

Evaluation results

DPA contest v2

November 2010

1 Introduction

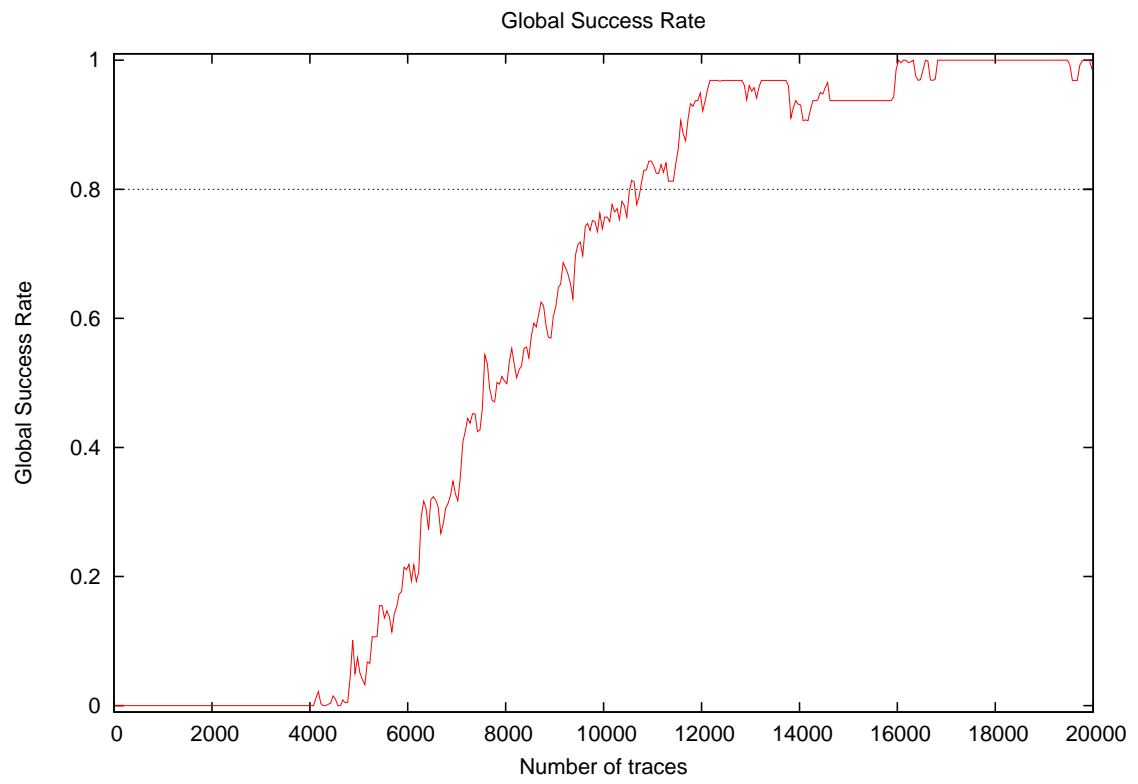
1.1 About the attack

- **Attack Name:** CPA AP SBOX PRD2
- **Sender/Team:** Maël Berthier, Yves Bocktaels
- **Institution:** Morpho, France
- **Language:** Matlab
- **Attacked subkey:** 10

1.2 About the evaluation

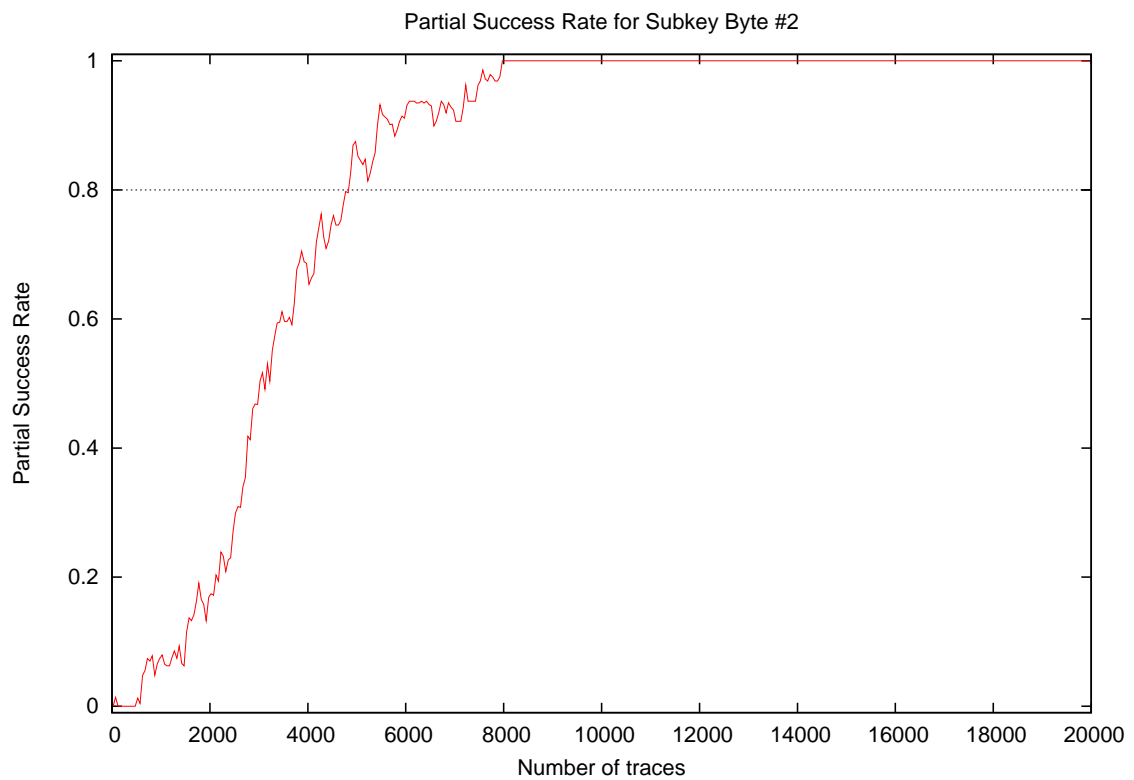
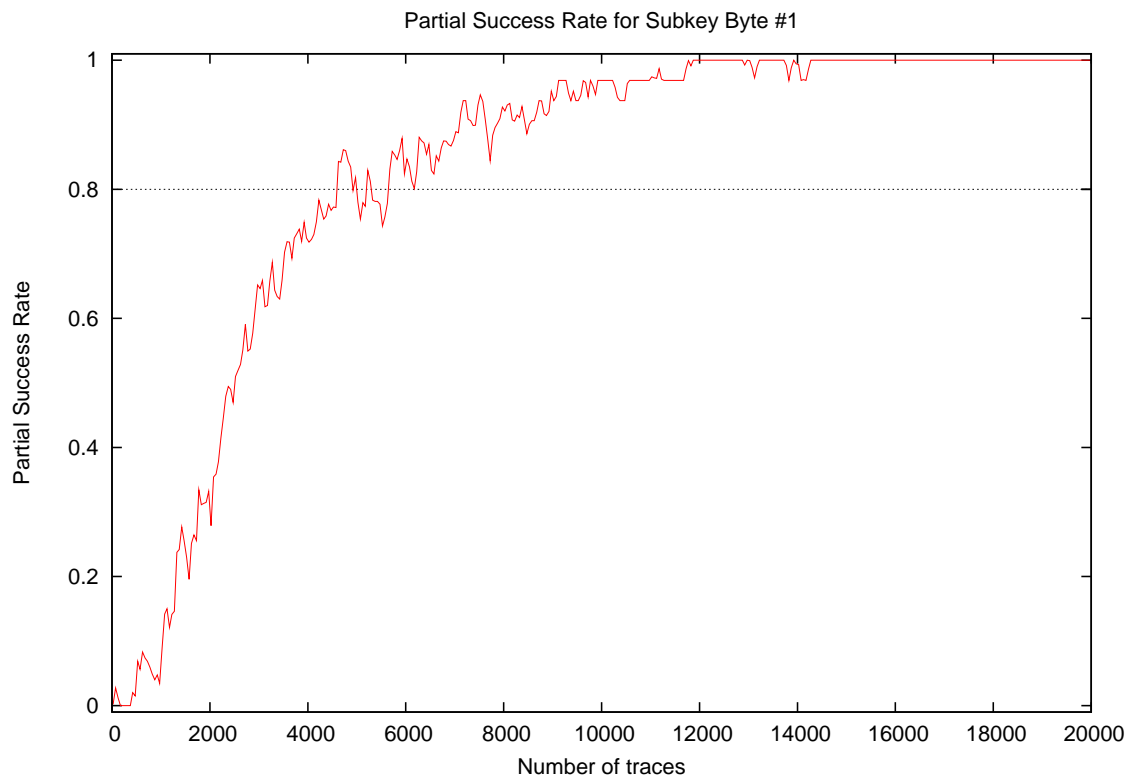
- **Date of evaluation:** November 2010

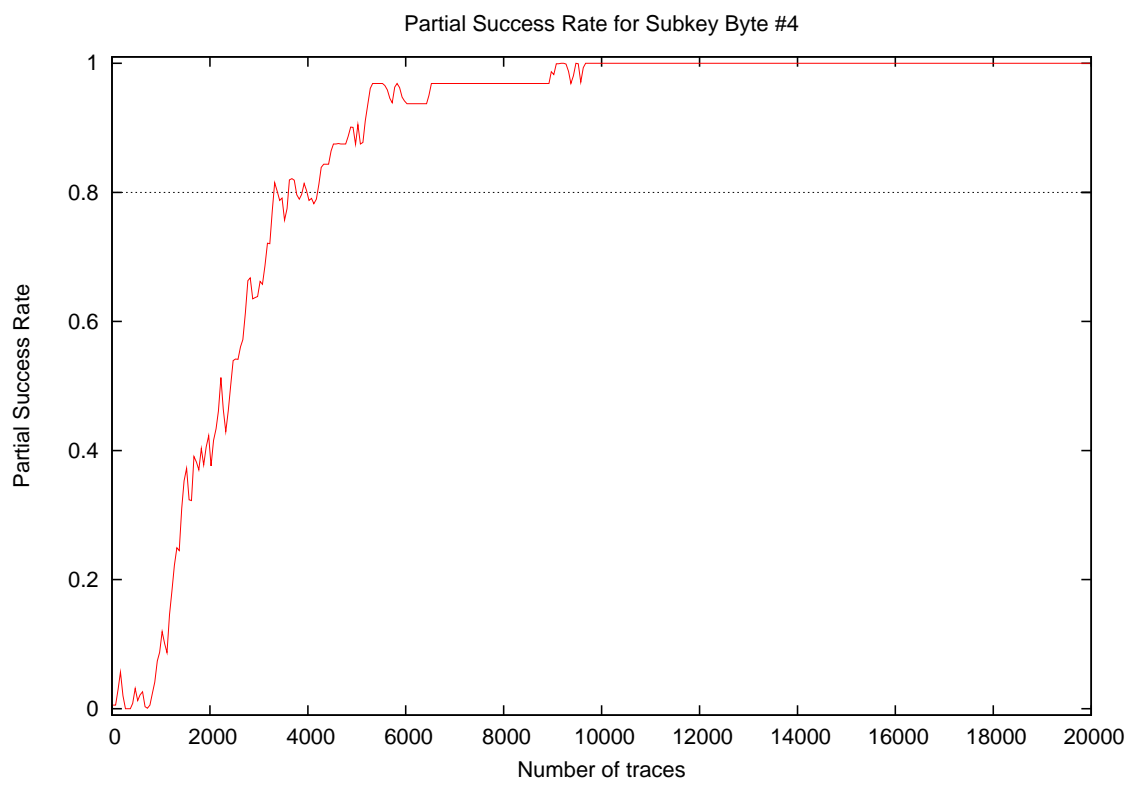
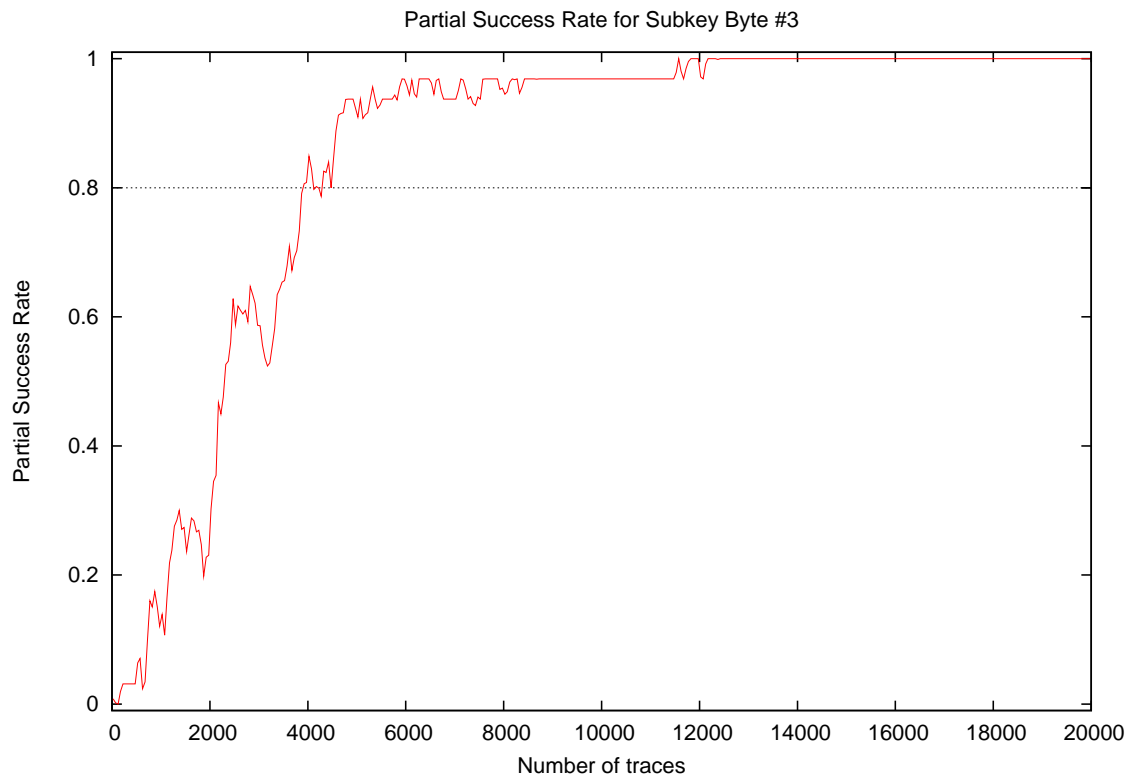
2 Global Success Rate

