# Evaluation results

DPA contest v2

February 2012

## 1 Introduction

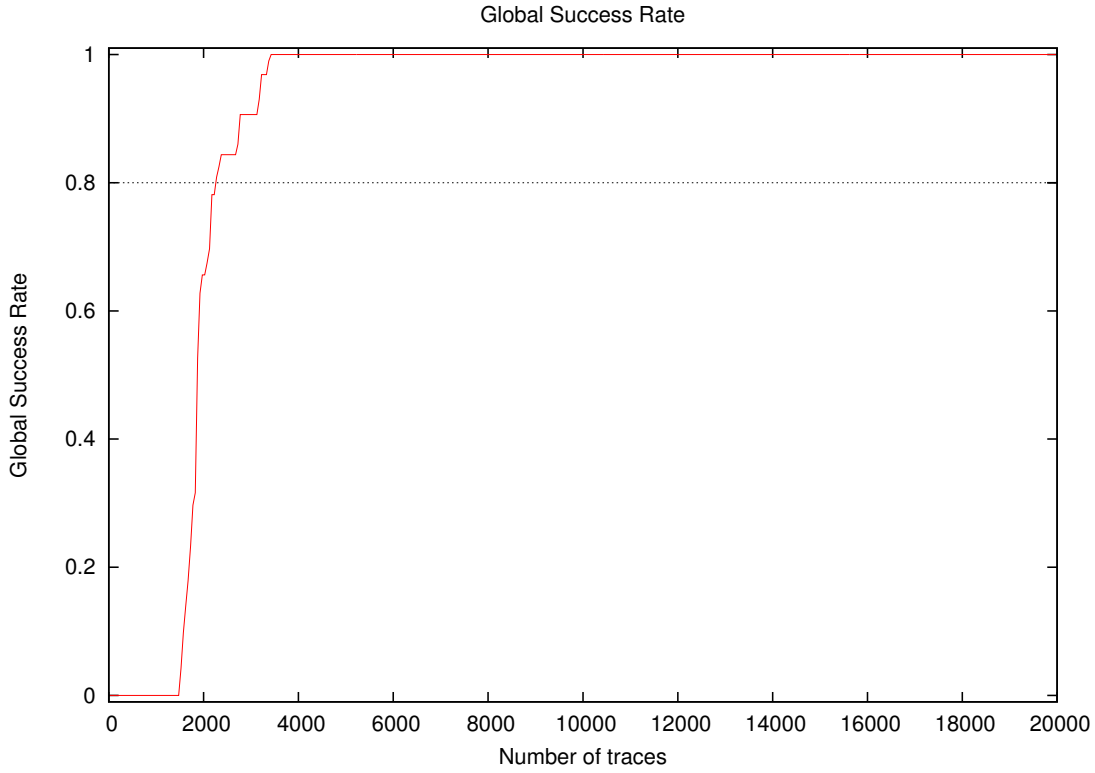
### 1.1 About the attack

- **Sender/Team:** Yang Li, Daisuke Nakatsu, Kazuo Sakiyama
- **Institution:** The University of Electro-Communications
- **Language:** Matlab
- **Attacked subkey:** 10

### 1.2 About the evaluation

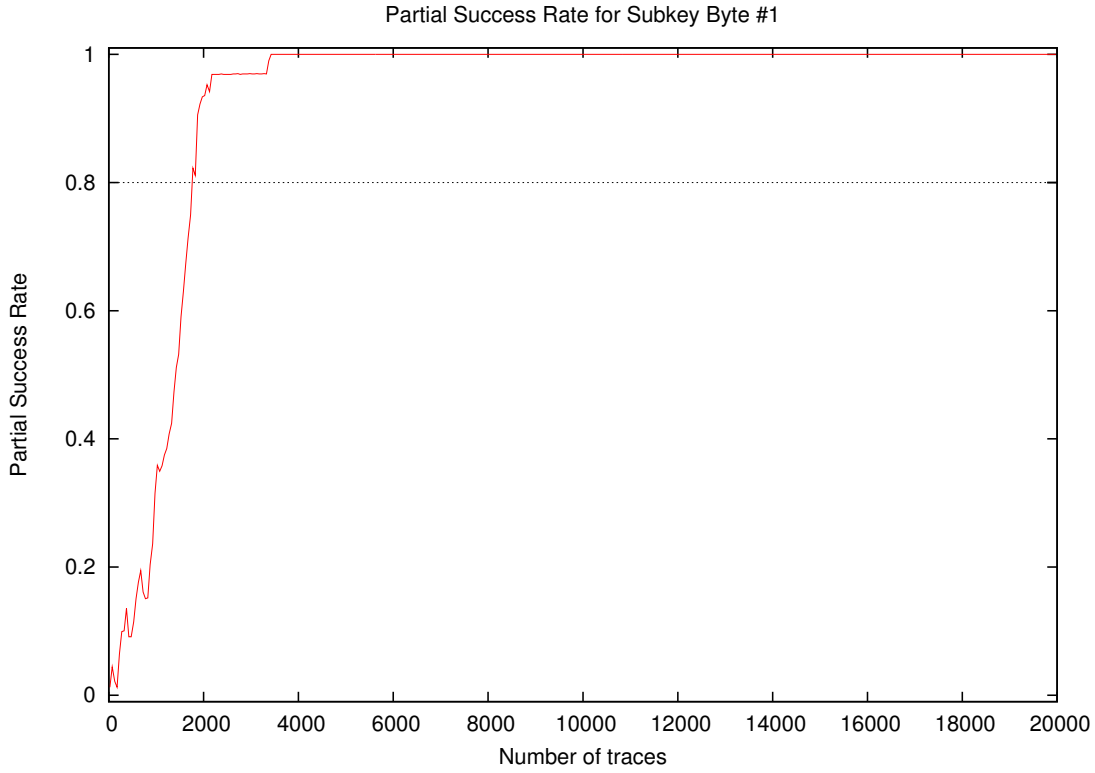
- **Date of evaluation:** February 2012

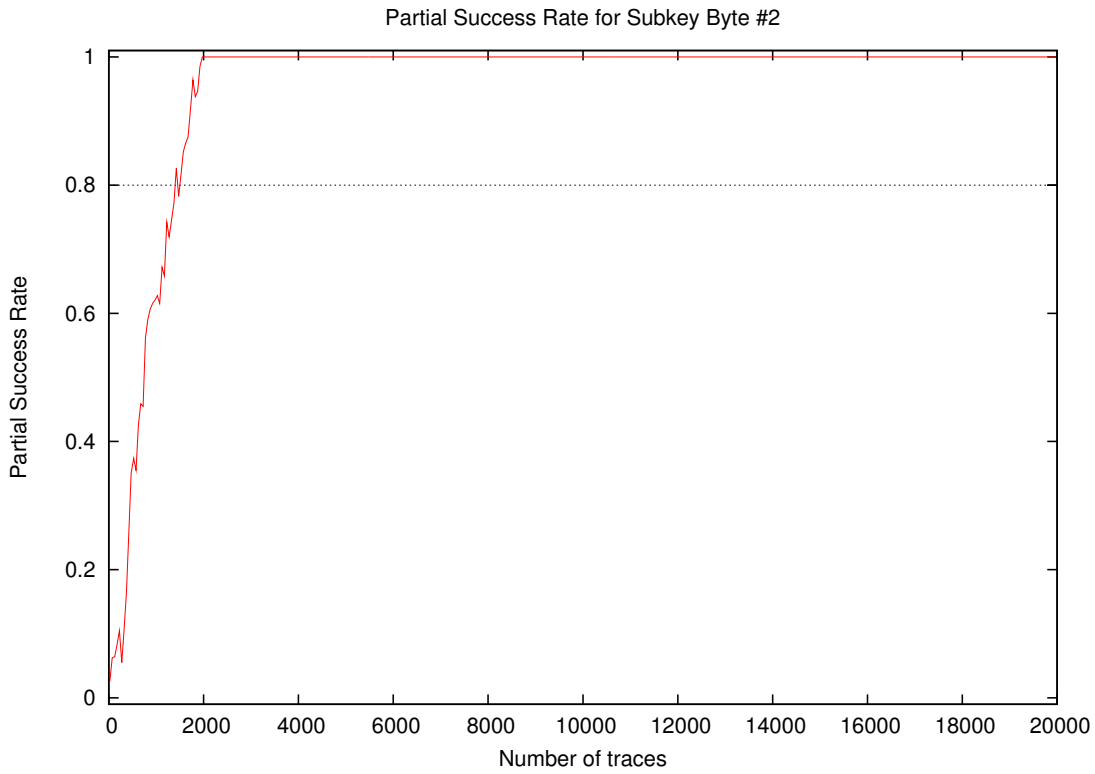
## 2 Global Success Rate

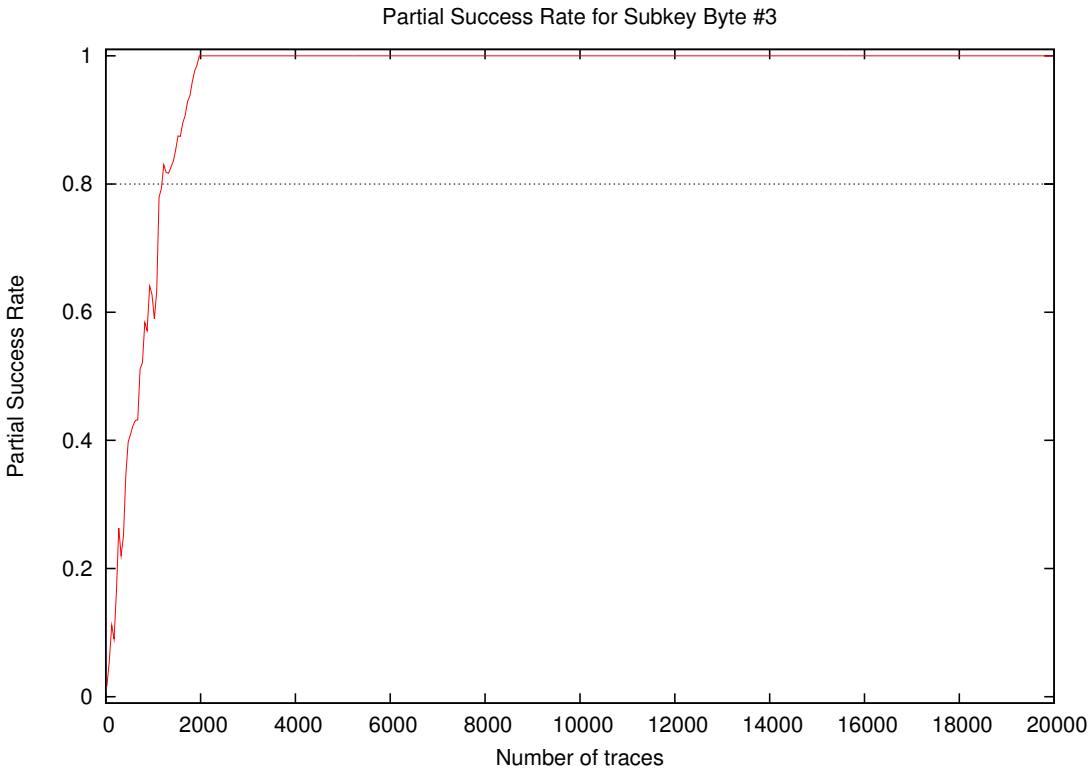


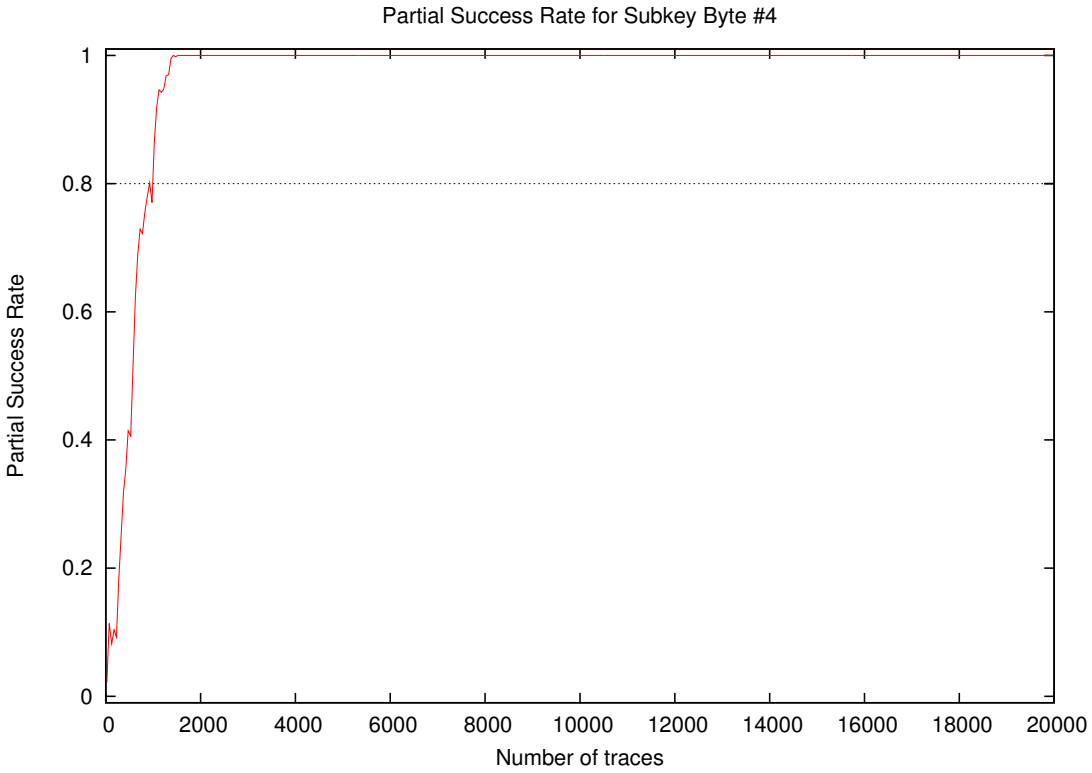
| Number of traces | Global Success Rate |
|---|---|
| 10 | 0.00 |
| 20 | 0.00 |
| 30 | 0.00 |
| 40 | 0.00 |
| 50 | 0.00 |
| 100 | 0.00 |
| 200 | 0.00 |
| 300 | 0.00 |
| 400 | 0.00 |
| 500 | 0.00 |
| 1000 | 0.00 |
| 2000 | 0.66 |
| 3000 | 0.91 |
| 4000 | 1.00 |
| 5000 | 1.00 |
| 10000 | 1.00 |
| 15000 | 1.00 |
| 20000 | 1.00 |

