

# DPA Contest v2

## Evaluation results

Reference attack

November 2010

## 1 Introduction

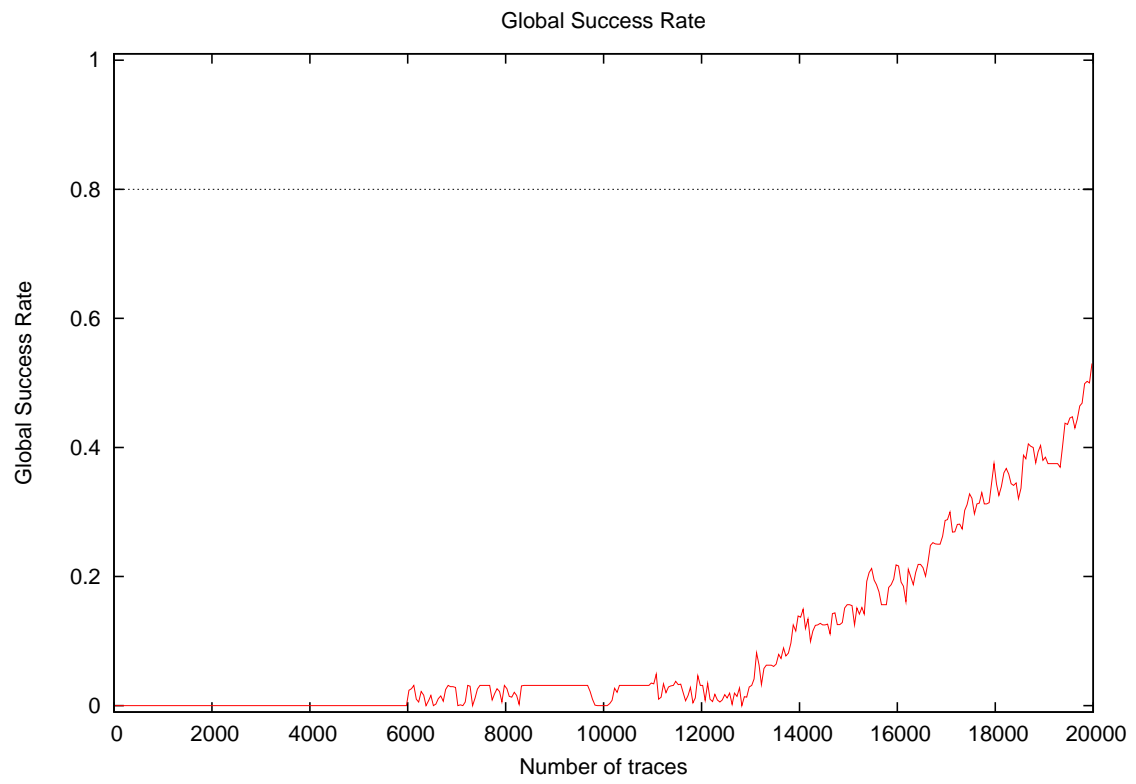
### 1.1 About the attack

- **Attack Name:** Correlation product
- **Sender/Team:** Olivier Meynard
- **Institution:** Télécom ParisTech, France
- **Language:** C
- **Operating system:** Linux
- **Attacked subkey:** 10

### 1.2 About the evaluation

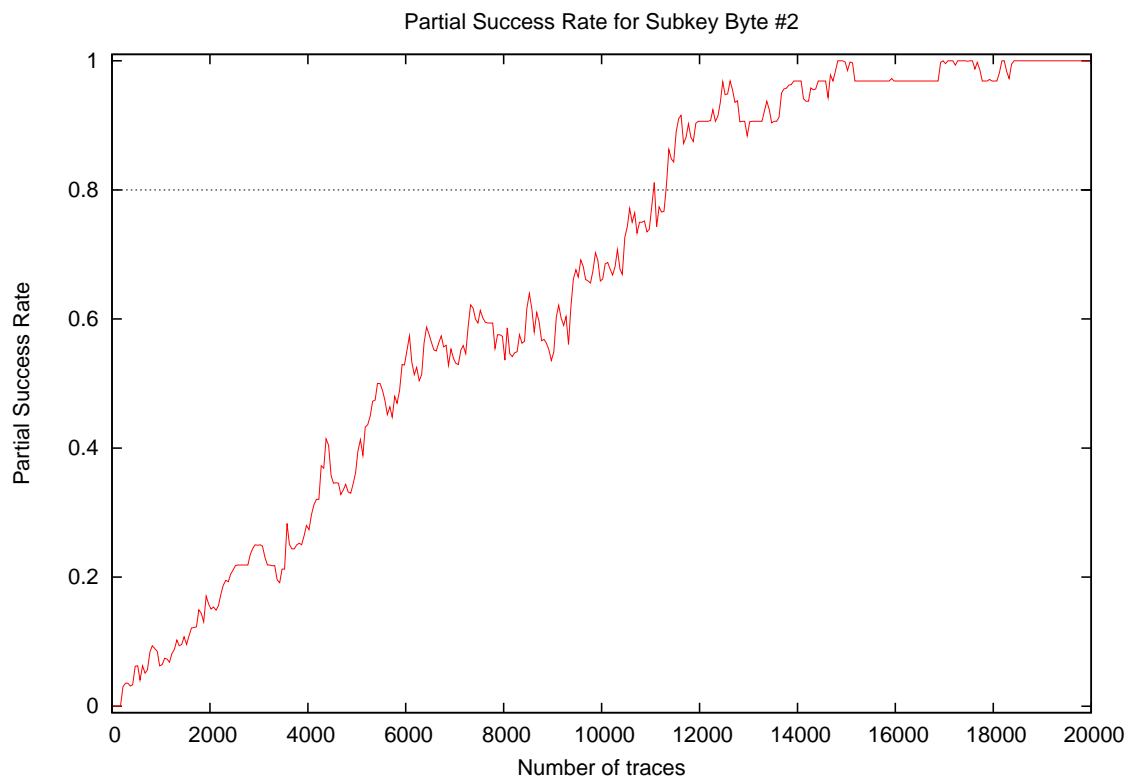
- **Date of evaluation:** November 2010

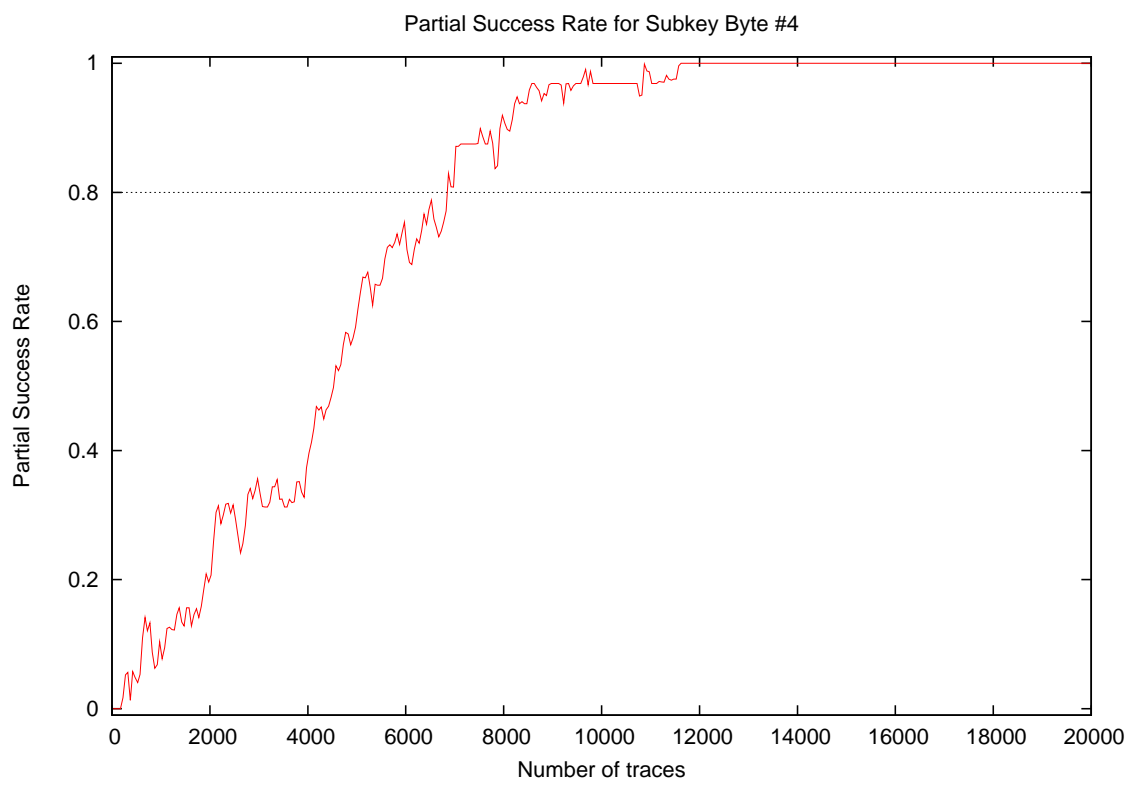
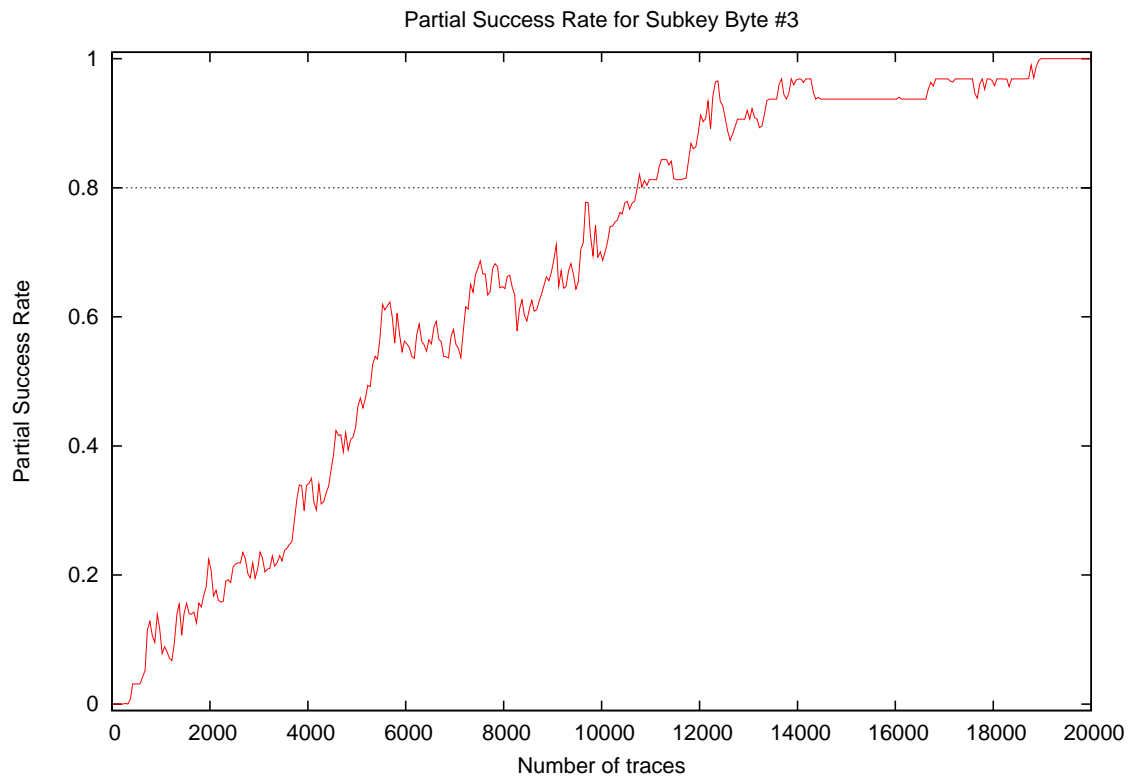
## 2 Global Success Rate

