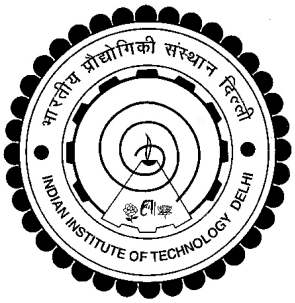
SIGNATURE SCHEMES AND SECRET SHARING SCHEMES WITH THEIR APPLICATIONS USING BLOCKCHAIN TECHNOLOGY

NEHA ARORA



DEPARTMENT OF MATHEMATICS
INDIAN INSTITUTE OF TECHNOLOGY DELHI
October 2024

SIGNATURE SCHEMES AND SECRET SHARING SCHEMES WITH THEIR APPLICATIONS USING BLOCKCHAIN TECHNOLOGY

by

NEHA ARORA

Department of Mathematics

Submitted

in fulfillment of the requirements of the degree of Doctor of Philosophy

to the

INDIAN INSTITUTE OF TECHNOLOGY DELHI

October 2024

Dedicated to

My Family

Certificate

This is to certify that the thesis entitled **"Signature Schemes and Secret Sharing Schemes with their Applications using Blockchain Technology"** submitted by **"Ms. Neha Arora"** to the Indian Institute of Technology Delhi, for the award of the Degree of **Doctor of Philosophy**, is a record of the original bonafide research work carried out by her under my supervision and guidance. The thesis has reached the standards fulfilling the requirements of the regulations relating to the degree.

The results contained in this thesis have not been submitted in part or full to any other university or institute for the award of any degree or diploma.

New Delhi
October 2024

Prof. R. K. Sharma
Professor
Department of Mathematics
Indian Institute of Technology Delhi

Acknowledgements

I am filled with immense gratitude as I extend my heartfelt appreciation to those who have supported and inspired me throughout my PhD journey.

First and foremost, I would like to express my deepest gratitude to God for the immense support, strength, and blessings that have guided me throughout this journey. The divine grace has provided me with the fortitude to overcome challenges and achieve this significant milestone.

I am deeply thankful to my supervisor, Prof. R.K. Sharma, for his exceptional guidance, unwavering support, and invaluable expertise. His encouragement and insightful suggestions have significantly contributed to the completion of this thesis. I sincerely appreciate the freedom he granted me to explore my research interests and his dedication to nurturing my academic growth.

I am also profoundly grateful to Prof. Ritumoni Sarma, my SRC Chairman, for his invaluable feedback and constant support. I extend my sincere thanks to my other SRC members, Prof. Shiv Prakash Patel and Prof. R.K. Soni, for their insightful comments and constructive criticism that greatly enhanced my research. I would also like to express my heartfelt gratitude to Prof. Aparna Mehra, Head of the Department of Mathematics, for her continuous guidance, unwavering support, and her trust in me.

A special note of thanks goes to my best and most loving friend and colleague, Dr. Mohit Kumar Baghel, for his unwavering support, motivation, and countless insightful discussions that have been instrumental in my research journey. I am grateful to him for sharing my sorrow and frustration, always believing in me, encouraging me to dream big, and pushing me every day to unlock my highest potential. His presence in both my professional and personal life has been a source of great strength and has had a significant positive impact on my life.

I would also like to express my gratitude to my senior, Dr. D.C. Mishra, colleague and friend Dr. Vidya Sagar, and junior, Kushagri Tandon, for their invaluable assistance in my research. Their contributions have been crucial to the successful completion of this work.

My heartfelt thanks go to my friends and seniors, Dr. Sandeep Malik, Dr. Pooja, and Ms. Soniya Takshak, colleagues Dr. Abhinay Kumar Gupta and Dr. Amit Arora, and my juniors Dr. Astha Agrawal and Dr. Gyanendra Kumar Verma, for their support and encouragement throughout this journey. Their camaraderie and guidance have been a significant part of my PhD experience.

I deeply appreciate the Indian Institute of Technology, Delhi, for granting me essential resources, library access, and facilities pivotal to my research. The Department of Mathematics at IIT Delhi has been an invaluable support throughout my academic journey, offering crucial intellectual discussions and seminars that enriched my research.

I am deeply indebted to my family for their unwavering love, support, and motivation. I would like to thank my parents, Mr. Anil Arora and Mrs. Pushpa Arora; my grandparents, Mr. Krishan Lal Arora and late Mrs. Satyawati Arora; my loving sister Varsha; and my brothers and guardians, Krishna and Maruti. Their faith in me and constant encouragement have been my driving force.

