

DPA Contest v4.2

Evaluation results

Dai Tian, Sun Xibo, Zhang Chi, Wang Lihui, Shan Weijun

August 2016

1 Introduction

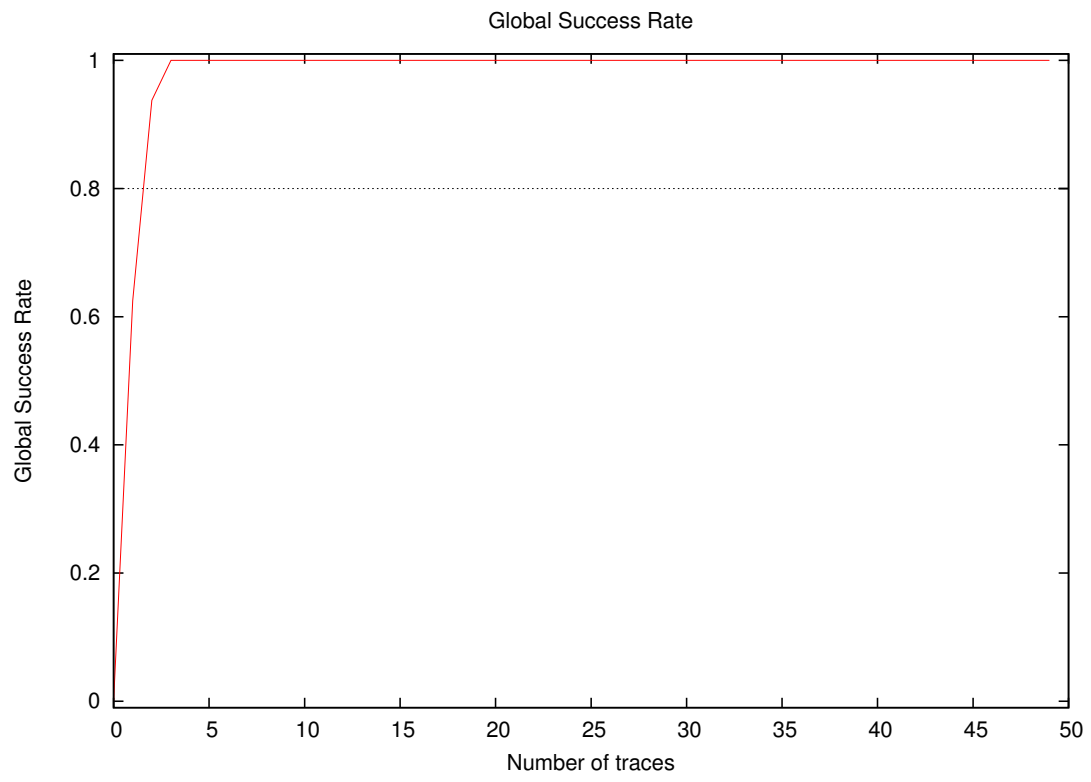
1.1 About the attack

- **Sender/Team:** Dai Tian, Sun Xibo, Zhang Chi, Wang Lihui, Shan Weijun
- **Institution:** Shanghai Fudan Microelectronics Group Company Limited, China
- **Language:** Matlab
- **Operating system:** Windows
- **Attacked subkey:** 0

1.2 About the evaluation

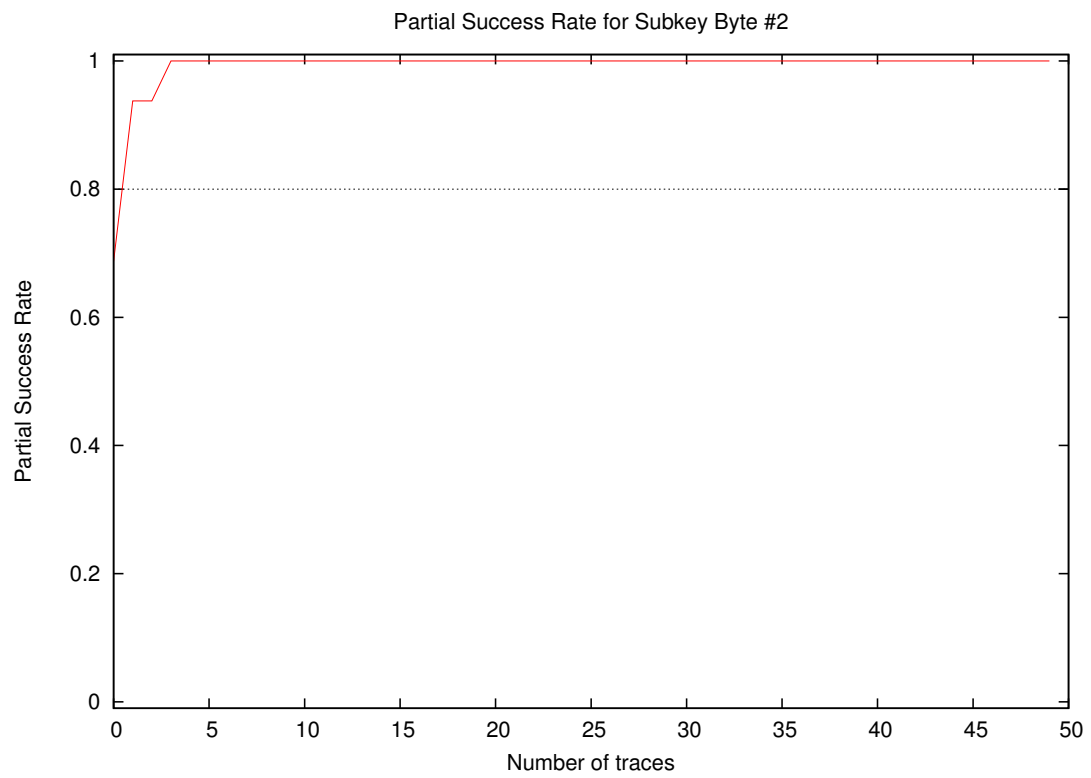
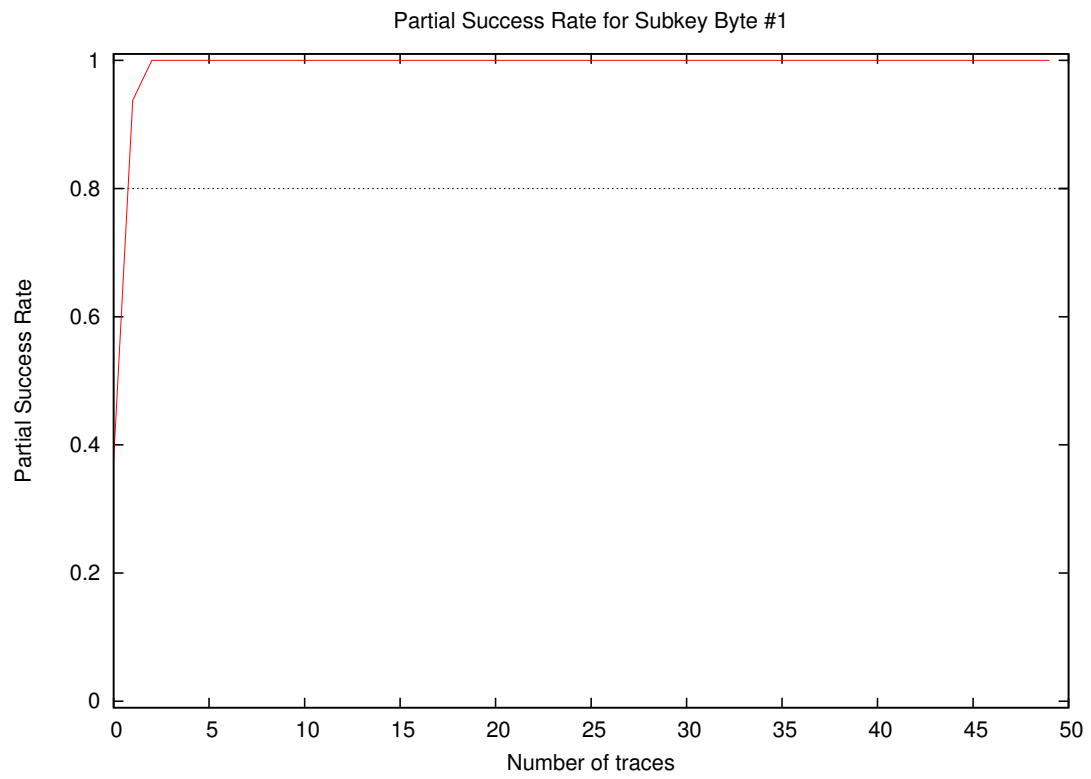
- **Date of evaluation:** August 2016

