

# Evaluation results

DPA contest v2

December 2012

## 1 Introduction

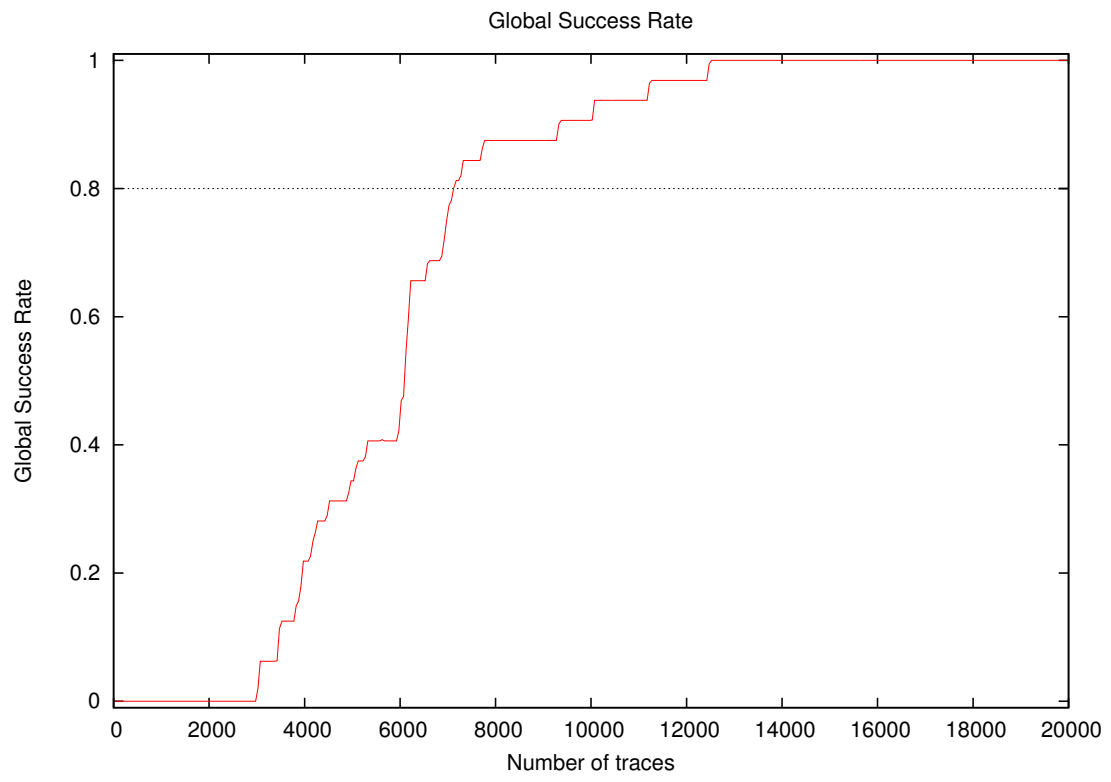
### 1.1 About the attack

- **Attack Name:** VoC exhaust
- **Sender/Team:** Suvadeep Hajra, Debdeep Mukhopadhyay
- **Institution:** Indian Institute of Technology Kharagpur
- **Language:** C++
- **Attacked subkey:** 10

### 1.2 About the evaluation

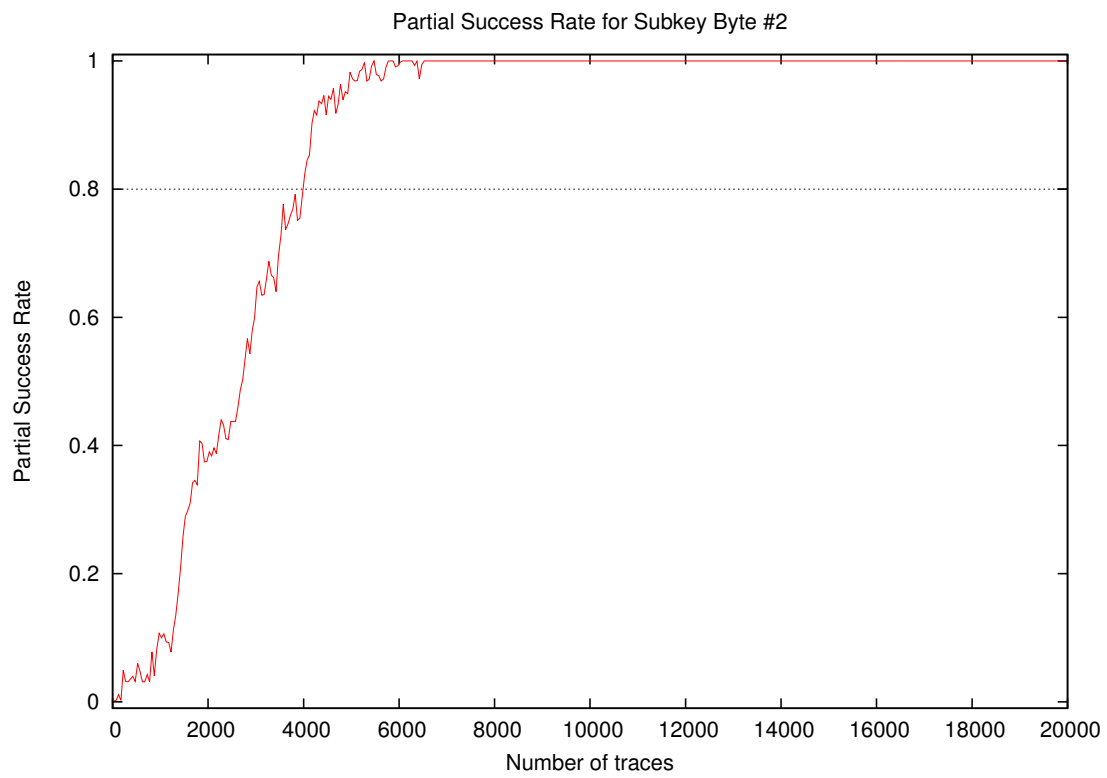
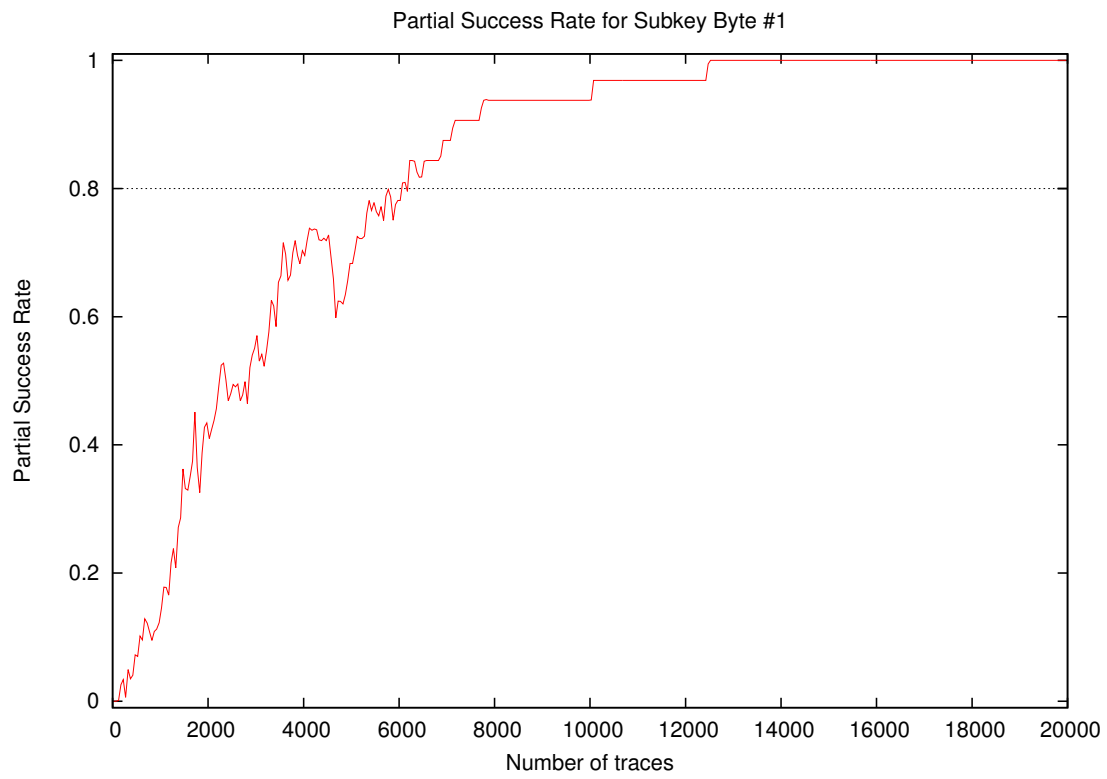
- **Date of evaluation:** December 2012

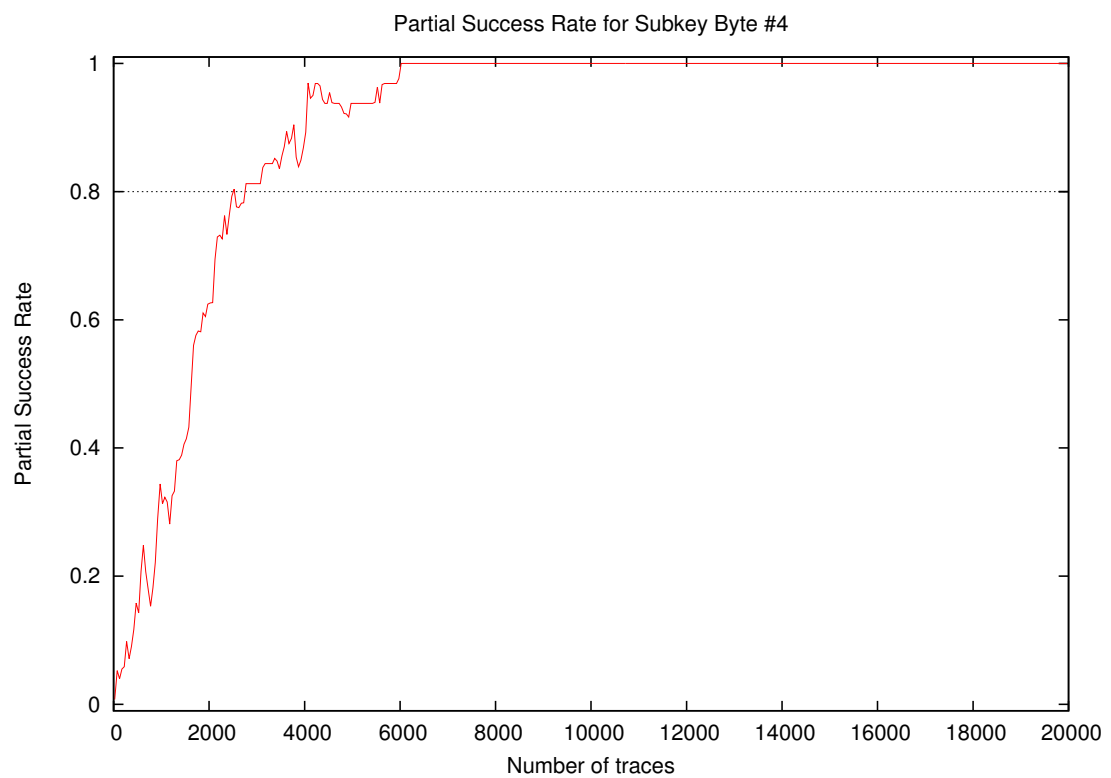
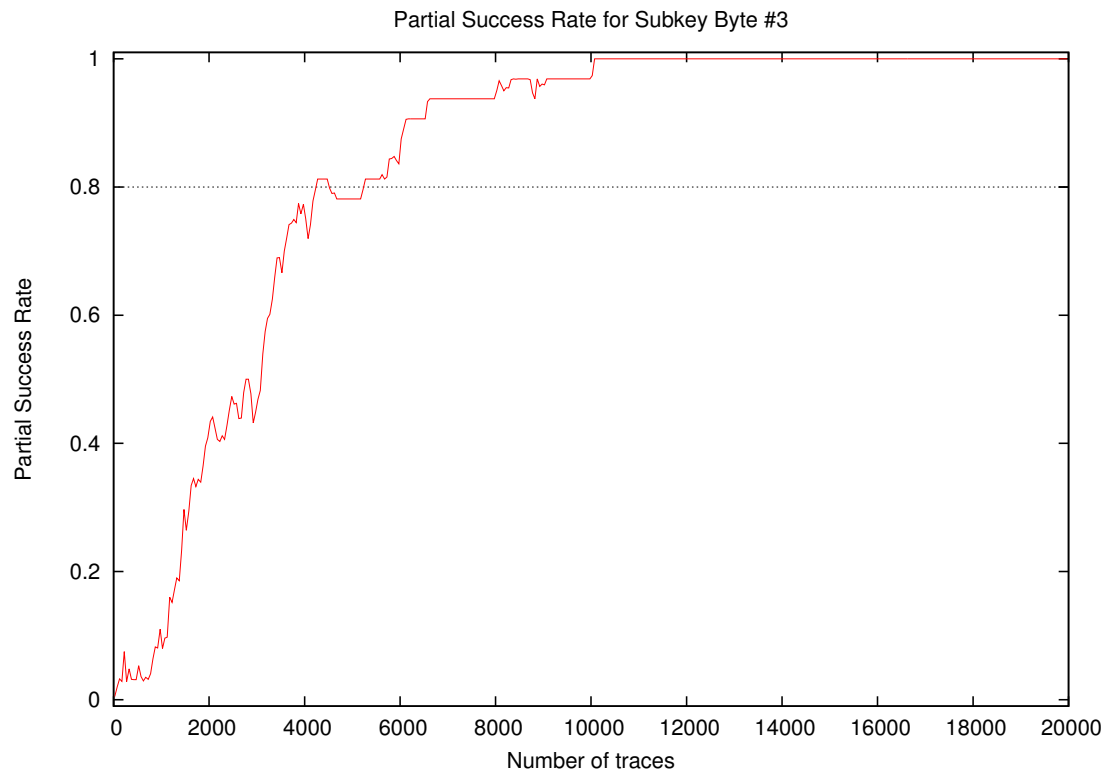
## 2 Global Success Rate

