DPA Contest v2
Evaluation results

Reference attack

November 2010

1 Introduction

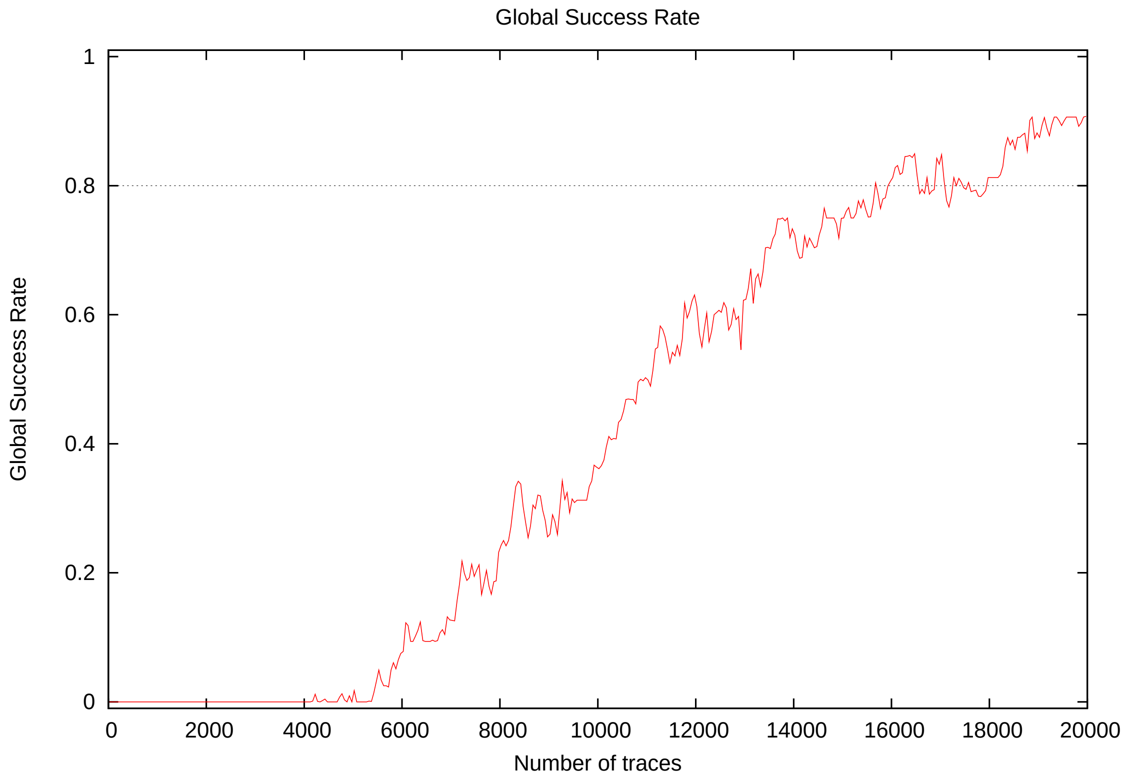
1.1 About the attack

- **Attack Name:** Correlation product v2
- **Sender/Team:** Olivier Meynard
- **Institution:** Télécom ParisTech, France
- **Language:** C
- **Operating system:** Linux
- **Attacked subkey:** 10

1.2 About the evaluation

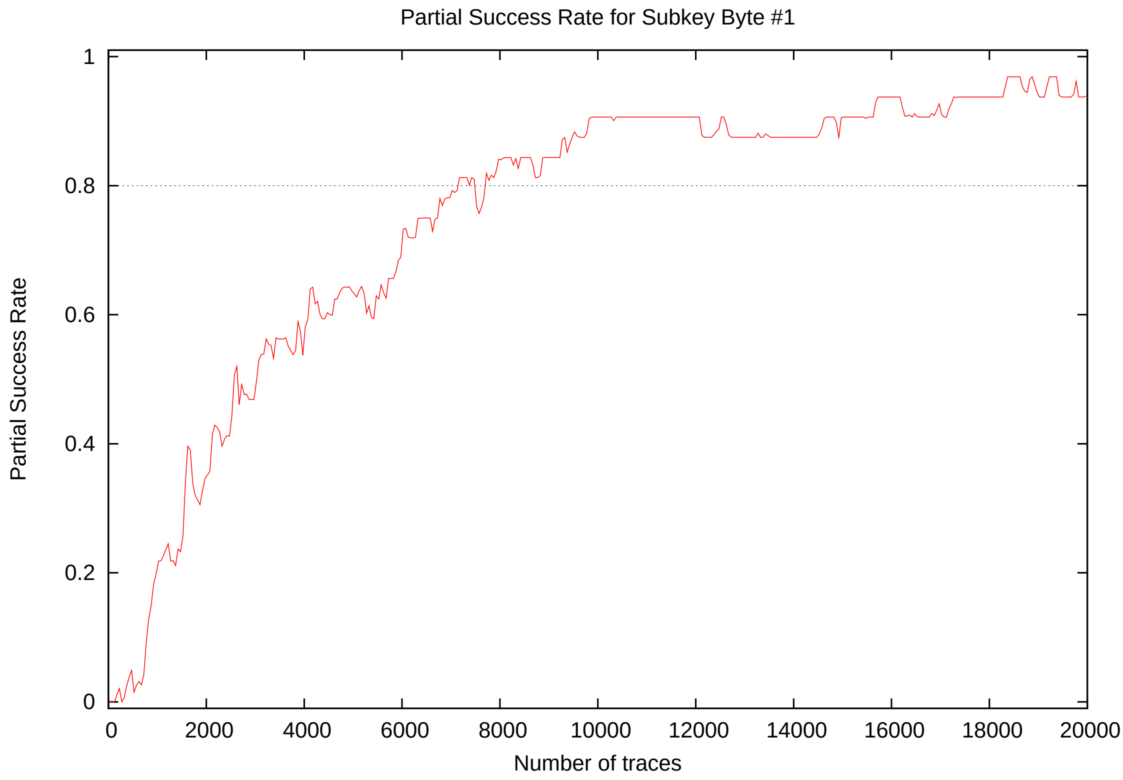
- **Date of evaluation:** November 2010

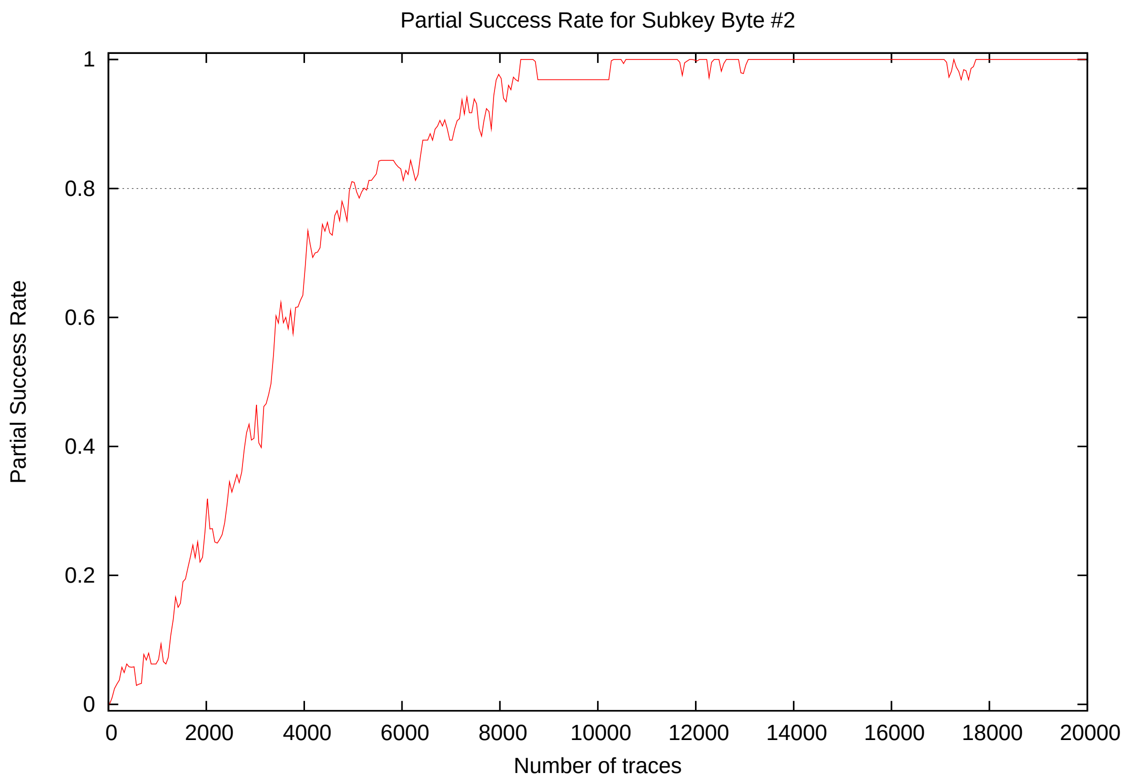
2 Global Success Rate

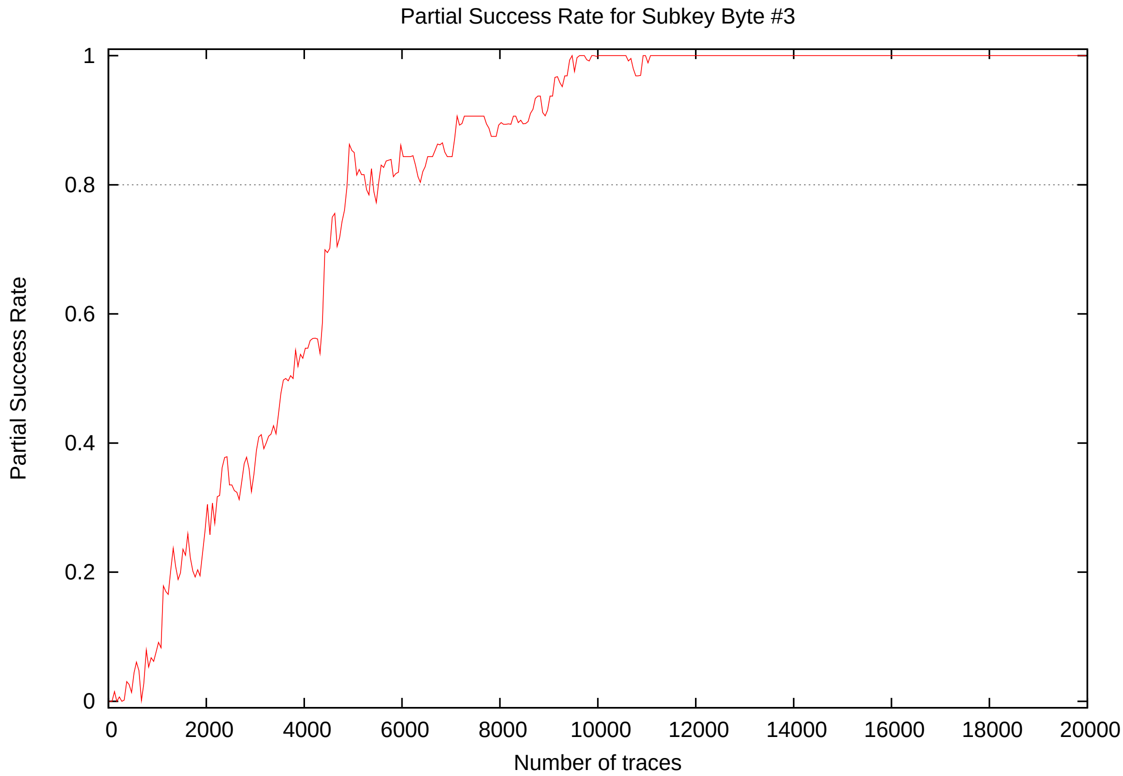


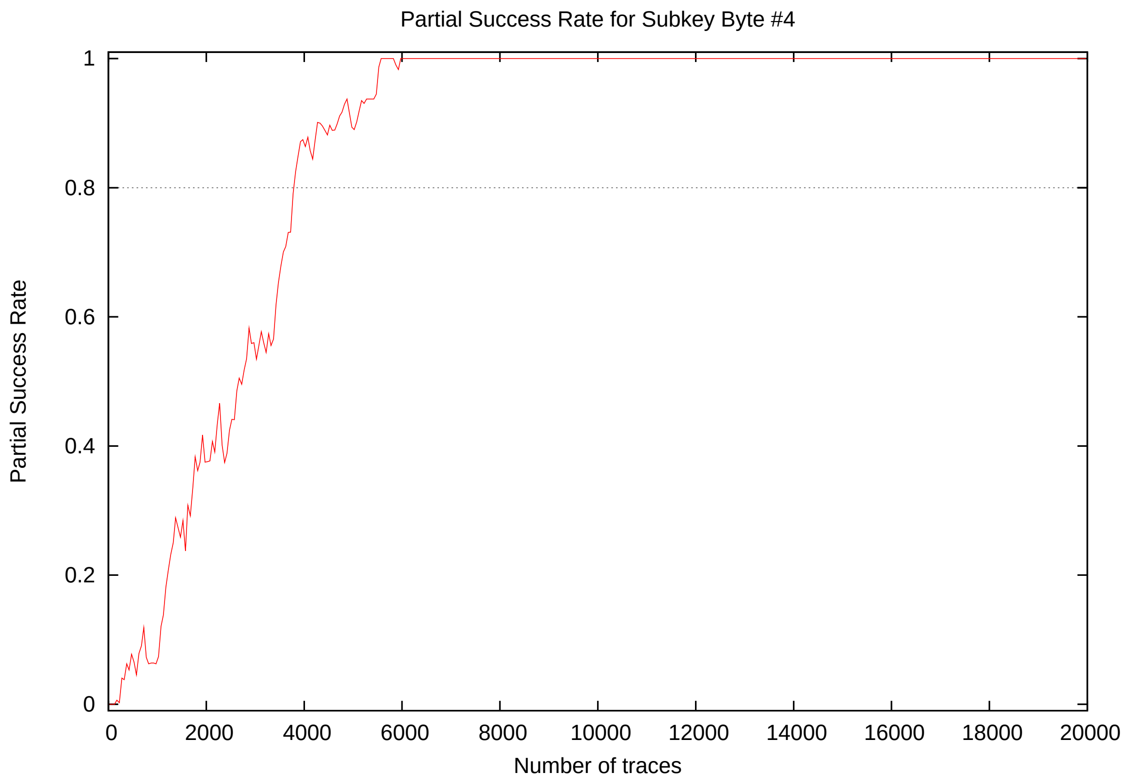
Number of traces	Global Success Rate
10	0.00
20	0.00
30	0.00
40	0.00
50	0.00
100	0.00
200	0.00
300	0.00
400	0.00
500	0.00
1000	0.00
2000	0.00
3000	0.00
4000	0.00
5000	0.00
10000	0.34
15000	0.75
20000	0.91

