DPA Contest v4.2
Evaluation results

Zeyi Liu, Neng Gao, Yuan Zhao, Jia Zhuang

February 2016

1 Introduction

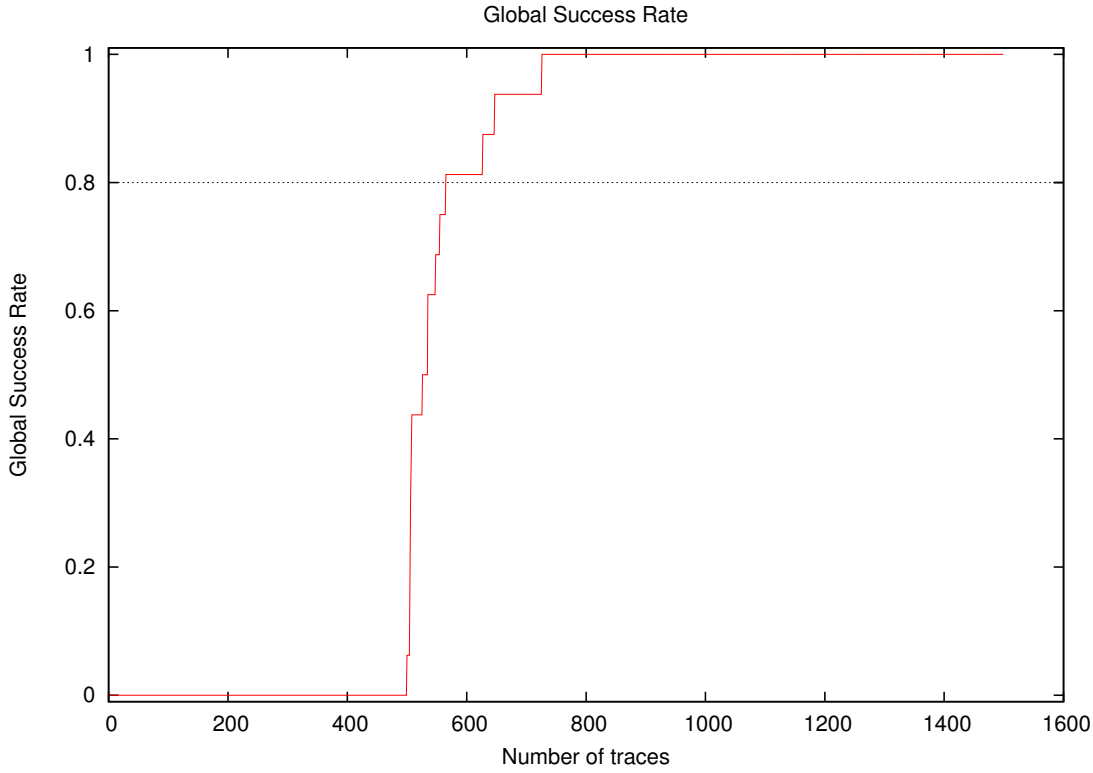
1.1 About the attack

- **Attack Name:** P4
- **Sender/Team:** Zeyi Liu, Neng Gao, Yuan Zhao, Jia Zhuang
- **Institution:** Data Assurance and Communication Security Research Center, CAS, China
- **Language:** C#
- **Operating system:** Windows
- **Attacked subkey:** 0

1.2 About the evaluation

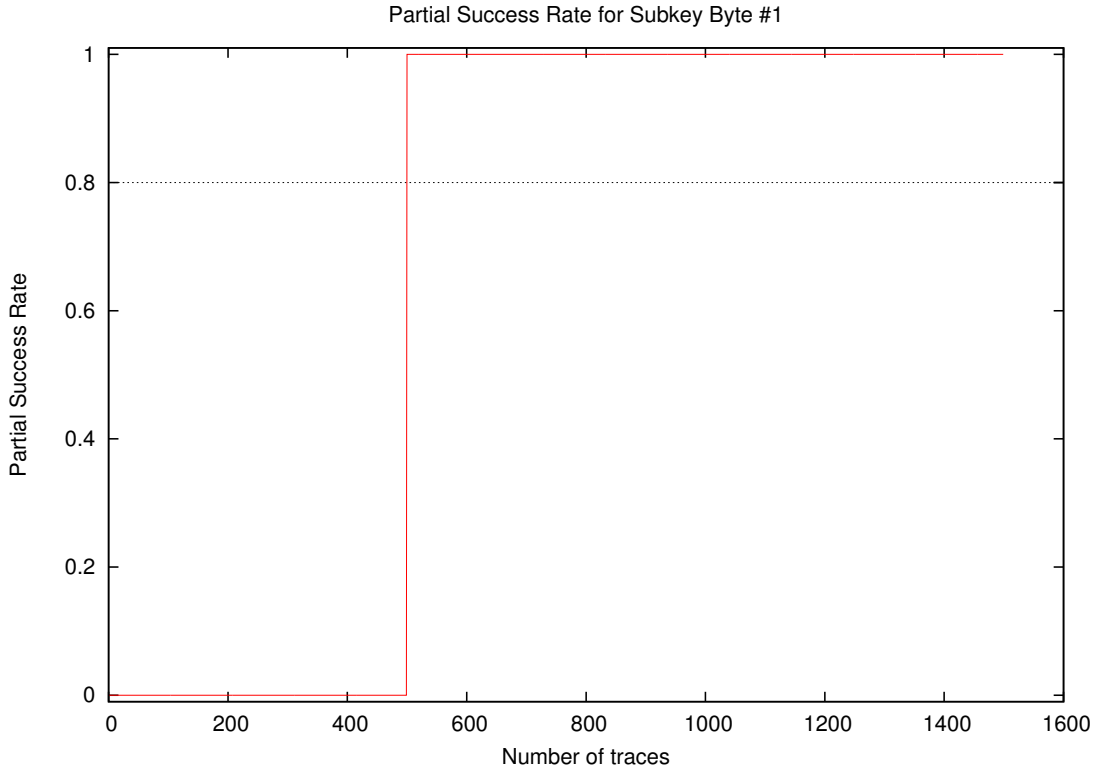
- **Date of evaluation:** February 2016

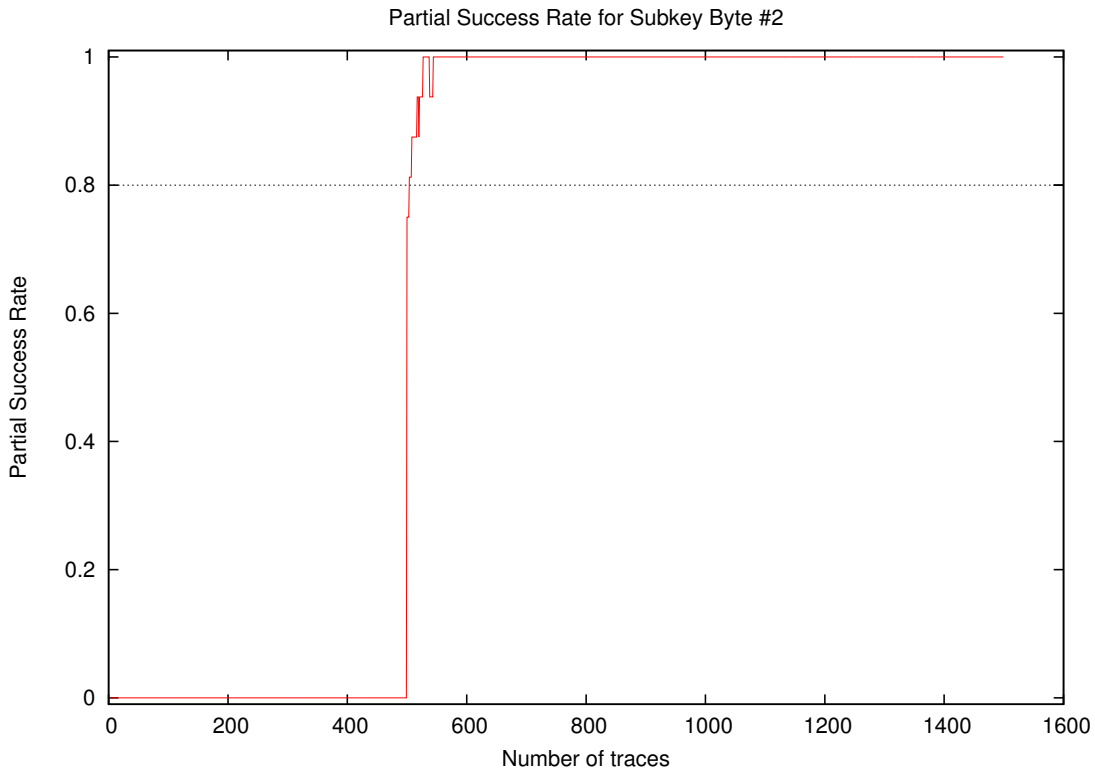
2 Global Success Rate

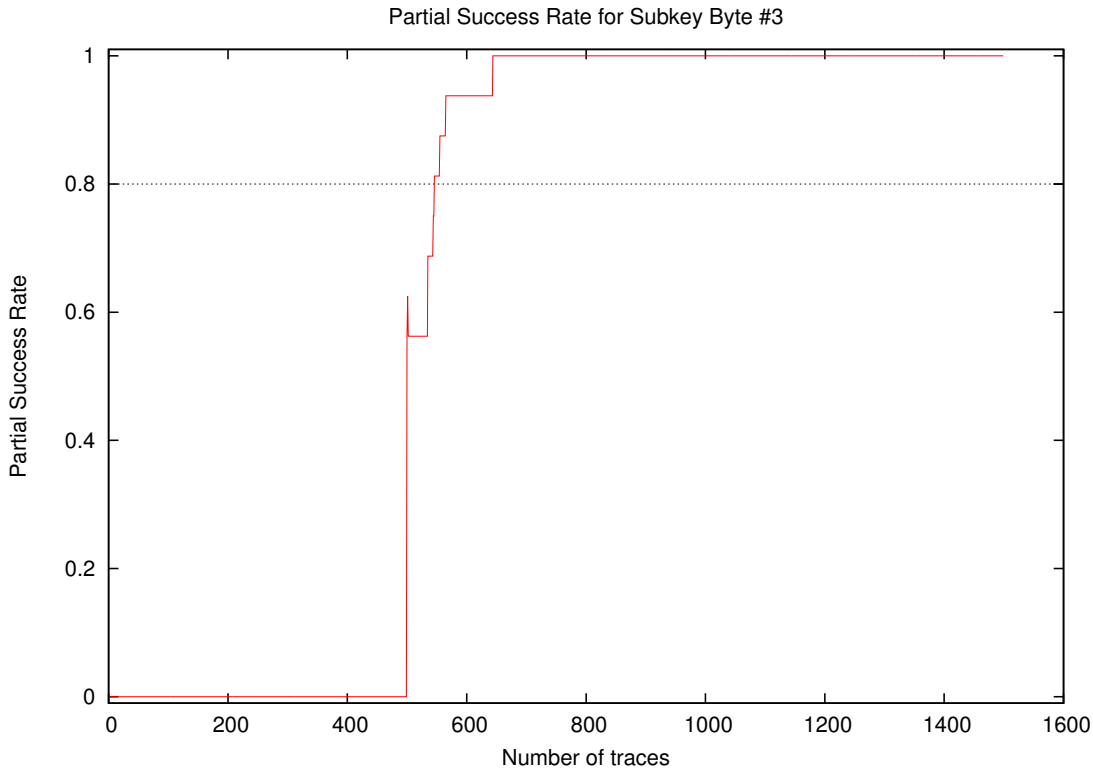


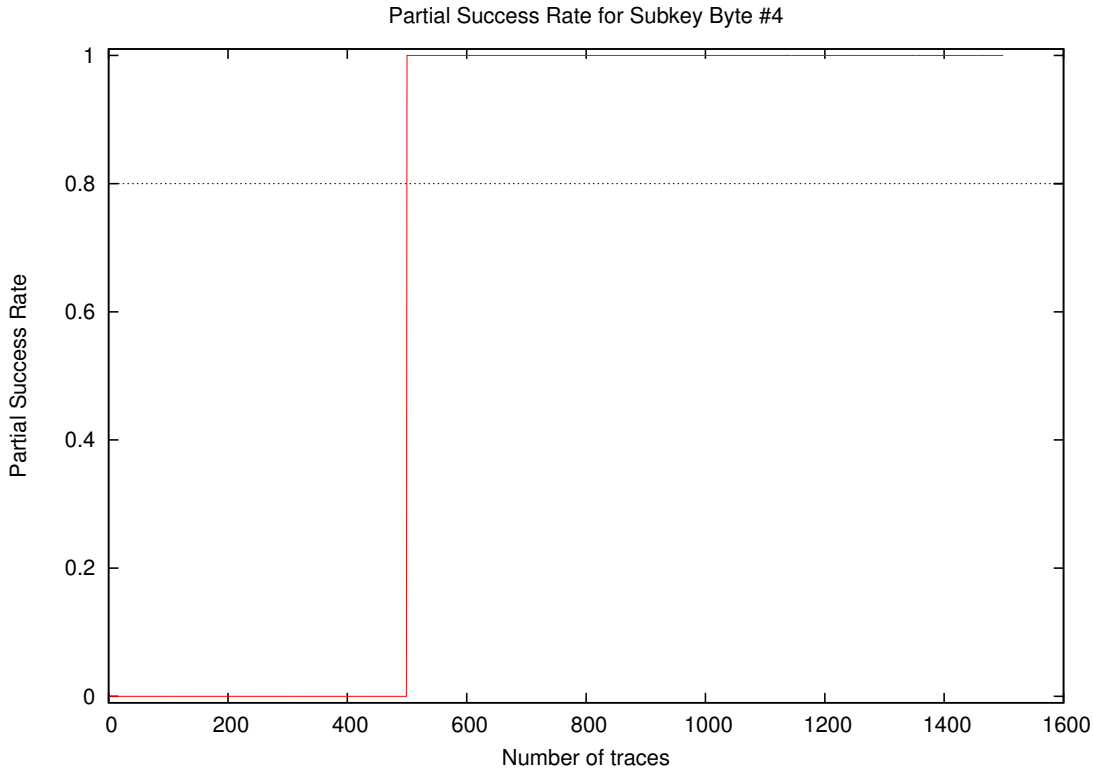
Number of traces	Global Success Rate
10	0.00
20	0.00
30	0.00
40	0.00
50	0.00
100	0.00
200	0.00
300	0.00
400	0.00
500	0.00
600	0.81
700	0.94
800	1.00
900	1.00
1000	1.00

