Preface

Yi Mu
University of Wollongong,
Wollongong, NSW 2522,
Australia
Email: ymu@uow.edu.au

David Pointcheval
Fcole Normale SupŹrieure,
France
Email: David.Pointcheval@ens.fr

Biographical notes: Yi Mu received his PhD from the Australian National University in 1994. Currently, he is an Associate Professor in the School of Computer Science and Software Engineering, University of Wollongong. Prior to joining the University of Wollongong, he worked as a Lecturer in the School of Computing and IT, the University of Western Sydney and later as a Senior Lecturer in the Department of Computing, Macquarie University. His current research interests include network security, computer security and cryptography. He serves as Editor seven international journals and has served in program committees for a number of international conferences. He is a Senior Member of the IEEE and a Member of the IACR.

David Pointcheval received his PhD in Computer Science from ENS in 1996. Since 1998, he has been a CNRS Researcher, in the Department of Computer Science at $f$cole normale sup^rieure, Paris, France, in the Cryptography Team, that he leads since 2005. His research focuses on provable security of cryptographic primitives and protocols. He is the author of almost 100 international conference papers and an inventor of 9 patents. He has served on the Program Committee of several international conferences, including Crypto, Eurocrypt, Asiacrypt and PKC, and was Program Chair for the Cryptographers' Track at the RSA Conference 2006 and for the 5th International Conference Cryptology and Network Security.

International Journal of Applied Cryptography (IJACT) is a new journal addressing security issues and providing security solutions to the internet and computer systems. *IJACT* aims to introduce new ground between cryptographic theory and applications. It proposes and fosters discussion on cryptographic algorithms and protocols that are directly applicable. The objectives of *IJACT* are to establish an international forum and promote applicable research in cryptography. It serves as a bridge between cryptographers and security engineers. *IJACT* provides a vehicle to help academics, researchers, and engineers, working in the fields of cryptography and information security, to disseminate information and to learn from each other's work. *IJACT* includes but not limited to the following topics:

Anonymity
Authentication
Broadcast encryption
Ciphers
Cryptanalysis
Data security
Digital cash
Digital signatures
E-auction
E-commerce
Encryption
E-gambling
E-voting
Key distribution
Identification
Identity-based cryptography
Online fraud and web security

The inaugural issue of *IJACT* consists of six invited papers, from reputable international security researchers. It serves as a sample for the future *IJACT* issues in terms of qualify and standard.

The first paper in this issue is: 'A tapestry of identity-based encryption: practical frameworks compared', authored by X. Boyen. This work surveys the practical benefits and drawbacks of several identity-based encryption schemes based on bilinear pairings and classifies the known constructions into a handful of general approaches. This paper describes efficient and fully secure IBE and IBKEM instantiations of each approach, with reducibility to practice

as the main design parameter. It also catalogues the strengths and weaknesses of each construction according to a few theoretical and many applied comparison criteria.

The second paper in this issue is: 'Homomorphic encryption and secure comparison', co-authored by I. Damgård, M. Geisler, and M. Krøigård. This paper proposes a protocol for secure comparison of integers based on homomorphic encryption and provides a homomorphic encryption scheme that can be used in the proposed protocol. The proposed scheme is more efficient than previous solutions and can also be used as the basis of efficient and general secure multiparty computation. It is shown how the proposed comparison protocol can be used to improve security of online auctions.

The third paper in this issue is: 'Practical key-recovery attack against APOP, an MD5-based challenge-response authentication', authored by G. Leurent. This paper shows how collisions can be used to recover part of the password used in the APOP authentication protocol. It looks into the details of MD5 collisions. This work shows how to choose small parts of the colliding messages, which will allow to build the APOP attack. This shows that collision attacks can be used to attack real protocols, which means that finding collisions is a real threat.

The fourth paper in this issue is: 'Delayed password disclosure', co-authored by M. Jakobsson and S. Myers. This paper presents a new authentication protocol called delayed password disclosure. Based on the traditional username and password paradigm, the protocol's goal is aimed at reducing the effectiveness of phishing/spoofing attacks that are becoming increasingly problematic for internet users. This is done by providing the user with dynamic feedback while password entry occurs. While this is a process that would normally be frowned upon by the cryptographic community, it is argued that it may result in more effective security than that offered by currently proposed 'cryptographically acceptable' alternatives.

The fifth paper in this issue is: 'The power of identification schemes', co-authored by K. Kurosawa and S-H. Heng. It is shown that identification schemes are very powerful in some areas of cryptography. They first prove an equivalence between non-interactive trapdoor commitment schemes and a natural class of identification schemes and then propose a more efficient online/off-line signature transformation than Shamir-Tauman. As an application, they present a variant of the Boneh-Boyen (BB) signature scheme which is not only online/off-line but also has a smaller public key size than the original BB scheme. Finally, they present the first identity-based ID-scheme which is secure against concurrent man-in-the-middle attack without random oracles.

The sixth paper in this issue is: 'An optimistic fair exchange protocol and its security in the universal composability framework', co-authored by Y. Okada, Y-F. Manabe and T. Okamoto. This paper presents an optimistic fair exchange protocol that is applicable to any digital signature by prescribing three forms of signatures, namely presignature, post-signature and notarised signature. They set an expiration date for presignature, and thus realise the timely termination of the protocol. They also define an ideal functionality of fair exchange protocols in the universal composability framework, construct an optimistic fair exchange protocol based on the above protocol, and prove its security in the universal composability framework.