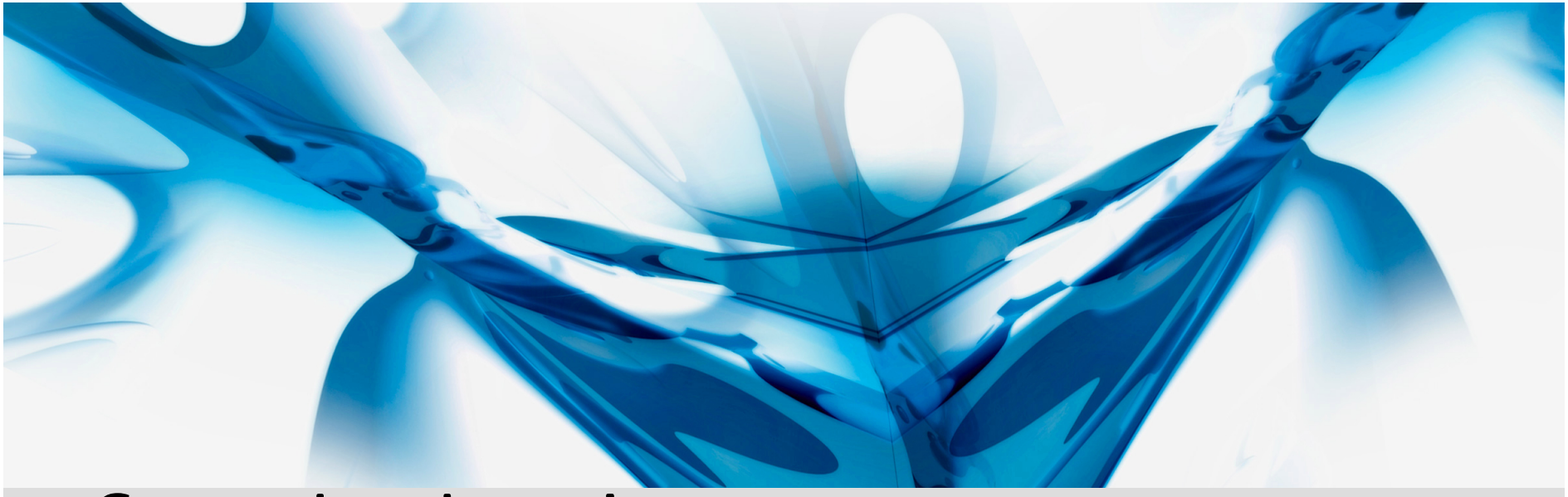
大学共同利用機関法人 情報・システム研究機構
国立情報学研究所
National Institute of Informatics

Information Systems
Architecture Science
Research Division



Context-based security

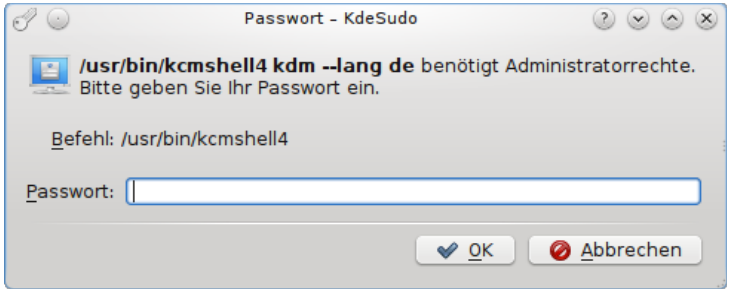
State of the art, open research topics and a case study

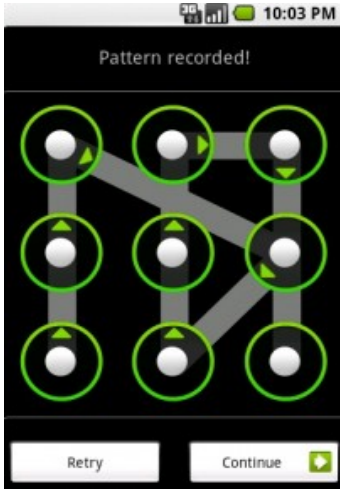
Stephan Sigg

The fifth International Workshop on Context-Awareness for Self-Managing Systems,
CASEMANS 2011, 18.09.2011, Beijing, China

