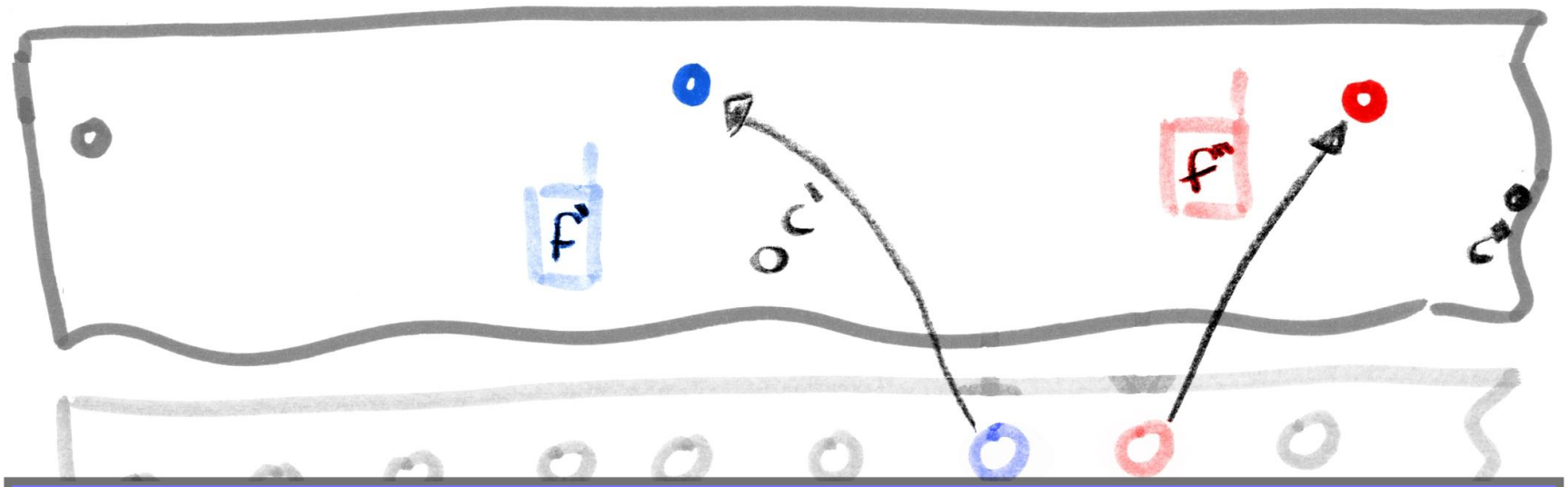
Aalto University
School of Science
and Technology

Fuzzy cryptography (for audio-based secure device pairing) – brief

Stephan Sigg

Department of Communications and Networking
Aalto University, School of Electrical Engineering
stephan.sigg@aalto.fi

Version 1.0, September 1, 2016



Secure spontaneous authentication from ambient audio

Motivation

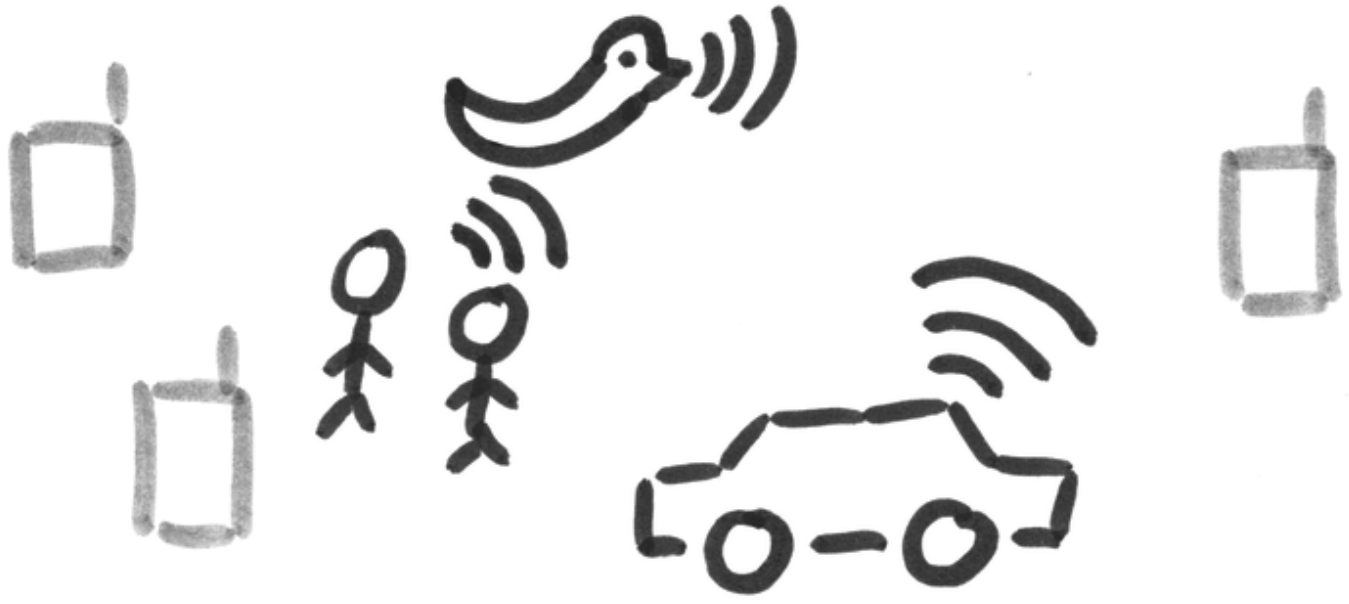
Motivation

Trust and proximity

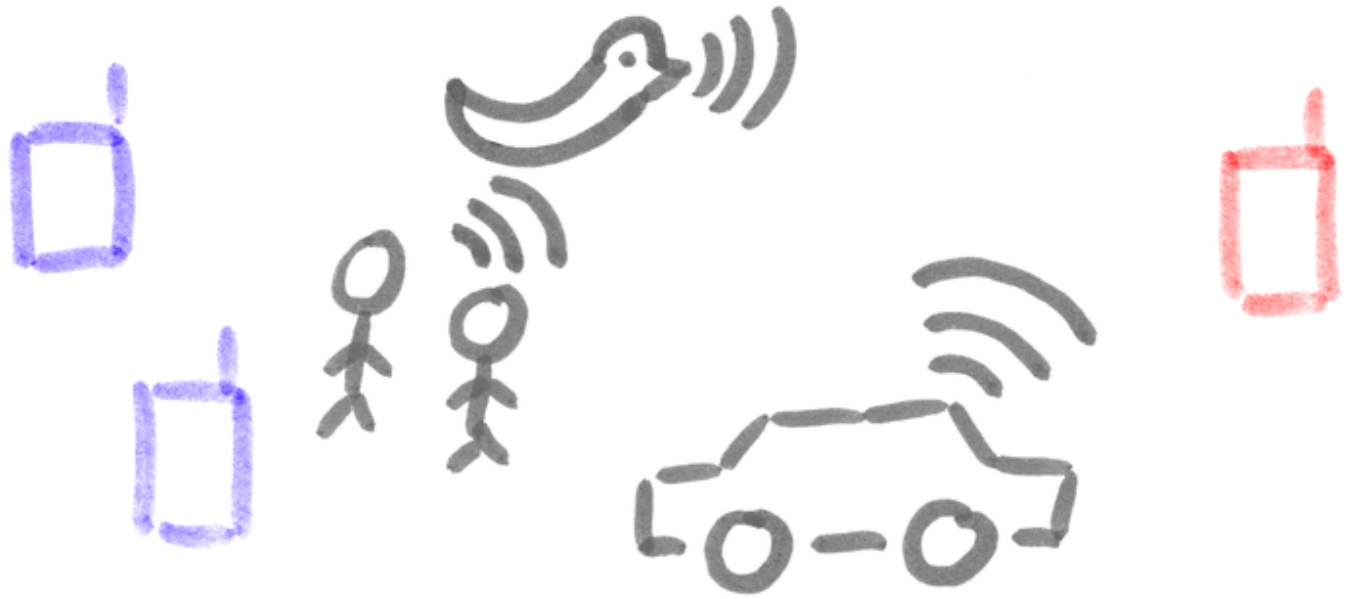
We will use audio as a source of common information in proximity

