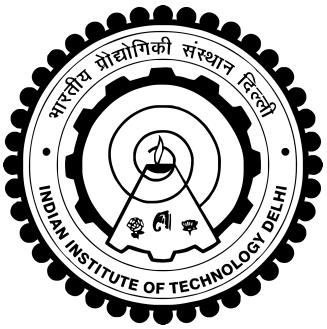
SECURING DEMOCRACIES: BUILDING TRUST IN LARGE PUBLIC ELECTIONS

PRASHANT AGRAWAL



DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING
INDIAN INSTITUTE OF TECHNOLOGY DELHI
AUGUST 2024

SECURING DEMOCRACIES: BUILDING TRUST IN LARGE PUBLIC ELECTIONS

by

PRASHANT AGRAWAL

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

Submitted

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

to the

INDIAN INSTITUTE OF TECHNOLOGY DELHI

AUGUST 2024

To the pursuit of knowledge

CERTIFICATE

This is to certify that the thesis titled **"SECURING DEMOCRACIES: BUILDING TRUST IN LARGE PUBLIC ELECTIONS"**, submitted by **Prashant Agrawal**, to the Indian Institute of Technology, Delhi, for the award of the degree of **Doctor of Philosophy**, is a bona fide record of the research work done by him under our supervision. The contents of this thesis, in full or in parts, have not been submitted to any other Institute or University for the award of any degree or diploma.

Prof. Subhashis Banerjee
Professor
Department of Computer Science
Ashoka University, 131 029

Retired Professor
Department of Computer Science and Engineering
Indian Institute of Technology Delhi, 110 016

Prof. Subodh Vishnu Sharma
Associate Professor
Department of Computer Science and Engineering
Indian Institute of Technology Delhi, 110 016

ACKNOWLEDGEMENTS

I wish to thank my advisors, Prof. Subhashis Banerjee and Prof. Subodh Sharma, for the invaluable guidance and support they provided throughout my PhD journey. Subhashis has been instrumental in teaching me how to choose research problems and approach them with a critical, principled mindset, significantly shaping the intellectual rigor of my work and maintaining clarity in my thought processes. I am equally grateful to Subodh for his unwavering belief in my capabilities and for providing the support needed during the most challenging times. His role in sustaining my motivation and resilience has been vital. Additionally, the thesis would not be possible without the support of Prof. Mahavir Jhawar from Ashoka University. I sincerely thank him for hosting me at Ashoka numerous times and for finding time for our extensive discussions despite his demanding schedule.

I also extend my thanks to my committee and the faculty members and colleagues at both IIT Delhi and Ashoka University. Special thanks are due to Prof. S. Arun-Kumar, Prof. Rohit Vaish, Prof. Vaishnavi Sundararajan, Prof. Venkata Koppula, and Dr. Mahesh Sreekumar Rajasree for their insightful discussions and reviews of my research and writings. My friends — Abhinav Nakarmi, Aarav Varshney, Bhavesh Neekhra, Kabir Tomer, Aritra Bagchi, Shashank Sharma, and Abhishek Rose — provided refreshing and thought-provoking conversations that were a respite from my intense research focus and allowed me to persevere. Rekha Rathee and Hemant Prasad from the IIT Delhi CSE department office deserve special thanks for their friendly support in administrative matters.

My research was supported by IIT Delhi Institute Fellowship, the Pankaj Jalote Doctoral Grant, the Pankaj Gupta Privacy Chair Funds, and the Centre for Digitalisation, AI and Society at Ashoka University. My sincere gratitude to all the donors and funding agencies. I also thank various anonymous reviewers of our papers for their helpful comments and feedback. Special thanks to Dr. Peter B. Rønne and other reviewers at the E-VOTE-ID 2023 PhD colloquium for their constructive feedback on an earlier version of Chapter 7.

Lastly, I cannot imagine undertaking this arduous journey without the unconditional love and support of my parents, my brother and my wife, who have always placed my career above their own needs. My wife, Archie, has been especially supportive, managing our home and raising our son even during my long days at the lab and extended visits to Ashoka. I must also thank my 4-year-old son, Madhur, whose uncaring and innocent smile has always brightened my days and kept the spirits high.

