# DPA Contest v2
# Evaluation results

Reference attack

November 2010

## 1 Introduction

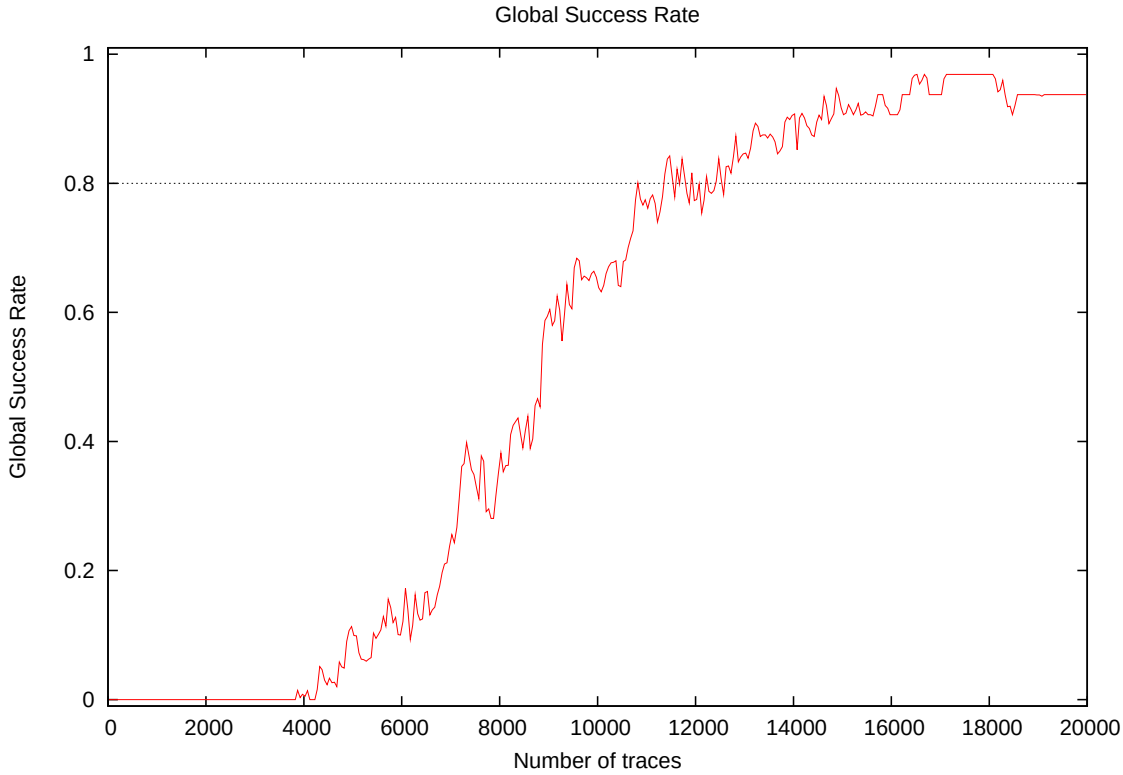
### 1.1 About the attack

- **Attack Name:** Correlation product v3
- **Sender/Team:** Olivier Meynard
- **Institution:** Télécom ParisTech, France
- **Language:** C
- **Operating system:** Linux
- **Attacked subkey:** 10

### 1.2 About the evaluation

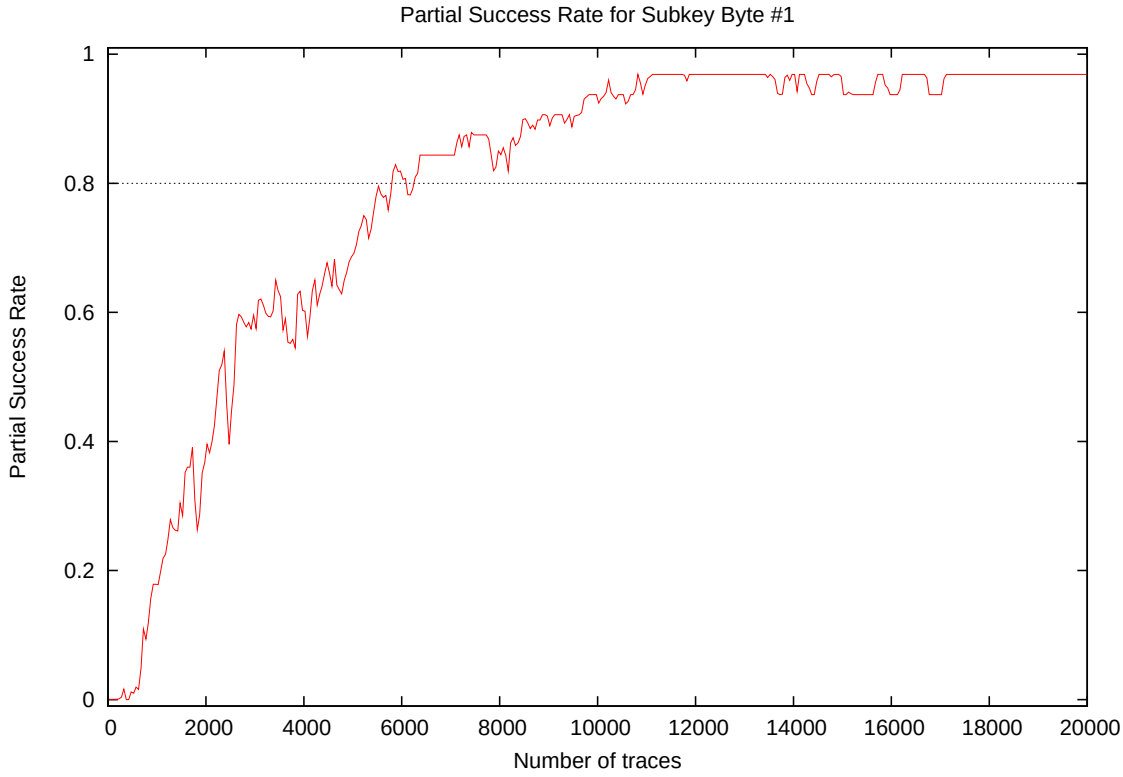
- **Date of evaluation:** November 2010

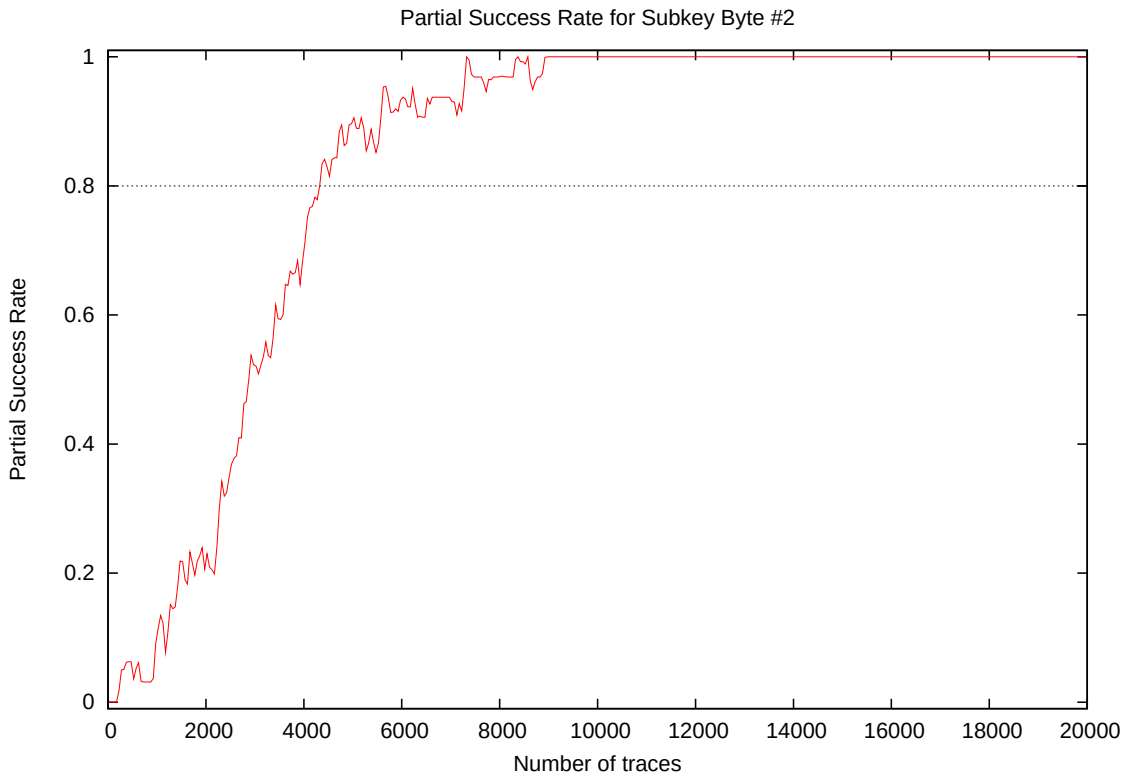
## 2 Global Success Rate

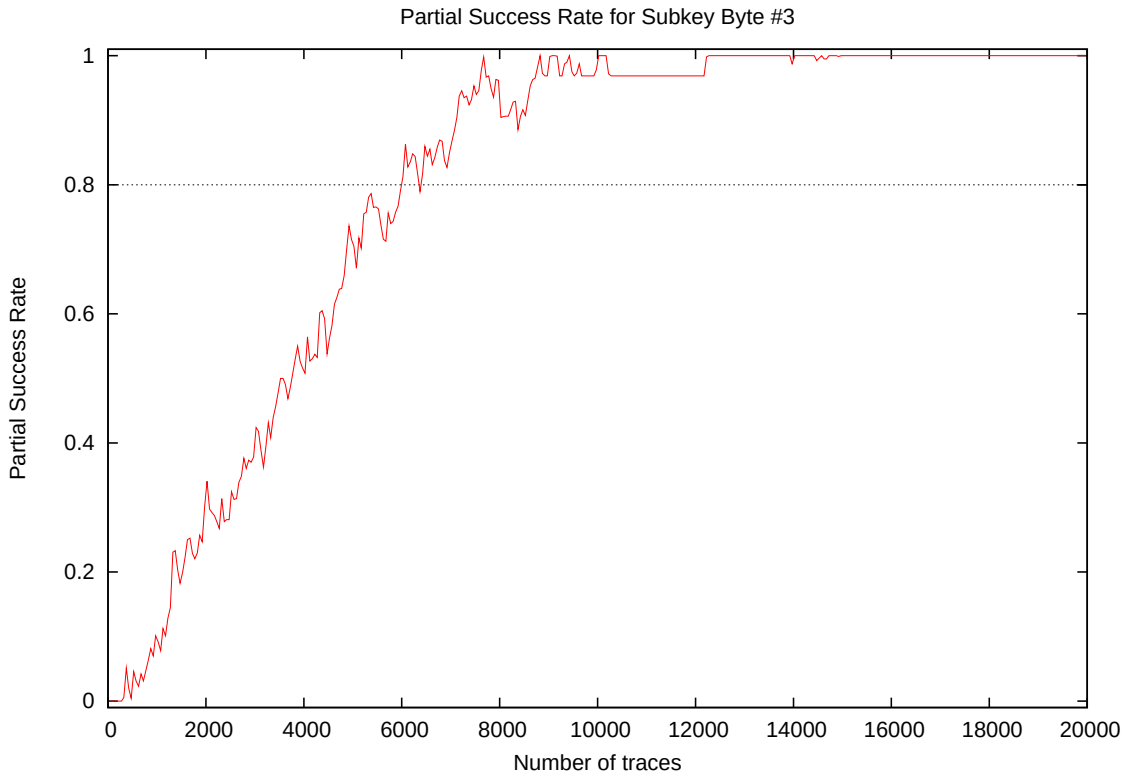


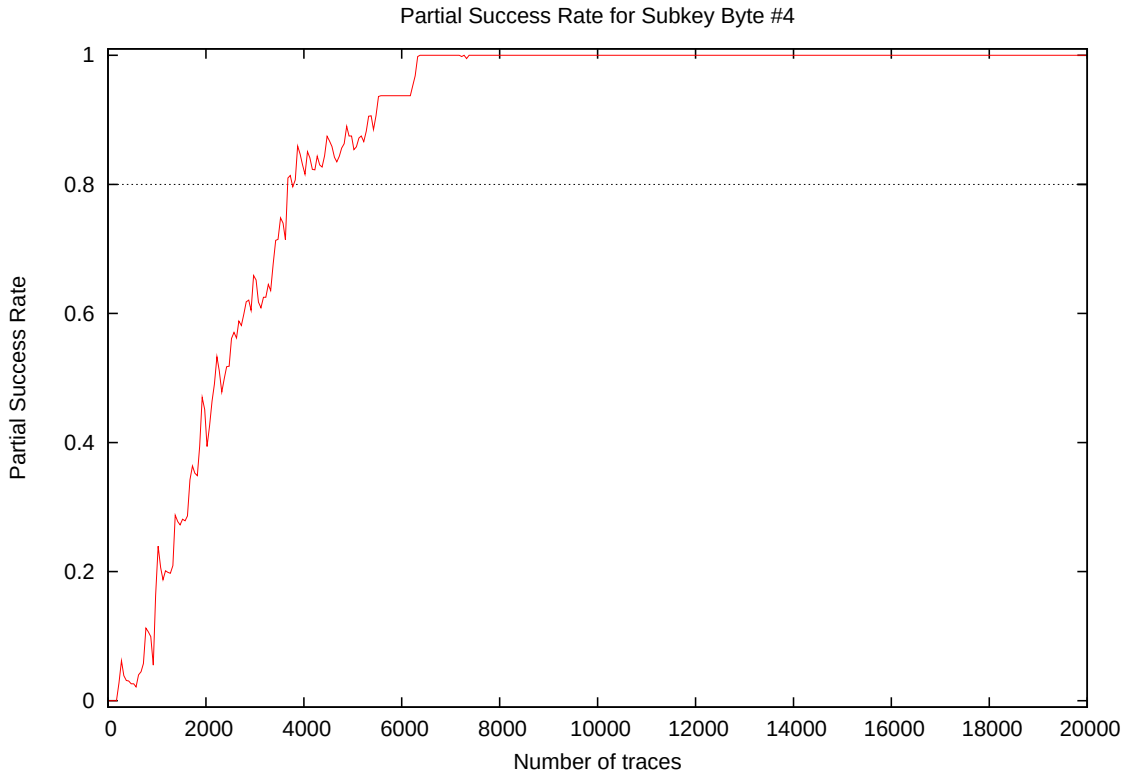
| Number of traces | Global Success Rate |
|---:|:---:|
| 10 | 0.00 |
| 20 | 0.00 |
| 30 | 0.00 |
| 40 | 0.00 |
| 50 | 0.00 |
| 100 | 0.00 |
| 200 | 0.00 |
| 300 | 0.00 |
| 400 | 0.00 |
| 500 | 0.00 |
| 1000 | 0.00 |
| 2000 | 0.00 |
| 3000 | 0.00 |
| 4000 | 0.00 |
| 5000 | 0.12 |
| 10000 | 0.62 |
| 15000 | 0.91 |
| 20000 | 0.94 |