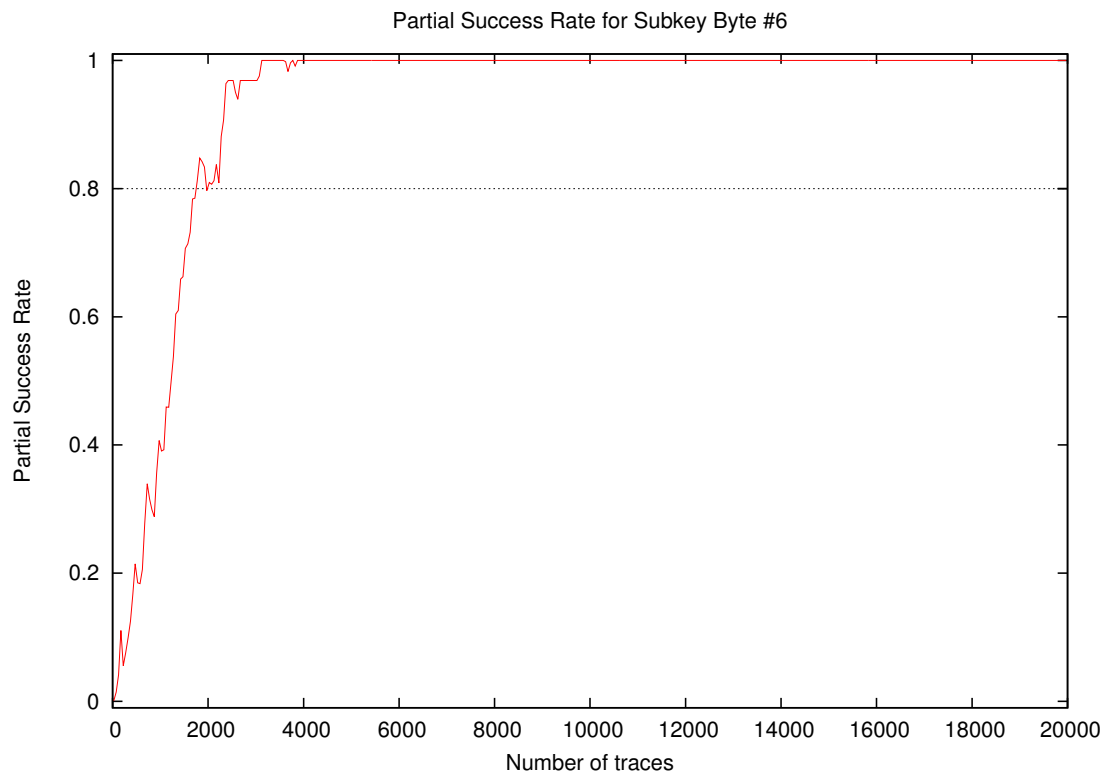
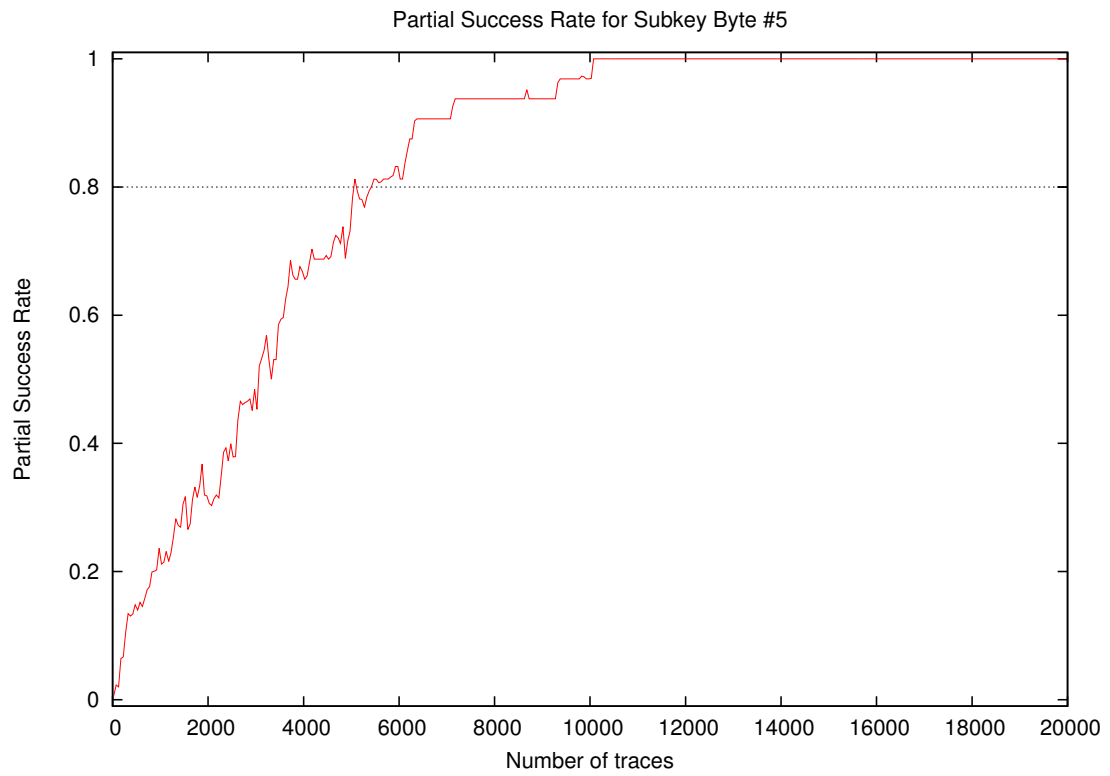


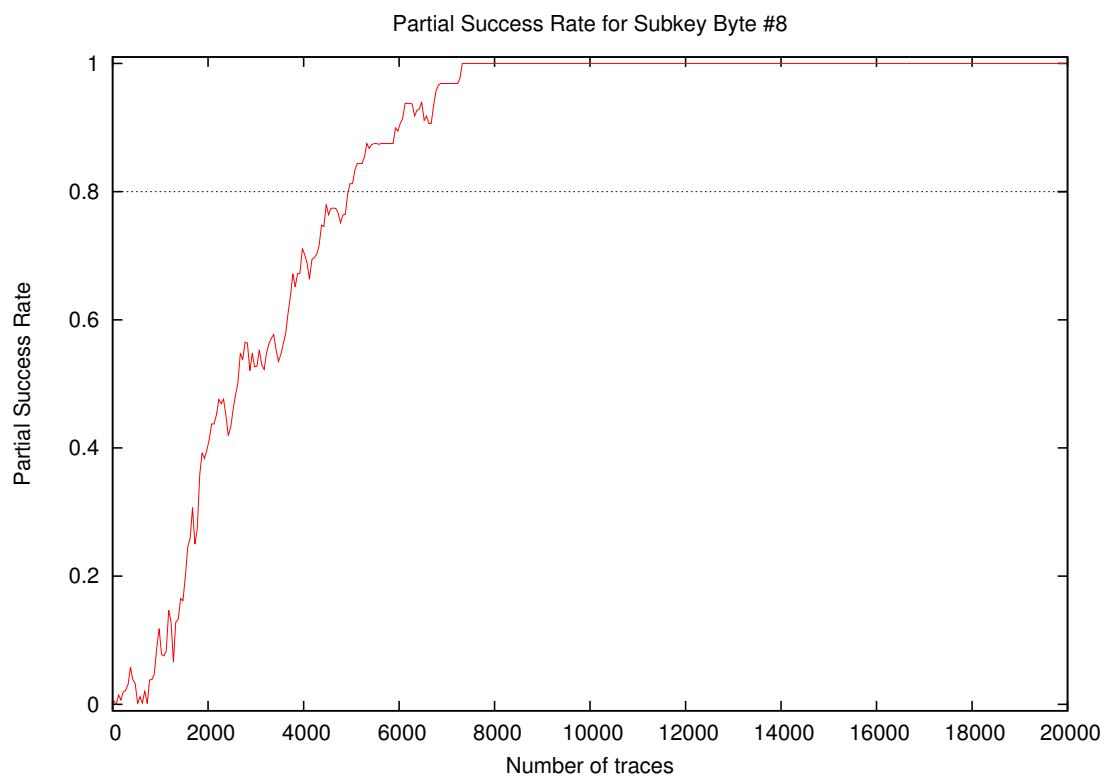
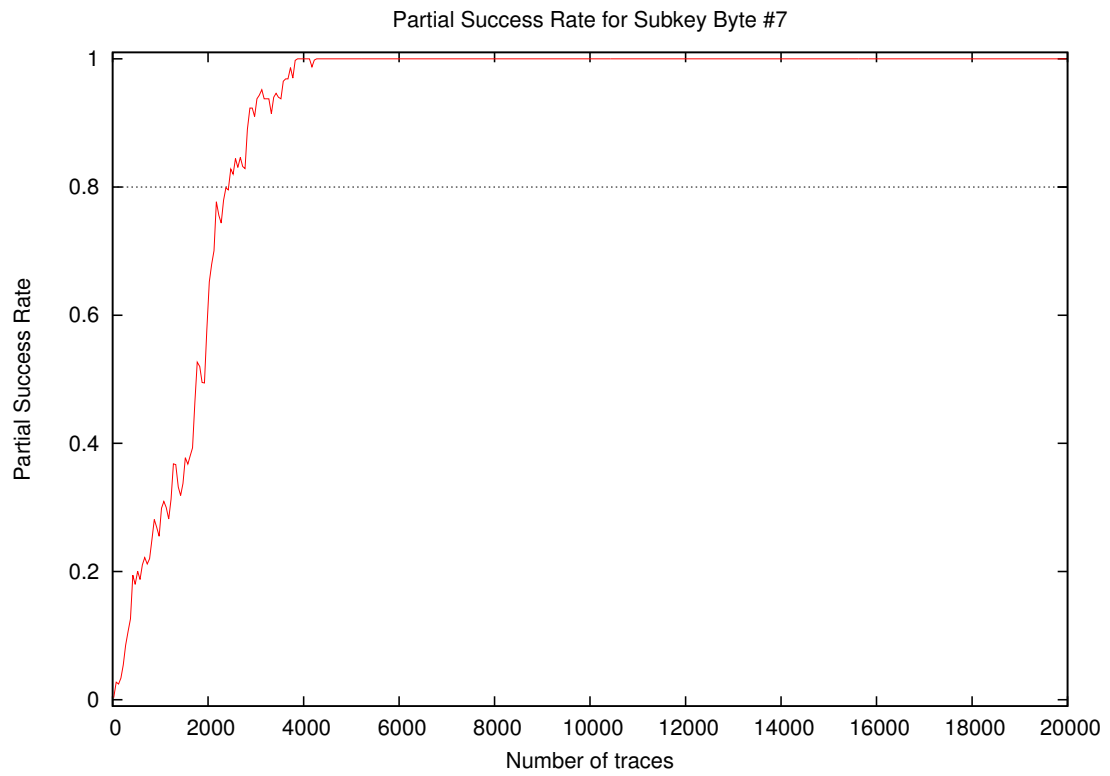
| Number of traces | Global Success Rate |
|------------------|---------------------|
| 10               | 0.00                |
| 20               | 0.00                |
| 30               | 0.00                |
| 40               | 0.00                |
| 50               | 0.00                |
| 100              | 0.00                |
| 200              | 0.00                |
| 300              | 0.00                |
| 400              | 0.00                |
| 500              | 0.00                |
| 1000             | 0.00                |
| 2000             | 0.00                |
| 3000             | 0.00                |
| 4000             | 0.22                |
| 5000             | 0.34                |
| 10000            | 0.91                |
| 15000            | 1.00                |
| 20000            | 1.00                |

