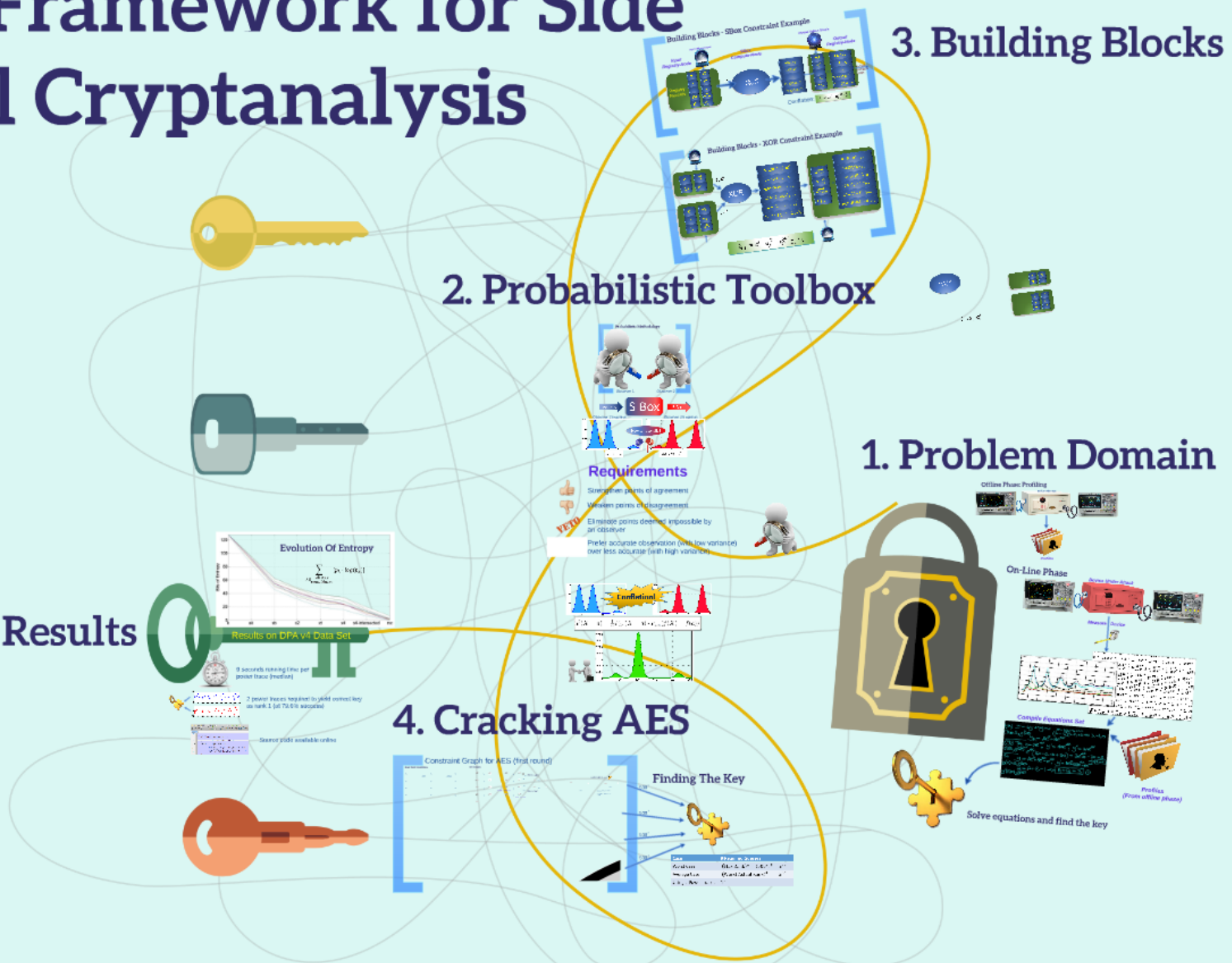
A New Framework for Side Channel Cryptanalysis

Yossef Oren
Columbia University, USA

Ofir Weisse
Tel-Aviv University, Israel

Avishai Wool
Tel-Aviv University, Israel

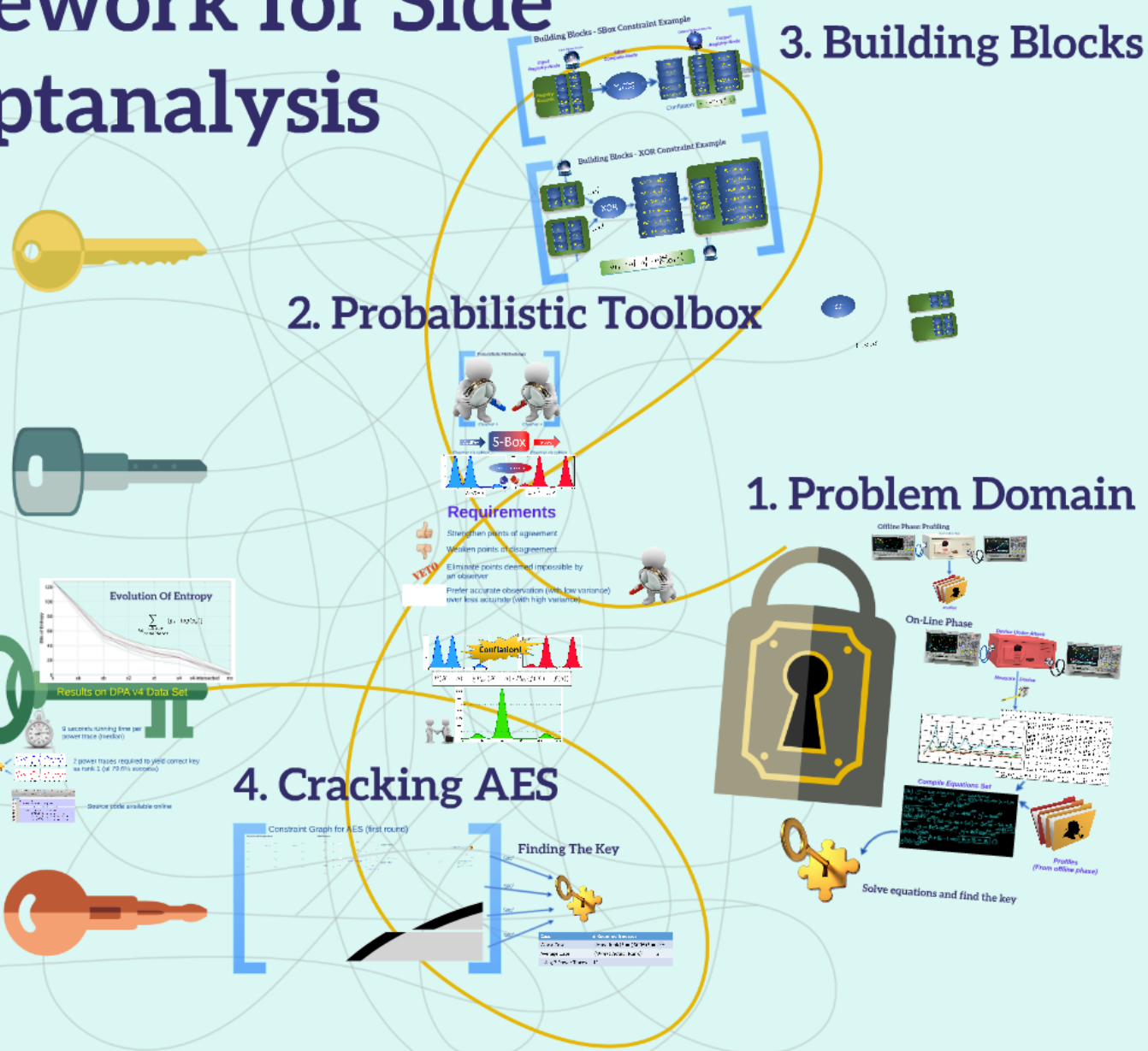


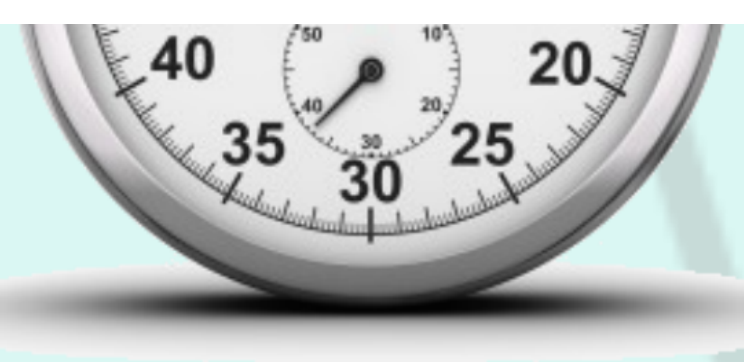
A New Framework for Side Channel Cryptanalysis

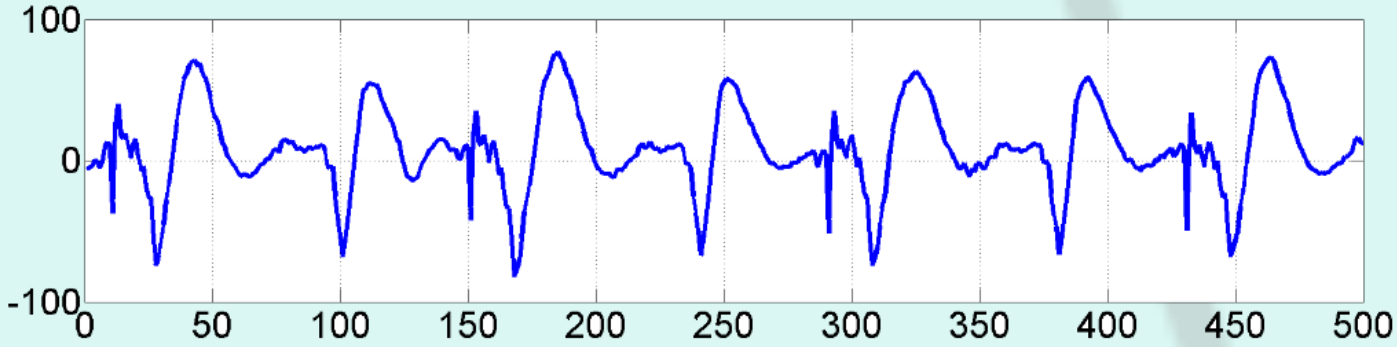
Yossef Oren
Columbia University, USA

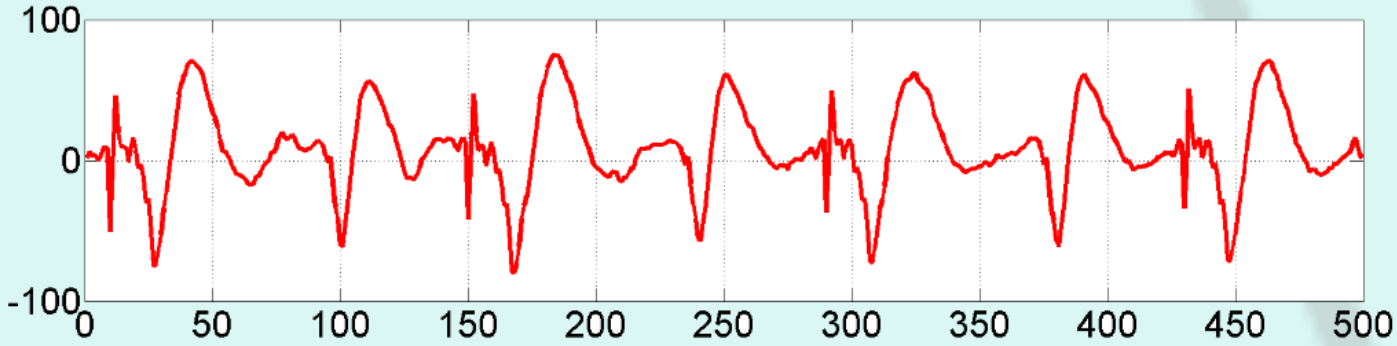
Ofir Weisse
Tel-Aviv University, Israel

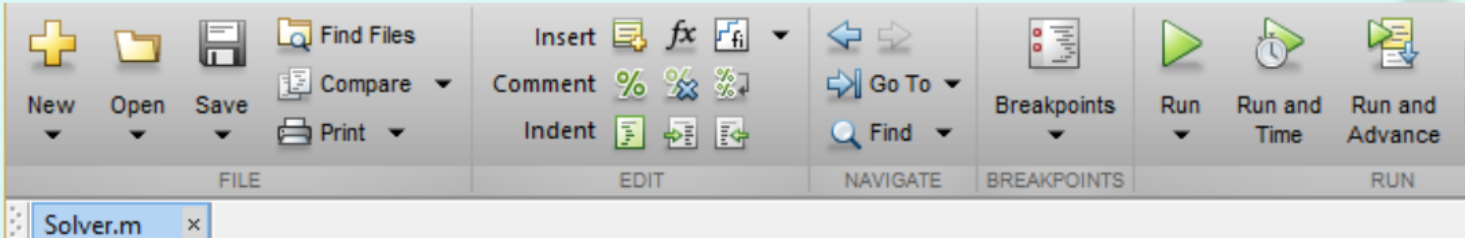
Avishai Wool
Tel-Aviv University, Israel




