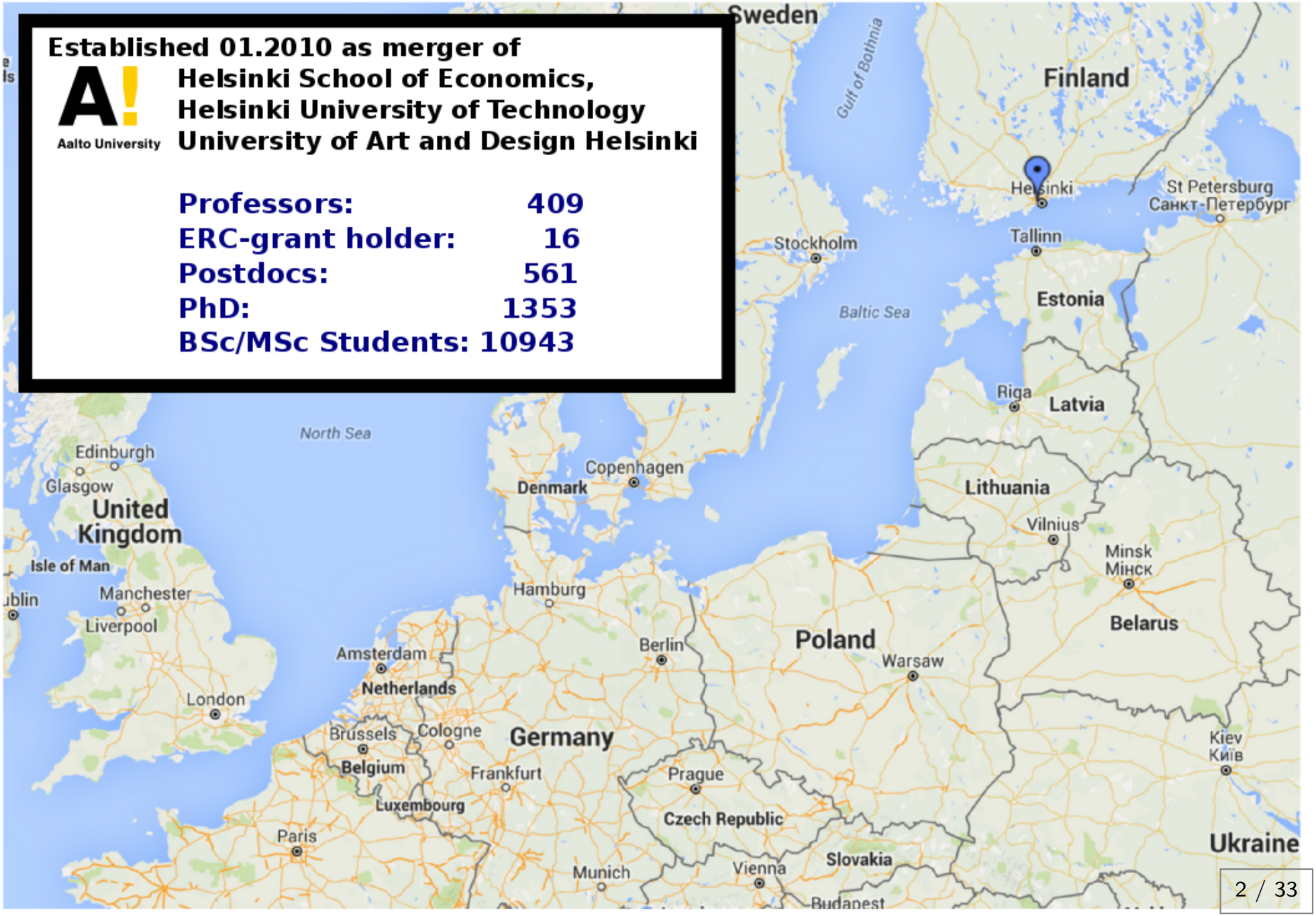
Implicit Fuzzy pairing for ad-hoc usable security

Stephan Sigg

Aalto University, Communications and Networking

June 13, 2016


Sweden
Norway
Finland
Gulf of Bothnia
Helsinki
St Petersburg
Санкт-Петербург
Oslo
Stockholm
Tallinn
Estonia
Baltic Sea
Riga
Latvia
North Sea
Edinburgh
Glasgow
United Kingdom
Copenhagen
Denmark
Lithuania
Vilnius
Minsk
Минск
Isle of Man
Manchester
Liverpool
Hamburg
Belarus
Poland
Berlin
Warsaw
Amsterdam
Netherlands
London
Brussels
Cologne
Germany
Belgium
Frankfurt
Prague
Kiev
Київ
Luxembourg
Czech Republic
Paris
Ukraine
Slovakia
Munich
Vienna
Budapest

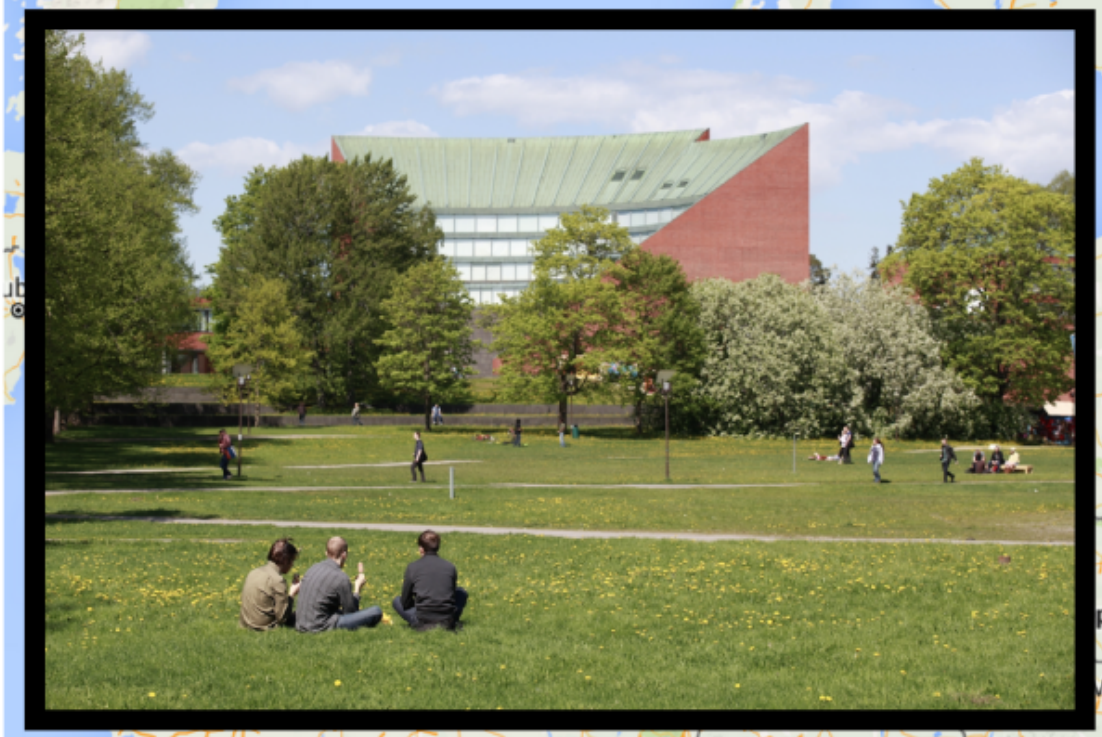

Established 01.2010 as merger of
Aalto University
Helsinki School of Economics,
Helsinki University of Technology
University of Art and Design Helsinki
Professors: 409
ERC-grant holder: 16
Postdocs: 561
PhD: 1353
BSc/MSc Students: 10943
Sweden
Gulf of Bothnia
Finland
Helsinki
St Petersburg
Санкт-Петербург
Tallinn
Stockholm
Baltic Sea
Estonia
Riga
Latvia
North Sea
Edinburgh
Glasgow
United Kingdom
Isle of Man
Manchester
Liverpool
London
Copenhagen
Denmark
Lithuania
Vilnius
Minsk
Минск
Belarus
Hamburg
Berlin
Poland
Warsaw
Amsterdam
Netherlands
Brussels
Cologne
Germany
Belgium
Frankfurt
Prague
Luxembourg
Czech Republic
Paris
Munich
Vienna
Slovakia
Ukraine
Kiev
Київ
Budapest

Established 01.2010 as merger of

Aalto University

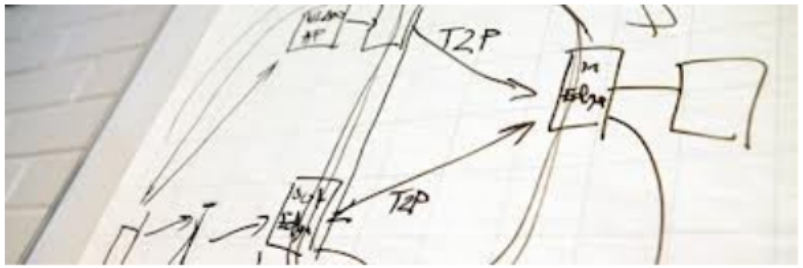
Helsinki School of Economics,
Helsinki University of Technology
University of Art and Design Helsinki

Professors:	**409**
ERC-grant holder:	**16**
Postdocs:	**561**
PhD:	**1353**
BSc/MSc Students:	**10943**



Comnet

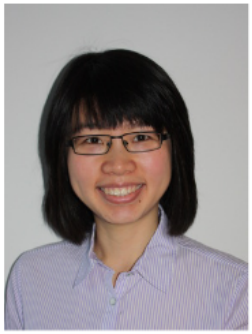
- Personnel: ~115
- 11 + 2 Professors
- budget ~7.8 M€
  ~ 60% external funding
- ~ 55 M.Sc thesis annually
- ~ 8 D.Sc thesis annually



Comnet is a multi-disciplinary unit of research and higher education covering communications and networking technology, networking business and human aspects of communications. In its area, Comnet is the largest unit in Finland.

http://comnet.aalto.fi/en/

Professors



Xiao Yu
Networking software and applications

Stephan Sigg
Ubiquitous computing

Antti Oulasvirta
Human-Computer Interaction
(User Interfaces)

Heikki Hämmäinen
Network Economics

Juuso Töyli
Network economics
Adjunct Prof.

Jarno Limnell
Cyber security
PoP

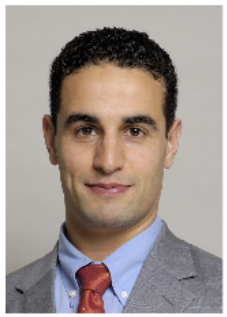
Patric Östergård
Information theory

Olav Tirkkonen
Communications theory

Riku Jäntti
Commuications Engineering
Head of department

Jyri Hämäläinen
Radio communications
Dean of ELEC

Raimo Kantola
Networking technology
Routing, trust, and privacy



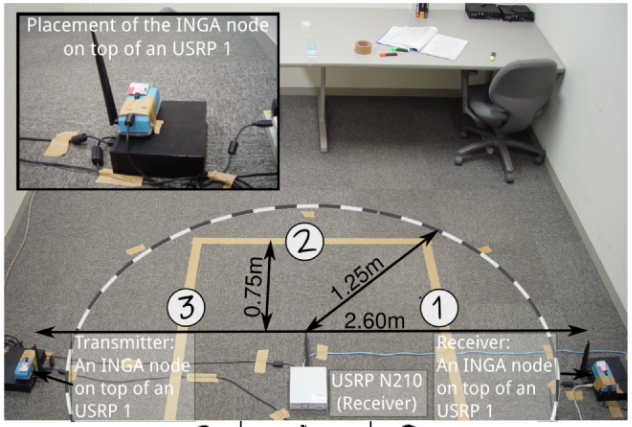
Tarik Taleb
Mobile Core Networks
Network Function Virtualization and Cloud Communications

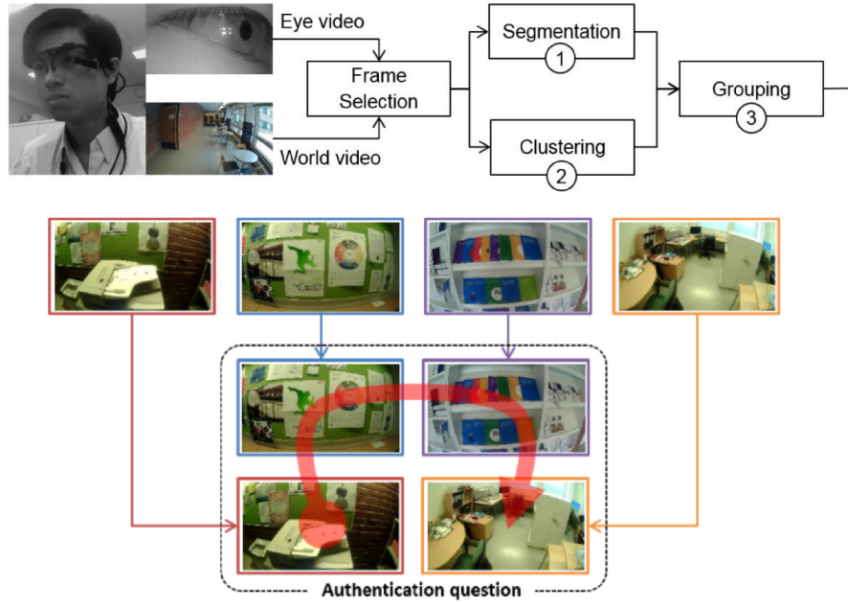
Jukka Manner
Internet technologies
Transport

Aalto University
School of Electrical Engineering

Comnet
6/8/16
3

Ambient Intelligence





Stephan Sigg

Randomized Algorithms, Optimization, Usable security, Activity recognition, Machine learning, Pervasive Computing

Le Ngu Nguyen

Usable Security, Activity recognition, Machine learning, Mobile applications

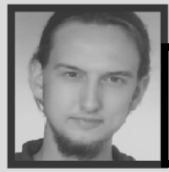
Bahareh Gholampooryazdi

Signal processing, RF-based Device-free activity recognition

Muneeba Raja

Sentiment sensing, Device-Free RF-based Activity recognition, Pervasive Computing

Visitors

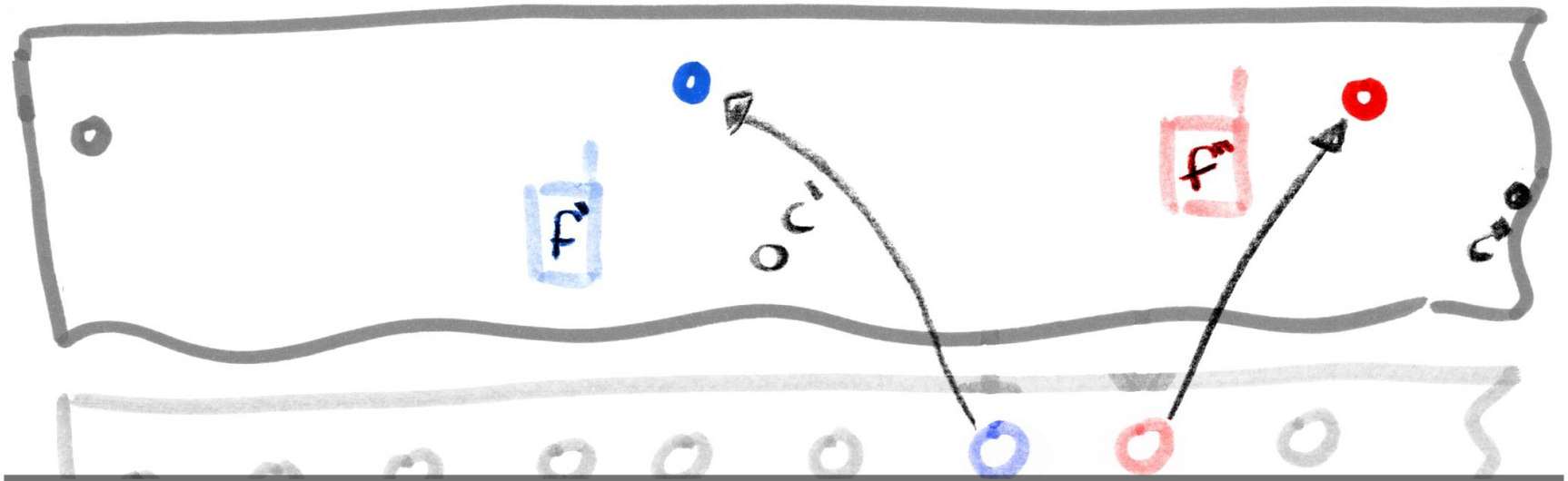


Dominik Schuermann

Security in DTN, Anonymity in decentralized networks, Authenticated Key Exchange Usable security