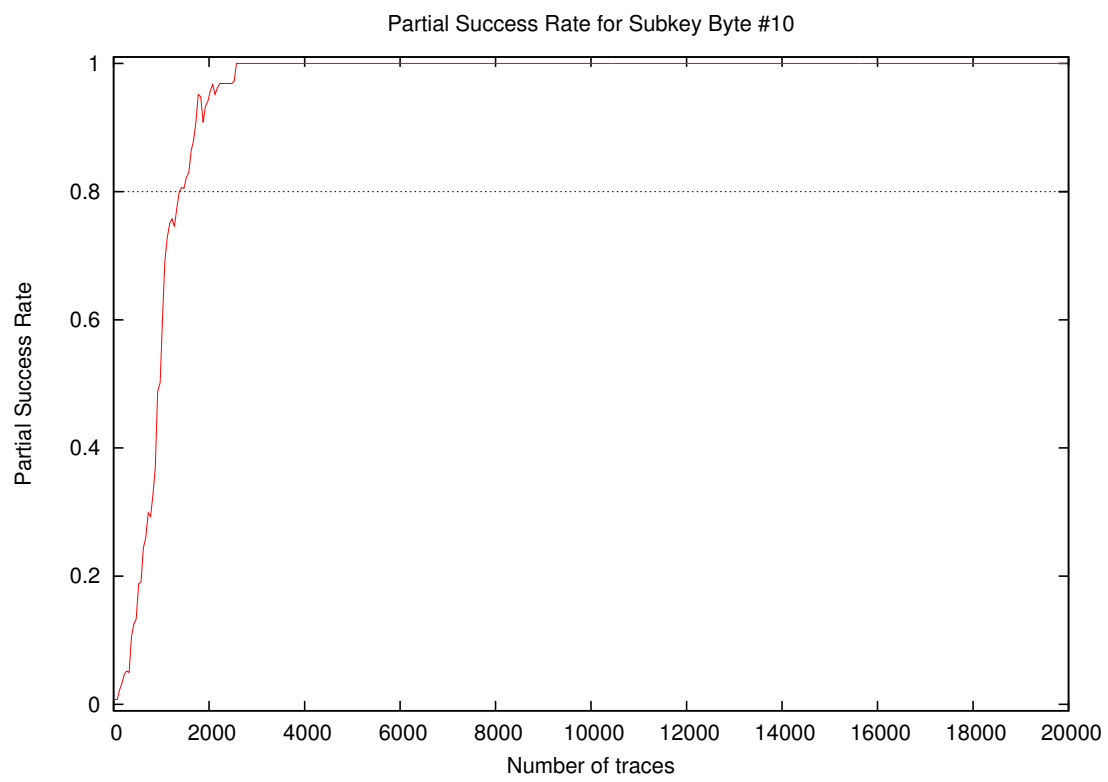
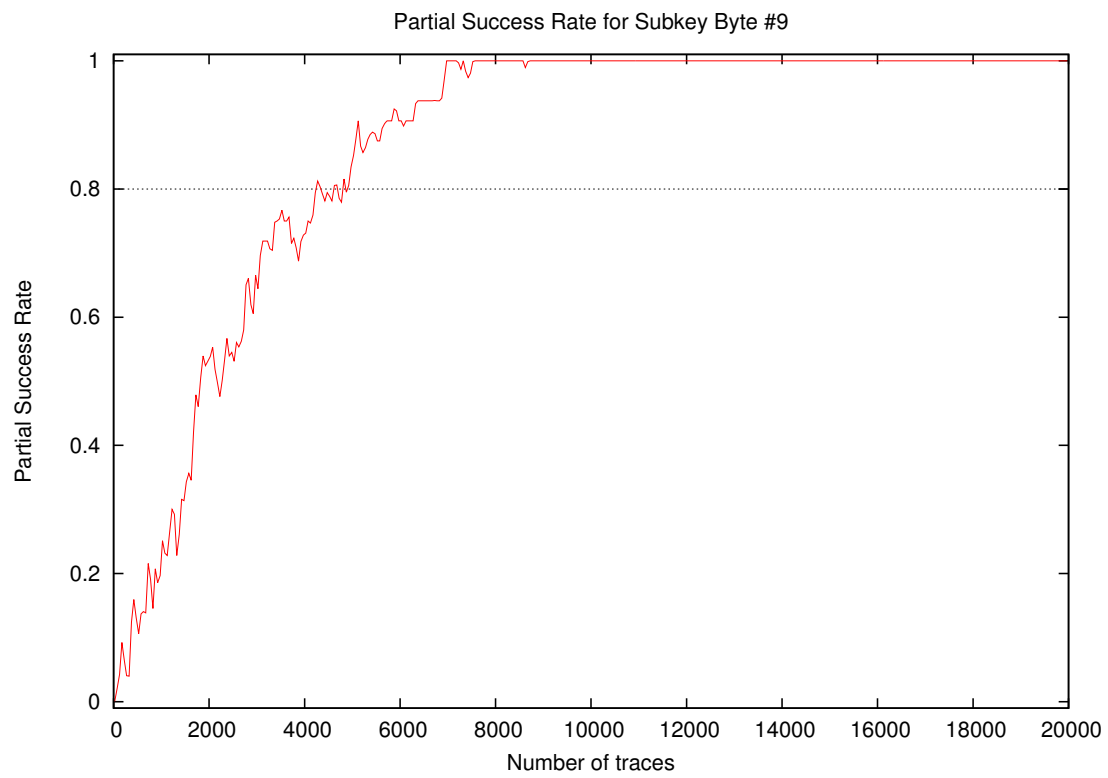
### 3 Partial Success Rate



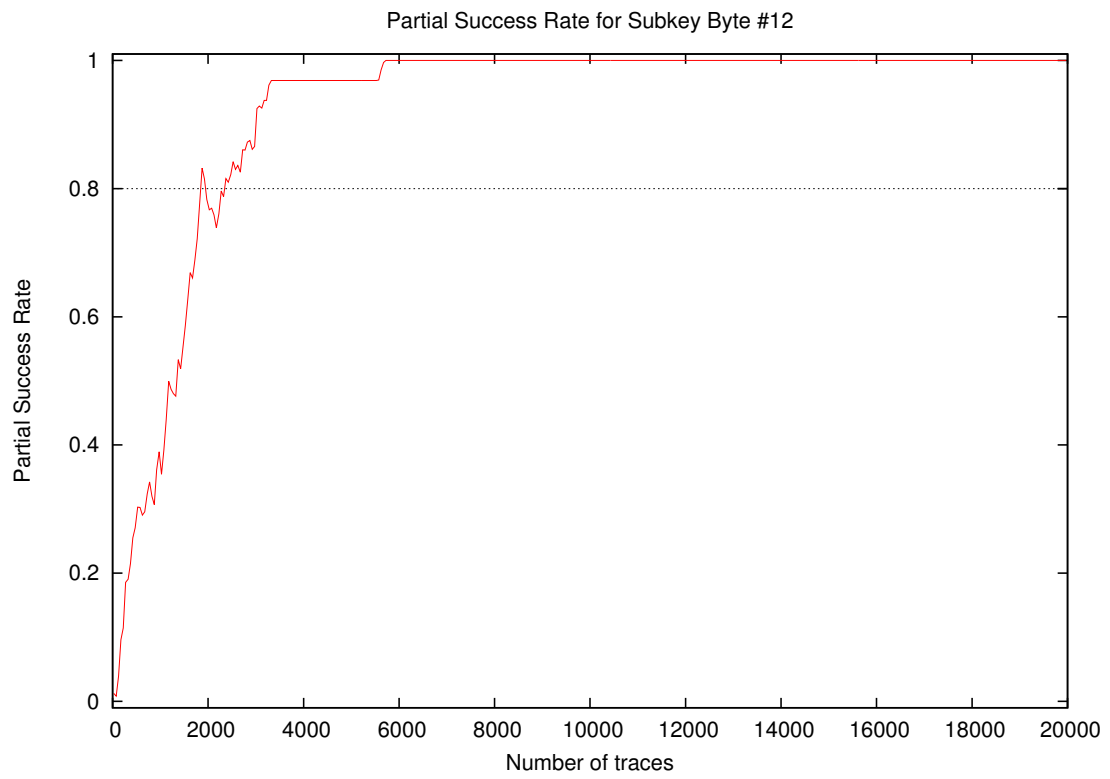
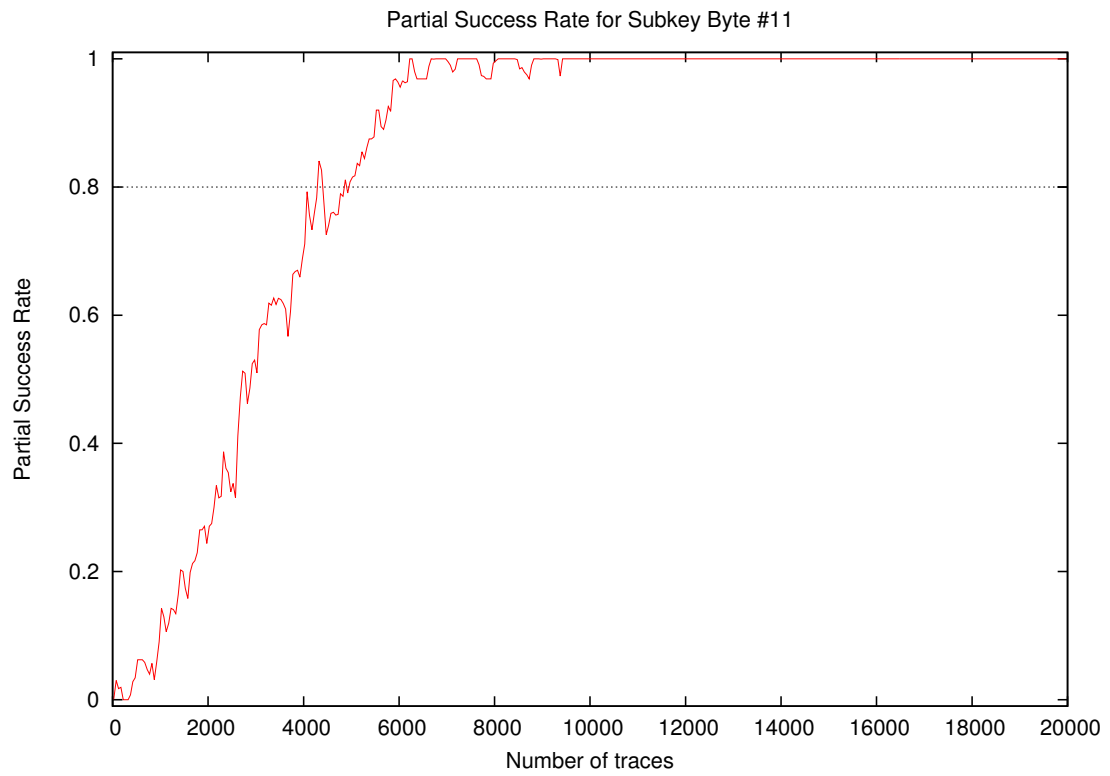


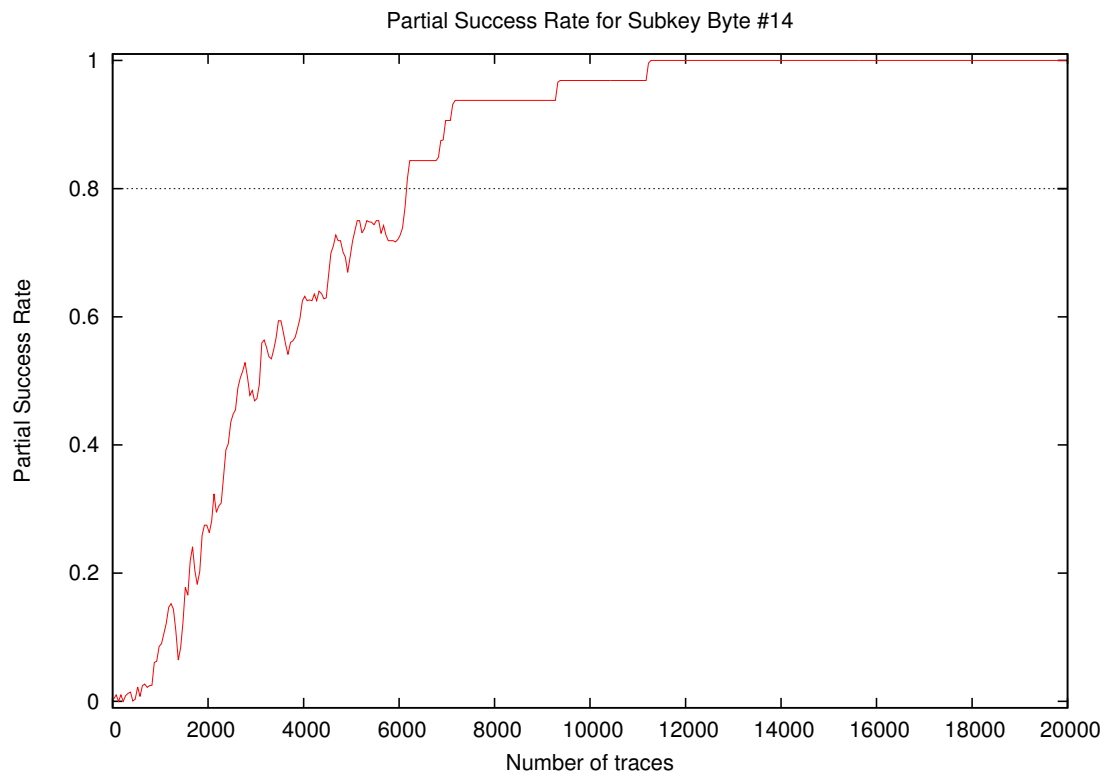
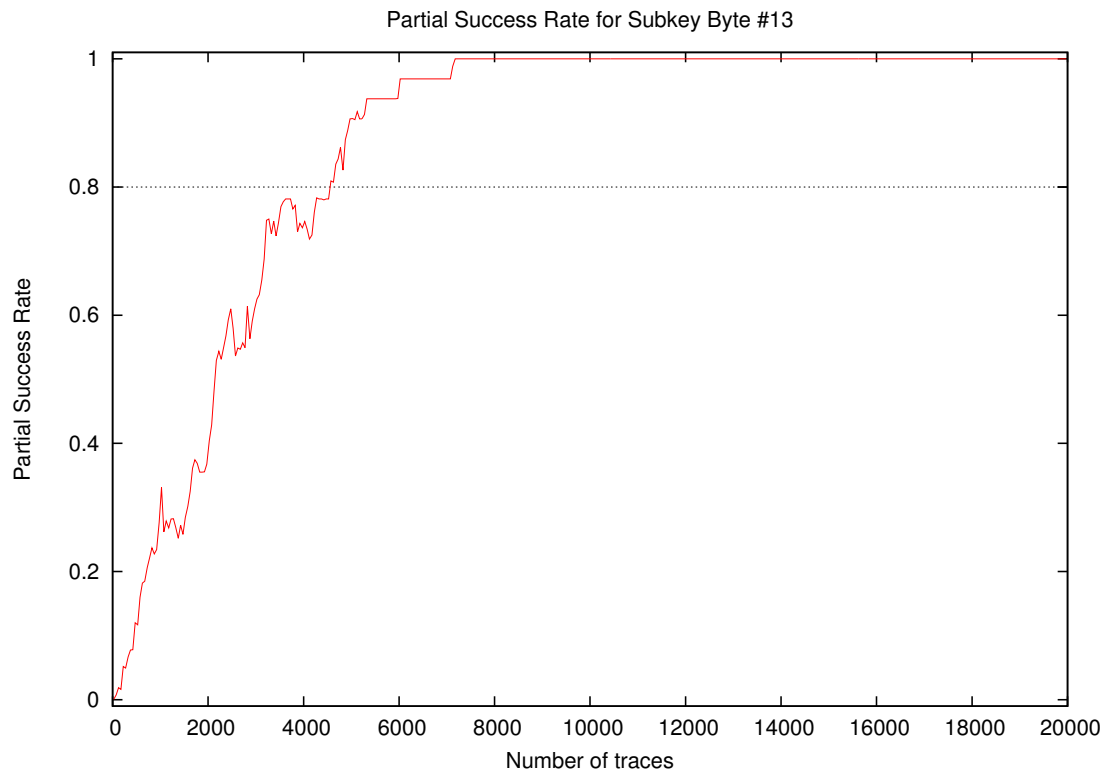


