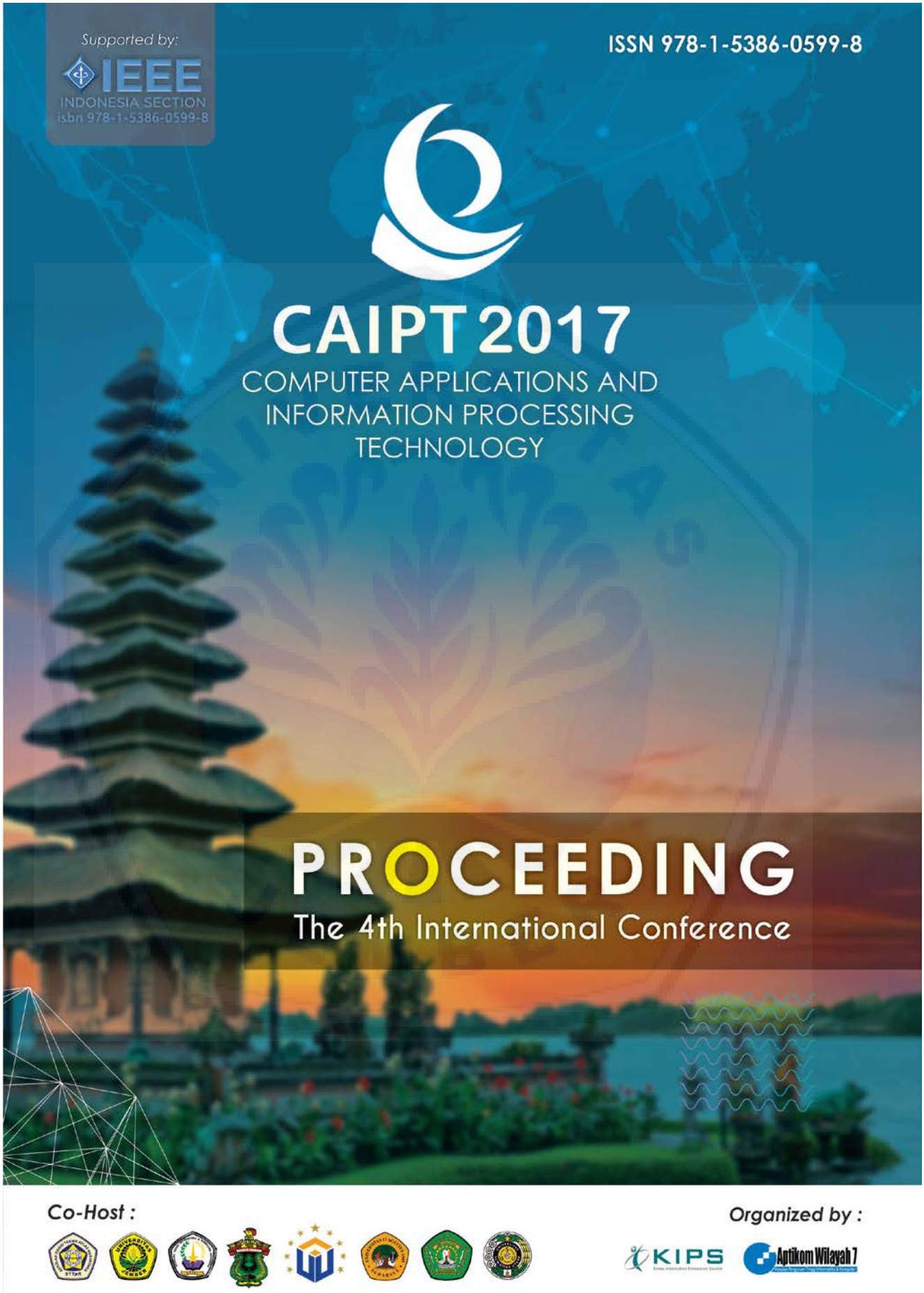


Supported by:
IEEE
INDONESIA SECTION
isbn 978-1-5386-0599-8

ISSN 978-1-5386-0599-8

COMPUTER APPLICATIONS AND INFORMATION PROCESSING TECHNOLOGY

for laptop, CD, and USB

Sponsor

Preface

Organization

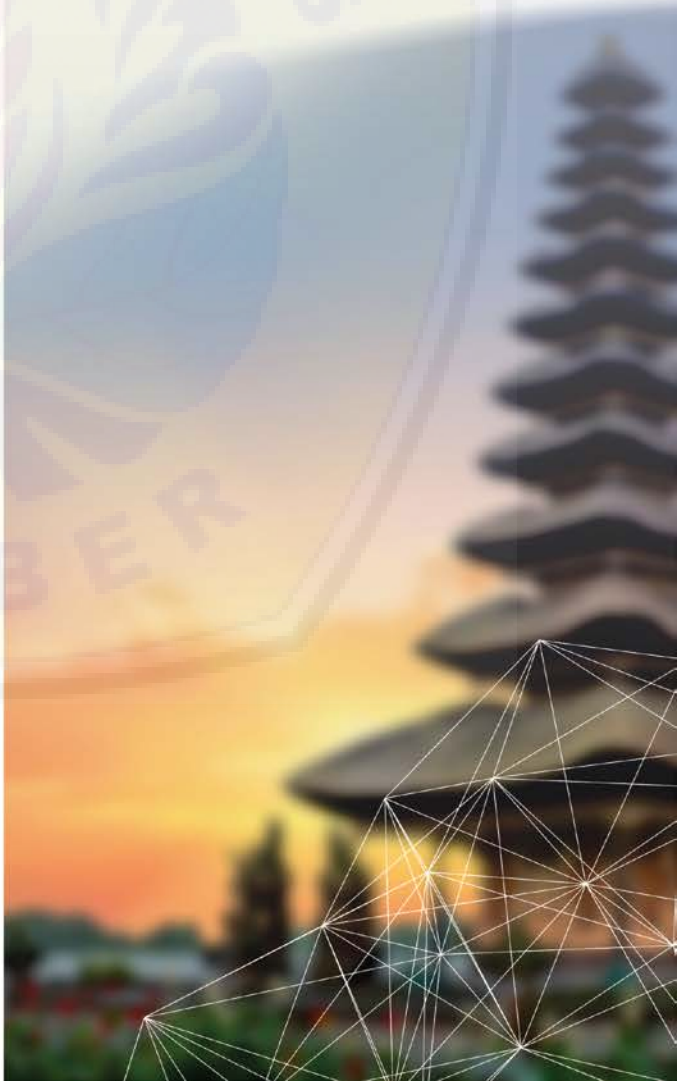
Table of Content

Co-Host :

Organized by :

KIPS

Aptikom Wilayah 7



Welcome Message from CAIPT 2017 Honorary Chair

It is our great pleasure to welcome you to the 4th International Conference on Computer Applications and Information Processing Technology(CAIPT 2017), which is held in the historically rich and naturally beautiful city, Bali, Indonesia on August, 8-10, 2017.

CAIPT 2017 is Organized by Korea Information Processing Society (KIPS) and Hosted by Association of Higher Education in Informatics and Computer (APTIKOM).

CAIPT 2017 will focus on various important aspects of advances in ubiquitous information technologies and applications and will provide an opportunity for researchers and practitioners in academia and industry to discuss the state-of-art issues, research results, and progress in ubiquitous information technologies and applications. We expect that the conference and its publications will stimulate related research and technology improvements on this important subject.

We would like to thank the Program Committee members for their contributions to build up an excellent technical program.

We would like to sincerely thank the following speakers who kindly accepted our invitations, and, in this way, helped to meet the objectives of the conference: Prof. Dr.,Ricardus Eko Indrajit (ABFI Institute Perbanas, Indonesia).

