

Evaluation results

DPA contest v2

November 2010

1 Introduction

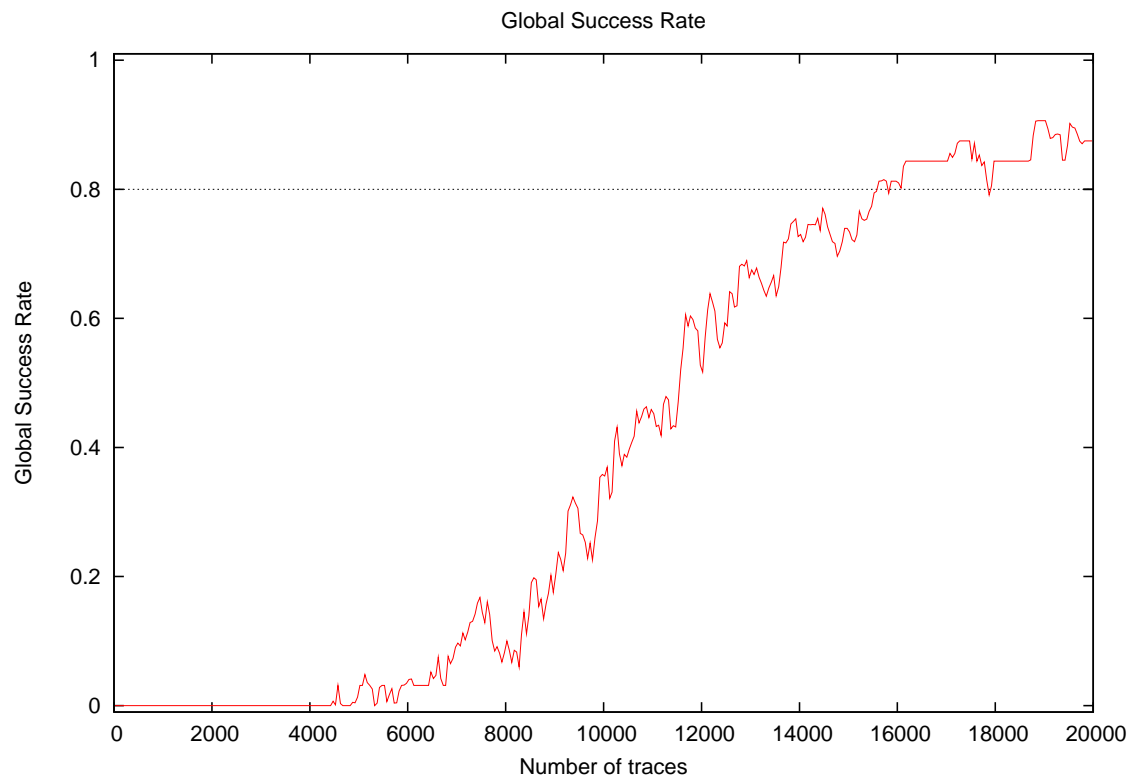
1.1 About the attack

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

1.2 About the evaluation

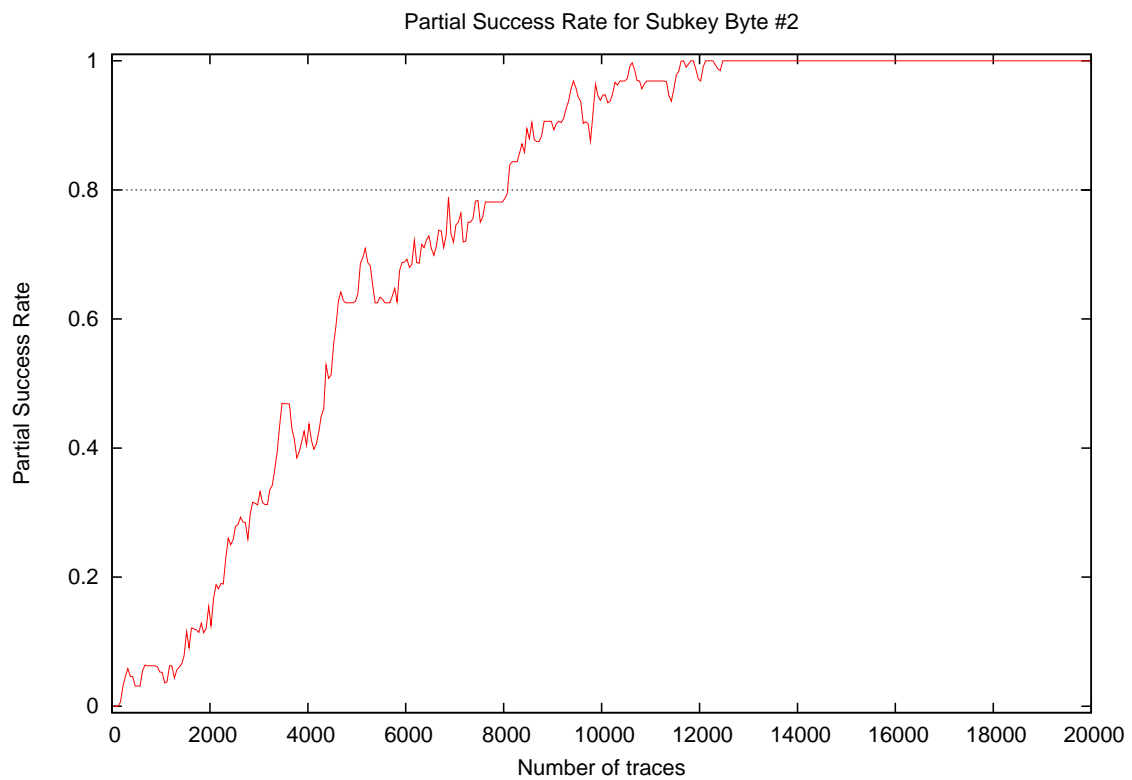
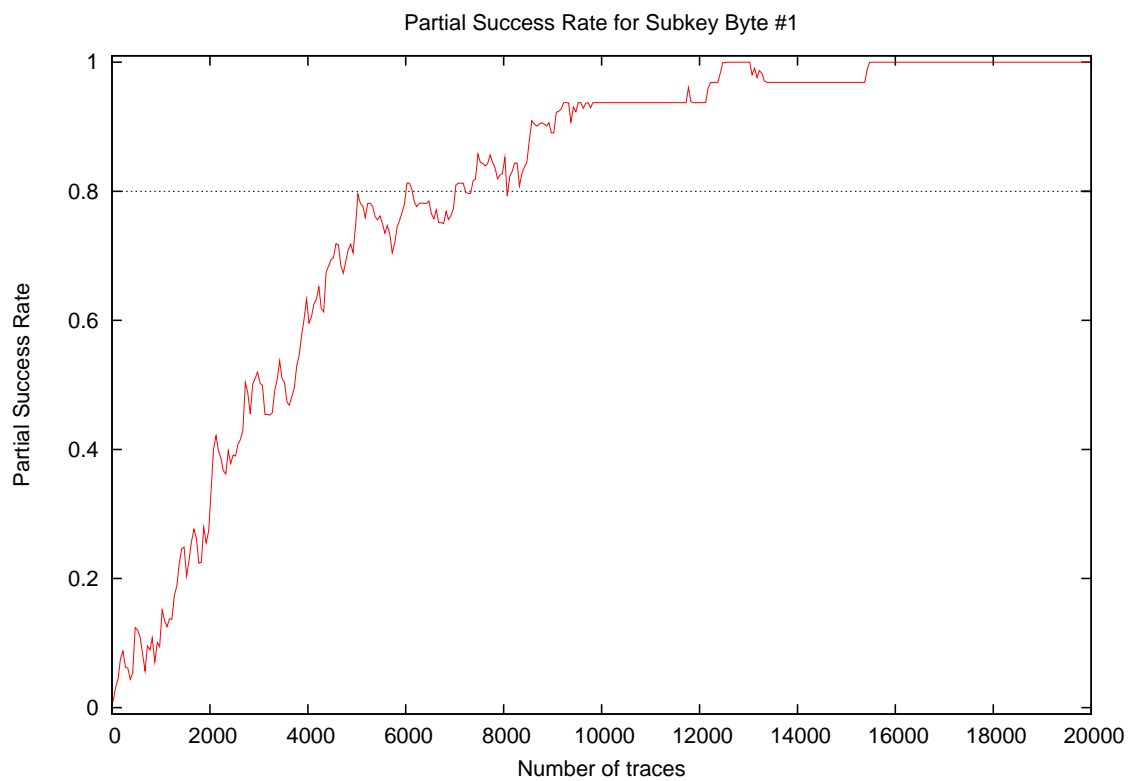
- **Date of evaluation:** November 2010

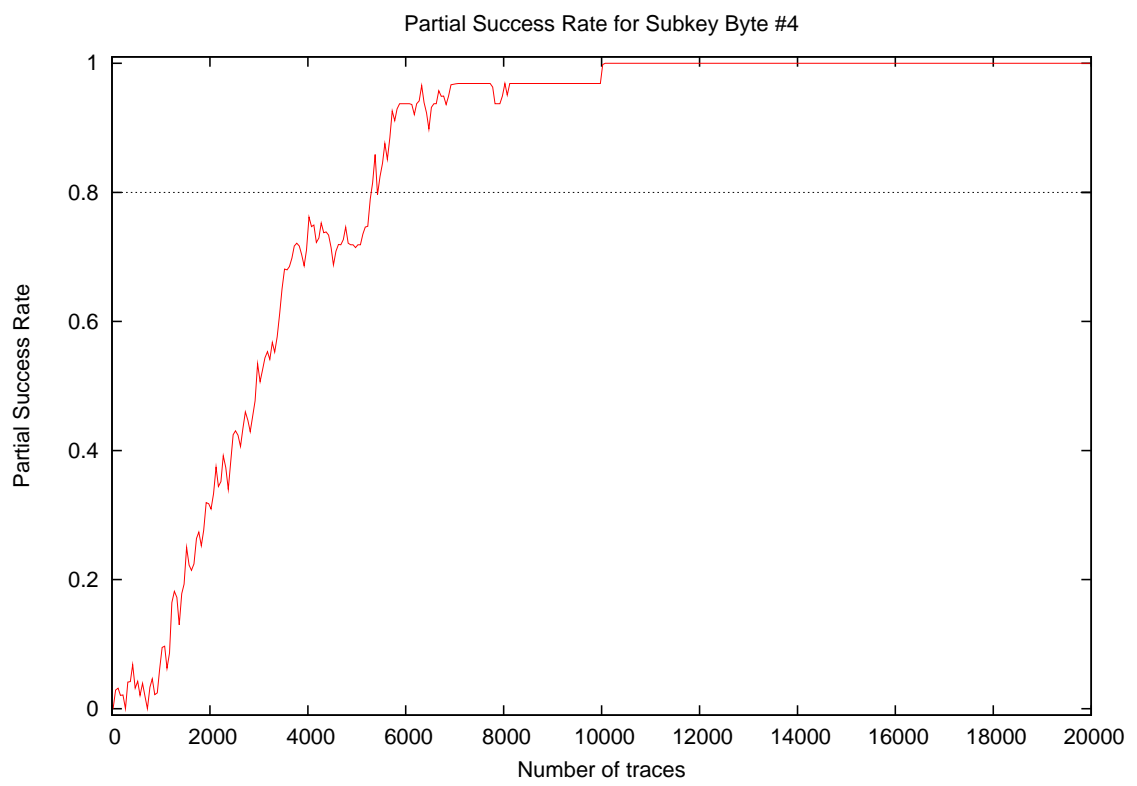
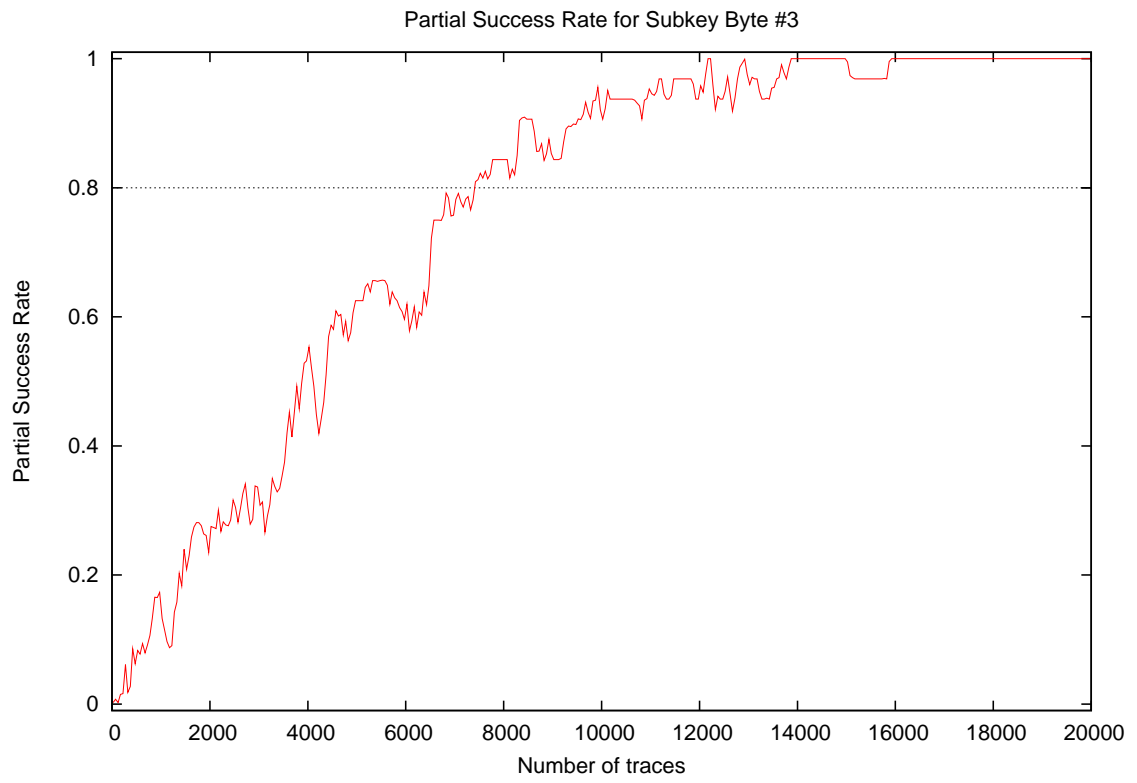
2 Global Success Rate

