ICOMITEE 2021
PROCEEDING

The 2021 International Conference on Computer Science, Information Technology and Electrical Engineering (ICOMITEE)

October
27th – 28th, 2021
El Hotel Royale, Banyuwangi

Co-Host :

Sponsorship :

IEEE INDONESIA SECTION

IEEE The Indonesia Section Computer Society Chapter

PROCEEDINGS

2021 International Conference on Computer Science, Information Technology, and Electrical Engineering (ICOMITEE 2021)

ISBN : 978-1-6654-0146-3 (USB, Part Number: CFP21U07-USB)
ISBN : 978-1-6654-0147-0 (XPLORE COMPLIANT, Part Number: CFP21U07-ART)

Additional copies may be ordered to:
Faculty of Computer Science
University of Jember
Jl. Kalimantan no.37, Kampus Bumi Tegalboto, Sumbersari, Jember, 68121
+62331 - 326935

Organizing Committee of ICOMITEE 2021

Steering Committee

- Iwan Taruna, University of Jember, Jember, Indonesia
- Wahyudi Hasbi, National Institute of Aeronautices & Space (LAPAN), Indonesia
- Ford Lumban Gaol, IEEE Indonesia Section Computer Society Chapter
- Son Kuswadi, Politeknik Negeri Banyuwangi, Banyuwangi, Indonesia
- Slamin, University of Jember, Jember, Indonesia
- Achmad Jazidie, Universitas Nahdlatul Ulama Surabaya, Surabaya, Indonesia
- Gamantyo Hendrantoro, Institut Teknologi Sepuluh Nopember, Surabaya, Indonesia

Conference Chair

- Saiful Bukhori, University of Jember, Jember, Indonesia

Treasurer

- Windi Eka Yulia Retnani, University of Jember, Jember, Indonesia

Technical Program Committee Chairs

- Antonius Cahya Prihandoko, University of Jember, Jember, Indonesia
- Khairul Anam, University of Jember, Jember, Indonesia
- Teguh Herlambang, Universitas Nahdlatul Ulama Surabaya, Surabaya, Indonesia
- Ryan Randi Suryono, Universitas Teknokrat Indonesia, Lampung, Indonesia

Publication Chairs

- Fahrobby Adnan, University of Jember, Jember, Indonesia
- Endang Sulistiyani, Universitas Nahdlatul Ulama Surabaya, Surabaya, Indonesia
- Ima Kurniastuti, Universitas Nahdlatul Ulama Surabaya, Surabaya, Indonesia
- Heni Sulistiani, Universitas Teknokrat Indonesia, Lampung, Indonesia
- Dedi Darwis, Universitas Teknokrat Indonesia, Lampung, Indonesia
- Eka Mistiko Rini, Politeknik Negeri Banyuwangi, Banyuwangi, Indonesia

Publicity and Sponsorship Chairs

- Januar Adi Putra, University of Jember, Jember, Indonesia

Secretary

- Beny Prasetyo, University of Jember, Jember, Indonesia

Technical Program Members

- Sasikumar A, K Ramakrishnan College of Technology, India
- Sharul Kamal A. Rahim, Universiti Teknologi Malaysia, Malaysia
- Ab Al-Hadi Ab Rahman, Universiti Teknologi Malaysia, Malaysia
- Shahliza Abd Halim, University of Technology Malaysia, Malaysia
- Dahlan Abdullah, Universitas Malikussaleh, Indonesia
- Shobit Agarwal, University of Bologna, Italy
- Anita Ahmad, University of Technology Malaysia, Malaysia
- Hani Ahmed, Universiti Malaysia Perlis, Malaysia

- Roselina Sallehuddin, University Technology Malaysia, Malaysia
- Vaibhav Saundarmal, Marathwada Institute of Technology, Aurangabad, India
- Ahmad Zuri Sha'ameri, Universiti Teknologi Malaysia, Malaysia
- Durga Prasad Sharma, AMUIT, MOSHE FDRE under UNDP & Adviser (IT) ILO-UN, India
- Robert Szabolcsi, Óbuda University, Hungary
- Said Touati, Nuclear Center Research Of Birine, Algeria
- Nguyen Tri-Hai, Chung-Ang University, Korea (South)
- Munirul Ula, Universitas Malikussaleh, Indonesia
- Y. V. Pavan Kumar, Vellore Institute of Technology - Andhra Pradesh (VIT-AP) University, India
- Azli Yahya, Universiti Teknologi Malaysia, Malaysia
- Aws Yonis, Ninevah University, Iraq
- Efil Yusrianto, UIN IMAM BONJOL PADANG, Indonesia

