Problem 3

Power traces, ARIA-128

2020. 06. 13.

2019330017 백승윤

분석 방법

- Samples : 97000 - 100000
- CPA - 1byte guessing

Algorithm 1 Unprotected ARIA-128 used for the problem 1

Input: Plaintext X, seen as 16 bytes X_i, $i \in [\![0, 15]\!]$,
Key schedule, 13 × 128-bit constants RoundKey$[r]$, $r \in [\![0, 12]\!]$
Output: Ciphertext X, seen as bytes X_i, $i \in [\![0, 15]\!]$

1: **for** $i \in [\![0, 15]\!]$ **do**
2: $X_i \leftarrow X_i \oplus$ RoundKey$[1]_i$
3: **end for**
4: **for** $r \in [\![1, 11]\!]$ **do**
5: $X \leftarrow$ **SubstLayer**(X)
6: $X \leftarrow$ **DiffLayer**(X) ← Hamming Weight
7: **for** $i \in [\![0, 15]\!]$ **do**
8: $X_i \leftarrow X_i \oplus$ RoundKey$[r]_i$
9: **end for**
10: **end for**
11: $X \leftarrow$ **SubstLayer**(X)
12: **for** $i \in [\![0, 15]\!]$ **do**
13: $X_i \leftarrow X_i \oplus$ RoundKey$[12]_i$
14: **end for**
15: **return** X

분석 방법

- 1. plaintext 별로 Trace를 나눠주기 (analyze_trace.c)
- 2. Single trace 분석하여 sample 어디서부터 어디까지 볼 지 확인하기
- 3. Hamming weight 계산하여 Max 값을 가지는 key가 real key (solve.cpp)

분석 결과

분석된 암호화 키

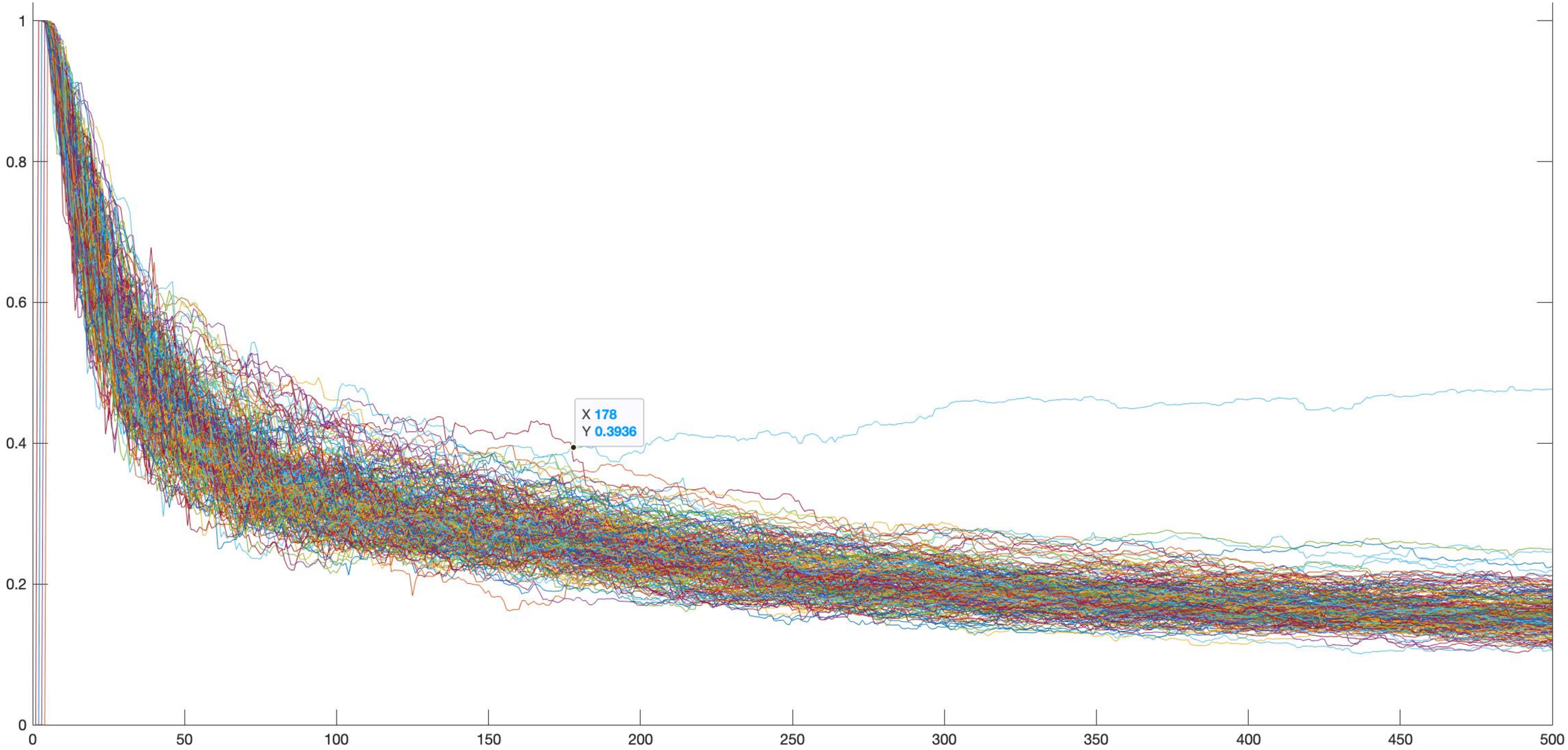
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
key	7F	0A	4a	06	98	52	2A	1B	64	E2	D3	DC	C0	52	7D	50

최소 분석 파형수

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
최소 분석 파형수	178	53	100	167	128	149	58	131	82	159	53	51	52	191	189	154