40
20
35
25
30


100
0
-100
0
50
100
150
200
250
300
350
400
450
500


100
0
-100
0
50
100
150
200
250
300
350
400
450
500

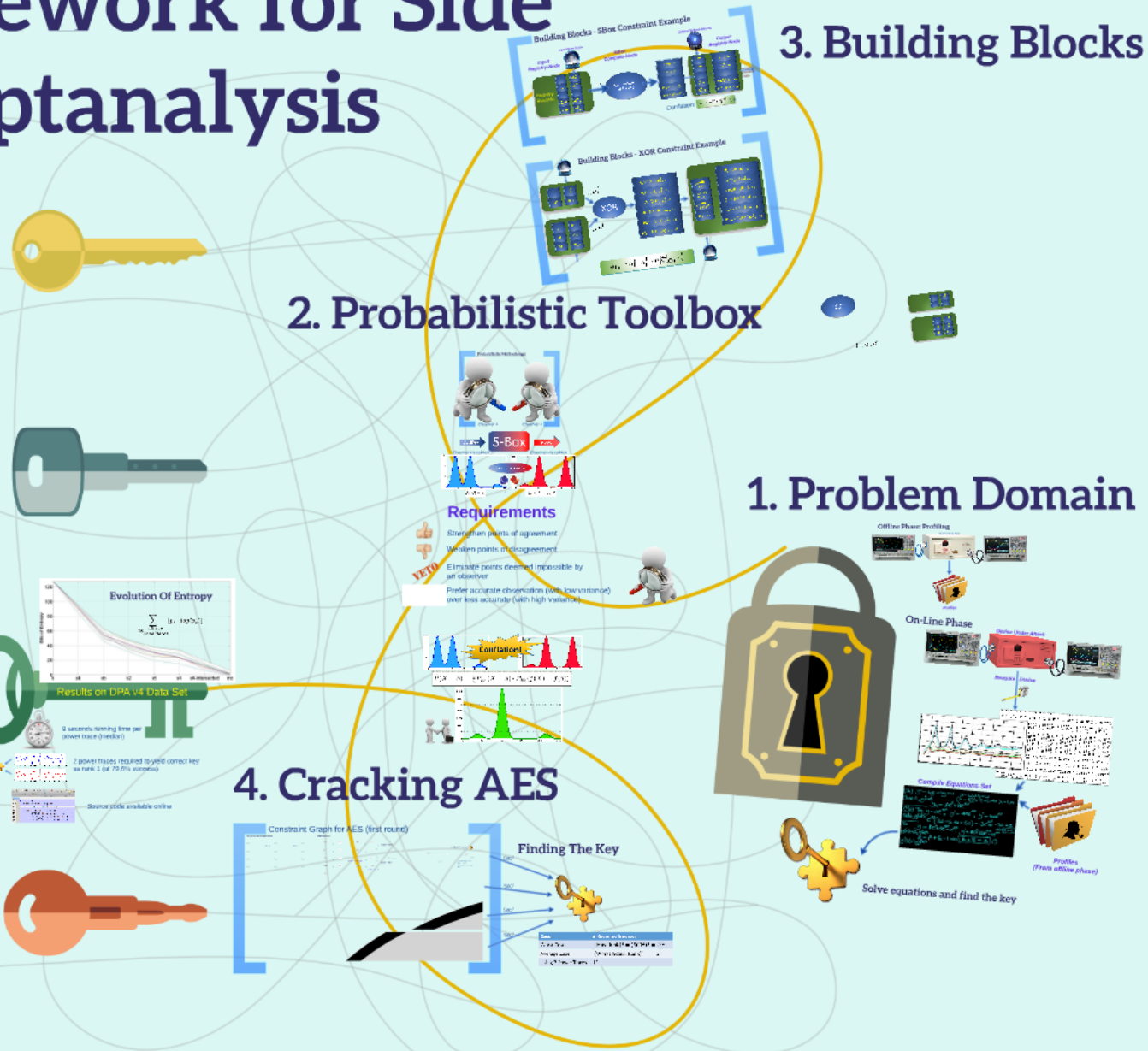

New
Open
Save
Find Files
Compare
Print
Insert
Comment
Indent
Go To
Find
Breakpoints
Run
Run and Time
Run and Advance
FILE
EDIT
NAVIGATE
BREAKPOINTS
RUN
Solver.m

A New Framework for Side Channel Cryptanalysis

Yossef Oren
Columbia University, USA

Ofir Weisse
Tel-Aviv University, Israel

Avishai Wool
Tel-Aviv University, Israel

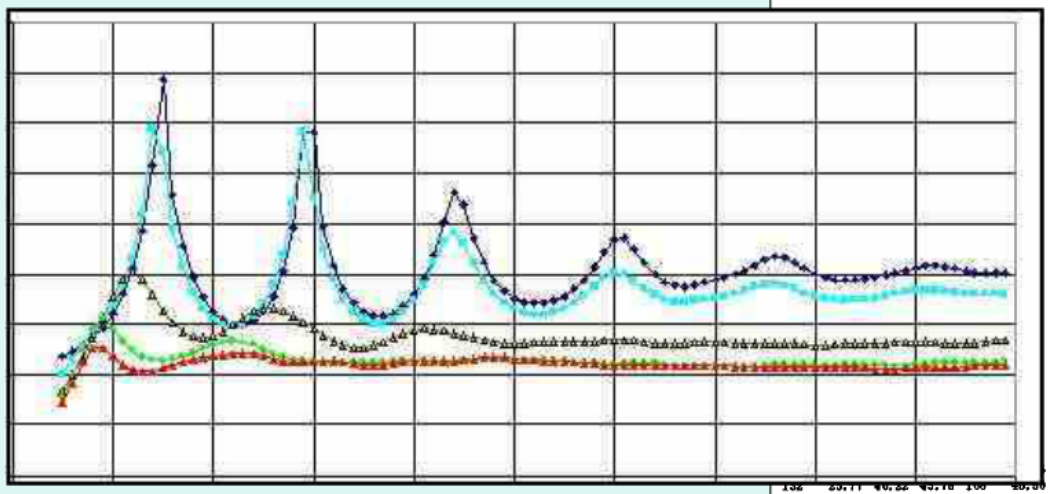


Device Under Test

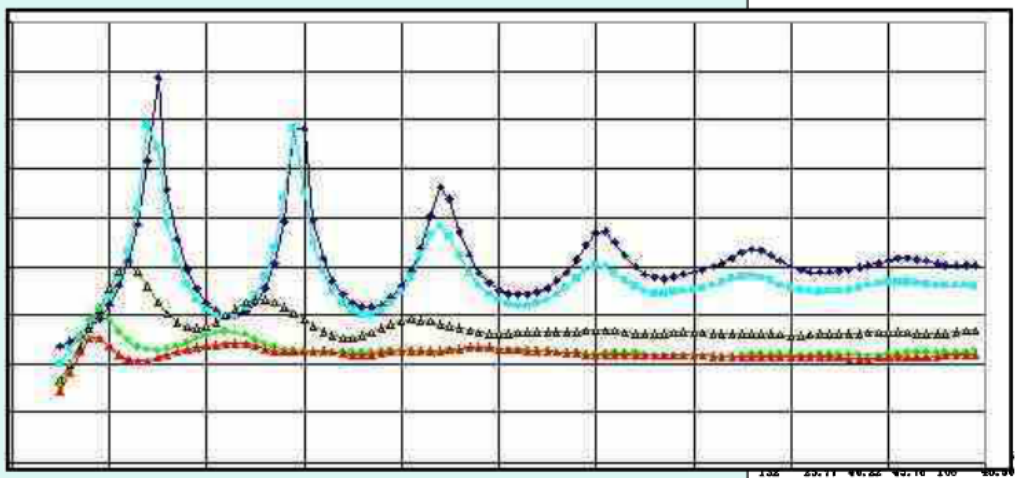
ffline Phase: Profiling

Profiles

n-Line Phase



380	24.9	39.61	45.2	298	45.1	48.71	52.0	209	52.1	54.71	56.5	380	27.2	42.87	48.0	298	48.3	52.64	55.4	209	56.9	59.45	61.4
225	25.5	40.33	46.2	188	46.4	49.72	53.0	143	53.0	55.84	57.4	225	28.2	43.68	49.5	188	50.0	54.00	56.5	143	57.0	60.86	62.5
135	24.2	38.88	44.2	110	43.8	47.71	51.0	66	51.1	53.59	55.6	135	26.3	41.65	46.5	110	46.8	51.28	54.3	66	55.0	58.04	60.4
						48.01	51.9	72	45.8	51.85	54.5	48	26.3	43.86	49.5	58	47.6	52.24	54.5	72	51.3	55.45	58.2
						45.00	46.8	35	48.7	48.41	50.8	86	27.9	41.14	44.5	53	45.8	47.51	48.6	38	49.8	51.31	53.4
						49.06	52.7	51	54.1	56.38	57.6	102	27.4	41.66	46.3	76	47.2	51.85	56.1	51	57.7	62.45	63.9
						52.78	56.7	48	58.7	62.21	63.0	127	27.3	43.99	51.8	111	52.6	58.85	62.1	48	65.5	68.69	70.2
						48.01	49.5	18	47.9	49.26	52.0	26	28.1	42.38	46.1	18	46.6	49.57	54.4	18	52.5	54.09	57.1
						48.92	51.5	23	50.2	53.37	54.7	34	28.5	43.75	49.0	26	48.6	52.45	54.8	23	53.3	57.62	59.5
						49.90	52.1	33	51.1	54.86	57.1	38	27.1	43.21	49.9	30	49.9	53.05	55.6	33	54.5	59.07	62.5
						49.16	51.2	9	51.2	54.58	57.3	21	26.9	41.43	47.6	9	46.0	50.58	53.3	9	54.7	61.20	62.0
						45.93	49.9	14	48.8	54.98	56.5	28	27.6	43.38	47.4	15	48.3	50.44	54.5	14	53.4	58.92	60.3
						44.04	49.3	25	50.5	54.46	56.2	29	27.3	43.39	47.3	34	45.8	49.32	54.2	25	56.0	60.35	61.9
						45.70	51.0	6	49.2	50.97	51.4	6	25.4	39.56	44.5	7	42.4	50.45	55.0	6	54.6	56.63	50.3
						51.51	58.1	3	60.9	60.92	63.3	-	-	-	-	3	53.1	59.51	57.8	3	60.9	63.04	70.2
						51.84	55.0	11	54.5	57.50	59.3	16	27.3	43.11	48.6	12	50.4	56.79	57.1	11	56.8	61.43	65.7
						49.39	52.2	17	53.2	54.12	54.8	39	26.8	41.51	47.3	33	48.4	53.22	55.3	17	56.9	59.03	58.7
						50.39	52.2	21	53.3	56.72	58.2	64	27.5	43.87	50.7	55	49.5	53.62	56.5	21	58.4	62.95	62.8
						50.17	52.2	29	54.0	56.12	58.8	59	27.6	43.71	50.0	54	50.1	53.70	55.9	29	58.4	59.07	60.2
						50.62	53.4	170	55.4	55.95	57.6	272	28.3	45.03	50.4	225	50.6	54.93	57.3	170	57.6	60.74	62.8
						46.50	50.7	39	50.8	53.48	55.3	68	26.1	40.30	45.7	73	46.0	50.36	53.4	39	54.4	58.16	60.1
						49.13	53.2	96	52.4	54.85	57.5	198	27.7	42.91	48.4	151	48.9	53.60	56.7	96	56.4	60.67	62.5
						46.29	50.8	113	51.6	54.57	56.5	162	26.8	42.42	47.6	147	47.7	51.69	54.0	113	55.7	58.23	60.3
						50.83	53.86	78	55.39	57.65	58.62	93	28.09	43.62	49.77	80	50.80	54.78	57.49	78	59.85	63.70	63.67
						48.50	52.32	65	50.75	54.03	56.27	132	28.35	43.74	49.22	108	49.34	53.22	55.51	65	54.29	58.01	61.41
Origin 2																							
32	23.3	37.29	43.5	21	42.7	46.03	50.8	13	49.6	54.79	55.6	32	24.8	39.11	44.6	21	43.8	50.13	54.0	13	52.8	58.26	55.7
39	24.0	38.97	43.8	30	43.6	46.50	51.2	19	52.2	53.26	54.7	39	26.6	41.99	46.7	30	46.9	51.58	54.7	19	57.5	59.29	62.6



