Aalto University
School of Electrical
Engineering

Ambient Intelligence

Usable Security

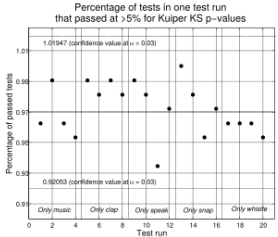
Stephan Sigg

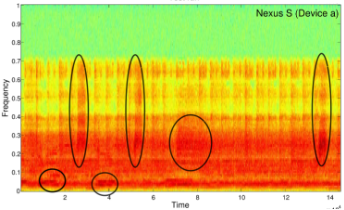
Department of Information and Communications Engineering
Aalto University, School of Electrical Engineering
stephan.sigg@aalto.fi

Version 1.0, February 1, 2023

Applicatons:

Audio





Acceleration (Gait)

Acceleration (Ballistocardiography)

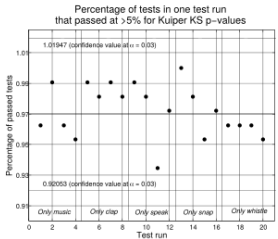
[1] Schuermann, Sigg. Secure communication based on ambient audio. IEEE TMC 12(2). 2013

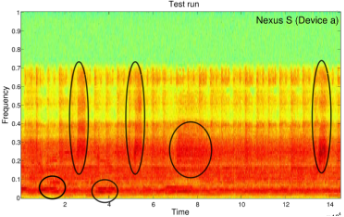
[2] Schuermann, Bruesch, Sigg, Wolf. BANDANA – Body Area Network Device-to-device Authentication using Natural gAit. IEEE PerCom'17.

[3] Schuermann, Bruesch, Nguyen, Sigg, Wolf. Moves like Jagger: Exploiting variations in instantaneous gait for spontaneous device pairing. PMC'18.

Applicatons:

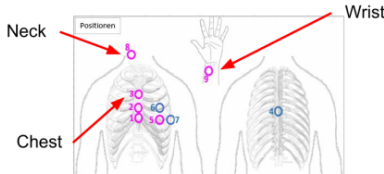
Audio

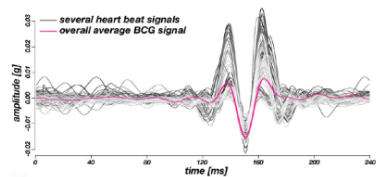




Acceleration (Gait)

Acceleration (Ballistocardiography)





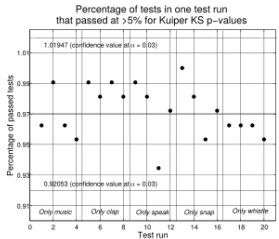
[1] Schuermann, Sigg. Secure communication based on ambient audio. IEEE TMC 12(2). 2013

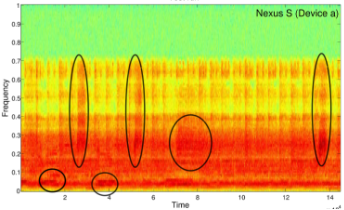
[2] Schuermann, Bruesch, Sigg, Wolf. BANDANA – Body Area Network Device-to-device Authentication using Natural gAit. IEEE PerCom'17.

[3] Schuermann, Bruesch, Nguyen, Sigg, Wolf. Moves like Jagger: Exploiting variations in instantaneous gait for spontaneous device pairing. PMC'18.

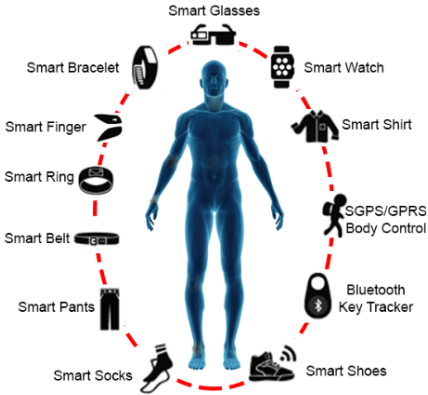
Applicatons:

Audio

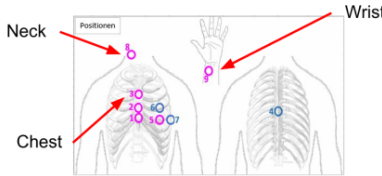


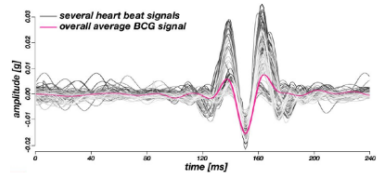


Acceleration (Gait)



Acceleration (Ballistocardiography)





[1] Schuermann, Sigg. Secure communication based on ambient audio. IEEE TMC 12(2). 2013

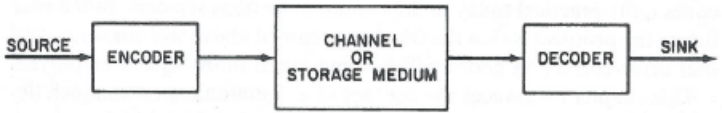
[2] Schuermann, Bruesch, Sigg, Wolf. BANDANA – Body Area Network Device-to-device Authentication using Natural gAit. IEEE PerCom'17.

