

Evaluation results

DPA contest v2

September 2010

1 Introduction

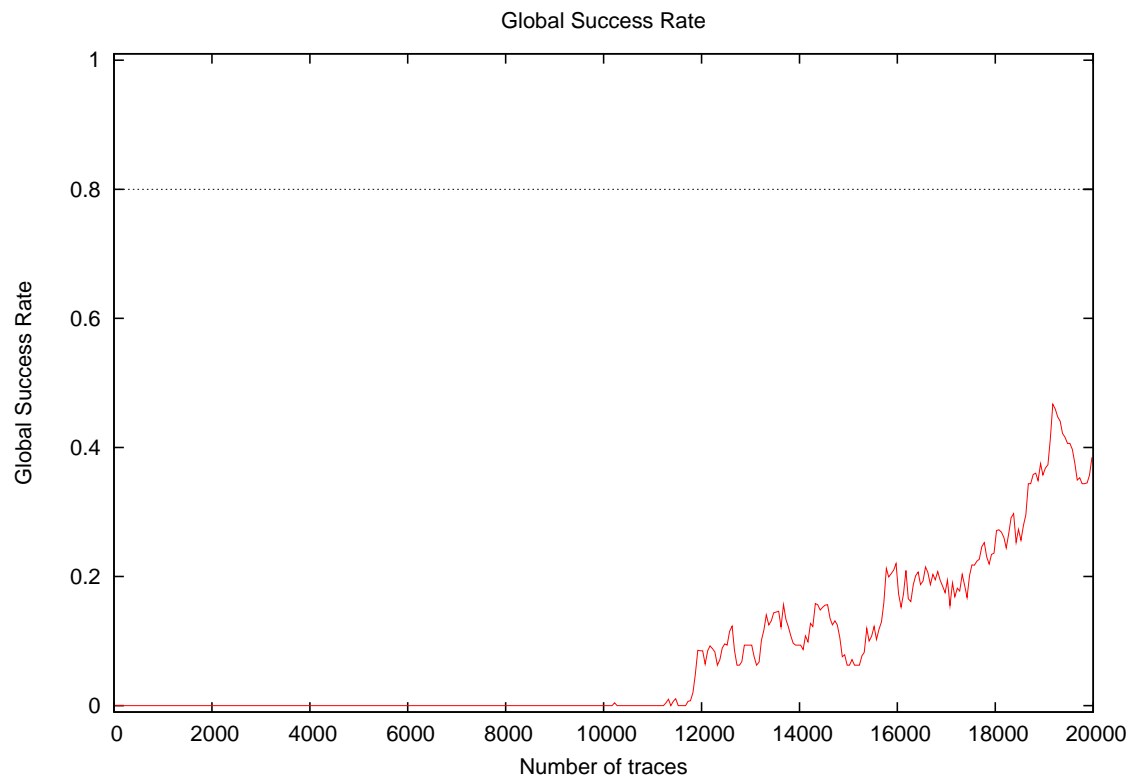
1.1 About the attack

- **Attack Name:** DPA
- **Sender/Team:** Alexis Bonnecaze
- **Institution:** IML, ERISCS
- **Language:** C++
- **Attacked subkey:** 10

1.2 About the evaluation

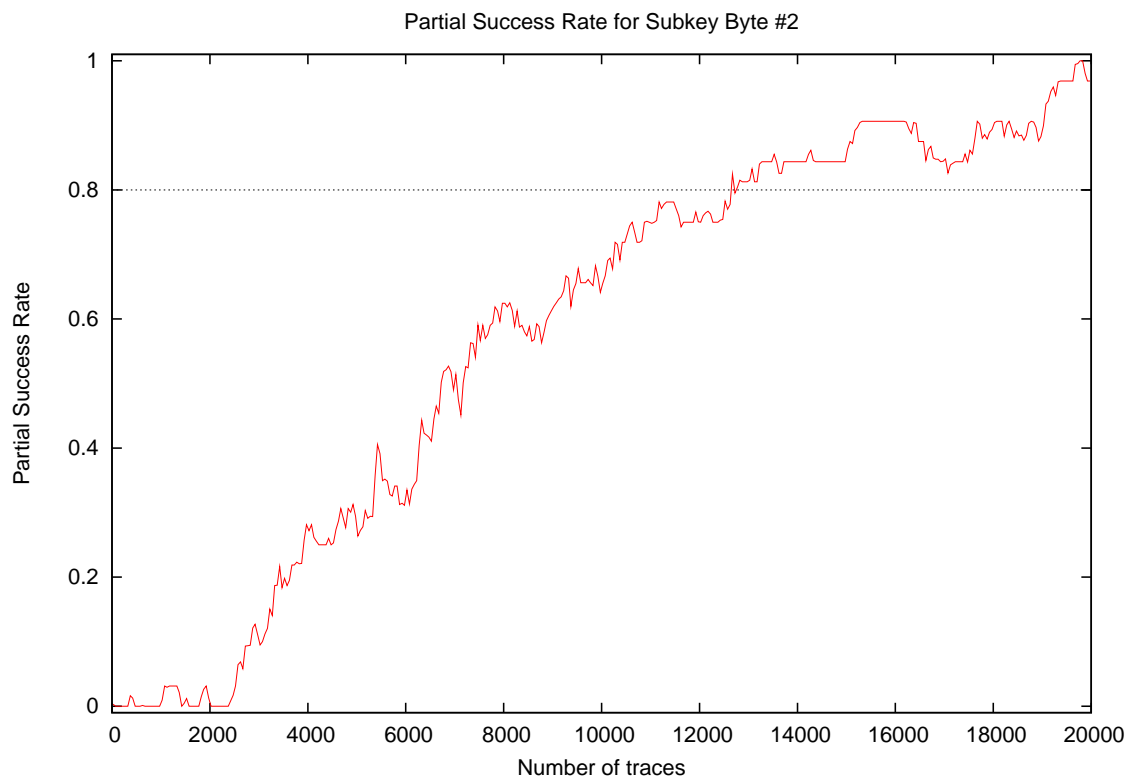
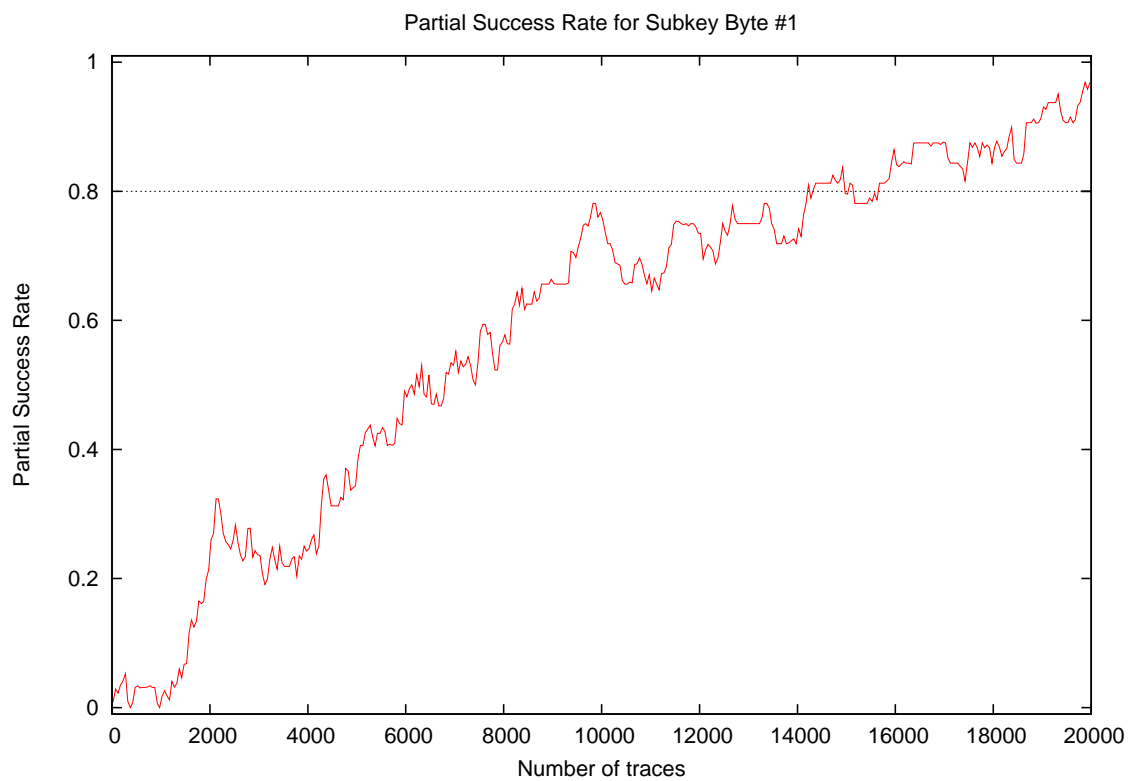
- **Date of evaluation:** August 2010

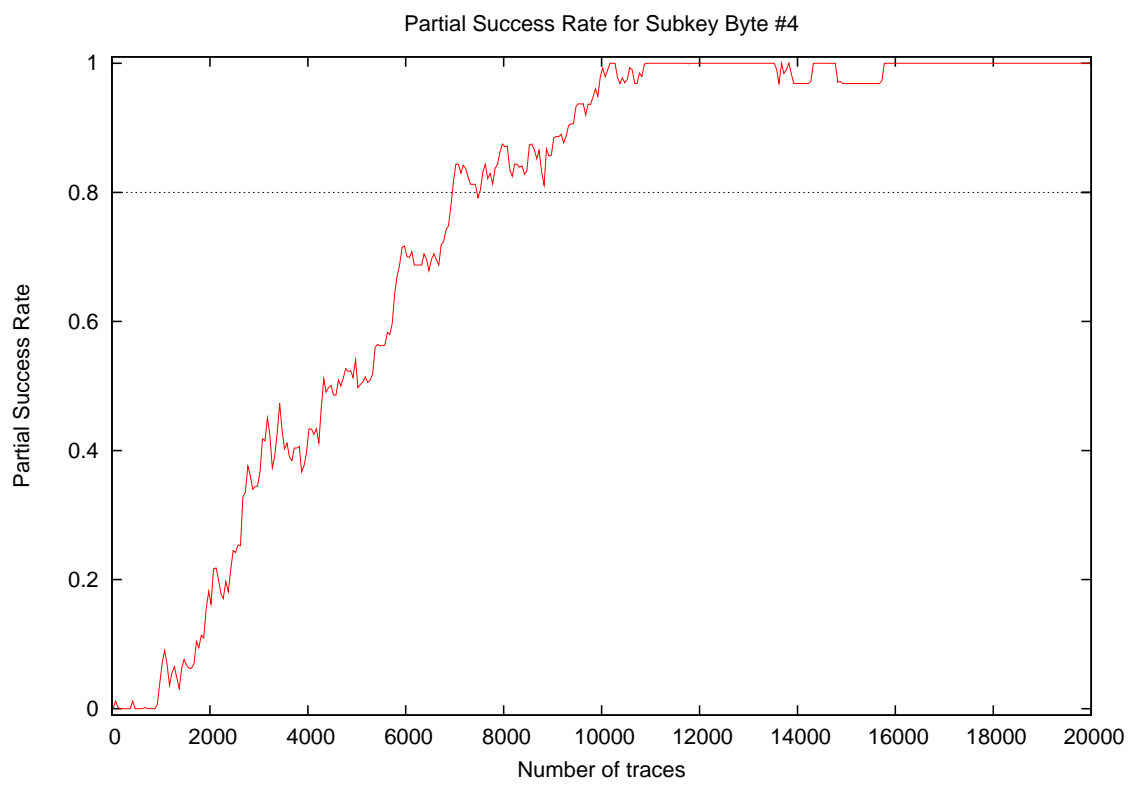
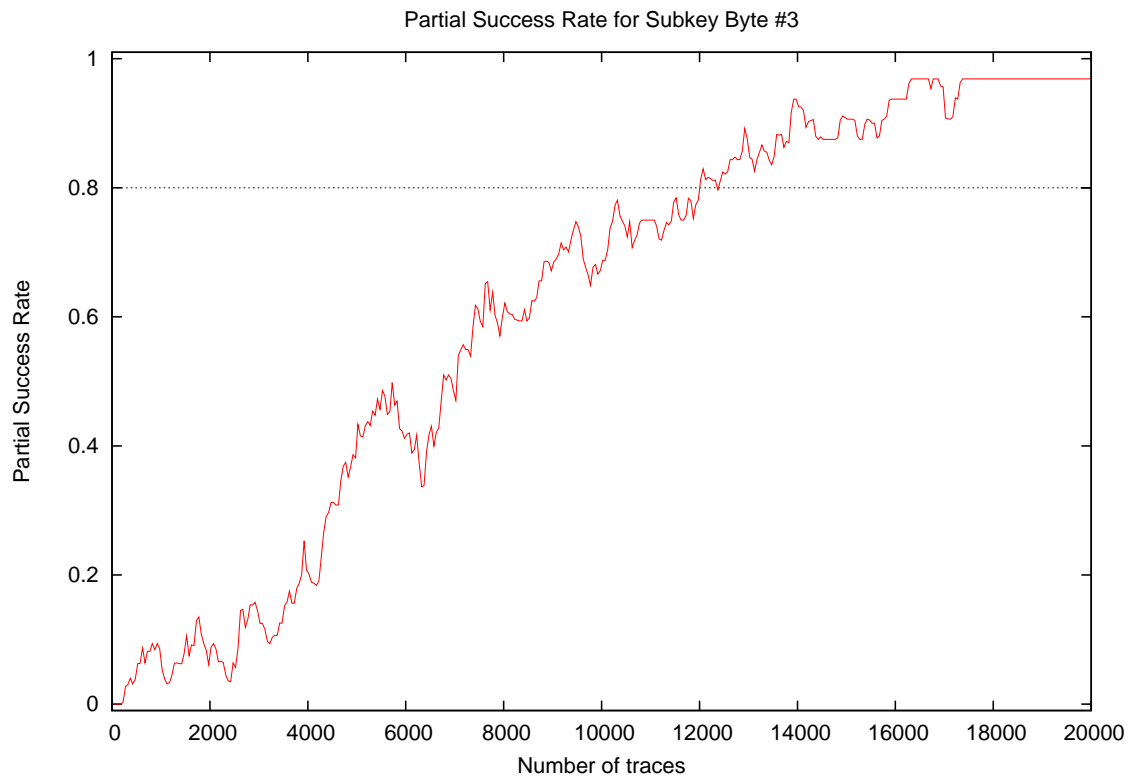
2 Global Success Rate