Spontaneous audio-based device pairing

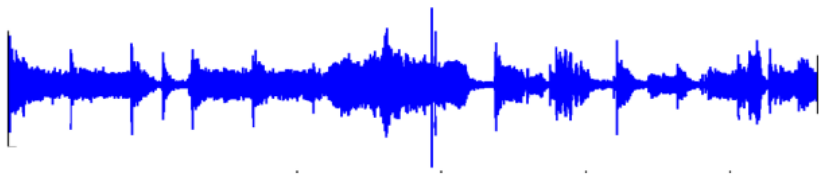
Spontaneous audio-based device pairing



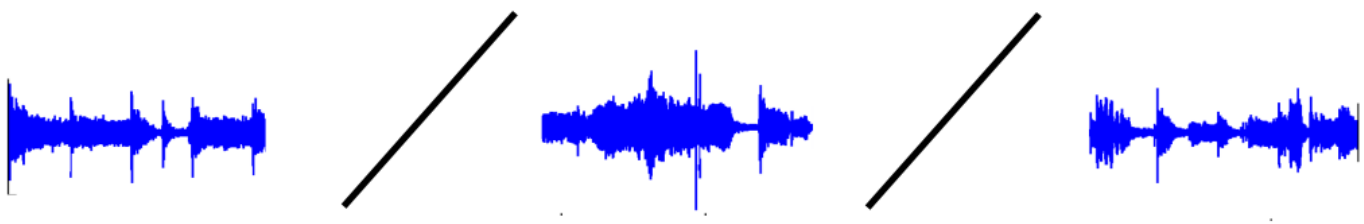
Spontaneous audio-based device pairing



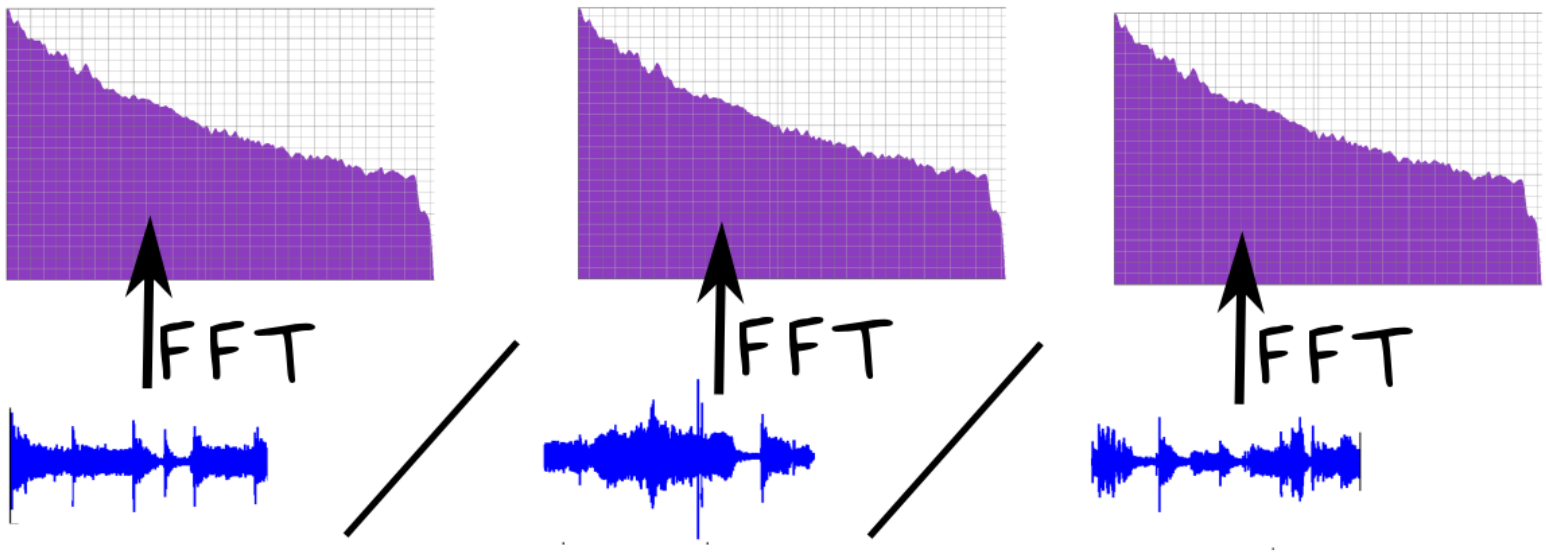
Spontaneous audio-based device pairing



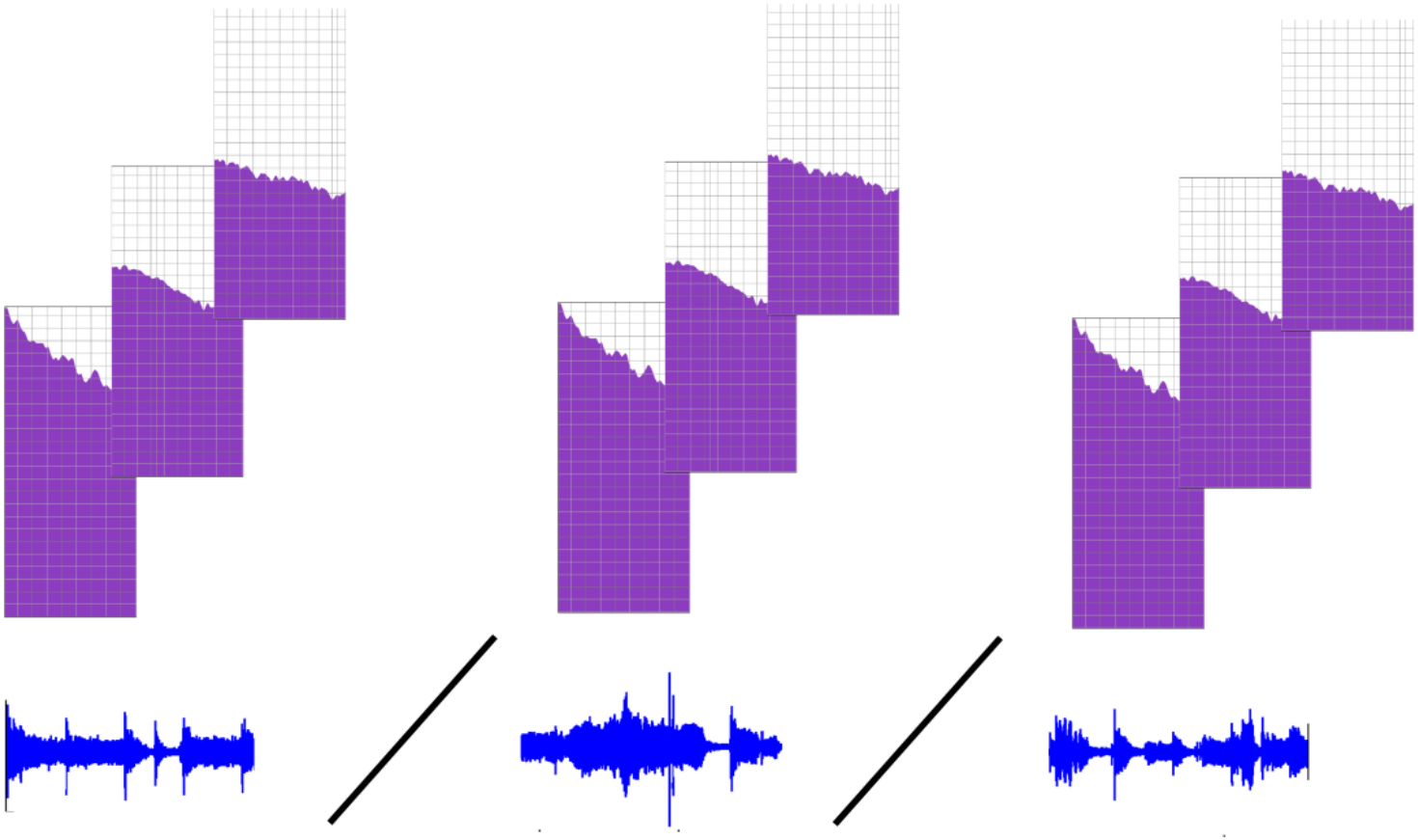
Spontaneous audio-based device pairing



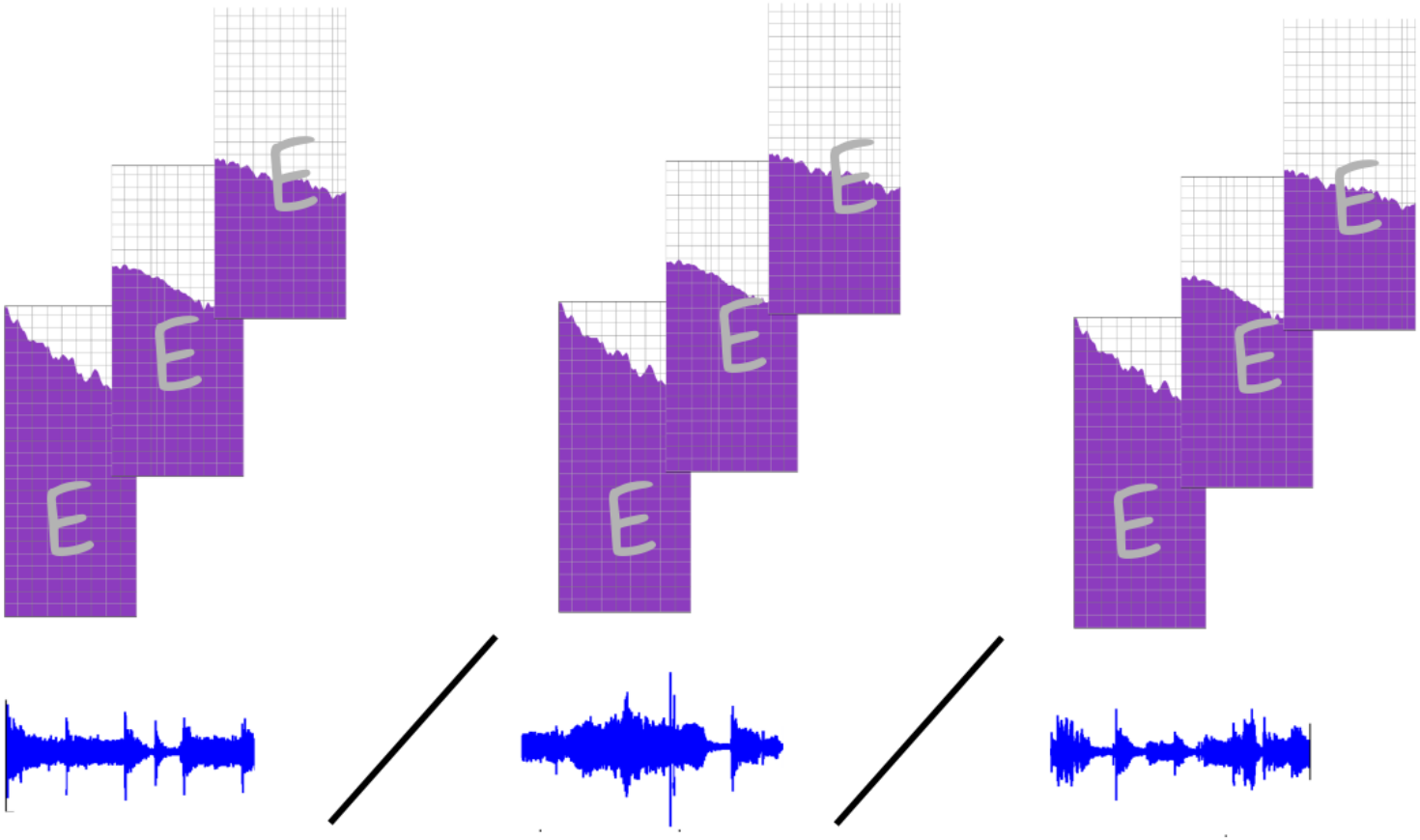
Spontaneous audio-based device pairing



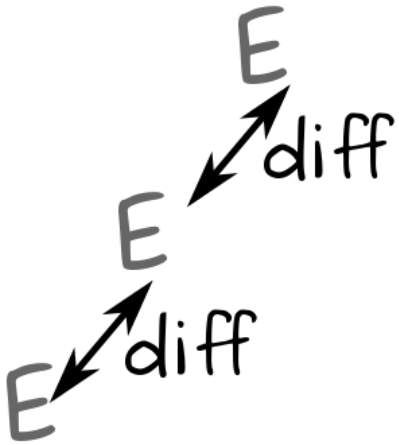