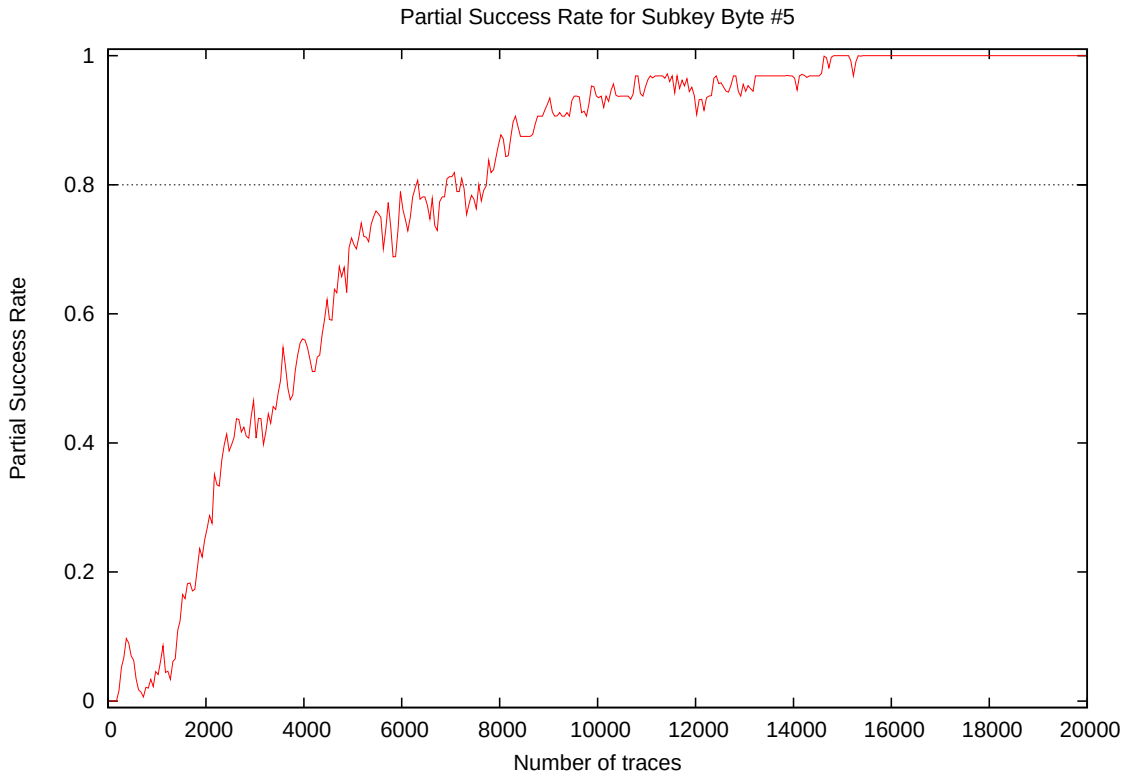
# 3 Partial Success Rate

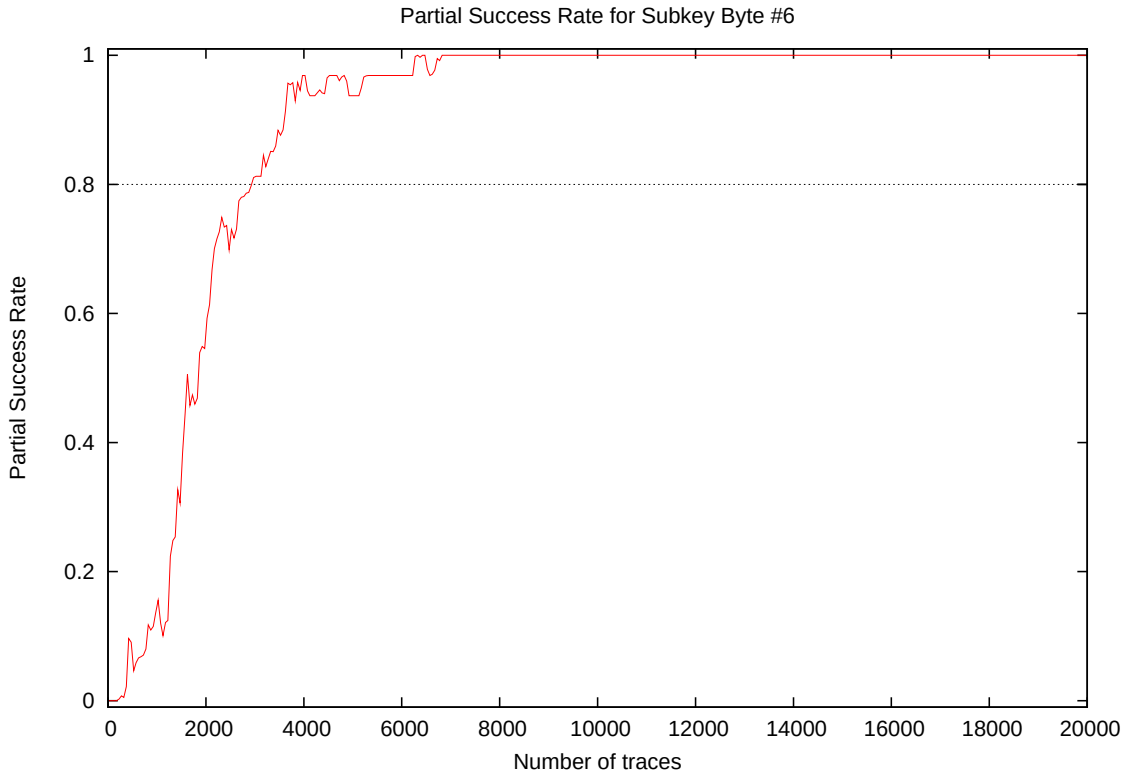


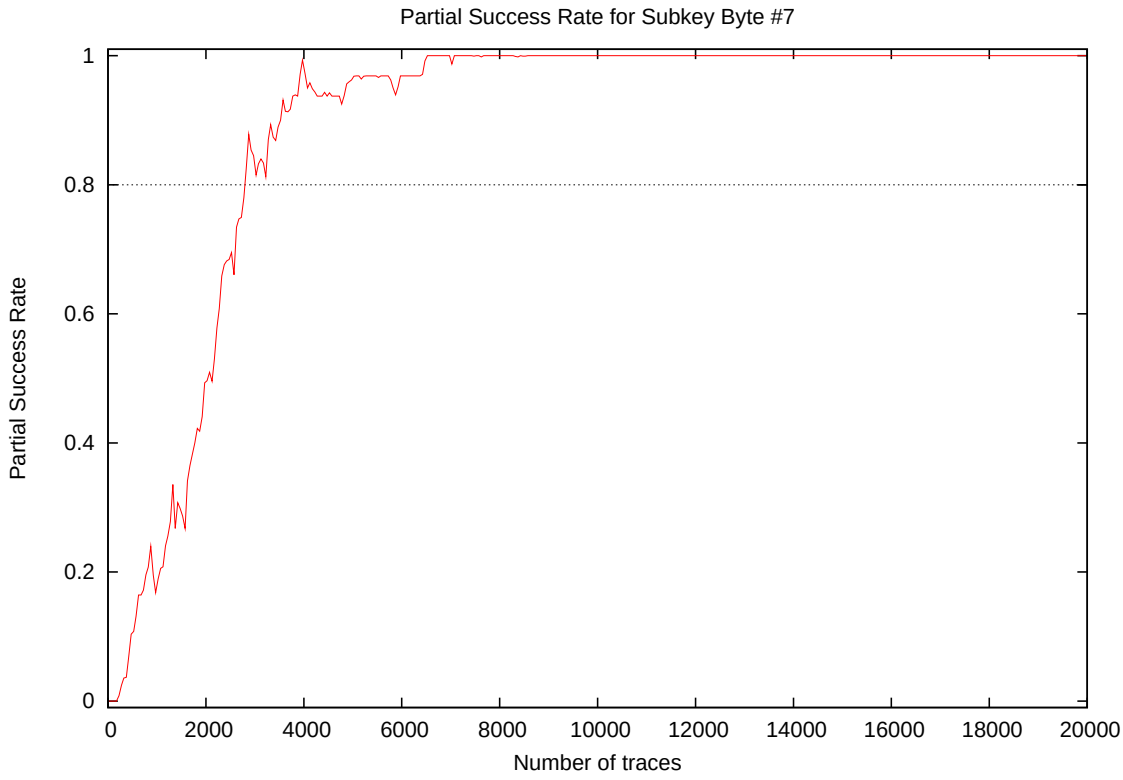



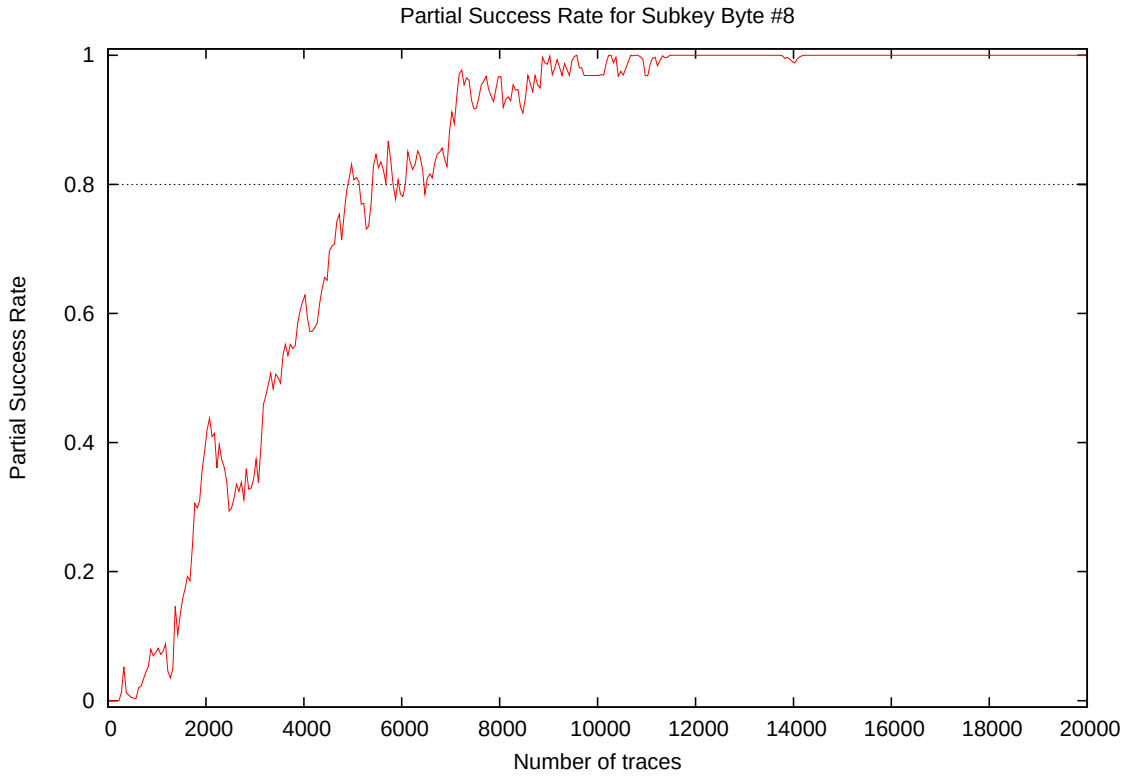

Partial Success Rate for Subkey Byte #3
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000

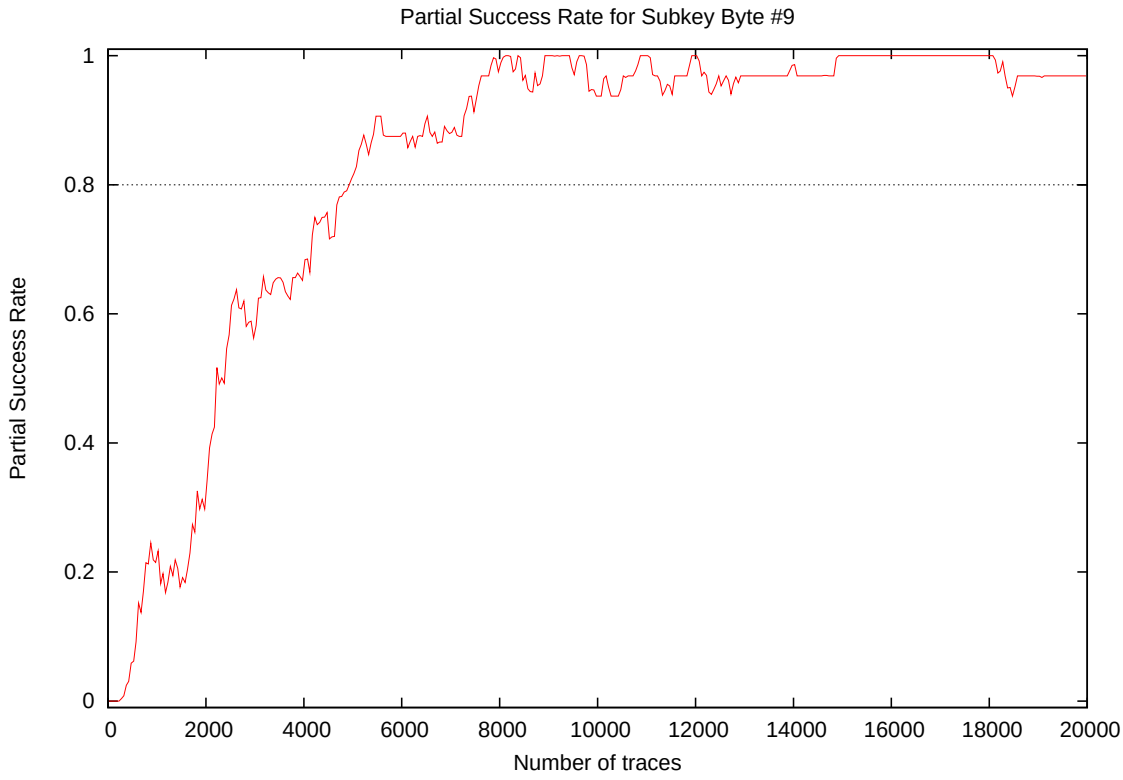

Partial Success Rate for Subkey Byte #4
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000