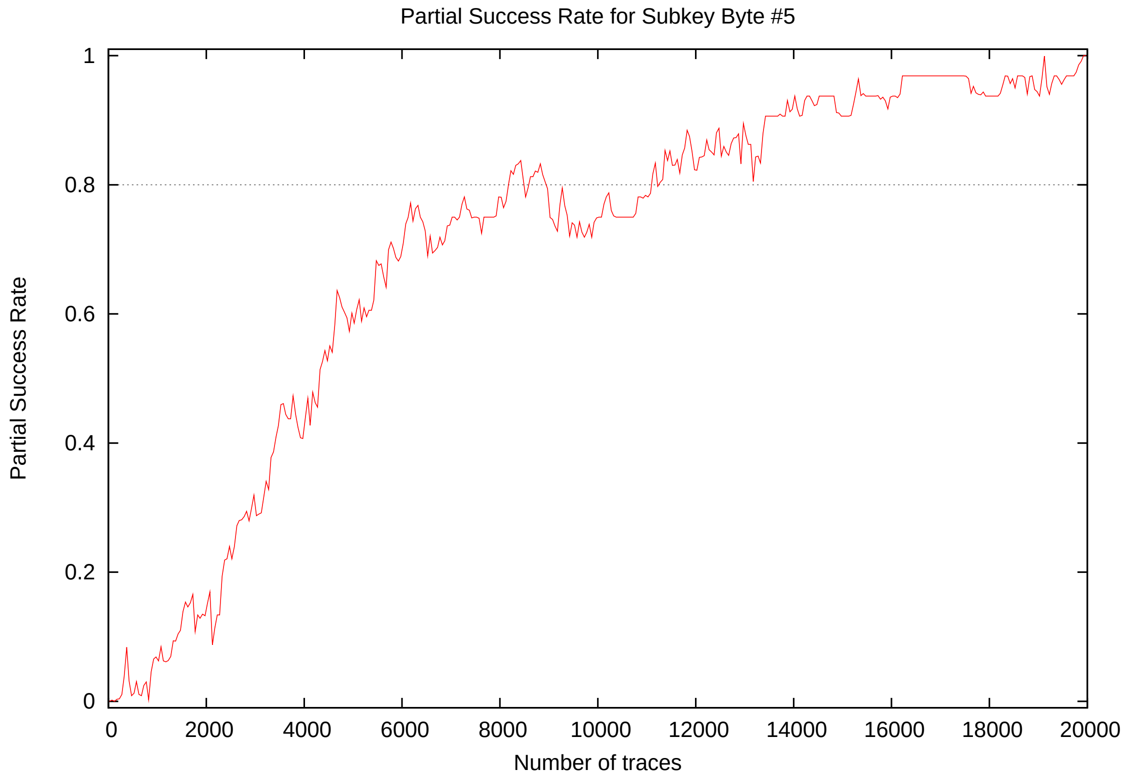
3 Partial Success Rate

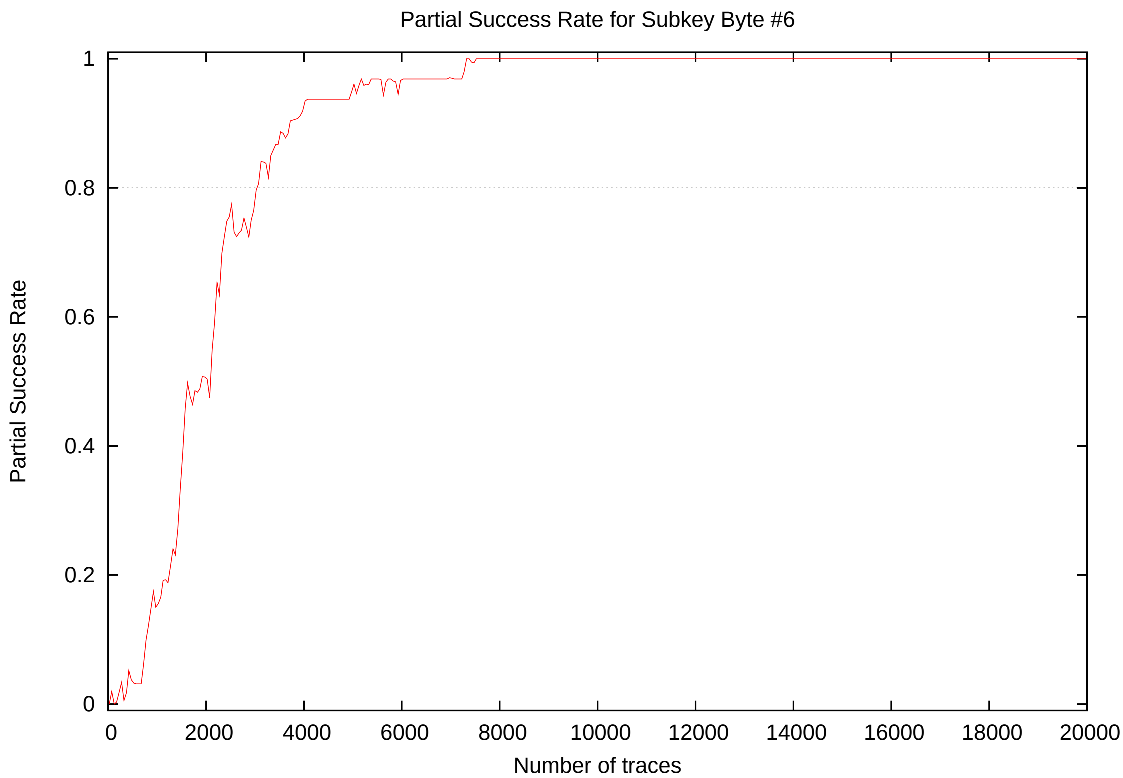


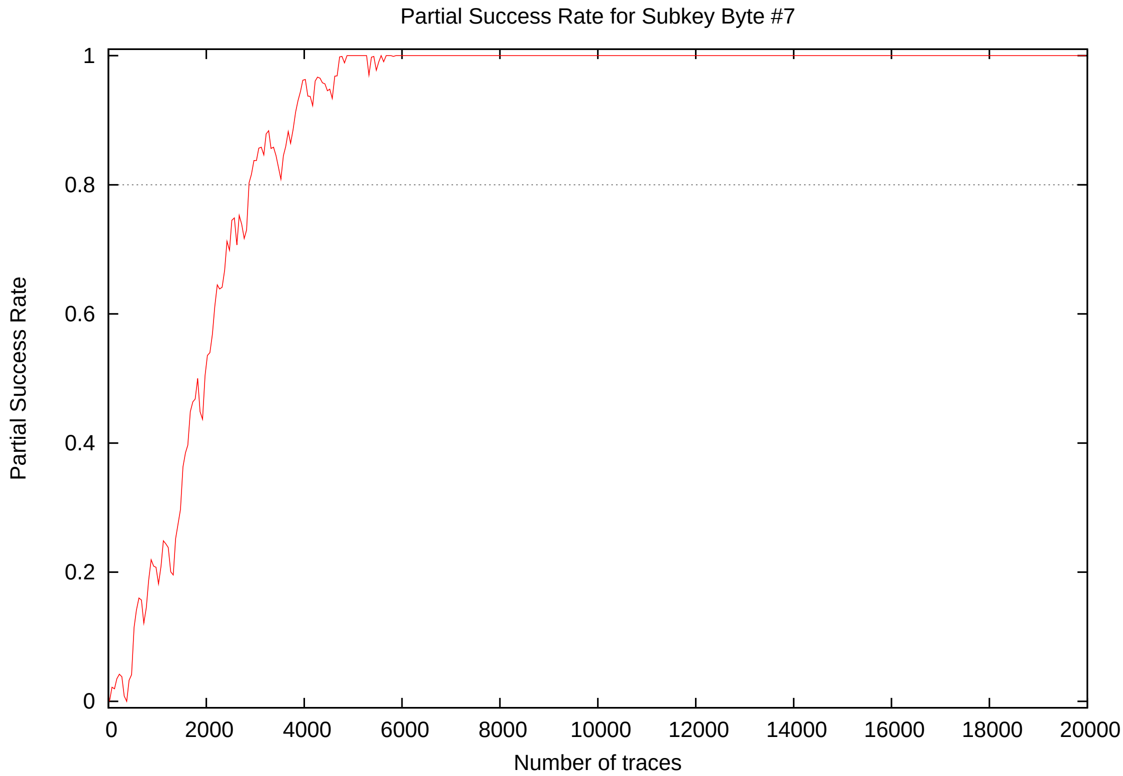


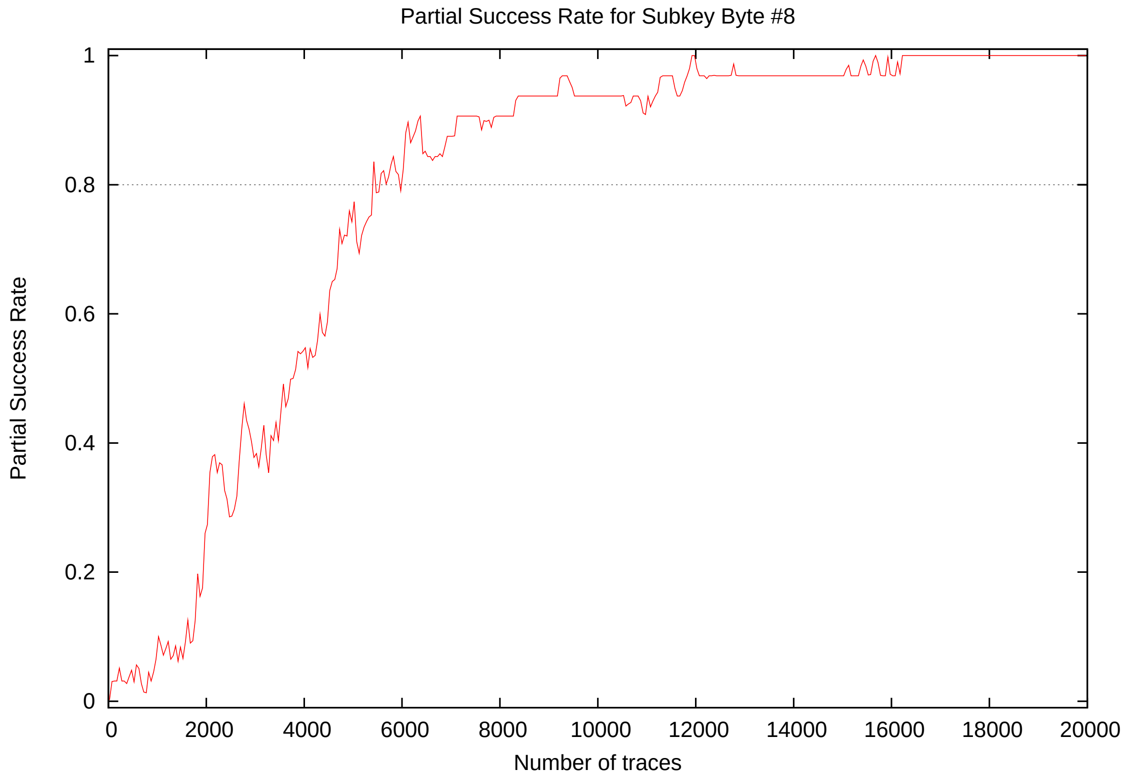

Partial Success Rate for Subkey Byte #3
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000

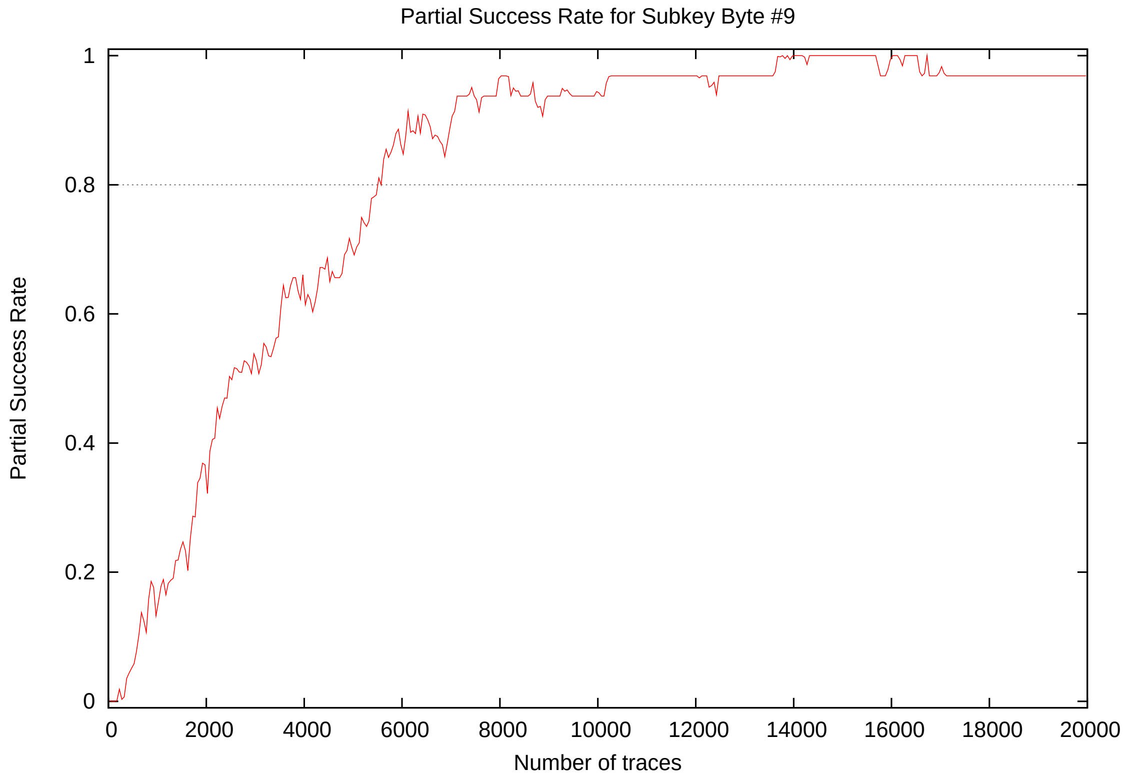

Partial Success Rate for Subkey Byte #4
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000