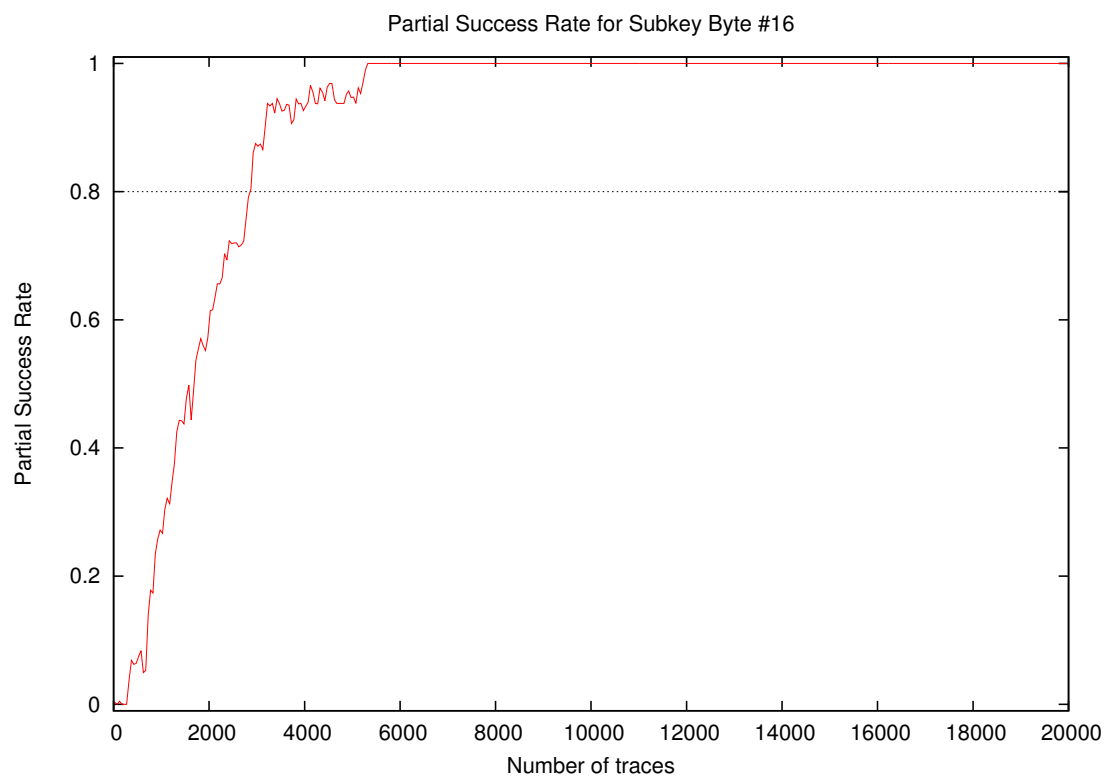
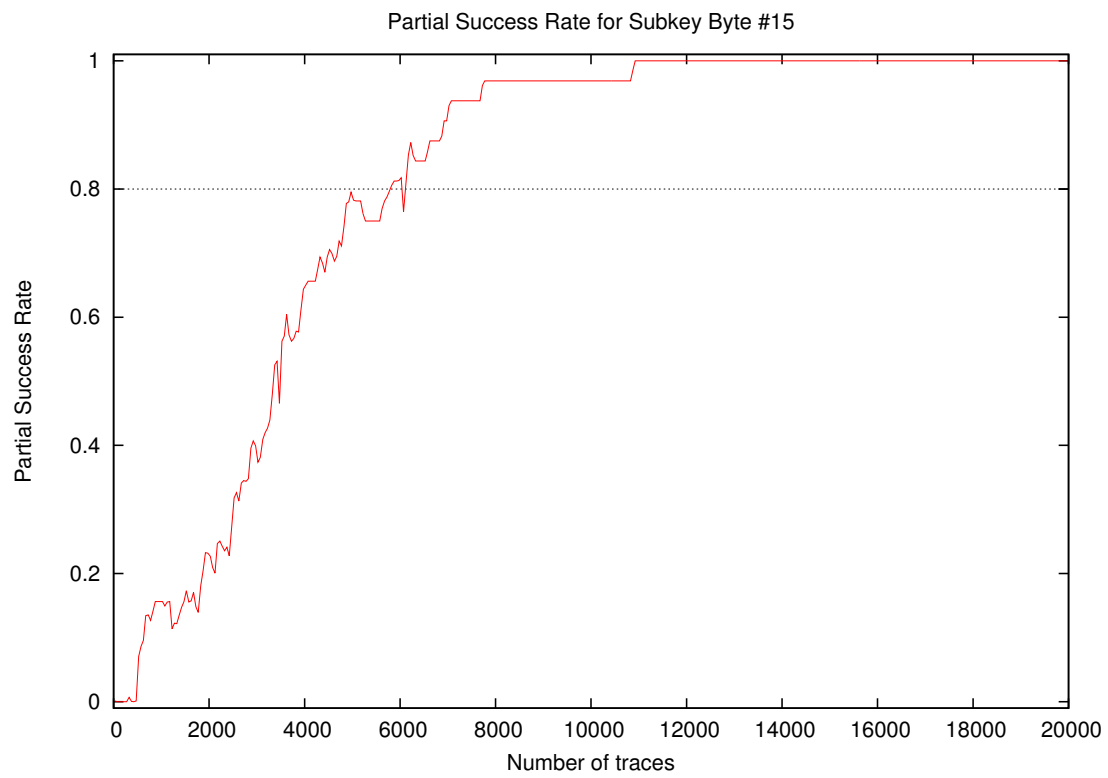


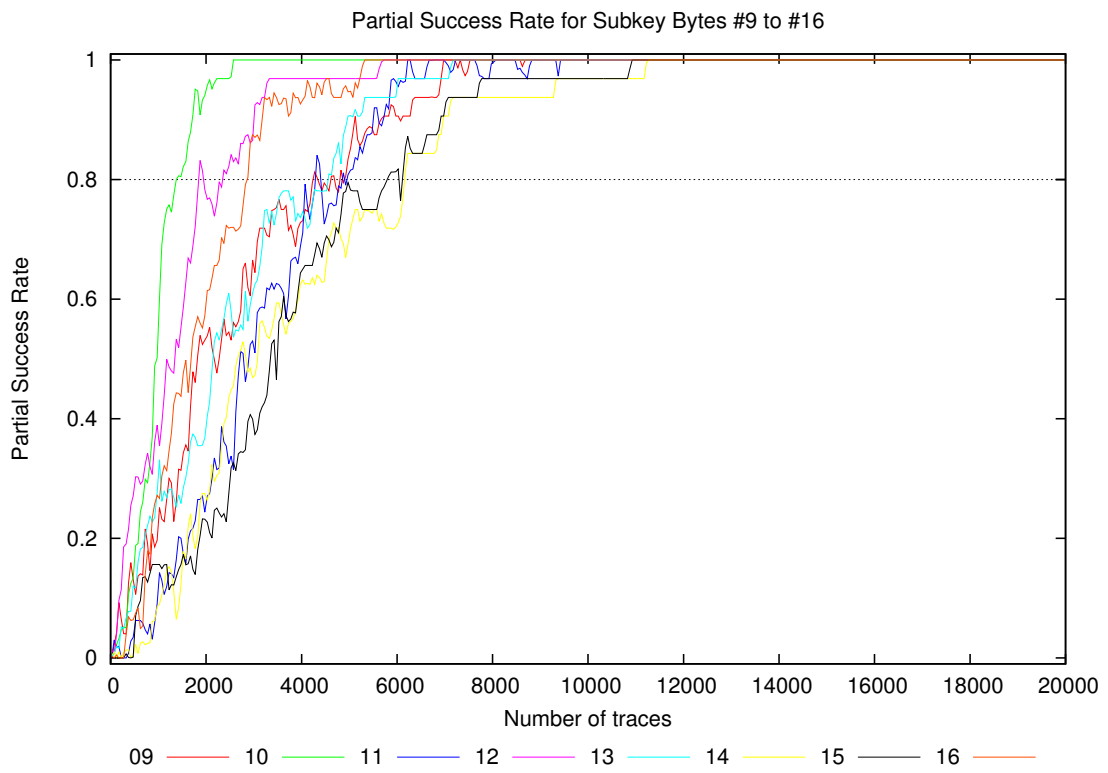
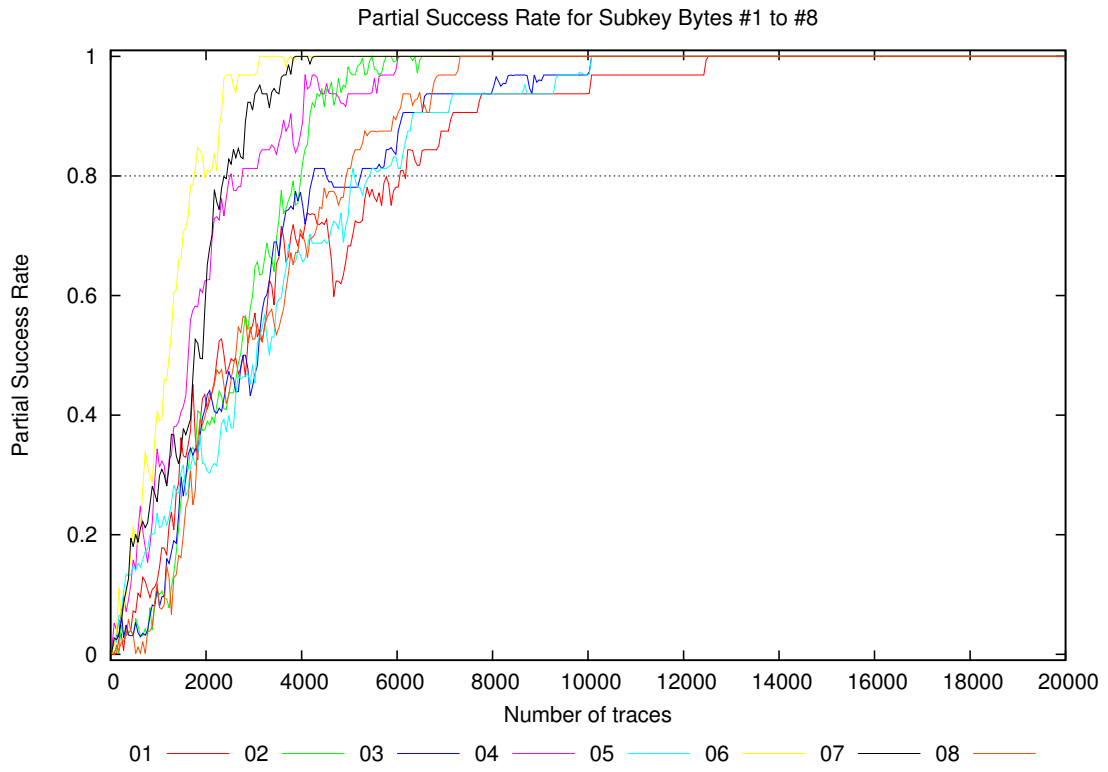


