

DPA Contest v4.2

Evaluation results

Mélissa Rossi

July 2016

1 Introduction

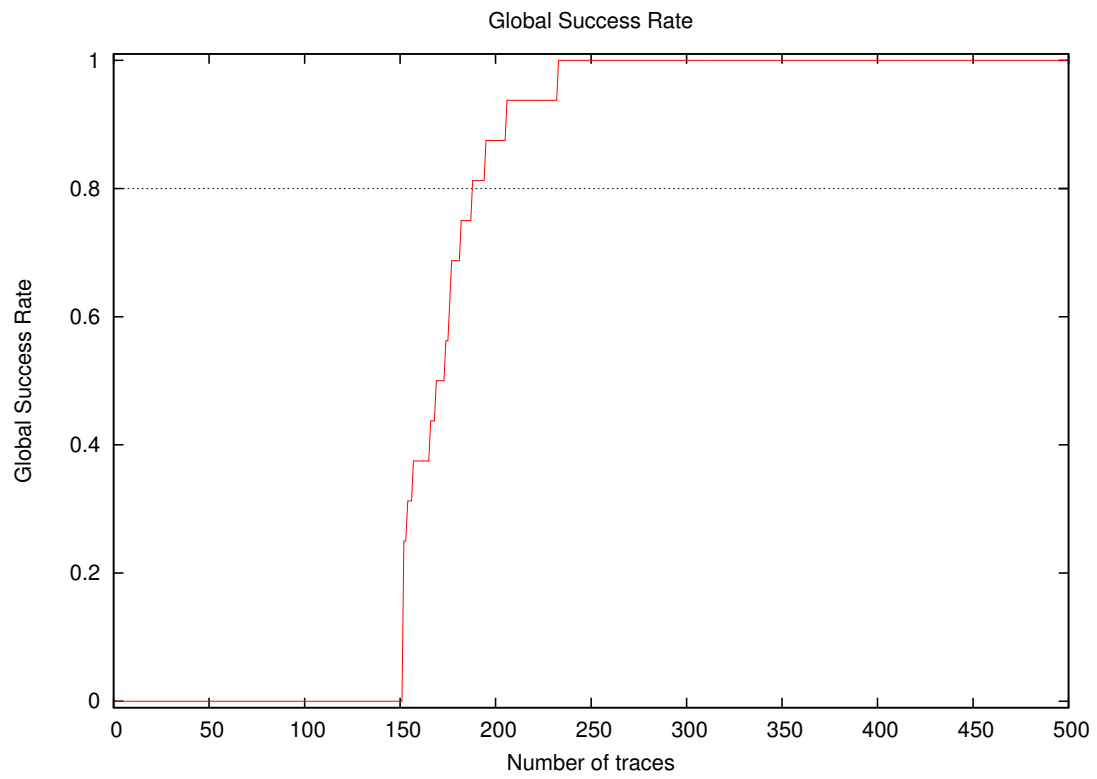
1.1 About the attack

- **Sender/Team:** Mélissa Rossi
- **Institution:** Thales, France
- **Language:** C++
- **Operating system:** Linux
- **Attacked subkey:** 0

1.2 About the evaluation

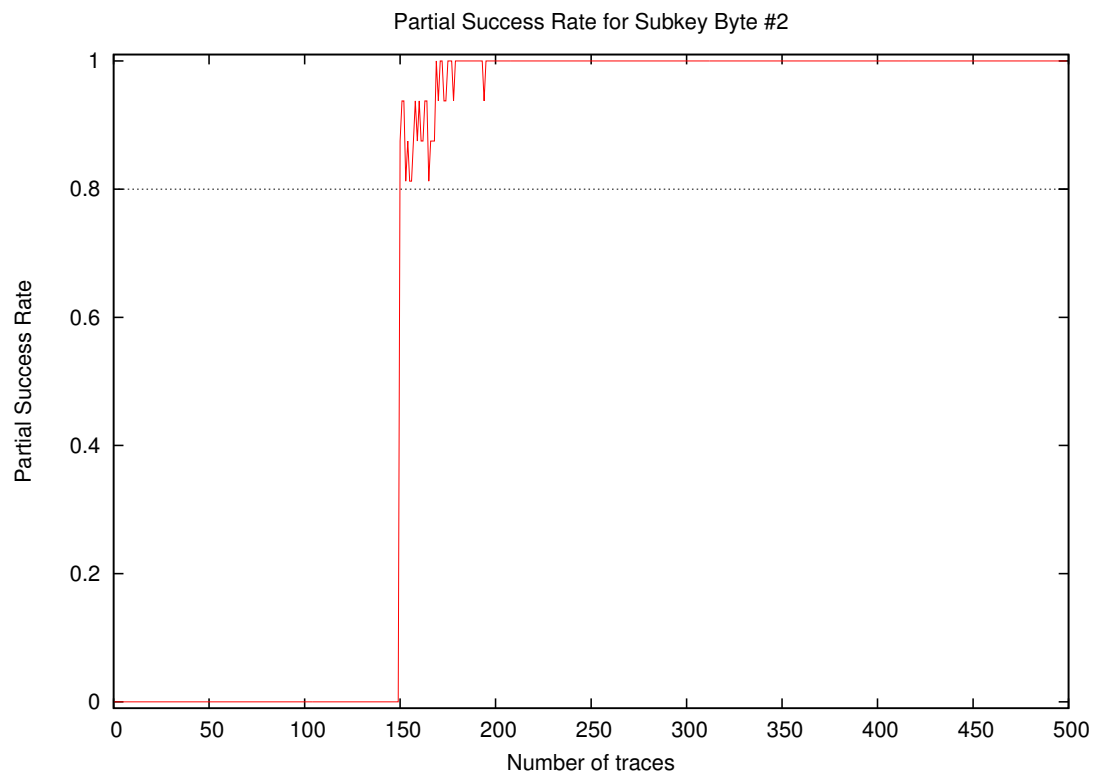
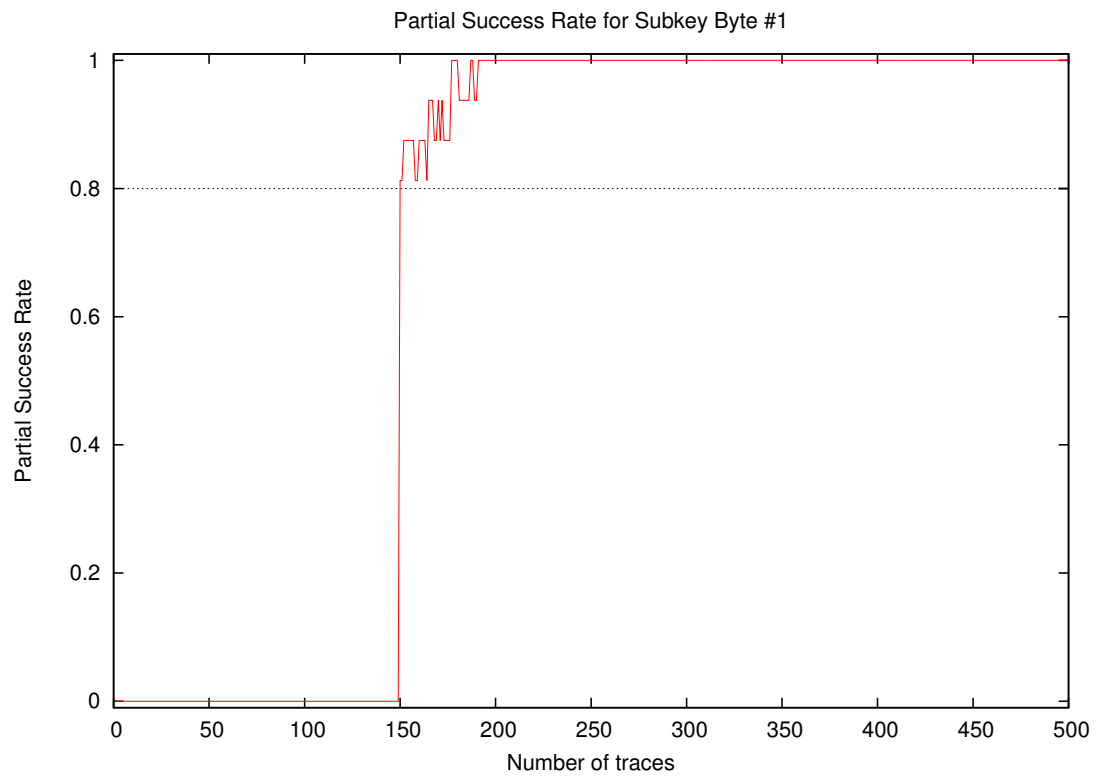
- **Date of evaluation:** July 2016

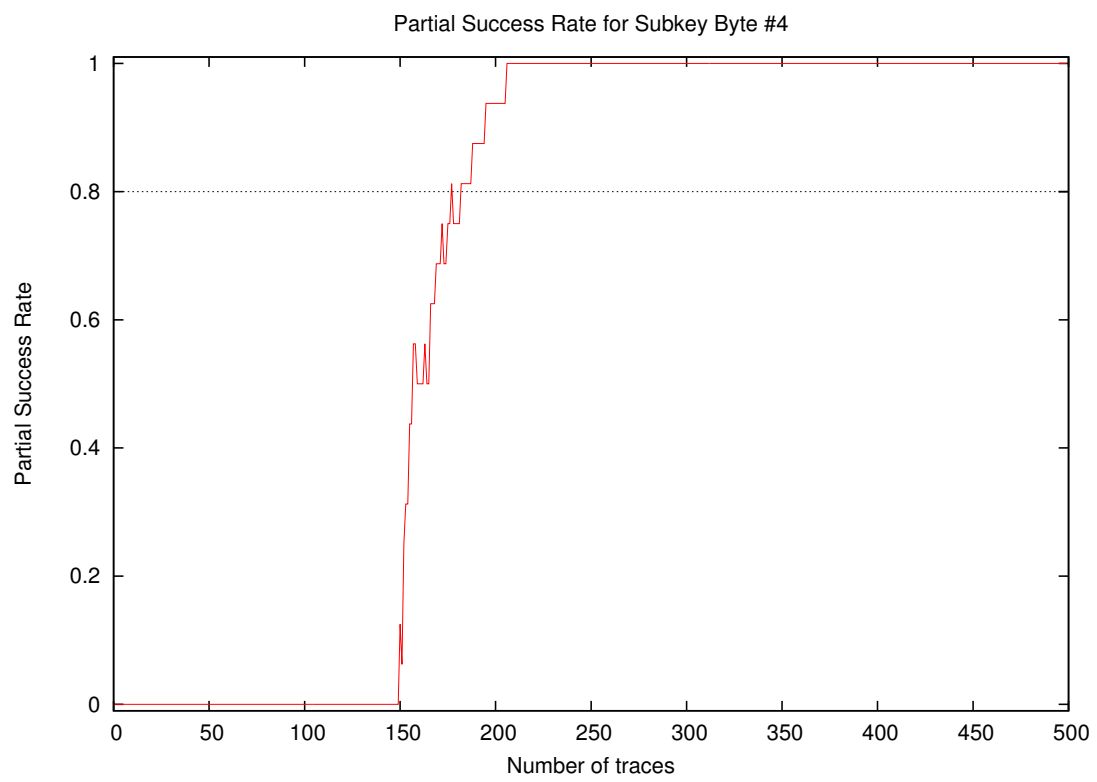
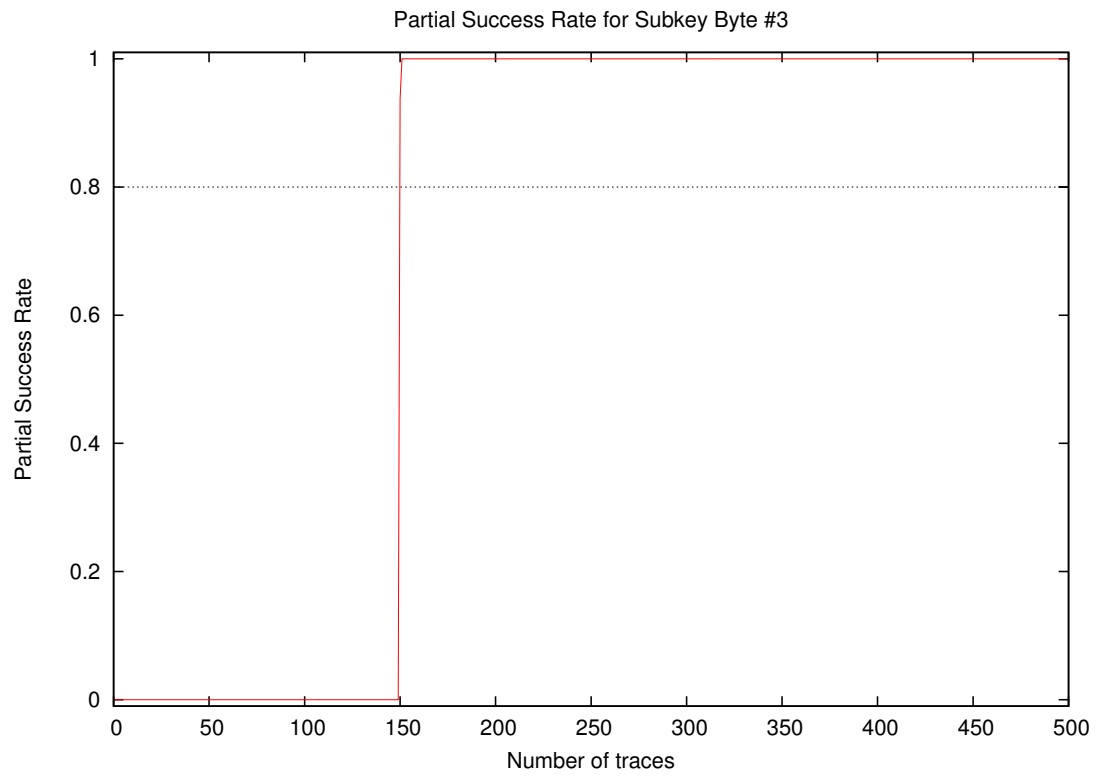
2 Global Success Rate

