

Evaluation results

DPA contest v2

August 2010

1 Introduction

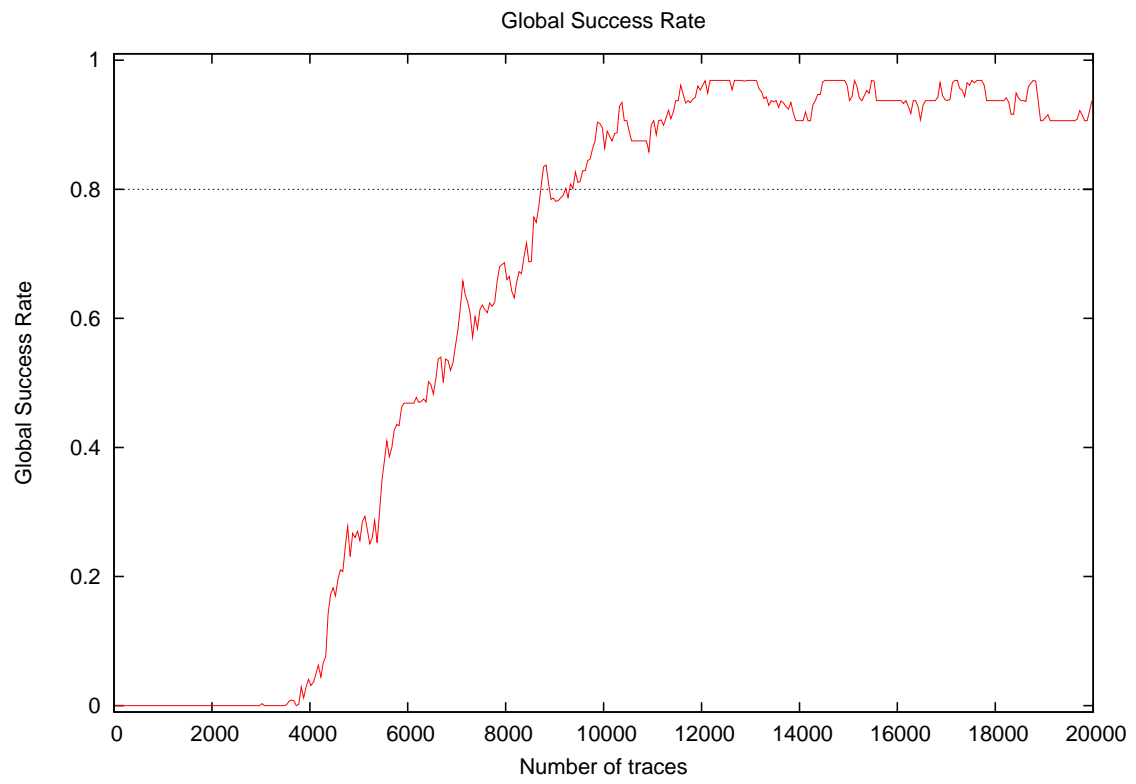
1.1 About the attack

- **Attack Name:** 9F
- **Sender/Team:** Matthieu Walle
- **Institution:** Thales Communications, France
- **Language:** C#
- **Attacked subkey:** 10

1.2 About the evaluation

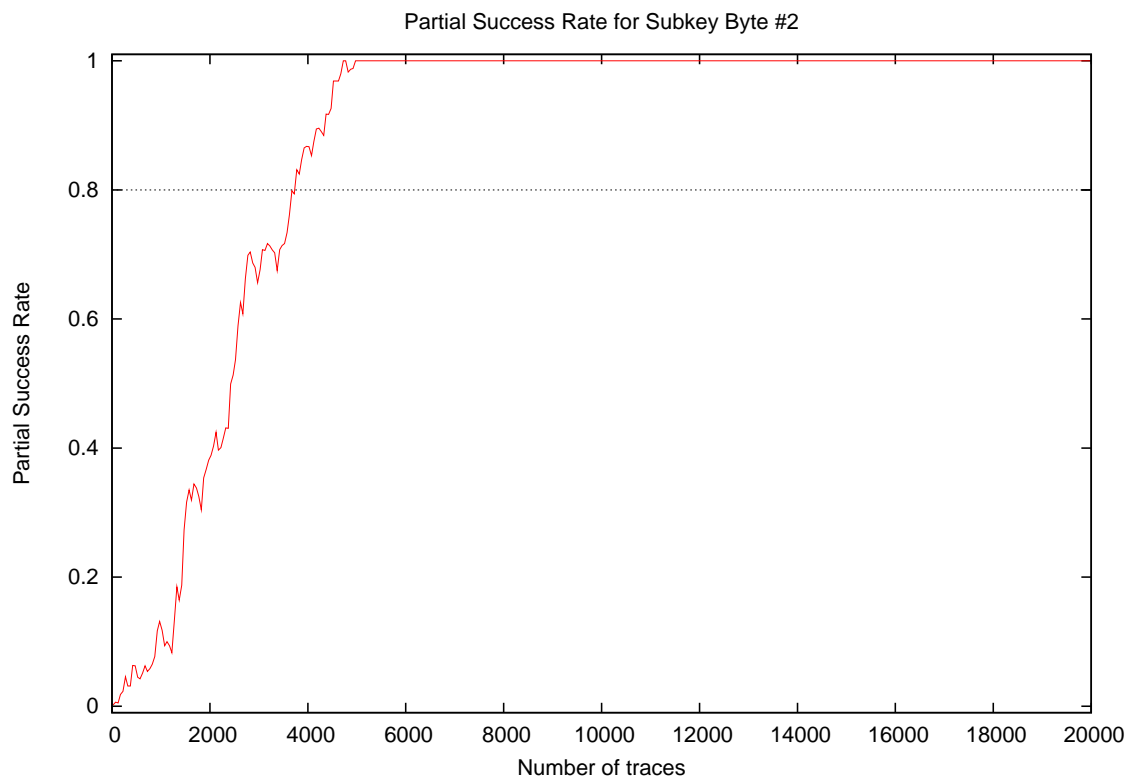
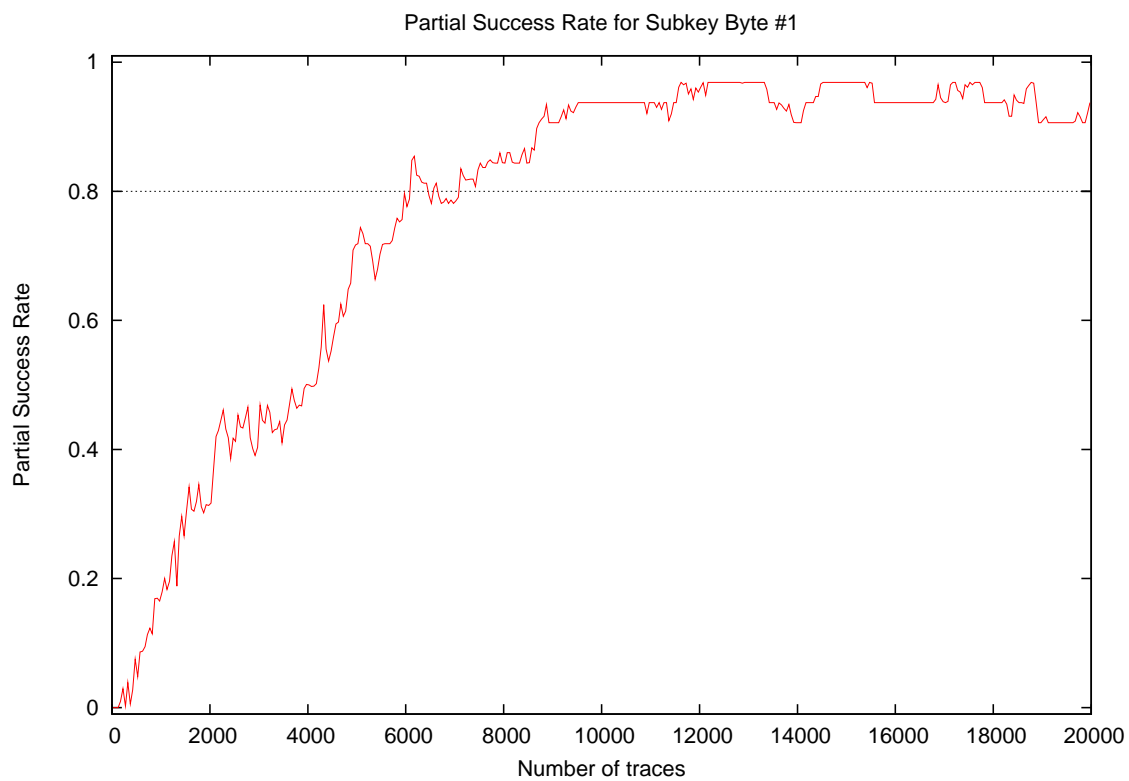
- **Date of evaluation:** August 2010

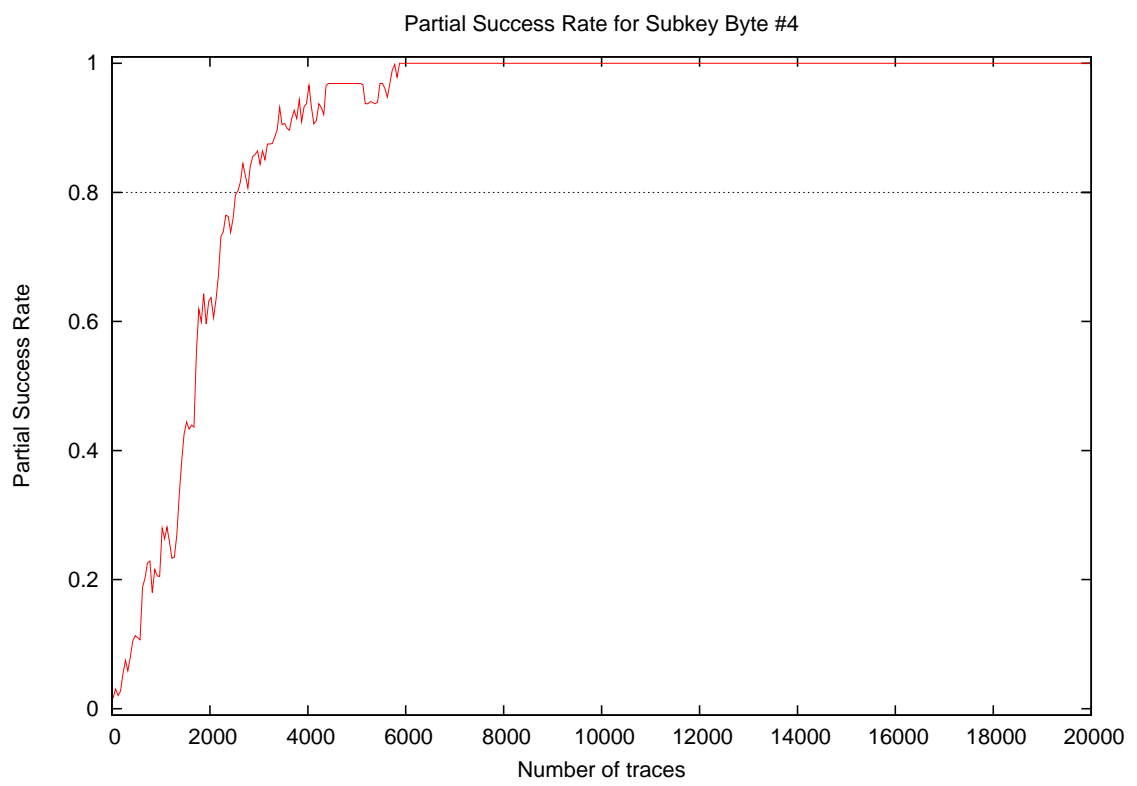
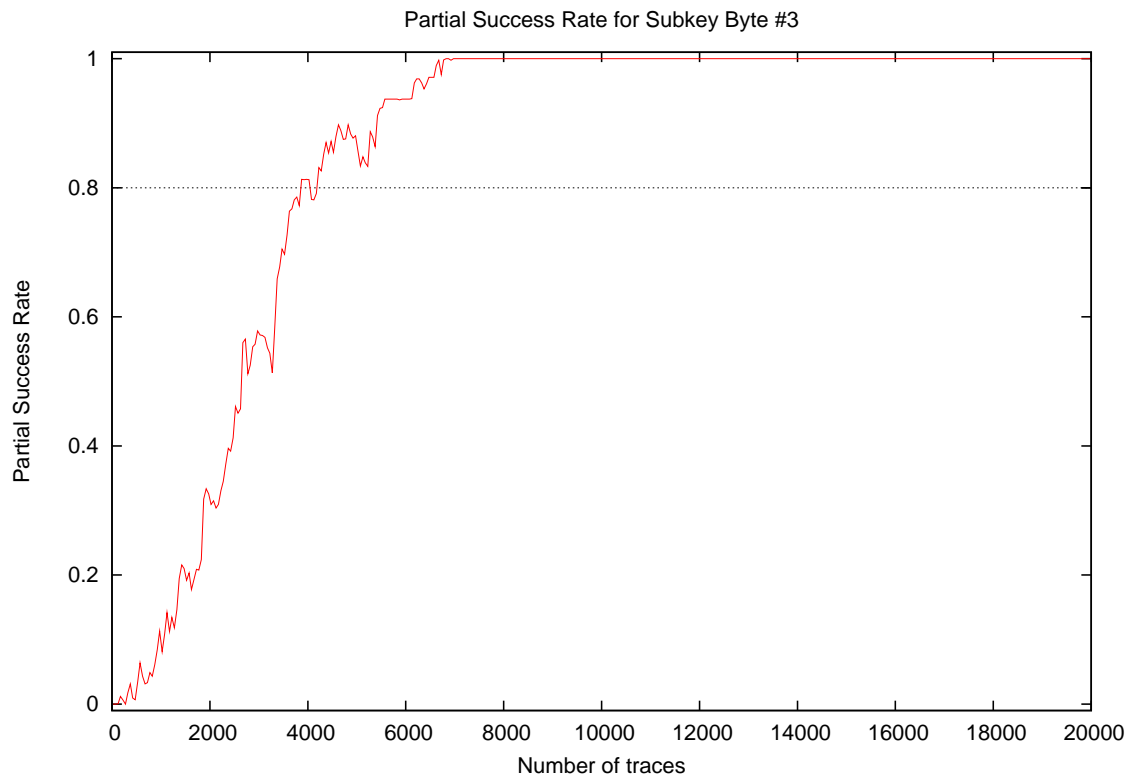
2 Global Success Rate