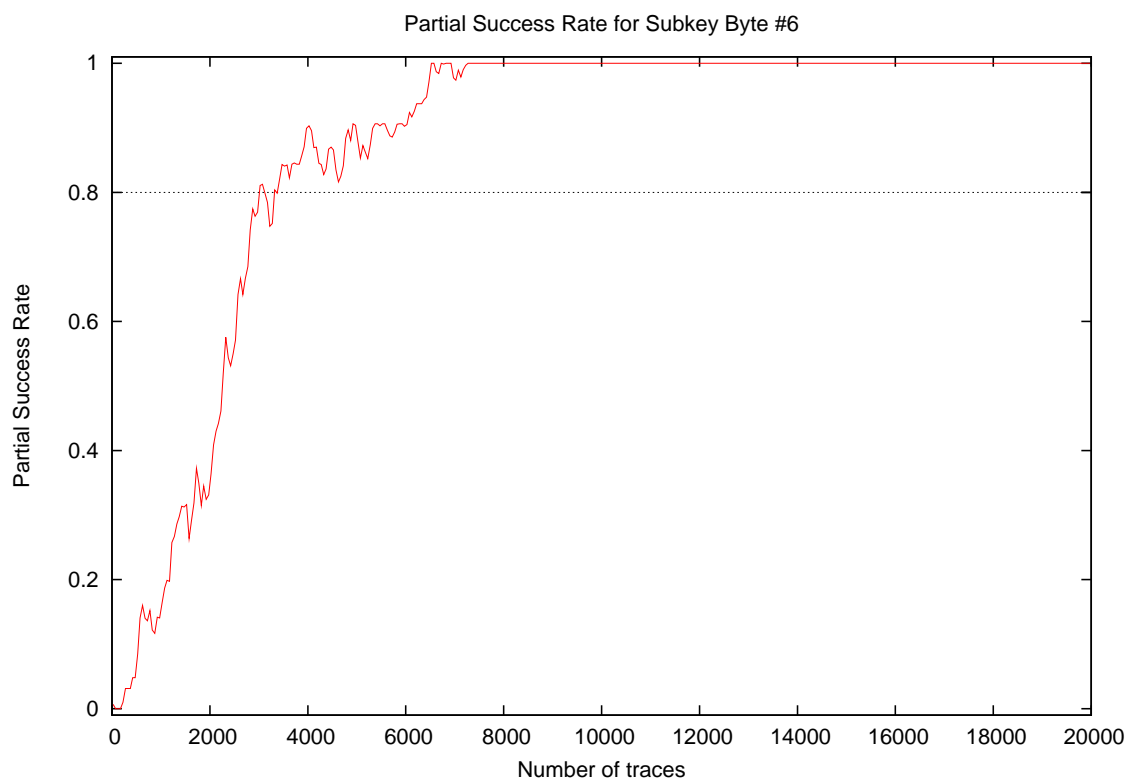
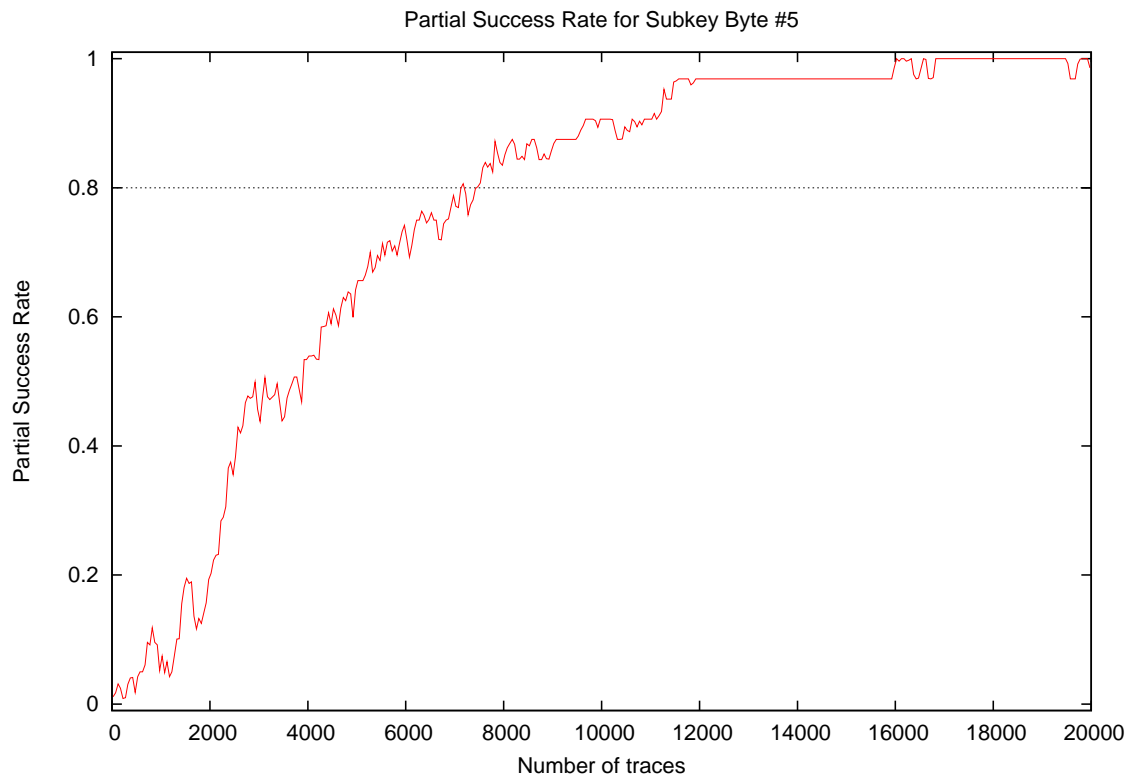


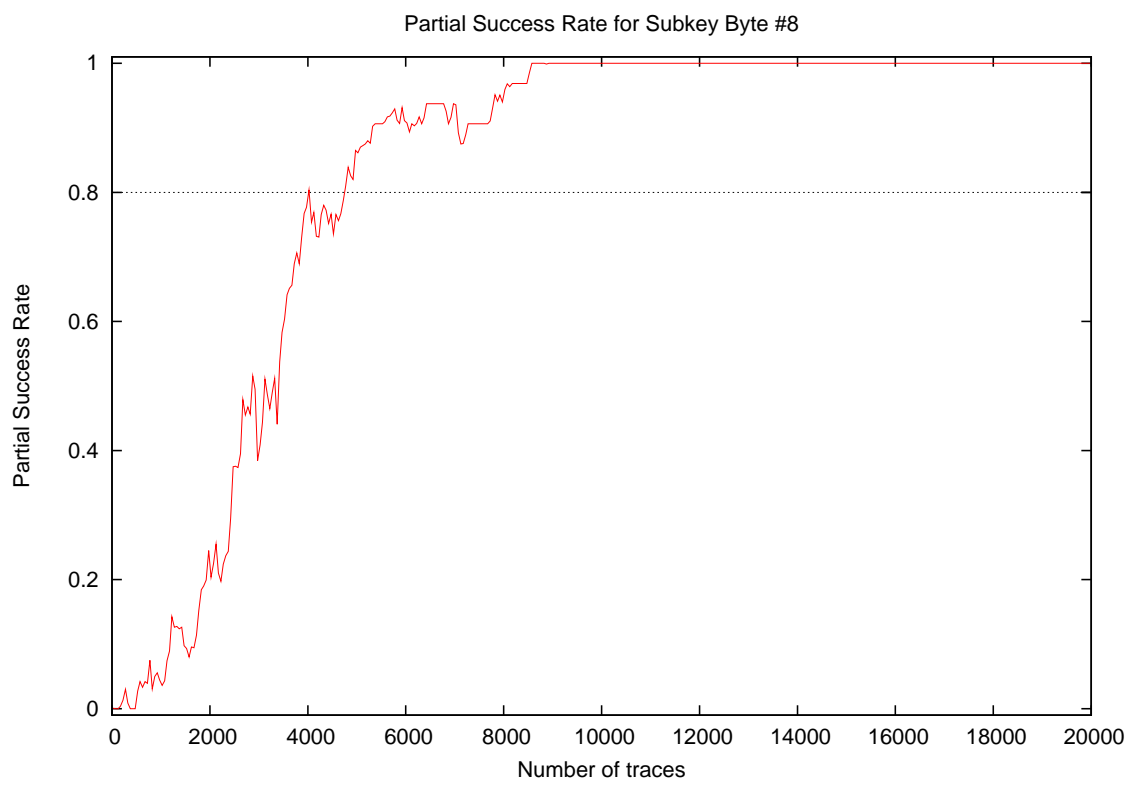
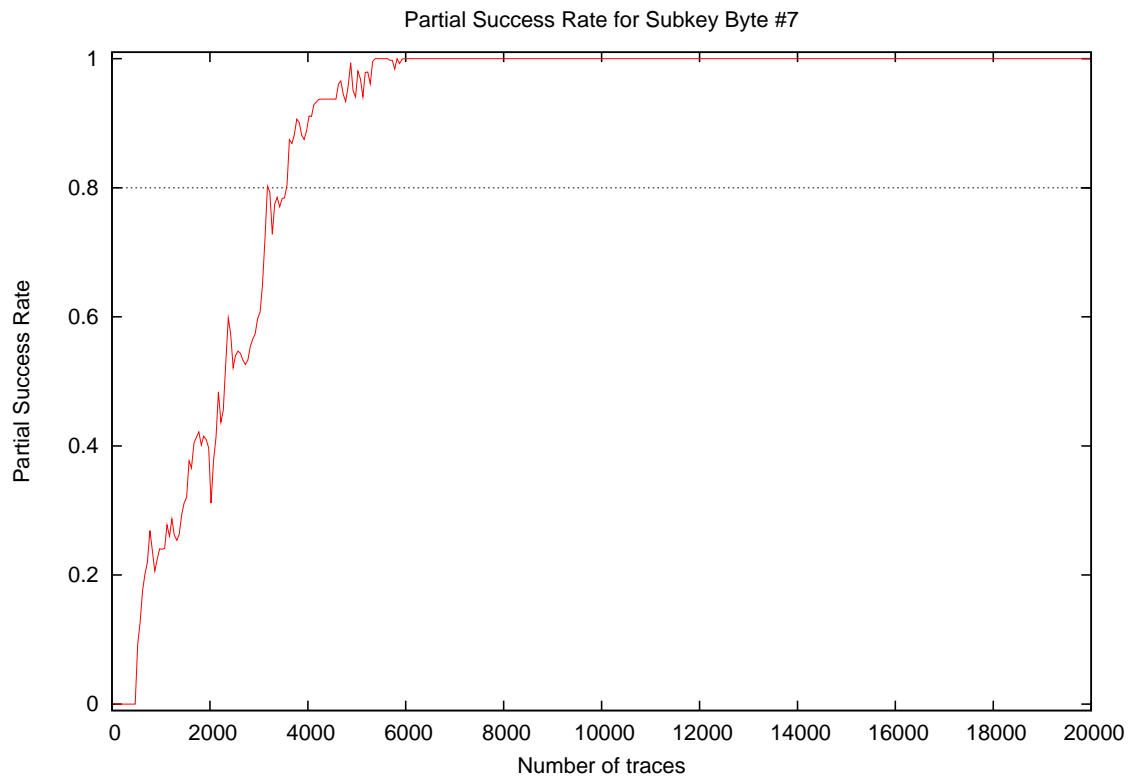
Number of traces	Global Success Rate
10	0.00
20	0.00
30	0.00
40	0.00
50	0.00
100	0.00
200	0.00
300	0.00
400	0.00
500	0.00
1000	0.00
2000	0.00
3000	0.00
4000	0.00
5000	0.09
10000	0.75
15000	0.94
20000	0.97