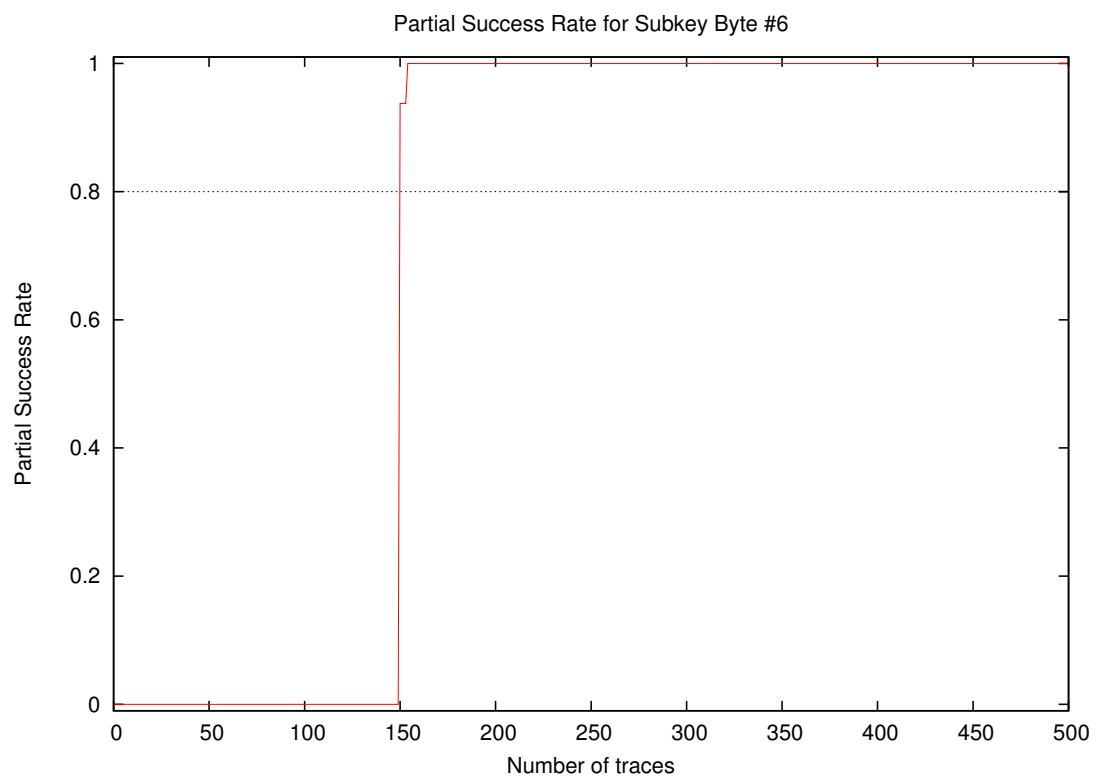
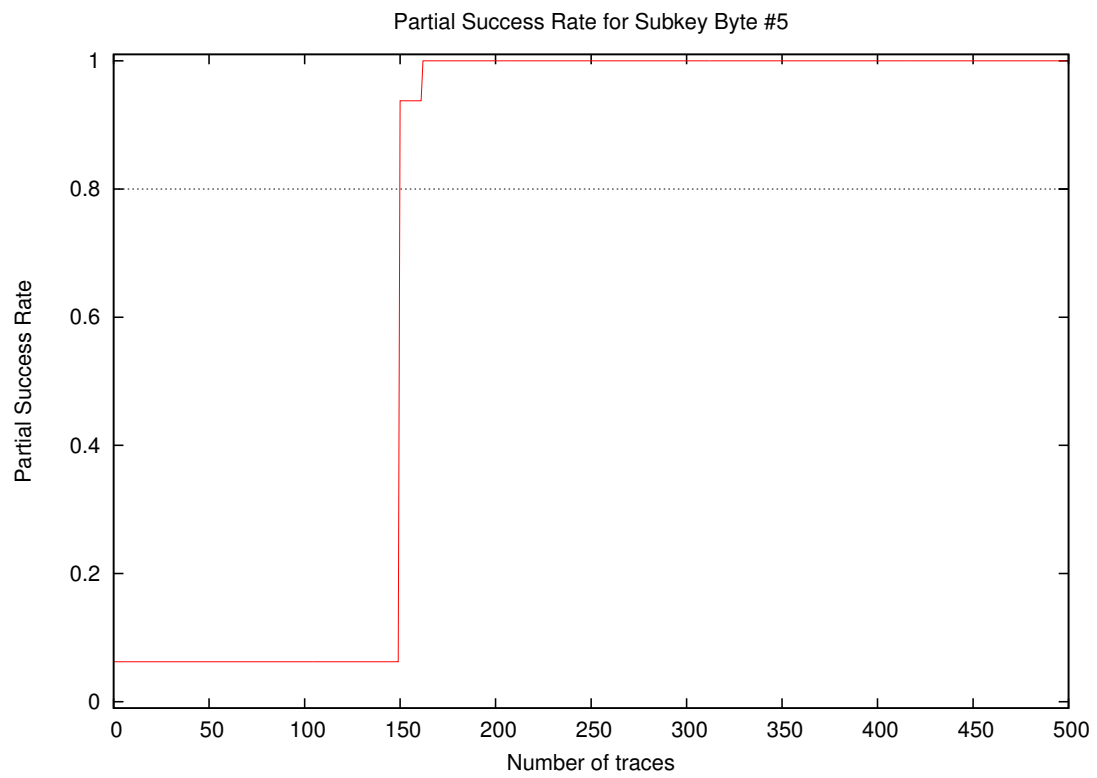


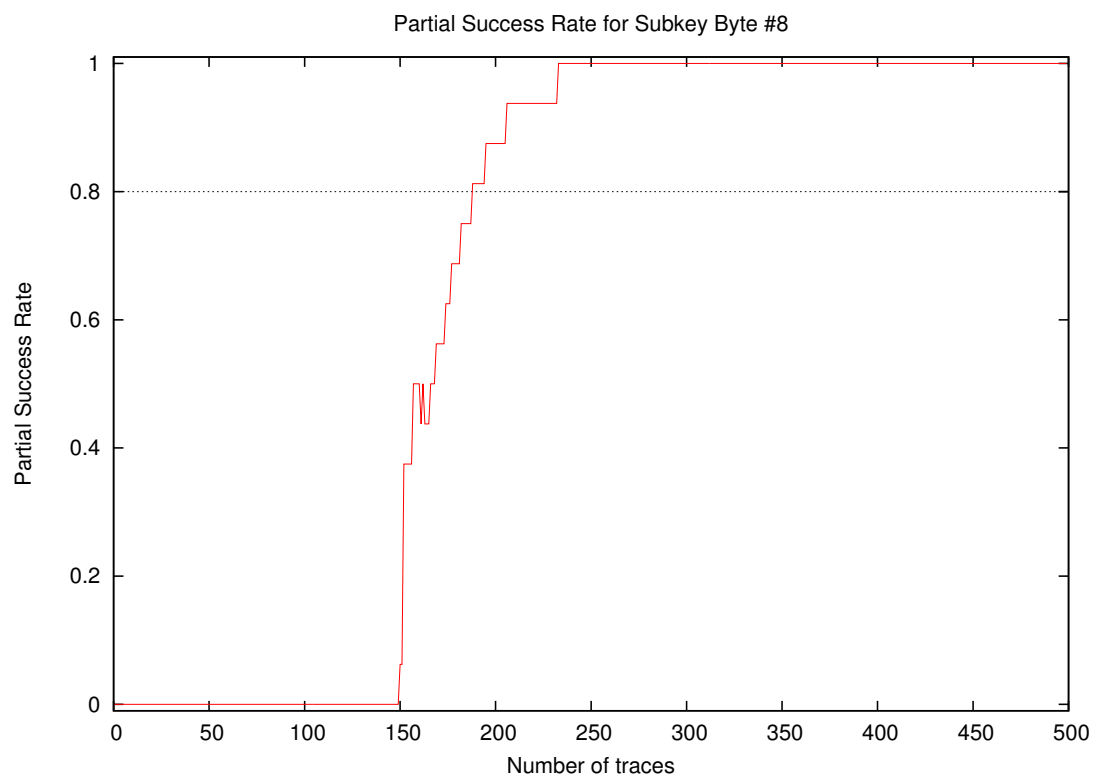
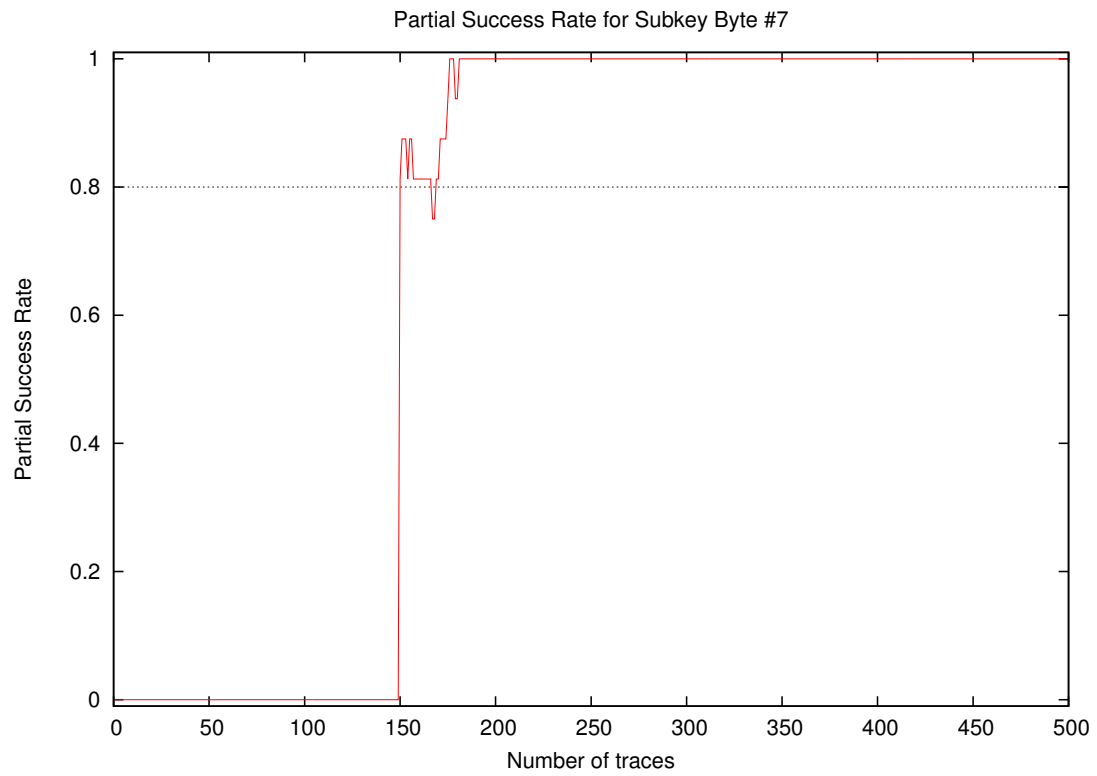
Number of traces	Global Success Rate
10	0.00
20	0.00
30	0.00
40	0.00
50	0.00
100	0.00
200	0.88
300	1.00
400	1.00
500	1.00

