Data Storage in Gentelligent Components – A New Way for Self-Authentication

Ralf Dragon [1], Jörn Ostermann [1],
Berend Denkena [2], Bernd Breidenstein [2], Tobias Mörke [2]

[1] Institut für Informationsverarbeitung (TNT)
[2] Insitut für Fertigungstechnik und Werkzeugmaschinen (IfW)
Leibniz Universität Hannover

2010-09-24

This work was funded as part of the Sonderforschungsbereich 653 by the DFG.

What is Authentication?

- Verifying genuineness, origin vs. forgery
- Means
  - Historically: Stamps and seals on deeds
  - Handwriting: Signature
  - Forensics: *Fingerprint*

Impression of cylinder seal, Mesopotamia, Uruk Period (4100 BC–3000 BC)

Fingerprints, taken since 19th century

What is Authentication?

- Verifying genuineness, origin vs. forgery
- Means
  - Historically: Stamps and seals on deeds
  - Handwriting: Signature
  - Forensics: *Fingerprint*
- Analog Authentication
  - Differences exist
  - Significance to original is detectable

Impression of cylinder seal, Mesopotamia, Uruk Period (4100 BC–3000 BC)

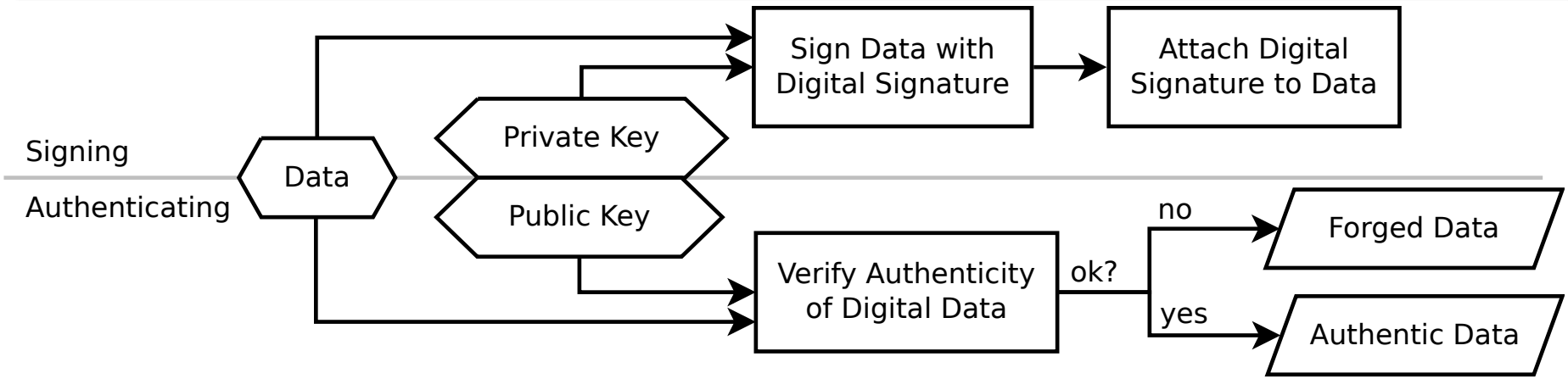
Fingerprints, taken since 19th century

Digital Authentication

- Digital data can be copied exact $\Rightarrow$ Fingerprints could be transfered to forgeries
- Digital signature was introduced (symmetric keys, e.g. AES 256)

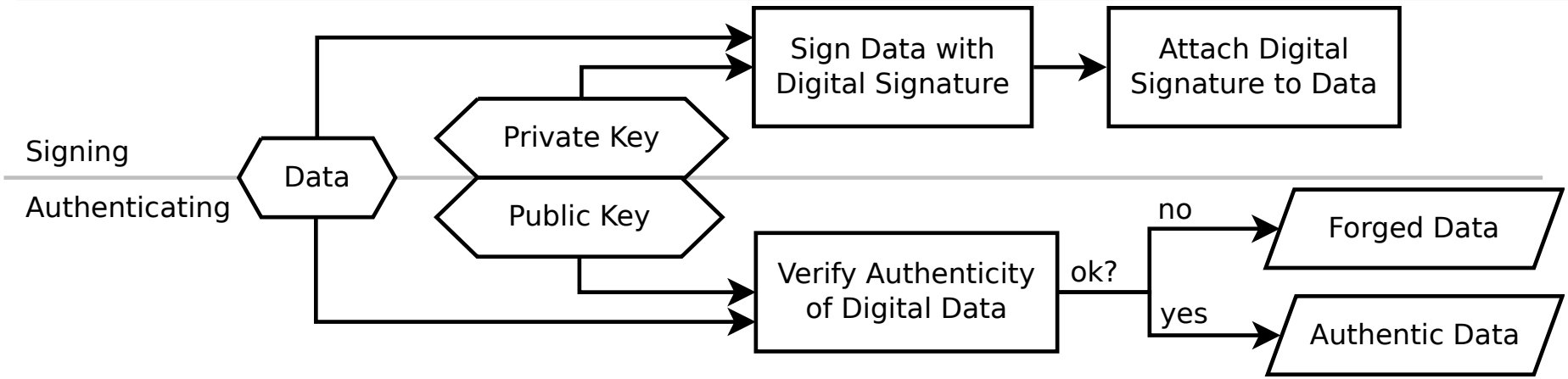
Digital Authentication

- Digital data can be copied exact ⇒ Fingerprints could be transfered to forgeries
- Digital signature was introduced (symmetric keys, e.g. AES 256)



Digital Authentication

- Digital data can be copied exact ⇒ Fingerprints could be transfered to forgeries
- Digital signature was introduced (symmetric keys, e.g. AES 256)

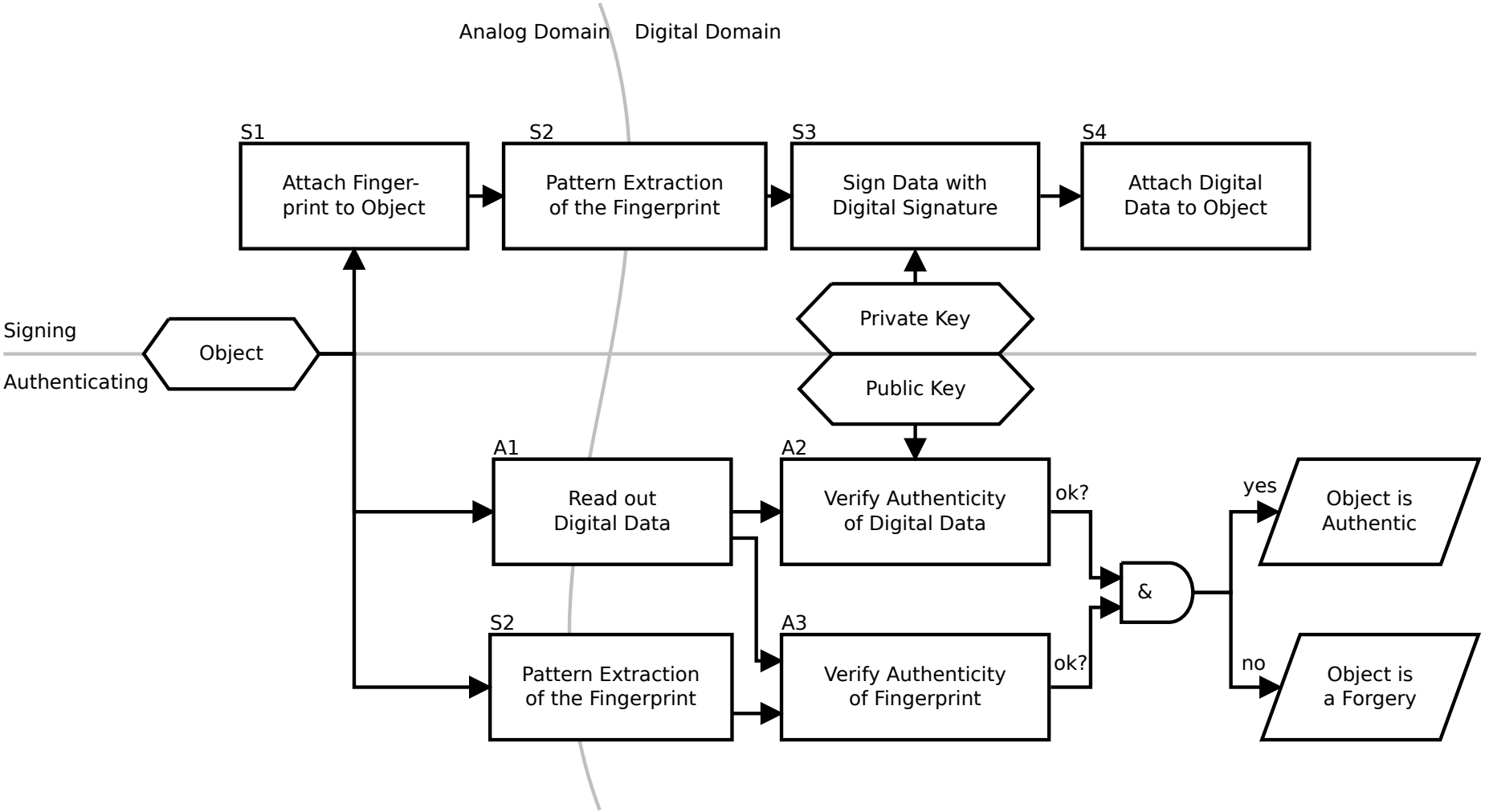


- Specific to data getting signed
- Specific to authenticating entity

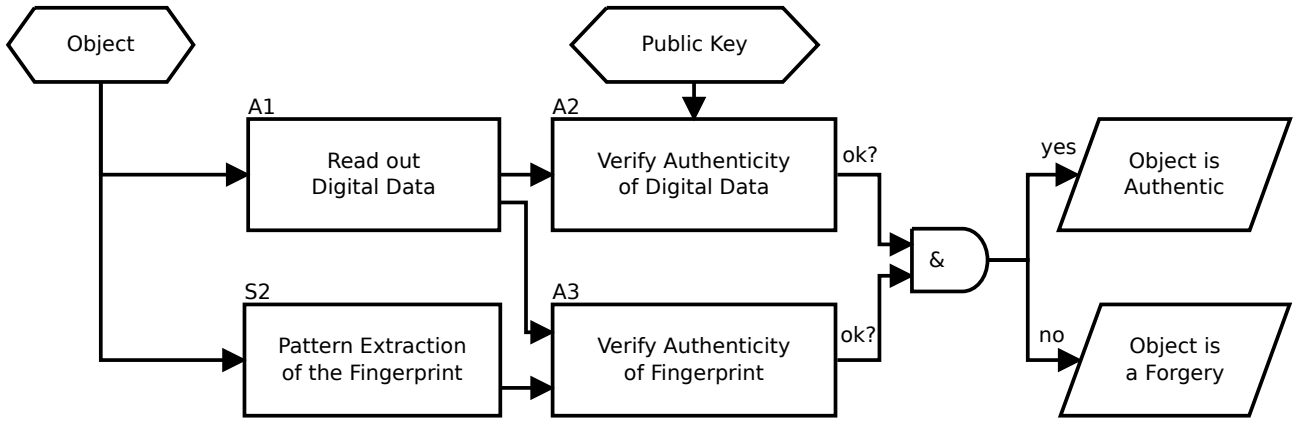
Digital Authentication for Objects

- Digital signature is cryptographically proved to be very strong
- Digital data is not related to real world
- Idea: Sign data describing specific component properties
  - None? Insert a random pattern!
  - Where to store data? Inherent!
- Every object/component may have a different pattern for verification

Self-Authentication



Why is this self-authentication?



