

Evaluation results

DPA contest v2

August 2012

1 Introduction

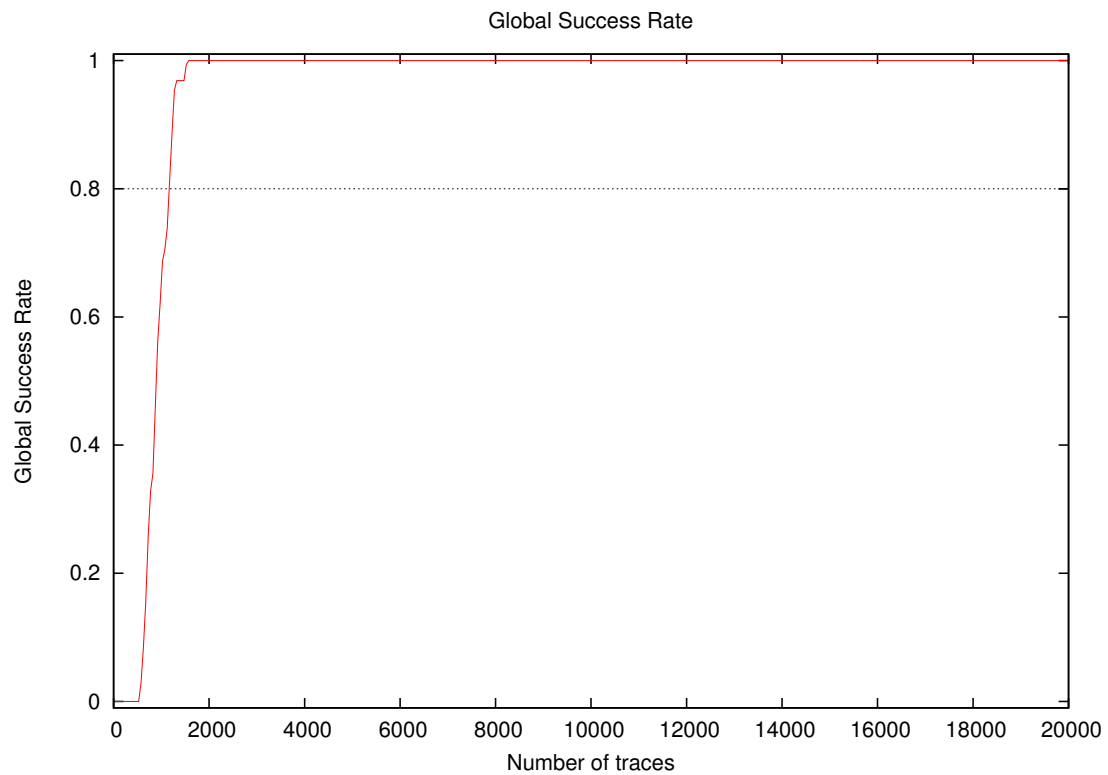
1.1 About the attack

- **Sender/Team:** Benoît Gérard, Nicolas Veyrat-Charvillon
- **Institution:** UCL
- **Language:** C++
- **Attacked subkey:** 10

1.2 About the evaluation

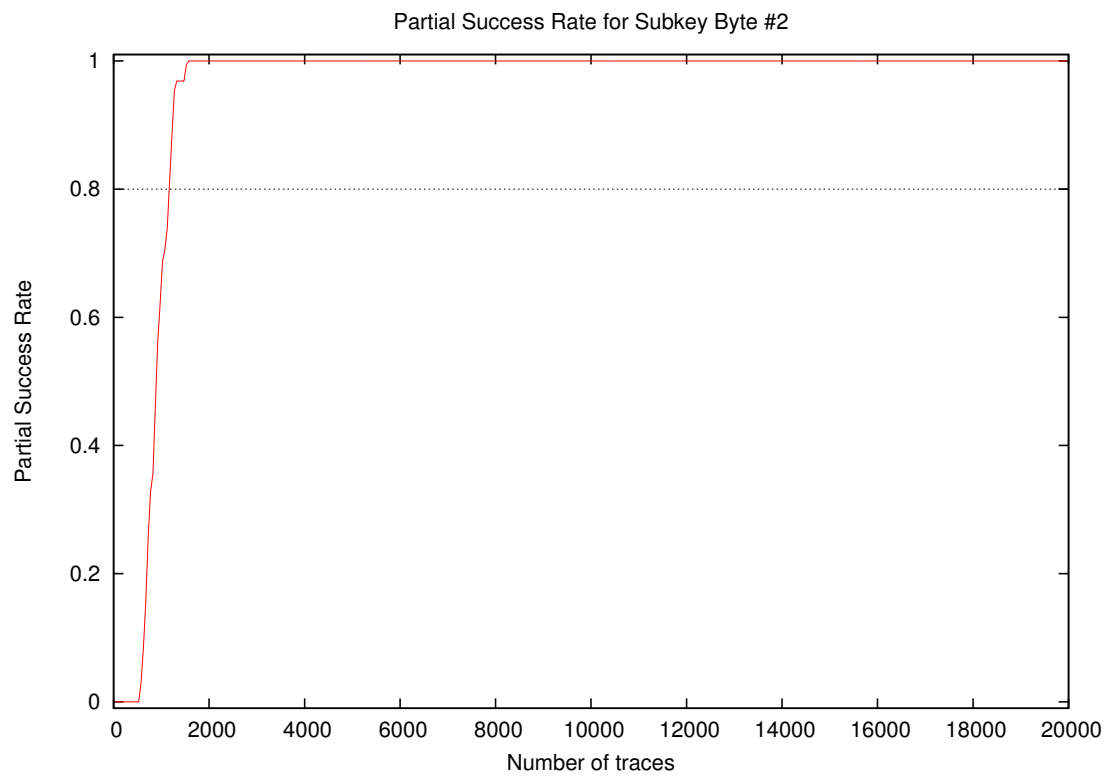
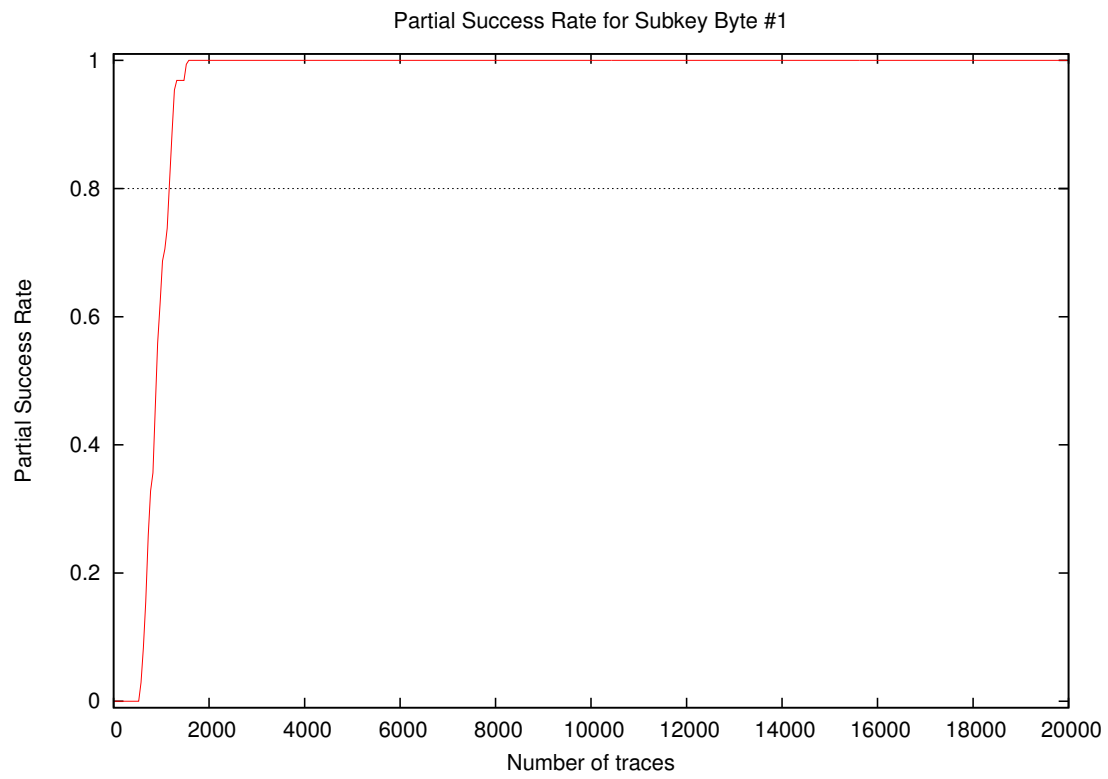
- **Date of evaluation:** August 2012

2 Global Success Rate

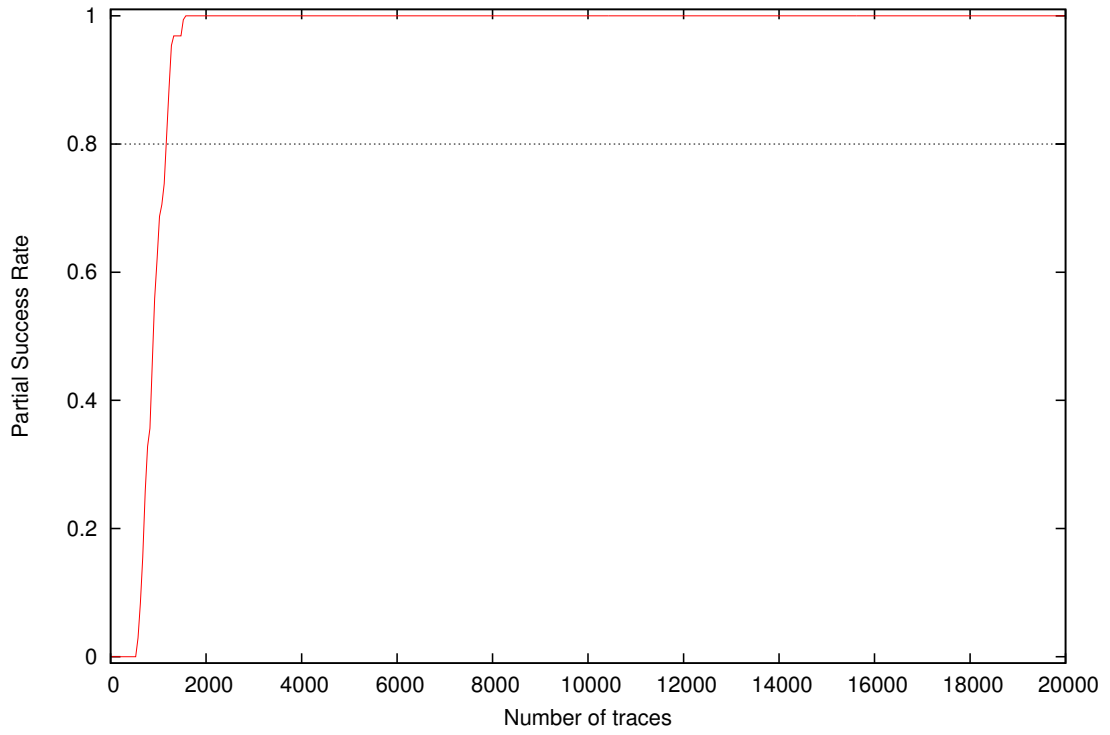


Number of traces	Global Success Rate
10	0.00
20	0.00
30	0.00
40	0.00
50	0.00
100	0.00
200	0.00
300	0.00
400	0.00
500	0.00
1000	0.66
2000	1.00
3000	1.00
4000	1.00
5000	1.00
10000	1.00
15000	1.00
20000	1.00

