



SpringerBriefs on Cyber Security Systems and Networks


Editor-in-Chief


Yang Xiang, Digital Research & Innovation Capability Platform, Swinburne University of Technology Digital Research & Innovation Capability, Hawthorn, VIC, Australia

Series Editors

Liqun Chen , Department of Computer Science, University of Surrey Department of Computer Science, Guildford, Surrey, UK

Kim-Kwang Raymond Choo , Department of Information Systems, University of Texas at San Antonio, San Antonio, TX, USA

Sherman S. M. Chow , Department of Information Engineering, the Chinese University of Hong Kong Department of Information Engineering, Hong Kong, Hong Kong


Robert H. Deng , School of Information Systems, Singapore Management University School of Information Systems, Singapore, Singapur, Singapore

Dieter Gollmann, E-15, TU Hamburg-Harburg E-15, Hamburg, Hamburg, Germany

Kuan-Ching Li, Department of Computer Science & Information Engineering, Providence University, Taichung, Taiwan

Javier Lopez, Computer Science Dept., University of Malaga Computer Science Dept., Malaga, Spain

Kui Ren, University at Buffalo null, Buffalo, NY, USA

Jianying Zhou , Infocomm Security Dept, Inst for Infocomm Research Infocomm Security Dept, Singapore, Singapore

The series aims to develop and disseminate an understanding of innovations, paradigms, techniques, and technologies in the contexts of cyber security systems and networks related research and studies.

It publishes thorough and cohesive overviews of state-of-the-art topics in cyber security, as well as sophisticated techniques, original research presentations and in-depth case studies in cyber systems and networks. The series also provides a single point of coverage of advanced and timely emerging topics as well as a forum for core concepts that may not have reached a level of maturity to warrant a comprehensive textbook.

It addresses security, privacy, availability, and dependability issues for cyber systems and networks, and welcomes emerging technologies, such as artificial intelligence, cloud computing, cyber physical systems, and big data analytics related to cyber security research. The mainly focuses on the following research topics:

Fundamentals and theories

- Cryptography for cyber security
- Theories of cyber security
- Provable security

Cyber Systems and Networks

- Cyber systems security
- Network security
- Security services
- Social networks security and privacy
- Cyber attacks and defense
- Data-driven cyber security
- Trusted computing and systems

Applications and others

- Hardware and device security
- Cyber application security
- Human and social aspects of cyber security

More information about this series at <http://www.springer.com/series/15797>

Chandra Sekhar Mukherjee ·
Dibyendu Roy · Subhamoy Maitra

Design and Cryptanalysis of ZUC

A Stream Cipher in Mobile Telephony



Springer

Chandra Sekhar Mukherjee
Indian Statistical Institute
Kolkata, West Bengal, India

Dibyendu Roy
Indian Statistical Institute
Kolkata, West Bengal, India

Subhamoy Maitra
Applied Statistics Unit
Indian Statistical Institute
Kolkata, West Bengal, India

ISSN 2522-5561 ISSN 2522-557X (electronic)
SpringerBriefs on Cyber Security Systems and Networks
ISBN 978-981-33-4881-3 ISBN 978-981-33-4882-0 (eBook)
<https://doi.org/10.1007/978-981-33-4882-0>

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2021

This work is subject to copyright. All rights are solely and exclusively licensed by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Singapore Pte Ltd.
The registered company address is: 152 Beach Road, #21-01/04 Gateway East, Singapore 189721, Singapore

*To grown-ups,
who plan to learn cryptology as science.*

Foreword

I am delighted to introduce the first complete book on ZUC, one of the recent and widely deployed stream ciphers in Mobile Telephony. Needless to mention that cryptology as a subject is now completely matured. There are a number of excellent books in the domain of general cryptology, or in the well-studied areas like public key cryptosystem or block cipher design and analysis. While there are outstanding research papers regularly appearing in design and analysis of stream ciphers, we still have a dearth of good monographs in this field. In this backdrop, I warmly welcome a dedicated book on the ZUC stream cipher.

This brief document of around a hundred pages has nicely assimilated all the results to make it a complete treatise on ZUC. This cipher is used to encrypt a good proportion of traffic in mobile communication and is believed to be widely used in China. The present book not only explains this stream cipher but also describes where it is placed in the broad spectrum of mobile telephony. Thus, I believe this book will be widely accepted as an important independent monograph for theory and practice in the domain of cryptology. Both students and experienced researchers should benefit from this book.

The book is written by three authors. Chandra Sekhar is presently an M. Tech. (Computer Science) student, Dibyendu is a postdoctoral research fellow and Subhamoy is a senior professor at the Indian Statistical Institute, Kolkata. That is why, this book has a fair blend of student's view, researcher's analysis and

teacher's explanation toward understanding a rather advanced subject in a simpler way. I sincerely wish this book will attract serious attention in the domain of Cryptology, Security and Communication as a whole.