360	24.9	39.61	45.2	288	45.1	48.71	52.0	209	52.1	54.71	56.5	360	27.2	42.67	48.0	296	48.3	52.64	55.4	209	56.0	59.46	61.4
225	25.5	40.33	46.2	188	46.4	49.72	53.0	143	53.0	55.84	57.4	225	28.2	43.68	49.5	186	50.0	54.00	56.5	143	57.0	60.86	62.5
135	24.2	38.88	44.2	110	43.8	47.71	51.0	66	51.1	53.59	55.6	135	26.3	41.65	46.6	110	46.5	51.28	54.3	66	55.0	58.04	60.4
						48.01	51.9	72	48.8	51.85	54.5	45	26.3	43.86	49.5	58	47.6	52.24	54.5	72	51.3	55.45	58.2
						45.00	48.8	38	48.7	48.41	50.8	86	27.9	41.14	44.5	53	45.8	47.51	48.6	38	49.8	51.31	53.4
						49.06	52.7	51	54.1	56.38	57.6	102	27.4	41.66	46.3	76	47.2	51.86	56.1	51	57.7	62.45	63.9
						52.78	56.7	48	58.7	62.21	63.0	127	27.3	43.99	51.8	111	52.6	58.85	62.1	48	65.6	68.69	70.2
						48.01	49.5	18	47.9	49.26	52.0	26	28.1	42.38	46.1	18	46.6	49.67	54.4	18	52.5	54.09	57.1
						48.92	51.6	23	50.2	53.37	54.7	34	28.5	43.75	49.0	26	48.6	52.45	54.8	23	53.3	57.62	59.5
						49.90	52.1	33	51.1	54.06	57.1	36	27.1	43.21	49.9	30	49.9	53.05	55.6	33	54.5	59.07	62.8
						46.16	51.2	9	51.2	54.58	57.3	21	26.9	41.43	47.6	9	46.0	50.58	53.3	9	54.7	61.20	62.0
						45.93	49.9	14	48.8	54.98	58.5	28	27.0	43.38	47.4	15	48.3	50.44	54.5	14	53.4	58.92	60.3
						44.04	49.3	25	50.5	54.46	56.2	29	27.3	43.39	47.3	34	45.8	49.32	54.2	25	56.0	60.35	61.9
						45.70	51.0	6	49.2	50.07	51.4	6	25.4	39.58	44.5	7	42.4	50.45	55.0	6	54.6	56.63	58.3
						51.51	58.1	3	60.9	60.02	63.3	-	-	-	-	3	53.1	59.51	57.8	3	60.9	63.04	70.2
						51.84	55.0	11	54.5	57.60	59.3	16	27.3	43.11	49.6	12	50.4	56.78	57.1	11	56.8	61.43	65.7
						49.58	52.2	17	53.2	54.12	54.8	39	26.8	41.51	47.3	33	48.4	53.22	55.3	17	56.9	59.03	58.7
						50.39	52.2	21	53.3	58.72	58.2	64	27.5	43.87	50.7	55	49.9	53.62	56.5	21	58.4	62.95	62.6
						50.17	52.2	29	54.9	56.12	58.8	59	27.5	43.71	50.0	54	50.1	53.70	55.9	29	58.4	59.87	60.2
						50.62	53.4	170	53.4	55.95	57.6	272	28.3	45.03	50.4	225	50.8	54.93	57.3	170	57.6	60.74	62.8
						46.80	50.7	39	50.8	52.43	55.3	88	26.1	40.30	45.7	73	46.0	50.36	53.4	39	54.4	58.16	60.1
						49.13	53.2	96	52.4	54.85	57.5	198	27.7	42.91	48.4	151	48.9	53.60	56.7	96	56.4	60.67	62.5
						48.29	50.8	113	51.8	54.57	56.5	162	25.8	42.42	47.6	147	47.7	51.69	54.0	113	55.7	58.23	60.3
						50.83	53.86	78	55.39	57.65	58.62	93	28.09	43.62	49.77	80	50.80	54.78	57.49	78	59.85	63.70	63.67
						48.60	52.33	65	50.76	54.03	56.27	132	28.35	43.74	49.22	108	49.34	53.22	55.51	65	54.29	58.01	61.41
Origin 2																							
32	23.3	37.29	43.5	21	42.7	46.03	50.6	13	49.6	54.79	55.6	32	24.8	39.11	44.6	21	43.8	50.15	54.0	13	52.8	58.26	55.7
39	24.0	38.97	43.8	30	43.6	46.50	51.2	19	52.2	53.20	54.7	39	26.6	41.99	46.7	30	46.9	51.56	54.7	19	57.5	58.29	62.6
64	25.4	40.38	46.1	59	45.3	48.69	51.0	34	51.6	52.78	56.4	64	27.4	43.35	48.6	59	49.0	52.15	54.0	34	54.7	57.57	62.8

Compile Equations Set

(h) $y'' - 6y' + 5y = 0$ $\quad \lambda^2 - 6\lambda + 5 = 0$

$(\lambda - 5)(\lambda - 1) = 0 \Rightarrow \lambda = 1, 5$

Case 1, gives $y_h = Ae^{x} + Be^{5x}$

(p) Try $y = ae^{4x}$, $y' = 4ae^{4x}$, $y'' = 16ae^{4x}$

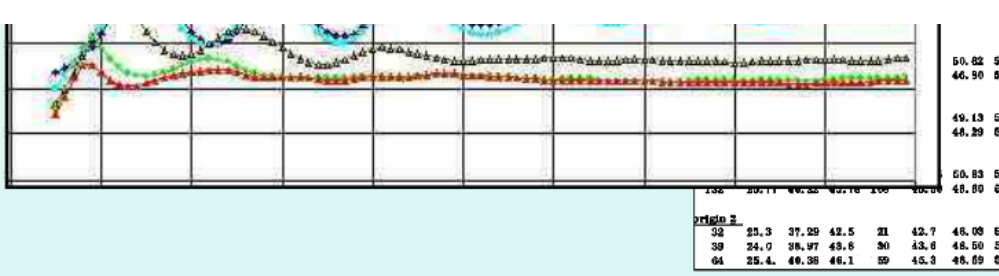
Subs, gives $e^{4x}(16a - 6 \cdot 4a + 5a) = 3e^{4x} \Rightarrow -3a = 3$

So $y = Ae^{x} + Be^{5x} - e^{4x}$. $y' = Ae^{x} + 5Be^{5x} - 4e^{4x}$ $\Rightarrow \boxed{a = -1}$

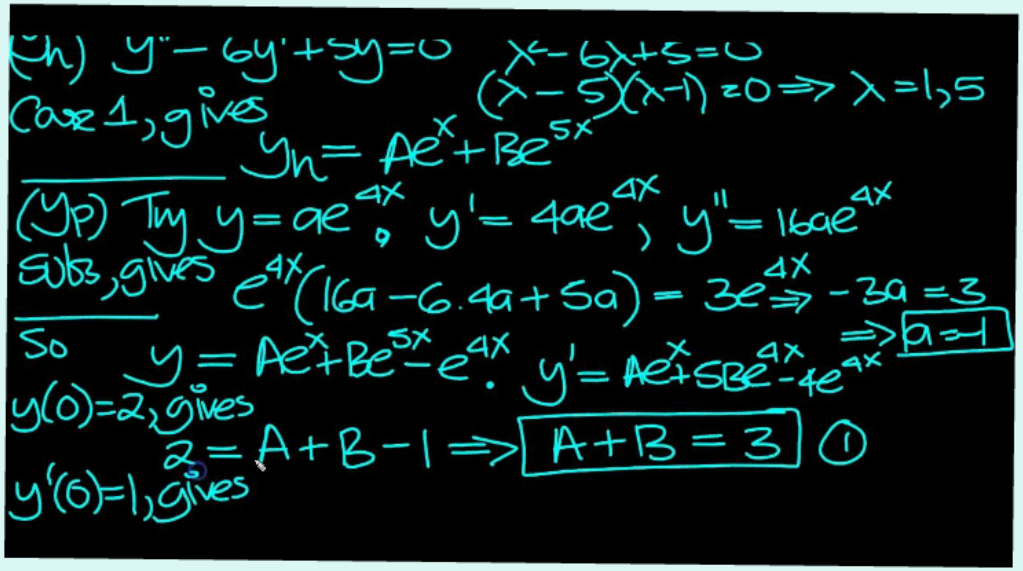
$y(0) = 2$, gives $2 = A + B - 1 \Rightarrow \boxed{A + B = 3}$ (1)

$y'(0) = 1$, gives

Profiles (From offline phase)

