Special Issue on "Information Security and Cryptology"

Guest Editorial

Information is becoming a crucial if not the most important resource of the economy and the society at large. Information differs radically from other resources; for instance, it can be copied without cost, it can be communicated at the speed of light, and it can be destroyed without leaving traces. This poses new challenges for the protection of this new resource and of intellectual property in general. Information security, in particular cryptography, is an enabling technology that is vital for the development of the information society. Information Security for protecting information in potentially hostile environments is a crucial factor in the growth of information-based processes in industry, business, and administration. Cryptography is a key technology for achieving information security in communications, computer systems, electronic commerce, and in the emerging information society. After peer review, the guest editors accepted 25 final accepted papers from 102 online submissions for the special issue to reflect the current development of information security and cryptology technology.

The first paper by Dongsheng Ning, Xiaoyan Xu, Yanping Yu, Xinxin Liu and Xiaoyan Wang is entitled "UWB-based Receiver Initiated MAC Protocol with Packet Aggregation and Selective Retransmission". The authors proposes a UWB-based MAC protocol for wireless multimedia networks named as UWB-based Receiver initiated MAC protocol with Packet aggregation and Selective retransmission (URMPS), which can reduce long acquisition time and large overhead, and support more concurrent transmissions. The receiver initiated request, packet aggregation and selective retransmission are used to reduce synchronization acquisition time and overhead. The combination of mutually exclusive area and time-hopping (TH) code is to mitigate the interference caused by concurrent transmissions of multiple nodes. The simulation results run over NS-2 show that URMPS protocol performs better in terms of network throughput and delay compared to S-MAC.

The second paper by Ting Han, Shoushan Luo, Hongliang Zhu, Yang Xin and Yong Peng is entitled "A Novel Trust Evaluation Model Based on Gray Clustering Theory for Routing Networks". In this paper, by learning trust relationship from routing network, a trust evaluation model based on Grey Clustering Theory is proposed. The model adopts improved Bayes theory to evaluate the behavior trust. By introducing Grey Clustering Theory, the model clusters the recommend node to different trust classes according to recommend credibility and calculates the recommend weight to resistance the fraud recommends information from the deceptive node. Simulation results show that trust evaluation model based on Grey Clustering Theory cannot only effectively evaluate the routing node behavior but also has better anti-attack performance, anti-deception performance and higher attack node detection rate.

The third paper by Wentao Cui, Kai Niu, Qian Wan, Weiling Wu is entitled "A Robust and Efficient Clustering Algorithm for Network MIMO System". The authors propose a heuristic algorithm to dynamically bind together some base stations, which can adjust itself to the ever-changing interference condition. Through utilizing the predefined connection graph, the complexity of proposed scheme is reduced while retaining a similar performance to exhaustive searching algorithm. Compared with other previous clustering methods, the proposed one demonstrates its robustness against the unrealistic feedback channel and mostly matches the performance gain produced by exhaustive searching clustering strategy.

The fourth paper by Mingzhi Cheng, Yanping Du, Yan Wang, Minchao Xi and Kaiguo Yuan is entitled "Video Watermarking Algorithm Based on Relative Relationship of DCT Coefficients". The paper proposes a video watermarking algorithm based on relative relationship of DCT coefficients. By modification of coefficients on chosen positions, the robustness of watermark embedding is ensured. Meanwhile, as the relationship of coefficients remains unchanged, the quality of video is not affected. The analysis results show that the performance of proposed algorithm is better than the typical algorithms.

The fifth paper by Dan Li, Peng Cao, Yucui Guo, and Min Lei is entitled "Time Weight Update Model Based on the Memory Principle in Collaborative Filtering". In this paper, the change of users' interests is considered as the memory process, and a time weight iteration model is designed based on memory principle. For a certain user, the proposed model introduces the time weight for each item, and updates the weight by computing the similarity with the items chosen in a recent period. In the recommend process, the weight will be applied to the prediction algorithm. Experimental results show that the modified algorithm can optimize the result of the recommendation in a certain extent, and performs better than traditional collaborative filtering.

The sixth paper by Ming Chen, Shupeng Wang and Liang Tian is entitled "A High-precision Duplicate Image Deduplication Approach". The paper proposes a high-precision duplicate image deduplication approach. The main idea of the proposed approach is eliminating the duplicate images by five stages including feature extraction, high-dimension indexing, accuracy optimization, centroid selection and deduplication evaluation. Experimental results demonstrate: in a real dataset, the proposed approach not only effectively saves storage space, but also significantly improves the retrieval precision of duplicate images.

