

# Evaluation results

DPA contest v2

September 2010

## 1 Introduction

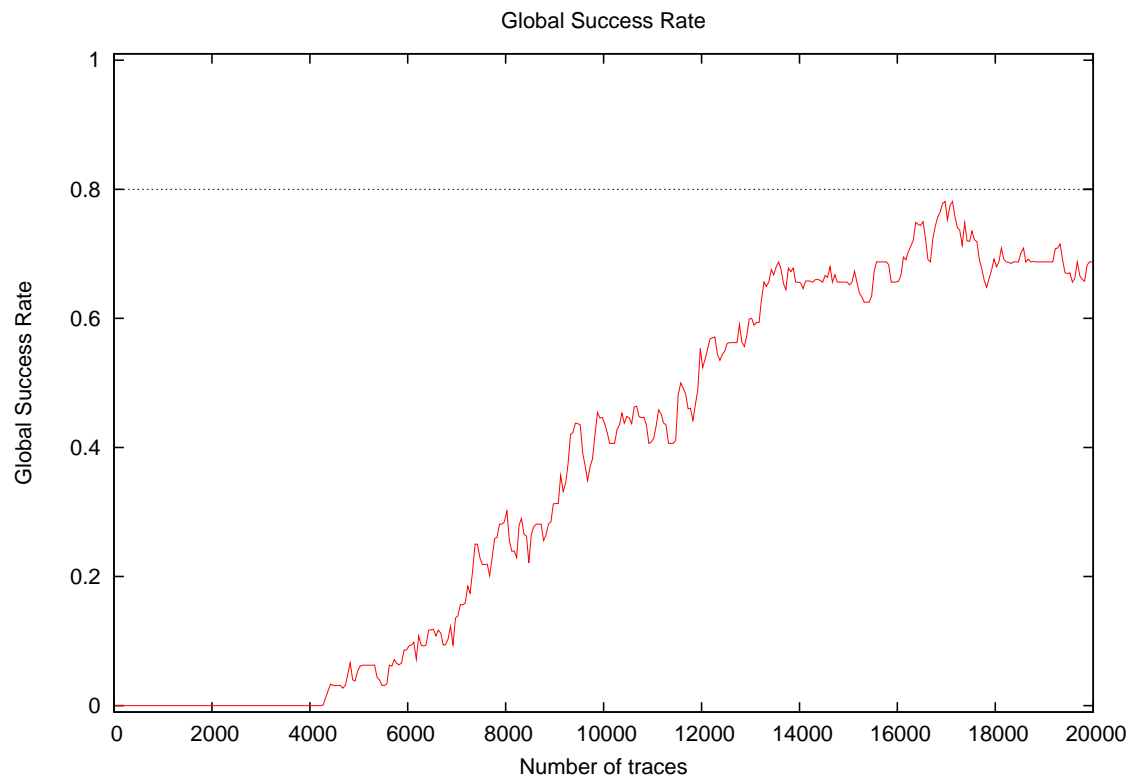
### 1.1 About the attack

- **Attack Name:** B
- **Sender/Team:** Antoine Wurcker
- **Institution:** UNILIM: Faculte des Sciences et Techniques de Limoges
- **Language:** C++
- **Attacked subkey:** 10

### 1.2 About the evaluation

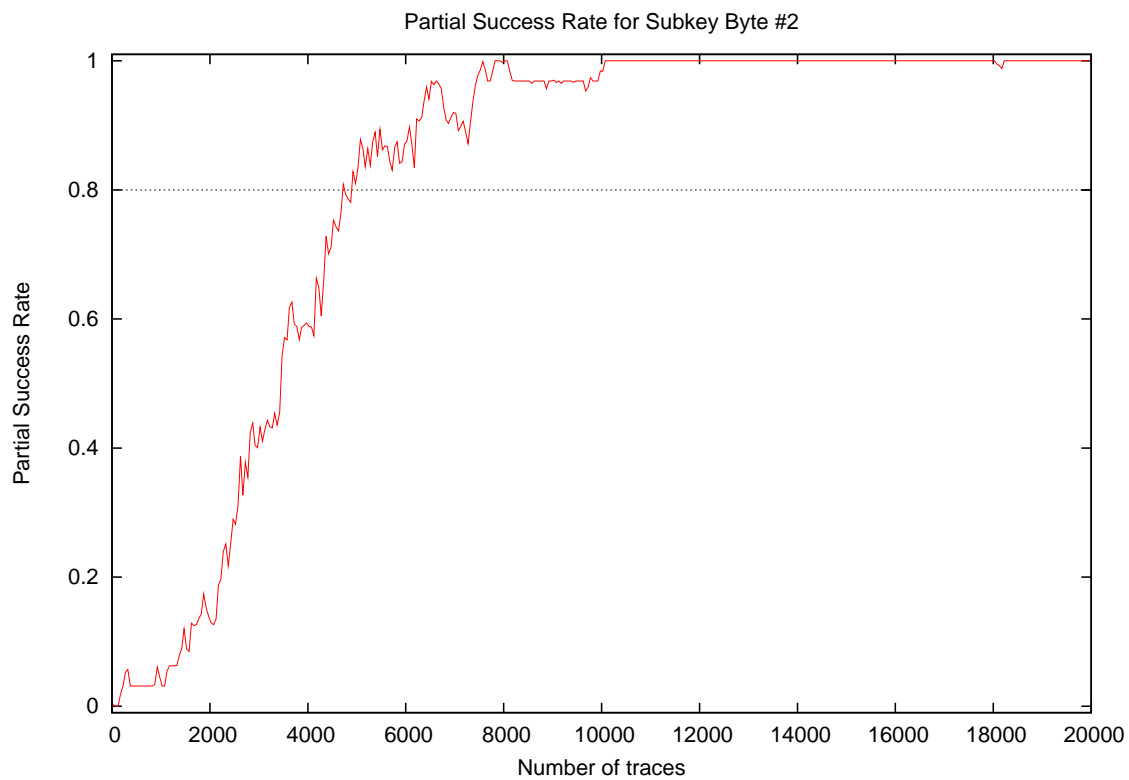
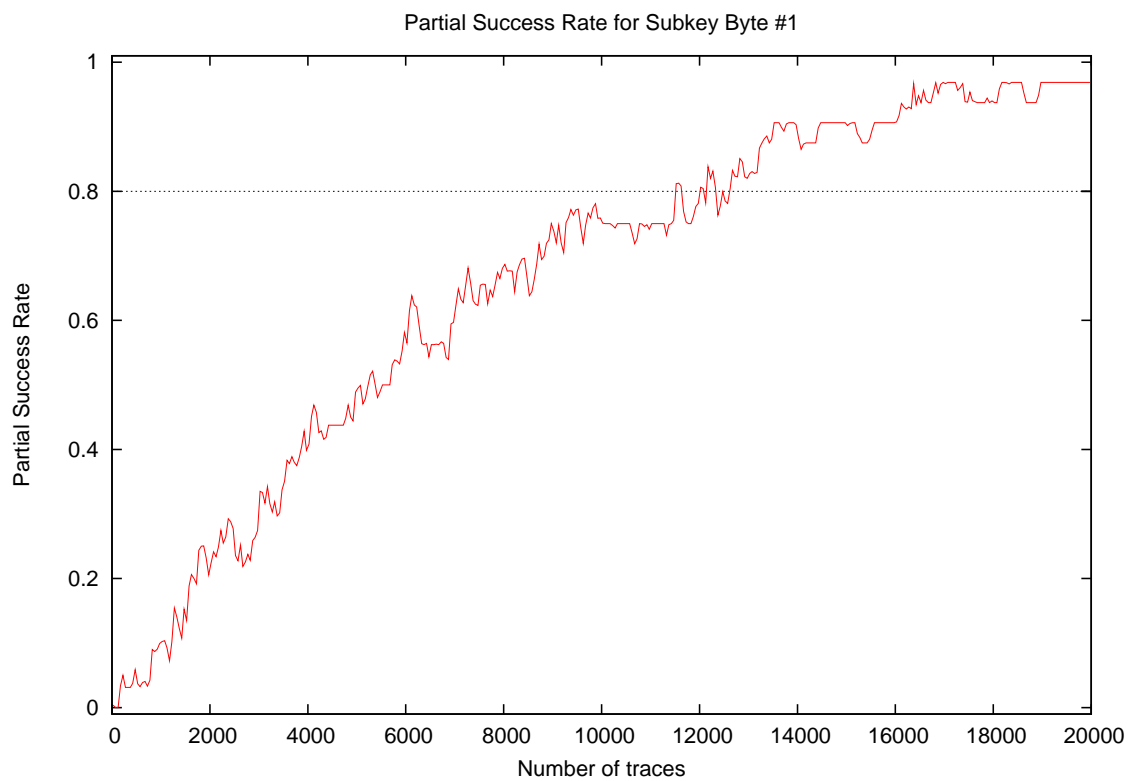
- **Date of evaluation:** August 2010

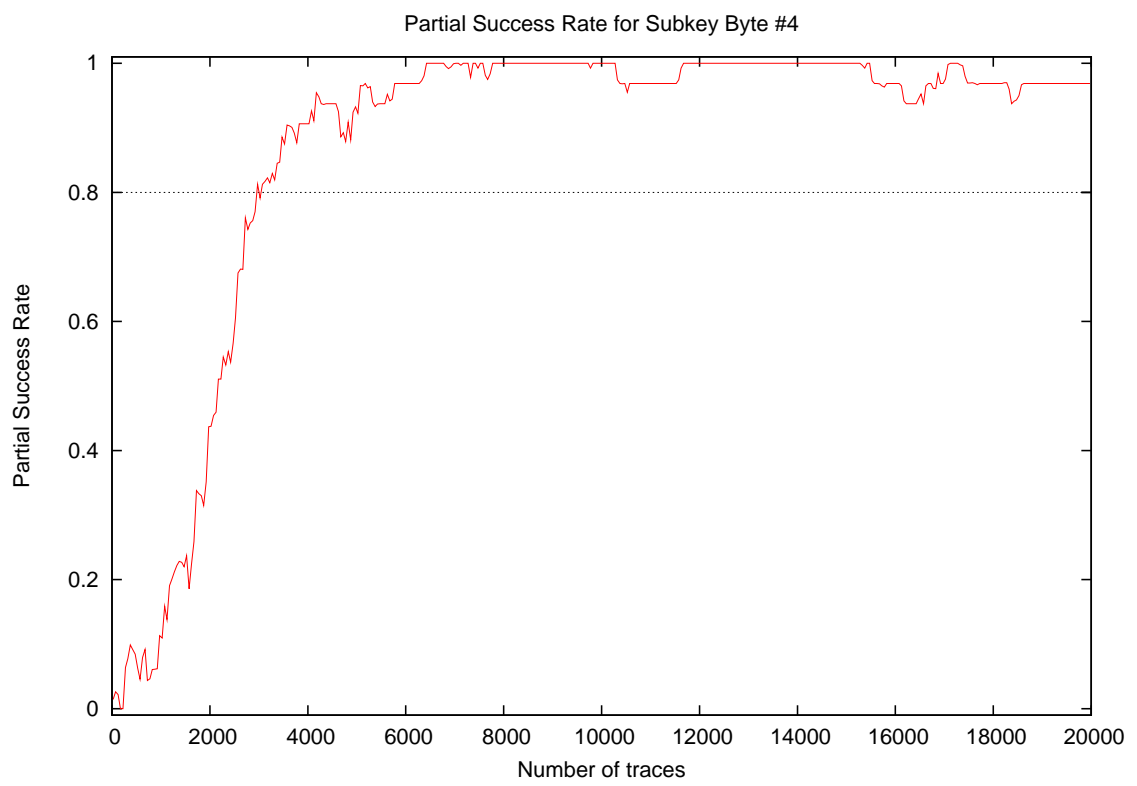
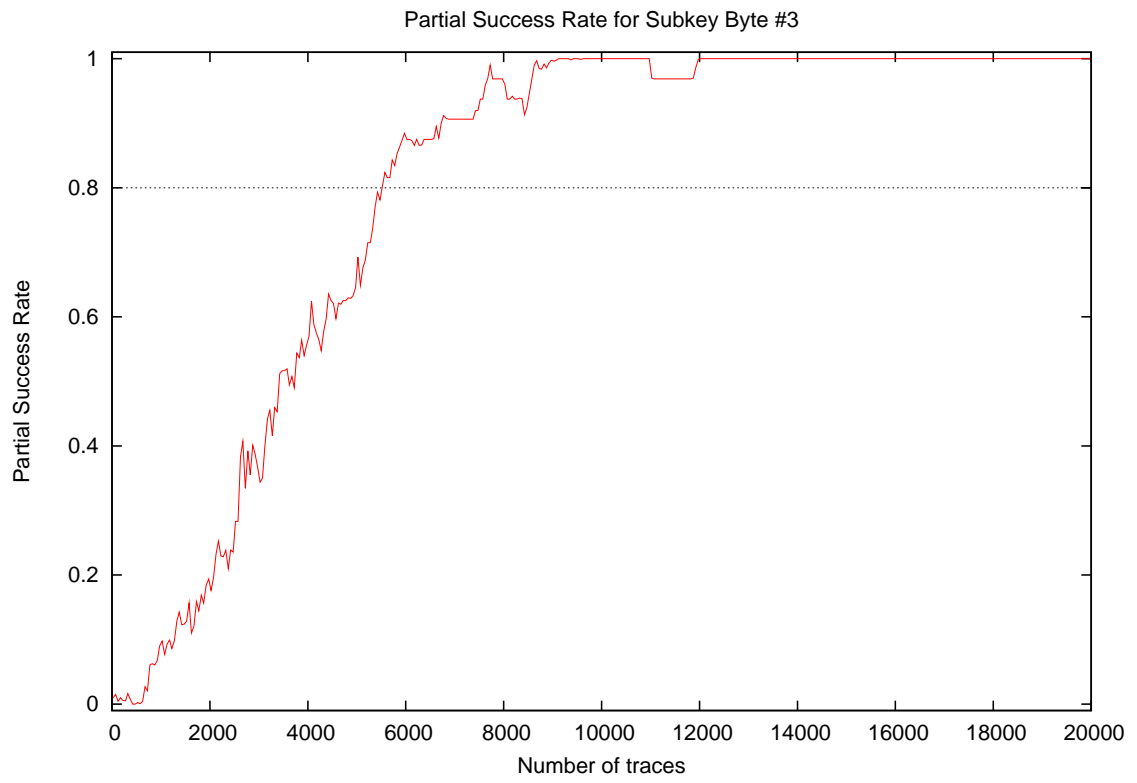
## 2 Global Success Rate

