

Evaluation results

DPA contest v2

July 2011

1 Introduction

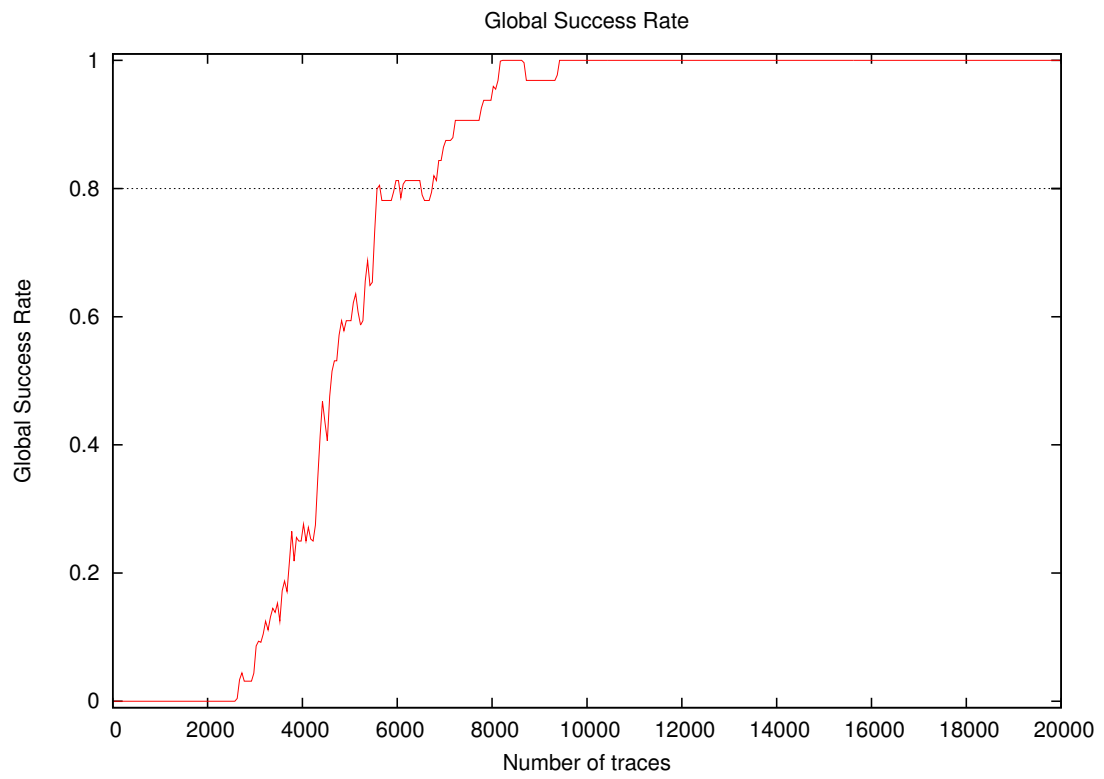
1.1 About the attack

- **Attack Name:** Stochastic approach
- **Sender/Team:** Annelie Heuser, Michael Kasper, Werner Schindler, Marc Stöttinger
- **Institution:** CASED (research group CASCADE); TU Darmstadt, Fraunhofer SIT, Bundesamt für Sicherheit in der Informationstechnik (BSI)
- **Language:** Matlab
- **Attacked subkey:** 10

1.2 About the evaluation

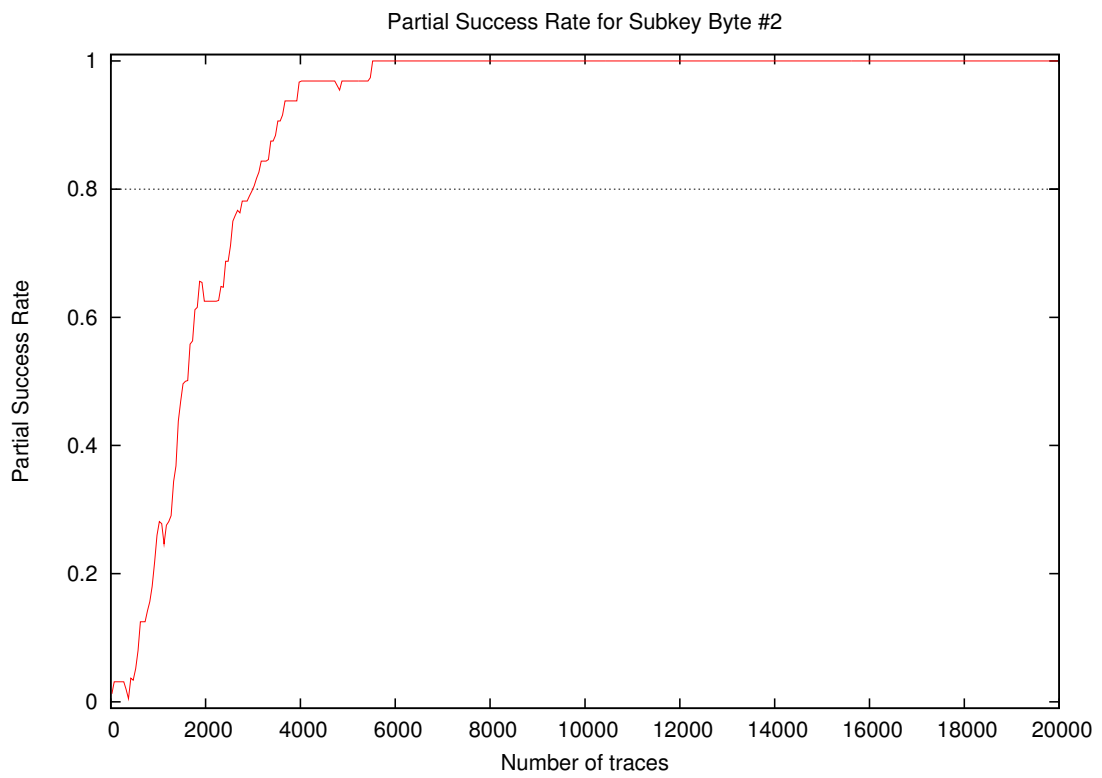
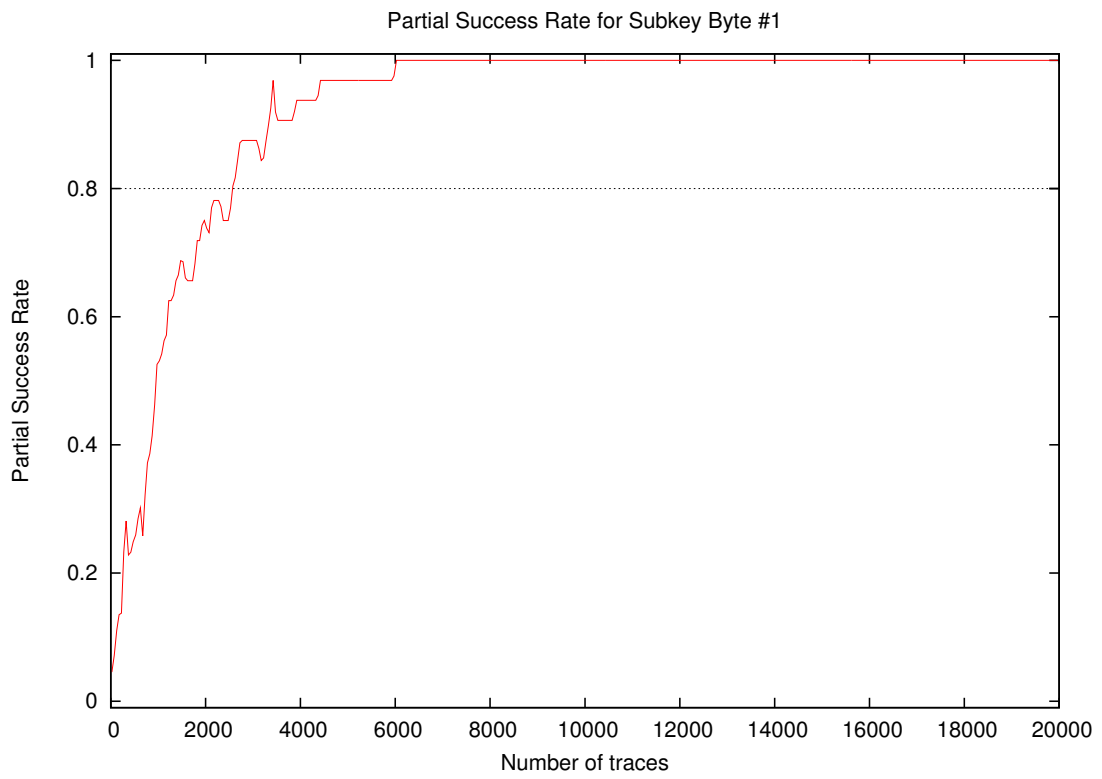
- **Date of evaluation:** July 2011

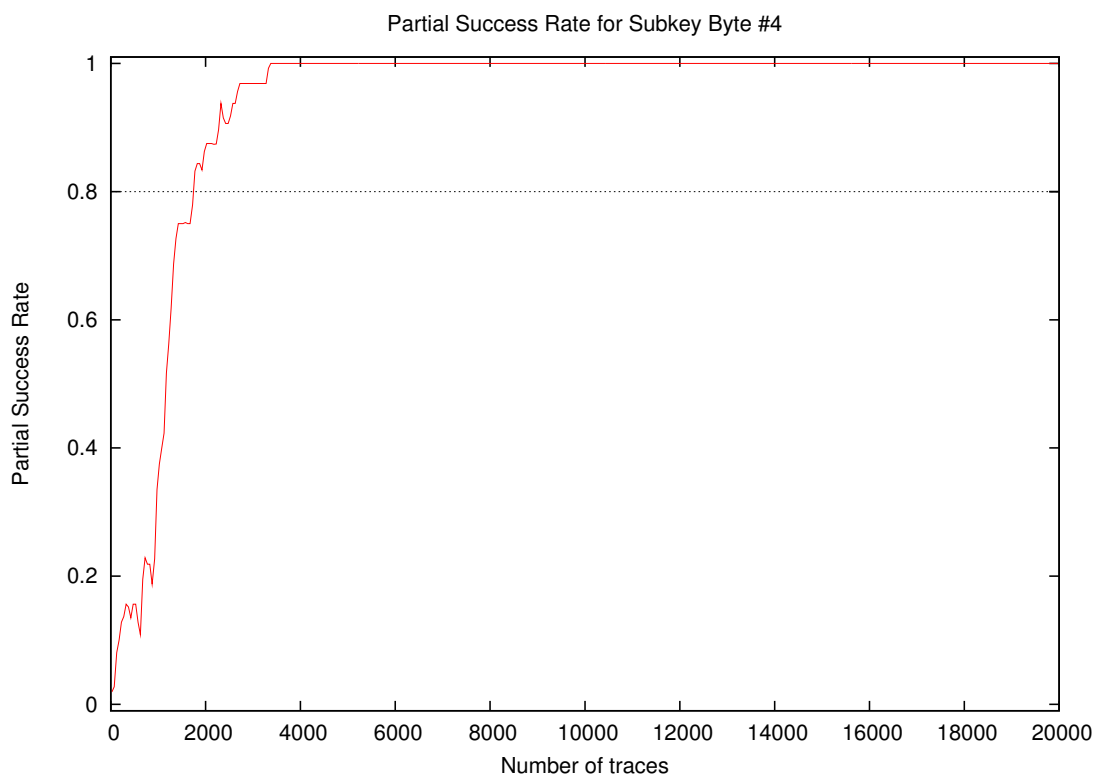
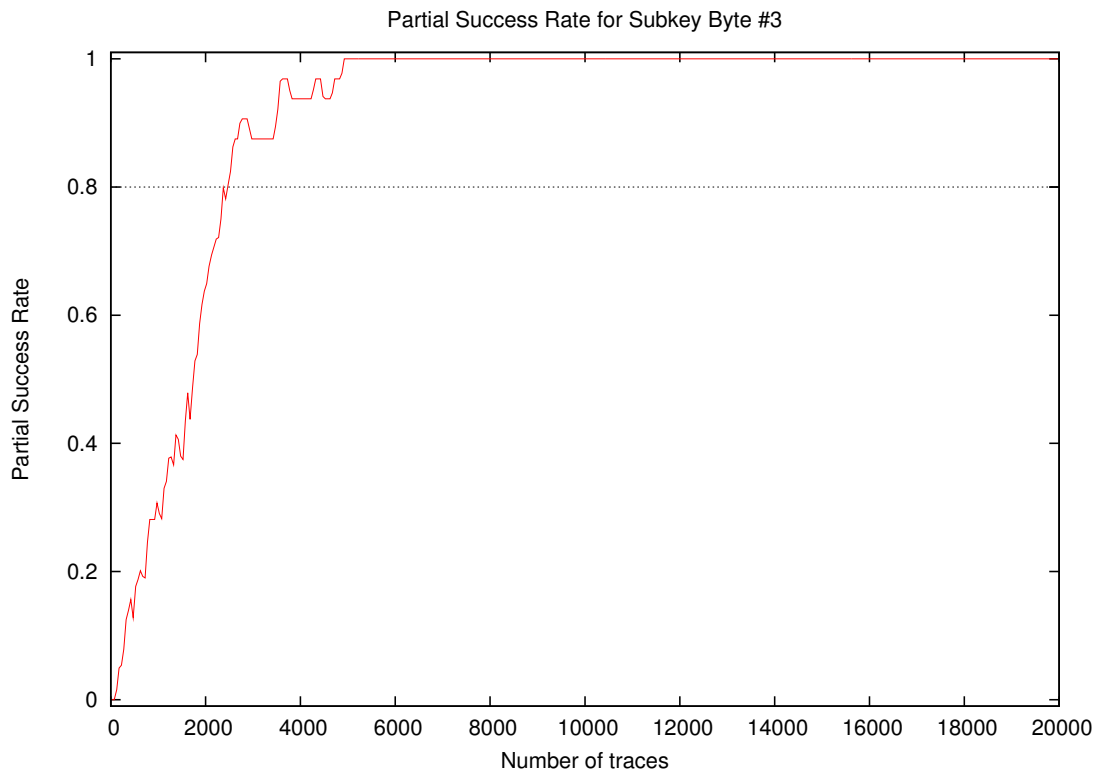
2 Global Success Rate