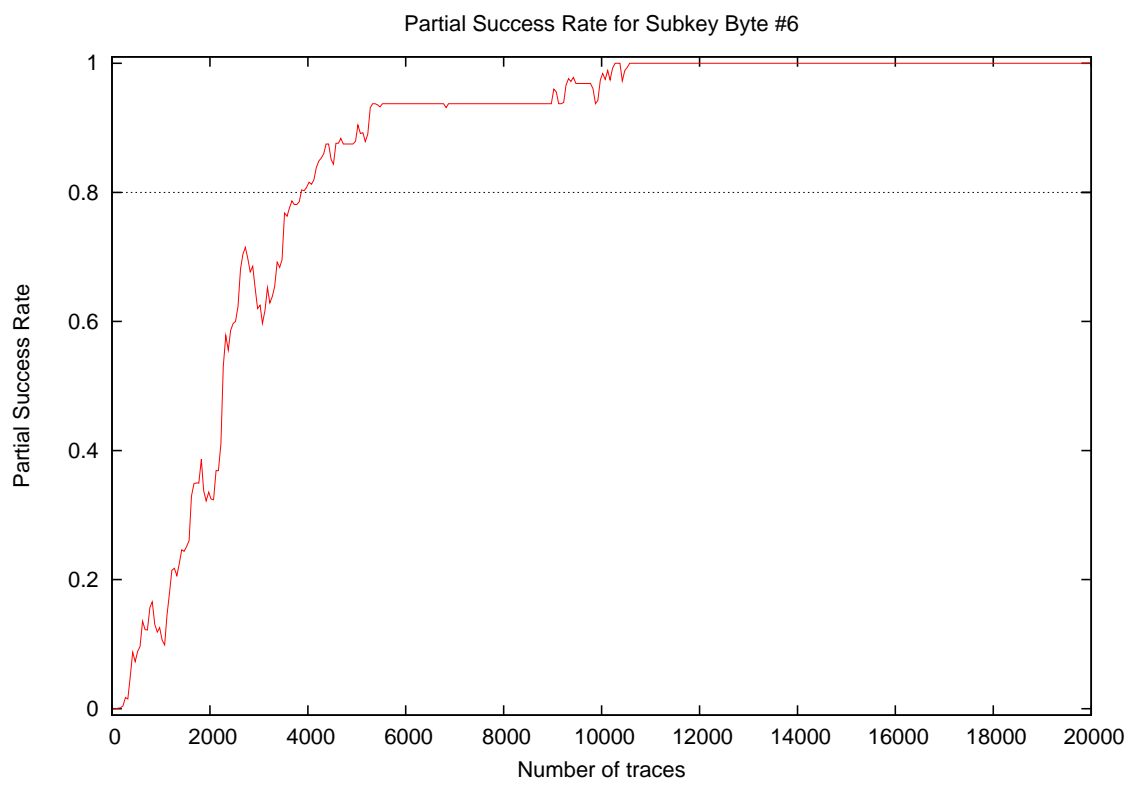
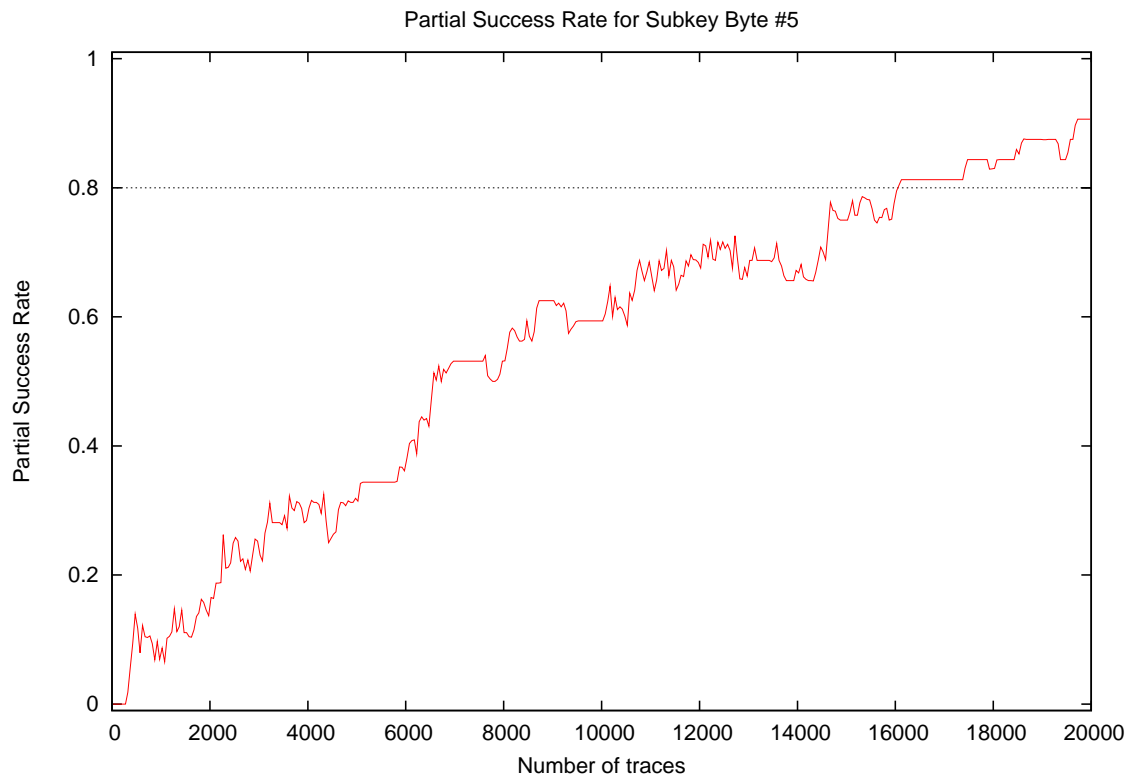


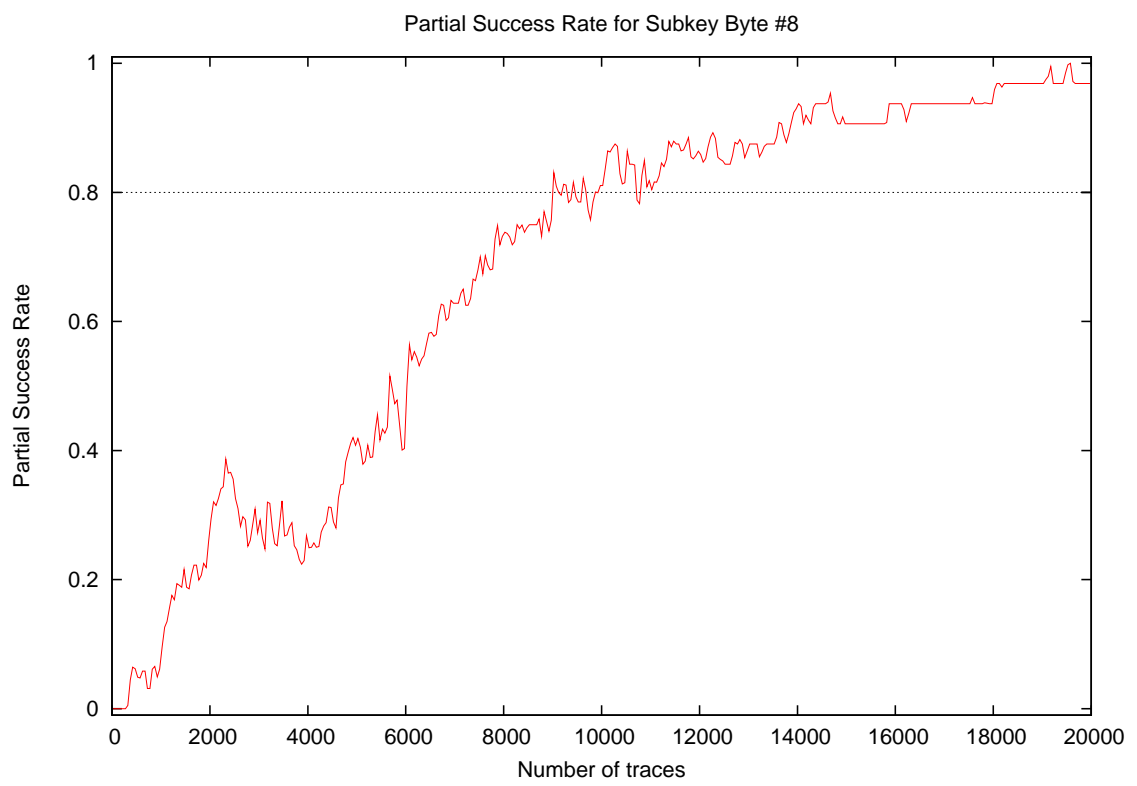
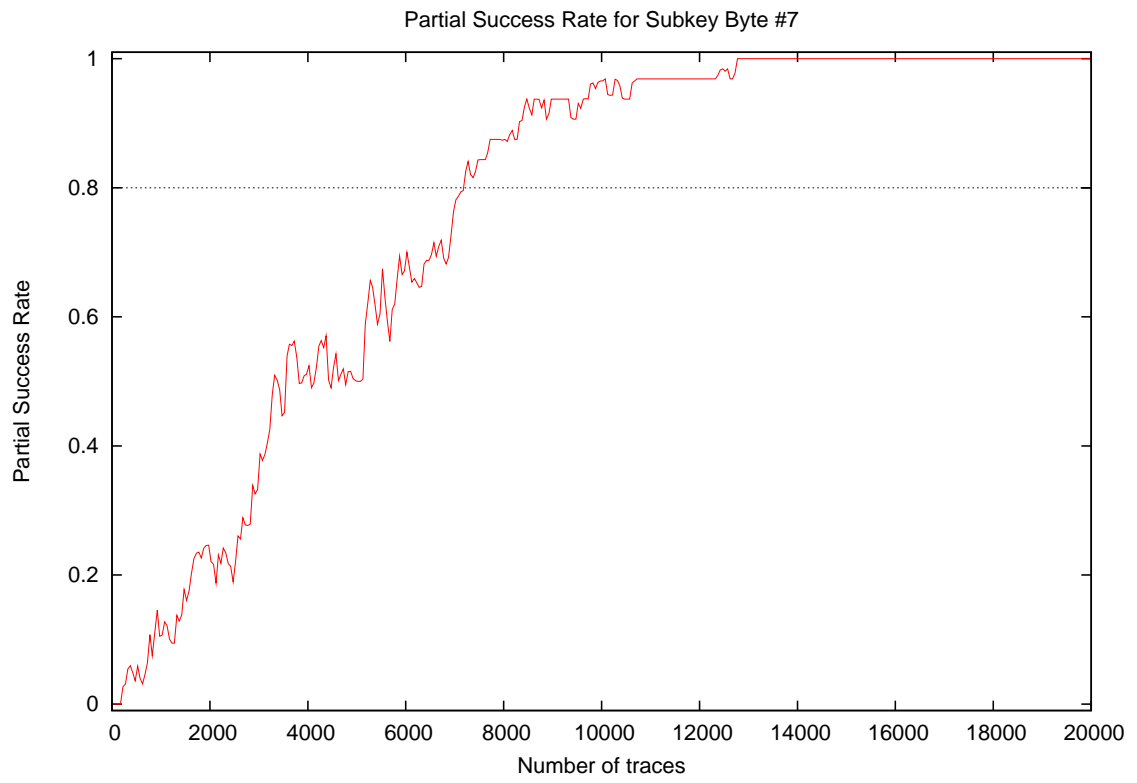
Number of traces	Global Success Rate
10	0.00
20	0.00
30	0.00
40	0.00
50	0.00
100	0.00
200	0.00
300	0.00
400	0.00
500	0.00
1000	0.00
2000	0.00
3000	0.00
4000	0.00
5000	0.00
10000	0.00
15000	0.16
20000	0.53

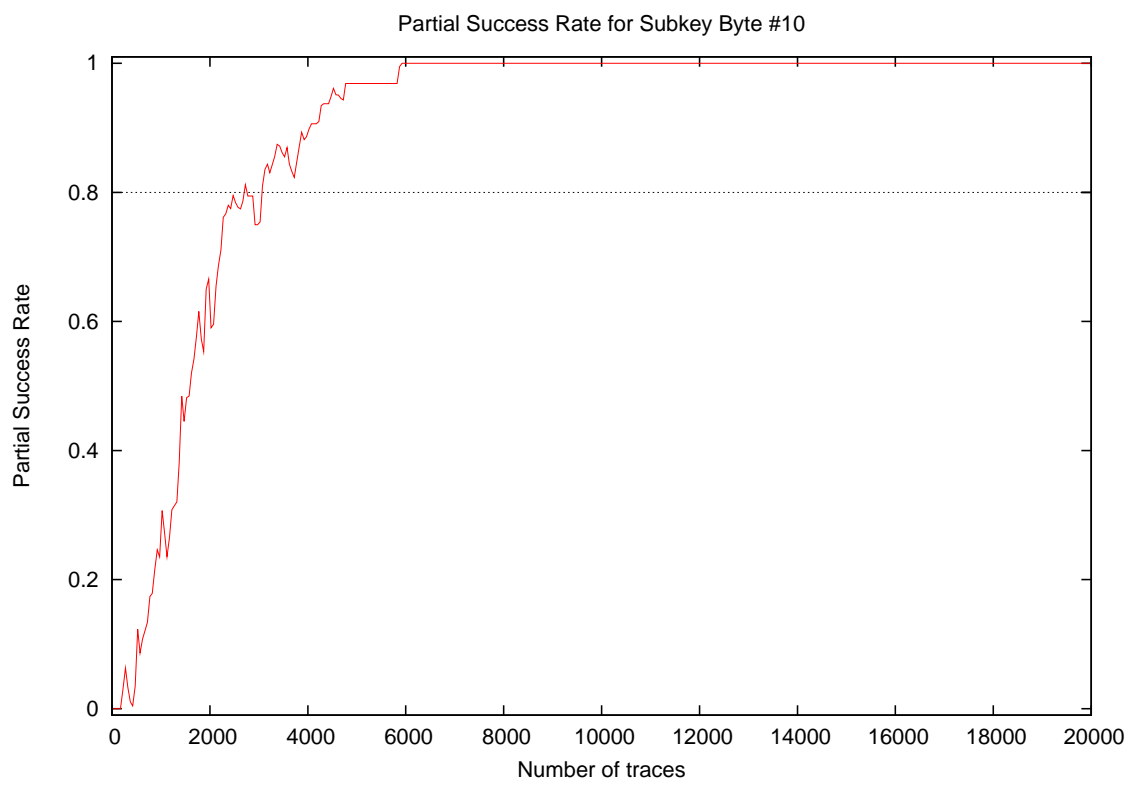
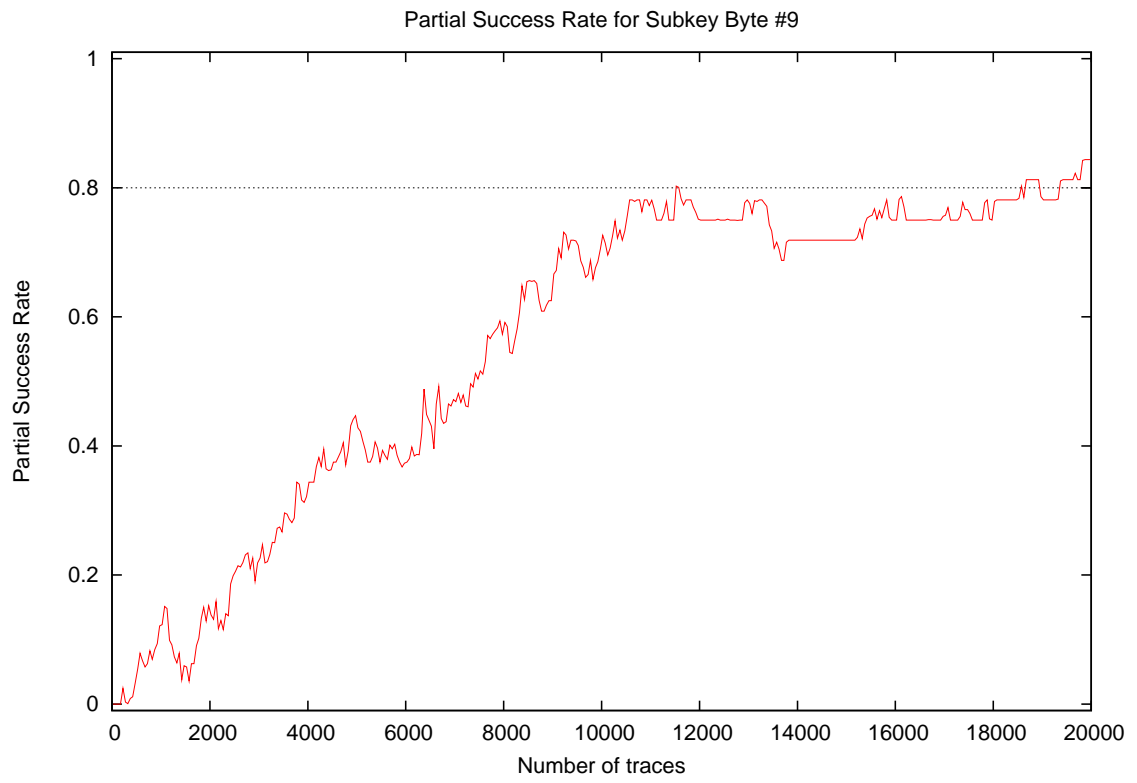
### 3 Partial Success Rate