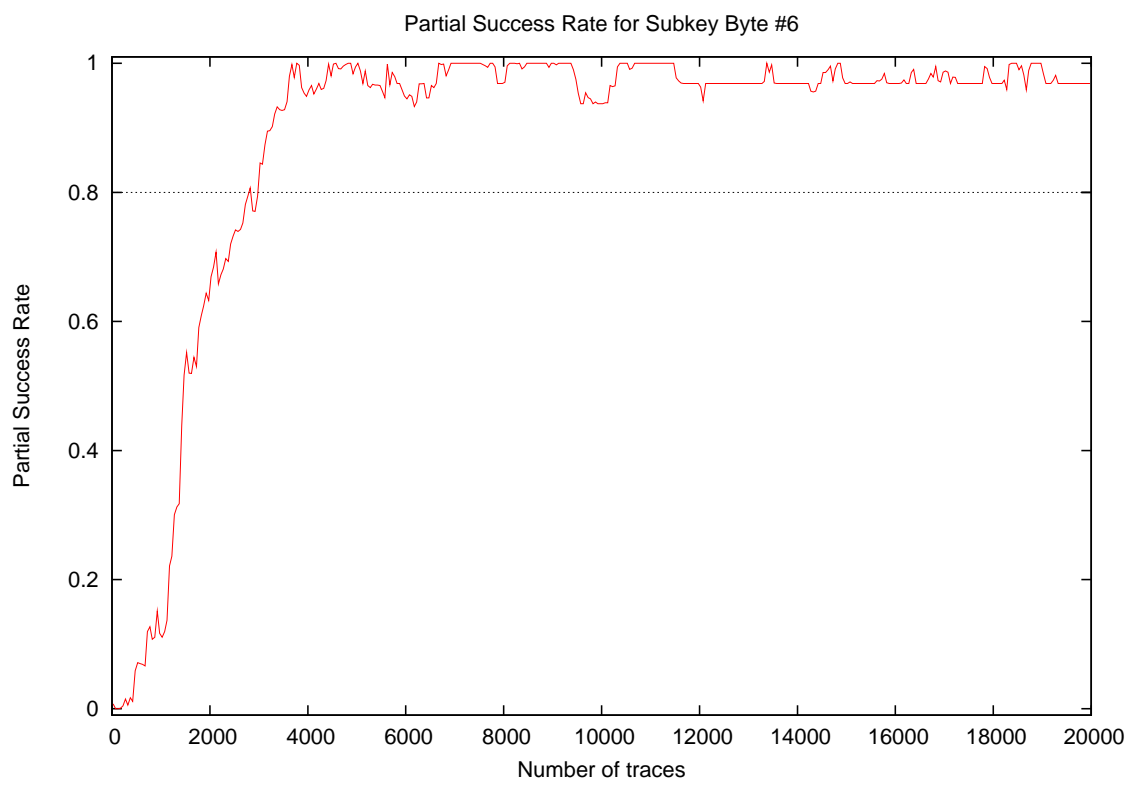
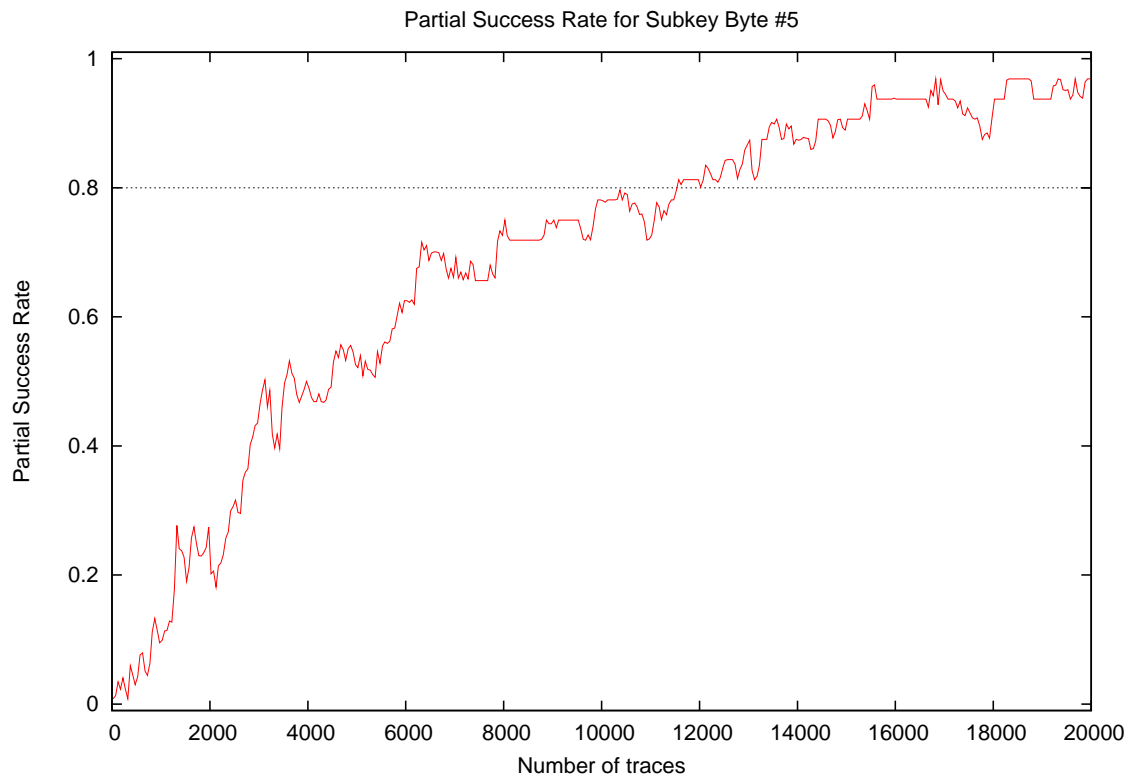


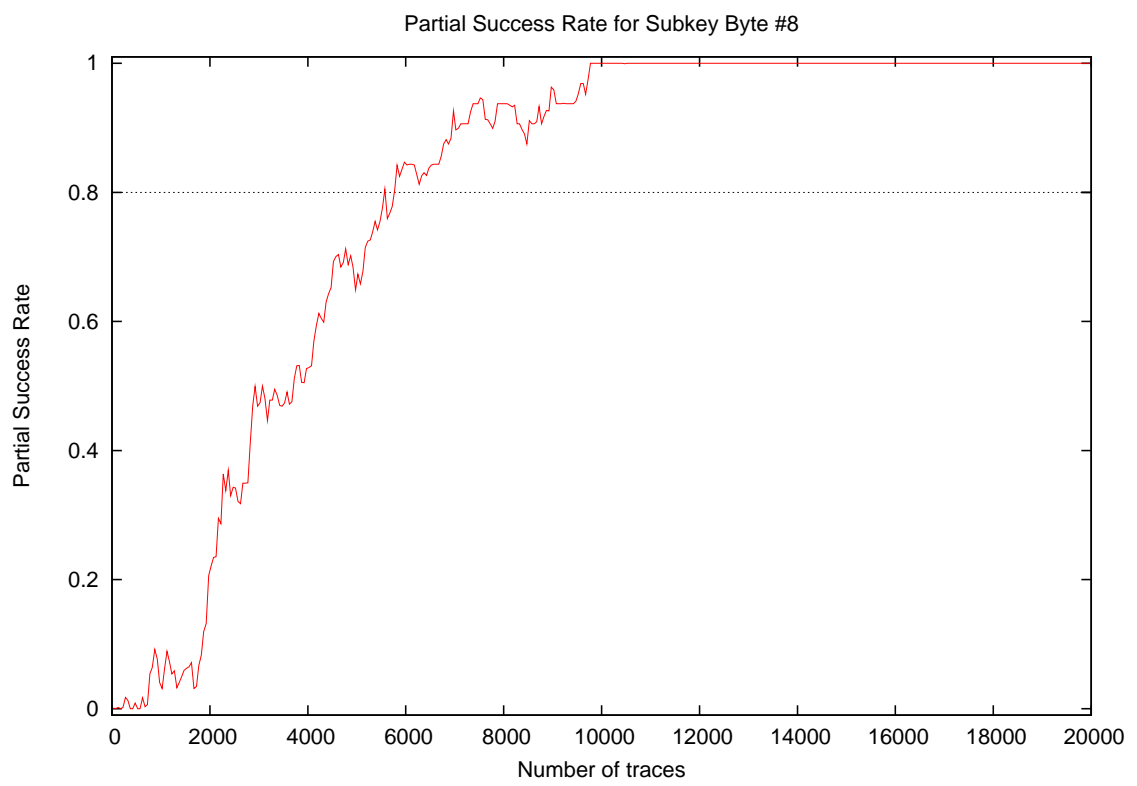
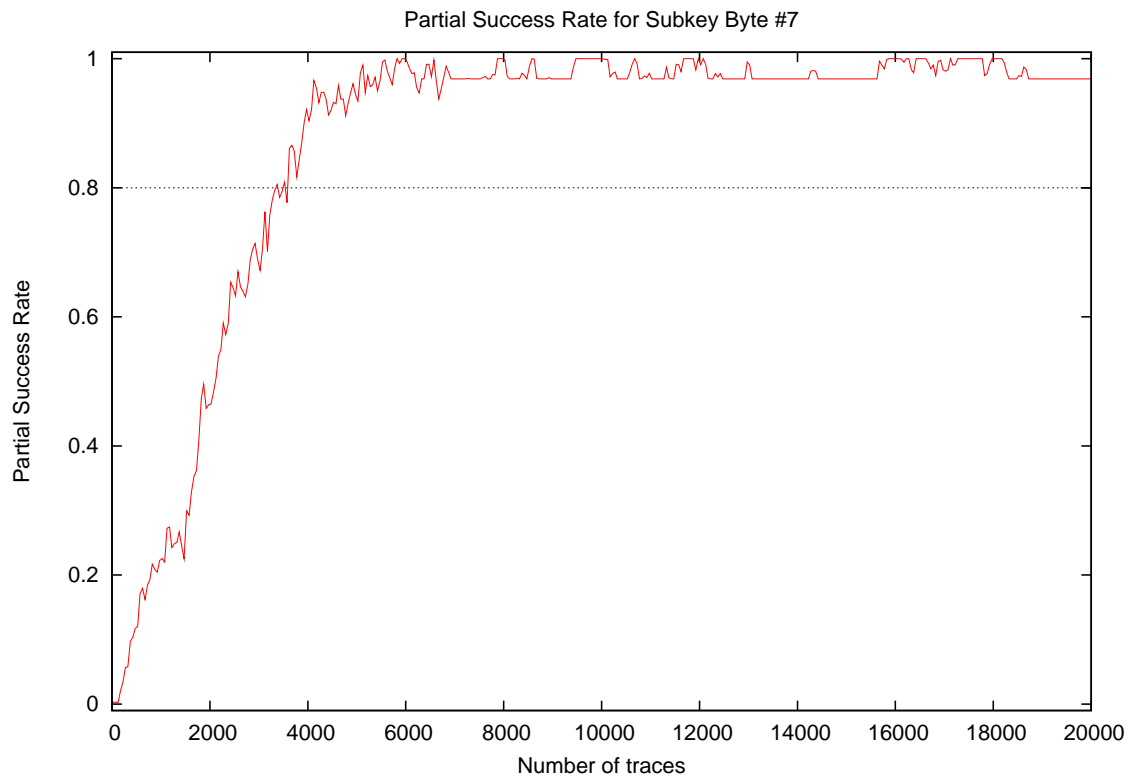
Number of traces	Global Success Rate
10	0.00
20	0.00
30	0.00
40	0.00
50	0.00
100	0.00
200	0.00
300	0.00
400	0.00
500	0.00
1000	0.00
2000	0.00
3000	0.00
4000	0.00
5000	0.03
10000	0.47
15000	0.66
20000	0.69

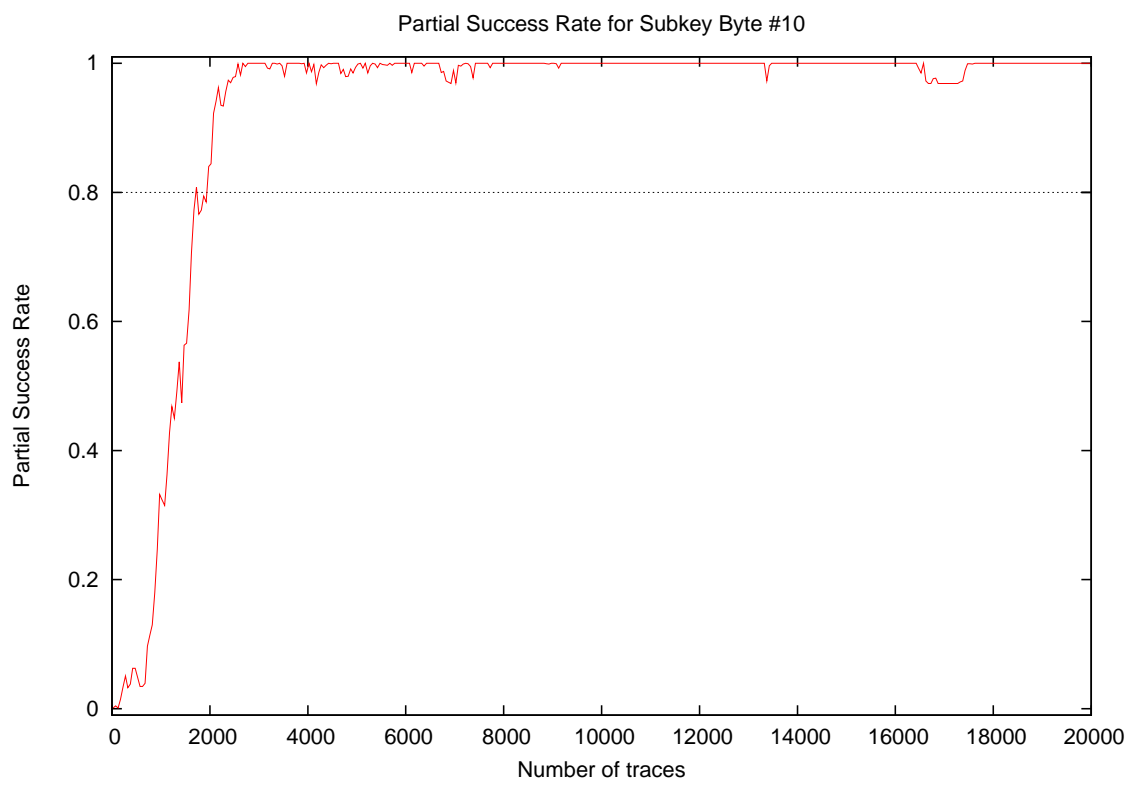
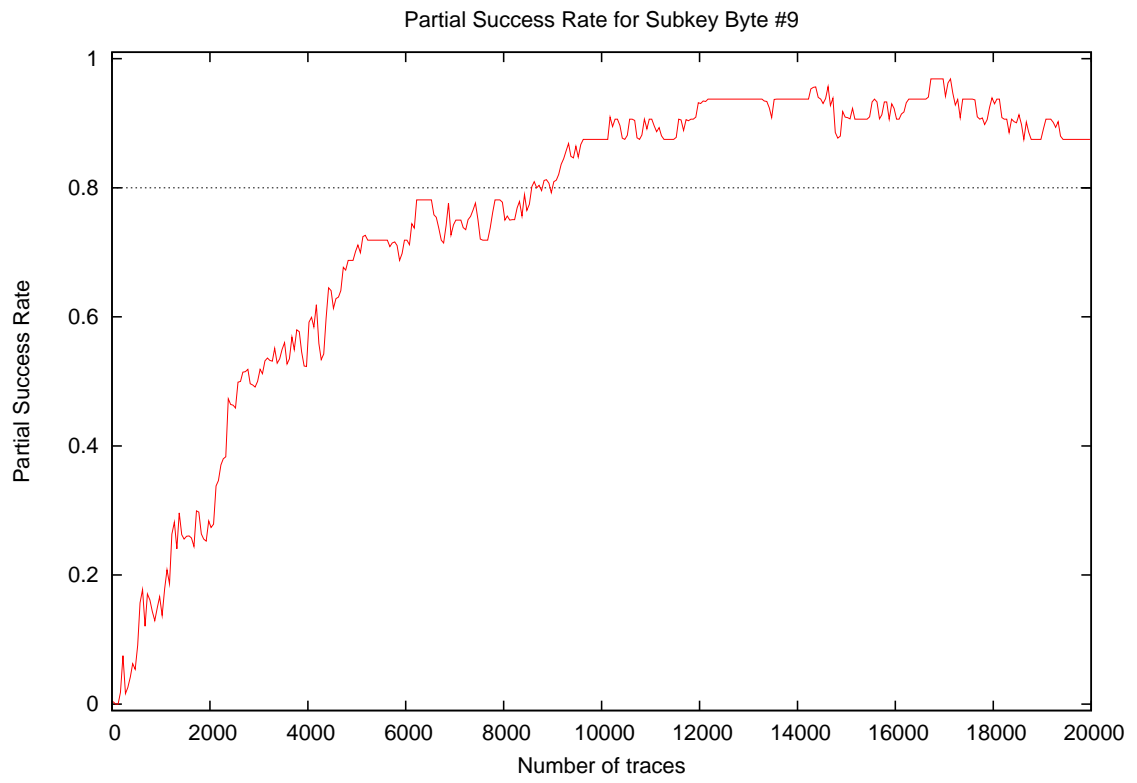
### 3 Partial Success Rate