The coordination with the General Co-Chairs (Sang Hoon Kim, Teddy Mantoro, Eva Handriyantini), the Steering Co-Chairs(Jin Kwak, Joko Lianto), the Program Co-Chairs(Kyung Oh Lee, Media A. Ayu),the Organization Chair (Betty Dewi Puspasari), the Publication Chair (Mukhlis Amien), the Publicity Co - Chairs (Eun Young Cho, Rangga Firdaus,Nurul Hidayat), was essential for the success of the final program. We sincerely appreciate their constant support and guidance.

Finally, we would like to thank the Korea Information Processing Society and Asosiasi Pendidikan Tinggi Ilmu Komputer Indonesia for providing valuable assistance to the conference.

We hope you will find the conference very productive and enjoyable.

CAIPT 2017 Honorary Chair
Seok-Cheon Park
Chairman of KIPS IT Convergence Society

Prof. Dr. Lee Kyeong Oh

The Fourth Industrial Revolution is a very hot topic in Korea and I want to share the notion of it with Indonesia educators and researchers.
The First Industrial Revolution used water and steam power to mechanize production. The Second used electric power to create mass production. The Third used electronics and information technology to automate production. Now a Fourth Industrial Revolution is building on the Third, the digital revolution that has been occurring since the middle of the last century. It is characterized by a fusion of technologies that is blurring the lines between the physical, digital, and biological spheres.
Previous industrial revolutions liberated humankind from animal power, made mass production possible and brought digital capabilities to billions of people. This Fourth Industrial Revolution is, however, fundamentally different. It is characterized by a range of new technologies that are fusing the physical, digital and biological worlds, impacting all disciplines, economies and industries, and even challenging ideas about what it means to be human.
The resulting shifts and disruptions mean that we live in a time of great promise and great peril. The world has the potential to connect billions more people to digital networks, dramatically improve the efficiency of organizations and even manage assets in ways that can help regenerate the natural environment, potentially undoing the damage of previous industrial revolutions.
The Fourth Industrial Revolution builds on the Digital Revolution, representing new ways in which technology becomes embedded within societies and even the human body. The Fourth Industrial Revolution is marked by emerging technology breakthroughs in a number of fields, including robotics, artificial intelligence, nanotechnology, quantum computing, biotechnology, The Internet of Things, 3D printing and autonomous vehicles. These technologies have great potential to continue to connect billions more people to the web, drastically improve the efficiency of business and organizations and help regenerate the natural environment through better asset management.[9]

Prof. Dr. Ir. R. Eko Indrajit, M.Sc., MBA., Mphil., MA

Utilizing Big Data to Gain Competitive Advantage: Hypothetical Cases of Indonesia

Many modern companies are flooded with data and information gleaned from their day-to-day business activities. However, there are very few of them who can turn it into a precious asset and provide benefits to the company. Lack of knowledge and competence in the field of data science became one of the causes.
Competition in the 21st century lies in how far the company can learn and master knowledge - where the main source is data and information. Initially, Big data is merely a supporting technology, but has now become a very powerful competing weapon for those who successfully utilize it effectively.
This session provides an overview of how strategic and technical big data use can improve business competitiveness during its significant utilization.

COMMITTEE

Honorary Co – Chairs
Seok Cheon Park, Gachon University, Korea
Im Yeong Lee, Soonchunhyang University, Korea
Bong Gyou Lee, Yonsei University, Korea
Young Sick Jeong, Dongkuk University, Korea
Ricardus Eko Indrajit, ABFI Institute Perbanas, Indonesia
Zainal A. Hasibuan, University of Indonesia, Indonesia
General Co - Chairs
Sang Hoon Kim, Hankyong National University, Korea
Teddy Mantoro, Sampoerna University, Indonesia
Eva Handriyantini, STIKI, Indonesia
Steering Co - Chairs
Jin Kwak, Ajou University, Korea
Joko Lianto, ITS, Indonesia
Organization Co - Chairs
Betty Dewi Puspasari, STTAR, Indonesia**Program Co - Chairs**
Kyung Oh Lee, Sunmoon University, Korea
Media A. Ayu, Sampoerna University, Indonesia
Publication Co - Chairs
Mukhlis Amien, STIKI, Indonesia
Publicity Co - Chairs
Eun Young Cho, Yonsei University, Korea
Rangga Firdaus, Lampung University, Indonesia
Nurul Hidayat, Unsoed ,Indonesia
TPC Members
Hsiao-Hwa Chen, National Cheng Kung University, Taiwan
Mario Freire, University of Beira Interior,Portugal
Charalampos Z Patrikakis, National Tech. University of Athens, Greece
Sherali Zeadally, University of the District of Columbia, USA
Isaac Woungang, Ryerson University, Canada
Daniel C. Doolan, Robert Gordon University, UK
Christian Becker, University of Mannheim, Germany
Roshayu Mohamad, Asia e University. Malaysia
Syed Malek Fakar Duani, Taif University, Saudi Arabia
Teddy Mantoro, Sampoerna University, Indonesia
Achmad Nizar Hidayanto, University of Indonesia, Indonesia
Riyanarto Sarno, Sepuluh November Institute of Technology (ITS), Indonesia
Paulus Insap Santosa, Gajah Mada University, Indonesia
Mahendrawathi ER, ITS, Indonesia
Iping Supriana Suwandi, Bandung Institute of Technology, Indonesia
Kuswara Setiawan, UPH Surabaya, Indonesia
Mi-Hui Kim, Hankyong National University, Korea
Achmad Benny Mutiara, Gunadarma University, Indonesia
Tae-Jin Lee, Hoseo University, Korea
Jun-Seop Kim, KISA, Korea
Woong Go, KISA, Korea
Endang Setyati, STTS, Indonesia
Syaiful Bukhori, UNEJ, Indonesia
Armin Lawi, Hasanuddin University, Indonesia

CAIPT 2017

COMPUTER APPLICATIONS AND INFORMATION PROCESSING TECHNOLOGY

Catalogue of publications at IEEE Xplore Digital Library

Co-Host :

Organized by :

Conference Page

IEEE Xplore Digital Library

Commitee

Publication Year: 2017, Page(s): 1 © | PDF *(78 KB)*

Copyright notice

Publication Year: 2017, Page(s): 1 © | PDF *(42 KB)*

Front cover

Publication Year: 2017, Page(s):1 – 2 © | PDF *(390 KB)*

Keynote speakers - 2 abstracts

Publication Year: 2017, Page(s): 1 © | Abstract | PDF *(91 KB)*

Welcome message from the CAIPT 2017 honorary chair

Publication Year: 2017, Page(s): 1 © | PDF *(90 KB)*

Content:

1. Chimera — Simple language agnostic framework for stand alone and distributed computing
   Authors: Go Frendi Gunawan ; Mukhlis Amien ; Jozua Ferjanus Palandi
   Publication Year: 2017, Page(s):1 – 10 © | Abstract | PDF *(273 KB)*
2. User effects of a distributed dynamic scheme in PMIPv6 networks
   Authors: Yoon-Deock Lee ; Jongpil Jeong
   Publication Year: 2017, Page(s):1 – 6 © | Abstract | PDF *(410 KB)*
3. Empirical test of Wi-Fi environment stability for smart farm platform
   Authors: O. JiHye ; Dong-Hee Noh ; Young-Ho Sohn
   Publication Year: 2017, Page(s):1 – 5 © | Abstract | PDF *(534 KB)*
4. Investigation on performance and energy efficiency of CNN-based object detection on embedded device
   Authors: Sangyoon Oh ; Minsub Kim ; Donghoon Kim ; Minjoong Jeong ;Minsu Lee
   Publication Year: 2017, Page(s):1 – 4 © | Abstract | PDF *(268 KB)*
5. A study on smart drone using quadcopter and object tracking techniques
   Authors: Woo-Seok Yang ; Myung-Hyun Chun ; Gun-Woo Jang ; Jong-Hwan Baek ; Sang-Hoon Kim
   Publication Year: 2017, Page(s):1 – 5 © | Abstract | PDF *(464 KB)*
6. Study on inspecting VR motion sickness inducing factors
   Authors: Su-min Jung ; Taeg-kuen Whangbo
   Publication Year: 2017, Page(s):1 – 5 © | Abstract | PDF *(303 KB)*
7. Sleep stage classification using fuzzy long short-term memory
   Authors: Intan Nurma Yulita ; Rudi Rosadi ; Sri Purwani
   Publication Year: 2017, Page(s):1 – 5 © | Abstract | PDF *(223 KB)*
8. Eloquent object relational mapping models for biodiversity information system
   Authors: Edy Budiman ; Muh Jamil ; Ummul Hairah ; Hario Jati ; Rosmasari
   Publication Year: 2017, Page(s):1 – 5 © | Abstract | PDF *(500 KB)*
9. The analysis of file carving process using PhotoRec and Foremost
   Authors: Nurhayati ; Nurul Fikri
   Publication Year: 2017, Page(s):1 – 6 © | Abstract | PDF *(234 KB)*

10. RFID presence monitoring system as an input to measure the workload of employee
Authors: Romi Fadillah Rahmat ; Eka Tama Herly ; Baihaqi Siregar ;Mohammad Fadly Syahputra ; Opim Salim Sitompul
Publication Year: 2017, Page(s):1 – 6 © / Abstract / PDF (754 KB)

11. Capability level assessment of IT governance in PTP Mitra Ogan: COBIT 5 framework for BAI 04 process
Authors: Sandfreni ; Fransiskus Adikara
Publication Year: 2017, Page(s):1 – 5 © / Abstract / PDF (209 KB)

12. Data mining for predicting students' learning result
Authors: Masna Wati ; Wahyu Indrawan ; Joan Angelina Widians ; Novianti Puspitasari
Publication Year: 2017, Page(s):1 – 4 © / Abstract / PDF (200 KB)

13. Design of a navigation and guidance system of missile with trajectory estimation using ensemble Kalman Filter square root (EnKF-SR)
Authors: Teguh Herlambang
Publication Year: 2017, Page(s):1 – 7 © / Abstract / PDF (324 KB)

14. Enabling disaster-resilient SDN with location trustiness
Authors: Van-Quyet Nguyen ; Sinh Ngoc Nguyen ; Kyungbaek Kim
Publication Year: 2017, Page(s):1 – 4 © / Abstract / PDF (570 KB)

15. A study of performance enhancement in big data anonymization
Authors: Sung-Bong Jang
Publication Year: 2017, Page(s):1 – 4 © / Abstract / PDF (236 KB)

16. A study on reduction of DDoS amplification attacks in the UDP-based CLDAP protocol
Authors: Suk-June Choi ; Jin Kwak
Publication Year: 2017, Page(s):1 – 4 © / Abstract / PDF (237 KB)

17. Improving dynamic ownership scheme for data deduplication
Authors: Won-Bin Kim ; Im-Yeong Lee ; Jae-Cheol Ryou
Publication Year: 2017, Page(s):1 – 4 © / Abstract / PDF (357 KB)

18. HXD: Hybrid XSS detection by using a headless browser
Authors: Hyunsang Choi ; Seongjin Hong ; Sanghyun Cho ; Young-Gab Kim
Publication Year: 2017, Page(s):1 – 4 © / Abstract / PDF (85 KB)

19. Cross-cultural training as part of policy and business strategies to prepare Indonesian IT engineers in global job market competition
Authors: Agung Prabowo ; Rosmiati ; Ika S. Windiarti
Publication Year: 2017, Page(s):1 – 5 © / Abstract / PDF (211 KB)

20. Encryption scheme in portable electric vehicle charging infrastructure: Encryption scheme using symmetric key
Authors: Chan-Kuk Jang ; JaeHoon Lee ; Okyeon Yi
Publication Year: 2017, Page(s):1 – 5 © / Abstract / PDF (410 KB)

21. A study on statistical map of air pollution in Korea using R
Authors: Jung Yeon Seo ; Hwa Min Lee

Publication Year: 2017, Page(s):1 – 5 © / Abstract / PDF *(340 KB)*

22. Determination of interface design attributes on e-learning based on user personality characteristics
Authors: **Supangat** ; **Ery Sadewa Yudha**
Publication Year: 2017, Page(s):1 – 8 © / Abstract / PDF *(358 KB)*

23. Adaptive spatiotemporal similarity measure for a consistent depth maps
Authors: **Yongho Shin** ; **Kuk-Jin Yoon**
Publication Year: 2017, Page(s):1 – 4 © / Abstract / PDF *(728 KB)*

24. Evaluation of the information technology system services for medium higher education based on ITIL (A case study of polytechnic XYZ)
Authors: **Agus Hermanto** ; **Gery Kusnanto**
Publication Year: 2017, Page(s):1 – 8 © / Abstract / PDF *(334 KB)*

25. Application of logarithmic fuzzy preference programming for determining priority as an institutional development strategy
Authors: **Emi Iryanti** ; **Ridwan Pandiya**
Publication Year: 2017, Page(s):1 – 5 © / Abstract / PDF *(244 KB)*

26. Expert system to optimize the best goat selection using topsis: Decision support system
Authors: **Alexius Endy Budianto** ; **E. P. Amak Yunus**
Publication Year: 2017, Page(s):1 – 5 © / Abstract / PDF *(356 KB)*

27. Design network security infrastructure cabling using network development life cycle methodology and ISO/IEC 27000 series in Yayasan Kesehatan (Yakes) Telkom Bandung
Authors: **Kartika Rianafirin** ; **Mochamad Teguh Kurniawan**
Publication Year: 2017, Page(s):1 – 6 © / Abstract / PDF *(533 KB)*

28. A CUDA-based implementation of convolutional neural network
Authors: **Sejin Choi** ; **Kwangyeob Lee**
Publication Year: 2017, Page(s):1 – 4 © / Abstract / PDF *(759 KB)*

29. A study of microscope structure and algorithm for 3D image implementation
Authors: **Sangjoon Lee** ; **Jaeyoung Park**
Publication Year: 2017, Page(s):1 – 5 © / Abstract / PDF *(716 KB)*

30. A review of deep learning in image recognition
Authors: **Myeongsuk Pak** ; **Sanghoon Kim**
Publication Year: 2017, Page(s):1 – 3 © / Abstract / PDF *(190 KB)*

31. Heartbeat count estimation in safety critical systems
Authors: **Hyeon Gyu Kim**
Publication Year: 2017, Page(s):1 – 4 © / Abstract / PDF *(346 KB)*

32. Adjusting initial weights for Adaboost learning
Authors: **Kisang Kim** ; **Hyung-Il Choi**
Publication Year: 2017, Page(s):1 – 5 © / Abstract / PDF *(408 KB)*

33. Fat separation using grid fit method at high-field MRI
Authors: Sung-Jong Eun ; Eun-Young Jung ; Dong Kyun Park ; Taeg-kuen Whangbo
Publication Year: 2017, Page(s):1 – 4 © | Abstract | PDF (345 KB)

34. Design of heterogeneous integrated digital signature system for ensuring platform independence
Authors: Hyung-Joon Kim ; Jung In Yoon ; Young-Hwan Jang ; Seok-Cheon Park
Publication Year: 2017, Page(s):1 – 4 © | Abstract | PDF (268 KB)

35. A study of image-making by personal color analysis: A focus on autumn type make-up and hair
Authors: Ran-Sug Seo
Publication Year: 2017, Page(s):1 – 3 © | Abstract | PDF (155 KB)