[3] Schuermann, Bruesch, Nguyen, Sigg, Wolf. Moves like Jagger: Exploiting variations in instantaneous gait for spontaneous device pairing. PMC'18.

Outline

Introduction

We consider a communication system in which the channel between the encoder and the decoder might be impaired by noise



Introduction

Types of Codes

Block codes Breaks the continuous sequence of information digits into k-symbol sections or blocks. It then operates on these blocks independently

Tree codes operate on the information sequence without breaking it up into independent blocks. An important subclass are convolutional codes since they are simple to implement

Block codes

Let q denote the number of distinct symbols employed on the channel

A block code is a set of M sequences of channel symbols of length n

Decision to which code word a received word belongs may be based on a decoding table

Code Words	1 1 0 0 0	0 0 1 1 0	1 0 0 1 1	0 1 1 0 1
	1 1 0 0 1	0 0 1 1 1	1 0 0 1 0	0 1 1 0 0
Other Received Words	1 1 0 1 0	0 0 1 0 0	1 0 0 0 1	0 1 1 1 1
	1 1 1 0 0	0 0 0 1 0	1 0 1 1 1	0 1 0 0 1
	1 0 0 0 0	0 1 1 1 0	1 1 0 1 1	0 0 1 0 1
	0 1 0 0 0	1 0 1 1 0	0 0 0 1 1	1 1 1 0 1
	1 1 1 1 0	0 0 0 0 0	0 1 0 1 1	1 0 1 0 1
	0 1 0 1 0	1 0 1 0 0	1 1 1 1 1	0 0 0 0 1

Linear Block codes – generating code vectors

For linear block codes we require a set of k basis vectors $\vec{g}$ (generator vectors) of length n

Basis vectors are linear independent vectors that span the basis of a vector space

These vectors are considered as rows of a matrix G

The row-space of G defines the linear code V and code vectors $\vec{v}$ are linear combinations of rows in G

It is important that the vectors g are linear independent since otherwise different linear combinations of vectors would lead to identical code vectors

$$G = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{bmatrix}$$

Linear Block codes – detect errors

Data vectors $\overrightarrow{d}$ define which generator vectors g are combined to a code vector $\overrightarrow{v}$

We define a matrix H of rank $n-k$ whose row space is a basis of vectors orthogonal to each vector in G (null space)

Since each code vector $\overrightarrow{v}$ is the result of a linear combination of generator vectors $\overrightarrow{g}$, we have

$$\overrightarrow{v} H^T = \overrightarrow{0}$$

In the case of errors in the code vector, the result is hence

$$(\overrightarrow{v} + \overrightarrow{e}) H^T \neq \overrightarrow{0}$$

iff $(\overrightarrow{v} + \overrightarrow{e}) \notin \overrightarrow{\alpha} G$

Block codes

In the case of errors in the code vector, the result is hence

$$(\overrightarrow{v} + \overrightarrow{e})H^T \neq \overrightarrow{0}$$

The error vector $\overrightarrow{e}$ then defines the linear combination of rows of H^T that lead to the syndrome:

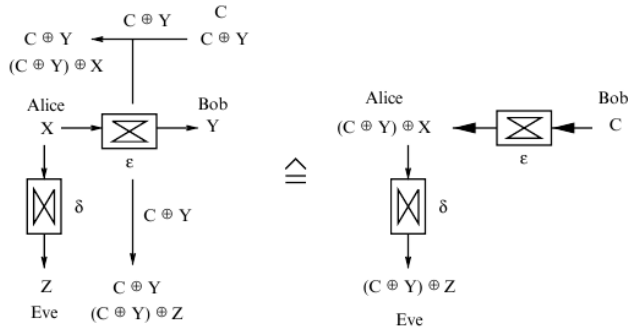
$$\begin{aligned} & (\overrightarrow{v} + \overrightarrow{e})H^T \\ = \overrightarrow{v}H^T & + \overrightarrow{e}H^T \\ = \overrightarrow{0} & + \overrightarrow{e}H^T \\ = \overrightarrow{s} & \end{aligned}$$

H is spanned by basis vectors$\rightarrow \overrightarrow{s}$ defines uniquely the error vectors that occurred.

Outline

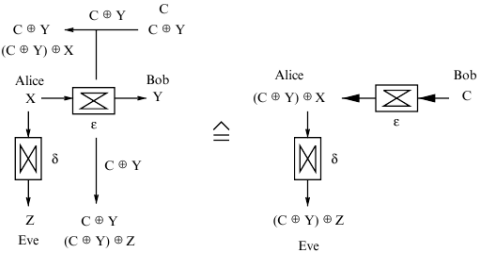
Fuzzy cryptography

Utilise noise to improve security



Fuzzy cryptography

Utilise noise to improve security

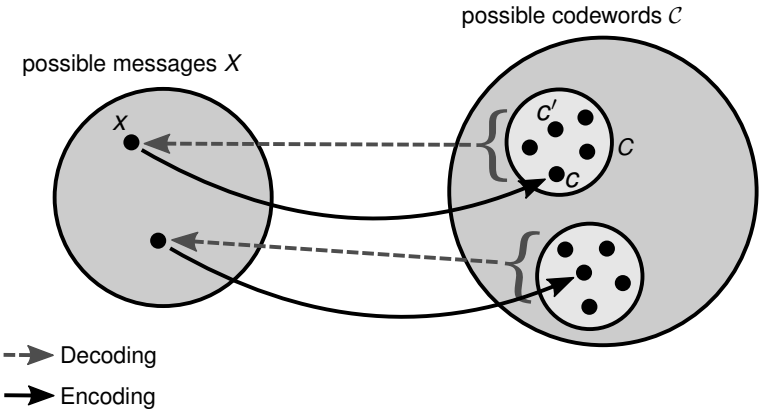


By inverting the direction of communication the noise in Eve's reception is increased above those in Alice's