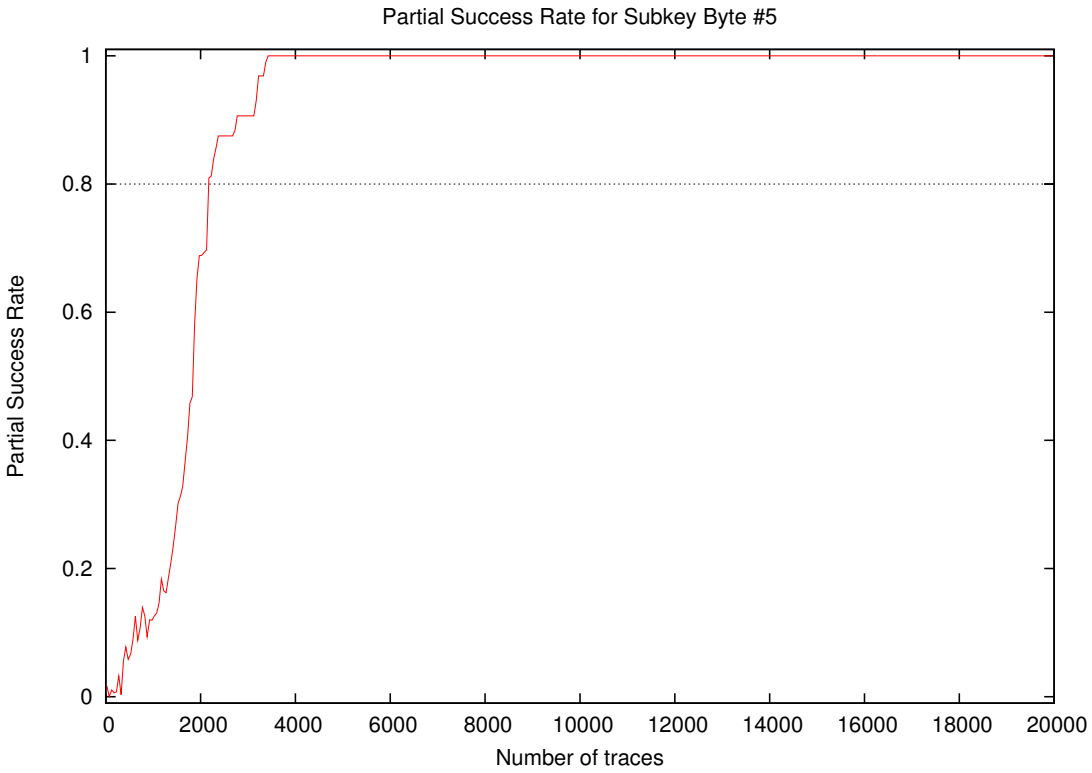
# 3 Partial Success Rate

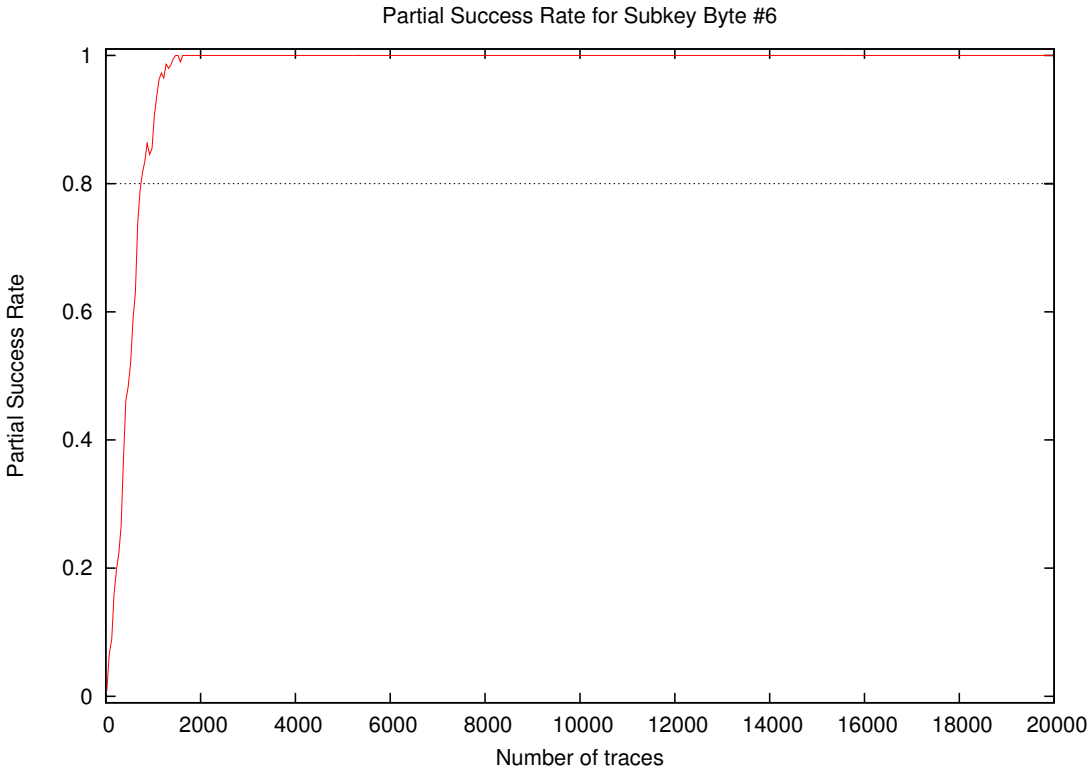


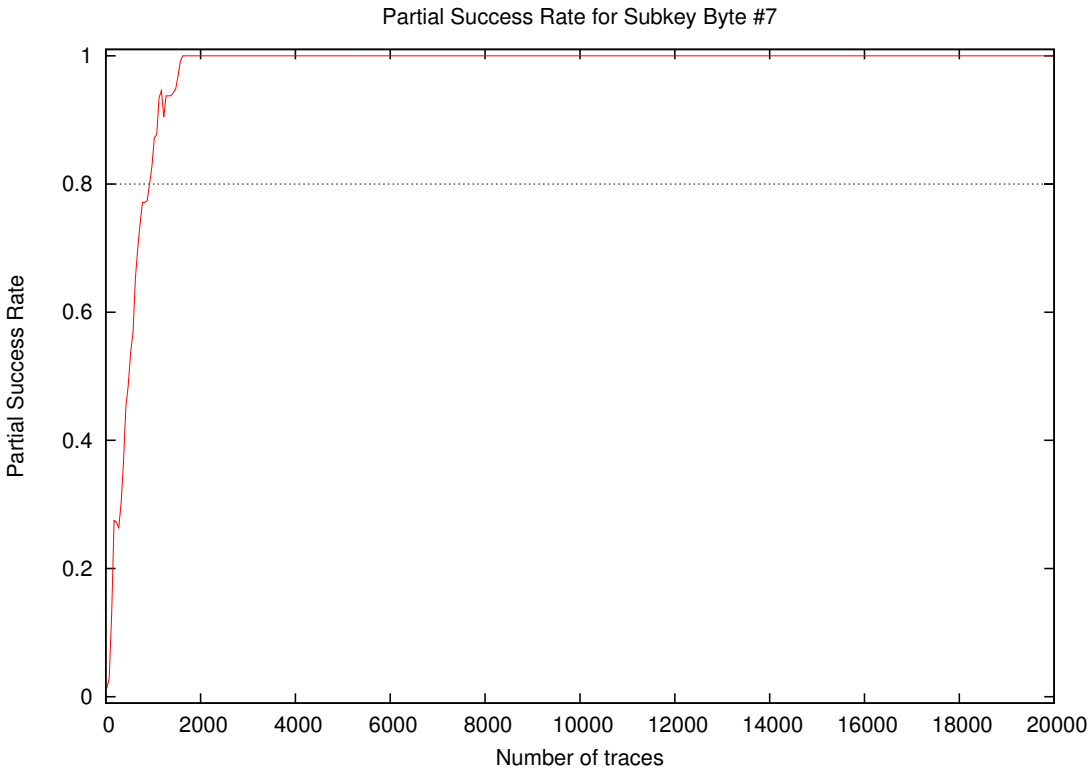



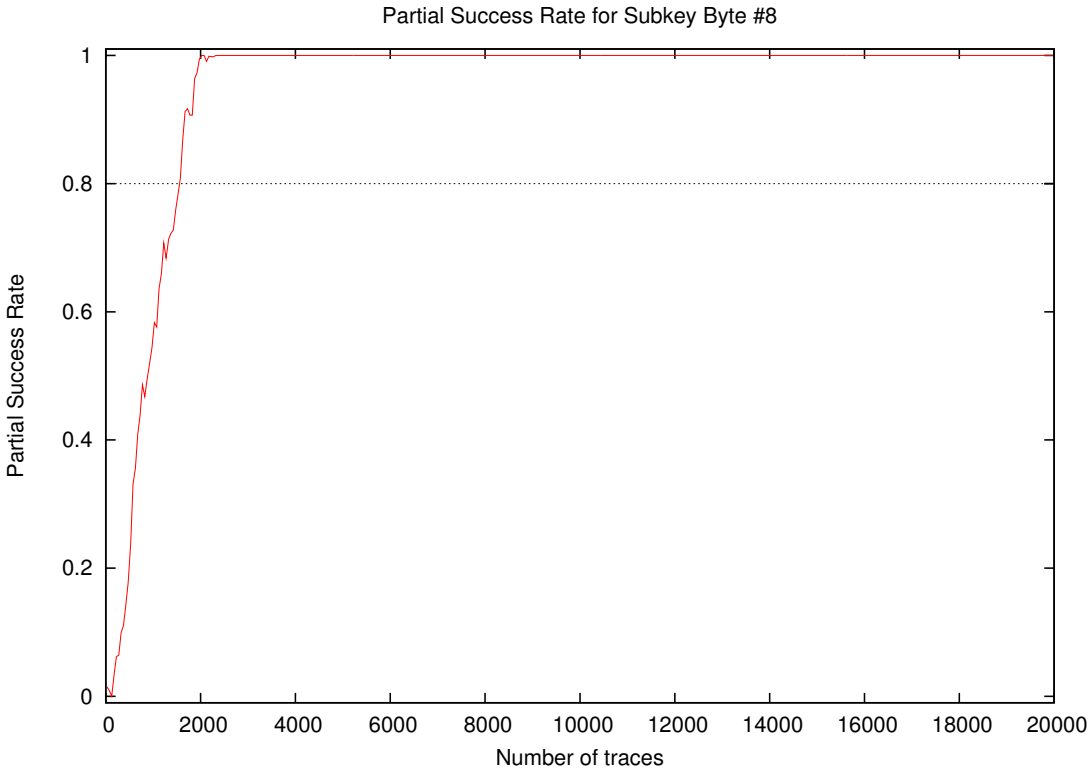

Partial Success Rate for Subkey Byte #3
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000

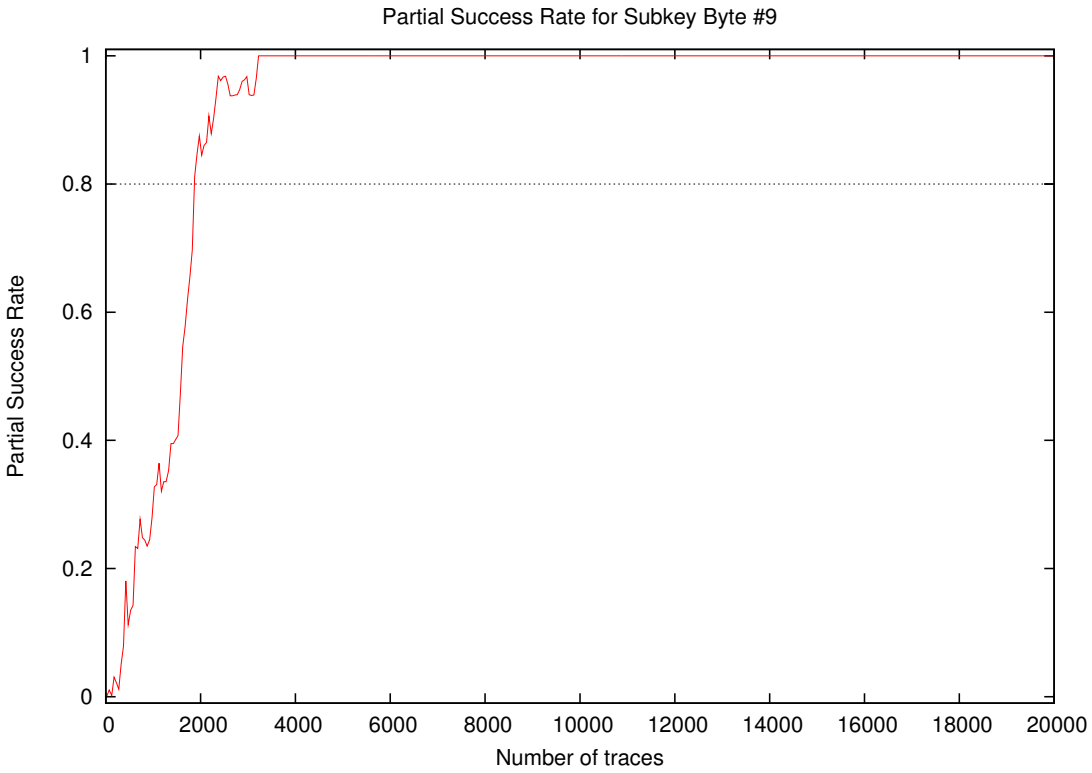

Partial Success Rate for Subkey Byte #4
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000