Motivation

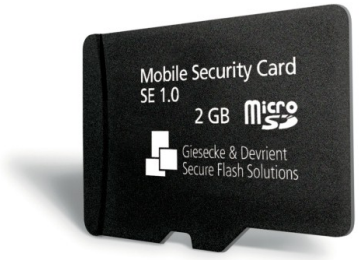
Security demands are omnipresent and increasing in number





Motivation

Threats + requirements for security precautions increase simultaneously

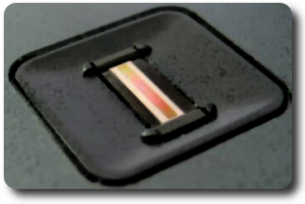


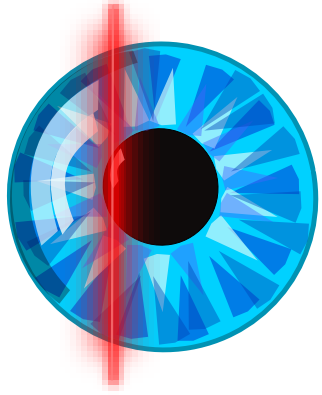
Have you ever...

- lost/forgot your password?
- wondered that the password has to be exchanged rather frequently
- utilised identical passwords for different accounts
- used weak passwords for convenience
- experienced security precautions as a hassle
- disabled password/pin ? (My phone was delivered with pin disabled by default)

Motivation

We could use biometric data



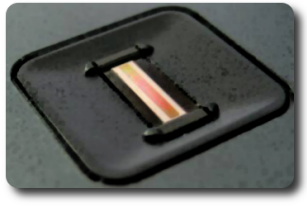


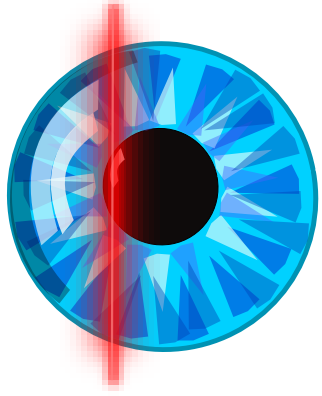
We could use biometric data ...

- Fingerprints
- Iris scan
- DNA
- Face recognition

Motivation

We could use biometric data, BUT ...



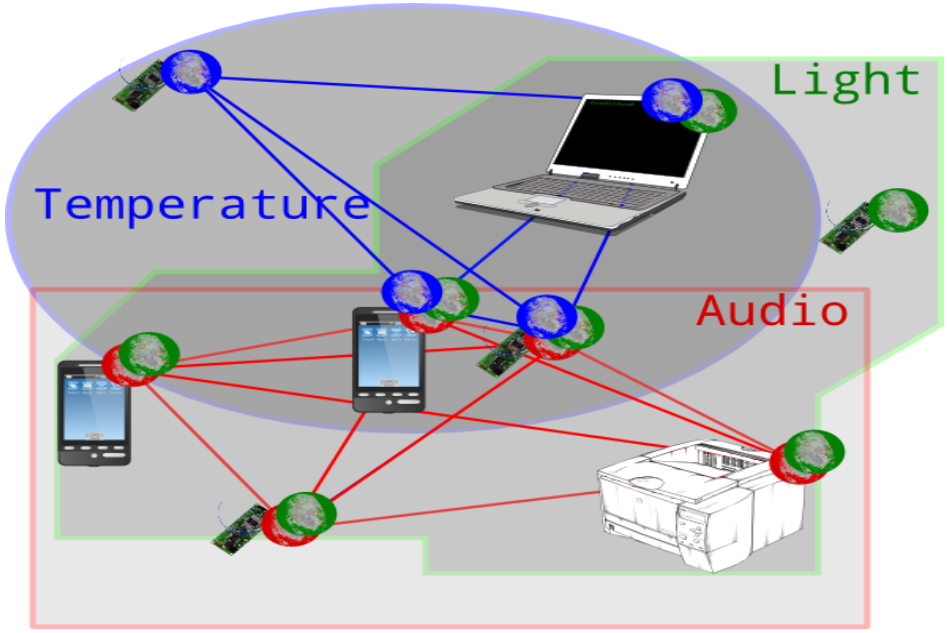


Is this really more secure than the pin/password-based approaches?

- Or is it probably only more convenient?
  - Biometric data shall be easy to obtain/verify by legal authorities but difficult to forge/steal.
  - Commonly, this contradiction is solved in favour of the former aspect for convenience.