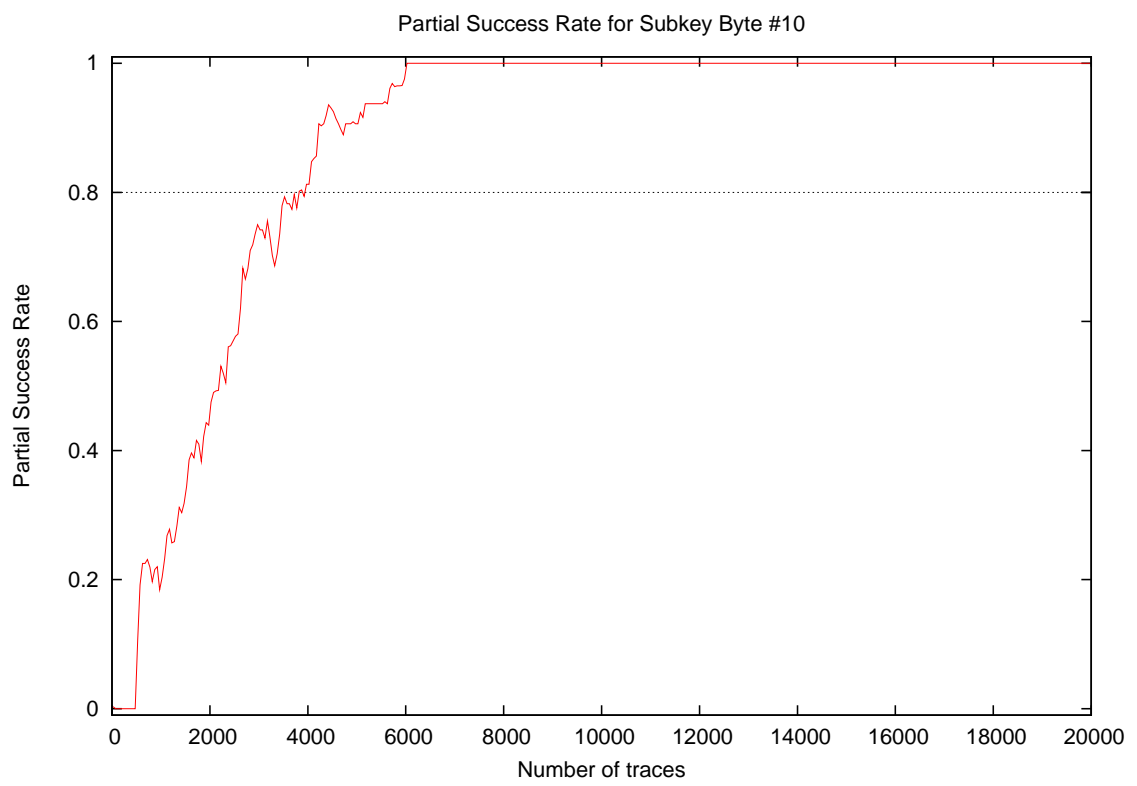
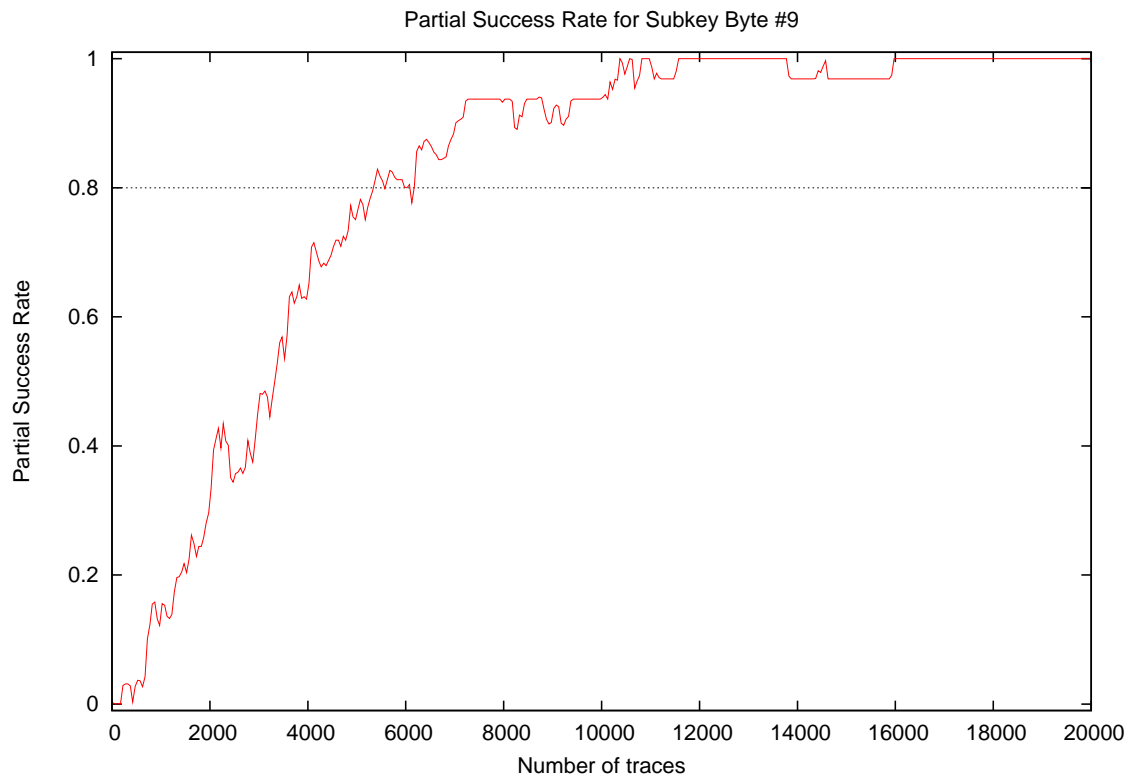
3 Partial Success Rate

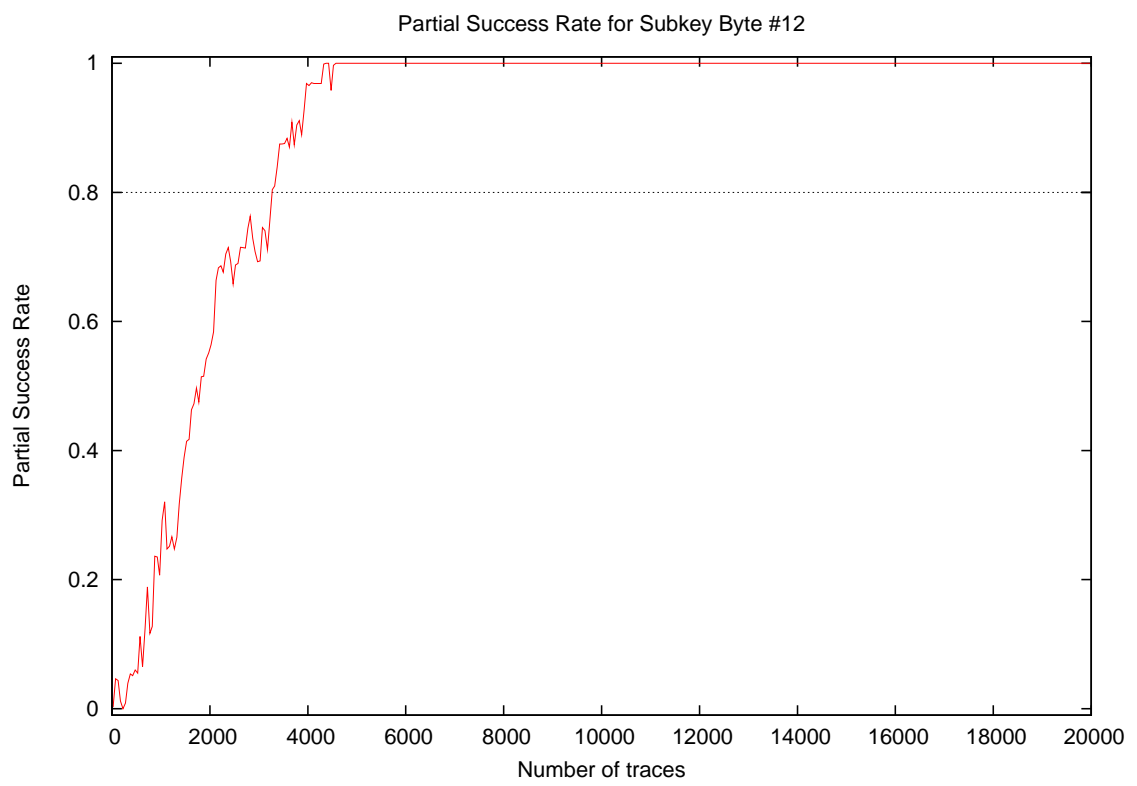
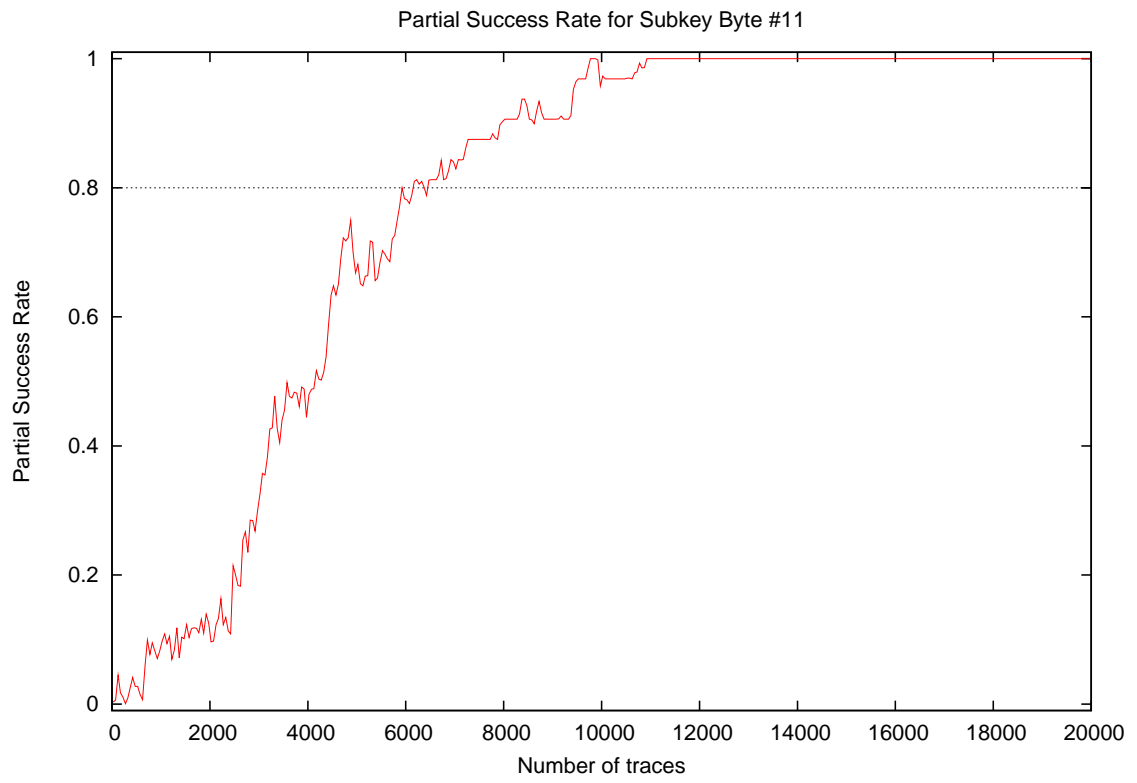


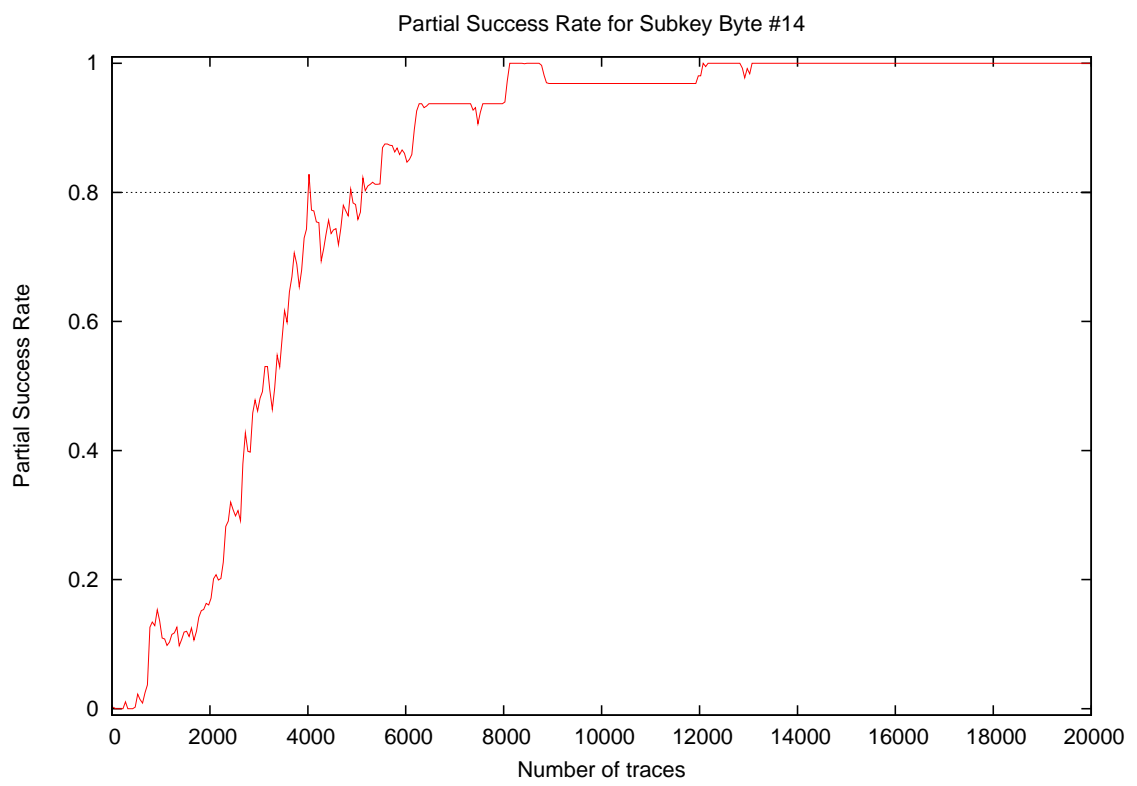
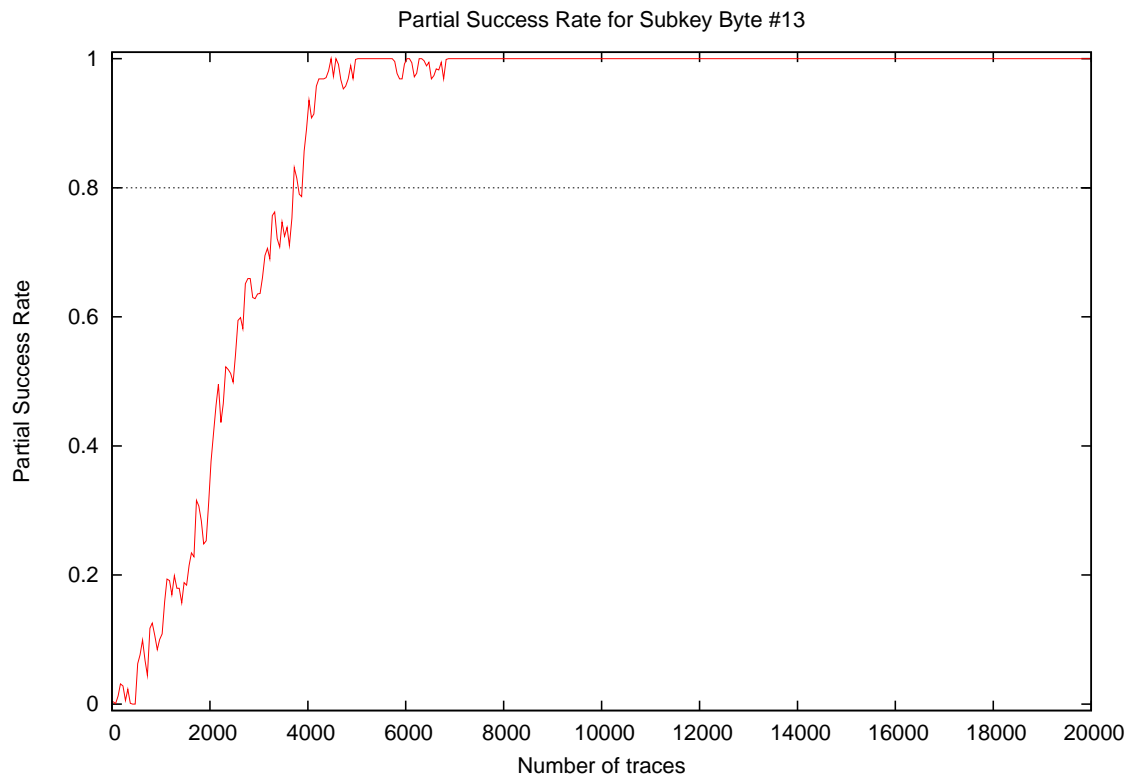


