

# Evaluation results

DPA contest v2

September 2010

## 1 Introduction

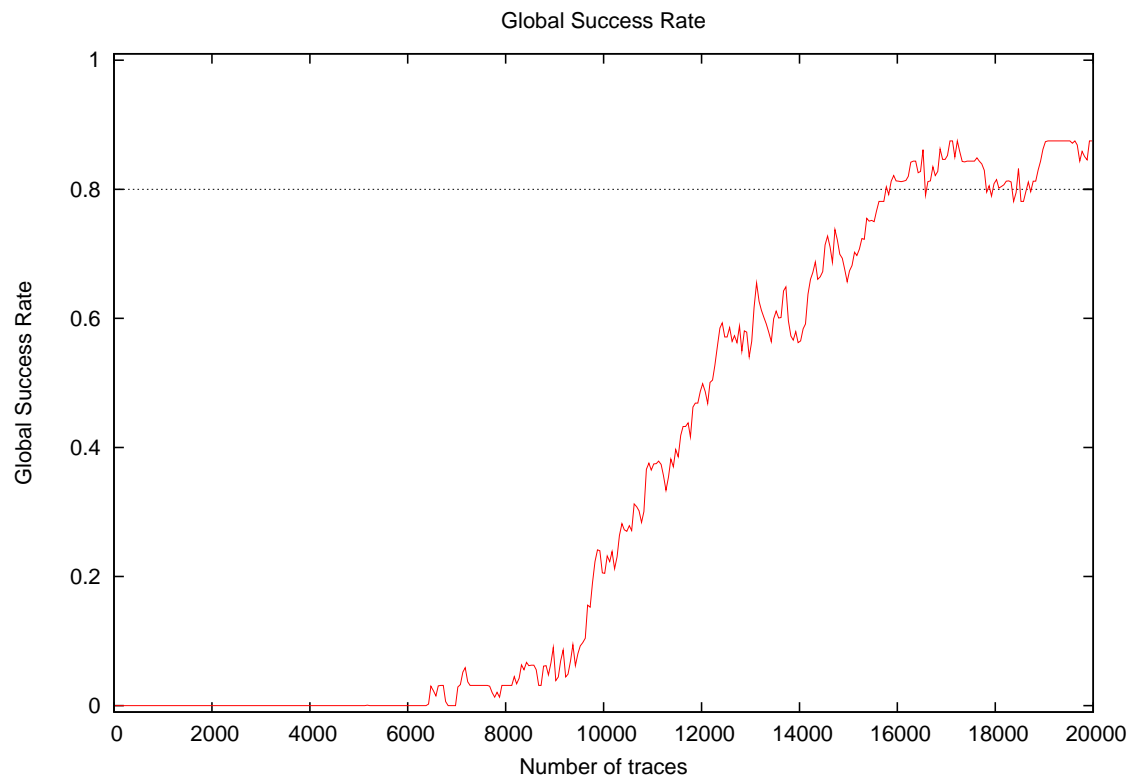
### 1.1 About the attack

- **Attack Name:** MI cumulant
- **Sender/Team:** Thanh-Ha Le
- **Institution:** Morpho, France
- **Language:** Matlab
- **Attacked subkey:** 10

### 1.2 About the evaluation

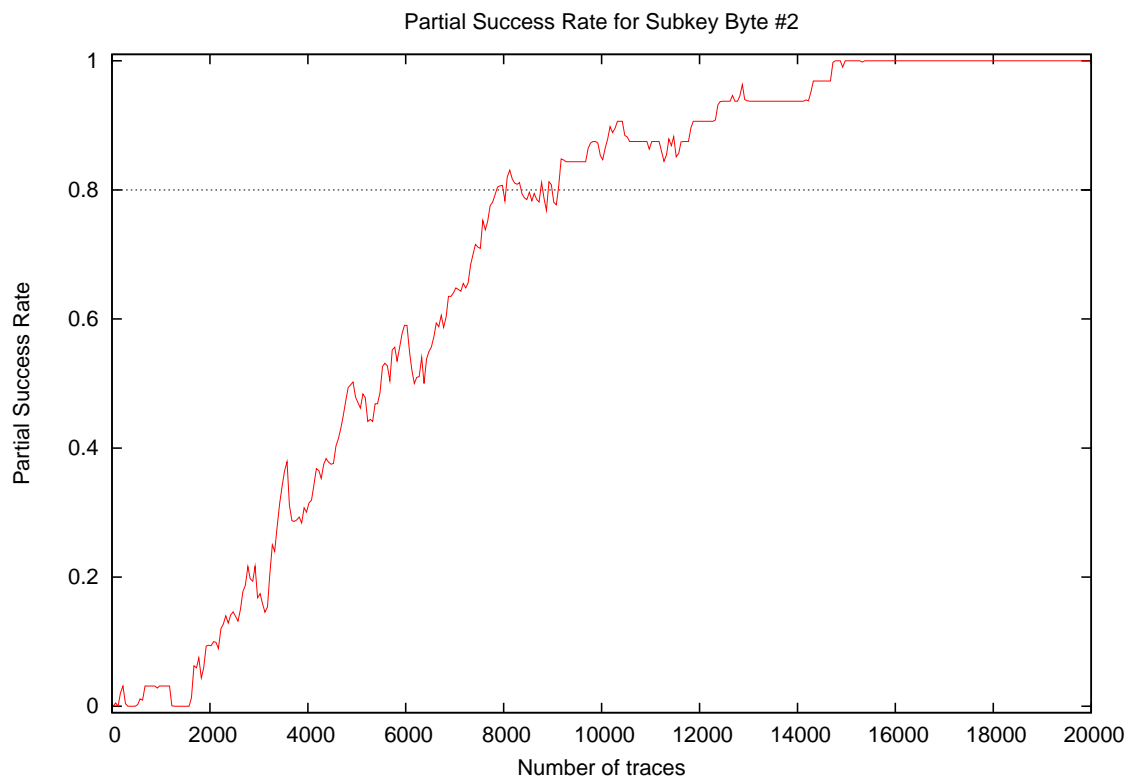
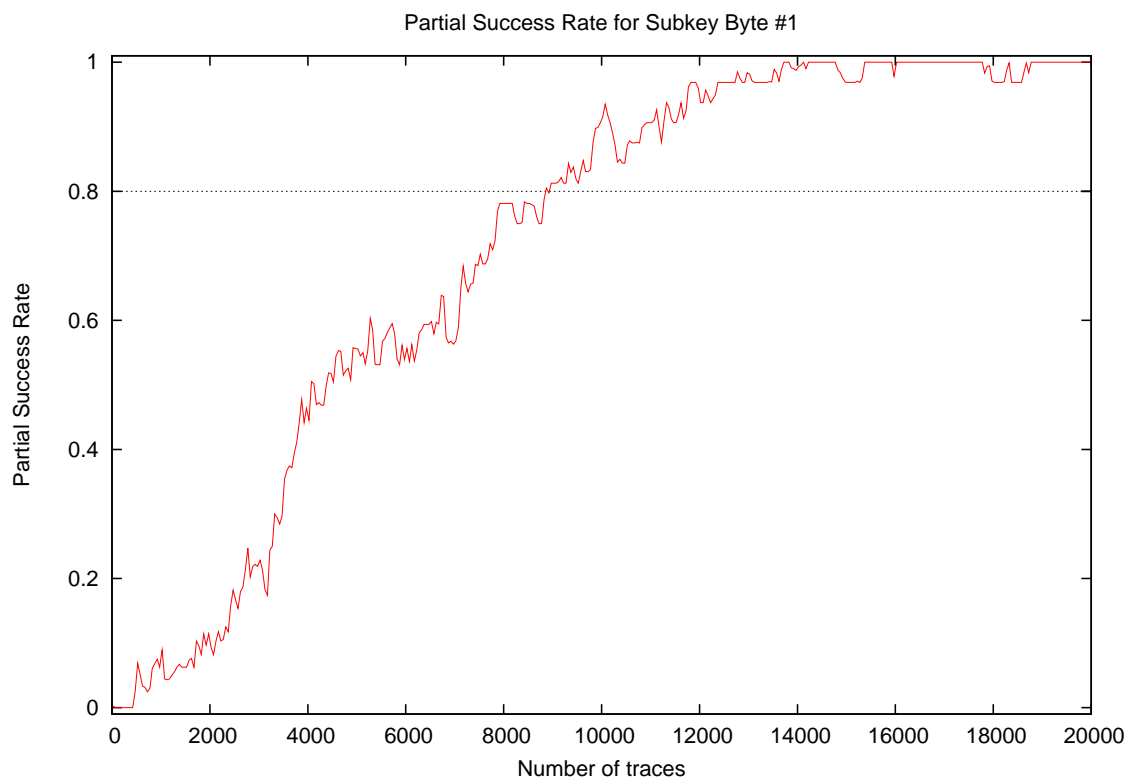
- **Date of evaluation:** August 2010

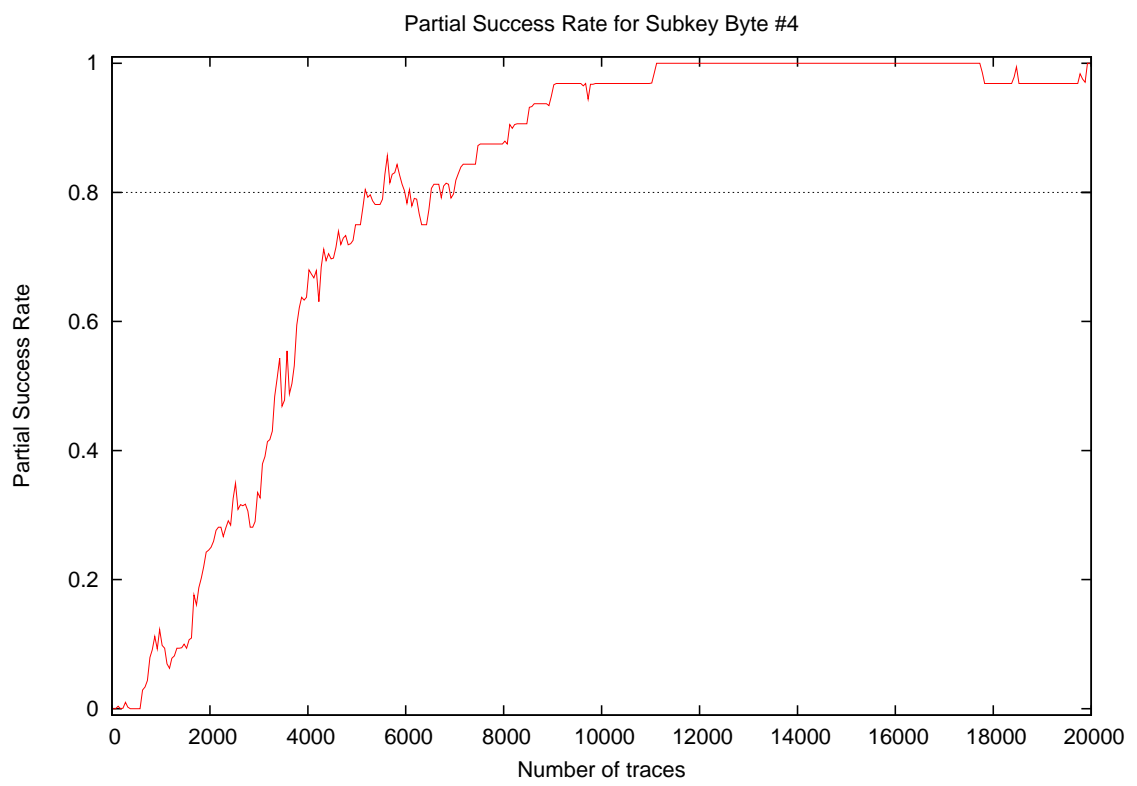
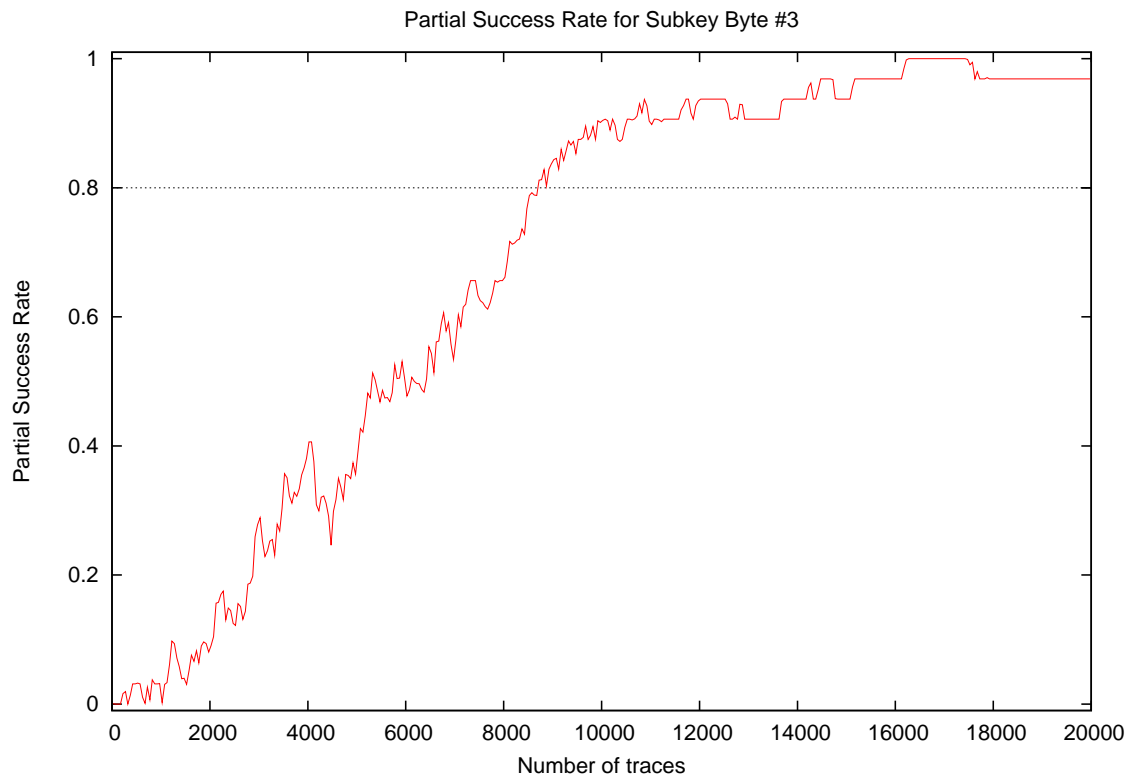
## 2 Global Success Rate