The seventh paper by Qinlong Huang, Zhaofeng Ma, Jingyi Fu, Xinxin Niu and Yixian Yang is entitled "Attribute Based DRM Scheme with Efficient Revocation in Cloud Computing". The authors propose an attribute-based DRM

doi:10.4304/jcp.8.11.2731-2734

scheme in cloud computing by combining the techniques of ciphertext-policy attribute-based encryption (CP-ABE) and proxy re-encryption (PRE). The users who satisfy the access policy can recover the content master key, and then obtain assistant key from the key server and decrypt the content in the proposed scheme. Furthermore, the proposed scheme achieves efficient attribute and user revocation by allowing the attribute authority to delegate the key server to refuse to issue the assistant key for the revoked users. The security and performance analyses indicate that the proposed scheme is secure, efficient, and privacy-preserving.

The eighth paper by Chiqiang Xing, Julong Lan and Yuxiang Hu is entitled "Virtual Network With Security Guarantee Embedding Algorithms". The paper firstly presents two security threats of virtual network and investigate them in depth, then proposes a novel virtual network with security guarantee that will take the trust value and security protection level as the new security constraints during its embedding. The simulation results show that the algorithm is effective.

The ninth paper by Wei Wang, Feng Zeng, Honglin Yuan and Xintao Duan is entitled "Identifying Image Composites by Detecting Discrepancies in Defocus and Motion Blur". The paper proposes a novel algorithm of detecting splicing in blurred images, which use blur parameters estimation through the cepstrum characteristics of blurred images in order to restore the spliced region and the rest of the image. The paper also develops a new measure to assist in inconsistent region segmentation in restored images that contain large amounts of ringing effect. Experimental results show efficacy of the proposed method even if the images to be tested have been noised with different levels. Compared with other existing algorithms, the proposed method has better robustness against Gaussian noise.

The tenth paper by Wen'an Zhou, Yiyu Zhang, Pei Qin, Wei Chen and Xu Li is entitled "Joint Scheduling Algorithms for LTE-A CoMP System". This paper investigates a novel type of Joint Scheduling algorithm for LTE-A CoMP system in a time and frequency selective fading channel. Two algorithms named SEB (Spectrum Efficiency Based) and JSB (Joint Score-Based) are proposed. Based on the spectrum efficiency optimization and the spectrum efficiency & users' fairness co-optimization, the authors formulate the optimization problems and give out the greedy- algorithm-based solutions. They try to select the best user and the best transmission method (CoMP or Non-CoMP) dynamically on every different time and frequency band to get better performance. From the simulation results, it is proven obviously superior to other CoMP scheduling algorithms, despite its overall throughput loss as compared with SEB.

The eleventh paper by Yongli An, Yang Xiao, Dong Wang and Zhanlin Ji is entitled "Security Spectrum Auction Framework for Cognitive Radio Networks". The paper proposes a security mechanism for the multi-user cognitive spectrum auction networks. This security auction framework is based on position information. The authors use this security spectrum auction framework to increase the total system revenue and prevent collusion. The simulation results show that the security spectrum auction framework can greatly improve spectrum efficiency.

The twelfth paper by Li-hong Zhu and Quan Zhou is entitled "A Novel Framework for Robust Lossless Data Hiding". The paper proposes a novel pragmatic framework for robust lossless data hiding (RLDH). It included pre-processing, side information storage, lossless data hiding (LDH) and RLDH, has better solved the specific problem in RLDH. Provide a new idea for the application of RLDH. In comparison with the existing RLDH methods, the proposed algorithm achieved better performance in terms of image quality and robustness.

The thirteenth paper by Jianhua Wu, Fangfang Guo and Nanrun Zhou is entitled "Single-Channel Color Image Encryption Using the Reality-Preserving Fractional Discrete Cosine Transform in YCbCr Space". A novel single-channel color image encryption algorithm is proposed, which utilizes the reality-preserving fractional discrete cosine transform in YCbCr space. The proposed algorithm enlarges the key space by employing the generating sequence as an extra key in addition to the fractional orders. Simulation results and security analysis demonstrate the proposed algorithm is feasible, effective and secure. The robustness to noise attack is also guaranteed to some extent.

The fourteenth paper by Jianni Xushuai, Zhihong Zhou, Wen Qin, Qiongxi Jiang and Nanrun Zhou is entitled "Multi-Party Concurrent Signature Scheme Based on Designated Verifiers". A new multi-party concurrent signature (MPCS) scheme based on designated verifiers is introduced, which features fairness and unforgeability based on the hardness of the Computational Diffie-Hellman (CDH) assumption in the random oracle model. In this scheme, each signer has the right to choose randomly his/her own individual keystone and retrieve all other individual keystones by the Extraction algorithm. If all signers release their own individual keystones, all signatures can be bound. There is not a decisive signer or a more power signer in selecting and releasing keystones. Therefore, the situation of keystones switched by dishonest signers can be effectively avoided and the fairness of the MPCS scheme is also apparently improved. The proposed MPCS scheme is proved to be secure and can counteract the adaptive chosen message attack.

