



Technische  
Universität  
Braunschweig

Institute of Operating Systems  
and Computer Networks



# Secure communication based on noisy input data

Introduction

**Stephan Sigg**

April 19, 2011

# Overview and Structure

- Classification methods
- Feature extraction
  - Features from audio
  - Features from RF
- Fuzzy Commitment
- Fuzzy Extractors
- Authentication with noisy data
- Error correcting codes
- Entropy
- Physically unclonable functions

# Outline

Introduction

Conclusion

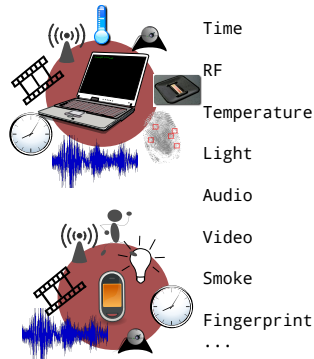


# Sensors and sensor classes

- We are surrounded by a multitude of sensors

- Sensor readings utilised for

- Information provisioning
- Situation classification
- Authentication
- Cryptography

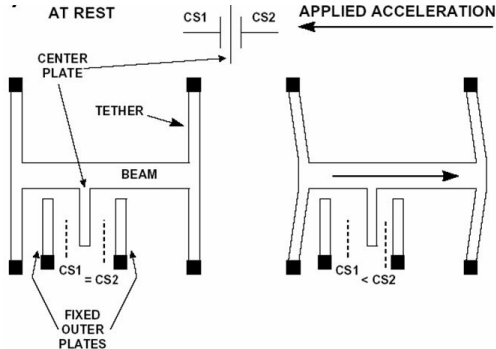


# Sensors and sensor classes



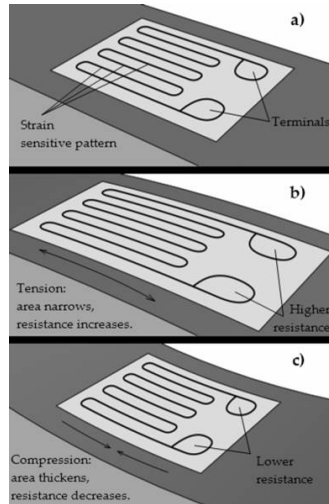
# Sensors and sensor classes

- MEMS acceleration sensors
  - E.g. Analogue Devices ADXL
  - Low energy consumption, small, cheap, medium precision
  - MEMS = Micro-mechanical System: Mechanic in Silicon (Silizium)
  - Here: Comparison of capacity  $CS1$  and  $CS2$  leads to acceleration



# Sensors and sensor classes

- Pressure sensors
  - Z.B. IEE about 3-10 Euro
  - Very imprecise



# Sensors and sensor classes

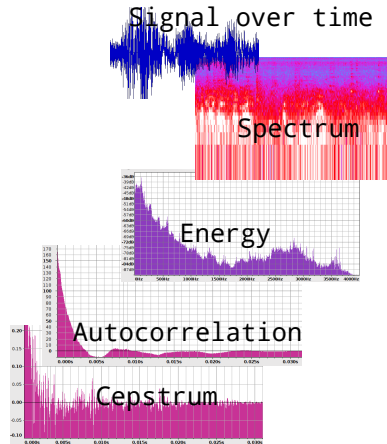
- Output of sensors has to be interpreted typically
  - Raw electrical signals
  - Interpretation of signals as electric values
  - Binary or Real valued representation
  - Further identification of features
  - Feature extraction
  - Interpretation of features and classification





# Features and feature extraction

- What is a feature and why do we need it?
  - Captured data might be hard to interpret
  - Many aspects can be contained in a single data stream
  - Example: Audio
    - Loudness
    - Energy on frequency bands
    - Zero crossings
    - Direction changes



# Examples and case studies: Media Cup

- Media Cup: Context recognition
  - Activity: Trigger sleep mode (save energy)
  - Level of activity
  - Own context: Object movement, person is nervous, specific handling of objects
  - Environmental context: Vibration, earthquake
- Sensor: Ballswitch
  - (nearly) no quiescent current
  - Various types, filled with gas/liquid
  - e.g. Acceleration with fixed value (liquid)
  - Vibration (filled with gas)



