

DPA Contest v4.2

Evaluation results

Li Yang, Wang Weiqi, Zhang Chi

March 2015

1 Introduction

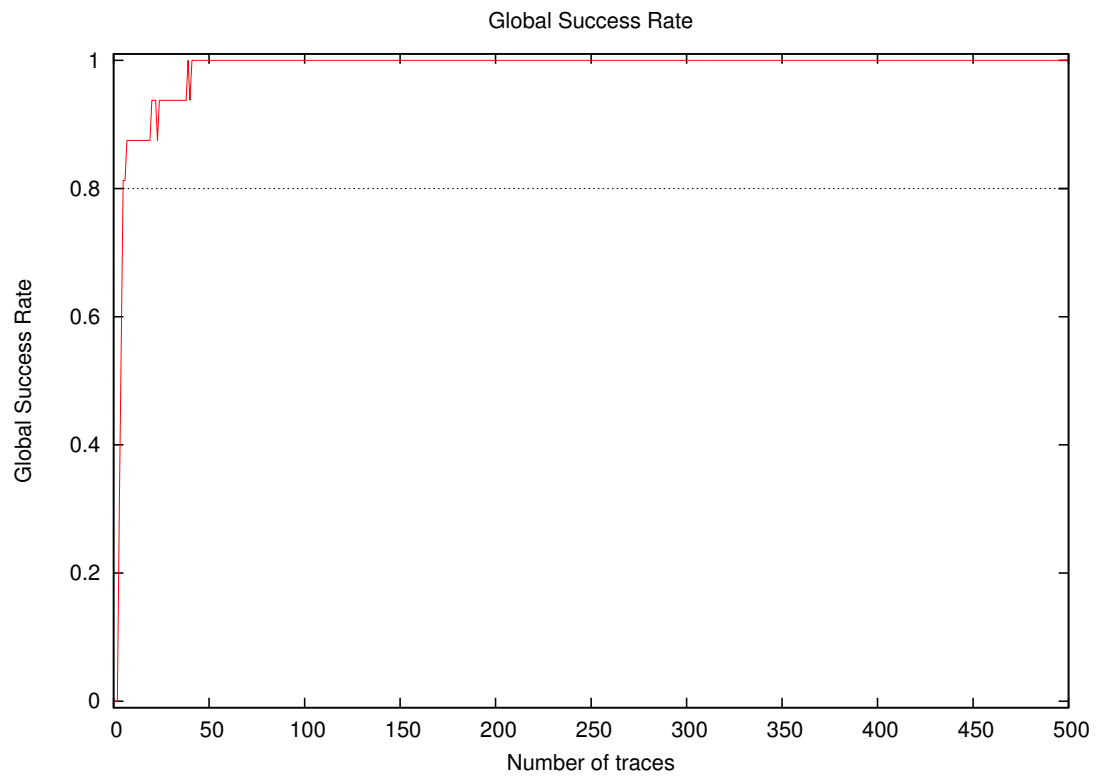
1.1 About the attack

- **Sender/Team:** Li Yang, Wang Weiqi, Zhang Chi
- **Institution:** Shanghai Fudan Microelectronics Group Company Limited, China
- **Language:** Matlab
- **Operating system:** Windows
- **Attacked subkey:** 0

1.2 About the evaluation

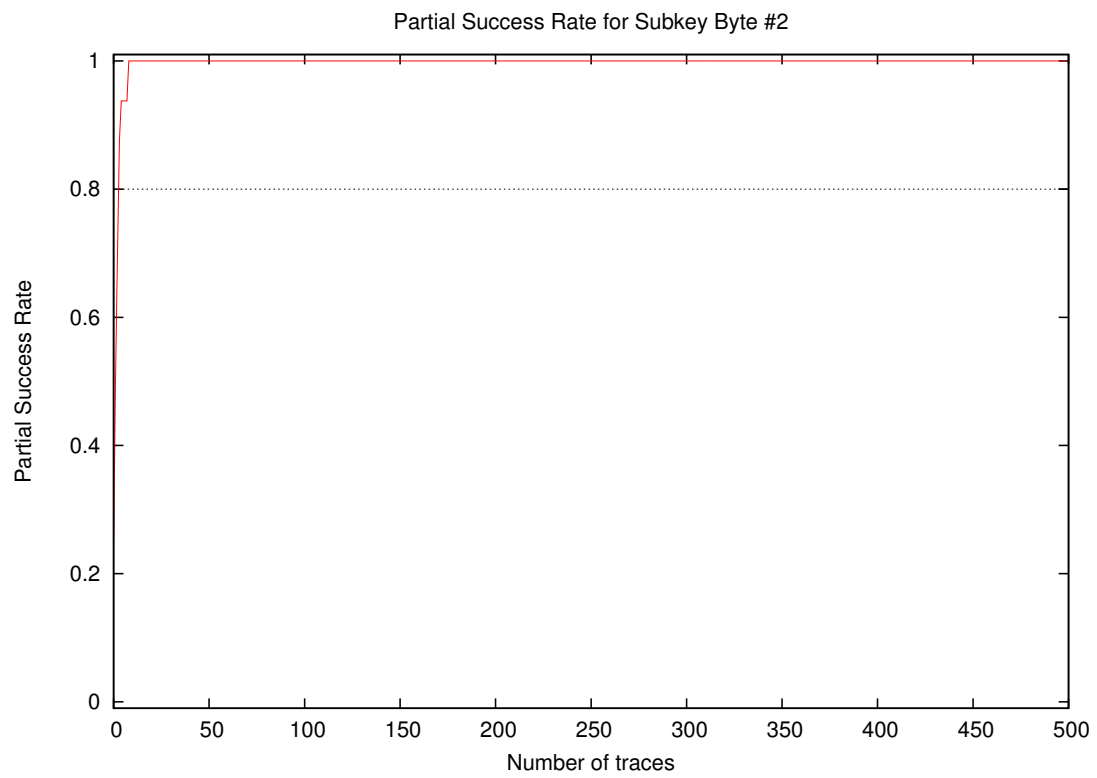
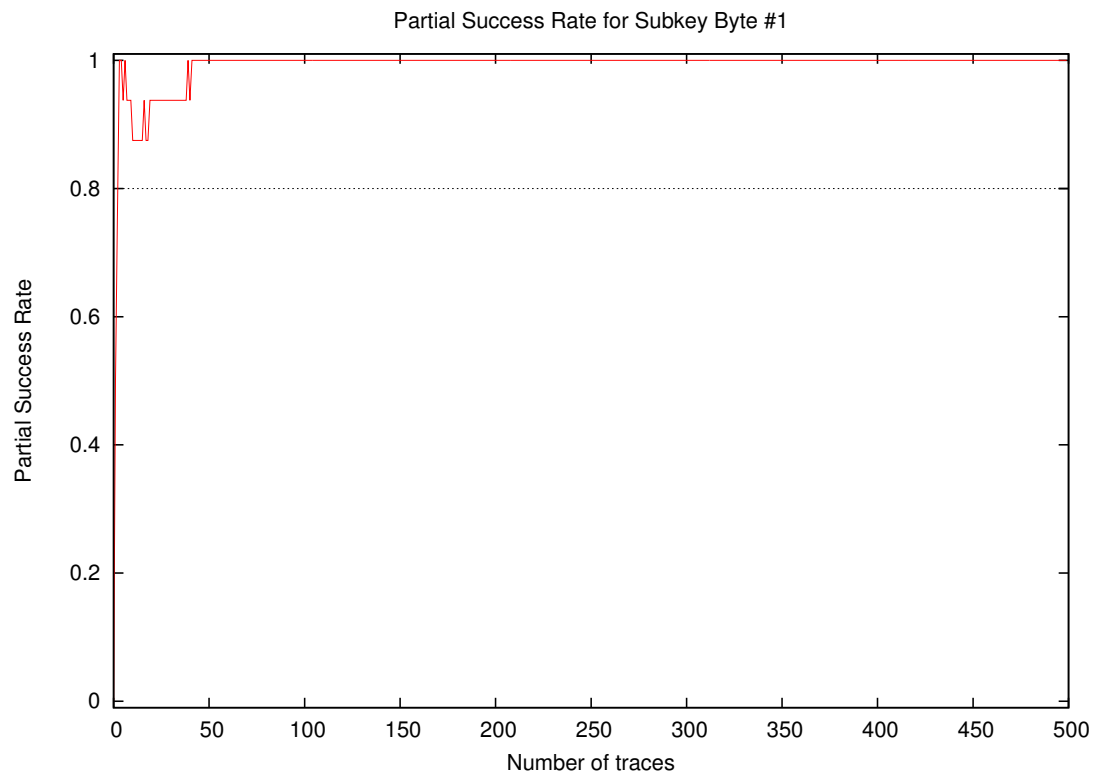
- **Date of evaluation:** September 2015

2 Global Success Rate

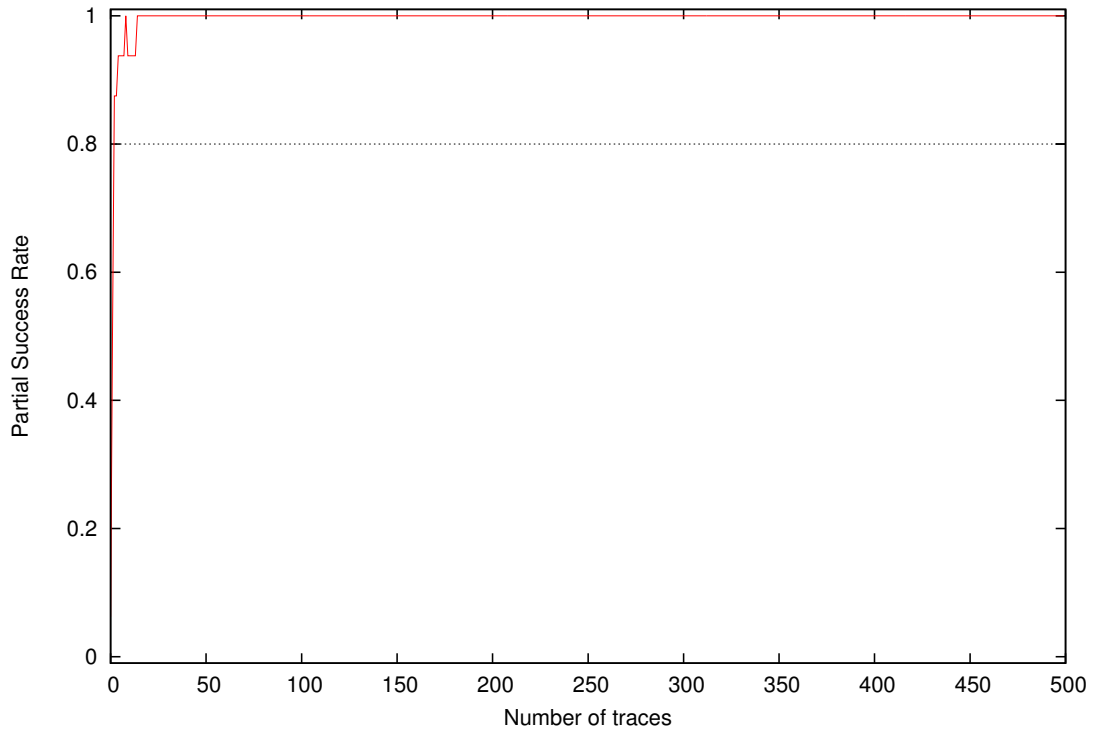


Number of traces	Global Success Rate
10	0.88
20	0.88
30	0.94
40	1.00
50	1.00
100	1.00
200	1.00
300	1.00
400	1.00
500	1.00