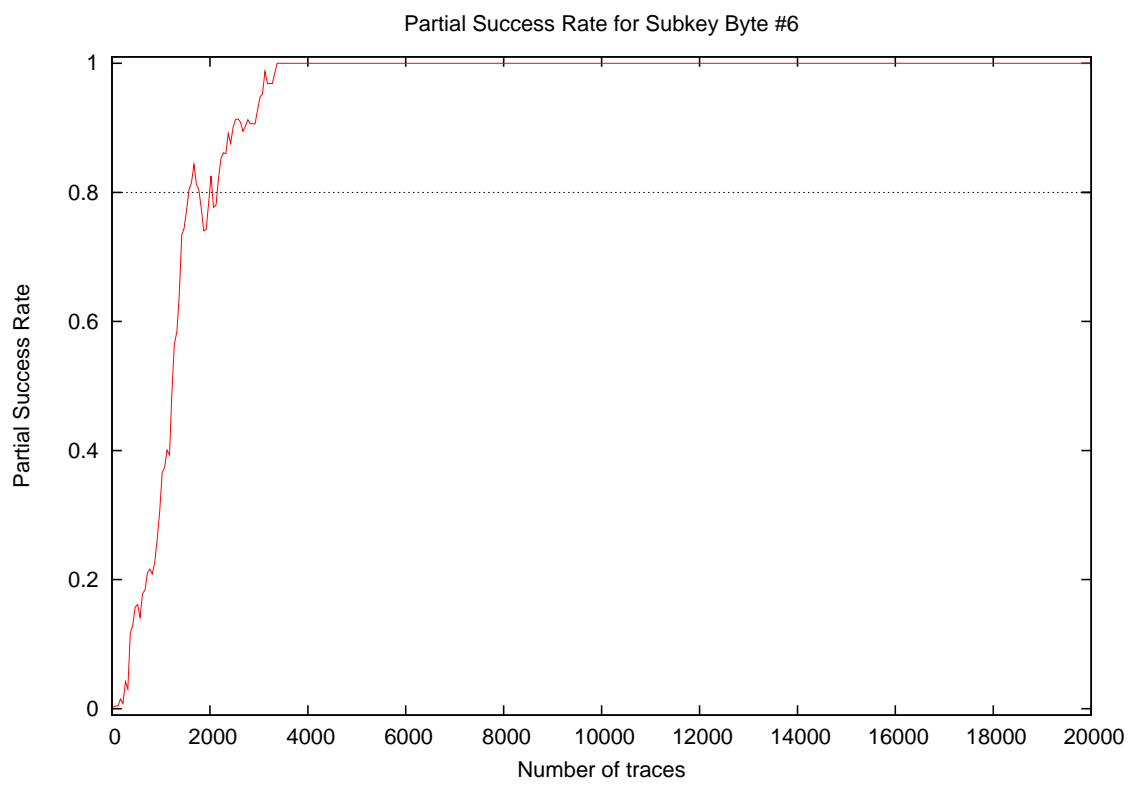
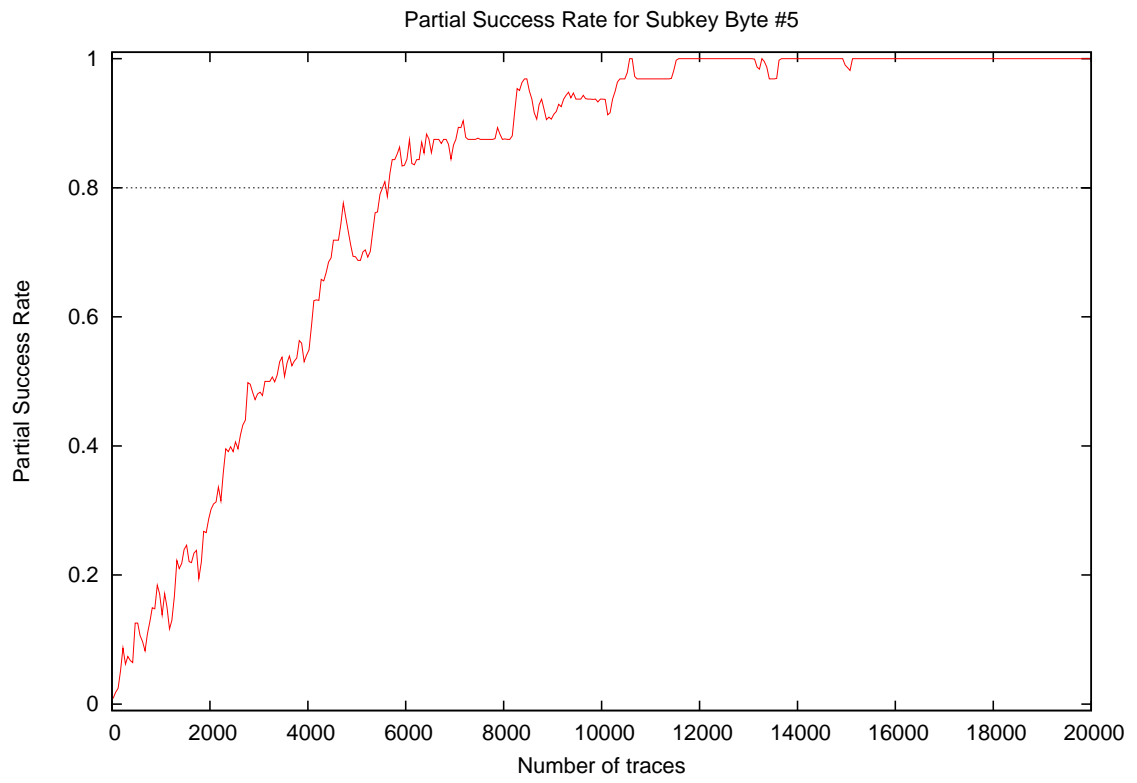


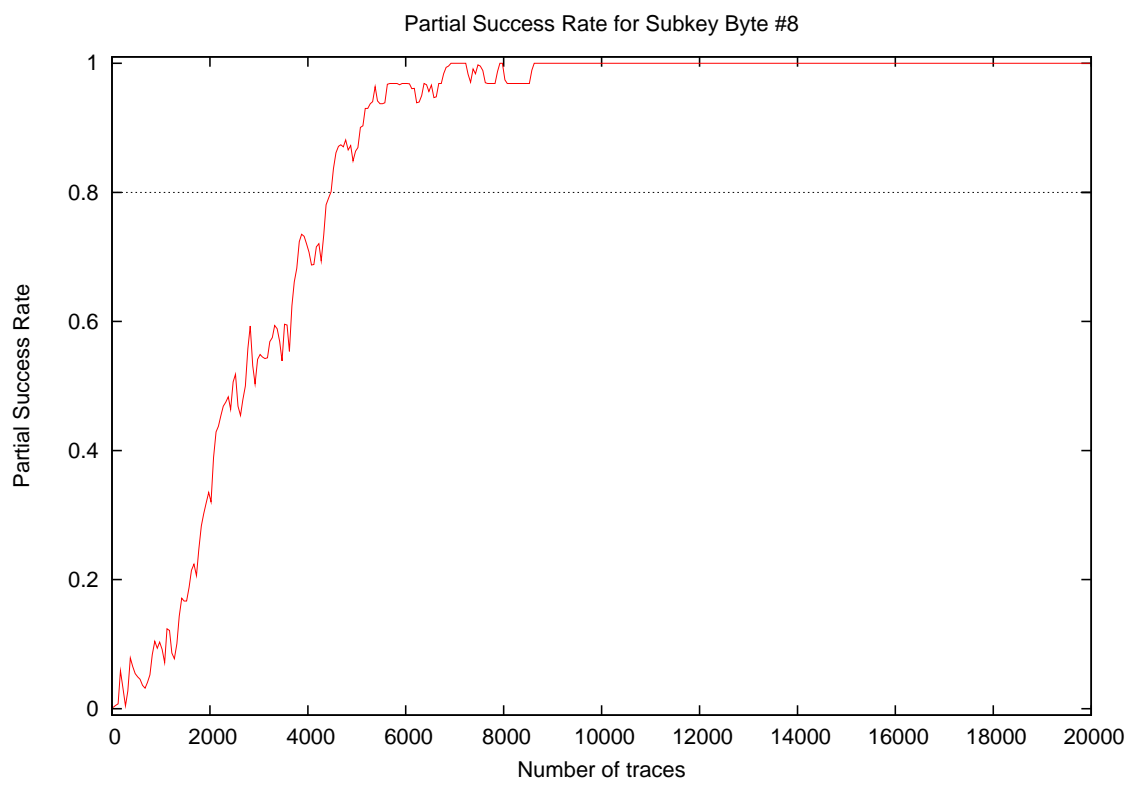
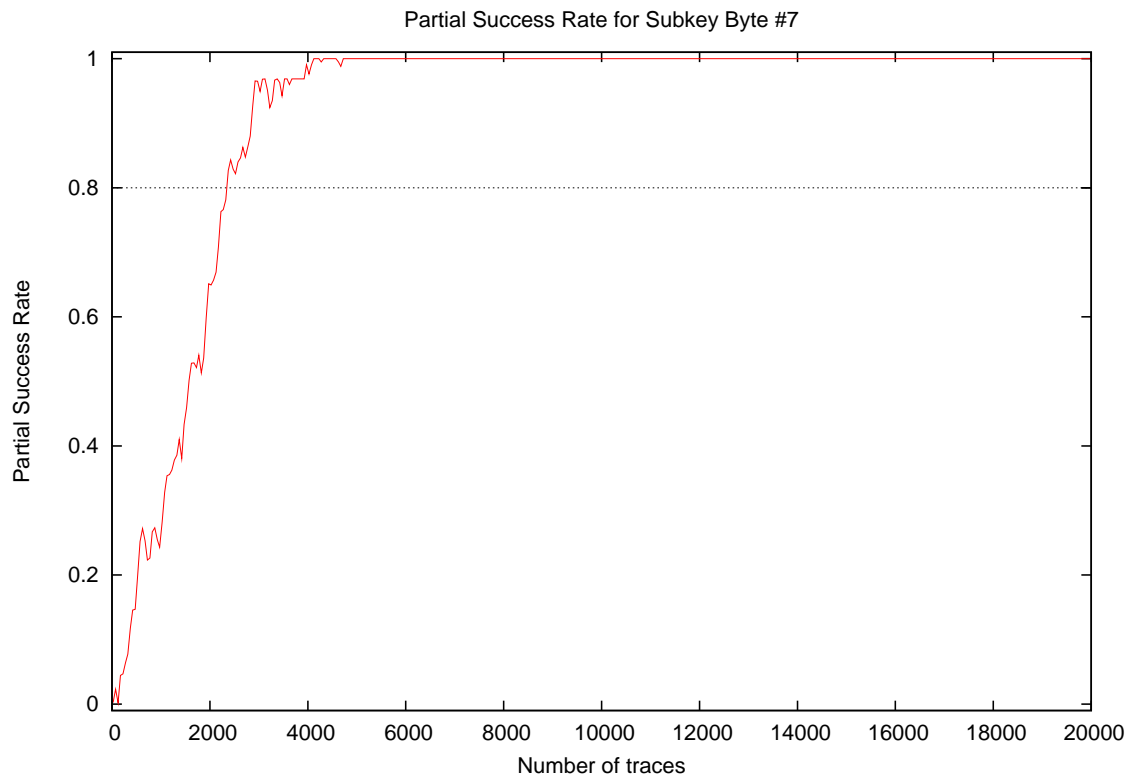
Number of traces	Global Success Rate
10	0.00
20	0.00
30	0.00
40	0.00
50	0.00
100	0.00
200	0.00
300	0.00
400	0.00
500	0.00
1000	0.00
2000	0.00
3000	0.00
4000	0.03
5000	0.25
10000	0.88
15000	0.94
20000	0.94

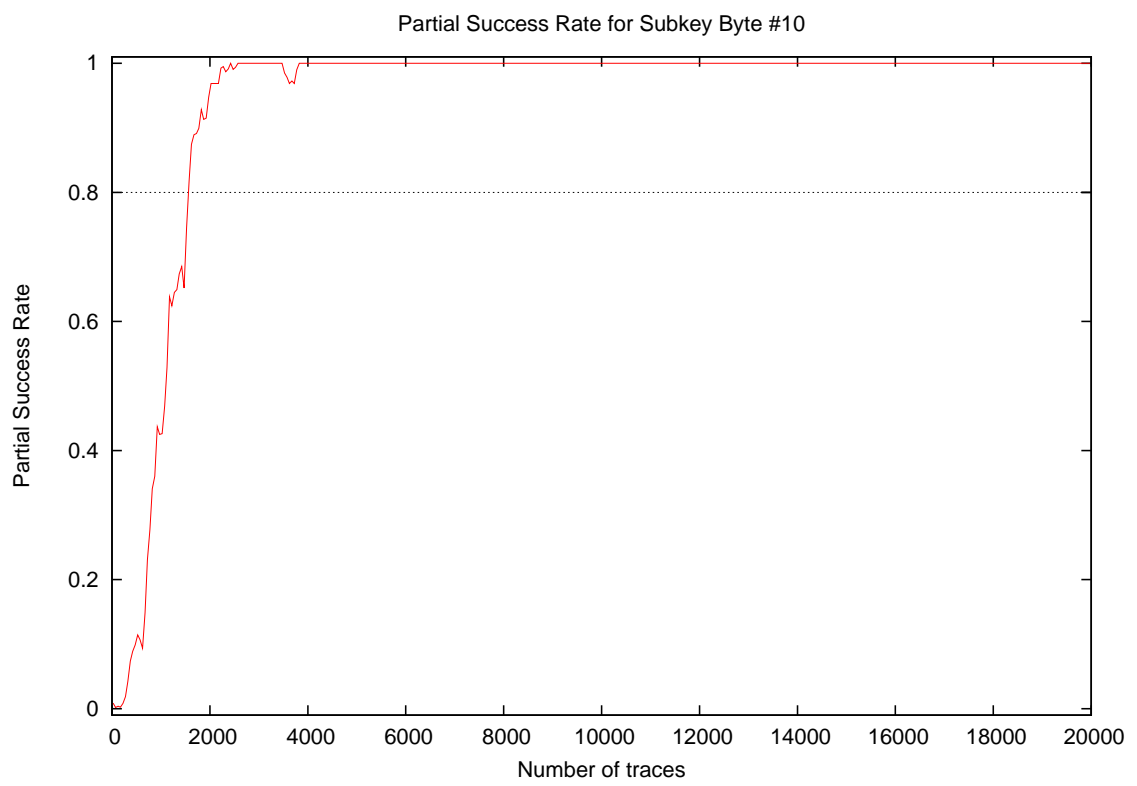
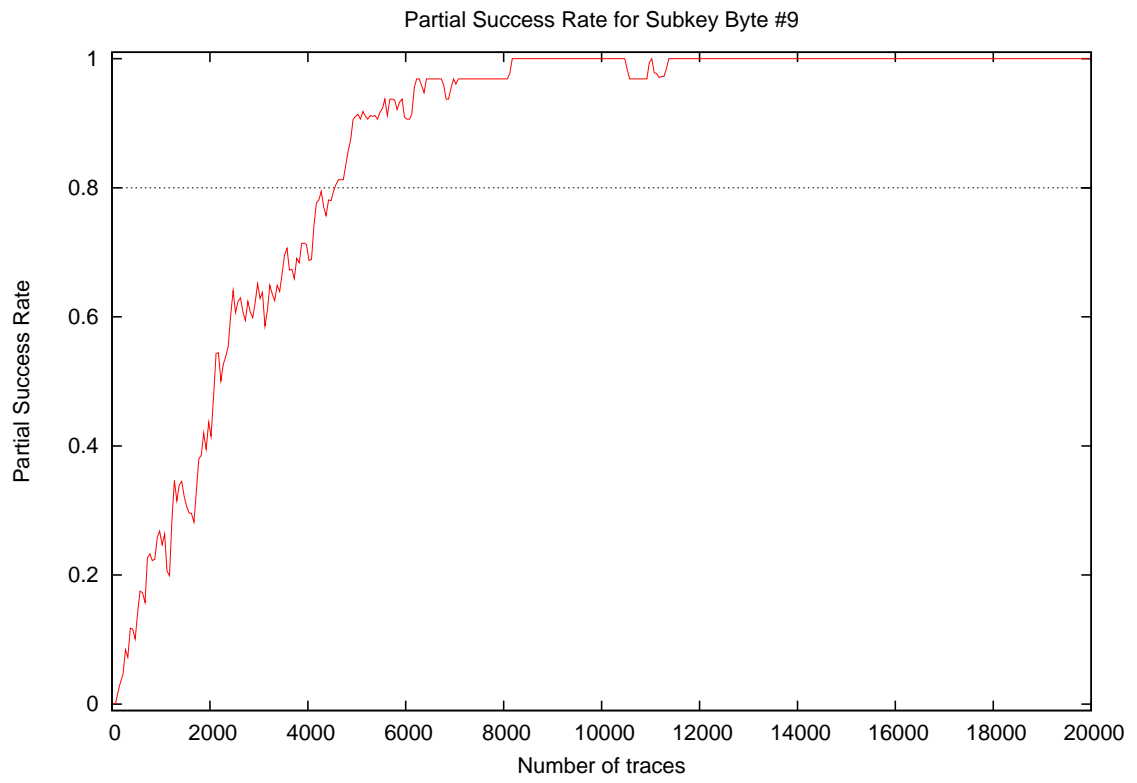
3 Partial Success Rate