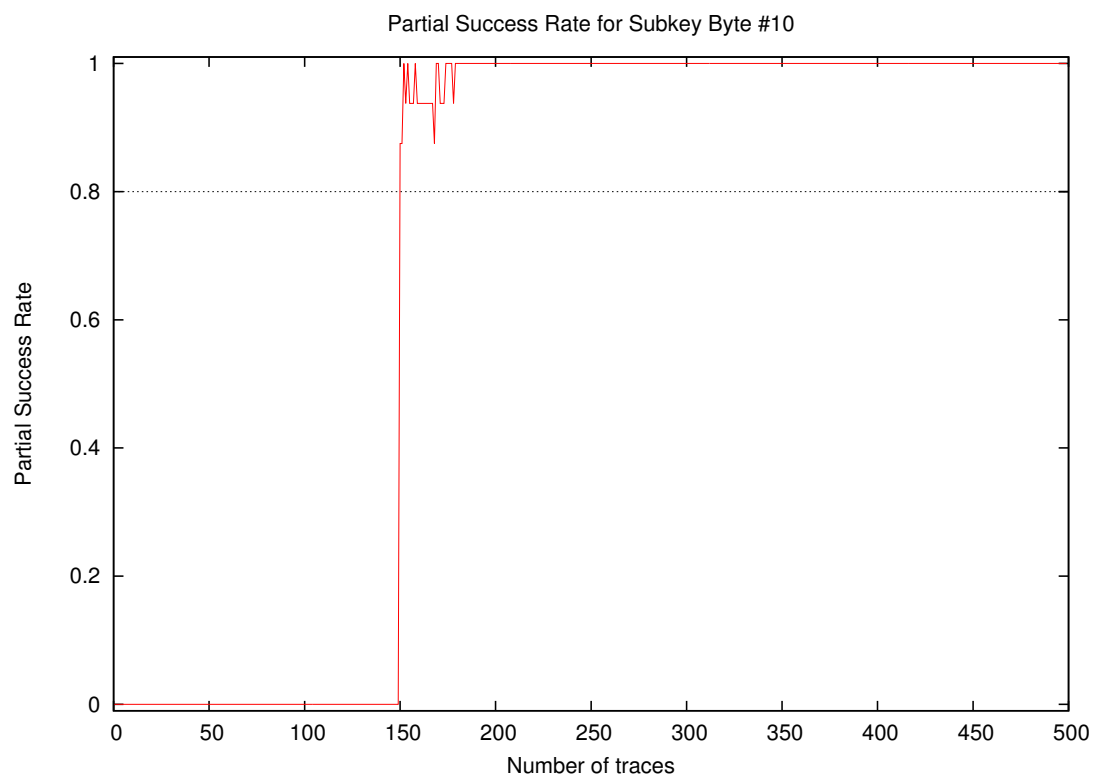
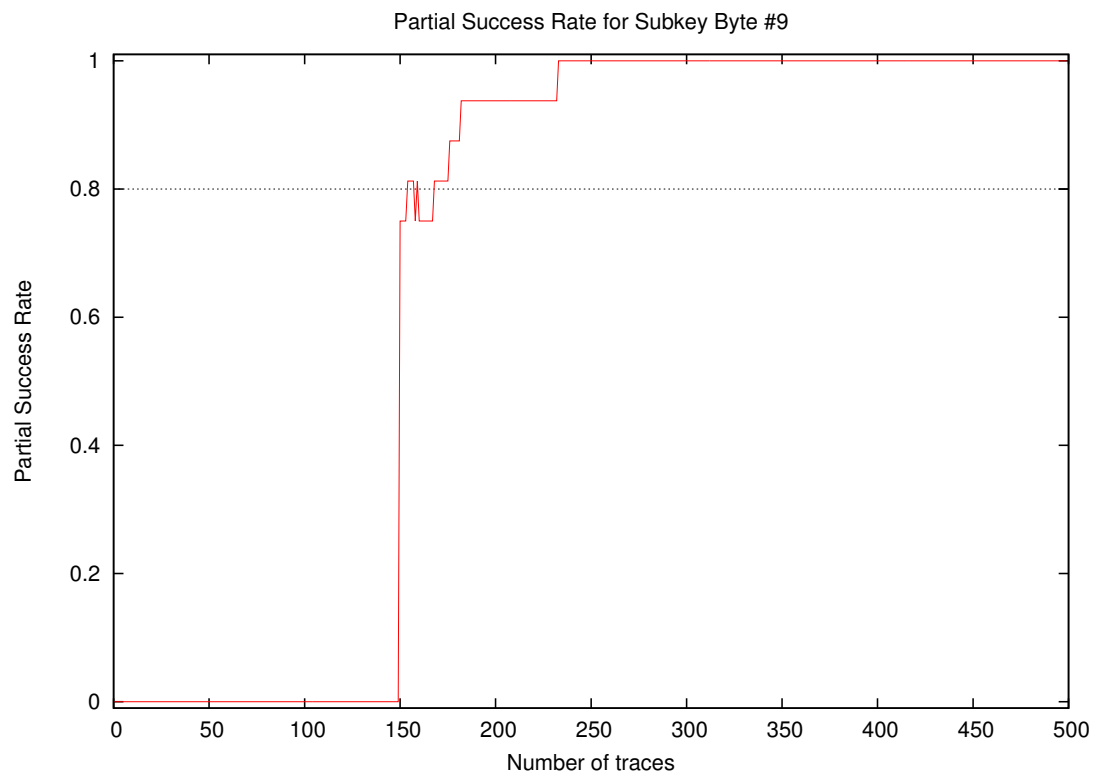
3 Partial Success Rate

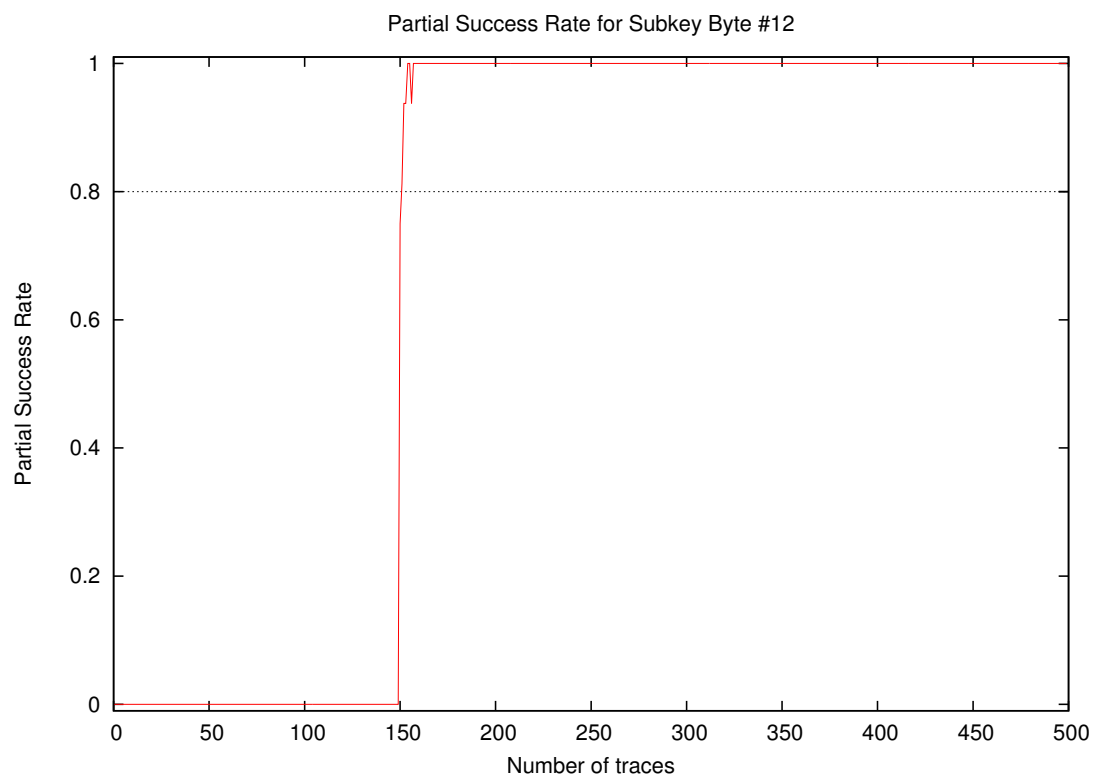
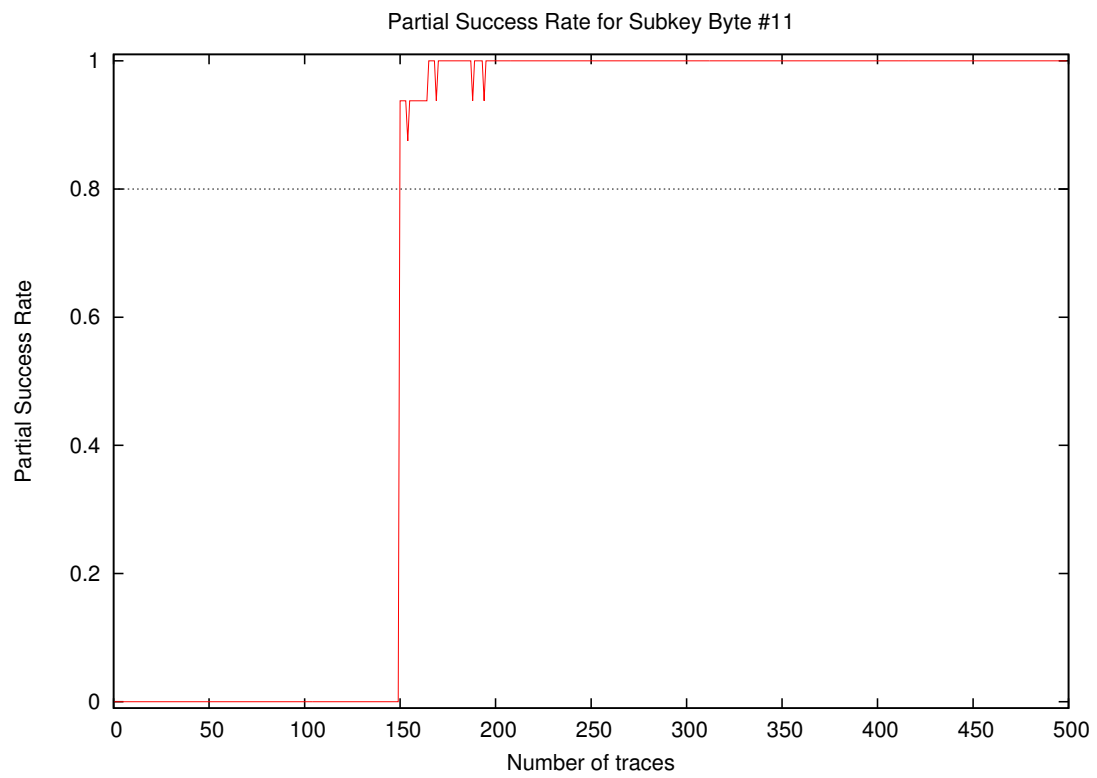


