

DPA Contest v2

Evaluation results

Reference attack

November 2010

1 Introduction

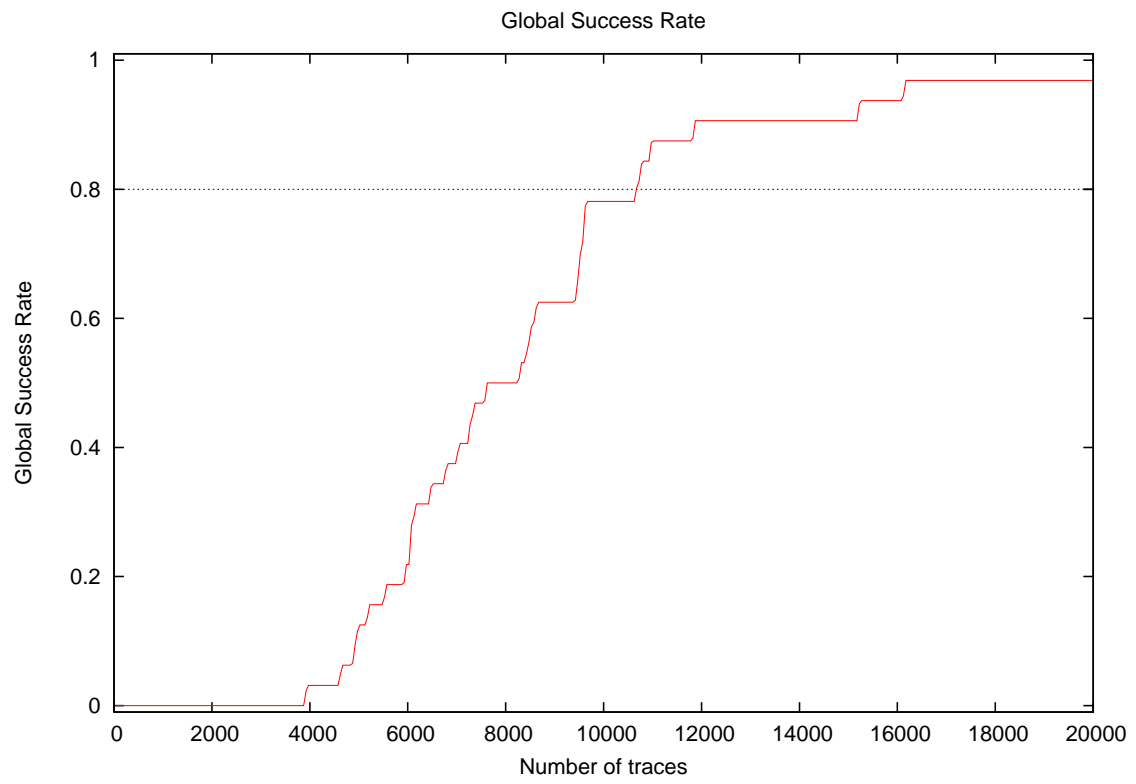
1.1 About the attack

- **Attack Name:** Recursive CPA
- **Sender/Team:** Victor Lomné
- **Institution:** ANSSI, France
- **Language:** C
- **Operating system:** Linux
- **Attacked subkey:** 10

1.2 About the evaluation

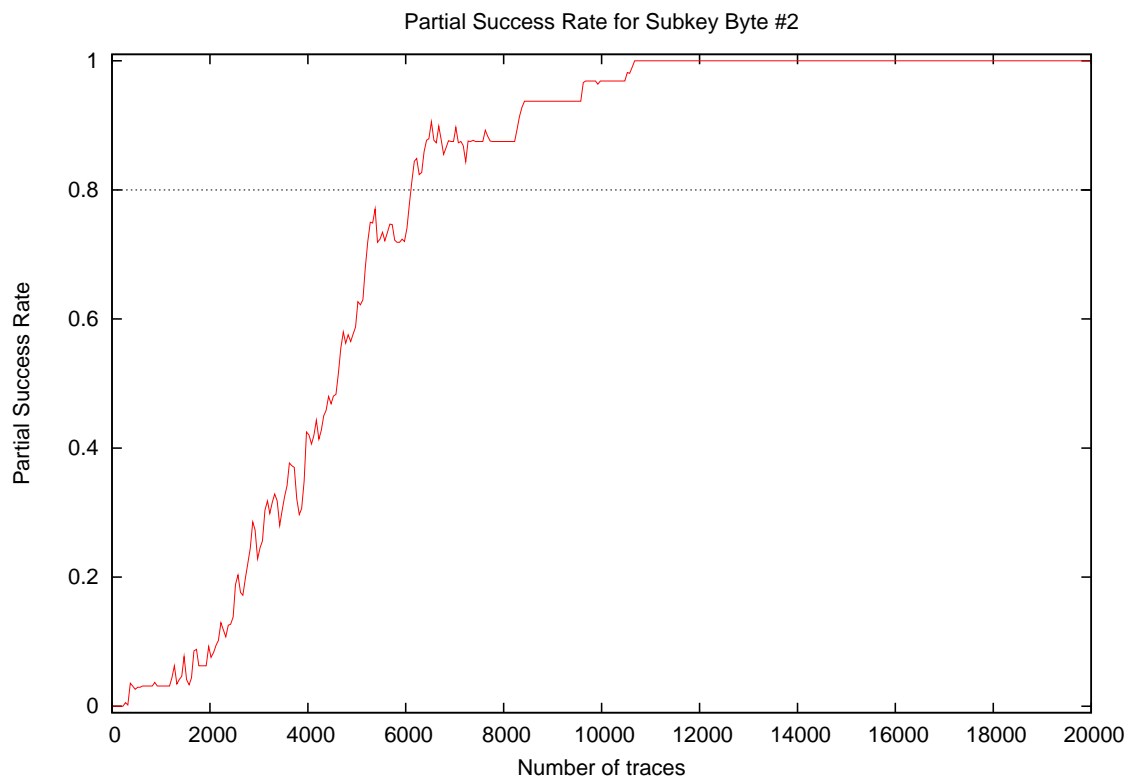
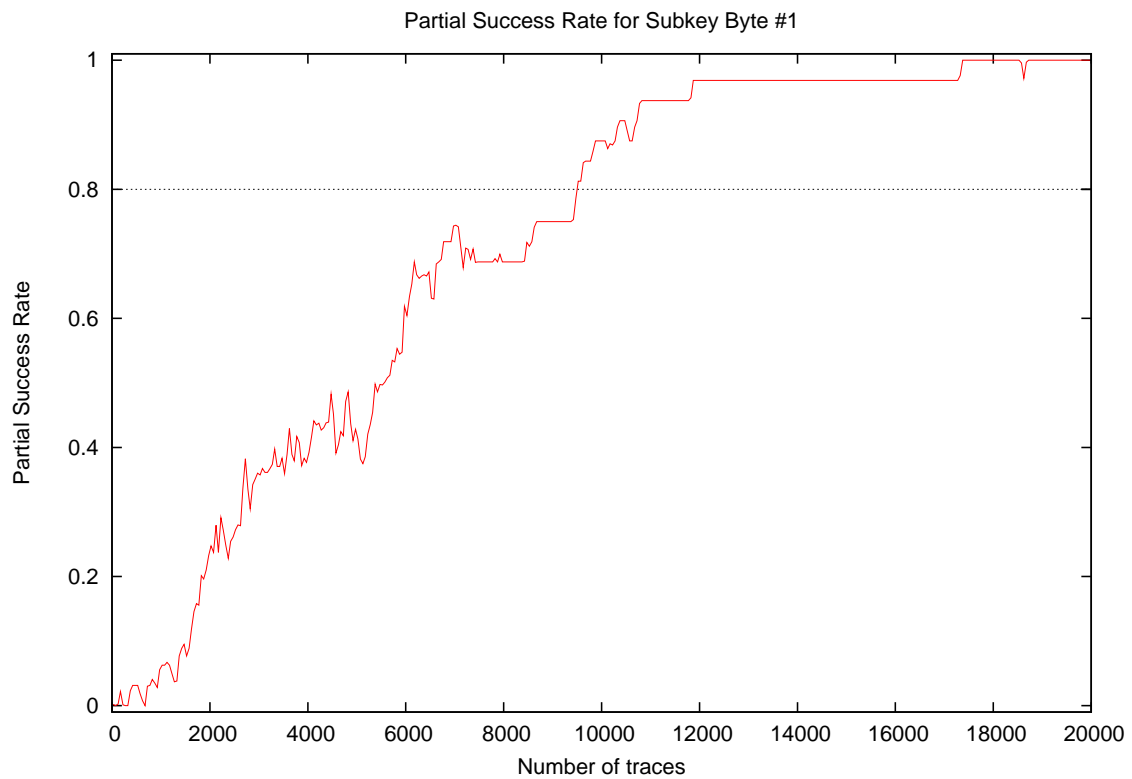
- **Date of evaluation:** November 2010

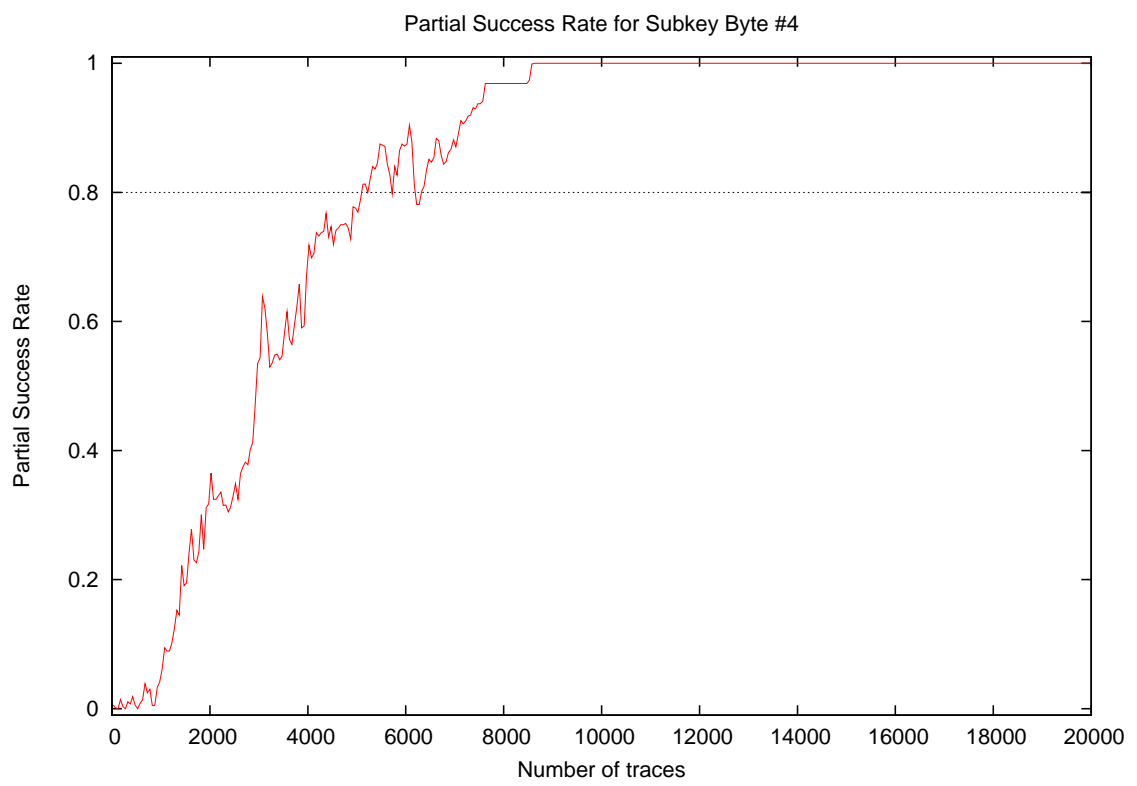
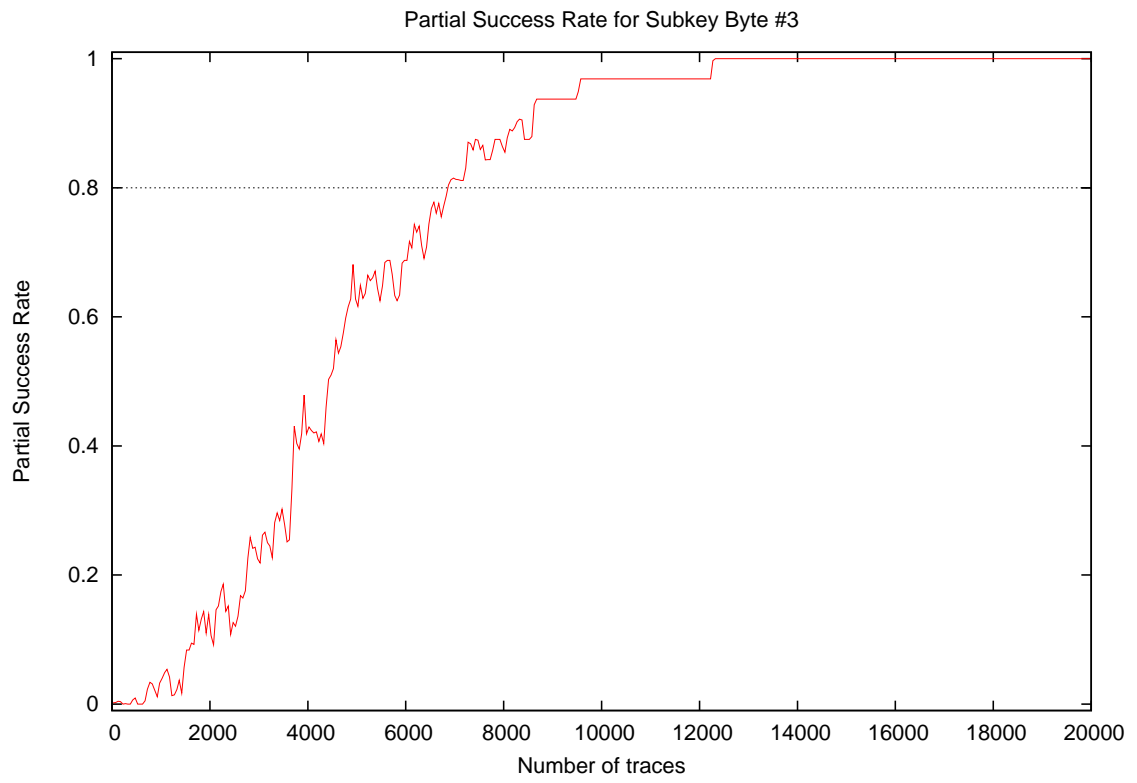
2 Global Success Rate