This thesis would not have been possible without the contributions of these individuals. I extend my thanks to all who have been a part of this significant milestone in my academic journey. If I have unintentionally omitted anyone, please know that your support has been deeply valued.

Delhi

October 2024 *Neha Arora*

Abstract

Cryptography, the science of encoding and decoding information, ensures data security and trust in an increasingly digital world. This thesis explores two critical cryptographic constructs: signature schemes and secret sharing schemes, emphasizing their applications using blockchain technology. Signature schemes authenticate and validate the integrity of messages, preventing repudiation and ensuring data authenticity, while secret sharing schemes distribute a secret among multiple participants to prevent unauthorized access and maintain data confidentiality.

The research presented here focuses on designing signature schemes and secret sharing schemes that offer enhanced security over existing solutions. Specifically, we investigate designated verifier signature schemes and undeniable signature schemes, applying these innovations to real-world scenarios, followed by secret sharing schemes and multi-secret sharing schemes based on various encryption techniques.

Initially, a novel approach is introduced for designated verifier signature schemes involving multiple signers and verifiers, utilizing various cryptographic algorithms to enhance security. Then, non-interactive undeniable designated verifier signature schemes are proposed and tailored for the healthcare sector using blockchain to ensure the privacy and integrity of sensitive data.

In addition, a threshold secret sharing scheme with two-level security is developed, leveraging Shamir's secret sharing scheme and incorporating a one-way function for enhanced security. This scheme's applications within blockchain networks are explored,

emphasizing its practicality in sectors like national security, healthcare, and supply chain management.

Furthermore, a multi-secret sharing scheme is designed using Shamir's secret sharing scheme, the affine Hill matrix cipher, and the hash function to ensure data integrity and robustness against various attacks.

The thesis also proposes traceable secret sharing schemes based on n-multilinear pairing and the ElGamal cryptosystem, demonstrating their use in a blockchain-based E-voting system to maintain voter privacy, transparency, and security.

In an era of increased digital interactions, robust cryptographic techniques are essential to safeguard data security and establish trust. This thesis embarks on a comprehensive exploration of these cryptographic algorithms, aiming to design, investigate, and enhance their capabilities and understand their roles in secure communication and data security, particularly through their applications in Blockchain Technology.

The work begins with the foundational concept of asymmetric encryption, which employs a public key for encryption and a private key for decryption, facilitating secure communication and forming the basis for digital signatures. Signature schemes, pivotal in ensuring authenticity and non-repudiation, are extensively discussed. These schemes enable signers to authenticate messages and allow verifiers to confirm the integrity and origin of communications, which is vital for applications such as financial transactions and medical data.

Non-interactive designated verifier signature schemes and undeniable signature schemes designed for multiple signers and verifiers are introduced, leveraging cryptographic techniques such as bilinear pairing, RSA, and the discrete logarithm problem. These schemes ensure strong, non-interactive signatures with unforgeability and non-transferability, and their practical applications, particularly in healthcare, demonstrate their efficacy in secure data transmission within blockchain networks.

The thesis also delves into secret sharing schemes and multi-secret sharing schemes. A (t, n)-threshold secret sharing scheme and multi-secret sharing scheme with two-level security based on Shamir's scheme, integrated with one-way function for participants'

honesty verification, are proposed and adapted for blockchain networks to ensure secure and efficient block generation. Furthermore, a multi-secret sharing scheme using the affine Hill matrix cipher is introduced, enhancing security through the non-commutativity of the matrix multiplication and being robust against various attacks. Finally, (t, n) single secret sharing scheme and multi-secret sharing scheme using n-multilinear map and the ElGamal cryptosystem are proposed and applied to a blockchain-based E-voting system, highlighting the scheme's utility in secure, transparent, and efficient voting processes.

Through rigorous security analyses and real-world implementations, this thesis underscores significant advancements in cryptographic techniques, particularly signature and secret sharing schemes, and their practical applications in blockchain technology. The work enhances the security and efficiency of modern cryptographic practices, offering valuable insights for future research and development.