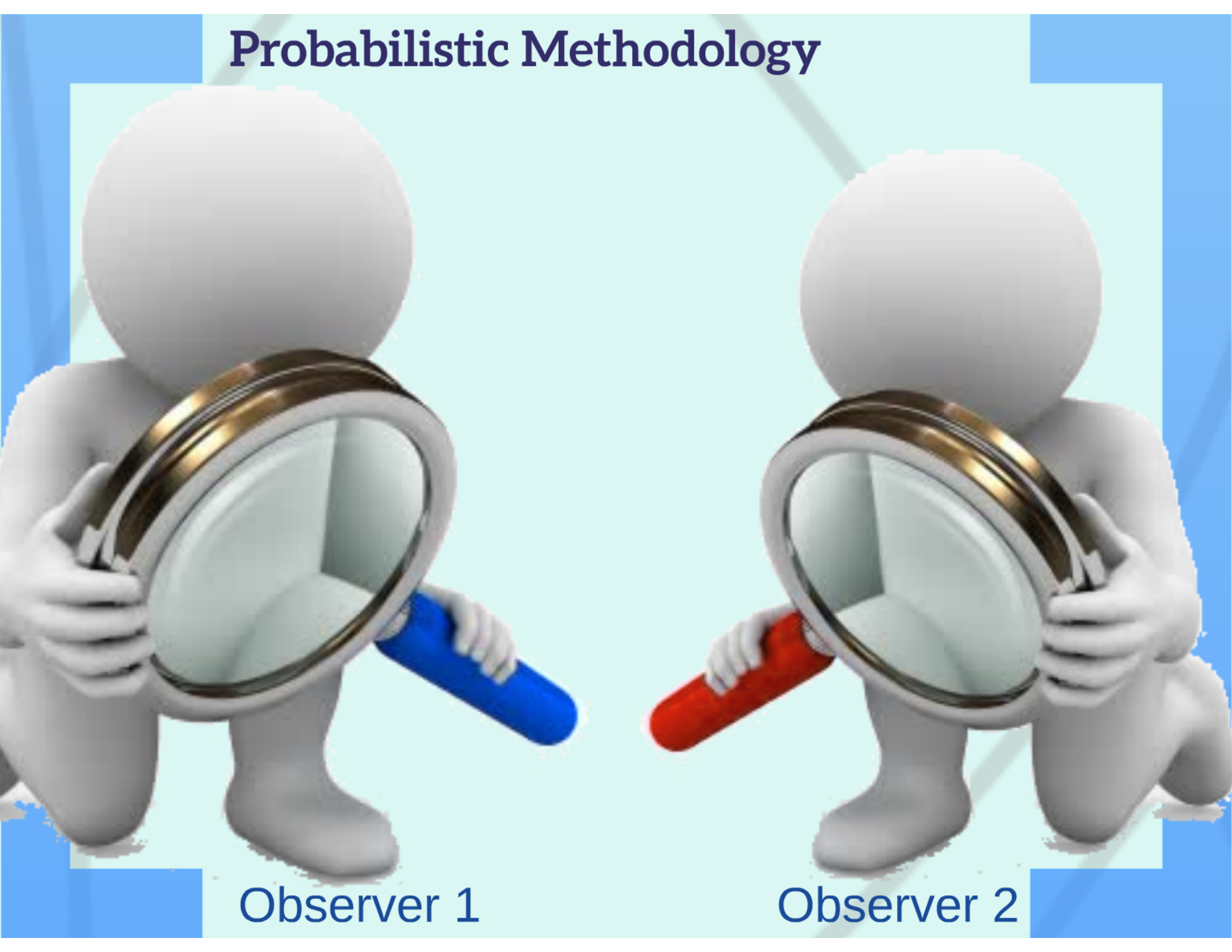


Compile Equations Set



Solve equations and find the key

Probabilistic Methodology



Observer 1

Observer 2

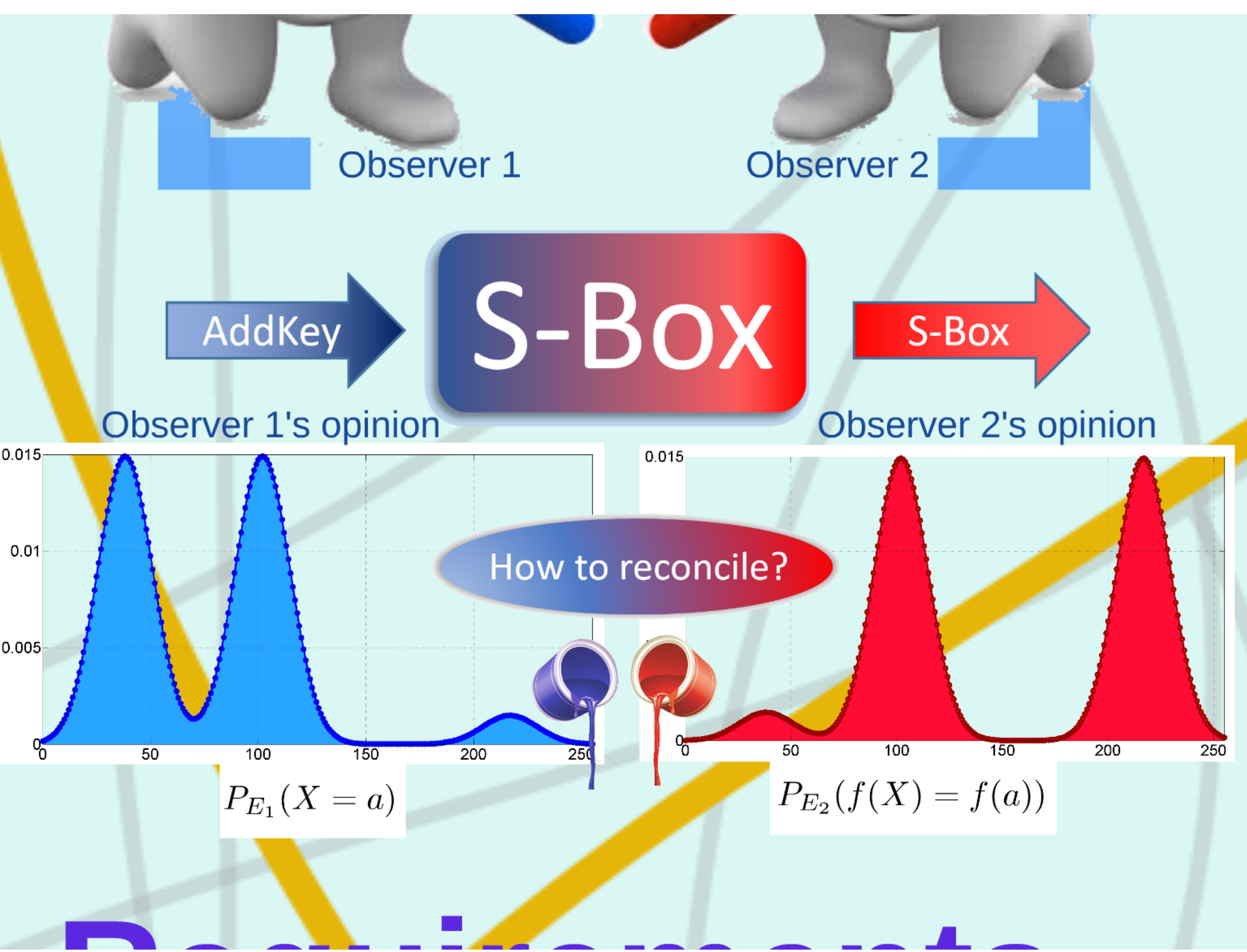
AddKey

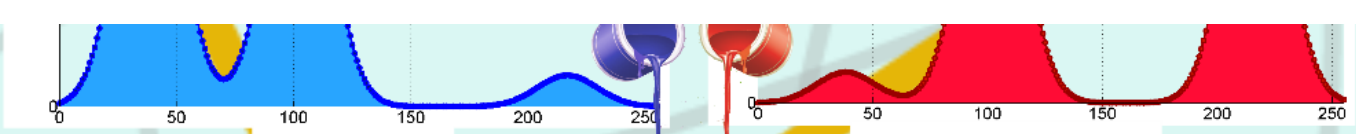
S-Box

S-Box

Observer 1's opinion

Observer 2's opinion


Observer 1
Observer 2
AddKey
S-Box
S-Box
Observer 1's opinion
Observer 2's opinion
How to reconcile?
0.015
0.01
0.005
0
0
50
100
150
200
250
$P_{E_1}(X = a)$
$P_{E_2}(f(X) = f(a))$



$P_{E_1}(X = a)$

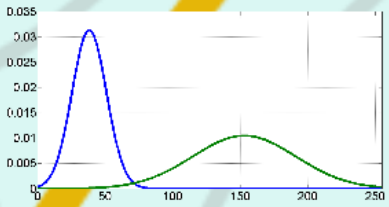
$P_{E_2}(f(X) = f(a))$

Requirements

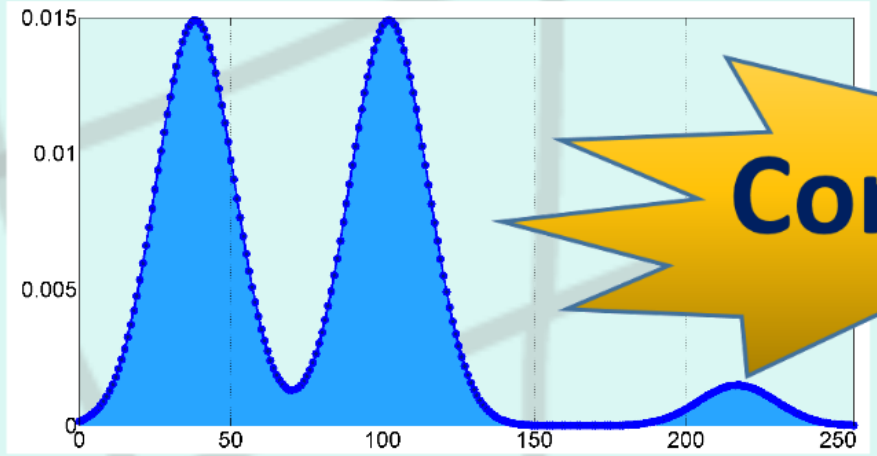
Strengthen points of agreement

Weaken points of disagreement

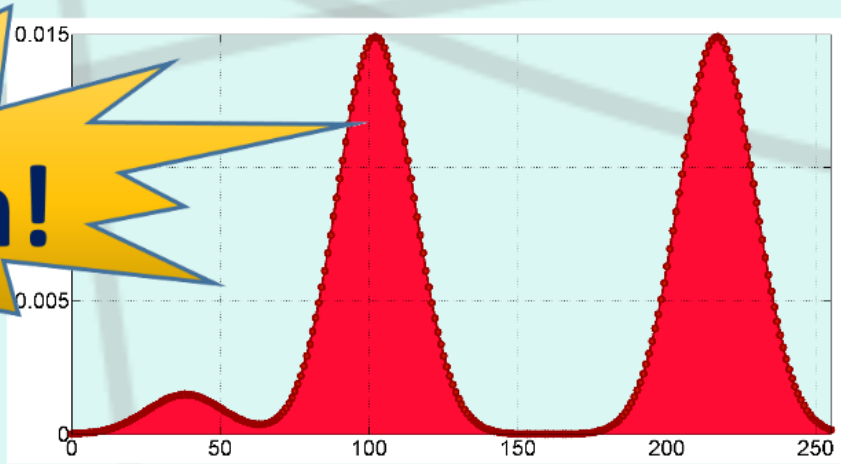
Eliminate points deemed impossible by an observer



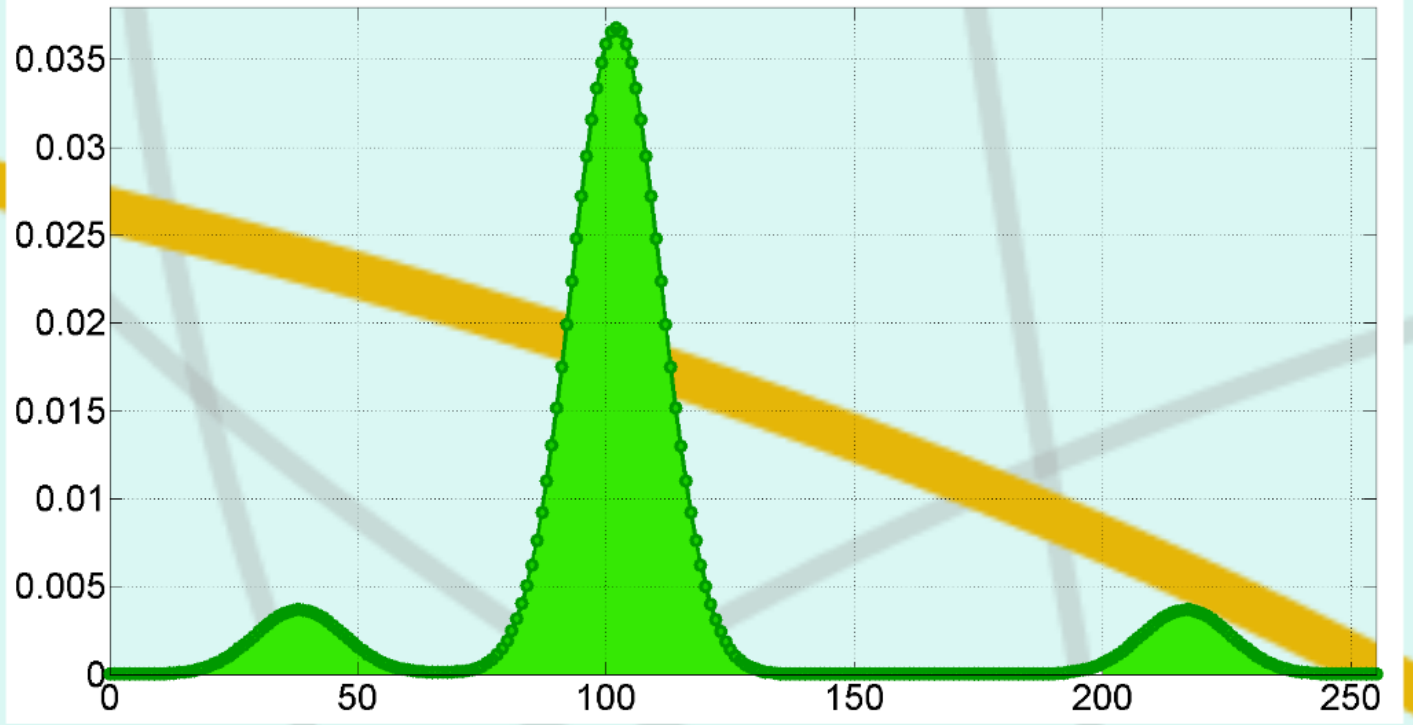
Prefer accurate observation (with low variance) over less accurate (with high variance)