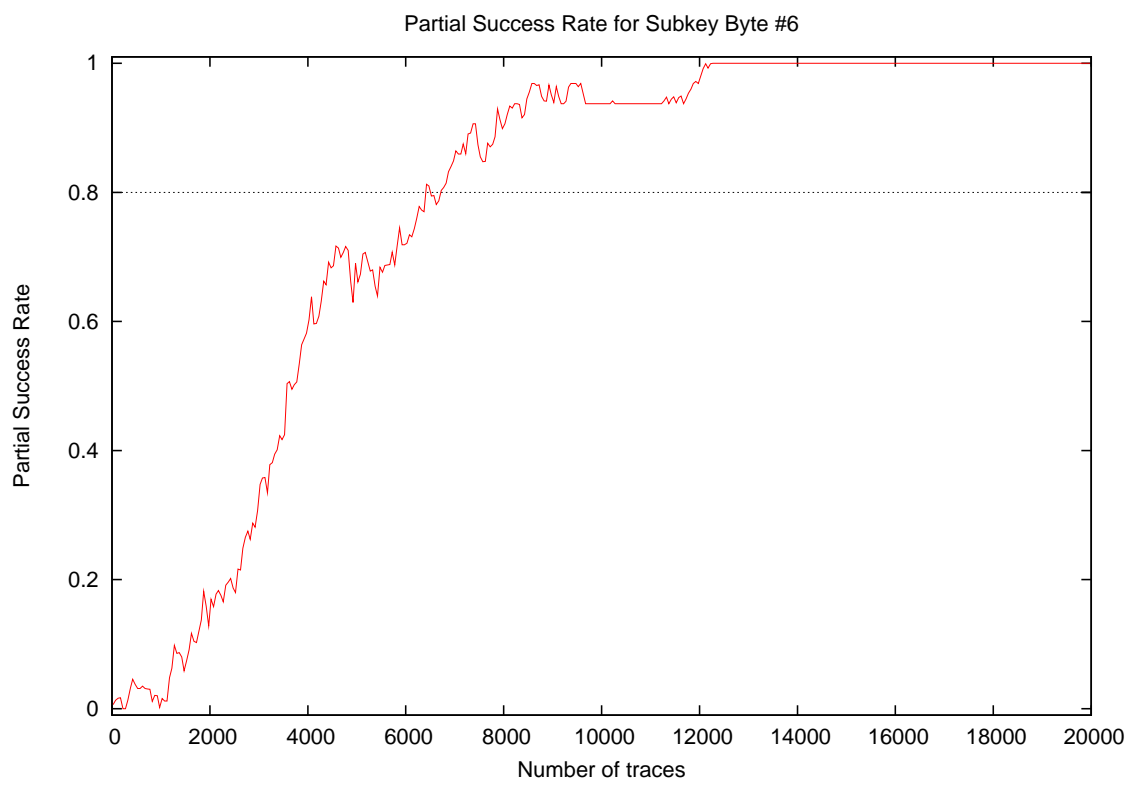
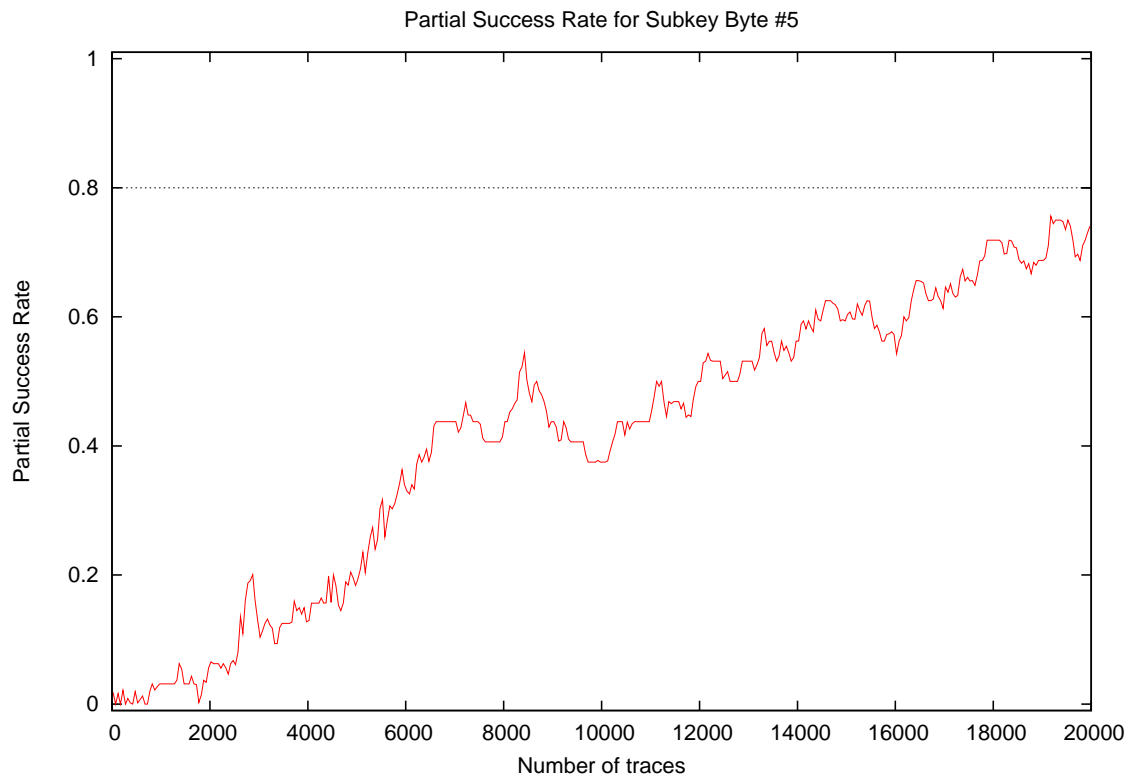


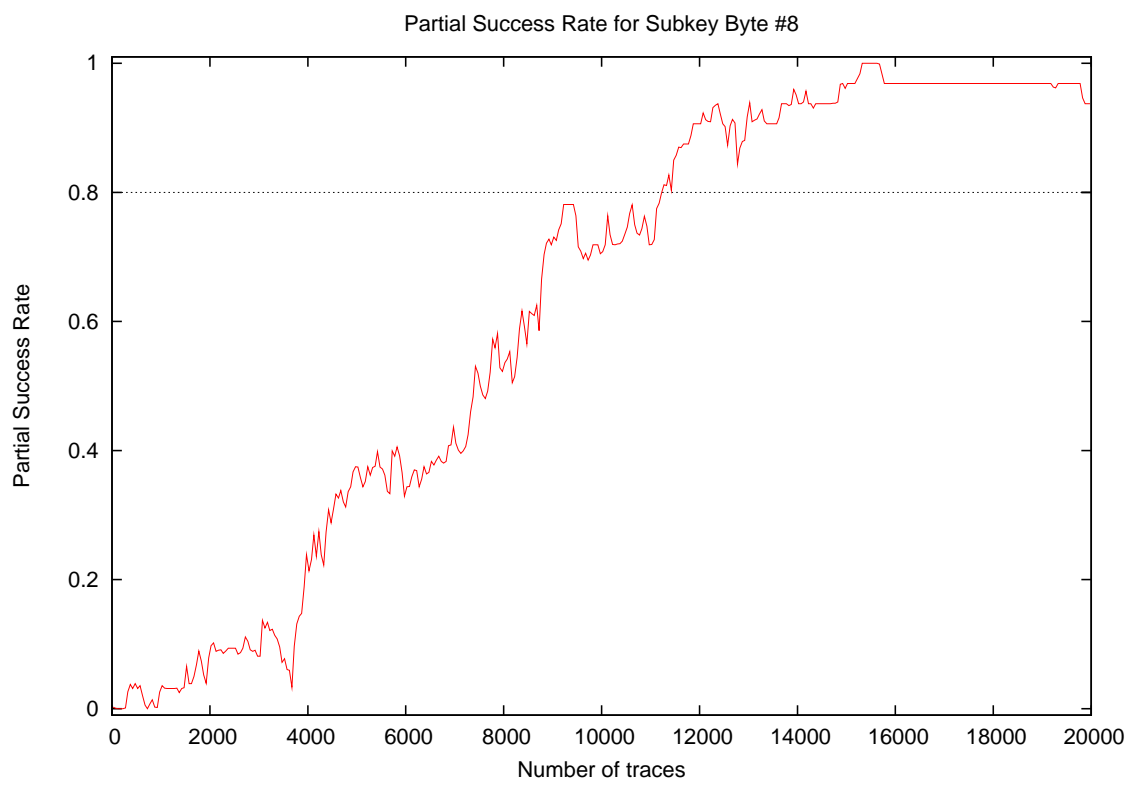
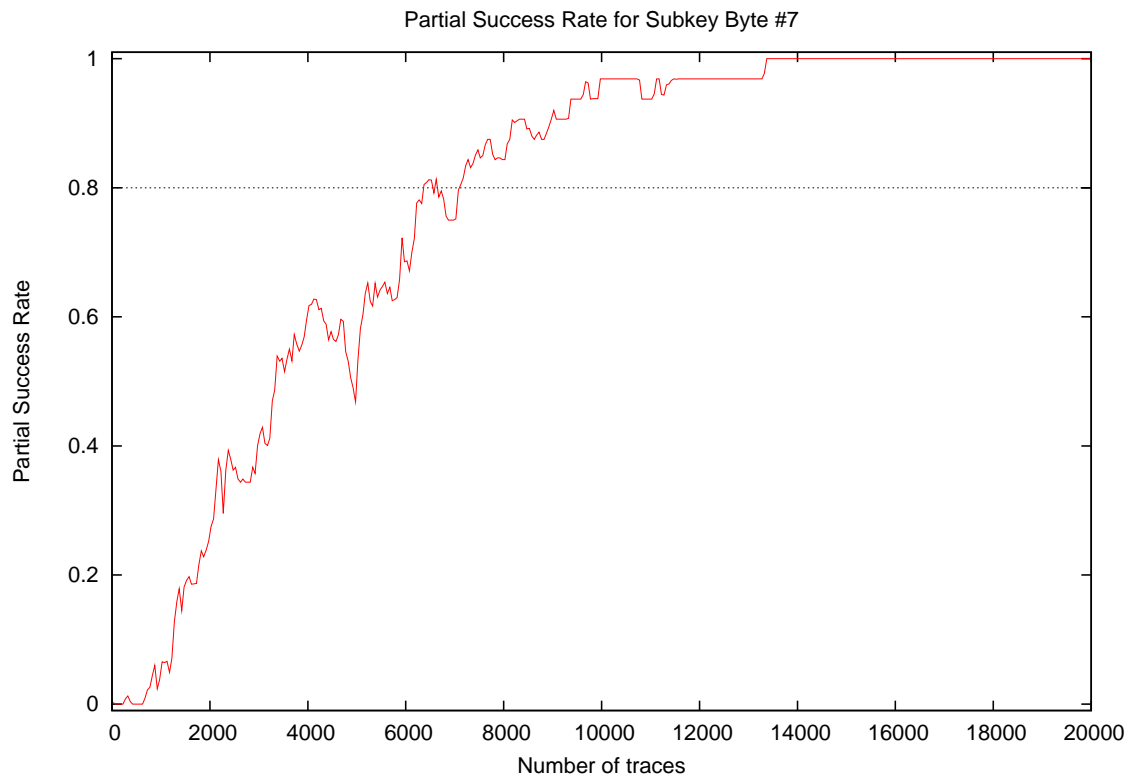
Number of traces	Global Success Rate
10	0.00
20	0.00
30	0.00
40	0.00
50	0.00
100	0.00
200	0.00
300	0.00
400	0.00
500	0.00
1000	0.00
2000	0.00
3000	0.00
4000	0.00
5000	0.00
10000	0.00
15000	0.06
20000	0.41

