# My Past and Current Research

Cunsheng Ding

Dept. of Comp. Science & Engineering

HKUST

# Research Areas

- Cryptography
- Coding theory
- Interplays between cryptography and coding theory
- Mathematical foundations of cryptography and coding theory

# Cryptography

- Main topics in cryptography
  - Security solutions for data confidentiality
  - Security solutions for data integrity
  - Security solutions for nonrepudiation
  - Security solutions for anonymity
  - Secret sharing schemes
- My research topics in cryptography
  - Stream ciphers, authentication codes, secret sharing schemes
  - Started in 1986, a cryptographer by training

# Coding Theory

- Main Topics
- Source coding and data compression
  - How to express information effectively?
- Channel coding
  - How to detect and correct errors occurred in data transmission and storage?

- Applications
- Communication systems
- Data storage systems
- Consumer electronics

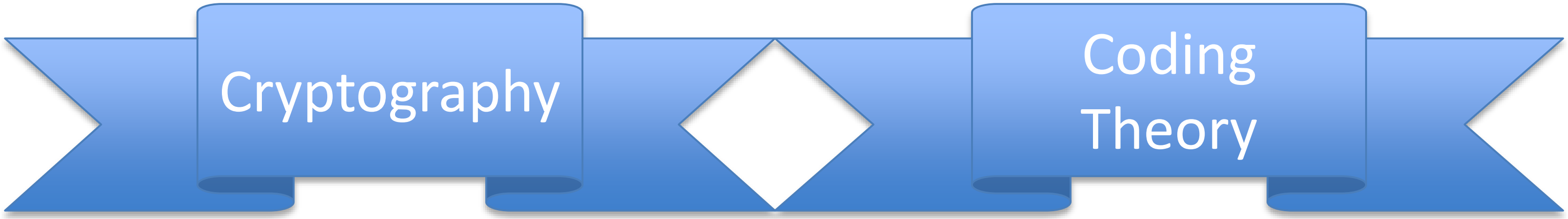
- My research topics in coding theory
  - Linear codes, cyclic codes
  - Started in 1997

# Interplays between Cryptography and Coding Theory

- Stream ciphers and linear codes
- Authentication codes and linear codes
- Secret sharing schemes and linear codes

# Mathematical Foundations

- Algebra, algebraic number theory, elementary number theory, finite fields, algebraic function fields
- Combinatorial designs
- Finite geometry, algebraic geometry
- Graph theory
- Discrete mathematics in general



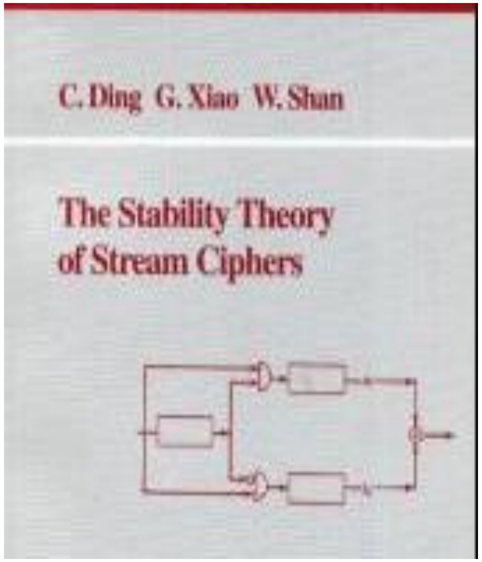
# End of Presentation

# Research Highlight (1)

- The stability theory of stream ciphers

- A new theory of stream ciphers, developed in 1989.
- Perhaps the 1st research monograph in English from Mainland China directly published in the Western over the past 5000 years.

Lecture Notes in Comp. Sci. 561, Springer Verlag, 1991

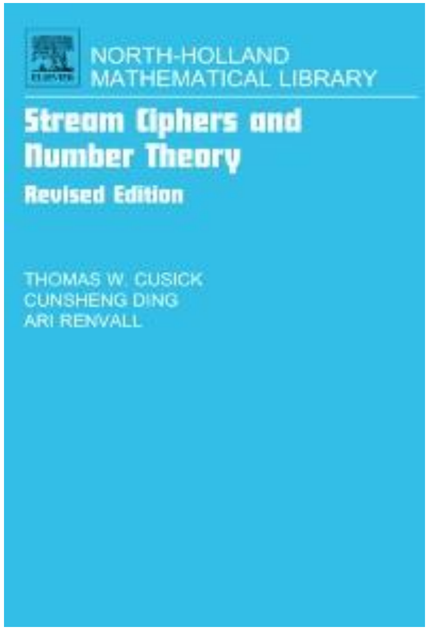


C. Ding G. Xiao W. Shan

The Stability Theory of Stream Ciphers

# Research Highlight (2)

- Stream Ciphers and Number Theory
- North-Holland Mathematical Library, Vol. 55, 1998
- Bridging stream ciphers and number theory



