DPA Contest v4.2
Evaluation results

Wei Cheng, Yuchen Cao, Yongbin Zhou, Chao Zheng, Hailong Zhang, Wei Yang

January 2017

1 Introduction

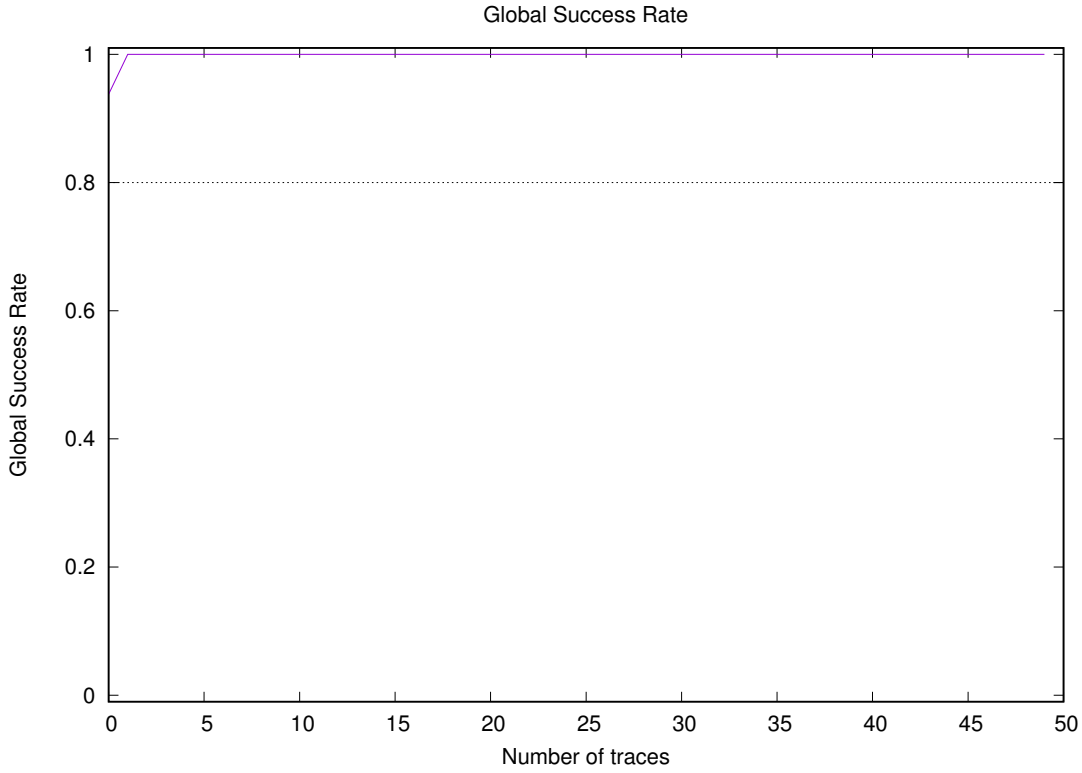
1.1 About the attack

- **Sender/Team:** Wei Cheng, Yuchen Cao, Yongbin Zhou, Chao Zheng, Hailong Zhang, Wei Yang
- **Institution:** State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences
- **Language:** C++
- **Operating system:** Linux
- **Attacked subkey:** 0

1.2 About the evaluation

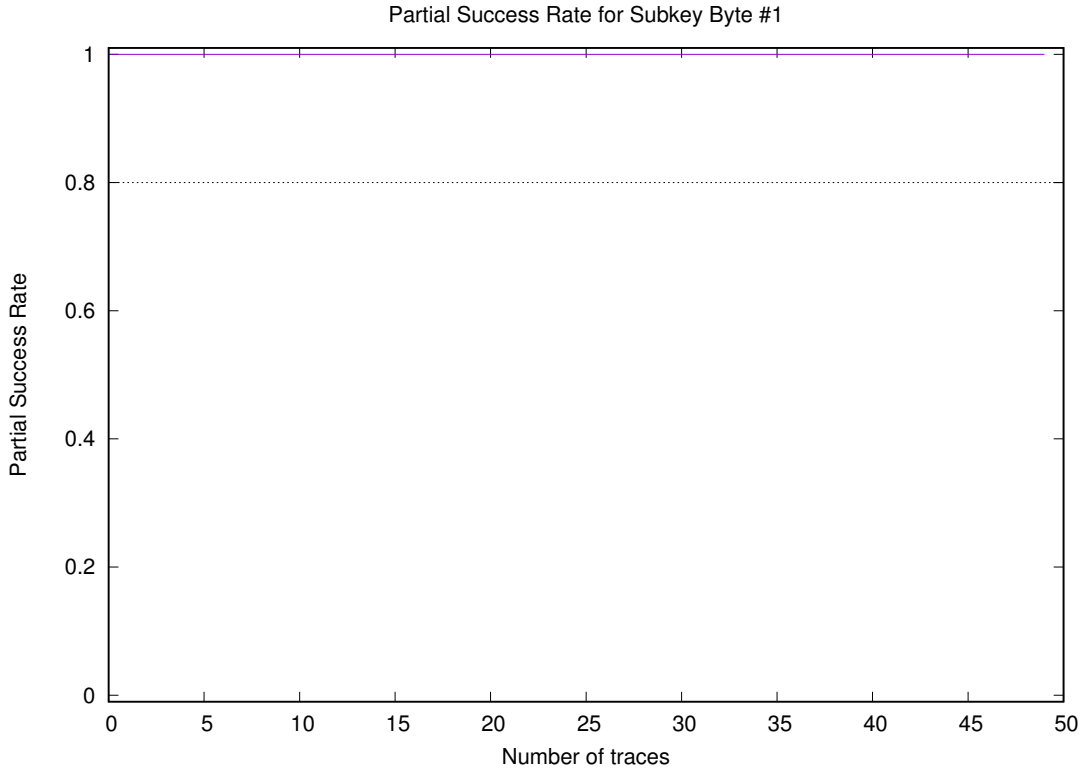
- **Date of evaluation:** January 2017

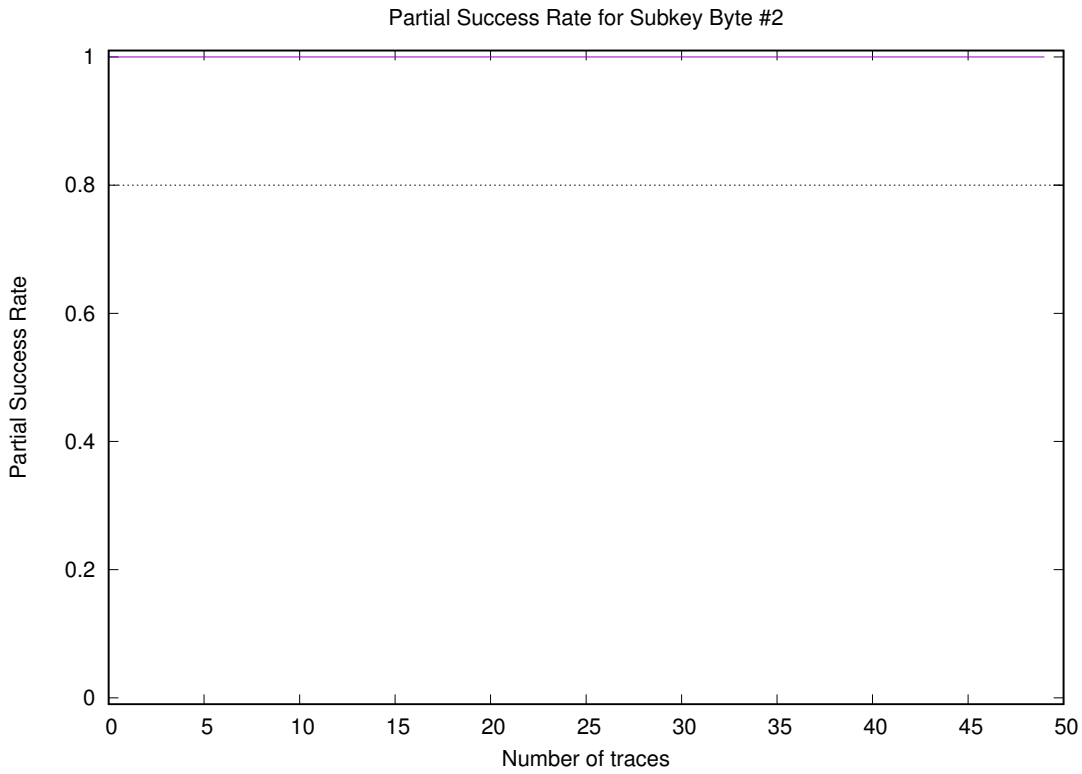
2 Global Success Rate

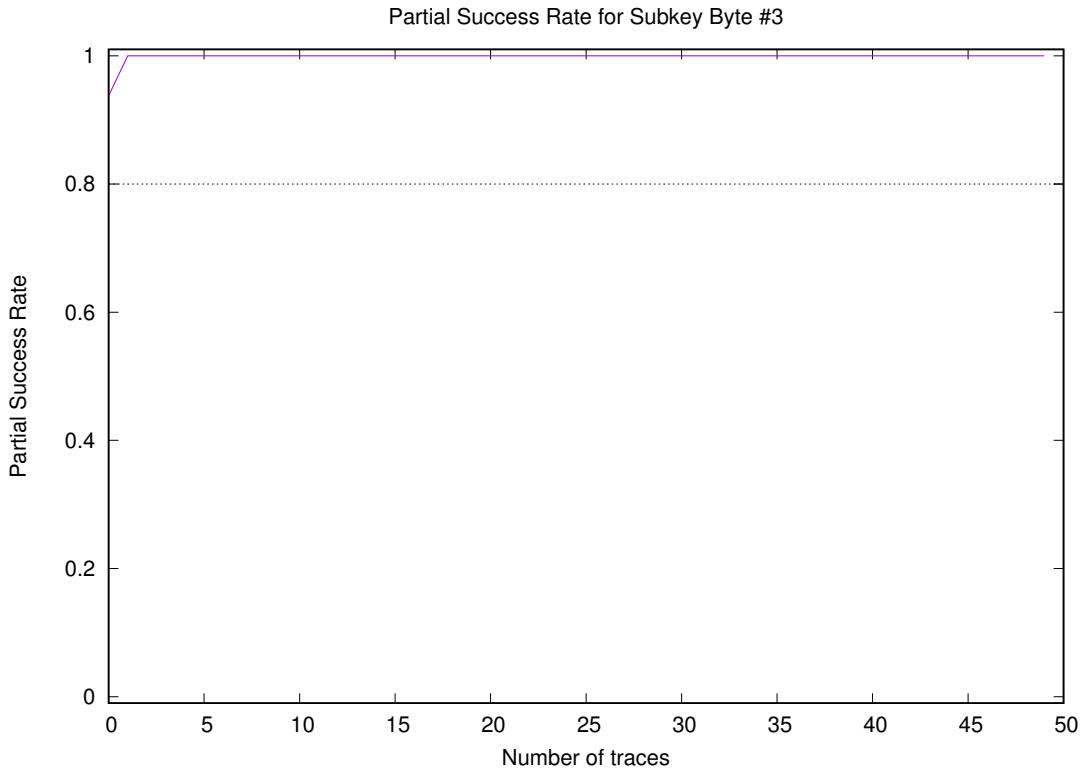


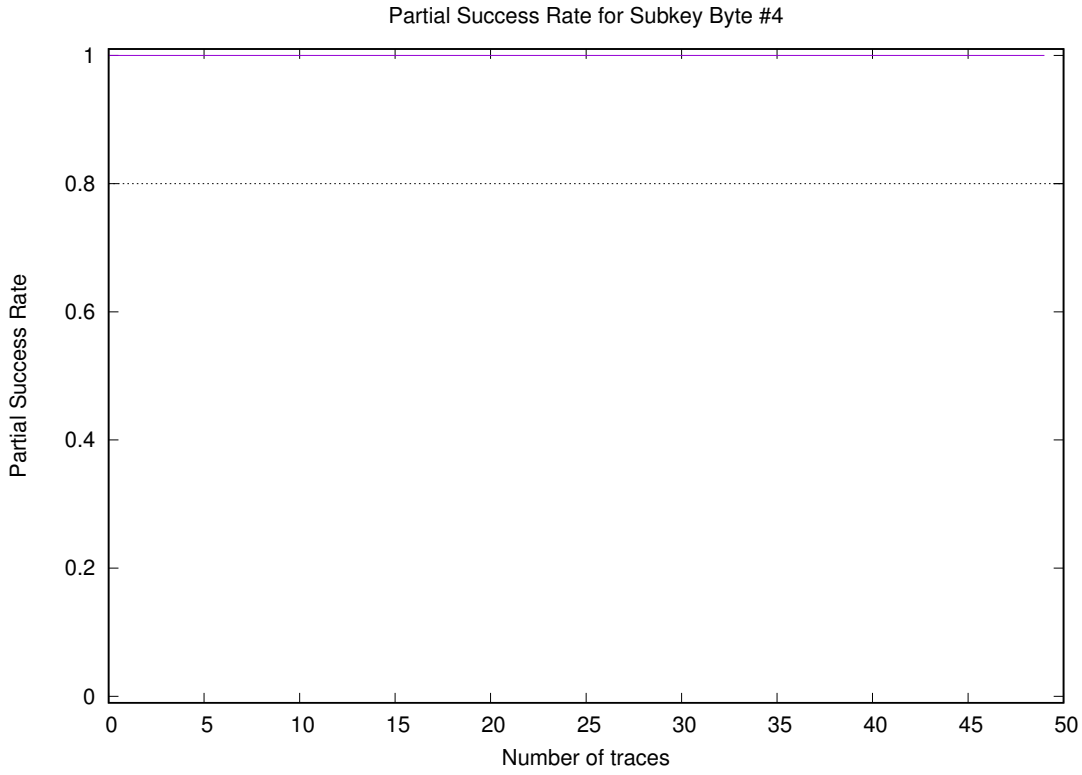
Number of traces	Global Success Rate
10	1.00
20	1.00
30	1.00
40	1.00
50	1.00