36. Analysis on spectrum policy of WAVE for V2X communication system in automobile industry
Authors: Seong Bin Jeong ; Hyun Ju Jo ; Sung Hwan Cho ; Bong Gyou Lee
Publication Year: 2017, Page(s):1 – 4 © | Abstract | PDF (261 KB)

37. On identifying potential direct marketing consumers using adaptive boosted support vector machine
Authors: Armin Lawi ; Ali Akbar Velayaty ; Zahir Zainuddin
Publication Year: 2017, Page(s):1 – 4 © | Abstract | PDF (185 KB)

38. Implementation of real-time static hand gesture recognition using artificial neural network
Authors: Rosalina ; Lita Yusnita ; Nur Hadisukmana ; R. B. Wahyu ;Rusdianto Roestam ; Yuyu Wahyu
Publication Year: 2017, Page(s):1 – 6 © | Abstract | PDF (357 KB)

39. e-KTP as the basis of home security system using arduino UNO
Authors: Miftah Andriansyah ; Muhammad Subali ; Imam Purwanto ; S Antonius Irianto ; Rizky Agung Pramono
Publication Year: 2017, Page(s):1 – 5 © | Abstract | PDF (366 KB)

40. Implementation of BCBimax algorithm to determine customer segmentation based on customer market and behavior
Authors: Anis R. Amna ; Agus Hermanto
Publication Year: 2017, Page(s):1 – 5 © | Abstract | PDF (252 KB)

41. A geographical information system design for analyzing food distribution in Indonesia
Authors: Henny Medyawati ; Budi Setiawan ; Imam Ahmad Trinugroho ;Ega Hegarini
Publication Year: 2017, Page(s):1 – 4 © | Abstract | PDF (207 KB)

42. Design monitoring of distribution transformer load by messenger based on microcontroller atmega 128
Authors: Firman Yudianto ; Sistem Informasi ; Fakultas Teknik
Publication Year: 2017, Page(s):1 – 3 © | Abstract | PDF (268 KB)

43. Malaysian to German sign language statistical machine translation using Markov chain and search algorithms
Authors: Fridy Mandita ; Harnan Malik Abdullah ; Toni Anwar
Publication Year: 2017, Page(s):1 – 5 © | Abstract | PDF (266 KB)

44. Symbiotic organisms search algorithm for scheduling laboratory sessions in University
Authors: C. Pickerling ; Hendrawan Armanto ; Eka Rahayu Setyaningsih
Publication Year: 2017, Page(s):1 – 6 © | Abstract | PDF (130 KB)

45. Application of baby's nutrition status using Macromedia Flash
Authors: Ima Kurniastuti
Publication Year: 2017, Page(s):1 – 6 © | Abstract | PDF (394 KB)

46. Ensemble GradientBoost for increasing classification accuracy of credit scoring
Authors: Armin Lawi ; Firman Aziz ; Syafruddin Syarif
Publication Year: 2017, Page(s):1 – 4 © | Abstract | PDF (243 KB)

47. Proposed priority packet data dissemination scheduling mechanism
Authors: Syafruddin Syarif ; Armin Lawi ; Jeffry
Publication Year: 2017, Page(s):1 – 5 © | Abstract | PDF (286 KB)

48. Hierarchical graph neuron scheme in classifying intrusion attack
Authors: Aulia Essra ; Opim Salim Sitompul ; Benny Benyamin Nasution ;Romi Fadillah Rahmat
Publication Year: 2017, Page(s):1 – 6 © | Abstract | PDF (290 KB)

49. Establishing decision support system for determination healthy menu based in multi criteria and interatice approach
Authors: Paramitha Nerisafitra ; Pratiwi Hariyani Putri
Publication Year: 2017, Page(s):1 – 5 © | Abstract | PDF (396 KB)

50. A neurocomputing approach for anomaly detection of Mt. Merapi monitoring activity
Authors: Paramitha Nerisafitra ; Tri Deviasari Wulan
Publication Year: 2017, Page(s):1 – 4 © | Abstract | PDF (249 KB)

51. Preliminary study of utilizing Internet of Things for monitoring energy use in building to support energy audit process
Authors: Muhammad Priyono Tri Sulistyanto ; Kurriawan Budi Pranata ;Solikhan
Publication Year: 2017, Page(s):1 – 7 © | Abstract | PDF (684 KB)

52. A rendezvous point estimation considering drone speed and data collection delay
Authors: Kwangsoo Jo ; Junyoung Heo ; Jinman Jung ; Bongjae Kim ; Hong Min
Publication Year: 2017, Page(s):1 – 4 © | Abstract | PDF (435 KB)

53. Secure multicast authentication scheme using DTLS
Authors: Si-Jae Woo ; Jin Kwak
Publication Year: 2017, Page(s):1 – 5 © | Abstract | PDF (509 KB)

54. Enabling external factors for consumption electricity forecasting using hybrid genetic algorithm and fuzzy neural system
Authors: Gayatri Dwi Santika
Publication Year: 2017, Page(s):1 – 6 © | Abstract | PDF (422 KB)

55. G-code conversion from 3D model data for 3D printers on Hadoop systems
Authors: Sungsuk Kim ; Kwangsik Chung ; Heonchang Yu ; Sun Ok Yang
Publication Year: 2017, Page(s):1 – 4 © | Abstract | PDF (382 KB)

56. Measuring end-user satisfaction of online marketplace using end-user computing satisfaction model (EUCS Model) (Case study: Tokopedia.com)
Authors: Beny Prasetyo ; R. Windi Eka Yulia ; Felisia
Publication Year: 2017, Page(s):1 – 5 © | Abstract | PDF (208 KB)

57. Trending topic prediction by optimizing K-nearest neighbor algorithm
Authors: Syafruddin Syarif ; Anwar ; Dewiani
Publication Year: 2017, Page(s):1 – 4 © | Abstract | PDF (252 KB)

58. First aid instructional media using Android platform
Authors: Andy Pramono ; S. Kom ; Betty Dewi Puspasari ; S. Kom
Publication Year: 2017, Page(s):1 – 5 © | Abstract | PDF (354 KB)

59. Designing gamification on Social Agriculture (SociAg) application to increase end-user engagement
Authors: Ifrina Nuritha ; Vandha Pradwiyasma Widartha ; Saiful Bukhori
Publication Year: 2017, Page(s):1 – 5 © | Abstract | PDF (225 KB)

60. Usability testing to evaluate the library's academic web site
Authors: Windi Eka Yulia Retnani ; Beny Prasetyo ; Yofanda Putra Prayogi ;M Abbi Nizar ; R Muhamat Abdul
Publication Year: 2017, Page(s):1 – 4 © | Abstract | PDF (226 KB)

61. A study on the effective interaction method to improve the presence in social virtual reality game
Authors: Seok Hee Oh ; Taeg Keun Whangbo
Publication Year: 2017, Page(s):1 – 2 © | Abstract | PDF (313 KB)

62. Performance analysis of extract, transform, load (ETL) in apache Hadoop atop NAS storage using ISCSI
Authors: Adnan ; Amil Ahmad Ilham ; Syahrul Usman
Publication Year: 2017, Page(s):1 – 5 © | Abstract | PDF (361 KB)

63. Governance of information system development as tourism support used IT balanced scorecard and McFarlan
Authors: Fajrin Nurman Arifin ; Oktalia Juwita
Publication Year: 2017, Page(s):1 – 7 © | Abstract | PDF (309 KB)

64. Selection of supplier using analytical hierarchy process: Creating value added in the supply chain agribusiness
Authors: Saiful Bukhori ; Diah Ayu Sukmawati ; Y. R. Windi Eka
Publication Year: 2017, Page(s):1 – 6 © | Abstract | PDF (200 KB)

