DPA Contest v4.2
Evaluation results

Zeyi Liu, Zongbin Liu, Neng Gao, Chenyang Tu, Yuan Ma, Jun Yuan

October 2015

1 Introduction

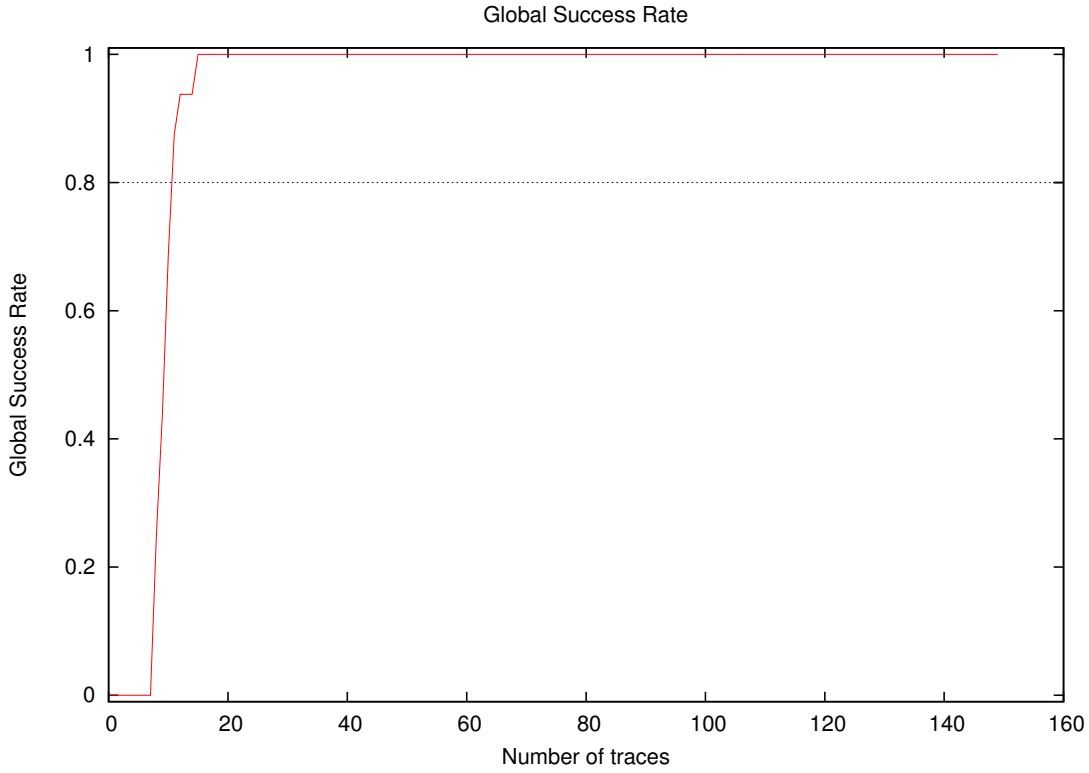
1.1 About the attack

- **Attack Name:** TA-CPA
- **Sender/Team:** Zeyi Liu, Zongbin Liu, Neng Gao, Chenyang Tu, Yuan Ma, Jun Yuan
- **Institution:** Data Assurance and Communication Security Research Center, CAS, China
- **Language:** C#
- **Operating system:** Windows
- **Attacked subkey:** 10

1.2 About the evaluation

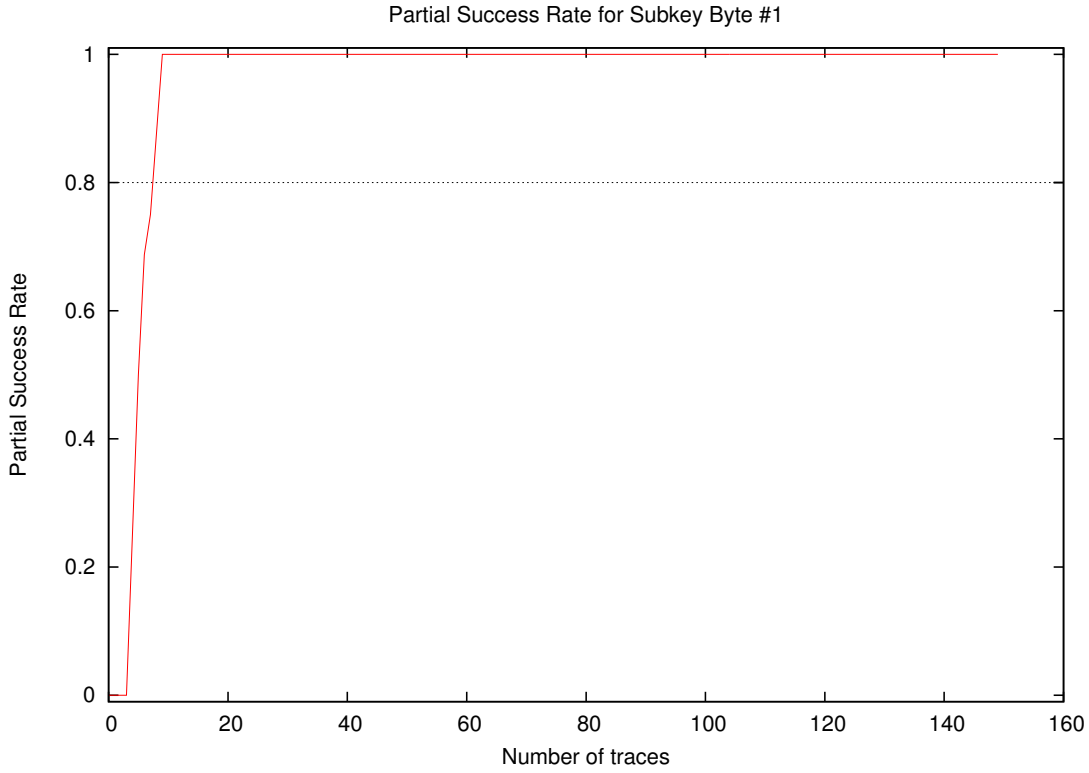
- **Date of evaluation:** October 2015

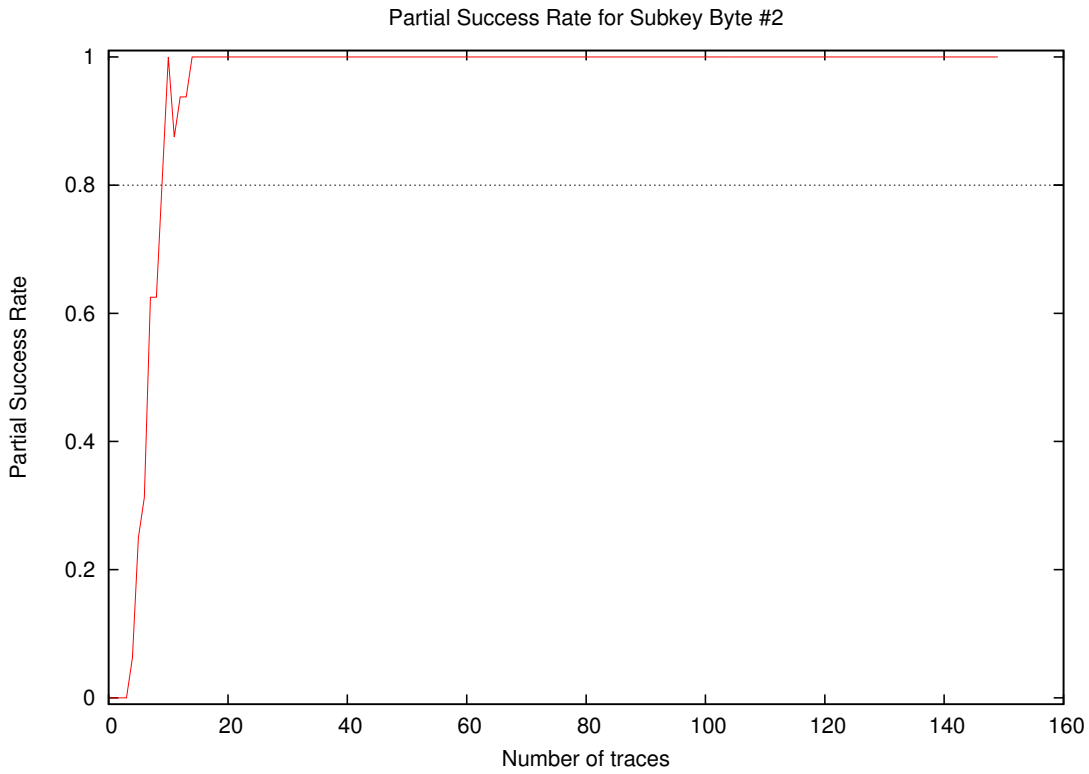
2 Global Success Rate

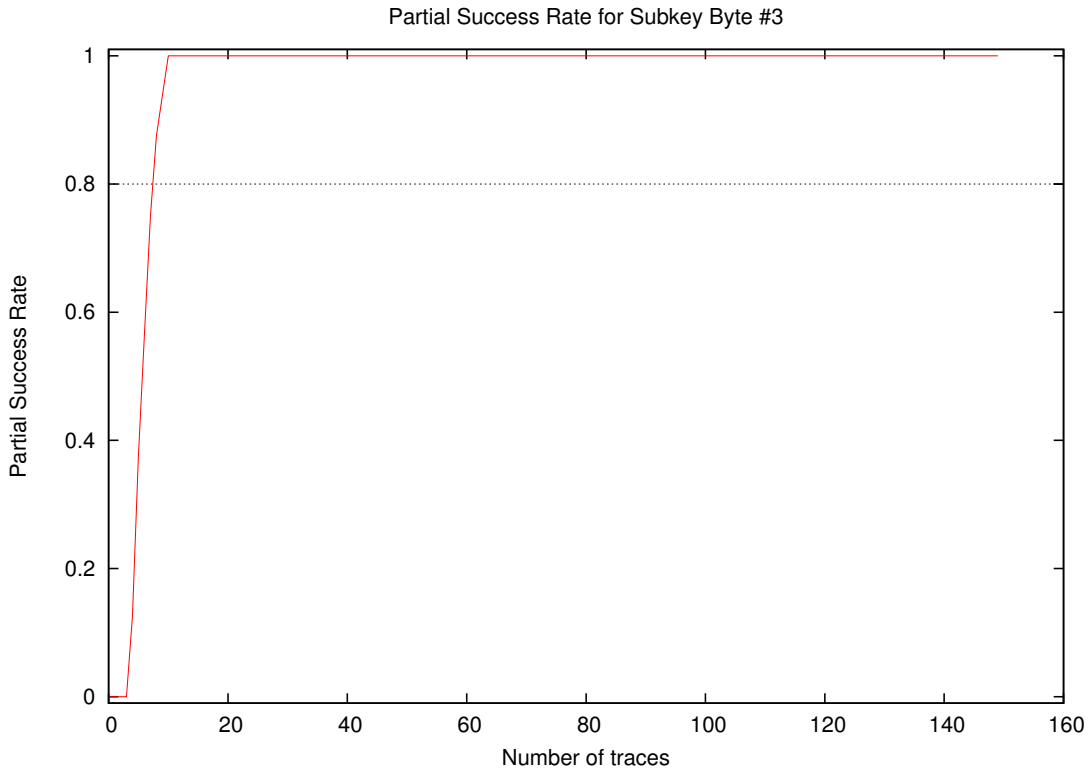


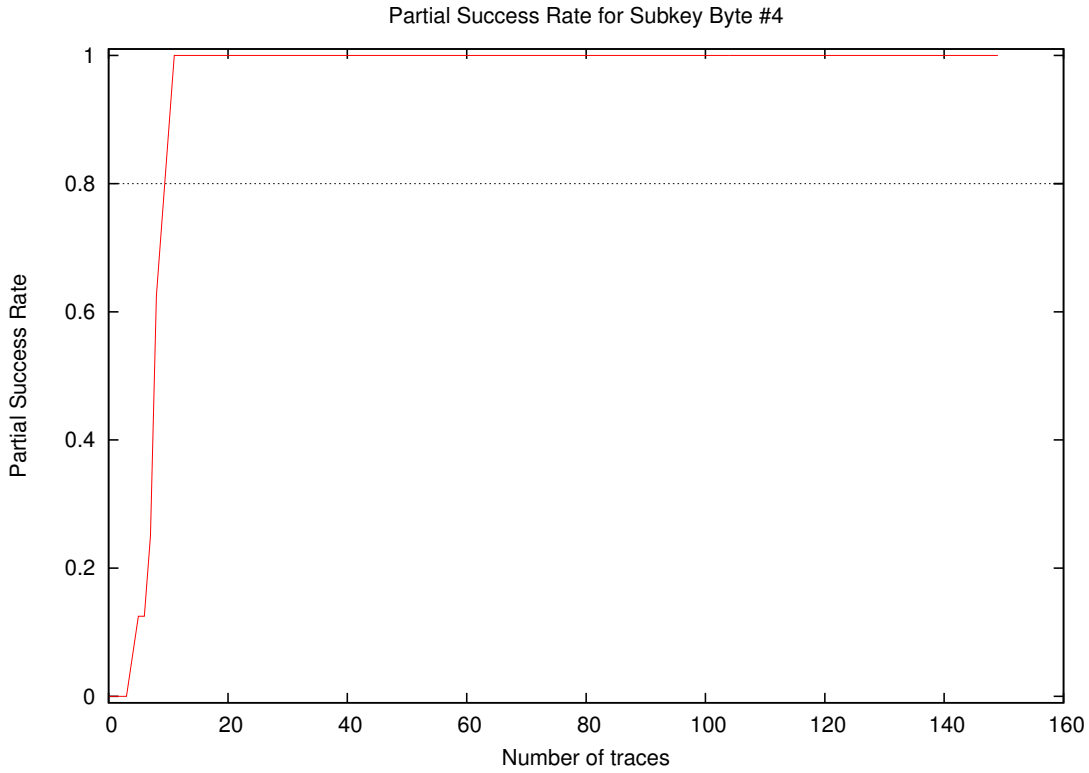
Number of traces	Global Success Rate
10	0.44
20	1.00
30	1.00
40	1.00
50	1.00
100	1.00