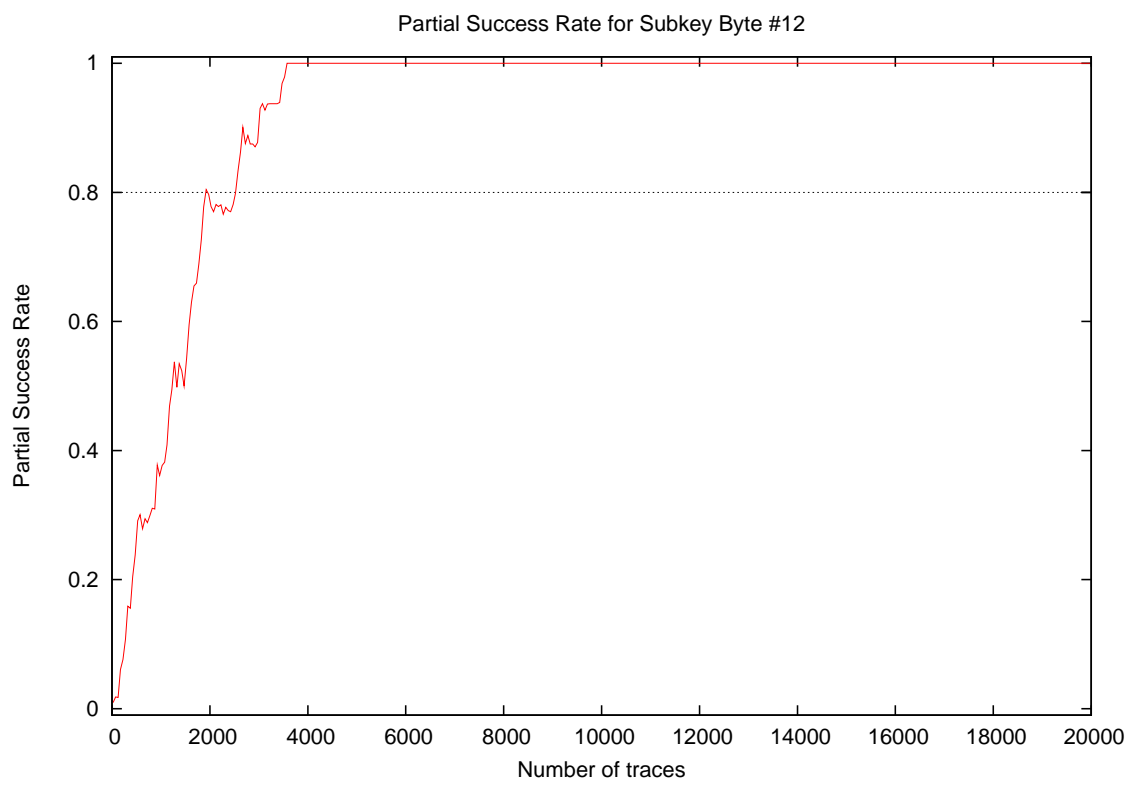
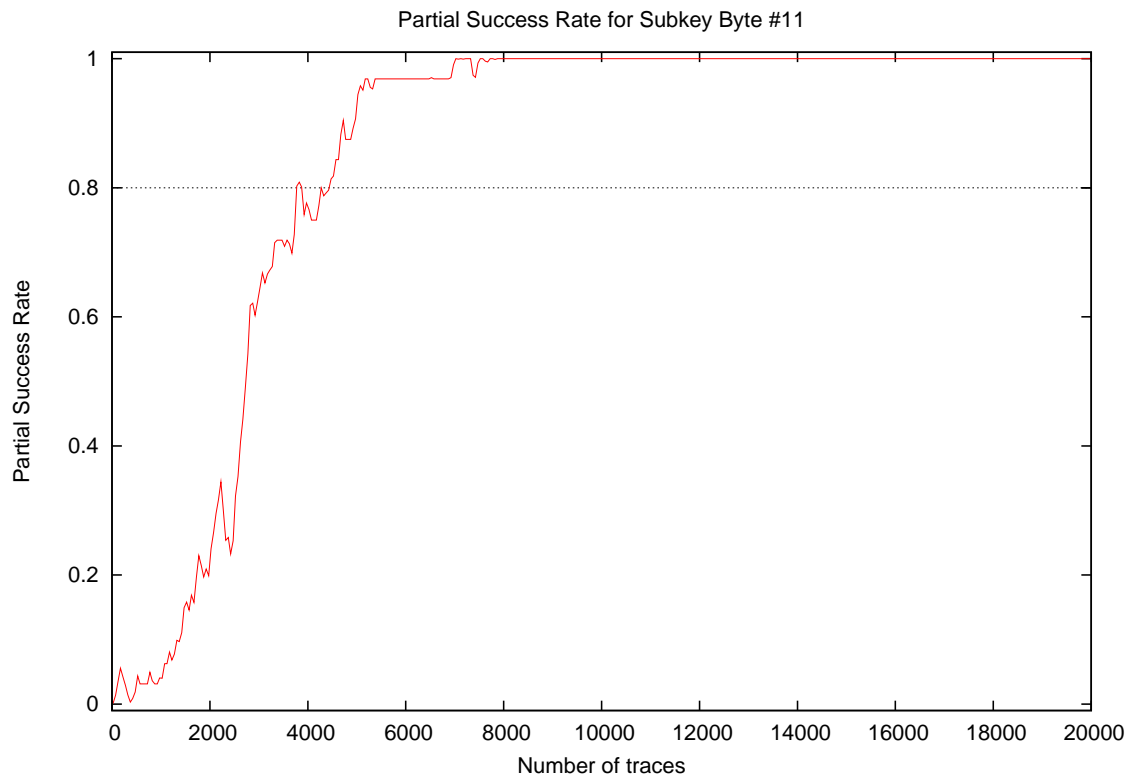


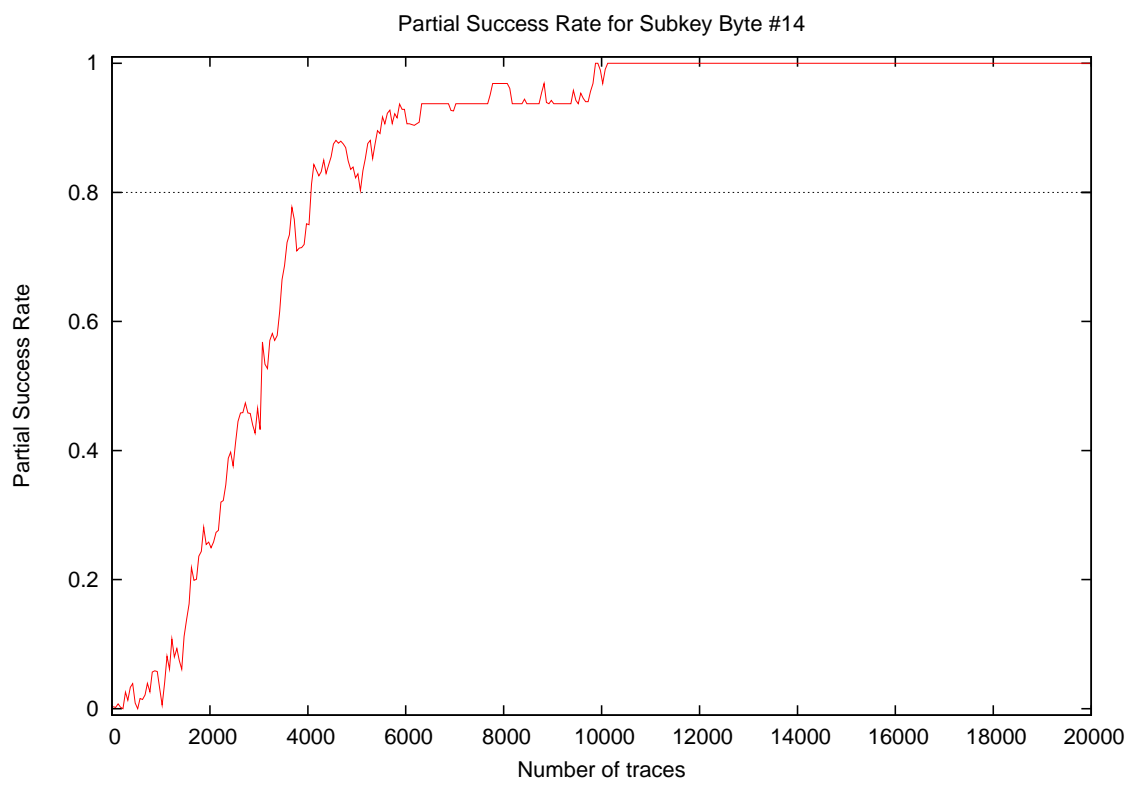
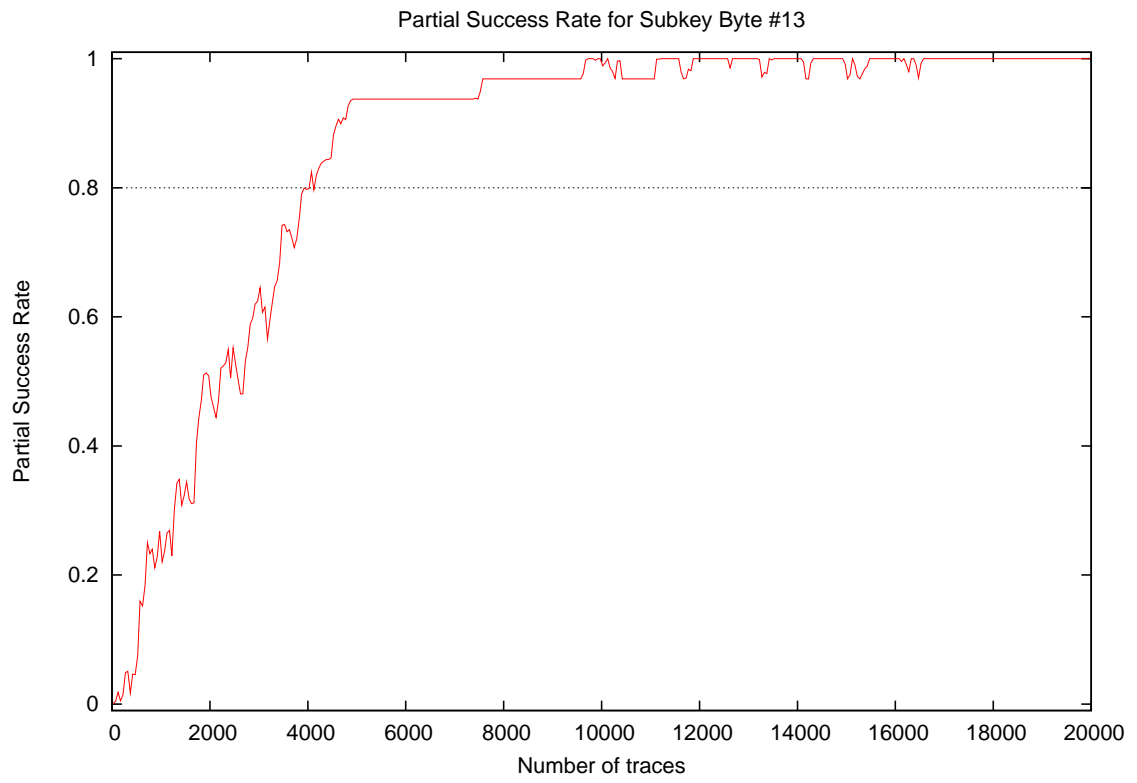