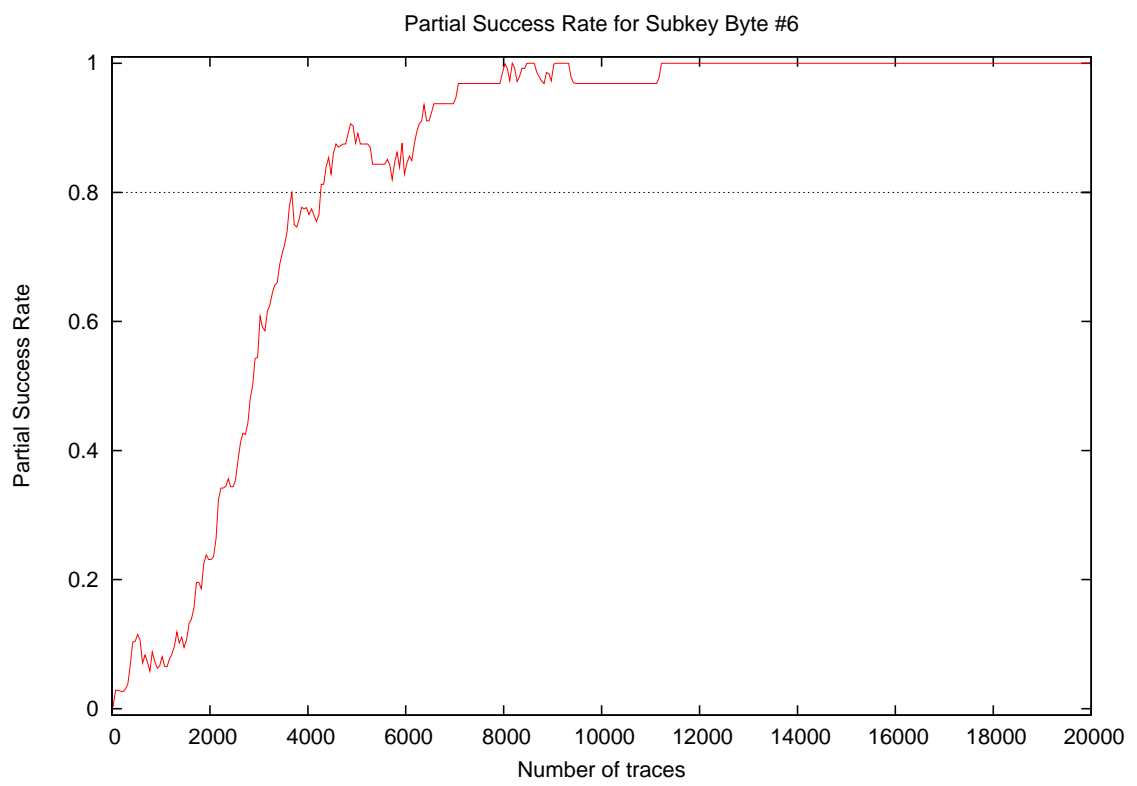
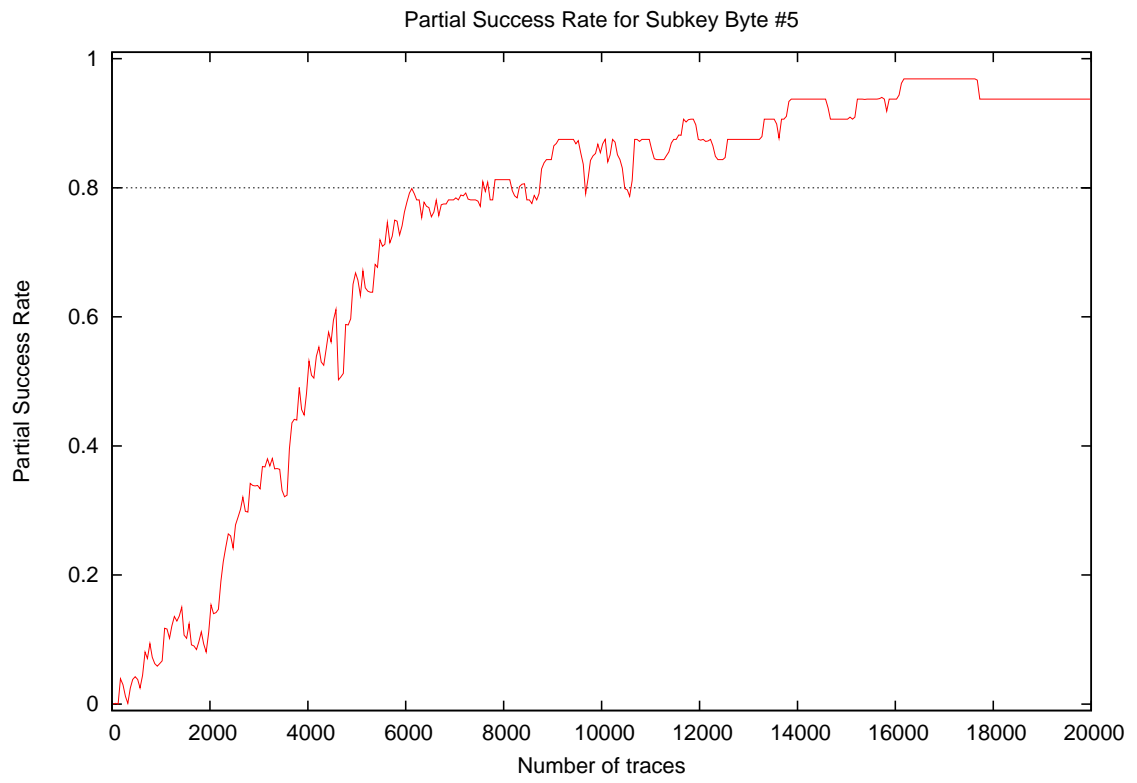


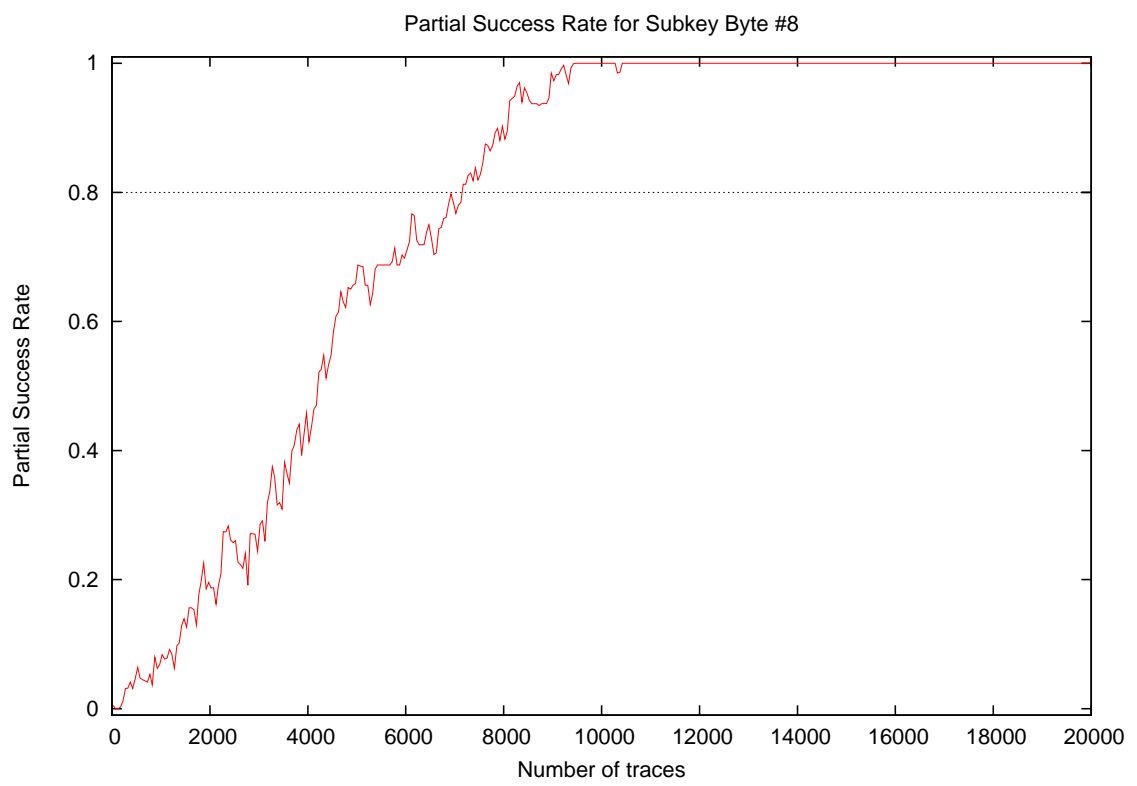
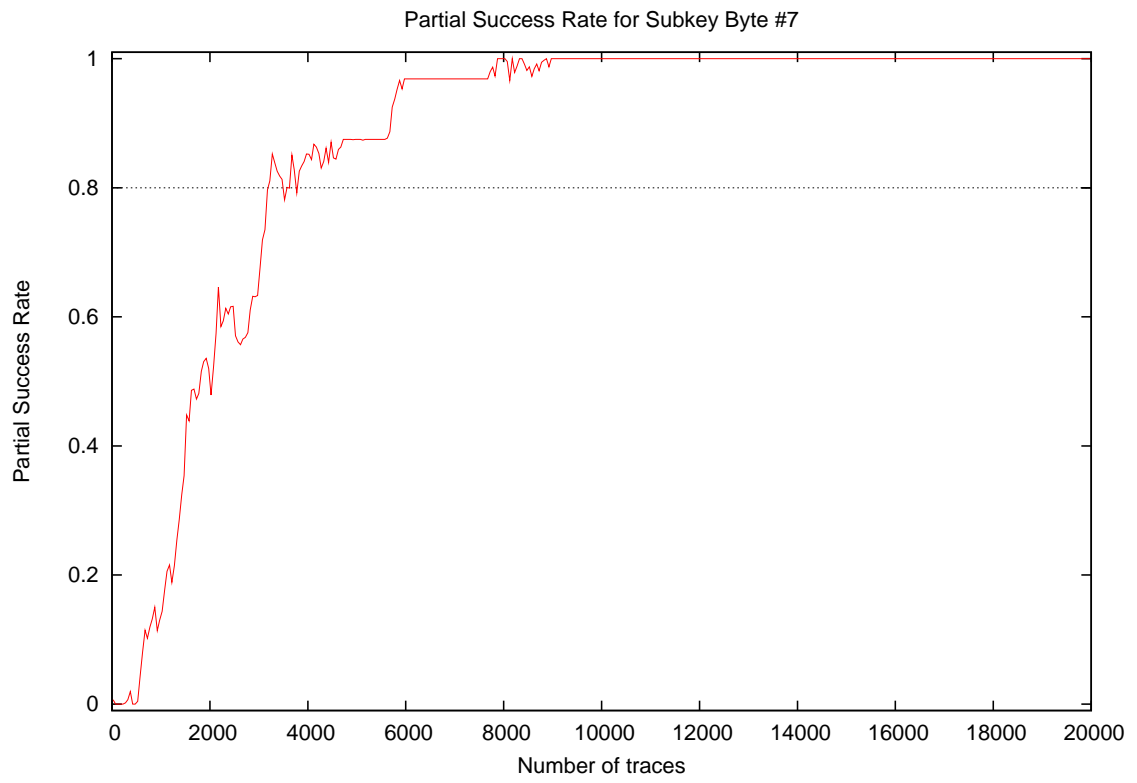
Number of traces	Global Success Rate
10	0.00
20	0.00
30	0.00
40	0.00
50	0.00
100	0.00
200	0.00
300	0.00
400	0.00
500	0.00
1000	0.00
2000	0.00
3000	0.00
4000	0.00
5000	0.03
10000	0.34
15000	0.72
20000	0.88

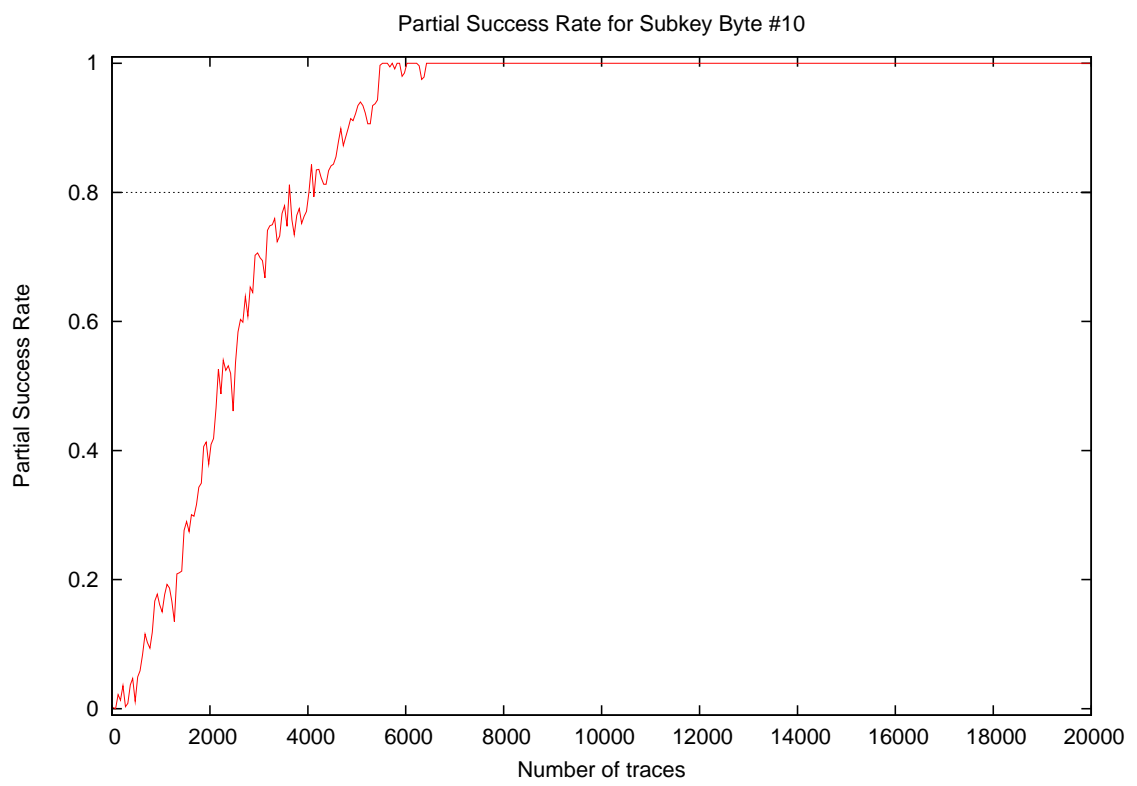
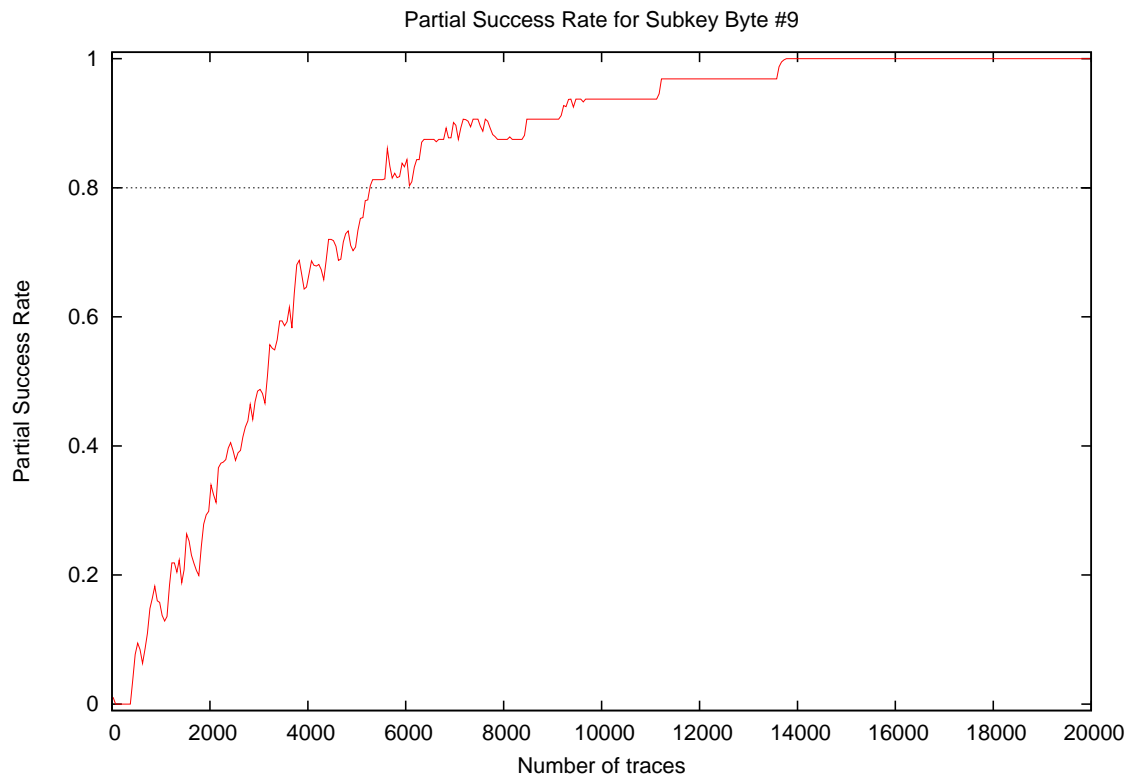
3 Partial Success Rate