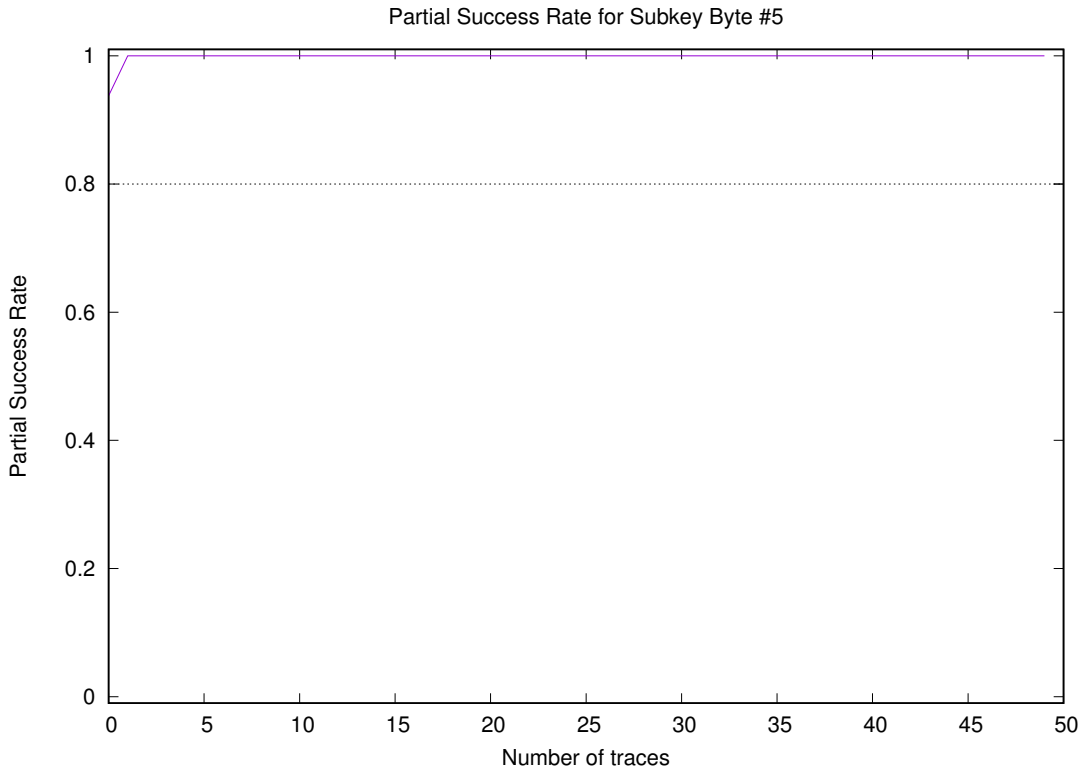
3 Partial Success Rate

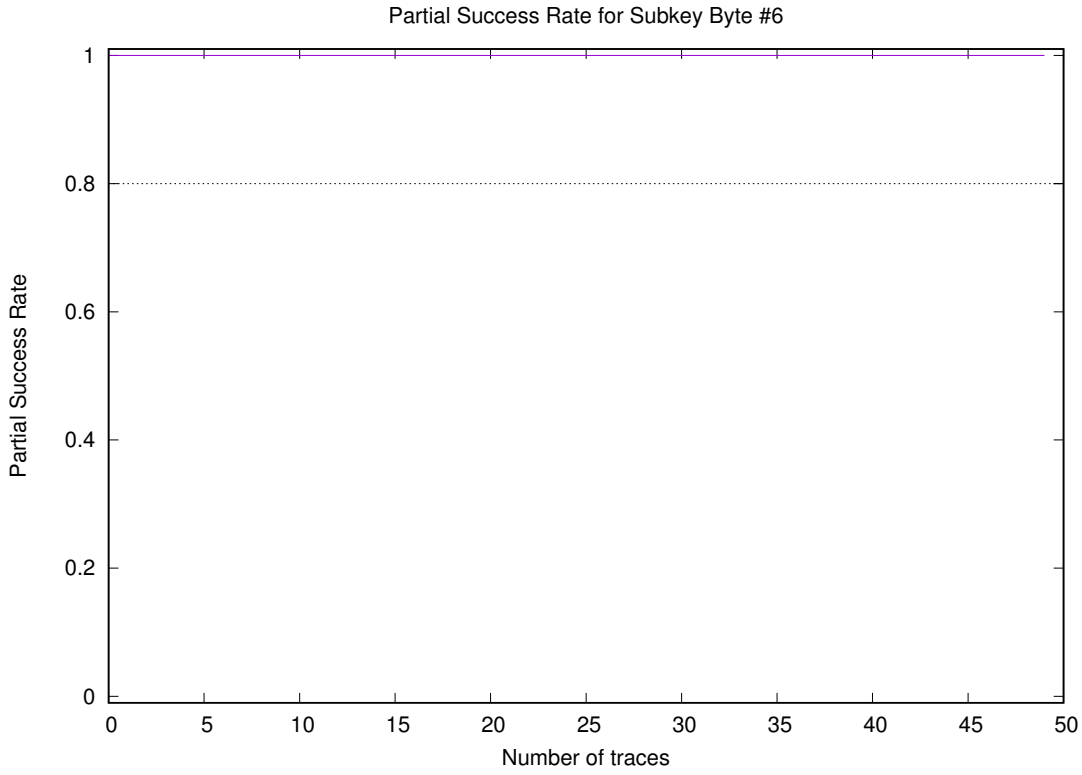


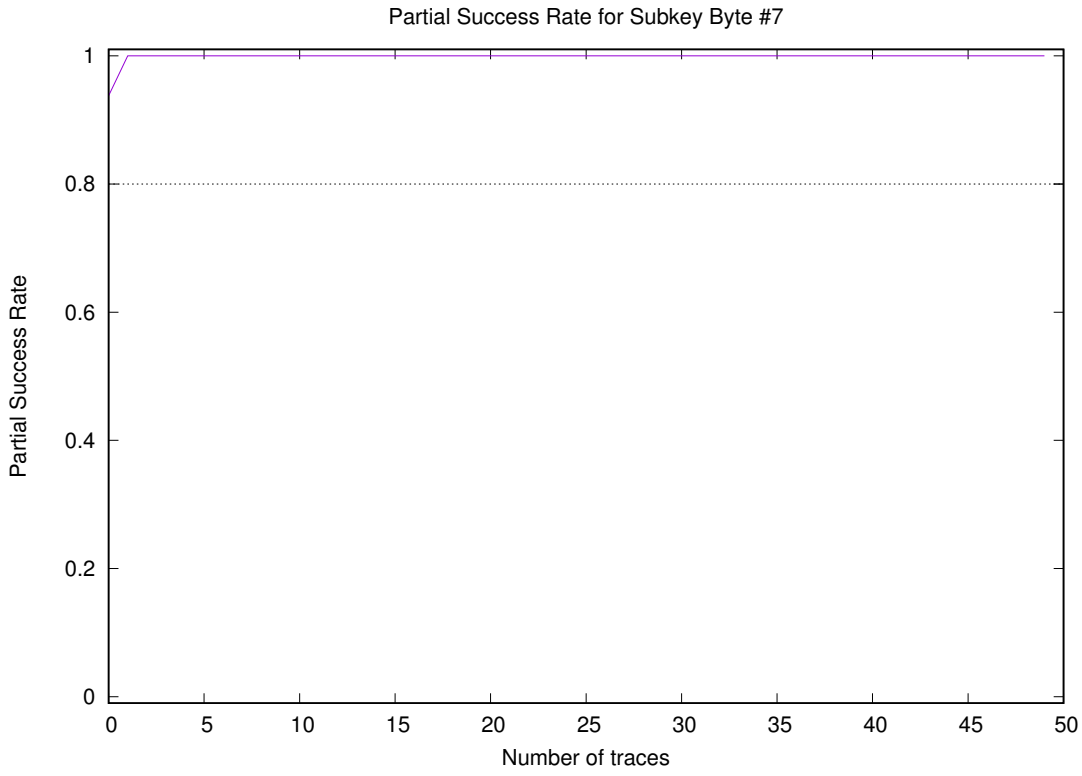


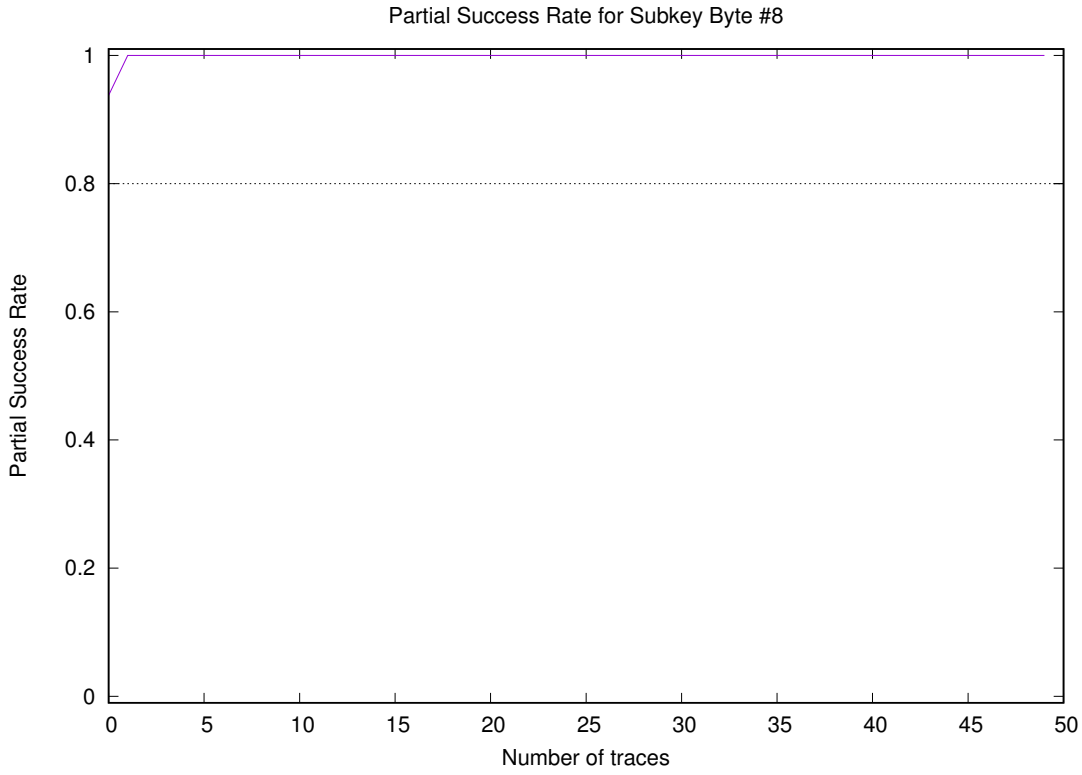

Partial Success Rate for Subkey Byte #3
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
5
10
15
20
25
30
35
40
45
50