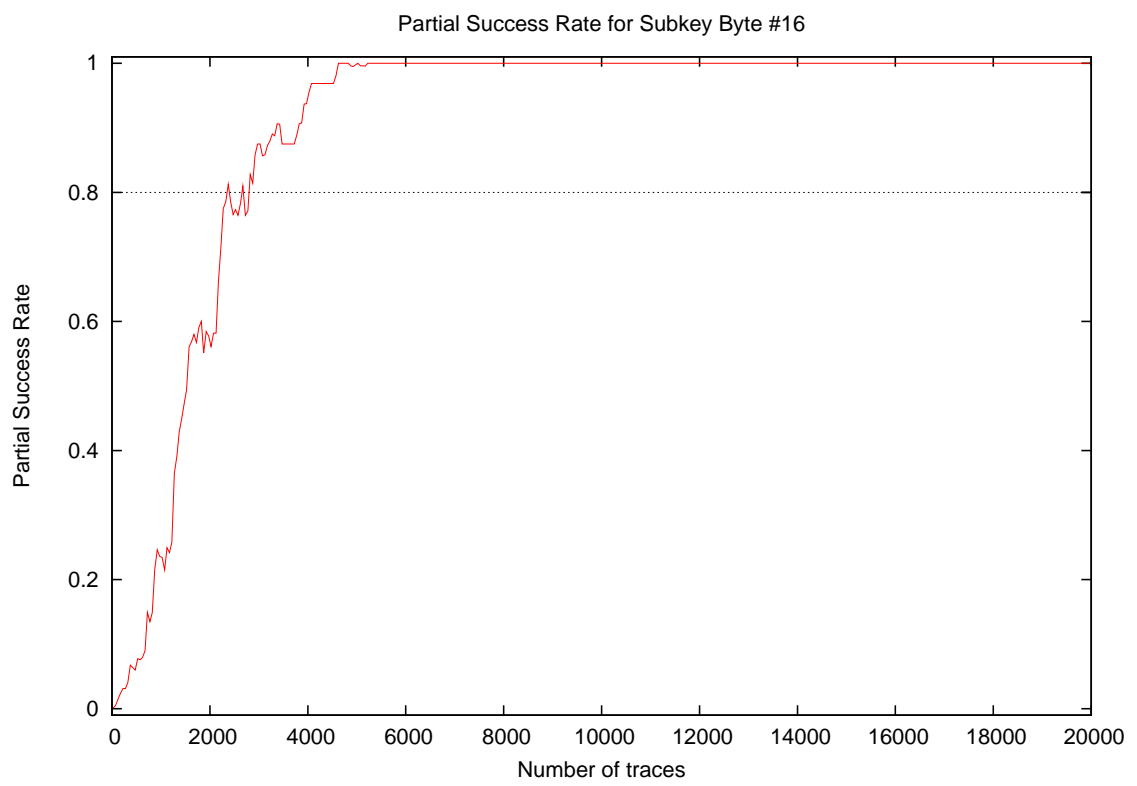
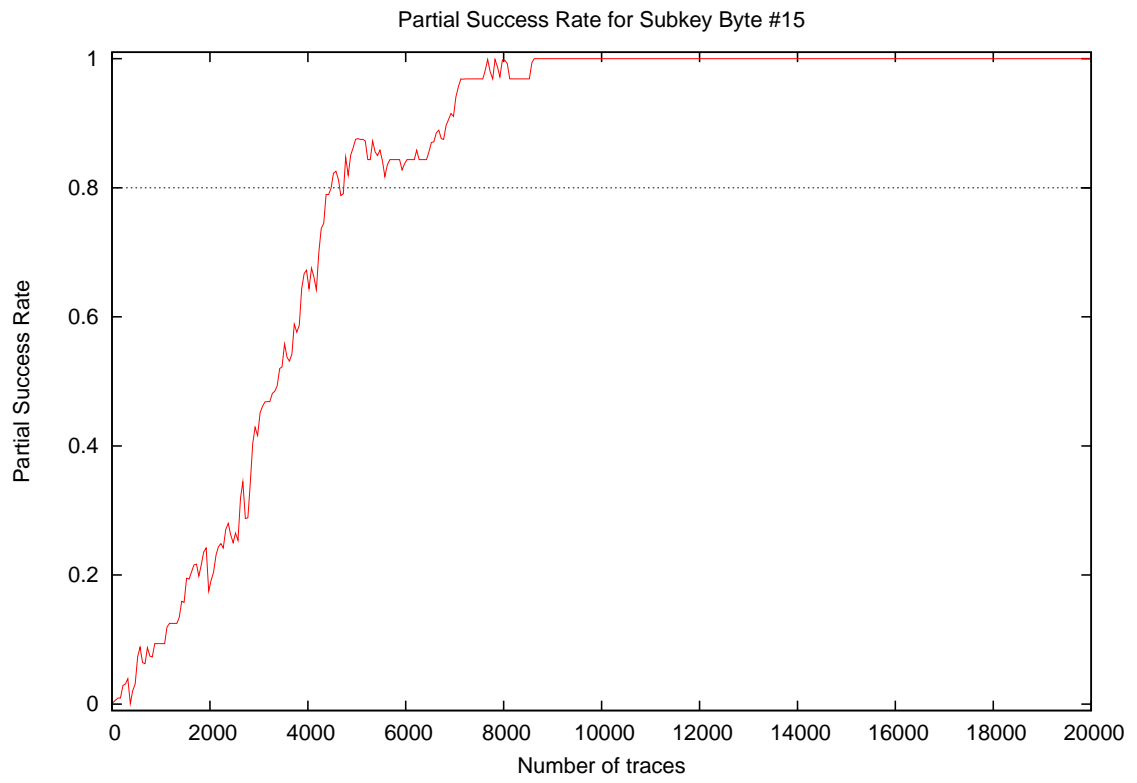


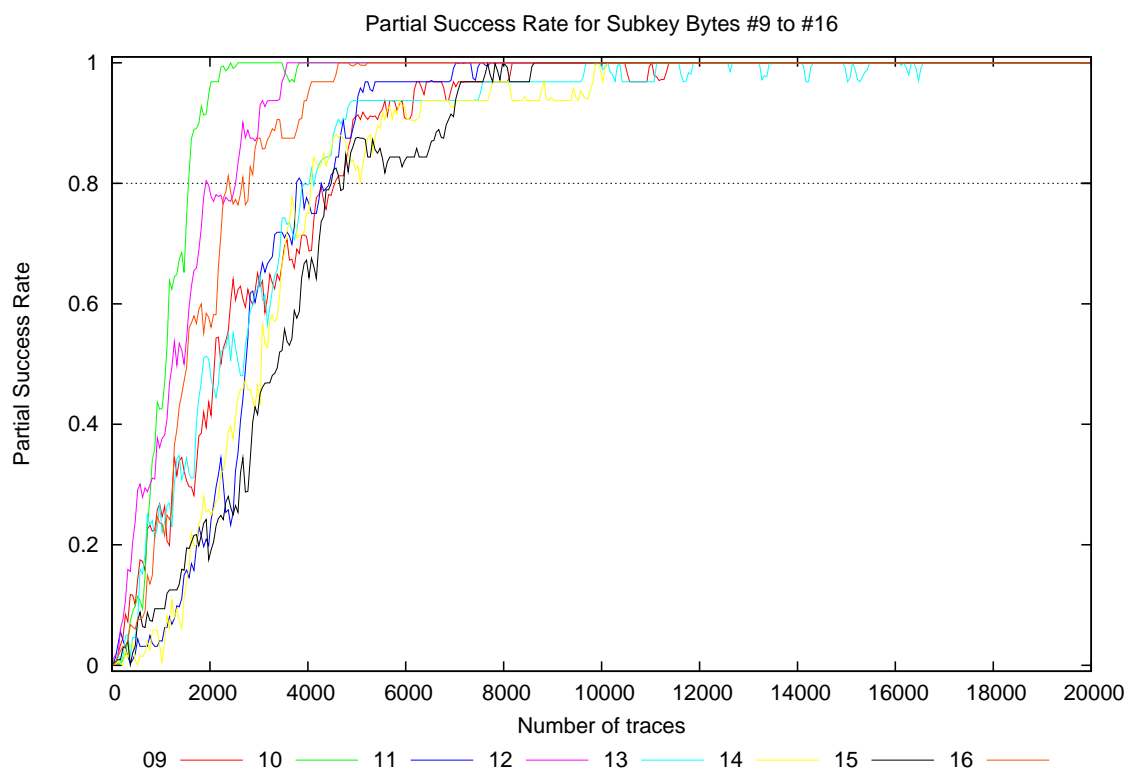
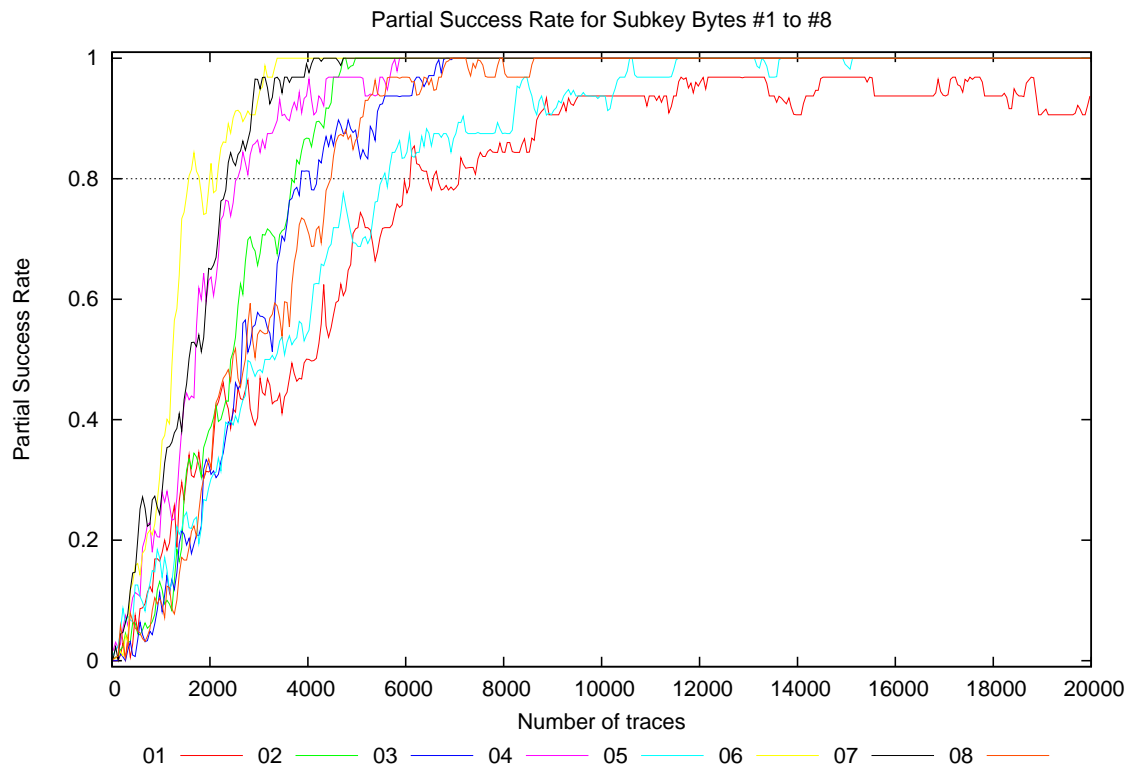




