# Evaluation results

DPA contest v2

September 2010

## 1 Introduction

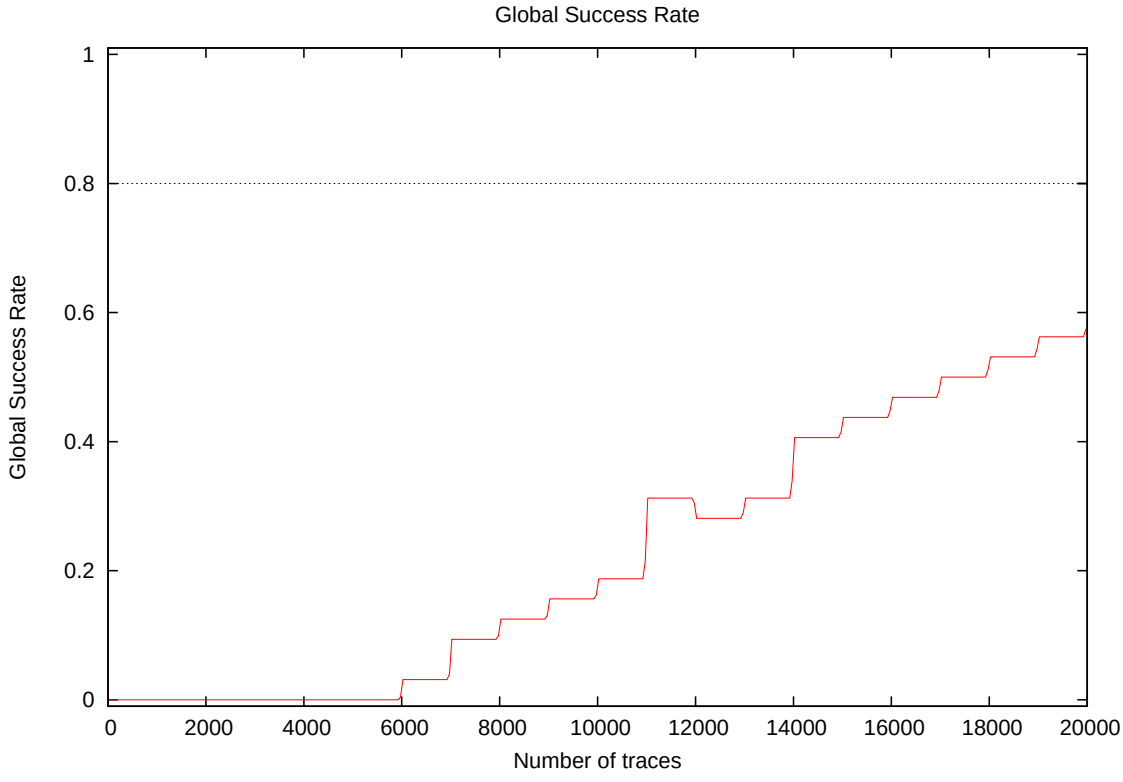
### 1.1 About the attack

- **Sender/Team:** Edgar Mateos
- **Institution:** Electrical and Computer Engineering Department, University of Waterloo
- **Language:** Matlab
- **Attacked subkey:** 10

### 1.2 About the evaluation

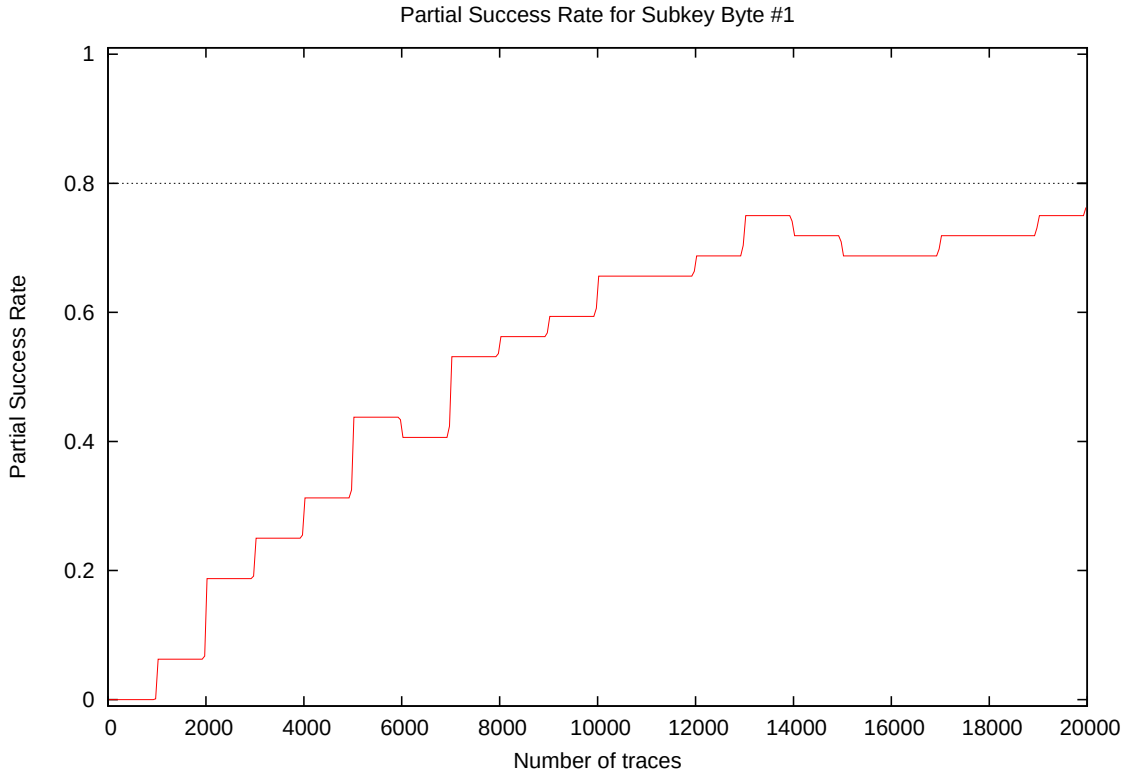
- **Date of evaluation:** August 2010

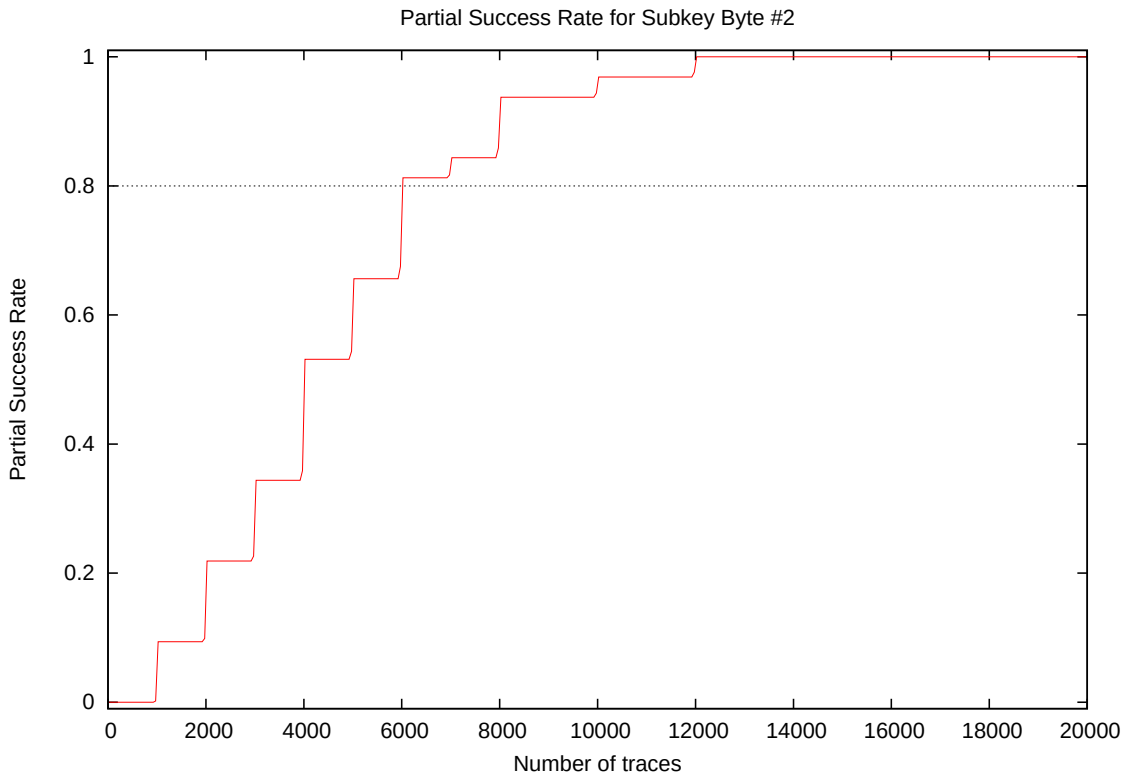
## 2 Global Success Rate

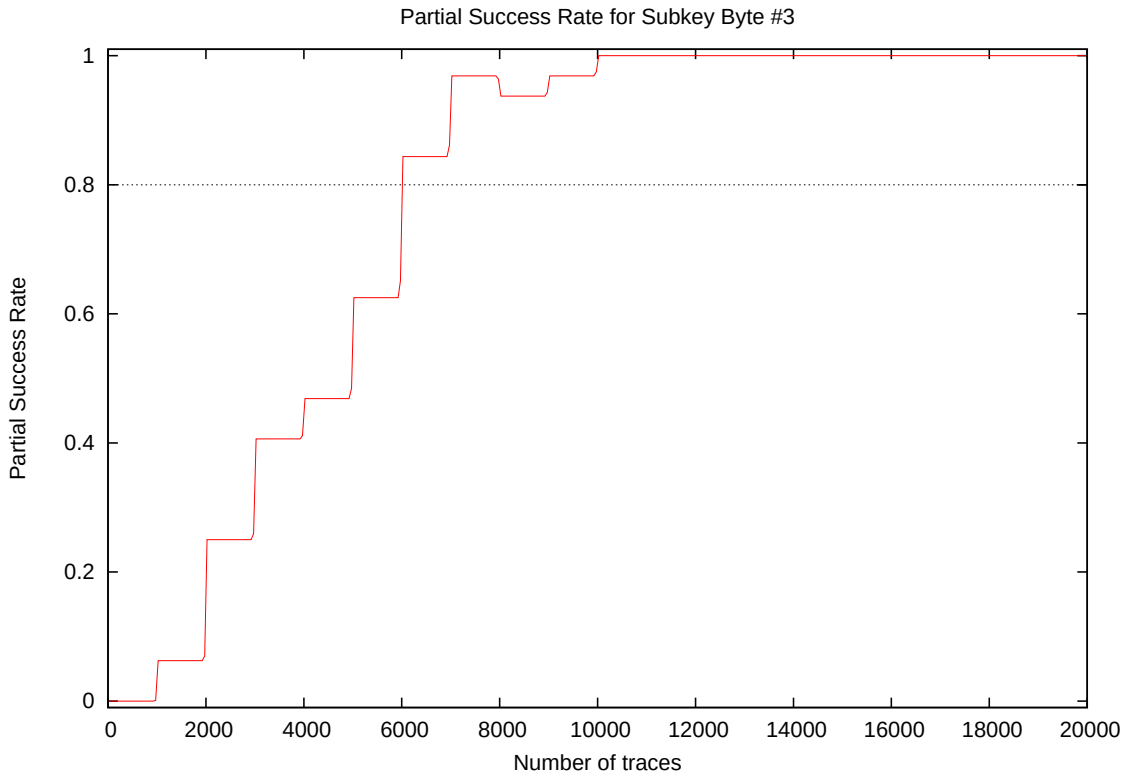


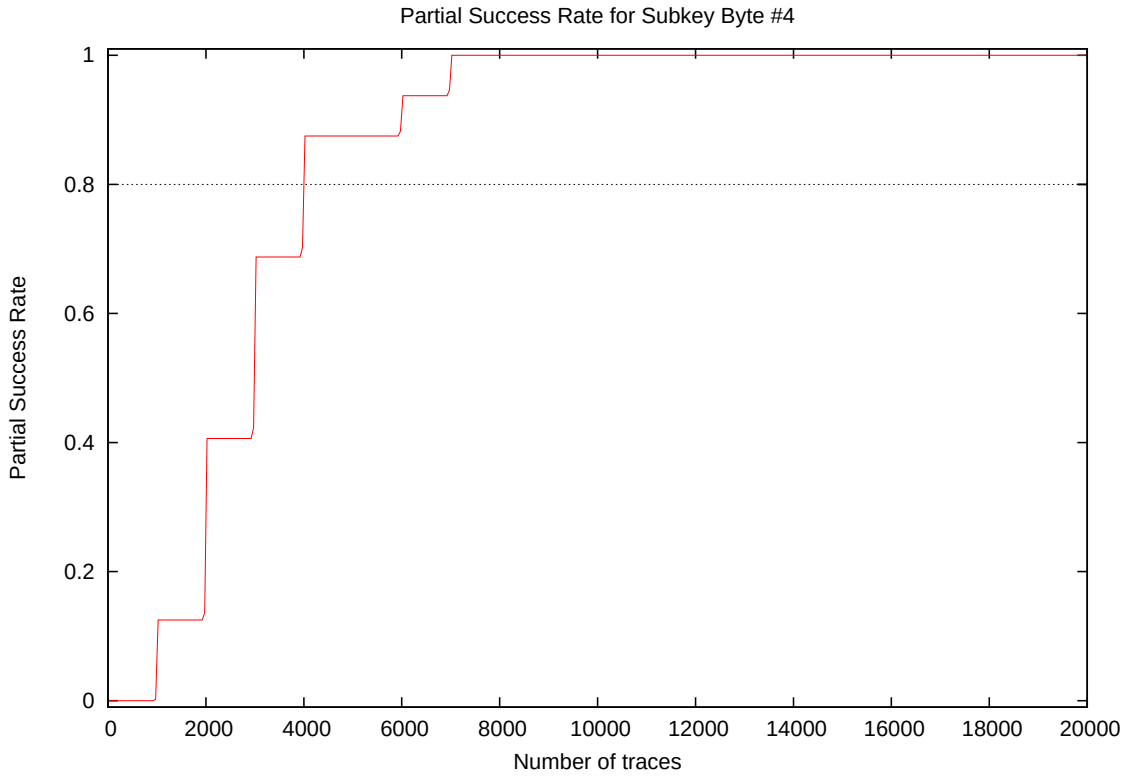
| Number of traces | Global Success Rate |
|---|---|
| 10 | 0.00 |
| 20 | 0.00 |
| 30 | 0.00 |
| 40 | 0.00 |
| 50 | 0.00 |
| 100 | 0.00 |
| 200 | 0.00 |
| 300 | 0.00 |
| 400 | 0.00 |
| 500 | 0.00 |
| 1000 | 0.00 |
| 2000 | 0.00 |
| 3000 | 0.00 |
| 4000 | 0.00 |
| 5000 | 0.00 |
| 10000 | 0.19 |
| 15000 | 0.44 |
| 20000 | 0.59 |

