SPECIAL COLLECTION: SECURITY

This Special Collection consists of extended and/or reworked versions of selected papers presented at the Australasian Information Security Workshop (Privacy Enhancing Technologies) 2007, and at the Australasian Information Security Conference 2008. These two conferences received a total of 50 submissions, 21 of which were accepted and presented. We invited the authors of the top 50% conference papers to extend their work and submit it for publication in the JRPIT Special Collection on Privacy and Cryptography. We conducted another refereeing process, and out of the ten submissions received we accepted four high quality papers for the Special Collection on Privacy and four for this Special Collection on Security.

Workflow management systems are investigated in the paper entitled "Deploying Access and Flow Control in Distributed Workflows" by Samiha Ayed, Nora Cuppens-Boulahia and Frederic Cuppens. The authors consider security issues in such systems and note that the current solutions are based on a centralised and static approach and do not support information flow control. They propose a new decentralized and dynamic system that incorporates both access and flow control. Furthermore, the authors study the complexity of this problem.

The remaining three papers focus on cryptography.

Stream ciphers and their keystream sequences are considered in "Linear Cellular Automata as Discrete Models for Generating Cryptographic Sequences" by Pino Caballero-Gil, Amparo Fúster-Sabater and Oscar Delgado-Mohatar. The authors use a Cellular Automata based linear model to generate all those keystream sequences that are solutions of linear binary difference equations. Such sequences are traditionally generated by Linear Feedback Shift Registers whose outputs are then combined by means of non-linear functions. The new approach is particularly valuable for applications that require high efficiency.

Elliptic curves over finite fields are becoming increasingly important for the design of cryptographic protocols as they make the problem of finding discrete logarithms significantly harder than is the case with traditionally used multiplicative groups over finite fields. This allows shorter keys to be used which is particularly important in hardware implementations of cryptographic systems. In their paper "Exploiting Isogeny Cordillera Structure to Obtain Cryptographically Good Elliptic Curves", J. Miret, D. Sadornil, J. Tena, R. Tomàs and M. Valls give an algorithm for generating cryptographically good elliptic curves from a given curve, thus simultaneously allowing for increased security and ease of implementation by changing the elliptic curve but not the underlying finite field.

"Correct, Private, Flexible and Efficient Range Test" by Kun Peng, Ed Dawson and Feng Bao proposes a novel range test, where a party holding a ciphertext learns only whether the corresponding plaintext is within a given range or not. Unlike previously proposed tests, it simultaneously achieves correctness, soundness, privacy and efficiency.

We thank Professor Sidney Morris, the Editor-in-Chief of JRPIT, and Ms Rosemary Hay for their invaluable help and support, the reviewers for their effort and constructive comments, and the authors for their high-quality submissions.

Ljiljana Brankovic, PhD
Guest Editor
School of Electrical Engineering and Computer Science
The University of Newcastle

Mirka Miller, PhD
Guest Editor
School of Electrical Engineering and Computer Science
The University of Newcastle

Chris Steketee, PhD
Guest Editor
School of Computer and Information Science
University of South Australia