Establishing of a secure key is possible over binary symmetric channel iff the noise in the reception of Eve's message is higher[1]

[1] Wyner, The wire-tap channel, Bell system Technical Journal, 54:1355-1387,1975

Utilisation of Fuzzy cryptography to mitigate errors



Fuzzy cryptography

Traditional cryptographic systems rely on secret bit-strings.

When key contains errors (e.g. noise or mistake), decryption fails.

impracticable in noisy systems.

Fuzzy commitment: cryptographic primitive to handle independent random corruptions of bits in a key.

Fuzzy cryptography

A cryptographic commitment scheme is a function

$$G : C \times X \to Y$$

To commit a value $\kappa \in C$ a witness $x \in X$ is chosen and $y = G(\kappa, x)$ is computed.

A decommitment function takes y and a witness to obtain the original κ

$$G^{-1} : Y \times X \to C$$

Fuzzy cryptography

Traditional Commitment

A well defined commitment scheme shall have two basic properties.

Binding It is infeasible to de-commit y under a pair (κ', x') such that $\kappa \neq \kappa'$

Hiding Given y alone, it is infeasible to compute κ

Fuzzy cryptography

Fuzzy commitment is an encryption scheme that allows for the use of *approximate* witnesses

Given a commitment $y = G(\kappa, x)$, the system can recover κ from any witness x' that is close to but not necessarily equal to x.

Closeness in fuzzy commitment is measured by Hamming distance.

Fuzzy cryptography

A fuzzy commitment scheme may be based on any (linear) error-correcting code

An error-correcting code consists of

Message space $M \subseteq F^a$ (F^i denotes all strings of length i from a finite set of symbols F)

Codeword space $C \subseteq F^b$ with $(b > a)$

Bijection $\theta : M \leftrightarrow C$

Decoding function $f : C' \rightarrow C \cup \perp$ (The symbol $\perp$ denotes the failure of f)

The function f maps an element in C' to its nearest codeword in C.

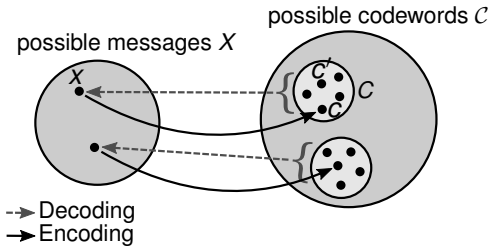
Fuzzy cryptography

Noise of physical function may be viewed as the difference $c - c'$

Decoding function f applied to recover original codeword c

This is successful if c' is close to c. In this case: $c = f(c')$

The minimum distance of the code is the smallest distance $d = Ham(c - c')$ between any two codewords $c, c' \in C$



Fuzzy cryptography

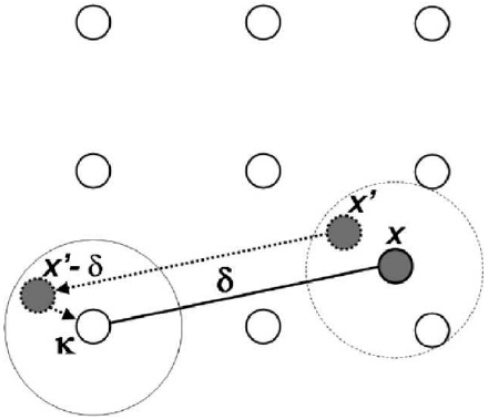
For fuzzy commitment, the secret key κ is chosen uniformly at random from the codeword space C. Then,

1. An offset $\delta = x - \kappa$ is computed
2. A one-way, collision-resistant hash function is applied to obtain $h(\kappa)$
3. $y = (\delta, h(\kappa))$ is made public
4. $\kappa' = f(x' - \delta)$ is computed
5. It is possible to de-commit y under a witness x' with $Ham(x, x') < \frac{d}{2}$

Once κ is recovered, its correctness may be verified by computing $z = h(\kappa)$