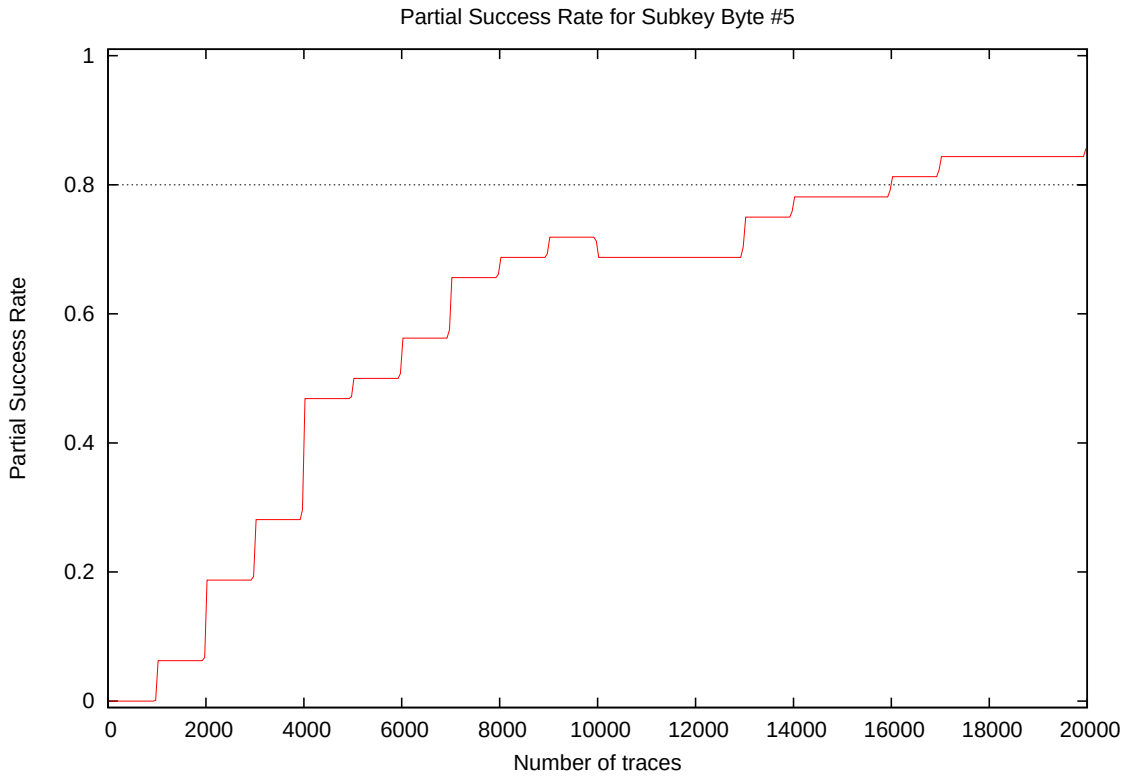
# 3 Partial Success Rate

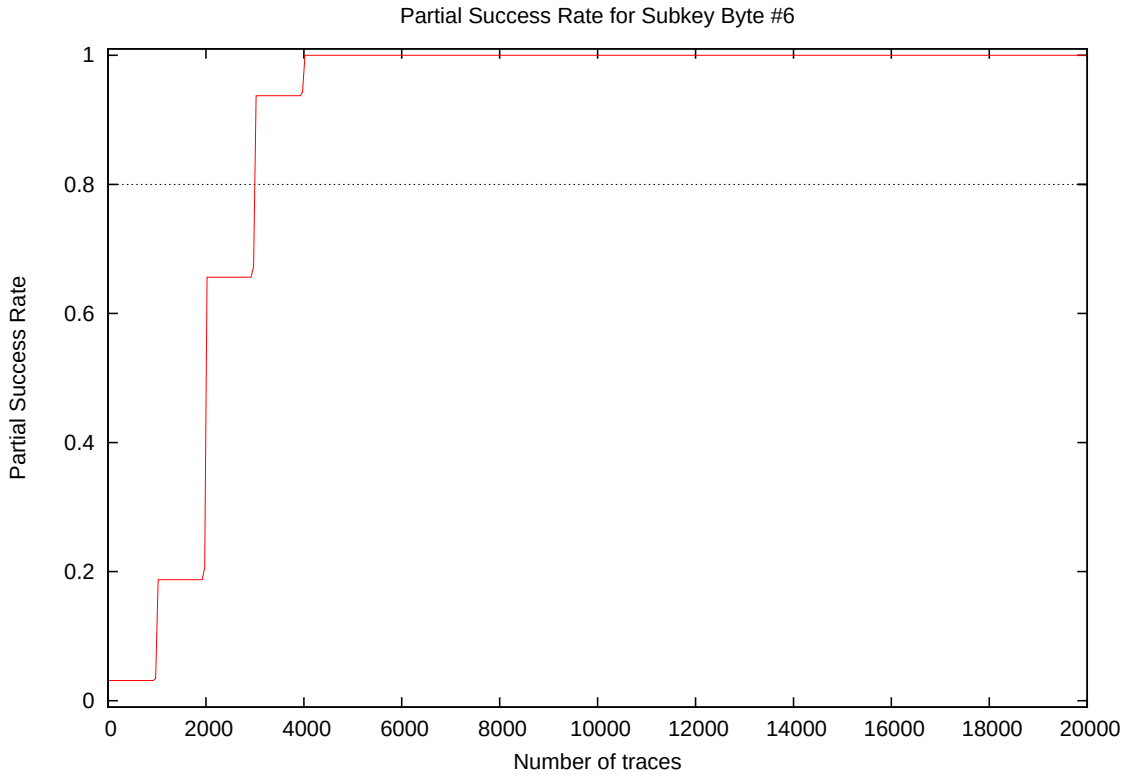


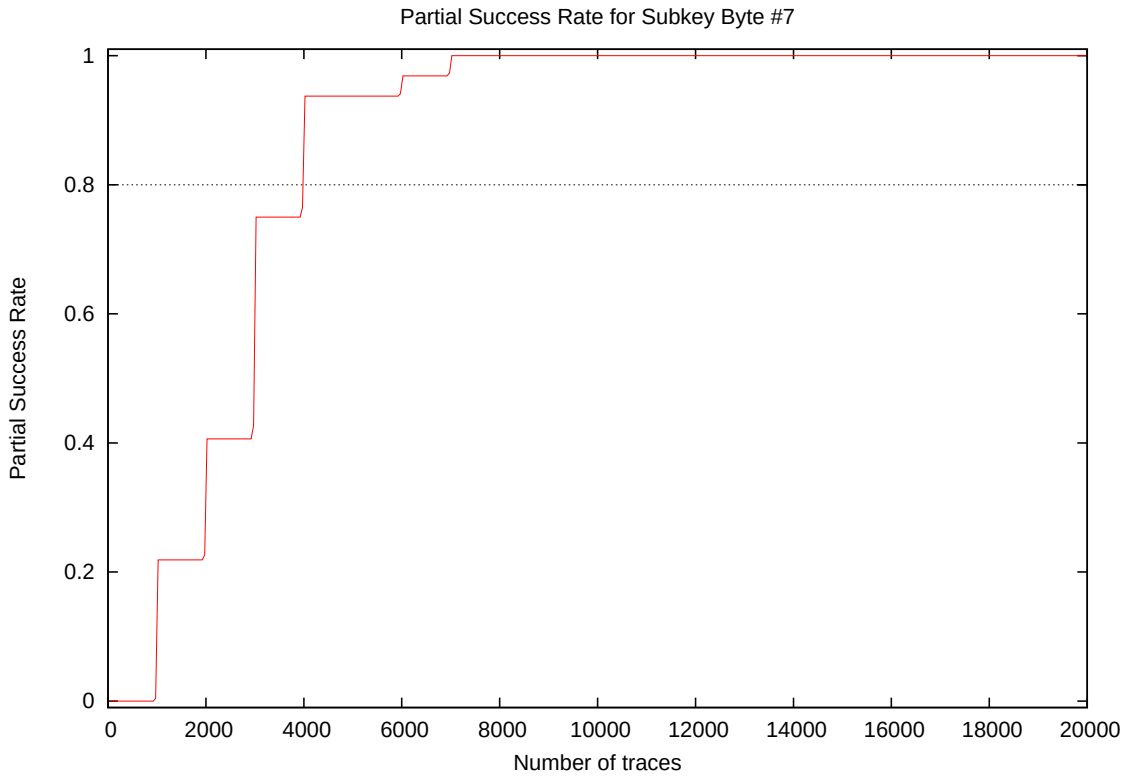



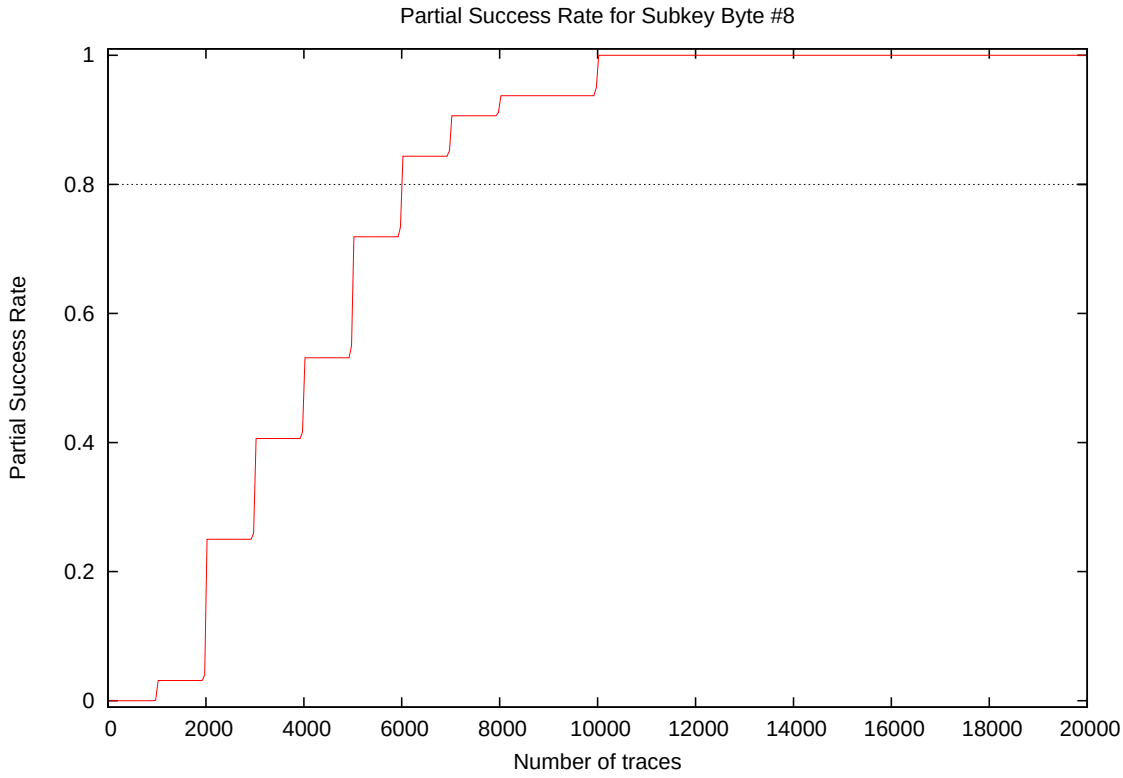

Partial Success Rate for Subkey Byte #3
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000

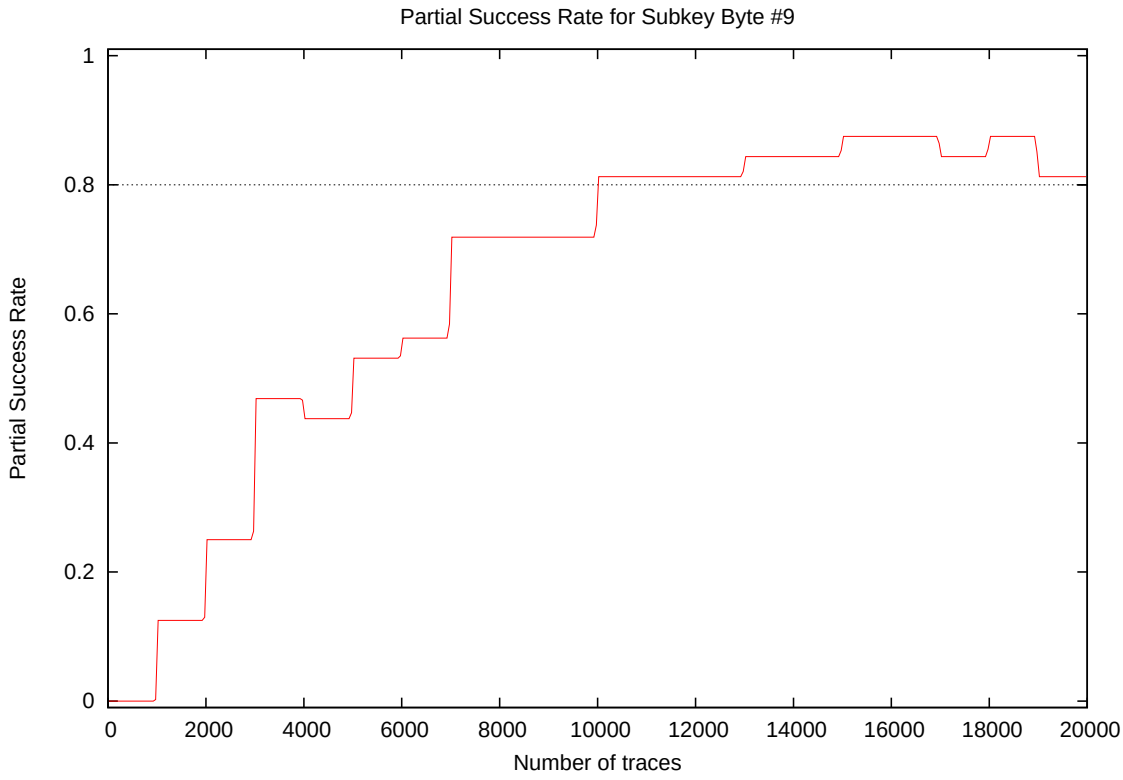

Partial Success Rate for Subkey Byte #4
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000