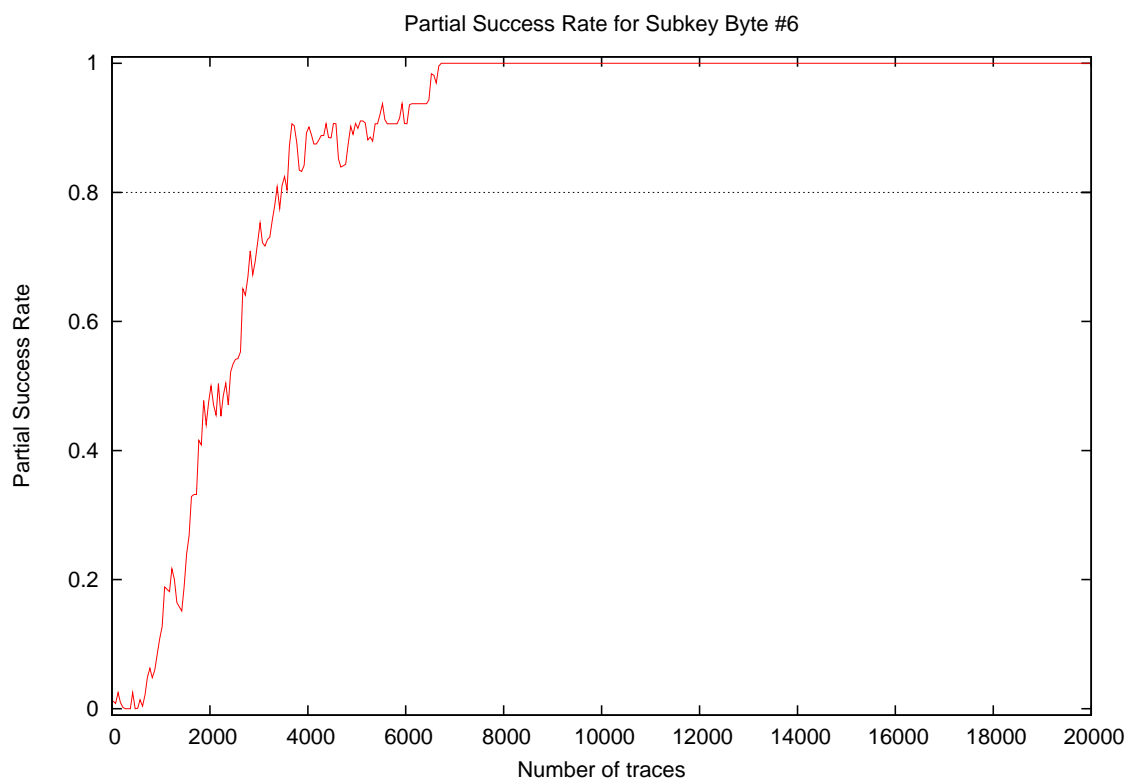
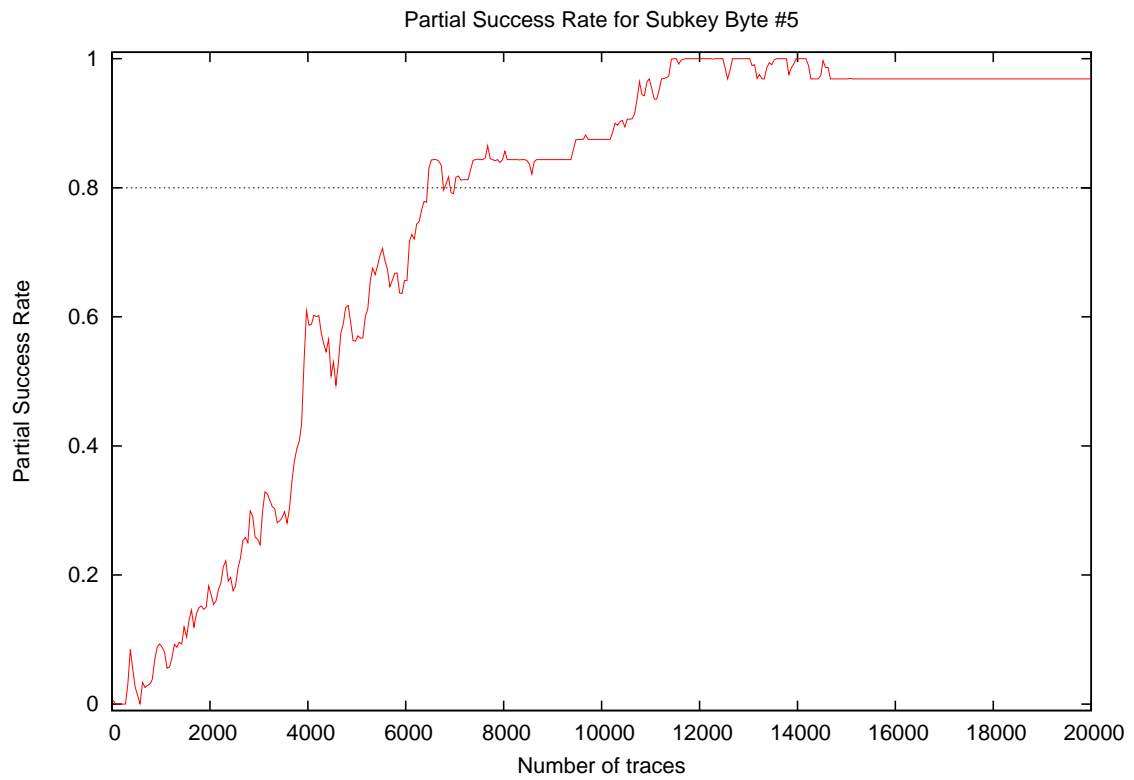


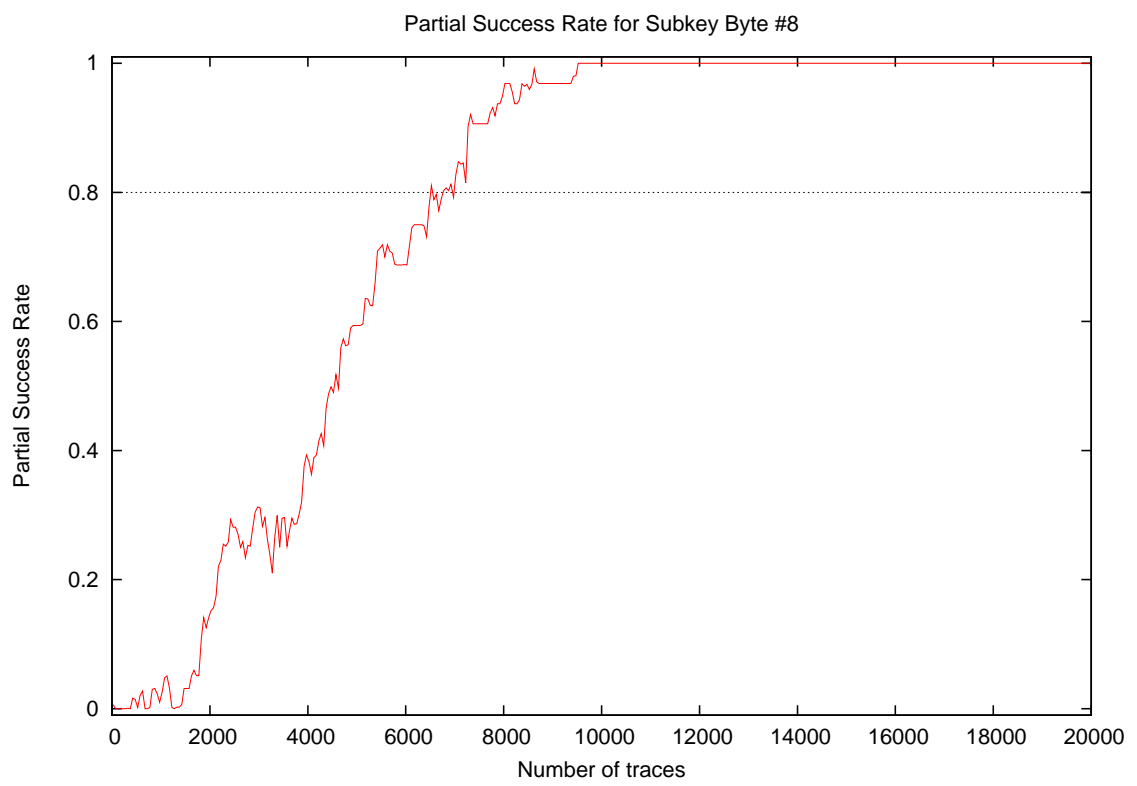
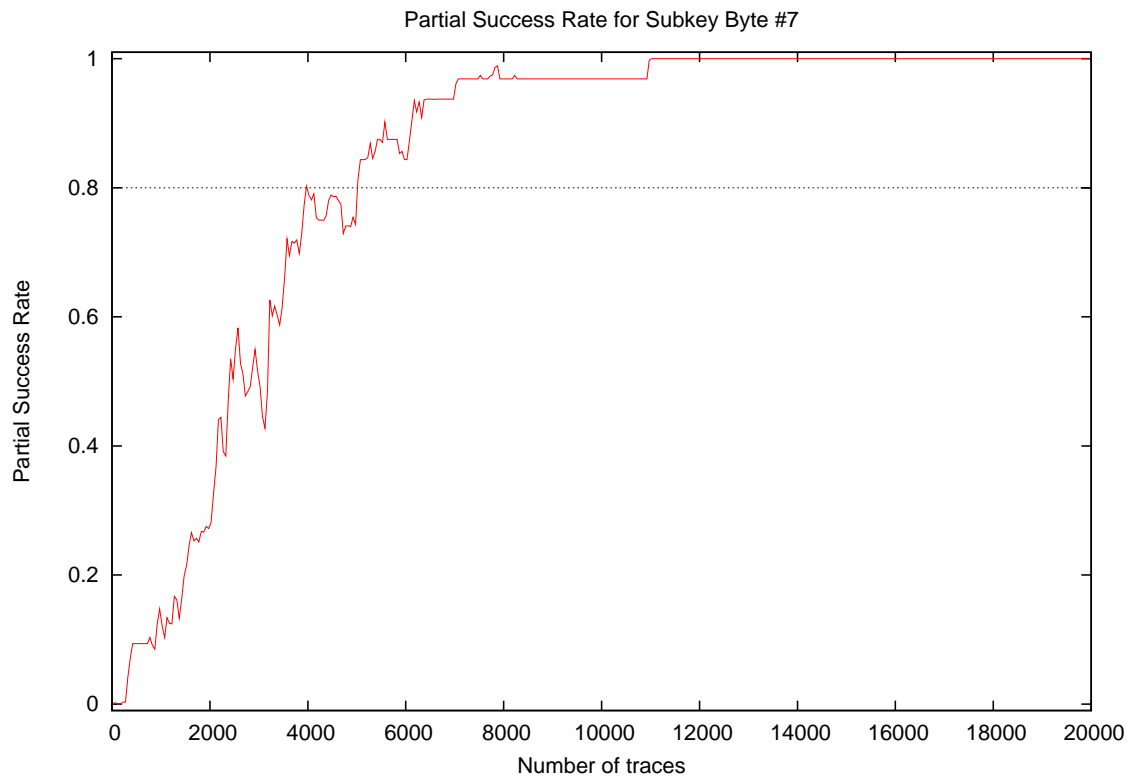
Number of traces	Global Success Rate
10	0.00
20	0.00
30	0.00
40	0.00
50	0.00
100	0.00
200	0.00
300	0.00
400	0.00
500	0.00
1000	0.00
2000	0.00
3000	0.00
4000	0.03
5000	0.12
10000	0.78
15000	0.91
20000	0.97