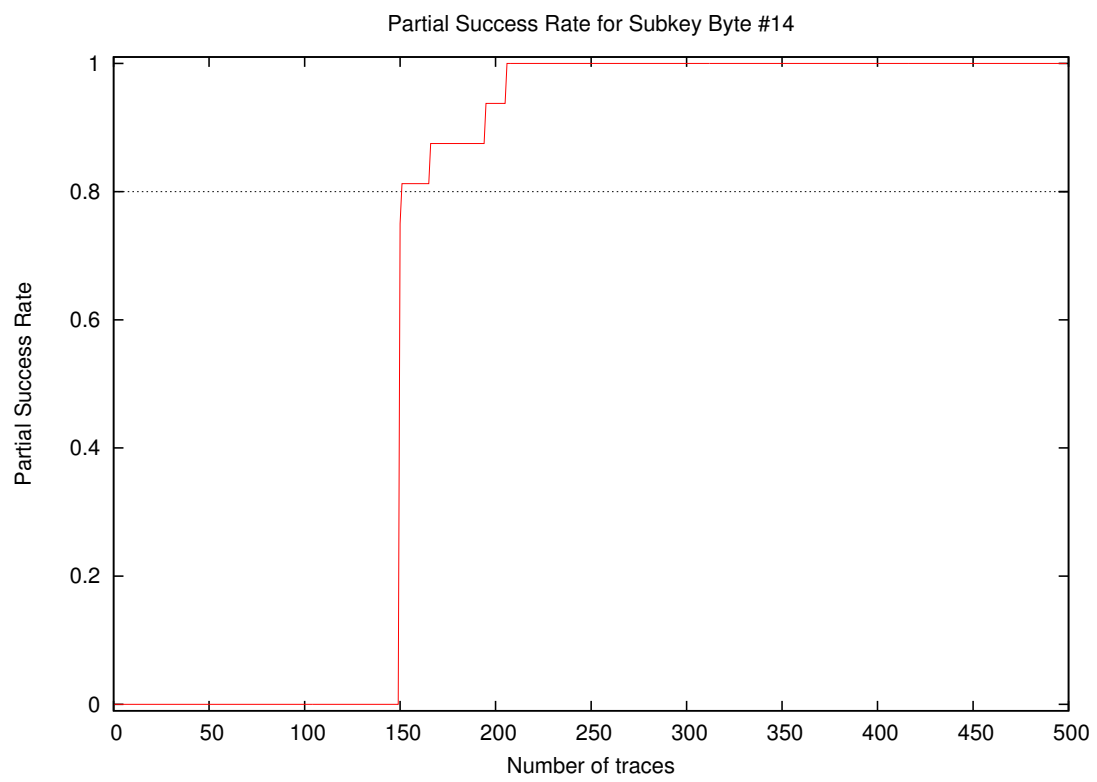
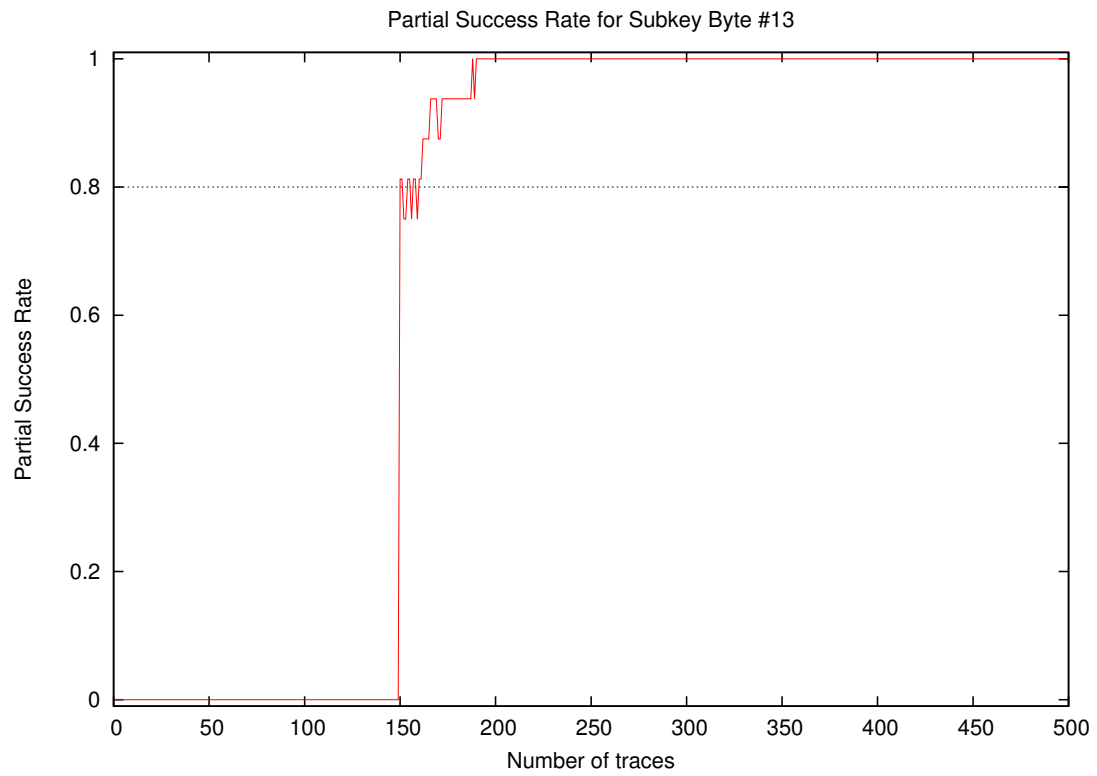


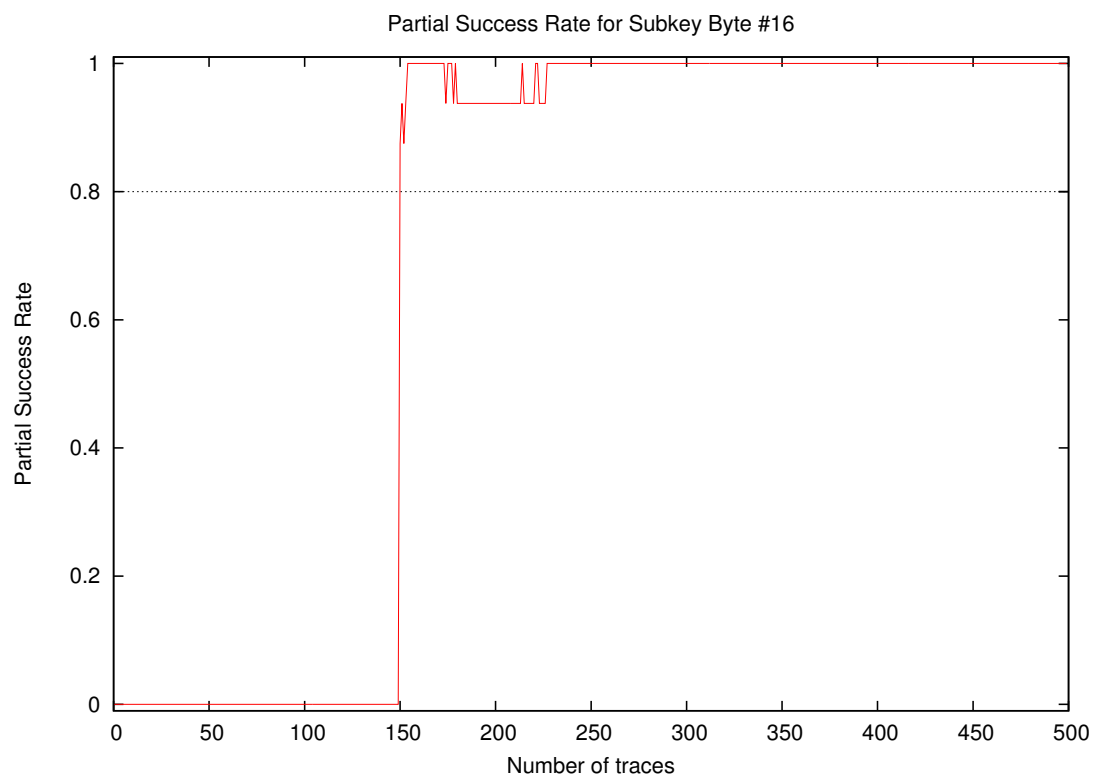
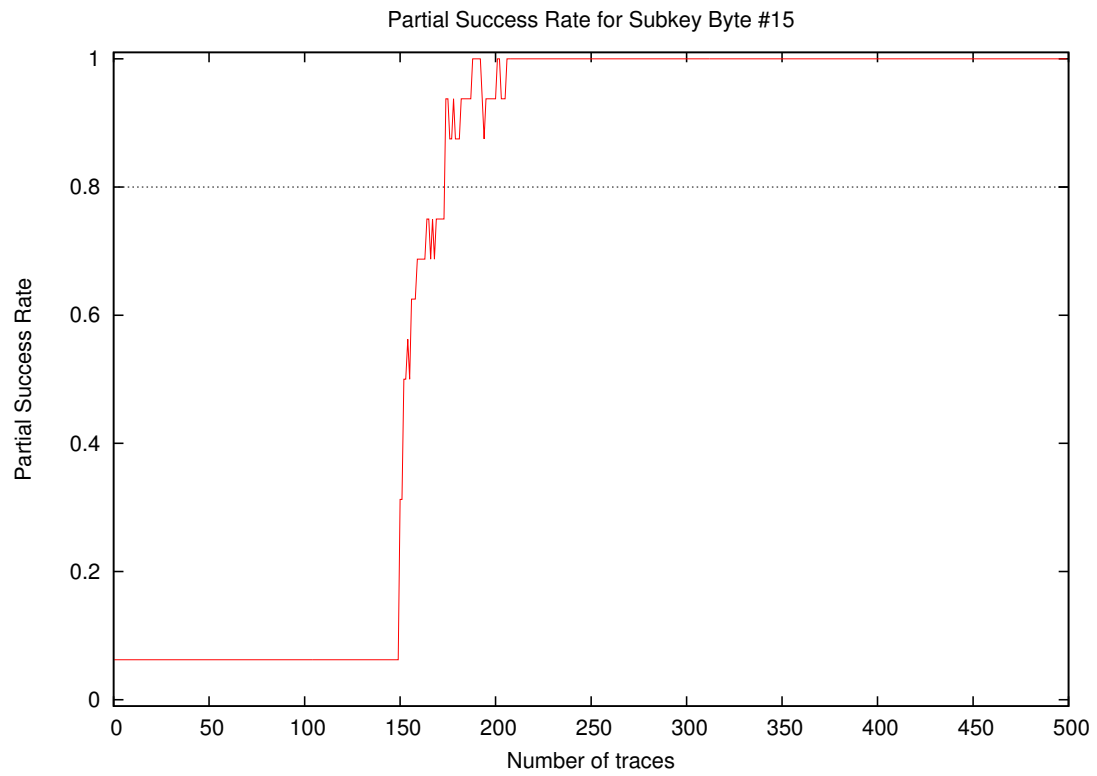