Prior Information

- Public key of signer needed
- Public key can also be stored in digital data structure
  - Signed by root public key

  $\Rightarrow$ Only prior knowledge needed: Public root certificate

Signature For Documents

Object to be authenticated

Analog label: Image features of document itself

No hand-written signature needed

Digital label where digital information about the fingerprint is stored

Individual Bank Notes

Object to be authenticated

Analog label where a fingerprint is situated

Digital label where digital information about the fingerprint is stored

Individual Bank Notes

Object to be authenticated

Analog label where a fingerprint is situated

Digital label where digital information about the fingerprint is stored

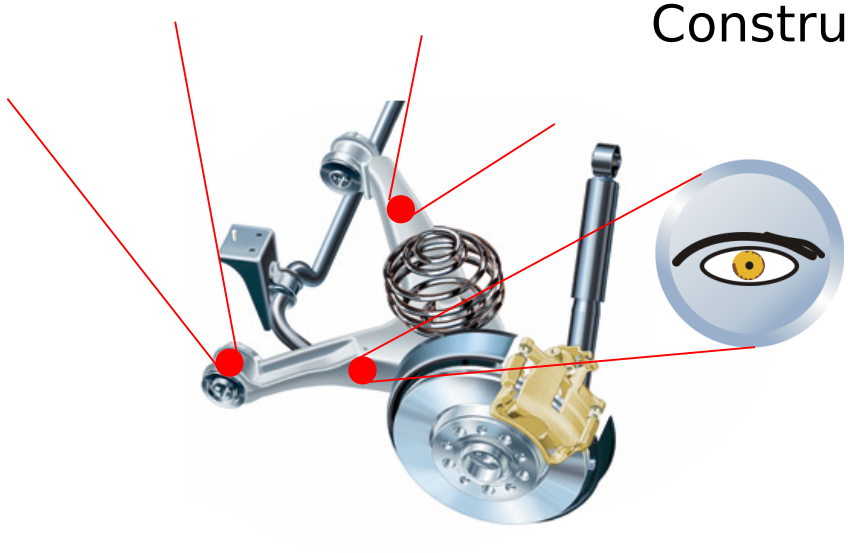
- Individual watermarks possible
- (Money is as virtual as information)

Why Inherent?

- Fingerprint
  - Must be fixed to component
  - Not inherent
    - Can get lost
    - Can be mixed up
- Data
  - Centralized from database
    - Accessability
    - Abuse to create forgeries
  - Not inherent
    - Can get lost
    - Can be mixed up

Gentelligent Components

Initial State of Component

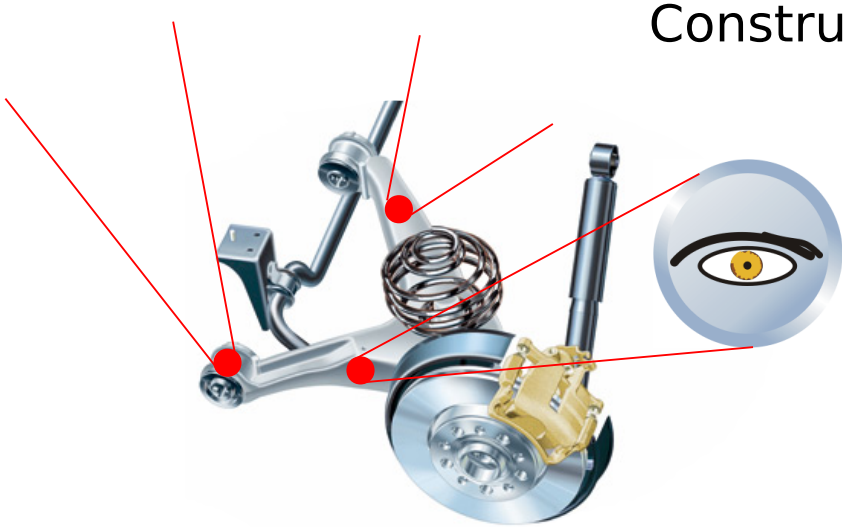


Construction Plans

Current State of Component

Gentelligent Components

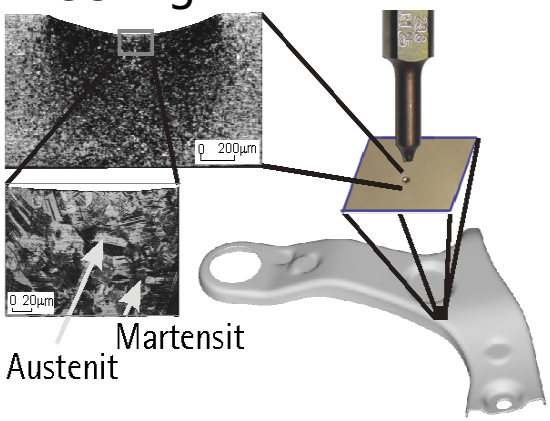
Initial State of Component



Construction Plans

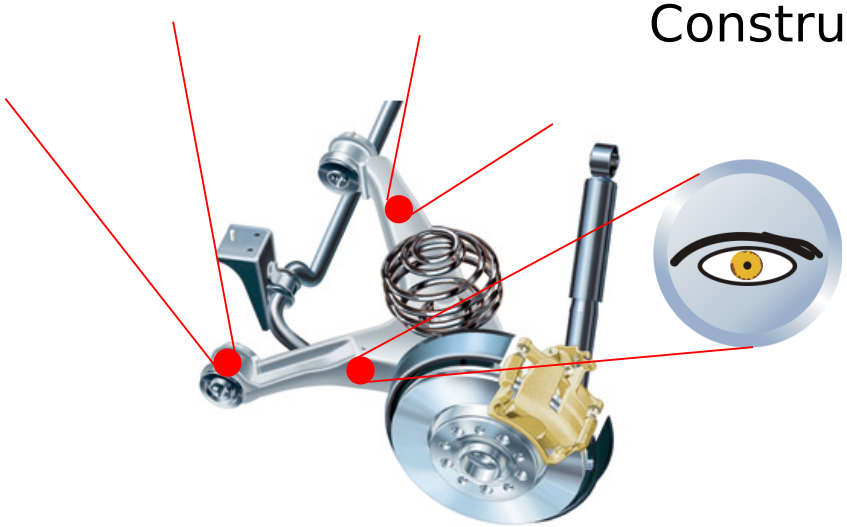
Current State of Component

"Feeling"



Gentelligent Components

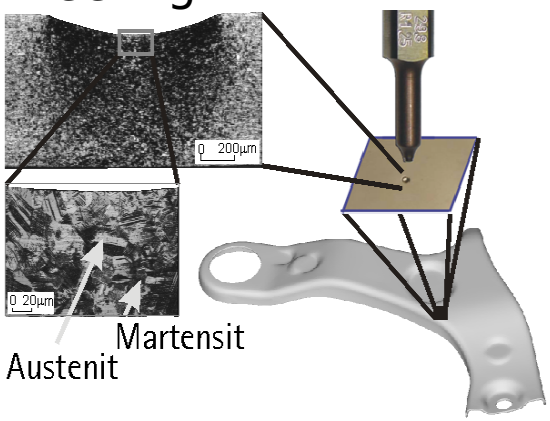
Initial State of Component



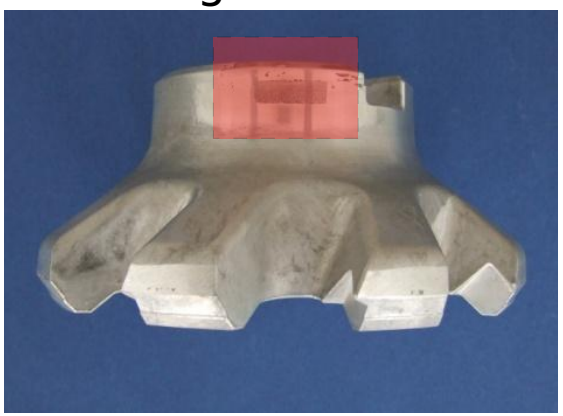
Construction Plans

Current State of Component

"Feeling"

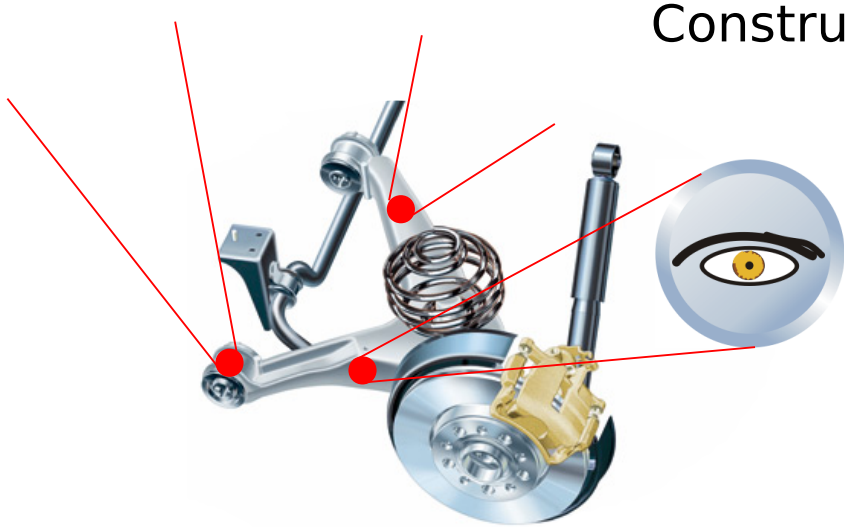


"Knowing"



Gentelligent Components

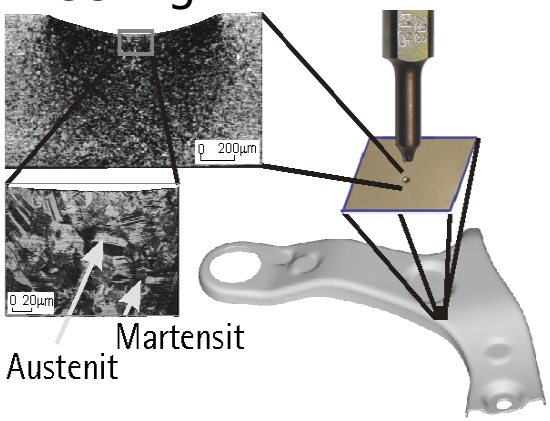
Initial State of Component



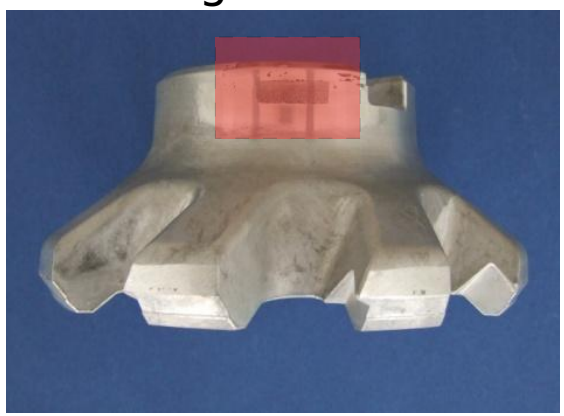
Construction Plans

Current State of Component

"Feeling"