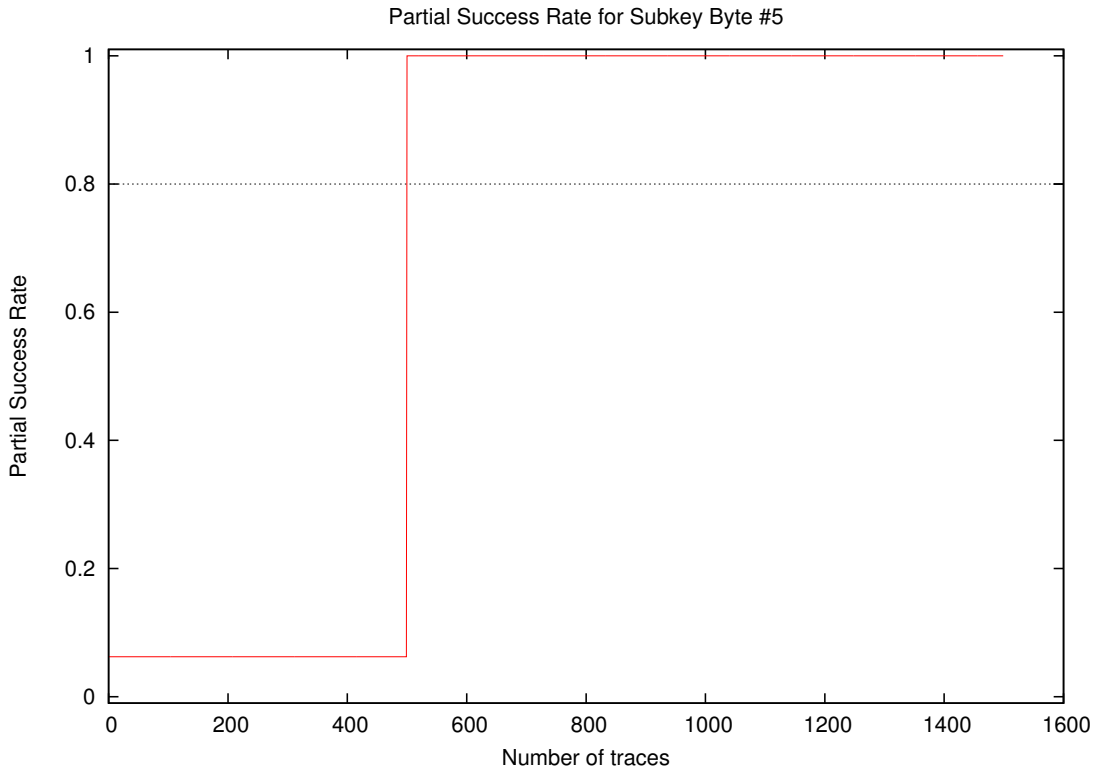
3 Partial Success Rate

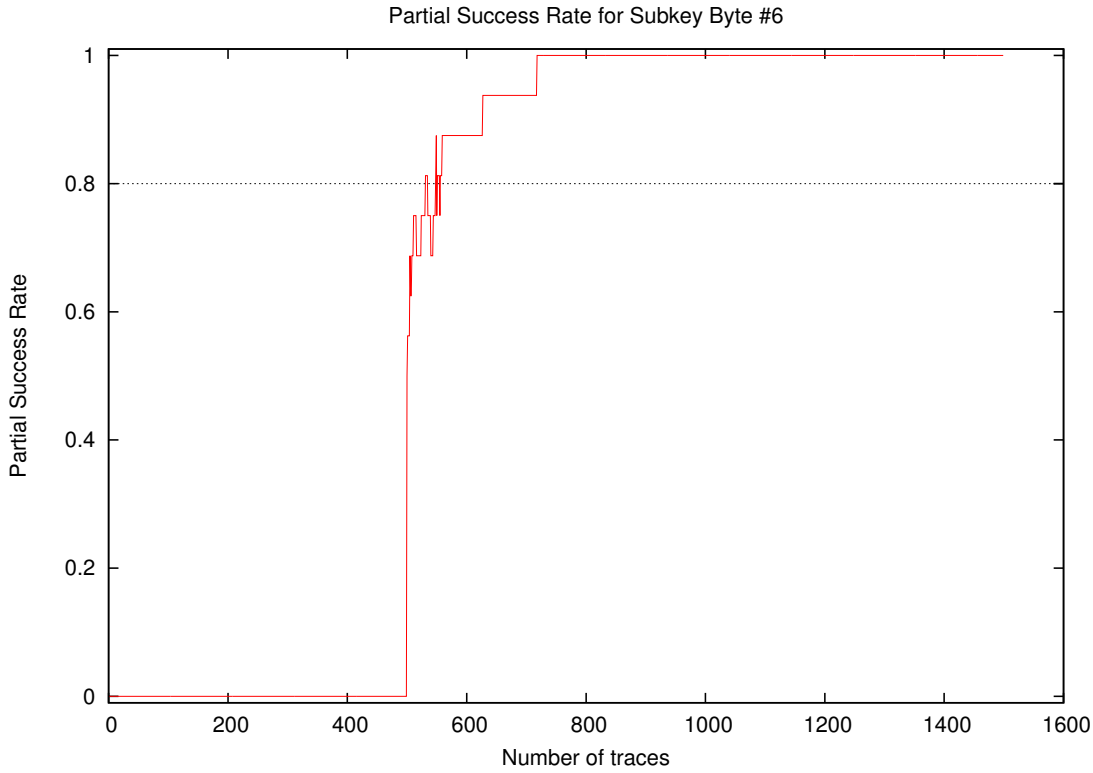


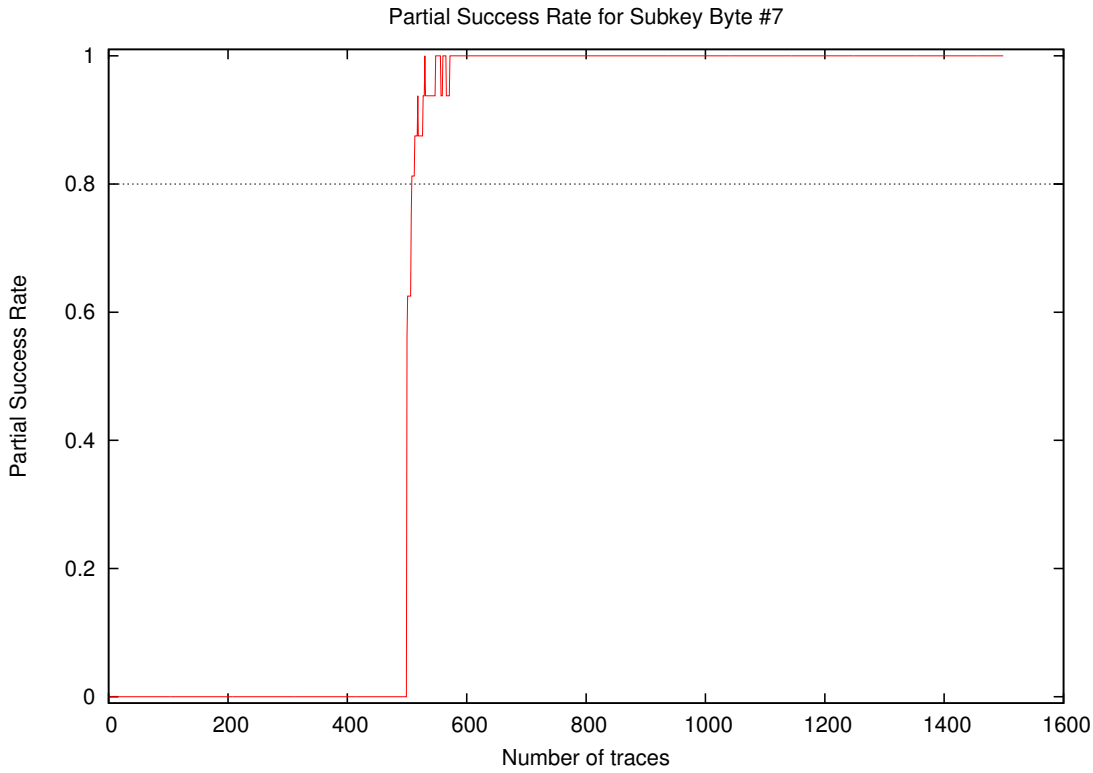


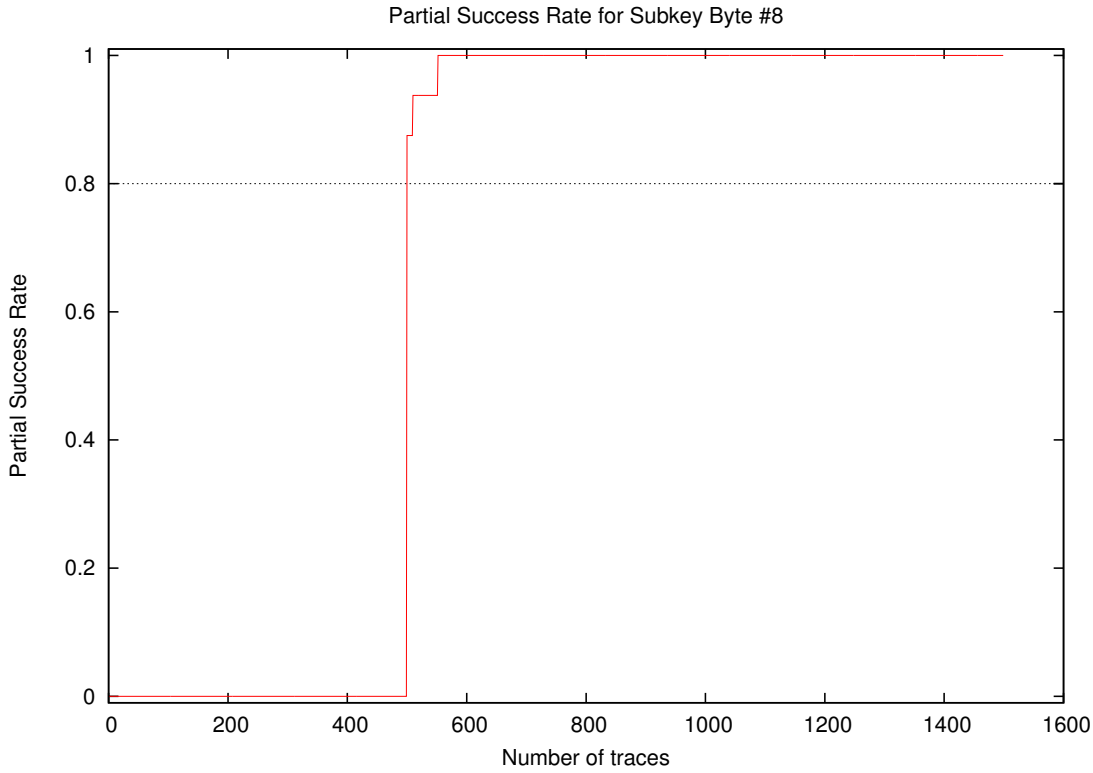

Partial Success Rate for Subkey Byte #3
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
200
400
600
800
1000
1200
1400
1600

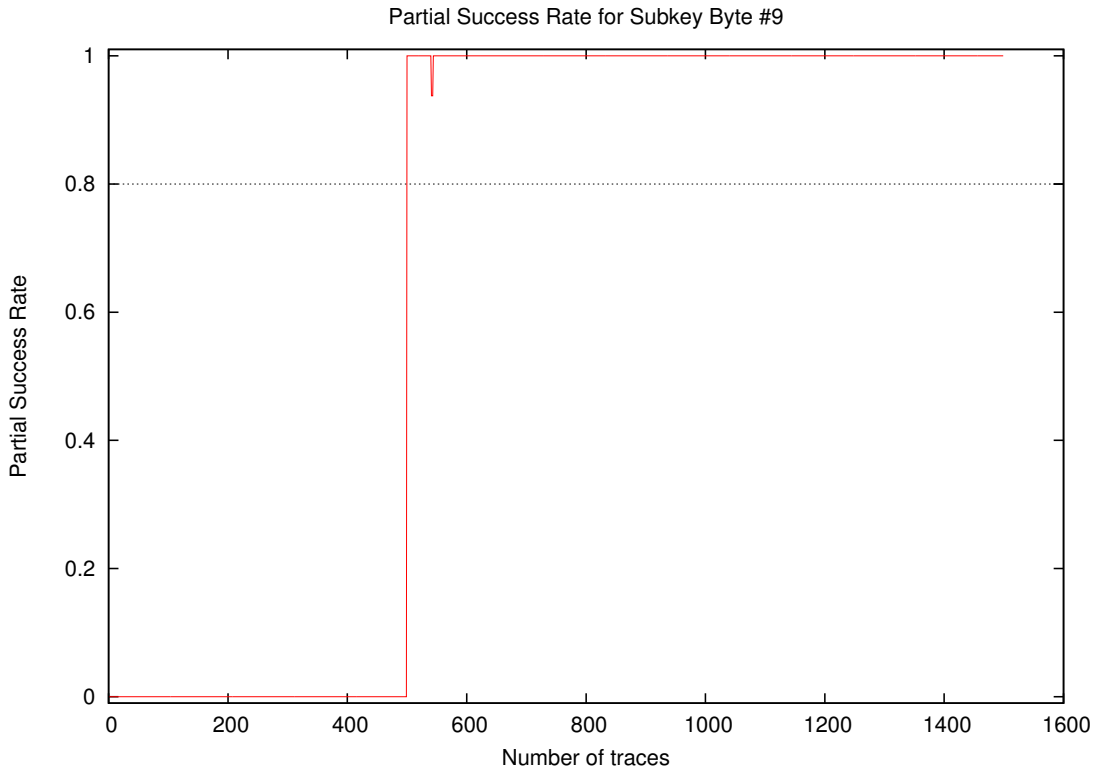

Partial Success Rate for Subkey Byte #4
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
200
400
600
800
1000
1200
1400
1600