सार

क्रिप्टोग्राफी, एन्कोडिंग और डिकोडिंग जानकारी का विज्ञान, एक तेजी से डिजिटल दुनिया में डेटा सुरक्षा और विश्वास सुनिश्चित करता है। यह थीसिस दो महत्वपूर्ण क्रिप्टोग्राफिक संरचनाओं की पड़ताल करता हैः हस्ताक्षर योजनाएं और गुप्त साझाकरण योजनाएं, जो ब्लॉकचेन तकनीक का उपयोग करके उनके अनुप्रयोगों पर जोर देती हैं। हस्ताक्षर योजनाएं संदेशों की अखंडता को प्रमाणित और मान्य करती हैं, खंडन को रोकती हैं और डेटा की प्रामाणिकता सुनिश्चित करती हैं, जबकि गुप्त साझाकरण योजनाएं अनधिकृत पहुंच को रोकने और डेटा गोपनीयता बनाए रखने के लिए कई प्रतिभागियों के बीच एक रहस्य वितरित करती हैं।

यहाँ प्रस्तुत शोध हस्ताक्षर योजनाओं और गुप्त साझाकरण योजनाओं को डिजाइन करने पर केंद्रित है जो मौजूदा समाधानों पर बेहतर सुरक्षा प्रदान करते हैं। विशेष रूप से, हम नामित सत्यापनकर्ता हस्ताक्षर योजनाओं और निर्विवाद हस्ताक्षर योजनाओं की जांच करते हैं, इन नवाचारों को वास्तविक दुनिया के परिदृश्यों पर लागू करते हैं, इसके बाद गुप्त साझाकरण योजनाएं और विभिन्न एन्क्रिप्शन तकनीकों के आधार पर बहु-गुप्त साझाकरण योजनाएं होती हैं।

प्रारंभ में, सुरक्षा बढ़ाने के लिए विभिन्न क्रिप्टोग्राफिक एल्गोरिदम का उपयोग करते हुए, कई हस्ताक्षरकर्ताओं और सत्यापनकर्ताओं को शामिल करते हुए निर्दिष्ट सत्यापनकर्ता हस्ताक्षर योजनाओं के लिए एक नया दृष्टिकोण पेश किया गया है। फिर, गैर-इंटरैक्टिव निर्विवाद नामित सत्यापन हस्ताक्षर योजनाओं को प्रस्तावित किया जाता है और संवेदनशील डेटा की गोपनीयता और अखंडता सुनिश्चित करने के लिए ब्लॉकचेन का उपयोग करके स्वास्थ्य सेवा क्षेत्र के लिए तैयार किया गया है।

इसके अलावा, दो-स्तरीय सुरक्षा के साथ एक सीमा गुप्त साझाकरण योजना विकसित की गई है, जो शमीर की गुप्त साझाकरण योजना का लाभ उठाती है और बढ़ी हुई सुरक्षा के लिए एक तरफा कार्य को शामिल करती है। राष्ट्रीय सुरक्षा, स्वास्थ्य सेवा और आपूर्ति श्रृंखला प्रबंधन जैसे क्षेत्रों में इसकी व्यावहारिकता पर जोर देते हुए, ब्लॉकचेन नेटवर्क के भीतर इस योजना के अनुप्रयोगों का पता लगाया जाता है।

इसके अलावा, विभिन्न हमलों के खिलाफ डेटा अखंडता और मजबूती सुनिश्चित करने के लिए शमीर की गुप्त साझाकरण योजना, एफाइन हिल मैट्रिक्स सिफर और हैश फ़ंक्शन का उपयोग करके एक बहु-गुप्त साझाकरण योजना तैयार की गई है।

थीसिस ने मतदाता गोपनीयता, पारदर्शिता और सुरक्षा बनाए रखने के लिए एक ब्लॉकचेन-आधारित ई-वोटिंग प्रणाली में उनके उपयोग का प्रदर्शन करते हुए n -multilinear पेयरिंग और ElGamal क्रिप्टोसिस्टम के आधार पर पता लगाने योग्य गुप्त साझाकरण योजनाओं का भी प्रस्ताव दिया है।

बढ़ती डिजिटल बातचीत के युग में, डेटा सुरक्षा की रक्षा करने और विश्वास स्थापित करने के लिए मजबूत क्रिप्टोग्राफिक तकनीकें आवश्यक हैं। यह थीसिस इन क्रिप्टोग्राफिक एल्गोरिदम के व्यापक अन्वेषण की शुरुआत करता है, जिसका उद्देश्य उनकी क्षमताओं को डिजाइन करना, जांच करना और बढ़ाना और सुरक्षित संचार और डेटा सुरक्षा में उनकी भूमिकाओं को समझना है, विशेष रूप से ब्लॉकचैन प्रौद्योगिकी में उनके अनुप्रयोगों के माध्यम से।

