# DPA Contest v4.2
# Evaluation results

Hideo Shimizu

September 2015

## 1 Introduction

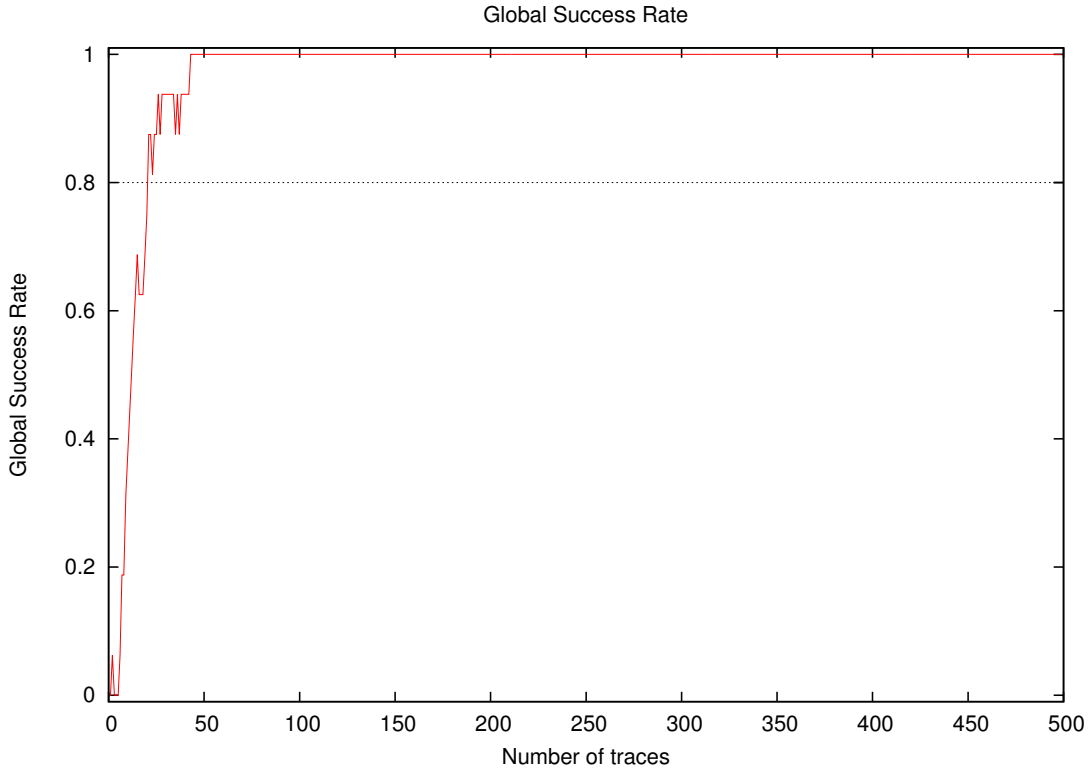
### 1.1 About the attack

- **Sender/Team:** Hideo Shimizu
- **Institution:** Toshiba Corporation Corporate Research & Development Center, Japan
- **Language:** Java
- **Operating system:** Windows
- **Attacked subkey:** 0

### 1.2 About the evaluation

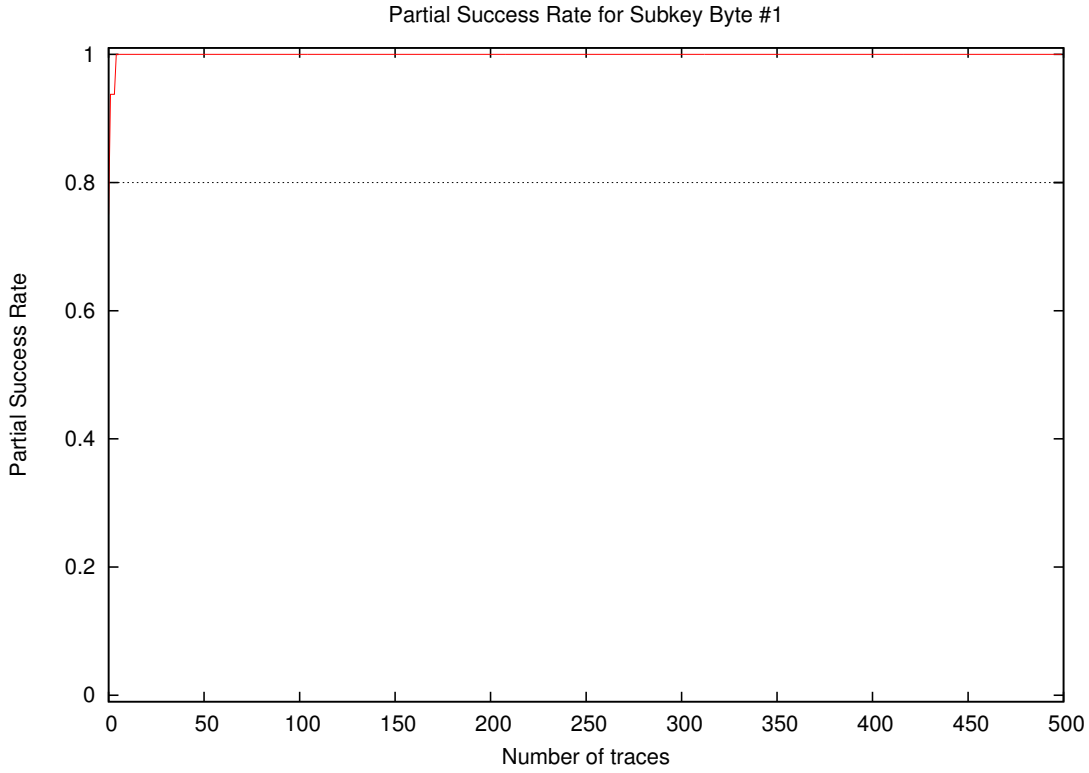
- **Date of evaluation:** September 2015

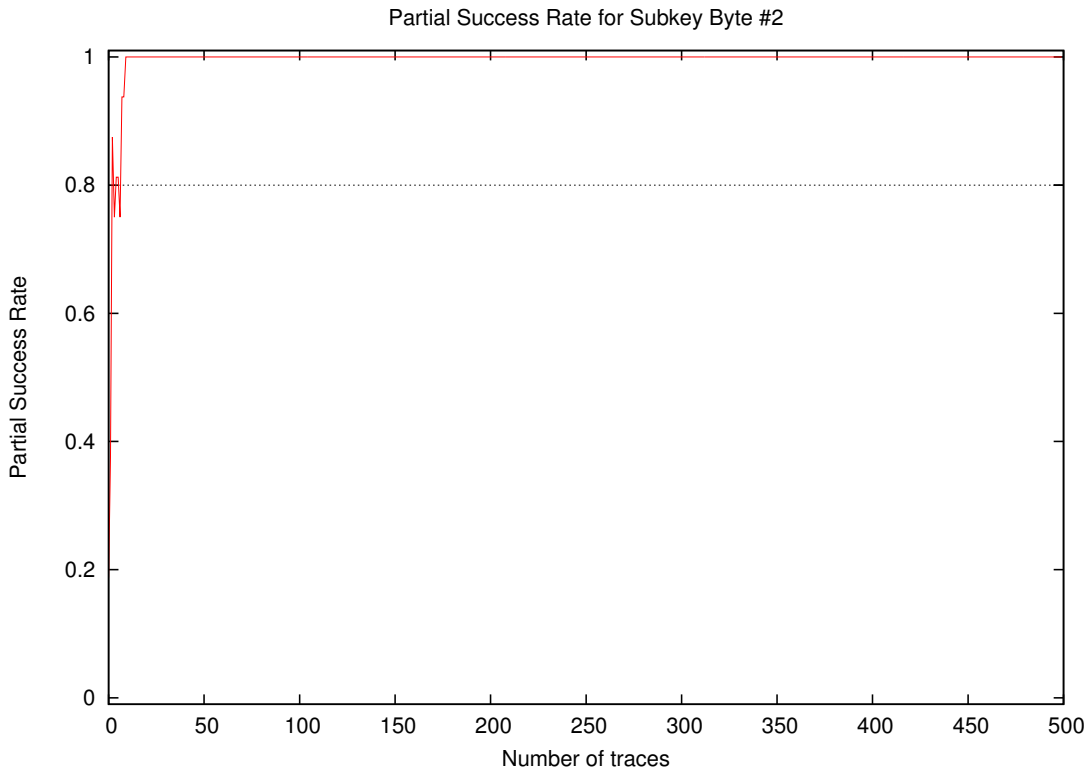
## 2 Global Success Rate

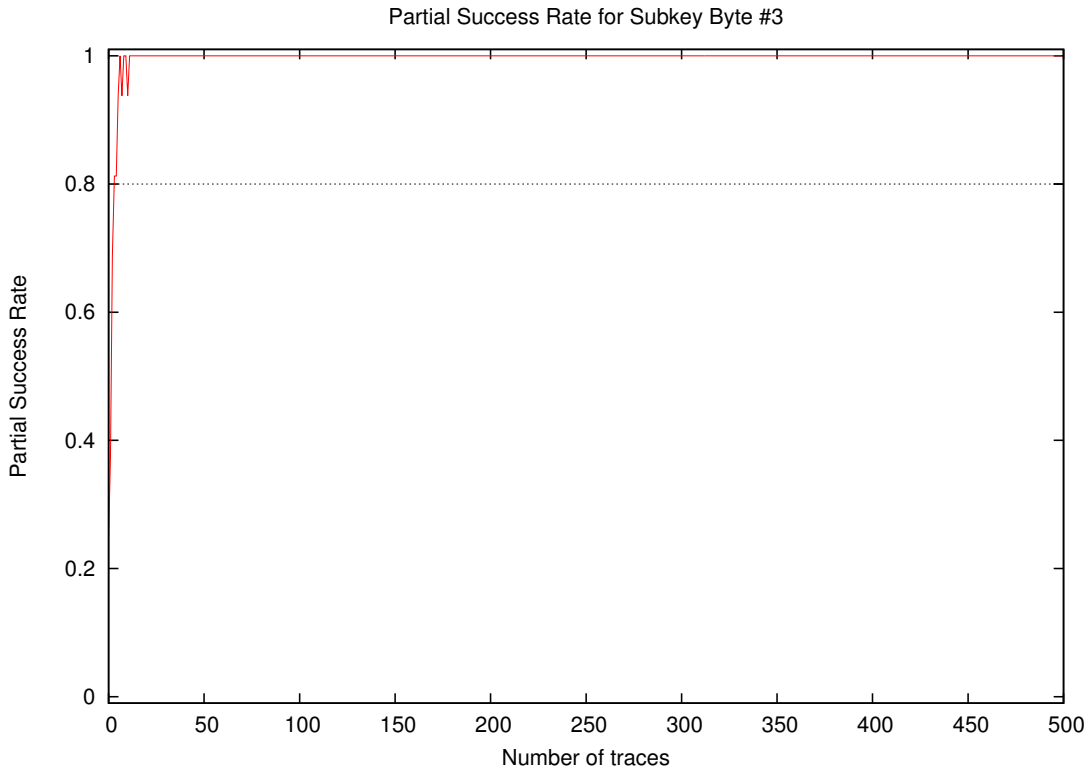


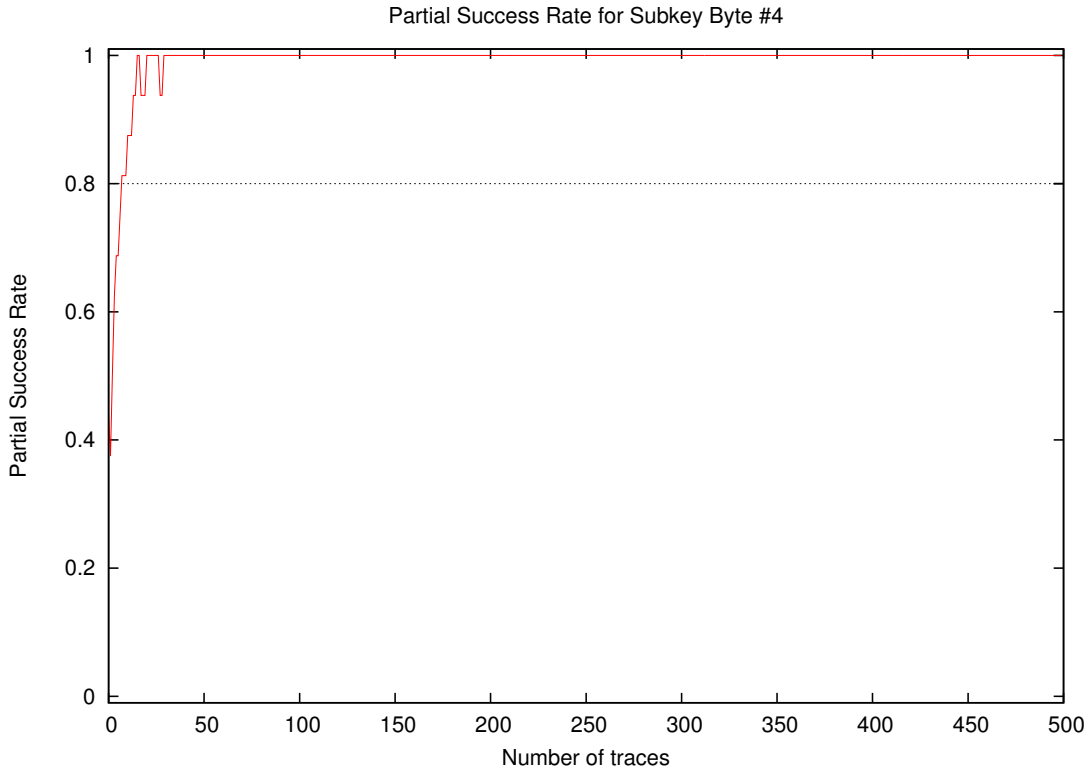
| Number of traces | Global Success Rate |
|---:|:---:|
| 10 | 0.31 |
| 20 | 0.69 |
| 30 | 0.94 |
| 40 | 0.94 |
| 50 | 1.00 |
| 100 | 1.00 |
| 200 | 1.00 |
| 300 | 1.00 |
| 400 | 1.00 |
| 500 | 1.00 |