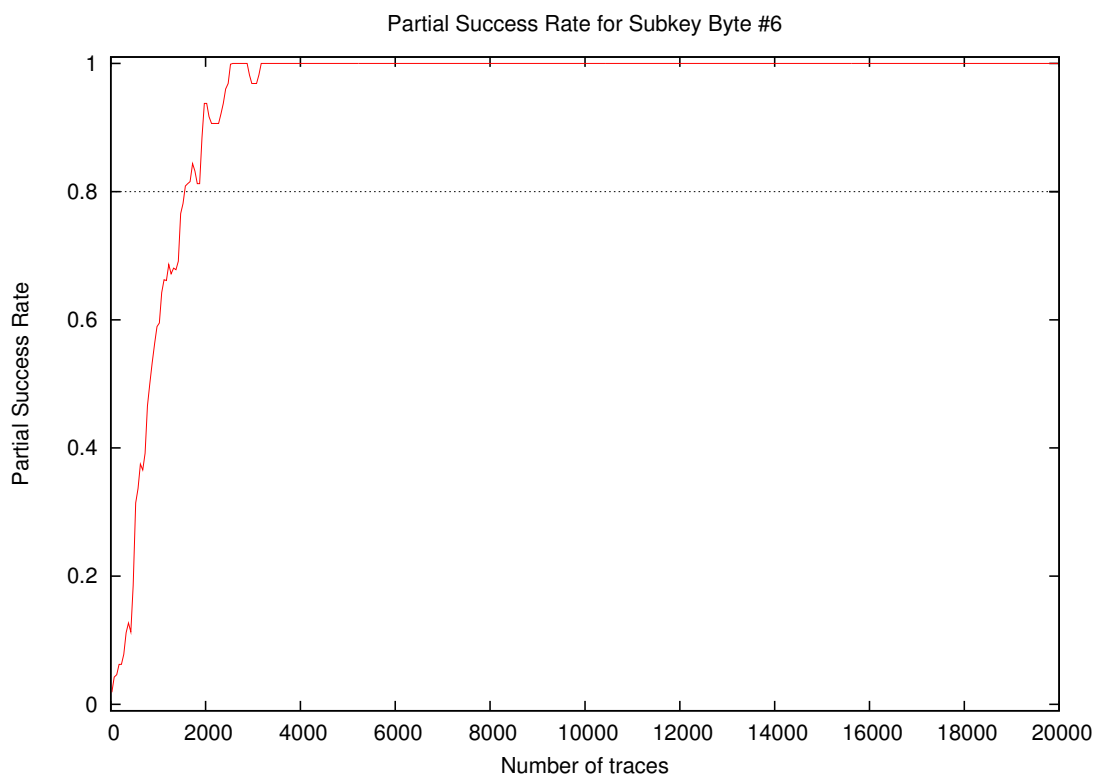
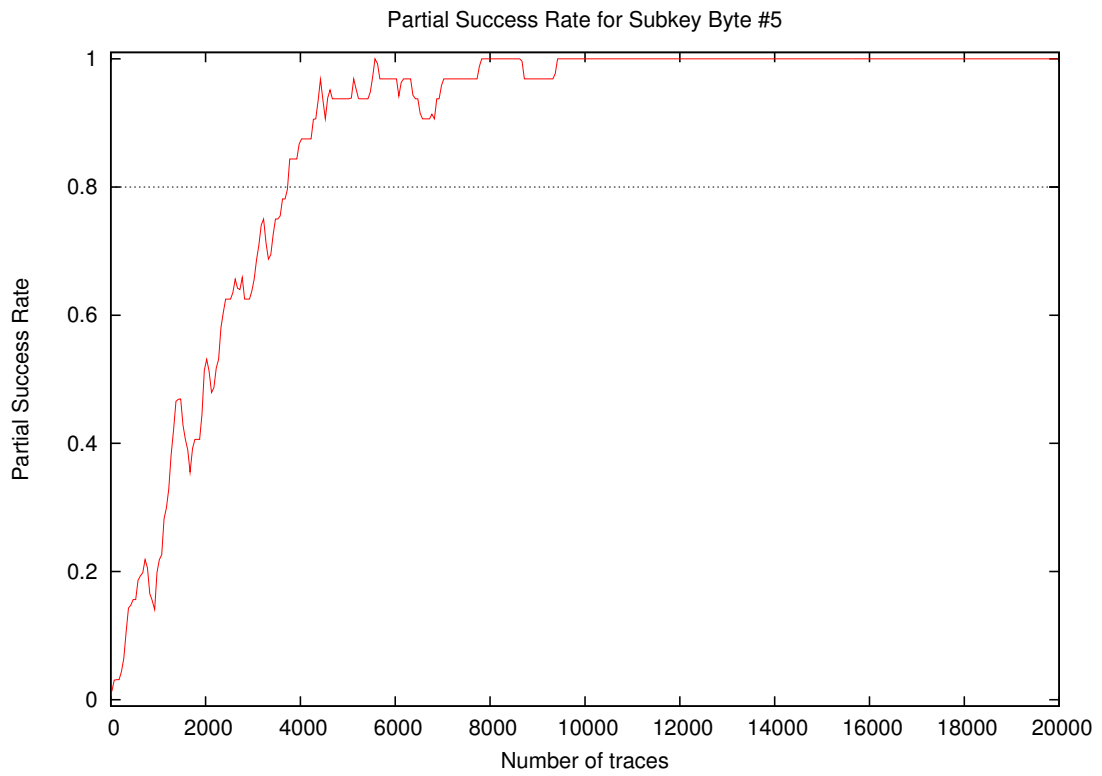


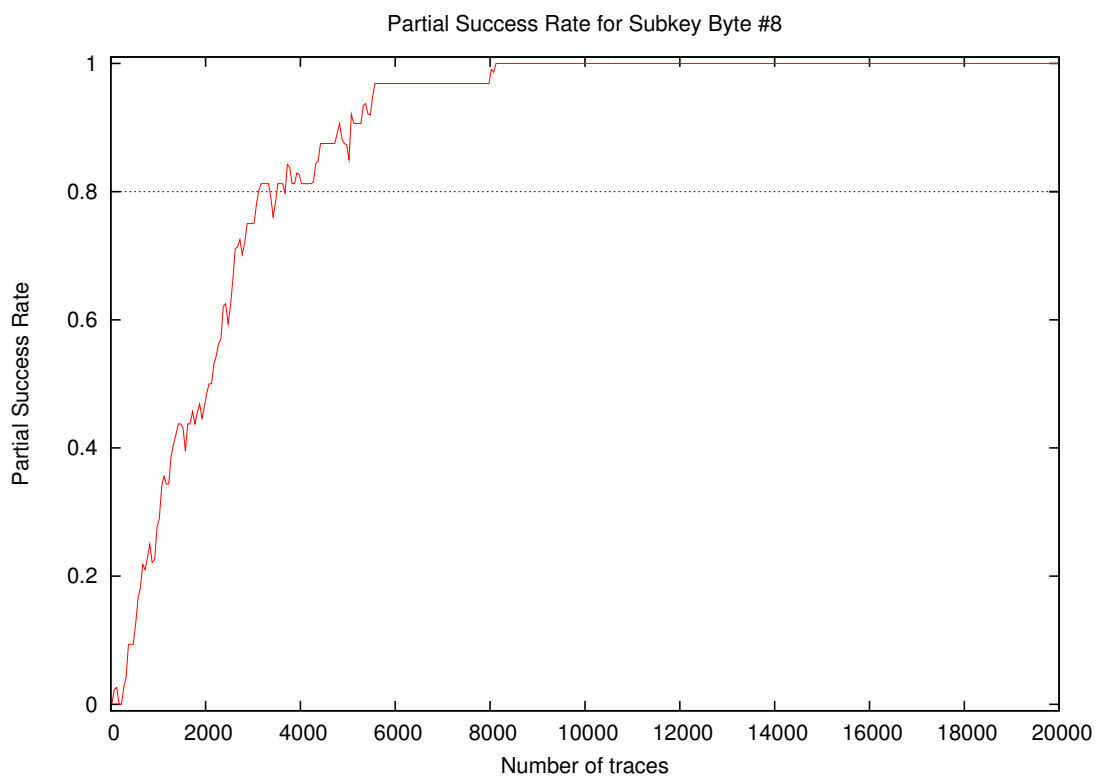
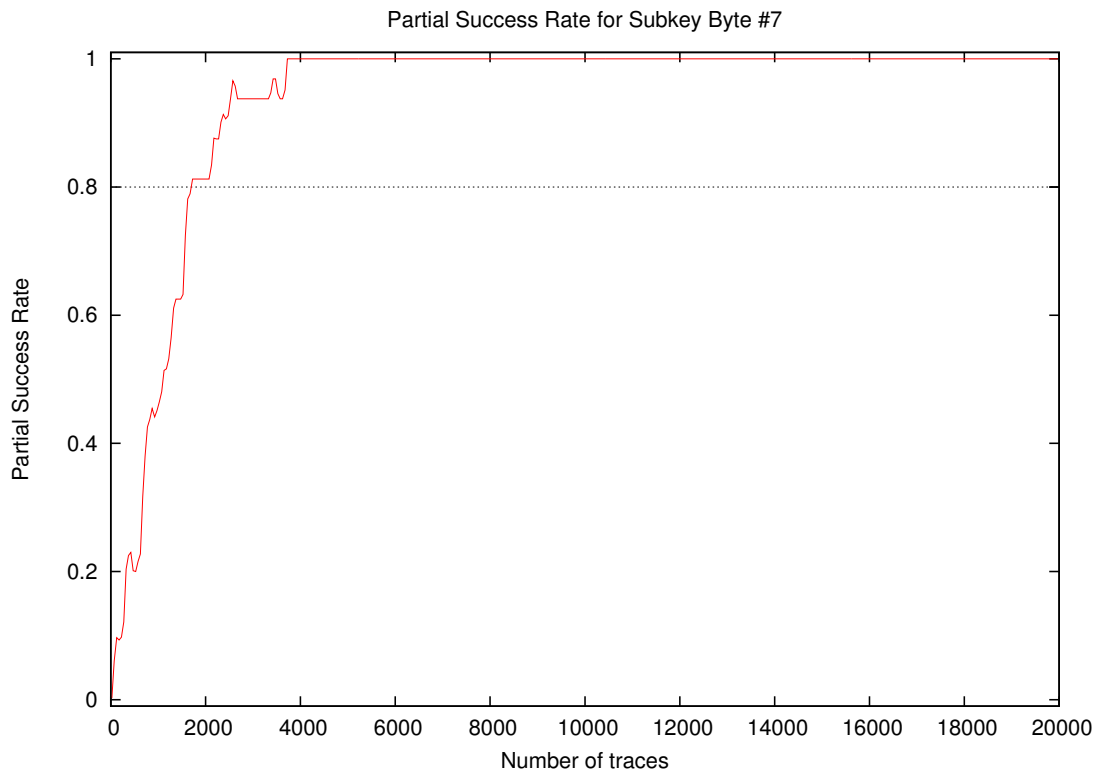
Number of traces	Global Success Rate
10	0.00
20	0.00
30	0.00
40	0.00
50	0.00
100	0.00
200	0.00
300	0.00
400	0.00
500	0.00
1000	0.00
2000	0.00
3000	0.06
4000	0.28
5000	0.59
10000	1.00
15000	1.00
20000	1.00

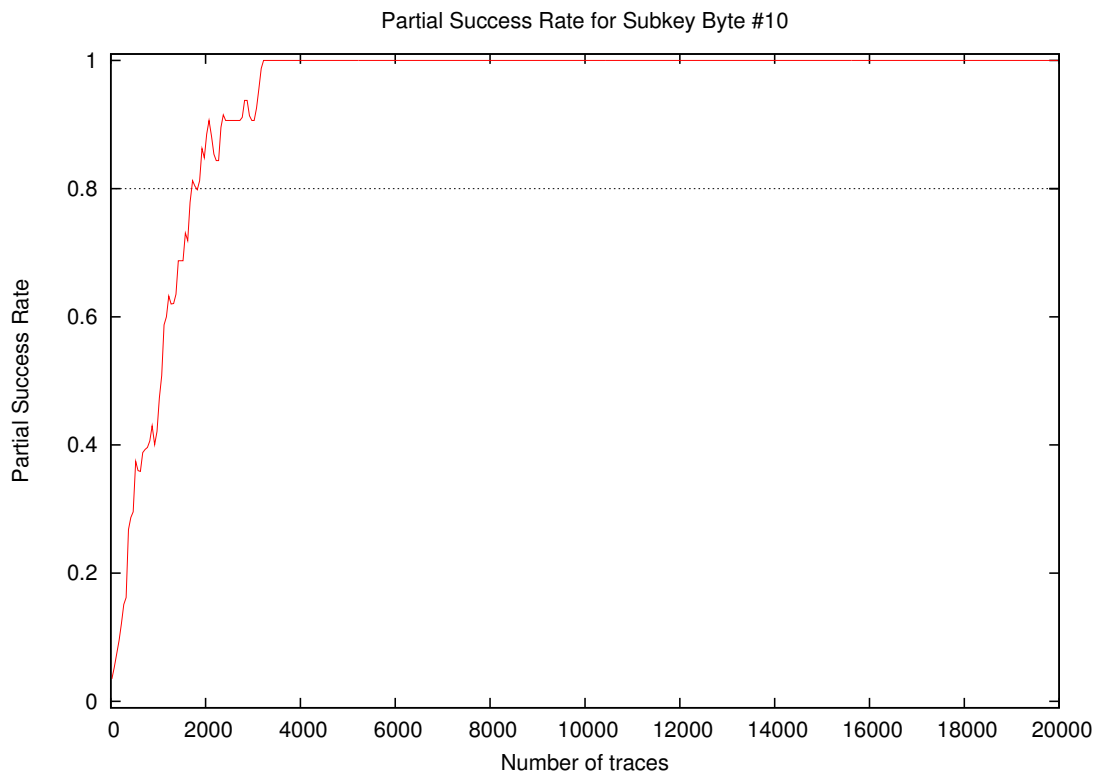
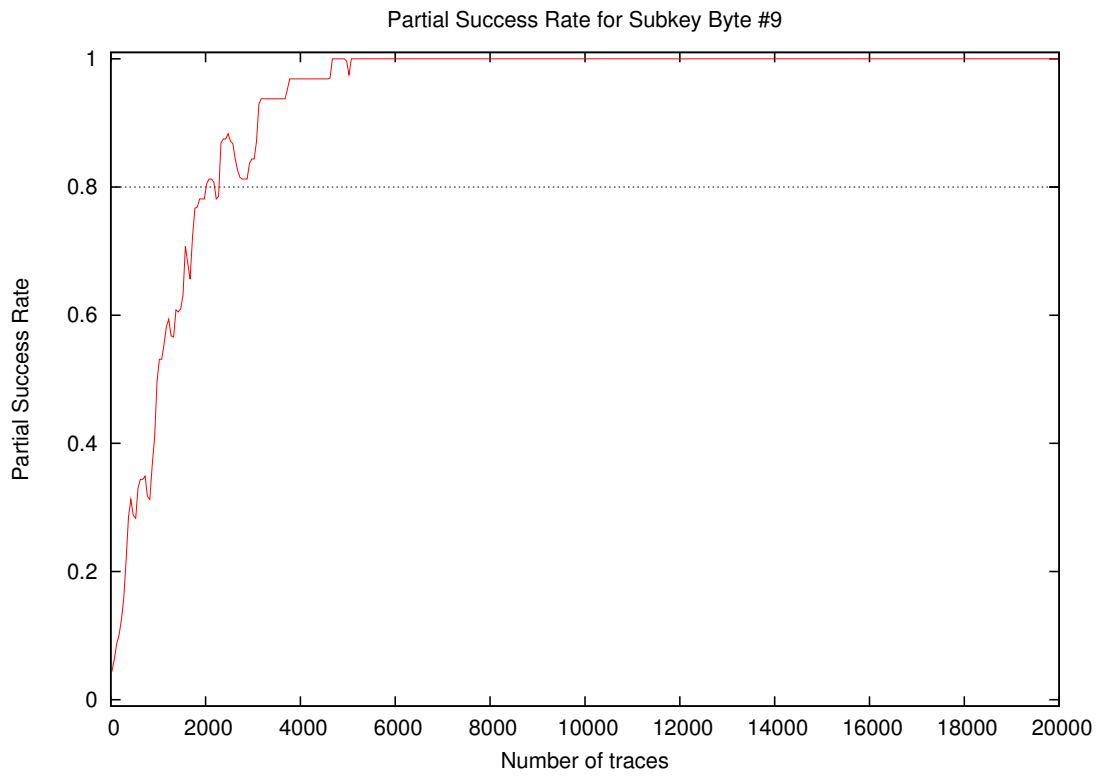
3 Partial Success Rate

