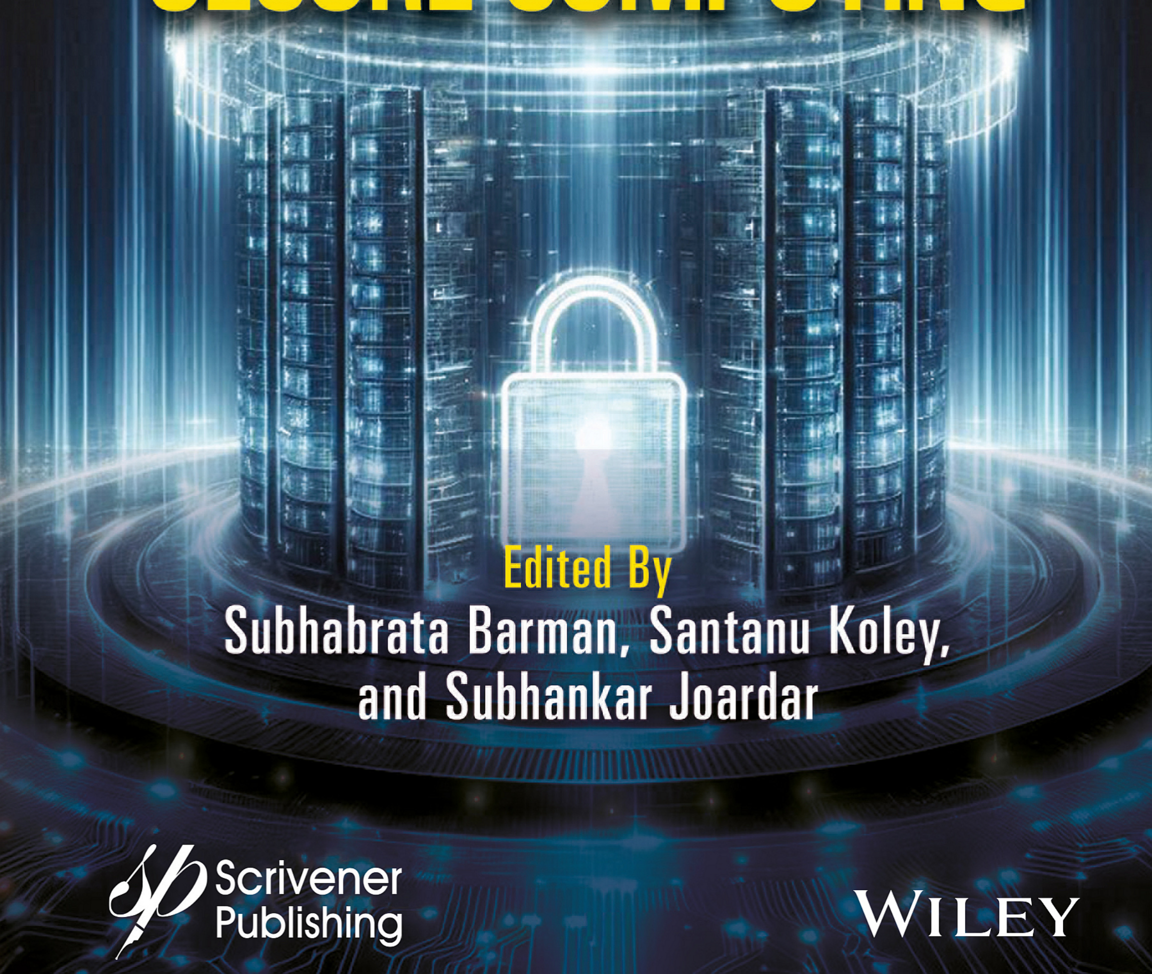
ADVANCES IN CYBER SECURITY

NEXT-GENERATION SYSTEMS AND SECURE COMPUTING



Edited By

Subhabrata Barman, Santanu Koley, and Subhankar Joardar

Scrivener Publishing

WILEY

Next-Generation Systems and Secure Computing

Scrivener Publishing
100 Cummings Center, Suite 541J
Beverly, MA 01915-6106

Advances in Cyber Security

Series Editors: Rashmi Agrawal and D. Ganesh Gopal

Scope: The purpose of this book series is to present books that are specifically designed to address the critical security challenges in today's computing world including cloud and mobile environments and to discuss mechanisms for defending against those attacks by using classical and modern approaches of cryptography, blockchain and other defense mechanisms. The book series presents some of the state-of-the-art research work in the field of blockchain, cryptography and security in computing and communications. It is a valuable source of knowledge for researchers, engineers, practitioners, graduates, and doctoral students who are working in the field of blockchain, cryptography, network security, and security and privacy issues in the Internet of Things (IoT). It will also be useful for faculty members of graduate schools and universities. The book series provides a comprehensive look at the various facets of cloud security: infrastructure, network, services, compliance and users. It will provide real-world case studies to articulate the real and perceived risks and challenges in deploying and managing services in a cloud infrastructure from a security perspective. The book series will serve as a platform for books dealing with security concerns of decentralized applications (DApps) and smart contracts that operate on an open blockchain. The book series will be a comprehensive and up-to-date reference on information security and assurance. Bringing together the knowledge, skills, techniques, and tools required of IT security professionals, it facilitates the up-to-date understanding required to stay one step ahead of evolving threats, standards, and regulations.

Publishers at Scrivener
Martin Scrivener (martin@scrivenerpublishing.com)
Phillip Carmical (pcarmical@scrivenerpublishing.com)

Next-Generation Systems and Secure Computing

Edited by

Subhabrata Barman

Santanu Koley

and

Subhankar Joardar

Scrivener Publishing

WILEY

This edition first published 2025 by John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, USA and Scrivener Publishing LLC, 100 Cummings Center, Suite 541J, Beverly, MA 01915, USA

For more information about Scrivener publications please visit www.scrivenerpublishing.com.

Wiley Global Headquarters
111 River Street, Hoboken, NJ 07030, USA

For details of our global editorial offices, customer services, and more information about Wiley products visit us at www.wiley.com.