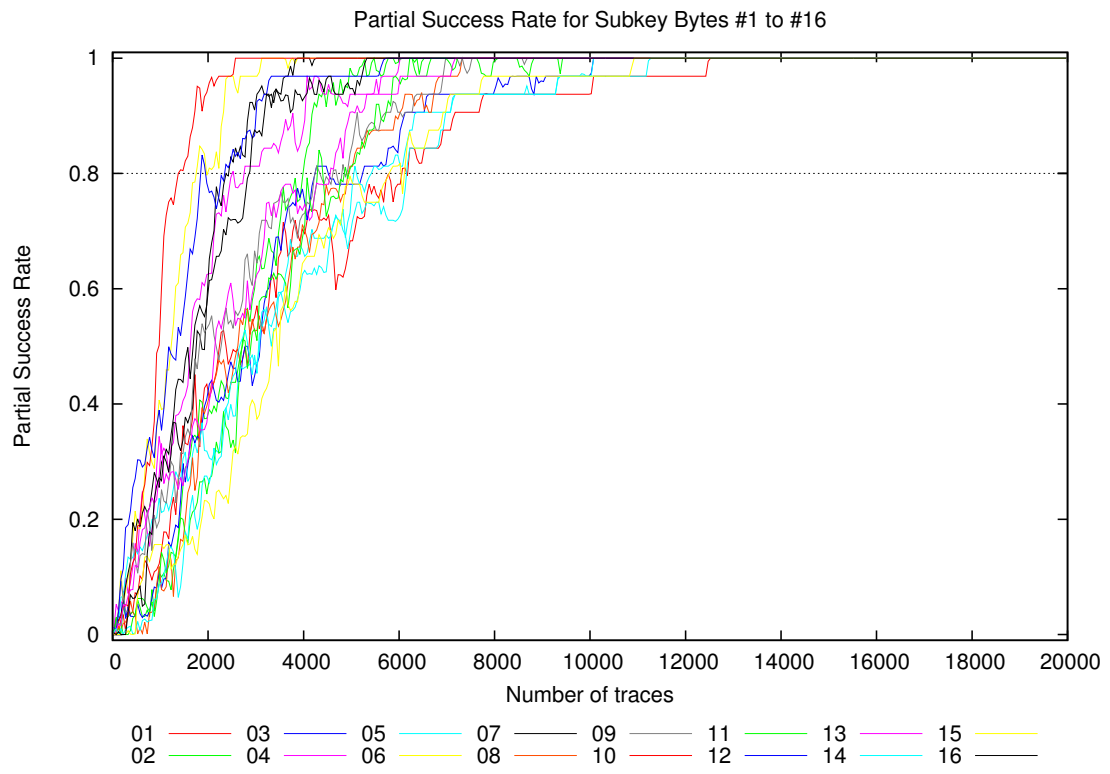






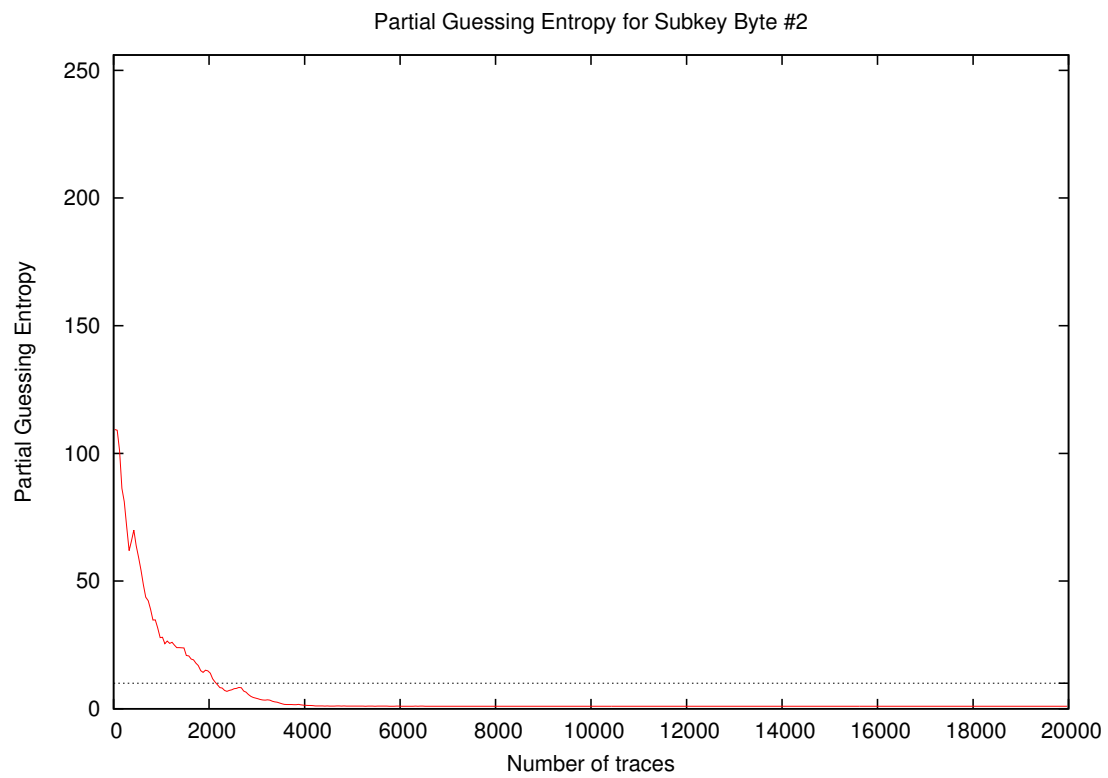
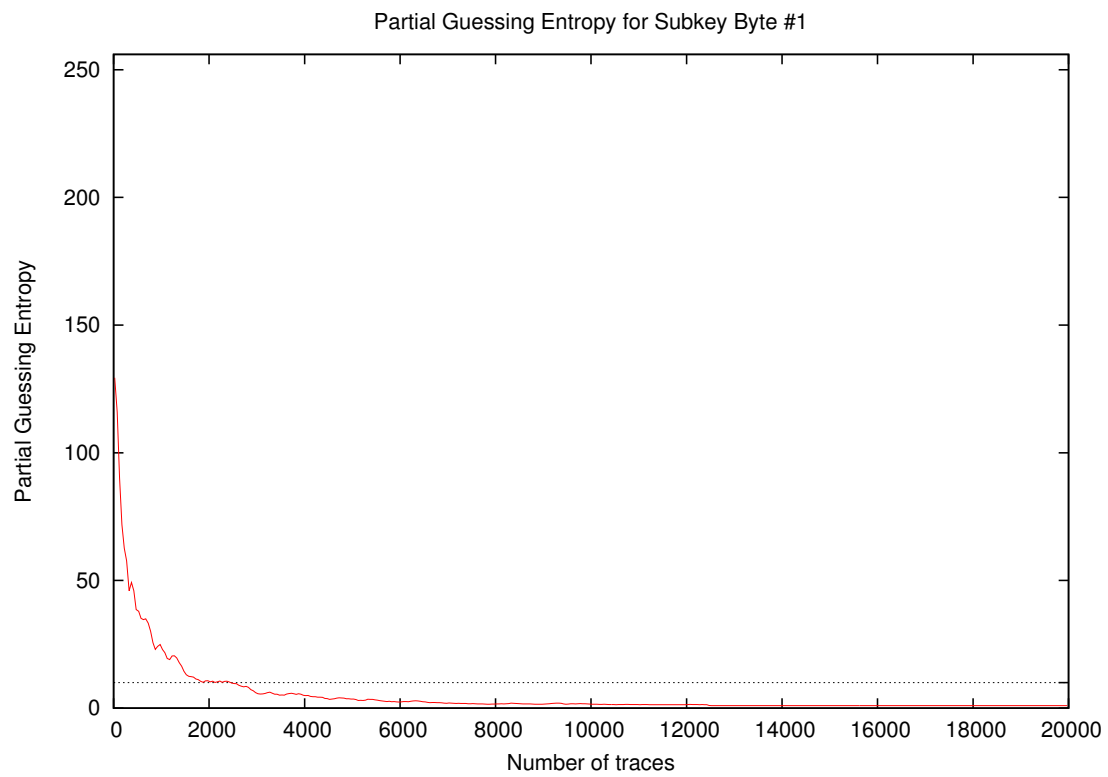