Kolkata, India
March 2020

Bimal Roy
Padmasree Awardee
Professor, Indian Statistical Institute
Head, R C Bose Centre for Cryptology and Security
Chairman, National Statistical Commission, India
Founder & Secretary, Cryptology Research Society of India
Former Director, Indian Statistical Institute

Preface

ZUC is a stream cipher which is used to encrypt communications in mobile networks. The basic idea of a stream cipher is simple. This is actually a methodology, where an initial seed will be provided and, in turn, it will generate a stream of data which looks random. However, this is not truly random as the same seed will always generate the same stream if the algorithm is deterministic and the machine is classical. This stream is mixed with plaintext for encryption. The encrypted text is communicated through an open channel with the understanding that no unauthorized third party will be able to decrypt it. On the other hand, the receiver will have the same secret key (the seed) and thus (s)he will be able to generate the same keystream. Then re-mixing the stream and the ciphertext, the plaintext will be recovered. That is, one may immediately understand that the cryptographic security of the whole system primarily depends on the secrecy of the seed (secret key). However, if the stream cipher is not designed properly, or if the complete protocol of data transfer is not properly evaluated, then there may be other problems that might compromise the security. Thus, we have to take care of two issues. One, the proper design of stream cipher, and two, a detailed evaluation of the complete protocol. In this book, we take care of both the issues. While we look at the cipher from cryptographic point of view (more mathematical), at the same time, we present how the stream cipher is placed in the infrastructure of mobile telephony (less mathematical, but an architectural point of view).

ZUC is a stream cipher proposed and designed by China, but it must be mentioned that the cipher was evaluated publicly in the international domain. The design of this cipher was initiated in the first decade of this millennium. In fact, the third author of this book (Subhamoy Maitra) was invited to the first International Workshop on ZUC algorithm during December 2–3, 2010, Beijing, China. Since then, the cipher has experienced several evaluations, certain weaknesses have been identified and the present version, ZUC 1.6 with 128-bit secret key, is believed to be secure. However, being one of the ciphers used in the commercial domain of mobile telephony, it attracts continuous evaluation of the cryptologic community. This should be mentioned that the term ‘cryptanalysis’ does not mean a complete break of a cipher without knowing the secret key. Cryptanalysis means the detailed

evaluation of the cipher using cryptologic techniques. In this book, we explain all the known cryptanalytic results on this cipher.

For analyzing the cipher, we primarily need substantial mathematical background. This is presented in the first introductory chapter. The second chapter is less mathematical, that discusses the mobile telephony architecture and where exactly ZUC is placed in that hierarchy. The experts in the domain of Cryptology and Security may selectively skip the materials of the first two chapters. Chapter 3 provides complete mathematical design and software implementation details (using C programming language) of the ZUC stream cipher. This is the core description of the cipher, that needs to be studied deeply to understand the strength and weaknesses of ZUC. Needless to mention, that the present version ZUC 1.6 does not have any weakness known so far in the public domain. This chapter also discusses how, based on ZUC, the confidentiality and integrity algorithms are implemented in mobile telephony standards such as 3GPP. The last technical chapter (Chap. 4) provides a detailed analysis in terms of the weaknesses of the stream cipher in the earlier version ZUC 1.4. It is very important to understand the details as the users need to be convinced that the present version is indeed secure and there is no obvious trap-door. We conclude this brief document in Chap. 5 with directions toward the future analysis of this cipher.

The readers of this book should have mathematical knowledge at the undergraduate level. However, the first chapter of this book presents the necessary mathematical background so that engineers with good high school-level knowledge can also access this document. A basic background in computer science is necessary with some hands-on experience in C programming. The book supplements all the mathematical details with implementation using C programs. This book does not expect any formal background on cryptology, though basic knowledge in this domain will indeed be an added advantage. This book is targeted toward students and researchers of any science and engineering discipline, and to engineers and professionals who work in the broad field of communication.