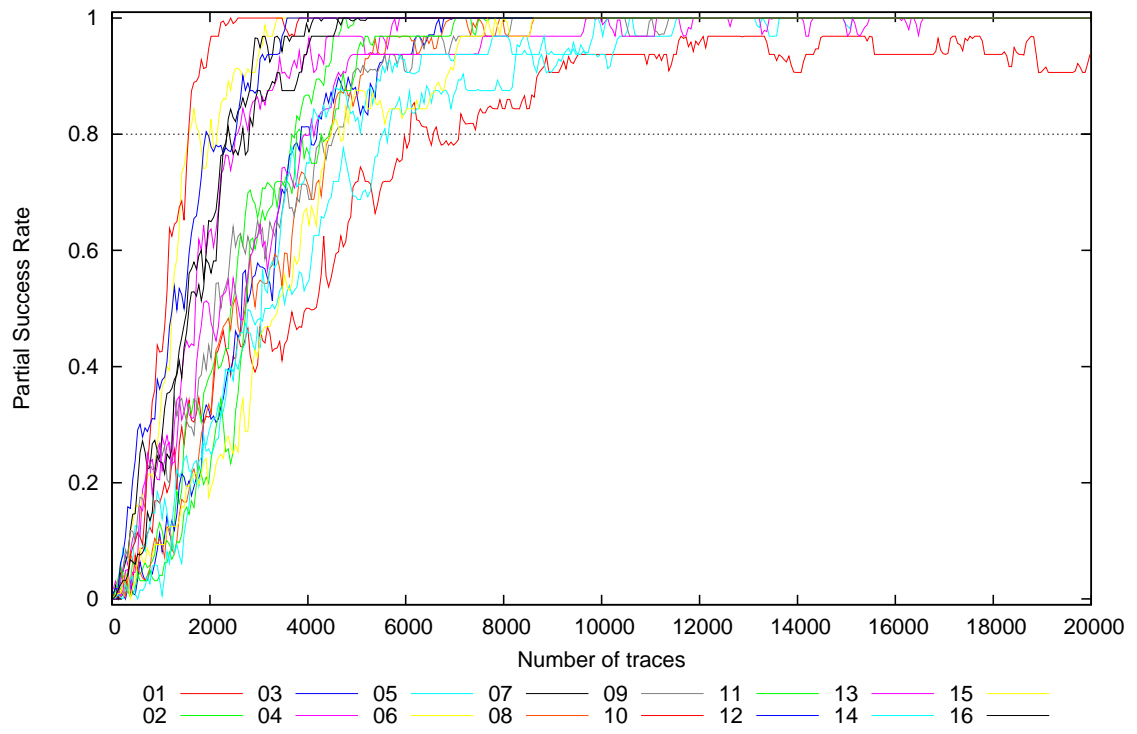






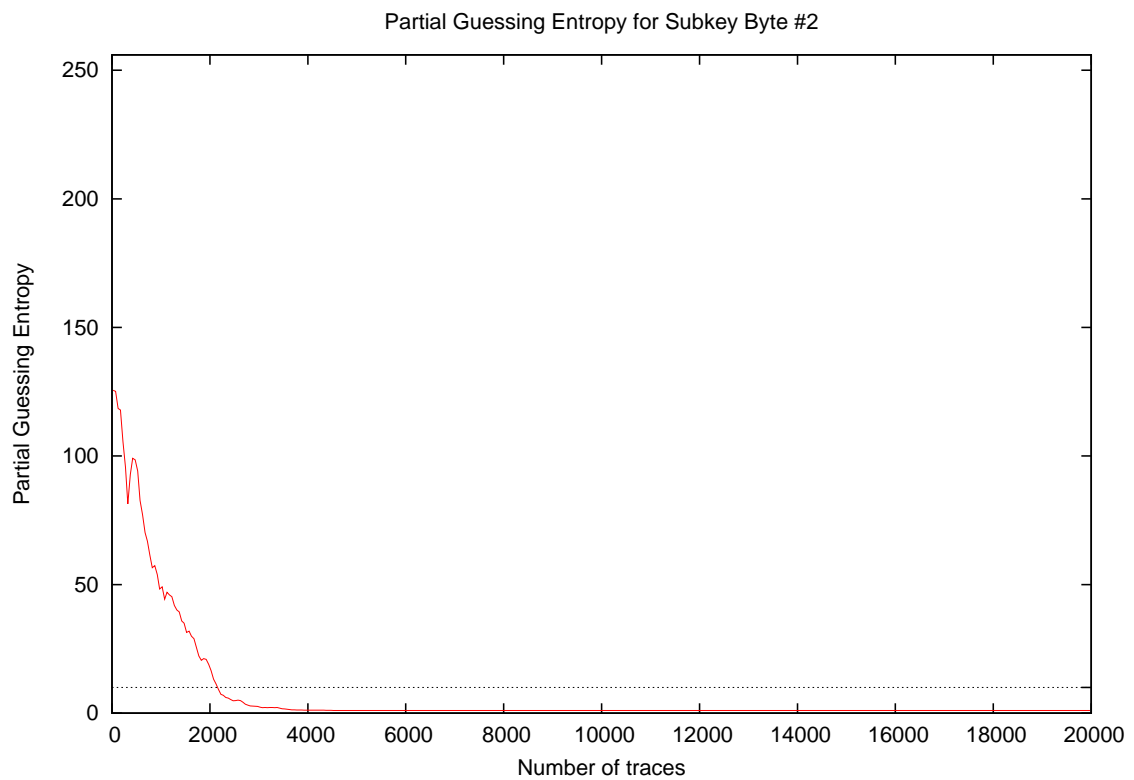
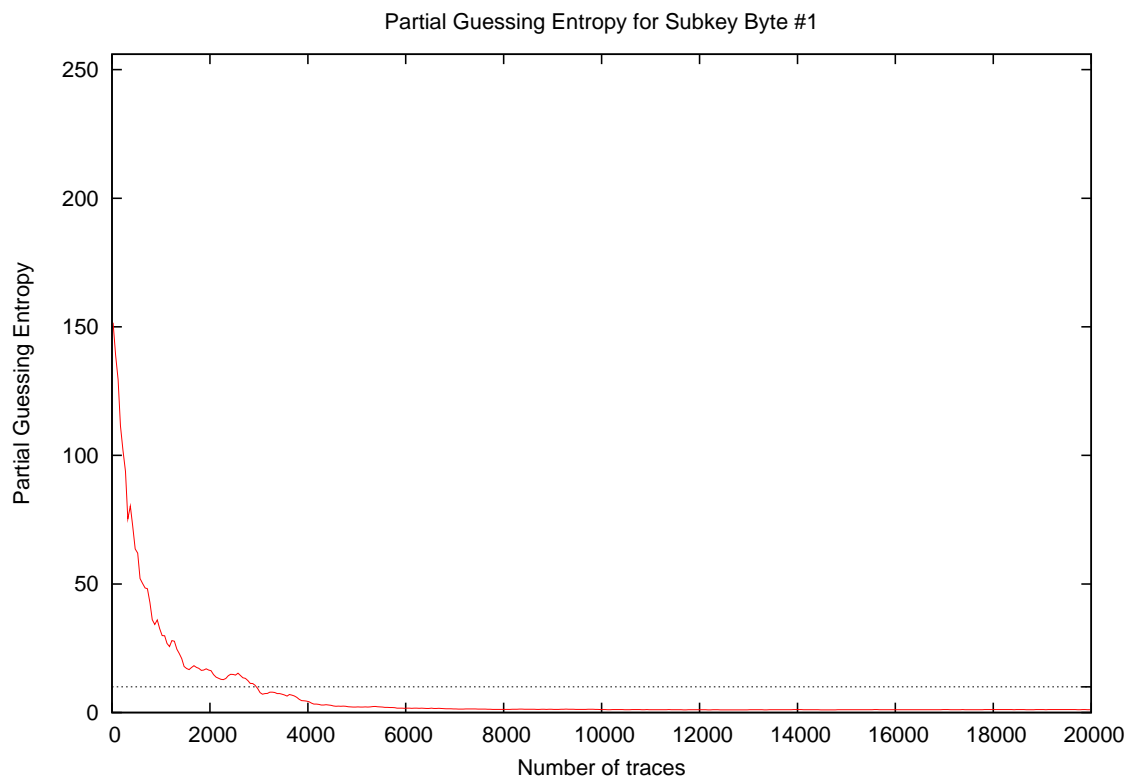


Partial Success Rate for Subkey Bytes #1 to #16

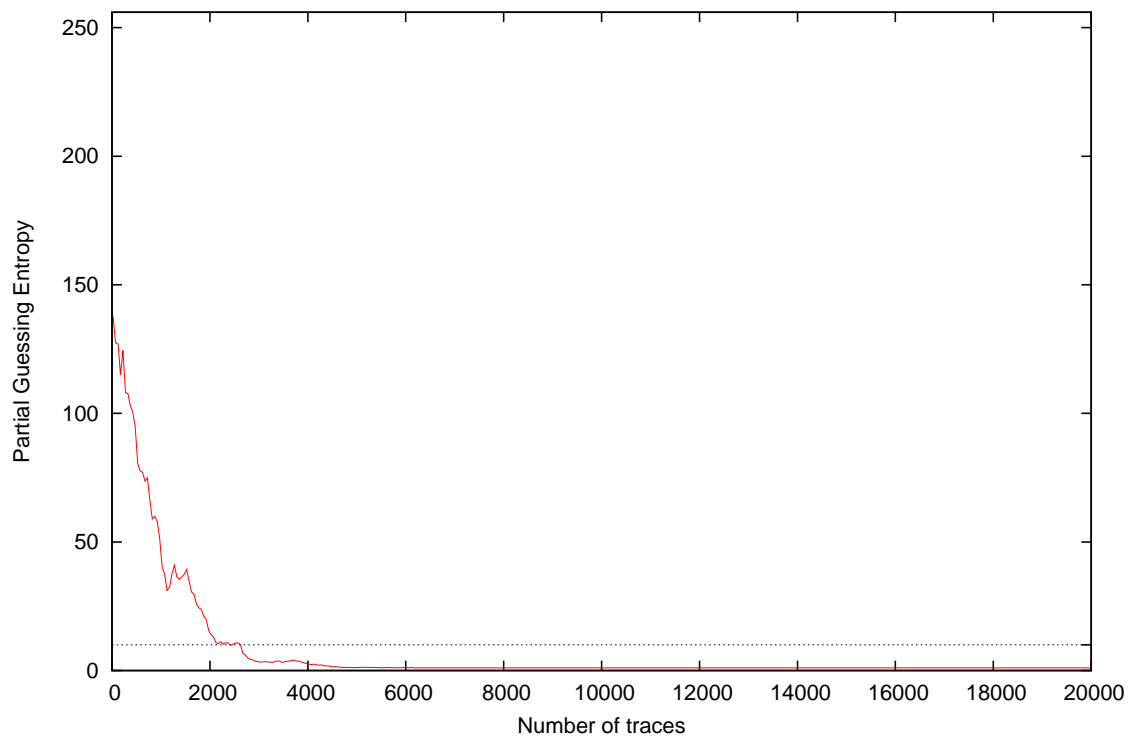


Traces	Partial Success Rate / Byte																Min	Max	Mean			
	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16						
10	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.03	0.00	0.00	0.00	0.00	0.00	0.00	0.03	0.00	0.00	0.03	0.00	0.00	0.03	0.00
20	0.00	0.00	0.00	0.03	0.03	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.03	0.00
30	0.00	0.00	0.00	0.03	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	0.00	0.00	0.00	0.03	0.00
40	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	0.00	0.00	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	0.00	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
100	0.00	0.00	0.00	0.00	0.00	0.00	0.03	0.00	0.00	0.00	0.00	0.03	0.03	0.00	0.00	0.00	0.03	0.00	0.00	0.00	0.03	0.01
200	0.03	0.03	0.00	0.03	0.06	0.03	0.03	0.06	0.06	0.03	0.06	0.09	0.00	0.00	0.03	0.03	0.00	0.09	0.00	0.00	0.09	0.04
300	0.00	0.03	0.00	0.09	0.06	0.03	0.03	0.00	0.06	0.06	0.00	0.16	0.06	0.03	0.03	0.03	0.16	0.06	0.00	0.16	0.16	0.04
400	0.00	0.03	0.03	0.09	0.06	0.16	0.12	0.06	0.16	0.09	0.00	0.16	0.03	0.06	0.06	0.03	0.16	0.03	0.00	0.16	0.16	0.07
500	0.09	0.06	0.00	0.12	0.09	0.16	0.19	0.03	0.09	0.09	0.03	0.28	0.03	0.00	0.06	0.09	0.28	0.03	0.00	0.28	0.28	0.09
1000	0.16	0.12	0.09	0.22	0.19	0.34	0.28	0.12	0.25	0.47	0.03	0.34	0.19	0.00	0.09	0.25	0.34	0.19	0.00	0.47	0.47	0.20
2000	0.28	0.38	0.31	0.66	0.31	0.81	0.66	0.31	0.44	0.97	0.19	0.78	0.50	0.22	0.19	0.59	0.78	0.50	0.19	0.97	0.97	0.47
3000	0.47	0.66	0.59	0.84	0.50	0.94	0.97	0.56	0.66	1.00	0.66	0.91	0.62	0.47	0.44	0.88	0.91	0.62	0.44	1.00	1.00	0.70
4000	0.50	0.84	0.81	0.94	0.56	1.00	1.00	0.72	0.69	1.00	0.78	1.00	0.78	0.75	0.66	0.94	1.00	0.78	0.50	1.00	1.00	0.81
5000	0.72	1.00	0.88	0.97	0.69	1.00	1.00	0.88	0.94	1.00	0.97	1.00	0.94	0.81	0.88	1.00	1.00	0.94	0.69	1.00	1.00	0.92
10000	0.94	1.00	1.00	1.00	0.94	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	0.97	1.00	1.00	1.00	1.00	0.94	1.00	1.00	0.99
15000	0.97	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	0.97	1.00	1.00	1.00	1.00	0.97	0.97	1.00	1.00	1.00
20000	0.94	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	0.94	1.00	1.00	1.00

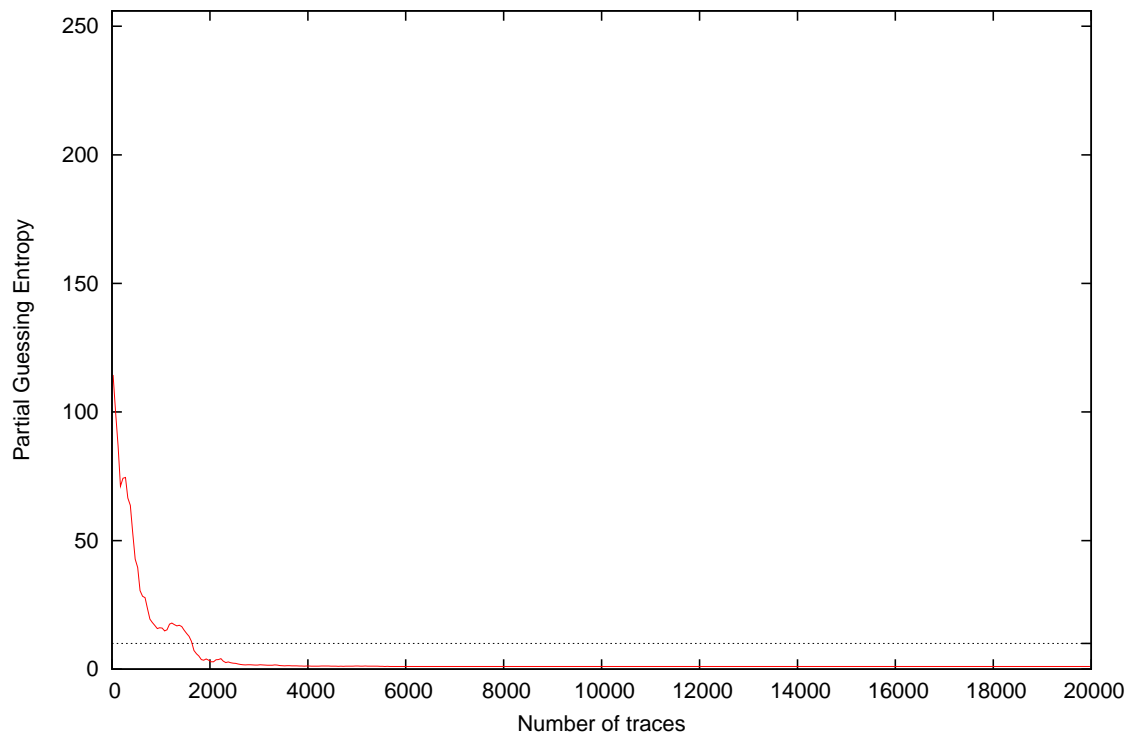
4 Partial Guessing Entropy



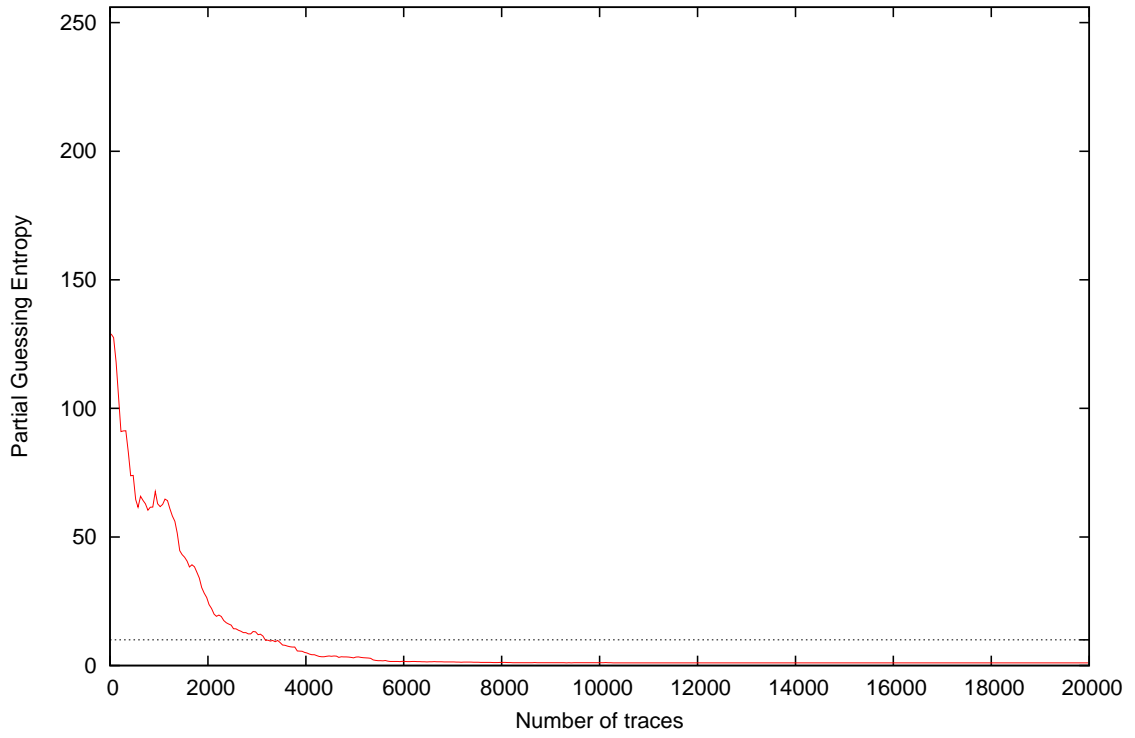
Partial Guessing Entropy for Subkey Byte #3