Library of Congress Cataloging-in-Publication Data

ISBN 978-1-394-22826-3

Front cover images supplied by Adobe Firefly
Cover design by Russell Richardson

Set in size of 11pt and Minion Pro by Manila Typesetting Company, Makati, Philippines

Printed in the USA

10 9 8 7 6 5 4 3 2 1

Contents

Preface

The rapid evolution of technology has brought us to an era where the convergence of systems, computing, and security is no longer an isolated domain, but an integral aspect of every facet of our digital lives. From advanced data analytics and machine learning to decentralized systems and cloud computing, we are witnessing a profound transformation in how we interact with technology, communicate, and conduct business.

Next-Generation Systems and Secure Computing represent the frontier of this digital revolution, shaping not only how we develop and deploy technology, but also how we protect it. The growing complexity of modern systems demands innovative approaches to both functionality and security, ensuring resilience against increasingly sophisticated threats. As we integrate more sophisticated algorithms, artificial intelligence, and distributed architectures into our systems, the stakes in safeguarding data and infrastructure have never been higher.

This book provides an in-depth exploration of these critical topics, with contributions from leading experts in the fields of systems design, cyber security, and computational theory. It offers a comprehensive look at the cutting-edge technologies that are defining the next generation of secure computing systems, from block chain and quantum computing to advanced cryptography and AI-driven security protocols.

By addressing both the theoretical underpinnings and practical applications of secure computing in modern systems, this book aims to equip researchers, practitioners, and students with the knowledge and tools to tackle the challenges of tomorrow's digital ecosystem. The chapters presented here cover a broad spectrum of topics, from the evolution of security paradigms to novel approaches in securing data, communications, and infrastructures.

The following research topics are well covered in this book:

Video Steganography
Watermarking
Malware Analysis
Cryptography

Cybersecurity and Block Chain
Cybersecurity and law
Secured Communication Systems
Security in Wireless Networks
Security in IoT Systems
Security in Mobile Crowd Sensing
Multimedia Security
Sentiment Analysis in Social Media

We believe that the integration of security at the very foundation of system design, coupled with the innovative solutions presented in this work, will lay the groundwork for the development of resilient, trustworthy, and future-proof systems. As we look ahead to a world increasingly reliant on interconnected technologies, the need for secure, efficient, and scalable computing systems has never been more urgent.