Reviewers

- Abu Bakar Abd Rahman, Universiti Malaysia Sabah, Malaysia
- Abdul Abdul, Federal Urdu University of Arts, Science & Technology Islamabad Pakistan, Pakistan
- Sakena Abdul Jabar, Universiti Malaysia Sarawak, Malaysia
- Antar Abdul-Qawy, Faculty of Science, SUMAIT University, Zanzibar, Tanzania
- Nelly Adiwijaya, Universitas Jember, Indonesia
- Sandeep Agrawal, RJIT Tekanpur, India
- Mohd Ashraf Ahmad, Universiti Malaysia Pahang, Malaysia
- Omar Al saif, Northern Technical University, Iraq
- Qusay Al-Doori, University of Technology, Iraq
- Mohammad Al-Mashhadani, Al-Maarif University College, Iraq
- Yahiea Al-Naiemy, Budapest University of Technology and Economics, Hungary
- Karim Al-Saedi, Mustansiriyah University, Iraq
- Atallah AL-Shatnawi, Al-albayt University, Jordan
- Maher Alasaady, Northern Technical University, Iraq
- Hamid Alasadi, IRAQ- BASRA, Iraq
- Mihaela Albu, Politehnica University of Bucharest, Romania
- Qutaiba Ali, University of Mosul, Iraq
- Wisam Ali, University of Technology, Iraq
- Mohammad AlShabi, University of Sharjah, United Arab Emirates
- Ahmed Alsheikhy, Northern Border University, Saudi Arabia
- Ghada Amer, Faculty of Engineering - Benha University, Egypt
- Manilal Amipara, Gujarat Technological University, India
- Khairul Anam, University of Jember, Indonesia
- Rakan Antar, Northern Technical University, Iraq
- Anna Antonyová, University of Prešov in Prešov, Slovakia
- Intan Sari Areni, Hasanuddin University, Indonesia
- Ezendu Ariwa, University of Bedfordshire, United Kingdom (Great Britain)
- Farrukh Arslan, Purdue University, USA
- Carlos Astudillo, State University of Campinas, Brazil
- Irfan Bahiuddin, Universitas Gadjah Mada, Indonesia
- Bakhyt Bakiyev, Suleyman Demirel University, Kazakhstan
- M'hamed Bakrim, University of Cadi Ayyad Marrakesh, Morocco
- Younes Balboul, ENSA, Sidi Mohamed Ben Abdellah University, Morocco
- Maushumi Barooah, Gauhati University, India
- Bikash Behera, International Institute of Information Technology Bhubaneswar, India
- Dinesh Bhatia, Biomedical Engineering Department, North Eastern Hill University, India
- Subhasis Bhattacharjee, Adobe Systems India Private Limited, India
- Parameshachari Bidare Divakarachari, GSSSIETW, Mysuru, India
- Tuğçe Bilen, Istanbul Technical University, Turkey
- Shilpi Birla, Manipal University Jaipur, India

- T Vijay Muni, K L University, India
- Rinaldi Munir, Institut Teknologi Bandung, Indonesia
- Sarhan Musa, Prairie View A&M University, USA
- Mas Rina Mustaffa, Universiti Putra Malaysia, Malaysia
- Marwan Nafea, University of Nottingham Malaysia, Malaysia
- Ali Nahar, University of Technology -Iraq, Malaysia
- Paniti Netinant, Rangsit University, Thailand
- Mohd Natashah Norizan, Universiti Malaysia Perlis, Malaysia
- Nurdin Nurdin, Universitas Islam Negeri (IAIN) Datokarama Palu, Indonesia
- Ahmad Fairuz Omar, Universiti Sains Malaysia, Malaysia
- Nor Azlan Othman, Universiti Teknologi MARA (UiTM) Cawangan Pulau Pinang, Malaysia
- Rosaura Palma-Orozco, Instituto Politécnico Nacional, Mexico
- Shashikant Patil, SVKM NMIMS Mumbai India, India
- Taraknath Paul, ICFAI University Jharkhand, India
- Yesaya Paulus, Dipa Makassar University, Japan
- Vanita Pawar, DIAT, Pune, India
- Rajesh Pindoriya, Indian Institute of Technology Mandi, India
- Petra Poulova, University of Hradec Kralove, Czech Republic
- Eko Prasetyo, PT. PLN (Persero), Indonesia
- Emil Pricop, Petroleum-Gas University of Ploiesti, Romania
- Salita Ulitia Prini, Indonesian Institute of Sciences, Indonesia
- Cong Pu, Marshall University, USA
- Sameerchand Pudaruth, University of Mauritius, Mauritius
- Pakawan Pugsee, Chulalongkorn University, Thailand
- Yogesh Pundlik, Kamala Institute of Technology and Science, Singapur-, India
- Asep Purnomo, Universitas Gadjah Mada, Indonesia
- Fitri Maya Puspita, University of Sriwijaya, Indonesia
- Fika Rachman, University of Trunojoyo Madura, Indonesia
- Ema Rachmawati, Telkom University, Indonesia
- Indra Raharjana, Universitas Airlangga, Indonesia
- Harikumar Rajaguru, Bannari Amman Institute of Technology, India
- Grienggrai Rajchakit, Maejo University, Thailand
- Ramadiani Ramadiani, Mulawarman University, Indonesia
- Shuvendu Rana, SRM University AP, United Kingdom (Great Britain)
- Priya Ranjan, SRM University, Amaravathi, India
- Nadana Ravishankar, VelTech High Tech Dr Rangarajan Dr Sakunthala Engineering College, India
- Windi Retnani, Universitas Jember, Indonesia
- Indra Riyanto, Universitas Indonesia, Indonesia
- Zairi Rizman, Universiti Teknologi MARA, Malaysia
- Nuno Rodrigues, Instituto Politécnico de Bragança, Portugal
- Vahideh Sadeghi, Isfahan University of Technology, Iran
- Ahmed Saeed, Future University in Egypt, Egypt
- Basil Saied, Formerly at University of Mosul, Iraq
- Arun Saini, The ICFAI University, Jaipur, India
- Sandeep Saini, The LNM Institute of Information Technology, Jaipur, India
- Wael Salah, Palestine Technical University - Kadoorie, Palestine
- Hussain Saleem, University of Karachi, Pakistan
- Azmi Saleh, Jember University, Indonesia
- Andrews Samraj, Mahendra Engineering College, India
- Tomonobu Sato, Hitachi ICT Business Services, Ltd., Japan
- Alfredo Satriya, University of Florida, USA
- Toufik Sebbagh, University of Skikda, Algeria
- Sandeep Sengar, Indian Institute of Technology (ISM) Dhanbad, India
- Tomonobu Senjyu, Faculty of Engneering, University of the Ryukyus, Japan
- Amel Serrat, USTO MB, Algeria