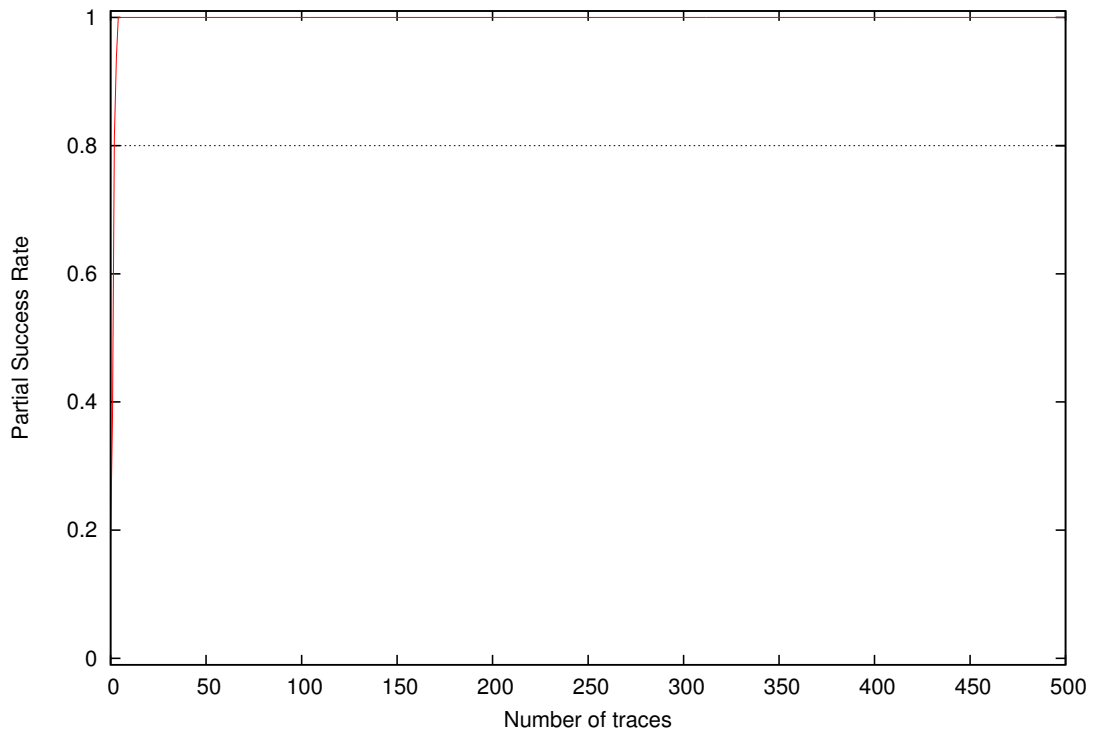
3 Partial Success Rate



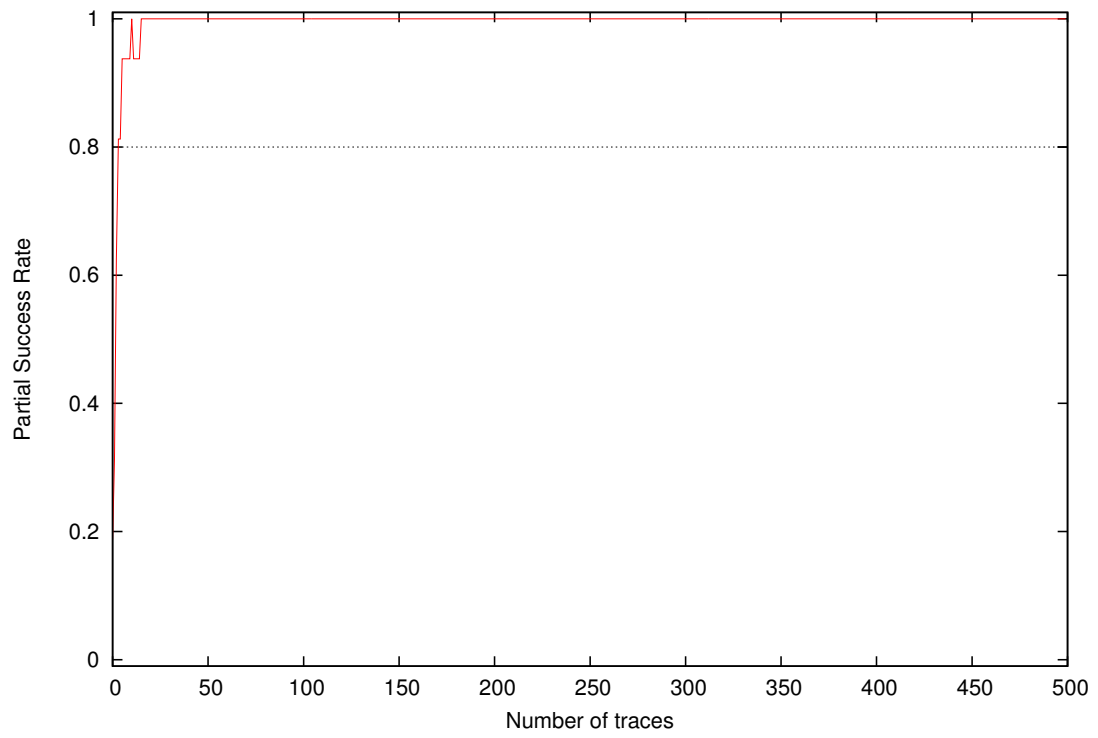
Partial Success Rate for Subkey Byte #3



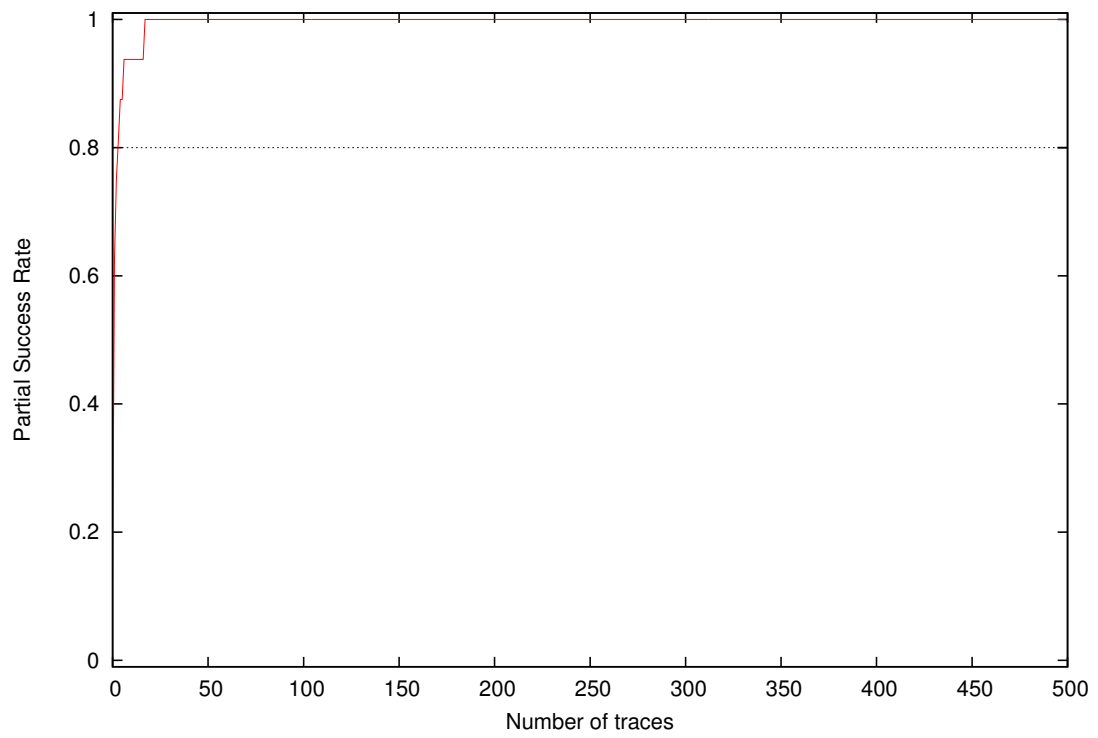
Partial Success Rate for Subkey Byte #4



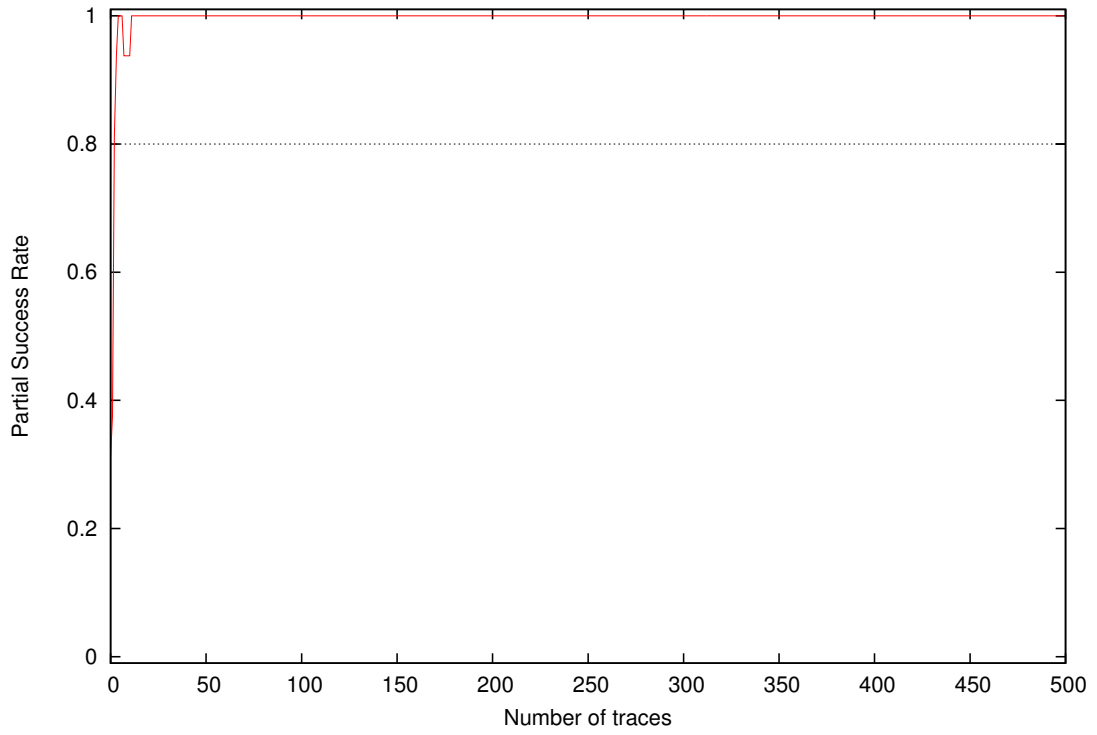
Partial Success Rate for Subkey Byte #5



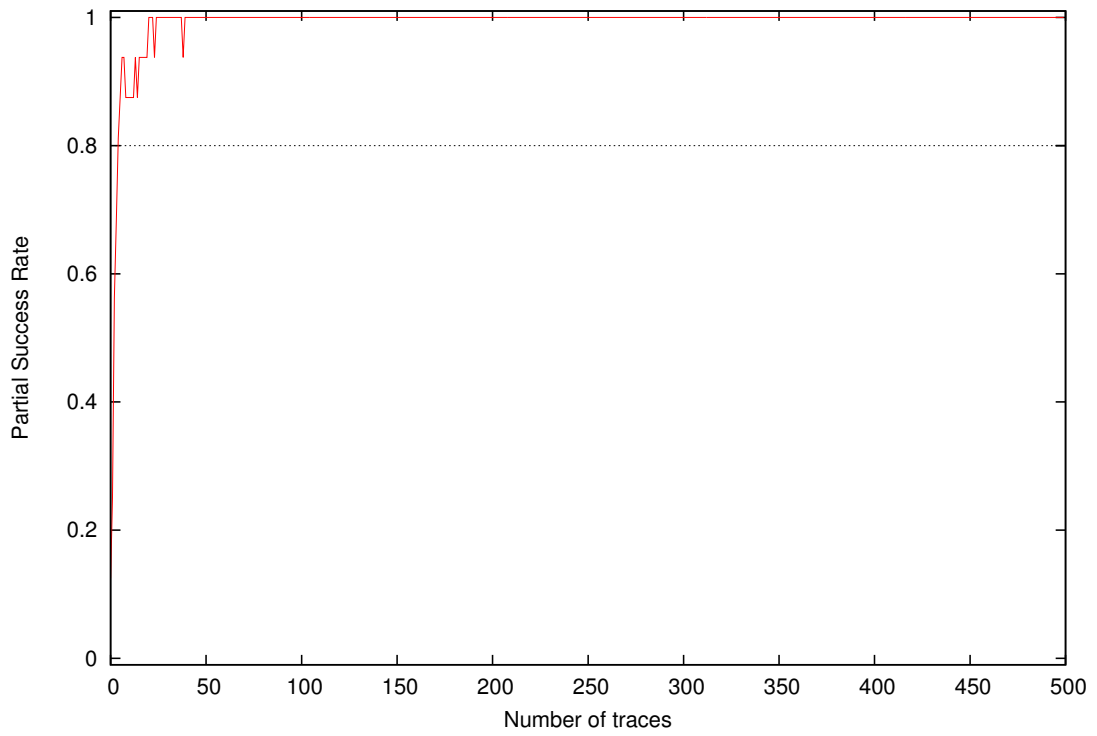
Partial Success Rate for Subkey Byte #6