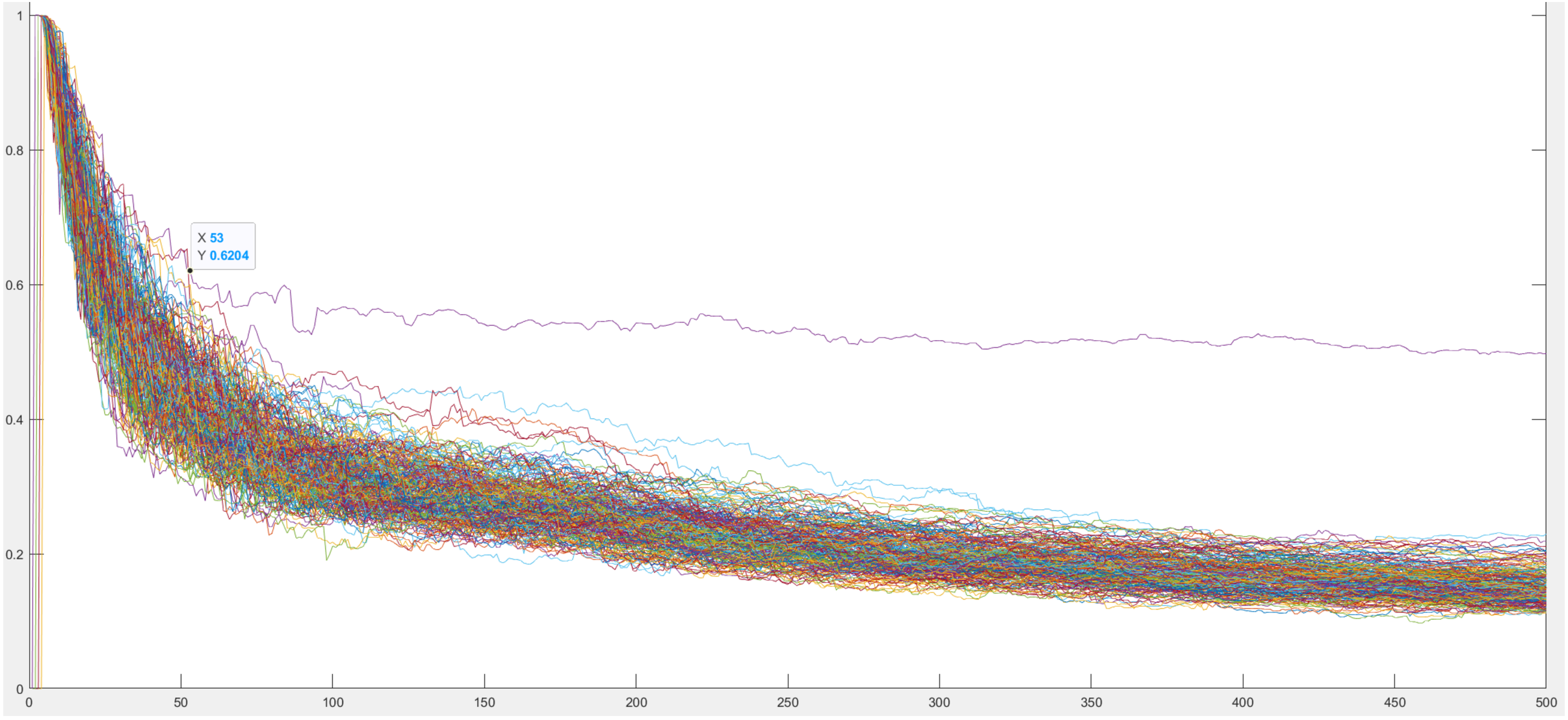
분석 결과

1st S-box output



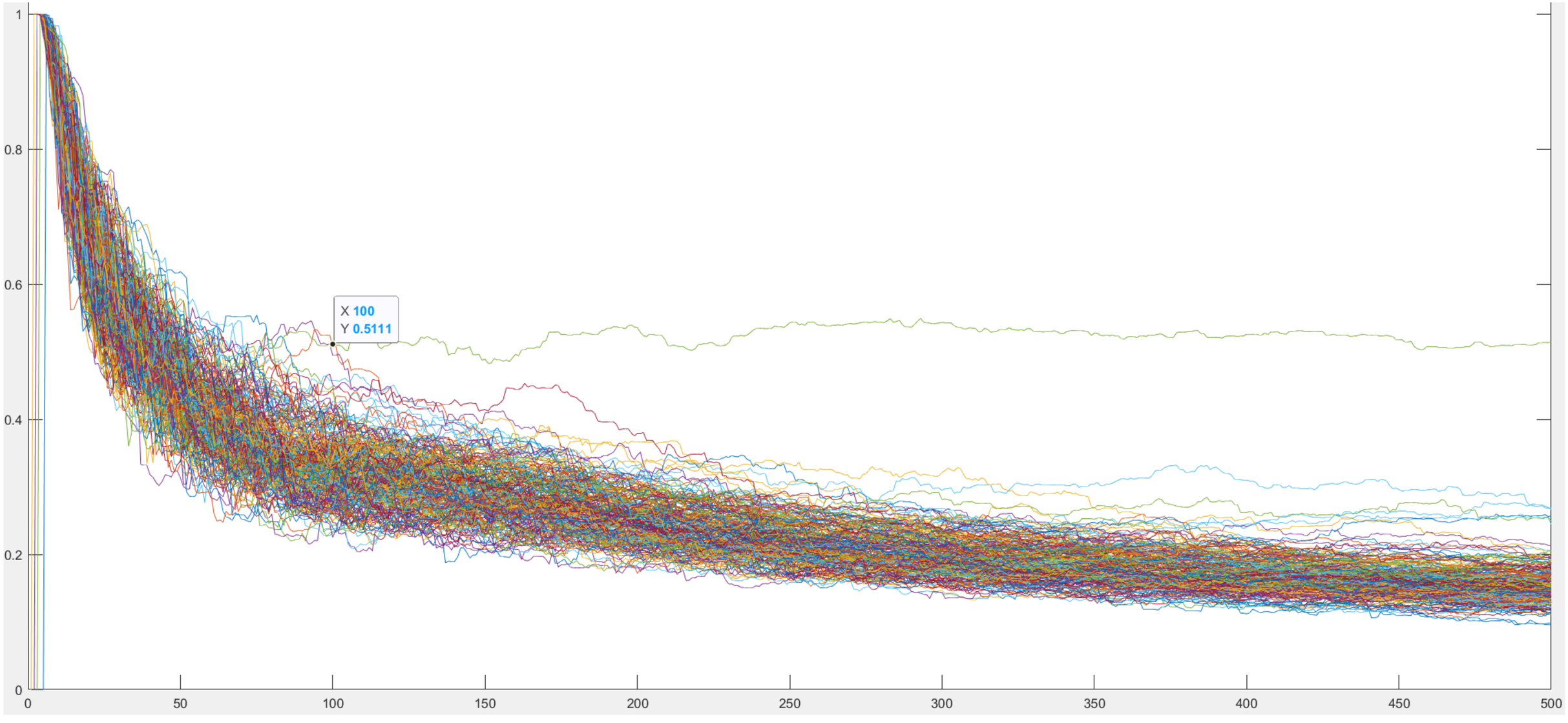
분석 결과

2nd S-box output