We hope this book serves as both a valuable reference and an inspiring resource for the next generation of technologists, researchers, and innovators working at the intersection of systems engineering and secure computing. Together, we can build a safer, more robust digital future.

1

Yet Another Move Towards Securing Video Using Sudoku-Fernet

Sunanda Jana[1], Swarnajit Bhattacharya[1], Mrinmoy Sen[1*], Abhinandan Khan[2], Arnab Kumar Maji[3] and Rajat Kumar Pal[2]

[1]Haldia Institute of Technology, WB, India
[2]University of Calcutta, Kolkata, India
[3]North-Eastern Hill University, Meghalaya, India

Abstract
In this era of digital communication and multimedia content sharing, ensuring the security and privacy of sensitive video data is of utmost importance. Symmetric key encryption is a widely used technique for securing video content; however, the generation of secure and unpredictable encryption keys remains a challenge. This study proposes a novel approach that employs Sudoku puzzles as a mechanism for generating symmetric keys. Then, by passing the key through fernet module, the Sudoku-Fernet cipher key was extracted for video encryption. The Sudoku puzzle's inherent properties of uniqueness, complexity, and nonlinearity make it an ideal candidate for key generation. The proposed method combines the strength of the Giant Sudoku instance of size 25 × 25 with a cryptographic fernet module to enhance the security of video encryption systems, offering an innovative solution to protect sensitive video content without affecting cost and time.

***Keywords*:** Symmetric key, fernet, sudoku-fernet cipher key, video encryption, security

1.1 Introduction

Sudoku puzzle [1] is a popular logic-based number-placement game that has gained worldwide popularity. Its structure consists of an $n \times n$ square

**Corresponding author*: mrinmoy.sen@gmail.com

Subhabrata Barman, Santanu Koley and Subhankar Joardar (eds.) Next-Generation Systems and Secure Computing, (1–16) © 2025 Scrivener Publishing LLC

grid, containing some clues as preassigned, forming a Sudoku puzzle, where n is an integer and $\sqrt{n}$ is an integer. Thus, minigrids are formed with size $\sqrt{n} \times \sqrt{n}$. In each minigrid, each integer between 1 and n appears only once. Standard Sudoku consists of a 9 × 9 grid divided into nine 3 × 3 subgrids. The goal is to fill in the empty cells with digits from 1 to 9, ensuring that each row, column, and subgrid contains every digit exactly once. Sudoku puzzles can be of various sizes and configurations beyond the classic 9 × 9 grid. Some common Sudoku types are based on different grid sizes [10]:

1. **Classic 9 × 9 Sudoku:** This is the standard version of Sudoku, where the puzzle is presented on a 9 × 9 grid divided into nine 3 × 3 subgrids. The objective is to fill in the grid such that each row, column, and 3 × 3 subgrid contains numbers 1 through 9 with no repetition.
2. **Mini Sudoku (4 × 4):** In Mini Sudoku, the puzzle is played on a 4 × 4 grid, divided into four 2 × 2 subgrids. Each row, column, and 2 × 2 subgrid contain numbers 1 through 4.
3. **6 × 6 Sudoku:** In 6 × 6 Sudoku, the grid is 6 × 6 in size and is divided into six 2 × 3 subgrids. Each row, column, and 2 × 3 subgrid must contain numbers 1–6.
4. **Samurai Sudoku:** Samurai Sudoku is a variant that consists of five overlapping 9 × 9 grids. The objective is to fill in the entire arrangement so that each row, column, and 3 × 3 subgrid in each of the five grids contains numbers 1–9.
5. **Hyper Sudoku (4 × 4 regions):** Hyper Sudoku uses a 9 × 9 grid, but the subgrids are irregular and can have different shapes. In addition, there were four 2 × 2 subregions within the grid. The objective was the same as that of the classic Sudoku.
6. **Giant Sudoku:** Giant Sudoku puzzles have larger grids, often ranging from 12 × 12 to 25 × 25, or even larger. Larger grid sizes provide more challenging puzzle-solving experience.
7. **Diagonal Sudoku:** In Diagonal Sudoku, along with the usual rows, columns, and 3 × 3 subgrids, the diagonals must also contain numbers 1 through 9 (or the corresponding numbers for different grid sizes).
8. **Irregular Sudoku:** Irregular Sudoku, also known as Jigsaw Sudoku, has irregularly shaped subgrids instead of standard 3 × 3 boxes. The objective remains the same: each row, column,