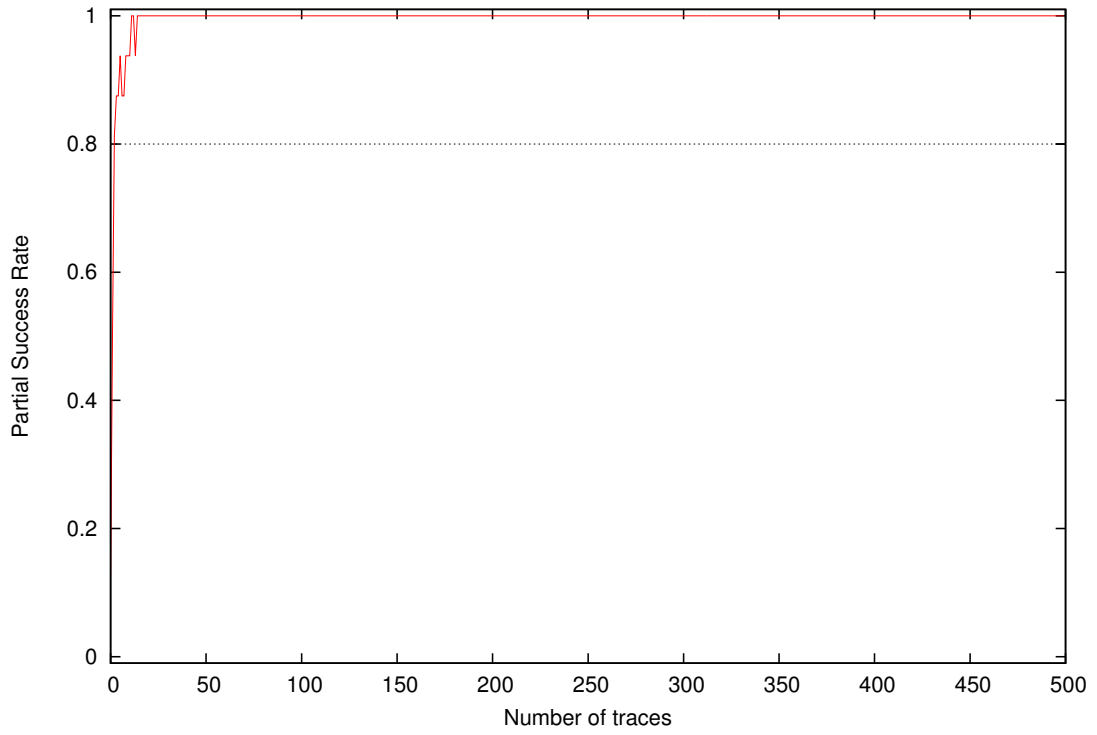
Partial Success Rate for Subkey Byte #7



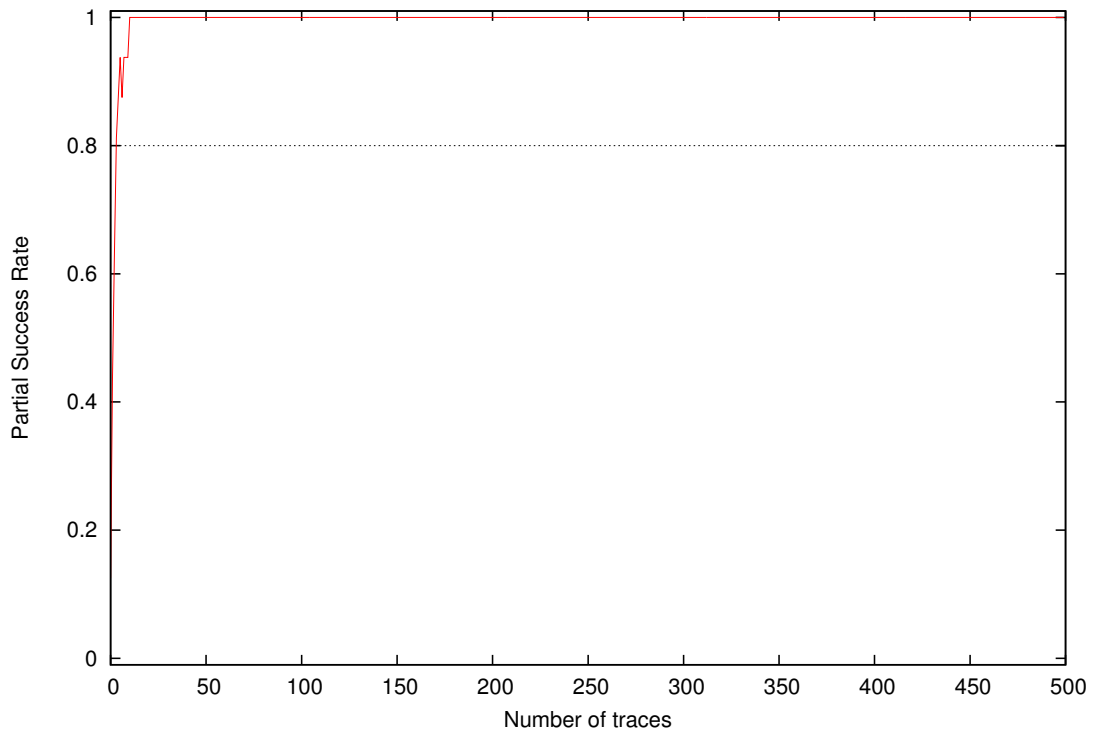
Partial Success Rate for Subkey Byte #8



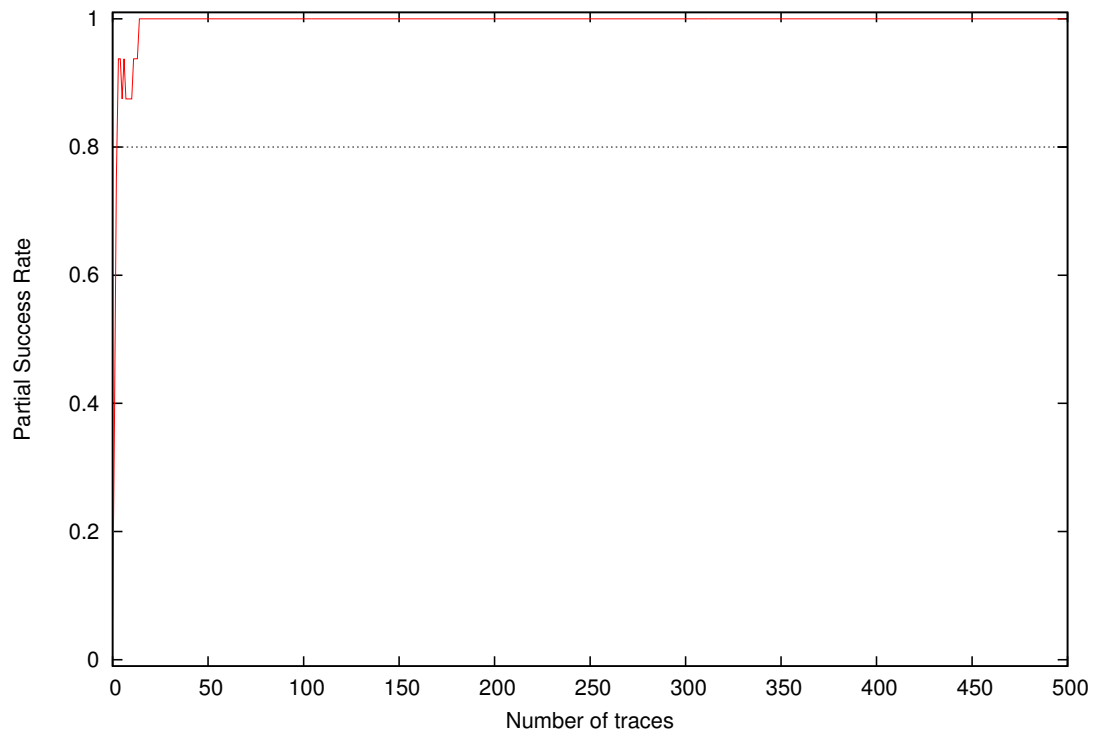
Partial Success Rate for Subkey Byte #9



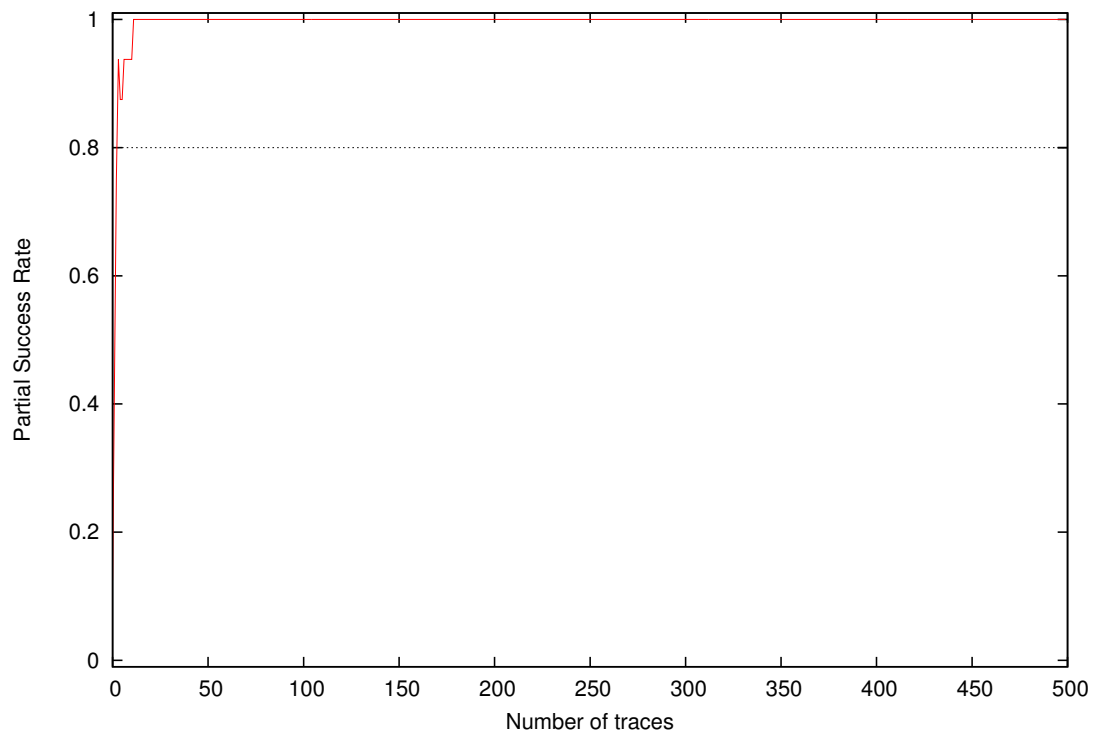
Partial Success Rate for Subkey Byte #10



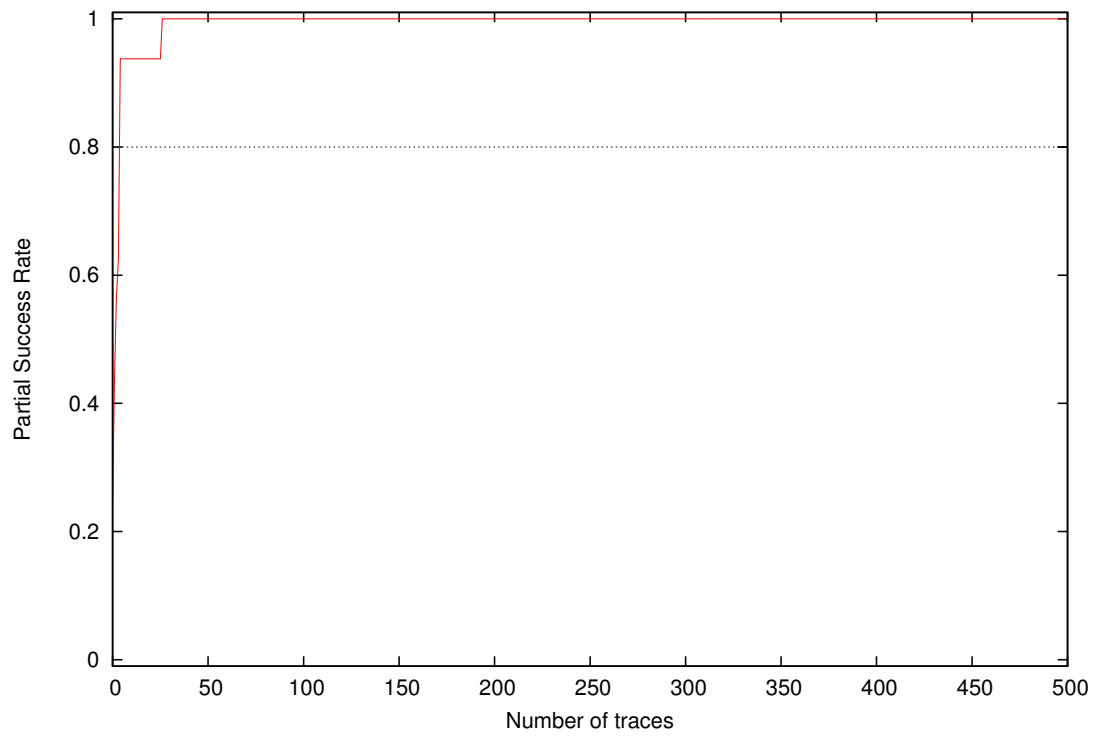
Partial Success Rate for Subkey Byte #11



