Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2018.Doc Number

Efficient Anonymous Certificateless Multi-Receiver Signcryption Scheme without Bilinear Pairings

Liaojun Pang[1,2], Member, IEEE, Man Kou[1], Mengmeng Wei[1], and Huixian Li[3]

[1]State Key Lab. of Integrated Services Networks, School of Life Science and Technology, Xidian Univ., Xi'an, 710071, China
[2]Dept. of Comput. Sci., Wayne State University, MI 48202, USA.
[3]School of Computer Science and Engineering, Northwestern Polytechnical Univ., Xi'an, 710072, China

Corresponding authors: Liaojun Pang(e-mail: liaojun.pang@wayne.edu) and Huixian Li(e-mail: lihuixian@nwpu.edu.cn).

ABSTRACT Certificateless multi-receiver encryption/signcryption (CLME/CLMS) has become a research hotspot in the field of information security. Almost all of the existing CLME/CLMS schemes are constructed based on the bilinear pairing computation, a time-consuming operation, which makes their computational efficiency relatively low. Although there are some CLME schemes constructed on scalar point multiplications on elliptic curve cryptography (ECC) instead of the bilinear pairing computation, too many scalar point multiplications involved still lead to the low computational efficiency. Therefore, there is still room for CLME/CLMS schemes in efficiency. Motivated by these concerns, an efficient anonymous certificateless multi-receiver signcryption scheme is proposed with its security proved under the random oracle model. The proposed scheme is improved largely in computational efficiency by the idea that it is designed based on scalar point multiplications on ECC instead of the bilinear pairing and the number of scalar point multiplications on ECC is reduced as small as possible.

INDEX TERMS Certificateless cryptography; Computational efficiency; Elliptic curve cryptography; Multi-receiver signcryption.

I. INTRODUCTION

Multi-receiver encryption/signcryption has been considered as an effective and promising way to achieve one-to-many secure communication. The first identity-based multi-receiver encryption (MIBE) scheme was brought forward by Baek *et al.* [1] in 2005. Afterwards, in order to ensure the ciphertext's validity, combining MIBE with Zheng's signcryption [2], Duan *et al.* [3] proposed the first multi-receiver identity-based signcryption (MIBS) scheme and gave the unforgeability security model at the same time. Since then, a large number of MIBS schemes [4]-[9], which are suitable for network conferences, paid-TV system and ad-hoc networks, have been proposed.

With the penetration of the Internet in all aspects of our daily life, people are increasingly focusing on their own privacy. For example, when watching a paid-TV program, people may not want others to know the specific program that they are watching, which belongs to their own privacy. Based on this practical need, introducing the receiver anonymity to MIBE, Fan *et al.* [10] put forward the first anonymous MIBE scheme by utilizing Lagrange interpolating polynomial. Unfortunately, both Wang *et al.* [11] and Chien [12] later prove that Fan *et al.*'s scheme fails to achieve the receiver anonymity as they have claimed. Afterwards, a new anonymous MIBS scheme was proposed by Pang *et al.* [13], in which the concept of decryption fairness is used to describe the characterization and enhancement of the receiver anonymity, but the receiver anonymity is not achieved due to the use of Lagrange interpolating polynomial, either. To truly achieve the receiver anonymity, in 2014, Tseng *et al.* [14] proposed another anonymous MIBE scheme, in which the receiver anonymity is realized by a modular large prime polynomial and the method is considered as one of the most effective ways to achieve the receiver anonymity so far. Nevertheless, there exits the terrible phenomenon that the number of the involved bilinear pairing operations grows linearly with the number of receivers in Tseng *et al.*'s scheme, which leads to it extremely low in computational efficiency. To further improve efficiency, security and performance, there are a few

Efficient Certificateless Anonymous Multi Receiver

Xingming Sun,Han-Chieh Chao,Xingang You,Elisa Bertino

Efficient Certificateless Anonymous Multi Receiver:

