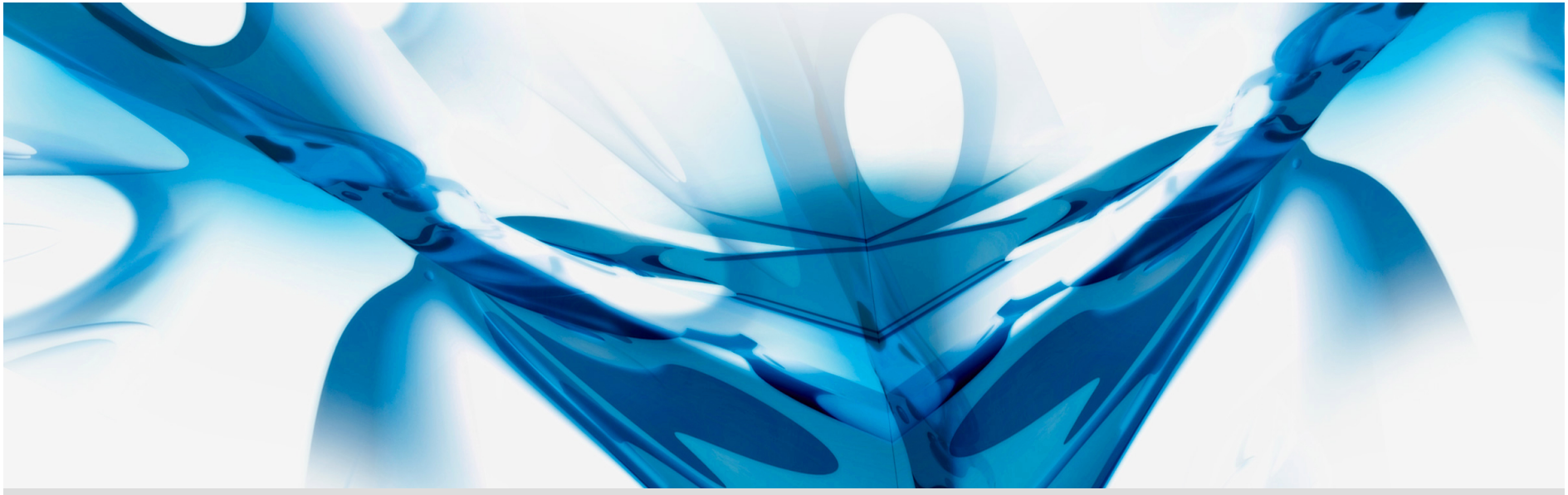
大学共同利用機関法人 情報・システム研究機構
国立情報学研究所
National Institute of Informatics

