

DPA Contest v4.2

Evaluation results

Zeyi Liu, Yuan Ma, Weijuan Zhang, Xiaona Zhang

February 2016

1 Introduction

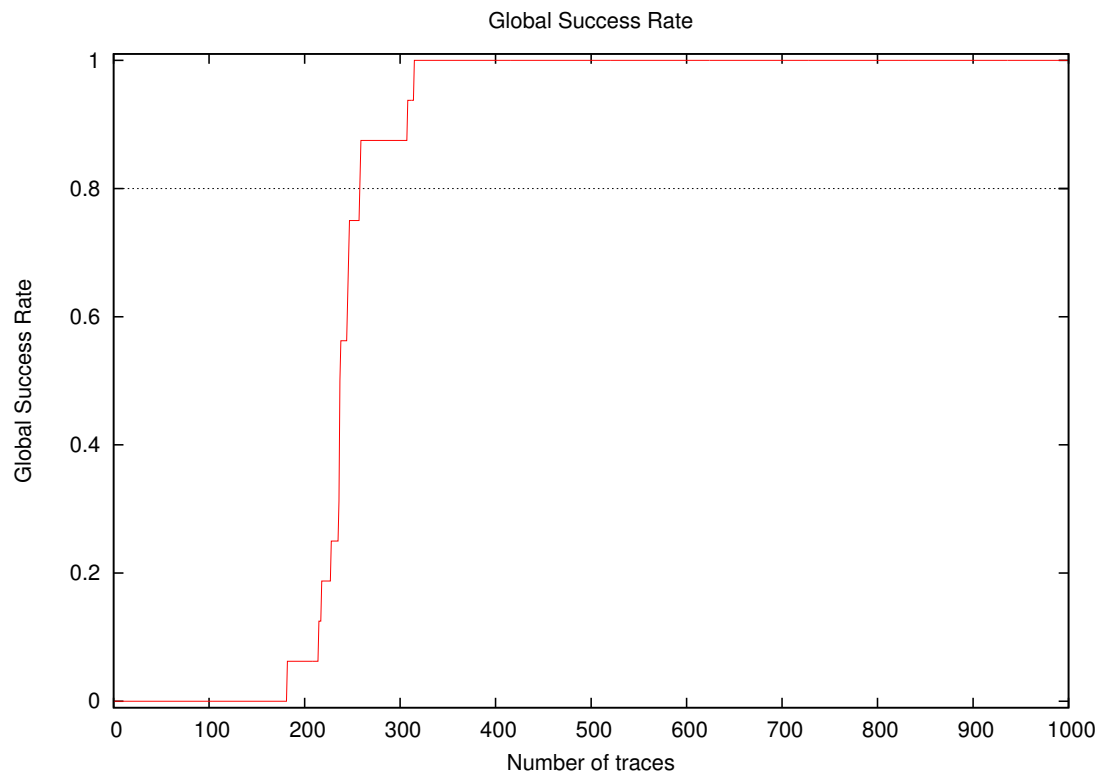
1.1 About the attack

- **Attack Name:** P3
- **Sender/Team:** Zeyi Liu, Yuan Ma, Weijuan Zhang, Xiaona Zhang
- **Institution:** Data Assurance and Communication Security Research Center, CAS, China
- **Language:** C#
- **Operating system:** Windows
- **Attacked subkey:** 0

1.2 About the evaluation

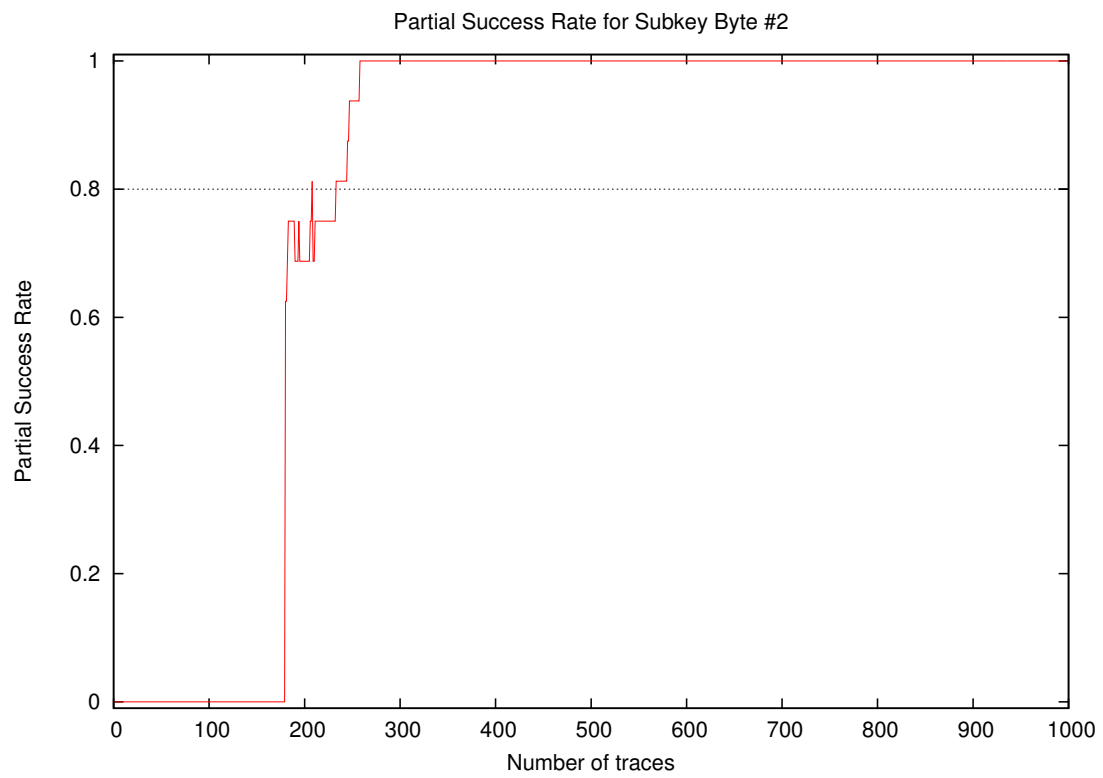
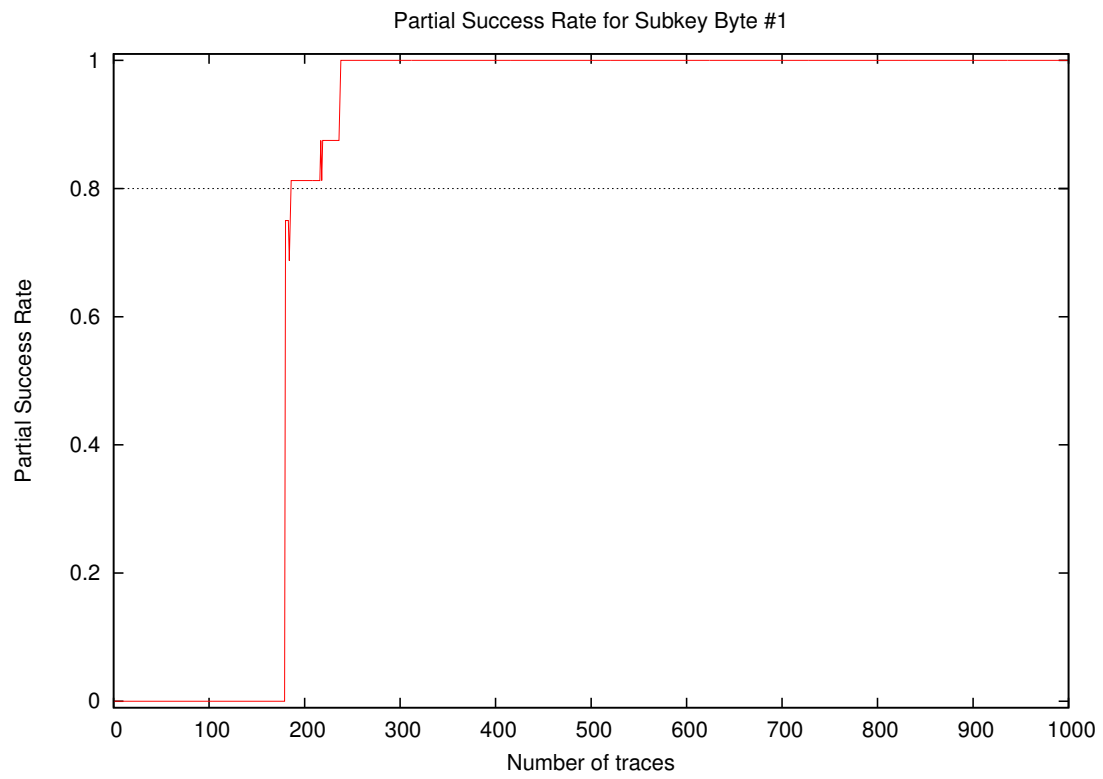
- **Date of evaluation:** February 2016

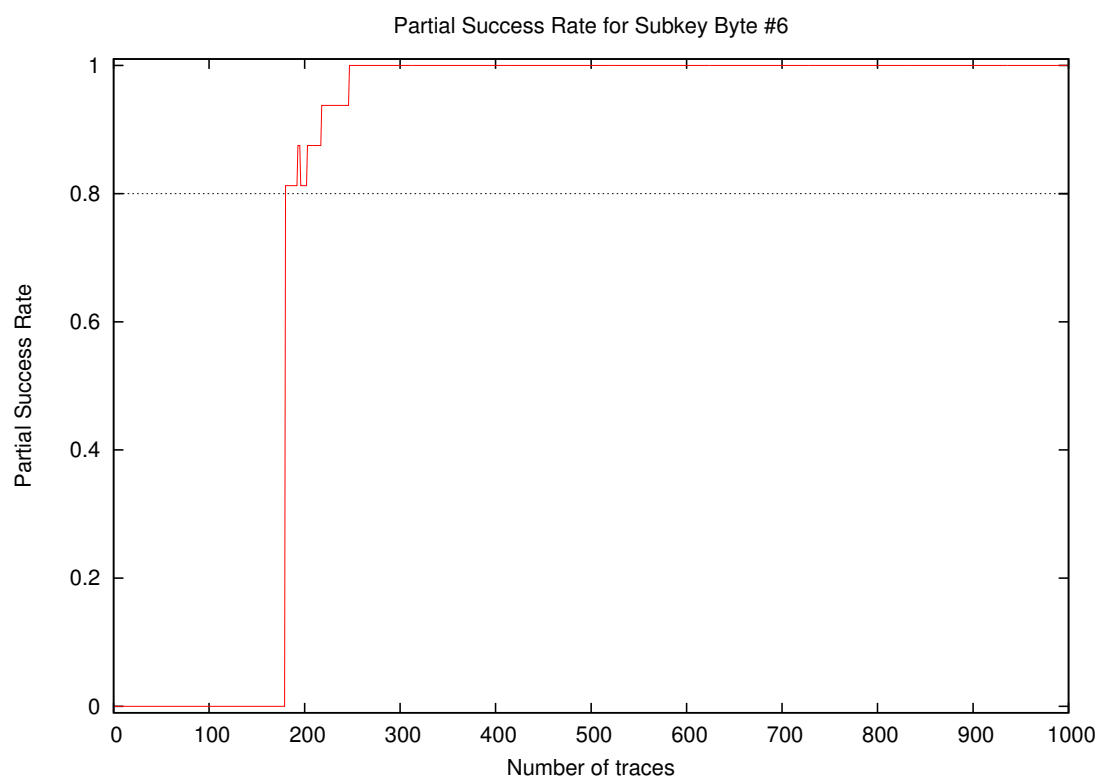
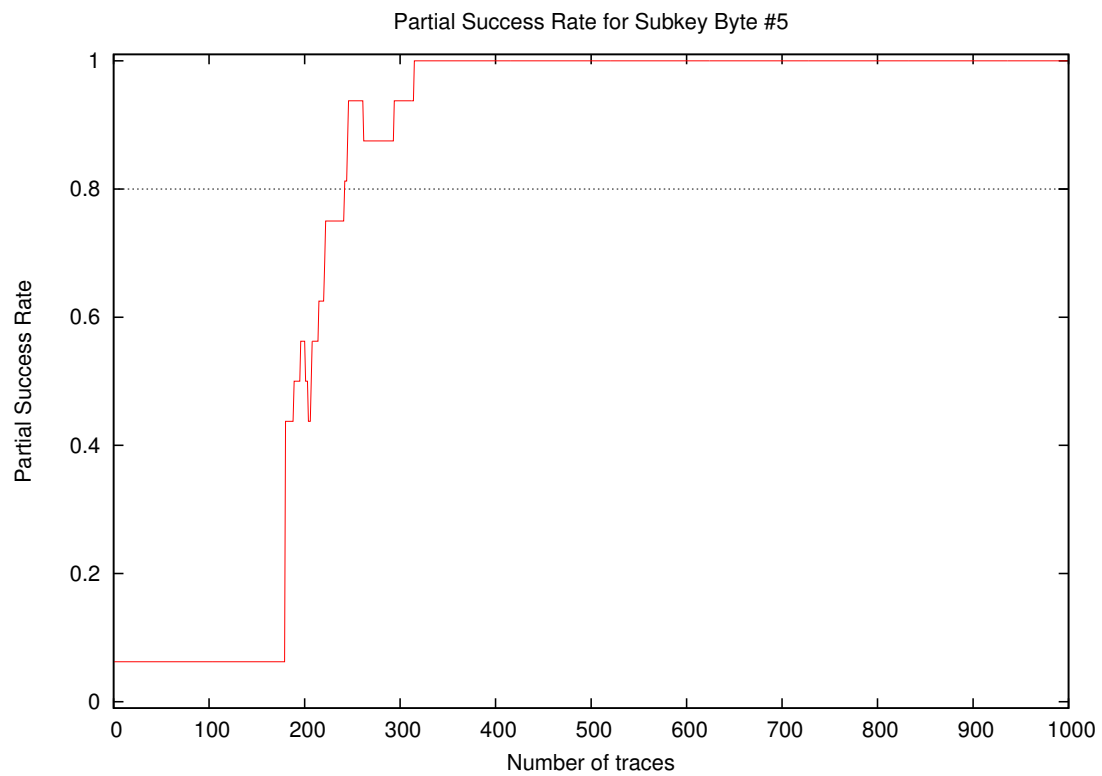
2 Global Success Rate