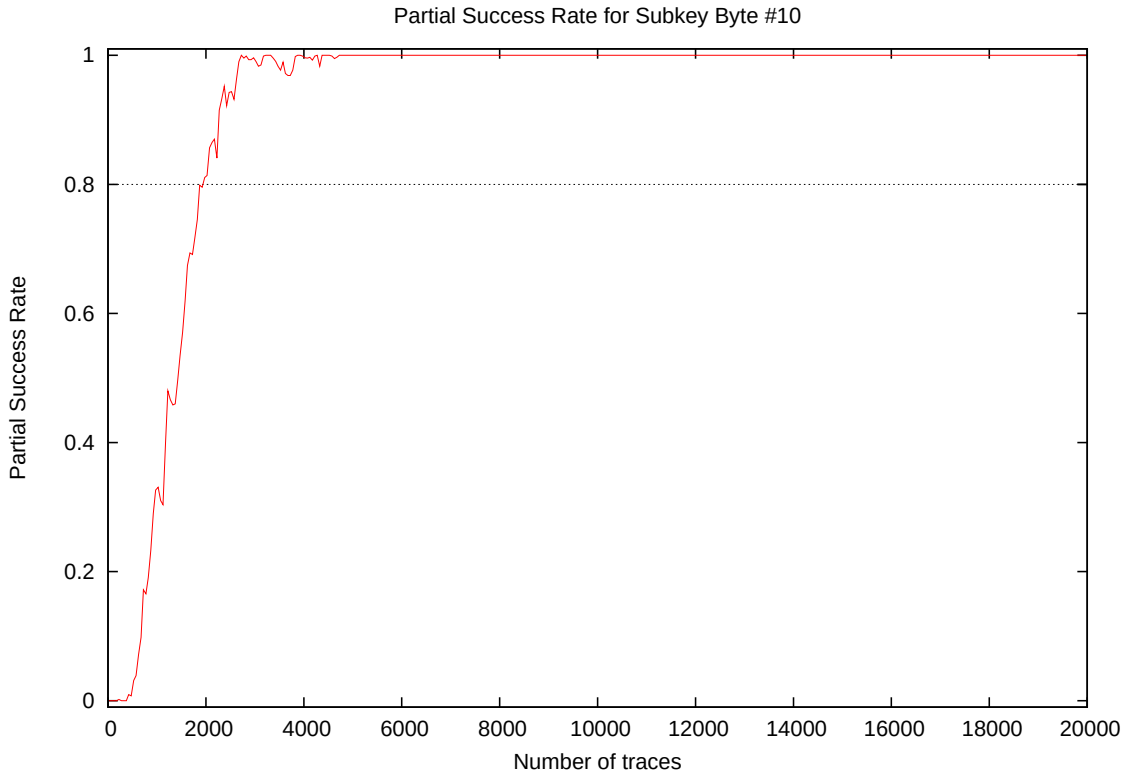

Partial Success Rate for Subkey Byte #5
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000

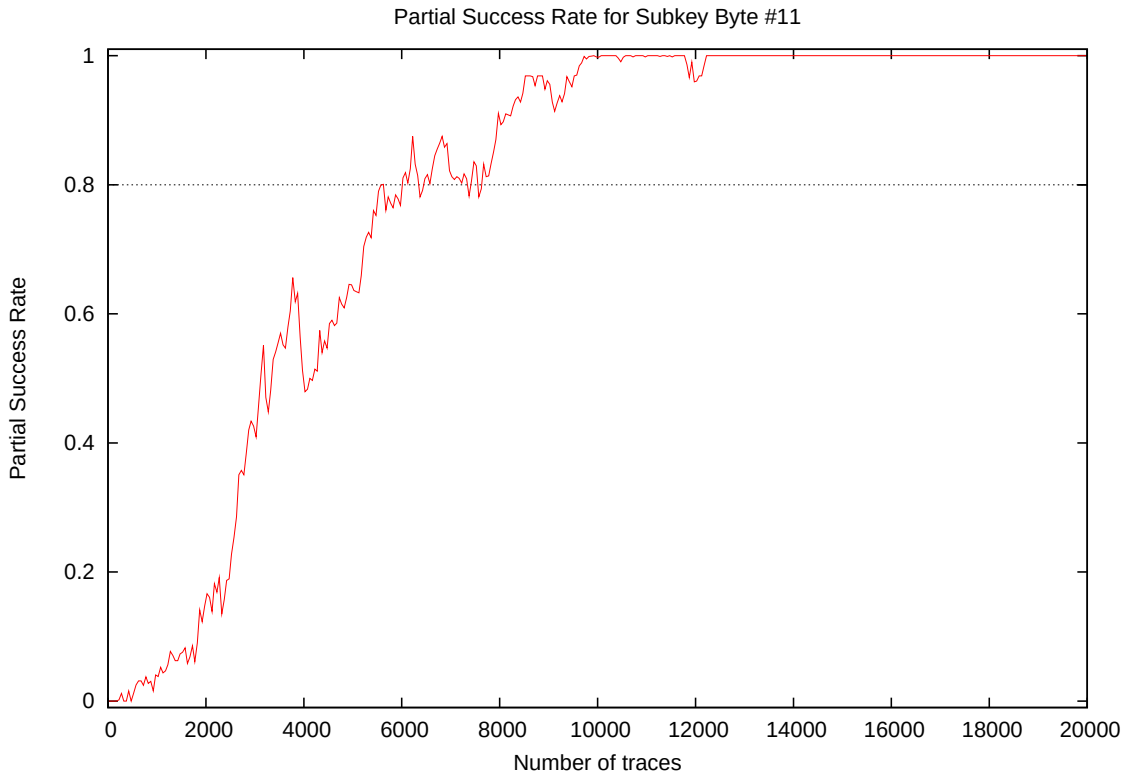

Partial Success Rate for Subkey Byte #6
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000

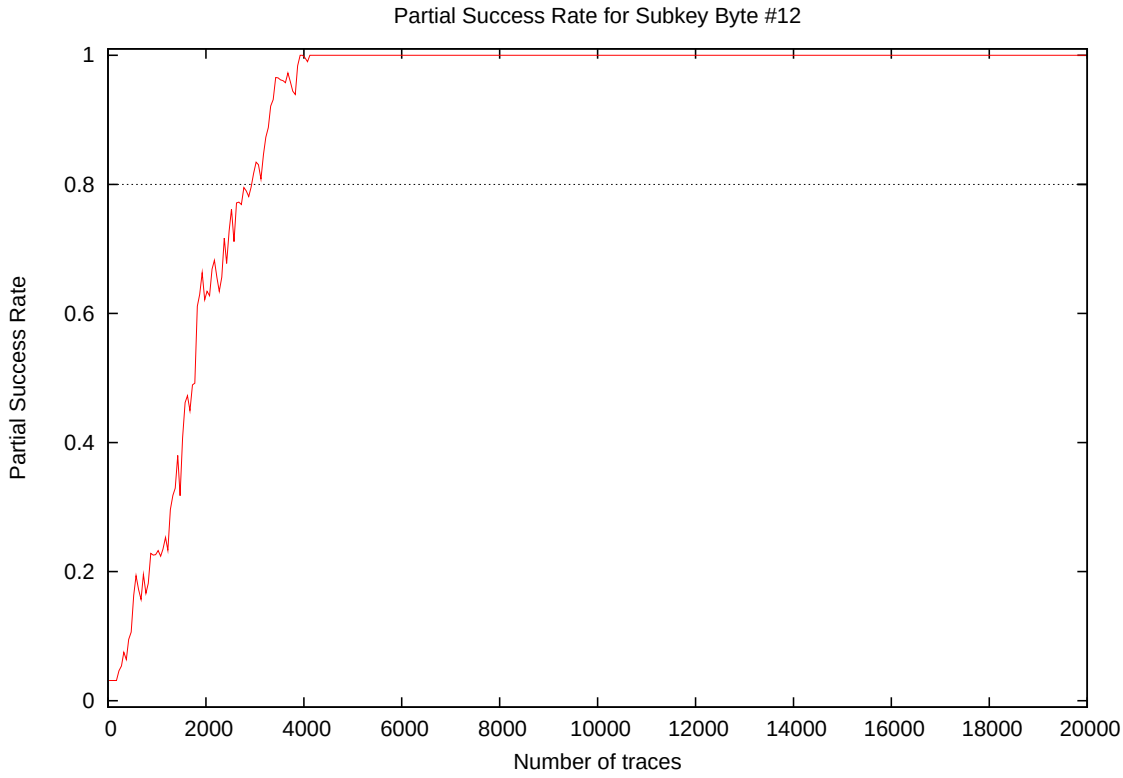

Partial Success Rate for Subkey Byte #7
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000

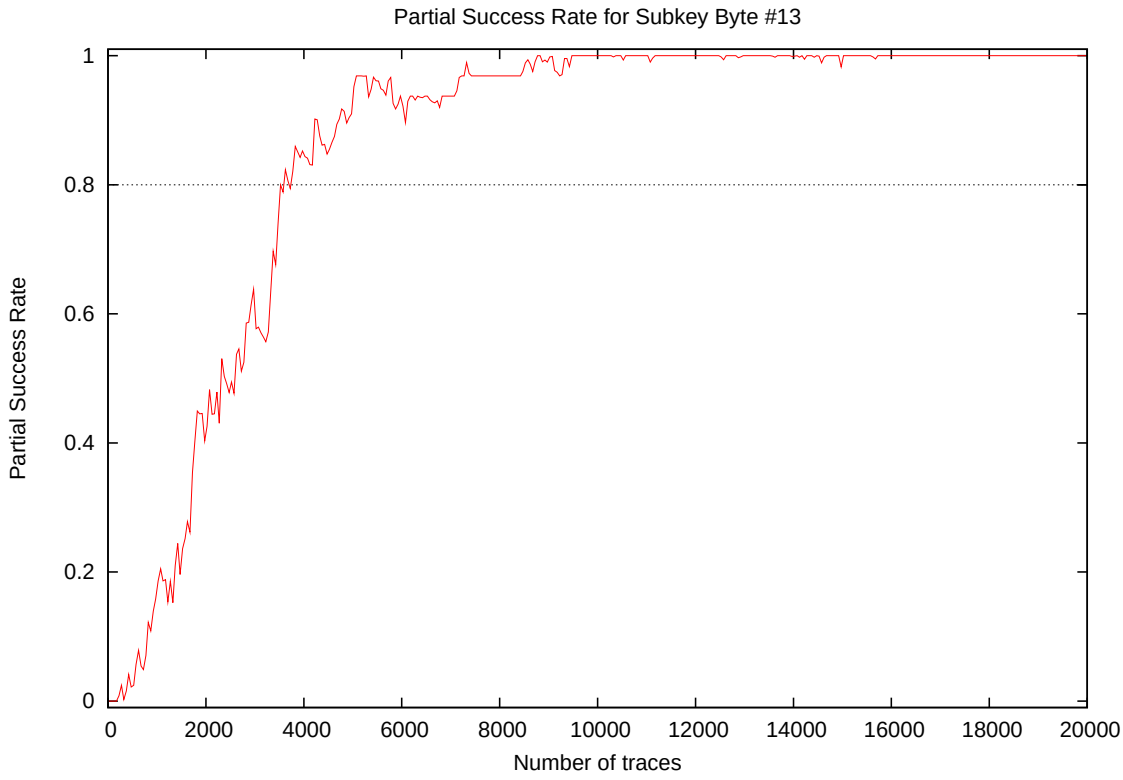

Partial Success Rate for Subkey Byte #8
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000

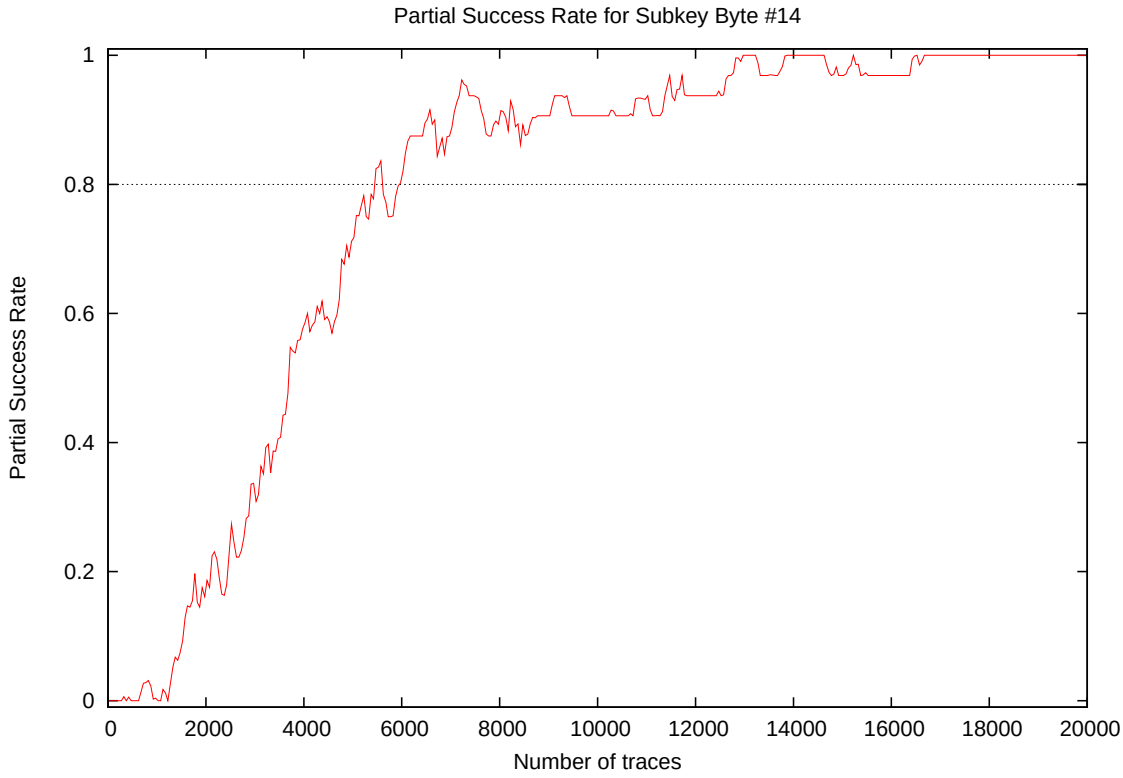

Partial Success Rate for Subkey Byte #9
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000

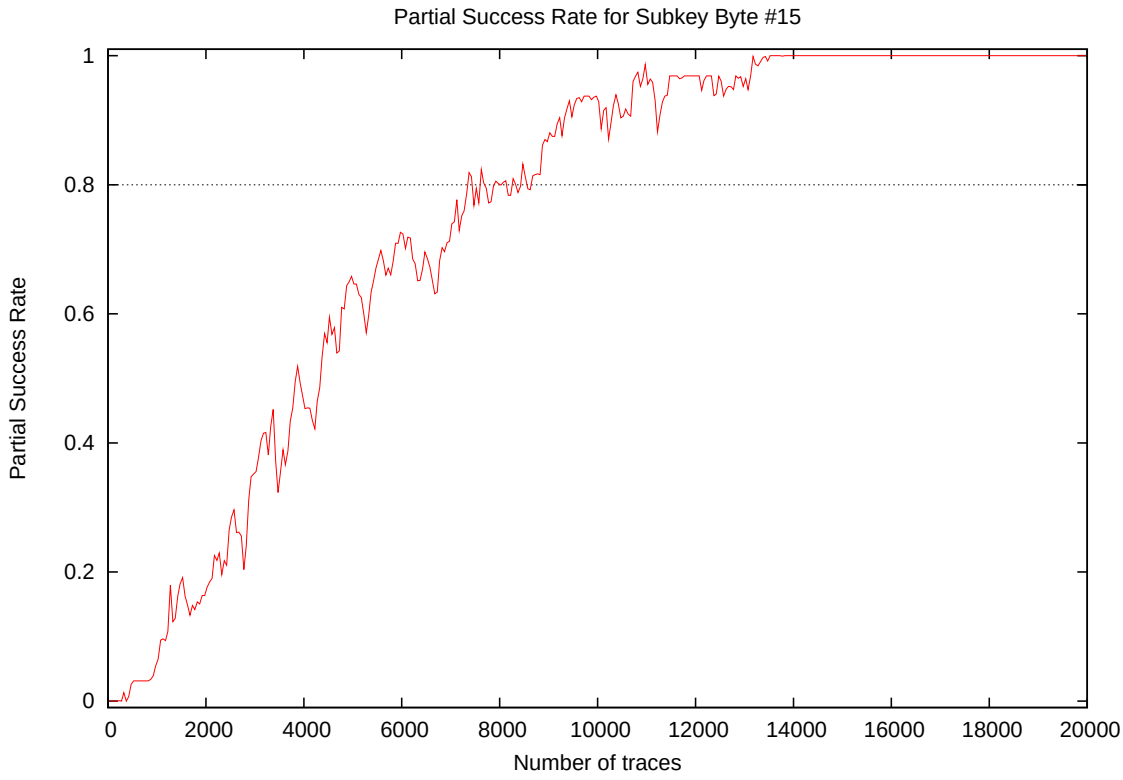

Partial Success Rate for Subkey Byte #10
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000

