Indian Statistical Institute Series

Pranab Chakraborty
Subhamoy Maitra
Mridul Nandi
Suprita Talnikar

Contact Tracing in Post-Covid World

A Cryptologic Approach

STATISTICAL INDIAN INSTITUTE
UNITY IN DIVERSITY

Springer

Indian Statistical Institute Series

The *Indian Statistical Institute Series* publishes high-quality content in the domain of mathematical sciences, bio-mathematics, financial mathematics, pure and applied mathematics, operations research, applied statistics and computer science and applications with primary focus on mathematics and statistics. Editorial board comprises of active researchers from major centres of Indian Statistical Institute. Launched at the 125th birth Anniversary of P.C. Mahalanobis, the series will publish high-quality content in the form of textbooks, monographs, lecture notes and contributed volumes. Literature in this series are peer-reviewed by global experts in their respective fields, and will appeal to a wide audience of students, researchers, educators, and professionals across mathematics, statistics and computer science disciplines.

More information about this series at http://www.springer.com/series/15910

Pranab Chakraborty · Subhamoy Maitra ·
Mridul Nandi · Suprita Talnikar

Contact Tracing in Post-Covid World

A Cryptologic Approach

Springer

Pranab Chakraborty
Learning and Development
Wipro Limited
Bengaluru, Karnataka, India

Mridul Nandi
Applied Statistics Unit
Indian Statistical Institute
Kolkata, West Bengal, India

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

Suprita Talnikar
Applied Statistics Unit
Indian Statistical Institute
Kolkata, West Bengal, India

ISSN 2523-3114 ISSN 2523-3122 (electronic)
Indian Statistical Institute Series
ISBN 978-981-15-9726-8 ISBN 978-981-15-9727-5 (eBook)
https://doi.org/10.1007/978-981-15-9727-5

Mathematics Subject Classification: 94A60, 68P25, 06E30, 94C10

To our colleagues in health sectors,
who are dedicating their lives to save us all.

Preface

We live in an age where exponential possibilities and shifting sands of uncertainties constantly redefine the "new normal". This time, it's COVID-19 that is controlling the playing field. Optimists will hope for a post-Covid world, while the rest, perhaps, will settle down to live with it for a long time, if not forever.

Given the pandemic nature of the infection and the high mortality rate associated with it, the world is facing an unprecedented challenge of tackling the disease at scale. On one hand, the people who are suffering from COVID-19 must have the best possible medical care and treatment, on the other hand, it is of utmost importance to ensure that the least number of uninfected people should come in close contact with the ones who are infectious. Moreover, an asymptomatic person may never know that he/she is infected (and possibly infectious), unless he/she is tested. At the same time, if it is known that a person is infected, then non-infected persons (other than the immediate family members and healthcare professionals) should be kept away from the infected person. It should be feasible to achieve this through the mobile phone network, software systems and tools and appropriate policies, processes and assumptions. The communication among the neighboring mobile phones can be achieved through the bluetooth protocol, while the location and other relevant information may be transmitted to some centralized authority through the mobile network.

Here, we assume that in the majority of circumstances, a person would choose to inform in case he/she is infected or in case he/she feels that he/she might have passed the infection to someone else. The other assumption is the trust of the community on the government and/or central administrative agencies so that the personally identifiable information of an individual (whether infected or not) does not get compromised or breached. It is known that the issue of individual privacy receives more attention in certain countries than in others. Thus, political and social issues may play a dominant role in deciding how an application related to "contact tracing" should be designed. From a practical point of view, manual contact tracing may still remain as one of the most effective options to limit the spread of the

infection. However, with remarkable development in computation and communication, it is only natural that the world will eventually move towards digital systems to handle such a global pandemic.

