

Evaluation results

DPA contest v2

September 2010

1 Introduction

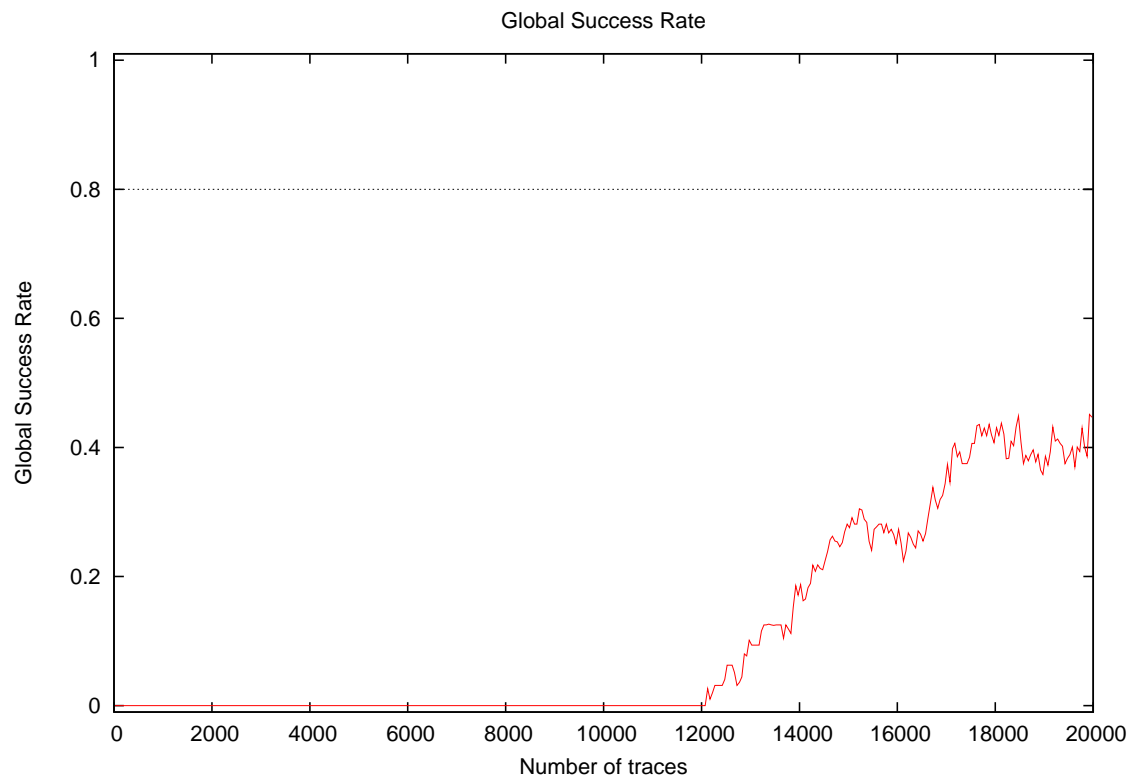
1.1 About the attack

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

1.2 About the evaluation

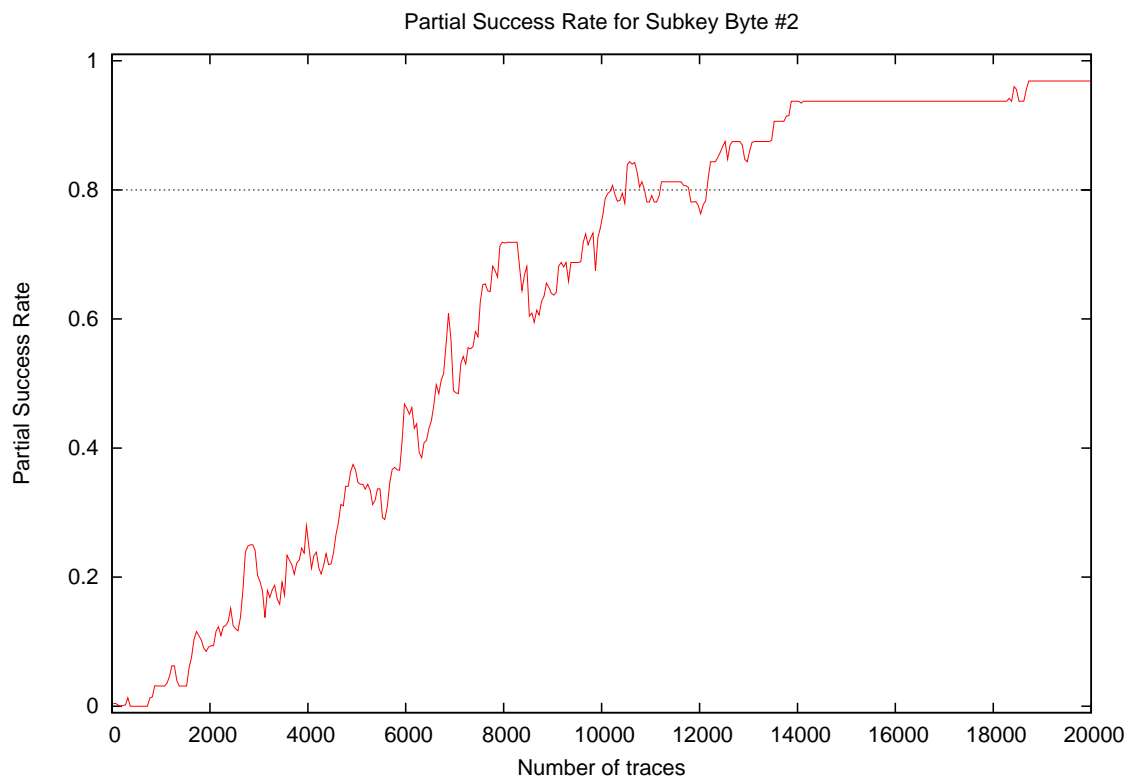
- **Date of evaluation:** August 2010

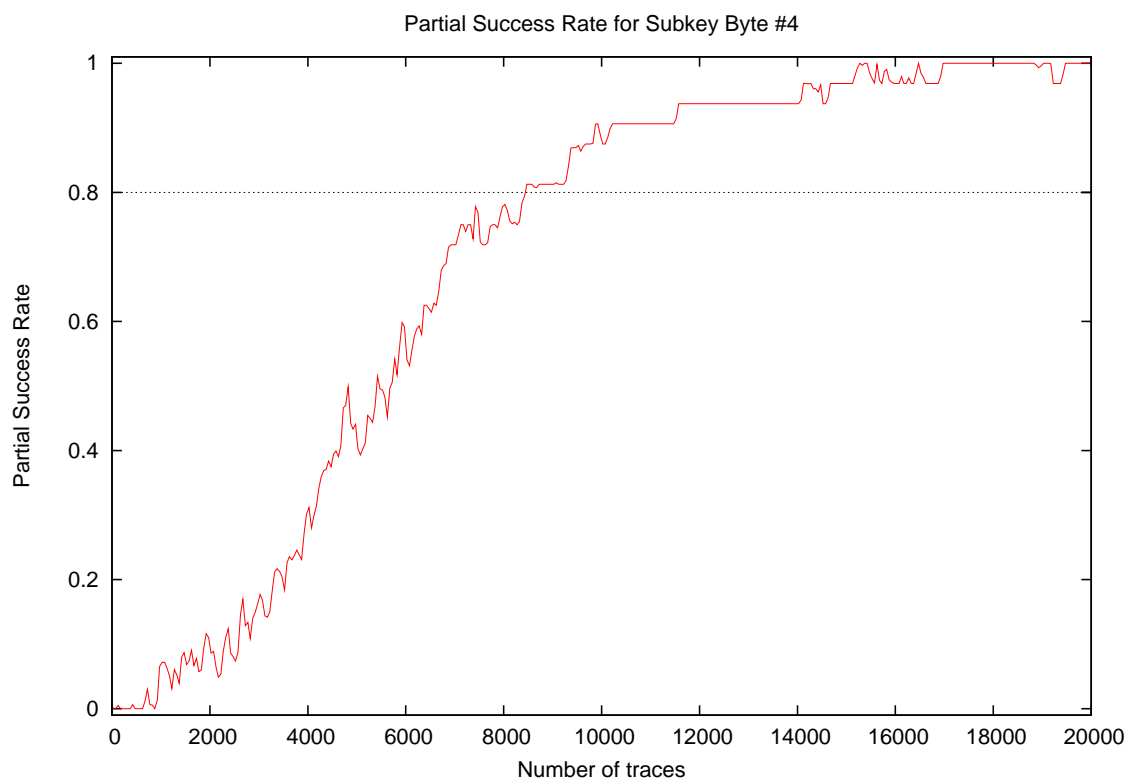
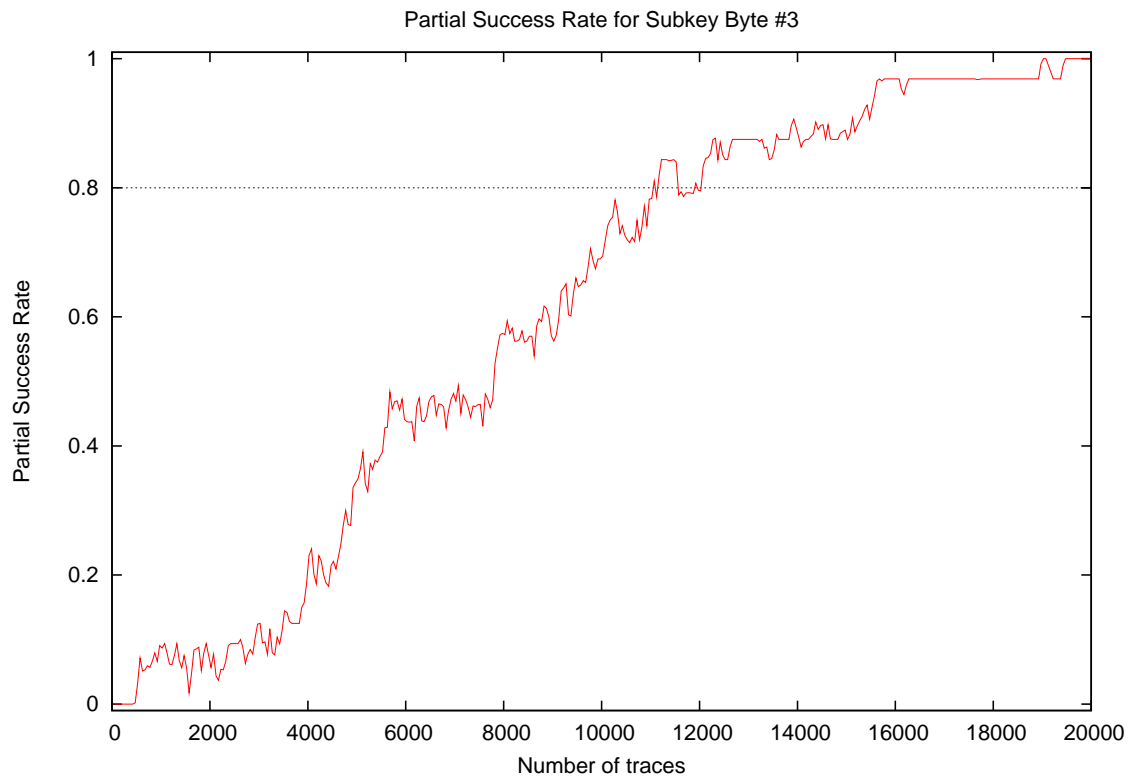
2 Global Success Rate