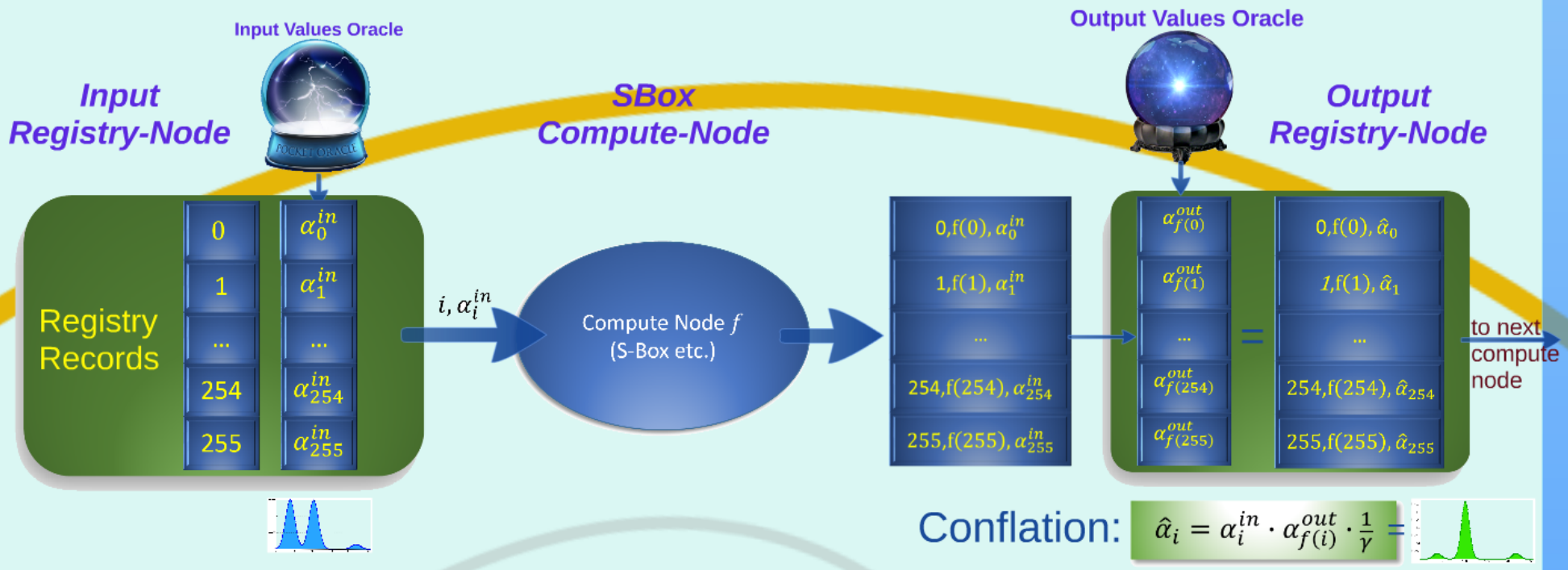
Conflation!



$$\hat{P}(X = a) = \frac{1}{\gamma} P_{E_1}(X = a) \cdot P_{E_2}(f(X) = f(a))$$



Building Blocks - SBox Constraint Example



Building Blocks - XOR Constraint Example

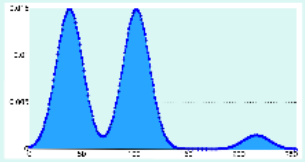
Input Values Oracle

Input Registry-Node

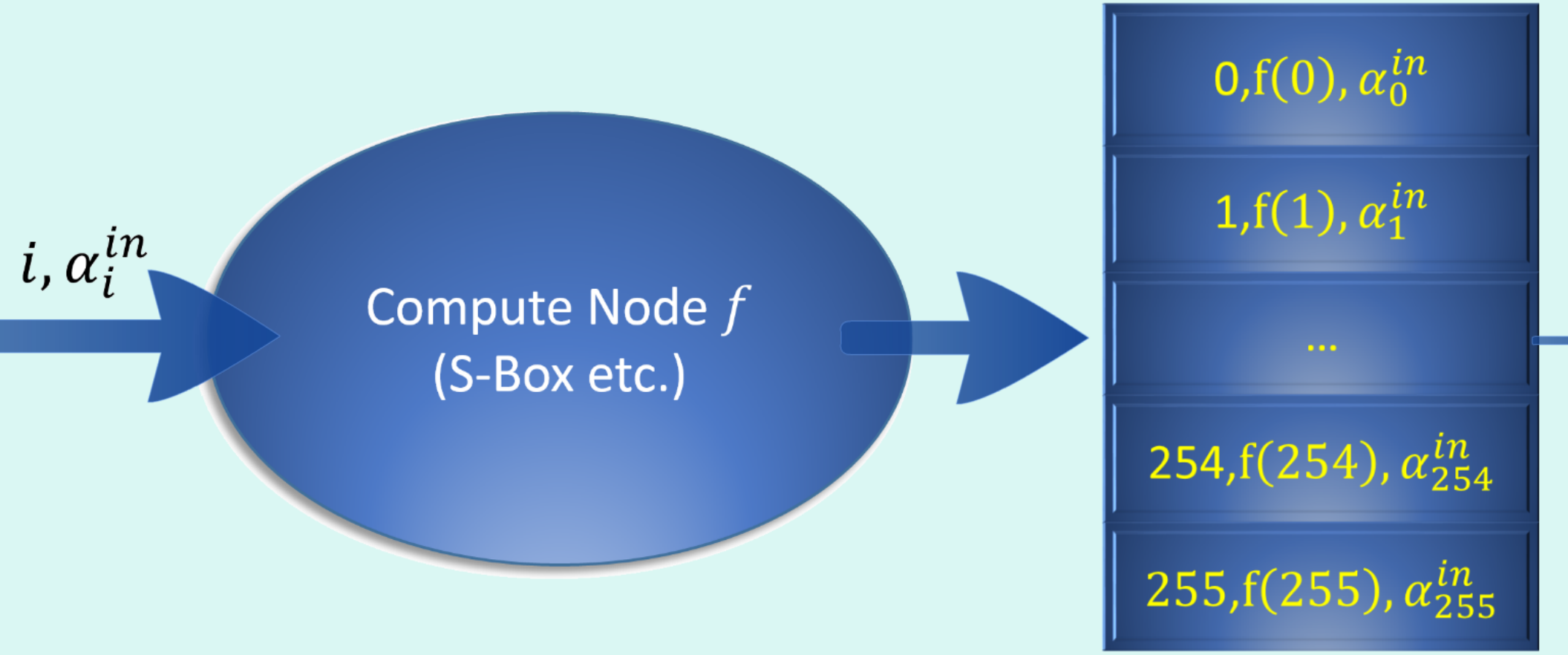
Registry Records

0	α_0^{in}
1	α_1^{in}
...	...
254	α_{254}^{in}
255	α_{255}^{in}

i, α_i^{in}



SBox Compute-Node



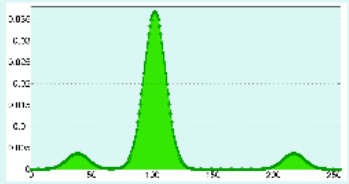
Output Values Oracle

Output Registry-Node

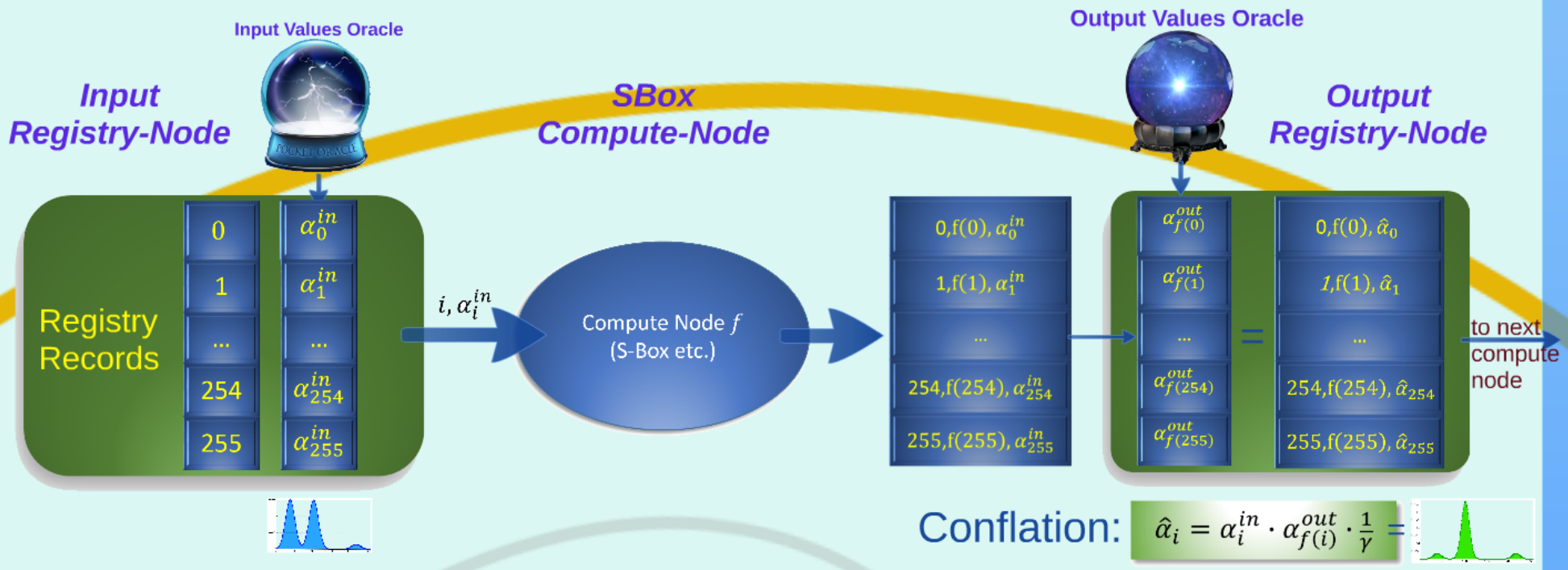
$0,f(0),\alpha_0^{in}$	$\alpha_{f(0)}^{out}$	=	$0,f(0),\hat{\alpha}_0$
$1,f(1),\alpha_1^{in}$	$\alpha_{f(1)}^{out}$		$1,f(1),\hat{\alpha}_1$
...	...		...
$254,f(254),\alpha_{254}^{in}$	$\alpha_{f(254)}^{out}$		$254,f(254),\hat{\alpha}_{254}$
$255,f(255),\alpha_{255}^{in}$	$\alpha_{f(255)}^{out}$		$255,f(255),\hat{\alpha}_{255}$

to next compute node

Conflation: $\hat{\alpha}_i = \alpha_i^{in} \cdot \alpha_{f(i)}^{out} \cdot \frac{1}{\gamma} =$