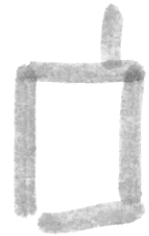
Arne Bruesch

Machine learning, Information systems, Ad-hoc secure device pairing, Inertial sensors

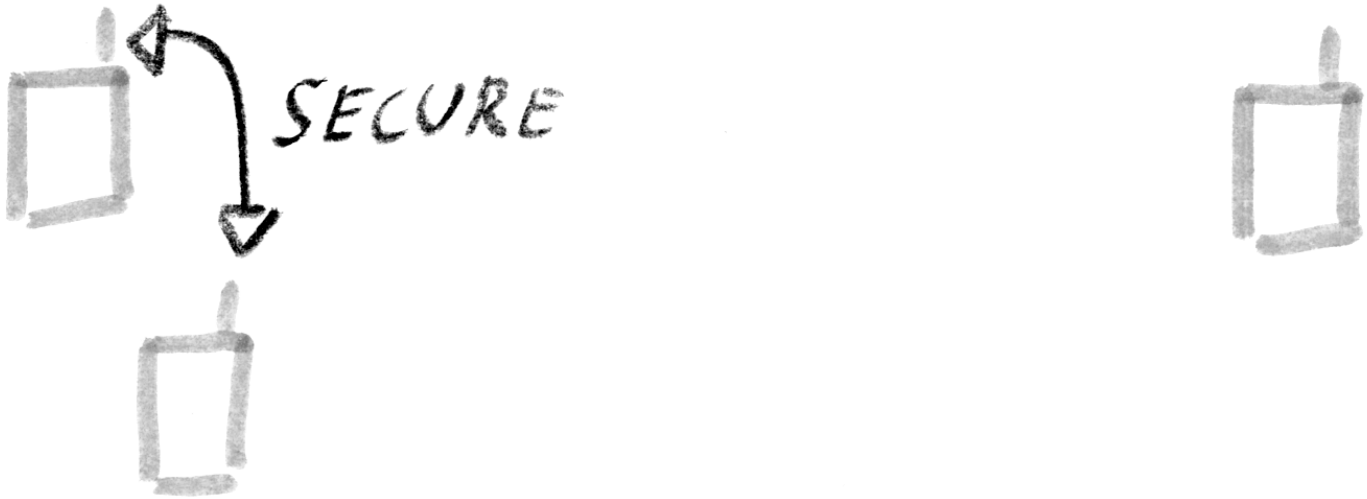


Secure spontaneous authentication from ambient audio

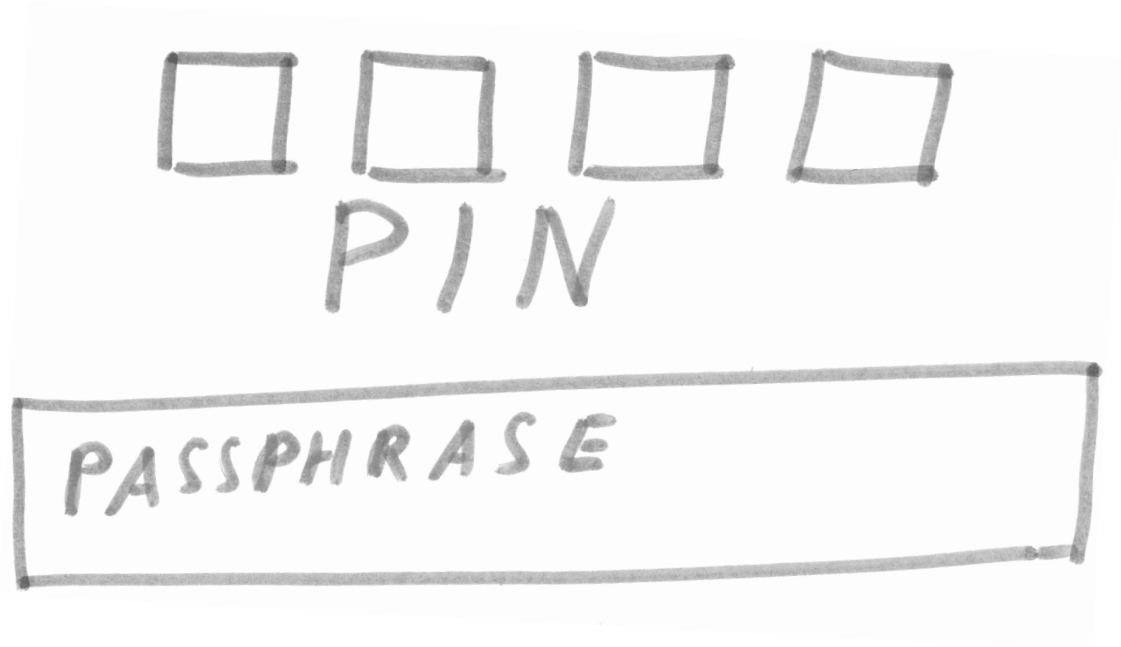
Motivation



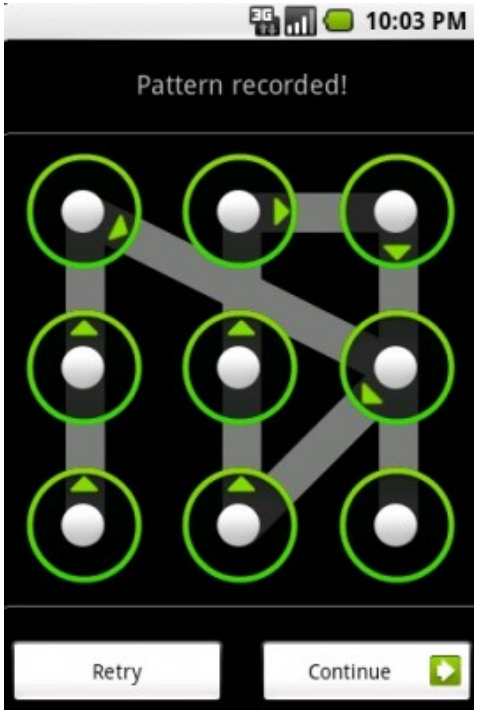
Motivation

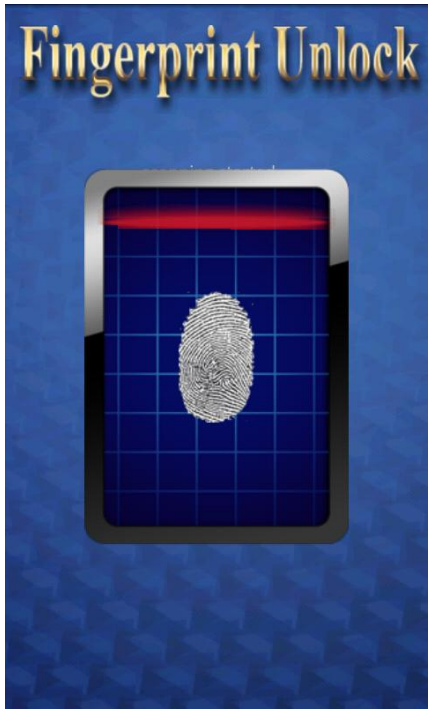


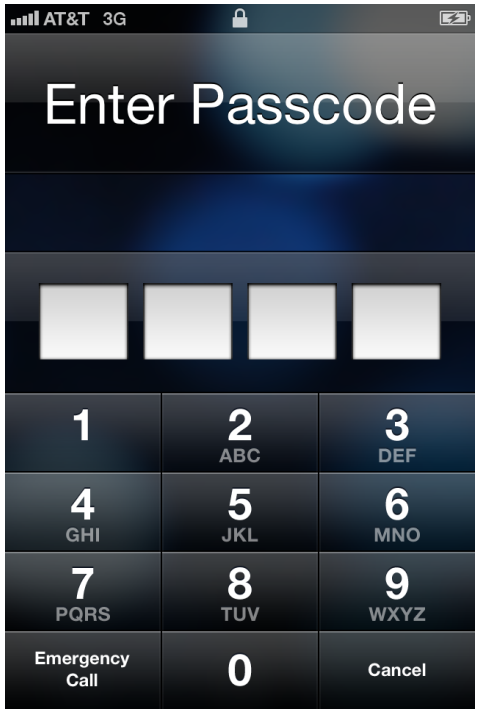
Motivation



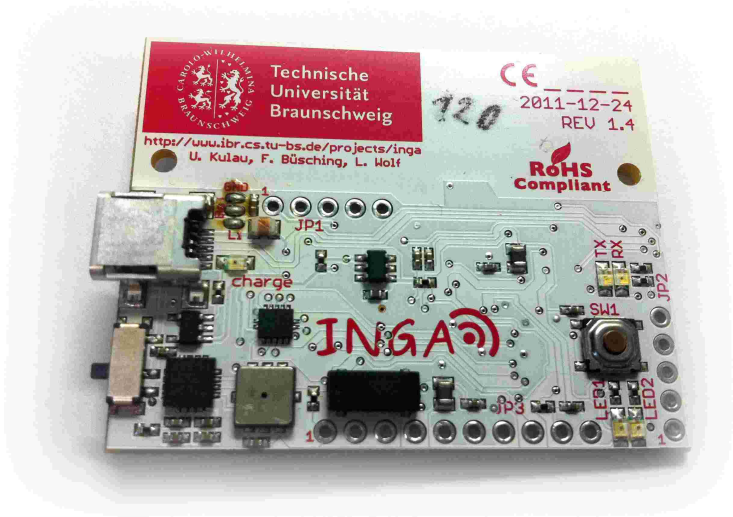
Motivation


10:03 PM
Pattern recorded!
Retry
Continue


Fingerprint Unlock


AT&T 3G
Enter Passcode
1
2 ABC
3 DEF
4 GHI
5 JKL
6 MNO
7 PQRS
8 TUV
9 WXYZ
Emergency Call
0
Cancel

Motivation


Technische
Universität
Braunschweig
https://www.ibr.cs.tu-bs.de/projects/inga
U. Kulau, F. Büsching, L. Wolf
2011-12-24
REV 1.4
RoHS
Compliant
JP1
charge
INGA
SW1
JP2
JP3
LED1
LED2
TX
RX

Motivation

Motivation


IOT
my crib has WiFi
huc · 99
iPod
Music
Extras
Settings
Shuffle Songs
Backlight
Wi Fi
FUTURE STORE INITIATIVE
Bananen
REISEPASS

Motivation

Trust and proximity

We will use audio as a source of common information in proximity

Motivation

Trust and proximity

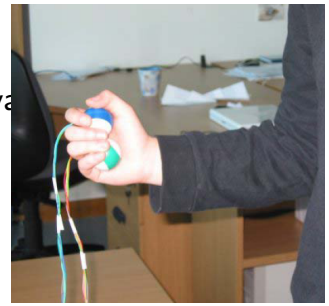
We will use audio as a source of common information in proximity

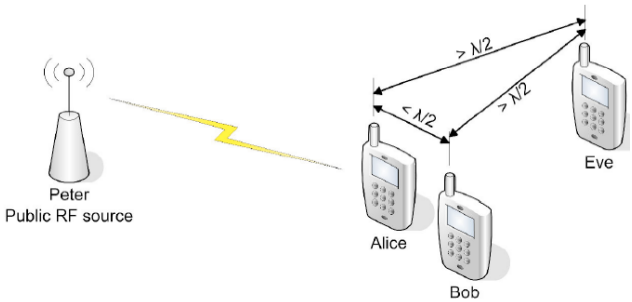
Security from environmental stimuli

Shake well before use[a]

[a] R. Mayrhofer et al., Shake well before use: Authentication based on Accelerometer data, Pe va

- Accelerometer data
- Secure key by iterative exchange of hashed key-sub-sequences





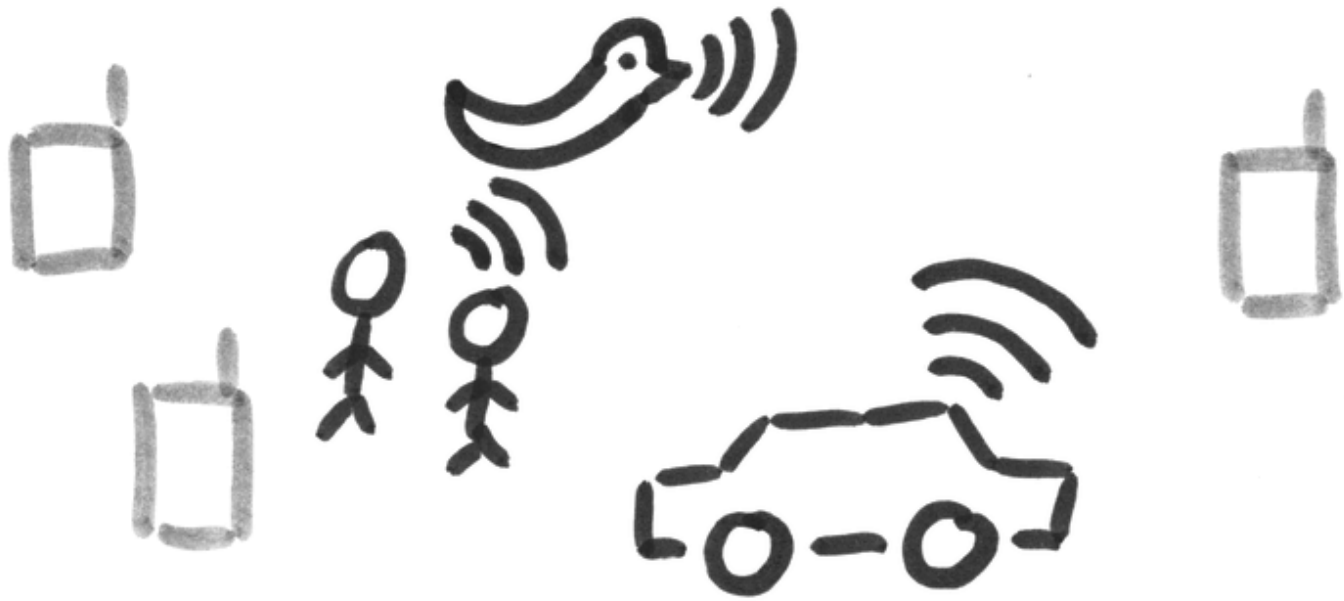
RF-based ad-hoc secure device pairing[a]

[a] S. Mathur et al., ProxiMate: proximity-based secure pairing using amb ent

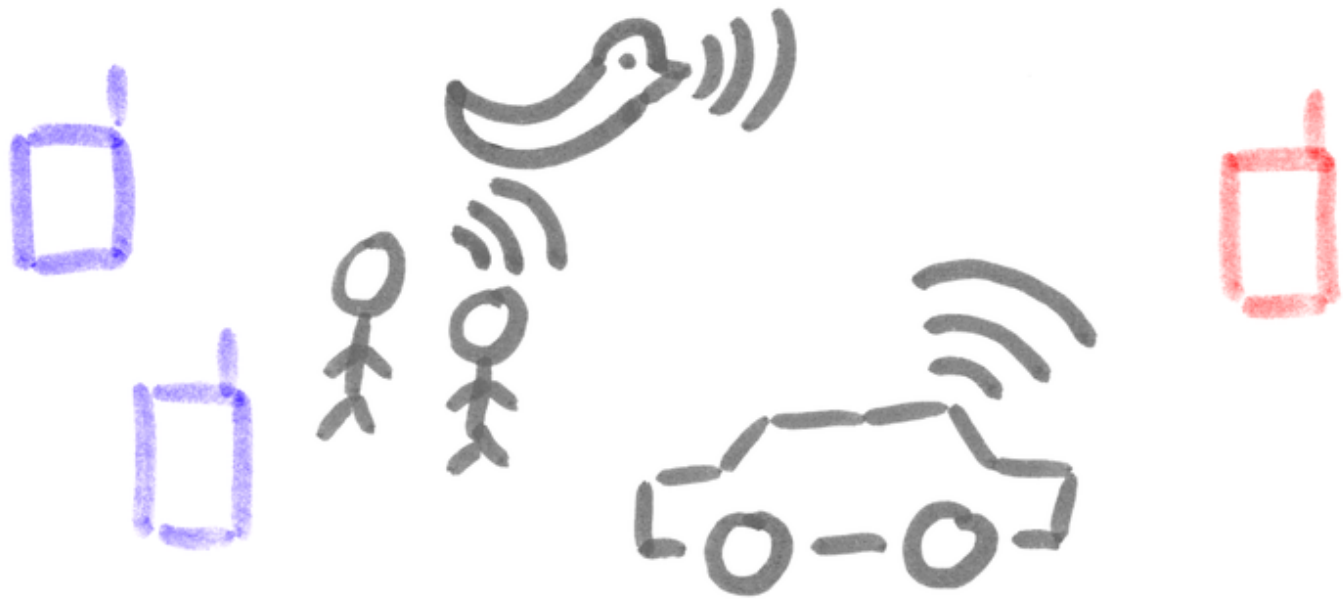
- Utilise error correcting codes
- Public RF-source