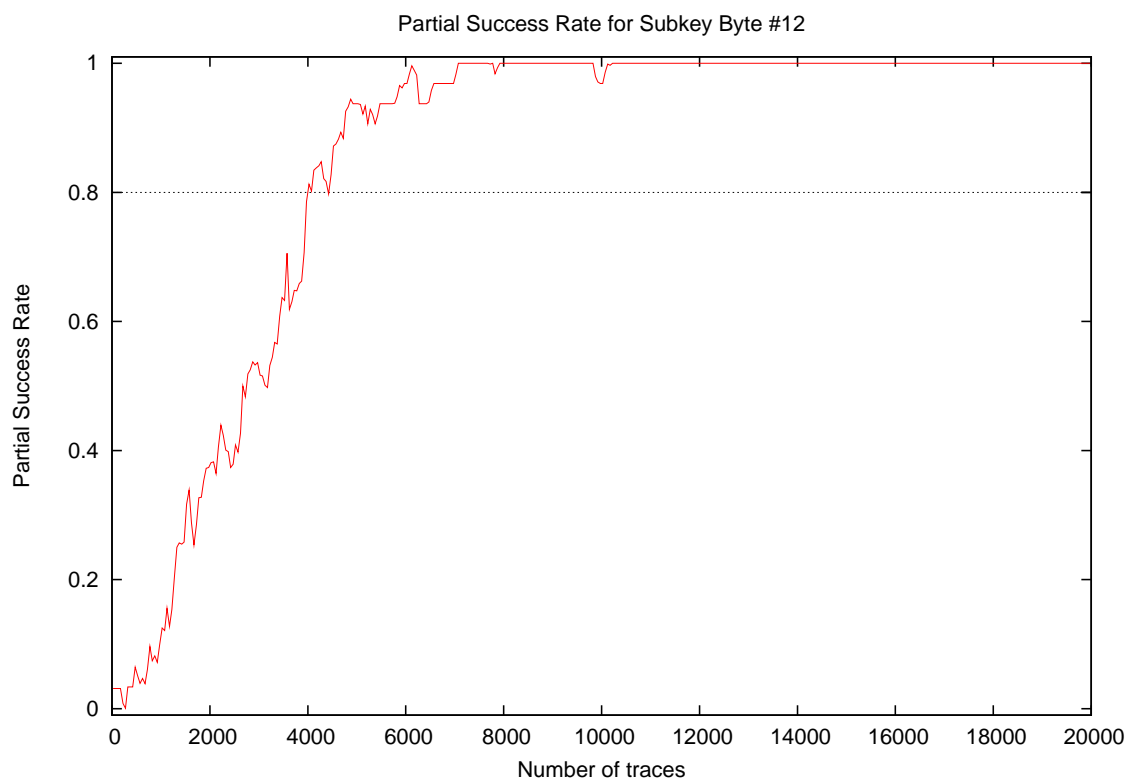
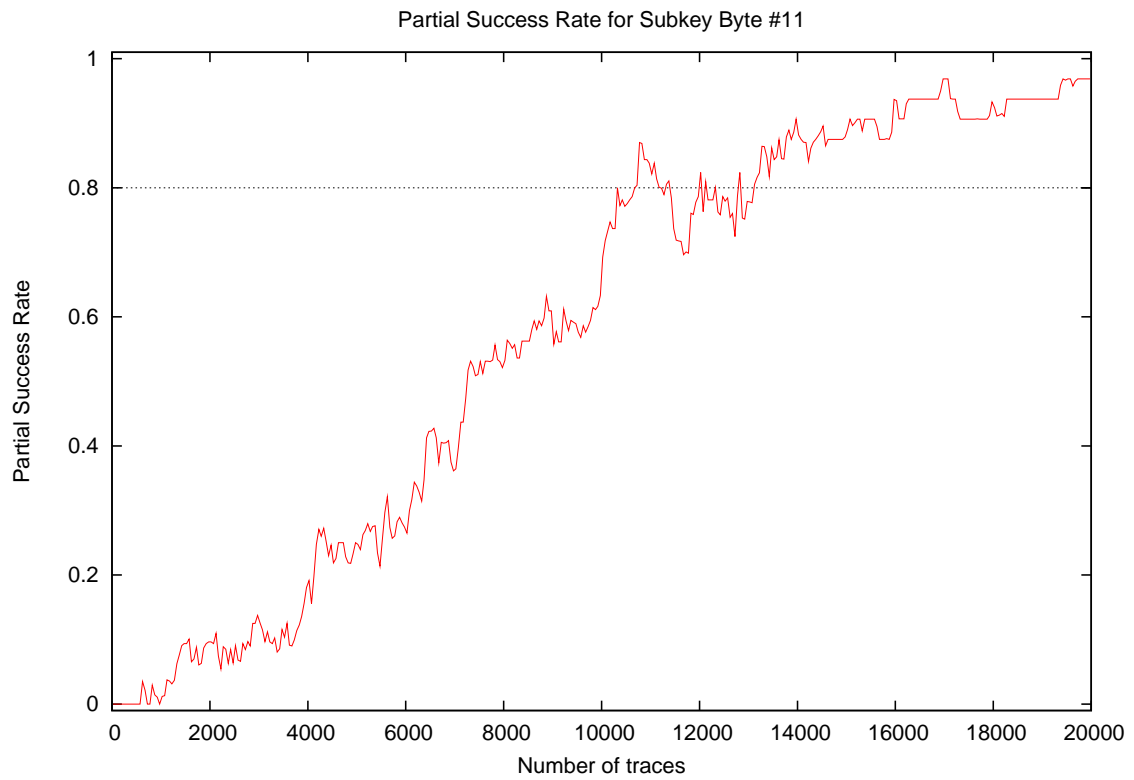


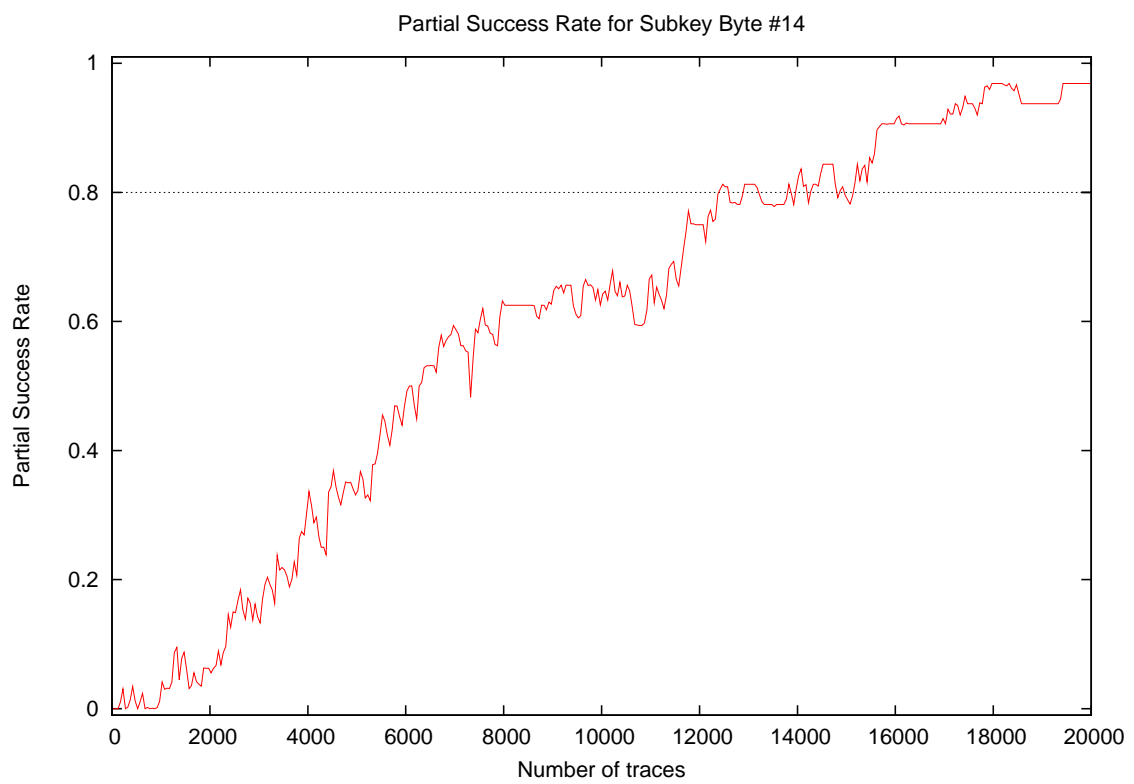
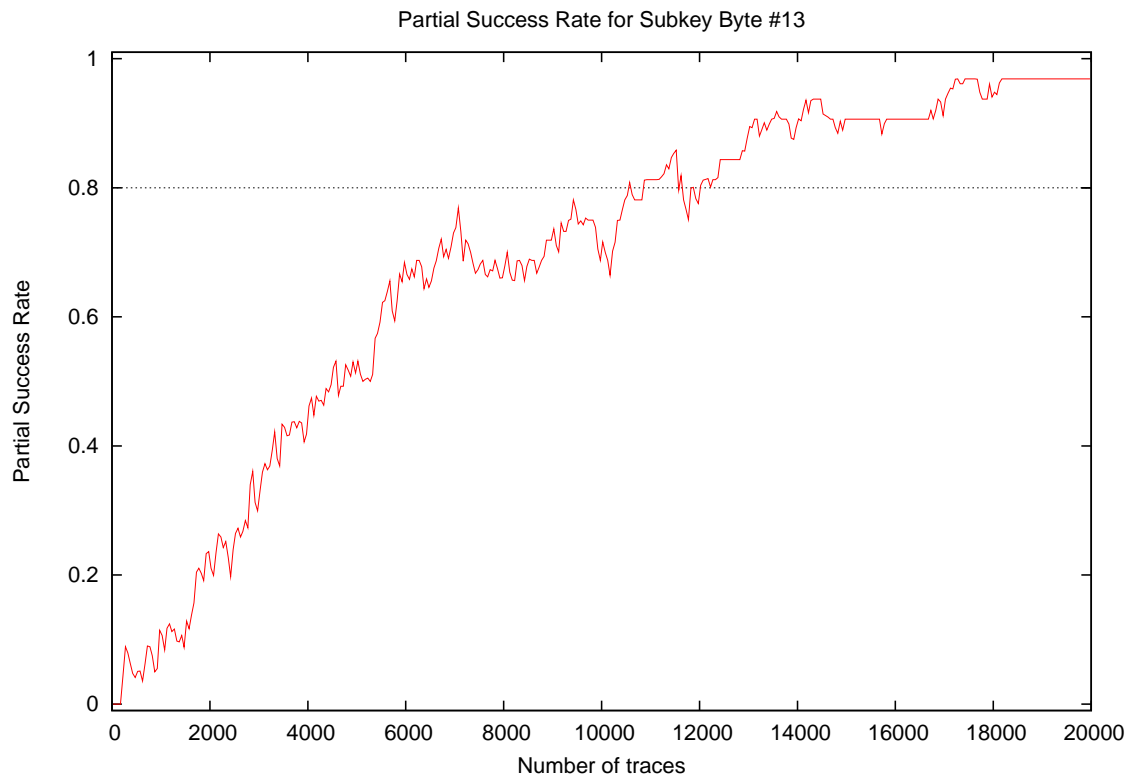