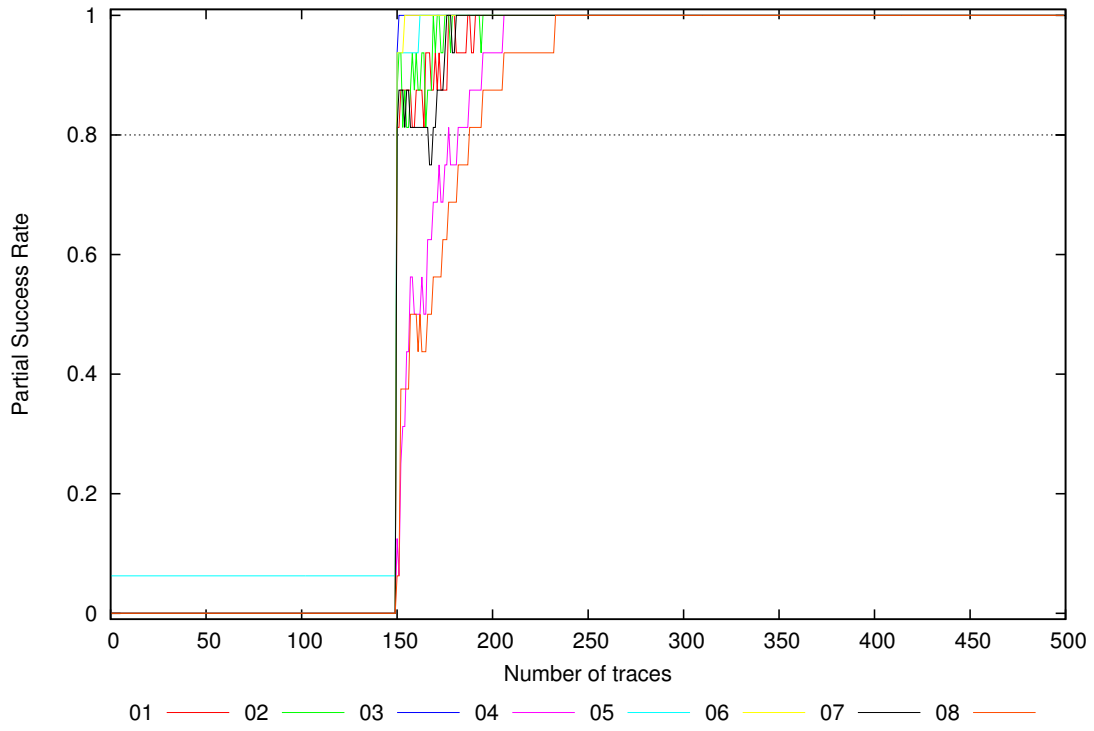




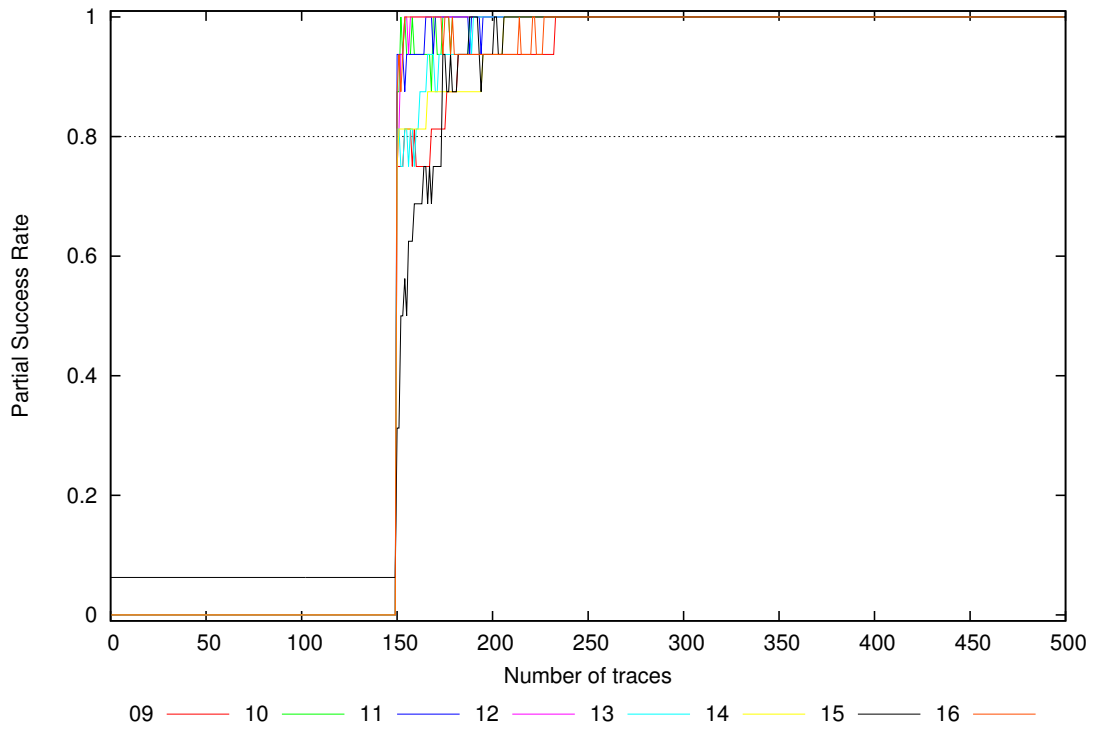




Partial Success Rate for Subkey Bytes #1 to #8

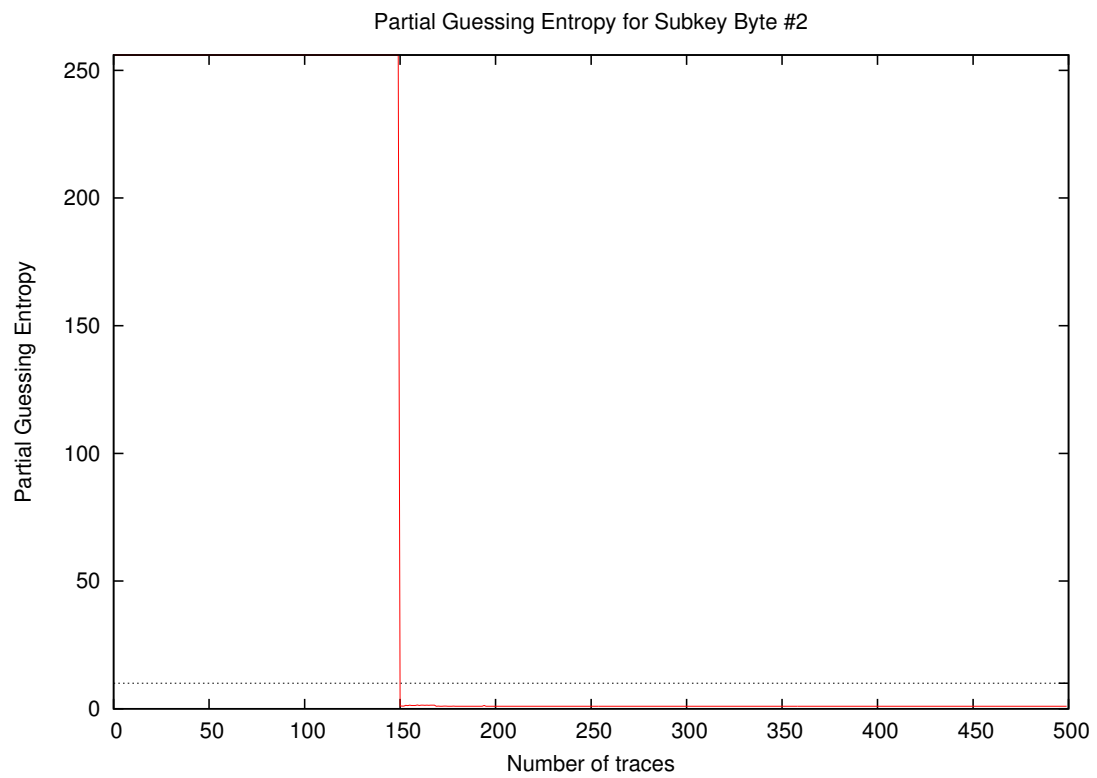
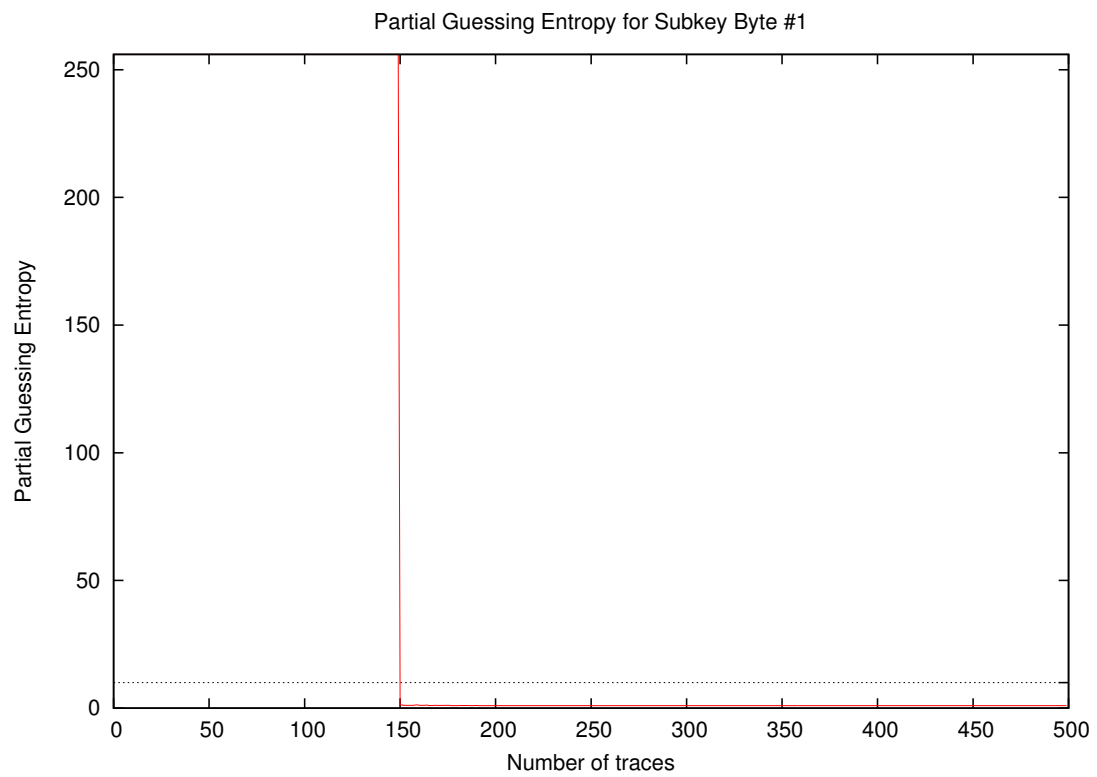


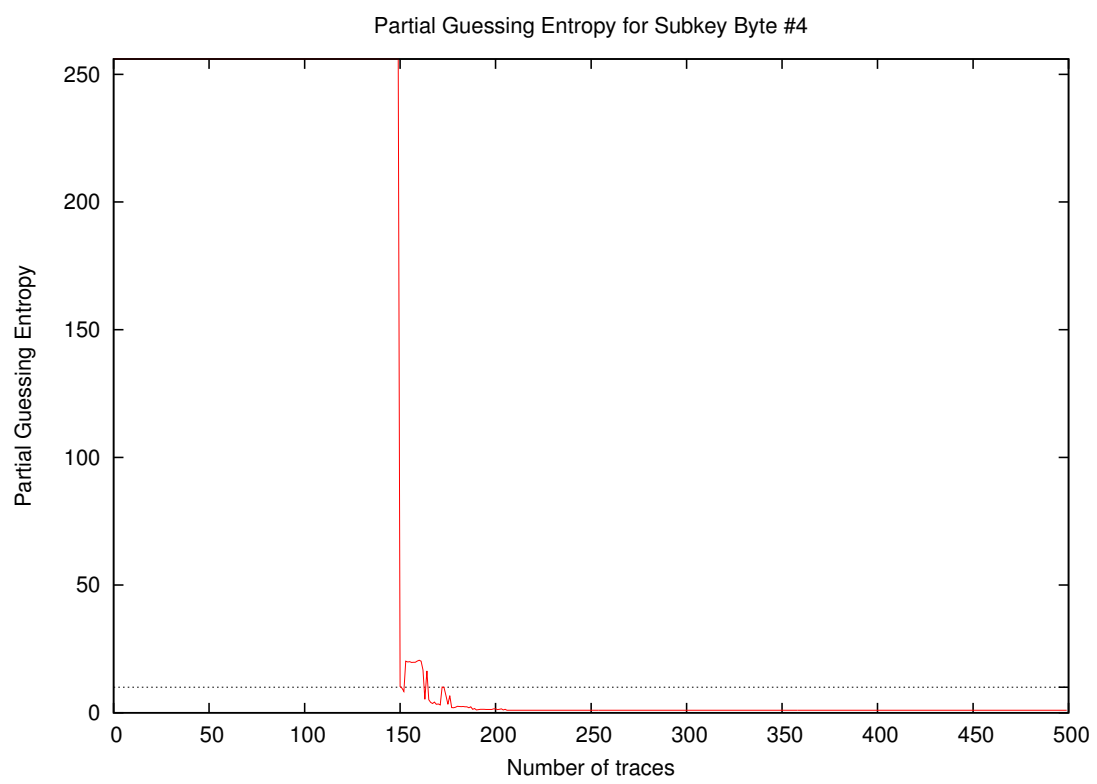
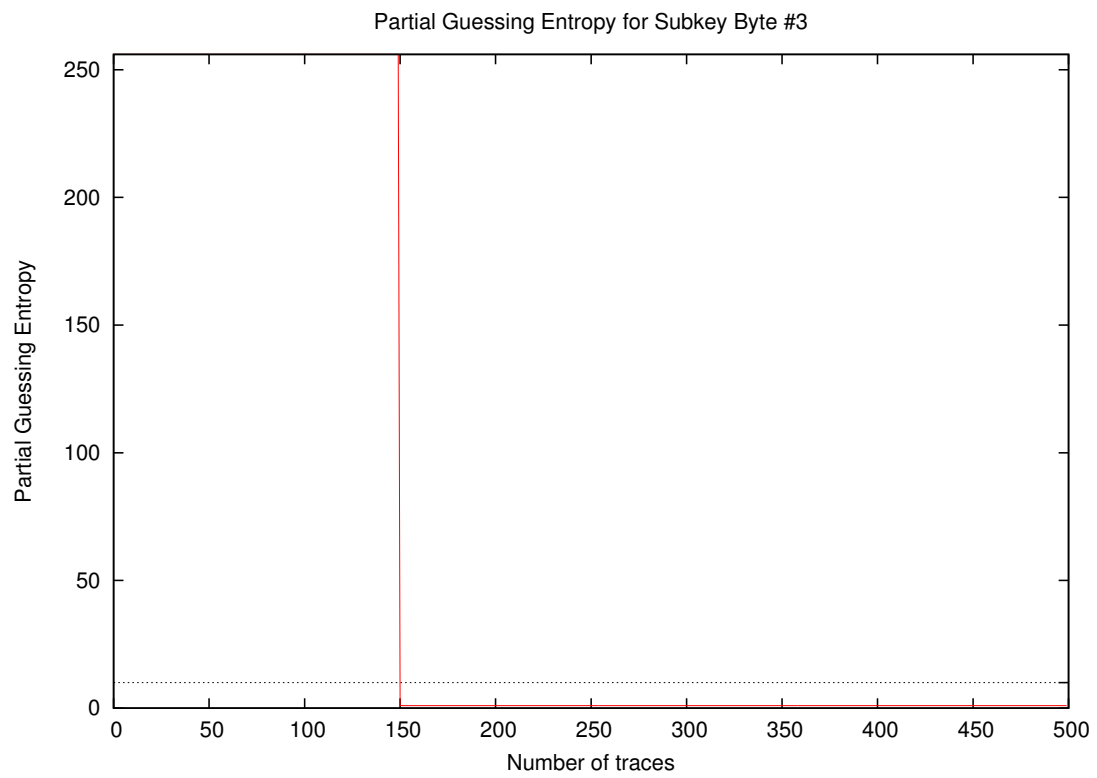
Partial Success Rate for Subkey Bytes #9 to #16