Spontaneous audio-based device pairing

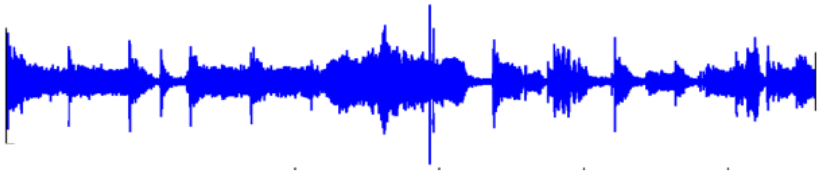
Spontaneous audio-based device pairing



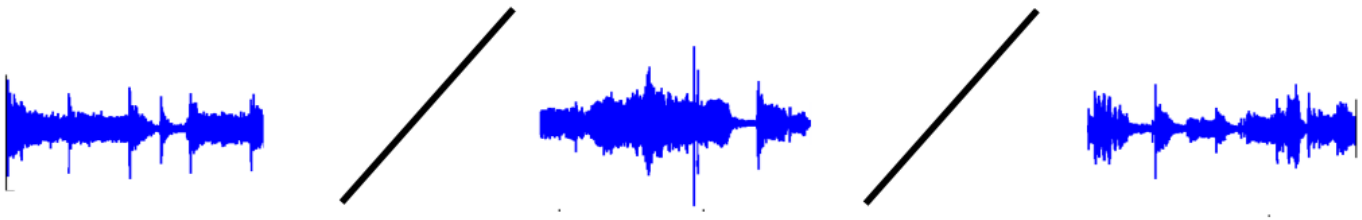
Spontaneous audio-based device pairing



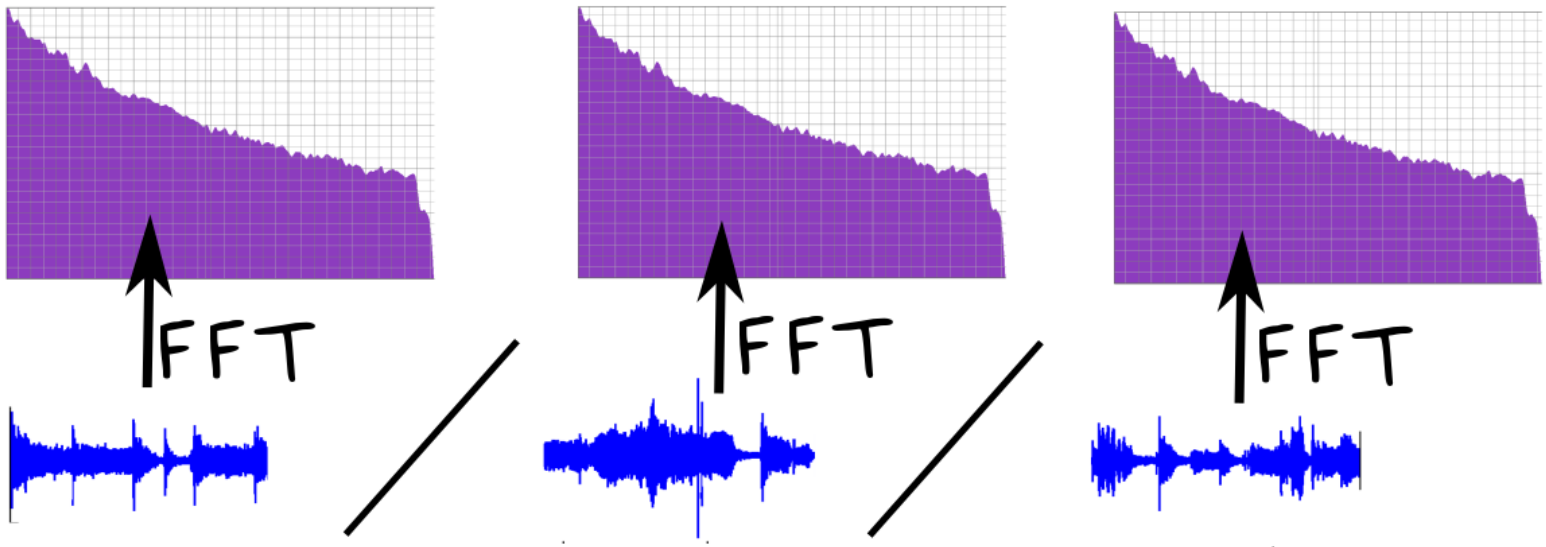
Spontaneous audio-based device pairing



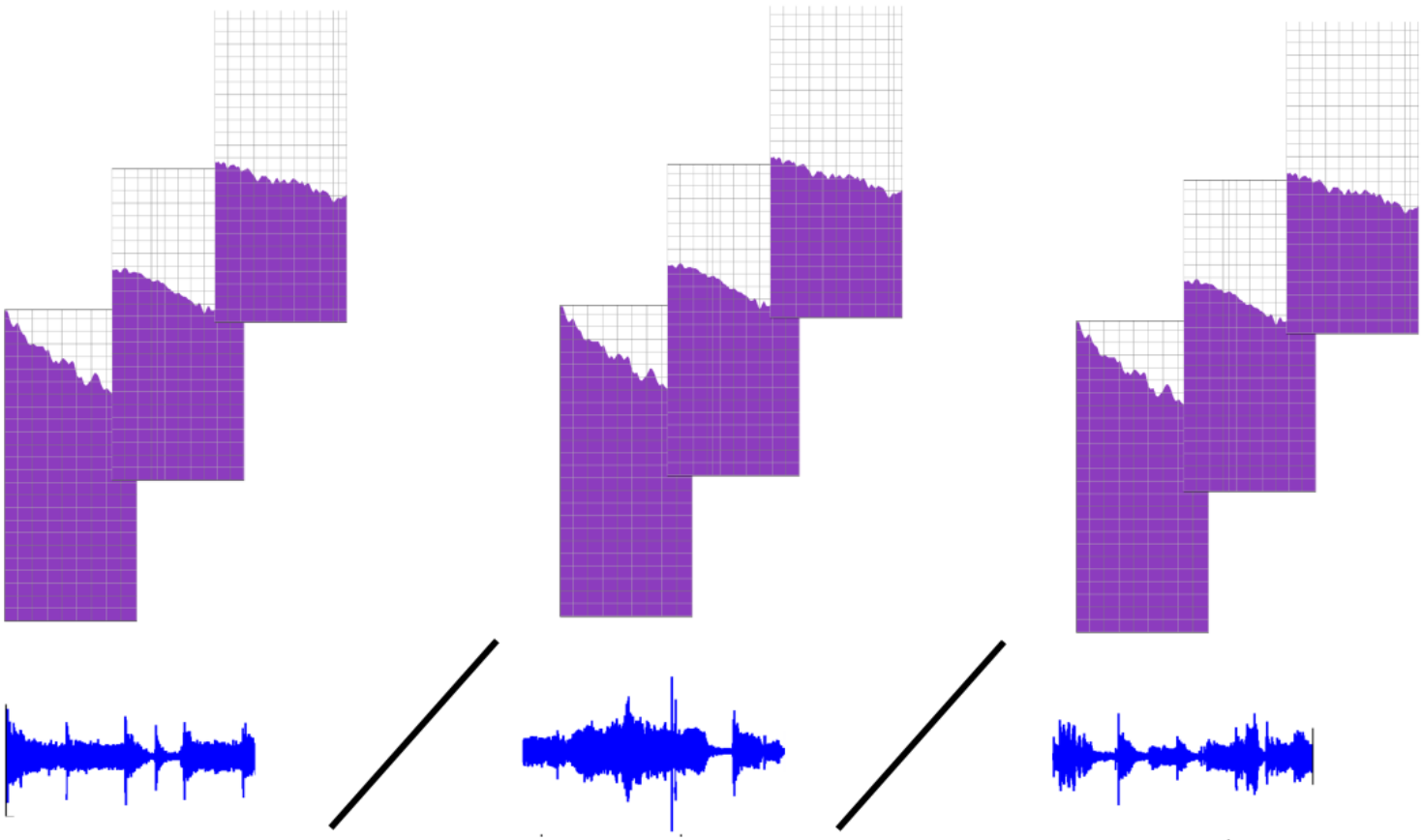
Spontaneous audio-based device pairing



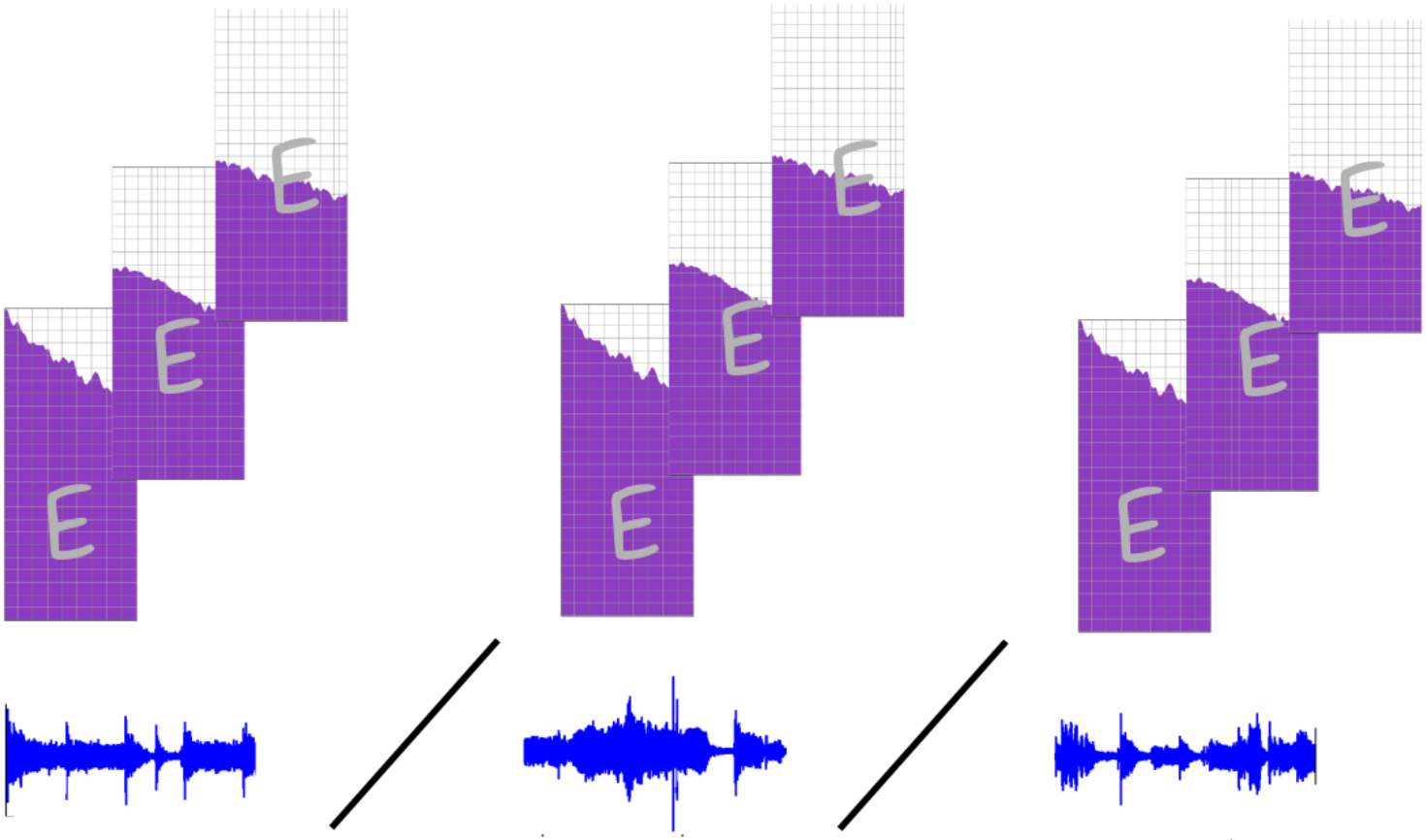
Spontaneous audio-based device pairing



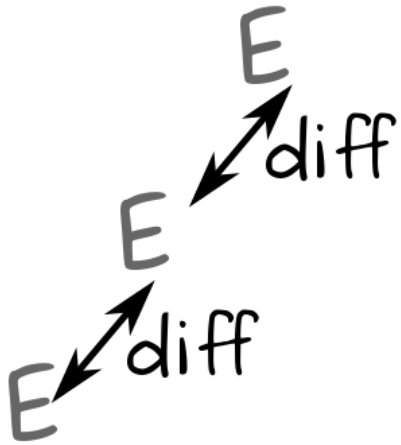
Spontaneous audio-based device pairing

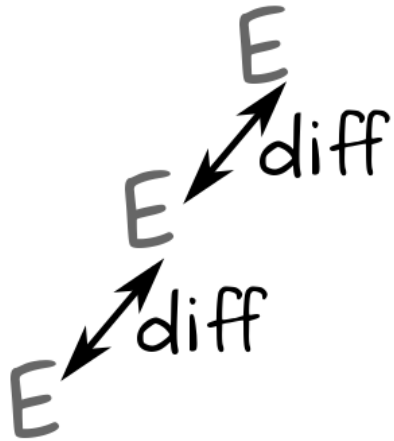


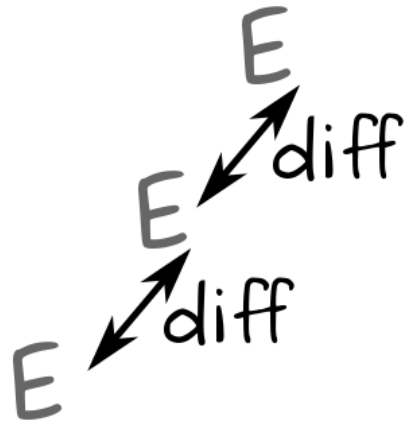