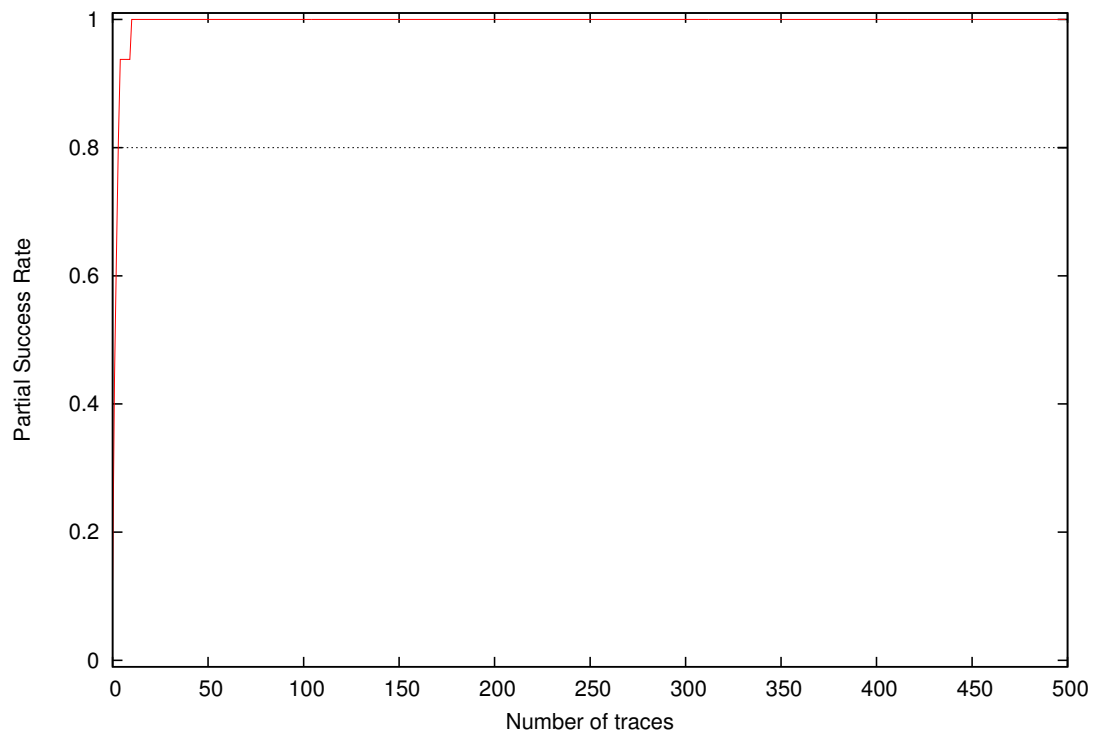
Partial Success Rate for Subkey Byte #12

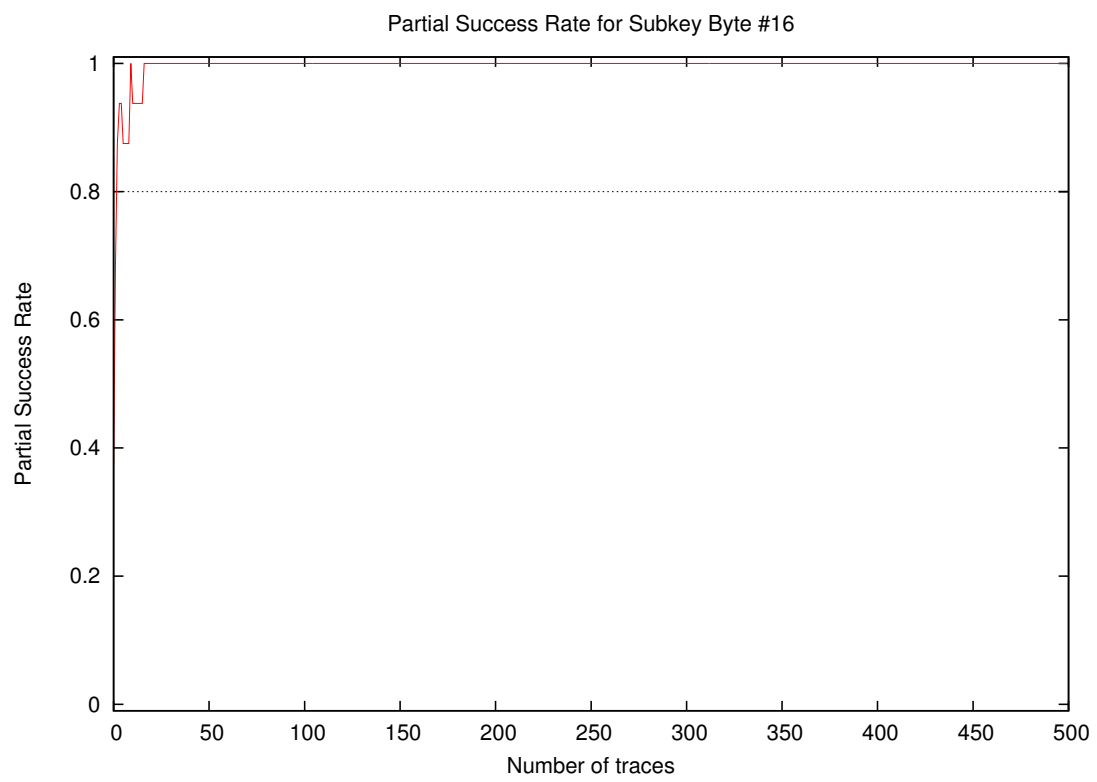
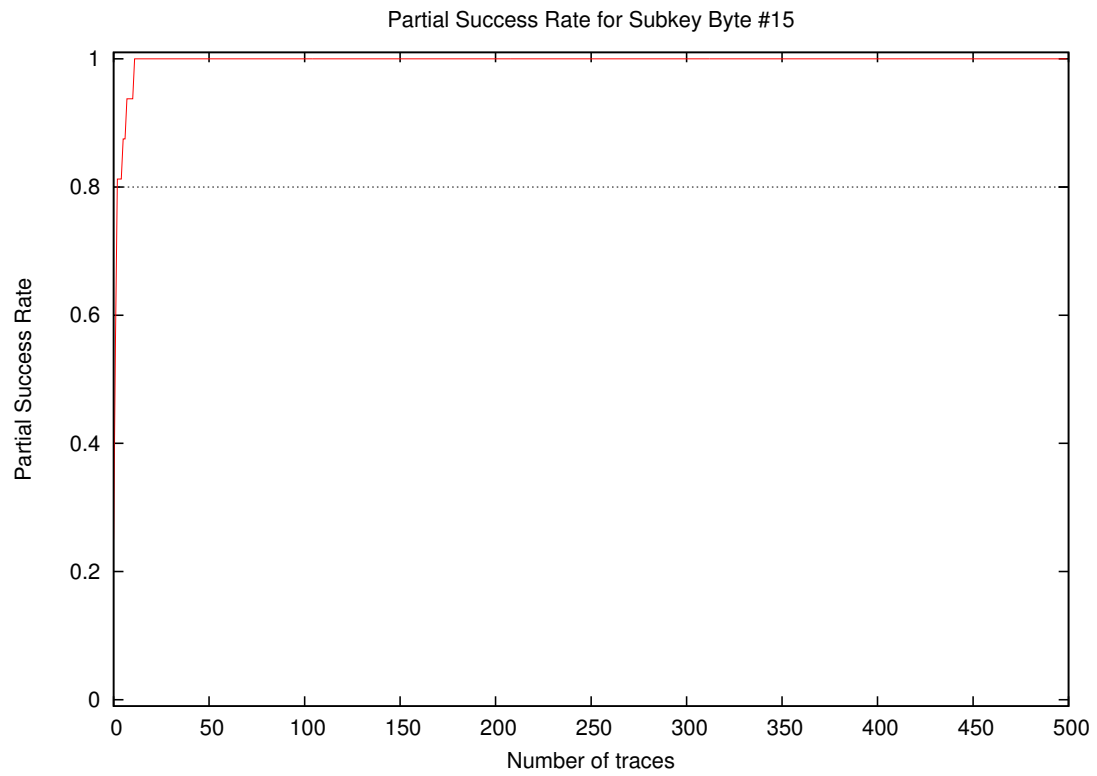