- Context Watcher

- 
- ```

graph TD
    subgraph Sensors
        GPS[GPS]
        Network[Network]
        Body[Body]
        Activity[Activity]
    end
    GPS --> CW[Context Watcher]
    Network --> CW
    Body --> CW
    Activity --> CW
    CW --- GPRS[GPRS/UMTS]
    CW --> CP[Clustering engine]
    CW --> PP[Photo Provider]
    CP --> LP[Location Provider]
    CP --> AP[Agenda Provider]
    PP --> LP
    LP --> F[Flickr]
    LP --> GE[Google Earth]
    LP --> B[Blog]
    LP --> C[Calendar]
    LP --> CW
    AP --> CW
    AP --> WP[Wellness Provider]
    AP --> PrP[Preference Provider]
    AP --> WPr[Weather Provider]
    AP --> TP[Transport Provider]
    AP --> PR[Presence Provider]
    
```

# Examples and case studies: Context Watcher



| Picture                                                                           | Context Data                                                                                                                                                          |
|-----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | cell id: 10571<br>altitude: 59.4<br>speed: 115.1 km/h<br>course: 246.6<br>pos: (52.279,6.503)<br>range: 1 m<br>street: E30<br>postal code: 7462<br>city: Rijssen (NL) |

## Johan's blog

📅 Saturday, March 24, 2007

### A day in Papendrecht

The weather that I enjoyed today: it has been rather cloudy in Alblasterdam, 1/9°C, with a relative humidity of 93%, a gentle breeze was blowing from north to northeast. The cities that I visited today: Papendrecht (7.4h), Dordrecht (1.6h), Alblasterdam (4.5h). The max of speed that I had today: 104.9. The photos that I took today:




# Examples and case studies: TEA

## TEA-Audio

- Requirements
  - Restricted memory space
  - Computing power restricted
- Benefit
  - Many sensors → Many features
- Example approach
  - Utilise time domain (no transformation)
  - Utilise statistic measures
  - Feature extraction based on small amount of data