Algorithms and Architectures for Parallel Processing Sheng Wen,Albert Zomaya,Laurence T. Yang,2020-01-21 The two volume set LNCS 11944 11945 constitutes the proceedings of the 19th International Conference on Algorithms and Architectures for Parallel Processing ICA3PP 2019 held in Melbourne Australia in December 2019 The 73 full and 29 short papers presented were carefully reviewed and selected from 251 submissions The papers are organized in topical sections on Parallel and Distributed Architectures Software Systems and Programming Models Distributed and Parallel and Network based Computing Big Data and its Applications Distributed and Parallel Algorithms Applications of Distributed and Parallel Computing Service Dependability and Security IoT and CPS Computing Performance Modelling and Evaluation *Security and Privacy* Sihem Mesnager,Pantelimon Stănică,Kamalesh Acharya,Sumit Kumar Debnath,2025-12-01 This book constitutes the conference proceedings of the 4th International Conference on Security and Privacy ICSP 2025 held in Rourkela India during December 5 7 2025 The 14 full papers in this book were carefully reviewed and selected from 52 submissions They were organized in topical sections as follows Mathematical Foundation of Cryptography Authentication Key Management and Machine Learning in Cybersecurity **The 8th International Conference on Information Science, Communication and Computing** Yanfeng Wang,Yang Xiao,Zhiqiang Wu,Yuan Tian,2025-02-13 This conference proceedings is a collection of the accepted papers of ISCC2024 the 8th International Conference on Information Science Communication and Computing held in Zhengzhou China 23 25 August 2024 The topics focus on intelligent information science and technology artificial intelligence and intelligent systems cloud computing and big data smart computing and communication technology wireless network and cyber security Each part can be used as an excellent reference by industry practitioners university faculties research fellows and undergraduate and graduate students who need to build a knowledge base of the latest advances and state of the practice in the topics covered by these conference proceedings This will enable them to build maintain and manage systems of high reliability and complexity We would like to thank the authors for their hard work and dedication and the reviewers for ensuring that only the highest quality papers were selected **Cloud Computing and Security** Xingming Sun,Han-Chieh Chao,Xingang You,Elisa Bertino,2017-10-31 This two volume set LNCS 10602 and LNCS 10603 constitutes the thoroughly refereed post conference proceedings of the Third International Conference on Cloud Computing and Security ICCCS 2017 held in Nanjing China in June 2017 The 116 full papers and 11 short papers of these volumes were carefully reviewed and selected from 391 submissions The papers are organized in topical sections such as information hiding cloud computing IOT applications information security multimedia applications optimization and classification

Thank you very much for reading **Efficient Certificateless Anonymous Multi Receiver**. Maybe you have knowledge that, people have look numerous times for their chosen novels like this Efficient Certificateless Anonymous Multi Receiver, but end up in harmful downloads.
Rather than enjoying a good book with a cup of tea in the afternoon, instead they cope with some malicious bugs inside their desktop computer.

Efficient Certificateless Anonymous Multi Receiver is available in our digital library an online access to it is set as public so you can download it instantly.
Our books collection spans in multiple locations, allowing you to get the most less latency time to download any of our books like this one.
Kindly say, the Efficient Certificateless Anonymous Multi Receiver is universally compatible with any devices to read

https://matrix.jamesarcher.co/results/Resources/HomePages/Microeconomics_8th_Edition_Pindyck_Solutions_Manual_Ch8.pdf

Table of Contents Efficient Certificateless Anonymous Multi Receiver

Efficient Certificateless Anonymous Multi Receiver Introduction

Free PDF Books and Manuals for Download: Unlocking Knowledge at Your Fingertips In todays fast-paced digital age, obtaining valuable knowledge has become easier than ever. Thanks to the internet, a vast array of books and manuals are now available for free download in PDF format. Whether you are a student, professional, or simply an avid reader, this treasure trove of downloadable resources offers a wealth of information, conveniently accessible anytime, anywhere. The advent of online libraries and platforms dedicated to sharing knowledge has revolutionized the way we consume information. No longer confined to physical libraries or bookstores, readers can now access an extensive collection of digital books and manuals with just a few clicks. These resources, available in PDF, Microsoft Word, and PowerPoint formats, cater to a wide range of interests, including literature, technology, science, history, and much more. One notable platform where you can explore and download free Efficient Certificateless Anonymous Multi Receiver PDF books and manuals is the internets largest free library. Hosted online, this catalog compiles a vast assortment of documents, making it a veritable goldmine of knowledge. With its easy-to-use website interface and customizable PDF generator, this platform offers a user-friendly experience, allowing individuals to effortlessly navigate and access the information they seek. The availability of free PDF books and manuals on this platform demonstrates its commitment to democratizing education and empowering individuals with the tools needed to succeed in their chosen fields. It allows anyone, regardless of their background or financial limitations, to expand their horizons and gain insights from experts in various disciplines. One of the most significant advantages of downloading PDF books and manuals lies in their portability. Unlike physical copies, digital books can be stored and carried on a single device, such as a tablet or smartphone, saving valuable space and weight. This convenience makes it possible for readers to have their entire library at their fingertips, whether they are commuting, traveling, or simply enjoying a lazy afternoon at home. Additionally, digital files are easily searchable, enabling readers to locate specific