Partial Success Rate for Subkey Byte #13

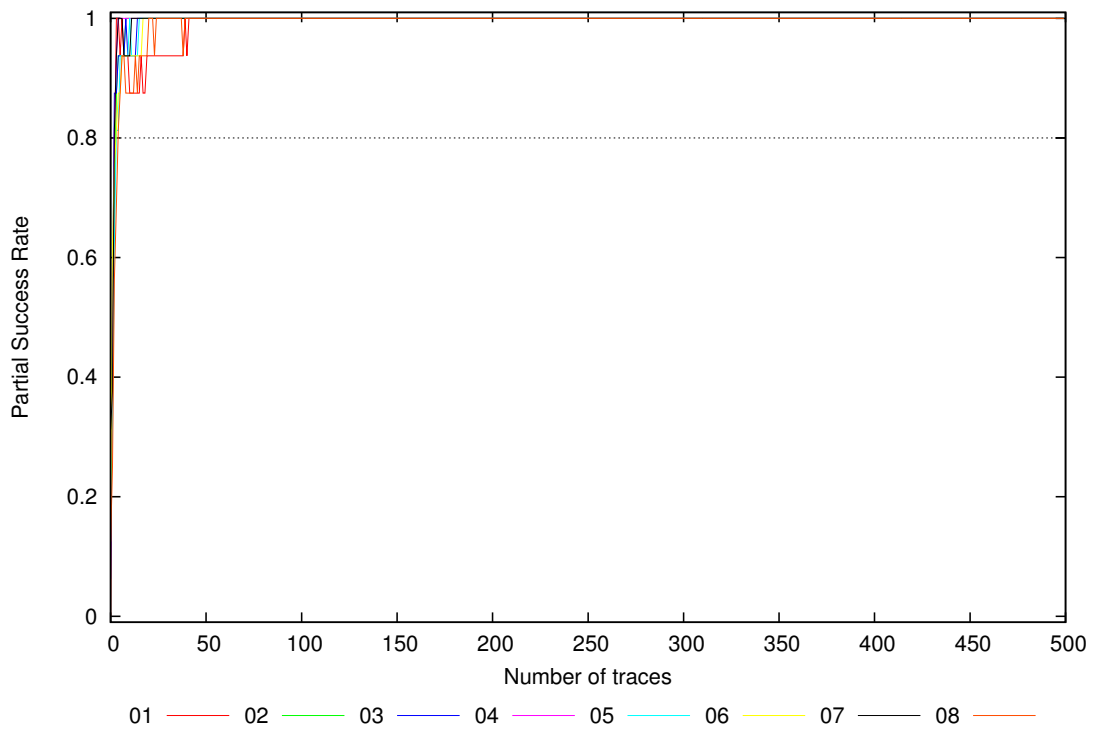


Partial Success Rate for Subkey Byte #14

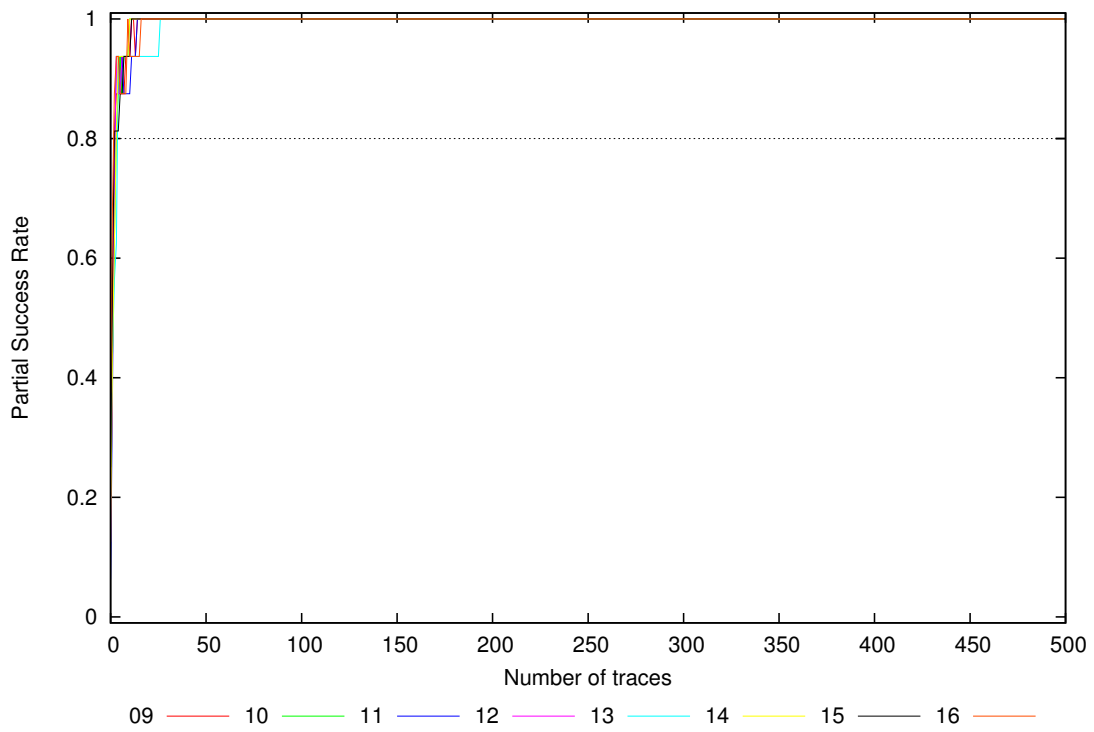




Partial Success Rate for Subkey Bytes #1 to #8

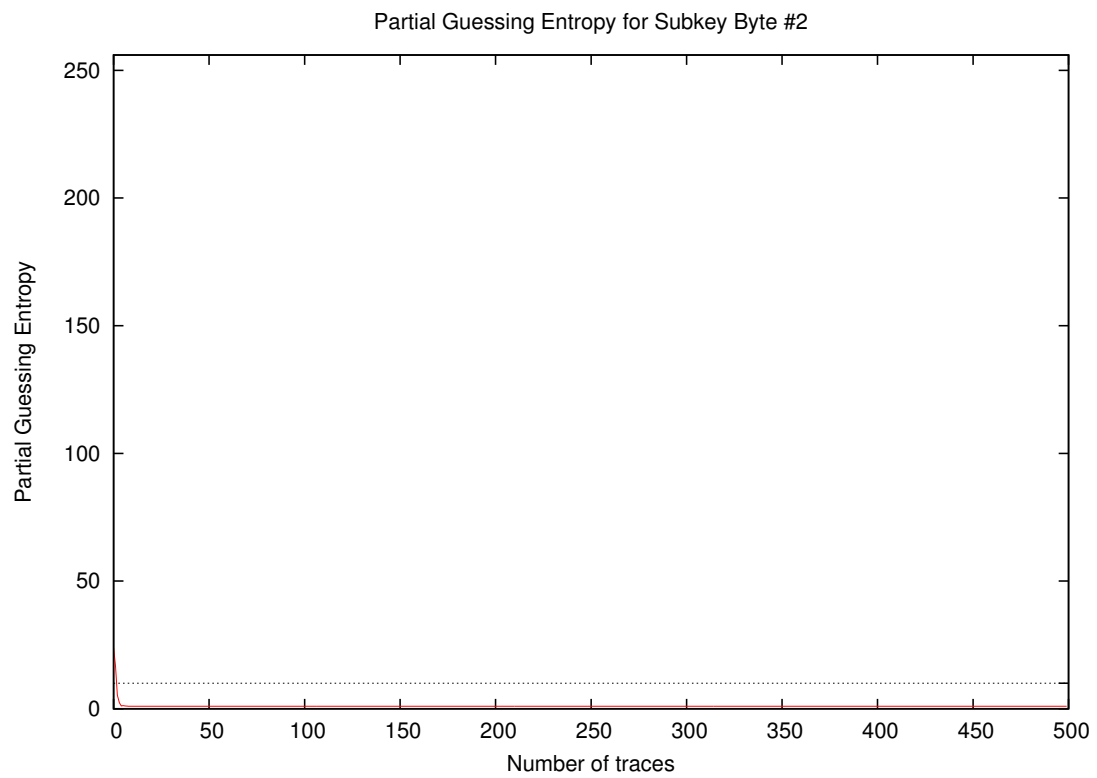
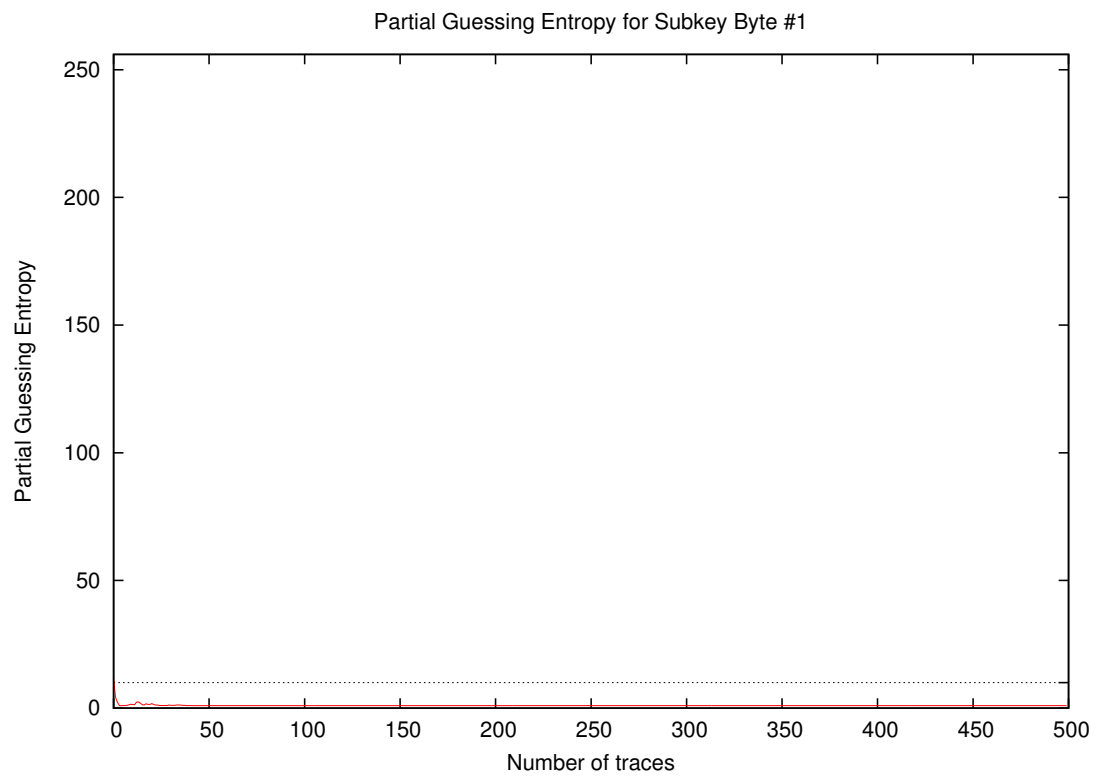


Partial Success Rate for Subkey Bytes #9 to #16

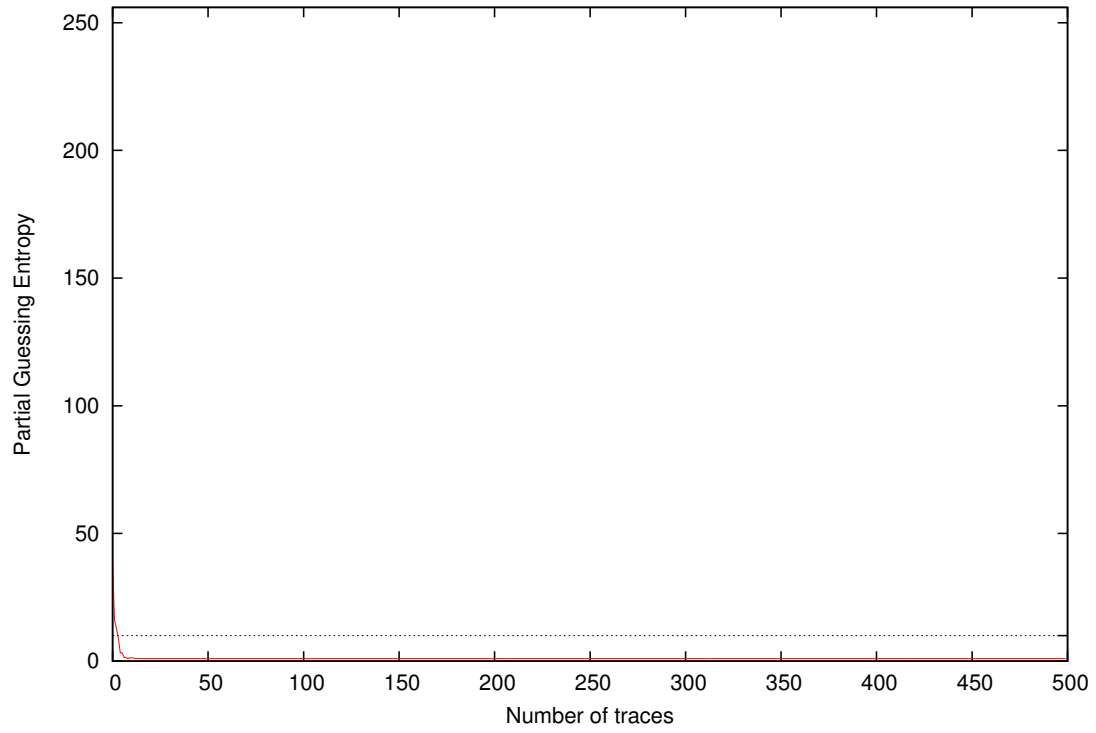


Traces	Partial Success Rate / Byte																Min	Max	Mean
	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16			
10	0.94	1.00	0.94	1.00	0.94	0.94	0.88	0.94	0.94	0.88	0.94	0.94	0.94	0.94	0.94	1.00	0.88	1.00	0.94
20	0.94	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	0.94	1.00	1.00	1.00	0.94	1.00	0.99
30	0.94	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	0.94	1.00	1.00
40	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
50	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
100	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
200	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
300	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
400	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
500	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