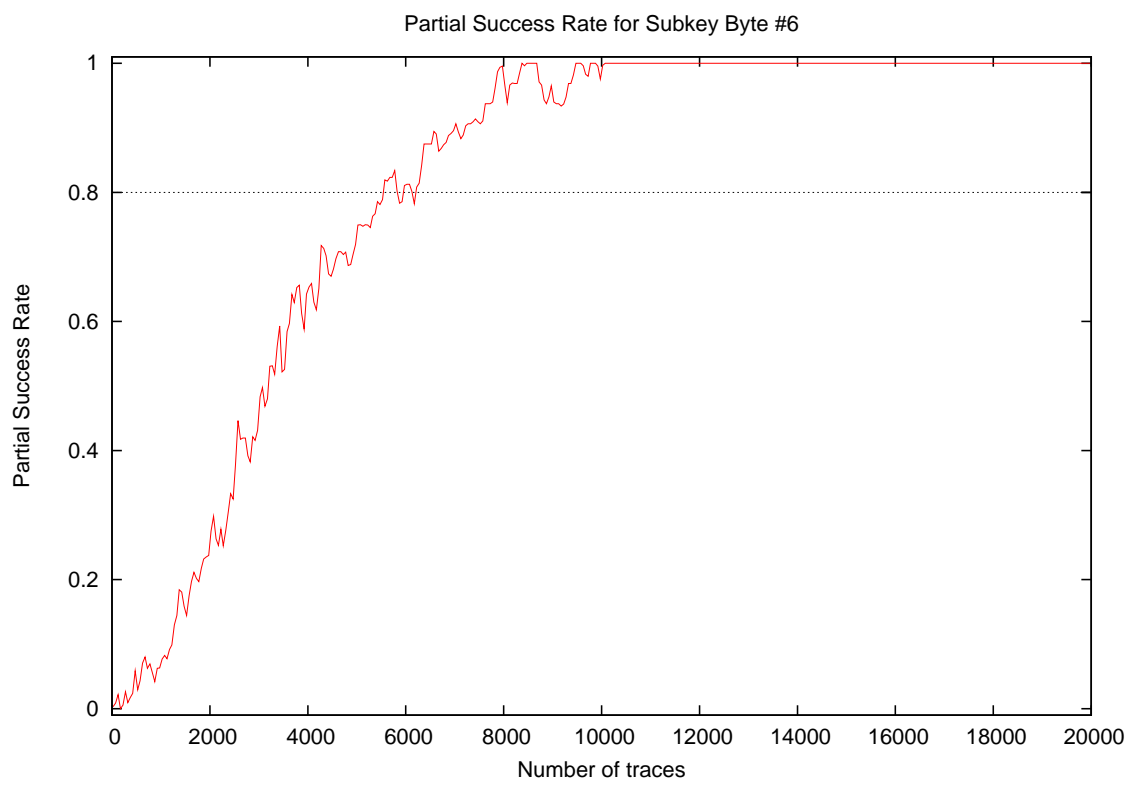
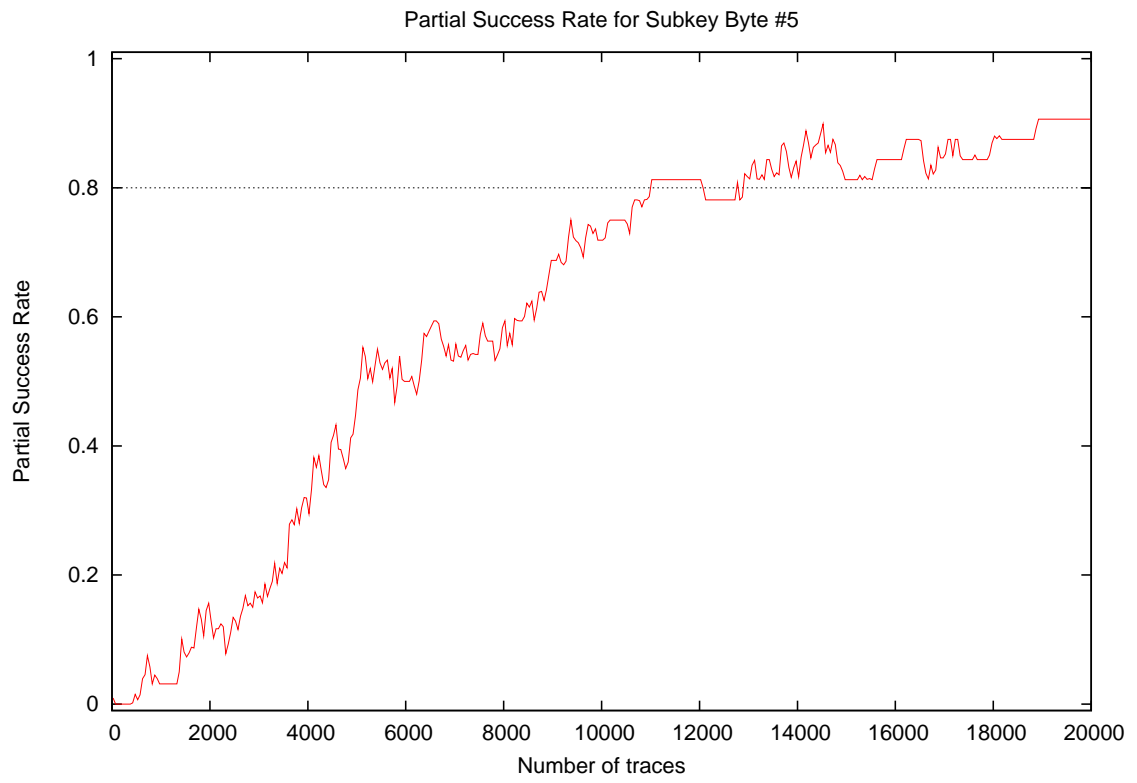


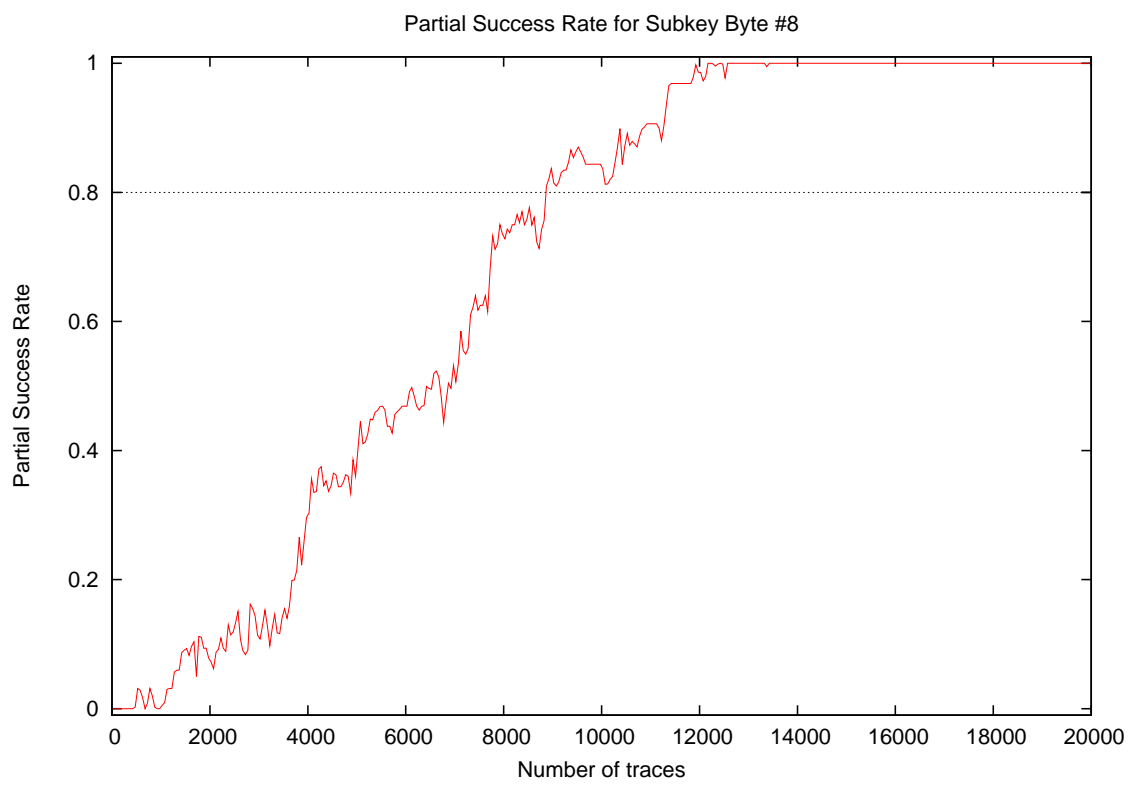
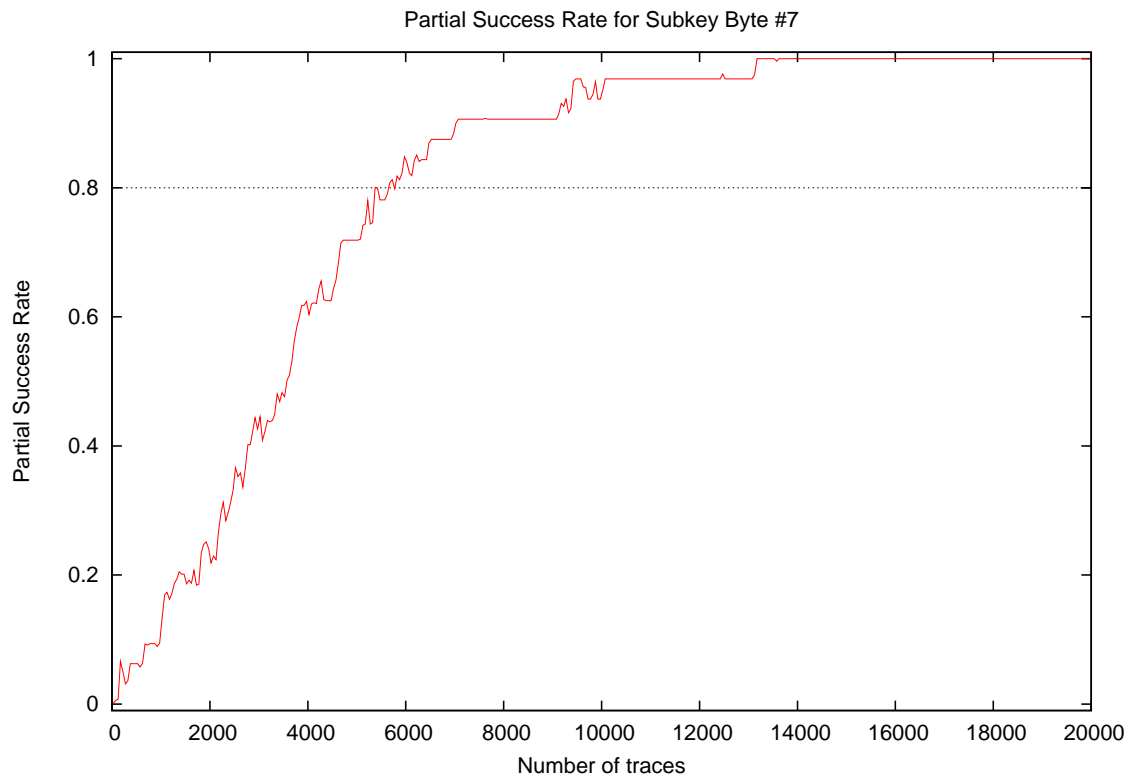
Number of traces	Global Success Rate
10	0.00
20	0.00
30	0.00
40	0.00
50	0.00
100	0.00
200	0.00
300	0.00
400	0.00
500	0.00
1000	0.00
2000	0.00
3000	0.00
4000	0.00
5000	0.00
10000	0.19
15000	0.66
20000	0.88

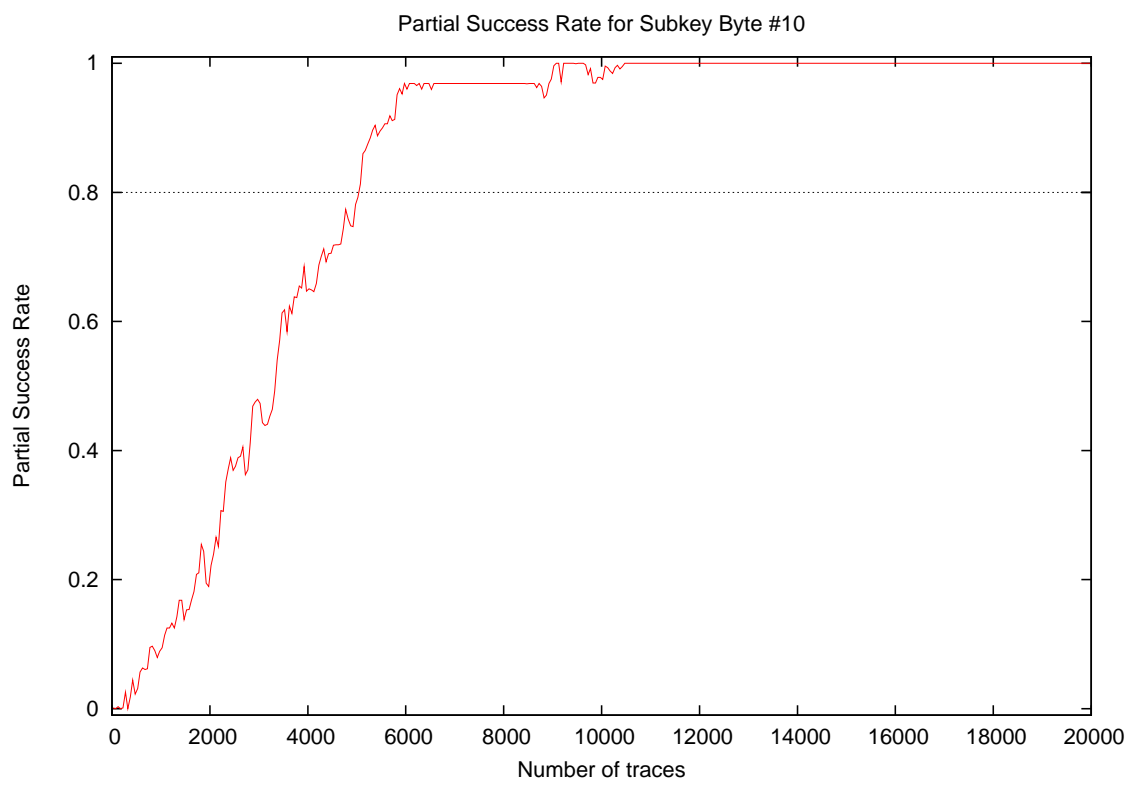
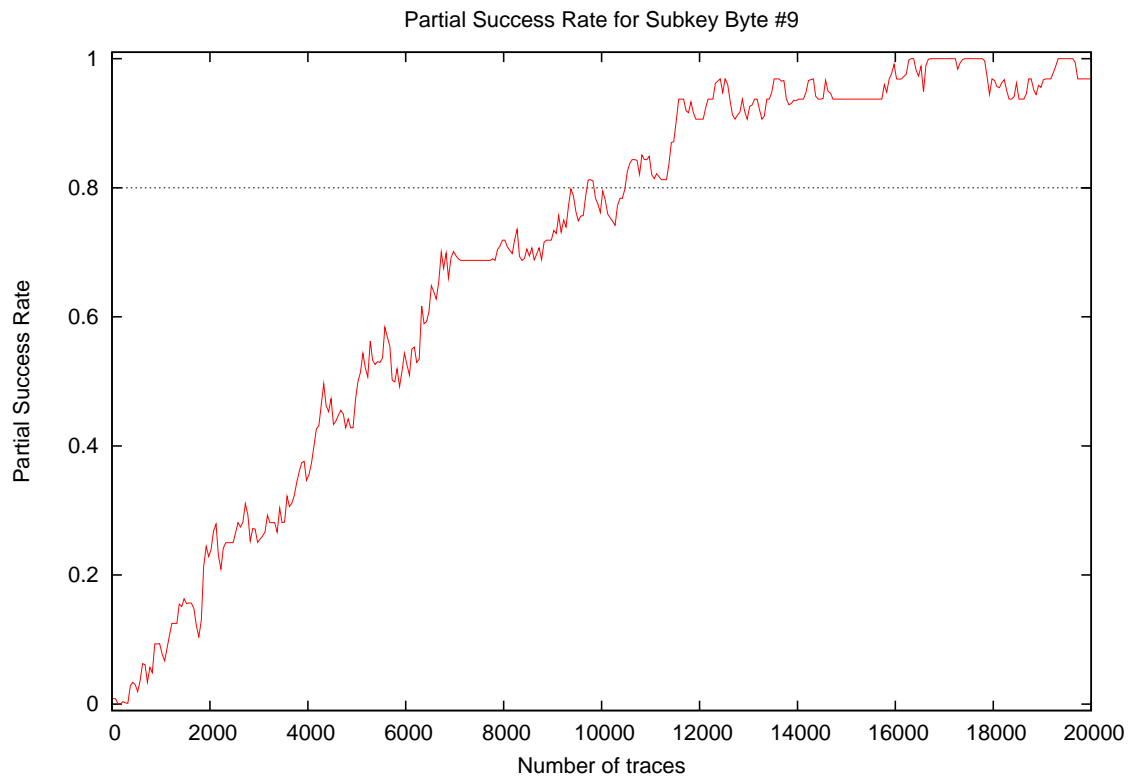
### 3 Partial Success Rate