Spontaneous audio-based device pairing

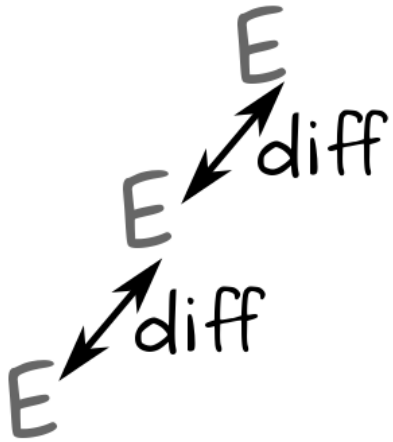


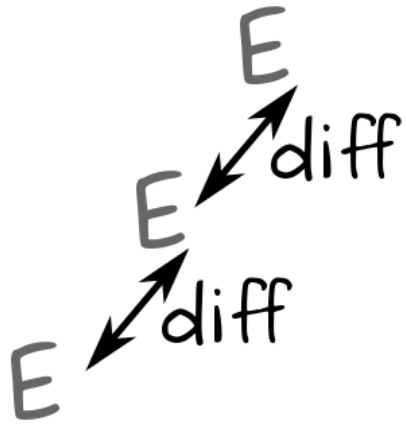
Spontaneous audio-based device pairing



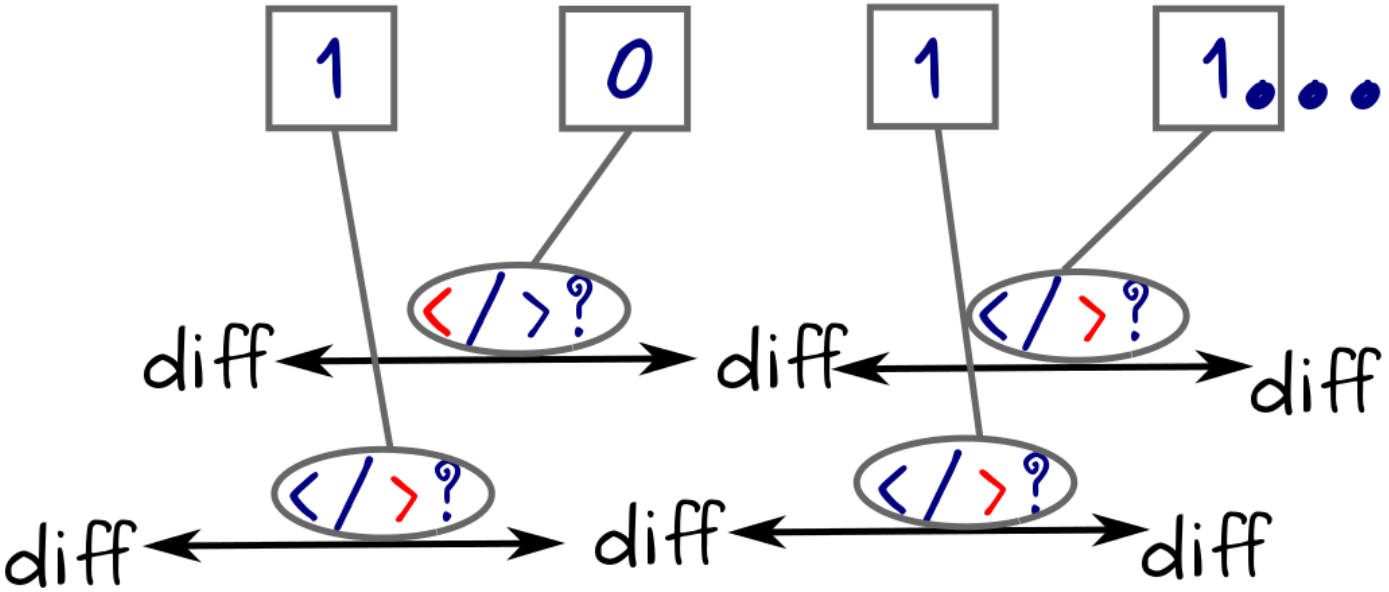
Spontaneous audio-based device pairing





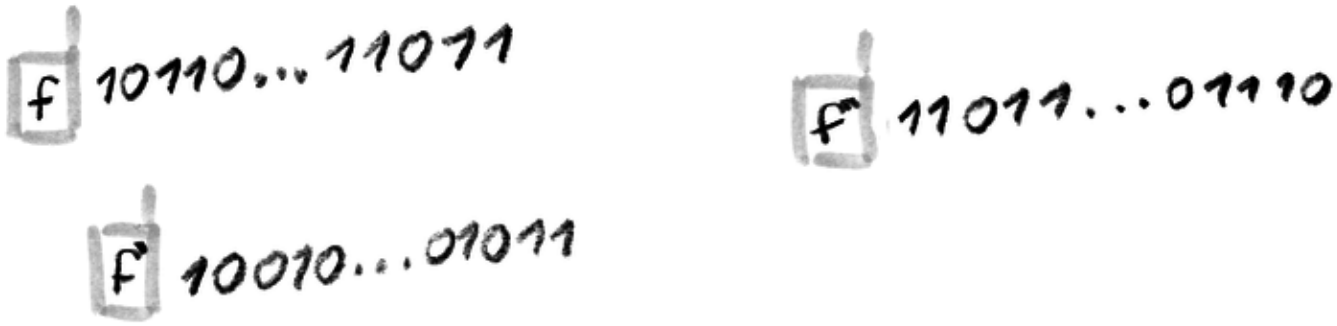


Spontaneous audio-based device pairing

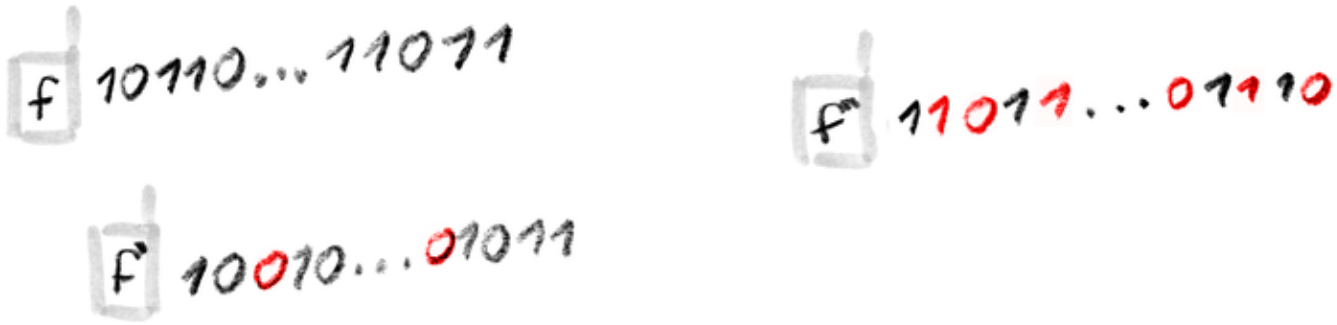


Spontaneous audio-based device pairing

Spontaneous audio-based device pairing

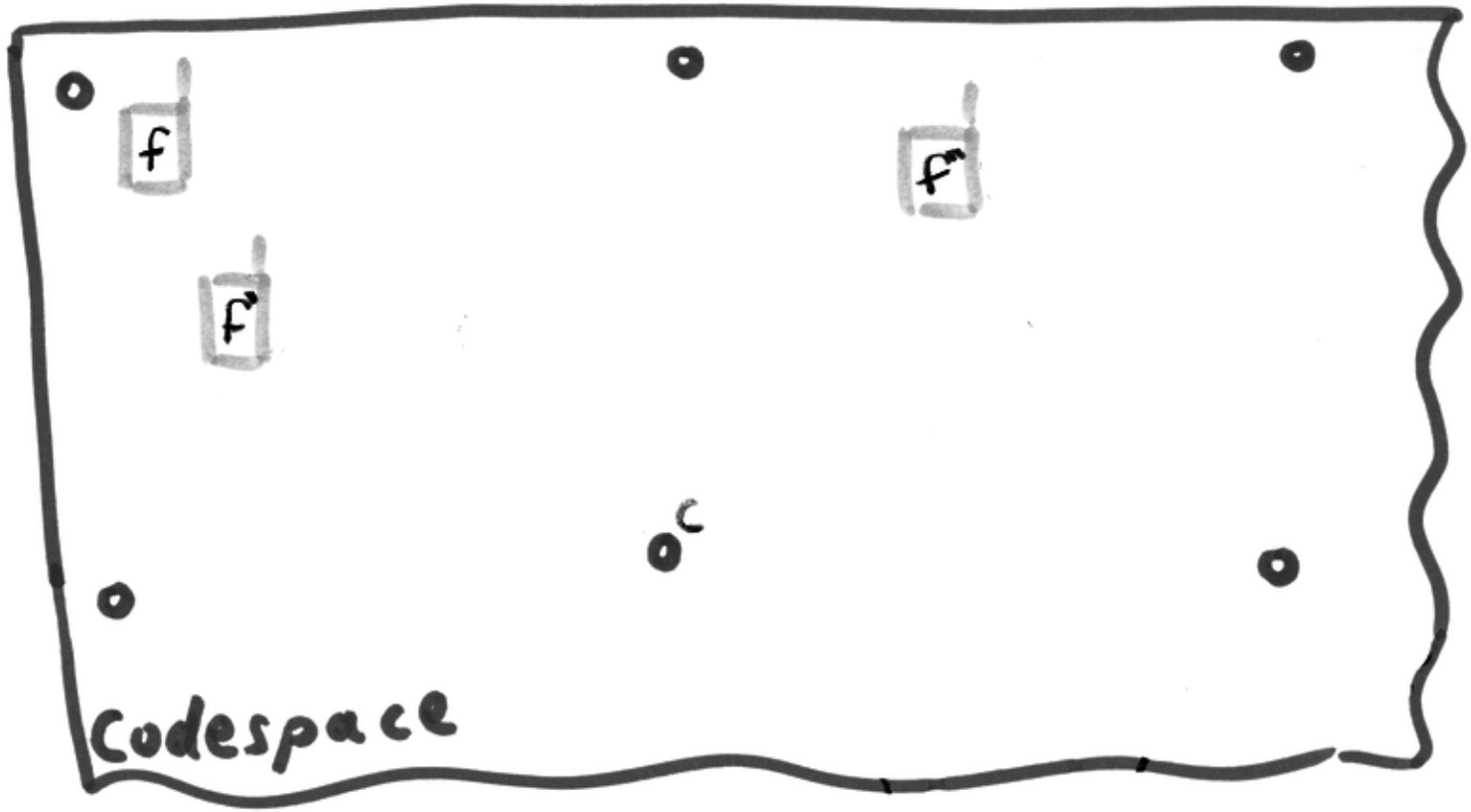


Spontaneous audio-based device pairing

