Privacy Preserving Speech Processing

Gérard CHOLLET, Research professor

Research director in CNRS, Télécom ParisTech, Paris, FRANCE
gerard.chollet@telecom-paristech.fr

Abstract

As computational and communications infrastructure expands in its capabilities, so has the resultant exposure of its users to unintended and undesired consequences. This is particularly so for voice-based services and communication. Increasing numbers of people are using voice-based services for a variety of purposes. Large amounts of private voice data are being stored on cloud platforms. However, in each of these actions the user unwittingly gives away highly private data – their voice. Voice is a legally accepted biometric. A person's voice contains information about their gender, origins, health, emotional state, age, ... In using any service, the user is giving away not only the content of their speech, but also this information. A malicious server, or an eavesdropper, may obtain unintended demographic information about the user by analyzing the voice and sell this information. It may edit recordings to create fake recordings the user never spoke. Merely encrypting the data for transmission or storage does not protect the user, since the recipient (the server) must finally have access to the data in the clear (i.e. decrypted form) in order to perform its processing.

In this tutorial, we will discuss solutions for privacy-preserving sound processing, which enable a user to employ sound- or voice-processing services without exposing themselves to risks such as the above. We will describe the basics of privacy-preserving techniques for data processing, including homomorphic encryption, oblivious transfer, secret sharing, and secure-multiparty computation.

We will describe how these can be employed to build secure "primitives" for computation, that enable users to perform basic steps of computation without revealing information. We will describe the privacy issues with respect to these operations. We will then briefly present schemes that employ these techniques for privacy-preserving signal processing and biometrics. We will then delve into uses for voice processing, including authentication, classification and recognition, and discuss computational and accuracy issues.

Finally we will close with a discussion of the current state of the art, future directions, and avenues for legal and scientific research.