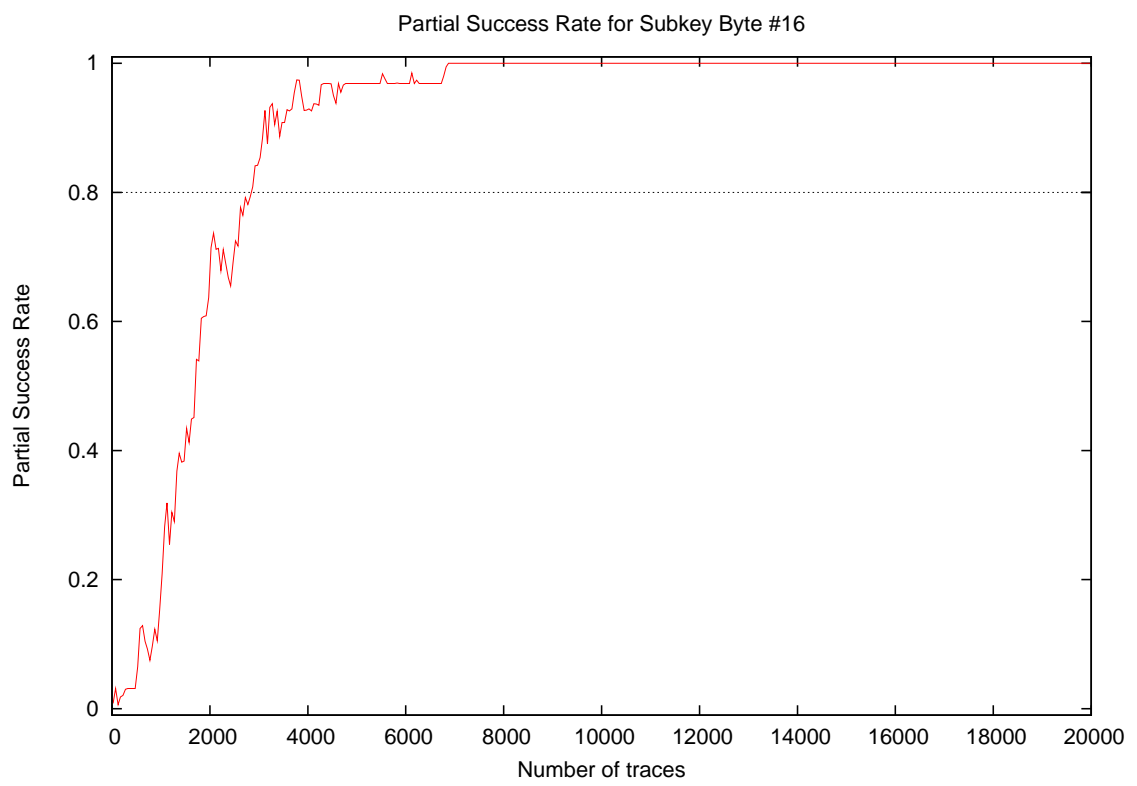
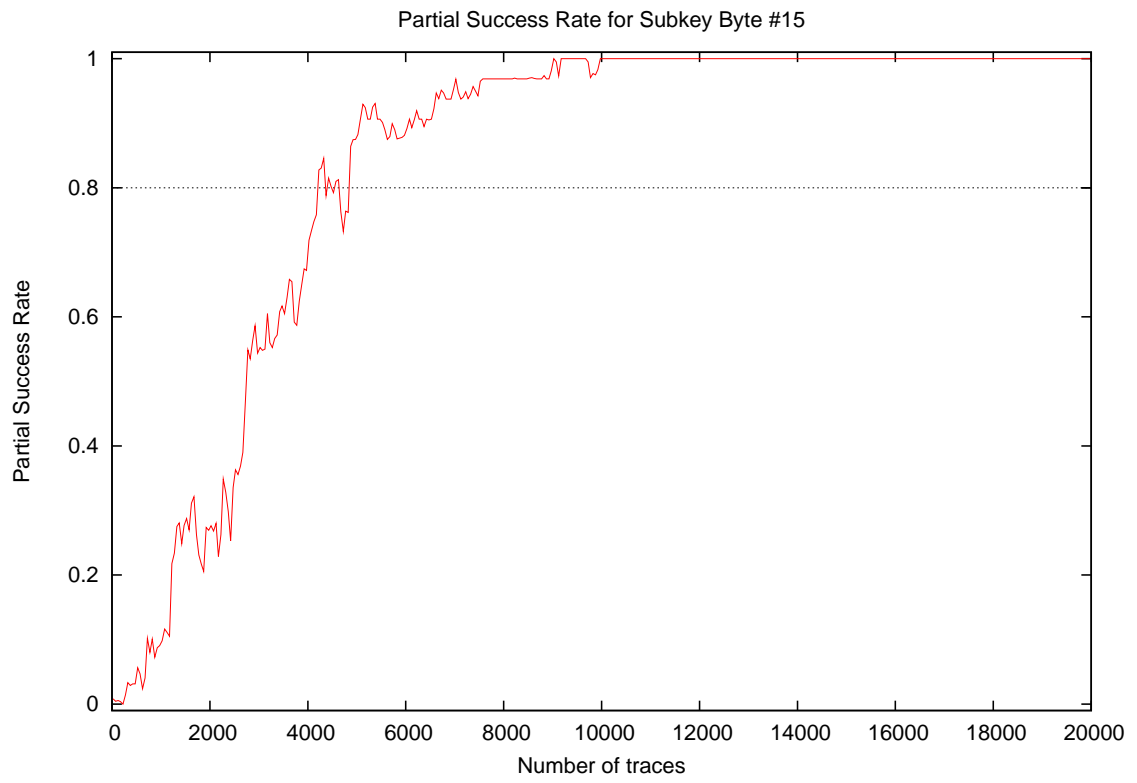


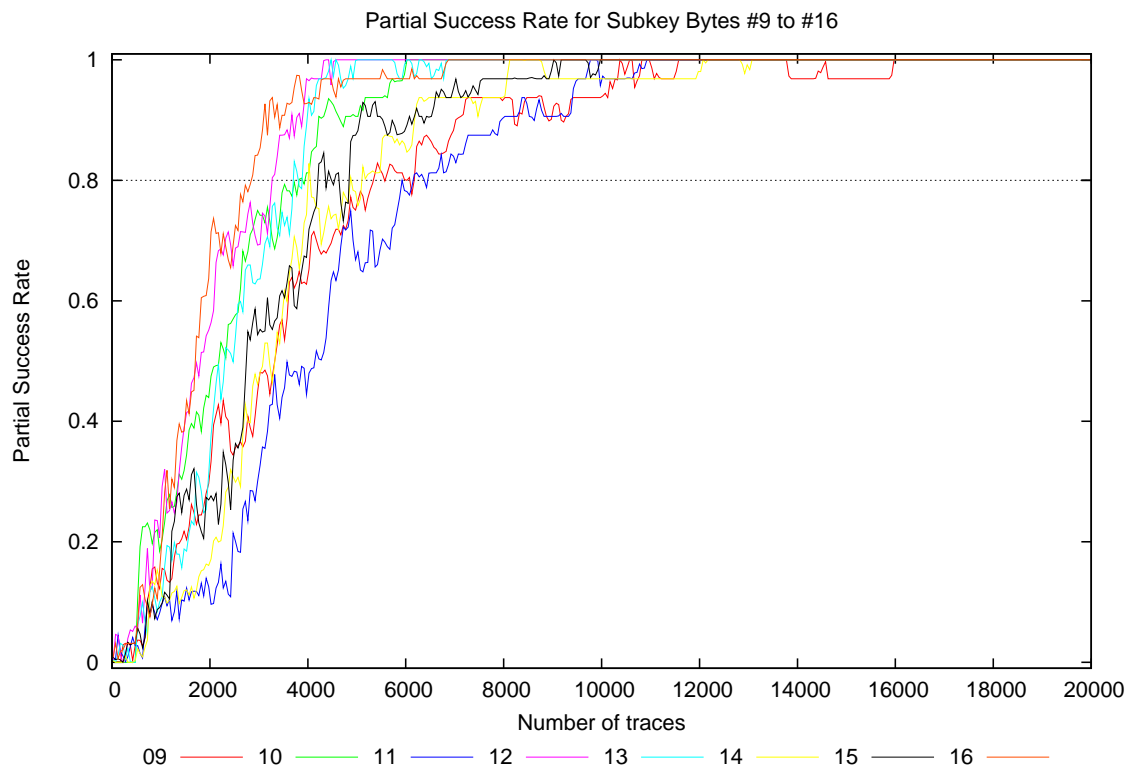
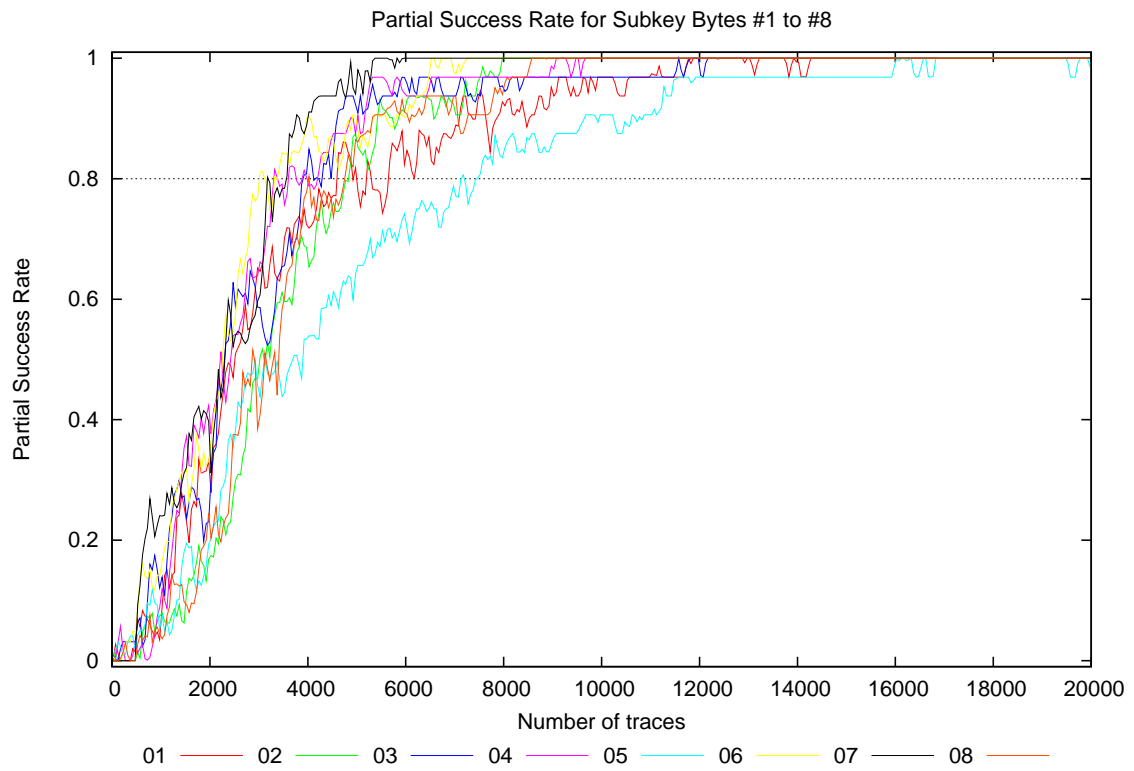


