Fundamenta Informaticae 157 (2018) v–viii
DOI 10.3233/FI-2018-1614
IOS Press

Special Issue on Advanced Cryptographic Techniques for Cloud and Big Data Computation

Preface

1. Introduction

Cloud computing enables the delivery of on-demand computing resources, from applications to data centers, based on the paradigm of everything as a service. On the other hand Big Data is a disruptive technology, at the centre of the future knowledge discovering society. The techniques by which Big Data is generated, collected, processed, computed and communicated are being developed at a good pace. However there are many security issues around Cloud and Big Data computation due to wide spread of Cloud and Big Data applications in people's everyday life. Many advanced cryptographic techniques developed in recent years can contribute to solve these challenging issues, such as attribute based encryption/signature, functional encryption/signature, homomorphic encryption/signature, garbled circuits and obfuscation, etc.

This special issue aims to provide recent research findings and new methods in the field of advanced cryptographic techniques for Cloud and Big Data computation, with special emphasis on efforts related to the foundational theory and practical engineering applications. Thus, the special issue addressed the topics of:

- Cryptographic access control techniques for cloud and big data storage
- Advanced cryptographic computation techniques for cloud and big data
- Flexible cryptographic searching techniques for cloud storage and big data stream
- Advanced cryptographic aggregating primitives for cloud and big data
- Proof of data position/ownership techniques for cloud and big data
- Advanced authentication techniques for cloud and big data computation

2. Special Issue Content

The special issue contains 12 papers, selected after a strict review process in 2-3 rounds of reviewing and revising. The papers of the special issue are organised into two groups as follows.

The first group of six papers covers research topics related to various forms of encryption.

In the first paper [1], Zhang deals with Attribute Based Encryption (ABE), namely, to model a fine-grained attribute revocable attribute-based encryption (ADR-lrABE) aimed to tolerate the possible key leakage. The author gives the concrete construction, security analysis and resilient-leakage performance and analyses the leakage-resilient performance of their scheme. It is shown that the scheme achieves approximate (82 + o(1)) fraction of the bits of a decryption key being leaked. The proposed schemes are the first ABE that support attribute direct revocation mechanism in the presence of key leakage in noise channel or memory leakage environments.

Li *et al.* in the second paper [2], propose the notion of star-topological encryption that achieves identity-based encryption and identity authenticity, simultaneously. An encryption scheme is constructed to achieve this cryptosystem based on non-abelian groups. The security of the scheme is based on the intractability of factorization search problem over non-abelian algebraic structures. The proposed cryptosystem is proven secure against determinant attacks and quantum attacks.

The third paper [3] by Wang *et al.*, proposes an efficient PRE scheme (Proxy re-encryption (PRE)) based on the intractability of the (semi)group factorization problems. The aim is to overcome some limitations of existing PRE schemes based on intractability assumptions such as integer factorization problems and discrete logarithm problems.The security of the proposed scheme is analysed according to some heuristic attacks. Moreover, a special instantiation technique is presented in detail, and some illustrations are provided to show the effectiveness and efficiency of the proposed scheme.

In the fourth paper [4], Wei *et al.* address the limitations of homomorphic encryption when operating over the ciphertext. The authors consider the specific case of marine sensor networks where sensors collect the multiple data using a single hardware unit. It is shown that directly using the homomorphic encryption cannot perform well in marine sensor data forwarding since the data need to turn to satellites or vessels as relays and be forwarded in multi-hop way. The authors design a secure data forwarding protocol based on the Paillier homomorphic encryption and multi-use proxy re-encryption. The experiment results show that the additional computational overhead brought by cryptographic operations could be minor and it has the merit of providing fixed data size passing through the multi-hop transmission.

Jeyabalu and Krishnamoorthy in the fifth paper [5] present application service that provides security as a service in the Cloud to the users. The proposed service is based on a symmetric key encryption scheme where a key generation is achieved from hybridization of improved cipher block chaining encryption operation and another one from nature inspired genetic algorithm. The aim is to minimize the execution time and storage space capacity. The experimental analysis reports that the proposed application service offers potential for authenticating multimedia files with better satisfaction while out-sourced as application in cloud computing environment.

The sixth paper by Jiguo Li *et al.* [6], studies the usefulness of aggregate signature schemes in resource constrained environment. The authors show that a recently improved scheme is not secure against a malicious-but-passive KGC attack. By analysing attack reason the authors propose an improved certificateless aggregate signature scheme. Based on the CDH difficult problem assumption, the proposed certificateless aggregate signature scheme is existentially unforgeable against adaptive chosen-message attacks in the random oracle model.

The second group of six papers covers research topics related to secure authentication schemes, secure Cloud storage and auditing protocols, secure access control schemes and secure IoT applications.

In the seventh paper, Wei *et al.* [7], investigate the lightweight block cipher, which is useful in Internet of Things to protect confidentiality as well as to authentication. The authors consider the LBlock –a lightweight block cipher designed for tiny computing devices, such as RFID tags and sensor network node– and is shown resistant against most classical attacks, such as differential and linear cryptanalysis. The authors propose differential fault analysis on LBlock based on different depth of fault model, the theoretical analysis demonstrates that LBlock is vulnerable to deep differential fault attack due to its Feistel structure and diffusion layer indicating that cryptographic devices supporting LBlock should be carefully protected.