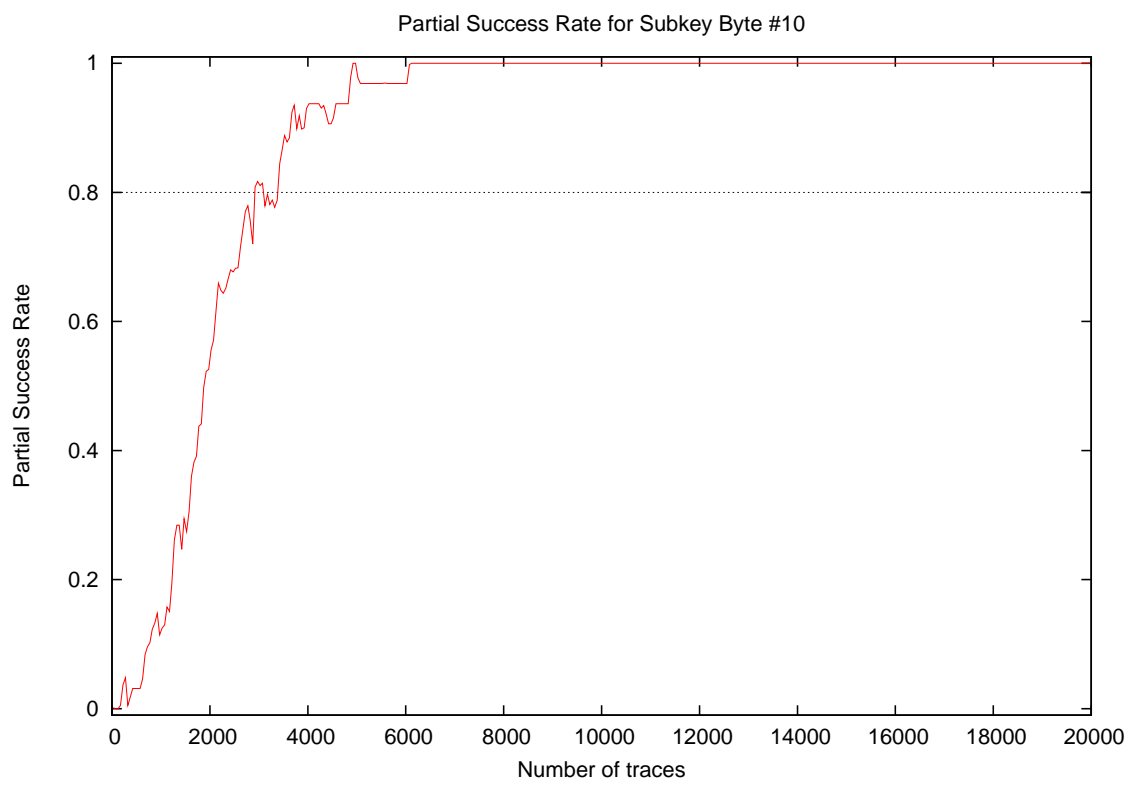
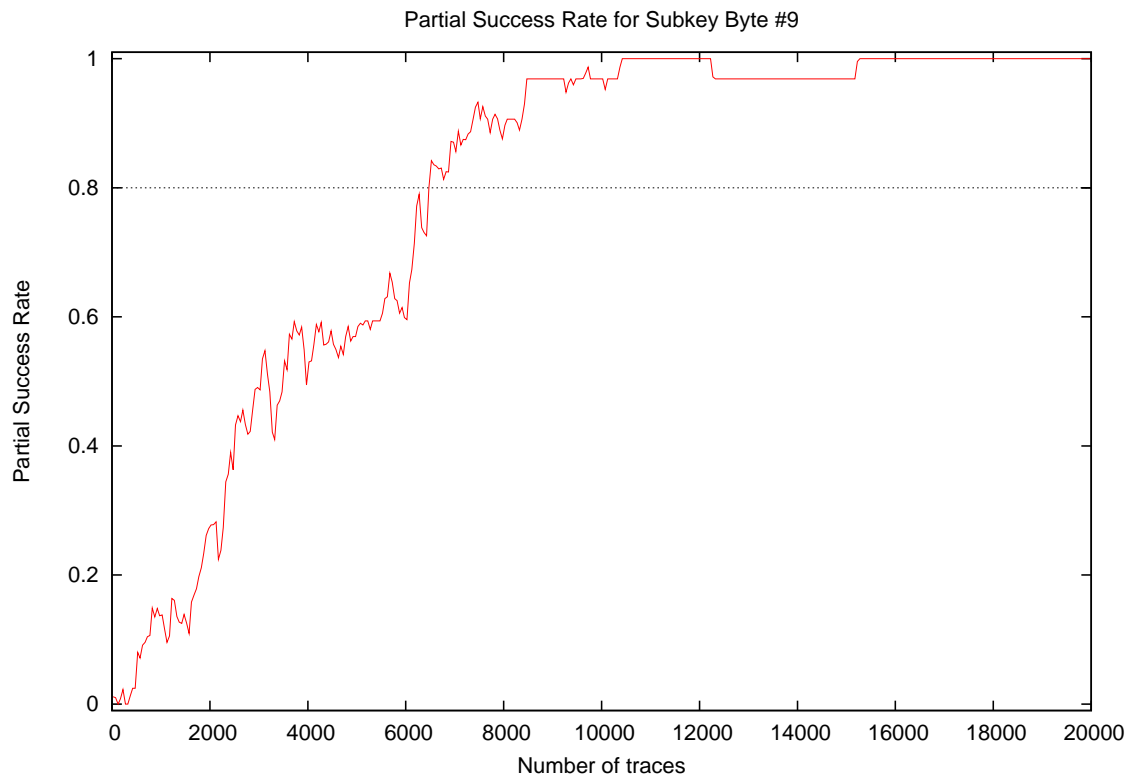
3 Partial Success Rate

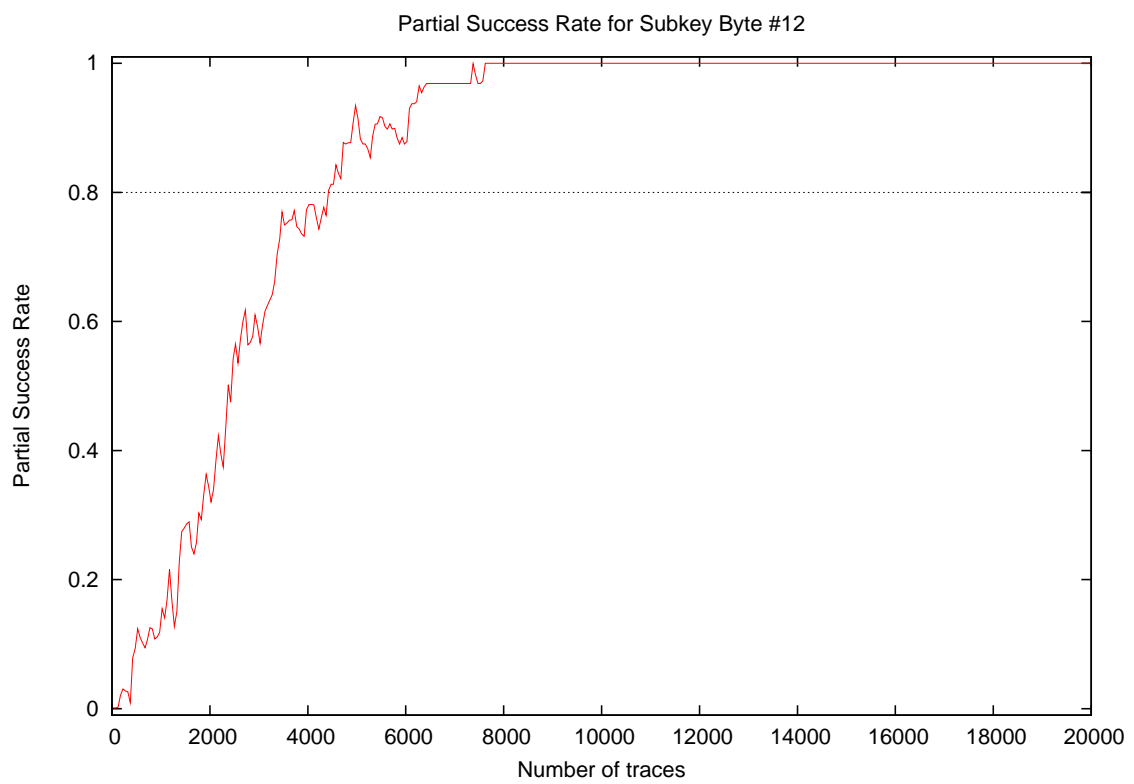
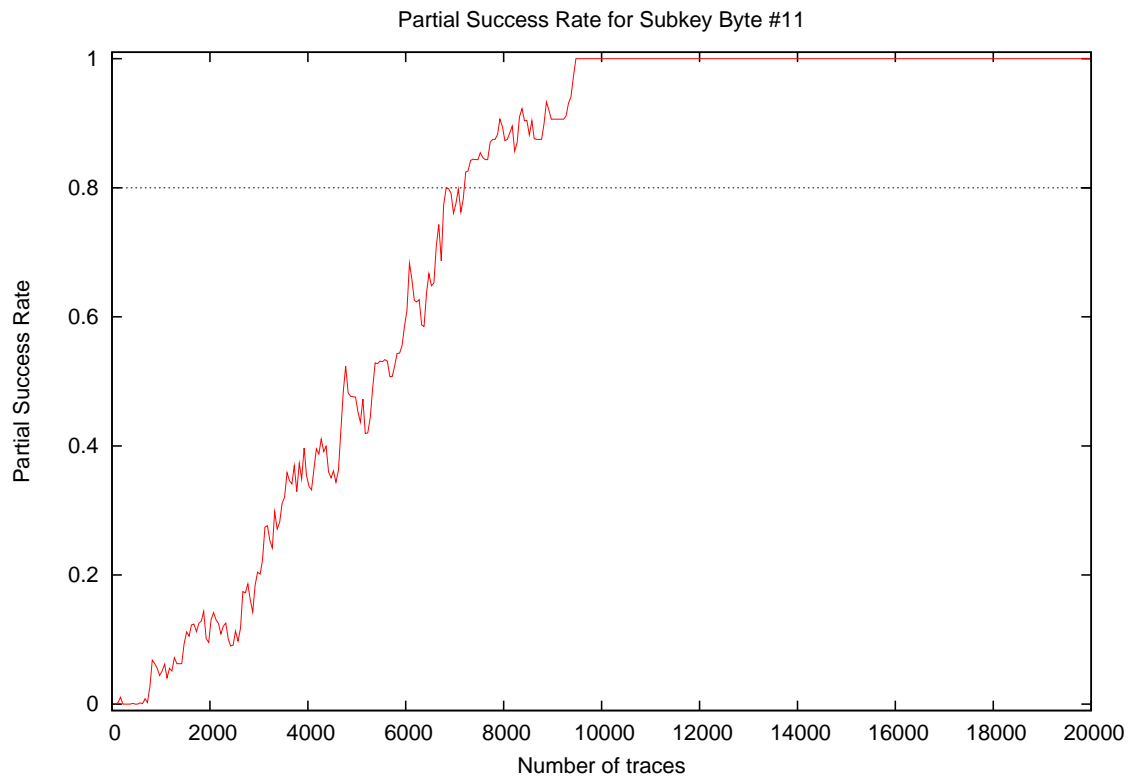


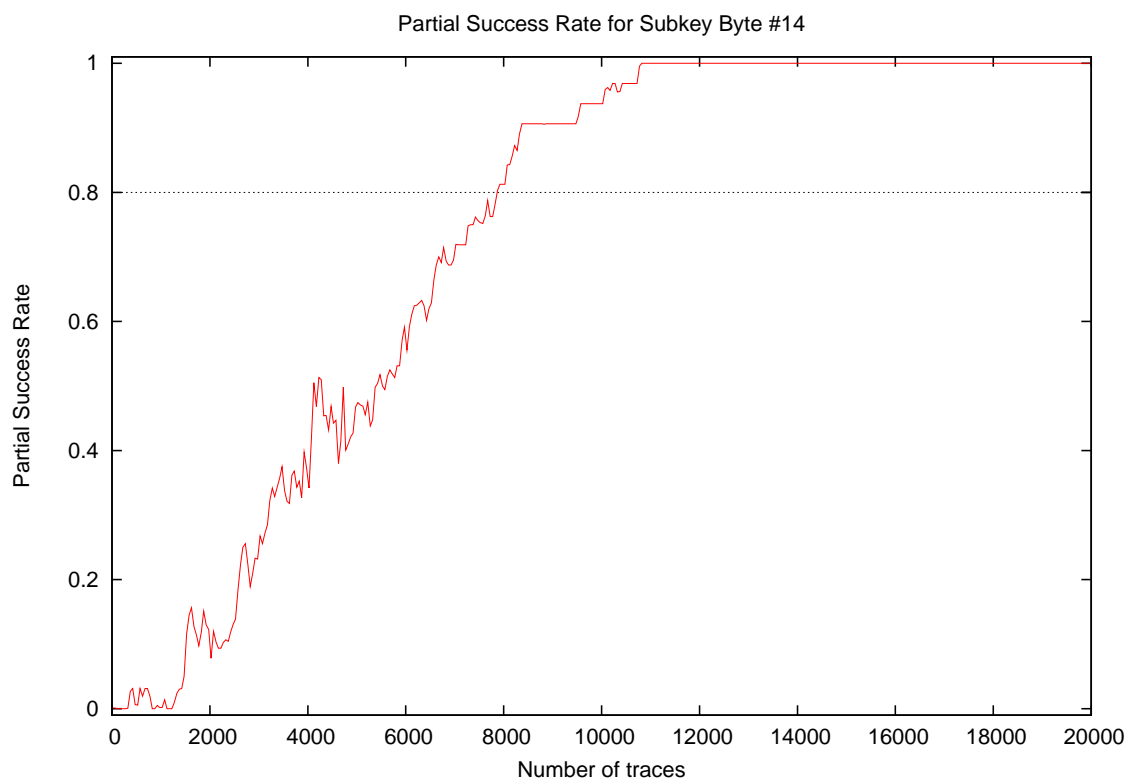
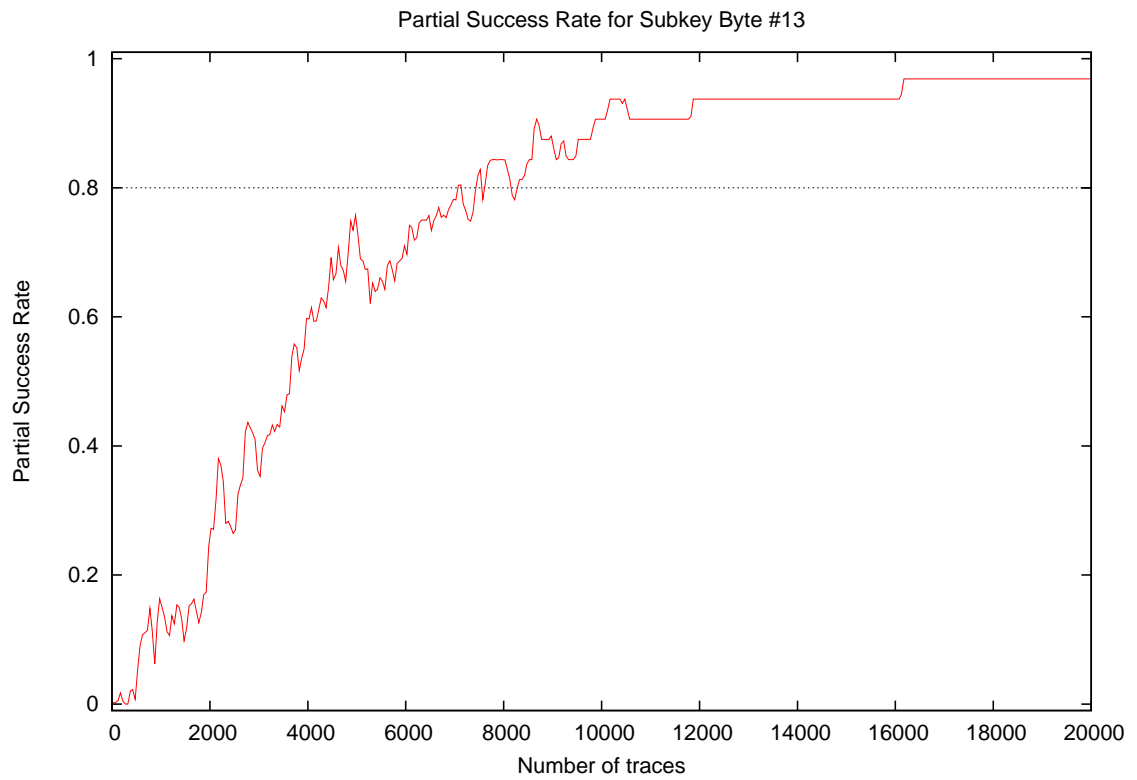