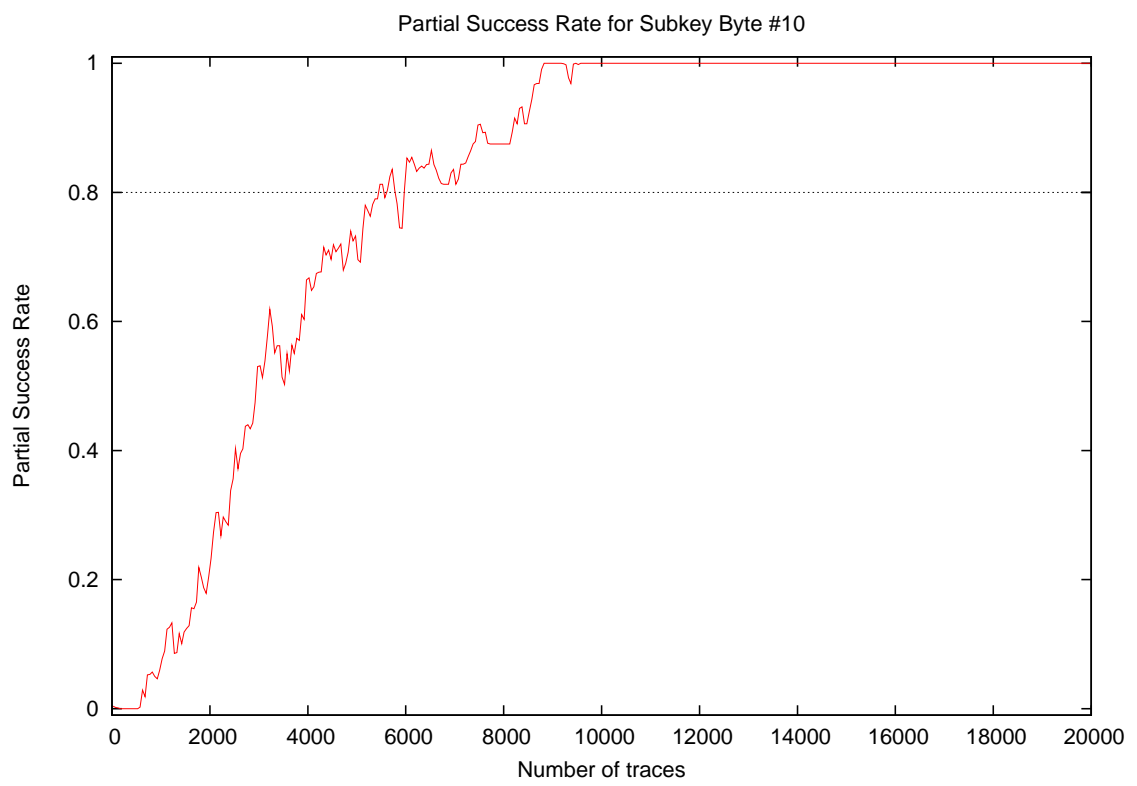
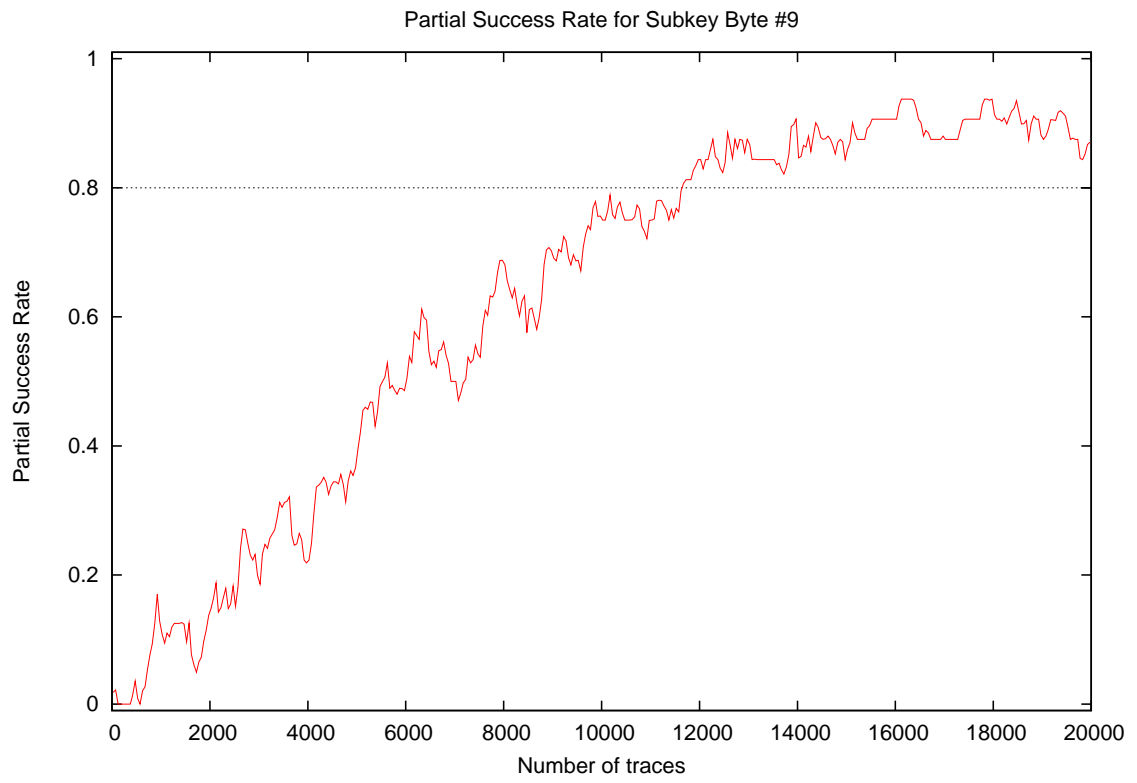
3 Partial Success Rate

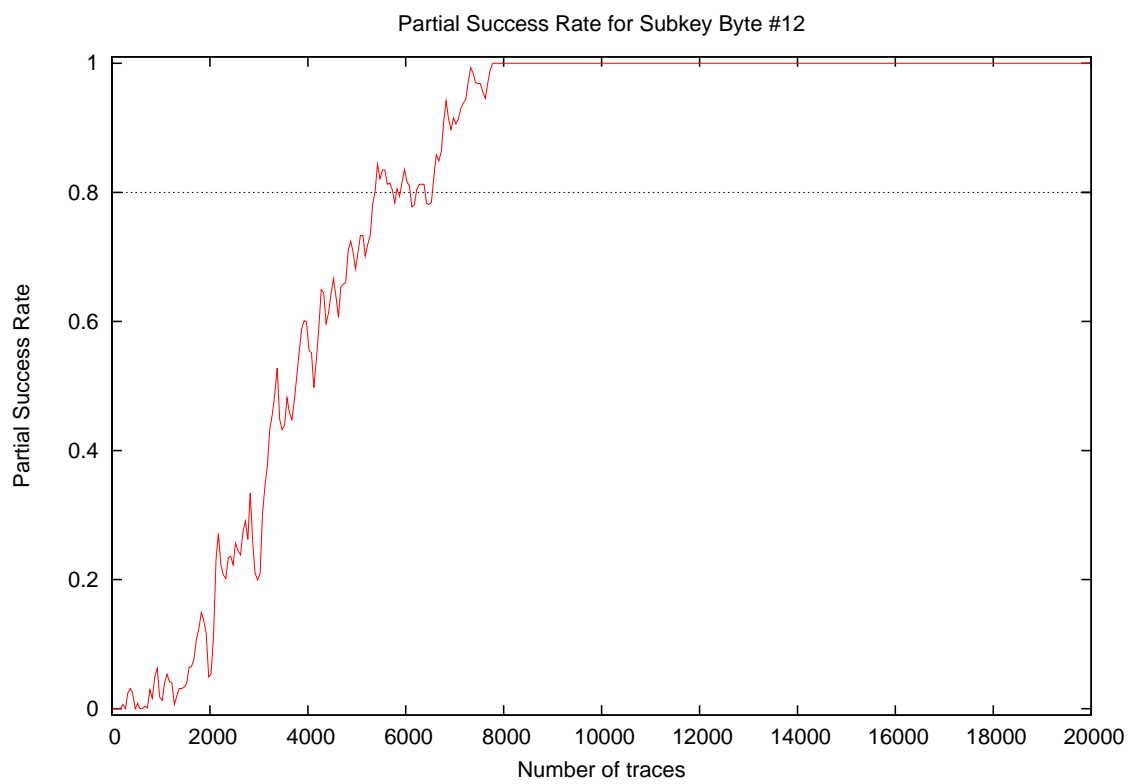
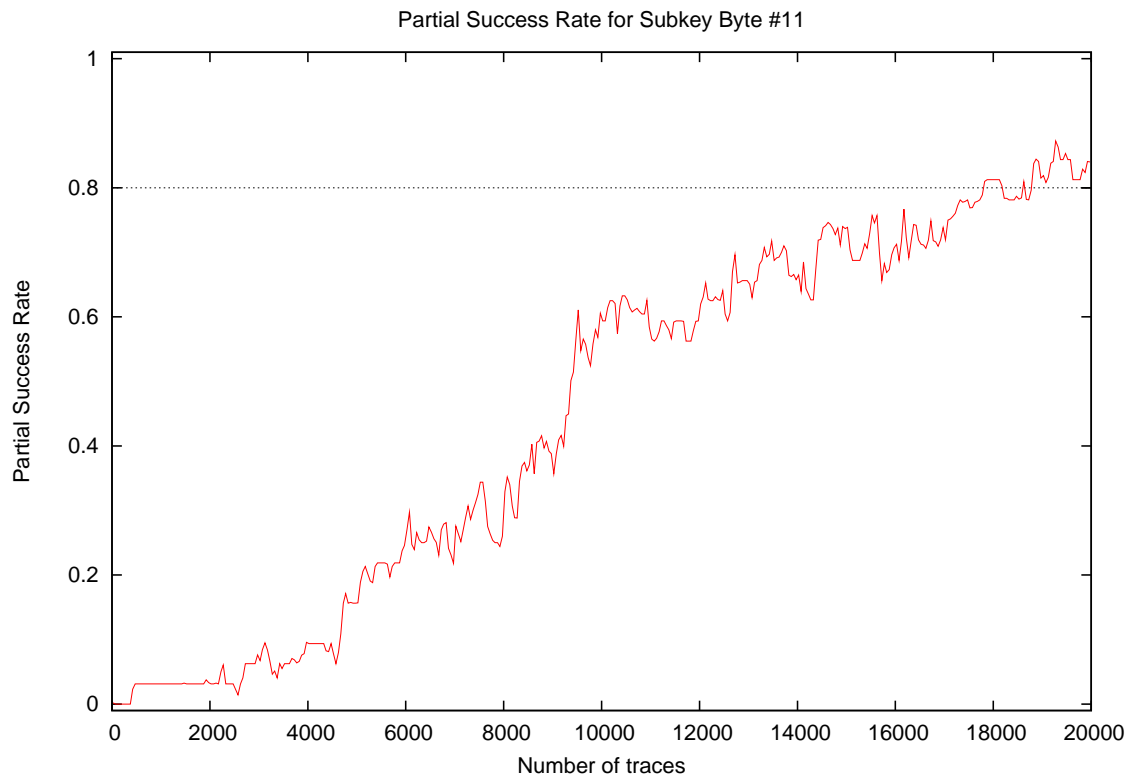


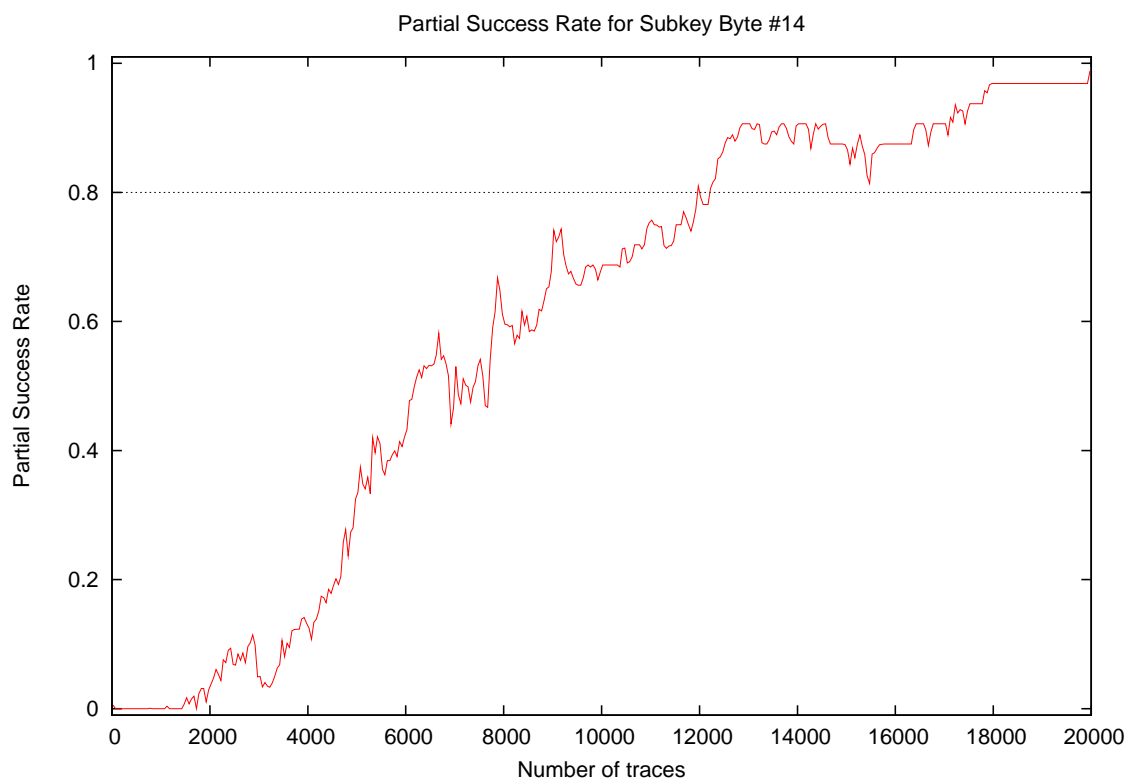
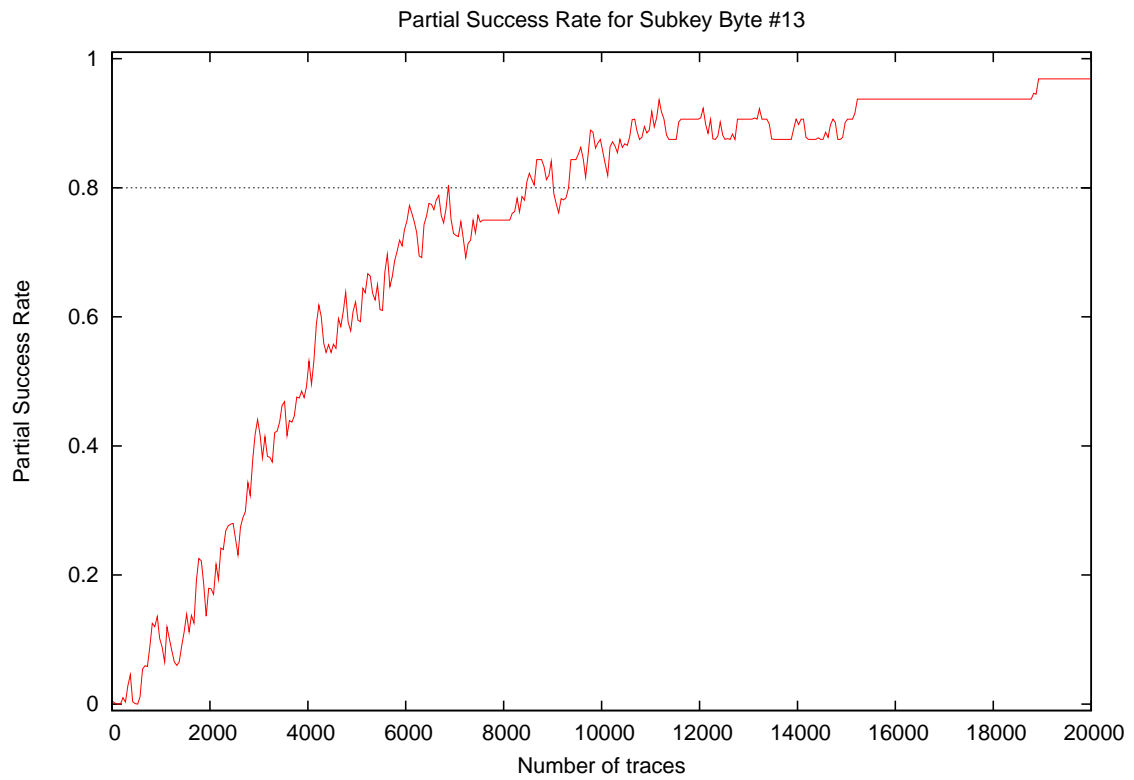