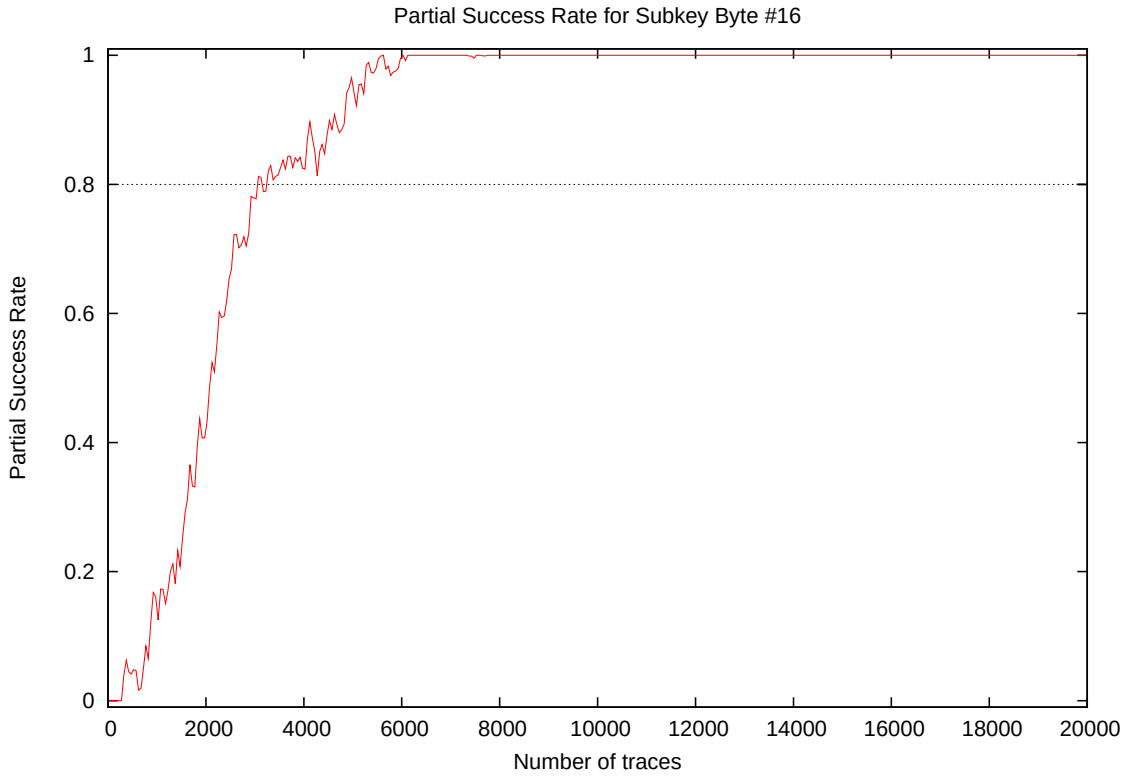

Partial Success Rate for Subkey Byte #11
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000

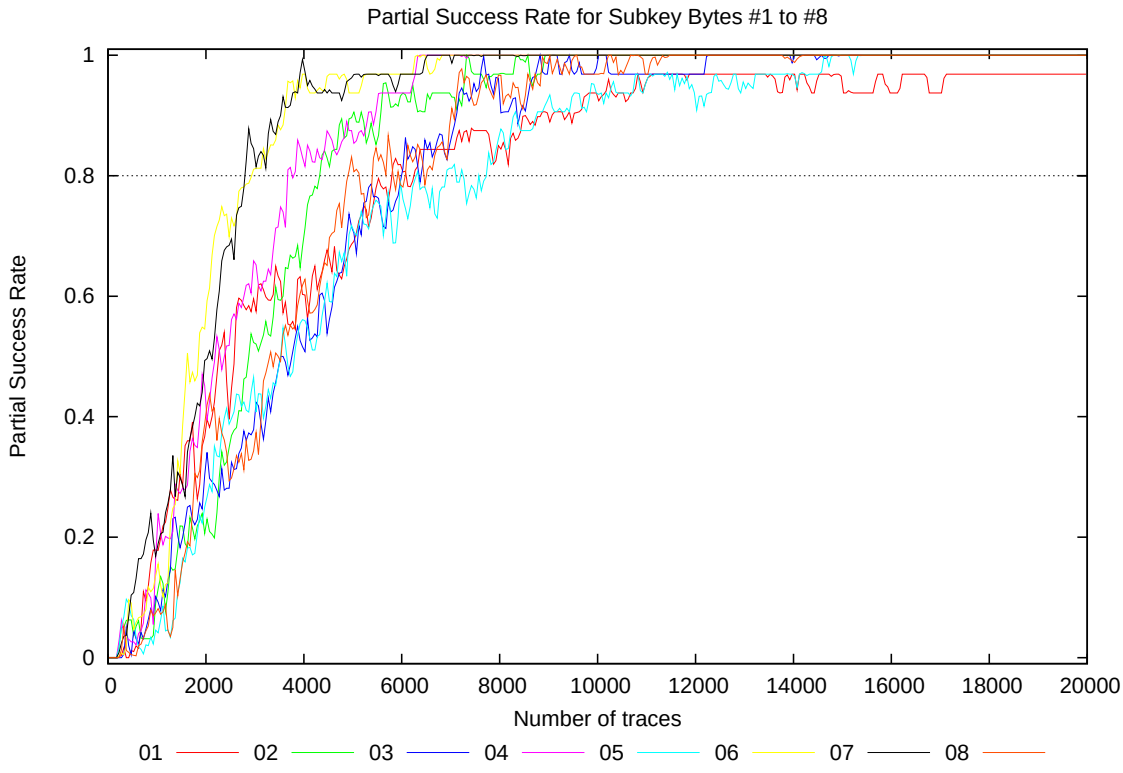

Partial Success Rate for Subkey Byte #12
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000

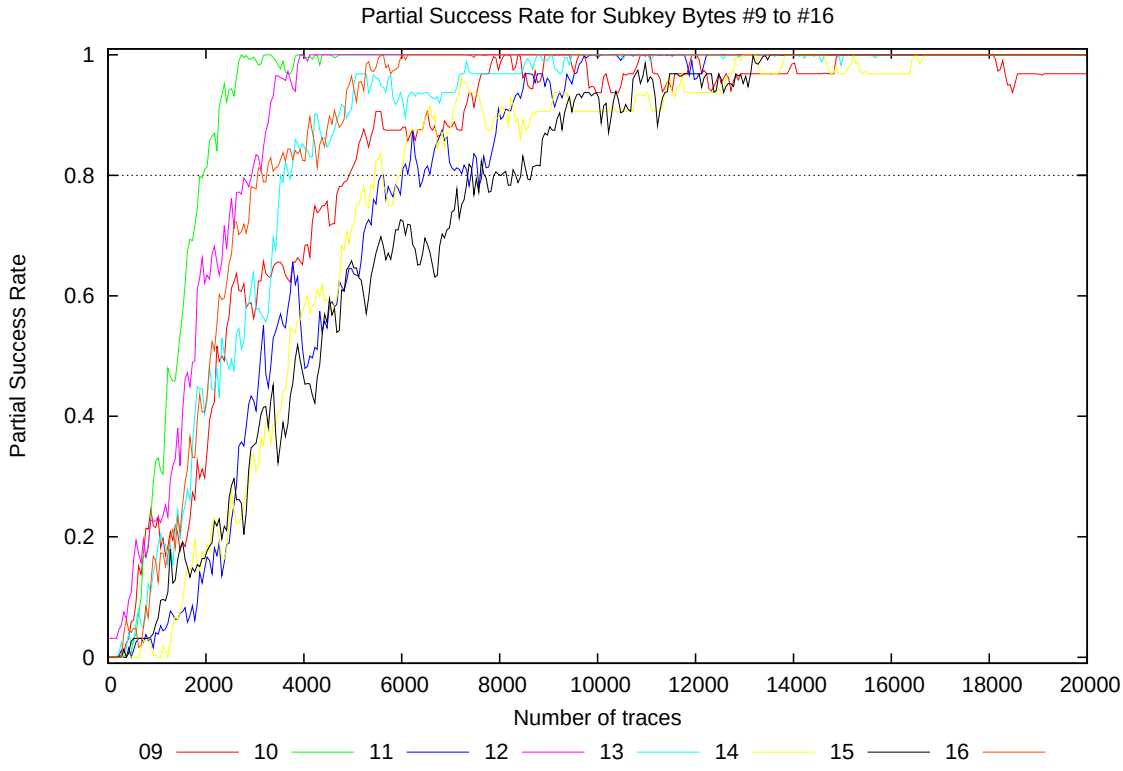

Partial Success Rate for Subkey Byte #13
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000

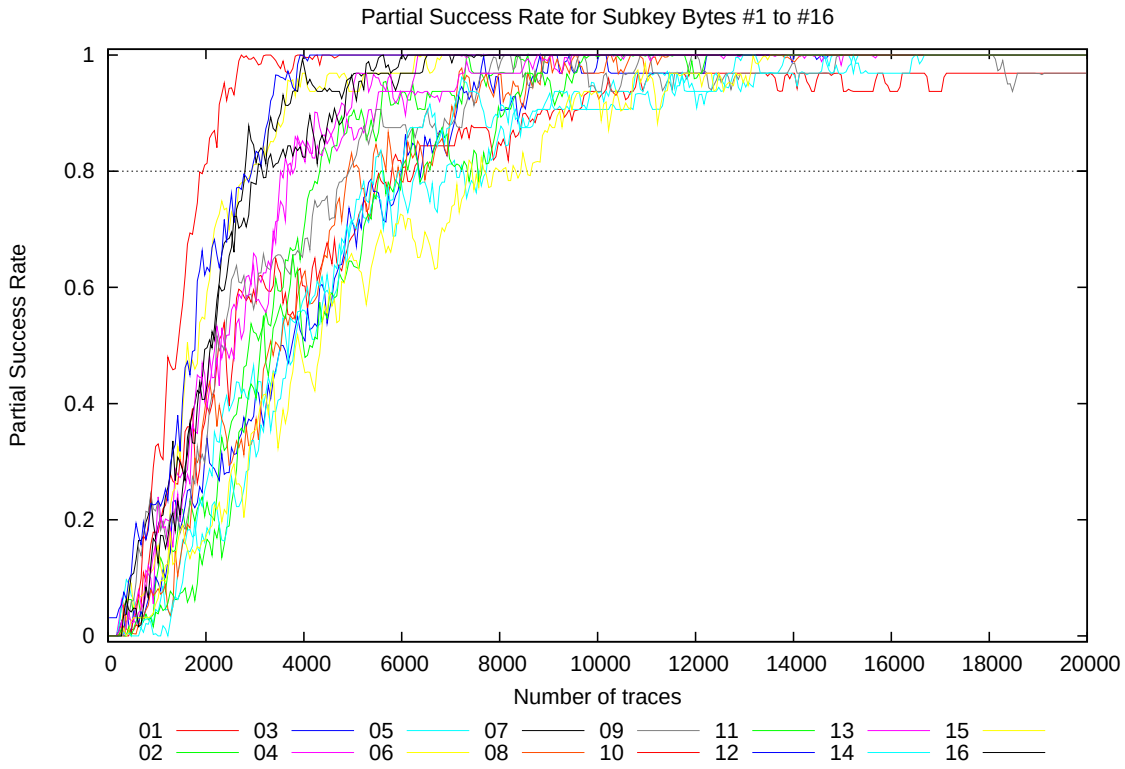

Partial Success Rate for Subkey Byte #14
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000


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

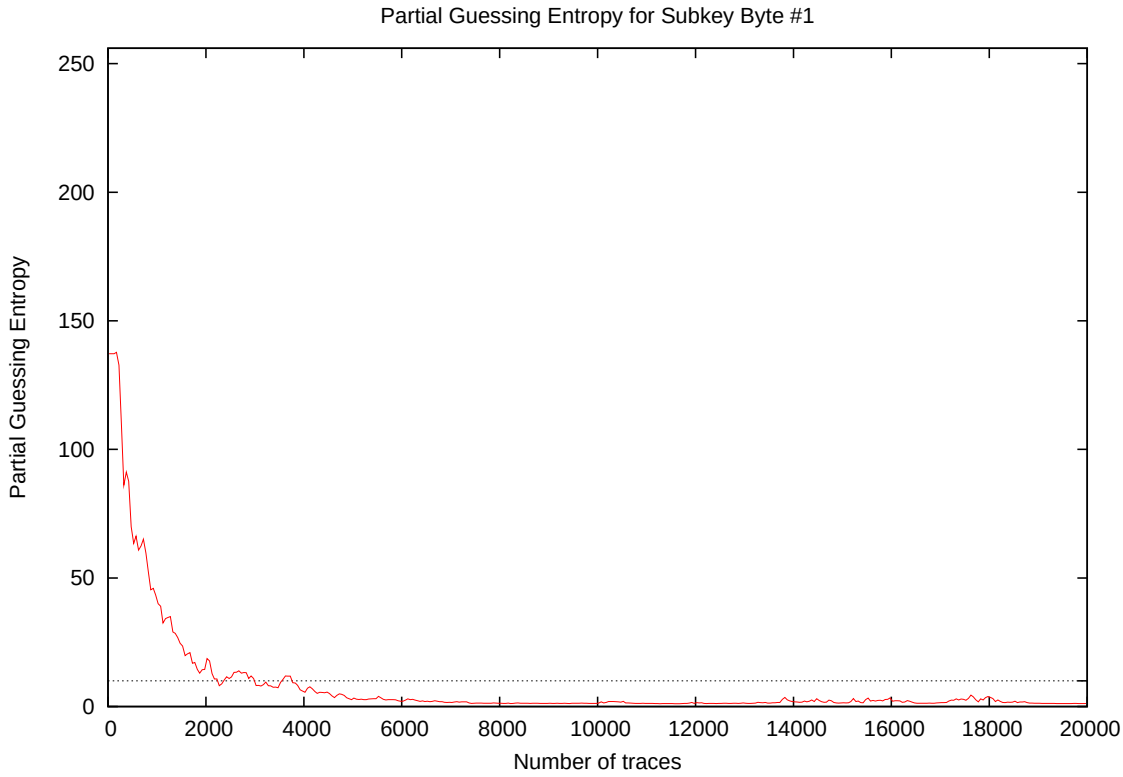

Partial Success Rate for Subkey Bytes #1 to #8
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000
01
02
03
04
05
06
07
08