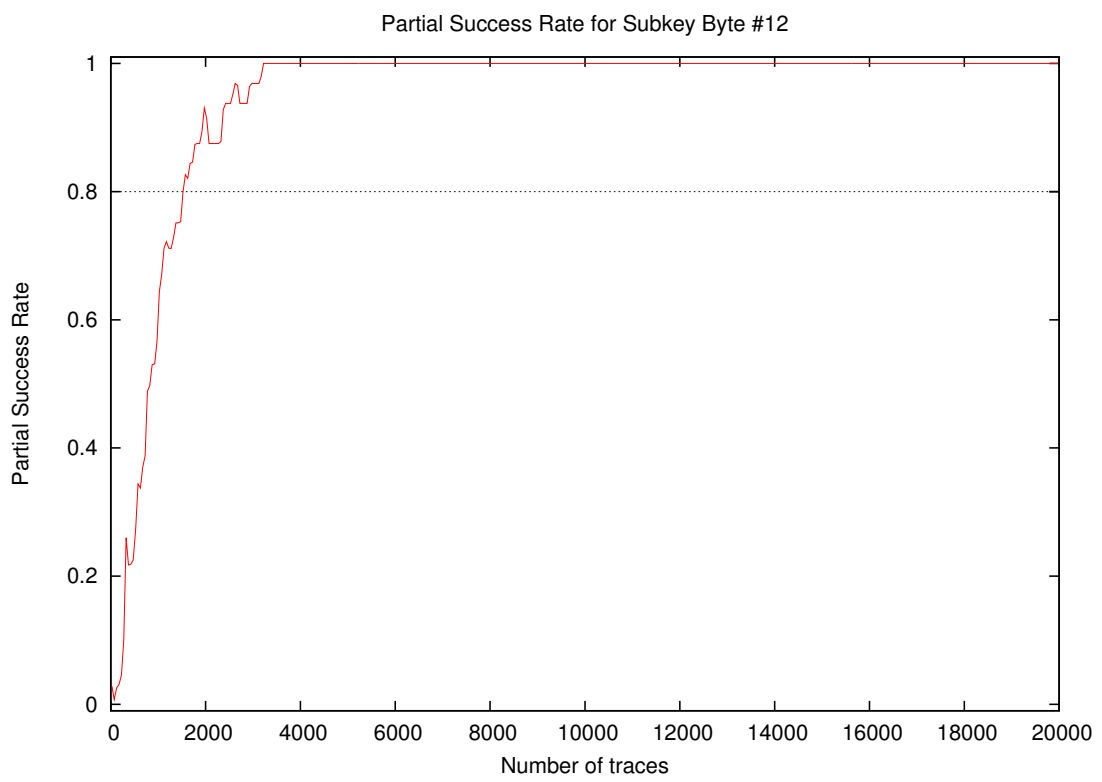
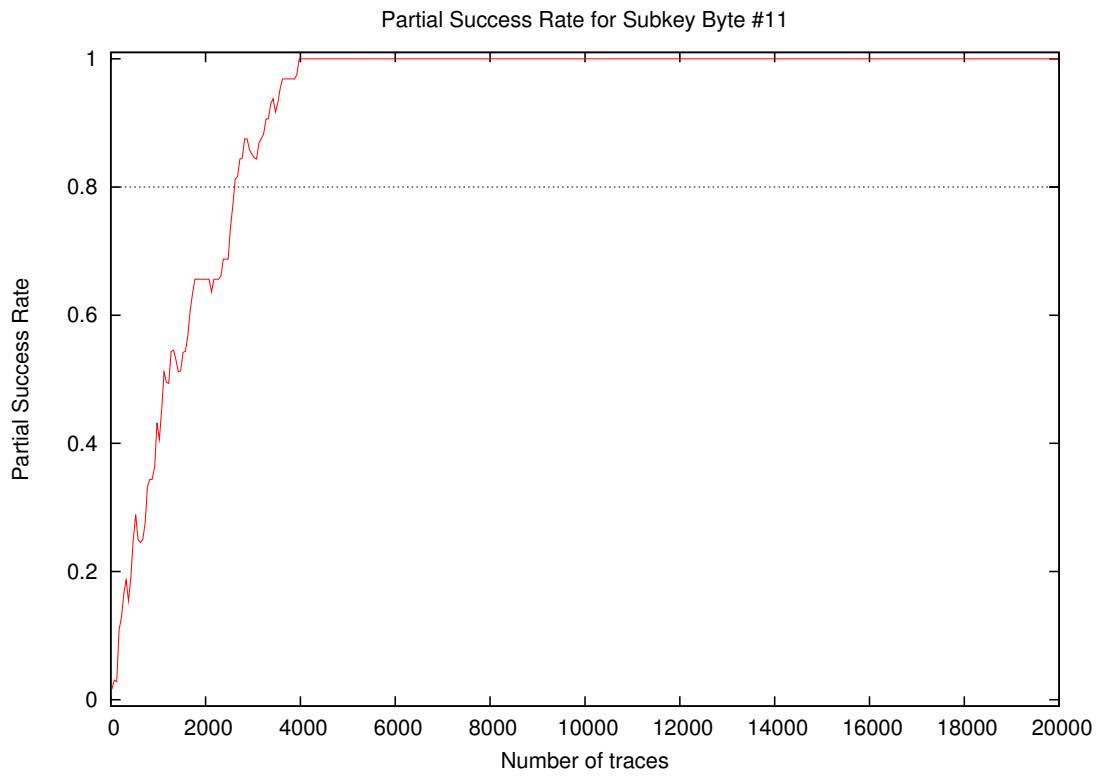


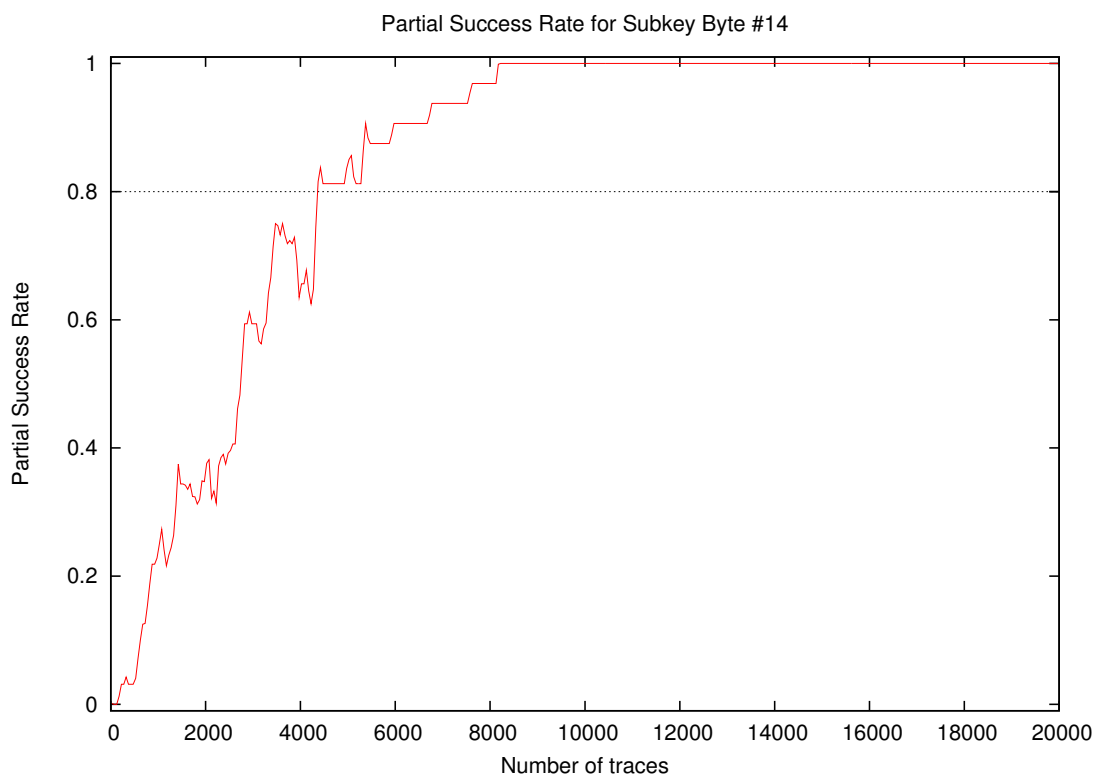
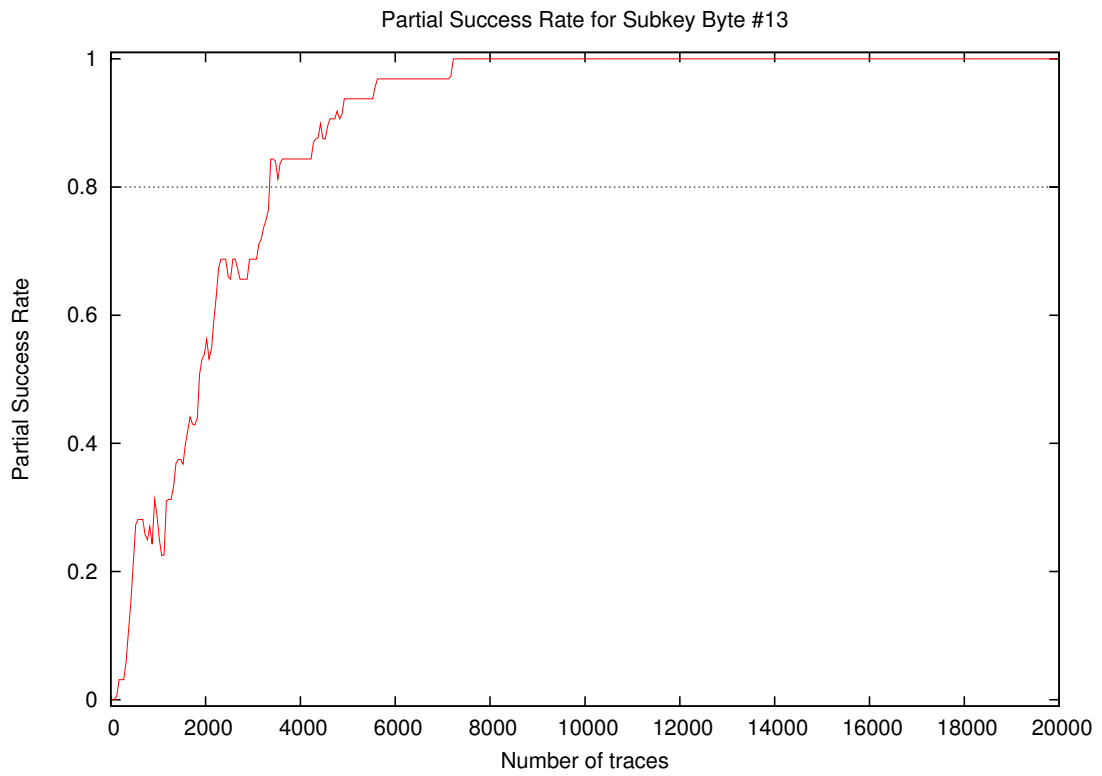