Motivation

What are the benefits of using context as a basis of security



- Context is very personalised information
- Context changes frequently with time and location
- We can adapt the security level of applications to their context
- Less obtrusive but at the same time more secure?

Aspects of security through context

Password-less authentication

- Context data is not forgotten like pins
- Enables new/intelligent, potentially intuitive security schemes
- High entropy has to be guaranteed
- Provide less-/un-obtrusive security schemes
- Prevent people from using weak passwords

Location is an important context

- Current applications location dependent

Privacy concerns

- People have grown sensitive to providing personal information
- Privacy threads are perceived differently [1]

[1] L. Nehmadi, J. Meyer. A system for studying usability of mobile security. *Third International Workshop on Security and Privacy in Spontaneous Interaction and Mobile Phone Use*, in conjunction with Pervasive 2011, 2011

Outline

Motivation

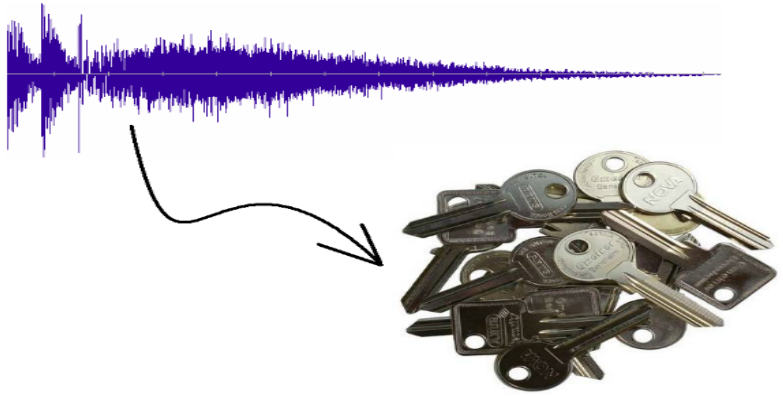
Audio as a key

Case study

Conclusion

Audio as a key

Using audio for device authentication

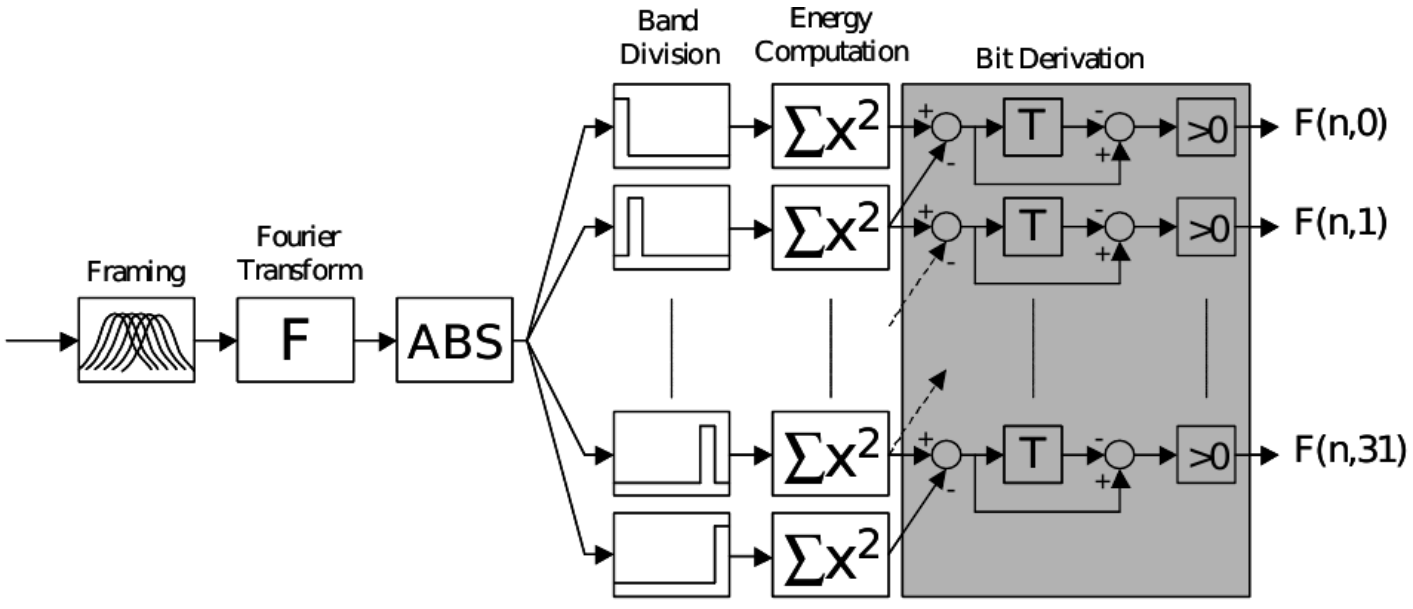


- Can we use ambient audio from devices in proximity as a common secret for device pairing?
  - Establish trust-based perception of security among mobile devices [2].
  - Establish ad-hoc secure channel among devices (non-interactive)