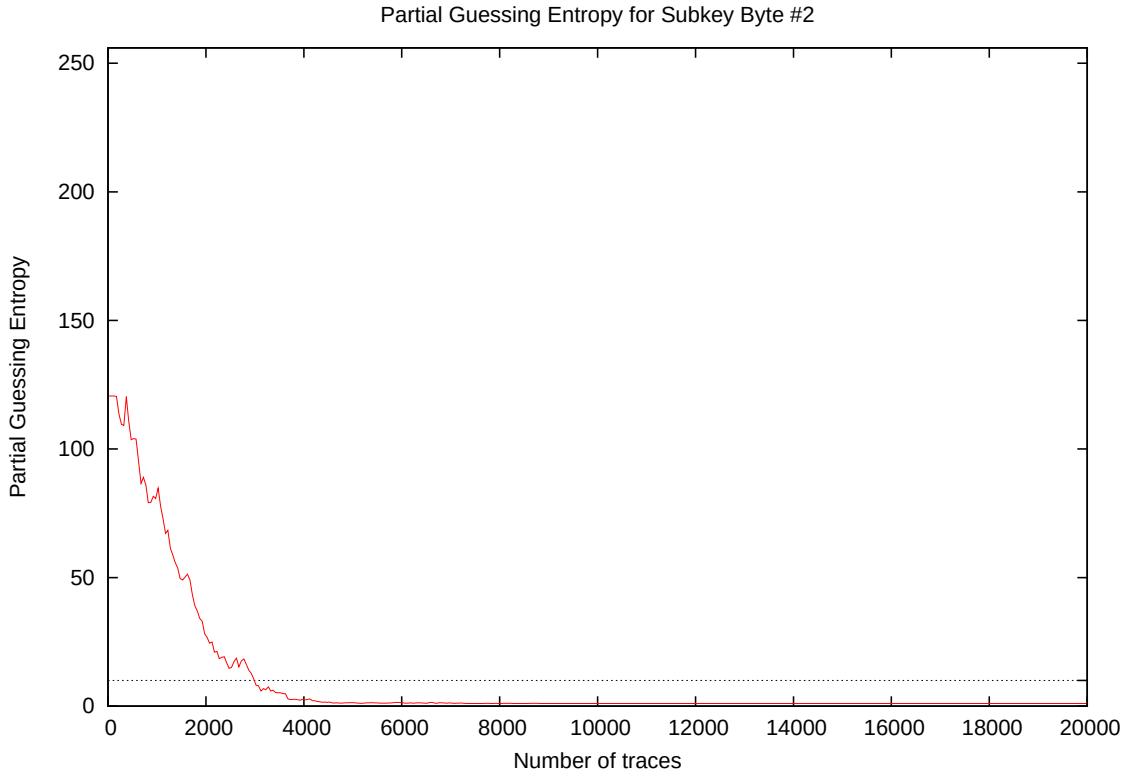

Partial Success Rate for Subkey Bytes #9 to #16
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000
09
10
11
12
13
14
15
16

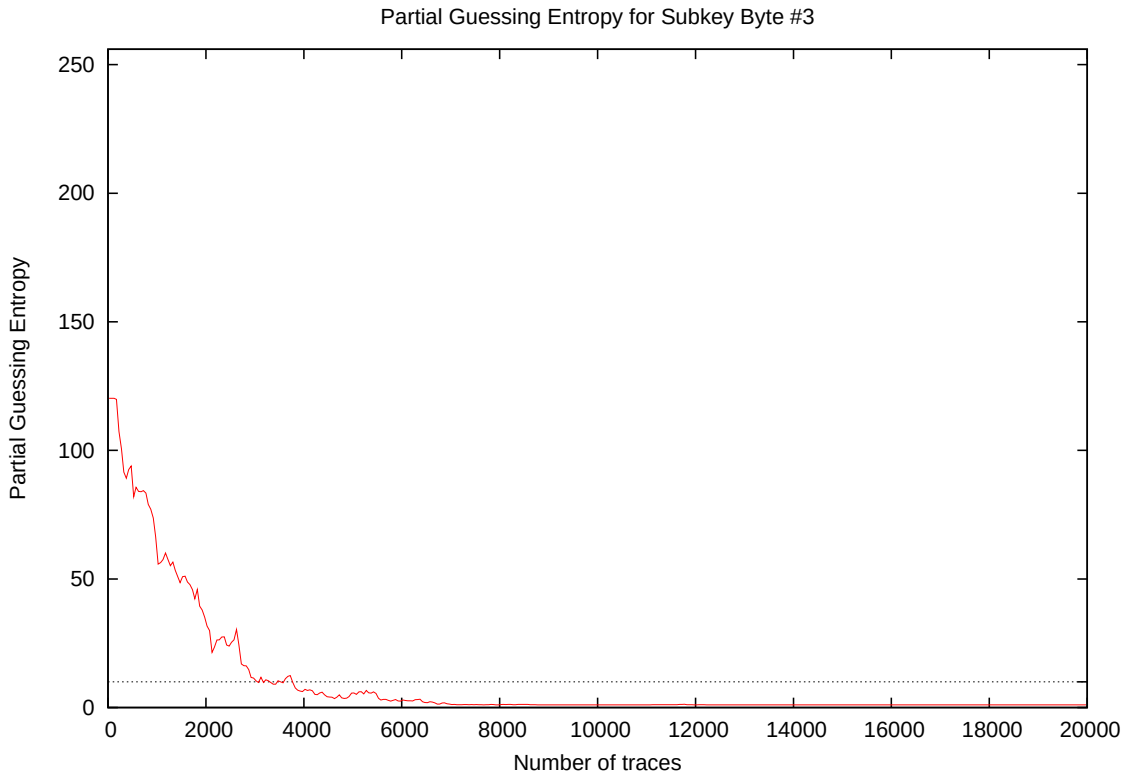

Partial Success Rate for Subkey Bytes #1 to #16
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000
01
02
03
04
05
06
07
08
09
10
11
12
13
14
15
16

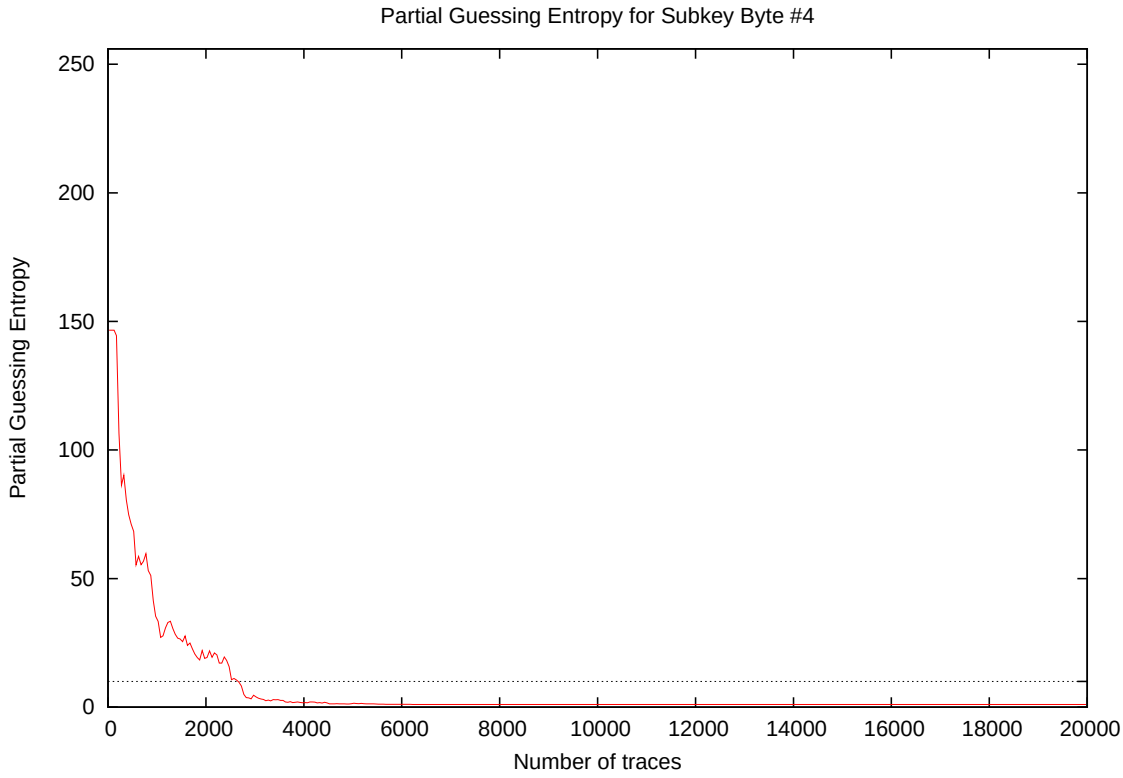
| Traces | Partial Success Rate / Byte | | | | | | | | | | | | | | | | Min | Max | Mean |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | | | |
| 10 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.03 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.03 | 0.00 |
| 20 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.03 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.03 | 0.00 |
| 30 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.03 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.03 | 0.00 |
| 40 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.03 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.03 | 0.00 |
| 50 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.03 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.03 | 0.00 |
| 100 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.03 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.03 | 0.00 |
| 200 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.03 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.03 | 0.00 |
| 300 | 0.00 | 0.06 | 0.00 | 0.06 | 0.06 | 0.00 | 0.00 | 0.03 | 0.00 | 0.00 | 0.00 | 0.03 | 0.03 | 0.00 | 0.00 | 0.00 | 0.00 | 0.06 | 0.02 |
| 400 | 0.00 | 0.06 | 0.03 | 0.03 | 0.09 | 0.06 | 0.03 | 0.00 | 0.00 | 0.00 | 0.00 | 0.06 | 0.03 | 0.00 | 0.00 | 0.06 | 0.00 | 0.09 | 0.03 |
| 500 | 0.09 | 0.06 | 0.03 | 0.03 | 0.06 | 0.09 | 0.09 | 0.03 | 0.06 | 0.03 | 0.00 | 0.09 | 0.00 | 0.00 | 0.03 | 0.06 | 0.00 | 0.09 | 0.05 |
| 1000 | 0.16 | 0.09 | 0.09 | 0.25 | 0.06 | 0.19 | 0.16 | 0.09 | 0.22 | 0.38 | 0.00 | 0.25 | 0.16 | 0.00 | 0.06 | 0.12 | 0.00 | 0.38 | 0.14 |
| 2000 | 0.38 | 0.19 | 0.28 | 0.44 | 0.25 | 0.56 | 0.50 | 0.34 | 0.31 | 0.81 | 0.19 | 0.66 | 0.41 | 0.19 | 0.16 | 0.41 | 0.16 | 0.81 | 0.38 |
| 3000 | 0.56 | 0.50 | 0.41 | 0.66 | 0.47 | 0.81 | 0.81 | 0.38 | 0.56 | 1.00 | 0.38 | 0.84 | 0.59 | 0.31 | 0.34 | 0.75 | 0.31 | 1.00 | 0.59 |
| 4000 | 0.62 | 0.72 | 0.47 | 0.84 | 0.56 | 0.97 | 1.00 | 0.59 | 0.66 | 1.00 | 0.53 | 1.00 | 0.88 | 0.62 | 0.41 | 0.81 | 0.41 | 1.00 | 0.73 |
| 5000 | 0.72 | 0.91 | 0.72 | 0.88 | 0.72 | 0.94 | 0.94 | 0.81 | 0.81 | 1.00 | 0.66 | 1.00 | 0.94 | 0.72 | 0.66 | 0.97 | 0.66 | 1.00 | 0.84 |
| 10000 | 0.94 | 1.00 | 1.00 | 1.00 | 0.94 | 1.00 | 1.00 | 0.97 | 0.94 | 1.00 | 0.97 | 1.00 | 1.00 | 0.91 | 0.94 | 1.00 | 0.91 | 1.00 | 0.97 |
| 15000 | 0.94 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 0.97 | 1.00 | 1.00 | 0.94 | 1.00 | 0.99 |
| 20000 | 0.97 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 0.97 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 0.97 | 1.00 | 1.00 |