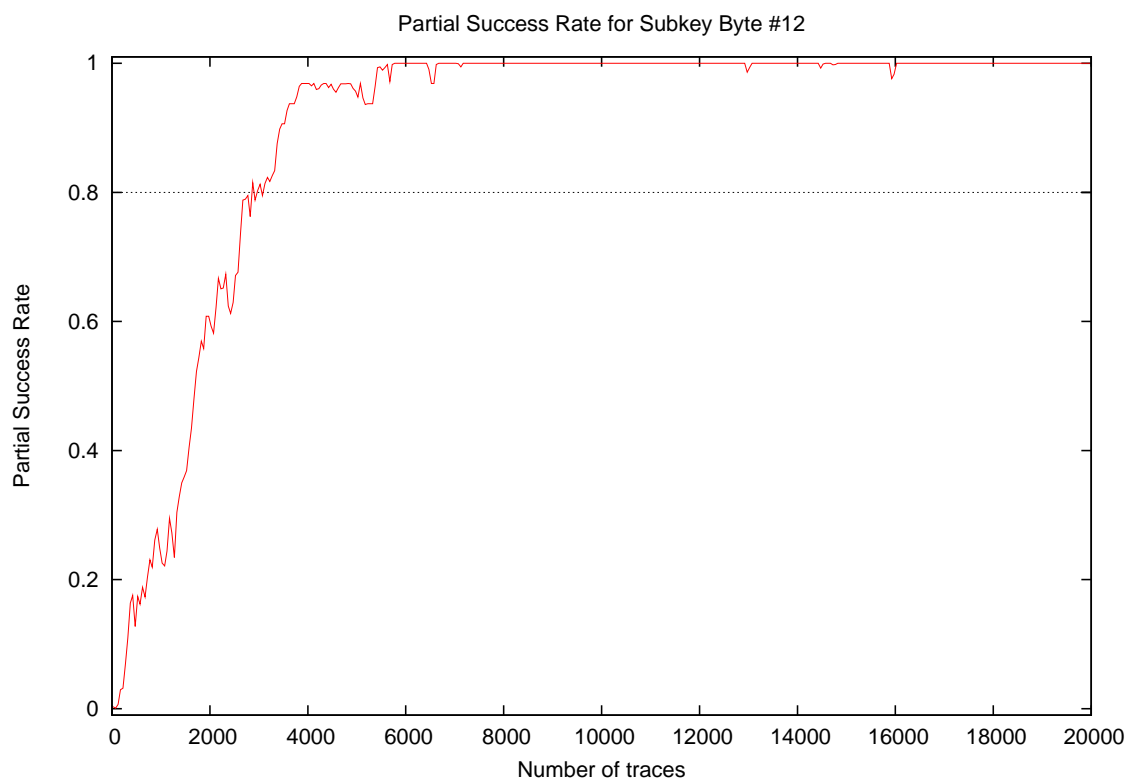
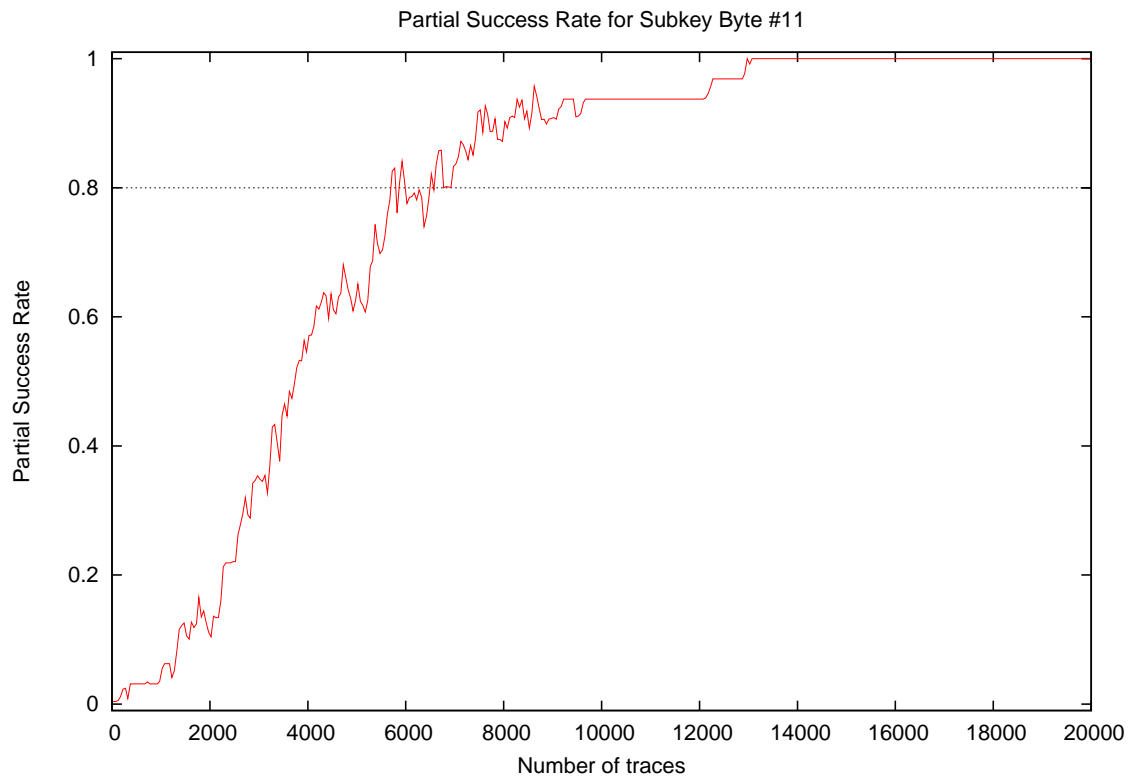


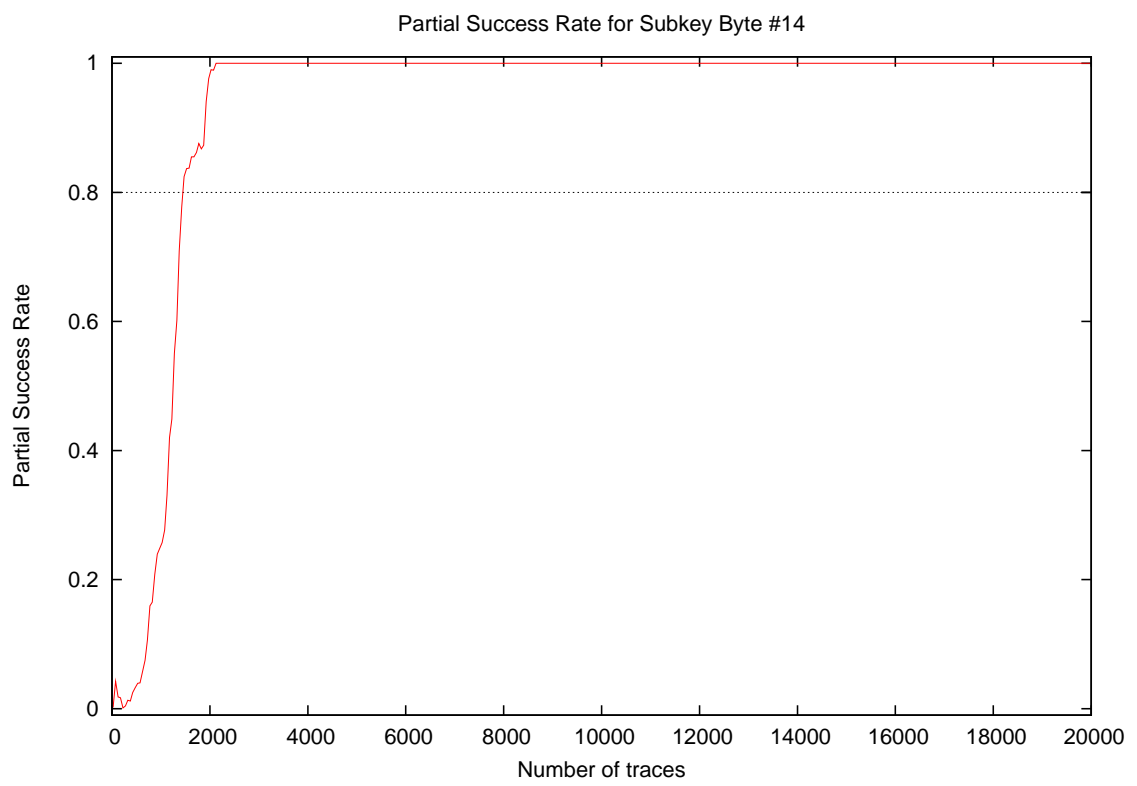
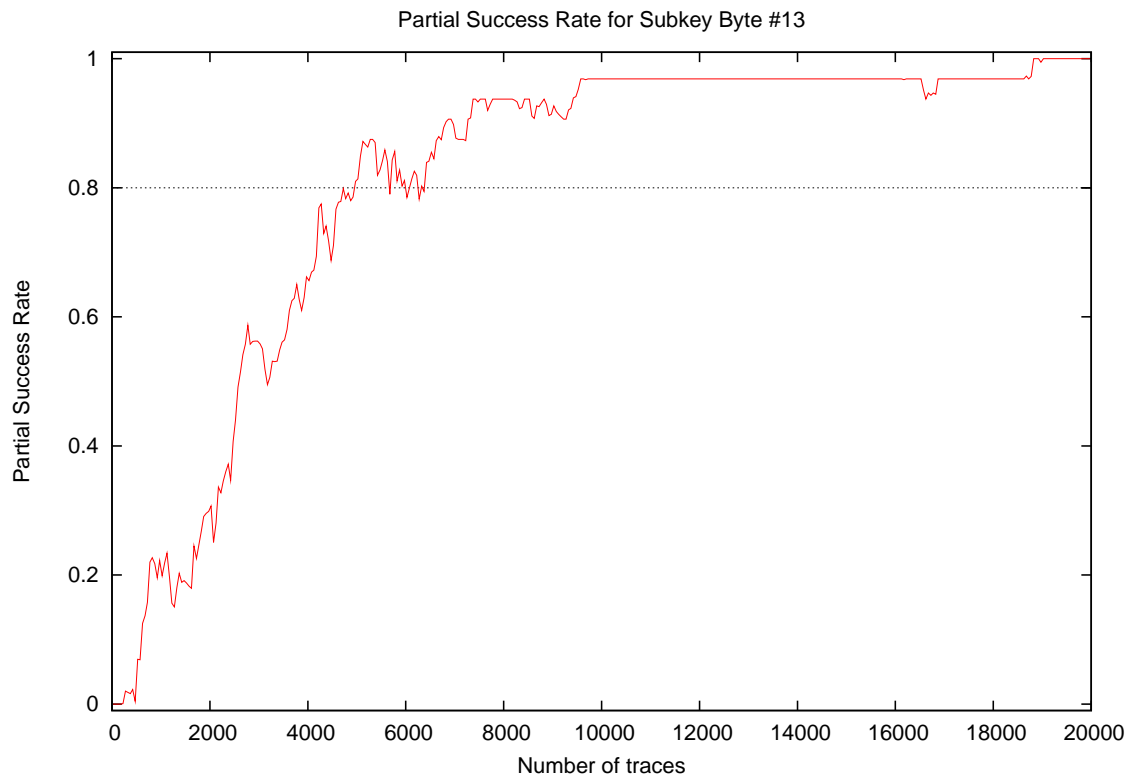


