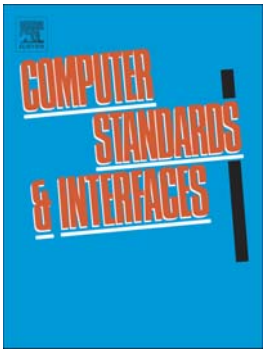


# Pairing-based CP-ABE with constant-size ciphertexts and secret keys for cloud environment

Vanga Odelu, Ashok Kumar Das, Y. Sreenivasa Rao, Saru Kumari, Muhammad Khurram Khan, Kim-Kwang Raymond Choo

PII: S0920-5489(16)30036-8
DOI: doi: 10.1016/j.csi.2016.05.002
Reference: CSI 3111

To appear in: *Computer Standards & Interfaces*

Received date: 21 January 2016
Revised date: 25 March 2016
Accepted date: 14 May 2016

Please cite this article as: Vanga Odelu, Ashok Kumar Das, Y. Sreenivasa Rao, Saru Kumari, Muhammad Khurram Khan, Kim-Kwang Raymond Choo, Pairing-based CP-ABE with constant-size ciphertexts and secret keys for cloud environment, *Computer Standards & Interfaces* (2016), doi: 10.1016/j.csi.2016.05.002

# Pairing-based CP-ABE with constant-size ciphertexts and secret keys for cloud environment

Vanga Odelu [a], Ashok Kumar Das [b], Y. Sreenivasa Rao [a], Saru Kumari [c], Muhammad Khurram Khan [d], Kim-Kwang Raymond Choo [e,f]

[a] Department of Mathematics, Indian Institute of Technology, Kharagpur 721 302, India
E-mail: odelu.vanga@gmail.com, odelu.phd@maths.iitkgp.ernet.in; y.sreenivasarao@yahoo.co.in
[b] Center for Security, Theory and Algorithmic Research, International Institute of Information Technology, Hyderabad 500 032, India
E-mail: iitkgp.akdas@gmail.com, ashok.das@iiit.ac.in
[c] Department of Mathematics, Ch. Charan Singh University, Meerut 250 005, Uttar Pradesh, India
E-mail: saryusiirohi@gmail.com
[d] Center of Excellence in Information Assurance, King Saud University, Riyadh 11451, Kingdom of Saudi Arabia
E-mail: mkhurram@ksu.edu.sa
[e] School of Computer Science, China University of Geosciences, Wuhan, China
[f] School of Information Technology & Mathematical Sciences, University of South Australia, SA, Australia
E-mail: raymond.choo@fulbrightmail.org

**Abstract**

Ciphertext-policy attribute-based encryption (CP-ABE) scheme can be deployed in a mobile cloud environment to ensure that data outsourced to the cloud will be protected from unauthorized access. Since mobile devices are generally resource-constrained, CP-ABE schemes designed for a mobile cloud deployment should have constant sizes for secret keys and ciphertexts. However, most existing CP-ABE schemes do not provide both constant size ciphertexts and secret keys. Thus, in this paper, we propose a new pairing-based CP-ABE scheme, which offers both constant size ciphertexts and secret keys (CSCTSK) with an expressive AND gate access structure. We then show that the proposed CP-ABE-CSCTSK scheme is secure against chosen-ciphertext adversary in the selective security model, and present a comparative summary to demonstrate the utility of the scheme.

*Keywords:* Ciphertext-policy attribute-based encryption, constant-size secret keys, constant-size ciphertexts, lightweight mobile devices, mobile cloud computing.

## 1. Introduction

Mobile devices have become the primary computing device for many individuals, and one popular mobile application (app) category is cloud apps. For example, Dropbox, a popular cloud storage app, has between 500 million and one billion downloads on Google Play store as of 16 December 2015. With the increasing popularity and adoption of mobile devices, vulnerabilities in mobile devices, mobile operating systems or mobile apps can be exploited by criminals to target mobile device and app users [1, 2, 3, 4, 5]. One popular cryptographic solution deployed in cloud is ciphertext-policy attribute-based encryption (CP-ABE), which allows the user to encrypt the data to be outsourced to the cloud using an access structure. The encrypted data (i.e. ciphertext) can only be decrypted if, and only if, the attribute set fulfills the ciphertext access structure. In other words, CP-ABE enables data owners to design and enforce access structure [6, 7, 8, 9].

However, in a mobile cloud setting where devices used to access the cloud services are generally resource-constrained (e.g. limited battery life), traditional cryptographic solutions (e.g. CP-ABE schemes) may not be fit-for-purpose. For example, for CP-ABE to be deployed on resource-constrained devices, the scheme should support constant size ciphertexts and constant size secret keys. An attribute-based encryption (ABE), an extension of identity-based encryption (IBE), has two variants, namely: key-policy ABE (KP-ABE) and ciphertext-policy ABE (CP-ABE). In the former, the secret key is associated with an access structure and the