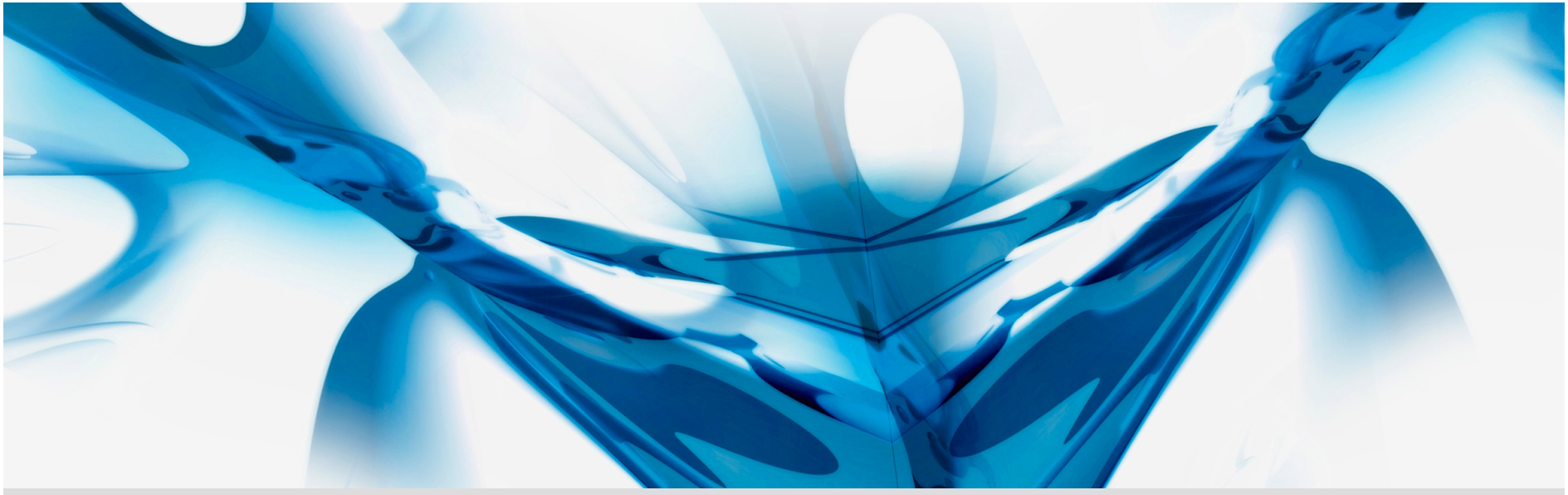
大学共同利用機関法人 情報・システム研究機構
国立情報学研究所
National Institute of Informatics

Information Systems
Architecture Science
Research Division



Pattern based alignment of audio data for Ad-hoc secure device pairing

Zero-communication data synchronisation

Ngu Nguyen, Stephan Sigg, An Huynh and Yusheng Ji

ISWC 2012, 21.06.2012, Newcastle

Security from environmental stimuli

The # of communicating devices increasingly exceeds mobile users

Among all other tasks we have on our minds, how shall we also take care of these device's security issues?

Security from environmental stimuli

The # of communicating devices increasingly exceeds mobile users

Among all other tasks we have on our minds, how shall we also take care of these device's security issues?

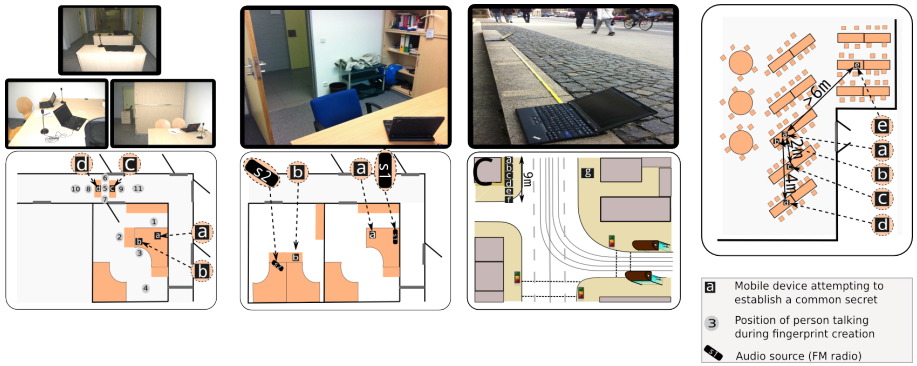
- Security must become not only unobtrusive but unattended
- We need a more natural perception of security