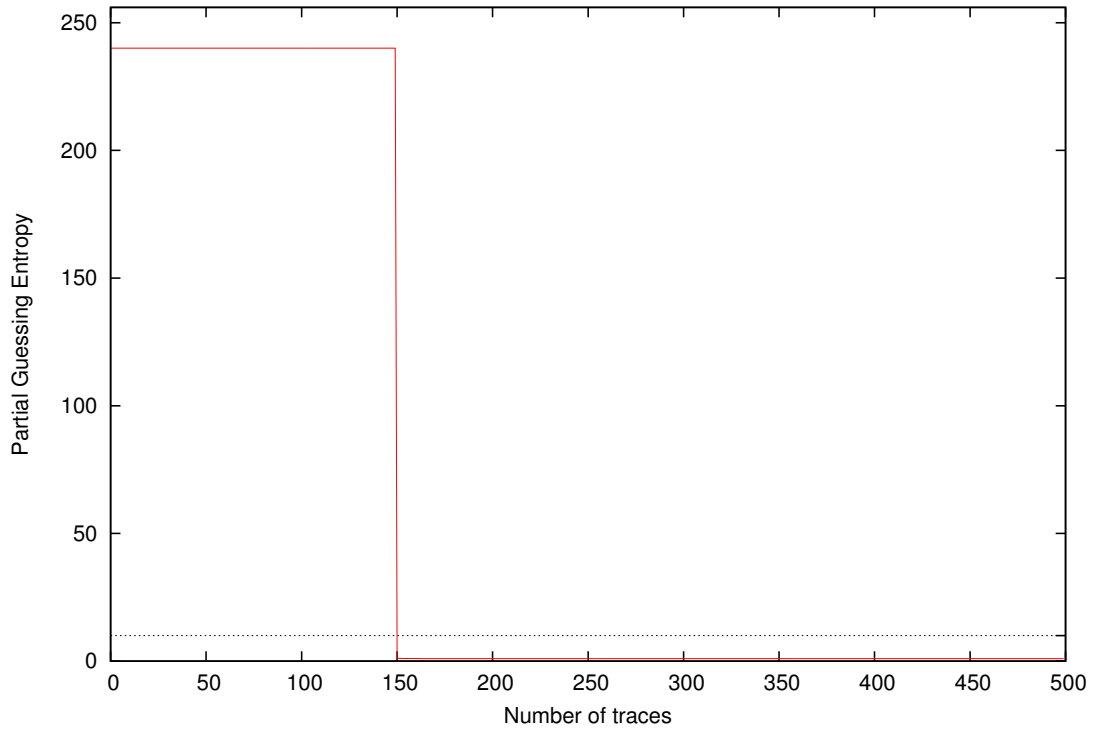
Traces	Partial Success Rate / Byte																Min	Max	Mean
	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16			
10	0.00	0.00	0.00	0.00	0.06	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.06	0.00	0.00	0.06	0.01
20	0.00	0.00	0.00	0.00	0.06	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.06	0.00	0.00	0.06	0.01
30	0.00	0.00	0.00	0.00	0.06	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.06	0.00	0.00	0.06	0.01
40	0.00	0.00	0.00	0.00	0.06	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.06	0.00	0.00	0.06	0.01
50	0.00	0.00	0.00	0.00	0.06	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.06	0.00	0.00	0.06	0.01
100	0.00	0.00	0.00	0.00	0.06	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.06	0.00	0.00	0.06	0.01
200	1.00	1.00	1.00	0.94	1.00	1.00	1.00	0.88	0.94	1.00	1.00	1.00	1.00	0.94	0.94	0.94	0.88	1.00	0.97
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

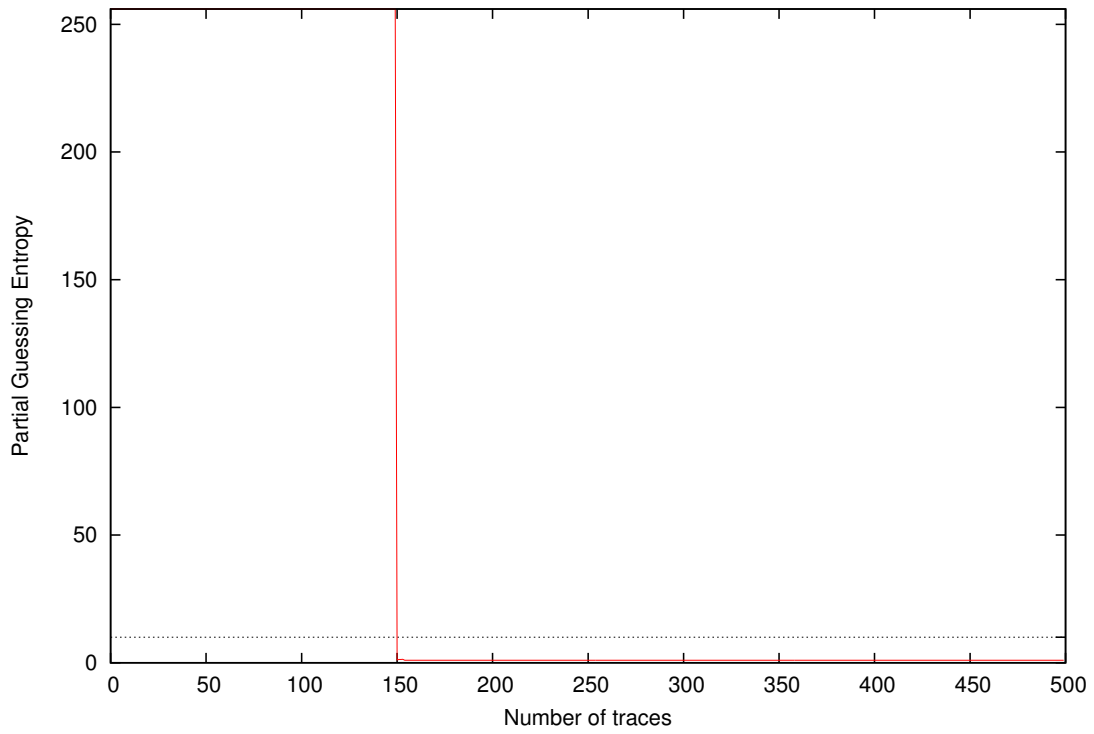




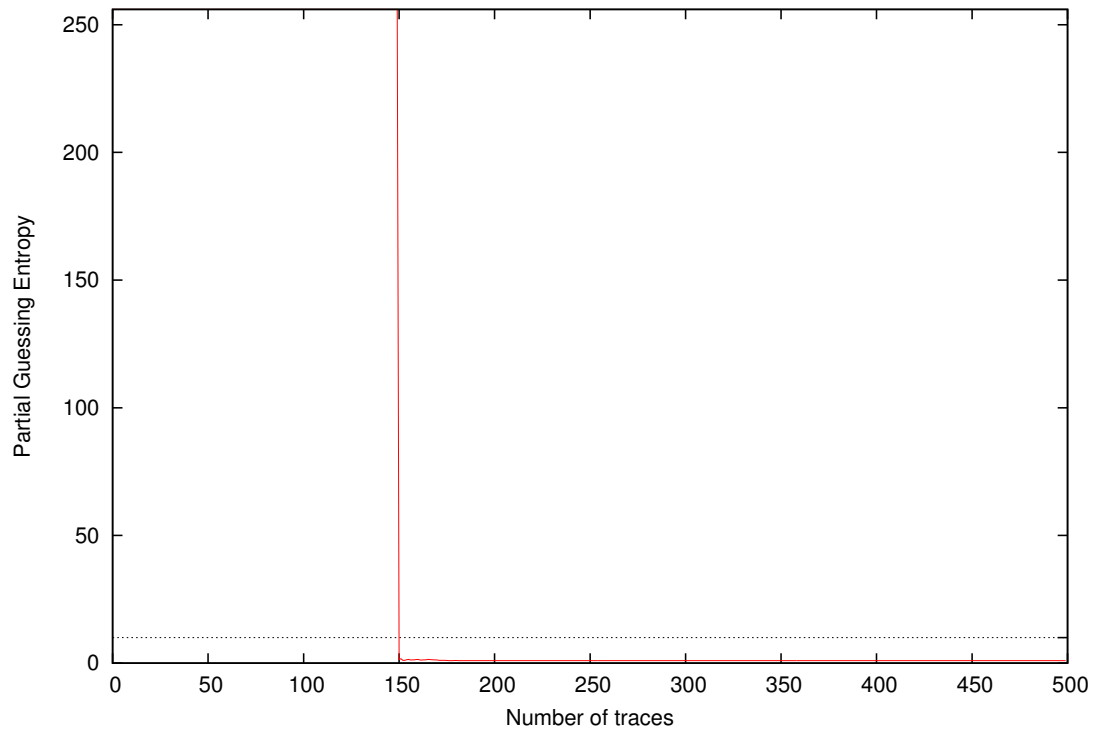
Partial Guessing Entropy for Subkey Byte #5



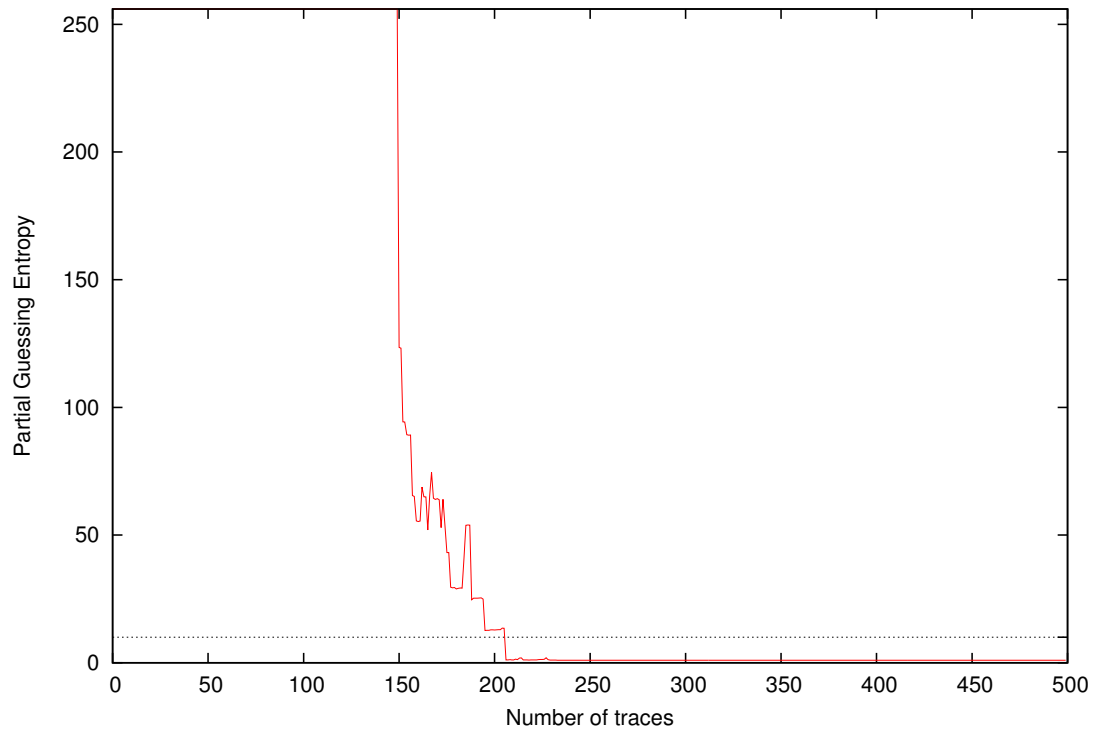
Partial Guessing Entropy for Subkey Byte #6

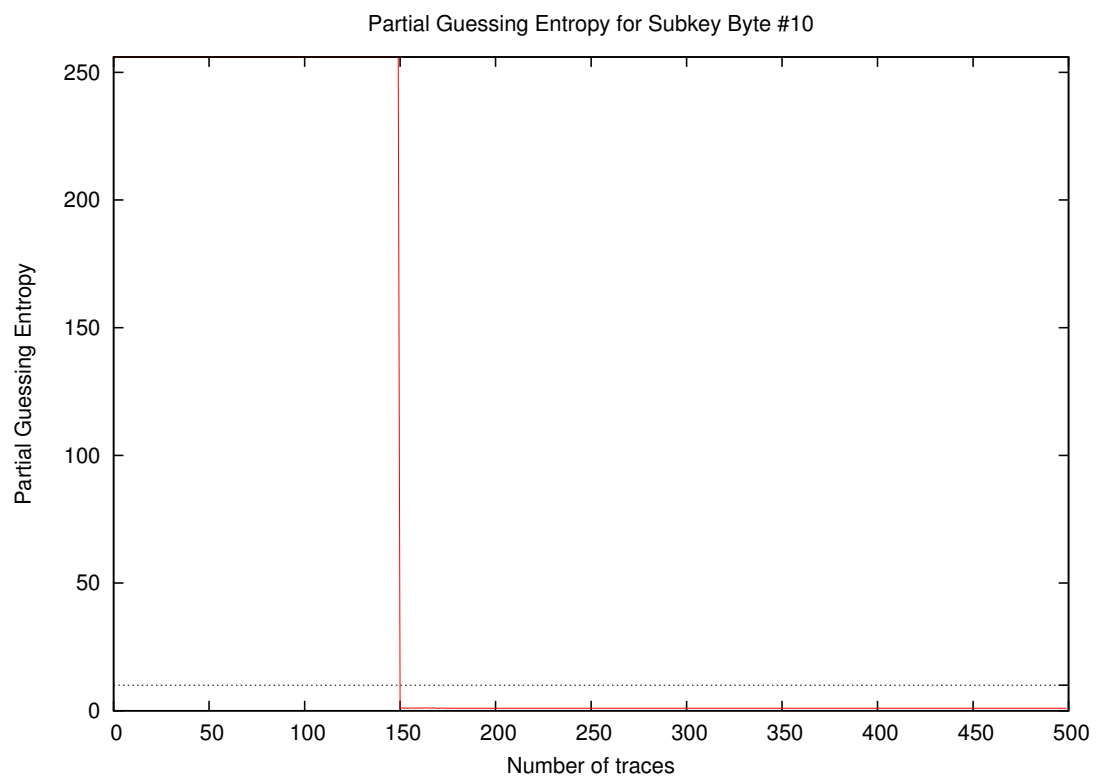
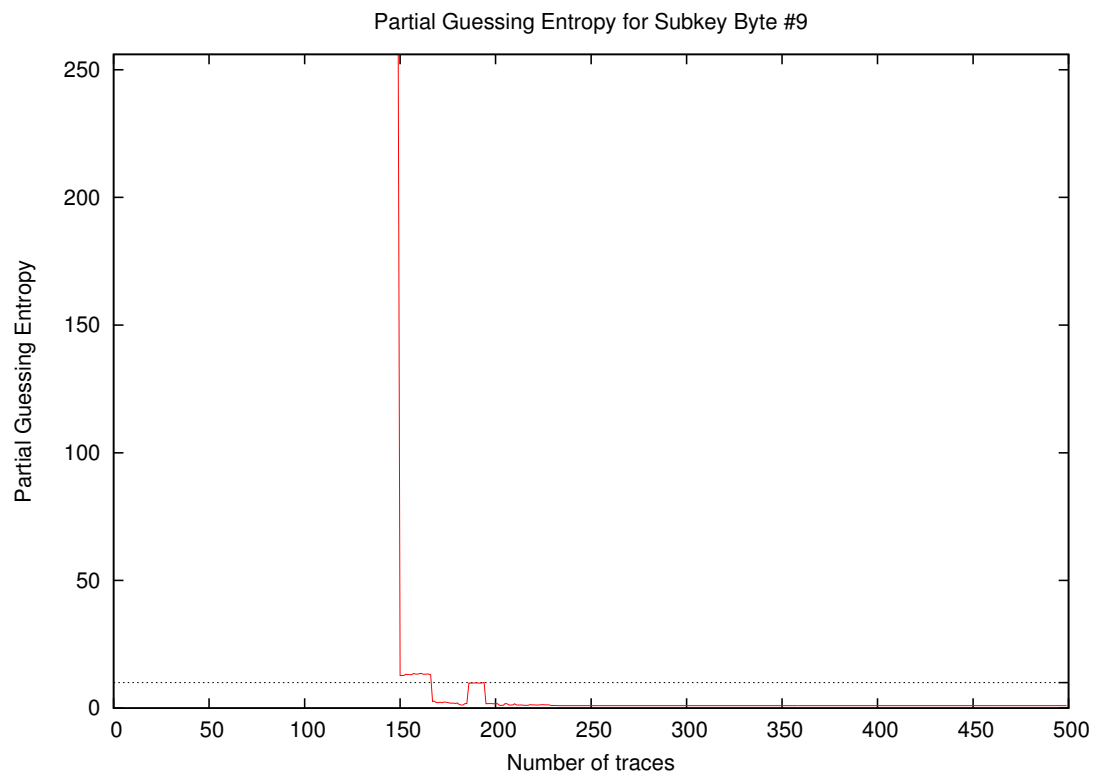