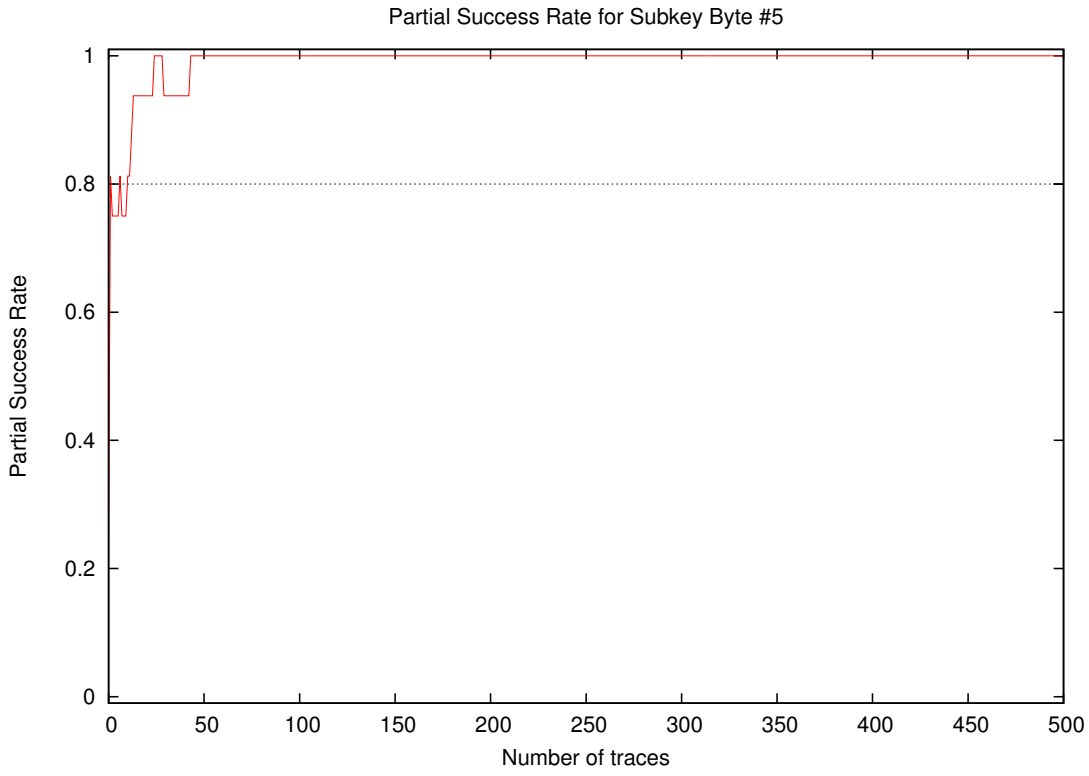
# 3 Partial Success Rate

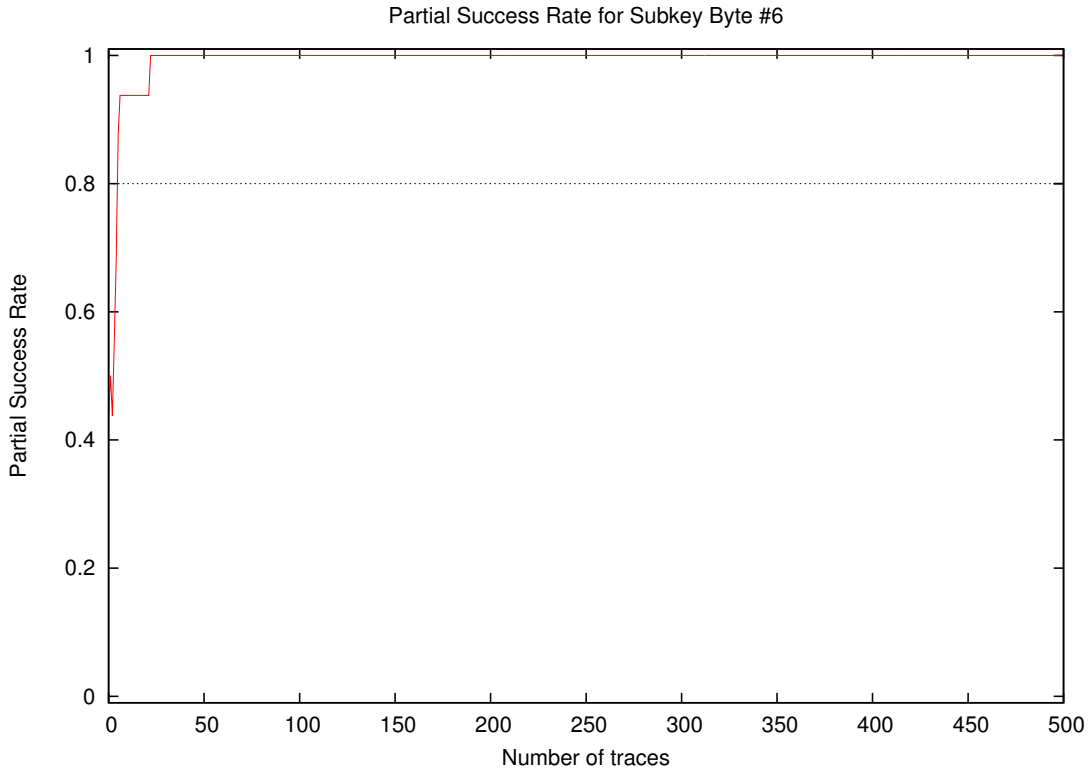


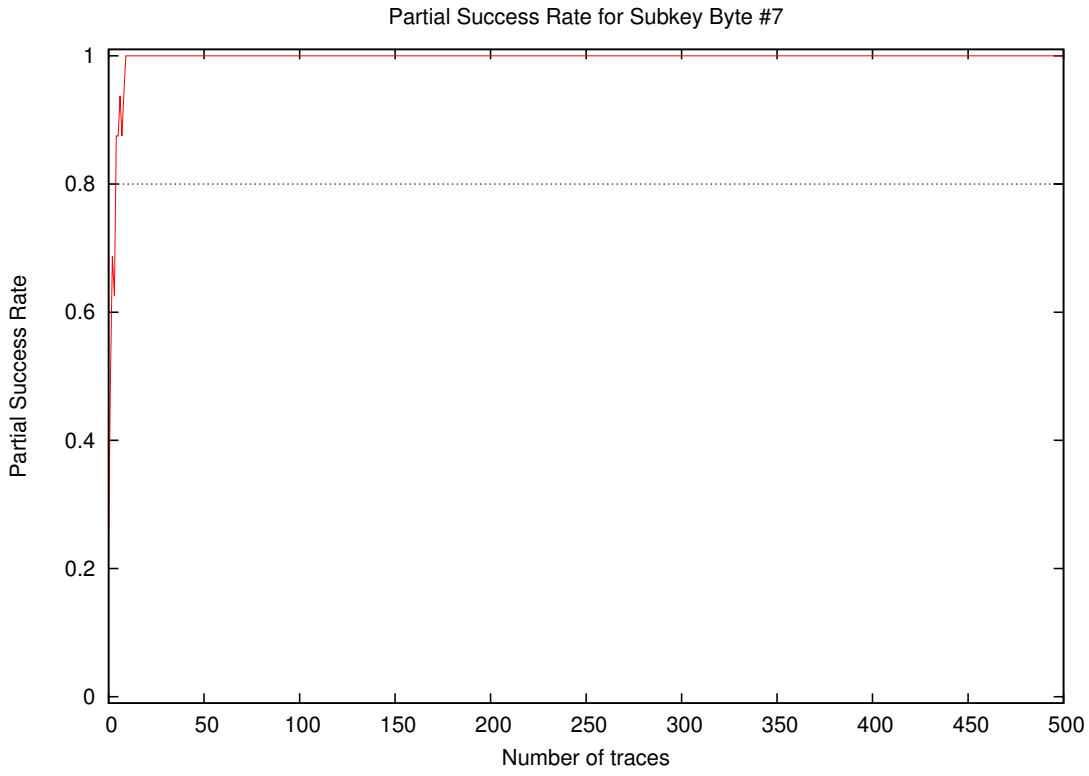



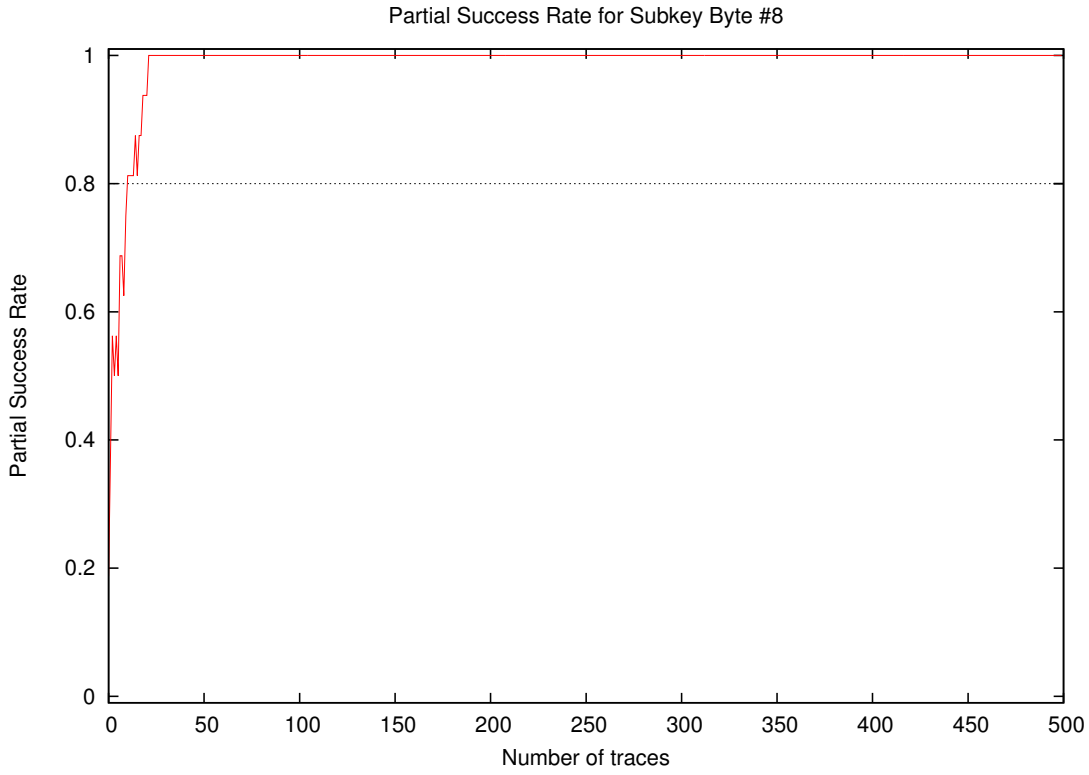

Partial Success Rate for Subkey Byte #3
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
50
100
150
200
250
300
350
400
450
500