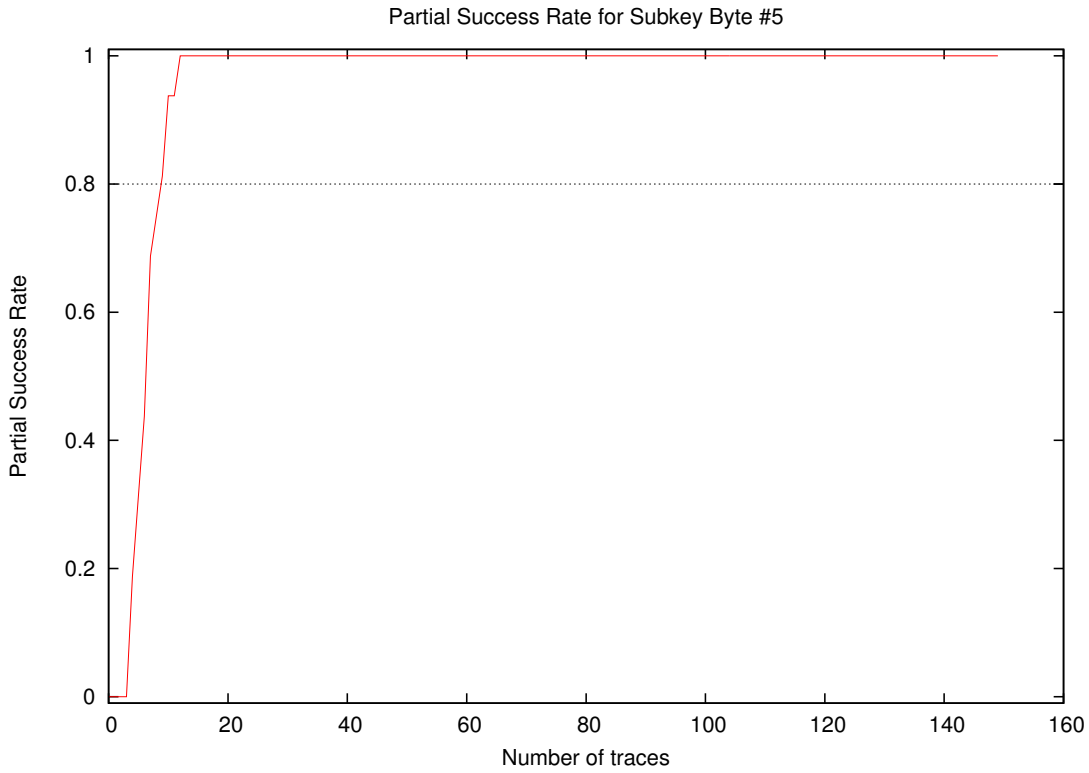
3 Partial Success Rate

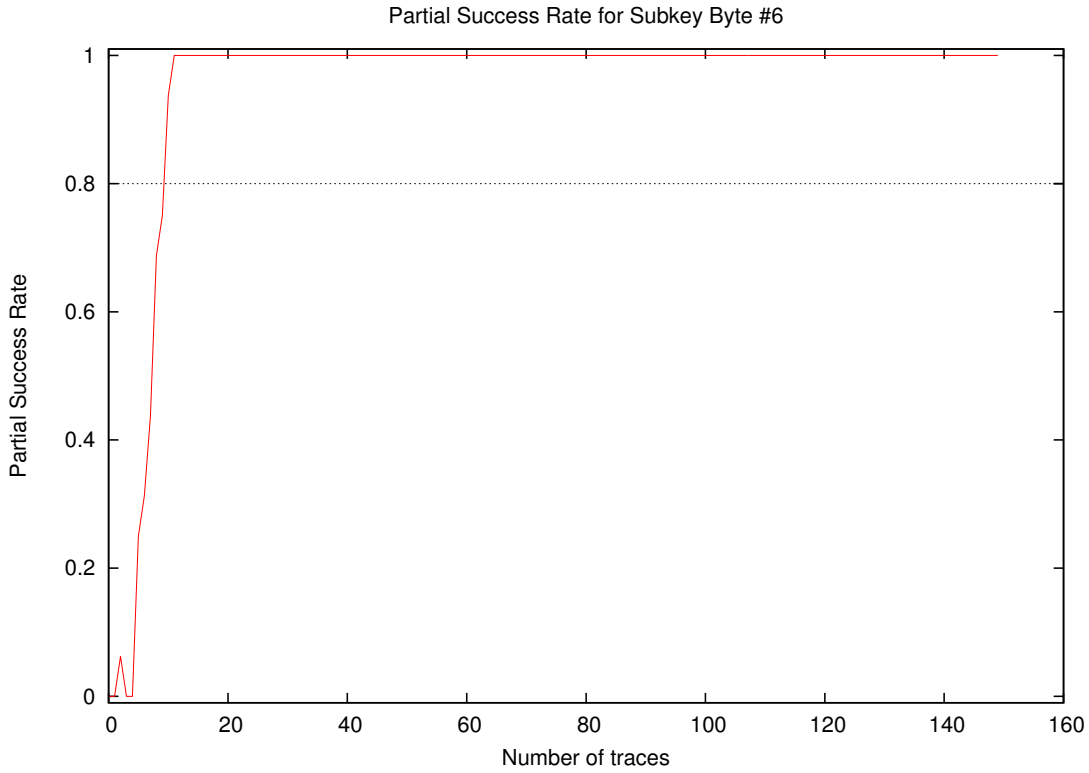


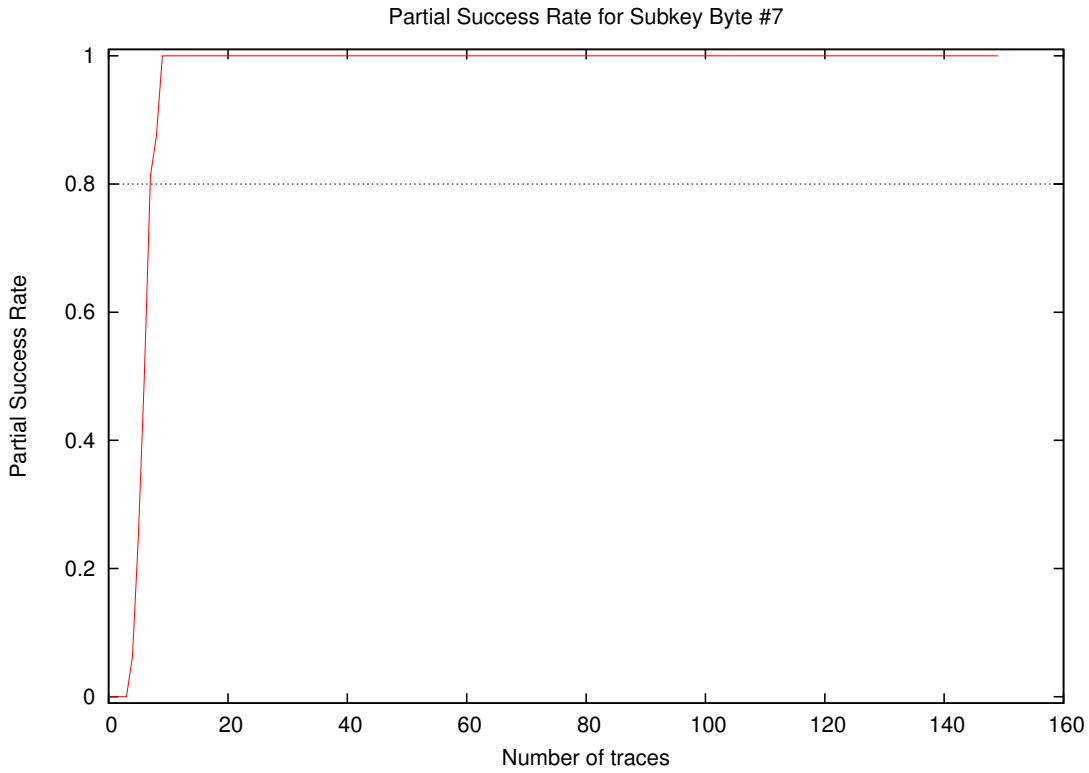


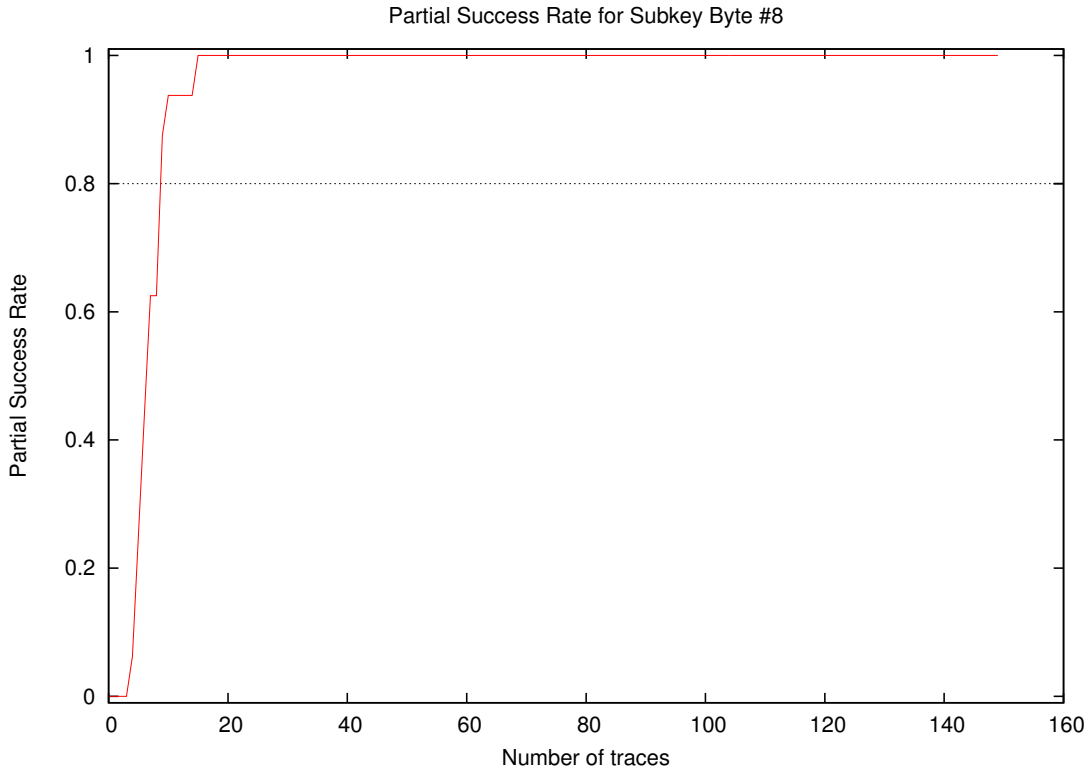

Partial Success Rate for Subkey Byte #3
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
20
40
60
80
100
120
140
160