Table of Contents

Blind Decryption for Preserving Privacy in the DRM System

Publisher: IEEE

Cite This PDF

Antonius Cahya Prihandoko ; Hossein Ghodosi All Authors

Abstract: This paper addresses the user's privacy problem in the DRM system. Focusing on achieving optimal security for content provider, DRM system often neglect user's privacy. W... **View more**

Metadata

Abstract:
This paper addresses the user's privacy problem in the DRM system. Focusing on achieving optimal security for content provider, DRM system often neglect user's privacy. We propose solutions to this problem in a new perspective: providing balance protection on privacy and security. Preserving user's privacy is approached by minimizing user's data acquisition. The implementation of this privacy protection has to be controlled so that the security of the content provider is preserved. All solutions presented in this paper are based on the blind decryption scheme. To demonstrate the advantages of a blind decryption based solution, we also compared it to an anonymous cash scheme.

Published in: 2021 International Conference on Computer Science, Information Technology, and Electrical Engineering (ICOMITEE)

Date of Conference: 27-28 October 2021

INSPEC Accession Number: 21530382

Date Added to IEEE *Xplore*: 24 December 2021

DOI: 10.1109/ICOMITEE53461.2021.9650123

ISBN Information:

Publisher: IEEE

Conference Location: Banyuwangi, Indonesia

More Like This

Incomplete Cryptography Method Using Invariant Huffman Code Length to Digital Rights Management

2012 IEEE 26th International Conference on Advanced Information Networking and Applications

Published: 2012

Digital Right Management Model Based on Cryptography and Digital Watermarking

2008 International Conference on Computer Science and Software Engineering

Published: 2008

Show More

Contents

I. Introduction

Digital Rights Management (DRM) provides technological approaches for controlling the use and distribution of content so that the copyright of a work can always be protected. In achieving optimal content provider's security protection, however,

DRM system often neglect user's privacy. A standard DRM system for content distribution usually contains four components: content provider, supplier, clearing-house and user [1]. In this system, content provider delivers encrypted item to the supplier and associated usage rules to the clearing-house. This mechanism provides an optimum security for content provider. In order to be able to decrypt the item obtained from the distributor, the user must apply for a license to the clearing-house. However, acquiring license from the clearing-house can cause a privacy problem as information presented by user to the clearinghouse is not warranted to be confidential, thus threaten the user's privacy.

Authors
References
Keywords
Metrics

Blind Decryption for Preserving Privacy in the DRM System

1st Antonius Cahya Prihandoko
Dept. of Information Technology
University of Jember
Jember, Indonesia
antoniuscp.ilkom@unej.ac.id

2nd Hossein Ghodosi
Dept. of Information Technology
James Cook University
Townsville, Australia
hossein.ghodosi@jcu.edu.au

***Abstract*— This paper addresses the user's privacy problem in the DRM system. Focusing on achieving optimal security for content provider, DRM system often neglect user's privacy. We propose solutions to this problem in a new perspective: providing balance protection on privacy and security. Preserving user's privacy is approached by minimizing user's data acquisition. The implementation of this privacy protection has to be controlled so that the security of the content provider is preserved. All solutions presented in this paper are based on the blind decryption scheme. To demonstrate the advantages of a blind decryption based solution, we also compared it to an anonymous cash scheme.**

Keywords—Digital Rights Management, Data Acquisition, Anonymous Cash, Blind Decryption, Blind Signature, Privacy, Security.

I. INTRODUCTION

Digital Rights Management (DRM) provides technological approaches for controlling the use and distribution of content so that the copyright of a work can always be protected. In achieving optimal content provider's security protection, however, DRM system often neglect user's privacy. A standard DRM system for content distribution usually contains four components: content provider, supplier, clearing-house and user [1]. In this system, content provider delivers encrypted item to the supplier and associated usage rules to the clearing-house. This mechanism provides an optimum security for content provider. In order to be able to decrypt the item obtained from the distributor, the user must apply for a license to the clearing-house. However, acquiring license from the clearing-house can cause a privacy problem as information presented by user to the clearing-house is not warranted to be confidential, thus threaten the user's privacy.

