entropy

MDPI

Editorial

Special Issue on Entropy-Based Applied Cryptography and Enhanced Security for Ubiquitous Computing

James (Jong Hyuk) Park [1,*] and Wanlei Zhou [2]

[1] Department of Computer Science and Engineering, Seoul National University of Science and Technology, Seoul 01811, Korea

[2] School of Information Technology, Deakin University, Victoria 3125, Australia; wanlei.zhou@deakin.edu.au

* Correspondence: jhpark1@seoultech.ac.kr; Tel.: +82-2-970-6702

Academic Editor: Raúl Alcaraz Martínez

Received: 7 September 2016; Accepted: 7 September 2016; Published: 13 September 2016

Abstract: Entropy is a basic and important concept in information theory. It is also often used as a measure of the unpredictability of a cryptographic key in cryptography research areas. Ubiquitous computing (Ubi-comp) has emerged rapidly as an exciting new paradigm. In this special issue, we mainly selected and discussed papers related with ore theories based on the graph theory to solve computational problems on cryptography and security, practical technologies; applications and services for Ubi-comp including secure encryption techniques, identity and authentication; credential cloning attacks and countermeasures; switching generator with resistance against the algebraic and side channel attacks; entropy-based network anomaly detection; applied cryptography using chaos function, information hiding and watermark, secret sharing, message authentication, detection and modeling of cyber attacks with Petri Nets, and quantum flows for secret key distribution, etc.

Keywords: applied cryptography; enhanced security; ubiquitous computing

Entropy is a basic and important concept in information theory introduced by Claude E. Shannon. It is also often used as a measure of the unpredictability of a cryptographic key in cryptography research areas. Ubi-comp has emerged rapidly as an exciting new paradigm. Together with these trends, applied cryptography and security have become rising big issues for providing secure and trusted computing in the next generation of information and communications. A detailed discussion of these issues includes applied cryptography and security concerns that cover amongst others, confidentiality, integrity, and availability including various application areas. In particular, these topics will comprehensively focus on the important aspects of entropy-based applied cryptography and enhanced security for Ubi-comp. Topics in Ubi-comp include entropy-based applied cryptographic aspects, entropy-based hash functions, mathematical and algorithmic foundations of applied cryptography, advanced design and analysis of cryptographic algorithms, authentication and access control, privacy protection and trust computing, entropy-based network security issues, information hiding and digital forensics, security issues in cloud computing and mobile social networks. This special issue aims to provide advanced theories and applications. Furthermore, researchers contribute with original research and review articles that present state-of-the-art research outcomes, practical results in entropy-based applied cryptographic models, and enhanced security system for Ubi-comp.

During our working period, we received a total of 33 submissions from at least 10 countries where the corresponding authors were majorly counted by the deadline for paper submission. All these submissions were found with significant contributions in main interested topics of our special issue. However, only 14 high quality papers were accepted after two or three-round strict and rigorous review processes. These accepted papers mainly look at our issue from the perspectives of

encryption technique, identity and authentication, credential cloning attack and countermeasures, side channel attack and countermeasure, entropy-based network security detection, applied cryptography, information hiding and watermark, secret sharing, message authentication, quantum flows for secret key distribution, which brought active discussions to the public readers.

The first paper [1] entitled "An Intelligent and Fast Chaotic Encryption Using Digital Logic Circuits for Ad-Hoc and Ubiquitous Computing" by Ankur K., et al. presents a novel fast and secure Chaotic Map-based encryption technique using 2's Compliment (CET-2C). Chaotic Encryption is more attack-resilient than other encryption techniques. One of the most attractive properties of cryptography is known as an avalanche effect, in which two different keys produce distinct cipher texts for the same information. This proposed scheme uses a logistic map which implies that a negligible difference in parameters of the map generates different cipher texts. Cryptanalysis of the proposed algorithm shows the strength and security of the algorithm and keys. Performance of the proposed algorithm has been analyzed in terms of running time, throughput and power consumption. Comparison graphs might show that the proposed algorithm gave better results compared to different algorithms like advanced encryption standard (AES).

The next paper [2], entitled "Identity Authentication over Noisy Channels" by Fanfan Z, et al. introduce a general analysis and design framework for identity authentication over noisy channels. Identity authentication is the process of verifying users' validity and is built on noiseless channels. In particular, in this paper, the authentication scenarios of single time and multiple times are investigated. For each scenario, the lower bound on the opponent's success probability is derived, and it is smaller than the classical identity authentication's. Remarkably, the Cartesian authentication code proves to be helpful for hiding the secret key to maximize the secrecy performance. In addition, authors show a potential application of this authentication technique.

The next paper, [3] entitled "Personal Information Leaks with Automatic Login in Mobile Social Network Services" by Jongwon Choi, et al. presents the possibility of a credential cloning attack. Because the credentials are convenient for users, they are utilized by most mobile social network service (SNS) apps. However, the current state of credential management for the majority of Android SNS apps is very weak. In this paper, authors analyze the vulnerabilities of the main Android-based SNS apps to credential cloning attacks, and examine the potential leakage of personal information that may result. In addition, authors introduce effective countermeasures to resolve these problems.