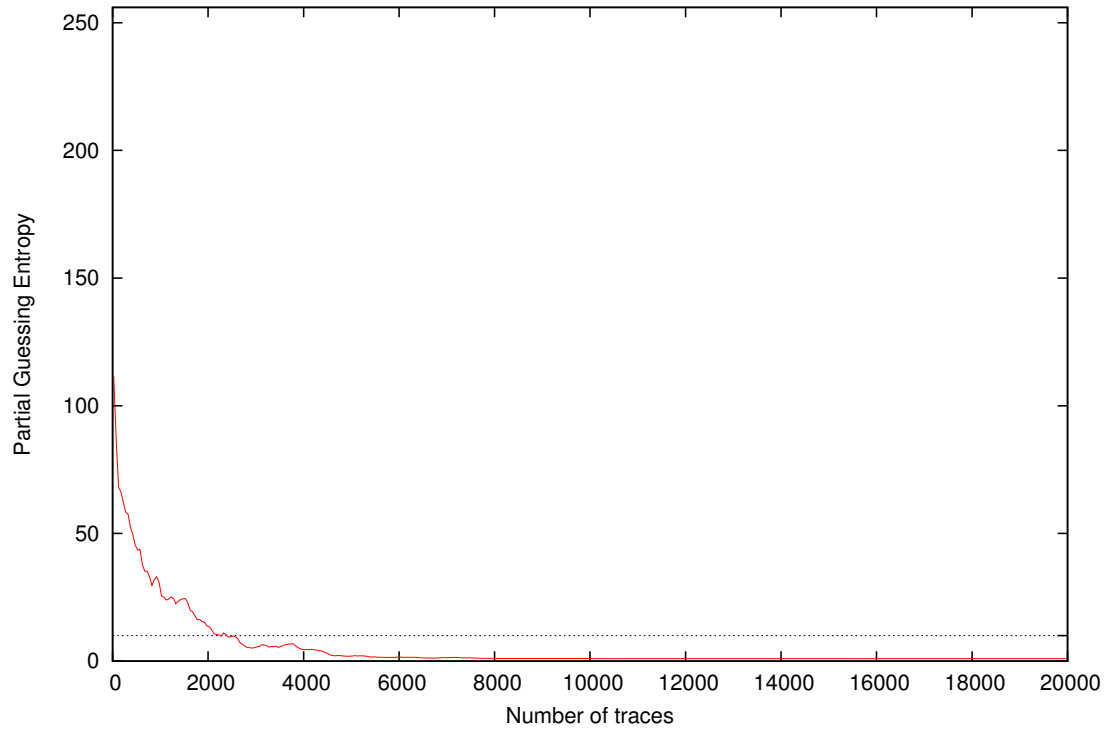




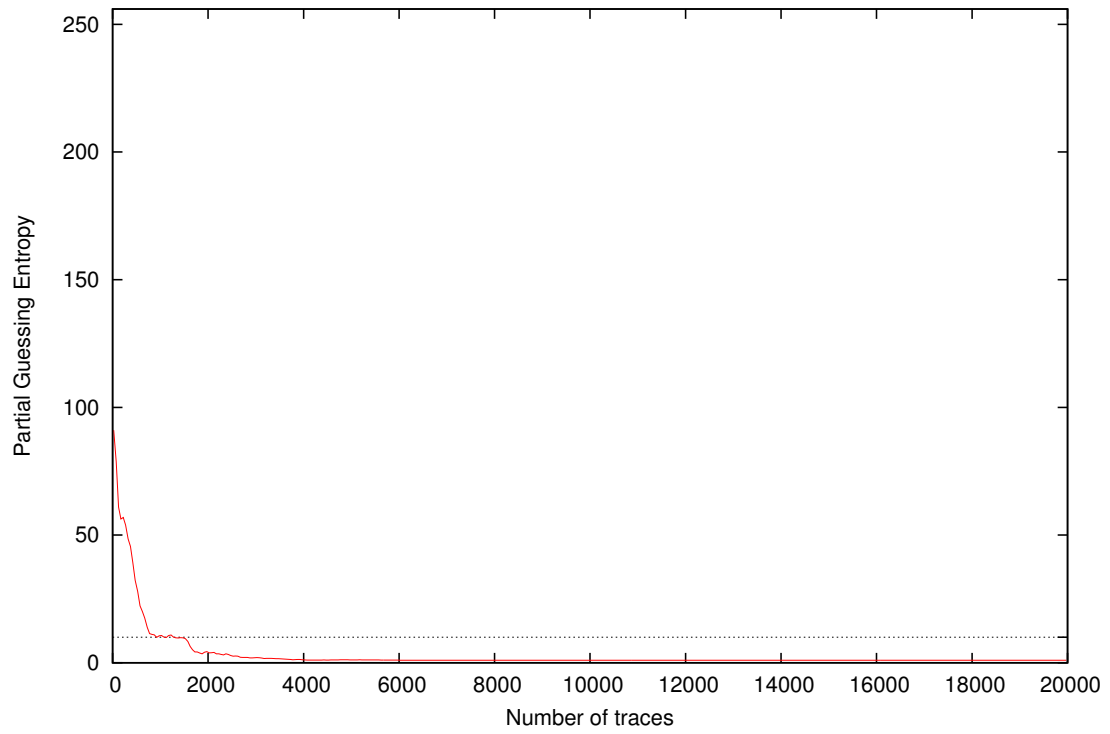
## 4 Partial Guessing Entropy



Partial Guessing Entropy for Subkey Byte #3

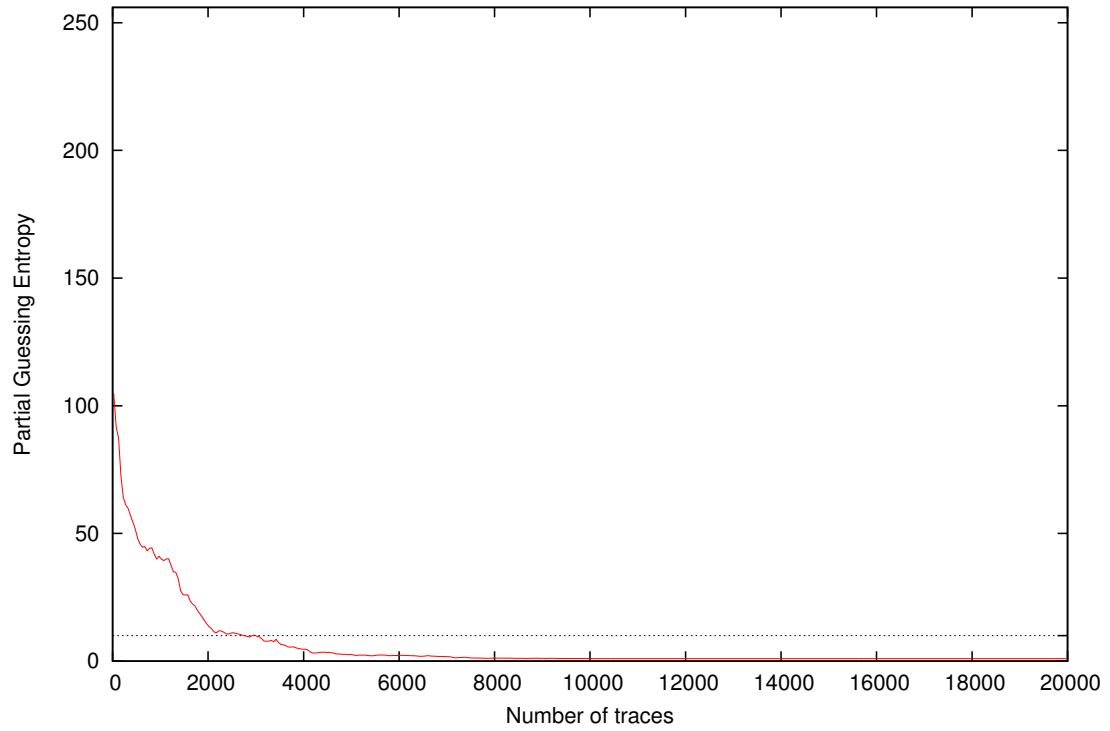


Partial Guessing Entropy for Subkey Byte #4

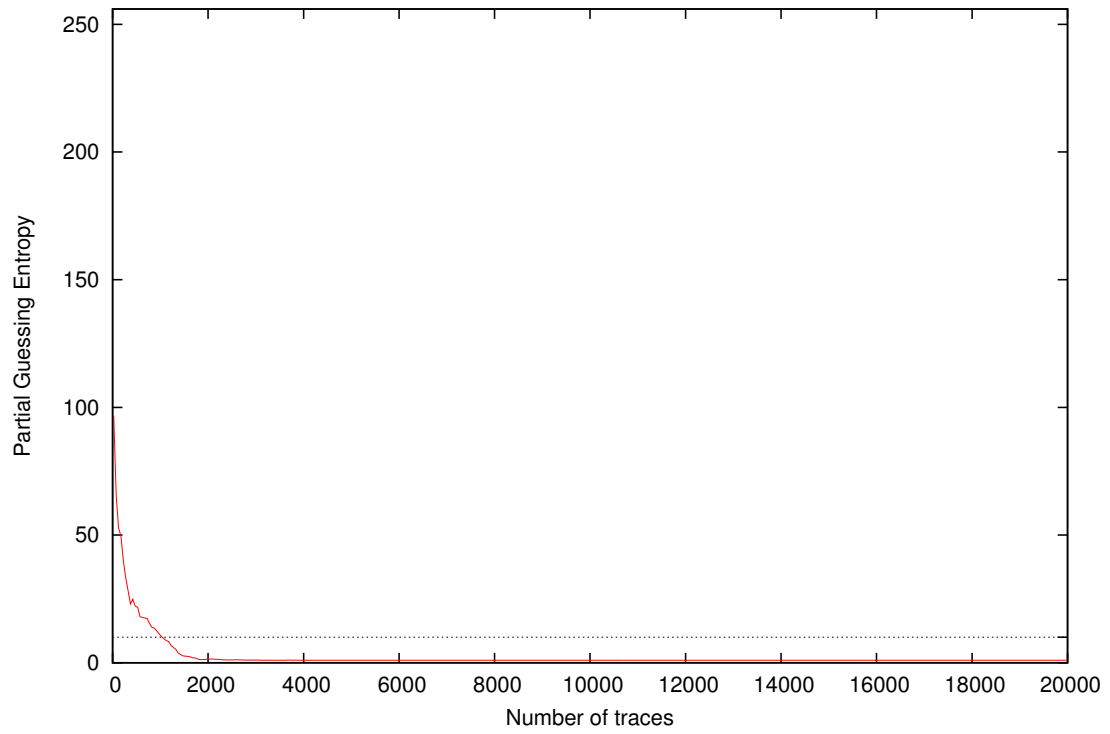




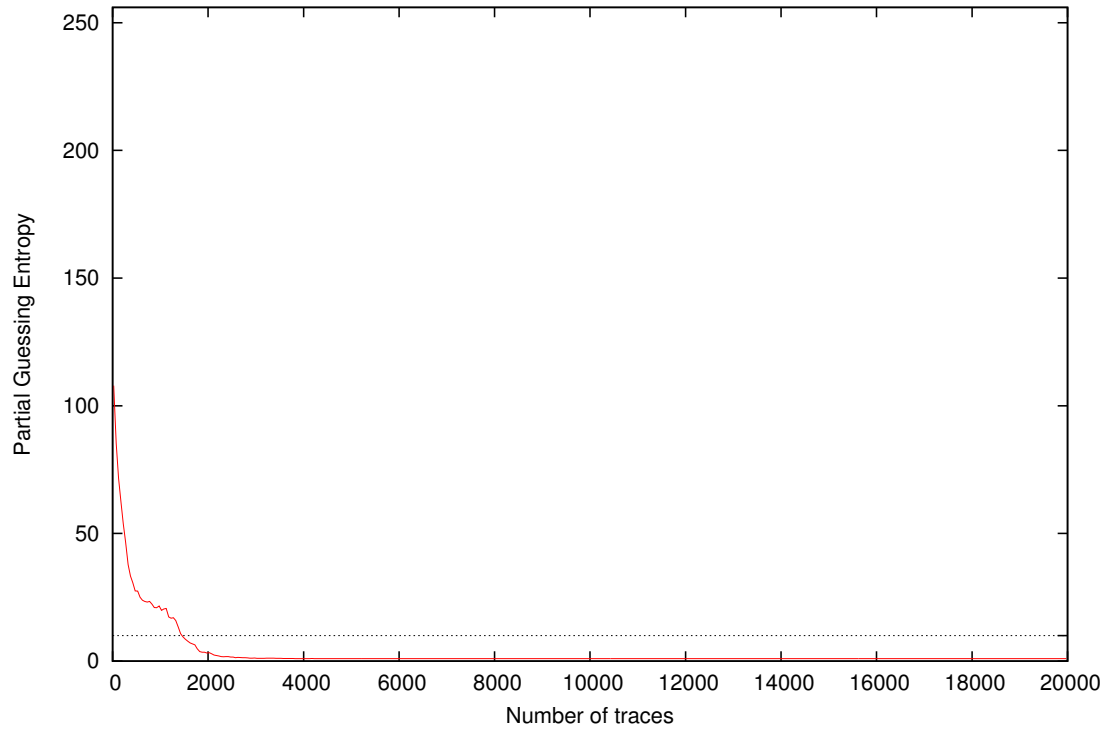
Partial Guessing Entropy for Subkey Byte #5



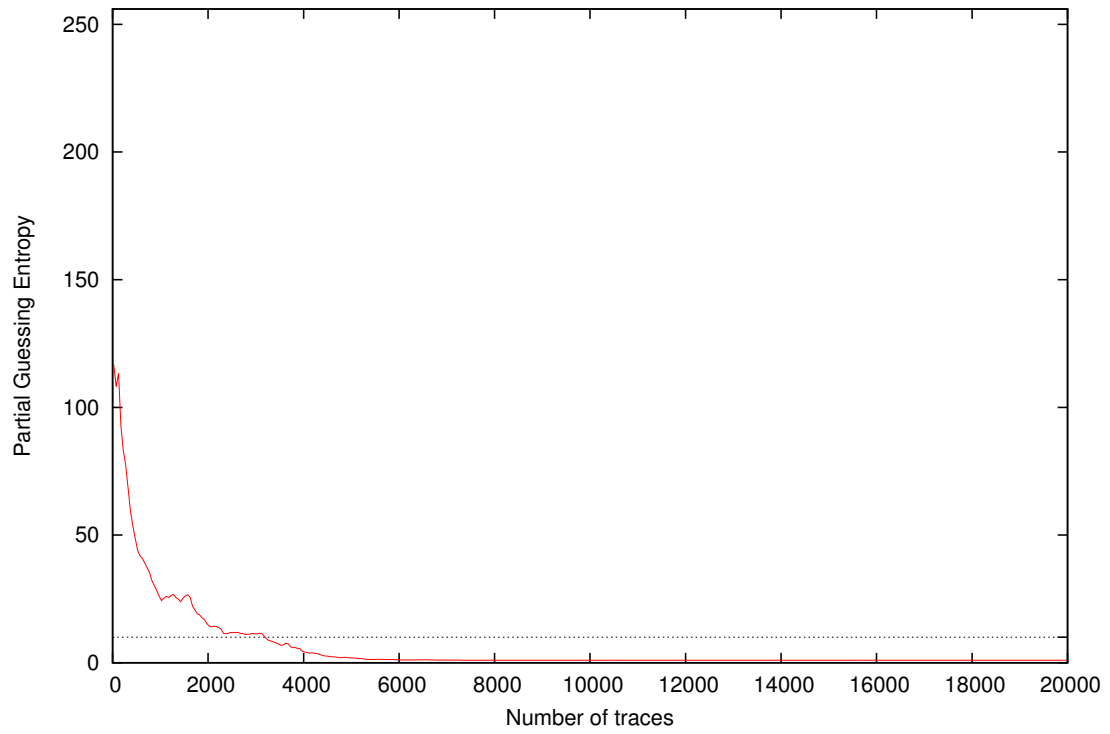
Partial Guessing Entropy for Subkey Byte #6



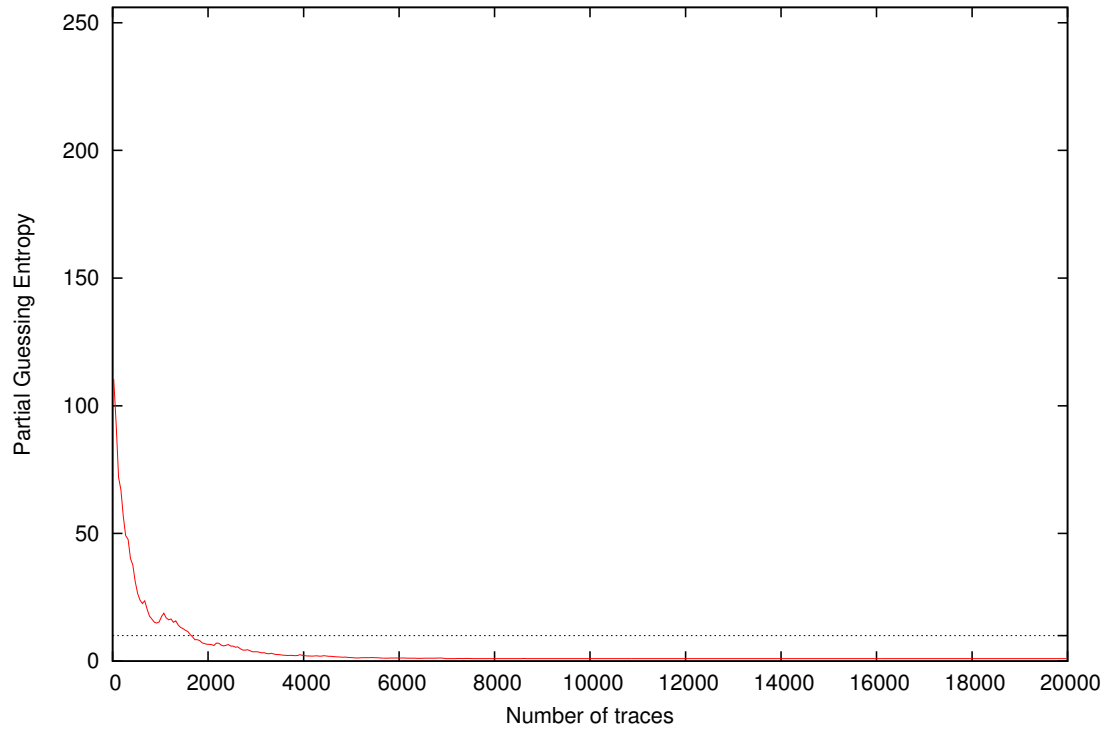
Partial Guessing Entropy for Subkey Byte #7



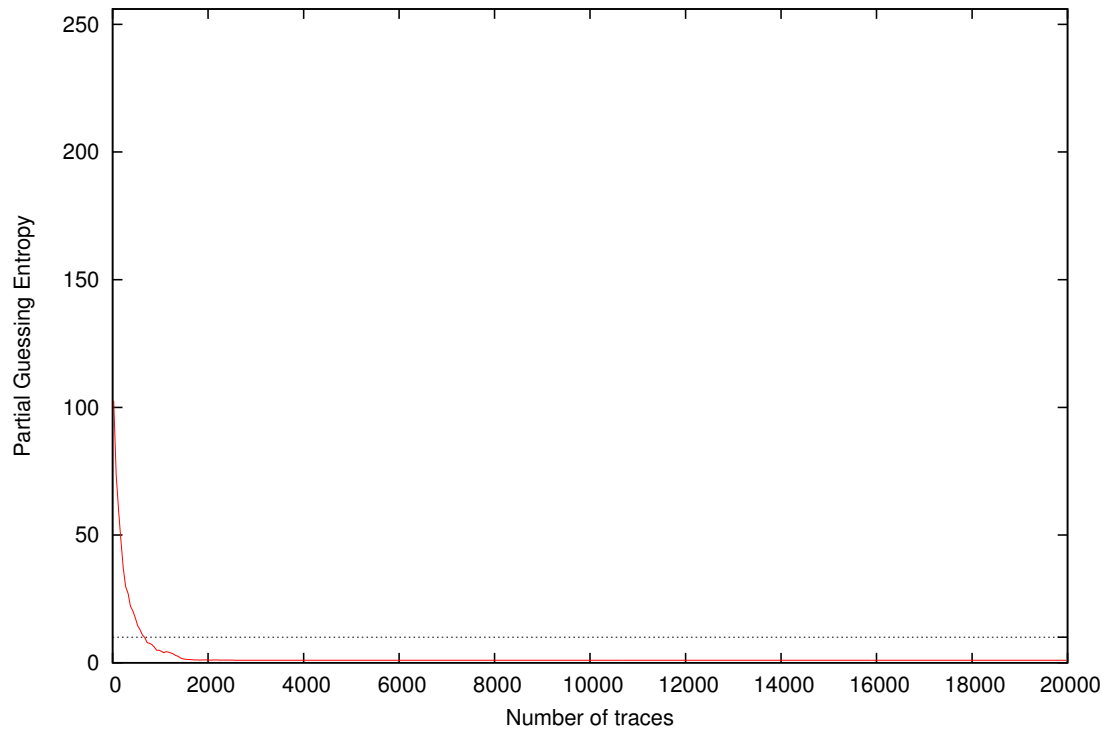
Partial Guessing Entropy for Subkey Byte #8