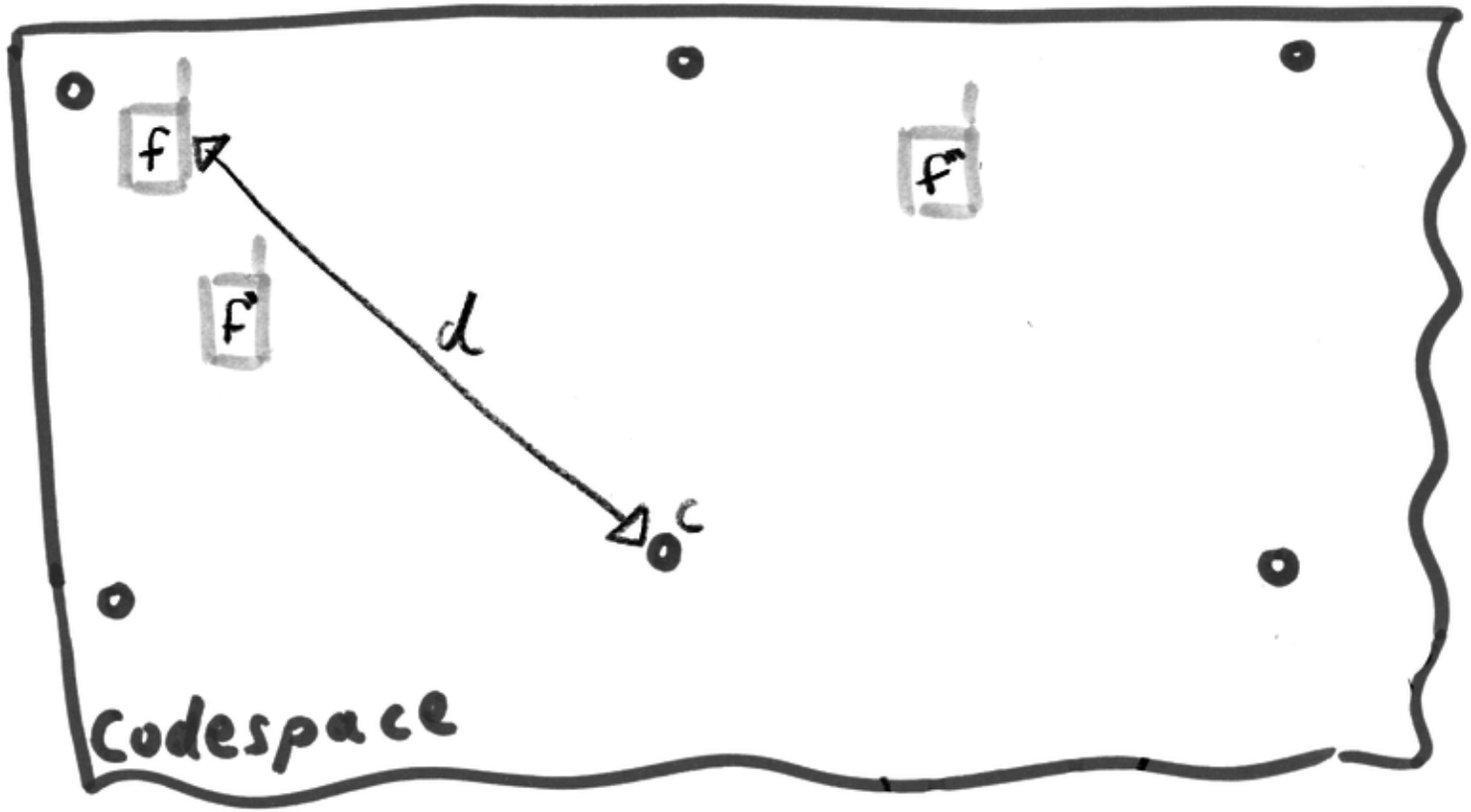


Spontaneous audio-based device pairing

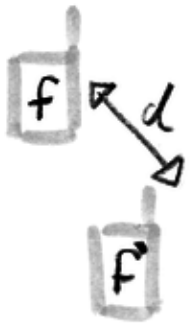
Spontaneous audio-based device pairing



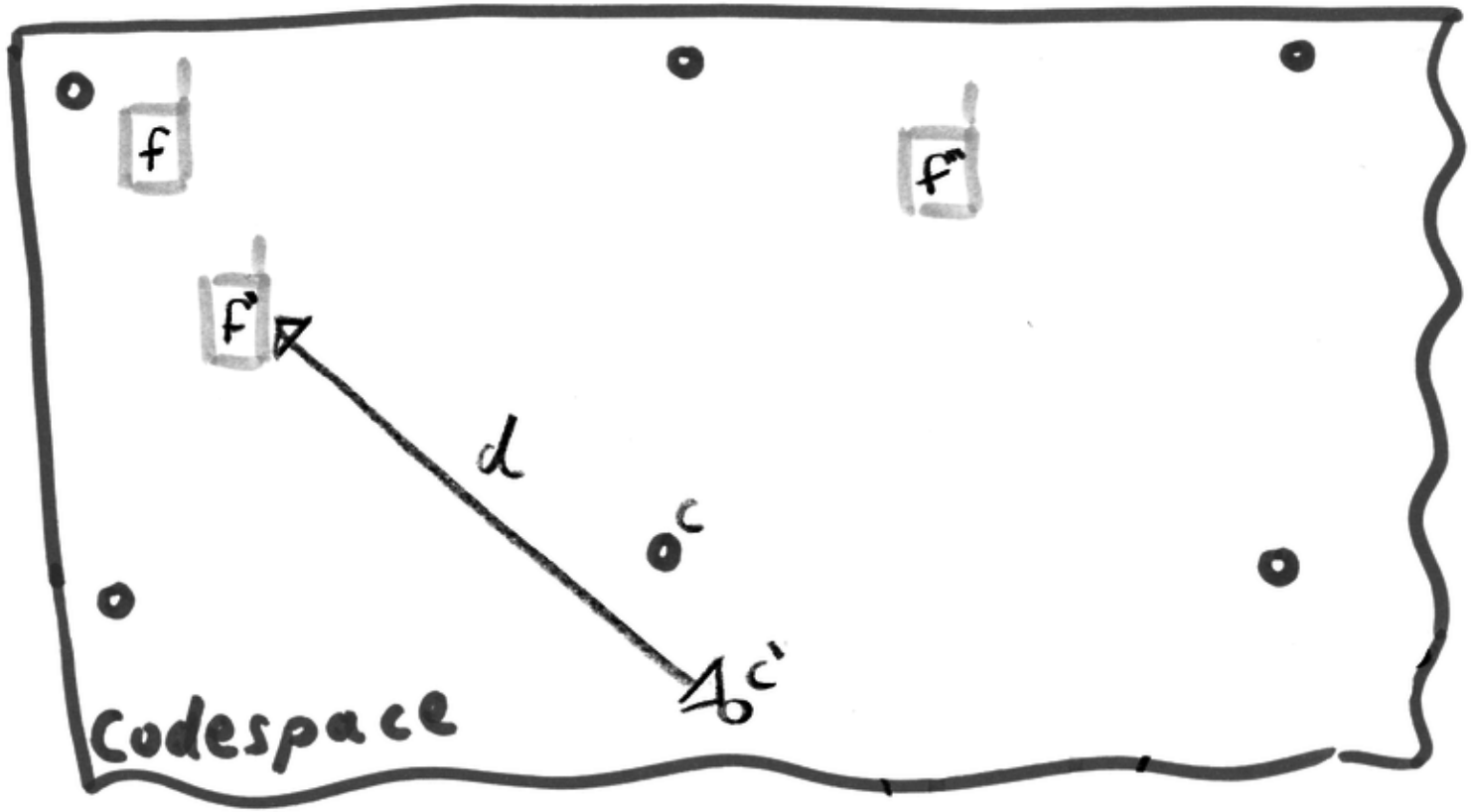
Spontaneous audio-based device pairing



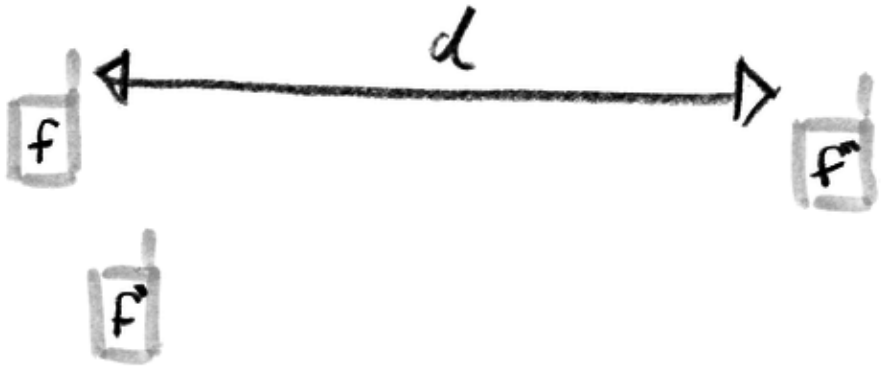
Spontaneous audio-based device pairing



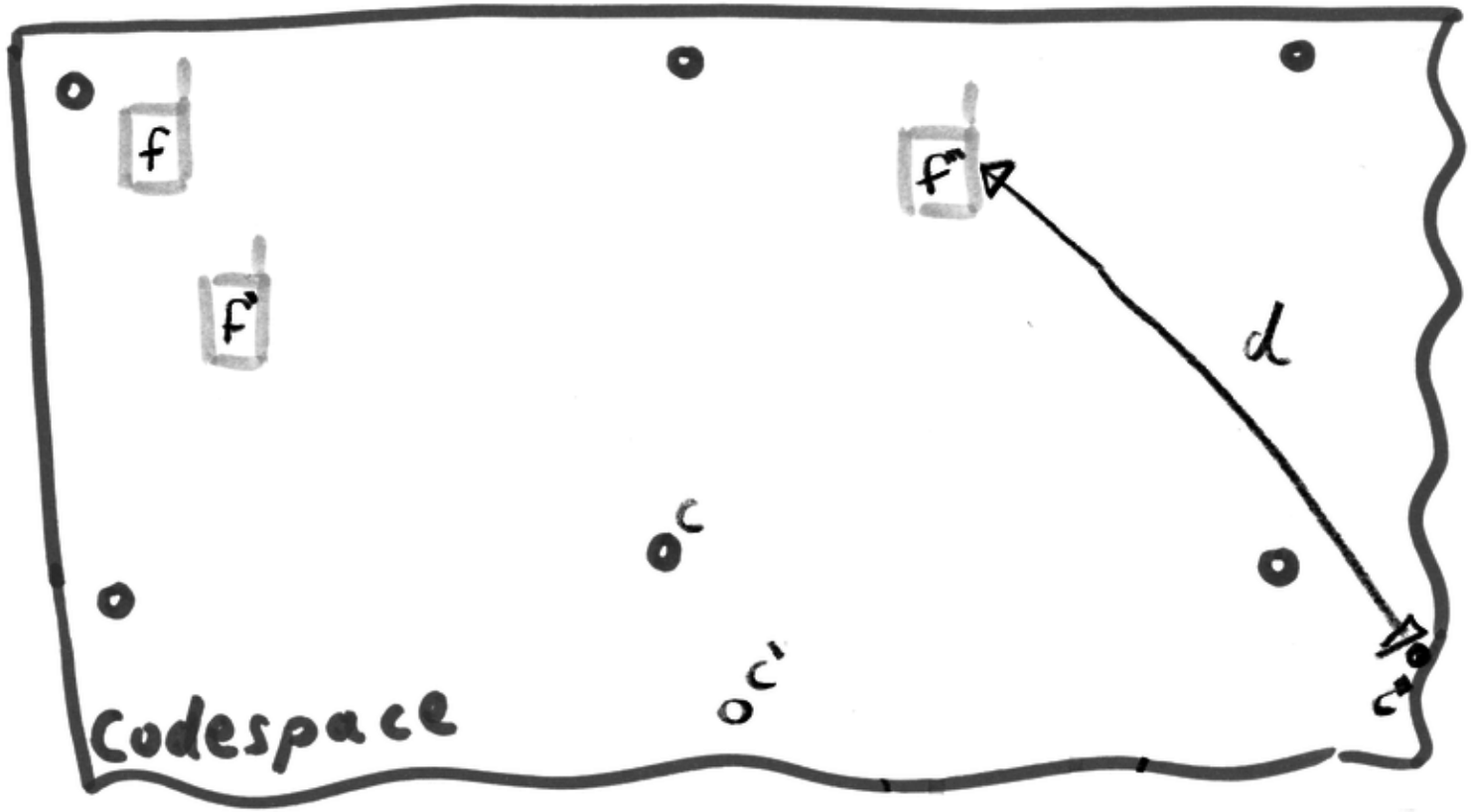
Spontaneous audio-based device pairing



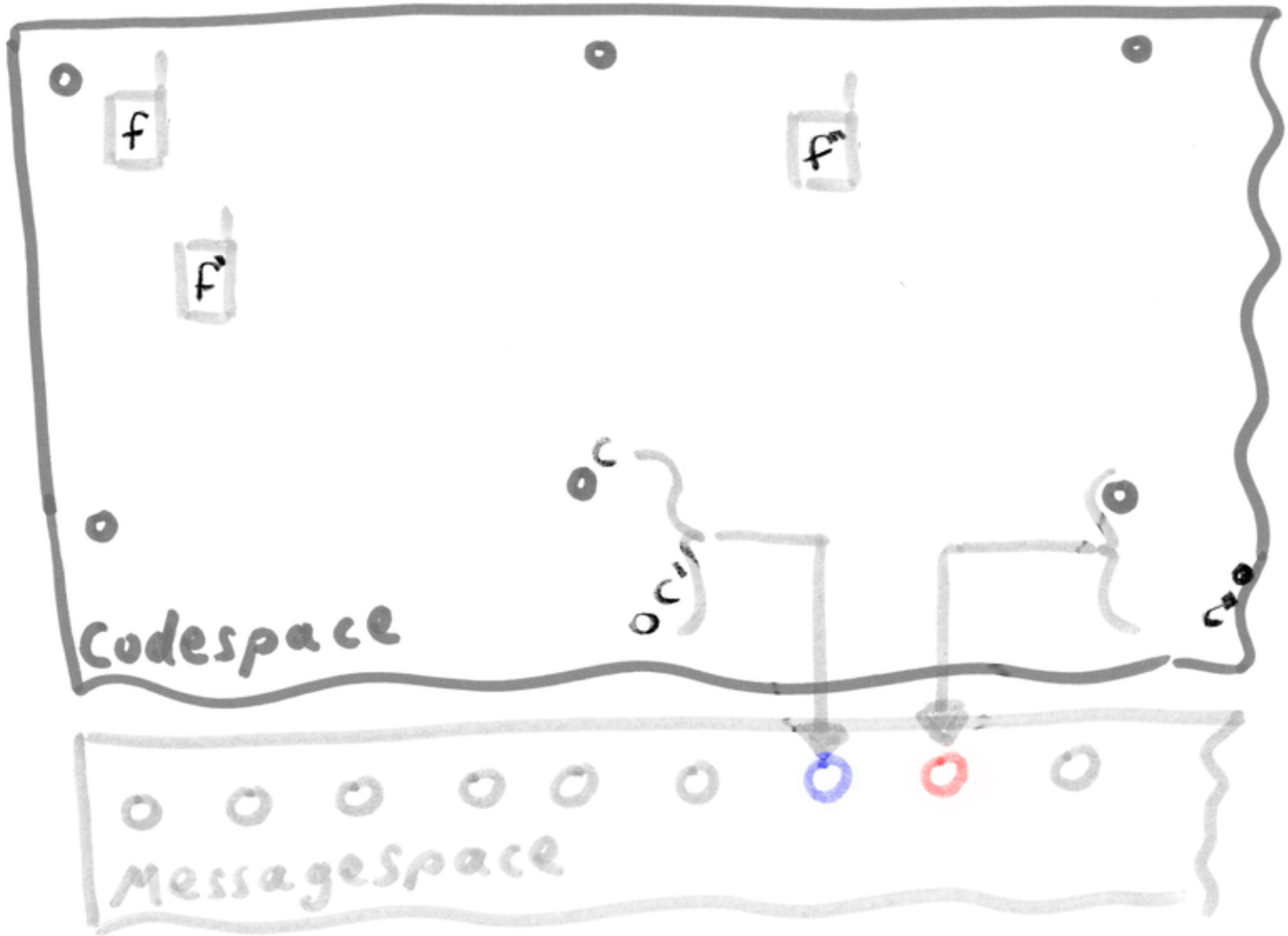
Spontaneous audio-based device pairing