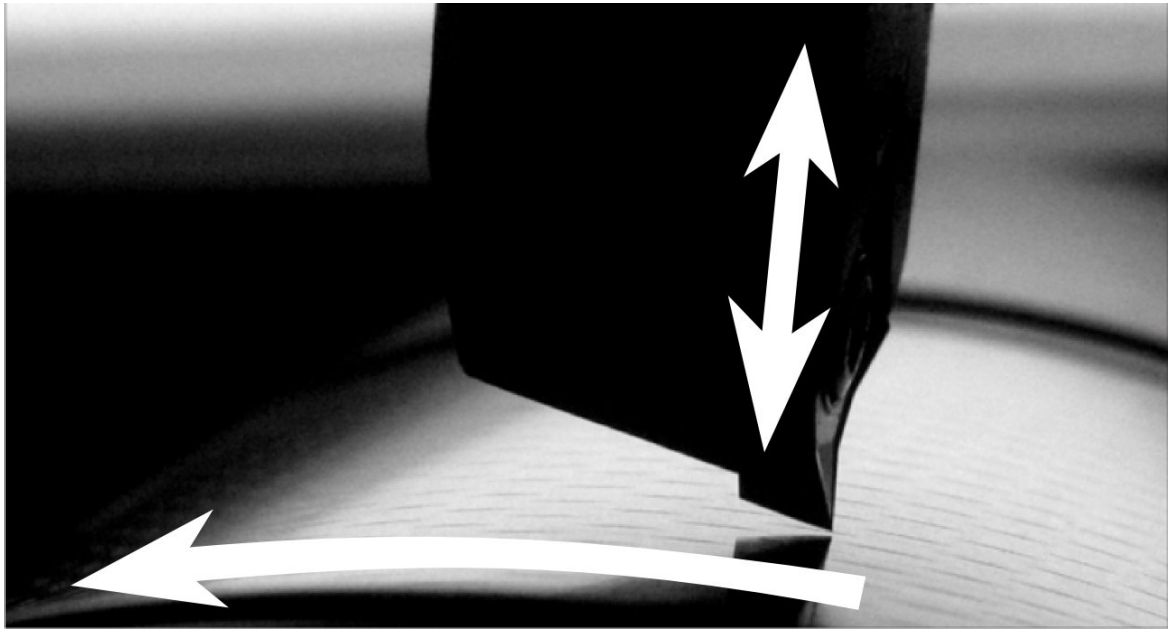
"Knowing"

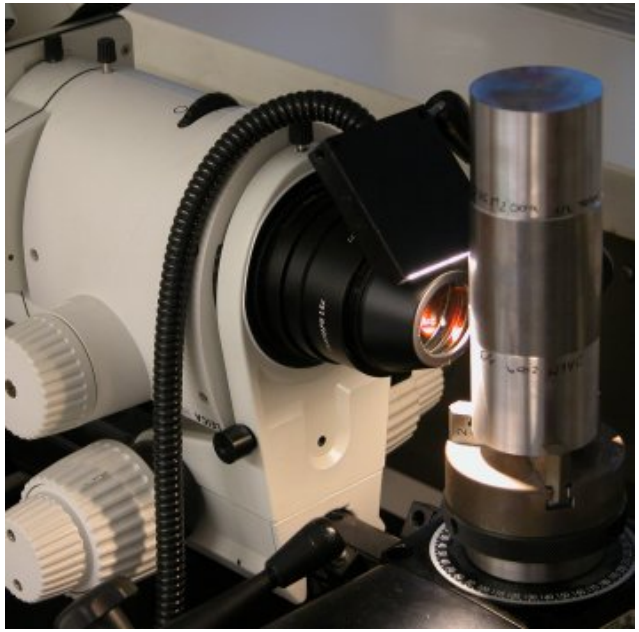


Using the knowledge

Genetics & Intelligence
⇒ Gentelligence

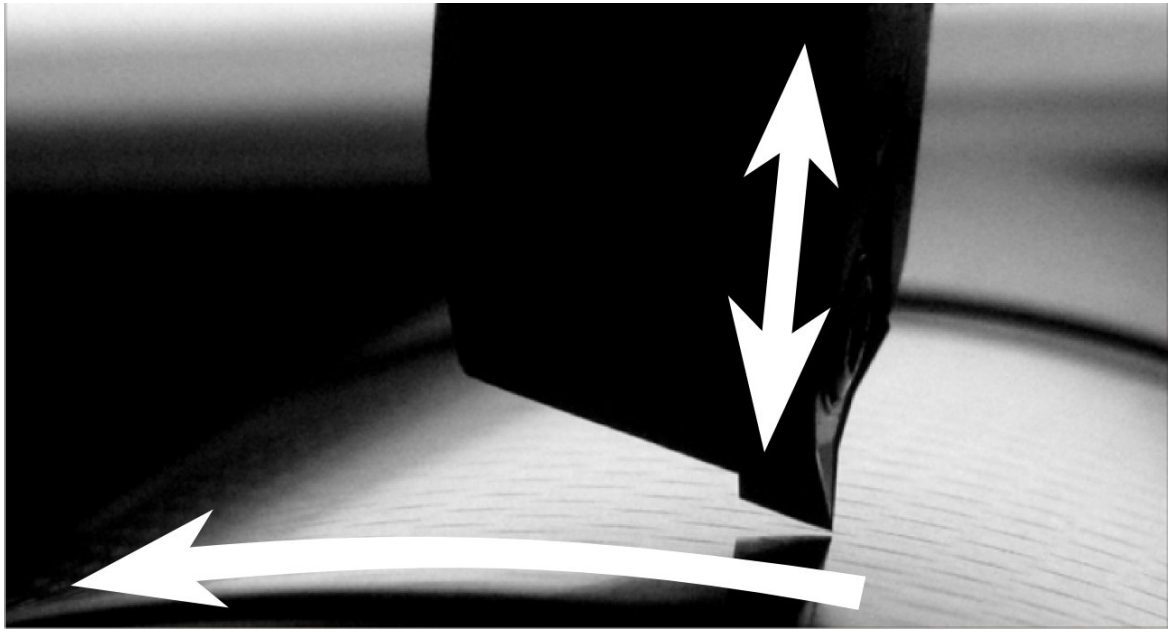
Inherent Data on Gentelligent Components

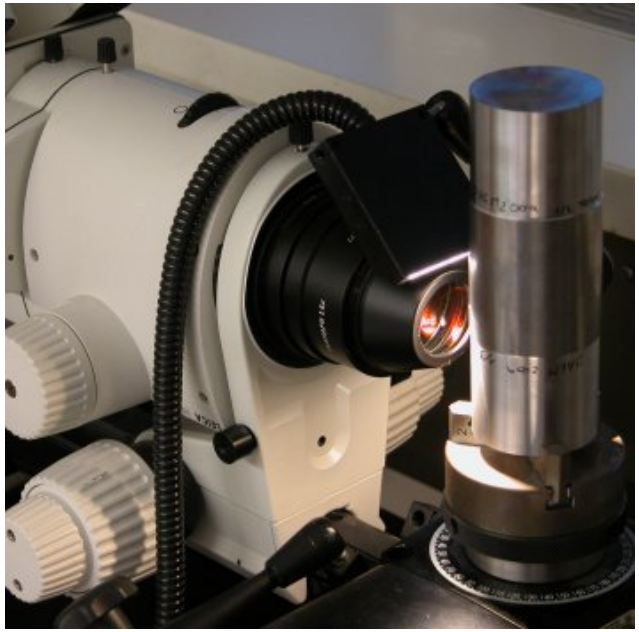




- Micro-structured surface for data storage
- Groove wound around component
- Cut in by Piezo tool during a turning process
- Depth is varied

Inherent Data on Gentelligent Components

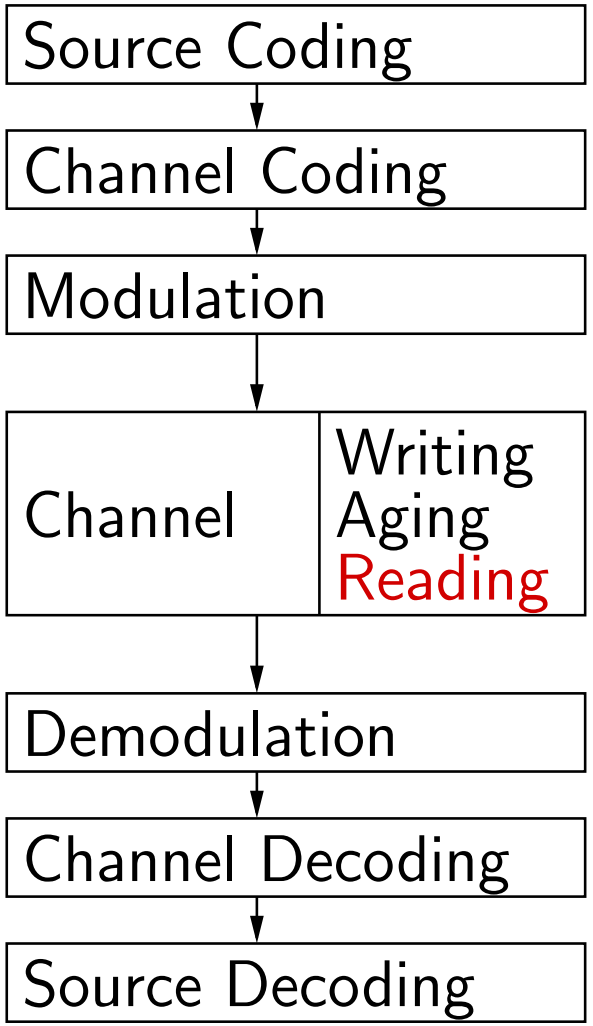




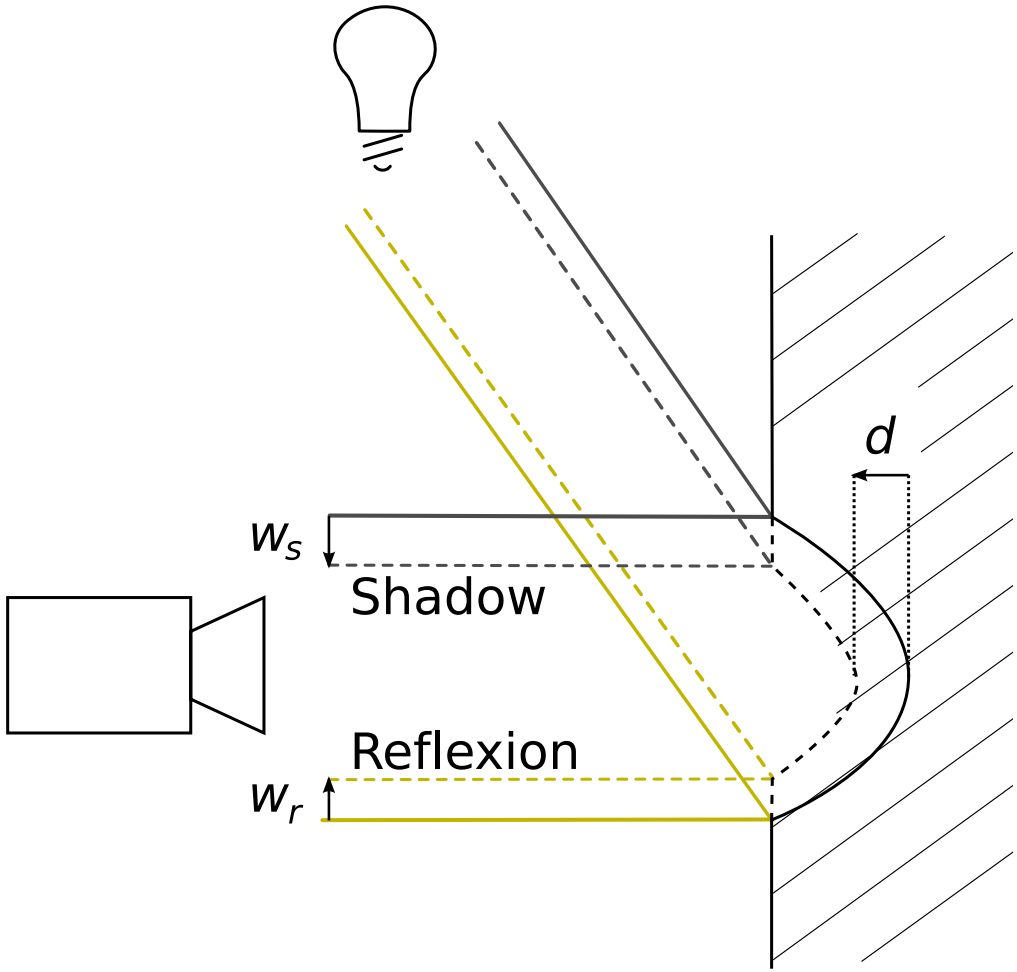
- Micro-structured surface for data storage
- Groove wound around component
- Cut in by Piezo tool during a turning process
- Depth is varied
- No digital structures can be created