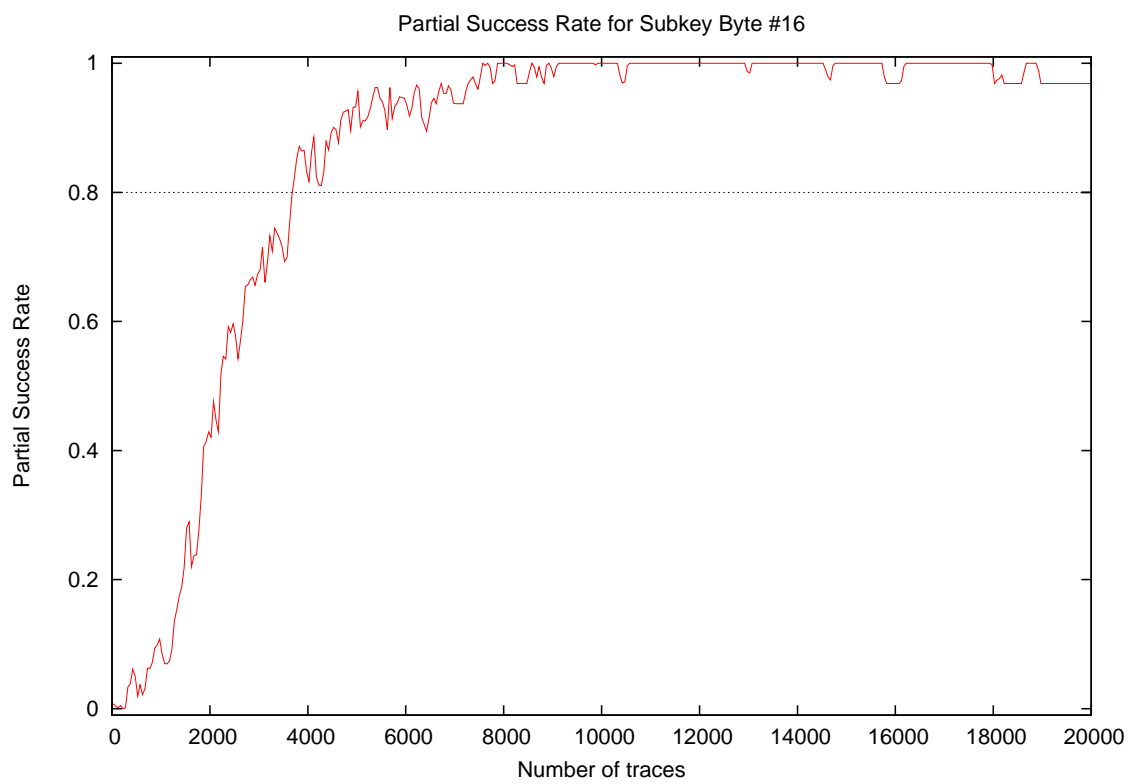
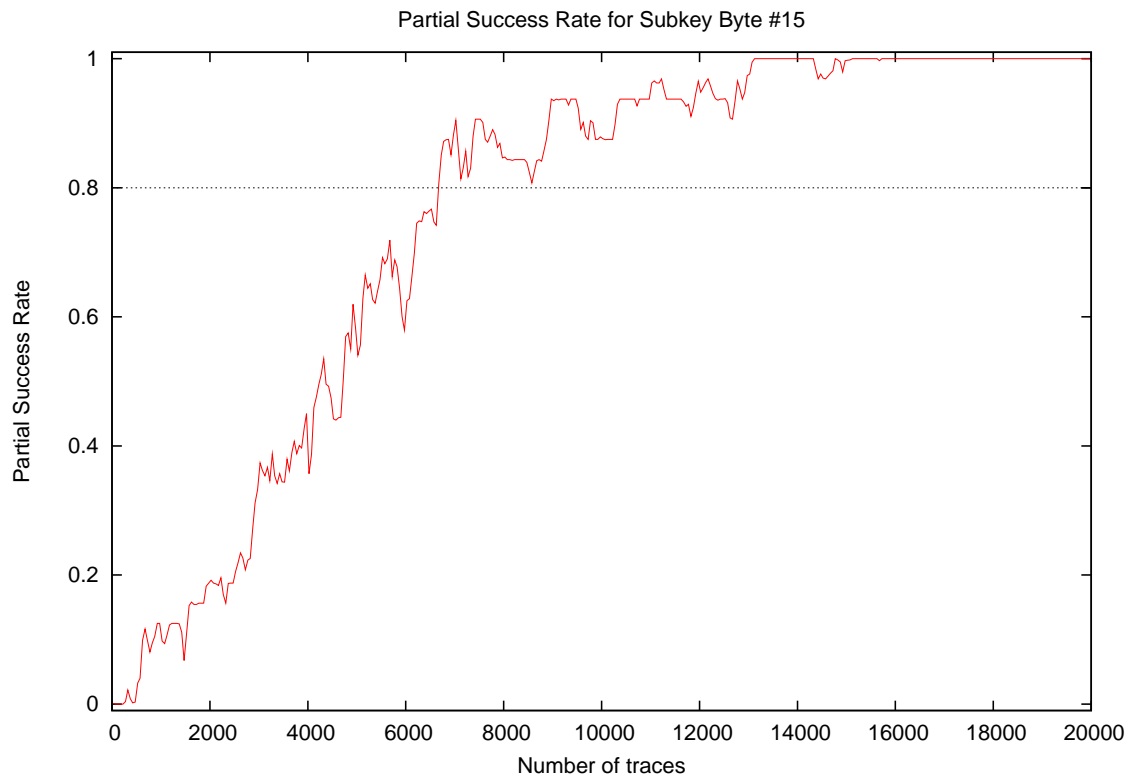


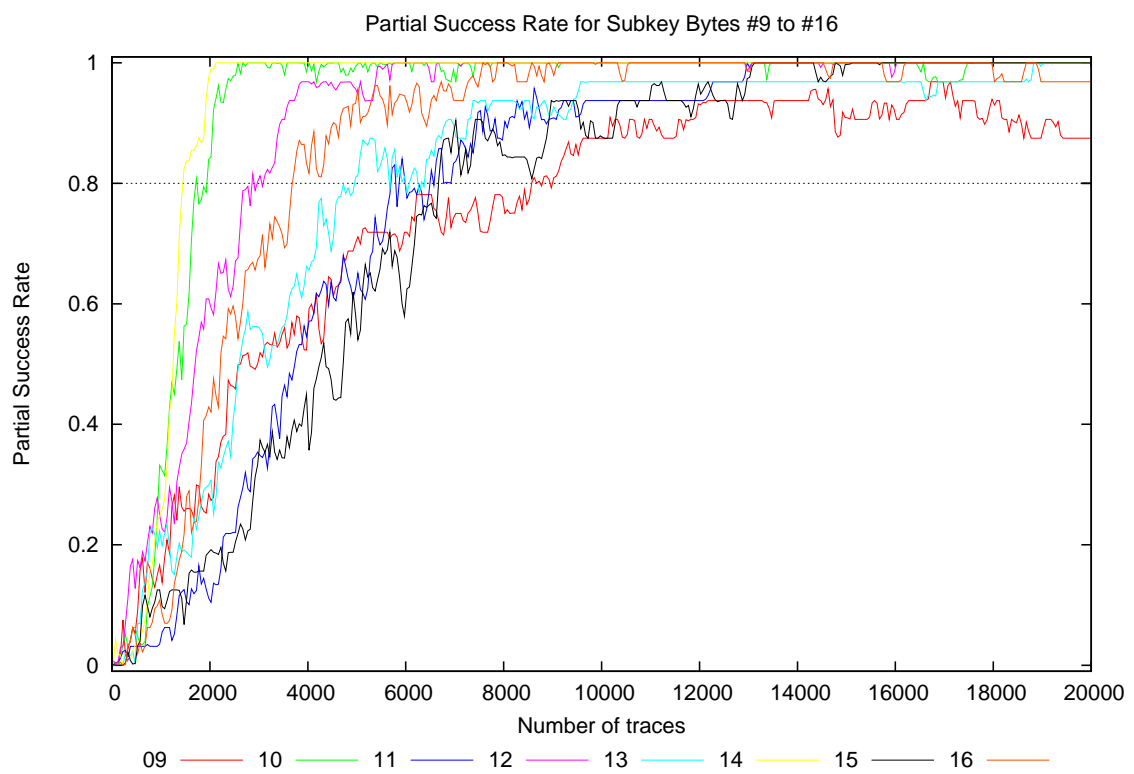
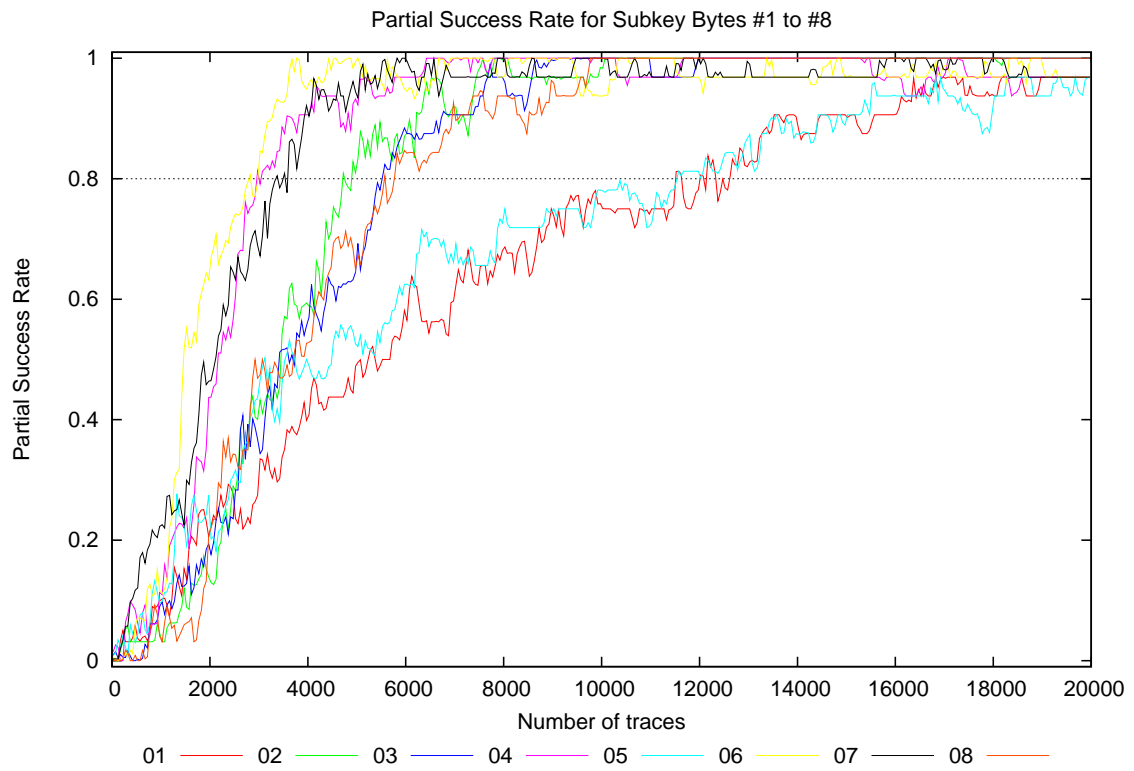