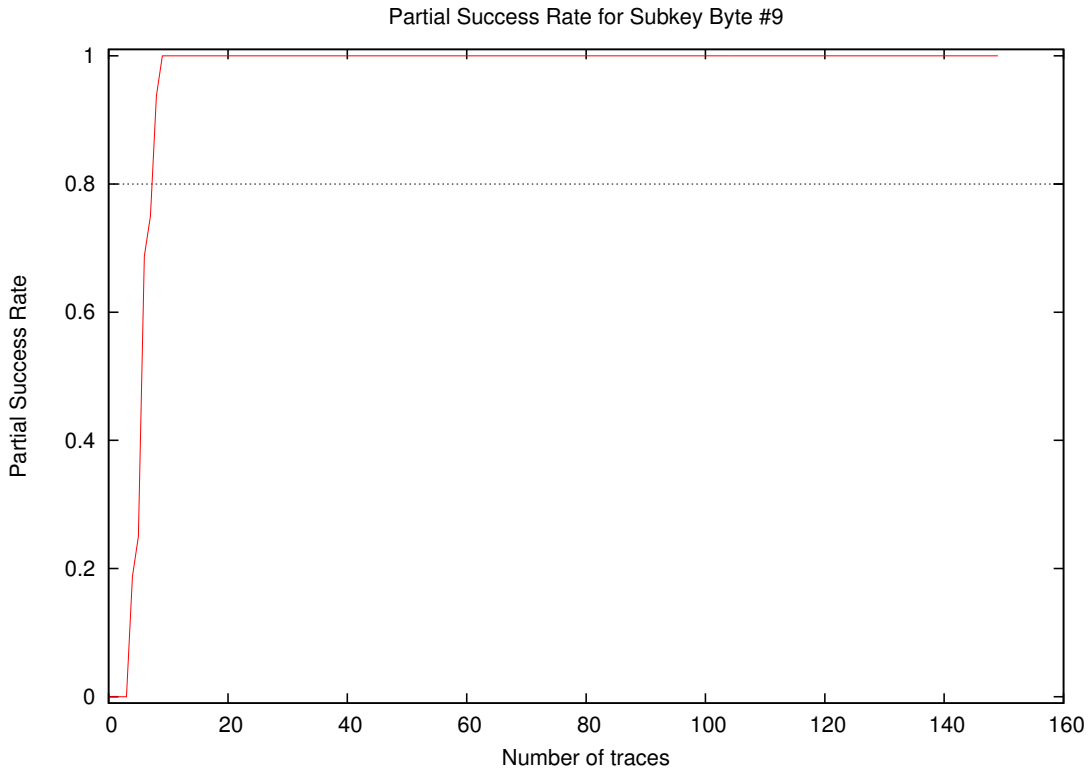

Partial Success Rate for Subkey Byte #4
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
20
40
60
80
100
120
140
160

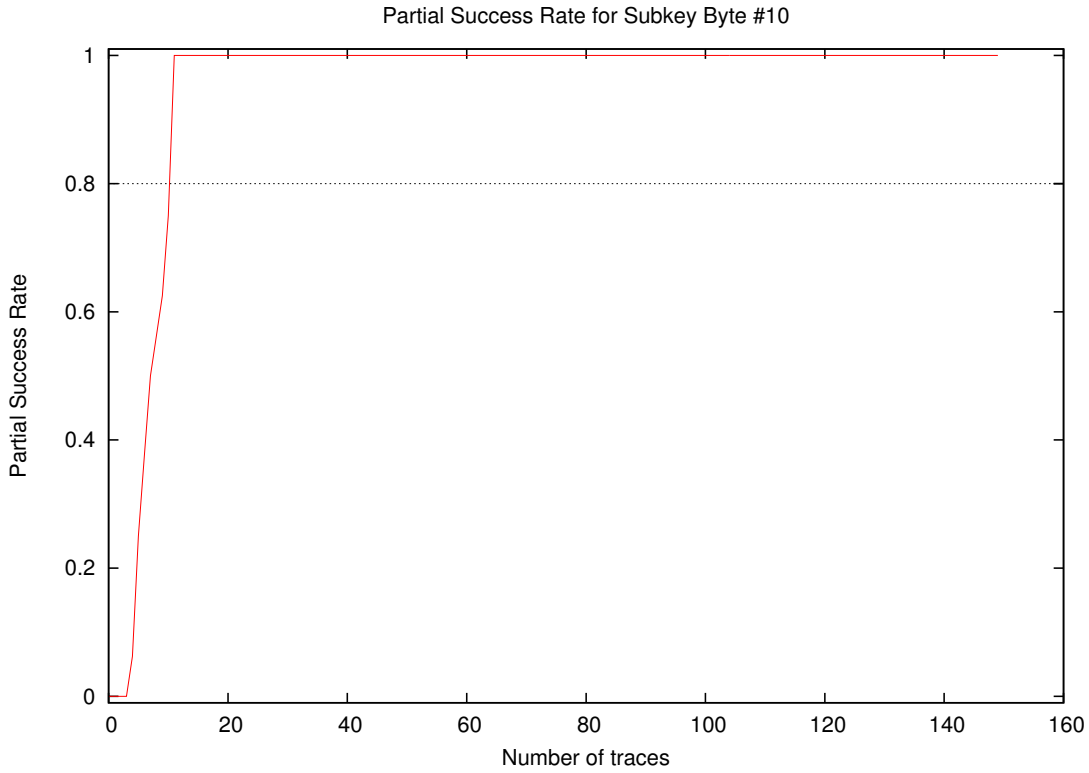

Partial Success Rate for Subkey Byte #5
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
20
40
60
80
100
120
140
160

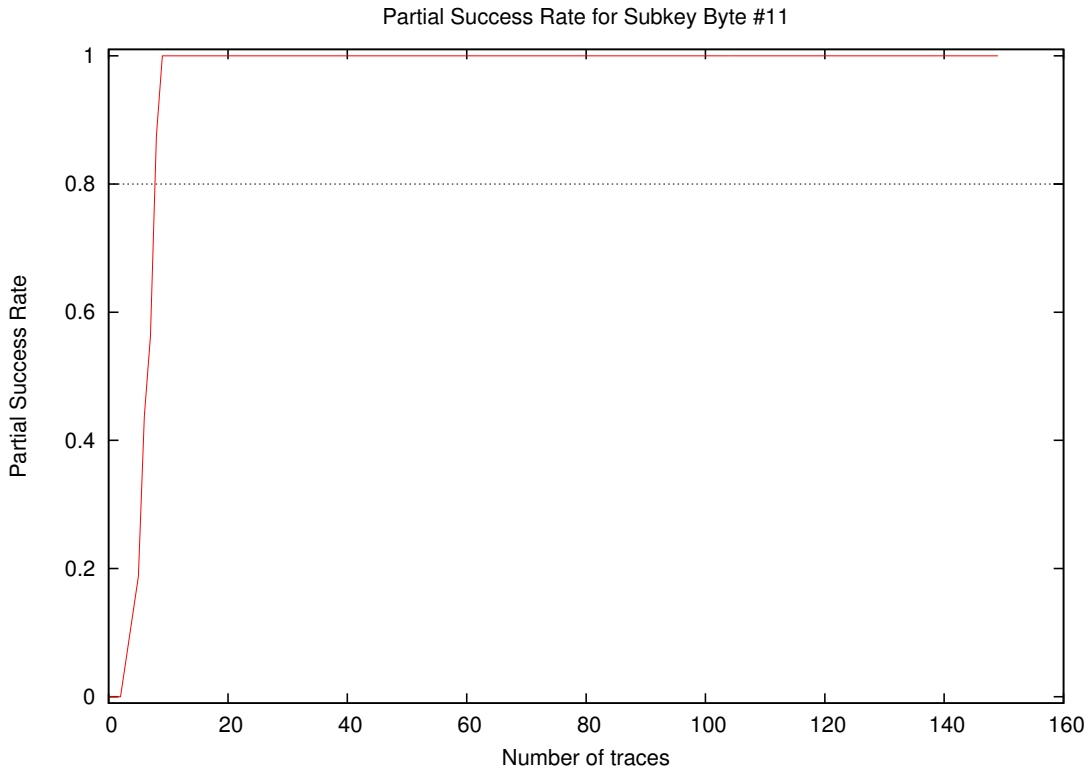

Partial Success Rate for Subkey Byte #6
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
20
40
60
80
100
120
140
160

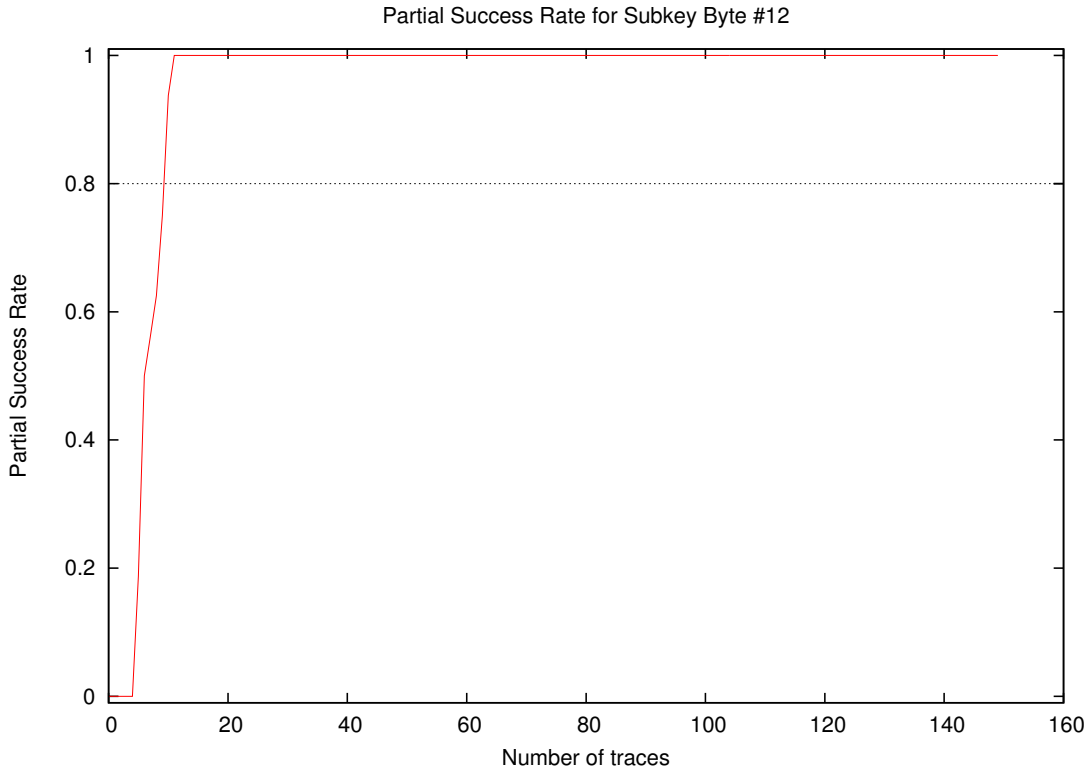

Partial Success Rate for Subkey Byte #7
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
20
40
60
80
100
120
140
160

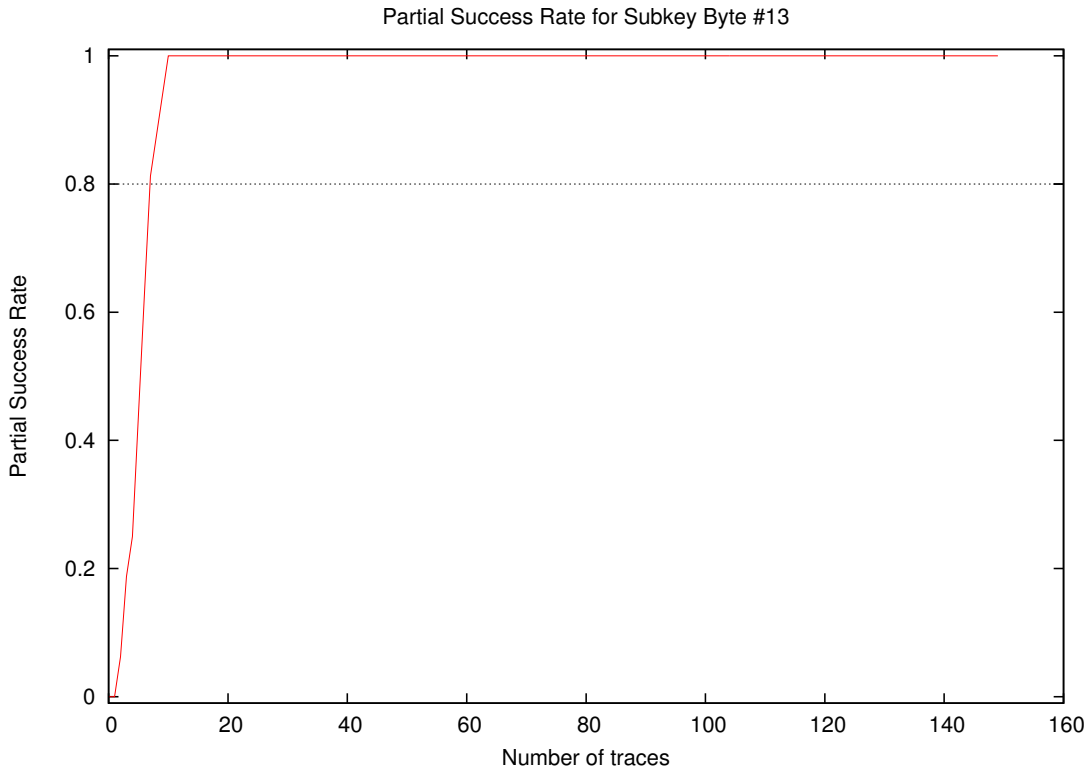

Partial Success Rate for Subkey Byte #8
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
20
40
60
80
100
120
140
160