Information Systems
Architecture Science
Research Division



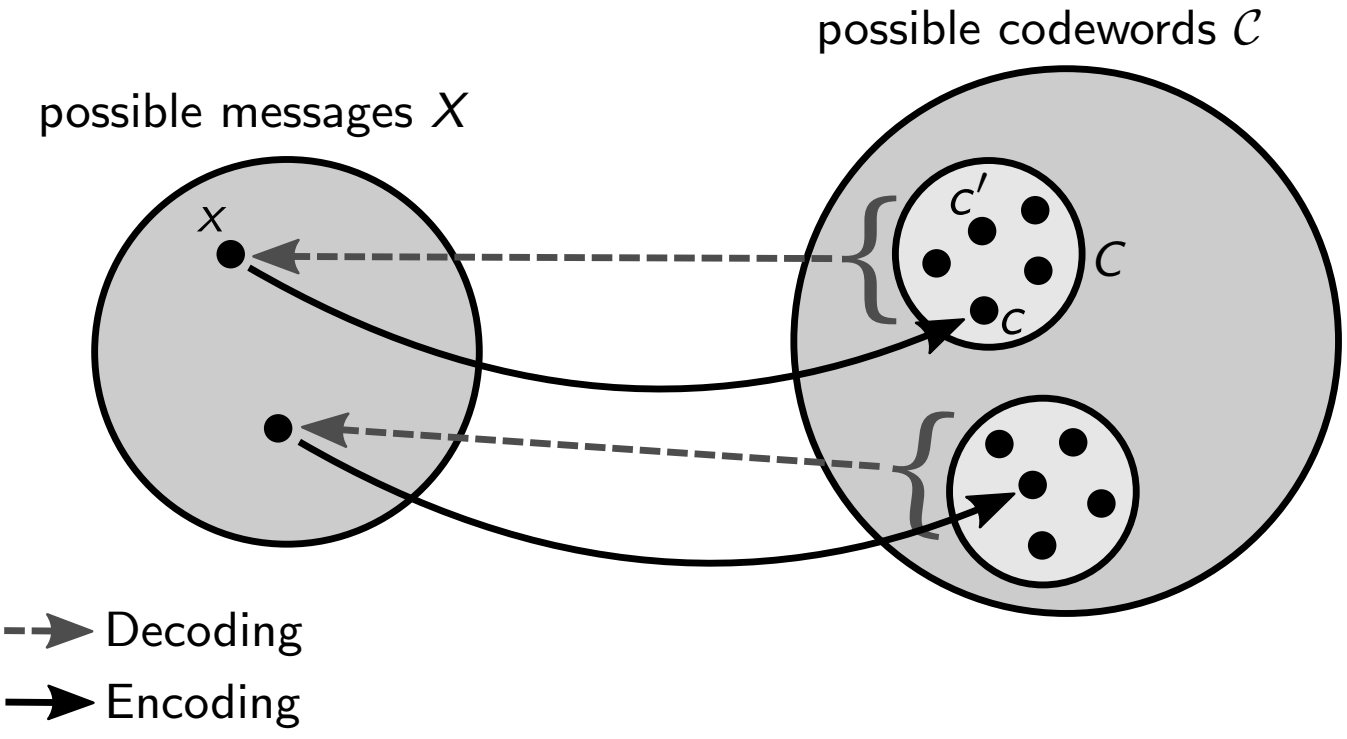
AdHocPairing

Spontaneous audio based secure device pairing for Android mobile devices

Stephan Sigg, Ngu Nguyen, An Huynh and Yusheng Ji

iwssi 2012, 18.06.2012, Newcastle

Security from environmental stimuli



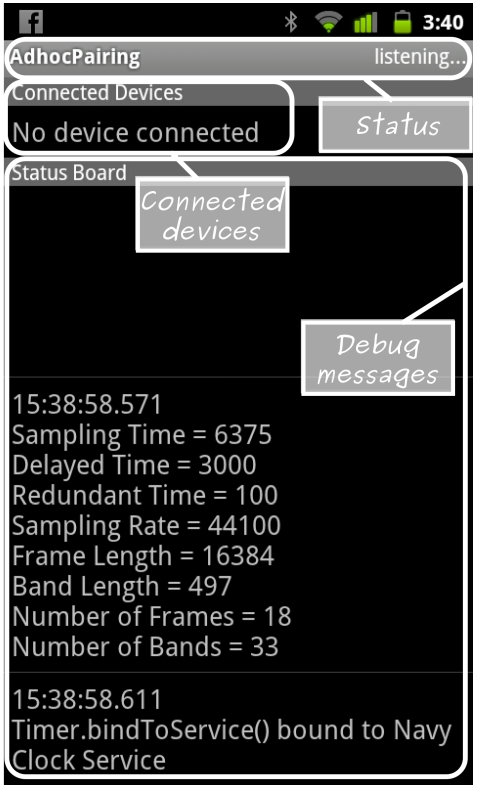
- Generation of Audio fingerprints[1]
- Utilise Fuzzy cryptography to obtain identical keys at devices[2]

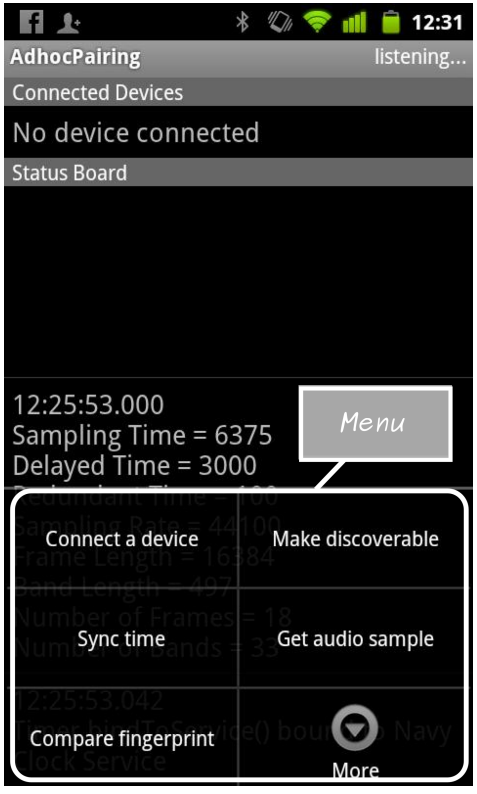
[1] J. Haitsma and T. Kalker, A highly robust audio fingerprinting system, ISMIR 2002