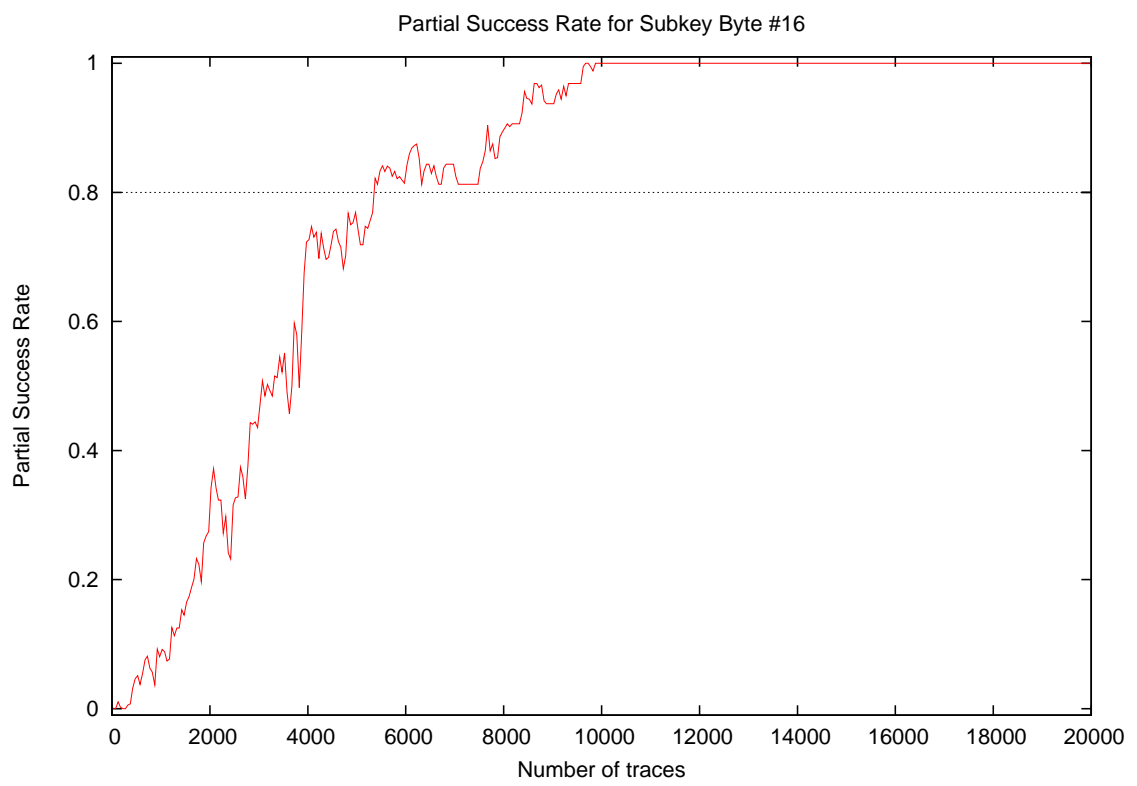
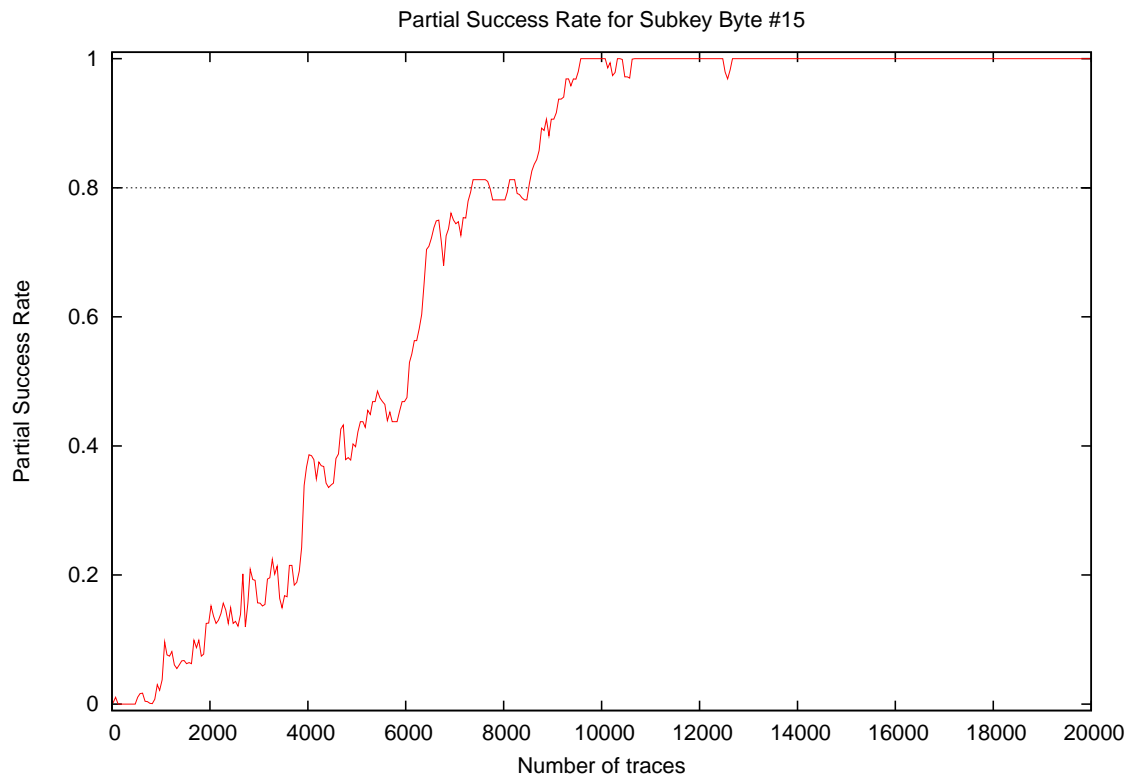


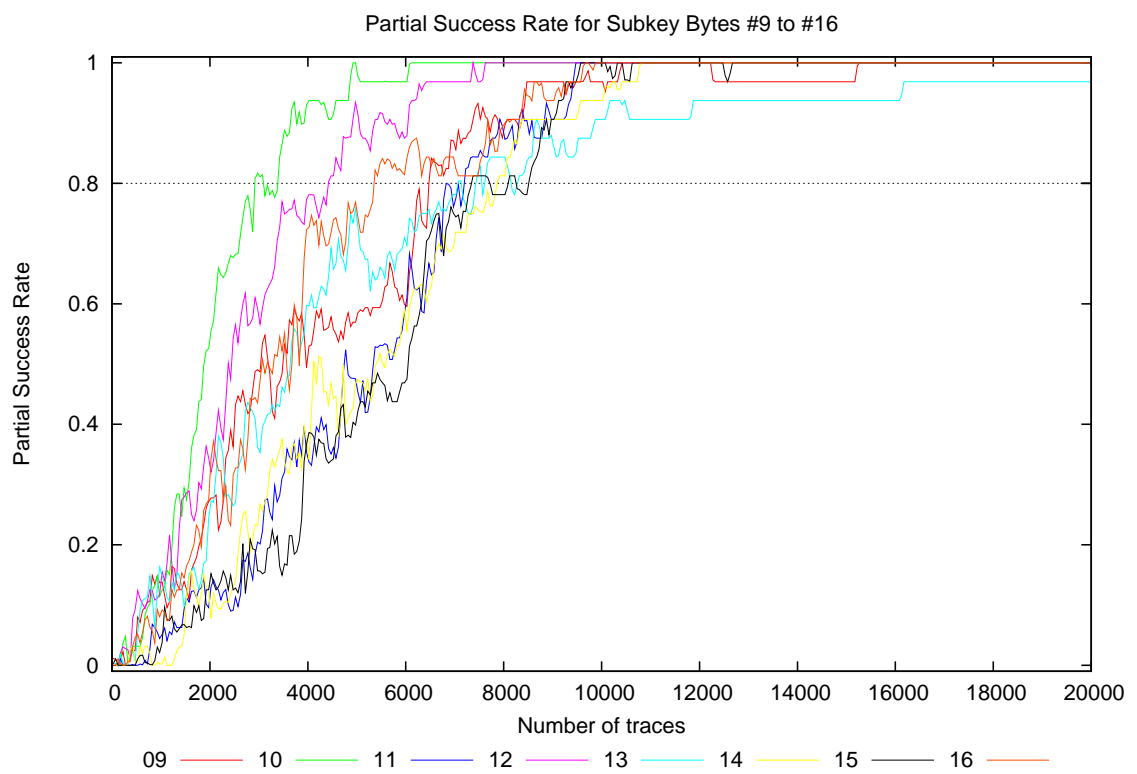
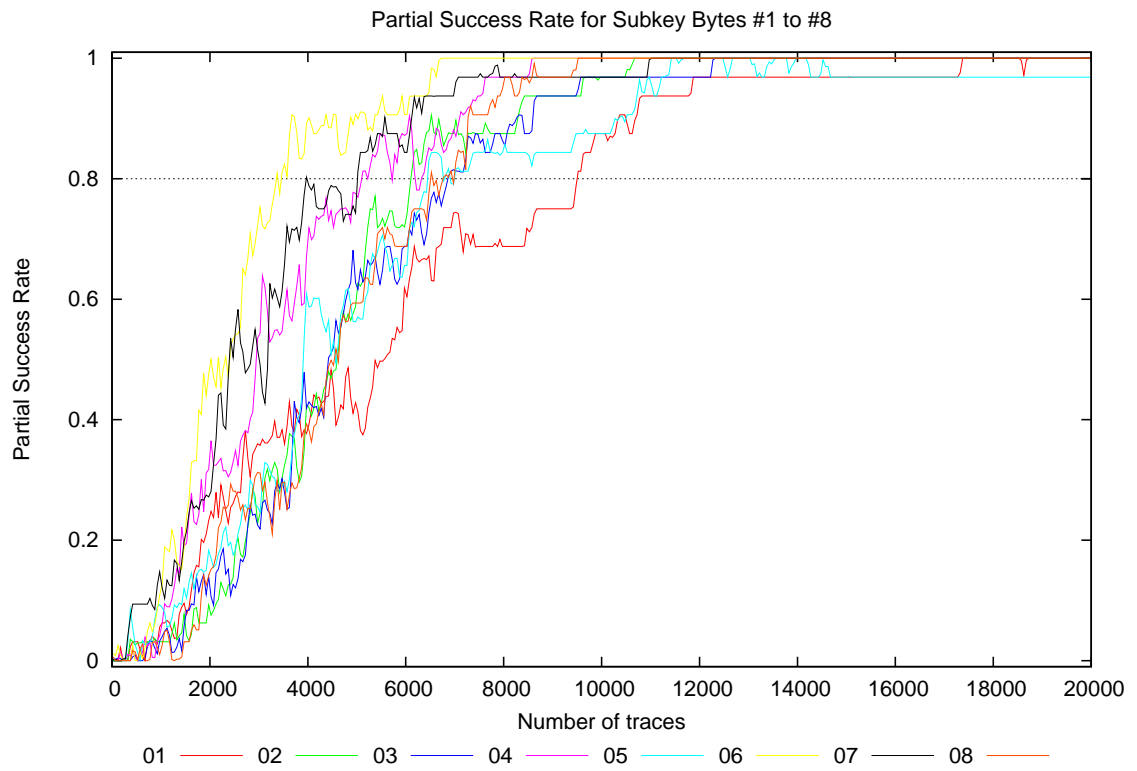