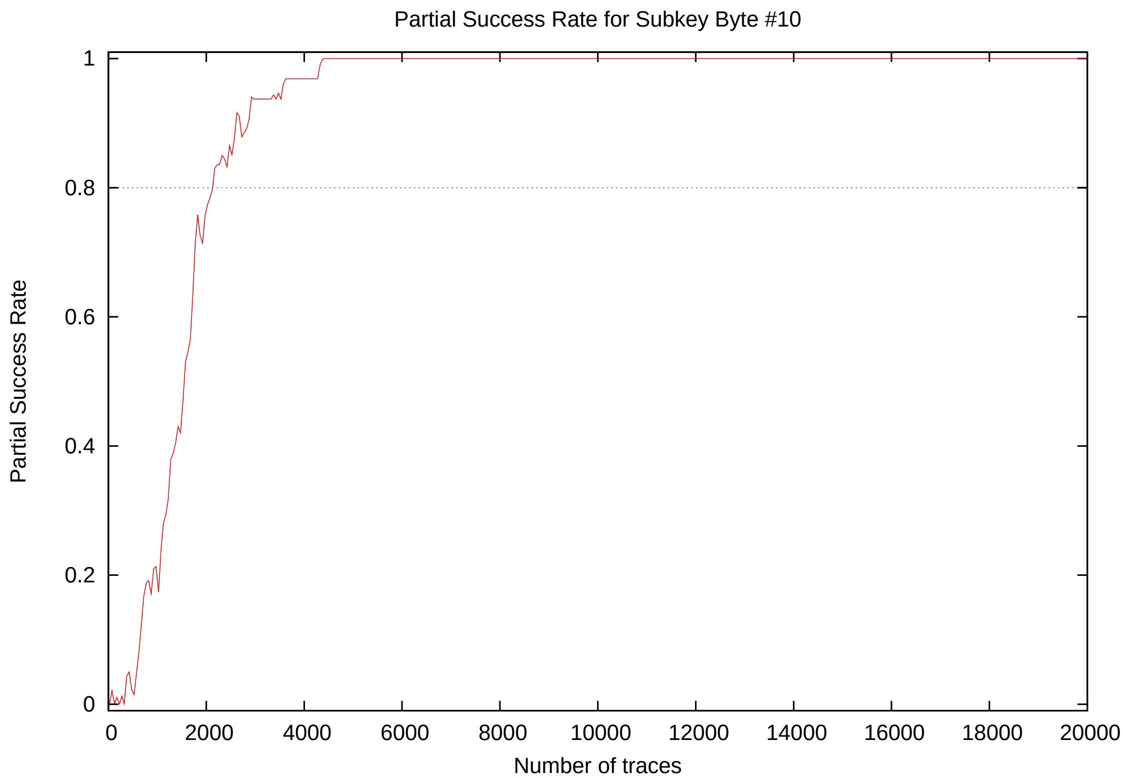

Partial Success Rate for Subkey Byte #5
Partial Success Rate
1
0.8
0.6
0.4
0.2
0
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000
Number of traces

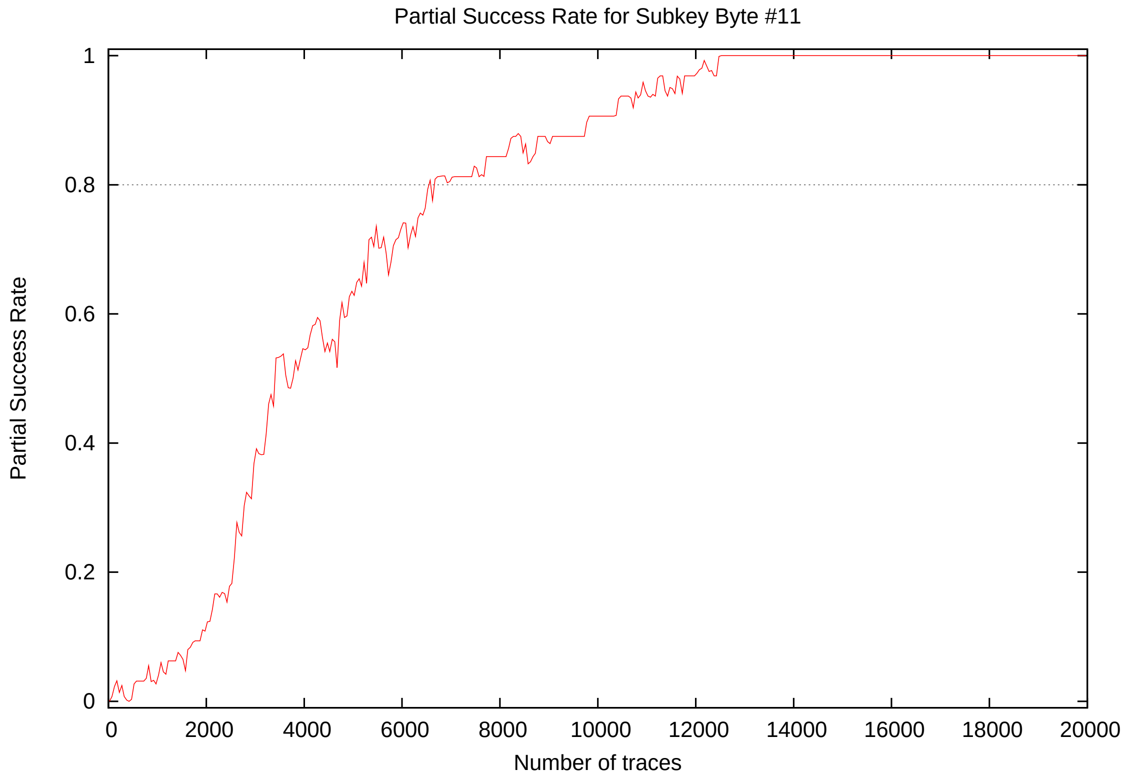

Partial Success Rate for Subkey Byte #6
Partial Success Rate
1
0.8
0.6
0.4
0.2
0
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000
Number of traces

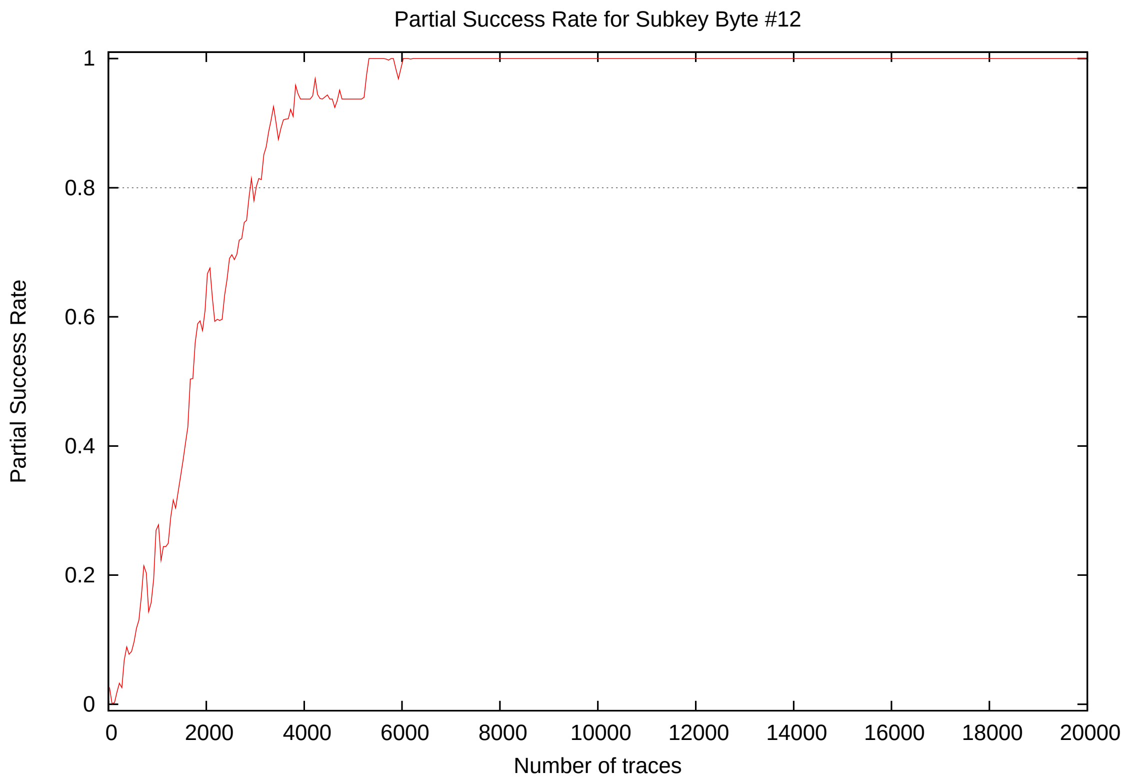

Partial Success Rate for Subkey Byte #7
Partial Success Rate
0
0.2
0.4
0.6
0.8
1
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000
Number of traces

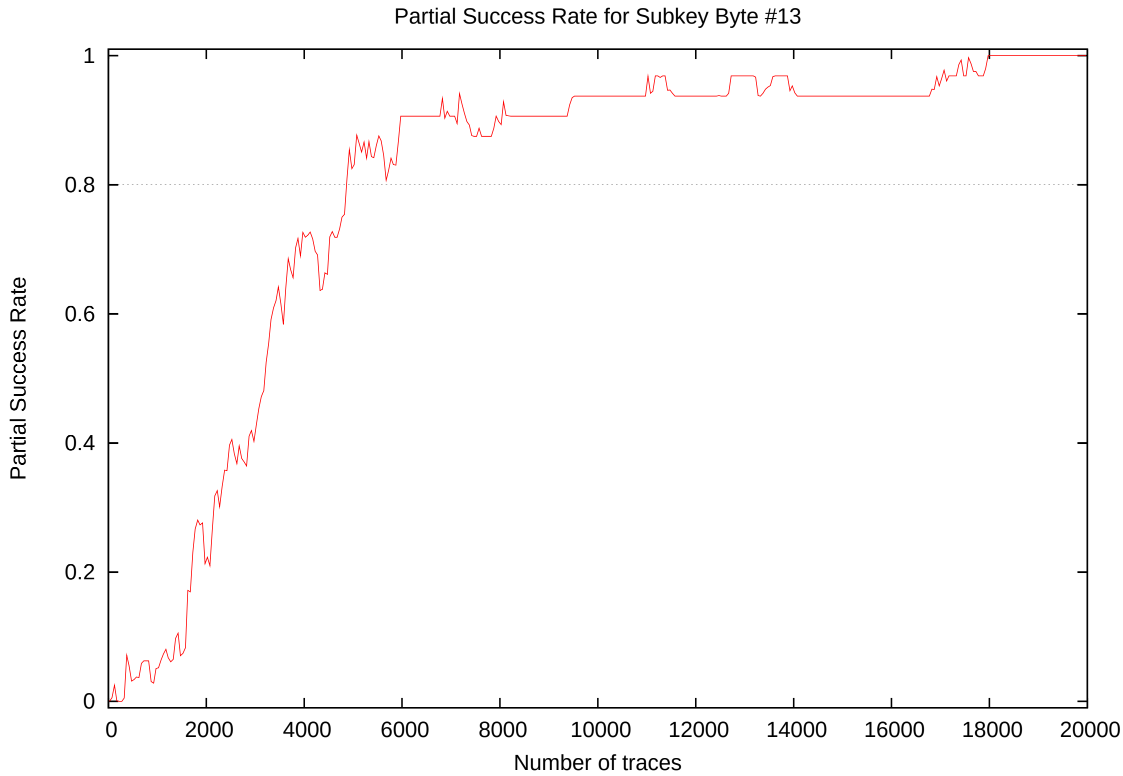

Partial Success Rate for Subkey Byte #8
Partial Success Rate
0
0.2
0.4
0.6
0.8
1
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000
Number of traces

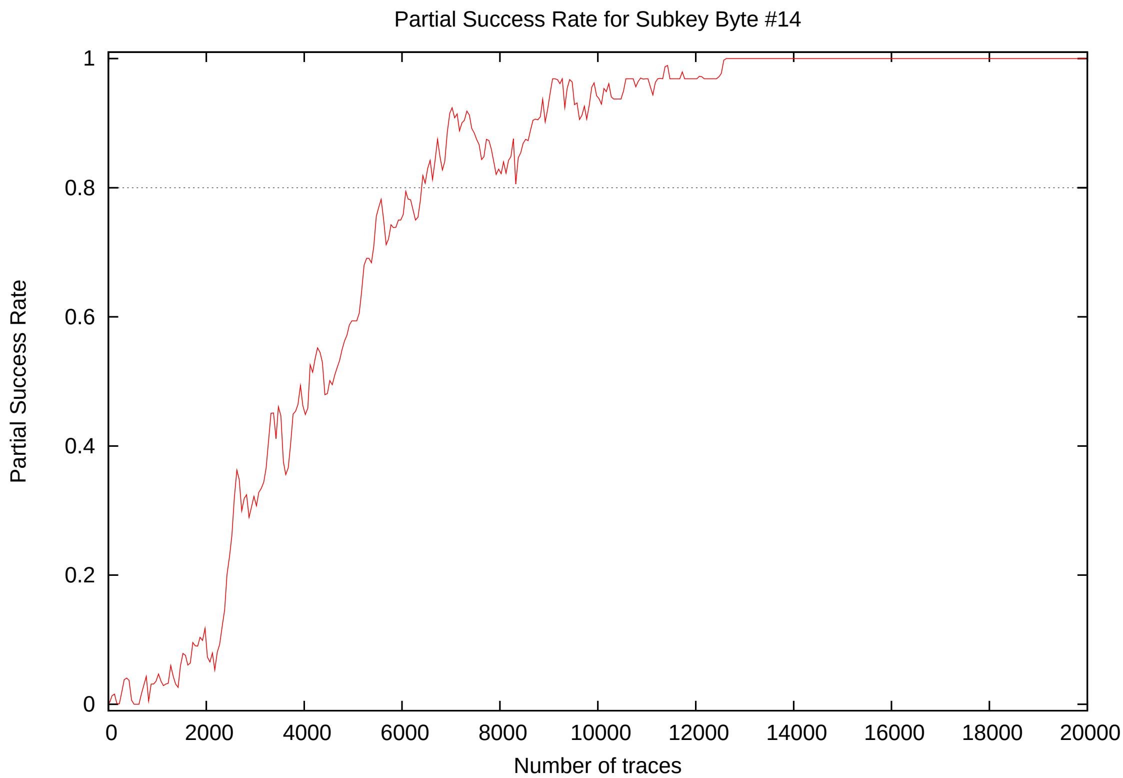

Partial Success Rate for Subkey Byte #9
Partial Success Rate
0
0.2
0.4
0.6
0.8
1
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000
Number of traces

