ALM 27

Advanced Lectures in Mathematics

Number Theory and Related Area

数论及其相关领域

Editors: Yi Ouyang • Chaoping Xing • Fei Xu • Pu Zhang

高等教育出版社
HIGHER EDUCATION PRESS

ALM 27

Advanced Lectures in Mathematics

Number Theory and Related Area

数论及其相关领域

Shulun Jiqi Xiangguan Lingyu

Editors: Yi Ouyang • Chaoping Xing • Fei Xu • Pu Zhang

高等教育出版社·北京
HIGHER EDUCATION PRESS BEIJING

International Press

图书在版编目（CIP）数据

数论及其相关领域 = Number Theory and Related Area : 英文 / 欧阳毅等主编 . -- 北京 : 高等教育出版社，2013. 3
ISBN 978-7-04-036775-1

Ⅰ. ①数… Ⅱ. ①欧… Ⅲ. ①数论－研究－英文 Ⅳ. ① O156

中国版本图书馆 CIP 数据核字 (2013) 第 020002 号

策划编辑 李华英　　责任编辑 李华英　　封面设计 张申申　　责任校对 陈　杨
责任印制 毛斯璐

出版发行	高等教育出版社	咨询电话	400 - 810 - 0598
社　址	北京市西城区德外大街 4 号	网　址	http://www. hep. edu. cn
邮政编码	100120		http://www. hep. com. cn
印　刷	北京中科印刷有限公司	网上订购	http://www. landraco. com
开　本	787mm × 1092mm　1/16		http://www. landraco. com. cn
印　张	15. 75	版　次	2013 年 3 月第 1 版
字　数	370 千字	印　次	2013 年 3 月第 1 次印刷
购书热线	010 - 58581118	定　价	69. 00 元

物 料 号　36775 - 00

ADVANCED LECTURES IN MATHEMATICS

ADVANCED LECTURES IN MATHEMATICS

(*Executive Editors*: *Shing-Tung Yau, Kefeng Liu, Lizhen Ji*)

1. Superstring Theory (2007)
(Editors: Shing-Tung Yau, Kefeng Liu, Chongyuan Zhu)

2. Asymptotic Theory in Probability and Statistics with Applications (2007)
(Editors: Tze Leung Lai, Lianfen Qian, Qi-Man Shao)

3. Computational Conformal Geometry (2007)
(Authors: Xianfeng David Gu, Shing-Tung Yau)

4. Variational Principles for Discrete Surfaces (2007)
(Authors: Feng Luo, Xianfeng David Gu, Junfei Dai)

5. Proceedings of The 4th International Congress of Chinese Mathematicians Vol. Ⅰ —Vol. Ⅳ (2007)
(Editors: Lizhen Ji, Kefeng Liu, Lo Yang, Shing-Tung Yau)

6. Geometry, Analysis and Topology of Discrete Groups (2008)
(Editors: Lizhen Ji, Kefeng Liu, Lo Yang, Shing-Tung Yau)

7. Handbook of Geometric Analysis Vol. Ⅰ (2008)
(Editors: Lizhen Ji, Peter Li, Richard Schoen, Leon Simon)

8. Recent Developments in Algebra and Related Areas (2009)
(Editors: Chongying Dong, Fu-An Li)

9. Automorphic Forms and the Langlands Program (2009)
(Editors: Lizhen Ji, Kefeng Liu, Shing-Tung Yau)

10. Trends in Partial Differential Equations (2009)
(Editors: Baojun Bian, Shenghong Li, Xu-Jia Wang)

11. Recent Advances in Geometric Analysis (2009)
(Editors: Yng-Ing Lee, Chang-Shou Lin, Mao-Pei Tsui)

12. Cohomology of Groups and Algebraic K-theory (2009)
(Editors: Lizhen Ji, Kefeng Liu, Shing-Tung Yau)

13–14. Handbook of Geometric Analysis Vol. Ⅱ, Ⅲ (2010)
(Editors: Lizhen Ji, Peter Li, Richard Schoen, Leon Simon)

15. An Introduction to Groups and Lattices (2010)
(Author: Robert L. Griess, Jr.)

16. Transformation Groups and Moduli Spaces of Curves (2010)
(Editors: Lizhen Ji, Shing-Tung Yau)

17–18. Geometry and Analysis Vol. Ⅰ, Ⅱ (2010)
(Editor: Lizhen Ji)