2 Global Success Rate

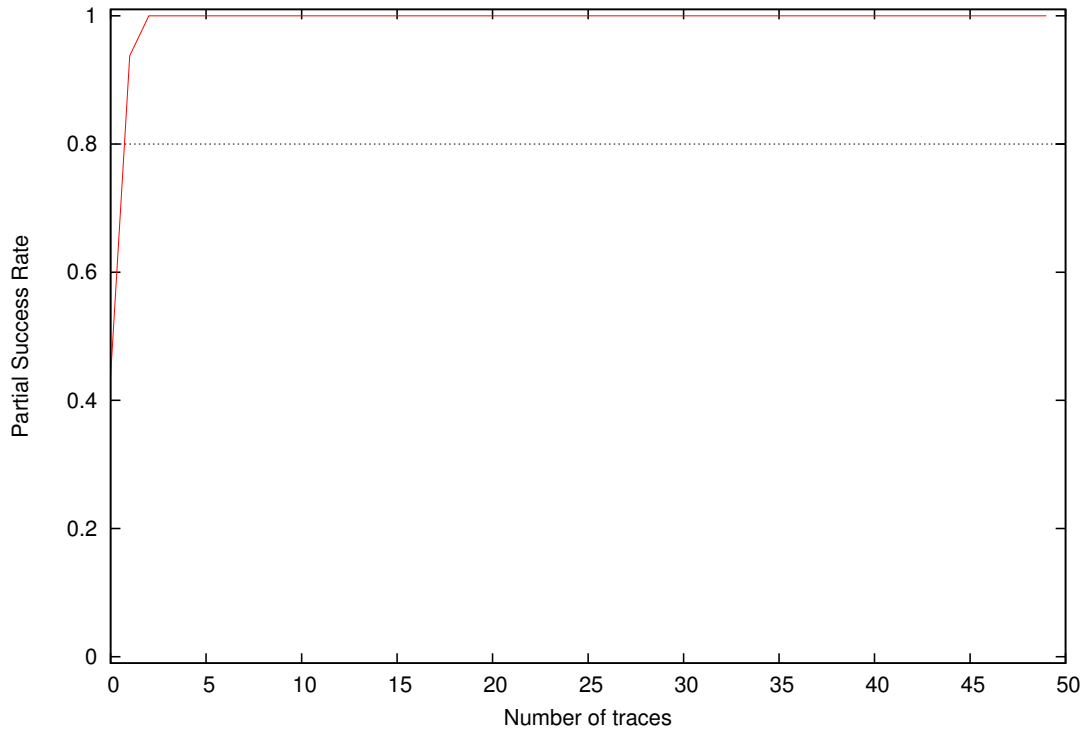


Number of traces	Global Success Rate
10	1.00
20	1.00
30	1.00
40	1.00
50	1.00

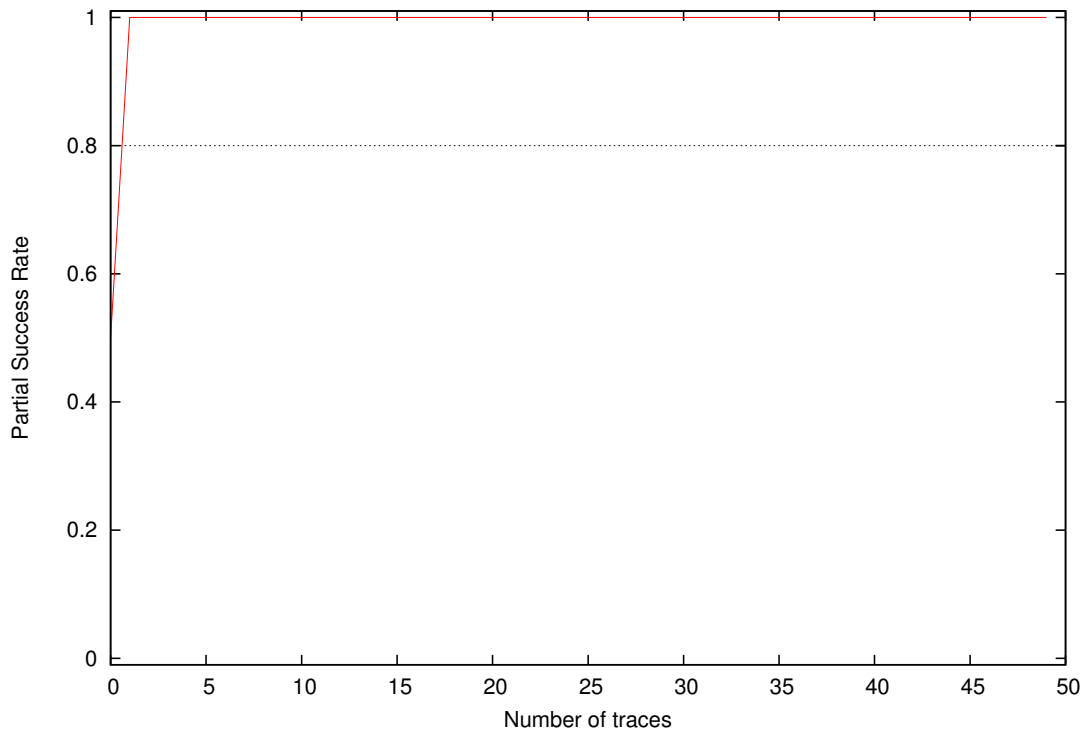
3 Partial Success Rate



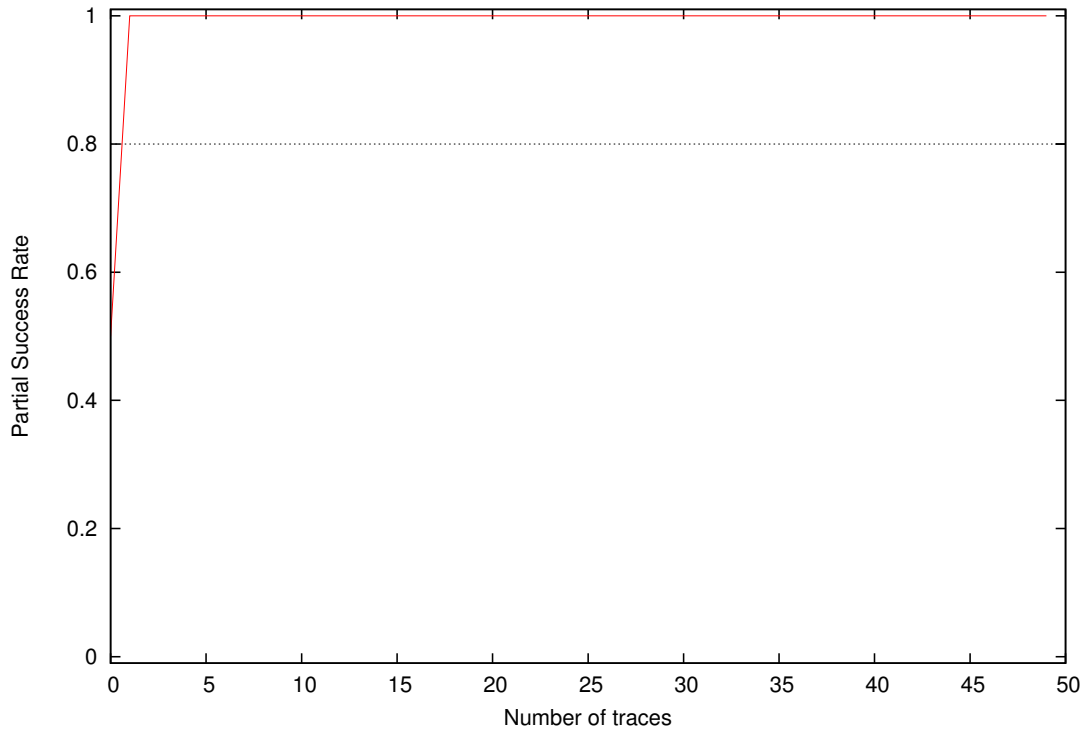
Partial Success Rate for Subkey Byte #3



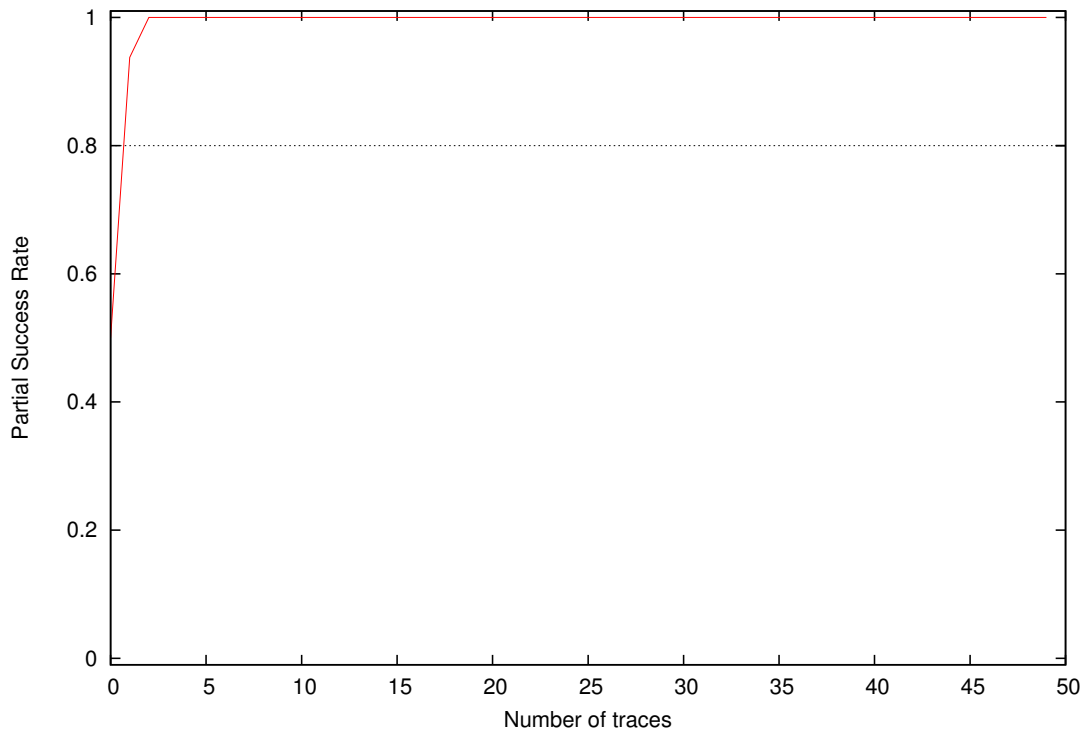
Partial Success Rate for Subkey Byte #4

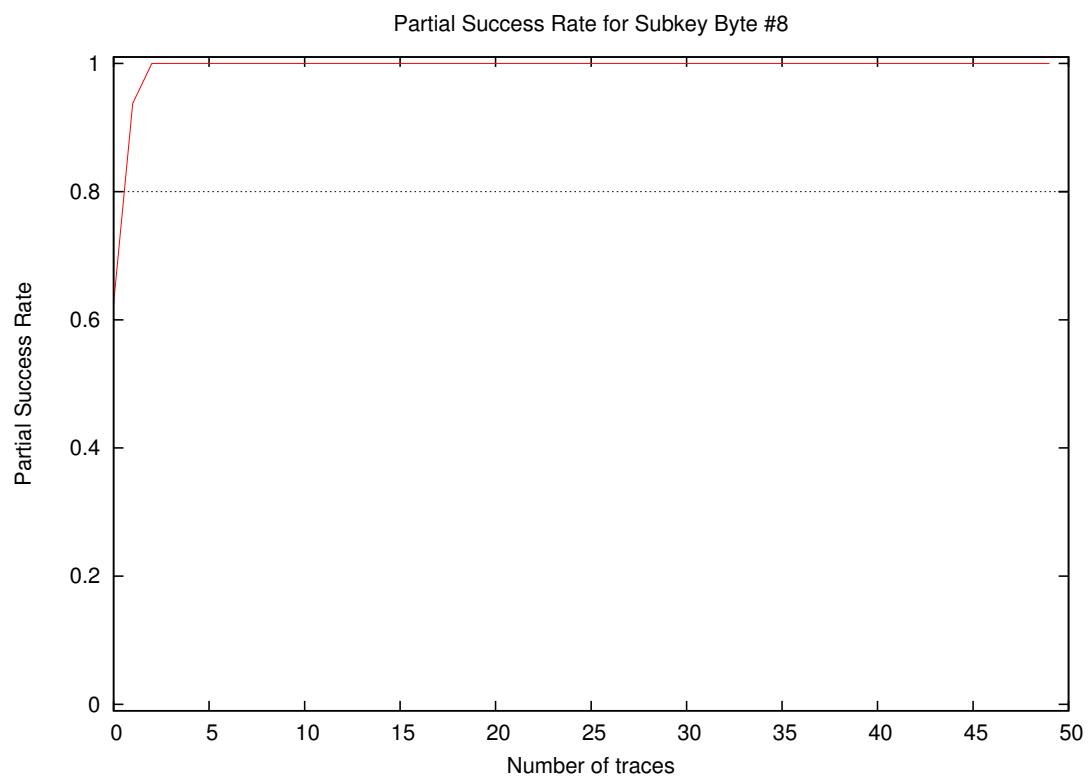
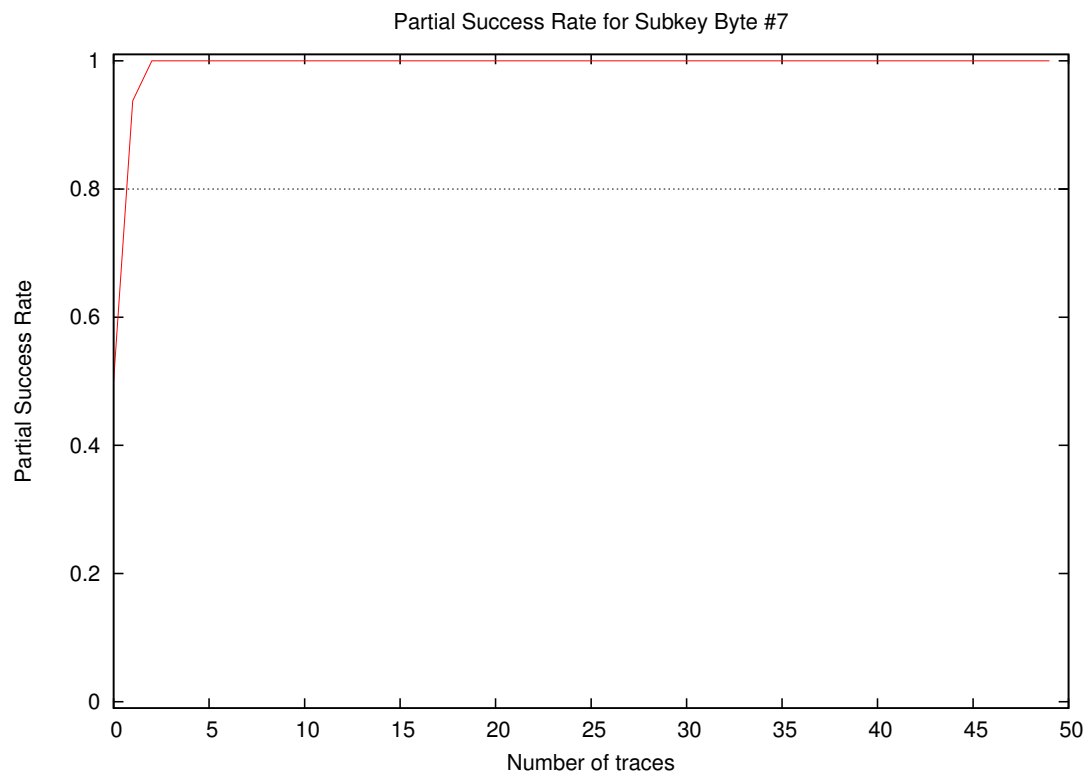