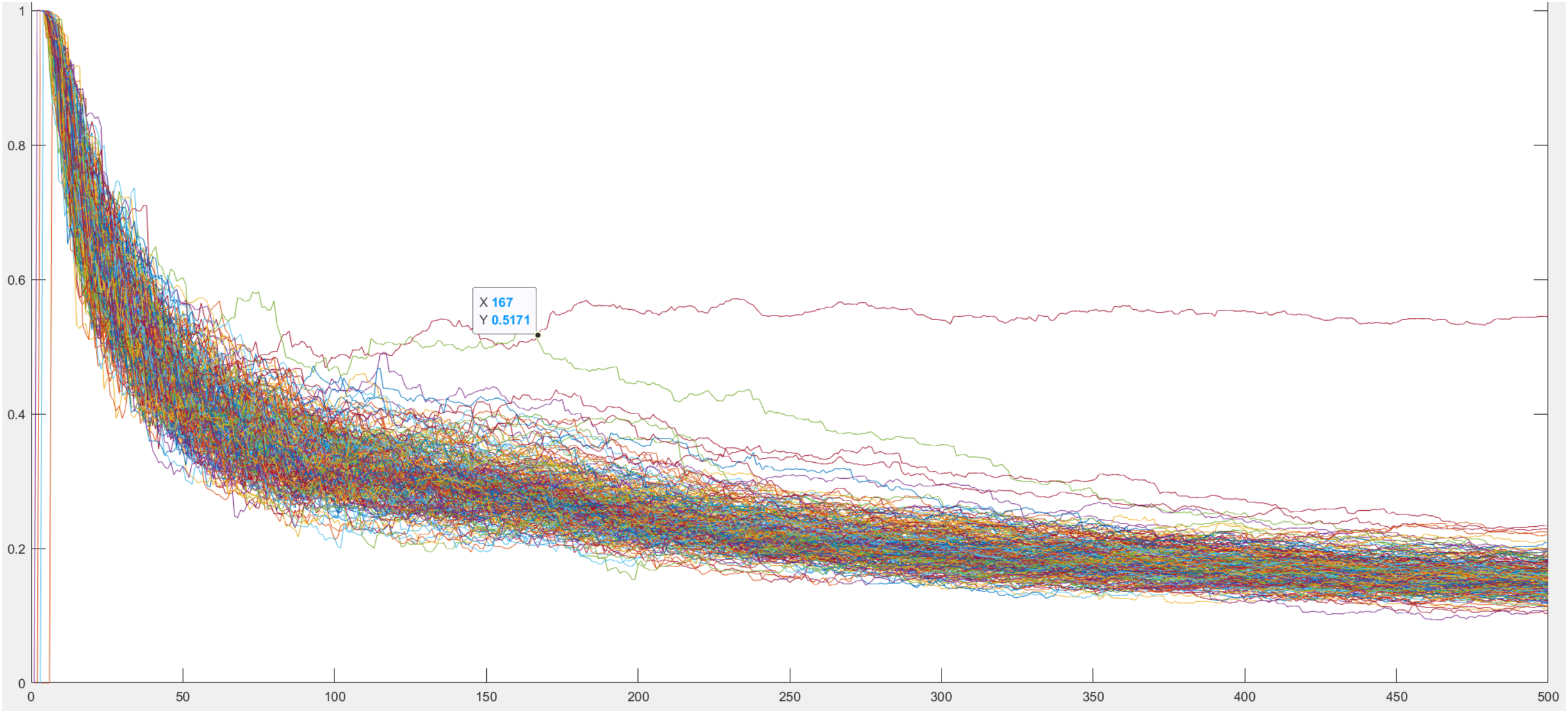
분석 결과

3rd S-box output



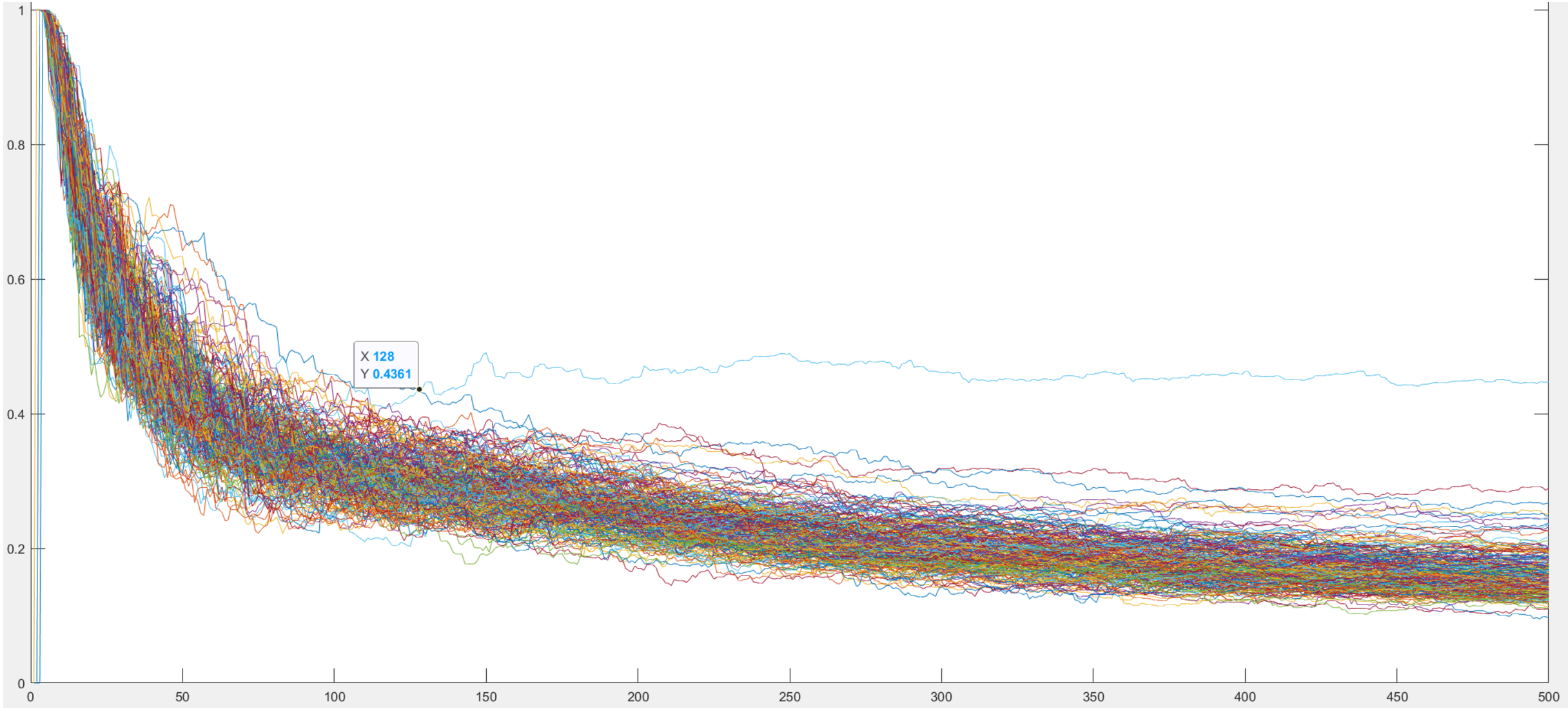
분석 결과

4th S-box output