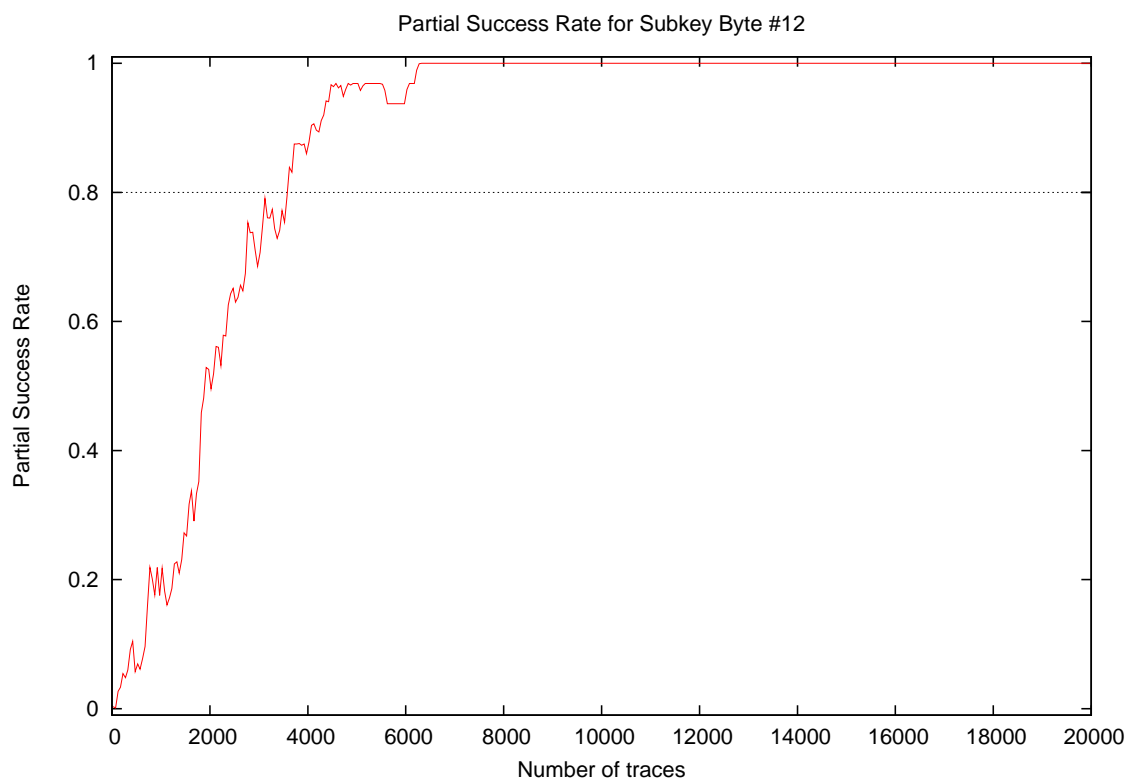
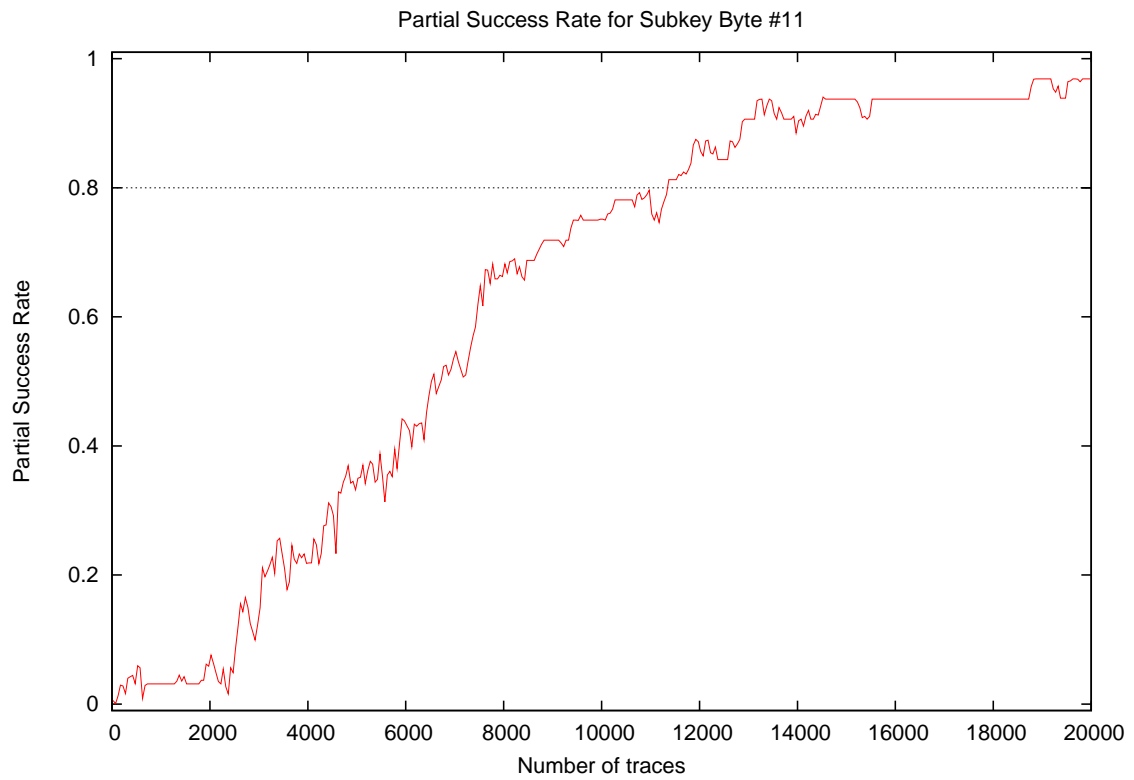


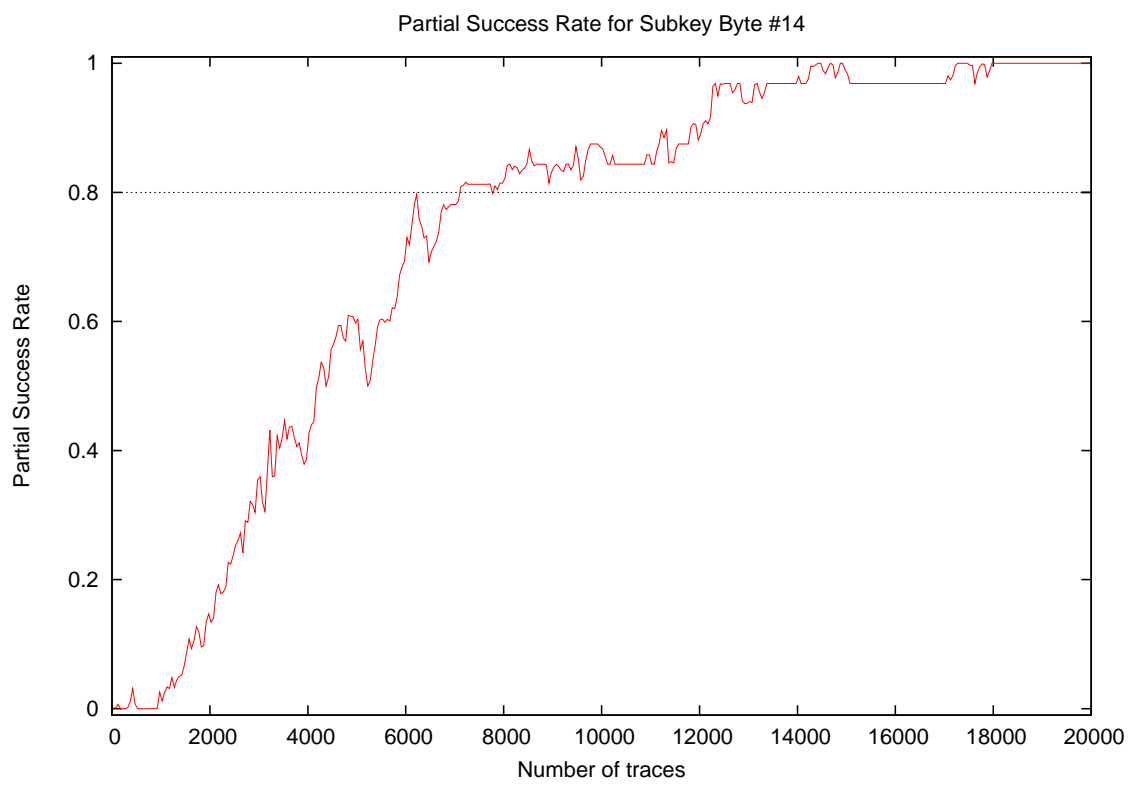
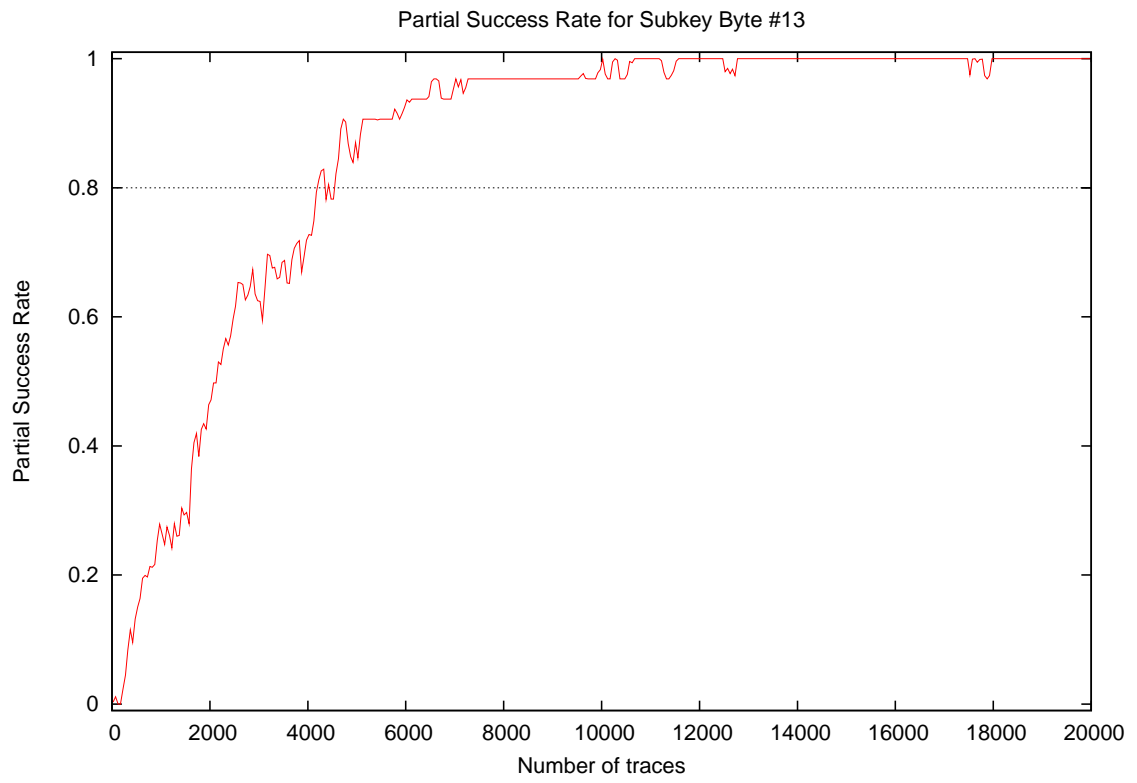