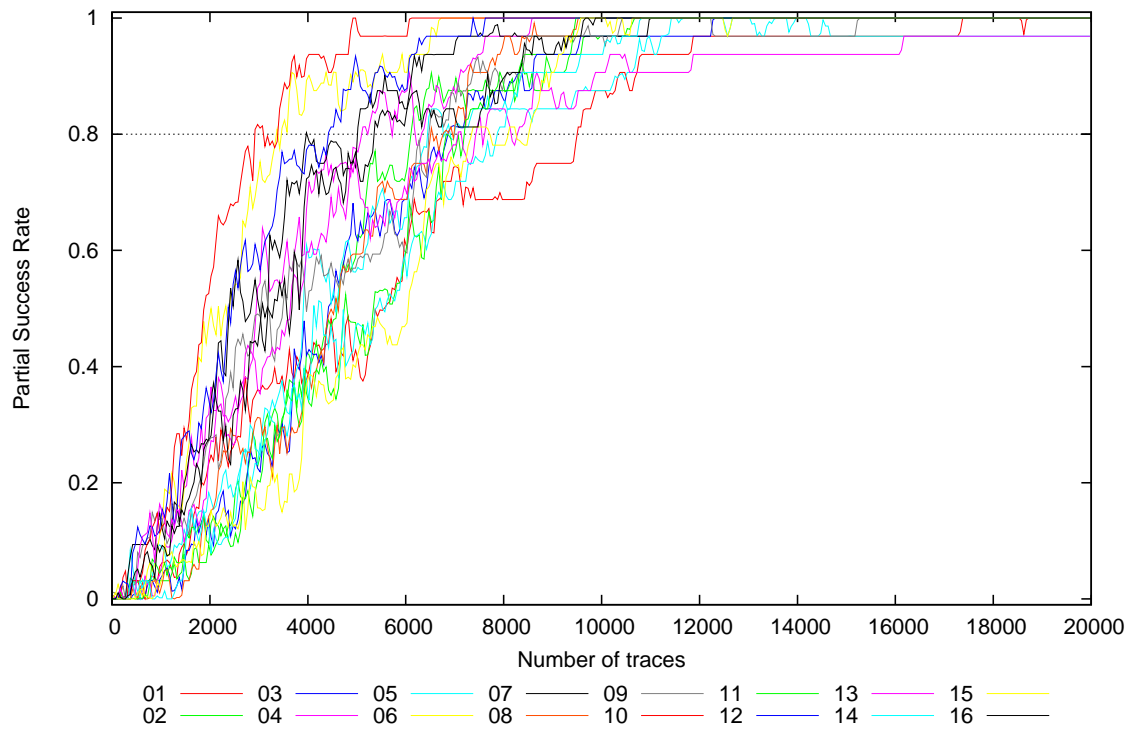






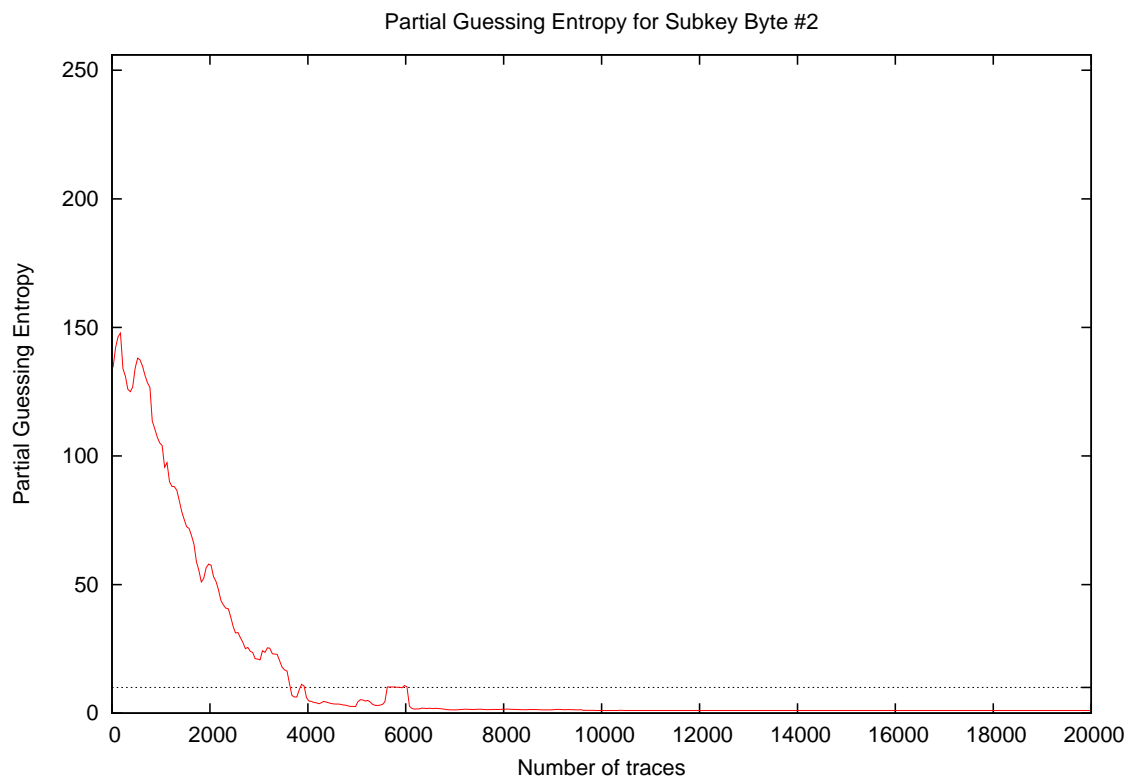
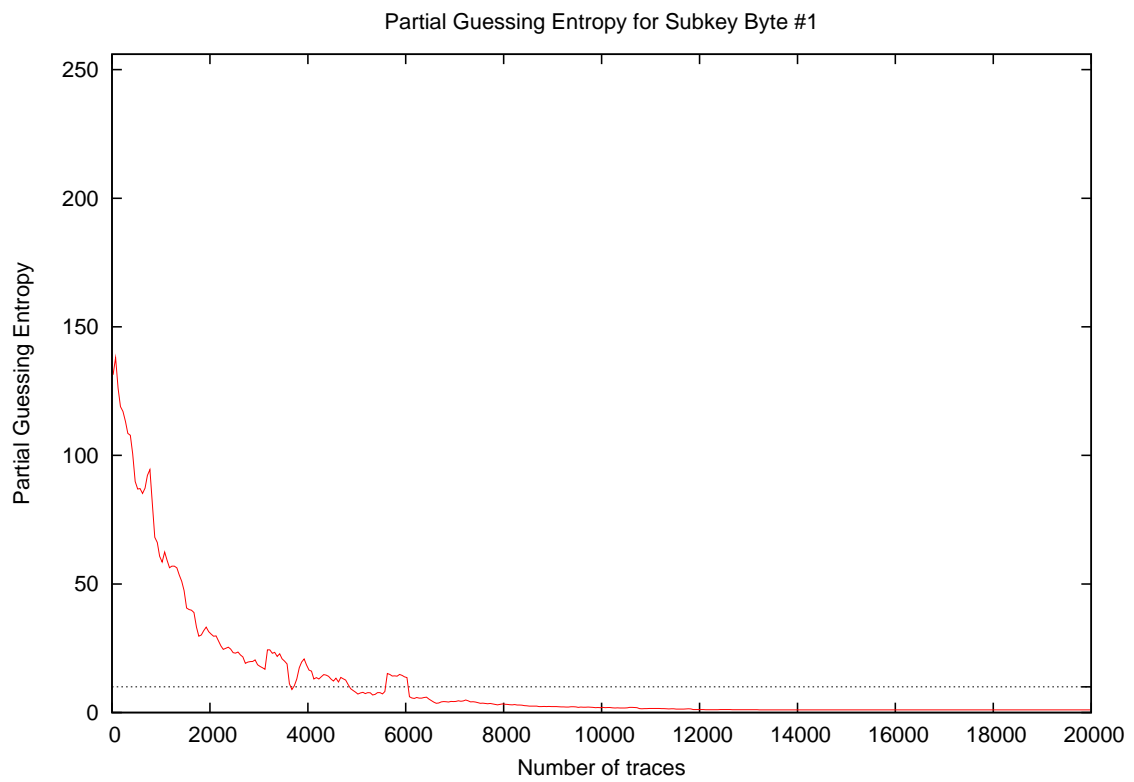


Partial Success Rate for Subkey Bytes #1 to #16

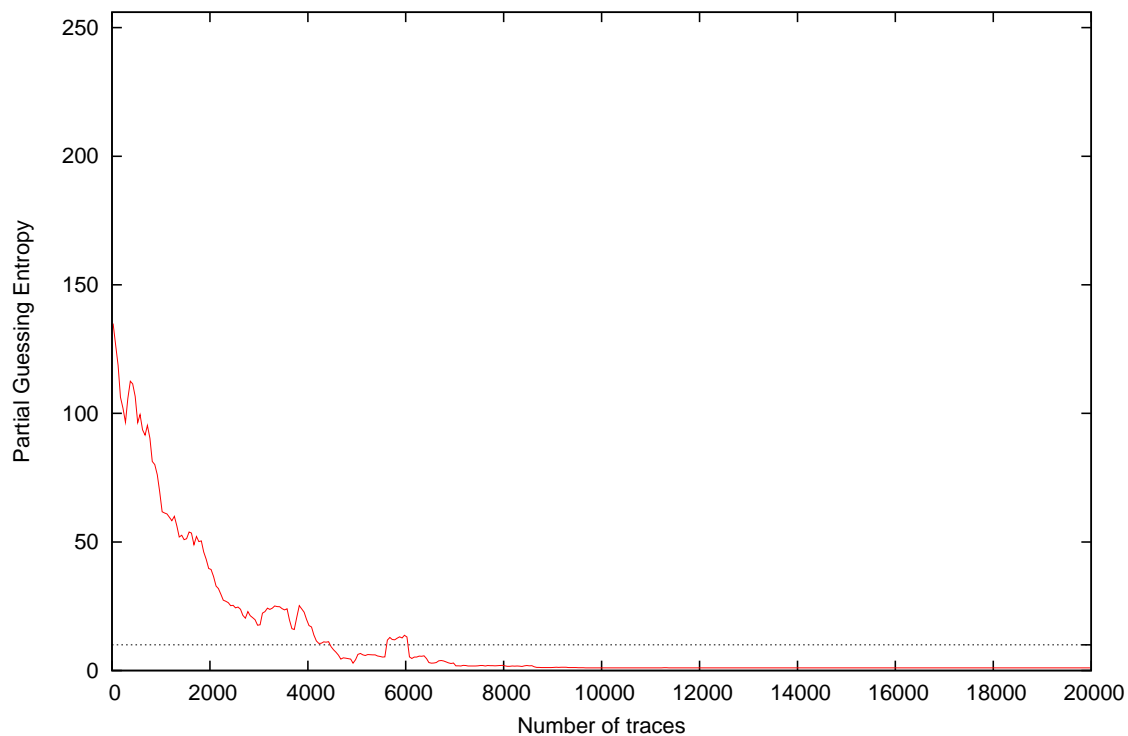


Traces	Partial Success Rate / Byte																Min	Max	Mean
	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16			
10	0.03	0.00	0.00	0.00	0.03	0.00	0.00	0.03	0.00	0.03	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.03	0.01
20	0.00	0.00	0.00	0.00	0.03	0.03	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.03	0.00
30	0.00	0.00	0.00	0.03	0.00	0.03	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.03	0.01
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	0.00	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	0.03	0.00	0.00	0.00	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	0.03	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
200	0.03	0.00	0.00	0.03	0.00	0.00	0.00	0.03	0.03	0.00	0.03	0.00	0.00	0.00	0.00	0.00	0.00	0.03	0.01
300	0.00	0.00	0.00	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	0.06	0.00
400	0.03	0.03	0.00	0.00	0.06	0.00	0.09	0.00	0.03	0.03	0.00	0.00	0.03	0.03	0.00	0.00	0.00	0.09	0.02
500	0.03	0.03	0.00	0.00	0.03	0.00	0.09	0.00	0.06	0.03	0.00	0.12	0.03	0.00	0.00	0.06	0.00	0.12	0.03
1000	0.06	0.03	0.03	0.06	0.12	0.09	0.16	0.00	0.16	0.09	0.06	0.16	0.19	0.00	0.03	0.06	0.00	0.19	0.08
2000	0.25	0.09	0.09	0.38	0.19	0.50	0.25	0.16	0.28	0.53	0.06	0.34	0.22	0.09	0.12	0.28	0.06	0.53	0.24
3000	0.34	0.25	0.22	0.53	0.28	0.75	0.50	0.31	0.47	0.78	0.19	0.53	0.34	0.25	0.16	0.44	0.16	0.78	0.40
4000	0.38	0.44	0.44	0.69	0.62	0.91	0.81	0.41	0.50	0.94	0.34	0.78	0.56	0.34	0.34	0.69	0.34	0.94	0.57
5000	0.44	0.62	0.59	0.75	0.56	0.91	0.78	0.59	0.56	1.00	0.47	0.94	0.75	0.47	0.41	0.75	0.41	1.00	0.66
10000	0.88	0.97	0.97	1.00	0.88	1.00	0.97	1.00	0.97	1.00	1.00	1.00	0.91	0.94	1.00	1.00	0.88	1.00	0.97
15000	0.97	1.00	1.00	1.00	0.97	1.00	1.00	1.00	0.97	1.00	1.00	1.00	0.94	1.00	1.00	1.00	0.94	1.00	0.99
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	0.97	1.00	1.00	1.00	0.97	1.00	1.00

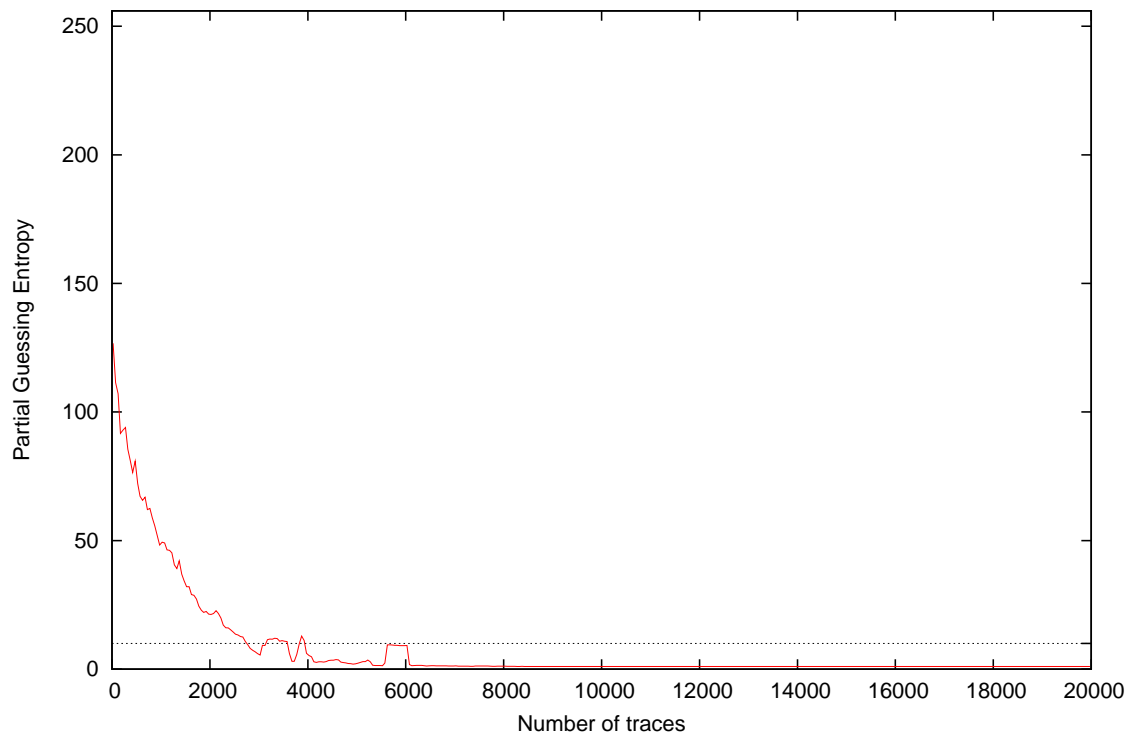
4 Partial Guessing Entropy



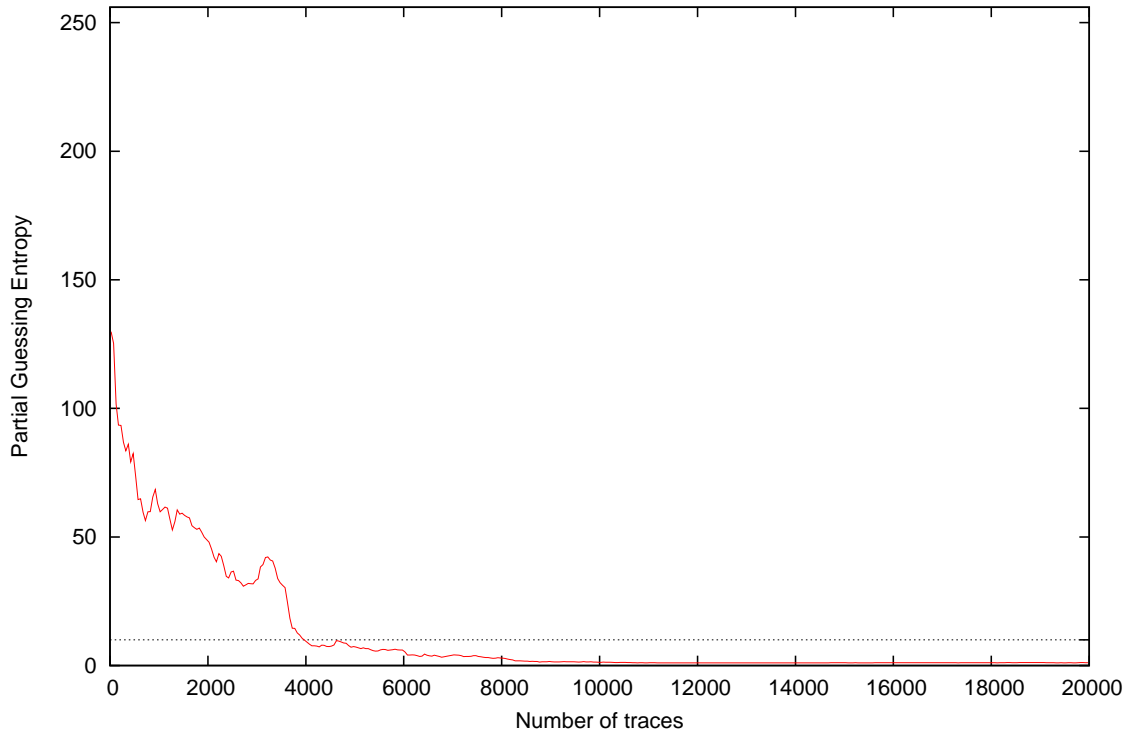
Partial Guessing Entropy for Subkey Byte #3



