1 Motivation

- It is generally expected that intelligent devices will respond to voice. The voice will often not be processed locally, but relegated to a remote server, as data owners may not have the resources to process their own data. This poses serious privacy risks to the user.
- A person’s voice is a legally-accepted biometric, and carries information about their identity, gender, nationality, health, emotional state and a variety of other factors.
- The remote voice service could potentially make undesired inferences about any of these factors, which may be unrelated to the actual service provided.
- This poster discusses “privacy preserving” computational approaches for voice processing that prevent such undesired inferences through cleverly-designed cryptographic and hashing schemes.

2 Can Cryptography Help?

- Secure Multiparty Computation
  - Homomorphic Encryption
- Computation recast as a sequence of primitives
- Garbled Circuits
- Secure Multiarty Computation
  - Garbled Circuits

3 Privacy-Preserving Speech Processing

- Work on sequence of feature vectors computed from speech
- Speech processing tasks:
  - Speaker Verification: *Are you really* Alice? Yes/No
  - Speaker Identification: *Which one of* Alice, Bob, Carol, Dave, ... *are you?*
  - Speech Recognition: *You said* “Hello, world”
  - Keyword Spotting: *You said* “blah blah blah ... *drugs* ... blah blah blah”

- Hashing techniques
  - Locality-Sensitive Hashing
- Examples:
  - Telephone company unwilling to expose audio to intelligence agency
    * May provide encrypted data to the agency
  - Agency cannot expose what it is trying to find (a voice, a key phrase) to the telephone company
    * May provide it in encrypted form to the telephone company

- Compromise between obtained results and computational efficiency

Acknowledgments

This work was partially supported by FCT project SUSPECT.