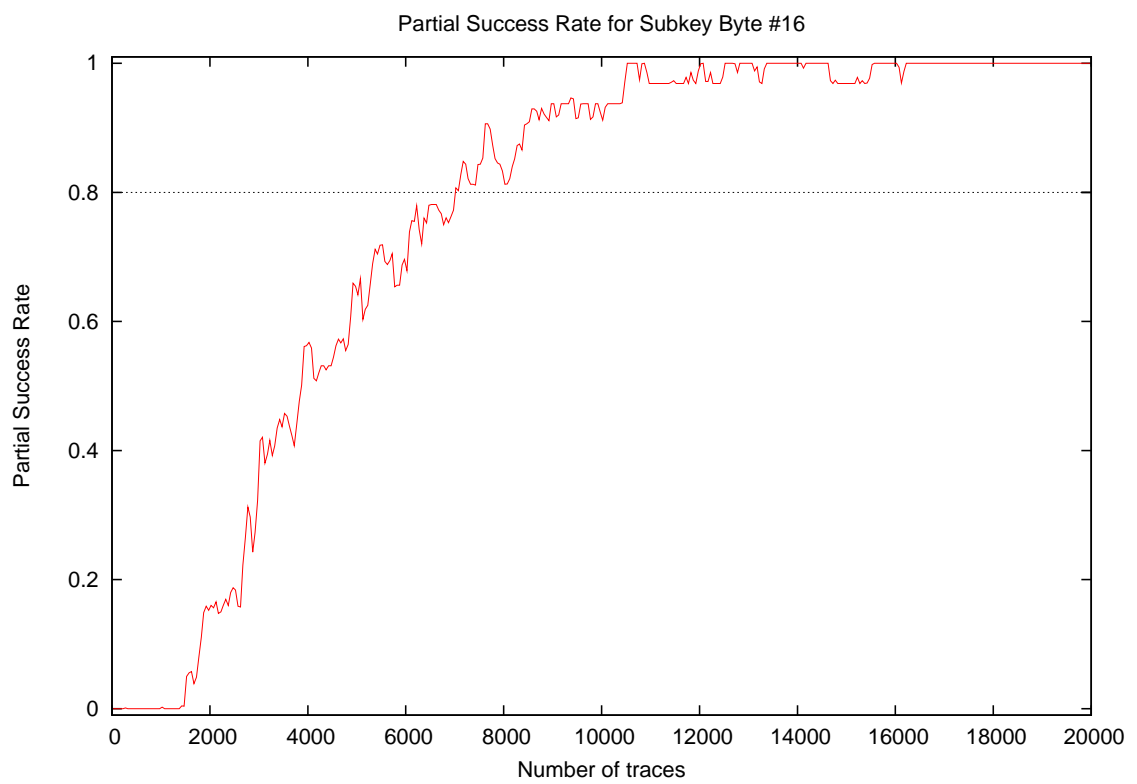
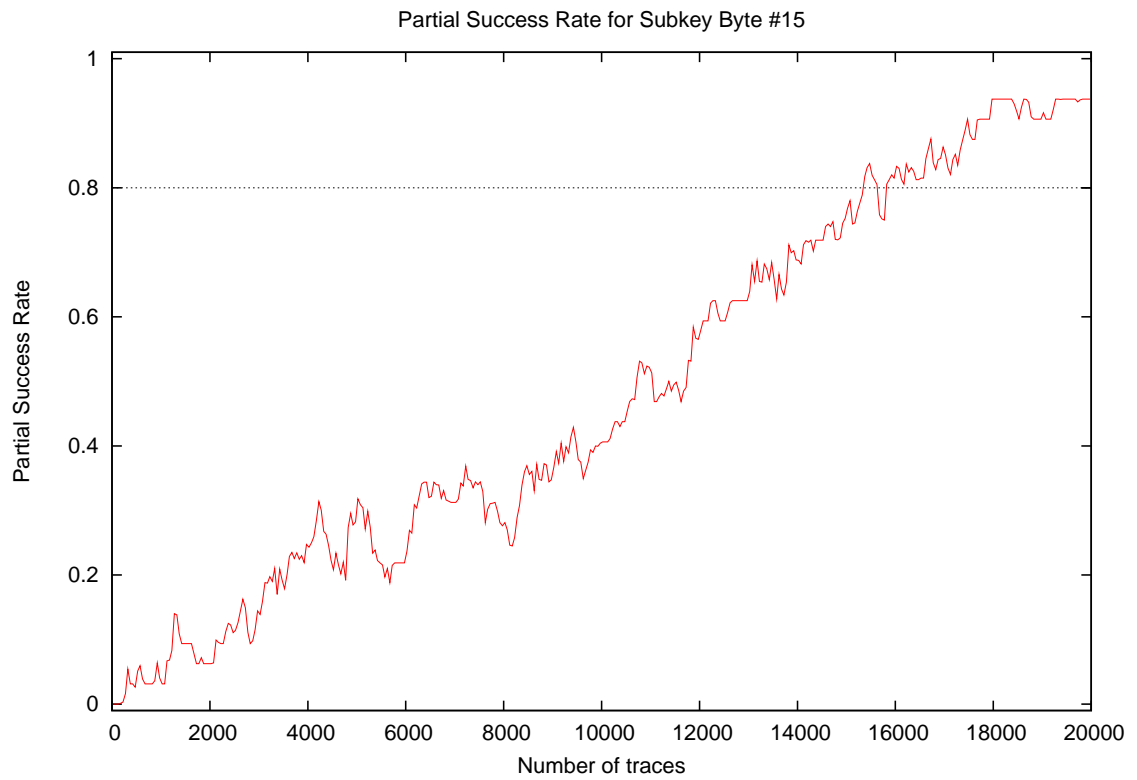


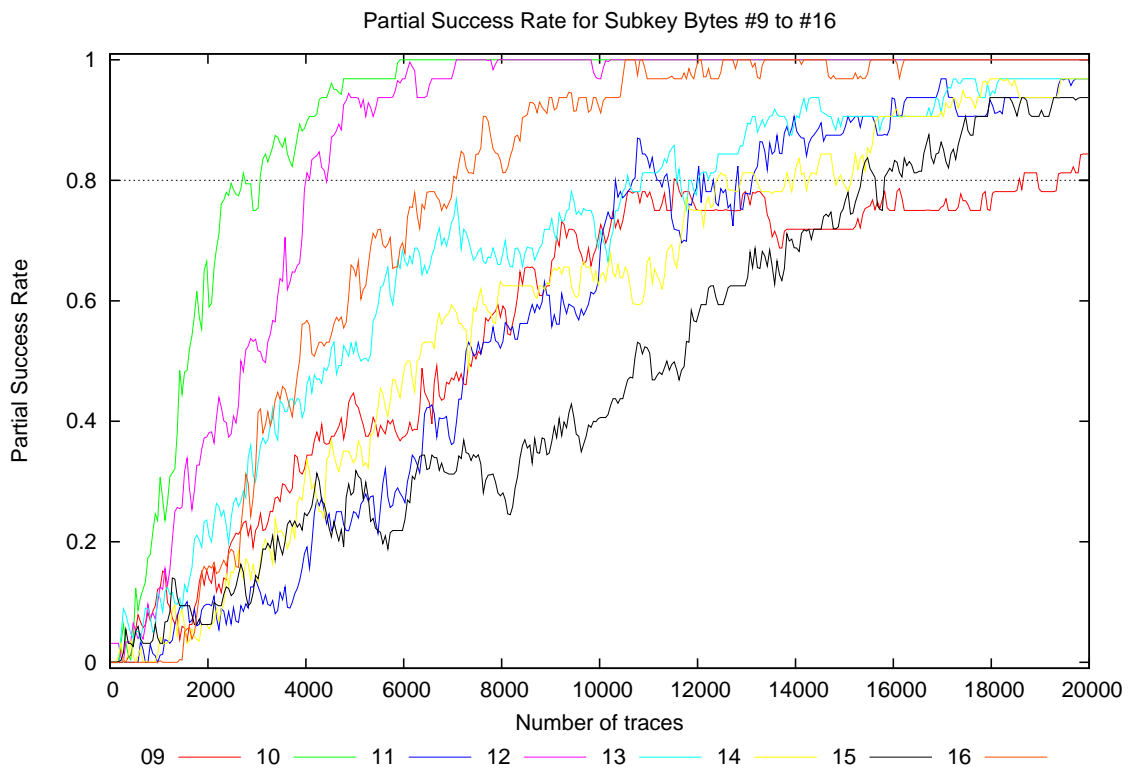
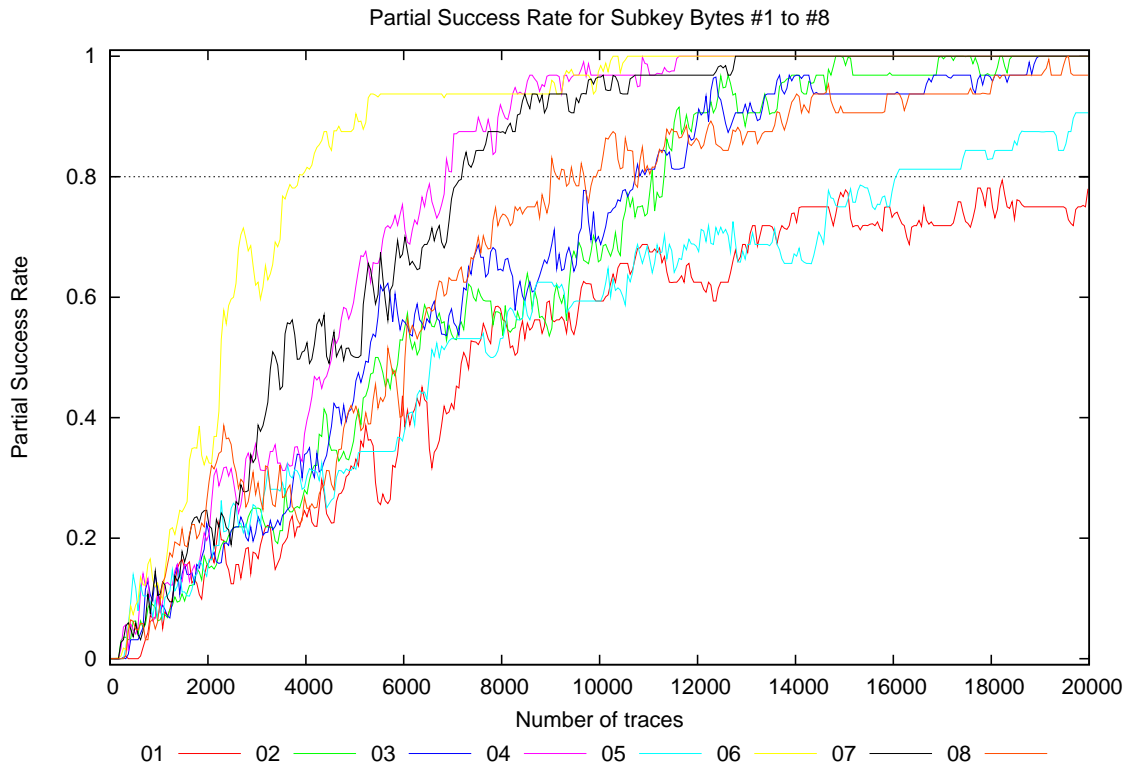