The fifteenth paper by Shushan Hu, Cunchen Tang, Riji Yu, Xiaojun Wang and Mei Lei is entitled "Scalable Distributed Address Assignment for Low Rate Wireless Personal Area Network". In this paper, a Scalable Distributed Address Assignment Mechanism (SDAAM) is designed, which adopts adaptive approach to handle the variability present in the topology of wireless networks. In the proposed approach, every newly arrived node can be correctly configured regardless of the current network topology so that it can communicate with other nodes within the same network. Another important advantage of SDAAM is its handling of unexpected events which may arise due to migration or departure of nodes in the network. Detailed description about SDAAM is presented and its effectiveness and high flexibility is demonstrated based on the simulation program.

The sixteenth paper by Zuowen Tan and Jianfeng Wang is entitled "Security Analysis on a Timestamp-based Remote

User Authentication Scheme". The paper analyzes that Awasthi et al.'s scheme suffers from offline password guessing attacks, password compromise to the server, impersonation attack and important message leakage attacks. In addition, Awasthi et al.'s scheme has poor reparability.

The seventeenth paper by Hai Fang, Quan Zhou, and Kaijia Li is entitled "Robust Watermarking Scheme for Multispectral Images Using Discrete Wavelet Transform and Tucker Decomposition". In this paper, a robust multispectral image watermarking technique based on the discrete wavelet transform (DWT) and the tucker decomposition (TD) is proposed. The core idea behind the proposed technique is to apply TD on the DWT coefficients of spectral bands of multispectral images. The experimental results on LANDSAT images show the proposed approach is robust against various types of attacks such as lossy compression, cropping, addition of noise etc.

The eighteenth paper by Yi Sun, Xingyuan Chen and Xuehui Du is entitled "An Efficient Elliptic Curve Discrete Logarithm based Trapdoor Hash Scheme without Key Exposure". An efficient trapdoor hash scheme without key exposure based on elliptic curve discrete logarithm is put forward and its security is analyzed, the scheme satisfies the five properties of trapdoor hash functions: effective calculation, trapdoor collision, collision resistance, key exposure resistance and semantic security. Through comparing and analyzing with the existing schemes, it shows that the proposed scheme, which has only multiplicative complexity and removes the operations of computing finite field element inverse, is more advantage in terms of safety and efficiency. Moreover, the scheme supports batch computation that it can greatly improve the efficiency of verification.

The nineteenth paper by Aidi Zhang, Nanrun Zhou and Lihua Gong is entitled "Color Image Encryption Algorithm Combining Compressive Sensing with Arnold Transform". A new color image encryption algorithm combining compressive sensing with Arnold transform is proposed, which can encrypt the color image into a gray image. Considering the dimensional reduction and random projection of compressive sensing, the authors utilize compressive sensing to encrypt and compress the three color components of color image simultaneously. The three encrypted and compressed color components' dimensions are smaller than the original image, thus they can be grouped into a gray image, and then the gray image is scrambled by Arnold transform to enhance the security. The proposed algorithm can also be applied in the multiple-image encryption. The experimental results show the validity and the reliability of the proposed algorithm.

The twentieth paper by Yongwei Wang, Kaiguo Yuan, Yunan Liu, Hongyong Jia and Wei Qiu is entitled "Multi-source Data Fusion Approach Based on Improved Evidence Theory". A multi-source data fusion method based on dissimilarity matrix and evidence theory is proposed. First, using the weighted Euclidean distance, evidence dissimilarity matrix is constructed. Second, dissimilarity between the evidences is measured. Third, using dissimilarity matrix, supporting degree, credibility and weight of evidence are calculated, and the original evidences are modified. Finally, using the improved combination rule, the information fusion is completed. Experimental results show that proposed method is superior to the existing typical methods in accuracy, discrimination and accuracy of fusion results.

The twenty-first paper by Jing Liu, Guo-sheng Xu, Da Xiao, Li-ze Gu and Xin-xin Niu is entitled "A Semi-supervised Ensemble Approach For Mining Data Streams". A semi-supervised ensemble approach for mining data streams is presented in this paper. Data streams are divided into data chunks to deal with the infinite length. An ensemble classification model E is trained with existing labeled data chunks and decision boundary is constructed using E for detecting novel classes. New labeled data chunks are used to update E while unlabeled ones are used to construct unsupervised models. Classes are predicted by a semi-supervised model Ex which is consist of E and unsupervised models in a maximization consensus manner, so better performance can be achieved by using the constraints from unsupervised models with limited labeled instances. Experiments with different datasets demonstrate that the proposed method outperforms conventional methods in mining data streams.