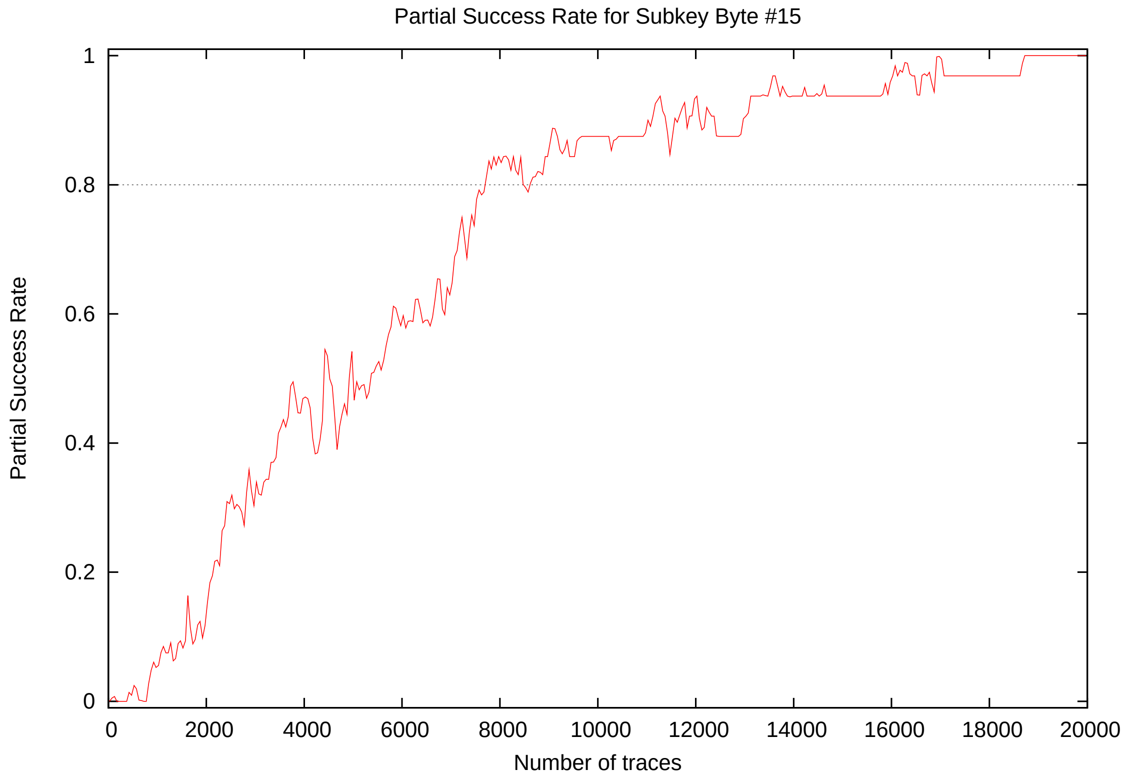

Partial Success Rate for Subkey Byte #10
Partial Success Rate
0
0.2
0.4
0.6
0.8
1
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000
Number of traces

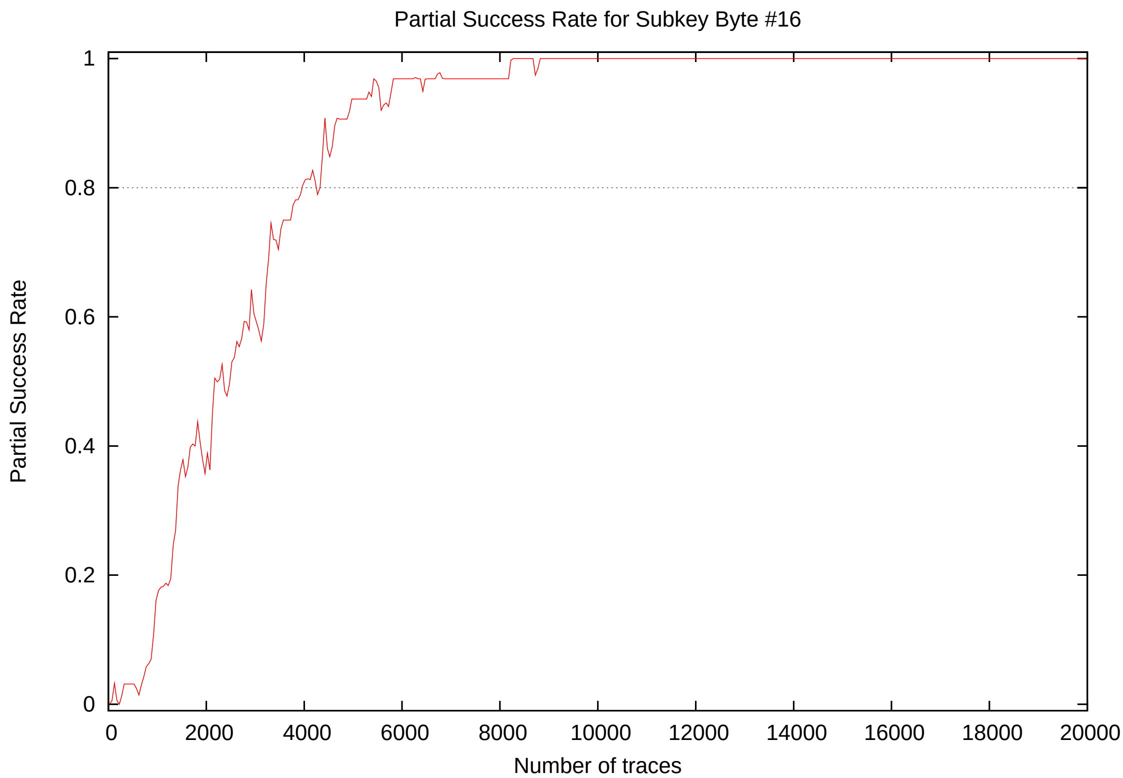

Partial Success Rate for Subkey Byte #11
Partial Success Rate
1
0.8
0.6
0.4
0.2
0
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000
Number of traces

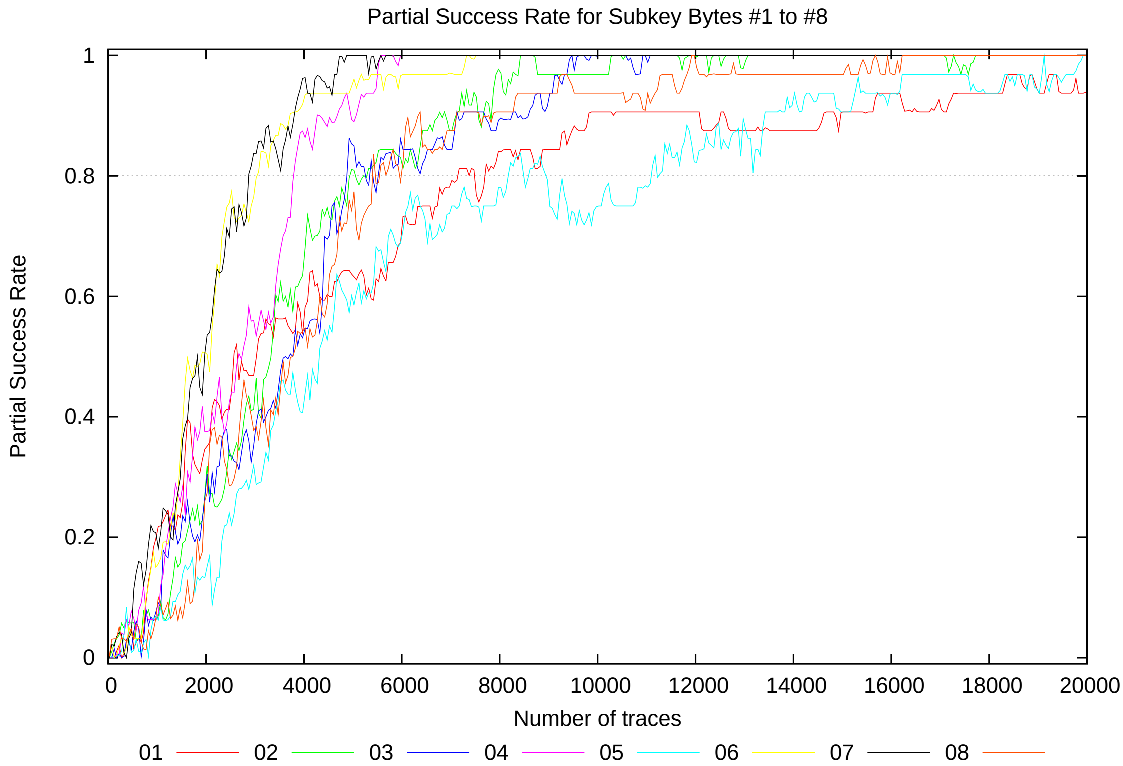

Partial Success Rate for Subkey Byte #12
Partial Success Rate
1
0.8
0.6
0.4
0.2
0
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000
Number of traces

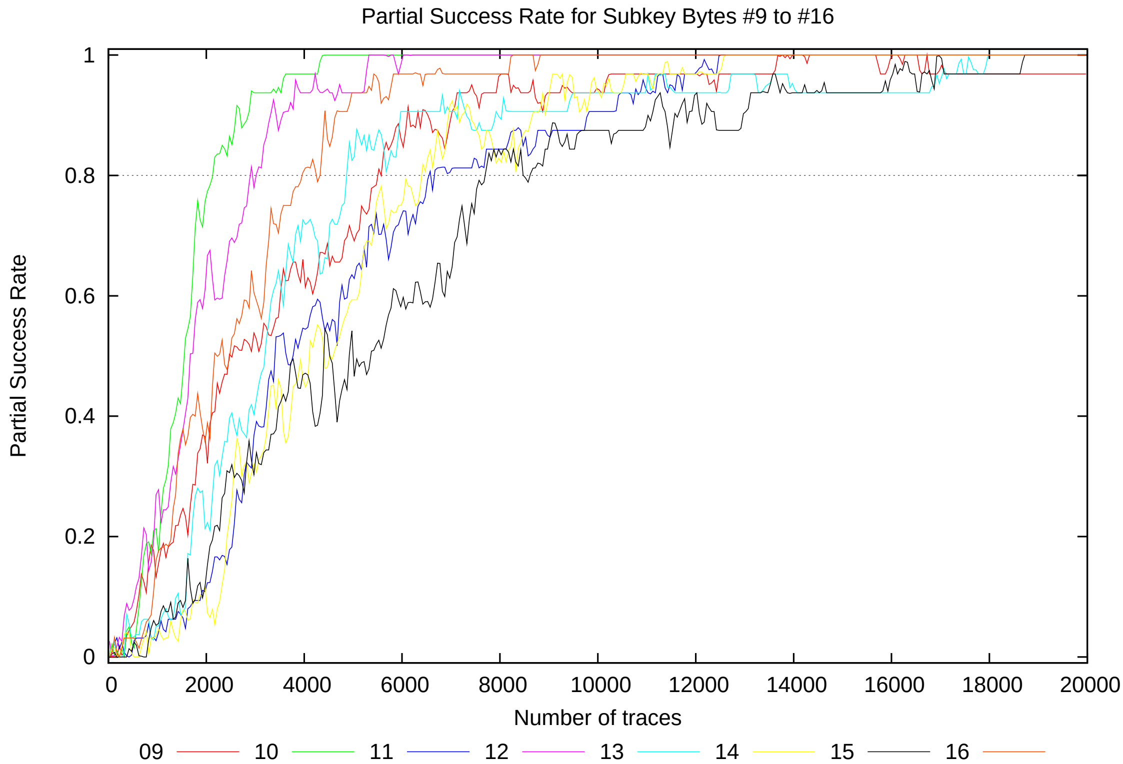

Partial Success Rate for Subkey Byte #13
Partial Success Rate
0
0.2
0.4
0.6
0.8
1
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000
Number of traces

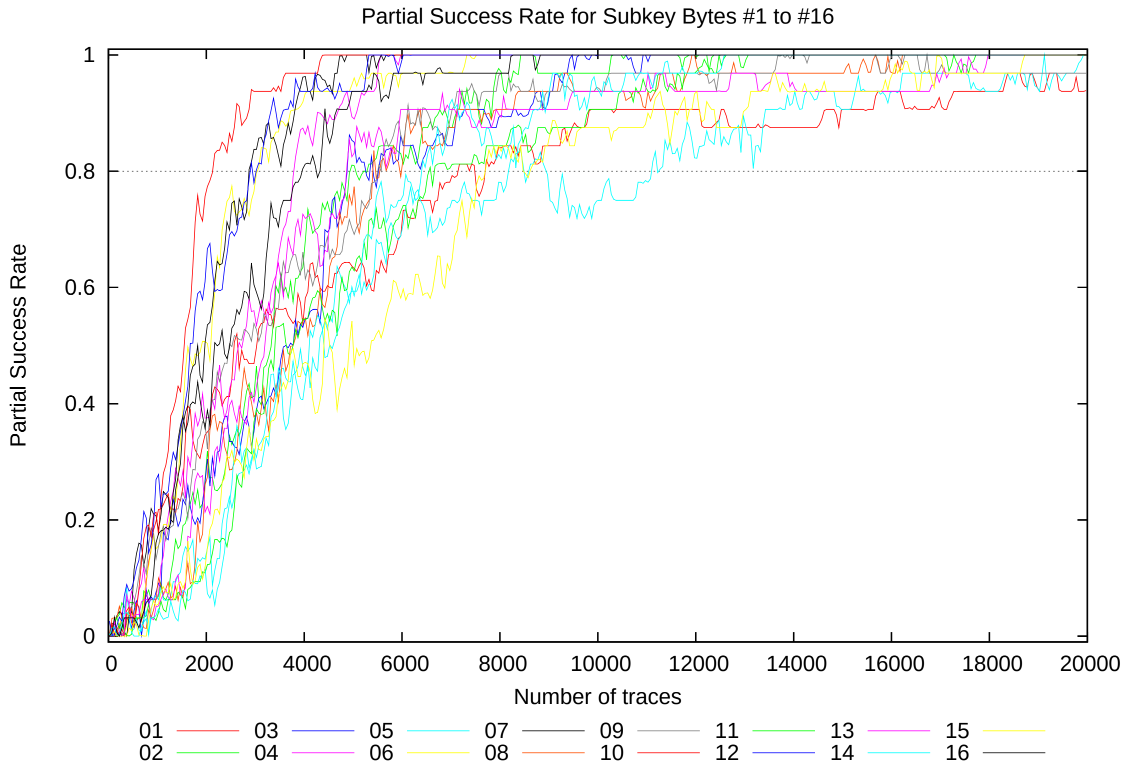

Partial Success Rate for Subkey Byte #14
Partial Success Rate
0
0.2
0.4
0.6
0.8
1
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000
Number of traces


Partial Success Rate for Subkey Byte #15
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000


Partial Success Rate for Subkey Byte #16
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000

