Accepted Manuscript

Multimodal biometric Identity Based Encryption

Neyire Deniz Sarier

PII: S0167-739X(17)30261-3
DOI: https://doi.org/10.1016/j.future.2017.09.078
Reference: FUTURE 3734

To appear in: *Future Generation Computer Systems*

Received date : 16 February 2017
Revised date : 1 September 2017
Accepted date : 30 September 2017

Please cite this article as: N. Deniz Sarier, Multimodal biometric Identity Based Encryption, *Future Generation Computer Systems* (2017), https://doi.org/10.1016/j.future.2017.09.078

Multimodal Biometric Identity Based Encryption ☆

Neyire Deniz Sarier[1]

B-IT cosec, Dahlmannstr. 2, D-53113 Bonn, Germany

Abstract

In this paper, we describe the first generic construction for multimodal biometric Identity Based Encryption considering two distance measures at the same time. Current protocols for fuzzy/biometric IBE are designed either for set overlap or Euclidean distance within unimodal biometrics. However, the similarity measures for biometric templates can be quite different from those considered in theoretical works. For instance, a fingerprint template usually consists of a set of minutiae, and two templates are considered as similar if more than a certain number of minutiae in one template are near distinct minutiae in the other. In this case, the similarity measure has to consider both Euclidean distance and set difference at the same time. Similarly, multimodal systems that are designed to address the limitations of unimodal systems may involve two different traits requiring different distance measures for each modality.

In order to have high recognition rate and thus increased possibility of decryption even in case of white noise (slight perturbation of biometric features), our generic construction is based on two different biometric IBE systems encoding the same message. This way, employment of both distance measures is possible using multiple matchers within multimodal setting and a failure on the decryption of a message encrypted using the first biometric representation, can be compensated with an attempt on the second part of the ciphertext encrypting the same message but using a different representation of the same receiver. Specifically, we combine a fuzzy IBE-type scheme and the recently introduced Distance Based Encryption (DBE) scheme with minimum overhead in terms of public parameters, ciphertext and private key size. For this purpose, we describe an efficient biometric IBE scheme denoted as ordFIBE, which is restricted for biometrics that can be represented as an ordered/grouped set of features. We study the security of ordFIBE both in random oracle model (ROM) and for small universe of attributes in standard model. In ROM, its efficiency is further improved by employing online/offline encryption technique. Next, we instantiate the new construction by combining ordFIBE and the DBE scheme of [1], which shares the same setup phase, in particular, common public parameters. Finally, we describe a new scheme for set difference metric that partially solves an open problem introduced in [2].

Keywords: Multimodal biometrics, fuzzy IBE, threshold ABE, Distance Based Encryption (DBE), online/offline IBE, Set Overlap Distance, Euclidean Distance, fingerprint

1. Introduction

Biometrics have been used for secure identification and authentication for more than two decades since biometric data is non-transferable, unforgettable, and always handy. In this context, multi-modal systems such as fusion of multiple biometrics (i.e. face and fingerprints) or multiple matching of the same biometric trait gained increasing popularity for practical applications, mainly due to the increased recognition performance and enhanced level of security. Recently, biometric data have emerged as a tool for fuzzy Identity Based Cryptography or to generate/bind a *key*, where this *key* could be used in encryption. Clearly, biometric cryptosystems that lock/generate a secret *key* using biometric features assume that biometric template of a user is secret data, whereas fuzzy cryptography requires biometric data as public info. There is a number of biometric cryptosystems that aim to guarantee the secrecy of this *key* such as fuzzy commitment, fuzzy extractors and fuzzy vault. Juels and Wattenberg [4] introduce the fuzzy commitment scheme, which is suitable for hamming distance and specific for biometrics that can be represented as an ordered set of features, i.e. a feature vector. However, biometrics can be affected from two types of noise, i.e. *white noise* that represents the slight perturbation of each feature, and the *replacement noise* caused by the replacement of some features. Thus, Juels and Sudan have developed the *fuzzy vault* [5], which assumes that biometrics consists of an unordered set of features and is designed for the set difference metric. Specifically, fuzzy vault is a *key* locking system that hides an encoded secret among some chaff

☆An extended abstract [3] of this paper is presented at the 11th IEEE International Conference for Internet Technology and Secured Transactions 2016.

[1]Dr. N. Deniz Sarier is an external researcher in Bonn-Aachen International Center for Information Technology, Computer Security Group, Dahlmannstr. 2, D-53113 Bonn, Germany (e-mail: denizsarier@yahoo.com)