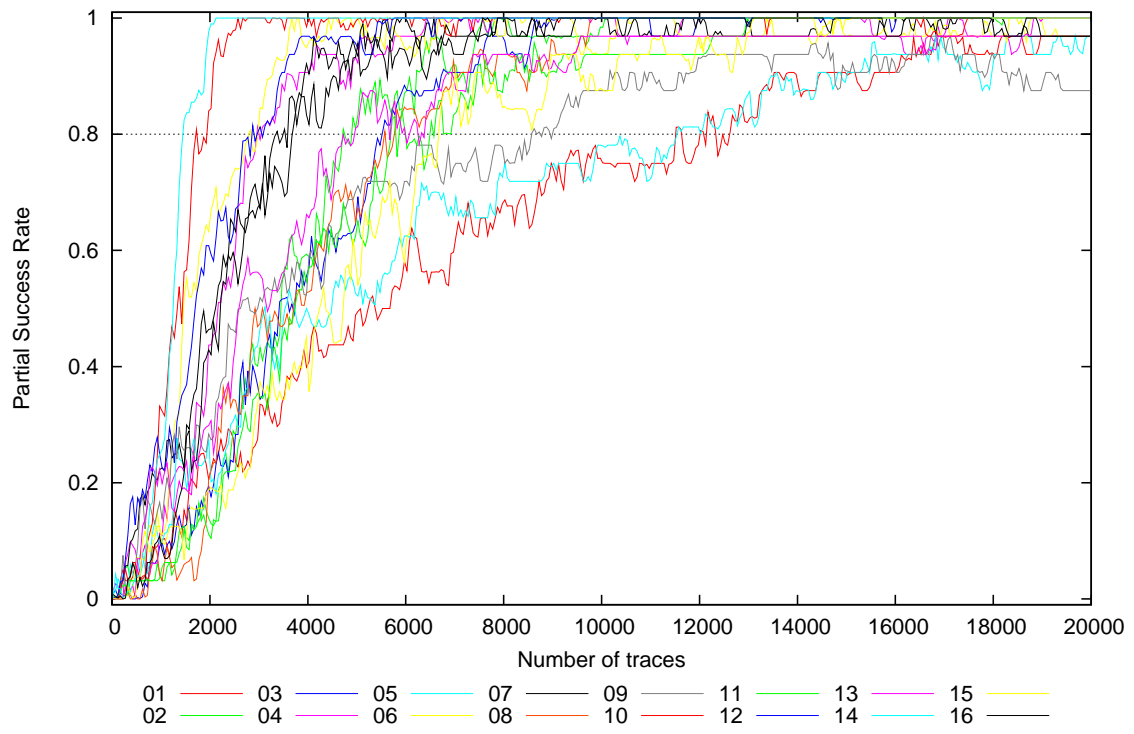






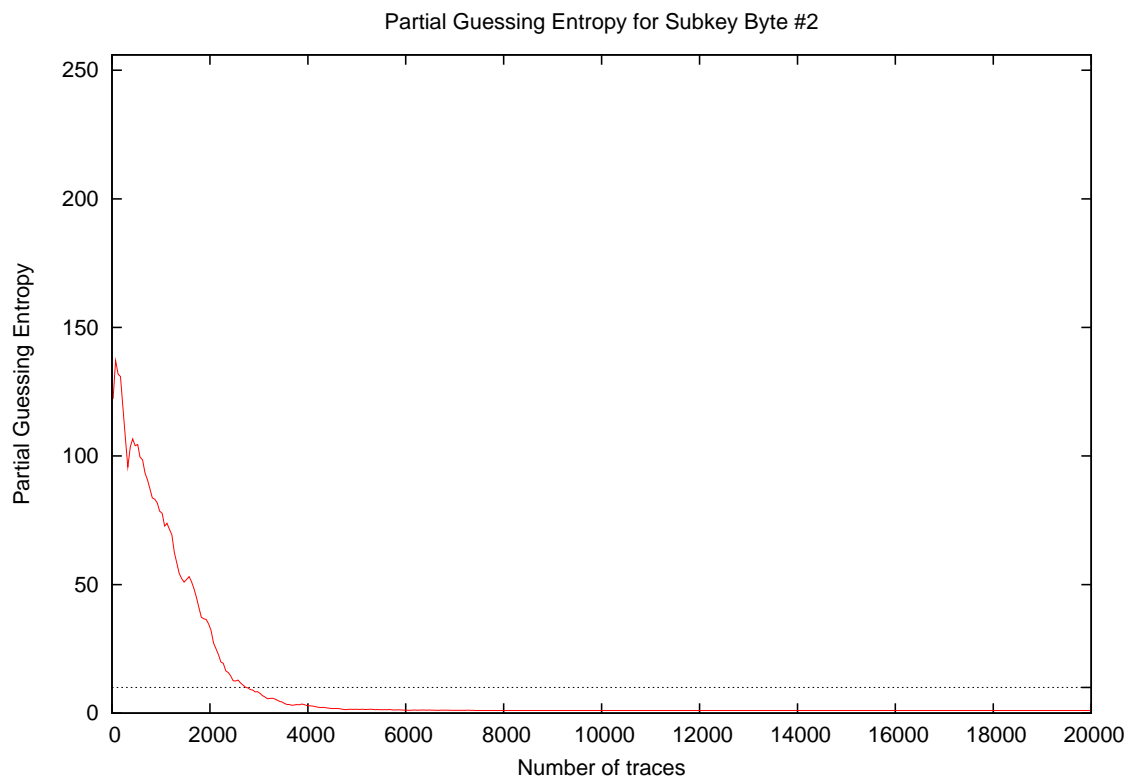
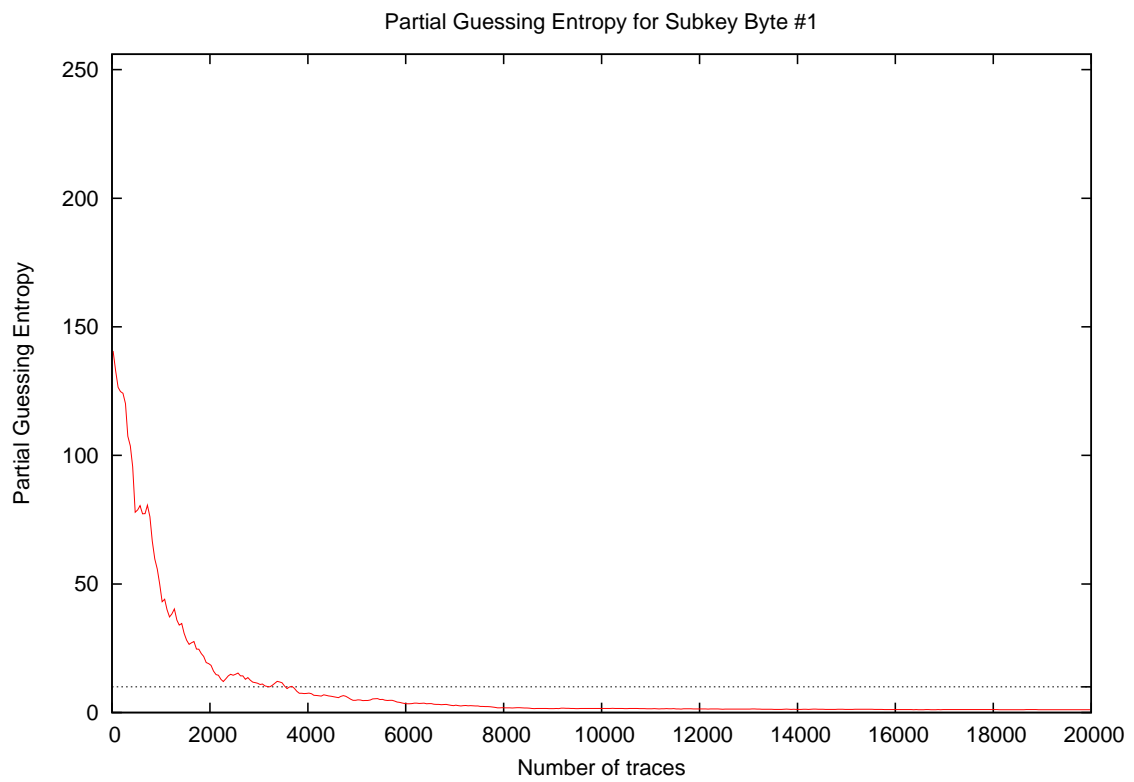


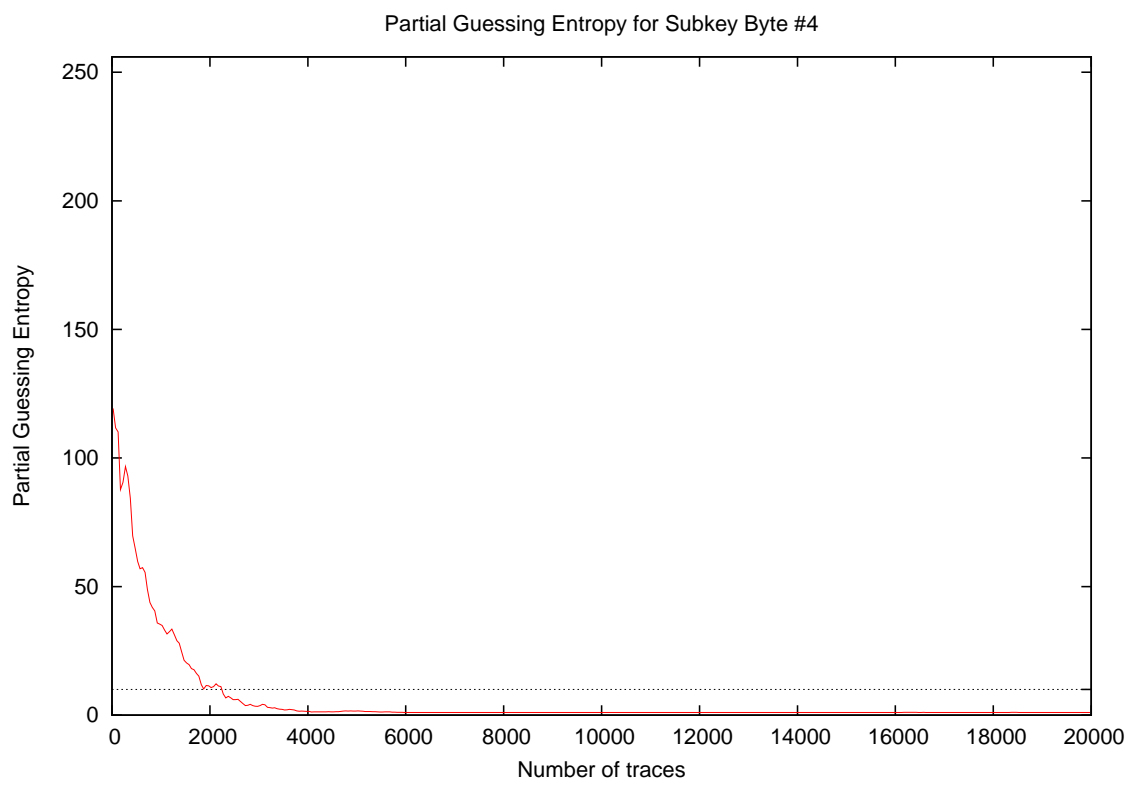
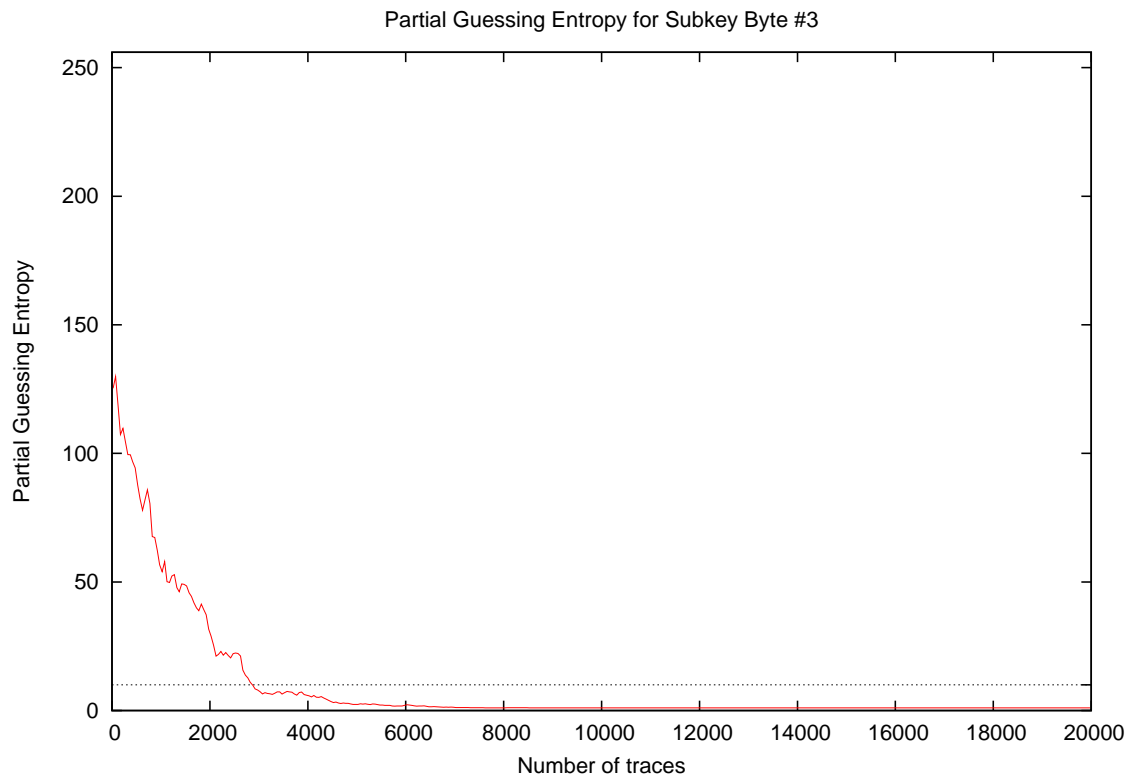
Partial Success Rate for Subkey Bytes #1 to #16



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	0.03	0.03	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.03	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	0.00	0.00	0.00	0.00	0.03	0.00	0.00	0.03	0.00	0.00	0.00	
30	0.00	0.00	0.03	0.00	0.00	0.00	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	0.03	0.01
40	0.00	0.00	0.03	0.03	0.00	0.03	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.03	0.01
50	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	0.00	0.00	0.00	0.00	0.00	0.03	0.00
100	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	0.00	0.00	0.00	0.00	0.03	0.00
200	0.06	0.03	0.00	0.00	0.03	0.00	0.00	0.00	0.03	0.03	0.03	0.03	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.06	0.02
300	0.03	0.06	0.03	0.09	0.06	0.00	0.06	0.00	0.00	0.03	0.00	0.12	0.03	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.12	0.04
400	0.03	0.03	0.00	0.09	0.06	0.03	0.12	0.00	0.06	0.03	0.03	0.22	0.03	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.22	0.05
500	0.03	0.03	0.00	0.06	0.03	0.06	0.09	0.00	0.09	0.06	0.03	0.16	0.03	0.06	0.03	0.06	0.00	0.00	0.00	0.00	0.16	0.05
1000	0.12	0.03	0.09	0.12	0.12	0.09	0.25	0.03	0.09	0.34	0.06	0.25	0.22	0.25	0.12	0.12	0.03	0.34	1.00	0.09	0.34	0.15
2000	0.19	0.12	0.19	0.41	0.28	0.69	0.44	0.22	0.28	0.81	0.09	0.62	0.34	1.00	0.19	0.41	0.09	1.00	1.00	0.09	1.00	0.39
3000	0.28	0.41	0.34	0.81	0.47	0.84	0.66	0.47	0.50	1.00	0.38	0.81	0.56	1.00	0.31	0.66	0.28	1.00	1.00	0.28	1.00	0.59
4000	0.38	0.59	0.59	0.91	0.50	0.97	0.91	0.53	0.53	1.00	0.56	0.97	0.69	1.00	0.38	0.84	0.38	1.00	1.00	0.38	1.00	0.71
5000	0.50	0.81	0.66	0.91	0.50	1.00	0.94	0.62	0.72	1.00	0.62	0.94	0.81	1.00	0.56	0.94	0.50	1.00	1.00	0.50	1.00	0.78
10000	0.78	1.00	1.00	1.00	0.78	0.94	1.00	1.00	0.88	1.00	0.94	1.00	0.97	1.00	0.88	1.00	0.78	1.00	1.00	0.78	1.00	0.95
15000	0.91	1.00	1.00	1.00	0.91	0.97	0.97	1.00	0.91	1.00	1.00	1.00	0.97	1.00	1.00	1.00	0.91	1.00	1.00	0.91	1.00	0.98
20000	0.97	1.00	1.00	0.97	0.97	0.97	0.97	1.00	0.88	1.00	1.00	1.00	1.00	1.00	1.00	1.00	0.88	1.00	1.00	0.88	1.00	0.98