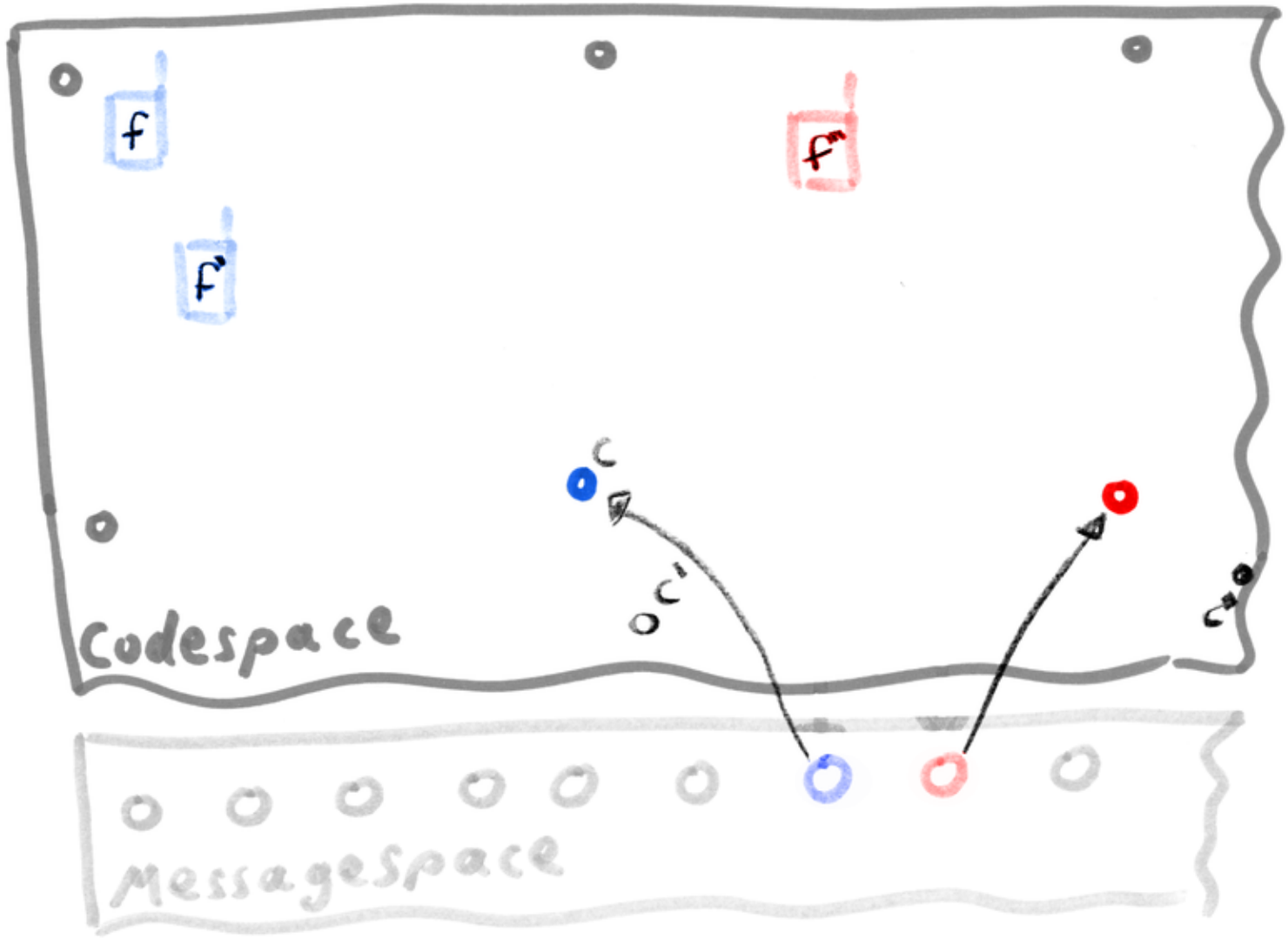
Spontaneous audio-based device pairing



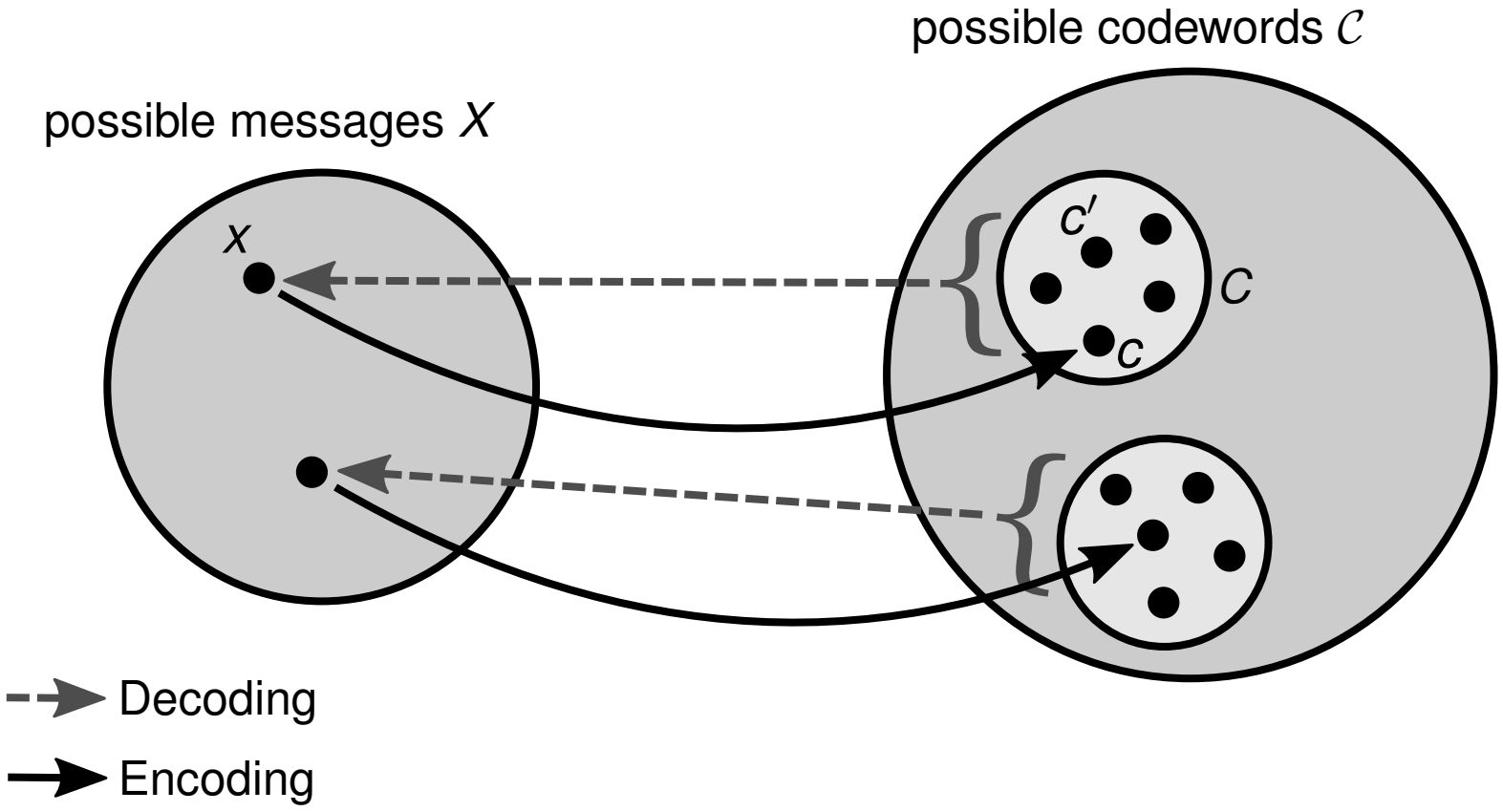
Spontaneous audio-based device pairing



Spontaneous audio-based device pairing

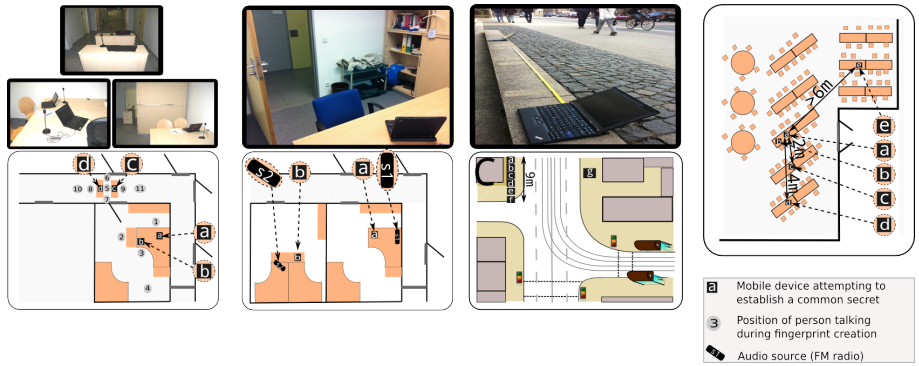


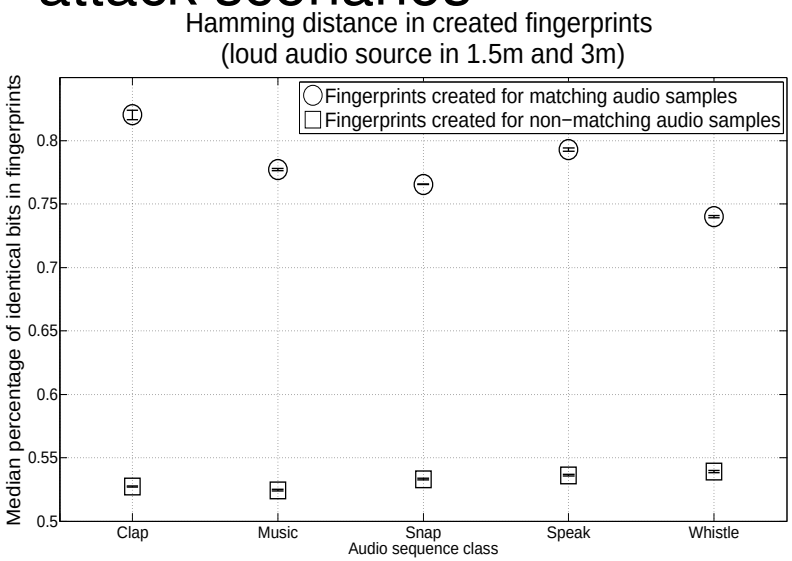
Secure pairing from noisy data

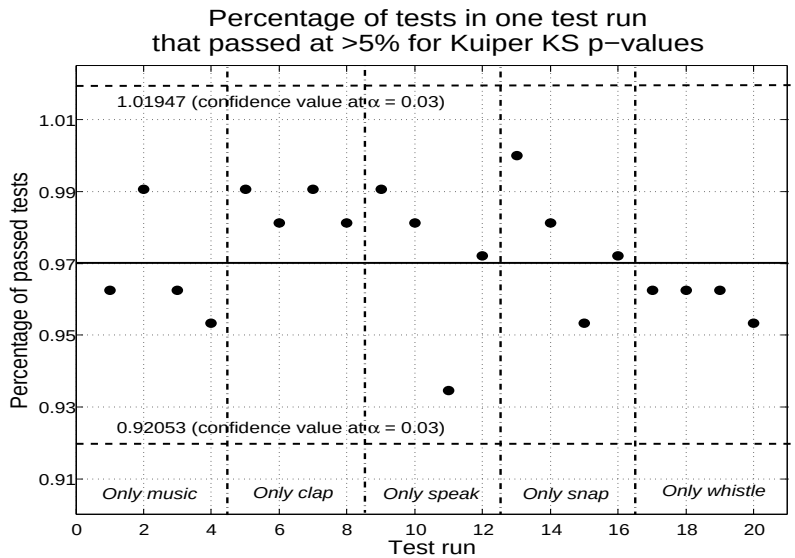


Audio-based ad-hoc secure pairing[1]

- Use audio to generate secret key
- high Entropy, fuzzy cryptography, case studies, attack scenarios