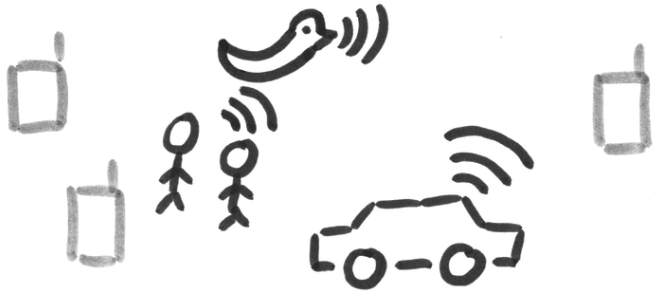
Fuzzy cryptography

Fuzzy Commitment

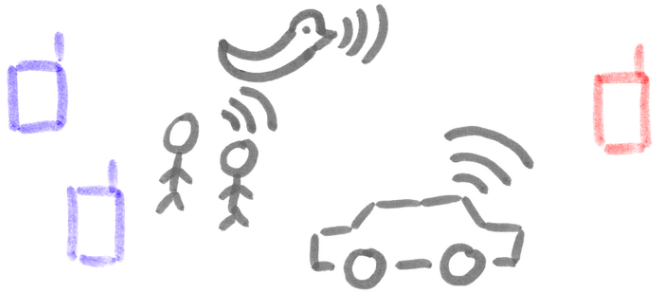


Example: Spontaneous audio-based device pairing

Example: Spontaneous audio-based device pairing

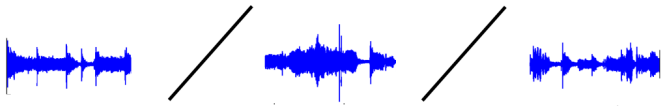


Example: Spontaneous audio-based device pairing

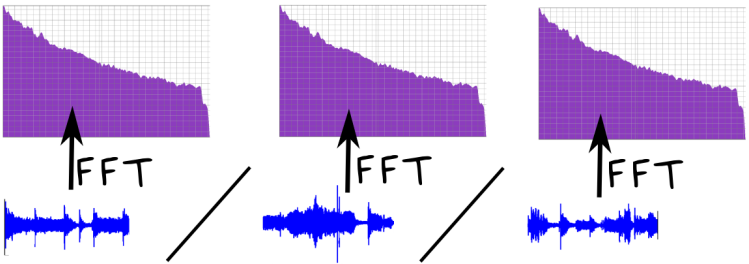


Example: Spontaneous audio-based device pairing

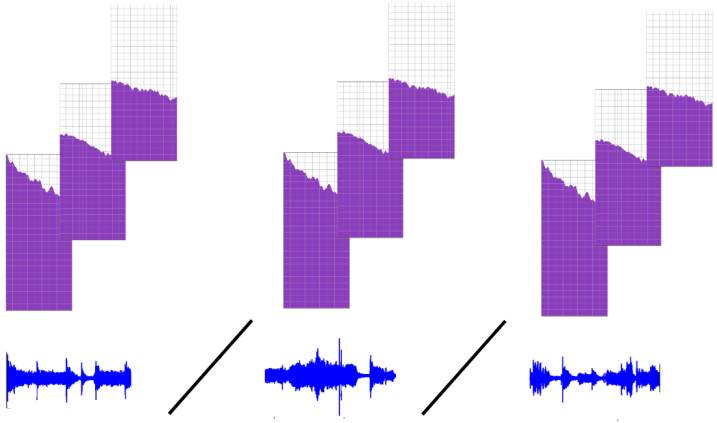
Example: Spontaneous audio-based device pairing



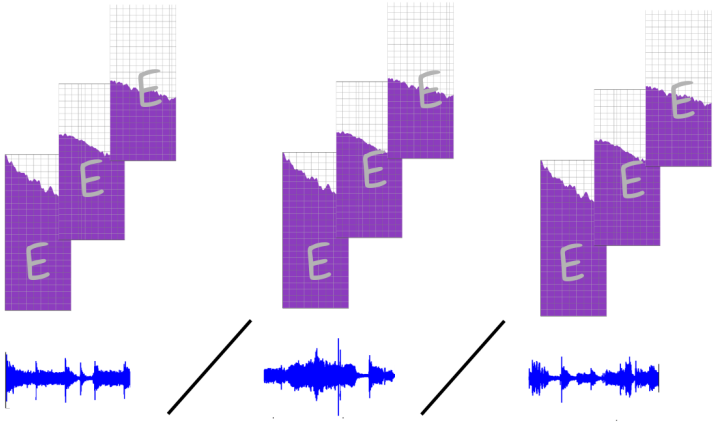
Example: Spontaneous audio-based device pairing



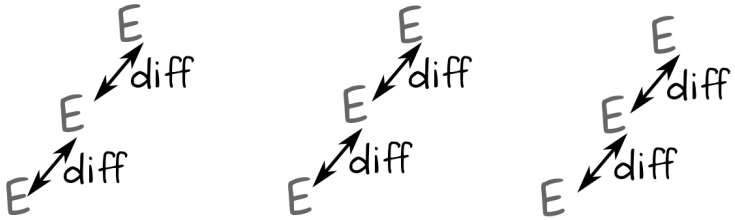
Example: Spontaneous audio-based device pairing



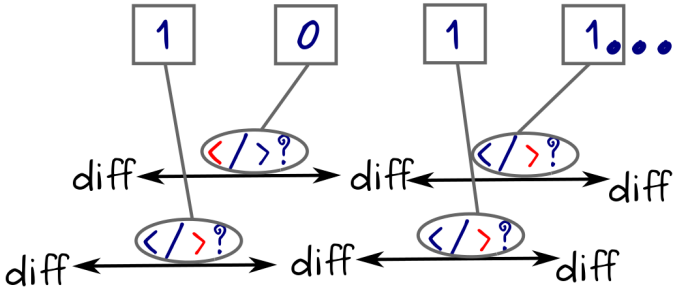
Example: Spontaneous audio-based device pairing