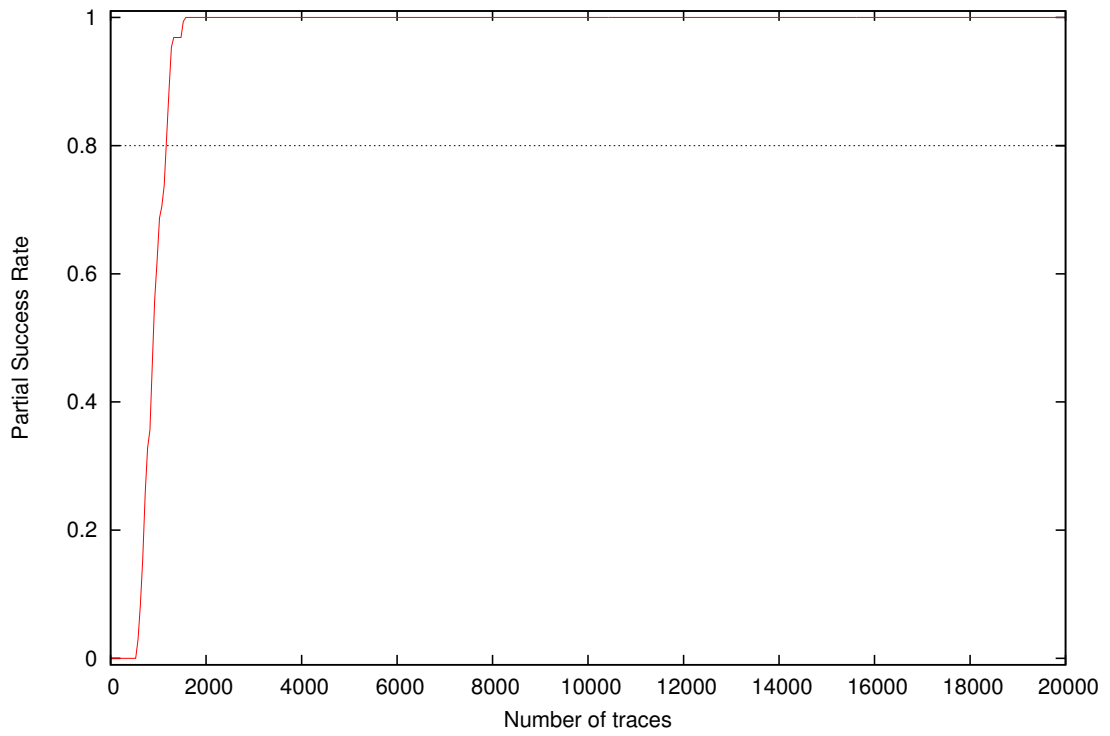
3 Partial Success Rate

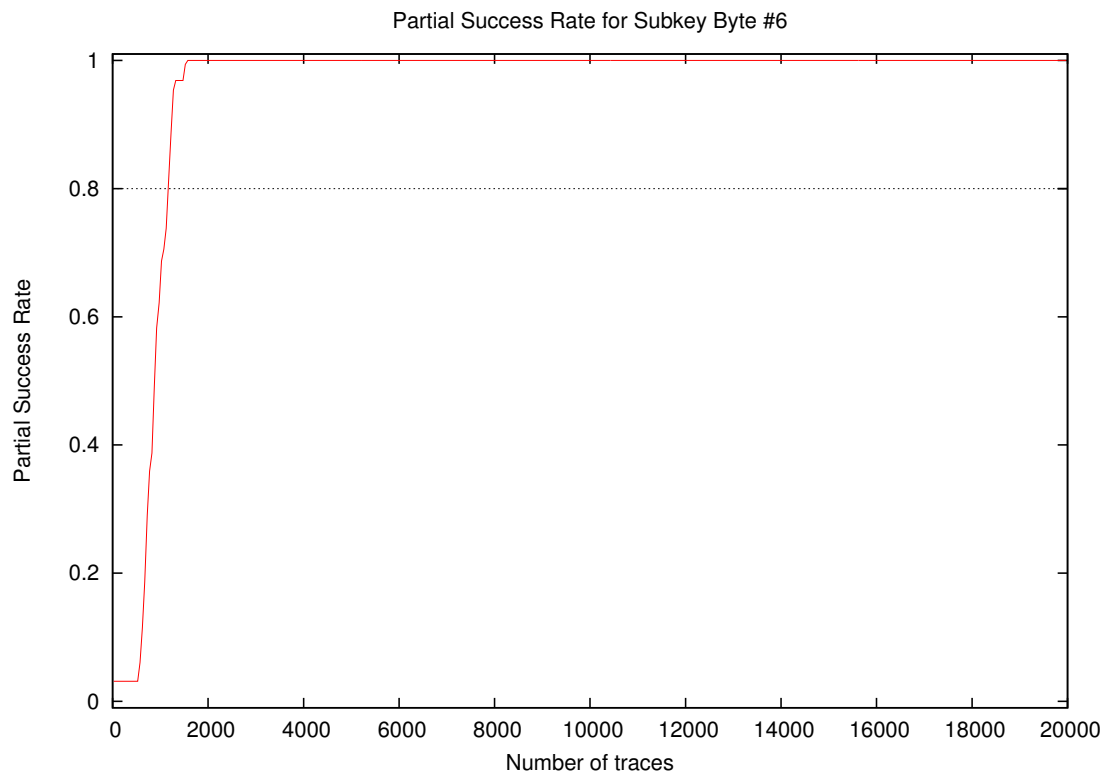
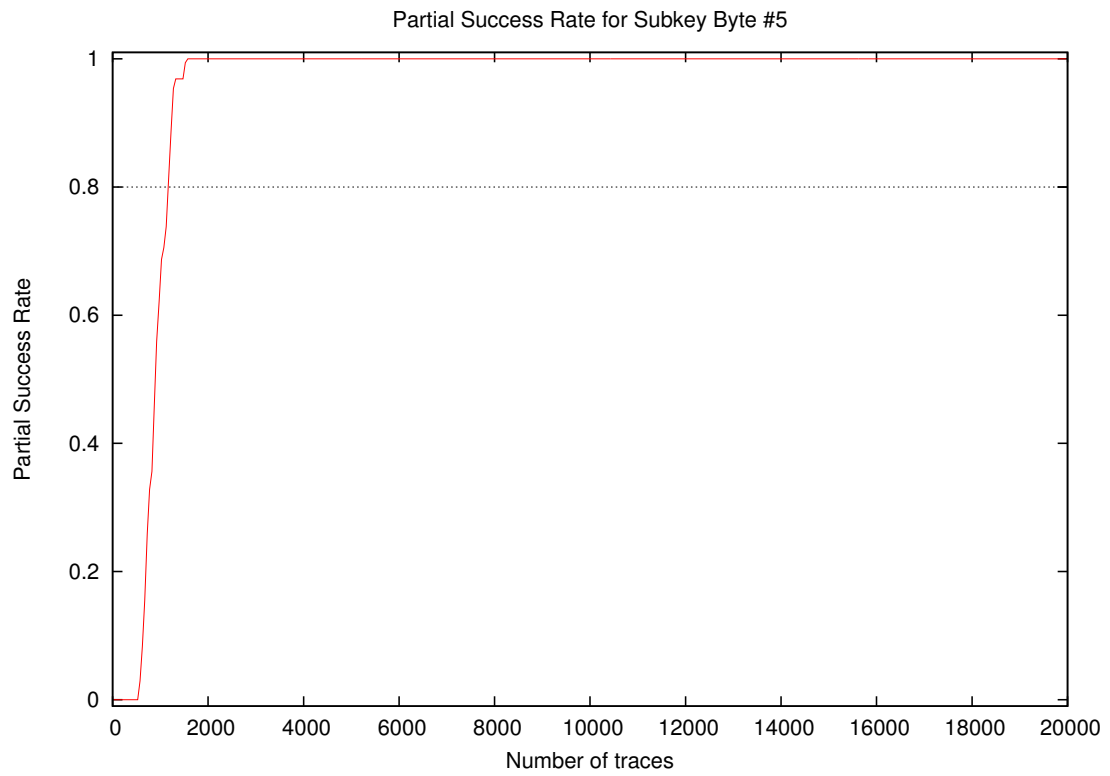