A recent proposed mechanism for preserving security and privacy in a digital rights management (DRM) system content distribution was called PrivDRM [2]. Their mechanism enables a buyer purchases digital item and its license without submitting complete personal data and without involving any third parties. Presentation of PrivDRM, however, did not mention how security of content provider would be protected. Another researchers proposed a framework for preserving security and privacy in content distribution systems using Peer-to-Peer (P2P) networks [3]. This framework provides an efficient distribution for big number of content while preserving security and privacy for content provider and consumer, respectively. The framework was claimed to be able to solve the problems of piracy tracing and buyer's anonymity. But, how any violation that can harm content provider's security can be avoided, did not presented in the proposal.

This paper addresses the user's privacy problem in a new perspective: providing a good protection for user's privacy while also preserving security for content provider. Privacy protection is approached by reducing personal data gaining. In this approach, information presented by user would not be associated to the item which the user purchase. This approach is implemented in a controlled manner so that any malevolent action that threaten content provider's security can be avoided. Investigation on minimizing personal data acquisition is based on two methods: Anonymous Cash and Blind Decryption. Both methods do not associate user's identity with the identity of the purchased content at different manners. In the first method, while the purchased item is disclosed to content provider, user's identity is hidden. In the second method, the opposite is true: user's identity is open to content provider and the information of the content is secret. We compare them to find out which method providing better solution for user's privacy problem in DRM system. Anonymous Cash and Blind Decryption are developed based on the Blind Signature protocol [4].

Blind Signature is a protocol that allows one person to get the signature of the other party while the signer does not know what is being signed [4]. This protocol can be explained as follows. Suppose someone, say Bob, requests a signer for signing his document, x. If suitable functions exist, the signing protocol is below.

- Bob applies encryption function E_B to x, and delivers $E_B(x)$ to the signer;
- The signer validates Bob, applies signature S' to $E_B(x)$, and returns $S'(E_B(x))$ to Bob.
- Bob applies decryption function D_B to $S'(E_B(x))$ to get $S'(x)$, and checks whether $S(S'(x)) = x$.

$S'(x)$ is the signer's signature for Bob's document, x.

A scheme that might be used to protect privacy is anonymous cash [5]. Anonymous cash enables user for purchasing an item in which content provider can identify the item but cannot identify the user. Implementation of this scheme involves two protocols; each for purchasing tokens and using the token for requesting content. User purchases tokens non-anonymously so that token seller can debit the

978-1-6654-0147-0/21/$31.00 ©2021 IEEE

user's account. Initially, the user selects x randomly, computes its hash $h(x)$, and encrypts $h(x)$ with encryption function E_B. The user then delivers the signed $E_B(h(x))$ to the token seller. The seller validates the user's signature, signs $E_B(h(x))$ using secret key, S', and charges the user for payment. Finally, the user decrypts $S'(E_B(h(x)))$ with his decryption function D_B to obtain $S'(h(x))$. This signed token is then used by the user to purchase content anonymously. At purchasing content, the user presents the pair $(S'(h(x)), x)$ and the content metadata to a trader. The trader verifies if $S\left(S'(h(x))\right) = h(x)$, and then delivers $S'(h(x))$ and x to the token seller. The token seller verifies the signature, pays the trader, and stores x as a token that has been spent.

A problem that may occur in the Anonymous Cash scheme is double spending. In this scheme, the key used for signing the tokens is assumed to be absolutely confidential, so that no one else can duplicate an authorized token. However, rogue users may use a valid token for more than one transaction. Unfortunately, when a double spending occurs, the user who attempt to do it could be instantly identified only if the trader is online and the token seller examines the token at the same time. Furthermore, implementation of the Anonymous Cash scheme is less efficient and costly [6]. This because the scheme needs two conversation: each for obtaining tokens and purchasing content. The scheme also necessitates at least three private-key computations: each for token seller signing token, establishing the encrypted content request channel, and setting up the encrypted purchasing token conversation. Finally, in this scheme, content provider is required to have a big storage capacity of all content keys. To overcome the weakness of this anonymous cash-based privacy protection scheme, we propose a blind decryption-based privacy protection scheme.

Subsequent sections are outlined as follows. Section II provides several preserving privacy protocols based on the blind decryption scheme. Section III discusses solutions to overcome problems that arise in the implementation of the blind decryption scheme. Section IV provides additional considerations regarding buyer authorization. Lastly, section V closes the entire presentation of the paper with a conclusion.

II. METHODOLOGY

This section presents some blind decryption-based protocols for preserving user's privacy in the DRM system. Compared to the anonymous cash scheme, blind decryption provides more efficient and cheaper implementations. This scheme needs only one protocol for requesting content key. Blind Decryption enables user to ask content provider to decrypt an encrypted content key while the provider cannot figure out which key is being decrypted [7]. To request blind decryption, user utilizes a specific function to make the encrypted content key meaningless to the content provider prior to decryption. After decryption, user applies the related inverse function to make the content key clear to him. By this property, blind decryption provides efficient user's privacy protection in online marketing [8]. In this scheme, user's identity is still presented to enable content provider to charge the user for payment. However, information about the purchased content is hidden from the content provider so that the user's identity will not be associated to the purchased content.

Blind Decryption can be executed both with and without the public key. Two public-key cyptosystems that can be used to support blind decryption-based protocol are RSA and Diffie-Helman ciphers.