Example: Spontaneous audio-based device pairing



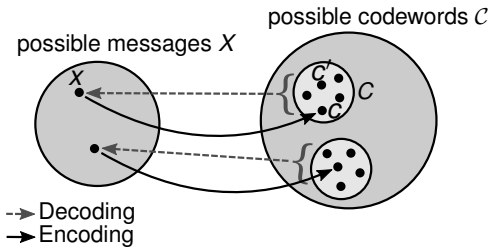
Example: Spontaneous audio-based device pairing



Encryption and decryption in the presence of noise

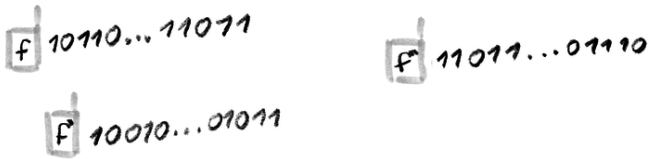
Fuzzy cryptography

- We can, however, utilise error correcting codes to account for errors in an input sequence
- The general idea is to utilise a function that maps from a feature space to another, key space

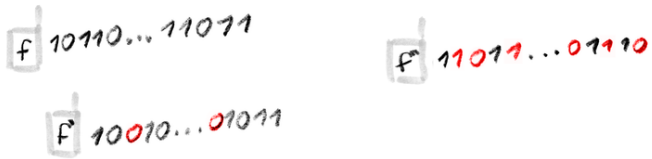


Example: Spontaneous audio-based device pairing

Example: Spontaneous audio-based device pairing

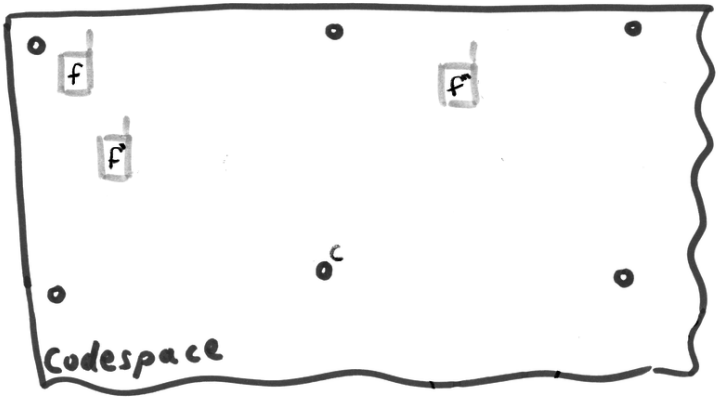


Example: Spontaneous audio-based device pairing

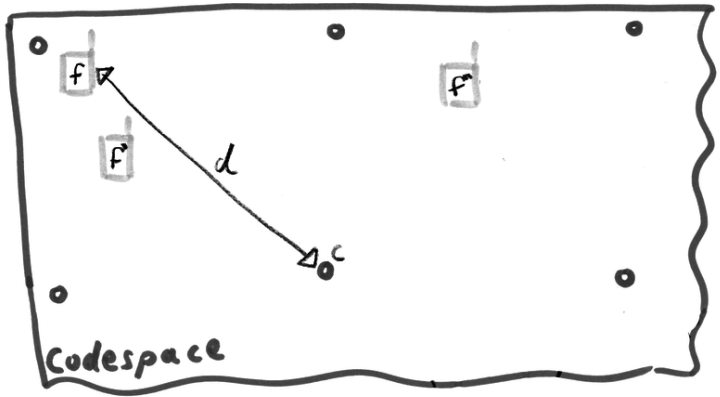


Example: Spontaneous audio-based device pairing

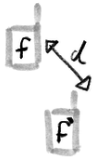
Example: Spontaneous audio-based device pairing



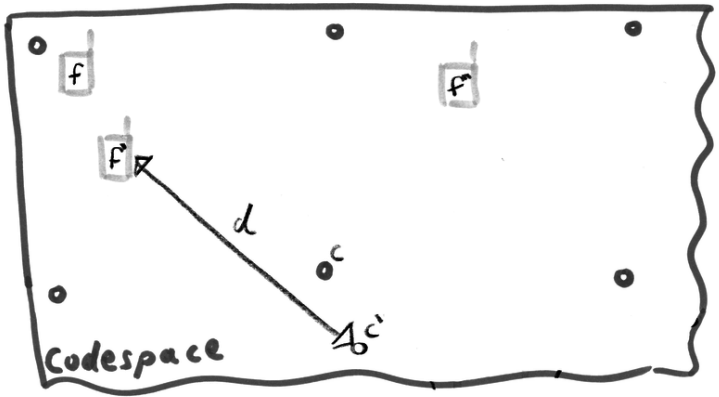
Example: Spontaneous audio-based device pairing



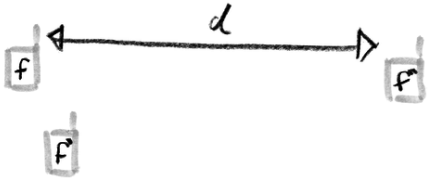
Example: Spontaneous audio-based device pairing