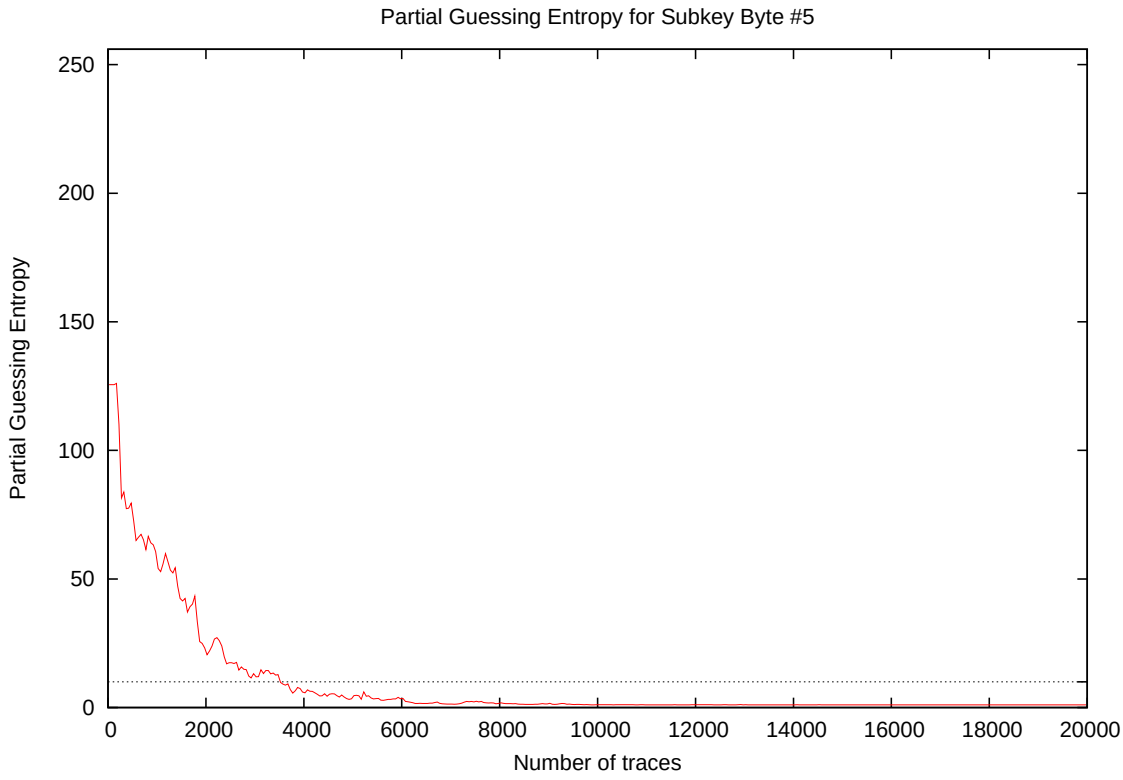
# 4 Partial Guessing Entropy

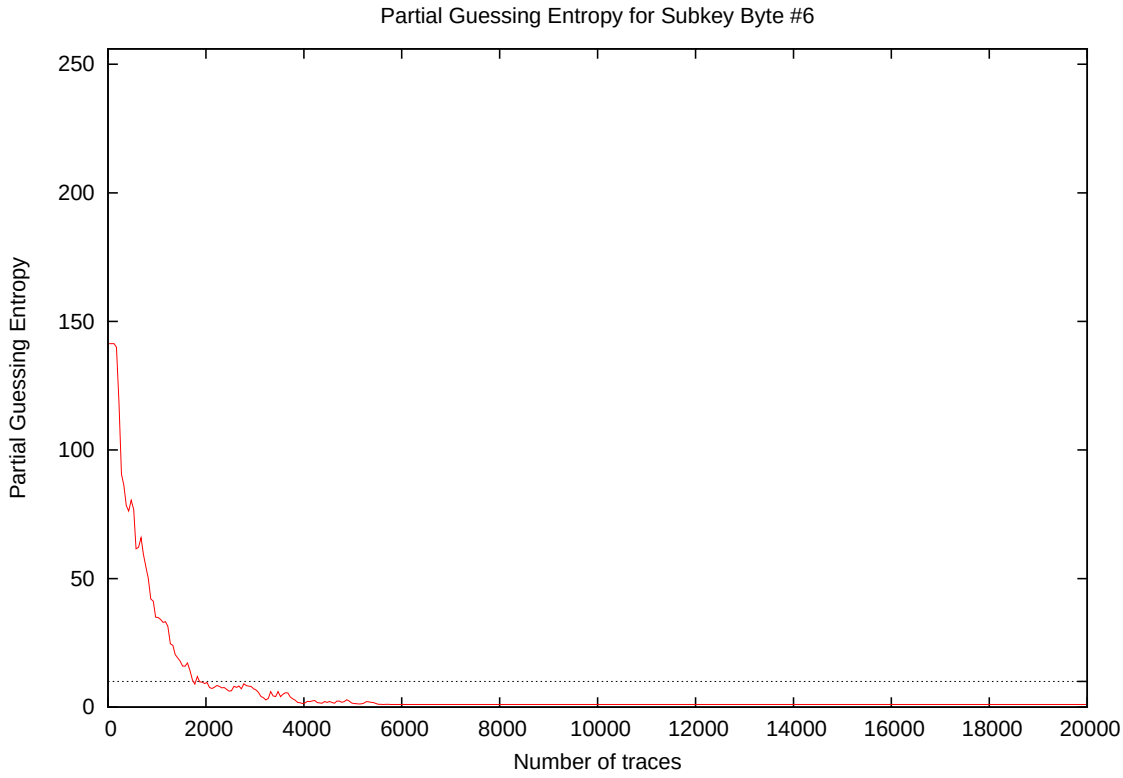


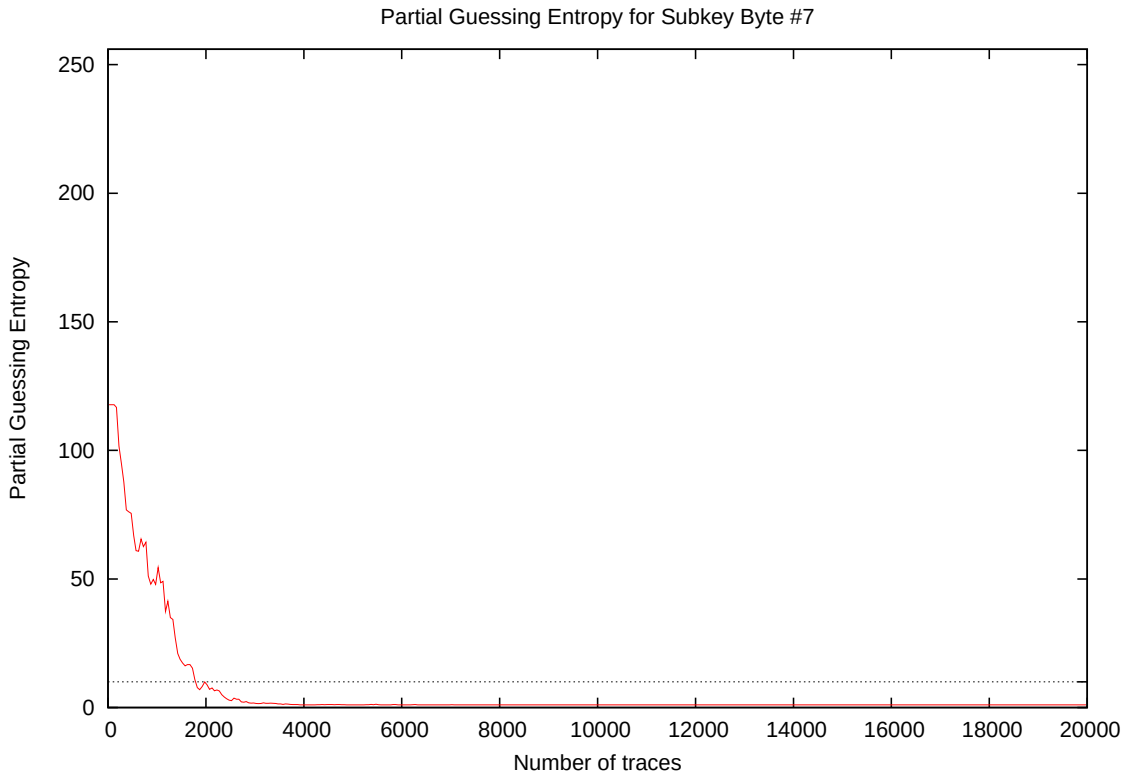



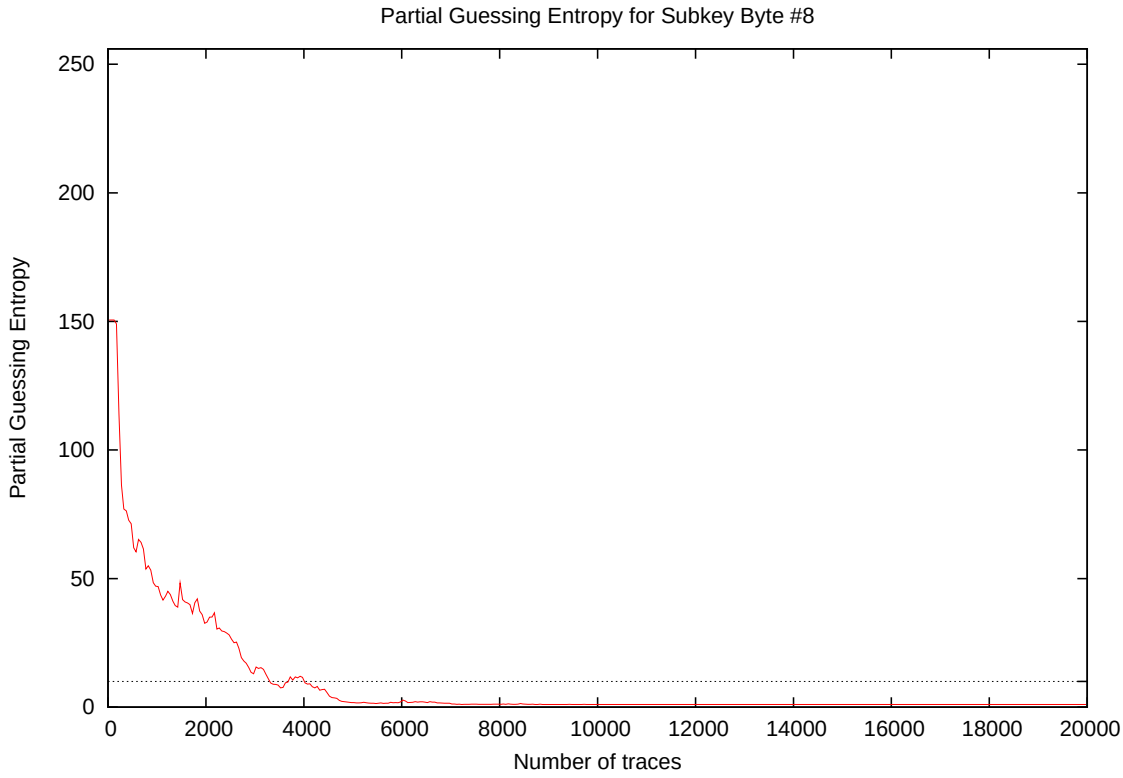

Partial Guessing Entropy for Subkey Byte #3
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000

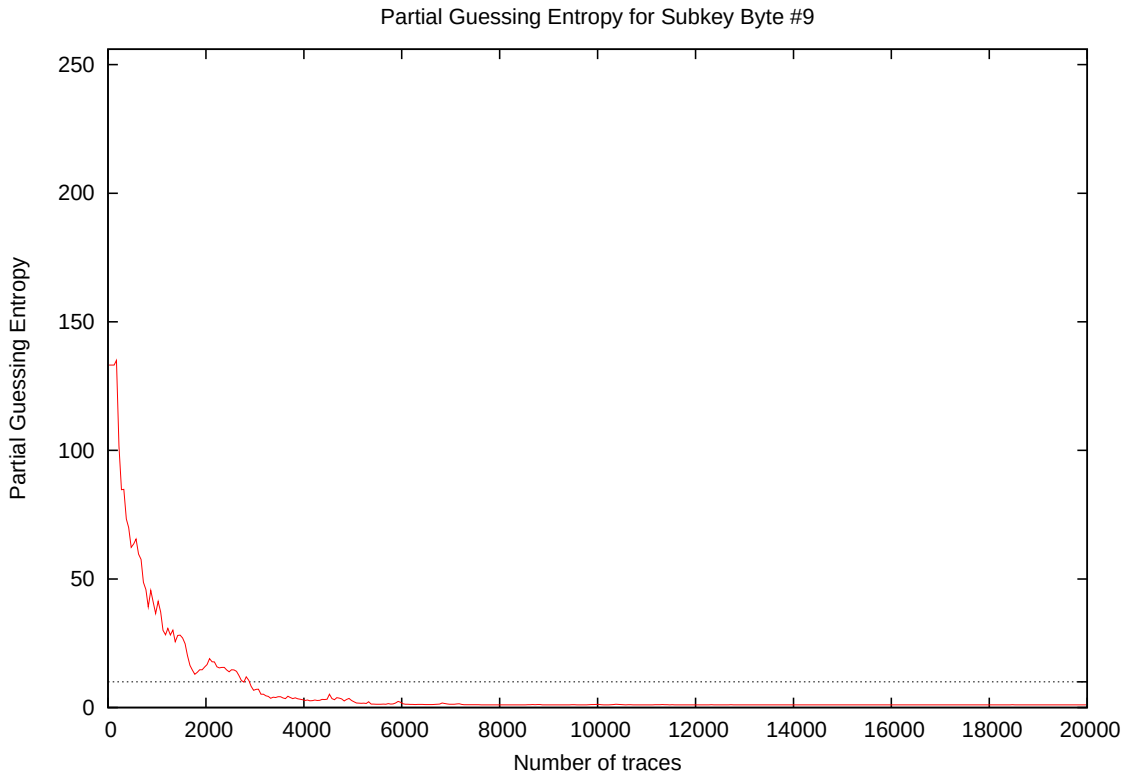

Partial Guessing Entropy for Subkey Byte #4
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000

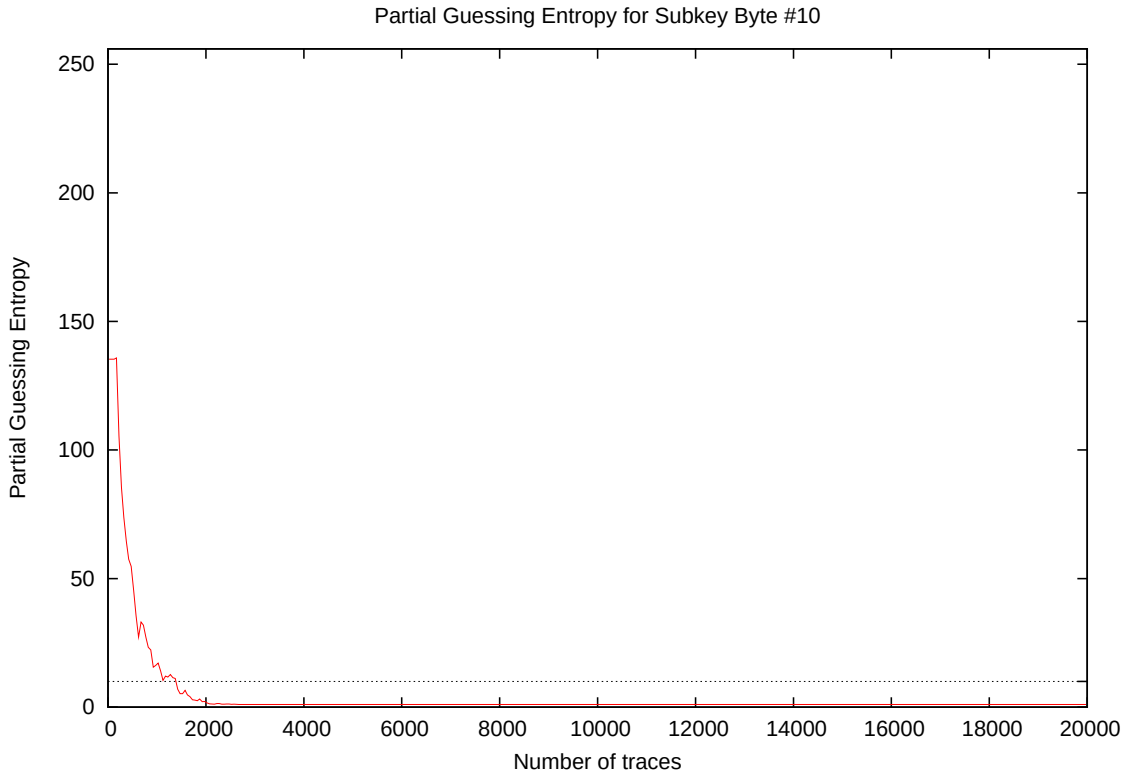

Partial Guessing Entropy for Subkey Byte #5
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000