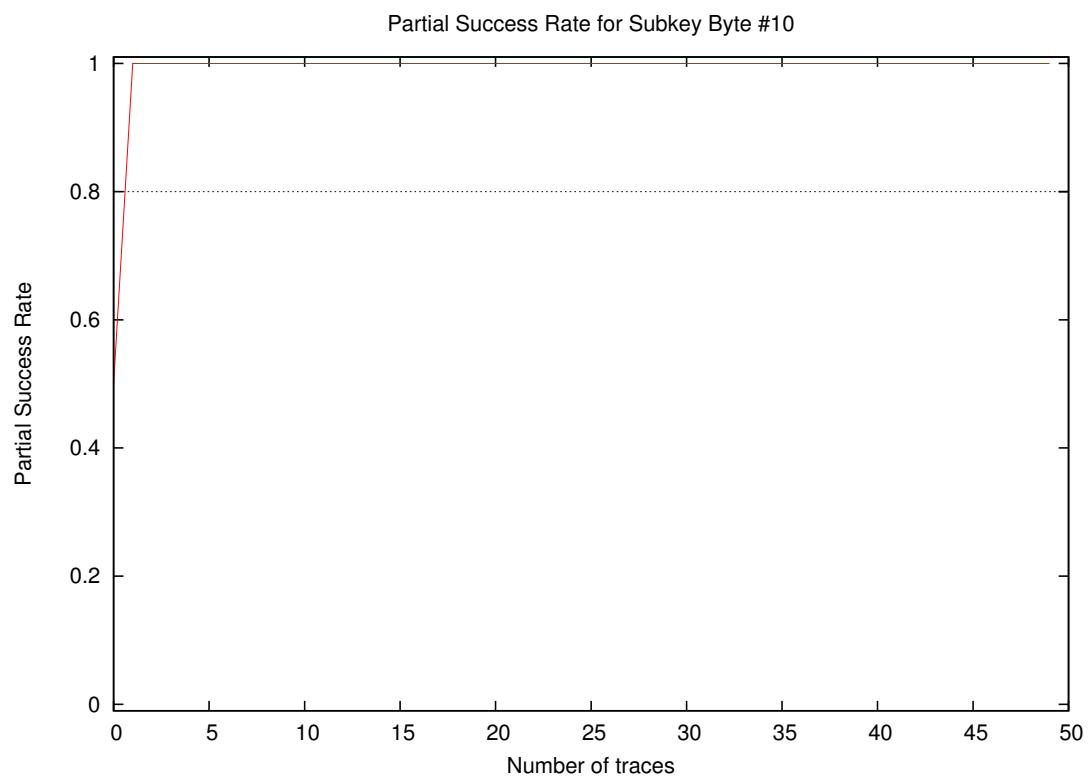
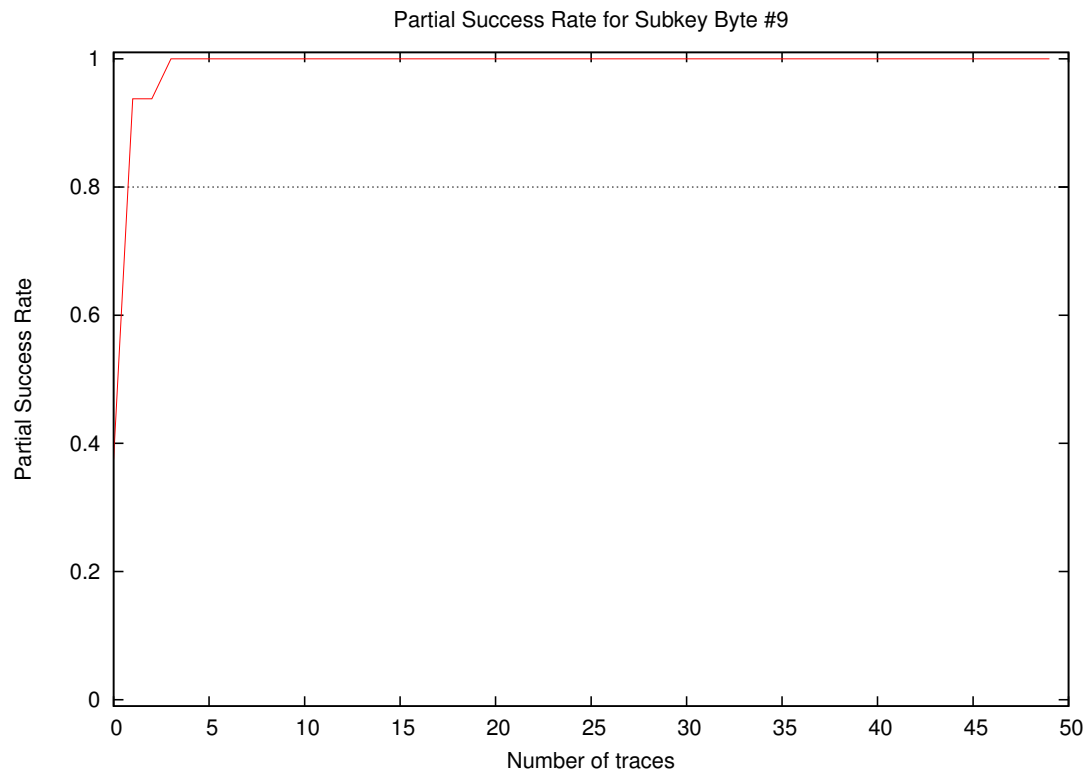
Partial Success Rate for Subkey Byte #5