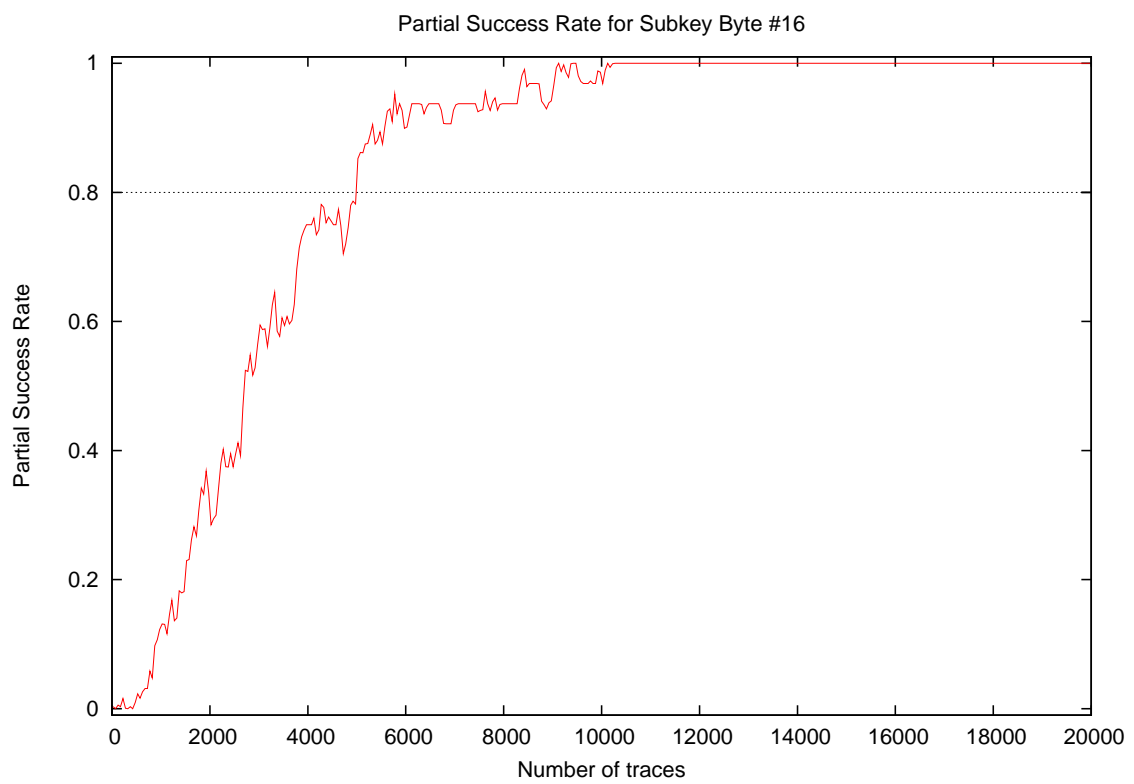
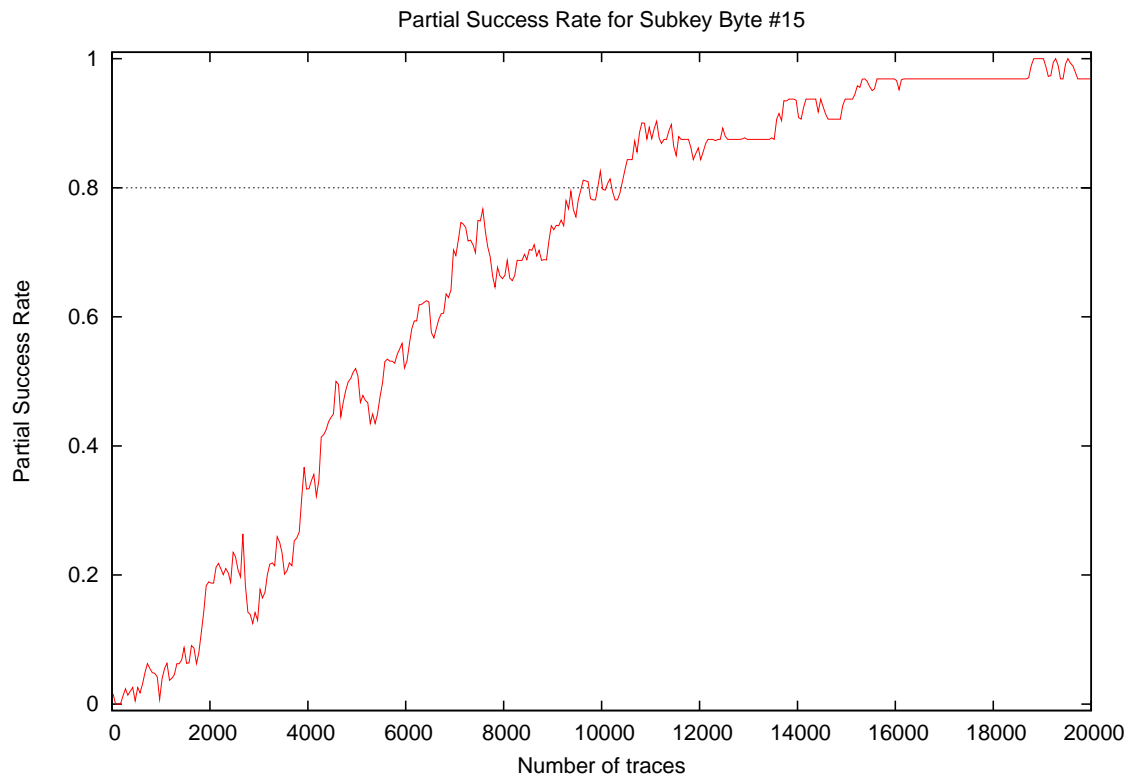


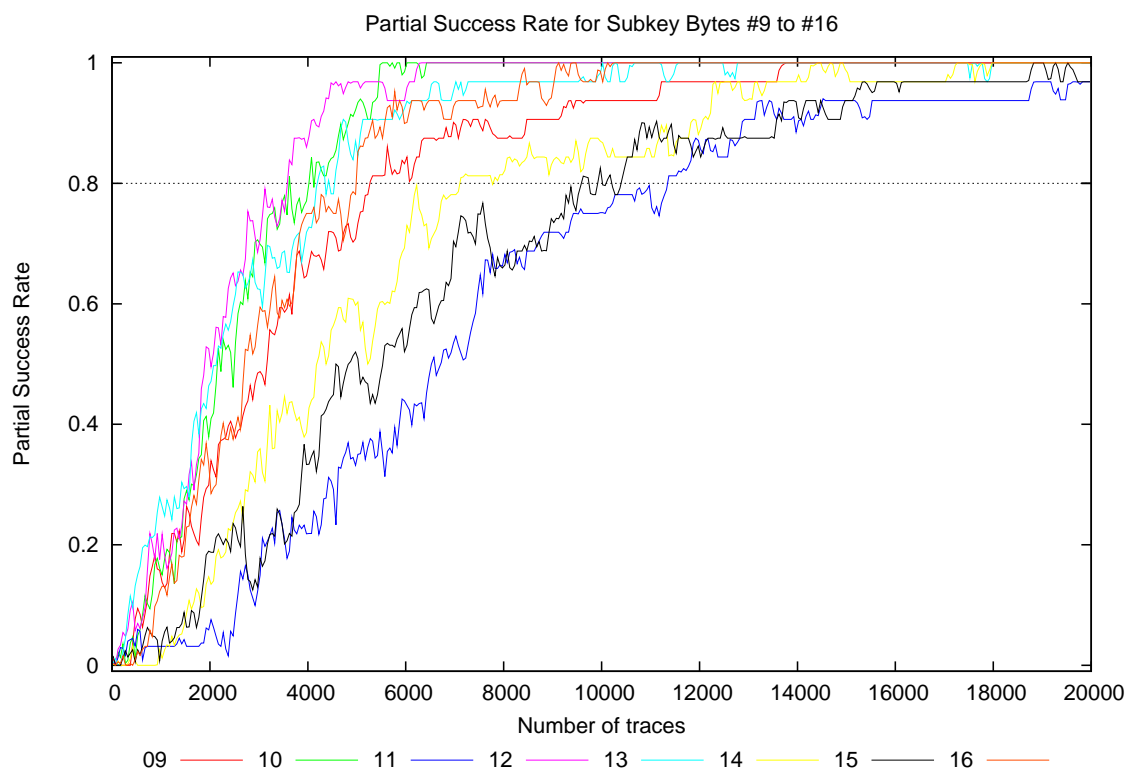
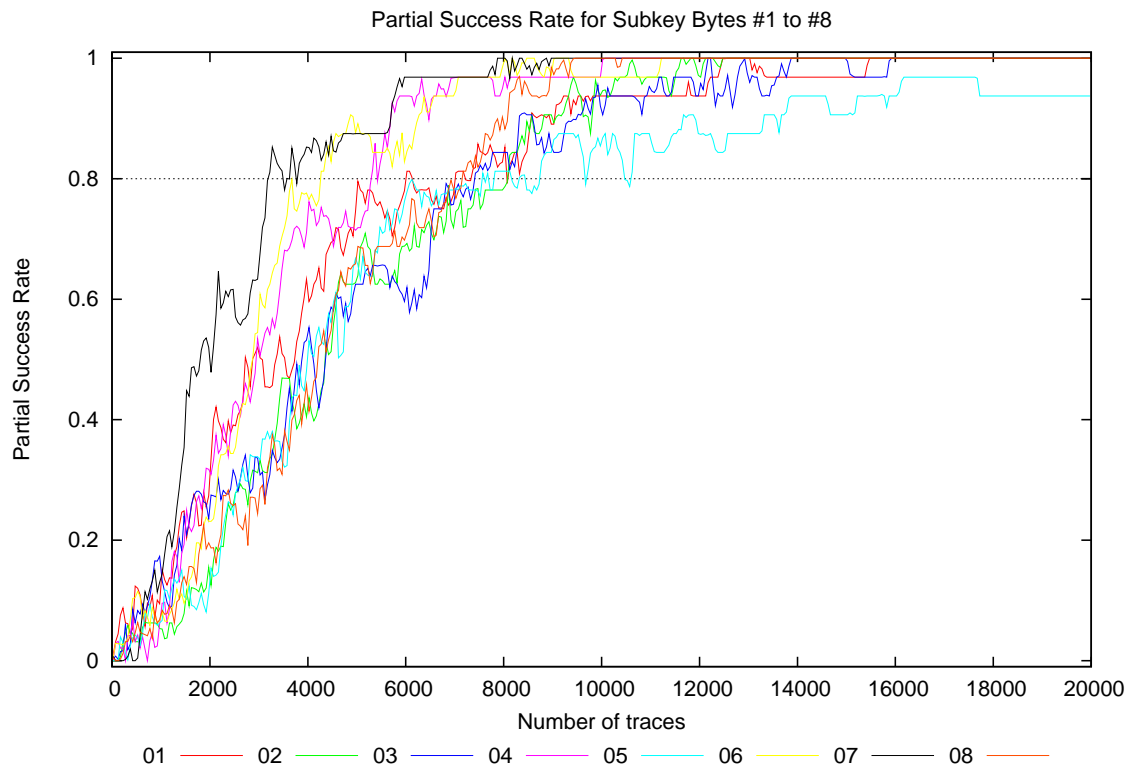