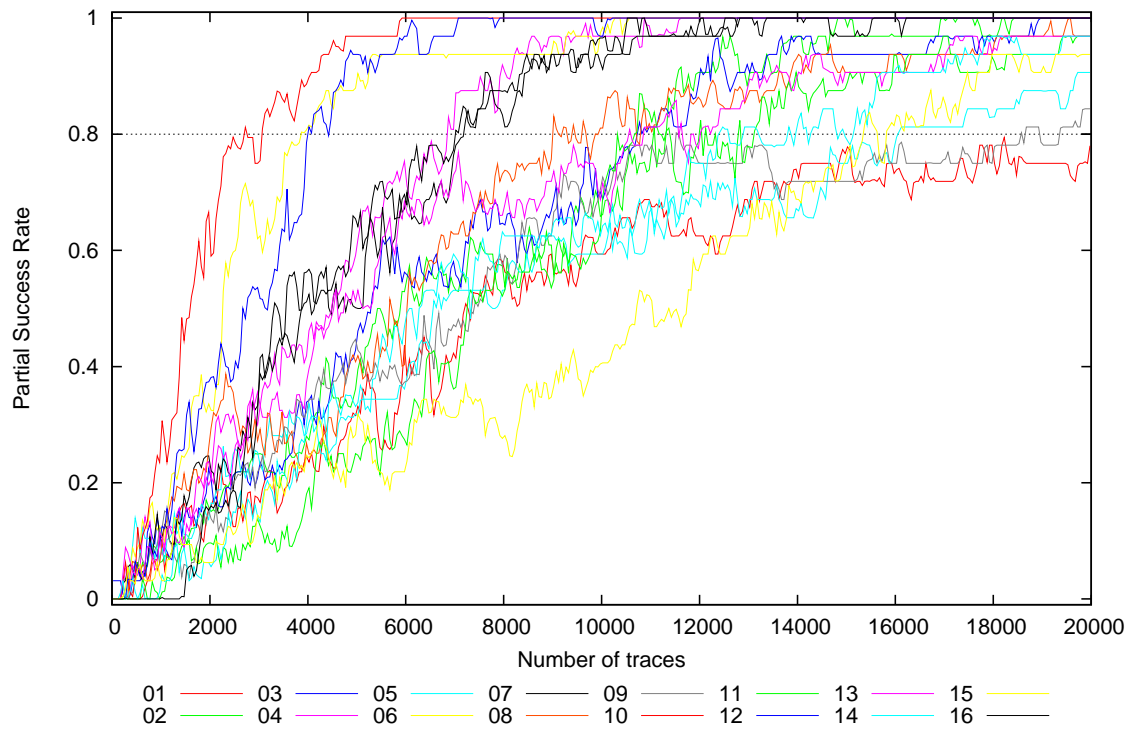






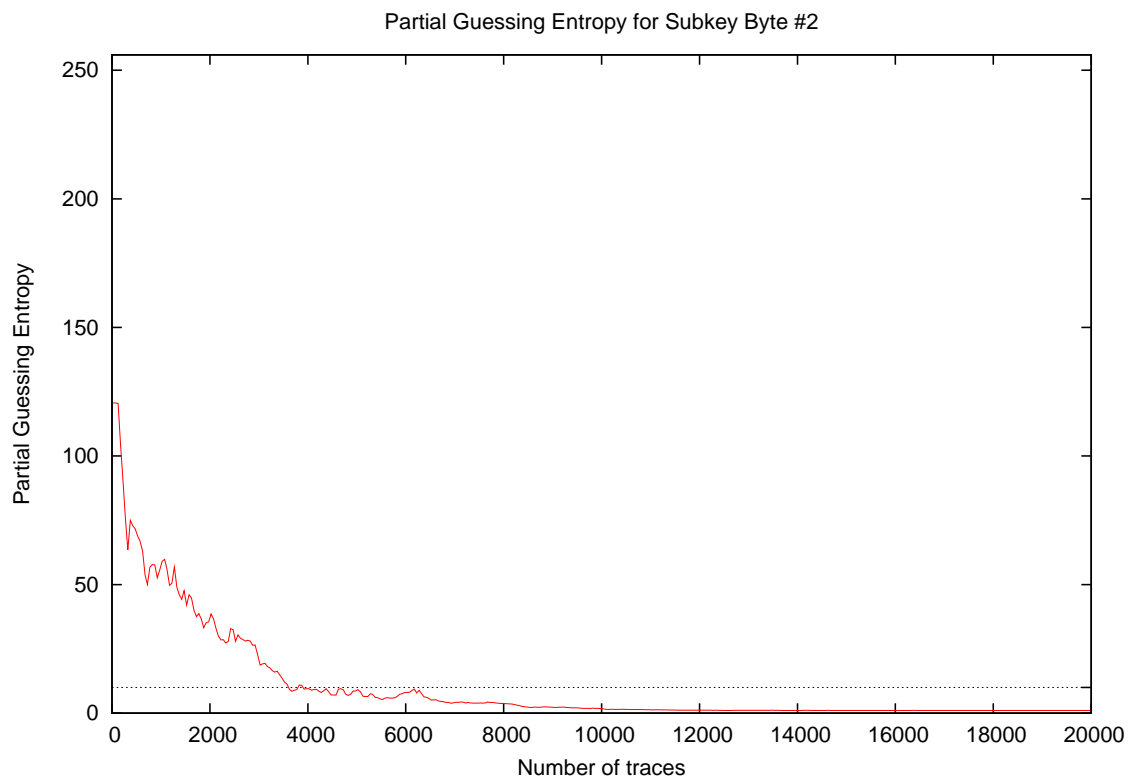
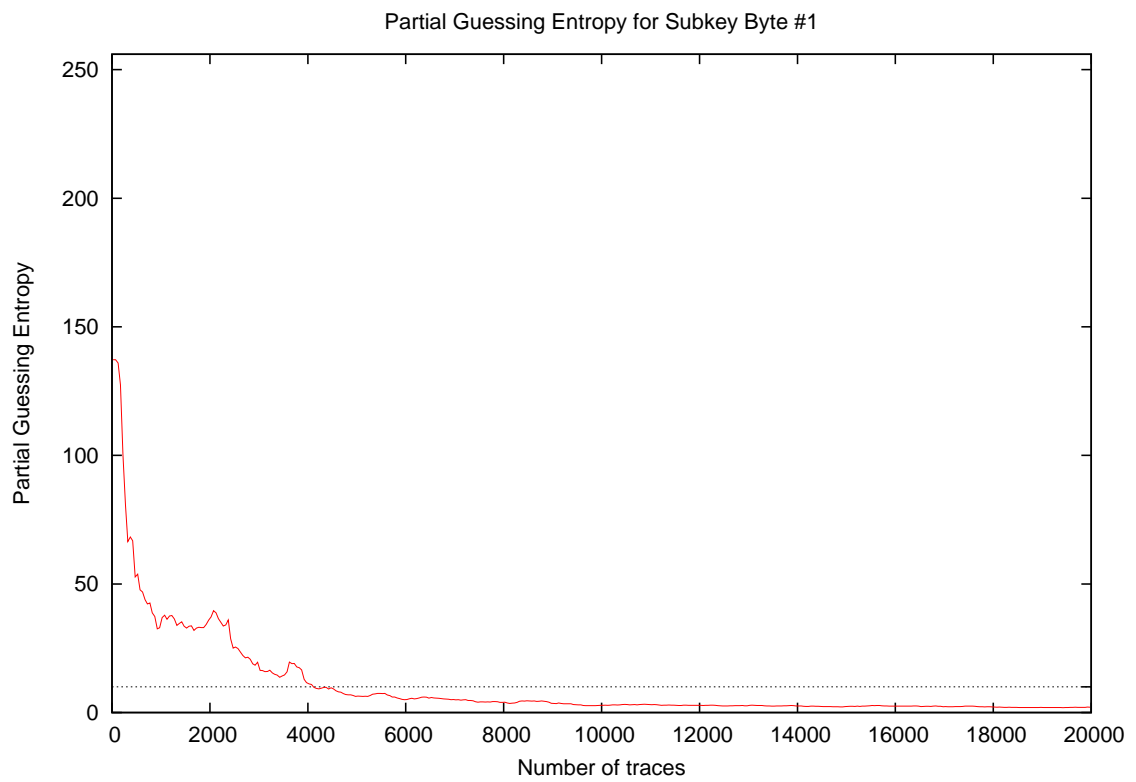


Partial Success Rate for Subkey Bytes #1 to #16

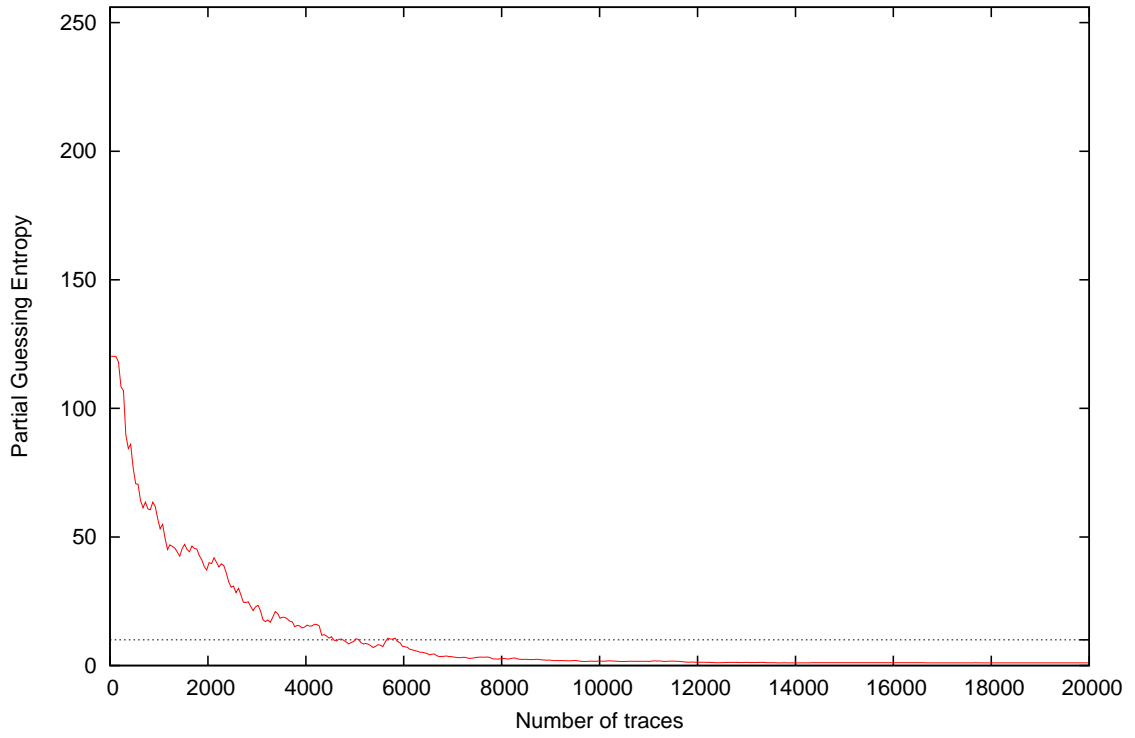


Traces	Partial Success Rate / Byte																Min	Max	Mean
	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16			
10	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.03	0.00	0.00	0.00	0.00	0.00	0.03	0.00
20	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.03	0.00	0.00	0.00	0.00	0.00	0.03	0.00
30	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	0.00	0.00	0.00	0.00	0.03	0.00
40	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	0.00	0.00	0.00	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	0.03	0.00	0.00	0.00	0.00	0.00	0.03	0.00
100	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	0.00	0.00	0.00	0.00	0.03	0.00
200	0.00	0.00	0.00	0.00	0.00	0.03	0.00	0.00	0.00	0.00	0.00	0.03	0.00	0.03	0.00	0.00	0.00	0.03	0.01
300	0.03	0.03	0.00	0.06	0.00	0.00	0.03	0.00	0.00	0.03	0.00	0.00	0.06	0.00	0.03	0.00	0.00	0.06	0.02
400	0.00	0.03	0.03	0.00	0.06	0.06	0.06	0.03	0.00	0.00	0.00	0.03	0.06	0.03	0.03	0.00	0.00	0.06	0.03
500	0.00	0.06	0.03	0.03	0.12	0.06	0.03	0.06	0.03	0.09	0.00	0.09	0.03	0.00	0.03	0.00	0.00	0.12	0.04
1000	0.12	0.06	0.09	0.09	0.09	0.09	0.12	0.06	0.12	0.25	0.00	0.12	0.12	0.03	0.03	0.00	0.00	0.25	0.09
2000	0.16	0.16	0.22	0.19	0.16	0.38	0.25	0.28	0.16	0.66	0.12	0.34	0.22	0.06	0.06	0.16	0.06	0.66	0.22
3000	0.16	0.25	0.19	0.38	0.25	0.62	0.38	0.31	0.22	0.75	0.16	0.56	0.31	0.12	0.12	0.38	0.12	0.75	0.32
4000	0.25	0.25	0.34	0.38	0.28	0.81	0.50	0.25	0.34	0.88	0.22	0.81	0.44	0.31	0.25	0.56	0.22	0.88	0.43
5000	0.34	0.41	0.44	0.62	0.31	0.88	0.53	0.47	0.44	0.97	0.25	0.94	0.53	0.31	0.28	0.66	0.25	0.97	0.52
10000	0.59	0.66	0.69	0.97	0.59	0.97	0.97	0.81	0.69	1.00	0.62	0.97	0.69	0.62	0.41	0.91	0.41	1.00	0.76
15000	0.78	1.00	0.94	1.00	0.75	1.00	1.00	0.91	0.72	1.00	0.88	1.00	0.91	0.81	0.75	0.97	0.72	1.00	0.90
20000	0.78	1.00	1.00	1.00	0.91	1.00	1.00	0.97	0.84	1.00	0.97	1.00	0.97	0.97	0.94	1.00	0.78	1.00	0.96

