Preface

Feng Bao

Institute for Infocomm Research,
1 Fusionopolis Way, Singapore
Email: baofeng@i2r.a-star.edu.sg

Guilin Wang*

The School of Computer Science,
University of Birmingham,
Birmingham B15 2TT, UK
Email: G.Wang@cs.bham.ac.uk
*Corresponding author

Biographical notes: Feng Bao is currently a Principal Scientist and the Head of Cryptography and Security Department of Institute for Infocomm Research (I^{2}R), Singapore. He is also an Adjunct Professor of the School of Information System, Singapore Management University. He received his BS in Mathematics and MS in Computer Science from Beijing University in 1984 and 1986 respectively. After that he was a Researcher with Chinese Academy of Science and a Visiting Scientist with Hamburg University. He received his PhD in Computer Science from Gunma University, Japan 1996 and has joined I^{2}R since then. His research interests include automata theory, distributed computing, fault tolerance, cryptography and information security. He has published over 200 refereed papers at international conferences and journals and owned 16 patents.

Guilin Wang is currently a Lecturer in the School of Computer Science, University of Birmingham, UK. Before this, he was a Research Scientist in the Institute for Infocomm Research (I^{2}R), Singapore, and an Assistant Professor in the Institute of Software, Chinese Academy of Sciences, where he received his PhD degree in Computer Science in March 2001. He has about 60 technical publications in the areas of applied cryptography, information security, and electronic commerce. In particular, he is interested in the design and analysis of digital signatures and security protocols. He has served as a programme committee member or reviewer for numerous international conferences, workshops and journals.

This special issue of *IJACT* is devoted to the 5th Information Security Practice and Experience Conference (ISPEC'09), which was held in Xi'an, China, 13–15 April 2009.

As an established technical forum, the ISPEC conference series brings together researchers and practitioners to provide a confluence of new information security technologies, including their applications and their integration with IT systems in various vertical sectors. In previous years, ISPEC has taken place in Singapore (2005), Hangzhou, China (2006), Hong Kong, China (2007) and Sydney, Australia (2008). As the response to the call for papers, 147 papers from 26 countries were submitted to ISPEC'09, and among them 34 were selected for inclusion in the proceedings, published by Springer in the Lecture Notes in Computer Science series.

This special issue contains the revised versions of seven papers presented at ISPEC'09. Each selected paper was essentially extended by the authors to include at least 30% new contents. The first paper is 'Achieving high security and efficiency in RFID-tagged supply chains' by Shaoying Cai, Yingjiu Li, Tieyan Li, Robert H. Deng and Haixia Yao. It aims to tackle a challenge in the area of Radio Frequency IDentiflcation (RFID) by designing secure and efficient RFID-tagged supply chain systems. Specifically, it proposes a set of RFID protocols to enable duel security modes: in the relatively secure environments, such a system is set to the weak security mode so that the tagged products can be processed in a highly efficient way, while in the less secure environments, the system can be changed into the strong security mode to maintain a high level of security without too much sacrifice on efficiency.

The second paper is contributed by Anders Moen Hagalisletto and Lars Strand, entitled 'Designing attacks on SIP call set-up'. This work studies the security of a practical protocol, called the Session Initiation Protocol (SIP), which is used in Voice over IP (VoIP) applications. By combining the information retrieved from the IETF specification documents and traces of real-world SIP traffic, the authors present a formal specification of the SIP protocol and consequently detect several weaknesses in both of SIP call set-up and the Asterisk implementation of the protocol. In particular, they identify a severe call hijack attack that allows an intruder to completely take over a phone call.

The third paper in this special issue is 'Defending against the pirate evolution attack' by Hongxia Jin, Jeffrey Lotspiech and Serdar Pehlivanoglu. A trace and revoke scheme for secure content distribution allows only authorised users to access the copyrighted content. This work presents an easy and efficient approach to prevent the state-of-art trace-revoke scheme from the potential pirate evolution attack, in which pirate users reveal their compromised secret keys to the clone decoder very slowly through a number of generations of pirate decoders so that disabling them will take long time. Moreover, this paper also gives a formal analysis on the trade off between the immunity to evolution attack and revocation efficiency.

The fourth contribution is 'Strongly unforgeable ID-based signatures without random oracles' by Chifumi Sato, Takeshi Okamoto and Eiji Okamoto. It presents a strongly unforgeable identity-based signature scheme in the standard model (i.e. without using random oracles). The security of the proposed scheme is formally proved to rely on the difficulty solving three problems related to the Diffie–Hellman problem and a one-way isomorphism. Compared to other similar signature schemes based on varieties of the Diffie–Hellman problem or the discrete logarithm problem, the new solution has a shorter signature size.

The fifth paper is 'A ciphertext-policy attribute-based encryption scheme with constant ciphertext length' by Keita Emura, Atsuko Miyaji, Kazumasa Omote, Akito Nomura and Masakazu Soshi. An Attribute-Based Encryption (ABE) allows users with some attributes to decrypt a ciphertext if the ciphertext is associated with these attributes. As in previous ABE schemes the length of the ciphertext depends on the number of attributes, the authors of this paper are motivated to propose the first Ciphertext-Policy Attribute-Based Encryption (CP-ABE) with constant ciphertext length.

The sixth paper, entitled 'Some results on cryptanalysis of SMS4 block cipher', is contributed by Wentao Zhang, Bozhan Su, Wenling Wu and Dengguo Feng. It has twofold contributions in analysing SMS4, a 128-bit block cipher used in the Chinese WAPI (WLAN Authentication and Privacy Infrastructure) national standard for wireless network products. On the one hand, some observations on the linear diffusion layer *L* of SMS4 are presented in order to illustrate the design rationales of it. On the other hand, an effective 19-round differential characteristic is derived and then a simple differential attack on 23-round SMS4 is given, which forms the best-known attack on SMS4 so far.

The seventh also the last paper in this special issue is 'TWISTER$_\pi$ – a framework for secure and fast hash functions' by Ewan Fleischmann, Christian Forler, Michael Gorski and Stefan Lucks. It presents a framework for secure and efficient hash functions, called TWISTER$_\pi$, which is an improved version of TWISTER, a candidate of the NIST SHA-3 hash function competition. The core feature of this framework is that it can be analysed very easily. According to the authors' analysis, the total security level of TWISTER$_\pi$ is not below than $2^{n/2}$ for collision attacks and 2^n for (2nd) pre-image attacks. Moreover, TWISTER$_\pi$ instantiations are shown to be secure against all known generic attacks. In addition, two particular instances are proposed to produce 256-bit and 512-bit hash output, which are highly optimised for 64-bit architectures with very fast hardware and software implementations.

As the conference organisers and the guest editors of this special issue, we are grateful to the Program Committee members and all of their sub-reviewers for their precious time and valued contributions to the tough and time-consuming reviewing process. In addition, we would like to thank Editor-in-Chief, Professor Yi Mu, for his kind advice and guidance on editing this special issue.