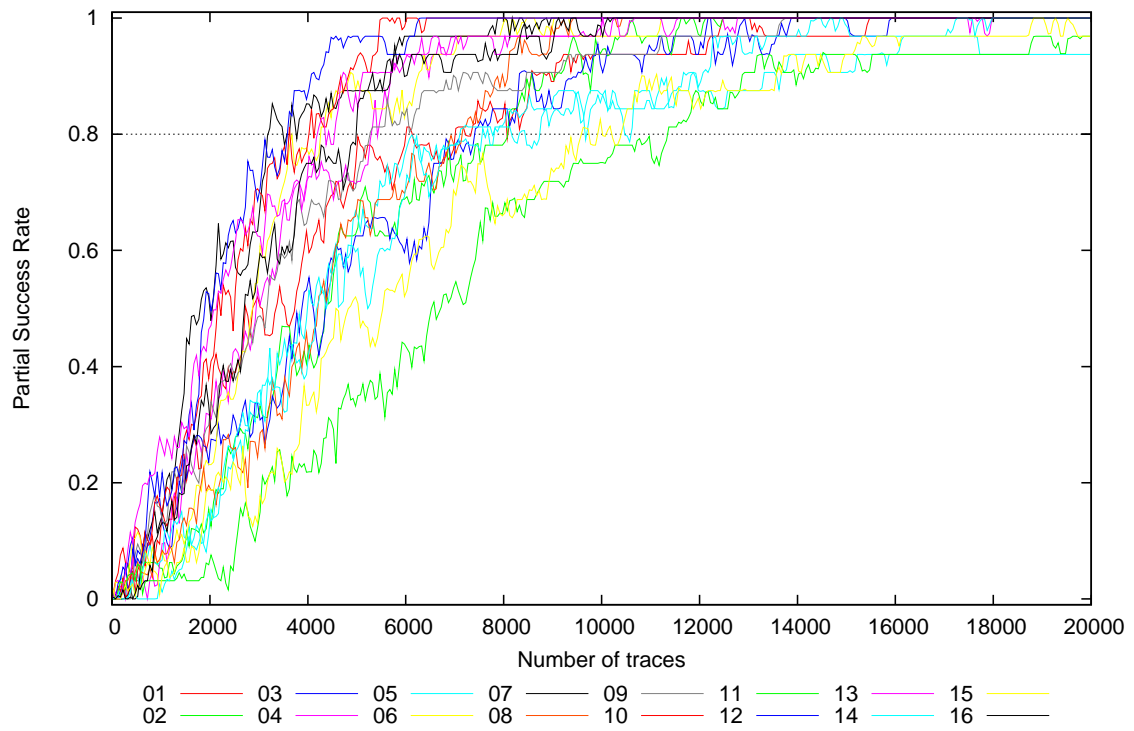






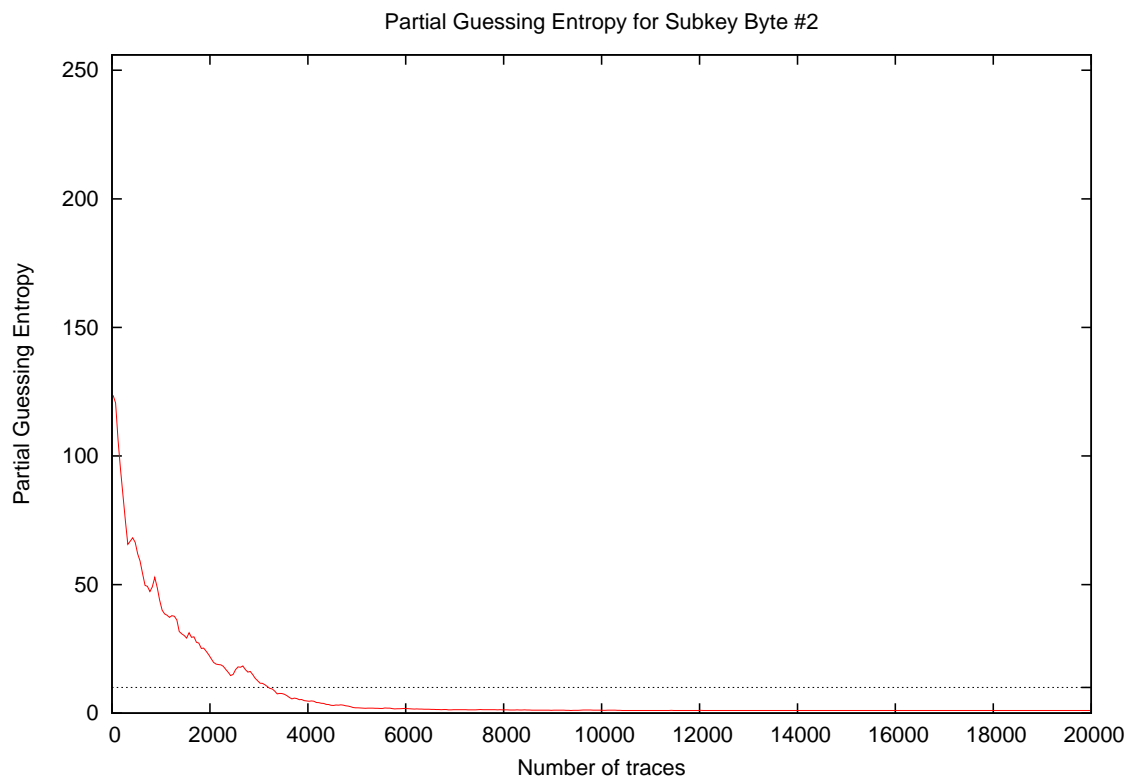
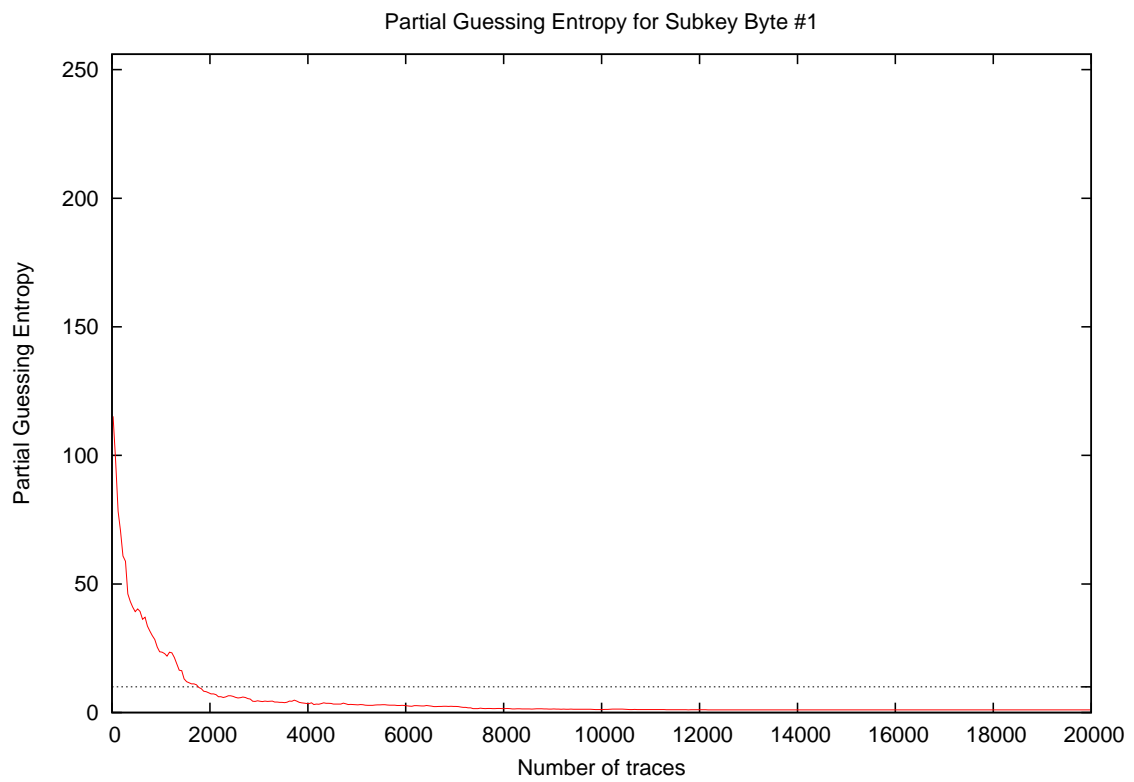


Partial Success Rate for Subkey Bytes #1 to #16

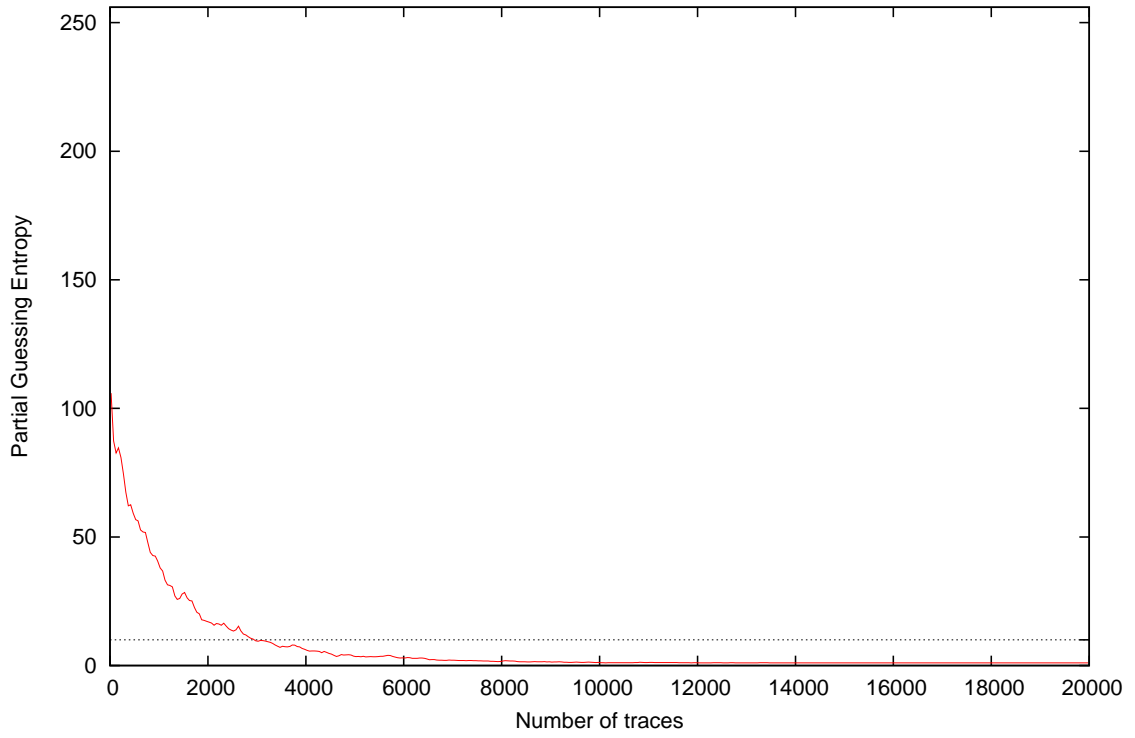


Traces	Partial Success Rate / Byte																Min	Max	Mean	
	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16				
	10	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.03	0.00	0.00	0.00	0.00				0.00
20	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.03	0.03	0.00	0.00	0.06	0.00	0.00	0.00	0.06	0.01
30	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	0.00	0.00	0.03	0.00
40	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	0.00	0.03	0.00
50	0.03	0.00	0.03	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.03	0.00	0.00	0.03	0.00	0.00	0.03	0.01
100	0.03	0.00	0.00	0.03	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	0.00	0.03	0.01
200	0.06	0.03	0.00	0.03	0.03	0.06	0.00	0.00	0.00	0.03	0.03	0.06	0.00	0.00	0.00	0.06	0.00	0.00	0.06	0.02
300	0.06	0.06	0.00	0.00	0.03	0.03	0.00	0.03	0.00	0.00	0.06	0.03	0.09	0.00	0.03	0.00	0.00	0.09	0.03	0.03
400	0.03	0.06	0.06	0.06	0.03	0.09	0.00	0.06	0.00	0.06	0.06	0.09	0.12	0.03	0.03	0.00	0.00	0.12	0.05	0.05
500	0.12	0.03	0.06	0.03	0.06	0.12	0.00	0.06	0.09	0.00	0.06	0.06	0.12	0.00	0.03	0.00	0.00	0.12	0.05	0.05
1000	0.16	0.06	0.16	0.06	0.06	0.09	0.12	0.09	0.12	0.19	0.03	0.25	0.28	0.03	0.03	0.12	0.03	0.28	0.12	0.12
2000	0.34	0.12	0.25	0.31	0.22	0.19	0.47	0.22	0.34	0.34	0.09	0.50	0.47	0.16	0.19	0.31	0.09	0.50	0.28	0.28
3000	0.47	0.28	0.31	0.53	0.34	0.59	0.66	0.28	0.44	0.69	0.16	0.66	0.62	0.34	0.12	0.62	0.12	0.69	0.45	0.45
4000	0.62	0.44	0.56	0.72	0.53	0.78	0.84	0.47	0.66	0.78	0.22	0.88	0.72	0.41	0.28	0.75	0.22	0.88	0.60	0.60
5000	0.78	0.62	0.62	0.72	0.69	0.88	0.88	0.69	0.72	0.94	0.34	0.97	0.84	0.59	0.53	0.78	0.34	0.97	0.72	0.72
10000	0.94	0.91	0.91	0.97	0.88	0.97	1.00	1.00	0.94	1.00	0.75	1.00	1.00	0.84	0.81	0.97	0.75	1.00	0.93	0.93
15000	0.97	1.00	1.00	1.00	0.91	1.00	1.00	1.00	1.00	1.00	0.94	1.00	1.00	0.97	0.94	1.00	0.91	1.00	0.98	0.98
20000	1.00	1.00	1.00	1.00	0.94	1.00	1.00	1.00	1.00	1.00	0.97	1.00	1.00	1.00	0.97	1.00	0.94	1.00	0.99	0.99

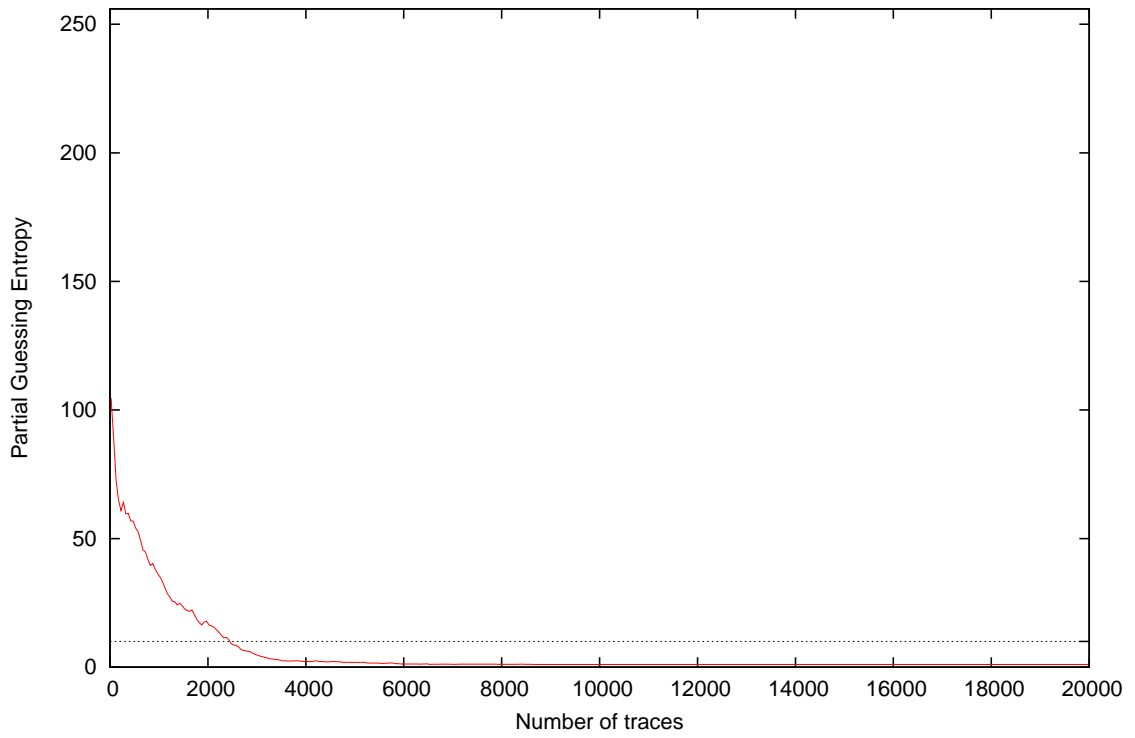
4 Partial Guessing Entropy



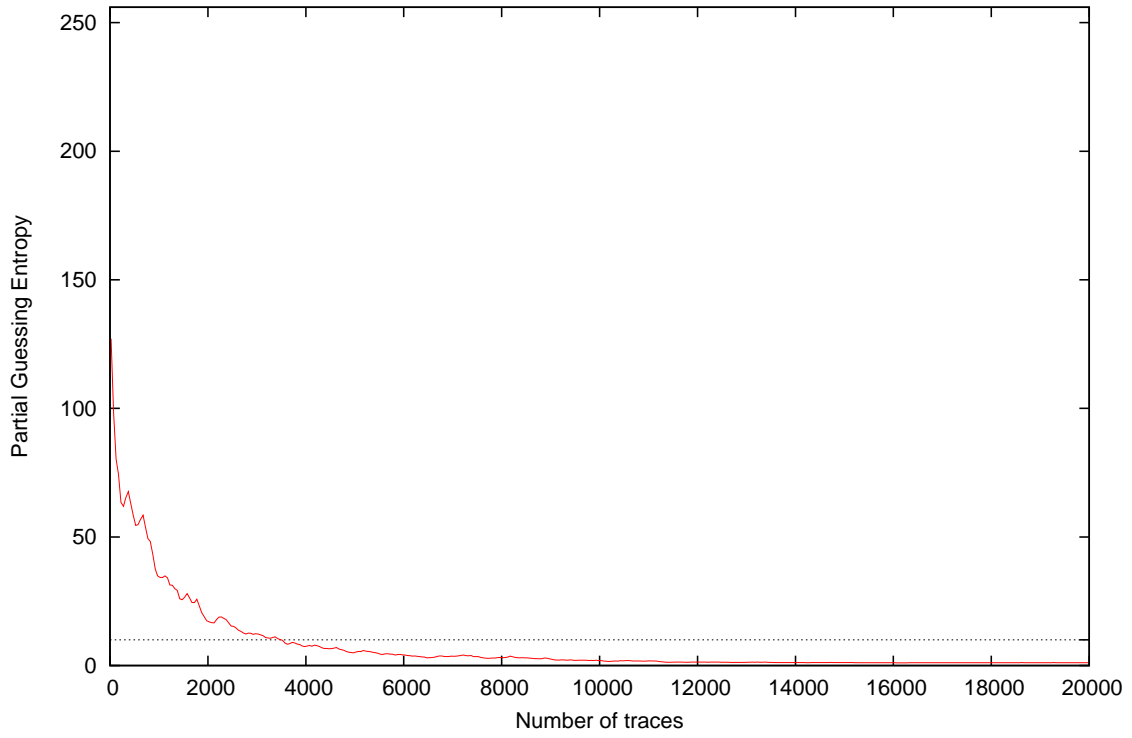
Partial Guessing Entropy for Subkey Byte #3