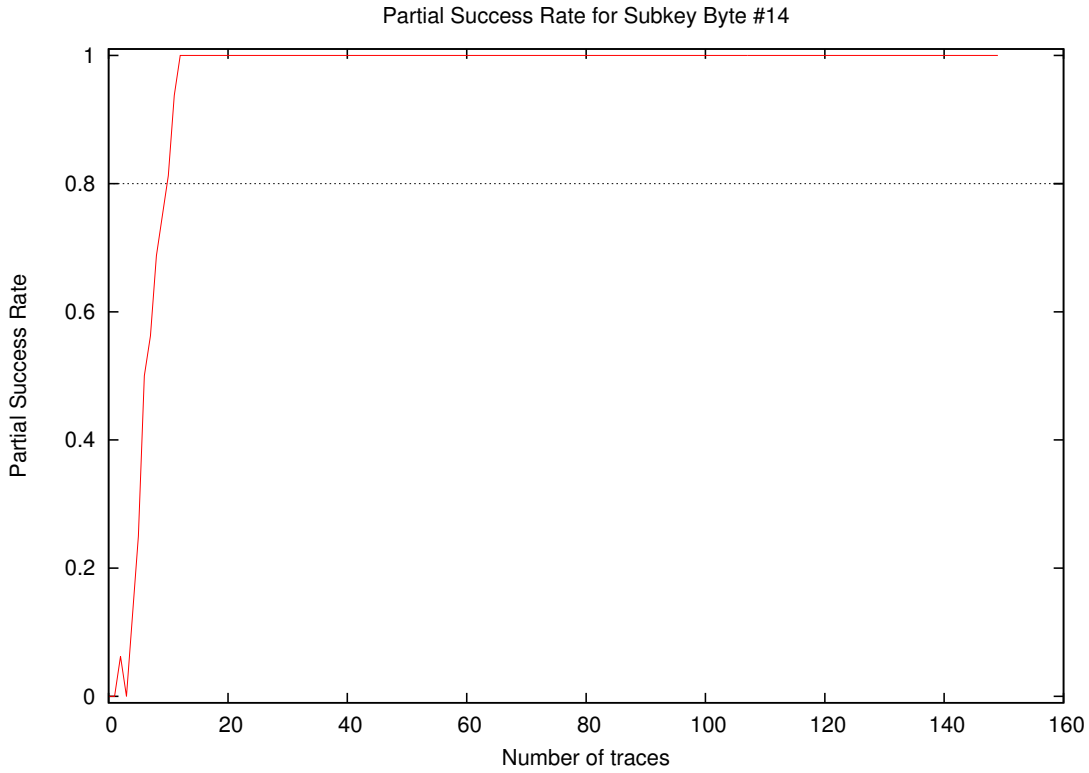

Partial Success Rate for Subkey Byte #9
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
20
40
60
80
100
120
140
160

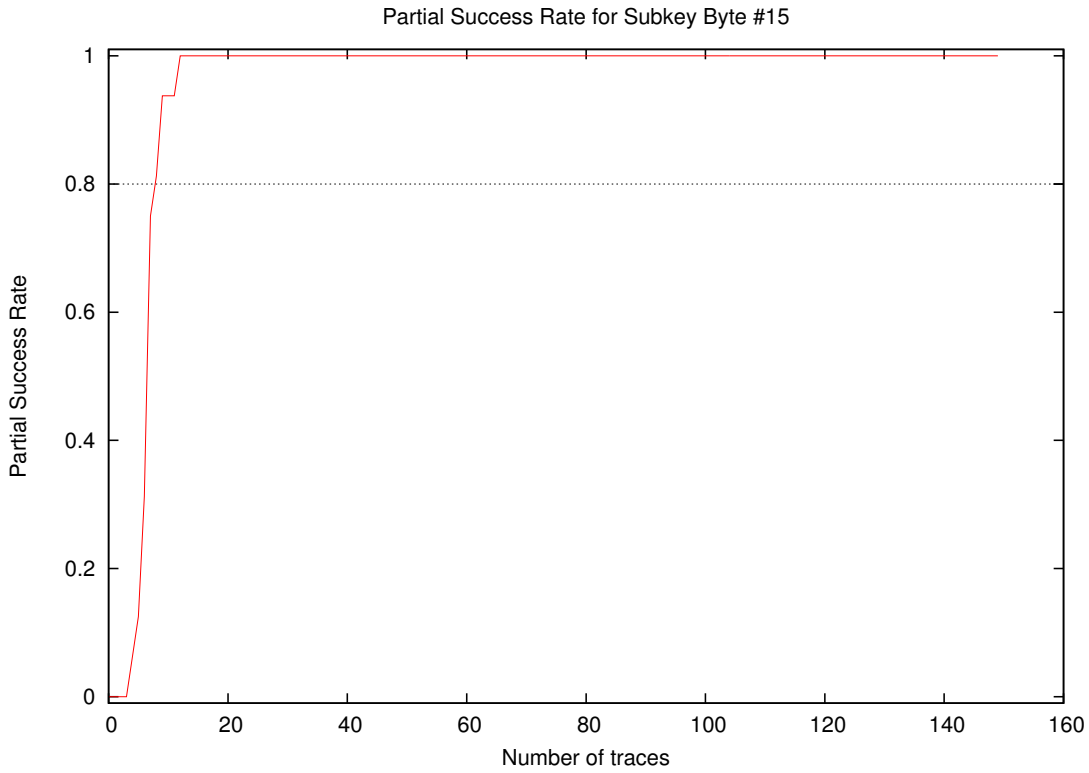

Partial Success Rate for Subkey Byte #10
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
20
40
60
80
100
120
140
160

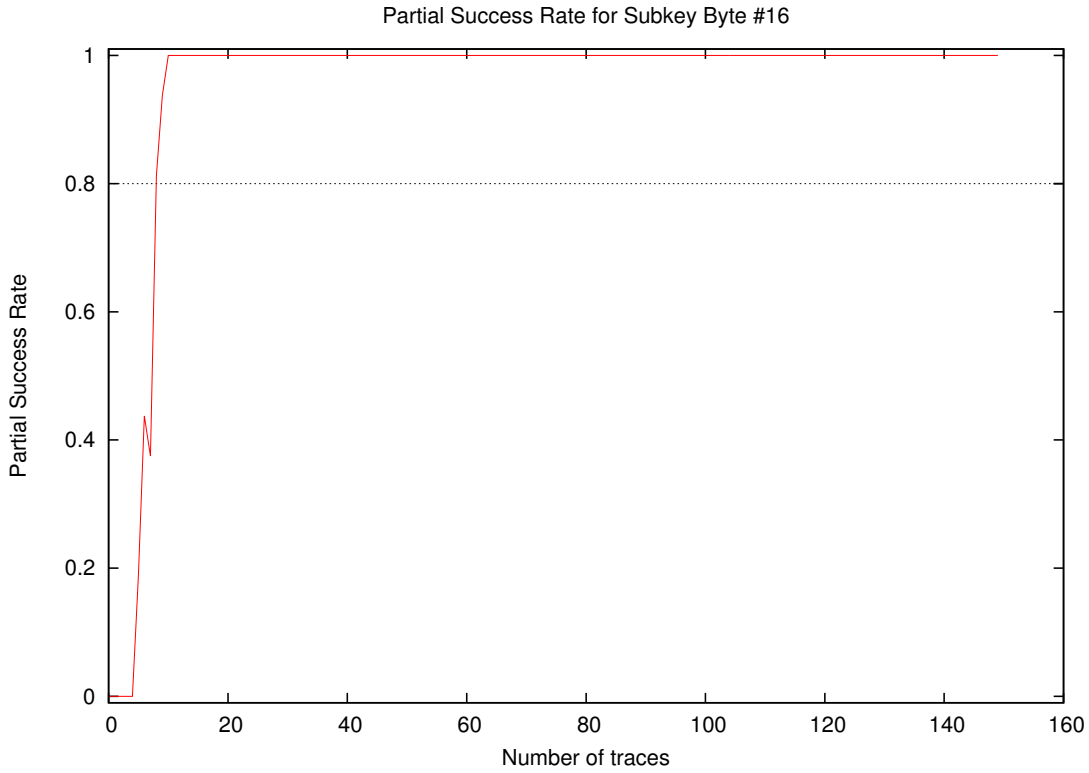

Partial Success Rate for Subkey Byte #11
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
20
40
60
80
100
120
140
160

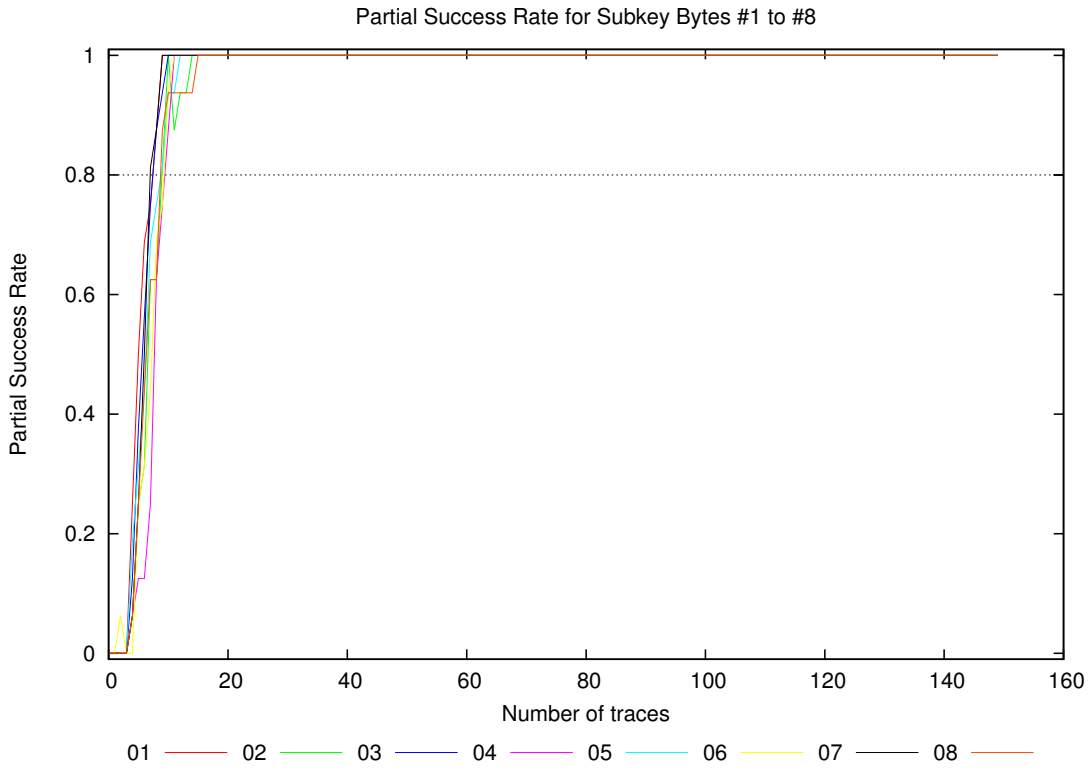

Partial Success Rate for Subkey Byte #12
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
20
40
60
80
100
120
140
160

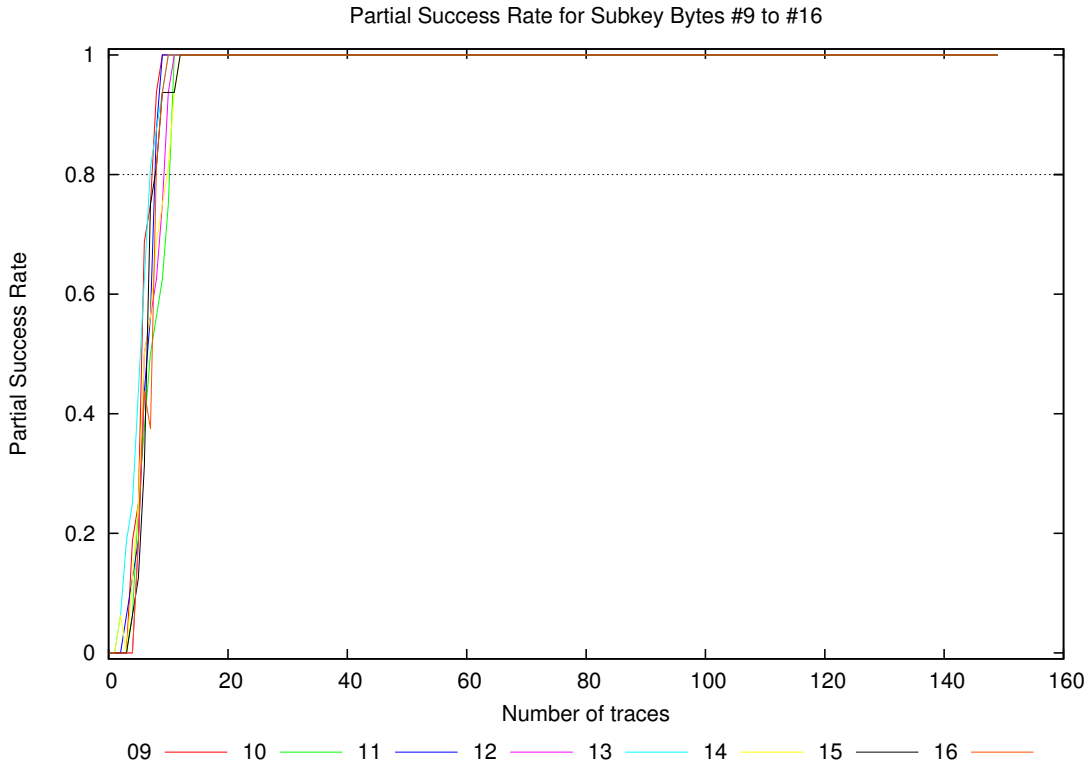

Partial Success Rate for Subkey Byte #13
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
20
40
60
80
100
120
140
160