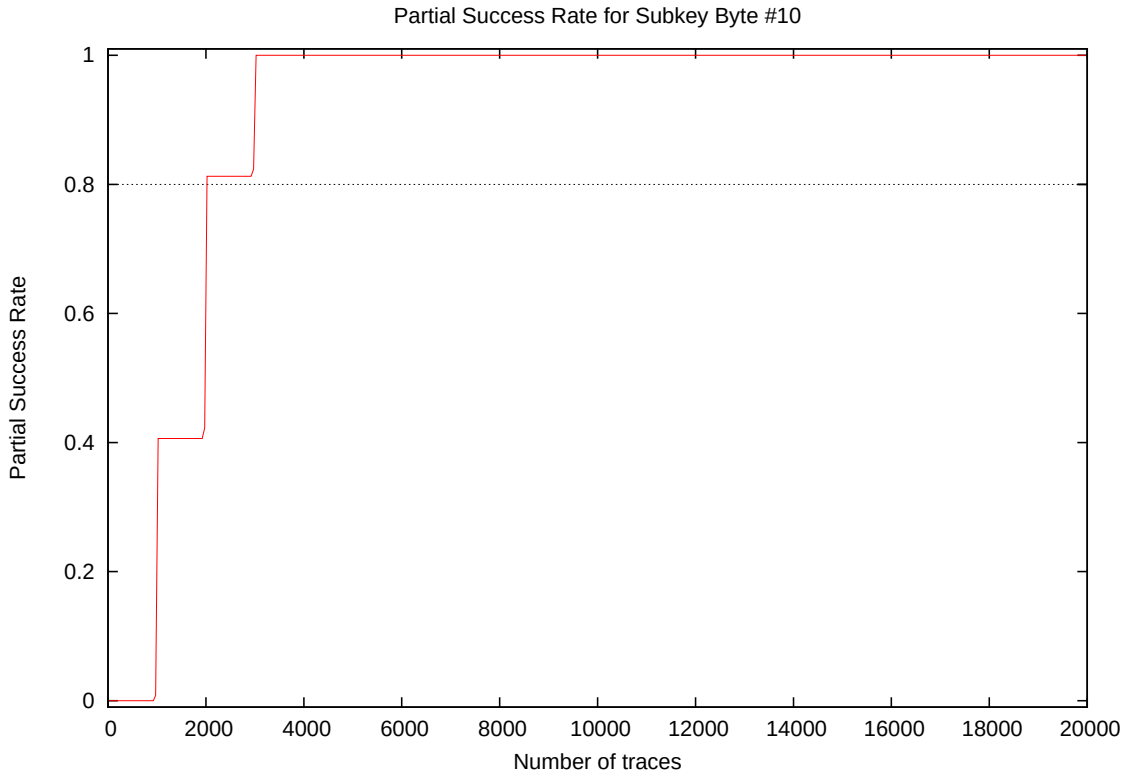

Partial Success Rate for Subkey Byte #5
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000

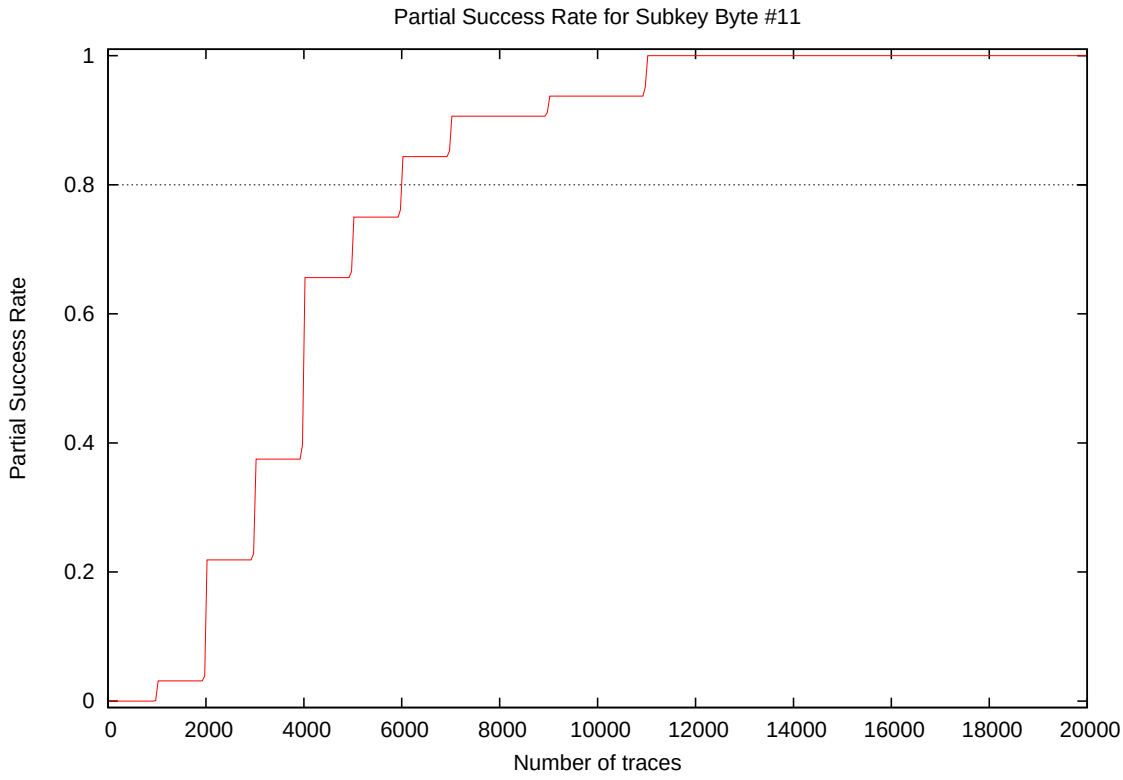

Partial Success Rate for Subkey Byte #6
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000

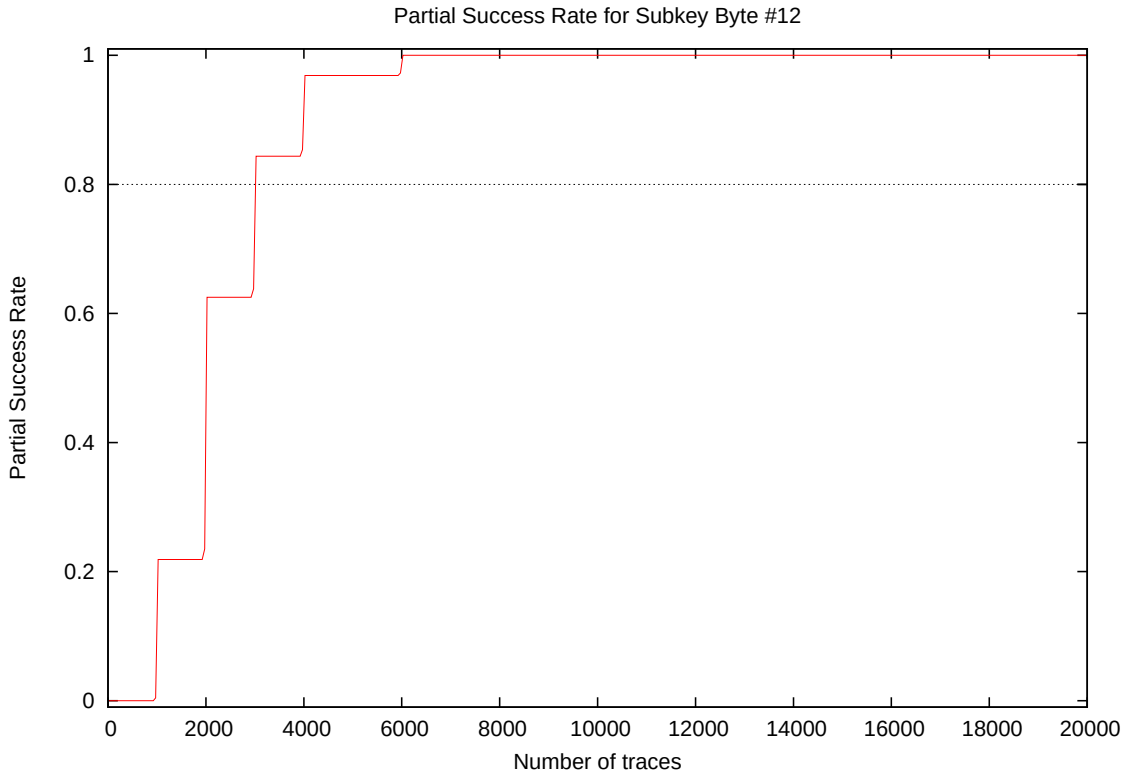

Partial Success Rate for Subkey Byte #7
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000

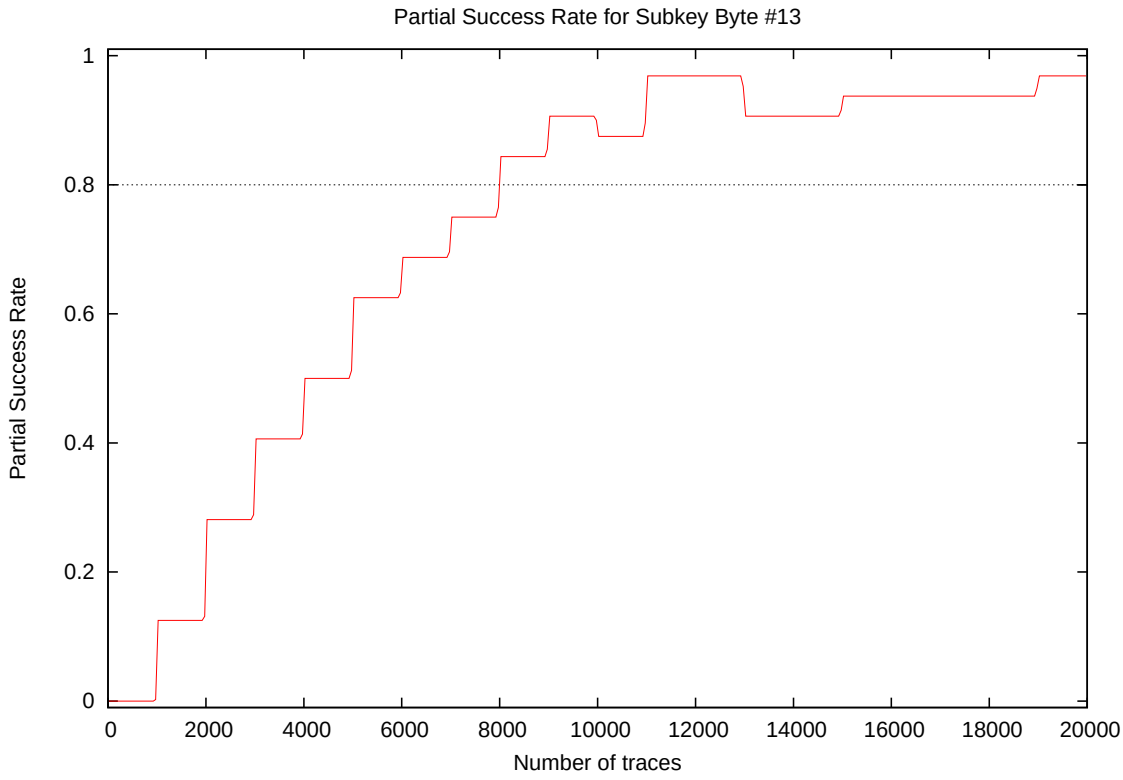

Partial Success Rate for Subkey Byte #8
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000

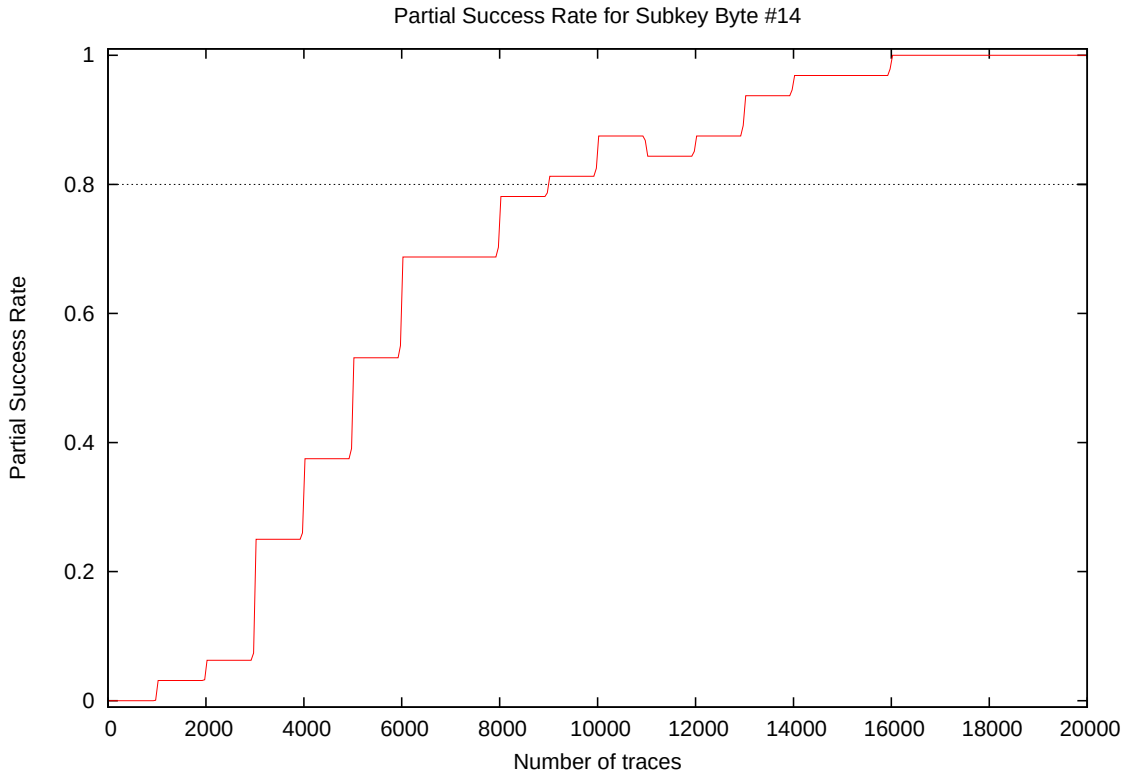

Partial Success Rate for Subkey Byte #9
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000