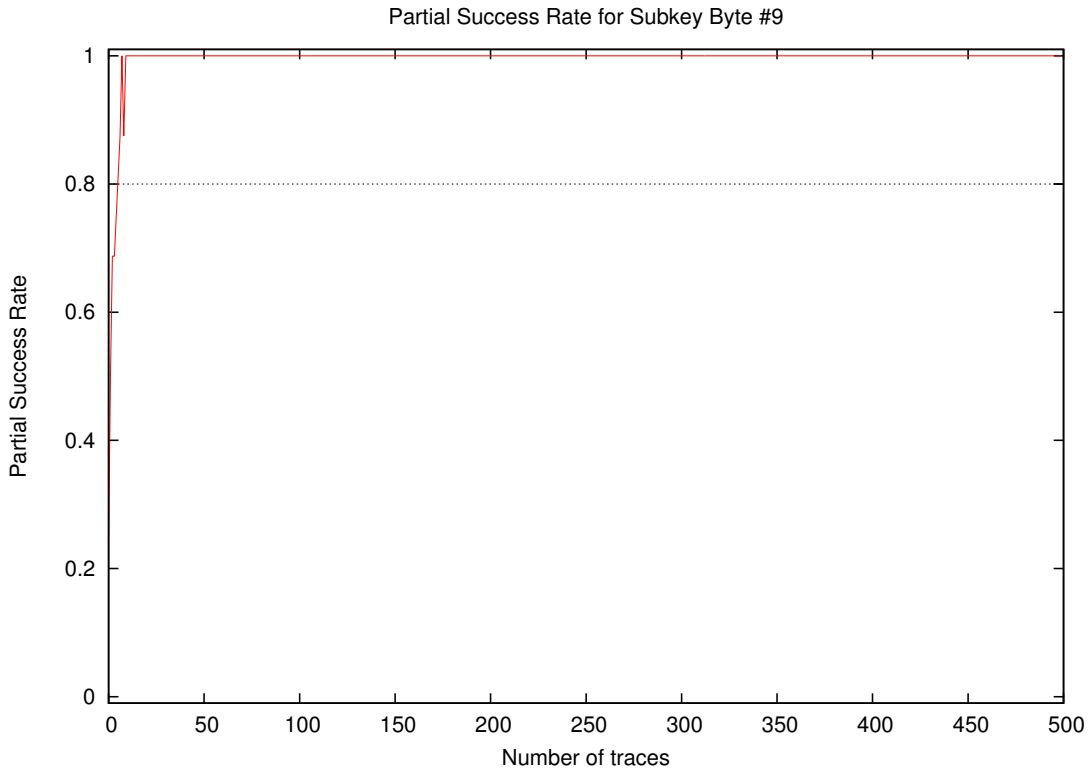

Partial Success Rate for Subkey Byte #4
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
50
100
150
200
250
300
350
400
450
500

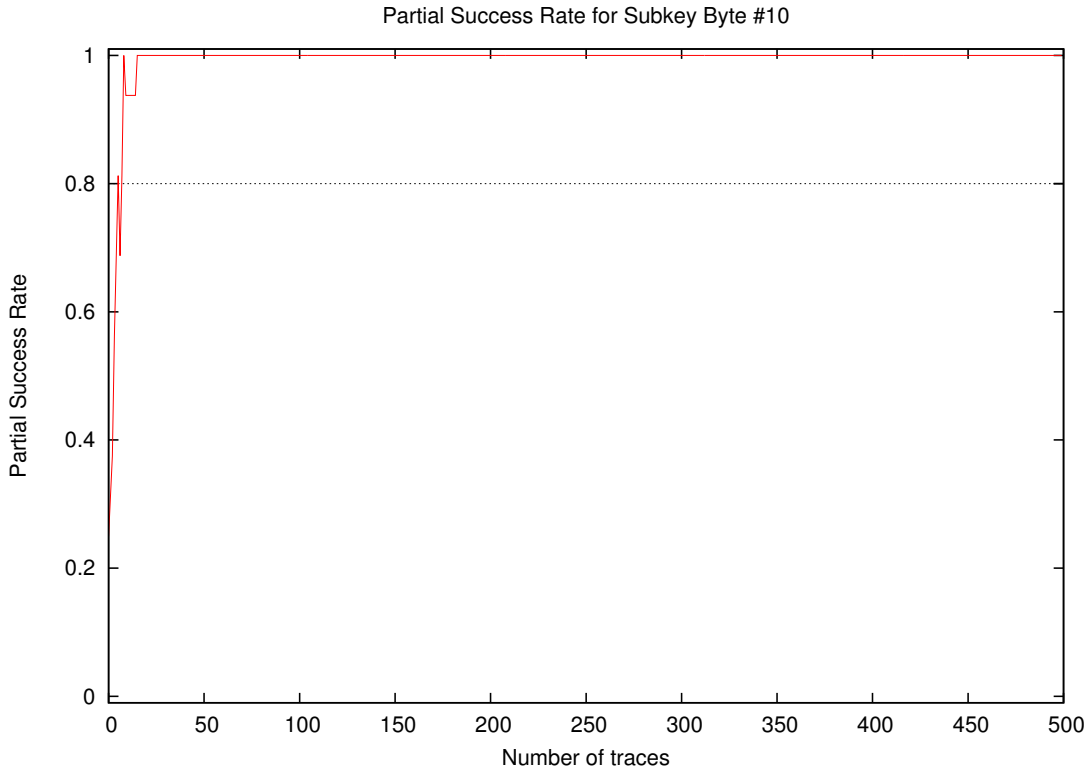

Partial Success Rate for Subkey Byte #5
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
50
100
150
200
250
300
350
400
450
500

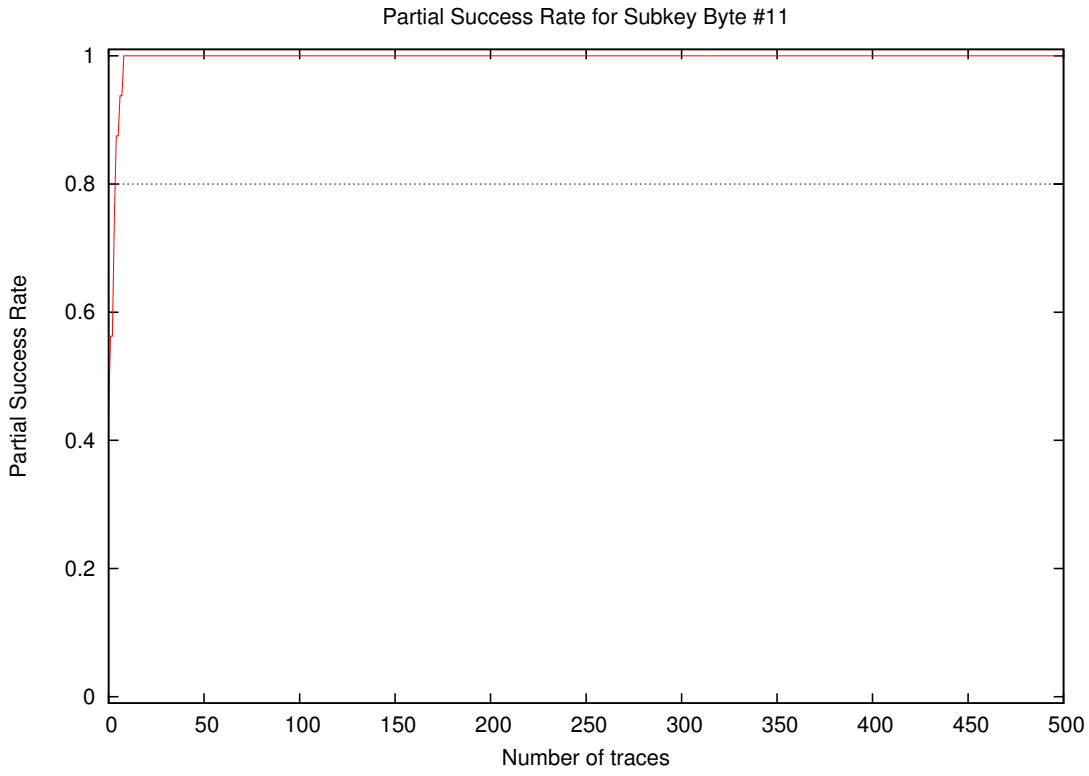

Partial Success Rate for Subkey Byte #6
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
50
100
150
200
250
300
350
400
450
500

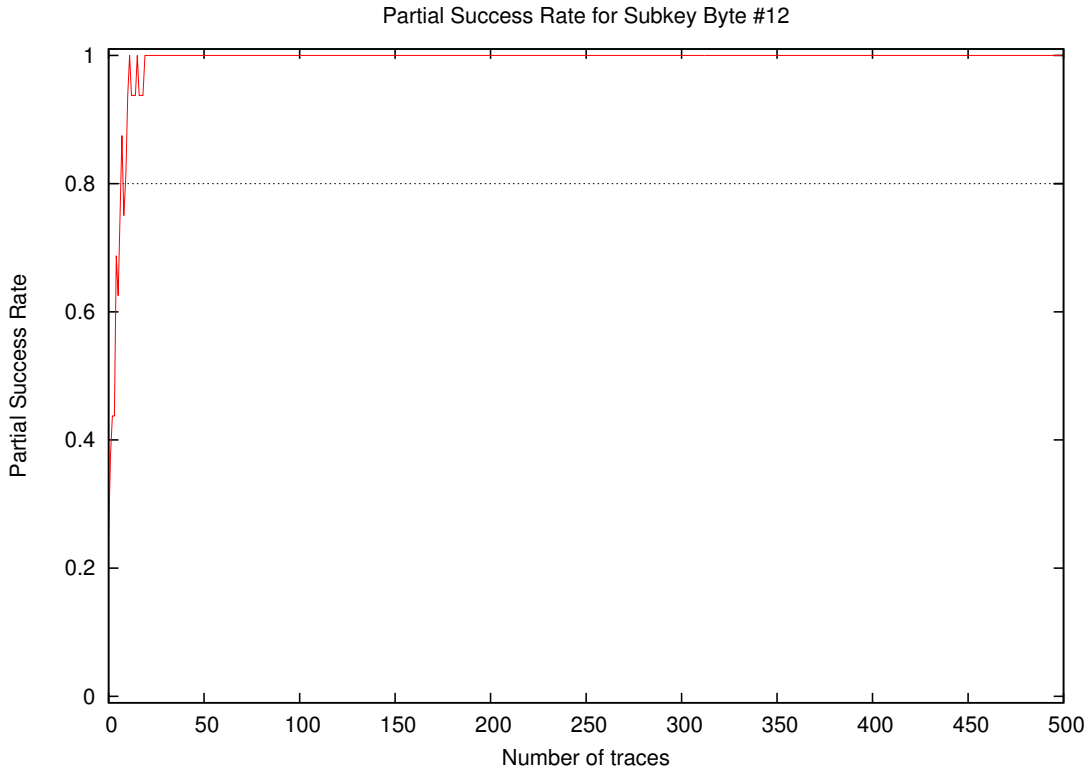

Partial Success Rate for Subkey Byte #7
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
50
100
150
200
250
300
350
400
450
500

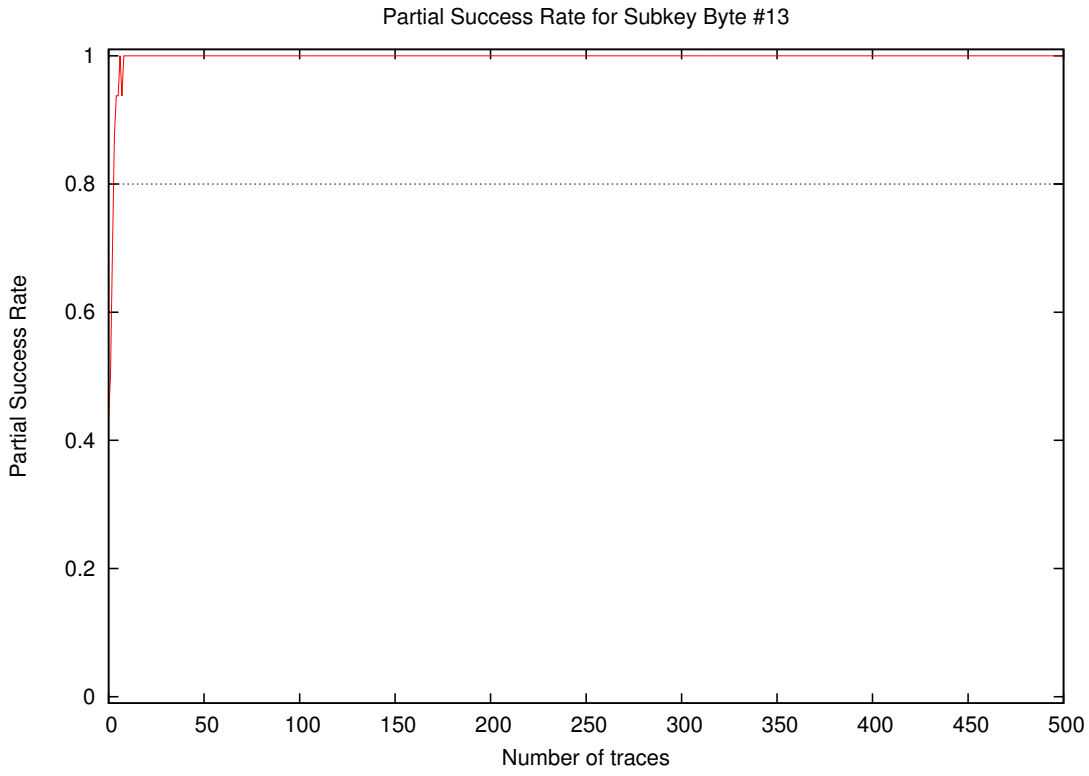

Partial Success Rate for Subkey Byte #8
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
50
100
150
200
250
300
350
400
450
500