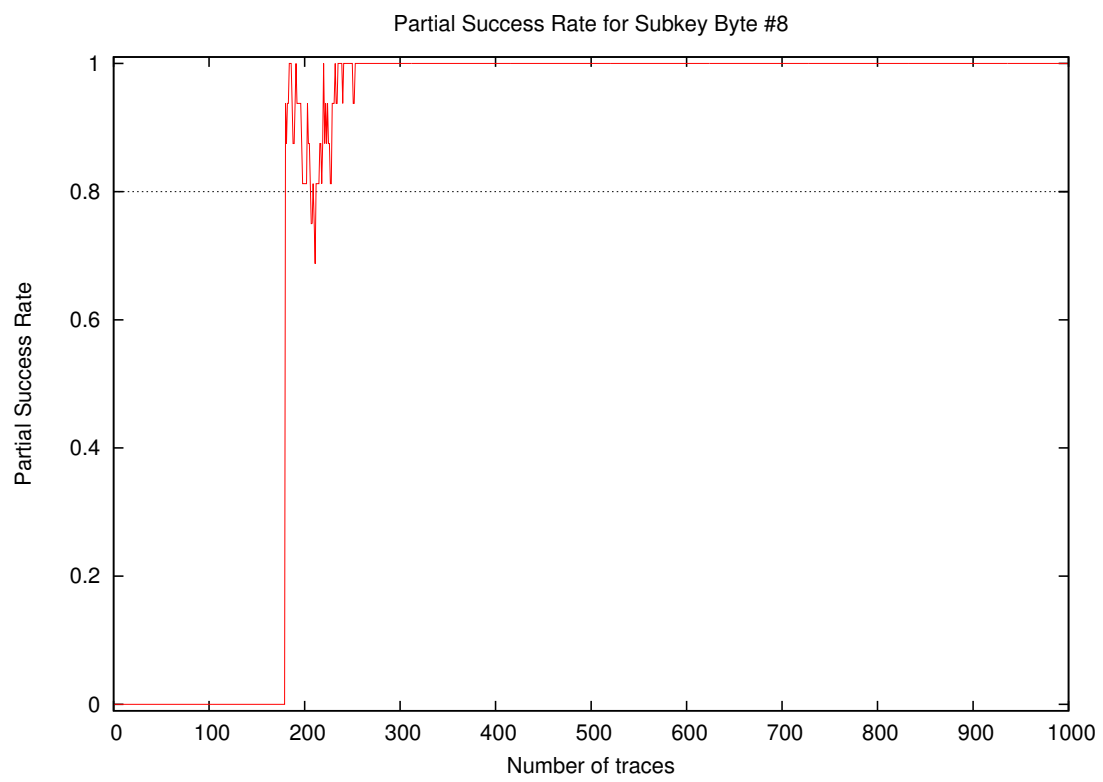
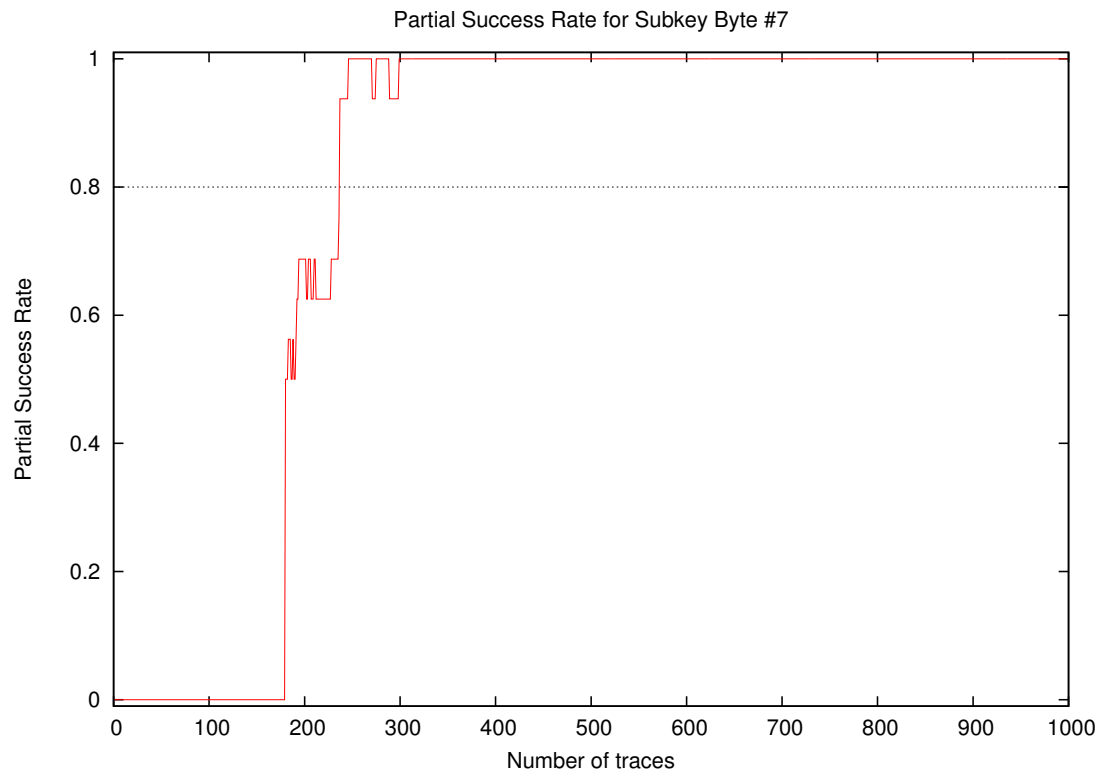


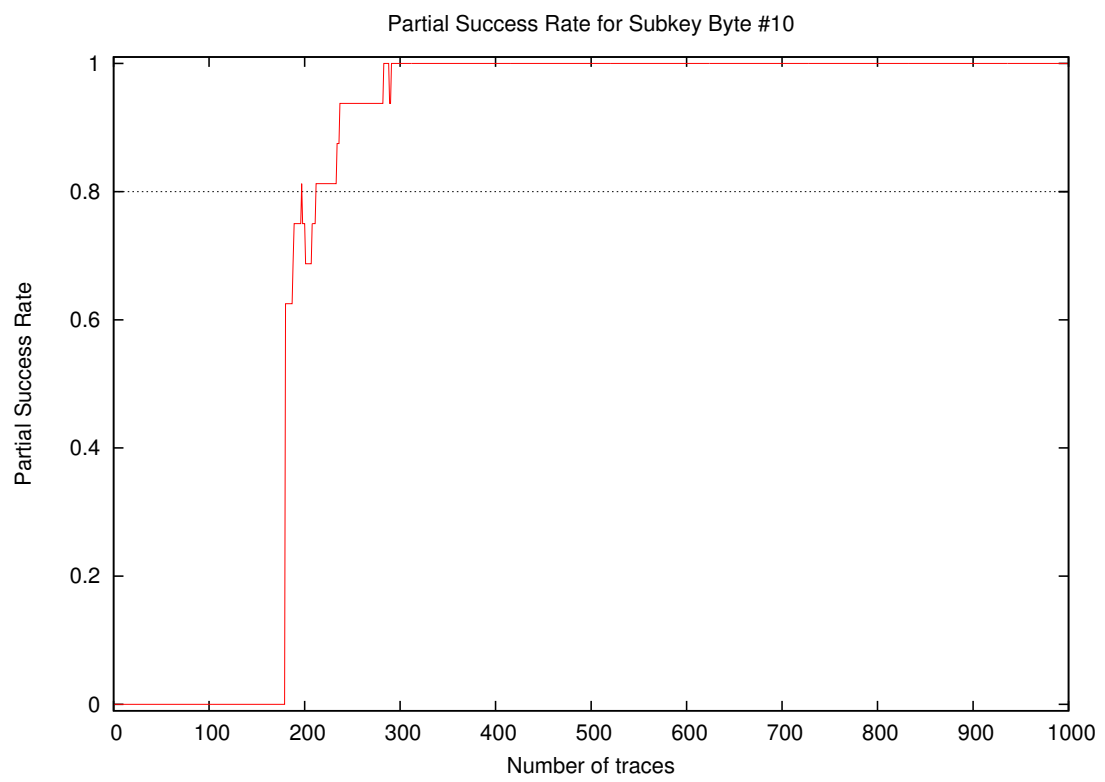
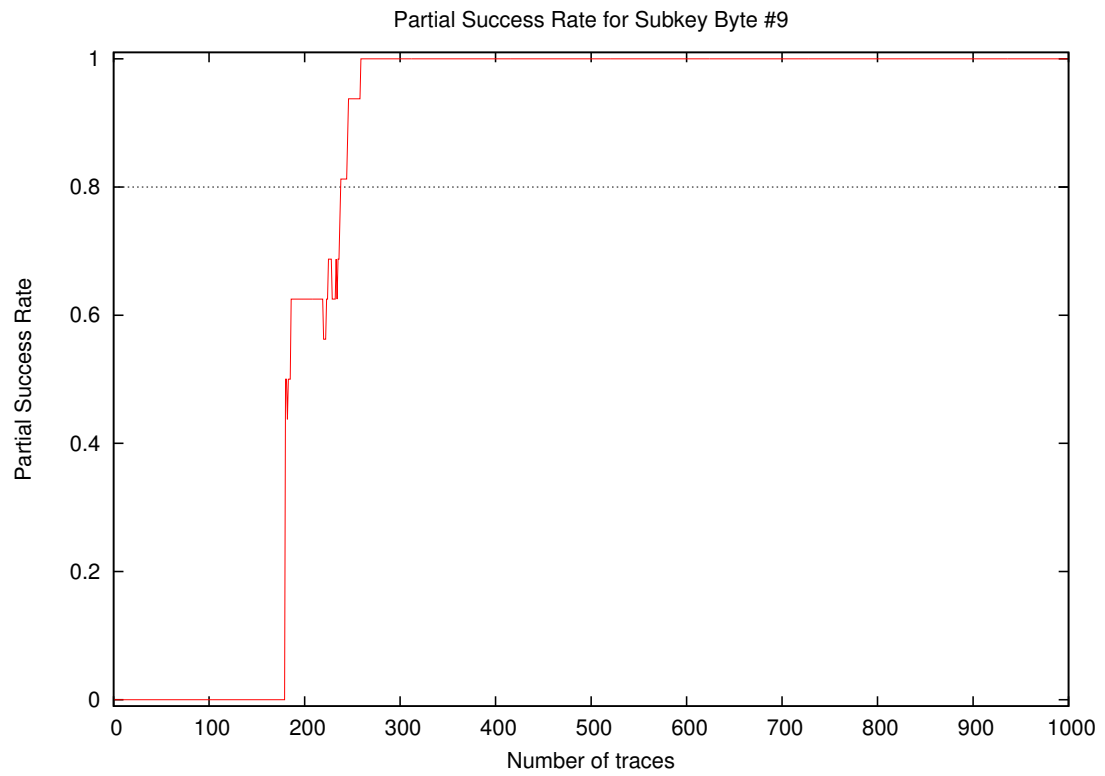
Number of traces	Global Success Rate
10	0.00
20	0.00
30	0.00
40	0.00
50	0.00
100	0.00
200	0.06
300	0.88
400	1.00
500	1.00
600	1.00
700	1.00
800	1.00
900	1.00
1000	1.00