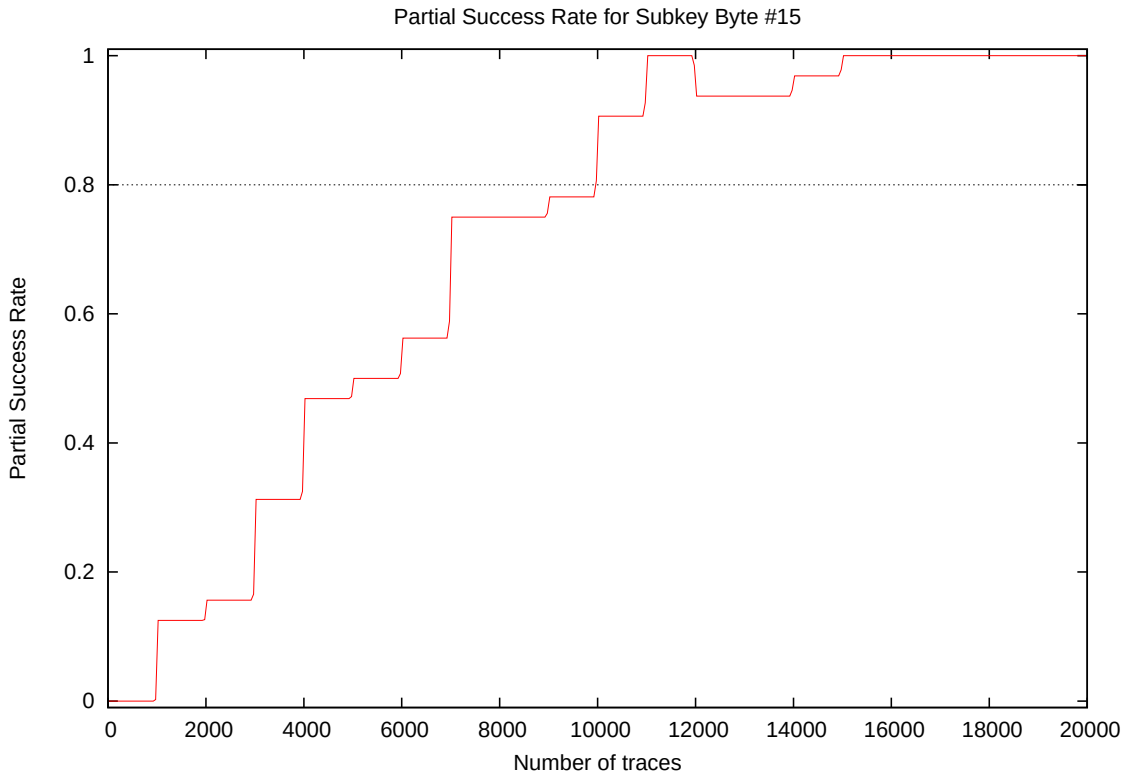

Partial Success Rate for Subkey Byte #10
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000

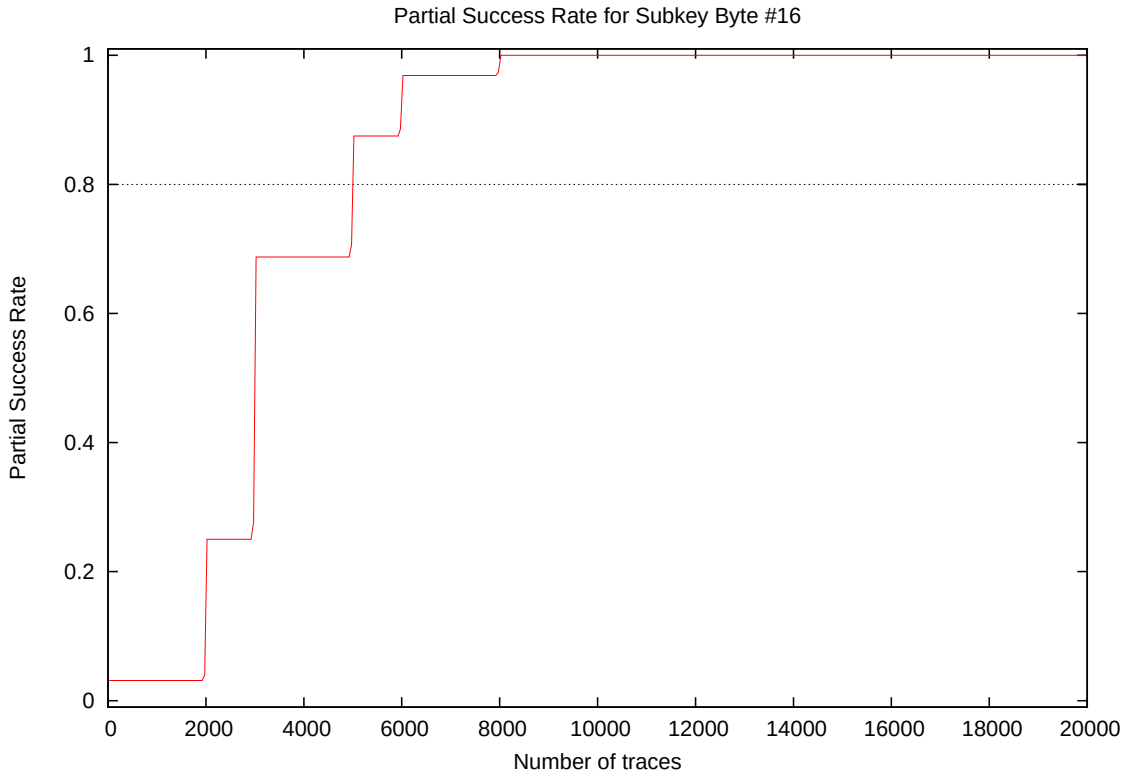

Partial Success Rate for Subkey Byte #11
Partial Success Rate
1
0.8
0.6
0.4
0.2
0
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000
Number of traces

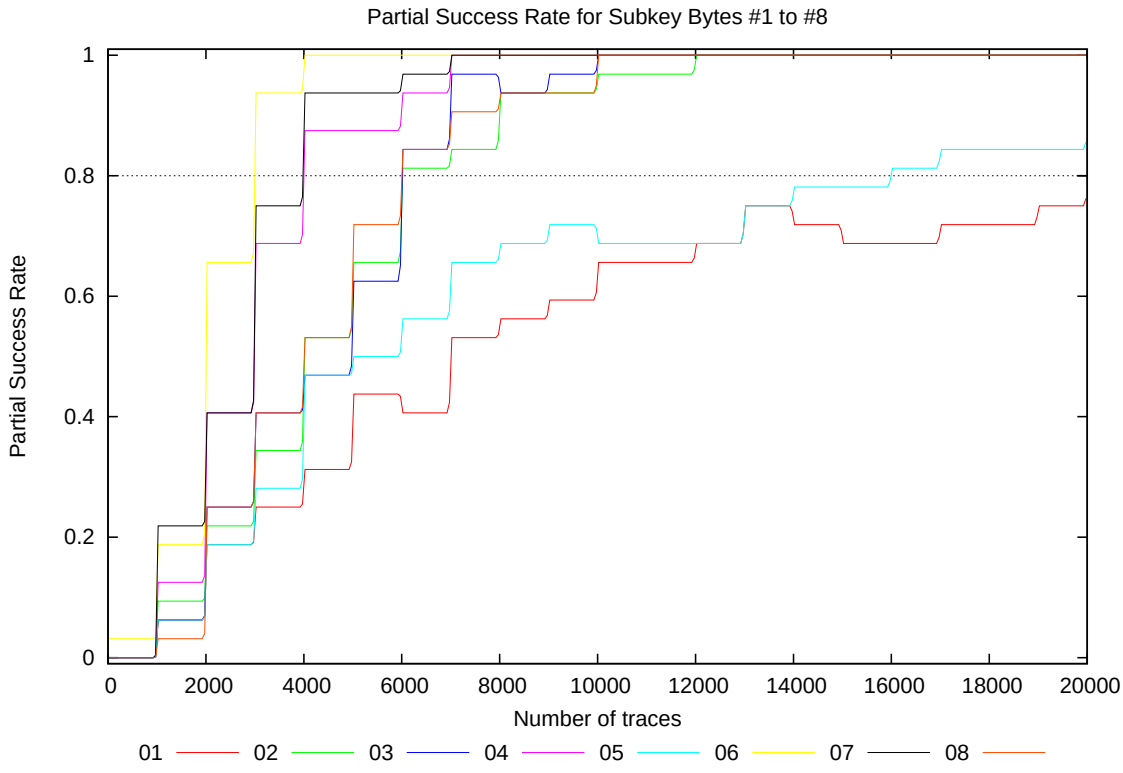

Partial Success Rate for Subkey Byte #12
Partial Success Rate
1
0.8
0.6
0.4
0.2
0
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000
Number of traces

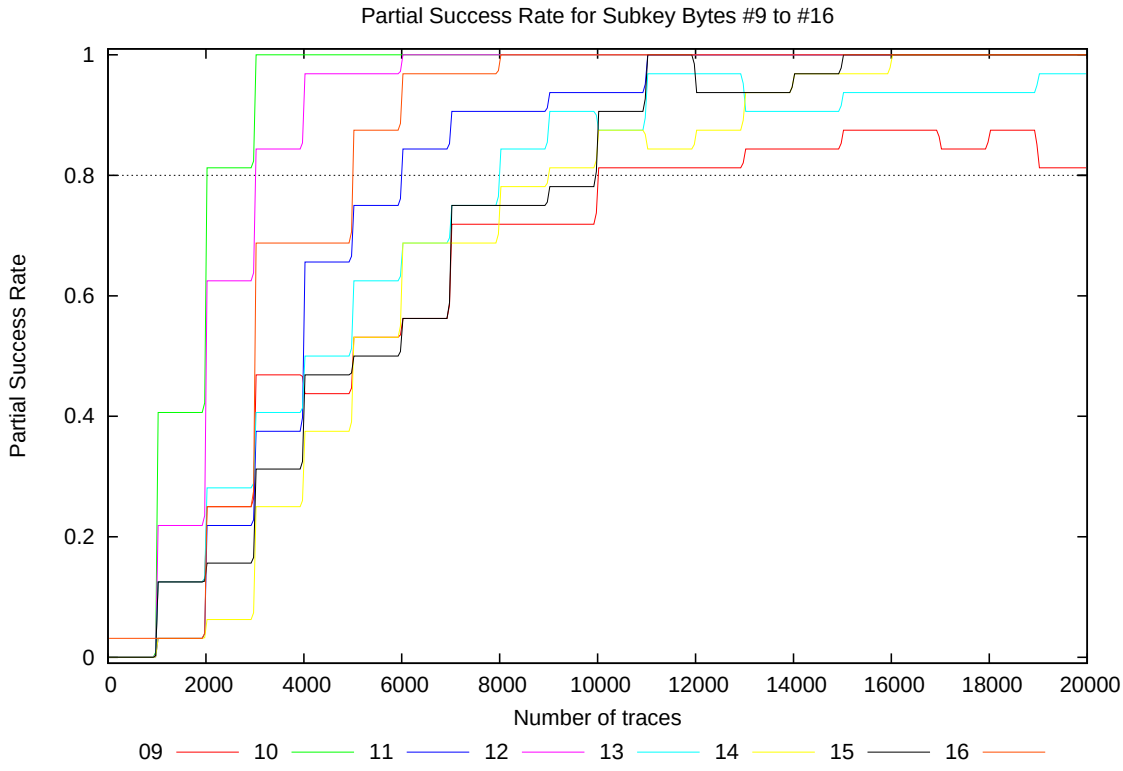

Partial Success Rate for Subkey Byte #13
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000

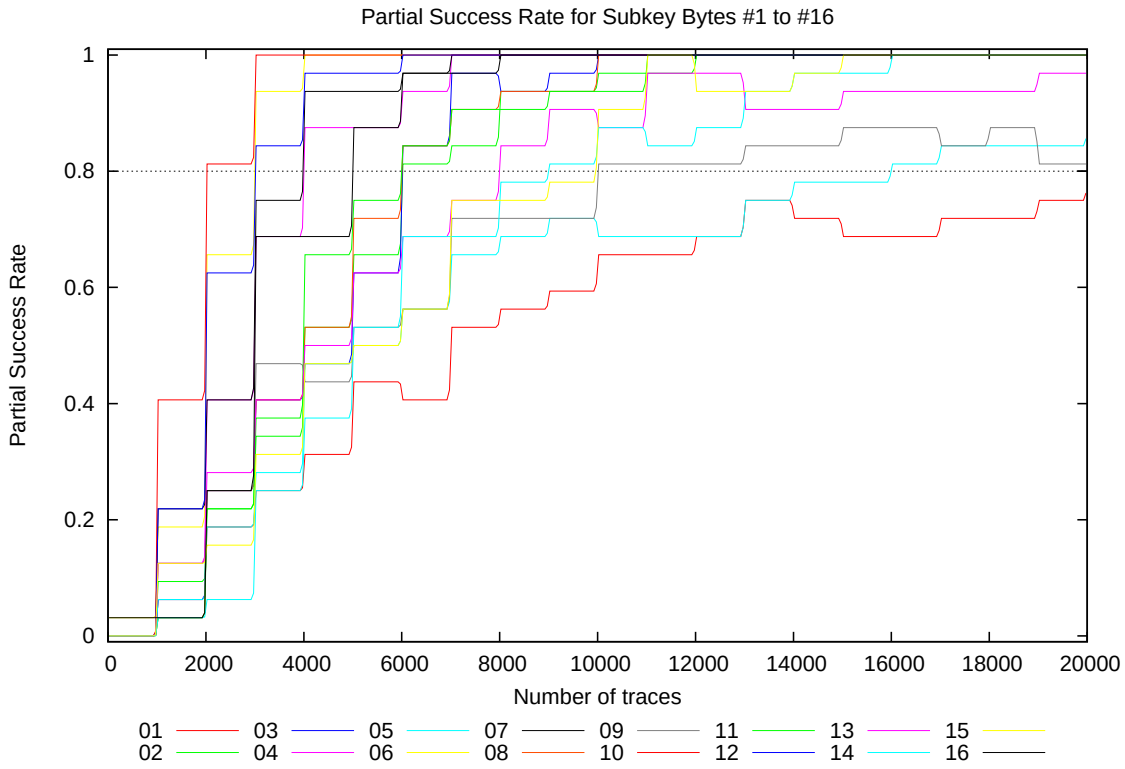

Partial Success Rate for Subkey Byte #14
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000