In our point-of-view, cryptology will continue to be used as the fundamental science behind contact tracing software (applications/apps) given the security and privacy issues. In this book, we mostly concentrate on different contact tracing protocols from cryptologic (i.e., cryptographic and cryptanalytic) point of view. Such applications are being developed in many countries. The designers and developers come from government organizations, industries, academics, and research institutions. Given the nature of the outbreak of Covid-19, we observe knee-jerk reactions in most of the decision making processes. The same is true in the design of contact tracing protocols and their implementations. In a very short span covering only a couple of months, there are more than two dozens of proposals. At the same time, we read different critical reports in the media concerning the privacy issues. There are significant technical analyses as well in the form of research manuscripts. In that backdrop, we step in to write the first brief and comprehensive book in this domain, where we try to study the existing protocols, analyze them, and, finally, make a technical proposal for yet another logical design.

We start with an introductory chapter where we move from the informal discussions of contact-tracing proposals towards more technical analysis. We touch upon most of the existing digital contact tracing protocols and software that are being used and/or developed around the world. The transmission mechanism of the virus infection is discussed so that it can be understood how the contact tracing applications should be designed. Then we proceed towards the technical framework. The basic cryptologic primitives are explained briefly. This is needed to understand the security and privacy issues in digital contact tracing. With this, we enumerate a few well-known proposals and attempt to divide them into two categories: centralized and decentralized. From a cryptologic point of view, the design and analysis of decentralized contact tracing protocols carry more diverse and innovative ideas with better handling of privacy considerations.

We discuss some of the centralized applications in the second chapter, including Arogya Setu, TraceTogether, BlueTrace, OpenTrace, COVIDSafe, etc., that are currently in use in countries like India, Singapore or Australia. We study the elements and characteristics of these proposals from a cryptologic point of view. Next, we discuss the ROBERT protocol that has both the centralized and decentralized characteristics before concluding the chapter.

The third chapter analyzes the well-known decentralized applications such as DP3T and PACT. Such designs are available in the public domain for complete analysis. The technological giants like Apple and Google are also involved in similar efforts. Different cryptologic primitives and cryptanalytic issues need to be discussed in this perspective. We go through the design as well as design methodologies of these algorithms and also note the cryptanalytic results towards the evaluation of the protocols. A detailed comparison of such protocols is also discussed to highlight the advantages and disadvantages.

In the fourth and final chapter, we concentrate on how a digital contact tracing system should be designed maintaining the privacy of the users. We explain all the assumptions and cryptologic issues in this regard and present the exact problem statement to the best of our understanding. We specifically discuss higher order contact tracing in terms of the neighborhood of a neighborhood. This is in the direction that the people in the first neighborhood should be immediately tested, whereas the second layer should be quarantined. We present a detailed analysis of our generic proposal and then conclude. The book contains a detailed list of references at the end of each chapter.

The readers of this document should have some basic understanding of cryptology and security. At the same time, the first chapter of the book provides a brief background so that the materials can be followed to a large extent. Some basic ideas of computer and communication sciences might also be useful. This book is targeted towards students and researchers of any science and engineering discipline, and to engineers and professionals who work in the broad field of computation and communication.

At the same time, this material opens up some deep research problems for the experts who have a formal background on cryptology. The protocols that are analyzed and described here need to be studied carefully and cryptanalysis of certain aspects might be interesting research problems.

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

- This is the first comprehensive book on the design and analysis of contact tracing applications from a cryptologic viewpoint.
- This book provides a clear understanding of the design of contact tracing applications developed in different countries and continents.
- This brief document provides a link between very recent efforts related to digital contact tracing in COVID-19 scenario and a brief contextual literature review in this field.
- This draft presents a snapshot on how such applications are developed in a mobile distributed environment keeping in mind the issues of security and privacy, which is an important challenge in the domain of computer and communication sciences.
- This book is a short presentation of core concepts in the design and analysis of contact tracing applications.
- For experts in cryptology, this book points out possible research directions towards the security evaluation of existing contact tracing applications.

