The ISC Int'l Journal of Information Security
ISeCure

January 2012, Volume 4, Number 1 (pp. 1–2)
http://www.isecure-journal.org

From the Editor-in-Chief

Editorial

Welcome to the first issue of the fourth volume of ISeCure. Based on the Editorial Board decision, this issue is devoted to the extended/revised versions of some of ISCISC'11 selected papers, which passed an additional review process by our referees. ISCISC is an international conference on security and cryptology, initiated and being organized annually by the Iranian Society of Cryptography (ISC). The eighth series of this conference (ISCISC'11) was held at the Ferdowsi University of Mashhad in September 2011. In this issue, we publish seven papers of this category. The title of the papers are similar to or the same as the corresponding papers in the conference, but the content was extended, and revised based on the comments received in the second (and possibly third) round of the review. In some cases, where the conference paper had been written in Persian, the article appearing here was rewritten in English.

In addition, starting from this issue, the Editorial Board decided to publish a single page per paper, containing the Persian translation of the title, author information, abstract, and keywords, to be utilized by Persian indexing centers.

Our **first paper** of this issue presents an efficient joint secret key encryption-channel coding cryptosystem, based on regular Extended Difference Family Quasi-Cyclic Low-Density Parity-Check codes. The improved cryptosystem has significant security and efficiency advantages over Rao-Nam and the previous secret key code-based cryptosystems. Besides, there is no trade-off between efficiency and security of the proposed cryptosystem.

The **second paper** concentrates on Multi–Chi-square tests. The ANF monomial test was modified to extract two new tests which were applied to Trivium with the same number of rounds. This resulted in 24 times reduction in the data complexity of the rounds. The paper also investigates the relation between the critical degrees of freedom and the chi-square statistic of a Multi–Chi-square test. A method to approximate the data complexity of a distinguishing Multi–Chi-square test is introduced and shown to perform properly in the special case of reduced round Trivium.

The **third paper** presents a dynamic hybrid approach based on the artificial bee colony (ABC) and negative selection (NS) algorithms, called BeeID, for intrusion detection in AODV-based MANETs. The approach runs a niching artificial bee colony algorithm to generate a set of negative detectors to cover the nonself space and uses the Monte Carlo integration to estimate the amount of the nonself space covered by negative detectors. The experimental results show that BeeID can achieve a better tradeoff between detection rate and false alarm rate as compared to other approaches in the literature.

The **fourth paper** focuses on data outsourcing through a prototype model of private-key based search on encrypted data. The model is improved to meet security requirements, while it handles queries on encrypted data, including arbitrary words, using a minimal trust model. The authors also present a model to balance between

ISSN: 2008-2045

performance and security based on user's requirements. In comparison with other methods, query response time is improved and the probability of statistical deductions is reduced.

The **fifth paper** proposes an unsupervised method for online detection of botnets in early stages of their lifecycle, called BotOnus. BotOnus is aimed to identify a group of bot-infected hosts within a monitored network that are part of the same botnet. The effectiveness of BotOnus to detect various botnets including HTTP-, IRC-, and P2P-based botnets is demonstrated using a testbed network. The results of experiments show that it can successfully detect various botnets with a high detection rate and a low false-alarm rate.

The **sixth paper** introduces two different approaches for designing image-based CAPTCHAs. The Tagging image CAPTCHA is based on pre-tagged images and uses geometric transformations to increase security. This is enhanced by eliminating the use of tags and relying on semantic visual concepts through the recognition of upright orientation. The usability and security of the proposed approaches are verified. The result of studies on the proposed transformations proposes a practical and secure Semantic Image CAPTCHA.

Our **last paper** in this issue proposes a video watermarking algorithm based on chaotic maps. The paper is devoted to the study of spatial domain watermarking, and exhibits potent defense against common unintended or malicious attacks. To make the technique immune against collusion attacks, embedding of different watermarks in different frames were carried out with good results. From the security perspective, assuming that watermarking based on tent map encryption was opted for.

Rasool Jalili

Editor-in-Chief,

ISeCure