Partial Success Rate for Subkey Byte #3

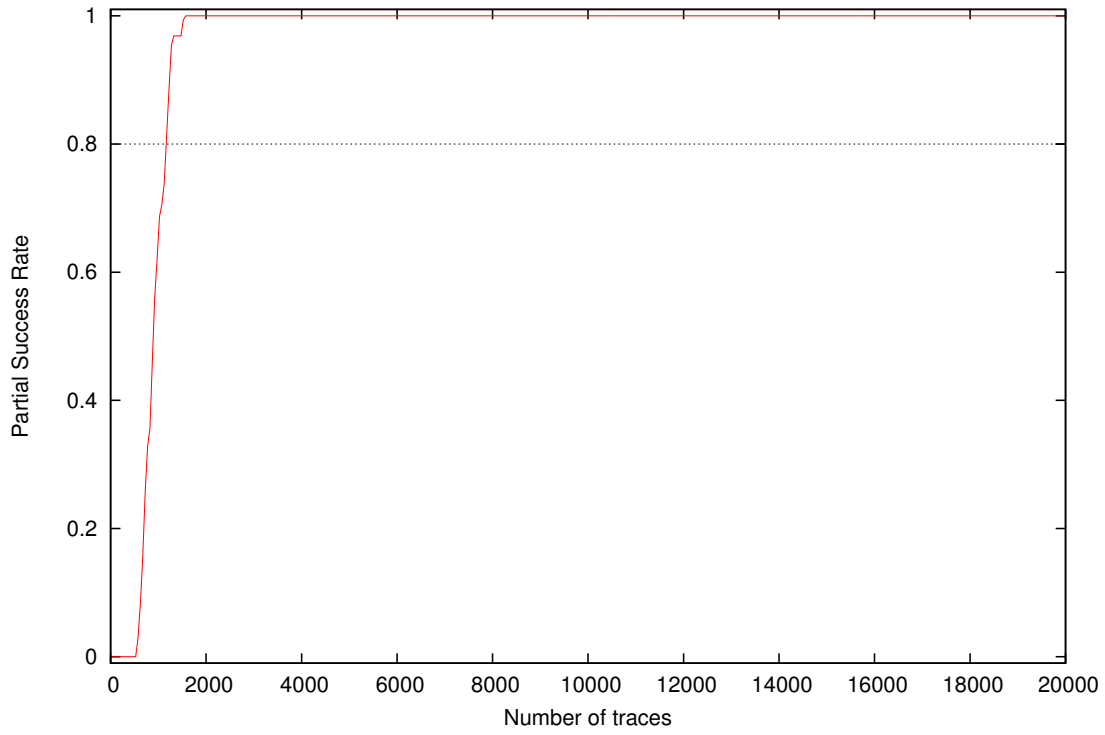


Partial Success Rate for Subkey Byte #4

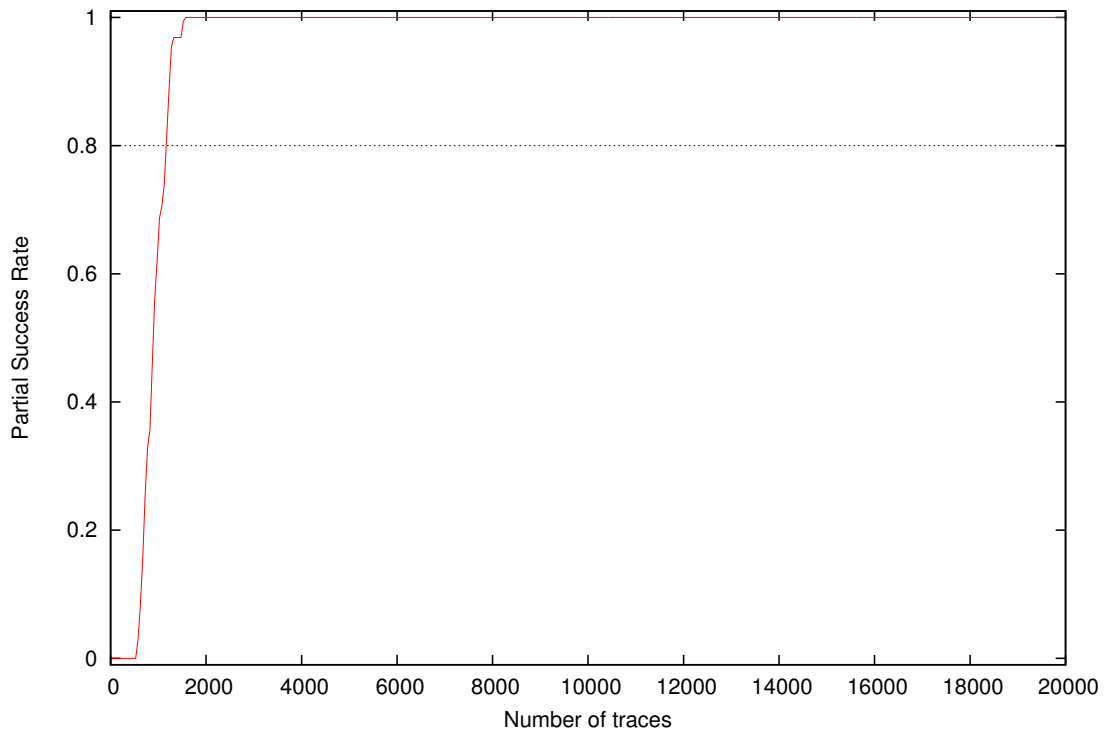




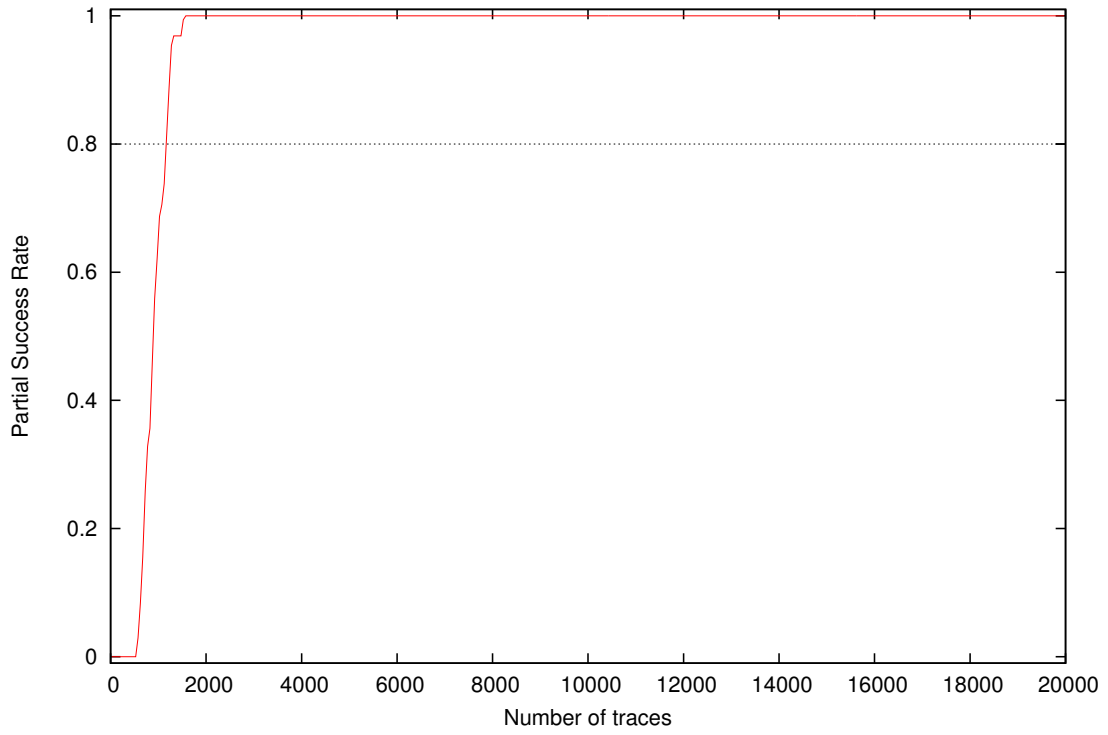
Partial Success Rate for Subkey Byte #7



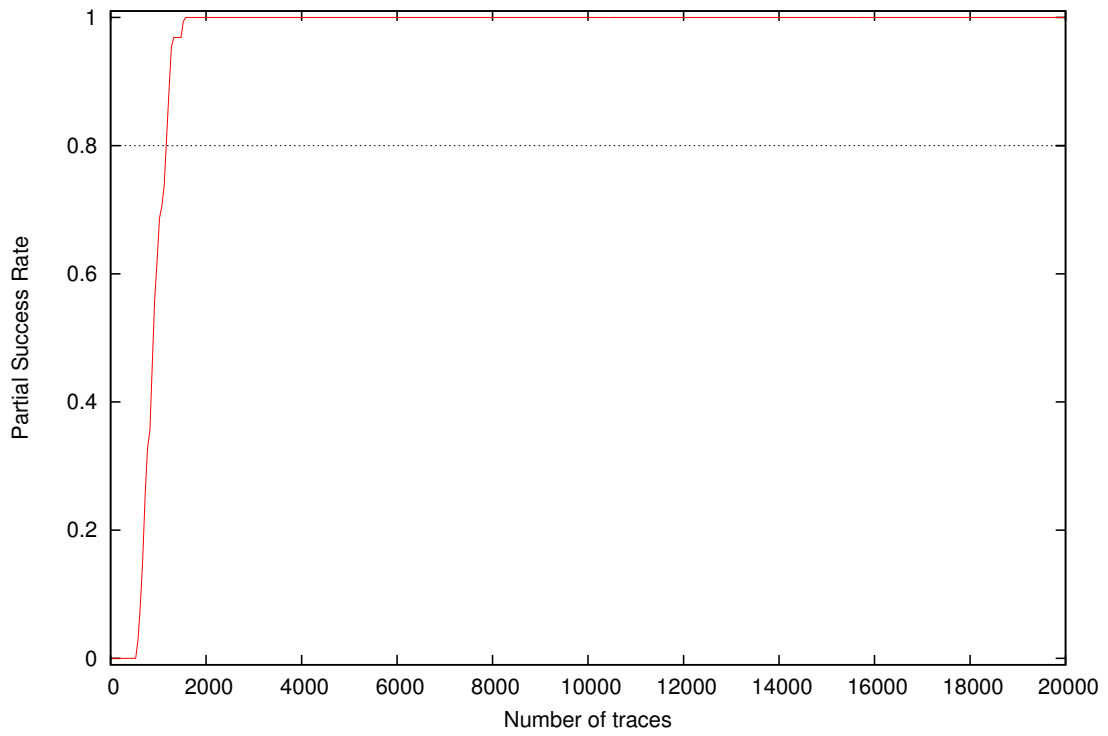
Partial Success Rate for Subkey Byte #8



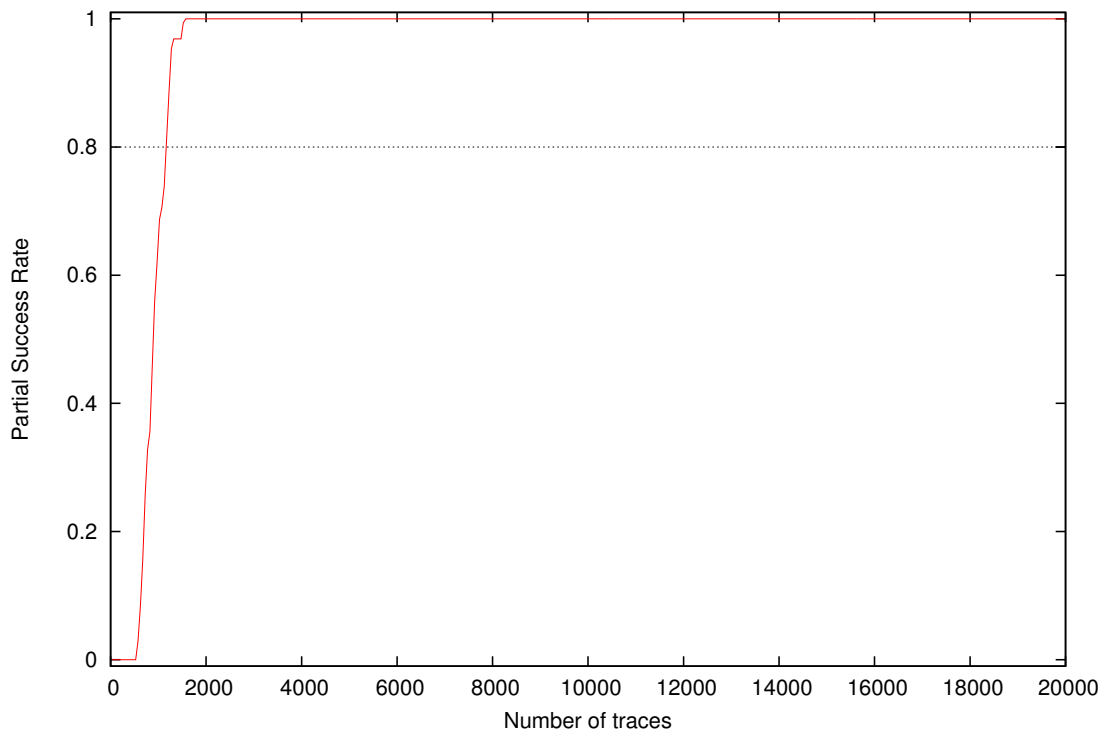
Partial Success Rate for Subkey Byte #9



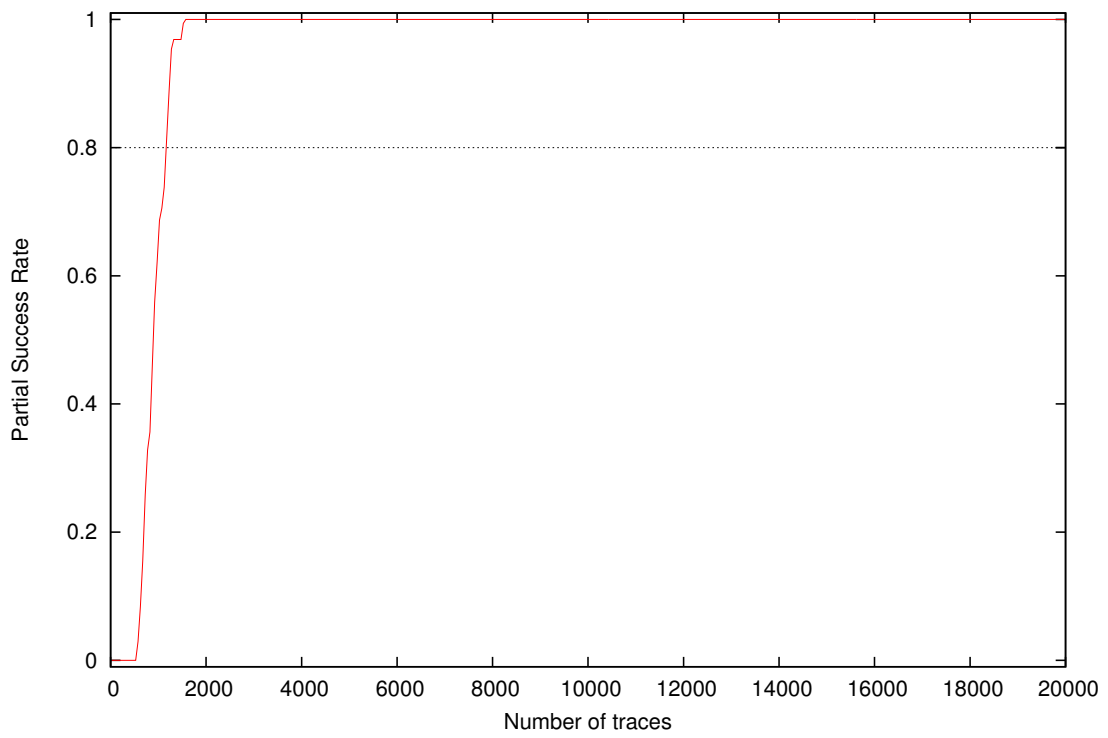
Partial Success Rate for Subkey Byte #10

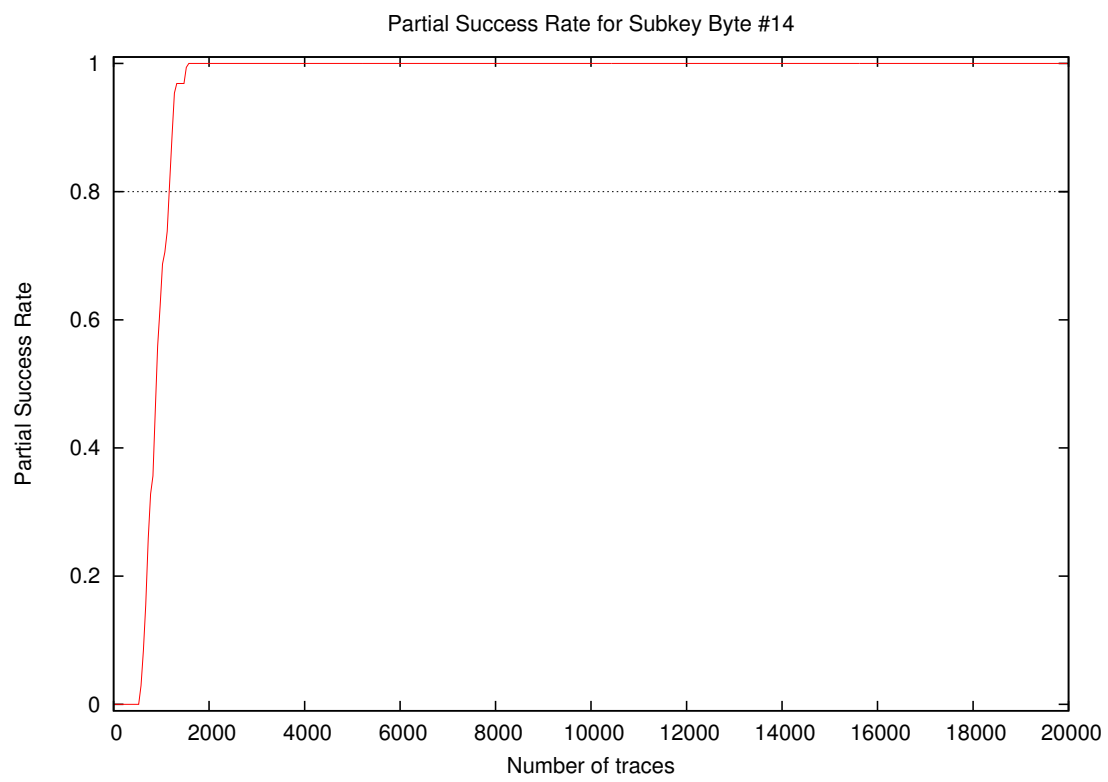
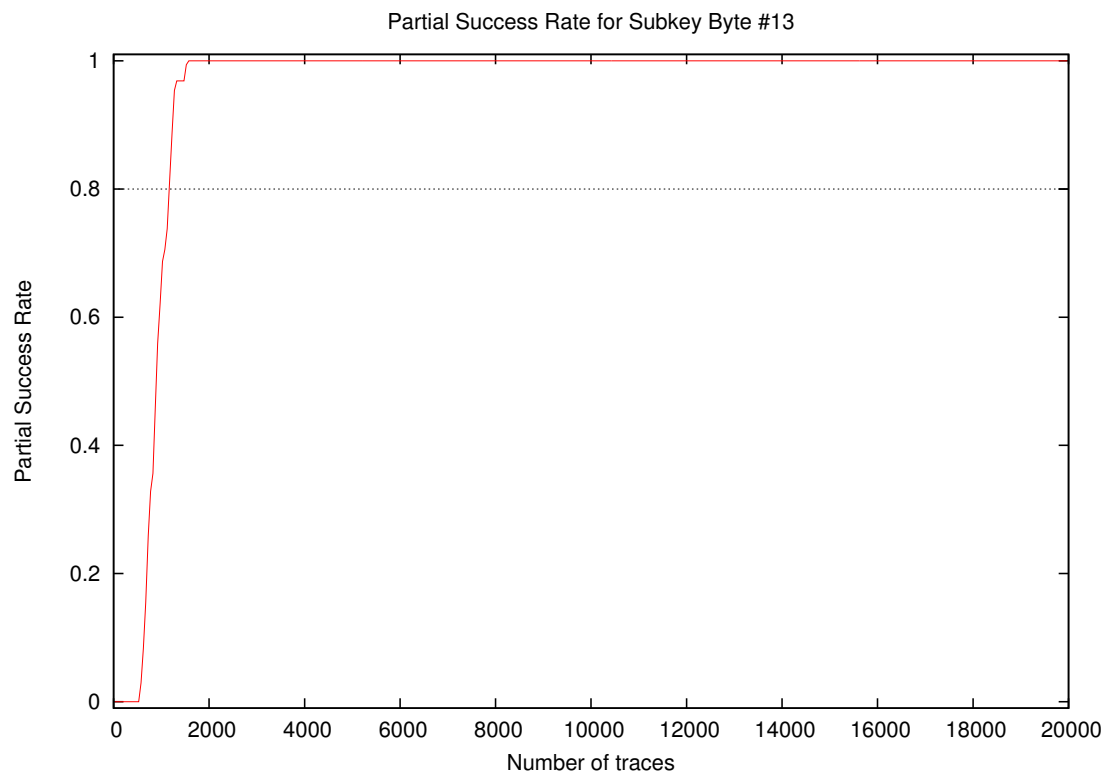