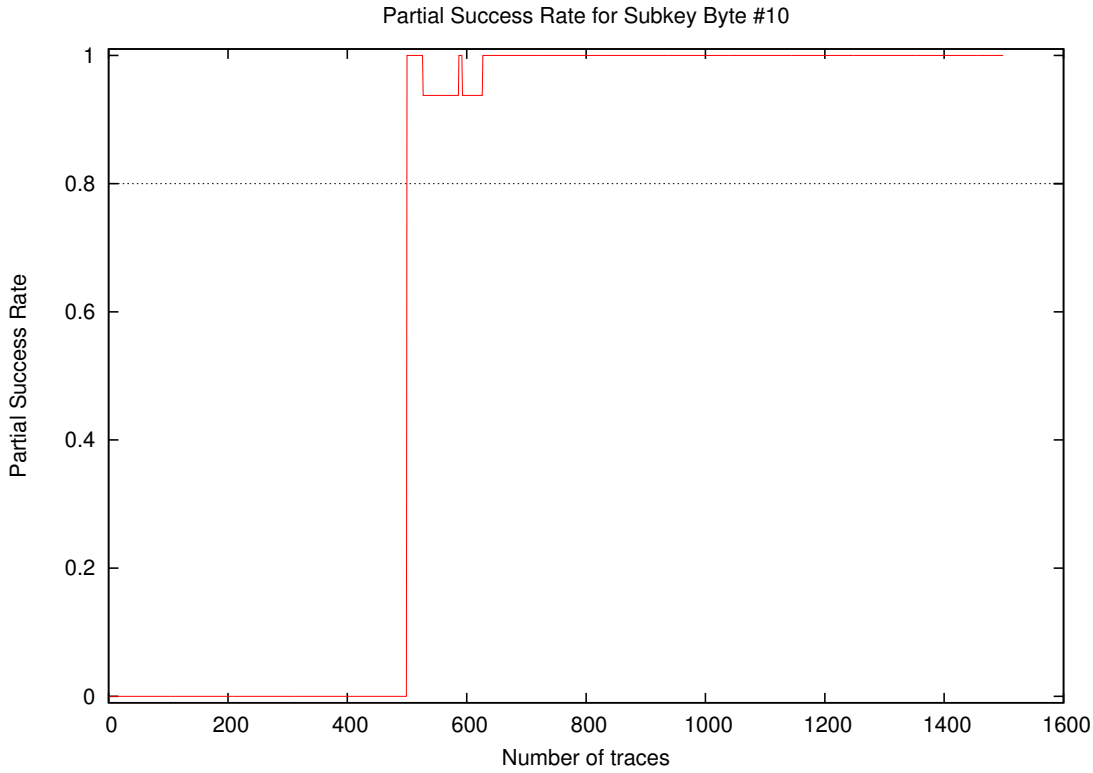

Partial Success Rate for Subkey Byte #5
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
200
400
600
800
1000
1200
1400
1600

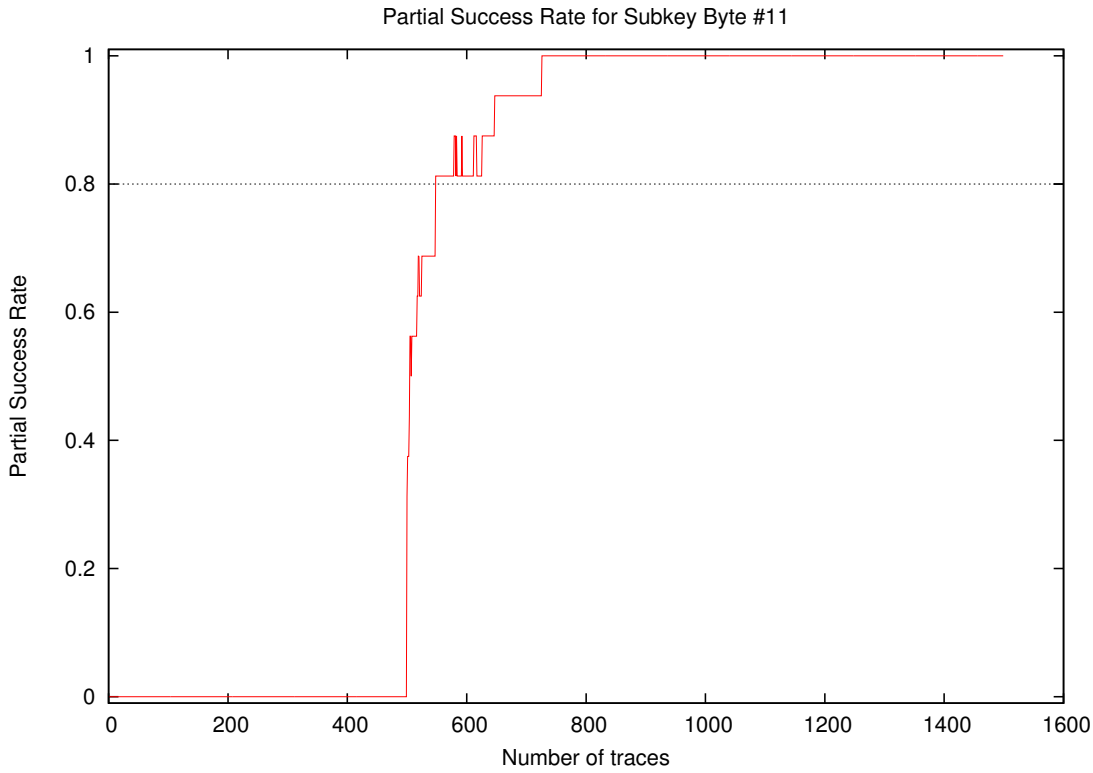

Partial Success Rate for Subkey Byte #6
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
200
400
600
800
1000
1200
1400
1600

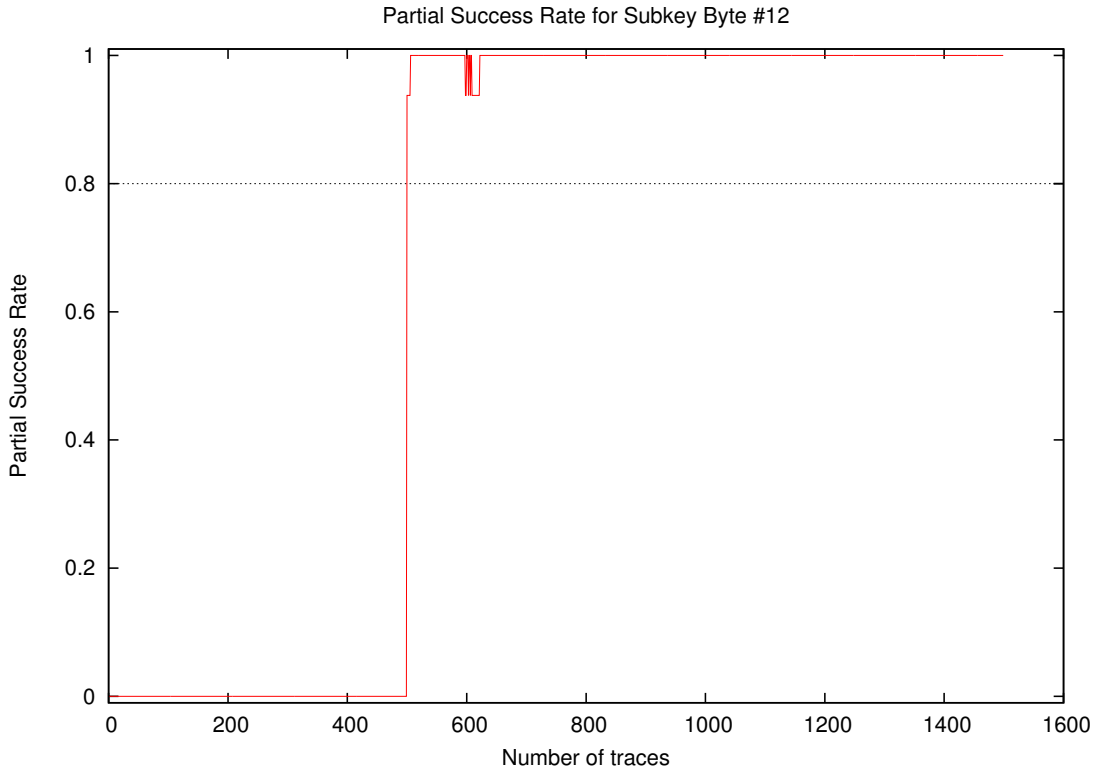

Partial Success Rate for Subkey Byte #7
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
200
400
600
800
1000
1200
1400
1600

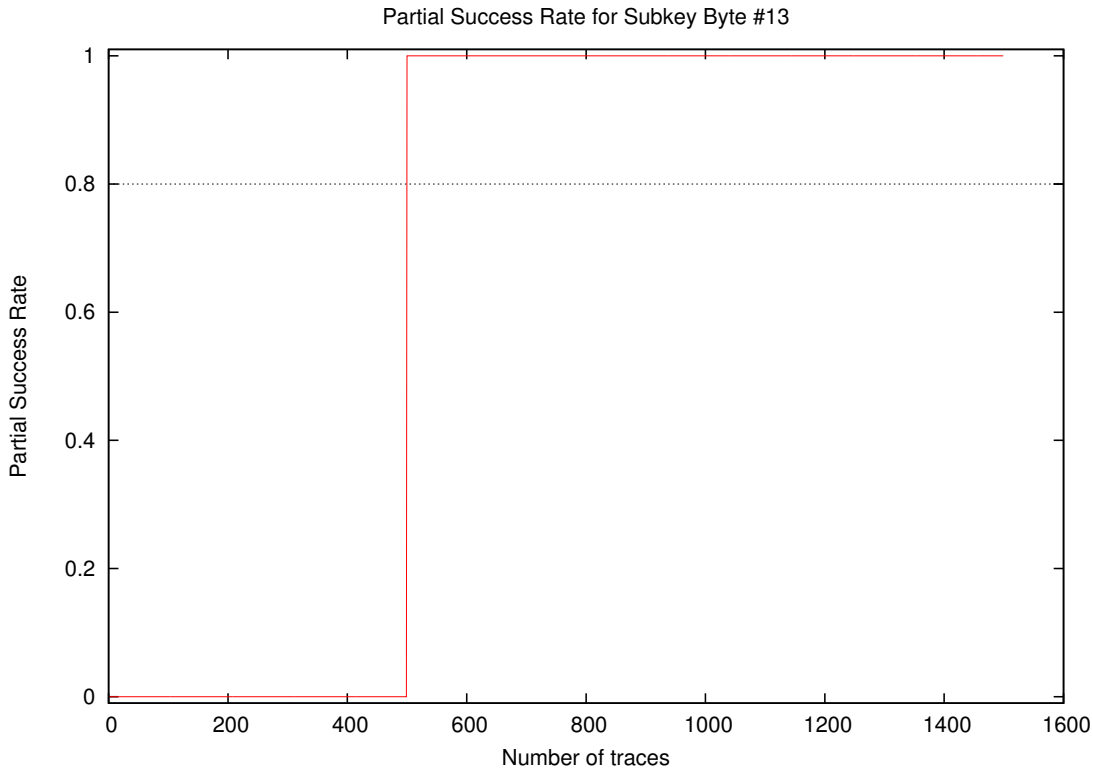

Partial Success Rate for Subkey Byte #8
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
200
400
600
800
1000
1200
1400
1600