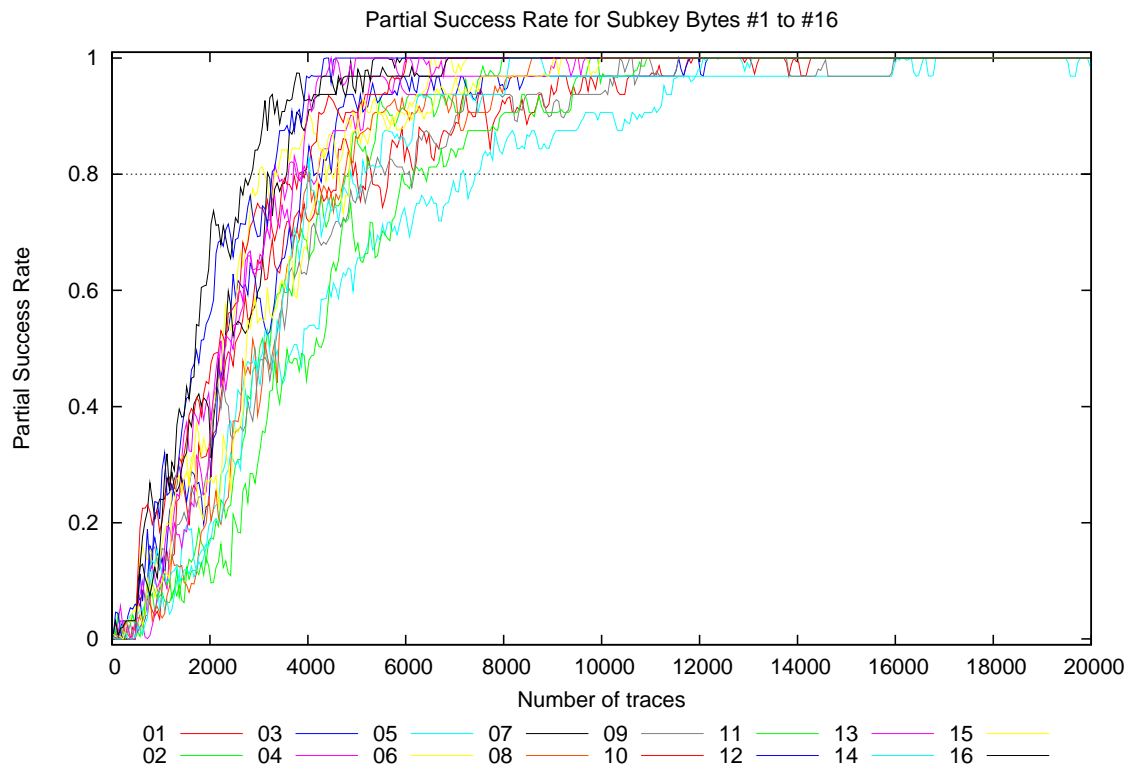






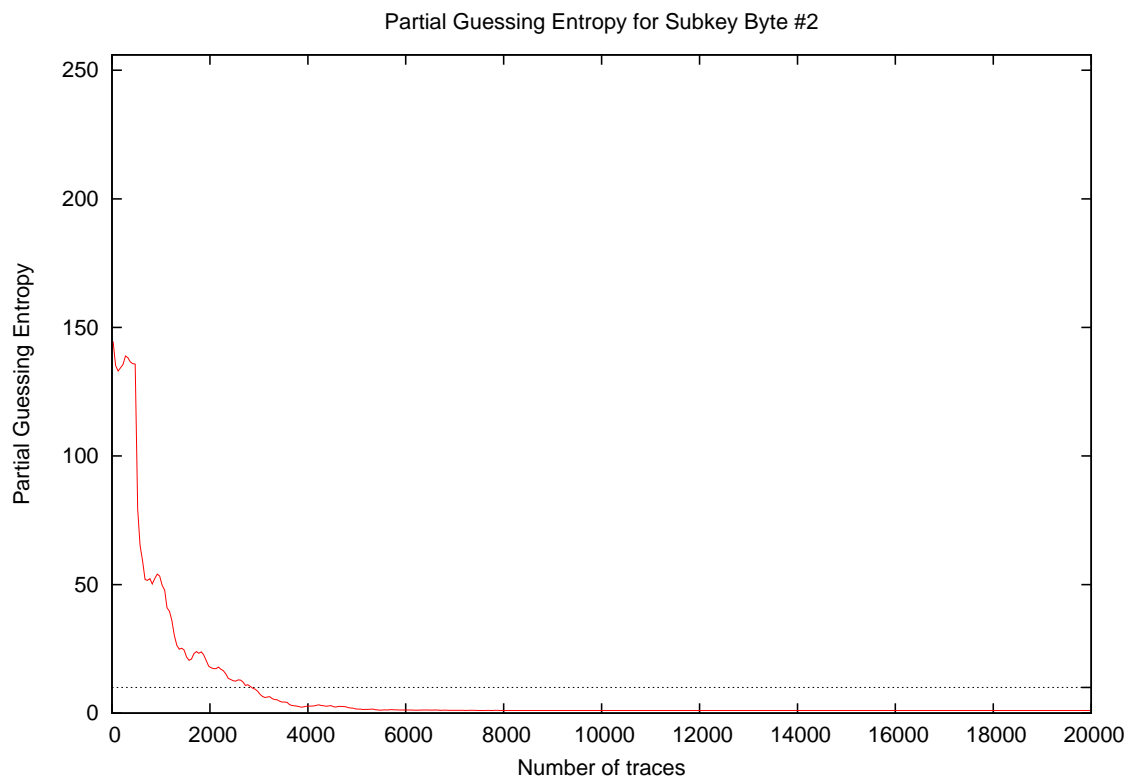
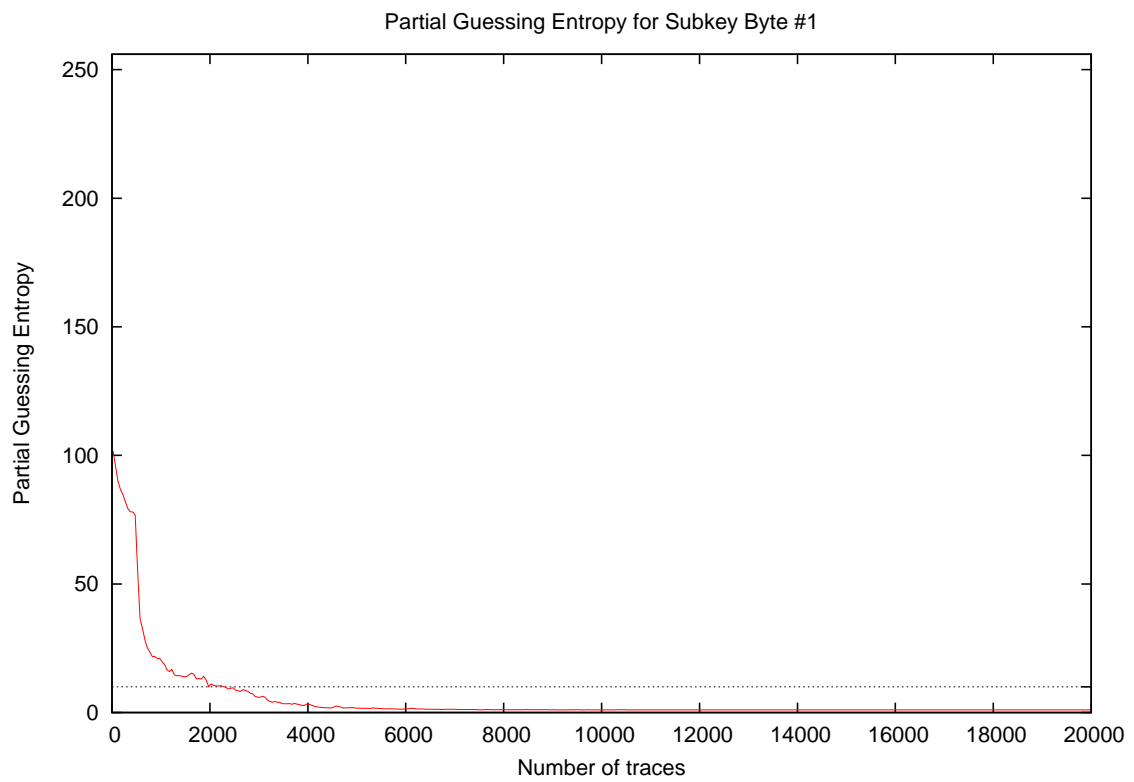




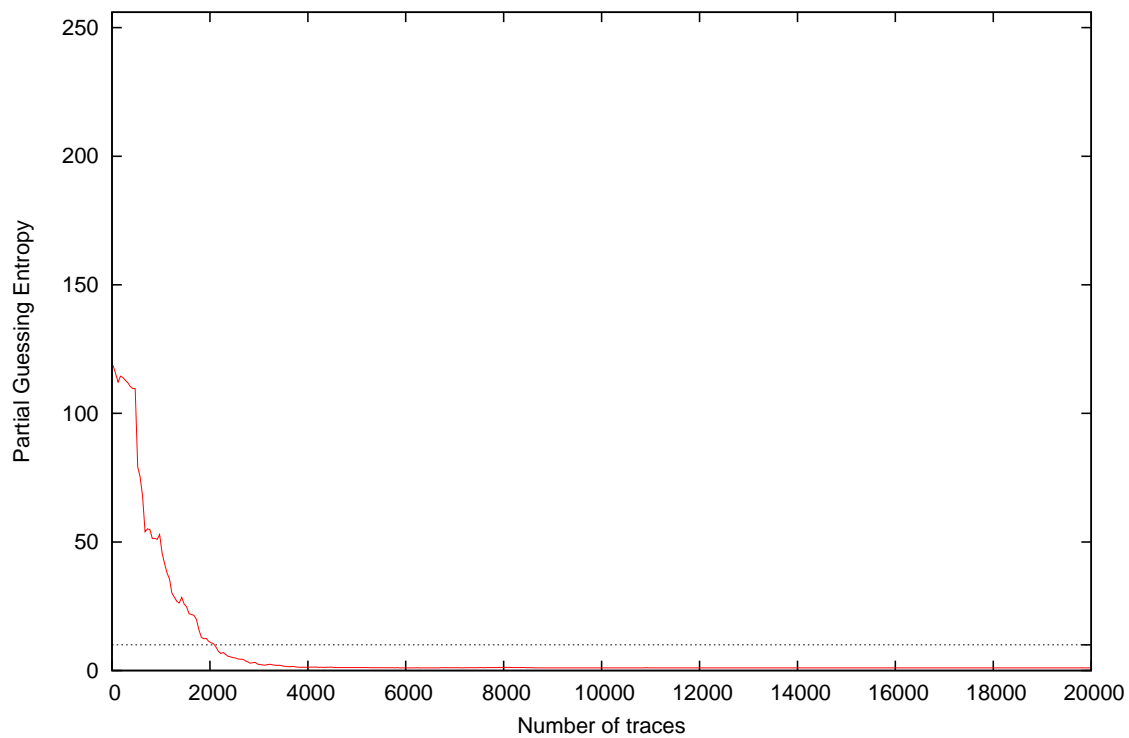


Traces	Partial Success Rate / Byte																Min	Max	Mean
	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16			
10	0.00	0.00	0.03	0.00	0.00	0.03	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.03	0.00
20	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
30	0.00	0.00	0.00	0.00	0.00	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
40	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
50	0.03	0.00	0.00	0.03	0.00	0.00	0.00	0.00	0.00	0.00	0.03	0.06	0.00	0.00	0.00	0.00	0.03	0.03	0.01
100	0.00	0.00	0.00	0.00	0.03	0.00	0.00	0.00	0.00	0.03	0.06	0.00	0.00	0.00	0.00	0.00	0.06	0.06	0.01
200	0.00	0.00	0.03	0.06	0.03	0.00	0.00	0.03	0.00	0.00	0.00	0.00	0.03	0.00	0.00	0.00	0.06	0.06	0.01
300	0.00	0.00	0.03	0.00	0.03	0.03	0.00	0.03	0.00	0.00	0.06	0.06	0.00	0.00	0.03	0.03	0.06	0.06	0.02
400	0.00	0.00	0.03	0.00	0.03	0.03	0.00	0.00	0.00	0.03	0.06	0.06	0.00	0.00	0.03	0.03	0.06	0.06	0.02
500	0.03	0.00	0.03	0.03	0.03	0.06	0.00	0.00	0.06	0.00	0.06	0.09	0.00	0.00	0.03	0.03	0.09	0.09	0.03
1000	0.09	0.06	0.09	0.03	0.03	0.16	0.25	0.06	0.09	0.19	0.06	0.25	0.06	0.12	0.09	0.16	0.25	0.25	0.11
2000	0.25	0.22	0.28	0.38	0.22	0.34	0.38	0.25	0.31	0.47	0.12	0.53	0.34	0.16	0.28	0.66	0.66	0.66	0.32
3000	0.62	0.41	0.62	0.69	0.44	0.78	0.62	0.44	0.50	0.75	0.34	0.72	0.69	0.50	0.50	0.84	0.84	0.84	0.59
4000	0.72	0.69	0.81	0.78	0.53	0.91	0.94	0.78	0.62	0.81	0.50	0.97	0.91	0.78	0.72	0.94	0.97	0.97	0.78
5000	0.81	0.88	0.91	0.91	0.66	0.88	0.97	0.88	0.75	0.91	0.69	1.00	1.00	0.78	0.88	0.97	1.00	1.00	0.87
10000	0.97	1.00	0.97	1.00	0.91	1.00	1.00	1.00	0.94	1.00	0.97	1.00	1.00	0.97	1.00	1.00	1.00	1.00	0.98
15000	1.00	1.00	1.00	1.00	0.97	1.00	1.00	1.00	0.97	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
20000	1.00	1.00	1.00	1.00	0.97	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

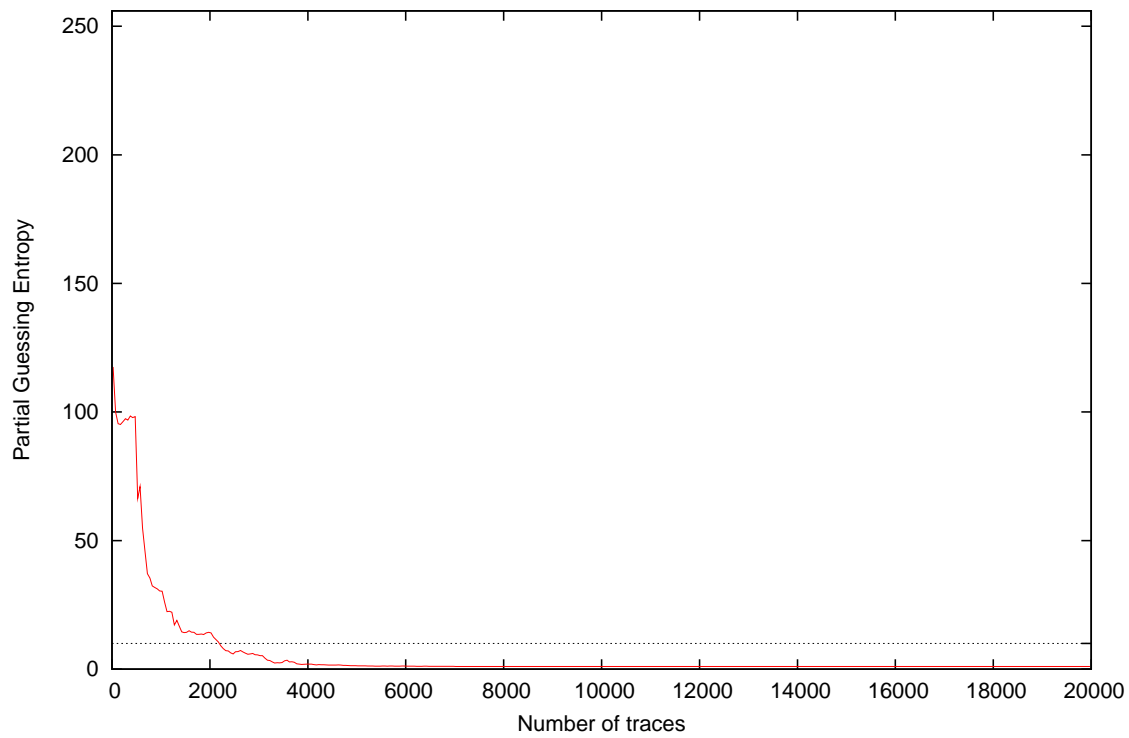
4 Partial Guessing Entropy



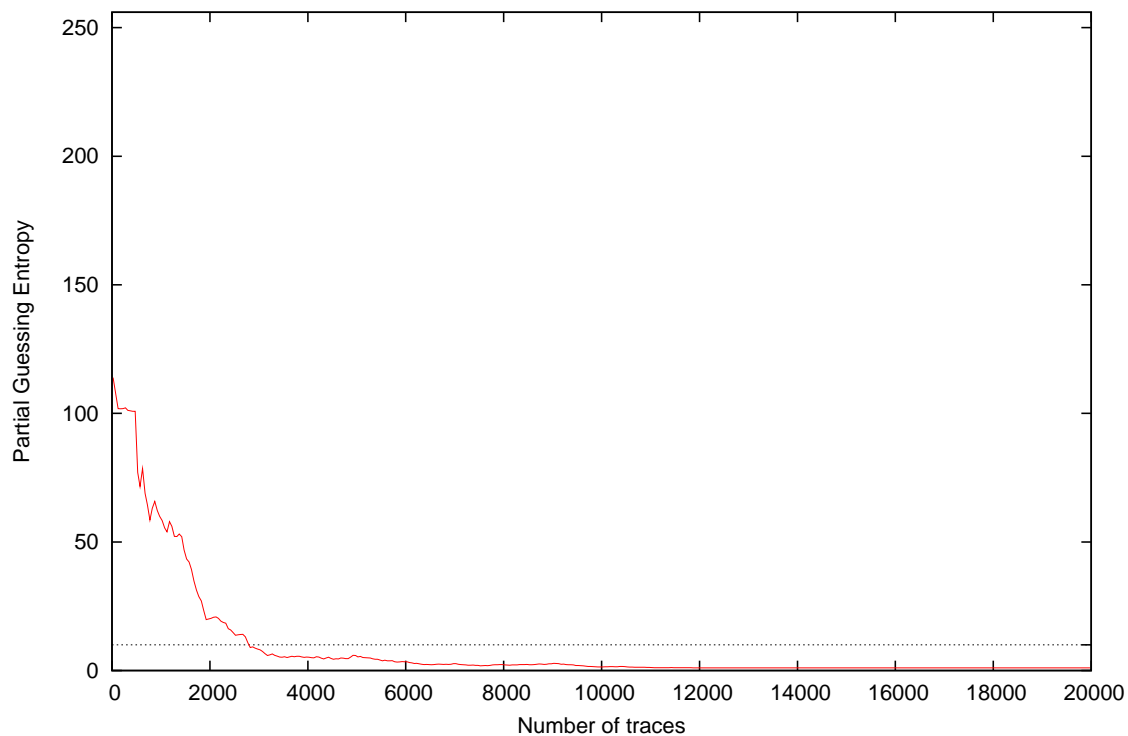
Partial Guessing Entropy for Subkey Byte #3