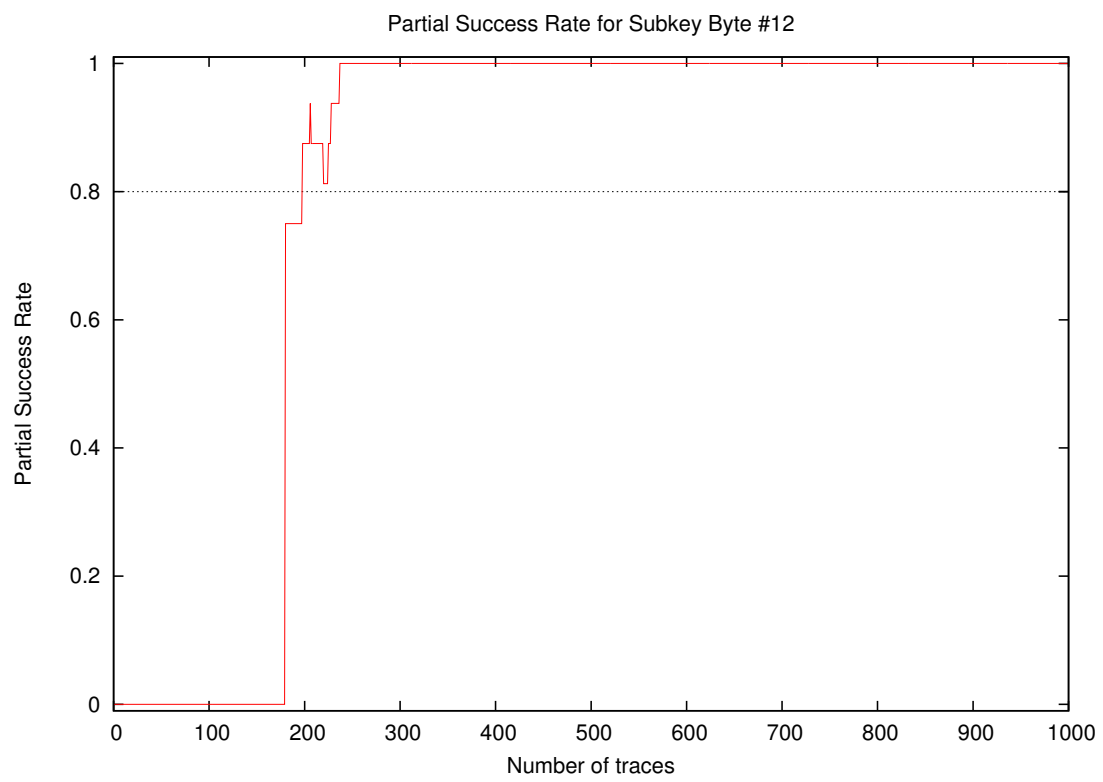
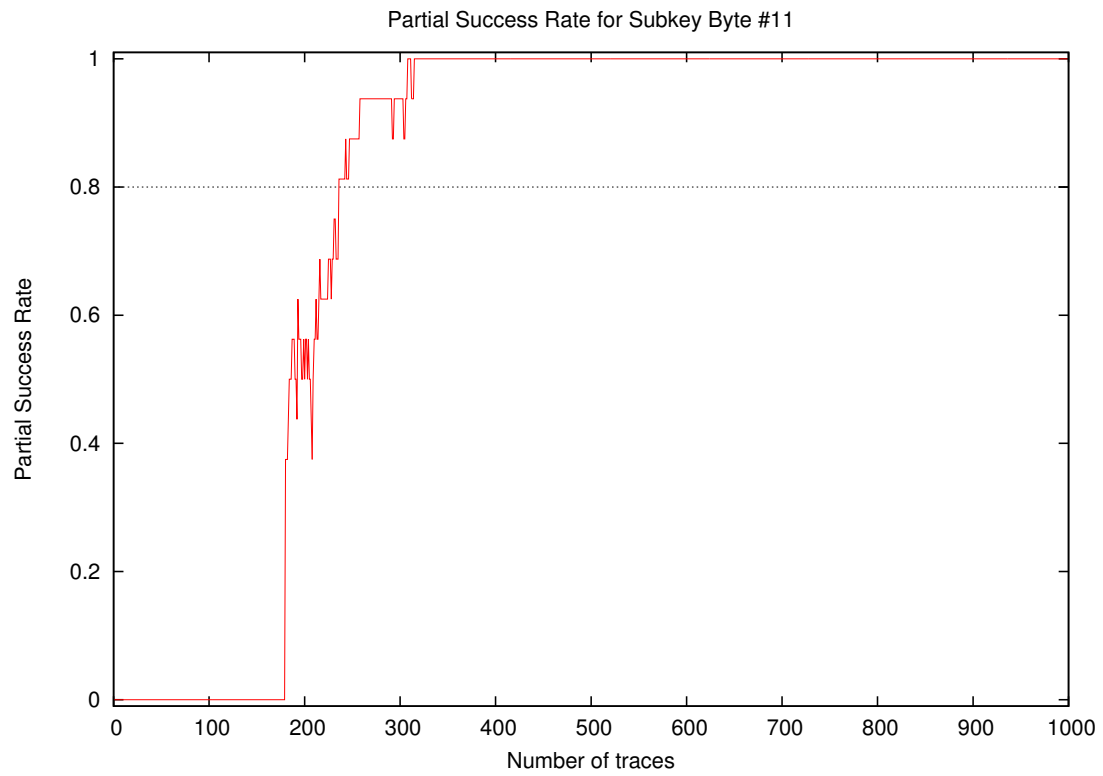
3 Partial Success Rate

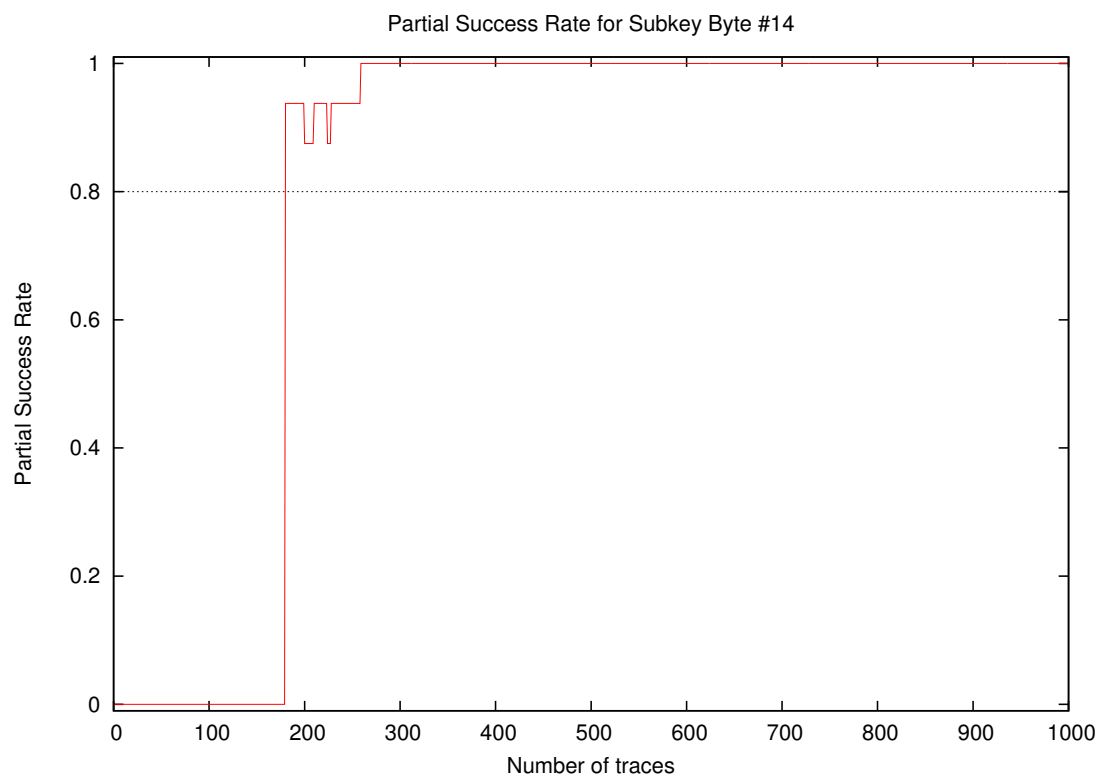
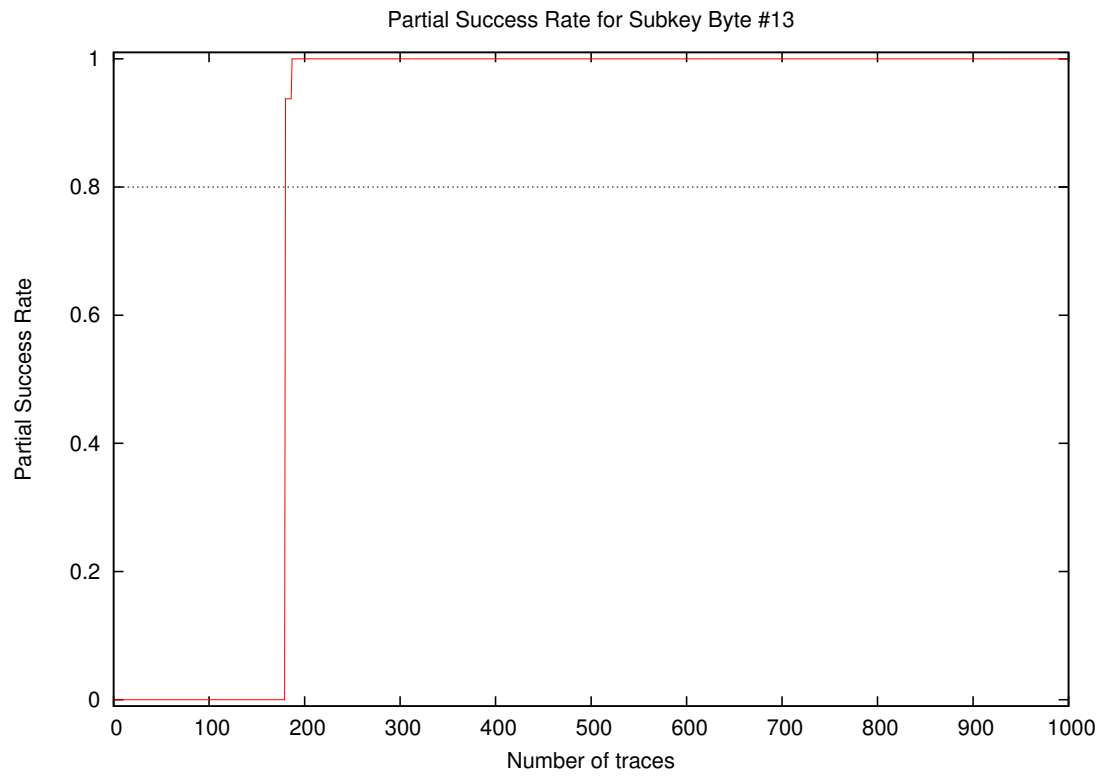