and irregular subgrid must contain numbers 1 through 9 (or the corresponding numbers for different grid sizes).

9. **Killer Sudoku:** Killer Sudoku combines elements of Sudoku and Kakuro. Kakuro is a crossword number puzzle in which each number word must add up to the number provided as a clue above or to the left of it. In this variant, you are given additional information in the form of "cages" that represent the sum of the numbers within that cage. The objective was to fill the grid with numbers that satisfied the sum constraints for each cage.

3D Sudoku [11] is a variation of the classic Sudoku puzzle that adds an extra dimension to the game. Instead of the usual 9 × 9 grid, 3D Sudoku is played on a 9 × 9 × 9 grid, which means that it has nine 3 × 3 × 3 cubes. The objective is the same as that of traditional Sudoku: fill in the grid so that every row, column, and 3 × 3 × 3 cube contains the numbers 1 through 9 with no repetition.

Figure 1.1 shows a 25 × 25 Sudoku instance where clues are highlighted in red, whereas Figure 1.2 provides a solution to that Sudoku instance. Although Sudoku puzzles are primarily enjoyed as recreational games,

1		4	20	25	24		15	17	10		8	18	14	22	6	12	9	3	16	2	7		23	5
5	2		23	24	8	22	12	9	3	16	6	7	20	17	18	21	25	14	13	10	11	4	1	15
17	14		6	3	25	21	5	7	20	11			1	13	4	8					12	16	22	19
16	7	21	8	18	4	2	13	11	23	5	19	15	24		10	20	17	22	1	9	6	25		3
10	13			22	14	1		6	16	23	9	25	4	3	7	5	19	11	2	8	24	20		17
12	1	11	10	6	5	13	23	24	15			8	17	21	25	19	3	4			14	2	20	18
8	19	13	21	9	16	4	25	12	2	15	3	5	11	20	14			18	22	1	10	7	24	6
4	17		18	7	9	3	22	21	19	25	1	24	2	23	5	13	20	10	6	16	15	8	11	12
22	3	24	15		18	20			7	10	13	4	6	14	16	2	12	21	8	5	19			9
20	16	2	25	5	10	8	6	14	17	9	22	12			1	11	15	7	24	3	23	21	13	4
13	25	3	5	10	2	23	14	4	18	22	15	17	19	24	20	7	1	9	21	12	16	6	8	11
14	23	1	24	12	19	16	8			2	7	20		10	3	4	13	17	11	21	9	5	18	22
7	8			17	20	24	21	22	9	3	4	1		16	2	6				25	13	15	10	
2	22	16	9	21	17	11	7	10	25	8	5	14	13	6	12	24	18	15	23	19	4	1	3	
6	15	20	19	4	13	12	3	5	1	18			21	9	8	22	16	25	10	7	17	24	2	14
21	18	12	2	16	7	10	19	3	13	1	24	22	9	4	11	15	6	20	14	17	8	23	5	25
9			13	1	6	25	4	20	12	17	14			18	23	16		5	19	11	21		15	2
23	10	22	7	15	21			18	14	6	20	16	8	11	17	1		13	25	4	3		12	24
25	5	6	14	11	1	17	2	8	24	13			23	15	9	3		12	4	20	18	22	16	7
3	20	17	4	19	22	15	16	23	11	12	25	10	5	2	21	18	8	24	7	6	1	14	9	13
19	6	23		8	15	18	1	25	4	14	2	9	3	7	13	10	11		20	24			17	21
15	4	5	17	14	3	7		19	8	20	23	11	10	25	22	9		1	12	13	2	18	6	16
11	12	7	16		23	6		2	21	24	18	13	15	1	19	25	5	8	3	14	22	9	4	10
18	9	25	1	2	11	14		13	22	4	12		16	5		23	7	6	17	15			19	8
24	21	10	3	13	12	9	20	16	5	19	17	6	22	8	15	14	4	2	18	23	25	11	7	1

Figure 1.1 An instance of a 2D Sudoku puzzle of size 25 × 25 with clues highlighted in red.

