The ISC Int'l Journal of Information Security

ISeCure

January 2019, Volume 11, Number 1 (pp. 1–2)

http://www.isecure-journal.org

From the Editor-in-Chief

Editorial

Welcome to the first issue of the eleventh volume of the journal. In this issue, we publish six regular 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.

In the **first** paper of this issue, security issues of data outsourcing and the problem of query result verification are addressed. When data and its management are outsourced to an external server, whose honesty is not guaranteed in practice, there should be a way to inspect the correctness of results returned from the server. This paper proposal exploits Merkle Hash Tree as an authentication data structure and uses the notion of trust, computed based on the history of client-server interactions, in order to reduce client-side computation overhead pertaining to the verification process. The amount of trust towards the server adjusts computation overhead during correctness verification. As much as the trust value increases due to previously verified results, the verification process becomes more efficient at the client side.

A new cryptosystem called searchable outsourcing scheme for ordered structured data (SESOS) and its extended variant (XESOS) were proposed in the **second** paper of this issue. SESOS provides the ability to execute LIKE queries, along with the search for exact matches, as well as comparison. Moreover, XSESOS allows for verifying the integrity of ciphertexts. Both schemes combined any order-preserving encryption (OPE) with a novel encryption scheme called Multi-map Perfectly Secure Cryptosystem (MuPS). By proving the perfect secrecy of MuPS, authors demonstrate that SESOS possess the same security properties of the underlying OPE scheme. In addition, SESOS and XSESOS were evaluated under various criteria. Besides, it is shown that the overhead is negligible compared to the underlying OPE scheme, while it outperforms the OPE.

The **third** paper of this issue characterized the MDS property of a class of 4×4 matrices which are the product of binary and companion matrices of Sigma-LFSRs. The result of this characterization is the optimization of the implementation cost, measured by the number of XORs required, of classical recursive MDS matrices. Moreover, it leads to a smart search to find lightweight 4×4 MDS matrices which have the same implementation cost as the lightest existent MDS matrix.

In the **fourth** paper of this issue, a scheme to both prevent and detect Hardware Trojan Horses (HTHs) attacks on Field Programmable Gate Array (FPGA) is proposed. The scheme employs shift register and gate-chain insertion to fill the unused space of FPGAs. Moreover, delay pattern and logical output analyzing of gate-chain and shift register would help with the detection process. According to the authors' experimental result, the protection/detection scheme imposes no power overhead with no degradation in delay and performance of the main design.

Early abort technique is used in the matching part of the biclique attack to reduce the data complexity enormously by a shorter biclique, in the **fifth** paper of this issue. A shorter biclique usually results in less data complexity, but at the expense of more computational complexity. However, in this paper instead of slight

ISSN: 2008-2045

improvement in the computational complexity, the amount of this complexity is kept the same. By utilizing this approach, full-round LBlock, LBlock with a modified key schedule, and TWINE-80 are analyzed with data complexity 212. The proposed key schedule is more resistant against biclique cryptanalysis, though the low diffusion of the cipher makes it vulnerable to this attack regardless of the strength of the key schedule. In all the attacks presented in this paper, the computational complexities are slightly improved in comparison to the existing attacks.

A new efficient ring-based smooth projective hash function (Ring-SPHF) is presented in the sixth paper of this issue. Using Ring-SPHF, the authors proposed the first efficient password-based authenticated key exchange (Ring-PAKE) protocol over rings. They claimed that Ring-PAKE is secure and its security relies on ideal lattice assumptions.

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

Mohammad Reza Aref
Editor-in-Chief,
ISeCure