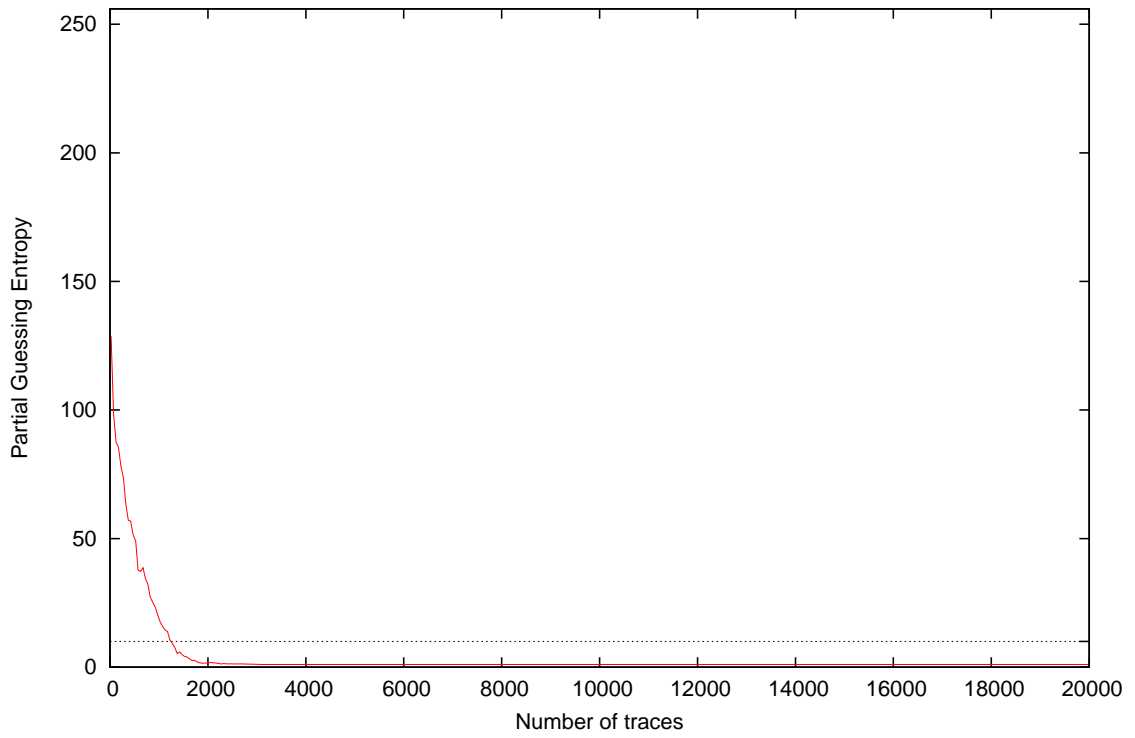
Partial Guessing Entropy for Subkey Byte #4



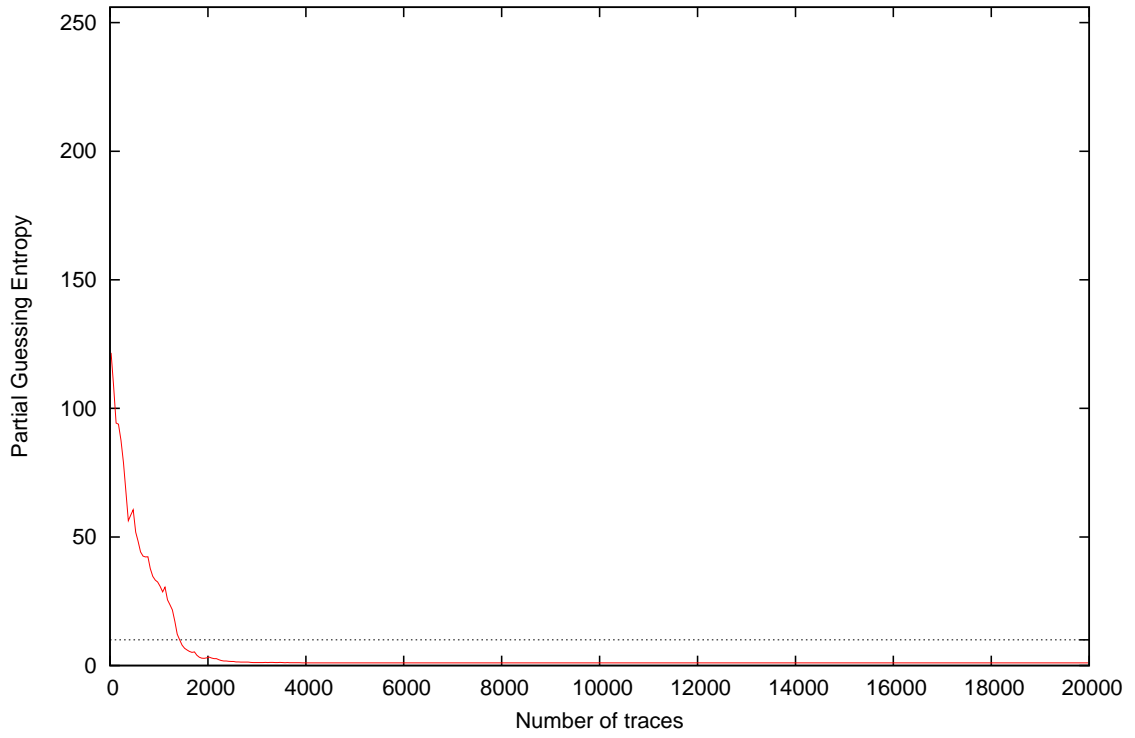
Partial Guessing Entropy for Subkey Byte #5



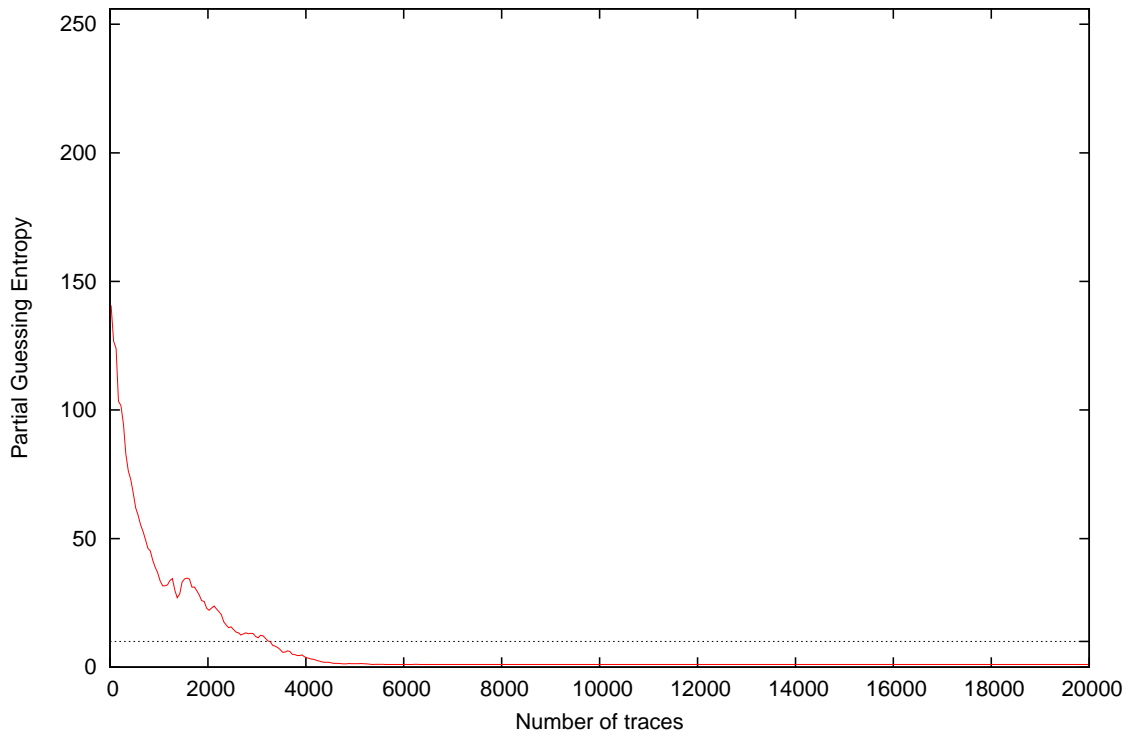
Partial Guessing Entropy for Subkey Byte #6



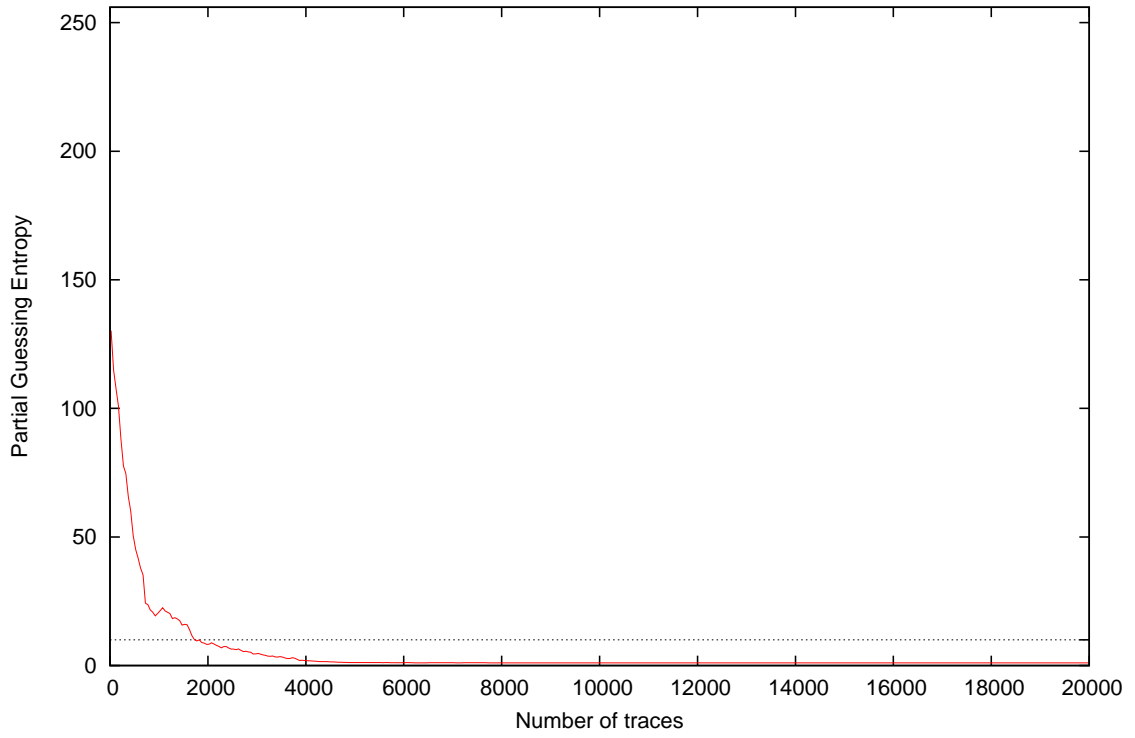
Partial Guessing Entropy for Subkey Byte #7



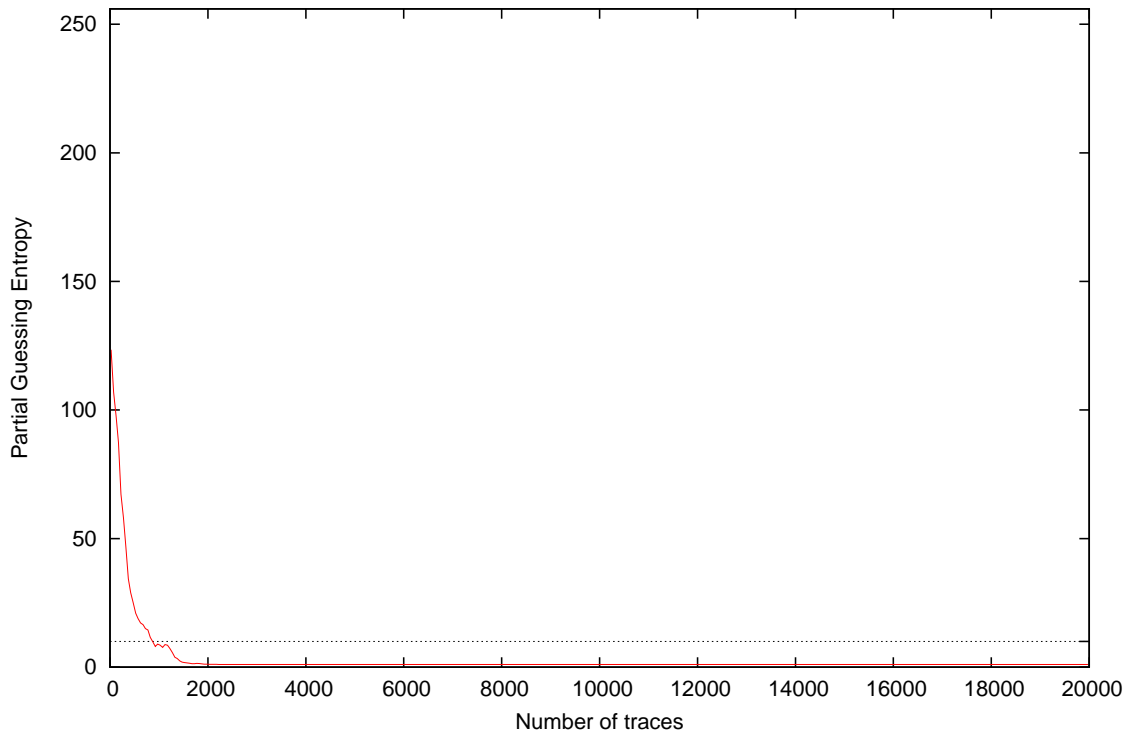
Partial Guessing Entropy for Subkey Byte #8