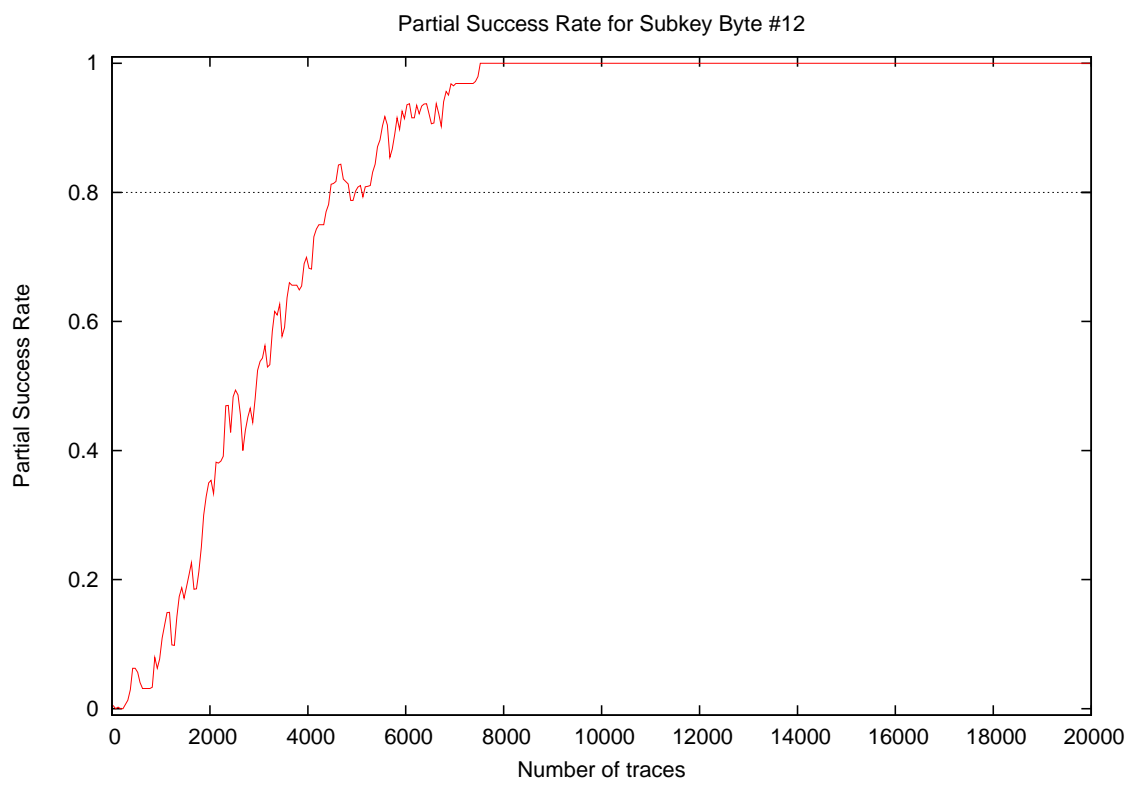
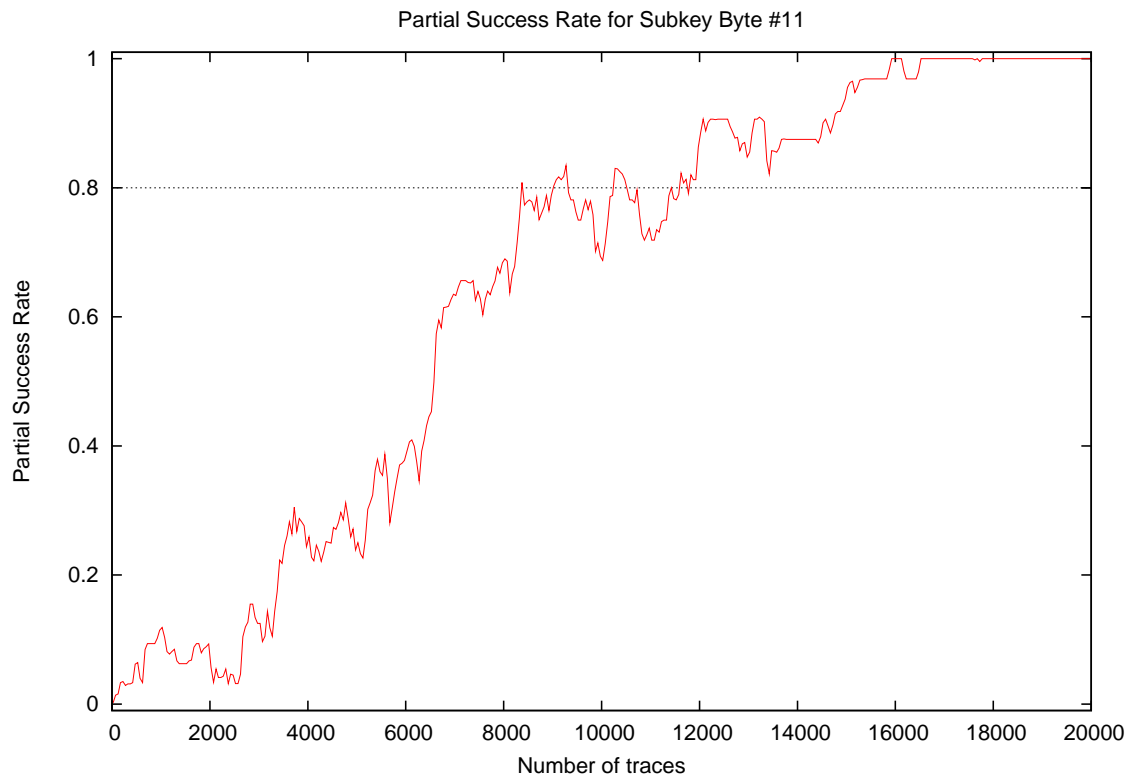


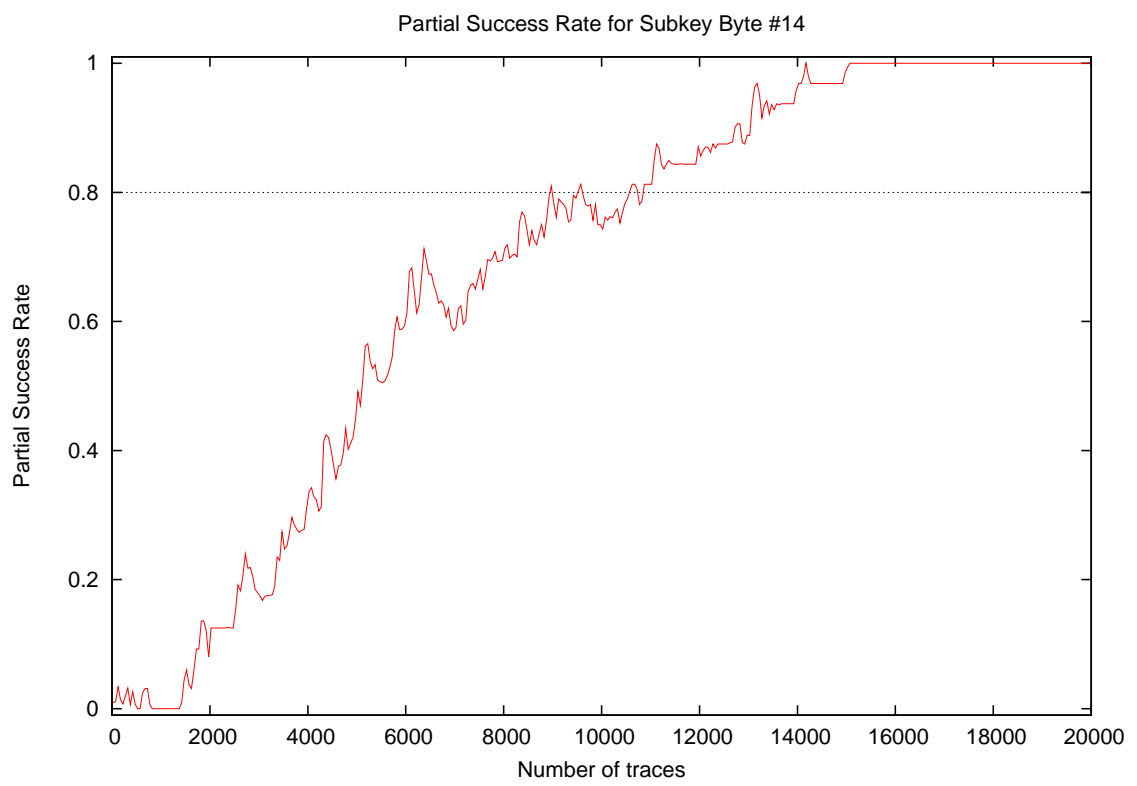
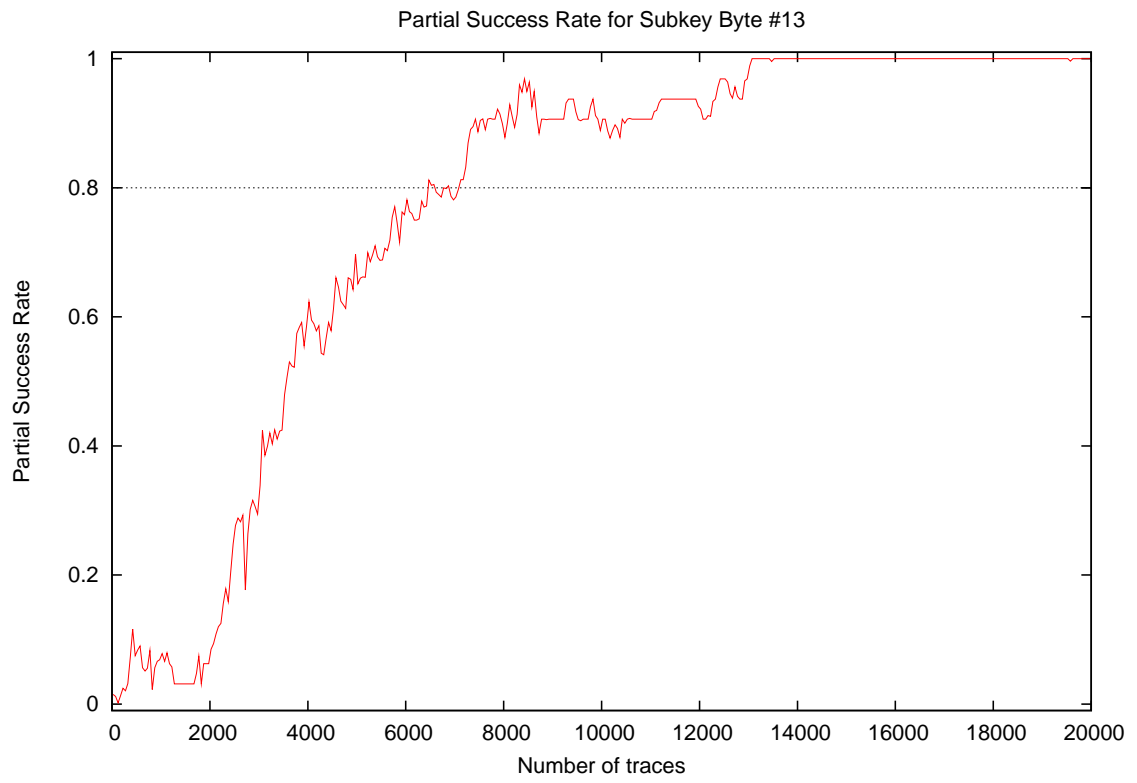