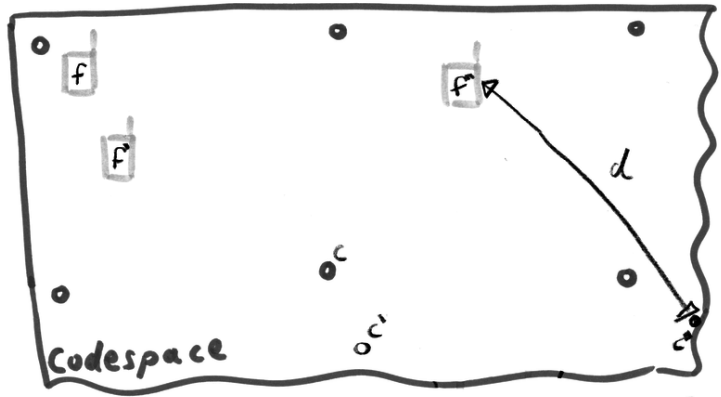
Example: Spontaneous audio-based device pairing



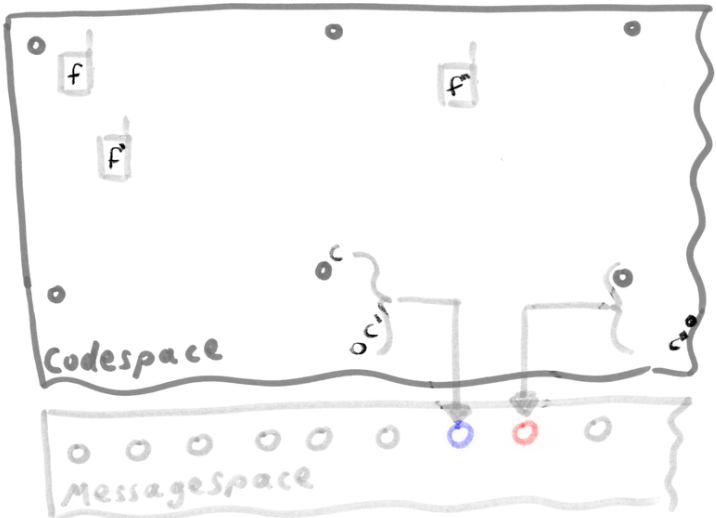
Example: Spontaneous audio-based device pairing



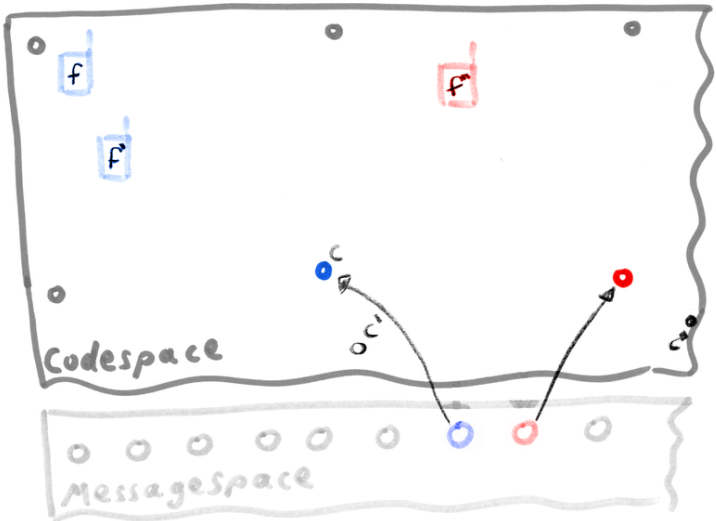
Example: Spontaneous audio-based device pairing



Example: Spontaneous audio-based device pairing



Example: Spontaneous audio-based device pairing



Outline

Introduction

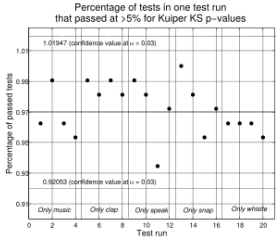
Error correcting codes

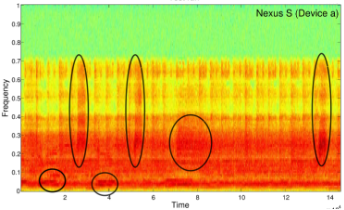
Fuzzy Cryptography

Applications in Usable Security

Applicatons:

Audio





Acceleration (Gait)

Acceleration (Ballistocardiography)

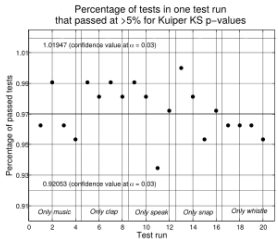
[1] Schuermann, Sigg. Secure communication based on ambient audio. IEEE TMC 12(2). 2013

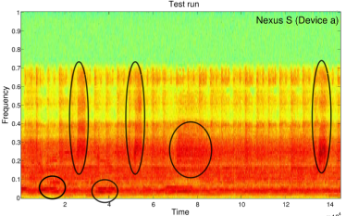
[2] Schuermann, Bruesch, Sigg, Wolf. BANDANA – Body Area Network Device-to-device Authentication using Natural gAit. IEEE PerCom'17.

[3] Schuermann, Bruesch, Nguyen, Sigg, Wolf. Moves like Jagger: Exploiting variations in instantaneous gait for spontaneous device pairing. PMC'18.