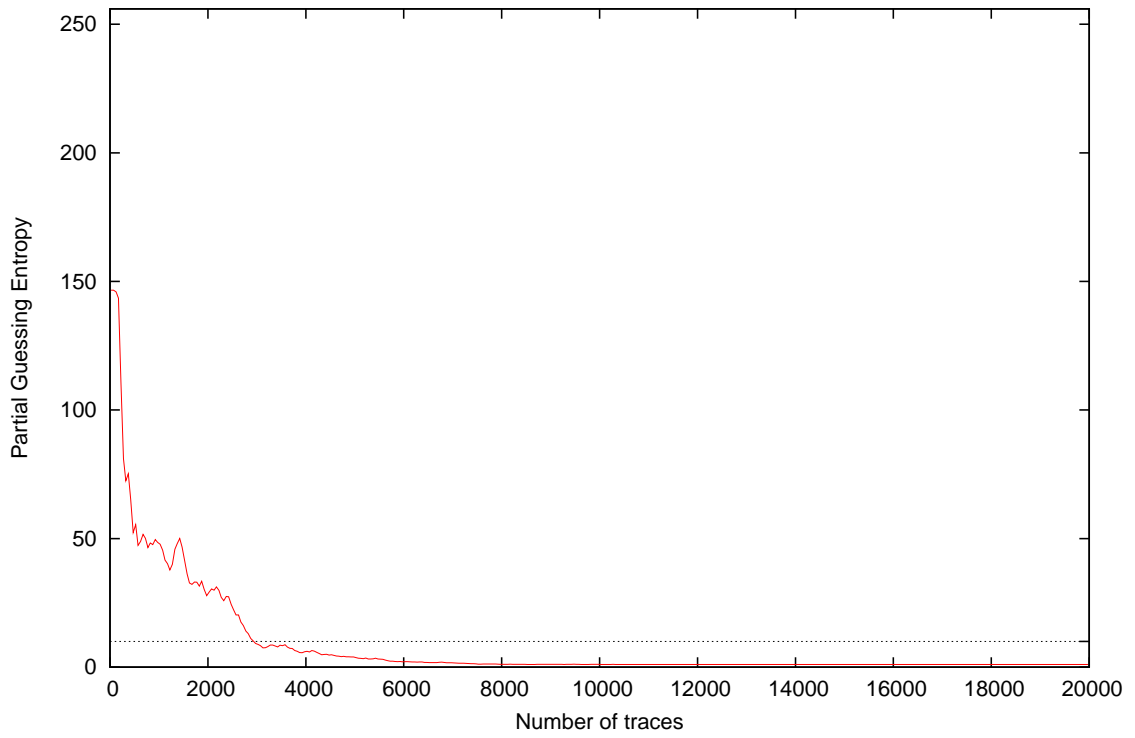
## 4 Partial Guessing Entropy



Partial Guessing Entropy for Subkey Byte #3

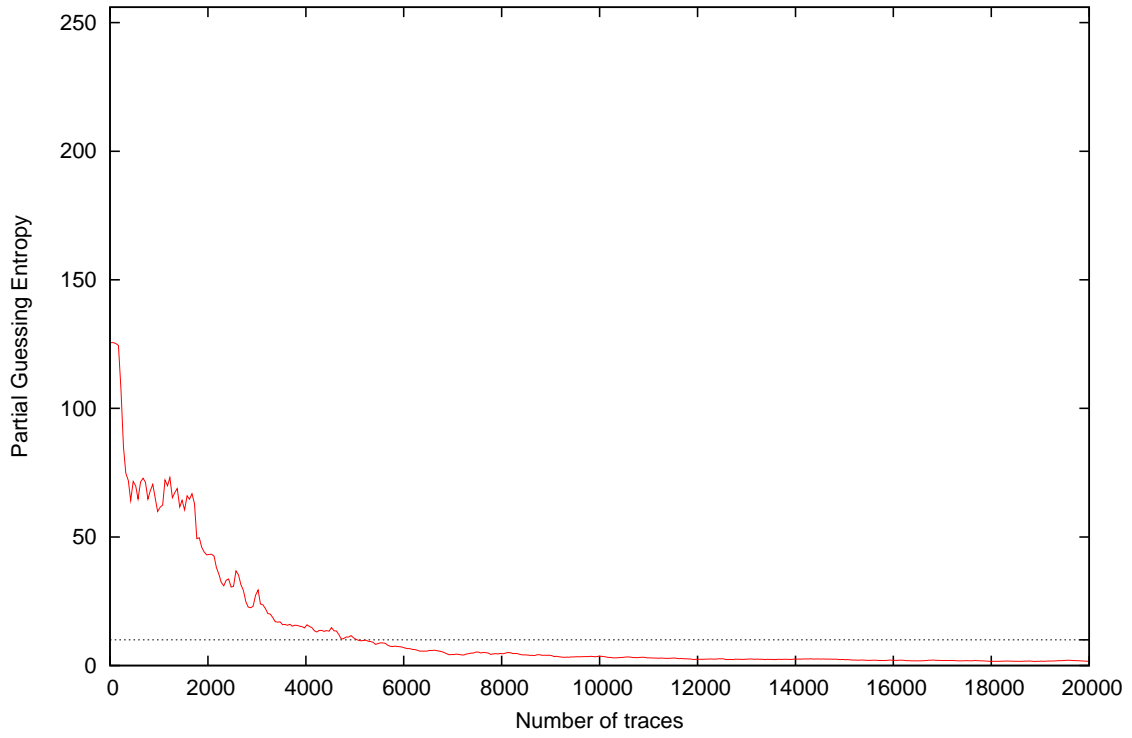


Partial Guessing Entropy for Subkey Byte #4

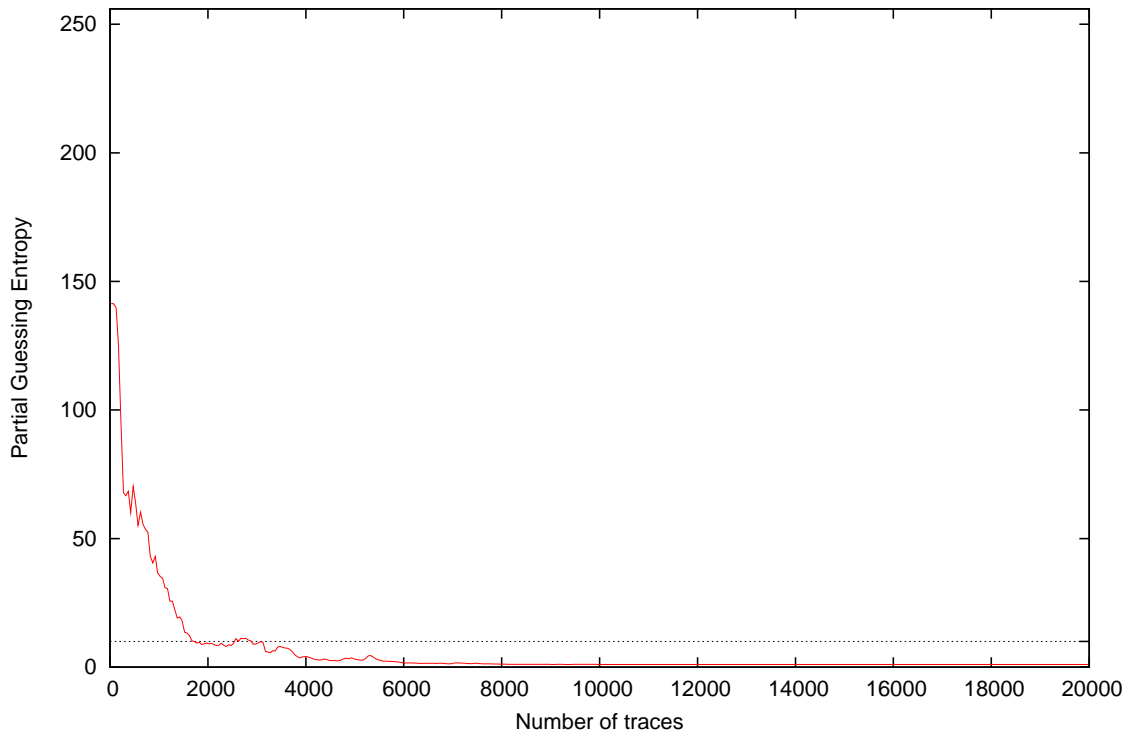




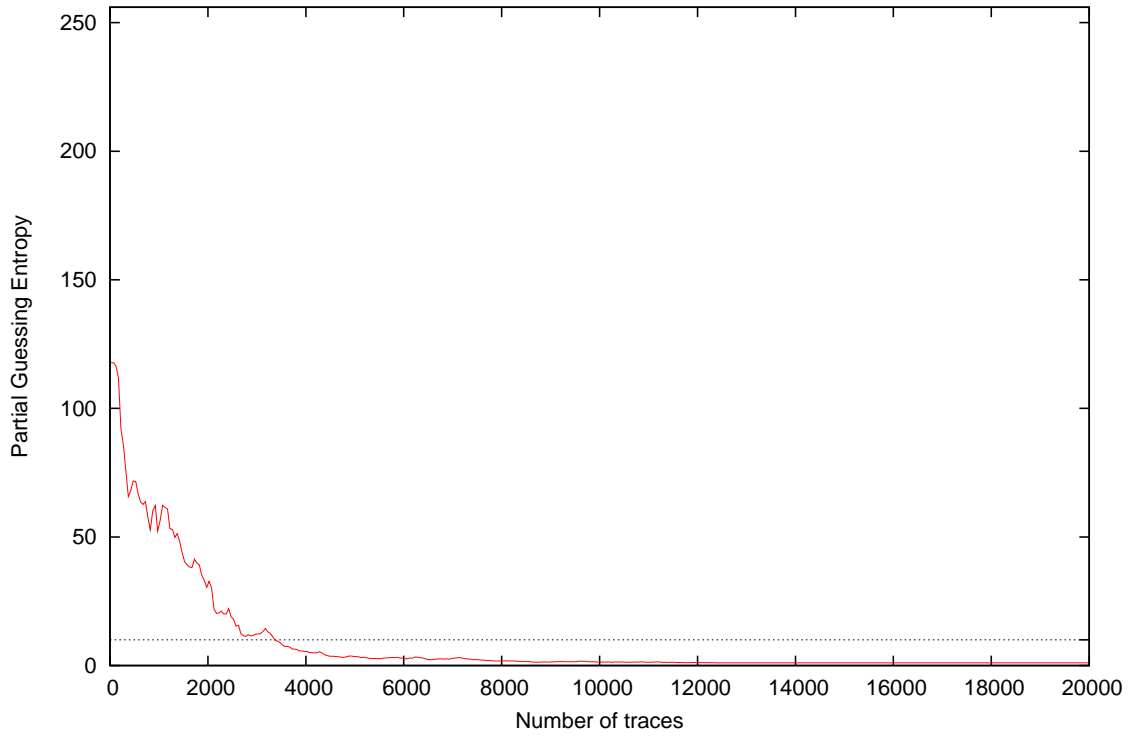
Partial Guessing Entropy for Subkey Byte #5



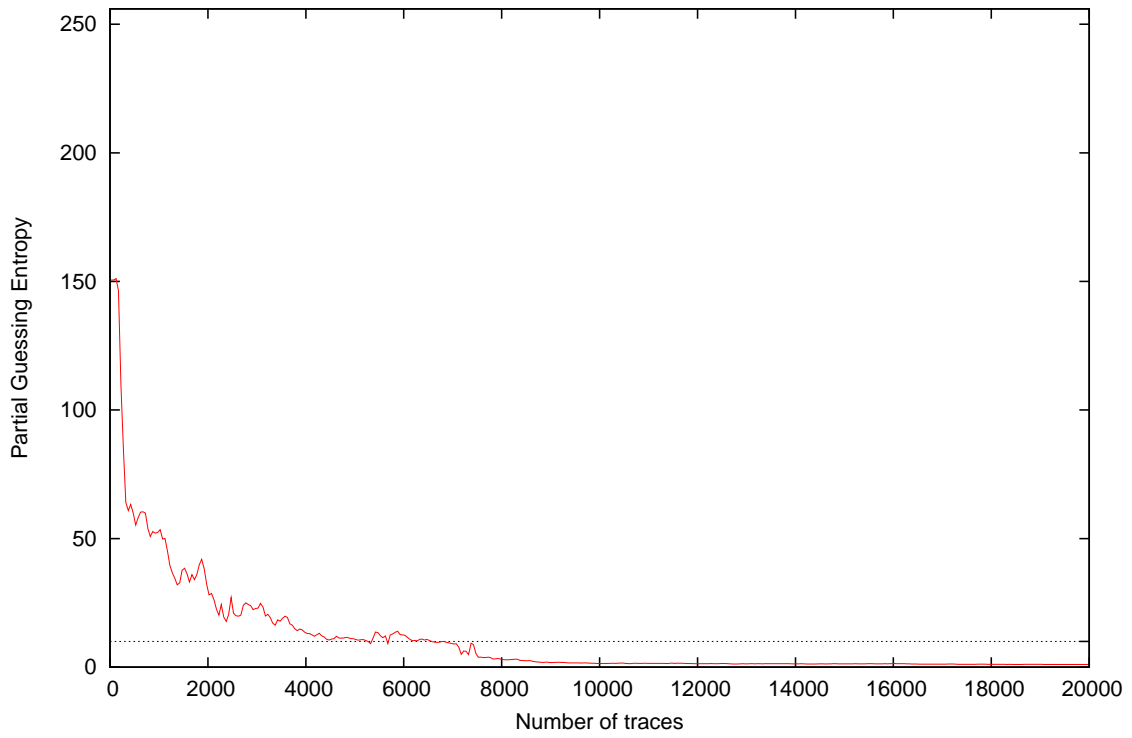
Partial Guessing Entropy for Subkey Byte #6

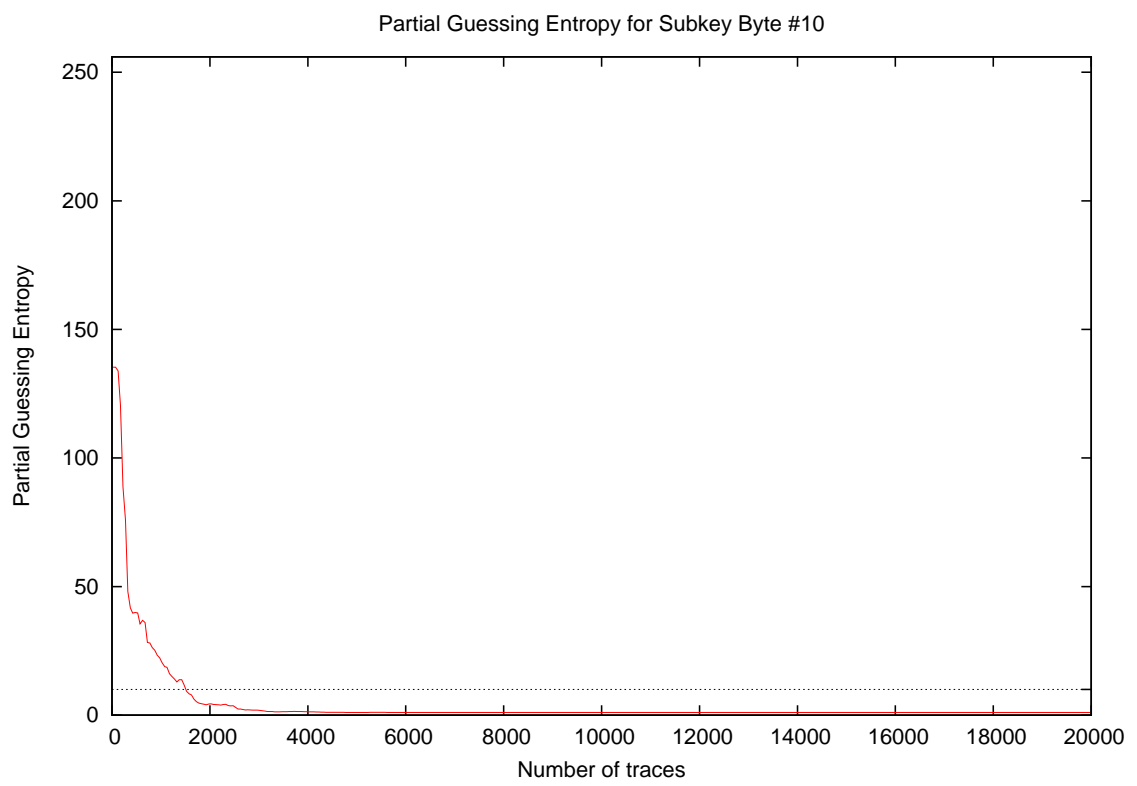
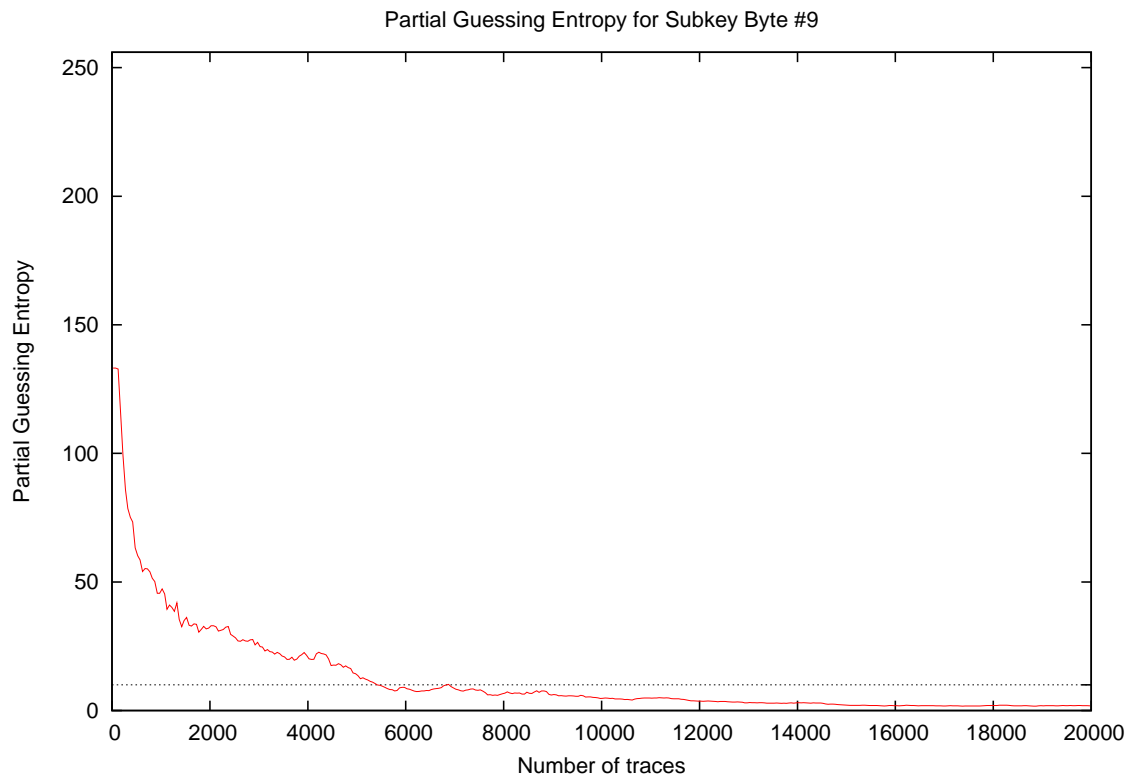