A. *Preserving Privacy Protocol with an RSA Key*

Preserving privacy protocol with an RSA key [9] is similar to RSA blind signatures scheme. Suppose *(e,n)* and *(d,p,q)* are the public (encryption) and secret (decryption) keys, respectively. The content key, m, is encrypted to be m^e. All computations are undertaken in modulo n. For obtaining m, a user runs the following protocol.

- The user selects a random number r, calculates $r^e m^e$, and then delivers the result to content provider.
- The provider calculates $(r^e m^e)^d$, and returns the result, rm, to the user.
- The user divides rm by r to get m.

B. *Preserving Privacy Protocol with a Diffie-Helman Key*

Preserving privacy protocol with a Diffie-Hellman key [10] can be presented as follows. Suppose $g^x mod\ p$ and x are the public and private keys. The content key of an item is $m = g^{xy}$, for a particular y. Metadata of the item which is encrypted with key g^{xy} includes g^y. To gain the key g^{xy}, a user executes the following protocol.

- The user opts a number z and finds $z^{-1}\ mod\ q$, where $q = |< g >|$.
- The user calculates g^{yz} and delivers it to the content provider.
- The provider calculates g^{xyz} and returns it to the user.
- The user calculates $(g^{xyz})^{-z}$ to get g^{xy}.

C. *Perseving Privacy Protocol Without Public Keys*

In the protocol without public keys, content provider utilizes two secret numbers, x and x^{-1}, which are exponentially inverses in modulo p, for encrypting and decrypting content key, respectively. Initially, the content key, m, is encrypted and m^x is publicly available. To get the content key, user proceeds the following protocol.

- The user selects random y, and computes y^{-1}.
- The user calculates m^{xy} and requests content provider for decryption.
- The provider implements x^{-1} and sends m^y to the user.
- The user applies y^{-1} to get m.

D. *Acquiring Blind Decryption*

Blind decryption only needs one non-anonymous protocol for purchasing content key. The conversation does not have to be encrypted, but is required to be signed by the user. Acquiring blind decryption can be illustrated as follows. Suppose the content key m is encrypted with the key K and the encrypted key is publicly available. A user who requests for m will blind the encrypted key with his function B and requests content provider for decrypting the blinded encrypted key. The request has to be signed by the user, so that content provider can verify the user and charge the user's account. To prevent double charge for the same decryption, the user adds a time-stamp in the signed request:

["User-name",time-stamp, $B(E_K(m))$].

After validating the user's signature, the provider charges the user's account, decrypts $B(E_K(m))$, and sends $B(m)$ to the user. Finally, the user decrypts $B(m)$ to obtain m.

III. Results and Discussion

All of the previously presented protocols provide a mechanism for getting items. However, in every transaction there must be a payment. Content providers must be able to charge users to pay according to the price of the item, which in real practice generally varies.

In the context of varying price, the anonymous cash scheme may be superior to the blind decryption scheme. Varying price gives no problem for the anonymouse cash protocol. Content providers can ask users to provide tokens according to the price of the purchased item without disturbing the user's privacy because of the anonymity in purchasing content. Even though the purchase of tokens is non-anonymous, the user's identity will not be associated with the item to be purchased. a large number of tokens is not always used to buy expensive items; users can use it to buy cheap items in large quantities. Thus, price variations will not affect the security and privacy in the anonymous cash scenario.

In the blind decryption scheme, item's price is the only clue for content provider to identify the key used decrypting an encrypted content key. Pricing causes no problem when all items have the same price. All blind decryption requests would be charged with the same price. However, if the price of the items varies, the user must notify the content provider about the item's price in order for content provider can select the key utilized for decrypting the content key. As a result, the identity of the item can be known based on its price.

To solve the varying price problem in the blind decryption scheme, we proposed two solutions: one decryption per unit cost and decryption with different valued keys.

A. One Decryption Per Unit Cost

One decryption per unit cost is the trivial solution for the varying prices and privacy problem. For an item worth n units, its content key, m, is divided into n pieces of m_i, where $1 \leq i \leq n$, such that $m = m_1 \oplus m_2 \oplus \ldots \oplus m_n$. Each piece is valued of 1 unit and is scrambled with key K to be $E_K(m_i)$, for $1 \leq i \leq n$.

Prior to blind decryption requests for m, user disguises encrypted key using function B, and then asks the content provider to execute n decryption, each for $B(E_K(m_i))$, where $1 \leq i \leq n$. The user will be charged for 1 unit for each decryption. Finally, the user decrypts each $B(m_i)$ with B^{-1} to obtain m_i, and combines all shares to get m.

Adding up all decryption requests allows content providers to know the price of an item. To prevent this reveal, the user can submit a blind decryption request at different times for different items [6]. This tactic will obscure the number of decrypted shares; or reduce the likelihood of the price of the item being recognizable.