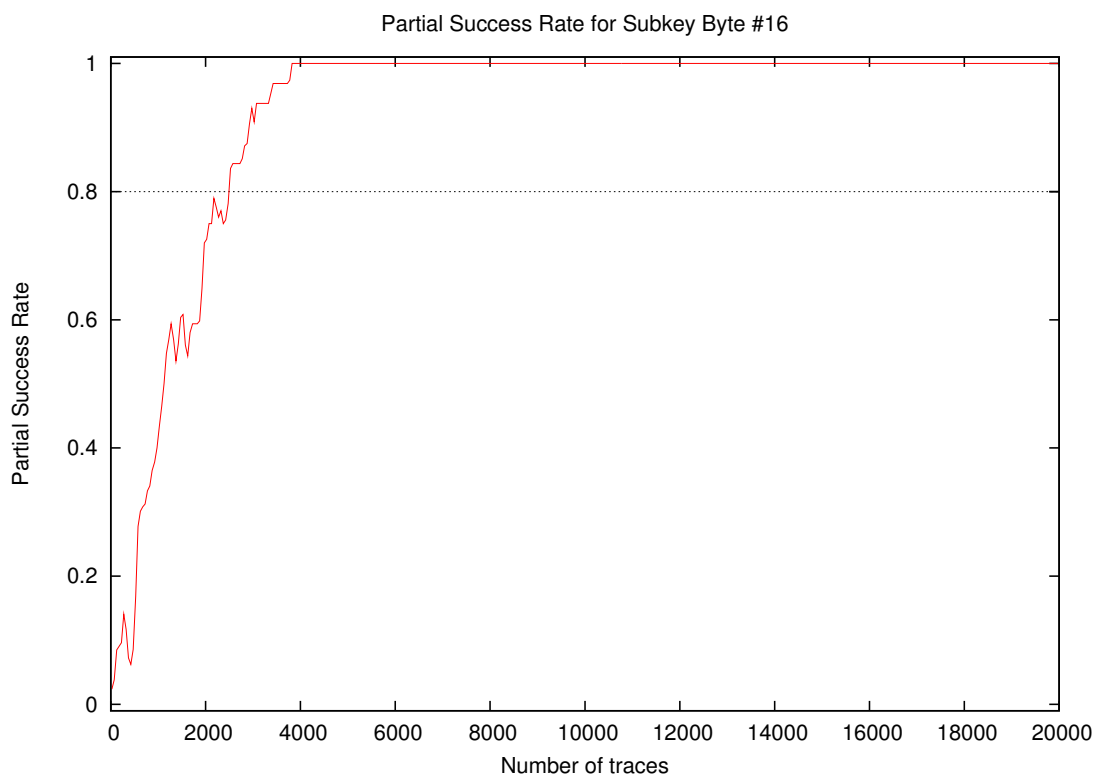
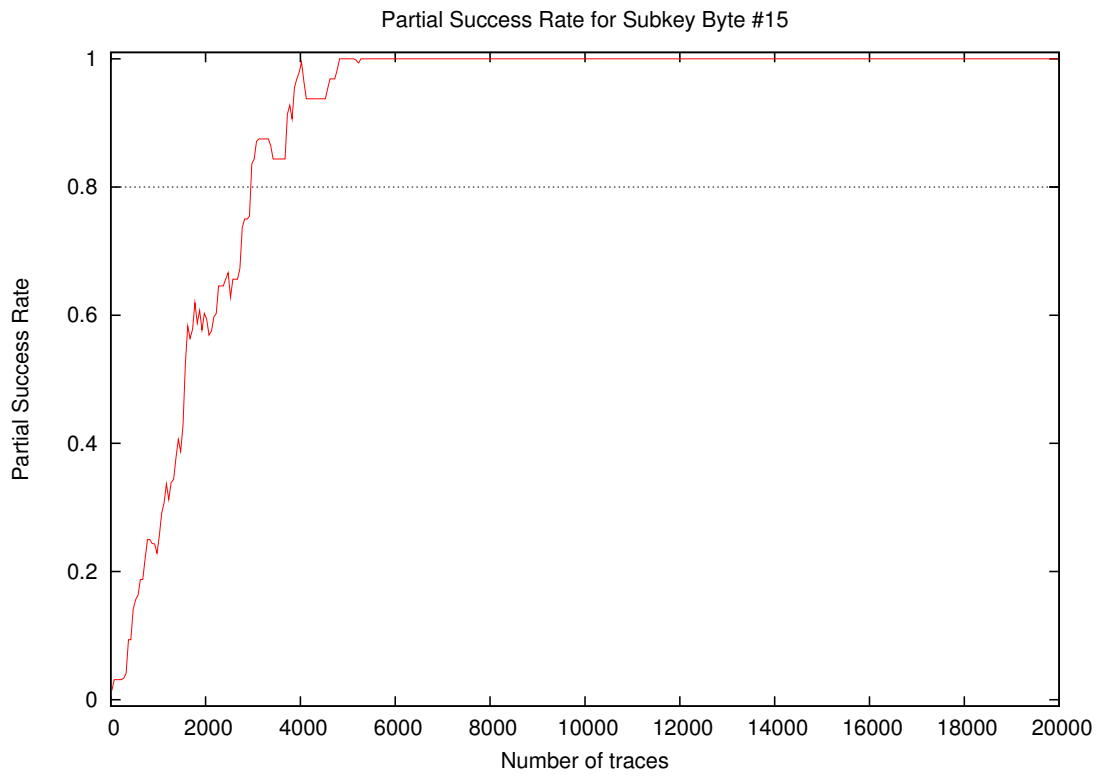


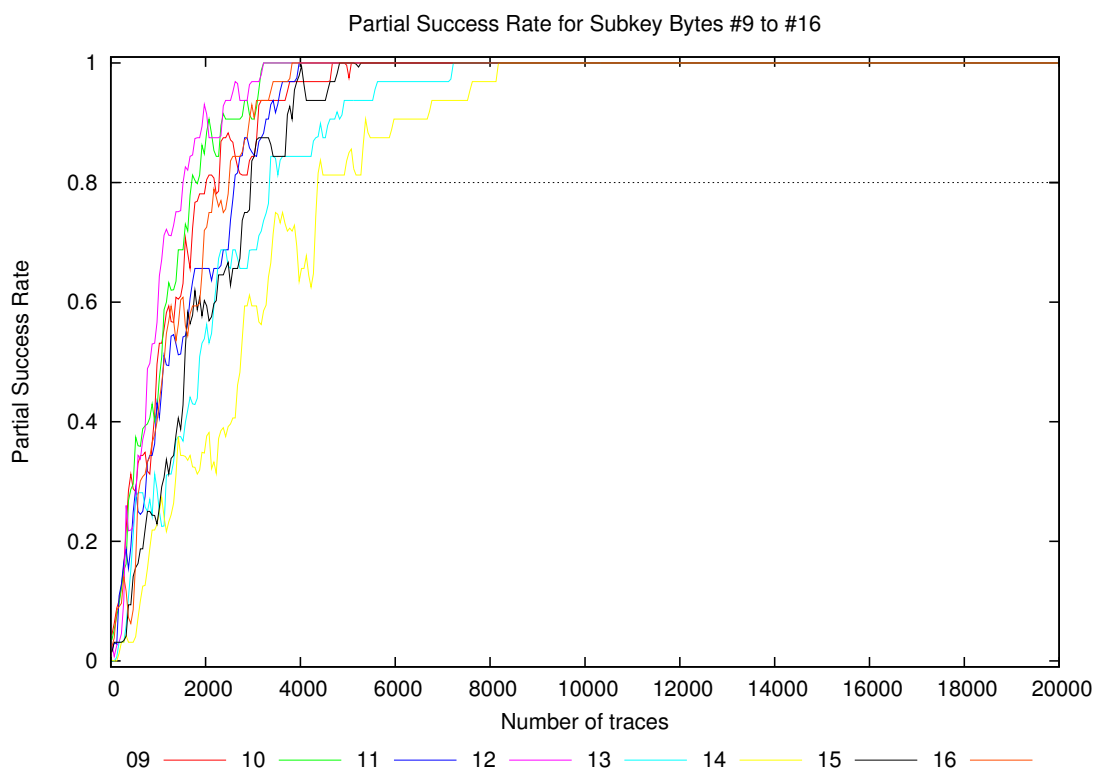
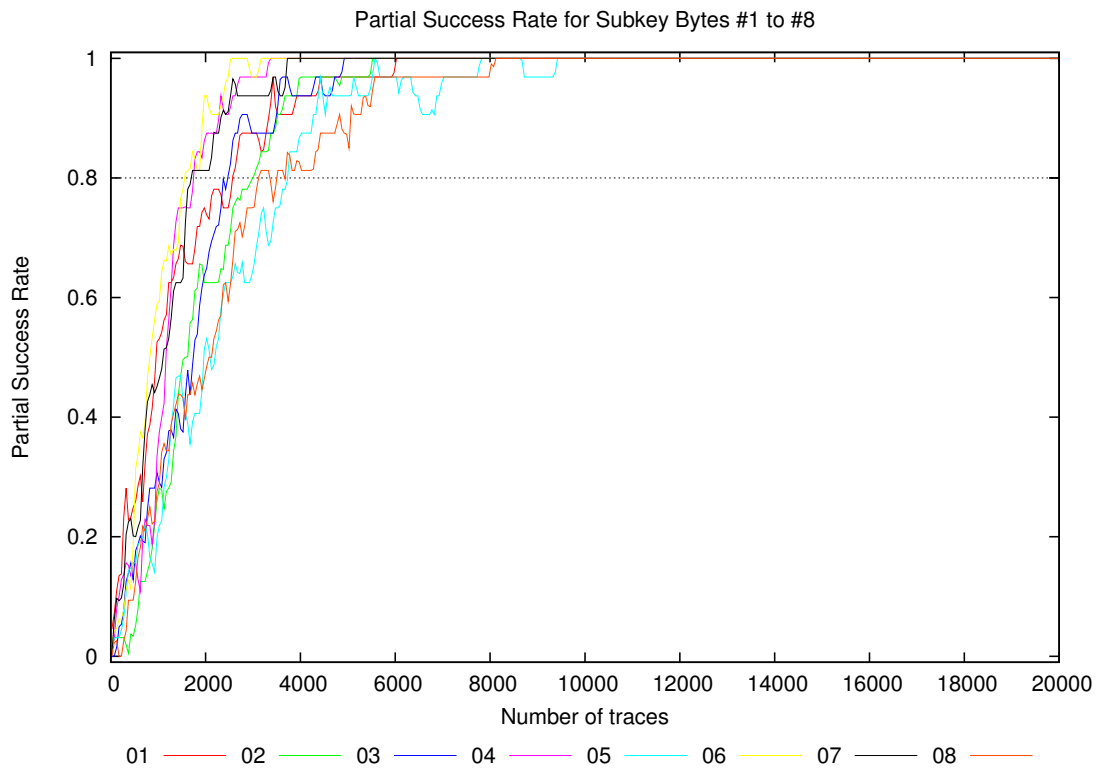


