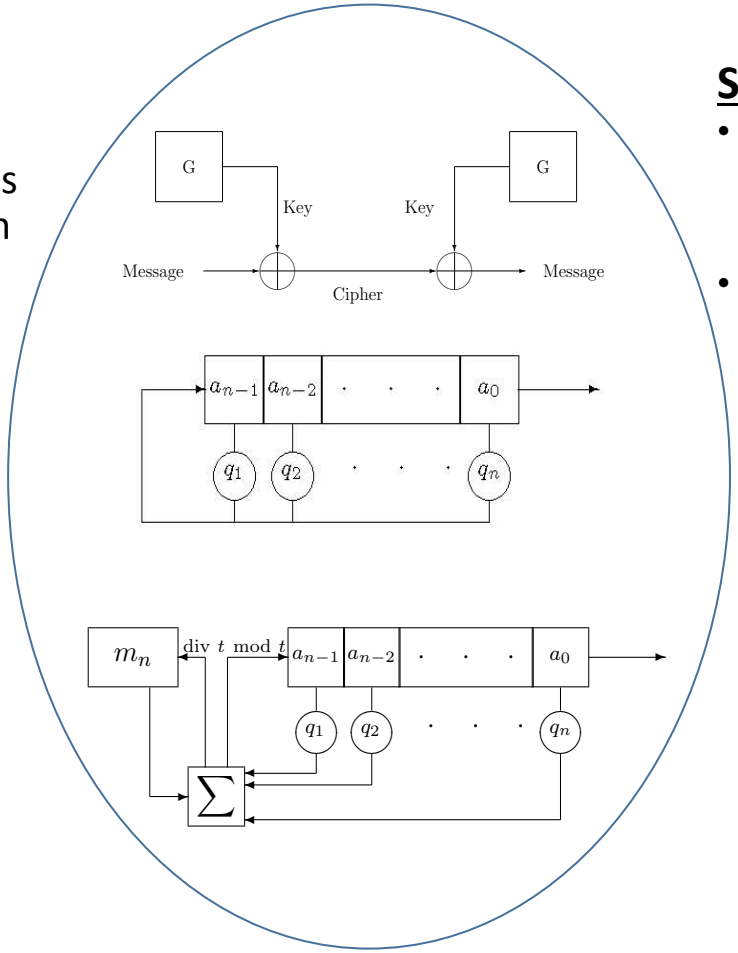
TWC: Small: Design and Analysis of Symmetric Key Ciphers

Challenge:

- Symmetric key cryptosystems are essential for securing high volume data, yet they eventually become obsolete
- Algebraic cryptanalysis threatens many ciphers

Solution:

- Replace LFSRs by FCSRs in stream ciphers
- Tools for analyzing approximability of Boolean functions by low degree functions



Scientific Impact:

- Provide new mathematical tools for building fast, secure block and stream ciphers
- Improve understanding of security of cryptographic tools

Broader Impact:

- Improved tools for design of the next generation of high speed cryptographic devices
- Support three PhD students, two female

Project number 1420227
University of Kentucky

PI: Andrew Klapper, klapper@cs.uky.edu