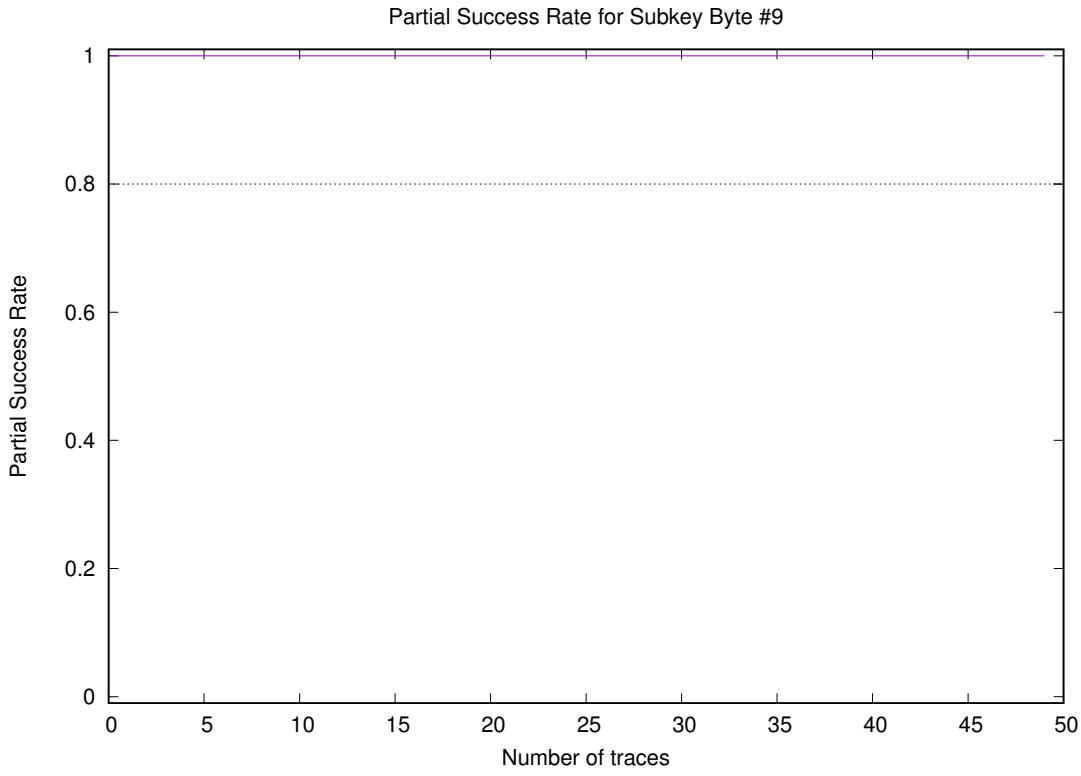

Partial Success Rate for Subkey Byte #4
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
5
10
15
20
25
30
35
40
45
50

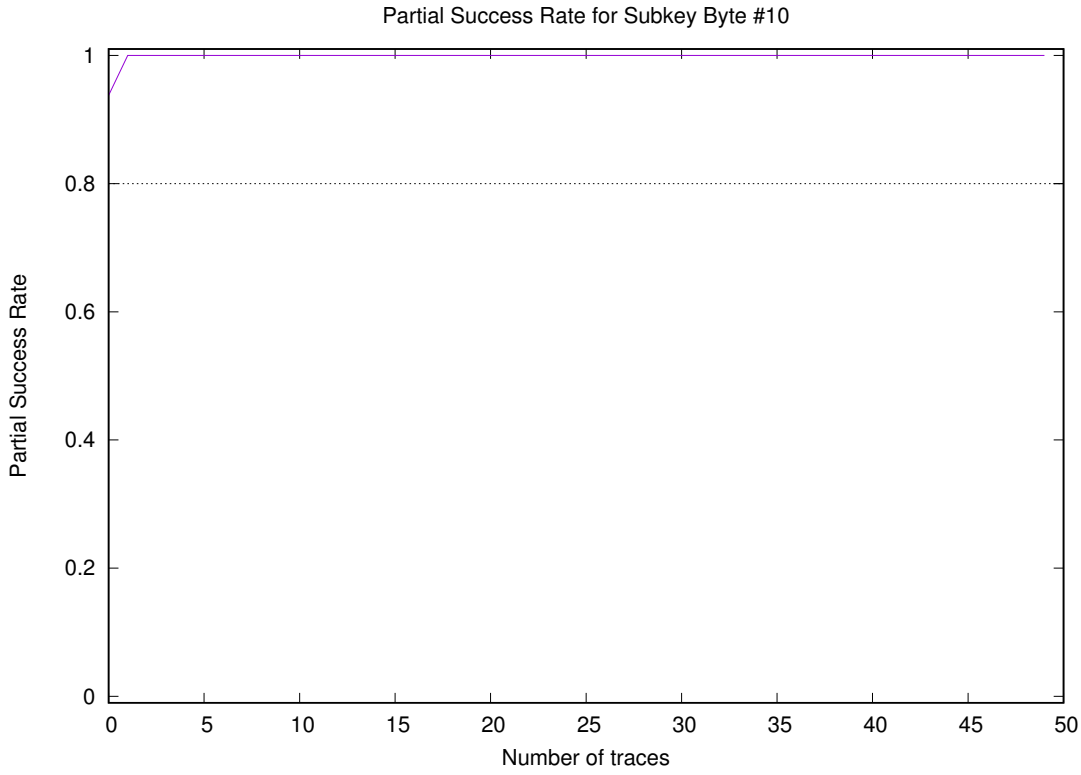

Partial Success Rate for Subkey Byte #5
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
5
10
15
20
25
30
35
40
45
50

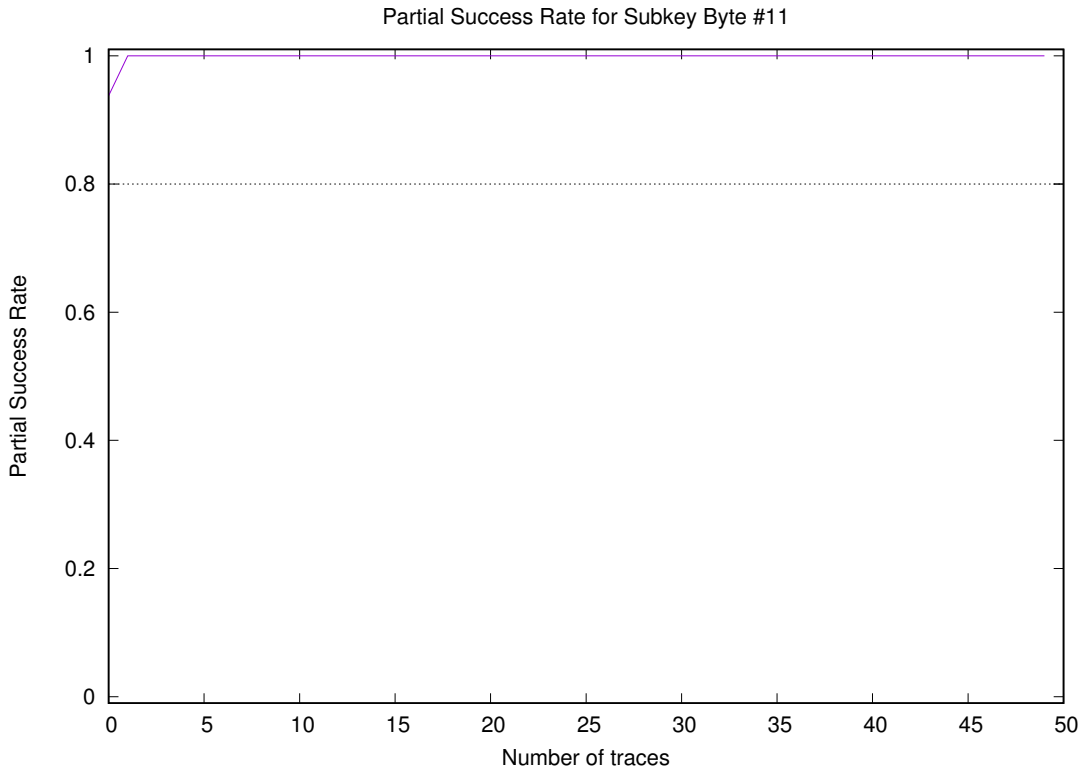

Partial Success Rate for Subkey Byte #6
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
5
10
15
20
25
30
35
40
45
50

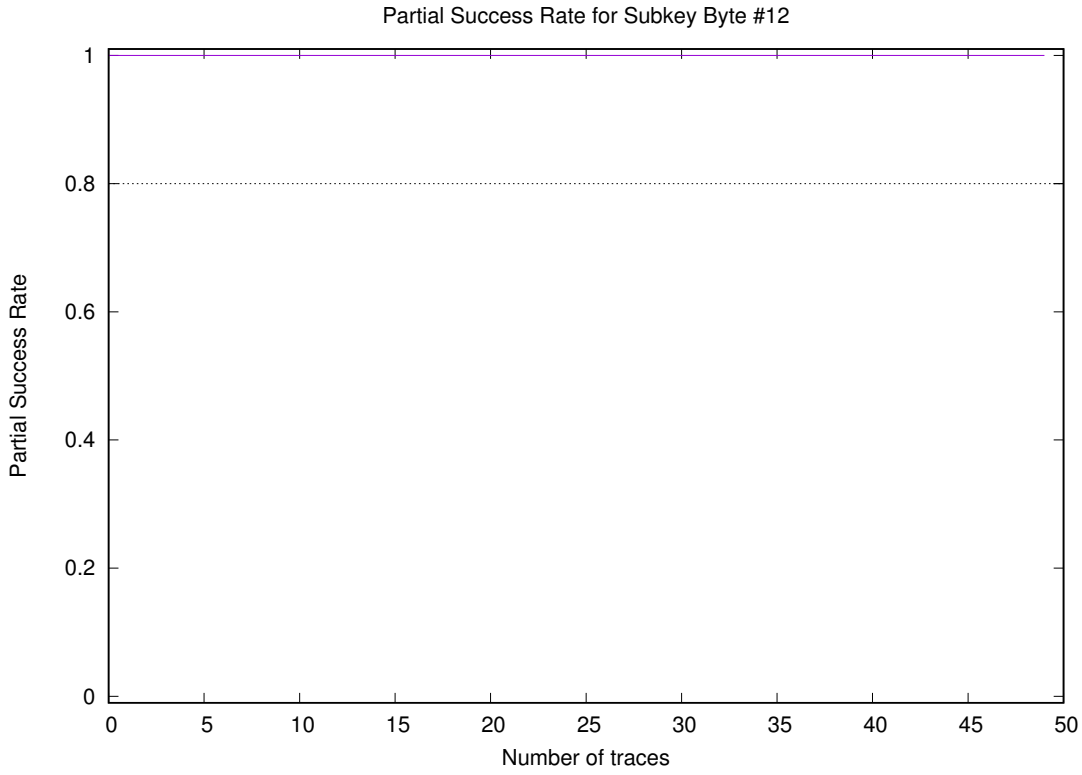

Partial Success Rate for Subkey Byte #7
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
5
10
15
20
25
30
35
40
45
50

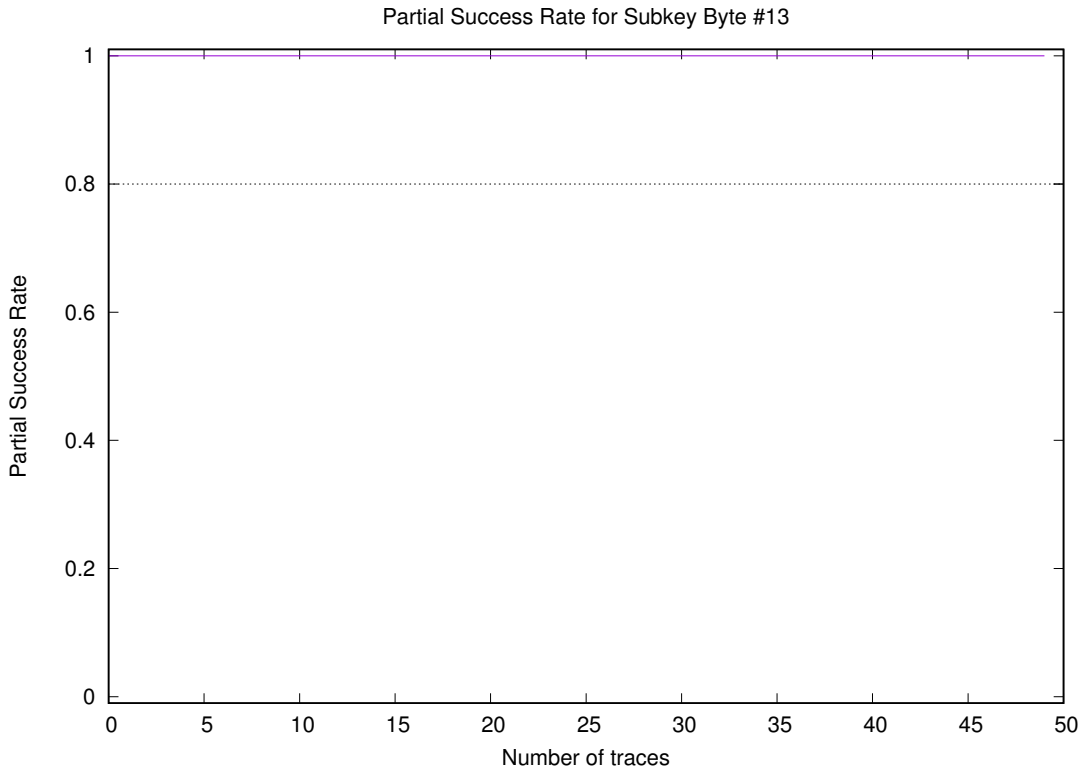

Partial Success Rate for Subkey Byte #8
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
5
10
15
20
25
30
35
40
45
50

