The Computer Journal is one of the longest-established journals of the academic computer science community. It publishes high-quality papers and the latest ideas in computer science in four sections.

Section A Computer Science Theory, Methods and Tools
Section A has as its primary focus the theory and methodologies that are central to computer science. The section welcomes contributions from across this spectrum as well as papers involving the novel application of theoretical research or the adaptation of established methodologies to computational problems in other domains or within software tools. Thematic areas include but are not restricted to: algorithms, data structures, combinatorics, computational complexity, cryptography, mathematical computing: models of computation and distributed computing; programming languages and semantics; and software engineering.

Section B Computer and Communications Networks and Systems
Section B focuses on new theories, ideas and developments in computer communications, networks, and related systems. The section seeks high-quality papers reporting new concepts, analyses and experimental results in areas including but not limited to: network architectures and protocols; traffic engineering; resource management and quality of service; network monitoring and traffic measurements; wireless networks; personal and body area networks; vehicular networks; content and service-centric networking; energy efficient/efficient networking; opportunistic and cognitive networks; and networking in extrastreem environments.

Section C Computational Intelligence, Machine Learning and Analytic
Section C provides solutions and addresses challenging problems in such areas as data mining, image and signal processing, knowledge-based systems and the semantic web. Further thematic areas covered in this section include computational statistics, pattern recognition, computational intelligence, machine intelligence and reasoning, science, information retrieval and emerging application domains in big data, e-science and u-science. It welcomes submissions with new methodology that is very extensively evaluated, and showing strong and significant results.

Section D Security in Computer Systems and Networks
The main focus of Section D is the provision of security and privacy in computer systems and networks. Contributions are welcome across all the main areas of computer security and privacy, including, but not limited to: cryptography and applications; security protocol design and analysis; intrusion detection systems and techniques; computer system security hardware and embedded system security issues; user authentication techniques and systems.

The issue date is December 2017.
CONTENTS

ORIGINAL ARTICLES

1729 Weakness and Improvement of a Certificate-Based Key-Insulated Signature in the Standard Model
Yang Lu, Jiguo Li, and Jian Shen

1745 Detection of Phishing Websites Based on Probabilistic Neural Networks and K-Medoids Clustering
El-Sayed M. El-Alfy

1760 Satisfiability-Based Privacy-Aware Cloud Computing
Abderrahim Aal Wakrim

1770 Detection of SIP-Based Denial of Service Attack Using Dual Cost Formulation of Support Vector Machine
Jayashree Poujajendy and Arun Raj Kumar Parthiban

1785 Homomorphic MAC from Algebraic One-Way Functions for Network Coding with Small Key Size
Ying Wu, Jinyong Chang, Rui Xue, and Rui Zhang

1801 Comment on ‘Attribute-Based Signatures for Supporting Anonymous Certification’ by N. Kaaniche and M. Laurent (ESORICS 2016)
Damien Vergnaud

1809 Fully Privacy-Preserving ID-Based Broadcast Encryption with Authorization
Jianchang Lai, Yi Mu, Fuchun Guo, and Rongmao Chen

1822 Authorized Equi-join for Multiple Data Contributors in the PKC-Based Setting
Sha Ma

1839 Statistical Cipher Feedback of Stream Ciphers
Howard M. Heys

1852 Difference-Comparison-based Malicious Meter Inspection in Neighborhood Area Networks in Smart Grid
Xiaofang Xia, Wei Liang, Yang Xiao, and Meng Zheng

1871 Auditing Revocable Privacy-Preserving Access Control for EHRs in Clouds
Weiran Liu, Xiao Liu, Jianwei Liu, and Qianhong Wu

1889 ASCENT: A Provably Terminating Decentralized Logging Service
Xavier Bonnaire, Rudyar Cortés, Fabrice Kordon, and Olivier Marín

1912 Partitioned Group Password-Based Authenticated Key Exchange
Dario Fiore, María Isabel González Vasco, and Claudio Soriñete