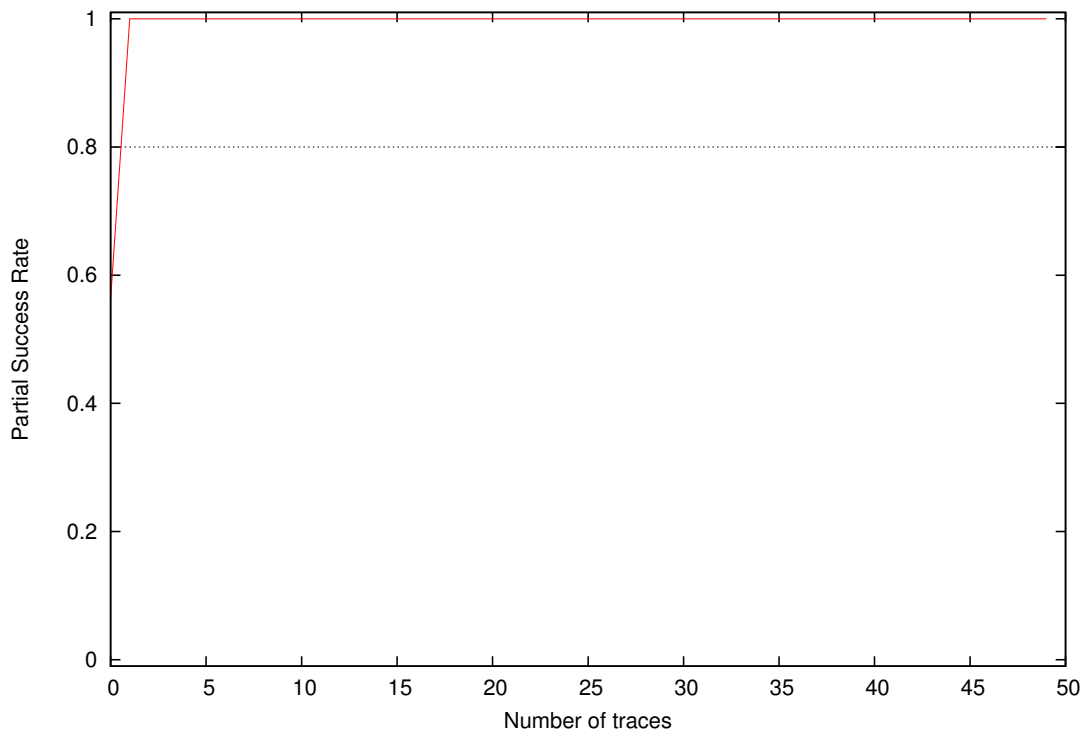
Partial Success Rate for Subkey Byte #6



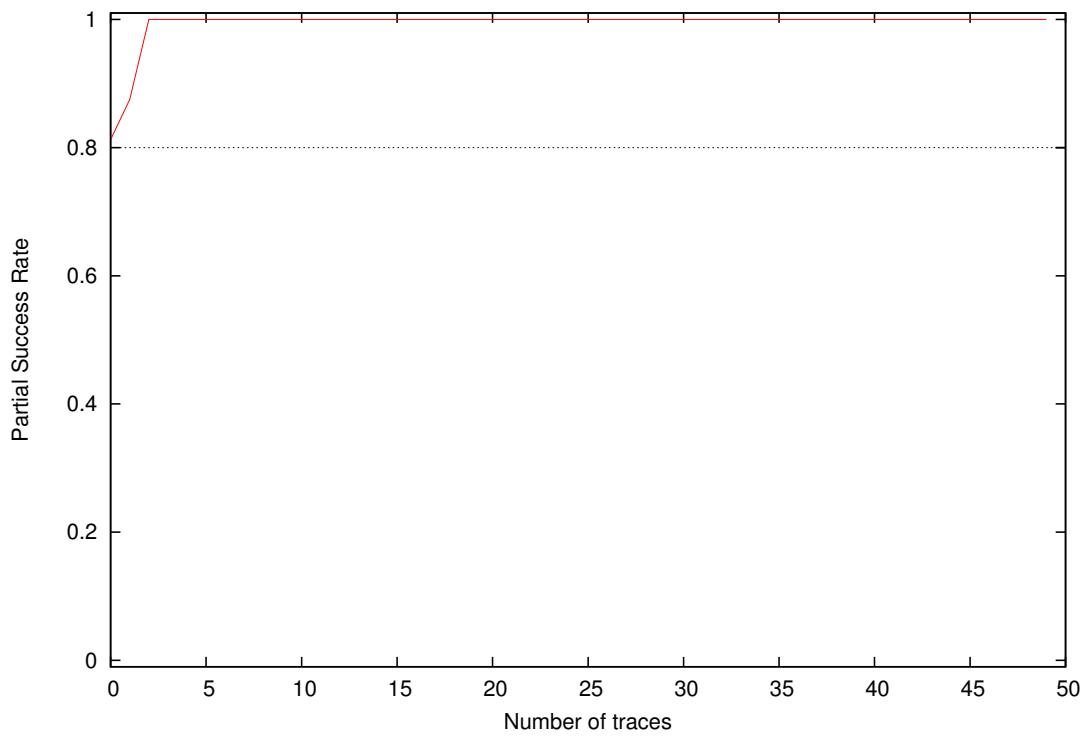


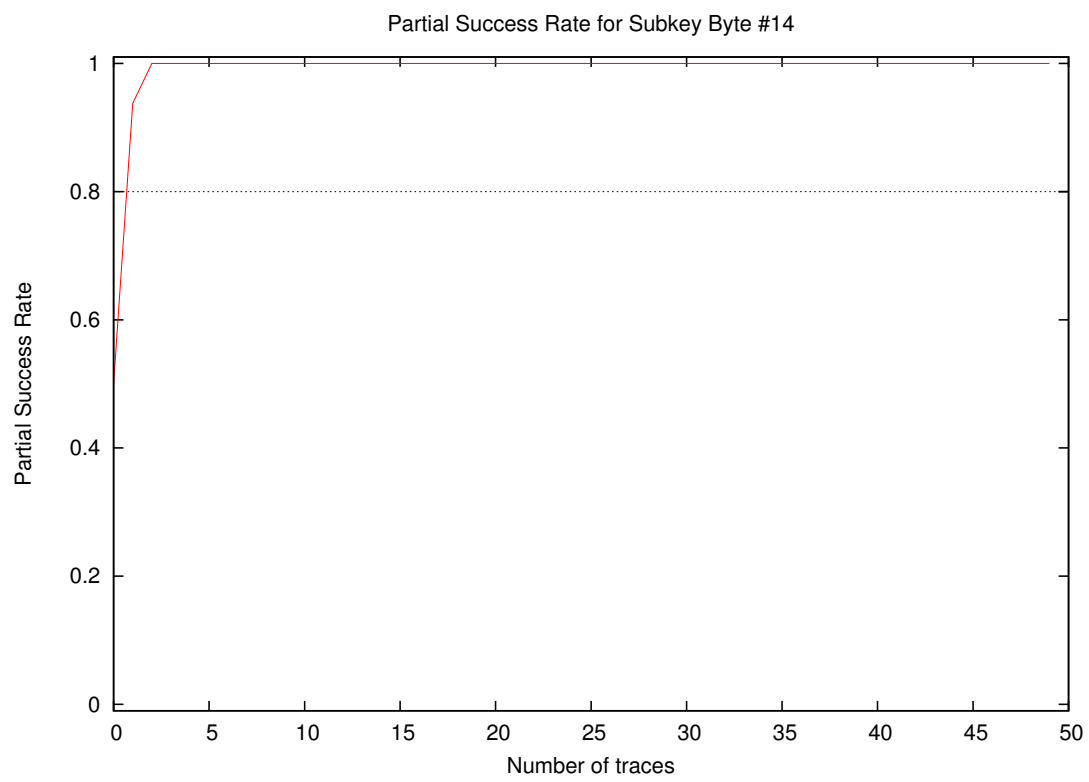
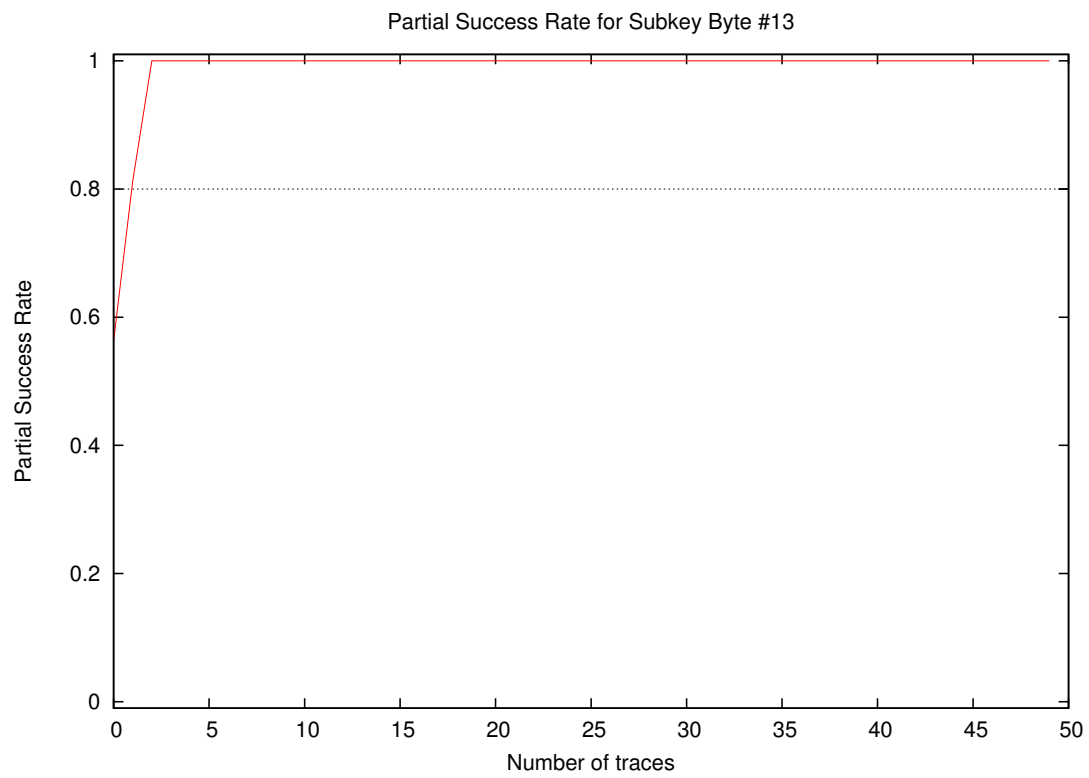