Applicatons:

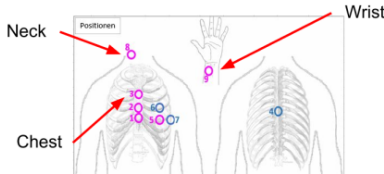
Audio

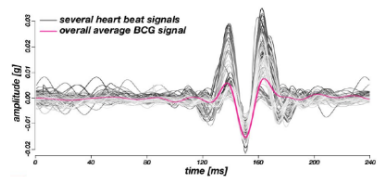




Acceleration (Gait)

Acceleration (Ballistocardiography)





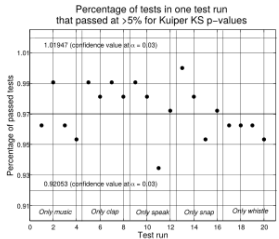
[1] Schuermann, Sigg. Secure communication based on ambient audio. IEEE TMC 12(2). 2013

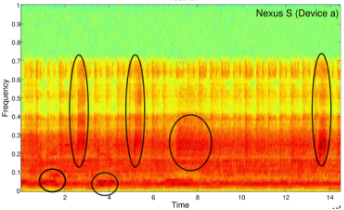
[2] Schuermann, Bruesch, Sigg, Wolf. BANDANA – Body Area Network Device-to-device Authentication using Natural gAit. IEEE PerCom'17.

[3] Schuermann, Bruesch, Nguyen, Sigg, Wolf. Moves like Jagger: Exploiting variations in instantaneous gait for spontaneous device pairing. PMC'18.

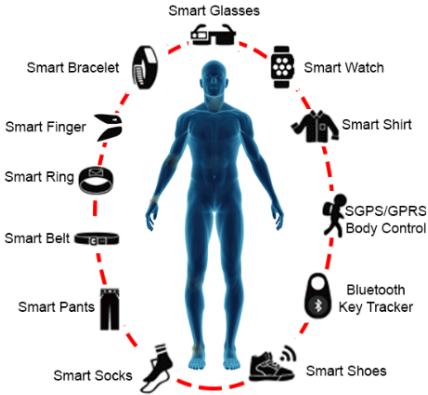
Applicatons:

Audio

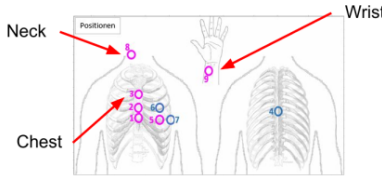


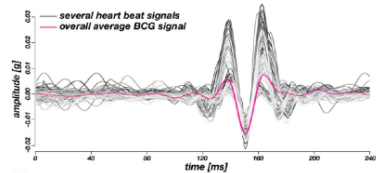


Acceleration (Gait)



Acceleration (Ballistocardiography)





[1] Schuermann, Sigg. Secure communication based on ambient audio. IEEE TMC 12(2). 2013

[2] Schuermann, Bruesch, Sigg, Wolf. BANDANA – Body Area Network Device-to-device Authentication using Natural gAit. IEEE PerCom'17.

[3] Schuermann, Bruesch, Nguyen, Sigg, Wolf. Moves like Jagger: Exploiting variations in instantaneous gait for spontaneous device pairing. PMC'18.

Securely pair devices on their first encounter – No trusted third party



Exploit data stream from local sensor to establish common secret

Exploit data stream from local sensor to establish common secret

$k_A = k_B$

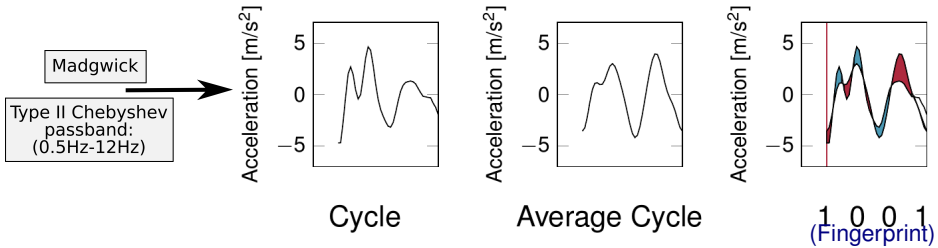
$$k_E \neq k_A = k_B$$

Observations:

- key strength depends on entropy in the data stream

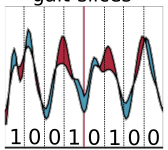
- access to sufficiently similar data stream grants ability to generate correct key

Quantization



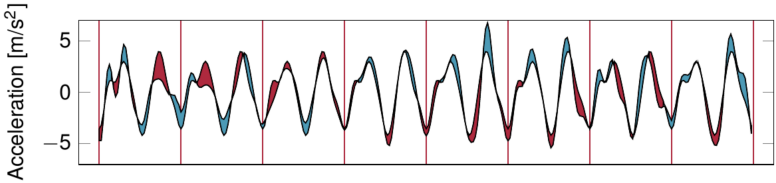
- Average gait cycle overlaid on each original gait cycle
- 4 bits per cycle

Fingerprint bits: Integration over gait-slices

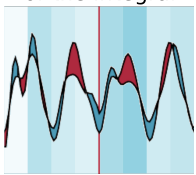


Quantization

Acceleration
(Gait)