Transmission principle

- Groove is imprint of the analog signal run of the Piezo tool
- Recovering the run means reconstructing the analog signal
- Data transmission system
- Depth reconstruction with optical means
- Re-use existing methods
- Only qualitative (no exact scaling) reconstruction needed

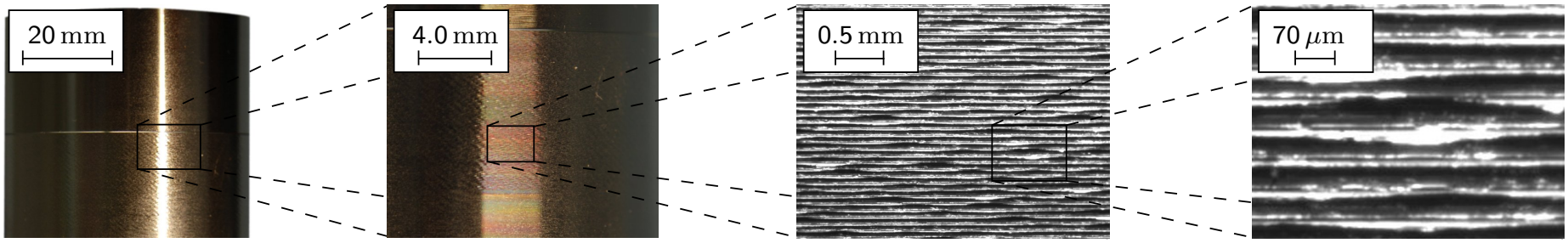


Depth from Directed Illumination

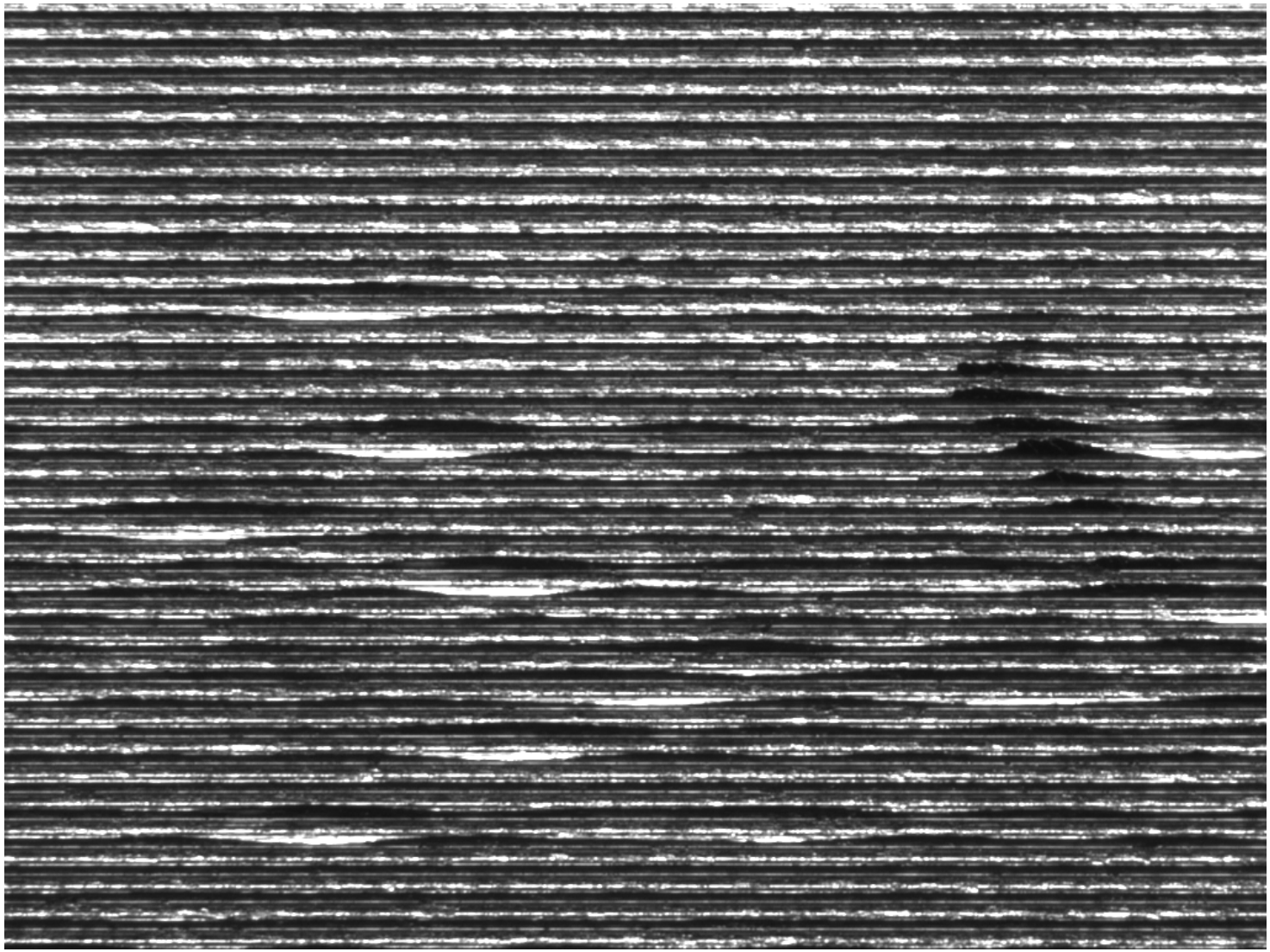


- Parallel illumination
- Groove consists of shadow and reflexion region
- Variation of groove depth by d shifts
  - shadow border by w_s
  - reflexion border by w_r
- We focus on reflexion
  - Geometry does not allow shadows and reflextions
  - Less image perturbation
- Edge tracking solves depth reconstruction qualitatively

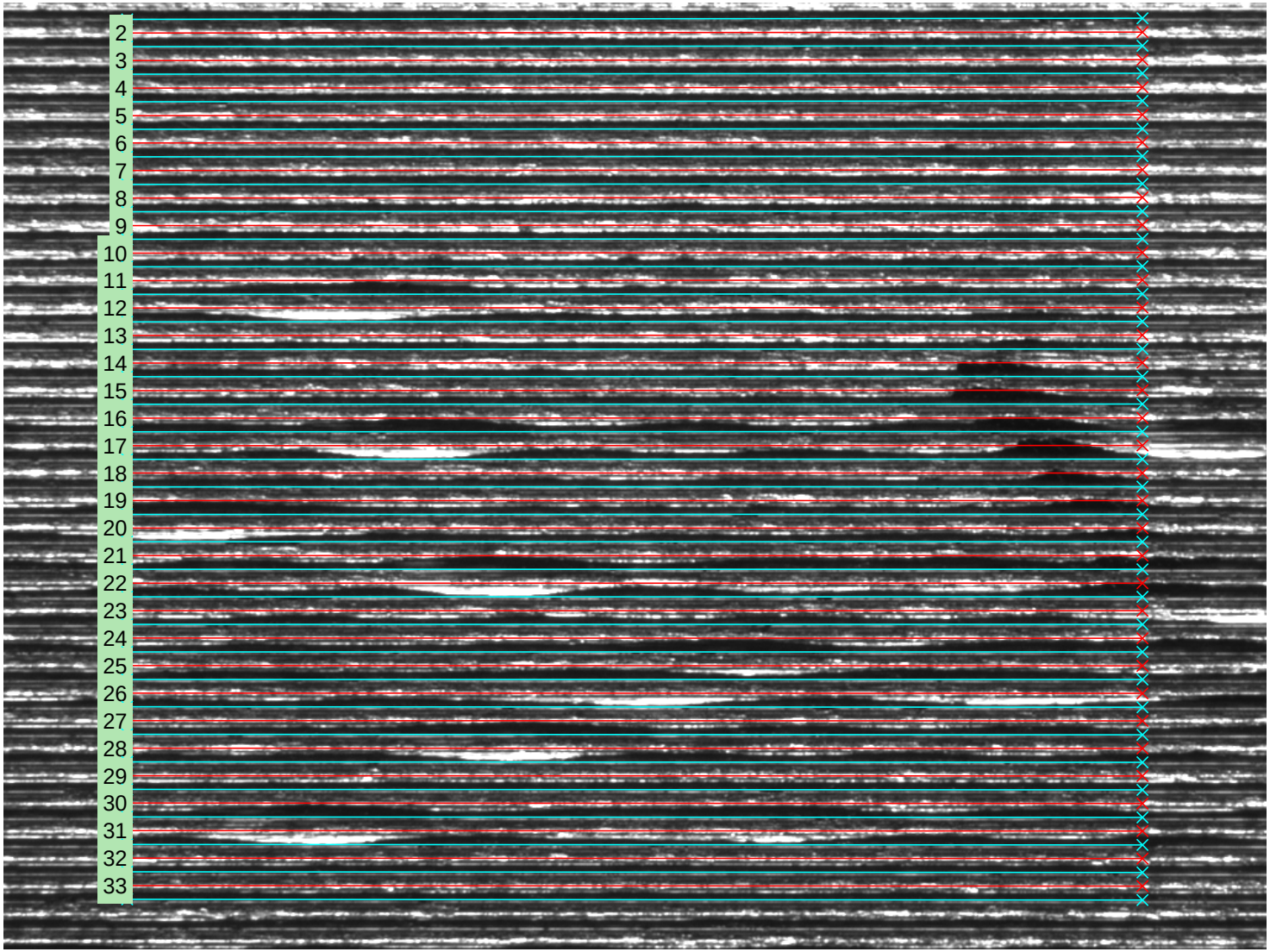
Surface under Directed Illumination



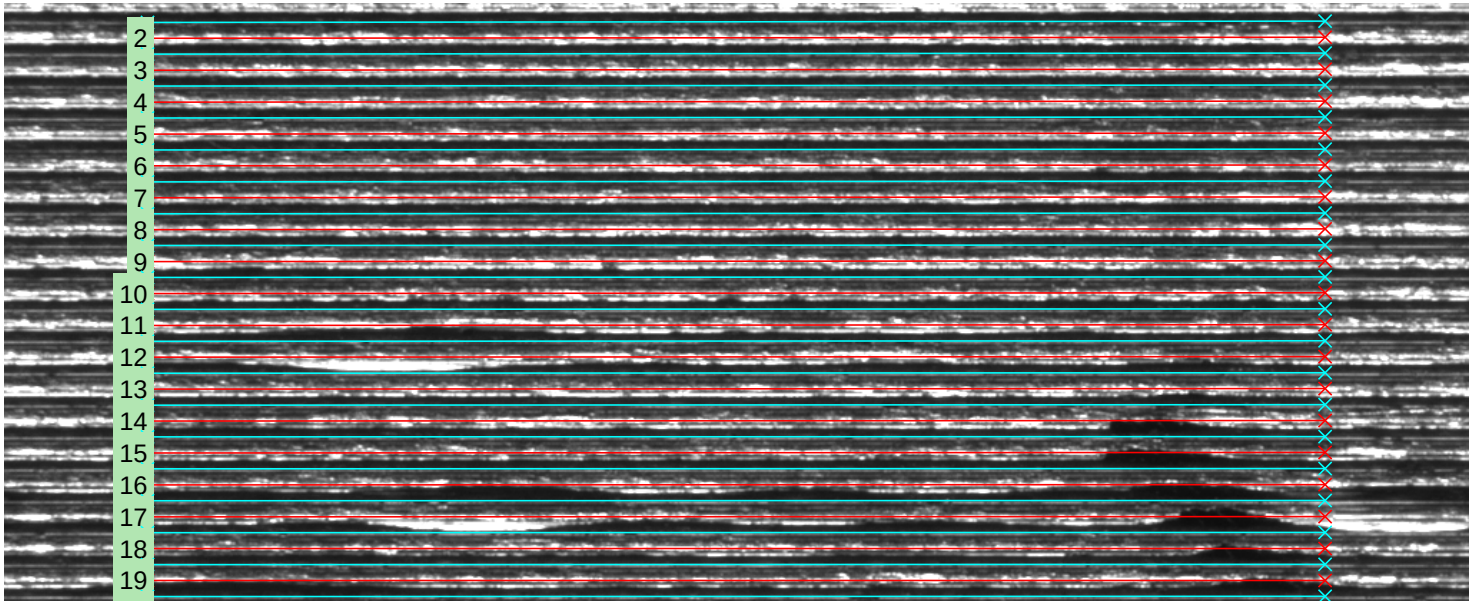
Inherent Data on Gentelligent Components