information within seconds. With a few keystrokes, users can search for keywords, topics, or phrases, making research and finding relevant information a breeze. This efficiency saves time and effort, streamlining the learning process and allowing individuals to focus on extracting the information they need. Furthermore, the availability of free PDF books and manuals fosters a culture of continuous learning. By removing financial barriers, more people can access educational resources and pursue lifelong learning, contributing to personal growth and professional development. This democratization of knowledge promotes intellectual curiosity and empowers individuals to become lifelong learners, promoting progress and innovation in various fields. It is worth noting that while accessing free Efficient Certificateless Anonymous Multi Receiver PDF books and manuals is convenient and cost-effective, it is vital to respect copyright laws and intellectual property rights. Platforms offering free downloads often operate within legal boundaries, ensuring that the materials they provide are either in the public domain or authorized for distribution. By adhering to copyright laws, users can enjoy the benefits of free access to knowledge while supporting the authors and publishers who make these resources available. In conclusion, the availability of Efficient Certificateless Anonymous Multi Receiver free PDF books and manuals for download has revolutionized the way we access and consume knowledge. With just a few clicks, individuals can explore a vast collection of resources across different disciplines, all free of charge. This accessibility empowers individuals to become lifelong learners, contributing to personal growth, professional development, and the advancement of society as a whole. So why not unlock a world of knowledge today? Start exploring the vast sea of free PDF books and manuals waiting to be discovered right at your fingertips.

FAQs About Efficient Certificateless Anonymous Multi Receiver Books

How do I know which eBook platform is the best for me? Finding the best eBook platform depends on your reading preferences and device compatibility. Research different platforms, read user reviews, and explore their features before making a choice. Are free eBooks of good quality? Yes, many reputable platforms offer high-quality free eBooks, including classics and public domain works. However, make sure to verify the source to ensure the eBook credibility. Can I read eBooks without an eReader? Absolutely! Most eBook platforms offer web-based readers or mobile apps that allow you to read eBooks on your computer, tablet, or smartphone. How do I avoid digital eye strain while reading eBooks? To prevent digital eye strain, take regular breaks, adjust the font size and background color, and ensure proper lighting while reading eBooks. What the advantage of interactive eBooks? Interactive eBooks incorporate multimedia elements, quizzes, and activities, enhancing the reader engagement and providing a more immersive learning experience. Efficient Certificateless Anonymous Multi Receiver is one of the best book in our library for free trial. We provide copy of Efficient Certificateless Anonymous Multi Receiver in digital format, so the resources that you find are reliable. There are also many Ebooks of related with

Efficient Certificateless Anonymous Multi Receiver. Where to download Efficient Certificateless Anonymous Multi Receiver online for free? Are you looking for Efficient Certificateless Anonymous Multi Receiver PDF? This is definitely going to save you time and cash in something you should think about.

Find Efficient Certificateless Anonymous Multi Receiver :

microeconomics 8th edition pindyck solutions manual ch8
mifano ya tanakali za sauti
mike rashid complete overtraining torrent
modern automotive technology chapter 1 autotechl
mechanical vibrations rao 4th edition
microsoft onenote step by step
mind the gap business studies study guide grade 12 pdf
mfm prayer points
mittle vn basic electrical engineering download
~~mercedes w202 workshop manual download~~
medical equipment maintenance management and oversight synthesis lectures on biomedical engineering
microwave engineering notes
~~mitsubishi lancer 2003 service repair manual pdf download~~
melodic dictation melodies using m2 m2 m3 m3 p4 p5
mechanical operations by anup k swain g k roy hemlata

Efficient Certificateless Anonymous Multi Receiver :

American Insurgents, American Patriots: The... by Breen, T. H. Challenging and displacing decades of received wisdom, T. H. Breen's strikingly original book explains how ordinary Americans—most of them members of farm ... American Insurgents, American Patriots Apr 13, 2016 — In 1774 a popular insurgency, led by “ordinary Americans” and organized into local committees of safety, was sweeping the 13 colonies. American Insurgents, American Patriots Breen's strikingly original book explains how ordinary Americans—most of them members of farm families living in small communities—were drawn into a successful ... T.H. Breen. American Insurgents, American Patriots In American Insurgents, American Patriots: The Revolution of the People he argues that “ordinary” men and women fueled the Revolution and pressured leaders to. American