Prashant Agrawal

ABSTRACT

KEYWORDS: election security, dual voting, recoverability, electoral rolls

This thesis presents innovative advancements to enhance public trust in large public elections, particularly in contexts similar to Indian elections. We develop our proposals based on the concept of dual voting, a hybrid approach combining cryptographic voting techniques with paper audit trails. Dual voting mitigates risks associated with relying solely on either electronic or paper ballots, which is crucial for engendering public trust in large elections.

Our first contribution is a comprehensive analysis of the voter-facing component of various existing voting protocols, identification of their usability and security flaws, and the development of a new dual voting design that addresses these flaws.

Next, we observe that although existing voting protocols are verifiable, they do not provide easy methods of recovery in case verifications fail, at least not without reposing trust on a paper audit trail. We introduce the novel concept of "recoverability" in dual voting systems, proposing mechanisms that allow for effective recovery from audit failures without a complete reliance on either electronic or paper records. Our approach allows selective re-elections in problematic polling stations without necessitating a full re-run of the election. This approach significantly enhances the robustness of the electoral process and maintains public confidence even if there are isolated discrepancies. A technical innovation underlying our recovery protocol is a novel concept we introduce, called "traceable mixnets," which extends traditional mixnets with the ability to prove special membership relationships between input ciphertexts and output plaintexts of a mixnet in zero-knowledge.

Lastly, we address the so-far overlooked issues of security and privacy of electoral rolls (voter lists) and polling-booth eligibility verification processes. We analyse various threats related to electoral roll manipulation, ballot stuffing, voter denial and voter profiling and propose a protocol that protects against them, ensuring that voters' identity information is protected from misuse, all eligible voters can fairly participate in the electoral process, and the eligibility verification process is sound, i.e., ballot stuffing is detectable.

Collectively, these contributions not only enhance the technical integrity of voting systems but also address broader concerns about public trust in electoral processes. By bridging the gap between cryptographic security and practical electoral requirements, this work lays a foundation for more secure, transparent, and inclusive democratic elections.

सार

मुख्य शब्द: चुनावी सुरक्षा, द्वैत मतदान, रिकवरेबिलिटी, मतदाता सूची

यह शोध बड़े सार्वजनिक चुनावों में और विशेष रूप से भारतीय चुनावों में जन–साधारण के विश्वास को बढ़ाने के लिए नवीन प्रगतियों को प्रस्तुत करता है। हम अपने प्रस्तावों का विकास द्वैत मतदान की अवधारणा पर आधारित करते हैं, जो कि क्रिप्टोग्राफिक मतदान तकनीकों और कागजी ऑडिट ट्रेल्स को मिलाने वाला एक हाइब्रिड दृष्टिकोण है। द्वैत मतदान केवल इलेक्ट्रॉनिक प्रणालियों या कागजी मतपत्रों पर निर्भर रहने से जुड़े जोखिमों को कम करता है, जो कि बड़े चुनावों में जनता के विश्वास को सुदृढ़ करने के लिए महत्वपूर्ण है।

हम अपने पहले योगदान के तौर पर विभिन्न मौजूदा मतदान प्रोटोकॉलों में मतदाता के अनुभव का व्यापक मूल्यांकन करते हैं, उनकी उपयोगिता और सुरक्षा–दोषों की पहचान करते हैं और इन दोषों को संबोधित करने के लिए एक नए द्वैत मतदान प्रोटोकॉल का विकास करते हैं।

दूसरे, हम पहचानते हैं कि हालांकि मौजूदा मतदान प्रोटोकॉल सत्यापनीय हैं, वे सत्यापन विफल होने की स्थिति में आसान रिकवरी के तरीके प्रदान नहीं करते, कम–से–कम कागजी ऑडिट ट्रेल पर भरोसा किए बिना नहीं। हम द्वैत मतदान में "रिकवरेबिलिटी" की नवीन अवधारणा प्रस्तुत करते हैं और ऐसे तंत्र प्रस्तुत करते हैं जो ऑडिट विफल होने पर प्रभावी रूप से उबरने में सहायक हैं और न तो पूर्ण रूप से इलेक्ट्रॉनिक न ही कागजी रिकॉर्ड्स पर संपूर्णतः निर्भर करते हैं। हमारा दृष्टिकोण ऑडिट विफल होने पर पूरे निर्वाचन क्षेत्र में पुनः चुनाव कराये बिना केवल समस्याग्रस्त मतदान केंद्रों में पुनः मतदान कराने में सहायक है। यह दृष्टिकोण चुनावी प्रक्रिया की दृढ़ता को काफी बढ़ाता है और अलग–थलग विसंगतियों की घटना में भी जनता का विश्वास बनाए रखता है। हमारे रिकवरी प्रोटोकॉल का तकनीकी आधार है "ट्रेसेबल मिक्सनेट्स"। यह एक नयी क्रिप्टोग्राफिक तकनीक है जो पारंपरिक मिक्सनेट्स पर आधारित है और मिक्सनेट के इनपुट साइफरटेक्स्ट और आउटपुट प्लेनटेक्स्ट के बीच विशेष सदस्यता संबंधों को साबित कर सकती है, बिना इससे अधिक कोई भी जानकारी दिये।