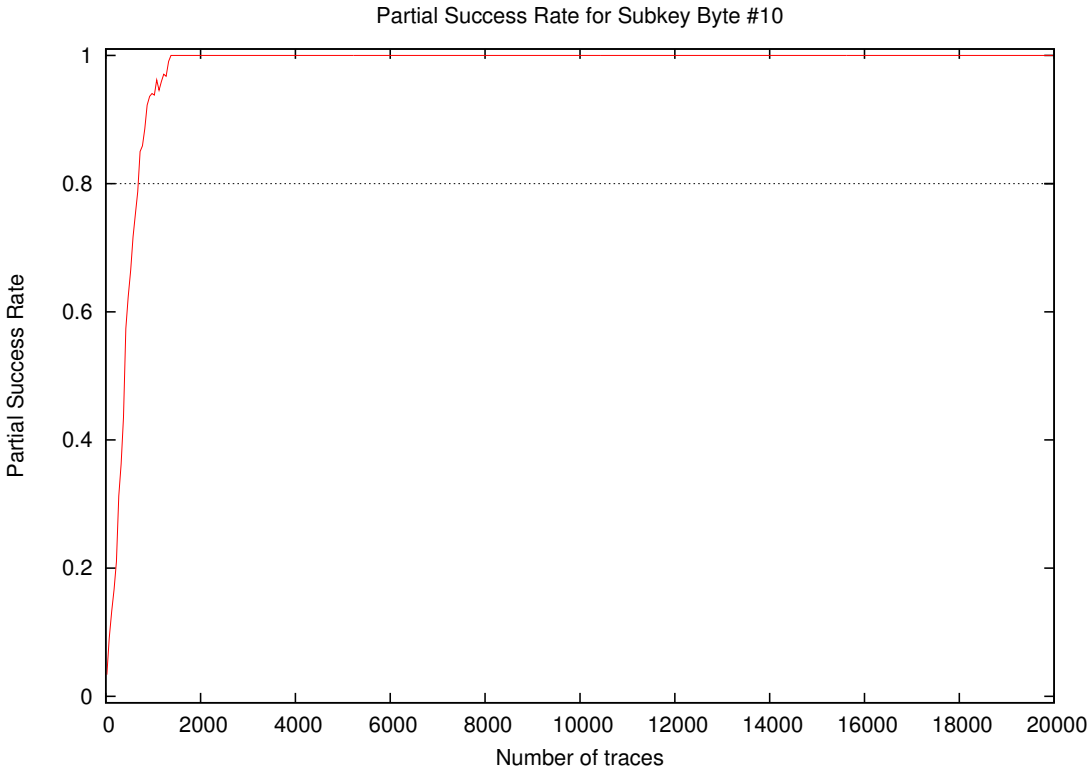

Partial Success Rate for Subkey Byte #5
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000

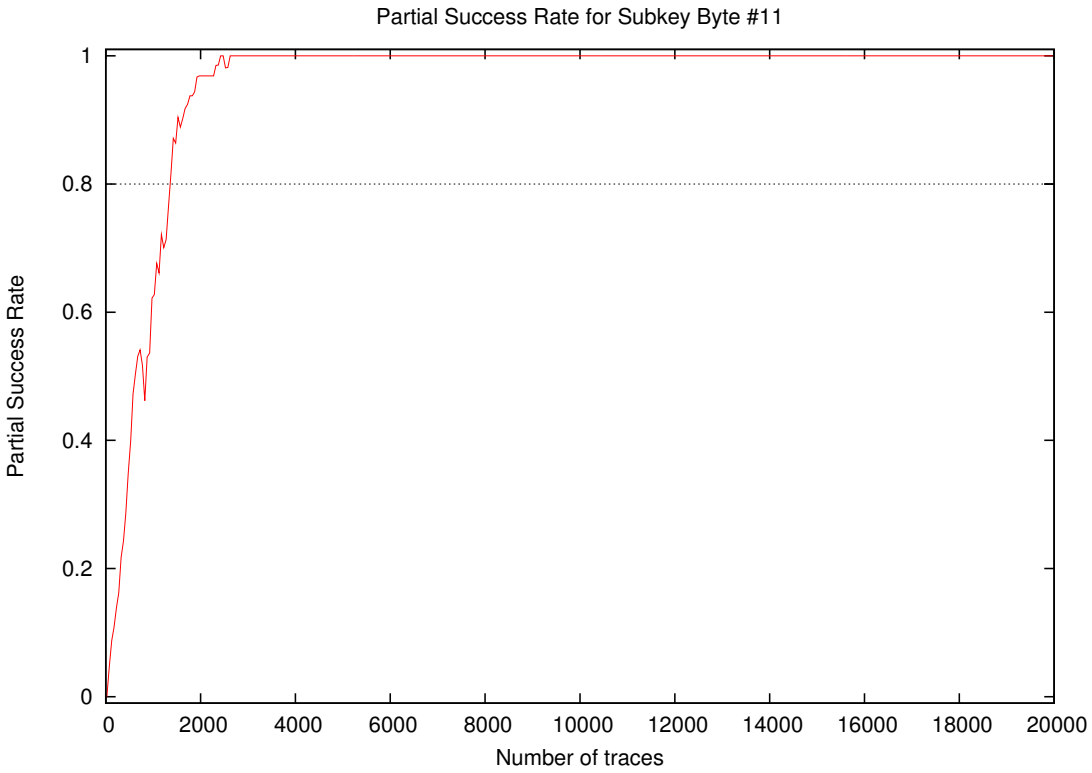

Partial Success Rate for Subkey Byte #6
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000

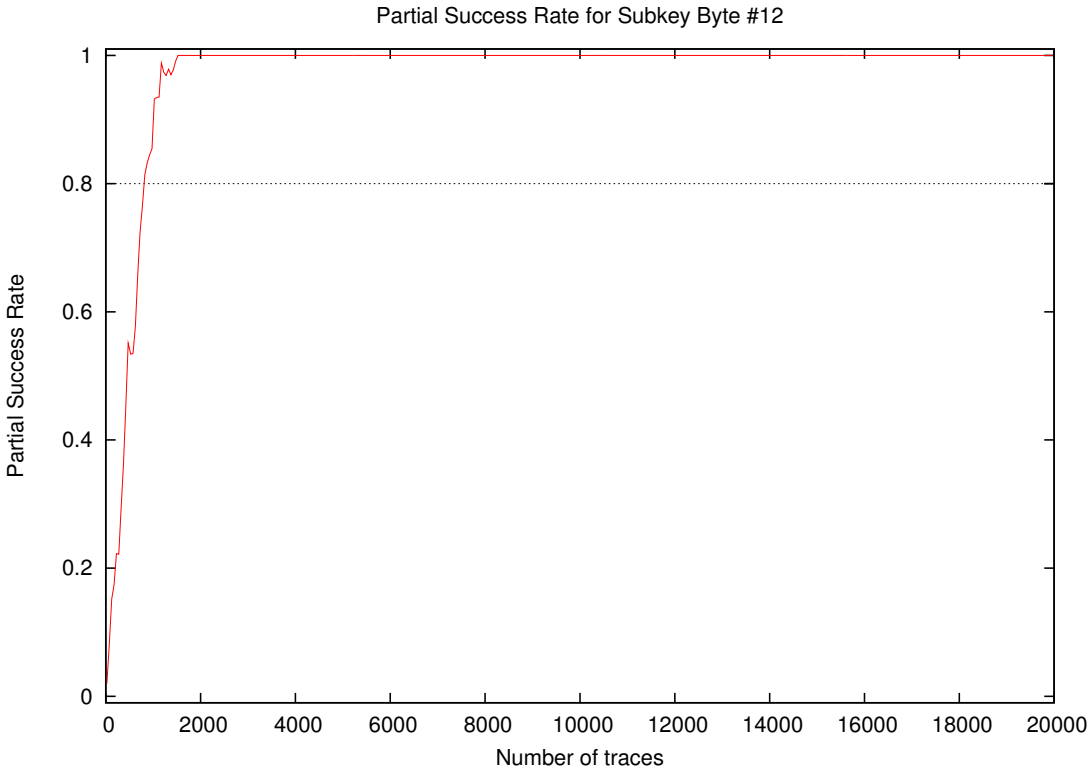

Partial Success Rate for Subkey Byte #7
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000

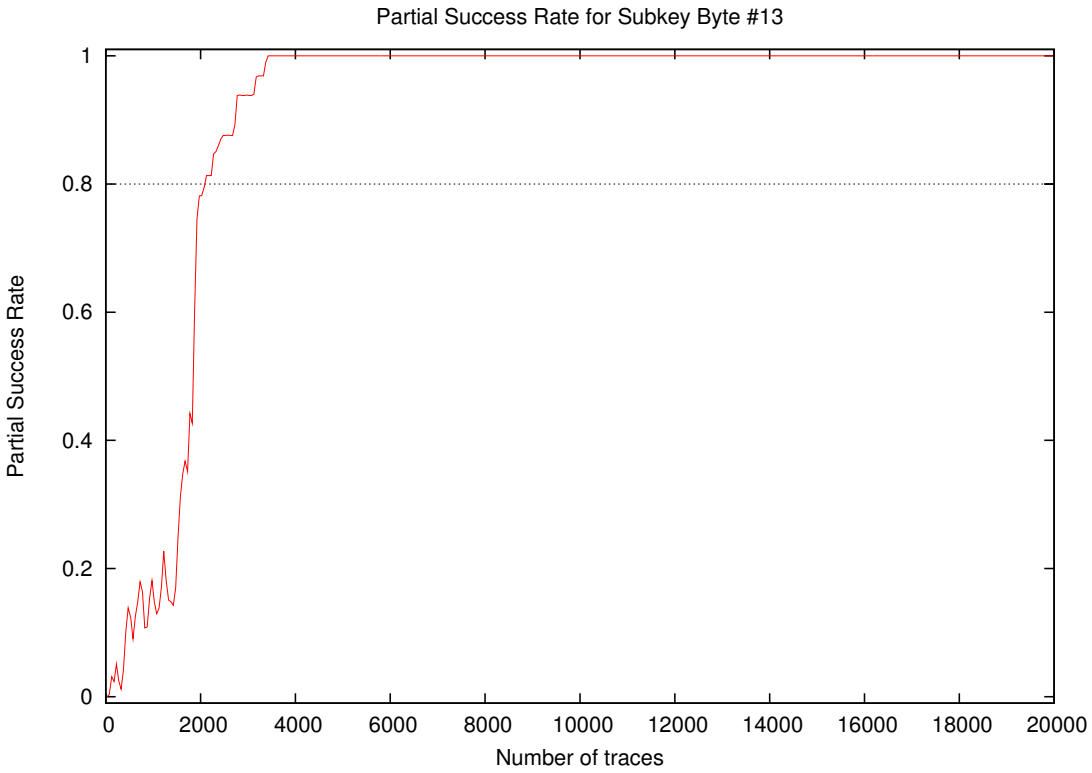

Partial Success Rate for Subkey Byte #8
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000

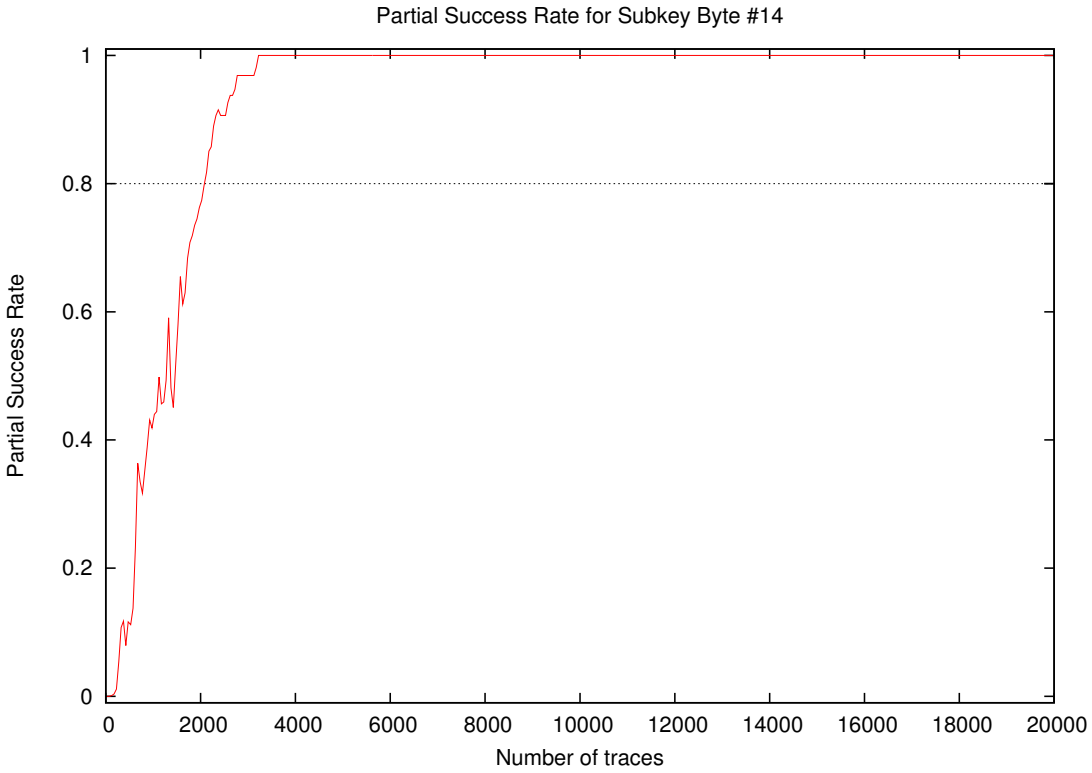

Partial Success Rate for Subkey Byte #9
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000

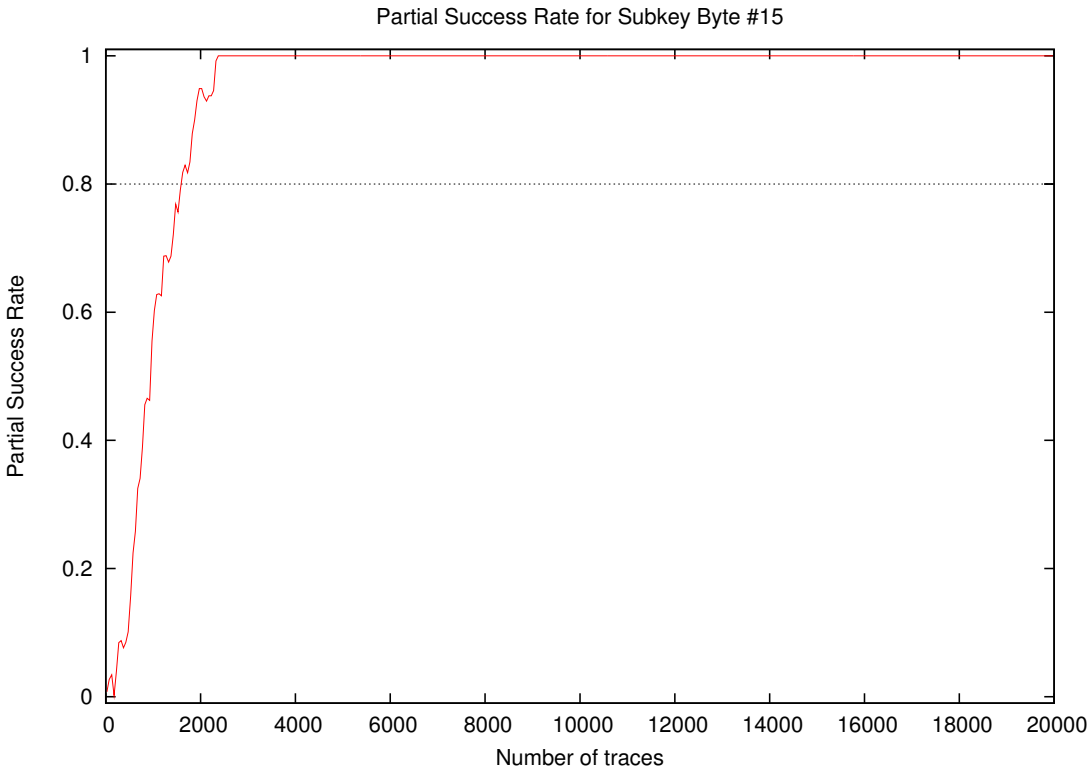

Partial Success Rate for Subkey Byte #10
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000