In the next paper [4] entitled "The Switching Generator: New Clock-Controlled Generator with Resistance against the Algebraic and Side Channel Attacks", Jun Choi, et al. propose new clock-controlled systems: the switching generator. There are many attack results using algebraic properties and side channel information against stream ciphers for hardware applications. In particular, many clock-controlled systems are indeed vulnerable against side channel attacks. Even if new clock-controlled systems were presented, such as the generalized alternating step generator, cascade jump-controlled generator, etc., the algebraic attack could be applied directly on these new systems. However, the proposed switching generator has resistance to algebraic and side channel attacks. The generator also preserves both security properties and the efficiency of existing clock-controlled generators.

In the next paper [5], entitled "An Entropy-Based Network Anomaly Detection Method", Przemysław Bereziński, et al. introduce an entropy-based network security method which supports anomaly detection. Authors prove that the proposed approach is suitable to detect modern botnet-like malware based on anomalous patterns in network. This aim is achieved by the realization of the following points: preparation of a concept of an original entropy-based network anomaly detection method, implementation of the method, preparation of an original dataset, and evaluation of the method.

The next paper [6], entitled "Applied Cryptography Using Chaos Function for Fast Digital Logic-Based Systems in Ubiquitous Computing" by Piyush Kumar Shukla, et al. presents a novel chaos-based data encryption techniques with digital logics dealing with hiding information. This paper

provides an overview of how traditional data encryption techniques are revised and improved to achieve good performance in a secure communication network environment. The comparative tables can be used as a guideline to select an encryption technique suitable for the application at hand.

In the next paper [7], entitled "Information Hiding Method Using Best DCT and Wavelet Coefficients and Its Watermark Competition", Hyunho Kang and Keiichi Iwamura develop an information hiding method that satisfies the Information Hiding and its Criteria (IHC) evaluation criteria. The proposed method uses the difference of the frequency coefficients derived from a discrete cosine transform or a discrete wavelet transform. The algorithm employs a statistical analysis to find the best positions in the frequency domains for watermark insertion.

In the next paper [8], entitled "Comparing Security Notions of Secret Sharing Schemes", Songsong Dai and Donghui Guo study the relations of several security notions for secret sharing schemes defined by the variational measures, including Shannon entropy, guessing probability, min entropy and Kolmogorov complexity.

In the next paper [9], entitled "Message Authentication over Noisy Channels", Fanfan Zheng, et al. reformulate the authentication problems in "Authentication over noisy channels" in IEEE Trans. Inf. Theory (2009) proposed by L. Lai, et al. and proposed an enhanced authentication scheme. Authors analyzed the eavesdropping agent's success probability of impersonation and substitution attacks, derived the necessary and sufficient conditions for secure authentication codes. Then, they offered the optimal constructions of the authentication scheme. Authors provide general perspectives to show that it is a reliable way to utilize channel noise in message authentication applications.

In the next paper [10], entitled Internet Protocol (IP), Félix Iglesias and Tanja Zseby propose a fast, lightweight method to distinguish different attack types observed in an Internet protocol (IP) dark space monitor. The method is based on entropy measures of traffic-flow features and machine learning techniques. The explored data belongs to a portion of the Internet background radiation from a large IP dark space such as real traffic captures that exclusively contain unsolicited traffic, ongoing attacks, attack preparation activities and attack aftermaths. In particular, the deep analysis of traffic is compared to a more lightweight traffic characterization method that is solely based on the entropy signals of different traffic features. The deep analysis disclosed a recent picture of the Internet background radiation (IBR), reflecting trends of network attacks and anomalies on a large scale with dominant traffic characterized by transmission control protocol (TCP) scanning activities and TCP backscatter. They expect that entropy-based methods can be a valuable building block for early warning systems and the detection of new attacks and attack preparation activities.

The next paper [11], entitled "Detection and Modeling of Cyber Attacks with Petri Nets" by Bartosz Jasiul, et al. presents an approach to develop and verify a method of formal modeling of cyber threats directed at computer systems. In addition, authors prove that the proposed method enables the creation of models resembling the behavior of malware that support the detection process of selected cyber-attacks and facilitate the application of countermeasures. This paper is addressed to cyber defense researchers, security architects, and developers to solve up-to-date problems regarding the detection and prevention of advanced persistent threats.

In the next paper [12], entitled "Improving the Authentication Scheme and Access Control Protocol for VANETs", Wei-Chen Wu and Yi-Ming Chen propose a cryptanalysis of an attachable blind signature and improved authentication and access control scheme for Vehicular Ad Hoc Networks (VANETs). An eavesdropper can construct an authorized credential from an intercepted blind document. Any eavesdropper can determine who has which access privileges to access which service. To address the problems, this paper deals with these challenges and proposes an efficient countermeasure method.