Partial Guessing Entropy for Subkey Byte #7

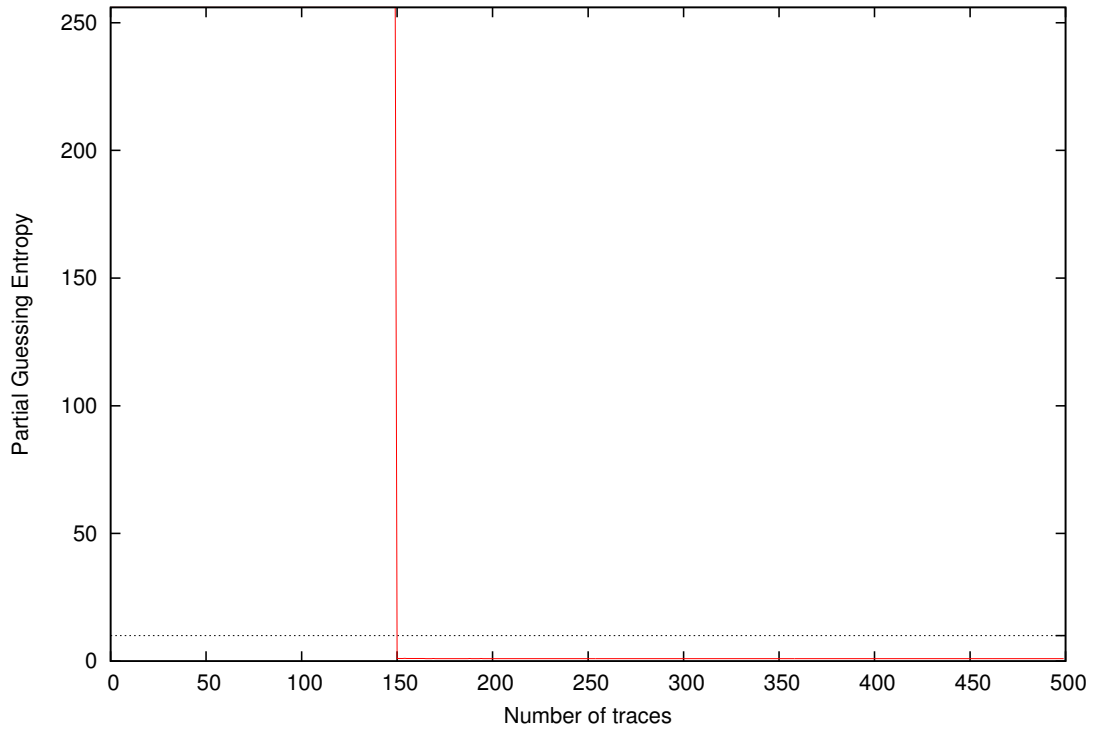


Partial Guessing Entropy for Subkey Byte #8

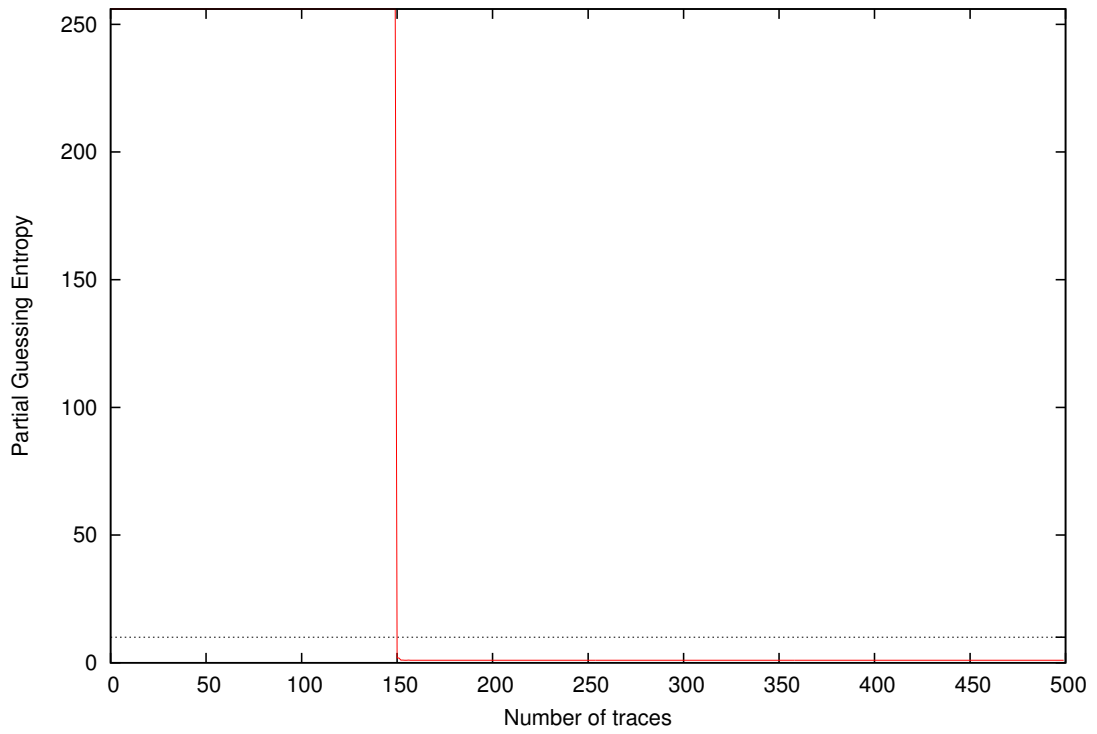




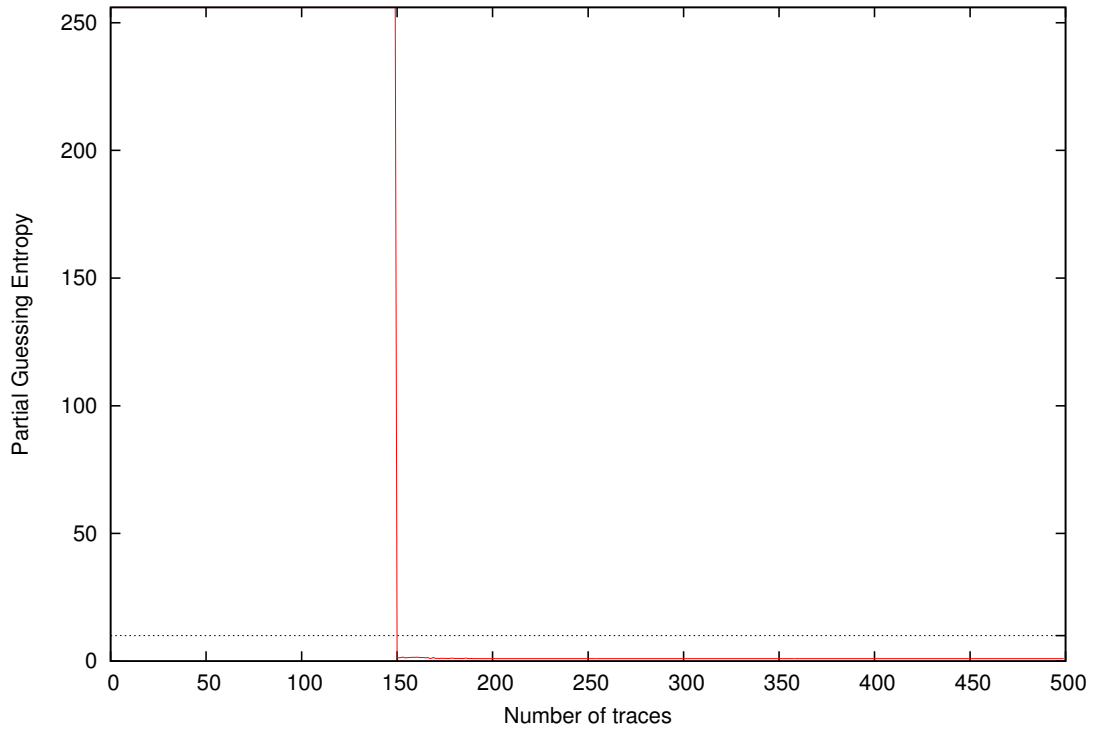
Partial Guessing Entropy for Subkey Byte #11



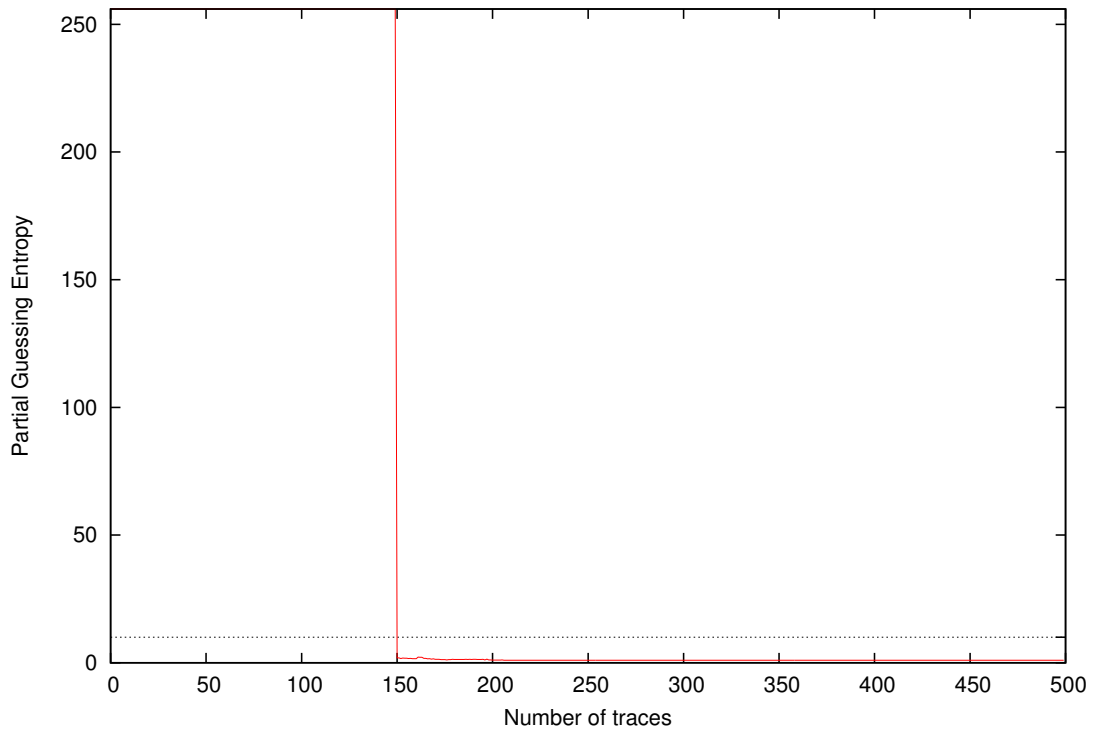
Partial Guessing Entropy for Subkey Byte #12

