Guest editorial

Subhamoy Maitra · Palash Sarkar

Published online: 23 August 2012
© Springer Science + Business Media, LLC 2012

Discrete structures, sequences and Boolean functions constitute the basic building blocks of stream ciphers, the primary goal of which is to produce pseudo-random sequences of keystream words for cryptographic applications. Over the last decade, the cryptology community has witnessed a huge volume of high-quality research work in the domain of stream ciphers, spearheaded by the eSTREAM project of the European Network of Excellence for Cryptology and the evolution of the security portfolio in modern tele-communication standards. The field of stream ciphers has reached a decent level of maturity over the last few years through the proposal and standardization of several new designs as well as a considerable amount of analysis put forward by eminent academicians.

In light of this, we thought that a special issue on “Stream Ciphers” could be of interest to the cryptology community. This is to harness some important research contributions devoted towards stream ciphers into a single literary volume with substantial archival value. We must thank Prof. Claude Carlet, the Editor-in-Chief of the journal “Cryptography and Communications” for accepting this proposal.

For this special issue, we solicited the following in the field of stream ciphers:

1. novel contributions;
2. research contributions published and/or presented at past conferences and workshops, with substantial revision and new contributions;
3. expository survey articles in relevant topics.

We received 17 submissions (including three invited ones) and most of them were of publishable quality. After a detailed two round review process (at a similar standard for the invited as well as the contributed papers), we could accept eight (8) papers

S. Maitra (✉) · P. Sarkar
Indian Statistical Institute, 203 B. T. Road, Kolkata 700 108, India
e-mail: subho@isical.ac.in

P. Sarkar
e-mail: palash@isical.ac.in

for this special issue. In fact, there are quite a few papers (that could not be accepted in this special issue) which are still being considered for the regular issues of this journal. This is because these papers need more revision which would have delayed the publication of this volume further.

Among the eight articles, we have four expository papers. These papers are on correlation attacks, fast correlation attacks, high order differential attacks and cube attacks on stream ciphers. The remaining papers concentrate on specific problems. In one of the papers, nonlinearity issues of NFSRs have been studied. The other three papers are on analysis of three stream ciphers Trivium, Rabbit (alongwith a related Hash function) and WG-7 respectively.

We would like to thank the authors of all the submitted papers and express our gratitude to the referees for their timely and thorough review work. Finally, we must acknowledge that this special issue would not have been possible without the support of Melissa Fearon, Jeyel Tecson and Yvette Bascon in the editorial office of the journal.