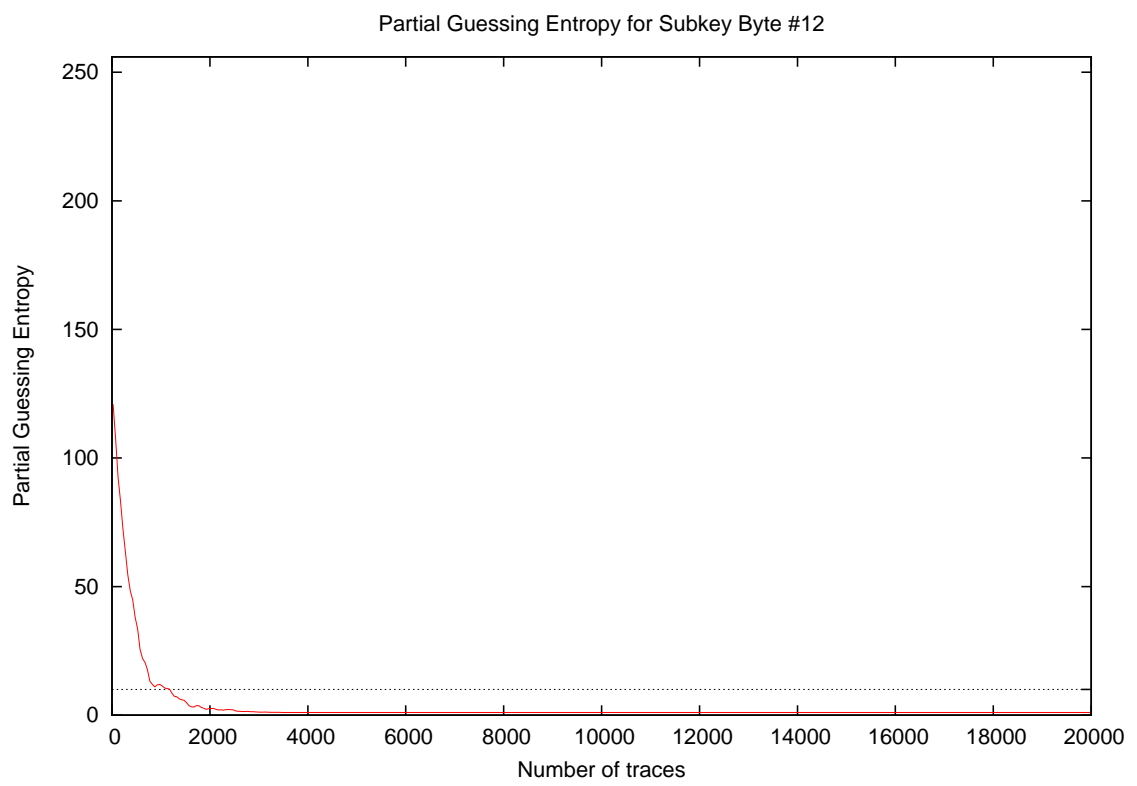
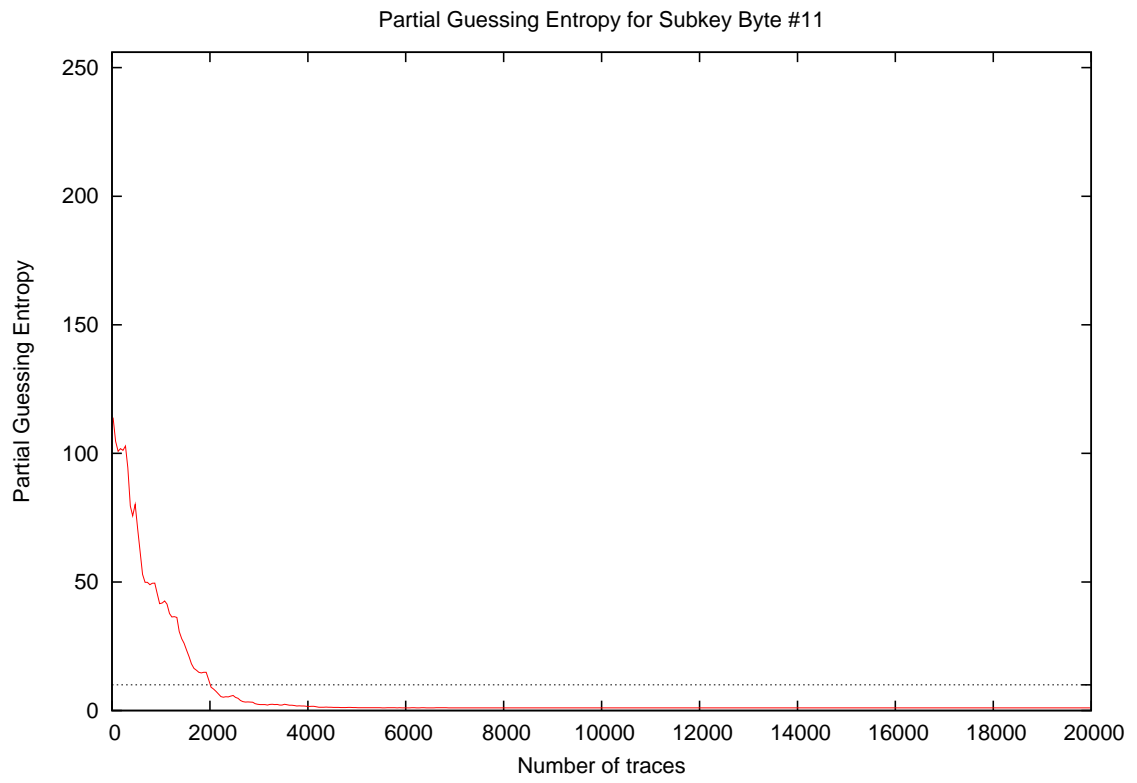


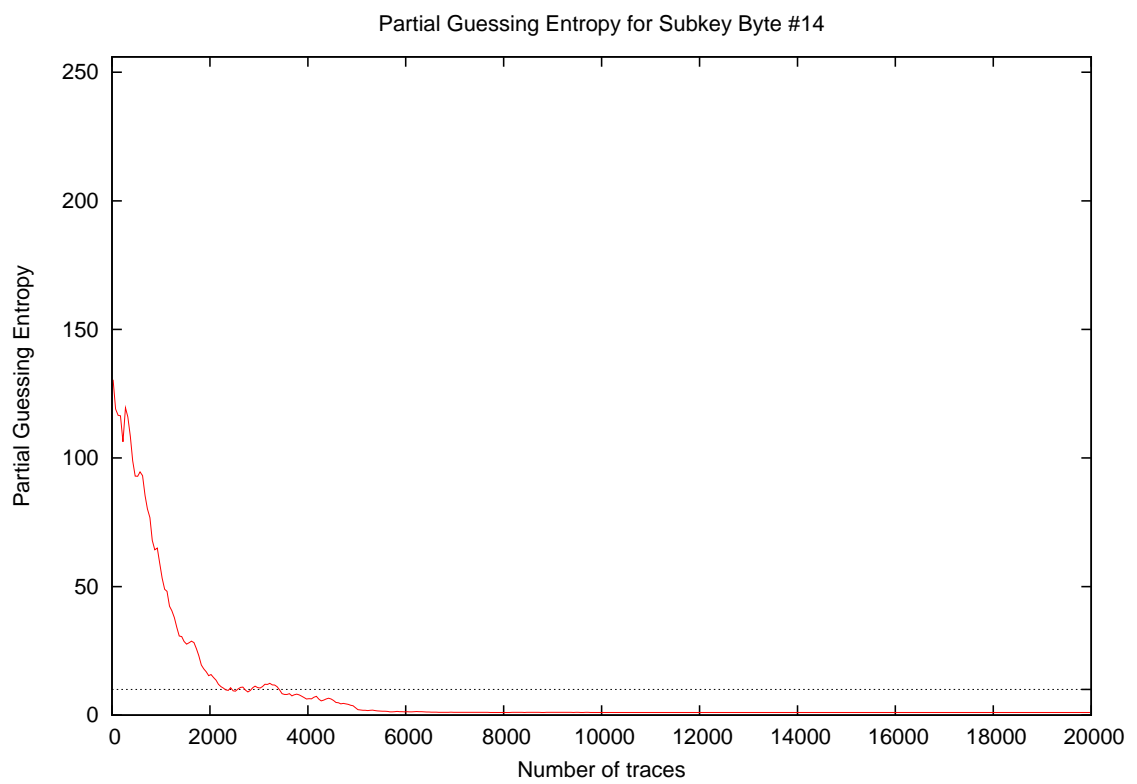
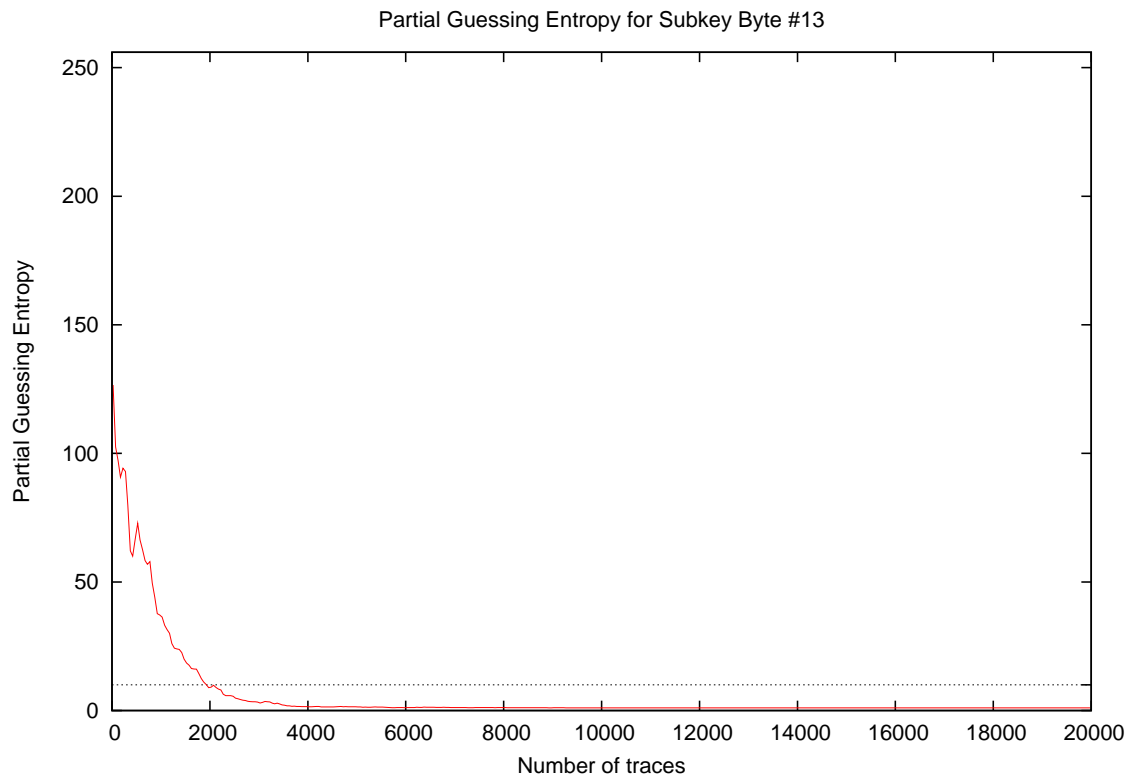
Partial Guessing Entropy for Subkey Byte #9

