Assignment 3 Report

Cryptanalysis of RC4

Submitted by

Vijay Kumar Meena	Burouj Armgaan
2017CS50421	2021VSN9003

Graph Results

- We observed that as the input size increases, the value of randomness (R) decreases (Fig 1).
  (Note: higher R means lower randomness).

- Increasing the number of bit flips has no effect on R for a fixed input size (Fig 2).

- We varied the counter size and observed that, as the number of counters increases the value of R also increases (Fig 5, 6, 7, 8).

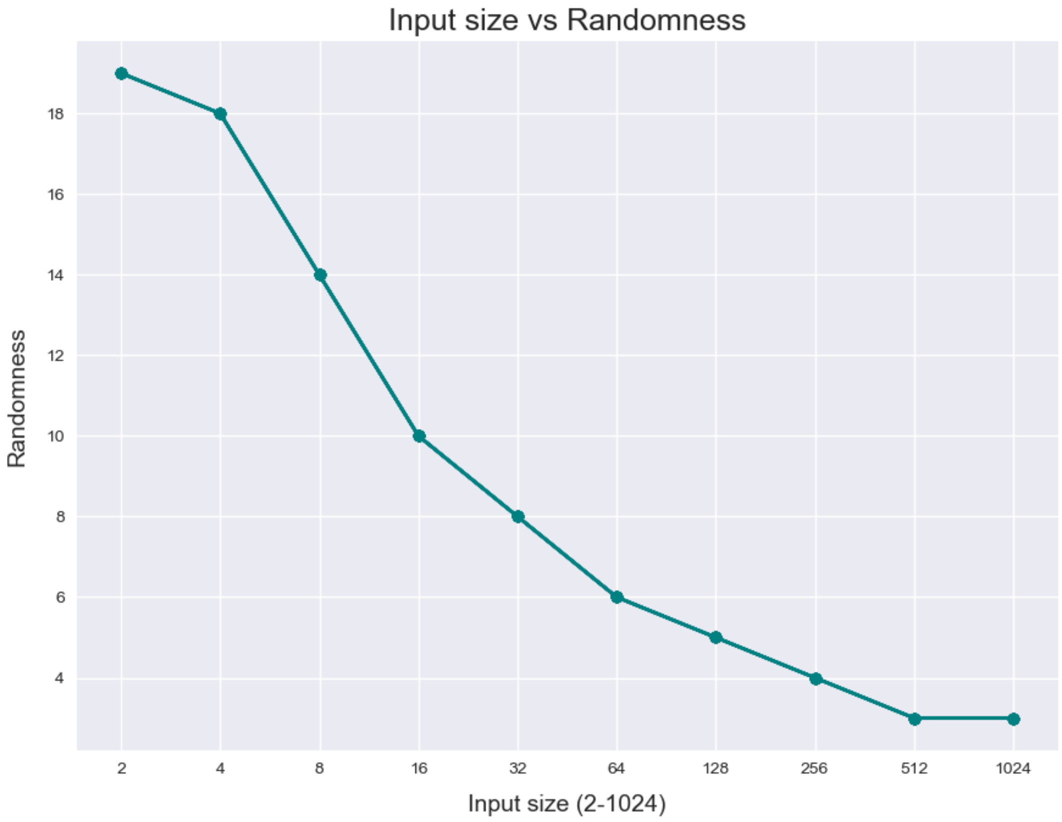

Fig 1: Randomness vs Input size