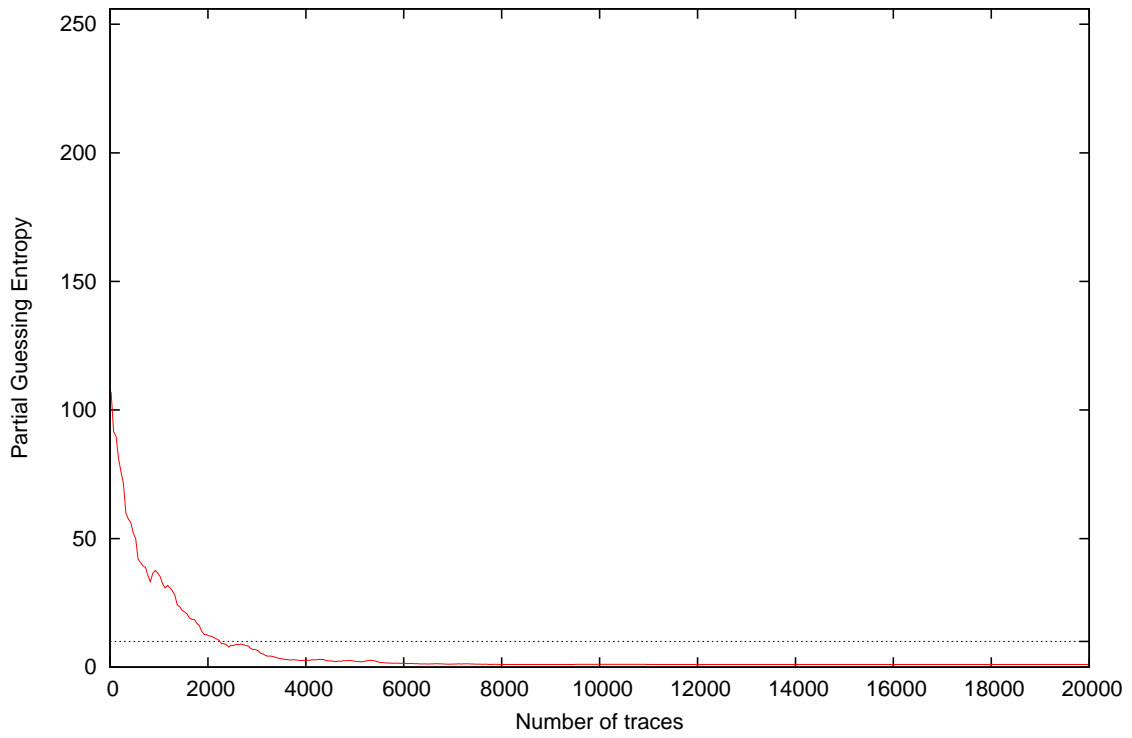
Partial Guessing Entropy for Subkey Byte #4



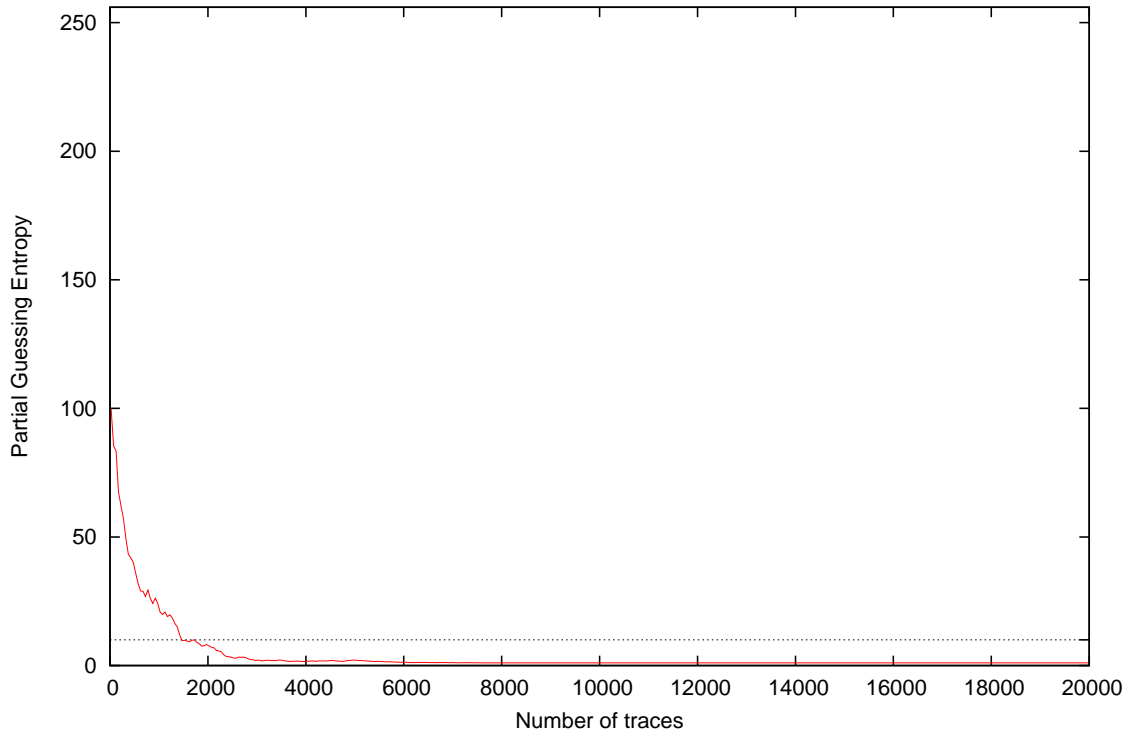
Partial Guessing Entropy for Subkey Byte #5



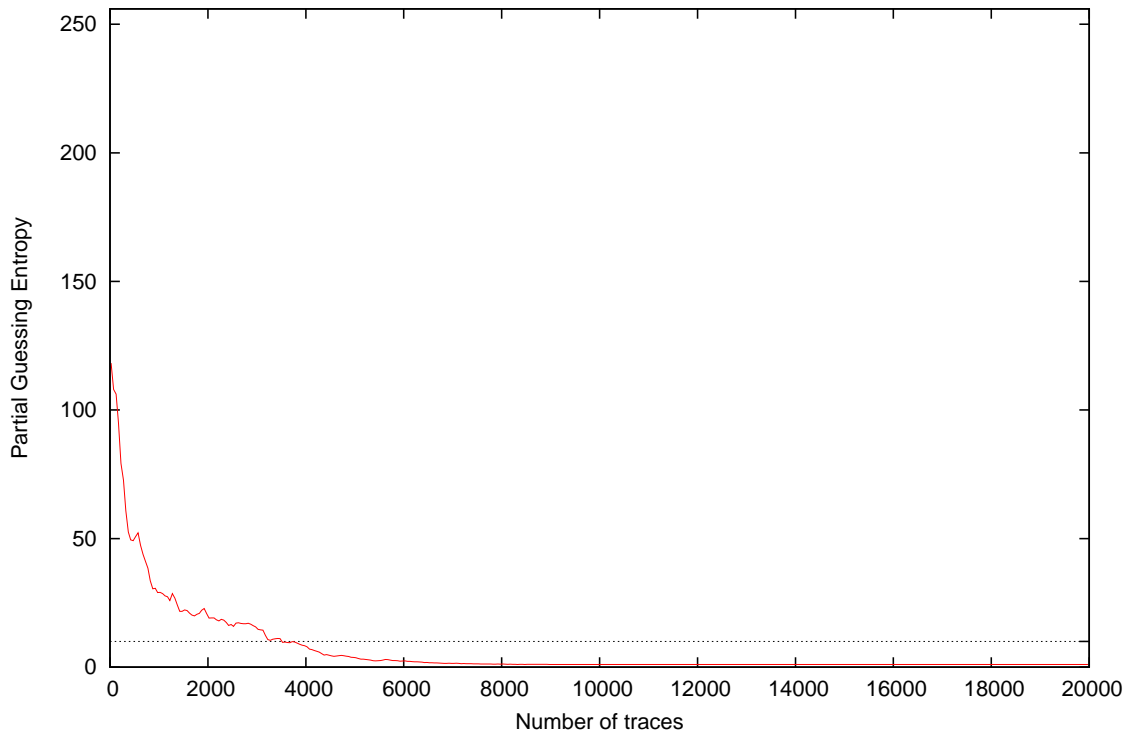
Partial Guessing Entropy for Subkey Byte #6



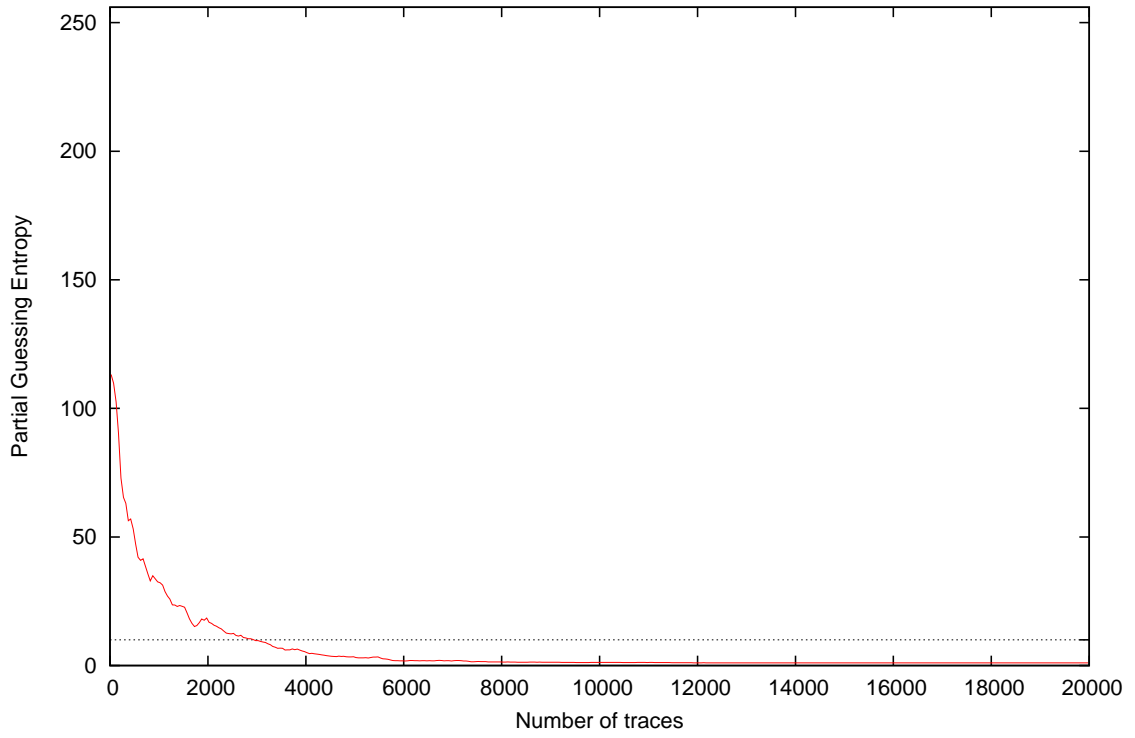
Partial Guessing Entropy for Subkey Byte #7



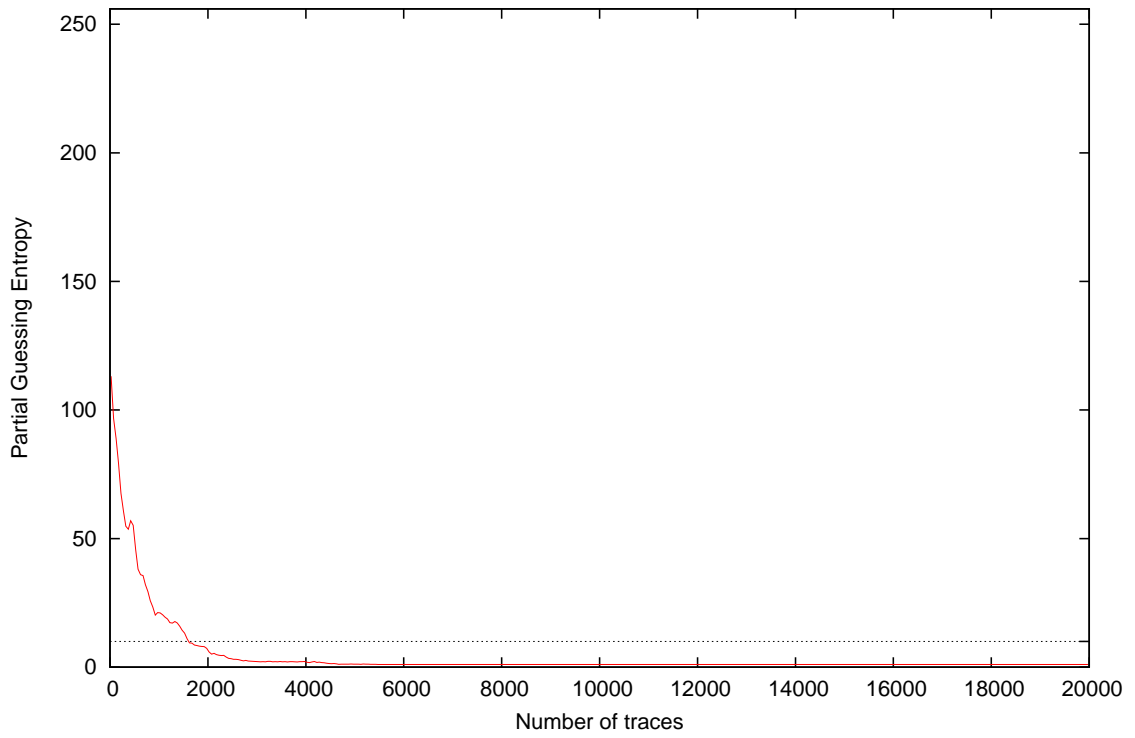
Partial Guessing Entropy for Subkey Byte #8