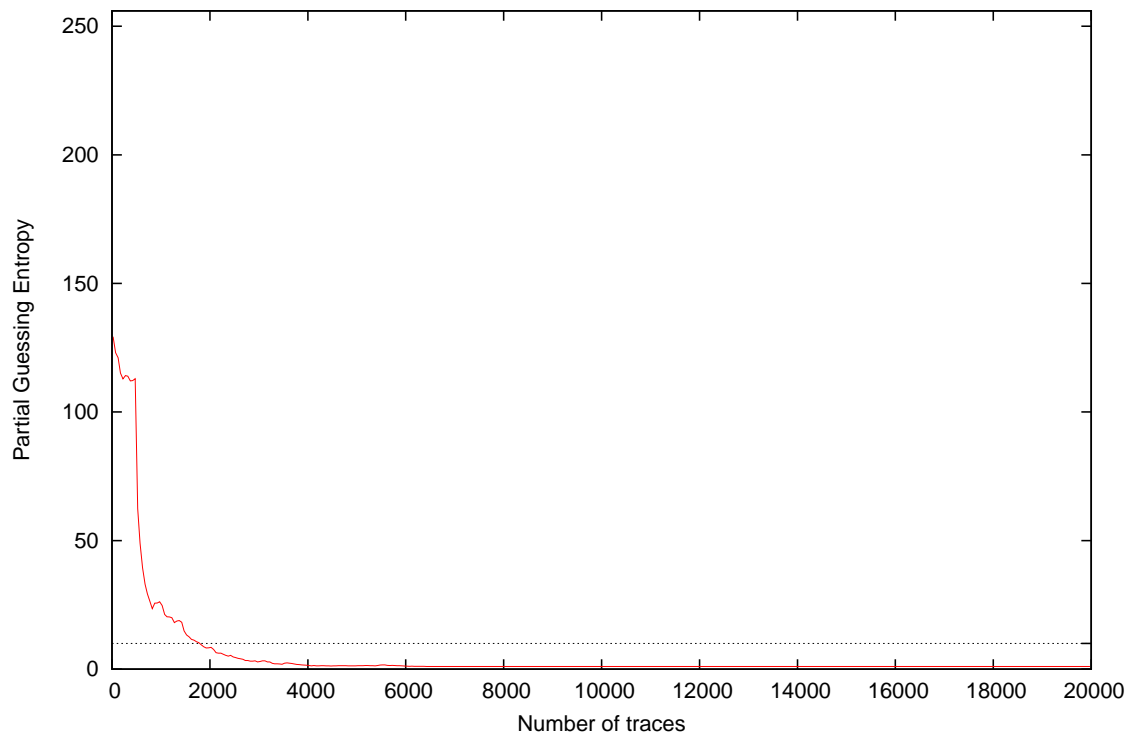
Partial Guessing Entropy for Subkey Byte #4



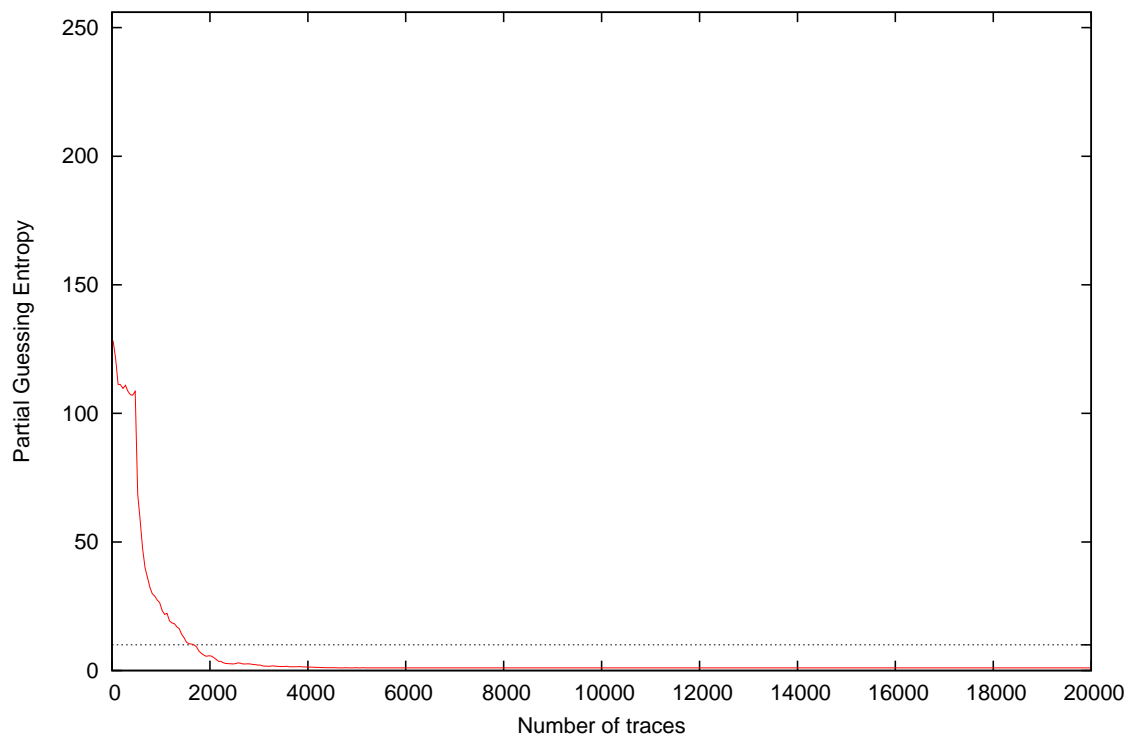
Partial Guessing Entropy for Subkey Byte #5



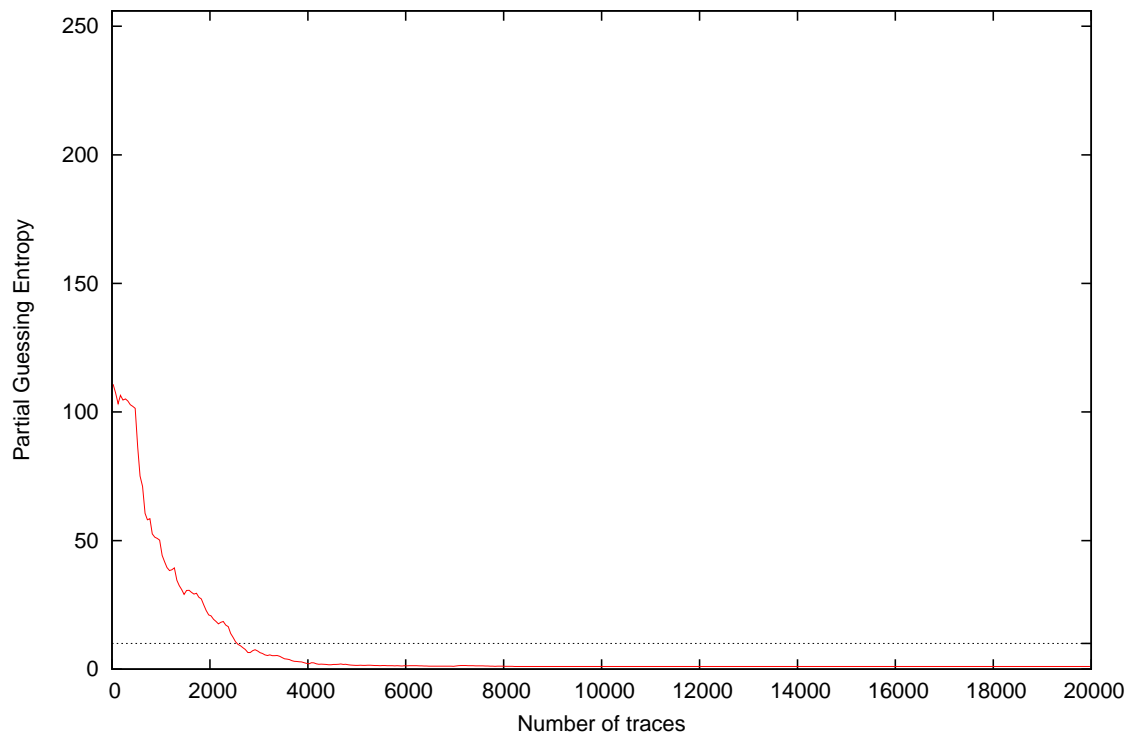
Partial Guessing Entropy for Subkey Byte #6



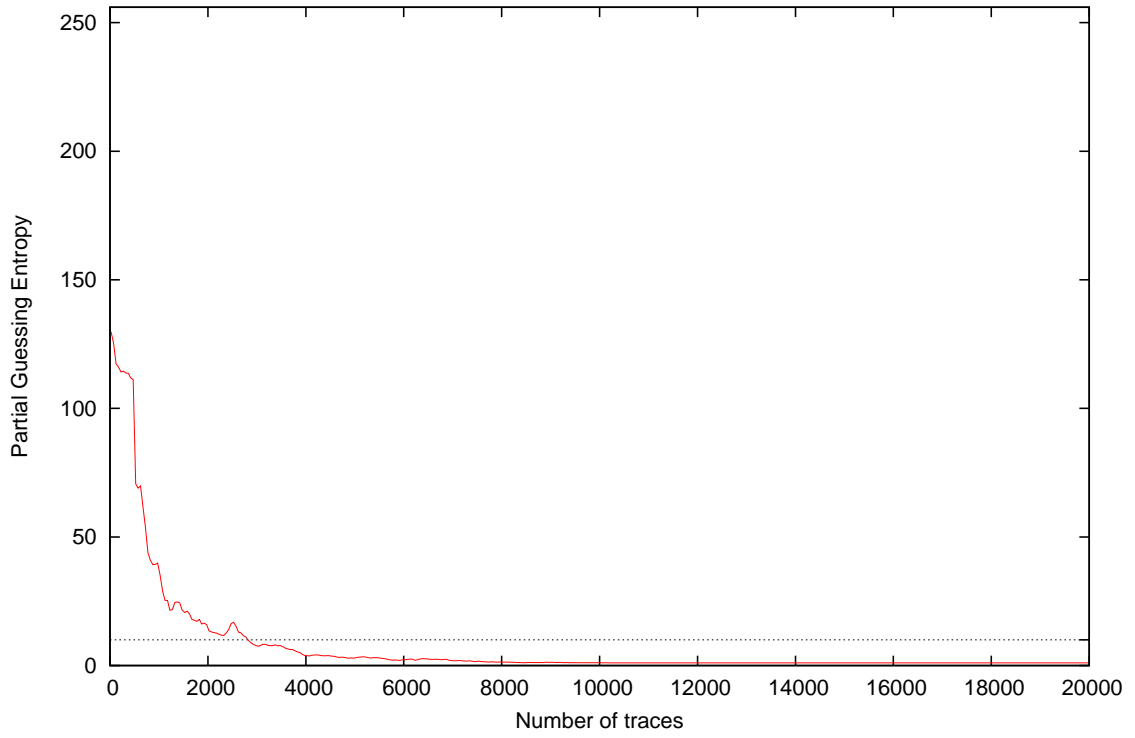
Partial Guessing Entropy for Subkey Byte #7



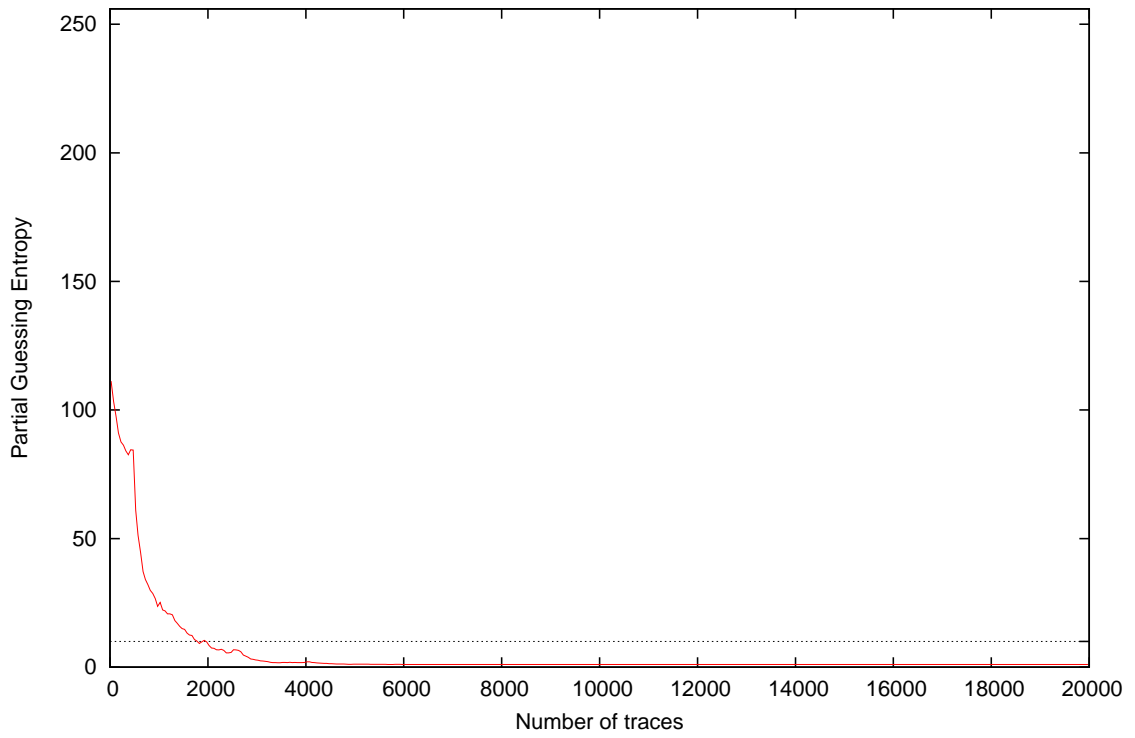
Partial Guessing Entropy for Subkey Byte #8