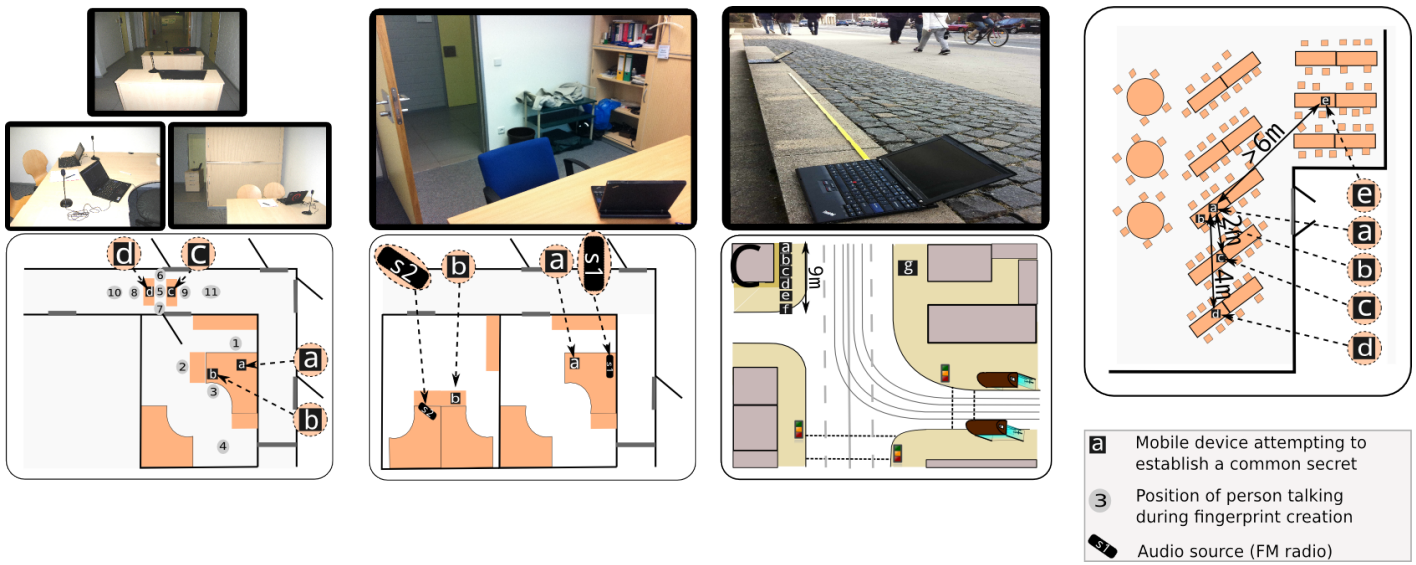


[1] S. Sigg et al., Secure Communication based on Ambient Audio, IEEE Transactions on Mobile Computing

Security from environmental stimuli

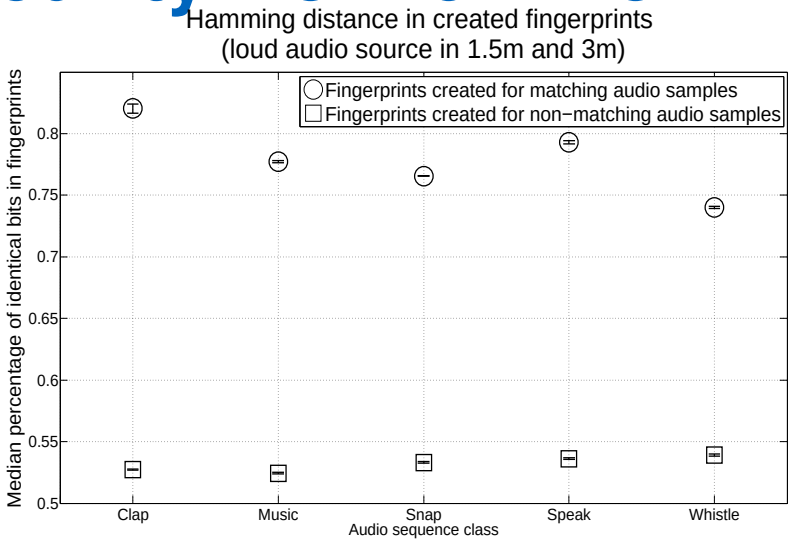
Audio-based ad-hoc secure pairing[2]

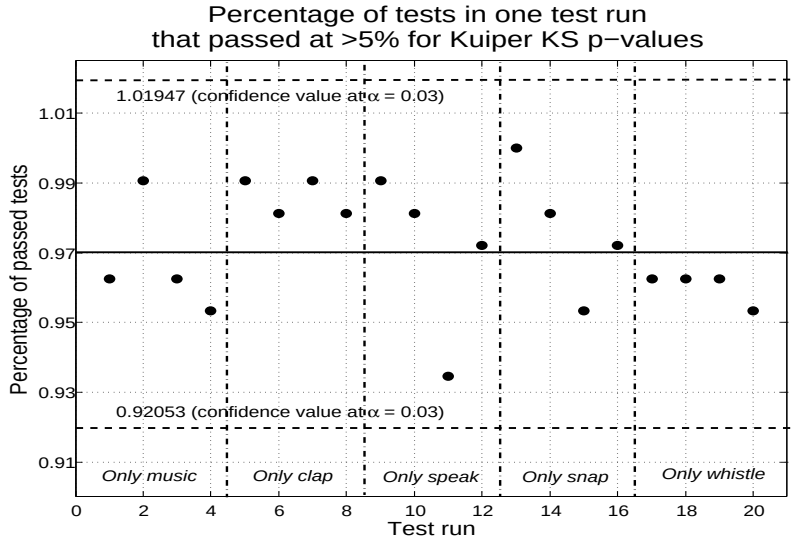
- Audio as common context source
- Fuzzy cryptography

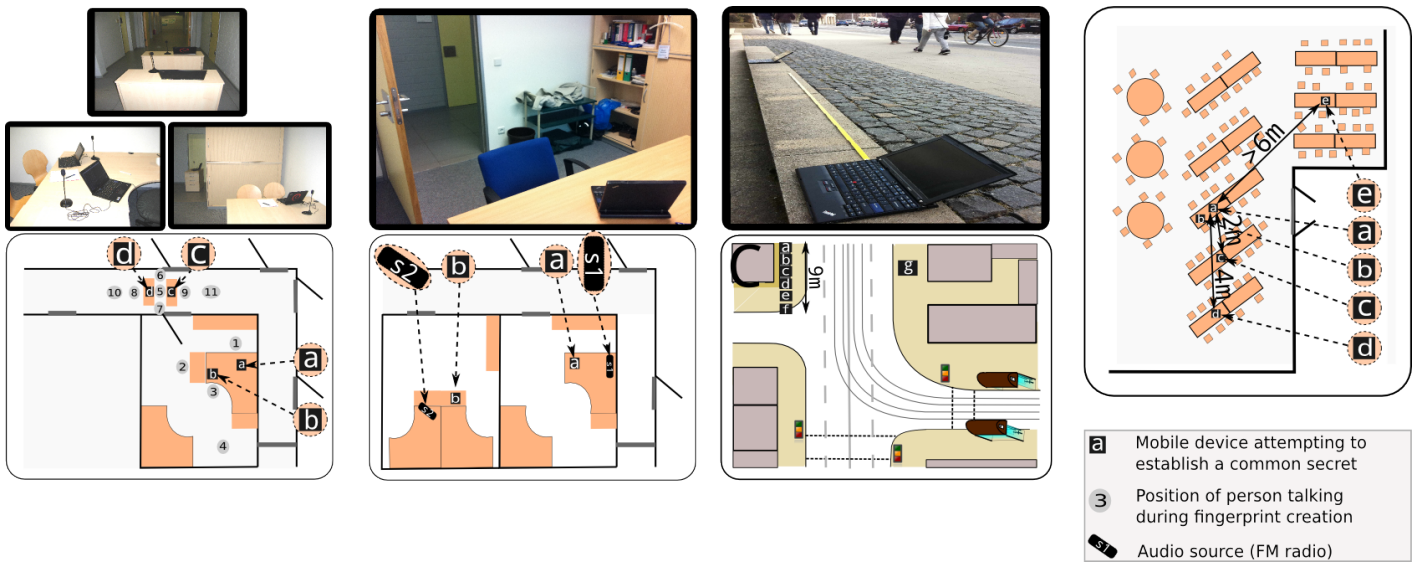


[2] S. Sigg et al., Secure Communication based on Ambient Audio, IEEE Transactions on Mobile Computing, vol. 12, no. 2, 2013