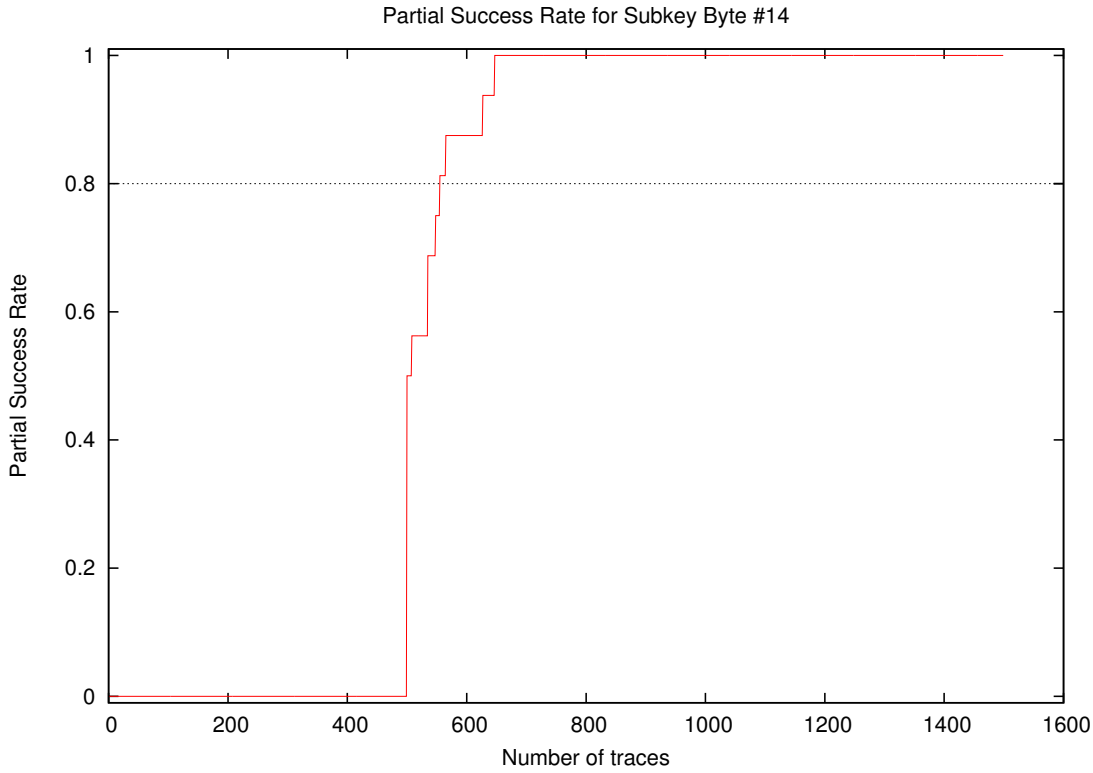

Partial Success Rate for Subkey Byte #9
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
200
400
600
800
1000
1200
1400
1600

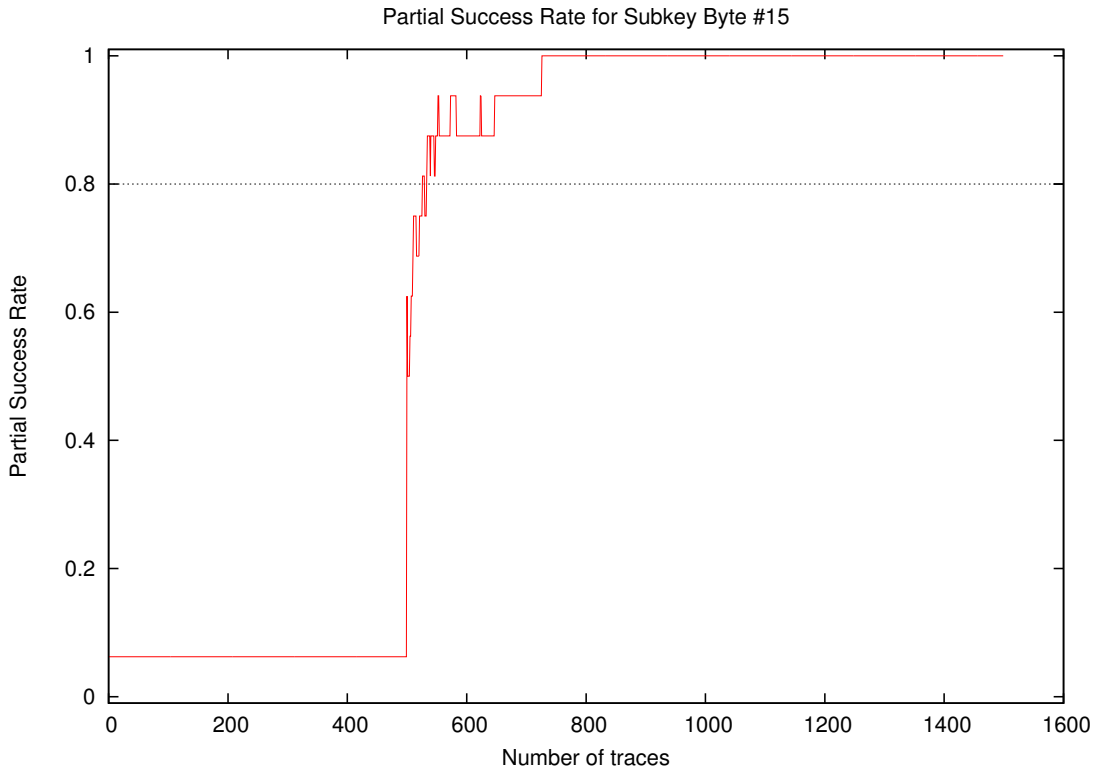

Partial Success Rate for Subkey Byte #10
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
200
400
600
800
1000
1200
1400
1600

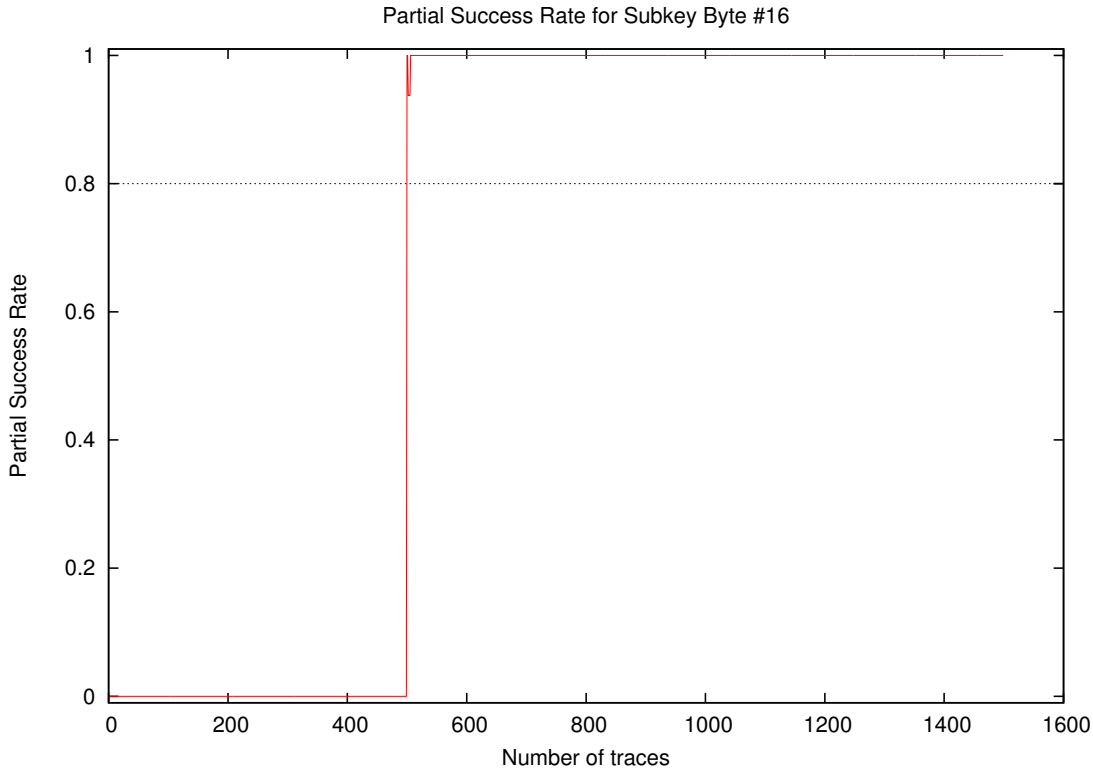

Partial Success Rate for Subkey Byte #11
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
200
400
600
800
1000
1200
1400
1600

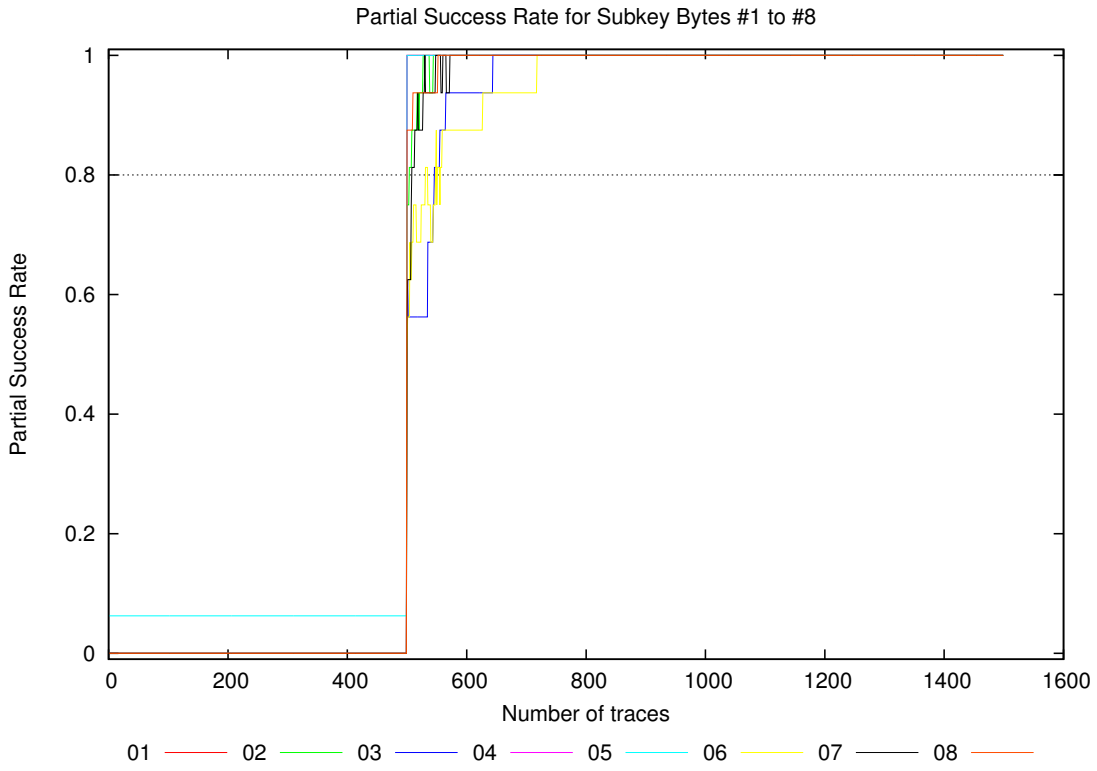

Partial Success Rate for Subkey Byte #12
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
200
400
600
800
1000
1200
1400
1600

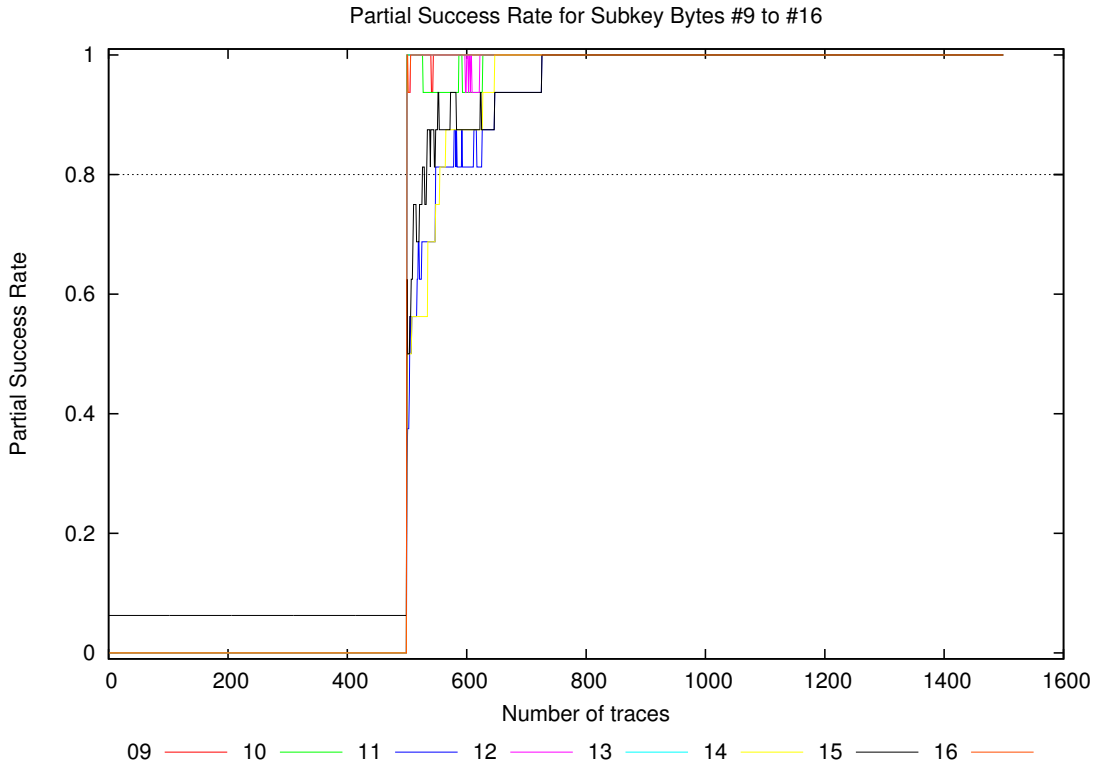

Partial Success Rate for Subkey Byte #13
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
200
400
600
800
1000
1200
1400
1600


Partial Success Rate for Subkey Byte #14
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
200
400
600
800
1000
1200
1400
1600


Partial Success Rate for Subkey Byte #15
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
200
400
600
800
1000
1200
1400
1600