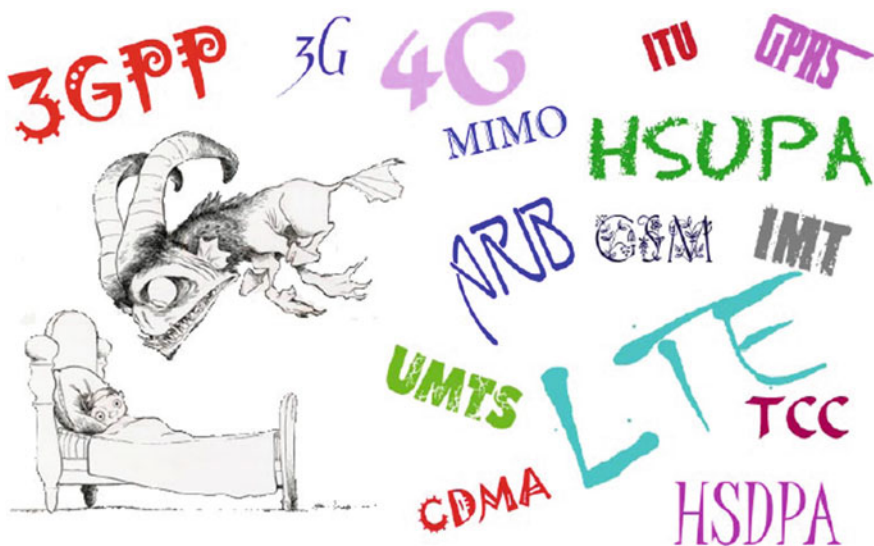
Before proceeding further, let us enumerate what is expected from this book.

- This book is a timely report of state-of-the-art analytical techniques in the domain of stream cipher design and analysis with a specific cipher, namely ZUC, in mind.
- This brief document provides a link between new research results and a brief contextual literature review in the domain of complex LFSR-based stream ciphers.
- This draft presents a snapshot of how stream ciphers are deployed in the mobile telephony architecture, one of the most well-known topics for more than half a century in the domain of computer and communication sciences.
- We provide an in-depth study on design and cryptanalysis of ZUC as well as relevant research results in this field.
- This book is a presentation of core concepts toward design and analysis of stream ciphers that involve a basic understanding of electronic circuits such as LFSRs with abstract mathematical objects such as primitive polynomials over finite fields. At the same time, this draft moves forward to explain a very

complex design of a state-of-the-art commercial stream cipher that is implemented in billions of mobile equipments around the world (mostly in China). The research students as well as professional engineers should understand and be aware of the complete timeline and technical know-how in order to make independent contributions in this domain.

A book contains the name of the authors, but we all know that this is actually assimilation of the continuous effort of many people who are continuously working around. We like to acknowledge our family members, co-researchers and friends in this regard. Without their support, this document could not be prepared. We also like to thank our institute, the Indian Statistical Institute. This is needless to mention how prominent this institute is in academic area. At the same time, the kind of academic independence we enjoy in this institute is un-parallel. In this regard, we must thank the Government of India for continuous support toward our research through different departments and agencies. Finally, all the authors like to acknowledge the project (2016–2021) “Cryptography & Cryptanalysis: How far can we bridge the gap between Classical and Quantum Paradigm”, awarded to the third author (Subhamoy Maitra) by the Scientific Research Council of the Department of Atomic Energy (DAE-SRC), the Board of Research in Nuclear Sciences (BRNS). Additionally, we would also like to thank Pranab Chakraborty of Wipro Limited as well as Pinakpani Pal and Manmatha Roy of Indian Statistical Institute for improving the quality of the text with valuable suggestions and comments.

As we have pointed out, the third author of this book (Subhamoy Maitra) was a participant in the first International Workshop on ZUC. He cherishes the two initial slides of that presentation a decade back (credit to Dr. Sourav SenGupta, who was Subhamoy’s research student at that point of time).



At that time, it was perceived that Cryptology might be an easier subject to handle than the gamut of mobile telephony.



Lets stick to Cryptography



Thus, only cryptology was discussed in the presentation 10 years back. Time flows, and after a decade, we plan to understand the basic framework of mobile telephony too.

We sincerely wish that the readers will enjoy flipping through the pages of this brief document.

Kolkata, India
March 2020

Chandra Sekhar Mukherjee
Dibyendu Roy
Subhamoy Maitra

Contents

1	Introduction and Preliminaries	1
1.1	Introduction	1
1.2	Symmetric Key Cryptosystem	2
1.3	Prerequisites	4
1.3.1	Finite Fields	4
1.3.2	Field Extension	6
1.3.3	LFSR-Based Stream Cipher	9
1.4	Nonlinear Combiner and Filter Generator Model	13
1.5	Cryptographic Properties of Boolean Function	14
1.6	Overview on 3GPP and Where ZUC Stands	20
1.6.1	ZUC	21
1.7	Confidentiality and Integrity Using Stream Cipher	22
	References	24
2	Telephony Architecture	27
2.1	Outline of Security Protocols	27
2.2	The Architecture of the Different Generations	27
2.2.1	GSM/2G	28
2.2.2	UMTS/3G	31
2.2.3	LTE/4G Architecture	35
2.2.4	New Radio (NR)/5G	37
	References	41
3	Design Specification of ZUC Stream Cipher	43
3.1	Structure of ZUC	43
3.1.1	Linear Feedback Shift Register of ZUC	44
3.1.2	Bit Reorganization Layer of ZUC	45
3.1.3	Nonlinear Function of ZUC (F)	46
3.2	Working Principle of ZUC 1.4	48
3.3	Differences Between ZUC 1.4 and ZUC 1.6	54