  - Establish a simplified and less-/un-obtrusive security mechanism
  - Switch among several security levels-based on context

[2] C. Dupuy, A. Torre. Local clusters, trust, confidence and proximity, Clusters and Globalisation: The development of urban and regional economies, pp. 175–195, 2006.

Audio as a key

Audio fingerprints for device pairing



- Create audio fingerprints as features for ambient audio [3]
- Utilise error correcting codes to account for differences in fingerprints

[3] A. Wang. An Industrial Strength Audio Search Algorithm, *International Conference on Music Information Retrieval*, 2003

Audio as a key

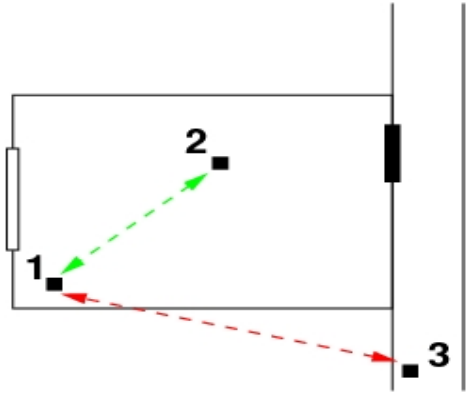
Audio fingerprints for device pairing

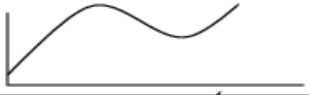
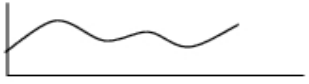
- An audio fingerprint is-based on the fluctuation in energy differences in adjacent frequency bands over time
  - Tolerant for low noise and changes in absolute energy

$$f(i,j) = \begin{cases} 1 & \text{if } E(i,j) - E(i,j+1) - \\ & (E(i-1,j) - E(i-1,j+1)) > 0, \\ 0 & \text{otherwise.} \end{cases}$$

Audio as a key

Using audio for device authentication

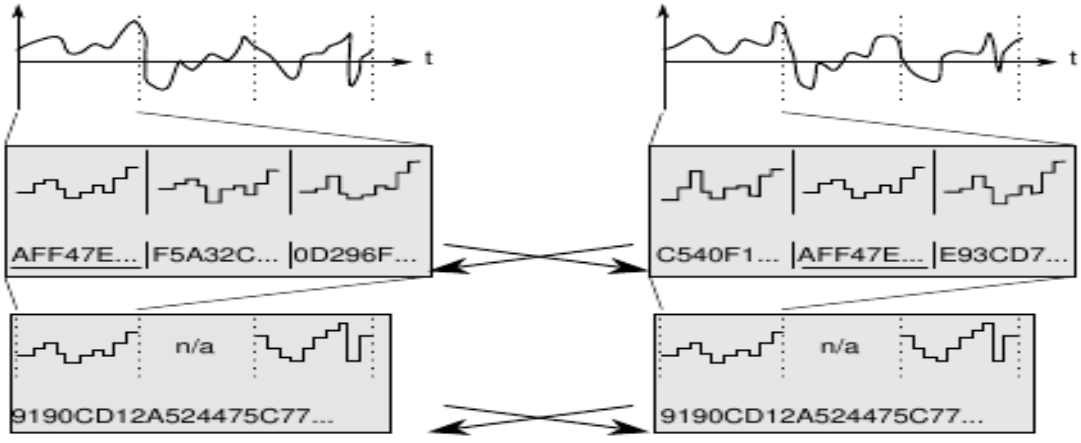


ID	Captured audio	Key
1		1100101000101
2		1000101010001
3		0001000110011

- Issues
  - Context is a noisy source.
    - Measurement inaccuracies
    - Often strict time or location dependence
    - Classification inaccuracies
  - Accurate time synchronisation required