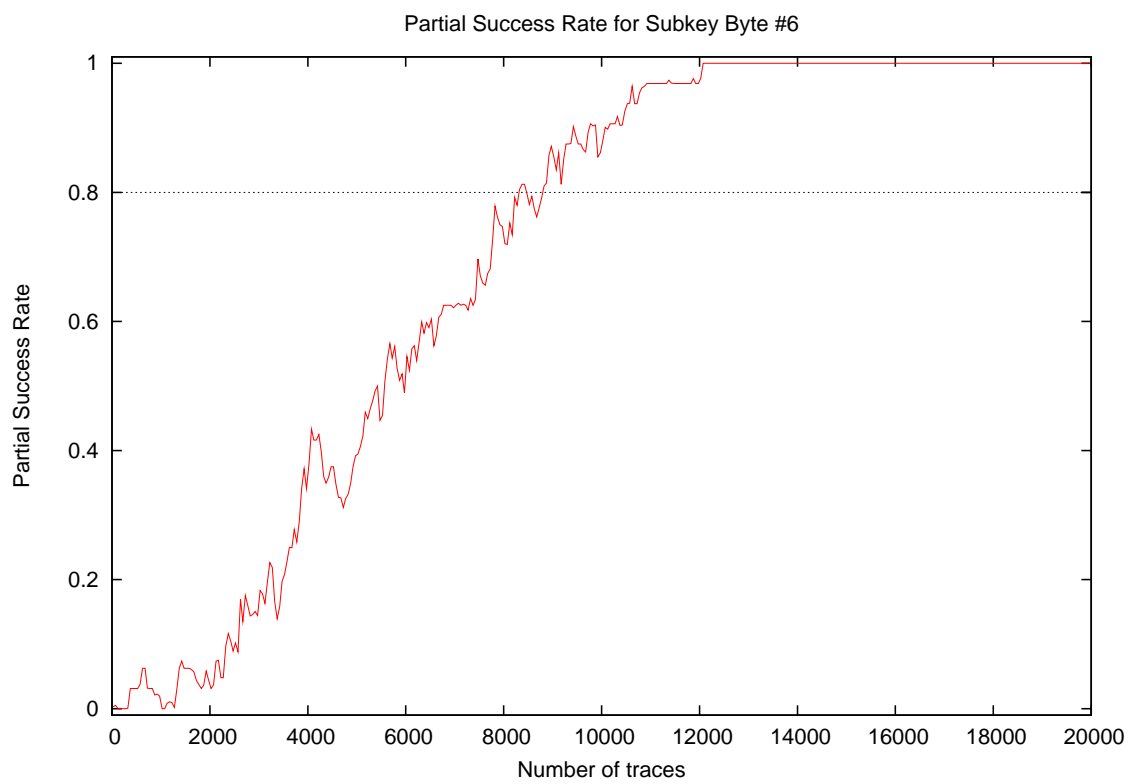
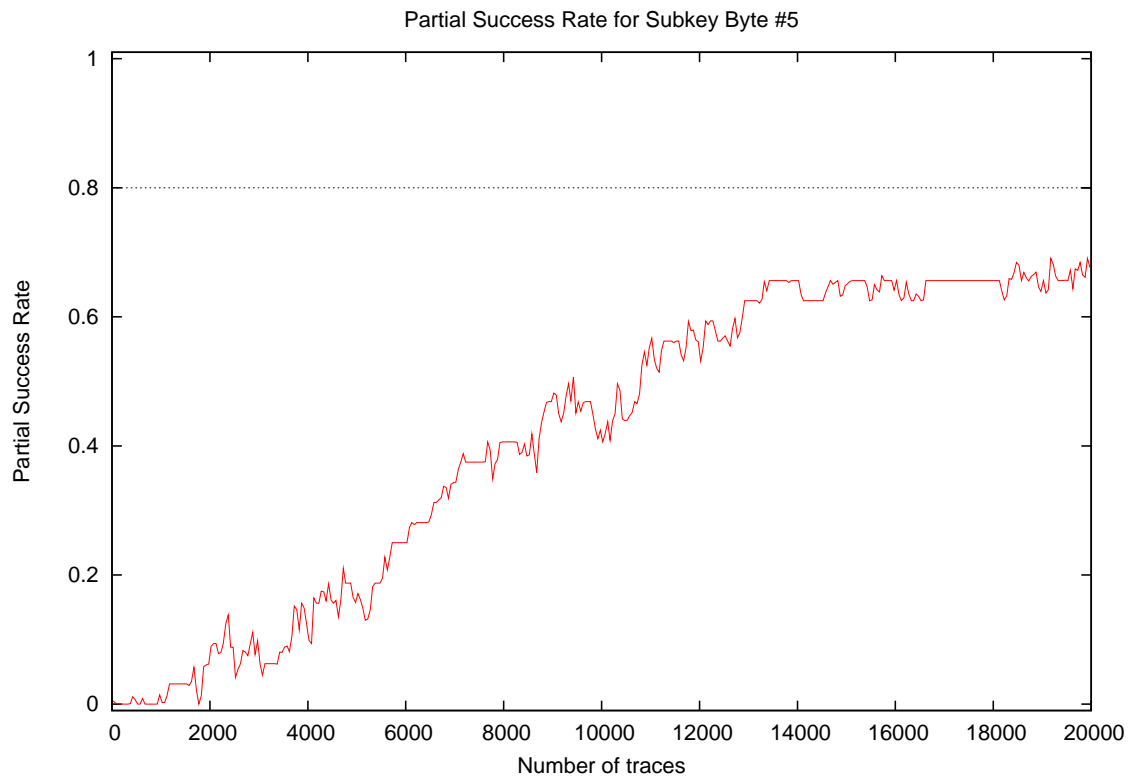


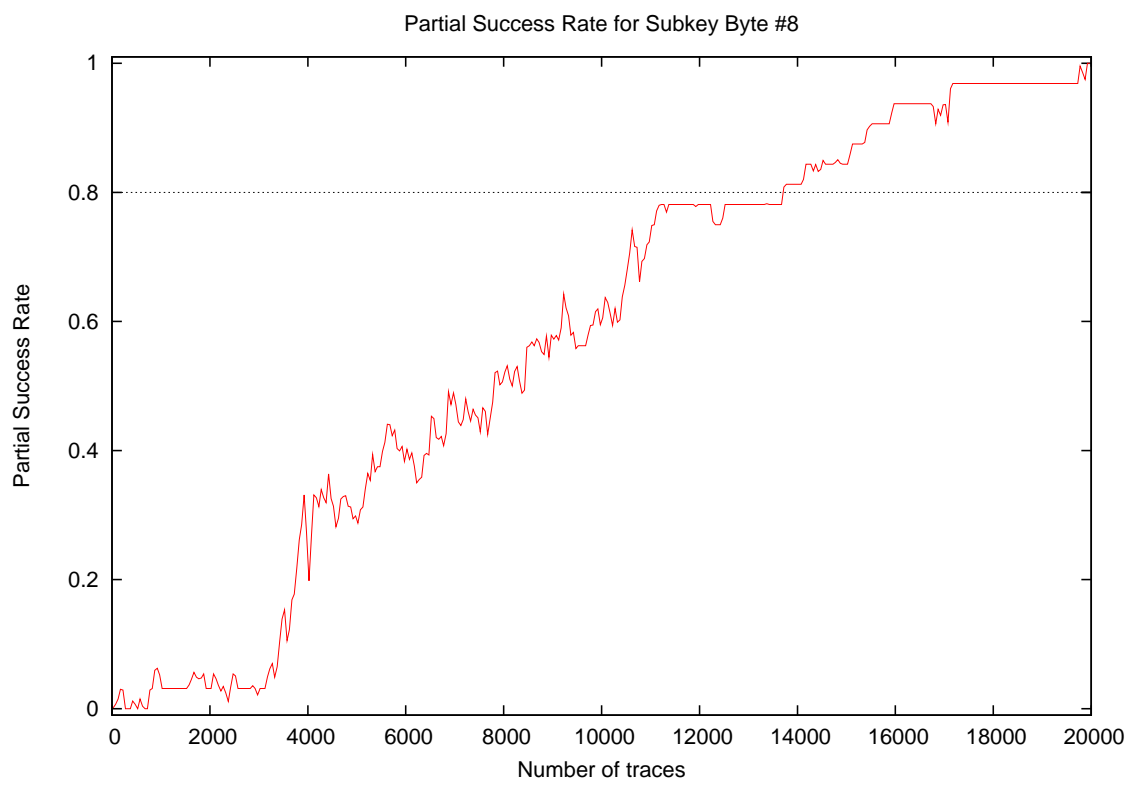
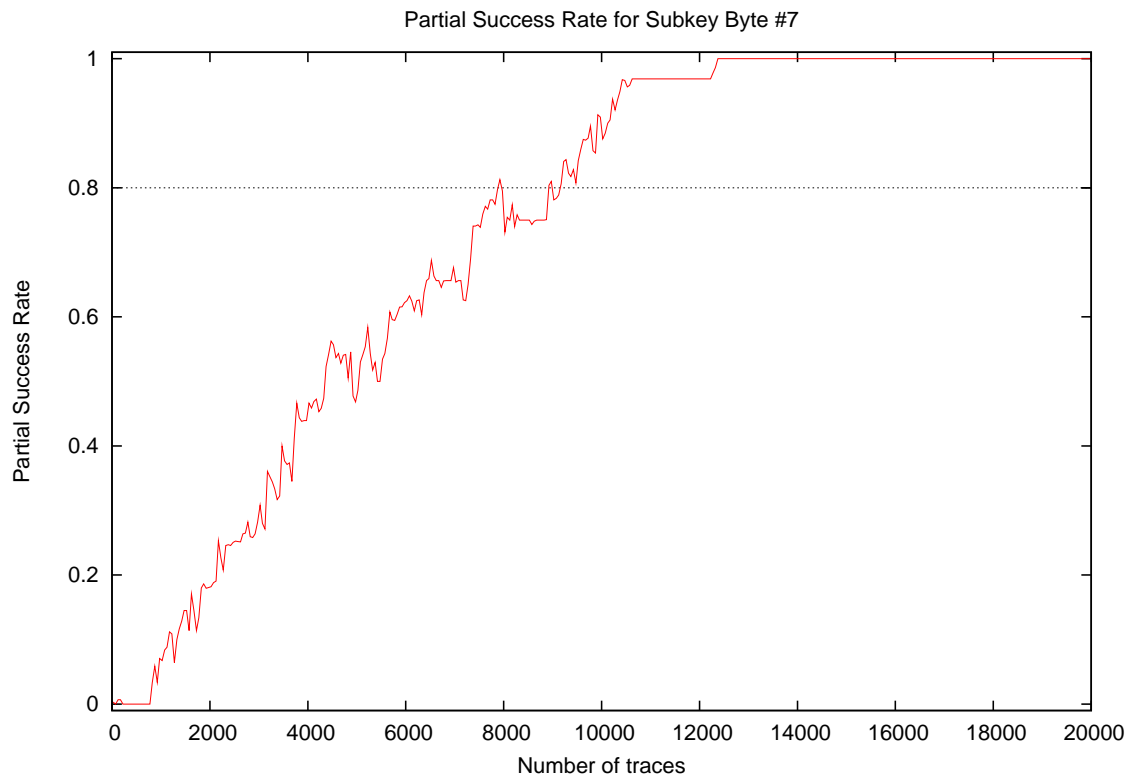
Number of traces	Global Success Rate
10	0.00
20	0.00
30	0.00
40	0.00
50	0.00
100	0.00
200	0.00
300	0.00
400	0.00
500	0.00
1000	0.00
2000	0.00
3000	0.00
4000	0.00
5000	0.00
10000	0.00
15000	0.28
20000	0.44

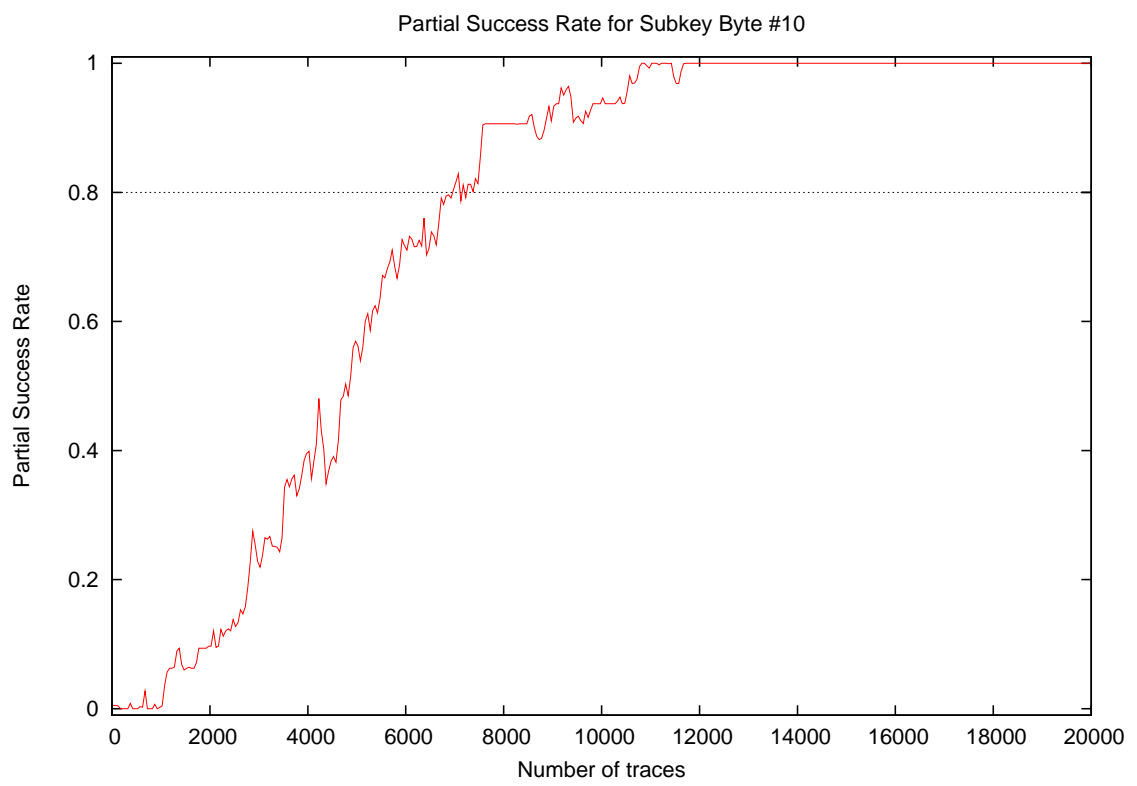
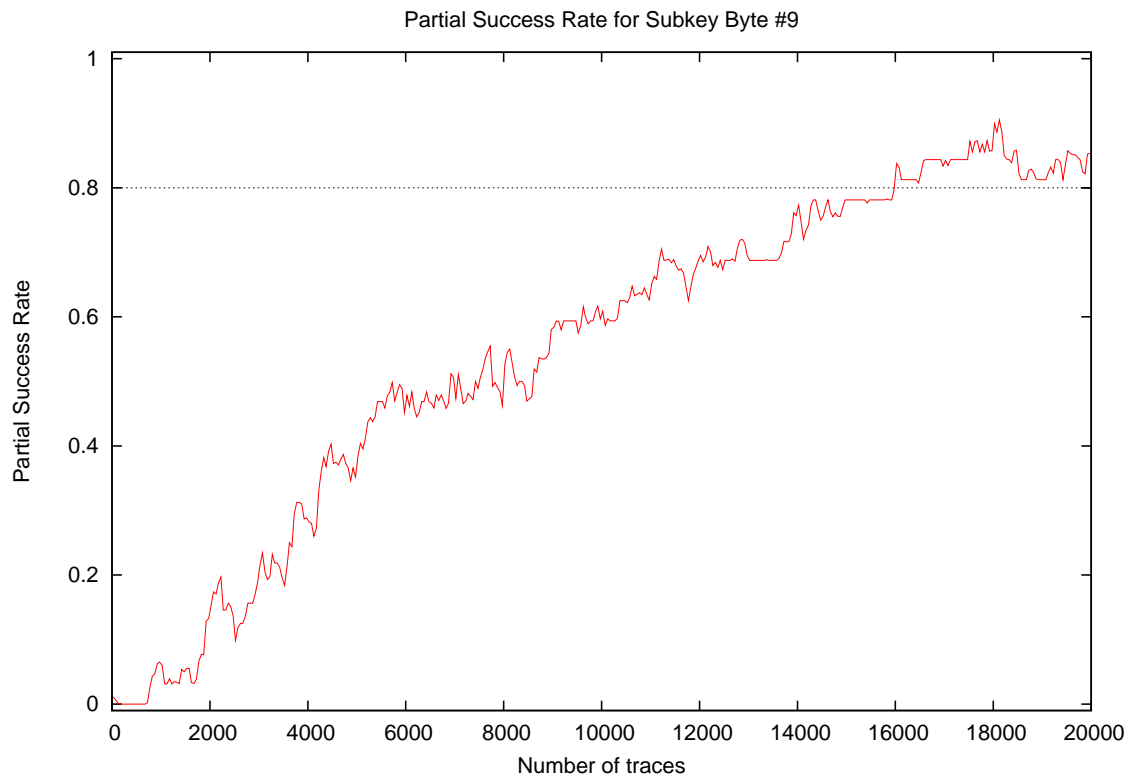
3 Partial Success Rate