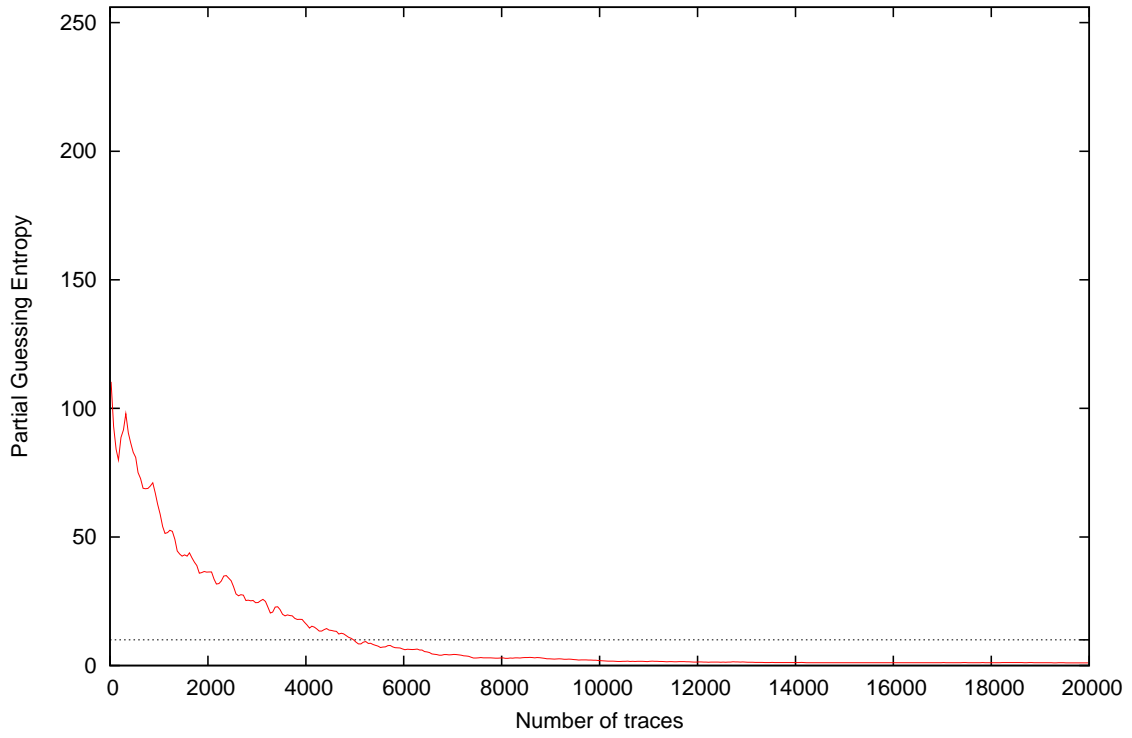
Partial Guessing Entropy for Subkey Byte #9



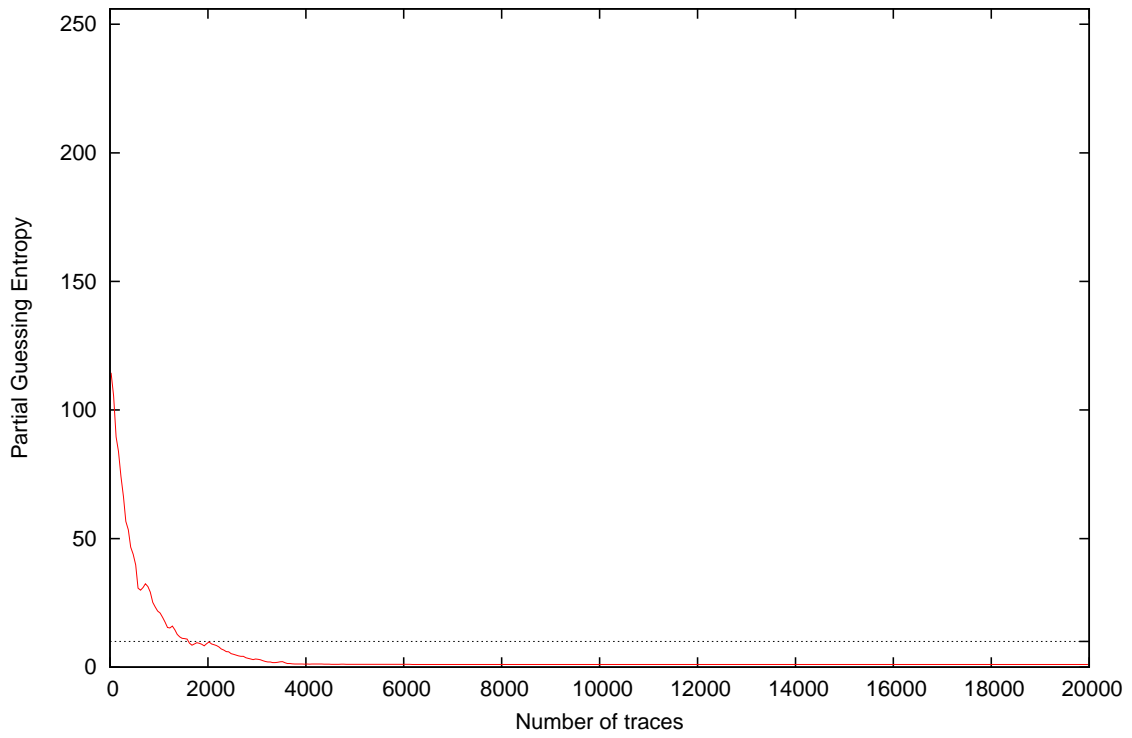
Partial Guessing Entropy for Subkey Byte #10

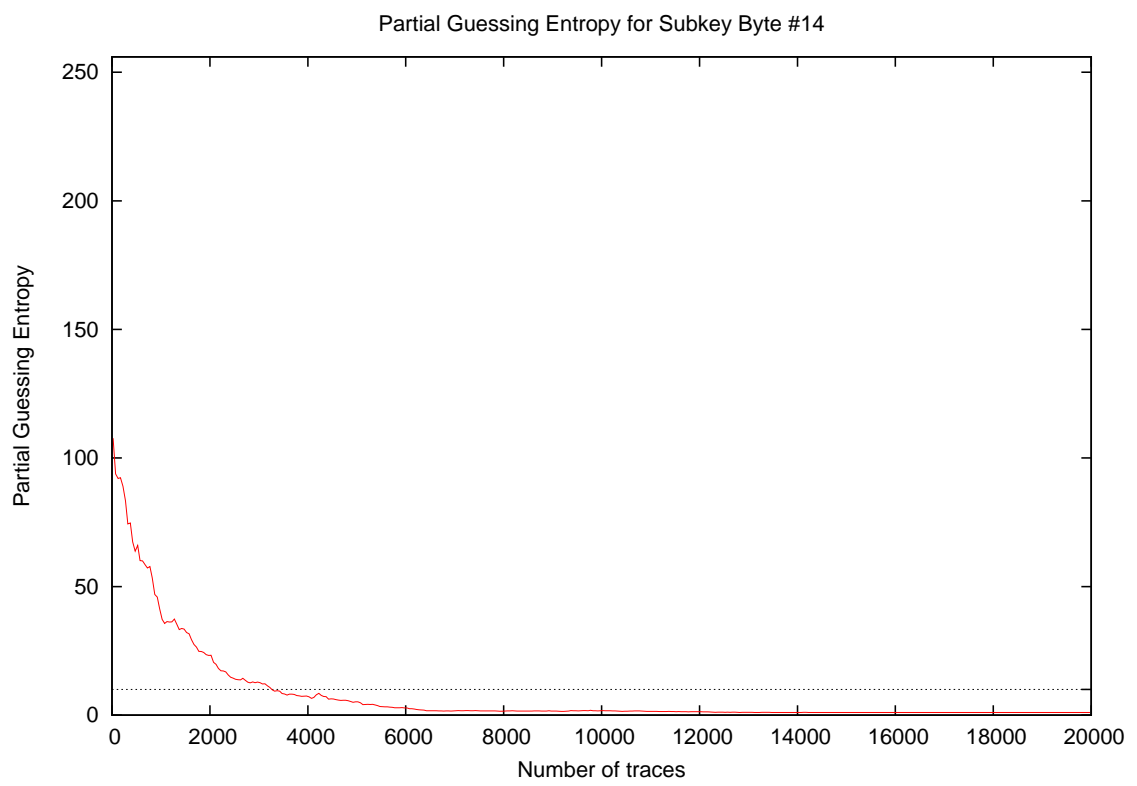
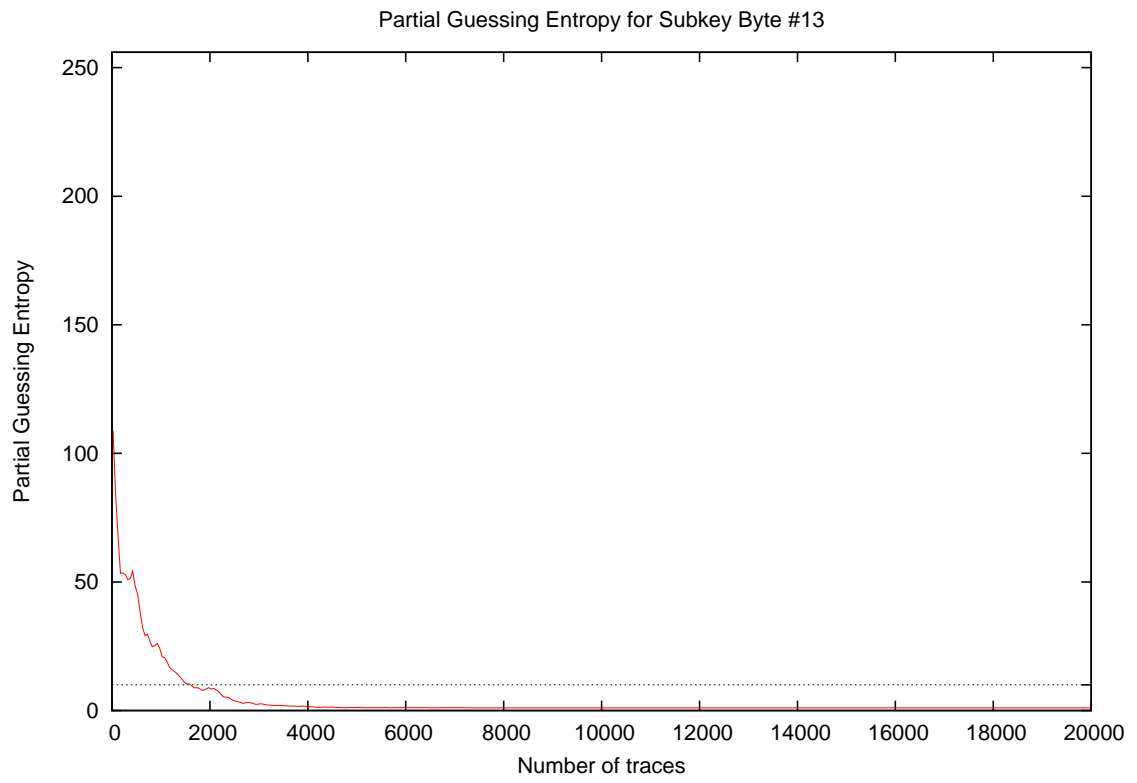