Audio as a key

Current approaches



- The Candidate key protocol[4]
  - Acceleration data of shaking processes
  - Iterative key generation
- Hamming distance among binary keys [5]

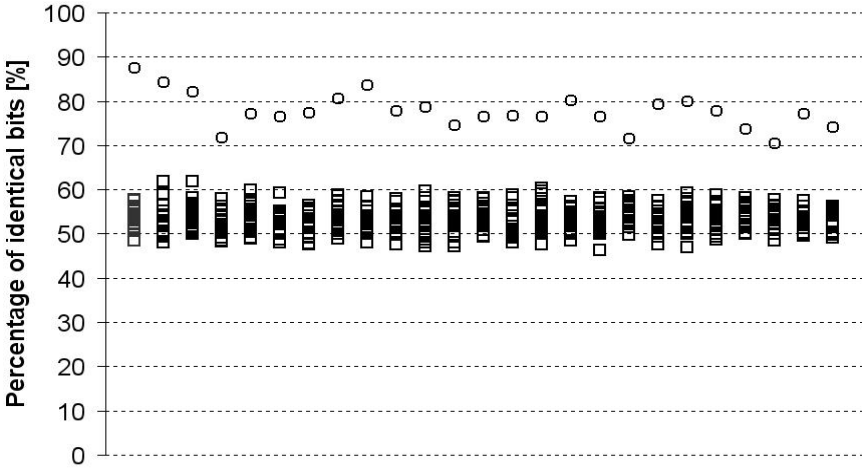
[4] Rene Mayrhofer. The Candidate Key Protocol for Generating Secret Shared Keys from Similar Sensor Data Streams, *Security and Privacy in Ad-hoc and Sensor Networks*, pp. 1–15, 2007

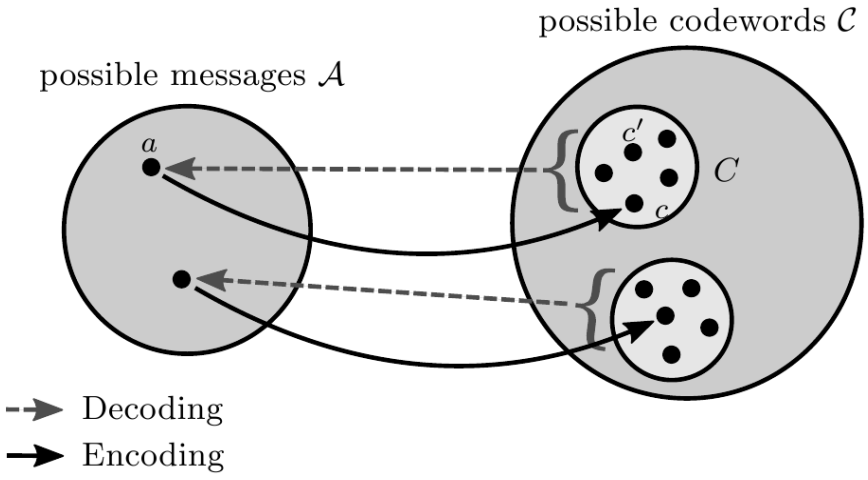
[5] D. Bichler, G. Stromberg, M. Muemer. Key generation-based on acceleration data of shaking processes, *9th international Conference on Ubiquitous Computing*, 2007.

Audio as a key

Device pairing with fuzzy cryptography

- The received fingerprint at two devices is not identical due to
  - Recording errors
  - Timing errors
  - Noise