Inherent Data on Gentelligent Components



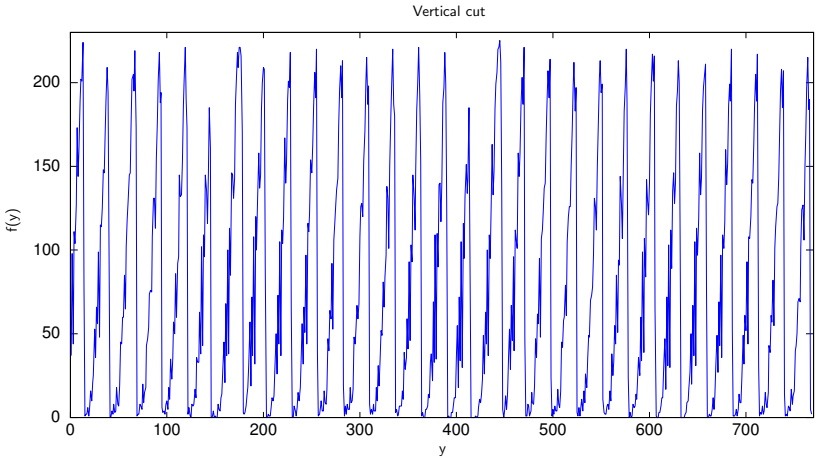
Inherent Data on Gentelligent Components



- Assumption: Groove runs approximately horizontal
- Perform several spectral analyses of the image $I(x, y)$ at column $x = x_i$ in vertical direction
- Filtering: Horizontal moving average (noise), vertical median (cutting artifacts)
- Vertical cut forms the 1D signal $f(y)$ which is analyzed

Inherent Data on Gentelligent Components

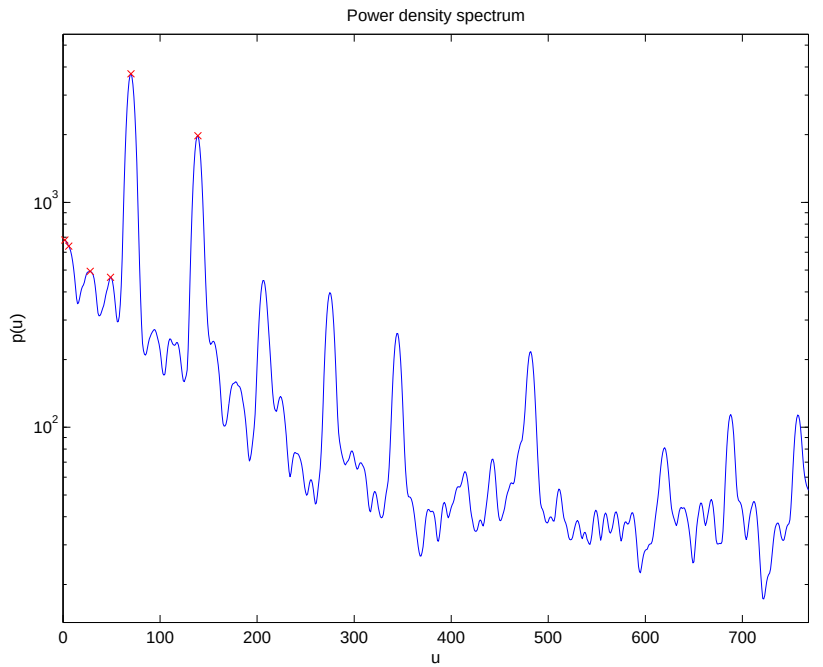
- Periodic reflexion area: $y = (n + \frac{1}{2})\lambda_0 + \phi_0$
- Distance λ_0 or frequency u_0
- Phase shift $\phi(u_0)$



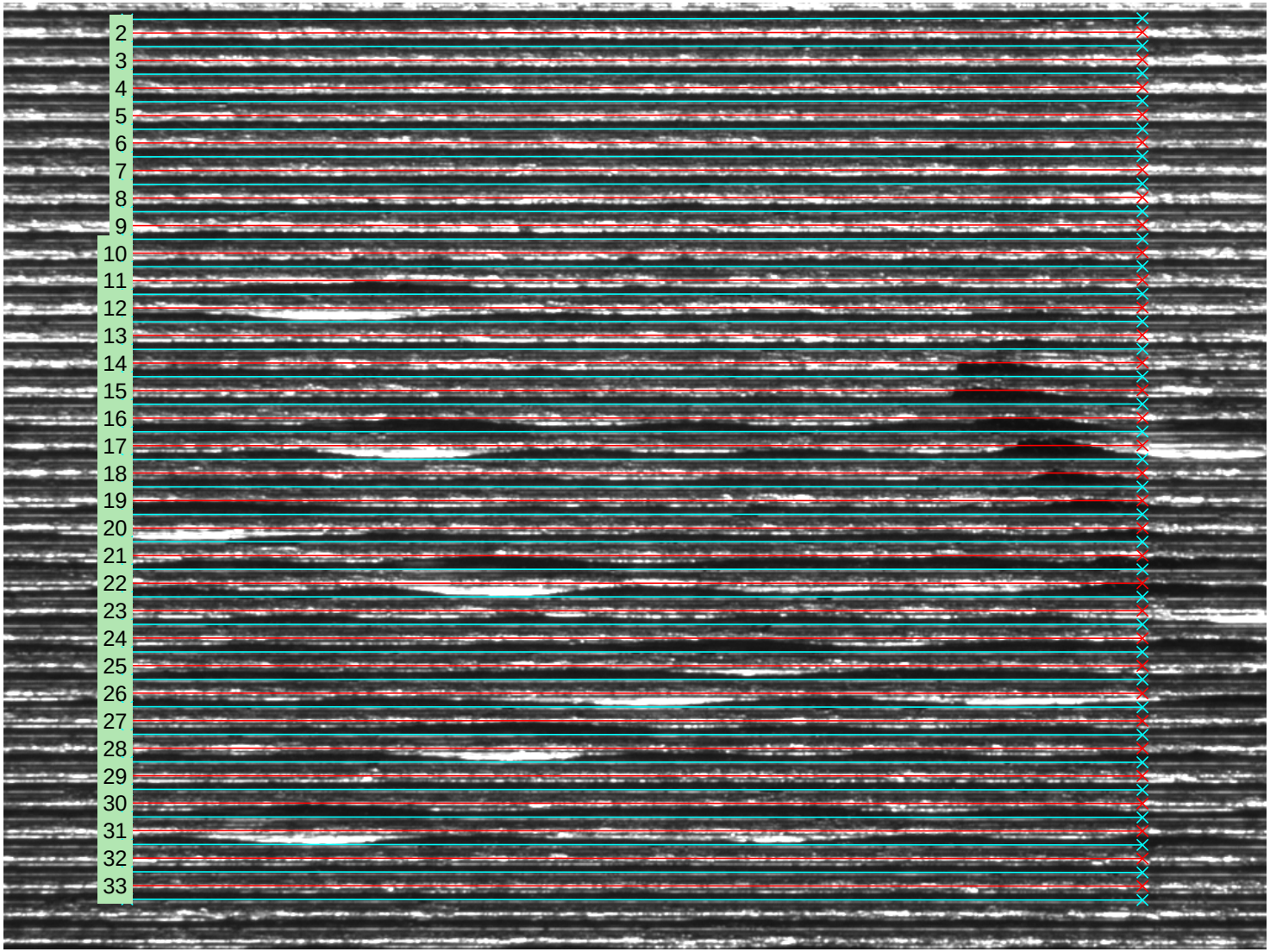
Spectral Estimation

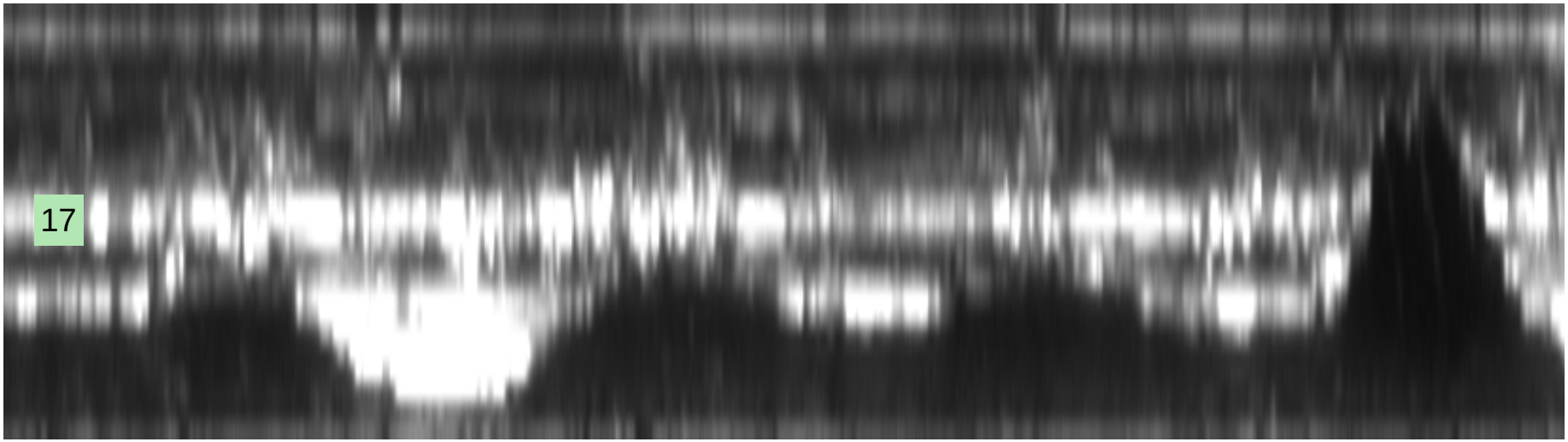
- $p(u) = {}^1/_R \sum_r |F_r(u)|$
- No phase information as $\phi(u)$ is not shift-invariant
- Phase estimation extention of average periodogram method[a]