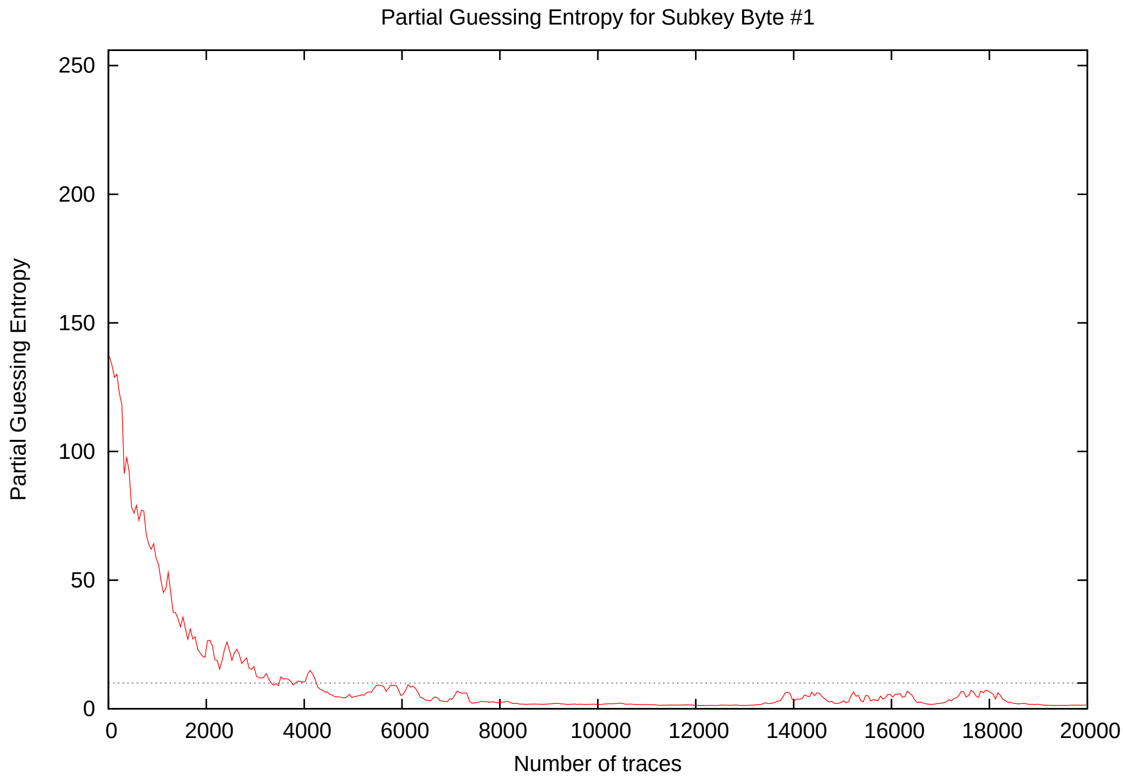

Partial Success Rate for Subkey Bytes #1 to #8
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000
01
02
03
04
05
06
07
08

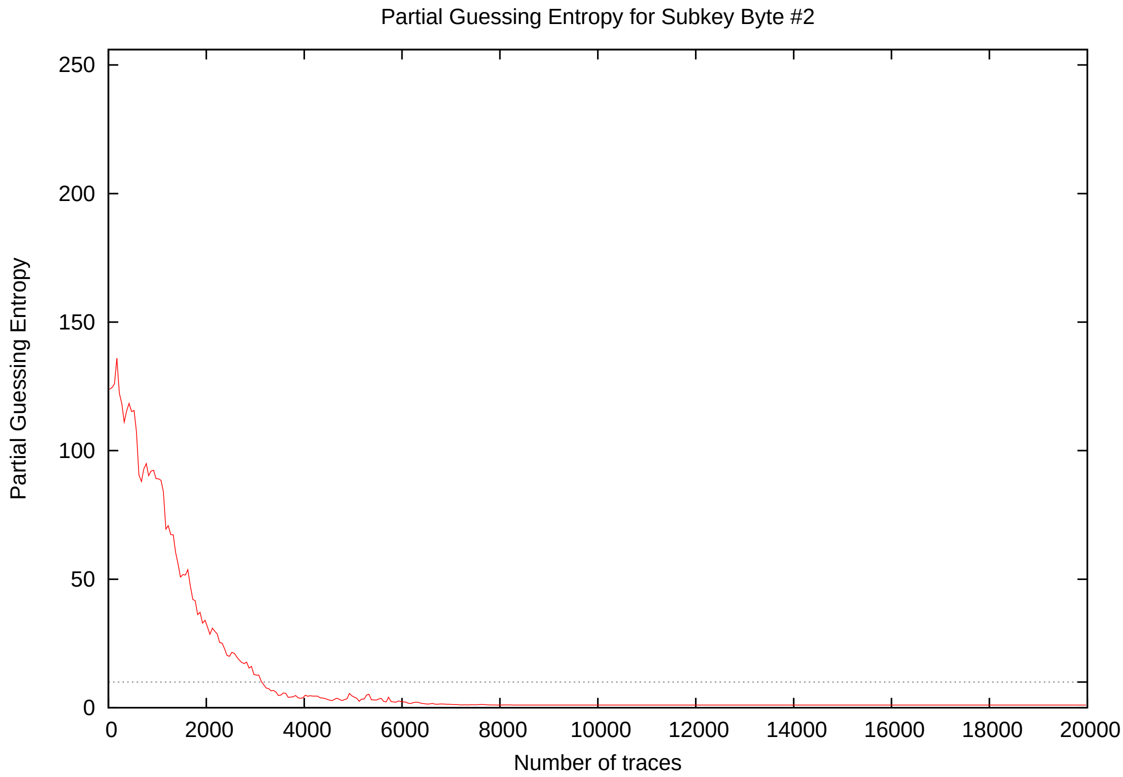

Partial Success Rate for Subkey Bytes #9 to #16
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000
09
10
11
12
13
14
15
16

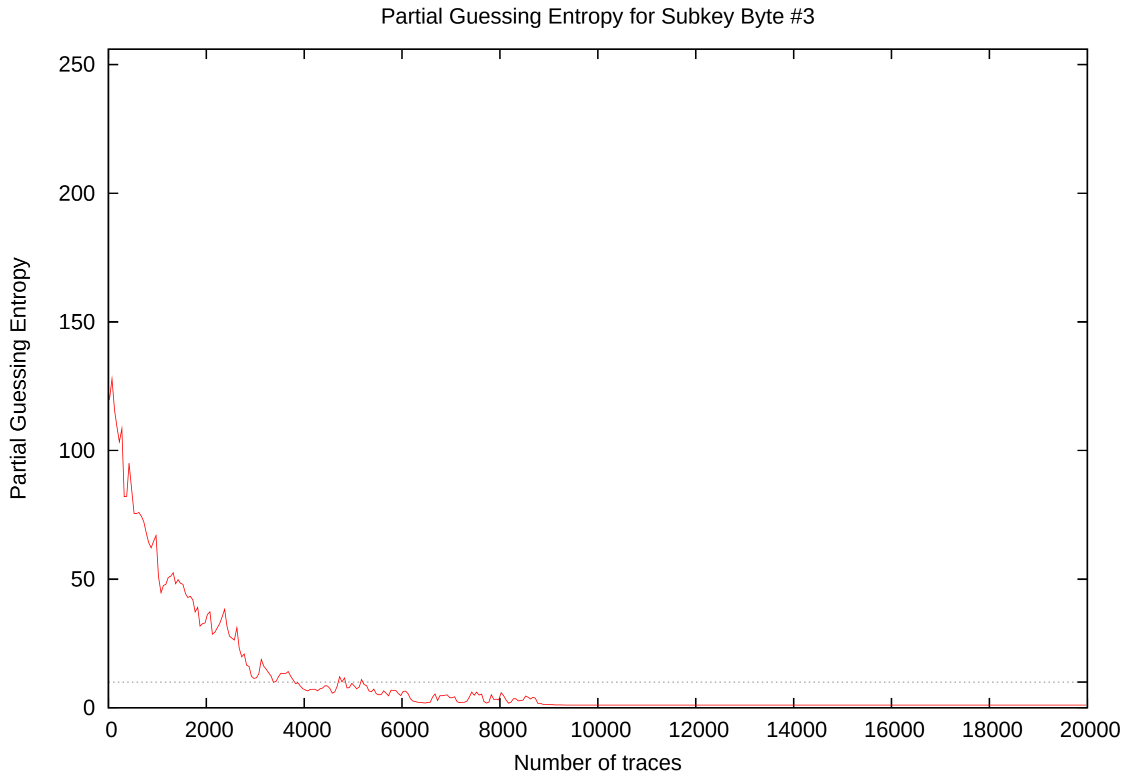

Partial Success Rate for Subkey Bytes #1 to #16
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000
01
02
03
04
05
06
07
08
09
10
11
12
13
14
15
16

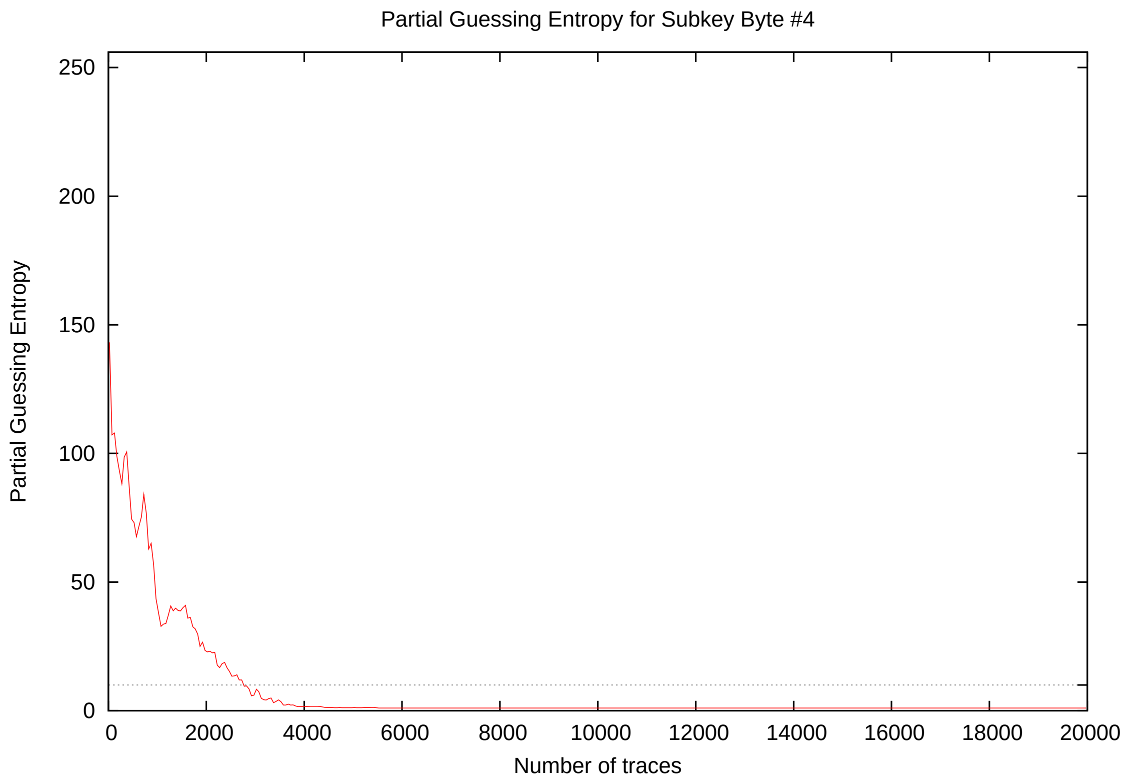
Traces	Partial Success Rate / Byte																Min	Max	Mean
	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16			
10	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.03	0.00	0.00	0.00	0.00	0.00	0.03	0.00
20	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.03	0.00	0.00	0.00	0.00	0.00	0.03	0.00
30	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.03	0.00	0.00	0.00	0.00	0.00	0.03	0.00
40	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.03	0.00	0.00	0.00	0.00	0.00	0.03	0.00
50	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.03	0.00	0.00	0.00	0.00	0.00	0.03	0.00	0.00	0.00	0.03	0.00
100	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.03	0.00	0.00	0.03	0.00	0.03	0.00	0.00	0.03	0.00	0.03	0.01
200	0.03	0.03	0.00	0.03	0.00	0.03	0.03	0.03	0.03	0.00	0.03	0.03	0.00	0.00	0.00	0.00	0.00	0.03	0.02
300	0.00	0.06	0.00	0.06	0.03	0.03	0.03	0.03	0.00	0.00	0.03	0.03	0.00	0.03	0.00	0.03	0.00	0.06	0.02
400	0.03	0.06	0.06	0.03	0.06	0.03	0.00	0.03	0.06	0.06	0.00	0.12	0.09	0.09	0.00	0.03	0.00	0.12	0.05
500	0.03	0.03	0.03	0.06	0.00	0.03	0.06	0.03	0.06	0.00	0.03	0.09	0.03	0.00	0.00	0.03	0.00	0.09	0.03
1000	0.19	0.06	0.06	0.06	0.06	0.12	0.19	0.09	0.16	0.19	0.03	0.28	0.06	0.06	0.06	0.19	0.03	0.28	0.12
2000	0.34	0.31	0.28	0.38	0.16	0.53	0.56	0.28	0.31	0.75	0.09	0.66	0.22	0.06	0.12	0.38	0.06	0.75	0.34
3000	0.47	0.50	0.38	0.56	0.31	0.78	0.84	0.41	0.53	0.94	0.38	0.78	0.47	0.34	0.34	0.62	0.31	0.94	0.54
4000	0.53	0.69	0.53	0.88	0.38	0.91	0.97	0.53	0.69	0.97	0.56	0.94	0.72	0.50	0.47	0.81	0.38	0.97	0.69
5000	0.62	0.81	0.84	0.88	0.59	0.97	1.00	0.72	0.69	1.00	0.66	0.94	0.81	0.59	0.50	0.94	0.50	1.00	0.79
10000	0.91	0.97	1.00	1.00	0.75	1.00	1.00	0.94	0.94	1.00	0.91	1.00	0.94	0.94	0.88	1.00	0.75	1.00	0.95
15000	0.91	1.00	1.00	1.00	0.91	1.00	1.00	0.97	1.00	1.00	1.00	1.00	0.94	1.00	0.94	1.00	0.91	1.00	0.98
20000	0.94	1.00	1.00	1.00	1.00	1.00	1.00	1.00	0.97	1.00	1.00	1.00	1.00	1.00	1.00	1.00	0.94	1.00	0.99