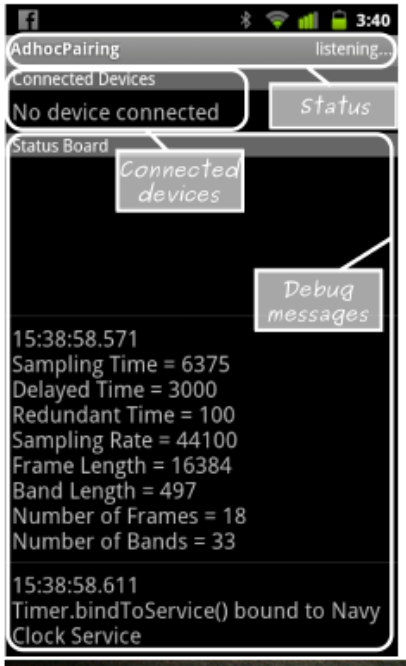
Security from environmental stimuli

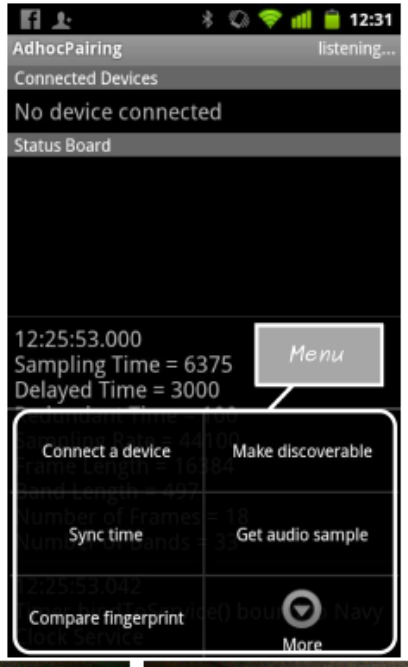


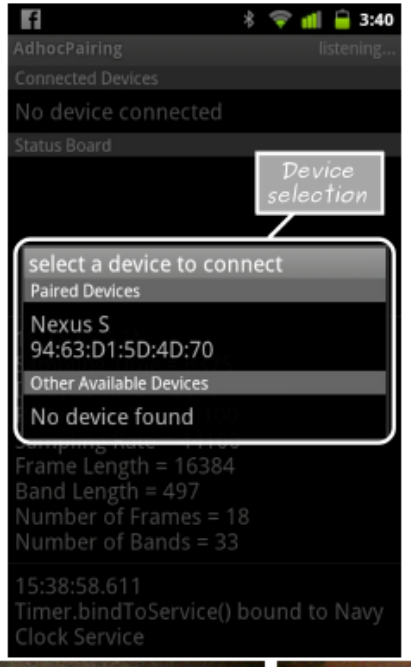


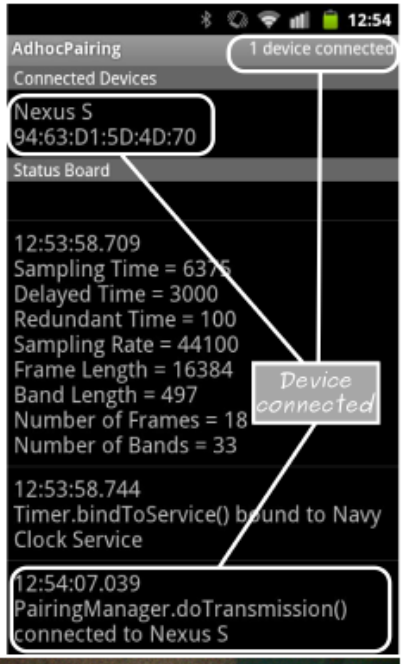


[2] S. Sigg et al., Secure Communication based on Ambient Audio, IEEE Transactions on Mobile Computing, vol. 12, no. 2, 2013

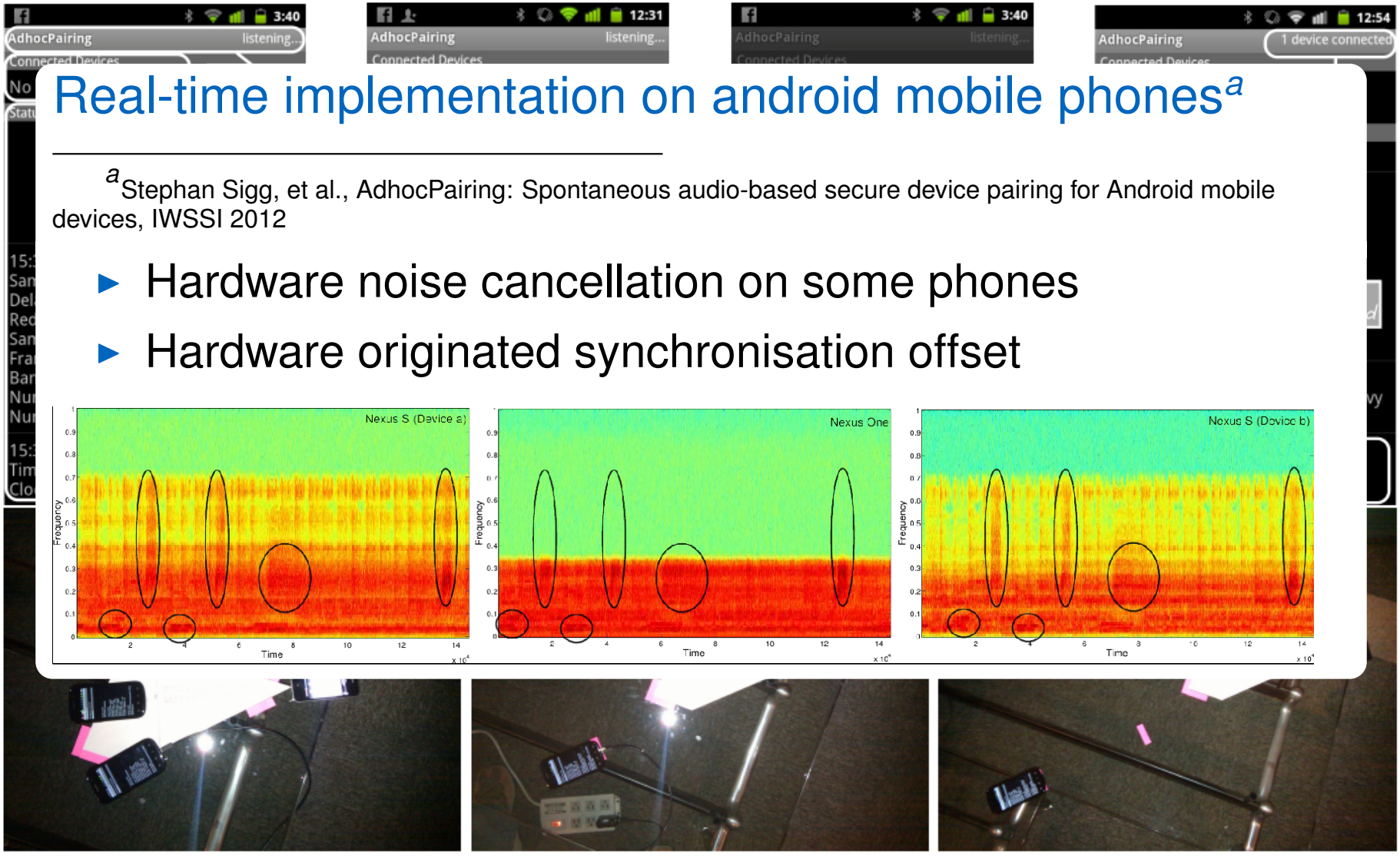

3:40
AdhocPairing
listening...
Connected Devices
No device connected
Status
Status Board
Connected devices
Debug messages
15:38:58.571
Sampling Time = 6375
Delayed Time = 3000
Redundant Time = 100
Sampling Rate = 44100
Frame Length = 16384
Band Length = 497
Number of Frames = 18
Number of Bands = 33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

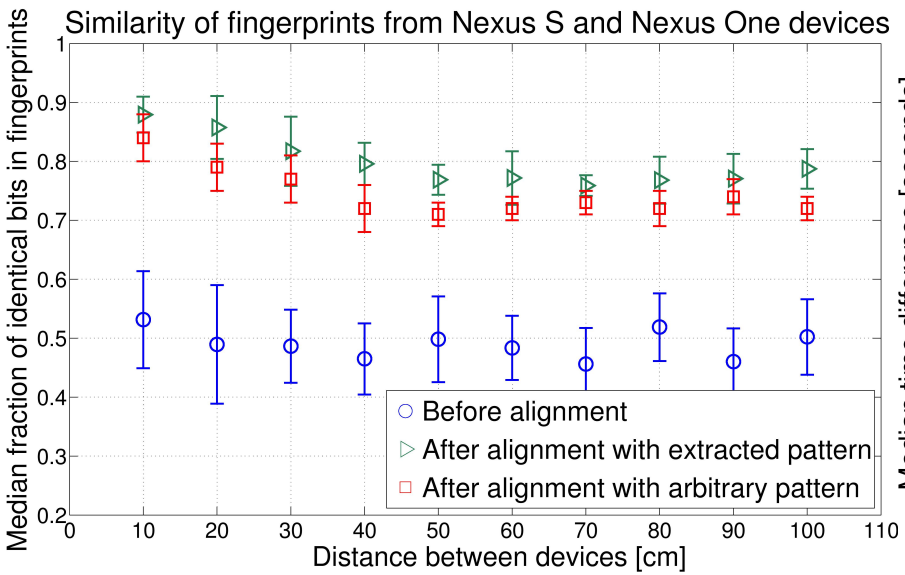
Hardware-originated synchronisation offset

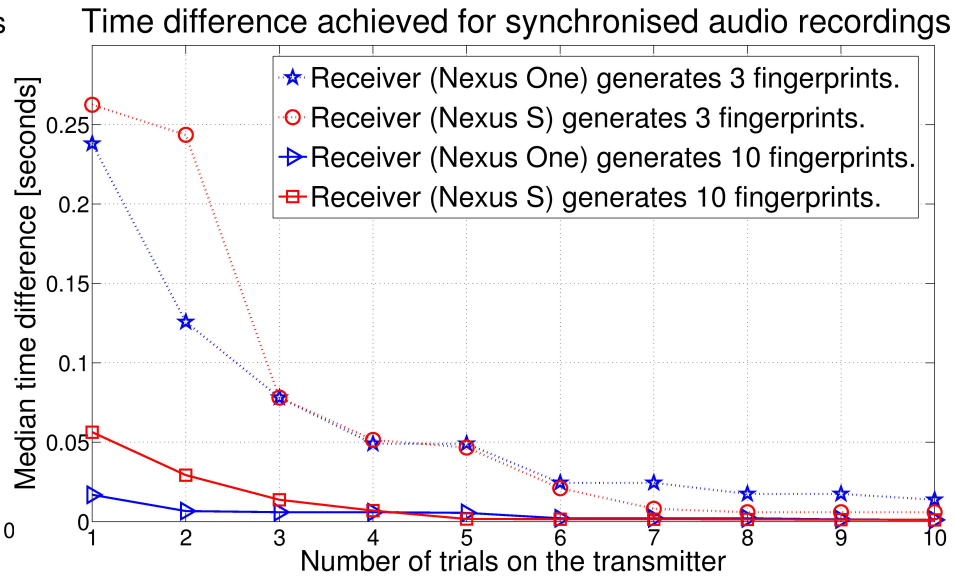
- Approximate pattern matching with arbitrary common sequence [a]