Spontaneous audio-based device pairing



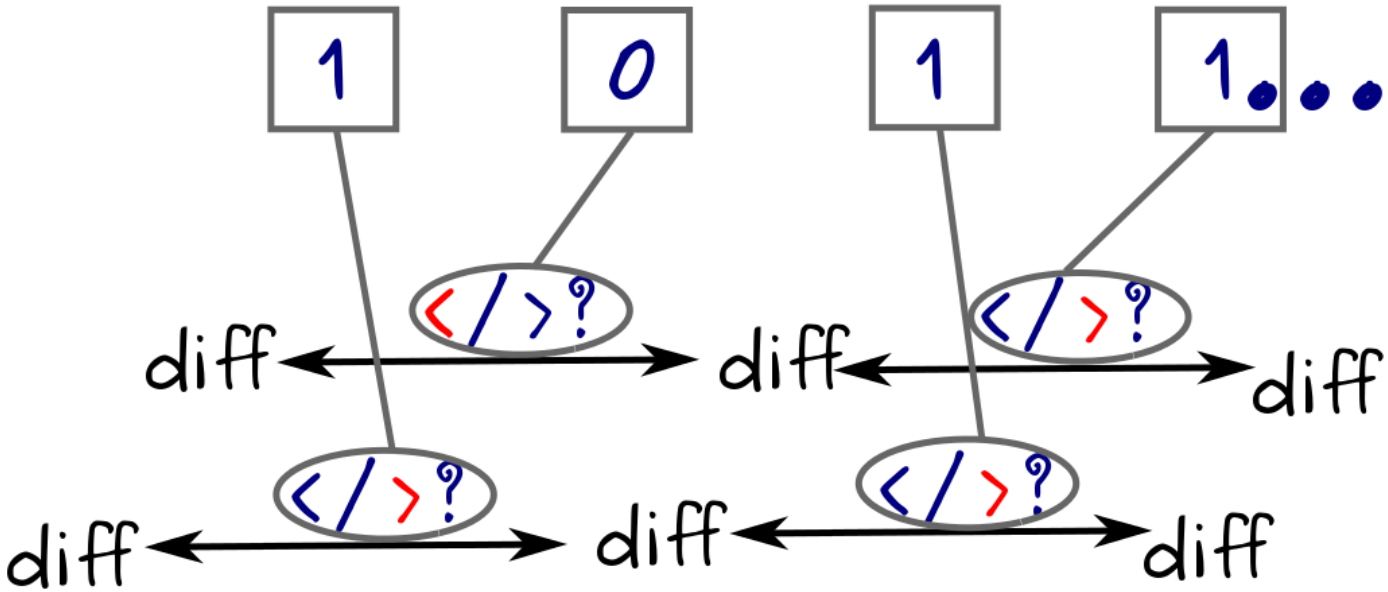
Spontaneous audio-based device pairing





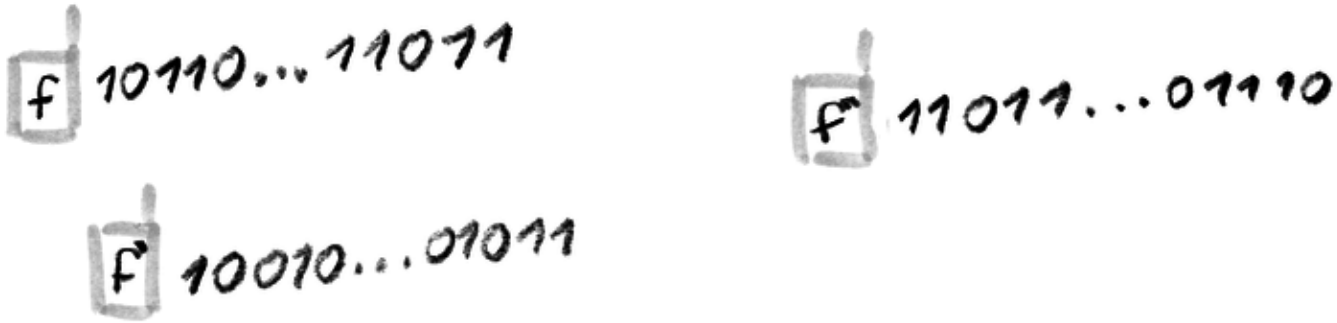


Spontaneous audio-based device pairing

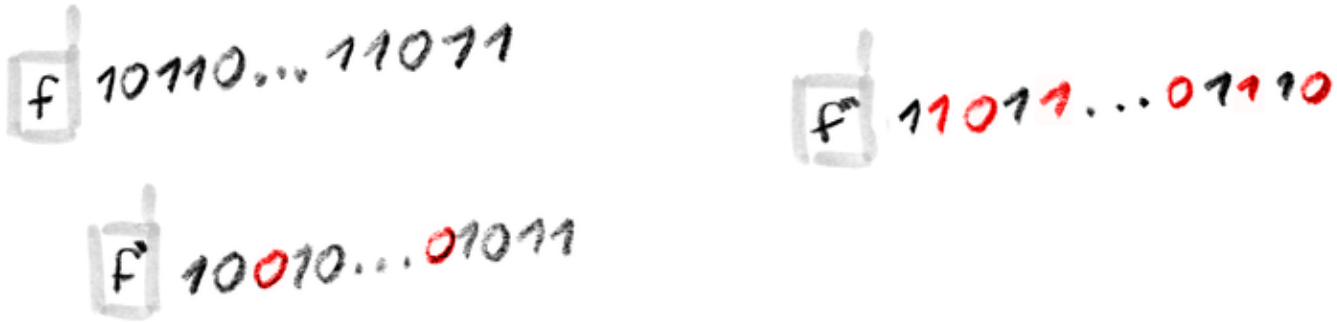


Spontaneous audio-based device pairing

Spontaneous audio-based device pairing

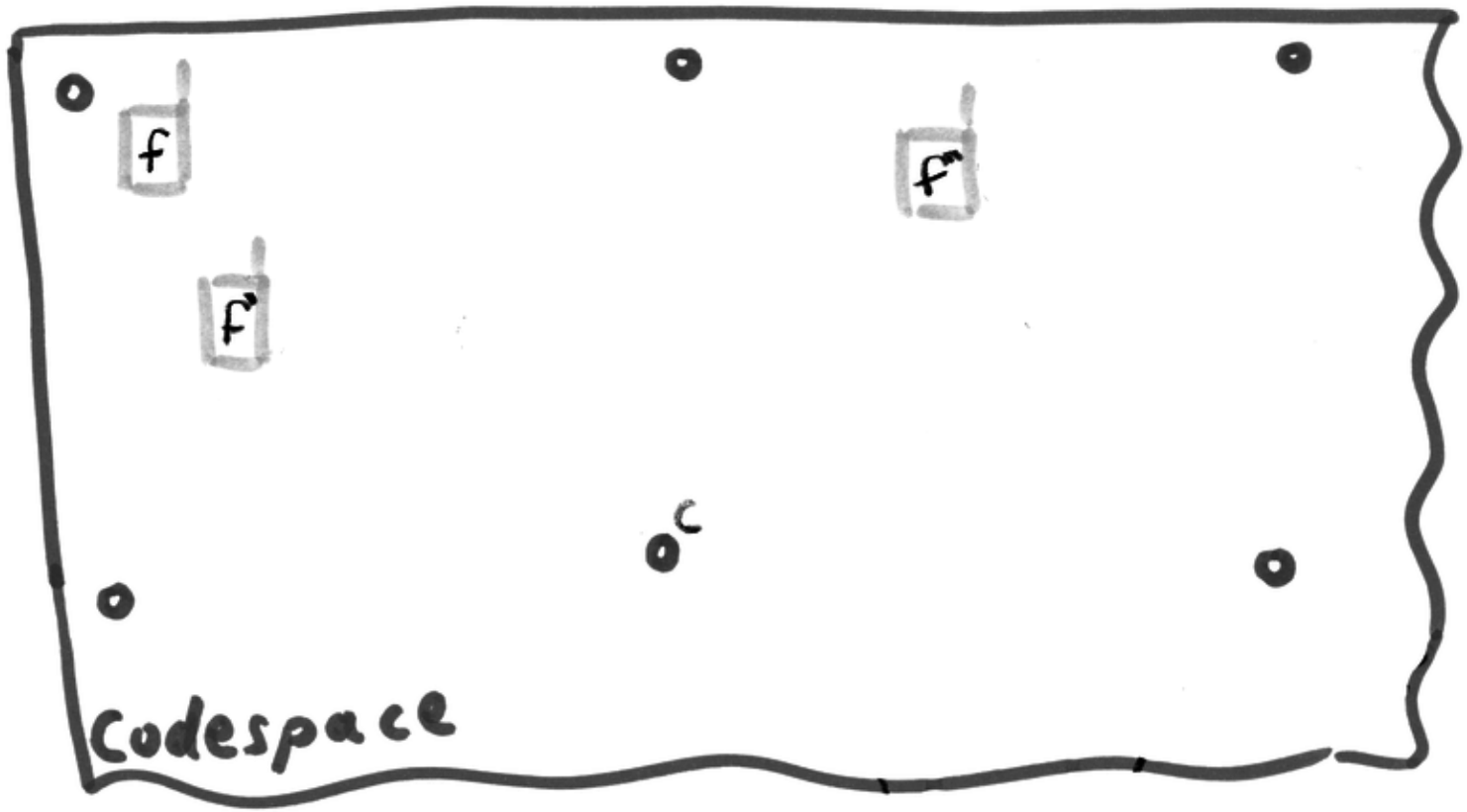


Spontaneous audio-based device pairing

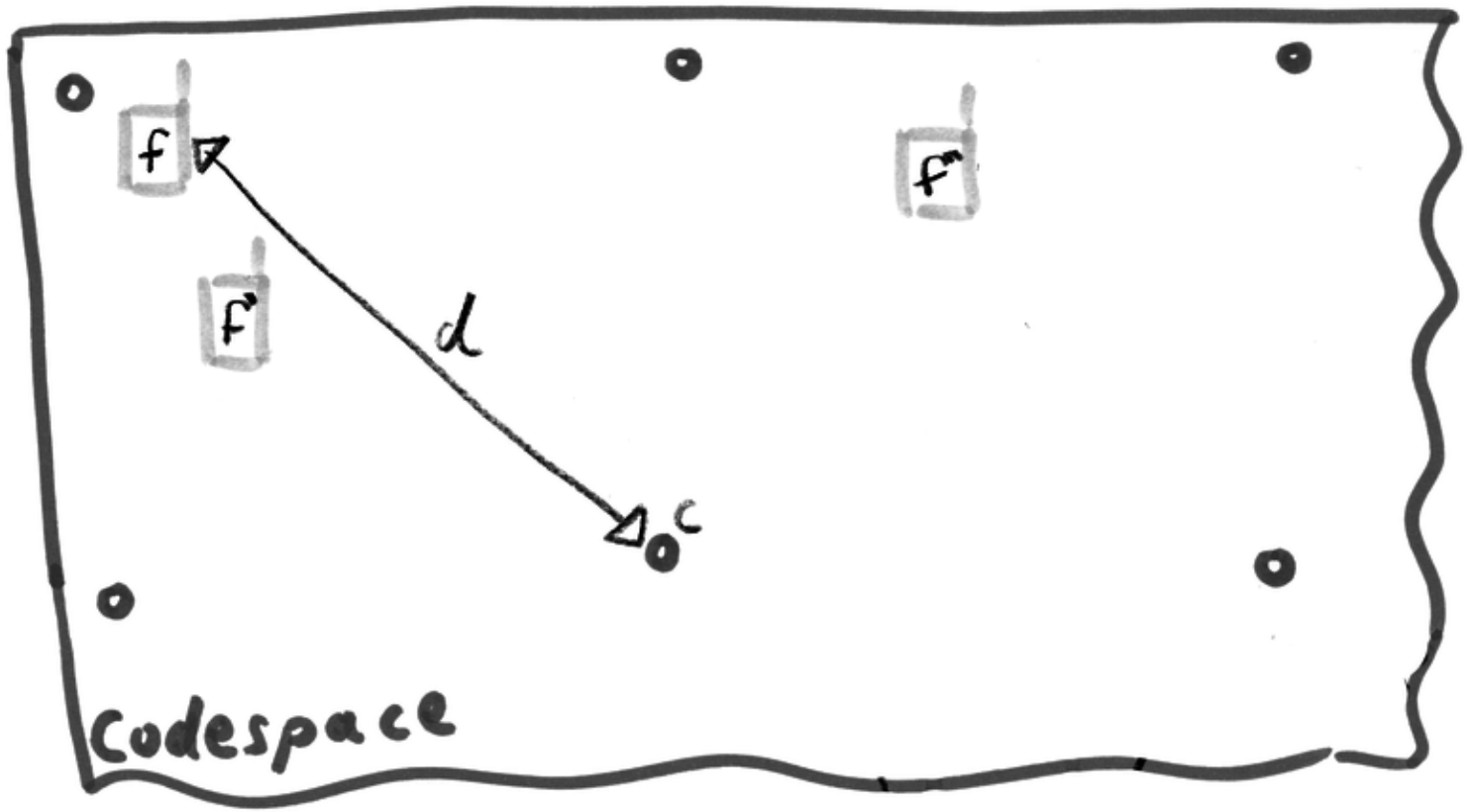


Spontaneous audio-based device pairing

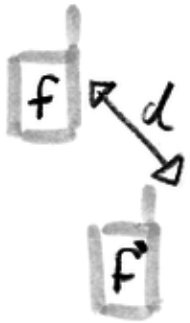
Spontaneous audio-based device pairing



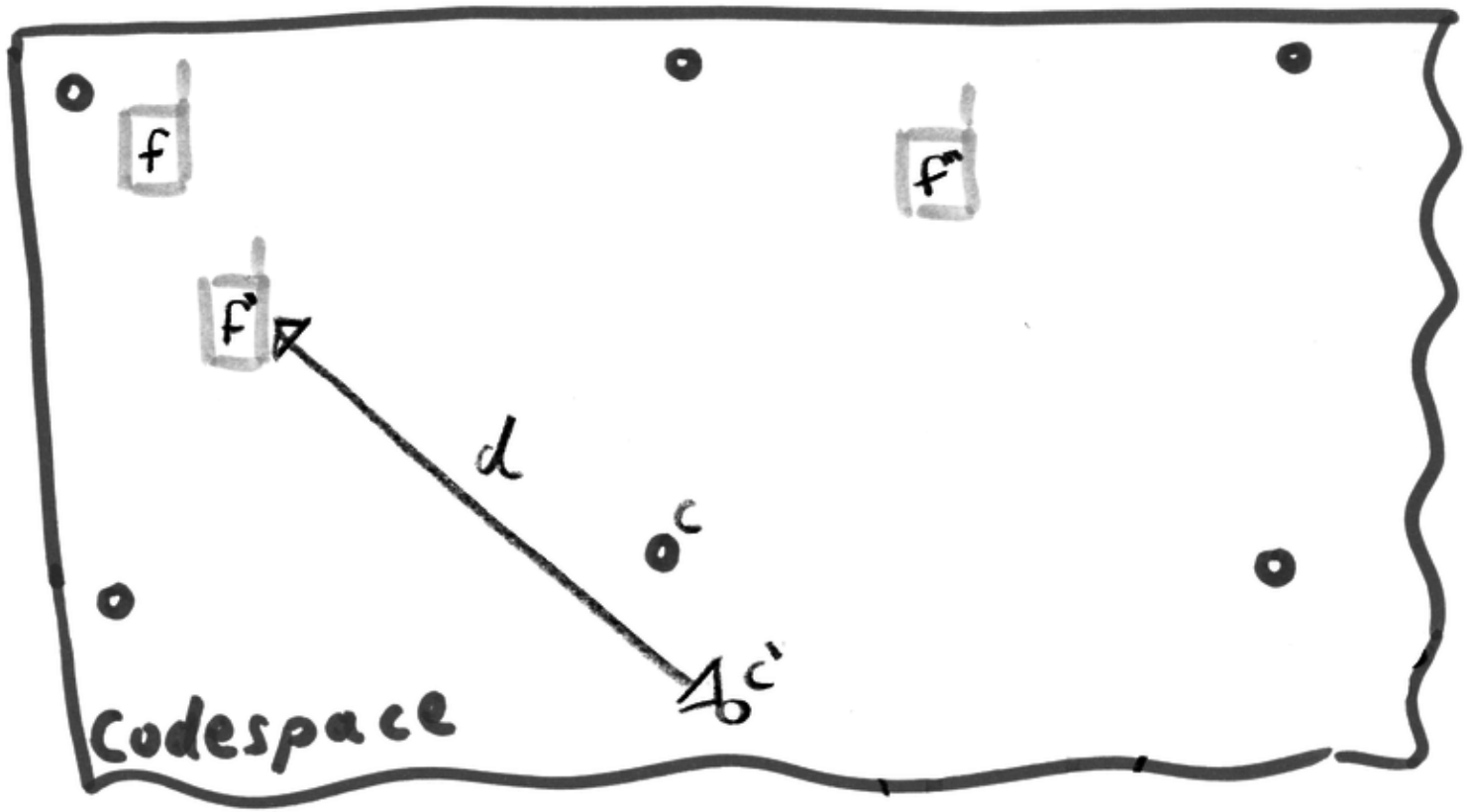