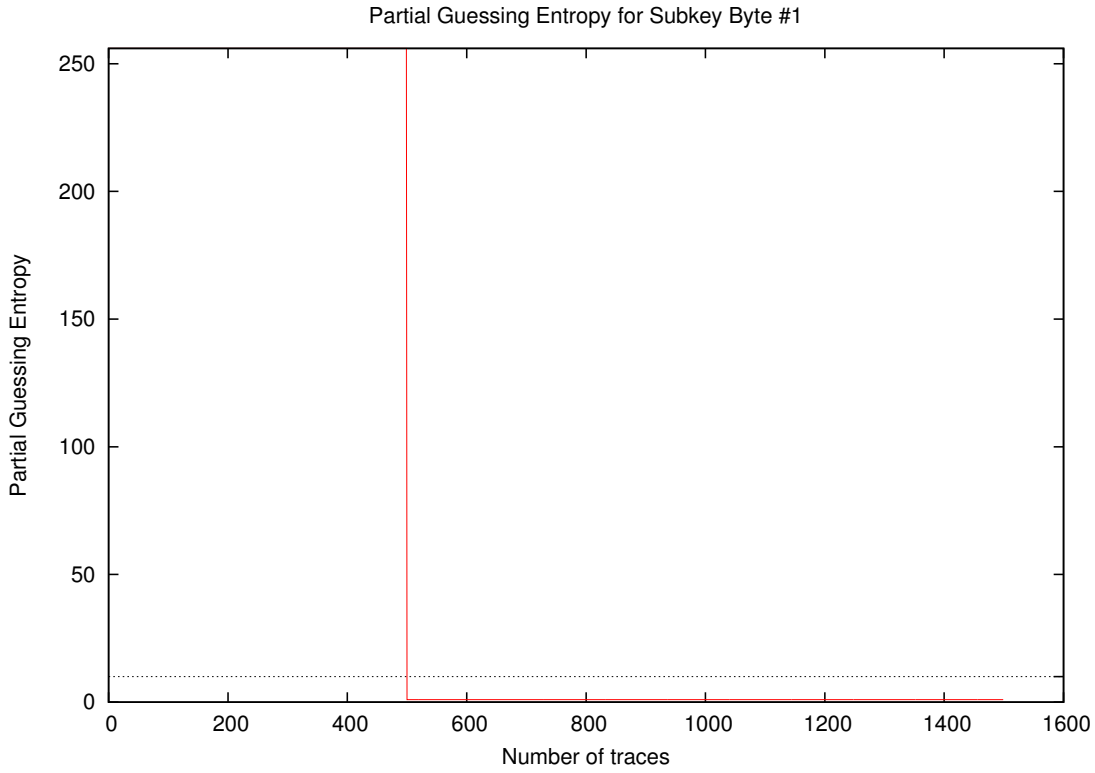

Partial Success Rate for Subkey Byte #16
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
200
400
600
800
1000
1200
1400
1600

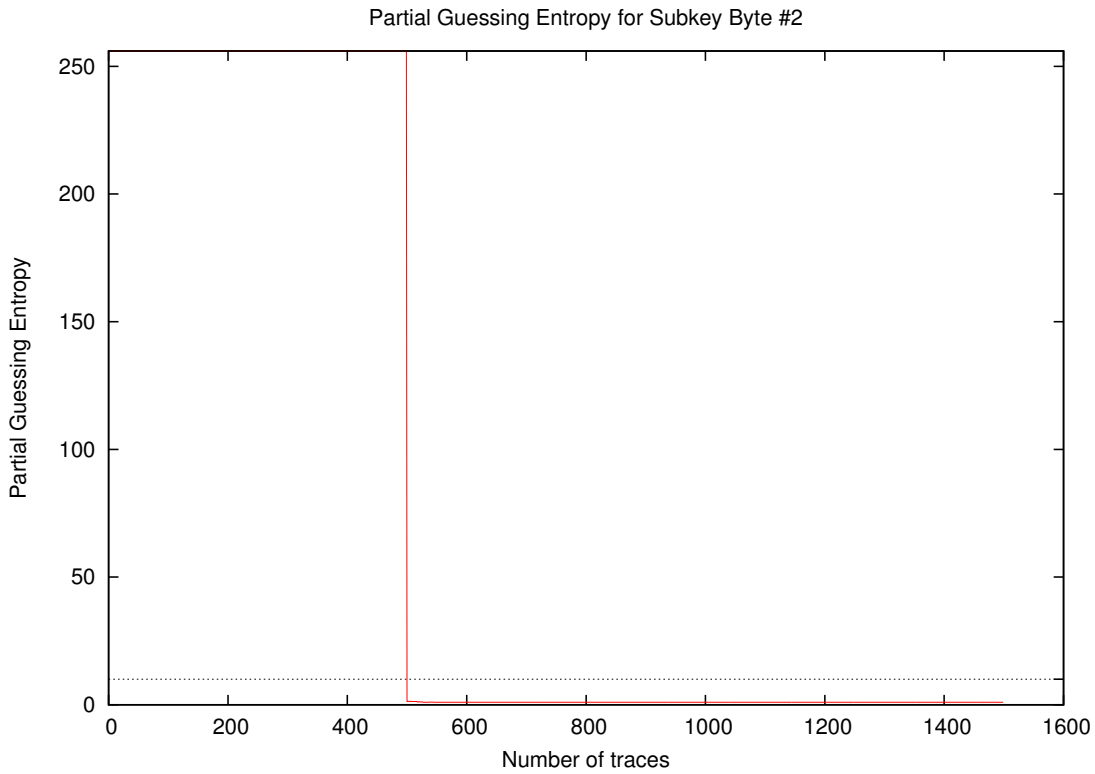

Partial Success Rate for Subkey Bytes #1 to #8
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
200
400
600
800
1000
1200
1400
1600
01
02
03
04
05
06
07
08

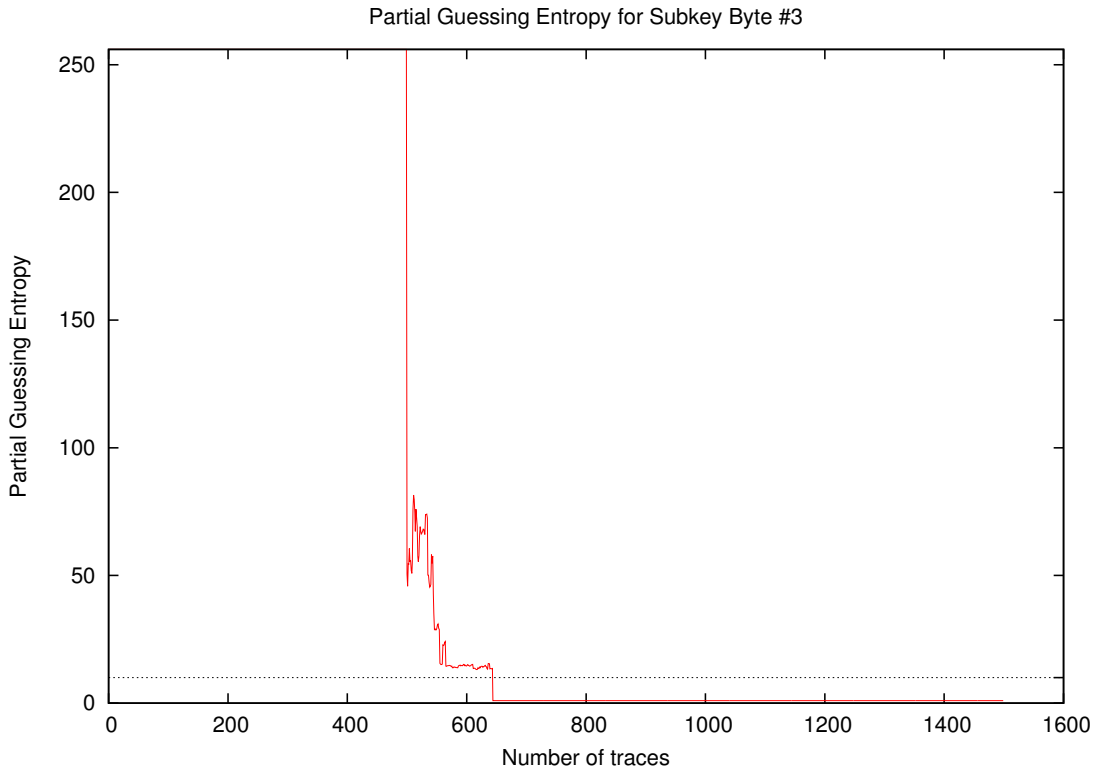

Partial Success Rate for Subkey Bytes #9 to #16
Partial Success Rate
Number of traces
0
0.2
0.4
0.6
0.8
1
0
200
400
600
800
1000
1200
1400
1600
09
10
11
12
13
14
15
16

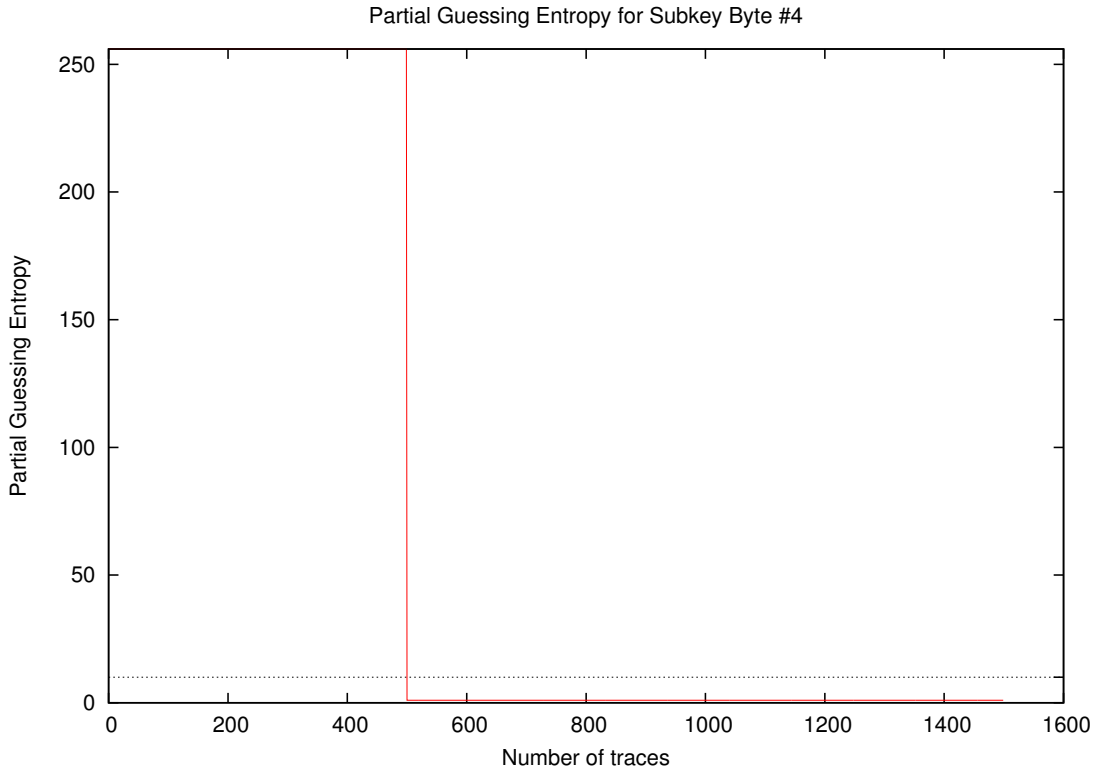
Traces	Partial Success Rate / Byte																Min	Max	Mean
	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16			
10	0.00	0.00	0.00	0.00	0.06	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.06	0.00	0.00	0.06	0.01
20	0.00	0.00	0.00	0.00	0.06	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.06	0.00	0.00	0.06	0.01
30	0.00	0.00	0.00	0.00	0.06	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.06	0.00	0.00	0.06	0.01
40	0.00	0.00	0.00	0.00	0.06	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.06	0.00	0.00	0.06	0.01
50	0.00	0.00	0.00	0.00	0.06	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.06	0.00	0.00	0.06	0.01
100	0.00	0.00	0.00	0.00	0.06	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.06	0.00	0.00	0.06	0.01
200	0.00	0.00	0.00	0.00	0.06	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.06	0.00	0.00	0.06	0.01
300	0.00	0.00	0.00	0.00	0.06	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.06	0.00	0.00	0.06	0.01
400	0.00	0.00	0.00	0.00	0.06	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.06	0.00	0.00	0.06	0.01
500	0.00	0.00	0.00	0.00	0.06	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.06	0.00	0.00	0.06	0.01
600	1.00	1.00	0.94	1.00	1.00	0.88	1.00	1.00	1.00	0.94	0.81	0.94	1.00	0.88	0.88	1.00	0.81	1.00	0.95
700	1.00	1.00	1.00	1.00	1.00	0.94	1.00	1.00	1.00	1.00	0.94	1.00	1.00	1.00	0.94	1.00	0.94	1.00	0.99
800	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
900	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
1000	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