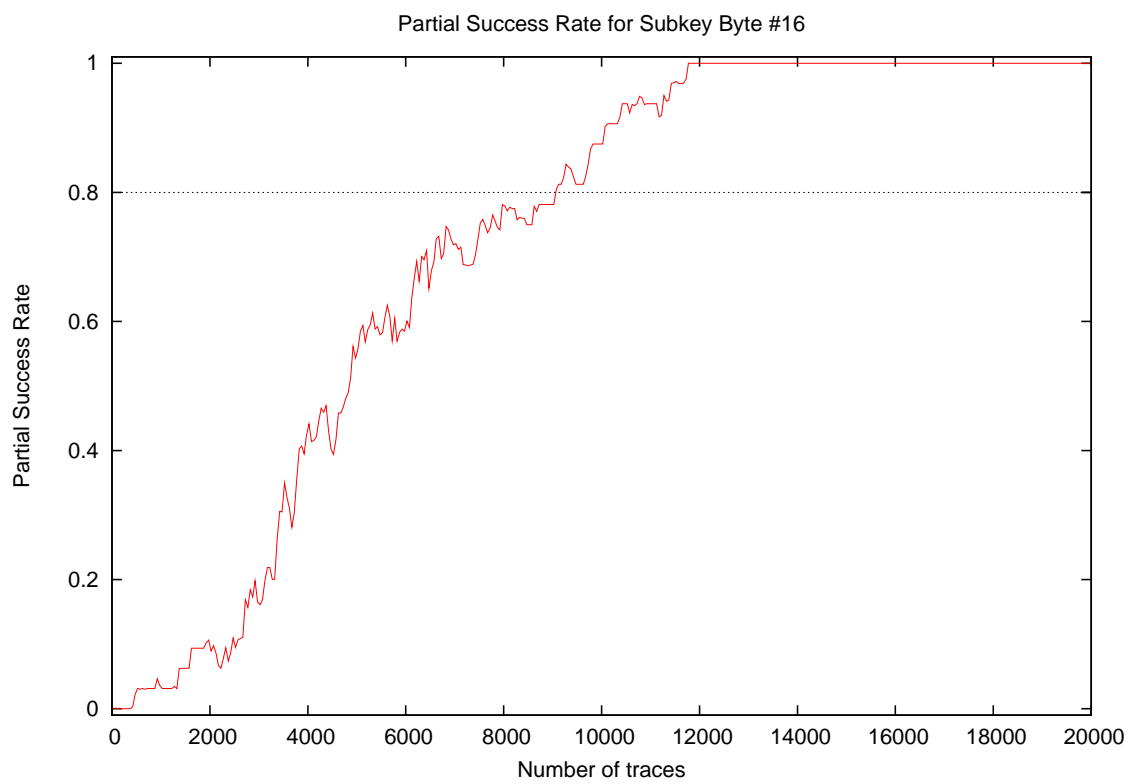
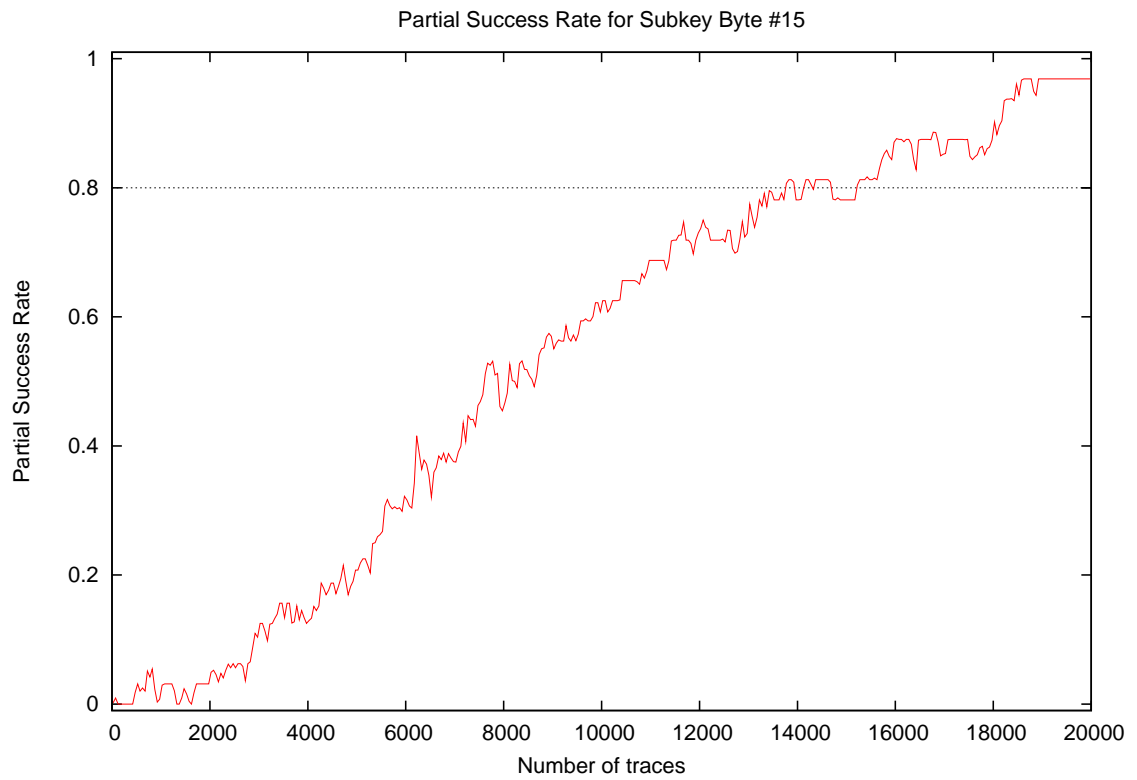




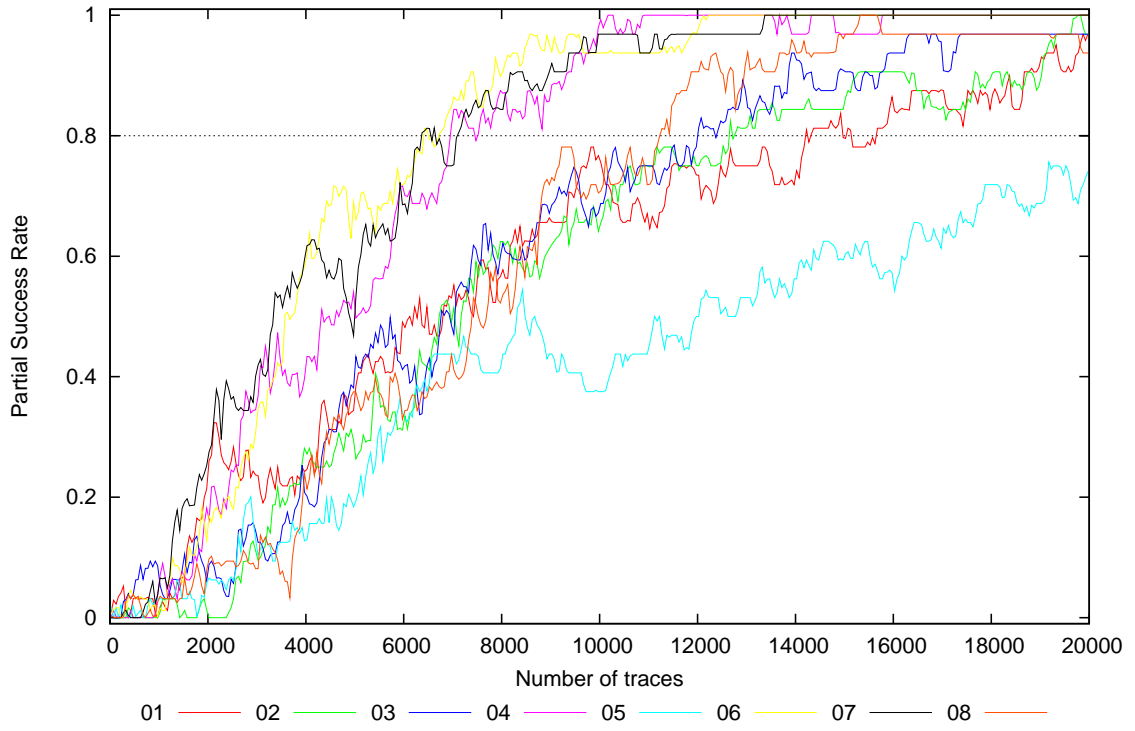




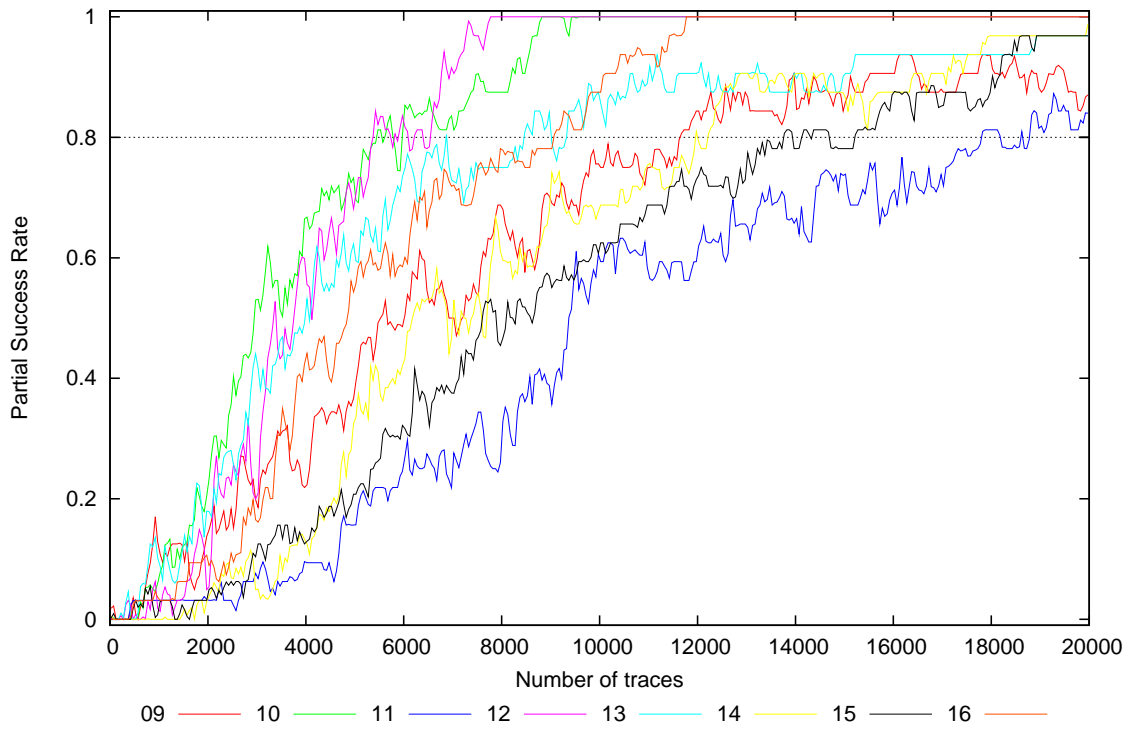




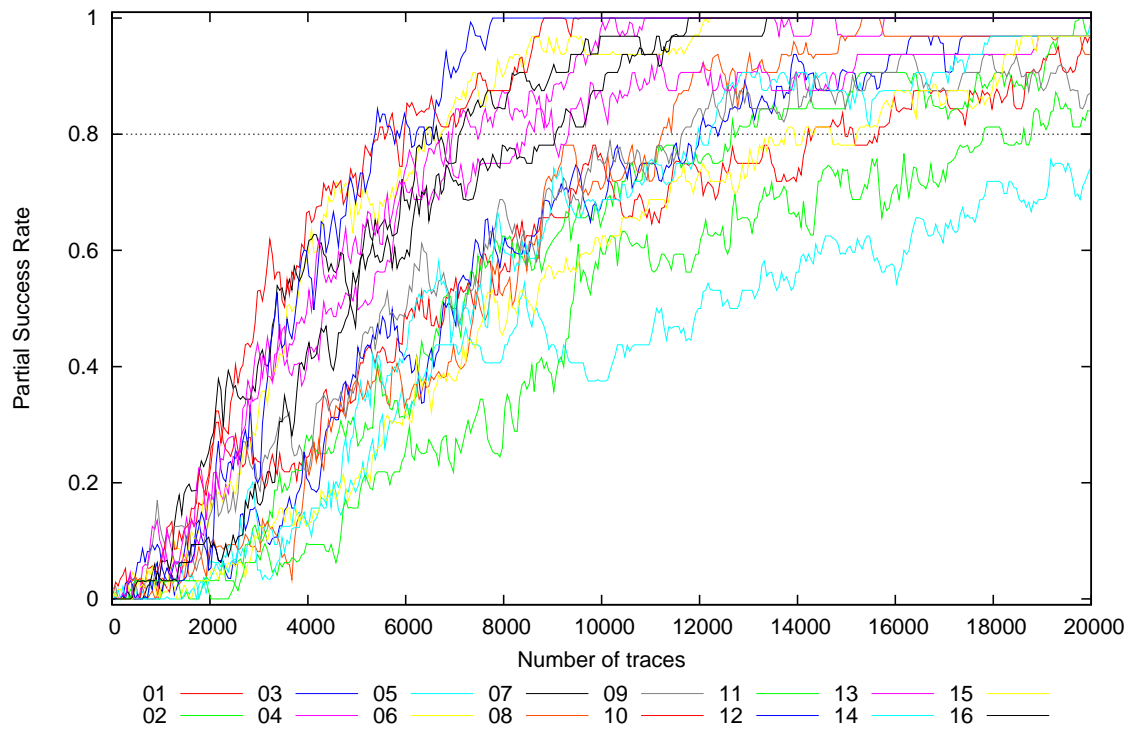
Partial Success Rate for Subkey Bytes #1 to #8