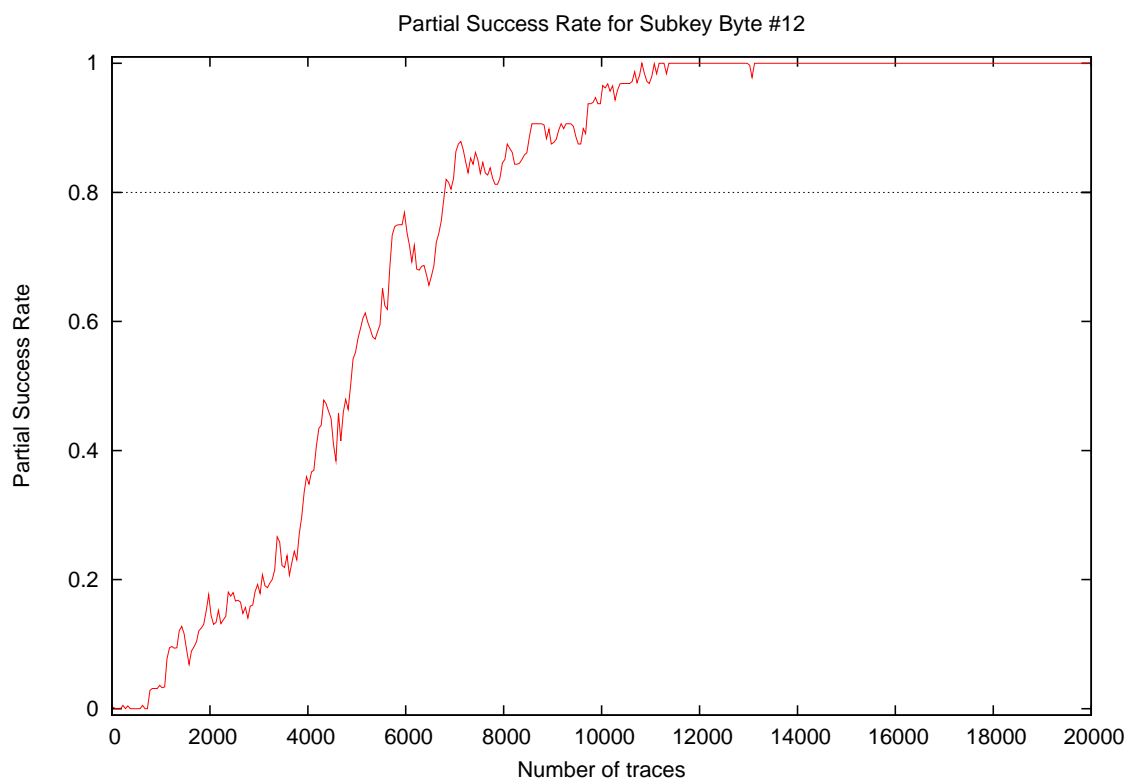
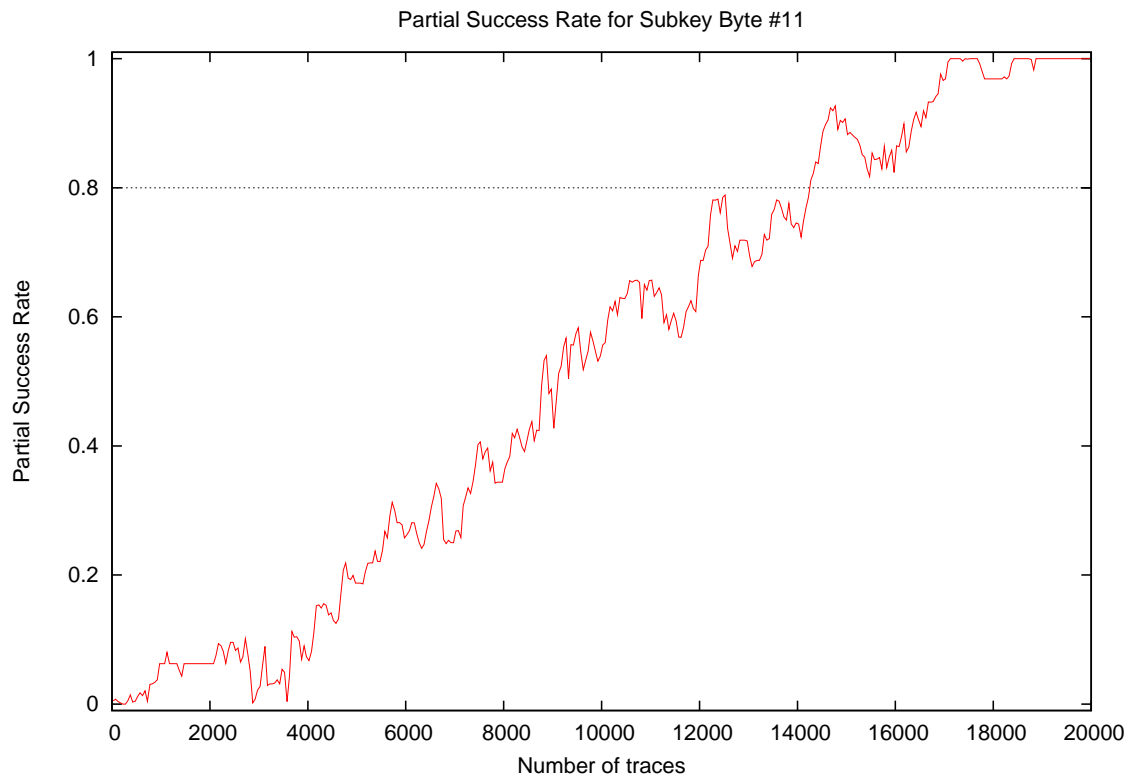


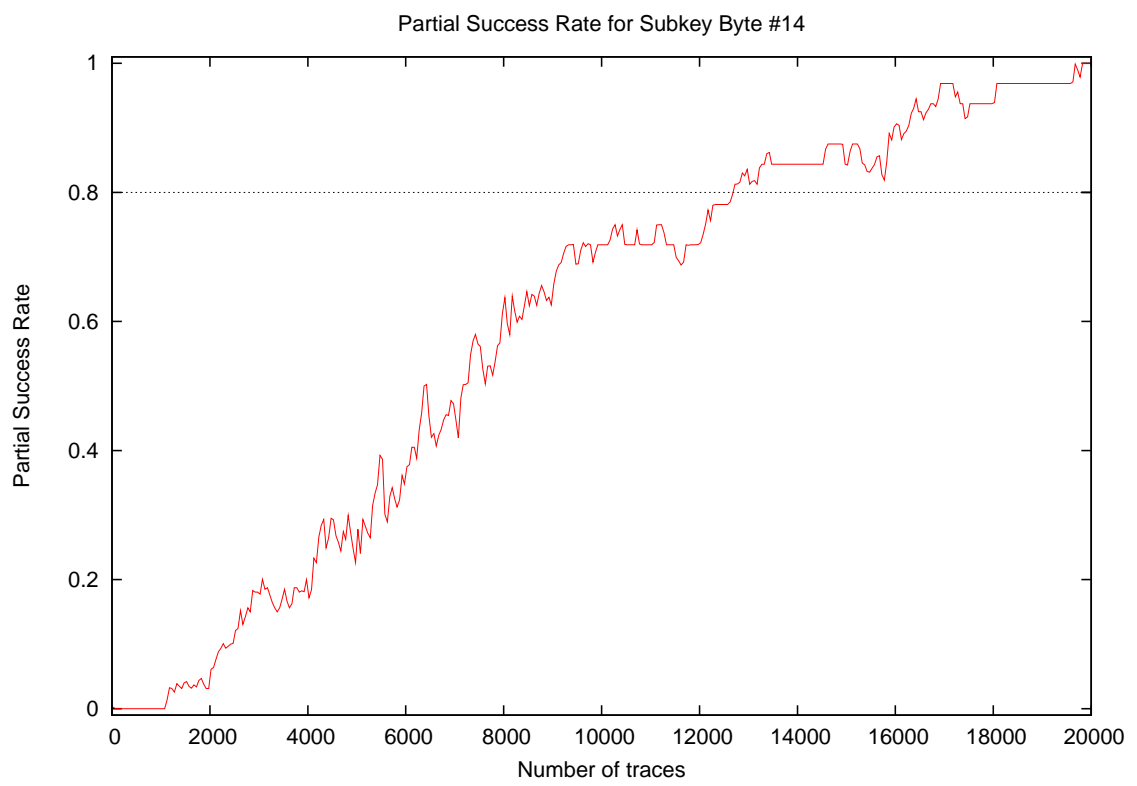
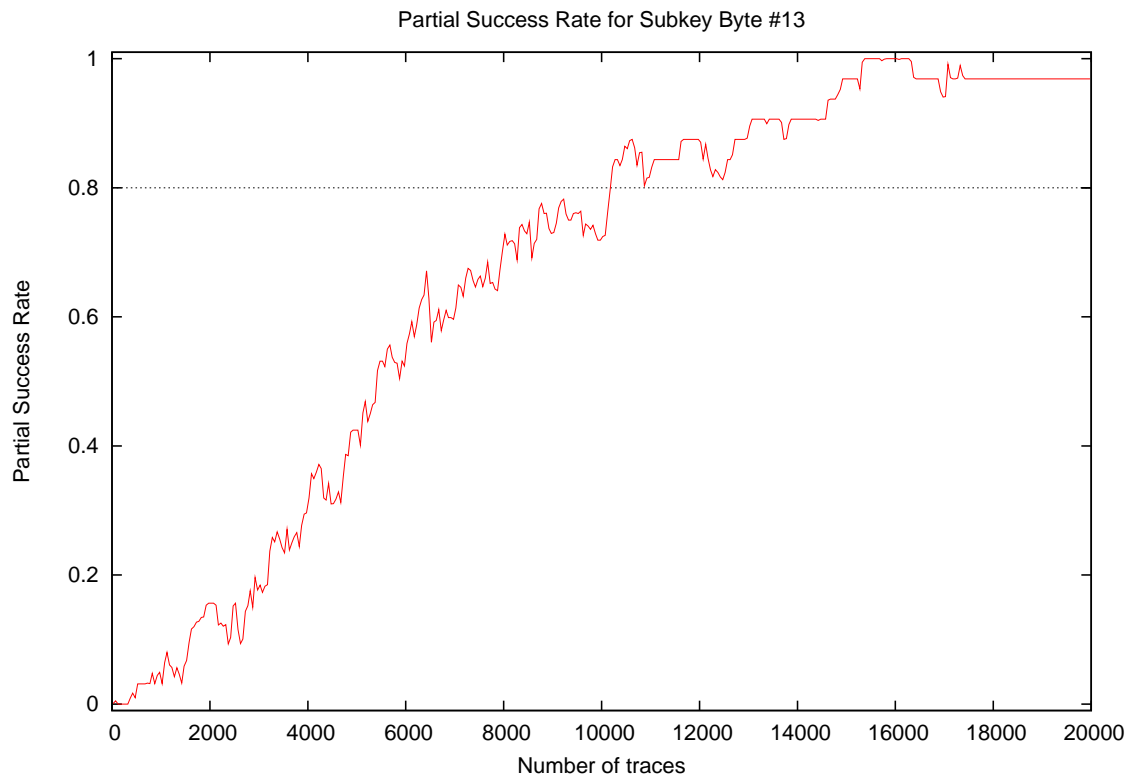


