2023 年 12 月 1 日

電気・電子情報工学専攻	学籍番号	M203238
申請者氏名	千葉 歩武	

指導教員氏名	市川 周一

論　文　要　旨（修士）

論文題目	暗号資産価格の揺らぎと LFSR を利用した乱数生成手法

真性乱数生成器 (TRNG; True Random Number Generator) は，物理現象を用いることで予測不可能な乱数を生成可能だが，専用のハードウェアが必要となり実装コストが高い．決定的アルゴリズムで乱数生成する疑似乱数生成器 (PRNG; Pseudo Random Number Generator) は，ソフトウェアで設計できるため低コスト高性能な実装が可能であるが，内部状態を推測することにより次の出力が予測可能であるという問題がある．そこで Suciu ら (2011) は True Random Number (TRN) と Pseudo Random Number (PRN) の中間的な性質を持つ Unpredictable Random Number (URN) を提案した．千葉と市川 (2023) は風向データで LFSR のサンプリング間隔に揺らぎを加えることにより URN を生成したが，風向データは生成レートや時系列における乱数性に難がある．

本研究では LFSR のサンプリング間隔の揺らぎに暗号資産価格を用いることで URN を生成した．研究に用いた銘柄は Bitcoin (BTC) である．始めに暗号資産価格 P_t と対数収益率 R_t の分布およびそれぞれの時系列データの推移からデータの特徴を確認する．サンプル期間において P_t はトレンドを形成しながら推移しており，R_t はトレンドの影響をあまり受けず平均付近を推移した．以上の特徴と分布を踏まえて P_t は最下位ビットを抽出する方法，R_t は分布をしきい値によって分割する方法で符号化する．またボラティリティとサンプル期間内の値幅によって，乱数生成に用いるサンプル期間を定めた．符号化したデータを LFSR のサンプリング間隔の揺らぎとして使用し，生成した乱数列の品質を DIEHARD テストで評価した．32-bit LFSR の FAIL 数が揺らぎなしの場合と比べて減少していることから，P_t, R_t による揺らぎによって乱数品質が向上したと考えられる．サンプル期間によって FAIL 数に差はあるが揺らぎとの間に関連性は見られない．DIEHARD テストでは OPERM5 が FAIL する確率が高かった．

DIEHARD テストにおいて，基本サンプリング間隔 β が 32 以上のとき一度も FAIL しなかった乱数をより厳格な NIST テストで評価する．P_t を使用した時にボラティリティが大きいサンプル期間ですべて PASS することが示された．しかしサンプル期間の違いによる有意な差が見られないため，ボラティリティによる影響は見出せない．R_t を使用した時は，しきい値を平均値に設定すると最も PASS 数が多くなることが分かった．DIEHARD テストの結果と同様にサンプル期間と揺らぎの間の関連性は示されていない．すべてのサンプル期間で PASS する LFSR 長は，P_t で 56-bit, R_t で 48-bit である．NIST テストを PASS する LFSR を用いる場合でも，適した揺らぎを使用することで乱数品質が向上すると考えられる．本研究では P_t と R_t のどちらを使っても NIST テストを PASS することが示された．BTC のデータを使用する時は P_t の最下位ビットか，R_t のしきい値を平均値に設定した符号化方法で揺らぎを加えることを推奨する．今後の課題は，使用するサンプル期間や銘柄を増やすことで揺らぎの相性や性能差を詳細に調査することである．