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

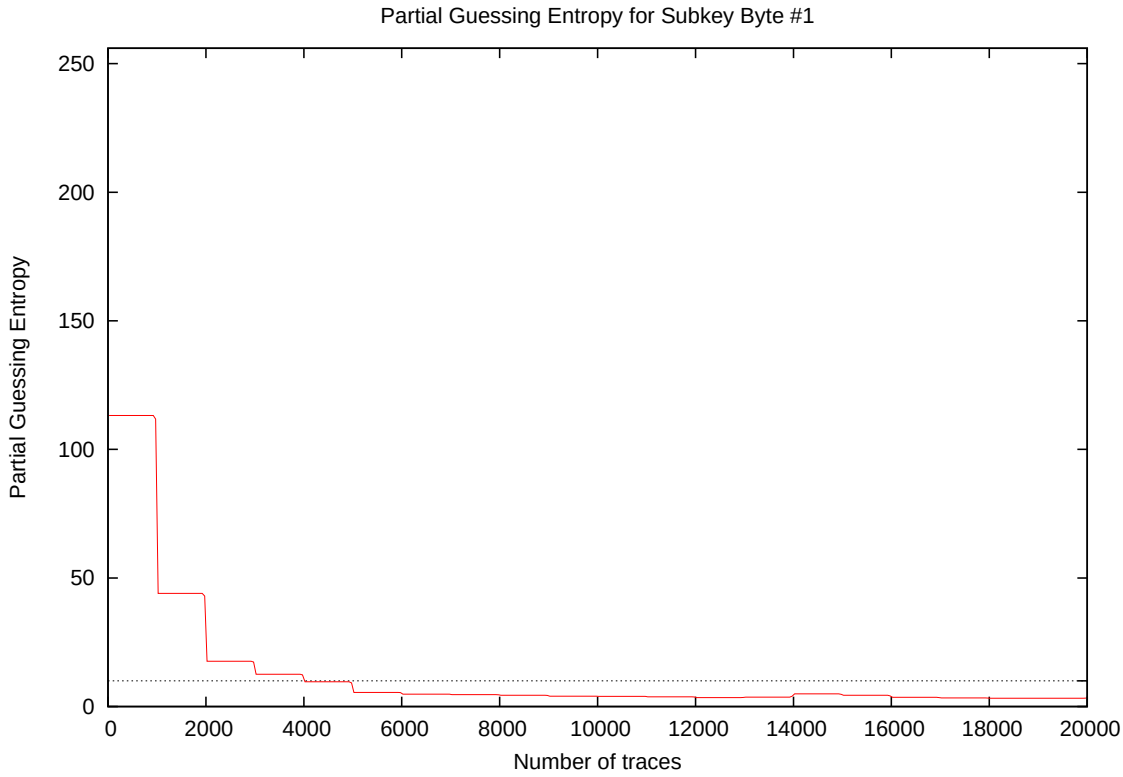

Partial Success Rate for Subkey Bytes #1 to #8
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000
01
02
03
04
05
06
07
08

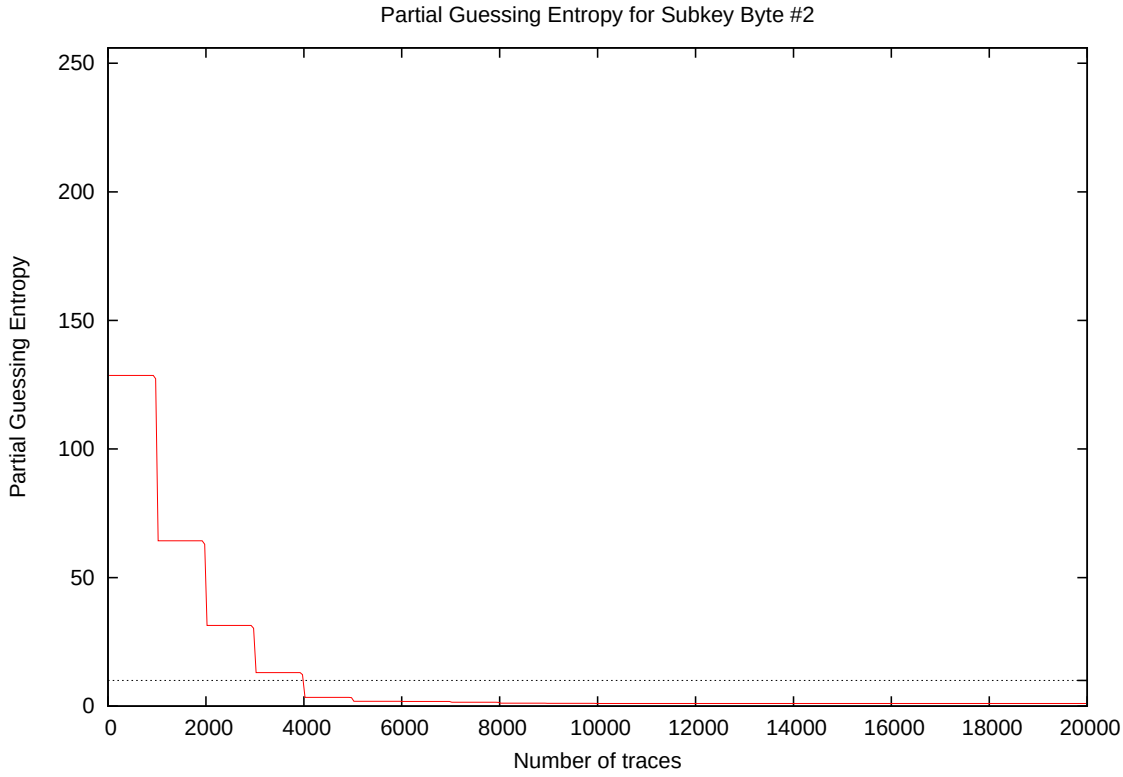

Partial Success Rate for Subkey Bytes #9 to #16
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000
09
10
11
12
13
14
15
16

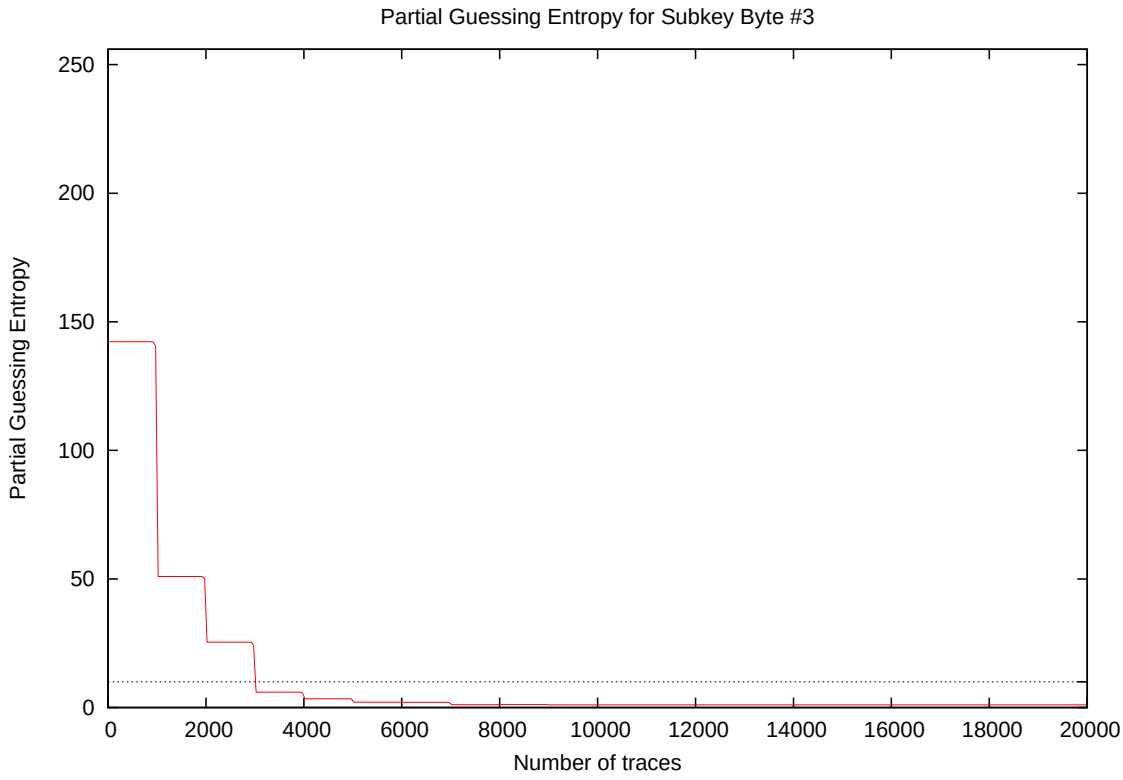

Partial Success Rate for Subkey Bytes #1 to #16
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000
01
02
03
04
05
06
07
08
09
10
11
12
13
14
15
16

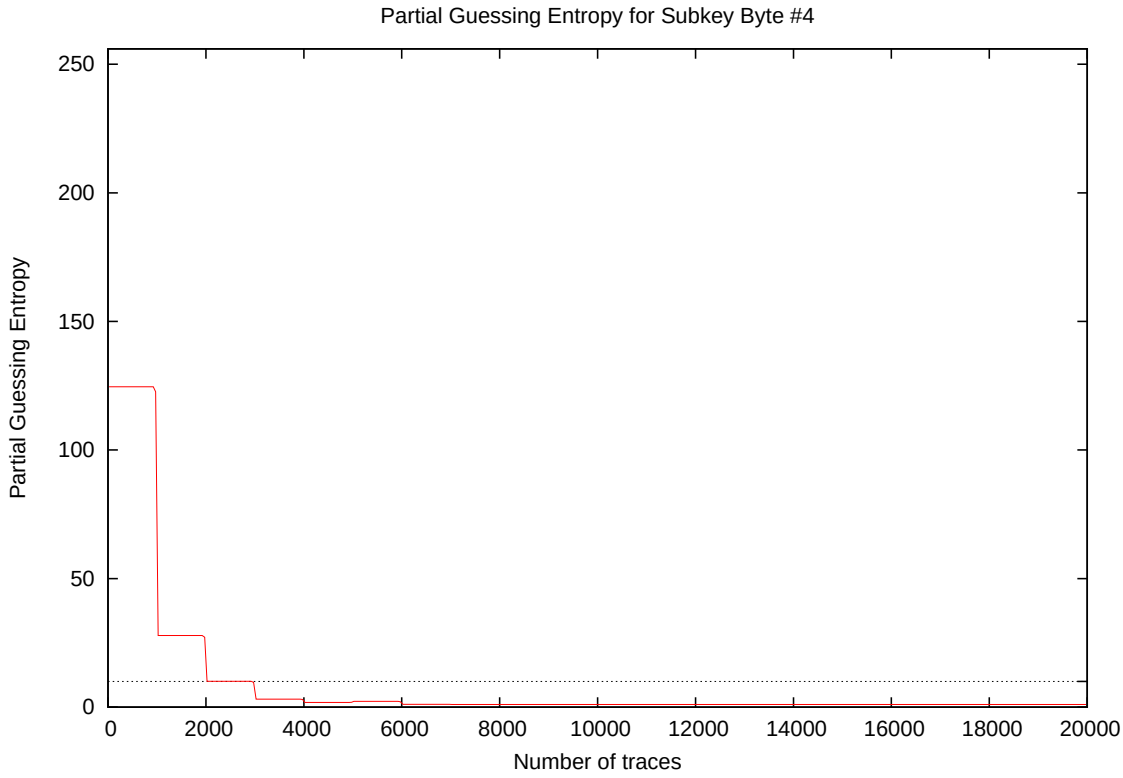
| Traces | Partial Success Rate / Byte | | | | | | | | | | | | | | | | Min | Max | Mean |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | | | |
| 10 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 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 | 0.00 | 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 |
| 30 | 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 |
| 40 | 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 |
| 50 | 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 |
| 100 | 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 |
| 200 | 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 |
| 300 | 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 |
| 400 | 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 |
| 500 | 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 |
| 1000 | 0.06 | 0.09 | 0.06 | 0.12 | 0.06 | 0.19 | 0.22 | 0.03 | 0.12 | 0.41 | 0.03 | 0.22 | 0.12 | 0.03 | 0.12 | 0.03 | 0.03 | 0.41 | 0.12 |
| 2000 | 0.19 | 0.22 | 0.25 | 0.41 | 0.19 | 0.66 | 0.41 | 0.25 | 0.25 | 0.81 | 0.22 | 0.62 | 0.28 | 0.06 | 0.16 | 0.25 | 0.06 | 0.81 | 0.33 |
| 3000 | 0.25 | 0.34 | 0.41 | 0.69 | 0.28 | 0.94 | 0.75 | 0.41 | 0.47 | 1.00 | 0.38 | 0.84 | 0.41 | 0.25 | 0.31 | 0.69 | 0.25 | 1.00 | 0.53 |
| 4000 | 0.31 | 0.53 | 0.47 | 0.88 | 0.47 | 1.00 | 0.94 | 0.53 | 0.44 | 1.00 | 0.66 | 0.97 | 0.50 | 0.38 | 0.47 | 0.69 | 0.31 | 1.00 | 0.64 |
| 5000 | 0.44 | 0.66 | 0.62 | 0.88 | 0.50 | 1.00 | 0.94 | 0.72 | 0.53 | 1.00 | 0.75 | 0.97 | 0.62 | 0.53 | 0.50 | 0.88 | 0.44 | 1.00 | 0.72 |
| 10000 | 0.66 | 0.97 | 1.00 | 1.00 | 0.69 | 1.00 | 1.00 | 1.00 | 0.81 | 1.00 | 0.94 | 1.00 | 0.88 | 0.88 | 0.91 | 1.00 | 0.66 | 1.00 | 0.92 |
| 15000 | 0.69 | 1.00 | 1.00 | 1.00 | 0.78 | 1.00 | 1.00 | 1.00 | 0.88 | 1.00 | 1.00 | 1.00 | 0.94 | 0.97 | 1.00 | 1.00 | 0.69 | 1.00 | 0.95 |
| 20000 | 0.78 | 1.00 | 1.00 | 1.00 | 0.88 | 1.00 | 1.00 | 1.00 | 0.81 | 1.00 | 1.00 | 1.00 | 0.97 | 1.00 | 1.00 | 1.00 | 0.78 | 1.00 | 0.96 |

