Using ambient audio in secure mobile phone communication

Ngu Nguyen, Stephan Sigg, An Huynh, Yusheng Ji

Introduction

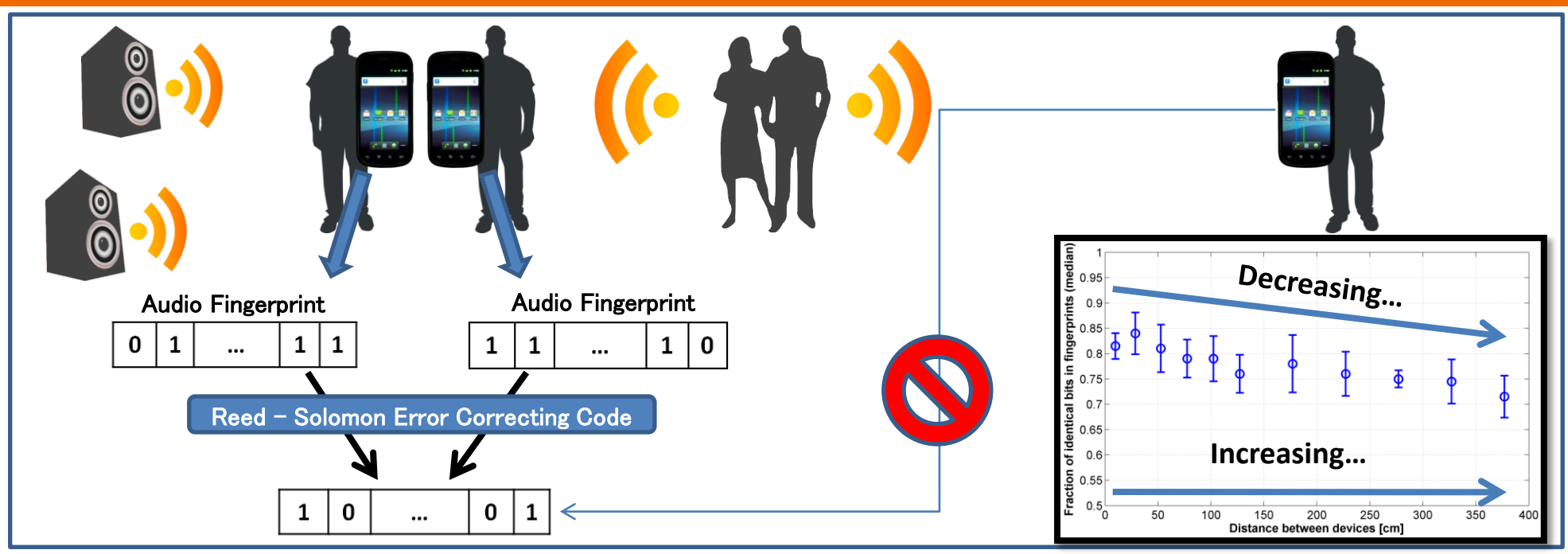
One of the central issue in adhoc mobile device pairing is the identification of devices. A pairing process usually depends on the users to validate which remote device conducting the pairing. For example, in Bluetooth-based communication, the users themselves verify the PIN codes.

Motivation

Adjacent devices may collect similar context data (ambient audio, movement, position,…):

- Can context help to avoid initial data exchange for the authentication of mobile phones?
- Can we design an unobtrusive device pairing mechanism?

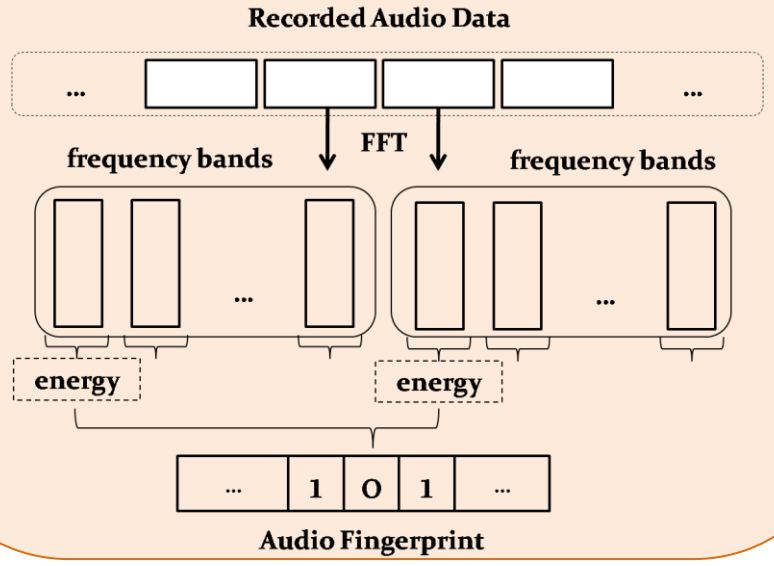
Using ambient audio to generate the common key in mobile phone communication



Issues of Audio Fingerprints

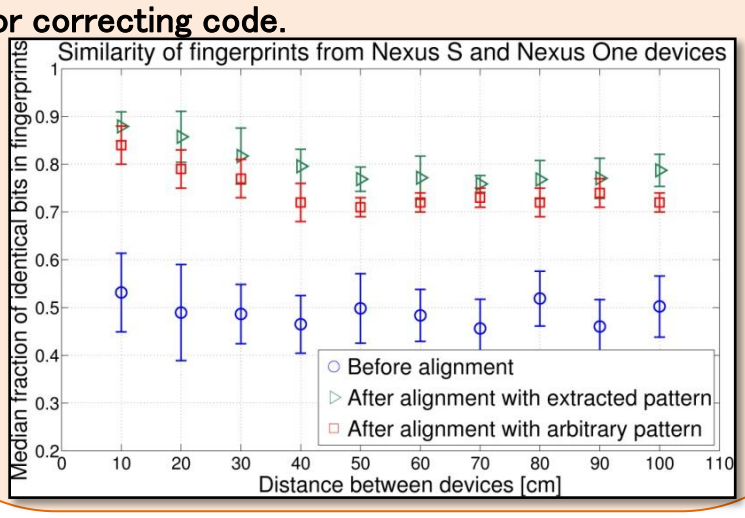
Fingerprint Generation

- Each fingerprint is a 512-bit binary sequence.
- Fingerprints are extracted from recorded audio data of each device.
- They are generated from the energy fluctuation of audio signals in frequency domain.
- The fingerprinting scheme can tolerate the variance in amplitude values of audio signals.



Audio Alignment

- We observed that there is misalignment in recorded audio data. This is due to the variety of smart-phone hardwares. To cope with the above problem, we proposed an pattern-based matching method combining with a multiple trial communication scheme.
- In the below figure, the characteristics of aligned audio fingerprints allows a sharper threshold of the error correcting code.



NII
連絡先: ●●●／ 国立情報学研究所 アーキテクチャ科学研究系 教授
TEL : 00-000-0000 FAX : 00-000-0000 Email : kei@nii.ac.jp & sigg@nii.ac.jp