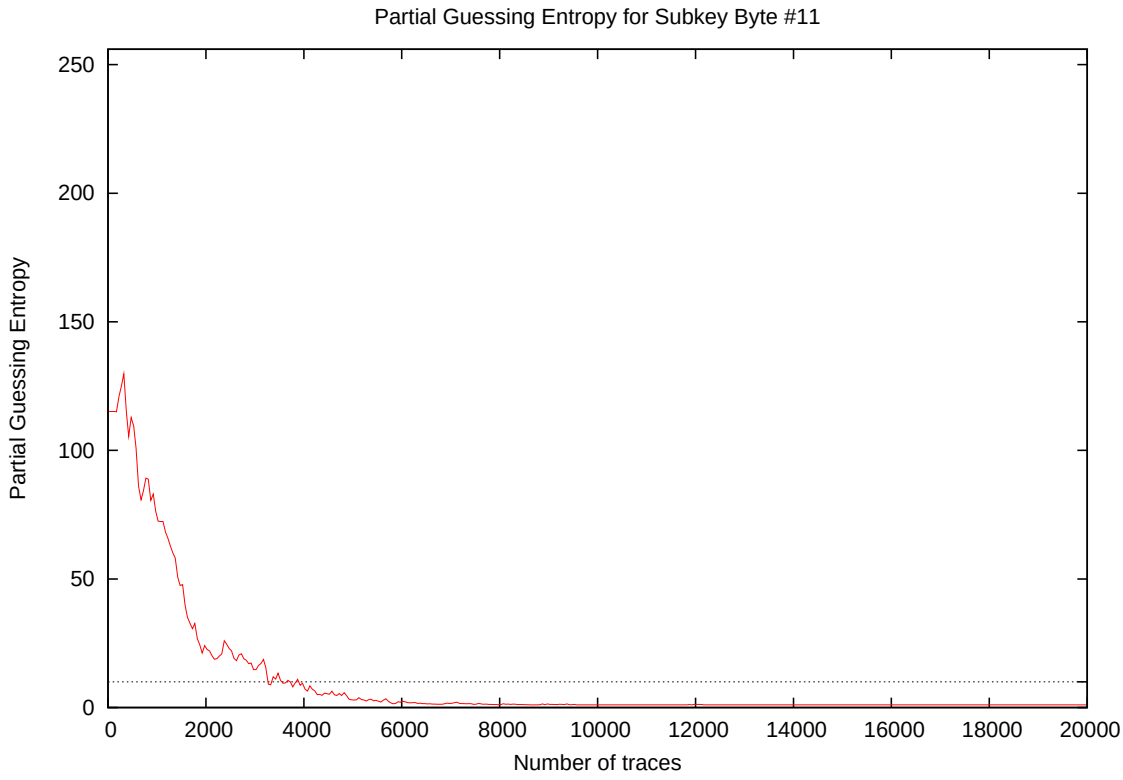

Partial Guessing Entropy for Subkey Byte #6
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000

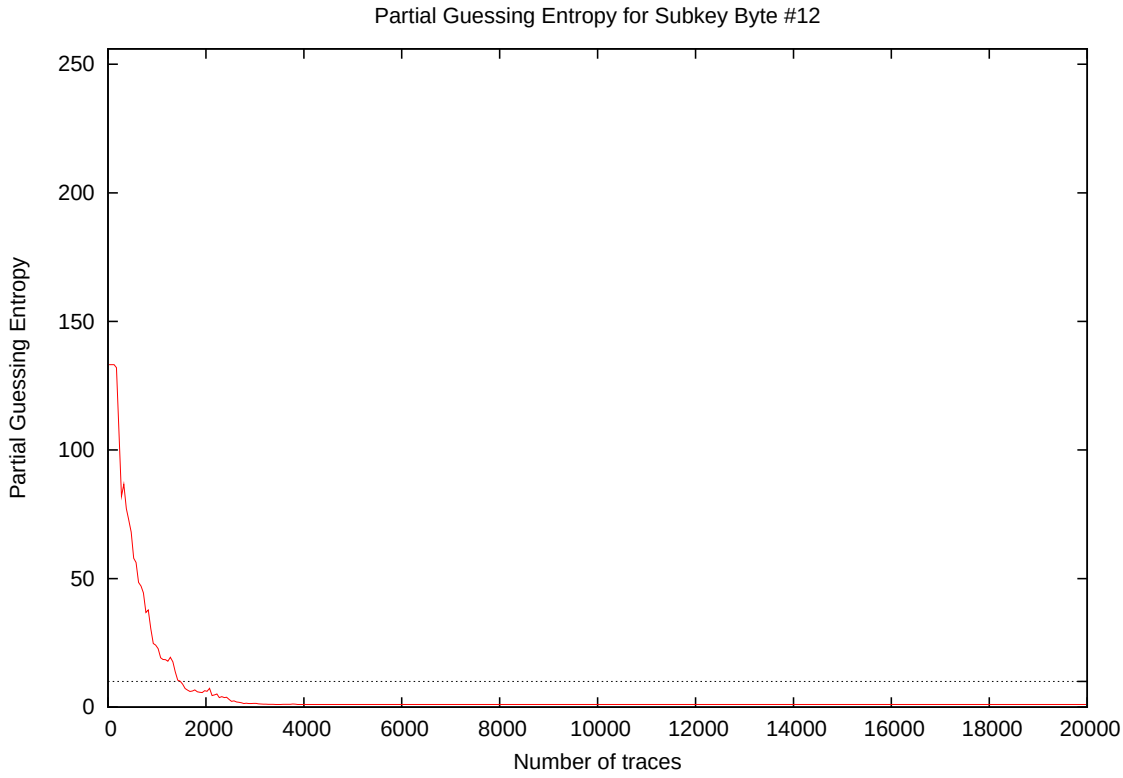

Partial Guessing Entropy for Subkey Byte #7
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000

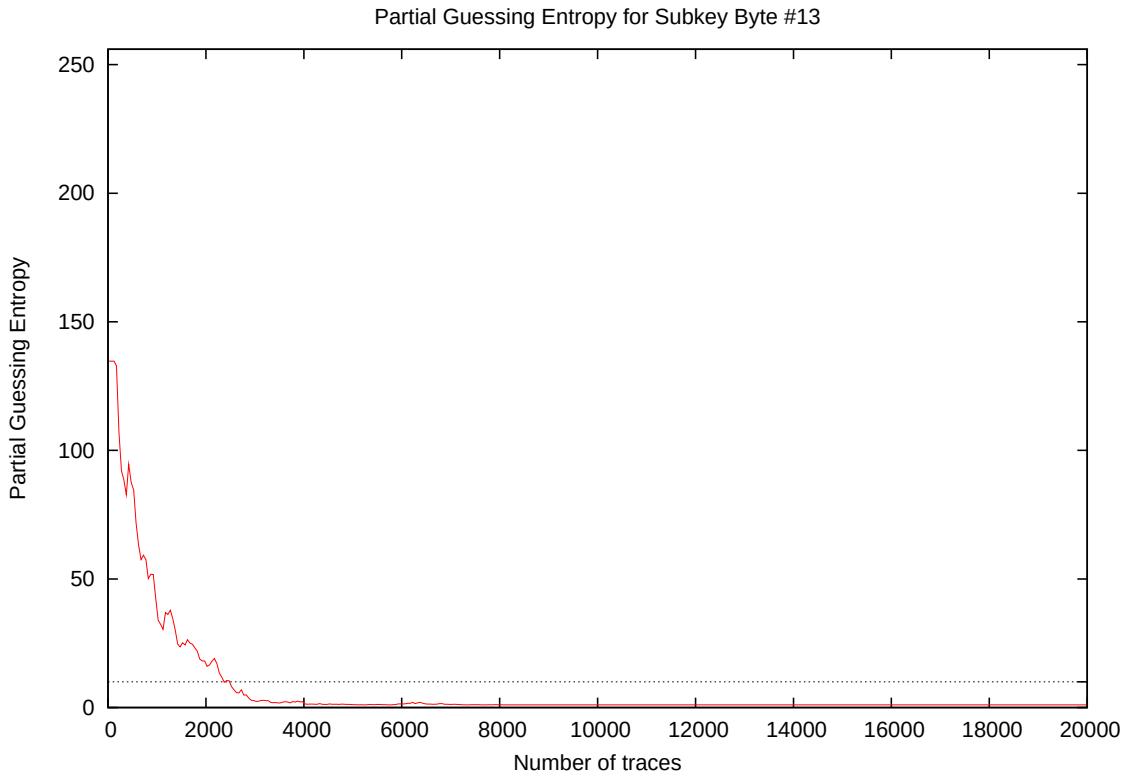

Partial Guessing Entropy for Subkey Byte #8
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000

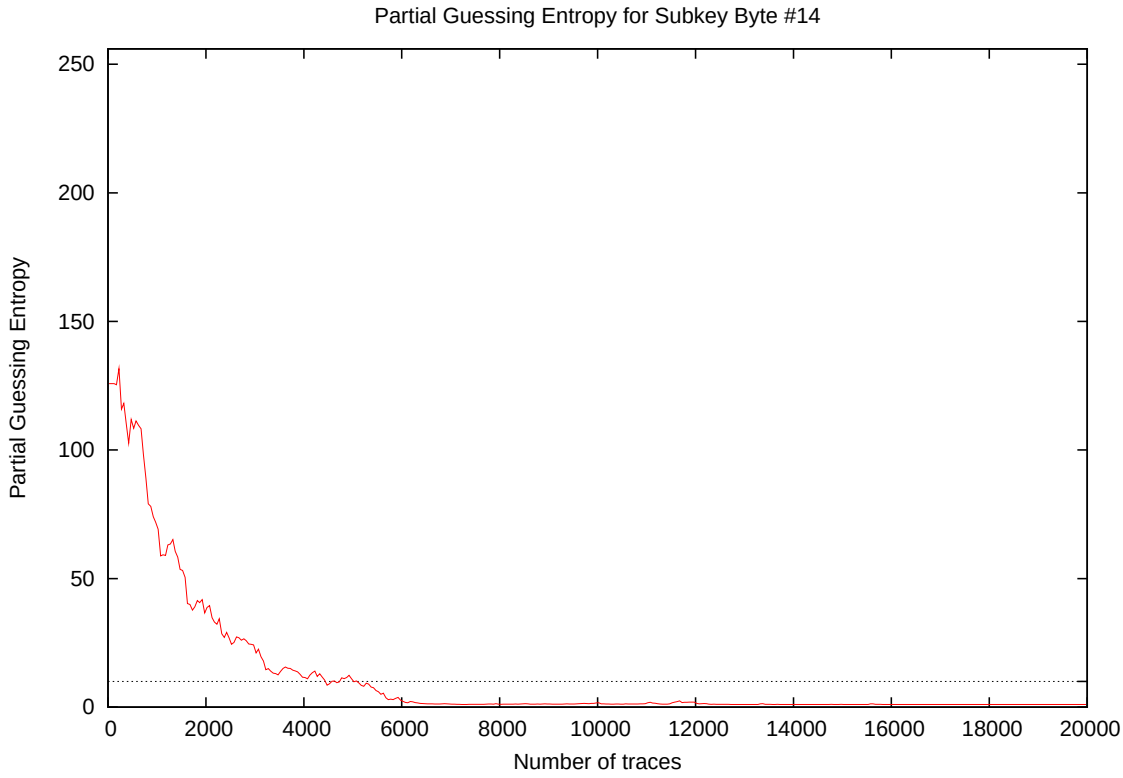

Partial Guessing Entropy for Subkey Byte #9
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000

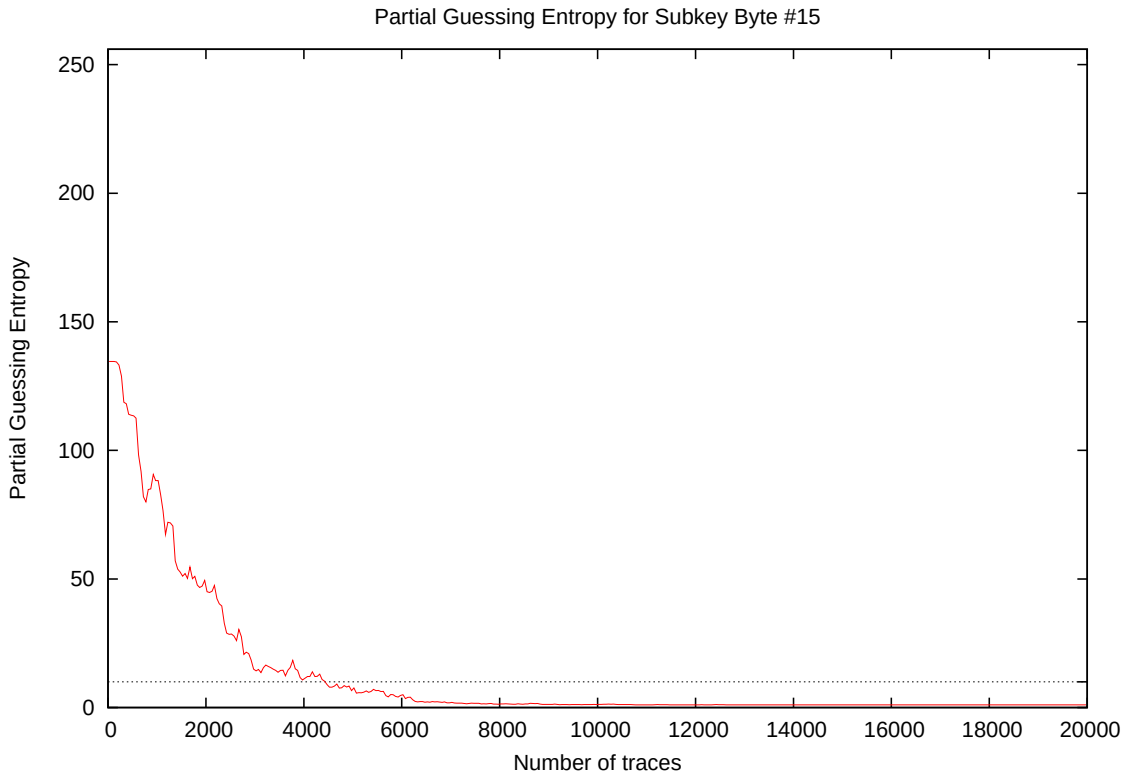

Partial Guessing Entropy for Subkey Byte #10
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000