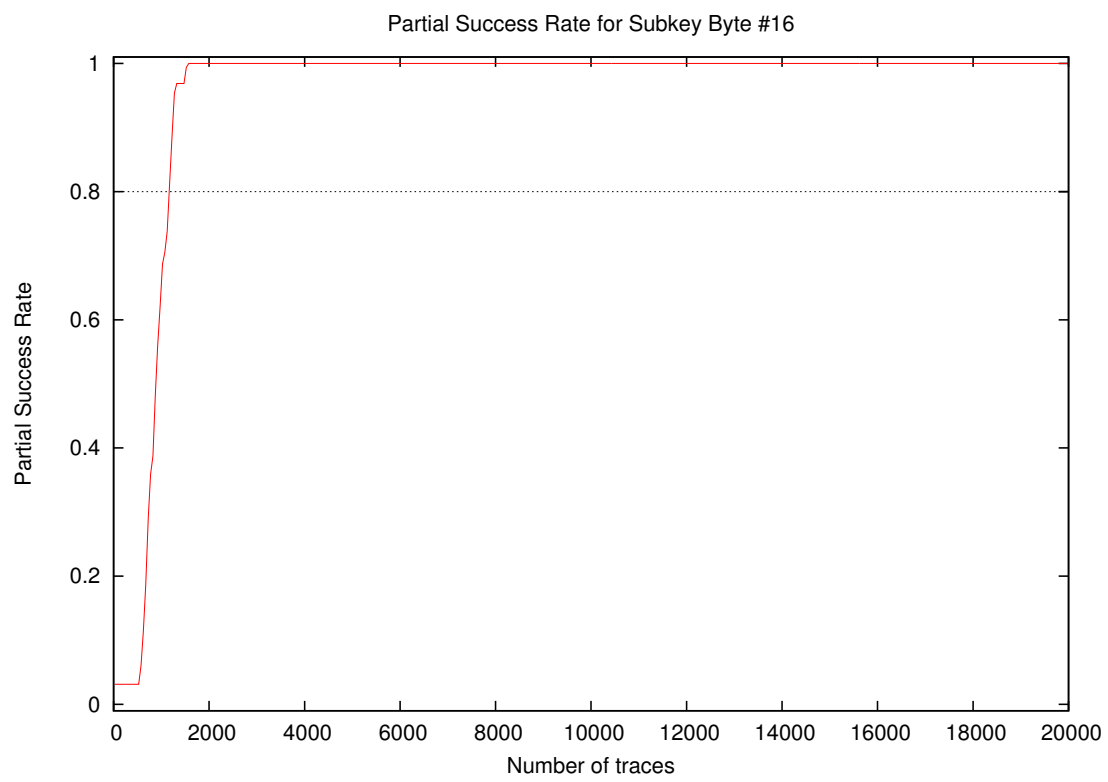
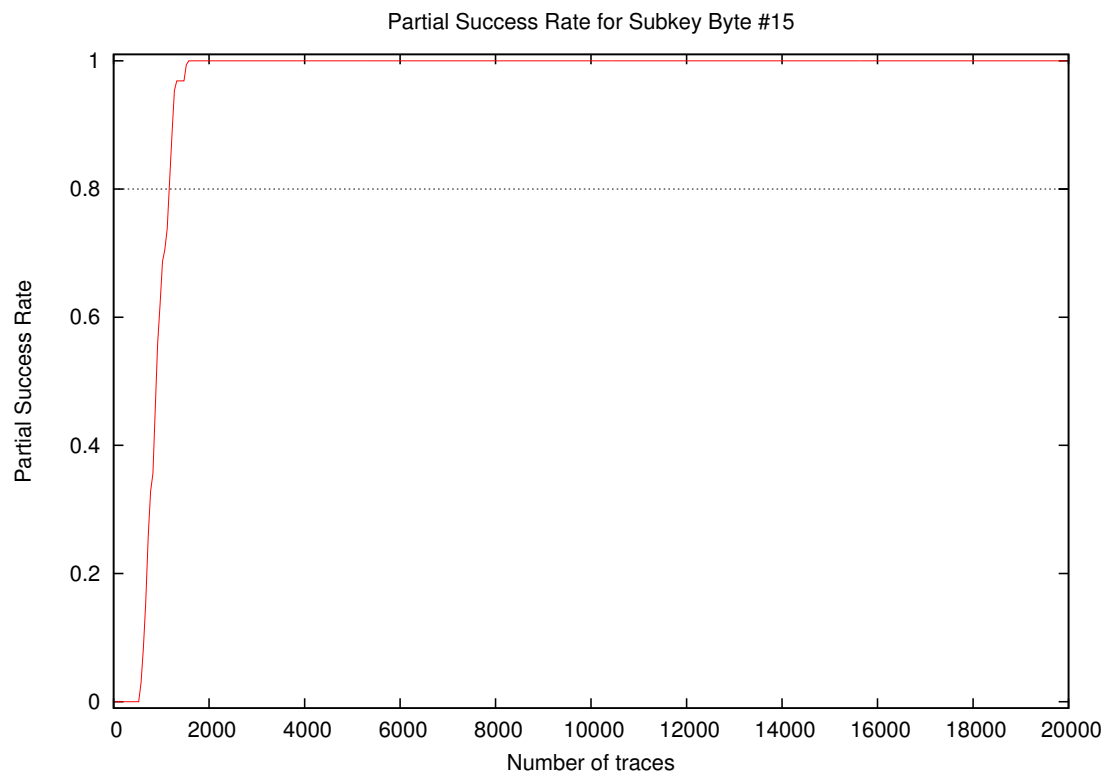
Partial Success Rate for Subkey Byte #11

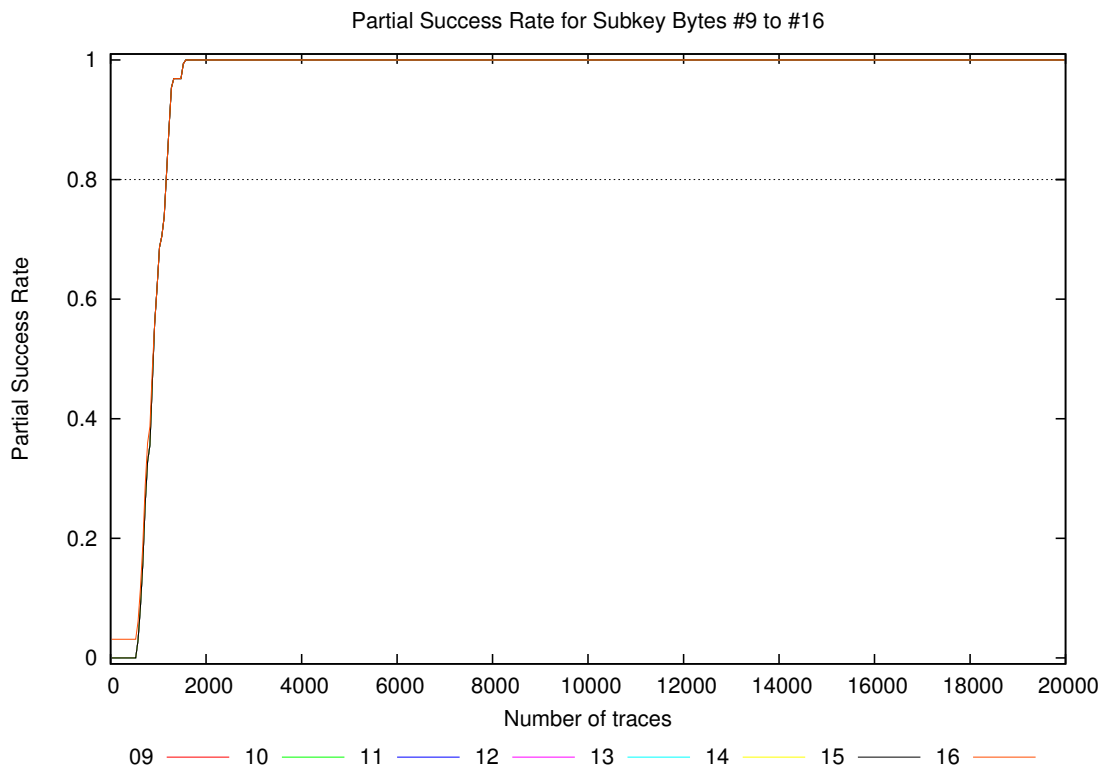
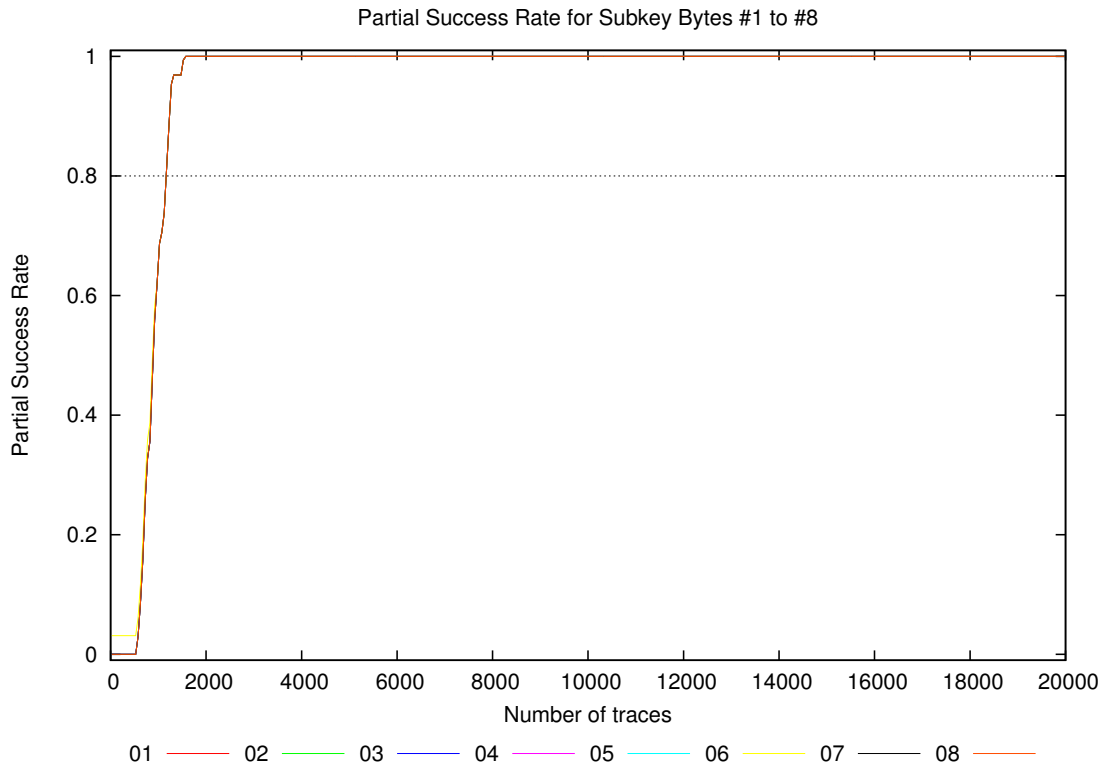