[a] T. F. Smith and M. S. Waterman. Identification of common molecular subsequences. Journal of molecular biology, 147(1):195?197, Mar. 1981

Security from environmental stimuli

Hardware-originated synchronisation offset





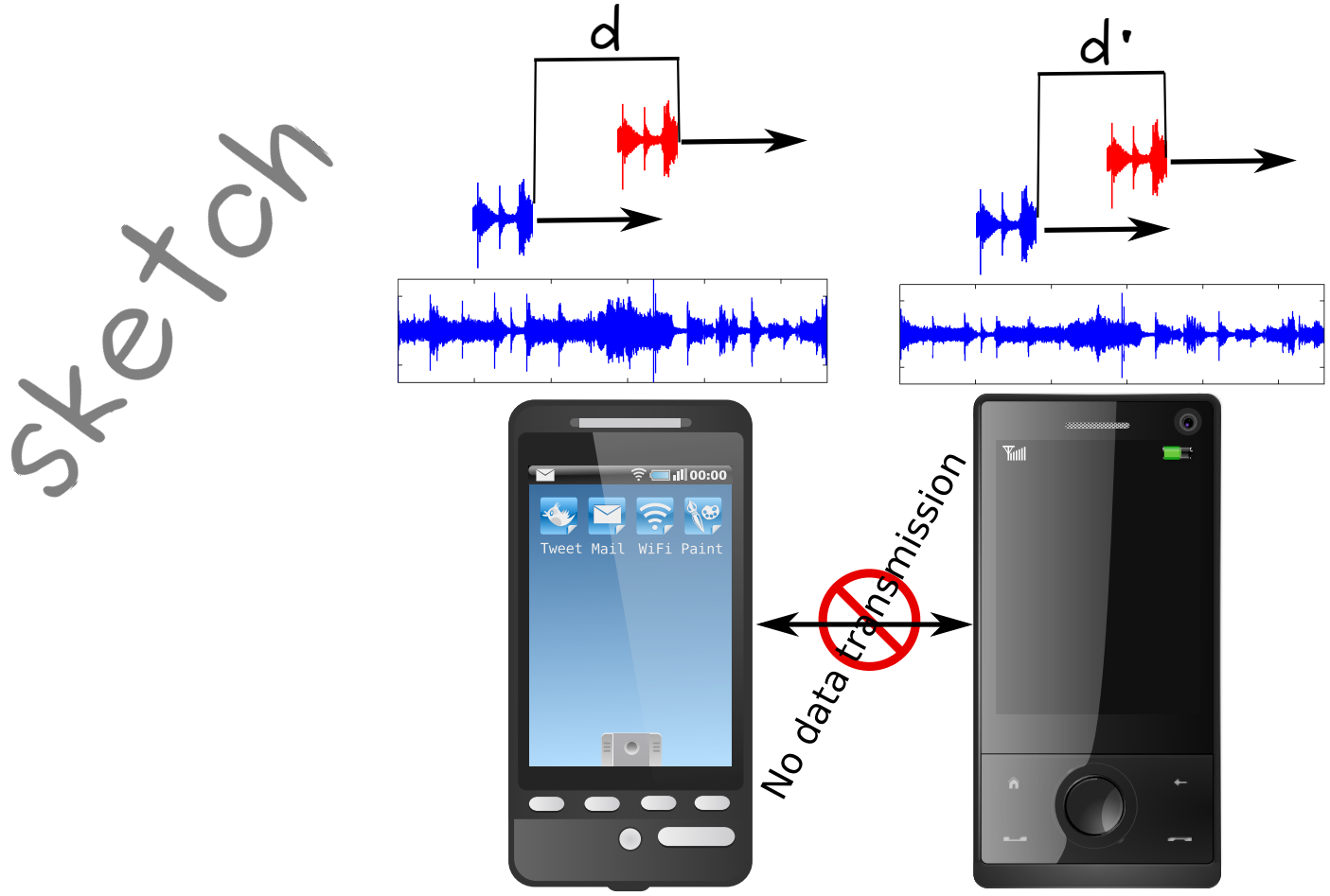
- Synchronisation in the order of 3ms possible
- No additional data transmitted among devices[3] [4]

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

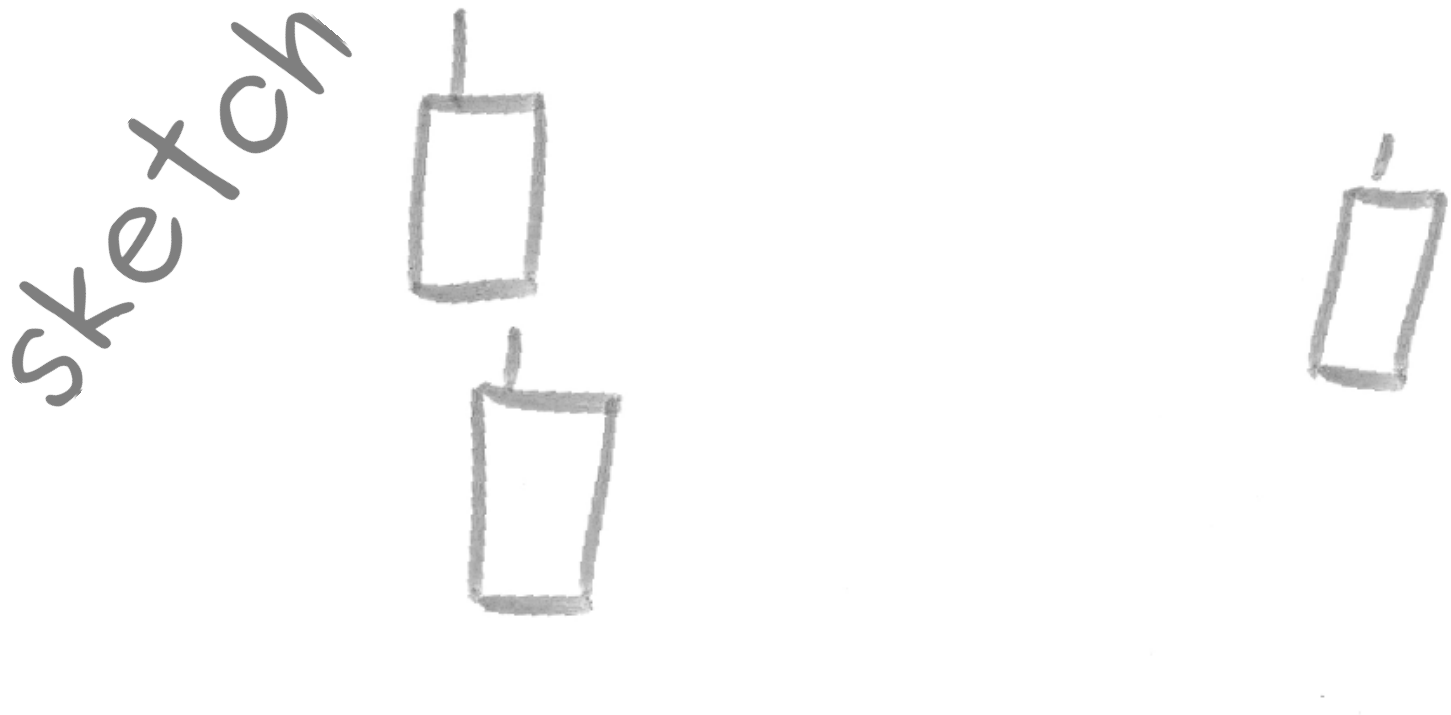
[4] N. Nguyen, S. Sigg, A. Huynh and Y. Ji: Using ambient audio in secure mobile phone communication, PerCom, 2012

Security from environmental stimuli

Security from environmental stimuli

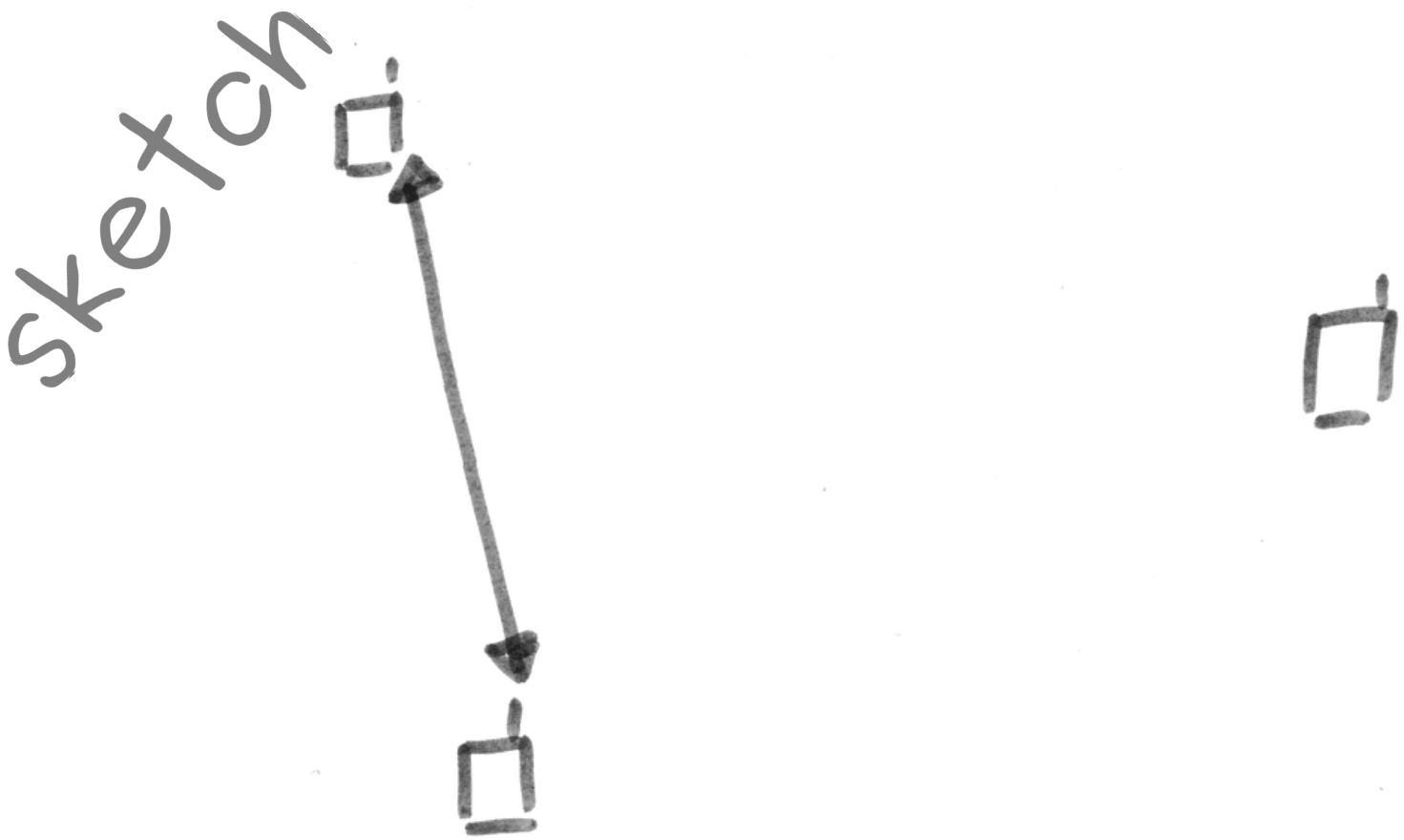


Security from environmental stimuli



Security from environmental stimuli

Security from environmental stimuli



Security from environmental stimuli