Journal of Universal Computer Science, vol. 14, no. 3 (2008), 314-317
submitted: 6/11/07, accepted: 12/11/07, appeared: 1/2/08 © J.UCS

Cryptography in Computer System Security J.UCS Special Issue

Liqun Chen
(Hewlett-Packard Labs, UK
liqun.chen@hp.com)

Ed Dawson
(Queensland University of Technology, Australia
e.dawson@qut.edu.au)

Xuejie Lai
(Shanghai Jiao Tong University, China
lai-xj@cs.sjtu.edu.cn)

Masahiro Mambo
(Tsukuba University, Japan
mambo@cs.tsukuba.ac.jp)

Atsuko Miyaji
(JAIST, Japan
miyaji@jaist.ac.jp)

Yi Mu (Lead Guest Editor)
(University of Wollongong, Australia
ymu@uow.edu.au)

David Pointcheval
(École Normale Supérieure, France
David.Pointcheval@ens.fr)

Bart Preneel
(Katholieke Universiteit Leuven, Belgium
bart.preneel@esat.kuleuven.be)

Nigel Smart
(Bristol University, UK
nigel@compsci.bristol.ac.uk)

Willy Susilo
(University of Wollongong, Australia
wsusilo@uow.edu.au)

Huaxiong Wang
(Nanyang Technological University, Singapore
HXWang@ntu.edu.sg)

Duncan S. Wong
(City University of Hong Kong, China
duncan@cityu.edu.hk)

Cryptography plays an important role on ensuring the security and reliability of modern computer systems. Since high speed and broad bandwidth have been becoming the keywords for modern computer systems, new cryptographic methods and tools must follow up in order to adapt to these new and emerging technologies. This Special Issue aims to provide a platform for security researchers to present their newly developed cryptographic technologies in computer systems. Areas of interest for this special journal issue include, but are not limited to, the following topics: Authentication, Cryptographic algorithms and their applications, Cryptanalysis, Email security, Electronic commerce, Data integrity, Fast cryptographic algorithms and their applications, Identity-based cryptography, IP security, Key management, Multicast security, Computer network security, Privacy protection, Security in Peer-to-Peer networks, Security in sensor networks, and Smartcards.

We received seventy-two manuscripts. After a pre-review process, fifty-one manuscripts were selected for further review. Eight manuscripts were finally selected for this Special Issue. The reviewing process took three months. Each manuscript selected from the pre-review was blindly reviewed by at least three reviewers consisting of guest editors and external reviewers.

The first paper in this special issue is Optimistic Fair Exchange in a Multi-user Setting, by Yeveniy Dodis, Pil Joong Lee, and Dae Hyun Yum. This work addresses the security of optimistic fair exchange in a multi-user setting. While the security of public key encryption and public key signature schemes in a single-user setting guarantees the security in a multi-user setting, they show that the situation is different in the optimistic fair exchange.

The second paper in this special issue is about New Results on NMAC/HMAC, by Christian Rechberger and Vincent Rijmen. They present a new method to recover both the inner- and the outer key used in HMAC when instantiated with a concrete hash function by observing text/MAC pairs. In addition to collisions, also other non-random properties of the hash function are used in this new attack. Among the examples of the proposed method, the first theoretical full key recovery attack on NMAC-MD5 is presented.

The third paper in this special issue is Parallel Key Exchange, by Ik Rae Jeong and Dong Hoon Lee. They study parallel key exchange among multiple parties. The status of parallel key exchange is depicted by a key graph. In a key graph, a vertex represents a party and an edge represents a relation of two parties who are to share a key. They propose a security model for a key graph, which extends the Bellare-Rogaway model for two-party key exchange and clarify the relations among the various security notions of key exchange. They construct an efficient key exchange protocol for a key graph using the randomness re-use technique.