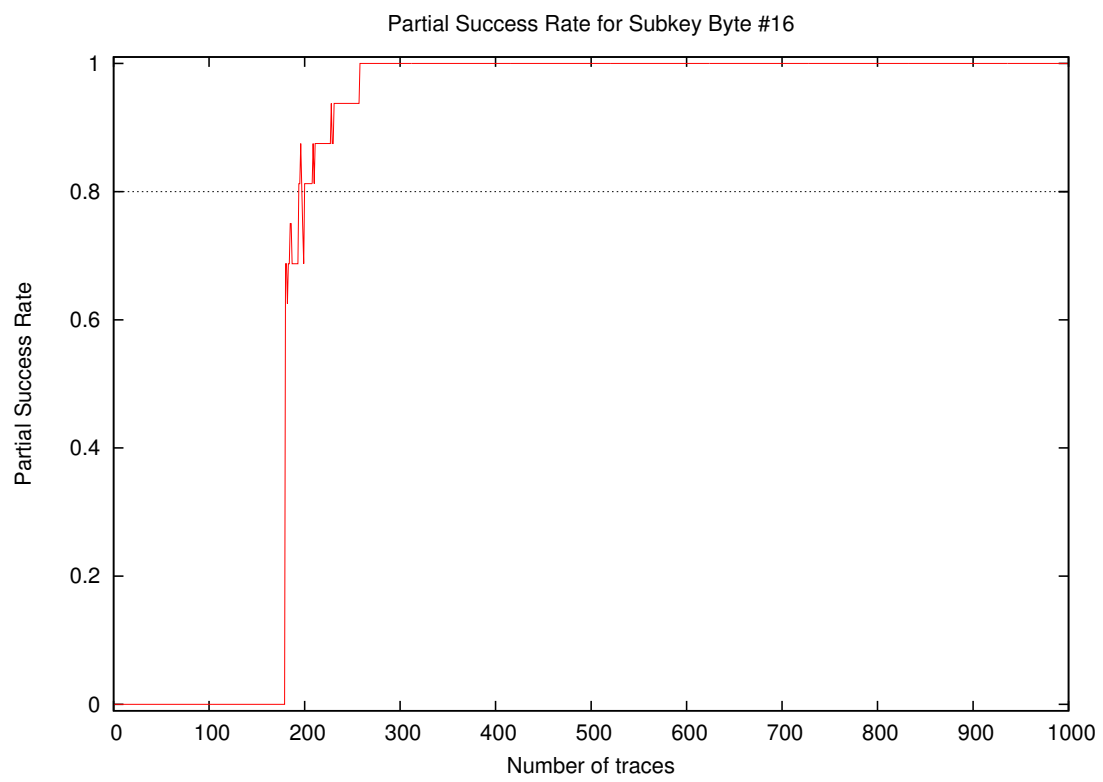
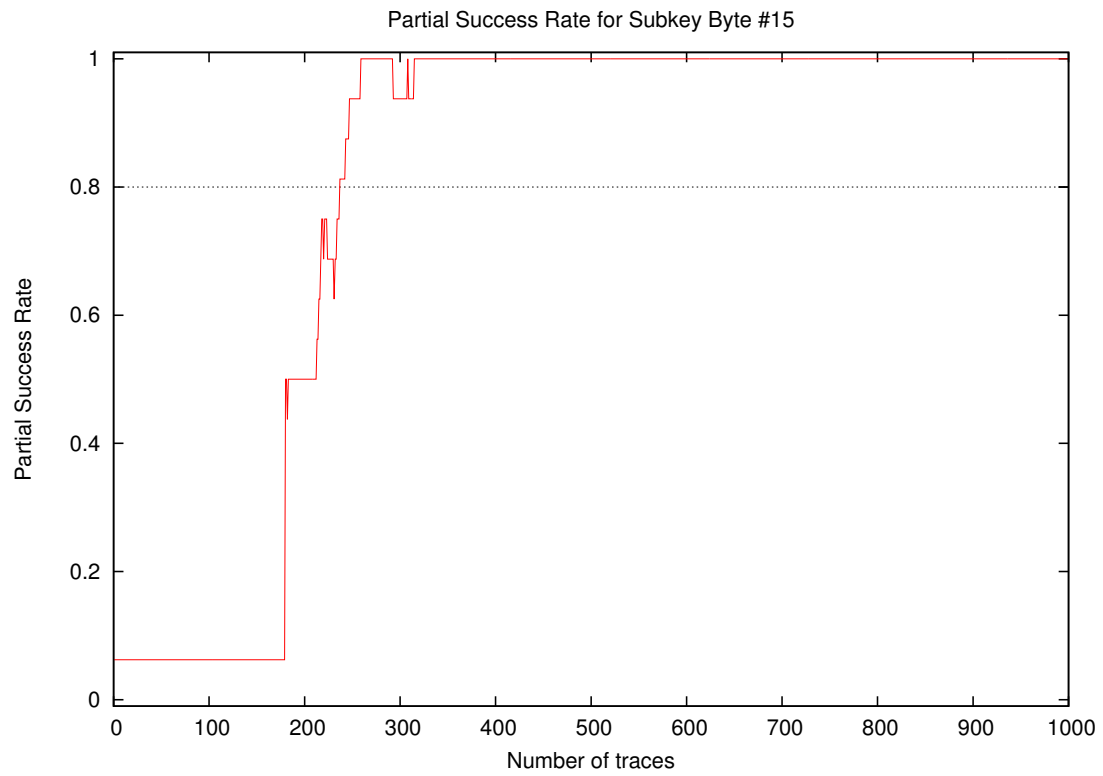