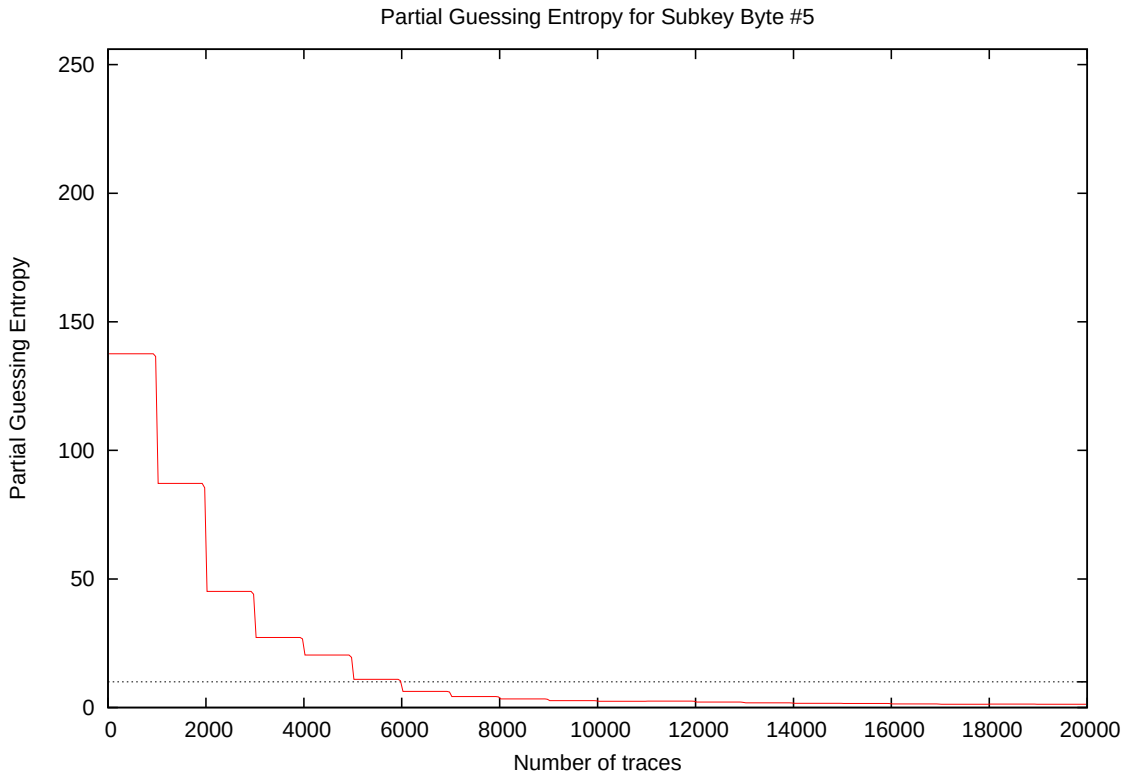
# 4 Partial Guessing Entropy

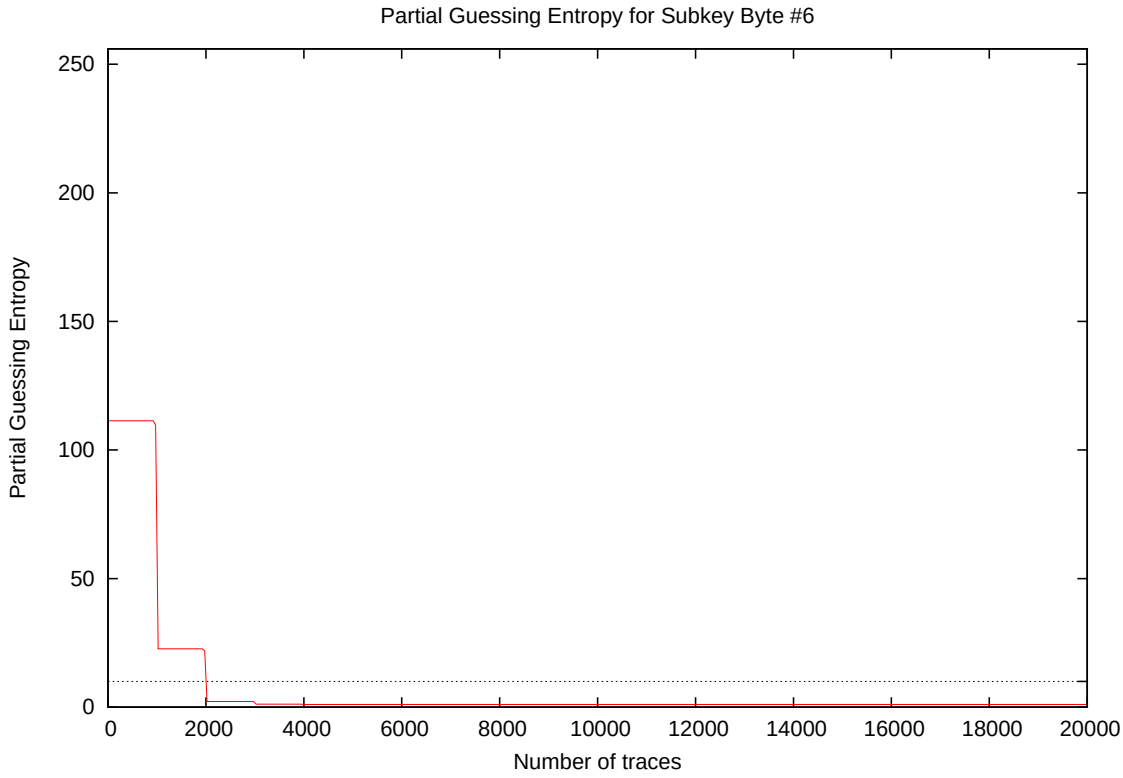


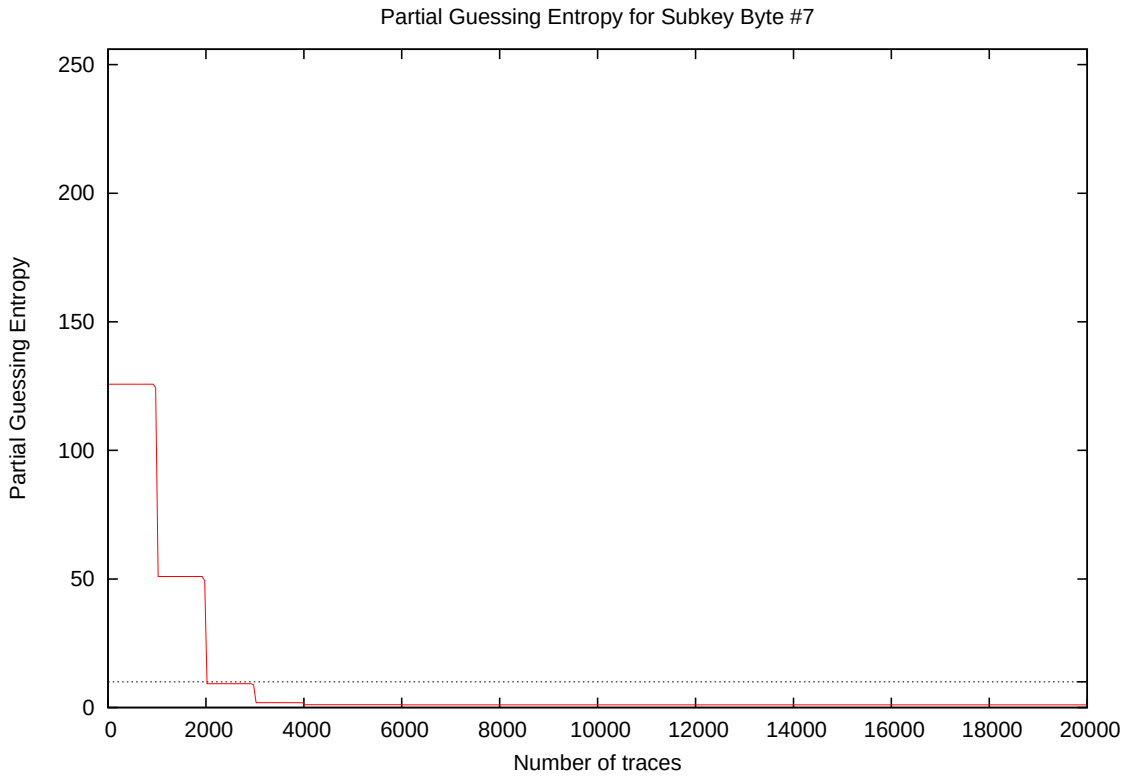



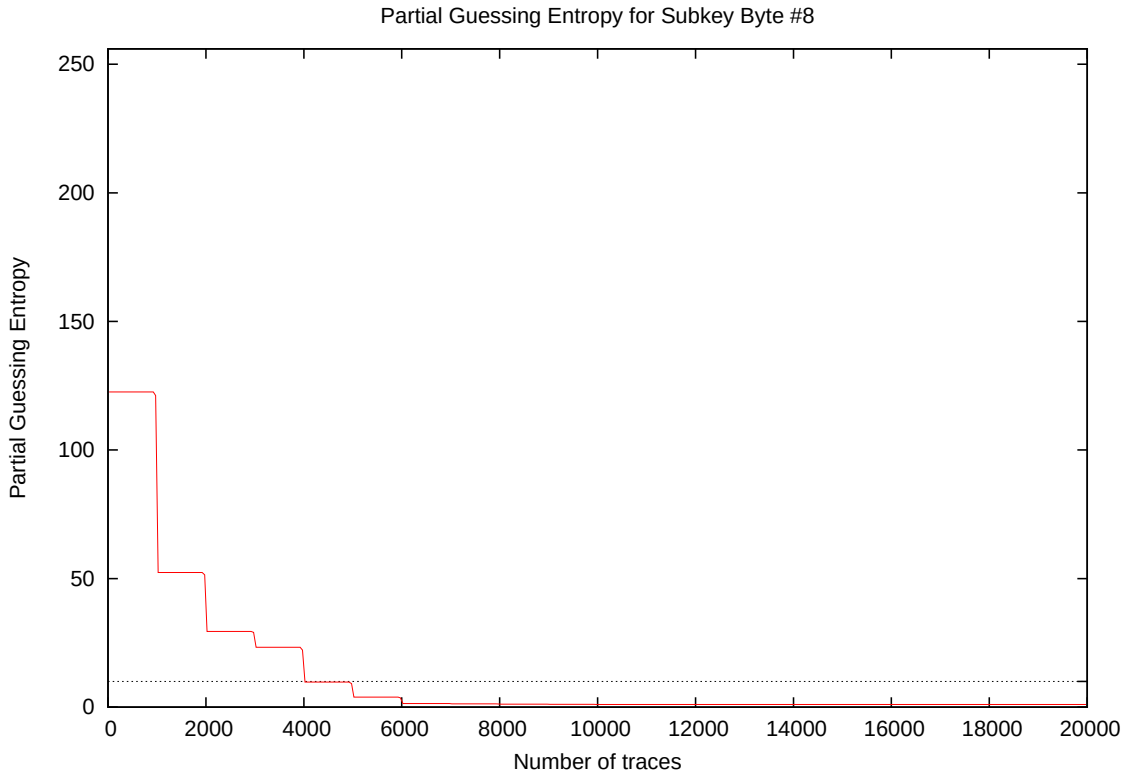

Partial Guessing Entropy for Subkey Byte #3
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000

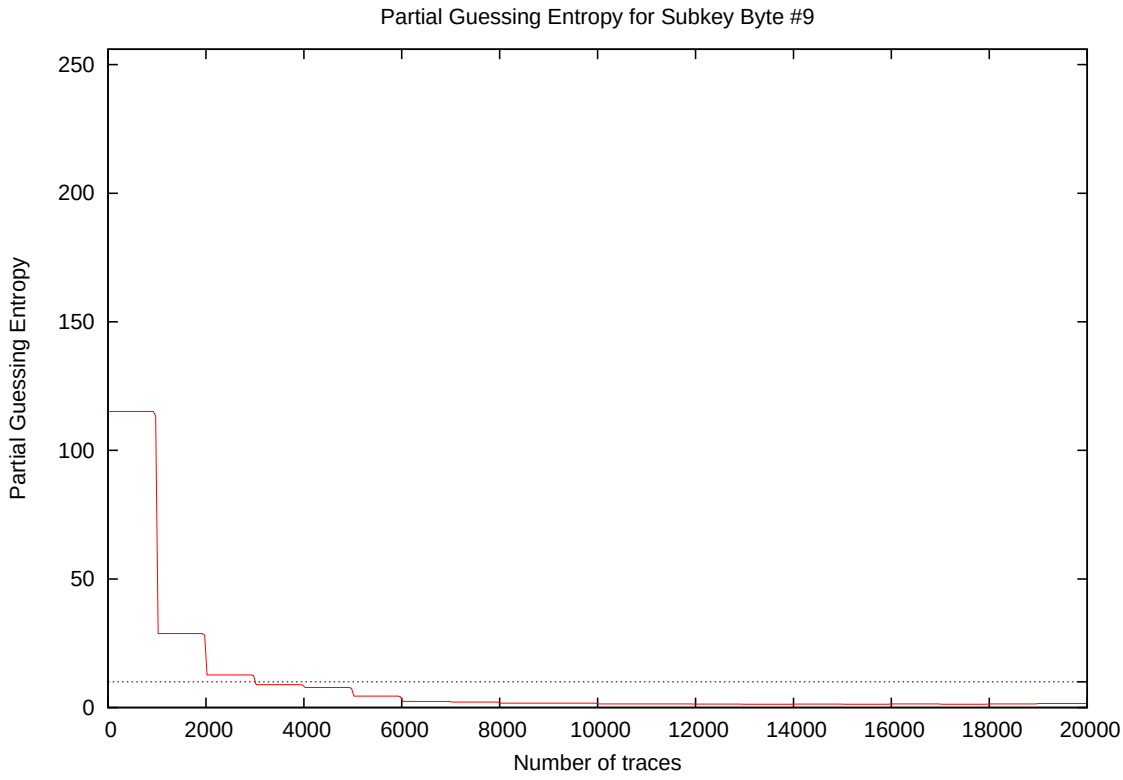

Partial Guessing Entropy for Subkey Byte #4
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000

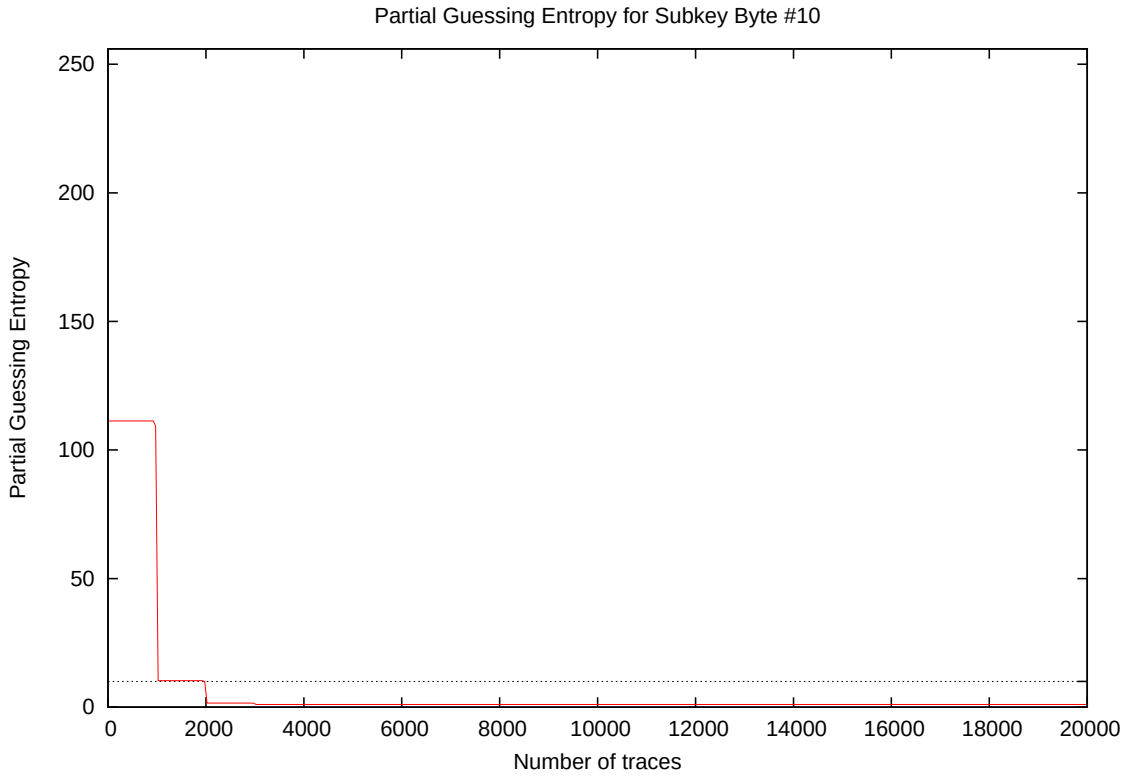

Partial Guessing Entropy for Subkey Byte #5
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000