Partial Success Rate for Subkey Byte #11

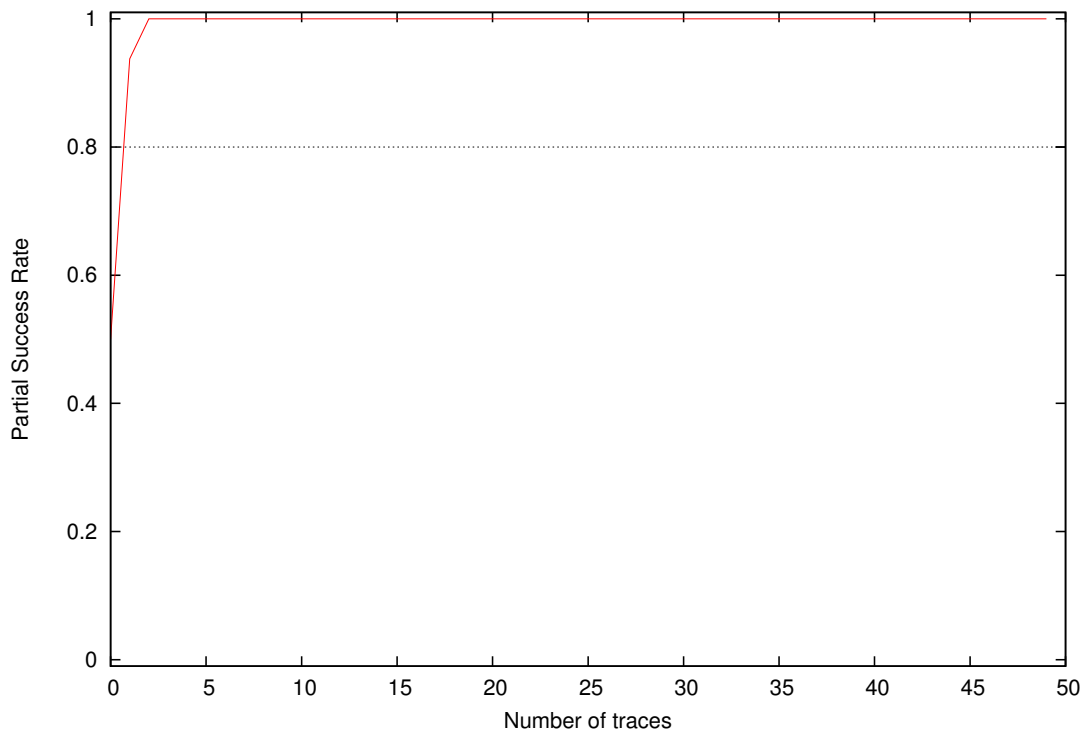


Partial Success Rate for Subkey Byte #12

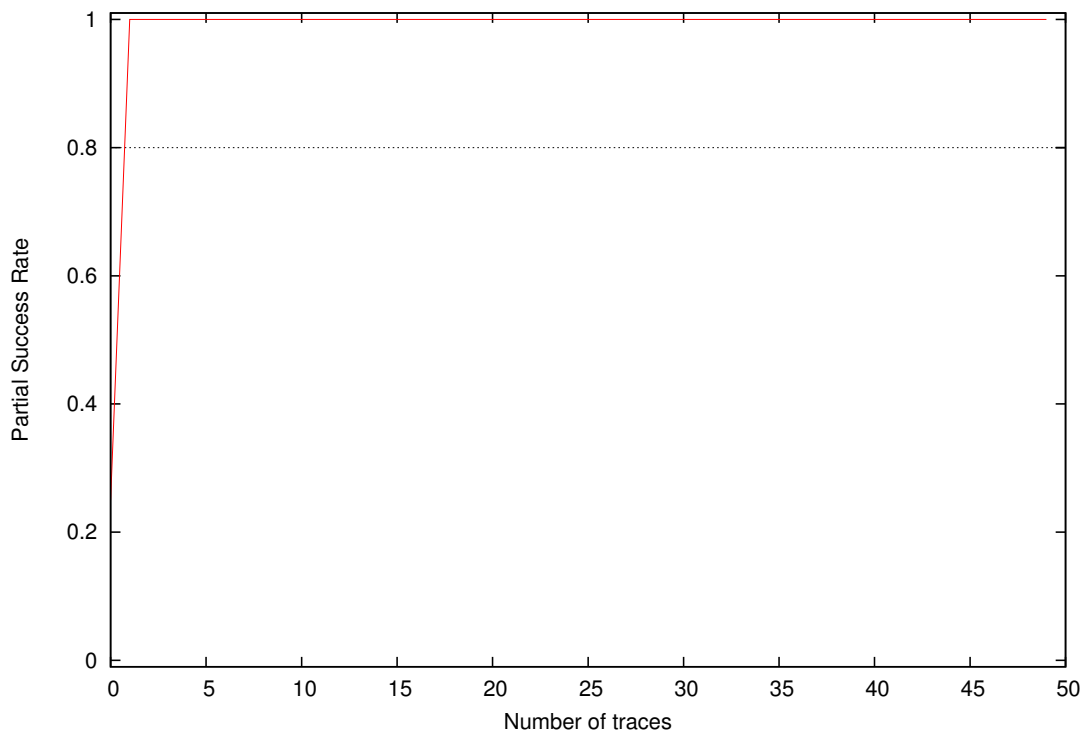


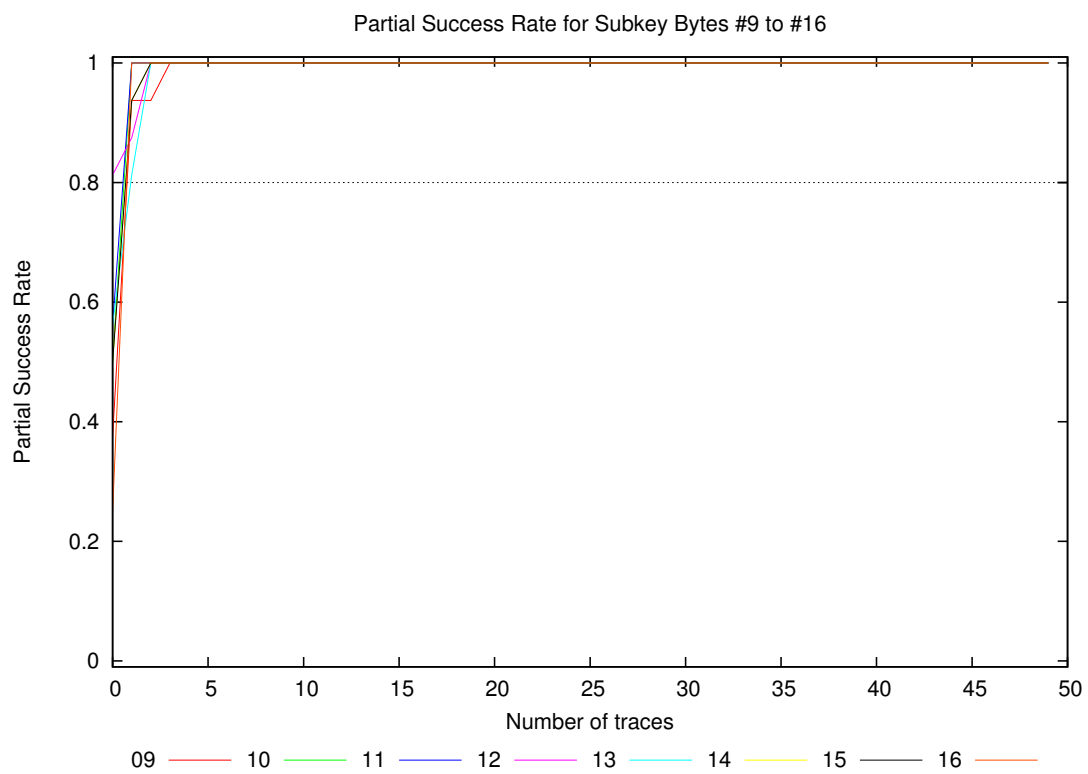
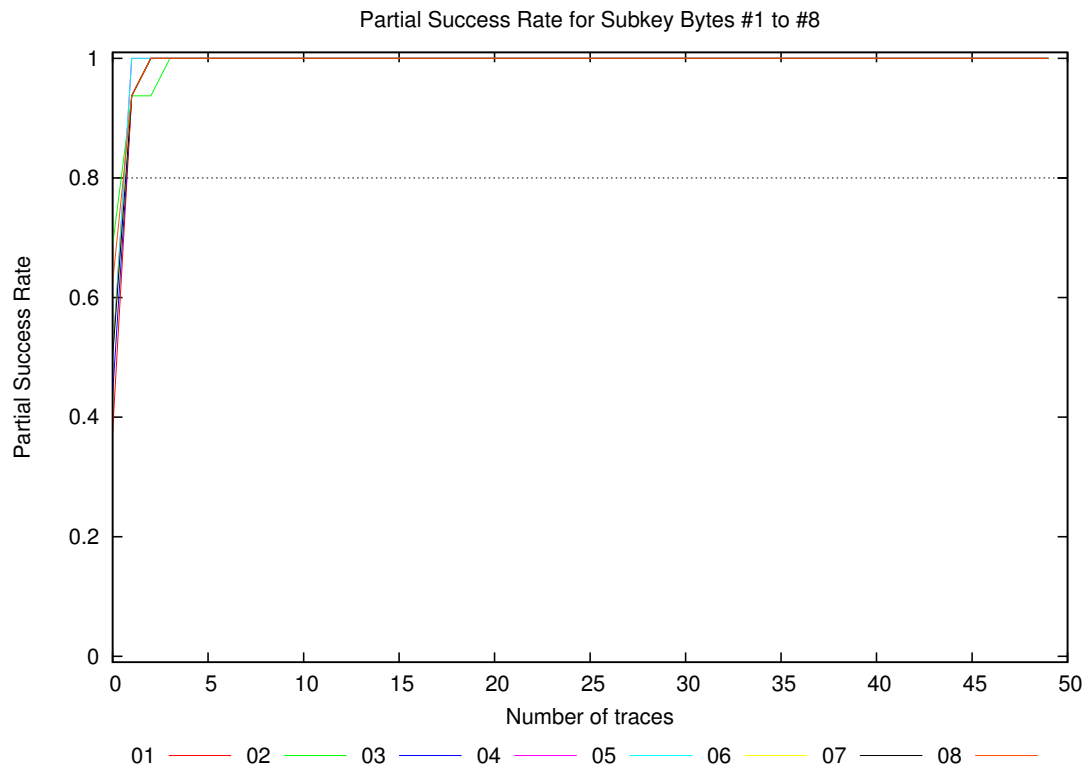


Partial Success Rate for Subkey Byte #15

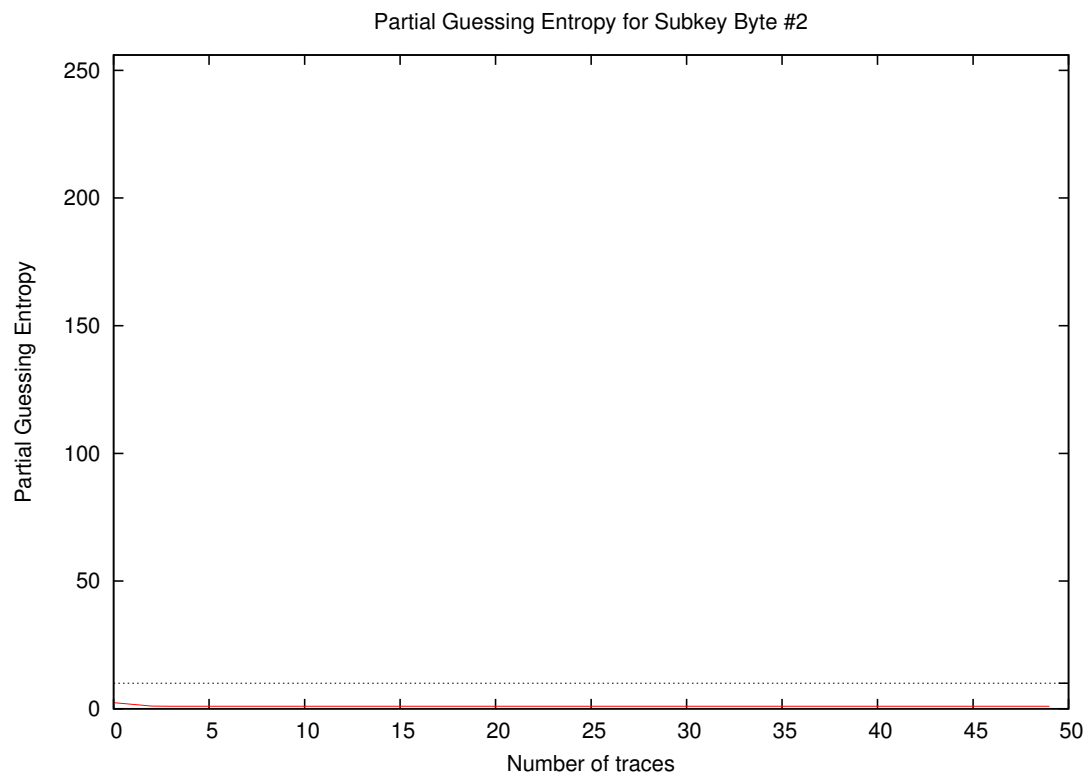


Partial Success Rate for Subkey Byte #16

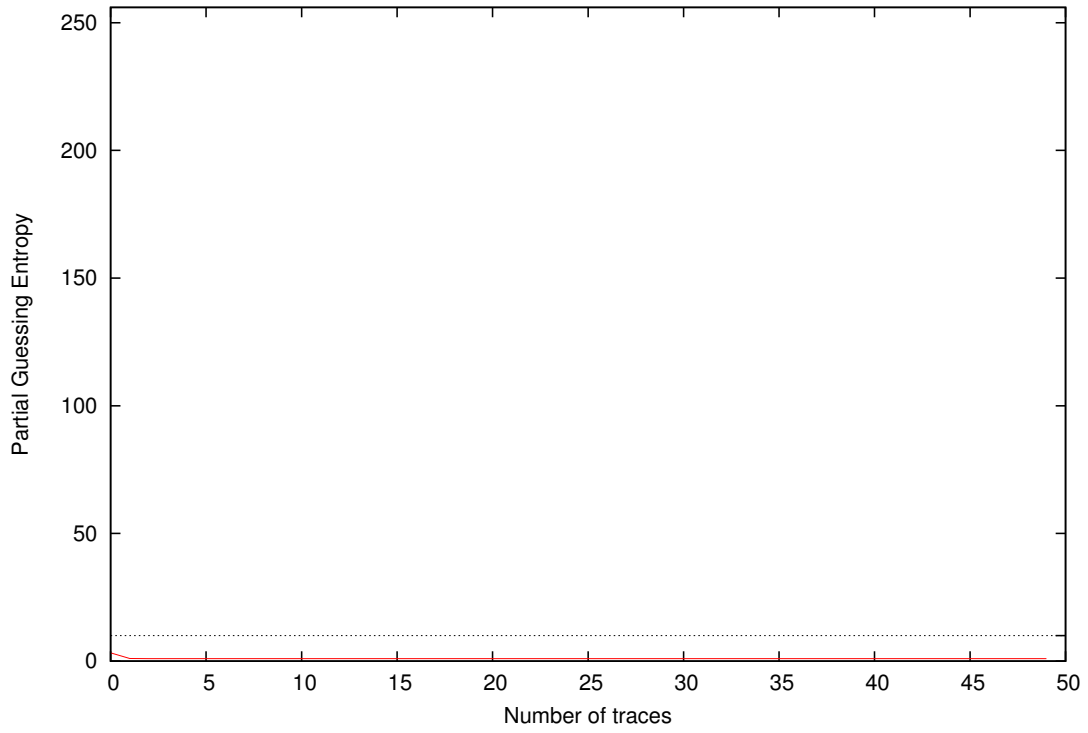




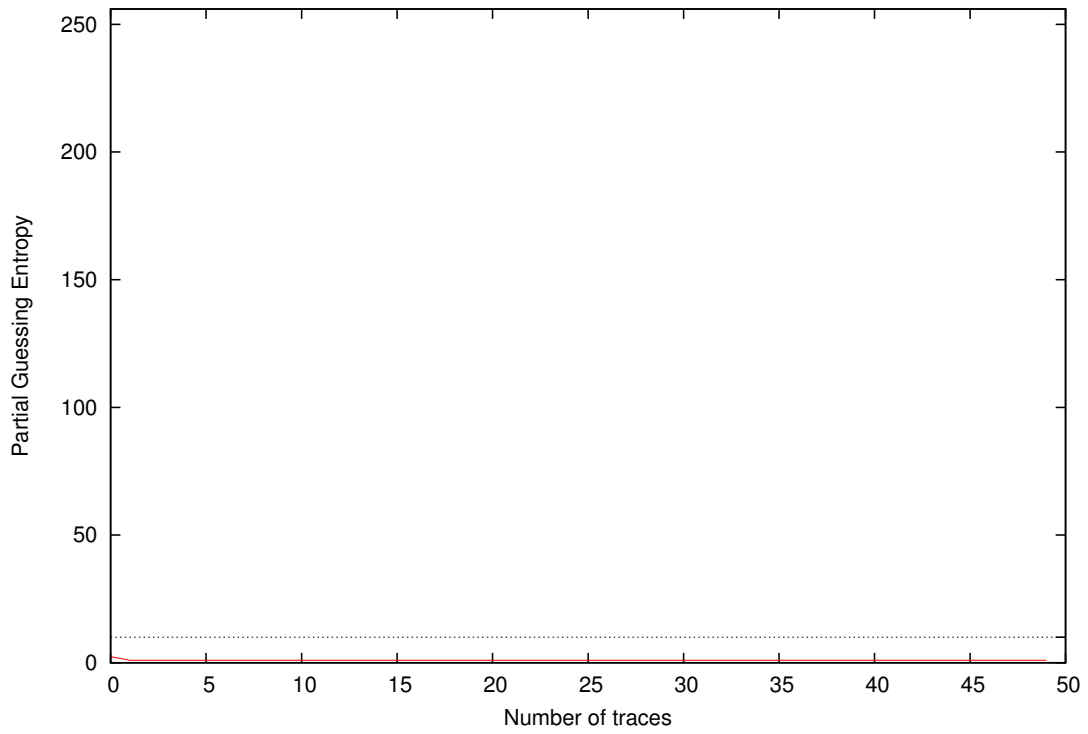
4 Partial Guessing Entropy



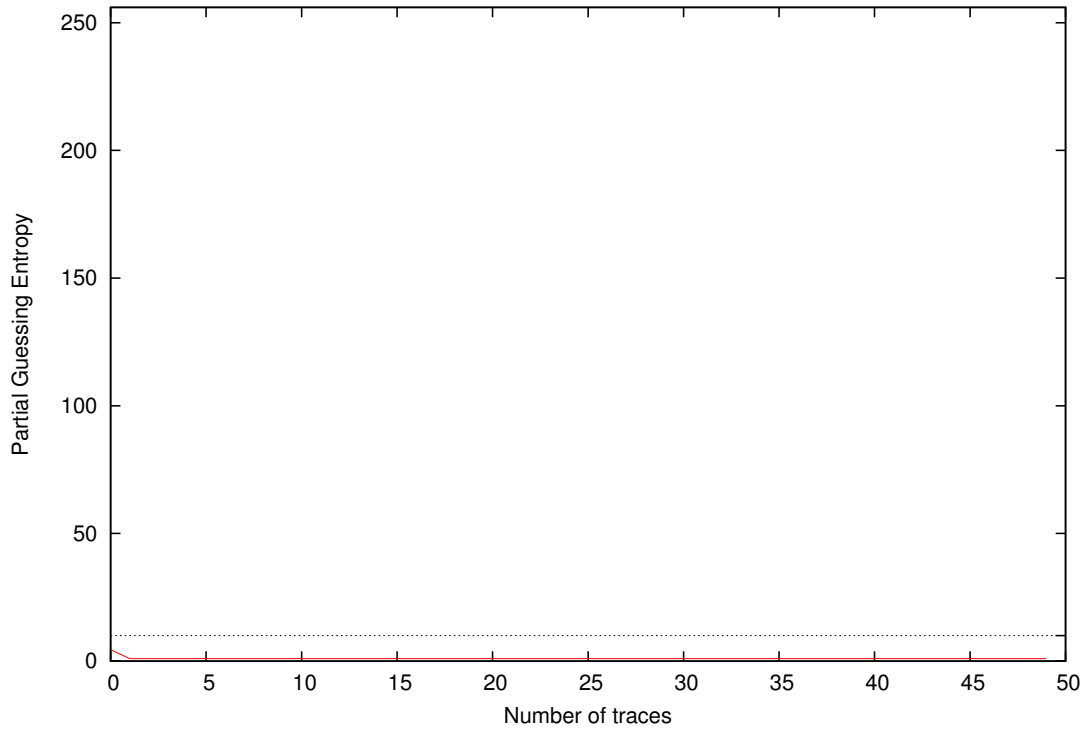
Partial Guessing Entropy for Subkey Byte #3