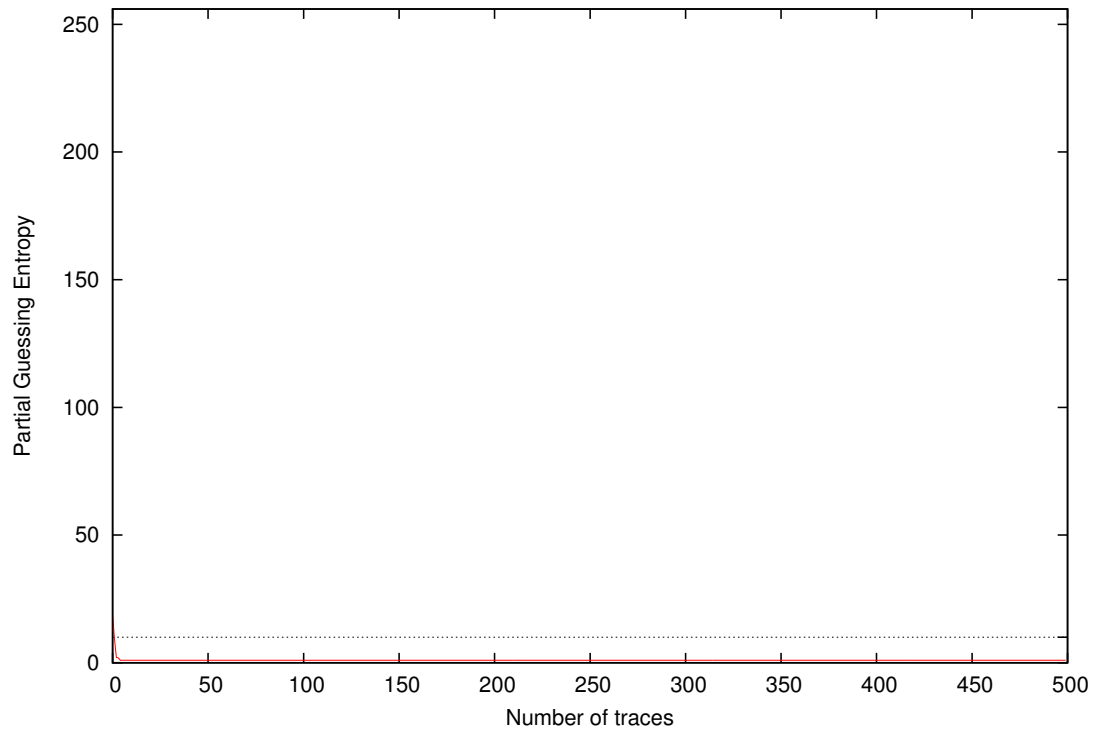
4 Partial Guessing Entropy



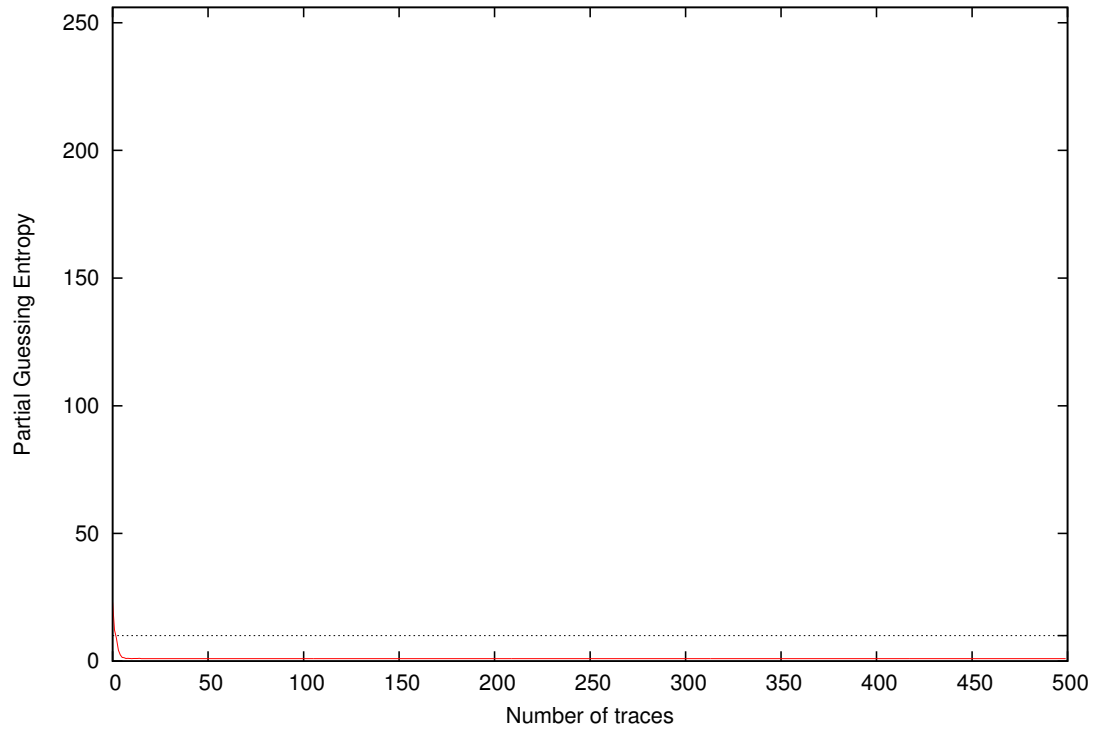
Partial Guessing Entropy for Subkey Byte #3



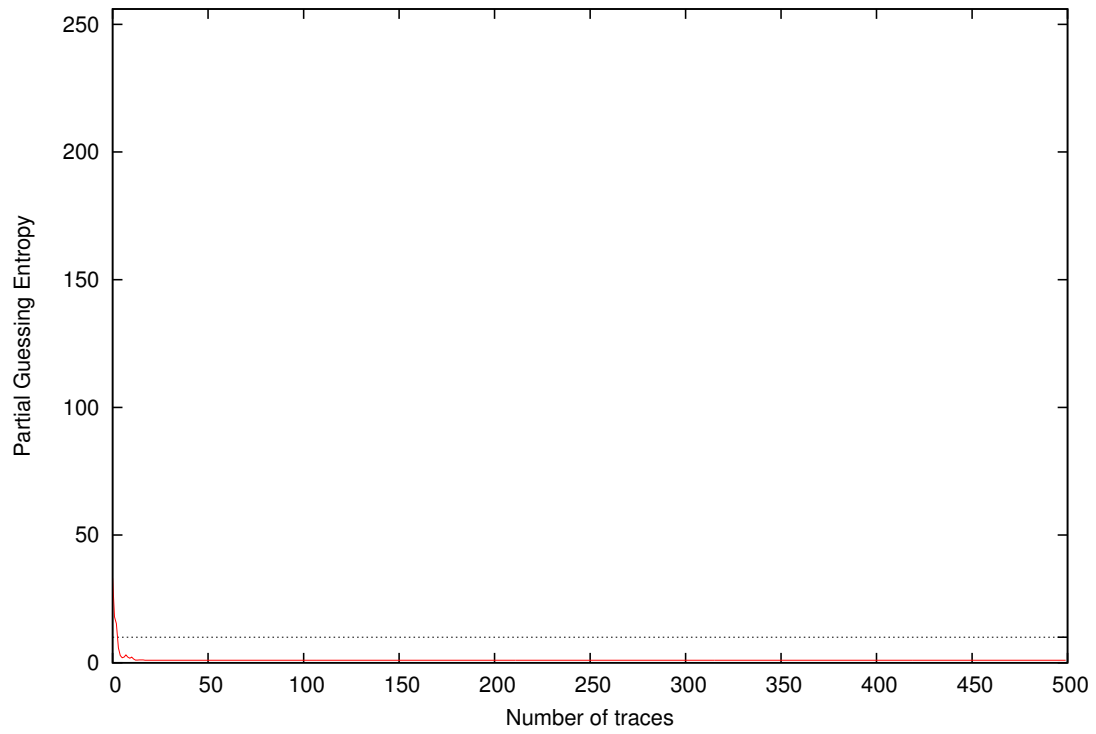
Partial Guessing Entropy for Subkey Byte #4



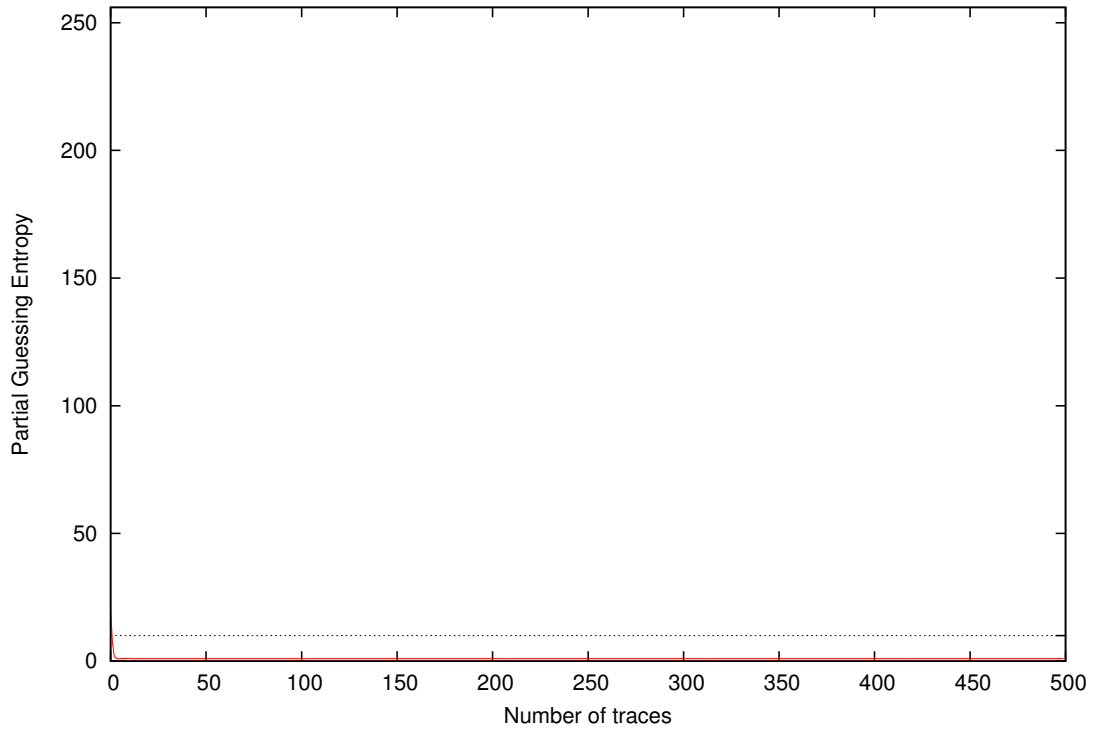
Partial Guessing Entropy for Subkey Byte #5



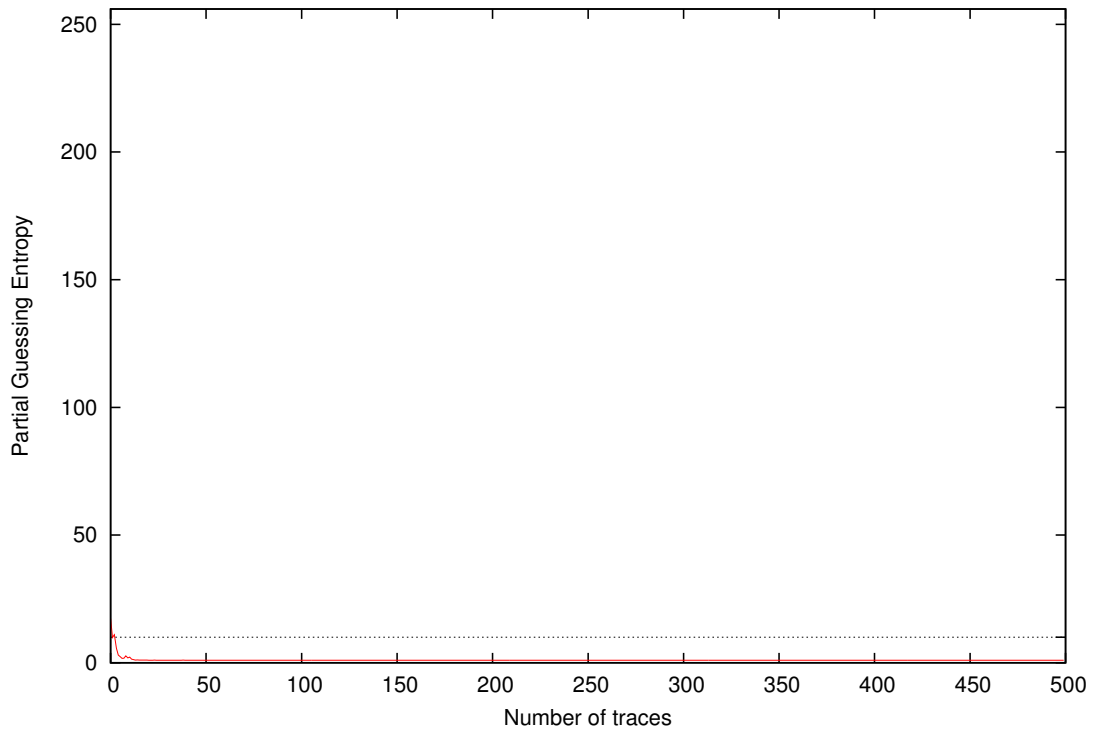
Partial Guessing Entropy for Subkey Byte #6



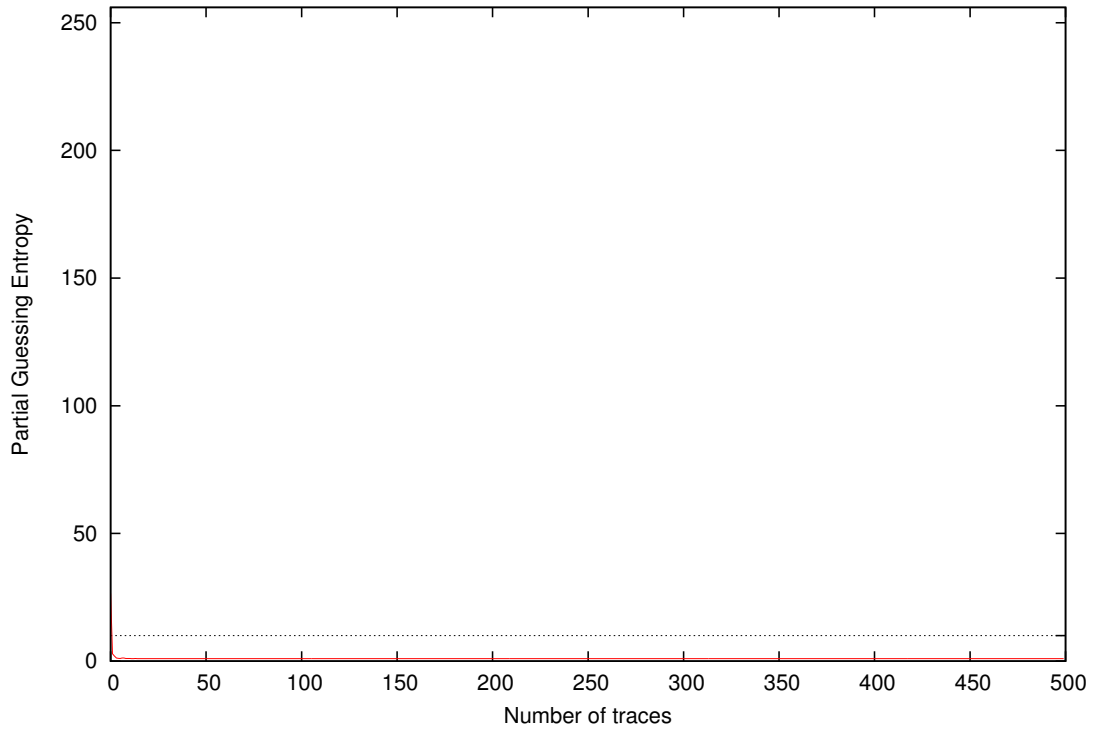
Partial Guessing Entropy for Subkey Byte #7



