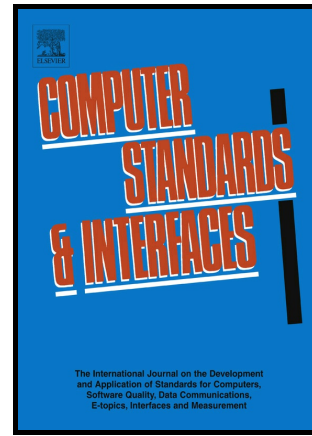


# Author's Accepted Manuscript

Identity-based conditional proxy re-encryption with fine grain policy

Chunpeng Ge, Willy Susilo, Jiandong Wang,  
Liming Fang



PII: S0920-5489(16)30234-3  
DOI: <http://dx.doi.org/10.1016/j.csi.2016.12.005>  
Reference: CSI3182

To appear in: *Computer Standards & Interfaces*

Received date: 18 May 2016  
Revised date: 22 October 2016  
Accepted date: 23 December 2016

Cite this article as: Chunpeng Ge, Willy Susilo, Jiandong Wang and Liming Fang, Identity-based conditional proxy re-encryption with fine grain policy *Computer Standards & Interfaces*, <http://dx.doi.org/10.1016/j.csi.2016.12.005>

This is a PDF file of an unedited manuscript that has been accepted for publication. As a service to our customers we are providing this early version of the manuscript. The manuscript will undergo copyediting, typesetting, and review of the resulting galley proof before it is published in its final citable form. Please note that during the production process errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain

# Identity-based conditional proxy re-encryption with fine grain policy

Chunpeng Ge<sup>1</sup>, Willy Susilo<sup>2\*</sup>, Jiandong Wang<sup>3</sup> & Liming Fang<sup>3</sup>

<sup>1</sup>Department of Computer Engineering,  
Jiangsu University of Technology, Changzhou, China  
Email: [gecp@nuaa.edu.au](mailto:gecp@nuaa.edu.au)

<sup>2</sup> Centre for Computer and Information Security Research (CCISR),  
School of Computing and Information Technology,  
University of Wollongong, Australia  
Email: [wsusilo@uow.edu.au](mailto:wsusilo@uow.edu.au)

<sup>3</sup>College of Computer Science and Technology  
Nanjing University of Aeronautics and Astronautics, Nanjing, China

**Abstract.** An identity-based conditional proxy re-encryption scheme (IB-CPRE) allows a semi-trusted proxy to convert a ciphertext satisfying one condition, which is set by the delegator, under one identity to another without the necessity to reveal the underlying message. In ICISC 2012, Liang, Liu, Tan, Wong and Tang proposed an IB-CPRE scheme, and left an open problem on how to construct chosen-ciphertext secure IB-CPRE supporting OR gates on conditions. In this work, we answer this aforementioned problem by constructing an identity-based conditional proxy re-encryption scheme with fine grain policy (IB-CPRE-FG). In an IB-CPRE-FG scheme, each ciphertext is labeled with a set of descriptive conditions and each re-encryption key is associated with an access tree that specifies which type of ciphertexts the proxy can re-encrypt. Furthermore, our scheme can be proved secure against adaptive access tree and adaptive chosen-ciphertext attack.

**Keywords:** Conditional proxy re-encryption, Identity-based proxy re-encryption, Chosen-ciphertext security.

## 1 Introduction

Identity-based proxy re-encryption (IB-PRE), introduced by Green and Ateniese [1], enables a proxy to convert a ciphertext encrypted under Alice's identity into one encrypted under Bob's identity. To capture the conditional property, Shao, Wei, Ling and Xie [2] introduced the notion of identity-based conditional proxy re-encryption (IB-CPRE), in which only ciphertexts satisfying a special condition can be converted by the proxy. However, their scheme is only proven secure in the random oracle. Further, Liang, Liu, Tan, Wong and Tang [3] proposed an identity-based conditional proxy re-encryption scheme in the standard model.

---

\*Corresponding Author: Willy Susilo.

Download English Version:

<https://daneshyari.com/en/article/4955031>

Download Persian Version:

<https://daneshyari.com/article/4955031>

[Daneshyari.com](https://daneshyari.com)