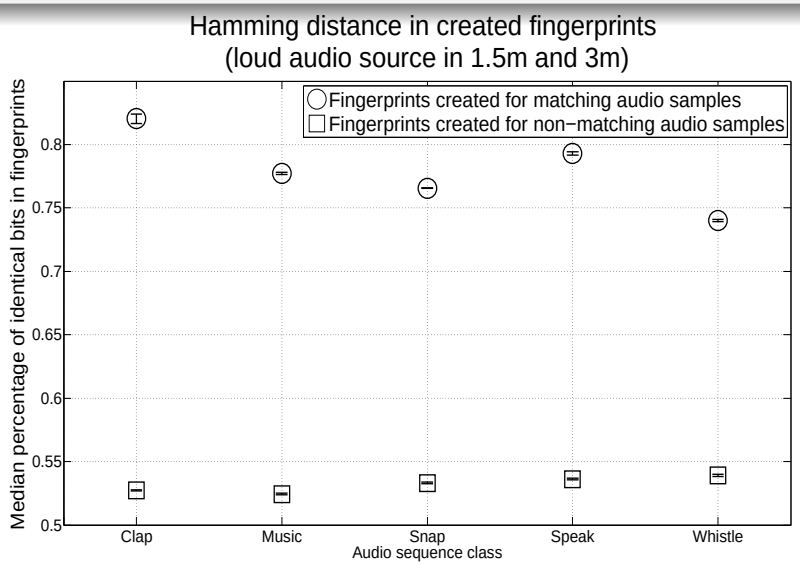
Security from environmental stimuli

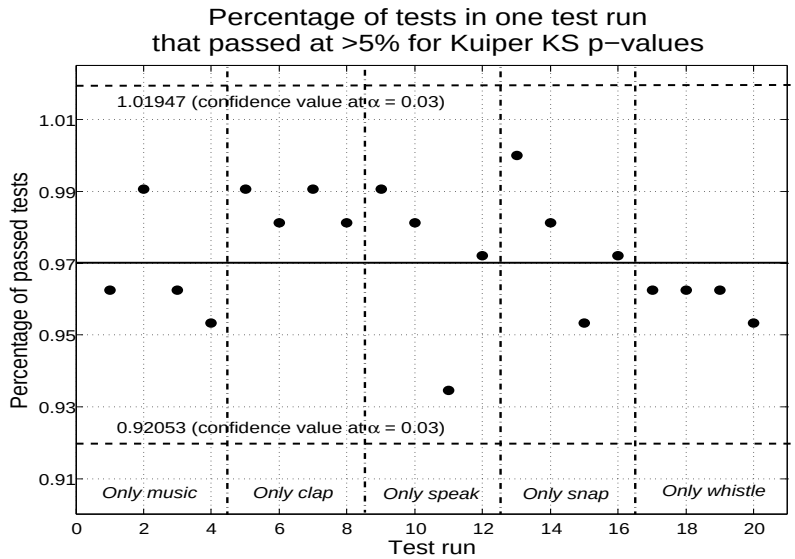
Audio-based ad-hoc secure pairing[a]

[a] S. Sigg et al., Secure Communication based on Ambient Audio, Accepted for IEEE Transactions on Mobile Computing