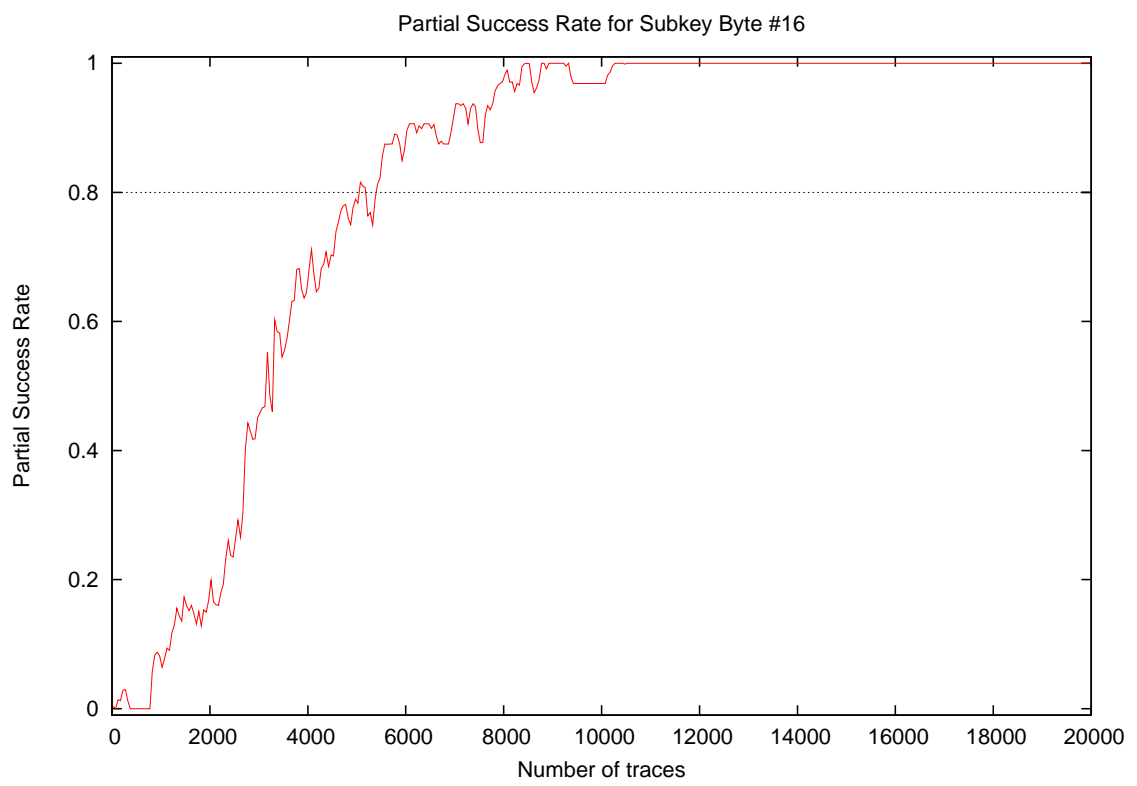
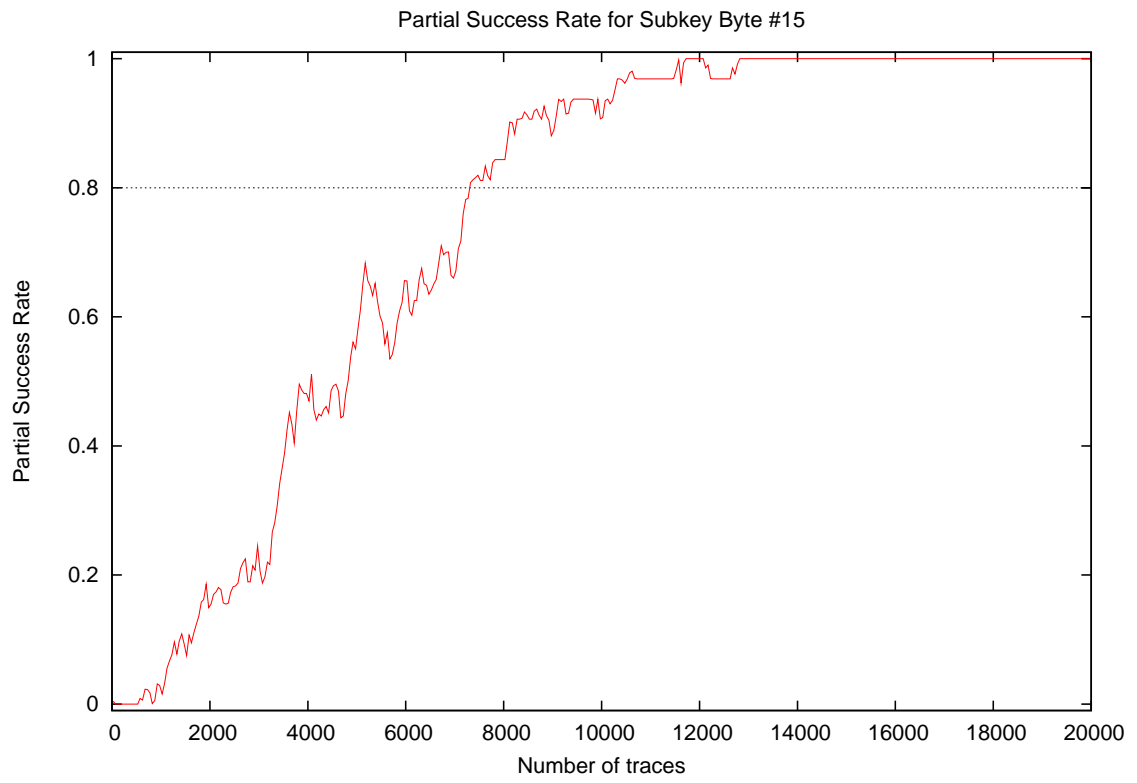


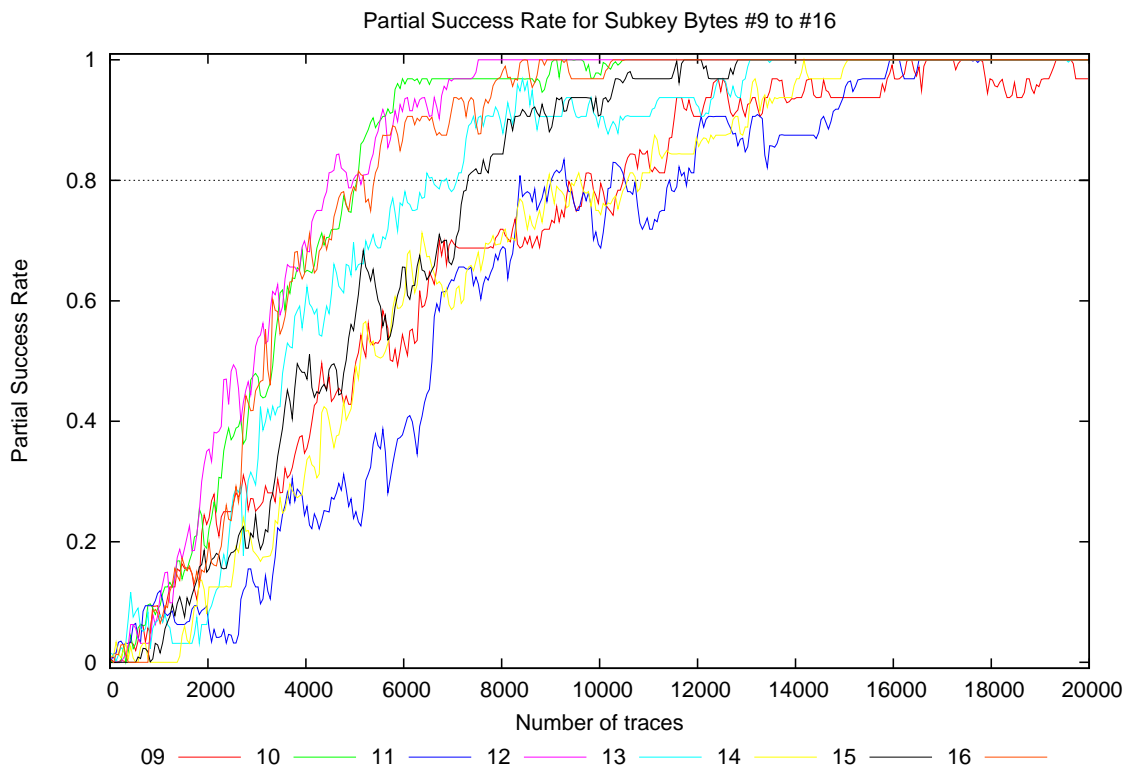
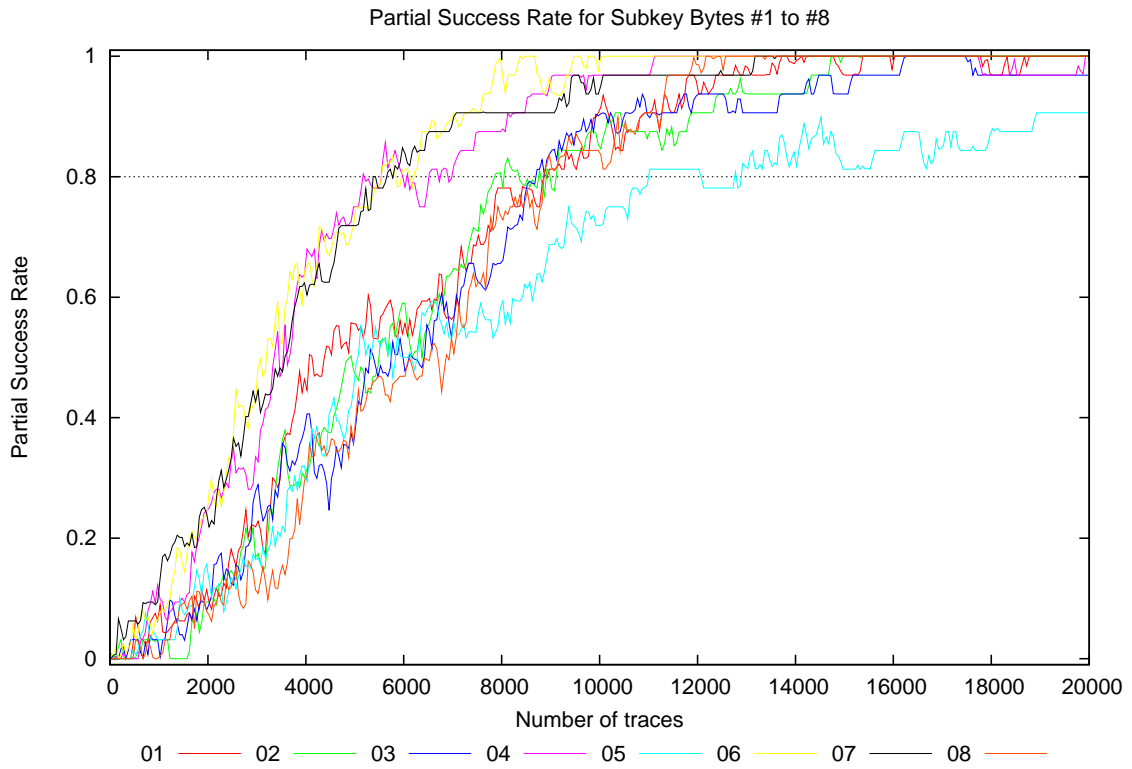