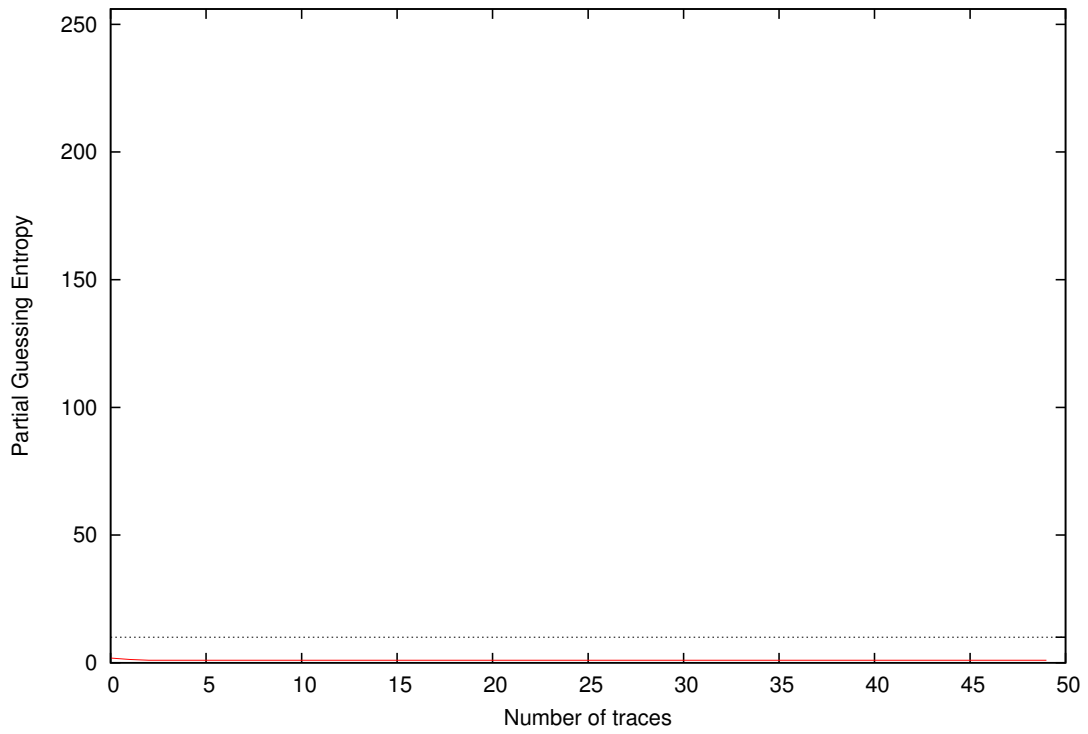
Partial Guessing Entropy for Subkey Byte #4



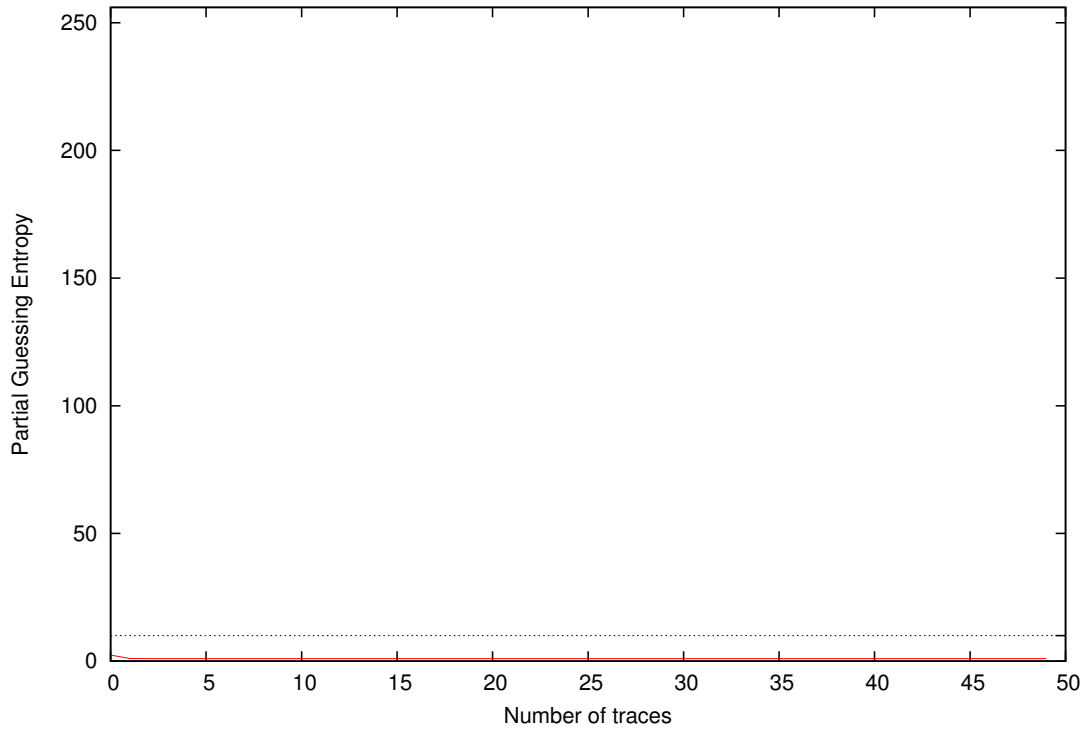
Partial Guessing Entropy for Subkey Byte #5



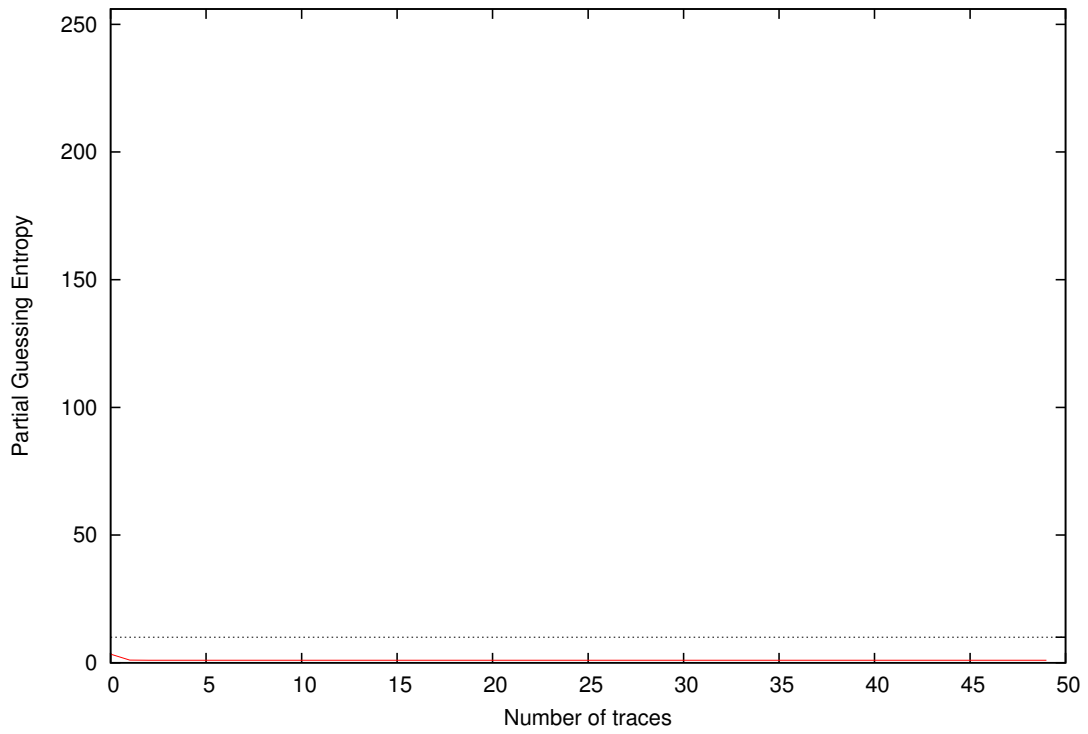
Partial Guessing Entropy for Subkey Byte #6