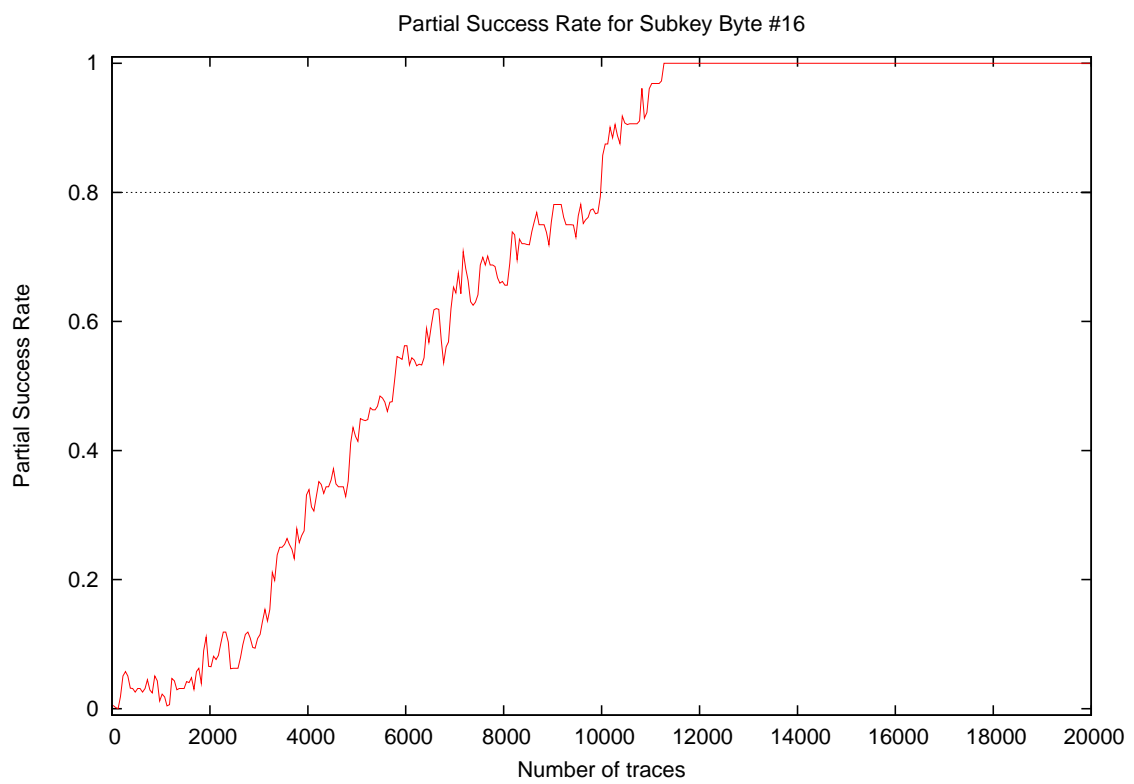
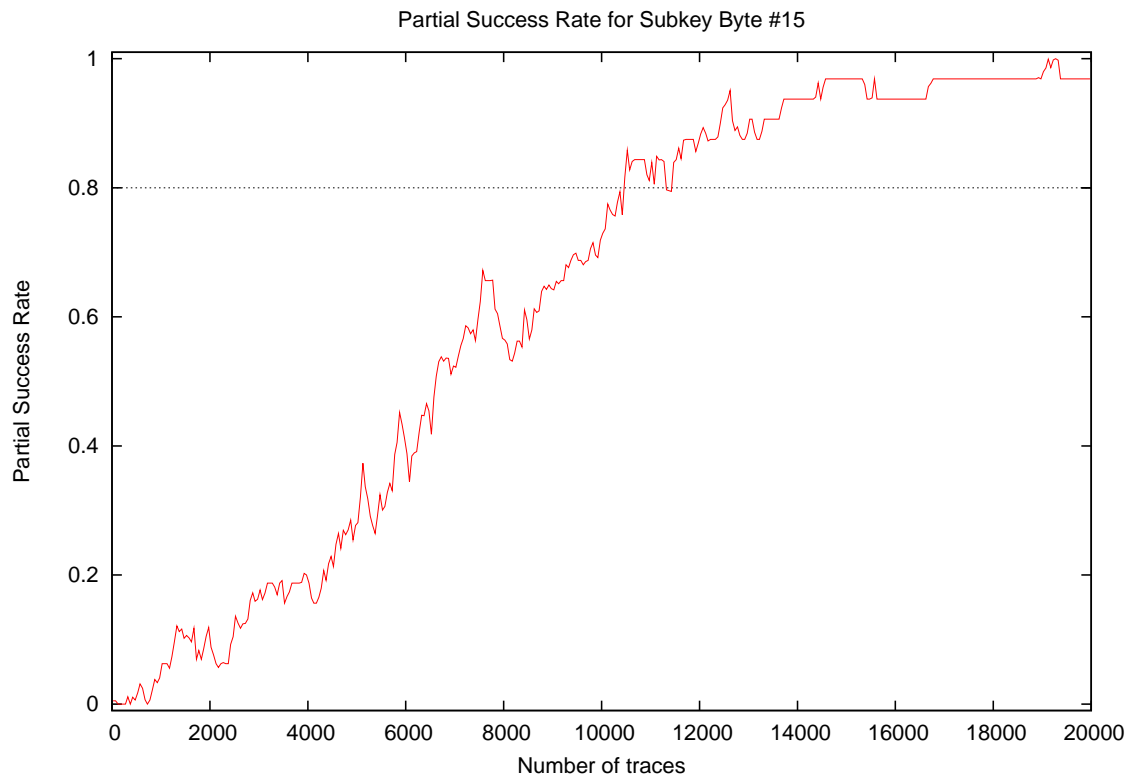




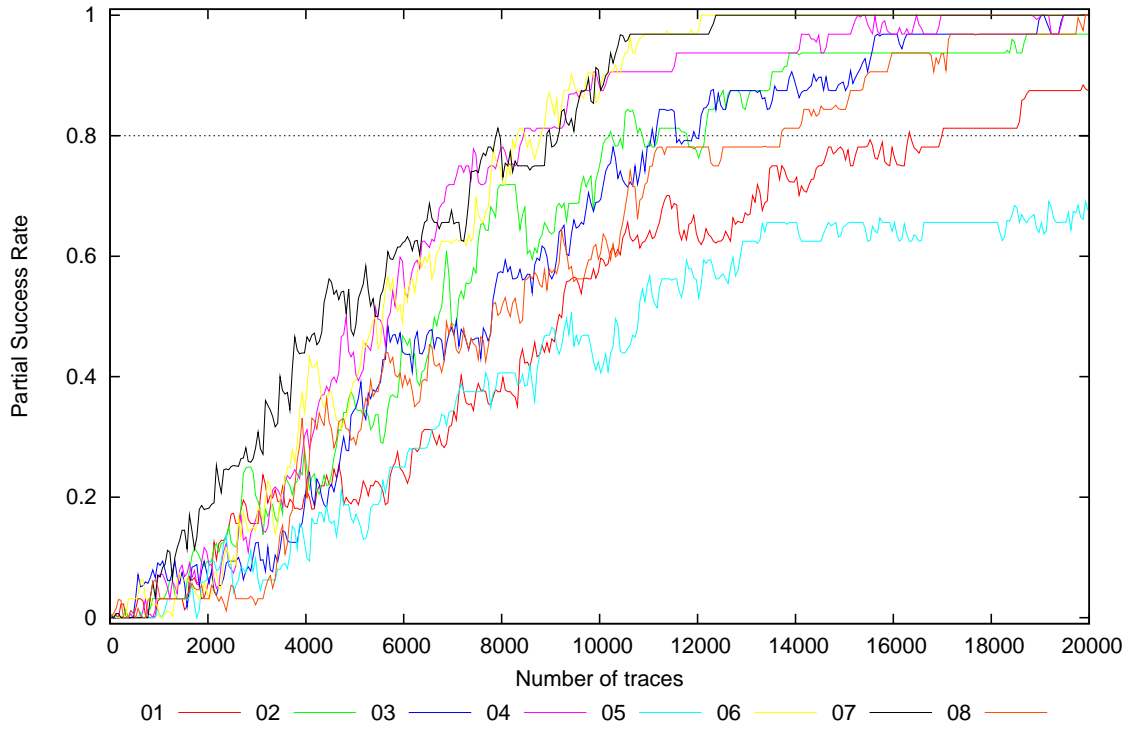




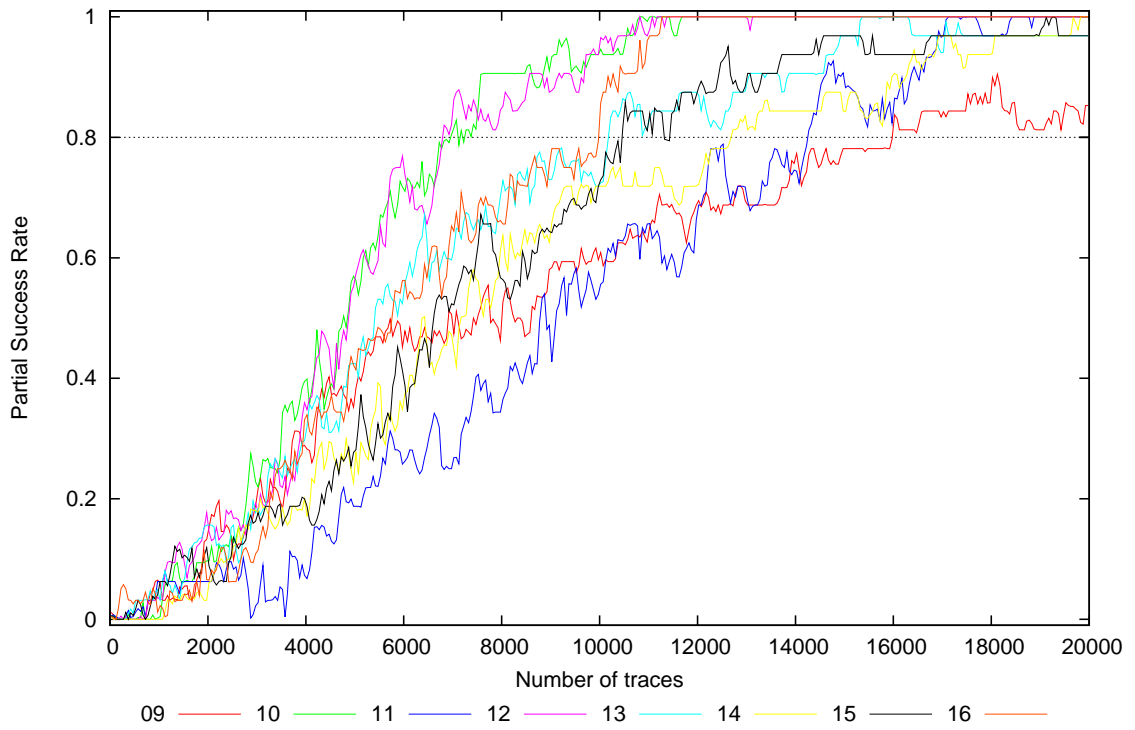




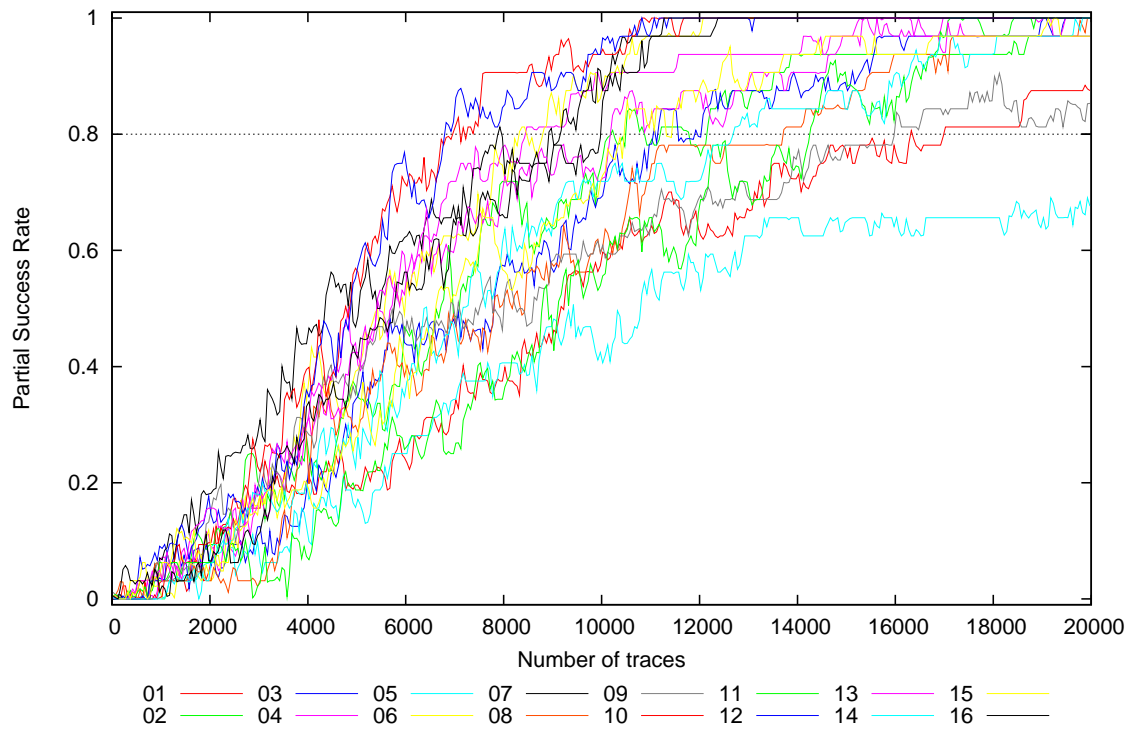
Partial Success Rate for Subkey Bytes #1 to #8