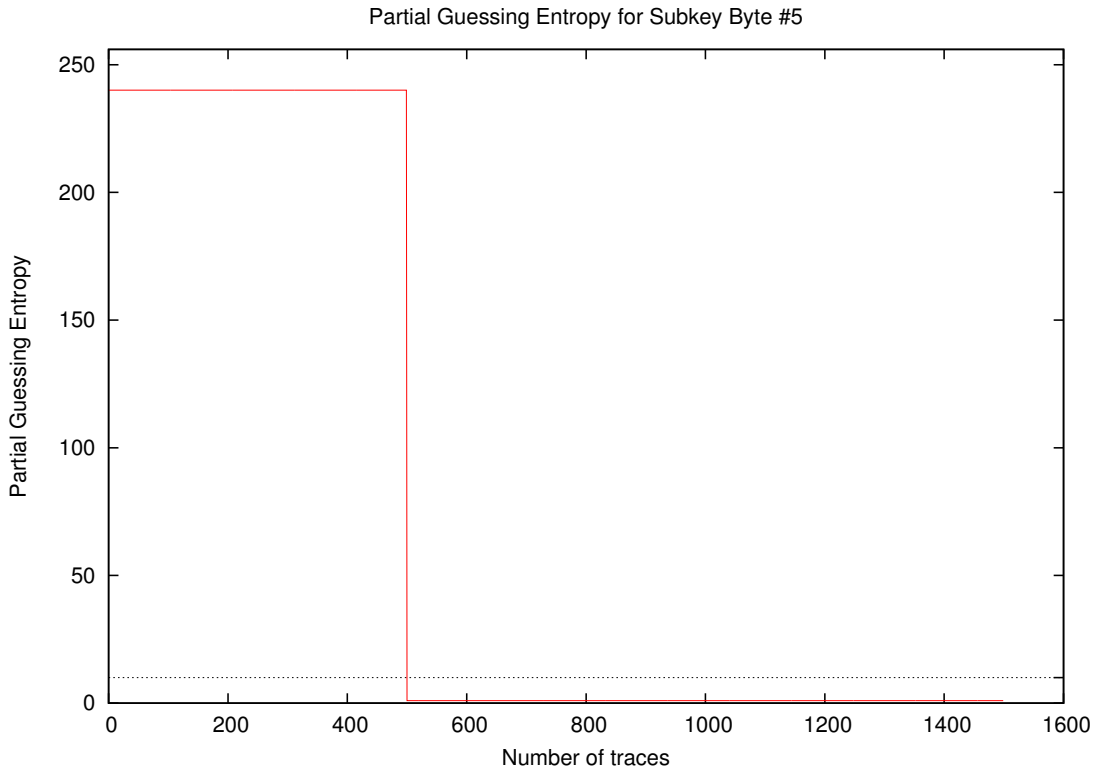
4 Partial Guessing Entropy

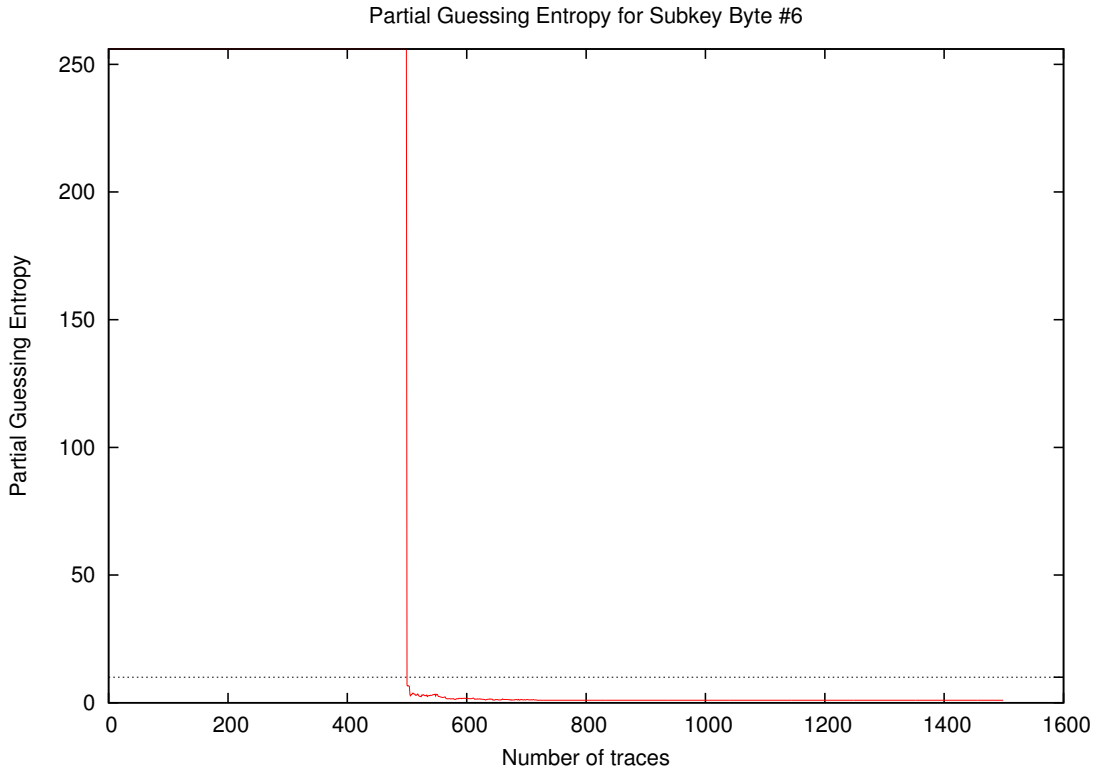


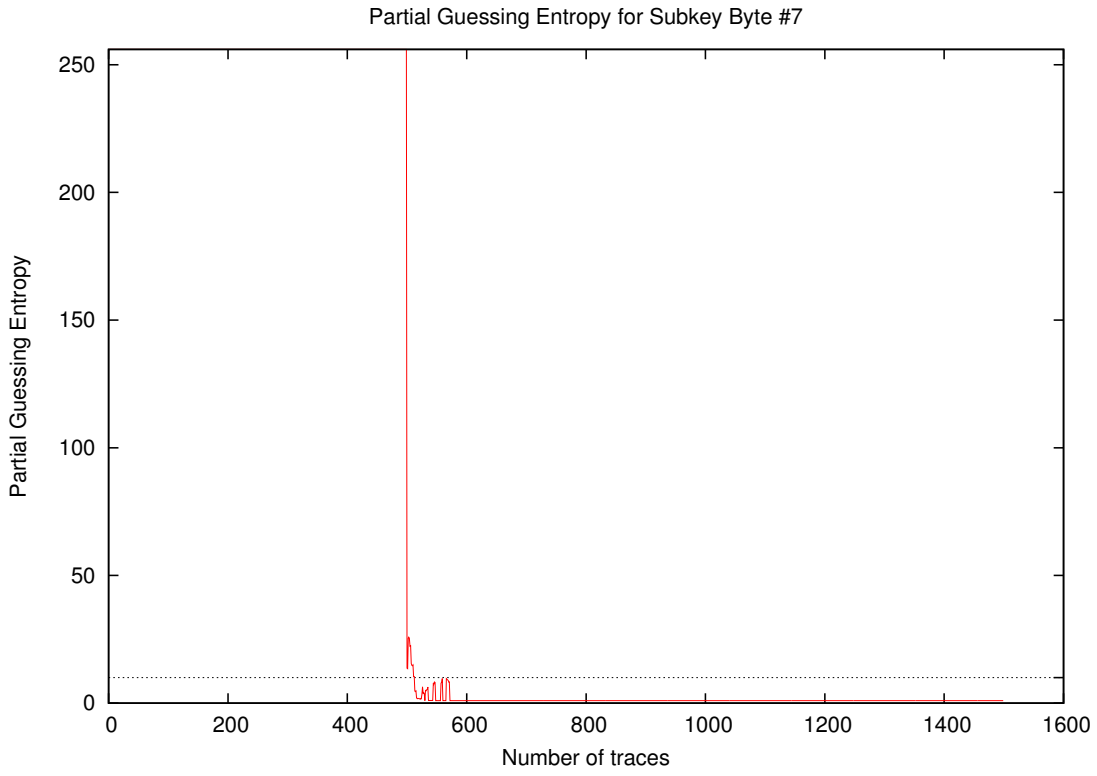


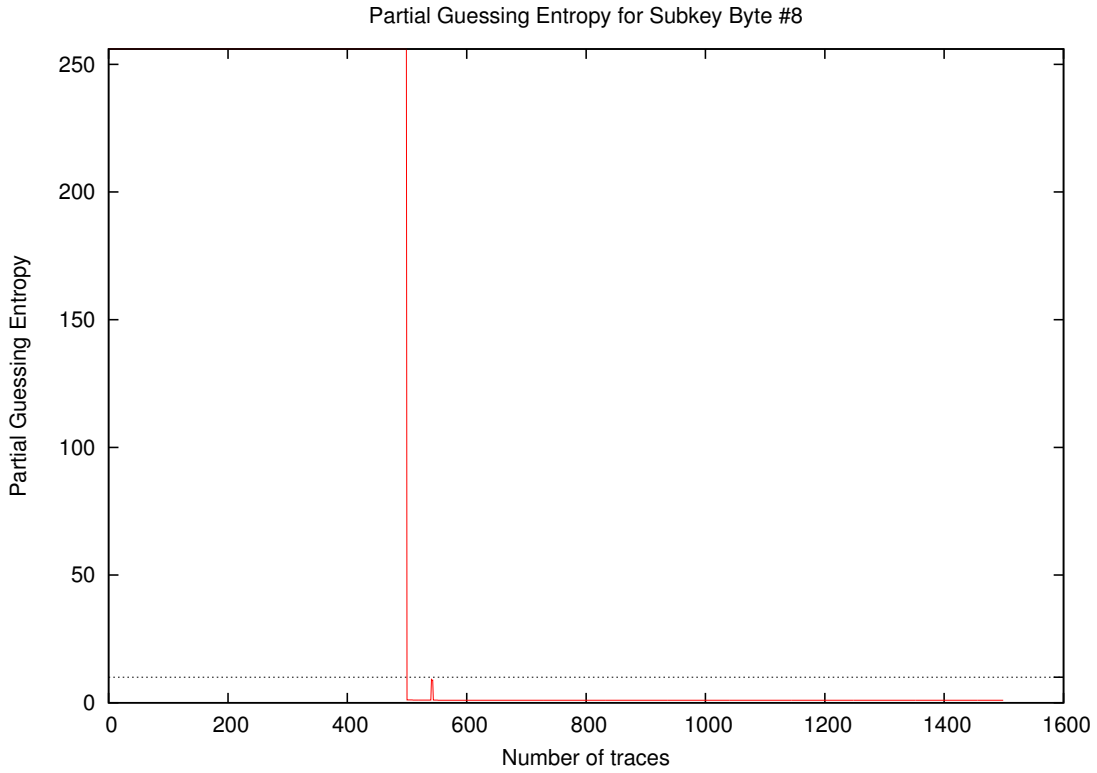

Partial Guessing Entropy for Subkey Byte #3
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
0
200
400
600
800
1000
1200
1400
1600

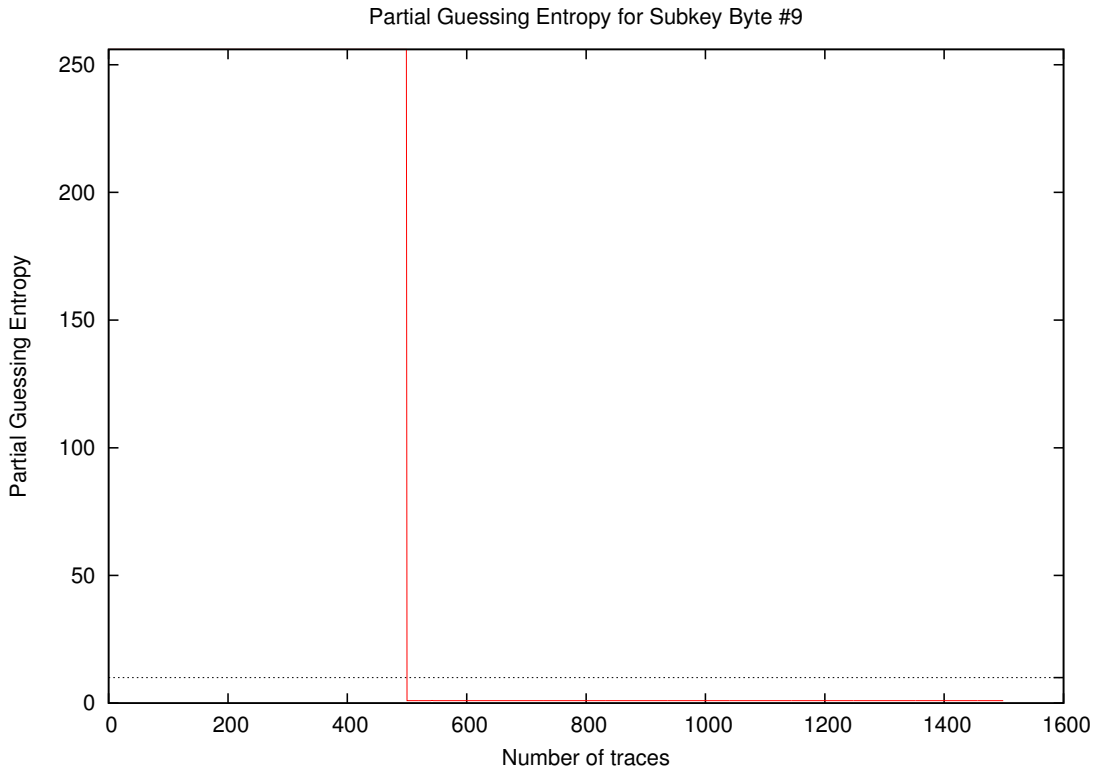

Partial Guessing Entropy for Subkey Byte #4
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
0
200
400
600
800
1000
1200
1400
1600