Spontaneous audio-based device pairing



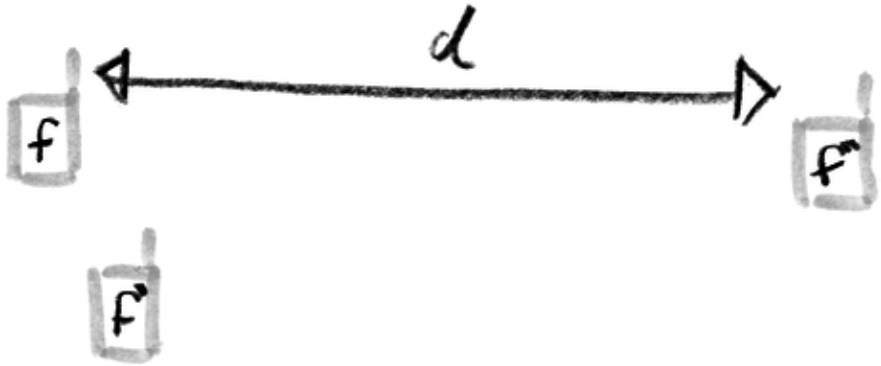
Spontaneous audio-based device pairing



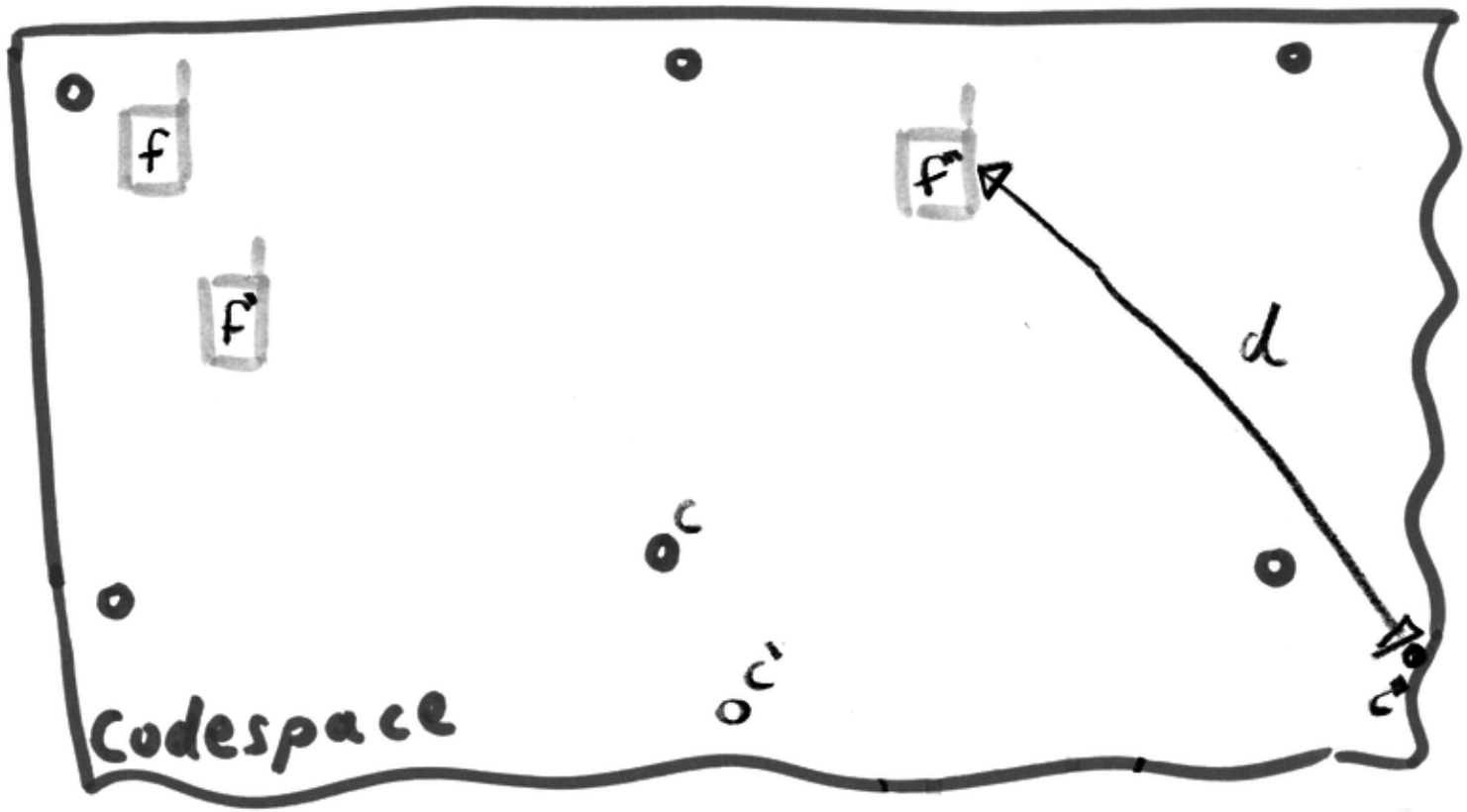
Spontaneous audio-based device pairing



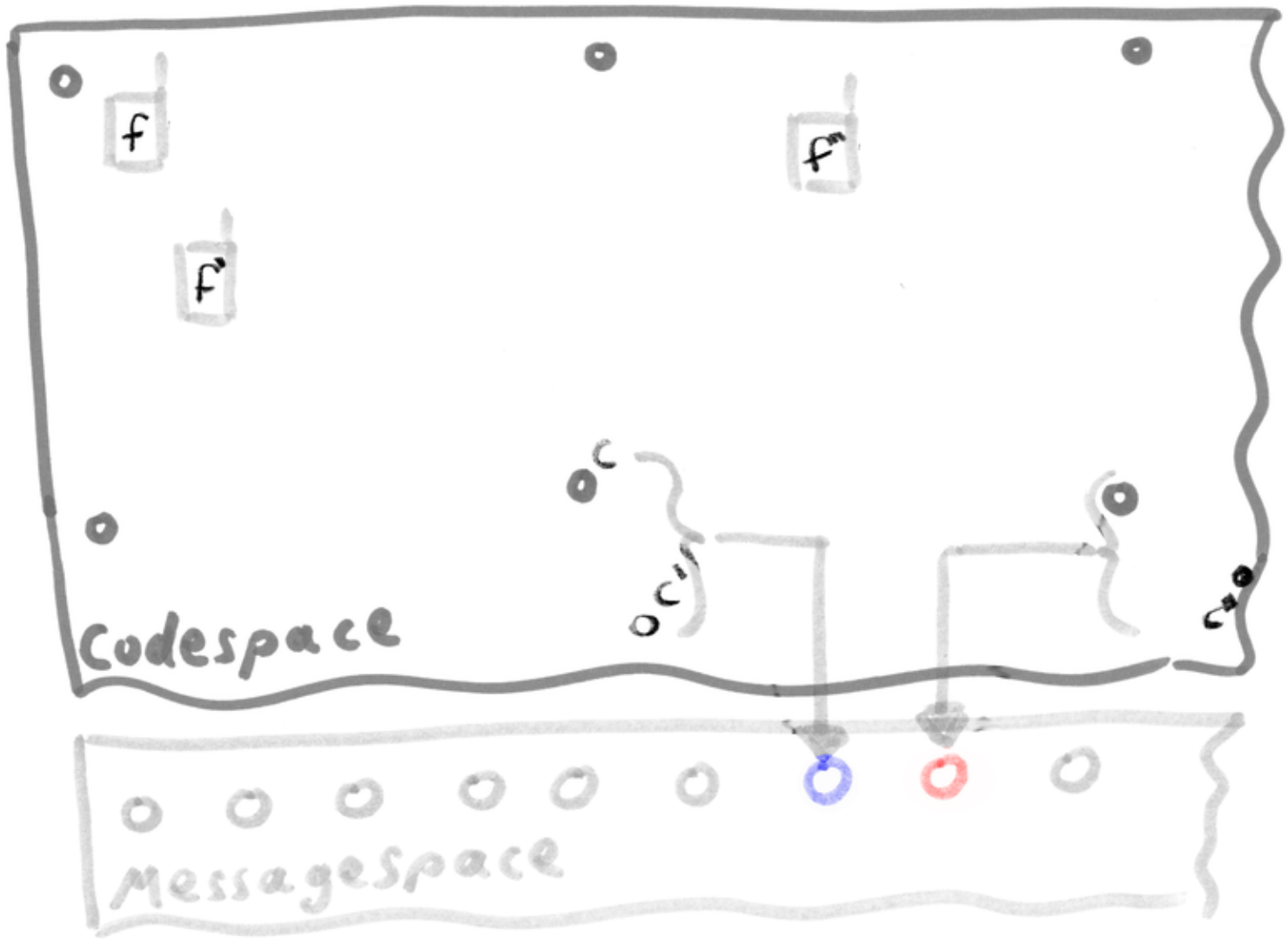
Spontaneous audio-based device pairing



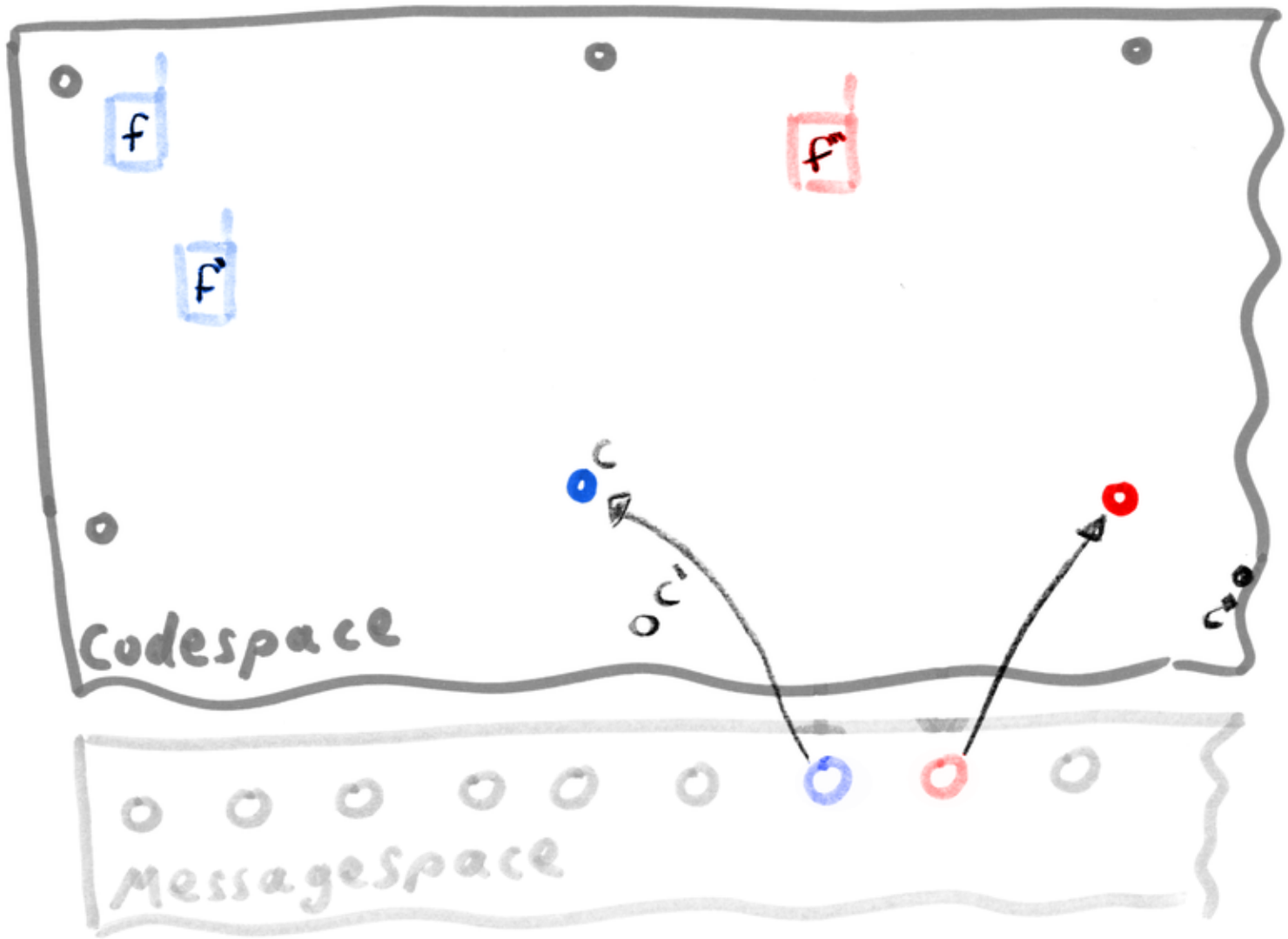
Spontaneous audio-based device pairing



Spontaneous audio-based device pairing



Spontaneous audio-based device pairing

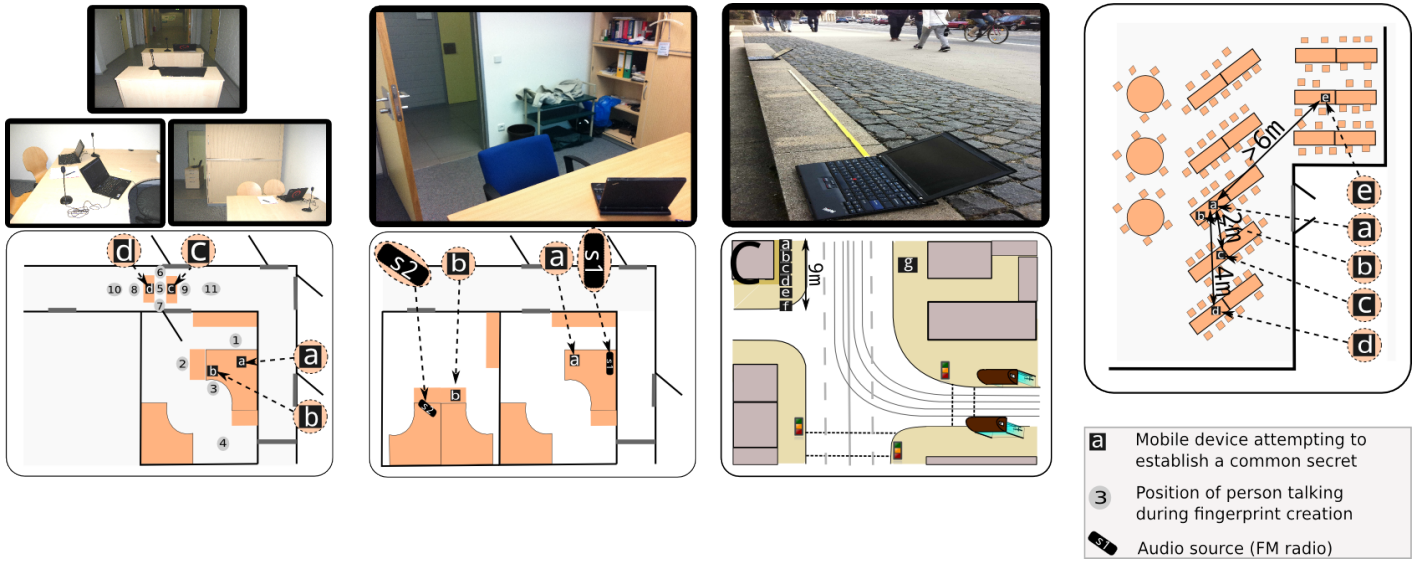


Security from environmental stimuli

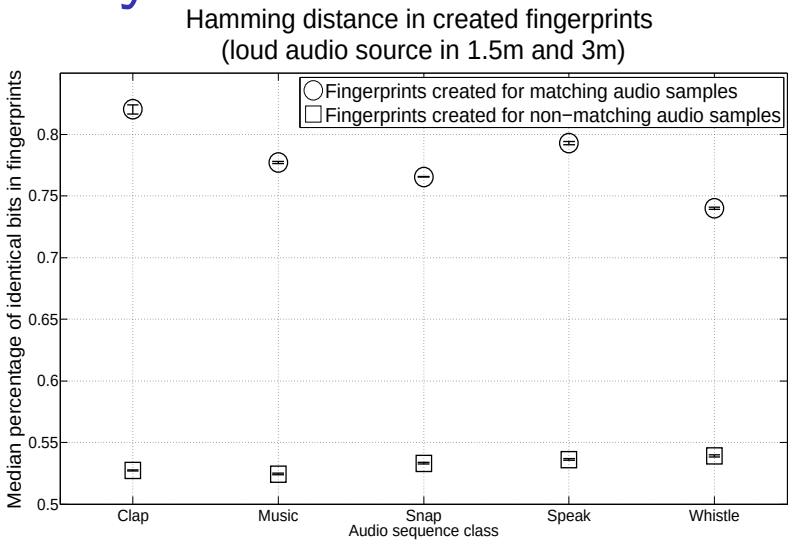
Audio-based ad-hoc secure pairing[a]