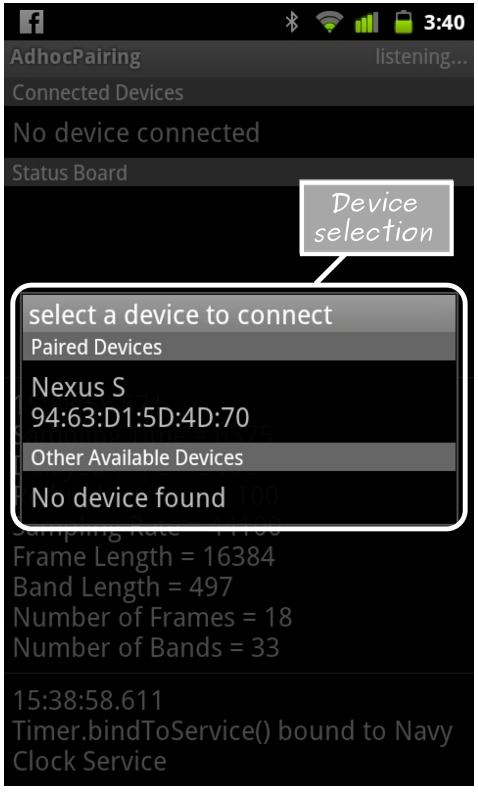
[2] P. Tuyls, B. Skoric, T. Kevenaar, Security with noisy Data, Springer, 2007