4 Partial Guessing Entropy

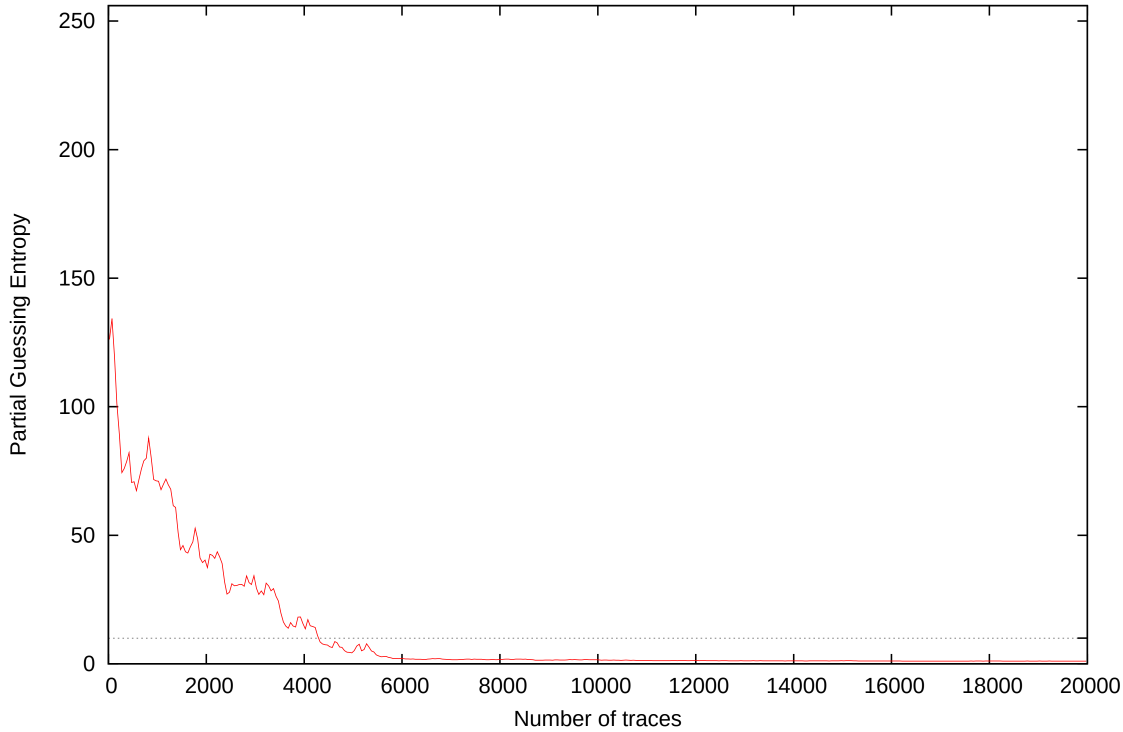




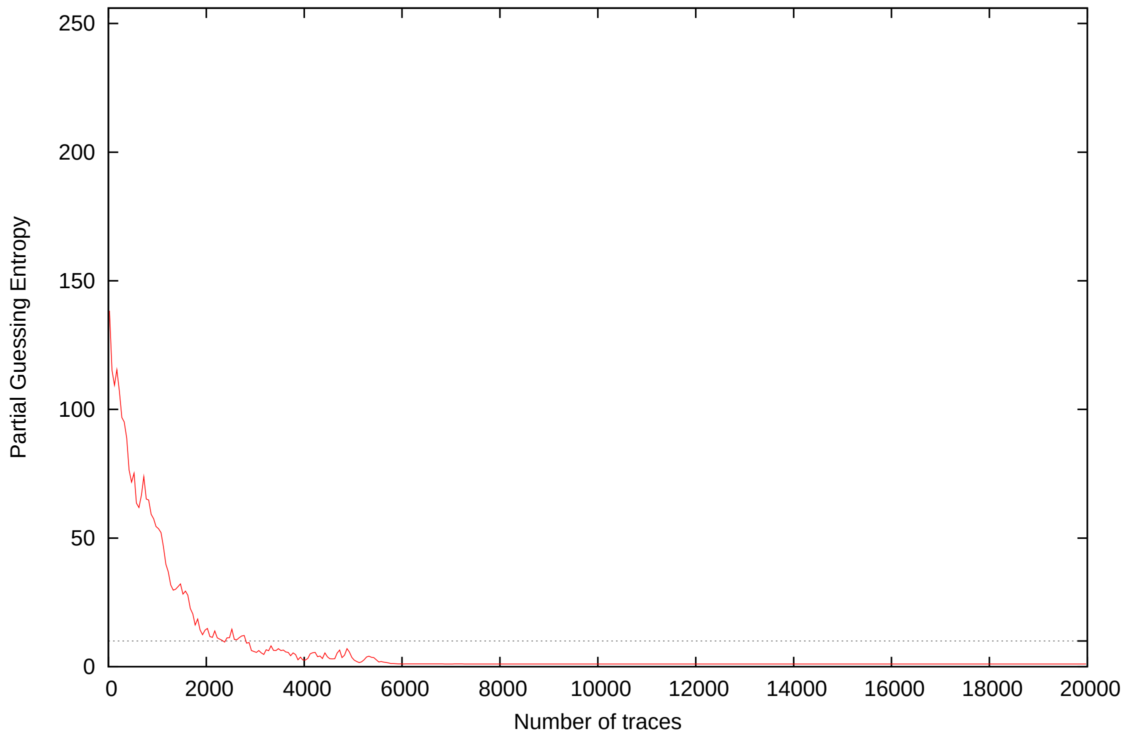

Partial Guessing Entropy for Subkey Byte #3
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000

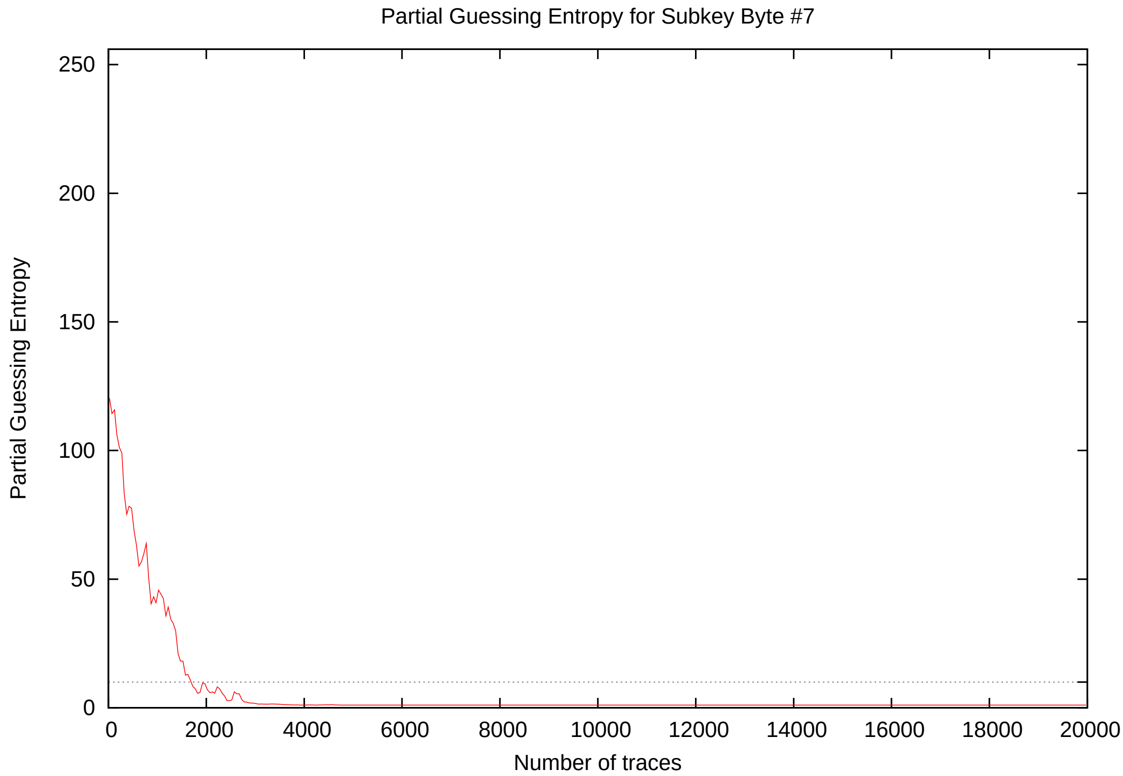

Partial Guessing Entropy for Subkey Byte #4
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000

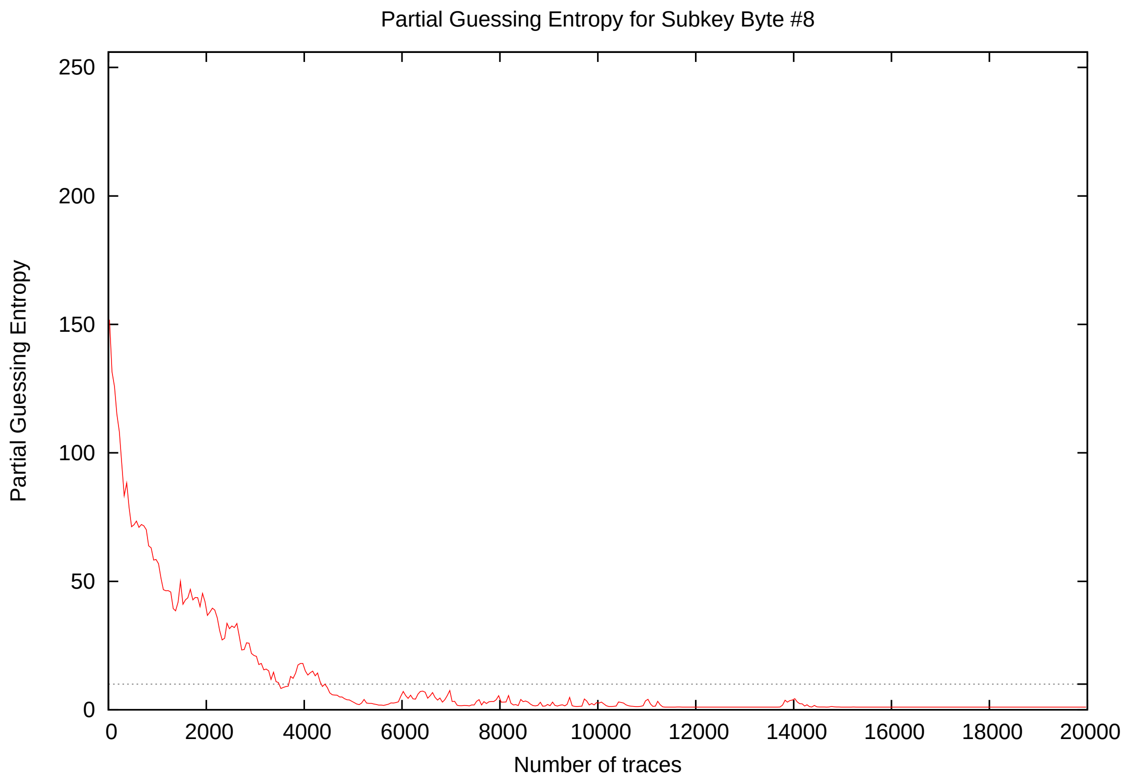
Partial Guessing Entropy for Subkey Byte #5



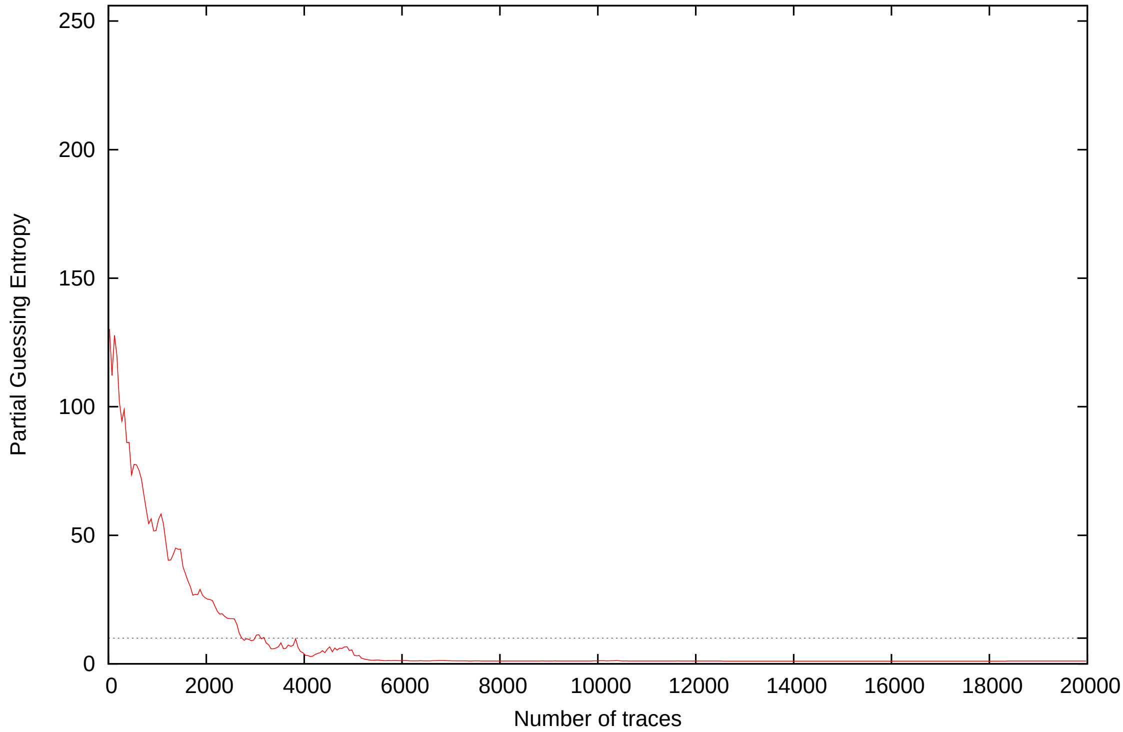
Partial Guessing Entropy for Subkey Byte #6



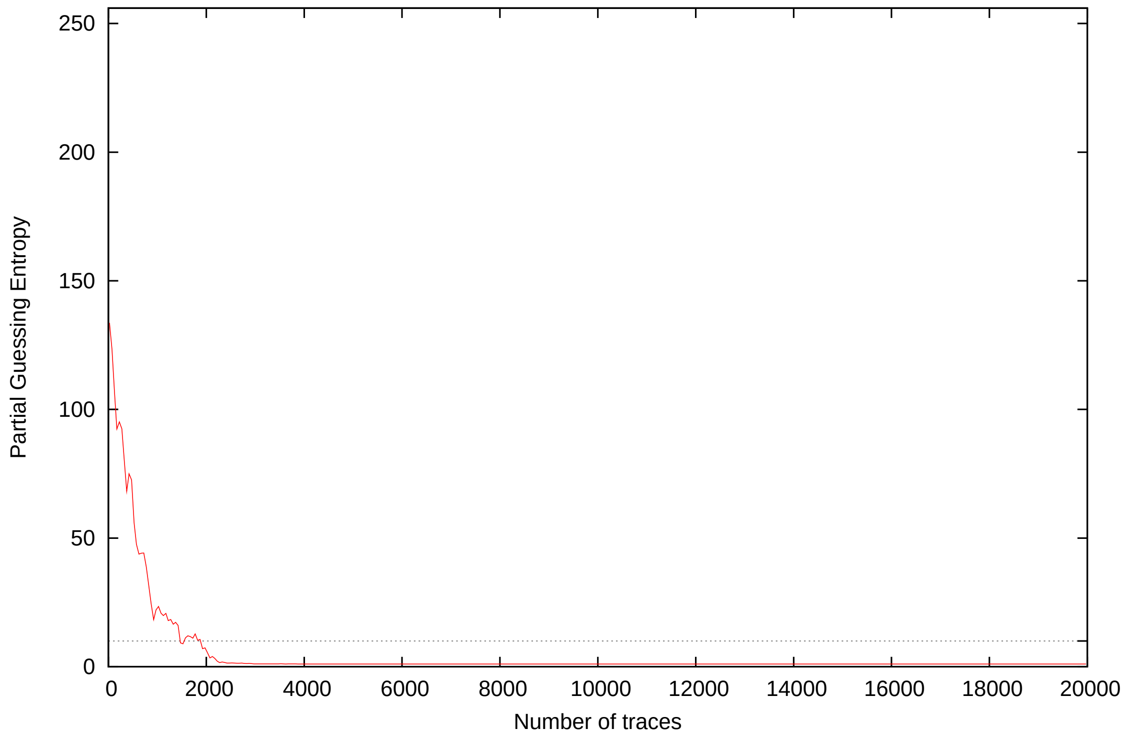

Partial Guessing Entropy for Subkey Byte #7
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000