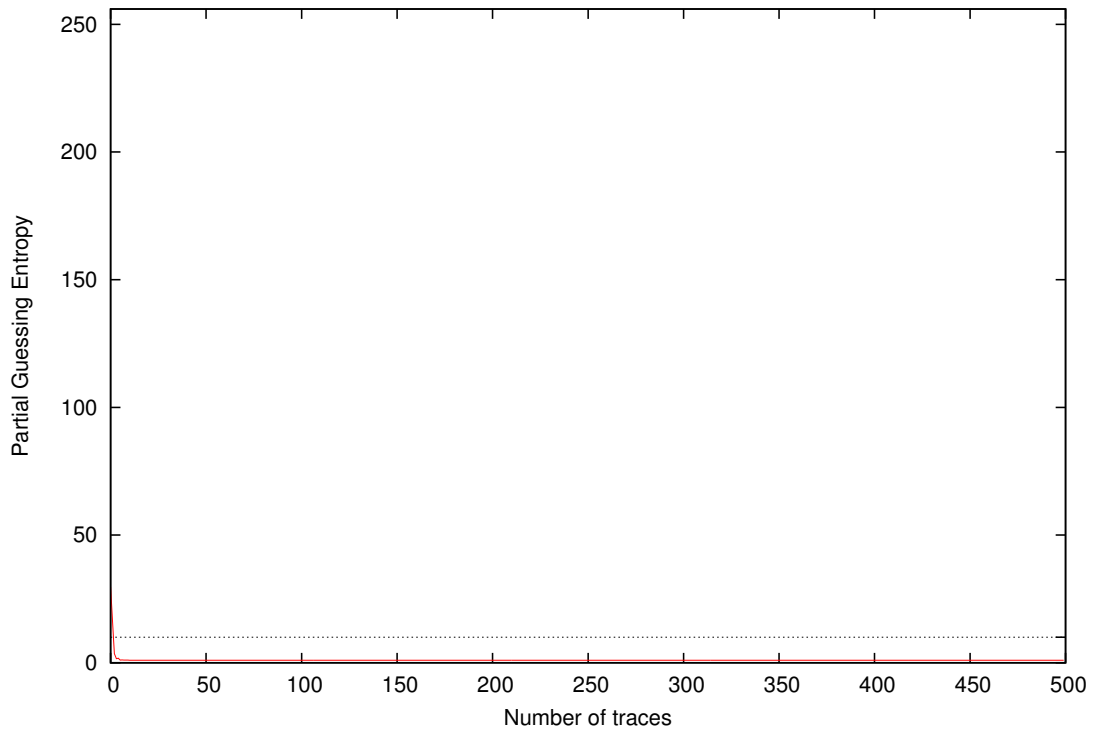
Partial Guessing Entropy for Subkey Byte #8

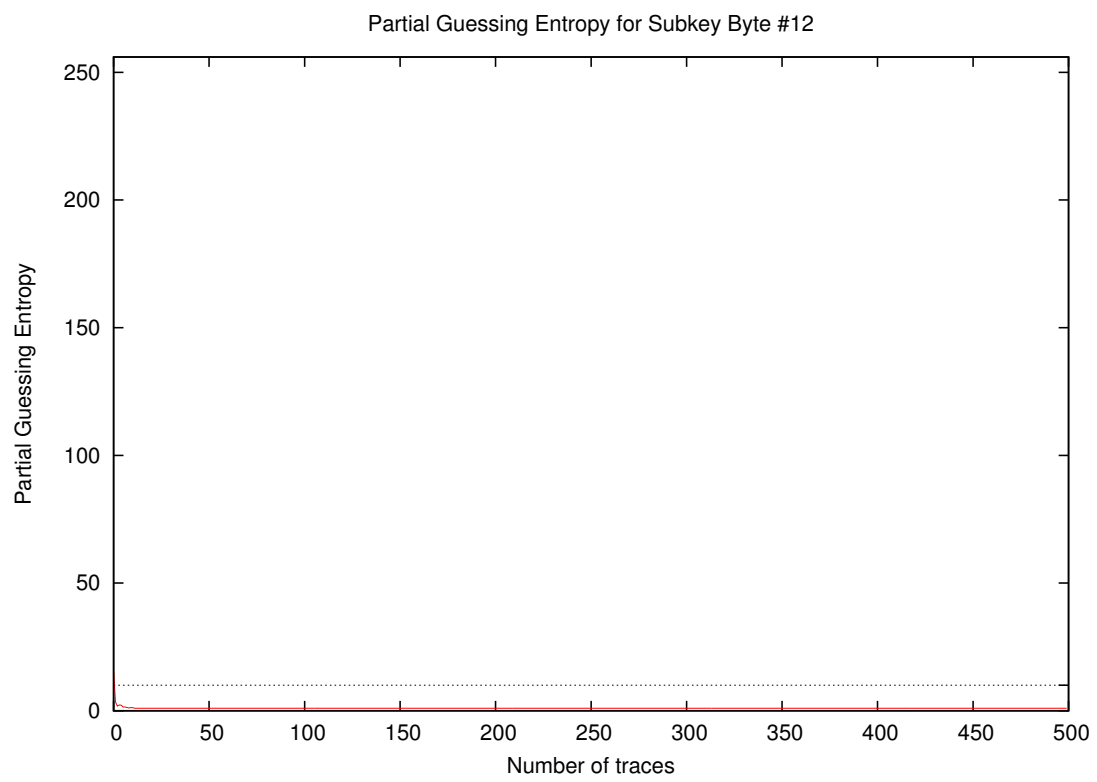
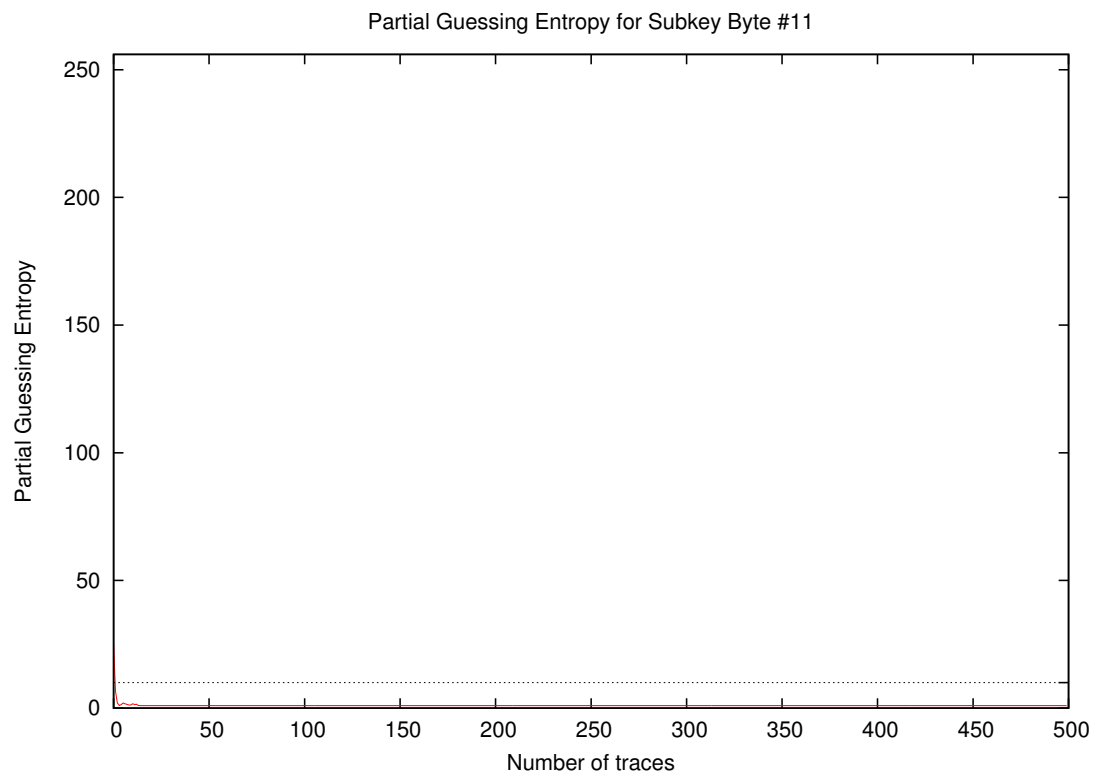


