The ISC Int'l Journal of Information Security
ISeCure

July 2015, Volume 7, Number 2 (pp. 89–90)
http://www.isecure-journal.org

From the Editor-in-Chief

Editorial

Welcome to the second issue of the seventh volume of the journal. In this issue, we publish six papers as well as a single page per paper incorporating the translation of the title and abstract in Persian, to be used by Persian indexing centers.

The **first** paper of this issue entitled "Computationally Secure Multiple Secret Sharing: Models, Schemes, and Formal Security Analysis" is the first formal model for indistinguishability against the chosen secret attacks (CSA) for multi-stage and general multi-secret sharing schemes. In this paper two CSA-secure multi secret sharing schemes are proposed and their security are proved in the standard model.

An "Efficient Implementation of Low Time Complexity and Pipelined Bit-Parallel Polynomial" is the **second** paper in this issue. The paper presents two efficient implementations of fast and pipelined bit-parallel polynomial basis multipliers over $GF(2^m)$ by irreducible pentanomials and trinomials. The architecture of the first multiplier is based on a parallel and independent computation of powers of the polynomial variable, and, in the second structure only even powers of the polynomial variable are used.

The **third** paper in this issue proposes a GGH-Like Public Key Cryptosystem Over The Eisenstein Integers Using Polynomial Representation, named EEH. EEH applies representations of polynomials to the GGH encryption scheme. Theoretical and experimental data for comparing the security and efficiency of EEH and GGH using comparable parameter sets shows that EEH is an improvement over GGH in terms of security and efficiency.

The **fourth** paper is "Cryptanalysis of Some First Round CAESAR Candidates". AES_CMCCv1, AVALANCHEv1, CLOCv1, and SILCv1 are four candidates of the first round of the CAESAR competition on authenticated encryption schemes.. CLOCv1, and SILCv1 were selected as the second round candidates in CAESAR, but AES_CMCCv1 and AVALANCHEv1 remained in the first round. In this paper, structural weakness of these candidates is studied. In this paper distinguishing attacks against AES_CMCCv1 with the complexity of two queries and the success probability of almost 1 is proposed. Also, distinguishing attacks on CLOCv1 and SILCv1 with the complexity of $O(2^{n/2})$ queries and the success probability of 0.63, in which n is bit length of message blocks, are proposed.

Privacy analysis of two novel RFID authentication protocols is the subject of the **fifth** paper in this issue. Different types of traceability attacks including traceability, backward traceability and forward traceability against the first protocol is proposed. It is shown that the second protocol not only suffers from the Denial-of-Service (DoS) attack, but also it is also vulnerable to the traceability and backward traceability attacks. Finally, in order to overcome the mentioned weaknesses, two novel mutual authentication protocols for RFID systems are proposed.

Our **sixth** paper in this issue is “Collusion Mitigation Scheme for Reputation Systems”. The proposed paper has three main contributions. First, a similarity measure (CSM) is proposed. Second, a heuristic clustering algorithm (CDA) which uses CSM, to detect colluders is introduced. Finally, an architecture for implementing the algorithm in a distributed manner is suggested by the authors.

Finally, I would like to sincerely thank all the authors for their submitted research papers, and acknowledge our reviewers for their invaluable and critical reviews, which helped us to keep the quality of ISeCure and its current standard.

Rasool Jalili

Editor-in-Chief,

ISeCure