Partial Success Rate for Subkey Bytes #9 to #16

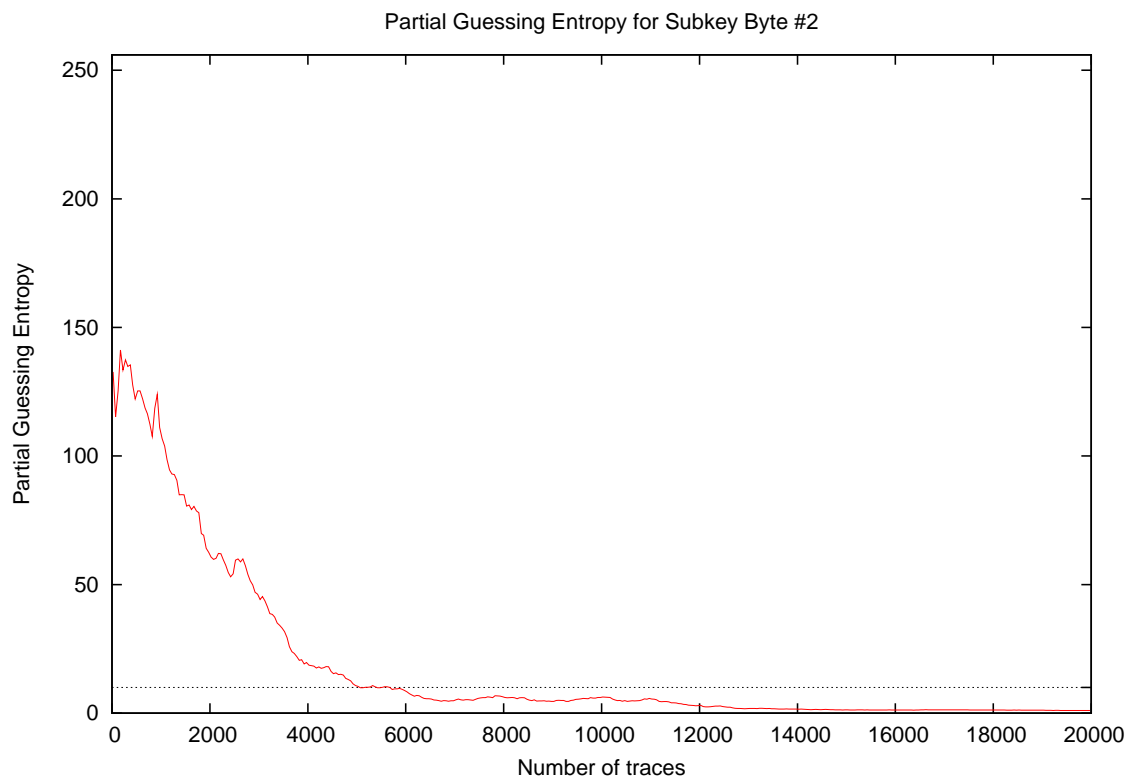
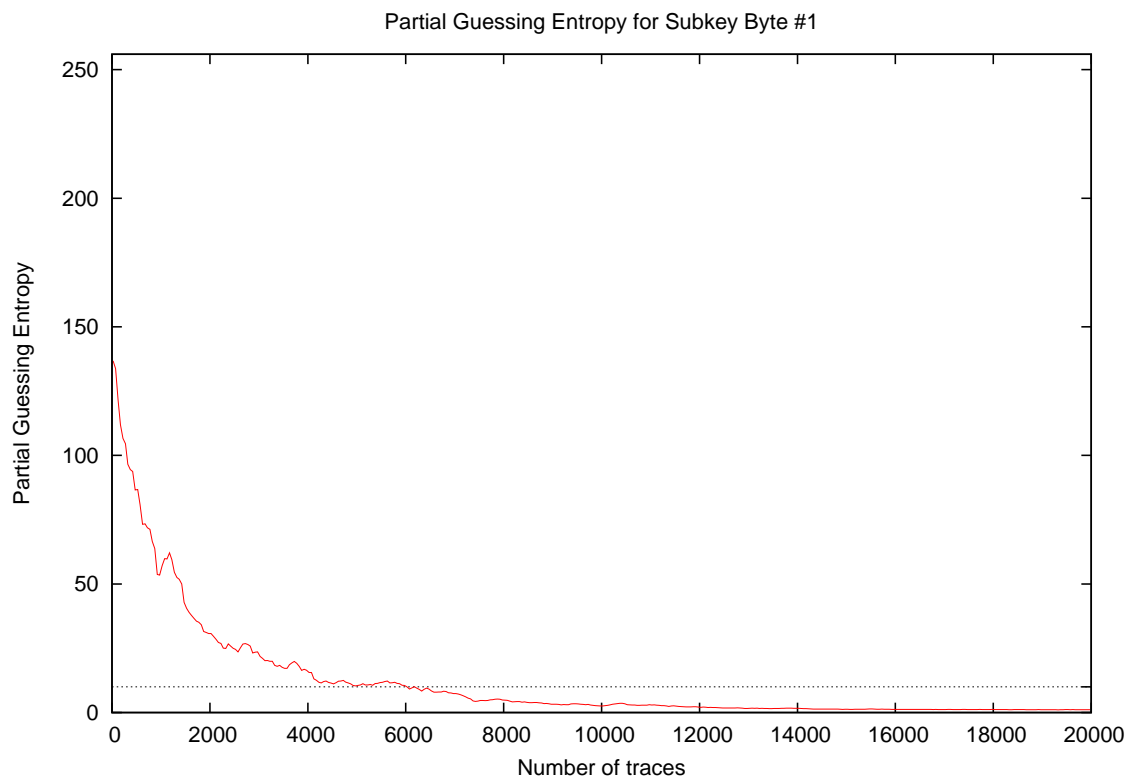


Partial Success Rate for Subkey Bytes #1 to #16

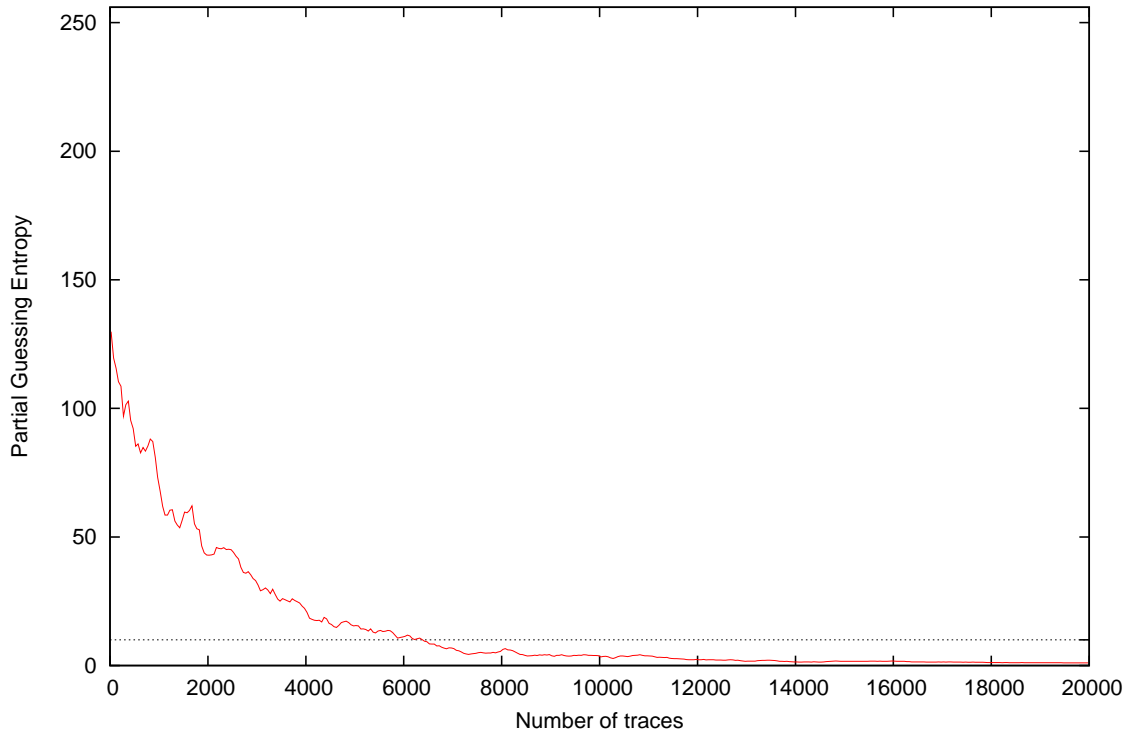


Traces	Partial Success Rate / Byte																Min	Max	Mean					
	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16								
10	0.00	0.00	0.00	0.00	0.00	0.00	0.03	0.00	0.00	0.00	0.03	0.00	0.00	0.00	0.00	0.00	0.00	0.03	0.00	0.00	0.00	0.03	0.00	
20	0.00	0.00	0.00	0.00	0.06	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
30	0.00	0.00	0.00	0.00	0.03	0.00	0.00	0.00	0.06	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	0.01
40	0.03	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	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
50	0.03	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.06	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	0.01
100	0.03	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.06	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	0.01
200	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	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
300	0.03	0.00	0.06	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	0.00	0.00	0.00	0.00	0.00	0.01
400	0.00	0.00	0.06	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	0.00	0.00	0.00	0.00	0.00	0.01
500	0.03	0.00	0.06	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	0.00	0.00	0.00	0.00	0.00	0.01
1000	0.00	0.00	0.06	0.06	0.03	0.00	0.06	0.06	0.12	0.12	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	0.02
2000	0.25	0.00	0.06	0.19	0.06	0.12	0.28	0.06	0.12	0.16	0.03	0.03	0.03	0.16	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.09	0.00	0.04
3000	0.22	0.09	0.12	0.34	0.12	0.31	0.41	0.12	0.22	0.53	0.09	0.22	0.41	0.03	0.12	0.16	0.03	0.03	0.03	0.12	0.16	0.03	0.03	0.11
4000	0.25	0.28	0.22	0.44	0.12	0.56	0.62	0.25	0.22	0.66	0.09	0.56	0.53	0.03	0.12	0.12	0.12	0.12	0.12	0.12	0.44	0.09	0.66	0.22
5000	0.34	0.28	0.41	0.50	0.22	0.69	0.47	0.38	0.38	0.72	0.16	0.66	0.62	0.31	0.19	0.56	0.16	0.72	0.16	0.72	0.44	0.09	0.66	0.34
10000	0.75	0.62	0.69	1.00	0.38	0.94	0.97	0.69	0.75	1.00	0.59	1.00	0.88	0.69	0.62	0.88	0.38	1.00	0.78	0.62	0.88	0.38	1.00	0.78
15000	0.78	0.84	0.91	0.97	0.59	1.00	1.00	0.97	0.84	1.00	0.72	1.00	0.91	0.88	0.78	1.00	0.59	1.00	0.89	0.78	1.00	0.59	1.00	0.89
20000	0.97	0.97	0.97	1.00	0.75	1.00	1.00	0.94	0.84	1.00	0.81	1.00	0.97	1.00	0.97	1.00	0.75	1.00	0.95	0.97	1.00	0.75	1.00	0.95

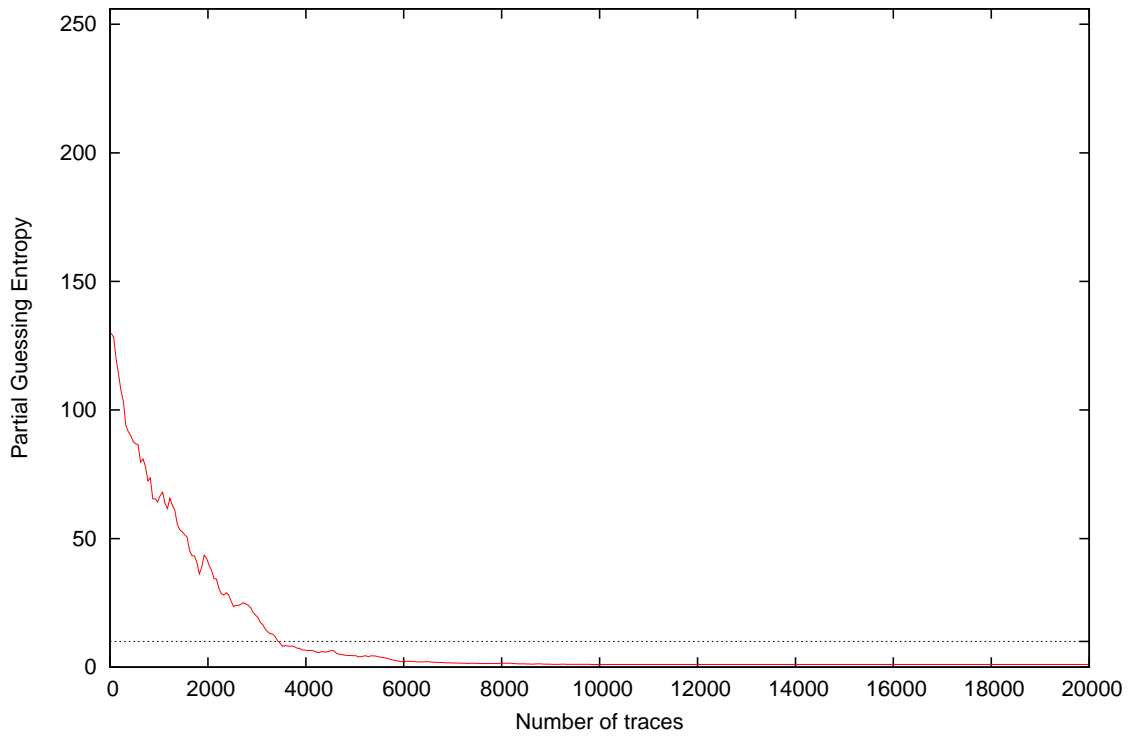
4 Partial Guessing Entropy



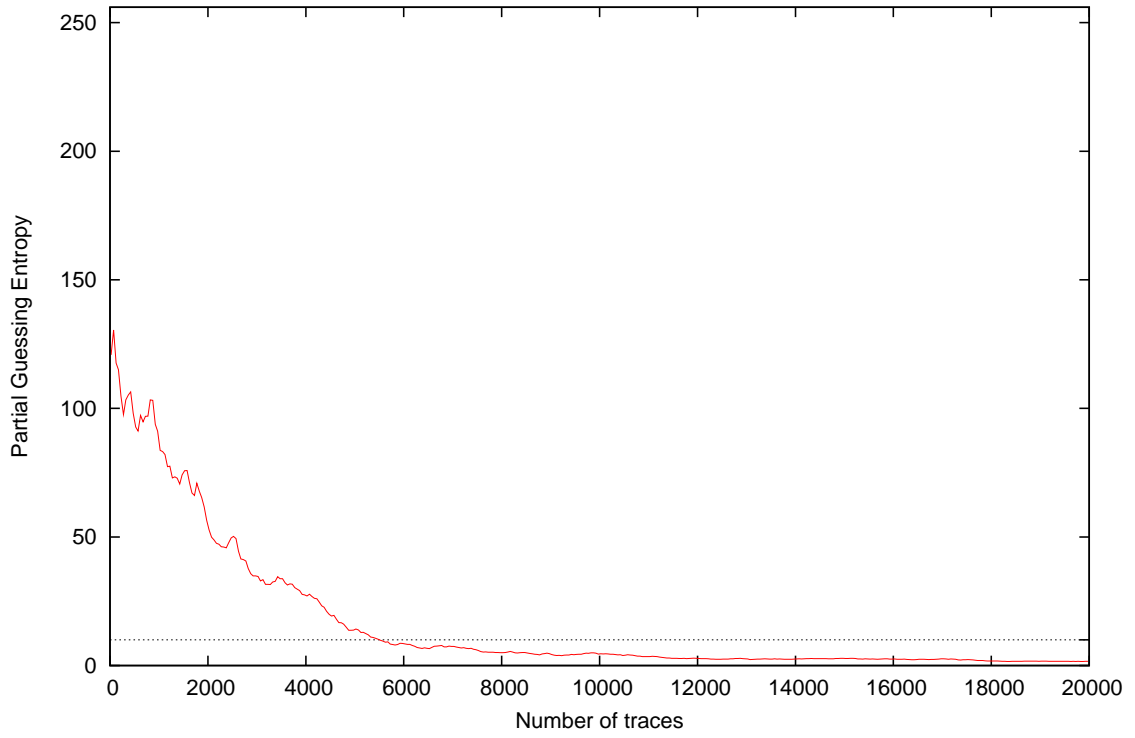
Partial Guessing Entropy for Subkey Byte #3