1	11	4	20	25	24	19	15	17	10	21	8	18	14	22	6	12	9	3	16	2	7	13	23	5
5	2	19	23	24	8	22	12	9	3	16	6	7	20	17	18	21	25	14	13	10	11	4	1	15
17	14	9	6	3	25	21	5	7	20	11	10	2	1	13	4	8	24	23	15	18	12	16	22	19
16	7	21	8	18	4	2	13	11	23	5	19	15	24	12	10	20	17	22	1	9	6	25	14	3
10	13	15	12	22	14	1	18	6	16	23	9	25	4	3	7	5	19	11	2	8	24	20	21	17
12	1	11	10	6	5	13	23	24	15	7	16	8	17	21	25	19	3	4	9	22	14	2	20	18
8	19	13	21	9	16	4	25	12	2	15	3	5	11	20	14	17	23	18	22	1	10	7	24	6
4	17	14	18	7	9	3	22	21	19	25	1	24	2	23	5	13	20	10	6	16	15	8	11	12
22	3	24	15	23	18	20	11	1	7	10	13	4	6	14	16	2	12	21	8	5	19	17	25	9
20	16	2	25	5	10	8	6	14	17	9	22	12	18	19	1	11	15	7	24	3	23	21	13	4
13	25	3	5	10	2	23	14	4	18	22	15	17	19	24	20	7	1	9	21	12	16	6	8	11
14	23	1	24	12	19	16	8	15	6	2	7	20	25	10	3	4	13	17	11	21	9	5	18	22
7	8	18	11	17	20	24	21	22	9	3	4	1	12	16	2	6	14	19	5	25	13	15	10	23
2	22	16	9	21	17	11	7	10	25	8	5	14	13	6	12	24	18	15	23	19	4	1	3	20
6	15	20	19	4	13	12	3	5	1	18	11	23	21	9	8	22	16	25	10	7	17	24	2	14
21	18	12	2	16	7	10	19	3	13	1	24	22	9	4	11	15	6	20	14	17	8	23	5	25
9	24	8	13	1	6	25	4	20	12	17	14	3	7	18	23	16	22	5	19	11	21	10	15	2
23	10	22	7	15	21	5	9	18	14	6	20	16	8	11	17	1	2	13	25	4	3	19	12	24
25	5	6	14	11	1	17	2	8	24	13	21	19	23	15	9	3	10	12	4	20	18	22	16	7
3	20	17	4	19	22	15	16	23	11	12	25	10	5	2	21	18	8	24	7	6	1	14	9	13
19	6	23	22	8	15	18	1	25	4	14	2	9	3	7	13	10	11	16	20	24	5	12	17	21
15	4	5	17	14	3	7	24	19	8	20	23	11	10	25	22	9	21	1	12	13	2	18	6	16
11	12	7	16	20	23	6	17	2	21	24	18	13	15	1	19	25	5	8	3	14	22	9	4	10
18	9	25	1	2	11	14	10	13	22	4	12	21	16	5	24	23	7	6	17	15	20	3	19	8
24	21	10	3	13	12	9	20	16	5	19	17	6	22	8	15	14	4	2	18	23	25	11	7	1

Figure 1.2 A solution instance of 2D Sudoku puzzle of size 25 × 25 given in Figure 1.1.

they have also found interesting applications in various fields. One such application is video encryption, in which Sudoku-based algorithms can be utilized to secure video content.

