Review of the book

"Chaos-Based Cryptography"
edited by Ljupco Kocarev & Shiguo Lian
Springer, 2011

ISBN: 978-3-642-20541-5

S.V.Nagaraj
RMK Engineering College

1 Summary of the review

Conventional cryptography based on number theory has been well studied by mathematicians and complexity theory specialists. Non-conventional cryptography such as cryptography based on chaos is being increasingly looked upon as an alternative. This review is about a book on chaos-based cryptography. The book has eleven chapters contributed by experts working on chaotic systems and their applications to cryptography.

2 Summary of the book

Chaos-based cryptography is a new research field that encompasses non-linear dynamical systems and the art of analyzing codes and ciphers. This book on chaos-based cryptography includes contributions by experts from all over the world. The book has eleven chapters that focus on key concepts, problems that have to be overcome, and emergent technologies.

Chapter 1 (Introduction to chaos)

The authors of this chapter introduce the readers to the fundamentals of non-linear dynamics and chaos so that the succeeding chapters may be understood without much difficulty. Their basic assumption is that applications frequently use complex and often chaotic sequences generated by discrete dynamical systems.

Chapter 2 (Chaos-based public-key cryptography)

The chapter presents an overview of the state of the art in the area of chaos-based public-key cryptography. It demonstrates that algorithms such as RSA and ElGamal when they employ Chebyshev polynomials on integers are secure whereas cryptosystems which make use of real numbers are insecure.

Chapter 3 (Digitized chaos for pseudo-random number generation in cryptography)

The chapter studies the design of pseudo random number generators based on non-linear congruences. For this purpose, certain chaotic systems are taken as a reference.

Chapter 4 (Formation of high-dimensional chaotic maps and their uses in cryptography)

In this chapter, two approaches are described for the formation of high-dimensional chaotic maps and their dynamical characteristics are studied. The potency of high-dimensional chaotic maps in cryptography is affirmed.

Chapter 5 (Chaos-based hash function)

This chapter focuses on the construction of hash functions based on chaos. The authors conclude that the use of chaos for constructing hash functions is promising and is attracting a lot of attention.

Chapter 6 (Chaos-based video encryption algorithms)

This chapter discussed the application of chaos for designing video encryption algorithms. The benefits of chaos-based algorithms for encrypting video content are highlighted. The performance of the algorithms is evaluated and challenges and open problems are discussed.

Chapter 7 (Cryptanalysis of chaotic ciphers)

Cryptanalysis is quite essential for estimating the strength of a cipher. This also applies to ciphers based on chaos. In this chapter, the power of algebraic attacks on a number of chaotic encryption algorithms is illustrated.

Chapter 8 (Lessons learnt from the cryptanalysis of chaos-based ciphers)

The authors study the main problems associated with chaos-based cryptography. This includes problems with the selection of the chaotic system, problems with the architecture used for encryption, and problems in implementation. As a result of studying these problems, the authors come up with design rules to overcome them.

Chapter 9 (Hardware implementation of chaos-based cipher: Design of embedded systems for security applications)

This chapter studies the design and implementation of 3D chaotic systems in embedded applications. The chapter discusses the Runge-Kutta numerical method for resolving chaotic system requirements. It also describes the Lorentz's chaotic system as implemented on a FPGA chip.

Chapter 10 (Hardware implementation of chaos-secured optical communication systems)

This chapter studies the implementation and performance of optical communication systems based on chaos. The focus is on security at the physical layer. Ultra-fast physical random number generators based on chaotic optical signals and their scope in secure communication systems is also studied.

Chapter 11 (Performance evaluation of chaotic and conventional encryption on portable and mobile platforms)

This chapter studies the performance of various encryption schemes including AES and chaotic encryption on different architectures. The study reveals that chaos-based schemes outdo AES implementations in terms of CPU usage, encryption speed, and energy consumption. Thus chaos-based schemes are suitable for portable and mobile platforms where there are constraints such as limited battery power and processing power.

3 What is the book like (style)?

This book published under the series "Studies in Computational Intelligence" of Springer includes eleven interesting and well-written chapters authored by experts from all over the world. Although the chapters have been written by various authors, there is homogeneity and focus. The book clearly explains the theory, algorithms, and applications related to chaos-based cryptography. The description is thorough and the focus is on recent work in the area. Open problems and emerging technologies are highlighted in the book. The book has numerous illustrations many of which are in color. An e-book version of the book is also available. The editors of the book have done a good job in producing this book which is timely. The work of the editors and authors has been cited by numerous researchers. As chaos-based cryptosystems do not have their foundations in number theory, mathematicians, cryptographers, and complexity theory experts are quite skeptical about using such systems as proving the security and computational complexity becomes difficult or even impossible.

4 Would you recommend this book?

The book will be useful for researchers, security experts, practitioners, students, faculty, law enforcement officers, and others who intend to understand, use, and experiment with chaos-based cryptography. I strongly recommend this book as a valuable reference on applications of chaos theory to cryptography.

The reviewer is a professor of Computer Science and Engg. at RMK Engg. College, Kavaraipettai, India