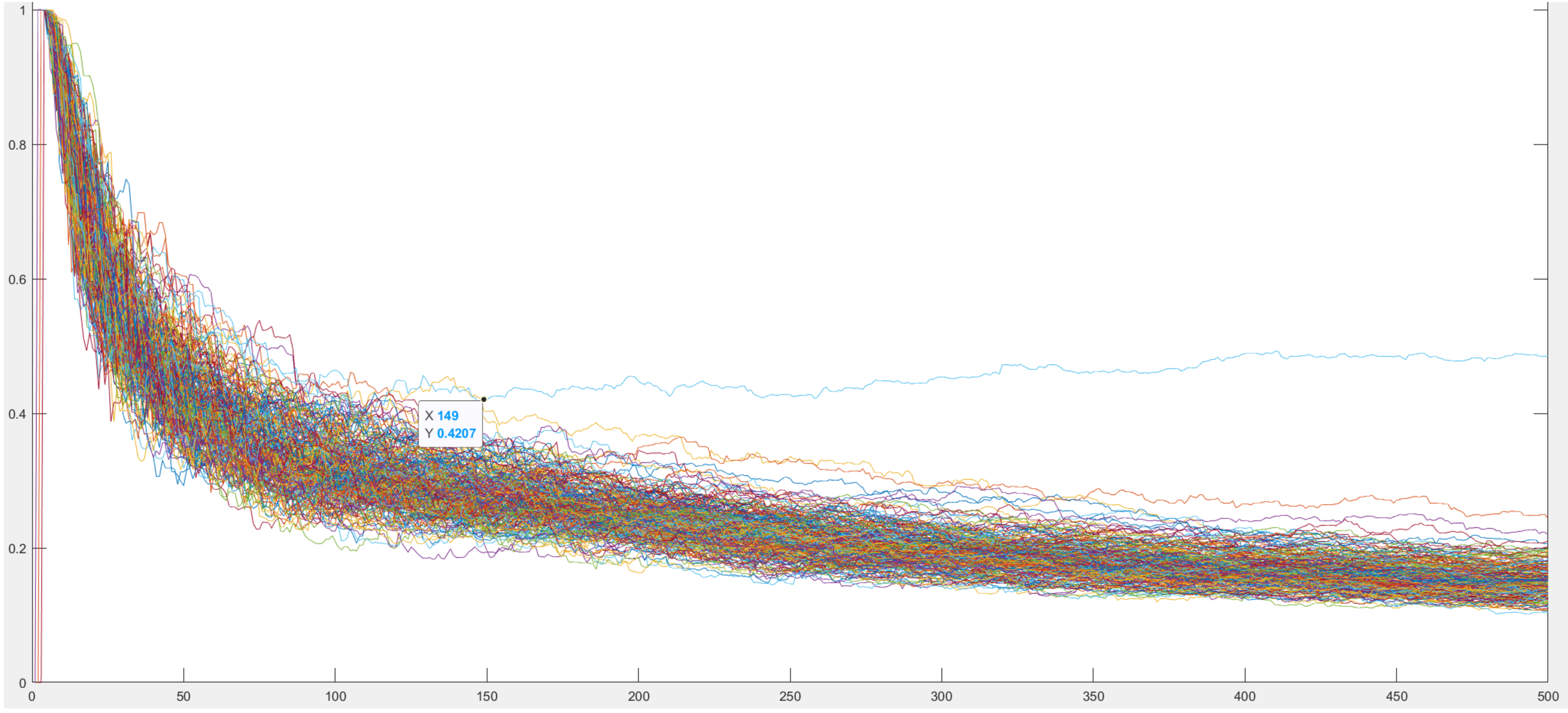
분석 결과

5th S-box output



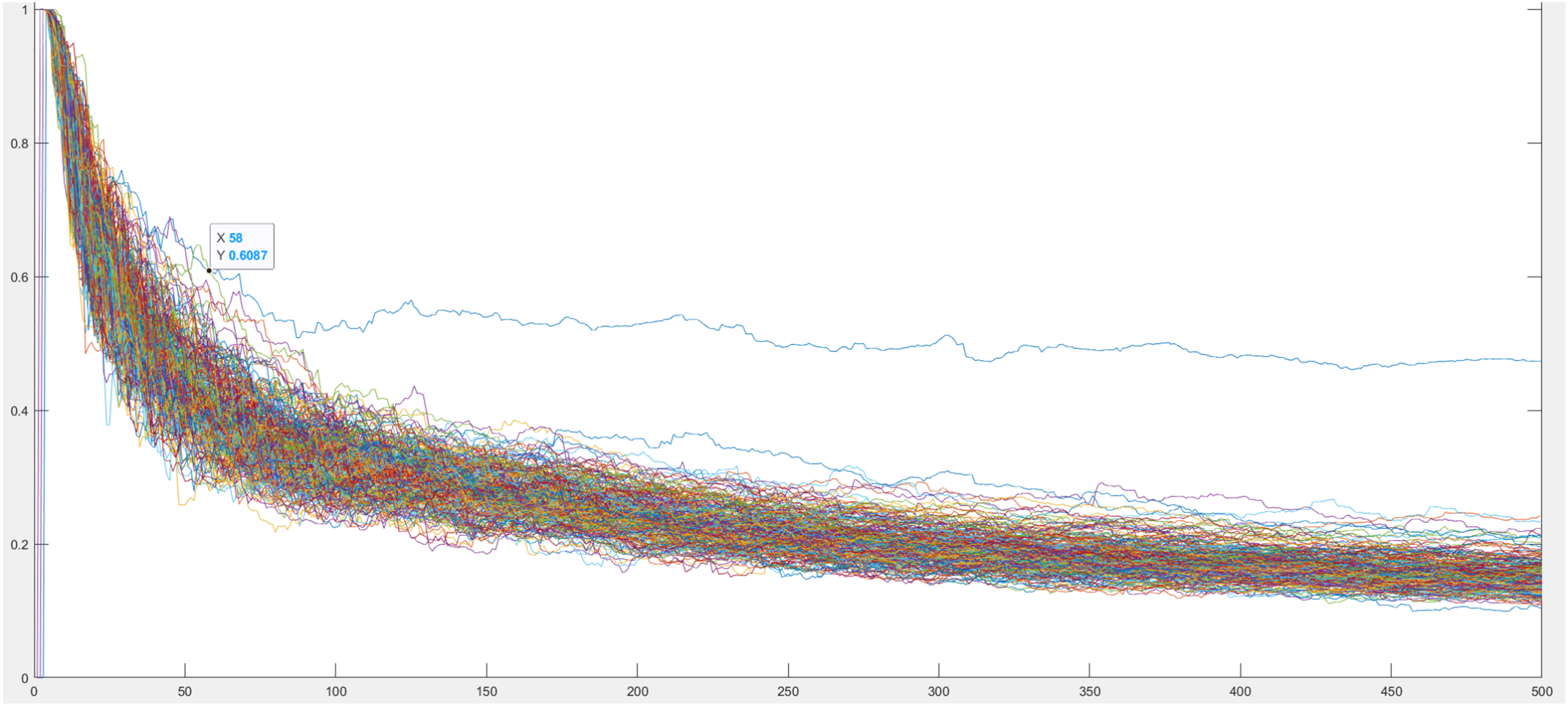
분석 결과

6th S-box output



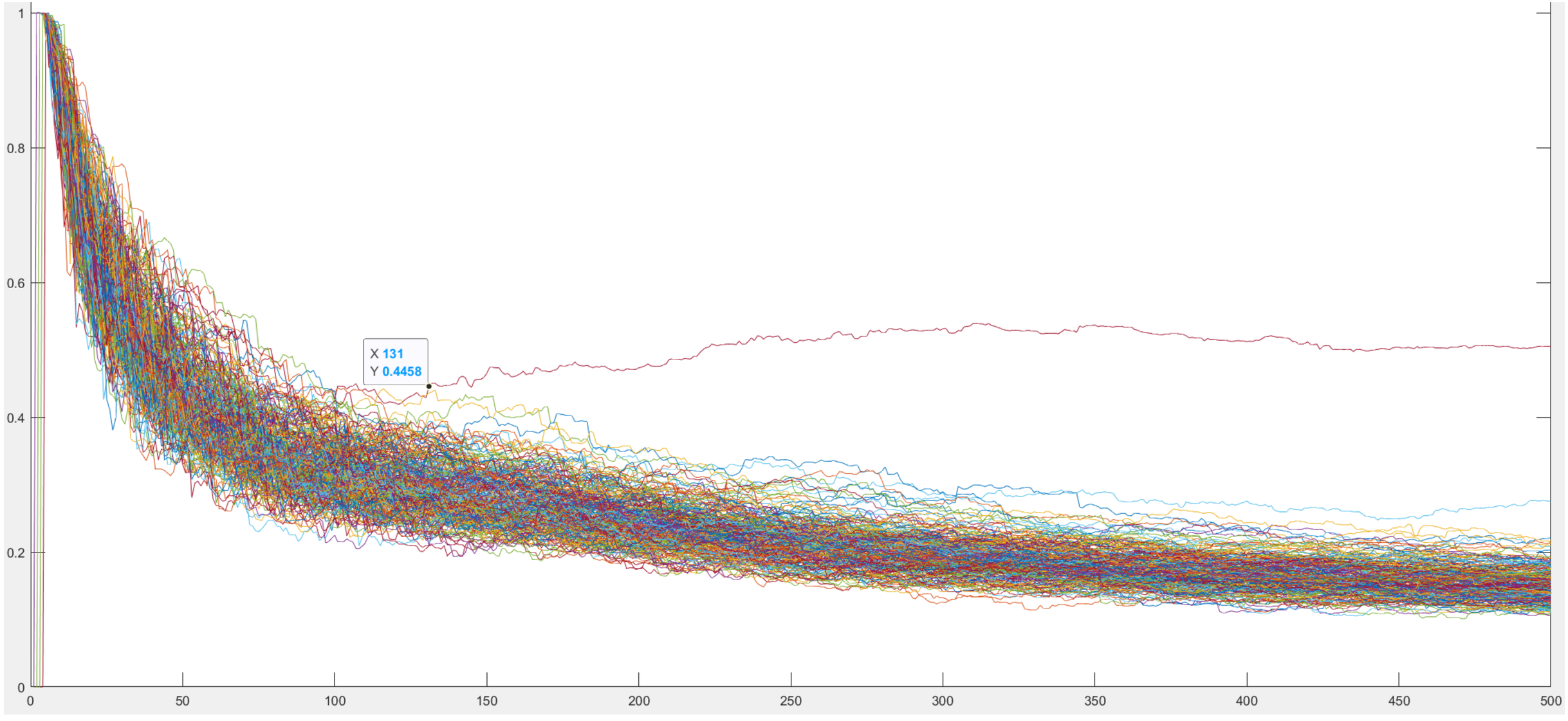