[a] Dragon et. al., DAGM 2009



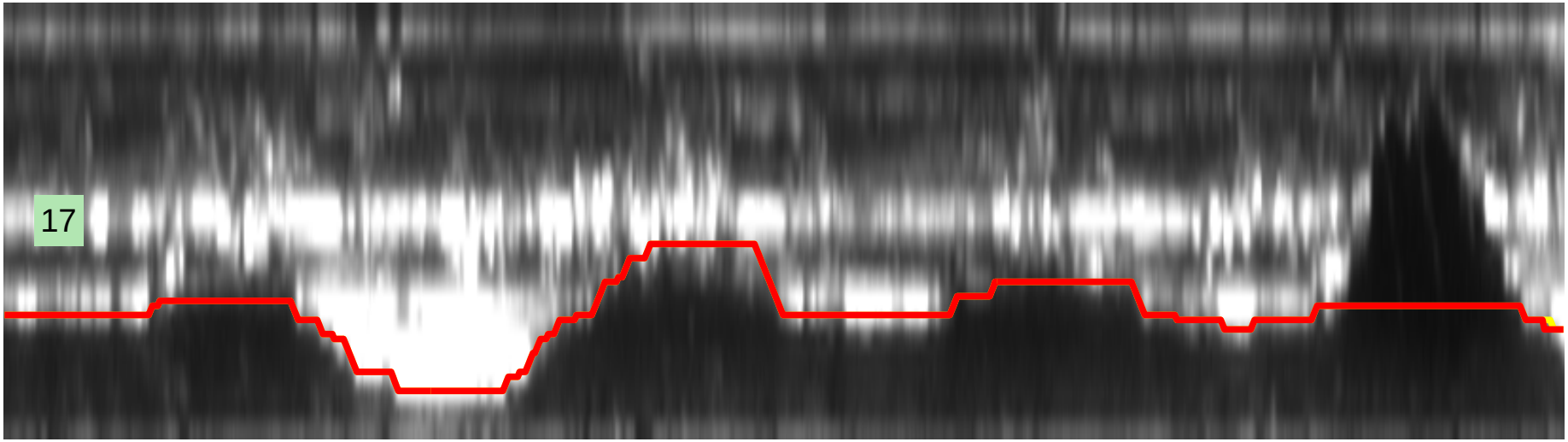
Inherent Data on Gentelligent Components





Extraction of the Groove Edge

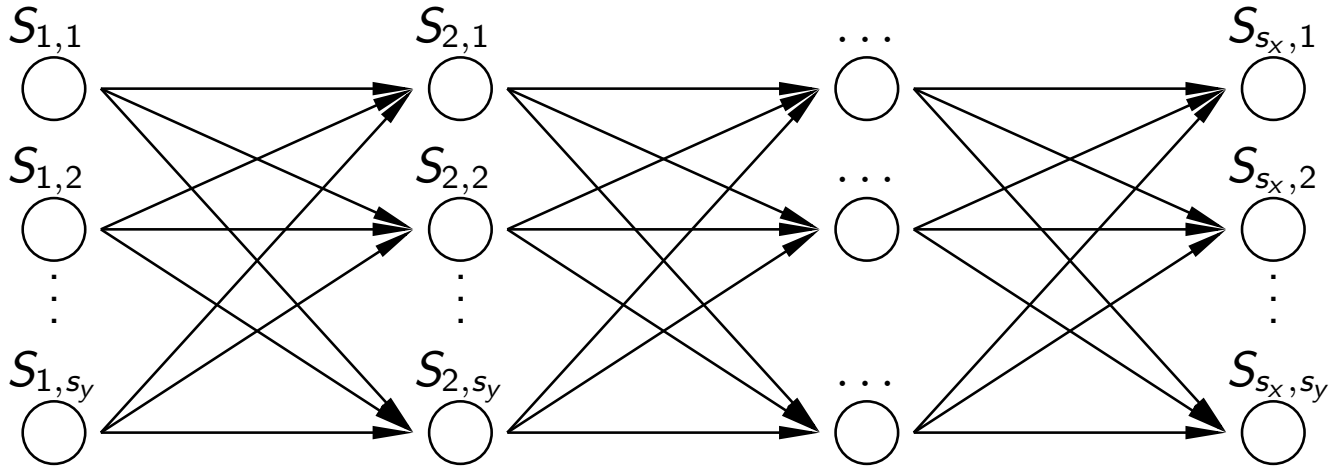
- Model appearance of the groove edge
- Model movement of the Piezo tool
- Robust to perturbations



Extraction of the Groove Edge

- Model appearance of the groove edge
- Model movement of the Piezo tool
- Robust to perturbations

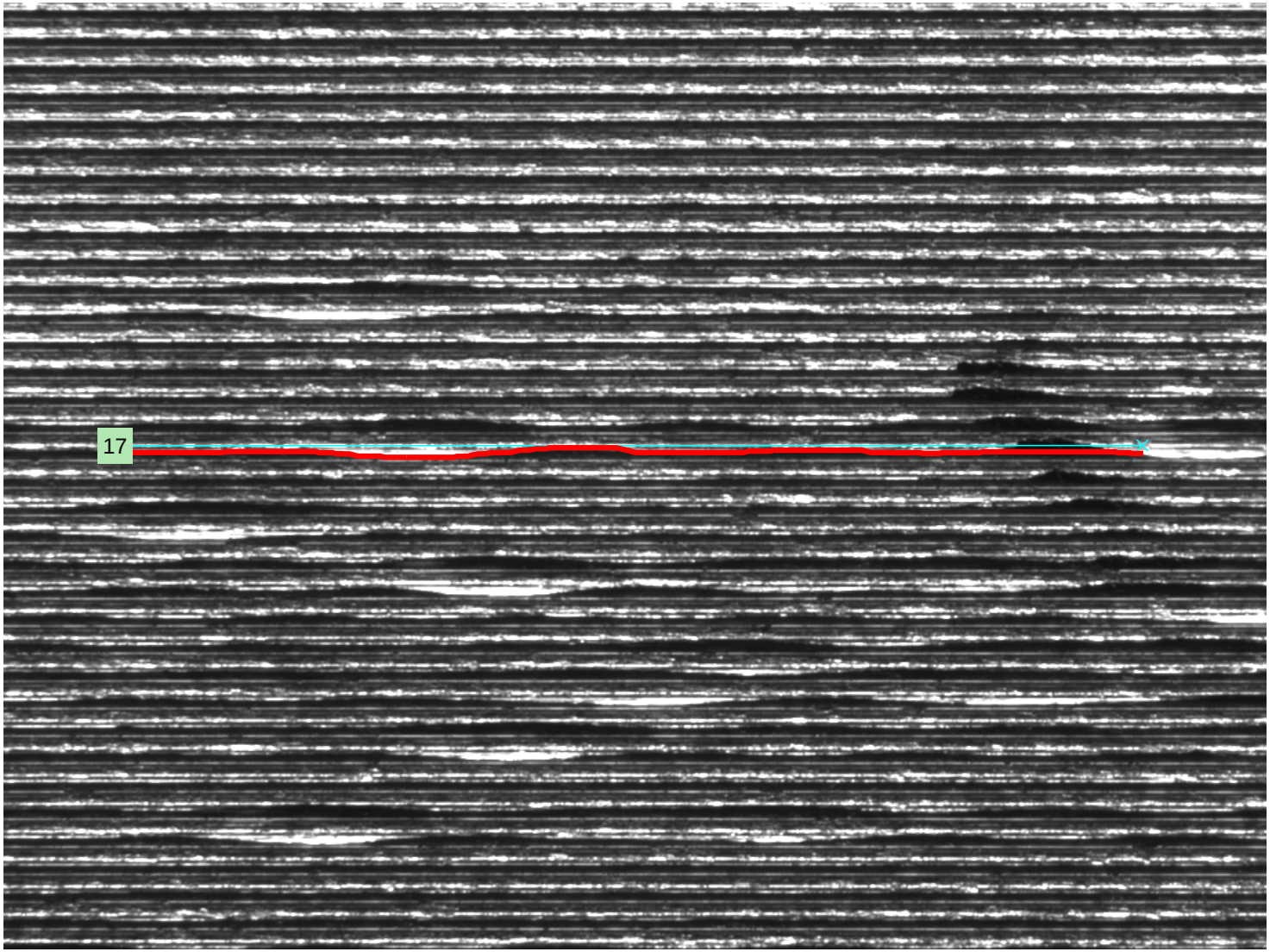
Inherent Data on Gentelligent Components



Adapted HMM Model

- Each node $S_{x,y}$ models one image pixel $I(x, y)$
- Observation probability: $p_o(x_i, y_i|I) \propto c - \frac{I(x_i,y_i+1)-I(x_i,y_i-1)}{2}$
- Transition probability: $p_t(x_{i+1}, y_{i+1}|y_i) \propto \mathcal{N}(\sigma^2, y_i)$
- Groove edge $Y = (y1, y2, \ldots, y_{s_x})$ is found with Viterbi algorithm finding maximum of $P = p_o(x_{s_x}, y_{s_x}) \prod_{i=1}^{s_x-1} p_t(x_{i+1}, y_{i+1}|y_i) p_o(x_i, y_i)$

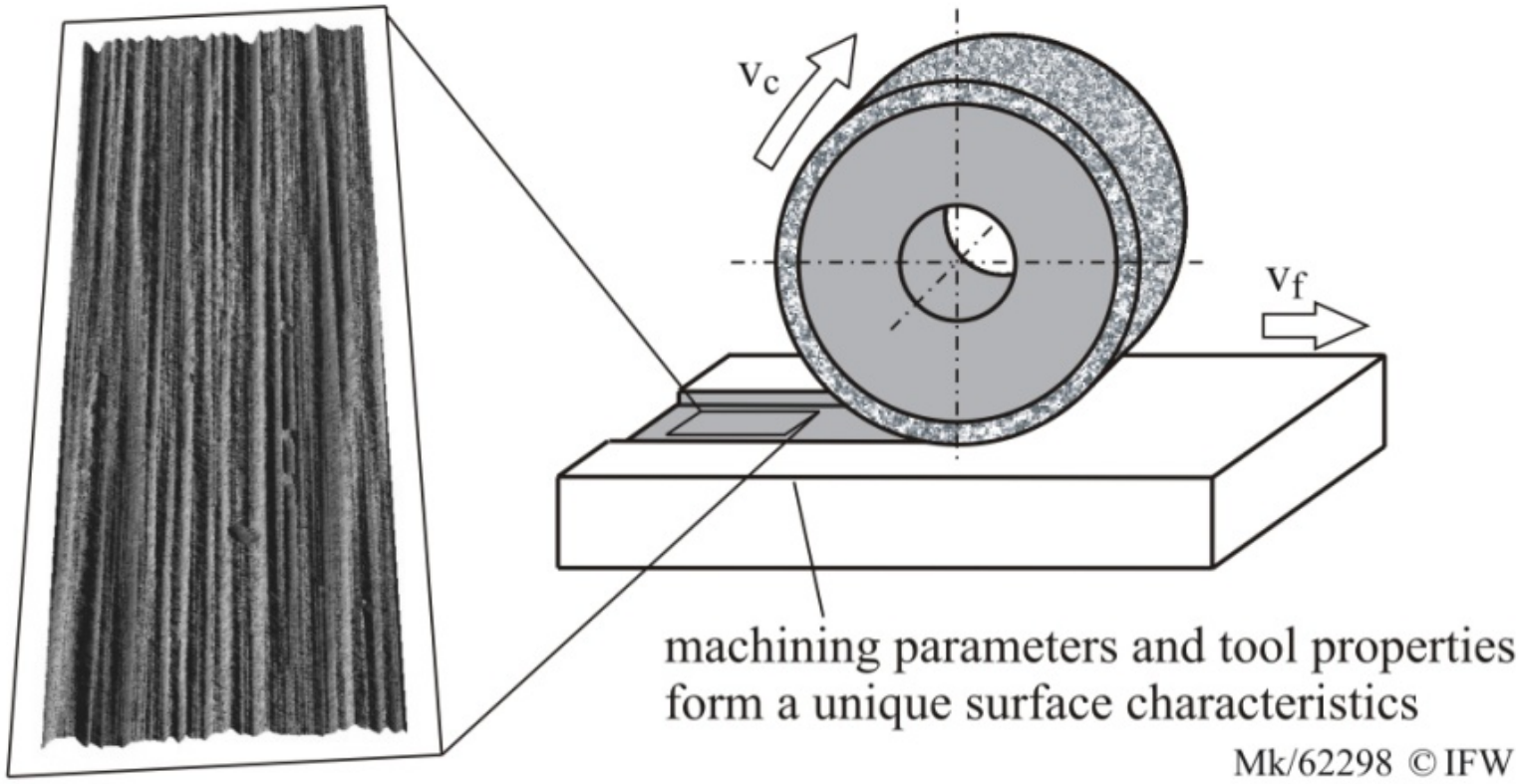
Inherent Data on Gentelligent Components