A Sudoku instance can be solved in multiple ways because we can start from any given clue present in the minigrids. However, in contemporary literature, no technique has been described to determine the number of starting cells. The starting cell becomes fascinating to a mathematician only if it follows a minimal route, and the removal or inclusion of a single clue may generate another Sudoku instance for which other new solutions may exist. Moreover, no current technique can determine the minimum number of clues to be provided to the cells. This accounts for the maximum number of variations in Sudoku puzzle instances. The authors in [8] stated that a minimum of 17 clues are needed to ensure that a Sudoku instance, if solvable, has only one unique solution. Therefore, any Sudoku puzzle instance with fewer than 17 givens, if valid, must have more than one solution. However, a valid Sudoku instance may have multiple correct solutions even if the instance includes more than 17 clues. Several techniques exist for the solving a Sudoku puzzle, which differ depending on the difficulty level of the puzzle. According to contemporary literature, the level of difficulty of a Sudoku puzzle is governed by its number of clues [9]. The relationship between the difficulty level of a Sudoku puzzle and the number of clues presented is shown in Table 1.1.

In addition to the number of clues, the position of the empty cells also influences the difficulty level. For any two Sudoku puzzle instances with the same number of clues, the puzzle where the clues are present in clusters/groups is assigned a higher difficulty level than the puzzle with an even distribution of clues. According to the row and column constraints presented in [9], the minimum possible number of clues, in each row and column for different difficulty levels is set as given in Table 1.2.

Sudoku can also be used for video encryption. Sudoku puzzles have a unique property that can be used to scramble and encrypt data. Sudoku puzzles can be used to create a 9 × 9 matrix that can be used to map the pixels of a video frame to new positions. This scrambling process makes it difficult for unauthorized users to decrypt a video without the correct key.

Table 1.1 Definition of the Sudoku instance difficulty level according to the number of given clues.

Difficulty level	Number of clues
1 (Extremely Easy)	>46
2 (Easy)	36–46
3 (Medium)	32–35
4 (Hard)	28–31
5 (Evil)	17–27

Table 1.2 Minimum possible number of clues, in each row and column of a Sudoku instance for different levels of difficulty.

Difficulty level	Minimum possible number of clues in each row and column
1 (Extremely Easy)	05
2 (Easy)	04
3 (Medium)	03
4 (Hard)	02
5 (Evil)	00

There are several different ways to use Sudoku puzzles for video encryption. A common method is to use the Sudoku matrix to create a permutation function. This function can then be applied to the pixels of a video frame to scramble them. Another common method is to use a Sudoku matrix to create a substitution function. This function can then be used to replace pixel values with new values. Sudoku-based video encryption is a relatively new and an emerging field. However, they have enormous potential advantages over other encryption methods. For example, Sudoku-based encryption is relatively simple to implement and does not require specialized hardware or software. In addition, Sudoku-based encryption is highly resistant to attacks.

Here are some of the potential applications of Sudoku-based video encryption:

- Securing confidential video communications
- Protecting copyrighted video content
- Enhancing the security of video surveillance systems

Video encryption involves the process of transforming a video file into ciphertext, which can only be deciphered with a corresponding decryption key. This ensures that unauthorized individuals cannot access or understand video content. Traditional encryption methods often employ complex mathematical algorithms; however, Sudoku-based encryption offers an alternative approach that combines simplicity and security. Sudoku-based encryption provides several advantages. First, it offers a visually pleasing and challenging encryption method that can engage users in solving the Sudoku puzzle to decrypt a video. Second, the simplicity of Sudoku rules and transformations makes them easier to implement and understand than the complex mathematical algorithms used in traditional encryption methods. Finally, Sudoku-based encryption can provide a level of security suitable for certain applications, particularly when combined with other encryption techniques and key management practices. This study used Giant Sudoku to generate the key. As for 25×25 Sudoku 7.5×10^{22}, possible Sudoku solution grids are there, which is huge. Therefore, extracting a key is impossible for an attacker.

1.2 Literature Survey

Sudoku has enormous applications in the fields of cryptography [12], steganography [2], and encryption of messages, texts, images, audio, and videos. In today's digital world, securing data from all possible attacks is very crucial. The proposed method works on a video file to transmit the