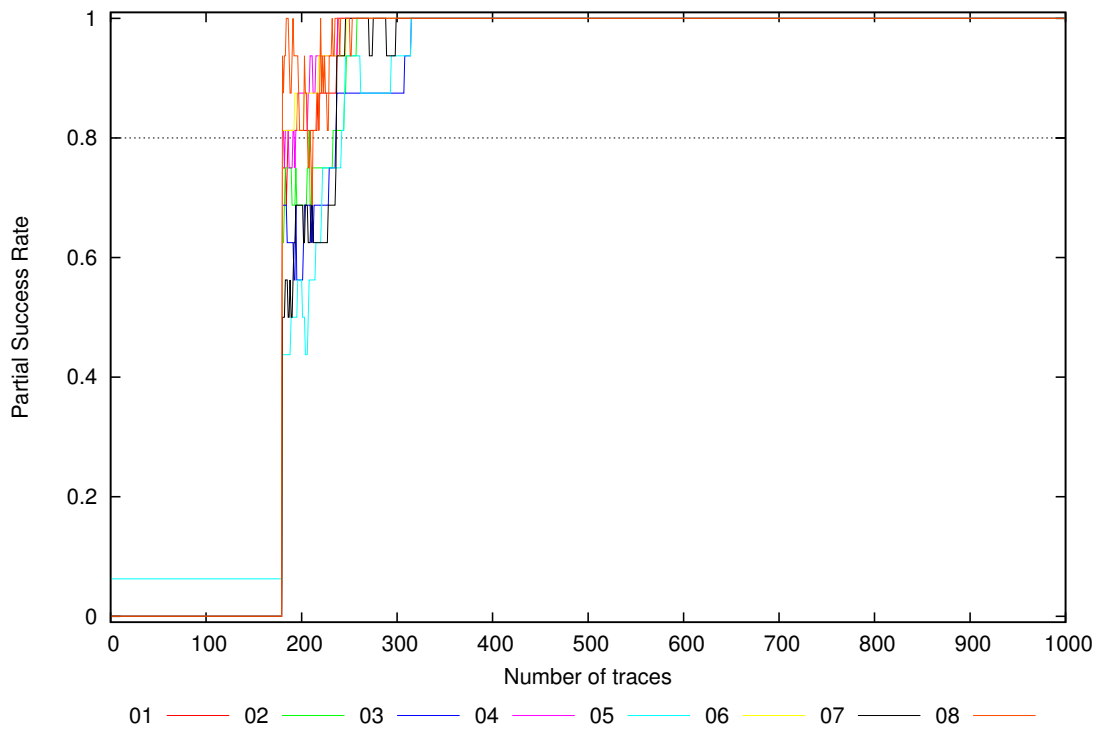




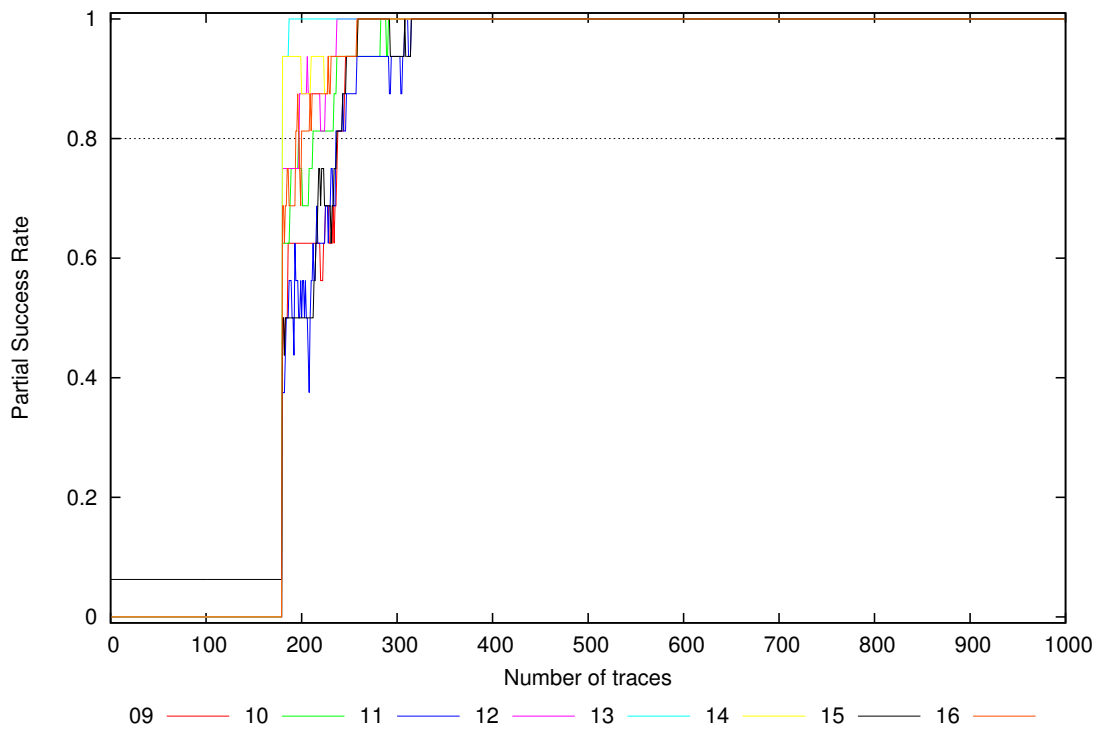




Partial Success Rate for Subkey Bytes #1 to #8

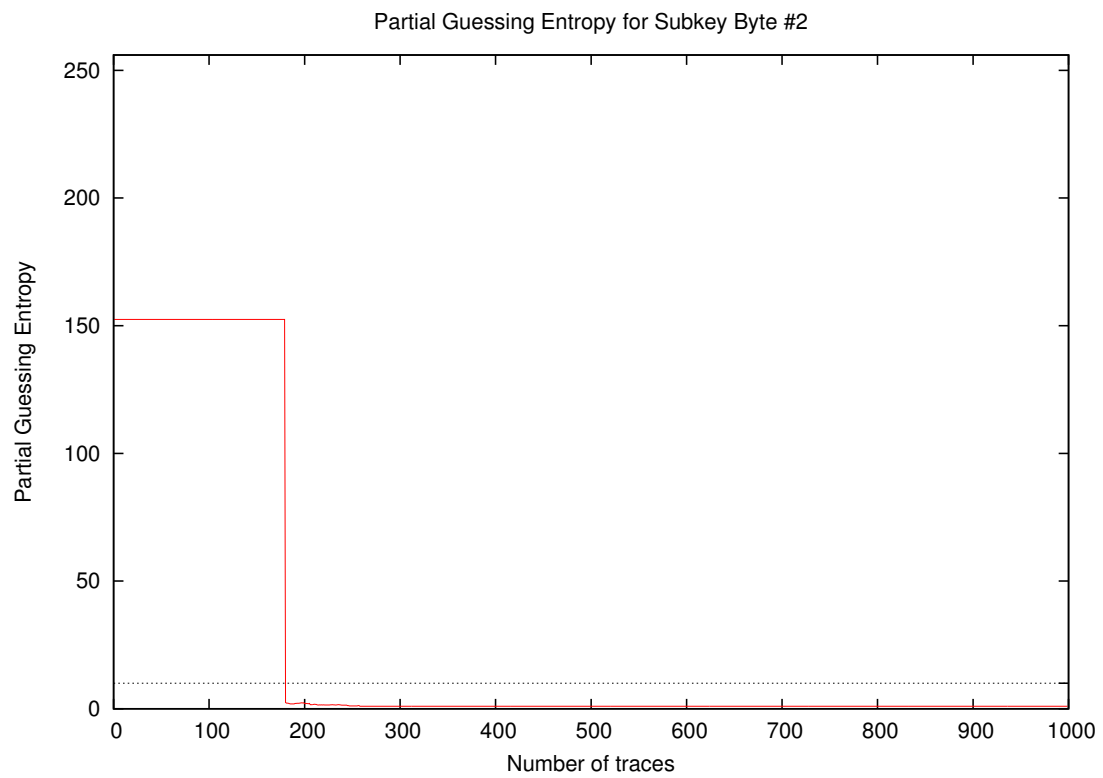
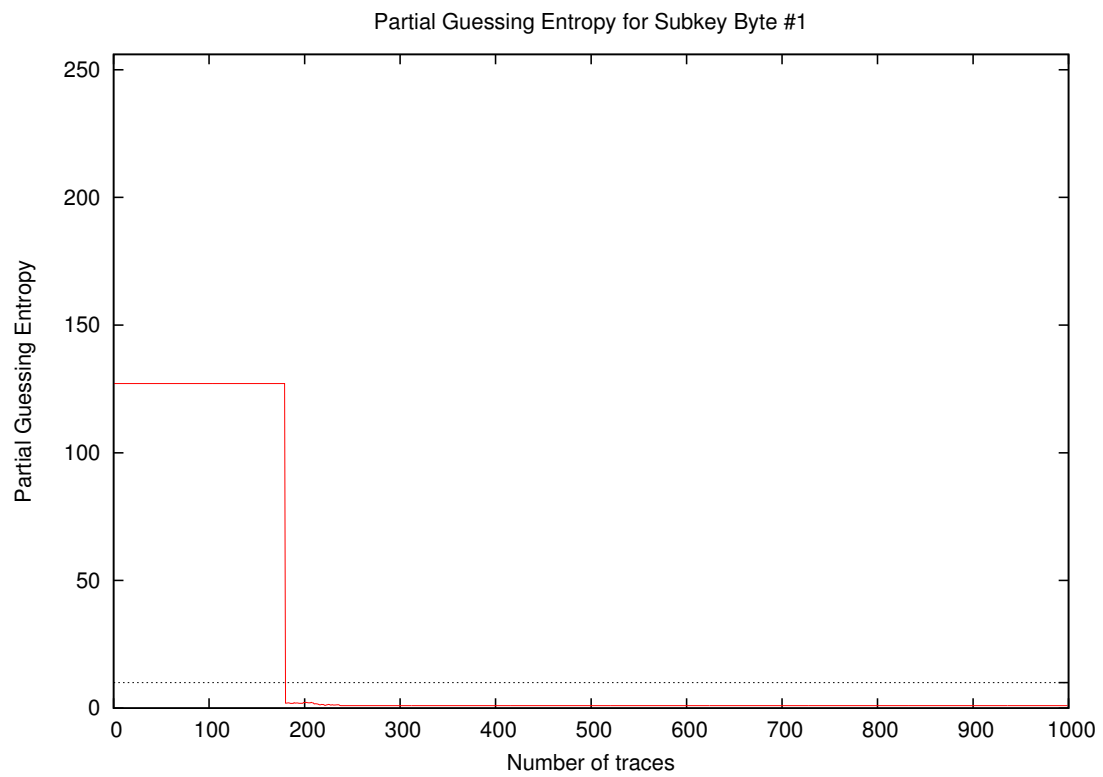


Partial Success Rate for Subkey Bytes #9 to #16

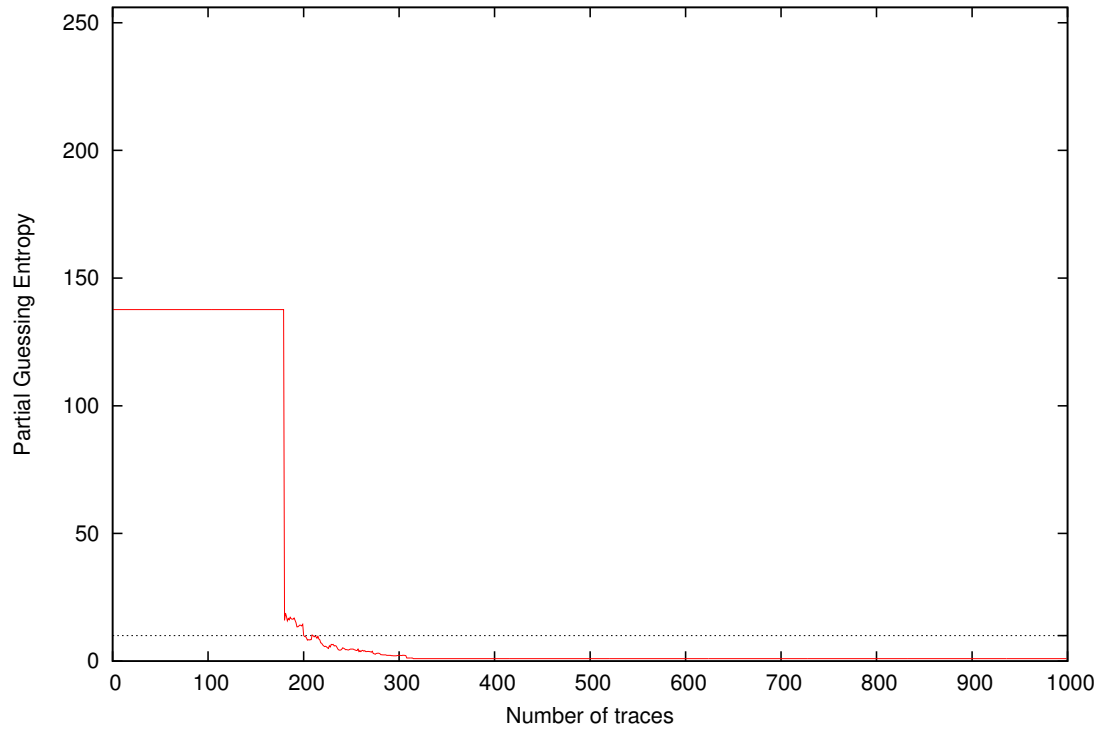


Traces	Partial Success Rate / Byte																Min	Max	Mean
	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16			
10	0.00	0.00	0.00	0.00	0.06	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.06	0.00	0.00	0.06	0.01
20	0.00	0.00	0.00	0.00	0.06	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.06	0.00	0.00	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	0.81	0.69	0.56	0.88	0.56	0.81	0.69	0.81	0.62	0.75	0.56	0.88	1.00	0.94	0.50	0.69	0.50	1.00	0.73
300	1.00	1.00	0.88	1.00	0.94	1.00	1.00	1.00	1.00	1.00	0.94	1.00	1.00	1.00	0.94	1.00	0.88	1.00	0.98
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
600	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
700	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
800	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
900	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
1000	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

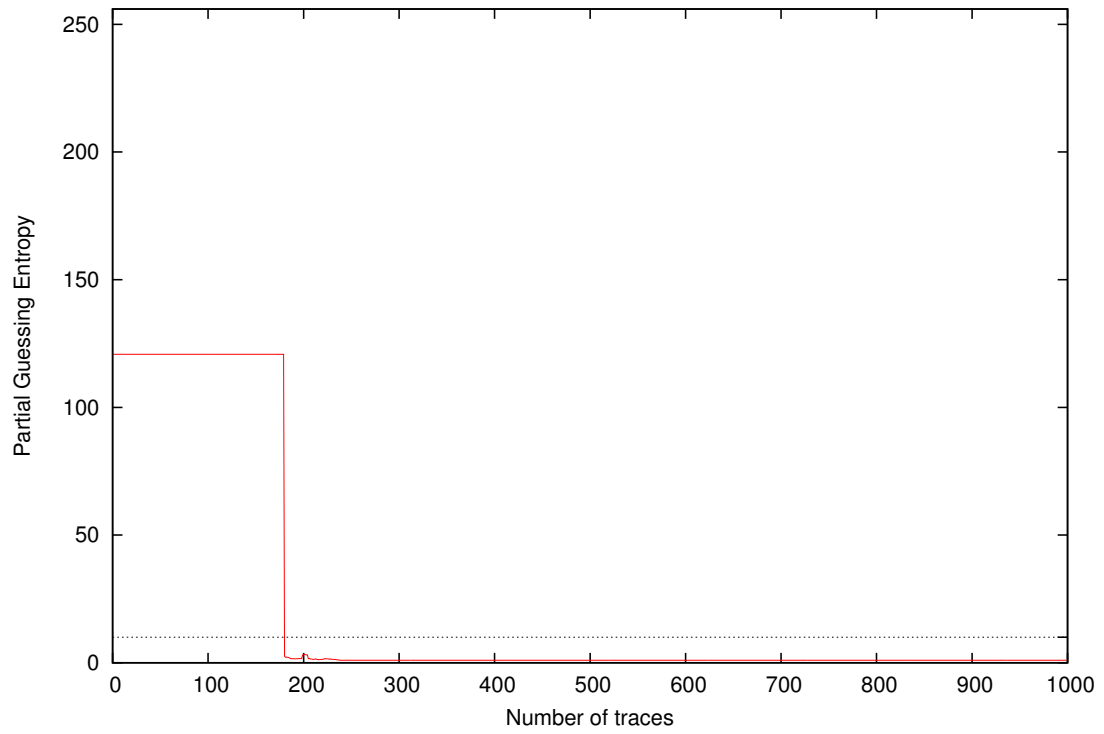
4 Partial Guessing Entropy



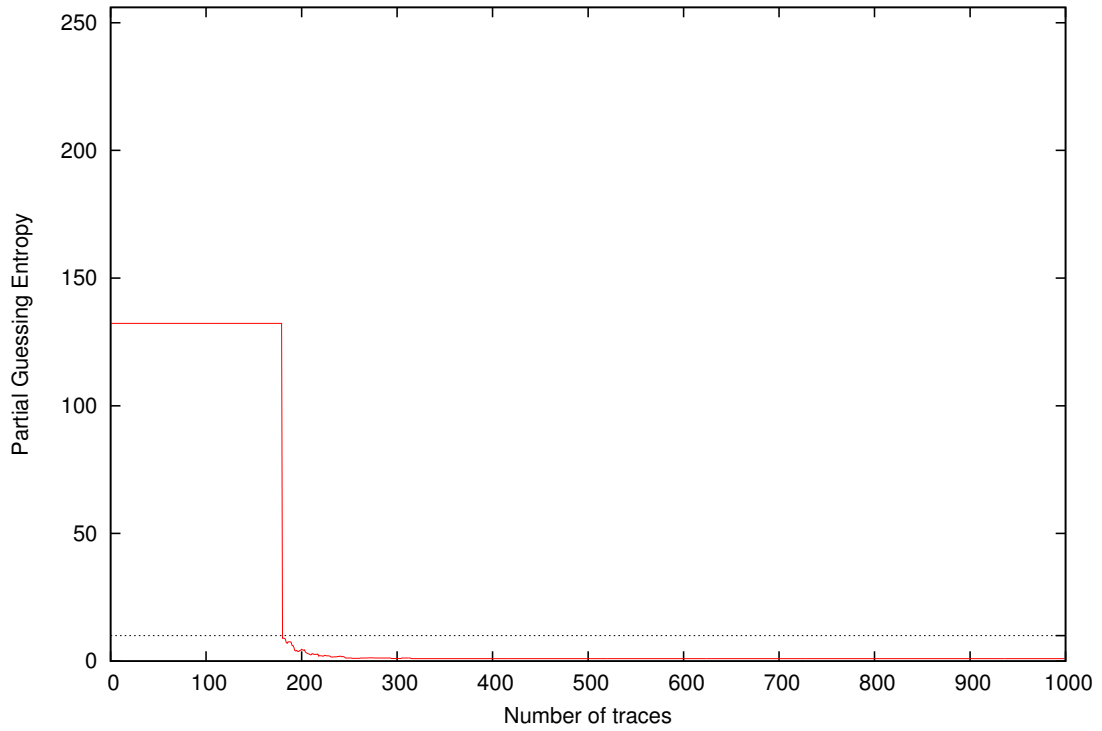
Partial Guessing Entropy for Subkey Byte #3