분석 결과

7th S-box output



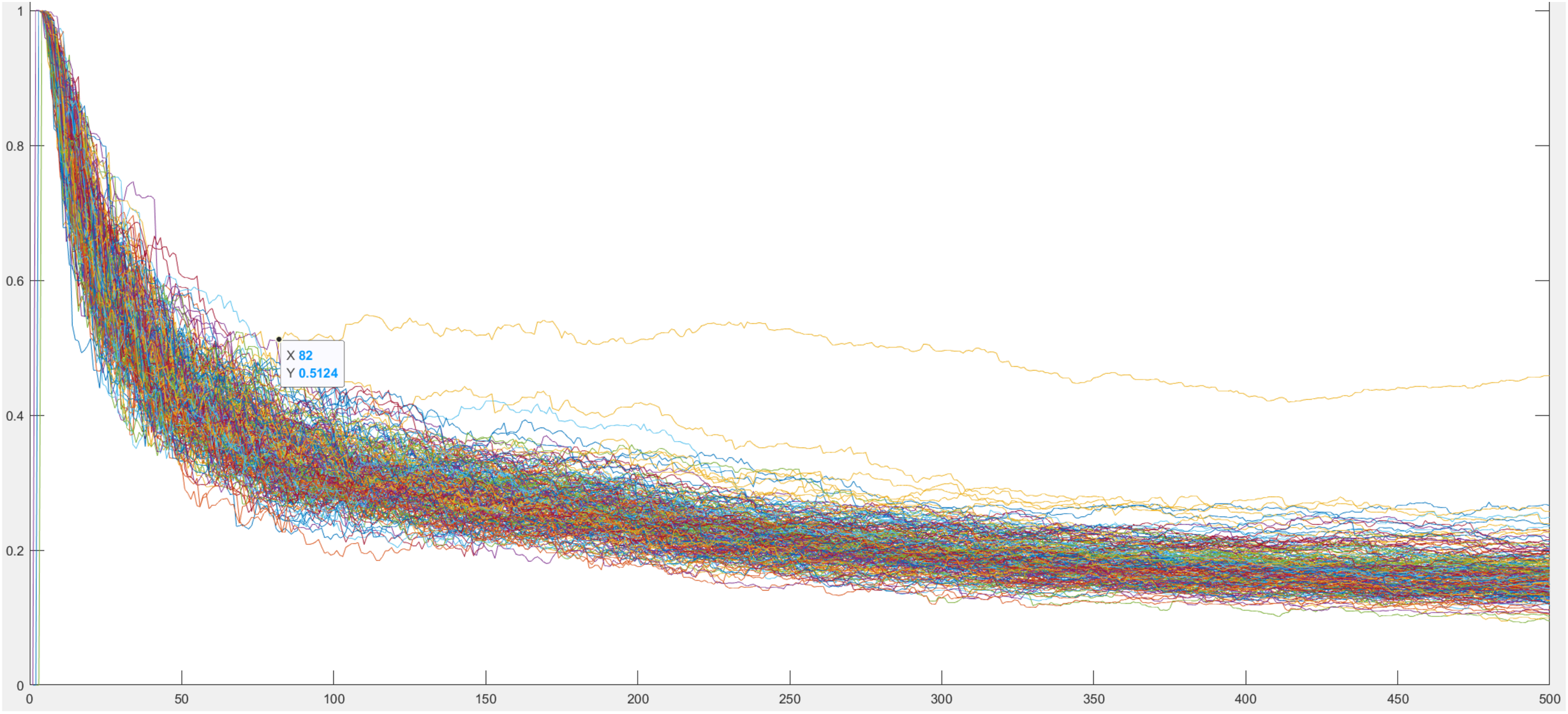
분석 결과

8th S-box output



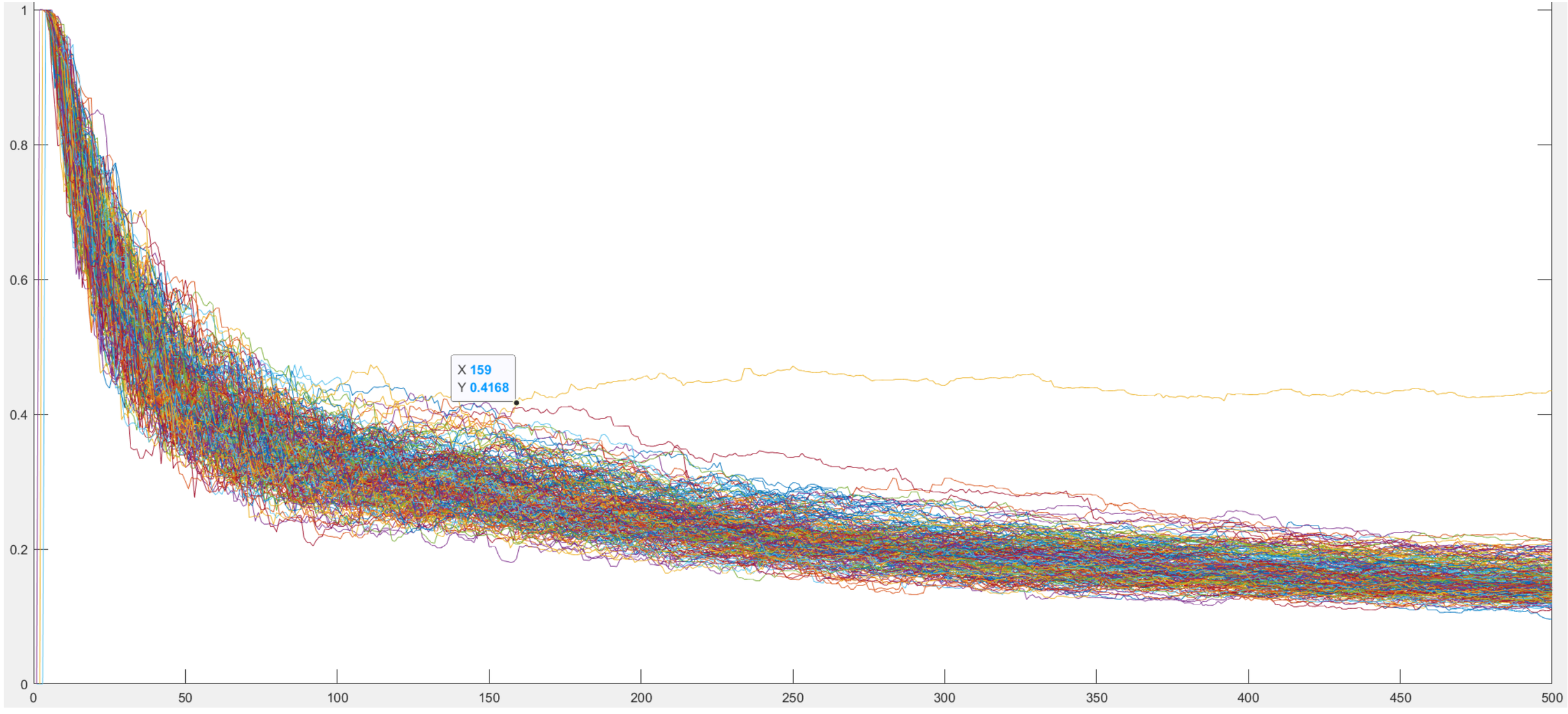