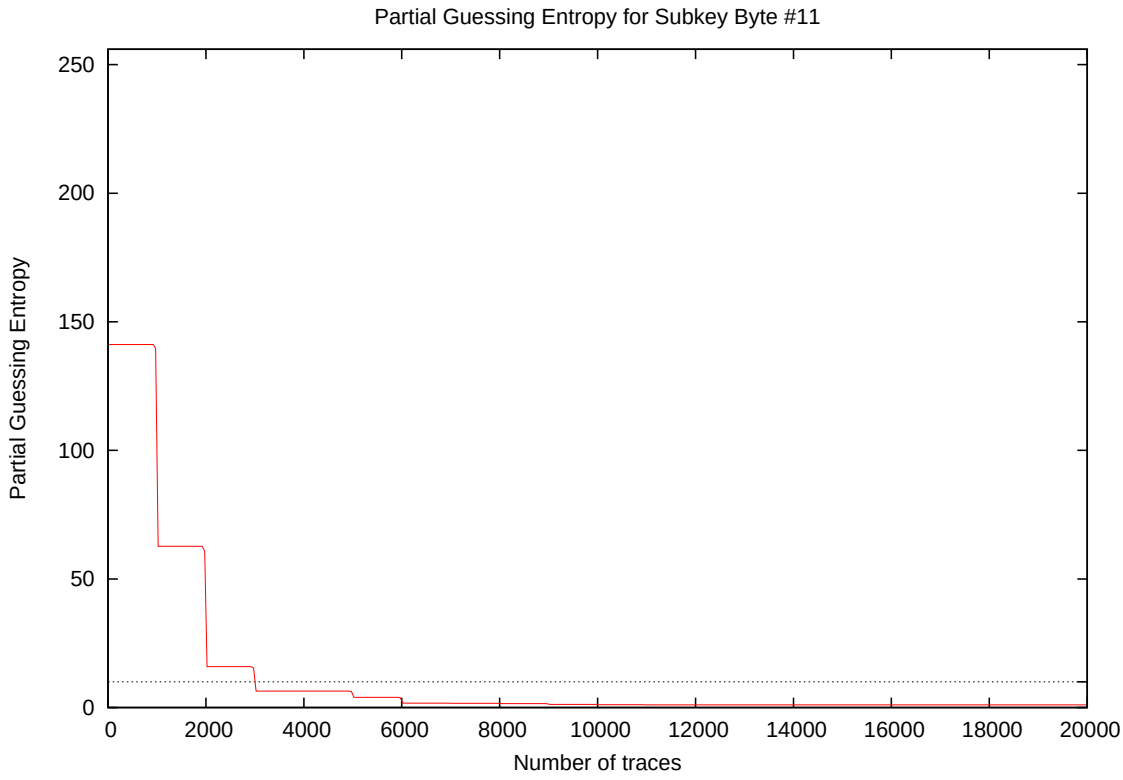

Partial Guessing Entropy for Subkey Byte #6
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000

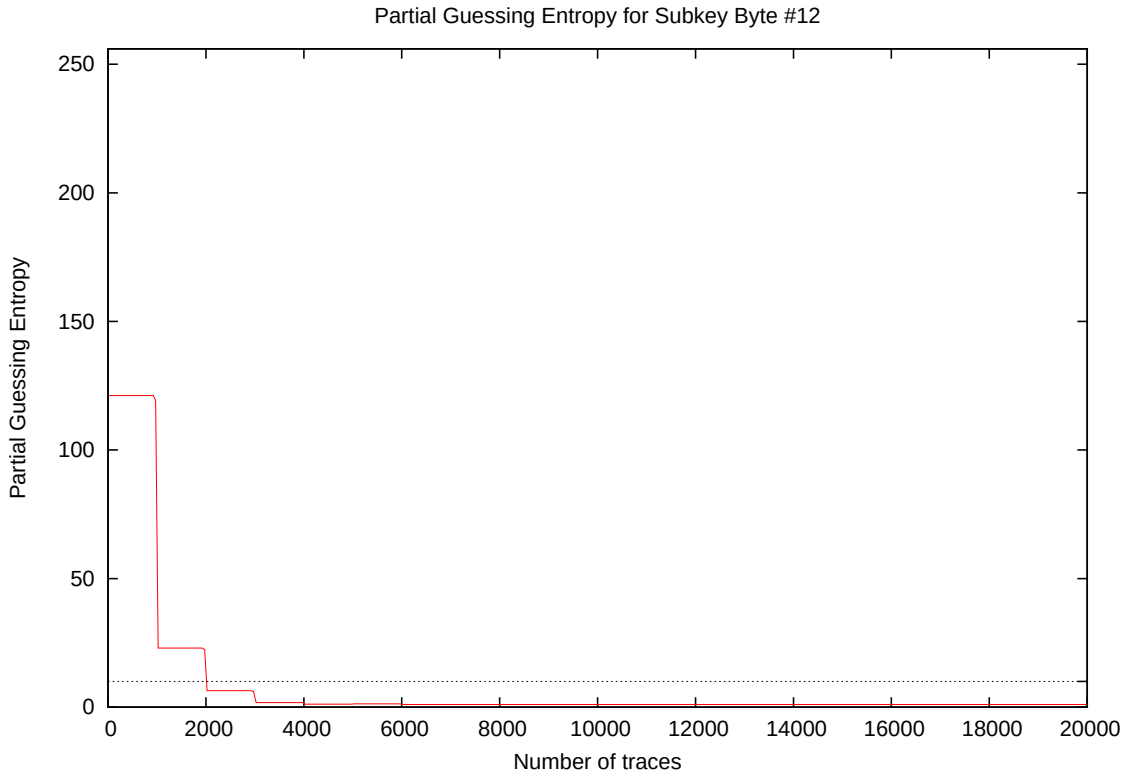

Partial Guessing Entropy for Subkey Byte #7
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000

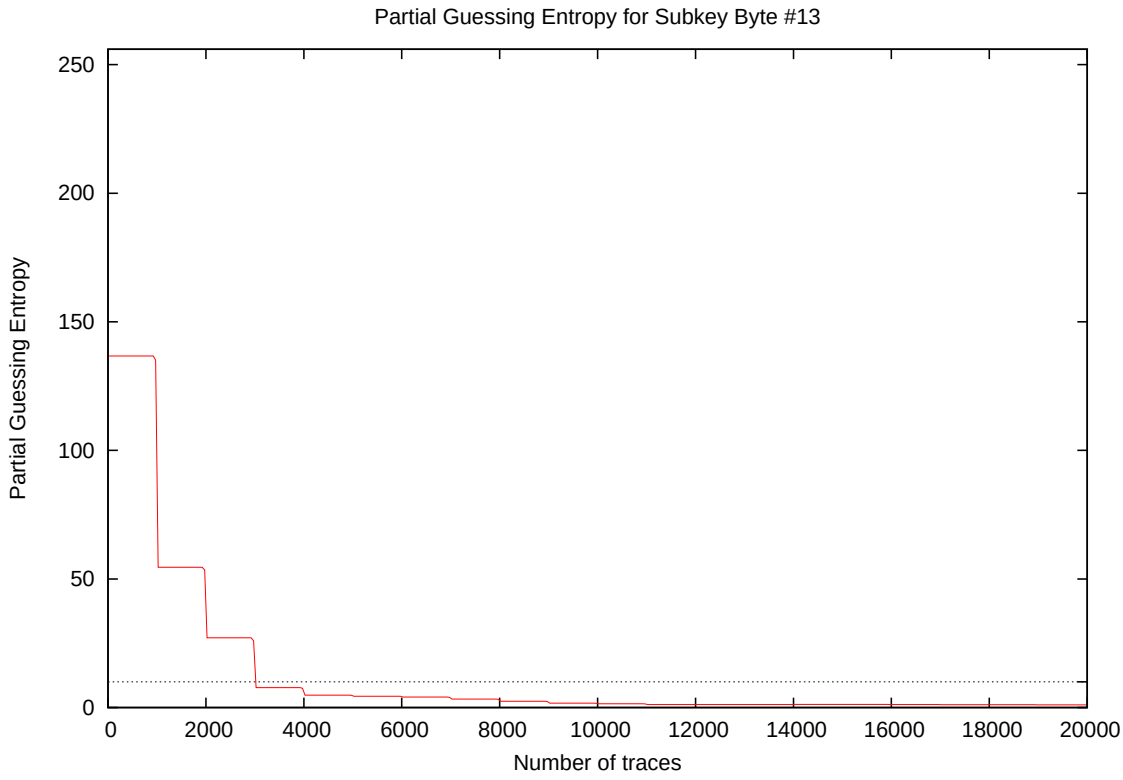

Partial Guessing Entropy for Subkey Byte #8
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000

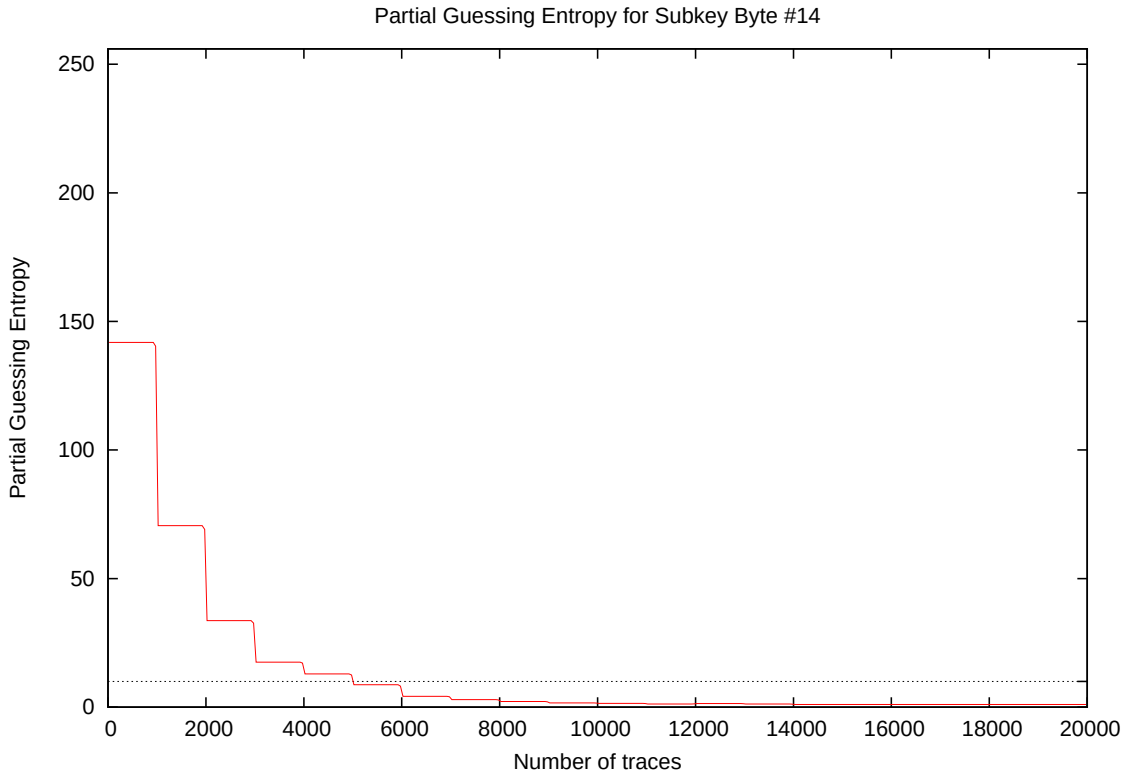

Partial Guessing Entropy for Subkey Byte #9
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000

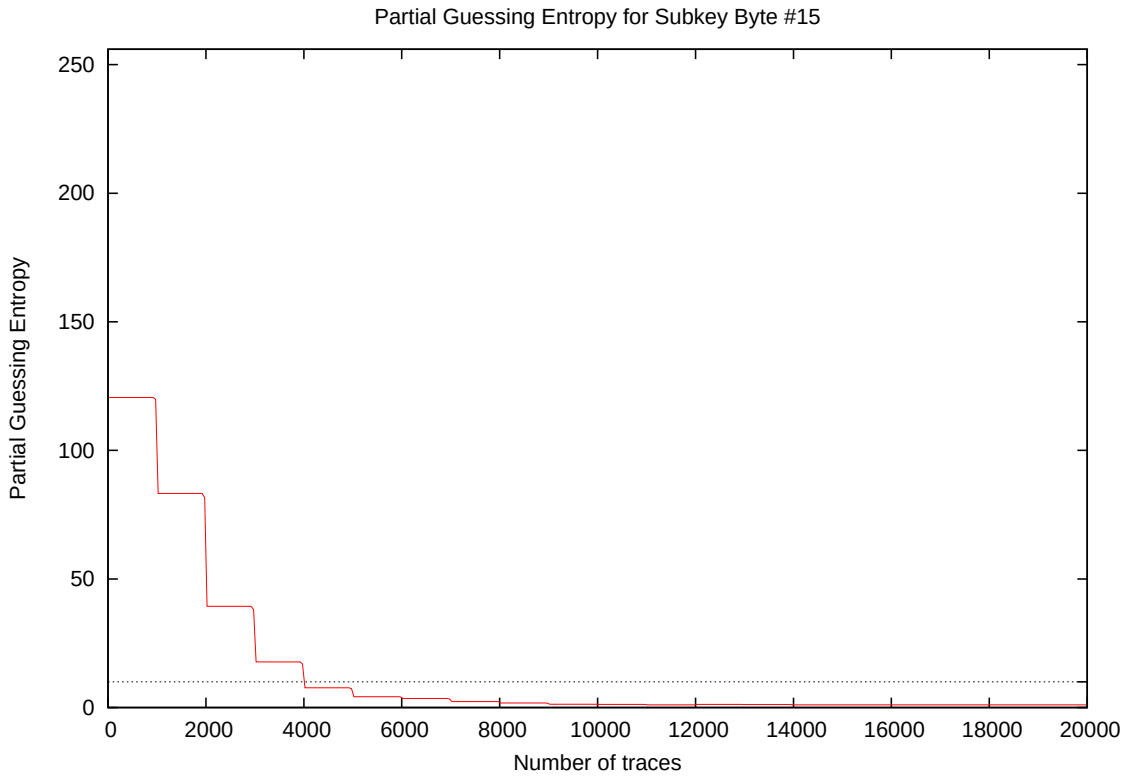

Partial Guessing Entropy for Subkey Byte #10
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000