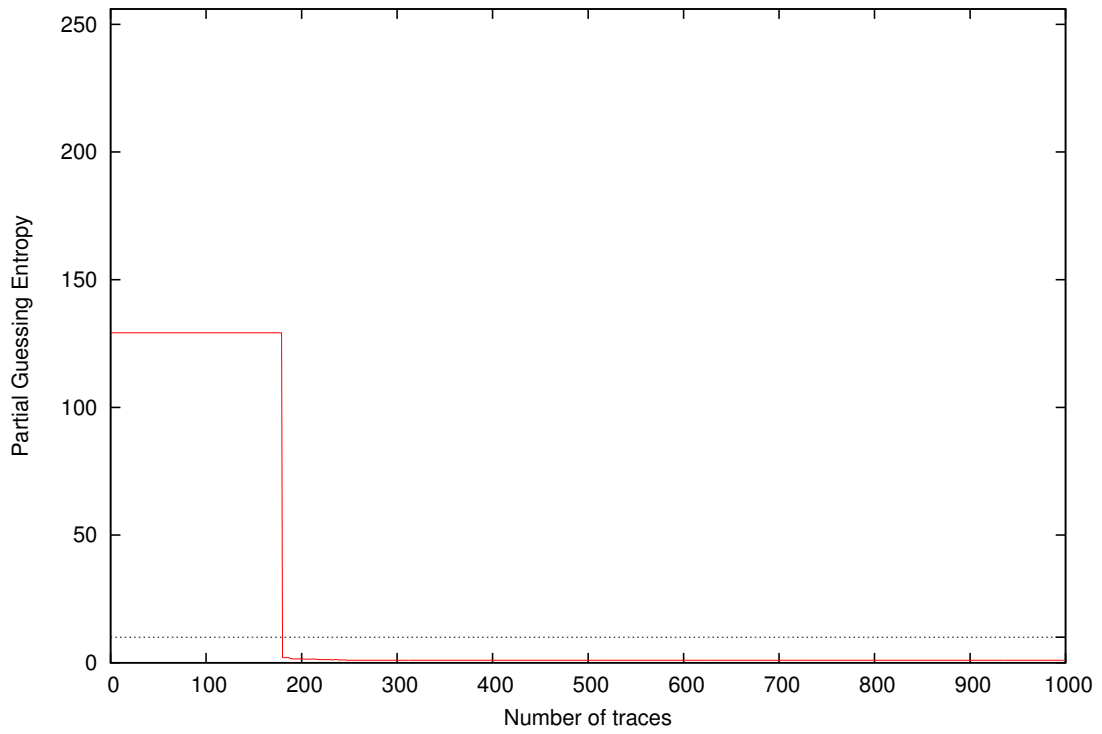
Partial Guessing Entropy for Subkey Byte #4



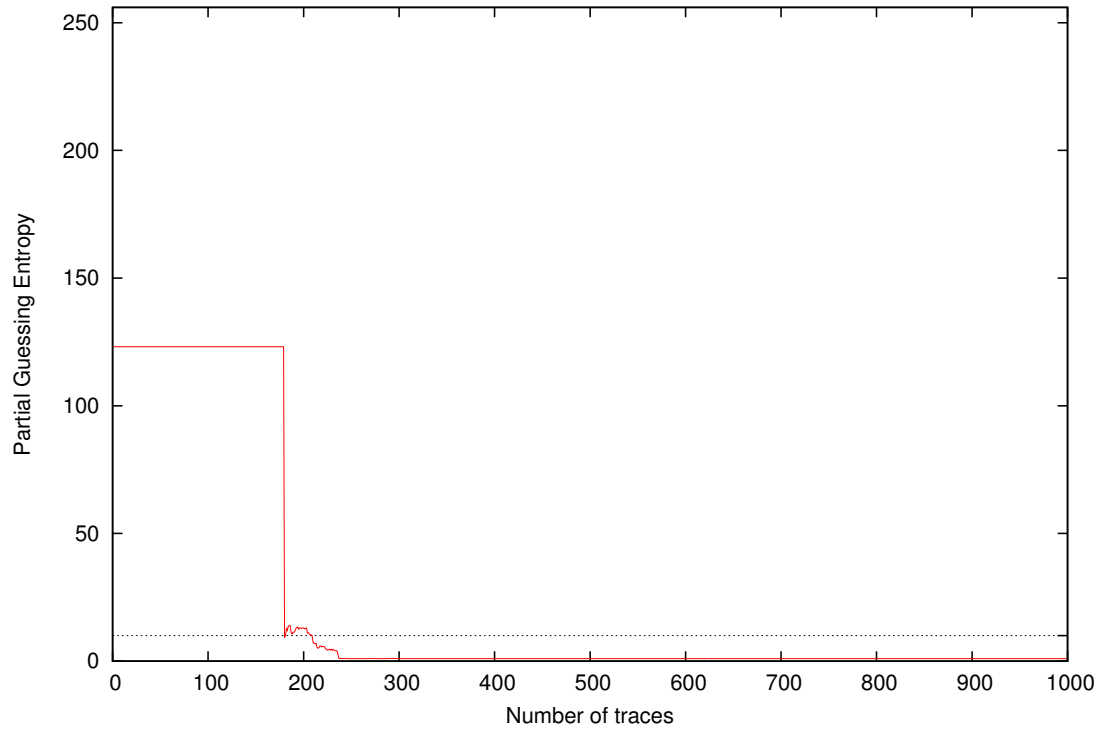
Partial Guessing Entropy for Subkey Byte #5



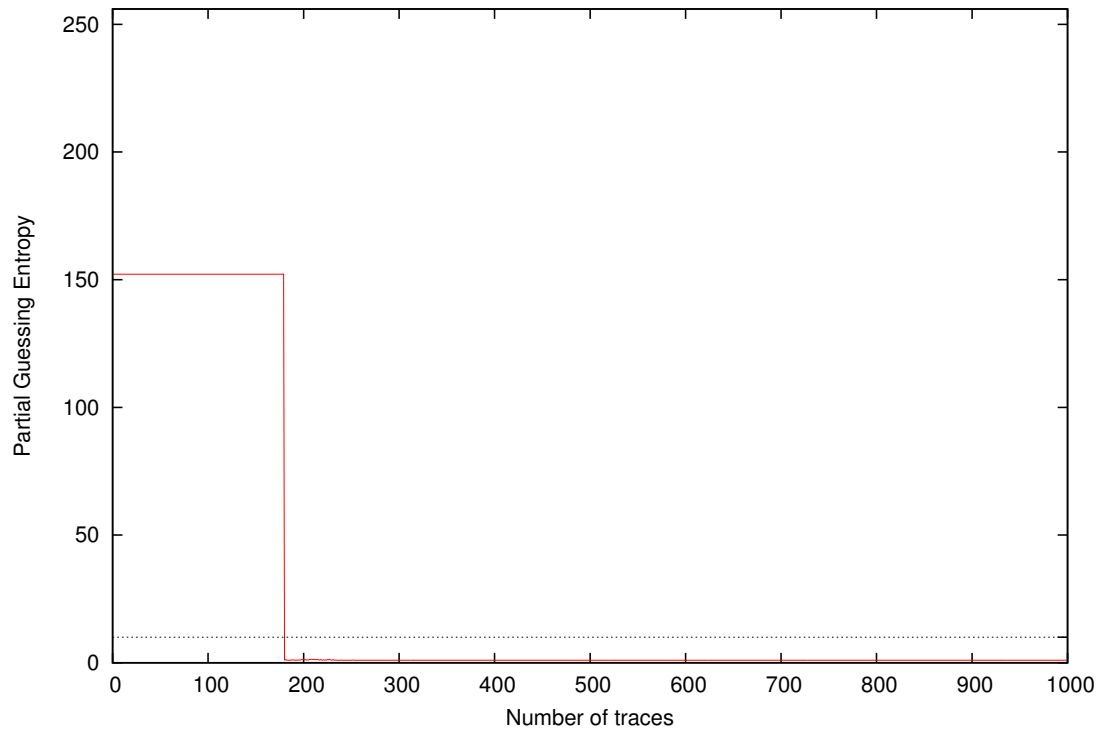
Partial Guessing Entropy for Subkey Byte #6



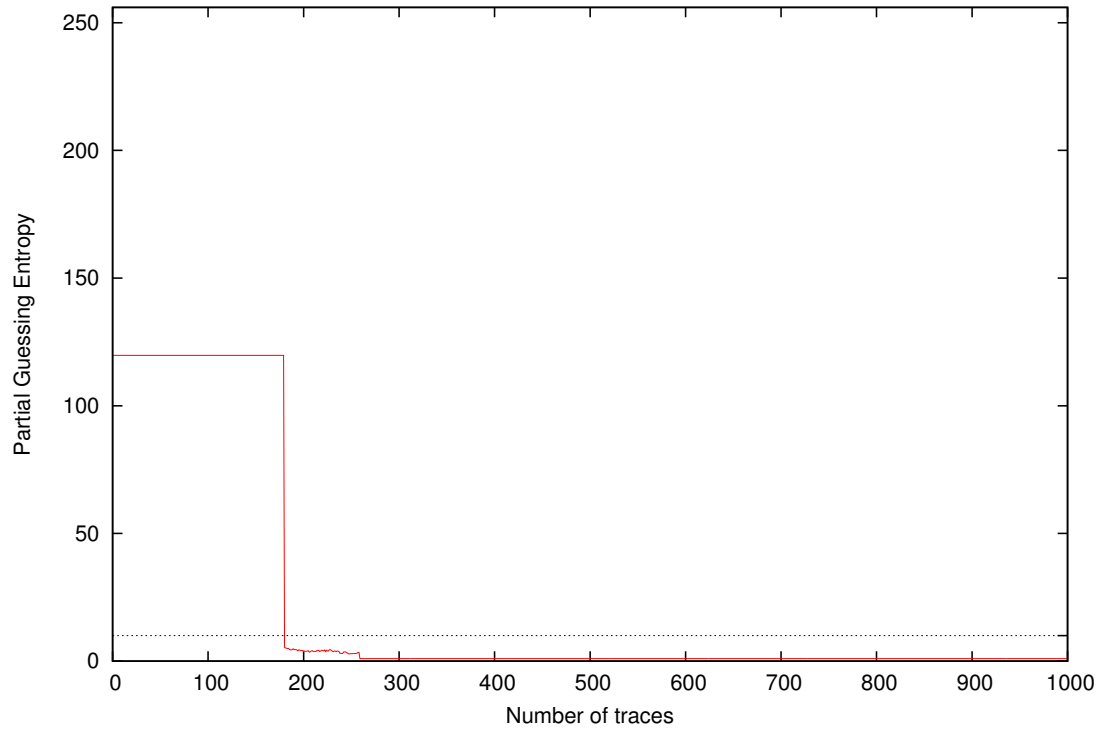
Partial Guessing Entropy for Subkey Byte #7



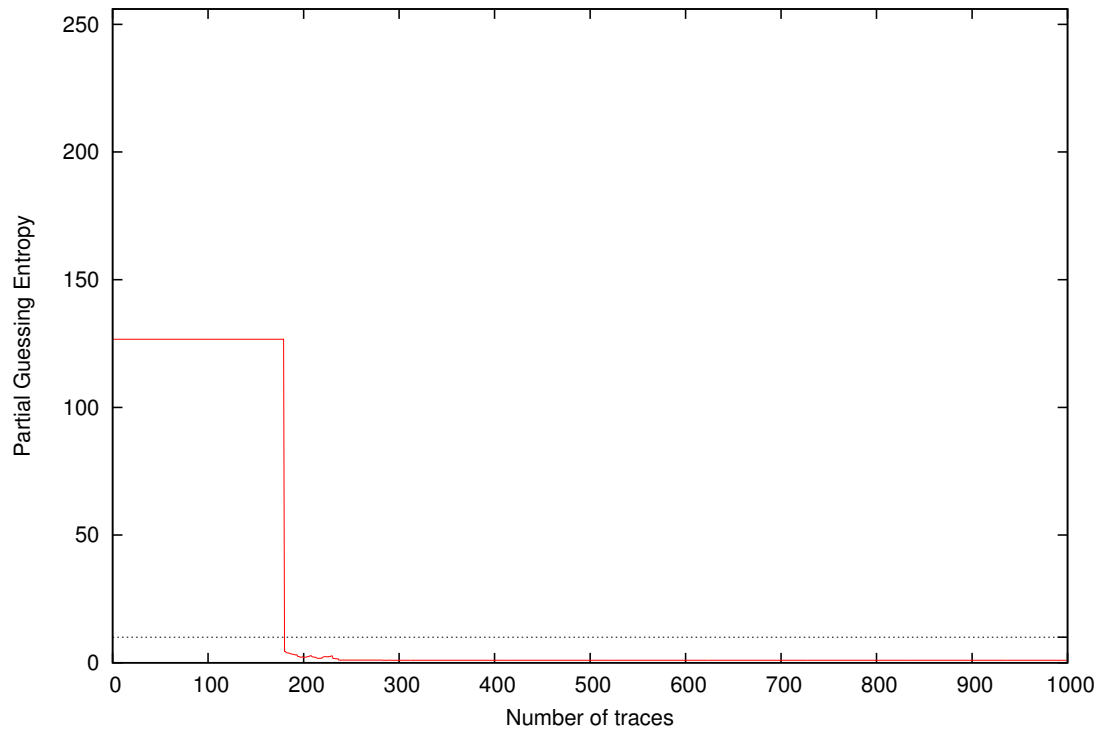
Partial Guessing Entropy for Subkey Byte #8