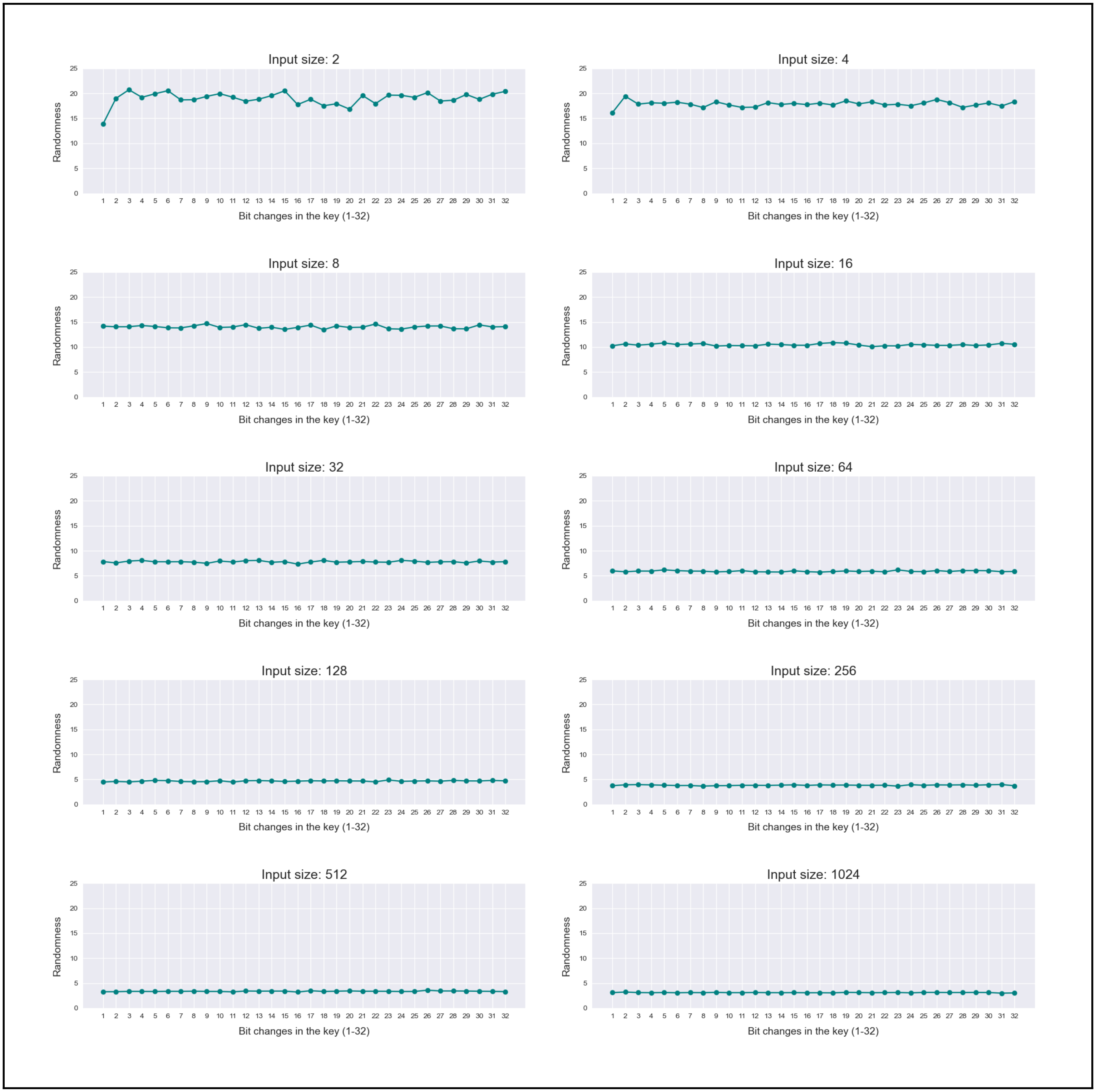

Fig 2: Randomness vs Bit flips in key for various input sizes.

Discussion

- As we saw in Fig 2, the value of R is independent of the number of bits flipped. 1 bit-flip has the same effect as 32 bit-flips. Hence, 1 bit-flip in the key is also sufficient to generate randomness in the cipher.

- Fig. 3 shows the variation of R with input size for a short message. It can be seen that the value of R remains consistent beyond input size of 36 bytes. Hence, for the first 36 bytes the key doesn't mix that well and should be thrown away.