Partial Success Rate for Subkey Byte #12

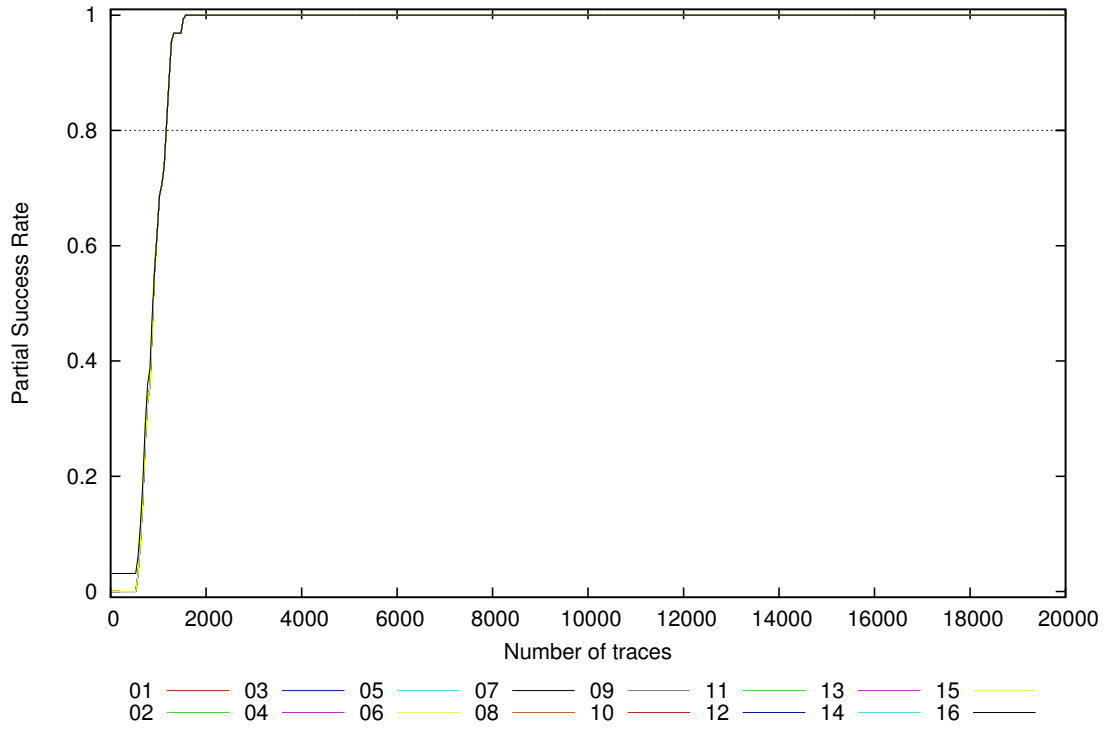






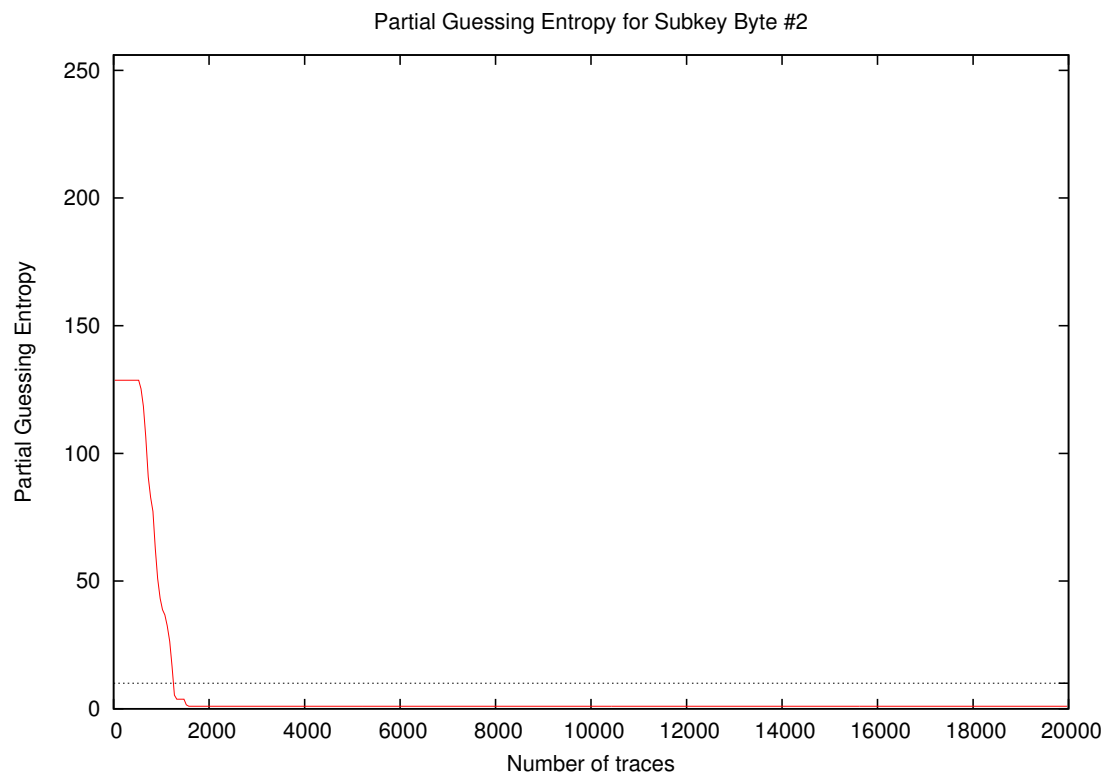
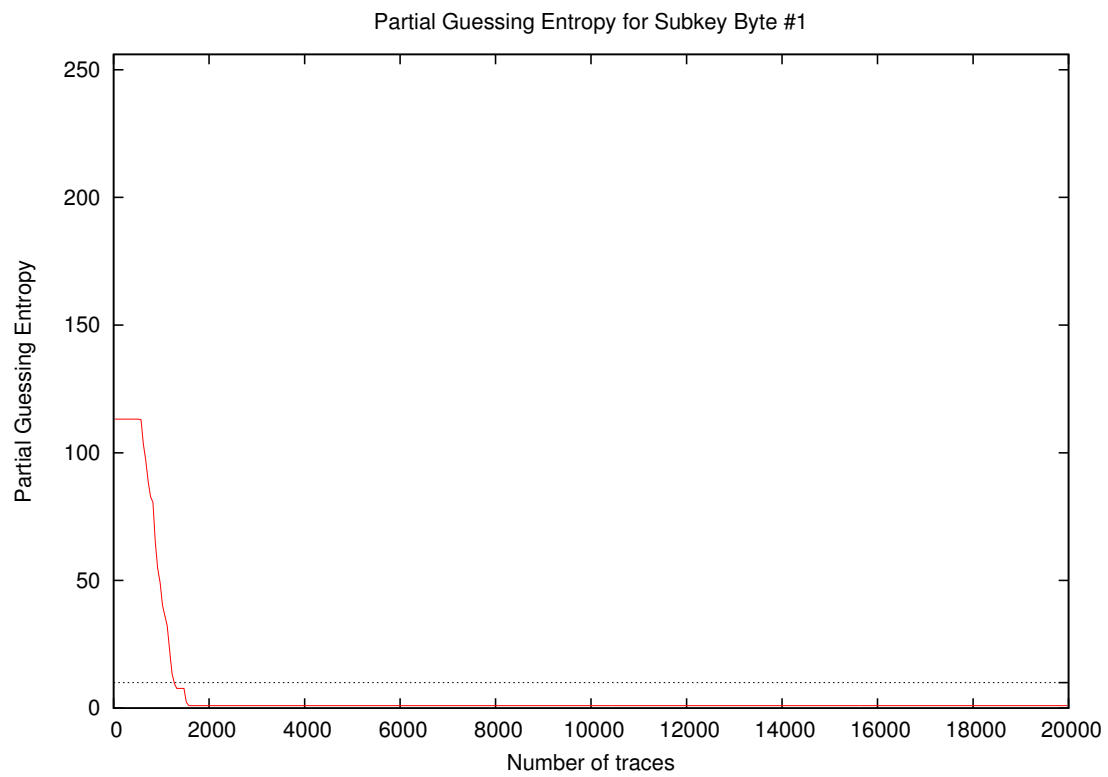


Partial Success Rate for Subkey Bytes #1 to #16

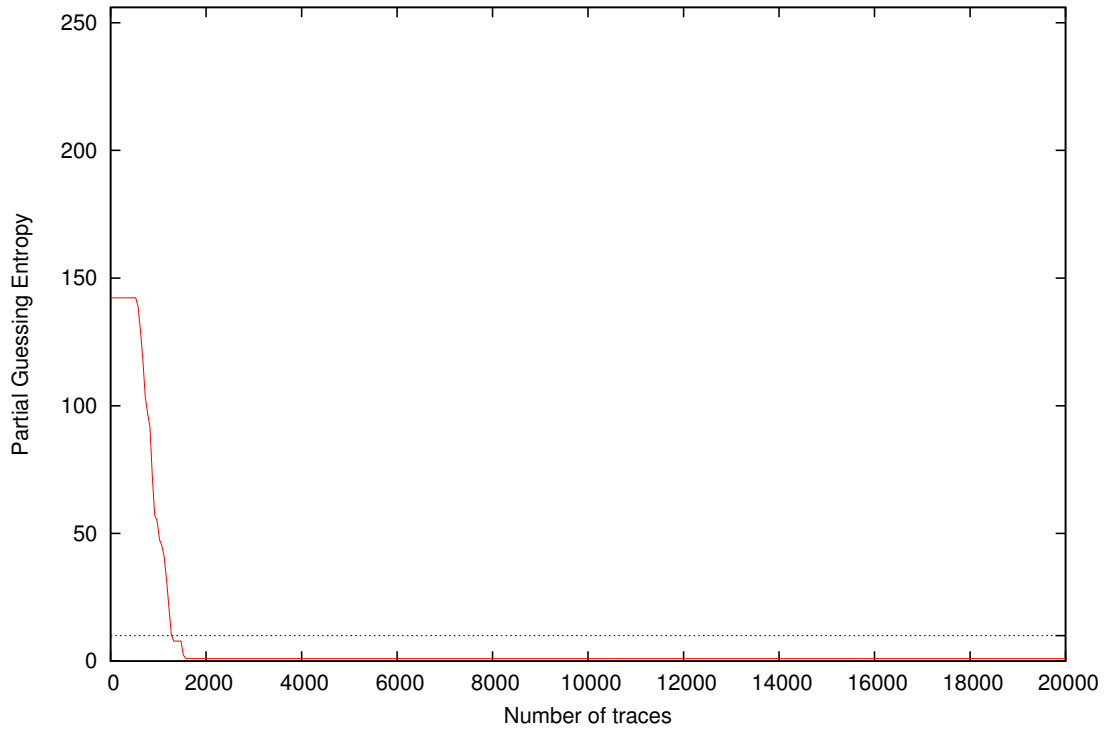


Traces	Partial Success Rate / Byte																Min	Max	Mean
	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16			
10	0.00	0.00	0.00	0.00	0.00	0.03	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.03	0.00	0.03	0.00
20	0.00	0.00	0.00	0.00	0.00	0.03	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.03	0.00	0.03	0.00
30	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	0.03	0.00
40	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	0.03	0.00
50	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	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	0.03	0.00	0.03	0.00
200	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	0.03	0.00
300	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	0.03	0.00
400	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	0.03	0.00
500	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	0.03	0.00
1000	0.66	0.66	0.66	0.66	0.66	0.66	0.66	0.66	0.66	0.66	0.66	0.66	0.66	0.66	0.66	0.66	0.66	0.66	0.66
2000	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
3000	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
4000	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
5000	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
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

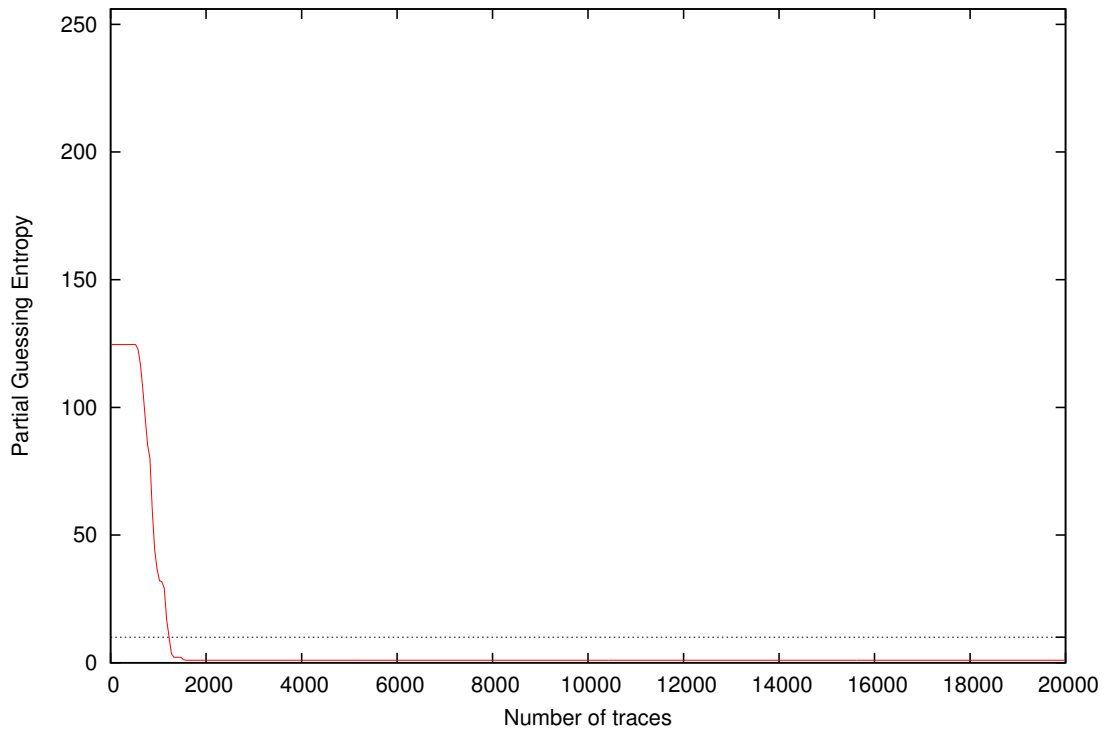
4 Partial Guessing Entropy



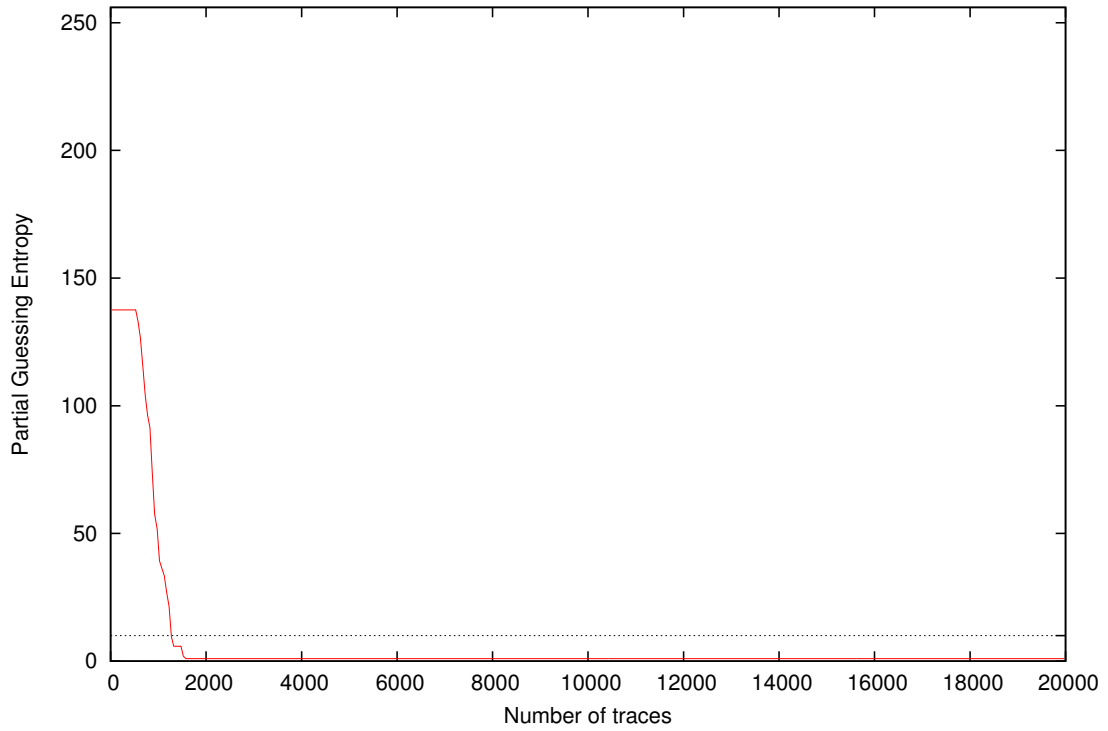
Partial Guessing Entropy for Subkey Byte #3