Security from environmental stimuli

AdHocPairing: Android-App for secure ad-hoc device pairing

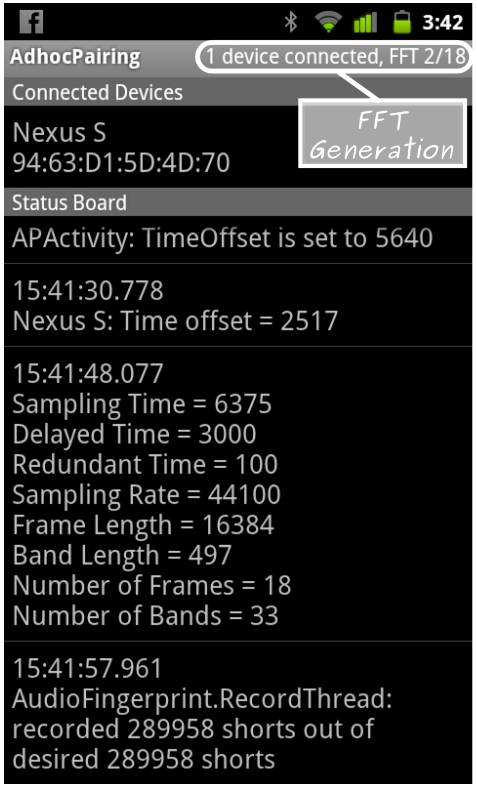






Security from environmental stimuli

AdHocPairing: Android-App for secure ad-hoc device pairing

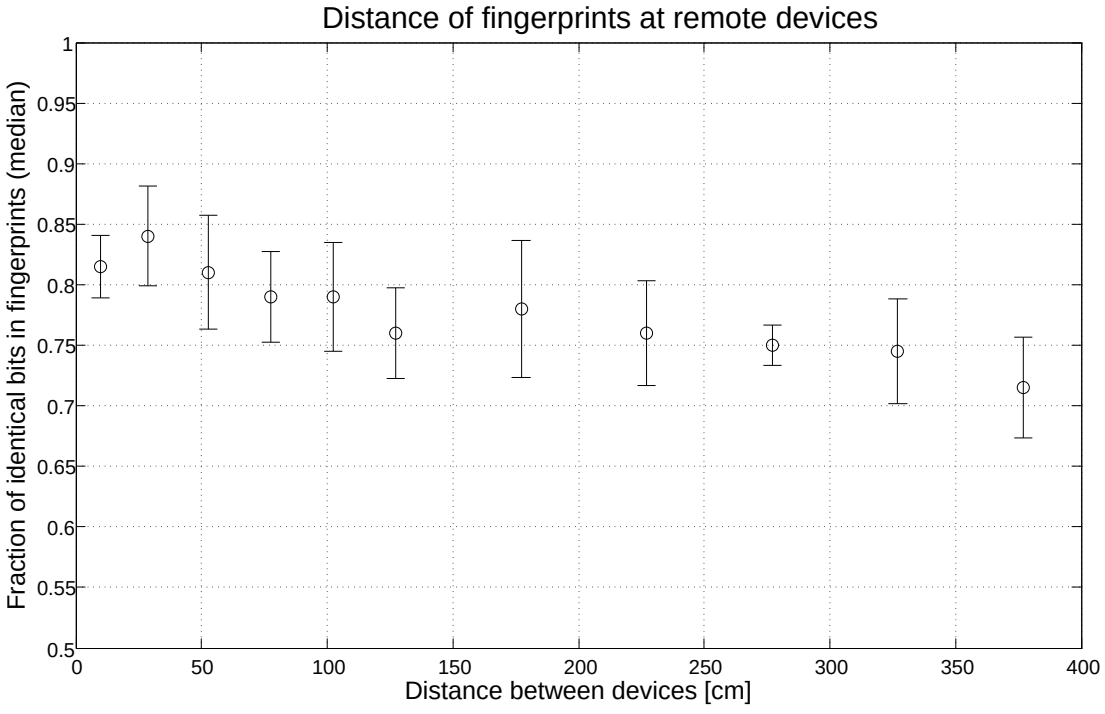


Security from environmental stimuli

Case study with up to four Android devices

- 3 · Nexus S, 1 · Nexus One
- Dominant audio created by audio source
- Distance to audio source kept identical (15cm to 4m)

Security from environmental stimuli



- With distance, similarity in fingerprints decreases
- Security sphere of about 2 meters
- Confirms earlier experiments in other settings

Conclusion

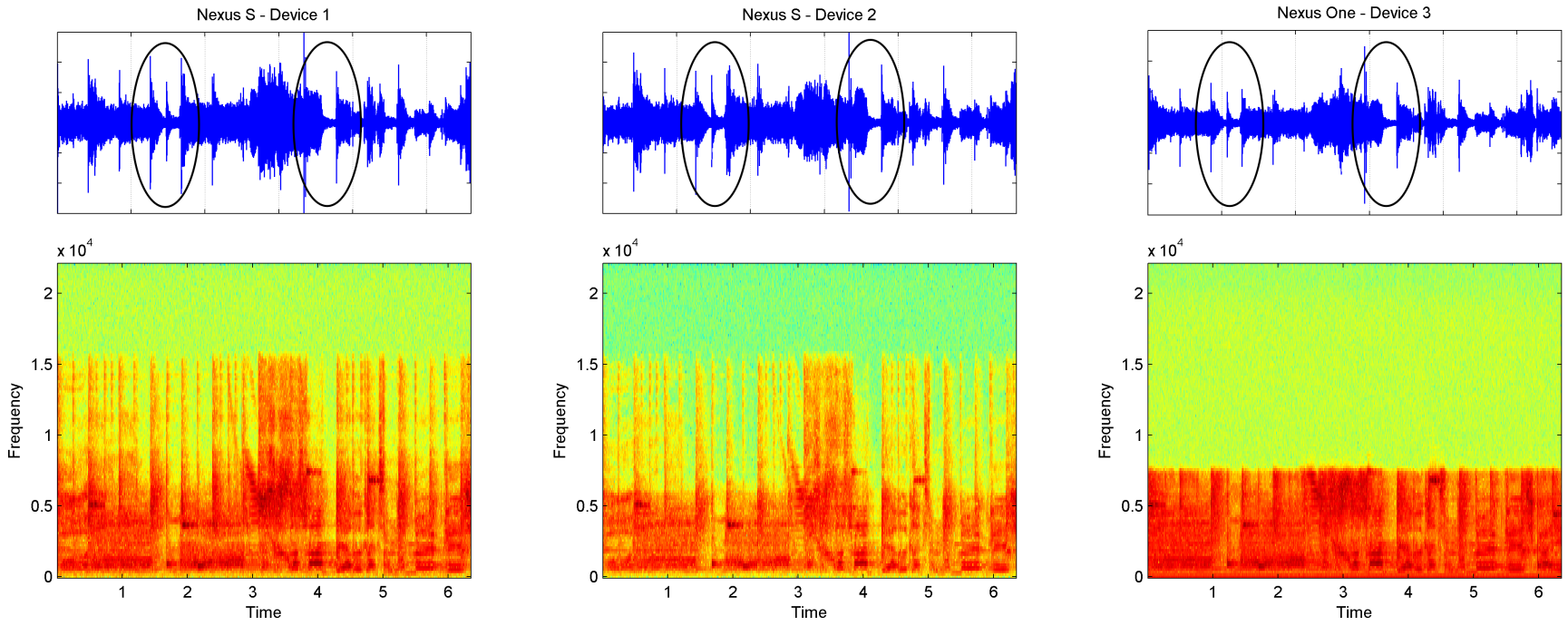
- Implementation on android
- Case study with mobile phones
- Synchronisation of context without data transmission

