Preface

Justin Zhan

Department of Computer Science,
North Carolina A&T State University,
1601 East Market Street, Greensboro, NC, 27410, USA
E-mail: zzhan@ncat.edu

Biographical notes: Justin Zhan is the Director of iLab within the Department of Computer Science at North Carolina A&T State University. His research interests include social network science, social computing, information assurance, data mining, and simulation tool development. He has founded the IEEE International Conference on Social Computing (SocialCom), one of the premier conferences focusing on the social network and computing field. He is the Steering Committee Chair of the IEEE International Conference on Privacy, Security, Risk and Trust (PASSAT). He is currently the Editor-in-Chief of the *International Journal of Privacy, Security and Integrity*. He has served as conference general chair, programme chair, publicity chair, workshop chair, and programme committee member for over 150 international conferences and as editor-in-chief, editor, associate editor, guest editor, editorial advisory board member, and editorial board member for 30 journals. In recent years, he has published 130 articles in peer-reviewed journals and conference proceedings and delivered 30 keynote speeches and invited talks.

In the past decades, information technology has influenced and changed many aspects of our lives and cultures. With the advancement of information technologies, the information insurance has come to an important stage. In this issue, there are seven papers having been selected. In the first paper, Chen and Li have introduced VLR group signatures with indisputable exculpability and efficient revocation. The original verifier-local revocation (VLR) together with the group signature scheme introduced by Boneh and Shacham requires a fully trusted key issuer to create each group member's private key. If the trustworthy of the key issuer is arguable, the entire scheme is then suffering from lacking exculpability, which no group members including a group issuer can produce signatures on behalf of other group members. The authors improved their group signature scheme by taking indisputable exculpability into account. The indisputable exculpability is achieved by adding a dispute process, upon which a true signer cannot deny that a given group signature was created under his private key and membership credential. In the next paper, Yap et al. presents a smart-card-based secure user-centric attestation framework for location-based services. In particular, they designed a secure user-centric attestation service framework that can help user to generate, attest, share and verify personal information without jeopardising the user's privacy. The framework incorporates user's action information into spatial-temporal information rendered from location-based service to generate attestable action-spatial-temporal evidence through secure means. In the following paper, Larsen and Huckett have proposed a scheme on multi-method synthetic data generation for confidentiality and measurement of disclosure risk. To enable government agencies to disseminate useful micro-data and maintain confidentiality of individual records, they propose to create synthetic data using a

combination of quantile regression, hot deck imputation, and rank swapping. The result is a releasable data set containing original values for a few key variables, synthetic quantile regression predictions for several variables, and imputed and perturbed values for remaining variables. The procedure provides quality data to the user and simultaneously protects the confidentiality of respondents.

Effective access to web resources requires the development of approaches for enabling the user to organise and manage all her credentials and regulate their release when interacting with other parties over the web. In the fourth paper, Ardagna et al. provide a means for the user to specify how much she values the release of different properties, credentials, or combinations thereof as well as additional constraints that she might impose on information disclosure. Exploiting a graph modelling of the problem, the user can determine the credentials and properties to disclose to satisfy a server request while minimising the sensitivity of the information disclosed. They also develop a heuristic approach that shows execution times compatible with the requirements of interactive access to web resources. In next paper, Cha et al. propose a scheme, which is adopted by the RFID applications for campus security and safety enhancement project in Taiwan, to help RFID application providers establish RFID privacy policies in consideration of enforcement of the policies. By using the proposed scheme, RFID application providers can clarify privacy practices for their applications in RFID privacy policies and communicate these policies with application users. Moreover, application providers can provide evidence to third parties trusted by both application providers and users to ensure that the application providers follow their disclosed policies. In sixth paper, Taheri et al. propose an RDIS protocol to provide destination location privacy in MANETs which is based on some modifications in the packet flows in the network layer. They applied RDIS on top of ANODR as the ID anonymity routing protocol while it could be applied to some other anonymous MANET routing protocols in the appropriate way. The main idea is to hide the real destination among an anonymity set of nodes in the network. The privacy level depends on the protocol parameters as well as the node density. The achieved level of location privacy is valid even against a global eavesdropping adversary and decreases when the network includes some internal adversaries which are modelled as captured nodes.

Many ciphertext policy attribute-based encryption (CP-ABE) schemes do not protect receivers' privacy, since all the attributes to describe the eligible receivers are transmitted in plaintexts. To address this issue, in the last paper, Zhou and Huang propose a new concept, gradual identity exposure (GIE), to protect data receivers' identity. Their main idea is to reveal the receivers' identities (i.e., the access policy) gradually in the process of decryption, where the required attributes are exposed one-by-one. If the receiver does not possess one attribute in the decryption procedure, the rest of attributes remain hidden. Compared to hidden-policy based solutions, GIE supports more flexible access policy and, more importantly, provides significant performance improvement in terms of both computation and communication performances.