NORTH-HOLLAND
MATHEMATICAL LIBRARY

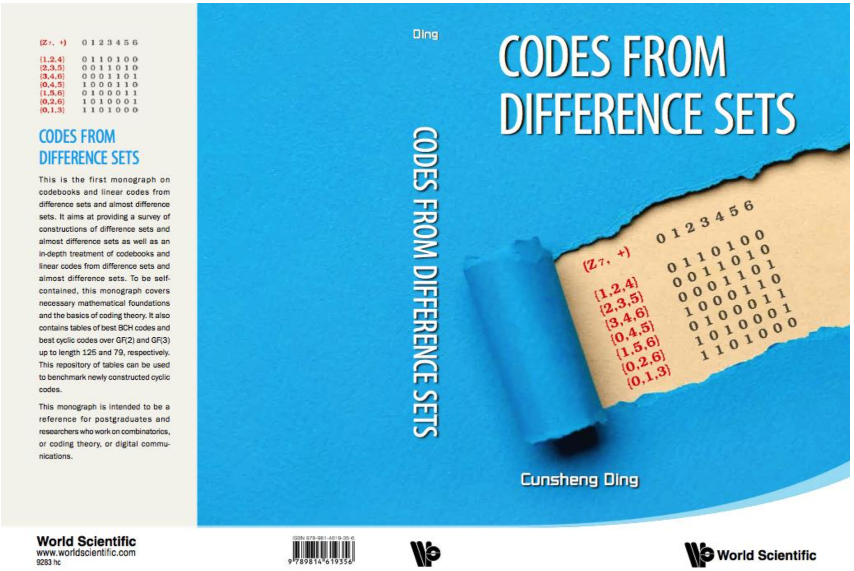
Stream Ciphers and Number Theory

Revised Edition

THOMAS W. CUSICK
CUNSHENG DING
ARI RENVALL

# Research Highlights (3)

- Difference Sets and Codes
- World Scientific, 2014
- Bridging combinatorial designs and codes



| $(\mathbb{Z}_7, +)$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|---|
| {1,2,4} | 0 | 1 | 1 | 0 | 1 | 0 | 0 |
| {2,3,5} | 0 | 0 | 1 | 1 | 0 | 1 | 0 |
| {3,4,6} | 0 | 0 | 0 | 1 | 1 | 0 | 1 |
| {0,4,5} | 1 | 0 | 0 | 0 | 1 | 1 | 0 |
| {1,5,6} | 0 | 1 | 0 | 0 | 0 | 1 | 1 |
| {0,2,6} | 1 | 0 | 1 | 0 | 0 | 0 | 1 |
| {0,1,3} | 1 | 1 | 0 | 1 | 0 | 0 | 0 |

CODES FROM DIFFERENCE SETS

This is the first monograph on codebooks and linear codes from difference sets and almost difference sets. It aims at providing a survey of constructions of difference sets and almost difference sets as well as an in-depth treatment of codebooks and linear codes from difference sets and almost difference sets. To be self-contained, this monograph covers necessary mathematical foundations and the basics of coding theory. It also contains tables of best BCH codes and best cyclic codes over GF(2) and GF(3) up to length 125 and 79, respectively. This repository of tables can be used to benchmark newly constructed cyclic codes.

This monograph is intended to be a reference for postgraduates and researchers who work on combinatorics, or coding theory, or digital communications.

World Scientific
www.worldscientific.com
9283 hc

ISBN 978-981-4619-35-6
9 789814 619356

Ding

CODES FROM DIFFERENCE SETS

CODES FROM DIFFERENCE SETS

(Z7, +) 0 1 2 3 4 5 6
{1,2,4} 0 1 1 0 1 0 0
{2,3,5} 0 0 1 1 0 1 0
{3,4,6} 0 0 0 1 1 0 1
{0,4,5} 1 0 0 0 1 1 0
{1,5,6} 0 1 0 0 0 1 1
{0,2,6} 1 0 1 0 0 0 1
{0,1,3} 1 1 0 1 0 0 0

Cunsheng Ding

World Scientific