B. Decryption with Different Valued Keys

Requesting n decryptions for purchasing an item worth n units creates a burden of $n-1$ additional computations. This burden can be helped by applying diverse keys for diverse category of units [6]. Content key can be shared in a certain method to achieve decryption efficiency. Suppose there are three keys: K_1, K_2, and K_3, each with a value of 1, 10 and 100, respectively. For an item worth 123 units, for example, its content key could be divided into six shares and the metadata can be listed as follows.

$$(unit = 100, E_{K_3}(m_1))$$
$$(unit = 10, E_{K_2}(m_2))$$
$$(unit = 10, E_{K_2}(m_3))$$
$$(unit = 1, E_{K_1}(m_4))$$
$$(unit = 1, E_{K_1}(m_5))$$
$$(unit = 1, E_{K_1}(m_6))$$

In this circumstance, content provider should have a single key for a specific denomination, so that all content keys in one denomination can be scrambled with the same key. To get the content key, user sends content provider six signed blind decryptions requests:

$$\text{["User-name",time-stamp,}B\left(E_{K_3}(m_1)\right), unit = 100]$$
$$\text{["User-name",time-stamp,}B\left(E_{K_3}(m_1)\right), unit = 10]$$
$$\text{["User-name",time-stamp,}B\left(E_{K_3}(m_1)\right), unit = 10]$$
$$\text{["User-name",time-stamp,}B\left(E_{K_3}(m_1)\right), unit = 1]$$
$$\text{["User-name",time-stamp,}B\left(E_{K_3}(m_1)\right), unit = 1]$$
$$\text{["User-name",time-stamp,}B\left(E_{K_3}(m_1)\right), unit = 1]$$

The user has to submit the decryption requests over different times to make the item's price remains unrevealed.

To preserve privacy, content provider can split m in various ways. For an item worth 34 units, for instance, the key m may be split into $m_1, m_2, \ldots, m_{34}$ each of which is worth 1 unit; m may also be split into $m_1, m_2, \ldots, m_7$, where m_1, m_2, m_3 are each worth 10 units and m_4, m_5, m_6, m_7 are each worth 1 unit. With these alternatives, user can choose in which way the provider decrypts m. The more decryption options, the better user's privacy protection.

C. Varying Price Versus Privacy Problem

Though requesting the decryptions over different times can minimize the possibility of disclosing content information, this strategy is time expending. Moreover, separate decryption needs additional operations for content provider. In the provider's perspective, the scheme with the least decryption is the best choice scheme. How could it be that a user can apply for a decryption once while the information about the item is not exposed?

One time decryption for all unit is applicable when content provider utilizes a single key for all encryption-decryption process. However, in this condition, varying prices creates a debiting issue. Suppose content provider utilizes RSA cipher with the pair of public and private keys, (e, d). For a content valued t units, its content's key m is divided into t pieces, $m_1, m_2, \ldots, m_t$ so that $m = m_1 . m_2 \ldots m_t$. Every pieces is valued 1 unit and is encrypted disjointely. To get m, instead of asking for decryption for each piece, user multiplies all encrypted pieces and computes $b = r^e . (m_1^e . m_2^e \ldots m_t^e)$ for a random number r. For any value of t, b can always be decrypted using d, and the user can successfully obtain m. However, without information on t, content provider is unable to figure out how much the user has to pay.

Similar issue can also be happen in a symmetric scheme. Suppose K is the key used by content provider to encrypt

content key. The content key m can be divided into t pieces: $m_1, m_2, \dots, m_t$ such that $m = m_1 \oplus m_2 \oplus \dots \oplus m_t$. Every piece is then encrypted disjointely. For obtaining m, user calculates $b = r \oplus (E_K(m_1) \oplus E_K(m_2) \oplus \dots \oplus E_K(m_t))$, where r is a random binary number, and requests for decrypting b. The content provider then decrypts b with E_K. The user will successfully obtain m by calculating $m = r \oplus E_K(b)$. In this case, t has to be odd. Otherwise, m will be disclosed when user calculates $\oplus_{i=1}^{t} E_K(m_i)$. Again, in this situation, content provider is unable to determine how much amount must be charged to the user.

Based on the analysis of some of the cases mentioned previously, in order for blind encryption can be requested once without being affected by pricing and privacy problem, we recommend that the following conditions should be met.

- For all items having the same price, their content keys must be encrypted with the same key; knowing price enables content provider to specify the key which must be used for decrypting the content key.
- A set of items with the same price should contain many elements so the content provider can figure out which set an item belongs to, but cannot identify which item it is.
- The price of an item should not straightaway reflect the class of the item. For instance, G-rated item may be cheaper that X-rated one. Content providers can pack multiple g-rated items in a package that costs the same as an X-rated item. Thus, users who apply for high-priced decryption do not necessarily buy X-rated items.

IV. Additional Consideration

Buyer authorization is another aspect to consider in a business deal. For instance, an item may only be allowed to be purchased by buyers from a particular organization, or citizens of certain countries, and so on. Therefore, content providers need to confirm whether a buyer meets the requirements to purchase a particular item. To be able to purchase restricted items, the user must first obtain the appropriate authorization certificate (Ac). An authorization certificate is a triple $(A_{ID}, A_{ATR}, A_{EXP})$ which indicates registration number, authorization attribute, and certificate usage limit, respectively. Of course, requesting a certificate have to be non anonymously.

After information of a user is validated, content provider will issue two copies of a signed authorization certificate $(Sign_K(Ac))$. The first copy is saved by the content provider and will be updated every time the certificate is used. The second is delivered to the user. Every time the user uses the certificate, it will be matched to one stored by the content provider. If A_{EXP} refers to the number of purchases, A_{EXP} will be reduced by 1 in every transaction. In the following two sub sections, we provide the implementation of authorization certificates both for Blind Decryption and Anonymous Cash schemes, and compare them.