분석 결과

9th S-box output



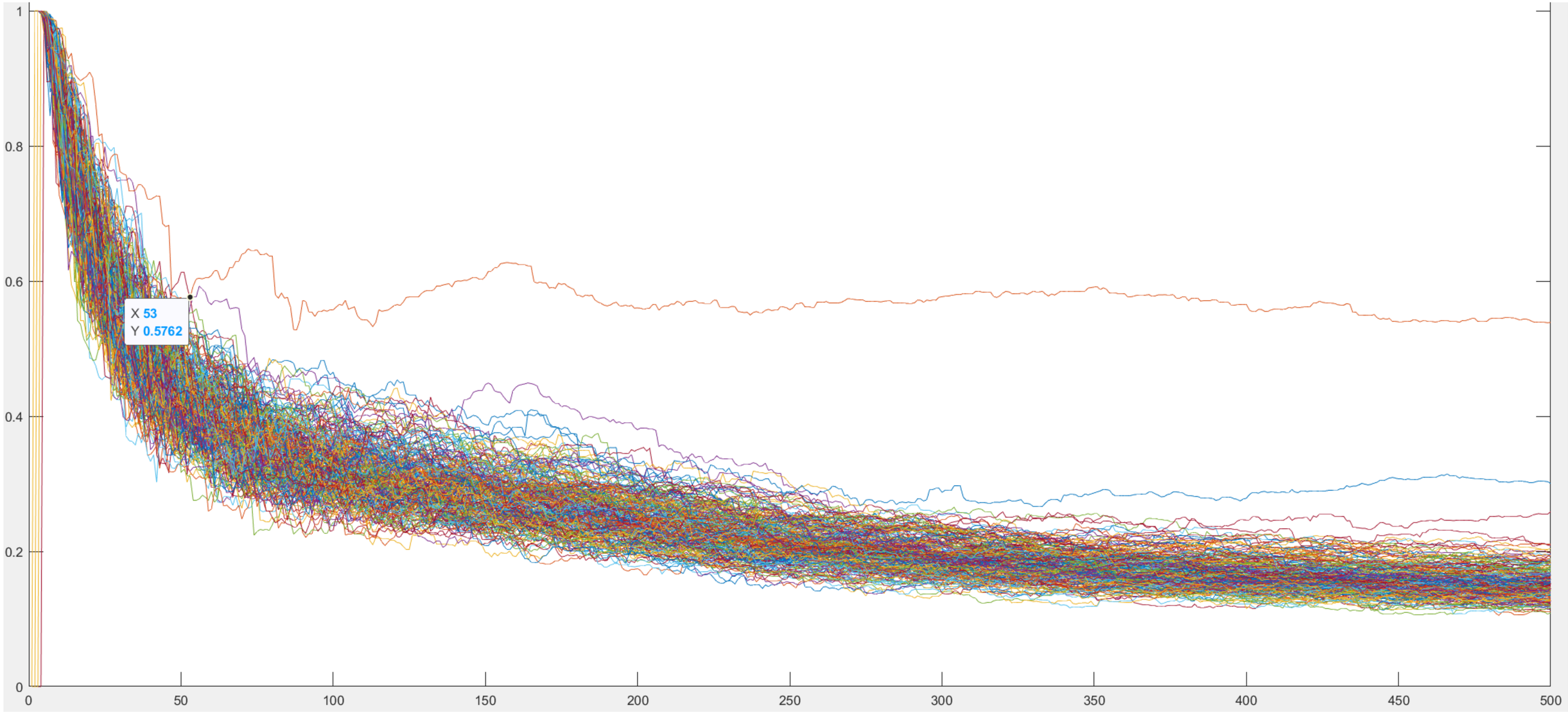
분석 결과

10th S-box output



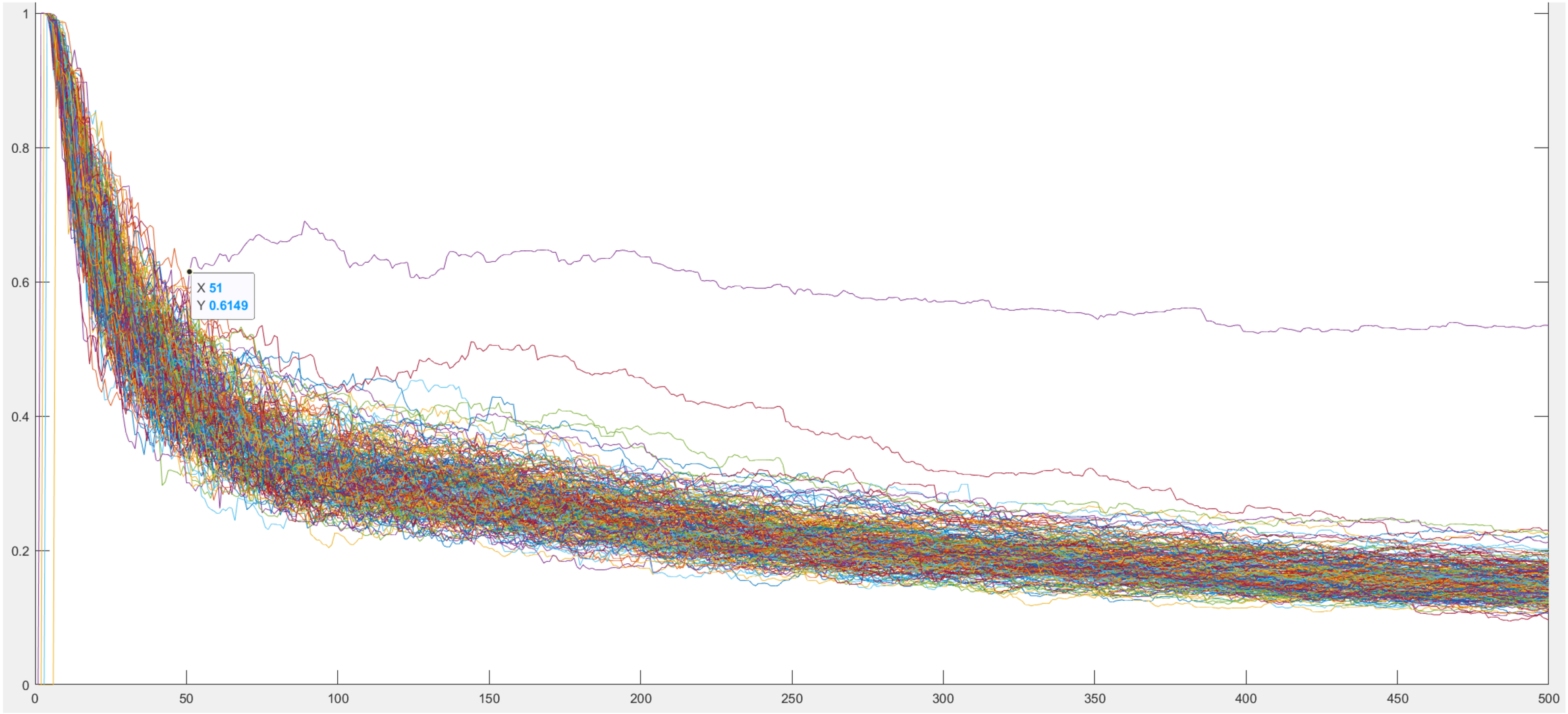