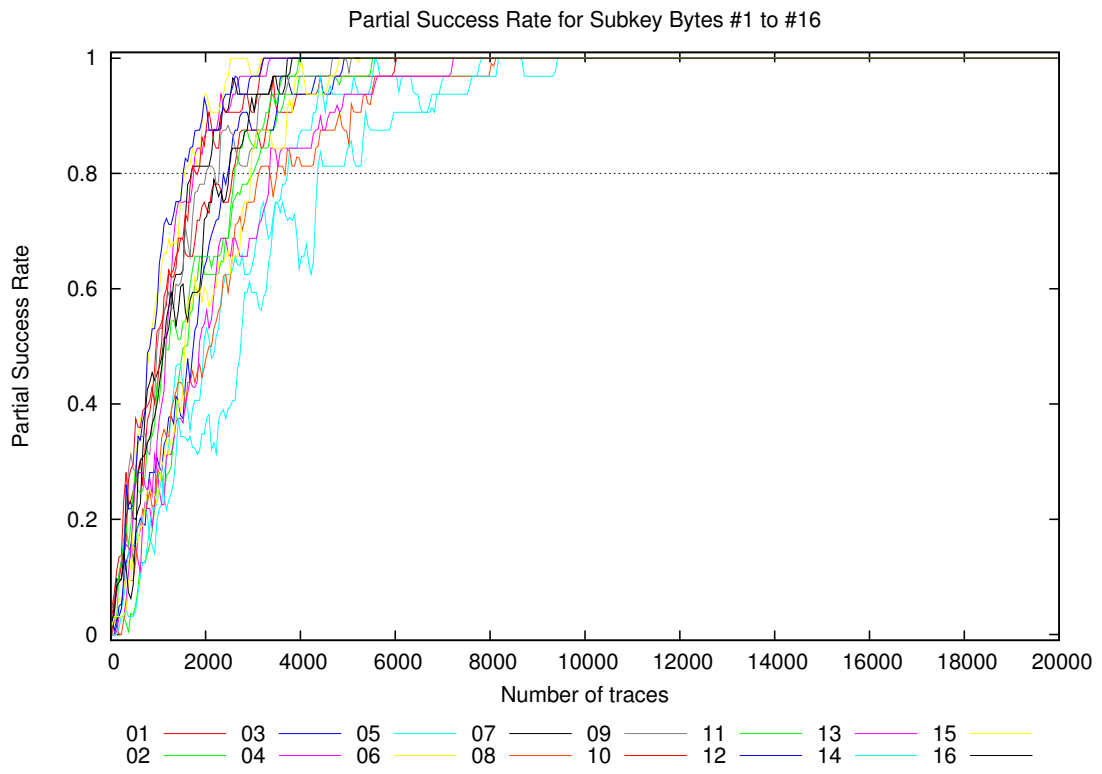






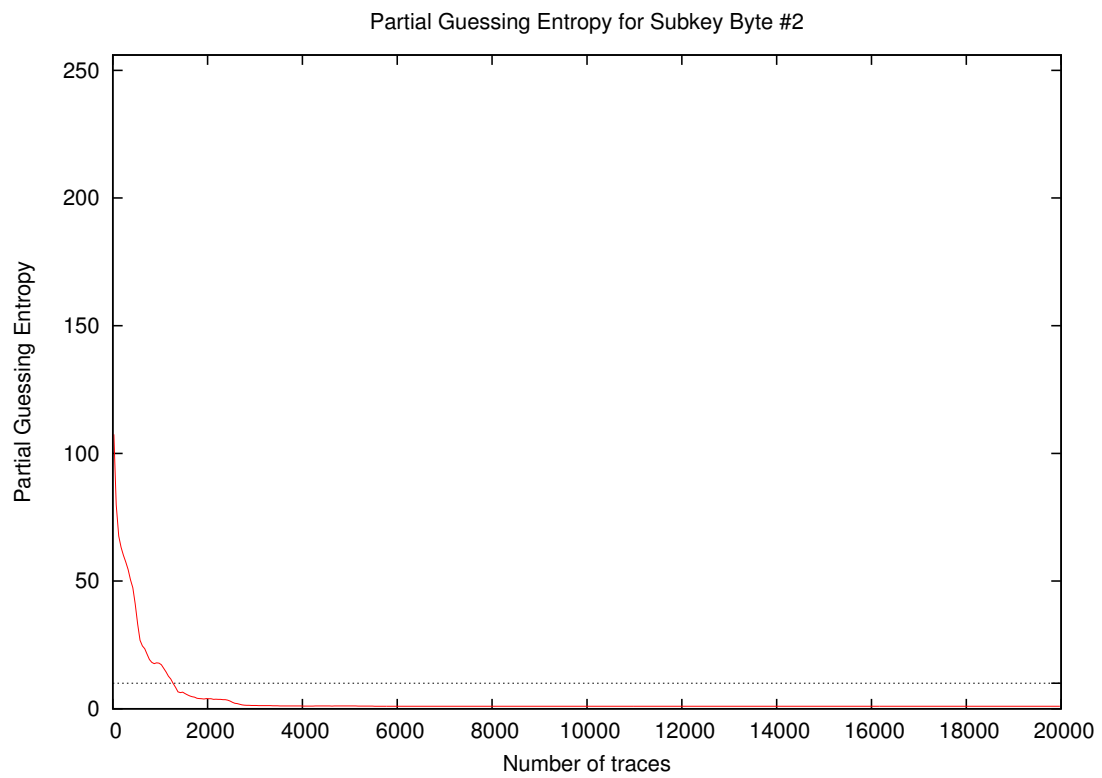
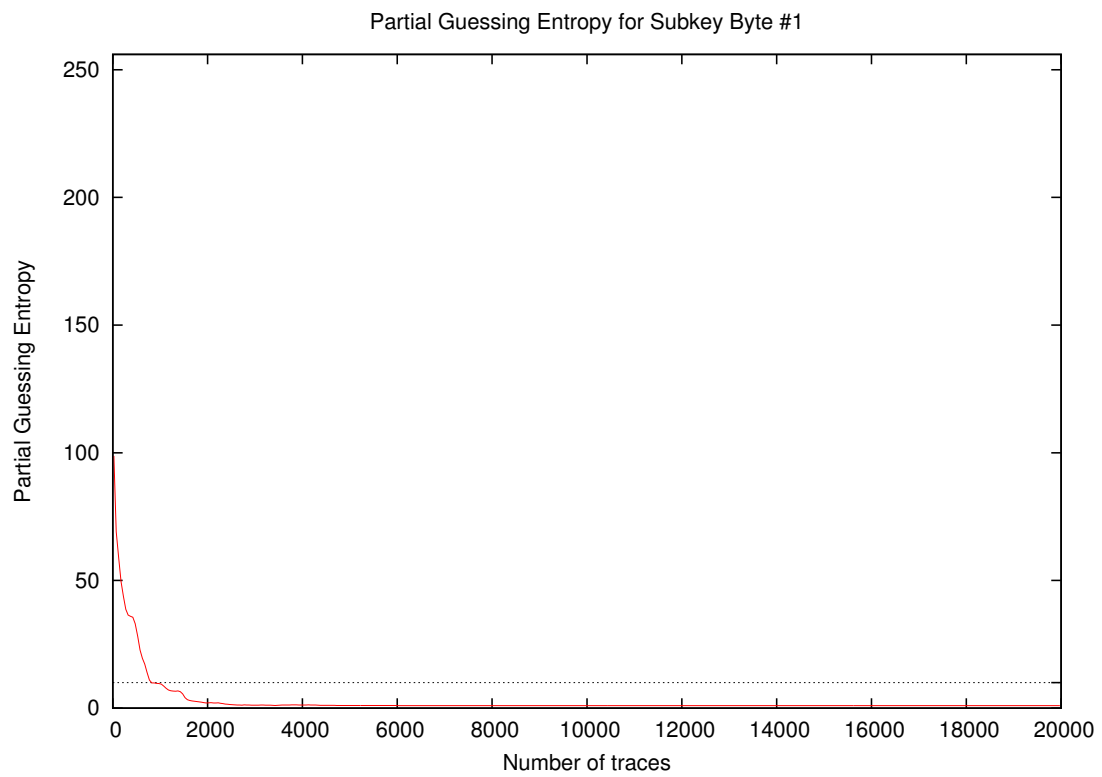


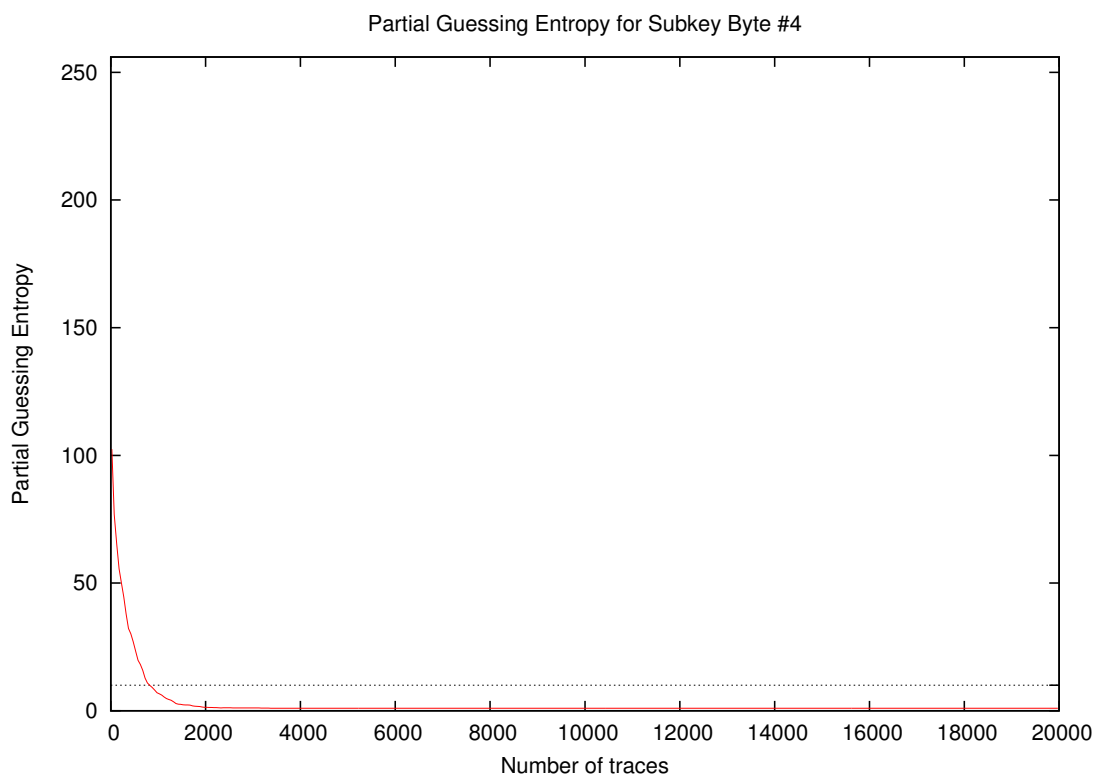
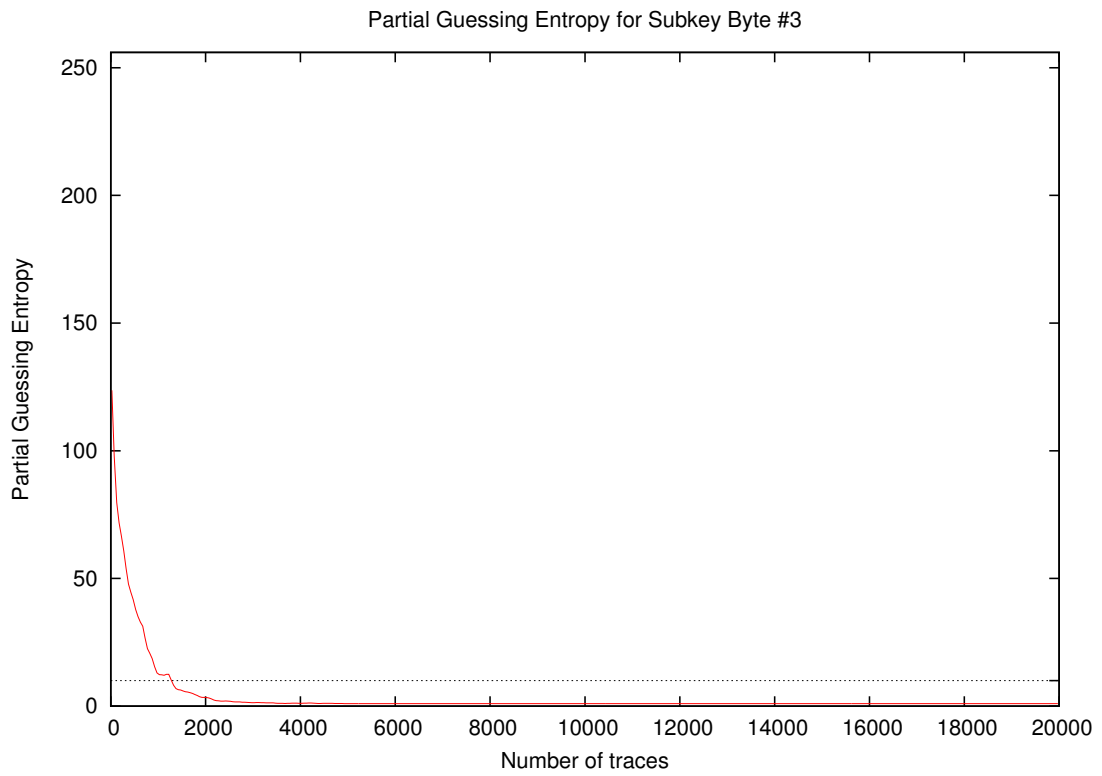


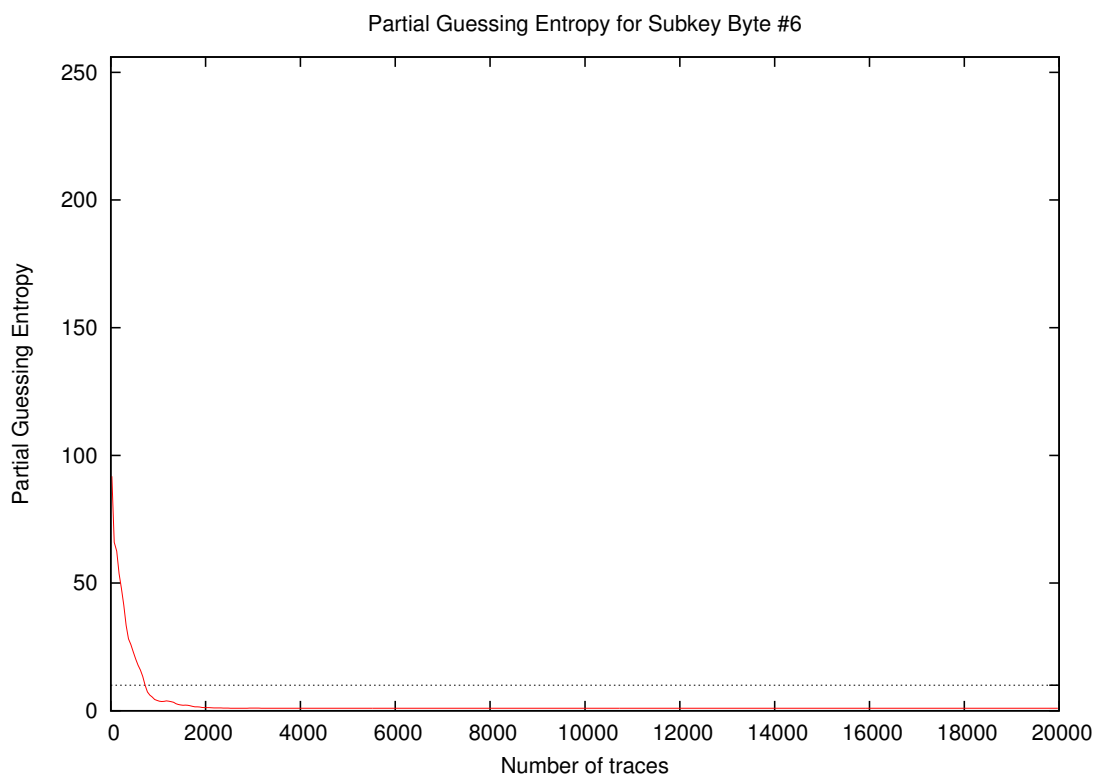
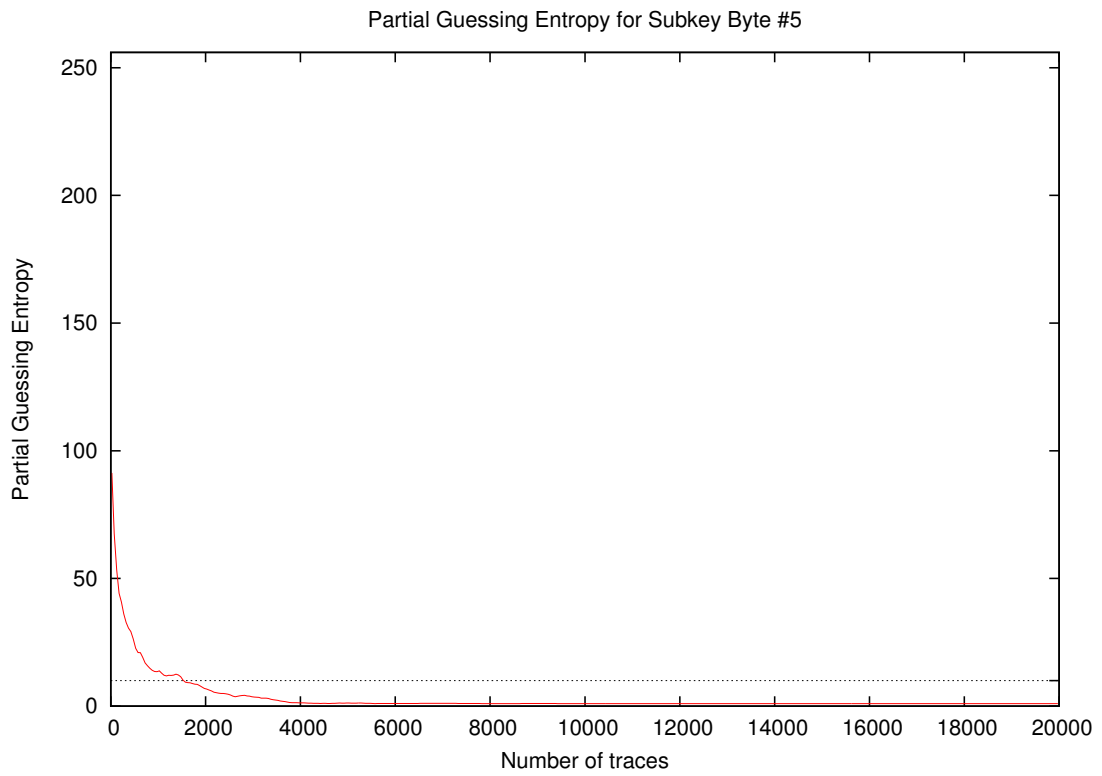