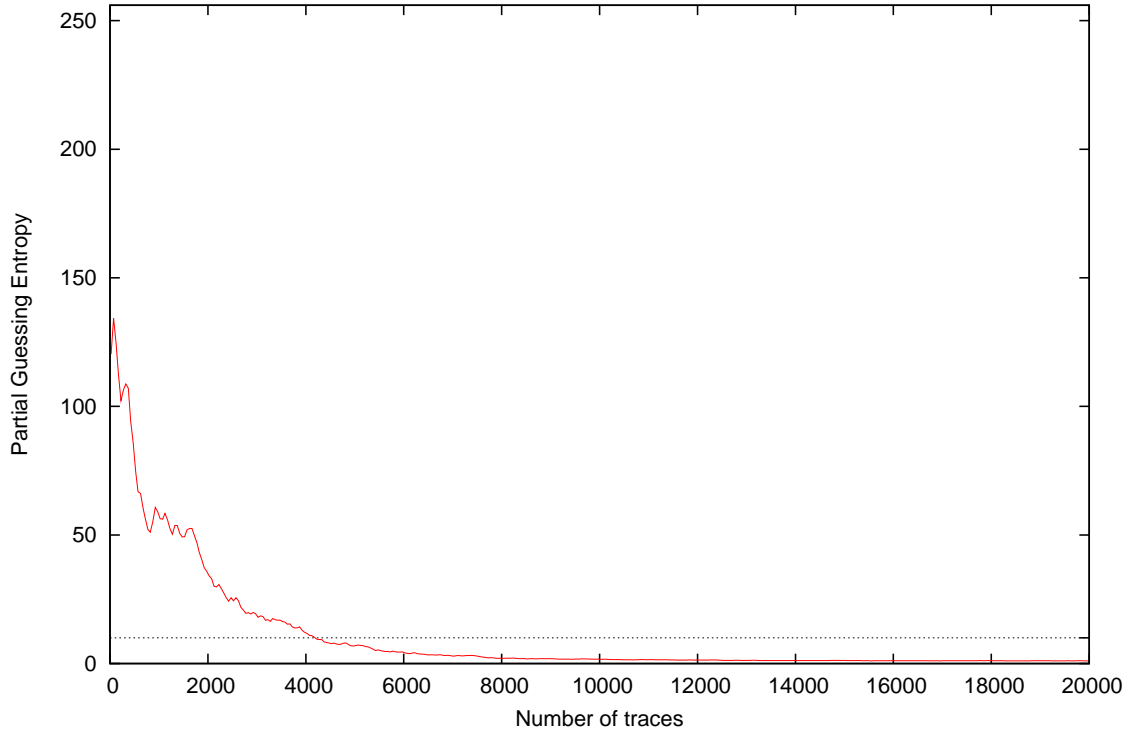
## 4 Partial Guessing Entropy



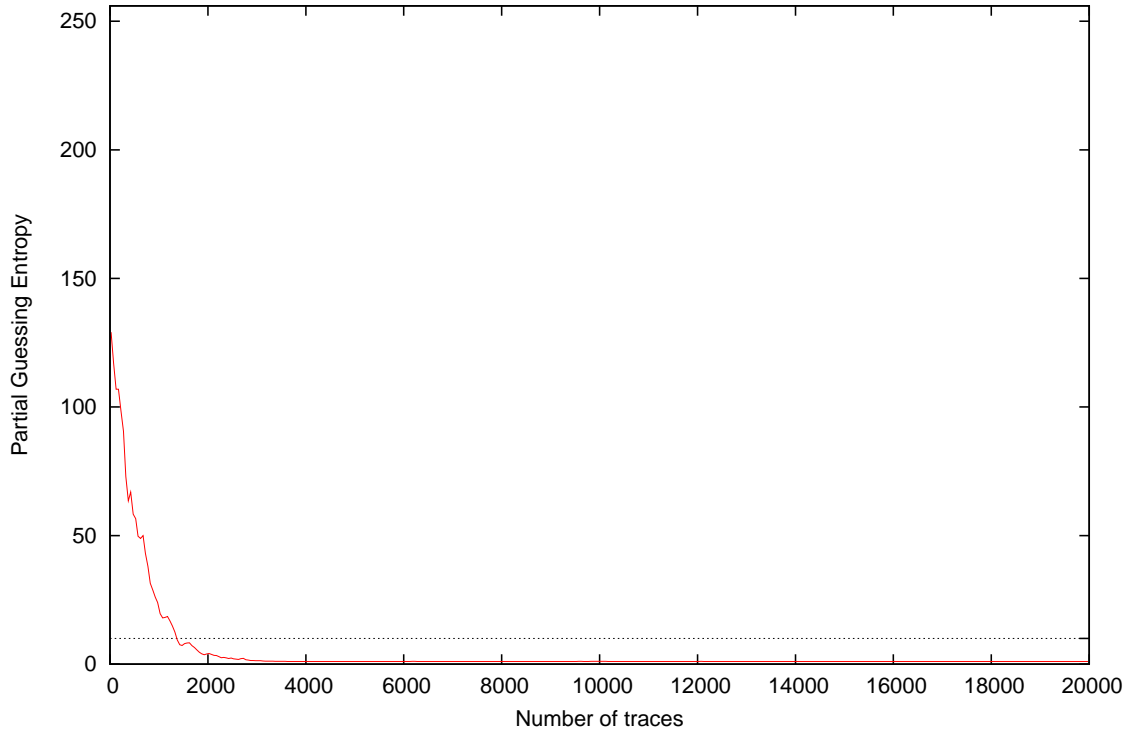


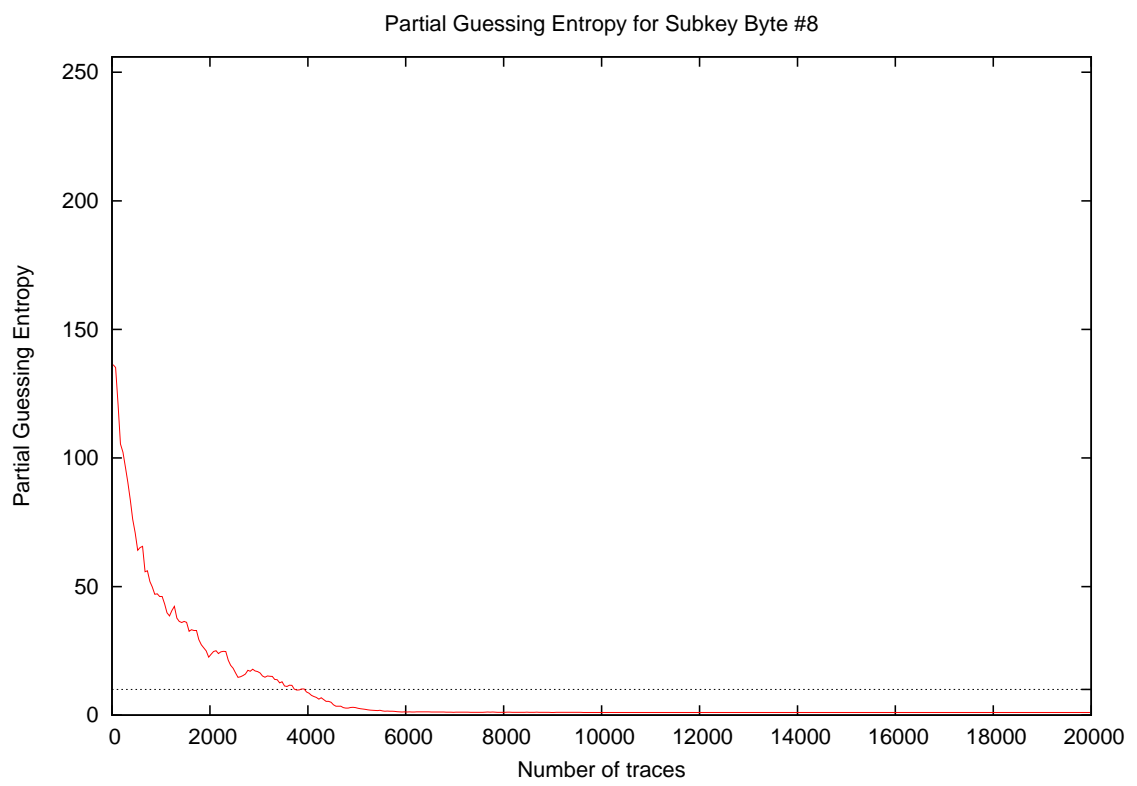
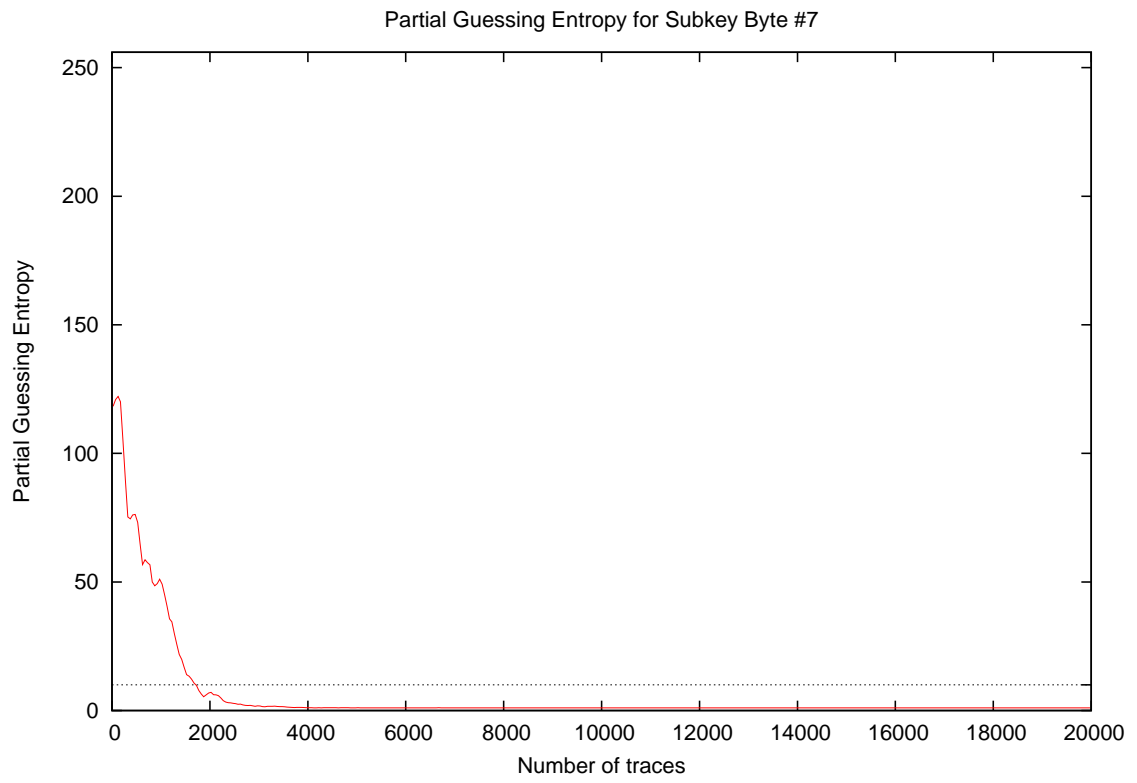


