DATE: 2023/12/1

Department of Electrical and Electronic Information Engineering		ID	M203238
Name	Ayumu Chiba		

Supervisor	Shuichi Ichikawa

Abstract

Title	Random number generation by using fluctuation of cryptocurrency prices and LFSR

TRNG (True Random Number Generator) can generate unpredictable random number using physical phenomena, while it requires specialized hardware and suffers from high cost for implementation. PRNG (Pseudo Random Number Generator), which generate random number by a deterministic algorithm, can be implemented by software. PRNG provides higher generation rate and lower implementation cost than TNRG, whereas its future output may be predicted by inferring its internal states. Suciu et al. (2011) proposed URN (Unpredictable Random Number), which has intermediate properties between TRN (True Random Number) and PRN (Pseudo Random Number). Chiba and Ichikawa (2023) generated URN by adding fluctuations to the sampling period of LFSR using the wind direction data, but the wind direction data has problems in terms of generation rate and randomness in the time series.

This study examines the URN generated by using cryptocurrency prices as the fluctuation of the sampling period of LFSR. This study adopts Bitcoin (BTC) as a representative of cryptocurrency. First, the characteristics of the data were examined based on the distribution of the cryptocurrency price (P_t), Log Return (R_t) and their trends of the respective time-series data. During the sample period, P_t changed on a trend, while R_t was not affected by the trend and changed near the mean. Based on the above characteristics and distribution, P_t was encoded by extracting the least significant bit and R_t was encoded by dividing the distribution by a threshold value. The sample periods used for random number generation were selected by the volatility and the value range within the whole period. The encoded data were used as the LFSR sampling period fluctuations, and the quality of the generated random number sequence was evaluated with the DIEHARD test. The number of FAILs for a 32-bit LFSR decreased compared to the case with no fluctuation, suggesting that the fluctuations by P_t, R_t improved the random number quality.

Random numbers that yielded no FAIL with the base period $\beta \geq 32$ were evaluated in the more rigorous the NIST test. It was shown that they passed the NIST test in the sample period with high volatility when P_t is used. However, the effect of volatility was not clearly observed, as there were no distinct differences among the sample periods. When R_t was used, the highest number of PASSs was observed when the threshold was set to the mean value. As with the results of the DIEHARD test, no relationship between the sample periods and the fluctuations was shown. The LFSR lengths that pass for all sample periods were 56-bit for P_t and 48-bit for R_t. Even when using a LFSR that pass the NIST test, the use of suitable fluctuations is expected to improve the random number quality. When using BTC data, it is recommended to add fluctuations by using a coding method that sets the threshold of P_t or R_t to the mean value. Future work includes the detailed investigation of the compatibility of fluctuations and performance differences by increasing the sample periods and the type of cryptocurrency used.