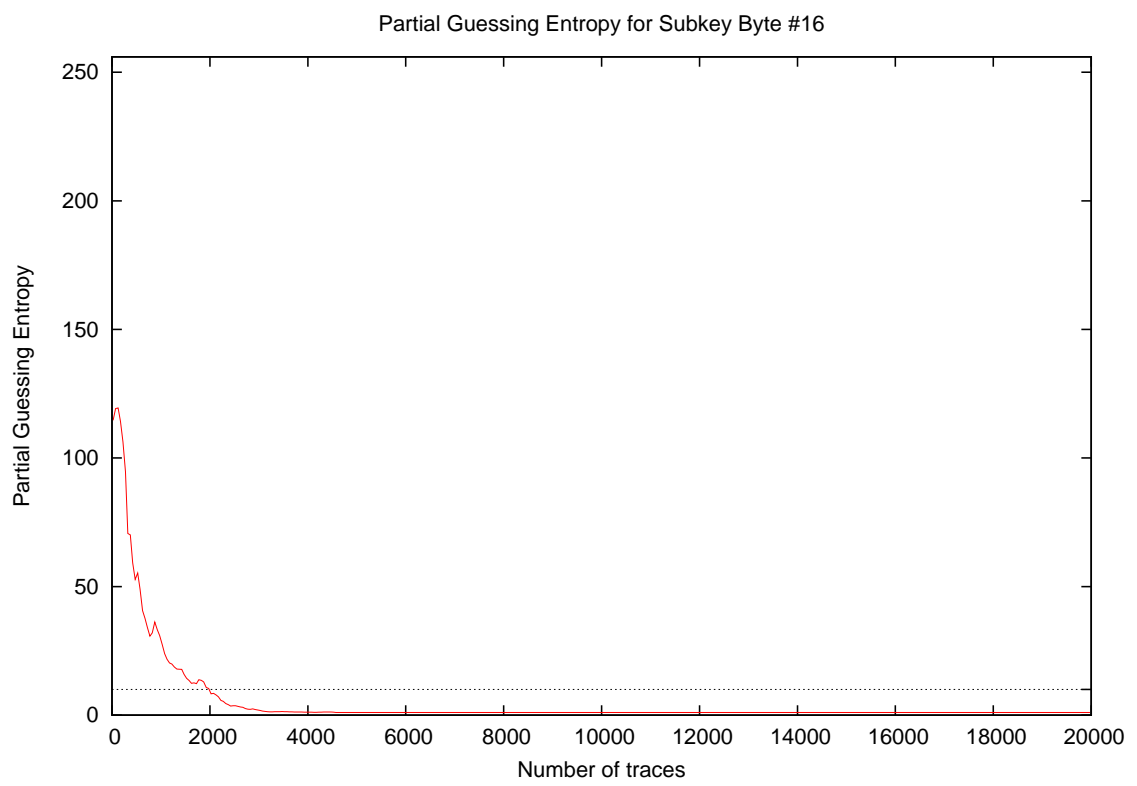
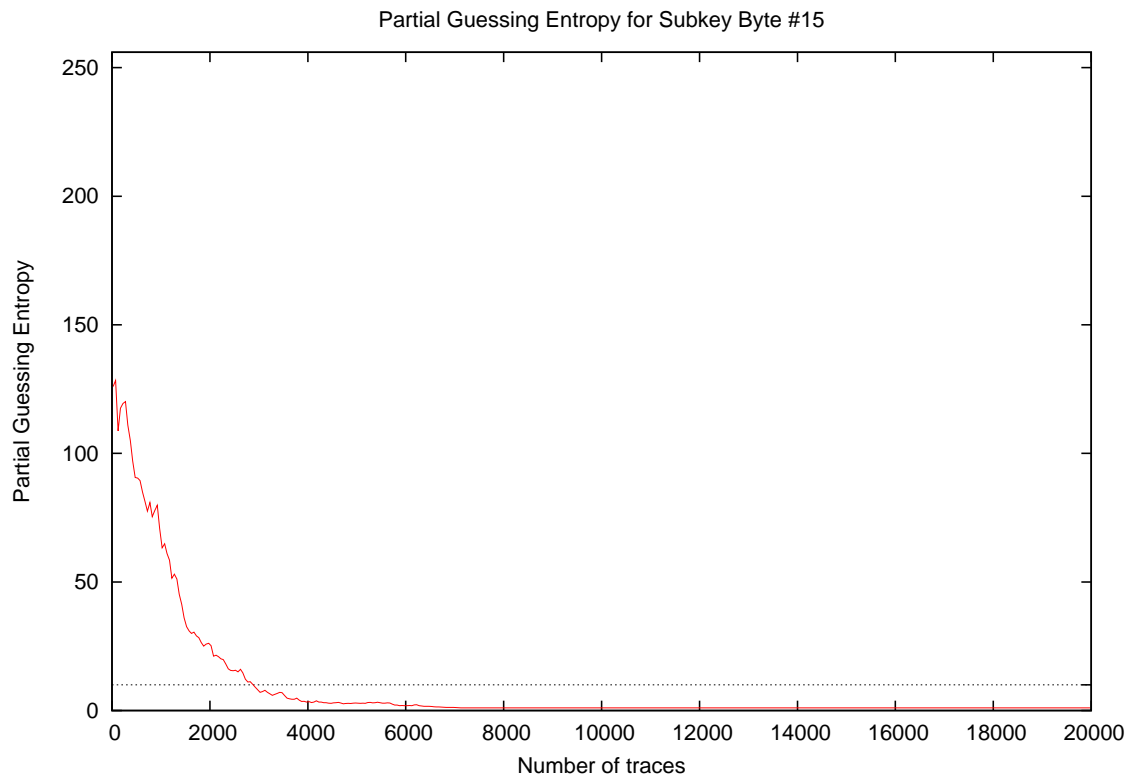


Partial Guessing Entropy for Subkey Byte #10

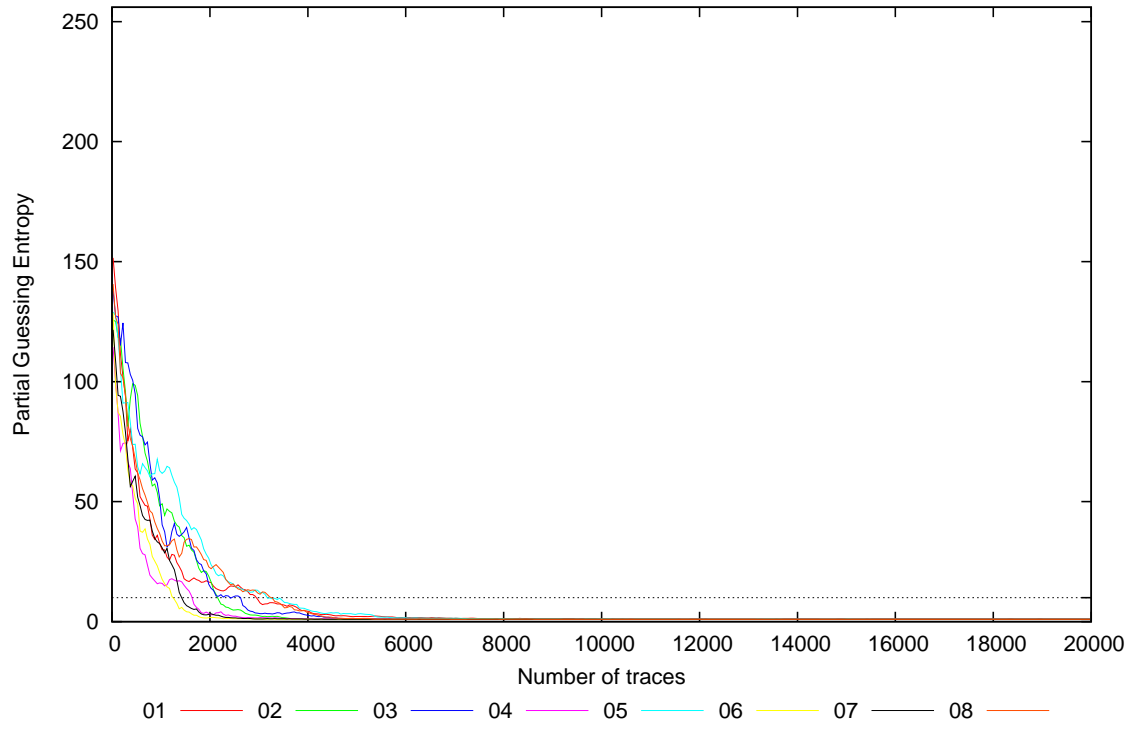




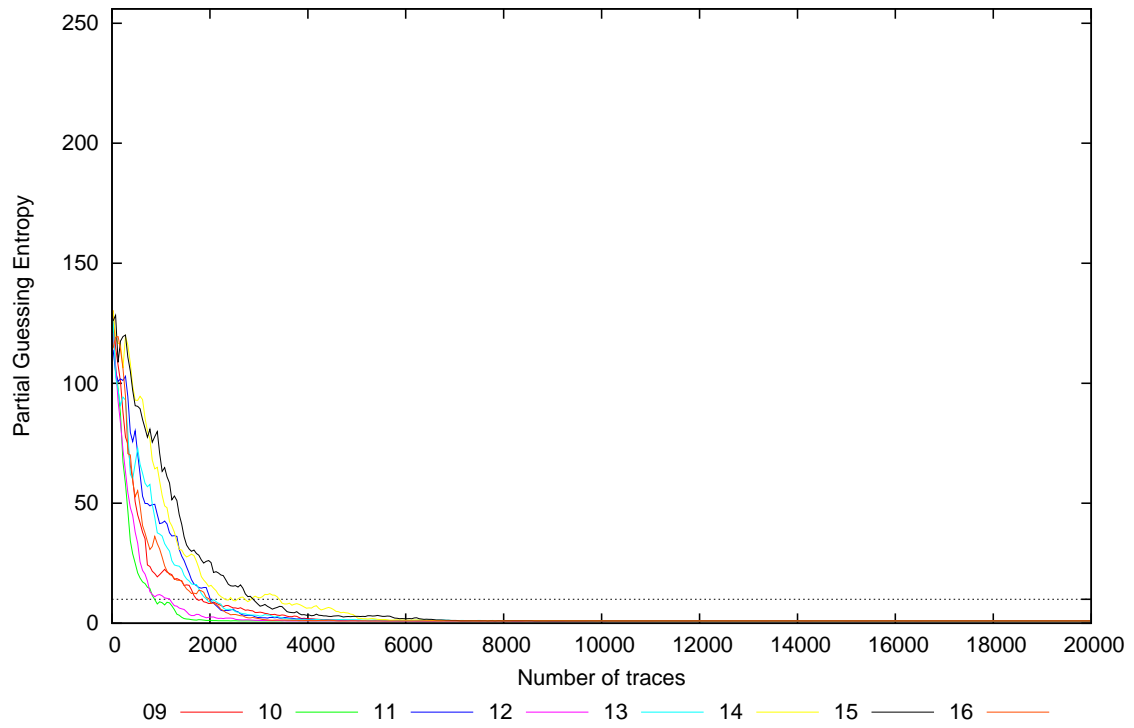




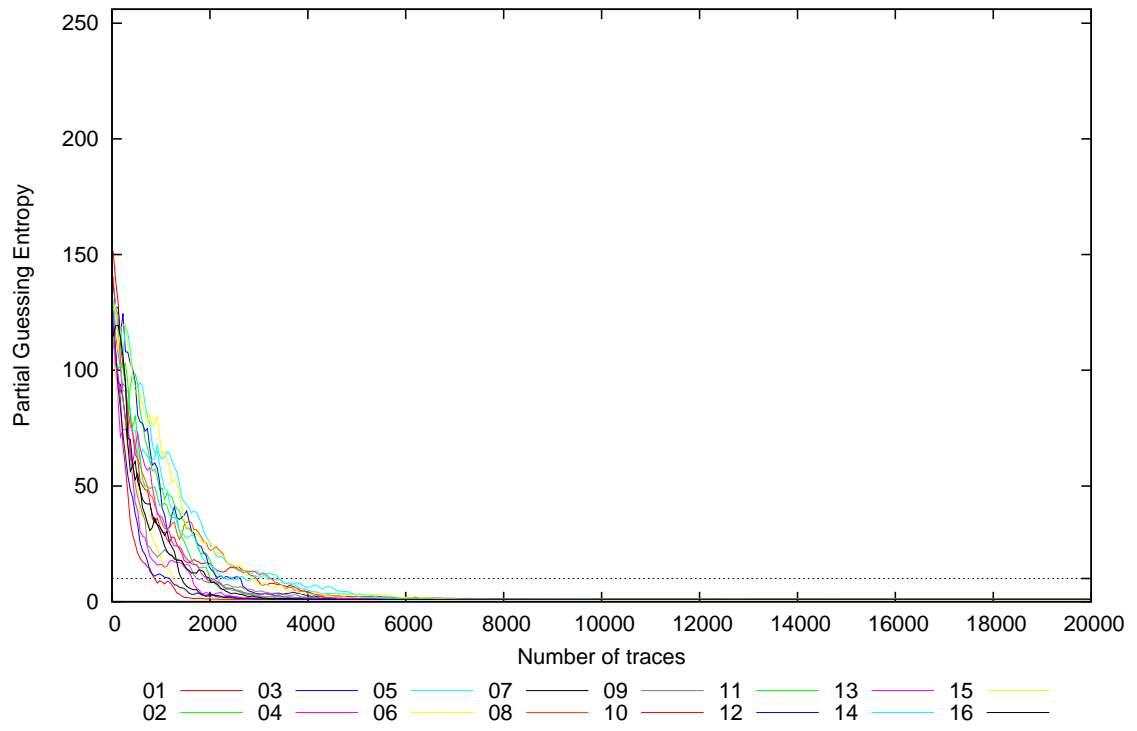
Partial Guessing Entropy for Subkey Bytes #1 to #8



Partial Guessing Entropy for Subkey Bytes #9 to #16



Partial Guessing Entropy for Subkey Bytes #1 to #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	118.0	134.0	133.7	141.1	122.0	136.9	123.8	157.2	148.1	121.0	123.4	149.2	127.1	123.5	116.5	132.0	116.5	157.2	131.7
20	157.7	130.6	156.0	110.4	131.3	140.6	127.8	138.6	145.8	107.4	105.5	117.5	137.6	152.5	118.6	102.5	102.5	157.7	130.0
30	158.4	116.7	148.9	119.6	128.2	127.0	130.7	141.3	119.9	123.1	115.9	119.0	125.4	136.3	135.4	110.7	110.7	158.4	128.5
40	164.1	125.9	129.2	105.0	127.2	127.3	115.9	147.6	128.0	121.6	111.4	114.2	116.7	127.6	131.1	110.1	105.0	164.1	125.2
50	150.1	141.9	110.5	104.6	134.9	119.2	117.1	140.3	127.0	118.0	100.7	107.2	103.2	123.2	132.2	105.0	100.7	150.1	120.9
100	140.8	112.7	130.2	103.8	117.5	88.3	97.6	115.6	112.4	93.1	107.4	88.5	95.0	123.8	119.1	125.8	88.3	140.8	110.7
200	102.2	110.9	121.9	66.0	96.6	78.7	91.5	102.7	100.0	73.4	95.7	81.7	94.1	112.7	115.4	102.8	66.0	121.9	96.6
300	79.8	86.7	108.4	75.5	90.3	71.7	71.6	85.9	78.0	53.5	99.9	55.0	90.5	113.3	113.0	82.6	53.5	113.3	84.7
400	76.6	102.6	101.9	56.4	83.0	61.2	52.3	70.5	60.1	30.6	74.9	44.2	58.7	99.9	102.9	67.5	30.6	102.9	71.5
500	62.8	99.7	85.8	44.0	69.5	53.5	53.9	61.7	46.0	22.5	77.8	33.7	74.2	92.5	88.2	55.4	22.5	99.7	63.8
1000	31.0	49.4	47.3	15.6	61.9	18.7	30.6	35.7	20.8	9.0	41.4	11.7	36.8	57.5	68.4	29.0	9.0	68.4	35.3
2000	16.4	17.9	14.6	2.9	24.9	1.8	3.3	23.7	7.8	1.1	10.3	2.7	9.7	15.5	25.5	9.2	1.1	25.5	11.7
3000	8.5	2.4	3.3	1.6	12.2	1.1	1.1	11.0	4.5	1.0	2.2	1.2	3.0	10.9	6.8	1.9	1.0	12.2	4.6
4000	4.3	1.2	2.7	1.2	5.2	1.0	1.0	3.7	1.9	1.0	1.6	1.0	1.5	6.1	3.3	1.2	1.0	6.1	2.4
5000	2.1	1.0	1.2	1.2	3.0	1.0	1.0	1.3	1.1	1.0	1.1	1.0	1.4	2.2	2.9	1.0	1.0	3.0	1.5
10000	1.1	1.0	1.0	1.0	1.1	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.1	1.0
15000	1.1	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.1	1.0
20000	1.1	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.1	1.0