Introduction

Biometric identification is a convenient and reliable method of authentication. However, the personal and irrevocable nature of biometric data motivates strong security on templates during both transmission and storage.

Among the security methods proposed, two distinct approaches can be identified, one from the world of cryptography, and the other from signal processing and error correction.

Background

Secure multi-party computation (SMC) is a method by which two or more parties collectively compute the output of a function without any party learning the inputs of the other parties. SMC generally builds upon cryptographic systems with provable security properties based on assumptions about the hardness of certain problems (for example, prime factorization).

A biometric cryptosystem (BCS) is a method for generating cryptographic keys from biometric templates, such as face, fingerprint, or iris data. These systems generally depend on “fuzzy” methods for turning biometric data into cryptographic primitives.

Methods of Biometric Security

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Trust Model</td>
<td>• “Semi-honest” parties: no information leakage if both parties respect the protocol</td>
<td>• Trusted matcher (though not against database compromise)</td>
</tr>
<tr>
<td>Security</td>
<td>• Provable semantic security based on hardness assumptions</td>
<td>• Difficult to determine semantic security</td>
</tr>
<tr>
<td>Accuracy</td>
<td>• Limited to very simple methods (fully homomorphic encryption is too expensive)</td>
<td>• Performance degradation from forced quantization (“fuzziness”)</td>
</tr>
<tr>
<td>Complexity</td>
<td>• Requires multiple online communication rounds</td>
<td>• Slight increase in both online and offline complexity</td>
</tr>
<tr>
<td></td>
<td>• Outsourceable</td>
<td>• Requires centralized matcher</td>
</tr>
</tbody>
</table>

Case Study: Outsourceable Privacy-Preserving Two-Party Biometric Authentication [3]

Building block: homomorphic encryption

For two plaintexts a and b, we can compute the encryption of a + b using only the ciphertexts [a] and [b]

Objective

Outsource computation to cloud services without revealing any information to service providers

Method

• Provider 1 holds encrypted database
• Provider 2 holds secret key
• Mutually compute distances

References


Acknowledgments

This project was made possible by National Science Foundation (IIS-1359199) and the University of Houston Computer Science Department REU Program. Special thanks to Prof. Kakadiaris and Panagiotis Moutafis.