Questions?

Stephan Sigg
sigg@nii.ac.jp

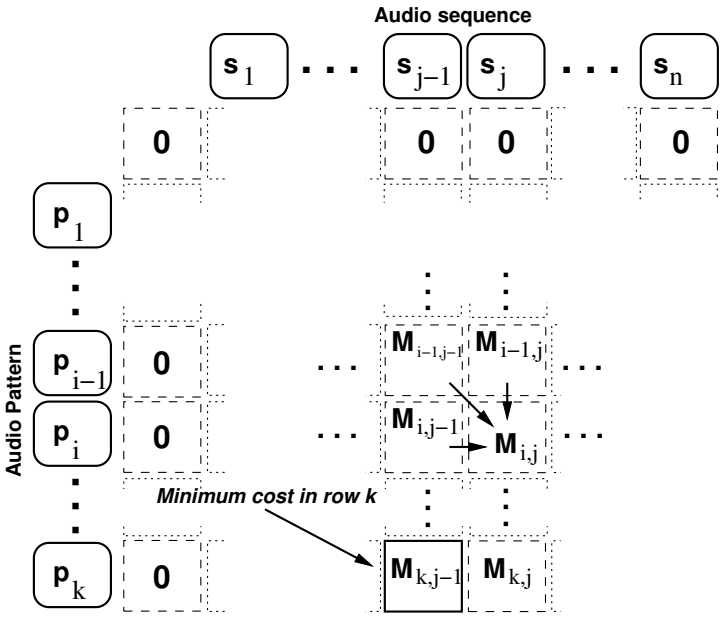
Security from environmental stimuli

Hardware-originated synchronisation offset



Security from environmental stimuli

Hardware-originated synchronisation offset

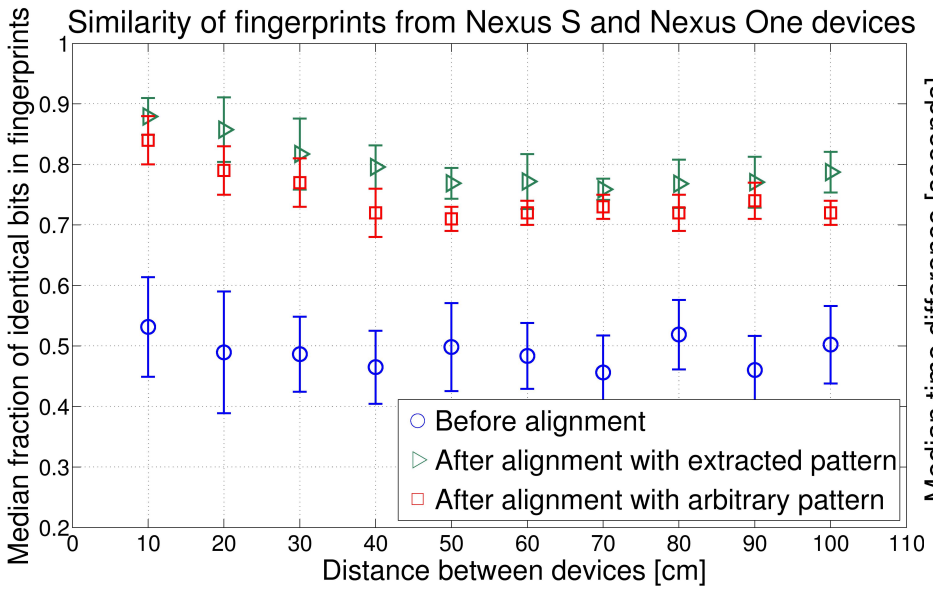


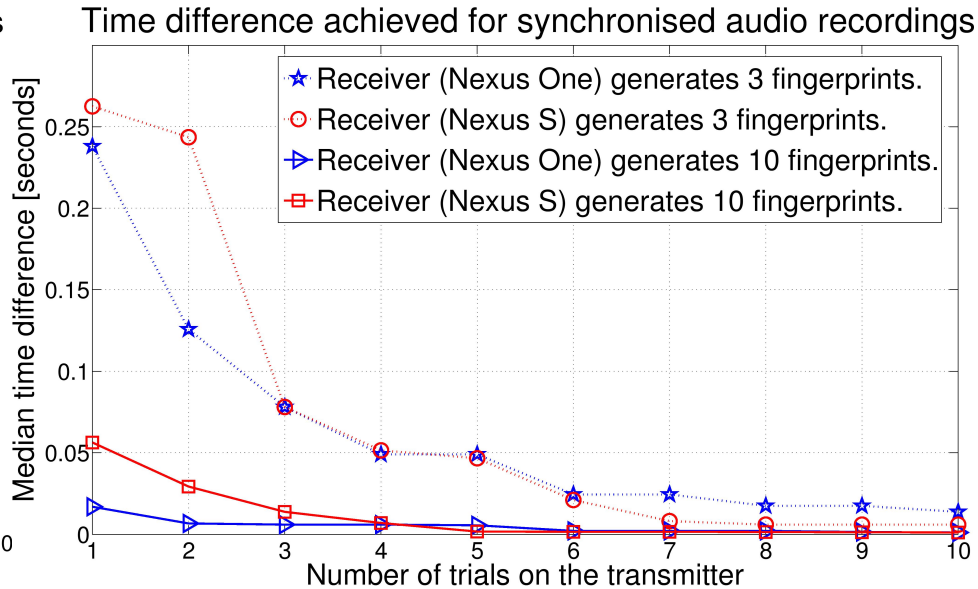
- Approximate pattern matching with arbitrary sequence[3]

[3] T. F. Smith and M. S. Waterman. Identification of common molecular subsequences. Journal of molecular biology, 147(1):195â197, Mar. 1981