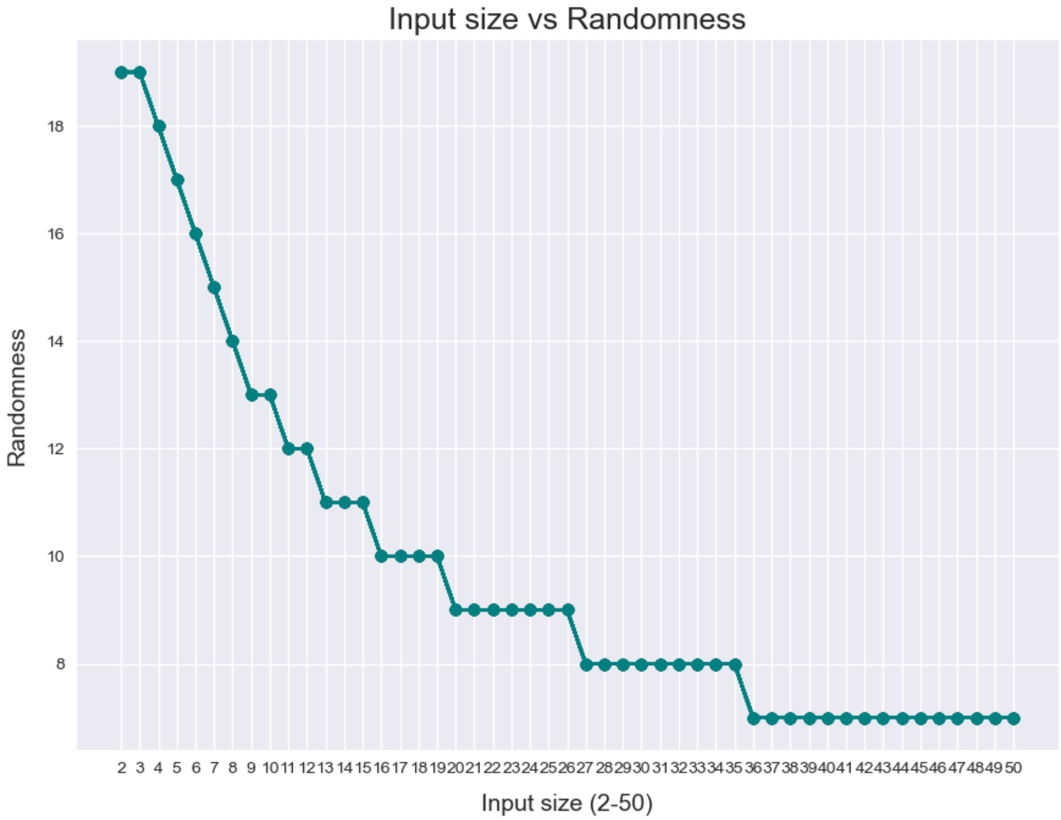

Fig 3: Randomness vs Input size for RC4 encryption on short messages

Another Analysis

Question: Try to measure the average length (in bytes) of identical output as a function of the number of bits you change in the key.

- Fig. 4 shows the variation of average number of identical bytes for 2 ciphers as a function of the number of bits flipped in the key.

- We saw in Fig 2, that the value of R is independent of bit-flips. Fig 4 complements that result. The similarity between ciphers doesn't dip as bit-flips are increased.