Fingerprint

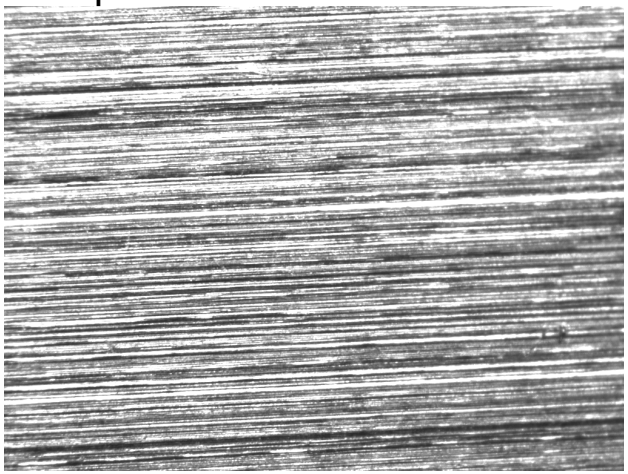
- Imprint of grinding process
- Pseudo-random

- Sample intensity profiles using directed illumination
- Compare using NCC

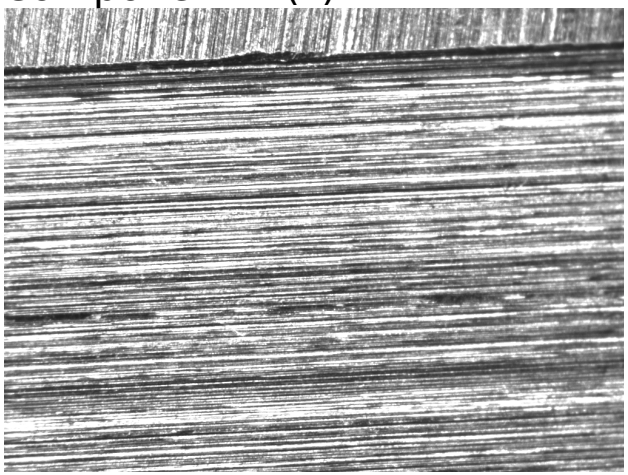


NCC of Depth Profile

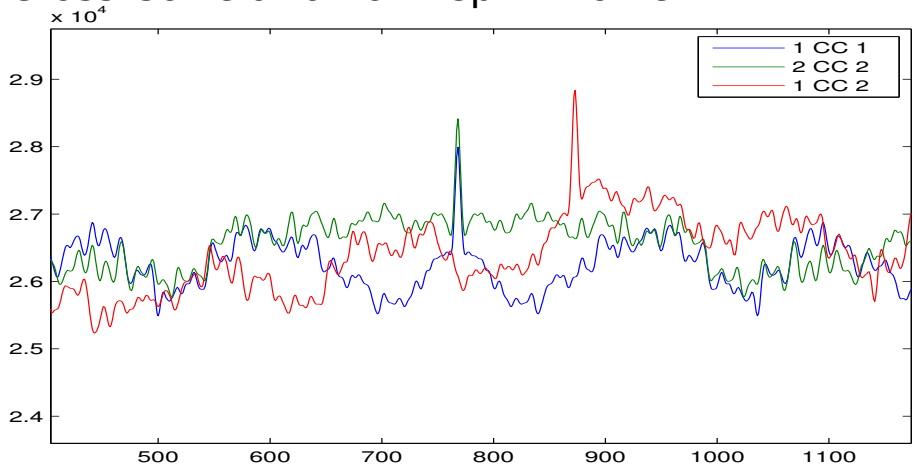
Component 1



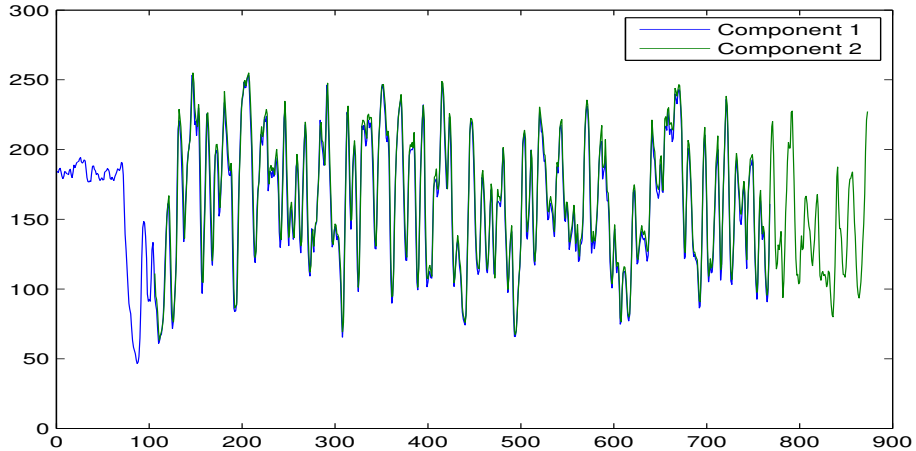
Component 2 (?)



Cross Correlation of Depth Profile



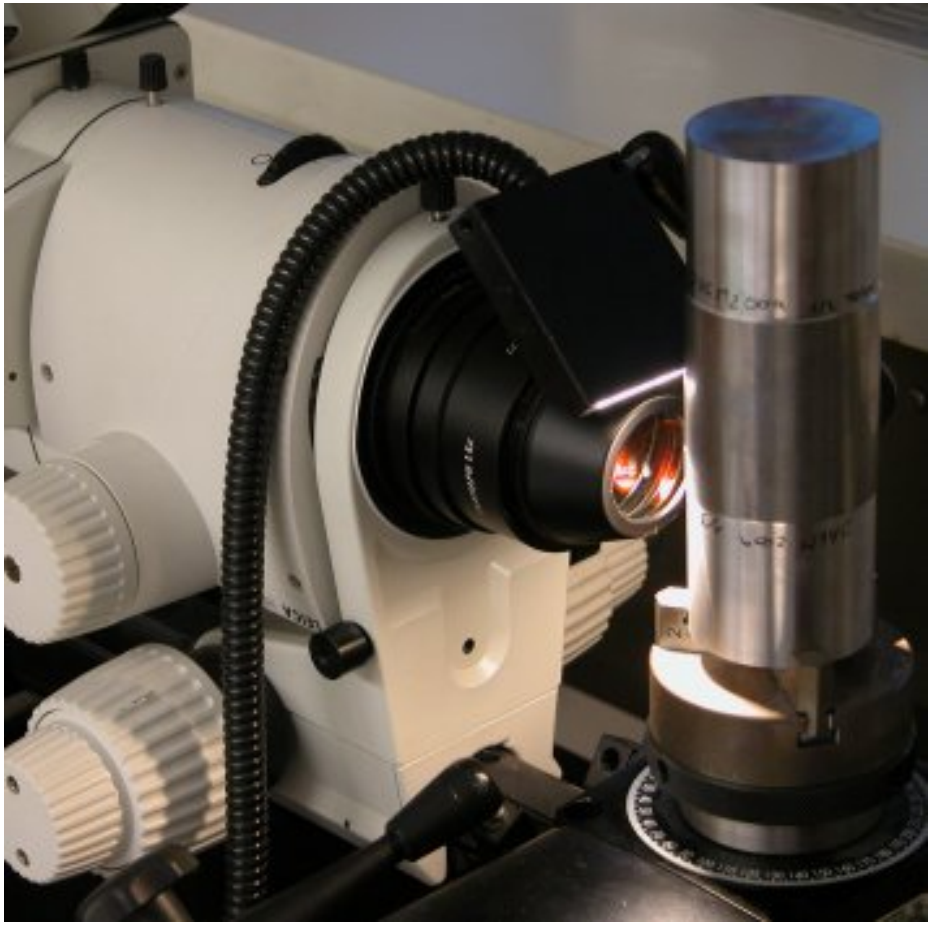
Shifted Normalized Profile

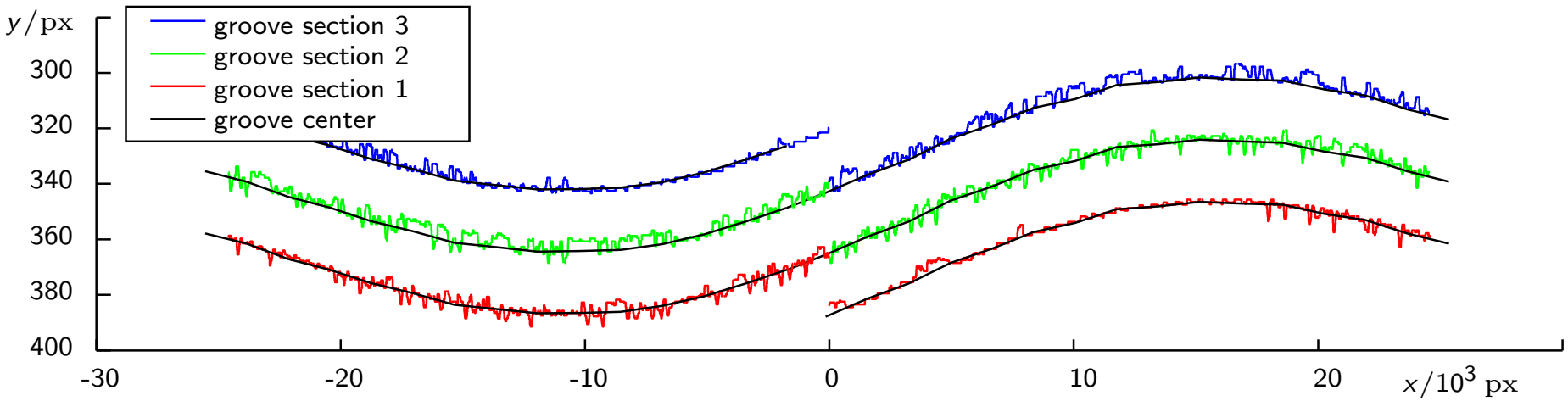


Reading out

Proceeding

- Microscope with low magnification ($2.6\,\mathrm{mm} \times 2\,\mathrm{mm}$)
- Images are stitched together using ≈ 100 views
- Overall surface view is partitioned using ≈ 200 cuts
- Groove sections are extracted and connected

