Chapter 16

Secure Speaker Recognition using BGN Cryptosystem with Prime Order Bilinear Group

S. Selva Nidhyananthan
Mepco Schlenk Engineering College, India

M. Prasad
Mepco Schlenk Engineering College, India

R. Shantha Selva Kumari
Mepco Schlenk Engineering College, India

ABSTRACT

Speech being a unique characteristic of an individual is widely used in speaker verification and speaker identification tasks in applications such as authentication and surveillance respectively. In this paper, framework for secure speaker recognition system using BGN Cryptosystem, where the system is able to perform the necessary operations without being able to observe the speech input provided by the user during speaker recognition process. Secure speaker recognition makes use of Secure Multiparty Computation (SMC) based on the homomorphic properties of cryptosystem. Among the cryptosytem with homomorphic properties BGN is preferable, because it is partially doubly homomorphic, which can perform arbitrary number of addition and only one multiplication. But the main disadvantage of using BGN cryptosystem is its execution time. In proposed system, the execution time is reduced by a factor of 12 by replacing conventional composite order group by prime order group. This leads to an efficient secure speaker recognition.

DOI: 10.4018/978-1-7998-1763-5.ch016

INTRODUCTION

Speech is one of the most private forms of personal communication. A sample of a person's speech contains information about the gender, accent, ethnicity, and the emotional state of the speaker apart from the message content. Speech processing technology is widely used in biometric authentication in the form of speaker verification. In a conventional speaker verification system, the speaker patterns are stored without any obfuscation and the system matches the speech input obtained during authentication with these patterns. If the speaker verification system is compromised, an adversary can use these patterns to later impersonate the user. Similarly, speaker identification is also used in surveillance applications. Most individuals would consider unauthorized recording of their speech, through eavesdropping or wiretaps as a major privacy violation. Yet, current speaker verification and speaker identification algorithms are not designed to preserve speaker privacy and require complete access to the speech data.

In many situations, speech processing applications such as speech recognition are deployed in a client-server model, where the client has the speech input and a server has the speech models. Due to the concerns for privacy and confidentiality of their speech data, many users are unwilling to use such external services. Even though the service provider has a privacy policy, the client speech data is usually stored in an external repository that may be susceptible to being compromised. The external service provider is also liable to disclose the data in case of a subpoena. It is, therefore, very useful to have secure speech processing algorithms that can be used without violating these constraints.

The objective of this paper is to develop a design for secure speaker recognition based on the homomorphic properties of BGN cryptosystem with low execution time. Usually, the main constraint in secure speaker recognition is the execution time which is dependent on the encryption of the speaker models. In existing work (Manas, 2013), they have used BGN cryptosystem and implemented it using composite order groups of larger size, which take large time to execute. In the proposed system, composite order group is replaced with prime order group of small size which gives the same security as composite order group implementation and reduces the execution time by a factor of 12. So we can obtain efficient secure speaker recognition using the proposed system.

LITERATURE SURVEY

Mel Frequency Cepstral Coefficient (MFCC) works better in noisy environment than that of Linear LPC as per Reynolds (1995). HMM needs higher computation than GMM but while considering the performance results they both are almost same. The ML parameter estimation using Expectation Maximization (EM) algorithm is used iteratively to estimate GMM parameters. It is also noted that the initial parameter for GMM is not making much difference to the final results. The speech feature vectors are separated into segments for performance evaluation. The performance of different models is compared with GMM.

BGN cryptosystem is a somewhat fully homomorphic cryptosystem which can perform arbitrary number of addition and only one multiplication (Boneh, Goh & Nissim, 2006). It is based on both Paillier and Okamoto Uchiyama encryption schemes. The cryptosystem depends on Subgroup decision problem of Composite order bilinear groups. The BGN cryptosystem is applied for calculation of 2-DNF formula, Private information retrieval, efficient election protocol without random oracles and universally verifiable computation.