Guest Editorial: Special Issue on Provable Security *

Xiaofeng Chen
Key Laboratory of Computer Networks and Information Security,
Ministry of Education, Xidian University, Xi'an 710071, P.R.China
xfchen@xidian.edu.cn

Provable security is an important research area in modern cryptography. Cryptographic primitives or protocols without a rigorous proof cannot be regarded as secure even in practice. In fact, there are many schemes that were originally thought as secure but eventually broken, which clearly indicates the need of formal security assurance. With provable security, we are confident in using cryptographic schemes and protocols in various real-world applications. Meanwhile, schemes with provable security sometimes give only theoretical feasibility rather than a practical construction, and correctness of the proofs may be difficult to verify.

This special issue on "Provable Security" attempts to highlight some of the latest research addressing those challenges. It consists of 11 papers selected from the contributions of the 5th International Conference on Provable Security (ProvSec 2011). More specifically:

- The paper of Mallouli, Mammar, Cavalli and Jimenez [1], titled "VDC-Based Dynamic Code Analysis: Application to C Programs", presents a novel approach to detect software vulnerabilities in C programs relying on formal models of vulnerabilities causes called "Vulnerability Detection Conditions" (VDCs). These models provide a formal interpretation of a vulnerability to facilitate its automatic detection using dynamic code analysis tool;

- Grześkowiak's paper on "Algorithm for generating primes for the Giuliani-Gong Public Key System" [2] proposes an algorithm for computing large primes p and q such that q divides $p^4+p^3+p^2+p+1$ or $p^4-p^3+p^2-p+1$. Such primes are key parameters for the Giuliani-Gong public key system;

- Huang's paper on "An eCK-Secure One Round Authenticated Key Exchange Protocol with Perfect Forward Security" [3] presents a new two-pass (one round) authenticated key exchange protocol which enjoys some desirable properties. It is shown that the protocol is secure in the enhanced Canetti-Krawczyk (eCK) model under the gap Diffie-Hellman (GDH) assumption. In addition, they prove that the protocol achieves perfect forward security against active adversary in one round under the same assumption;

- The paper of Yang and Yang [4], titled "A Novel Multi-factor Authenticated Key Exchange Scheme With Privacy Preserving", presents a new multi-factor authenticated key exchange scheme, which combines with biometrics, password and the smart card. The scheme is proved to be secure under the random oracle and is suitable to the environment which lacked communication resource and needed higher security;

- Larangeira and Tanaka's paper "Programmability in the Generic Ring and Group Models" [5] introduces four models named *programmable and non-programmable* for the generic group models (GGM) and analogously for the generic ring models (GRM). They show that in the programmable generic models it is possible to turn around the negative result, regarding the non-committing encryption in the presence of an adversary who corrupts the receiver.

Journal of Internet Services and Information Security, volume: 1, number: 2/3, pp. 1-3

*This special issue is financially supported by the National Natural Science Foundation of China (No.60970144), China 111 Project (No.B08038), and Key Laboratory of Computer Networks and Information Security, Ministry of Education, Xidian University.

- Liu, Lai, and Deng's paper on "General Construction of Chameleon All-But-One Trapdoor Functions" [6] proposes a black-box construction for transforming any all-but-one trapdoor functions (ABO-TDFs) into chameleon ABO-TDFs with the help of chameleon hash functions. They obtain a chameleon ABO-TDFs based on the Decisional Diffie-Hellman (DDH) assumption;

- The paper of Gjøsteen, Petrides and Steine [7], titled "A Novel Framework for Protocol Analysis", describes a novel reformulation of Canetti's Universal Composability (UC) framework for the analysis of cryptographic protocols. They illustrate how the theory can be used with several examples.

- Pan and Wang's paper on "TMQV: A Strongly eCK-secure Diffie-Hellman Protocol without Gap Assumption" [8] proposes an authenticated key exchange (AKE) protocol under the computational Diffie-Hellman (CDH) assumption with respect to the strengthened eCK-security (seCK-security) model. They present the TMQV protocol using the twinning technique and the MQV key derivation method. Furthermore, by using trapdoor test theorem, they prove that TMQV is provably seCK-secure under the standard CDH assumption in the random oracle model.