- Audio as common context source
- Fuzzy cryptography

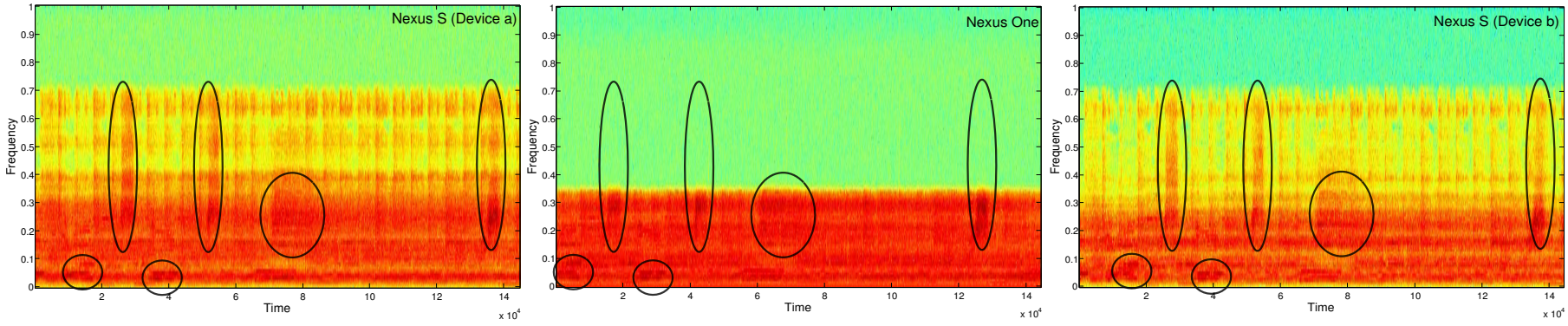






Security from environmental stimuli

Hardware-originated synchronisation offset



- We experiences significant differences in audio samples from devices with differing hardware(Nexus One; Nexus S)
- How can we correct these without disclosing information on the channel?

Security from environmental stimuli

How to synchronise audio without disclosing information?

No data shall be transmitted among devices

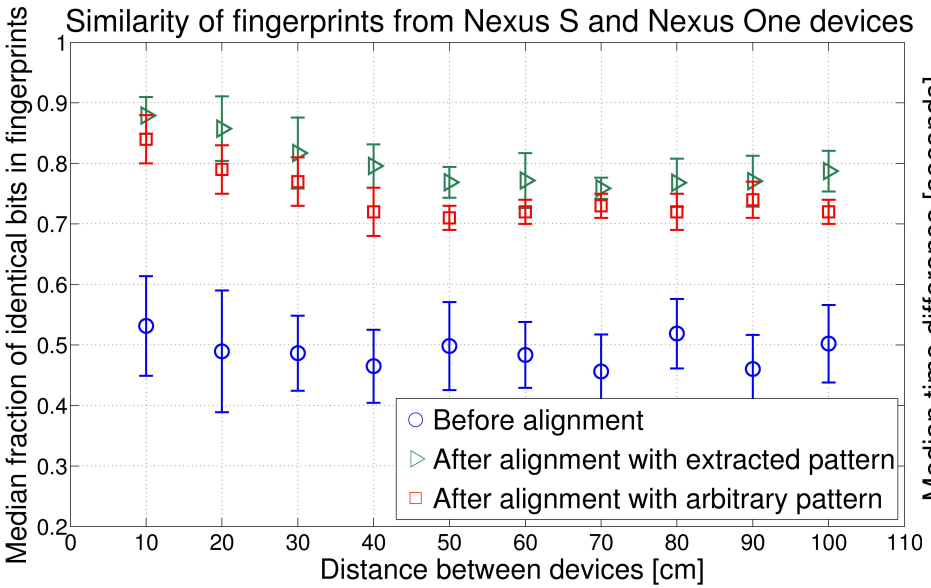
Hardware-originated synchronisation offset

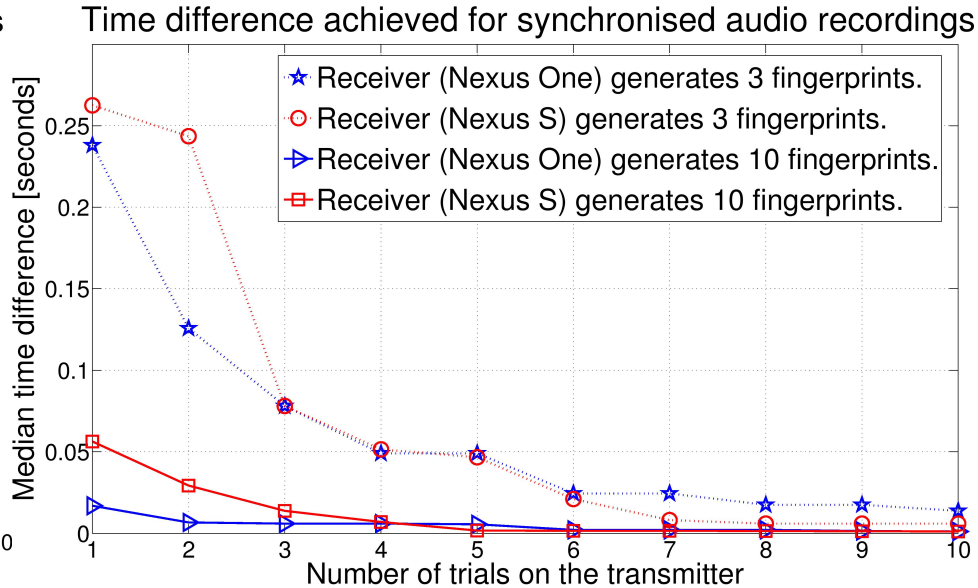
- Approximate pattern matching with arbitrary common sequence[a]