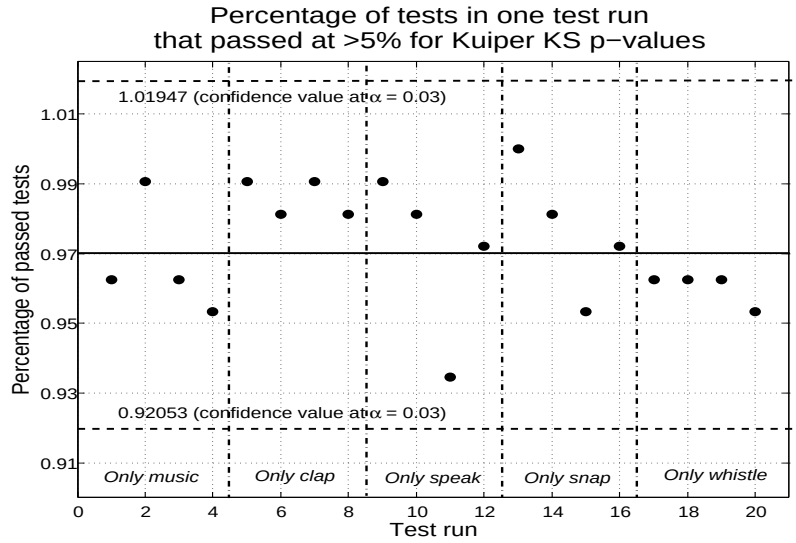
[a] S. Sigg et al., Secure Communication based on Ambient Audio, IEEE Transactions on Mobile Computing, vol. 12, no. 2, 2013

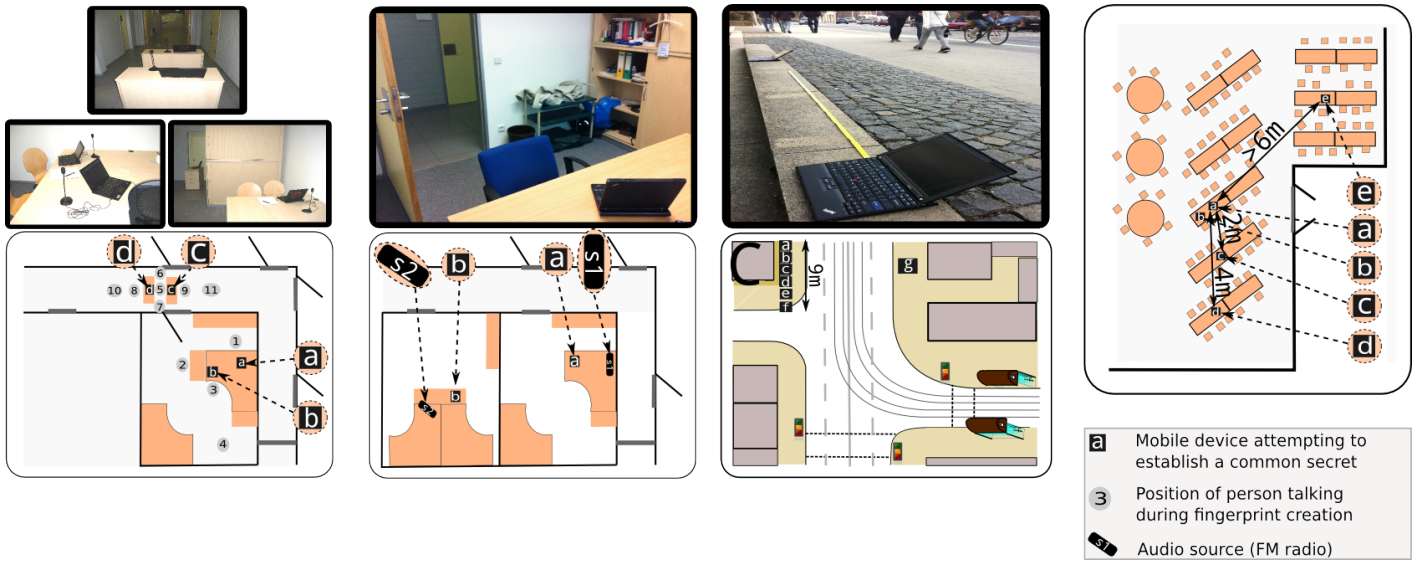
- Audio as common context source
- Fuzzy cryptography

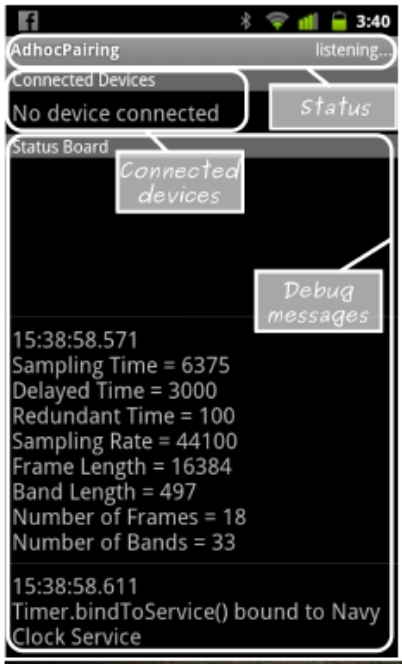


Security from environmental stimuli

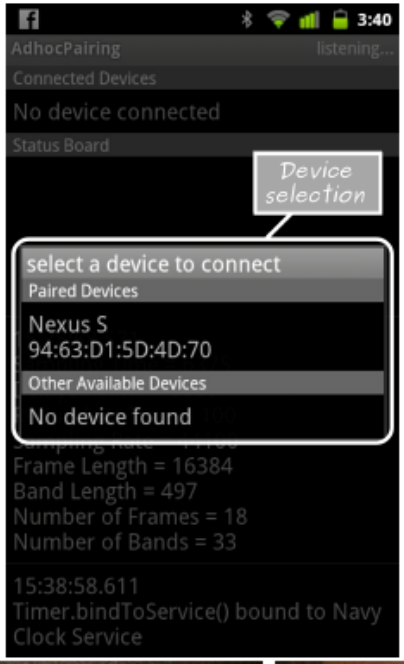


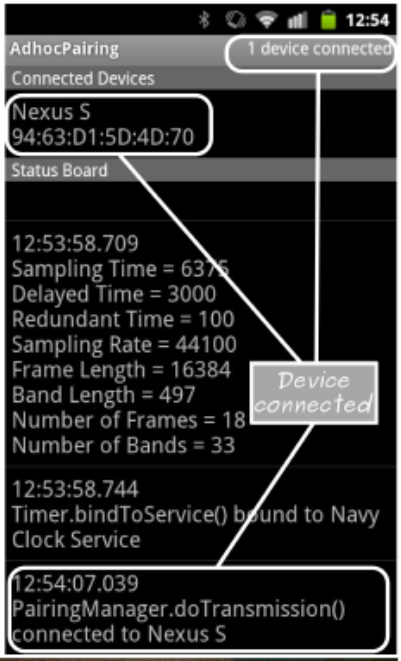


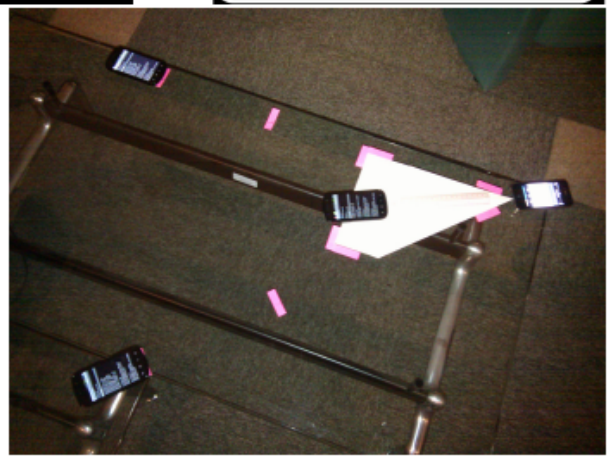



3:40
AdhocPairing
listening...
Connected Devices
No device connected
Status
Status Board
Connected devices
Debug messages
15:38:58.571
Sampling Time = 6375
Delayed Time = 3000
Redundant Time = 100
Sampling Rate = 44100
Frame Length = 16384
Band Length = 497
Number of Frames = 18
Number of Bands = 33
15:38:58.611
Timer.bindToService() bound to Navy Clock Service


12:31
AdhocPairing
listening...
Connected Devices
No device connected
Status Board
12:25:53.000
Sampling Time = 6375
Delayed Time = 3000
Menu
Connect a device
Make discoverable
Sync time
Get audio sample
Compare fingerprint
More


3:40
AdhocPairing
listening...
Connected Devices
No device connected
Status Board
Device selection
select a device to connect
Paired Devices
Nexus S
94:63:D1:5D:4D:70
Other Available Devices
No device found
Frame Length = 16384
Band Length = 497
Number of Frames = 18
Number of Bands = 33
15:38:58.611
Timer.bindToService() bound to Navy Clock Service


12:54
AdhocPairing
1 device connected
Connected Devices
Nexus S
94:63:D1:5D:4D:70
Status Board
12:53:58.709
Sampling Time = 6375
Delayed Time = 3000
Redundant Time = 100
Sampling Rate = 44100
Frame Length = 16384
Band Length = 497
Number of Frames = 18
Number of Bands = 33
Device connected
12:53:58.744
Timer.bindToService() bound to Navy Clock Service
12:54:07.039
PairingManager.doTransmission()
connected to Nexus S

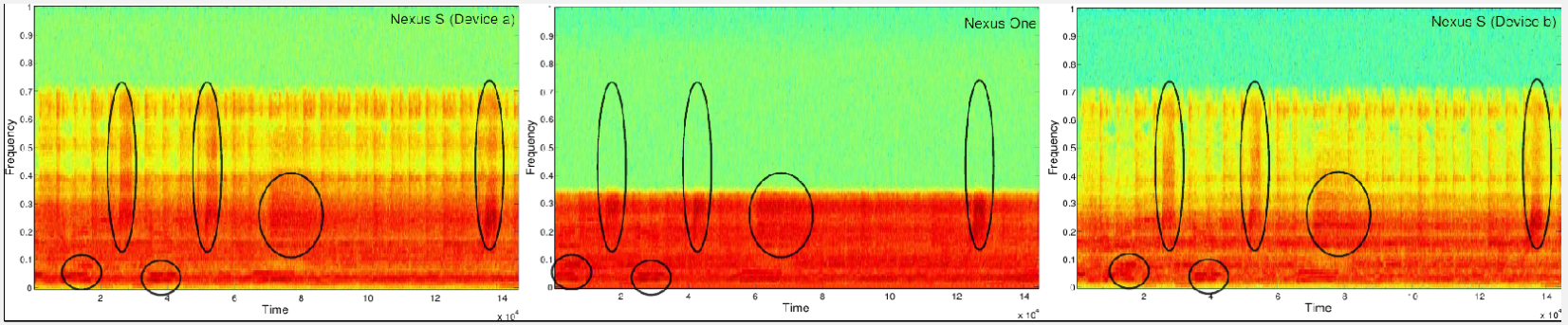


Security from environmental stimuli

Real-time implementation on android mobile phones[a]

[a] Stephan Sigg, et al., AdhocPairing: Spontaneous audio-based secure device pairing for Android mobile devices, IWSSI 2012

- Hardware noise cancellation on some phones
- Hardware originated synchronisation offset



Security from environmental stimuli

How to synchronise audio without disclosing information?

No data shall be transmitted among devices

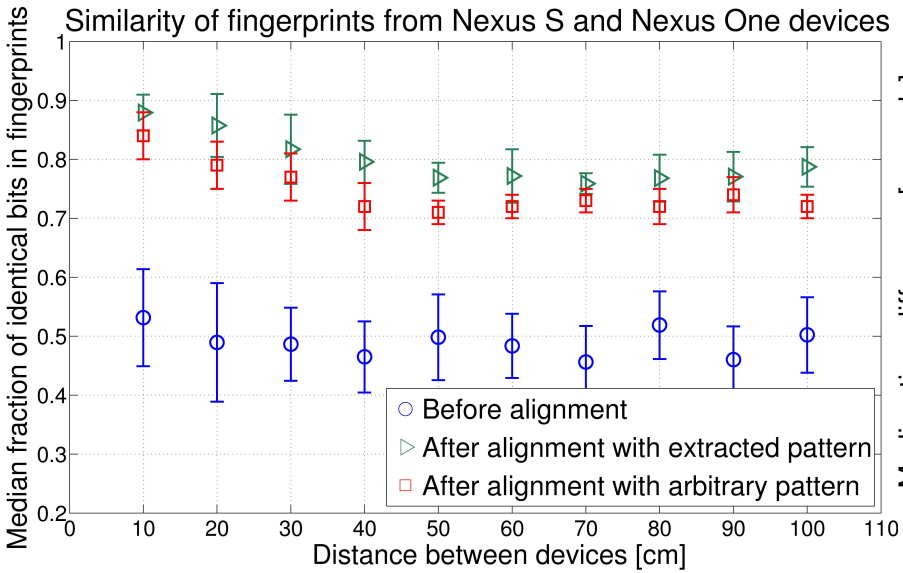
Hardware-originated synchronisation offset

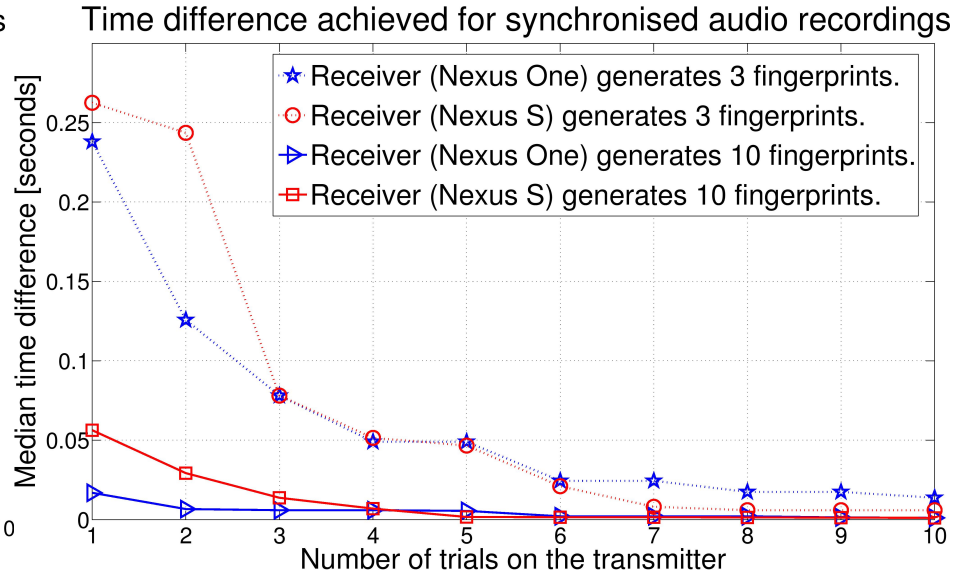
- Approximate pattern matching with arbitrary common sequence [a]

[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[1] [2]

[1] N. Nguyen, S. Sigg, A. Huynh and Y. Ji: Pattern-based Alignment of Audio Data for Ad-hoc Pairing, ISWC, 2012

[2] N. Nguyen, S. Sigg, A. Huynh and Y. Ji: Using ambient audio in secure mobile phone communication, PerCom, 2012