The eighth paper by Huajun Zhang *et al.* [8], discusses issues related to disaster recovery of files in Cloud storage systems when backups of a file are stored in several positions far away from each other. The authors construct a generic transformation from "Proof of Retrievability" to "Proof of Multicopy". Their approach is achieved in two stages, namely, in the first is designed a generic protocol of "Proof of File Position" based on an arbitrary secure "Proof of Retrievability" protocol; in the second stage, the authors construct a "Proof of Multicopy" protocol based on our "Proof of File Position" protocol. Both protocols are shown provably secure.

Miao Zhang *et al.* in the ninth paper [9], analyse the authentication challenges in smart home systems. To thoroughly detect, defense and foresee the authentication vulnerabilities existing in smart home networks, the authors propose a security evaluation technique based on attack graph generation. The authors discuss the distinction between the attack graphs deployed in traditional networks and in smart home networks. Furthermore, they apply this technique in an experimental setting, and the results prove its practicality.

In the tenth paper [10], Lei *et al.*, introduce an encryption scheme for access control in Cloud-Internet of Things. The proposed scheme is constructed in three steps. The first step makes use of cipher-policy attributes based encryption to empower robustness and flexibility. In a second step an advanced scheme to improve the computation efficiency by taking the advantages of proxy-reencryption is designed. Finally in the third step, the authors propose an enhanced scheme to protect integrity by using aggregate signature. The robustness and the flexibility of the proposed schemes is analysed by performance analysis.

The eleventh paper [11] by Zhang and Wang is concerned with auditing protocols for cloud storage. The authors achieve an improvement of Chen *et al.* cloud storage audit protocol presented at Infocom 2015. The aim of the new protocol is to strengthen its security. In particular, the authors show that if the data owners reuse pseudo-random function on the same order number of file block when uploading file block tags to the cloud, the protocol may be not secure any more. The authors also discuss some issues in the traditional security model of cloud storage auditing protocol, which deserve further investigation and attention.

Finally, in the last paper [12] Fushan Wei *et al.* investigate issues related to Two-Factor Authenticated Key Exchange (TFAKE) protocols, which are are critical tools for ensuring identity authentication and secure data transmission for cloud computing.The authors analyse the security requirements and put forward a formal security model for TFAKE protocols for cloud computing. Then, an efficient TFAKE protocol without using expensive asymmetric cryptology mechanisms to achieve high efficiency is presented. The proposed protocol can be proven secure in the random oracle model achieve, user anonymity and be more efficient than existing similar protocols.

Acknowledgment

The editors of this special issue would like to thank all authors for their contributions. The time and efforts of reviewers for their constructive and useful feedback to authors are highly appreciated. We would like to thank Prof. Damian Niwinski, the Editor-in-Chief of *Fundamenta Informaticae*, for the opportunity to edit this special issue and his support. Finally, we would like to acknowledge the help by Marcin Szczuka during the preparation of this special issue.

References

[1] Zhang M. ADR-lrABE: New Mechanism of Direct-revocable Attribute-Based Encryption with Continual-leakage Tolerances. *Fundamenta Informaticae*, 2017. (This Issue).

[2] Li J, Wang L, Niu X, Gu L. Star-Topological Encryption: Talking to the Sever but Hiding Identities to Others. *Fundamenta Informaticae*, 2017. (This Issue).

[3] Wang L, Li J, Gu L, Yan J, Quy Z. An Efficient Construction of Quantum Attack Resistant Proxy Re-Encryption Based on (Semi)group Factorization Problems. *Fundamenta Informaticae*, 2017. (This Issue).

[4] Wei L, Zhang K, Zhangy L, Huang D. A Secure Data Forwarding Protocol for Data Statistics Service in Multi-Hop Marine Sensor Networks. *Fundamenta Informaticae*, 2017. (This Issue).

[5] Jeyabalu M, Krishnamoorthy K. Hybridization of ICBC and Genetic Algorithm for Optimizing Encryption process in Cloud Computing Application Service. *Fundamenta Informaticae*, 2017. (This Issue).

[6] Li J, Yuan H, Zhang Y. Cryptanalysis and Improvement for Certificateless Aggregate Signature. *Fundamenta Informaticae*, 2017. (This Issue).

[7] Wei Y, Rong Y, Fan C. Differential Fault Attacks on Lightweight Cipher LBlock. *Fundamenta Informaticae*, 2017. (This Issue).

[8] Zhang H, Cao Z, Dong X, Shen J. Proof of Multicopy via Proof of File Position in Cloud. *Fundamenta Informaticae*, 2017. (This Issue).

[9] Zhang M, Wang C, Liy Y, Wang J, Tian S. A New Approach to Security Analysis of Smart Home Authentication Systems. *Fundamenta Informaticae*, 2017. (This Issue).

[10] Lei M, Yang Y, Ren W, Ren Y. RoFa: A Robust and Flexible Fine-Grained Access Control Scheme for Mobile Cloud and IoT based Medical Monitoring. *Fundamenta Informaticae*, 2017. (This Issue).

[11] Zhang J, Wang B. An Improved Secure Cloud Storage Auditing Protocol Based on Distributed String Equality Checking. *Fundamenta Informaticae*, 2017. (This Issue).

[12] Wei F, Zhang R, Ma C. A Provably Secure Anonymous Two-Factor Authenticated Key Exchange Protocol for Cloud Computing. *Fundamenta Informaticae*, 2017. (This Issue).

Editors:

Fatos Xhafa
Department of Computer Science
Technical University of Catalonia, Spain
fatos@cs.upc.edu

Zhenfu Cao
School of Computer Science and Software Engineering
East China Normal University, China
zfcao@sei.ecnu.edu.cn