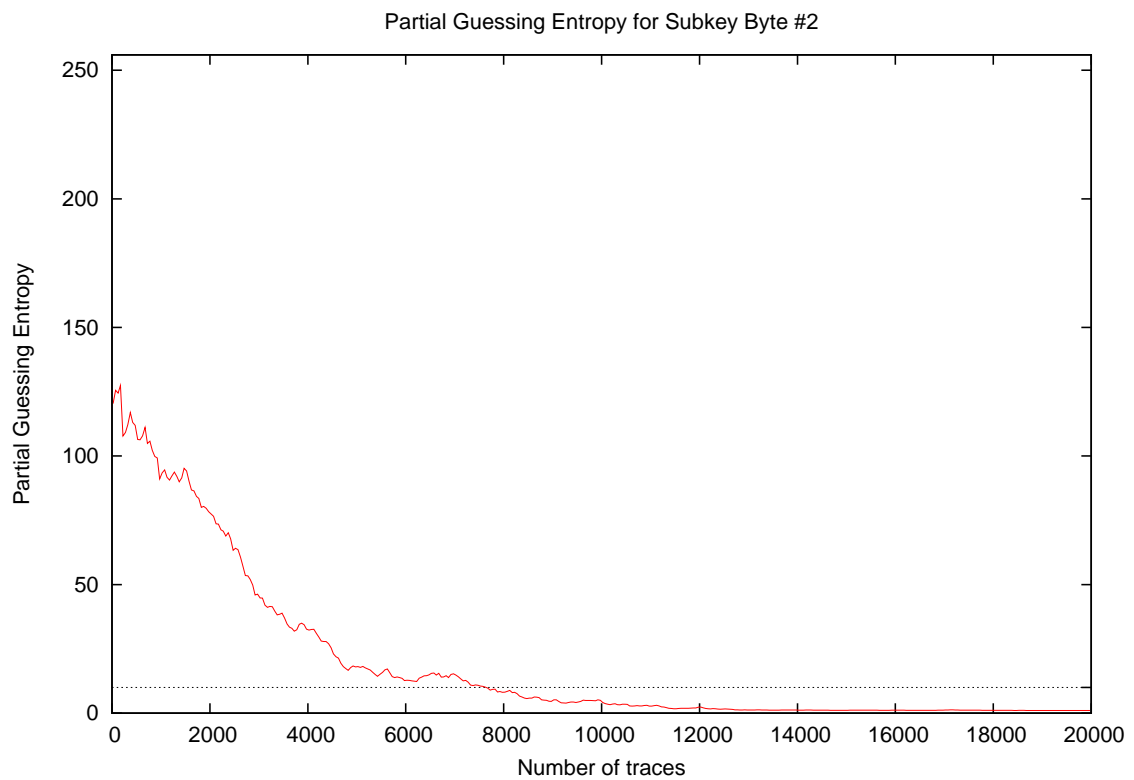
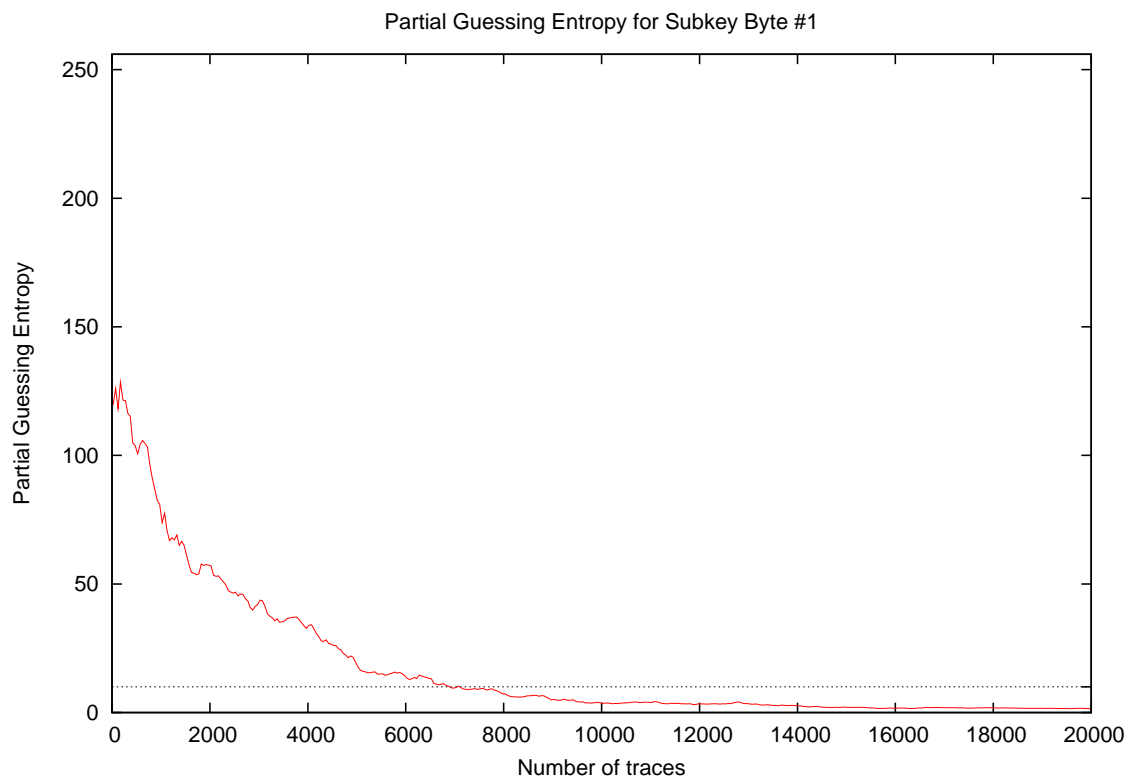
Partial Success Rate for Subkey Bytes #9 to #16



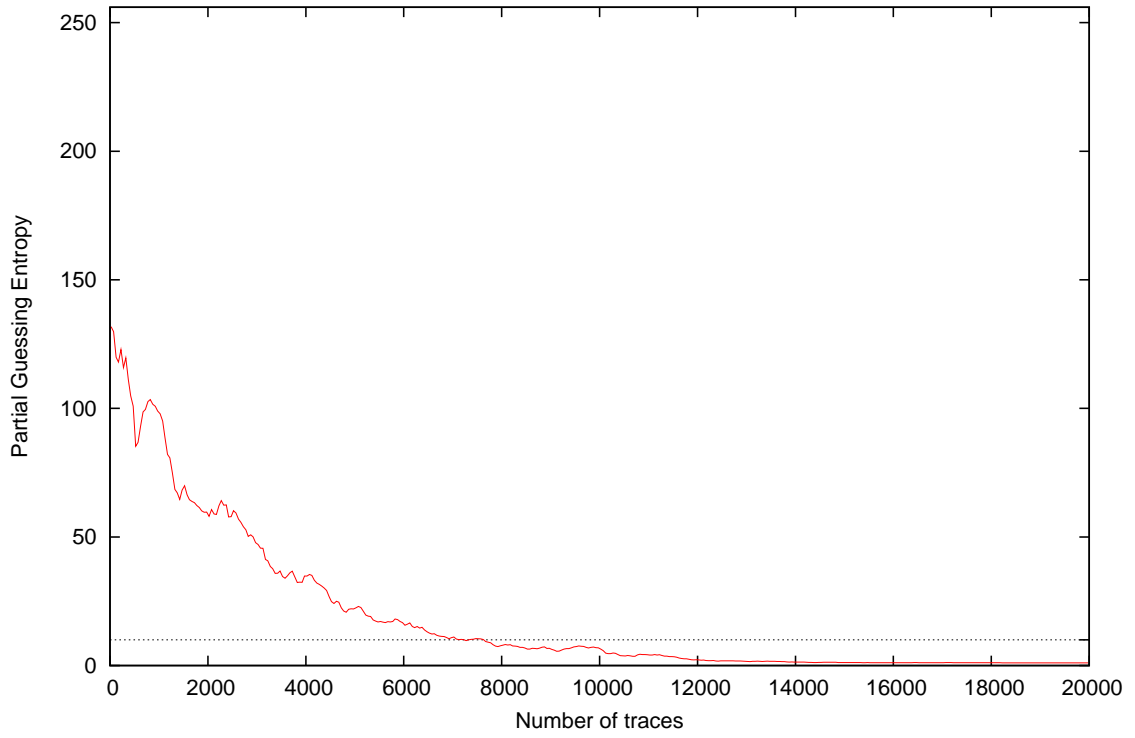
Partial Success Rate for Subkey Bytes #1 to #16



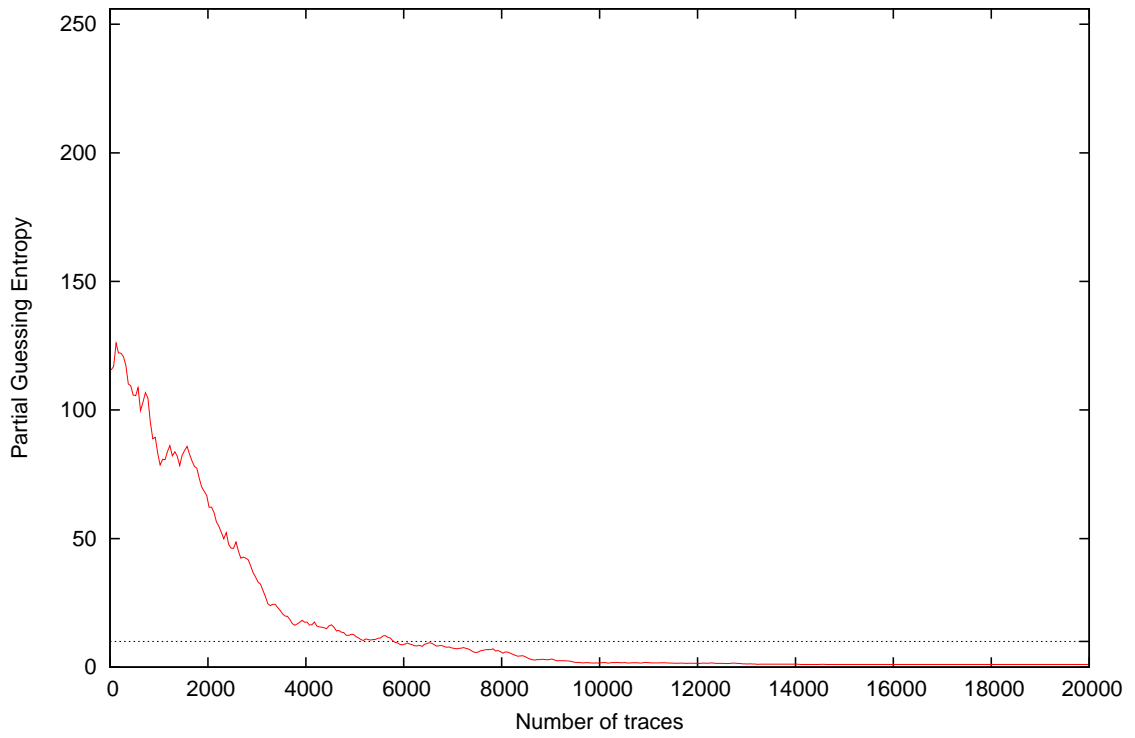
4 Partial Guessing Entropy



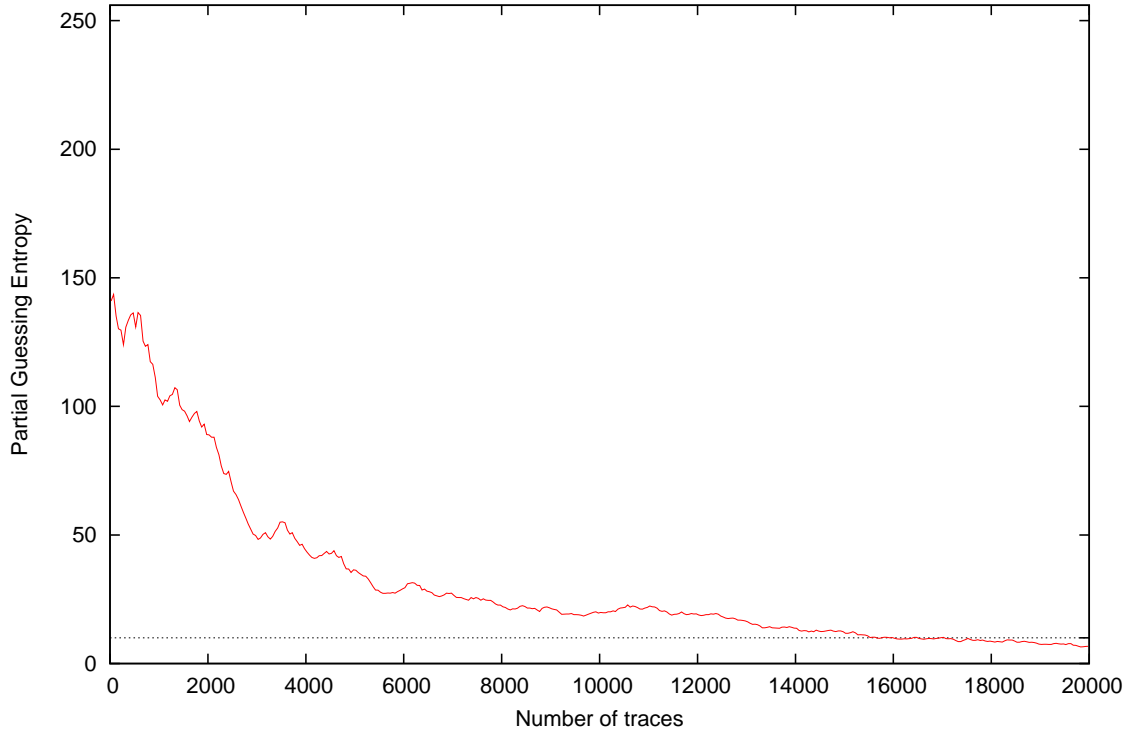
Partial Guessing Entropy for Subkey Byte #3