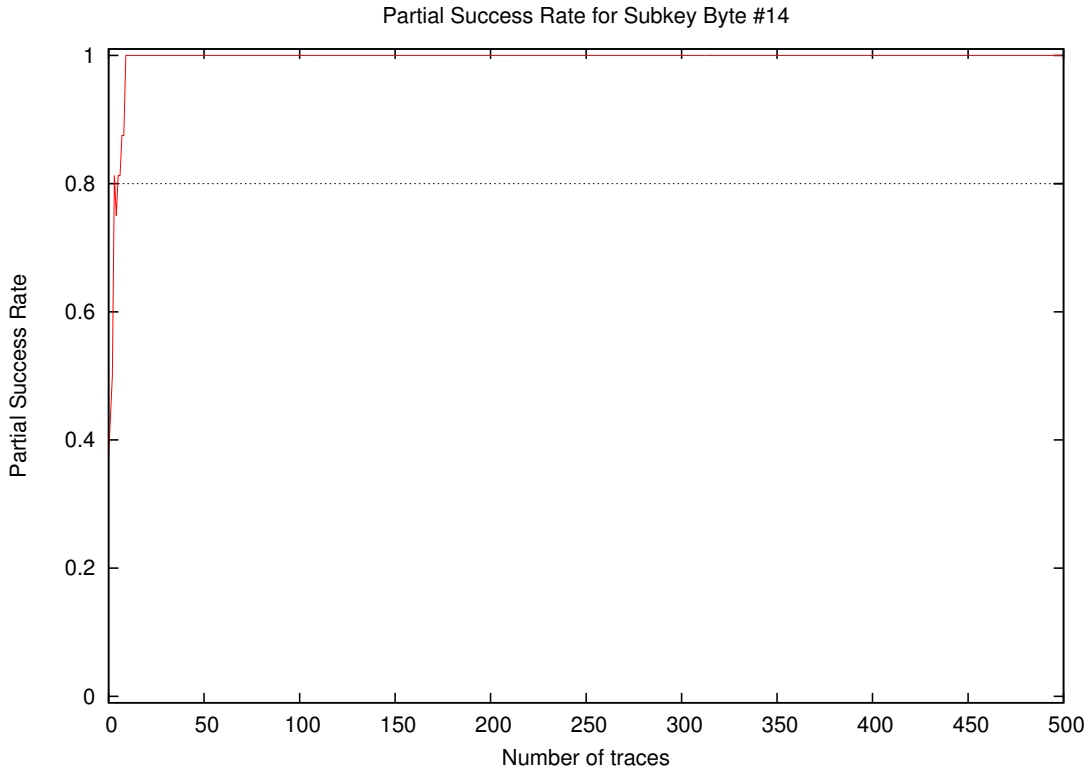

Partial Success Rate for Subkey Byte #9
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
50
100
150
200
250
300
350
400
450
500

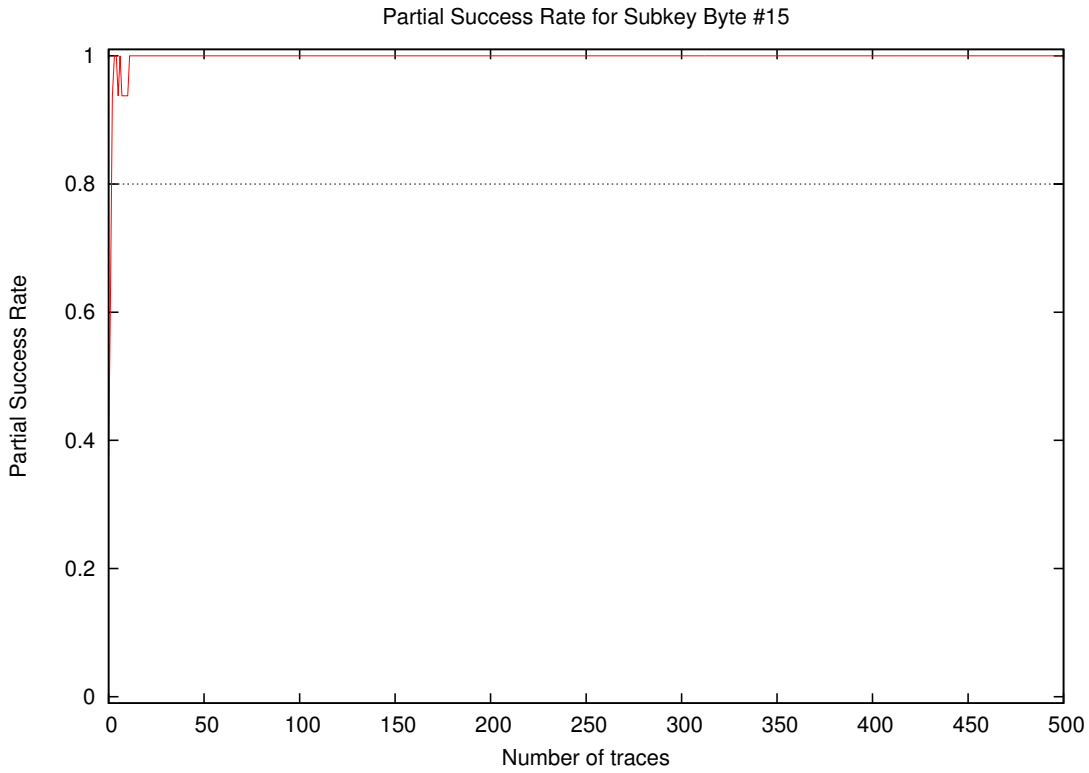

Partial Success Rate for Subkey Byte #10
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
50
100
150
200
250
300
350
400
450
500

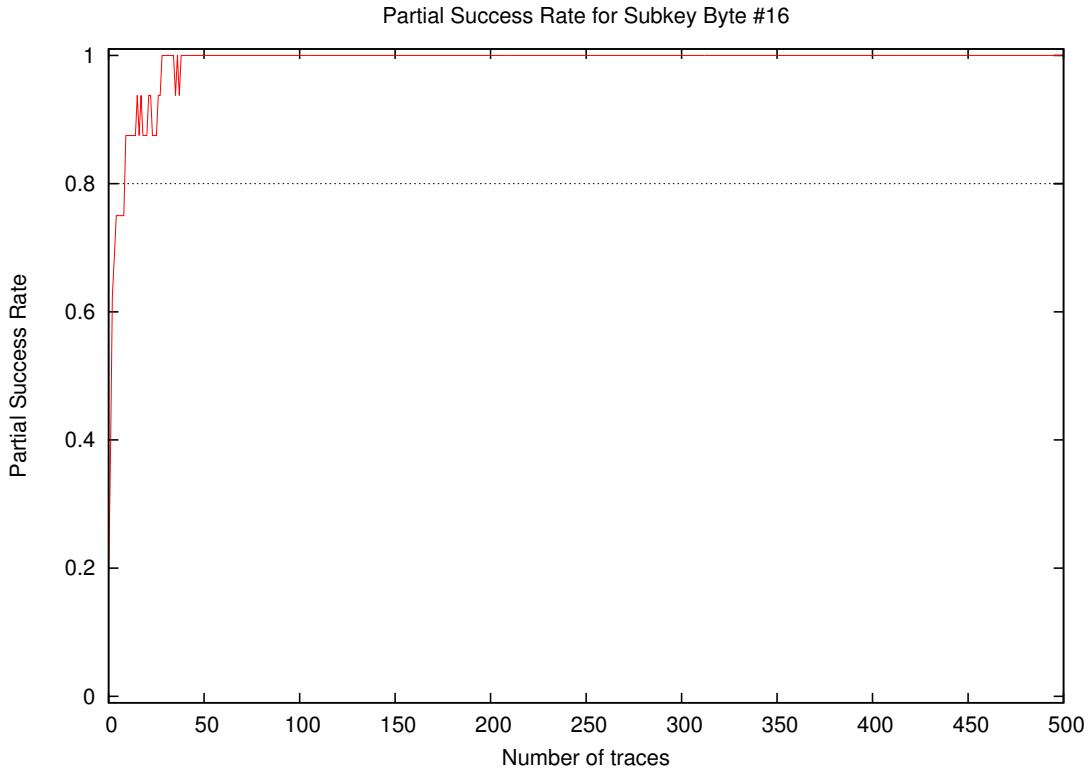

Partial Success Rate for Subkey Byte #11
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
50
100
150
200
250
300
350
400
450
500

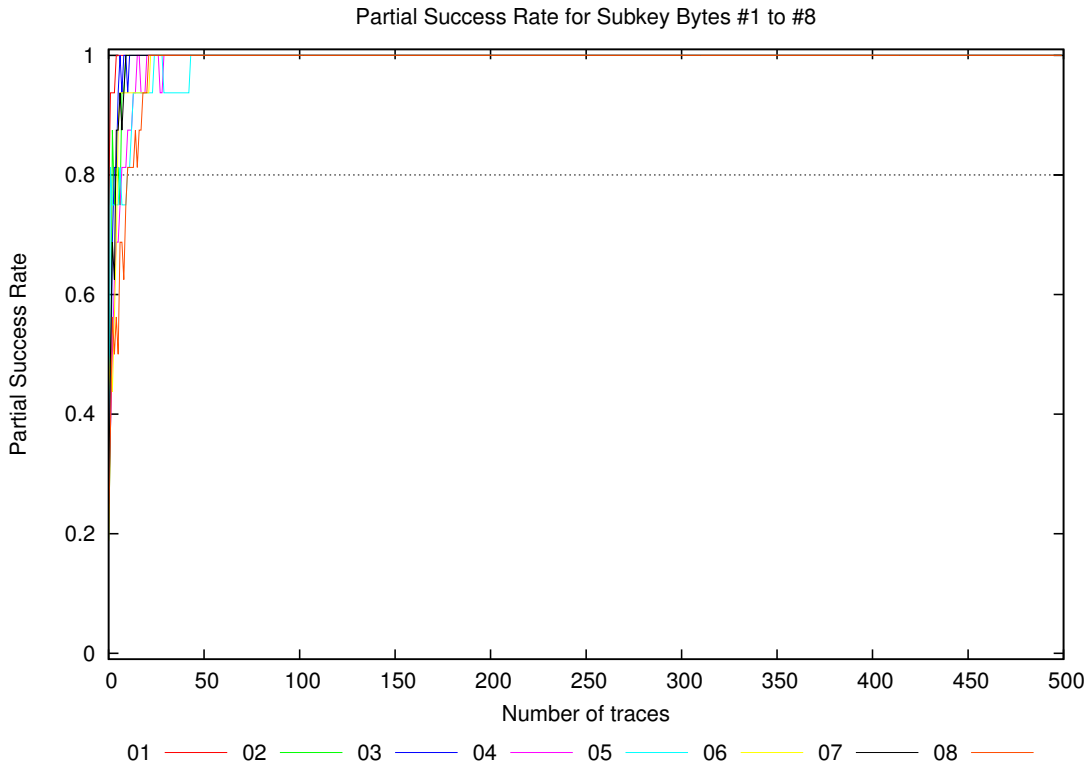

Partial Success Rate for Subkey Byte #12
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
50
100
150
200
250
300
350
400
450
500

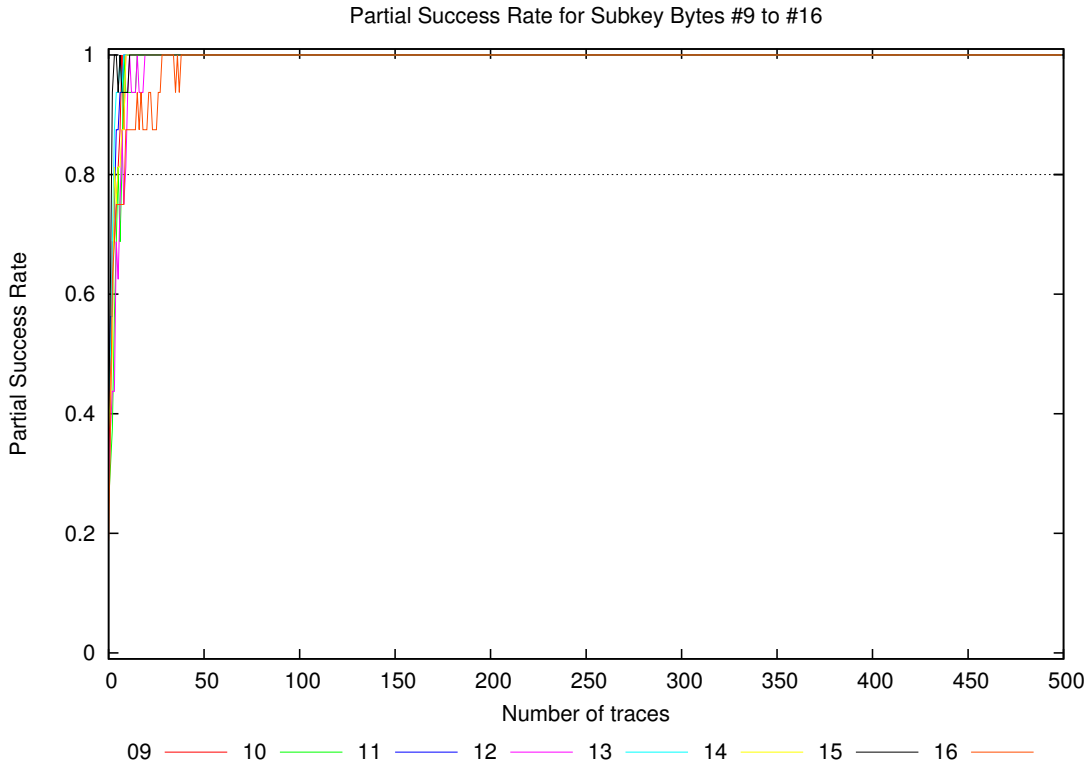

Partial Success Rate for Subkey Byte #13
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
50
100
150
200
250
300
350
400
450
500