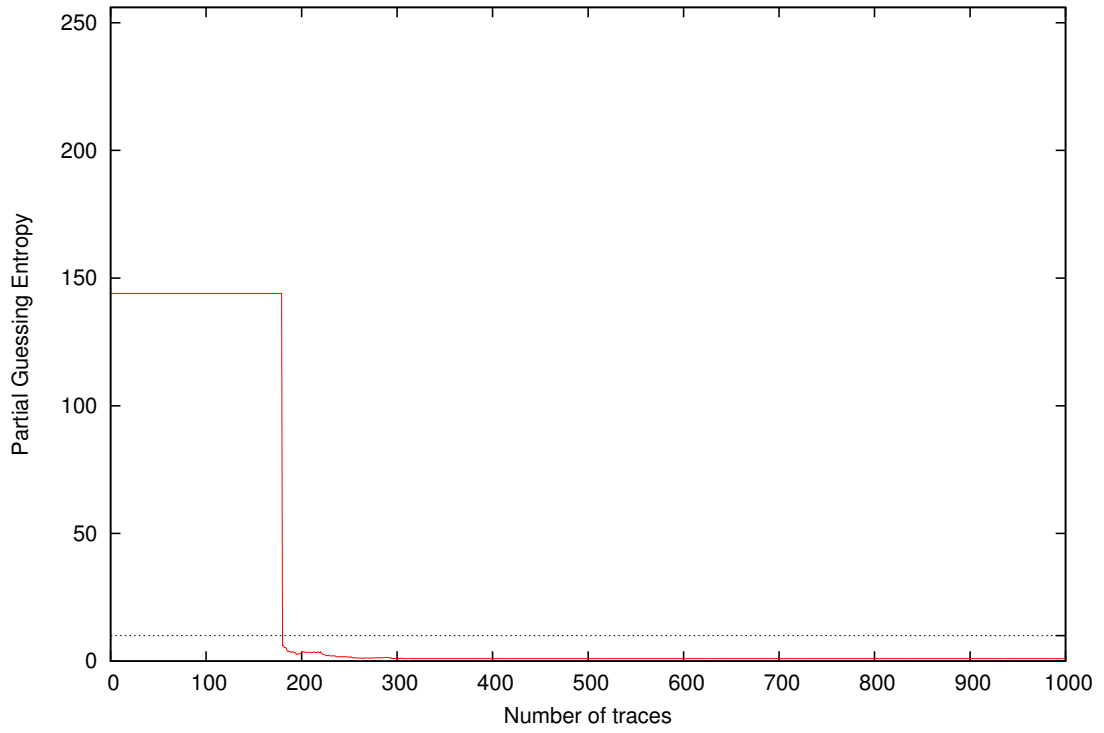
Partial Guessing Entropy for Subkey Byte #9



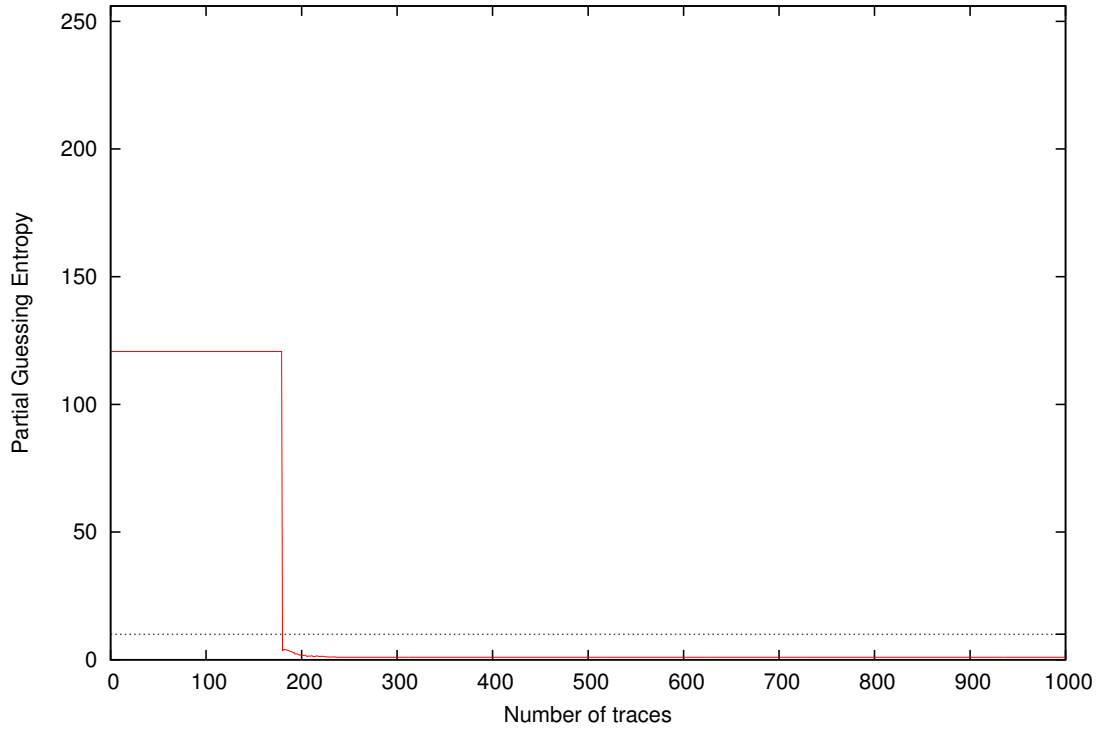
Partial Guessing Entropy for Subkey Byte #10

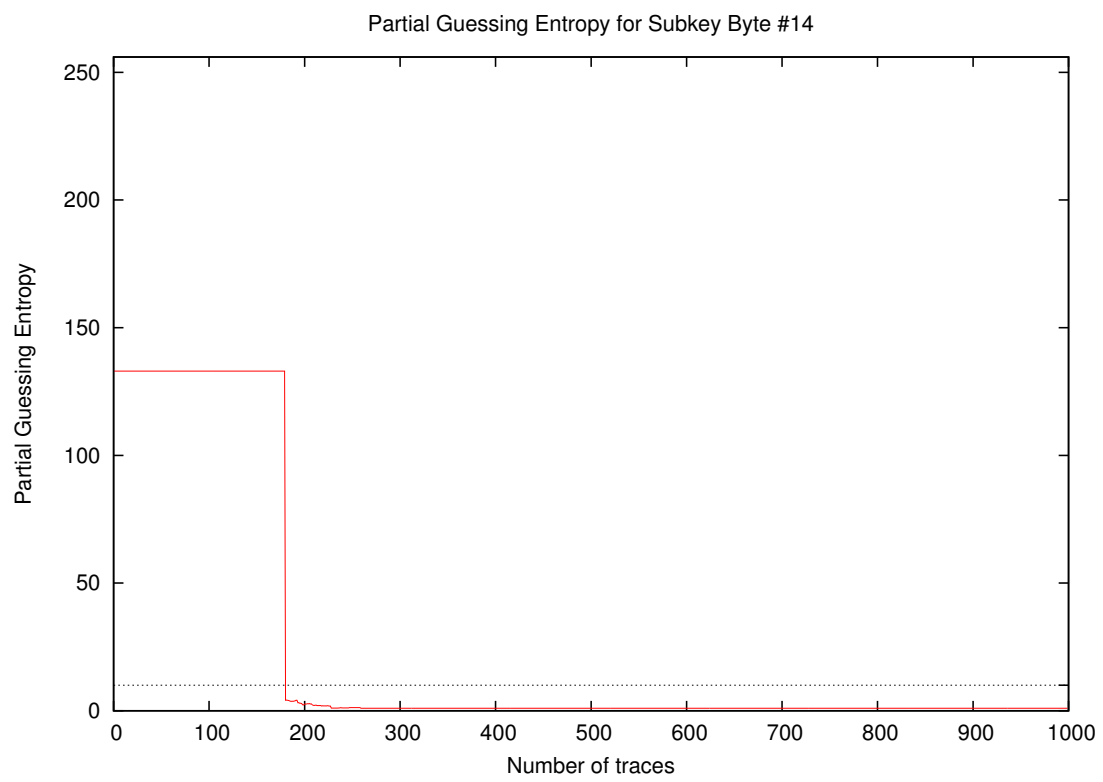
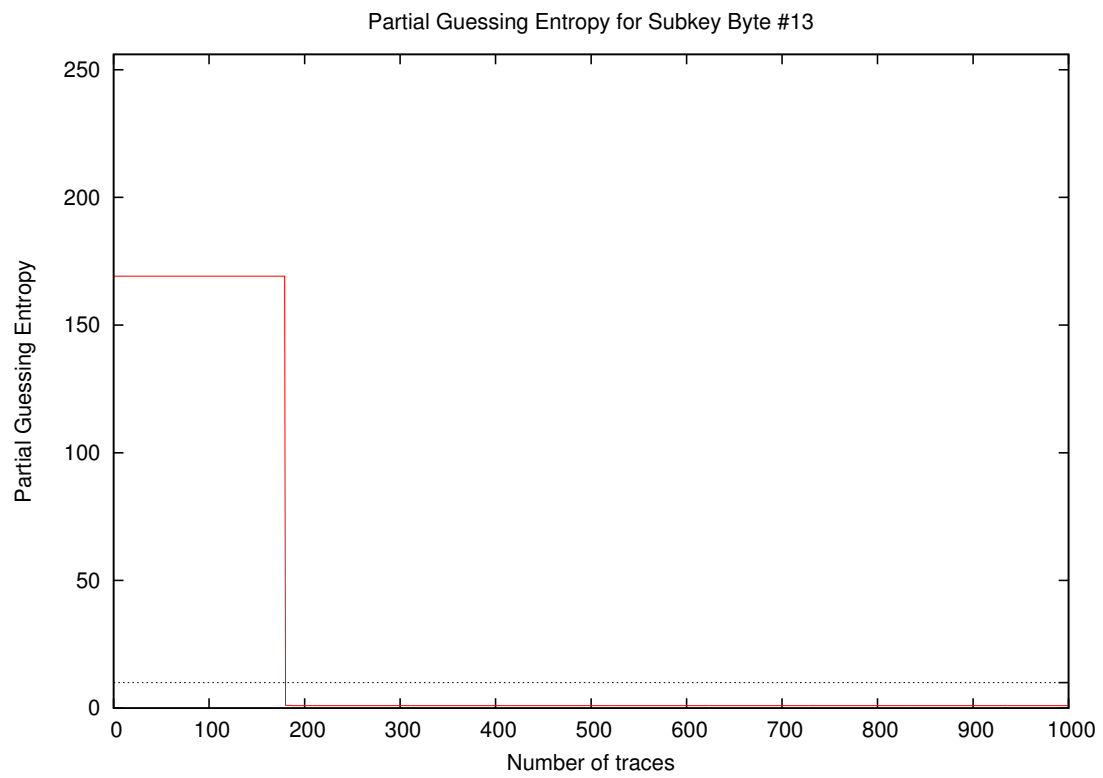