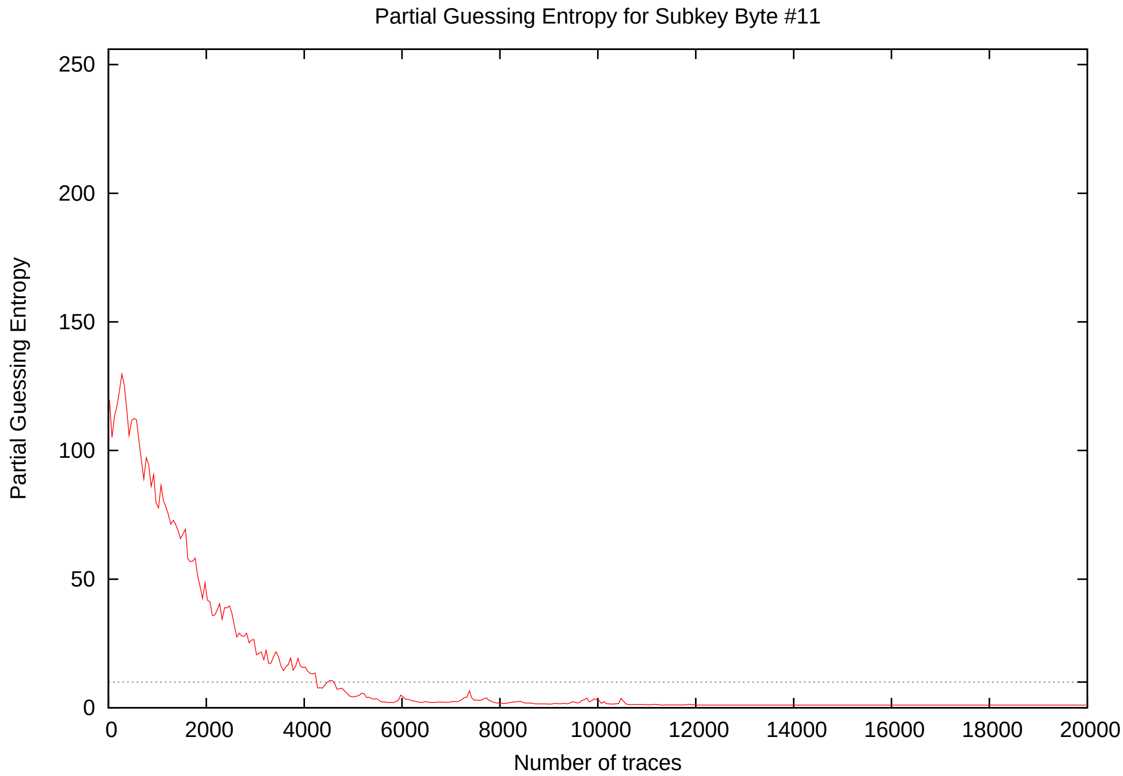

Partial Guessing Entropy for Subkey Byte #8
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000

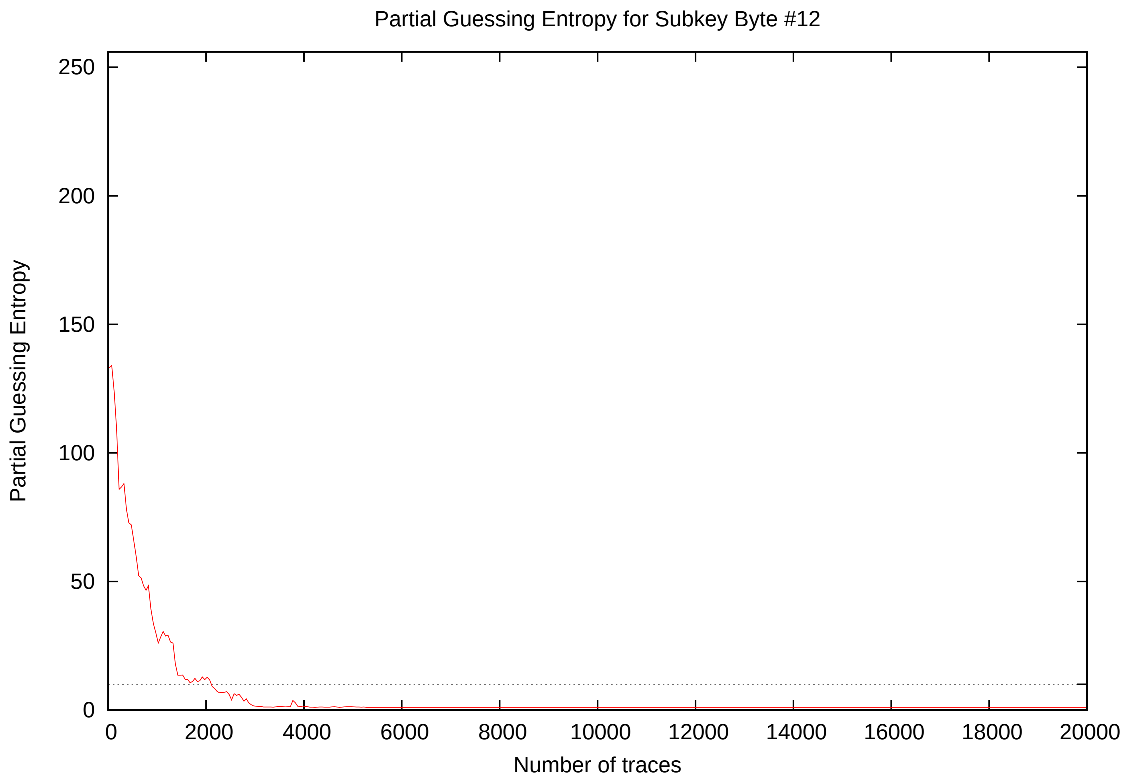
Partial Guessing Entropy for Subkey Byte #9



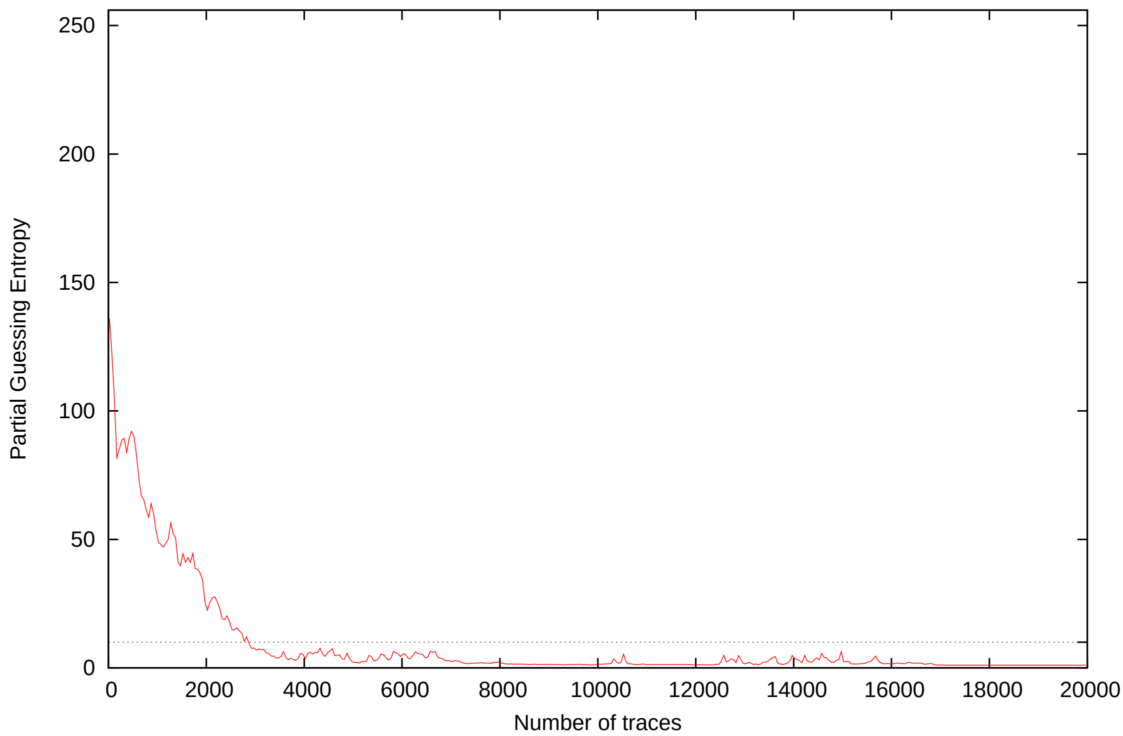
Partial Guessing Entropy for Subkey Byte #10



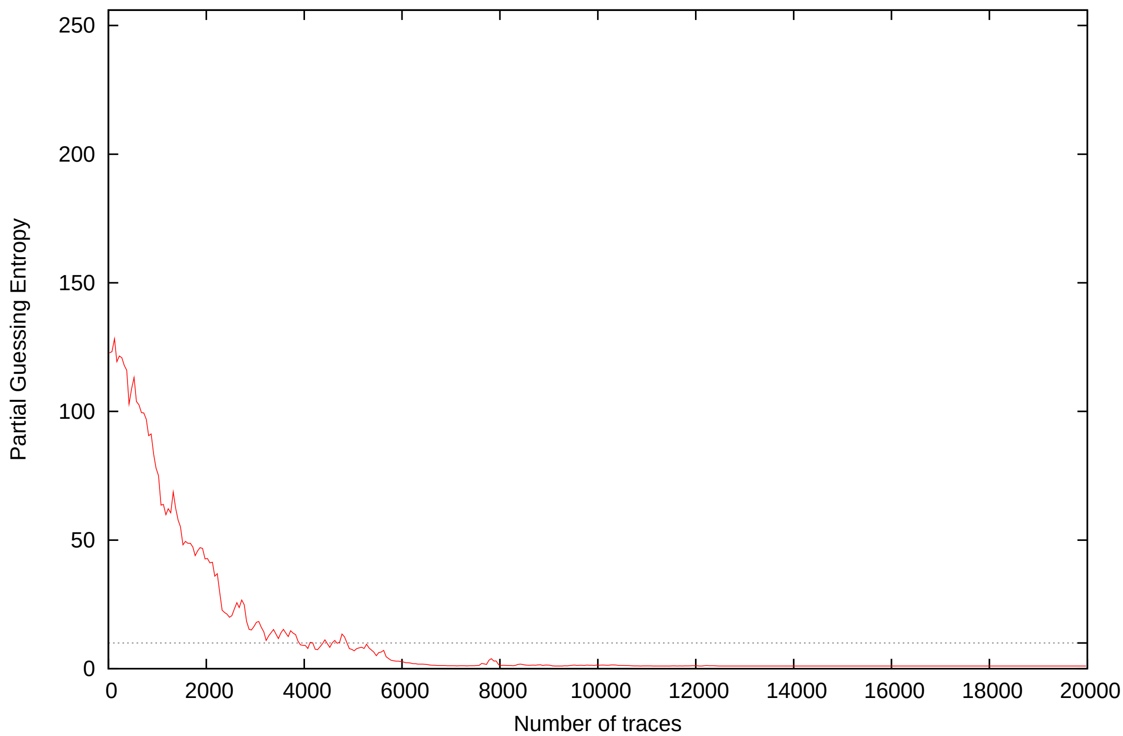

Partial Guessing Entropy for Subkey Byte #11
Partial Guessing Entropy
0
50
100
150
200
250
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000
Number of traces


Partial Guessing Entropy for Subkey Byte #12
Partial Guessing Entropy
0
50
100
150
200
250
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000
Number of traces

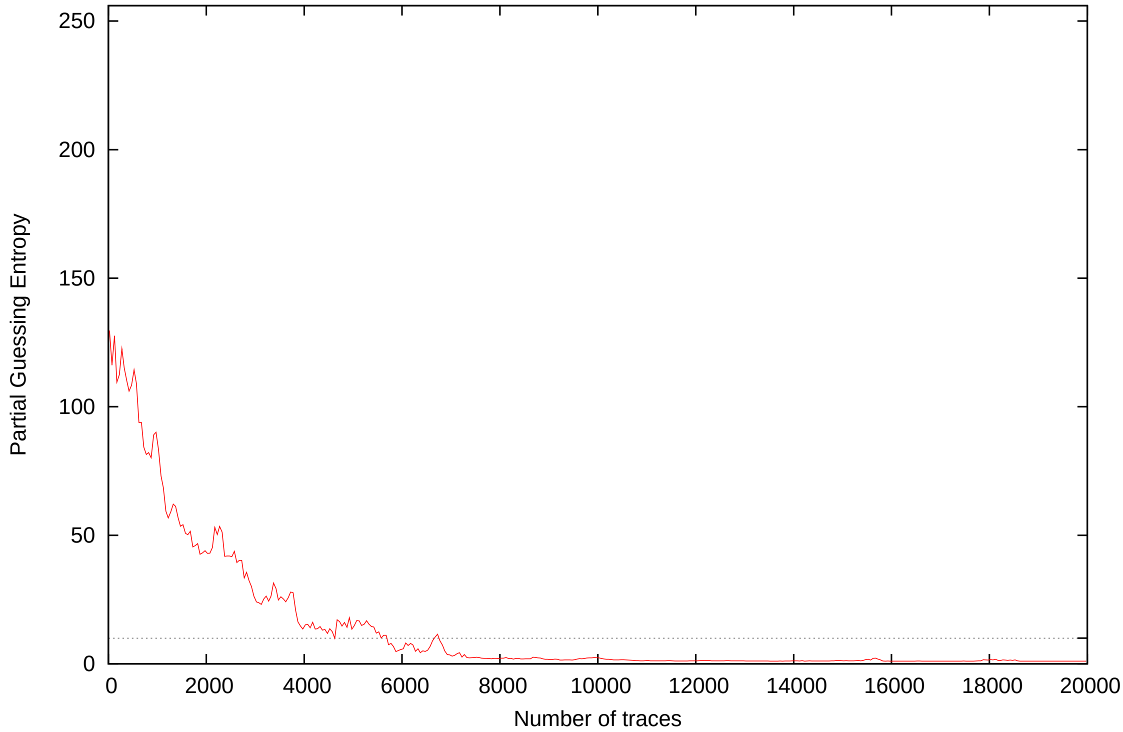
Partial Guessing Entropy for Subkey Byte #13