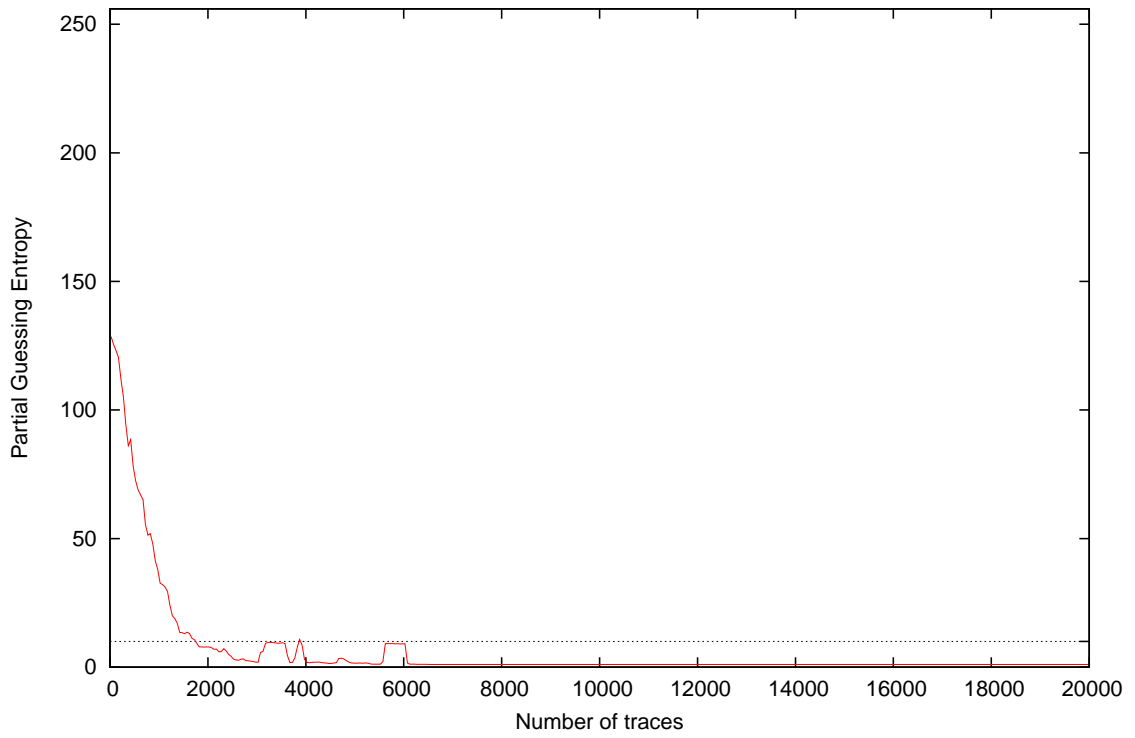
Partial Guessing Entropy for Subkey Byte #4



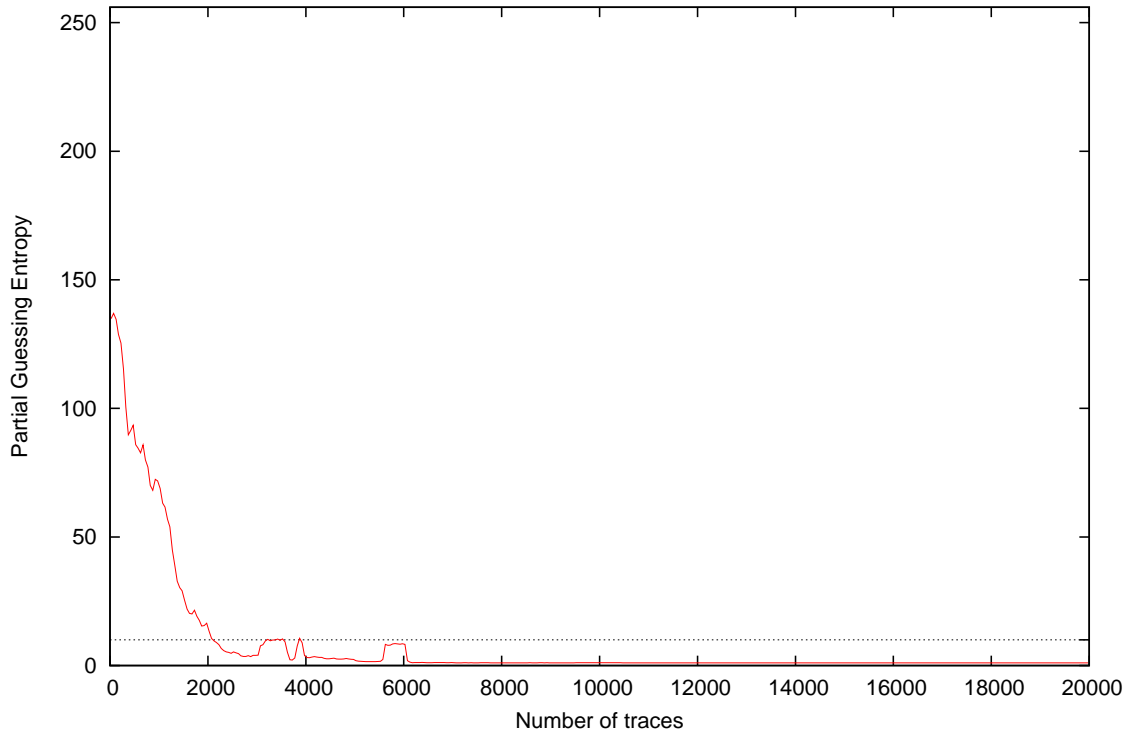
Partial Guessing Entropy for Subkey Byte #5



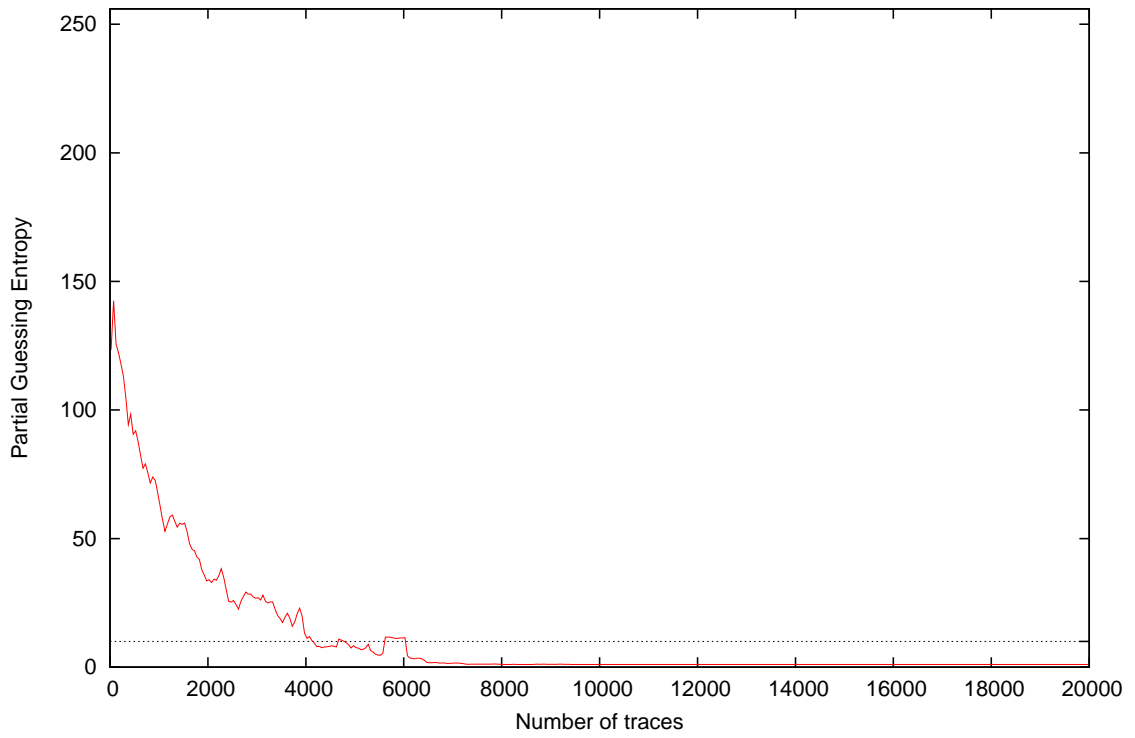
Partial Guessing Entropy for Subkey Byte #6



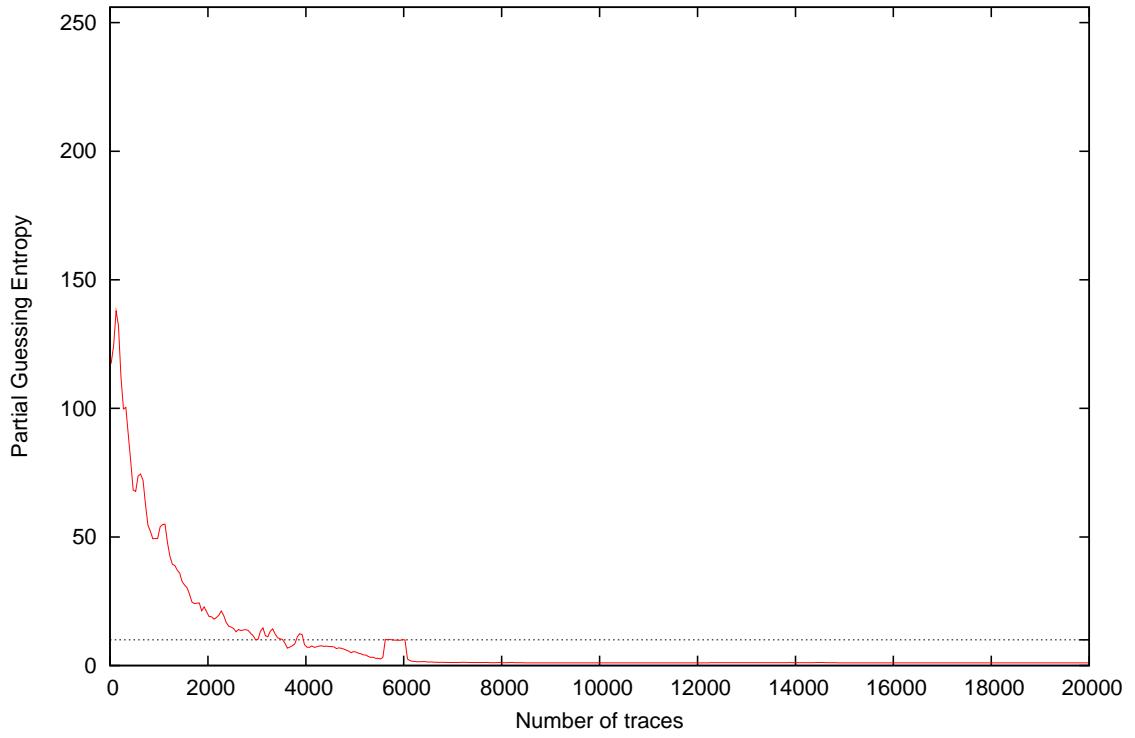
Partial Guessing Entropy for Subkey Byte #7



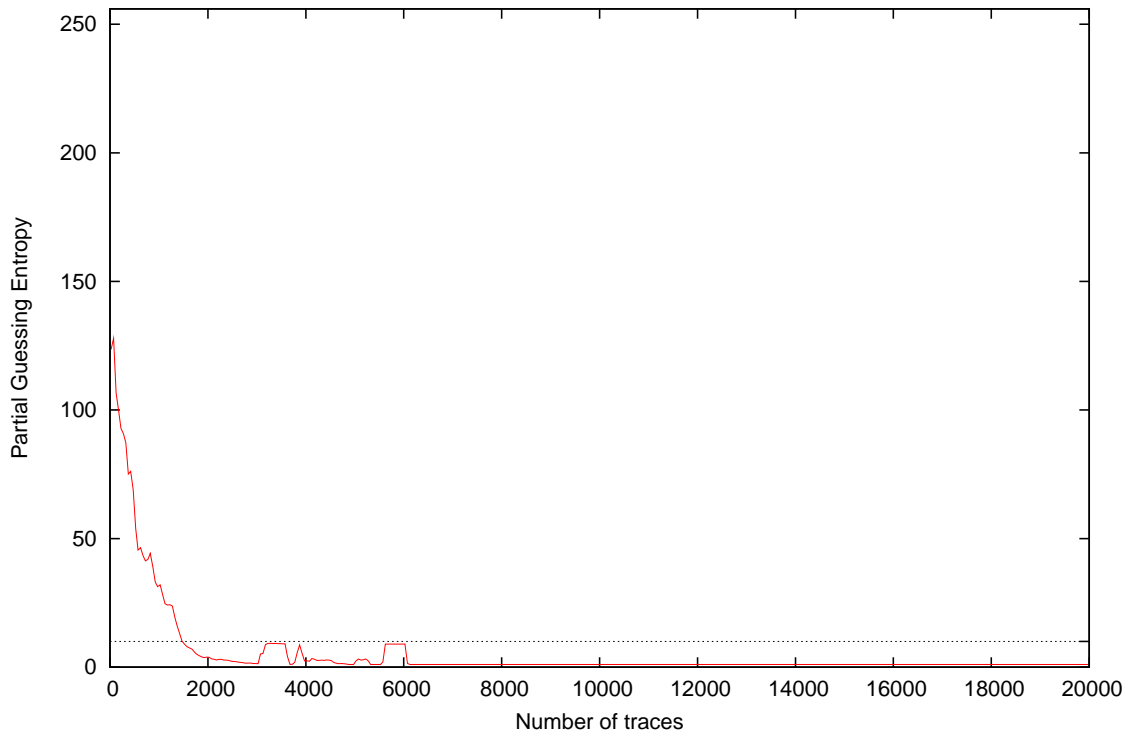
Partial Guessing Entropy for Subkey Byte #8