There are four listed authors of this book (in alphabetical order of surnames), but this effort is an outcome of the research efforts around the world. We thank all the researchers who are working in the domain of contact tracing. At the same time, we must acknowledge our family members and friends who constantly encouraged us in this trying time. Their kindness, love, and inspiration provided the prime motivation behind every word of this printed material. We also thank the support of Mr. Rishabh Kothary, a B.S. Mathematics and Scientific Computing student from

Indian Institute of Technology Kanpur, who worked as an intern during this effort and provided some interesting pointers. Dr. Dibyendu Roy, Dr. Pinakpani Pal, and Mr. Manmatha Roy of Indian Statistical Institute, Kolkata, have also contributed in providing additional inputs in this regard. We must acknowledge Mr. Shamim Ahmad, the Senior Editor from Springer Nature India Private Limited, for his able guidance. Last, but not the least, all the authors thank their respective family members for providing great support during this pandemic. Without all these encouragements and inputs, this book could not be written in a short time.

Each author likes to mention that all the views and recommendations expressed in this book (along with other co-authors) are entirely personal and not in any way related to each one's current organization. In addition, this work is purely based on a personal research interest and not related to their professional work.

The domain of digital contact tracing is an emerging field. However, we all wish that the present pandemic should be over as soon as possible. We will be happier than ever to have our world without any need of contact tracing, where this book would become useless. By any chance, are you still flipping the pages?

Bangalore, India — Pranab Chakraborty
Kolkata, India — Subhamoy Maitra
Kolkata, India — Mridul Nandi
July 2020 — Suprita Talnikar

Contents

About the Authors

Pranab Chakraborty is Senior Manager at the Learning and Development team of Wipro Limited, Bengaluru, India. He earned his graduate degree in computer science from the Indian Statistical Institute, Kolkata, India, and undergraduate degree in electronics and telecommunications engineering from Jadavpur University, Kolkata, India. He has implemented various network protocol stacks including TCP/IP and played different organizational roles including that of a technical architect and technical delivery manager apart from his current involvement in the behavioral and leadership development field. He has a special interest in the research areas of cryptology.

Subhamoy Maitra is Senior Professor at the Applied Statistics Unit of the Indian Statistical Institute, Kolkata, India. He earned his Ph.D. and graduate degree in computer science from the Indian Statistical Institute, Kolkata, India, and undergraduate degree in electronics and telecommunications engineering from Jadavpur University, Kolkata, India. Post working in the domain of hardware and software engineering for a few years, Prof. Maitra joined the Indian Statistical Institute, Kolkata, as a faculty in 1997. Having around 6000 citations to his name, Prof. Maitra has authored several books and around 200 research papers in the area of cryptology and quantum information.

Mridul Nandi is Professor at the Applied Statistics Unit of the Indian Statistical Institute, Kolkata, India. Earlier, he worked for the National Institute of Standards and Technology (NIST), USA, as one of the technical members in the selection process of the SHA3 hash function. His research areas focus on different aspects of cryptography, including hash functions, MAC, authenticated encryption, identity (or attribute) based encryption, IoT, hardware implementation and lightweight cryptography. He is the co-designer of COLM (authenticated encryption), selected as a winner in the security category of CAESAR portfolio. Algorithms of his

designed 10 lightweight ciphers were selected for the second round of NIST lightweight standard process. He actively publishes papers in top tier conferences like Eurocrypt, Crypto, Asiacrypt, FSE and renowned journals.

Suprita Talnikar is Senior Research Fellow at the Applied Statistics Unit of the Indian Statistical Institute, Kolkata, India. She is pursuing her Ph.D. in Computer Science, under the supervision of Prof. Mridul Nandi. She completed her M.Sc. in Mathematics from Visvesvaraya National Institute of Technology, Nagpur, India, with a gold medal, and her B.Sc. in Physics, Computer Science and Mathematics from Rashtrasant Tukadoji Maharaj Nagpur University, Nagpur, India. Her research focuses on various areas of cryptography, with particular interest in provable security and cryptanalysis in symmetric key cryptography.