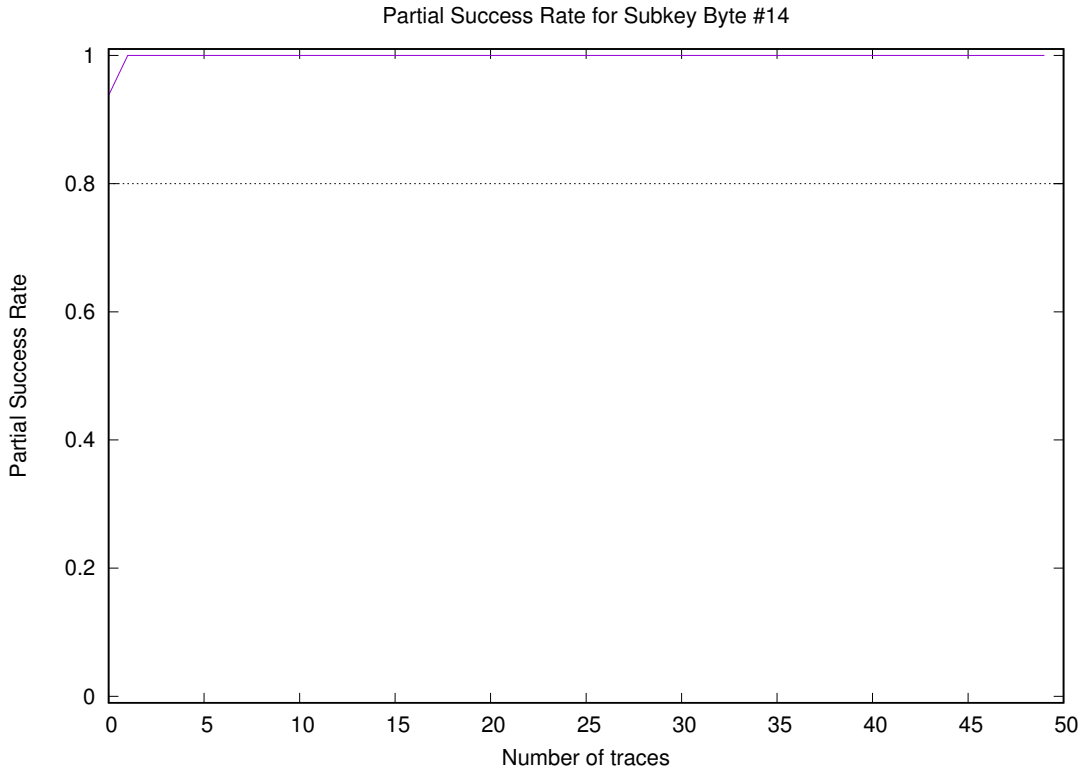

Partial Success Rate for Subkey Byte #9
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
5
10
15
20
25
30
35
40
45
50

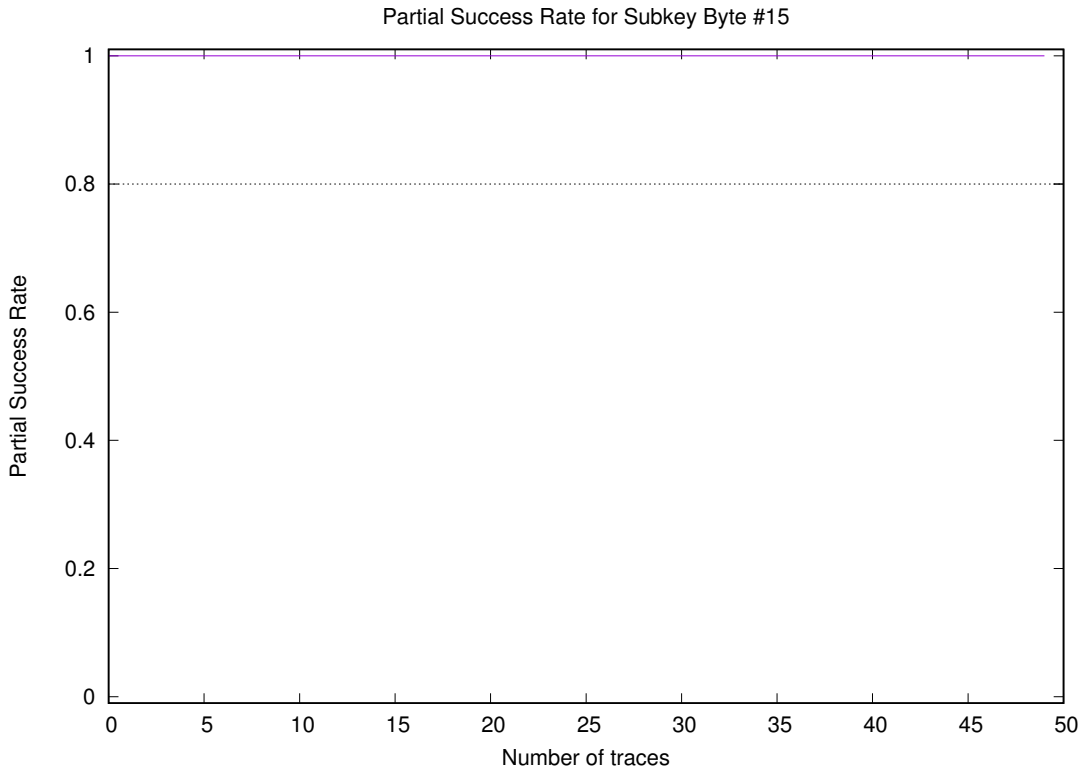

Partial Success Rate for Subkey Byte #10
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
5
10
15
20
25
30
35
40
45
50

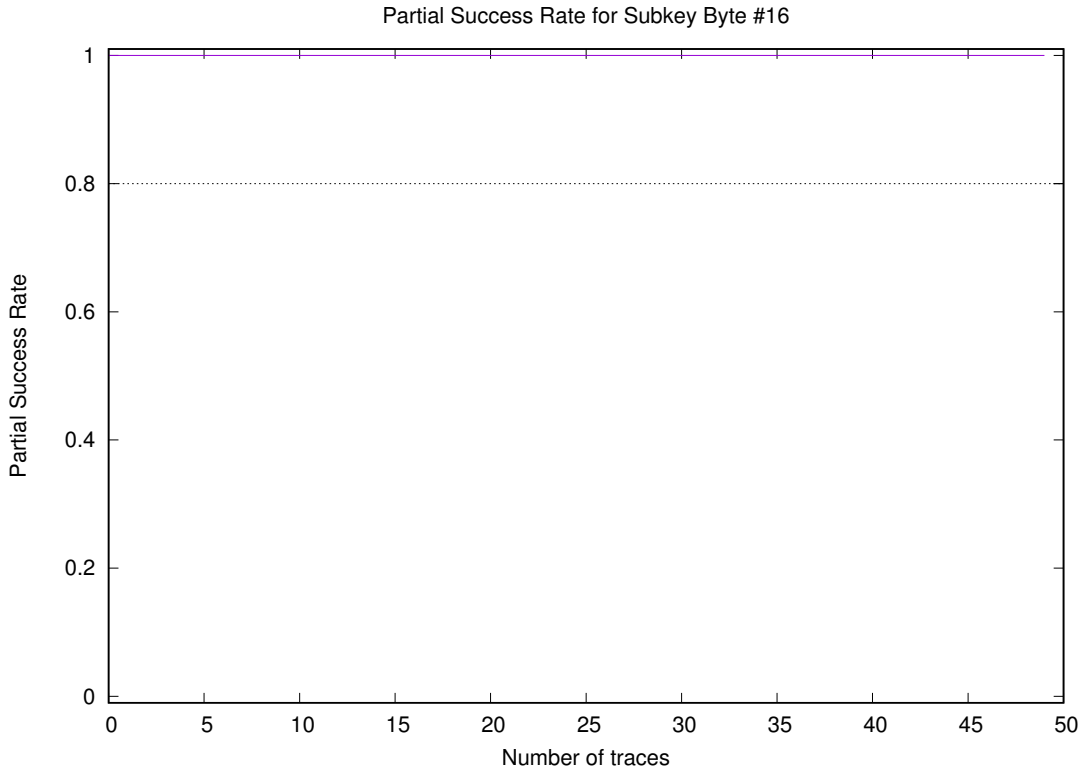

Partial Success Rate for Subkey Byte #11
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
5
10
15
20
25
30
35
40
45
50

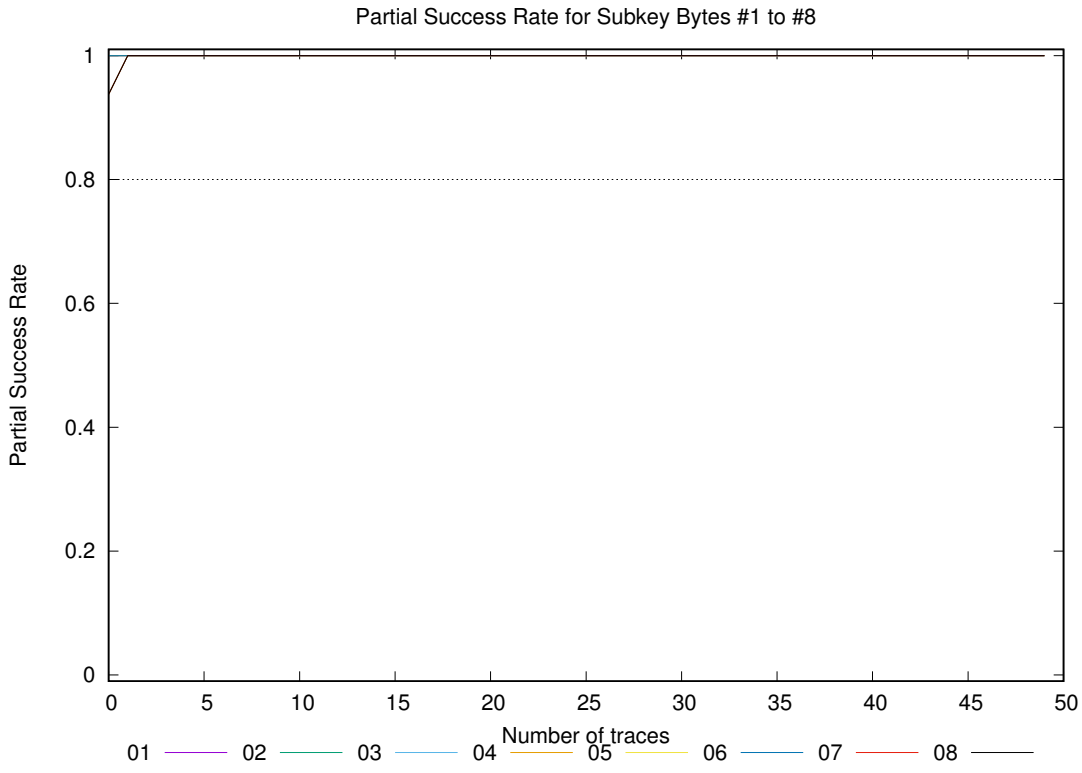

Partial Success Rate for Subkey Byte #12
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
5
10
15
20
25
30
35
40
45
50

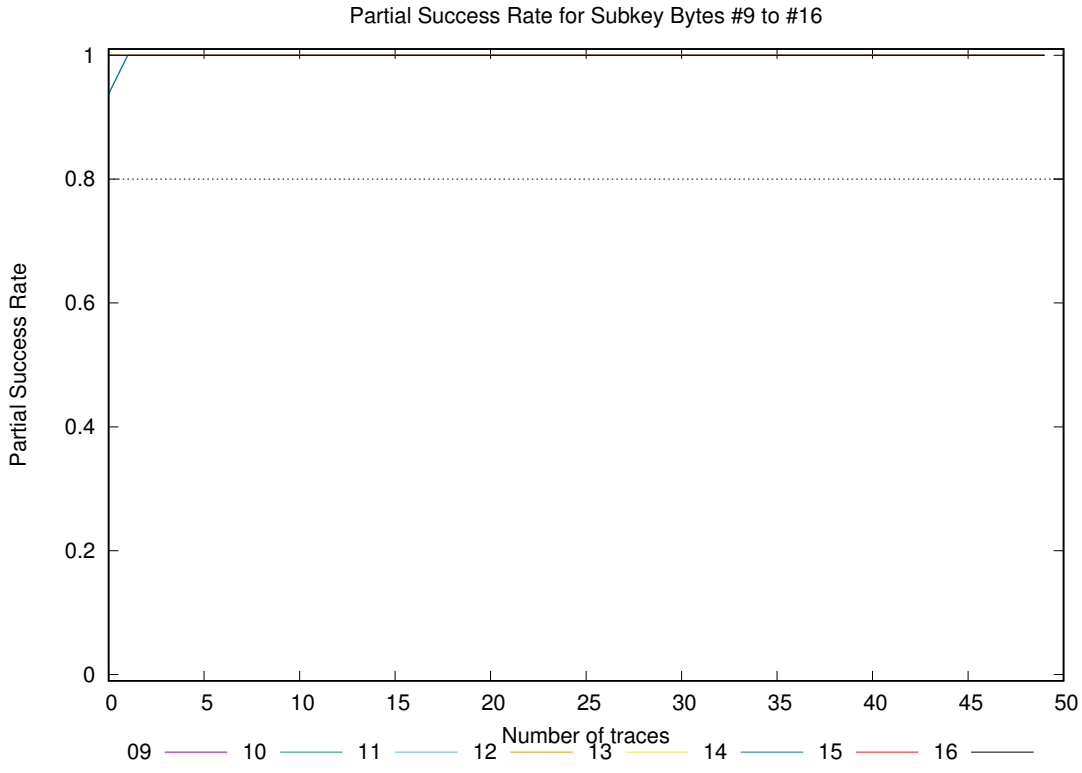

Partial Success Rate for Subkey Byte #13
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
5
10
15
20
25
30
35
40
45
50