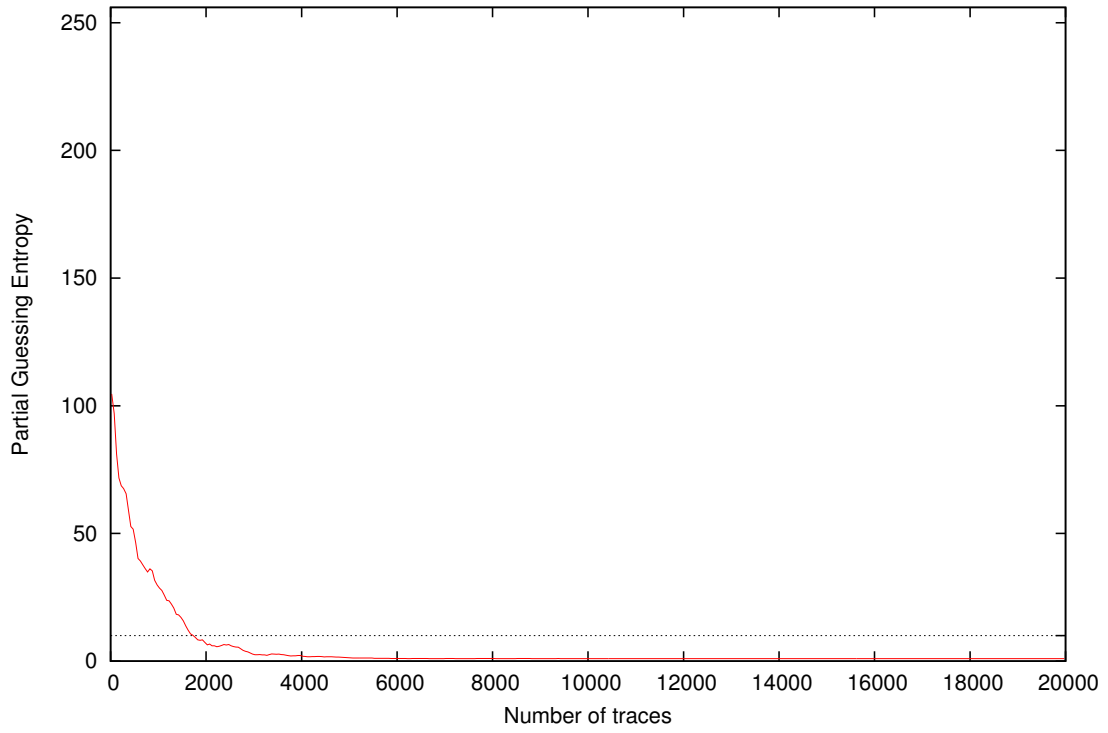
Partial Guessing Entropy for Subkey Byte #9



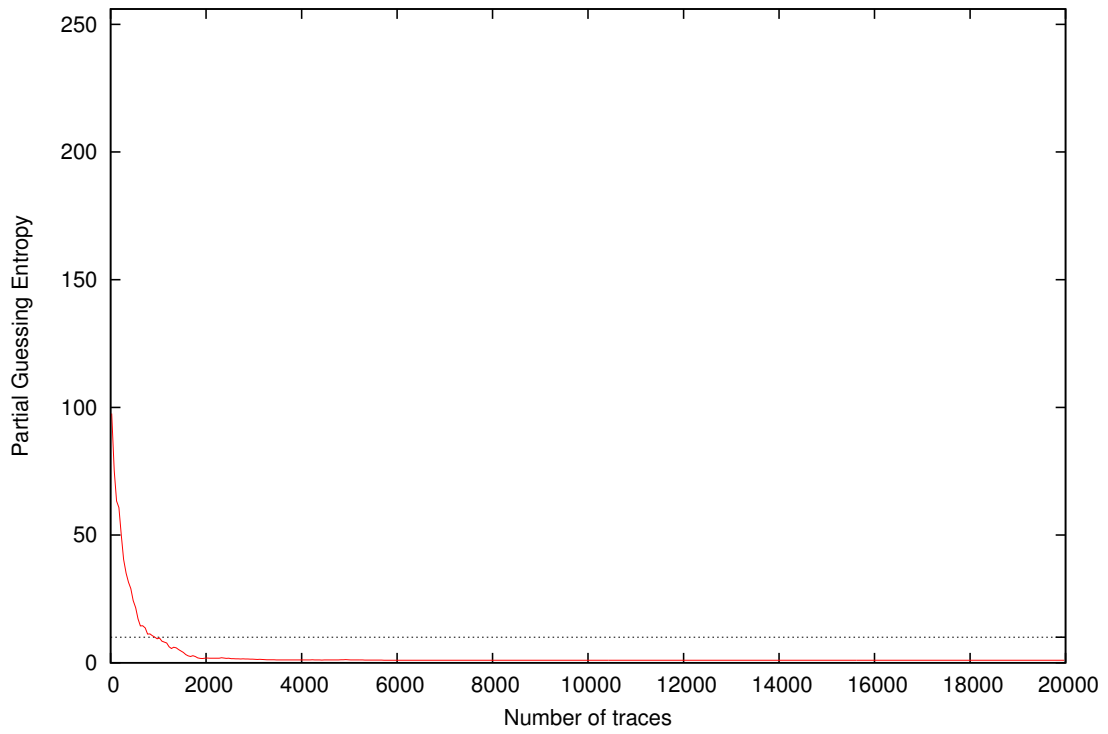
Partial Guessing Entropy for Subkey Byte #10



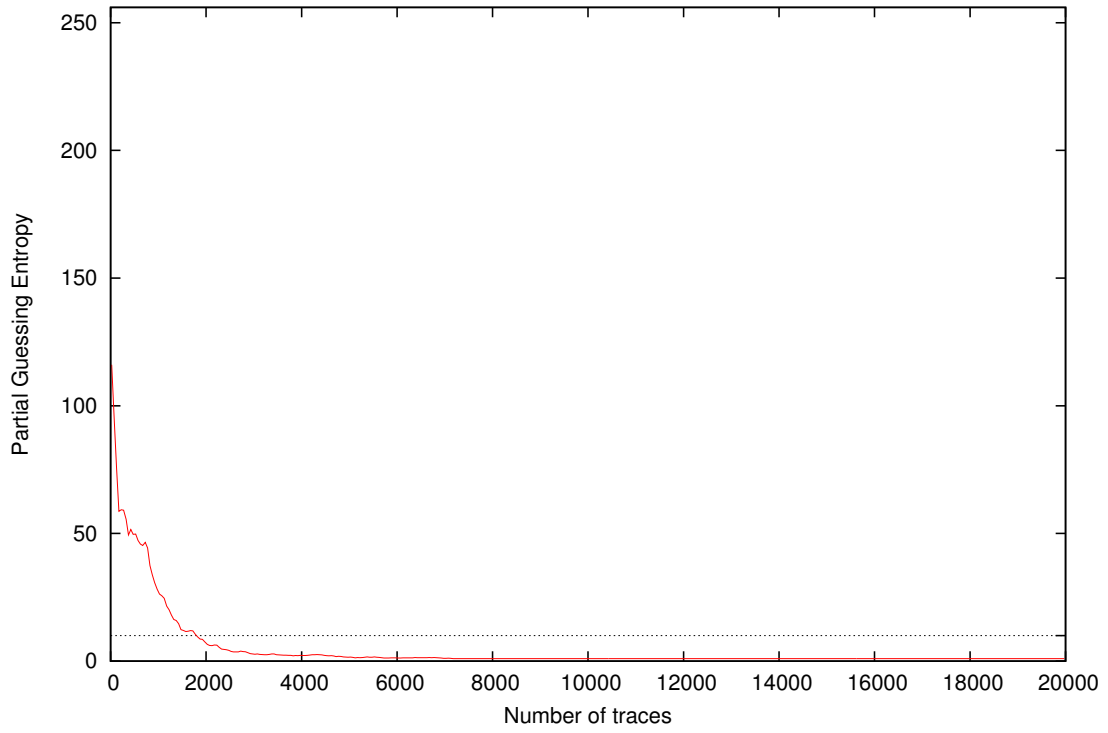
Partial Guessing Entropy for Subkey Byte #11



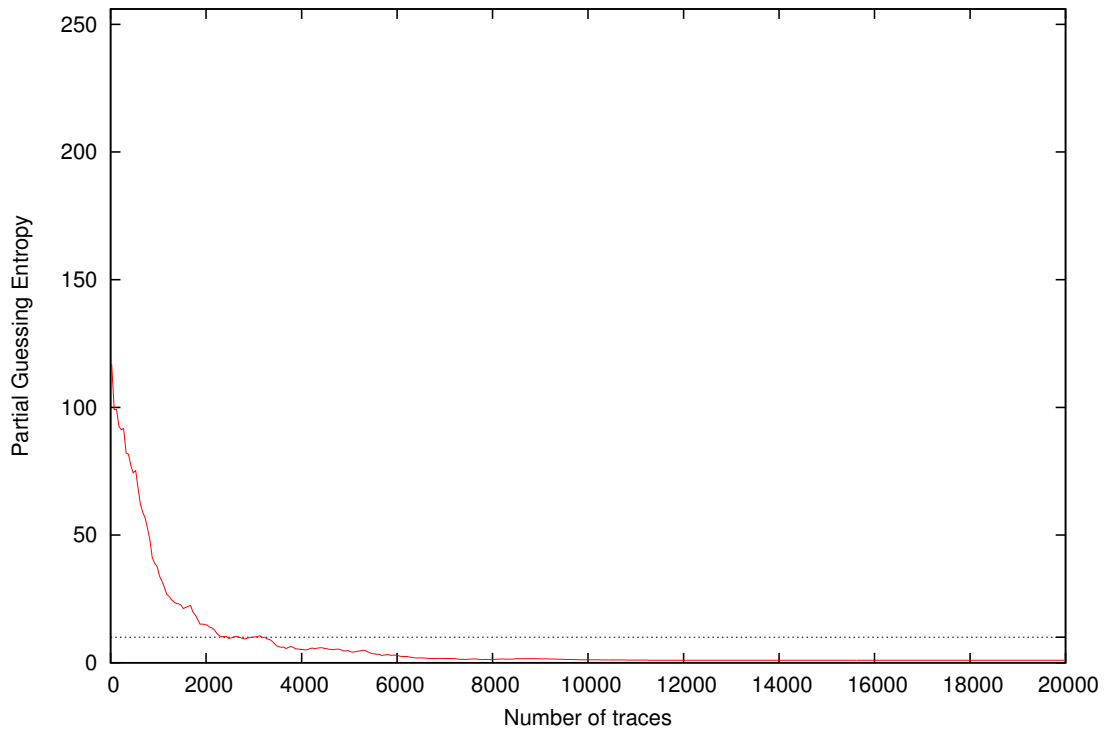
Partial Guessing Entropy for Subkey Byte #12



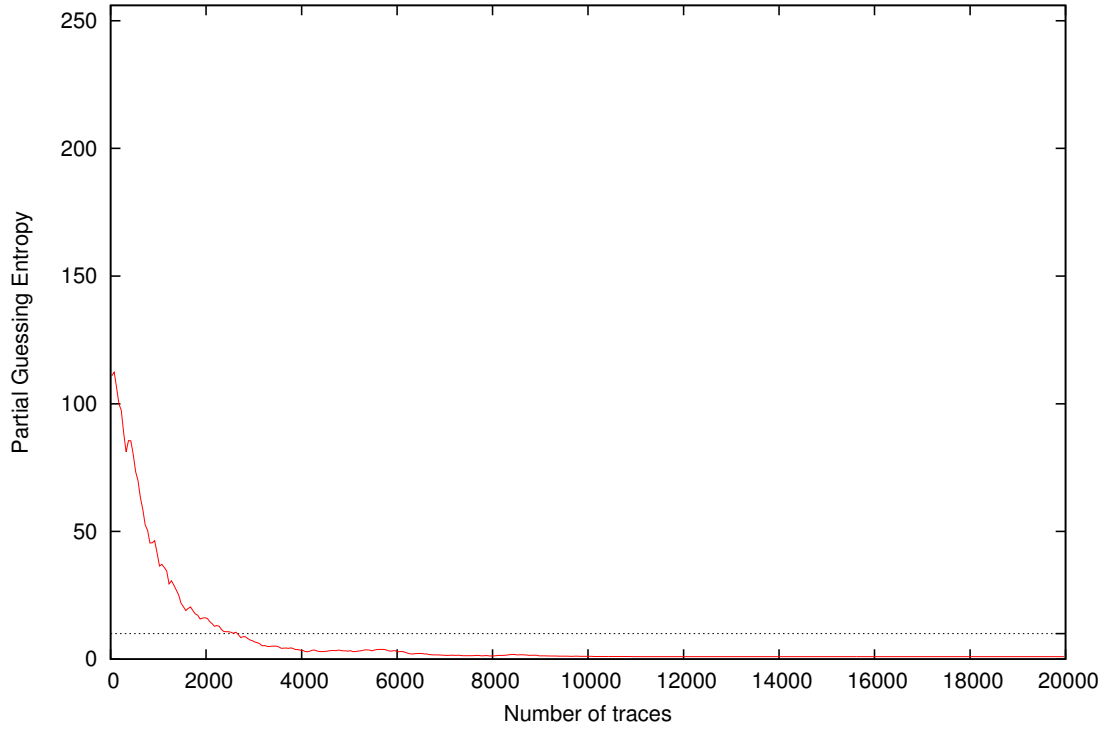
Partial Guessing Entropy for Subkey Byte #13