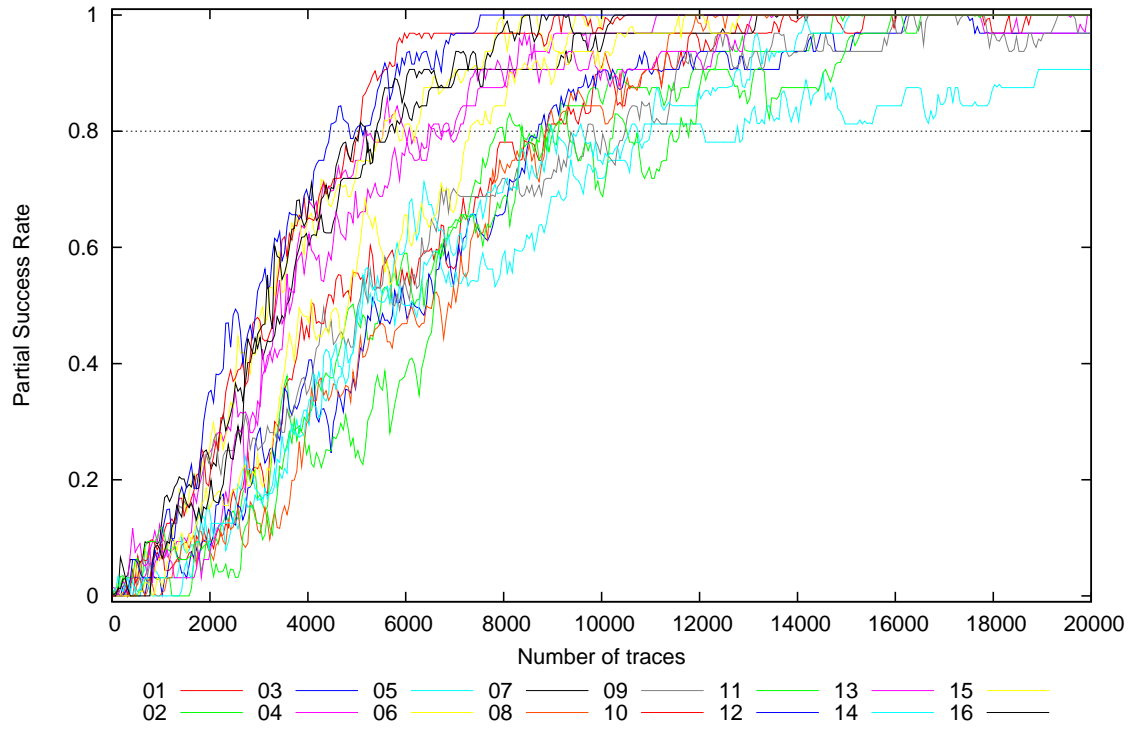






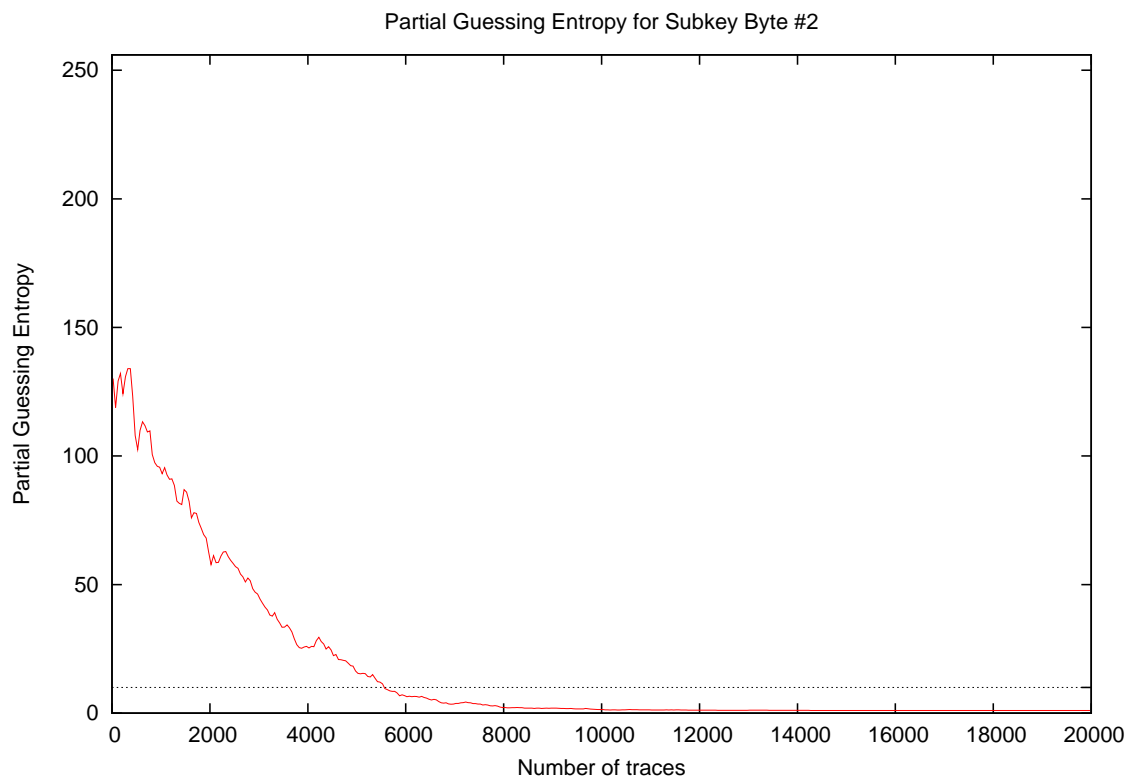
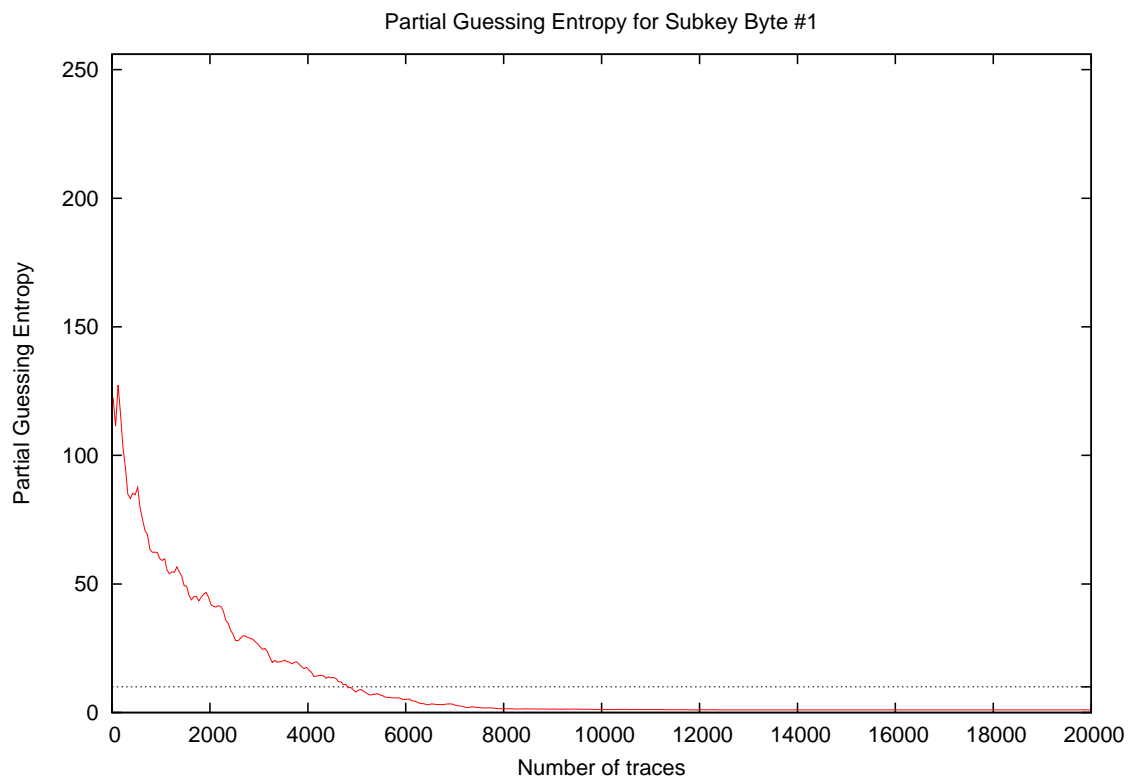


Partial Success Rate for Subkey Bytes #1 to #16

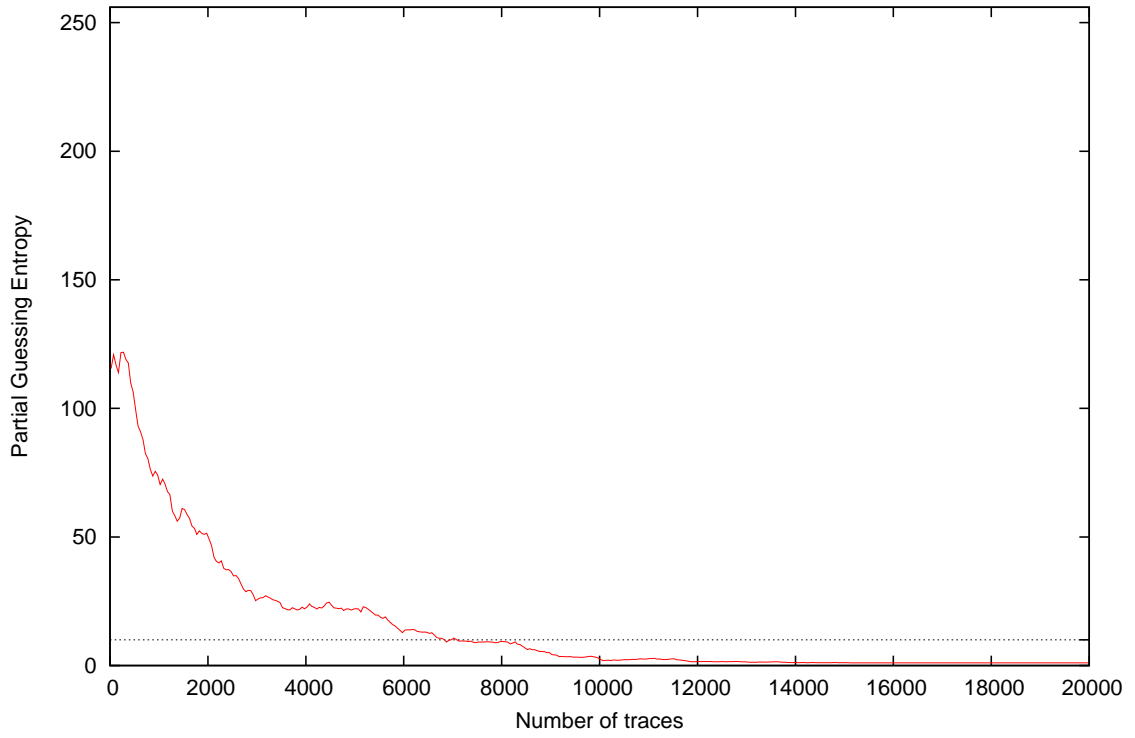


Traces	Partial Success Rate / Byte																Min	Max	Mean
	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16			
10	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.03	0.00	0.03	0.00	0.03	0.00
20	0.00	0.00	0.00	0.00	0.03	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.03	0.00	0.03	0.00	0.03	0.00
30	0.00	0.00	0.00	0.00	0.03	0.00	0.00	0.00	0.00	0.00	0.00	0.03	0.00	0.03	0.00	0.03	0.00	0.03	0.01
40	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.03	0.00	0.00	0.00	0.03	0.00	0.03	0.00	0.03	0.00	0.03	0.00
50	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.06	0.00	0.06	0.00	0.06	0.00	0.06	0.00
100	0.00	0.00	0.00	0.00	0.00	0.03	0.00	0.00	0.00	0.00	0.03	0.00	0.00	0.03	0.00	0.03	0.00	0.03	0.01
200	0.00	0.03	0.00	0.00	0.00	0.00	0.06	0.00	0.00	0.00	0.00	0.00	0.03	0.00	0.00	0.03	0.00	0.06	0.01
300	0.00	0.00	0.00	0.00	0.00	0.03	0.03	0.00	0.00	0.00	0.03	0.03	0.03	0.03	0.00	0.03	0.00	0.03	0.01
400	0.00	0.00	0.03	0.00	0.00	0.00	0.06	0.00	0.03	0.09	0.03	0.06	0.06	0.00	0.00	0.06	0.00	0.09	0.02
500	0.06	0.00	0.03	0.00	0.03	0.03	0.06	0.00	0.03	0.06	0.09	0.06	0.06	0.00	0.00	0.06	0.00	0.09	0.03
1000	0.06	0.03	0.00	0.12	0.03	0.06	0.12	0.00	0.09	0.09	0.12	0.09	0.06	0.00	0.03	0.06	0.00	0.12	0.06
2000	0.09	0.09	0.06	0.25	0.16	0.25	0.22	0.06	0.25	0.19	0.06	0.38	0.06	0.12	0.16	0.19	0.06	0.38	0.16
3000	0.22	0.19	0.34	0.34	0.16	0.47	0.41	0.12	0.25	0.50	0.12	0.53	0.31	0.19	0.25	0.47	0.12	0.53	0.30
4000	0.47	0.31	0.41	0.69	0.28	0.66	0.62	0.28	0.31	0.62	0.25	0.72	0.62	0.34	0.50	0.62	0.25	0.72	0.48
5000	0.56	0.47	0.38	0.75	0.50	0.75	0.72	0.38	0.50	0.78	0.25	0.81	0.69	0.47	0.59	0.78	0.25	0.81	0.59
10000	0.91	0.84	0.91	0.97	0.72	0.97	0.94	0.84	0.78	0.97	0.69	1.00	0.91	0.75	0.91	0.97	0.69	1.00	0.88
15000	0.97	1.00	0.94	1.00	0.81	1.00	1.00	1.00	0.94	1.00	0.94	1.00	1.00	1.00	1.00	1.00	0.81	1.00	0.97
20000	1.00	1.00	0.97	1.00	0.91	1.00	1.00	1.00	0.97	1.00	1.00	1.00	1.00	1.00	1.00	1.00	0.91	1.00	0.99