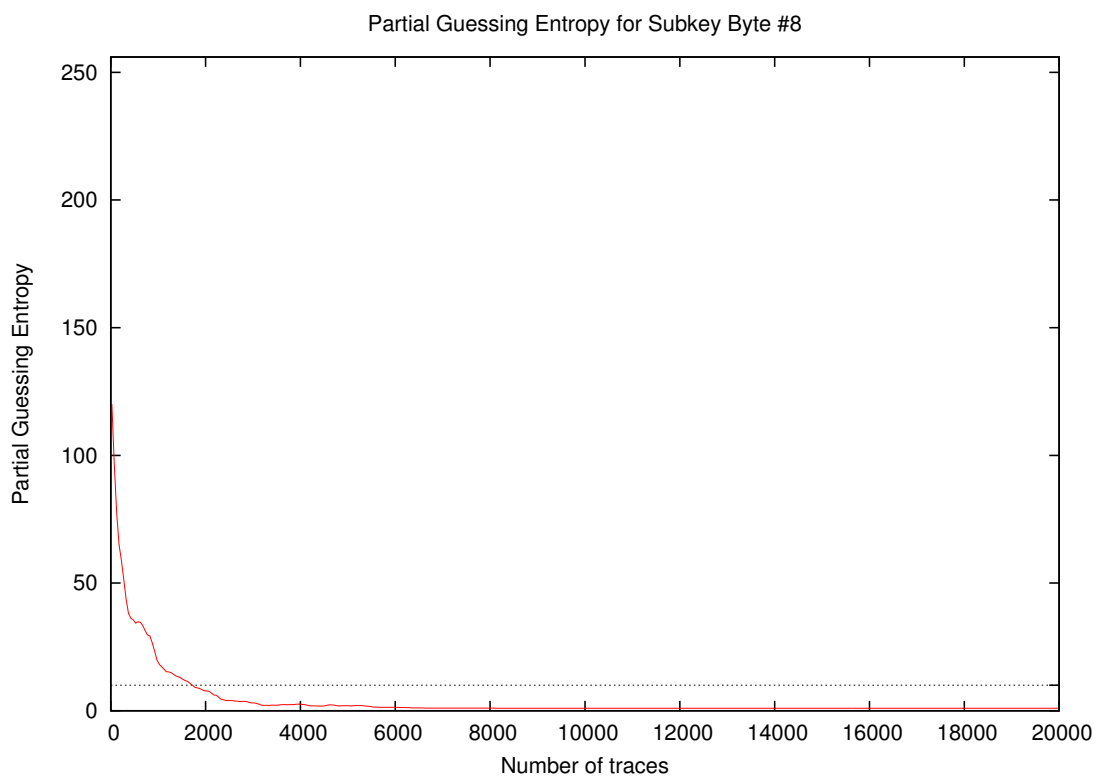
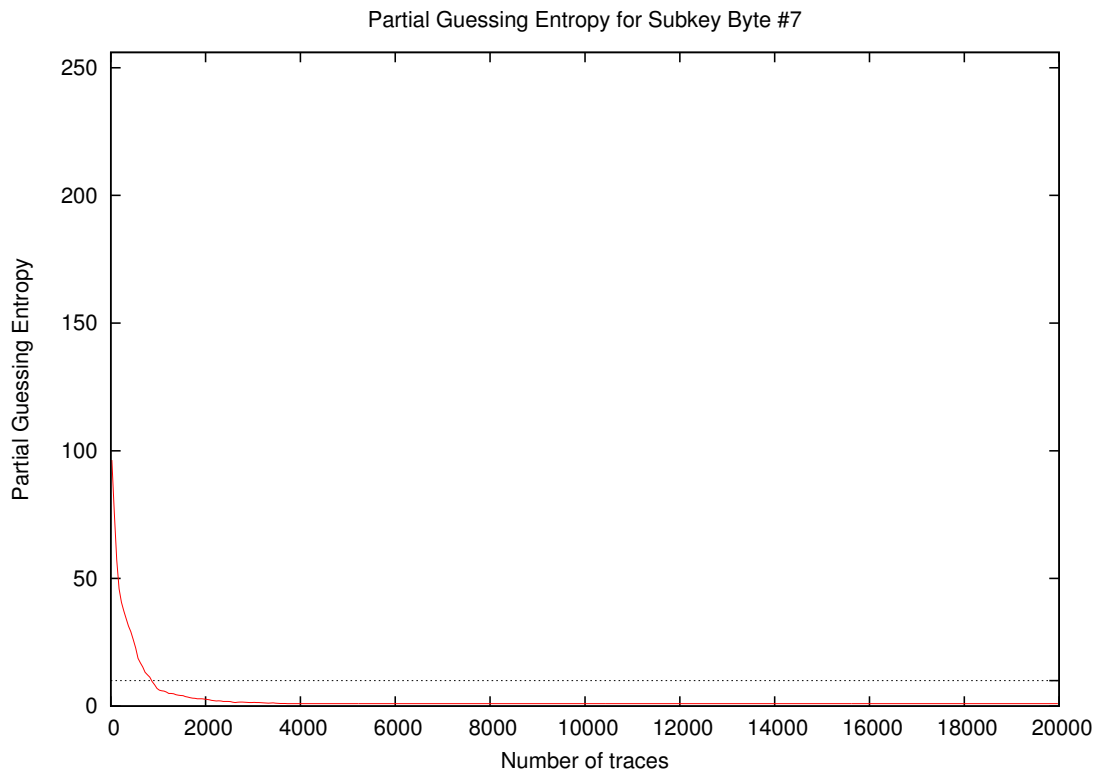
Traces	Partial Success Rate / Byte																Min	Max	Mean
	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16			
10	0.03	0.03	0.00	0.03	0.00	0.03	0.00	0.00	0.03	0.03	0.06	0.00	0.00	0.00	0.00	0.00	0.00	0.06	0.02
20	0.03	0.03	0.00	0.00	0.00	0.00	0.00	0.00	0.03	0.00	0.03	0.03	0.00	0.00	0.00	0.03	0.00	0.03	0.01
30	0.03	0.00	0.00	0.03	0.03	0.03	0.00	0.00	0.06	0.00	0.03	0.00	0.00	0.00	0.03	0.03	0.00	0.06	0.02
40	0.09	0.00	0.00	0.03	0.03	0.03	0.00	0.00	0.03	0.06	0.00	0.03	0.00	0.00	0.03	0.03	0.00	0.09	0.02
50	0.12	0.03	0.00	0.00	0.00	0.03	0.03	0.00	0.06	0.06	0.03	0.00	0.00	0.00	0.03	0.03	0.00	0.12	0.03
100	0.06	0.03	0.00	0.06	0.03	0.06	0.03	0.06	0.06	0.06	0.00	0.00	0.00	0.00	0.03	0.06	0.00	0.06	0.04
200	0.12	0.03	0.06	0.09	0.03	0.06	0.12	0.00	0.12	0.09	0.12	0.03	0.03	0.03	0.03	0.09	0.00	0.12	0.07
300	0.28	0.03	0.12	0.16	0.06	0.09	0.22	0.03	0.19	0.16	0.19	0.22	0.03	0.03	0.03	0.16	0.03	0.28	0.12
400	0.25	0.03	0.16	0.12	0.16	0.16	0.22	0.09	0.31	0.31	0.19	0.22	0.16	0.03	0.09	0.06	0.03	0.31	0.16
500	0.25	0.03	0.12	0.16	0.16	0.25	0.19	0.09	0.28	0.34	0.31	0.25	0.25	0.03	0.16	0.09	0.03	0.34	0.19
1000	0.53	0.28	0.31	0.38	0.22	0.59	0.44	0.28	0.53	0.44	0.41	0.62	0.25	0.25	0.25	0.41	0.22	0.62	0.39
2000	0.75	0.62	0.62	0.88	0.53	0.94	0.81	0.47	0.78	0.84	0.66	0.94	0.56	0.38	0.59	0.72	0.38	0.94	0.69
3000	0.88	0.78	0.88	0.97	0.66	0.97	0.94	0.75	0.84	0.91	0.84	0.97	0.69	0.59	0.84	0.91	0.59	0.97	0.84
4000	0.94	0.97	0.94	1.00	0.88	1.00	1.00	0.81	0.97	1.00	1.00	1.00	0.84	0.66	1.00	1.00	0.66	1.00	0.94
5000	0.97	0.97	1.00	1.00	0.94	1.00	1.00	0.84	0.97	1.00	1.00	1.00	0.94	0.84	1.00	1.00	0.84	1.00	0.97
10000	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	1.00	1.00
15000	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	1.00	1.00
20000	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	1.00	1.00

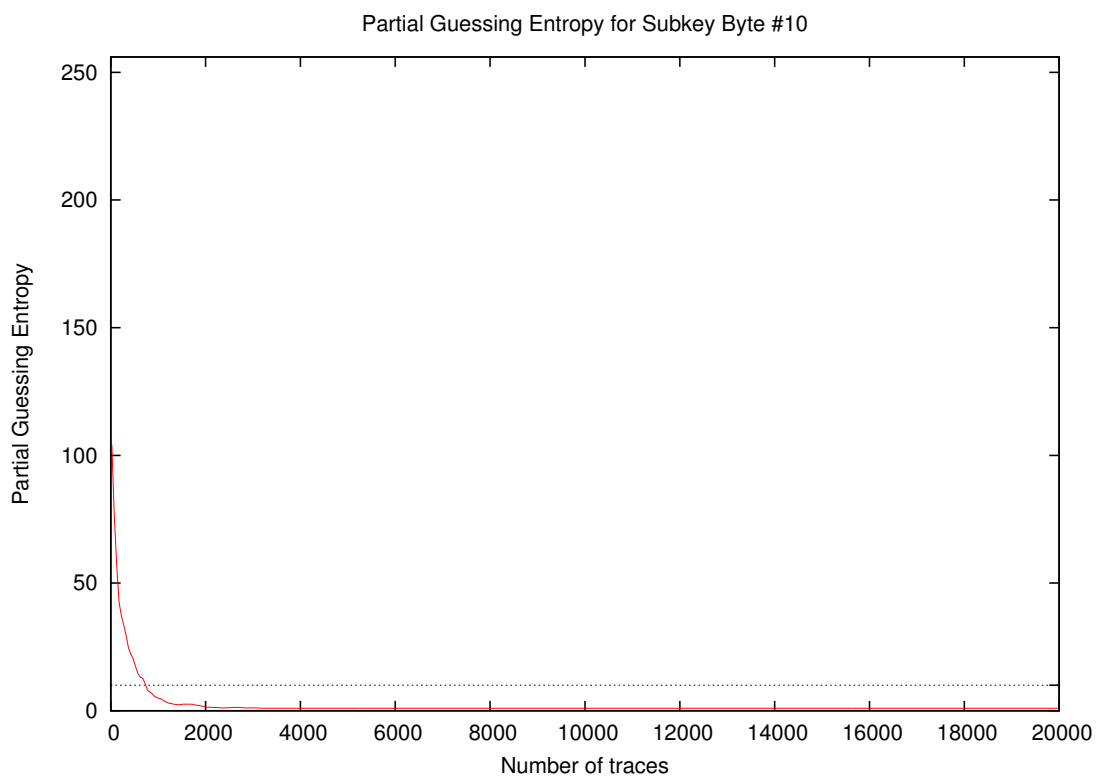
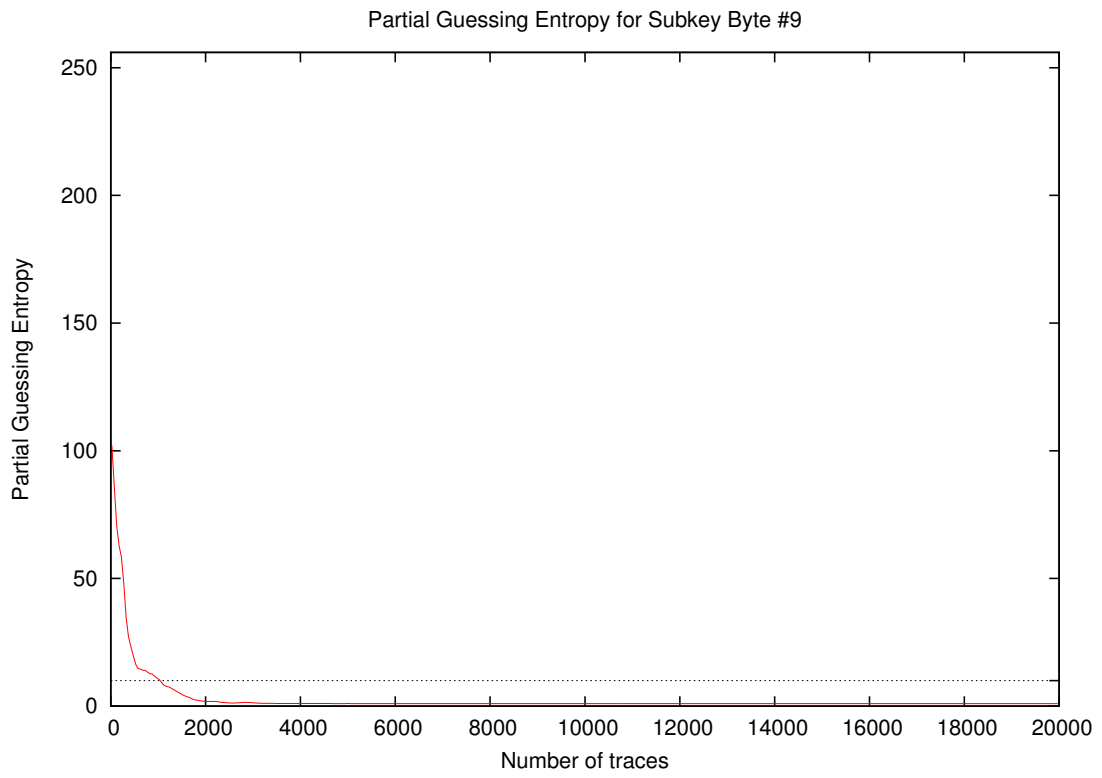
4 Partial Guessing Entropy