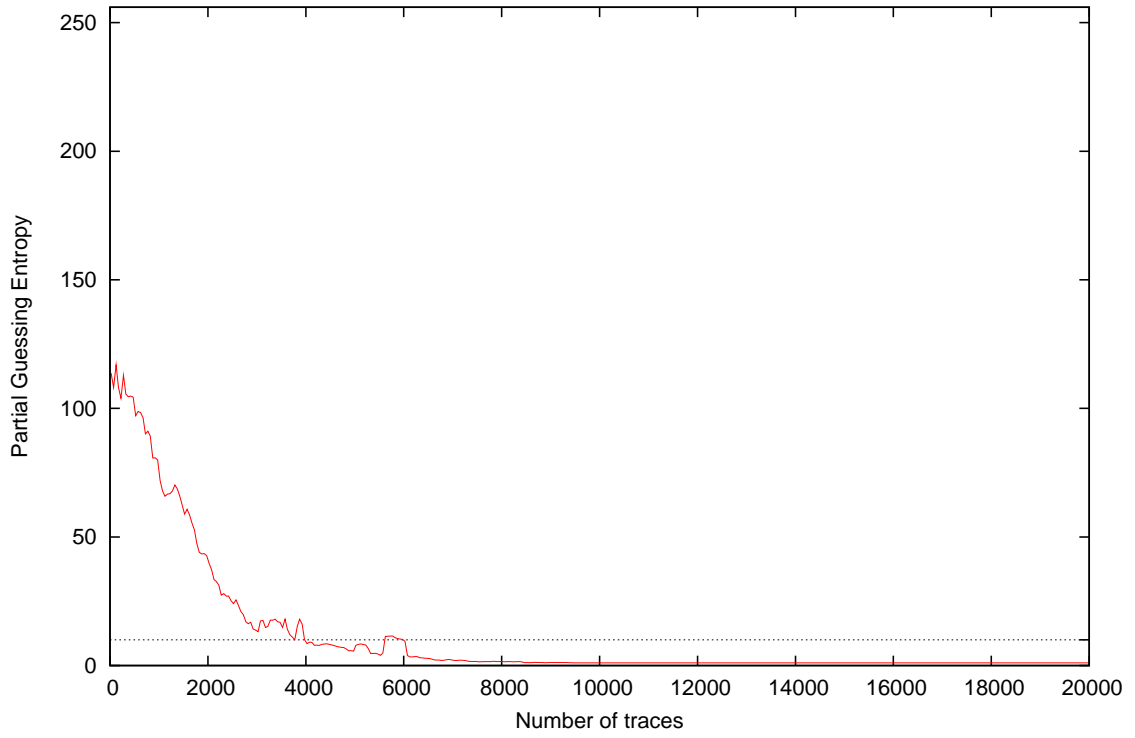
Partial Guessing Entropy for Subkey Byte #9



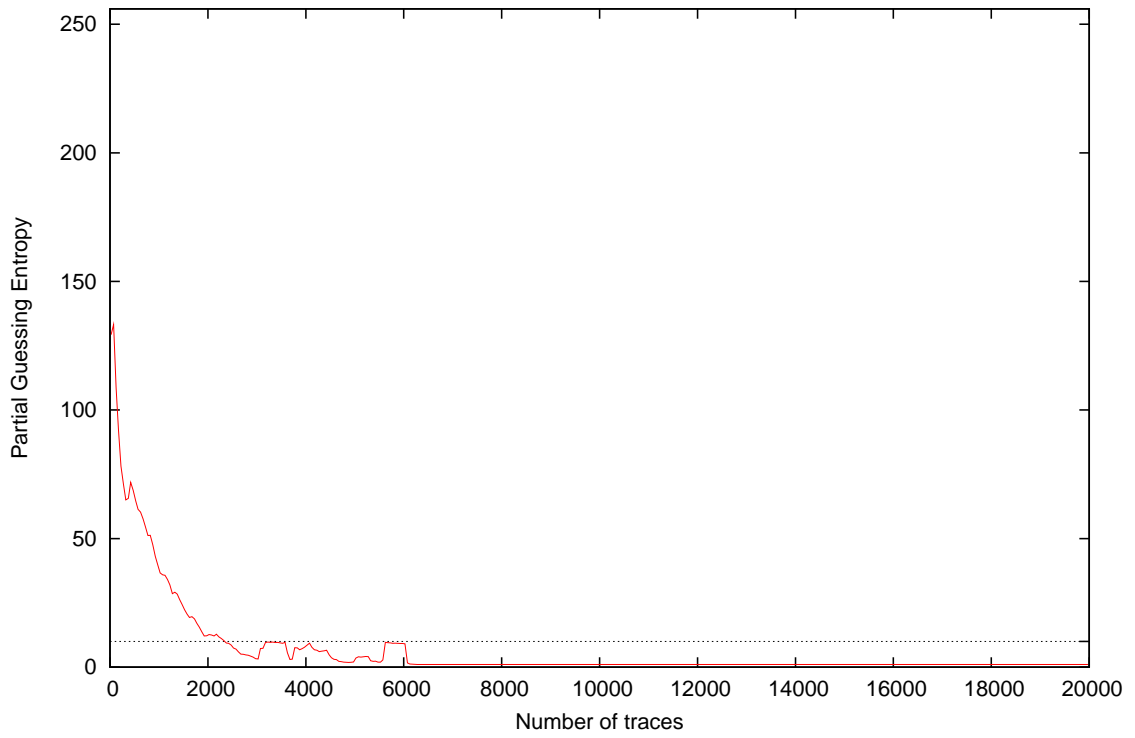
Partial Guessing Entropy for Subkey Byte #10



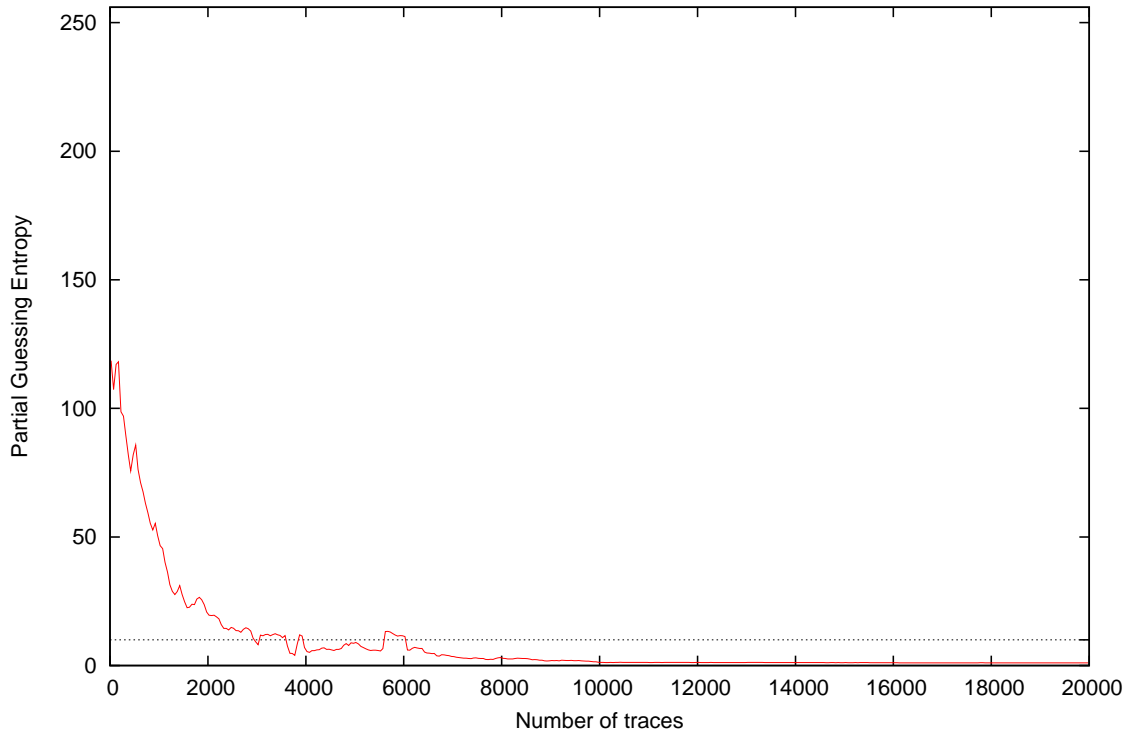
Partial Guessing Entropy for Subkey Byte #11



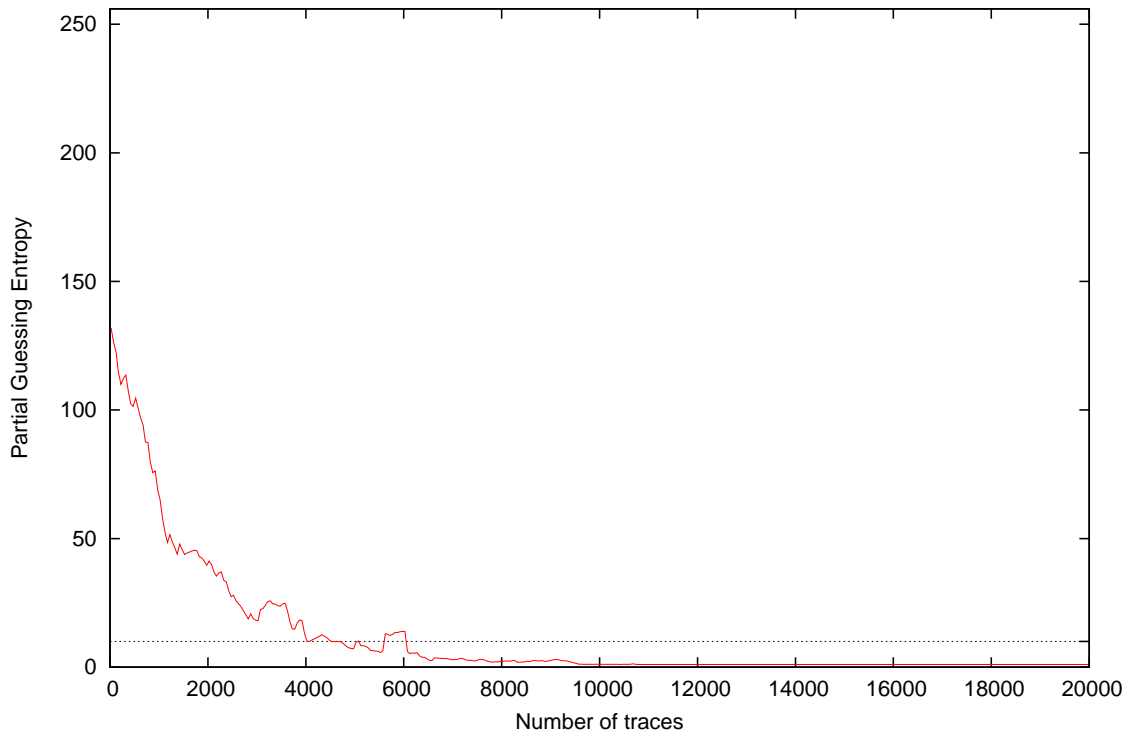
Partial Guessing Entropy for Subkey Byte #12