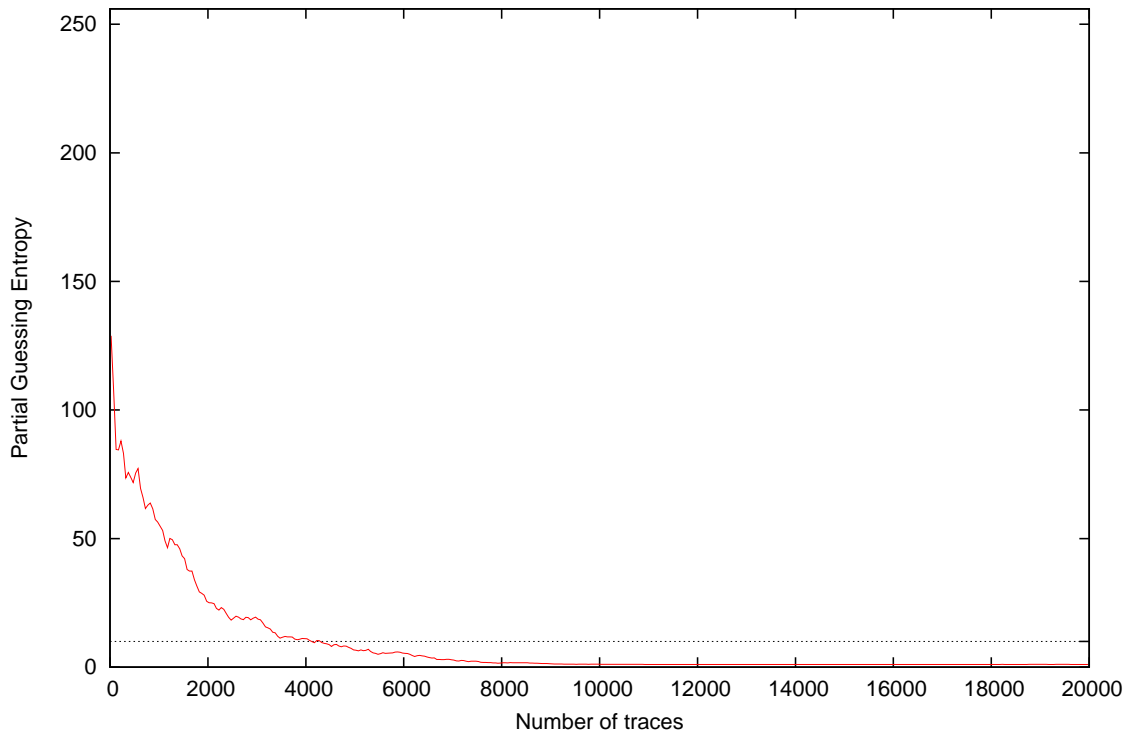
## 4 Partial Guessing Entropy



Partial Guessing Entropy for Subkey Byte #3

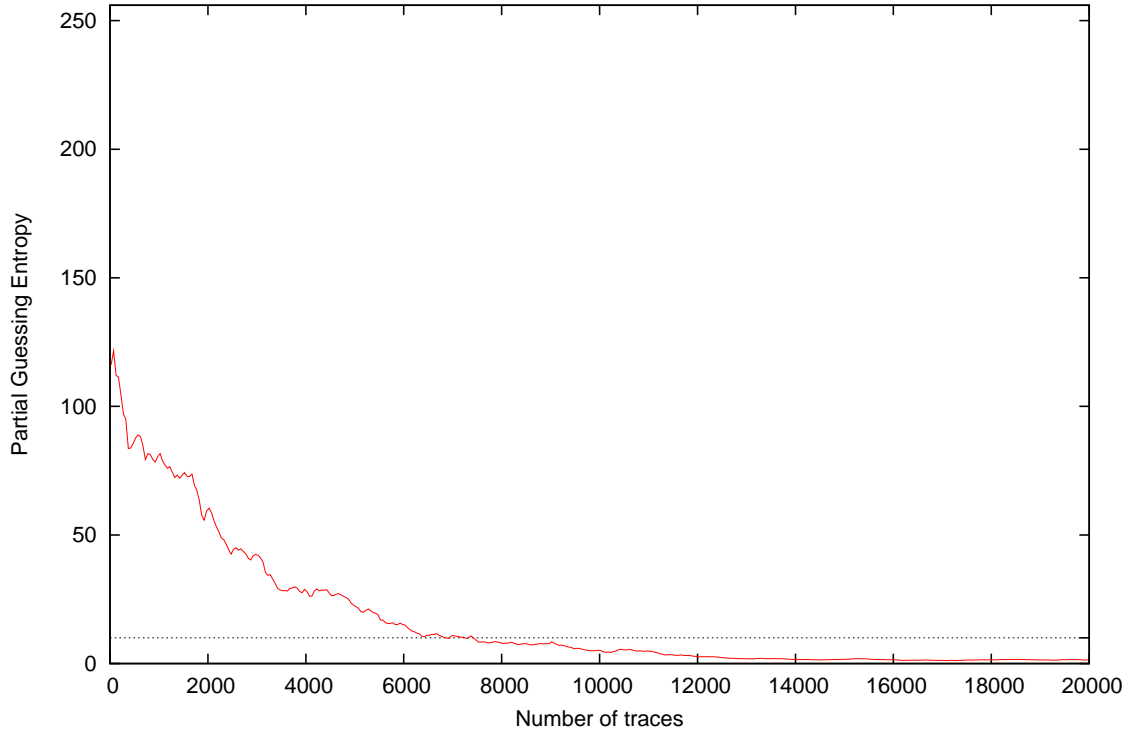


Partial Guessing Entropy for Subkey Byte #4

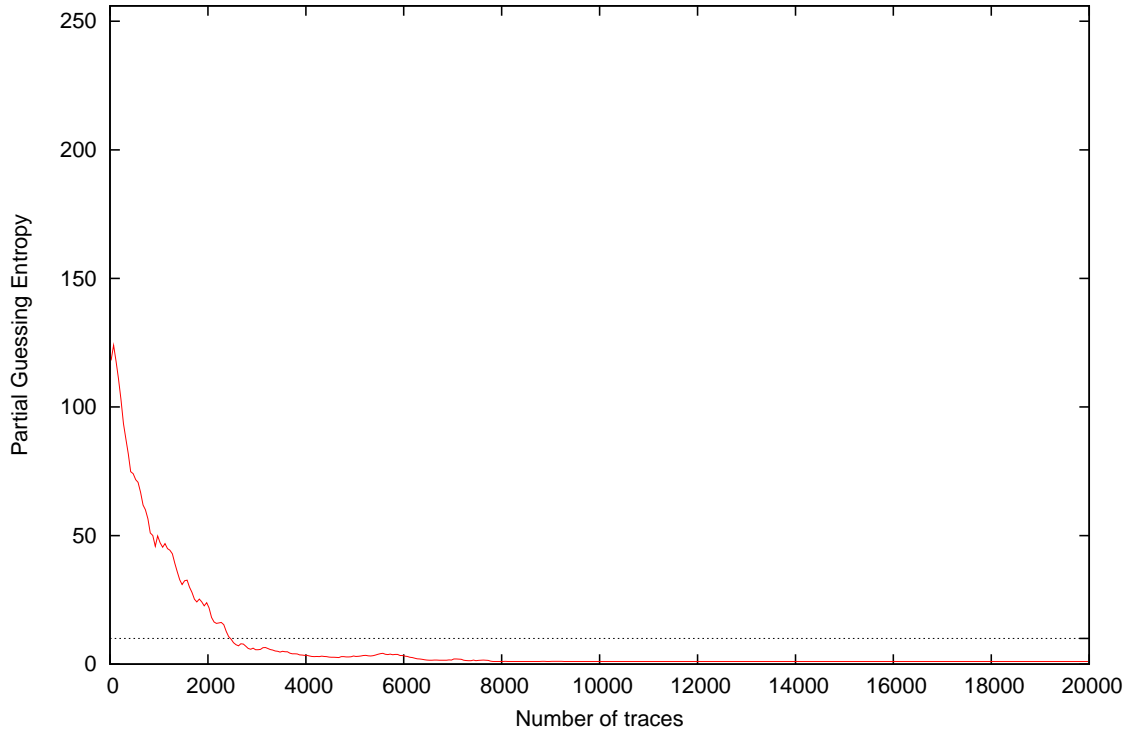




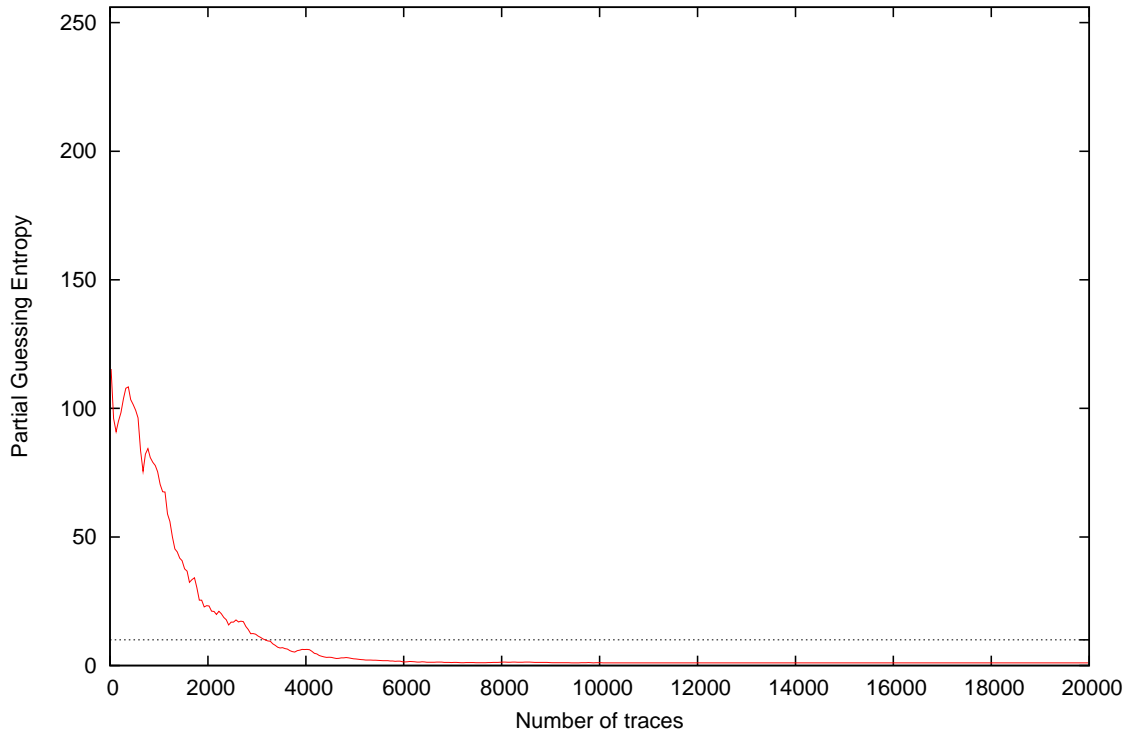
Partial Guessing Entropy for Subkey Byte #5



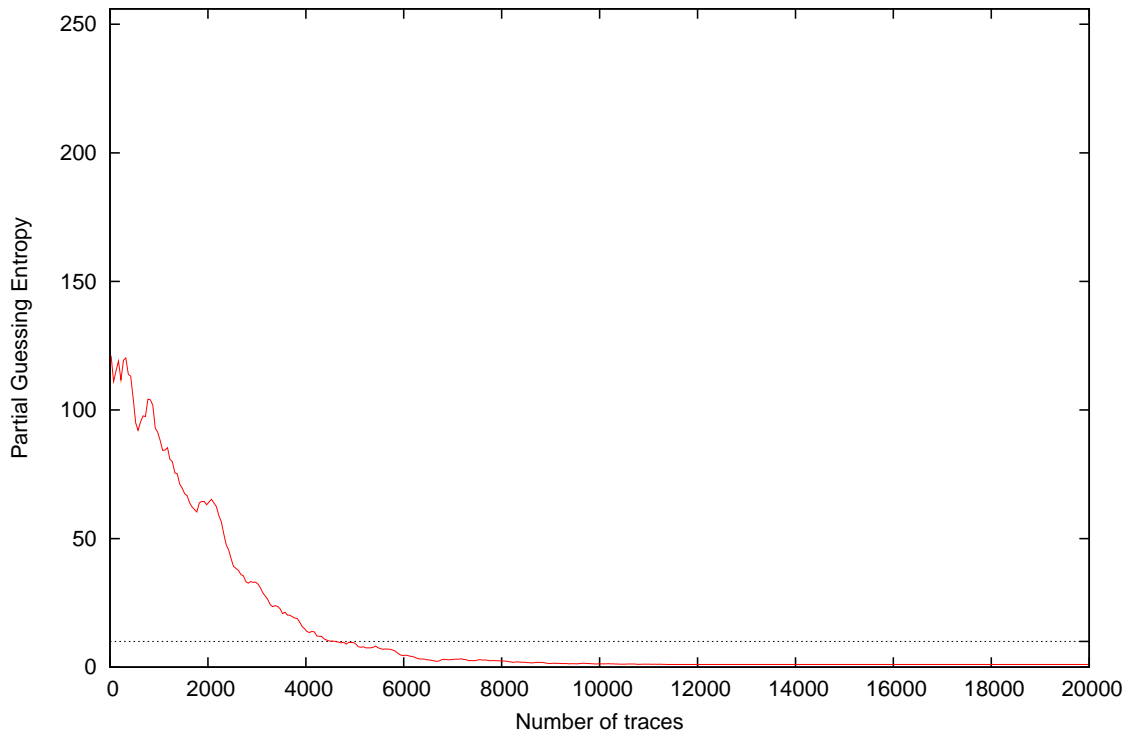
Partial Guessing Entropy for Subkey Byte #6



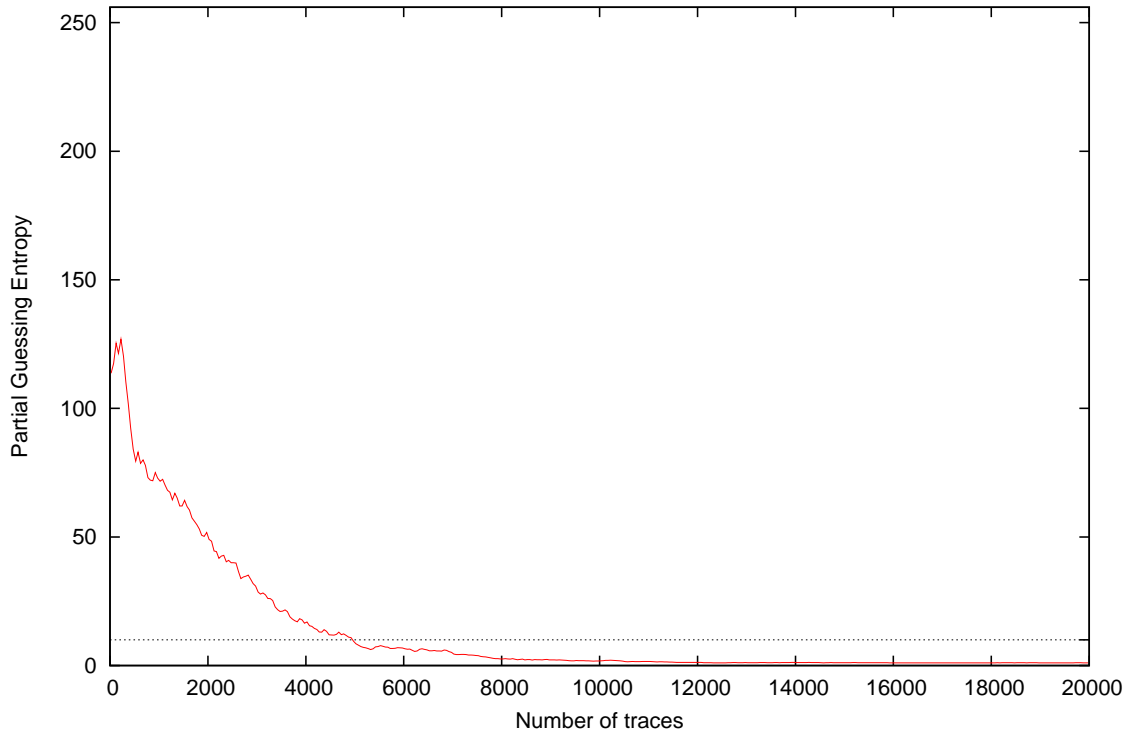
Partial Guessing Entropy for Subkey Byte #7



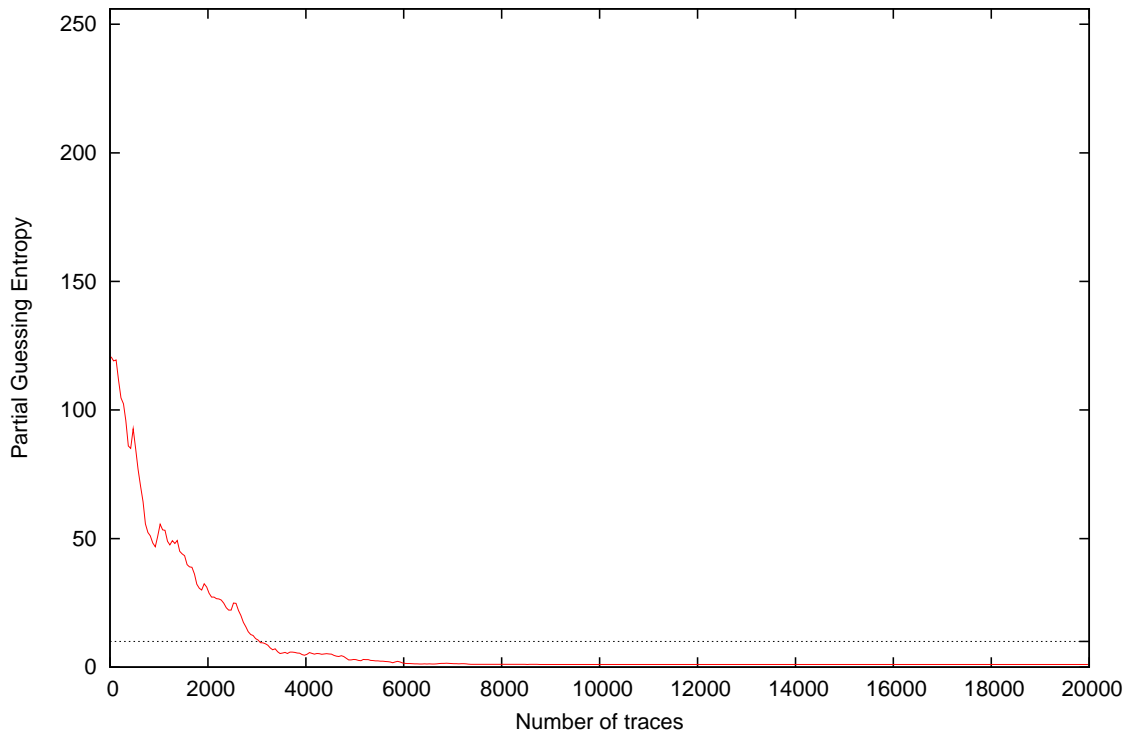
Partial Guessing Entropy for Subkey Byte #8