19. Arithmetic Geometry and Automorphic Forms (2011)
(Editors: James Cogdell, Jens Funke, Michael Rapoport, Tonghai Yang)

20. Surveys in Geometric Analysis and Relativity (2011)
(Editors: Hubert L. Bray, William P. Minicozzi Ⅱ)

21. Advances in Geometric Analysis (2011)
(Editors: Stanisław Janeczko, Jun Li, Duong H. Phong)

22. Differential Geometry (2012)
(Editors: Yibing Shen, Zhongmin Shen, Shing-Tung Yau)

23. Recent Development in Geometry and Analysis (2012)
(Editors: Yuxin Dong, Jixiang Fu, Guozhen Lu, Weimin Sheng, Xiaohua Zhu)

24–26. Handbook of Moduli Vol. Ⅰ, Ⅱ, Ⅲ (2012)
(Editors: Gavril Farkas, Ian Morrison)

27. Number Theory and Related Area (2013)
(Editors: Yi Ouyang, Chaoping Xing, Fei Xu, Pu Zhang)

ADVANCED LECTURES IN MATHEMATICS

A special volume dedicated to
Professor Keqin Feng

Contents

Number Theory and Related Area
ALM 27, pp. 1–23

Binary Additive Counter Stream Ciphers

Cunsheng Ding*, Wenpei Si†

Abstract

Although a number of block ciphers have been designed and are available in the public domain, they are usually used in one of the four modes: the cipher block chaining mode, the cipher feedback mode, the output feedback mode, and the counter mode. In all these cases, a stream cipher is actually used, as any block cipher used in any of these modes becomes a stream cipher. Stream ciphers are preferred, as they can destroy statistical properties of natural languages to some extent. The objective of this paper is to provide the state-of-the-art of a special type of stream ciphers, called *binary additive counter stream ciphers*, by surveying known results in the literature, deriving design criteria, and presenting experimental results. Two examples of binary additive counter stream ciphers are analysed in details, and are used to illustrate that it is possible to construct a practical stream cipher with many security properties. The security of the two ciphers with respect to known plaintext attacks is proven to be equivalent to the computational complexity of two number-theoretic problems. This is the first time that the security of a cipher with respect to known plaintext attacks is proved to be equivalent to the computational complexity of a mathematical problem.

2000 Mathematics Subject Classification: 11T71, 68P25, 94A55, 94A60.
Keywords and Phrases: Additive synchronous stream ciphers, Counter generator, Difference sets, Highly nonlinear functions.

1 Introduction

Ciphers are classified into stream and block ciphers, depending on whether or not the encryption transformation is time-varying. In most applications, stream ciphers are preferred, as they can destroy statistical properties of natural languages to some extent.

The only cipher which is provably secure in the information sense and simple in structure is the one-time pad, which is not practical for real applications. Ciphers employed in real systems are usually complex in structure and it is thus hard to analyse and prove their security. Two open problems in cryptography are the following:

*Department of Computer Science and Engineering, The Hong Kong University of Science and Technology, Clearwater Bay, Kowloon, Hong Kong, China. Email: cding@cse.ust.hk.
†Department of Computer Science and Engineering, The Hong Kong University of Science and Technology, Clearwater Bay, Kowloon, Hong Kong, China. Email: siwenpei@ust.hk.