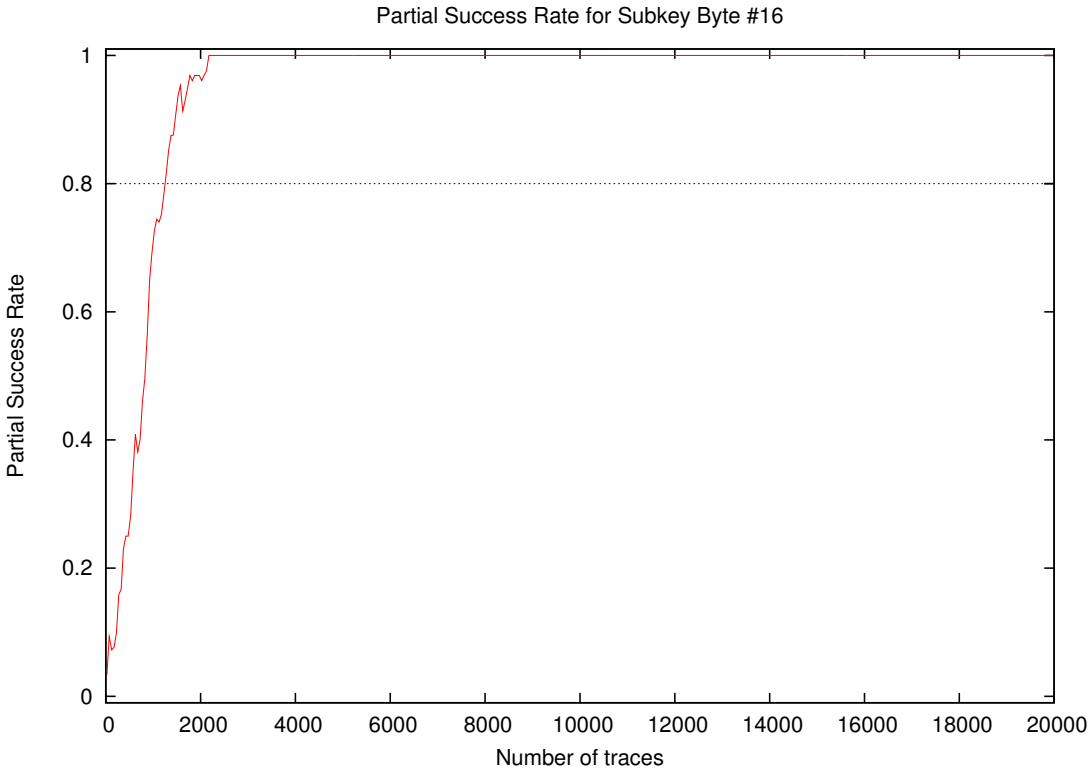

Partial Success Rate for Subkey Byte #11
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000

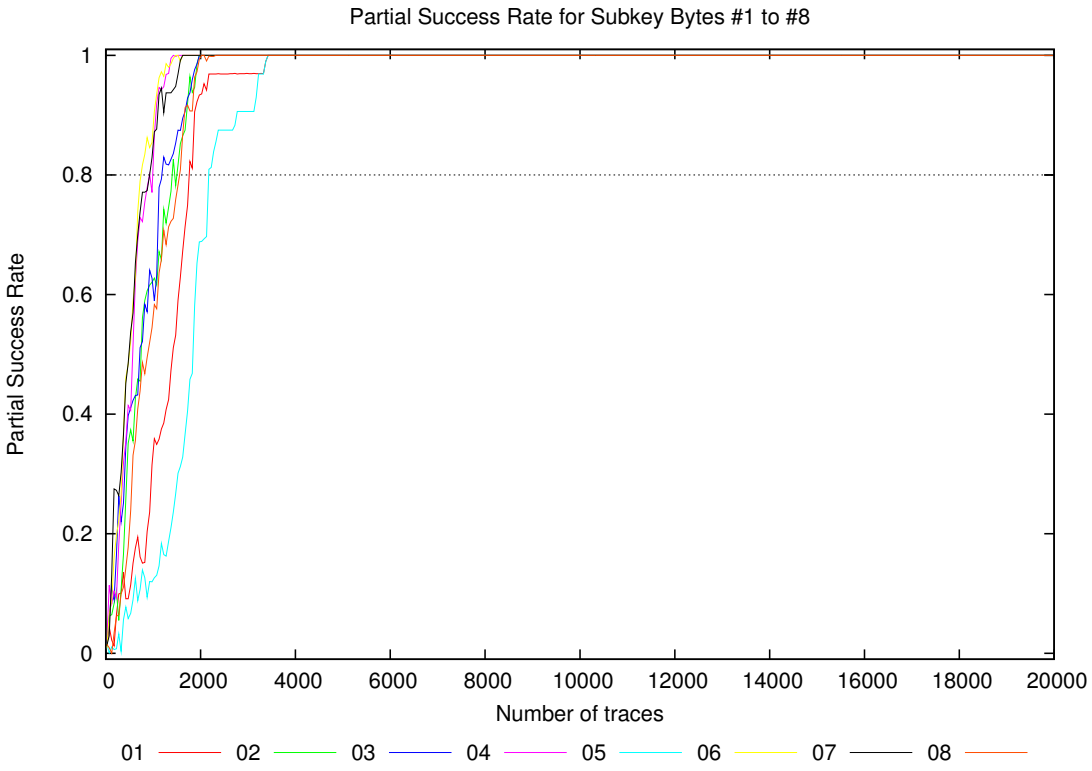

Partial Success Rate for Subkey Byte #12
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000

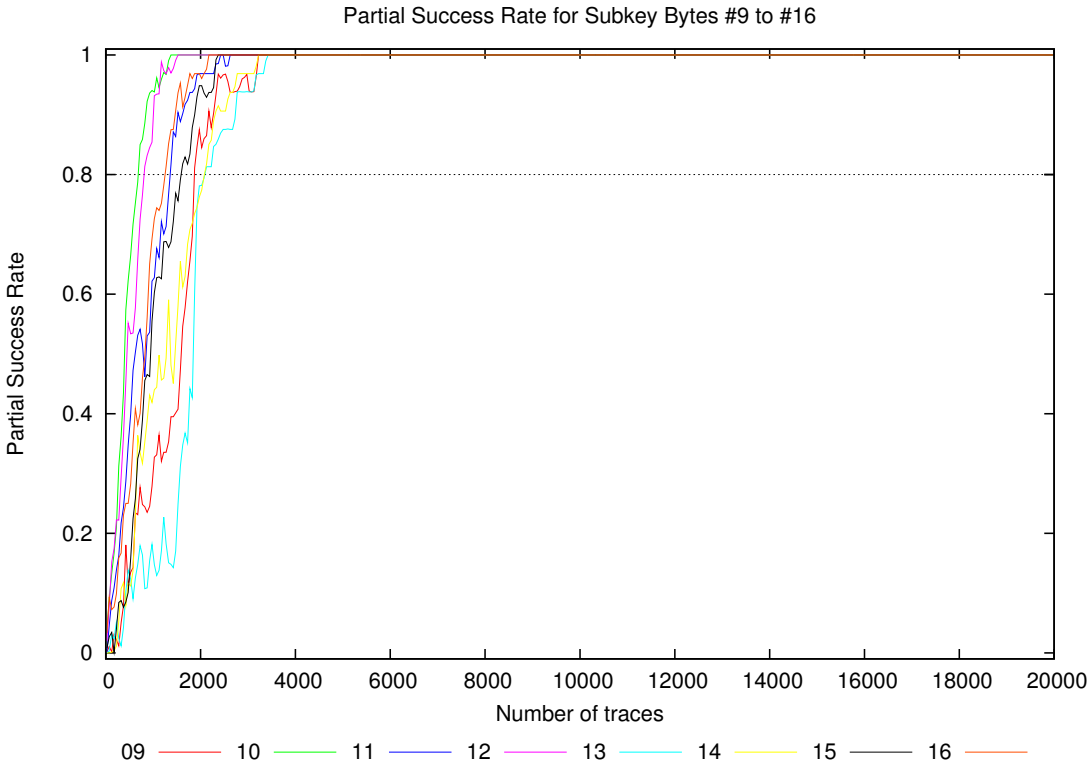

Partial Success Rate for Subkey Byte #13
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000

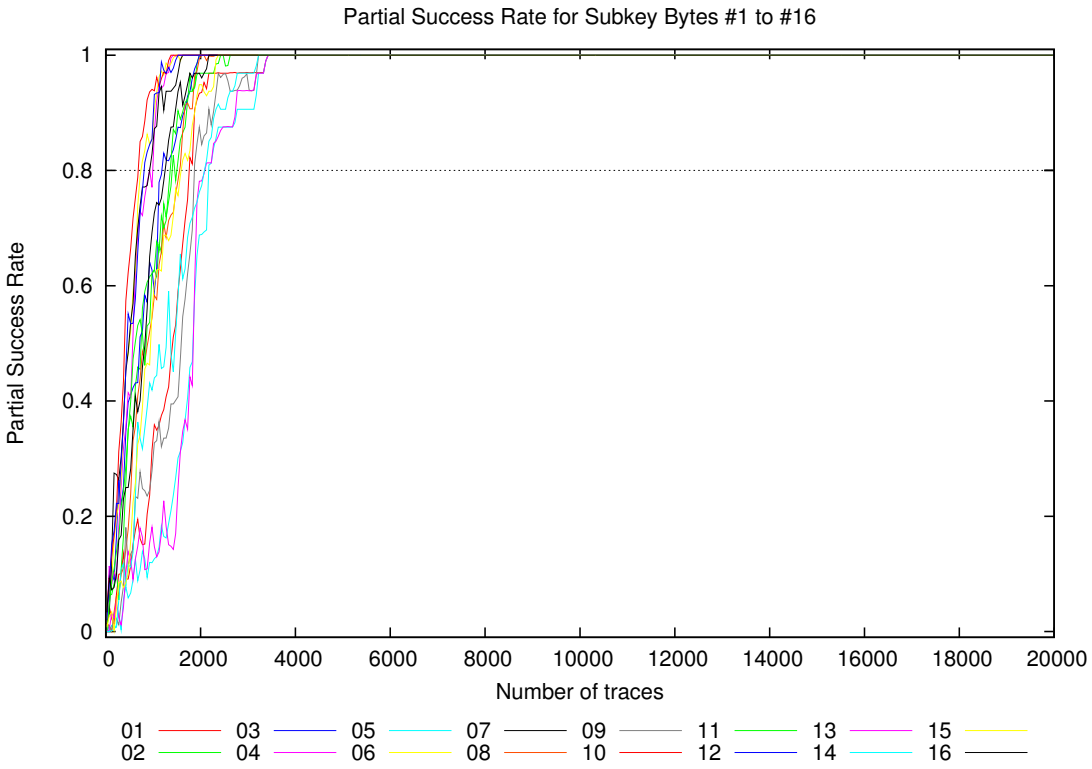

Partial Success Rate for Subkey Byte #14
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000


Partial Success Rate for Subkey Byte #15
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000


Partial Success Rate for Subkey Byte #16
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000

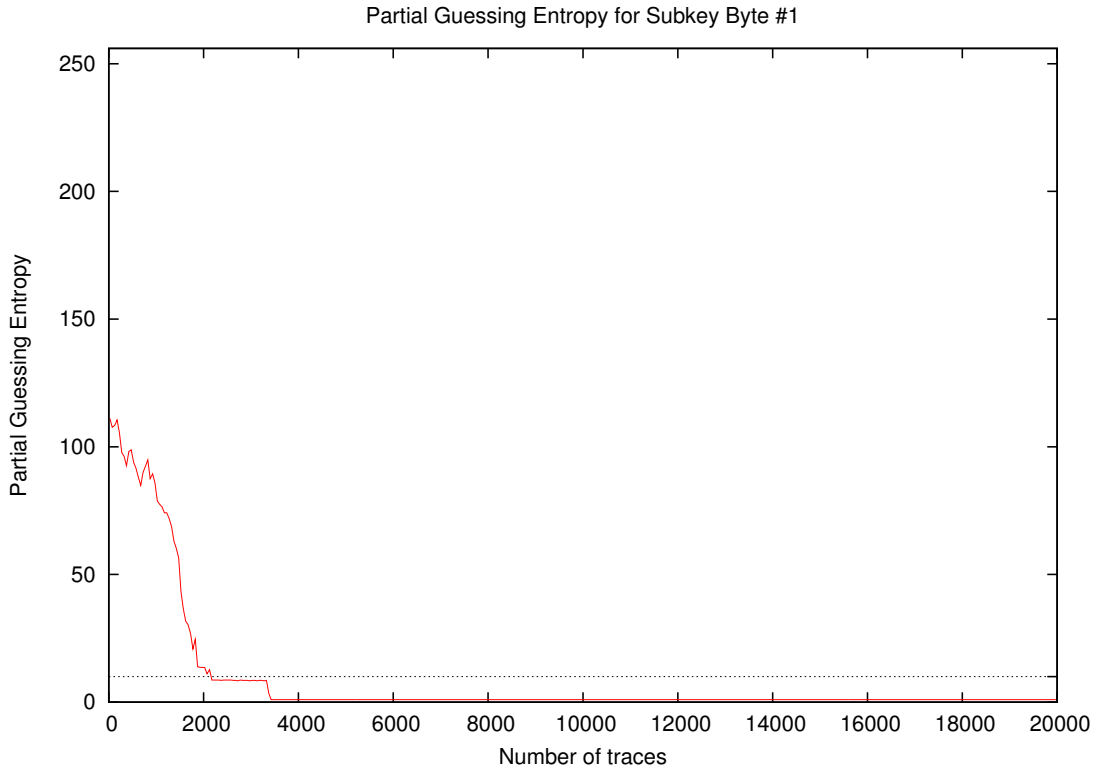

Partial Success Rate for Subkey Bytes #1 to #8
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000
01
02
03
04
05
06
07
08