65. Analysis on characteristics of vehicle and parking lot as a datacenter
Authors: Taesik Kim ; Hong Min ; Jisu Park ; Jaeuk Lee ; Jinman Jung
Publication Year: 2017, Page(s):1 – 4 © | Abstract | PDF (233 KB)

66. Measurement systems of individual E-business competency in an E-business management environment
Authors: Chui Young Yoon
Publication Year: 2017, Page(s):1 – 4 © | Abstract | PDF (196 KB)

67. A microservice development for document management system
Authors: Pankamol Srikaew ; Inkyu Kim
Publication Year: 2017, Page(s):1 – 4 © / Abstract / PDF (370 KB)

68. A key distribution system for user authentication using pairing-based in a WSN
Authors: Gun-Wook Choi ; Im-Yeong Lee
Publication Year: 2017, Page(s):1 – 4 © / Abstract / PDF (309 KB)

69. PassPositions: A secure and user-friendly graphical password scheme
Authors: Gi-Chul Yang
Publication Year: 2017, Page(s):1 – 5 © / Abstract / PDF (207 KB)

70. Malware behavior analysis using binary code tracking
Authors: Jihun Kim ; Jonghee M. Youn
Publication Year: 2017, Page(s):1 – 4 © / Abstract / PDF (213 KB)

71. Shared secret key update scheme between RADIUS server and access point using PUFs
Authors: Jungsoo Park ; Souhwan Jung
Publication Year: 2017, Page(s):1 – 5 © / Abstract / PDF (398 KB)

72. AiTES: The self-adaptive framework for environment change of IoT
Authors: JungHyen Ahn ; Young B. Park
Publication Year: 2017, Page(s):1 – 4 © / Abstract / PDF (280 KB)

73. Design of the Korean medicine symptom diagnosis system using Word2Vec
Authors: Sang-Baek Lee ; Kyu-Chul Lee
Publication Year: 2017, Page(s):1 – 2 © / Abstract / PDF (212 KB)

74. Implementation of random parameter filtering using OpenMP
Authors: Seong-Hyeon Han ; Kwang-Yeob Lee
Publication Year: 2017, Page(s):1 – 4 © / Abstract / PDF (455 KB)

75. Incentive mechanism with privacy-preservation on intelligent parking system utilizing mobile crowdsourcing
Authors: Mihui Kim
Publication Year: 2017, Page(s):1 – 4 © / Abstract / PDF (276 KB)

76. Systematic literature review: Model refactoring
Authors: Tio Dharmawan ; Siti Rochimah
Publication Year: 2017, Page(s):1 – 5 © / Abstract / PDF (215 KB)

77. Search engine optimization: Raising the ranking of “Suku Osing” websites on search engine page
Authors: Nur Kholis Mansur ; Fahrobby Adnan
Publication Year: 2017, Page(s):1 – 4 © / Abstract / PDF (589 KB)

78. Design of information system development strategy based on the conditions of the organization
Authors: Oktalia Juwita ; Fajrin Nurman Arifin
Publication Year: 2017, Page(s):1 – 5 © / Abstract / PDF (235 KB)

79. Oblivious content distribution system to advantage digital rights management
Authors: Antonius Cahya Prihandoko ; Hossein Ghodosi
Publication Year: 2017, Page(s):1 – 5 © | Abstract | PDF (233 KB)

80. A comparison of classification algorithms for Event Related Potentials
Authors: Abdulmajeed Alsufyani
Publication Year: 2017, Page(s):1 – 5 © | Abstract | PDF (340 KB)

81. Implementation of integer programming in decision support system for operational optimize procurement of public bus transport distribution (Case study: Trans Jogja)
Authors: Diah Ayu Retnani Wulandari
Publication Year: 2017, Page(s):1 – 7 © | Abstract | PDF (236 KB)

82. Risk analysis on the development of a business continuity plan
Authors: Alexander Setiawan ; Adi Wibowo ; Andrew Hartanto Susilo
Publication Year: 2017, Page(s):1 – 4 © | Abstract | PDF (191 KB)

83. New approach toward data hiding by using affine cipher and least significant bit algorithm
Authors: D. Rachmawati ; M. A. Budiman
Publication Year: 2017, Page(s):1 – 6 © | Abstract | PDF (325 KB)

84. Information systems strategic planning: Using design thinking method at startup company
Authors: Jarot S. Suroso ; Riswan E. Tarigan ; Fatkhurozaq B. Setyawan
Publication Year: 2017, Page(s):1 – 6 © | Abstract | PDF (331 KB)

85. Abnormality classification on the shape of red blood cells using radial basis function network
Authors: Mohammad Fadly Syahputra ; Anita Ratna Sari ; Romi Fadillah Rahmat
Publication Year: 2017, Page(s):1 – 5 © | Abstract | PDF (206 KB)

86. Quality framework for quality assuring enterprise architecture model
Authors: Sri Agustina Rumapea ; Benhard Sitohang
Publication Year: 2017, Page(s):1 – 5 © | Abstract | PDF (346 KB)

87. Analysis of radio based train control system using LTE-R and analysis of security requirements: The security of the radio based train control system
Authors: JaeHoon Lee ; Chan-Kuk Jang ; Okyeon Yi
Publication Year: 2017, Page(s):1 – 4 © | Abstract | PDF (242 KB)

88. Vision based distance measurement system using two-dimensional barcode for mobile robot
Authors: Jong Hwan Beck ; Sang Hoon Kim
Publication Year: 2017, Page(s):1 – 4 © | Abstract | PDF (415 KB)

89. The mechanism of personalized service recommendation for the academic field
Authors: Yun-Young Hwang ; Junghoon Park ; Seoung Eun Park ; Jungsun Yoon
Publication Year: 2017, Page(s):1 – 4 © | Abstract | PDF (164 KB)

90. Live colors: Visualizing celluar automata
Authors: Hyeri Rhee ; Moon-Ryul Jung ; Sook-Jin Kim
Publication Year: 2017, Page(s):1 – 5 © | Abstract | PDF (577 KB)

91. Issues and concerns: Record management in cloud services
Authors: Youngkon Lee ; Ukhyun Lee
Publication Year: 2017, Page(s):1 – 6 © | Abstract | PDF *(645 KB)*

92. VANET routing algorithm performance comparison using ns-3 and SUMO
Authors: Seung-Seok Kang ; Ye-Eun Chae ; Seunguk Yeon
Publication Year: 2017, Page(s):1 – 5 © | Abstract | PDF *(435 KB)*

93. Adaptive video coding selection scheme for solar-powered wireless video sensor networks
Authors: Jun Min Yi ; Ikjune Yoon ; Dong Kun Noh
Publication Year: 2017, Page(s):1 – 4 © | Abstract | PDF *(355 KB)*

94. Migration scheme based machine learning for QoS in cloud computing: Survey and research challenges
Authors: A-Young Son ; Eui-Nam Huh ; Sang-Ho Na ; Pill-Woo Lee
Publication Year: 2017, Page(s):1 – 4 © | Abstract | PDF *(175 KB)*

95. Design of car license plate area detection algorithm for enhanced recognition plate
Authors: Chi-Sung Ahn ; Bong-Gyou Lee ; Seung-Su Yang ; Seok-Cheon Park
Publication Year: 2017, Page(s):1 – 4 © | Abstract | PDF *(568 KB)*

96. Analyzing consumption trends of broadcasting contents with theoretical frameworks
Authors: Eun-Young Cho ; Bong Gyou Lee
Publication Year: 2017, Page(s):1 – 4 © | Abstract | PDF *(225 KB)*

97. Policy development of sharing economy in Korea: Case of home-sharing
Authors: Sanghyun Lee ; Bong Gyou Lee
Publication Year: 2017, Page(s):1 – 4 © | Abstract | PDF *(182 KB)*

Table of content

Publication Year: 2017, Page(s):1 - 8

© | PDF (87 KB)

Title page

Publication Year: 2017, Page(s): 1

© | PDF (38 KB)

Oblivious content distribution system to advantage digital rights management

2 Author(s)

Antonius Cahya Prihandoko ; Hossein Ghodosi

View All Authors

Abstract:
This research aims to construct a content distribution protocol that preserves the content provider's security and users' privacy. The protocol can improve Digital Rights Management (DRM) that is required to provide balanced protection for the content provider and the users in a content distribution system. The concept of oblivious transfer (OT) is utilized to fulfill the DRM requirement. The OT concept allows a sender to securely send a set of information to a receiver in such a way that, at the end of the protocol, the receiver cannot learn more than he was supposed to learn while the sender cannot determine what the receiver has learned. Assuming that tamper-proof device exists, the constructed protocol achieves perfect security for the content provider and privacy for the users. This oblivious content distribution ultimately enables DRM to be a privacy-aware protection system. The system does not merely focus on content providers' rights, but also seriously considers users' privacy protection.