अंत में, यह शोध चुनावी सुरक्षा में एक और अनसुलझे मुद्दे को संबोधित करता है: मतदाता सूचियों की सुरक्षा और गोपनीयता। हम इस मुद्दे से जुड़ी विभिन्न समस्याओं का विश्लेषण करते हैं, जैसे मतदाता सूचियों में हेरफेर, मतदाताओं का मताधिकार वंचन और मतदाता प्रोफ़ाइलिंग। हम मतदाता सूची बनाने और मतदान के दौरान उनका उपयोग करने में सहायक एक नया प्रोटोकॉल प्रस्तुत करते हैं जो एक तरफ़ पंजीकरण व मतदाता परीक्षण प्रक्रियाओं को सुरक्षित करता है वहीं दूसरी तरफ़ मतदाता प्रोफ़ाइलिंग से जुड़ी समस्याओं के प्रति संरक्षण प्रदान करता है। हमारा प्रोटोकॉल सुनिश्चित करता है कि सभी योग्य मतदाता चुनावी प्रक्रिया में निष्पक्ष रूप से भाग ले सकें।

कुल मिला कर, ये सभी योगदान ना सिर्फ़ चुनावी प्रक्रिया की तकनीकी अखंडता को सुदृढ़ करते हैं बल्कि उनमें जनता के विश्वास को स्थापित करने के मुद्दे को भी उचित रूप से संबोधित करते हैं। इस तरह से यह कार्य क्रिप्टोग्राफिक सुरक्षा और व्यावहारिक चुनावी ज़रूरतों के बीच के अंतर को पाटते हुए अधिक सुरक्षित, पारदर्शी और समावेशी लोकतांत्रिक चुनावों के लिए एक आधार तैयार करता है।

Contents

List of Figures

ABBREVIATIONS

BMD	Ballot Marking Device
CDH	Computational Diffie-Hellman
DB-RSM	Distributed Batched Reverse Set Membership
DB-SM	Distributed Batched Set Membership
DCR	Decisional Composite Residuosity
DDH	Decisional Diffie-Hellman
DL	Discrete Logarithm
DPK	Distributed Proof of Knowledge
DRE	Direct Recording Electronic
E2E-V	End-to-End Verifiable
EA	Election Authority
ECI	Election Commission of India
EO	Eligibility Officer
ER	Electoral Roll
ERR	Encrypted Registration Request(s)
EUF-CMA	Existential Unforgeability under Chosen Message Attacks
EV	Encrypted Vote(s)
EVM	Electronic Voting Machine
GCD	Greatest Common Divisor
HRPAT	Human-Readable Paper Audit Trail
IND-CPA	Indistinguishability under Chosen Plaintext Attacks
ITM	Interactive Turing Machine
NIZK	Non-interactive Zero Knowledge
NIZKPK	Non-interactive Zero-Knowledge Proof(s) of Knowledge
OSV	Optical Scan Voting
PK/PoK	Proof(s) of Knowledge
PO	Polling Officer
PPT	Probabilistic Polynomial Time
RLA	Risk-Limiting Audit(s)
RO	Registration Officer
RPC	Randomised Partial Checking
RSA	Rivest-Shamir-Adleman (the cryptosystem)
SDH	Strong Diffie-Hellman
TM	Turing Machine
TTP	Trusted Third Party
VVPAT	Voter Verified Paper Audit Trail
VVPR	Voter Verified Paper Record
ZKP	Zero-Knowledge Proof(s)
ZKPoK	Zero-Knowledge Proof(s) of Knowledge
zkSNARK	Zero-Knowledge Succinct Non-interactive Argument(s) of Knowledge