Partial Success Rate for Subkey Byte #14
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
50
100
150
200
250
300
350
400
450
500


Partial Success Rate for Subkey Byte #15
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
50
100
150
200
250
300
350
400
450
500

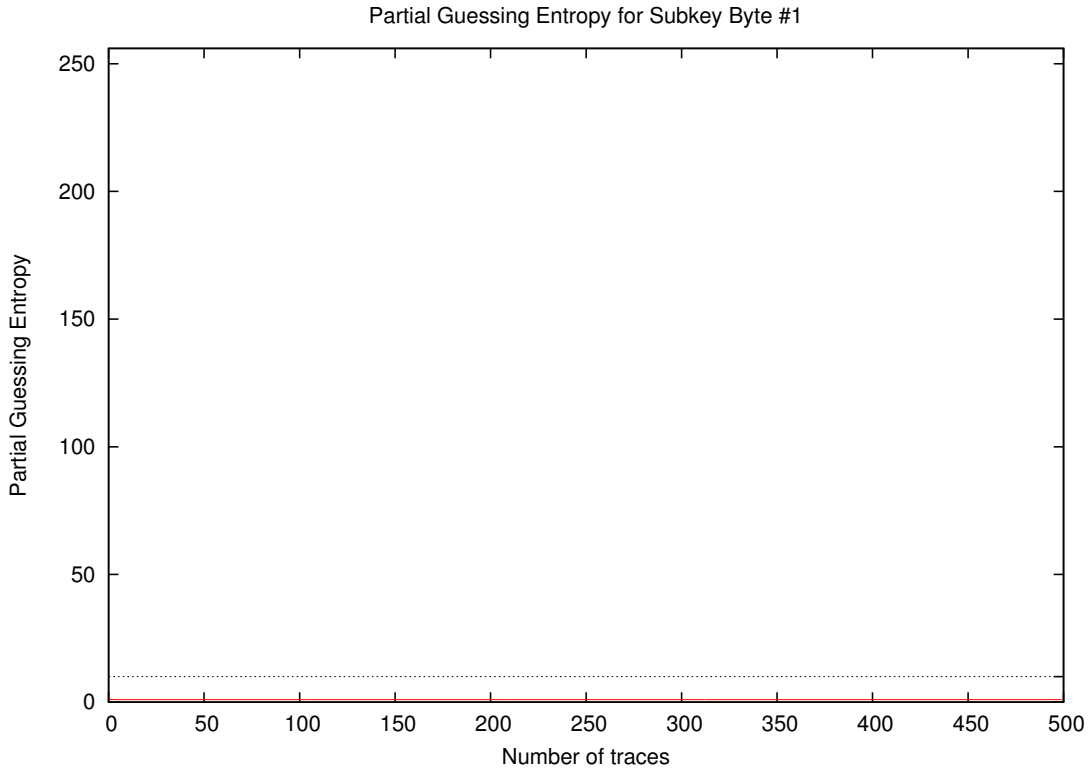

Partial Success Rate for Subkey Byte #16
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
50
100
150
200
250
300
350
400
450
500

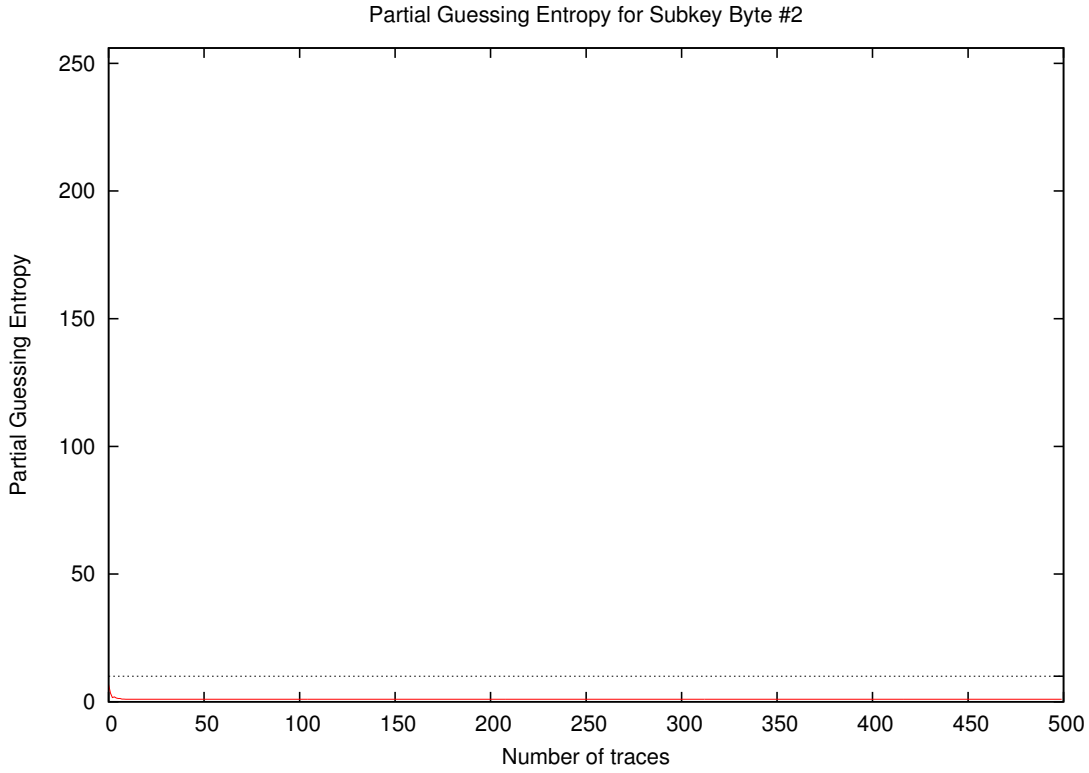

Partial Success Rate for Subkey Bytes #1 to #8
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
50
100
150
200
250
300
350
400
450
500
01
02
03
04
05
06
07
08

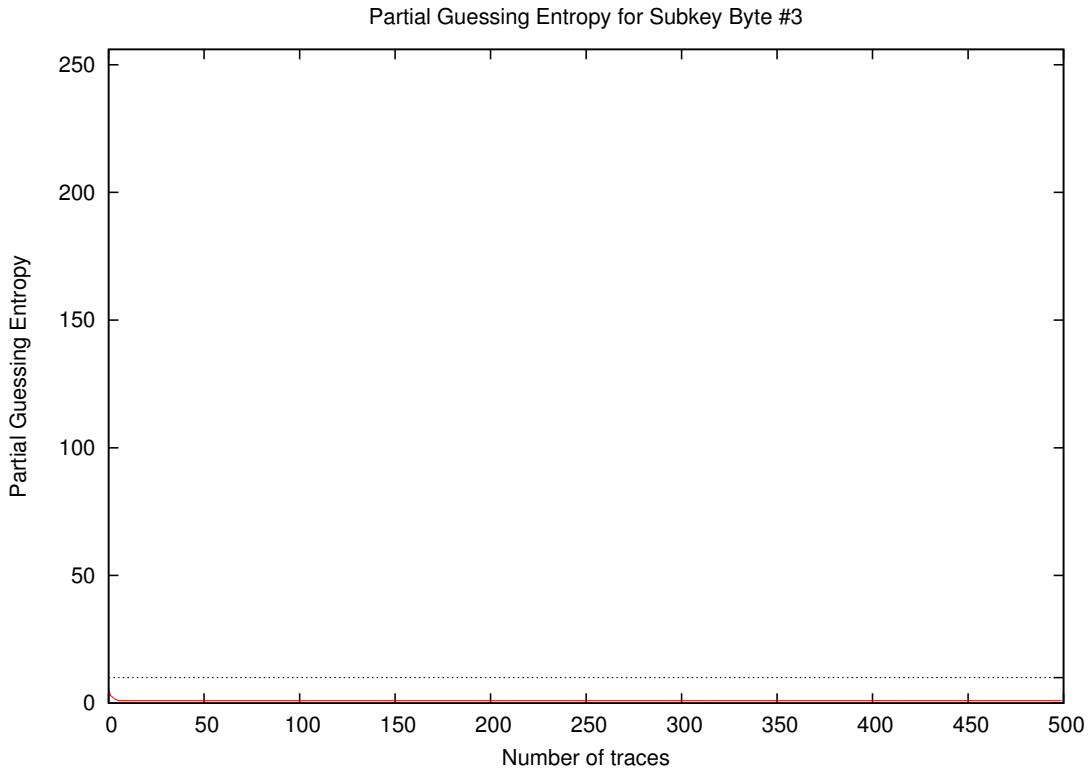

Partial Success Rate for Subkey Bytes #9 to #16
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
50
100
150
200
250
300
350
400
450
500
09
10
11
12
13
14
15
16

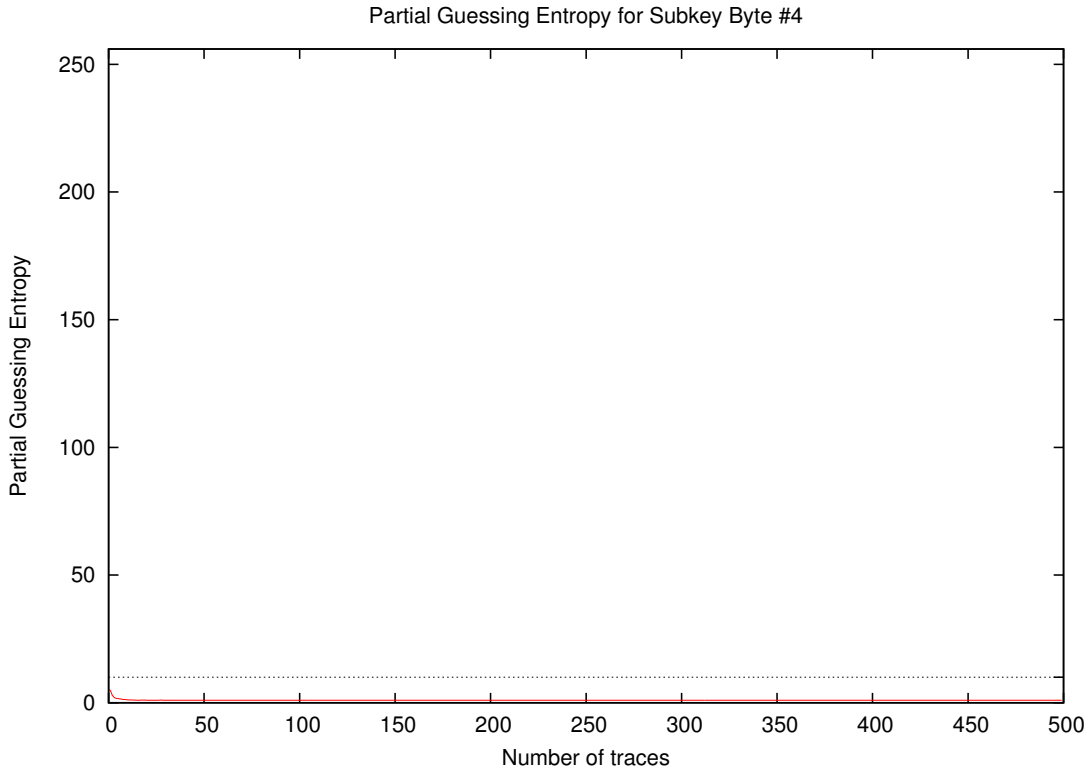
| Traces | Partial Success Rate / Byte | | | | | | | | | | | | | | | | Min | Max | Mean |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | | | |
| 10 | 1.00 | 1.00 | 1.00 | 0.81 | 0.75 | 0.94 | 1.00 | 0.75 | 1.00 | 0.94 | 1.00 | 0.81 | 1.00 | 1.00 | 0.94 | 0.88 | 0.75 | 1.00 | 0.93 |
| 20 | 1.00 | 1.00 | 1.00 | 0.94 | 0.94 | 0.94 | 1.00 | 0.94 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 0.88 | 0.88 | 1.00 | 0.98 |
| 30 | 1.00 | 1.00 | 1.00 | 1.00 | 0.94 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 0.94 | 1.00 | 1.00 |
| 40 | 1.00 | 1.00 | 1.00 | 1.00 | 0.94 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 0.94 | 1.00 | 1.00 |
| 50 | 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 |
| 100 | 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 |
| 200 | 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 |
| 300 | 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 |
| 400 | 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 |
| 500 | 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 |