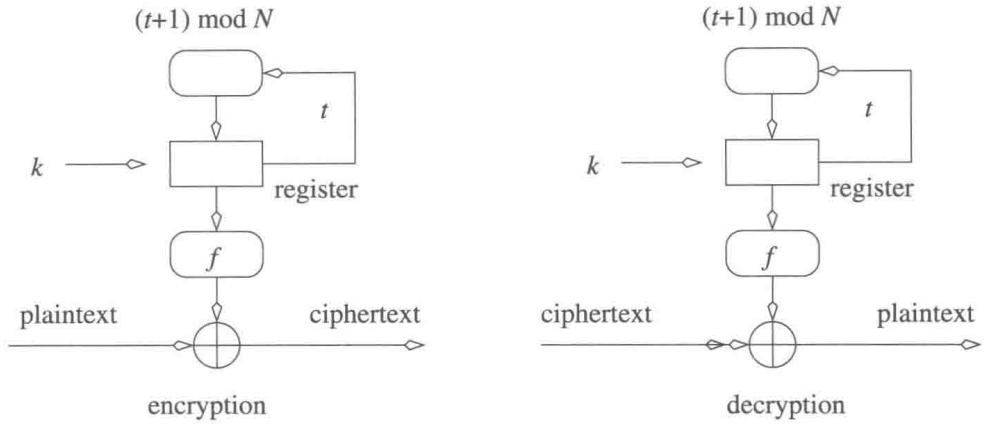

Figure 1: The binary additive counter stream cipher.

1. Is there a practical cipher with provable security in terms of computational complexity?
2. If there is a practical cipher with provable security in terms of computational complexity, how do we design it?

One simple and natural type of stream ciphers is the binary additive counter stream ciphers depicted in Figure 1, where the keystream generator consists of a cyclic counter with period N and a function f from $\mathbb{Z}_N =: \{0, 1, 2, \cdots, N-1\}$ to $\mathbb{Z}_2 := \{0, 1\}$, where N is a huge integer. The cyclic counter has a memory unit and counts the integers in $\mathbb{Z}_N$ cyclically. The initial content of the memory unit of the cyclic counter is the secret key, which could be any integer between 0 and $N-1$. If the secret key is k, the keystream bit k_t at time unit t is then $k_t = f((t+k) \bmod N)$. The encryption of a message bit is the exclusive-or of the message bit and the corresponding keystream bit. The decryption process is the same as the encryption process.

The objectives of this paper are to survey all known results scattered over a number of references and present new ones about the binary additive counter stream ciphers of Figure 1. This is to provide the reader with the state-of-the-art of the binary additive counter stream ciphers. The paper is organized as follows. Section 2 presents a number of design criteria for the binary additive counter stream ciphers depicted in Figure 1. Section 3 documents an example of the binary additive counter stream ciphers, called *Legendre cipher*, and its security properties. Section 4 describes another example of the binary additive counter stream ciphers, called *two-prime cipher*, and its security properties. Section 5 provides information on functions f from $\mathbb{Z}_N$ to $\mathbb{Z}_2$ with optimal nonlinearity p_f which may be employed in the ciphers of Figure 1, and concludes this paper.

In this paper, the security of the Legendre and two-prime ciphers with respect to known plaintext attacks is proven to be equivalent to the computational complexity of two number-theoretic problems. This is the first time that the security of a cipher with respect to known plaintext attacks is proved to be equivalent

to the computational complexity of a mathematical problem.

2 Possible attacks and design criteria

2.1 The linear and sphere complexity attacks and the associated design criteria

2.1.1 The linear complexity attack and the design criterion associated to this attack

Let $z^n = z_0 z_1 \cdots z_{n-1}$ be a sequence of length n over the finite field GF(q). The *linear complexity* (also called the *linear span*) of the sequence z^n is defined to be the smallest nonnegative integer L such that there exist constants $c_1, c_2, \cdots, c_{L-1} \in$ GF(q) for which

$$z_j + c_1 z_{j-1} + \cdots + c_L z_{j-L} = 0, \text{ for all } L \leq j < n. \tag{1}$$

This definition applies also to semi-infinite sequences $z^\infty = z_0 z_1 \cdots$ over GF(q), where $n = \infty$. For an ultimately periodic sequence z^∞ over GF(q), the linear complexity must be a finite number. The corresponding polynomial $1 + c_1 x + c_2 x^2 + \cdots + c_L x^L \in$ GF(q)[x] is called the *minimal polynomial* of the sequence. In engineering terms, the linear complexity is the length of the shortest linear feedback shift register that can produce the sequence, where the minimal polynomial is called the *feedback polynomial* of the linear feedback shift register (LFSR).

If the linear complexity of the output sequence of the counter generator is L, then $2L$ consecutive output bits of the counter generator can be used to construct an LFSR of length L that produces the same keystream sequence. The equivalent LFSR can be constructed using the Berlekamp-Massey algorithm or by solving a system of linear equations. Hence, the keystream sequence of an additive synchronous stream cipher must have large linear complexity.