Buyer authorization may not work in the anonymous cash scheme as user purchasing content anonymously. Although user may submit tokens together with an appropriate authorization certificate, but it is hard to verify that the user is the valid certificate holder. An approach to avoid certificate sharing is by integrating anonymous cash in the blind decryption scenario. For example, content key m is divided into two pieces m_0 and m_1, where one of these pieces, say m_1, corresponds to an authorization attribute. Users may utilize anonymous cash to purchase m_0 and request blind decryption to obtain m_1 and m_2. This scenario works as decryption on encrypted pieces can be requested disjointely.

An authorization certificate for Blind Decryption has a particular form. The A_{ID} section is a combination of the registration number and the user account. When the certificate is presented for purchasing item, the corresponding account will be debited This mechanism prevents users to share their certificate to unauthorized persons.

We provide an illustration to clarify the implementation of authorization certificates in the Blind Decryption scheme,. Suppose buyers of an item valued of 111 units are required to be an IEEE student member. The item's key, m, could be divided into 3 pieces m_0, m_1, m_2, such that $m = m_0 \oplus m_1 \oplus m_2$. The pieces m_0, m_1 and m_2 are then encrypted with keys K_0 which is worth 100 units, K_1worth 10 units, and K_2worth 1 unit, respectively. The item's meta data contains three encrypted pieces and two authorization attributes:

$$\left(unit = 111, E_{K_0}(m_0), E_{K_1}(m_1), E_{K_2}(m_2), \text{"stu"}, \text{"}IEEE\text{"}\right)$$

If a user has A_{c_1} and A_{c_2} with "student" and "IEEE member" attributes, respectively, then the user is permitted to buy such item. The user can submit three signed decryption requests below separately.

["User",time-stamp,$B(E_{K_0}(m_0)$, unit=111]
["User",time-stamp,$B(E_{K_1}(m_1), Sign_K(Ac_1)]$
["User",time-stamp,$B(E_{K_2}(m_2), Sign_K(Ac_2)]$

If items' pricing follows our recommendations described in sub section III-C and there are many items for each requirement, content provider will not know the identity of the purchased item. Thus, the system protects user privacy perfectly. On the other hand, this mechanism also prevents user for sharing the certificate to others; this will deter unauthorized buyers and thus, preserve content provider's security.

V. Conclusion

Schemes for preserving user's privacy enable user to purchase item in which user's ID would not be associated with the purchased item. Anonymous cash scheme may perfectly protect user's privacy as user can buy item anonymously. However, there is a double spending issue in this scheme that potentially compromises the security of the content provider. Furthermore, implementation of this scheme is less efficient and costly.

Blind decryption has more efficient and cheaper implementations. Although varying prices can cause privacy issue in this scheme, we provided a guideline to overcome the problem. Furthermore, when buyer authorization is required, this scheme provides compatible protocols that perfectly prevent unauthorized buyers.

In general, the Blind Decryption scheme is superior to the Anonymous Cash scheme in terms of efficiency, cost and implementation of the buyer's authorization. Only in one aspect, namely price variations, the Blind Decryption scheme is weaker than the Anonymous Cash scheme. Nevertheless,

we have provided a solution to solve the problem of this aspect on the Blind Decryption scheme.

REFERENCES

[1] Q. Liu, R. Safavi-Naini, and N. P. Sheppard, "Digital rights management for content distribution," *Proc. Australas. Inf. Secur. Work. Conf. {ACSW} Front. 2003 - Vol. 21*, vol. 21, pp. 49–58, 2003.

[2] T. Gaber, A. Ahmed, and A. Mostafa, "PrivDRM: A Privacy-preserving Secure Digital Right Management System," *ACM Int. Conf. Proceeding Ser.*, pp. 481–486, 2020, doi: 10.1145/3383219.3383289.

[3] A. Qureshi, D. Megías, and H. Rifà-Pous, "Framework for preserving security and privacy in peer-to-peer content distribution systems," *Expert Syst. Appl.*, vol. 42, no. 3, pp. 1391–1408, 2015, doi: 10.1016/j.eswa.2014.08.053.

[4] D. Chaum, "Blind Signatures for Untraceable Payments," *Crypto*, vol. 82. pp. 199–203, 1982, doi: 10.1016/j.ins.2004.10.010.

[5] D. Chaum, A. Fiat, and M. Naor, "Untraceable Electronic Cash," *Adv. Cryptol.*, vol. LNCS 403, pp. 319–327, 1990.

[6] R. Perlman, C. Kaufman, and R. Perlner, "Privacy-preserving DRM," *Proc. 9th Symp. Identity Trust Internet - IDTRUST '10*, p. 69, 2010, doi: 10.1145/1750389.1750399.

[7] R. Perlman, "The Ephemerizer : Making Data Disappear," 2005.

[8] M. Al-Fayoumi and S. Aboud, "Blind Decryption and Privacy Protection," *Am. J. Appl. Sci.*, vol. 2, no. 4, pp. 873–876, 2005.

[9] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, 1978, doi: 10.1145/359340.359342.

[10] W. Diffie and M. E. Hellman, "New Directions in Cryptography," *IEEE Trans. Inf. Theory*, vol. 22, no. 6, pp. 644–654, 1976, doi: 10.1109/TIT.1976.1055638.