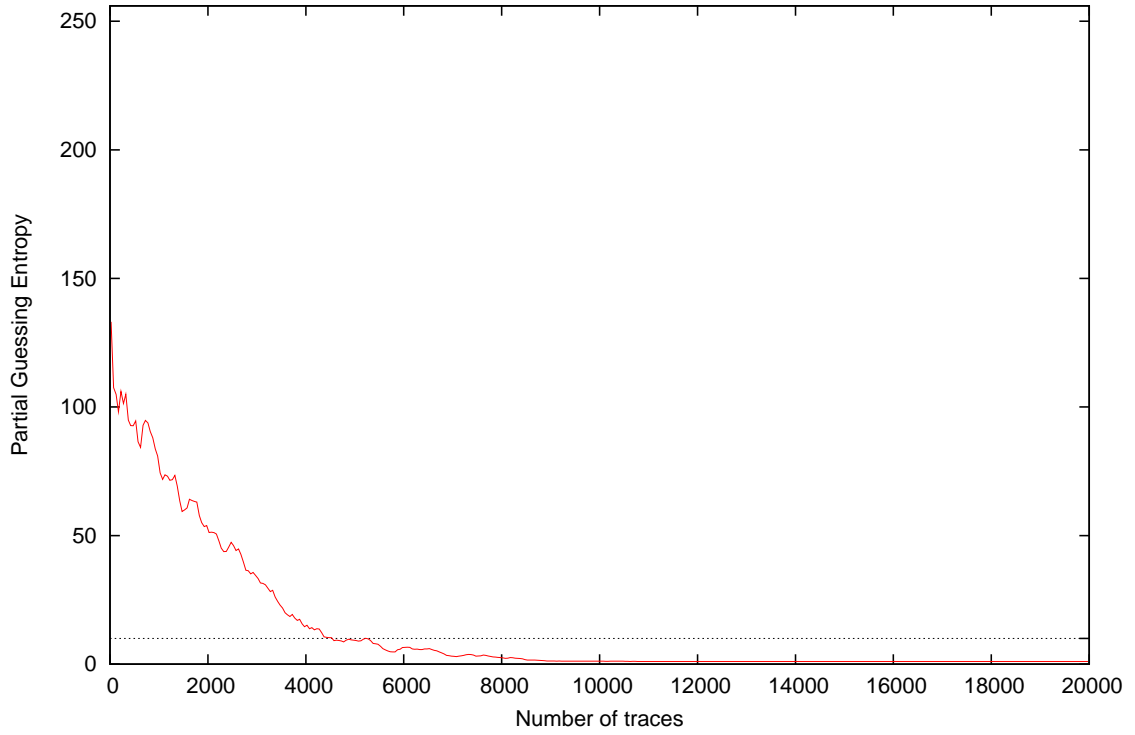
Partial Guessing Entropy for Subkey Byte #4



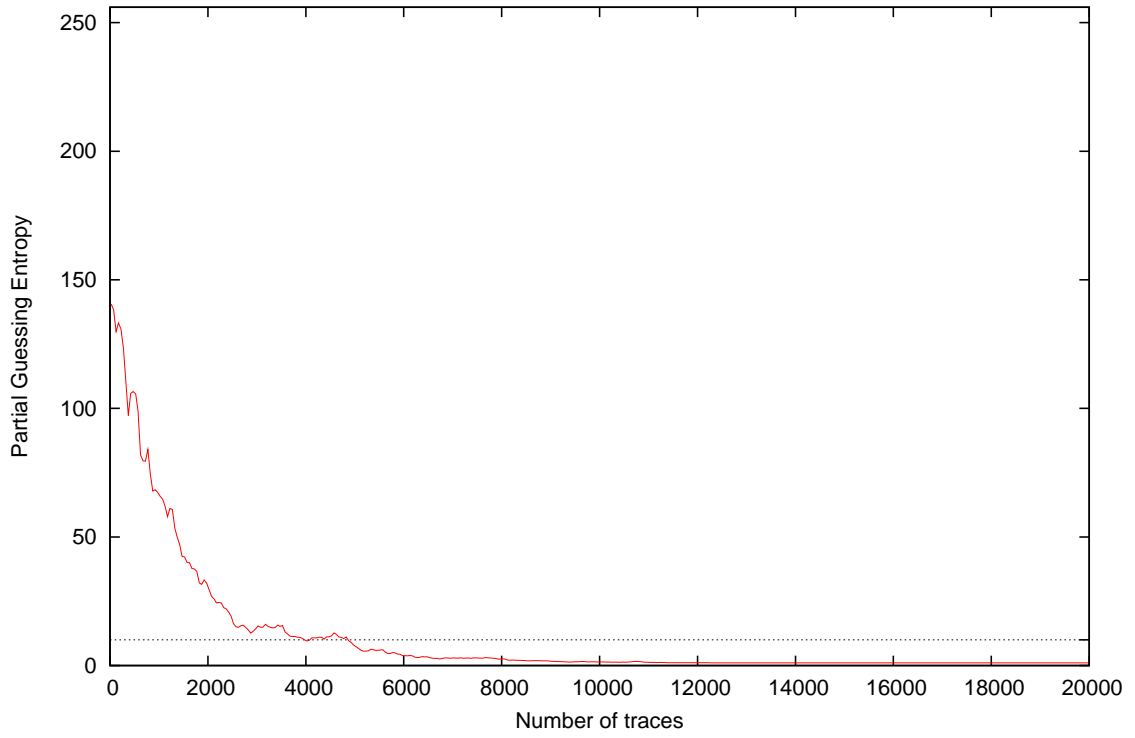
Partial Guessing Entropy for Subkey Byte #5



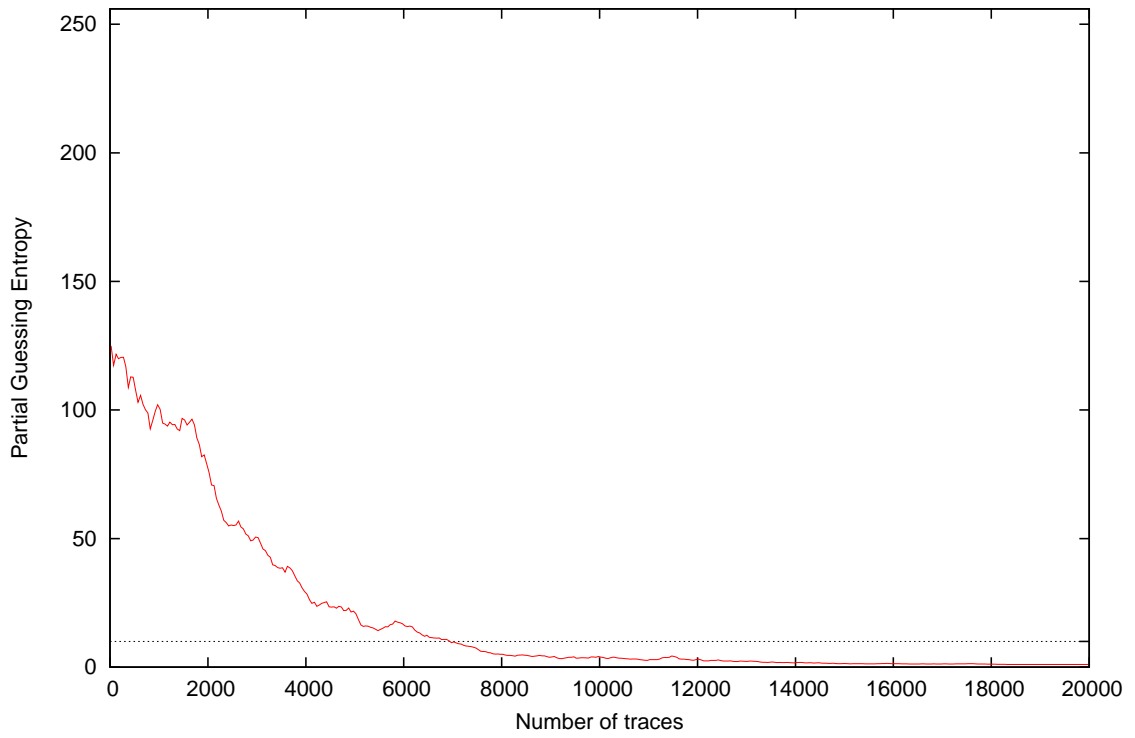
Partial Guessing Entropy for Subkey Byte #6



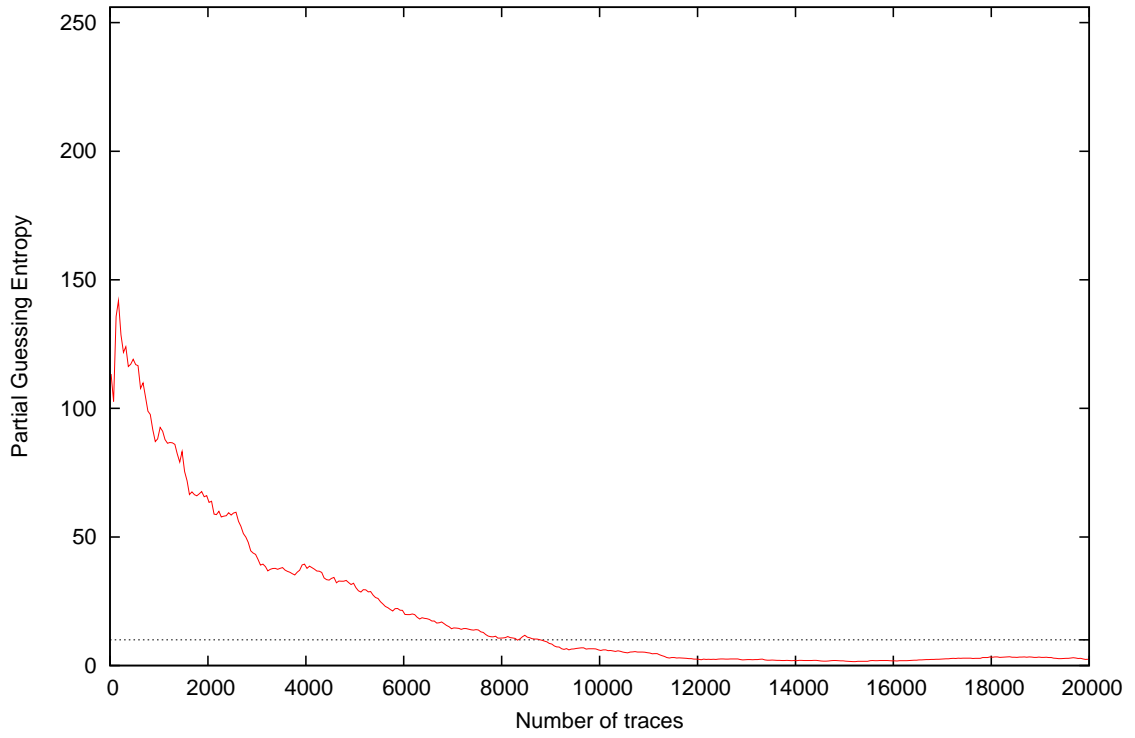
Partial Guessing Entropy for Subkey Byte #7



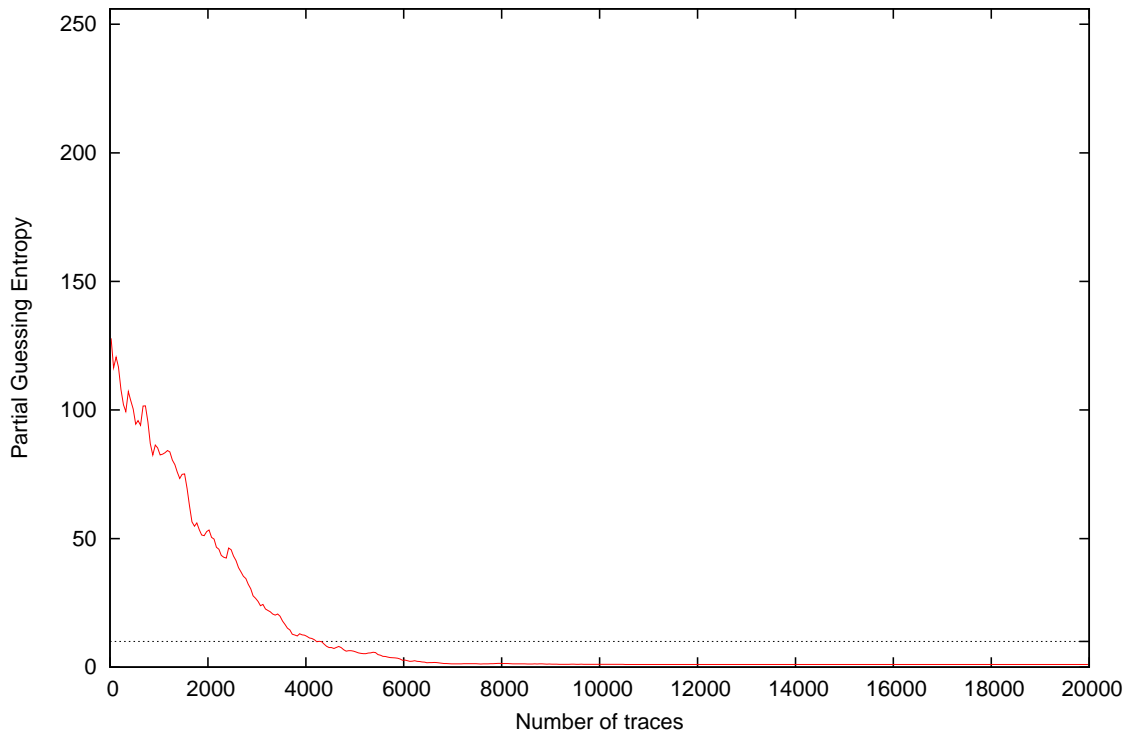
Partial Guessing Entropy for Subkey Byte #8