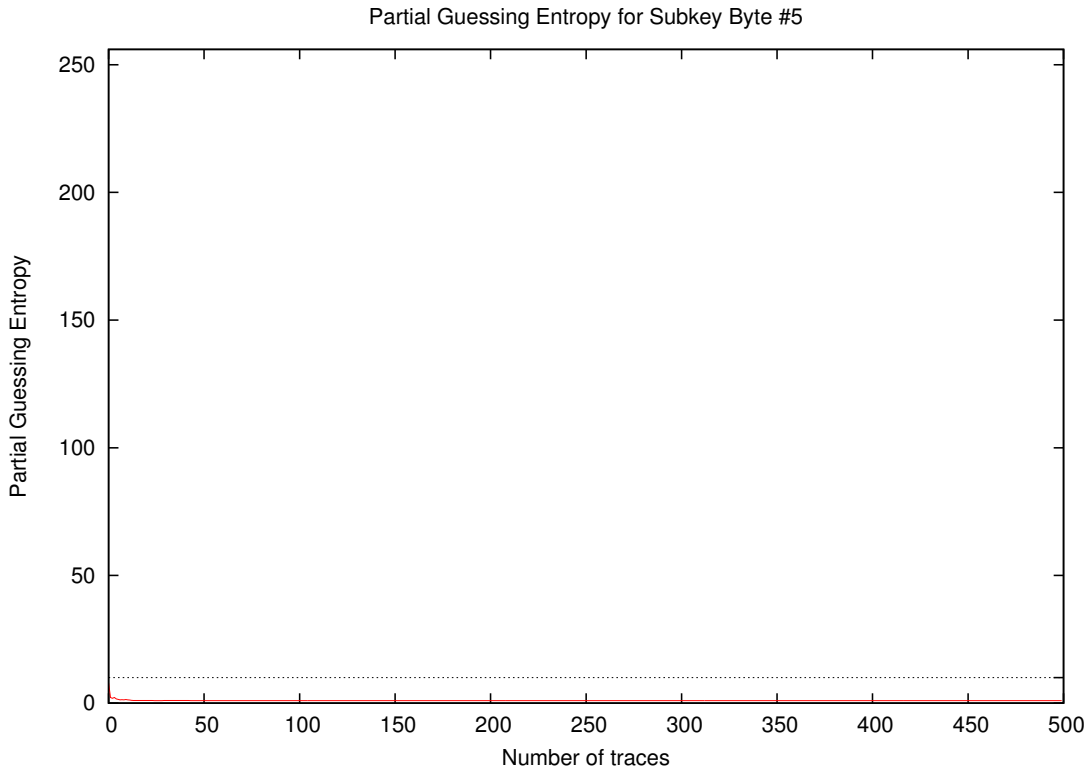
# 4 Partial Guessing Entropy

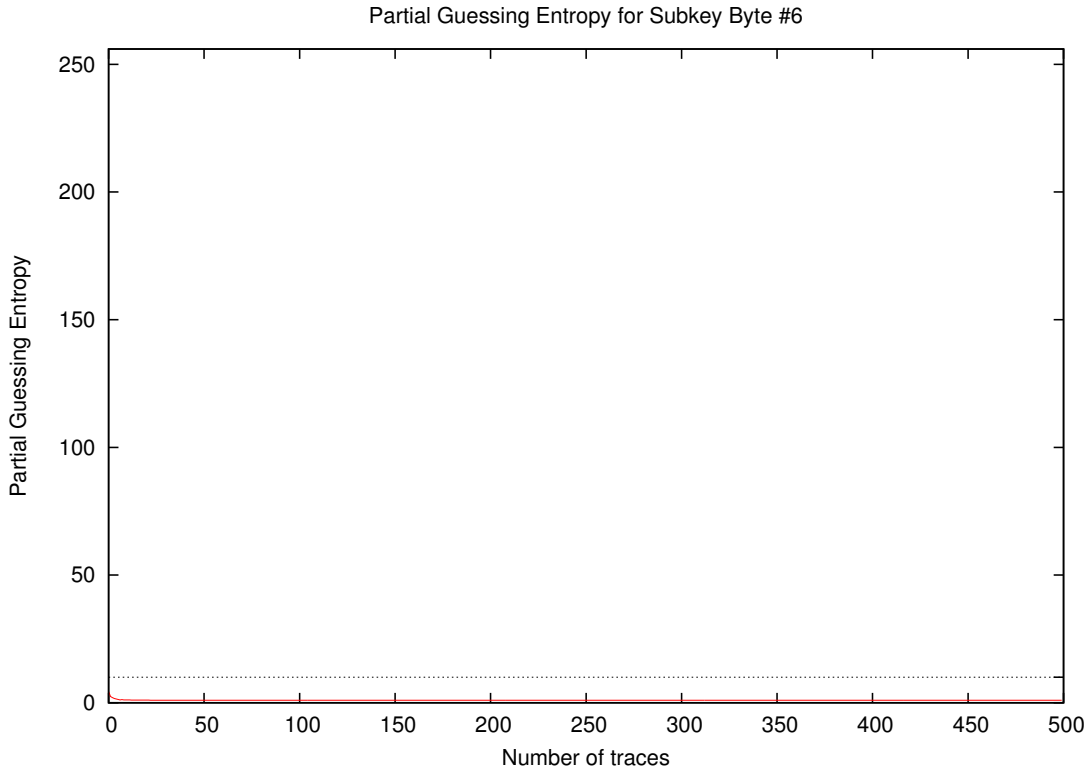


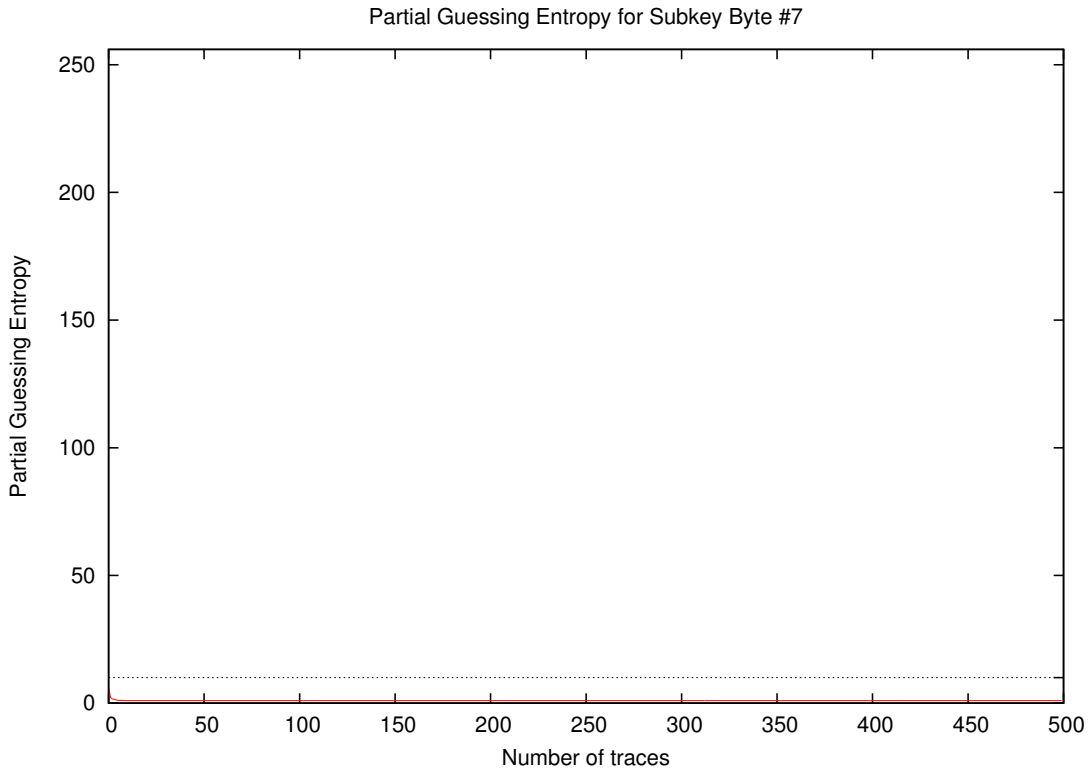



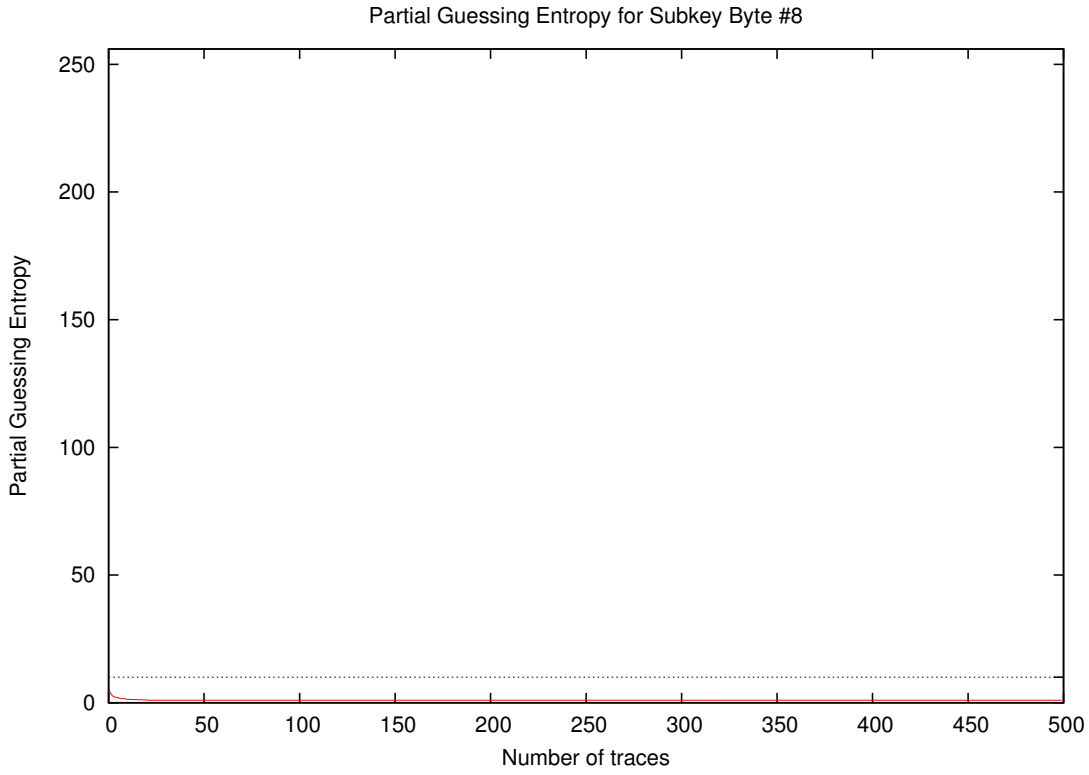

Partial Guessing Entropy for Subkey Byte #3
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
300
350
400
450
500

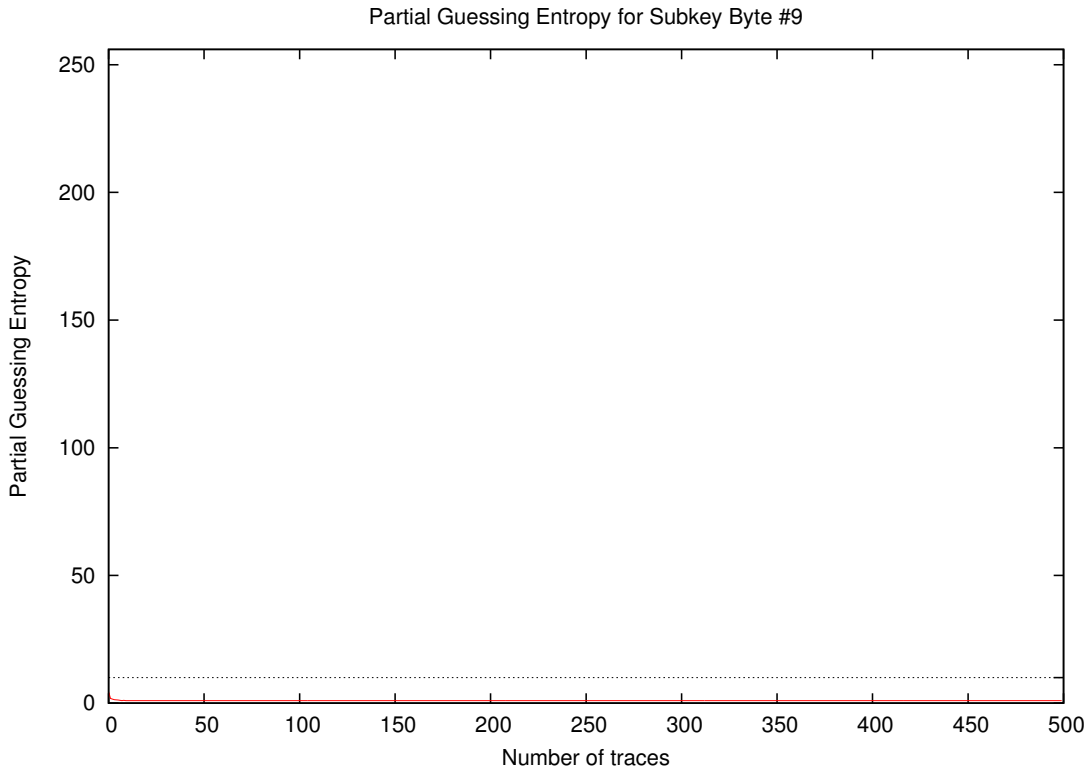

Partial Guessing Entropy for Subkey Byte #4
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
300
350
400
450
500