[a] 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





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

Conclusion

Unattended, spontaneous ad-hoc security scheme

Capable of rising the base-level for security on mobile devices

Conclusion

Unattended, spontaneous ad-hoc security scheme

Capable of rising the base-level for security on mobile devices

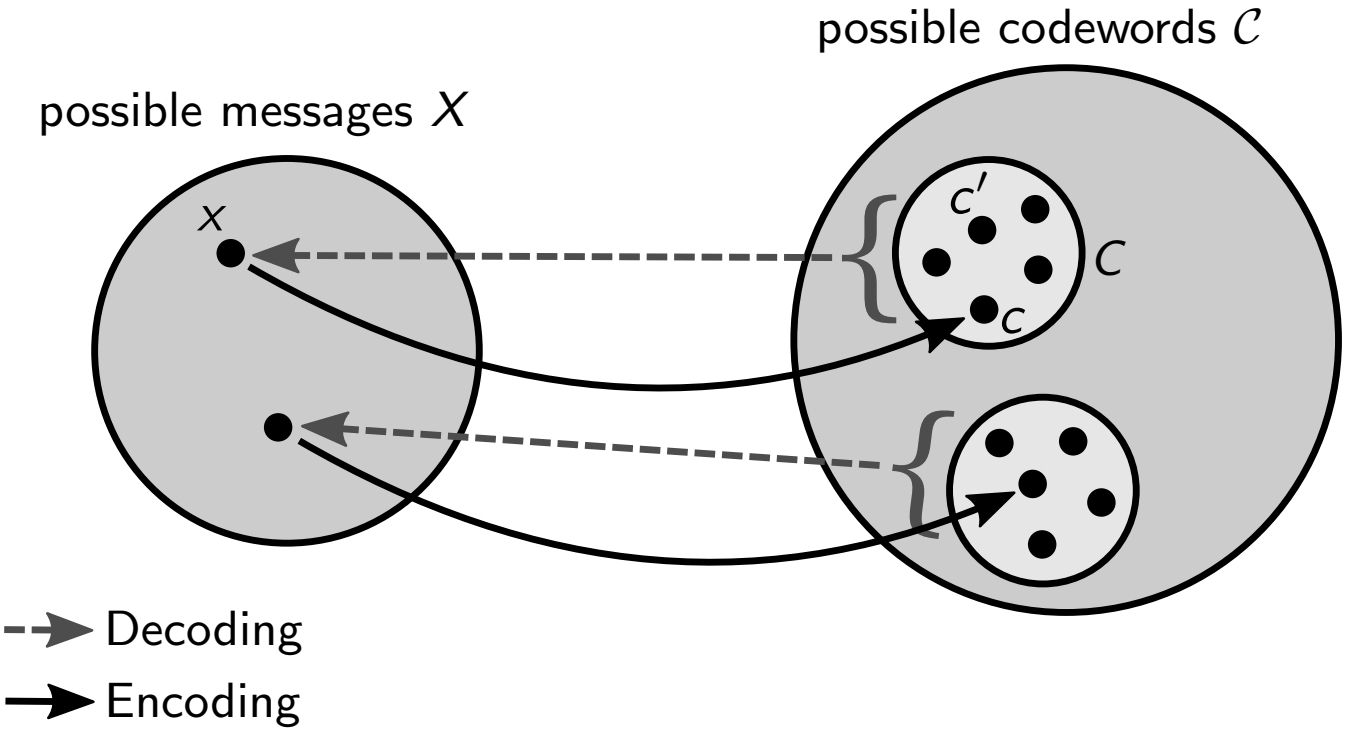
- Synchronisation of context data with zero data transmission
- Case study on audio-based secure pairing

Conclusion

Questions?

Stephan Sigg
sigg@nii.ac.jp

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