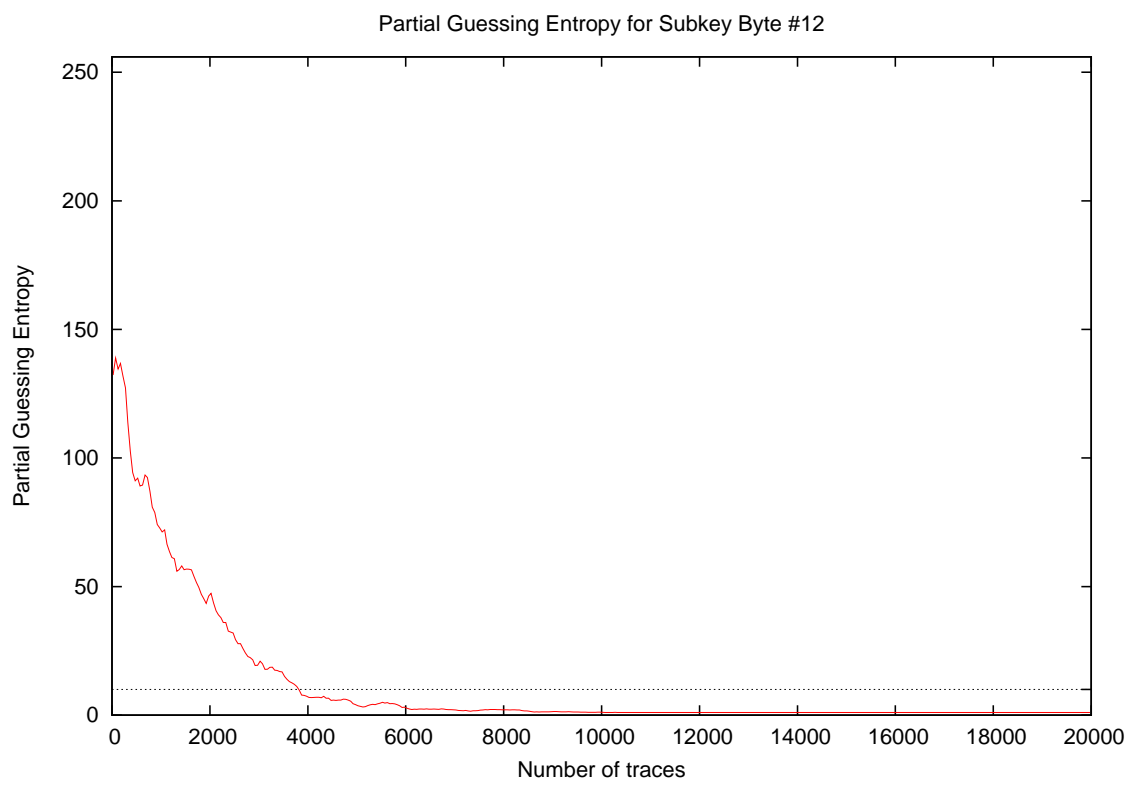
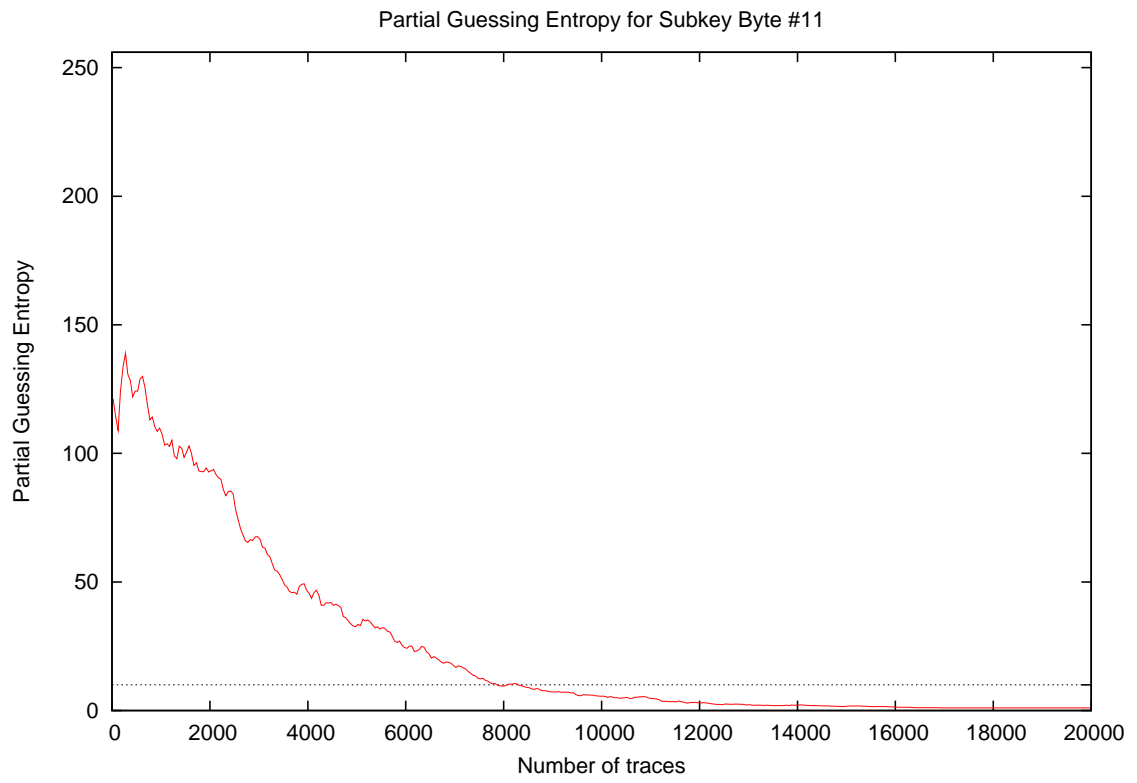


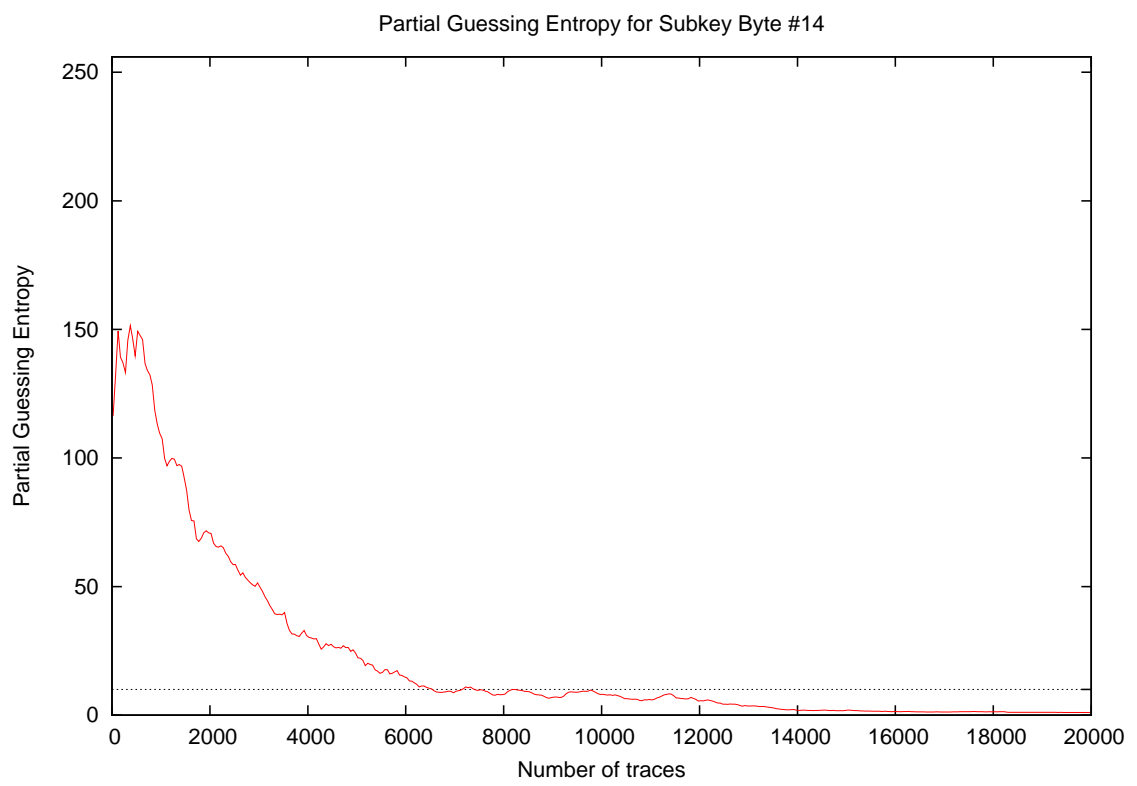
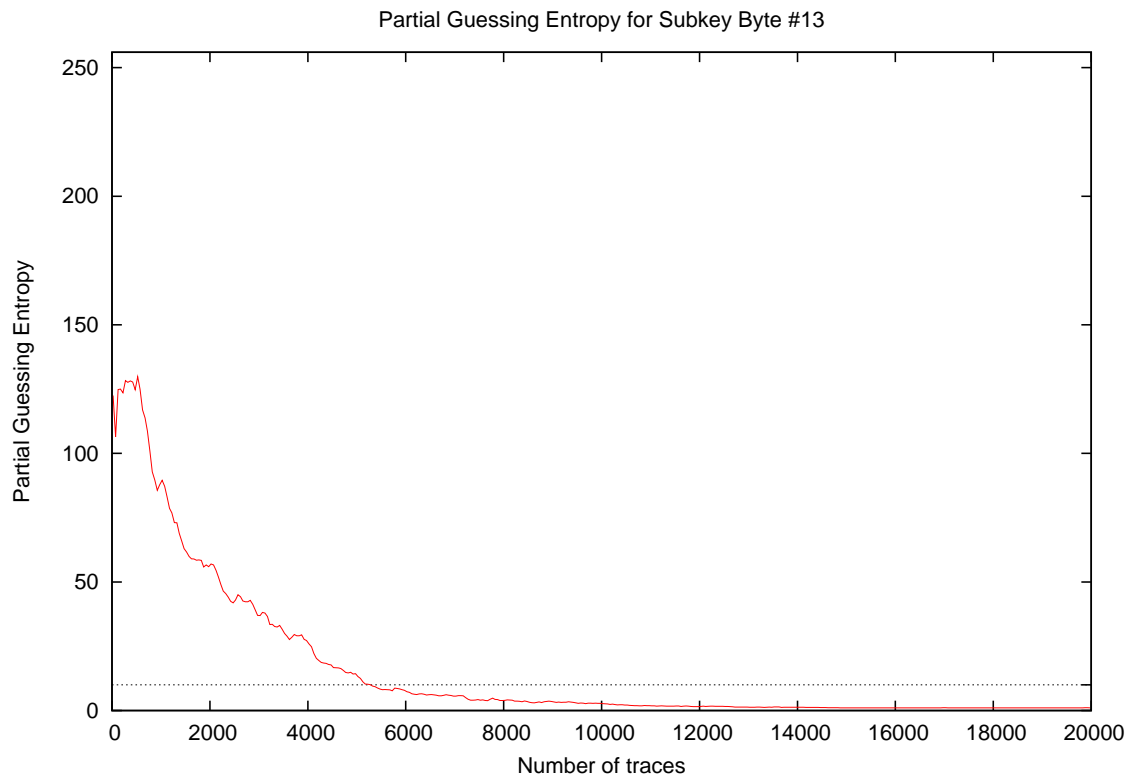
Partial Guessing Entropy for Subkey Byte #9

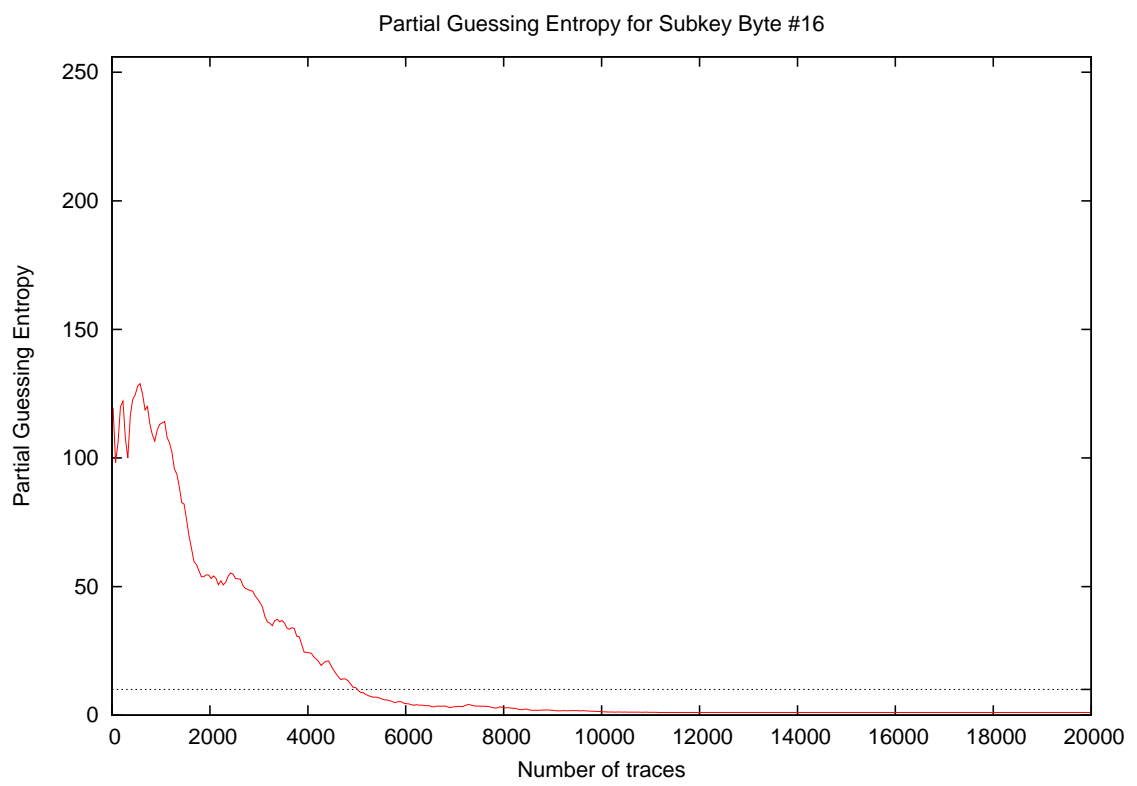
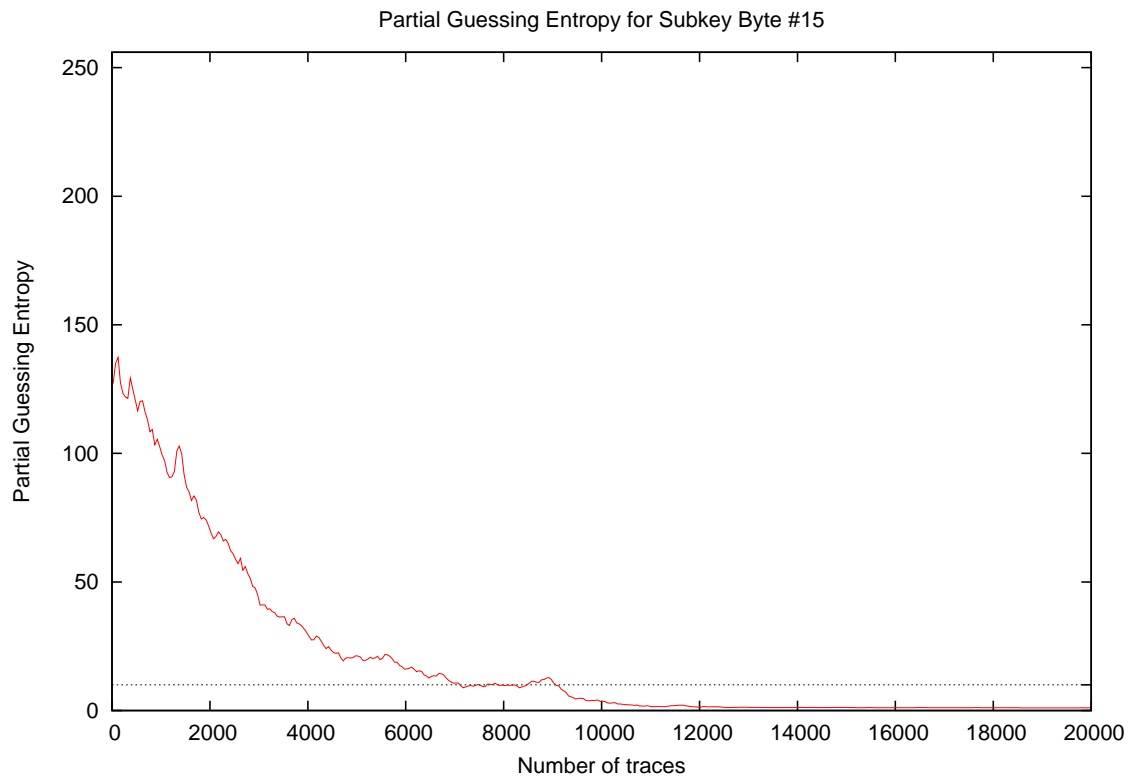