This author profile is generated by Scopus Learn more

Prihandoko, Antonius Cahya

Universitas Jember, Jember, Indonesia

https://orcid.org/0000-0001-7112-5458

Edit profile | Set alert | Save to list | Potential author matches

Export to SciVal

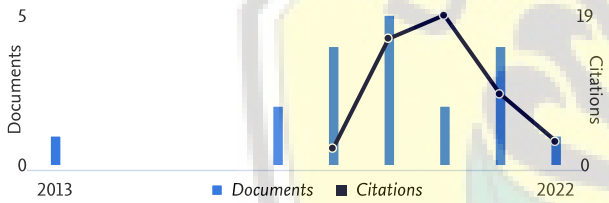
Metrics overview

19
Documents by author

49
Citations by **40** documents

3
h-index: View *h*-graph

Document & citation trends



Most contributed Topics 2016–2020

Lesson Study; Initial Teacher Education; Professional Development
5 documents

Reverse Engineering; Watermarking; Computer Crime
2 documents

Visual Cryptography; Secret Sharing Scheme; Access Structure
1 document

View all Topics

19 Documents | Cited by 40 Documents | 0 Preprints | 37 Co-Authors | 8 Topics
0 Awarded Grants

Beta

Note:
Scopus Preview users can only view an author's last 10 documents, while most other features are disabled. Do you have access through your institution? Check your institution's access to view all documents and features.

Export all | Save all to list | Sort by Date (...

View list in search results format

View references

Set document alert

Article • *Open access*

Stream-keys generation based on graph labeling for strengthening Vigenere encryption

0
Citations

Prihandoko, A.C., Dafik, Agustin, I.H.

International Journal of Electrical and Computer Engineering, 2022, 12(4), pp. 3960–3969

Show abstract | Related documents

Conference Paper • *Open access*

Developing of learning tools based on science, technology, engineering, and mathematics (STEM) based on learning community to improve critical thinking ability in class X student's arithmetic sequences and arithmetic materials

1 Citations

Insani, K., Hobri, Prihandoko, A.C., Sa'id, I.A., Safik, M.

Journal of Physics: Conference Series, 2021, 1839(1), 012020

Show abstract Related documents

Conference Paper • *Open access*

Development of mathematics e-module with STEM-collaborative project based learning to improve mathematical literacy ability of vocational high school students

0 Citations

Hadiyanti, N.F.D., Hobri, Prihandoko, A.C., ...Khasanah, N., Maharani, P.

Journal of Physics: Conference Series, 2021, 1839(1), 012031

Show abstract Related documents

Conference Paper

Blind Decryption for Preserving Privacy in the DRM System

0 Citations

Prihandoko, A.C., Ghodosi, H.

2021 International Conference on Computer Science, Information Technology, and Electrical Engineering, ICOMITEE 2021, 2021, pp. 213–217

Show abstract Related documents

Article

On the resolving strong domination number of corona and cartesian product of graphs

0 Citations

Dafik, Agustin, I.H., Prihandoko, A.C., ...Nisviasari, R., Mohanapriya, N.

Palestine Journal of Mathematics, 2021, 10(Special Issue II), pp. 169–177

Show abstract Related documents

Conference Paper • *Open access*

The students' mathematical communication skill on caring community-based learning cycle 5E

1 Citations

Aini, K., Hobri, Prihandoko, A.C., ...Faozi, A.K.A., Asmoni

Journal of Physics: Conference Series, 2020, 1538(1), 012075

Show abstract Related documents

Conference Paper • *Open access*

The analyze of students' creative thinking skills on Lesson Study for Learning Community (LSLC) based on Science, Technology, Engineering, and Mathematics (STEM) approach

0 Citations

Yuniar, D., Hobri, Prihandoko, A.C., Aini, K., Faozi, A.K.A.

Journal of Physics: Conference Series, 2020, 1538(1), 012072

Show abstract Related documents

Conference Paper

Flaws in Strong t-Consistency

0 Citations

Cianciullo, L., Ghodosi, H., Thuremilla, K., Prihandoko, A.C.

Proceedings - 2019 International Conference on Computer Science, Information Technology, and Electrical Engineering, ICOMITEE 2019, 2019, pp. 118–122, 8921313

Show abstract Related documents

Conference Paper • *Open access*

Development of mathematical learning tools through discovery learning based on lesson study for learning community and their influence with students' problem solving

2 Citations

Trawikhi, A., Hobri, Prihandoko, A.C., Utomo, B.T.

Journal of Physics: Conference Series, 2019, 1211(1), 012082

Show abstract Related documents

Conference Paper • *Open access*

Students' creative thinking process in completing mathematical PISA test concerning space and shape

2
Citations

Leksmono, A., Sunardi, Prihandoko, A.C., Murtikusuma, R.P.

Journal of Physics: Conference Series, 2019, 1211(1), 012073

Show abstract Related documents

Back to top

About Scopus

What is Scopus

Content coverage

Scopus blog

Scopus API

Privacy matters

Language

日本語版を表示する

查看简体中文版本

查看繁體中文版本

Просмотр версии на русском языке

Customer Service

Help

Tutorials

Contact us

ELSEVIER

ICOMITEE
2021