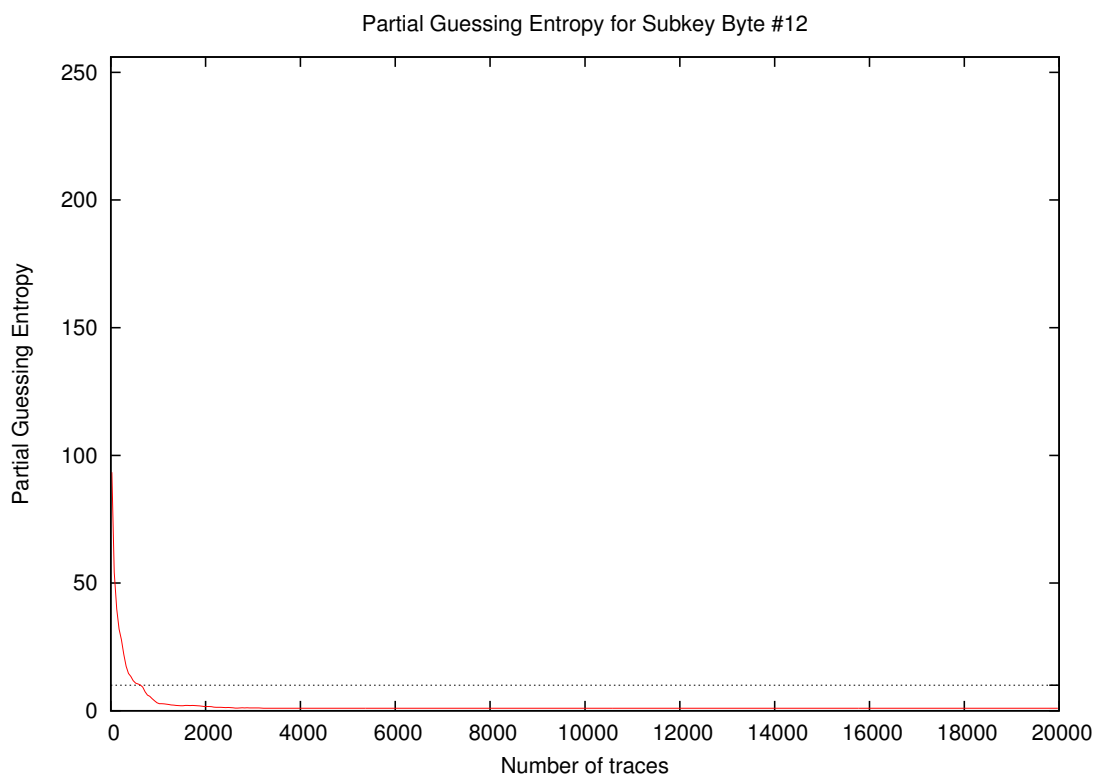
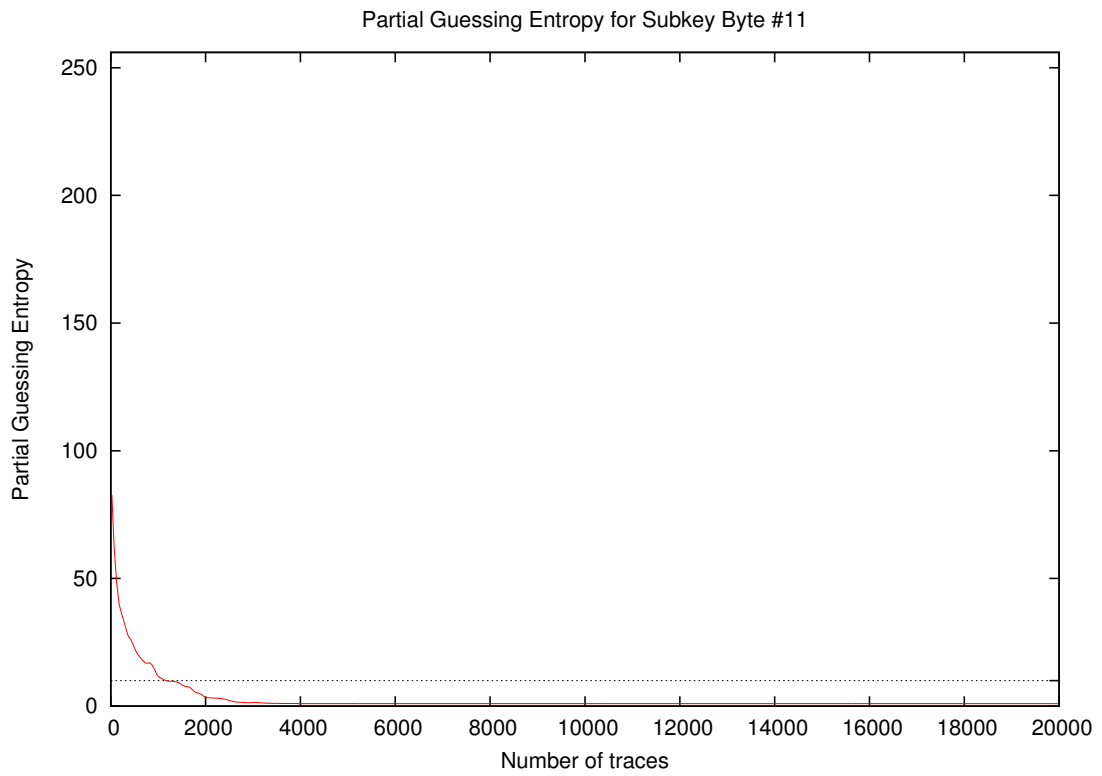


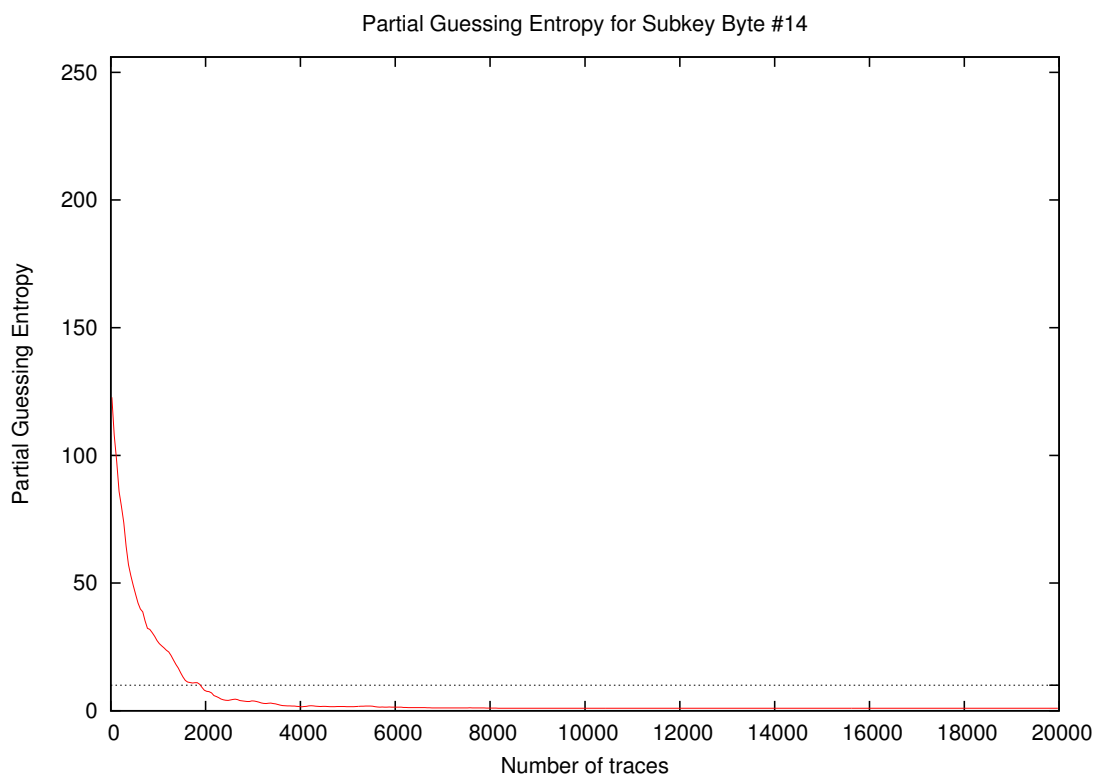
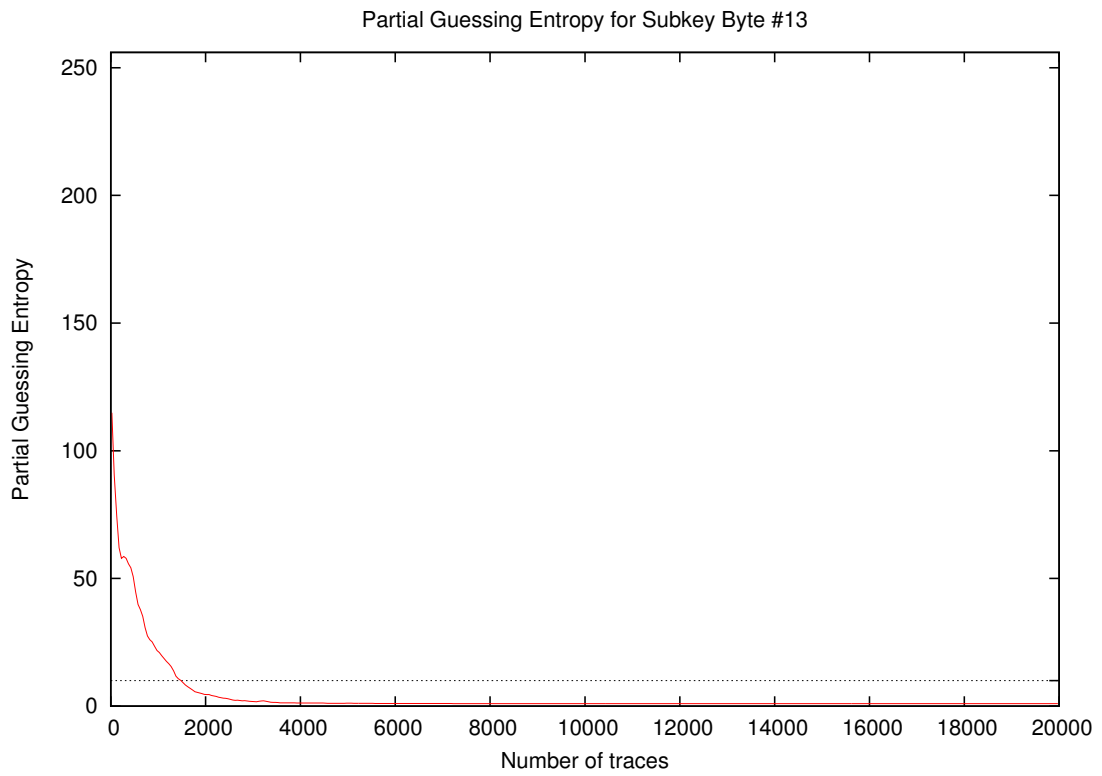