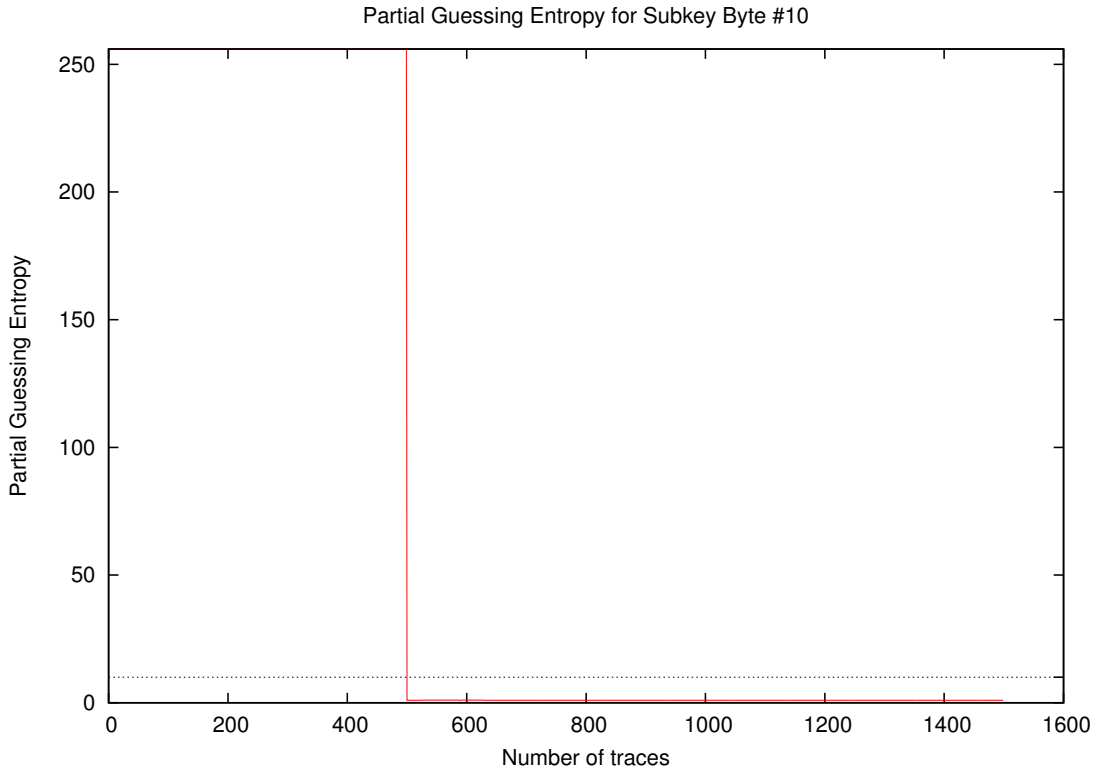

Partial Guessing Entropy for Subkey Byte #5
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
0
200
400
600
800
1000
1200
1400
1600

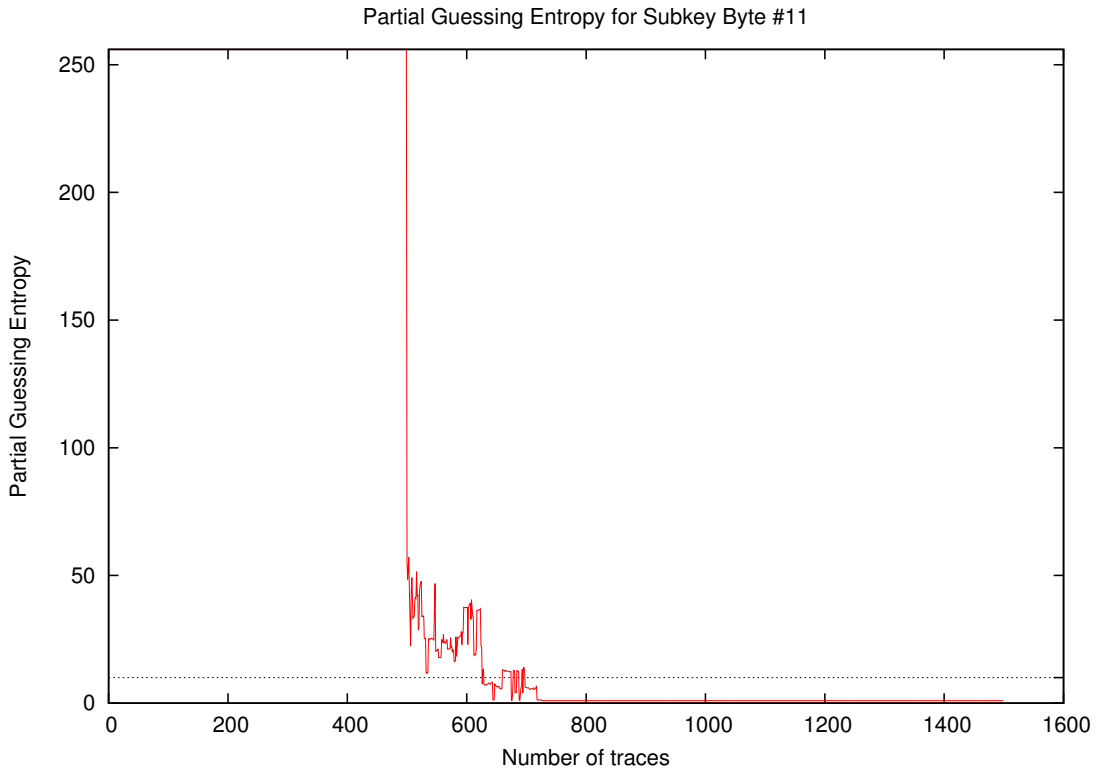

Partial Guessing Entropy for Subkey Byte #6
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
0
200
400
600
800
1000
1200
1400
1600

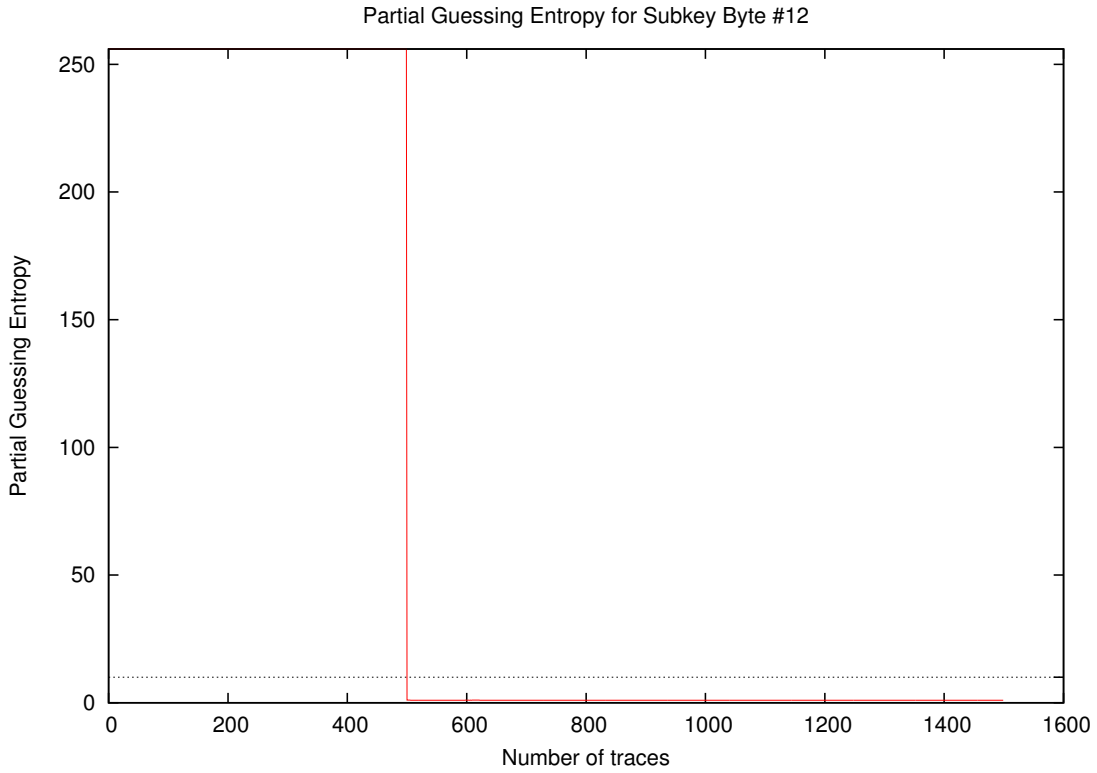

Partial Guessing Entropy for Subkey Byte #7
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
0
200
400
600
800
1000
1200
1400
1600

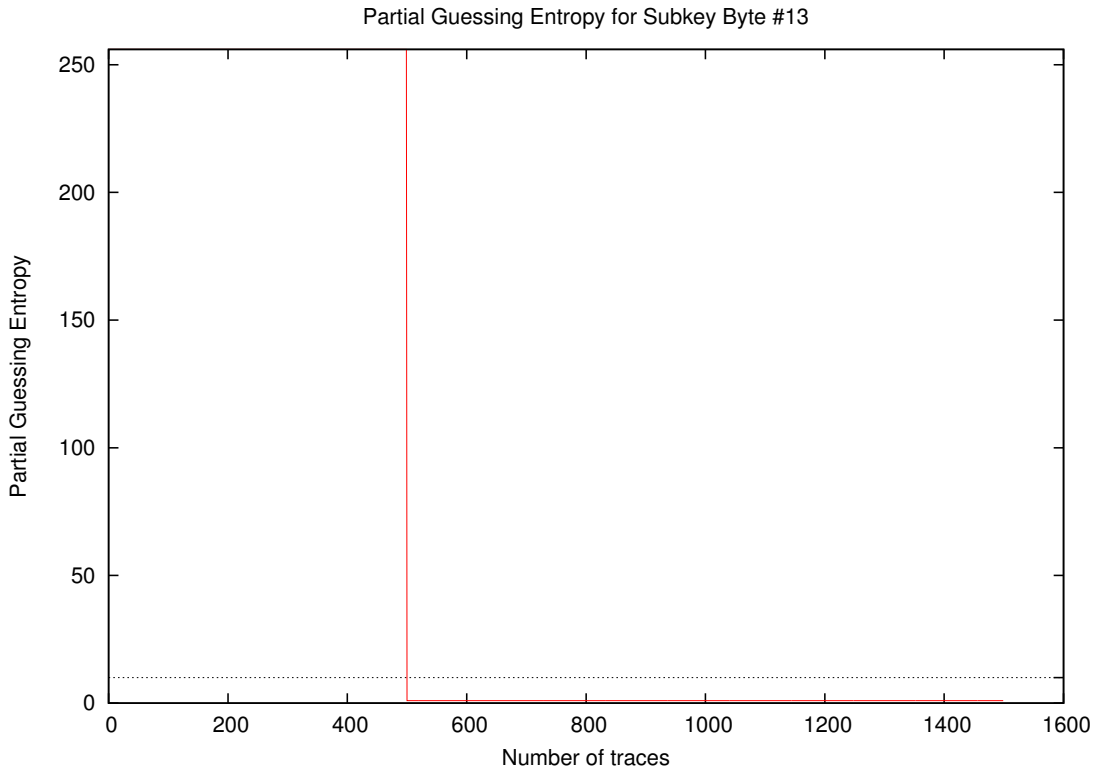

Partial Guessing Entropy for Subkey Byte #8
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
0
200
400
600
800
1000
1200
1400
1600

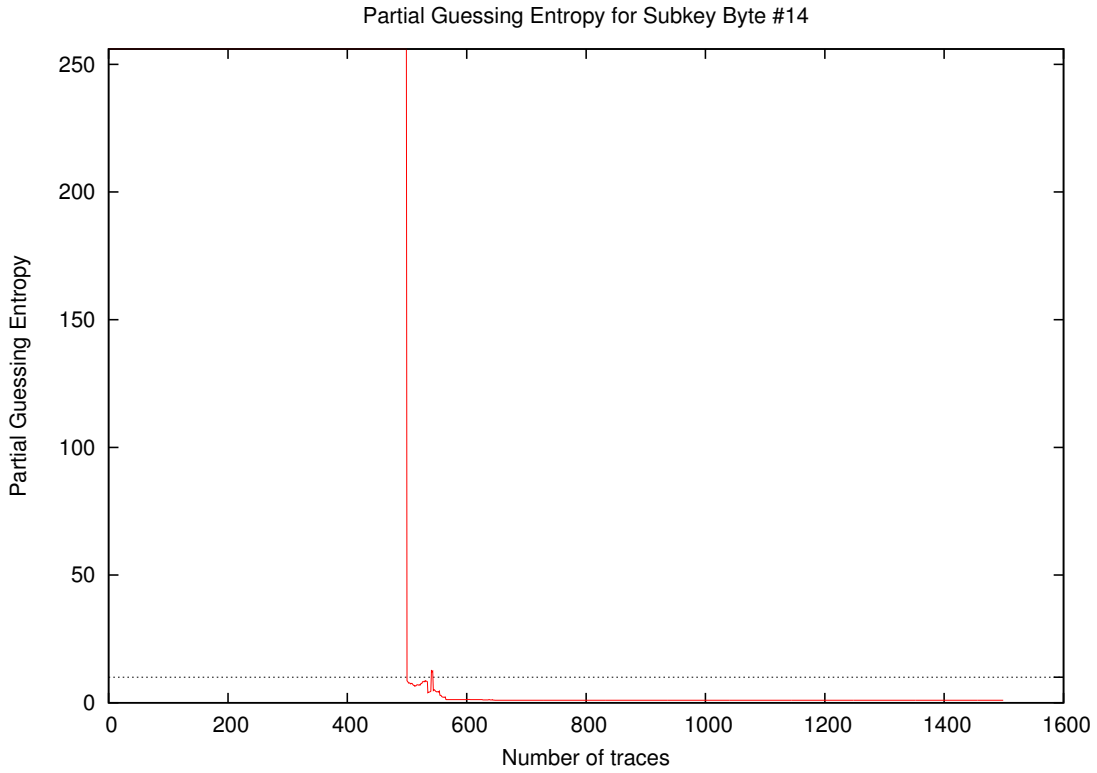

Partial Guessing Entropy for Subkey Byte #9
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
0
200
400
600
800
1000
1200
1400
1600

