

# Cryptology ePrint Archive: Report 2011/358

## Constructing a Diversified FCSR with a Given Connection Integer

*Zhiqiang Lin and Dingyi Pei*

**Abstract:** A new FCSR representation called a diversified representation is used to replace the Galois one, avoiding the LFSRization attack. Hence, to build hardware and software oriented diversified FCSRs becomes an important problem. In this paper, we show a method of constructing a diversified FCSR for hardware implementation with a given connection integer. The construction is simple and convenient. And the diversified FCSRs we get are able to meet the hardware criteria.

**Category / Keywords:** secret-key cryptography / stream cipher, 2-adic number, diversified FCSRs,  $\mathbb{F}_2$ -sequences

**Date:** received 3 Jul 2011

**Contact author:** linzhiqiang0824 at yahoo cn

**Available formats:** [Postscript \(PS\)](#) | [Compressed Postscript \(PS.GZ\)](#) | [PDF](#) | [BibTeX Citation](#)

**Version:** 20110704:062306 ([All versions of this report](#))

**Discussion forum:** [Show discussion](#) | [Start new discussion](#)

---

[ [Cryptology ePrint archive](#) ]