Partial Guessing Entropy for Subkey Byte #10

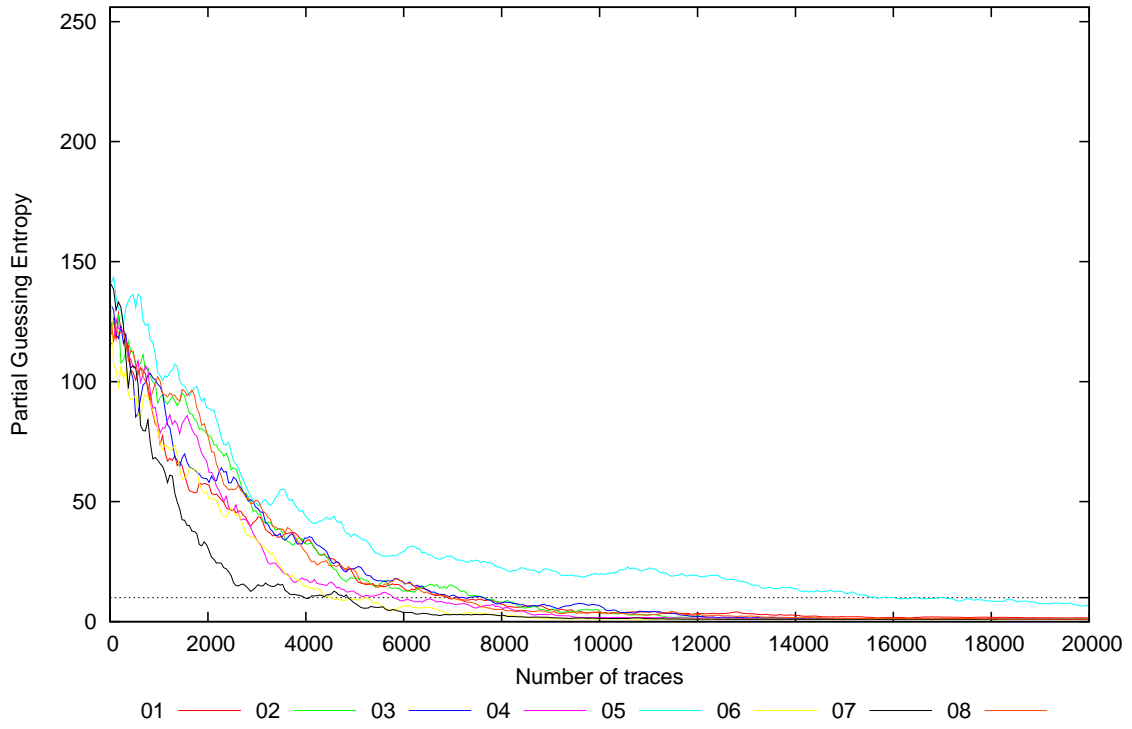




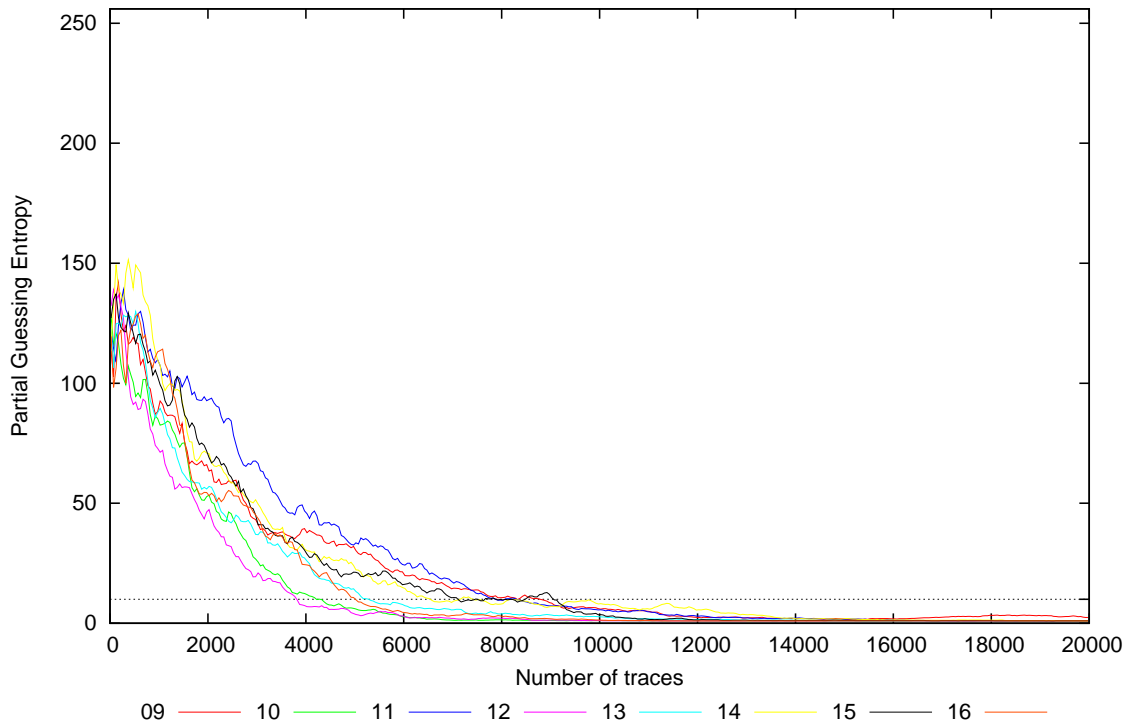


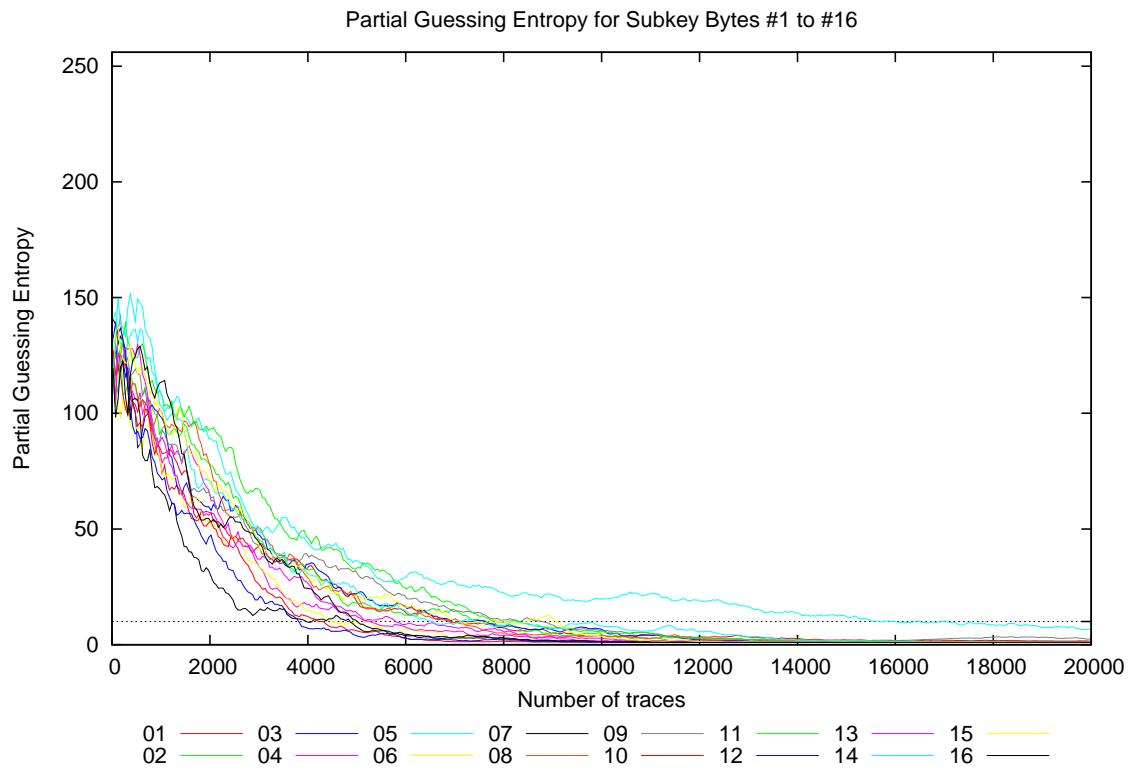


Partial Guessing Entropy for Subkey Bytes #1 to #8



Partial Guessing Entropy for Subkey Bytes #9 to #16





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	127.9	114.9	117.9	104.2	116.7	141.2	150.1	135.6	133.3	123.0	117.9	150.9	134.3	106.5	120.9	124.0	104.2	150.9	126.2
20	111.1	108.8	145.0	124.1	148.2	147.5	141.1	140.0	125.6	118.7	108.0	128.1	124.8	130.6	126.0	129.1	108.0	148.2	128.5
30	119.3	129.1	140.5	109.0	146.0	133.4	131.8	104.0	99.7	132.1	120.4	129.7	120.2	107.5	132.1	121.7	99.7	146.0	123.5
40	119.7	122.3	127.3	109.1	152.2	125.5	147.2	110.6	95.8	131.5	135.4	129.3	109.7	119.7	124.2	109.2	95.8	152.2	123.0
50	123.3	115.6	128.9	120.7	157.4	117.6	145.9	114.2	93.2	135.6	129.5	145.9	103.3	102.3	142.8	105.0	93.2	157.4	123.8
100	121.5	123.2	133.0	115.3	137.2	101.0	126.8	117.4	120.5	118.8	106.2	123.8	115.9	151.2	136.6	95.4	95.4	151.2	121.5
200	125.6	121.2	125.6	111.1	130.8	104.9	136.6	120.9	132.6	111.6	131.9	137.1	115.5	135.4	127.2	124.3	104.9	137.1	124.5
300	121.3	112.7	115.3	122.5	126.6	104.3	116.0	118.6	117.4	101.4	131.2	125.0	130.3	139.4	125.3	102.5	101.4	139.4	119.4
400	111.3	114.5	109.5	110.7	132.8	92.2	100.8	111.1	117.1	105.6	128.9	95.0	130.7	147.2	132.7	121.8	92.2	147.2	116.4
500	100.8	108.8	91.2	105.6	135.3	98.9	108.2	109.7	117.5	94.2	124.0	94.3	129.4	146.5	112.6	126.8	91.2	146.5	112.7
1000	76.9	94.7	99.6	77.8	104.5	74.4	65.7	99.8	91.3	85.0	112.9	70.2	89.3	107.2	100.5	112.8	65.7	112.9	91.4
2000	57.8	77.0	58.8	62.9	87.8	50.3	30.1	77.5	66.0	53.2	91.6	46.4	57.1	71.7	70.1	55.9	30.1	91.6	63.4
3000	43.4	45.4	48.9	35.0	48.4	32.4	15.5	50.7	43.7	26.0	65.3	19.4	36.5	50.8	42.2	44.4	15.5	65.3	40.5
4000	33.0	32.8	34.8	17.5	44.1	15.5	10.2	28.7	38.0	11.9	46.2	7.2	26.3	30.5	30.0	24.1	7.2	46.2	26.9
5000	18.7	18.0	22.0	12.4	37.6	9.1	7.5	21.9	31.1	6.2	33.8	3.8	13.9	23.1	21.5	10.7	3.8	37.6	18.2
10000	3.5	4.8	7.1	1.7	19.4	1.2	1.3	4.1	5.7	1.1	5.7	1.1	2.8	8.1	3.6	1.3	1.1	19.4	4.5
15000	2.1	1.1	1.2	1.0	12.2	1.0	1.0	1.4	1.8	1.0	1.6	1.0	1.0	2.0	1.2	1.0	1.0	12.2	2.0
20000	1.4	1.0	1.0	1.0	6.6	1.0	1.0	1.0	2.5	1.0	1.0	1.0	1.0	1.0	1.1	1.0	1.0	6.6	1.5