# Cryptology ePrint Archive: Report 2011/711

### Evolutionary Construction of de Bruijn Sequences

*Meltem Sonmez Turan*

**Abstract:** A binary de Bruijn sequence of order $n$ is a cyclic sequence of period $2^n$, in which each $n$-bit pattern appears exactly once. These sequences are commonly used in random number generation and symmetric key cryptography particularly in stream cipher design, mainly to their good statistical properties. Constructing de Bruijn sequences is of interest and well studied in the literature. In this study, we propose a n randomized construction method based on genetic algorithms. The method models de Bruijn sequences as a special type of traveling salesman t (TSP) and tries to find optimal solutions. We present some experimental results for $n\leq 14$.

**Category / Keywords:** secret-key cryptography / De Bruijn sequences, Genetic algorithms, Traveling salesman problem

**Publication Info:** Previous version of this paper was published in AISec'11, October 21, 2011, Chicago, Illinois, USA

**Date:** received 30 Dec 2011

**Contact author:** meltemsturan at gmail com

**Available formats:** PDF | BibTeX Citation

**Version:** 20111231:155358 (All versions of this report)

**Discussion forum:** Show discussion | Start new discussion

[ Cryptology ePrint archive ]