insurgents, American patriots : the revolution of the ... American insurgents, American patriots : the revolution of the people / T.H. Breen. ; ISBN: 0809075881 (hardcover : alk. paper) ; ISBN: 9780809075881 (hardcover : ... American Insurgents, American Patriots by T. H. Breen - Ebook This is the compelling story of our national political origins that most Americans do not know. It is a story of rumor, charity, vengeance, and restraint. American Insurgents, American Patriots: The Revolution of ... Breen's strikingly original book explains how ordinary Americans—most of them members of farm families living in small communities—were drawn into a successful ... American Insurgents American Patriots The Revolution of ... This is the compelling story of our national political origins that most Americans do not know. It is a story of rumor, charity, vengeance, and restraint. American Insurgents, American Patriots: The Revolution of ... May 10, 2011 — American Insurgents, American Patriots: The Revolution of the People ; Publisher Hill and Wang ; Publication Date 2011-05-10 ; Section US History. American Insurgents, American Patriots: The Revolution of ... American Insurgents, American Patriots: The Revolution of the People by Breen, T. H. - ISBN 10: 0809075881 - ISBN 13: 9780809075881 - Hill and Wang - 2010 ... Psychiatry.org - DSM by APA Join — The Diagnostic and Statistical Manual of Mental Disorders, Fifth Edition, Text Revision (DSM-5-TR) features the most current text updates based on ... Diagnostic and statistical manual of mental disorders : DSM-5 by F EDITION · Cited by 5556 — The correct citation for this book is American Psychiatric Association: Diagnostic and Statisti- cal Manual of Mental Disorders, Fifth Edition. Arlington, VA, ... Diagnostic and Statistical Manual of Mental Disorders The DSM-5® is out of print and available as PDF-only. For the updated DSM-5-TR®, please visit dsm.psychiatryonline.org. DSM-5: What It Is & What It Diagnoses Oct 14, 2022 — The Diagnostic and Statistical Manual of Mental Illnesses, or DSM-5, is the American Psychiatric Association's professional guide to mental ... DSM - Diagnostic and Statistical Manual of Mental Disorders The Diagnostic and Statistical Manual of Mental Disorders, Fifth Edition, Text Revision (DSM-5-TR), is the most comprehensive, current, and critical ... DSM-5 The Diagnostic and Statistical Manual of Mental Disorders, Fifth Edition (DSM-5), is the 2013 update to the Diagnostic and Statistical Manual of Mental ... Diagnostic and statistical manual of mental disorders: DSM ... The American Psychiatric Association's Diagnostic and Statistical Manual of Mental Disorders (DSM) is a classification of mental disorders with associated ... Diagnostic and Statistical Manual of Mental Disorders Fifth ... The Diagnostic and Statistical Manual of Mental Disorders, Fifth Edition, Text Revision (DSM-5-TR), is the most comprehensive, current, and critical resource ... Diagnostic and Statistical Manual of Mental Disorders (5th ... The American Psychiatric Association's "Diagnostic and Statistical Manual of Mental Disorders" (DSM-5) is used to diagnose and classify mental disorders. Diagnostic and Statistical Manual of Mental Disorders, Text ... The Diagnostic and Statistical Manual of Mental Disorders, Fifth Edition, Text Revision (DSM-5-TR), is the most comprehensive, current, and critical ... The Norton Sampler: Short Essays for Composition (Eighth ... A trusted collection of short essays arranged by rhetorical mode—with charming, practical writing instruction. With 71 readings (half new to this edition), ... The Norton Sampler | Thomas Cooley Short, diverse essays that spark students'

interest—now with more reading support., The Norton Sampler, Thomas Cooley, 9780393537123. The Norton Sampler: Short Essays for Composition ... A trusted collection of short essays arranged by rhetorical mode—with charming, practical writing instruction. The Norton Sampler: Short Essays for Composition (Eighth ... This new edition shows students thatdescription, narration, and the other patterns of exposition are notjust abstract concepts used in composition classrooms ... The Norton Sampler: Short Essays for Composition (Eighth ... The Norton Sampler: Short Essays for Composition (Eighth Edition) ; ISBN: 0393919463 ; Authors: Cooley, Thomas ; Edition: Eighth ; Publisher: W. W. Norton & Company ... The Norton Sampler: Short Essays for Composition (Eighth ... The Norton Sampler: Short Essays for Composition (Eighth Edition) - satisfaction guaranteed. Give this Used Book by Cooley, Thomas a good home. 8th edition. The Norton Sampler: Short Essays for Composition (Eighth ... The Norton Sampler: Short Essays for Composition (Eighth Edition) - VERY GOOD ; Item Number. 274336187371 ; Brand. Unbranded ; MPN. Does not apply ; Accurate ... The Norton Sampler: Short Essays for Composition A trusted collection of short essays arranged by rhetorical mode—with charming, practical writing instruction. With 71 readings (half new to this edition), ... The Norton Sampler: Short Essays for Composition Eighth ... The Norton Sampler: Short Essays for Composition Eighth Edition , Pre-Owned Paperback 0393919463 9780393919462 Thomas Cooley · How you'll get this item: · About ... The Norton Sampler Short Essays for Composition | Buy Edition: 8th edition ; ISBN-13: 978-0393919462 ; Format: Paperback/softback ; Publisher: WW Norton - College (2/1/2013) ; Dimensions: 5.9 x 7.9 x 1 inches.