Cryptogr. Commun. (2018) 10:729–730
https://doi.org/10.1007/s12095-018-0312-7

Guest editorial

Subhamoy Maitra[1]

Received: 03 May 2018 / Accepted: 03 May 2018 / Published online: 19 May 2018

Prasanta Chandra Mahalanobis (29 June 1893 - 28 June 1972) was a visionary Indian scientist whose prime contribution was in development of Statistics. Around his 100-th birthday, cryptology research has been initiated at Indian Statistical Institute. After 25 years, the contribution of this institute in the field of cryptology has certainly received positive attention from the international community. In this context, to commemorate the 125-th Birthday of Professor (this is the name by which most of the persons at Indian Statistical Institute remember Professor Prasanta Chandra Mahalanobis, the founder), we thought it could be a good idea to underline the connection of Statistics and Cryptology once more. I must thank the Editor-in-Chief Prof. Claude Carlet for kindly accepting our proposal.

Over the last few decades, the cryptology community has witnessed a huge volume of high-quality research work in the domain of symmetric ciphers. There had been different proposals and standardization of several new designs as well as a considerable amount of analysis put forward by eminent academicians. In most of the cases the analysis is based on statistical techniques and in turn it helped the design process too. In light of this, a special issue on "Statistics in Design and Analysis of Symmetric Ciphers" could be of significant interest to the cryptology community. This is to harness some important research contributions devoted towards symmetric ciphers into a single literary volume with substantial archival value.

We received ten papers out of which six were invited and four were contributed. After a detailed and several (at least two) rounds of review process (at a similar standard for the invited as well as the contributed papers which is maintained for this journal), we could accept nine papers for this special issue. All the accepted papers consider deep and interesting statistical tools in the field of symmetric ciphers. We sincerely hope that this special

This article is part of the Topical Collection on *Special Issue on Statistics in Design and Analysis of Symmetric Ciphers*

✉ Subhamoy Maitra
subho@isical.ac.in

[1] Applied Statistics Unit, Indian Statistical Institute, Kolkata 700 108, India

issue, on “Statistics in Design and Analysis of Symmetric Ciphers” in the journal “Cryptography and Communications - Discrete Structures, Boolean Functions and Sequences”, will receive serious attention from the research community.

We would like to thank the authors of all the submitted papers and express our gratitude to the reviewers for their timely and thorough review work. We also acknowledge that this special issue would not have been possible without the support of Melissa Fearon and Katrina Turner in the editorial office of the journal.

Around the 100-th birthday of Professor Prasanta Chandra Mahalanobis, cryptology research at Indian Statistical Institute has been initiated by another young professor of Statistics. This year, we will have 60-th birthday of Prof. Bimal Roy. His contribution must also be acknowledged in the context of 25 years of cryptology research at Indian Statistical Institute and in Indian academia.