In the next paper [13], entitled "Block Access Token Renewal Scheme Based on Secret Sharing in Apache Hadoop", Su-Hyun Kim and Im-Yeong Lee propose a weight-applied exclusive or (XOR)-based efficient distribution storage and recovery scheme. As various data services are now allowed over a distributed computing environment, distributed management of big data has become a major

issue. In addition, security vulnerability and privacy infringement can occur by means of various usage types of big data. In particular, various security vulnerabilities can occur in the block access token, which is used for the permission control of data blocks in Hadoop. This paper presents a secret sharing-based block access token management scheme to overcome the security vulnerabilities. In addition, the proposed scheme is relatively efficient because a block access token is applied to a hash function only once and sent along with a secret segment after the initial secret segment creation and distribution process.

In the last paper [14], entitled "Quantum Flows for Secret Key Distribution in the Presence of the Photon Number Splitting Attack", Luis A. Lizama-Pérez, et al. propose a new quantum key distribution (QKD) protocol which is resistant to the photon number splitting (PNS) attack. Physical implementations of QKD protocols are forced to use attenuated coherent quantum states. When using attenuated coherent states, the relatively high rate of multi-photonic pulses introduces vulnerabilities that can be exploited by the PNS attack to brake the quantum key. Even if some QKD protocols have been developed to be resistant to the PNS attacks, those define a single photonic gain in the quantum channel. In this paper, authors use attenuated quantum states, but define two interleaved photonic quantum flows to detect the eavesdropper activity by means of the quantum photonic error gain or the quantum bit error rate. They emphasize that the proposed protocol does not require additional hardware other than the Bennett-Brassard protocol hardware and that it can be implemented mostly at a high level as a software application.

Our special thanks go to Kevin H. Knuth who is Editor-in-Chief of the Entropy journal and all editorial staff for their valuable support throughout the preparation and publication of this special issue. We would like to thank all authors for their contributions to this special issue. We also extend our thanks to the external reviewers for their excellent help in reviewing the papers.

Acknowledgments: This research was supported by the MSIP (Ministry of Science, ICT and Future Planning), Korea, under the ITRC (Information Technology Research Center) support program (IITP-2016-H8601-16-1009) supervised by the IICTP (Institute for Information & Communications Technology Promotion).

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Ankur, K.; Piyush, K.; Murtaza, A.; Shalini, S. An Intelligent and Fast Chaotic Encryption Using Digital Logic Circuits for Ad-Hoc and Ubiquitous Computing. *Entropy* **2016**, *18*, 201.
2. Zheng, F.; Xiao, Z.; Zhou, S.; Wang, J.; Hunag, L. Identity Authentication over Noisy Channels. *Entropy* **2015**, *17*, 4940–4958. [CrossRef]
3. Choi, J.; Cho, H.; Yi, J.H. Personal Information Leaks with Automatic Login in Mobile Social Network Services. *Entropy* **2015**, *17*, 3947–3962. [CrossRef]
4. Choi, J.; Moon, D.; Hong, S.; Sung, J. The Switching Generator: New Clock-Controlled Generator with Resistance against the Algebraic and Side Channel Attacks. *Entropy* **2015**, *17*, 3692–3709. [CrossRef]
5. Bereziński, P.; Jasiul, B.; Szpyrka, M. An Entropy-Based Network Anomaly Detection Method. *Entropy* **2015**, *17*, 2367–2408. [CrossRef]
6. Shukla, P.K.; Khare, A.; Rizvi, M.A.; Stalin, S.; Kumar, S. Applied Cryptography Using Chaos Function for Fast Digital Logic-Based Systems in Ubiquitous Computing. *Entropy* **2015**, *17*, 1387–1410. [CrossRef]
7. Kang, H.; Iwamura, I. Information Hiding Method Using Best DCT and Wavelet Coefficients and Its Watermark Competition. *Entropy* **2015**, *17*, 1218–1235. [CrossRef]
8. Dai, S.; Guo, D. Comparing Security Notions of Secret Sharing Schemes. *Entropy* **2015**, *17*, 1135–1145. [CrossRef]
9. Zheng, F.; Xiao, Z.; Zhou, S.; Wang, J.; Huang, L. Message Authentication over Noisy Channels. *Entropy* **2015**, *17*, 368–383. [CrossRef]
10. Iglesias, F.; Zseby, T. Entropy-Based Characterization of Internet Background Radiation. *Entropy* **2015**, *17*, 74–101. [CrossRef]
11. Jasiul, B.; Szpyrka, M.; Śliwa, J. Detection and Modeling of Cyber Attacks with Petri Nets. *Entropy* **2014**, *16*, 6602–6623. [CrossRef]

12. Wu, W.-C.; Chen, Y.-M. Improving the Authentication Scheme and Access Control Protocol for VANETs. *Entropy* **2014**, *16*, 6152–6165. [CrossRef]
13. Kim, S.-H.; Lee, I.-Y. Block Access Token Renewal Scheme Based on Secret Sharing in Apache Hadoop. *Entropy* **2014**, *16*, 4185–4198. [CrossRef]
14. Lizama-Pérez, L.A.; López, J.M.; de Carlos-López, E.; Venegas-Andraca, S.E. Quantum Flows for Secret Key Distribution in the Presence of the Photon Number Splitting Attack. *Entropy* **2014**, *16*, 3121–3135. [CrossRef]