Reconfigurable Feedback Shift Registers

Agnes Hui Chan
College of Computer Science
Northeastern University
Boston, MA 02115
ahchan@ccs.neu.edu

Muriel Médard
Lincoln Laboratory
Massachusetts Institute of Technology
Lexington, MA 02173
medard@ll.mit.edu

Abstract — **Transfer of large, bursty files has been made possible by the advancement of technology in ultrafast optical TDM networks. Such transfers require ultrafast encryption using pseudorandom key streams. We propose a new sequence generator, based on both optical logic and electronic FSRs, that generates sequences at optical rates. The complexity of the sequence depends on that of the electronic controller.**

I. Introduction

As technology for 100 Gbps local/metropolitan area TDM networks [1] is evolving rapidly, the demand for a cost-effective, ultrafast key stream generator for encryption purposes becomes more urgent. Unfortunately, current high-speed encryption systems only operate around 2.5 Gbps.

In the optical domain, data storage and logical operations have been demonstrated at rates on the order of 40 Gbps [2]. The implementation of logic at such high rate, whether it is electronic or optical, is often limited in scope and extremely expensive. To increase the complexity of a sequence, nonlinear functions with number of taps comparable to the length of the FSR are introduced to serve as feedforward and/or combiner functions [3][4]. Therefore a direct migration of design from electronic FSRs to optical FSRs becomes infeasible. We propose a new sequence generator, based on both optical logic and electronic FSR, that generates sequences at optical rates.

II. Reconfigurable Feedback Shift Register

Optical FSRs have lengths of at least 10^4, whereas the gate count is greatly limited by cost and technology. To overcome our limitations on optical taps, we use a "slow" electronic sequence generator to control the logic functions operating on an optical FSR that runs at a high data rate. The complexity of the sequence relies heavily on the design of the electronic controller while the optical FSR yields the ultrafast data rate.

We consider an optical FSR of length L which outputs a symbol at every clock cycle. Let δ be the ratio of the optical data rate to the electronic data rate (e.g. $\delta \geq 100$ for electronics at 1Gbps and optics at 100Gbps). The taps of the FSR are reconfigured every δ clock cycles according to the output symbol of an electronic sequence generator with period τ. The optical FSR thus has feedback function f_i for all times in $\bigcup_{k=0}^{\infty} [k\tau\delta + (i-1)\delta + 1, k\tau\delta + i\delta]$. The f_is need not all be different.

Definition 1 *A Reconfigurable Feedback Shift Register (RFSR) consists of a FSR of length L, a collection of feedback functions $(f_0, f_1, ..., f_{\tau-1})$ and a controller that outputs a τ-ary sequence* **t**. *The RFSR generates the sequence* s *given by*

$$s_{i\delta+j+L} = f_{t_i}(s_{i\delta+j}, s_{i\delta+j+1}, ..., s_{i\delta+j+L-1}) \qquad (1)$$

where $0 \leq i, 0 \leq j < \tau$, $i \geq 0$ and $0 \leq j\tau$.

If the logic functions f_i are linear, then a RFSR is called a Reconfigurable Linear Feedback Shift Register (RLFSR). Such a scheme is an extension of the one presented in [5], where $\delta = 1$. The following theorem shows that any RLFSR needs at most δ simultaneously active taps.

Theorem 1 *Let δ be fixed. Let* **S** *be any RLFSR. Then there exists a RLFSR* **S**$'$ *such that* **S**$'$ *has at most δ taps and* **S**$'$ *generates the same key stream as* **S**.

We may establish some properties about the period, ρ, of an RLFSR. Let $\phi = f_1^{\delta} \circ \ldots \circ f_{\tau}^{\delta}$, where the superscript denotes composition. Let the period of ϕ be p.

Proposition 1 *ρ divides $p\delta\tau$.*

Proposition 2 *If $p > 1$, then ρ does not divide $\delta\tau$.*

Proposition 3 *If τ and δ are prime, then if ρ divides p, there exists a ρ-vector $(s_0, ..., s_{\rho-1})$ such that for all $0 \leq j \leq \rho - 1$*

$$f_i(s_j, \ldots, s_{j+L-1}) = s_{j+L \bmod p}. \qquad (2)$$

III. Conclusions

RLFSRs may yield sequences with very large periods. If τ is an acceptable period at "slow" speeds, then $\delta\tau$ is an acceptable period at "high" speeds. Proposition 3 indicates that we may attain $\rho = p\delta\tau$ under mild constraints for the f_is. In practice, τ will be chosen to be very large, therefore, it may be difficult to establish its primality. We have also considered quadratic feedback functions. In our simulations, we use FSRs of length $10 \leq L \leq 15$, we reconfigure between two functions with 4 taps each, $\tau = 26$, and $\delta = 100$. Even with such small parameters, we observe periods of 10^9 or higher.

Acknowledgements

We thank Dr. V. Chan, Dr. K. Hall, Dr. J. Moores and Dr. K. Rauschenbach for discussions about optical technology. We also thank S. Parikh for discussions and programming support.

References

[1] V.W.S. Chan, *All Optical Networks*, Scientific American, vol. 273, no. 3, September 1995.

[2] N.S. Patel, K.A. Rauschenbach, K.L. Hall, *40 Gb/s Cascadable All-Optical Logic Using an Ultrafast Nonlinear Interferometer*, OFC '96, vol. 2, 1996, Postconference Edition.

[3] E.L. Key, *An Analysis of the Structure and Complexity of Nonlinear Binary Sequence Generators*, Computer, vol.24, no. 2, February 1991.

[4] T. Siegenthaler, *Cryptanalysis Representation of Nonlinearly Filtered ML-Sequences* , Proc. Eurocrypt '85.

[5] Y. Roggeman, *Quelques classes de registres a décalage et leurs applications en cryptographie*, Doctor in Science Thesis, Université Libre de Bruxelles, 1987.