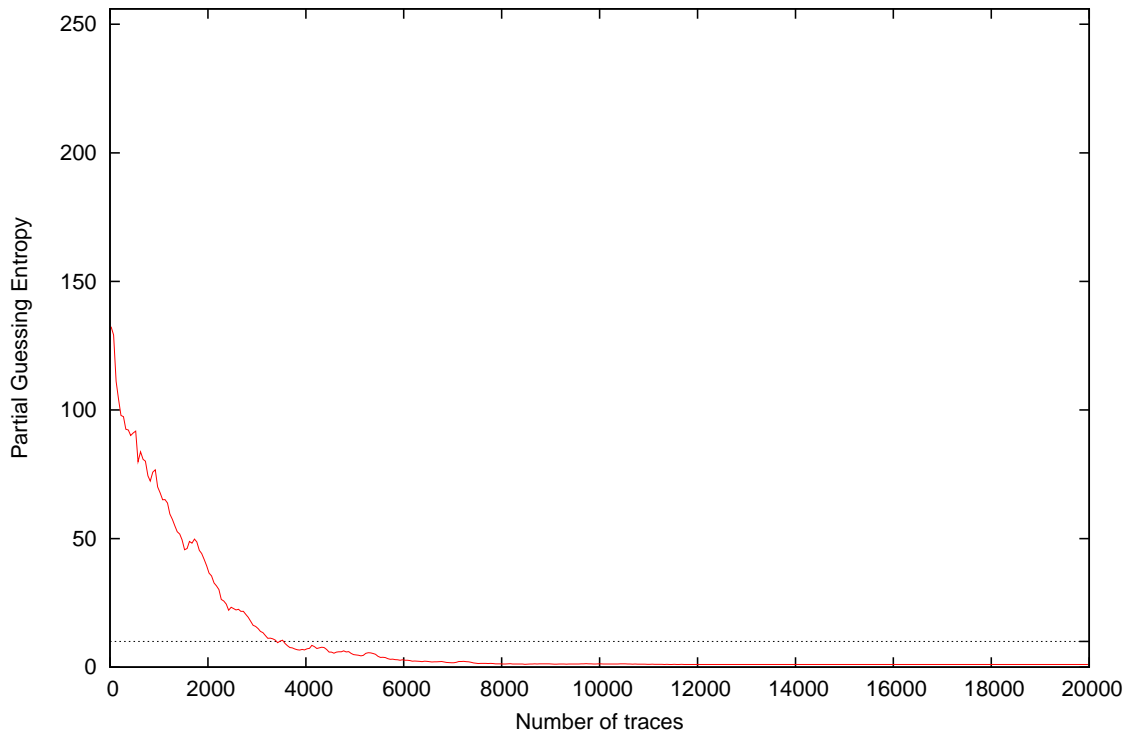
Partial Guessing Entropy for Subkey Byte #4



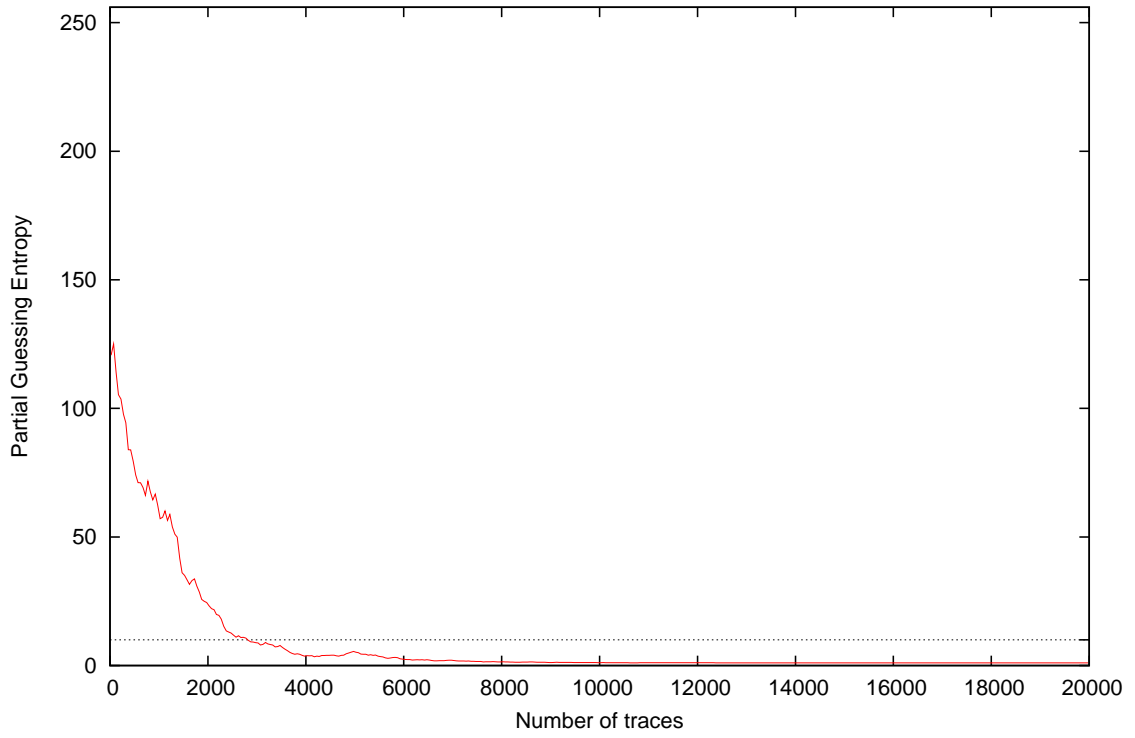
Partial Guessing Entropy for Subkey Byte #5



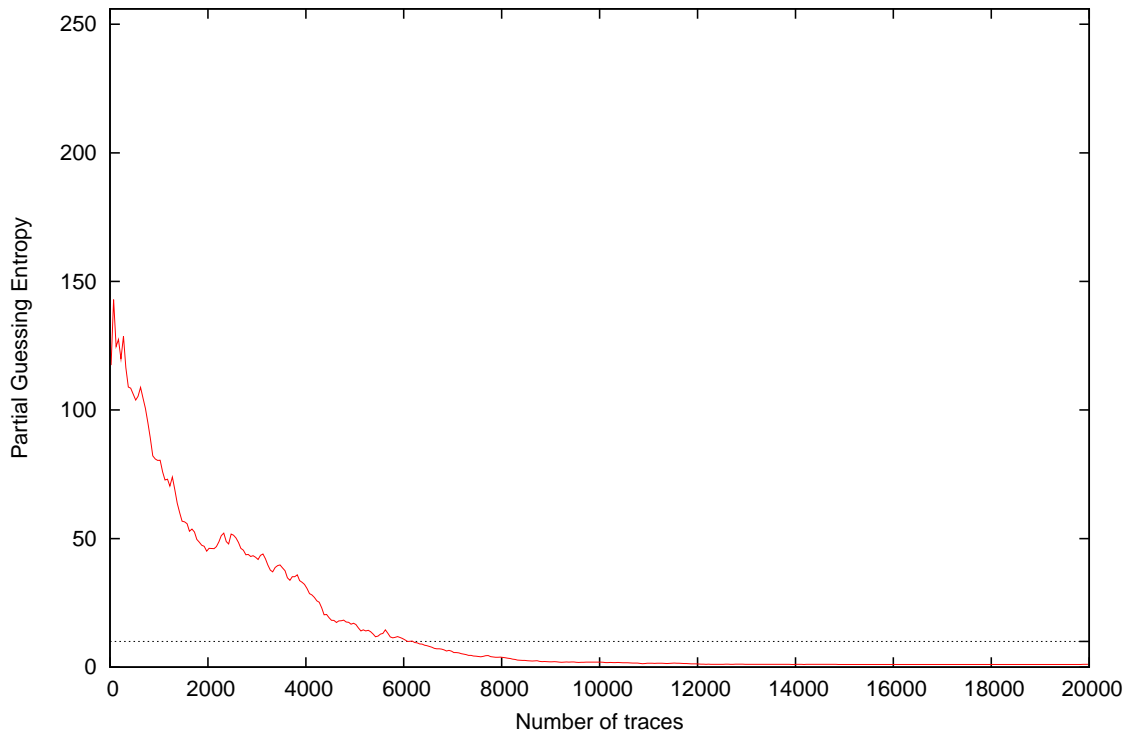
Partial Guessing Entropy for Subkey Byte #6



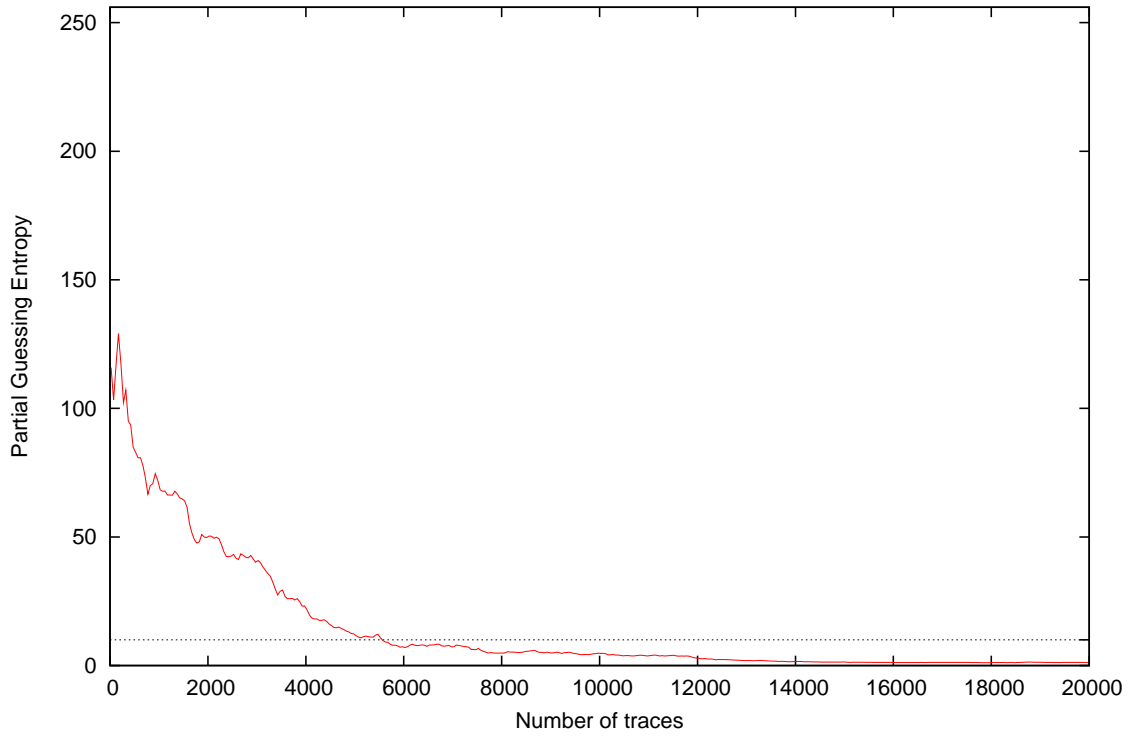
Partial Guessing Entropy for Subkey Byte #7



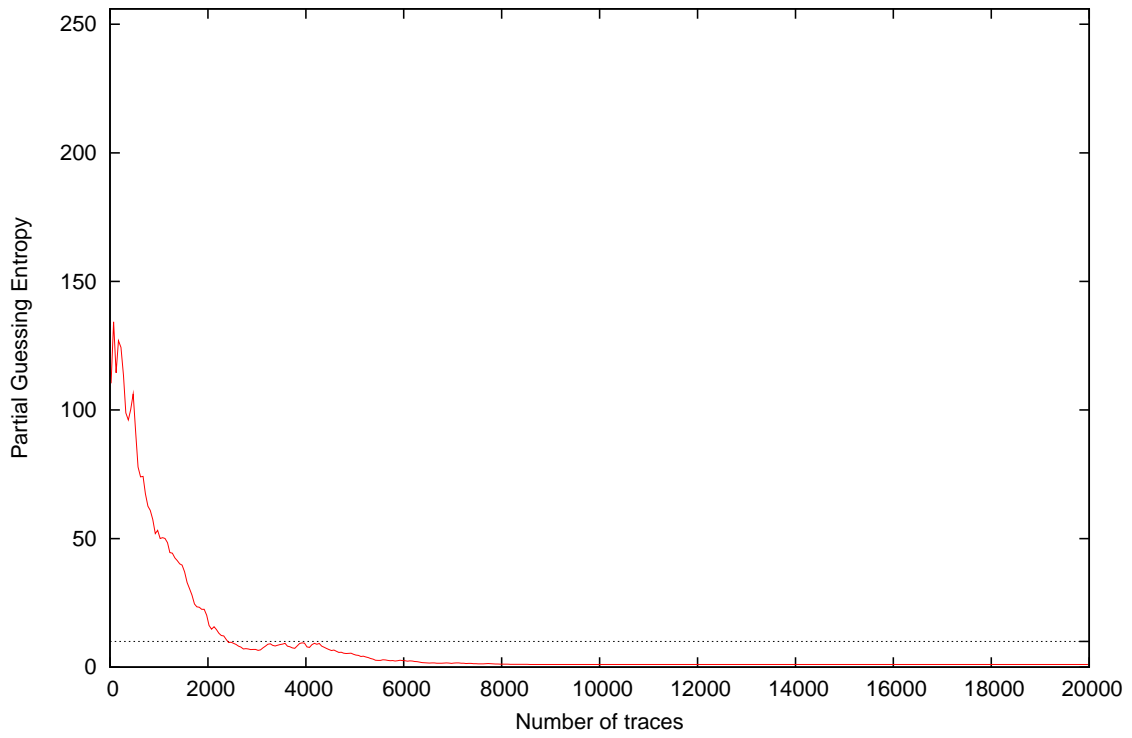
Partial Guessing Entropy for Subkey Byte #8