Unobtrusive Ad-Hoc Pairing for Body Area Networks

- 15 Subjects
- 8 Actions
- 7 Sensor-positions
- 6 Sensors

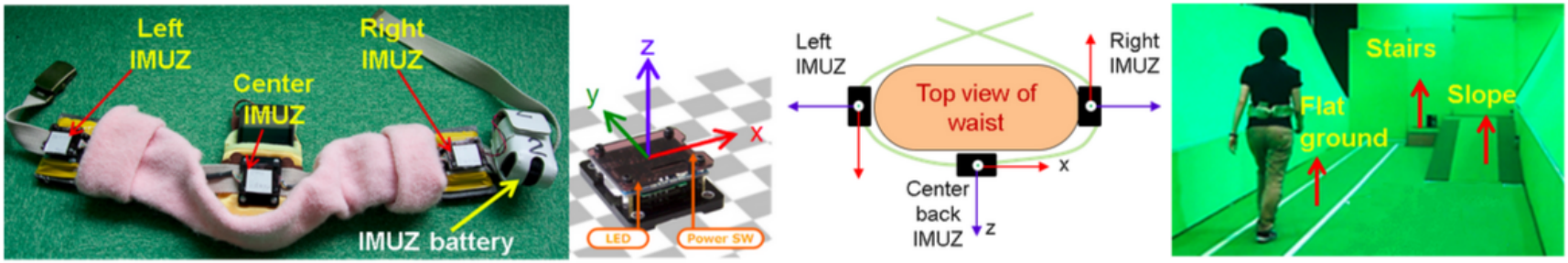
Sztyler et al.:*On-body Localization of Wearable Devices [...]*

Osaka University (OU-ISIR Gait database)

- 460 participants aged between 8 and 78
- gender ratio almost 50:50
- max. 8 gait cycles
- Sensorpositions: Waist right, left, back
- 3D-Accelerometer and Gyroskope (100Hz)

URL: http://www.am.sanken.osaka-u.ac.jp/BiometricDB/SimilarActionsInertialDB.htm

Sensor Setup



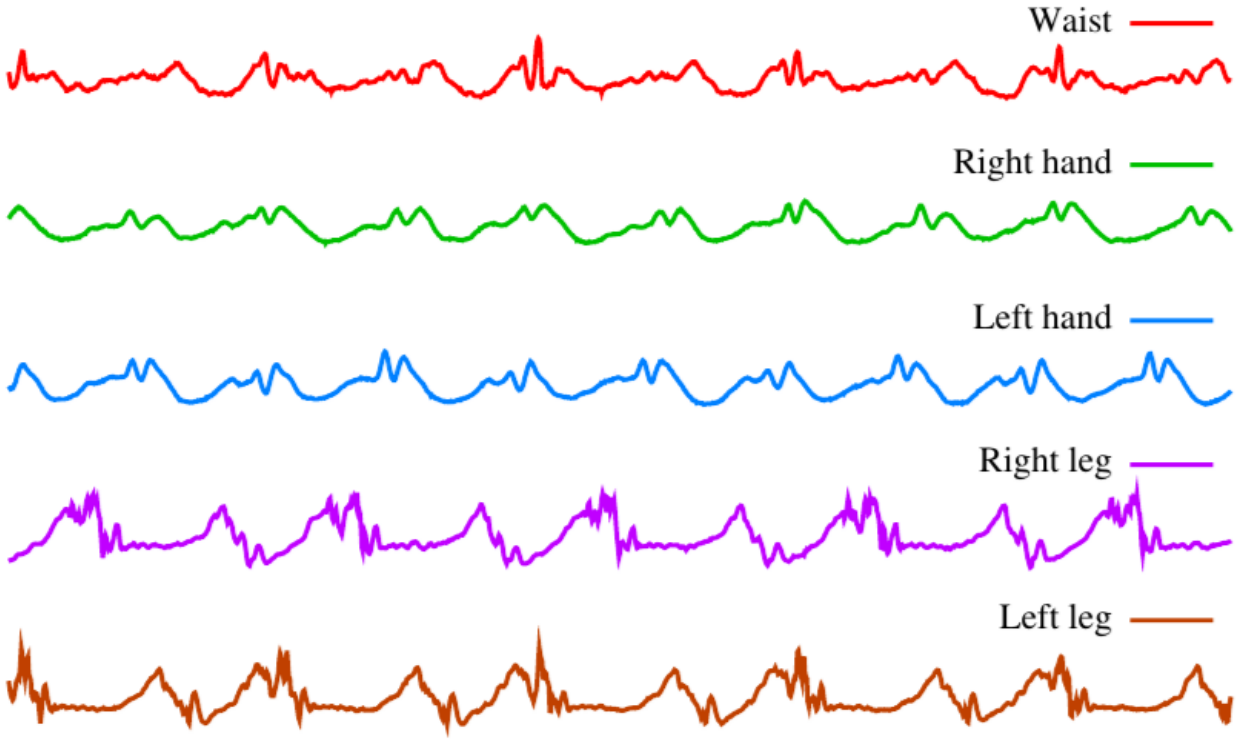
(a) Uncovered 3 IMUZ sensors on a belt (b) IMUZ (c) Sensor attachment (d) Subject wearing a belt in the scene

Thanh Trung Ngo, Yasushi Makihara, Hajime Nagahara, Yasuhiro Mukaigawa,Yasushi Yagi, "Similar gait action recognition using an inertial sensor," Pattern Recognition Vol.48 (4), pp. 1289-1301, 2015

Dartmouth

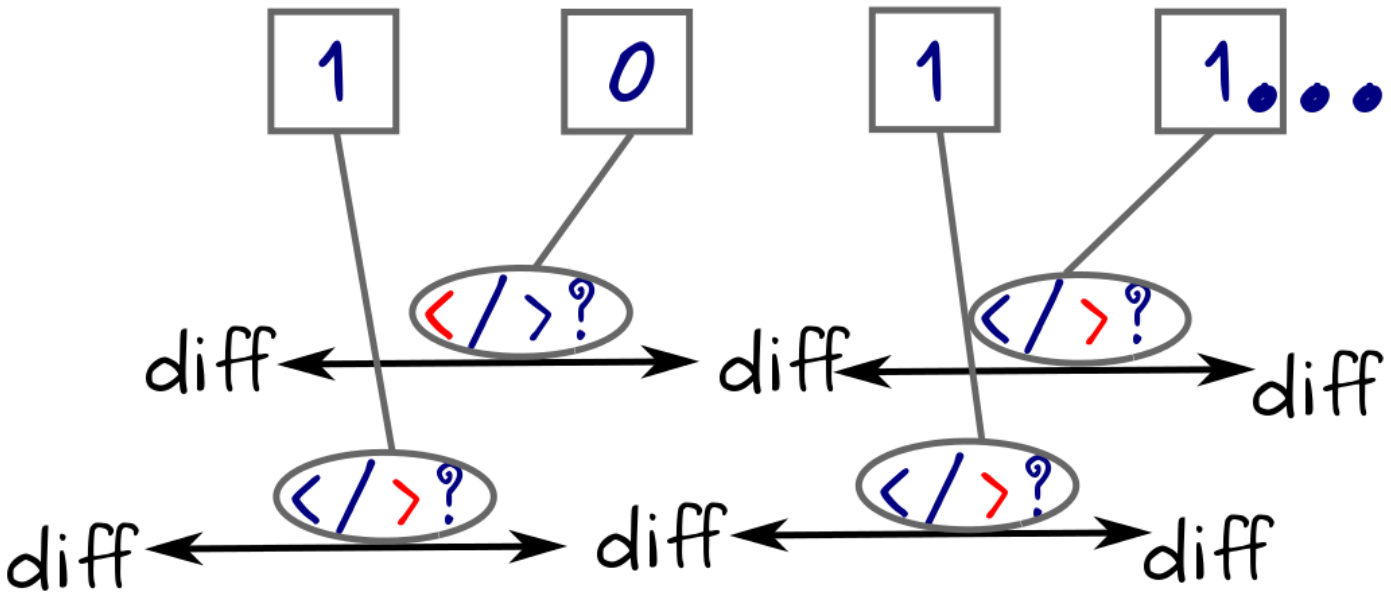
- 7 Subjects
- 5 Accelerometers - no Gyroscopes
- 13 hours at 255Hz
- waist, left wrist, right wrist, left ankle, right ankle

http://www.cs.dartmouth.edu/~dfk/papers/cornelius-same-body.pdf



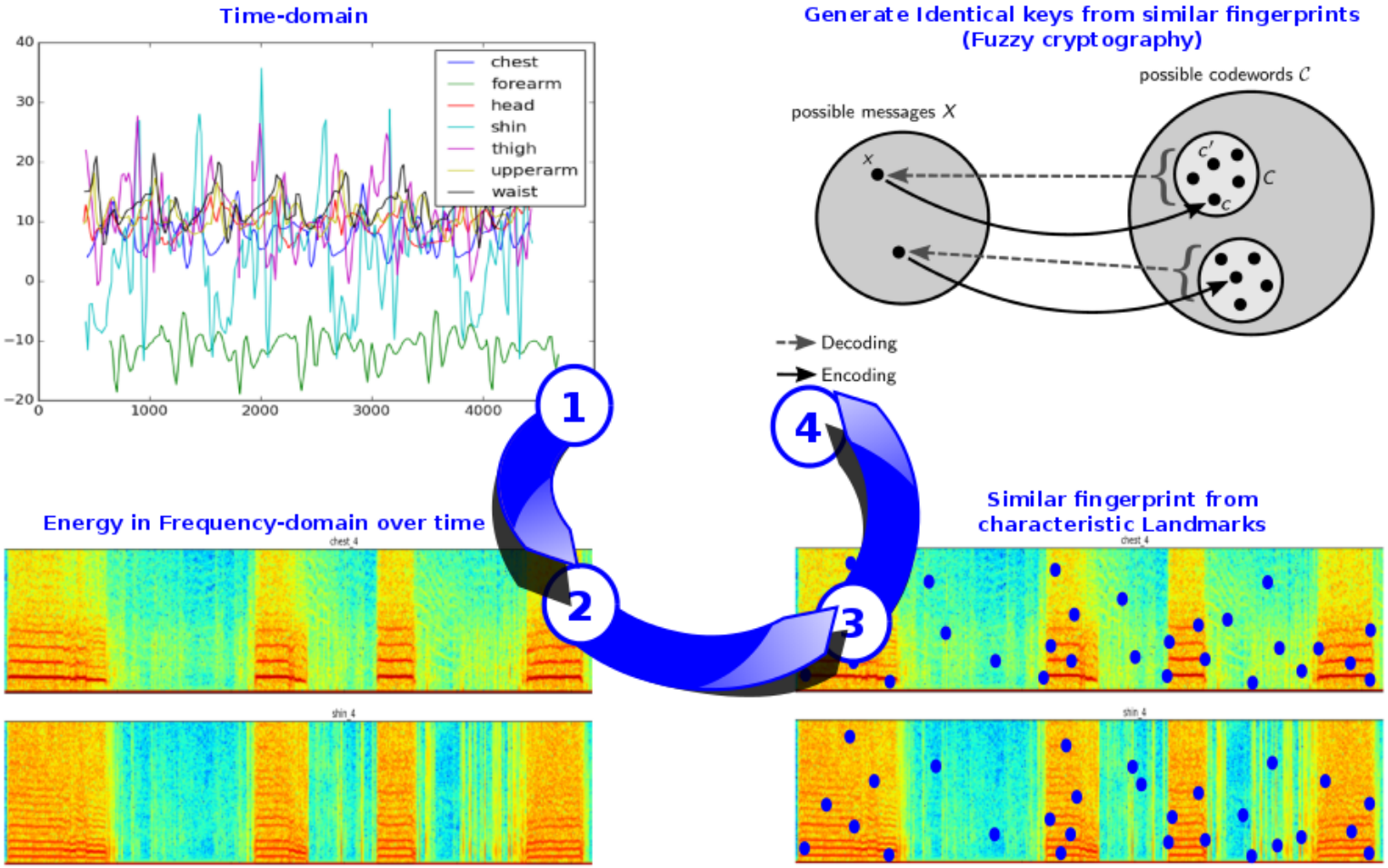
Cory Cornelius and David Kotz. 2011. Recognizing whether sensors are on the same body. In Proceedings of the 9th international conference on Pervasive computing (Pervasive'11), Kent Lyons, Jeffrey Hightower, and Elaine M. Huang (Eds.). Springer-Verlag, Berlin, Heidelberg, 332-349.

Audio Fingerprinting (Haitsma & Kalker, ISMIR 2002)



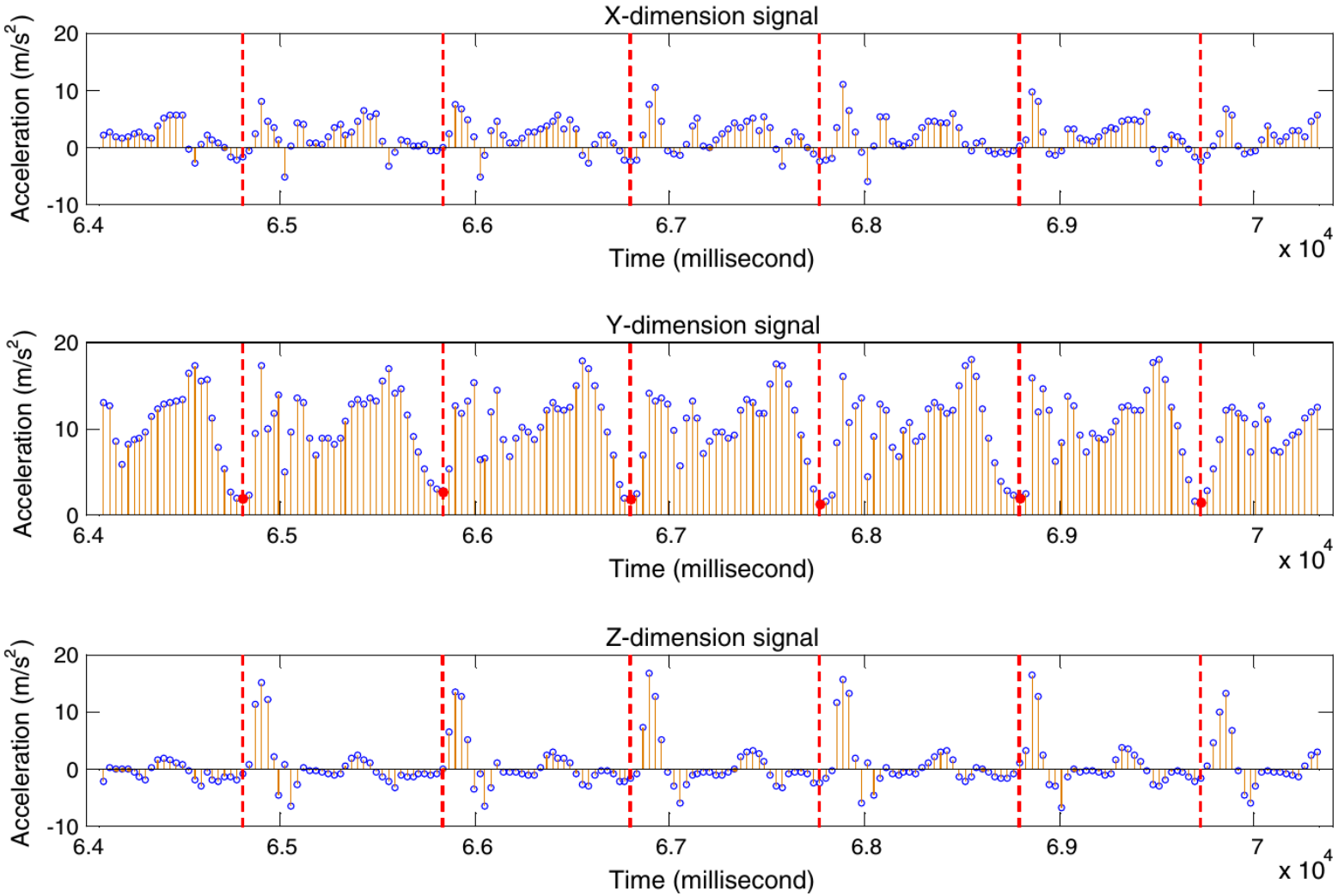
Haitsma, Kalker: A highly robust audio fingerprinting system. ISMIR. 2002.