काम असममित कूटलेखन की मूलभूत अवधारणा के साथ शुरू होता है, जो कूटलेखन के लिए एक सार्वजनिक कुंजी और डिक्रिप्शन के लिए एक निजी कुंजी को नियोजित करता है, सुरक्षित संचार की सुविधा प्रदान करता है और डिजिटल हस्ताक्षर के लिए आधार बनाता है। प्रामाणिकता और अस्वीकृति सुनिश्चित करने में महत्वपूर्ण हस्ताक्षर योजनाओं पर व्यापक रूप से चर्चा की जाती है। ये योजनाएं हस्ताक्षरकर्ताओं को संदेशों को प्रमाणित करने में सक्षम बनाती हैं और सत्यापनकर्ताओं को संचार की अखंडता और उत्पत्ति की पुष्टि करने की अनुमति देती हैं, जो वित्तीय लेनदेन और चिकित्सा डेटा जैसे अनुप्रयोगों के लिए महत्वपूर्ण है।

कई हस्ताक्षरकर्ताओं और सत्यापनकर्ताओं के लिए डिज़ाइन की गई गैर-इंटरैक्टिव नामित सत्यापनकर्ता हस्ताक्षर योजनाएं और निर्विवाद हस्ताक्षर योजनाएं शुरू की गई हैं, जो द्वि-रेखीय युग्मन, आरएसए और असतत लघुगणक समस्या जैसी क्रिप्टोग्राफिक तकनीकों का लाभ उठाती हैं। ये योजनाएं अपरिवर्तनीयता और गैर-हस्तांतरणीयता के साथ मजबूत, गैर-अंतःक्रियात्मक हस्ताक्षर सुनिश्चित करती हैं, और उनके व्यावहारिक अनुप्रयोग, विशेष रूप से स्वास्थ्य सेवा में, ब्लॉकचेन नेटवर्क के भीतर सुरक्षित डेटा संचरण में अपनी प्रभावकारिता प्रदर्शित करते हैं।

यह शोध प्रबंध गुप्त साझाकरण योजनाओं और बहु-गुप्त साझाकरण योजनाओं पर भी प्रकाश डालता है। एक (t, n)-थ्रेशोल्ड गुप्त साझाकरण योजना और शमीर की योजना पर आधारित दो-स्तरीय सुरक्षा के साथ बहु-गुप्त साझाकरण योजना, प्रतिभागियों के ईमानदारी सत्यापन के लिए एक तरफा कार्य के साथ एकीकृत, सुरक्षित और कुशल ब्लॉक उत्पादन सुनिश्चित करने के लिए ब्लॉकचेन नेटवर्क के लिए प्रस्तावित और अनुकूलित हैं। इसके अलावा, एफाइन हिल मैट्रिक्स सिफर का उपयोग करके एक बहु-गुप्त साझाकरण योजना शुरू की गई है, जो मैट्रिक्स गुणन की गैर-कम्यूटेटिविटी के माध्यम से सुरक्षा को बढ़ाती है और विभिन्न हमलों के खिलाफ मजबूत होती है। अंत में, (t, n) एकल गुप्त साझाकरण योजना और बहु-गुप्त साझाकरण योजना n -multilinear पेयरिंग और ElGamal क्रिप्टोसिस्टम का उपयोग करके प्रस्तावित और एक ब्लॉकचेन-आधारित ई-मतदान प्रणाली पर लागू की जाती है, जो सुरक्षित, पारदर्शी और कुशल मतदान प्रक्रियाओं में योजना की उपयोगिता को उजागर करती है।

कठोर सुरक्षा विश्लेषण और वास्तविक दुनिया के कार्यान्वयन के माध्यम से, यह थीसिस क्रिप्टोग्राफिक तकनीकों, विशेष रूप से हस्ताक्षर और गुप्त साझाकरण योजनाओं और ब्लॉकचेन तकनीक में उनके व्यावहारिक अनुप्रयोगों में महत्वपूर्ण प्रगति को रेखांकित करता है। यह कार्य भविष्य के अनुसंधान और विकास के लिए मूल्यवान अंतर्दृष्टि प्रदान करते हुए आधुनिक क्रिप्टोग्राफिक प्रथाओं की सुरक्षा और दक्षता को बढ़ाता है।

Contents

List of Figures

List of Tables