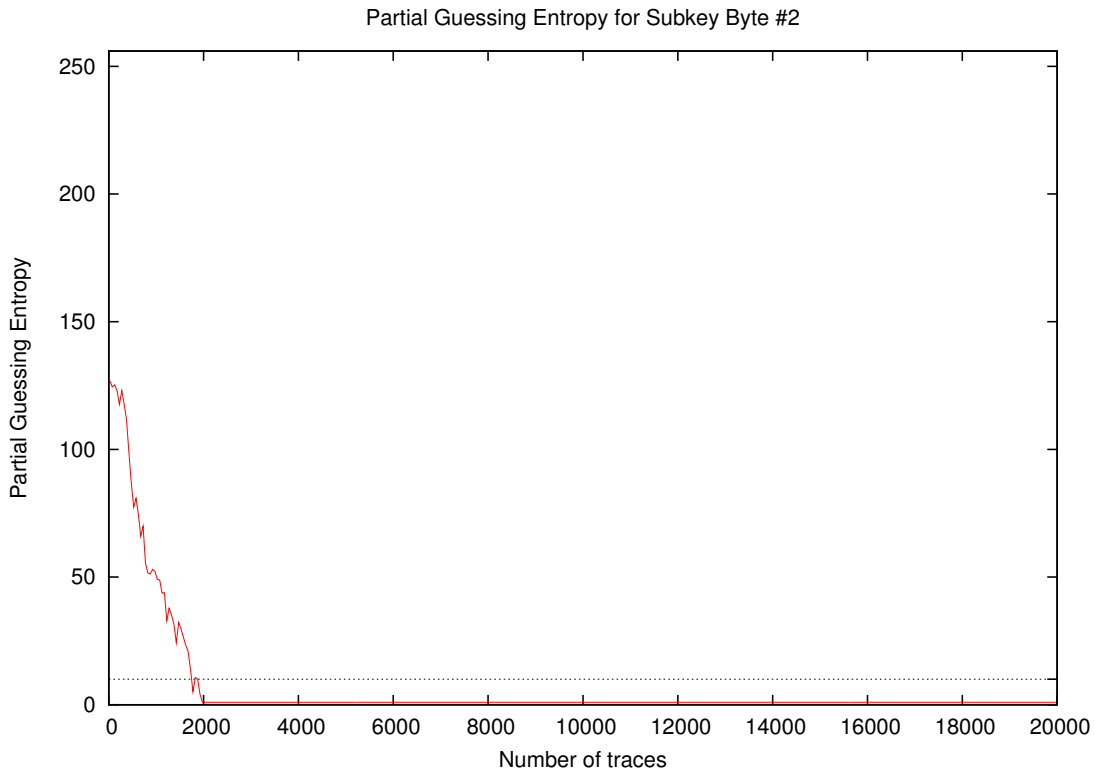

Partial Success Rate for Subkey Bytes #9 to #16
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000
09
10
11
12
13
14
15
16

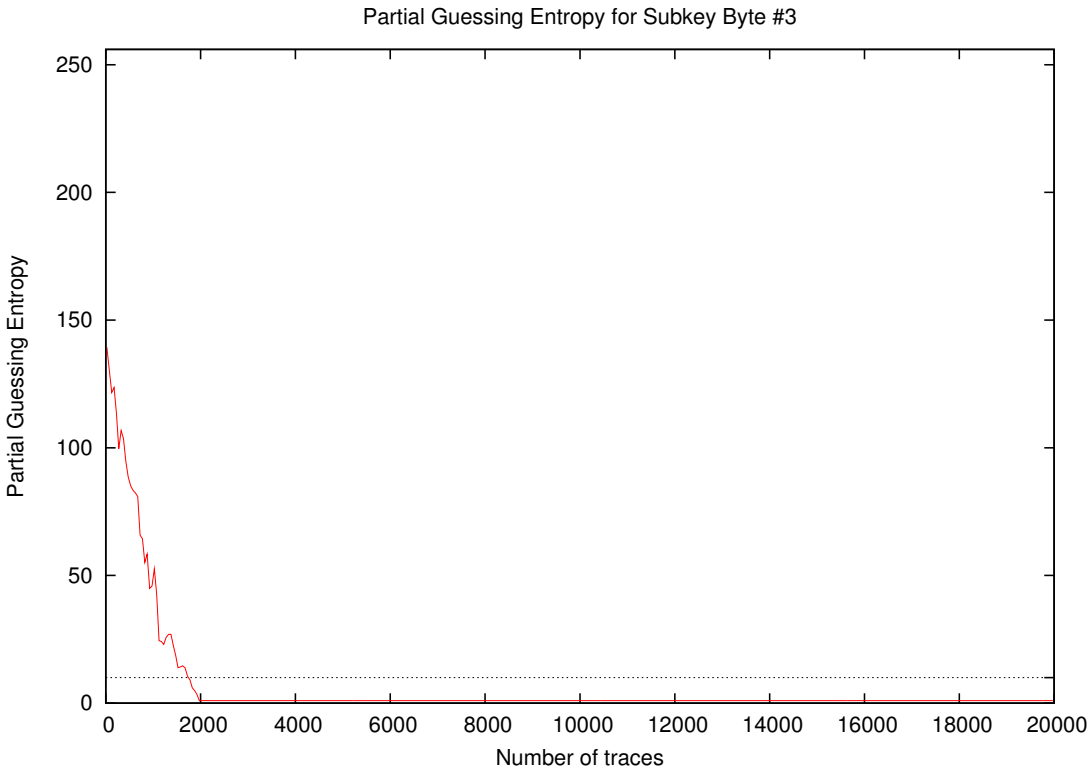

Partial Success Rate for Subkey Bytes #1 to #16
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000
01
02
03
04
05
06
07
08
09
10
11
12
13
14
15
16

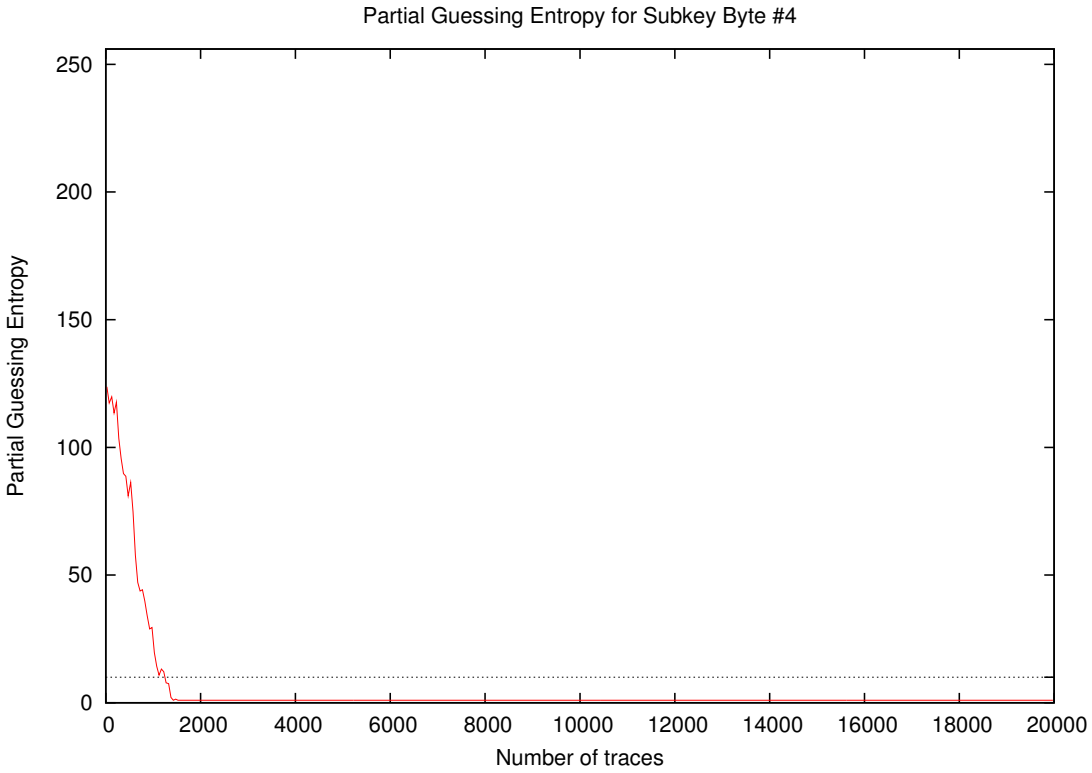
| Traces | Partial Success Rate / Byte | | | | | | | | | | | | | | | | Min | Max | Mean |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | | | |
| 10 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.03 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.03 | 0.00 | 0.03 | 0.00 |
| 20 | 0.00 | 0.03 | 0.00 | 0.00 | 0.03 | 0.00 | 0.00 | 0.03 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.03 | 0.00 | 0.03 | 0.01 |
| 30 | 0.00 | 0.03 | 0.03 | 0.00 | 0.03 | 0.00 | 0.03 | 0.03 | 0.00 | 0.06 | 0.00 | 0.00 | 0.00 | 0.00 | 0.03 | 0.00 | 0.00 | 0.06 | 0.02 |
| 40 | 0.03 | 0.03 | 0.00 | 0.06 | 0.00 | 0.00 | 0.03 | 0.00 | 0.00 | 0.06 | 0.00 | 0.03 | 0.00 | 0.00 | 0.00 | 0.06 | 0.00 | 0.06 | 0.02 |
| 50 | 0.06 | 0.03 | 0.03 | 0.09 | 0.03 | 0.00 | 0.00 | 0.03 | 0.00 | 0.06 | 0.00 | 0.09 | 0.00 | 0.00 | 0.00 | 0.03 | 0.00 | 0.09 | 0.03 |
| 100 | 0.00 | 0.03 | 0.09 | 0.12 | 0.00 | 0.09 | 0.03 | 0.00 | 0.00 | 0.16 | 0.09 | 0.09 | 0.00 | 0.00 | 0.03 | 0.09 | 0.00 | 0.16 | 0.05 |
| 200 | 0.00 | 0.09 | 0.09 | 0.03 | 0.00 | 0.19 | 0.31 | 0.09 | 0.03 | 0.12 | 0.12 | 0.22 | 0.03 | 0.00 | 0.03 | 0.12 | 0.00 | 0.31 | 0.09 |
| 300 | 0.12 | 0.03 | 0.25 | 0.16 | 0.00 | 0.22 | 0.28 | 0.09 | 0.00 | 0.34 | 0.22 | 0.31 | 0.03 | 0.06 | 0.12 | 0.12 | 0.00 | 0.34 | 0.15 |
| 400 | 0.09 | 0.22 | 0.28 | 0.31 | 0.09 | 0.41 | 0.44 | 0.16 | 0.09 | 0.50 | 0.31 | 0.47 | 0.09 | 0.09 | 0.06 | 0.31 | 0.06 | 0.50 | 0.25 |
| 500 | 0.06 | 0.41 | 0.38 | 0.41 | 0.03 | 0.44 | 0.41 | 0.25 | 0.12 | 0.59 | 0.38 | 0.56 | 0.09 | 0.16 | 0.16 | 0.28 | 0.03 | 0.59 | 0.29 |
| 1000 | 0.34 | 0.66 | 0.59 | 0.78 | 0.16 | 0.91 | 0.88 | 0.56 | 0.28 | 0.94 | 0.62 | 0.88 | 0.16 | 0.41 | 0.56 | 0.75 | 0.16 | 0.94 | 0.59 |
| 2000 | 0.94 | 1.00 | 1.00 | 1.00 | 0.69 | 1.00 | 1.00 | 1.00 | 0.88 | 1.00 | 0.97 | 1.00 | 0.78 | 0.78 | 0.97 | 0.97 | 0.69 | 1.00 | 0.94 |
| 3000 | 0.97 | 1.00 | 1.00 | 1.00 | 0.91 | 1.00 | 1.00 | 1.00 | 0.97 | 1.00 | 1.00 | 1.00 | 0.94 | 0.97 | 1.00 | 1.00 | 0.91 | 1.00 | 0.98 |
| 4000 | 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 |
| 5000 | 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 |
| 10000 | 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 |
| 15000 | 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 |
| 20000 | 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 |