Published in: Computer Applications and Information Processing Technology (CAIPT), 2017 4th International Conference on

Date of Conference: 8-10 Aug. 2017

DOI: 10.1109/CAIPT.2017.8320733

Date Added to IEEE *Xplore*: 22 March 2018

Publisher: IEEE

ISBN Information:

Conference Location: Kuta Bali, Indonesia, Indonesia

Contents

I. Introduction
Digital Rights Management (DRM) is a popular approach to achieve security required in digital content distribution systems. Under DRM protection, dig content is usually encrypted before distributed. To strengthen security, the implementation of the encryption algorithms needs to be modified, so that th algorithms are unintelligible to adversaries. Some methods, such as code obfuscation [1] and white-box cryptography [2]–[5], have been proposed to undertake such modifications. These methods ultimately aim to keep the decryption key secret, so that only authorized users can access protected co In addition, traitor tracing schemes [6], [7] have also been implemented to trace nasty users that redistribute the content illegally.

Read document

Authors

Oblivious Content Distribution System to Advantage Digital Rights Management

Antonius Cahya Prihandoko
Information Technology Department
University of Jember
Jember, Indonesia
antoniuscp.ilkom@unej.ac.id

Hossein Ghodosi
Information Technology Department
James Cook University
Townsville, Australia
hossein.ghodosi@jcu.edu.au

***Abstract*— This research aims to construct a content distribution protocol that preserves the content provider's security and users' privacy. The protocol can improve Digital Rights Management (DRM) that is required to provide balanced protection for the content provider and the users in a content distribution system. The concept of oblivious transfer (*OT*) is utilized to fulfill the DRM requirement. The *OT* concept allows a sender to securely send a set of information to a receiver in such a way that, at the end of the protocol, the receiver cannot learn more than he was supposed to learn, while the sender cannot determine what the receiver has learned. Assuming that tamper-proof device exists, the constructed protocol achieves perfect security for the content provider and privacy for the users. This oblivious content distribution ultimately enables DRM to be a privacy-aware protection system. The system does not merely focus on content providers' rights, but also seriously considers users' privacy protection.**

Keywords—component; digital rights management, content distribution system, oblivious transfer, security, privacy

I. INTRODUCTION

Digital Rights Management (DRM) is a popular approach to achieve security required in digital content distribution systems. Under DRM protection, digital content is usually encrypted before distributed. To strengthen security, the implementation of the encryption algorithms needs to be modified, so that the algorithms are unintelligible to adversaries. Some methods, such as code obfuscation [1] and white-box cryptography [2-5], have been proposed to undertake such modifications. These methods ultimately aim to keep the decryption key secret, so that only authorized users can access protected content. In addition, traitor tracing schemes [6, 7] have also been implemented to trace nasty users that redistribute the content illegally.

Focusing on the security aspect, however, DRM systems often neglect users' privacy. The systems usually collect users' data to allocate appropriate usage rights. This data acquisition is also useful to view users' buying patterns. The provider may use the data for marketing purposes without users' permission. This situation increasingly invades users' privacy and, thus, reduces users' satisfaction. Therefore, DRM systems need to provide balanced protection for content providers' security and users' privacy [8].

A typical DRM for content distribution consists of four parties: content provider, distributor, clearing house and consumer (user) [9]. First of all, the content provider delivers encrypted content to the distributor and corresponding usage rules to the clearinghouse. The distributor makes the protected content available on a web server that enables users to download it. A consumer then retrieves the content through the distribution channel and requests a license from the clearinghouse. Downloading content from the distributor's web does not seriously threaten the content provider's security neither the users' privacy. While the users can download content anonymously, they cannot unlock the content, unless having the proper decryption key. In contrast, acquiring a license from the clearinghouse creates a concern over security and privacy. If an eavesdropper steals the license when a user requests it from the clearinghouse, revenue will be lost, and thus threaten the provider's security. Moreover, personal information submitted by a user to the clearinghouse is not guaranteed to be kept secret, thus potentially threat the user's privacy.

To overcome the problem, we construct a content distribution protocol by utilizing the oblivious transfer concept. Oblivious Transfer (OT) is a cryptographic protocol that allows two parties to privately exchange one or more secret messages. An OT protocol has to be set up in such a way that it will achieve security for the sender and privacy for the receiver [10]. The former means that the receiver will not be able to learn more than he was supposed to learn. The latter means that the sender will not know what the receiver has learned. The first OT protocol, introduced by Rabin [11], was intended to overcome the exchange of secrets (EOS) problem. This protocol enables a sender to deliver a message to a receiver in such a way that the receiver can access the message with probability $1/2$ and the sender will not know whether the message was received. Rabin's protocol was then generalized to the OT_1^2 [12] . In the OT_1^2 protocol, the sender has two secret messages and the receiver wishes to learn one of them. This scheme has been studied extensively and

generalized to a wide variety of models including OT_1^N [13-15] and OT_K^N [16, 17]. The security of the OT protocols has been intensively studied [18-21]. The OT protocols are also aimed at overcoming the restriction in the availability of the secret message.

II. The Proposed Protocol and Implementation

To provide a solution for the identified DRM problem, we undertake four stages: (1) constructing an oblivious content distribution protocol; (2) implementing the protocol to improve the DRM model for content distribution; (3) analyzing the security and privacy aspects of the improved DRM; and (4) extending the protocol to cover more variables.

A. Oblivious Content Distribution Protocol

Our oblivious content distribution protocol, described in our previous paper [22], utilizes tamper-proof devices. A tamper-proof device means any device that can be used only in a particular way, otherwise the device will be corrupted and its content will no longer be accessible. Utilizing tamper-proof devices in this protocol is less expensive. The device contains only two types of functions, `GetKey` and `GetContent`. `GetKey` function allows the user to ask for the key; that is, the input parameter to the `GetContent` function. `GetContent`, on the other hand, requires an authorized key to reveal the message stored in it. With this characteristic, the device can be mass produced at a low cost. Creating a single device containing all pairs of functions (`GetKey`,`GetContent`) may be reasonable and more efficient. However, for the sake of clarity in this sub section, we assume that one device contains a pair of functions (`GetKey`,`GetContent`).

The protocol allows content provider to deliver contents to user in such a way that at the end of the protocol the user cannot access contents more than he is supposed to access and the content provider will not know which contents are accessed by the user. Suppose the content provider (say, Alice) provides N contents (e.g. movies), (M_1, ..., M_N), and the user (say, Bob) wishes to access K, where $K < N$, of these contents. Alice has a secret code S to access the contents, and utilizes Shamir's secret sharing scheme [23], with the threshold parameter N-K, to share the secret. That is, she splits the secret into N pieces such that any set of at least N-K shares can reconstruct the secret.