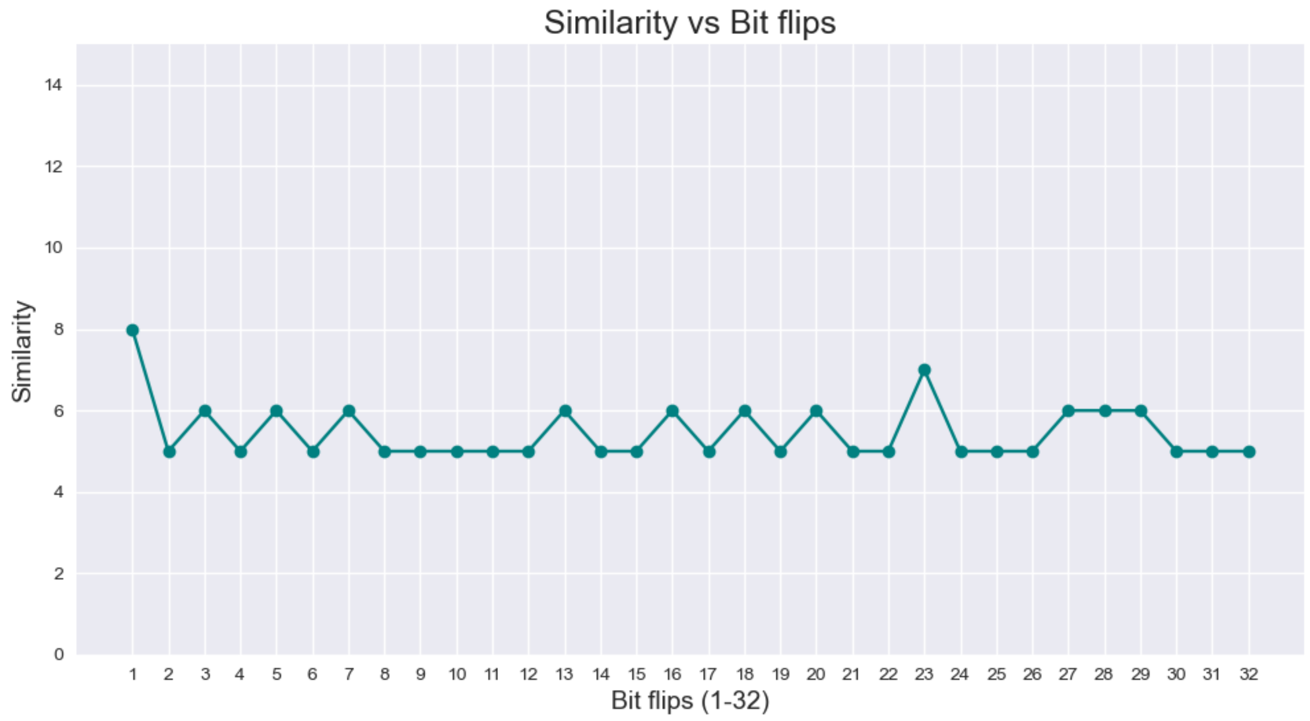

Fig 4: Similarity (Identical bytes across the 2 ciphers) vs Bit flips in the key

Variation in Randomness with number of Counters

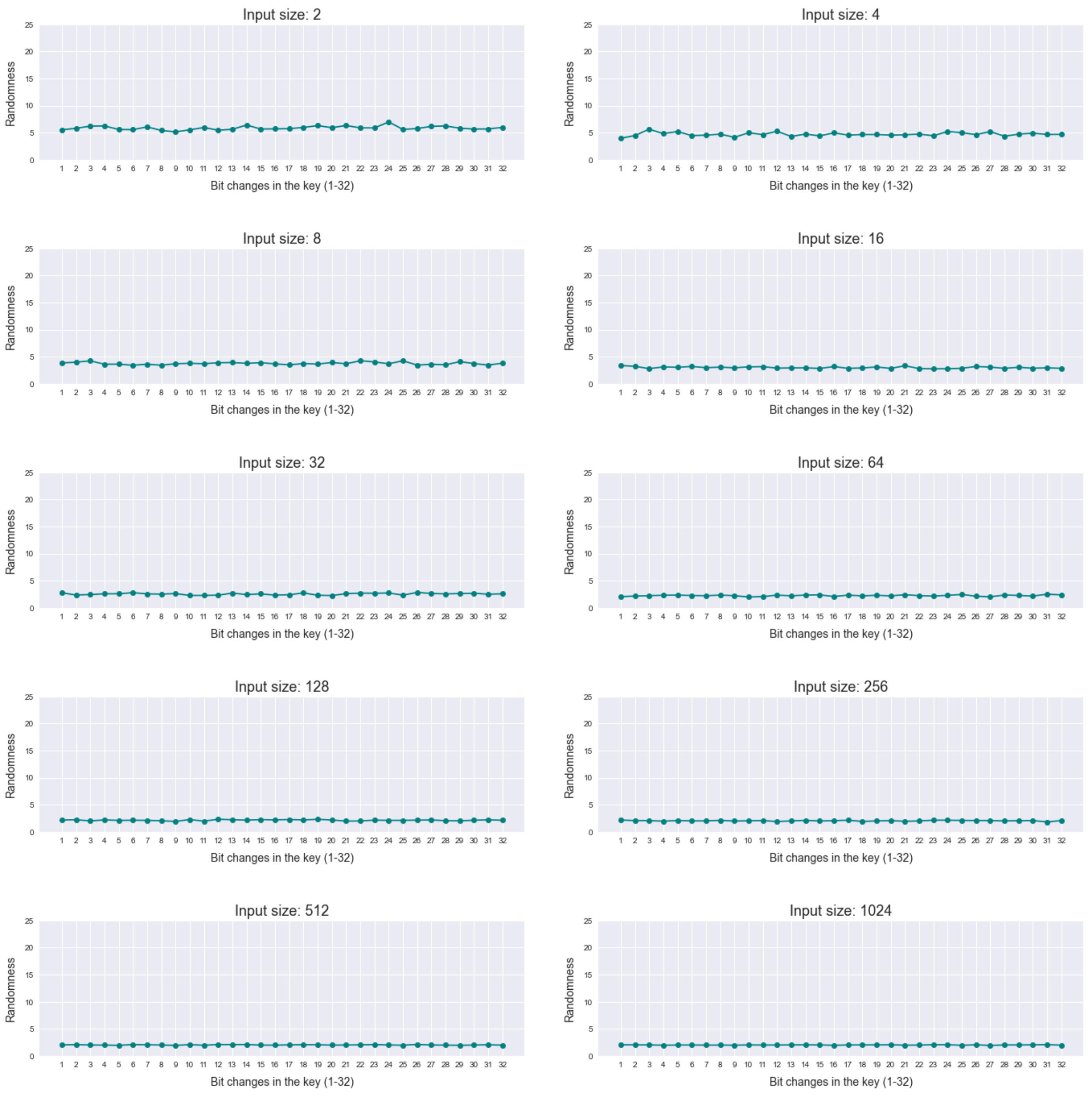