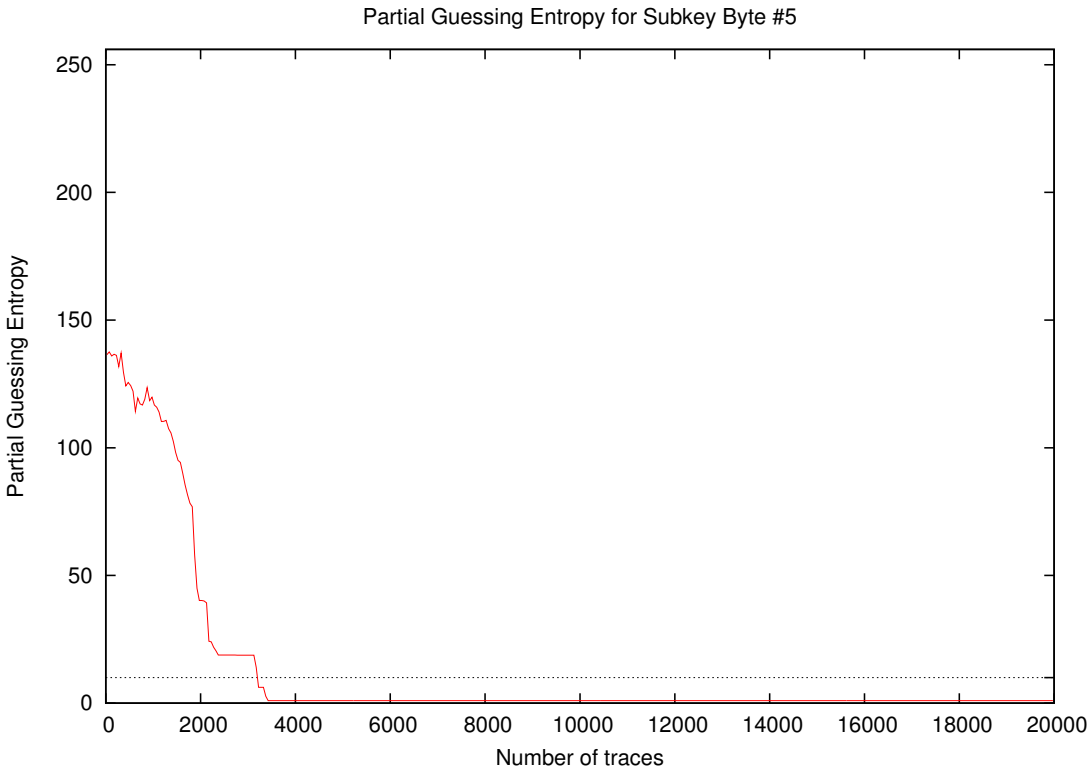
# 4 Partial Guessing Entropy

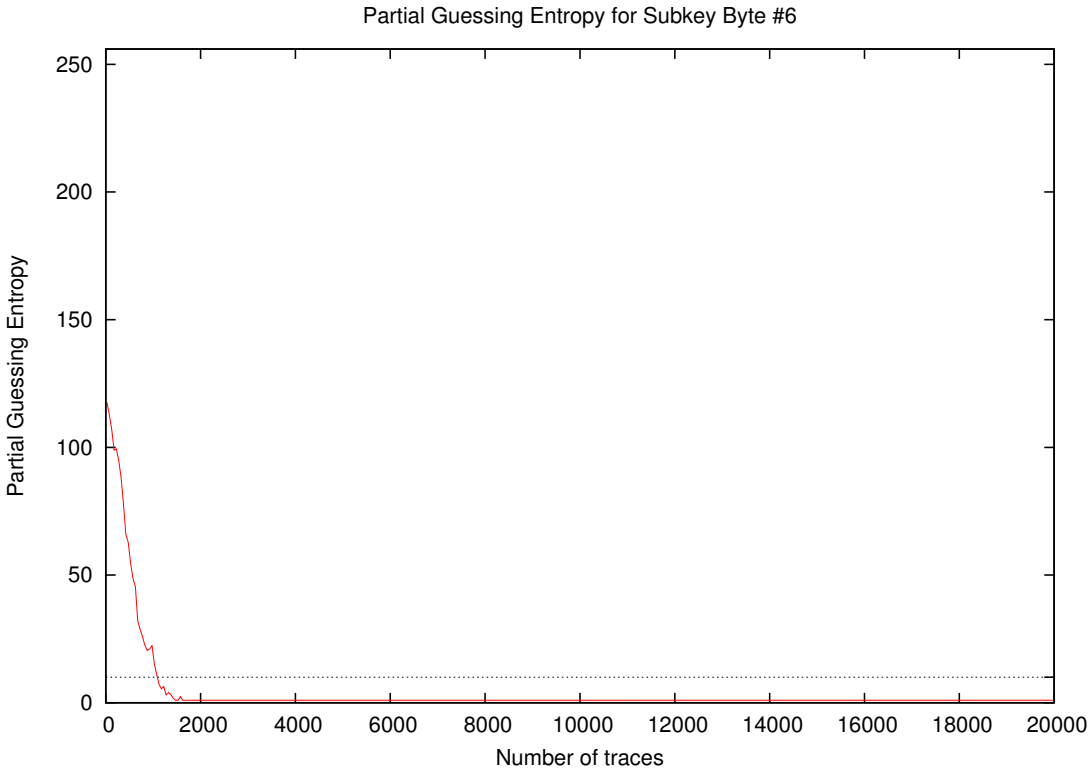


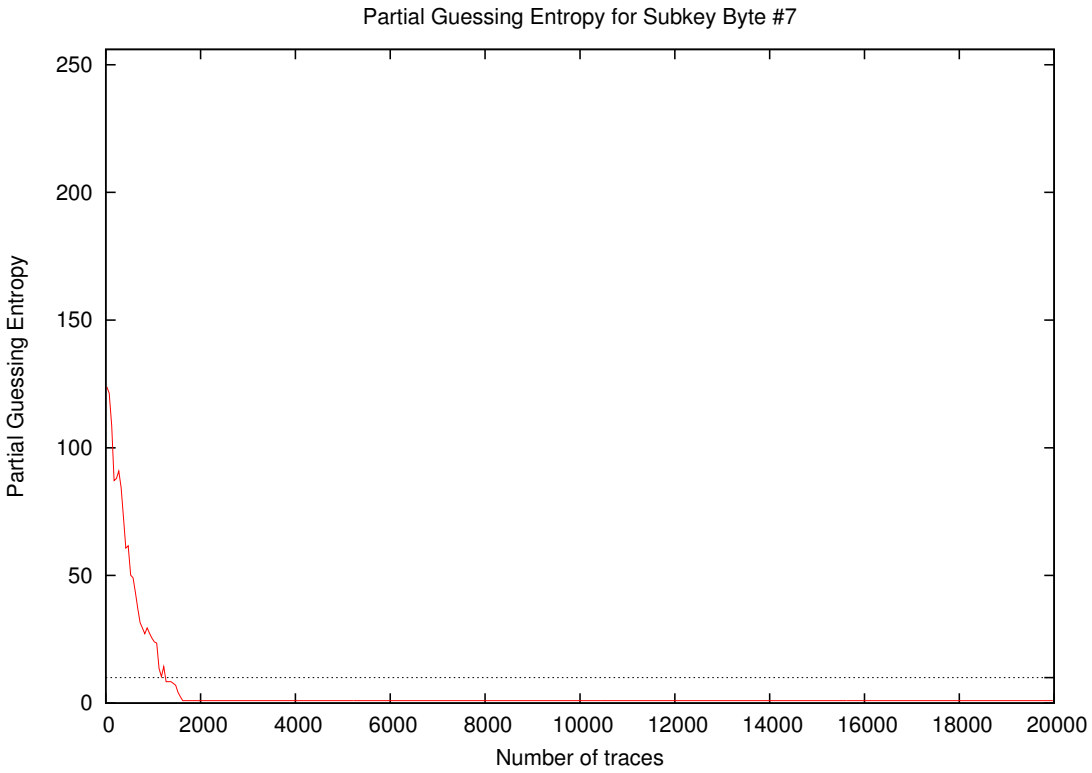



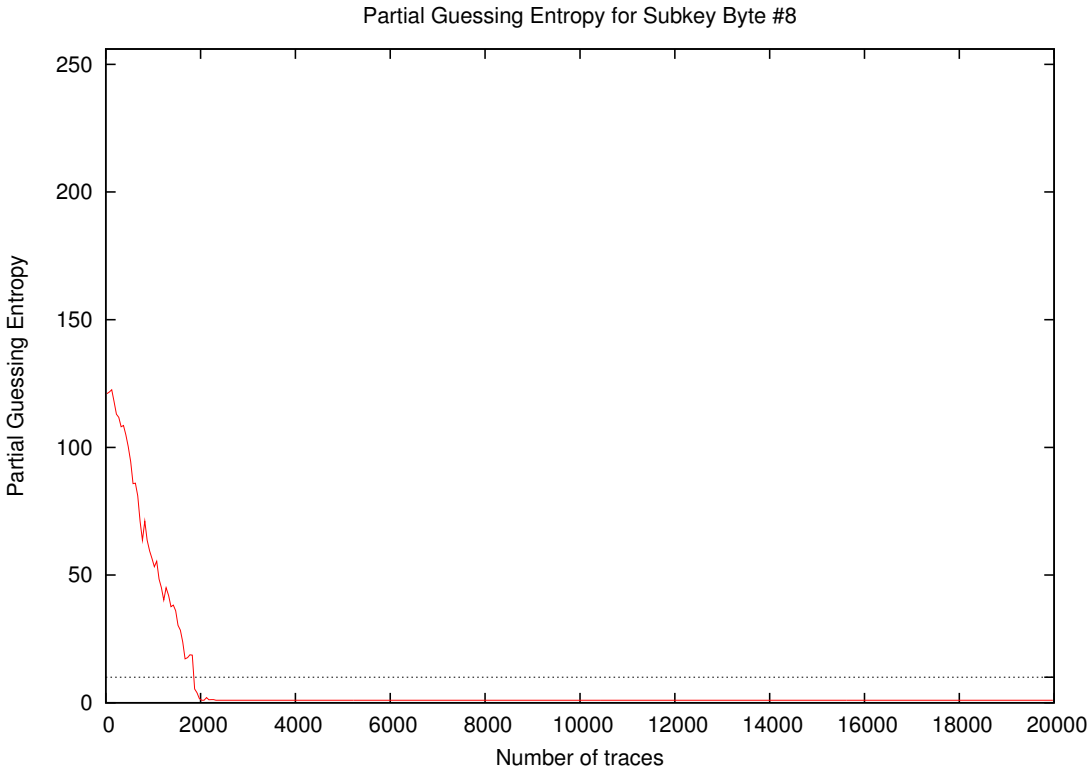

Partial Guessing Entropy for Subkey Byte #3
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000

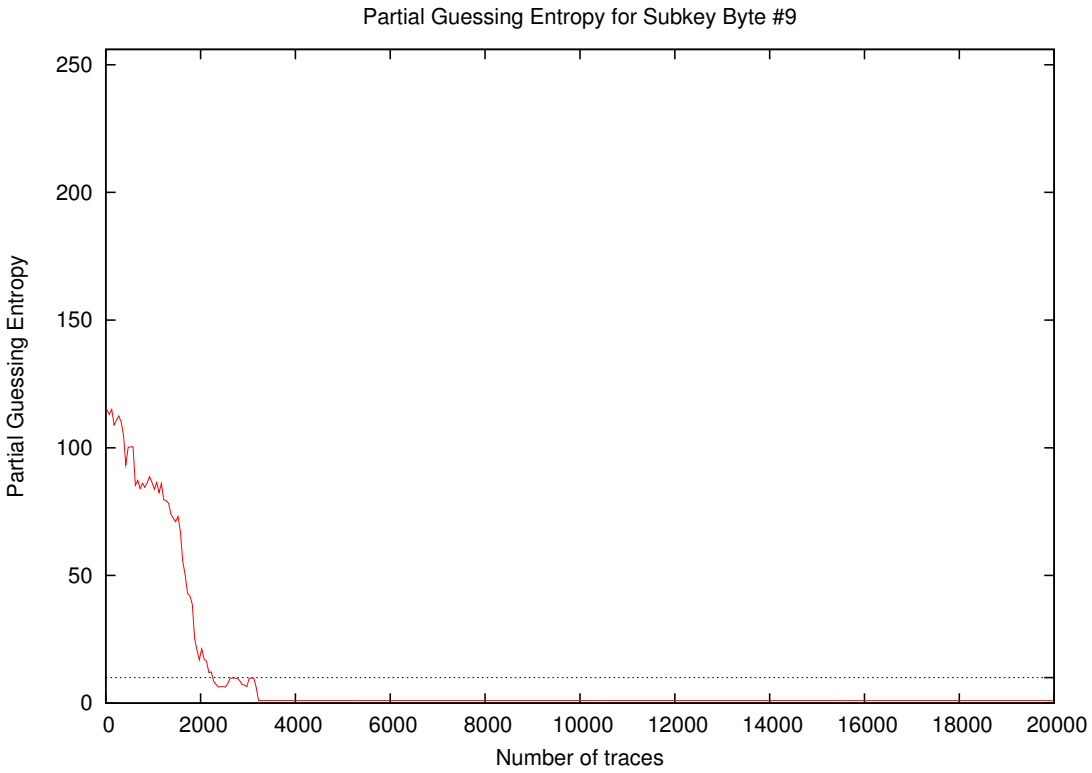

Partial Guessing Entropy for Subkey Byte #4
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000

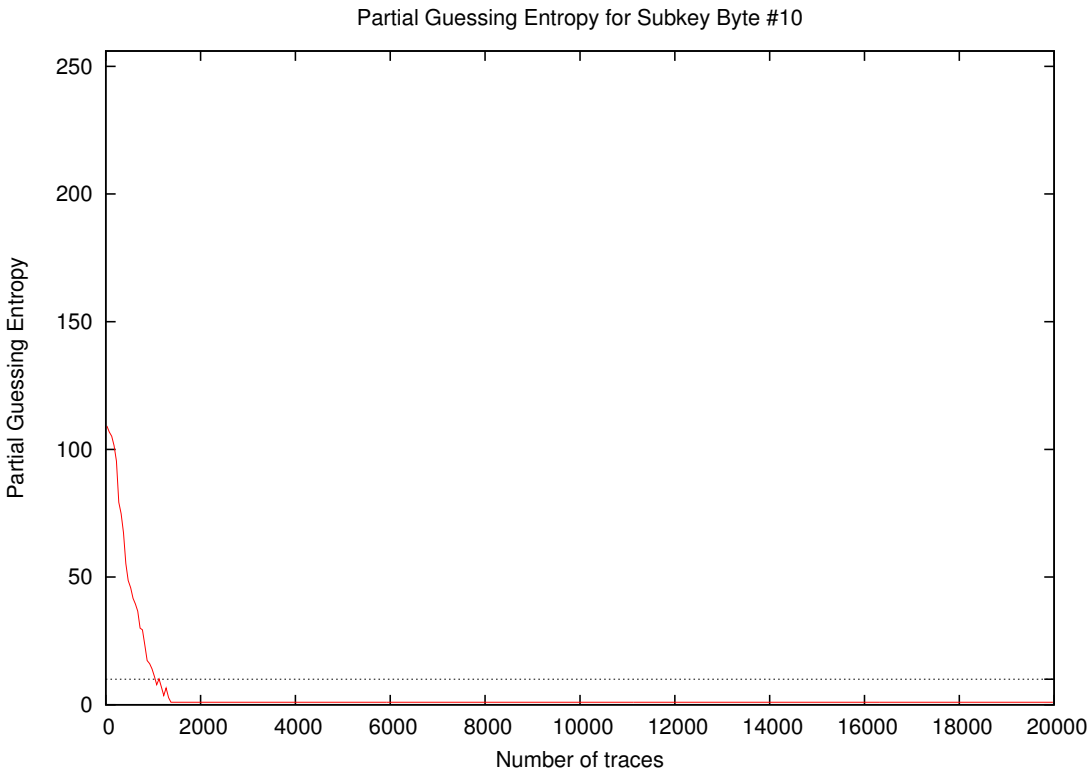

Partial Guessing Entropy for Subkey Byte #5
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000