The detail protocol is as follows. To share the secret and send the contents, Alice performs the following steps:

1. She secretly chooses random N-K-1 elements of Z_p, denoted a_1, ..., a_{N-K-1} and forms the polynomial $f(x) = S + a_1 x^1 + ... + a_{N-K-1} x^{N-K-1}$. Note that p is a prime and $p > N$.
2. For $i = 1, ..., N$, she computes s_i, where $s_i = f(i) \bmod p$
3. She loads device d_i with s_i as the key value, and M_i as the content value.
4. She gives all devices to Bob.

After delivering the devices there is no subsequent communication between Alice and Bob. Bob can access K contents if he accepts sacrificing N-K contents that are not supposed to be accessed. This condition is applied with assumption that once a device is executed, it will be corrupted or will destroy itself. To obtain K contents, Bob performs the following steps (see also Figure 1 for a clear illustration).

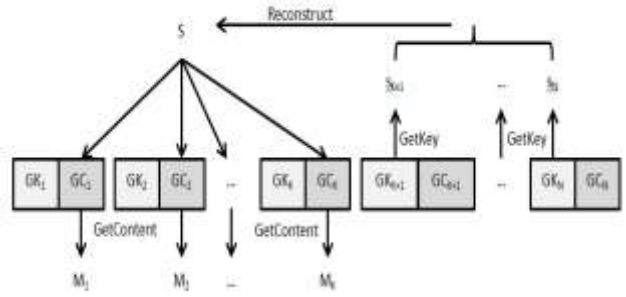


Figure 1. Process for obtaining K out of N contents

1. For simplicity, assume that K contents Bob want to access are M_1, ..., M_K. Bob performs the `GetKey` function on the devices d_{K+1},...,d_N (namely GK_{K+1},...,GK_N), to obtain N-K shares.
2. With the N-K shares, s_{K+1},...,s_N, Bob can reconstruct the polynomial, e.g. using the Lagrange interpolation, and learn the secret S.
3. Using the access code S, Bob performances the `GetContent` function on devices d_1, ..., d_K (namely GC_1,...,GC_K) to obtain the contents M_1, ..., M_K.

B. Implementation to Improve DRM

To implement the constructed protocol in the DRM applications, we employ smart cards. A smart card contains an embedded microprocessor so that it can be used not only to store data, but also to process the data [24]. The microprocessor is also used for security purposes. Data are never directly available to the external applications as the microprocessor controls data handling and memory access according to a given set of conditions.

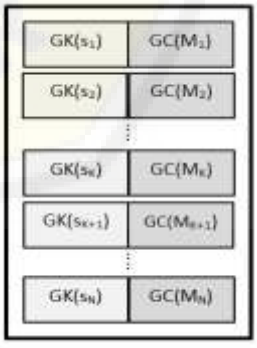


Figure 2. Smart card model; *GK* and *GC* stand for `GetKey` and `GetContent`, respectively.

Suppose the content provider provides N contents, M_1, ..., M_N. First of all, the content provider encrypts all contents using a secret key S. For a particular value K, $1 \leq K \leq N-1$, S is split into N shares, $s_1,\ldots,s_N$, using Shamir's scheme with the threshold parameter $N-K$. The content provider then passes the protected contents to the distributor and the key's shares to the smart card (SC) manufacturer.

The SC manufacturer creates smart cards and sends them to the distributor. The smart card model (see Figure 2) has the following characteristics.

1. For a particular K, a smart card contains N pairs of functions (`GetKey(s_i)`, `GetContent(M_i)`), where $i = 1,2,\ldots,N$.
2. Only one function can be executed from each pair. That is, executing the function `GetKey(s_i)` will disable the associated function `GetContent(M_i)` and, thus, will deny access to the associated content M_i. Conversely, executing the function `GetContent(M_i)` will disable `GetKey(s_i)`.
3. In concrete terms, the smart card executes N-K `GetKey` functions associated with N-K unselected contents. The shares revealed by these functions are then combined to construct the key S that be used to unlock K selected contents

A user can download the protected contents from the distributor's channel and purchases an appropriate smart card. To access the downloaded contents, the user's player must be connected to a compatible smart card reader. A K-valued smart card can be used to unlock K selected contents and denies access to N-K unselected contents.

C. Security and Privacy Analysis

The improved DRM model for content distribution provides an efficient mechanism. Instead of a clearing house, the system employs a smart card manufacturer. Users obtain the content and the corresponding license (provided by an appropriate smart card) from one party, that is, the distributor. This mechanism makes the process more efficient. Furthermore, the improved system also achieves security and privacy for the content provider and the users, respectively. An analysis of both characteristics follows.

Assuming that the smart card is a tamper-proof device, the proposed oblivious content distribution protocol achieves perfect security for the content provider. In the proposed protocol, the shares of the secret key and the function for accessing content are stored in tamper-proof devices. The user cannot access content without obtaining the secret key. The key, however, is split into several pieces of shares and distributed among the pairs of functions (`GetKey`,`GetContent`) inside the device, using Shamir's secret sharing scheme [23]. This scheme is secure because knowing less than a predetermined number of shares gives the user no way to reconstruct the secret. As a result, the user can only obtain the secret key if (and only if) he sacrifices all contents that he is not supposed to access. This means that the user is not able to access anything other than the contents that are supposed to be accessed. Additionally, the smart card is only allocated to the user who has made the payment for it. A particular smart card allows the user to access a limited number of contents as determined in it. Therefore, the proposed protocol achieves perfect security for the content provider.

By the same assumption, the proposed oblivious content distribution protocol preserves high privacy for the users. In the proposed protocol, there is no interaction between content provider and user after the content provider gives all devices to the user. There is no way for the content provider to determine which devices the user has used. As all pairs of functions (`GetKey`,`GetContent`) are corrupted at the end of the protocol, the content provider has no knowledge about which content that has been accessed by the user. Additionally, in the protocol implementation, to unlock the content, a user does not need to provide his personal data for the license. Instead, he purchases the corresponding smart card anonymously. The content and its associated smart card will not be connected to the user's identity. Therefore, the user's privacy is protected.

III. Extended Protocol

In the basic protocol described previously, a user can decrypt a set of contents no more than he was supposed to access. However, once the content has been decrypted, the user can play it without limit. If the restriction of the number of plays is also considered in a business scheme, then an extra variable must be added to the content distribution protocol.

This section describes how the proposed protocol can be enlarged to cover more variables of the usage rules. That is, how we can combine the variable *number_of_items* and *number_of_plays* in one scheme. For example, a user may purchase 5 items, namely content M_1,M_2,M_3,M_4,M_5, and 20 plays. In this case, the user can play all items, but no more than 20 times overall. He may play M_1 for 3 times, M_2 for 4 times, M_3 for 7 times, M_4 for 4 times and M_5 twice. However, he cannot play M_2 for 10 times and M_5 for 11 times.