Fig 5: Counter size 4, #Counters = 2^4

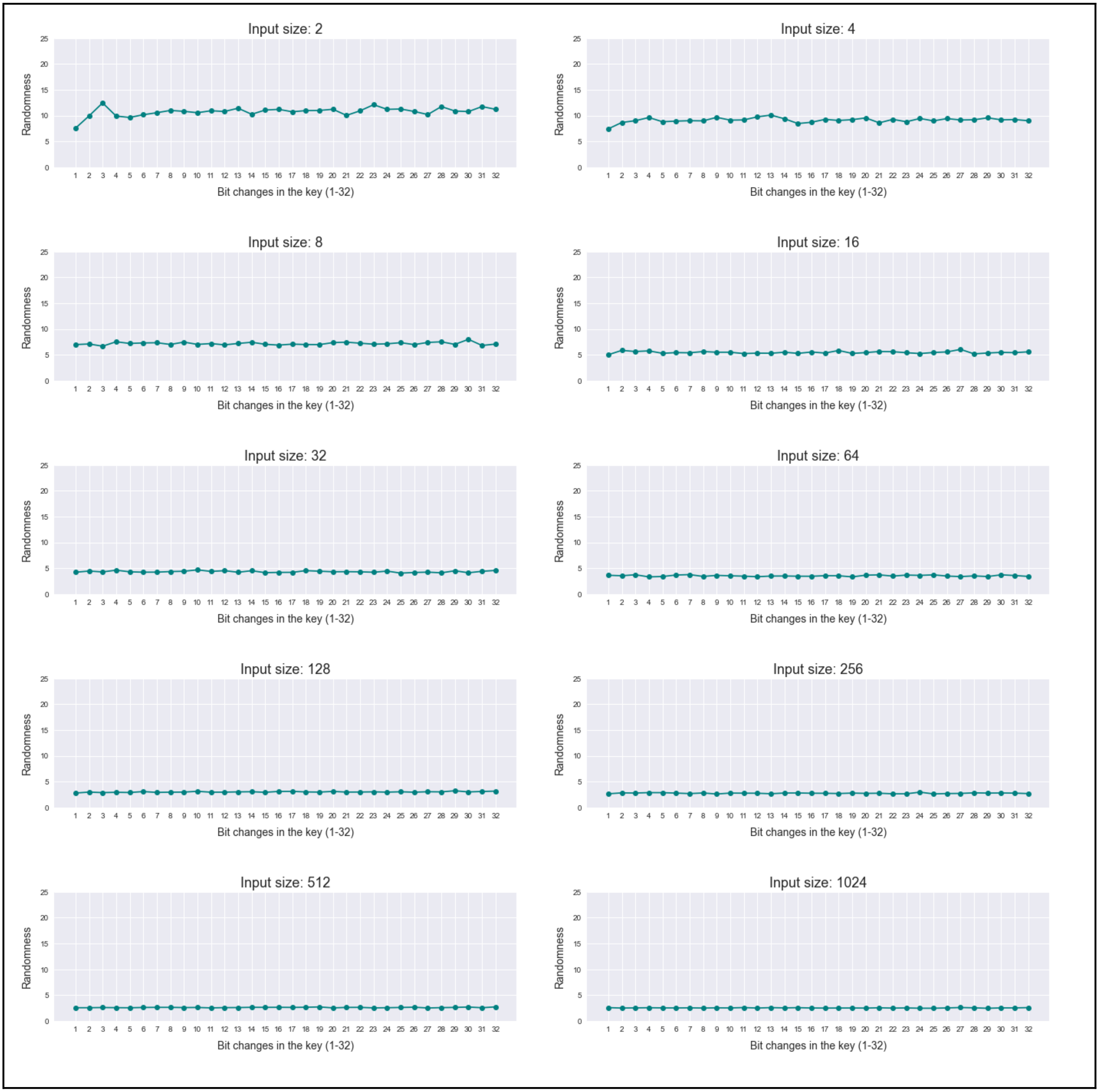

Fig 6: Counter size 6, #Counters = 2^6

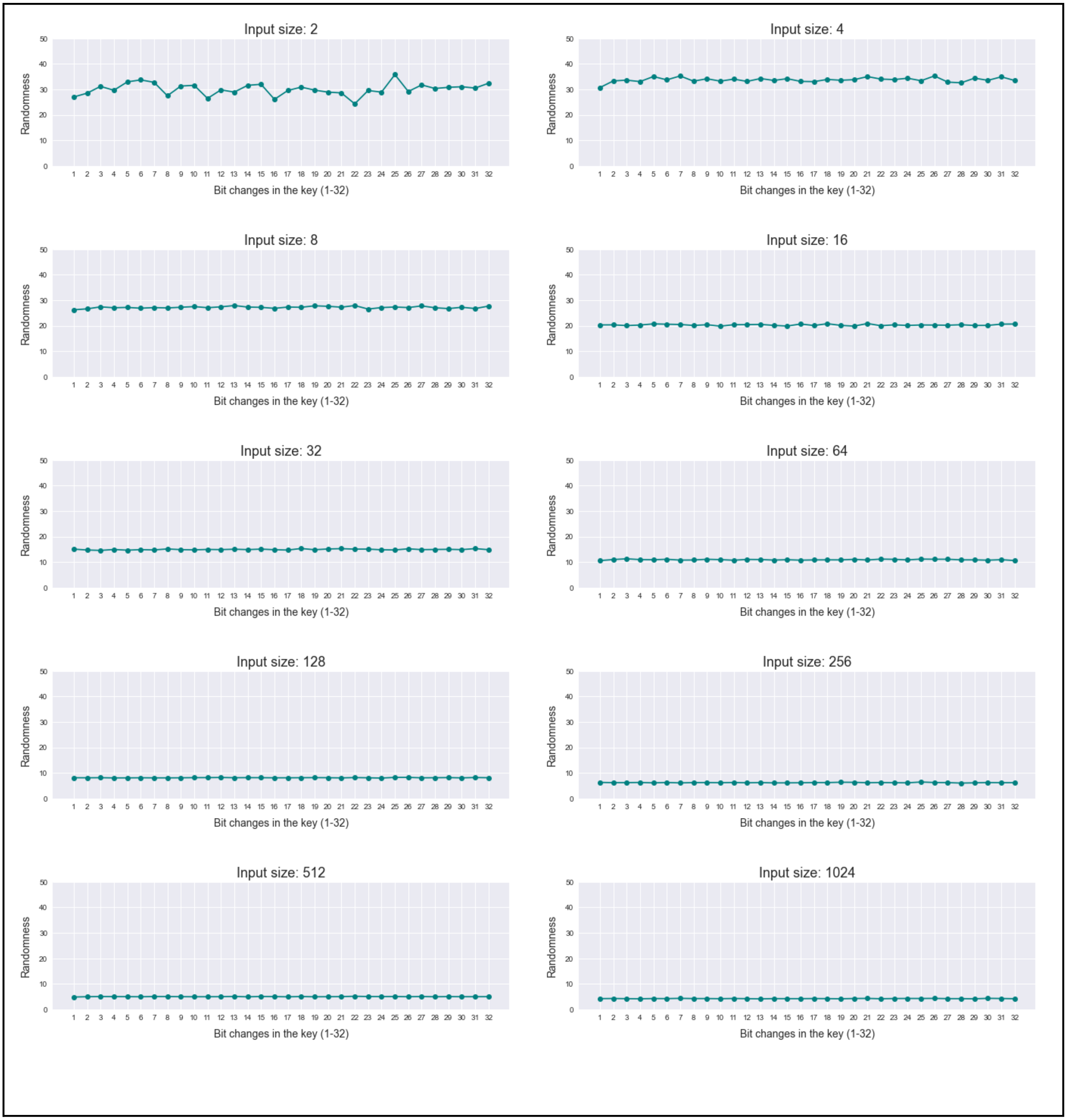

Fig 7: Counter size 10, #Counters = 2^10