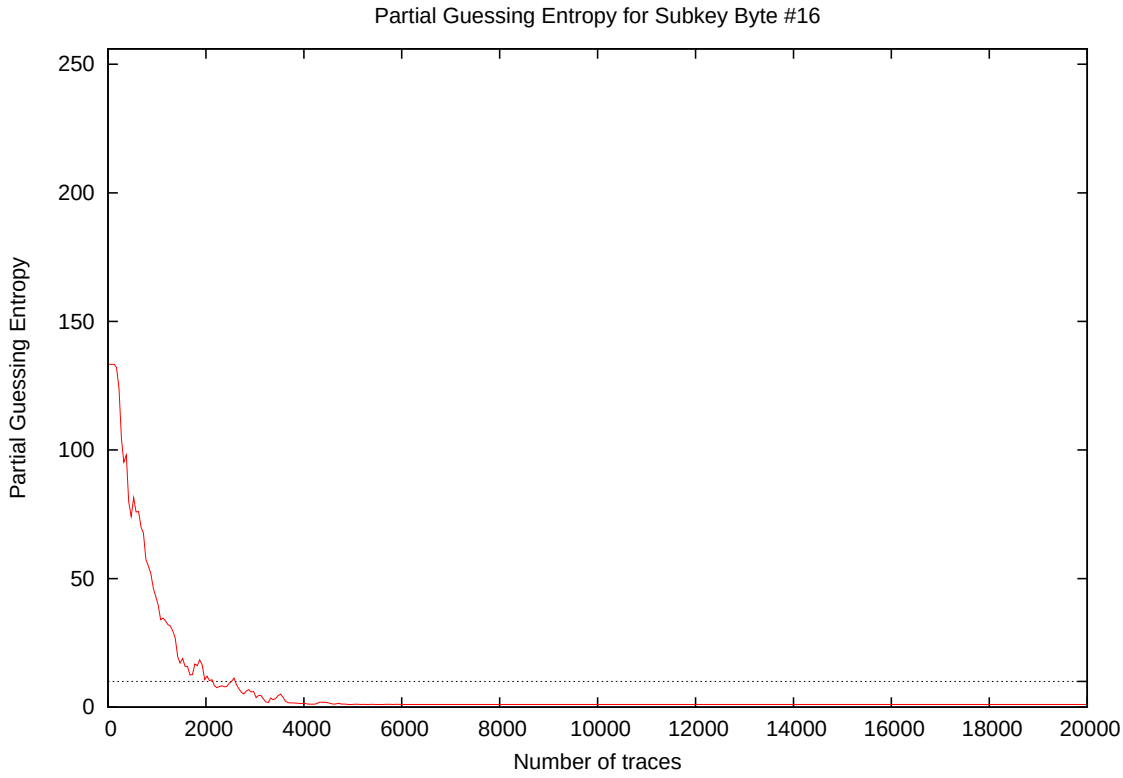

Partial Guessing Entropy for Subkey Byte #11
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000

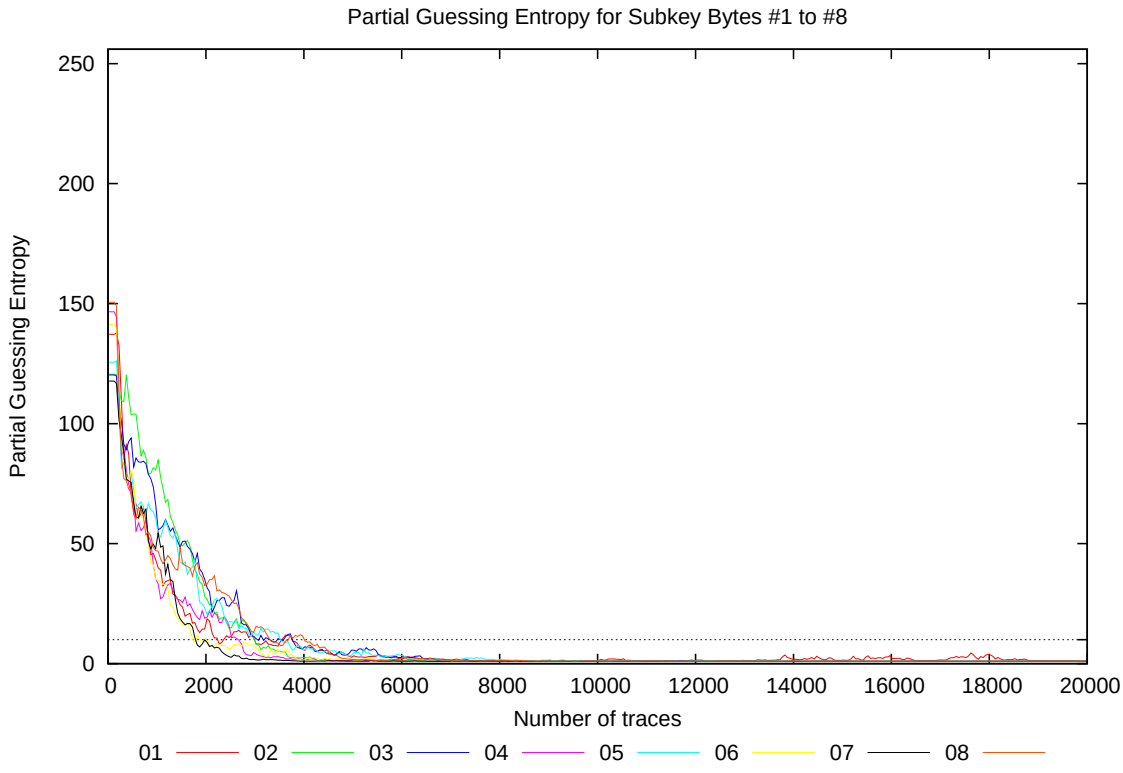

Partial Guessing Entropy for Subkey Byte #12
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000

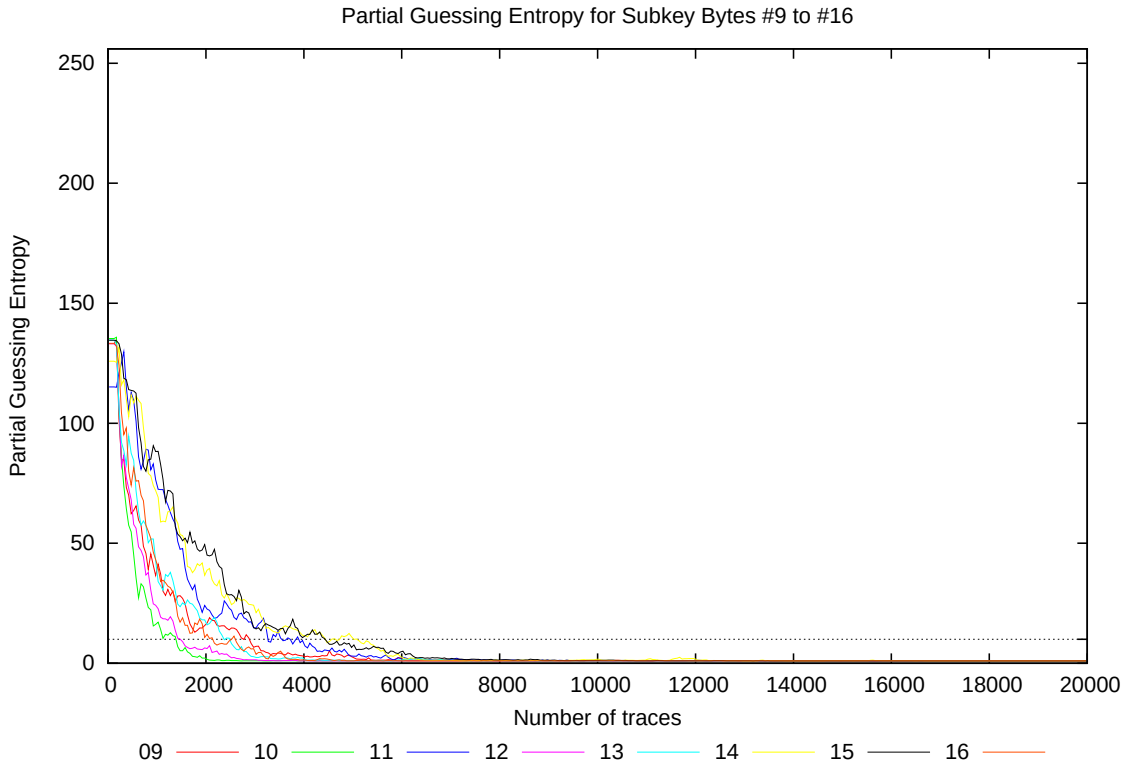

Partial Guessing Entropy for Subkey Byte #13
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000

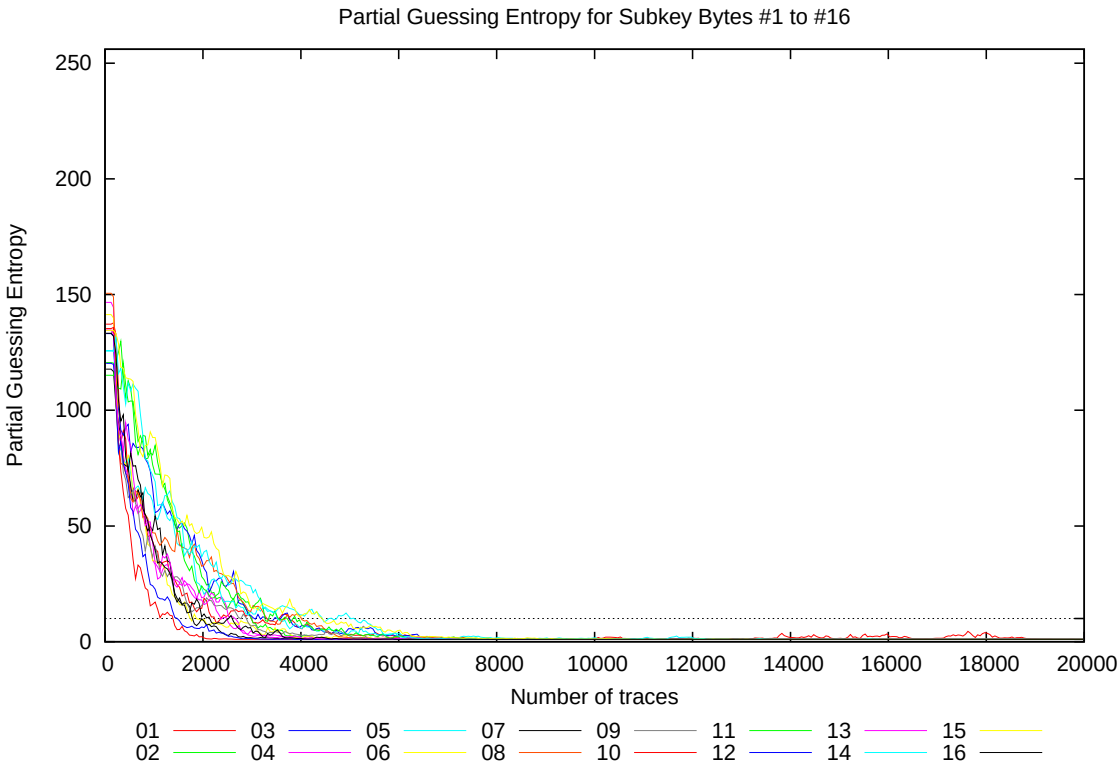

Partial Guessing Entropy for Subkey Byte #14
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000


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 | 137.2 | 120.6 | 120.3 | 146.6 | 125.6 | 141.3 | 117.8 | 150.6 | 133.2 | 135.3 | 115.2 | 133.2 | 134.7 | 125.8 | 134.6 | 133.3 | 115.2 | 150.6 | 131.6 |
| 20 | 137.2 | 120.6 | 120.3 | 146.6 | 125.6 | 141.3 | 117.8 | 150.6 | 133.2 | 135.3 | 115.2 | 133.2 | 134.7 | 125.8 | 134.6 | 133.3 | 115.2 | 150.6 | 131.6 |
| 30 | 137.2 | 120.6 | 120.3 | 146.6 | 125.6 | 141.3 | 117.8 | 150.6 | 133.2 | 135.3 | 115.2 | 133.2 | 134.7 | 125.8 | 134.6 | 133.3 | 115.2 | 150.6 | 131.6 |
| 40 | 137.2 | 120.6 | 120.3 | 146.6 | 125.6 | 141.3 | 117.8 | 150.6 | 133.2 | 135.3 | 115.2 | 133.2 | 134.7 | 125.8 | 134.6 | 133.3 | 115.2 | 150.6 | 131.6 |
| 50 | 137.2 | 120.6 | 120.3 | 146.6 | 125.6 | 141.3 | 117.8 | 150.6 | 133.2 | 135.3 | 115.2 | 133.2 | 134.7 | 125.8 | 134.6 | 133.3 | 115.2 | 150.6 | 131.6 |
| 100 | 137.2 | 120.6 | 120.3 | 146.6 | 125.6 | 141.3 | 117.8 | 150.6 | 133.2 | 135.3 | 115.2 | 133.2 | 134.7 | 125.8 | 134.6 | 133.3 | 115.2 | 150.6 | 131.6 |
| 200 | 140.6 | 120.2 | 120.4 | 134.4 | 128.7 | 135.8 | 110.6 | 145.0 | 140.8 | 138.7 | 111.0 | 126.9 | 127.2 | 125.3 | 133.4 | 128.9 | 110.6 | 145.0 | 129.3 |
| 300 | 80.9 | 109.3 | 97.8 | 94.5 | 88.9 | 93.4 | 92.5 | 78.0 | 87.0 | 100.0 | 128.4 | 85.8 | 99.1 | 111.2 | 122.5 | 101.6 | 78.0 | 128.4 | 98.2 |
| 400 | 94.8 | 122.0 | 89.9 | 70.0 | 77.2 | 89.2 | 73.4 | 72.7 | 72.2 | 64.8 | 110.3 | 70.4 | 90.1 | 101.4 | 118.9 | 85.2 | 64.8 | 122.0 | 87.7 |
| 500 | 66.1 | 99.9 | 80.4 | 80.4 | 77.4 | 82.3 | 77.8 | 62.8 | 65.6 | 47.6 | 104.2 | 64.5 | 89.8 | 118.3 | 117.2 | 81.8 | 47.6 | 118.3 | 82.2 |
| 1000 | 42.9 | 78.6 | 61.0 | 31.7 | 46.3 | 33.4 | 47.6 | 41.0 | 39.6 | 16.3 | 78.5 | 26.0 | 32.8 | 68.2 | 84.8 | 39.6 | 16.3 | 84.8 | 48.0 |
| 2000 | 15.4 | 26.9 | 34.2 | 17.6 | 21.7 | 9.5 | 9.6 | 30.2 | 14.1 | 1.8 | 23.7 | 5.5 | 17.6 | 35.9 | 51.4 | 11.2 | 1.8 | 51.4 | 20.4 |
| 3000 | 8.9 | 9.2 | 13.0 | 5.5 | 14.2 | 5.8 | 1.6 | 12.4 | 6.8 | 1.0 | 13.2 | 1.3 | 2.3 | 19.6 | 14.4 | 4.7 | 1.0 | 19.6 | 8.4 |
| 4000 | 5.6 | 2.3 | 5.7 | 1.7 | 6.7 | 1.6 | 1.0 | 12.6 | 3.0 | 1.0 | 8.4 | 1.0 | 2.2 | 10.6 | 12.5 | 1.4 | 1.0 | 12.6 | 4.8 |
| 5000 | 2.7 | 1.3 | 6.5 | 1.4 | 3.7 | 1.5 | 1.1 | 1.8 | 2.2 | 1.0 | 3.0 | 1.0 | 1.1 | 10.1 | 6.9 | 1.0 | 1.0 | 10.1 | 2.9 |
| 10000 | 1.2 | 1.0 | 1.0 | 1.0 | 1.1 | 1.0 | 1.0 | 1.0 | 1.2 | 1.0 | 1.0 | 1.0 | 1.0 | 4.2 | 1.1 | 1.0 | 1.0 | 4.2 | 1.2 |
| 15000 | 1.4 | 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 | 1.4 | 1.0 |
| 20000 | 1.2 | 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 | 1.2 | 1.0 |