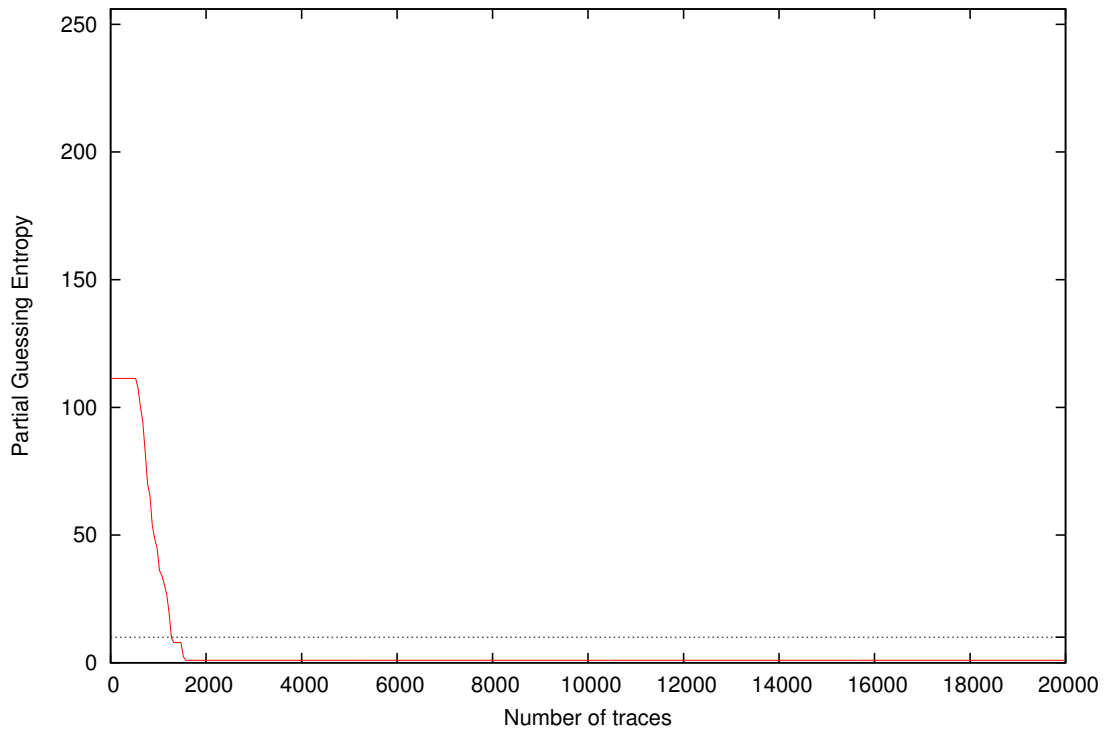
Partial Guessing Entropy for Subkey Byte #4



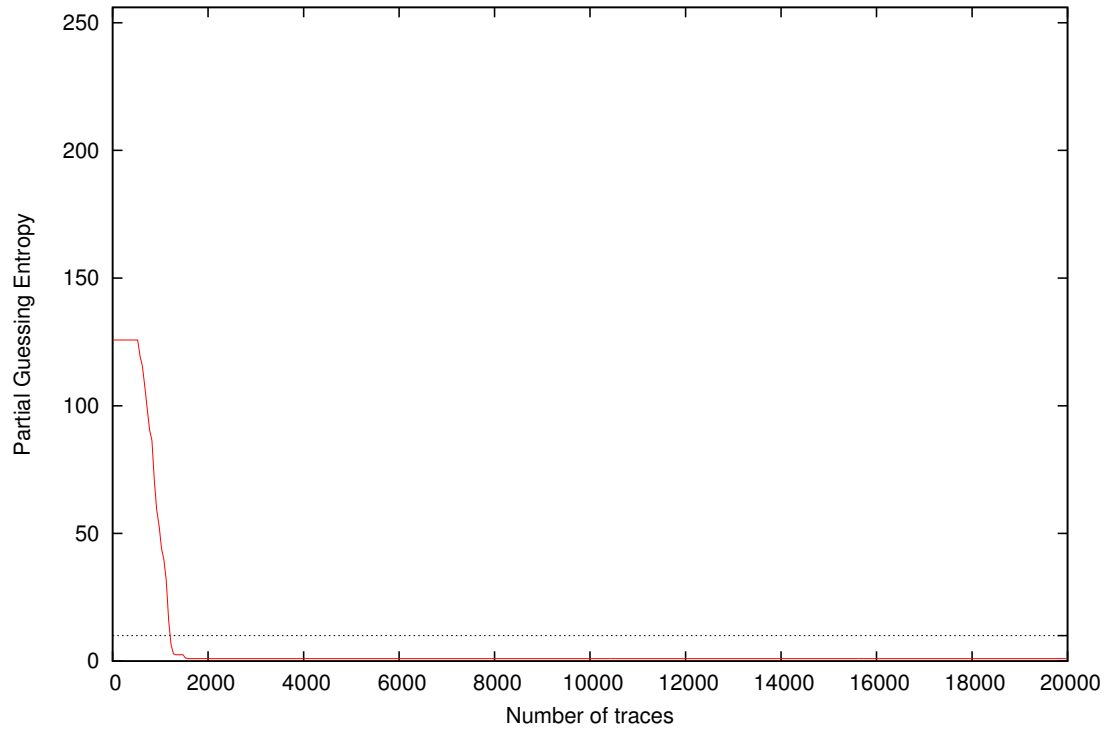
Partial Guessing Entropy for Subkey Byte #5



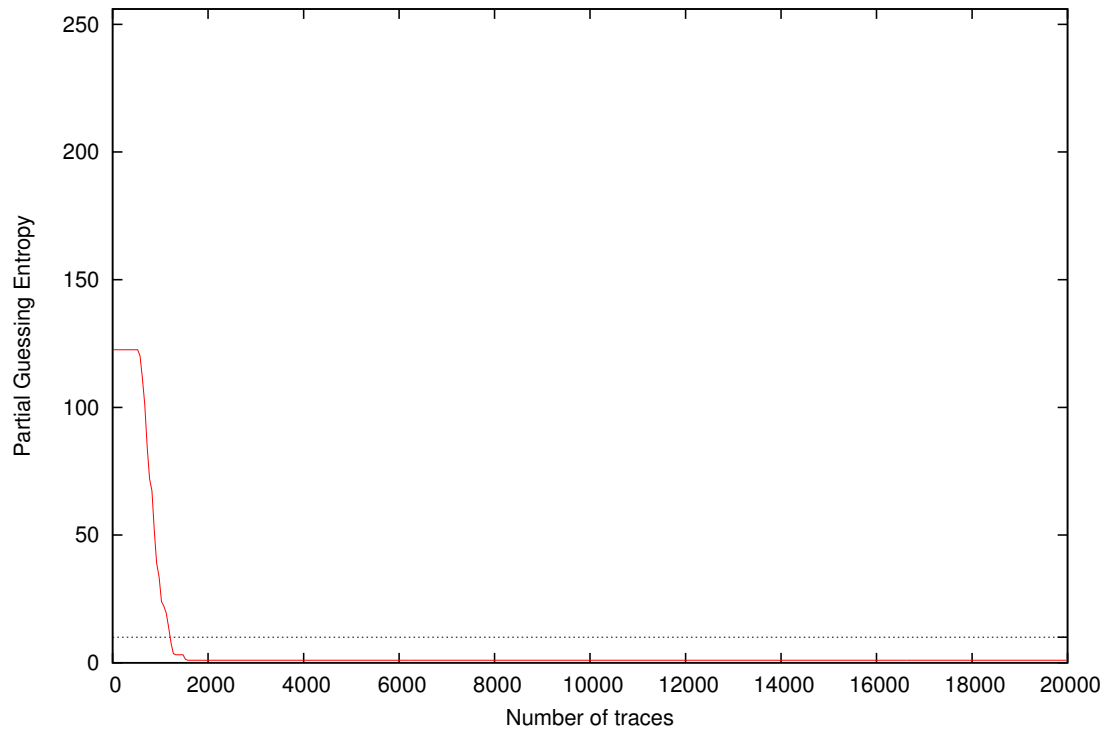
Partial Guessing Entropy for Subkey Byte #6



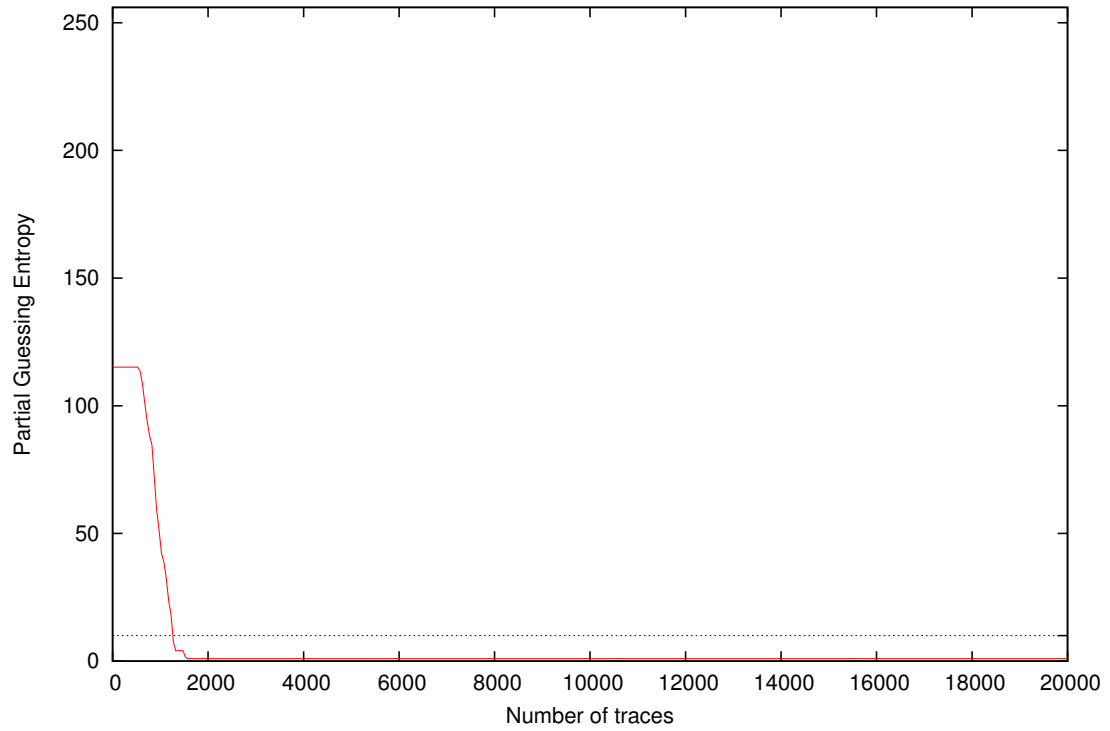
Partial Guessing Entropy for Subkey Byte #7



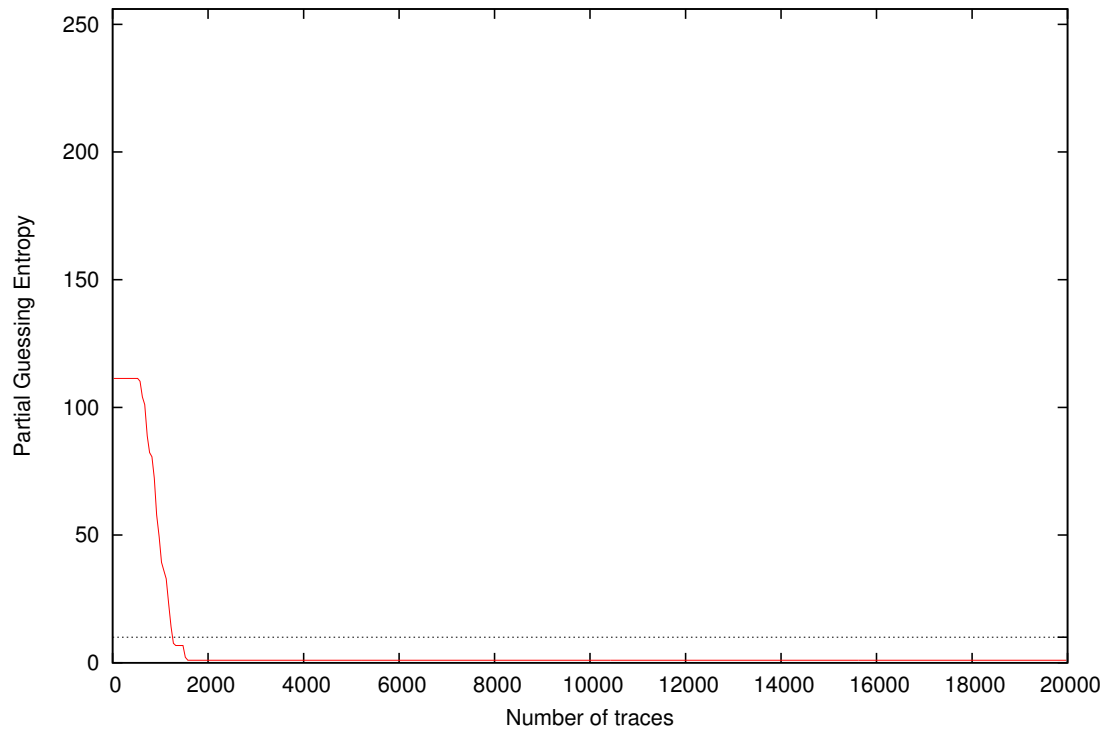
Partial Guessing Entropy for Subkey Byte #8