Partial Success Rate for Subkey Byte #14
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
20
40
60
80
100
120
140
160


Partial Success Rate for Subkey Byte #15
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
20
40
60
80
100
120
140
160

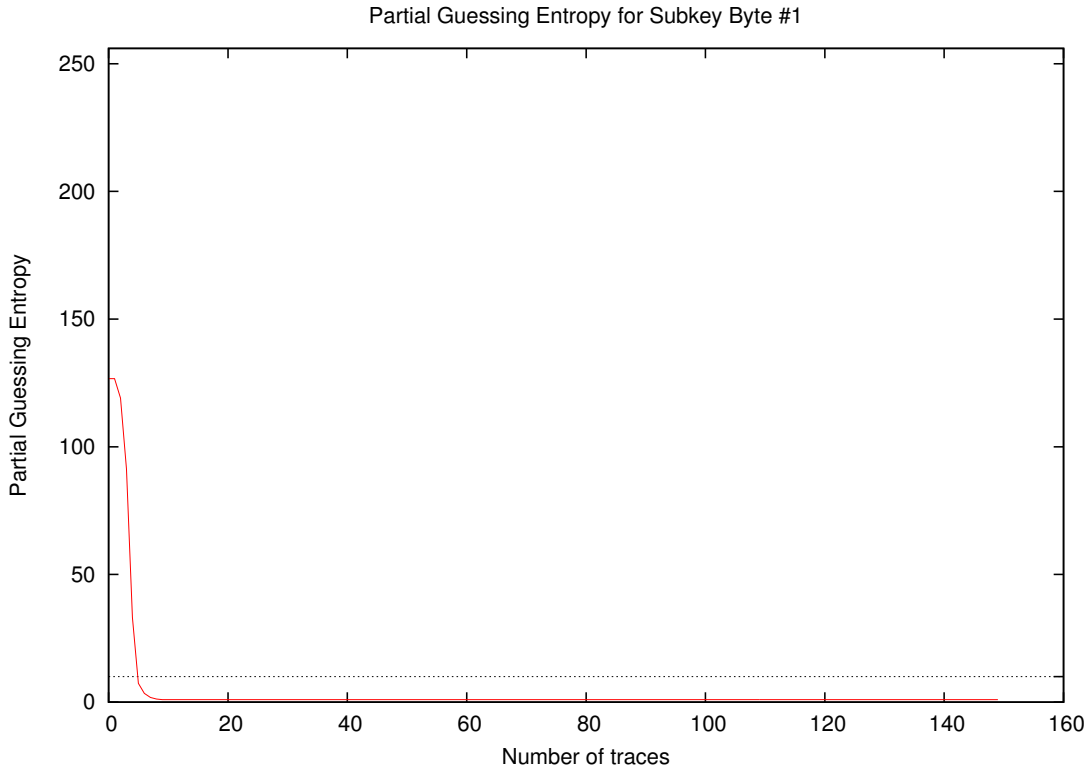

Partial Success Rate for Subkey Byte #16
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
20
40
60
80
100
120
140
160

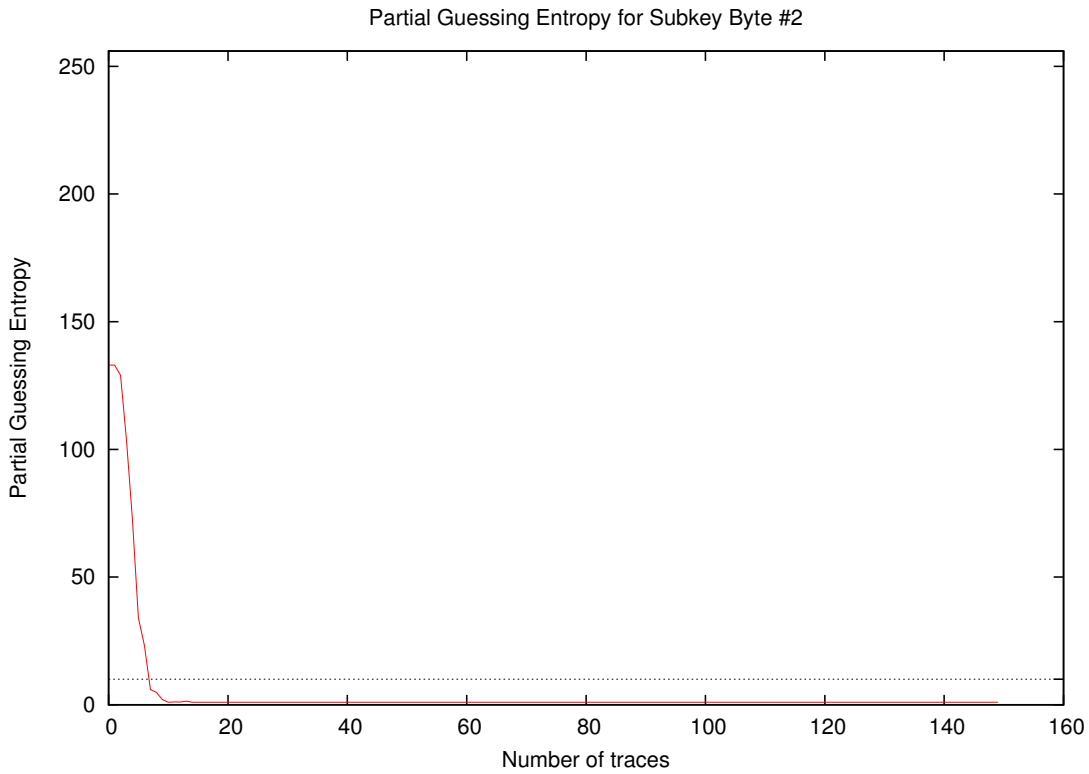

Partial Success Rate for Subkey Bytes #1 to #8
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
20
40
60
80
100
120
140
160
01
02
03
04
05
06
07
08

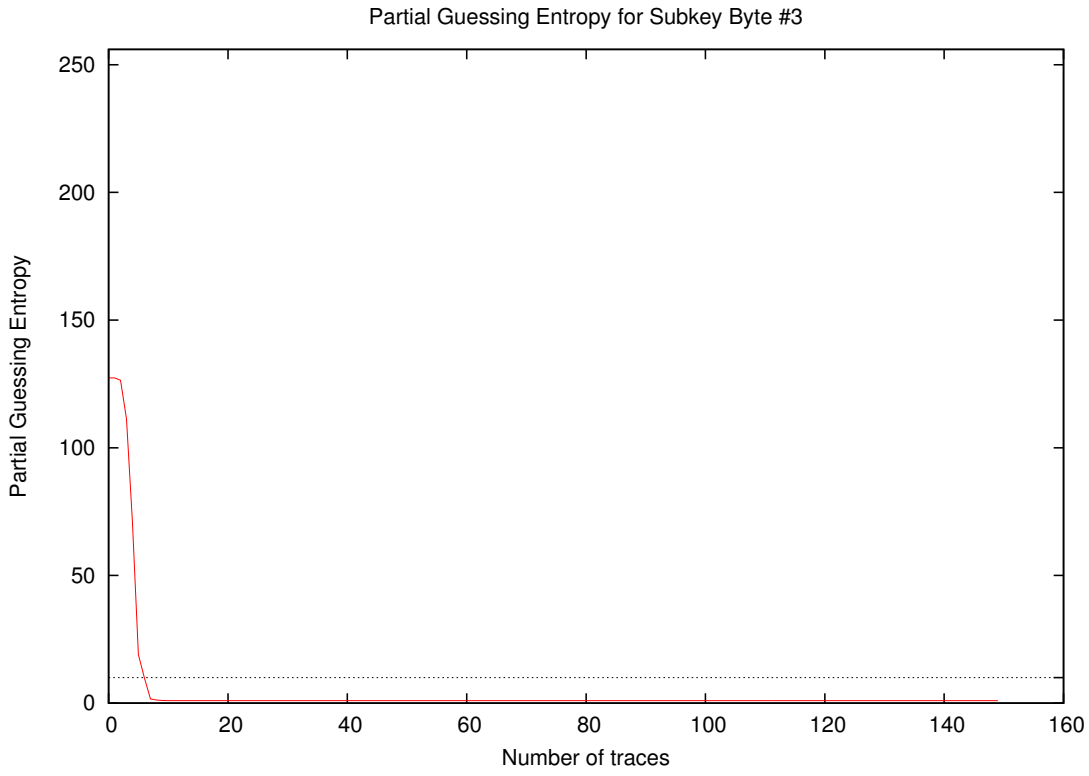

Partial Success Rate for Subkey Bytes #9 to #16
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
20
40
60
80
100
120
140
160
09
10
11
12
13
14
15
16

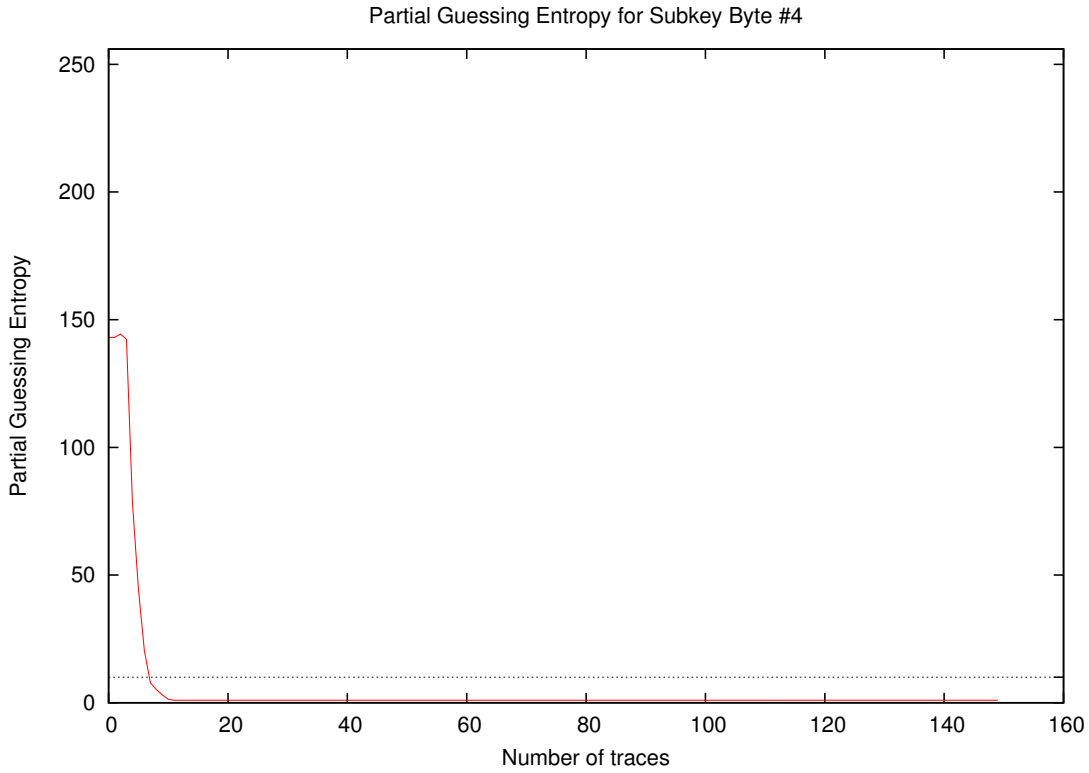
Traces	Partial Success Rate / Byte																Min	Max	Mean
	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16			
10	1.00	0.81	0.94	0.75	0.81	0.75	1.00	0.88	1.00	0.62	1.00	0.75	0.94	0.75	0.94	0.94	0.62	1.00	0.87
20	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	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
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