Design Criterion 1. *The linear complexity of the keystream sequence of the binary additive counter stream cipher in Figure* 1 *should be large.*

2.1.2 The linear complexity stability attack and the associated design criterion

Although the linear complexity of a keystream sequence may be very large, there might be another sequence with very low linear complexity such that the Hamming distance between the two sequences is very small. If this is the case, one can use the sequence with low linear complexity to approximate the original keystream sequence. In other words, in this case one can construct an LFSR with short length to approximate the original keystream generator.

If changing a small number of entries in a sequence decreases the linear complexity of the sequence to a large extent, we say that the linear complexity of the original sequence is not stable. The linear complexity stability issue was observed in 1989 ([7]) and a measure of the linear stability (called *weight complexity*) was

introduced there. Shortly afterwards, the sphere complexity for both finite and periodic sequences was introduced in the monograph [16], as a measure of the linear complexity stability.

Let x^n be a sequence of length n over GF(q), and let ℓ be any integer with $0 < \ell < n$. The *sphere complexity* of x^n is defined to be

$$\mathrm{SC}_\ell(x^n) = \min_{0<W_H(y^n)\le \ell} \mathrm{LC}(x^n + y^n),$$

where y^n is any sequence of length n over GF(q), $W_H(y^n)$ denotes the Hamming weight of y^n, and $\mathrm{LC}(x^n)$ is the linear complexity of the sequence x^n.

Let x^∞ be a sequence of period n (not necessarily the least period) over GF(q), and let ℓ be any integer with $0 < \ell < n$. The *sphere complexity* of x^∞ is defined to be

$$\mathrm{SC}_\ell(x^\infty) = \min_{\substack{\mathrm{Per}(y^\infty)=n \\ 0<W_H(y^n)\le \ell}} \mathrm{LC}(x^\infty + y^\infty),$$

where y^n denotes the first periodic segment of the sequence y^∞ over GF(q), $\mathrm{Per}(x)$ is the period of x, and $\mathrm{LC}(x^\infty)$ is the linear complexity of the sequence x^∞.

The sphere complexity was introduced in 1991 in [16], two years earlier than the ℓ-error linear complexity, which is defined to be $\min\{\mathrm{LC}(x^\infty), \mathrm{SC}_\ell(x^\infty)\}$. Clearly, the ℓ-error linear complexity is nothing new, but the minimum of the two earlier measures: linear complexity and sphere complexity.

Based on the linear complexity stability, the best affine approximation (BAA) attack on certain stream ciphers was developed in [16, Chapter 3]. For the binary additive counter stream ciphers of Figure 1, one can construct an LFSR to approximate the original keystream cipher if the sphere complexity $\mathrm{SC}_\ell(s^\infty)$ of the keystream sequence is small for small ℓ. Hence, another design requirement is that the sphere complexity $\mathrm{SC}_\ell(s^\infty)$ of the keystream sequence of the binary additive counter stream ciphers should be large enough for small ℓ.

Design Criterion 2. *The sphere complexity* $\mathrm{SC}_\ell(s^\infty)$ *of the keystream sequence of the binary additive counter stream ciphers in Figure* 1 *should be large enough for small* ℓ.

2.1.3 The control of the linear and sphere complexity

The linear complexity and sphere complexity of periodic sequences can be controlled easily as follows [9].

Proposition 1. ([9]) *Suppose* $N = p_1^{e_1} \cdots p_t^{e_t}$, *where* $p_1, \cdots, p_t$ *are* t *pairwise distinct primes, and* q *is a power of a prime such that* $\gcd(q, N) = 1$. *Then for each nonconstant sequence* x^∞ *of period* N *over* GF(q),

$$\mathrm{LC}(x^\infty) \ge \min\{\mathrm{ord}_{p_1}(q), \cdots, \mathrm{ord}_{p_t}(q)\},$$
$$\mathrm{SC}_k(x^\infty) \ge \min\{\mathrm{ord}_{p_1}(q), \cdots, \mathrm{ord}_{p_t}(q)\}, \text{ if } k < \min\{W_H(x^N), N - W_H(x^N)\},$$

where $W_H(x^N)$ *denotes the Hamming weight of the first periodic segment* x^N *of the sequence* x^∞, *and* $\mathrm{ord}_{p_i}(q)$ *is the order of* q *modulo* p_i.