Confidence:
absolute value
of the integral



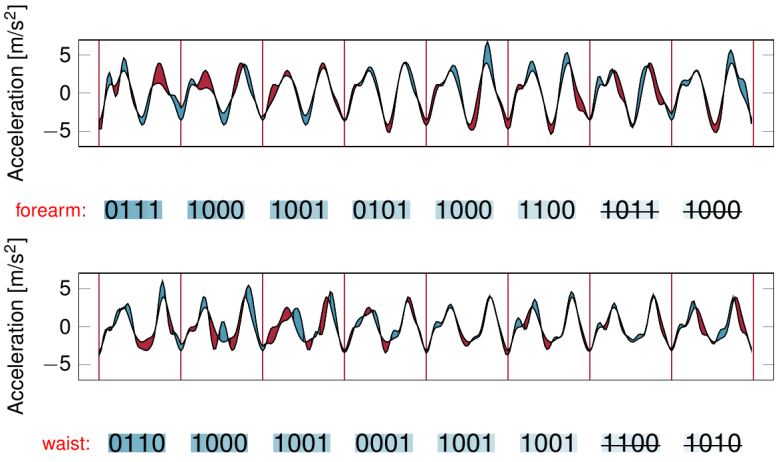
a) 1001 0100 1001 1010 1010 1001 0101 0110 ←Fingerprint

b) 1001 0100 1001 1010 1010 1001 0101 0110 ←Confidence values

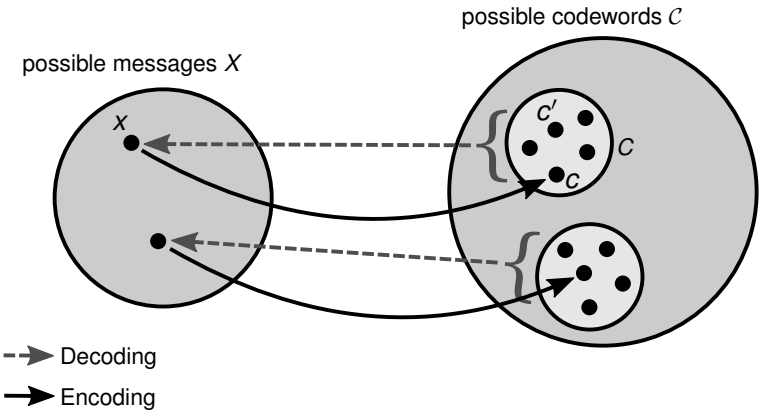
c) 0111 1000 1001 0101 1000 1100 ~~1011~~ ~~1000~~ ←Sorted (Confidence)

Disregard least confident bits

Quantization



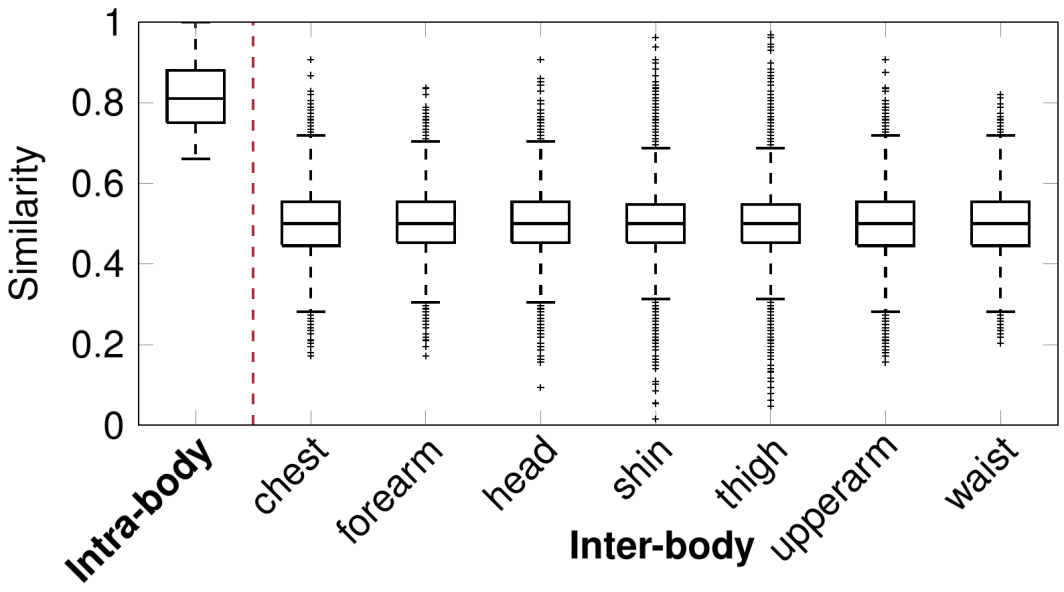
From fingerprints to keys



Acceleration
(Gait)

Audio

Acceleration
(Ballistocardiography)


Similarity
1
0.8
0.6
0.4
0.2
0
Intra-body
chest
forearm
head
shin
thigh
upperarm
waist
Inter-body

Questions?

Stephan Sigg
stephan.sigg@aalto.fi

Si Zuo
si.zuo@aalto.fi

Literature

- C.M. Bishop: Pattern recognition and machine learning, Springer, 2007.
- R.O. Duda, P.E. Hart, D.G. Stork: Pattern Classification, Wiley, 2001.