- The paper of Kawai, Sakai and Kunihiro [9], titled "On the (Im)possibility Results for Strong Attack Models for Public Key Cryptsystems", discusses the strong attack model security for public key encryption scheme and digital signature scheme. They prove several impossibility results under strong chosen ciphertext attack (SCCA) model.

- The paper of Canard, Devigne and Laguillaumie [10], titled "Improving the Security of an Efficient Unidirectional Proxy Re-Encryption Scheme", presents an improvement on an efficient unidirectional proxy re-encryption scheme published in Africacrypt 2010. The resulting scheme can achieve a full chosen ciphertext attacks (CCA) security. Moreover, the scheme does not rely on pairings and can be implemented efficiently with any traditional modular arithmetic.

- Pandey and Barua's paper on "Efficient Construction of Identity Based Signcryption Schemes from Identity Based Encryption and Signature Schemes" [11] uses an Identity Based Encryption (IBE) and an Identity Based Signature (IBS) schemes to construct an Identity Based Signcryption Scheme (IBSC), and show that the security of the IBSC scheme–indistinguishability as well as unforgeablity–is derived from the security of the underlying IBE and IBS schemes.

Finally, we appreciate all authors and reviewers for their valuable contributions, without which this special issue cannot be reality.

References

[1] Wissam Mallouli, Amel Mammar, Ana Cavalli, and Willy Jimenez. VDC-Based Dynamic Code Analysis: Application to C Programs. *Journal of Internet Services and Information Security (JISIS)*, 1(2/3):4–20, 2011.

[2] Maciej Grześkowiak. Algorithm for Generating Primes for the Giuliani-Gong Public Key System. *Journal of Internet Services and Information Security (JISIS)*, 1(2/3):21–31, August 2011.

[3] Hai Huang. An eCK-Secure One Round Authenticated Key Exchange Protocol with Perfect Forward Security. *Journal of Internet Services and Information Security (JISIS)*, 1(2/3):32–43, August 2011.

[4] Dexin Yang and Bo Yang. A Novel Multi-factor Authenticated Key Exchange Scheme With Privacy Preserving. *Journal of Internet Services and Information Security (JISIS)*, 1(2/3):44–56, August 2011.

[5] Mario Larangeira and Keisuke Tanaka. Programmability in the Generic Ring and Group Models. *Journal of Internet Services and Information Security (JISIS)*, 1(2/3):57–73, August 2011.

[6] Shengli Liu, Junzuo Lai, and Robert H. Deng. General Construction of Chameleon All-But-One Trapdoor Functions. *Journal of Internet Services and Information Security (JISIS)*, 1(2/3):74–88, August 2011.

[7] Kristian Gjøsteen, George Petrides, and Asgeir Steine. A Novel Framework for Protocol Analysis. *Journal of Internet Services and Information Security (JISIS)*, 1(2/3):89–106, August 2011.

[8] Jiaxin Pan and Libin Wang. TMQV: A Strongly eCK-secure Diffie-Hellman Protocol without Gap Assumption. *Journal of Internet Services and Information Security (JISIS)*, 1(2/3):107–124, August 2011.

[9] Yutaka Kawai, Yusuke Sakai, and Noboru Kunihiro. On the (Im)possibility Results for Strong Attack Models for Public Key Cryptsystems. *Journal of Internet Services and Information Security (JISIS)*, 1(2/3):125–139, August 2011.

[10] Sébastien Canard, Julien Devigne, and Fabien Laguillaumie. Improving the Security of an Efficient Unidirectional Proxy Re-Encryption Scheme. *Journal of Internet Services and Information Security (JISIS)*, 1(2/3):140–160, August 2011.

[11] Sumit Kumar Pandey and Rana Barua. Efficient Construction of Identity Based Signcryption Schemes from Identity Based Encryption and Signature Schemes. *Journal of Internet Services and Information Security (JISIS)*, 1(2/3):161–180, August 2011.

Xiaofeng Chen received his Ph.D. in cryptography from the Xidian University in 2003. He is currently a Professor at the School of Telecommunications Enginnering, Xidian University. His research interests include public key cryptography, financial cryptography, and cloud computing security.