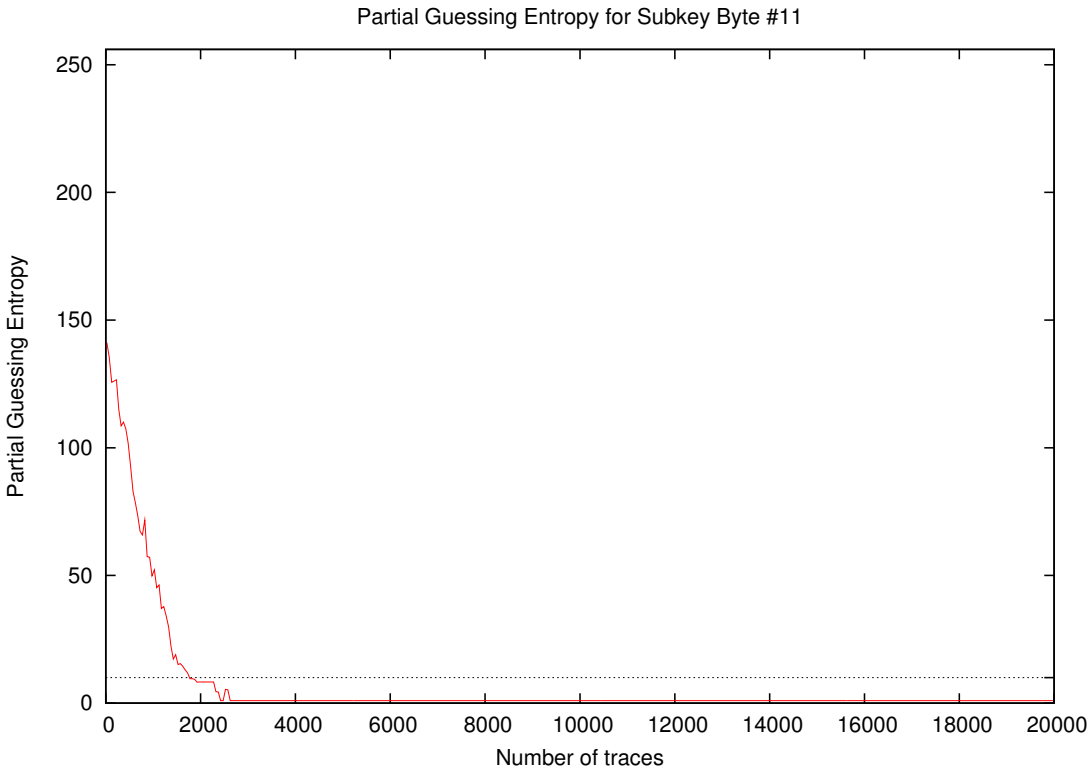

Partial Guessing Entropy for Subkey Byte #6
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000

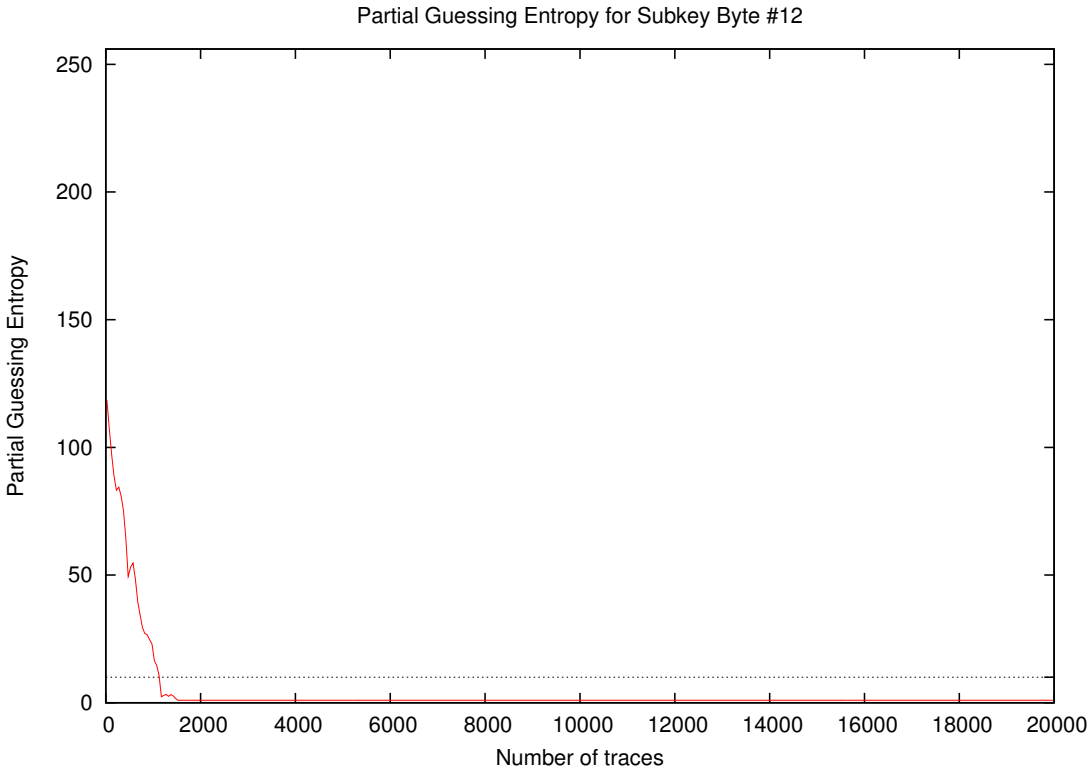

Partial Guessing Entropy for Subkey Byte #7
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000

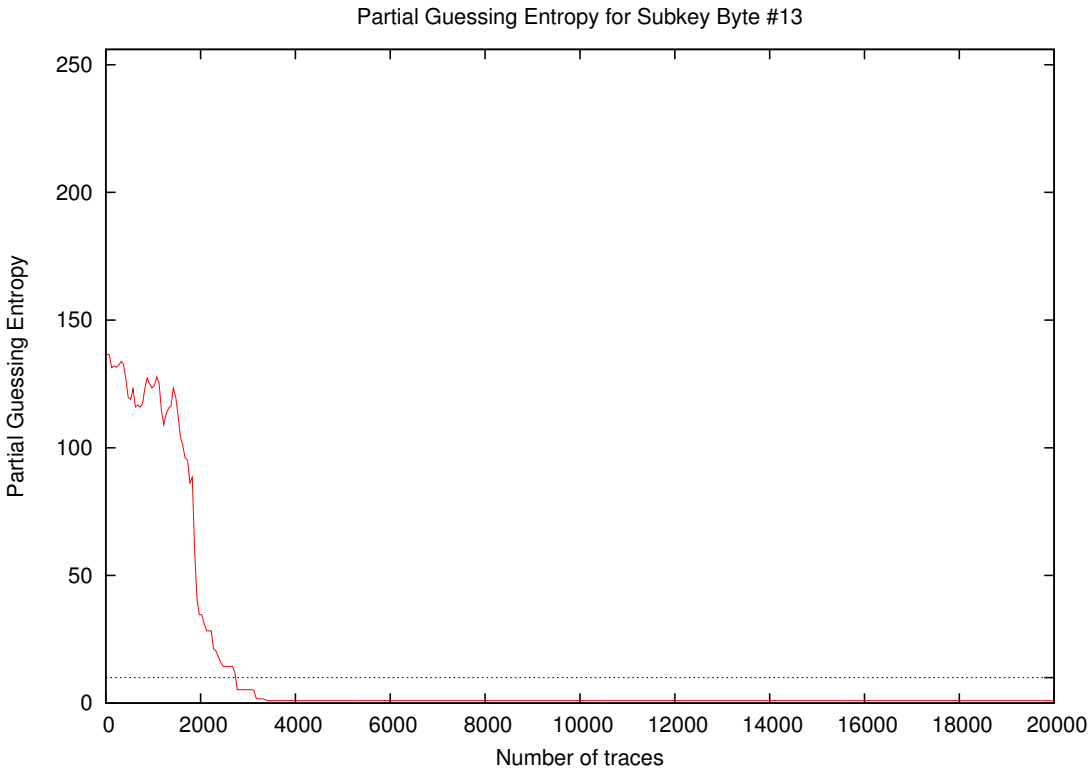

Partial Guessing Entropy for Subkey Byte #8
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000

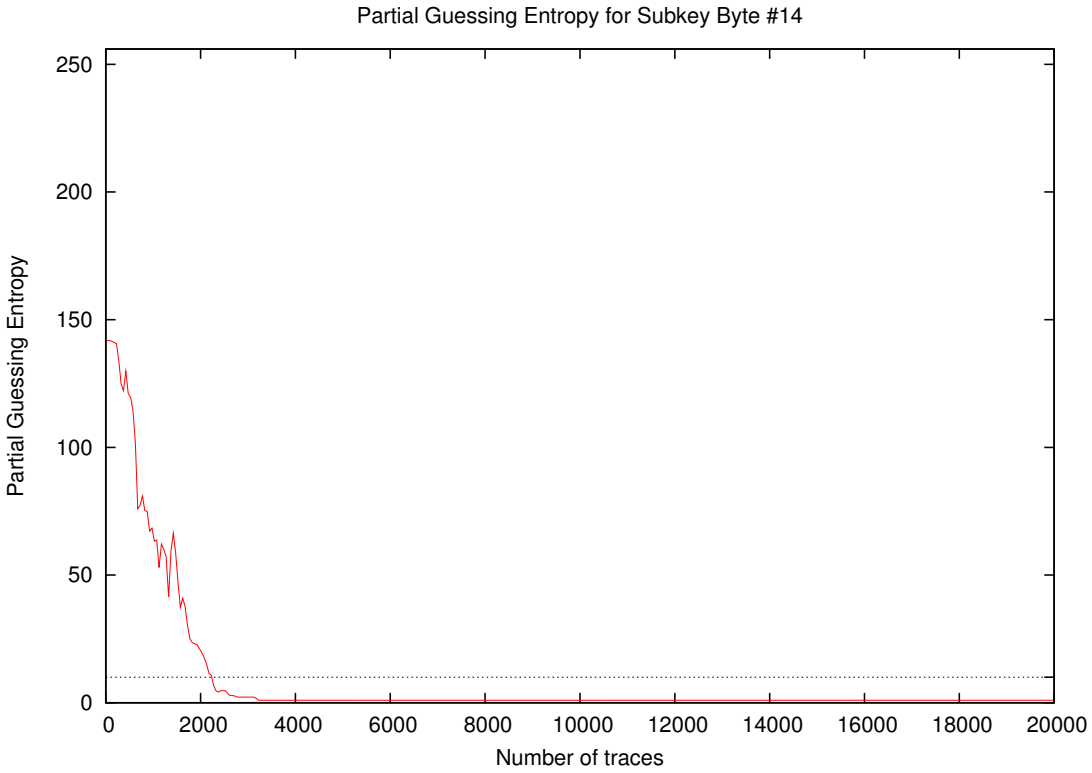

Partial Guessing Entropy for Subkey Byte #9
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000

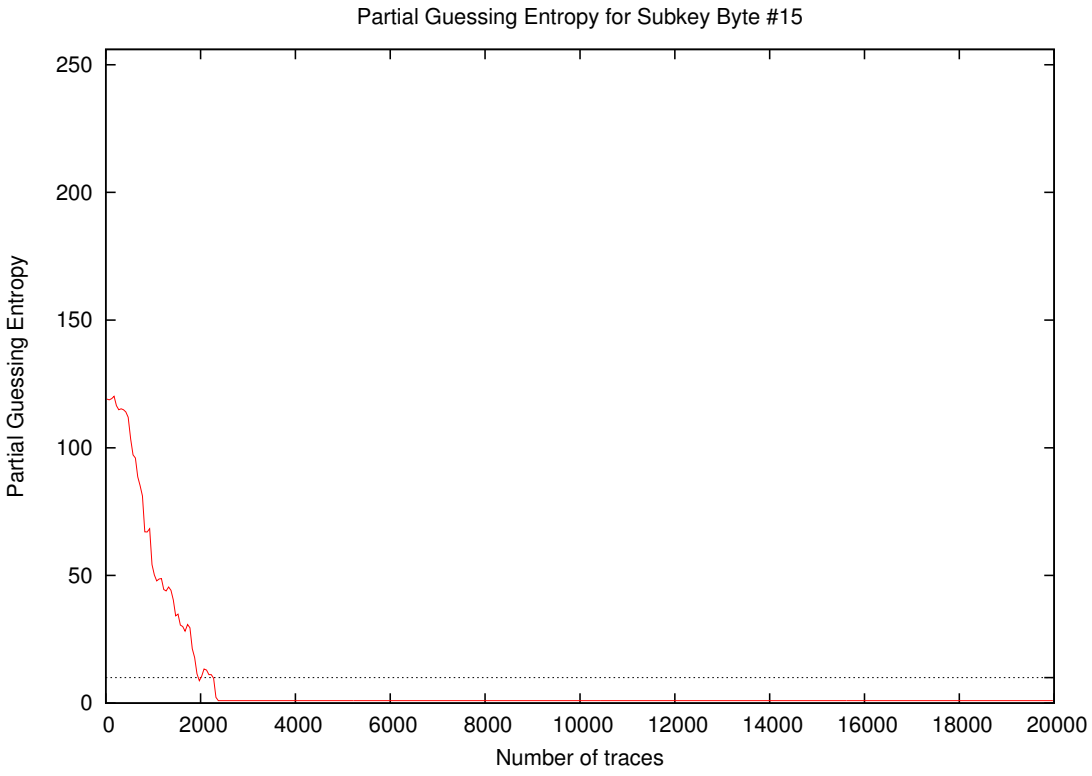

Partial Guessing Entropy for Subkey Byte #10
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000