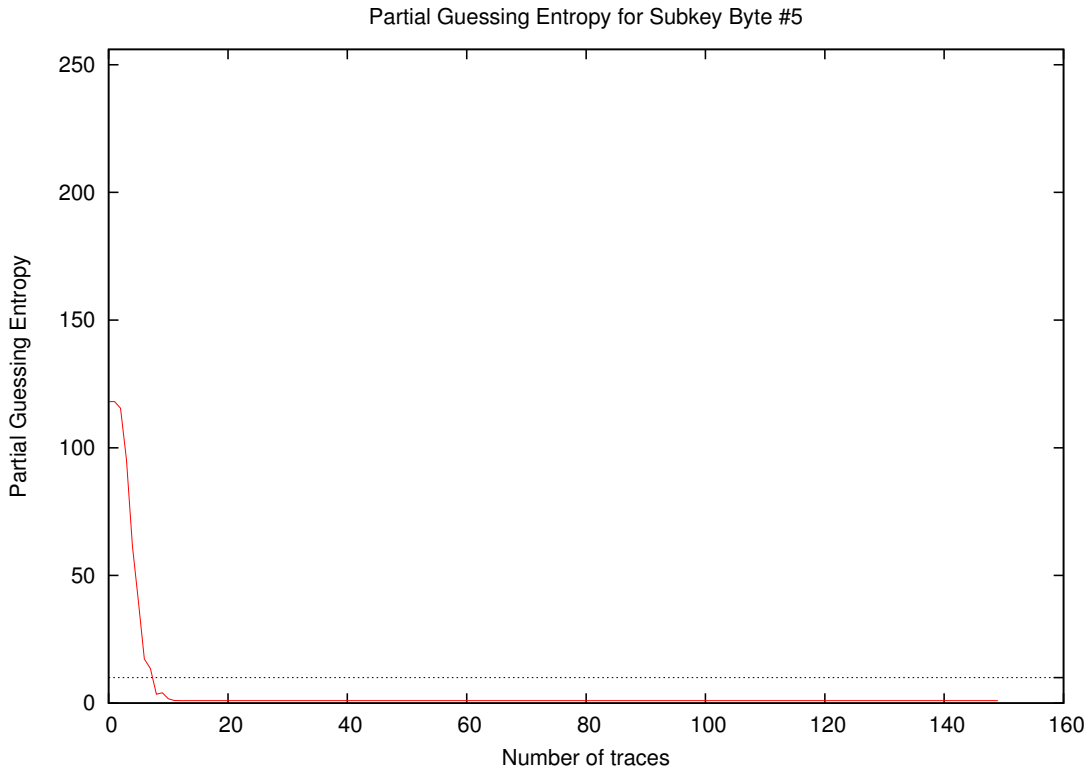
4 Partial Guessing Entropy

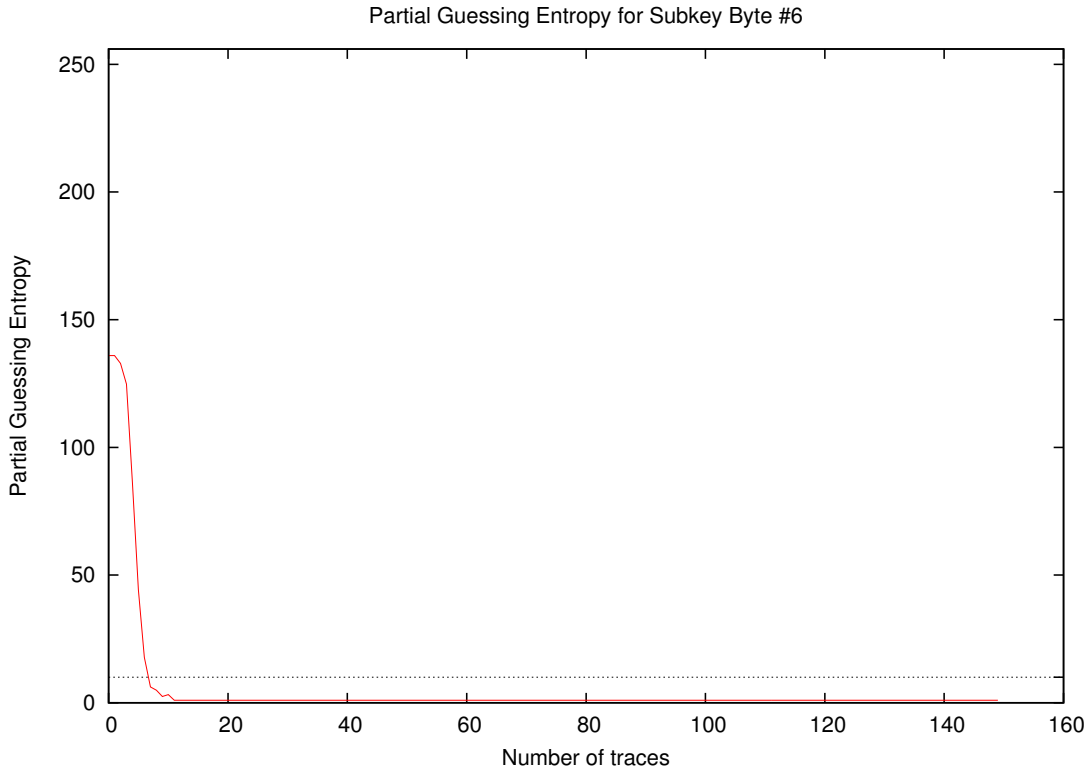


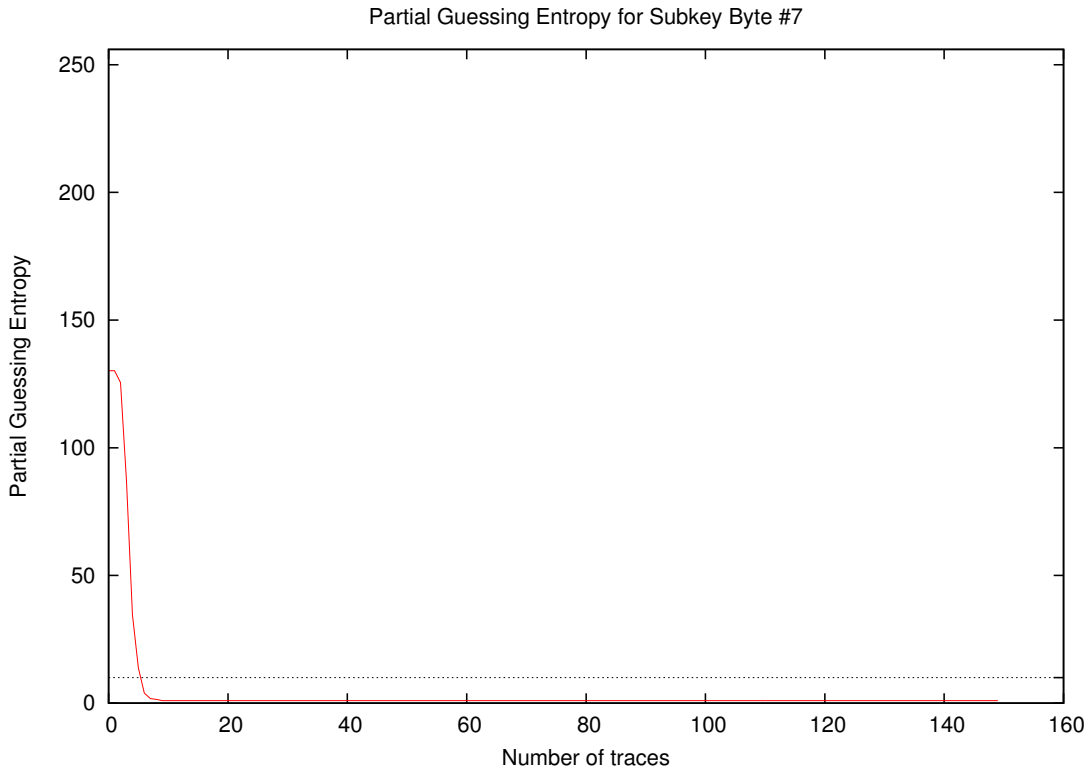


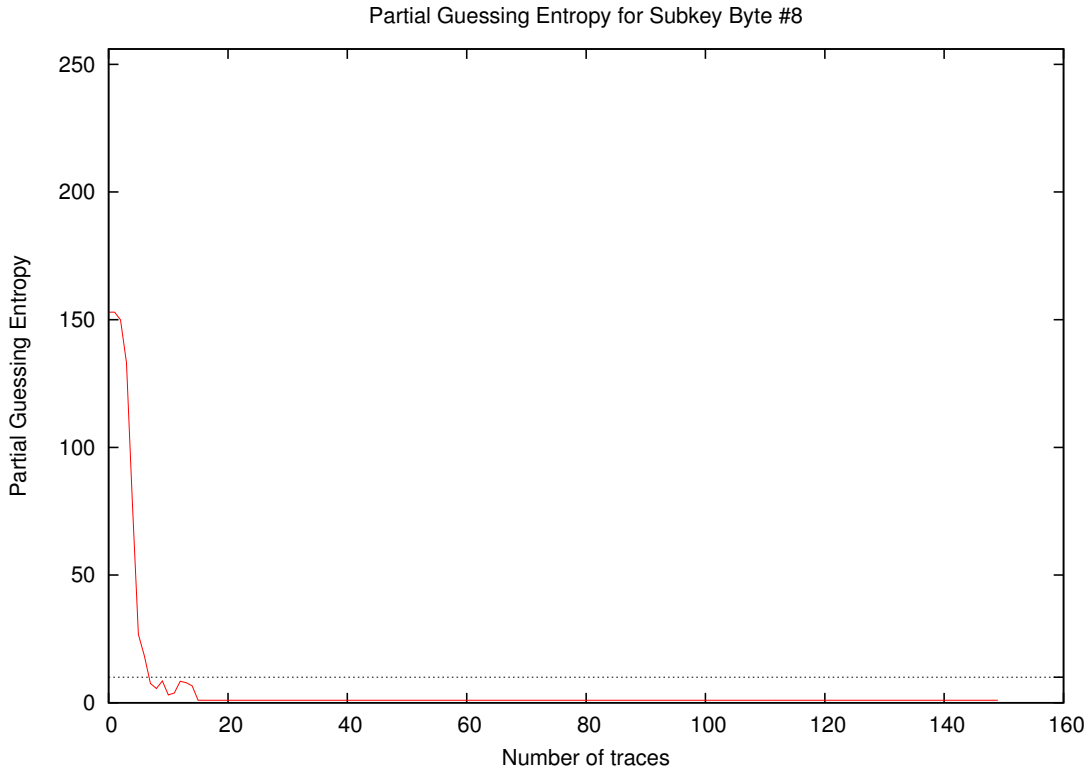

Partial Guessing Entropy for Subkey Byte #3
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
0
20
40
60
80
100
120
140
160

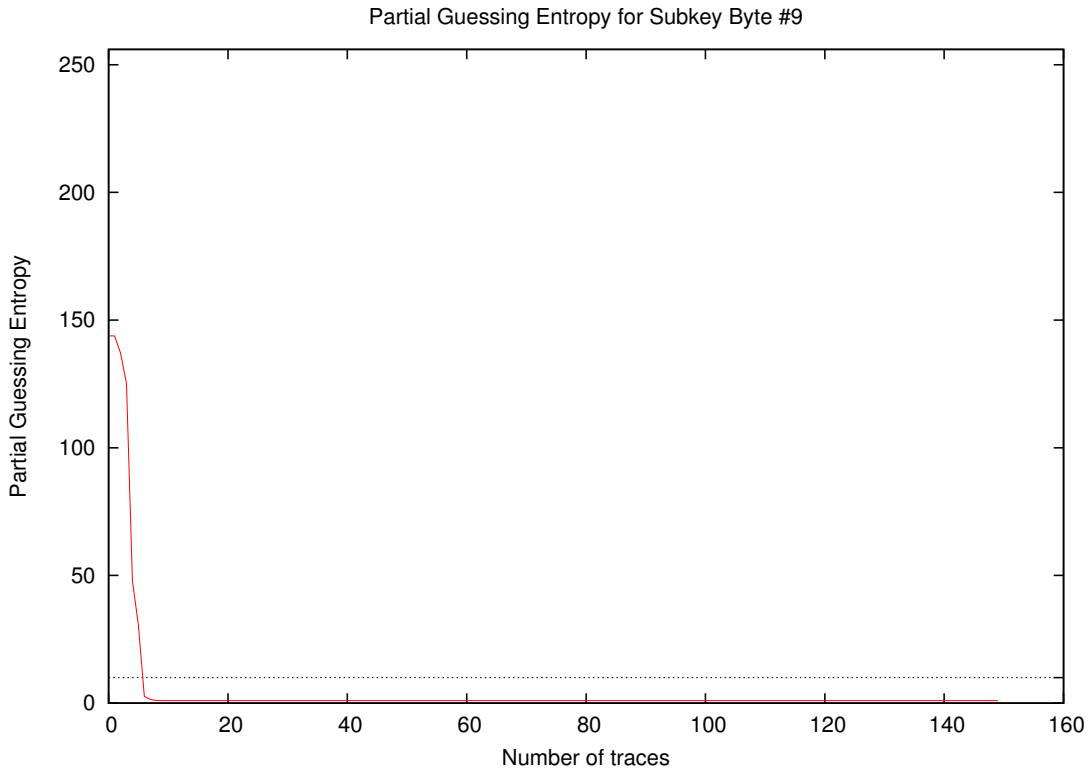

Partial Guessing Entropy for Subkey Byte #4
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
0
20
40
60
80
100
120
140
160