Security from environmental stimuli

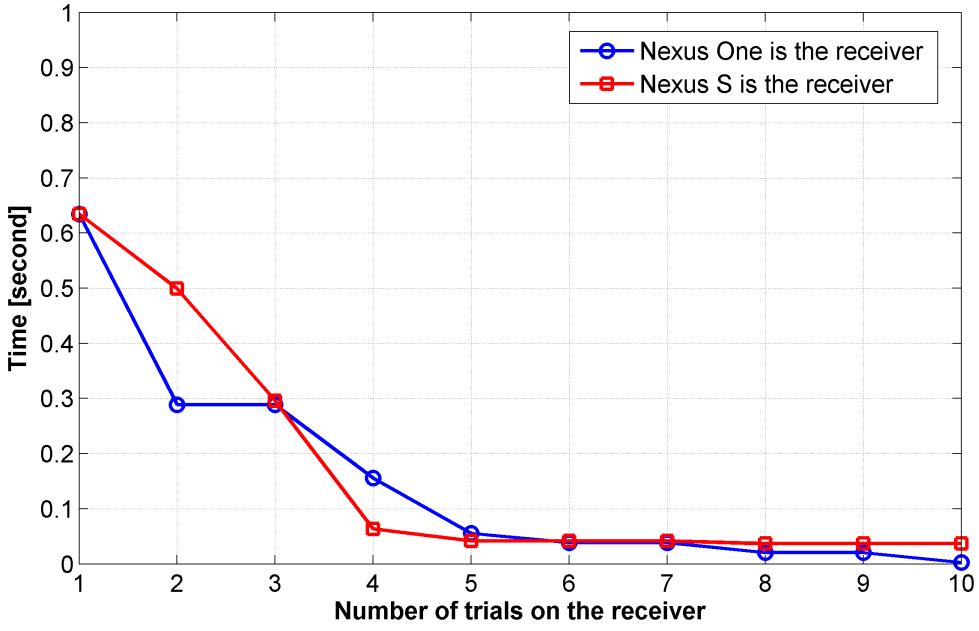
Hardware-originated synchronisation offset[4]





- Synchronisation in the order of 3ms possible
- No additional data transmitted among devices

[4] Ngu Nguyen, Stephan Sigg, An Huynh, Yusheng Ji, Using ambient audio in secure mobile phone communication, PerCom 2011

Security from environmental stimuli

Hardware-originated synchronisation offset