Partial Success Rate for Subkey Byte #14
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
5
10
15
20
25
30
35
40
45
50


Partial Success Rate for Subkey Byte #15
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
5
10
15
20
25
30
35
40
45
50

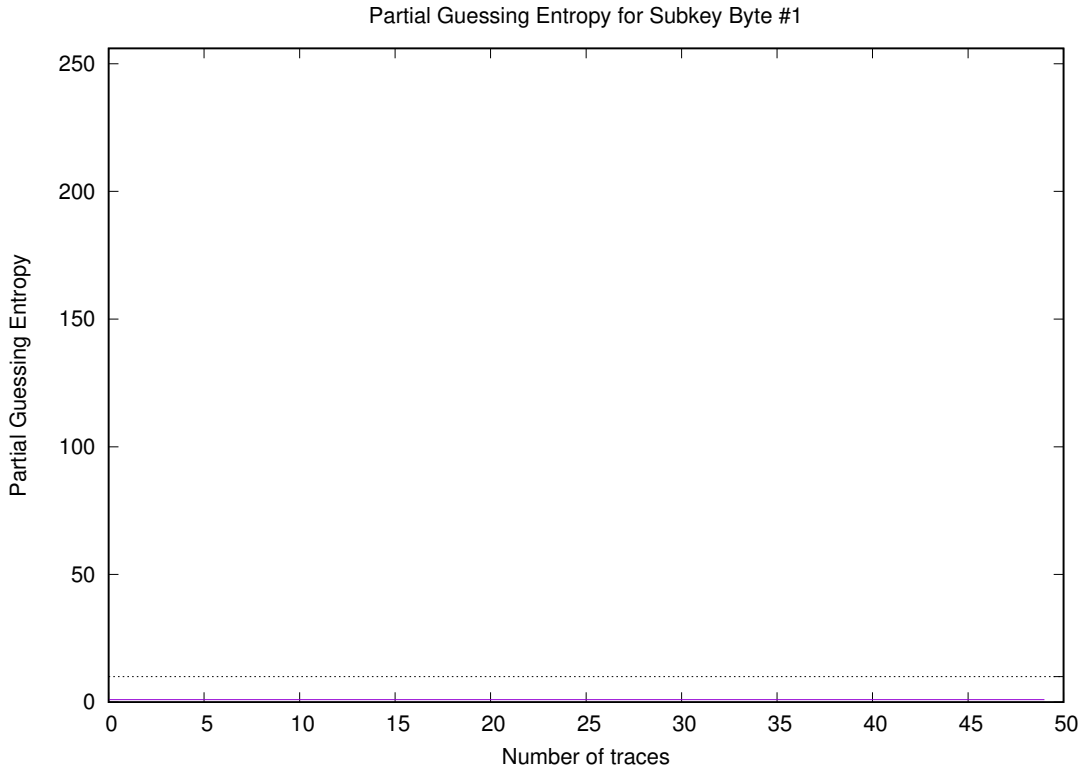

Partial Success Rate for Subkey Byte #16
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
5
10
15
20
25
30
35
40
45
50

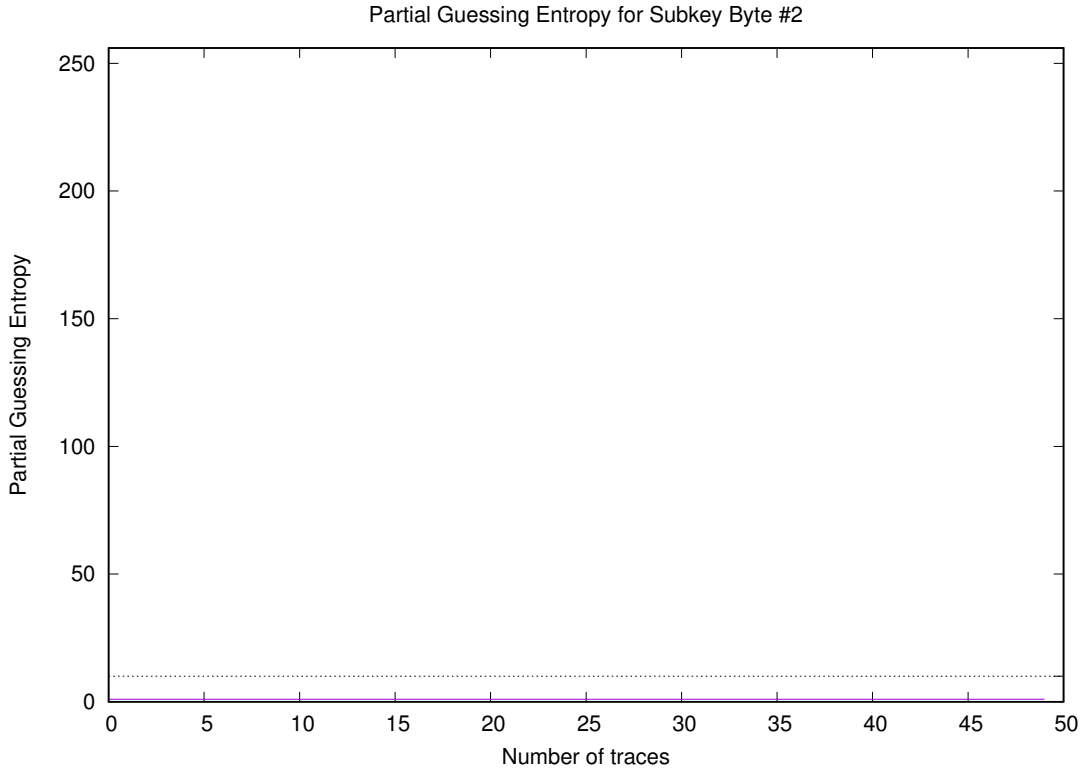

Partial Success Rate for Subkey Bytes #1 to #8
Partial Success Rate
Number of traces
01 02 03 04 05 06 07 08

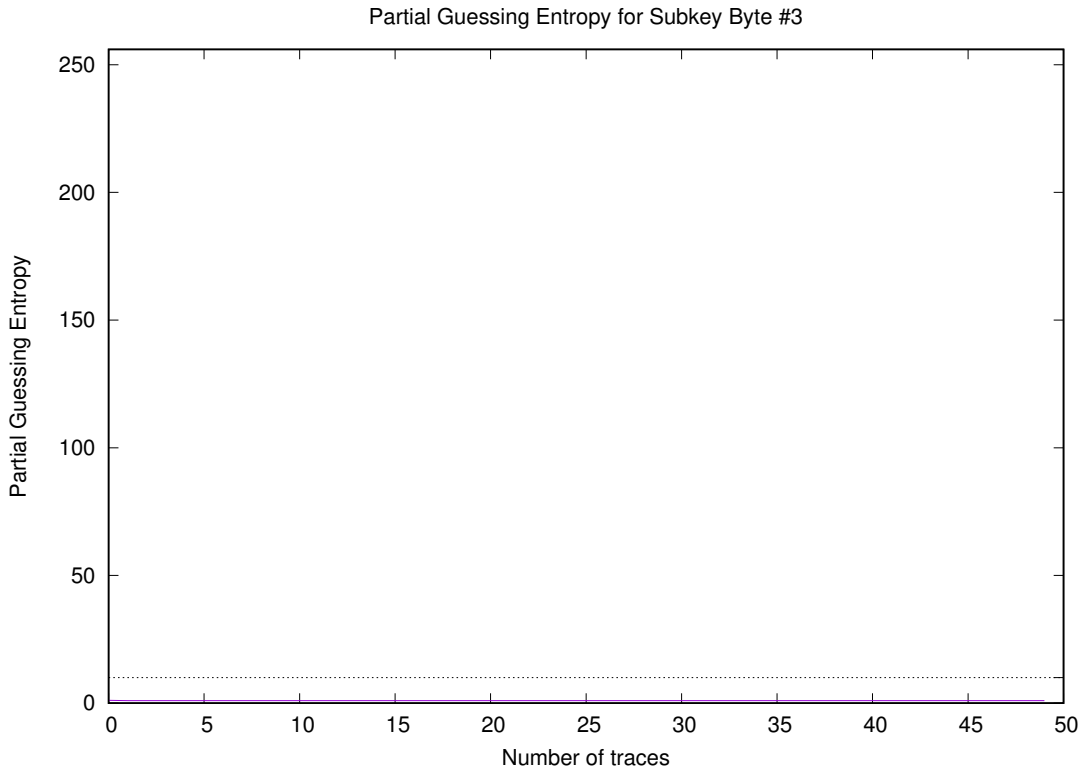

Partial Success Rate for Subkey Bytes #9 to #16
Partial Success Rate
Number of traces
09 10 11 12 13 14 15 16

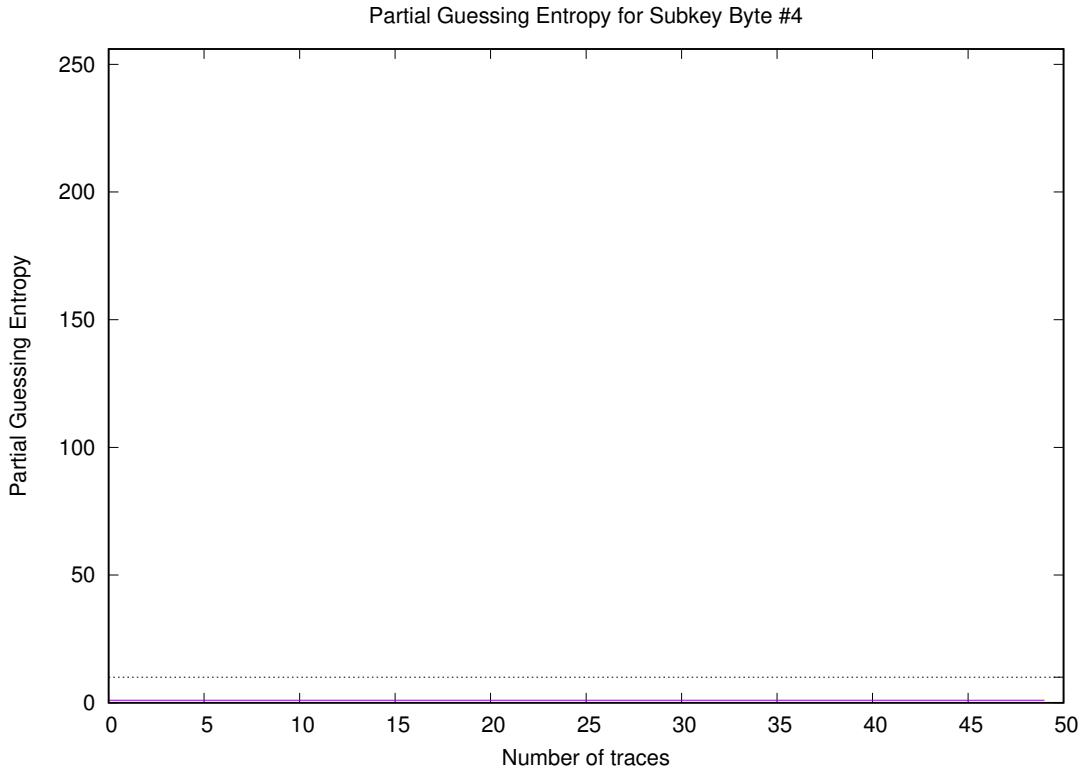
Traces	Partial Success Rate / Byte																Min	Max	Mean
	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16			
10	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
20	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
30	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
40	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
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