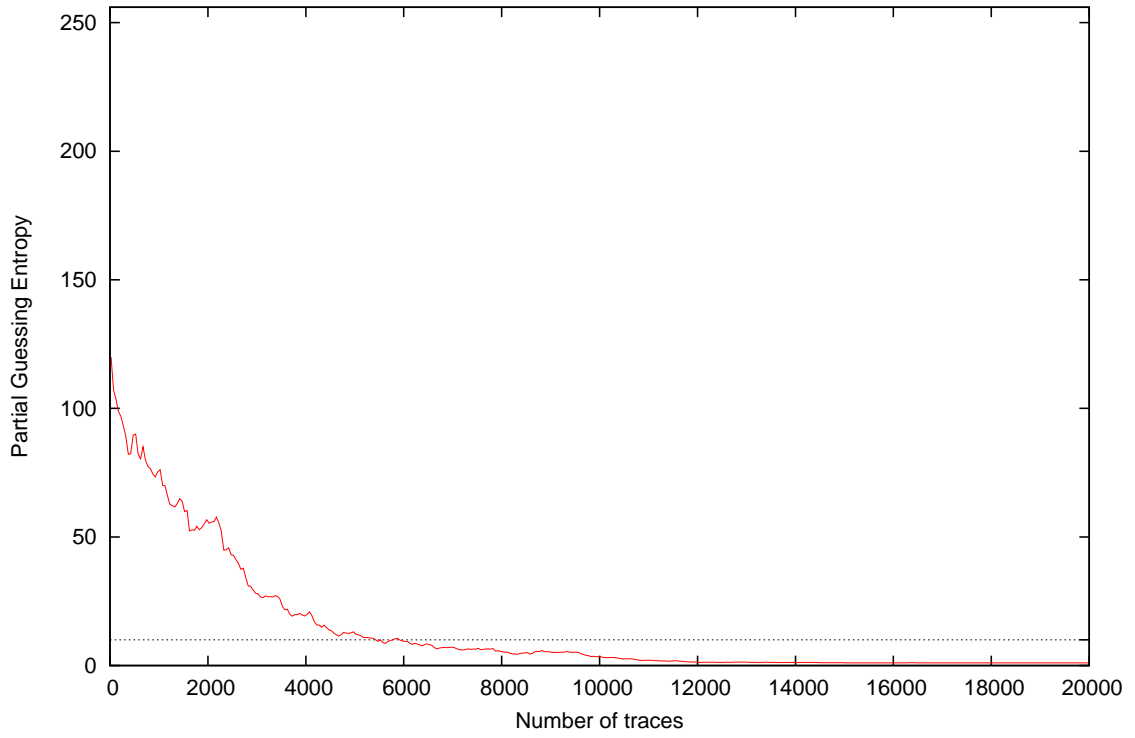
Partial Guessing Entropy for Subkey Byte #9



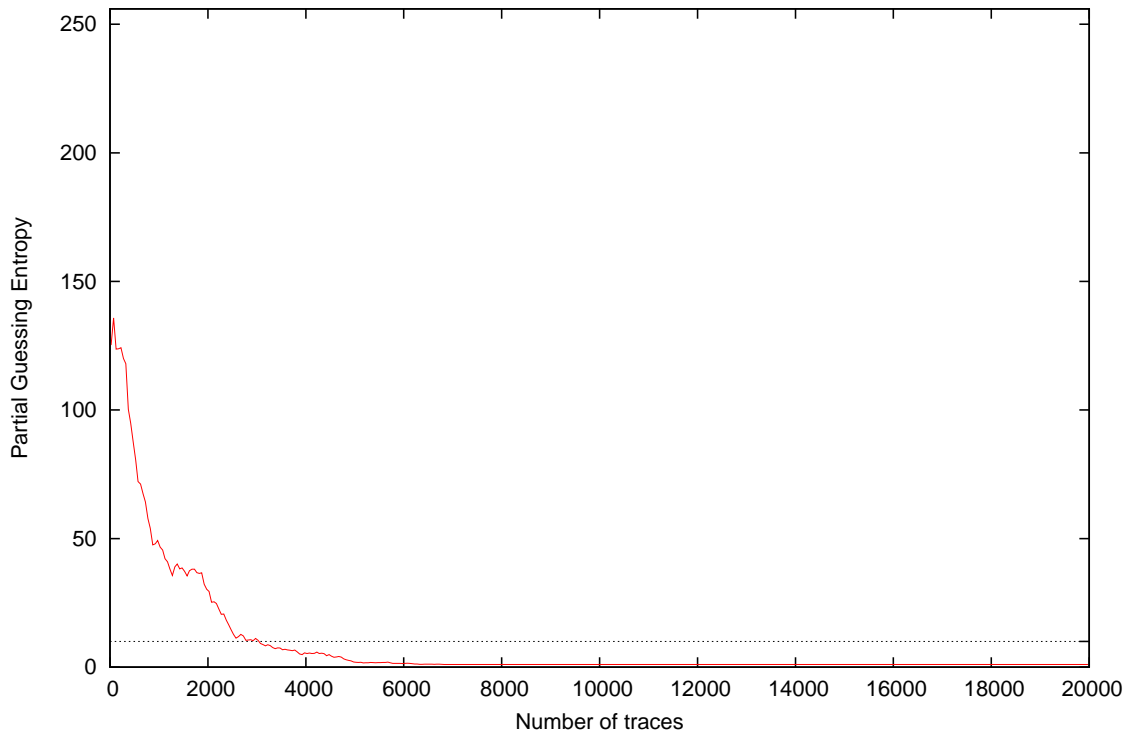
Partial Guessing Entropy for Subkey Byte #10



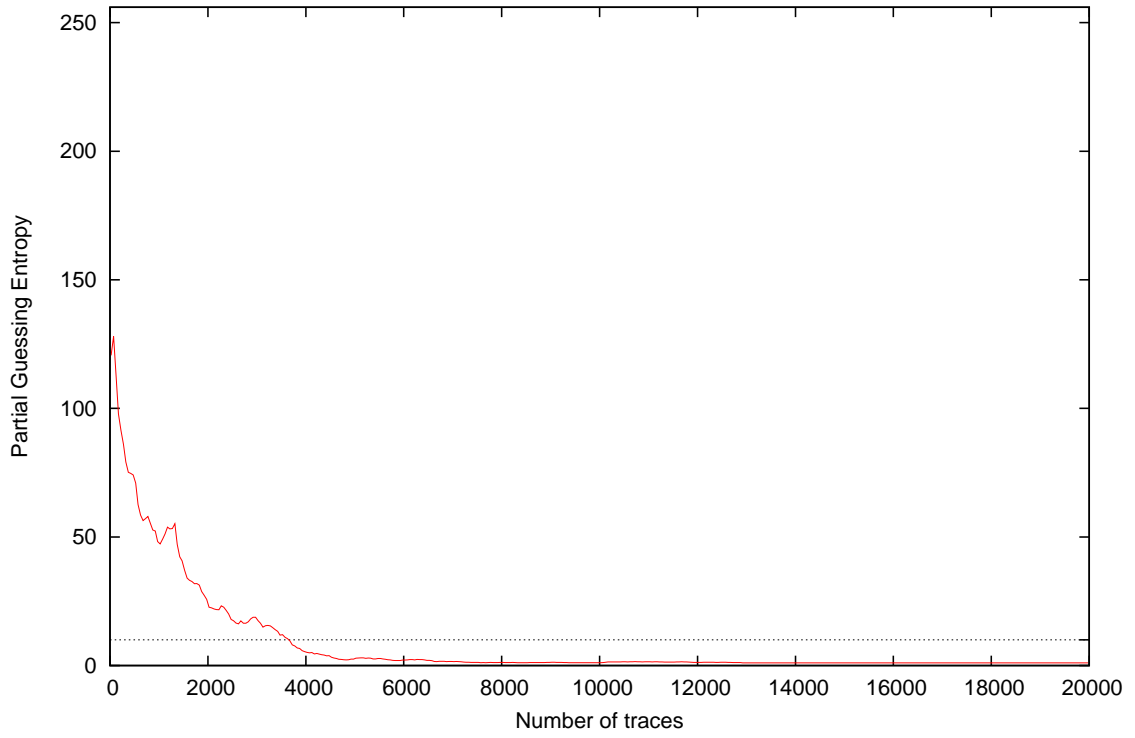
Partial Guessing Entropy for Subkey Byte #11



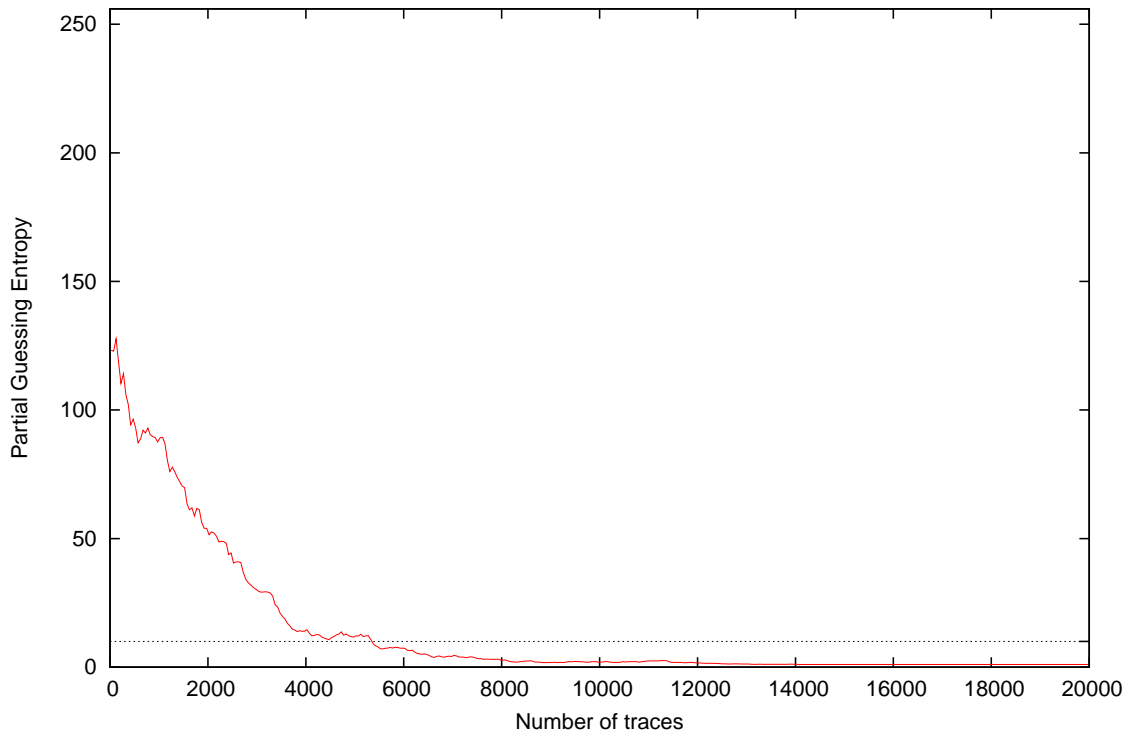
Partial Guessing Entropy for Subkey Byte #12