Partial Guessing Entropy for Subkey Byte #7

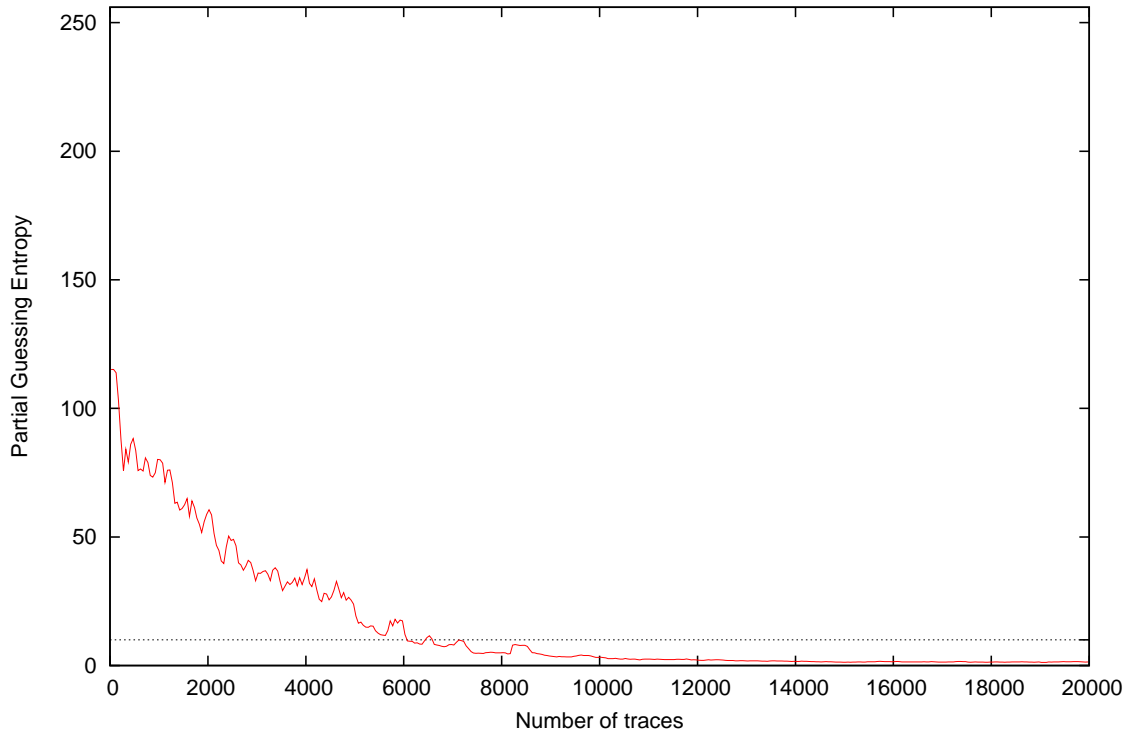


Partial Guessing Entropy for Subkey Byte #8

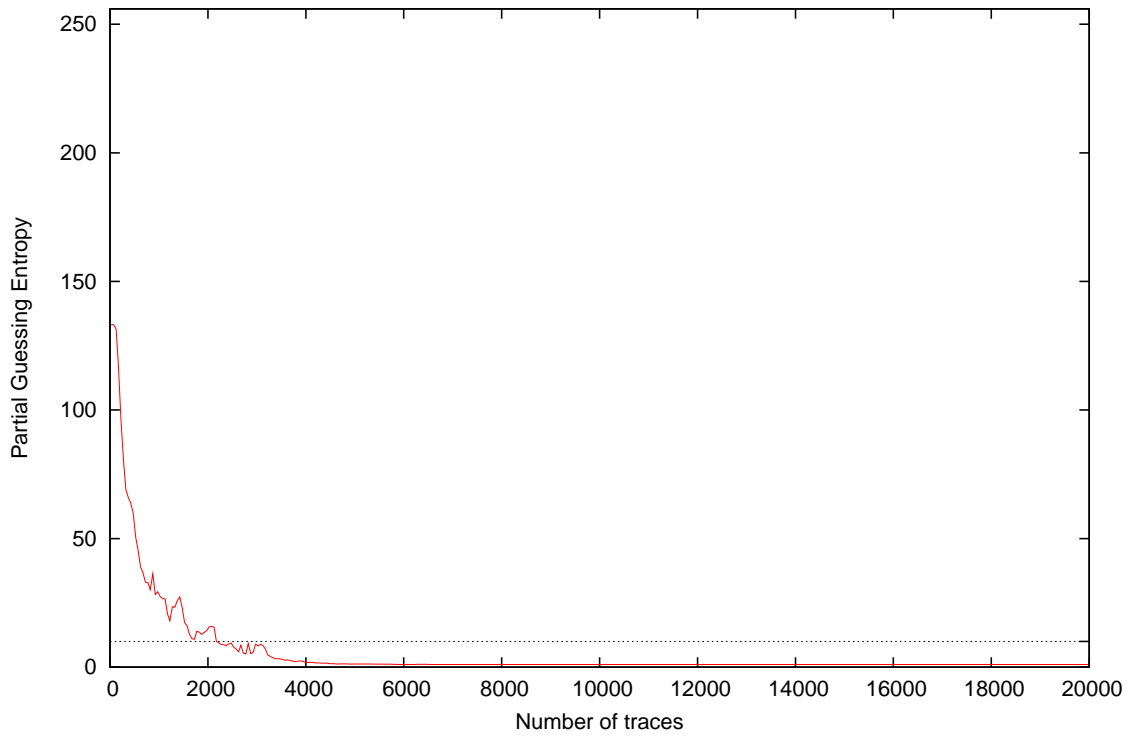




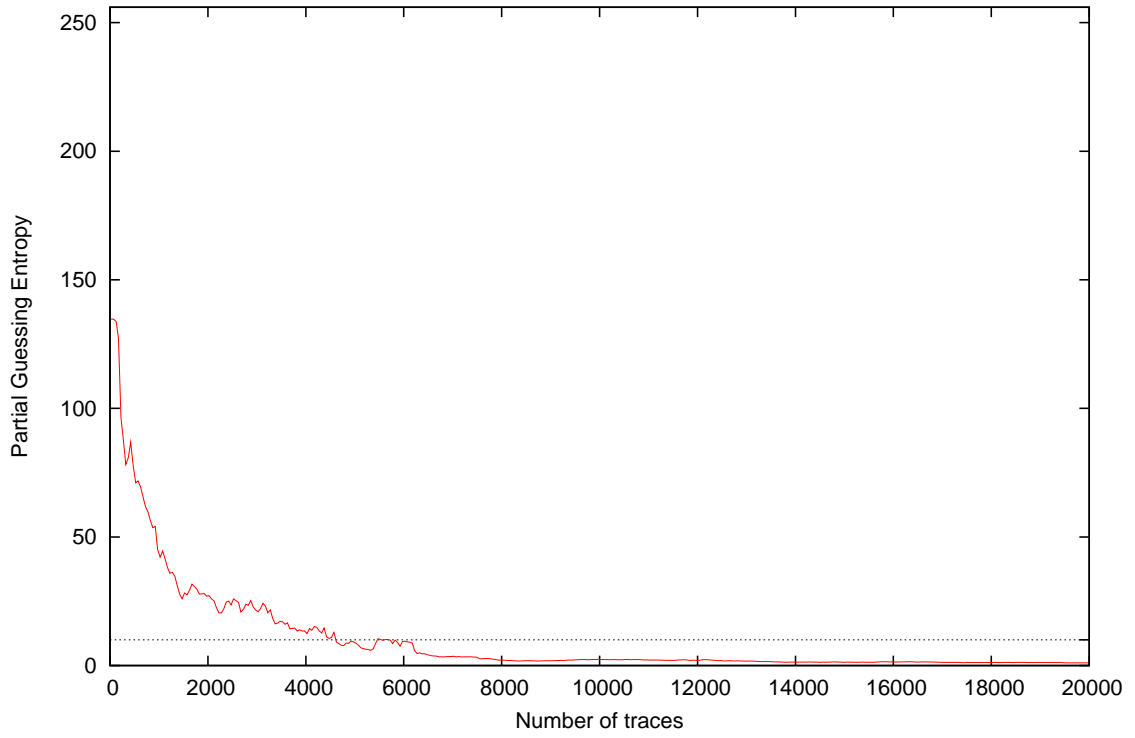
Partial Guessing Entropy for Subkey Byte #11



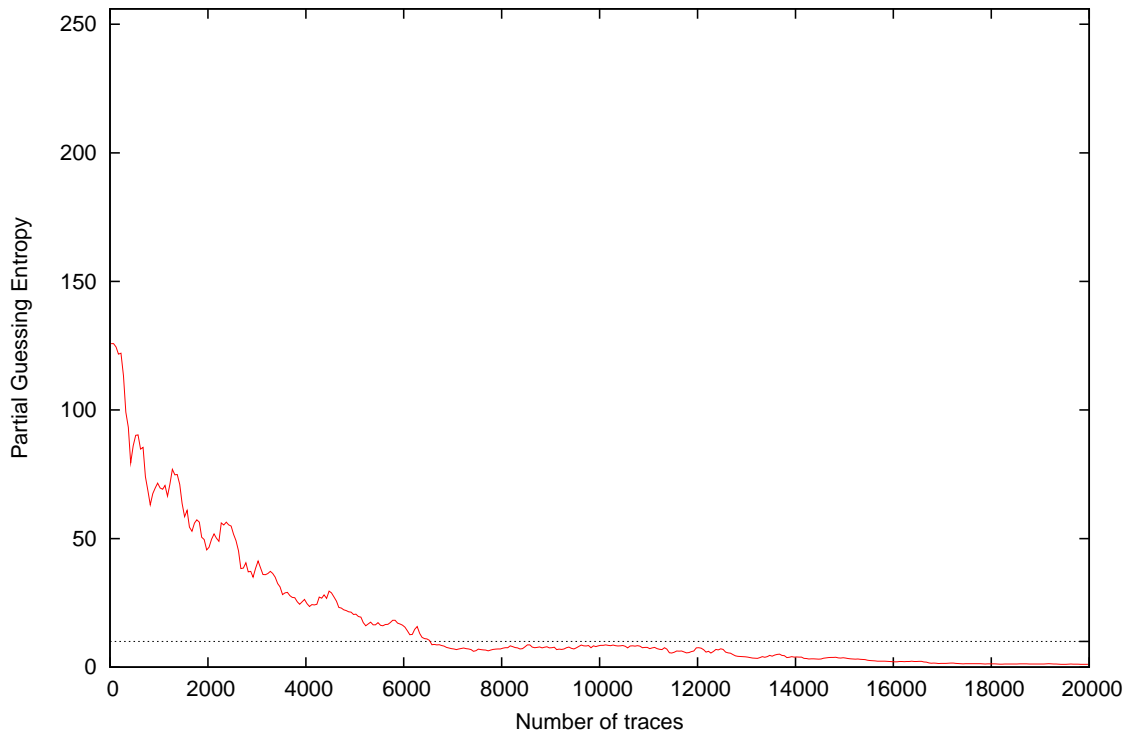
Partial Guessing Entropy for Subkey Byte #12



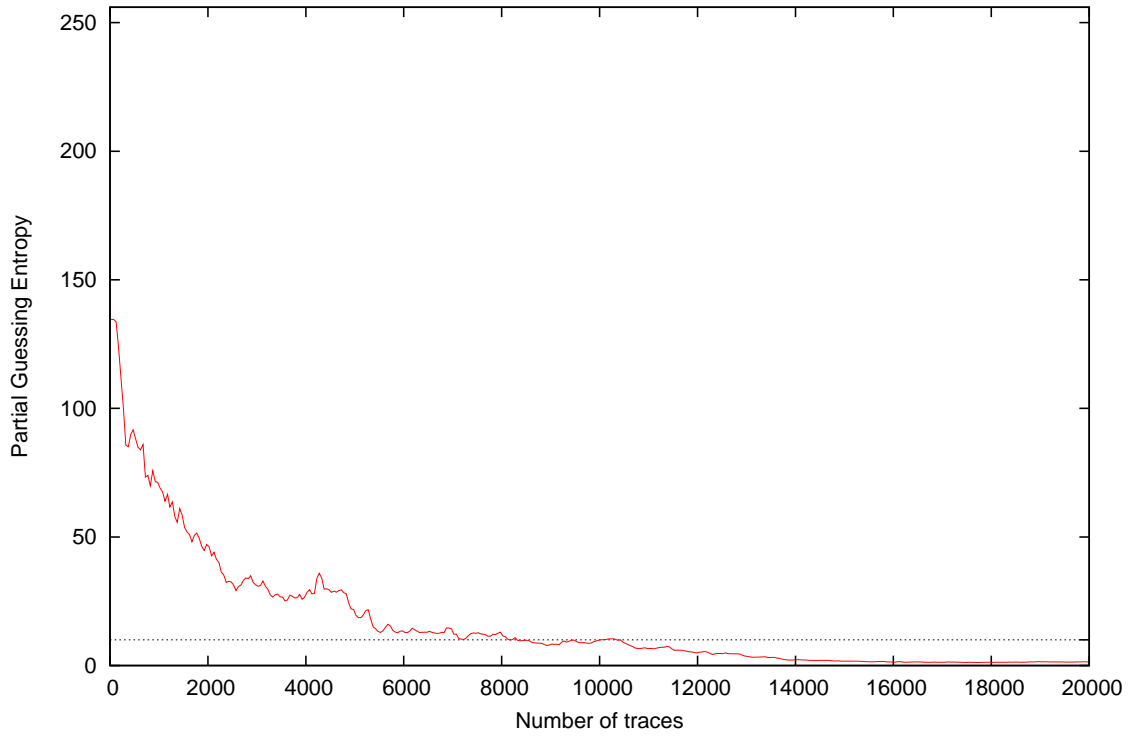
Partial Guessing Entropy for Subkey Byte #13