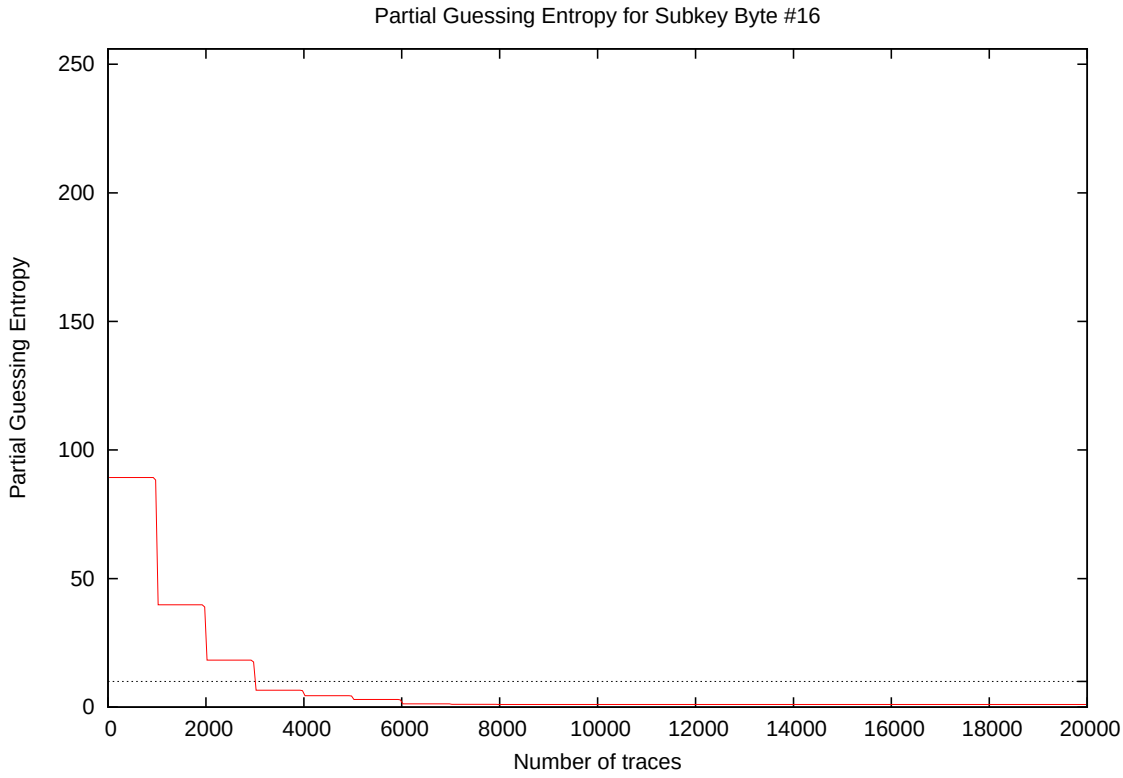

Partial Guessing Entropy for Subkey Byte #11
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000

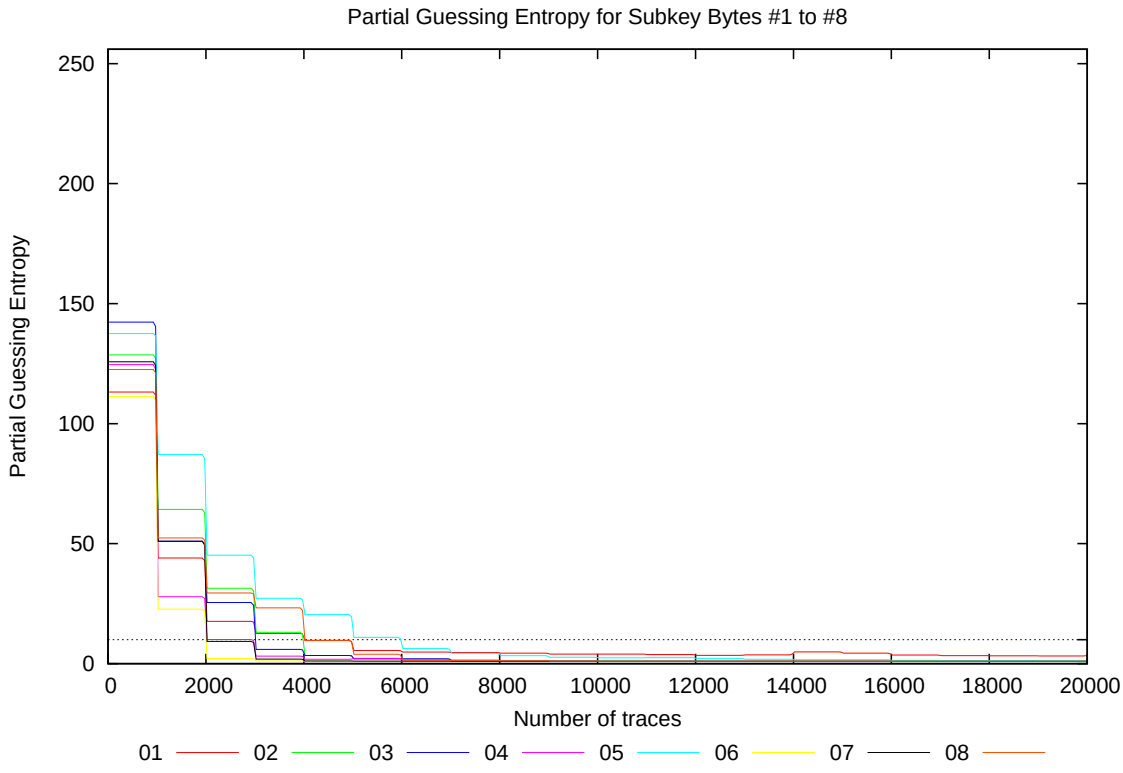

Partial Guessing Entropy for Subkey Byte #12
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000

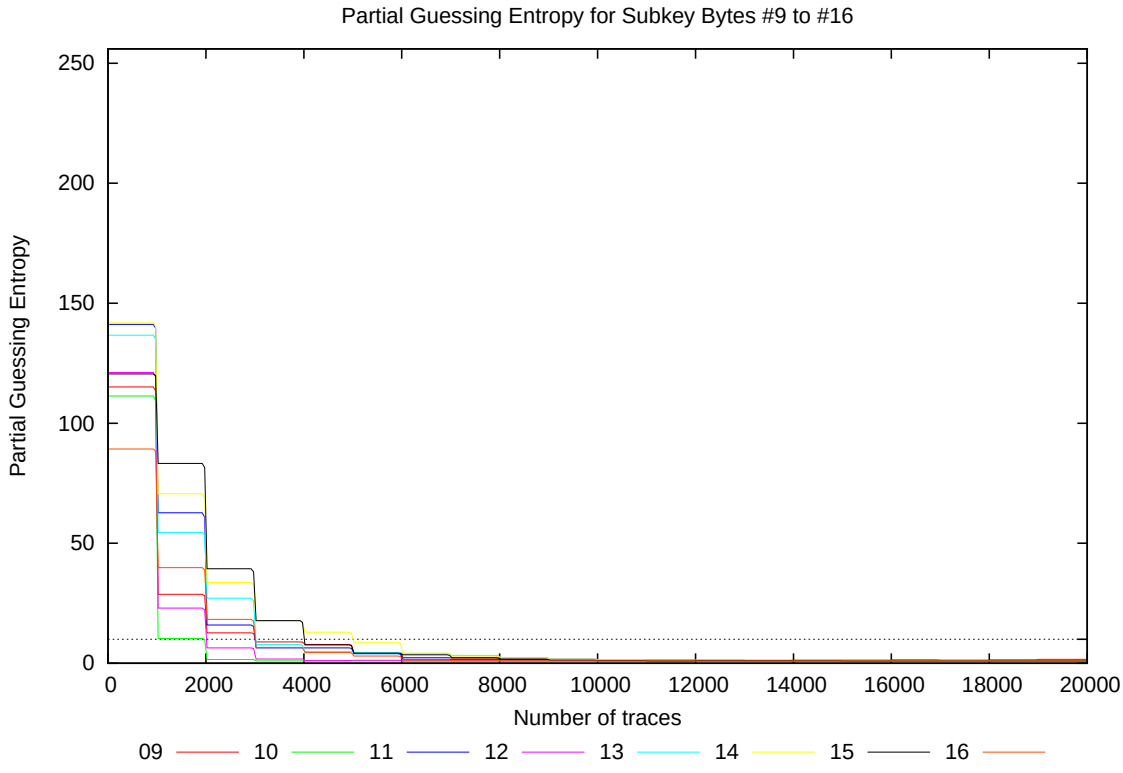

Partial Guessing Entropy for Subkey Byte #13
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000

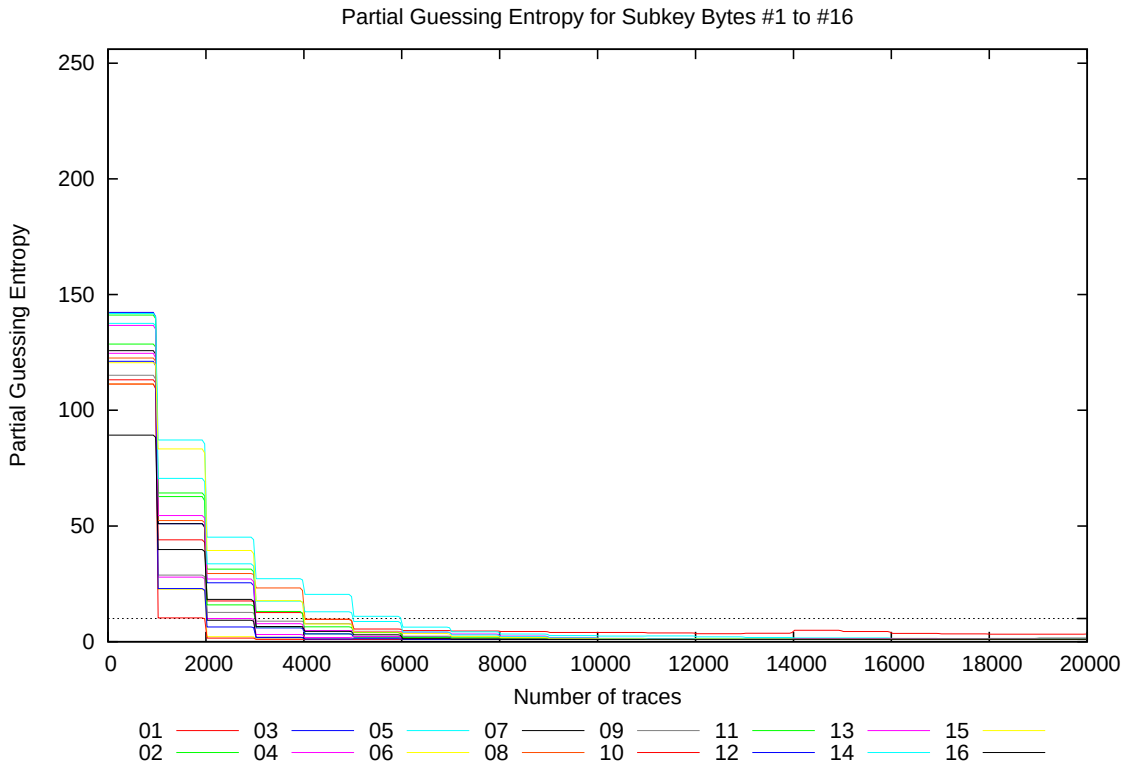

Partial Guessing Entropy for Subkey Byte #14
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
20000


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 | 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 |
| 30 | 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 |
| 40 | 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 |
| 50 | 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 |
| 100 | 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 |
| 200 | 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 |
| 300 | 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 |
| 400 | 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 |
| 500 | 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 |
| 1000 | 44.0 | 64.3 | 51.0 | 27.9 | 87.2 | 22.7 | 51.0 | 52.3 | 28.8 | 10.3 | 62.7 | 23.0 | 54.5 | 70.6 | 83.3 | 39.8 | 10.3 | 87.2 | 48.3 |
| 2000 | 17.6 | 31.4 | 25.4 | 10.0 | 45.2 | 2.2 | 9.3 | 29.4 | 12.7 | 1.6 | 15.9 | 6.4 | 27.1 | 33.7 | 39.4 | 18.2 | 1.6 | 45.2 | 20.3 |
| 3000 | 12.6 | 13.0 | 5.9 | 3.1 | 27.2 | 1.1 | 1.9 | 23.2 | 8.9 | 1.0 | 6.4 | 1.8 | 7.8 | 17.5 | 17.8 | 6.6 | 1.0 | 27.2 | 9.7 |
| 4000 | 9.6 | 3.4 | 3.4 | 1.8 | 20.4 | 1.0 | 1.1 | 9.7 | 7.8 | 1.0 | 6.4 | 1.1 | 4.8 | 12.9 | 7.7 | 4.5 | 1.0 | 20.4 | 6.0 |
| 5000 | 5.5 | 1.9 | 2.1 | 2.2 | 11.0 | 1.0 | 1.1 | 3.9 | 4.4 | 1.0 | 4.0 | 1.2 | 4.4 | 8.7 | 4.2 | 3.0 | 1.0 | 11.0 | 3.7 |
| 10000 | 4.0 | 1.0 | 1.0 | 1.0 | 2.4 | 1.0 | 1.0 | 1.0 | 1.4 | 1.0 | 1.1 | 1.0 | 1.4 | 1.4 | 1.2 | 1.0 | 1.0 | 4.0 | 1.4 |
| 15000 | 4.4 | 1.0 | 1.0 | 1.0 | 1.6 | 1.0 | 1.0 | 1.0 | 1.3 | 1.0 | 1.0 | 1.0 | 1.2 | 1.0 | 1.0 | 1.0 | 1.0 | 4.4 | 1.3 |
| 20000 | 3.4 | 1.0 | 1.0 | 1.0 | 1.2 | 1.0 | 1.0 | 1.0 | 1.6 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 3.4 | 1.2 |