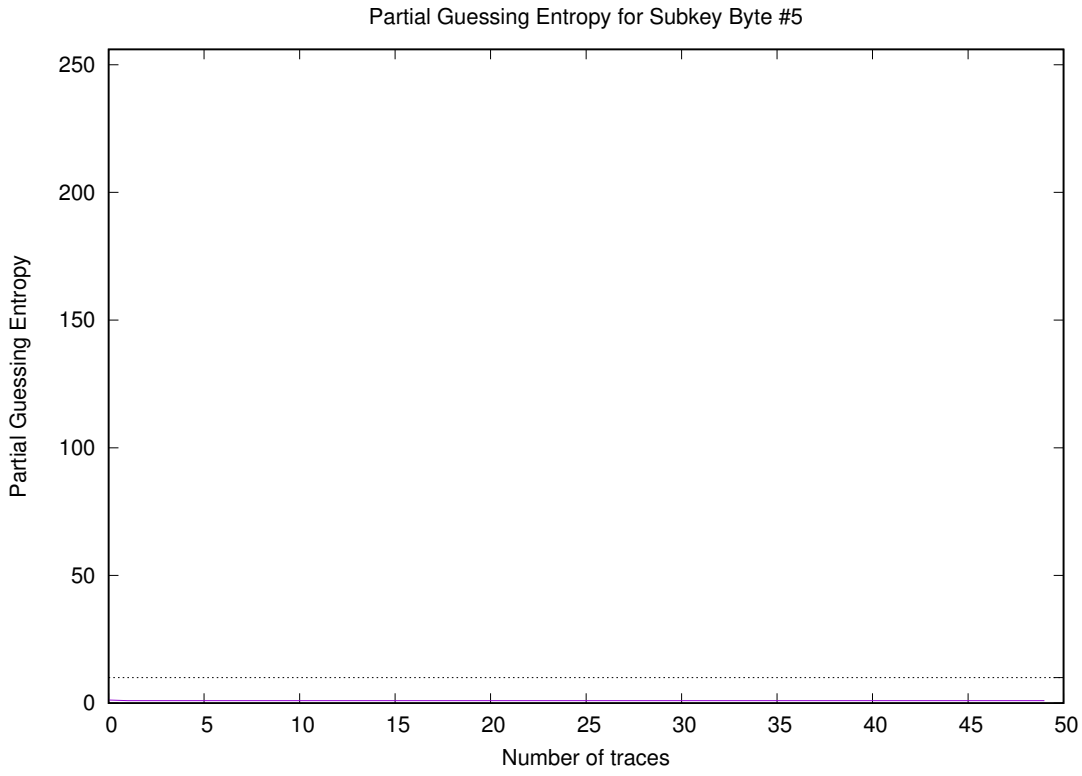
4 Partial Guessing Entropy

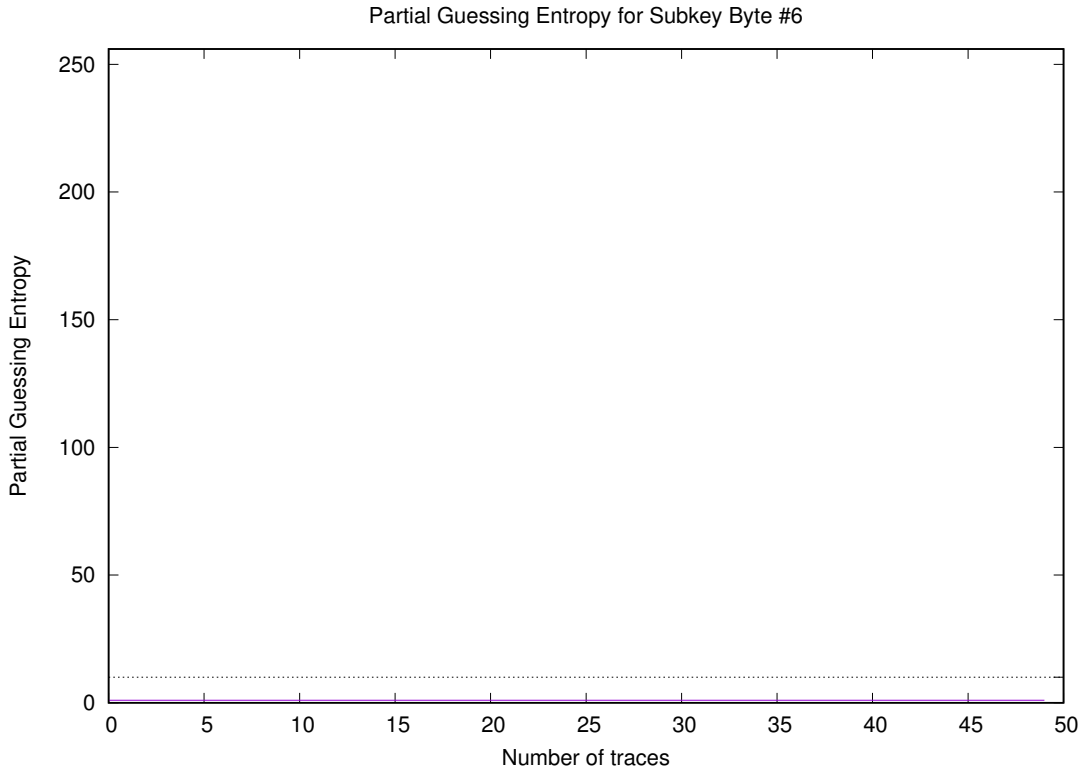


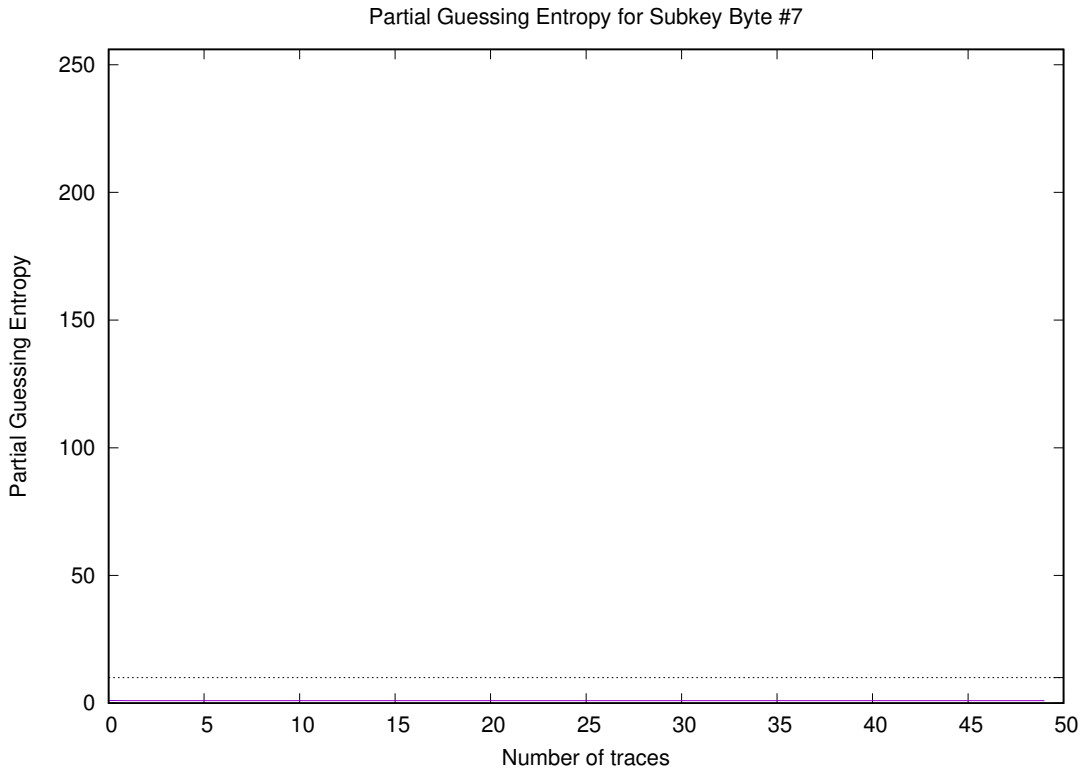


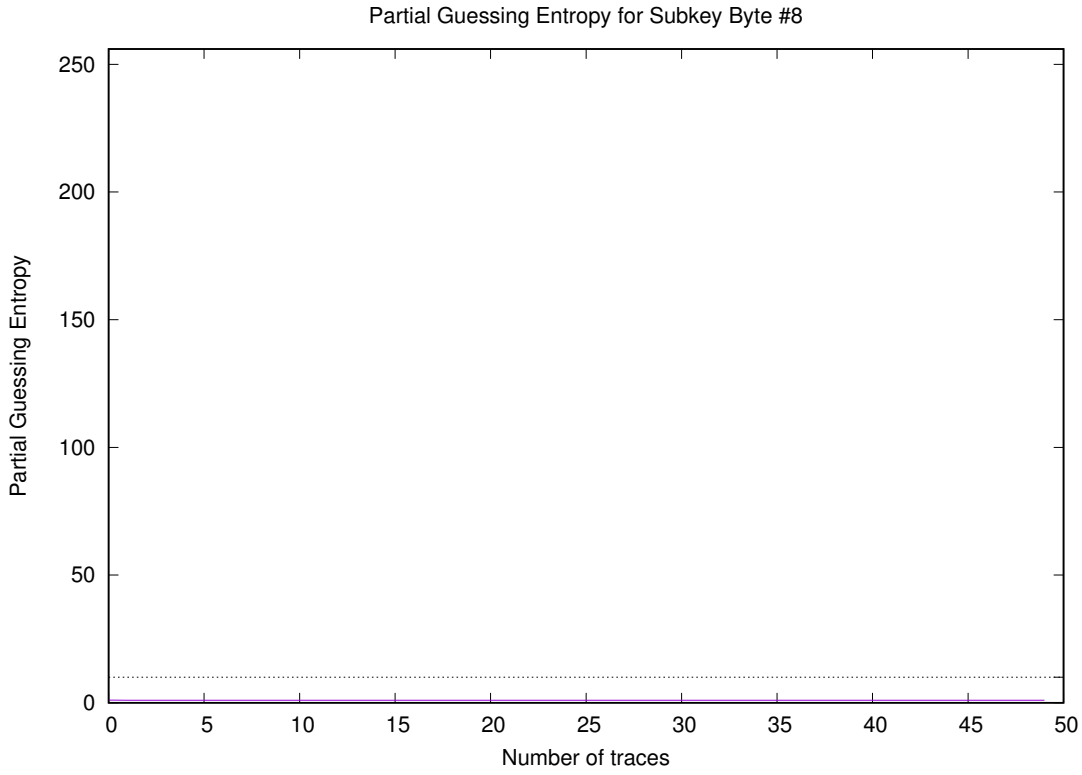

Partial Guessing Entropy for Subkey Byte #3
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
0
5
10
15
20
25
30
35
40
45
50

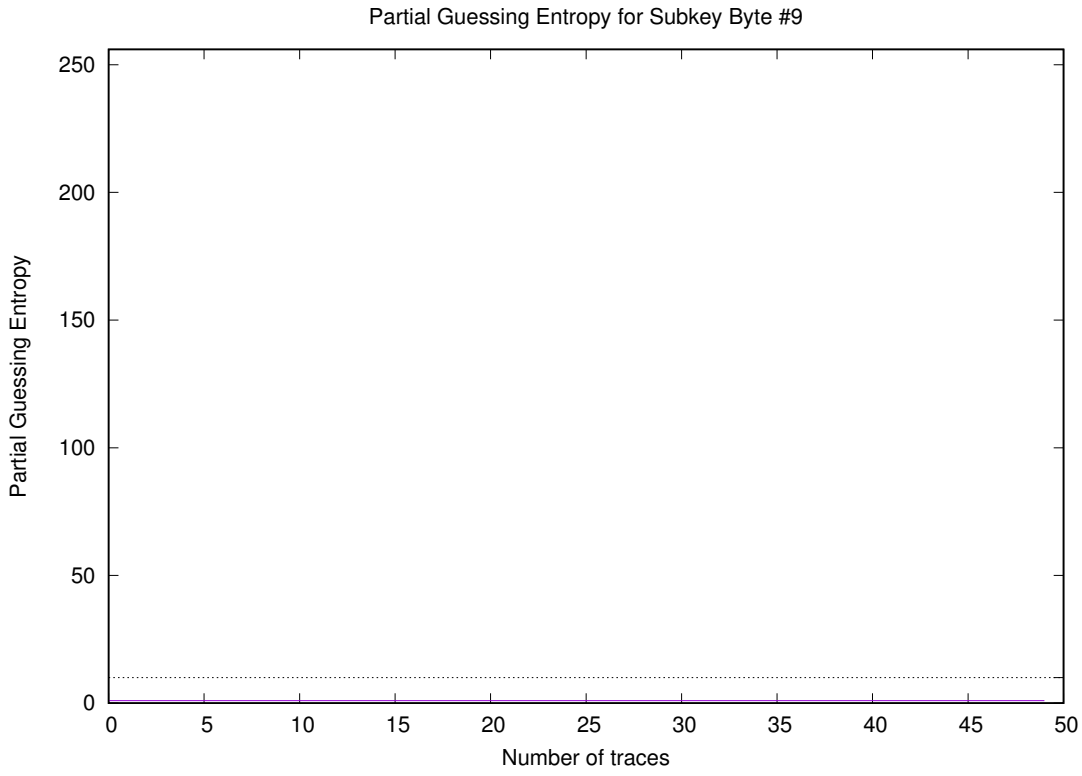

Partial Guessing Entropy for Subkey Byte #4
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
0
5
10
15
20
25
30
35
40
45
50