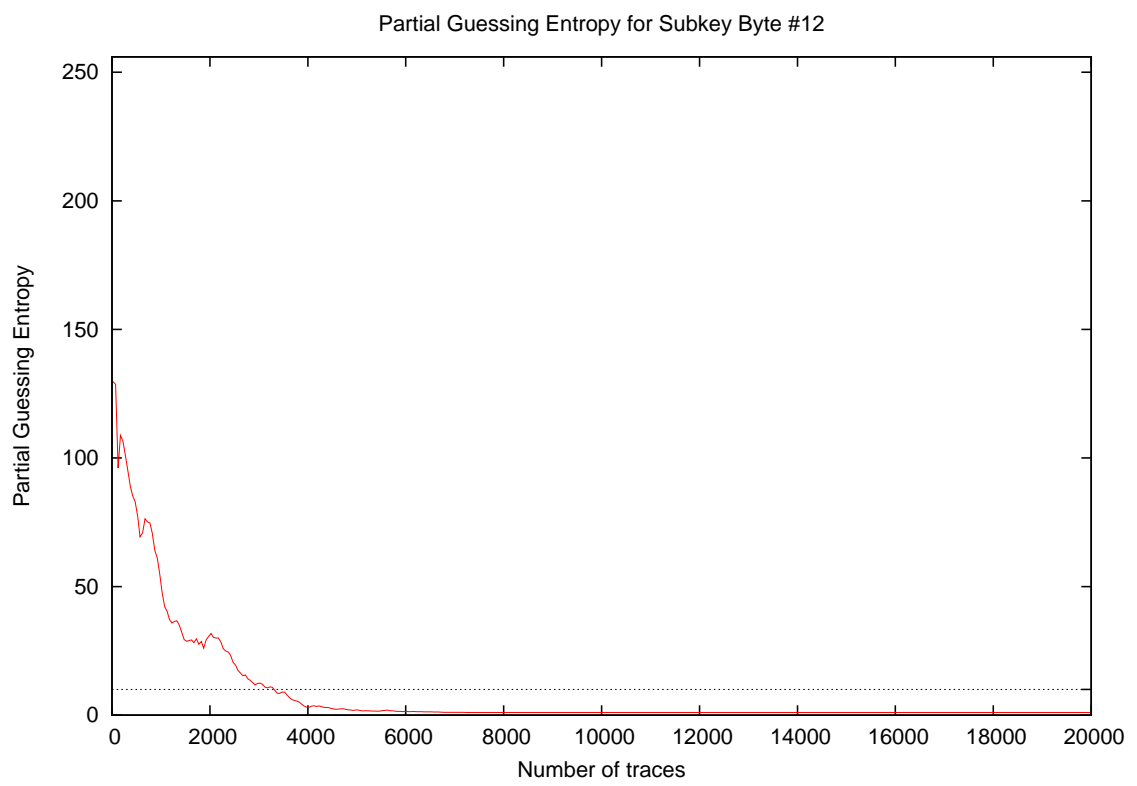
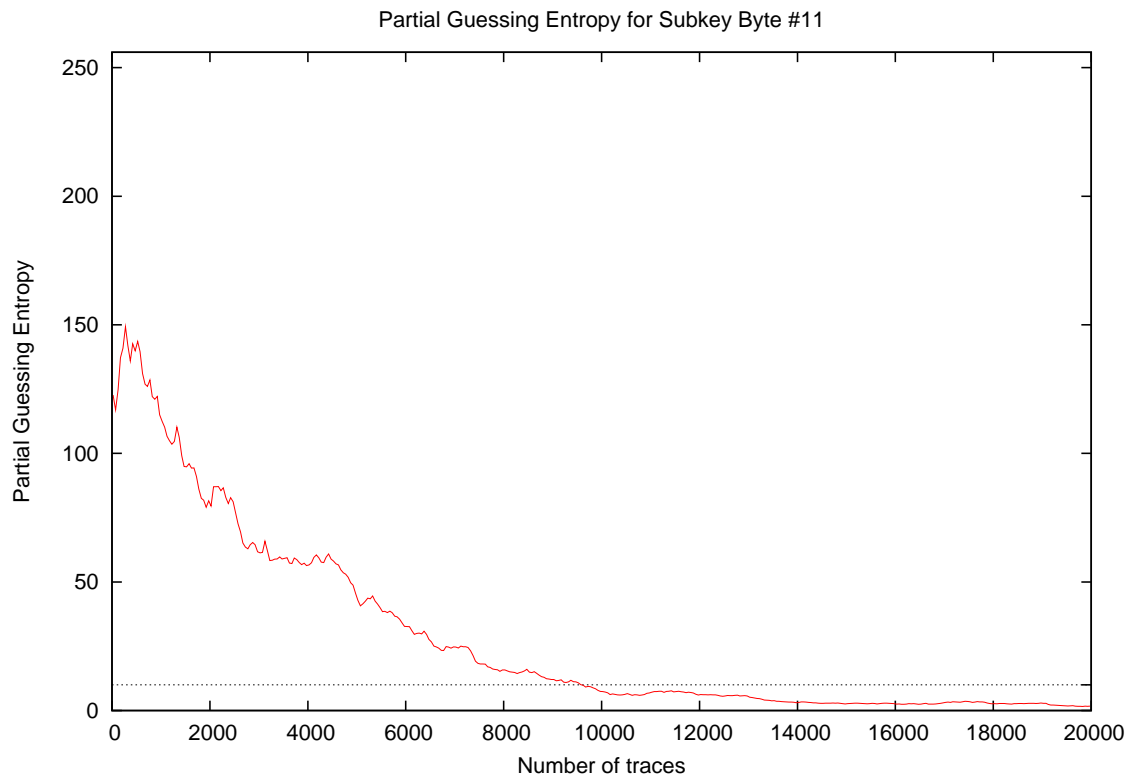


Partial Guessing Entropy for Subkey Byte #9

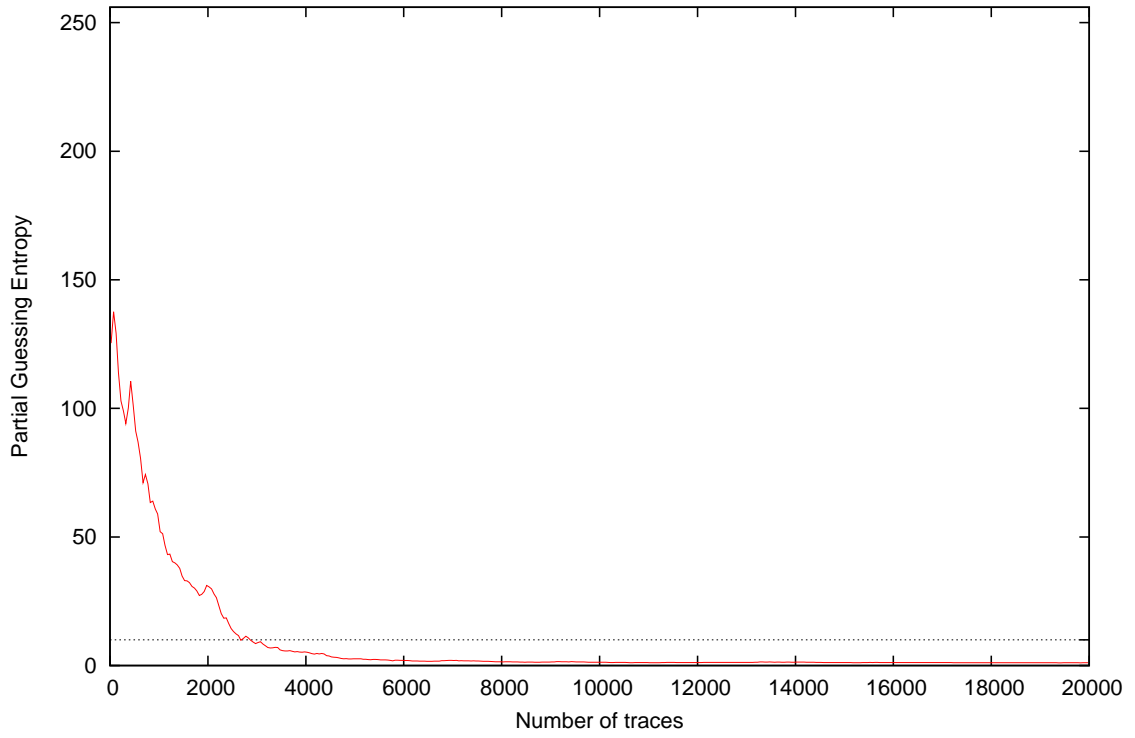


Partial Guessing Entropy for Subkey Byte #10

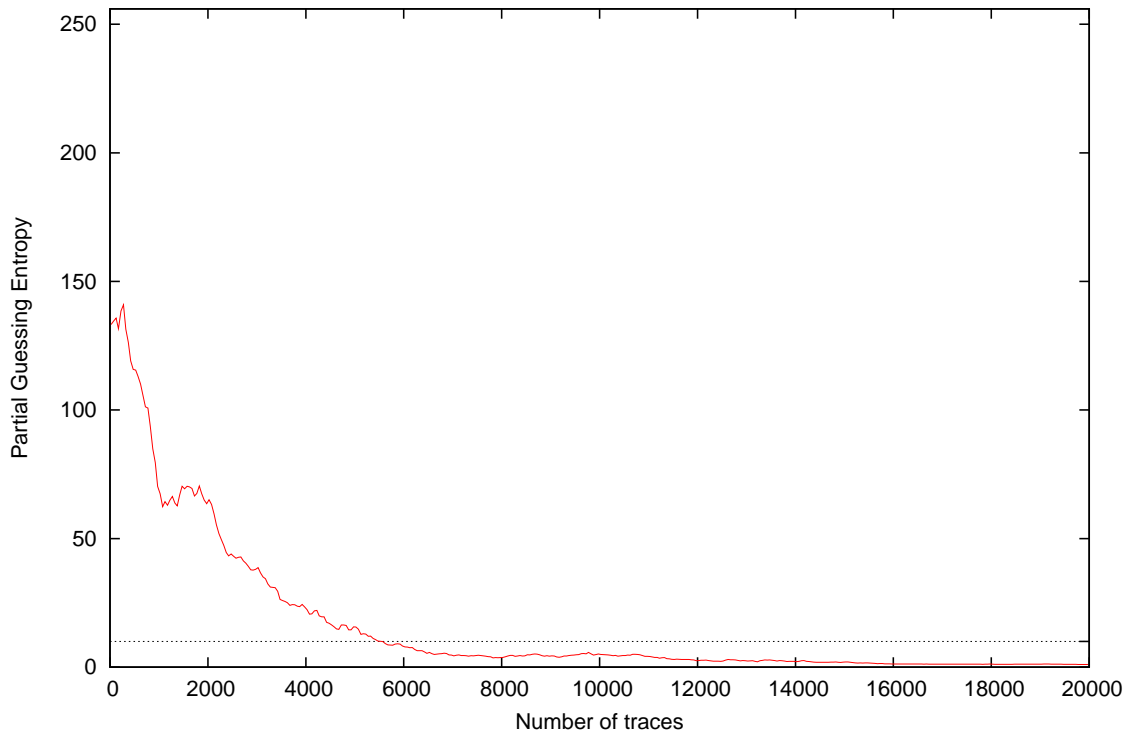


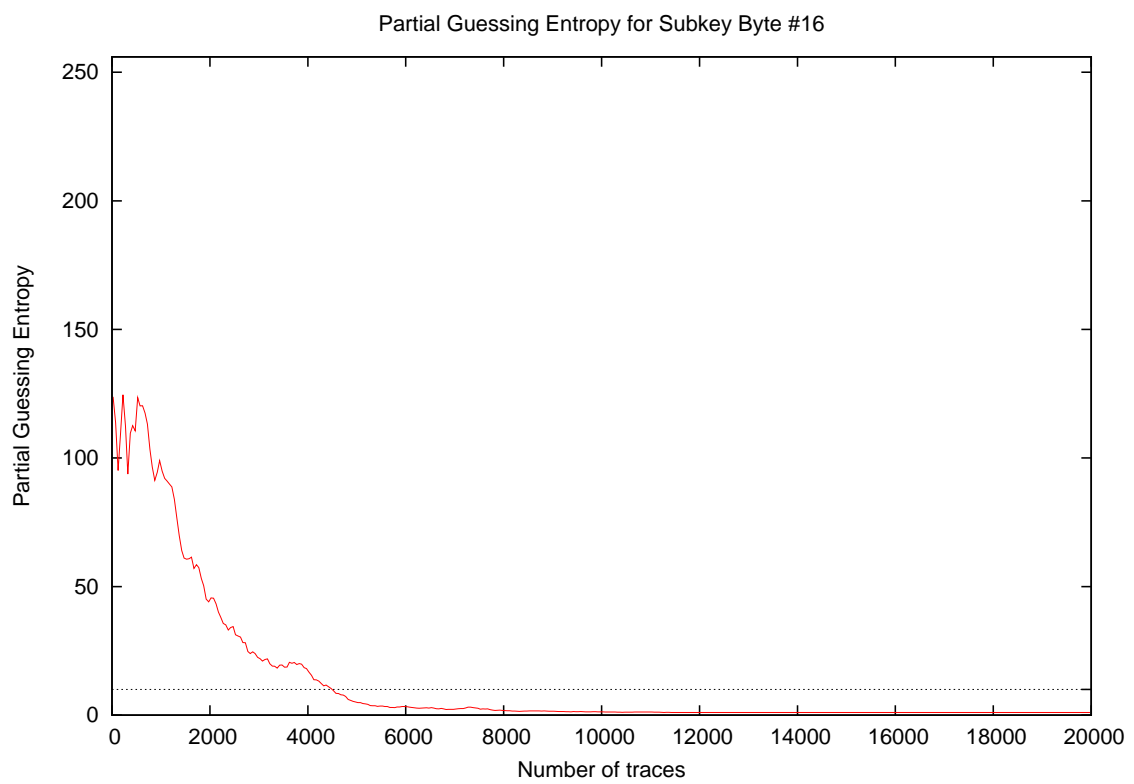
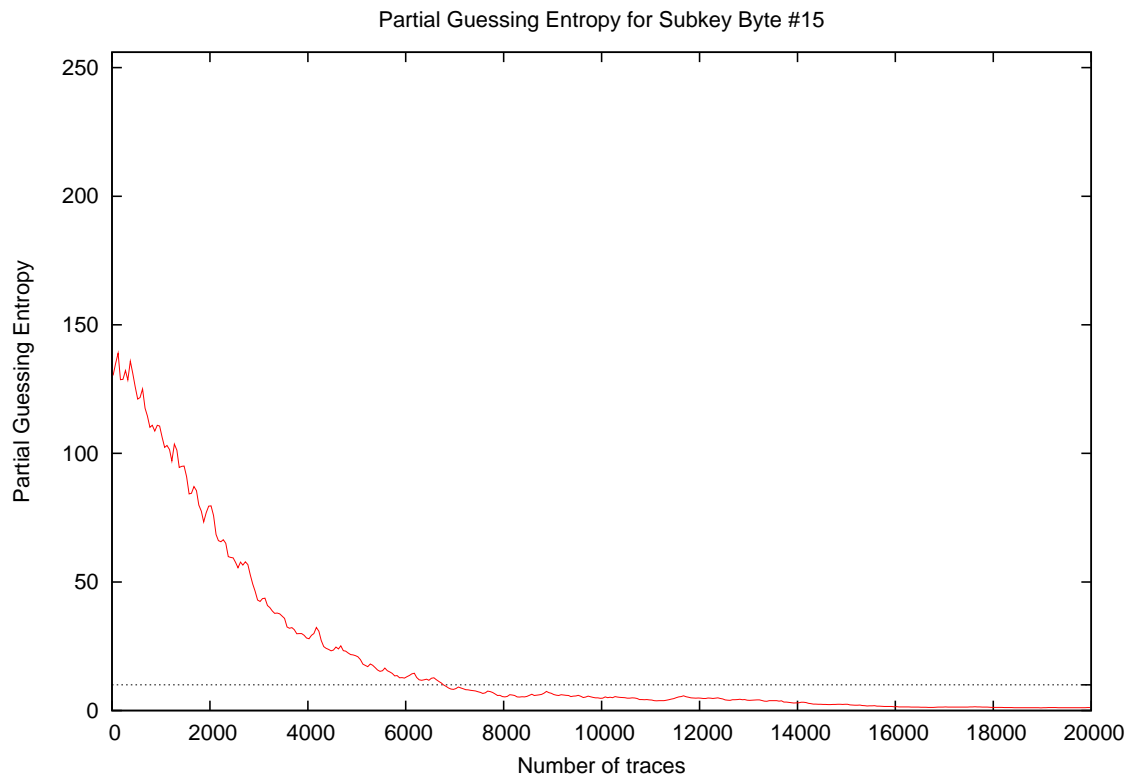