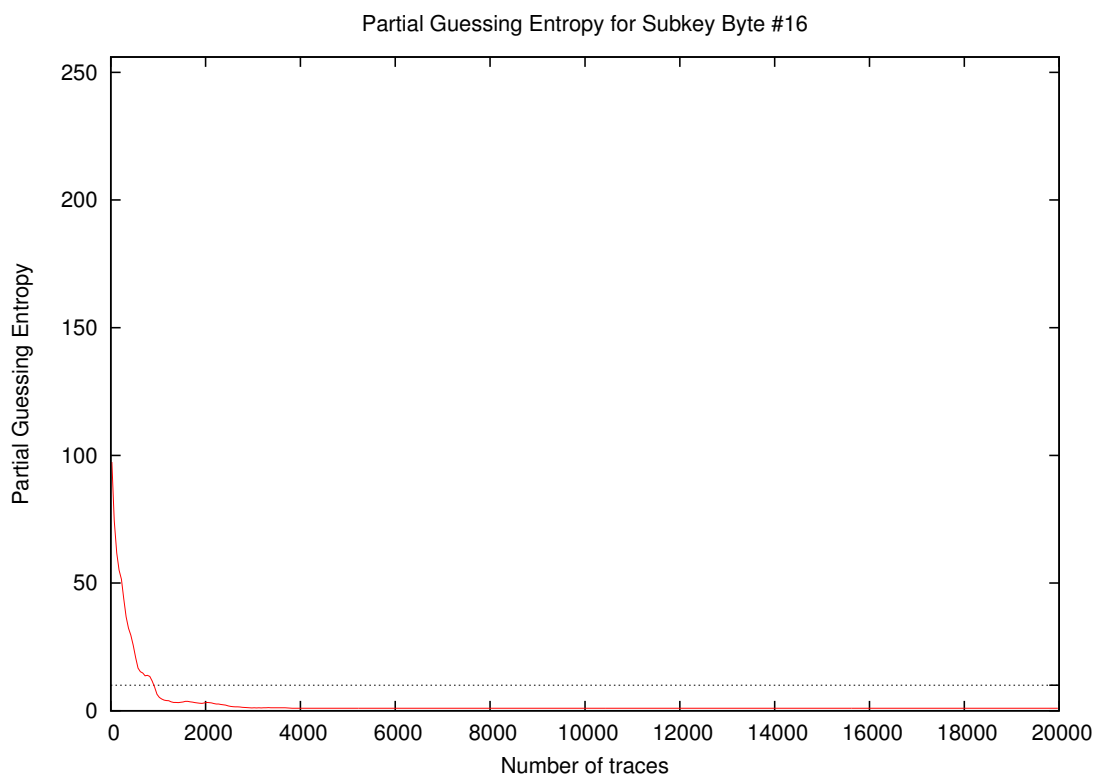
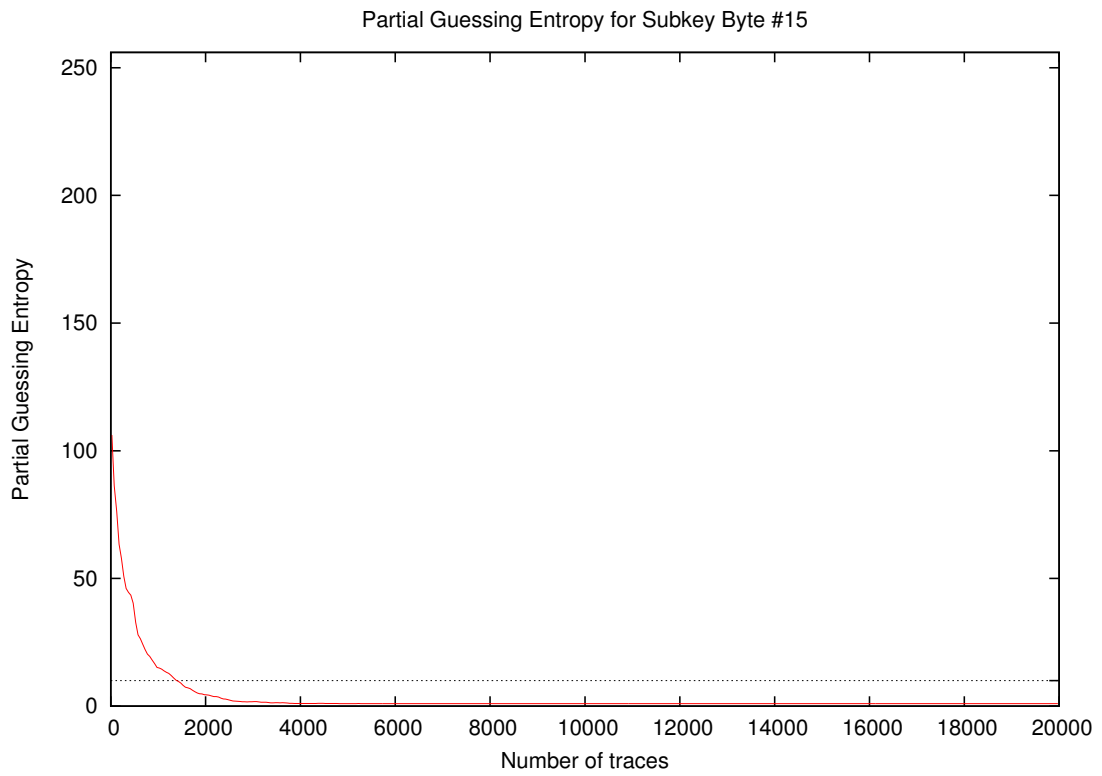


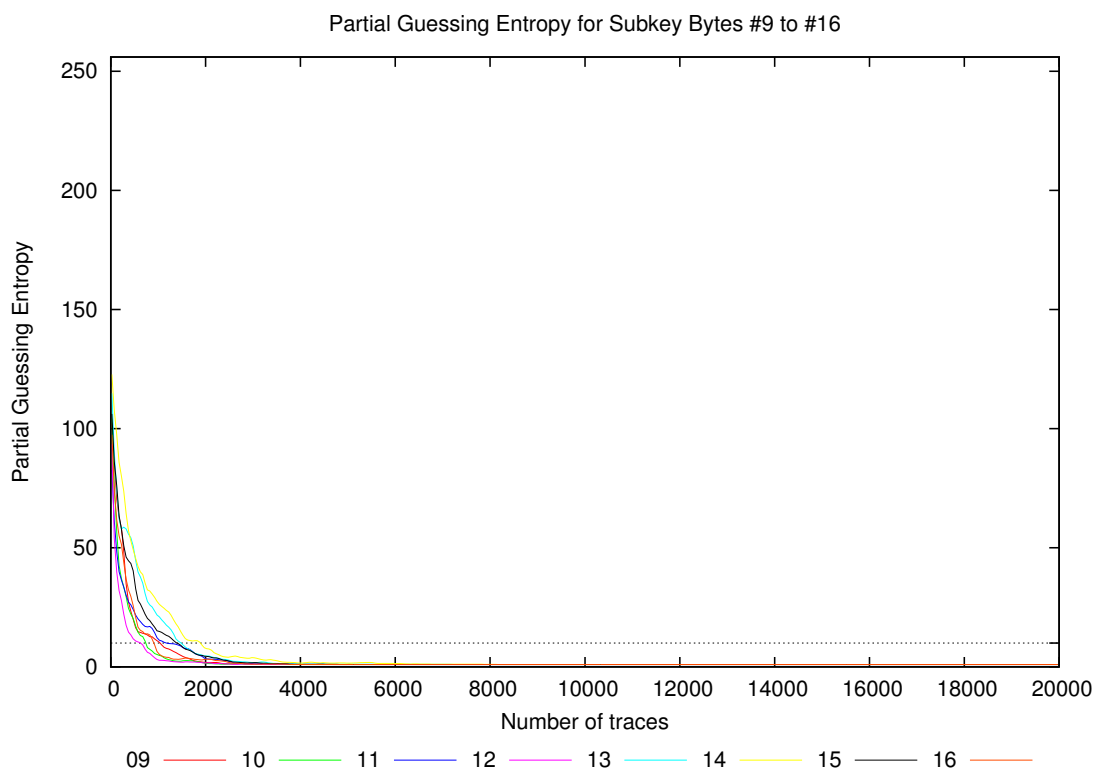
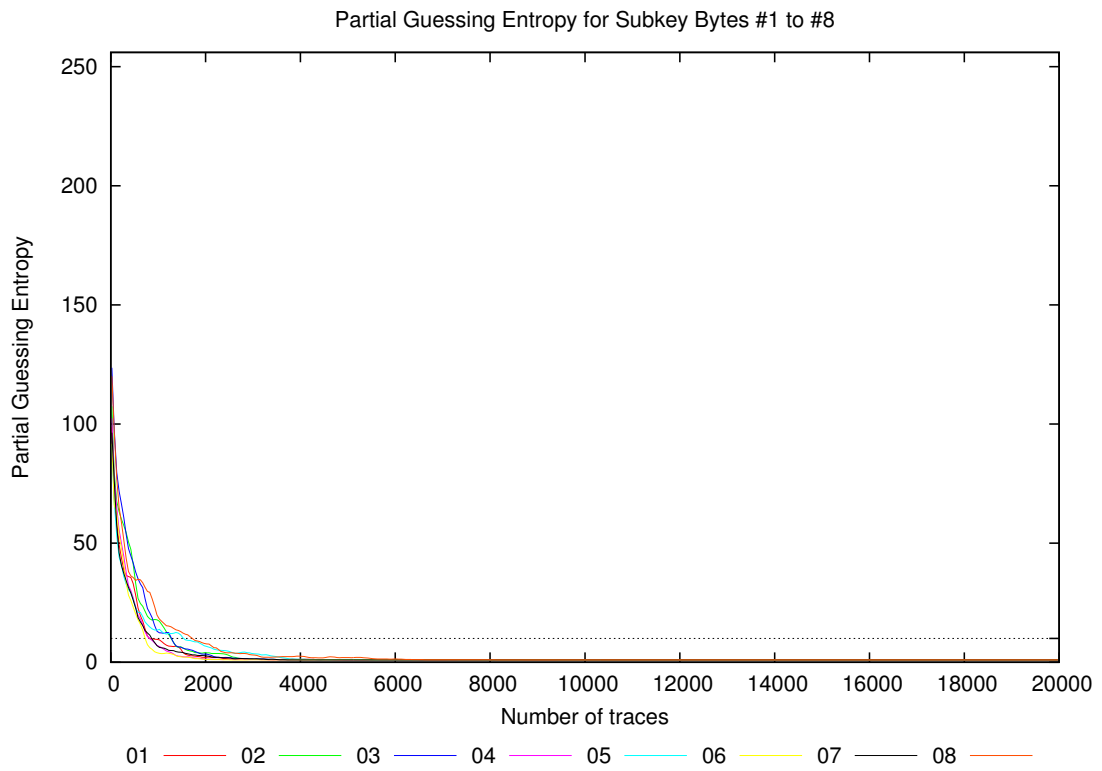


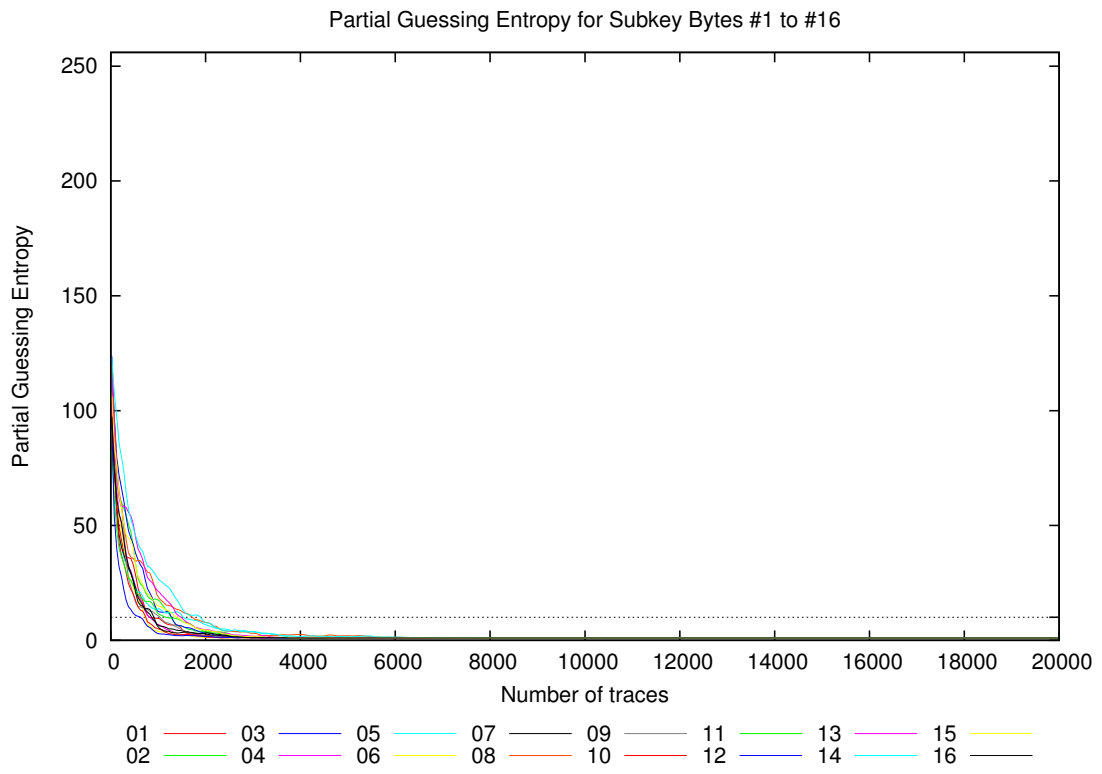












Traces	Partial Guessing Entropy / Byte																Min	Max	Mean
	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16			
10	113.2	114.6	134.9	106.2	105.4	105.5	101.2	107.7	109.1	109.9	90.1	112.8	122.2	125.3	111.3	95.6	90.1	134.9	110.3
20	100.9	105.2	118.9	102.3	86.0	91.2	94.9	118.2	98.5	103.8	77.5	99.6	113.4	123.7	100.9	91.6	77.5	123.7	101.7
30	92.2	101.0	115.8	98.5	80.5	79.8	86.8	123.2	95.9	98.3	72.9	83.5	108.6	117.3	96.6	92.6	72.9	123.2	96.5
40	82.8	96.2	111.7	92.3	78.2	74.0	86.6	119.1	92.7	94.5	70.3	69.9	103.7	113.6	95.7	87.2	69.9	119.1	91.8
50	76.5	91.1	108.3	86.5	76.8	69.8	84.4	113.3	91.6	89.9	67.9	61.6	100.6	110.9	92.6	84.4	61.6	113.3	87.9
100	64.0	71.8	87.7	70.3	60.3	62.9	66.4	86.2	77.4	65.7	54.1	46.4	82.1	102.3	81.7	66.6	46.4	102.3	71.6
200	45.5	61.2	68.3	51.3	41.9	49.2	41.6	60.5	59.8	38.0	37.0	29.8	57.1	80.8	59.2	53.3	29.8	80.8	52.1
300	37.2	56.1	57.2	41.6	34.0	37.3	35.8	47.3	41.1	31.4	31.7	19.3	59.2	68.9	48.0	39.9	19.3	68.9	42.9
400	35.8	49.1	45.4	31.1	29.6	26.9	30.1	36.4	24.1	22.6	26.6	13.8	54.9	54.1	44.2	30.5	13.8	54.9	34.7
500	31.0	37.6	39.8	25.3	24.5	21.7	24.6	34.8	18.0	18.8	23.0	11.3	47.6	47.0	37.1	23.4	11.3	47.6	29.1
1000	9.5	17.6	12.2	6.8	14.0	3.8	6.4	18.4	10.8	4.8	11.2	2.8	21.1	26.4	14.8	5.3	2.8	26.4	11.6
2000	2.1	3.9	3.4	1.3	6.8	1.2	2.7	7.7	1.9	1.5	3.4	1.6	4.5	7.6	4.4	3.3	1.2	7.7	3.6
3000	1.2	1.3	1.3	1.1	3.6	1.0	1.4	3.1	1.3	1.1	1.4	1.1	1.8	3.9	1.8	1.2	1.0	3.9	1.7
4000	1.2	1.1	1.1	1.0	1.2	1.0	1.0	2.5	1.0	1.0	1.0	1.0	1.2	1.5	1.0	1.0	1.0	2.5	1.2
5000	1.1	1.1	1.0	1.0	1.2	1.0	1.0	2.0	1.0	1.0	1.0	1.0	1.2	1.6	1.0	1.0	1.0	2.0	1.1
10000	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
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