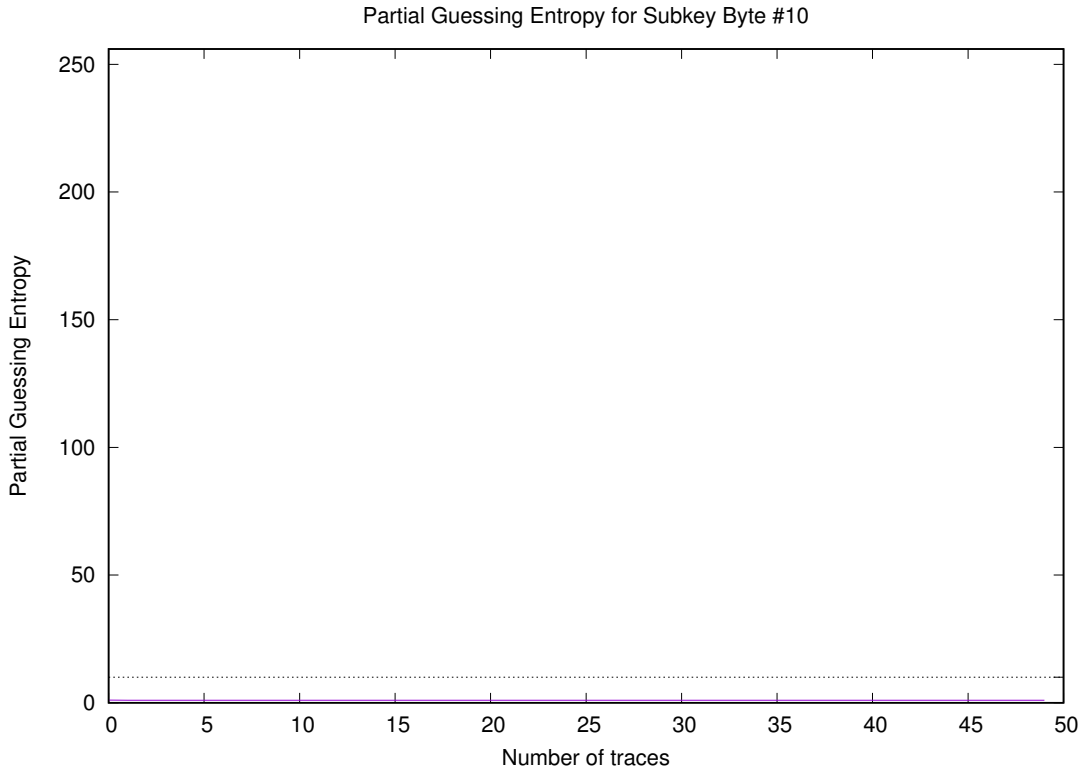

Partial Guessing Entropy for Subkey Byte #5
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
0
5
10
15
20
25
30
35
40
45
50

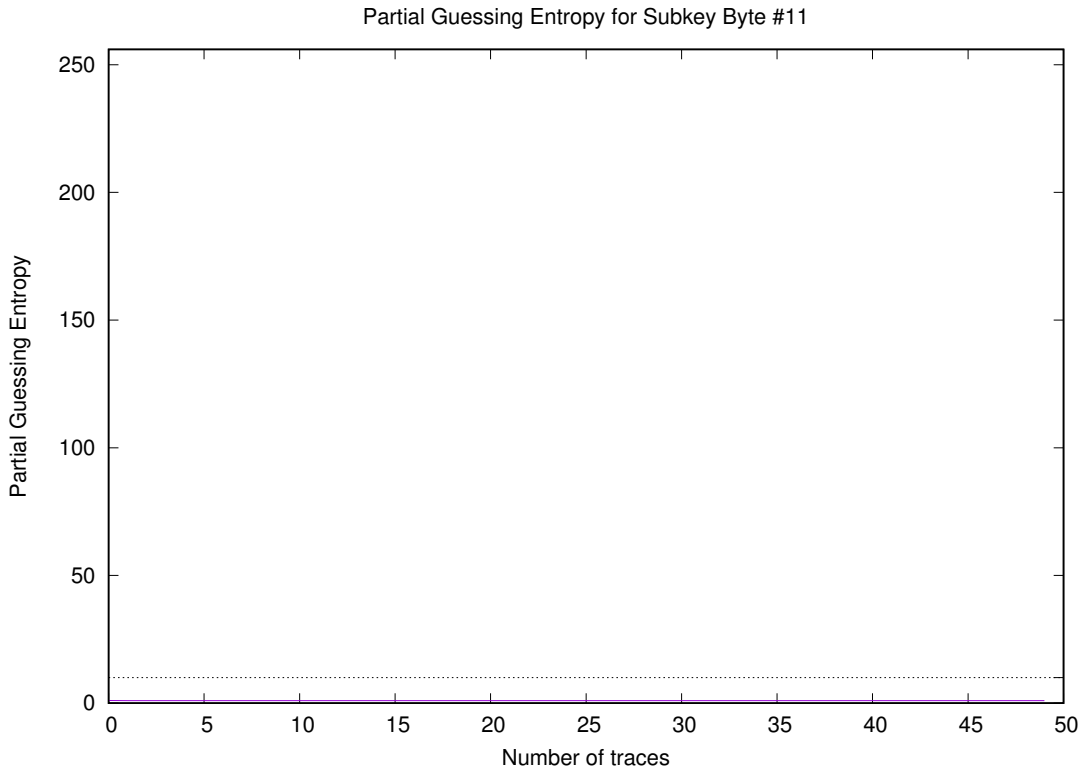

Partial Guessing Entropy for Subkey Byte #6
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
0
5
10
15
20
25
30
35
40
45
50

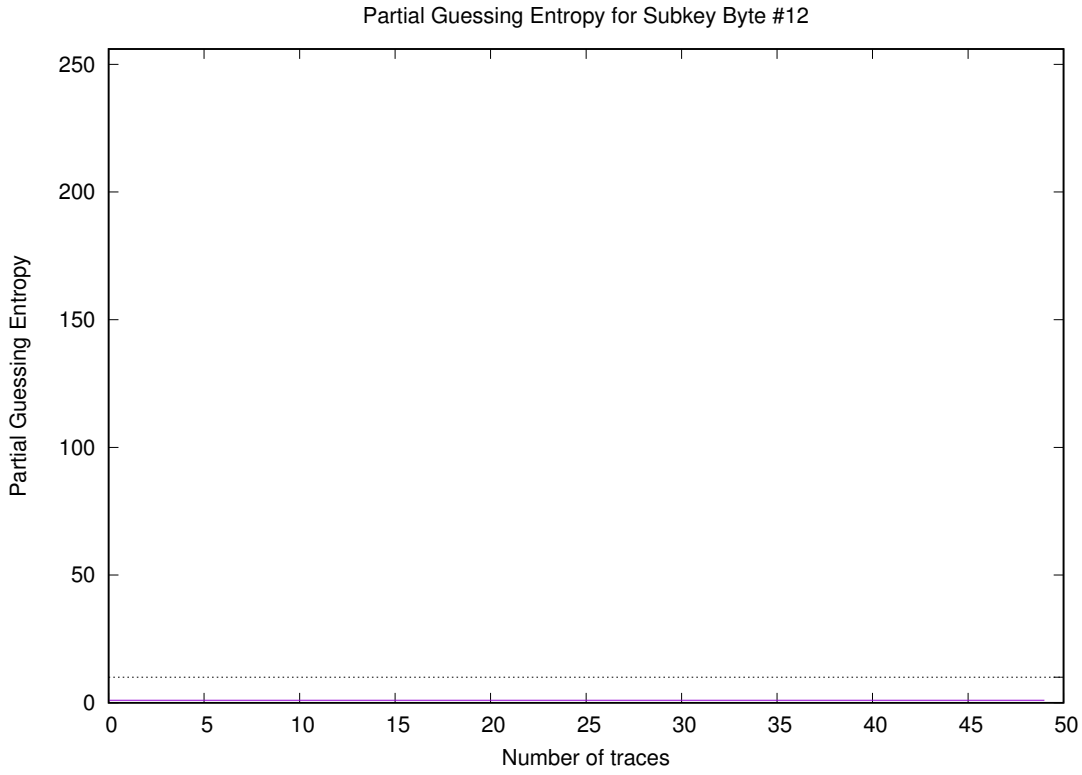

Partial Guessing Entropy for Subkey Byte #7
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
0
5
10
15
20
25
30
35
40
45
50

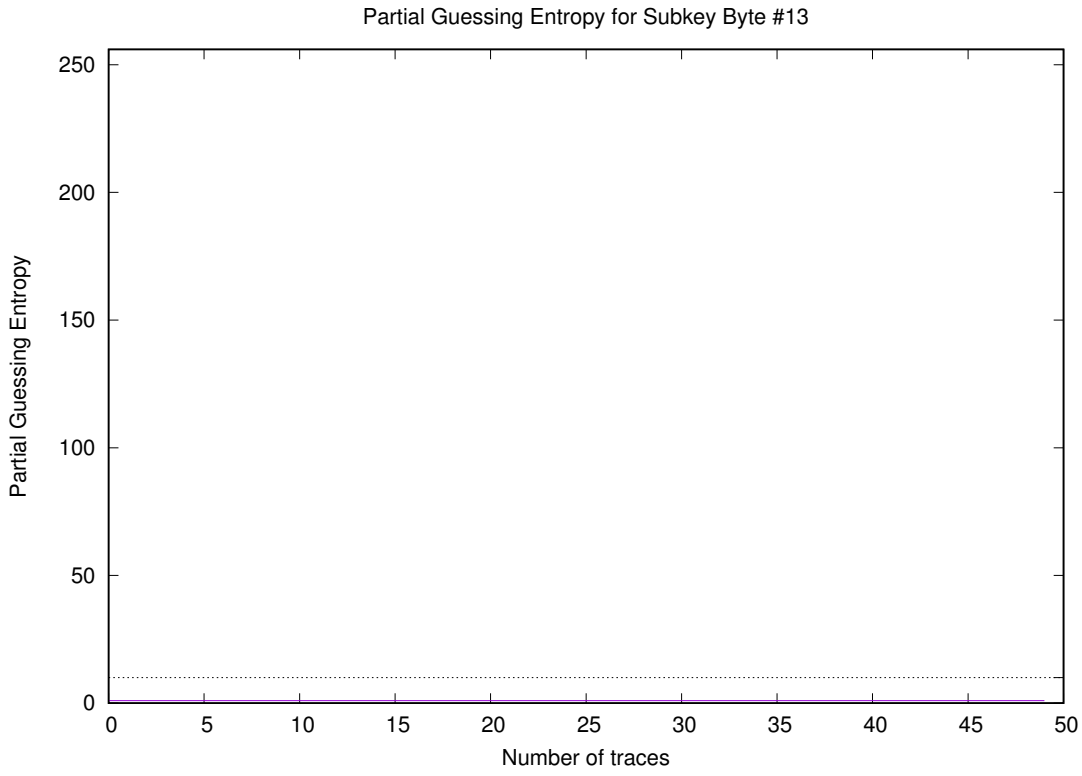

Partial Guessing Entropy for Subkey Byte #8
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
0
5
10
15
20
25
30
35
40
45
50

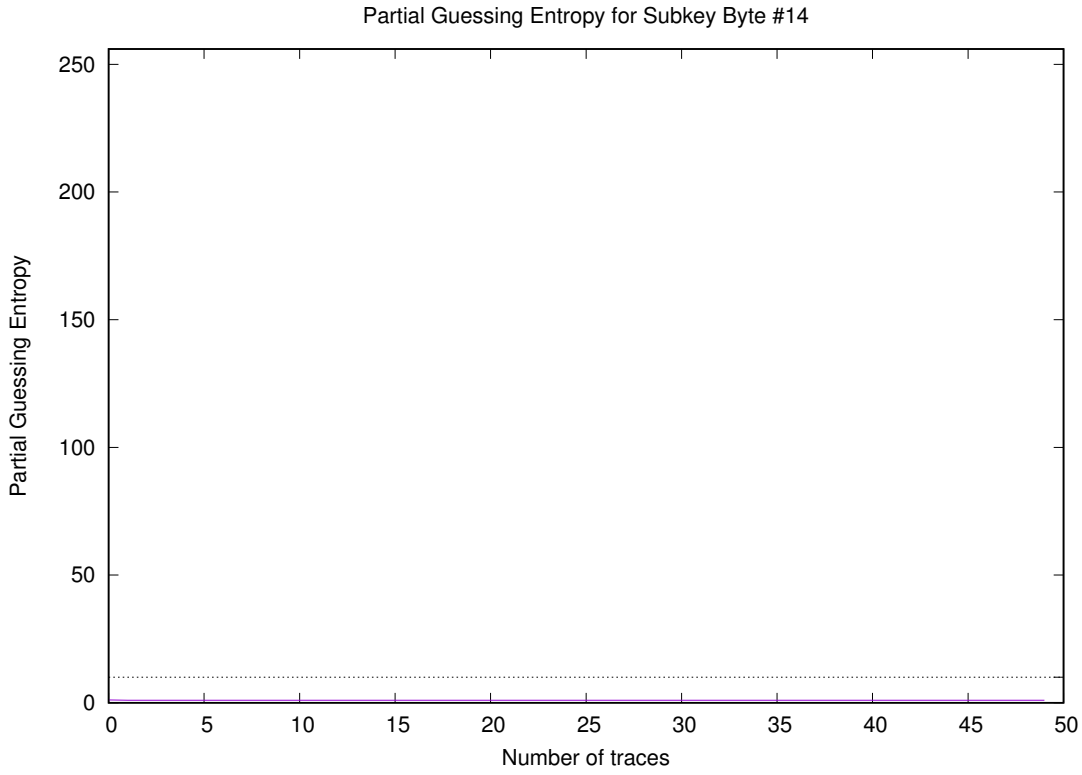

Partial Guessing Entropy for Subkey Byte #9
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
0
5
10
15
20
25
30
35
40
45
50