Partial Guessing Entropy for Subkey Byte #13

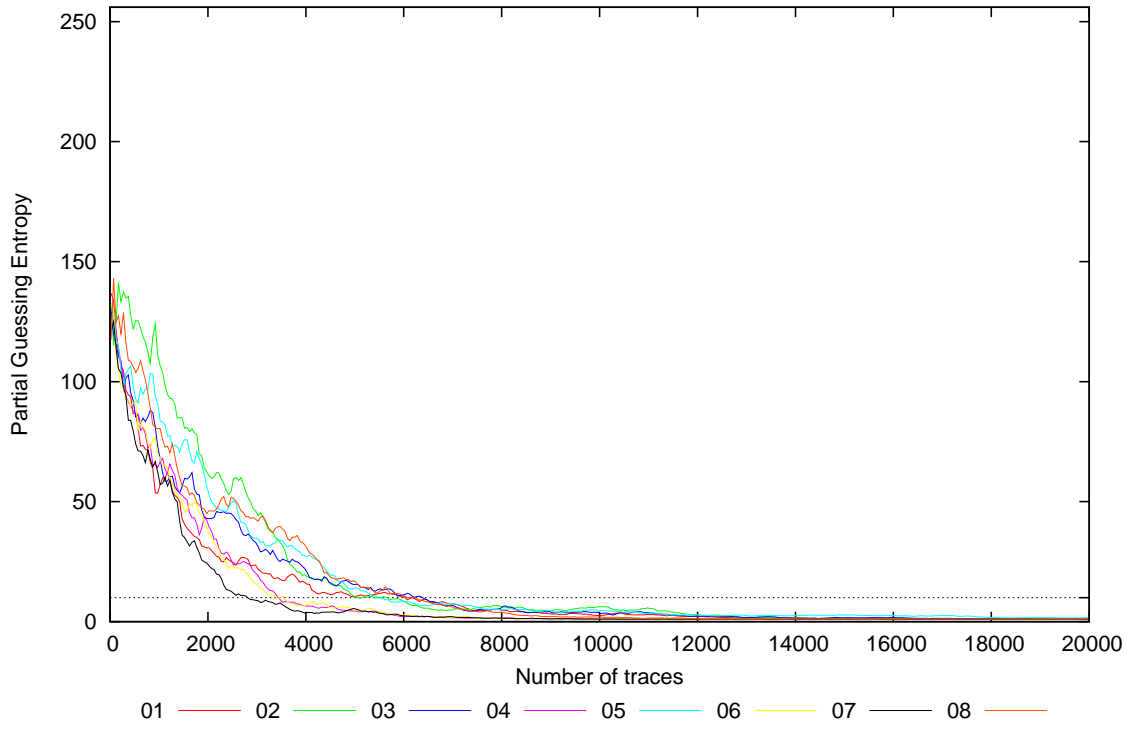


Partial Guessing Entropy for Subkey Byte #14

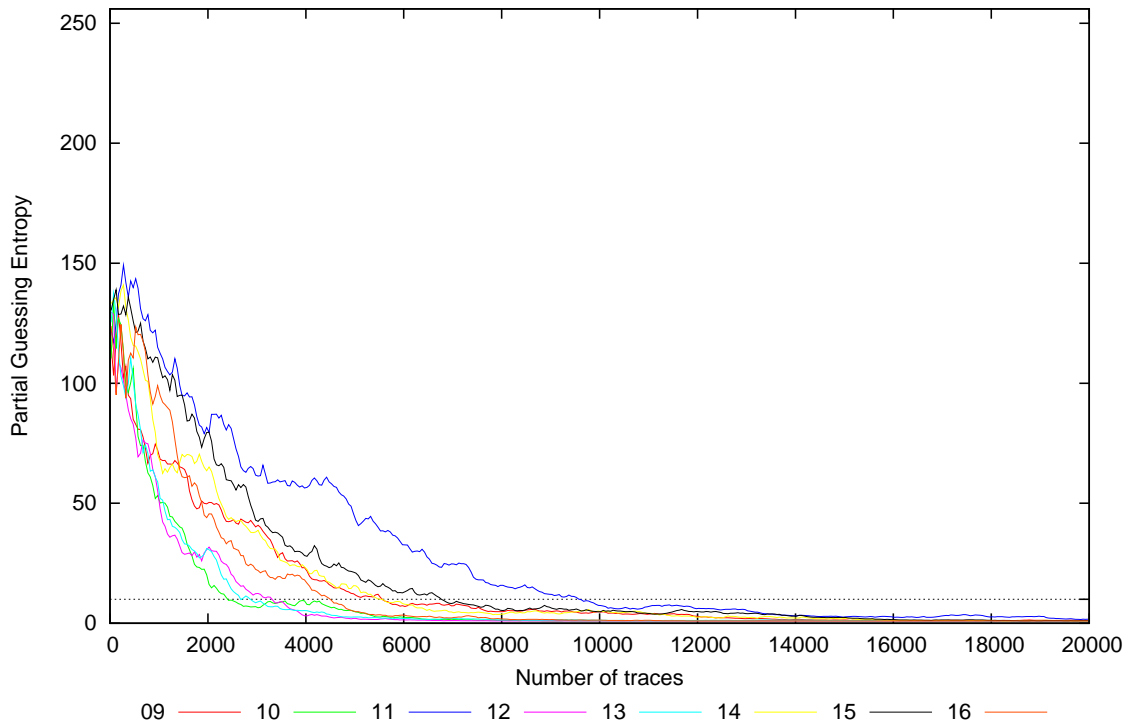


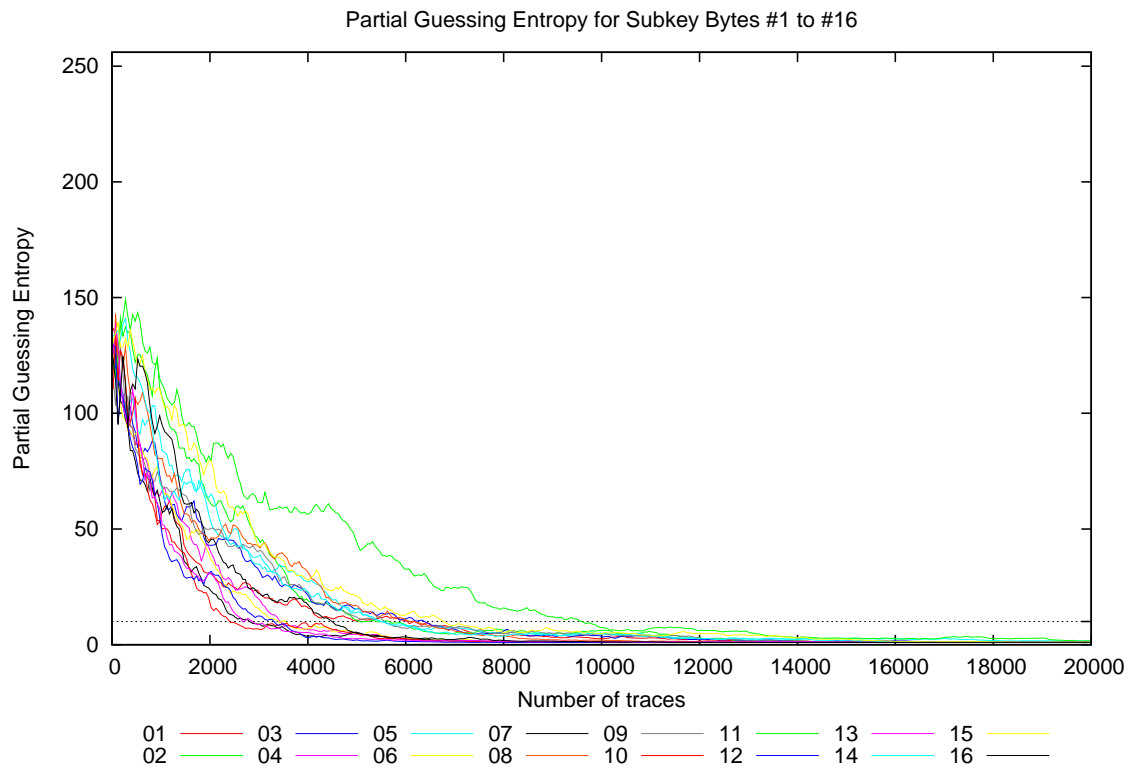


Partial Guessing Entropy for Subkey Bytes #1 to #8



Partial Guessing Entropy for Subkey Bytes #9 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	125.8	136.3	125.6	151.2	98.9	139.1	122.3	123.8	138.7	106.4	124.2	128.4	124.3	137.8	129.6	136.7	98.9	151.2	128.1
20	136.7	120.4	126.9	120.7	130.6	135.3	126.0	126.7	128.0	95.8	119.7	132.5	134.8	147.8	139.8	115.3	95.8	147.8	127.3
30	142.5	137.6	141.2	129.7	117.7	136.1	97.5	101.6	103.7	110.9	110.4	119.3	125.1	129.8	132.4	125.2	97.5	142.5	122.5
40	143.7	138.9	140.5	116.4	126.4	120.0	123.3	104.3	113.0	107.7	129.3	128.9	125.2	134.8	135.7	131.6	104.3	143.7	126.2
50	136.5	129.8	110.5	119.5	139.1	137.5	120.3	134.5	95.7	117.9	129.0	140.4	130.0	117.5	141.8	129.2	95.7	141.8	126.8
100	131.0	116.0	122.2	129.1	121.5	103.4	120.7	136.6	118.9	125.7	119.3	101.2	141.2	146.5	123.2	97.2	97.2	146.5	122.1
200	108.8	136.2	116.4	110.5	119.6	94.4	113.6	128.8	111.3	129.4	139.1	103.1	107.6	131.2	124.5	119.2	94.4	139.1	118.4
300	98.5	139.8	97.0	92.2	93.7	95.7	98.8	127.3	104.1	105.5	149.2	99.5	93.0	129.8	128.4	102.7	92.2	149.2	109.7
400	94.9	135.4	97.4	84.5	102.9	89.7	78.6	108.0	93.7	92.7	139.1	84.0	106.5	119.4	136.2	112.2	78.6	139.1	104.7
500	83.5	127.0	91.4	89.7	98.4	92.4	77.7	105.1	79.9	97.7	139.9	79.6	96.0	114.2	124.6	114.9	77.7	139.9	100.7
1000	55.4	107.9	72.1	65.7	86.0	71.8	59.9	81.2	70.3	51.0	115.7	48.7	57.6	66.1	110.2	97.9	48.7	115.7	76.1
2000	31.3	62.7	43.1	41.3	54.2	37.0	23.6	44.8	50.4	17.9	80.8	31.2	33.2	64.1	80.7	44.2	17.9	80.8	46.3
3000	23.4	45.2	32.8	20.5	35.0	16.3	8.9	40.6	39.4	6.7	60.6	12.1	8.7	38.4	41.4	21.4	6.7	60.6	28.2
4000	15.5	18.9	21.9	5.8	27.1	6.8	3.6	31.8	22.7	8.8	55.9	3.0	5.3	22.5	27.3	16.9	3.0	55.9	18.4
5000	10.5	10.9	15.3	4.5	14.1	4.9	5.2	17.2	12.5	4.8	45.8	2.2	2.6	16.0	21.5	4.9	2.2	45.8	12.0
10000	2.6	6.3	3.6	1.0	4.4	1.2	1.1	1.9	4.8	1.0	7.5	1.0	1.2	5.0	4.8	1.3	1.0	7.5	3.0
15000	1.3	1.3	1.6	1.0	2.8	1.0	1.0	1.0	1.4	1.0	2.7	1.0	1.1	2.1	2.4	1.0	1.0	2.8	1.5
20000	1.1	1.0	1.0	1.0	1.7	1.0	1.0	1.1	1.2	1.0	1.7	1.0	1.1	1.0	1.1	1.0	1.0	1.7	1.1