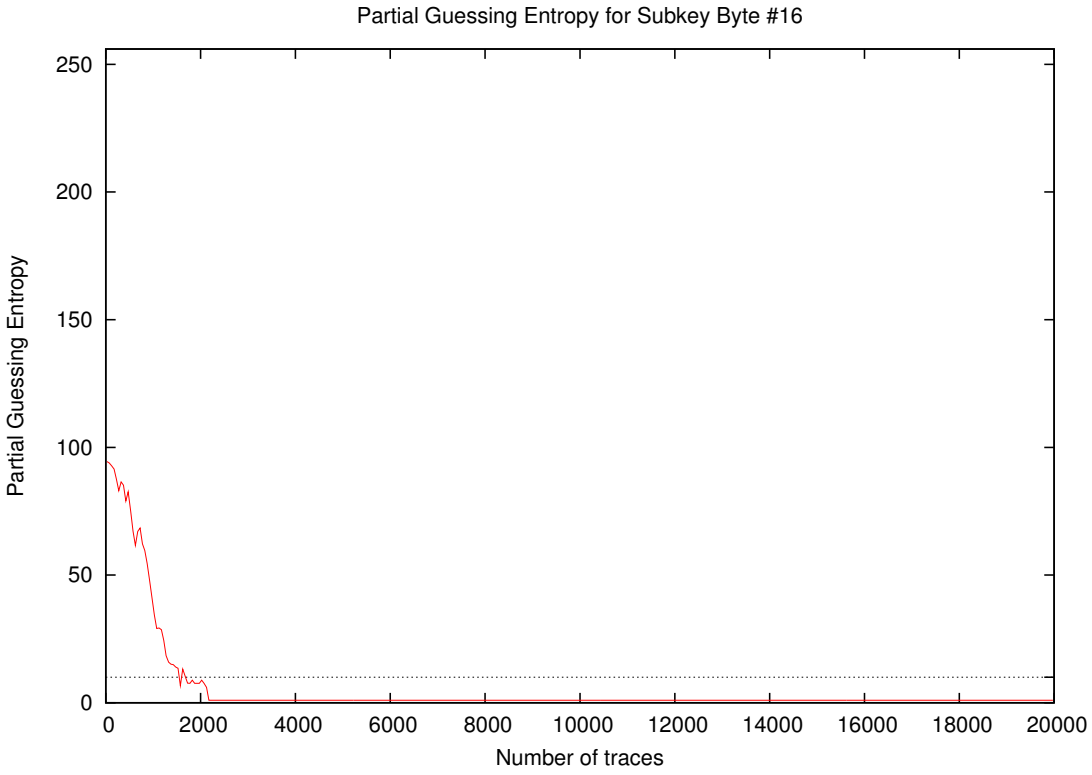

Partial Guessing Entropy for Subkey Byte #11
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000

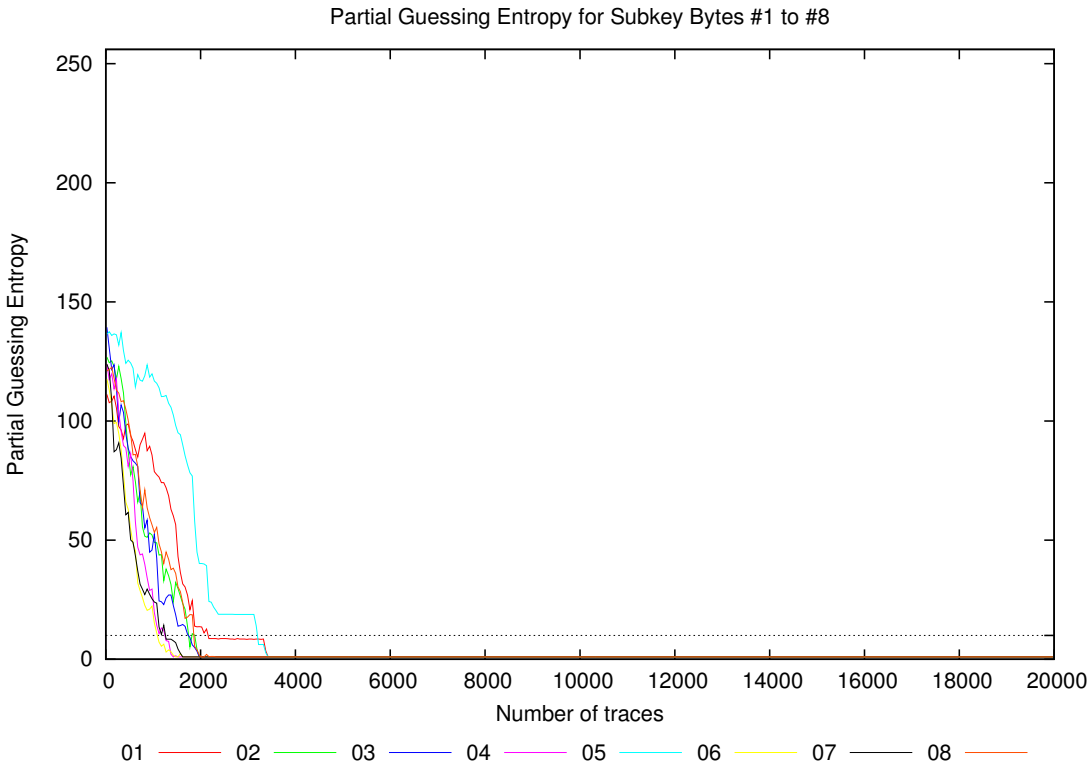

Partial Guessing Entropy for Subkey Byte #12
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000

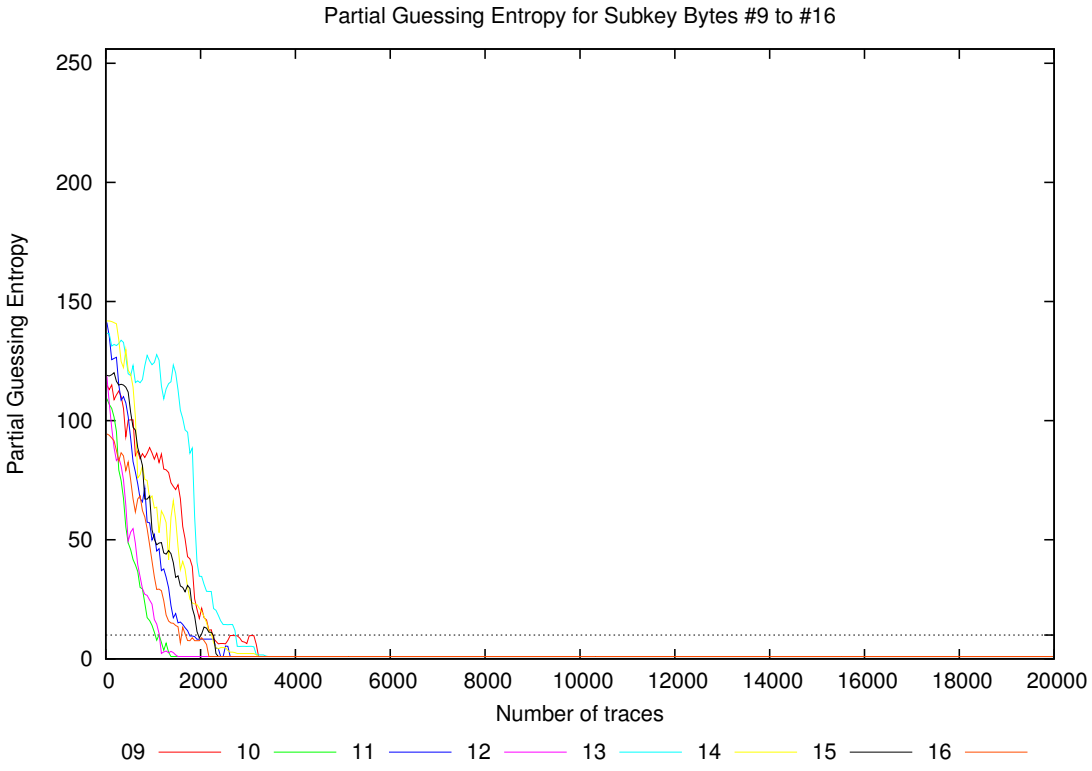

Partial Guessing Entropy for Subkey Byte #13
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000

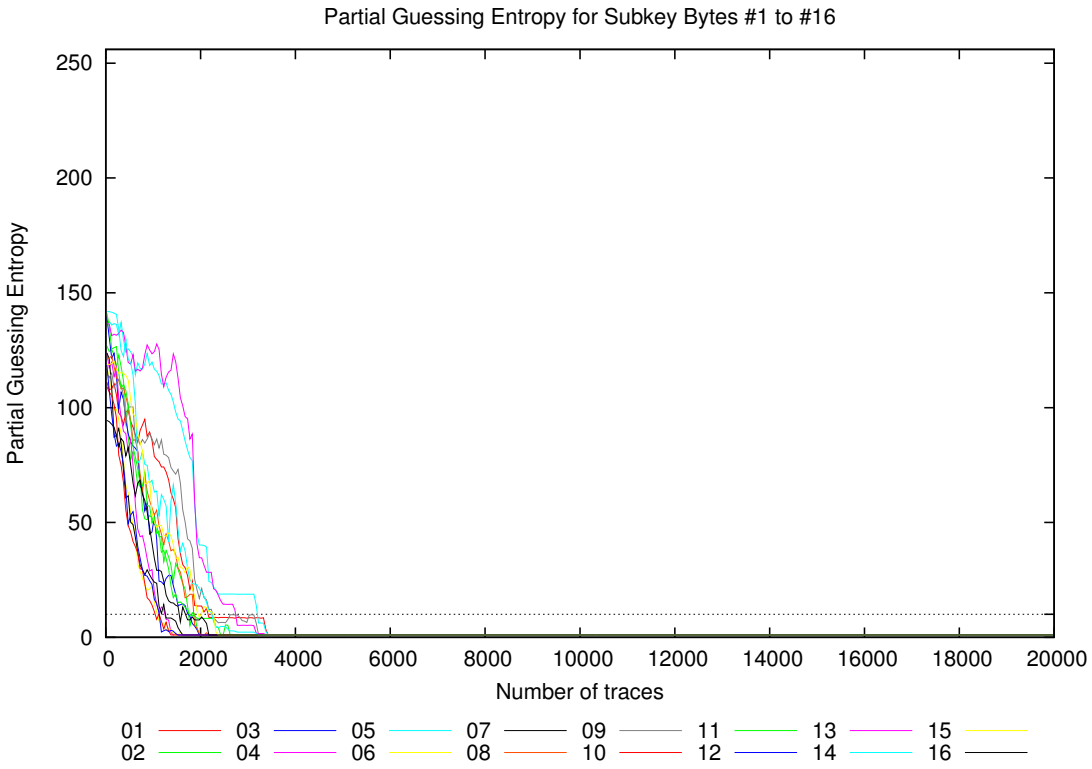

Partial Guessing Entropy for Subkey Byte #14
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000


Partial Guessing Entropy for Subkey Byte #15
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000


Partial Guessing Entropy for Subkey Byte #16
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000


Partial Guessing Entropy for Subkey Bytes #1 to #8
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000
01
02
03
04
05
06
07
08


Partial Guessing Entropy for Subkey Bytes #9 to #16
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000
09
10
11
12
13
14
15
16


Partial Guessing Entropy for Subkey Bytes #1 to #16
Partial Guessing Entropy
250
200
150
100
50
0
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000
Number of traces
01
02
03
04
05
06
07
08
09
10
11
12
13
14
15
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 | 113.2 | 128.6 | 142.3 | 124.6 | 137.6 | 111.3 | 125.8 | 122.6 | 115.2 | 111.3 | 141.2 | 121.2 | 136.7 | 141.8 | 120.6 | 89.3 | 89.3 | 142.3 | 123.9 |
| 20 | 113.2 | 126.7 | 142.3 | 124.6 | 136.2 | 119.3 | 125.8 | 119.2 | 115.2 | 111.3 | 141.2 | 121.2 | 136.7 | 141.8 | 120.6 | 96.0 | 96.0 | 142.3 | 124.4 |
| 30 | 113.2 | 126.7 | 135.3 | 124.6 | 136.2 | 119.3 | 124.5 | 119.2 | 115.2 | 107.8 | 141.2 | 121.2 | 136.7 | 141.8 | 114.2 | 97.2 | 97.2 | 141.8 | 123.4 |
| 40 | 110.5 | 126.7 | 142.3 | 120.8 | 137.6 | 119.3 | 120.2 | 122.6 | 115.2 | 107.8 | 141.2 | 114.4 | 136.7 | 141.8 | 120.6 | 95.2 | 95.2 | 142.3 | 123.3 |
| 50 | 105.7 | 126.7 | 135.3 | 121.3 | 136.2 | 119.3 | 125.8 | 119.2 | 115.2 | 107.8 | 141.2 | 106.8 | 136.7 | 141.8 | 120.6 | 95.3 | 95.3 | 141.8 | 122.2 |
| 100 | 113.2 | 126.7 | 123.2 | 120.4 | 137.6 | 105.8 | 120.2 | 122.6 | 115.2 | 104.7 | 129.0 | 105.9 | 136.7 | 141.8 | 120.2 | 93.5 | 93.5 | 141.8 | 119.8 |
| 200 | 113.2 | 119.1 | 121.8 | 120.9 | 137.6 | 98.8 | 78.7 | 111.5 | 107.9 | 105.8 | 129.1 | 82.5 | 130.4 | 141.8 | 113.8 | 84.8 | 78.7 | 141.8 | 112.4 |
| 300 | 92.9 | 125.9 | 105.4 | 98.7 | 137.6 | 96.5 | 88.8 | 108.1 | 115.2 | 71.6 | 103.0 | 75.6 | 129.0 | 134.3 | 110.3 | 87.8 | 71.6 | 137.6 | 105.0 |
| 400 | 93.5 | 104.5 | 100.2 | 88.1 | 121.8 | 72.8 | 61.0 | 102.6 | 101.3 | 63.4 | 101.1 | 59.9 | 125.0 | 126.4 | 115.3 | 78.2 | 59.9 | 126.4 | 94.7 |
| 500 | 100.7 | 78.8 | 87.5 | 84.8 | 130.7 | 65.8 | 75.0 | 90.1 | 98.6 | 52.8 | 97.0 | 49.9 | 122.8 | 110.8 | 107.0 | 77.6 | 49.9 | 130.7 | 89.4 |
| 1000 | 82.9 | 48.3 | 54.9 | 27.1 | 110.2 | 15.2 | 23.9 | 57.5 | 86.9 | 10.8 | 52.7 | 25.2 | 123.0 | 69.2 | 54.1 | 34.6 | 10.8 | 123.0 | 54.8 |
| 2000 | 13.4 | 1.0 | 1.0 | 1.0 | 40.4 | 1.0 | 1.0 | 1.0 | 17.2 | 1.0 | 8.3 | 1.0 | 34.7 | 18.8 | 6.4 | 7.6 | 1.0 | 40.4 | 9.7 |
| 3000 | 8.7 | 1.0 | 1.0 | 1.0 | 18.8 | 1.0 | 1.0 | 1.0 | 6.3 | 1.0 | 1.0 | 1.0 | 5.3 | 2.2 | 1.0 | 1.0 | 1.0 | 18.8 | 3.3 |
| 4000 | 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 |
| 5000 | 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 |
| 10000 | 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 |
| 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 |