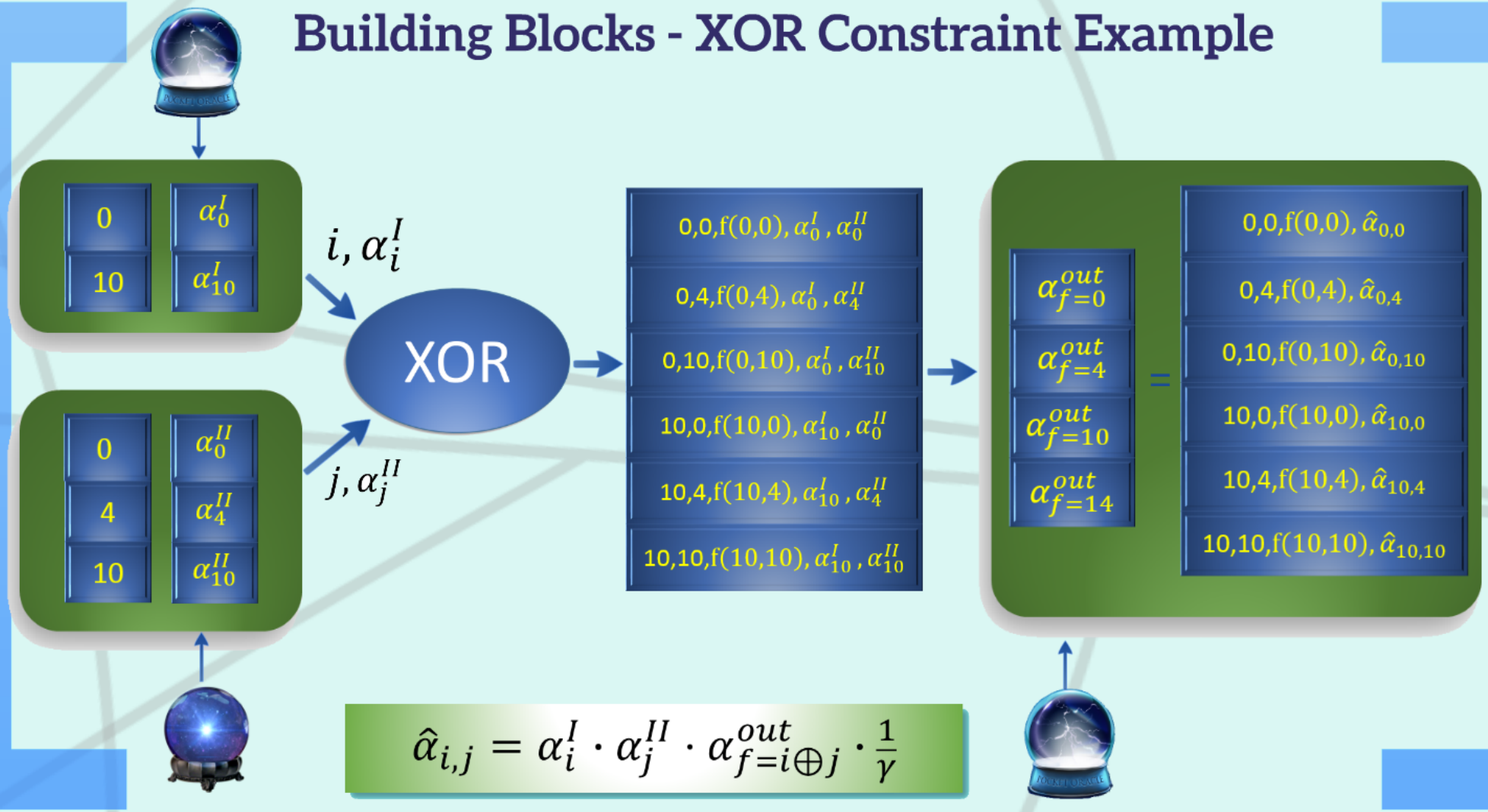


Building Blocks - SBox Constraint Example



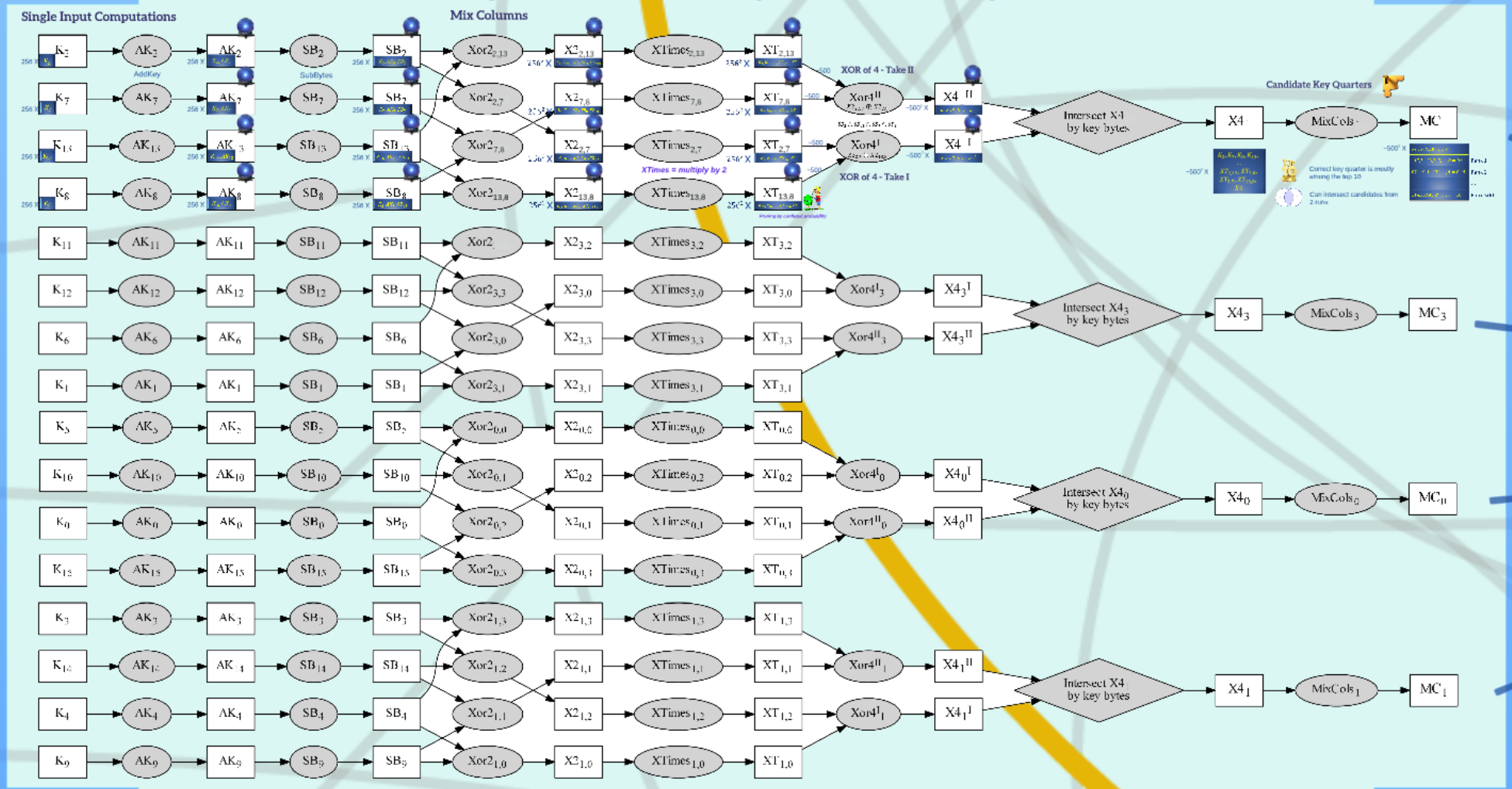
Building Blocks - XOR Constraint Example

Building Blocks - XOR Constraint Example



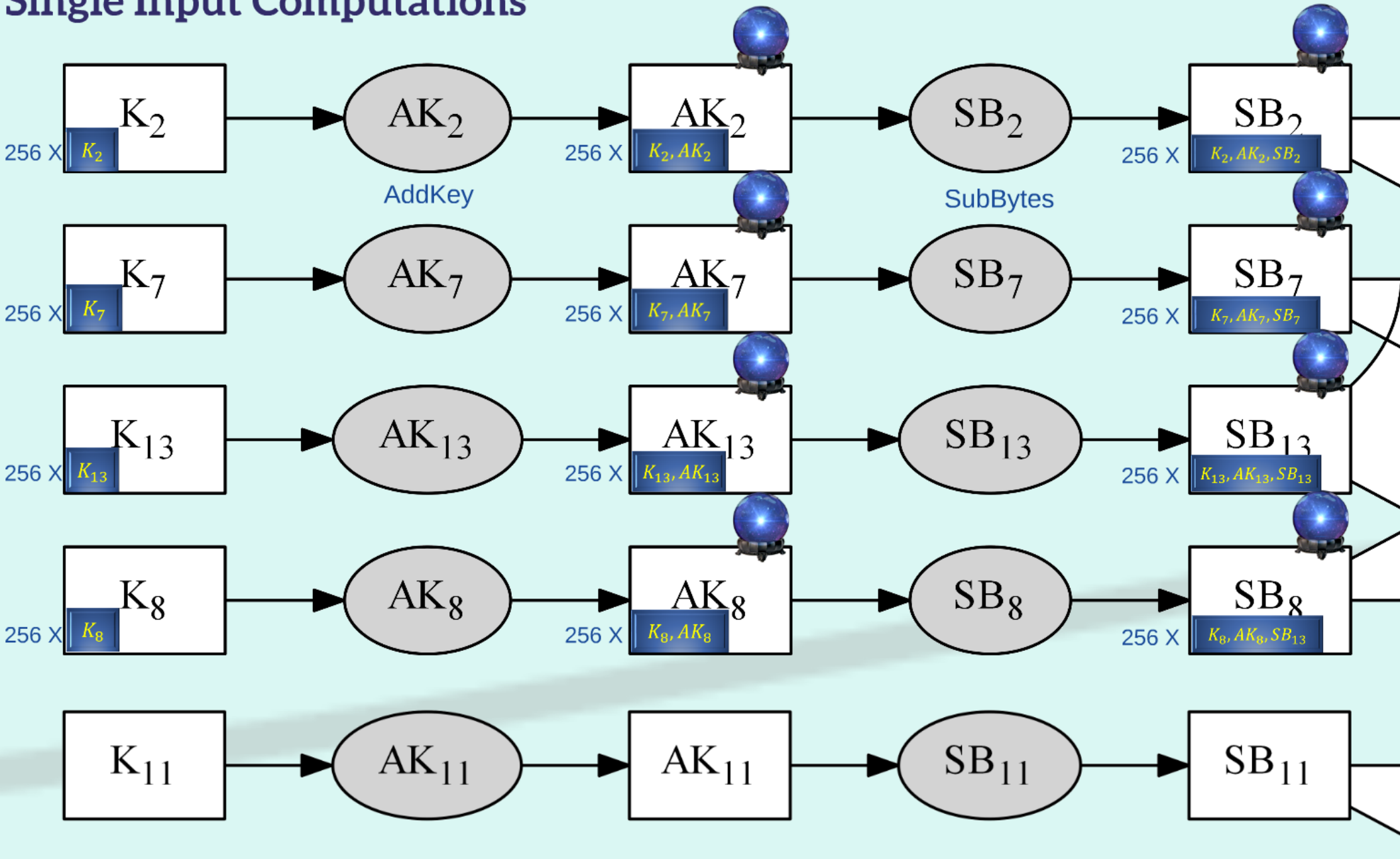
$$\hat{\alpha}_{i,j} = \alpha_i^I \cdot \alpha_j^{II} \cdot \alpha_{f=i\oplus j}^{out} \cdot \frac{1}{\gamma}$$

Constraint Graph for AES (first round)