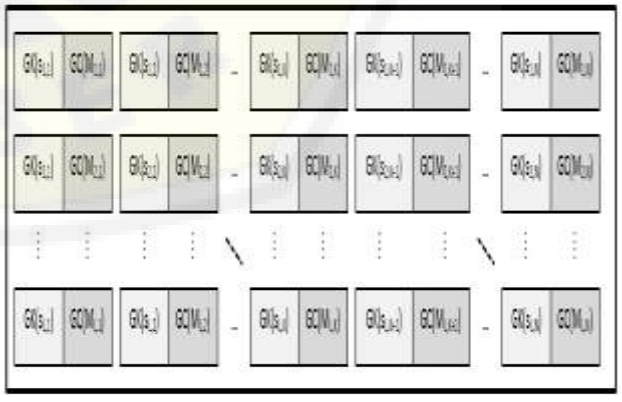


Figure 3. Extended smart card model for the extended protocol

Generally, suppose content provider has N items and a user purchases K items and L plays. An extended smart card utilized to fulfill this need is called (L,K)-smart card. In the (L,K)-smart card model, we place $L \times N$ pairs of functions $(\texttt{GetKey}(s_{i,j}), \texttt{GetContent}(M_{i,j}))$ in a $L \times N$ matrix. For a particular j and $1 \leq i \leq L$, all $s_{i,j}$ and $M_{i,j}$ associate with the key share s_j and the item M_j, respectively. The extended smart card (see Figure 3) has following characteristics:

a. As the previous model, only one function can be executed from each pair.
b. The secret decryption key S can be obtained by executing some `GetKey` functions at the first play (i.e at the first row of the matrix). Once S is reconstructed, it can be used to decrypt other selected items at subsequent plays.
c. Executing $\texttt{GetKey}(s_{1,j})$ functions will disable associated $\texttt{GetContent}(M_{i,j})$ functions for all $1 \leq i \leq L$, and thus, unable user to access item M_j in all plays.
d. For each i, executing a $\texttt{GetContent}(M_{i,j})$ function, will disable all $\texttt{GetContent}(M_{i,h})$ functions, for $h \neq j$. This means that for each play user can only access one item.

To access K items and L plays, Bob has to perform the following protocol.

1. Bob determines K items he wants to access. For simplicity, without lost of generalization, assume that K items Bob chooses are $M_1, ..., M_K$.
2. Smart card then executes $\texttt{GetKey}(s_{1,K+1}), \ldots, \texttt{GetKey}(s_{1,N})$ functions to obtain shares $s_{K+1}, \ldots, s_N$ and reconstruct the secret key S. The key is then be used for all plays. These executions disable all $\texttt{GetContent}(M_{i,j})$ functions, for $1 \leq i \leq L$ and $K+1 \leq j \leq N$.
3. For each i, where $1 \leq i \leq L$, smart card can only execute one of K $\texttt{GetContent}(M_{i,j})$ functions, for $1 \leq j \leq K$

The characteristics of (L,K)-smart card and the protocol it performs guarantee that the user can play all K items, but no more than L times overall. This advanced scenario provides a flexible content distribution system that still preserves security and privacy.

IV. Conclusion

The oblivious content distribution protocol developed in this research provides balanced protection for the content provider and the users in a content distribution system. To strengthen security of the distributed content, the decryption key is split into a number of shares. Decrypting the protected content requires adequate shares to reconstruct the key. It means that a user can only access content that he has paid for. On the other hand, utilizing tamper-proof devices in the protocol guarantees that the users' privacy is protected.

The proposed protocol can also be enlarged to cover more variables. Despite providing flexibility, the system still preserves security and privacy. The implementation of the protocol can potentially improved DRM to be a privacy-aware rights protection system – providing balanced achievement on content provider's security and users' privacy.

Acknowledgment

This paper is an extended version of our paper titled *Secure and Private Content Distribution in the DRM* Environment that was presented at Information System International Conference (ISICO) 2013[22]

References

[1] B. Barak, O. Goldreich, R. Impagliazzo, S. Rudich, A. Sahai, S. Vadhan, and K. Yang, "On the (Im)possibility of Obfuscating Program," in *Advance in Cryptology - CRYPTO 2001: 21st Annual International Cryptology Conference*, Santa Barabara, California, USA, 2001, pp. 1-18.

[2] A. C. Prihandoko, H. Ghodosi, and B. Litow, "White-box Implementation to Advantage DRM," *International Journal on Advanced Science, Engineering dan Information Technology*, vol. 7, pp. 460-467, 2017.

[3] S. Chow, P. Eisen, H. Johnson, and P. C. v. Oorschot, "A White-Box DES Implementation for DRM Applications," presented at the DRM 2002, 2003.

[4] S. Chow, P. Eisen, H. Johnson, and P. C. v. Oorschot, "White-Box Cryptography and an AES Implementation," presented at the SAC 2002, 2003.

[5] B. Wyseur. (2012, April) White-Box Cryptography: Hiding Keys in Software. *MISC HS 5 Magazine*. 65-72. Available: http://whiteboxcrypto.com/files/2012_misc.pdf

[6] B. Chor, A. Fiat, M. Naor, and B. Pinkas, "Tracing Traitors," *IEEE Transaction on Information Theory*, vol. 46, pp. 893-910, 2000.

[7] A. C. Prihandoko, H. Ghodosi, and B. Litow, "Deterring Traitor Using Double Encryption Scheme," in *The IEEE International Conference on Communication, Network and Satellite*, Yogyakarta, Indonesia, 2013, pp. 100-104.

[8] A. C. Prihandoko, B. Litow, and H. Ghodosi, "DRM's Rights Protection Capability: A Review," in *The First International Conference on Computational Science and Information Management*, Medan, Indonesia, 2012, pp. 12-17.

[9] Q. Liu, R. Safavi-Naini, and N. P. Sheppard, "Digital Rights Management for Content Distribution," presented at the Australian Information Security Workshop on ACSW Frontiers'03, 2003.

[10] H. Ghodosi, "A General Model for Oblivious Transfer," in *the Sixth International Workshop for Applied PKC*, Perth, Australia, 2007, pp. 79-87.

[11] M. O. Rabin, "How to Exchange Secrets with Oblivious Transfer," Aiken Computation Lab, Harvard University, Technical Report TR-81, 1981.

[12] S. Even, O. Goldriech, and A. Lempel, "A Randomized Protocol for Signing Contracts," *Communications of the ACM*, vol. 28, pp. 637-647, 1985.

[13] M. Naor and B. Pinkas, "Oblivious Transfer and Polynomial Evaluation," in *Thirty-first Annual ACM Symposium on Theory of Computing*, Atlanta, Georgia, USA, 1999, pp. 245-254.

[14] W.-G. Tzeng, "Efficient 1-Out-n Oblivious Transfer Schemes," in *PKC 2002*, 2002, pp. 159-171.

[15] W.-G. Tzeng, "Efficient 1-Out-of-n Oblivious Transfer Schemes with Universally Usable Parameters," *IEEE Transactions on Computers*, vol. 53, pp. 232-240, 2004.
[16] M. Naor and B. Pinkas, "Oblivious Transfer with Adaptive Queries," in *CRYPTO'99*, 1999, pp. 573-590.
[17] C.-K. Chu and W.-G. Tzeng, "Efficient k-Out-of-n Oblivious Transfer Schemes with Adaptive and Non-adaptive Queries," in *PKC 2005*, 2005, pp. 172-183.
[18] C. L. F. Corniaux and H. Ghodosi, "An Information-Theoretically Secure Threshold Distributed Oblivious Transfer Protocol," in *Information Security and Cryptology - ICISC 2012*, 2013, pp. 184-201.
[19] C. L. F. Corniaux and H. Ghodosi, "A Verifiable 1-out-of-n Distributed Oblivious Transfer Protocol," Cryptology ePrint Archive, Report 2013/063, 2013.
[20] H. Ghodosi, "Analysis of an Unconditionally Secure Distributed Oblivious Transfer," *Journal of Cryptology*, vol. 2013, pp. 75-79, 2013.
[21] C. Blundo, P. D'Arco, A. D. Santis, and D. R. Stinson, "On Unconditionally Secure Distributed Oblivious Transfer," *Journal of Cryptology*, vol. 20, pp. 323-373, 2007.
[22] A. C. Prihandoko, H. Ghodosi, and B. Litow, "Secure and Private Content Distribution in the DRM Environment," in *The 2013 Information System International Conference*, Bali, Indonesia, 2013, pp. 659-664.
[23] A. Shamir, "How to Share a Secret," *Communications of the ACM*, vol. 22, pp. 612-613, 1979.
[24] Z. Chen. (2000). *Java Card Technology for Smart Cards: Architecture and Programmer's Guide*.