분석 결과

11th S-box output



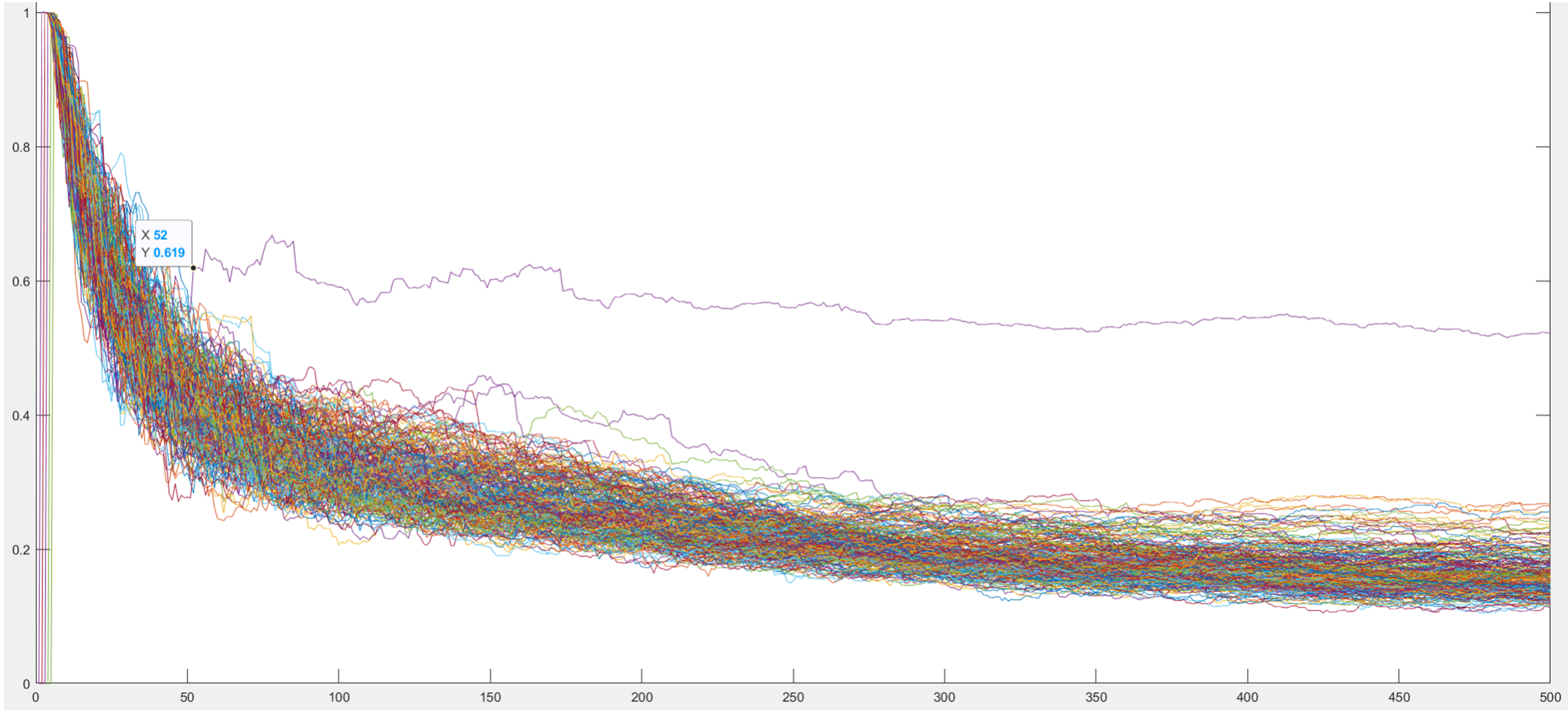
분석 결과

12th S-box output



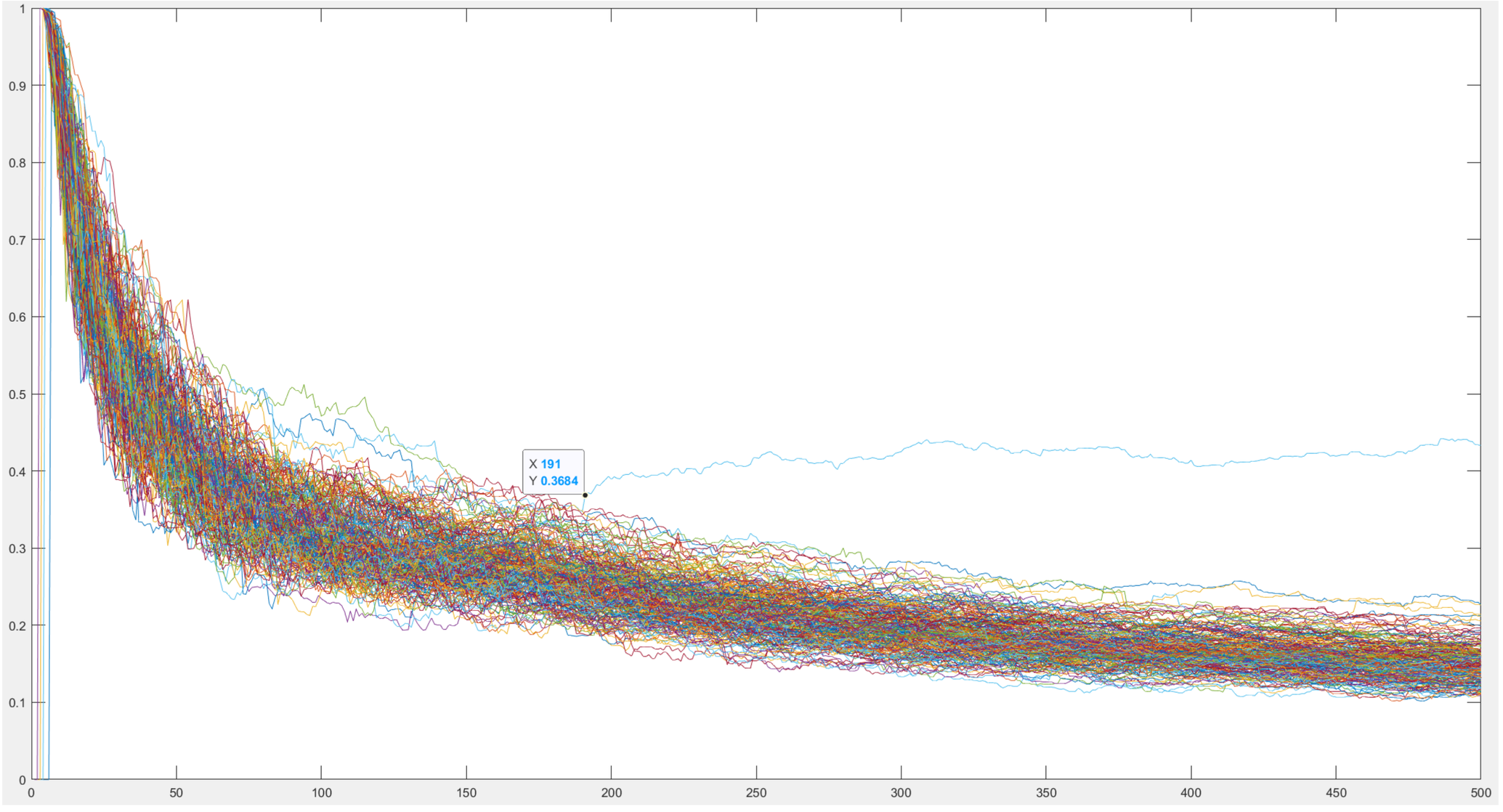
분석 결과