Outline

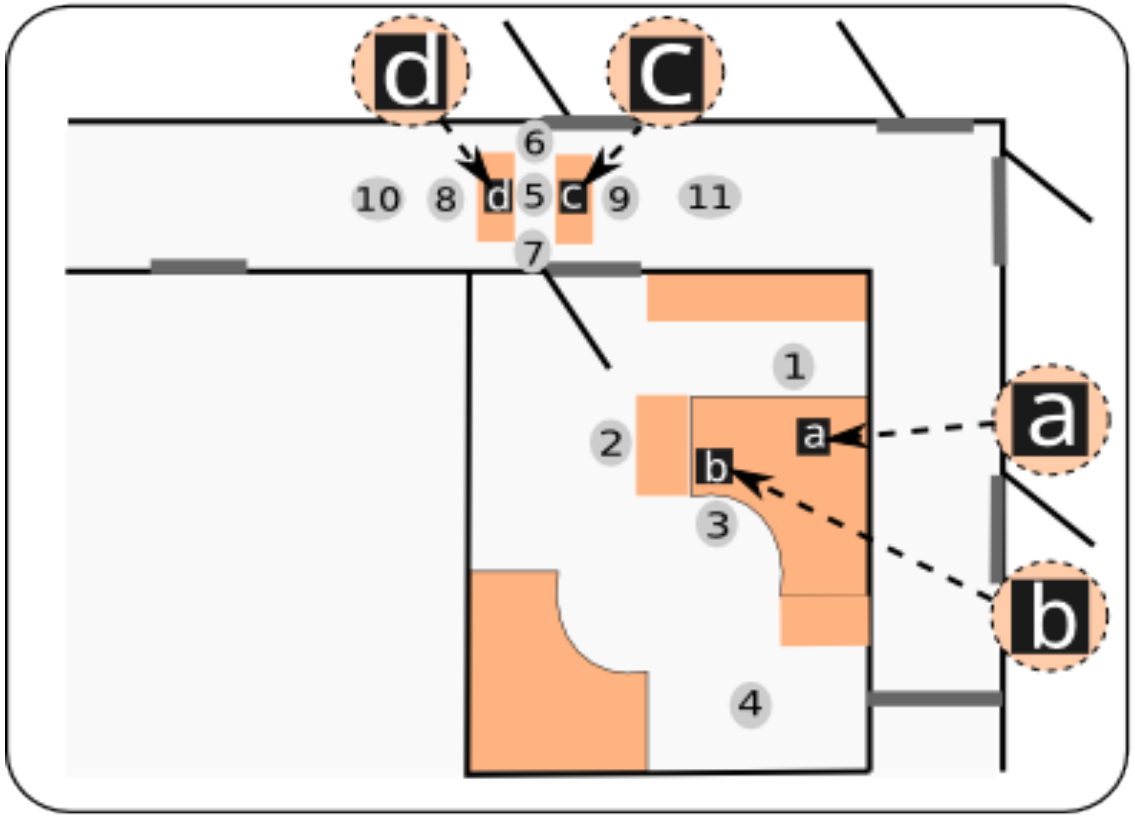
Motivation

Audio as a key

Case study

Conclusion

Case study

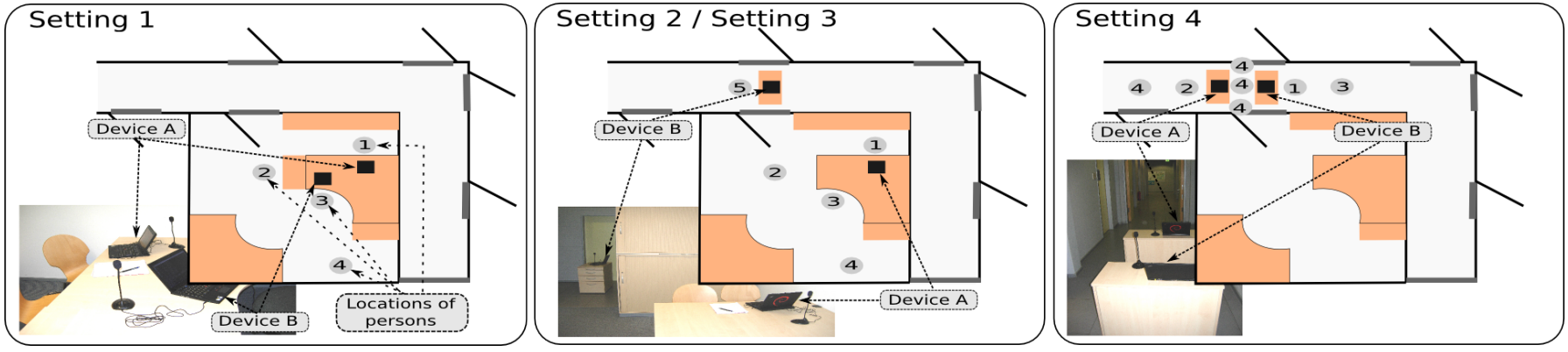


Case study

- We utilised Reed-Solomon error correcting codes in order to account for these bit errors ($RS(q, m, n)$)
  - $\mathcal{A} = \mathbb{F}_q^m, \mathcal{C} = \mathbb{F}_q^n : q$ prim.
- in conjunction with the Secure Hash Algorithm with 256 bit (SHA-256)