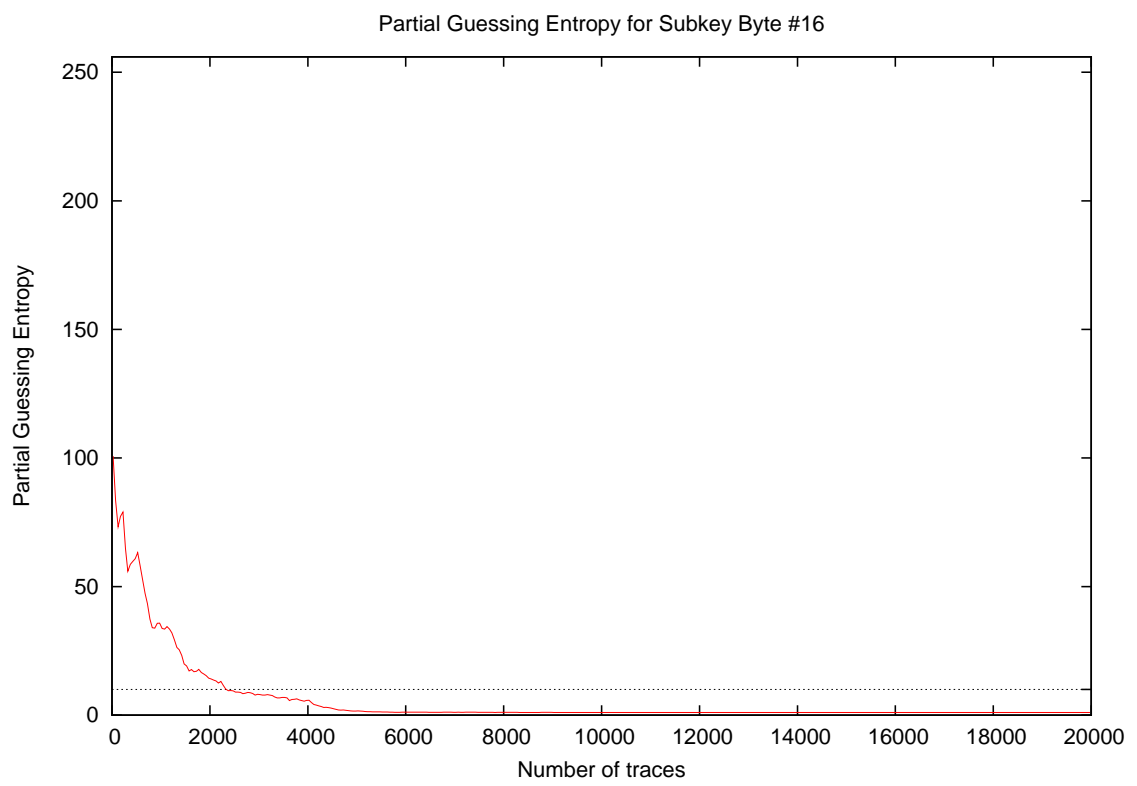
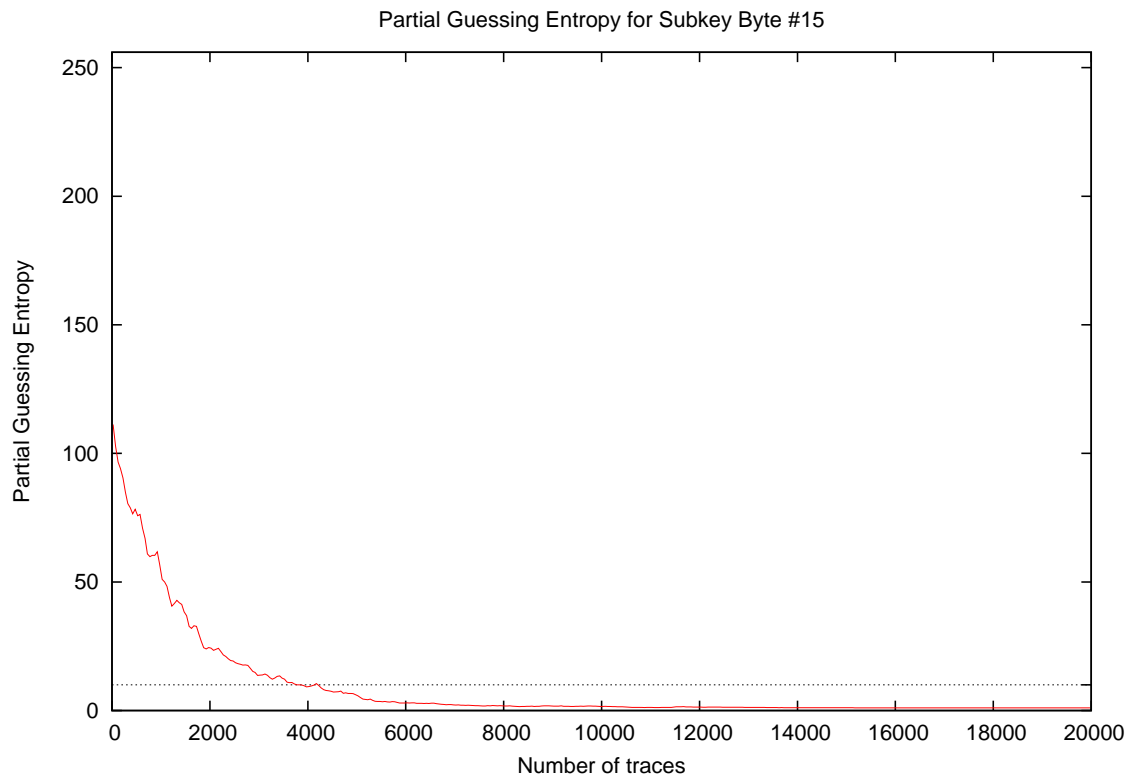
Partial Guessing Entropy for Subkey Byte #11



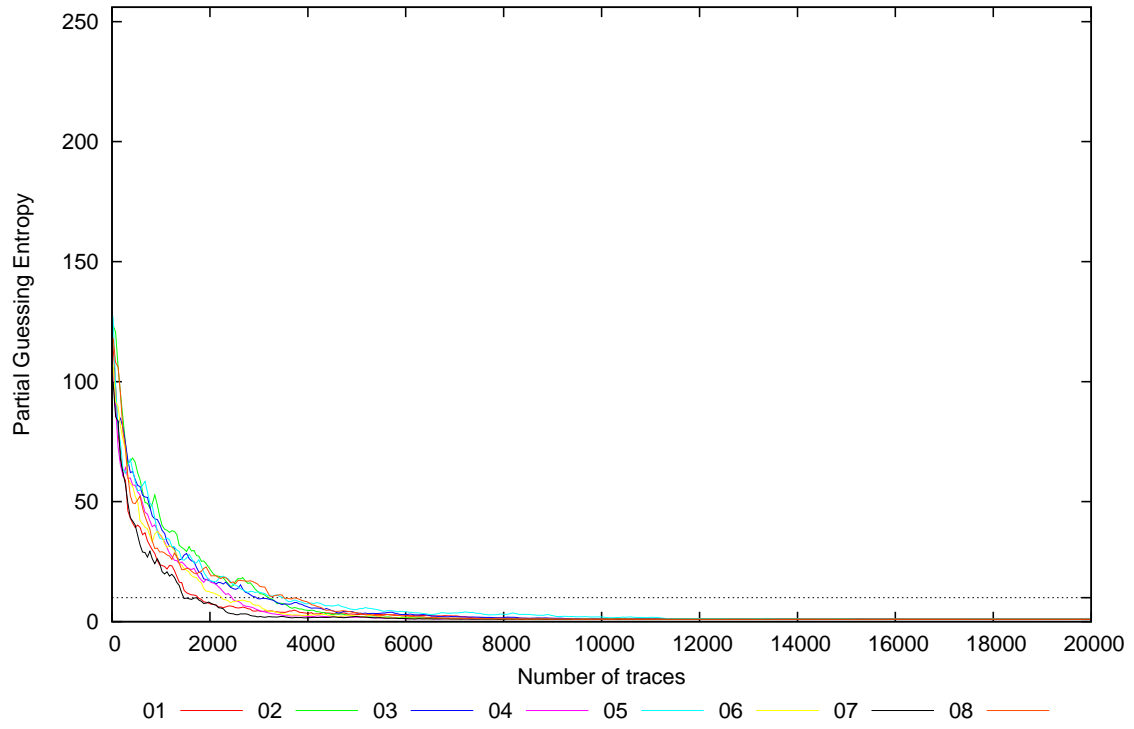
Partial Guessing Entropy for Subkey Byte #12



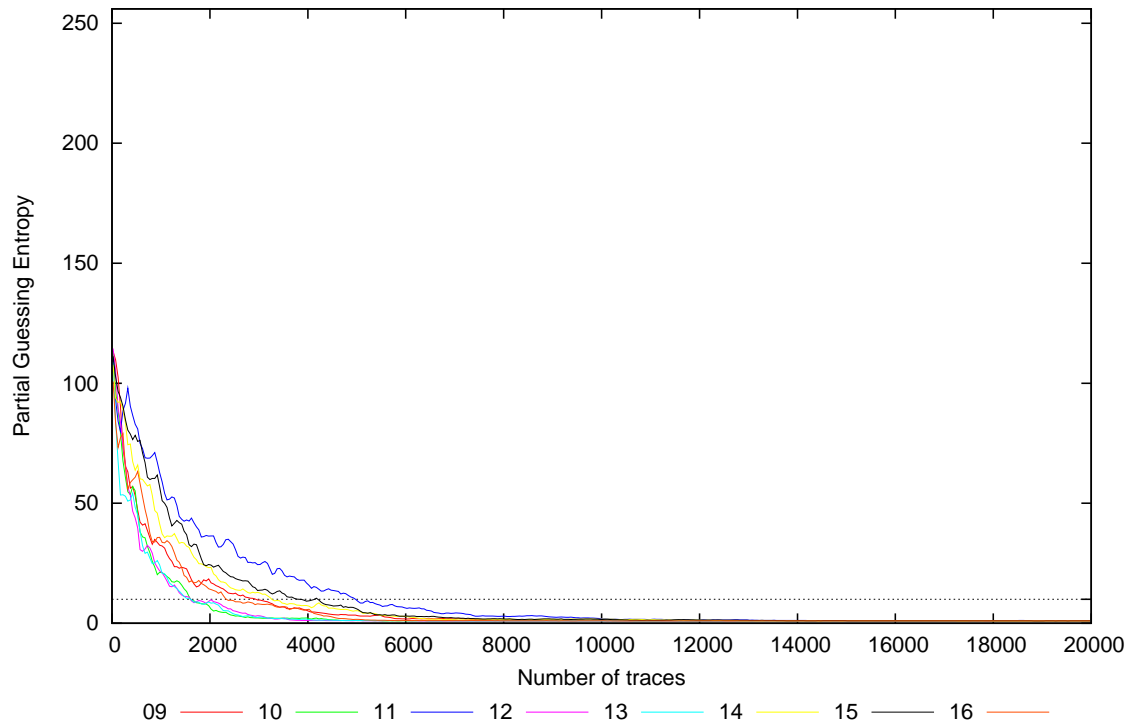


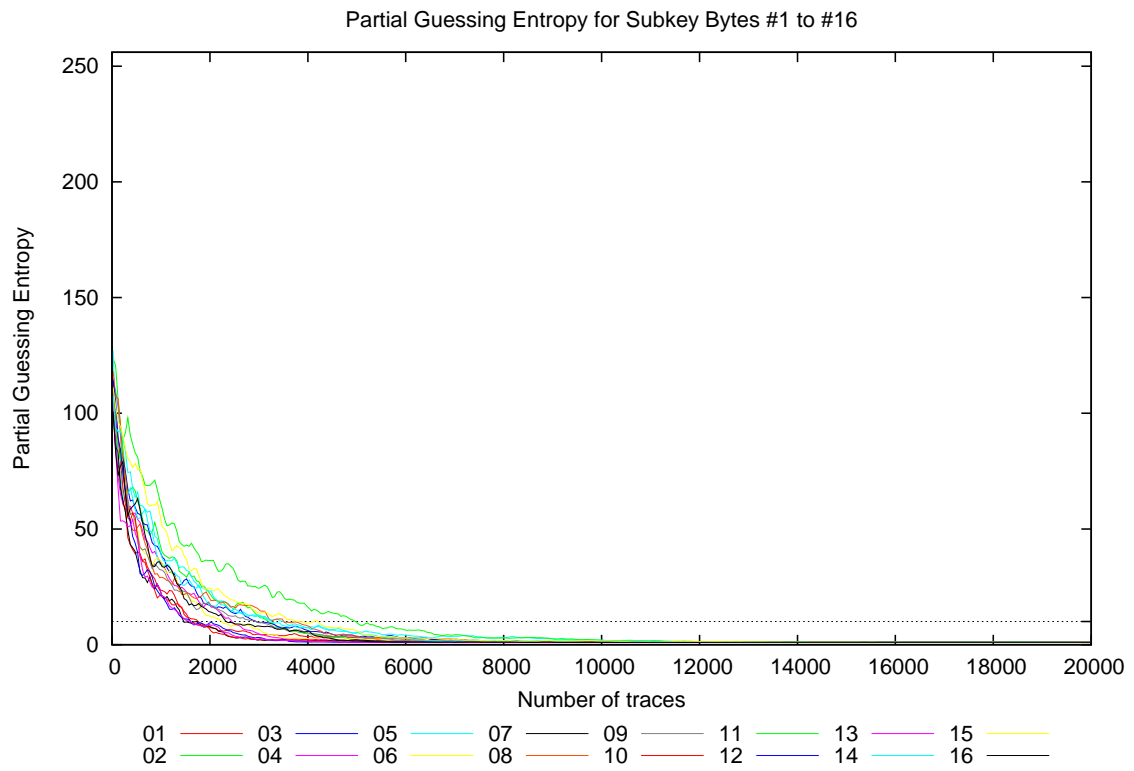


Partial Guessing Entropy for Subkey Bytes #1 to #8



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	121.5	128.2	114.2	106.3	138.0	130.5	101.8	135.6	120.9	119.6	115.8	126.8	127.8	108.1	110.9	104.3	101.8	138.0	119.4
20	119.2	117.2	110.9	104.3	135.6	104.8	102.9	108.9	111.9	114.1	111.5	112.2	108.1	105.5	120.2	108.4	102.9	135.6	112.2
30	117.0	117.4	105.4	100.0	122.1	101.8	90.5	114.9	107.6	110.8	110.4	112.6	95.6	96.6	113.9	95.6	90.5	122.1	107.0
40	109.2	126.6	96.2	98.4	121.7	87.5	97.7	117.6	118.1	101.7	106.3	110.4	99.7	101.2	100.4	95.2	87.5	126.6	105.5
50	102.2	121.8	81.0	96.6	112.6	93.9	91.8	112.5	111.3	101.7	106.5	105.2	96.9	98.5	110.6	88.1	81.0	121.8	101.9
100	86.6	114.8	81.0	85.8	88.4	90.0	86.9	100.6	110.0	94.2	86.1	92.8	78.0	98.3	91.9	74.3	74.3	114.8	91.2
200	62.0	92.8	79.2	60.9	68.5	77.2	64.2	88.5	76.6	70.7	89.3	74.4	48.3	88.3	92.6	79.5	48.3	92.8	75.8
300	50.8	70.4	70.1	60.4	63.8	68.9	55.6	67.5	64.8	57.5	94.8	62.8	52.5	74.3	83.3	60.2	50.8	94.8	66.1
400	41.8	66.8	64.3	57.7	70.1	56.6	39.9	50.3	58.4	57.4	89.5	49.5	55.1	68.1	77.4	58.9	39.9	89.5	60.1
500	40.4	65.2	55.5	56.3	57.2	52.6	37.8	50.4	48.4	49.1	83.5	42.7	47.1	65.5	79.9	64.2	37.8	83.5	56.0
1000	24.2	43.1	40.1	35.9	34.2	35.6	23.1	28.6	31.9	21.0	59.9	20.6	22.9	39.3	54.0	34.5	20.6	59.9	34.3
2000	7.6	21.8	16.6	16.5	17.3	12.3	7.9	19.8	18.0	7.1	36.6	9.3	9.1	23.5	24.7	14.0	7.1	36.6	16.4
3000	4.6	12.2	9.5	4.6	12.2	6.8	2.0	14.9	9.5	2.2	24.2	3.1	2.7	13.3	13.2	8.3	2.0	24.2	9.0
4000	3.4	4.6	6.0	2.2	7.4	2.6	1.6	8.4	5.2	2.0	16.2	1.2	1.6	7.4	8.8	5.8	1.2	16.2	5.3
5000	3.0	2.1	3.5	1.8	5.0	2.4	2.1	3.8	3.4	1.1	9.7	1.1	1.2	5.2	6.2	1.7	1.1	9.7	3.3
10000	1.2	1.2	1.2	1.0	1.9	1.1	1.0	1.0	1.2	1.0	1.9	1.0	1.0	1.8	1.5	1.0	1.0	1.9	1.2
15000	1.0	1.0	1.0	1.0	1.2	1.0	1.0	1.0	1.0	1.0	1.1	1.0	1.0	1.0	1.1	1.0	1.0	1.2	1.0
20000	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	1.0	1.0	1.0	1.0	1.1	1.0