Big Data Analytics (BDA) is one of the mainstream technologies that change our perspectives on processing of information. Together with information security, BDA could be an extremely effective tool to learn more about communication and social networks. There will be infinite possibilities to find new methods of tracking cybercrimes using big data from different sources. BDA in information security also changes our thinking about security algorithms; they must change from a small data paradigm to big ones. This special issue is to analyze how the latest trends in this area help learn more about cyberspace and new threats using big data approaches. It contains seven papers and the details were listed as follows:

(1) J. Li et al. proposed a privacy protection framework to preserve multiparty data privacy throughout its lifecycle in cloud computing, which was built upon several cryptography primitives and differential privacy. They also gave related security analysis, instantiation, and application scenarios. To conquer potential attacks in the semihonest model, they further presented the new extensions to proposed framework. The performance discussion indicated that the proposed framework owned advantages in security guarantees and thus was more desirable for secure multiparty data aggregation and publishing.

(2) X. Niu et al. proposed an E-cent-based privacy-preserving incentive mechanism (EPPI). Inspired by physical currency circulation system, they introduced the notion of E-cent, an exchangeable unit bearer currency. EPPI seems to be the first attempt to build an incentive mechanism while maintaining the desired privacy preserving in participatory sensing systems. Extensive simulation and analysis results showed that EPPI could achieve high anonymity level and remarkable incentive effects.

(3) S. Zhang et al. proposed a model of virtual machine security monitoring based on memory introspection. Compared with previous memory introspection technologies, the proposed solution can automatically reconstruct the comprehensive running state of a target virtual machine without any prior knowledge and is strongly resistant to attacks with high reliability. Experimental results indicated that a prototype system can handle the virtual machines of mainstream Linux and Windows OS versions with high efficiency and does not influence the performance of the host machine and virtual machines.

(4) H. Rong et al. proposed a set of privacy-preserving building blocks and outsourced $k$-means clustering protocol under Spark framework. Theoretical analysis showed that proposed scheme protects the confidentiality of the joint database, mining results, and access patterns under the standard semihonest model with relatively small computational overhead. Experimental evaluations on real datasets also demonstrated its efficiency improvements compared with existing approaches.

(5) D. Hu et al. analyzed the problem of concept drift phenomenon in Android malware detection and
proposed a solution based on an ensemble classifier, where each random feature set is deployed on each subclassifier. Based on the performance of the subclassifiers inside the sliding window, the ensemble classifier makes dynamic adjustments to address the concept drift problem in Android malware detection.

(6) Y. Ping et al. analyzed hidden field equations (HFE) family of schemes in multivariate public key cryptography and proposed a new variant of HFE. They showed that the proposed scheme is secure against known attacks including the MinRank attack, the algebraic attacks, and the linearization equations ones. The proposal gained some advantages over the original HFE scheme with respect to the encryption speed and public key size.

(7) Z. Xiangyang et al. proposed an efficient and accurate and verifiable privacy-preserving multikeyword text search over encrypted cloud data based on hierarchical agglomerative clustering. According to hierarchical agglomerative clustering, they constructed a binary tree structure as the index, which was named HAC-tree. Based on HAC-tree, they provided a noncandidate pruning depth-first search algorithm to improve search efficiency. Besides, the authors utilized secure inner product algorithm against two threat models. The experimental results showed that the scheme proposed in this paper had better comprehensive performance in terms of efficiency and accuracy compared with the existing methods.

Acknowledgments

We would like to thank all the authors for their fine contributions to this special issue and all the reviewers who upheld the quality of this special issue by critically evaluating the papers and reviewing several revisions within a short time.

Krzysztof Szczypiorski
Liqiang Wang
Xiangyang Luo
Dengpan Ye