Microphones			
Impedance			$\leq 22\ \mathrm{k}\Omega$
Current consumption			$\leq 0.5\ \mathrm{mA}$
Frequency response			$100\ \mathrm{Hz} \sim 16\ \mathrm{KHz}$
Sensitivity			$-38\ \mathrm{dB} \pm 2\ \mathrm{dB}$
Scenarios	Scenario 1	Scenario 2/3	Scenario 4
Microphone distance	$\approx 1\ \mathrm{m}$	$\approx 4\ \mathrm{m}$	$\approx 1\ \mathrm{m}$
Distance to speaker	$.8\ \mathrm{m} - 3\ \mathrm{m}$	$.8\ \mathrm{m} - 4\ \mathrm{m}$	$.5\ \mathrm{m} - 3\ \mathrm{m}$

Case study

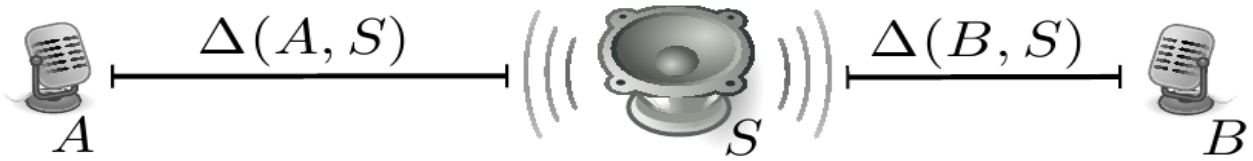


Scenarios	1	2	3	4
Successful attempts	0.9	0.4	0.0	0.8
Bit errors corrected (∅)	179.6	170.75	–	173.75

Case study

Audio playback can improve success rate for low ambient audio

- Controlled Indoor environment
- Microphones attached to left and right ports of an audio card (1.5m, 3m, 4.5m, 6m)
- Audio source (music, clap, snap, speak, whistle)
- Loudness:
  - quiet (*approx* 10 – 23dB)
  - medium (*approx* 23 – 33dB)
  - loud ($\approx$ 33 – 45dB)
- Pairwise comparison of hamming distance: 7500 comparisons; 300 comparisons for simultaneous recordings



Case study

Audio playback can improve success rate for low ambient audio

- m=128
- minimum overlap 62.5%

	Audio sample				
	clap	music	snap	speak	whistle
1	189	192	190	191	191
2	192	192	192	191	191
3	191	188	192	191	–
4	190	192	190	191	192
5	192	190	191	192	–
6	192	191	191	188	192
7	189	190	190	192	192
8	192	186	186	192	192
9	192	189	189	192	189
10	192	196	196	192	–

Case study

Audio playback can improve success rate for low ambient audio

- m=152
- minimum overlap 65%

	Audio sample				
	clap	music	snap	speak	whistle
1	180	179	180	180	–
2	179	179	180	180	180
3	179	–	180	180	178
4	–	–	180	–	180
5	180	180	180	180	179
6	180	180	179	180	180
7	179	180	180	180	180
8	–	178	180	179	180
9	–	179	178	180	180
10	180	179	179	178	179

Case study

Audio playback can improve success rate for low ambient audio

- m= 204
- minimum overlap 70%

	Audio sample				
	clap	music	snap	speak	whistle
1	–	–	–	–	–
2	–	–	–	154	–
3	–	–	153	–	–
4	–	–	–	–	–
5	–	–	–	–	–
6	–	–	154	–	–
7	–	–	–	–	–
8	–	–	–	–	–
9	–	–	–	–	–
10	–	–	–	–	–

Conclusion

- We have demonstrated an unobtrusive mechanism for secure ad-hoc device pairing-based on ambient audio
  - Noise tolerant due to utilisation of error correcting codes
  - Error tolerance is a design parameter
- Audio fingerprint as feature
- Can be generalised to other context classes
- Instrumented and tested on laptop computers
- Entropy: No bias observed in dieHarder statistical tests
- Check our paper for open research issues and opportunities of context-based security

Questions?

Stephan Sigg
sigg@nii.ac.jp