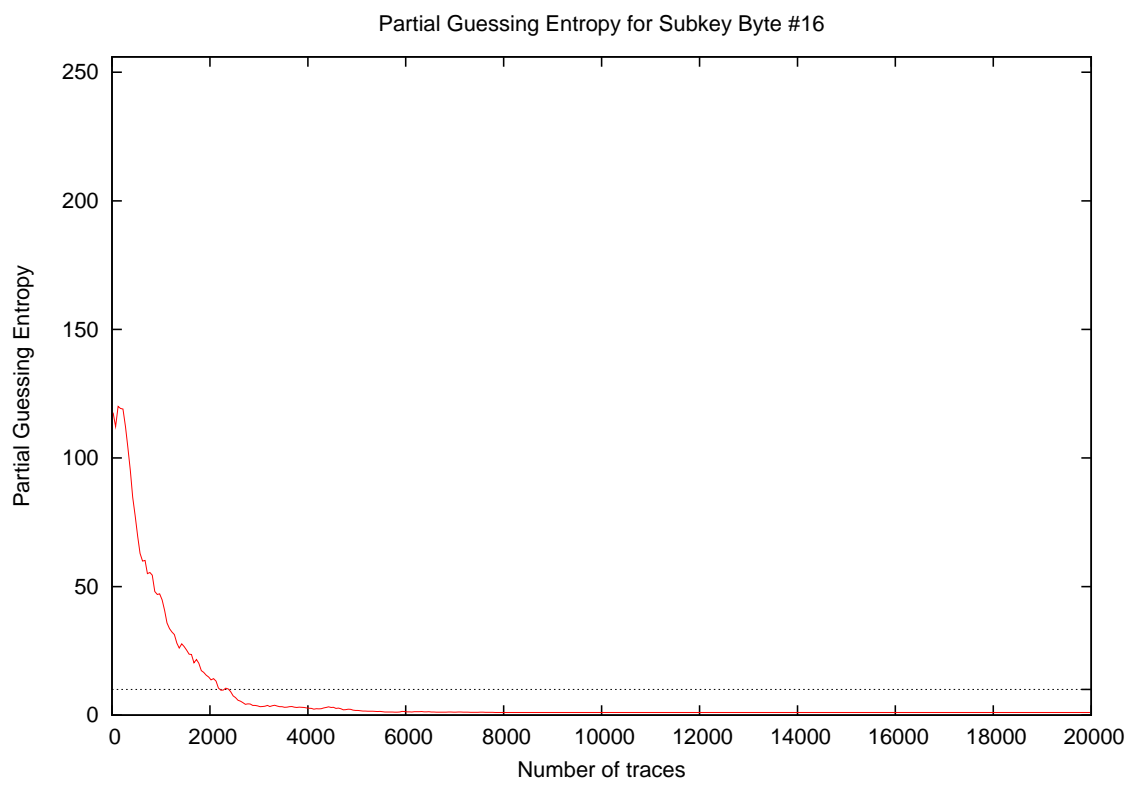
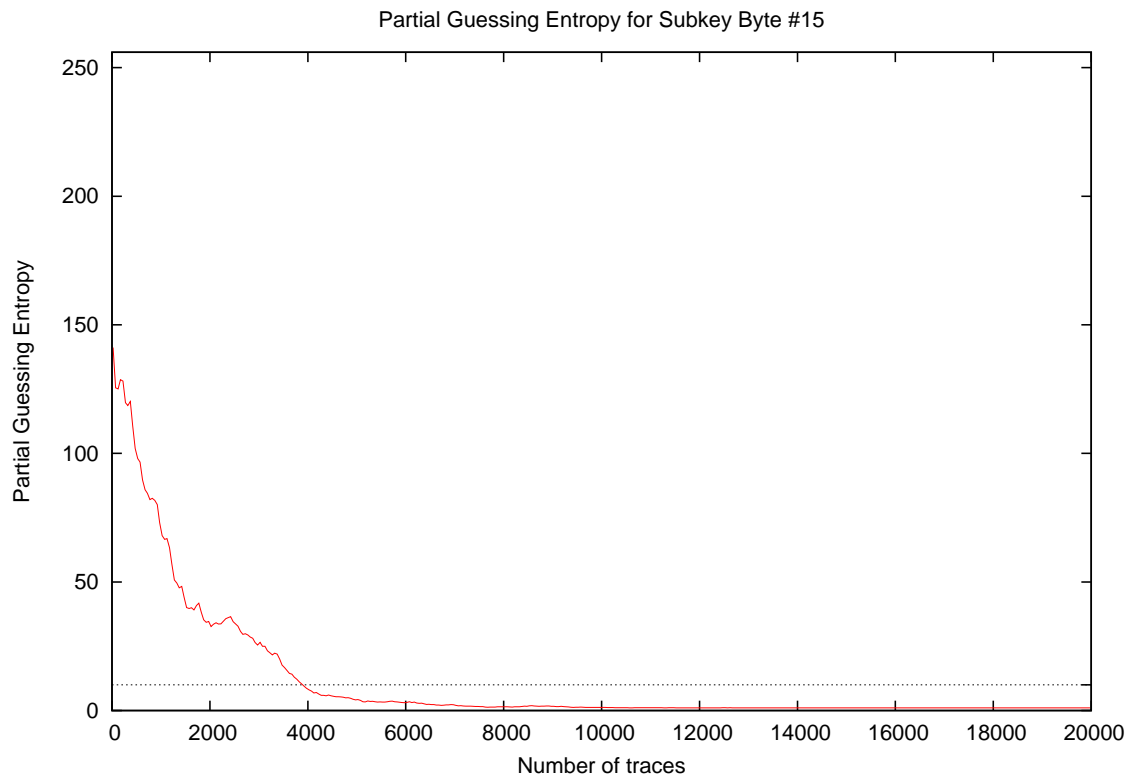


Partial Guessing Entropy for Subkey Byte #13

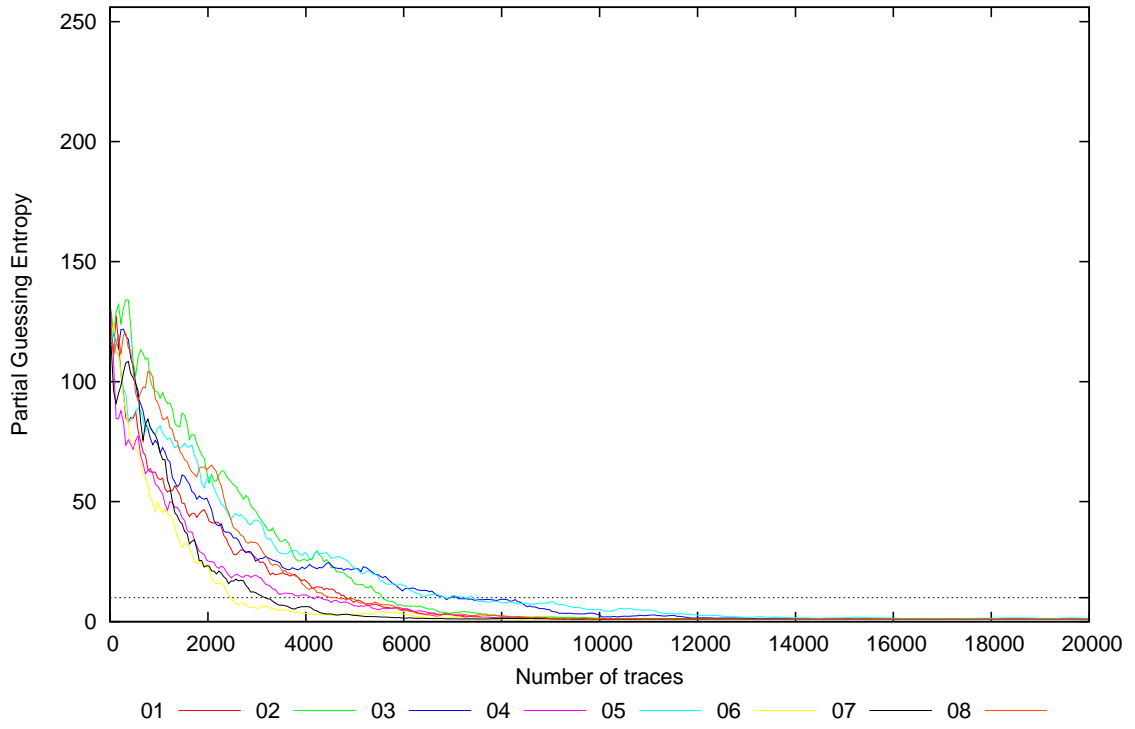


Partial Guessing Entropy for Subkey Byte #14

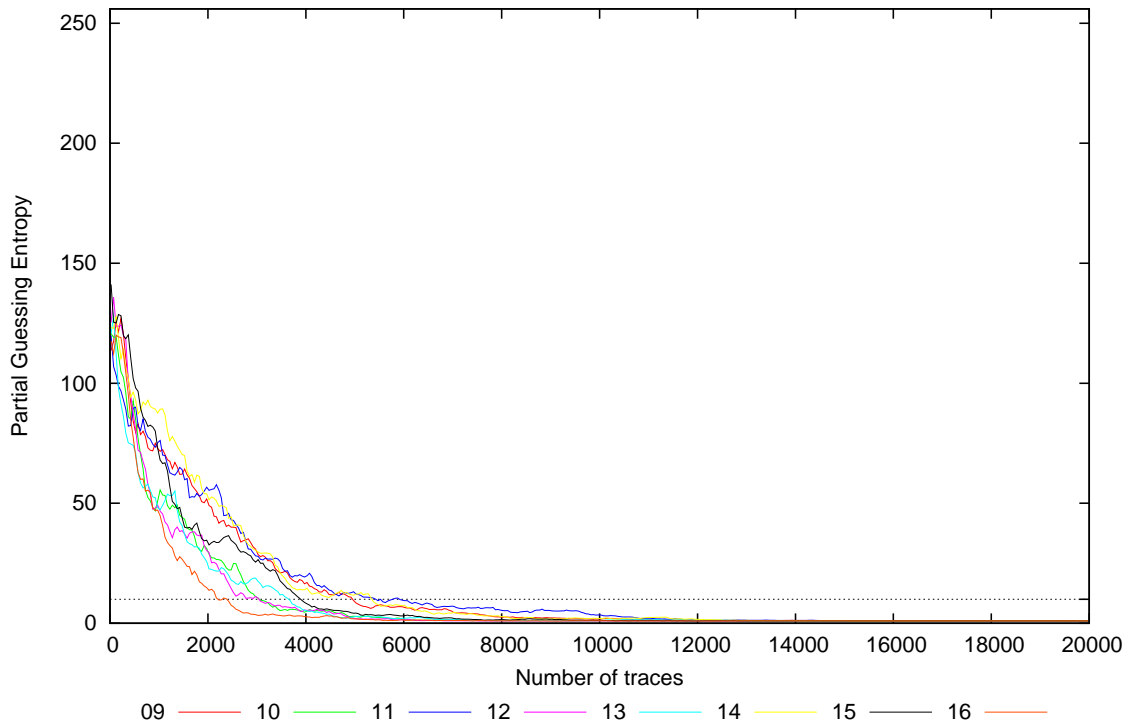




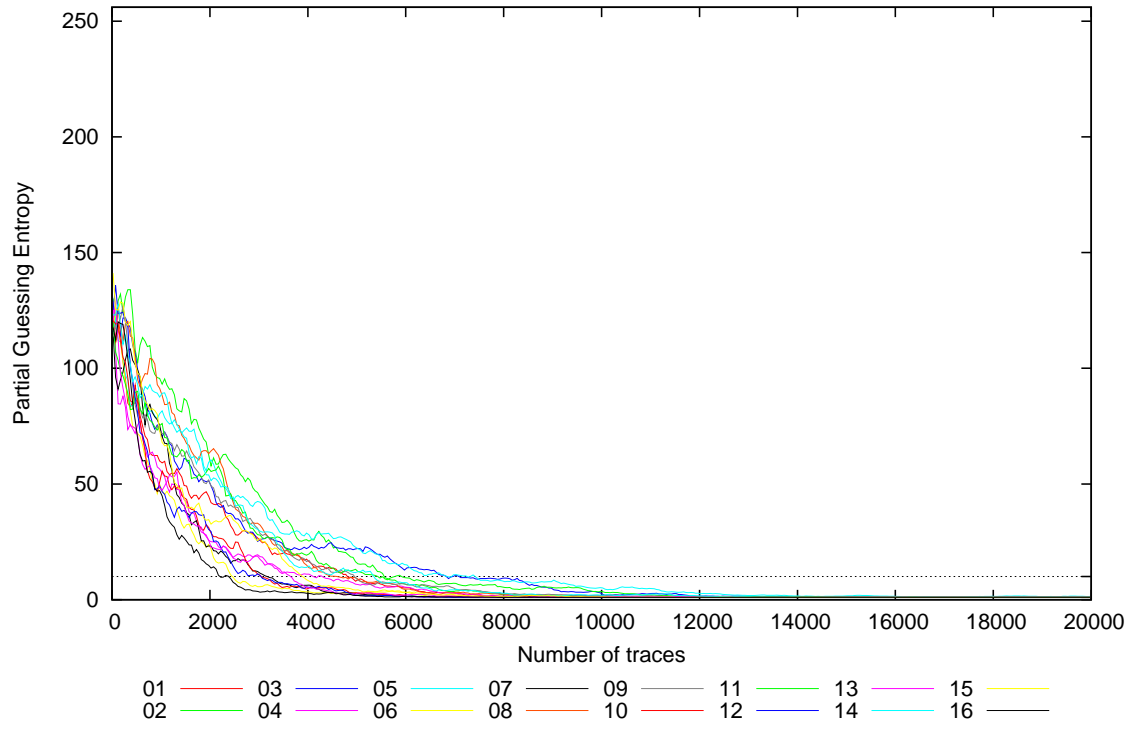
Partial Guessing Entropy for Subkey Bytes #1 to #8



Partial Guessing Entropy for Subkey Bytes #9 to #16



Partial Guessing Entropy for Subkey Bytes #1 to #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	137.4	116.7	112.1	138.2	110.2	127.1	135.1	123.8	130.5	116.0	133.0	129.5	127.3	98.7	135.4	104.5	98.7	138.2	123.5
20	134.0	129.2	116.1	152.1	108.3	101.8	123.5	123.7	117.4	113.3	118.0	115.5	109.8	113.9	148.4	119.6	101.8	152.1	121.5
30	117.2	134.0	112.2	128.0	119.7	116.0	102.5	114.2	101.7	118.3	114.7	133.0	113.2	126.9	143.8	120.2	101.7	143.8	119.7
40	118.5	127.3	119.0	116.1	110.3	118.9	98.6	121.6	108.6	121.0	112.1	120.8	108.3	132.3	146.0	121.0	98.6	146.0	118.8
50	104.7	119.5	109.8	127.6	127.7	117.5	101.7	122.7	112.5	120.7	118.0	124.8	119.5	121.5	128.3	123.2	101.7	128.3	118.7
100	120.9	125.2	118.4	88.8	119.7	121.7	88.0	114.9	126.9	126.9	107.2	133.8	122.0	131.9	136.3	118.2	88.0	136.3	118.8
200	108.1	124.8	115.9	86.4	104.7	109.6	92.8	115.9	121.2	103.8	101.5	126.6	94.9	111.1	128.1	125.4	86.4	128.1	110.7
300	89.0	131.7	119.0	75.8	95.8	87.4	104.3	121.9	117.8	103.3	88.8	121.2	82.1	109.2	116.7	103.0	75.8	131.7	104.2
400	83.3	132.3	111.1	77.1	80.3	82.0	105.5	111.6	97.3	82.1	84.4	97.7	73.5	95.2	119.9	89.8	73.5	132.3	95.2
500	84.7	104.0	104.2	73.0	88.3	73.8	103.4	100.8	84.6	95.0	91.9	85.5	71.1	93.8	99.7	75.3	71.1	104.2	89.3
1000	57.5	93.5	71.5	56.0	79.3	49.1	74.2	88.2	69.9	54.1	80.6	48.1	47.1	87.7	68.2	47.2	47.1	93.5	67.0
2000	43.5	59.1	50.9	24.4	59.2	23.8	23.6	62.8	50.6	29.9	57.6	30.0	24.8	53.2	33.1	14.6	14.6	62.8	40.1
3000	26.5	45.6	24.8	18.9	41.9	5.5	12.3	32.2	30.6	11.0	28.7	11.2	18.4	29.8	26.5	3.6	3.6	45.6	23.0
4000	17.0	25.8	21.9	10.9	28.6	3.3	6.3	14.7	17.1	4.8	19.4	5.5	5.2	14.8	8.4	2.8	2.8	28.6	12.9
5000	7.9	15.9	22.1	6.3	21.9	3.0	2.5	9.2	8.7	2.9	12.8	2.0	2.6	11.4	4.2	1.8	1.8	22.1	8.5
10000	1.2	1.4	2.7	1.1	5.2	1.0	1.1	1.3	1.8	1.0	3.5	1.0	1.1	1.8	1.2	1.0	1.0	5.2	1.7
15000	1.0	1.0	1.1	1.0	1.7	1.0	1.0	1.0	1.1	1.0	1.1	1.0	1.0	1.0	1.0	1.0	1.0	1.7	1.1
20000	1.0	1.0	1.0	1.0	1.4	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.4	1.0