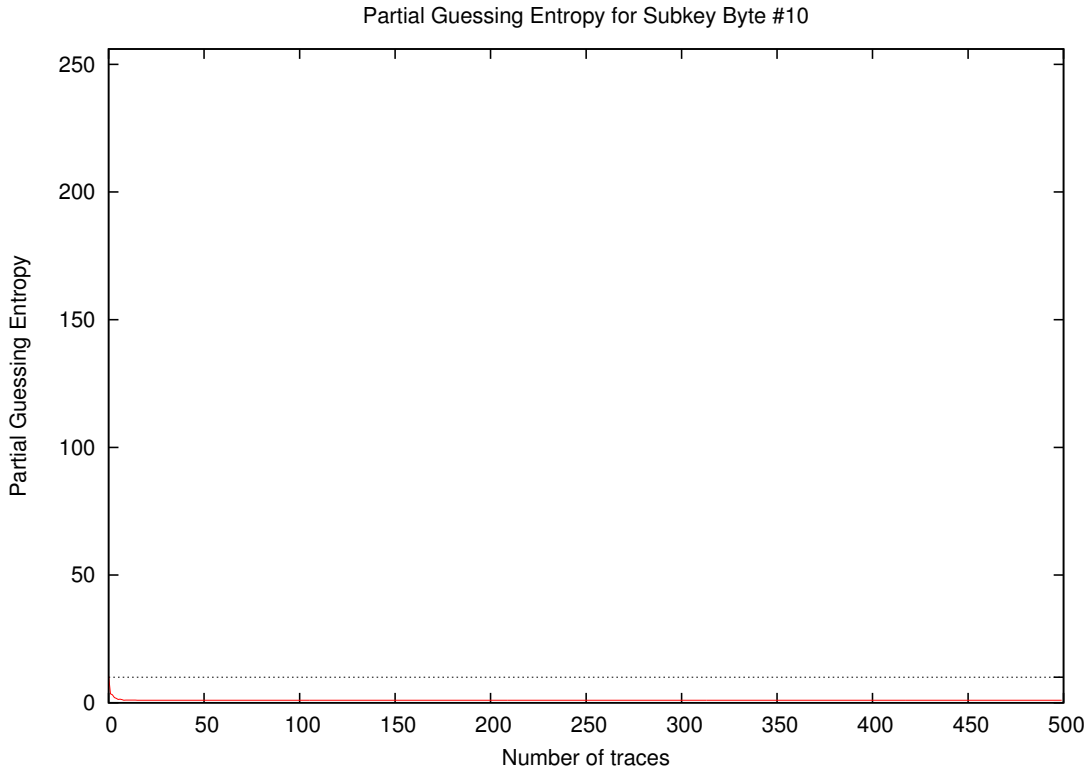

Partial Guessing Entropy for Subkey Byte #5
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
300
350
400
450
500

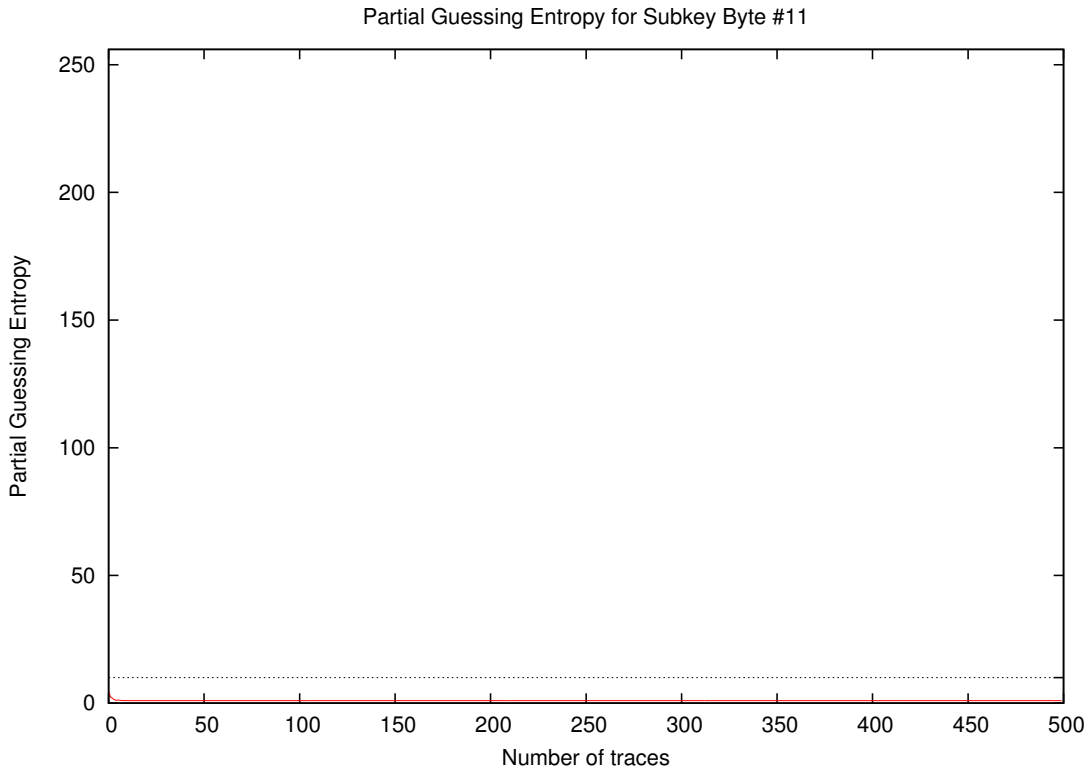

Partial Guessing Entropy for Subkey Byte #6
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
300
350
400
450
500

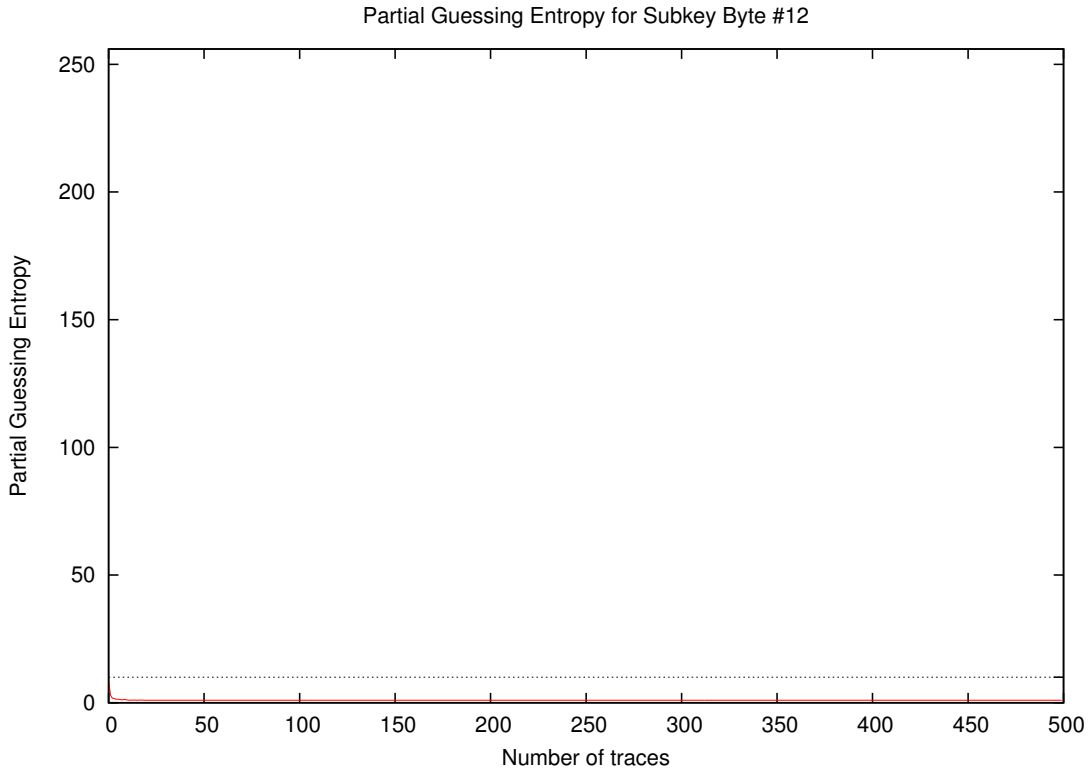

Partial Guessing Entropy for Subkey Byte #7
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
300
350
400
450
500

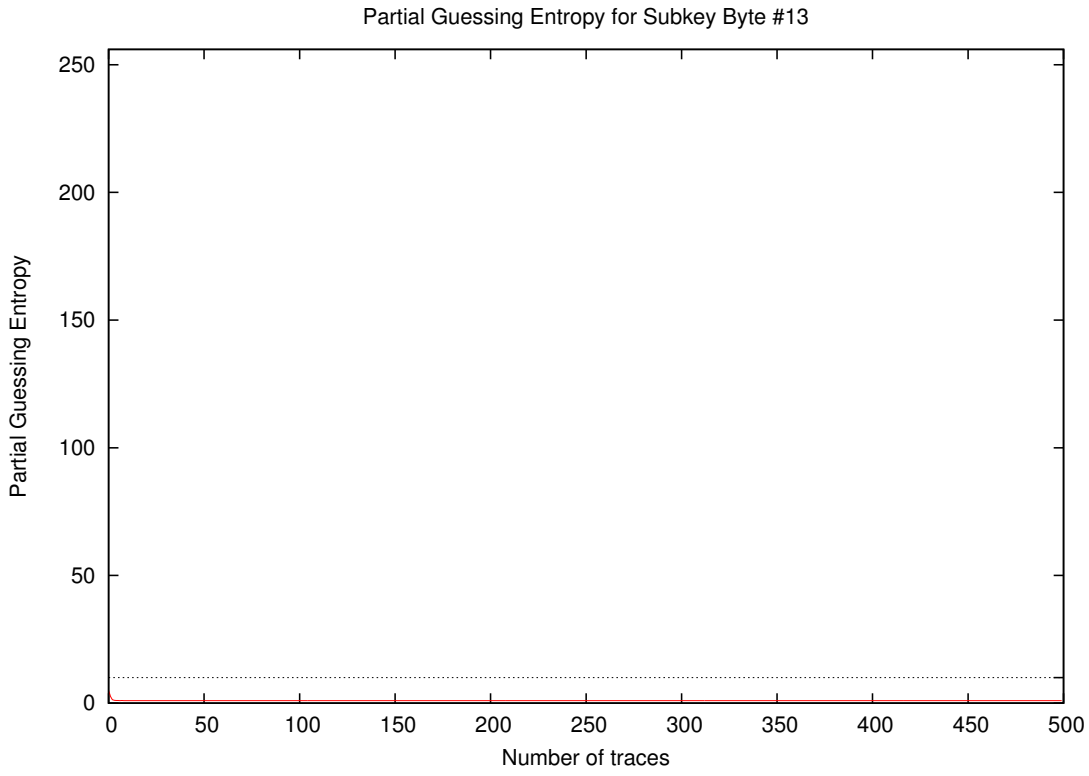

Partial Guessing Entropy for Subkey Byte #8
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
300
350
400
450
500

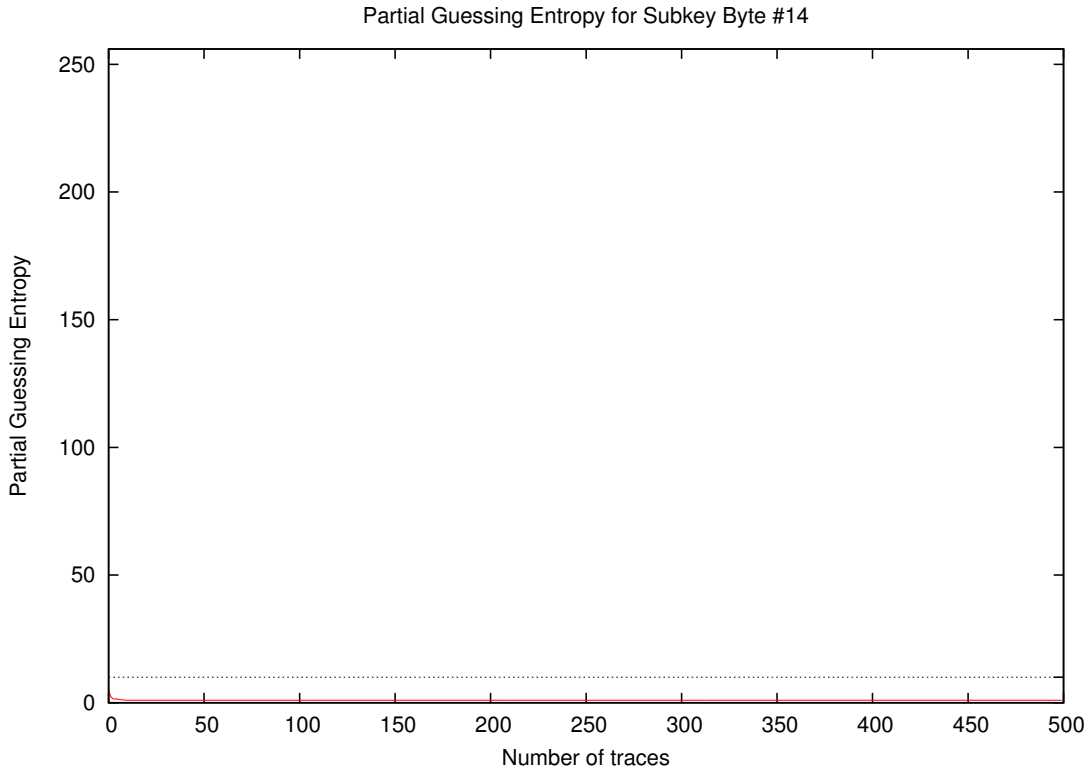

Partial Guessing Entropy for Subkey Byte #9
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
300
350
400
450
500