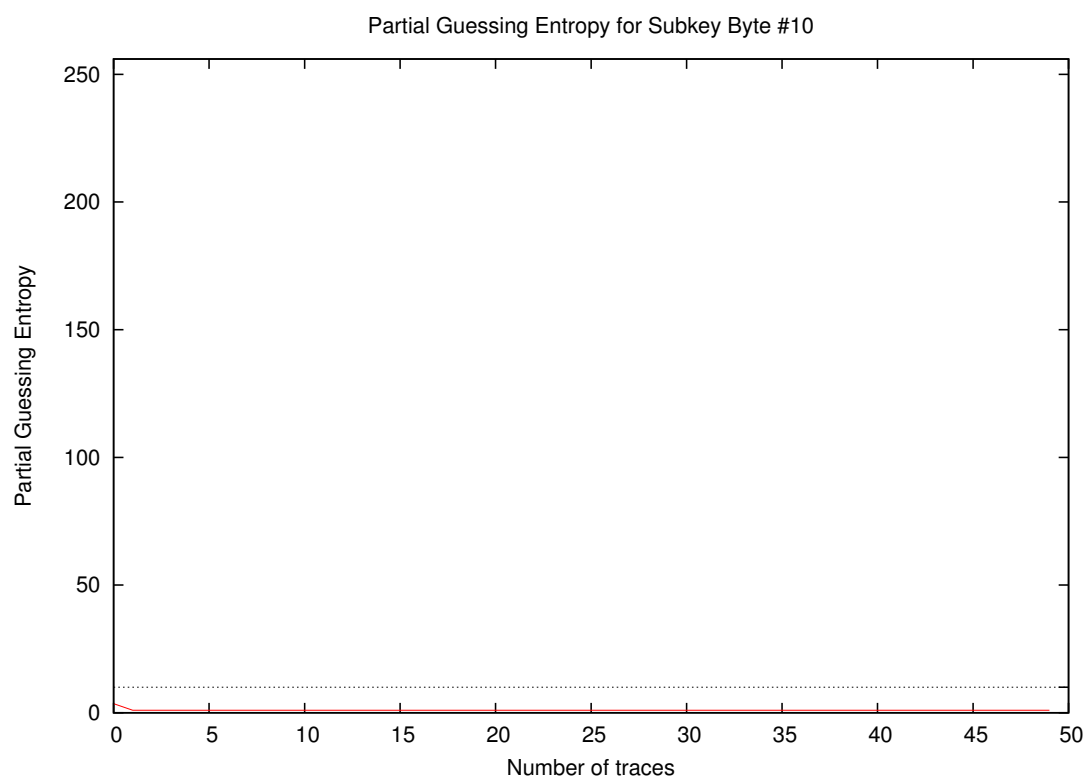
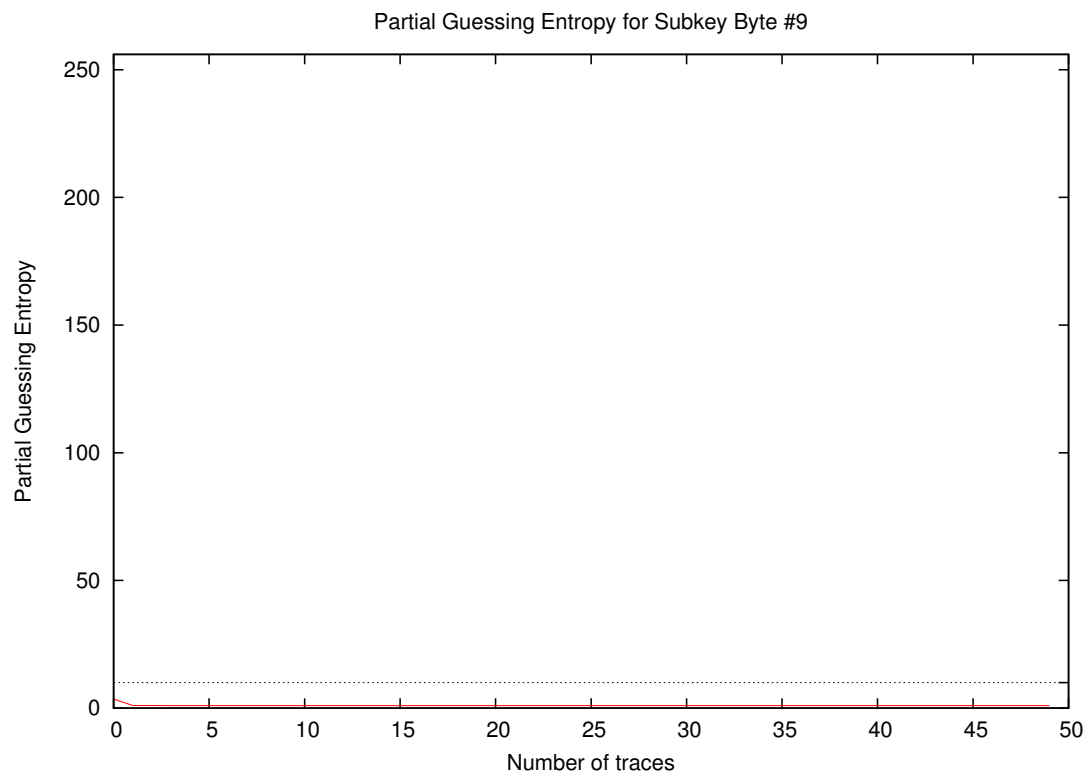


Partial Guessing Entropy for Subkey Byte #7

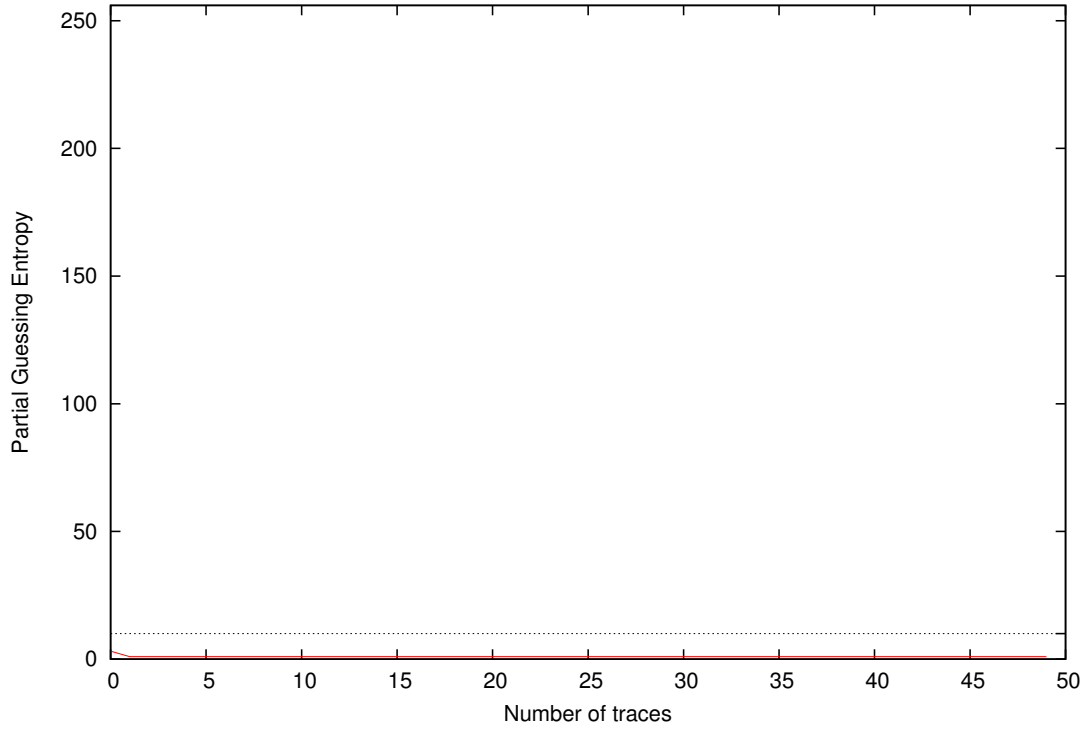


Partial Guessing Entropy for Subkey Byte #8

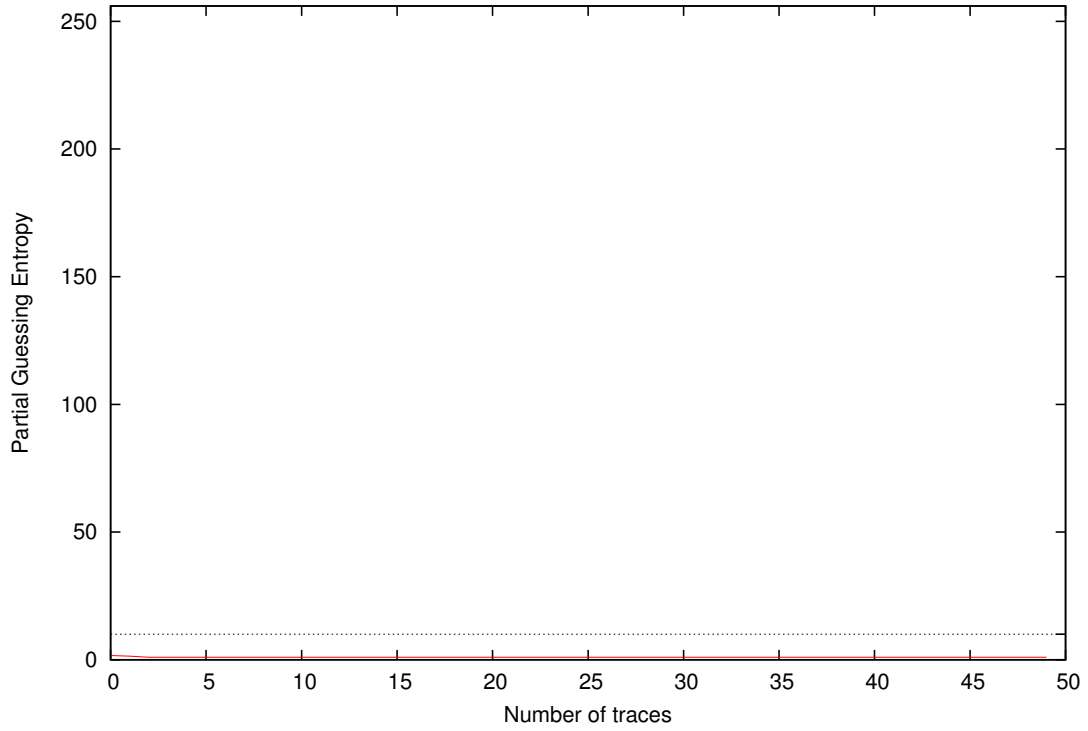




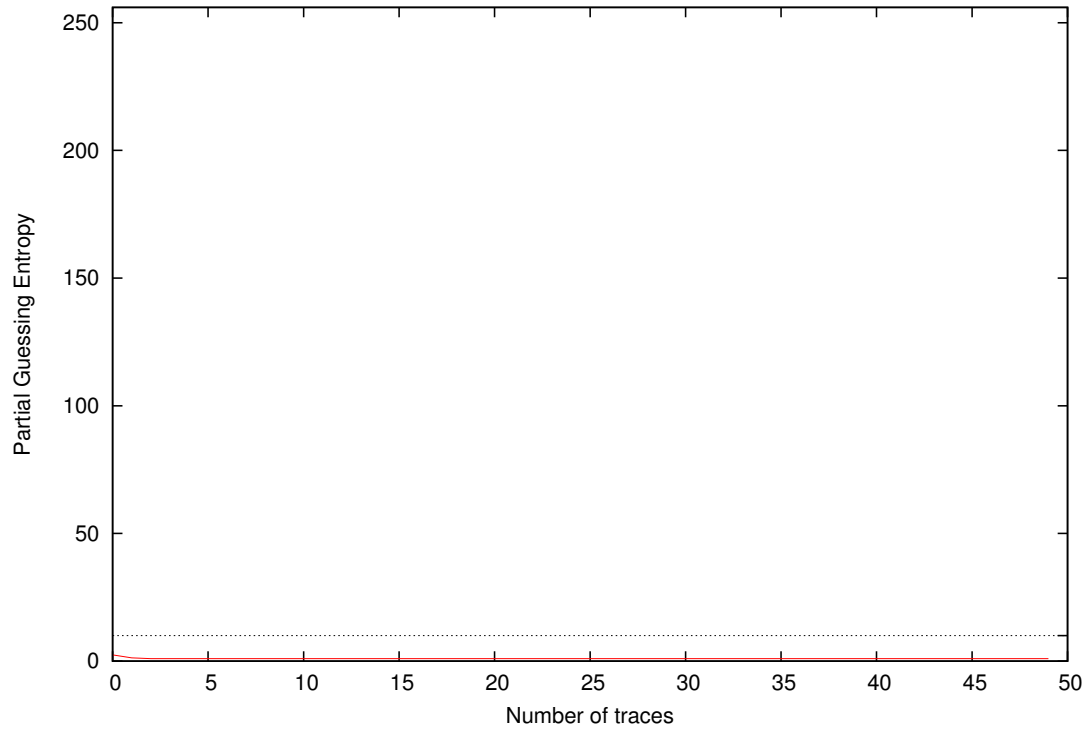
Partial Guessing Entropy for Subkey Byte #11



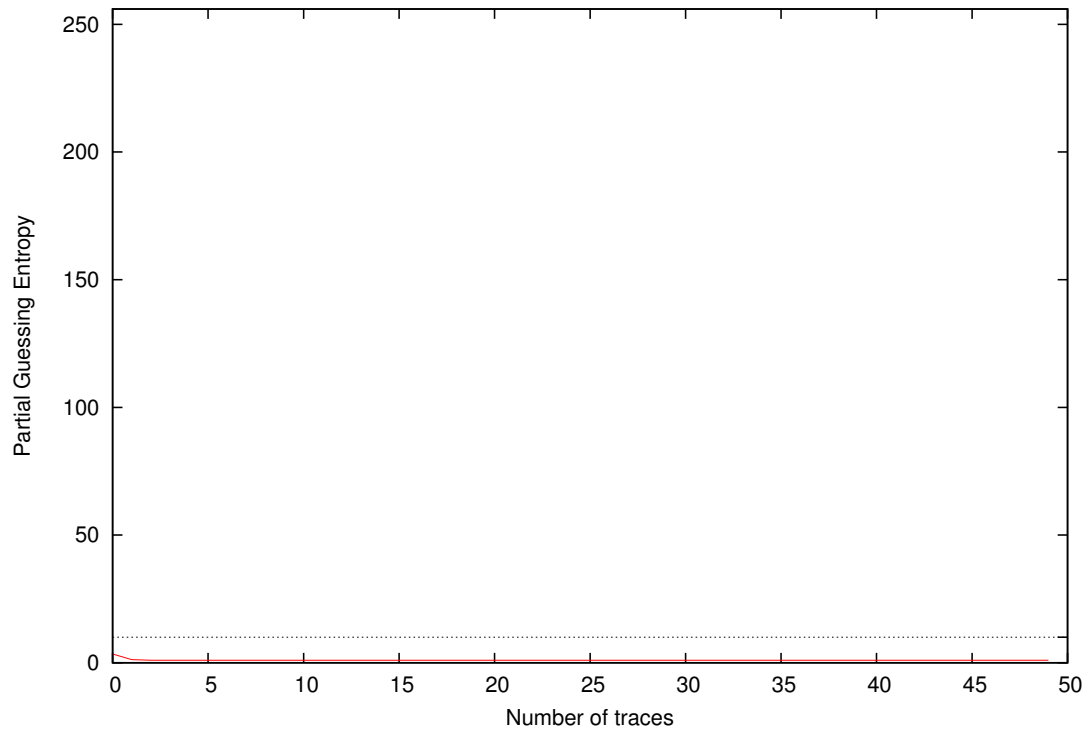
Partial Guessing Entropy for Subkey Byte #12