Partial Guessing Entropy for Subkey Byte #11

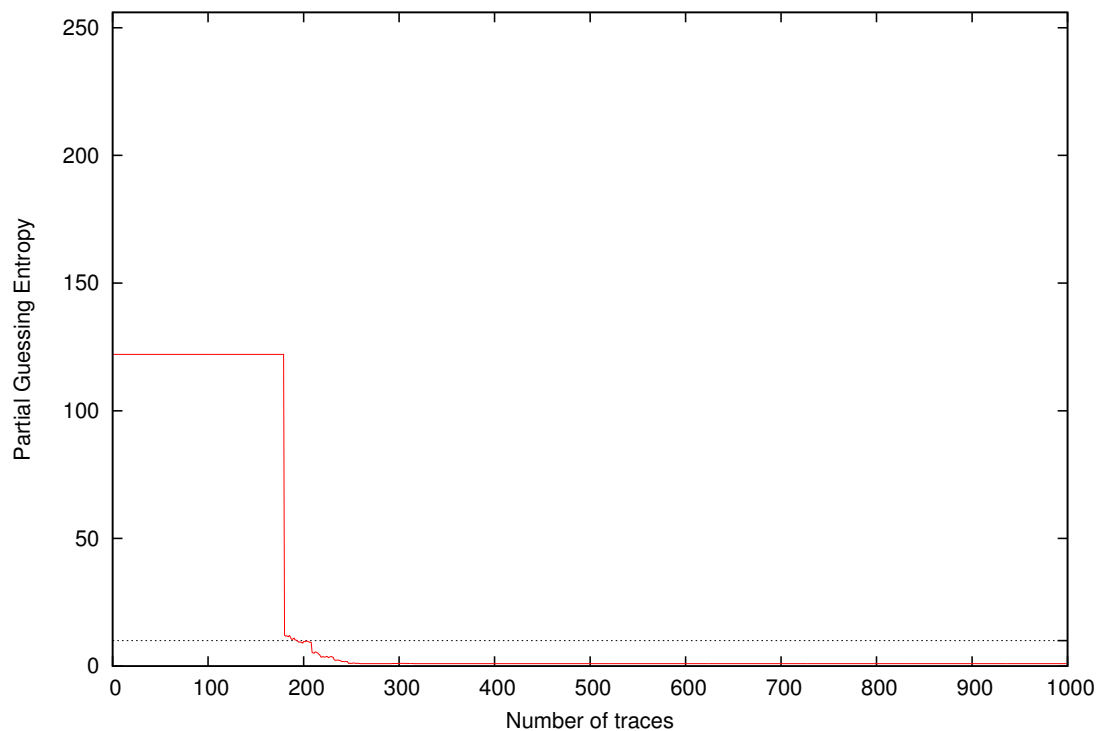


Partial Guessing Entropy for Subkey Byte #12

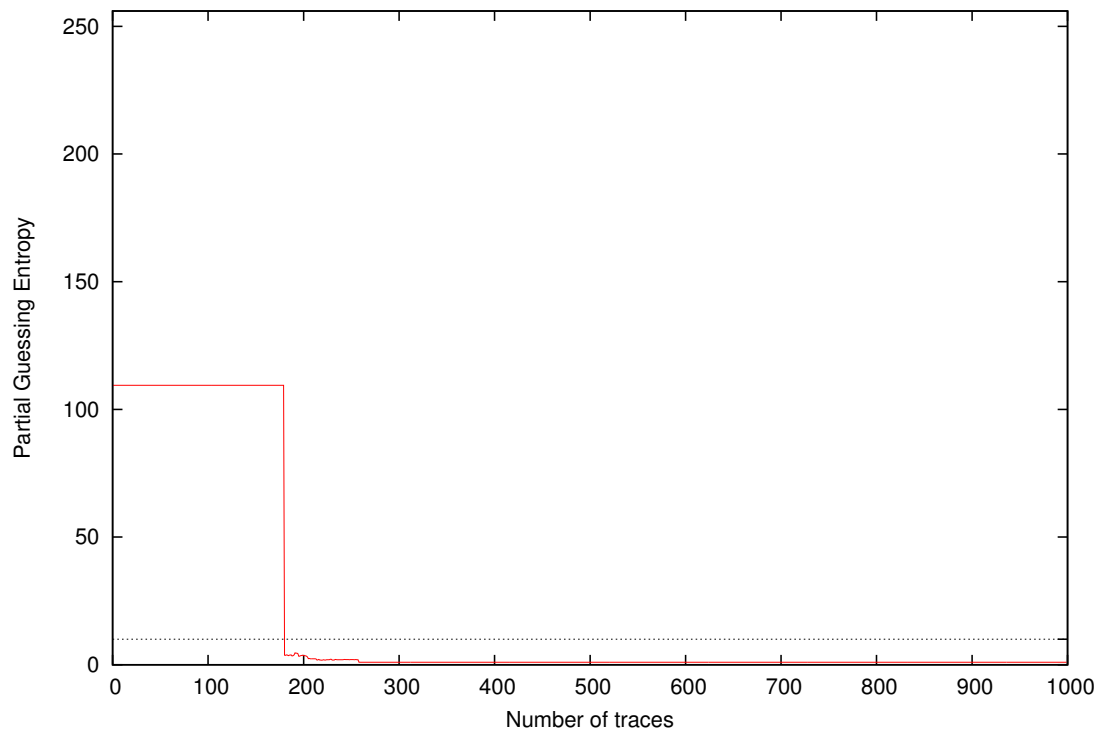




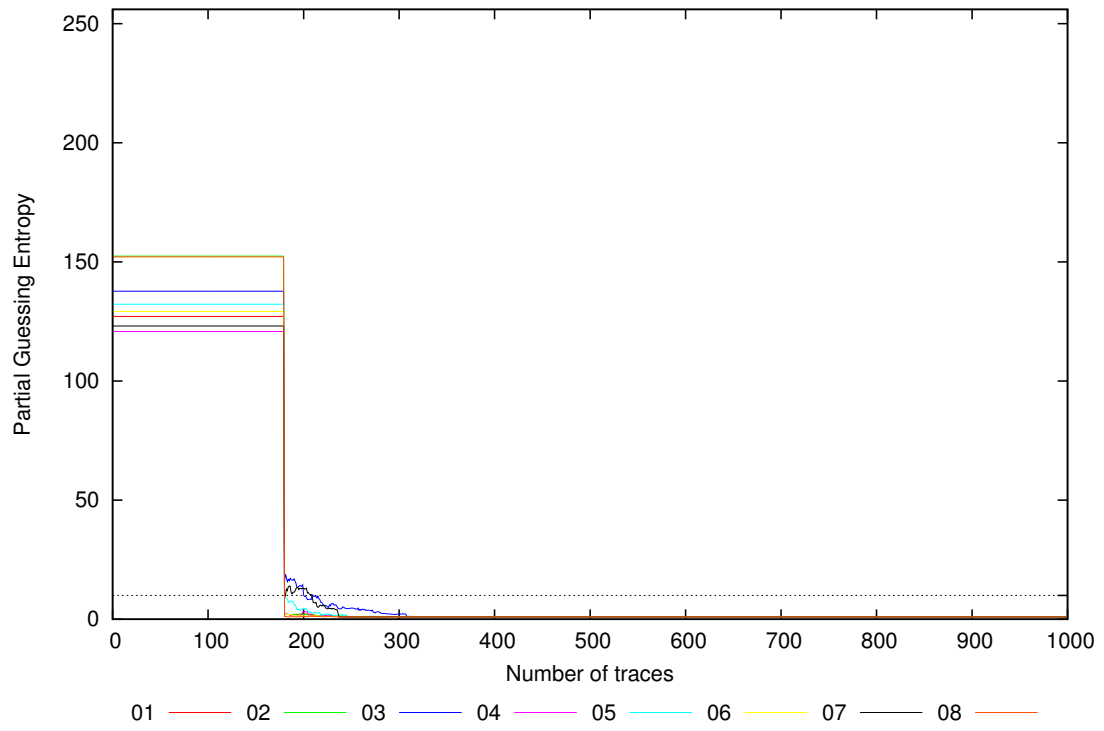
Partial Guessing Entropy for Subkey Byte #15



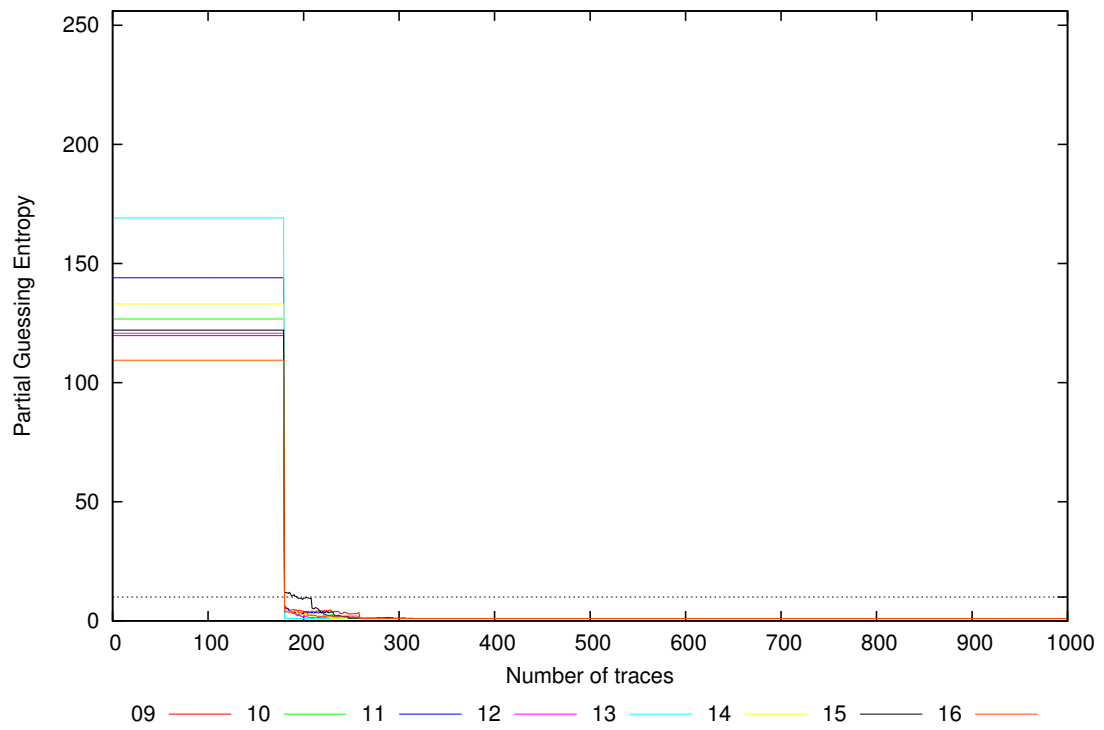
Partial Guessing Entropy for Subkey Byte #16



Partial Guessing Entropy for Subkey Bytes #1 to #8



Partial Guessing Entropy for Subkey Bytes #9 to #16



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	127.1	152.4	137.7	120.8	132.2	129.2	123.1	152.1	119.8	126.7	144.0	120.8	169.1	133.0	122.1	109.4	109.4	169.1	132.5
20	127.1	152.4	137.7	120.8	132.2	129.2	123.1	152.1	119.8	126.7	144.0	120.8	169.1	133.0	122.1	109.4	109.4	169.1	132.5
30	127.1	152.4	137.7	120.8	132.2	129.2	123.1	152.1	119.8	126.7	144.0	120.8	169.1	133.0	122.1	109.4	109.4	169.1	132.5
40	127.1	152.4	137.7	120.8	132.2	129.2	123.1	152.1	119.8	126.7	144.0	120.8	169.1	133.0	122.1	109.4	109.4	169.1	132.5
50	127.1	152.4	137.7	120.8	132.2	129.2	123.1	152.1	119.8	126.7	144.0	120.8	169.1	133.0	122.1	109.4	109.4	169.1	132.5
100	127.1	152.4	137.7	120.8	132.2	129.2	123.1	152.1	119.8	126.7	144.0	120.8	169.1	133.0	122.1	109.4	109.4	169.1	132.5
200	2.2	2.3	14.4	3.1	4.2	1.4	13.0	1.2	4.0	2.3	3.1	1.8	1.0	2.2	9.0	3.8	1.0	14.4	4.3
300	1.0	1.0	2.2	1.0	1.1	1.0	1.0	1.0	1.0	1.0	1.1	1.0	1.0	1.0	1.1	1.0	1.0	2.2	1.1
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
600	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
700	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
800	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
900	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
1000	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