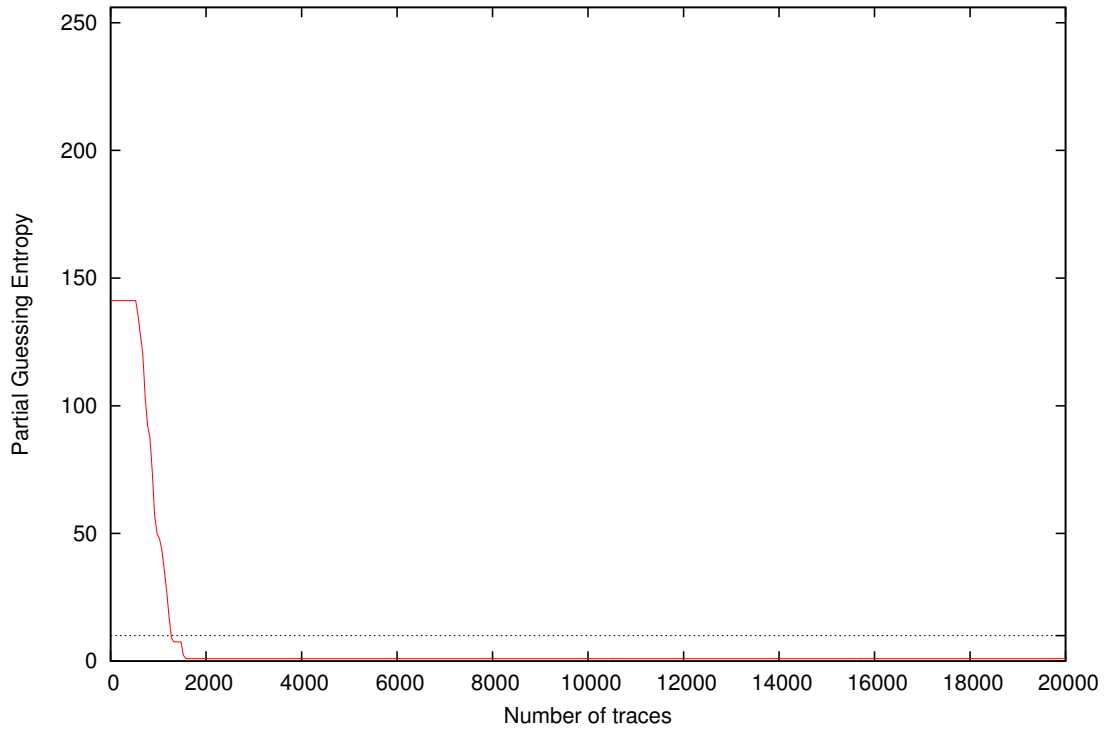
Partial Guessing Entropy for Subkey Byte #9



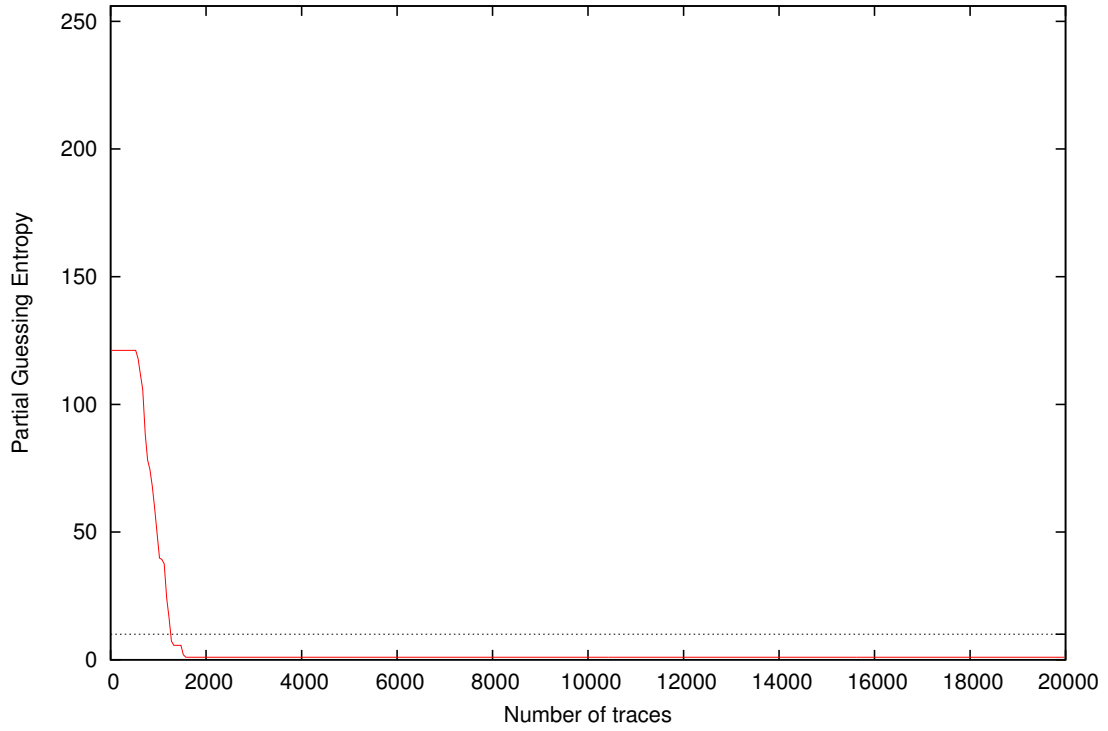
Partial Guessing Entropy for Subkey Byte #10



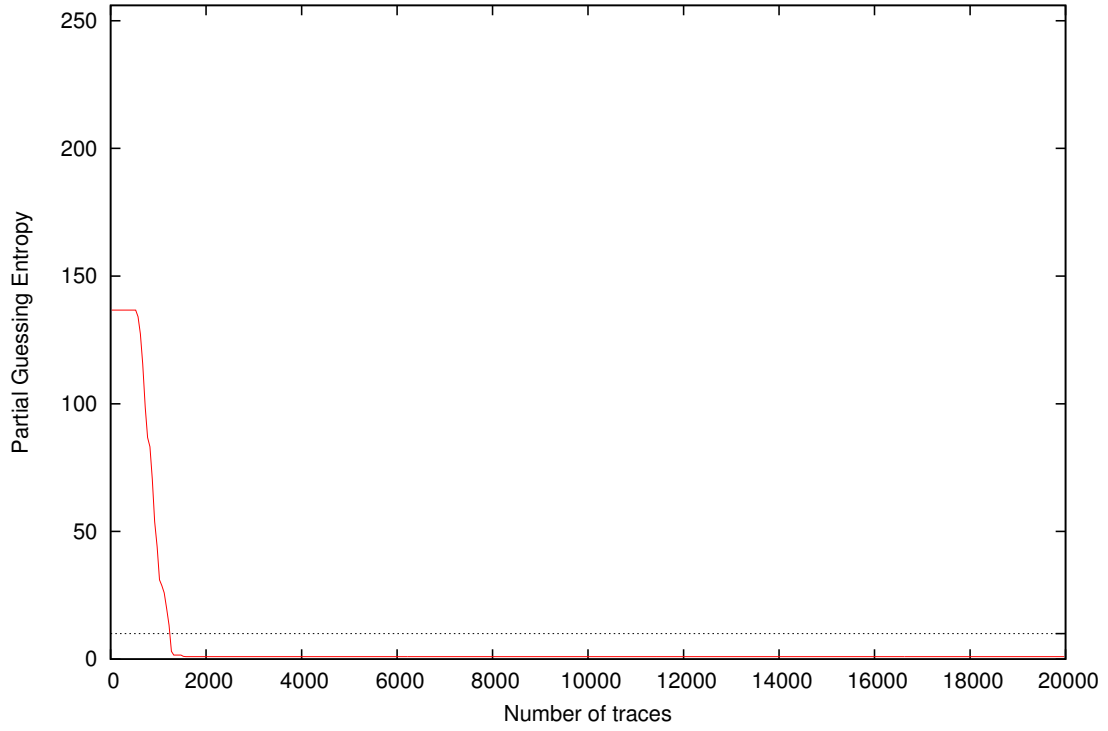
Partial Guessing Entropy for Subkey Byte #11



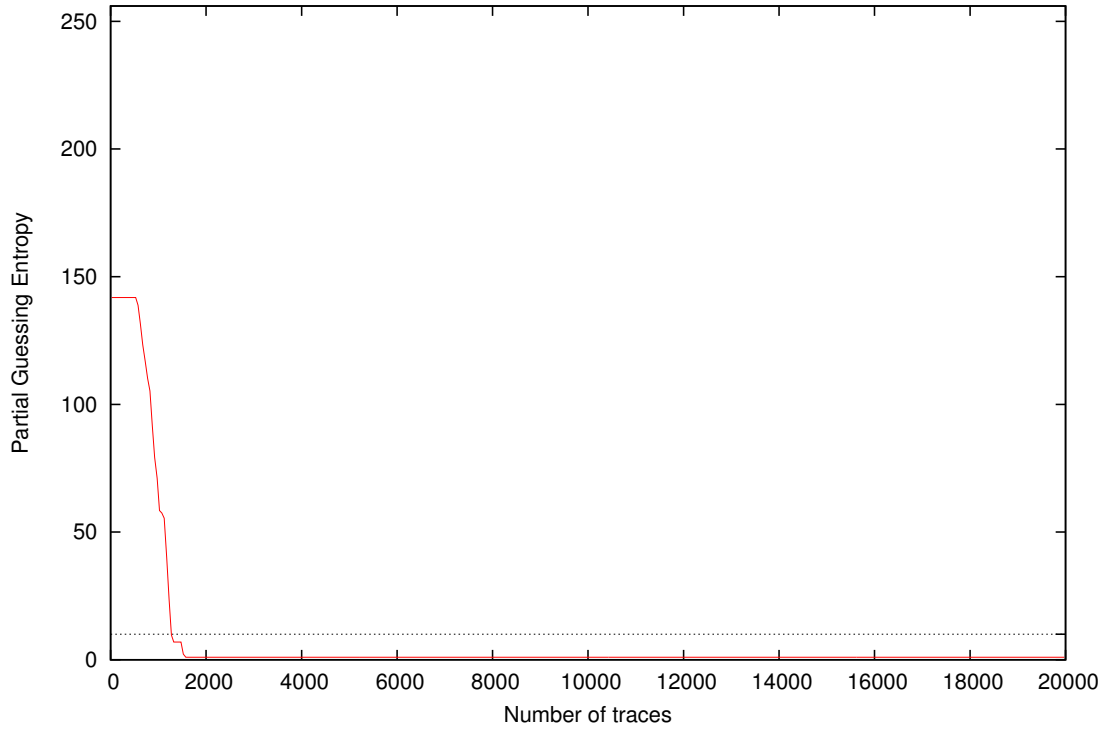
Partial Guessing Entropy for Subkey Byte #12



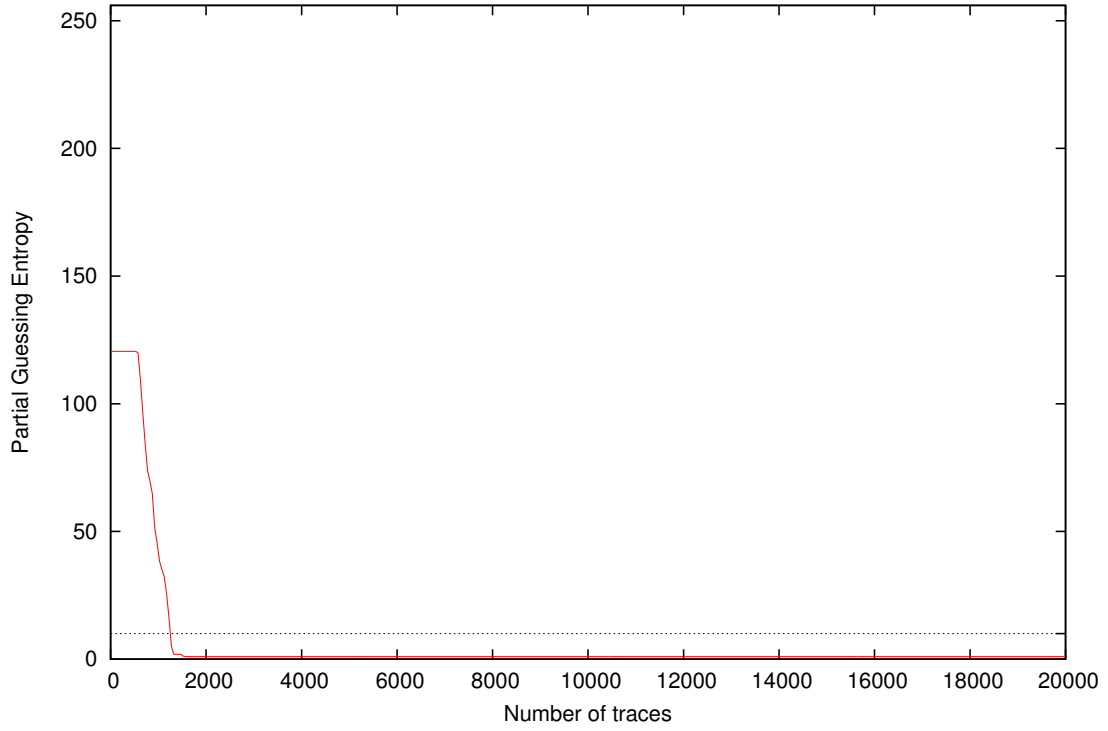
Partial Guessing Entropy for Subkey Byte #13



