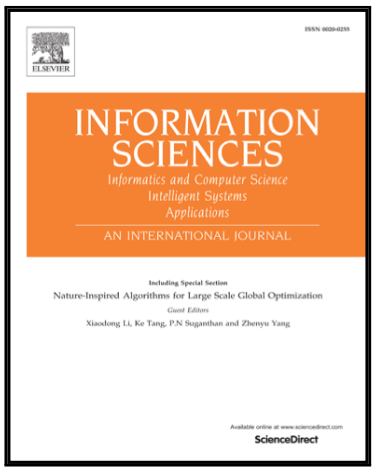

Efficient biometric identity-based encryption

Xiaoguo Li, Tao Xiang, Fei Chen, Shangwei Guo

PII: S0020-0255(18)30540-1
DOI: 10.1016/j.ins.2018.07.028
Reference: INS 13795

To appear in: *Information Sciences*

Received date: 9 March 2018
Revised date: 18 May 2018
Accepted date: 8 July 2018

Please cite this article as: Xiaoguo Li, Tao Xiang, Fei Chen, Shangwei Guo, Efficient biometric identity-based encryption, *Information Sciences* (2018), doi: 10.1016/j.ins.2018.07.028

Efficient biometric identity-based encryption

Xiaoguo Li[a], Tao Xiang[a,b,*], Fei Chen[c], Shangwei Guo[d]

[a] *College of Computer Science, Chongqing University, Chongqing 400044, China*
[b] *Key Laboratory of Dependable Service Computing in Cyber Physical Society (Chongqing University), Ministry of Education*
[c] *Department of Computer Science and Engineering, Shenzhen University, Shenzhen 518060, China*
[d] *Department of Computer Science, Hong Kong Baptist University, Hong Kong 999077, China*

Abstract

As a special case of public key encryption, identity-based encryption (IBE) takes any public known information as public key for encryption and then decrypts a ciphertext by a well-generated private key from private key generator (PKG). Unlike the traditional IBE using a text-based identity (e-mail, etc.) as public key, in this paper, we aim to design a secure, time-saving and space-saving biometric identity-based encryption (BIBE) regarding the biometric-based identity (face, etc.) as public key. To overcome the challenge introduced by the fuzziness of biometric identities, First, we propose a provable-secure inner-product encryption (IPE) with short ciphertext and show the IPE is indistinguishable against selective identity, adaptive chosen-plaintext attack (IND-sID-CPA). Then, we construct a distance-based encryption (DBE) leveraging the proposed IPE and prove that the DBE captures the same security with the underlying IPE. Furthermore, we optimize the proposed DBE so that it also has short private key. We theoretically analyze the overhead of IPE, DBE, and optimized DBE (ODBE) in terms of time, space, and communication complexities. We also conduct experiments to measure the time and space costs of the proposed ODBE, and experimental results validate its effectiveness and efficiency.

Keywords: Biometrics, identity-based encryption, distance-based encryption, inner-product encryption, IND-sID-CPA.

1. Introduction

Identity-based encryption (IBE) possesses the ability of doing public key encryption without accessing to the public key certificate, and can be deployed in various practical applications. IBE allows for a sender to encrypt a message into a ciphertext using publicly known identity information of the receiver, such as e-mail address, social security number, or physical IP address. At the receiver's side, he can extract the message from the ciphertext by decrypting it with a key generated from the identity. Figure 1 depicts the basic principle of IBE, where Alice and Bob serve as the sender and the receiver respectively.

*Corresponding author.
Email address: txiang@cqu.edu.cn (Tao Xiang)