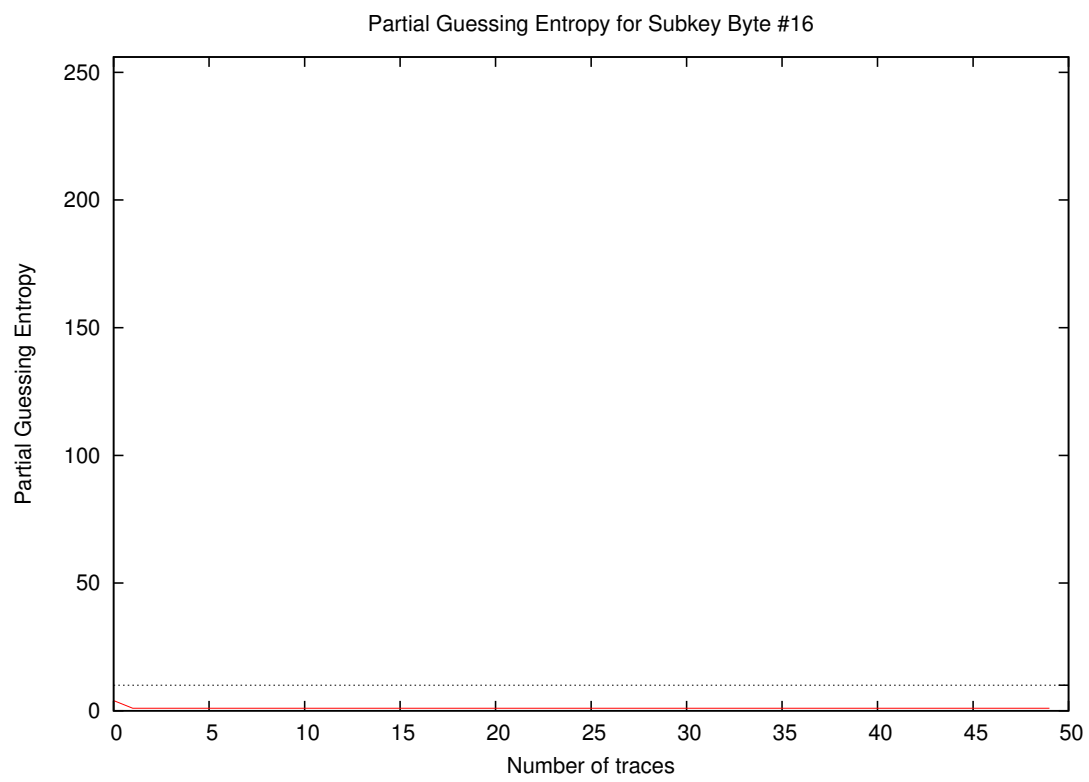
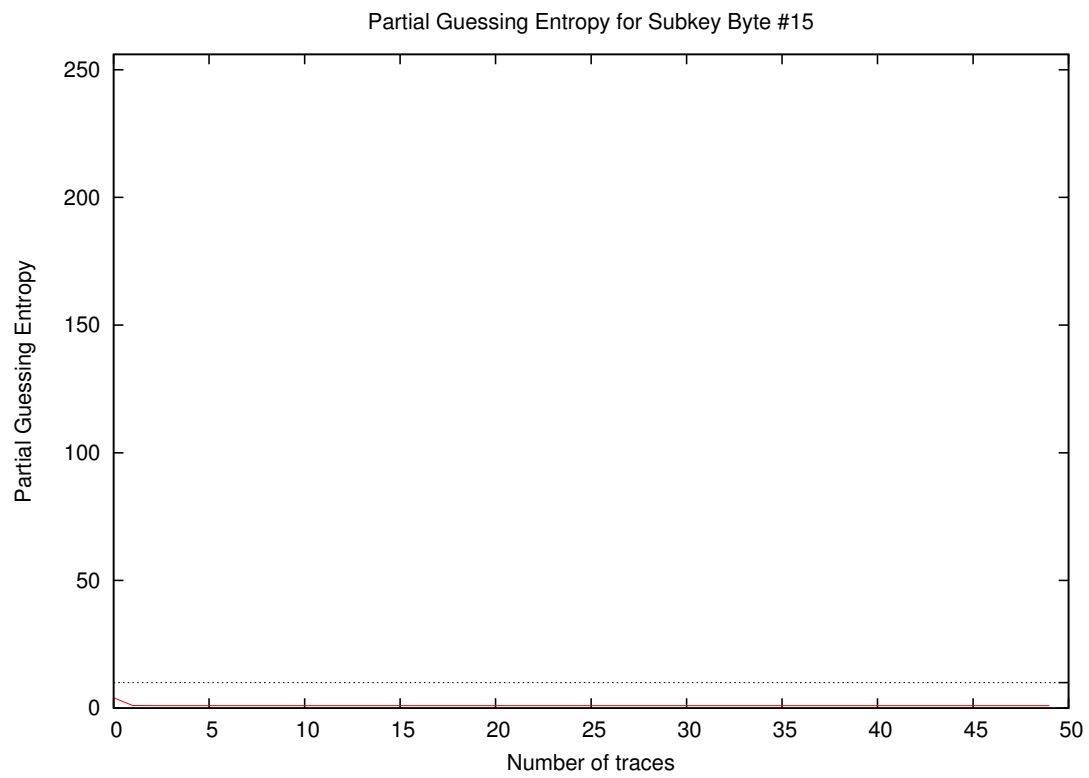


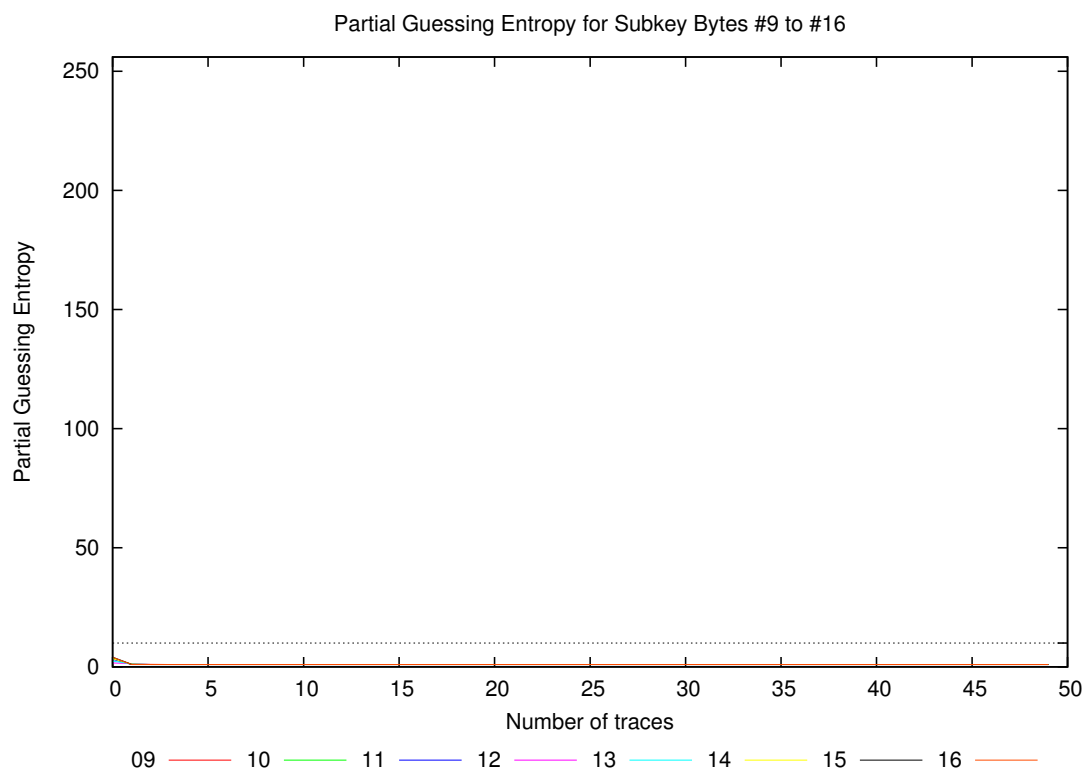
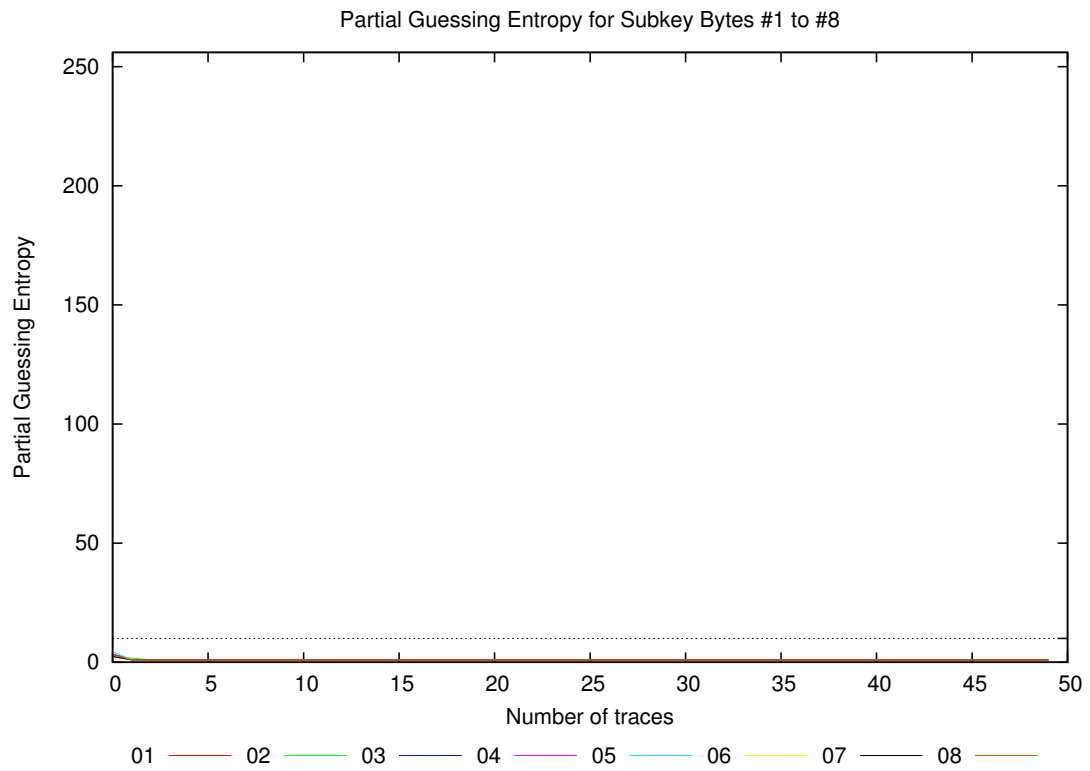
Partial Guessing Entropy for Subkey Byte #13



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	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
20	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
30	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
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