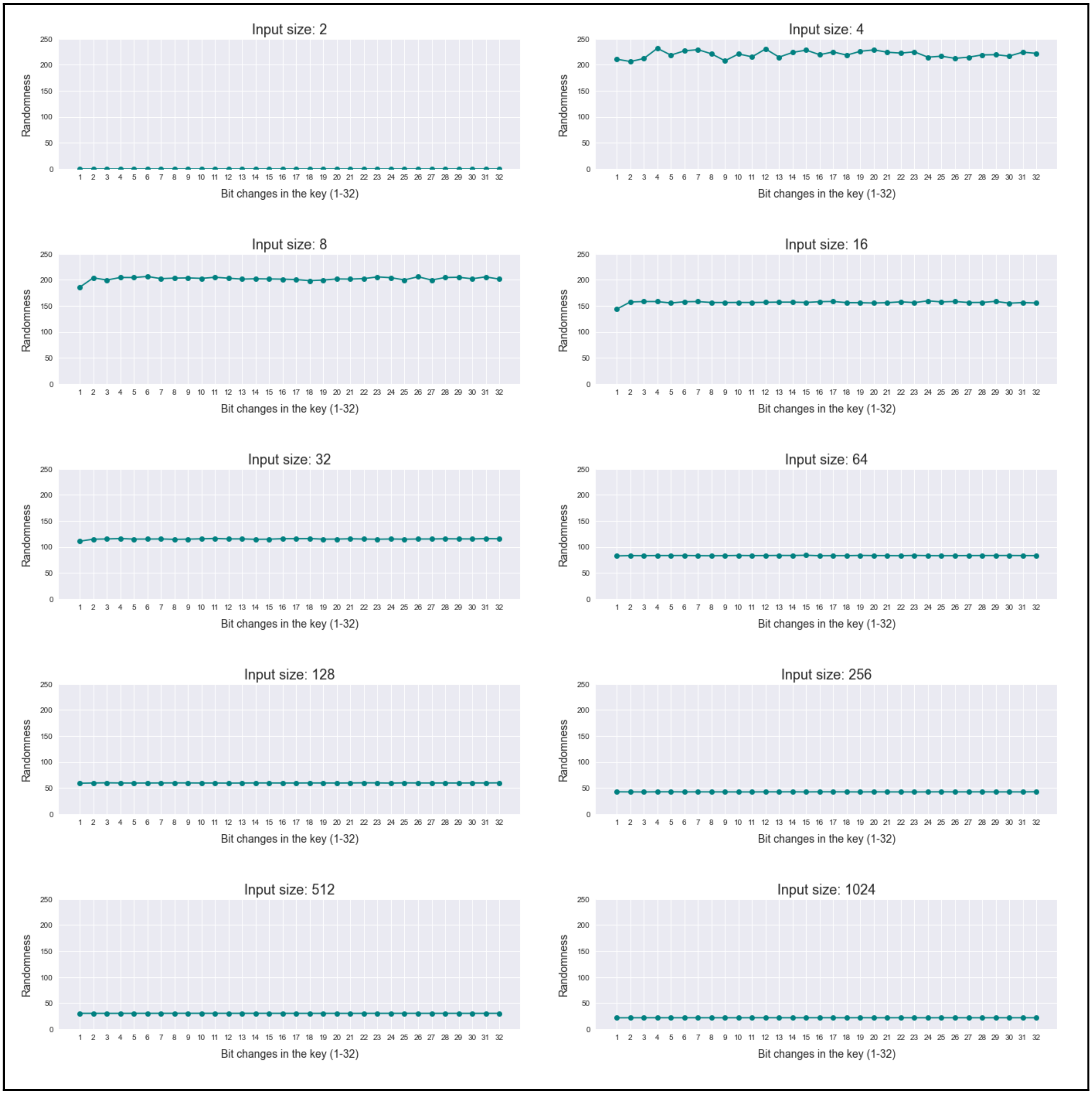

Fig 8: Counter size 16, #Counters = 2^16

As the counter size increases, the value of R increases.

- For counter size 4 i.e. 2^4 counters, the max value of R goes to 6.
- For counter size 6 i.e. 2^6 counters, the max value of R goes to 14.
- For counter size 10 i.e. 2^10 counters, the max value of R goes to 38.
- For counter size 16 i.e. 2^16 counters, the max value of R goes above 200!!