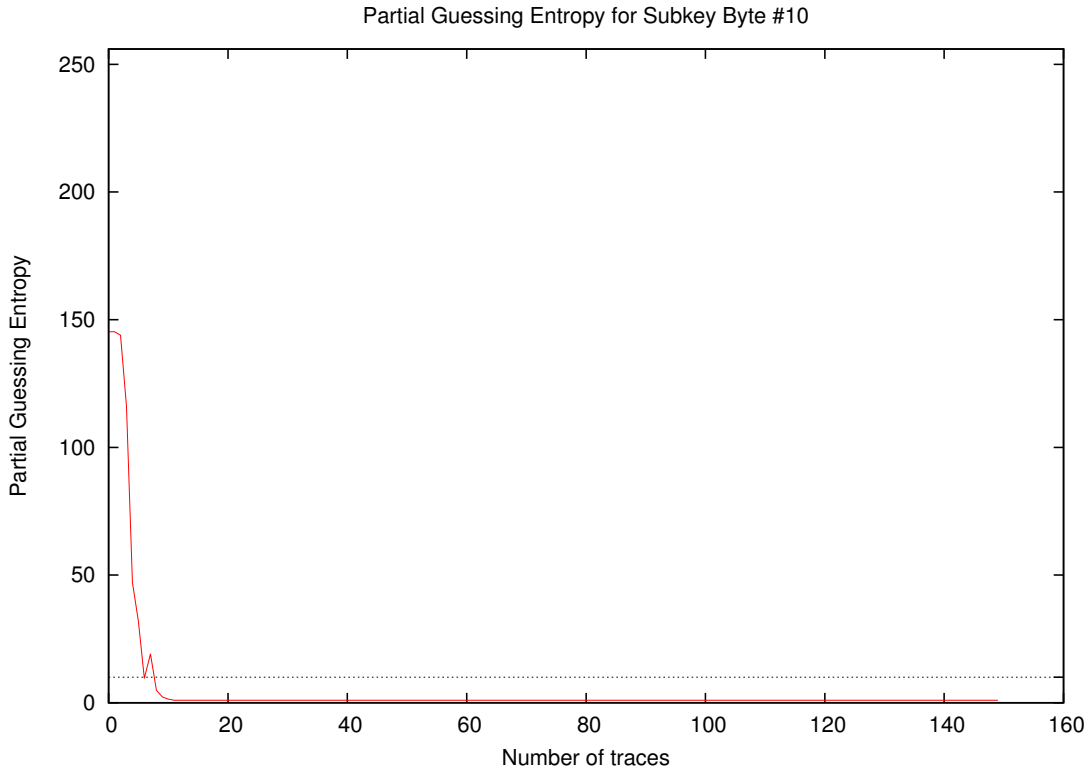

Partial Guessing Entropy for Subkey Byte #5
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
0
20
40
60
80
100
120
140
160

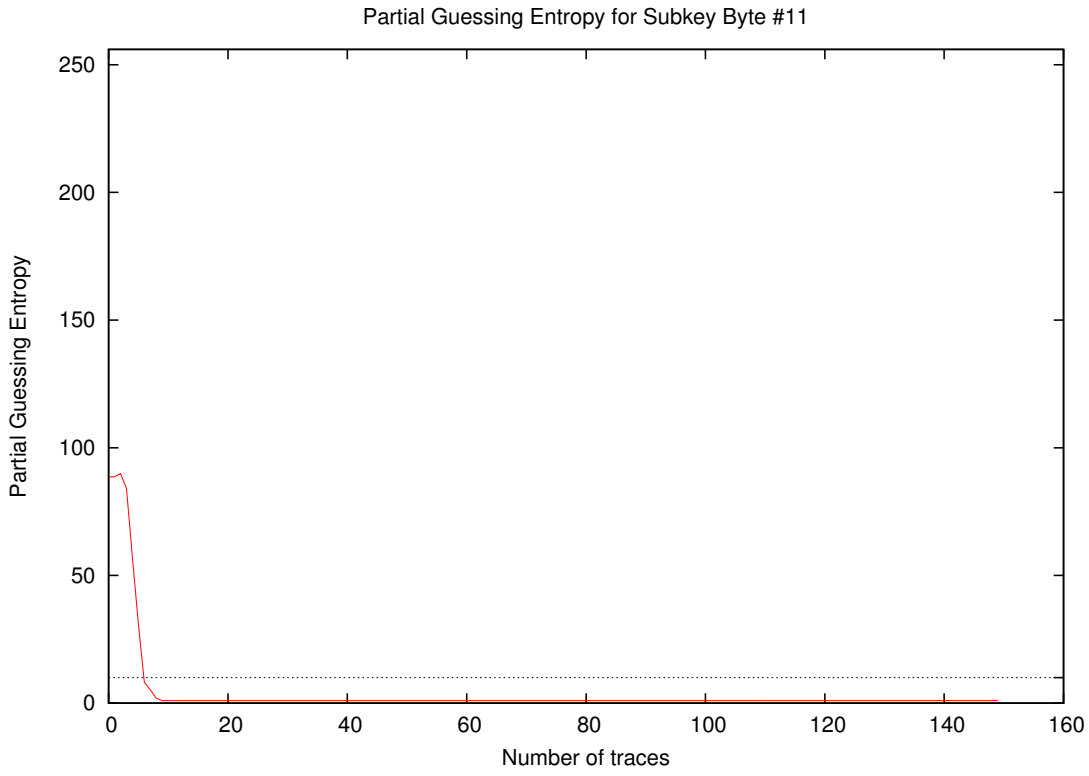

Partial Guessing Entropy for Subkey Byte #6
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
0
20
40
60
80
100
120
140
160

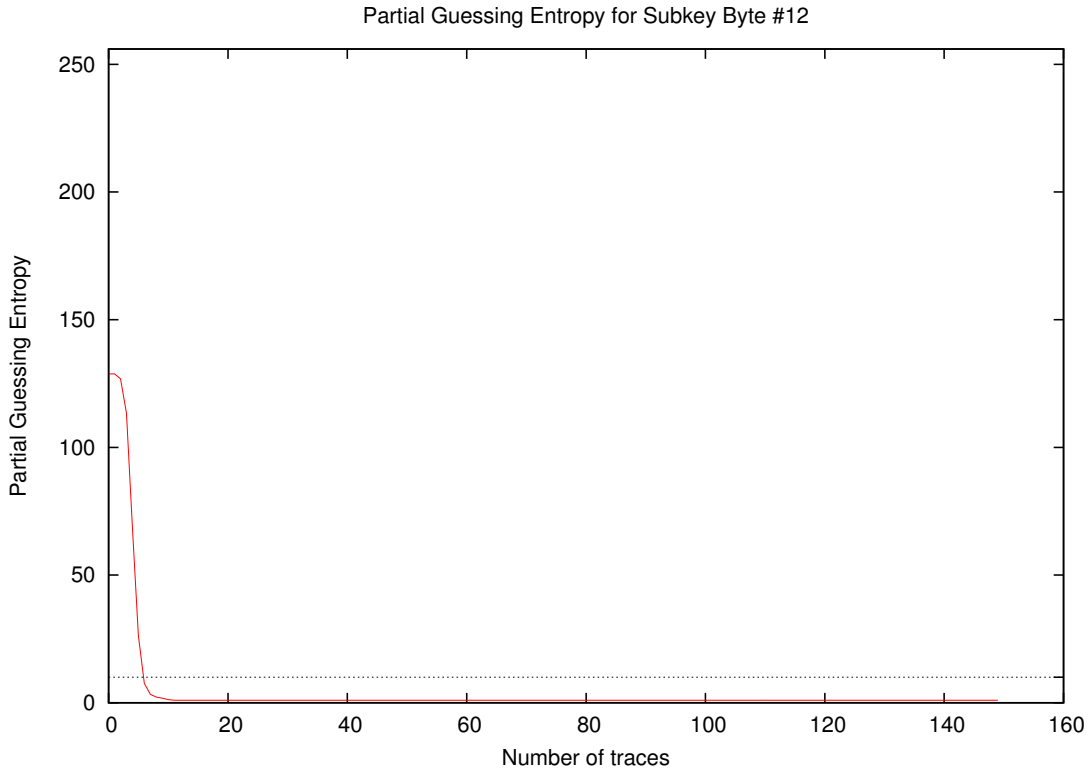

Partial Guessing Entropy for Subkey Byte #7
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
0
20
40
60
80
100
120
140
160

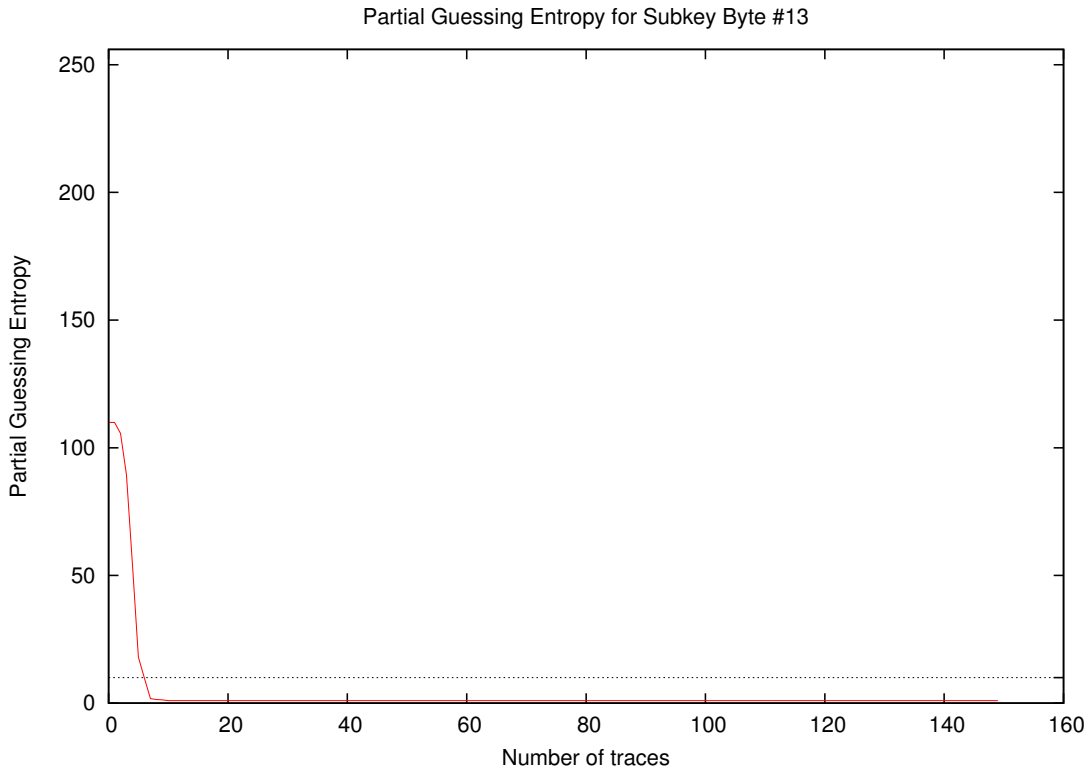

Partial Guessing Entropy for Subkey Byte #8
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
0
20
40
60
80
100
120
140
160

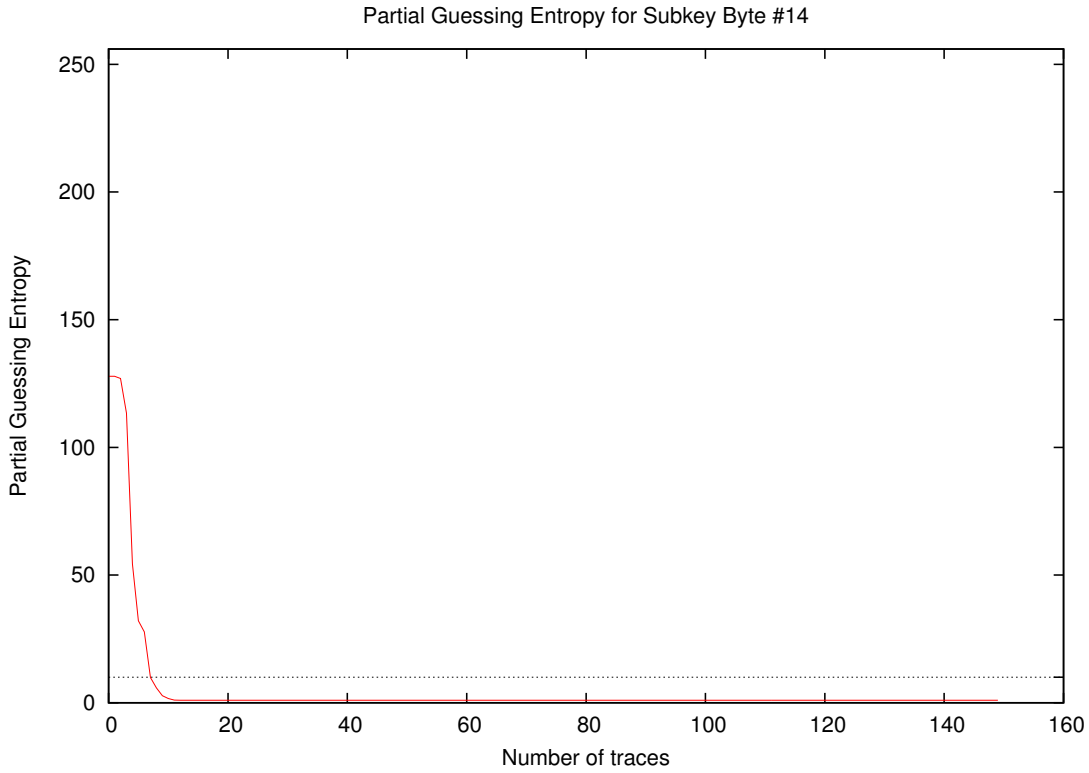

Partial Guessing Entropy for Subkey Byte #9
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
0
20
40
60
80
100
120
140
160