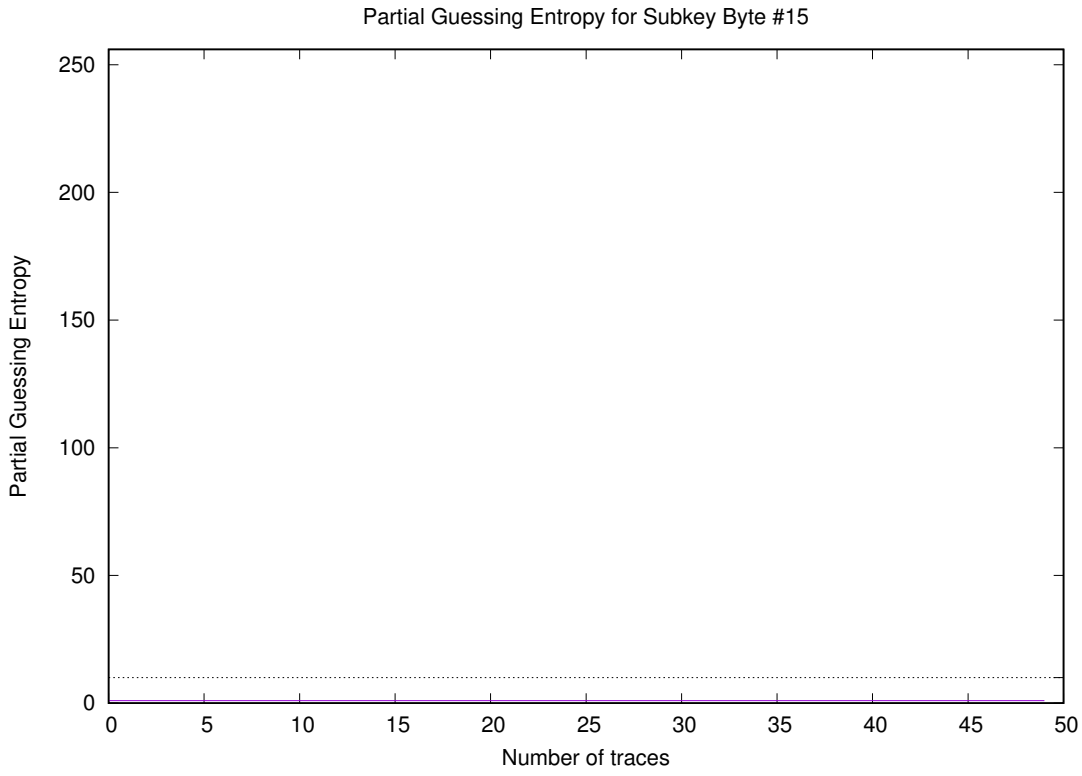

Partial Guessing Entropy for Subkey Byte #10
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
0
5
10
15
20
25
30
35
40
45
50

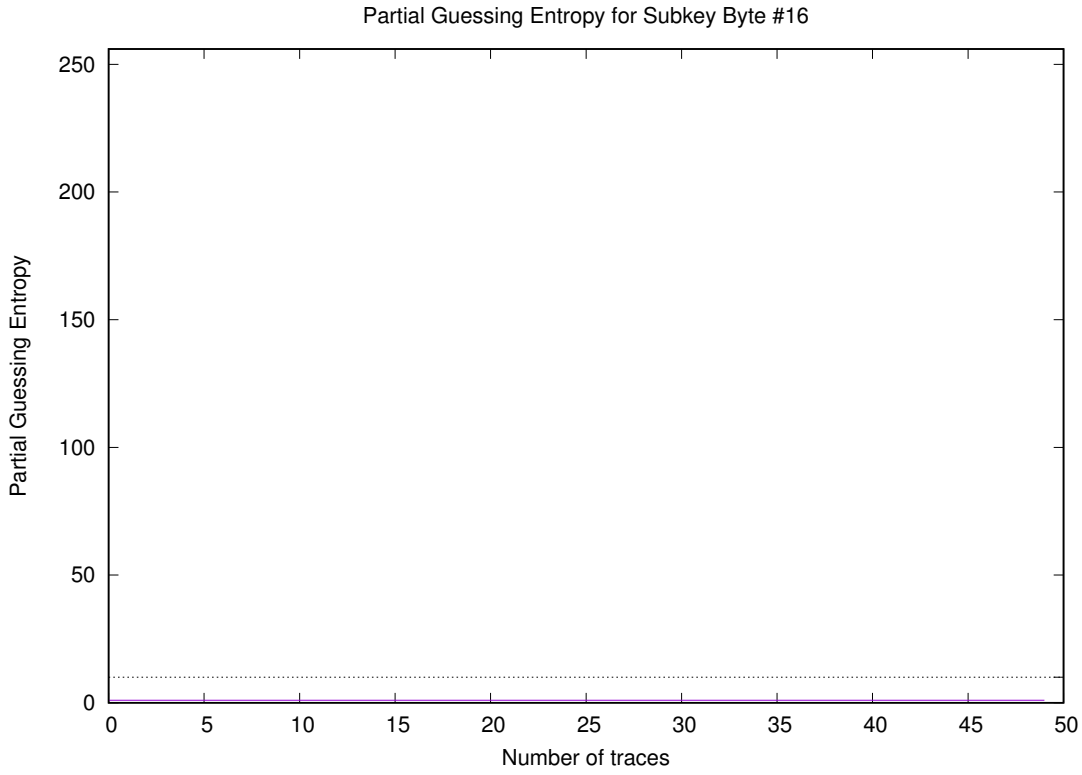

Partial Guessing Entropy for Subkey Byte #11
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
0
5
10
15
20
25
30
35
40
45
50

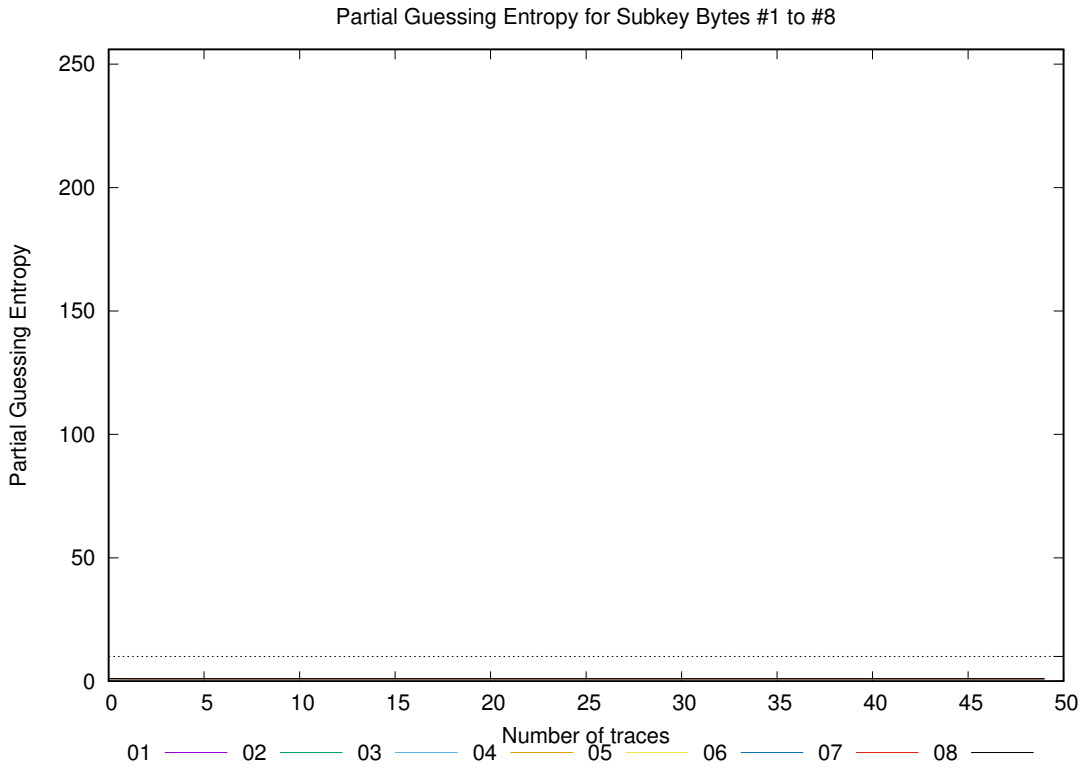

Partial Guessing Entropy for Subkey Byte #12
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
0
5
10
15
20
25
30
35
40
45
50

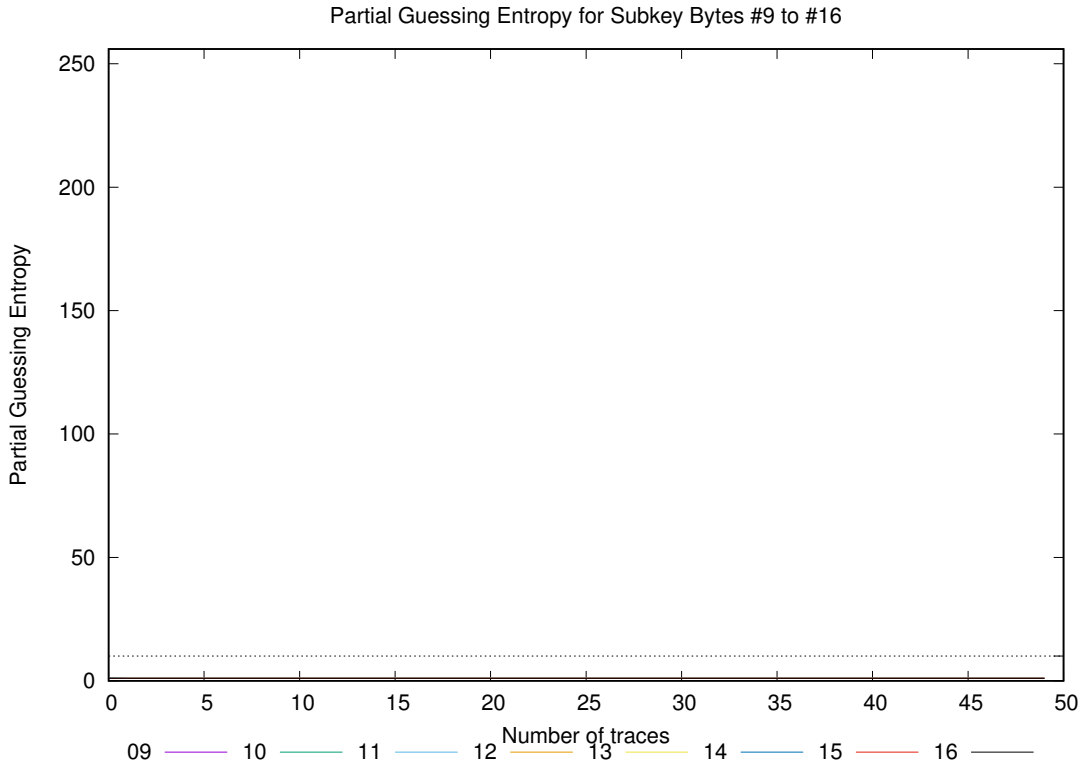

Partial Guessing Entropy for Subkey Byte #13
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
0
5
10
15
20
25
30
35
40
45
50


Partial Guessing Entropy for Subkey Byte #14
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
0
5
10
15
20
25
30
35
40
45
50


Partial Guessing Entropy for Subkey Byte #15
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
0
5
10
15
20
25
30
35
40
45
50


Partial Guessing Entropy for Subkey Byte #16
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
0
5
10
15
20
25
30
35
40
45
50


Partial Guessing Entropy for Subkey Bytes #1 to #8
Partial Guessing Entropy
250
200
150
100
50
0
0
5
10
15
20
25
30
35
40
45
50
Number of traces
01
02
03
04
05
06
07
08


Partial Guessing Entropy for Subkey Bytes #9 to #16
Partial Guessing Entropy
250
200
150
100
50
0
0
5
10
15
20
25
30
35
40
45
50
Number of traces
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	1.0	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
20	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
30	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
40	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
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