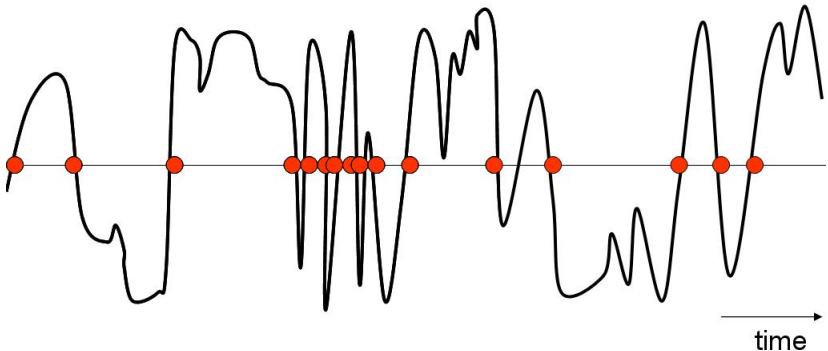
# Examples and case studies: TEA

- Audio data in time domain



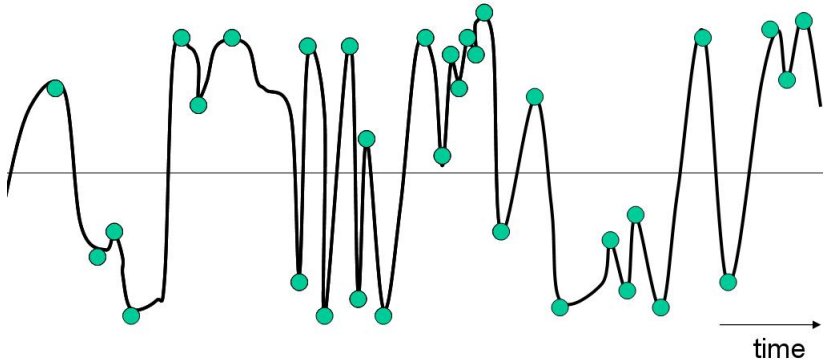
# Examples and case studies: TEA

- Count zero crossings
- Distance between zero crossings



# Examples and case studies: TEA

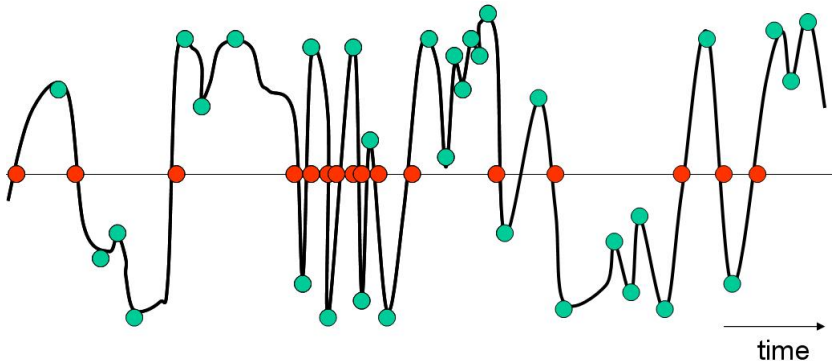
- Count of direction changes





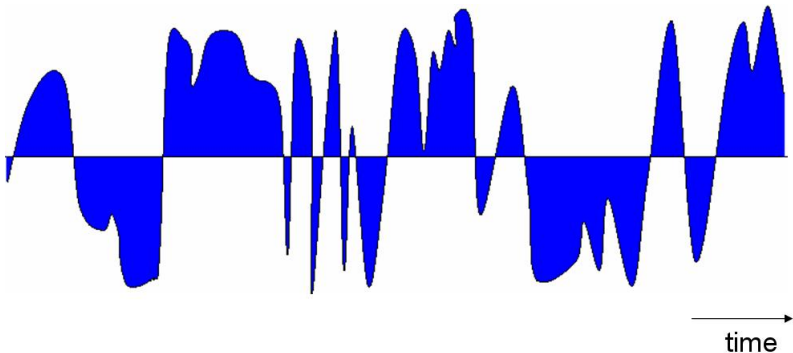
# Examples and case studies: TEA

• ratio:  $\frac{\text{direction changes}}{\text{zero crossings}}$



# Examples and case studies: TEA

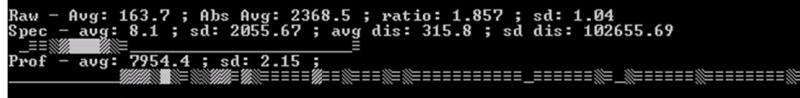
- Integral



# Examples and case studies: TEA

- Several chunks for speech

whistling



Whistling

speech



1

2

3

4

# Examples and case studies: TEA

- Distance between zero crossings: distinct behaviour of oscillation at start and end

whistling



speech



# Examples and case studies: TEA

- Distinct ratio:  $\frac{\text{zero crossings}}{\text{direction changes}}$


whistling

```
Raw - Avg: 163.7 ; Abs Avg: 2368.5 ; ratio: 1.857 ; sd: 1.04
Spec - avg: 8.1 ; sd: 2055.67 ; avg dis: 315.9 ; sd dis: 102655.69
Prof - avg: 7954.4 ; sd: 2.15 ;
```



speech

```
Raw - Avg: 170.5 ; Abs Avg: 471.0 ; ratio: 12.190 ; sd: 566179.8
Spec - avg: 12.5 ; sd: 4447.67 ; avg dis: 115.4 ; sd dis: 13669.85
Prof - avg: 1411.2 ; sd: 1673821.1 ;
```



# Examples and case studies: TEA

- Significant change in standard deviation of chunks

whistling

```
Raw - Avg: 163.7 ; Abs Avg: 2368.5 ; ratio: 1.857 ; sd: 1.04  
Spec - avg: 8.1 ; sd: 2058.18 ; avg dis: 315.8 ; sd dis: 102655.69  
Prof - avg: 7954.4 ; sd: 2.15 ;
```

speech

```
Raw - Avg: 170.5 ; Abs Avg: 471.0 ; ratio: 12.190 ; sd: 566179.8  
Spec - avg: 12.5 ; sd: 4440.50 ; avg dis: 115.4 ; sd dis: 13669.85  
Prof - avg: 1411.2 ; sd: 1673821.1 ;
```

# Outline

Introduction

Conclusion



# Questions?

Stephan Sigg  
`sigg@ibr.cs.tu-bs.de`



# Literature

- C.M. Bishop: Pattern recognition and machine learning, Springer, 2007.
- P. Tuly, B. Skoric, T. Kevenaar: Security with Noisy Data – On private biometrics, secure key storage and anti-counterfeiting, Springer, 2007.
- R.O. Duda, P.E. Hart, D.G. Stork: Pattern Classification, Wiley, 2001.