Partial Guessing Entropy for Subkey Byte #9

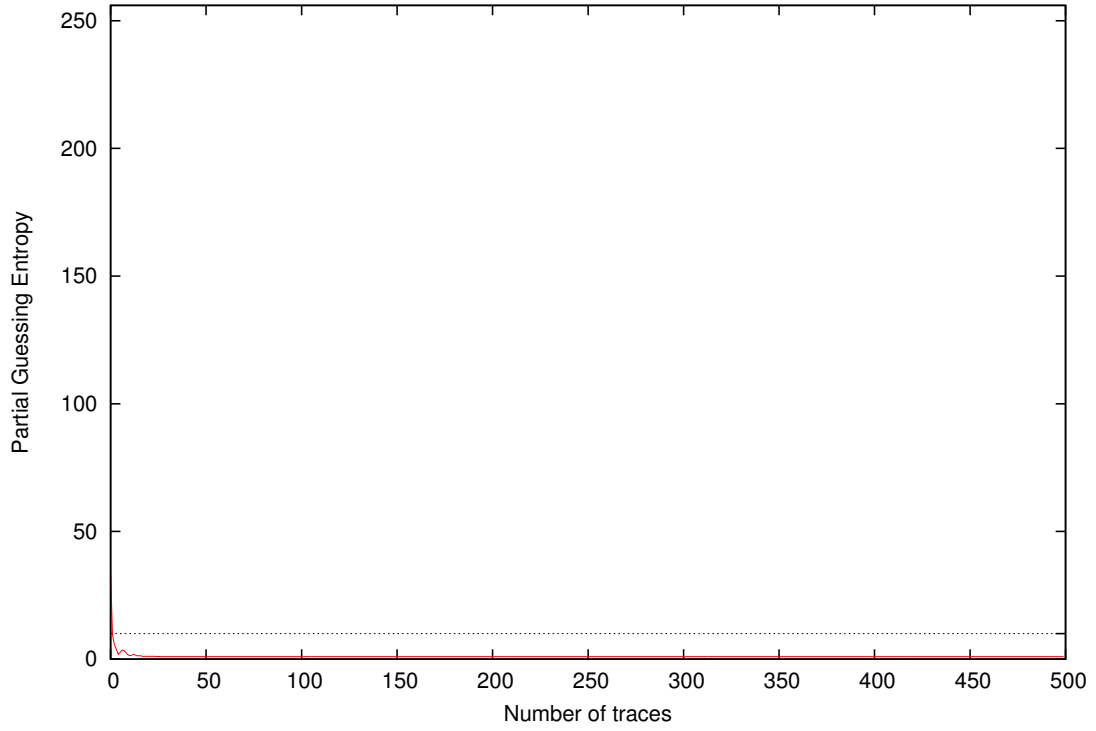


Partial Guessing Entropy for Subkey Byte #10

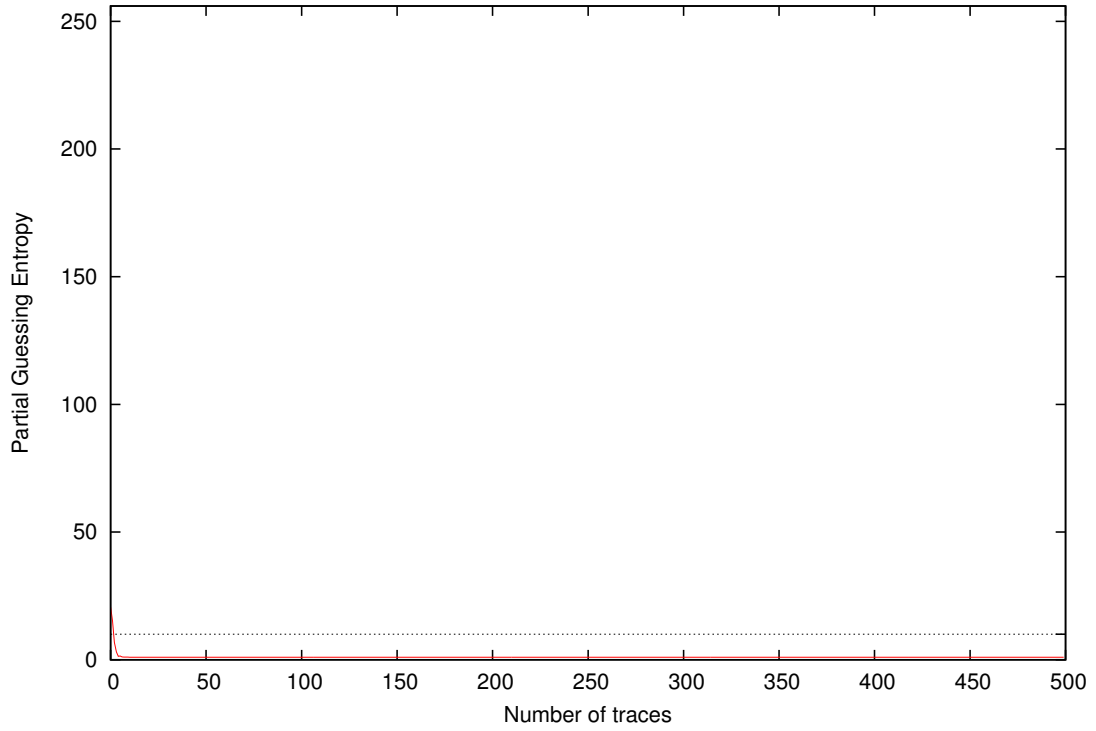


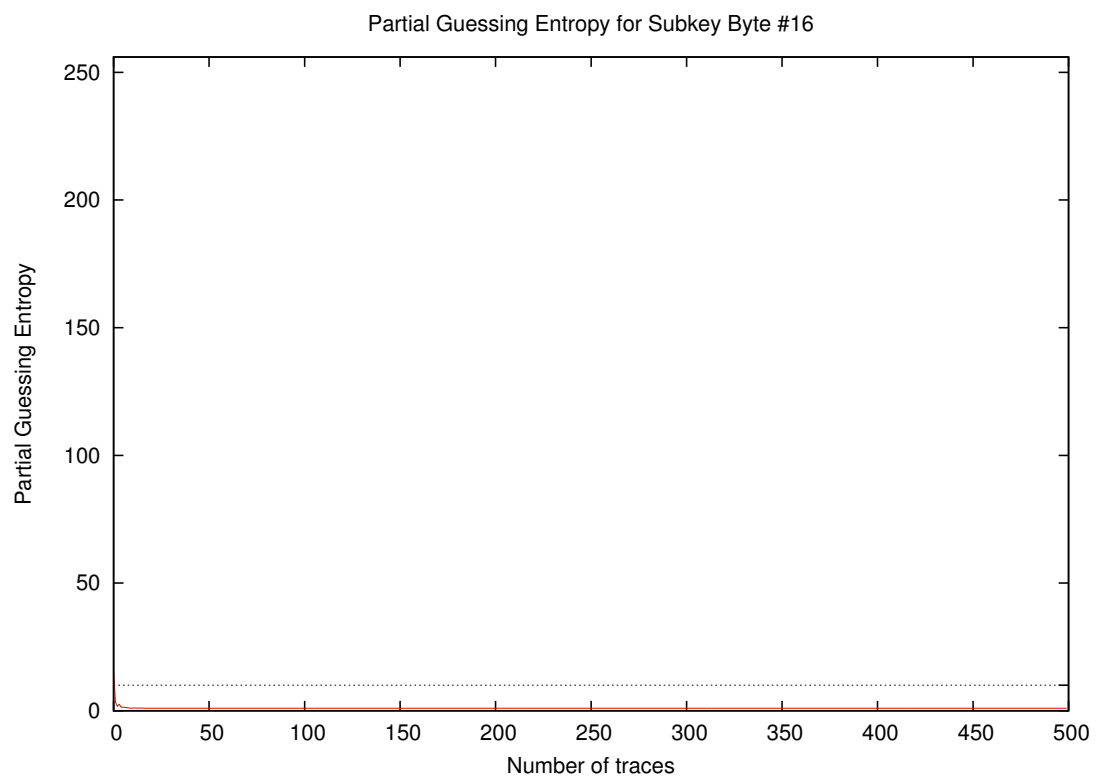
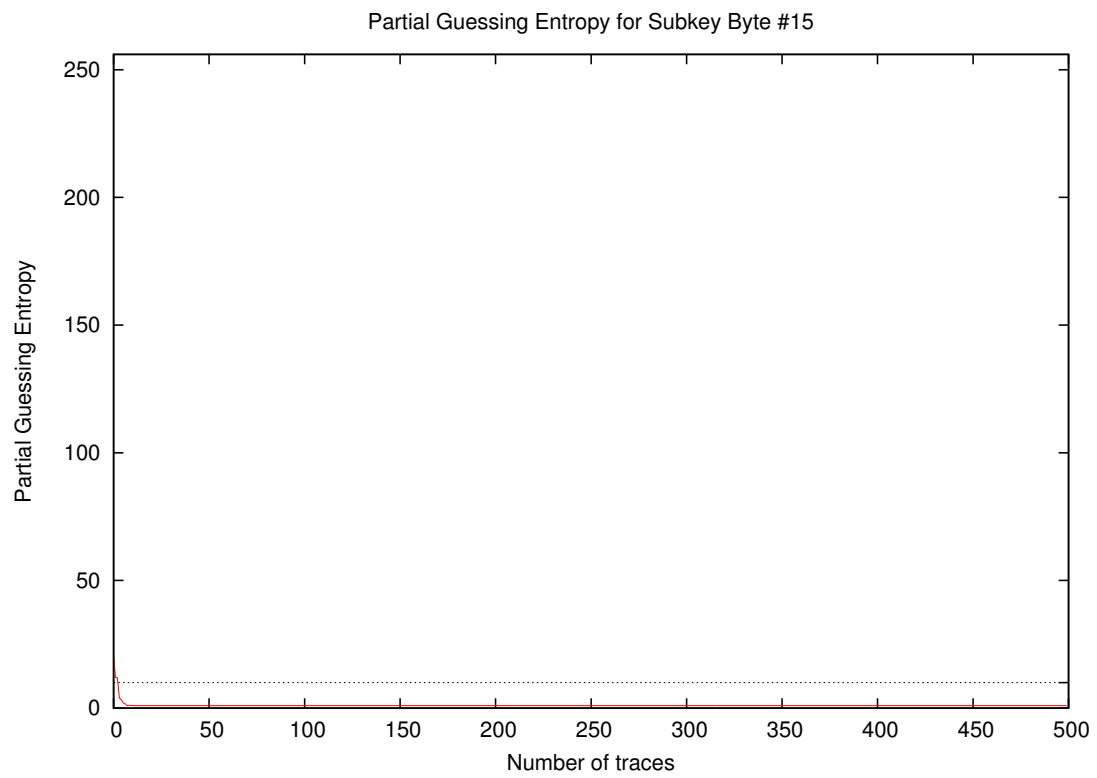


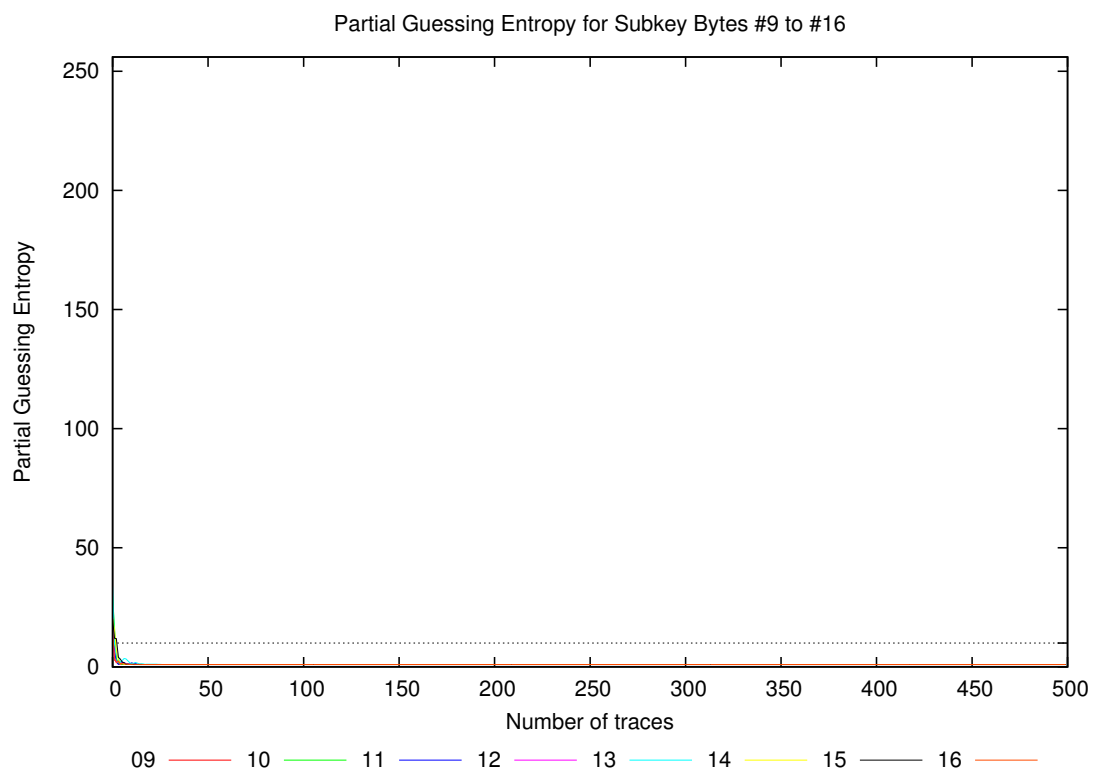
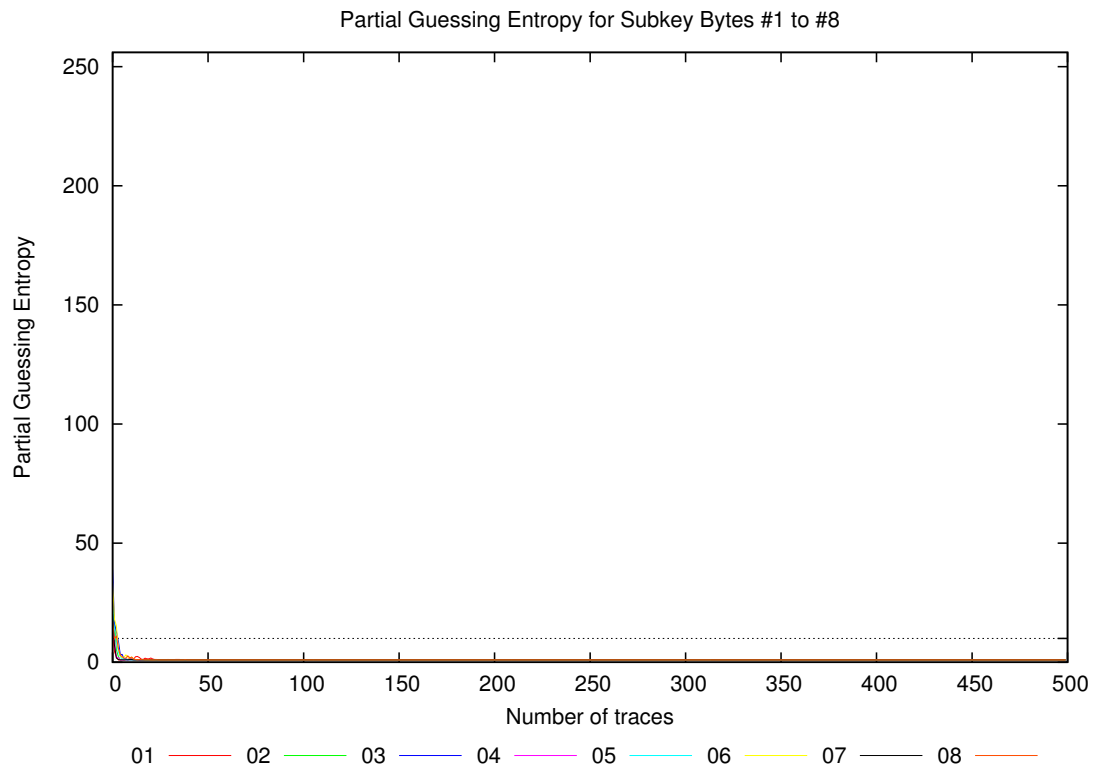
Partial Guessing Entropy for Subkey Byte #13



Partial Guessing Entropy for Subkey Byte #14







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	1.5	1.0	1.3	1.0	1.1	1.8	1.1	1.9	1.1	1.1	1.2	1.2	1.7	1.1	1.1	1.0	1.0	1.9	1.2
20	1.4	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	1.0	1.0	1.0	1.4	1.0
30	1.2	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	1.2	1.0
40	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
50	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
100	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
200	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
300	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
400	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
500	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