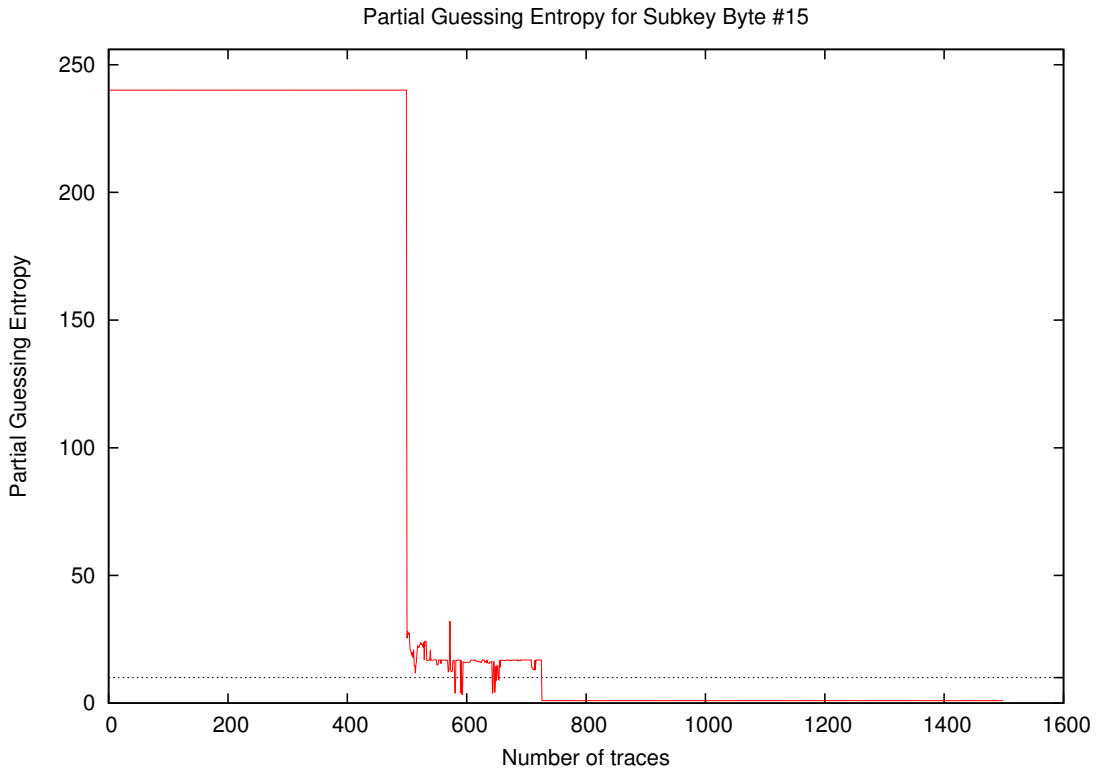

Partial Guessing Entropy for Subkey Byte #10
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
0
200
400
600
800
1000
1200
1400
1600

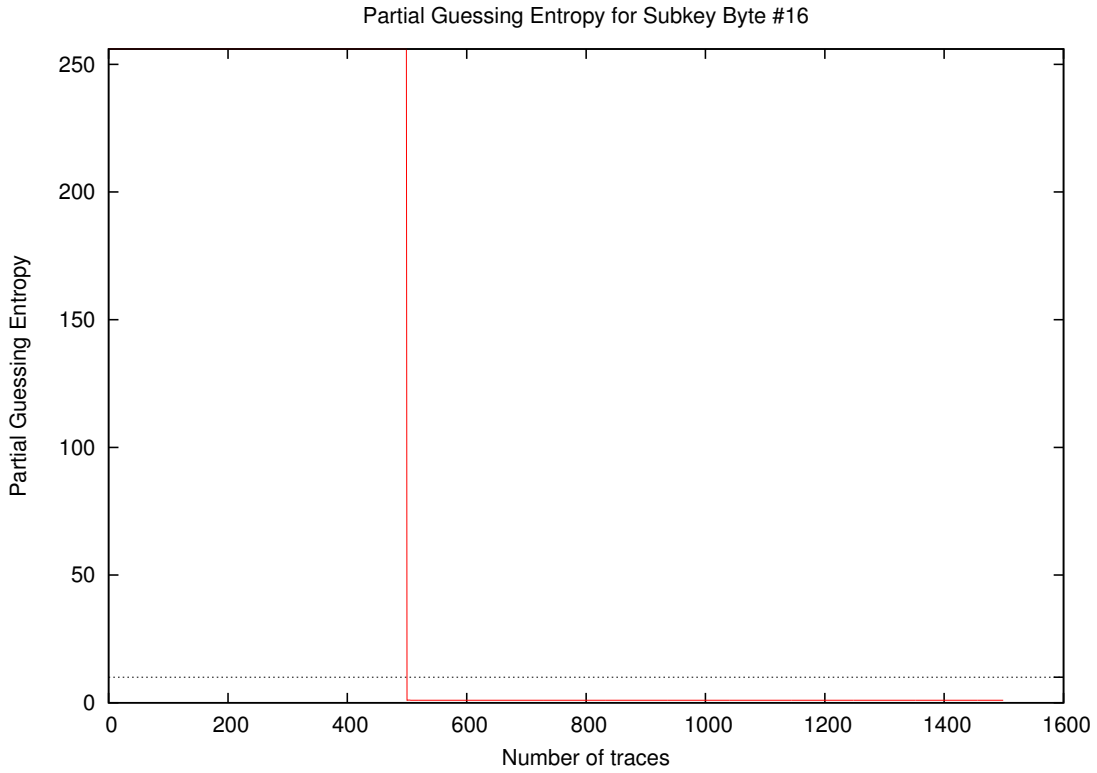

Partial Guessing Entropy for Subkey Byte #11
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
0
200
400
600
800
1000
1200
1400
1600

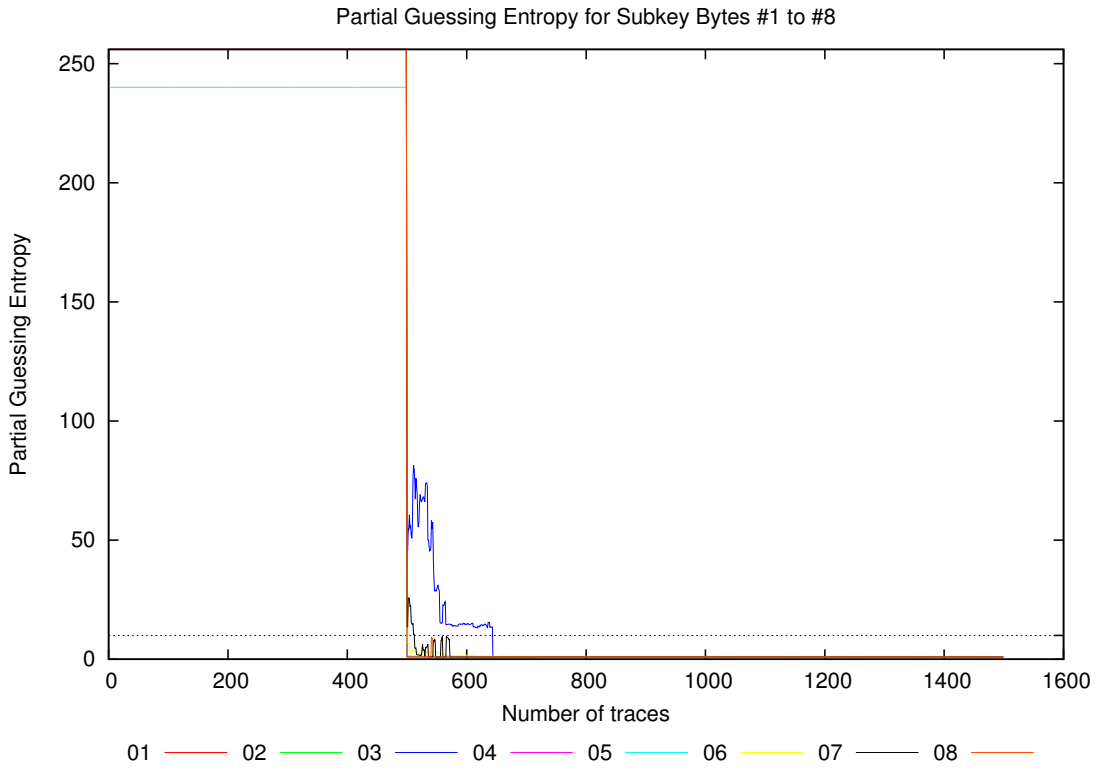

Partial Guessing Entropy for Subkey Byte #12
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
0
200
400
600
800
1000
1200
1400
1600

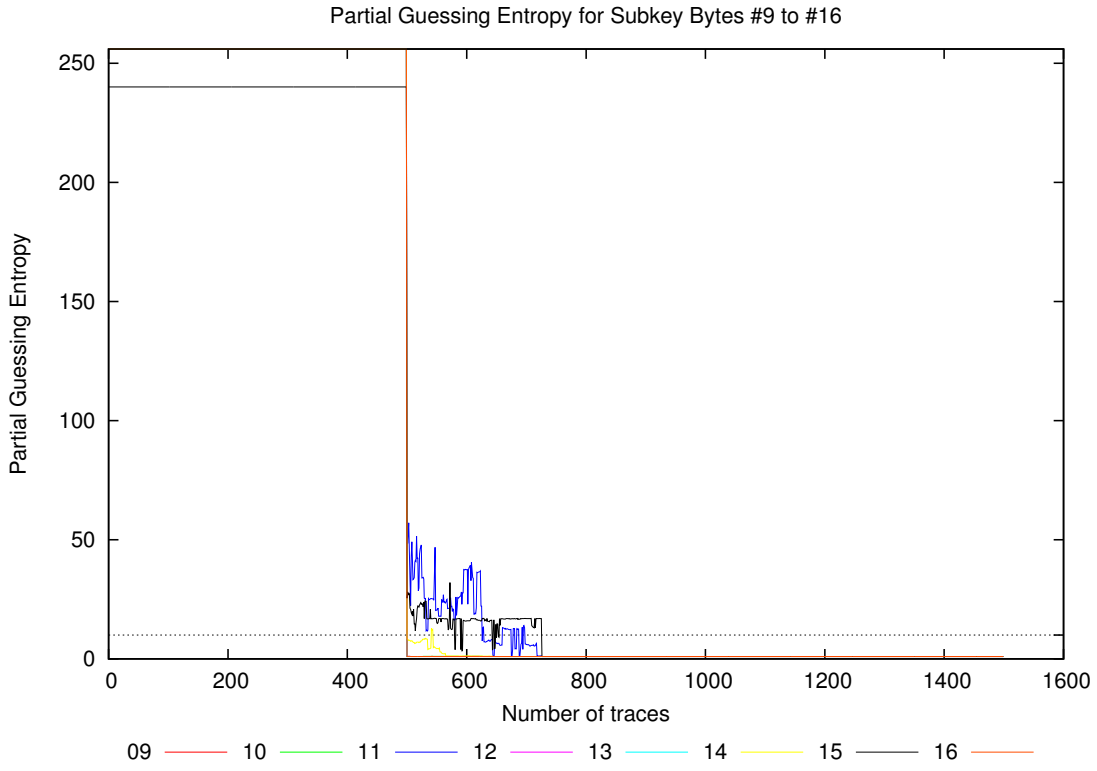

Partial Guessing Entropy for Subkey Byte #13
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
0
200
400
600
800
1000
1200
1400
1600


Partial Guessing Entropy for Subkey Byte #14
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
0
200
400
600
800
1000
1200
1400
1600


Partial Guessing Entropy for Subkey Byte #15
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
0
200
400
600
800
1000
1200
1400
1600


Partial Guessing Entropy for Subkey Byte #16
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
0
200
400
600
800
1000
1200
1400
1600


Partial Guessing Entropy for Subkey Bytes #1 to #8
Partial Guessing Entropy
Number of traces
0
50
100
150
200
250
0
200
400
600
800
1000
1200
1400
1600
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
200
400
600
800
1000
1200
1400
1600
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	256.0	256.0	256.0	256.0	240.1	256.0	256.0	256.0	256.0	256.0	256.0	256.0	256.0	256.0	240.1	256.0	240.1	256.0	254.0
20	256.0	256.0	256.0	256.0	240.1	256.0	256.0	256.0	256.0	256.0	256.0	256.0	256.0	256.0	240.1	256.0	240.1	256.0	254.0
30	256.0	256.0	256.0	256.0	240.1	256.0	256.0	256.0	256.0	256.0	256.0	256.0	256.0	256.0	240.1	256.0	240.1	256.0	254.0
40	256.0	256.0	256.0	256.0	240.1	256.0	256.0	256.0	256.0	256.0	256.0	256.0	256.0	256.0	240.1	256.0	240.1	256.0	254.0
50	256.0	256.0	256.0	256.0	240.1	256.0	256.0	256.0	256.0	256.0	256.0	256.0	256.0	256.0	240.1	256.0	240.1	256.0	254.0
100	256.0	256.0	256.0	256.0	240.1	256.0	256.0	256.0	256.0	256.0	256.0	256.0	256.0	256.0	240.1	256.0	240.1	256.0	254.0
200	256.0	256.0	256.0	256.0	240.1	256.0	256.0	256.0	256.0	256.0	256.0	256.0	256.0	256.0	240.1	256.0	240.1	256.0	254.0
300	256.0	256.0	256.0	256.0	240.1	256.0	256.0	256.0	256.0	256.0	256.0	256.0	256.0	256.0	240.1	256.0	240.1	256.0	254.0
400	256.0	256.0	256.0	256.0	240.1	256.0	256.0	256.0	256.0	256.0	256.0	256.0	256.0	256.0	240.1	256.0	240.1	256.0	254.0
500	256.0	256.0	256.0	256.0	240.1	256.0	256.0	256.0	256.0	256.0	256.0	256.0	256.0	256.0	240.1	256.0	240.1	256.0	254.0
600	1.0	1.0	14.6	1.0	1.0	1.7	1.0	1.0	1.0	1.1	37.4	1.1	1.0	1.2	15.9	1.0	1.0	37.4	5.1
700	1.0	1.0	1.0	1.0	1.0	1.1	1.0	1.0	1.0	1.0	6.2	1.0	1.0	1.0	16.9	1.0	1.0	16.9	2.3
800	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
900	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
1000	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