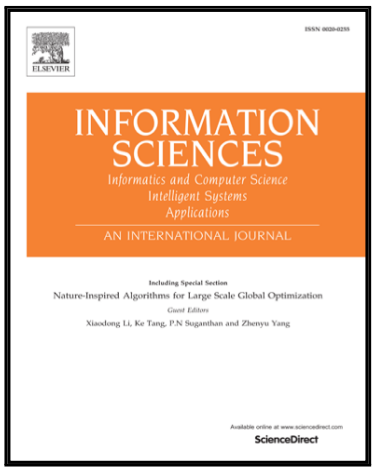

Key-Policy Attribute-Based Encryption against Continual Auxiliary Input Leakag

Jiguo Li , Qihong Yu , Yichen Zhang , Jian Shen

PII: S0020-0255(16)30837-4
DOI: https://doi.org/10.1016/j.ins.2018.07.077
Reference: INS 13844

To appear in: *Information Sciences*

Received date: 10 September 2016
Revised date: 21 April 2018
Accepted date: 31 July 2018

Please cite this article as: Jiguo Li , Qihong Yu , Yichen Zhang , Jian Shen , Key-Policy Attribute-Based Encryption against Continual Auxiliary Input Leakag, *Information Sciences* (2018), doi: https://doi.org/10.1016/j.ins.2018.07.077

Key-Policy Attribute-Based Encryption against Continual Auxiliary Input Leakage

Jiguo Li[1,2,4], Qihong Yu[3], Yichen Zhang[1,2,4], Jian Shen[5]

[1](College of Mathematics and Informatics, Fujian Normal University, Fuzhou 350117, China)

[2] (State Key Laboratory of Cryptology, P.O.Box 5159, Beijing, 100878, China)

[3] (School of Computer Science, Suqian College, Suqian 223800, China)

[4] (Jiangsu Key Laboratory of Big Data Security & Intelligent Processing, Nanjing University of Posts and Telecommunications, Nanjing 210023, China)

[5] (School of Computer and Software, Nanjing University of Information Science and Technology, No. 219, Ningliu Road, Nanjing 210044, China)

Email: ljg1688@163.com

Abstract: Attribute-based encryption mechanism can achieve very flexible access control, so it has a wide range of applications in the distributed environment, such as fine-grained access control, audit log applications, cloud storage systems. Key-policy attribute-based encryption (KP-ABE) scheme is especially suitable for video on demand, pay TV, etc. Most of the existing KP-ABE schemes do not consider the side channel attacks which probably leak some secret information about the cryptosystems. In the paper, we present the formal definition and security model of key-policy attribute-based encryption scheme which is resilient to continual auxiliary input (CAI) leakage. What is more, we present a concrete KP-ABE scheme. The proposed scheme is proved secure under the static assumptions.

Key words: Key-policy attribute-based encryption, continual auxiliary input leakage, dual system encryption, static assumptions.

1. INTRODUCTION

In order to implement the fine-grained access control in traditional public key encryption and identity based encryption (IBE), Sahai and Waters presented attribute-based encryption (ABE) [44], which can be applied in cloud storage system [30,47]. ABE is usually divided into two kinds: ciphertext-policy ABE (CP-ABE) and key-policy ABE (KP-ABE). In CP-ABE schemes [5,26,16,45], the ciphertext is associated with an access policy, while the user's private key is associated with some attributes. In KP-ABE schemes [9,18,19,41], the user's private key is associated with an access policy, while the ciphertext is associated with some attributes. ABE schemes have attracted more concern due to its fine-grained access control. Many ABE schemes were presented, such as hierarchical attribute-based encryption [16,11], ABE with verifiable outsourcing decryption[25,28], multi-authority ABE [4,42], user collusion avoidance ABE [31], traceable ABE [36,39,40], anonymous ABE [29,50], outsourcing ABE [14, 24], flexible and fine-grained ABE [32] and hierarchical attribute based encryption [34].

The existing KP-ABE schemes are almost designed under "black box" model which is based on the absolute security of the secret information. However, the adversary can utilize the cold boot attack [12] and side channel attack [37] to obtain some secret information by the characteristics of