Partial Guessing Entropy for Subkey Byte #5

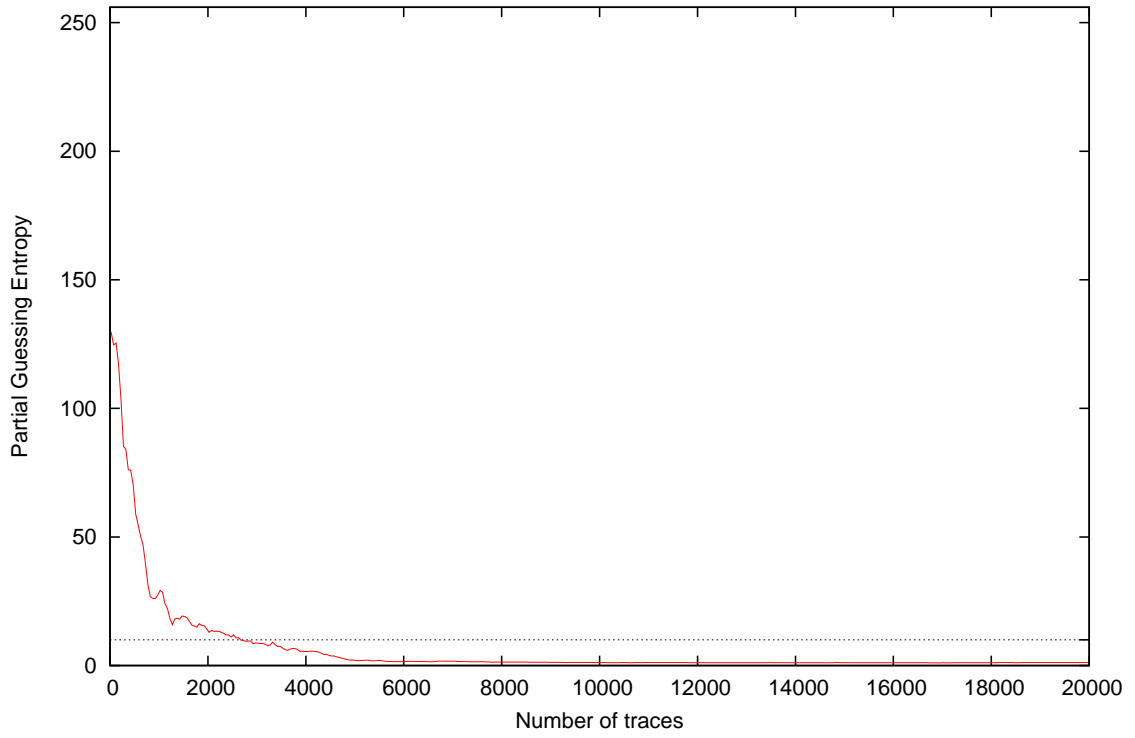


Partial Guessing Entropy for Subkey Byte #6

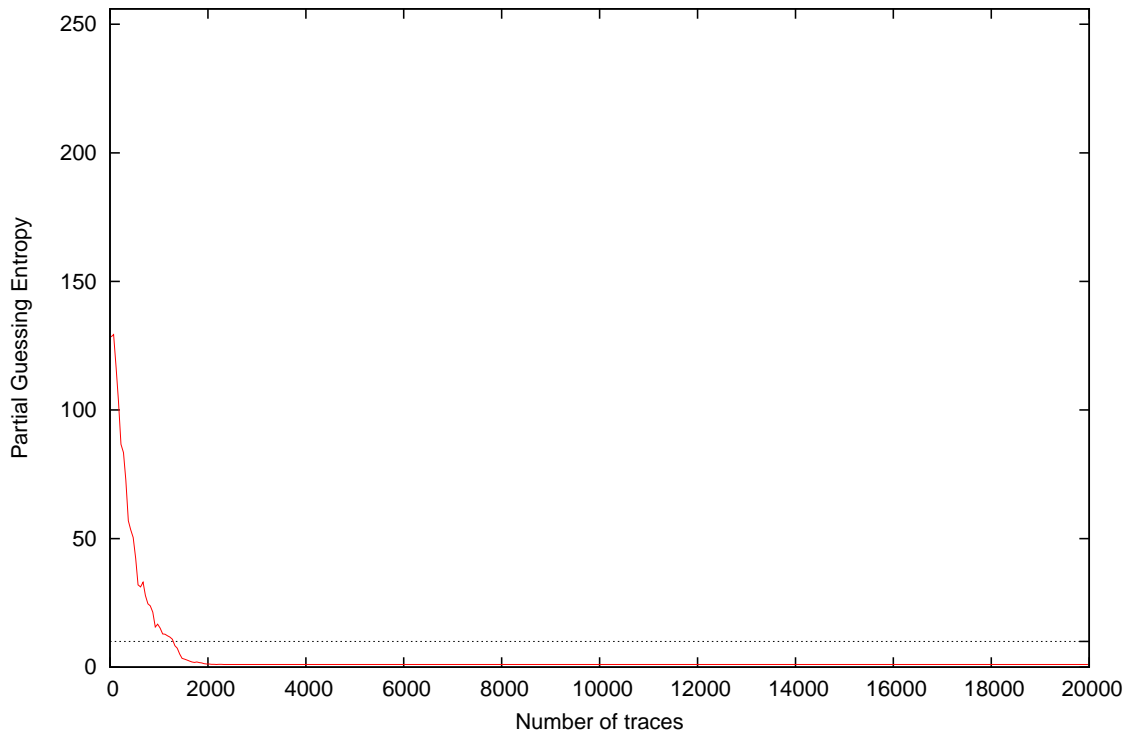




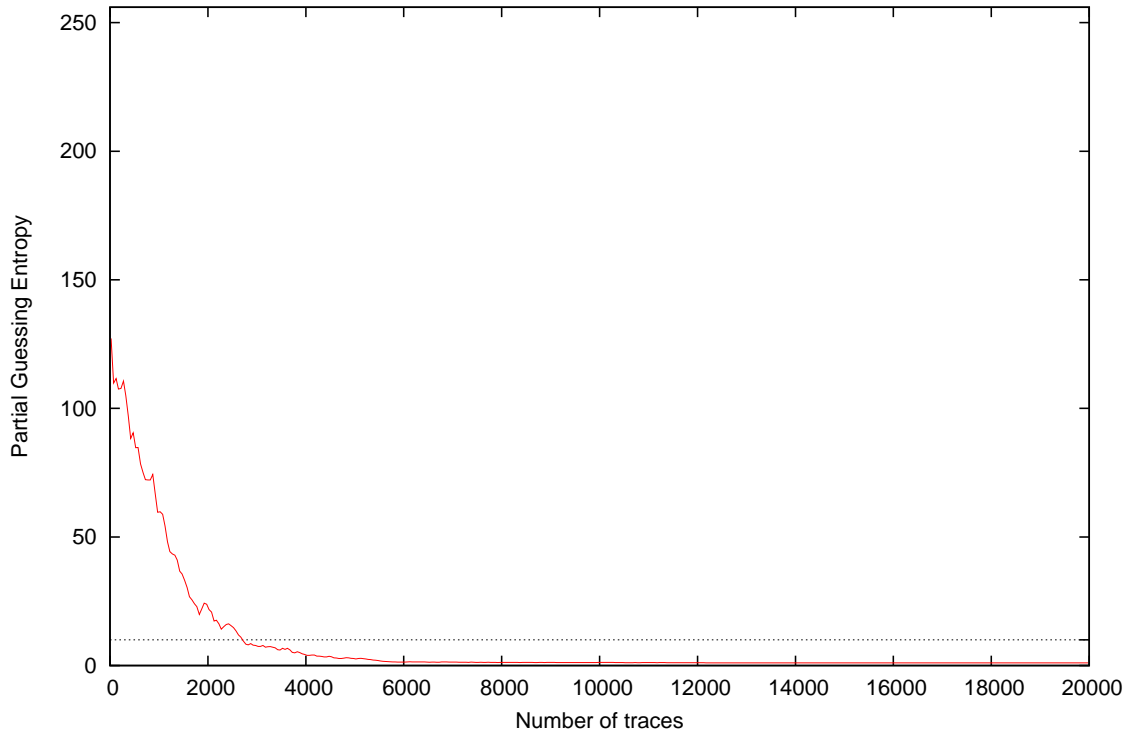
Partial Guessing Entropy for Subkey Byte #9



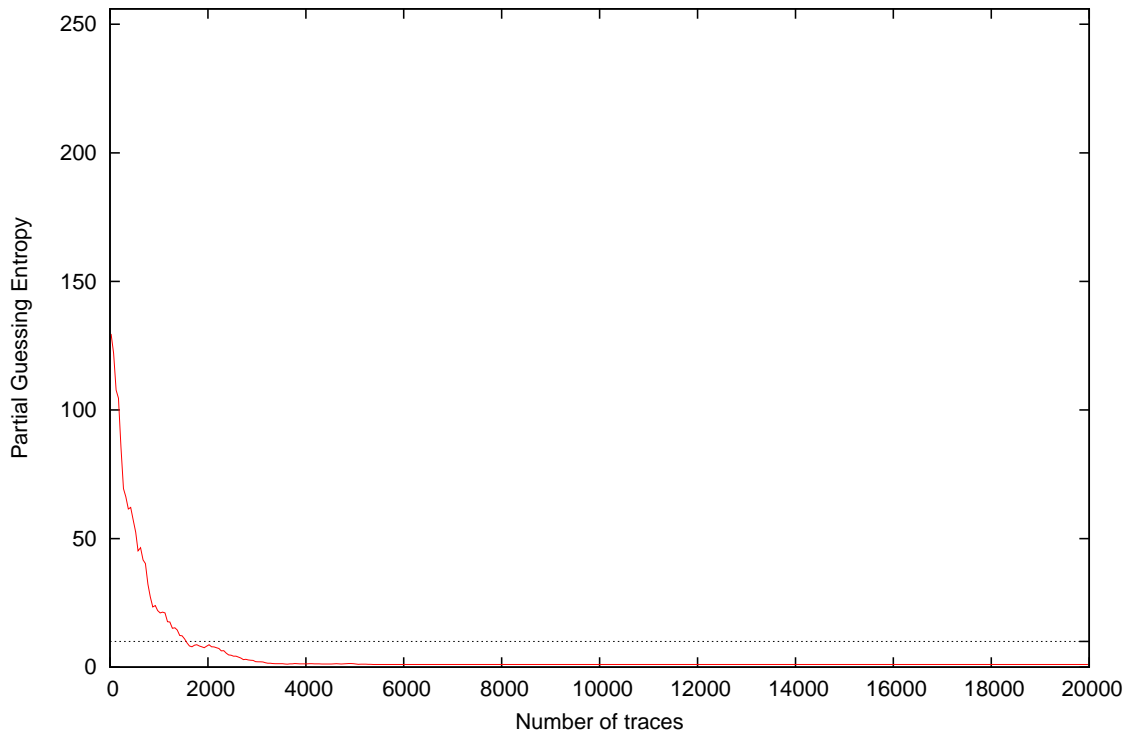
Partial Guessing Entropy for Subkey Byte #10

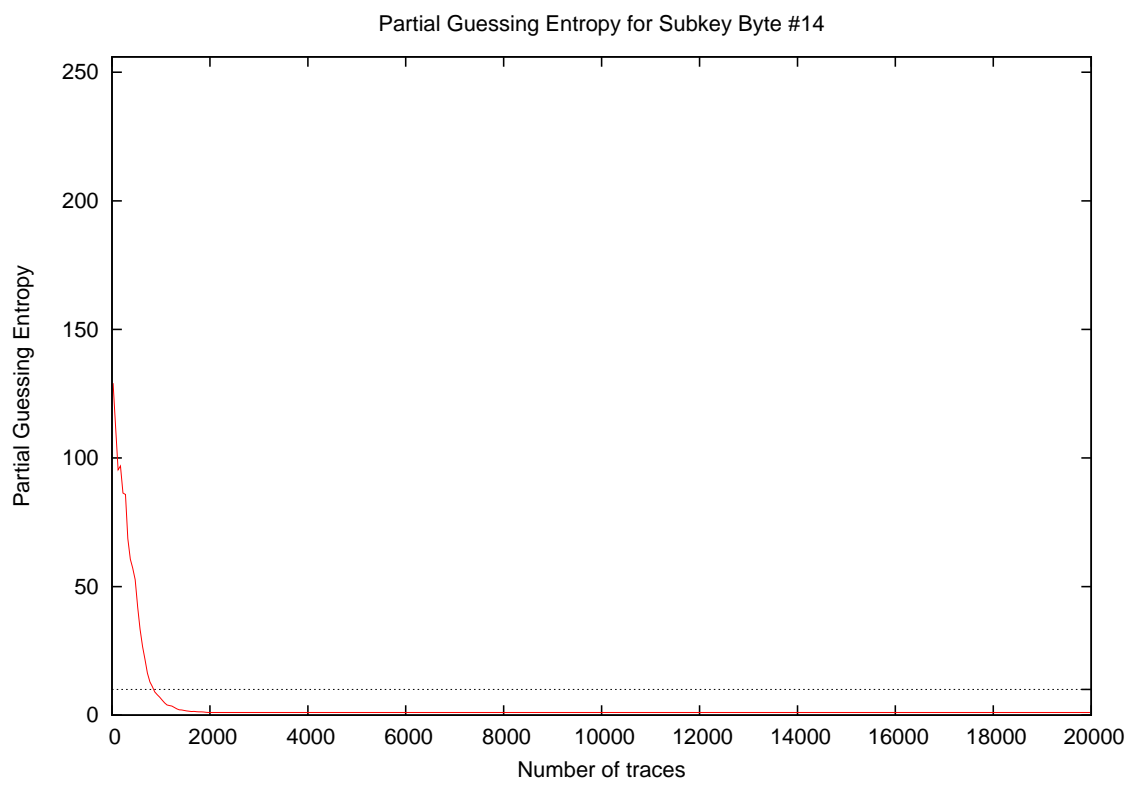
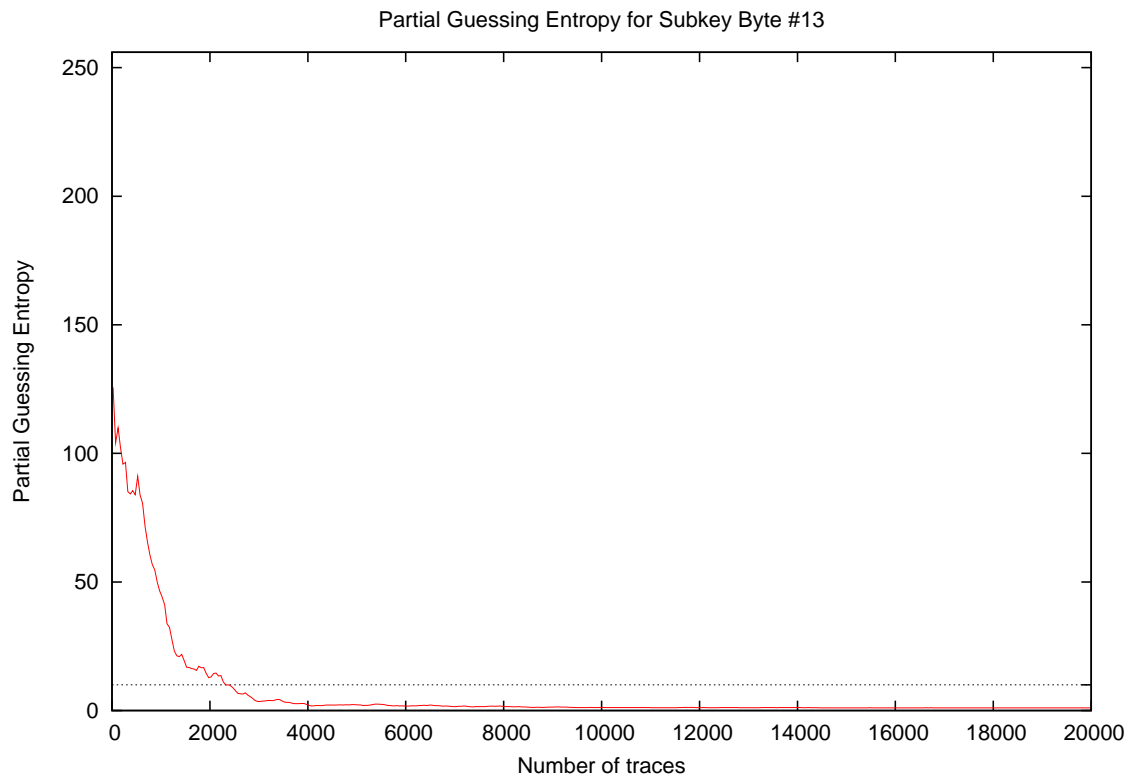