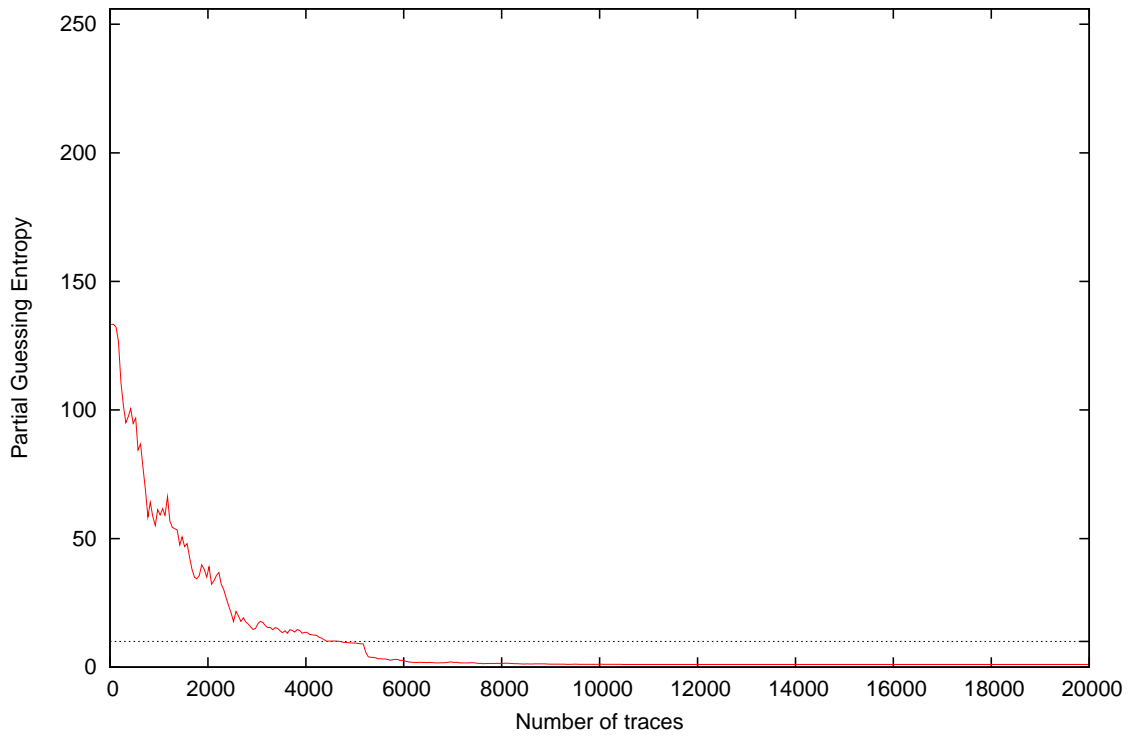
Partial Guessing Entropy for Subkey Byte #14



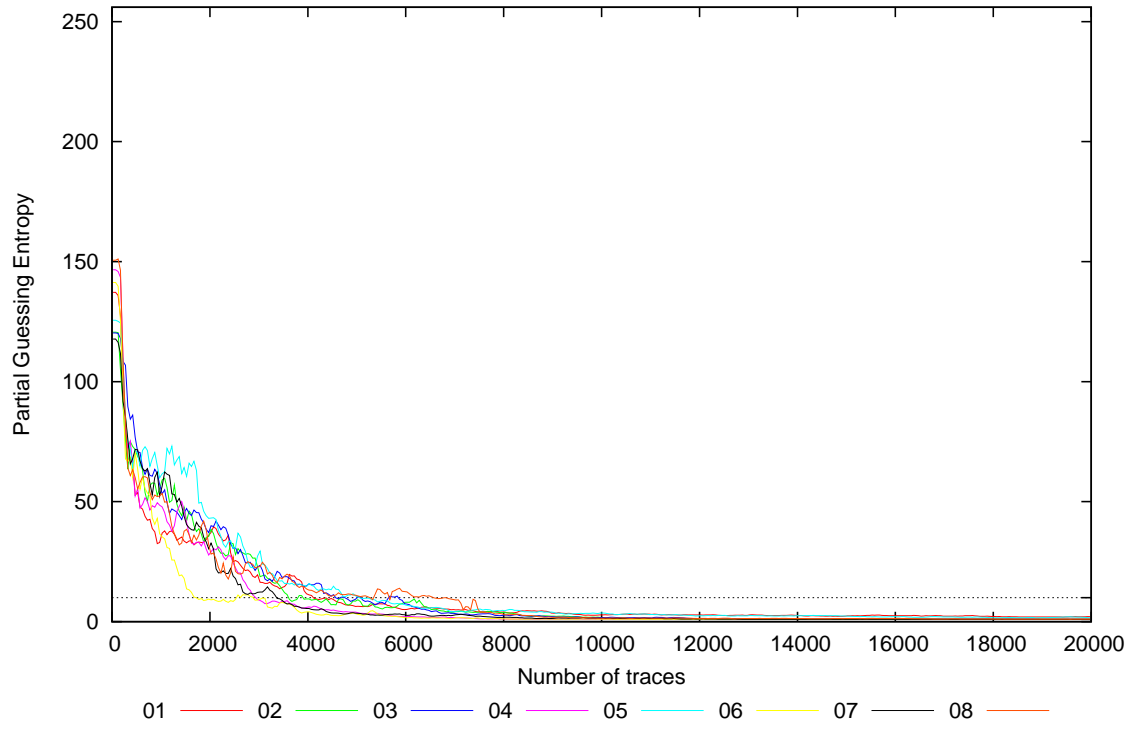
Partial Guessing Entropy for Subkey Byte #15



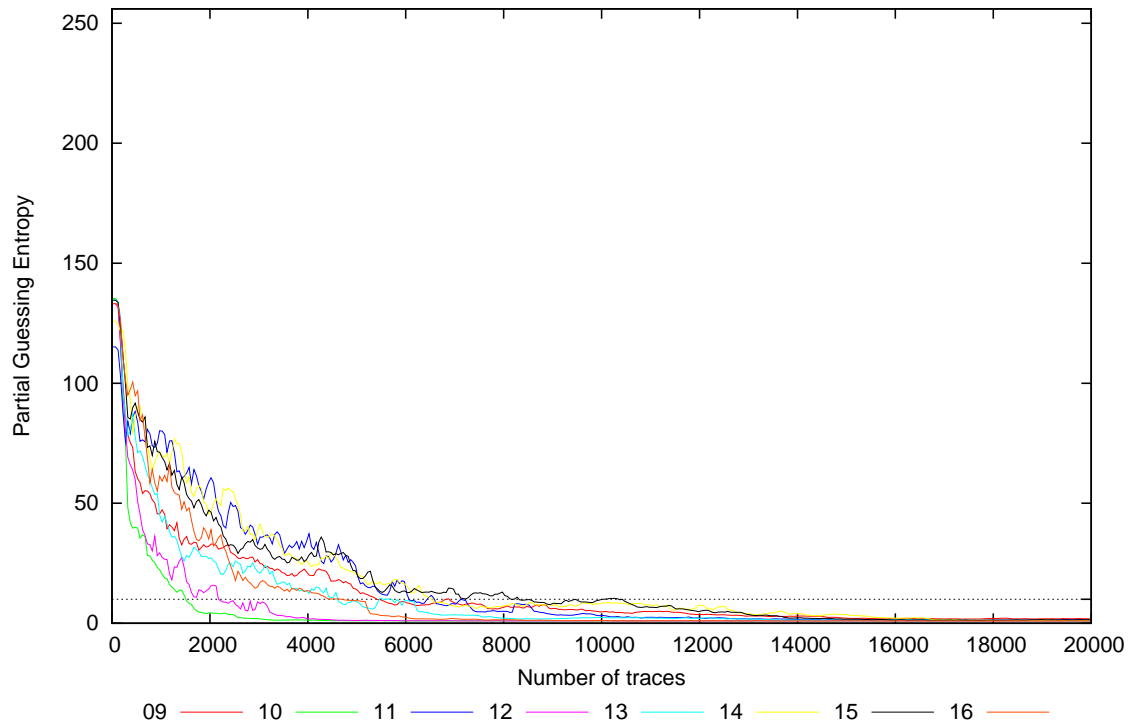
Partial Guessing Entropy for Subkey Byte #16



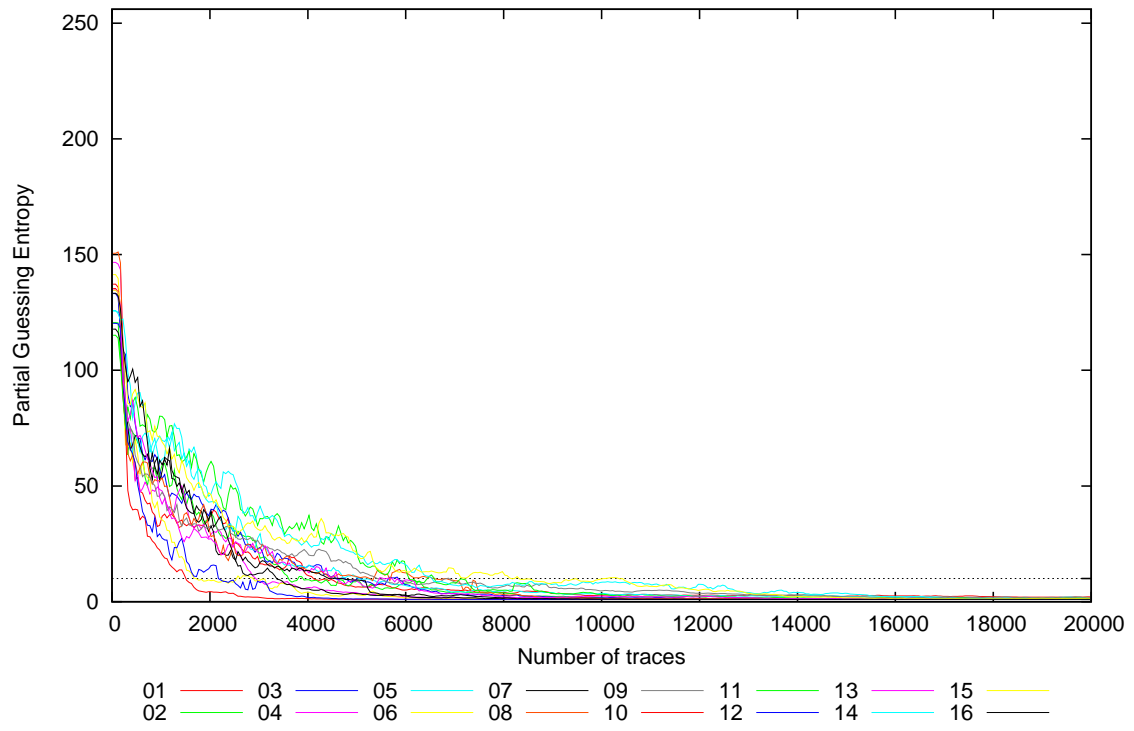
Partial Guessing Entropy for Subkey Bytes #1 to #8



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	137.2	120.6	120.3	146.6	125.6	141.3	117.8	150.6	133.2	135.3	115.2	133.2	134.7	125.8	134.6	133.3	115.2	150.6	131.6
20	137.2	120.6	120.3	146.6	125.6	141.3	117.8	150.6	133.2	135.3	115.2	133.2	134.7	125.8	134.6	133.3	115.2	150.6	131.6
30	137.2	120.6	120.3	146.6	125.6	141.3	117.8	150.6	133.2	135.3	115.2	133.2	134.7	125.8	134.6	133.3	115.2	150.6	131.6
40	137.2	120.6	120.3	146.6	125.6	141.3	117.8	150.6	133.2	135.3	115.2	133.2	134.7	125.8	134.6	133.3	115.2	150.6	131.6
50	137.2	120.6	120.3	146.6	125.6	141.3	117.8	150.6	133.2	135.3	115.2	133.2	134.7	125.8	134.6	133.3	115.2	150.6	131.6
100	137.2	120.6	120.3	146.6	125.6	141.3	117.8	150.6	133.2	135.3	115.2	133.2	134.7	125.8	134.6	133.3	115.2	150.6	131.6
200	120.1	96.0	111.7	135.0	120.0	107.8	112.1	137.4	100.1	116.8	94.8	108.3	112.7	123.9	113.3	127.7	94.8	137.4	114.9
300	72.8	69.5	101.7	80.6	83.2	62.7	76.3	67.5	82.2	67.9	71.3	72.3	83.6	103.1	96.1	91.4	62.7	103.1	80.1
400	69.0	73.8	94.1	78.9	72.3	60.8	63.2	60.7	74.0	43.7	91.5	61.6	86.1	84.1	87.2	94.3	43.7	94.3	74.7
500	49.1	70.2	73.6	58.6	70.0	71.5	67.9	57.8	53.8	39.0	91.9	51.9	73.8	89.6	94.8	96.8	39.0	96.8	69.4
1000	33.5	55.1	54.4	48.8	62.8	36.3	46.7	49.3	47.1	22.9	79.9	26.5	41.6	73.2	66.0	60.8	22.9	79.9	50.3
2000	36.3	34.5	36.6	28.9	45.8	9.3	31.8	29.8	32.8	4.3	61.4	15.3	29.8	45.0	49.3	40.7	4.3	61.4	33.2
3000	17.1	18.8	23.9	9.1	29.6	8.6	12.5	21.9	26.2	1.9	32.8	8.8	17.5	43.2	32.4	16.7	1.9	43.2	20.1
4000	11.3	9.8	16.0	6.1	15.6	3.8	5.5	13.3	21.8	1.3	36.8	1.8	14.6	24.9	25.4	13.5	1.3	36.8	13.9
5000	6.2	9.1	9.6	3.8	10.5	3.2	3.4	10.9	14.1	1.0	24.9	1.2	9.0	20.7	21.7	9.3	1.0	24.9	9.9
10000	2.7	1.8	1.7	1.1	3.6	1.0	1.3	1.4	4.6	1.0	3.3	1.0	2.5	8.3	10.0	1.1	1.0	10.0	2.9
15000	2.4	1.0	1.1	1.0	2.3	1.0	1.0	1.3	2.2	1.0	1.3	1.0	1.3	3.5	1.7	1.0	1.0	3.5	1.5
20000	2.1	1.0	1.0	1.0	1.5	1.0	1.0	1.0	1.8	1.0	1.4	1.0	1.0	1.1	1.3	1.0	1.0	2.1	1.2