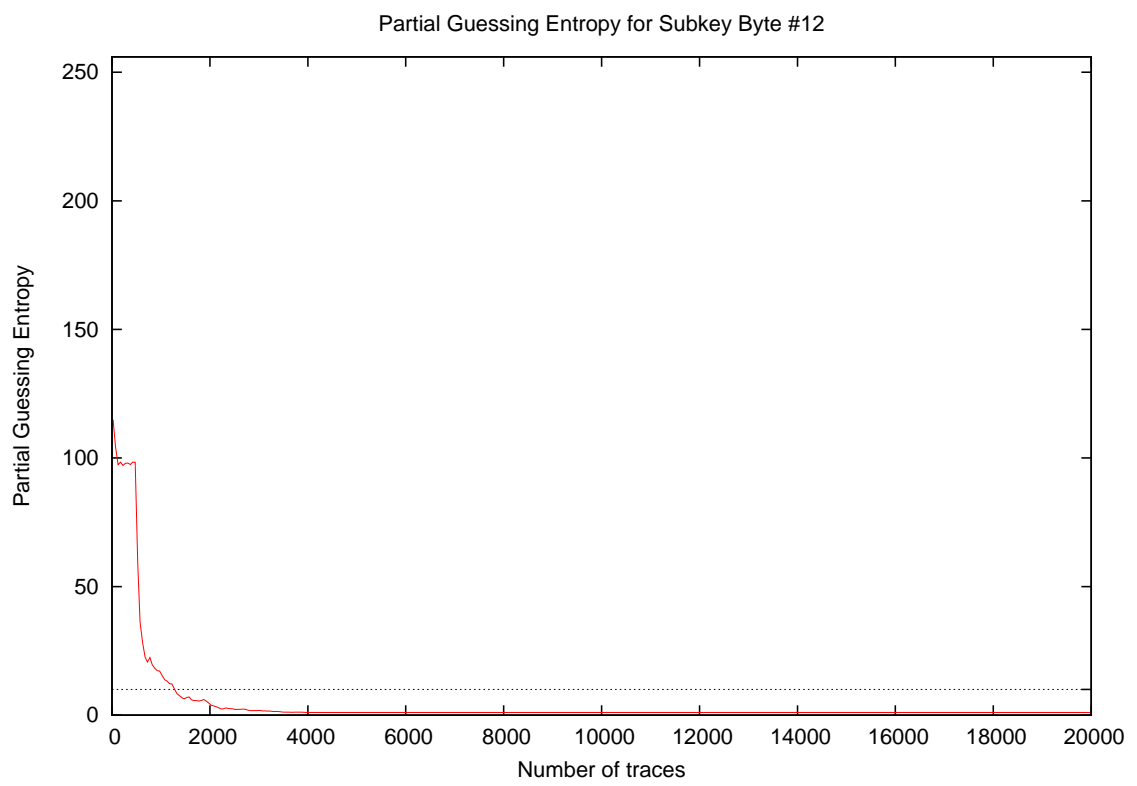
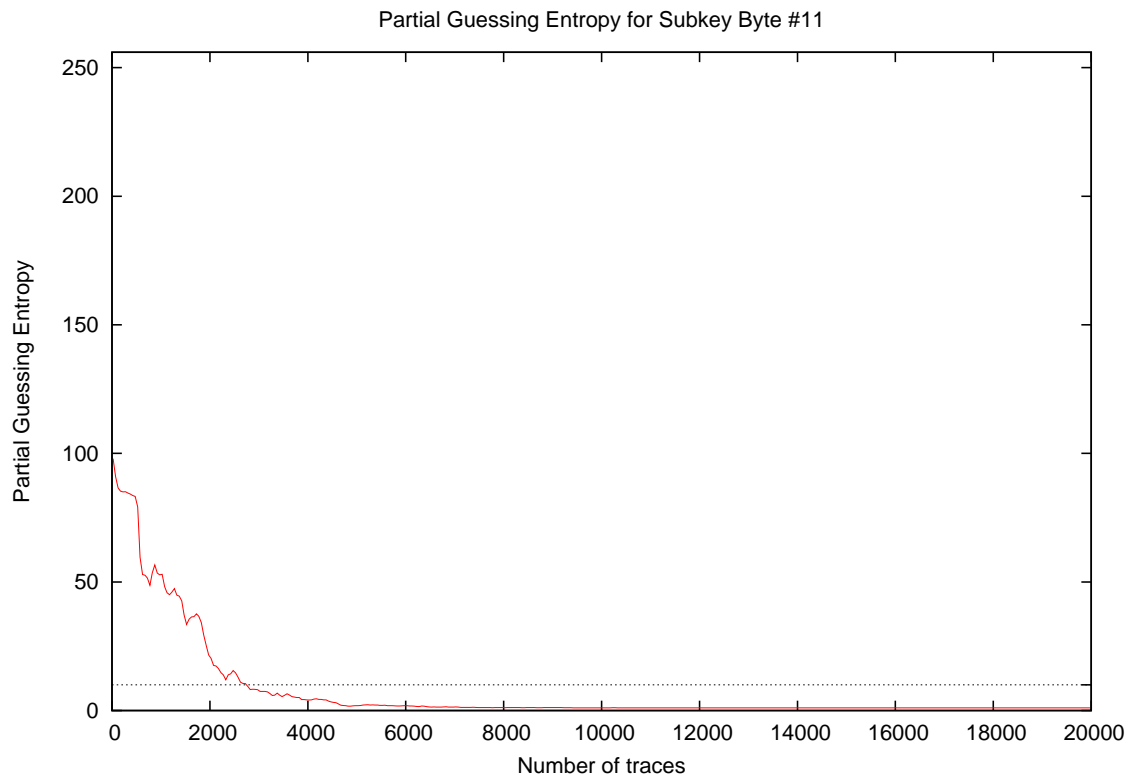


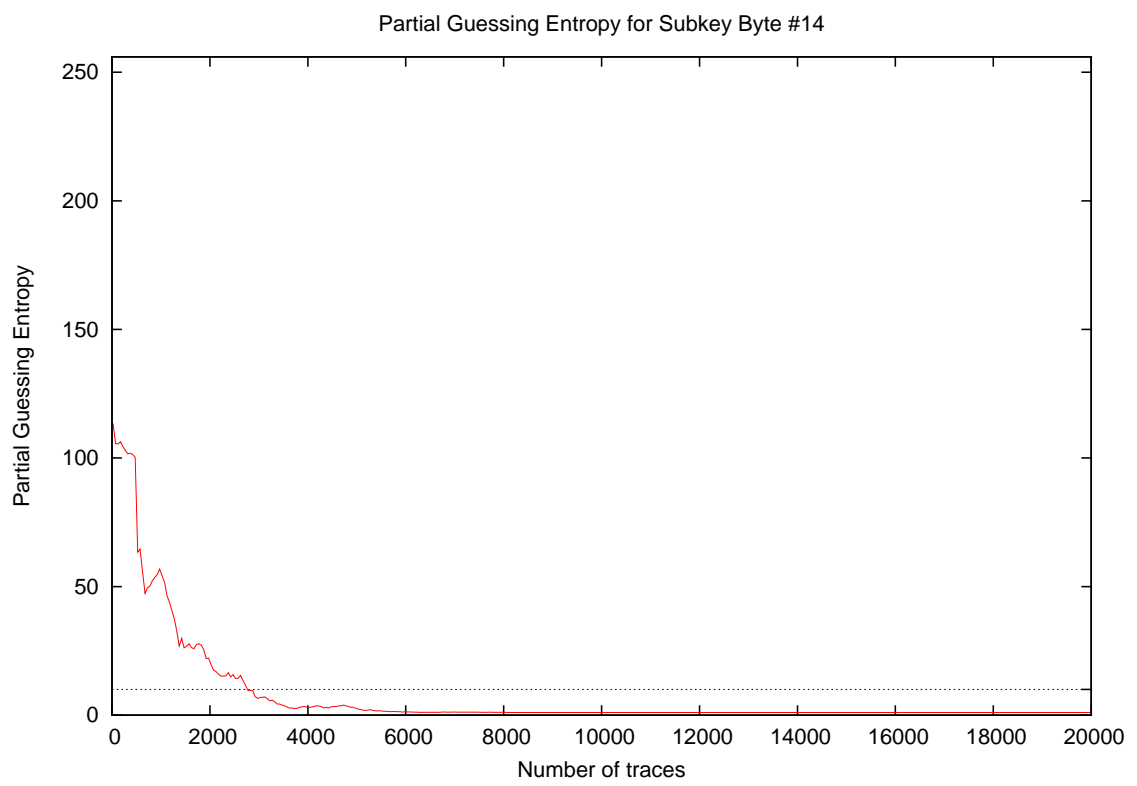
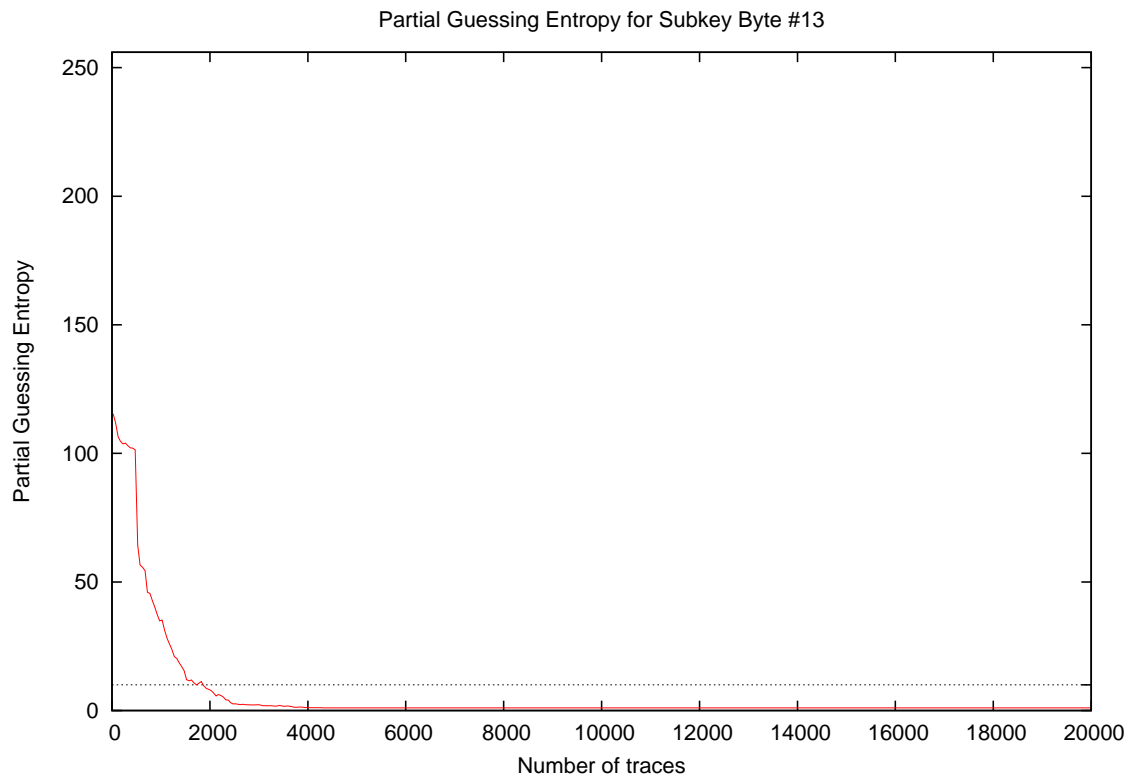
Partial Guessing Entropy for Subkey Byte #9