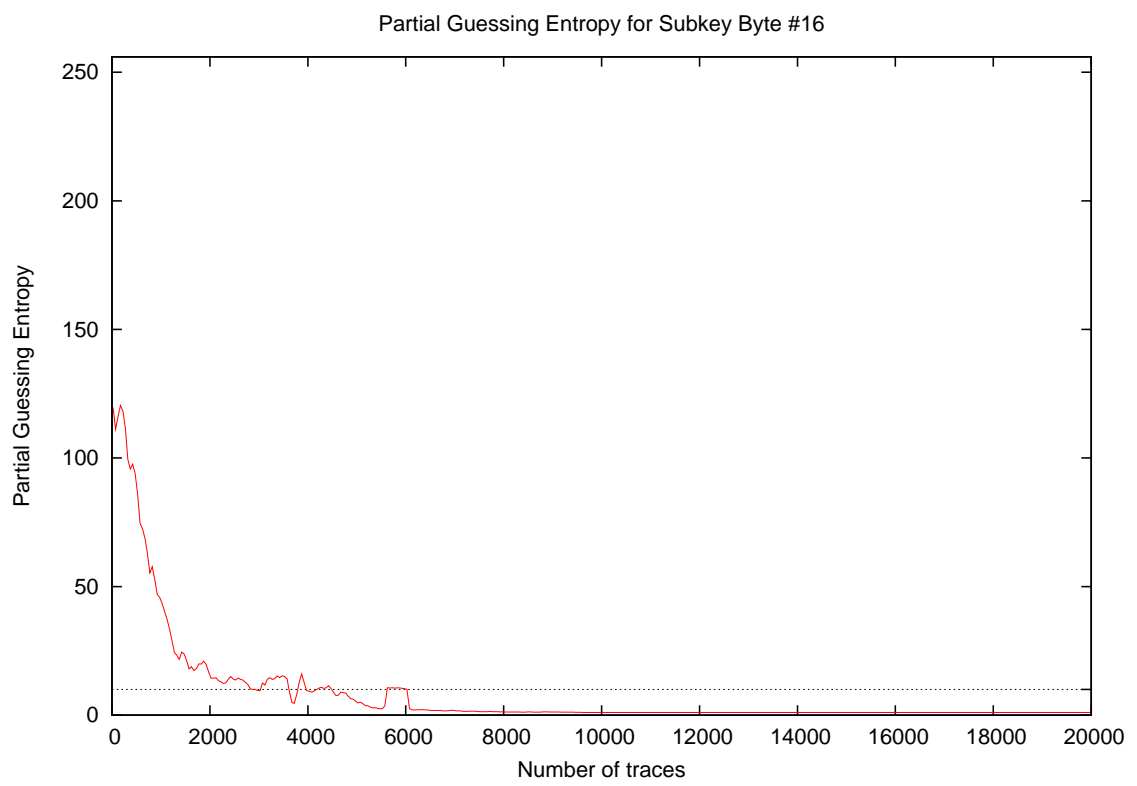
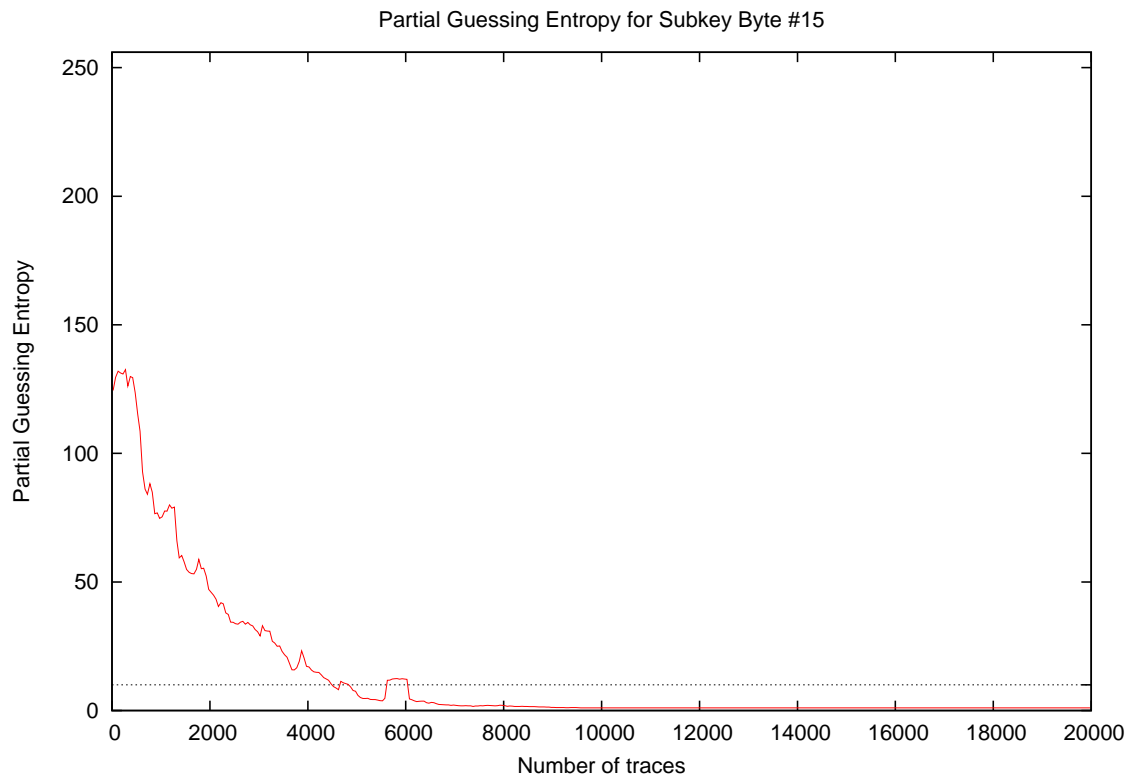


Partial Guessing Entropy for Subkey Byte #13

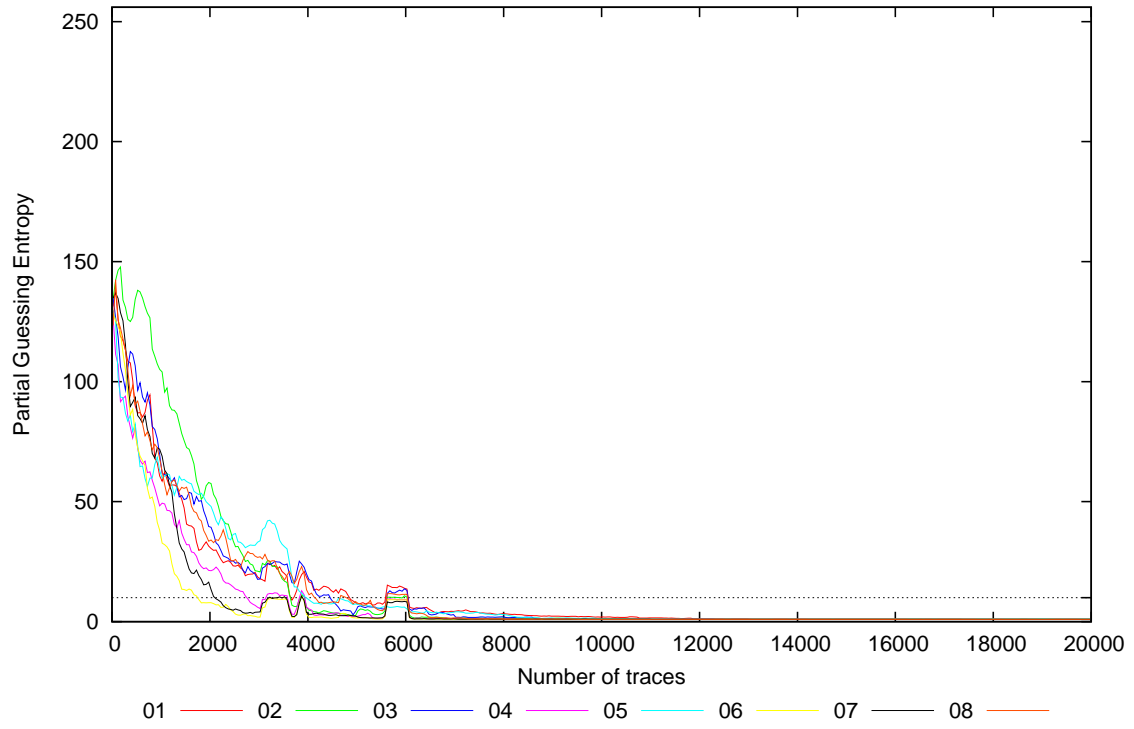


Partial Guessing Entropy for Subkey Byte #14

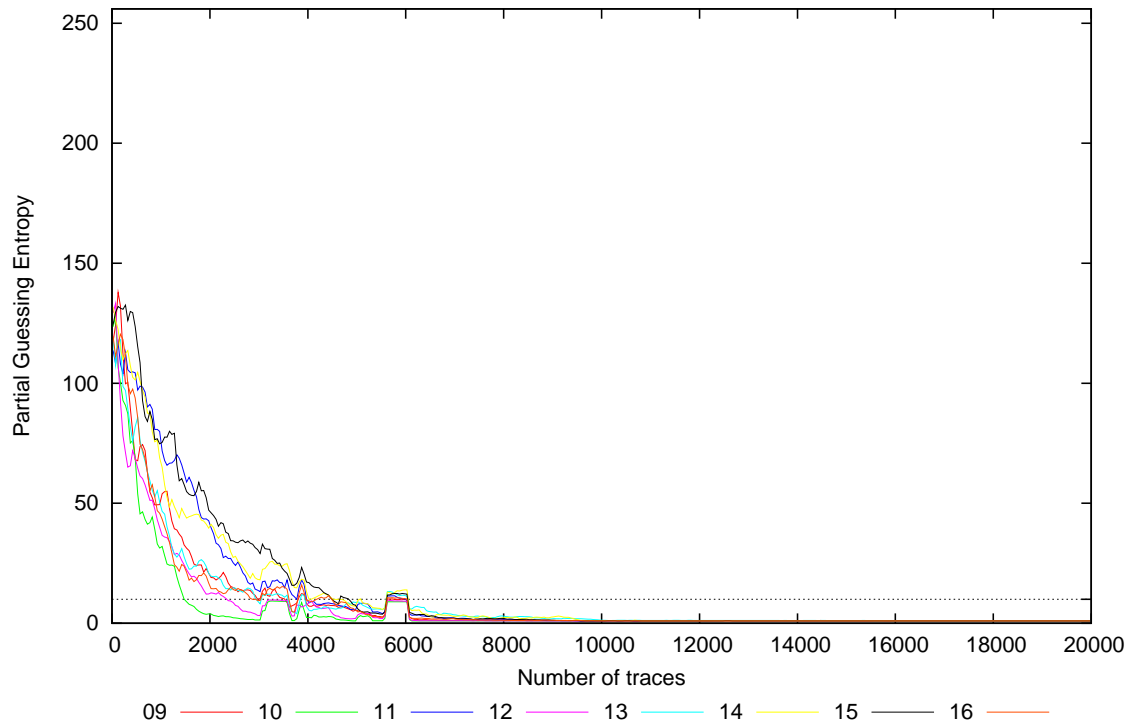




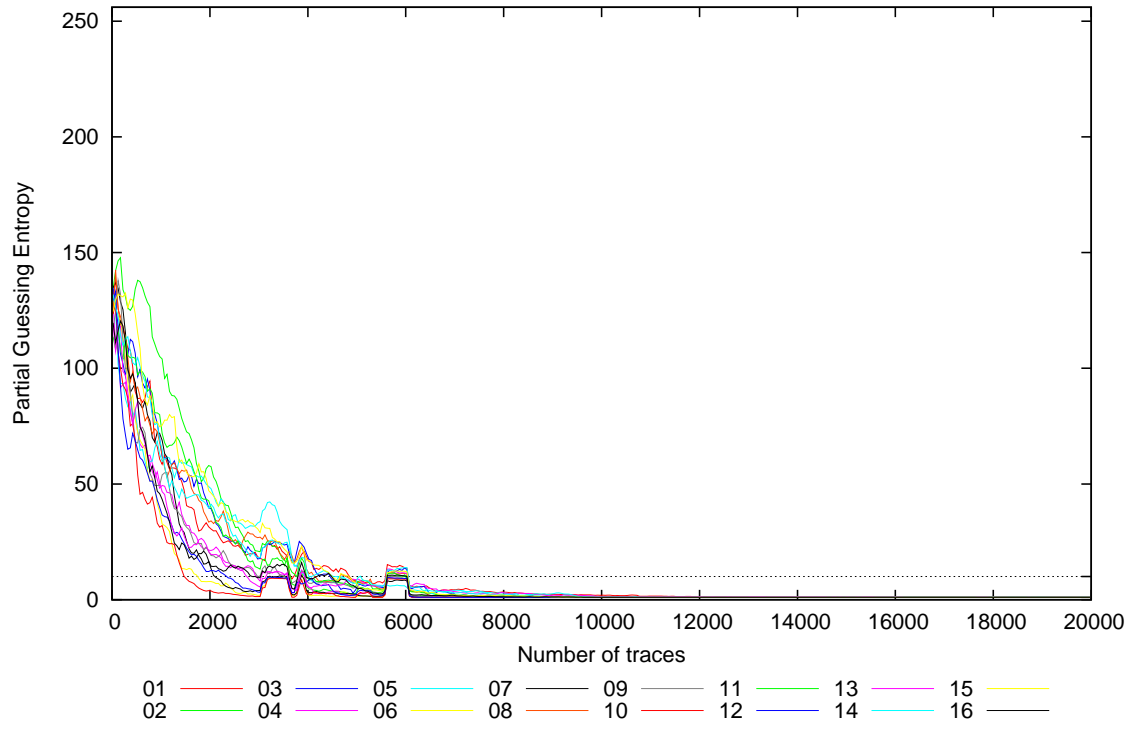
Partial Guessing Entropy for Subkey Bytes #1 to #8



Partial Guessing Entropy for Subkey Bytes #9 to #16



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	122.3	129.2	122.5	148.3	107.3	126.4	132.6	137.2	126.4	118.9	123.7	116.0	135.4	138.8	116.7	137.2	107.3	148.3	127.4
20	123.5	127.5	142.9	114.1	144.1	116.0	142.0	120.4	130.3	115.6	110.7	130.3	124.5	135.8	132.2	128.8	110.7	144.1	127.4
30	134.8	137.4	144.8	132.1	127.6	143.5	136.8	122.7	100.8	126.9	106.0	131.5	117.0	137.2	128.9	109.2	100.8	144.8	127.3
40	139.2	133.1	134.3	131.4	132.2	137.8	142.7	116.7	120.2	115.0	118.9	132.8	115.3	116.3	121.6	110.0	110.0	142.7	126.1
50	130.8	137.7	134.6	131.6	137.8	133.3	133.2	140.0	109.3	112.4	101.0	128.8	105.7	129.1	116.9	112.6	101.0	140.0	124.7
100	133.7	143.5	122.9	105.0	104.7	125.9	126.7	133.1	136.3	110.8	121.8	115.0	103.8	129.3	128.4	110.3	103.8	143.5	122.0
200	119.4	143.3	107.7	84.9	87.2	115.2	131.4	120.5	123.6	94.4	100.6	82.3	114.5	107.2	122.6	120.0	82.3	143.3	110.9
300	116.7	132.3	105.8	93.8	83.2	106.3	108.8	115.4	98.0	90.9	105.8	70.5	91.2	107.8	126.4	109.8	70.5	132.3	103.9
400	105.6	131.0	111.2	75.2	89.2	90.2	86.2	94.8	82.9	71.8	101.5	65.1	76.7	98.8	136.9	96.0	65.1	136.9	94.6
500	86.8	134.1	105.5	76.6	78.9	74.0	84.9	87.5	63.4	59.4	97.8	66.8	88.5	105.9	118.8	88.6	59.4	134.1	88.6
1000	60.9	105.8	64.3	49.7	60.9	35.6	71.4	64.1	55.4	32.4	77.4	36.4	49.1	66.7	76.2	42.4	32.4	105.8	59.3
2000	30.5	58.2	37.8	20.8	47.5	8.0	14.7	34.9	20.1	4.2	42.6	12.4	19.2	39.2	45.2	15.3	4.2	58.2	28.2
3000	17.6	20.6	18.1	5.9	32.8	1.8	4.1	27.7	9.9	1.4	14.1	3.5	8.7	18.4	29.3	9.6	1.4	32.8	14.0
4000	17.3	4.7	17.4	5.0	9.0	1.9	3.0	11.0	7.0	2.5	8.3	8.1	6.1	10.6	16.8	9.3	1.9	17.4	8.6
5000	7.3	2.5	5.7	2.0	7.6	1.4	2.1	7.8	5.4	1.0	5.5	2.2	8.5	7.5	7.3	5.3	1.0	8.5	4.9
10000	1.9	1.0	1.0	1.0	1.2	1.0	1.1	1.0	1.0	1.0	1.0	1.0	1.2	1.1	1.0	1.0	1.0	1.9	1.1
15000	1.0	1.0	1.0	1.0	1.1	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.1	1.0	1.0	1.0	1.0	1.1	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