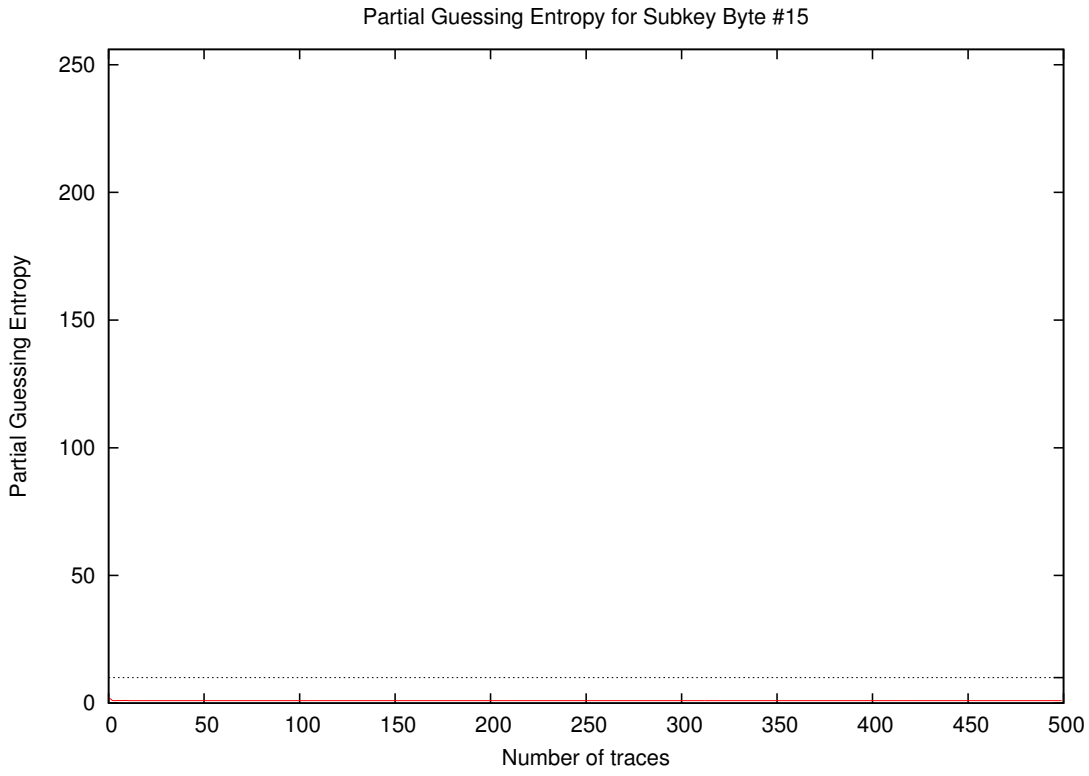

Partial Guessing Entropy for Subkey Byte #10
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
300
350
400
450
500

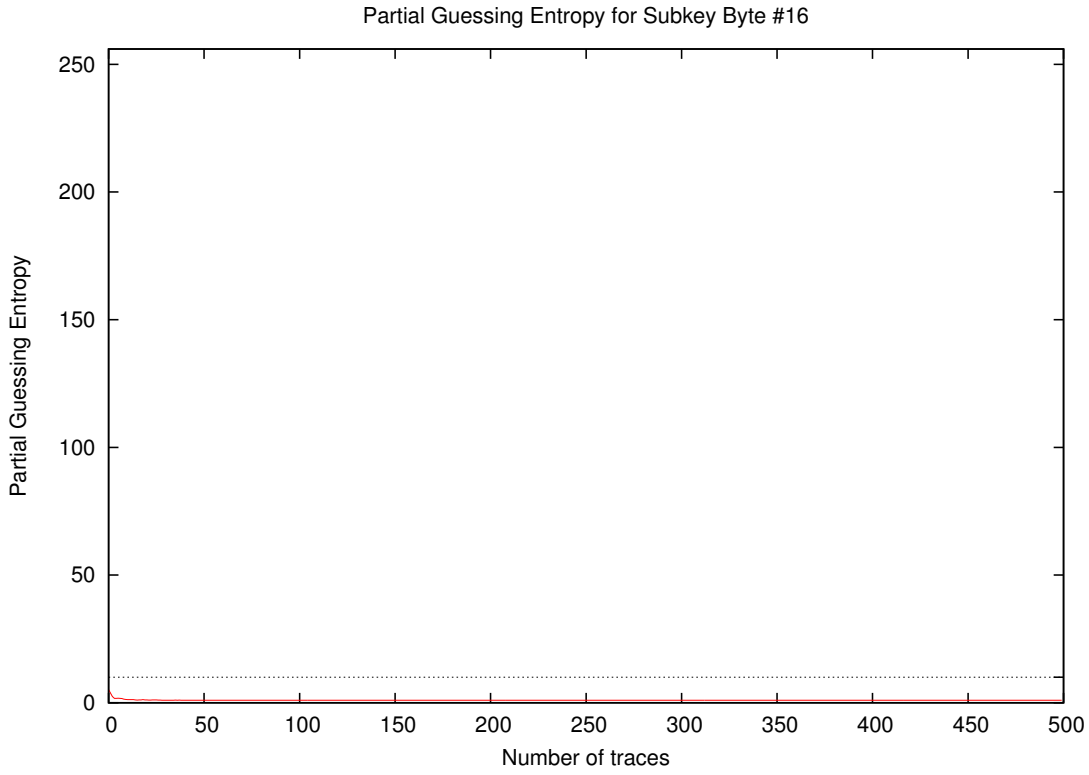

Partial Guessing Entropy for Subkey Byte #11
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
300
350
400
450
500

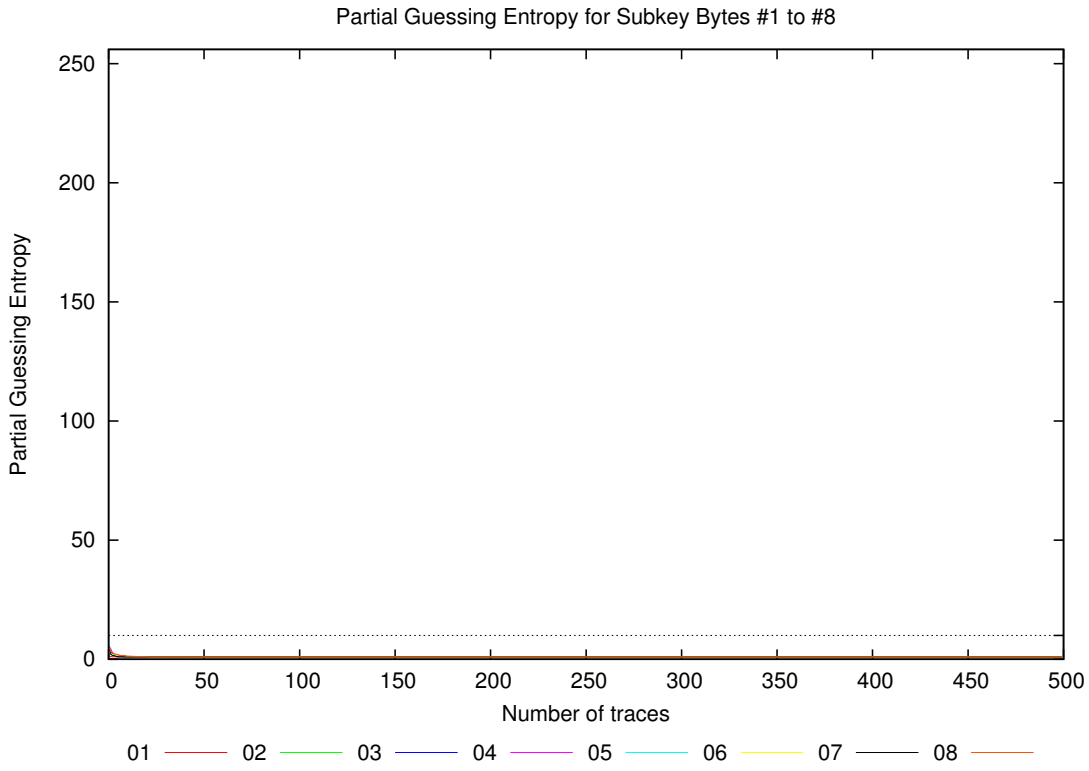

Partial Guessing Entropy for Subkey Byte #12
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
300
350
400
450
500

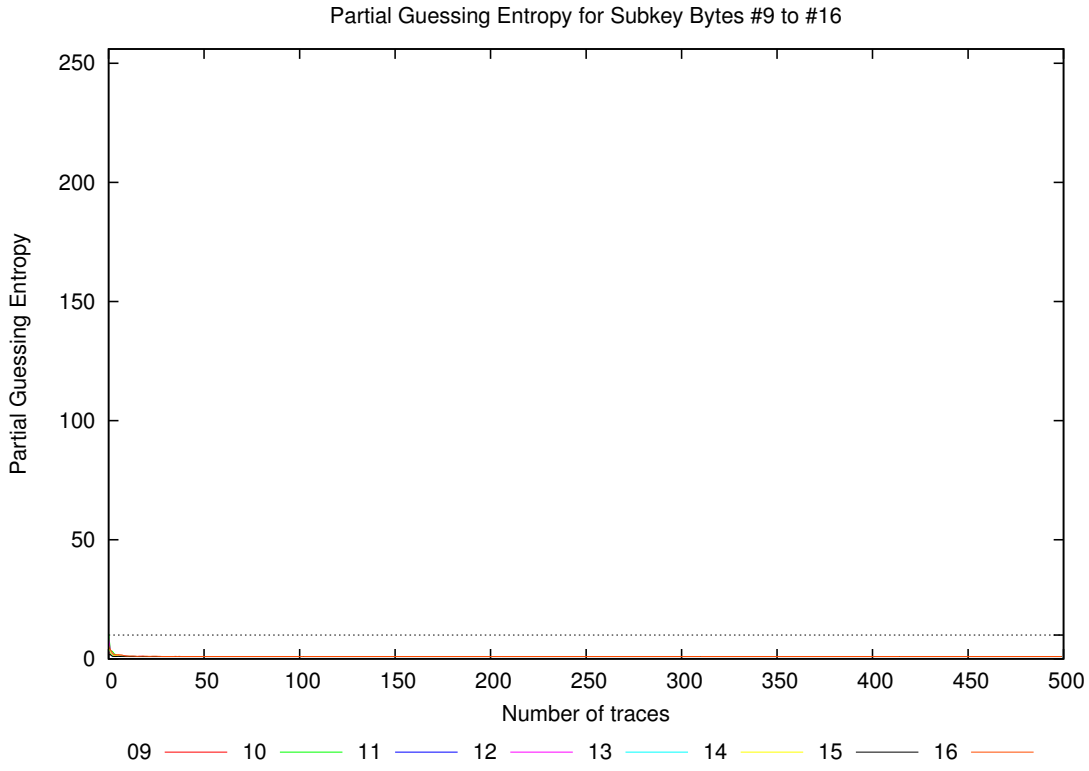

Partial Guessing Entropy for Subkey Byte #13
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
300
350
400
450
500


Partial Guessing Entropy for Subkey Byte #14
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
300
350
400
450
500


Partial Guessing Entropy for Subkey Byte #15
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
300
350
400
450
500


Partial Guessing Entropy for Subkey Byte #16
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
300
350
400
450
500


Partial Guessing Entropy for Subkey Bytes #1 to #8
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
300
350
400
450
500
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
300
350
400
450
500
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 | 1.0 | 1.0 | 1.0 | 1.2 | 1.4 | 1.1 | 1.0 | 1.4 | 1.0 | 1.1 | 1.0 | 1.2 | 1.0 | 1.0 | 1.1 | 1.2 | 1.0 | 1.4 | 1.1 |
| 20 | 1.0 | 1.0 | 1.0 | 1.1 | 1.1 | 1.1 | 1.0 | 1.1 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.1 | 1.0 | 1.1 | 1.0 |
| 30 | 1.0 | 1.0 | 1.0 | 1.0 | 1.1 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.1 | 1.0 |
| 40 | 1.0 | 1.0 | 1.0 | 1.0 | 1.1 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.1 | 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 |
| 100 | 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 |
| 200 | 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 |
| 300 | 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 |
| 400 | 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 |
| 500 | 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 |