3.4	Confidentiality Algorithm Using ZUC	55
3.4.1	Initialization Phase	56
3.4.2	Keystream Generation Phase	57
3.4.3	Encryption/Decryption Phase	57
3.5	Integrity Algorithm	58
3.5.1	Initialization Phase	58
3.5.2	Keystream Generation Phase	59
3.5.3	Generation of MAC	59
3.6	Description of ZUC-256	60
3.6.1	Generation of MAC in ZUC-256	61
	References	62
4	Cryptanalysis on ZUC 1.4	63
4.1	Analysis of ZUC	63
4.1.1	Analysis of the S-Box	63
4.1.2	Reversibility of ZUC	65
4.2	Differential Attack on ZUC 1.4	75
4.2.1	Difference in the First Byte of IV	77
4.2.2	Difference in the Second Byte of IV	84
4.3	Forgery Attack on EIA-128	84
4.3.1	Methodology of the Forgery Attack	85
	References	87
5	Concluding Remarks	89
	References	91
	Appendix: Test Vectors for ZUC	93
	Index	97

About the Authors

Chandra Sekhar Mukherjee is currently pursuing M.Tech in Computer Science in Indian Statistical Institute (ISI). He received his B.Tech degree in Computer Science from Heritage Institute of Technology, Kolkata, India in 2019. He was introduced to the field of Cryptology during his internship under the supervision of Prof. Subhamoy Maitra prior to his admission to ISI. The deep connection between probability, combinatorics and number theory that led to the fine line between randomness and bias deeply intrigued him in the domain of Cryptology. Currently his areas of research interest are Cryptology, Quantum Algorithms and Analysis of Boolean Functions. Being in the formative years of his research career, he wishes to contribute in the broad area of secure communication in a meaningful way.

Dr. Dibyendu Roy is a postdoctoral research fellow at the Indian Statistical Institute, Kolkata, India. He obtained his Ph.D. and M.Sc. in Mathematics from the Indian Institute of Technology Kharagpur, India. Earlier, he was a consultant at ERTL (E), STQC, Kolkata, India, and worked in the domain of security analysis. He was also a postdoctoral fellow at the National Institute of Science Education and Research, India, for two years. His primary research area is cryptology, more specifically the domain of symmetric ciphers. His research articles have been published in journals of repute.

Prof. Subhamoy Maitra is Professor at the Indian Statistical Institute (ISI), Kolkata, India. He received his Ph.D. in computer science from the ISI, Kolkata. He holds a M.Tech. in Computer Science from the ISI, Kolkata, and B.Tech. in Electronics and Telecommunications Engineering from Jadavpur University, Kolkata, India. After working briefly in the domain of hardware and software engineering, he joined the ISI, Kolkata, as a faculty in 1997. He has authored several books and around 200 research papers in various fields of cryptology and quantum information.

Notations

0_n	String of zeros of length n .
1_n	String of ones of length n .
$Pr[X]$	Probability of an event X .
\oplus	Addition modulo 2 i.e., logical XOR operation.
\oplus_n	Bitwise \oplus between two n -bit strings.
$a b$	Logical OR operation between a, b .
\bar{x}	Complement of x , i.e., $1 \oplus x$.
$\mathbf{0}$	Zero vector.
\mathbf{x}	A bit string of certain length.
$a \parallel b$	Concatenation of a and b .
$\#S, S $	The number of elements of a set S .
$\gcd(a, b)$	Greatest common divisor of a, b .
$ x $	Absolute value of an integer x .
$GF(2)$	Field with $\{0, 1\}$, addition and multiplication modulo 2 operation.
$x \lll_n b$	Left rotate by b bits of the n -bit integer x .
$a \gg t$	Right shift of the integer a by t bits.
$a \ll t$	Left shift of the integer a by t bits.
\boxplus	Addition modulo 2^{32} .
abc_2	Binary representation of a positive integer.
abc_{16}	Hexadecimal representation of a positive integer.
$\lceil x \rceil$	The smallest integer not less than x .
x, \tilde{x}	x, \tilde{x} differ at certain bit/byte positions.
Δx_i	Denotes difference at i -th bit/byte between two bit/byte strings.
$a \equiv b \bmod n$	n divides $(b - a)$
$wt(S)$	Total number of 1's present in a bit string S .
\mathcal{B}_n	Set of all n -variable Boolean function.
$L(n)$	Set of all n -variable linear Boolean function.

A_H	Most significant half of bit/byte string A .
A_L	Least significant half of bit/byte string A .
A_{iL}	Least significant i bits of bit string A .
A_{iH}	Most significant i bits of bit string A .