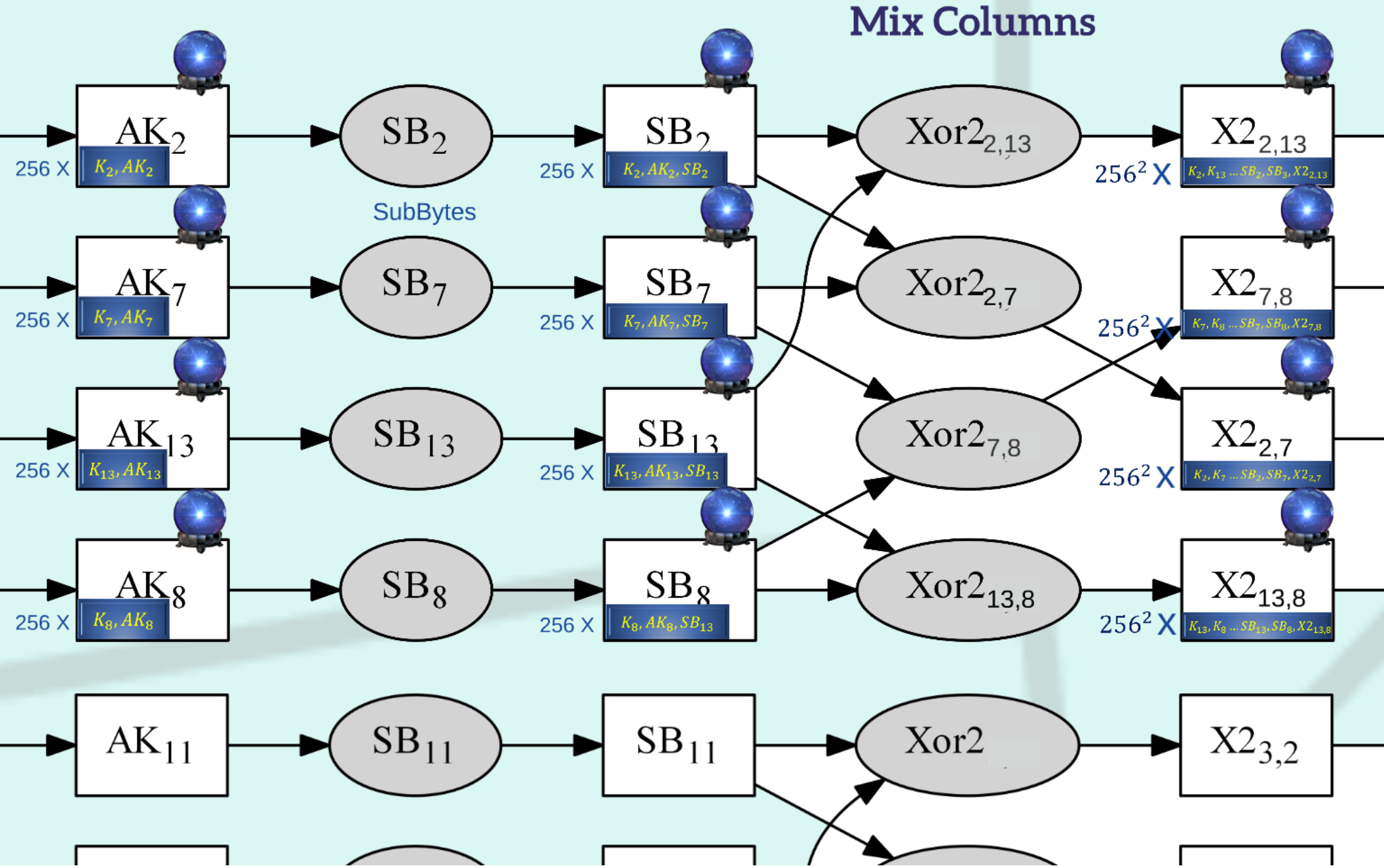


Constraint G

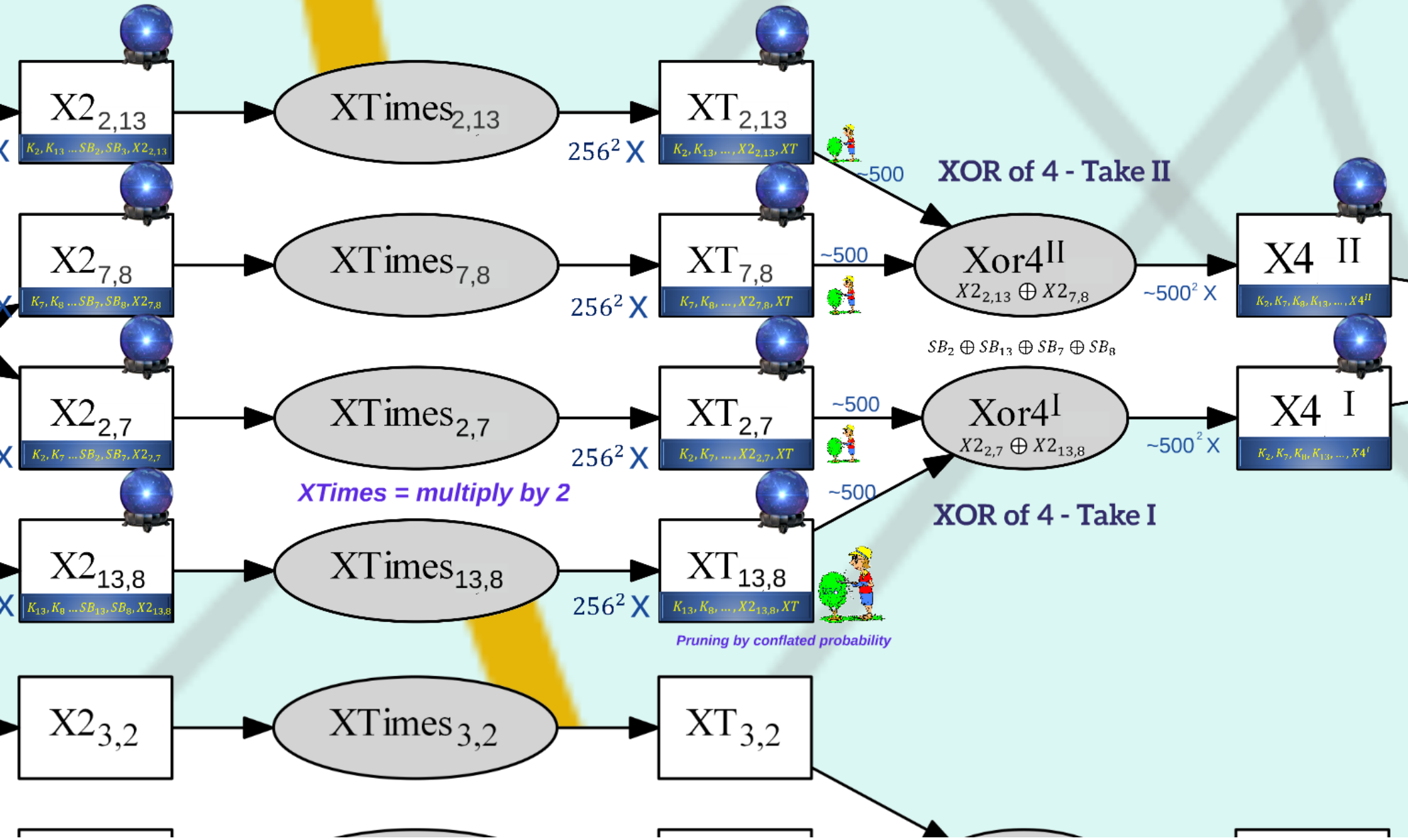
Single Input Computations



Constraint Graph for



for AES (first round

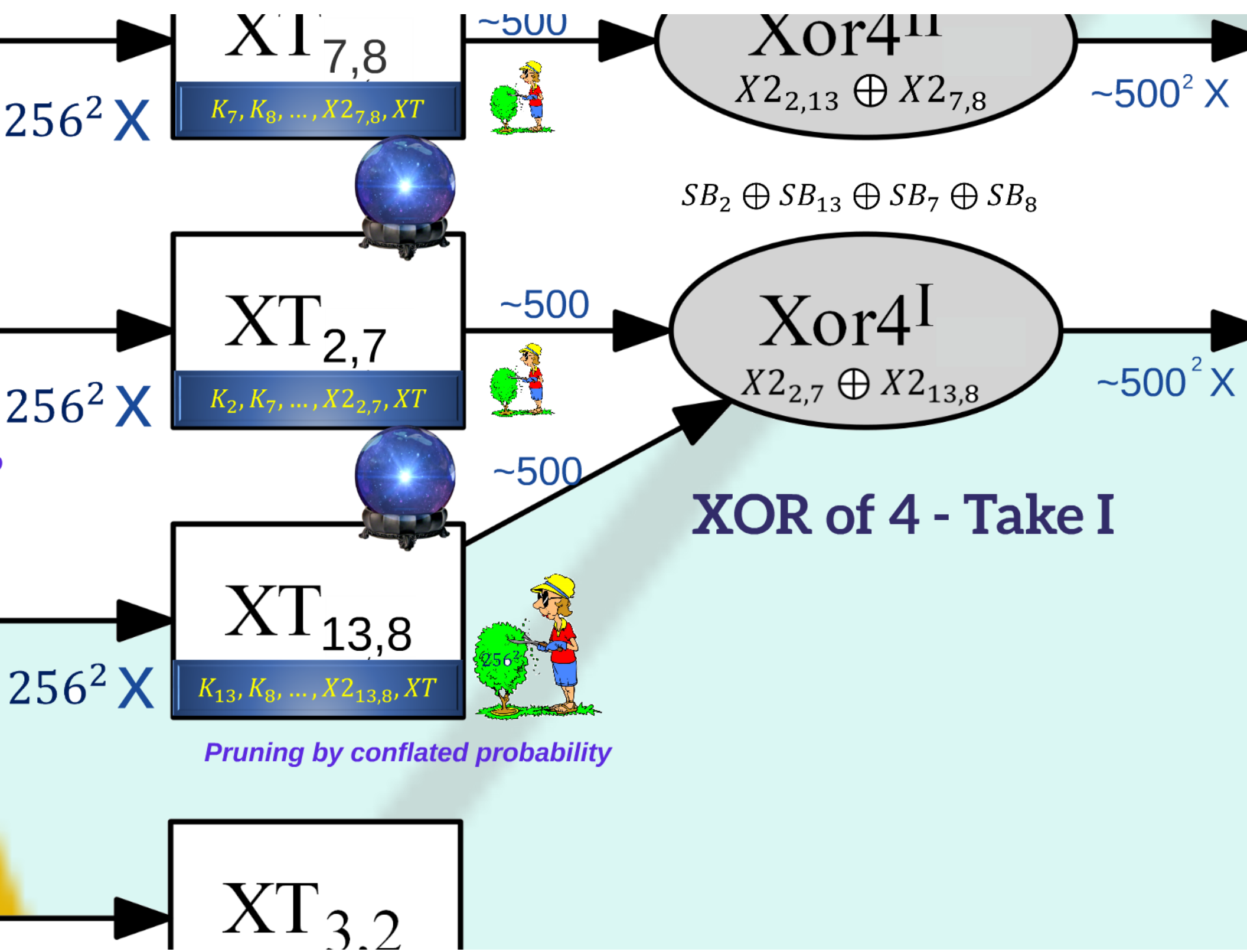


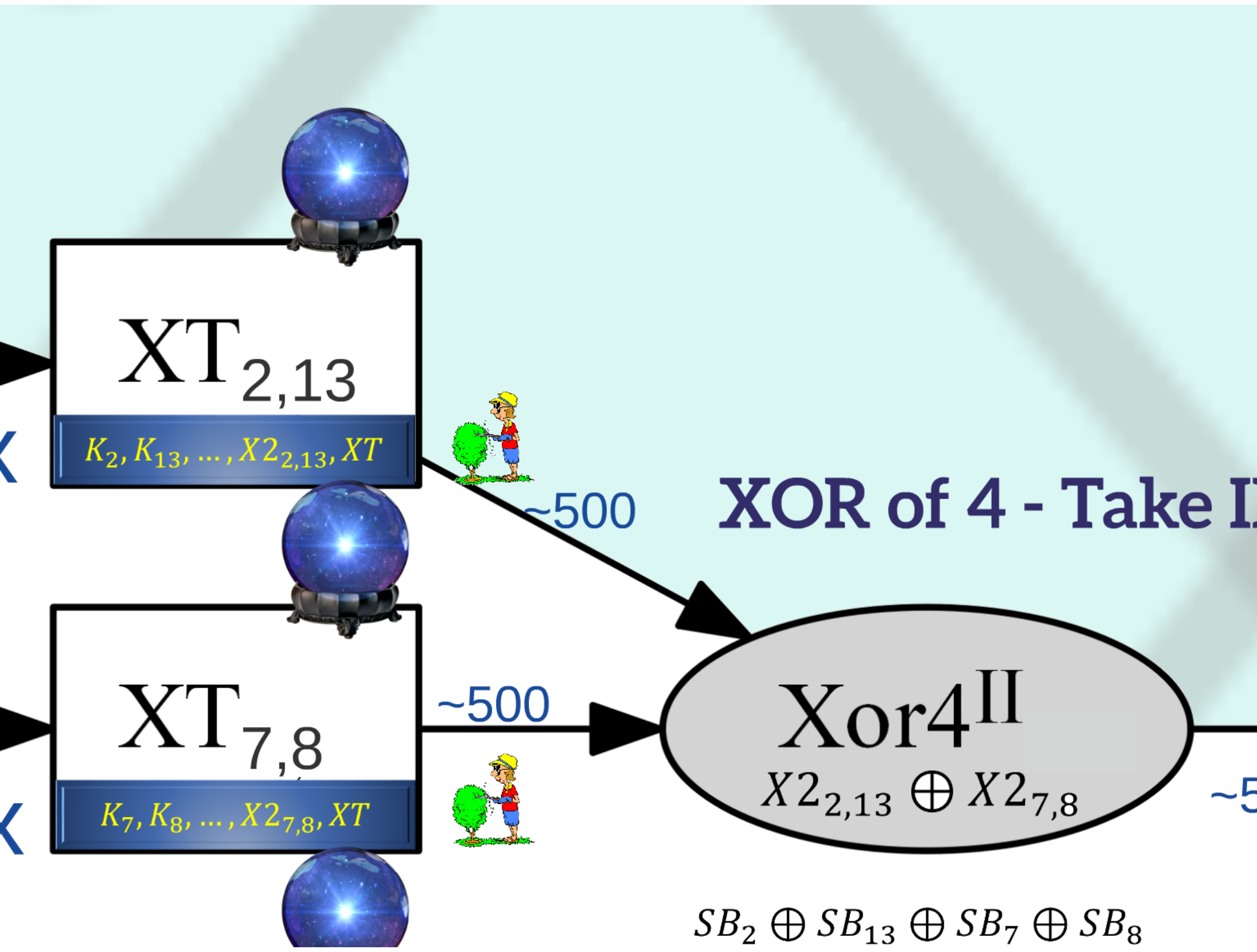
~500

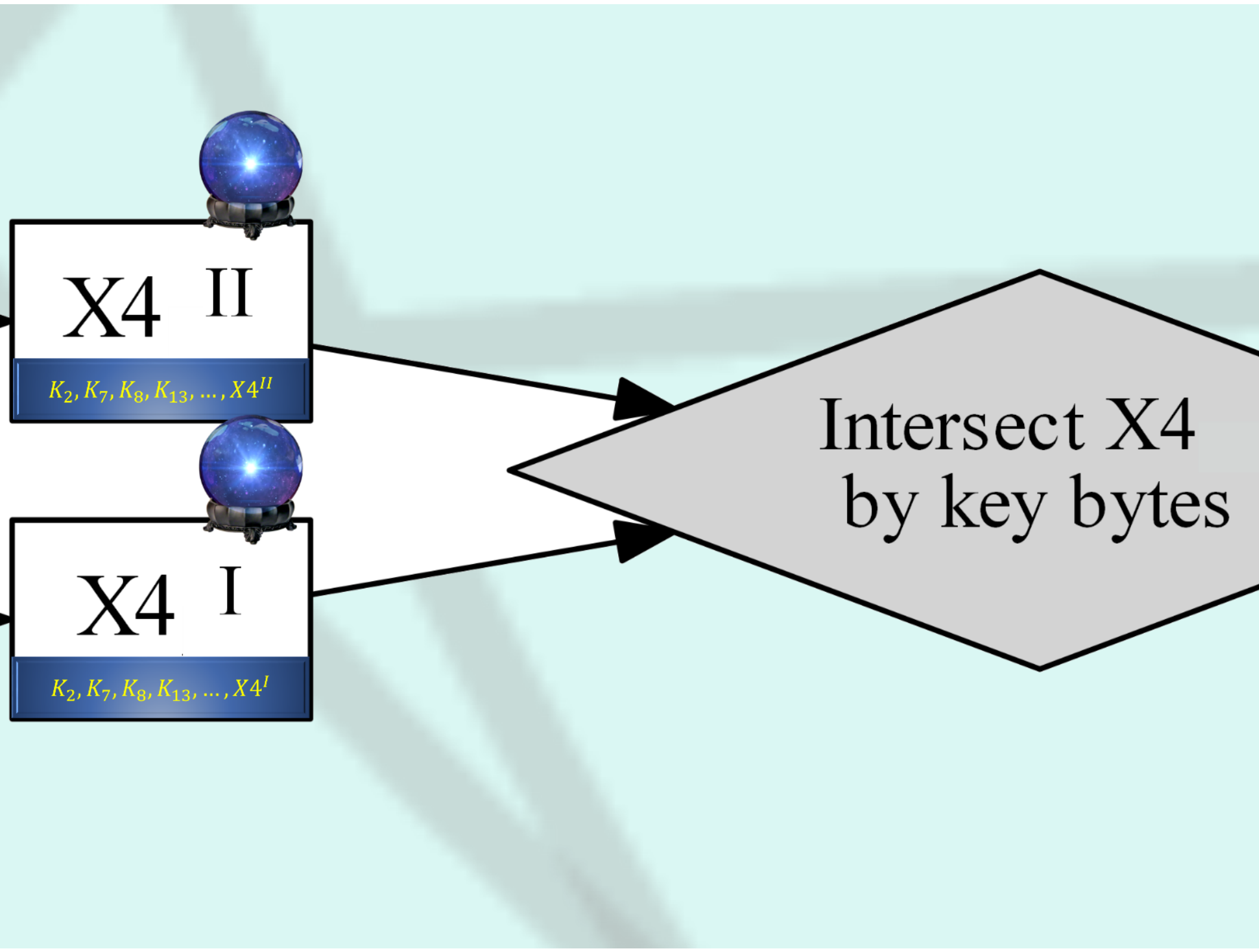
$XT_{13,8}$

$K_{13}, K_{8}, \ldots, X2_{13,8}, XT$

Pruning by conflated probability


$XT_{7,8}$
$K_7, K_8, \ldots, X2_{7,8}, XT$
256^2 X
~500
$Xor4^{II}$
$X2_{2,13} \oplus X2_{7,8}$
~500^2 X
$SB_2 \oplus SB_{13} \oplus SB_7 \oplus SB_8$
$XT_{2,7}$
$K_2, K_7, \ldots, X2_{2,7}, XT$
256^2 X
~500
$Xor4^{I}$
$X2_{2,7} \oplus X2_{13,8}$
~500^2 X
~500
$XT_{13,8}$
$K_{13}, K_8, \ldots, X2_{13,8}, XT$
256^2 X
256^2
XOR of 4 - Take I
Pruning by conflated probability
$XT_{3,2}$


XT2,13
K2, K13, … , X22,13, XT
XT7,8
K7, K8, … , X27,8, XT
~500
~500
XOR of 4 - Take I
Xor4II
X22,13 ⊕ X27,8
SB2 ⊕ SB13 ⊕ SB7 ⊕ SB8

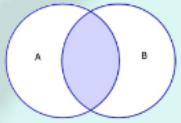

X4 II
$K_2, K_7, K_8, K_{13}, \ldots, X4^{II}$
X4 I
$K_2, K_7, K_8, K_{13}, \ldots, X4^{I}$
Intersect X4
by key bytes

Candidate Key Quarters