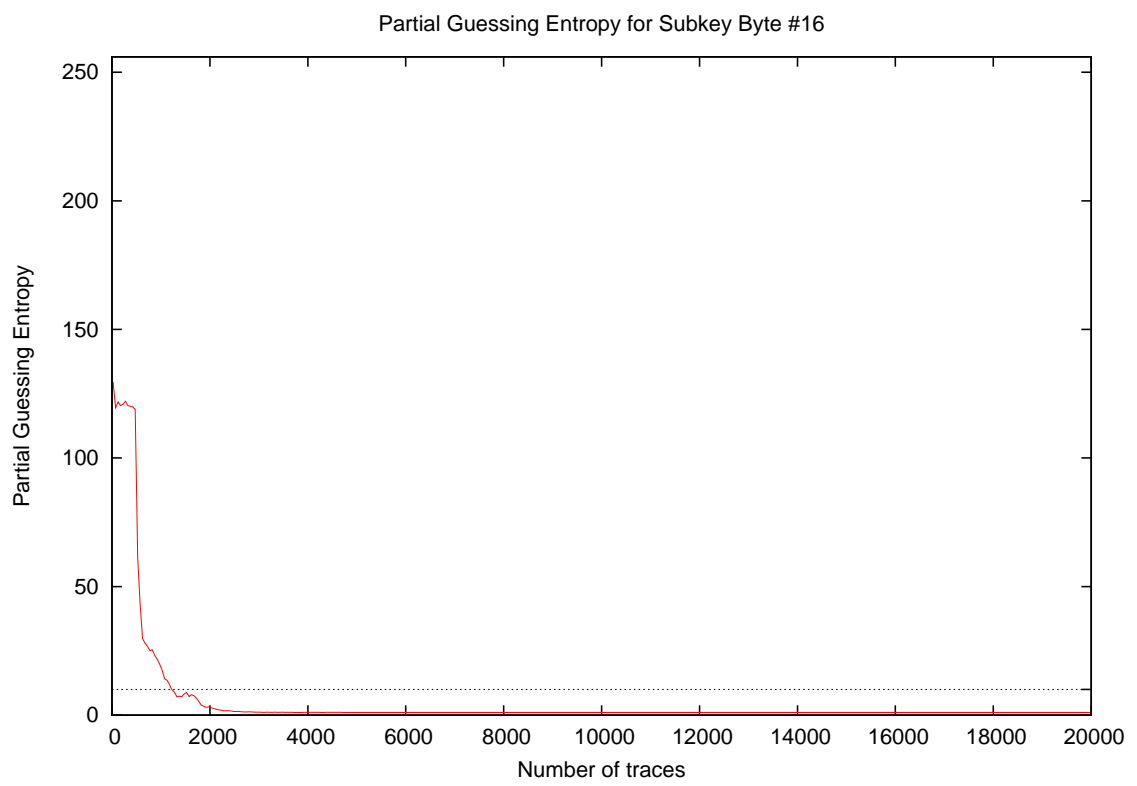
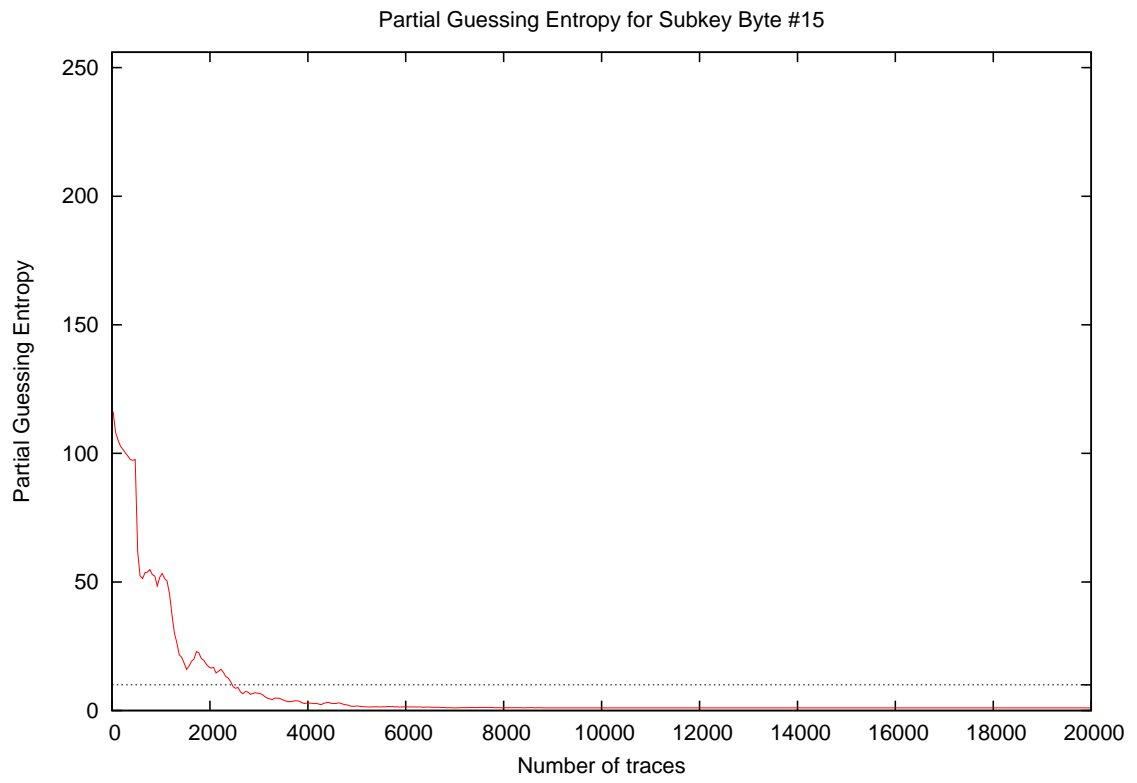


Partial Guessing Entropy for Subkey Byte #10

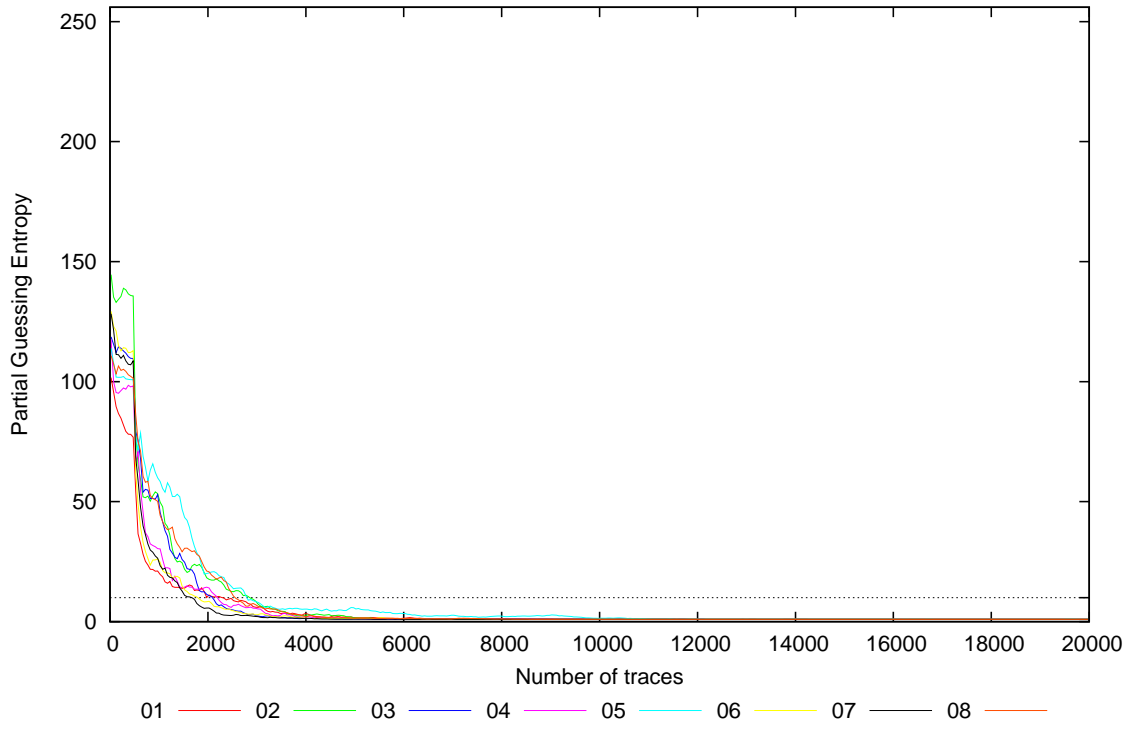




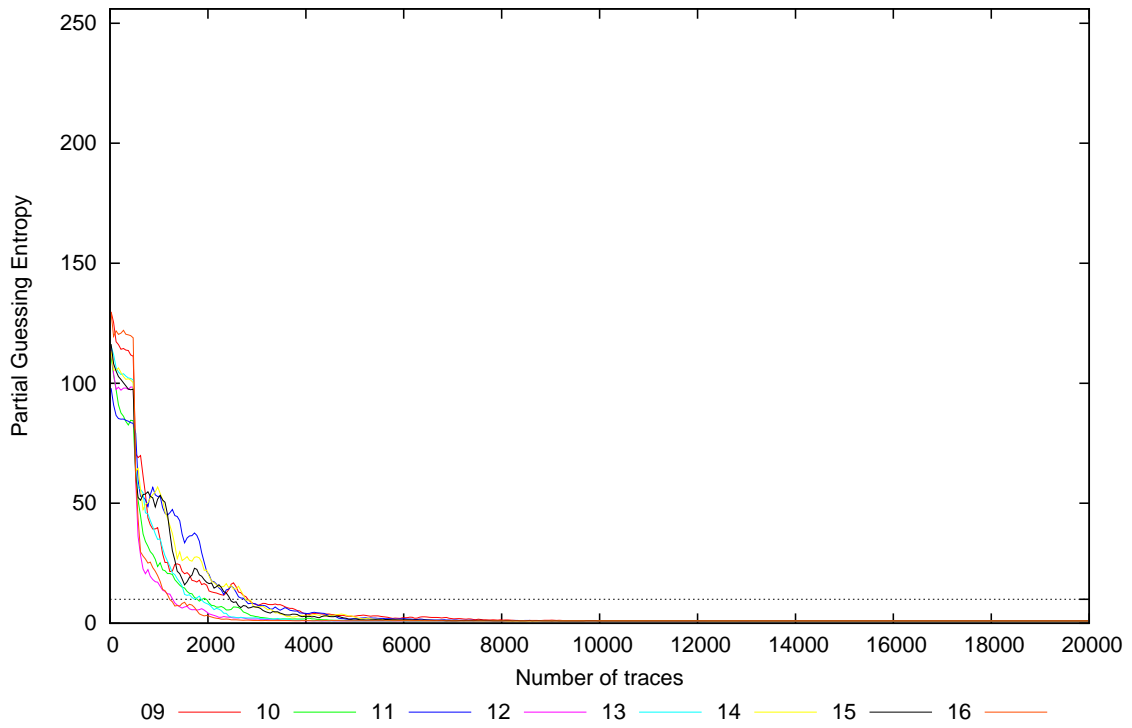




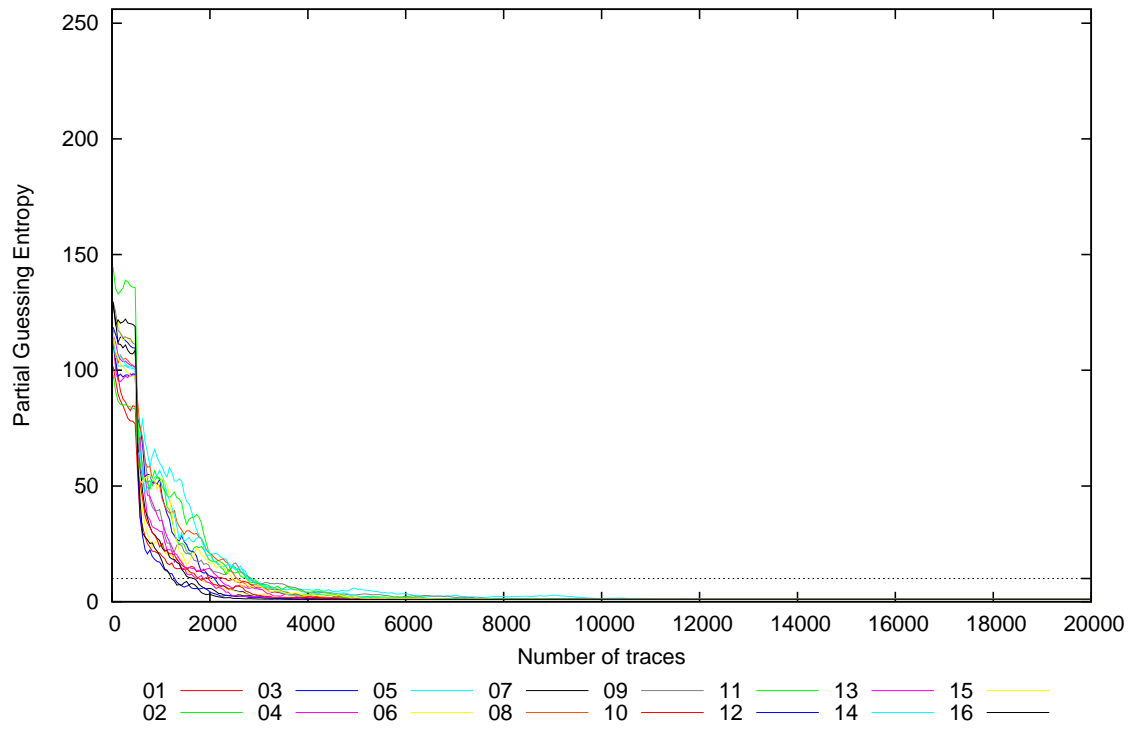
Partial Guessing Entropy for Subkey Bytes #1 to #8



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	99.8	151.5	118.0	126.8	120.1	133.3	138.8	117.3	133.5	106.4	94.1	120.3	118.7	116.4	121.7	133.4	94.1	151.5	121.9
20	99.7	146.7	113.5	122.6	117.4	133.3	125.7	110.5	124.0	114.8	98.3	114.9	114.8	117.2	115.8	139.8	98.3	146.7	119.3
30	105.2	146.2	124.3	119.3	107.9	131.4	127.6	114.0	129.7	106.1	100.1	109.1	116.9	111.7	118.8	129.7	100.1	146.2	118.6
40	97.0	137.8	113.3	111.4	108.2	124.4	126.5	109.4	129.7	107.2	94.8	106.9	113.6	111.3	112.0	127.9	94.8	137.8	114.5
50	94.0	138.3	118.5	111.6	108.9	128.7	127.2	106.6	125.3	106.1	91.6	105.1	114.1	107.7	110.5	124.3	91.6	138.3	113.7
100	90.8	133.1	109.6	95.4	103.1	122.1	113.6	105.7	121.8	100.8	86.8	102.6	108.5	105.5	105.6	121.0	86.8	133.1	107.9
200	85.9	135.0	113.4	95.6	102.5	114.0	111.0	105.8	112.8	88.7	84.7	98.4	103.5	104.3	102.4	121.3	84.7	135.0	105.0
300	81.1	138.9	111.5	97.1	102.0	114.8	110.2	104.5	115.2	87.5	84.6	97.4	103.7	101.6	99.6	121.8	81.1	138.9	104.5
400	78.2	136.2	109.2	97.9	100.9	112.2	106.4	102.4	112.7	83.0	84.2	98.2	102.2	101.5	97.6	120.5	78.2	136.2	102.7
500	73.7	132.6	106.8	97.7	100.1	109.3	104.7	99.8	108.8	81.7	81.9	95.0	99.7	98.5	96.1	115.5	73.7	132.6	100.1
1000	21.8	51.3	50.5	33.5	58.9	25.3	25.2	51.1	39.1	23.7	57.7	17.0	36.8	60.9	54.9	19.9	17.0	60.9	39.2
2000	10.0	17.2	11.5	15.1	21.0	8.3	5.5	20.7	14.8	8.8	21.9	4.4	7.9	21.2	17.2	3.4	3.4	21.9	13.1
3000	5.8	8.8	2.1	5.3	8.0	2.8	2.2	7.1	7.2	2.7	7.2	1.8	2.1	6.4	6.6	1.2	1.2	8.8	4.8
4000	3.4	2.8	1.3	1.8	5.0	1.4	1.3	2.2	3.9	2.1	4.0	1.0	1.2	3.2	2.7	1.1	1.0	5.0	2.4
5000	1.7	1.6	1.2	1.3	5.2	1.2	1.0	1.5	2.8	1.1	1.8	1.0	1.0	2.6	1.8	1.0	1.0	5.2	1.8
10000	1.0	1.0	1.0	1.0	1.4	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
15000	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	1.0	1.0	1.0
20000	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	1.0	1.0	1.0