13th S-box output



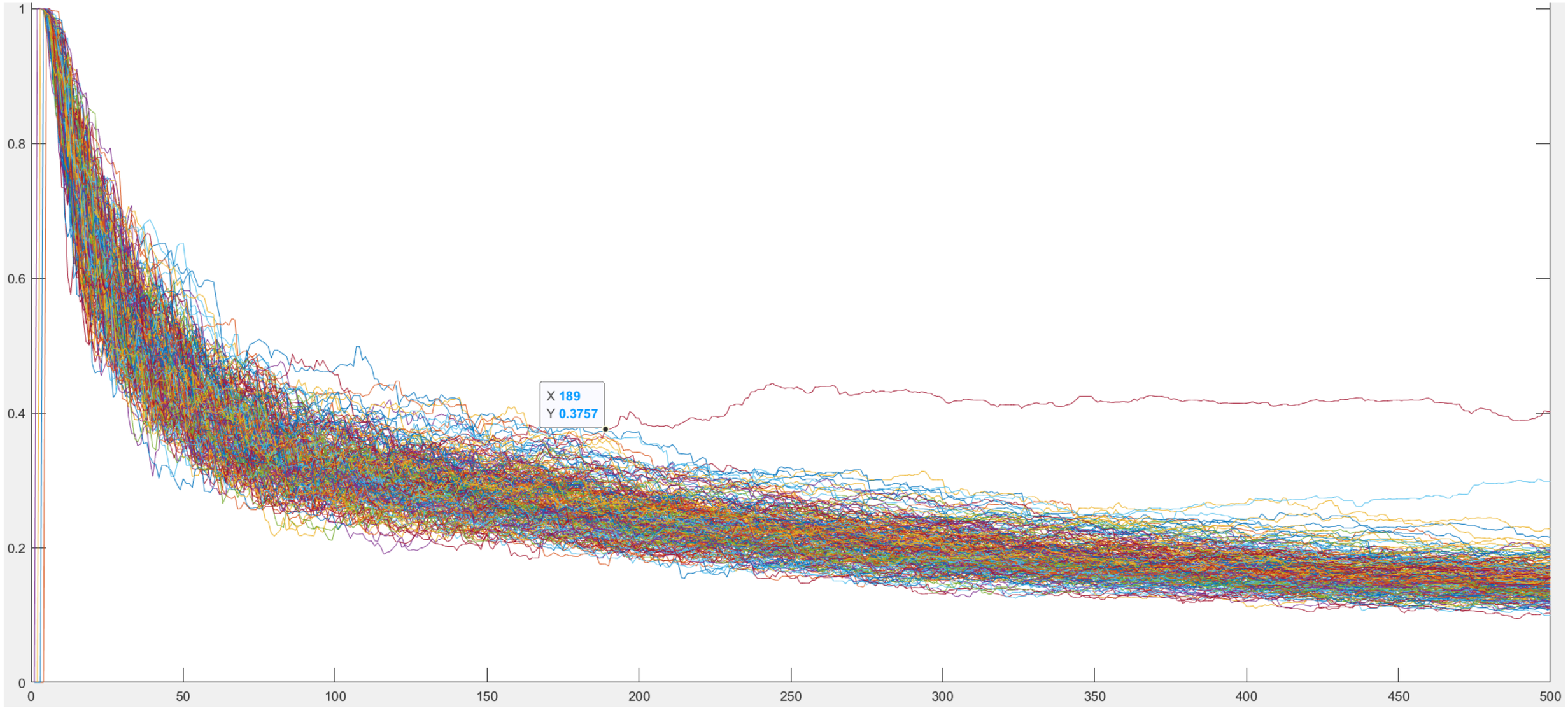
분석 결과

14th S-box output



분석 결과

15th S-box output



분석 결과

16th S-box output