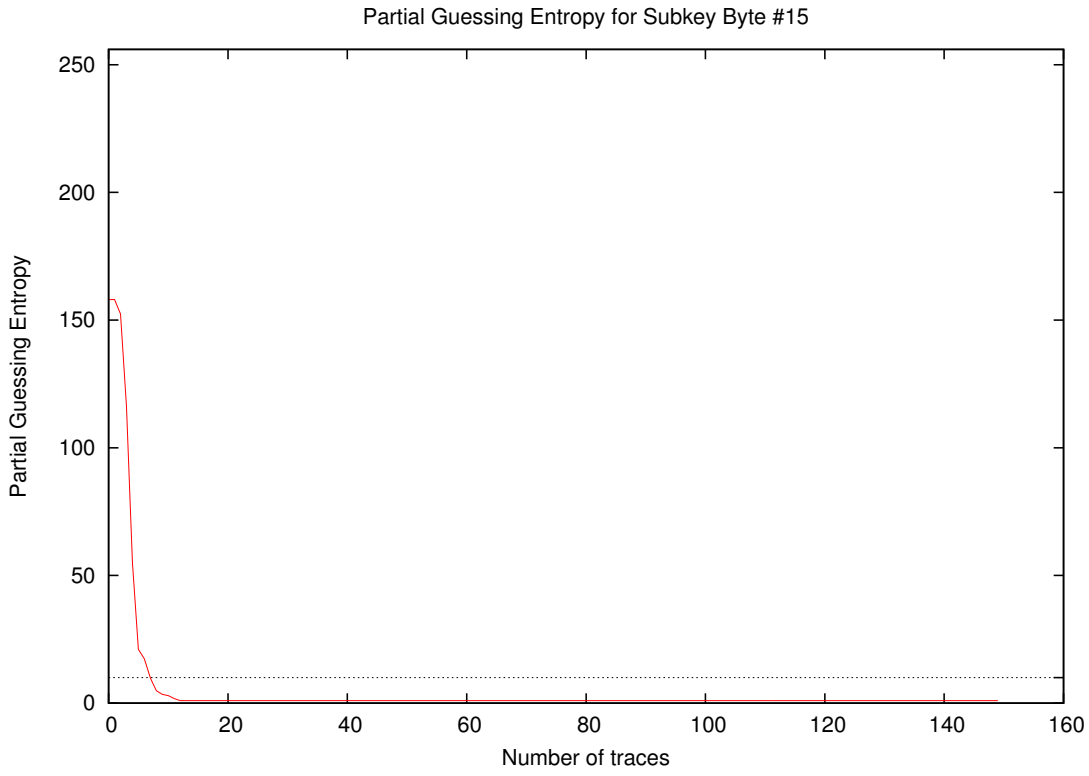

Partial Guessing Entropy for Subkey Byte #10
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
0
20
40
60
80
100
120
140
160

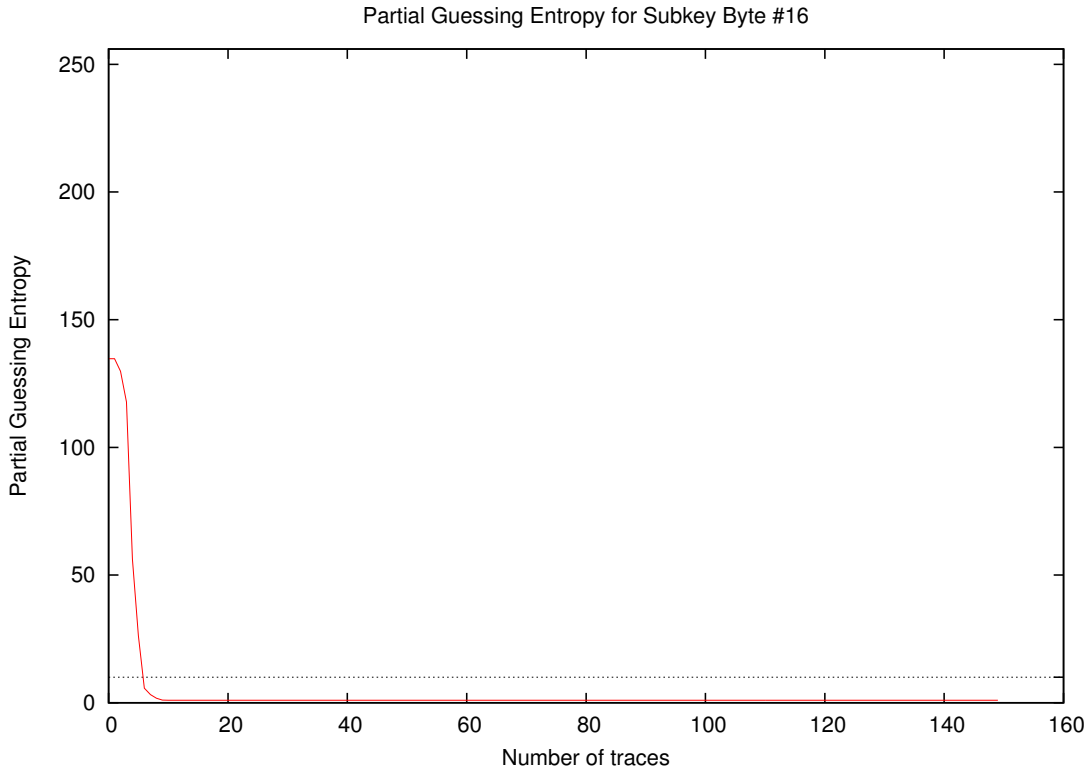

Partial Guessing Entropy for Subkey Byte #11
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
0
20
40
60
80
100
120
140
160

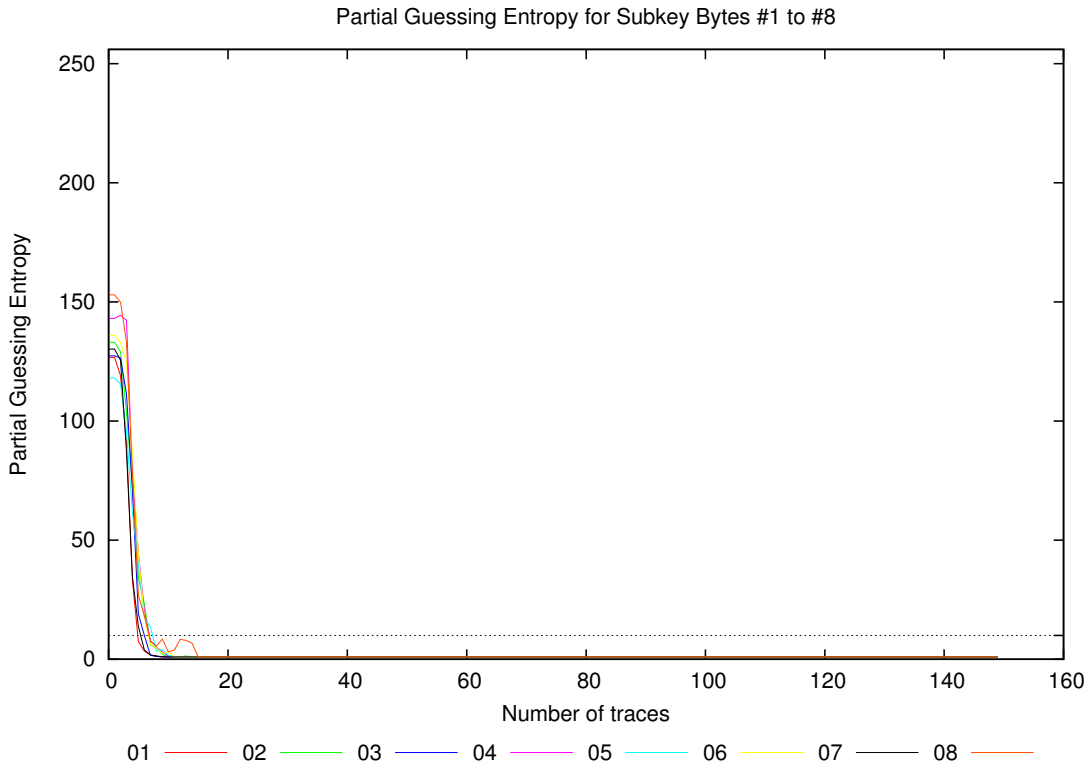

Partial Guessing Entropy for Subkey Byte #12
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
0
20
40
60
80
100
120
140
160

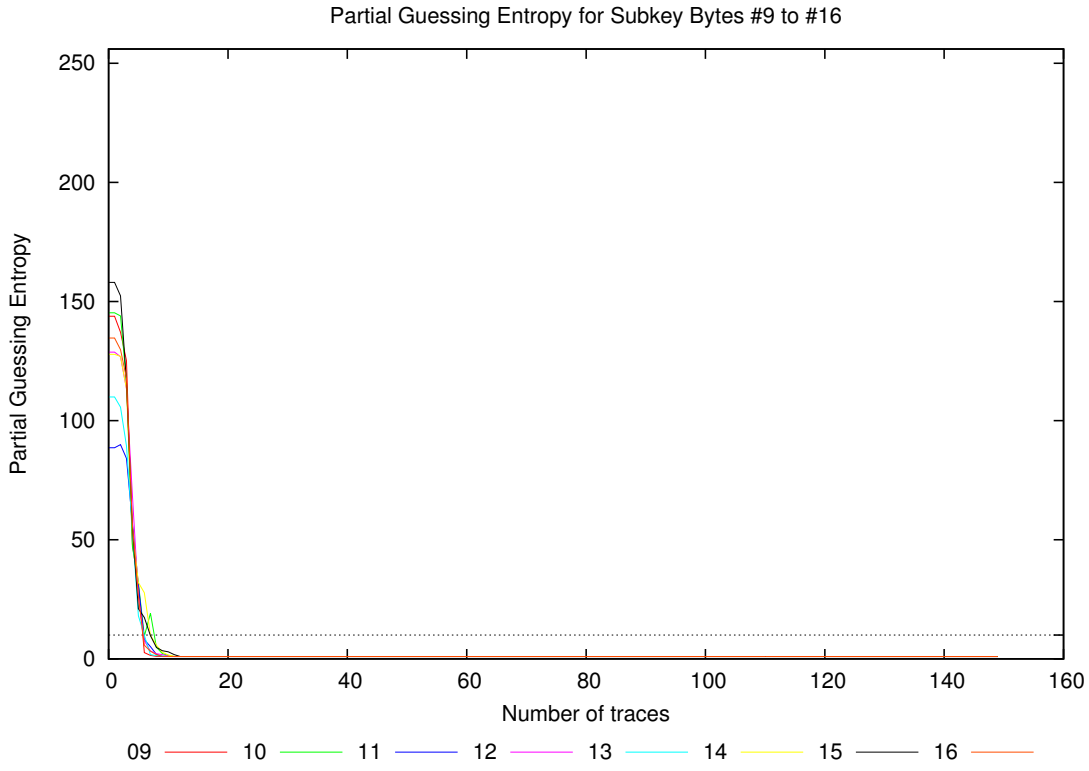

Partial Guessing Entropy for Subkey Byte #13
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
0
20
40
60
80
100
120
140
160


Partial Guessing Entropy for Subkey Byte #14
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
0
20
40
60
80
100
120
140
160


Partial Guessing Entropy for Subkey Byte #15
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
0
20
40
60
80
100
120
140
160


Partial Guessing Entropy for Subkey Byte #16
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
0
20
40
60
80
100
120
140
160


Partial Guessing Entropy for Subkey Bytes #1 to #8
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
0
20
40
60
80
100
120
140
160
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
20
40
60
80
100
120
140
160
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	2.0	1.1	3.1	4.1	2.4	1.0	8.5	1.0	2.2	1.0	1.8	1.2	2.8	3.4	1.1	1.0	8.5	2.4
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
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