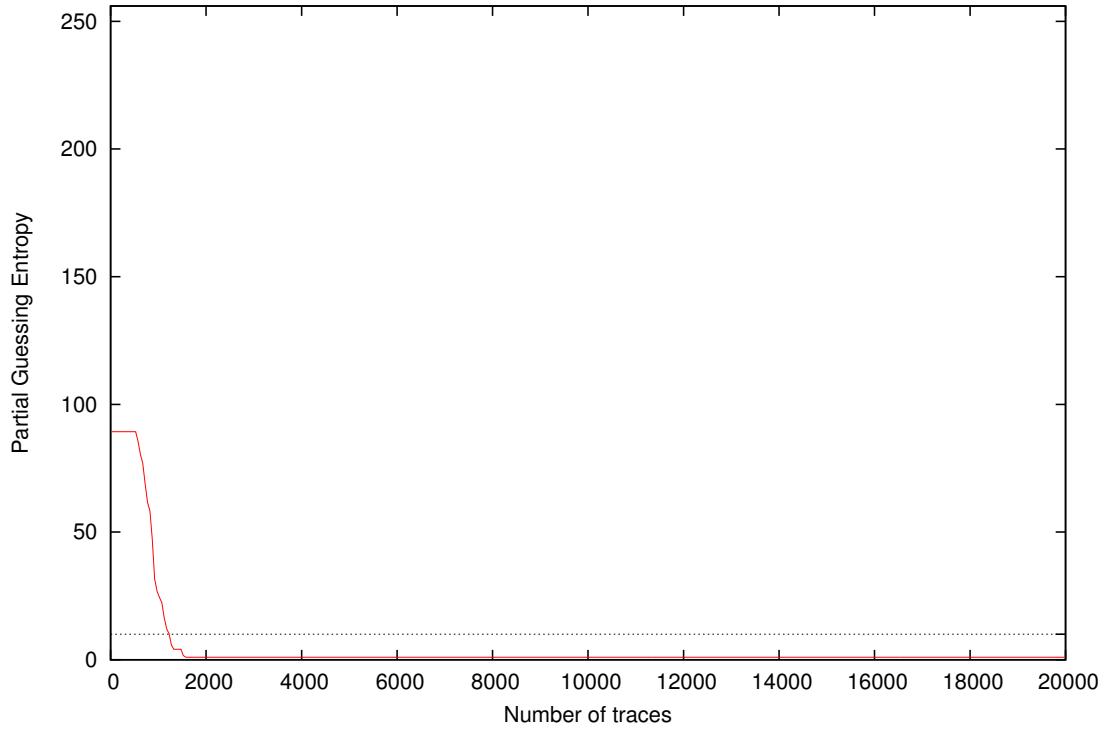
Partial Guessing Entropy for Subkey Byte #14



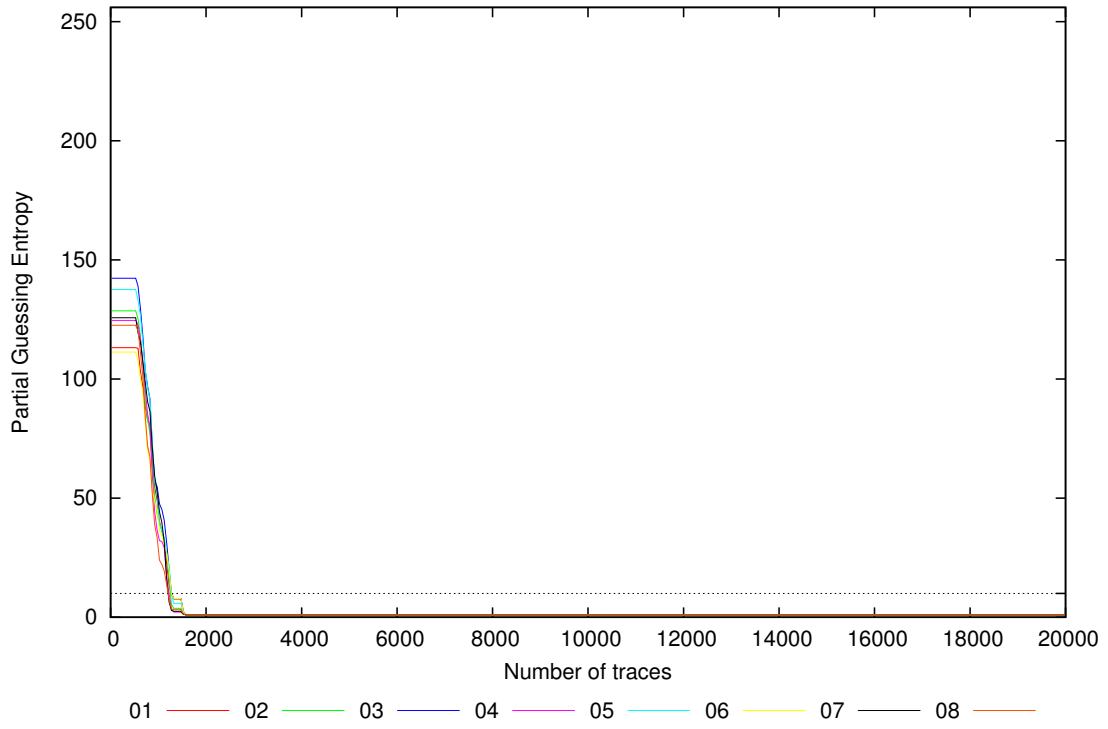
Partial Guessing Entropy for Subkey Byte #15



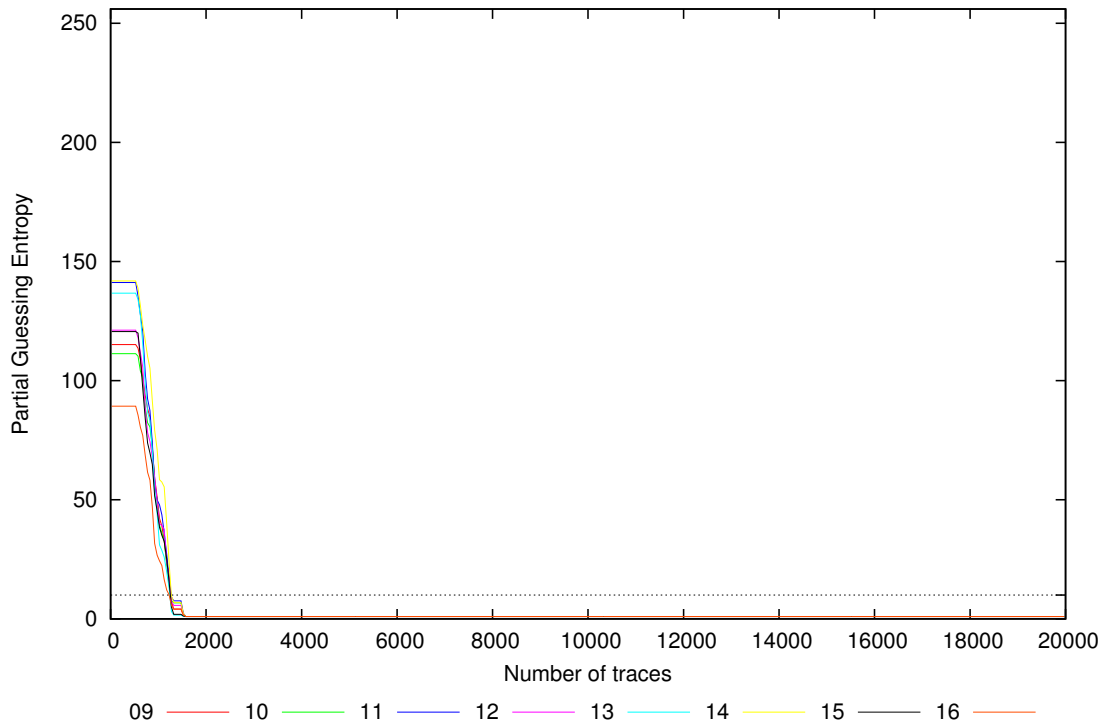
Partial Guessing Entropy for Subkey Byte #16



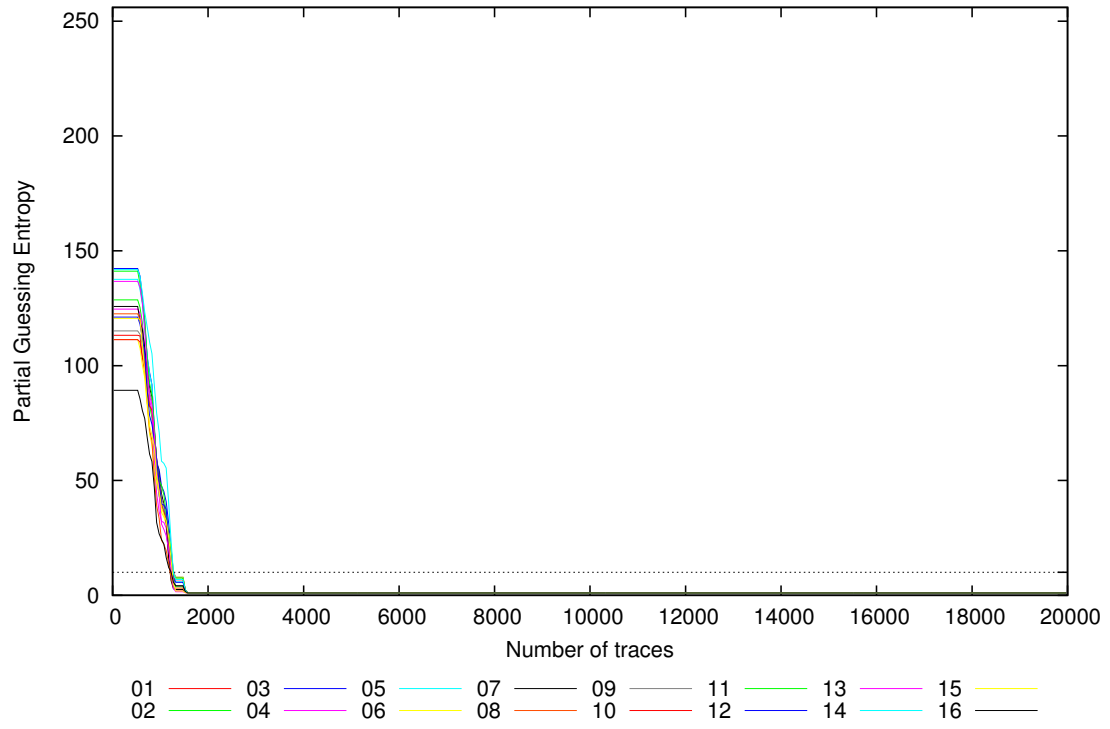
Partial Guessing Entropy for Subkey Bytes #1 to #8



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	113.2	128.6	142.3	124.6	137.6	111.3	125.8	122.6	115.2	111.3	141.2	121.2	136.7	141.8	120.6	89.3	89.3	142.3	123.9
20	113.2	128.6	142.3	124.6	137.6	111.3	125.8	122.6	115.2	111.3	141.2	121.2	136.7	141.8	120.6	89.3	89.3	142.3	123.9
30	113.2	128.6	142.3	124.6	137.6	111.3	125.8	122.6	115.2	111.3	141.2	121.2	136.7	141.8	120.6	89.3	89.3	142.3	123.9
40	113.2	128.6	142.3	124.6	137.6	111.3	125.8	122.6	115.2	111.3	141.2	121.2	136.7	141.8	120.6	89.3	89.3	142.3	123.9
50	113.2	128.6	142.3	124.6	137.6	111.3	125.8	122.6	115.2	111.3	141.2	121.2	136.7	141.8	120.6	89.3	89.3	142.3	123.9
100	113.2	128.6	142.3	124.6	137.6	111.3	125.8	122.6	115.2	111.3	141.2	121.2	136.7	141.8	120.6	89.3	89.3	142.3	123.9
200	113.2	128.6	142.3	124.6	137.6	111.3	125.8	122.6	115.2	111.3	141.2	121.2	136.7	141.8	120.6	89.3	89.3	142.3	123.9
300	113.2	128.6	142.3	124.6	137.6	111.3	125.8	122.6	115.2	111.3	141.2	121.2	136.7	141.8	120.6	89.3	89.3	142.3	123.9
400	113.2	128.6	142.3	124.6	137.6	111.3	125.8	122.6	115.2	111.3	141.2	121.2	136.7	141.8	120.6	89.3	89.3	142.3	123.9
500	113.2	128.6	142.3	124.6	137.6	111.3	125.8	122.6	115.2	111.3	141.2	121.2	136.7	141.8	120.6	89.3	89.3	142.3	123.9
1000	47.3	41.5	54.5	33.0	46.9	40.3	46.3	28.3	47.8	41.1	48.3	44.8	37.8	64.6	41.2	25.1	25.1	64.6	43.1
2000	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
3000	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
4000	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
5000	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
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