**BENT SEQUENCES AND FEEDBACK WITH CARRY SHIFT REGISTERS**

Midshipman Charles Celerier (Font: Arial 12)

United States Naval Academy

[m121062@usna.edu](mailto:m121062@usna.edu)

A stream cipher uses pseudorandom sequences to mimic the security of a one-time pad. This paper will investigate how Bent functions can be used to generate Bent sequences with large 2-adic span for use in feedback with carry shift registers (FCSRs). The linear complexity of an FCSR, a commonly used device in stream ciphers, directly relates to the magnitude of the 2-adic span of the sequence generated. This affects the resistance of the stream cipher against register synthesis attacks. In this paper, it is shown that it is possible to compute the 2-adic value of a Bent sequence.

**Advisor: Professor David Joyner, USNA Department of Mathematics,** [**wdj@usna.edu**](mailto:wdj@usna.edu)**.**