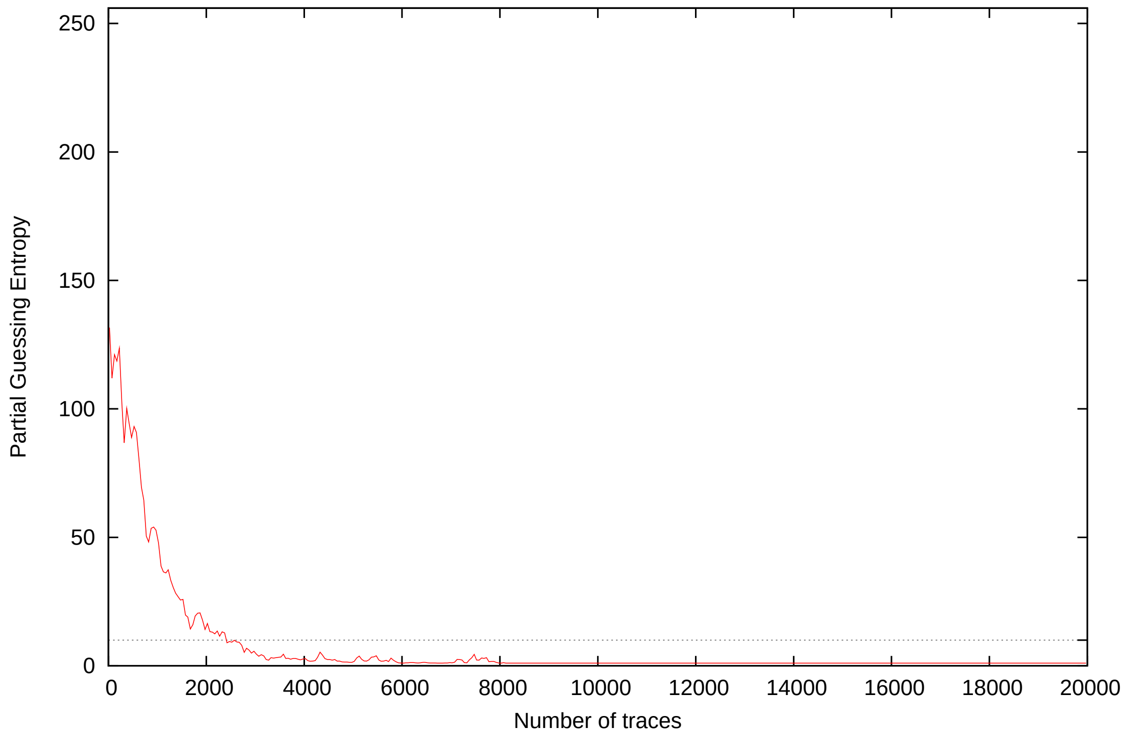
Partial Guessing Entropy for Subkey Byte #14

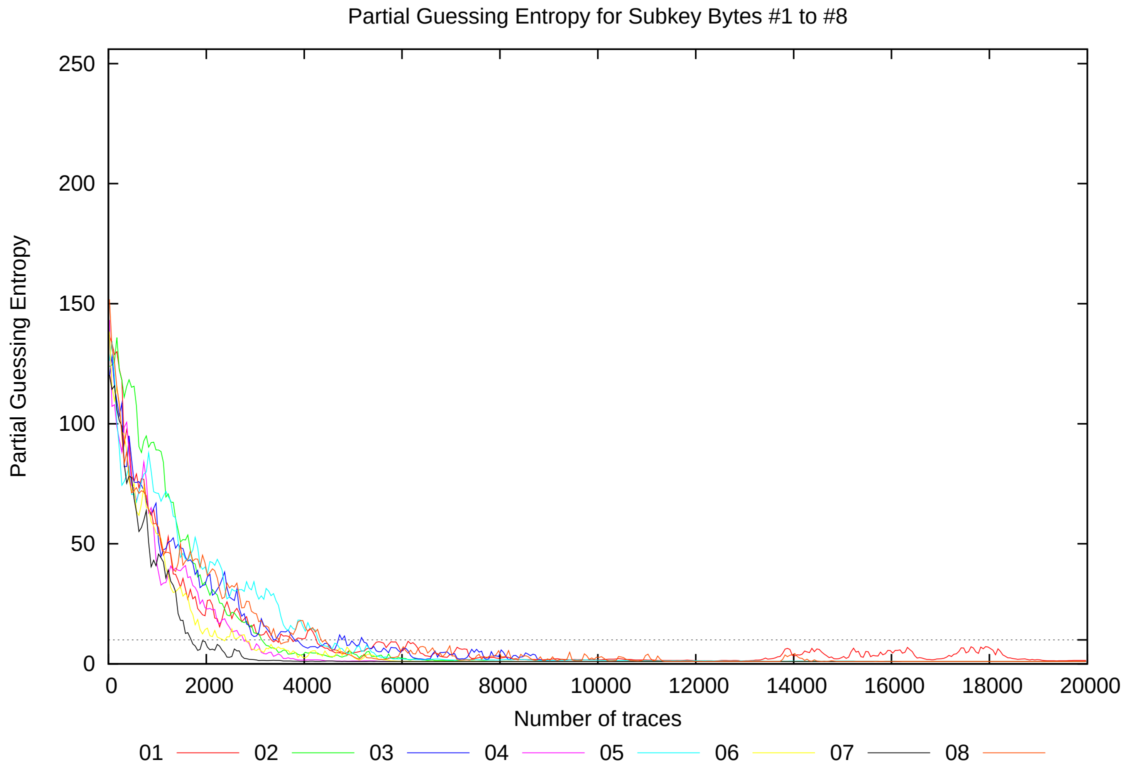


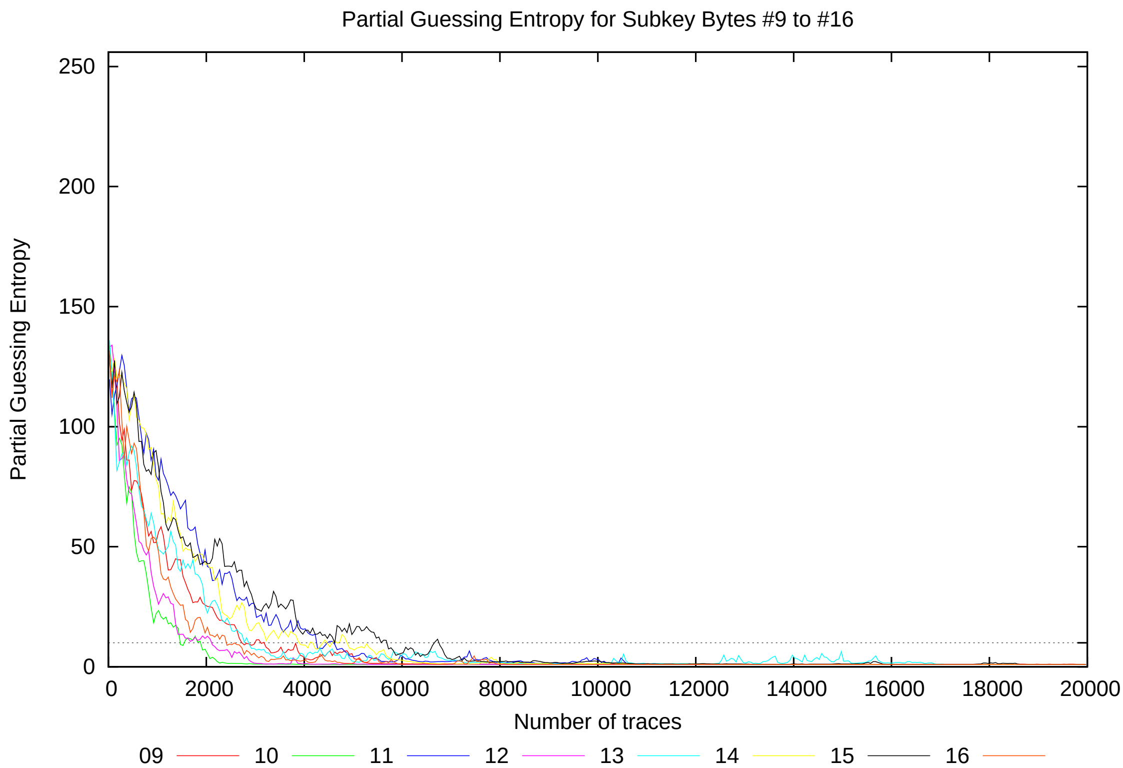
Partial Guessing Entropy for Subkey Byte #15

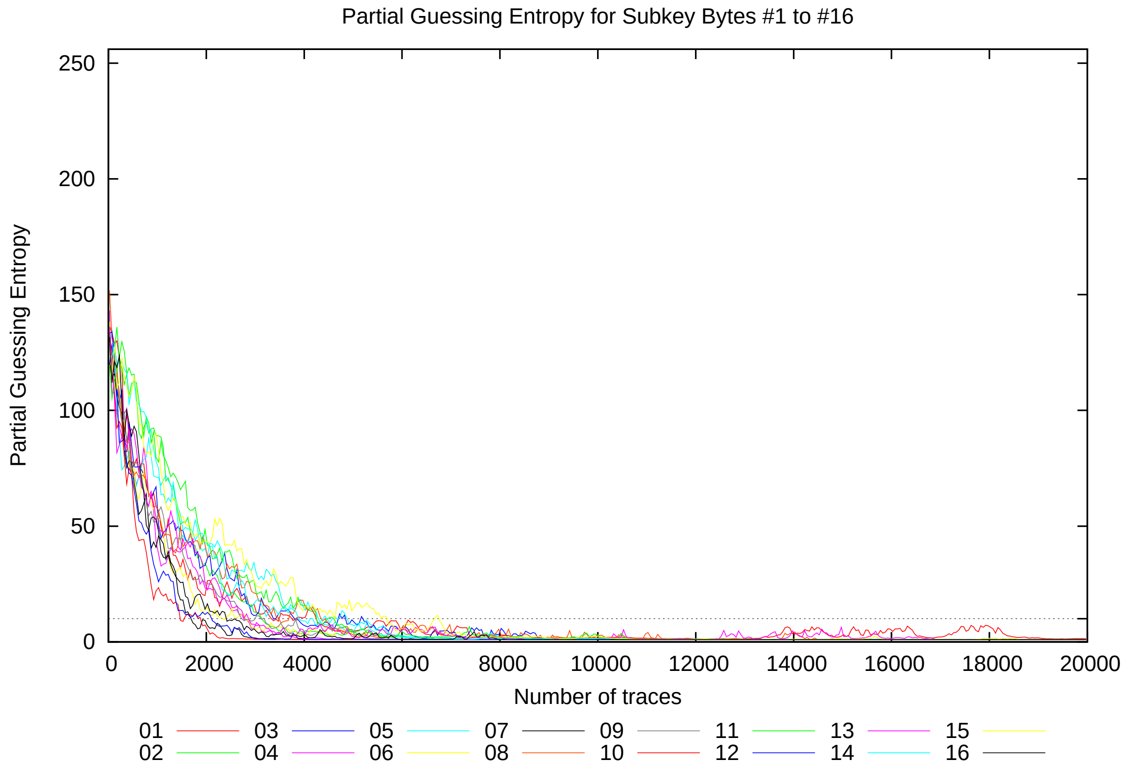


Partial Guessing Entropy for Subkey Byte #16




Partial Guessing Entropy for Subkey Bytes #1 to #8
Partial Guessing Entropy
250
200
150
100
50
0
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000
Number of traces
01
02
03
04
05
06
07
08


Partial Guessing Entropy for Subkey Bytes #9 to #16
Partial Guessing Entropy
250
200
150
100
50
0
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000
Number of traces
09
10
11
12
13
14
15
16


Partial Guessing Entropy for Subkey Bytes #1 to #16
Partial Guessing Entropy
250
200
150
100
50
0
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000
Number of traces
01
02
03
04
05
06
07
08
09
10
11
12
13
14
15
16

Traces	Partial Guessing Entropy / Byte																Min	Max	Mean
	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16			
10	137.2	120.6	120.3	146.6	125.6	141.3	117.8	150.6	133.2	135.3	115.2	133.2	134.7	125.8	134.6	133.3	115.2	150.6	131.6
20	137.2	120.6	120.3	146.6	125.6	141.3	117.8	150.6	133.2	135.3	115.2	133.2	134.7	125.8	134.6	133.3	115.2	150.6	131.6
30	131.8	117.9	122.6	142.4	129.8	137.4	119.1	151.2	132.1	134.1	111.0	131.6	134.6	122.5	133.1	131.4	111.0	151.2	130.2
40	142.8	134.3	119.6	136.9	126.4	129.3	124.0	160.6	126.5	130.8	117.8	129.0	147.4	115.8	127.8	128.8	115.8	160.6	131.1
50	144.4	126.2	114.7	133.1	125.7	139.2	111.9	152.3	120.4	130.8	149.2	139.4	120.0	128.4	116.2	118.7	111.9	152.3	129.4
100	125.2	115.0	123.8	109.1	121.2	100.3	115.6	120.2	136.4	128.9	100.4	121.0	120.0	142.7	126.9	114.0	100.3	142.7	120.0
200	125.5	131.0	113.0	91.4	89.6	117.3	101.0	109.2	107.4	96.1	117.1	94.5	76.9	119.1	97.9	117.2	76.9	131.0	106.5
300	95.1	127.7	95.9	93.1	73.2	101.6	95.5	85.3	98.3	98.1	125.6	81.4	92.4	113.1	114.3	89.9	73.2	127.7	98.8
400	104.8	120.7	88.5	87.7	82.8	97.9	78.4	90.4	86.1	78.3	109.5	67.3	83.0	106.1	114.0	101.3	67.3	120.7	93.5
500	72.4	110.0	77.0	73.5	69.0	75.3	73.9	72.0	73.4	67.1	102.1	71.0	96.9	120.8	107.8	87.2	67.1	120.8	84.3
1000	60.9	86.8	65.4	39.3	64.4	52.4	42.1	53.3	53.1	20.1	75.3	29.8	51.4	71.3	89.2	50.3	20.1	89.2	56.6
2000	20.9	32.9	32.2	20.5	39.0	17.1	8.9	36.1	24.6	8.0	42.7	9.2	22.6	43.1	45.1	16.0	8.0	45.1	26.2
3000	13.4	12.7	11.8	6.5	35.1	5.2	1.6	18.6	12.9	1.1	23.7	1.4	6.9	15.3	25.2	4.2	1.1	35.1	12.2
4000	11.0	4.5	6.6	1.6	14.0	3.3	1.0	18.8	3.8	1.0	18.2	1.3	3.2	8.5	14.0	2.7	1.0	18.8	7.1
5000	4.3	4.2	8.8	1.2	4.4	3.0	1.0	3.6	4.6	1.0	4.2	1.2	2.1	7.3	15.2	1.4	1.0	15.2	4.2
10000	1.7	1.0	1.0	1.0	1.5	1.0	1.0	2.7	1.2	1.0	4.6	1.0	1.3	1.5	2.1	1.0	1.0	4.6	1.5
15000	2.7	1.0	1.0	1.0	1.2	1.0	1.0	1.0	1.0	1.0	1.0	1.0	4.2	1.0	1.2	1.0	1.0	4.2	1.3
20000	1.4	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.1	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.4	1.0