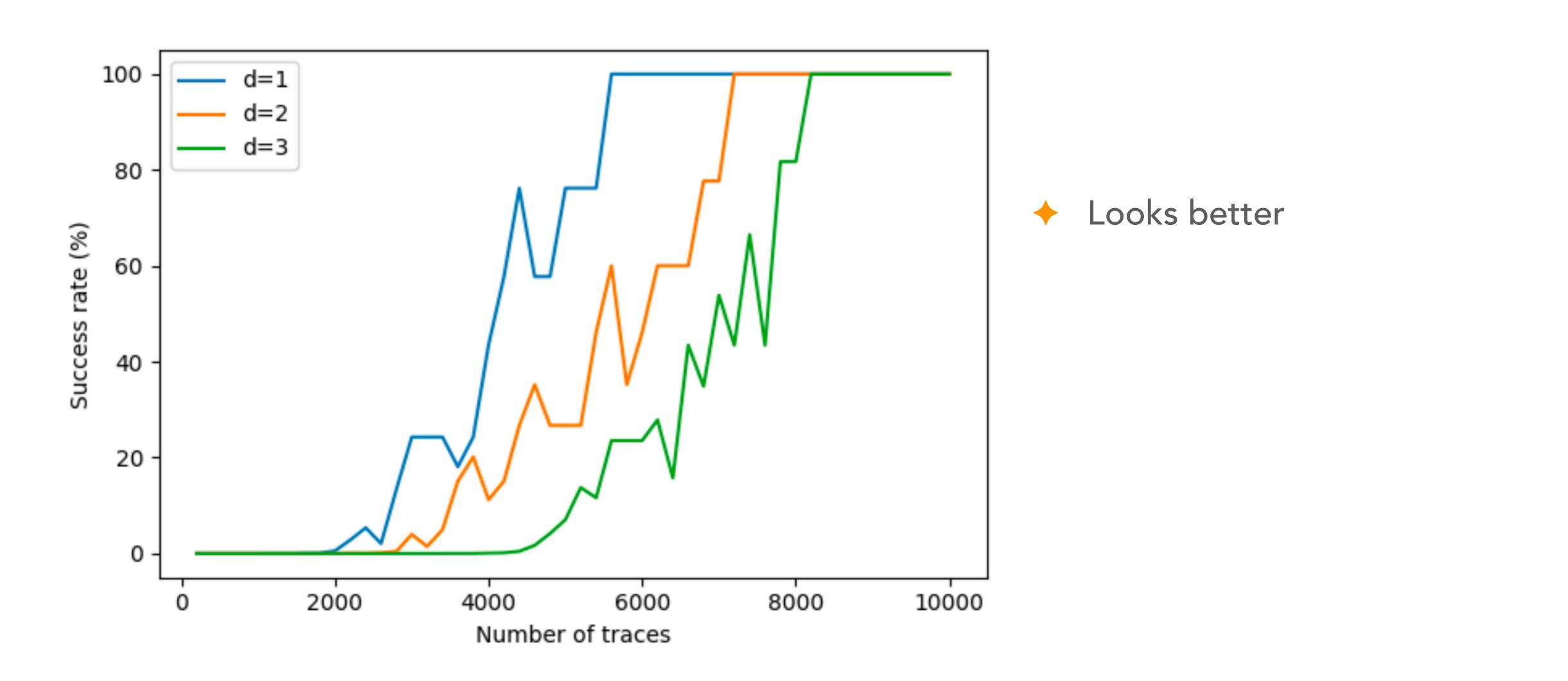


Viet-Sang Nguyen

viet.sang.nguyen@univ-st-etienne.fr





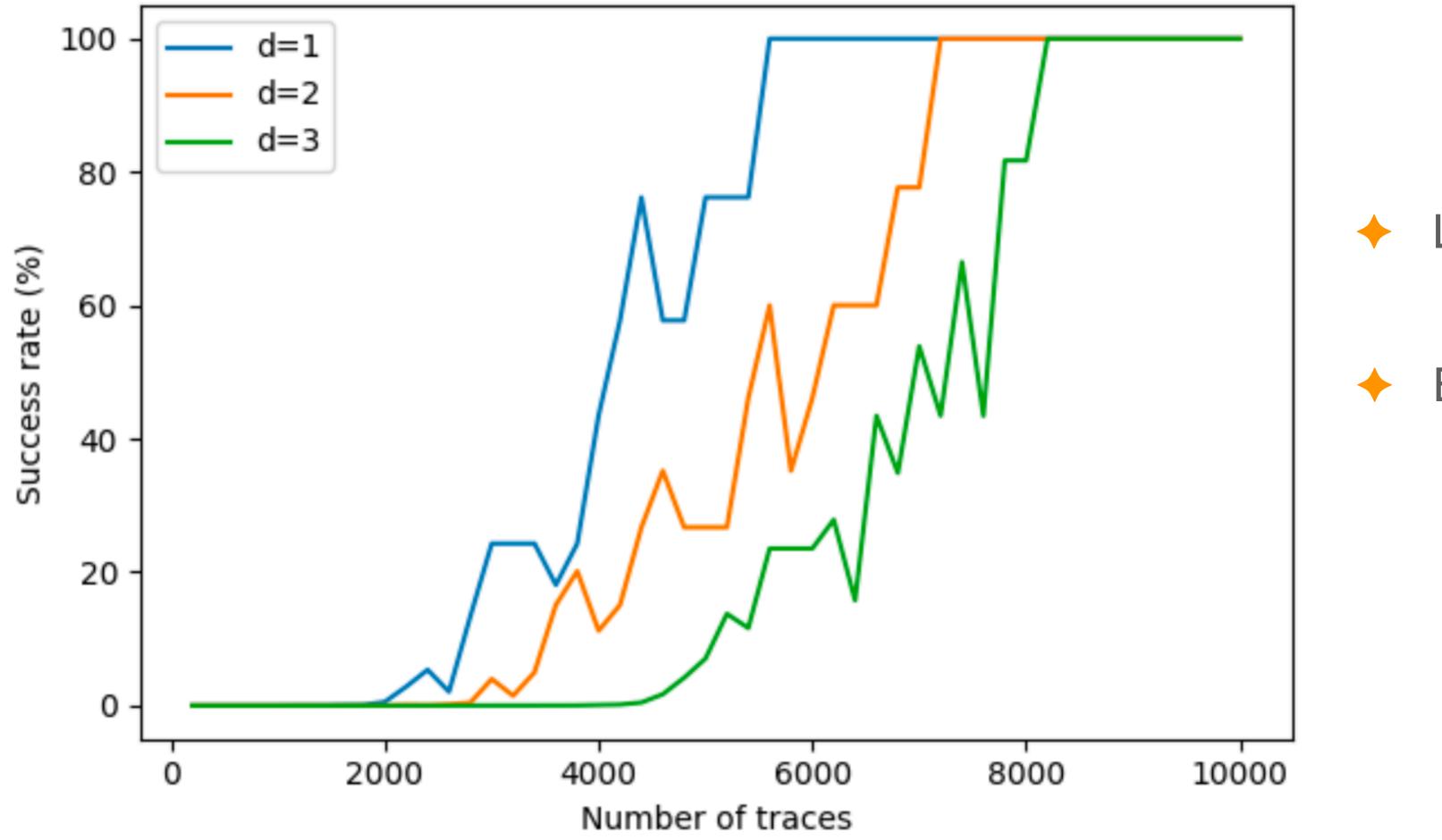


Viet-Sang Nguyen

viet.sang.nguyen@univ-st-etienne.fr







Viet-Sang Nguyen

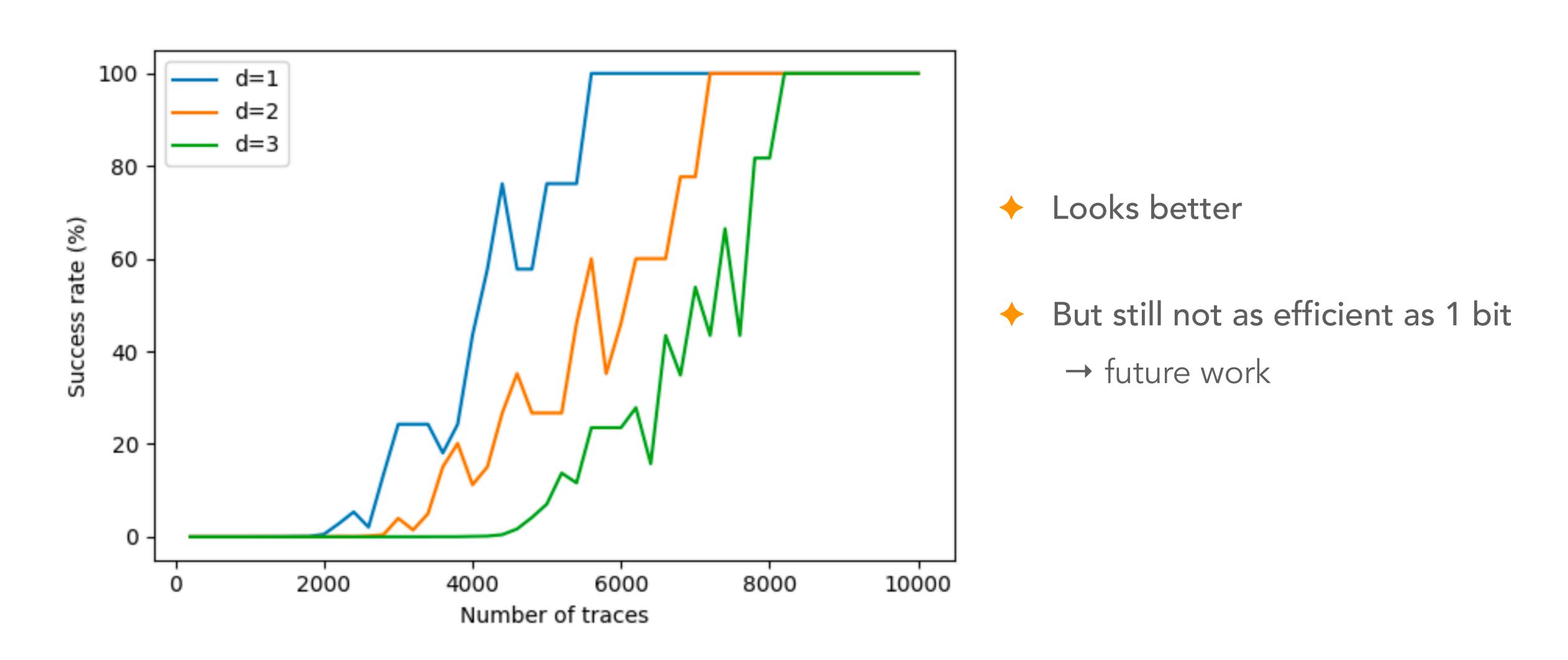
viet.sang.nguyen@univ-st-etienne.fr

Looks better

But still not as efficient as 1 bit







Viet-Sang Nguyen

viet.sang.nguyen@univ-st-etienne.fr





Viet-Sang Nguyen

viet.sang.nguyen@univ-st-etienne.fr



+ Extend hypothetical power consumption to multi-bit scenario

Viet-Sang Nguyen

viet.sang.nguyen@univ-st-etienne.fr



Extend hypothetical power consumption to multi-bit scenario

+ Found the root cause of poor performance



viet.sang.nguyen@univ-st-etienne.fr



Extend hypothetical power consumption to multi-bit scenario

+ Found the root cause of poor performance

Proposed approach for key recovery

Viet-Sang Nguyen

viet.sang.nguyen@univ-st-etienne.fr



Correlation Power Analysis on Ascon with Multi-bit Selection Function

Viet-Sang Nguyen

joint work with Vincent Grosso and Pierre-Louis Cayrel

Bilbao, 11 June, 2025







SECRYPT