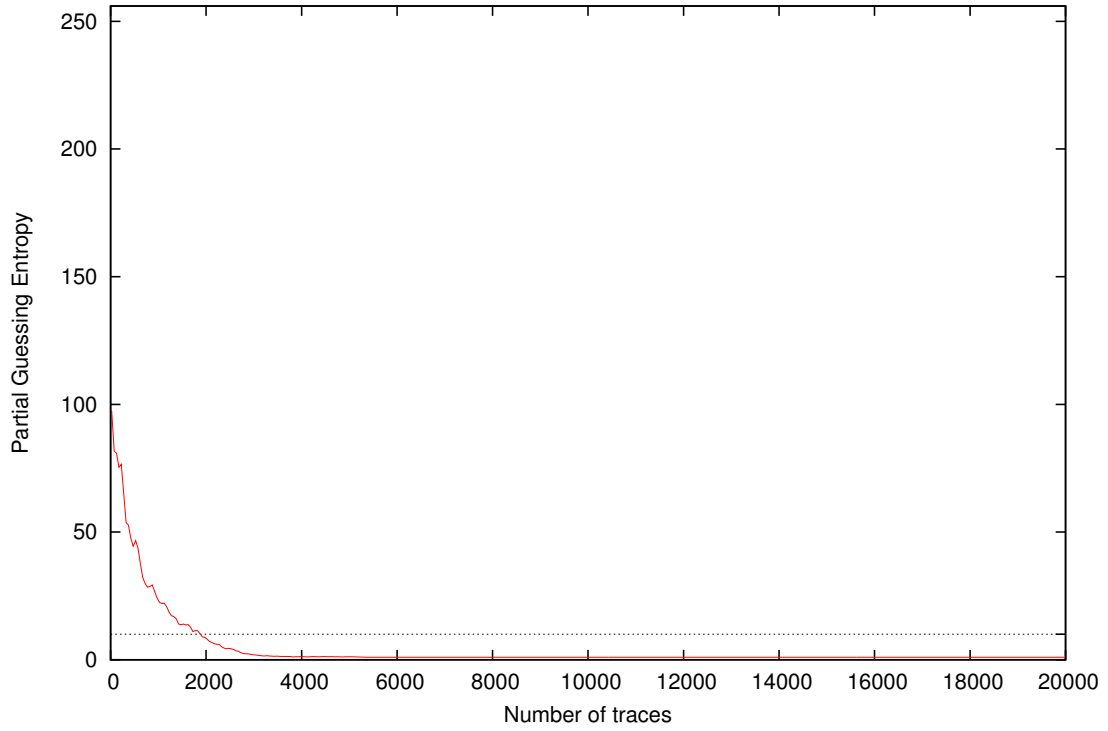
Partial Guessing Entropy for Subkey Byte #14



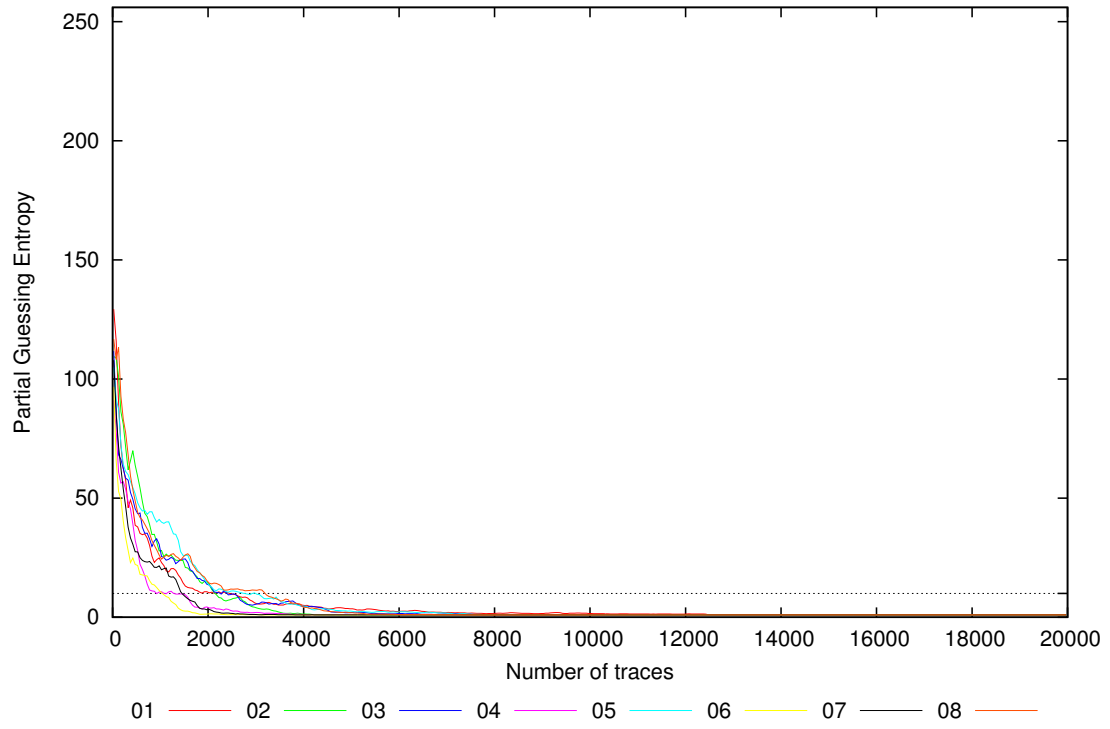
Partial Guessing Entropy for Subkey Byte #15



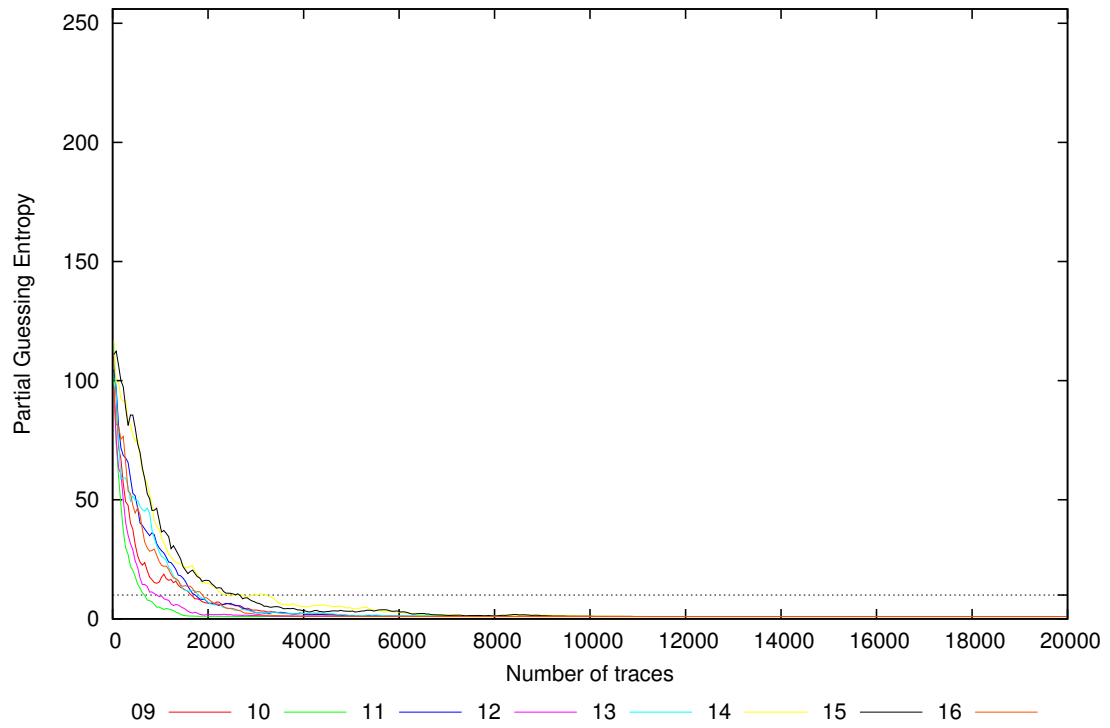
Partial Guessing Entropy for Subkey Byte #16



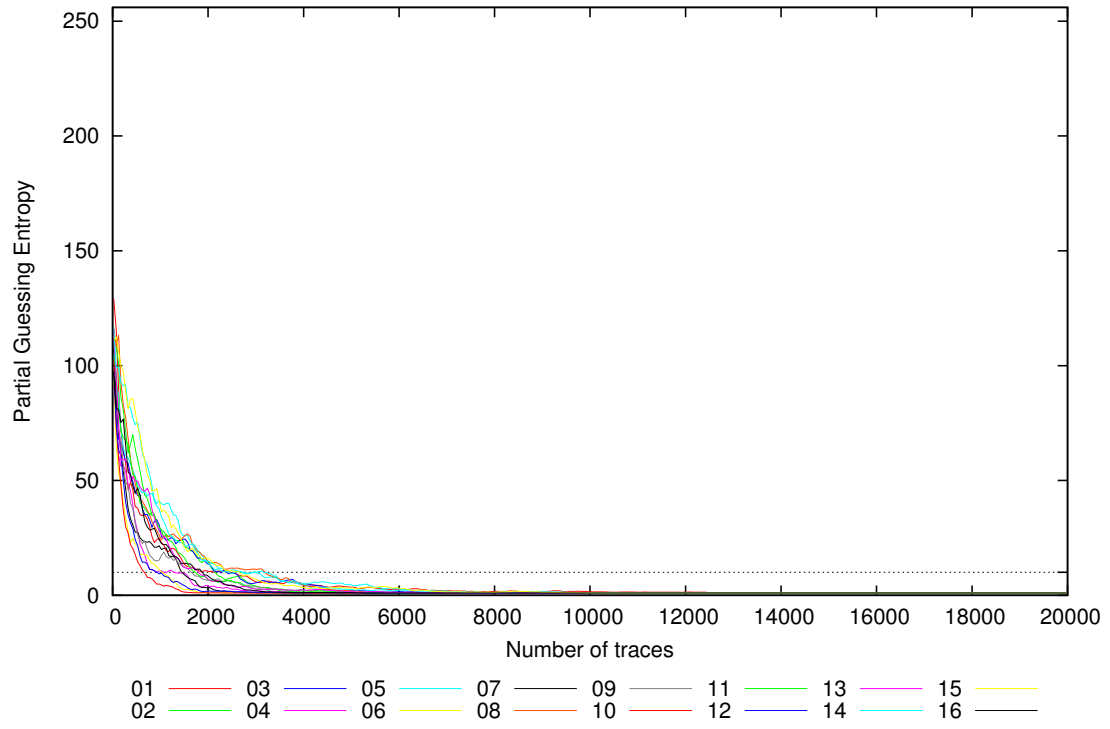
Partial Guessing Entropy for Subkey Bytes #1 to #8



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     | 122.4                           | 96.1  | 116.2 | 87.4 | 120.1 | 117.5 | 121.8 | 124.5 | 122.3 | 118.2 | 112.5 | 113.9 | 136.4 | 125.7 | 116.0 | 109.1 | 87.4 | 136.4 | 116.3 |
| 20     | 129.9                           | 93.1  | 117.0 | 87.9 | 102.7 | 93.8  | 109.8 | 103.9 | 119.7 | 98.2  | 101.0 | 91.4  | 123.7 | 121.5 | 106.2 | 103.2 | 87.9 | 129.9 | 106.4 |
| 30     | 134.7                           | 106.8 | 115.0 | 86.9 | 98.3  | 96.3  | 98.6  | 114.7 | 108.3 | 94.8  | 104.9 | 96.3  | 108.0 | 109.2 | 112.2 | 98.5  | 86.9 | 134.7 | 105.2 |
| 40     | 130.4                           | 118.6 | 105.1 | 92.2 | 103.5 | 79.3  | 97.7  | 111.3 | 102.1 | 89.1  | 103.7 | 85.7  | 100.2 | 109.1 | 112.7 | 93.9  | 79.3 | 130.4 | 102.1 |
| 50     | 130.5                           | 114.8 | 91.7  | 89.6 | 89.6  | 76.4  | 97.1  | 114.4 | 97.9  | 84.6  | 104.4 | 80.8  | 109.9 | 101.3 | 119.2 | 82.0  | 76.4 | 130.5 | 99.0  |
| 100    | 103.7                           | 98.5  | 69.2  | 71.1 | 95.4  | 57.8  | 76.1  | 100.5 | 82.8  | 65.2  | 86.7  | 65.9  | 86.1  | 105.8 | 107.5 | 89.7  | 57.8 | 107.5 | 85.1  |
| 200    | 63.8                            | 83.4  | 62.2  | 56.6 | 68.2  | 47.1  | 59.4  | 86.7  | 63.5  | 38.6  | 73.2  | 58.8  | 56.5  | 89.7  | 99.0  | 74.5  | 38.6 | 99.0  | 67.6  |
| 300    | 49.5                            | 65.7  | 59.9  | 53.6 | 61.5  | 31.3  | 42.9  | 72.5  | 49.4  | 29.8  | 65.2  | 38.0  | 57.4  | 82.3  | 82.7  | 61.1  | 29.8 | 82.7  | 56.4  |
| 400    | 48.6                            | 70.2  | 52.1  | 41.7 | 57.3  | 23.6  | 30.4  | 55.2  | 36.0  | 21.5  | 59.2  | 30.5  | 50.1  | 76.8  | 90.5  | 51.8  | 21.5 | 90.5  | 49.7  |
| 500    | 36.3                            | 62.9  | 42.5  | 30.5 | 49.9  | 23.0  | 26.4  | 45.3  | 28.0  | 15.2  | 51.0  | 22.1  | 50.8  | 77.0  | 76.4  | 47.1  | 15.2 | 77.0  | 42.8  |
| 1000   | 24.1                            | 28.1  | 27.7  | 10.8 | 40.0  | 10.0  | 20.7  | 25.0  | 15.6  | 4.6   | 29.3  | 9.3   | 27.2  | 36.2  | 38.5  | 23.2  | 4.6  | 40.0  | 23.1  |
| 2000   | 10.3                            | 14.8  | 13.6  | 4.0  | 13.9  | 1.3   | 3.3   | 15.5  | 6.5   | 1.1   | 7.0   | 1.8   | 6.9   | 15.1  | 16.1  | 8.3   | 1.1  | 16.1  | 8.7   |
| 3000   | 5.7                             | 3.9   | 5.4   | 2.1  | 10.0  | 1.0   | 1.2   | 11.0  | 3.6   | 1.0   | 2.4   | 1.3   | 2.8   | 10.2  | 6.9   | 2.1   | 1.0  | 11.0  | 4.4   |
| 4000   | 5.2                             | 1.3   | 4.6   | 1.2  | 5.0   | 1.0   | 1.0   | 4.1   | 2.2   | 1.0   | 2.2   | 1.1   | 2.2   | 5.2   | 3.4   | 1.3   | 1.0  | 5.2   | 2.6   |
| 5000   | 3.3                             | 1.0   | 2.0   | 1.1  | 2.6   | 1.0   | 1.0   | 1.8   | 1.3   | 1.0   | 1.3   | 1.1   | 1.5   | 4.7   | 3.2   | 1.2   | 1.0  | 4.7   | 1.8   |
| 10000  | 1.6                             | 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   | 1.1   | 1.0   | 1.0  | 1.6   | 1.1   |
| 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   |