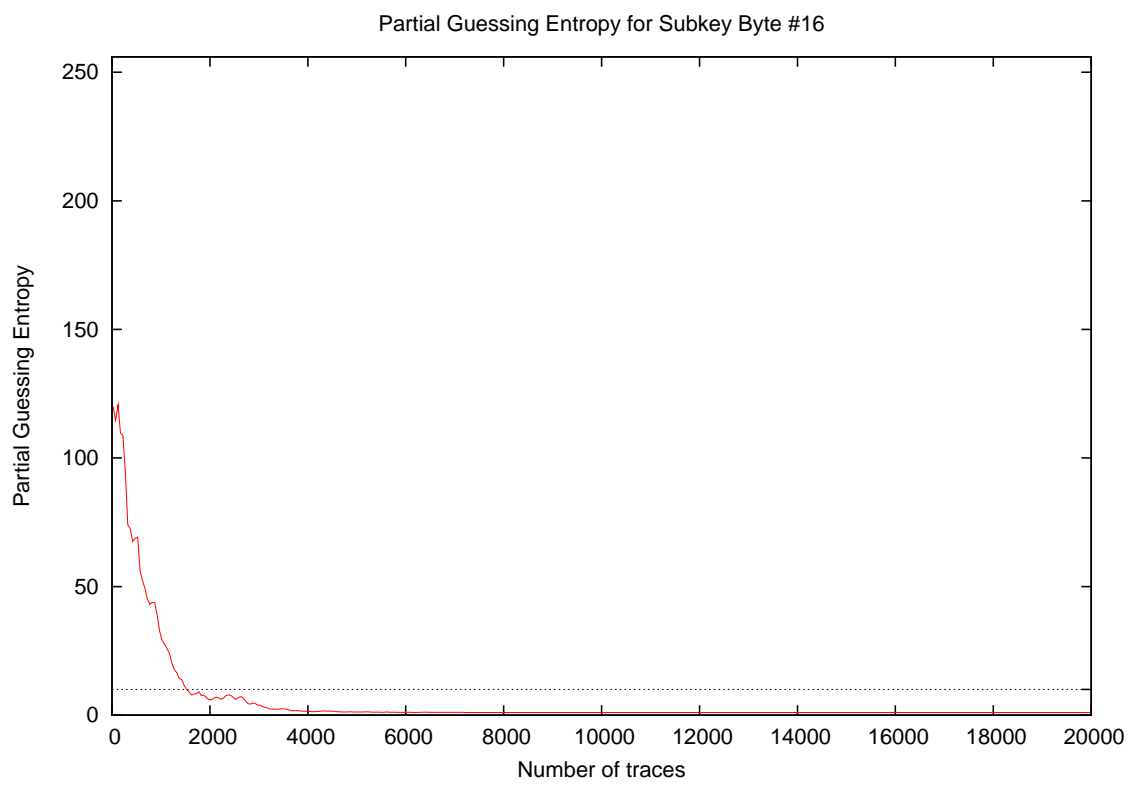
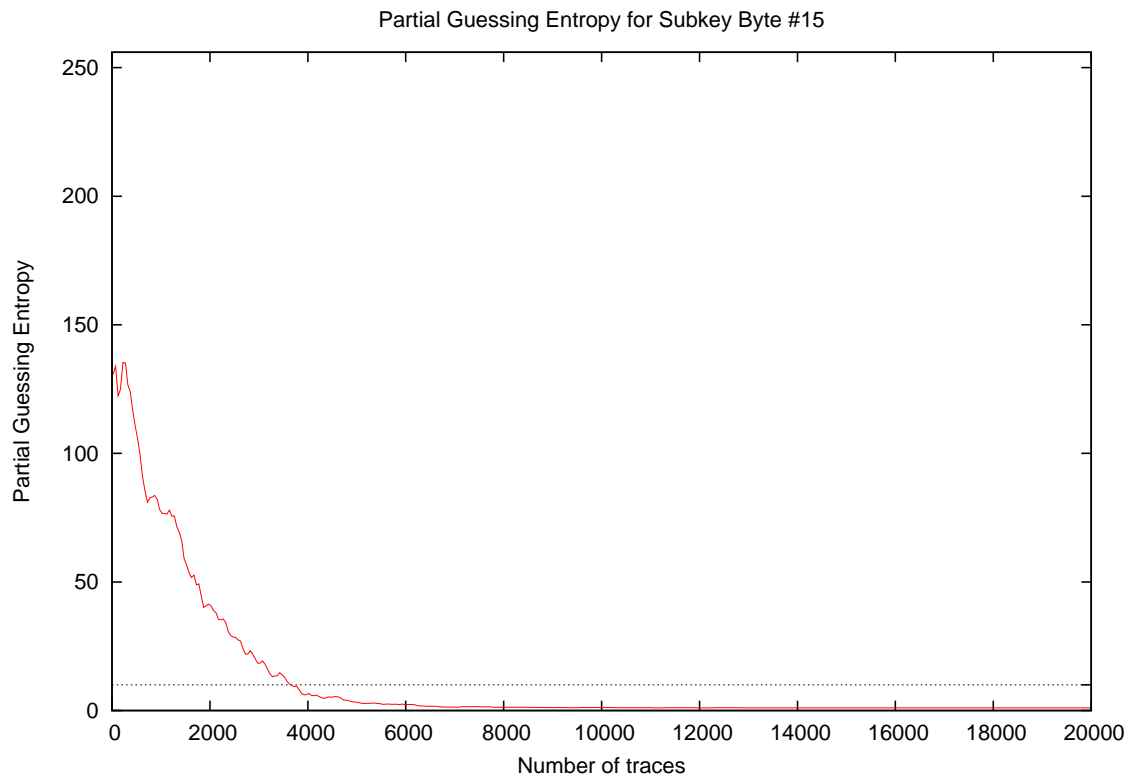
Partial Guessing Entropy for Subkey Byte #11

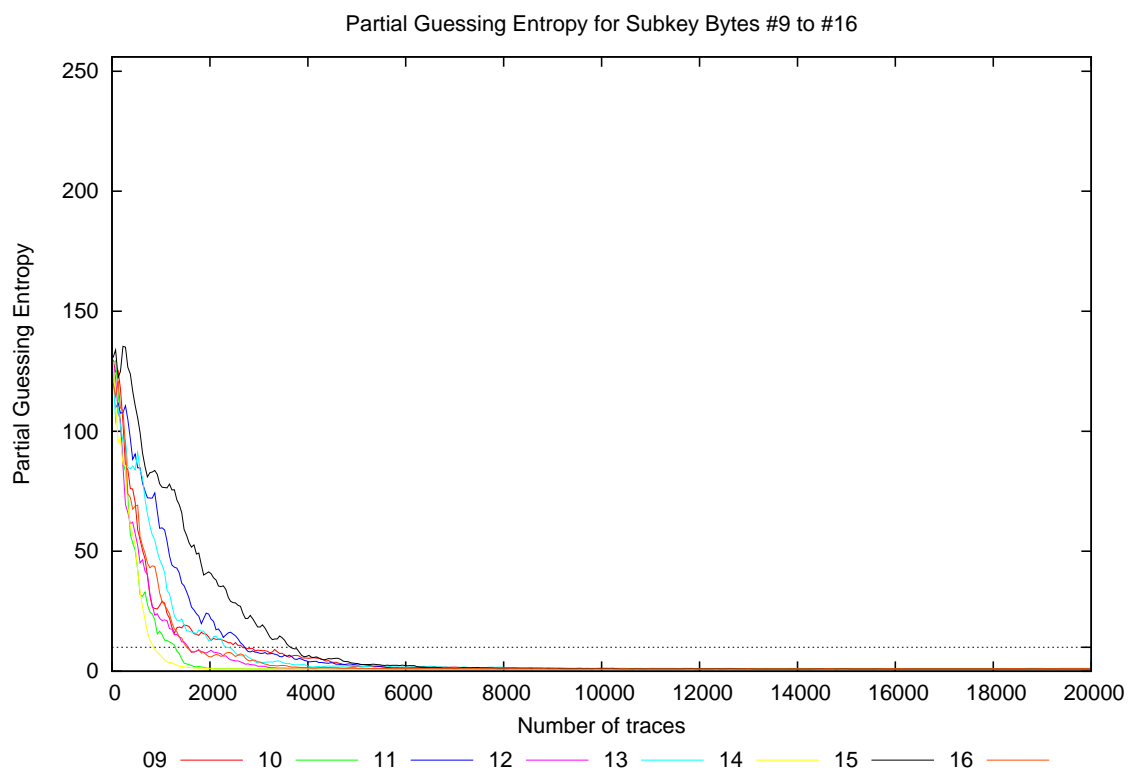
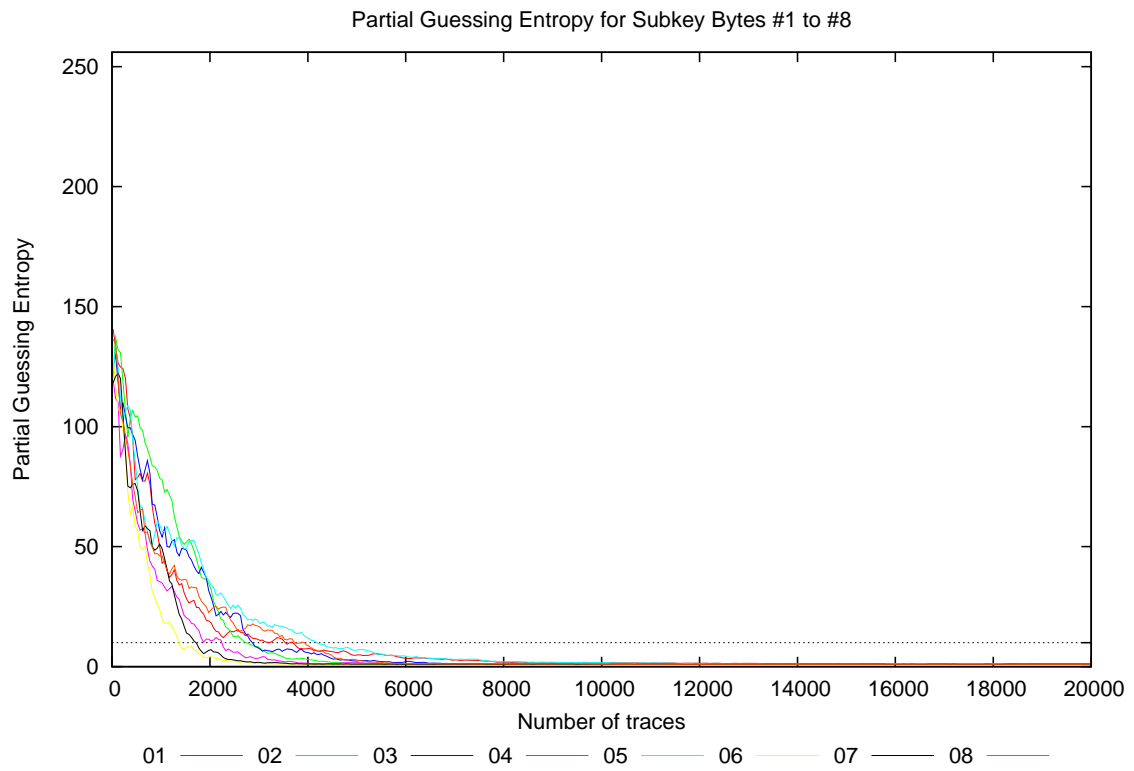


Partial Guessing Entropy for Subkey Byte #12

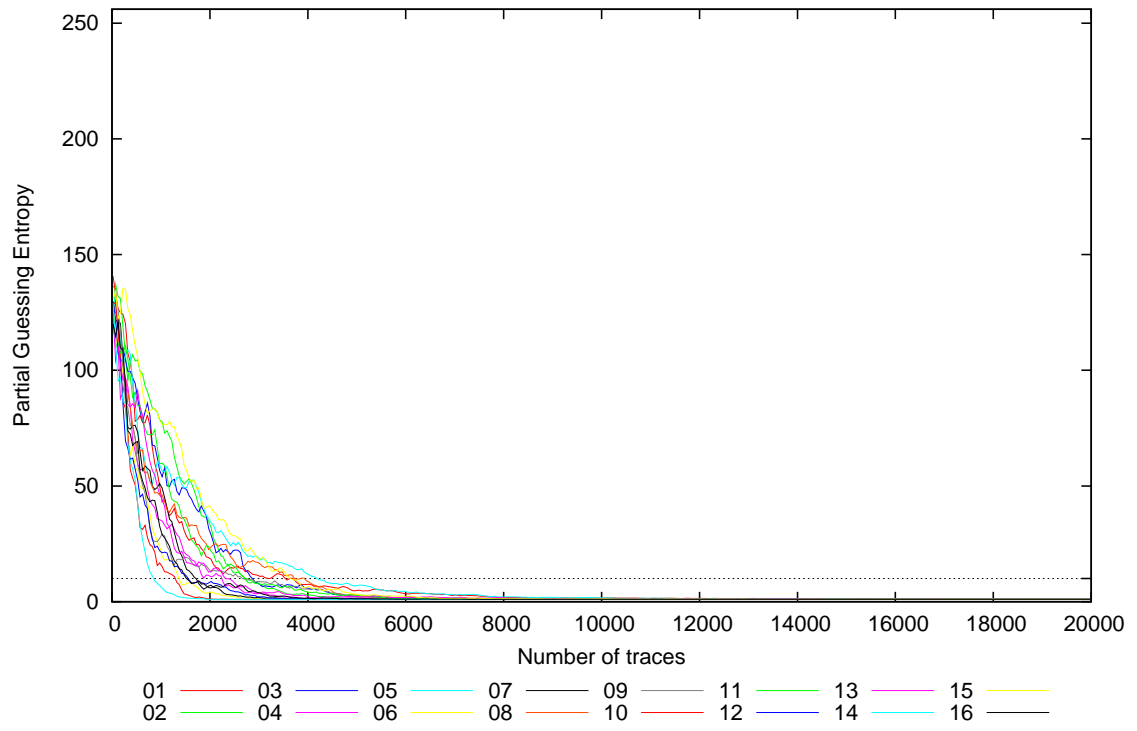








Partial Guessing Entropy for Subkey Bytes #1 to #16





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	111.5	117.0	125.4	147.0	106.9	142.7	118.7	150.5	136.8	130.5	147.0	142.2	137.3	112.5	115.3	137.8	106.9	150.5	130.0
20	152.3	116.1	116.7	112.6	124.4	134.2	113.0	130.2	135.9	124.6	121.9	120.1	138.8	120.5	121.9	123.7	112.6	152.3	125.4
30	156.1	123.1	126.4	115.0	123.2	128.7	119.8	132.1	121.9	122.5	125.8	132.0	125.1	135.9	138.5	111.4	111.4	156.1	127.4
40	145.6	132.8	126.9	114.5	133.5	129.4	116.9	139.8	120.0	126.1	130.4	129.4	112.2	136.8	144.4	118.3	112.2	145.6	128.6
50	133.0	135.0	118.7	108.8	123.7	119.3	117.7	142.1	126.2	131.4	112.5	132.5	94.6	115.7	138.8	104.0	94.6	142.1	122.1
100	134.8	132.0	125.8	117.0	126.5	113.4	118.2	123.8	133.1	110.1	116.4	108.6	96.6	95.7	129.5	126.8	95.7	134.8	119.3
200	125.4	130.8	107.4	79.2	104.2	102.1	121.0	101.4	113.0	96.9	108.3	100.0	103.8	84.4	128.9	110.9	79.2	130.8	107.4
300	117.1	100.4	105.7	99.9	110.2	84.1	83.2	92.3	87.0	81.3	108.1	68.7	93.5	77.2	126.8	85.9	68.7	126.8	95.1
400	107.1	111.2	101.4	72.0	105.3	66.5	70.7	78.2	71.4	51.1	87.8	61.1	86.2	59.3	125.2	68.4	51.1	125.2	82.7
500	74.5	102.9	89.3	62.7	79.0	58.8	74.1	66.6	61.5	45.4	90.0	55.4	89.2	46.4	111.4	73.4	45.4	111.4	73.8
1000	46.1	79.2	54.6	35.0	57.0	20.8	47.2	47.4	28.5	16.3	57.5	21.5	45.7	6.4	79.2	29.3	6.4	79.2	42.0
2000	19.2	32.7	29.7	10.3	34.6	4.3	7.3	24.6	13.9	1.3	22.8	8.5	13.0	1.0	39.1	6.0	1.0	39.1	16.8
3000	11.0	7.8	7.8	3.6	18.2	1.3	1.8	16.9	8.5	1.0	7.6	2.0	3.5	1.0	18.0	4.0	1.0	18.2	7.1
4000	7.6	2.8	6.0	1.4	12.1	1.0	1.1	8.6	5.2	1.0	3.9	1.3	2.2	1.0	6.5	1.4	1.0	12.1	3.9
5000	4.6	1.5	2.3	1.7	6.8	1.0	1.1	3.0	2.0	1.0	2.7	1.3	2.1	1.0	3.3	1.2	1.0	6.8	2.3
10000	1.6	1.0	1.0	1.0	1.7	1.1	1.0	1.0	1.2	1.0	1.2	1.0	1.2	1.0	1.2	1.0	1.0	1.7	1.1
15000	1.2	1.0	1.0	1.0	1.2	1.0	1.0	1.0	1.1	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.2	1.0
20000	1.1	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.2	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.2	1.0