~500^2 X

K_2, K_7, K_8, K_{13},
...
$XT_{2,13}, XT_{7,8}$,
$XT_{2,7}, XT_{13,8}$,
$X4$

Correct key quarter is mostly among the top 10

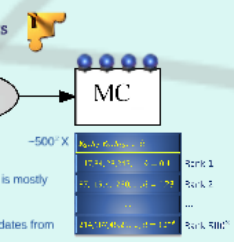


Can intersect candidates from 2 runs

~500^2 X

$K_2, K_7, K_8, K_{13}, \ldots, \hat{\alpha}$	
$117,34, 23,245, \ldots, \hat{\alpha} = 0.4$	Rank 1
$87,\ 19,4,\ 230, \ldots, \hat{\alpha} = 0.23$	Rank 2
...	...
$214,187,45,29, \ldots, \hat{\alpha} = 10^{-9}$	Rank 500^2

Finding The Key



MC_3

MC_0

MC_1

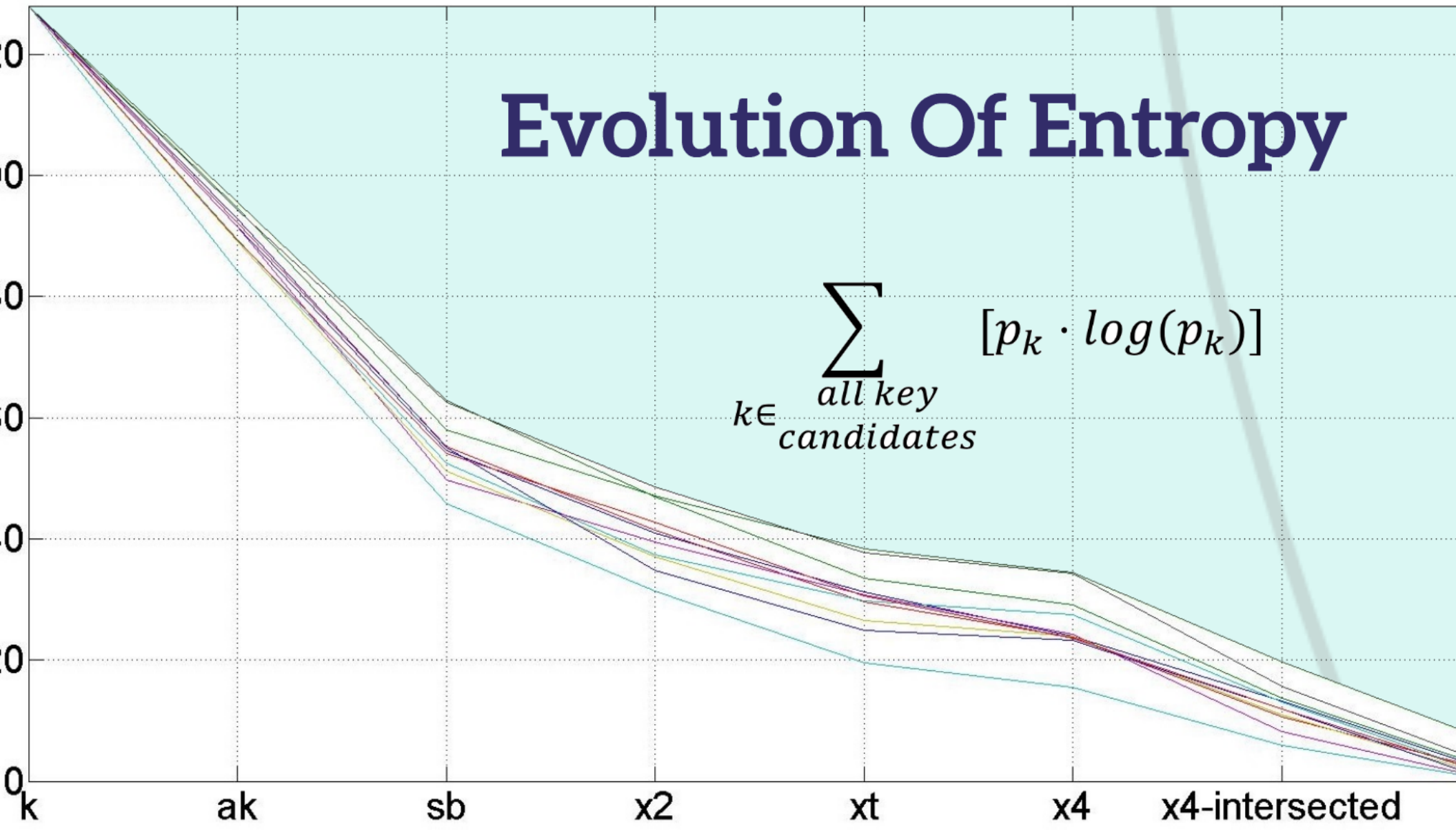
500^2

500^2

500^2

500^2

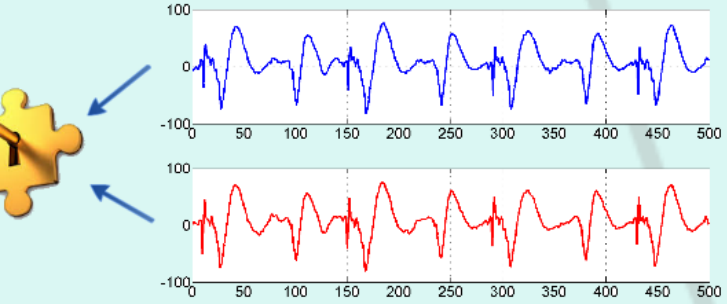
Case	# Required Guesses
Worst Case	$(\text{Max Rank})^4 = (500^2)^4 = 2^7$
Average Case	$(\text{Worst Actual Rank})^4 = 2^3$
Using 2 Power Traces	1^*



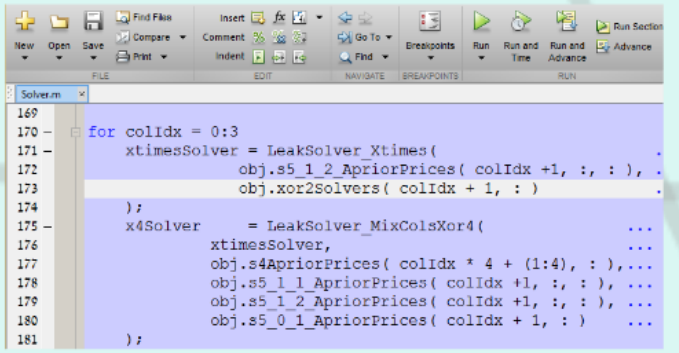
Results on DPA v4 Data Set

Results on DPA v4 Data Set

9 seconds running time per power trace (median)



2 power traces required to yield correct key as rank 1 (at 79.6% success)



Source code available online

Questions?

Sources available at
www.OfirWeisse.com
OfirWeisse@Gmail.com