線形／非線形フィードバックシフトレジスタ用いた乱数生成・暗号システムに関する研究

Random Number Generation and Cipher Systems Using Linear/Nonlinear Feedback Shift Registers

キーワード：LFSR/NFSR, 乱数，暗号，カオス/key words: LFSR/NFSR, random number, cipher, chaos

常田　明夫　准教授　Ph. D.　/ **Akio TSUNEDA**　Assoc. Prof., Ph.D.
情報・エネルギー部門　波動情報処理分野　/ Research Field of Wave Information Processing
E-mail : tsuneda@cs.※　Tel : 096-342-3853　URL : http://www.cs.kumamoto-u.ac.jp/~tsuneda/

●非周期乱数生成

モンテカルロシミュレーションにおいては長周期で様々な統計的性質をもつ乱数が必要とされている．このニーズに応えるため，ベルヌイ写像に対するカオス理論と線形フィードバックシフトレジスタ(LFSR)に基づいた後処理(Figure 1)により，指定した自己相関特性をもつ非周期乱数の生成を試みている．

●NFSRを用いたブロック暗号システム

非線形フィードバックシフトレジスタ(NFSR)を用いたブロック暗号システム(Figure 2)を提案し，その安全性や暗号化／復号化速度などについて検討している．

Generation of aperiodic random numbers : In Monte-Carlo simulations, random numbers with long period and various statistical properties are required. We propose post-processing methods to generate random bit sequences with prescribed auto-correlation properties as shown in Figure 1.

Block cipher systems based on NFSRs: We propose block cipher systems based on nonlinear feedback shift registers (NFSRs) as shown in Figure 2. We also investigate the security and the speed of encryption/decryption.

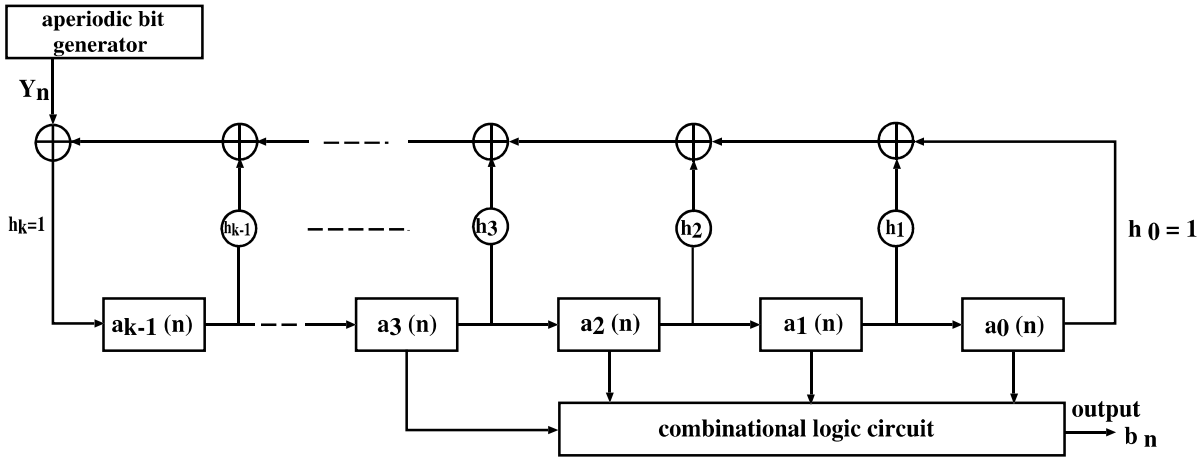

Figure 1 Post-processing based on LFSR and chaos theory

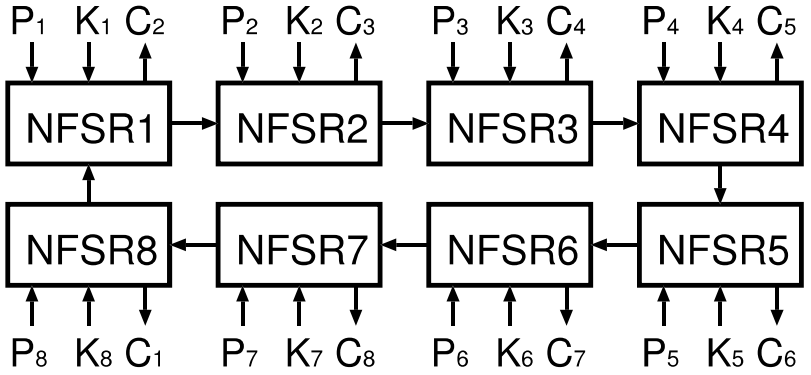

Figure 2 Block cipher system based on NFSRs