Audio Landmarks (Wang, ISMIR 2003)

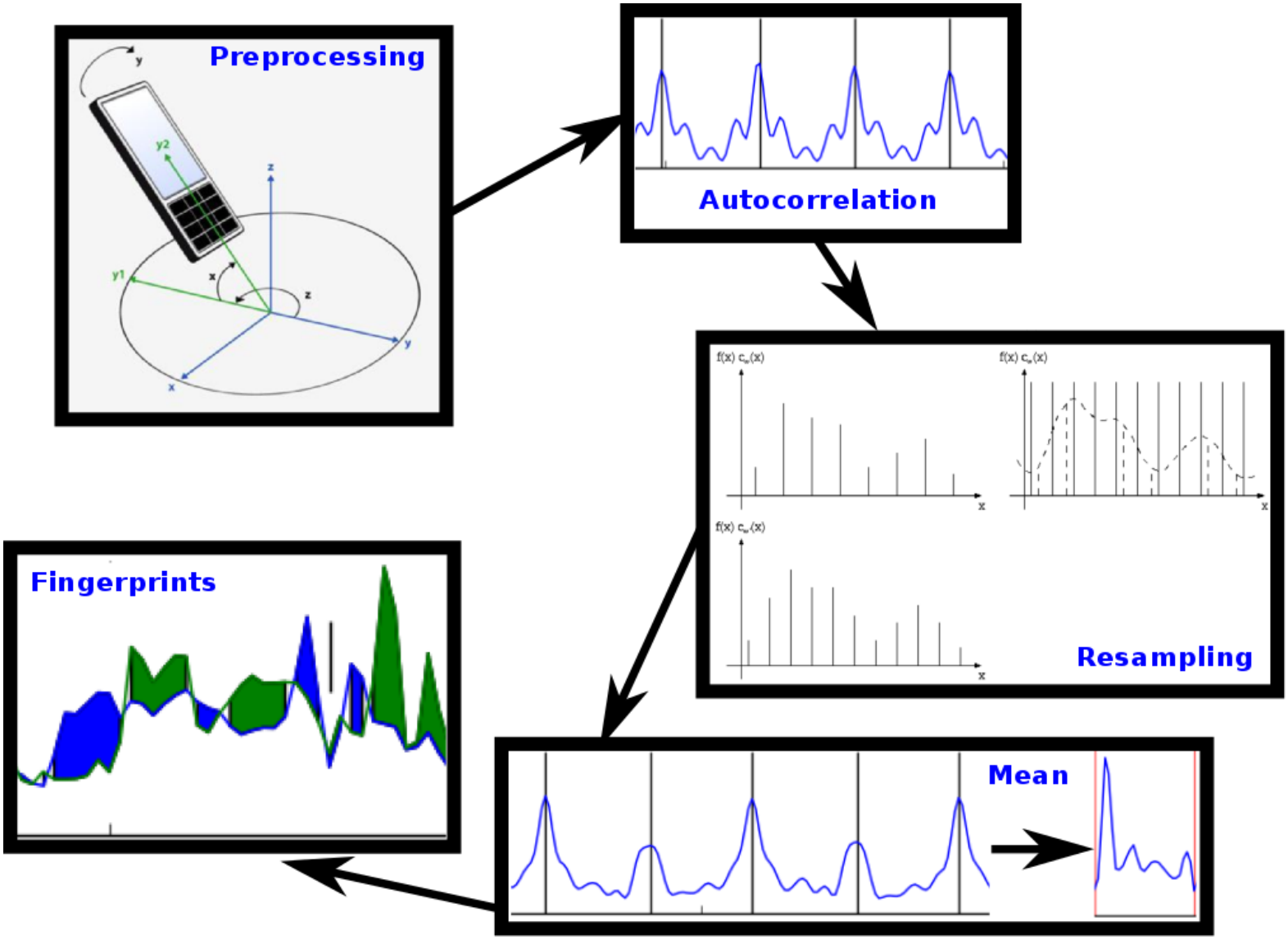


Wang: An Industrial Strength Audio Search Algorithm. ISMIR. 2003.

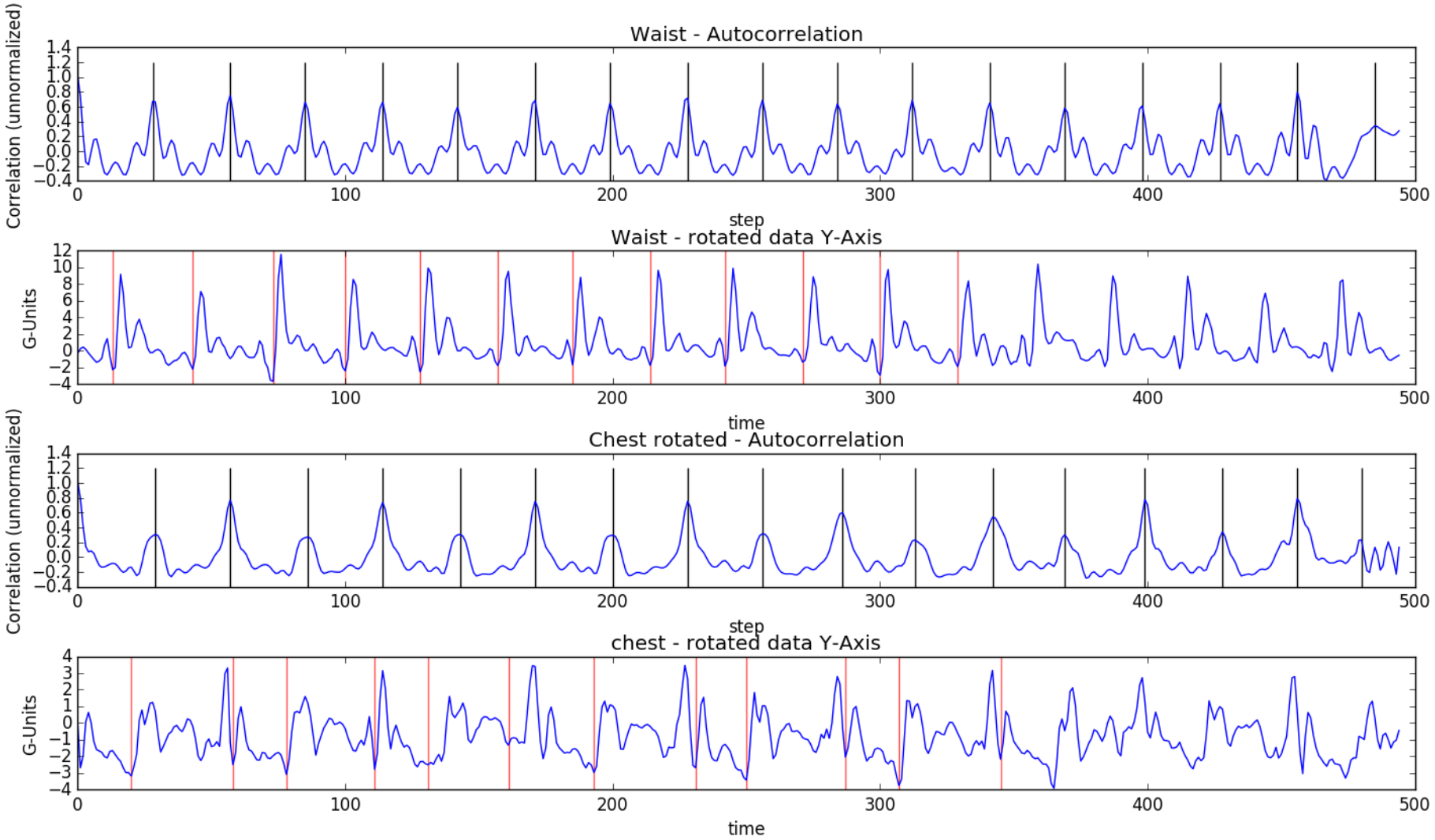
Gait recognition (Hoang & Choi & Nguyen, IJIS 2015)



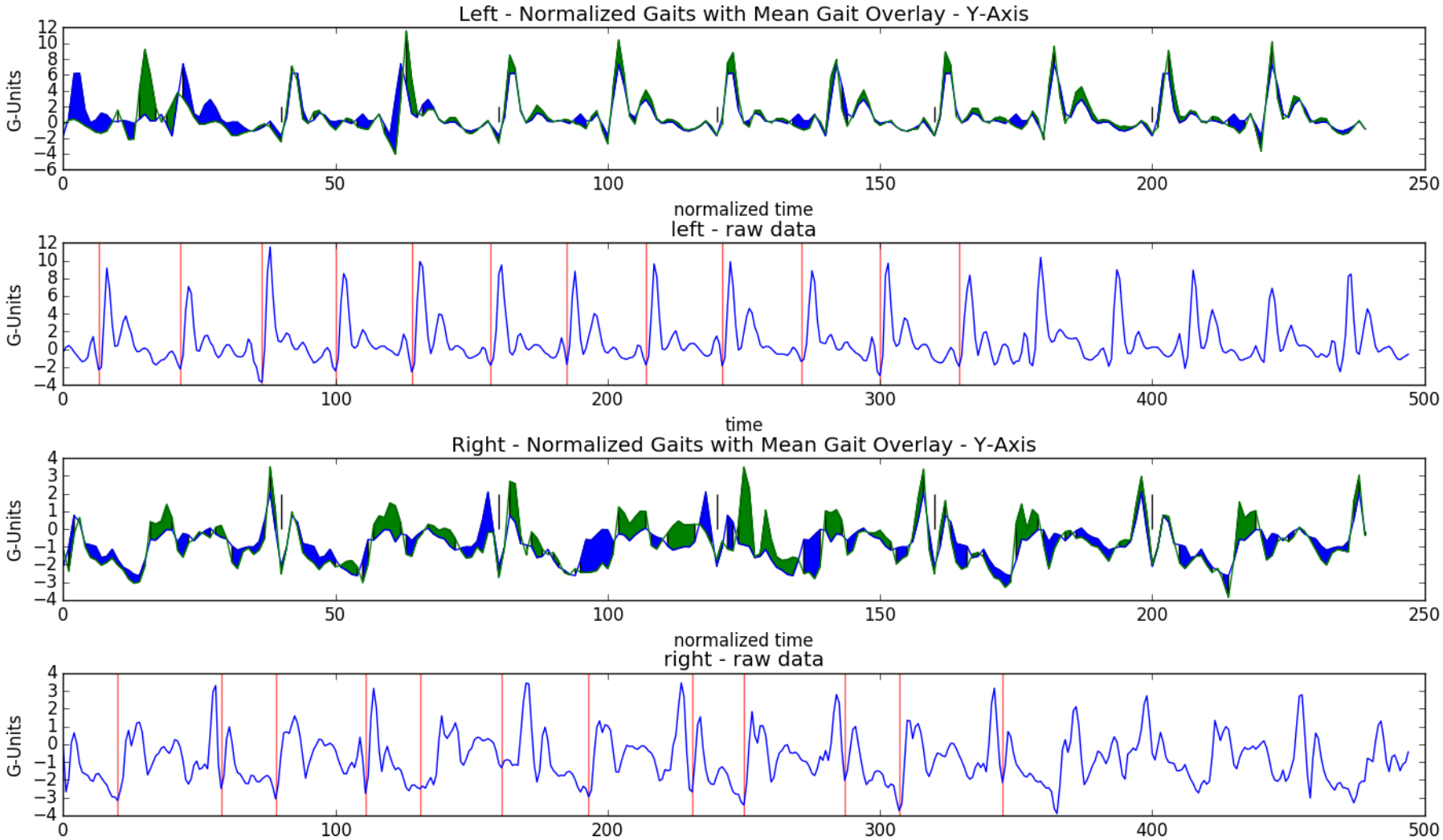
Hoang, Choi, Nguyen: Gait authentication on mobile phone using biometric cryptosystem and fuzzy commitment


Preprocessing
Autocorrelation
Resampling
Fingerprints
Mean

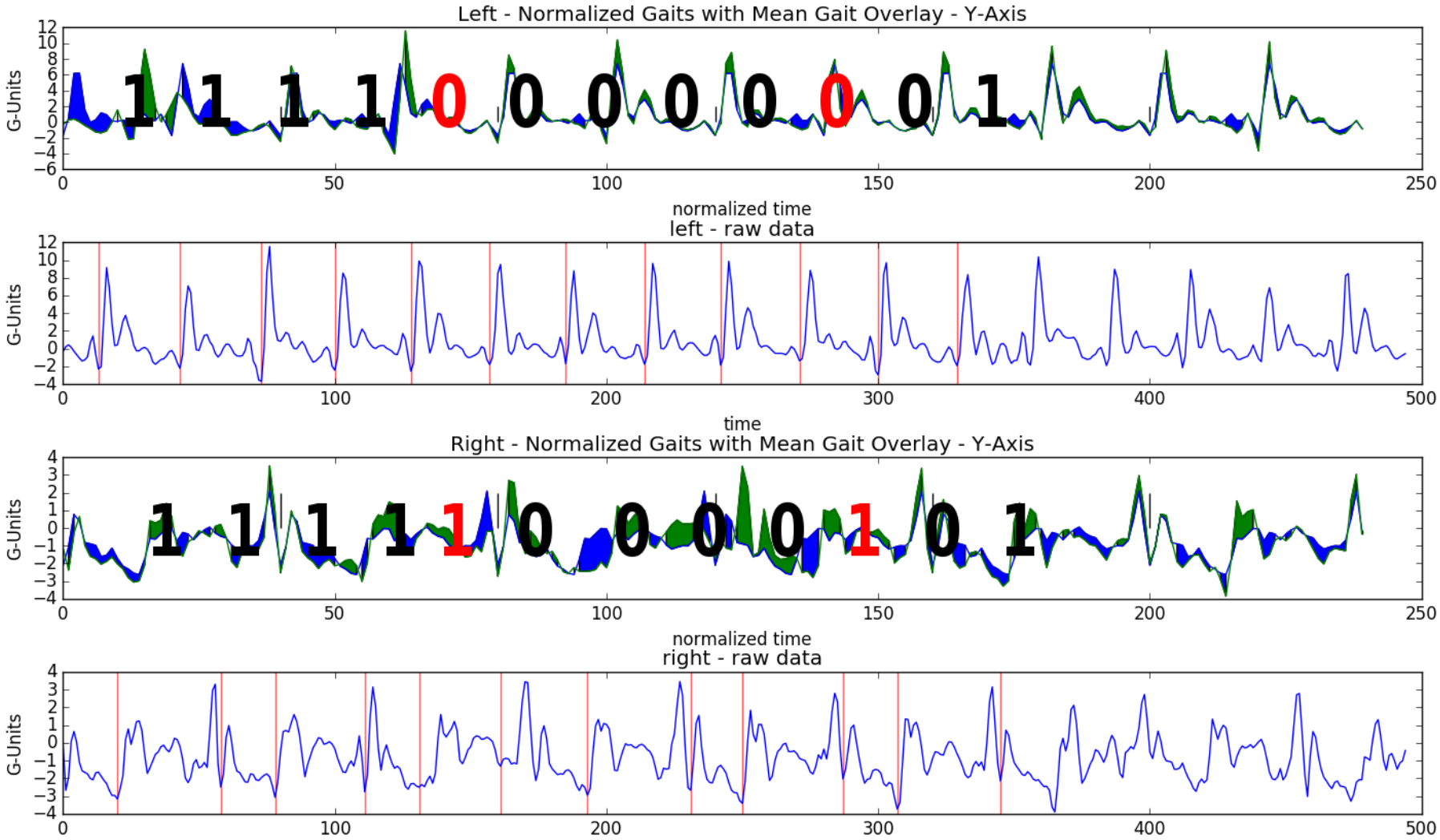
Results


Waist - Autocorrelation
Correlation (unnormalized)
step
Waist - rotated data Y-Axis
G-Units
time
Chest rotated - Autocorrelation
Correlation (unnormalized)
step
chest - rotated data Y-Axis
G-Units
time

Results


Left - Normalized Gaits with Mean Gait Overlay - Y-Axis
G-Units
normalized time
left - raw data
G-Units
time
Right - Normalized Gaits with Mean Gait Overlay - Y-Axis
G-Units
normalized time
right - raw data
G-Units

Results


Left - Normalized Gaits with Mean Gait Overlay - Y-Axis
G-Units
1 1 1 1 0 0 0 0 0 0 0 1
normalized time
left - raw data
G-Units
time
Right - Normalized Gaits with Mean Gait Overlay - Y-Axis
G-Units
1 1 1 1 1 0 0 0 0 1 0 1
normalized time
right - raw data
G-Units

Thank you!

Stephan Sigg
stephan.sigg@aalto.fi