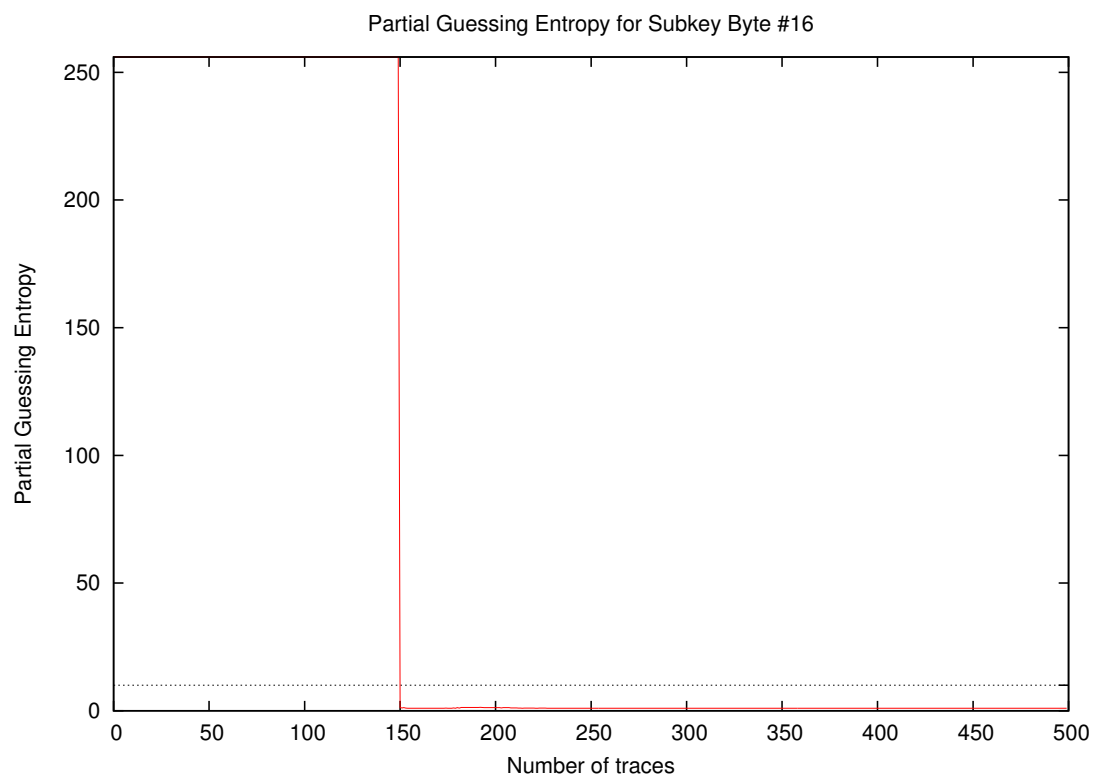
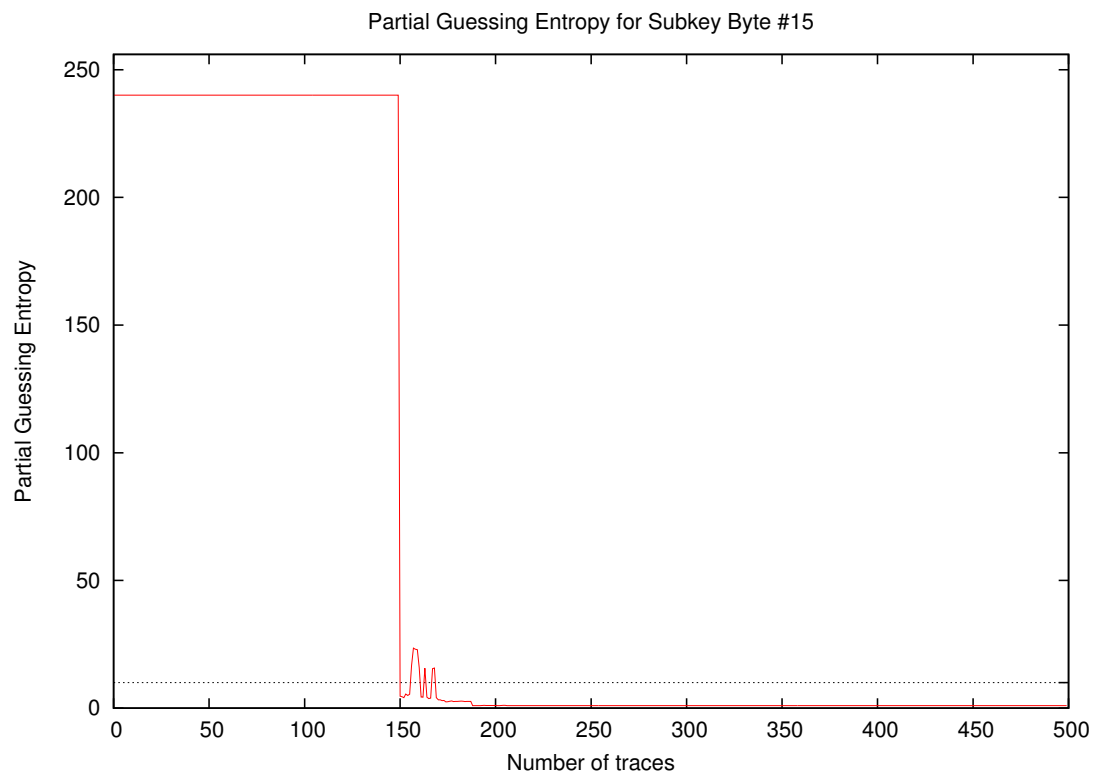


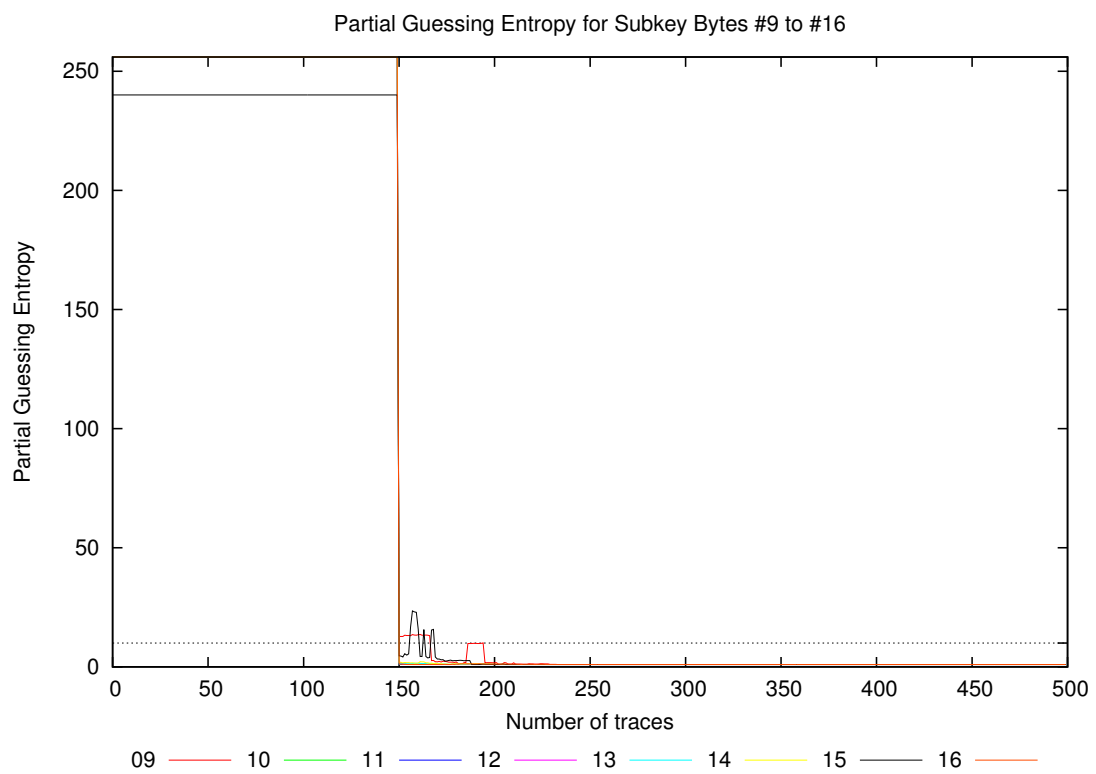
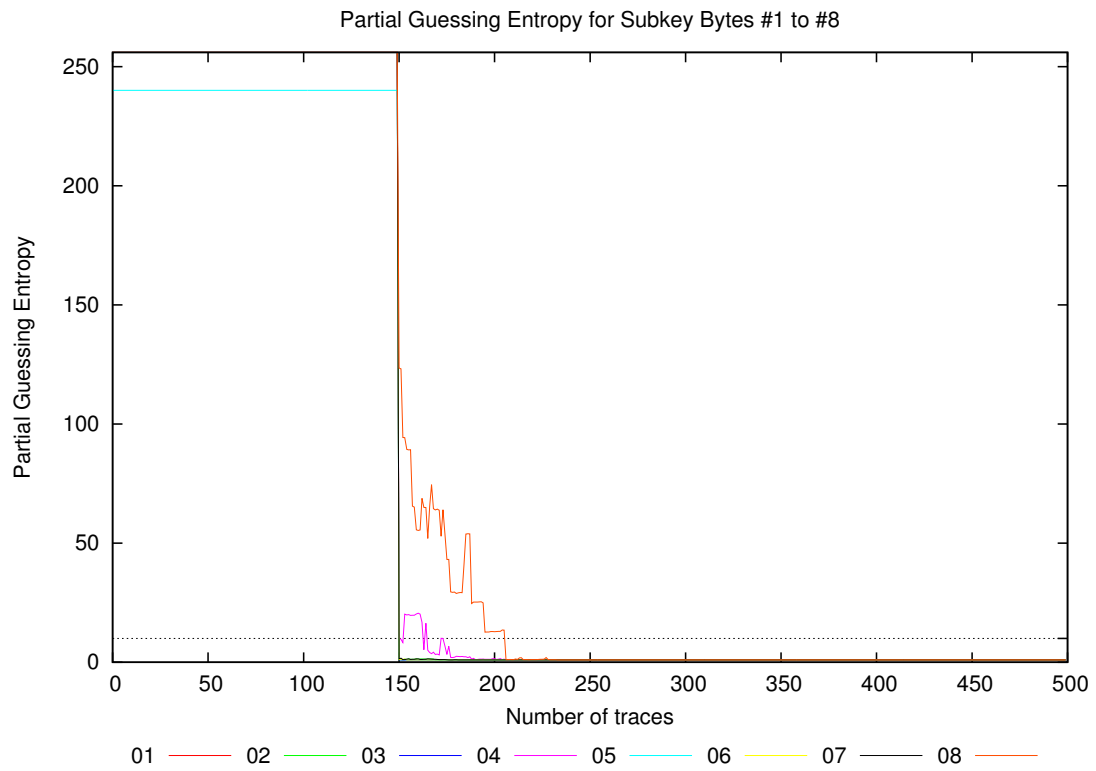
Partial Guessing Entropy for Subkey Byte #13



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	256.0	256.0	256.0	256.0	240.1	256.0	256.0	256.0	256.0	256.0	256.0	256.0	256.0	256.0	240.1	256.0	240.1	256.0	256.0	254.0
20	256.0	256.0	256.0	256.0	240.1	256.0	256.0	256.0	256.0	256.0	256.0	256.0	256.0	256.0	240.1	256.0	240.1	256.0	256.0	254.0
30	256.0	256.0	256.0	256.0	240.1	256.0	256.0	256.0	256.0	256.0	256.0	256.0	256.0	256.0	240.1	256.0	240.1	256.0	256.0	254.0
40	256.0	256.0	256.0	256.0	240.1	256.0	256.0	256.0	256.0	256.0	256.0	256.0	256.0	256.0	240.1	256.0	240.1	256.0	256.0	254.0
50	256.0	256.0	256.0	256.0	240.1	256.0	256.0	256.0	256.0	256.0	256.0	256.0	256.0	256.0	240.1	256.0	240.1	256.0	256.0	254.0
100	256.0	256.0	256.0	256.0	240.1	256.0	256.0	256.0	256.0	256.0	256.0	256.0	256.0	256.0	240.1	256.0	240.1	256.0	256.0	254.0
200	1.0	1.0	1.0	1.5	1.0	1.0	1.0	12.9	1.7	1.0	1.0	1.0	1.0	1.1	1.1	1.1	1.2	1.0	12.9	1.8
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	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	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	1.0