EDITORIAL
Vol. 12 No. 3

Special Issue on Applied Cryptography & Data Security

Cryptography can be succinctly defined as the study of how to establish secure communication in an adversarial environment. Due to the numerous technological improvements, research in cryptography has addressed a whole new spectrum of more advanced practical problems, which has propelled this research area to become one of the most applied and active disciplines in computer science.

This special issue gives a glimpse of modern cryptography covering important areas such as computational number theory, construction of boolean functions, modes of operation for block ciphers and design and analysis of special purpose cryptographic hardware. We received a total of twenty-one manuscripts. Out of them, only six contributions were finally selected. The reviewing process took six months. Each manuscript was blindly reviewed by at least three reviewers consisting of guest editors and external reviewers.

The first paper in this special issue "Nontrivial Solutions to Cubic Sieve Congruence Problem: $x^3 \equiv y^2 z \bmod p$", was written by Subhamoy Maitra et al. This work addresses the cubic sieve congruence problem, which consists on finding small non-trivial solutions to the congruence $x^3 \equiv y^2 z \bmod p$.

The second paper in this issue is "Construction of Rotation Symmetric Boolean Functions with optimal Algebraic Immunity", by Sumanta Sarkar and Subhamoy Maitra. They present theoretical constructions of a special type of Boolean functions known as Rotation Symmetric Boolean Functions (RSBFs) of n variables, with n an odd number.

In the third paper, "A Generic Method to Extend Message Space of a Strong Pseudorandom Permutation", by Mridul Nandi, the author proposes a generic method to extend the message space of a strong pseudo-random permutation (SPRP) by using a primitive called weak pseudo-random permutation.

The fourth paper in this special issue is "Algebraic Immunity of Boolean Functions Analysis and Construction", by Deepak Kumar Dalai and Subhamoy Maitra. They study the problem of constructing a particular family of boolean functions that presents maximum possible algebraic immunity.

The fifth paper in this special issue is "Searching Prime Numbers with Short Binary Signed Representations", by José Angel Angel and Guillermo Morales-Luna. Authors provide an estimation of the density of primes with short binary signed representation.

The last paper in this special issue is "Hardware Architecture and Cost/time/data Trade-off for Generic Inversion of One-way Function", by Sourav Mukhopadhyay and Palash Sarkar. They propose a customized pipelined hardware architecture for implementing time-memory tradeoff attacks against generic cryptographic algorithms.

Finally, we would like to thank all authors who have submitted their manuscripts to this Special Issue. We would like also to express our gratitude to the following external reviewers: Omran Ahmadi, Rana Barua, Sanjit Chatterjee, Tanmoy Kanti Das, Arturo Díaz-Pérez, Levent Ertaul, Gerardo de la Fraga, Darrel Hankerson, Tetsu Iwata, Valery Korzhik, Julio López, Peris López, Subhamoy Maitra, Alfred Menezes, Sihem Mesnager, Peter Montgomery, Guillermo Morales-Luna, Daniel Ortiz-Arroyo, Dipti Prashad Mukherjee, Mridul Nandi, Carles Padró, Tomás Pevný, Bimal Roy, Erkay Savas, Somitra Sanadhya, Nazar A. Saqib, Francesc Sebé, Hebertt Sira-Ramírez, Berk Sunar, Jaime Velasco-Medina, King-Hang Wang, Amr M. Yousef and Xiangyong Zeng,

Guest Editors
Francisco Rodríguez-Henríquez and Debrup Chakraborty.
Computer Science Department, CINVESTAV-IPN.