The twenty-second paper by Ya-li Liu, Xiao-lin Qin, Chao Wang and Bo-han Li is entitled "A Lightweight RFID Authentication Protocol based on Elliptic Curve Cryptography". The paper proposes a robust authentication protocol based on Elliptic Curve Cryptography (ECC), which meets the requirement of resource-limited RFID systems. The proposed protocol achieves mutual authentication and possesses lightweight feature by reducing the computation cost over the tag end. Moreover, the proposed protocol possesses remarkable security properties in RFID system and the immunity against the possible malicious attacks as well as an excellent performance through the detailed security analysis. Performance evaluation and function comparison demonstrate that the proposed protocol makes a balance between cost and security in RFID authentication protocol. Compared to the previous relevant RFID authentication protocols, the proposed protocol improves efficiency, enhances robustness, which is well suitable for RFID tags with the scarceness of resources.

The twenty-third paper by Wei Li, Zhi Tao, Dawu Gu, Yi Wang, Zhiqiang Liu and Ya Liu is entitled "Differential Fault Analysis on the MD5 Compression Function". The paper proposes a new differential fault analysis on the MD5 compression function in the word-oriented random fault model. The simulating experimental results show that 144 random faults on average are required to obtain the current input message block. The proposed method not only increases the efficiency of fault injection, but also decreases the number of fault hash values. It provides a new reference for the security analysis of the same structure of the hash compression functions.

The twenty-fourth paper by Jia Zhang, Dongfeng Yuan and Haixia Zhang is entitled "On Stochastic Cell Association Scheme Over Carrier Aggregated Heterogenous Networks". In the paper, a cell association scheme based on stochastic

control theory is explored to attain improved network performance in carrier aggregated HetNets. Simulation results have shown the advantages of the proposed scheme under different kinds of carrier deployments across multiple tiers.

The twenty-fifth paper by Wunan Wan and Wang Suo is entitled “An Efficient MDS Array Code on Toleration Triple Node Failures in Storage System”. A new class of Maximum Distance Separable (MDS) array codes is presented for correcting triple storage failures, which is an extension of the double-erasure-correcting EVENODD code and is called the HDD-EOD code. The encoding and decoding procedures are described by geometrical line graph, which are easily implemented by soft hardware. The analysis shows that the HDD-EOD code provides better decoding performance and higher reliability compared to other popular codes. Thus the HDD-EOD code is practically very meaningful for storage systems.

Guest Editors

Xinxin Niu, Beijing University of Posts and Telecommunications, Beijing, China

Peng Cao, Beijing Institute of Graphic Communication, Beijing, China

Professor Xinxin Niu has graduated from Beijing University of Posts and Telecommunications with a Bachelor’s degree of Science in 1985 and a Master degree in 1988. She receives the Ph.D. degrees from the Department of Electronic Engineering of the Chinese University of Hong Kong (CUHK). As the dean of State Key Laboratory of Networking and Switching Technology and Information Security Center of Beijing University of Posts and Telecommunications, Prof. Niu is also the doctoral Supervisor of Computer Science of her university. She is a fellow of the China Institute of Communications, the Chinese Institute of Electronics and other related professional societies.

Her research areas include Information and Network Security, Signal Processing and Information Processing, Information Hiding and Digital Watermark, Digital Content and Security, communication Theory, Graph Theory, Neural Networks, Signal Processing, Software Radio. Professor Xinxin Niu has more than 50 research papers published in domestic or foreign academic journals such as IEEE Trans. On AES、Chinese Journal of Electronics, as well as 6 books and monographs. She has undertaken National key scientific research projects like the "863" Program, National Science Foundation of China, Ministry of Education Foundation for College Backbone Teacher, Beijing Natural Sciences Foundation, Major Project of Chinese National Program s for Fundamental Research and Development (973 Program) and so on. She has been awarded the Second and Third Prize of Scientific Development Award from the China Institute of Communications and Ministry of Information Industry.

Professor Peng Cao, PhD, is one of the sponsors of the Professional Regulation Construction Union of Digital Media Technology, also is the dean of Information and Mechanical Engineer of Beijing Institute of Graphic Communication, the principal of Beijing Municipal Key Construction of the Discipline of Signal and Information Processing.

He mainly engaged in halftone network printing image information hiding, ink-jet printing electronic equipment, printing equipment of digital intelligent technology. He has published more than forty academic papers and two books. He won the second prize of The National Teaching Achievement Award and the first prize of The Provincial and Ministerial Teaching Achievement Award.