The fourth paper in this special issue is Efficient k-out-of-n Oblivious Transfer Schemes, by Cheng-Kang Chu and Wen-Guey Tzeng. They propose several efficient two-round k-out-of-n oblivious transfer schemes, in which the receiver R sends $O(k)$ messages to the sender S, and S sends $O(n)$ messages back to R. The schemes provide unconditional security for either sender or receiver. Their schemes have the property of universal parameters and efficient.

The fifth paper in this special issue is Bilateral Unknown Key-Share Attacks in Key Agreement Protocols, by Liqun Chen and Qiang Tang. They propose a new type of Unknown Key-Share (UKS) attack. They call this attack a Bilateral Unknown Key-Share (BUKS) attack and demonstrate that a few well-known authenticated key agreement protocols are vulnerable to this attack.

The sixth paper in this special issue is Formal Security Definition and Efficient Construction for Roaming with a Privacy-Preserving Extension, by Guomin Yang, Duncan S. Wong, and Xiaotie Deng. They propose a formal key exchange definition and formalize secure roaming under the Canetti-Krawczyk (CK) model. We also propose a formal model for capturing the notions of user anonymity and untraceability. By using the modular approach supported by the CK-model, they construct an efficient key exchange protocol for roaming and then extend it to support user anonymity and untraceability.

The seventh paper in this special issue is Certificateless Public Key Encryption Secure against Malicious KGC Attacks in the Standard Model, by Yong Ho Hwang, Joseph K. Liu, and Sherman S.M. Chow. They show that two existing CL-PKE schemes without random oracles are not secure against malicious KGC and then propose the first CL-PKE scheme secure against malicious KGC attack, with proof in the standard model.

The last paper in this special issue is Parallel Formulations of Scalar Multiplication on Koblitz Curves, by Omran Ahmadi, Darrel Hankerson, and Francisco Rodríguez-Henríquez. They present an algorithm that by using the τ and τ^{-1} Frobenius operators concurrently allows them to obtain a parallelized version of the classical τ-and-add scalar multiplication algorithm for Koblitz elliptic curves.

Finally, we would like to think all authors who have submitted their manuscripts to this Special Issue and the following external reviewers for their invaluable contributions to the reviewing process: Man Ho Au, Lejla Batina, Christophe De Canniere, Chris Charnes, Jing Chen, Micheal Cheng, Eikoh Chida, Kim-Kwang Raymond Choo, Sherman S. M. Chow, Hiroshi Doi, Ling Dong, Pooya Farshim, Gangwei Fu, Jun Furukawa, Kris Gaj, Praveen Gauravaram, Fuchun Guo, Hua Guo, Wei Han, Helena Handschuh, Xuan Hong, Qiong Huang, Xinyi Huang, Kouichi Itoh, Seungjoo Kim, Izuru Kitamura, Hiroki Koga, Markulf Kohlweiss, Noboru Kunihiro, Junzuo Lai, Pil Joong Lee, Gaëtan Leurent, Yu Long, Yiyuan Luo, Hideyuki Miyake, Kunihiro Miyazaki, Shingo Miyazaki, Gregory Neven, Akito Niwa, Attrapadung Nuttapong, Dan Page, Kun Peng, Mohammad Reza Reyhanitabar, Nicholas Sheppard, Jason Smith, Koutarou Suzuki,

Katsuyuki Takashima, Chunming Tang, Christophe Tartary, Carmela Troncoso, Frederik Vercauteren, Peishun Wang, Yan Wang, Dai Watanabe, Mi Wen, Stevanus Wibowo, Mu En Wu, Qianhong Wu, Guomin Yang, Jin Yuan, Qingsong Ye, Jinmin Zhong, Rui Zhang, and Xianmo Zhang.

Liqun Chen
Ed Dawson
Xuejie Lai
Masahiro Mambo
Atsuko Miyaji
Yi Mu
David Pointcheval
Bart Preneel
Nigel Smart
Willy Susilo
Huaxiong Wang
Duncan S. Wong

(November, 2007)