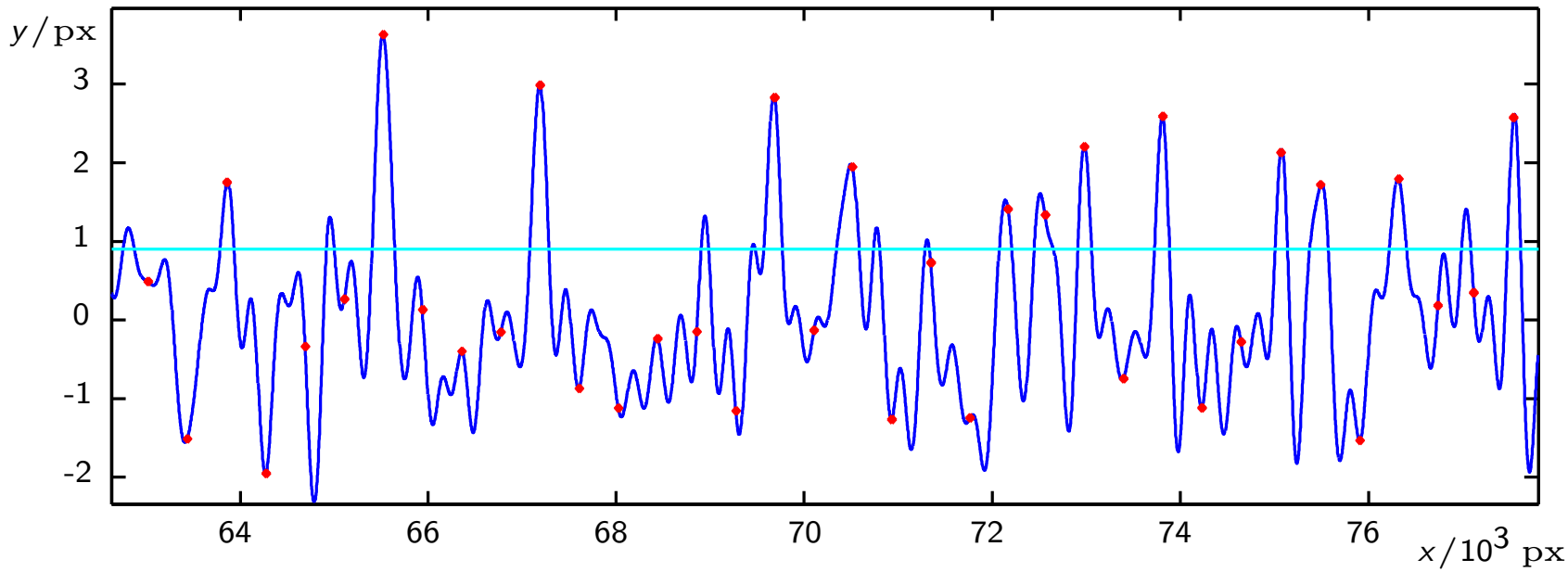




Run of the groove over one rotation

- Center of the groove wobbles (mechanical inaccuracies)
- Groove sections n and $n+1$ are fused
- Exacly one groove wound around the component
- Groove center is subtracted $\Rightarrow$ signal is available

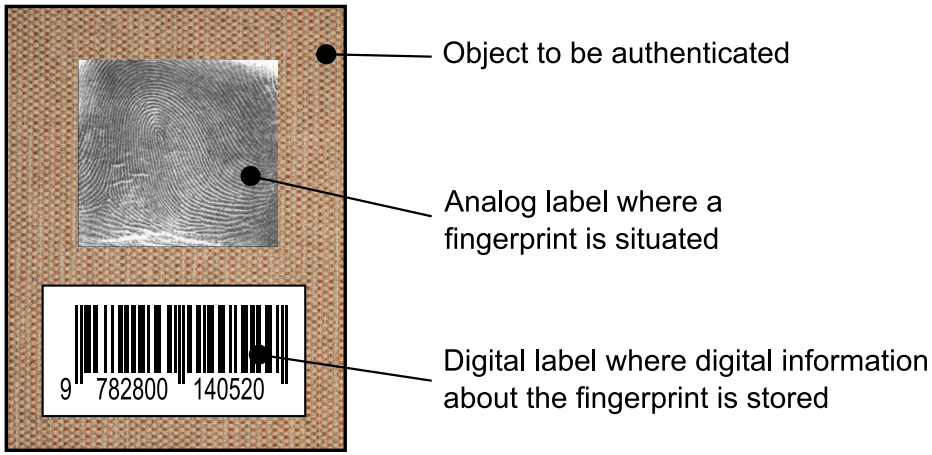
Self-Authentication in Gentelligent Components



- Inherent data storage and readout possible
  - Further error-correcting channel-code could be used
- Inherent fingerprint possible
  - Local disruptions can be overcome by using several grinding profiles

Conclusion

Conclusion



General idea

- Inherently store fingerprint in digital form
- Sign digital data with a public key

$\Rightarrow$ No prior information needed besides a root public key

Self-authentication in gentelligent components

- Groove ($6\,\mu\mathrm{m} \pm 3\,\mu\mathrm{m}$) on surface
- Reading: Directed illumination
- Data density of $1.6\,\mathrm{kbit/cm^2}$
- Fingerprint is grinding imprint
- Digital notation by sampled depth profiles

Data Density Calculation

Calculation

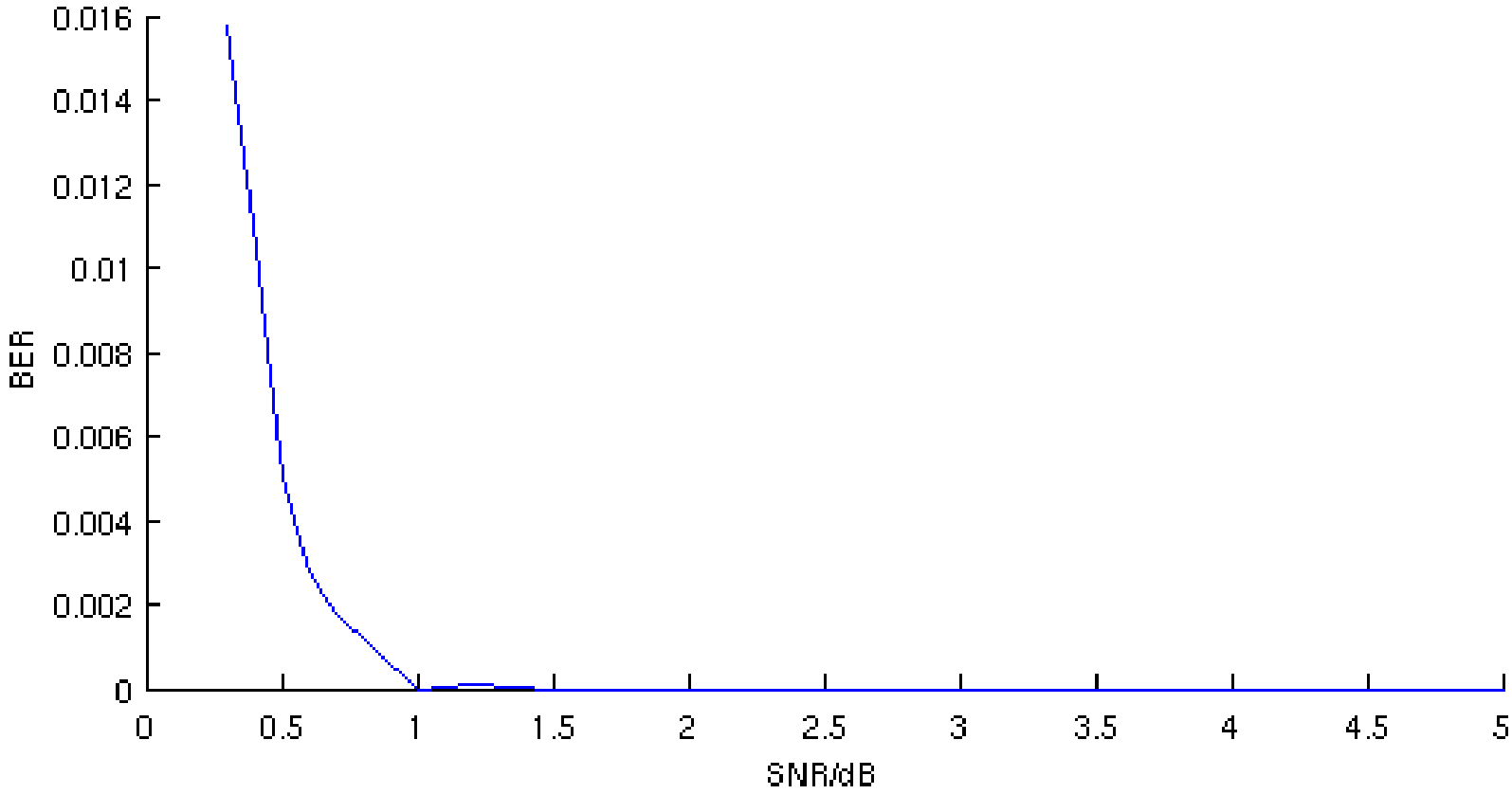
- 2-ASK: 1Bit/Symbol
- Data rate: $R = 1.1/\mathrm{mm}$
- Groove distance: $d_f = 0.07\,\mathrm{mm}$
- Density: $R \times \frac{1}{d_f} \approx 1.6\,\mathrm{kbit/cm^2}$

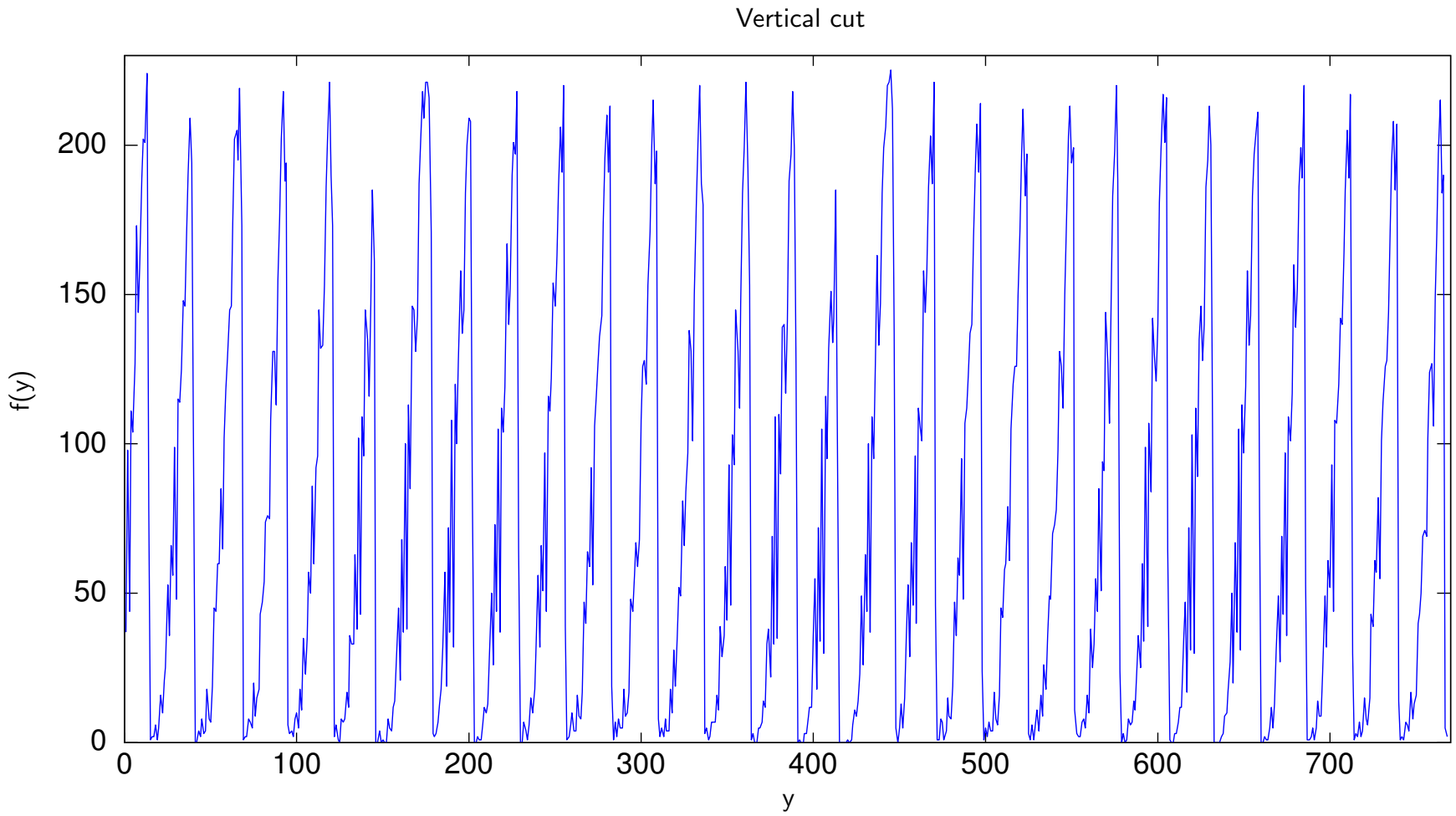
Not taken into account

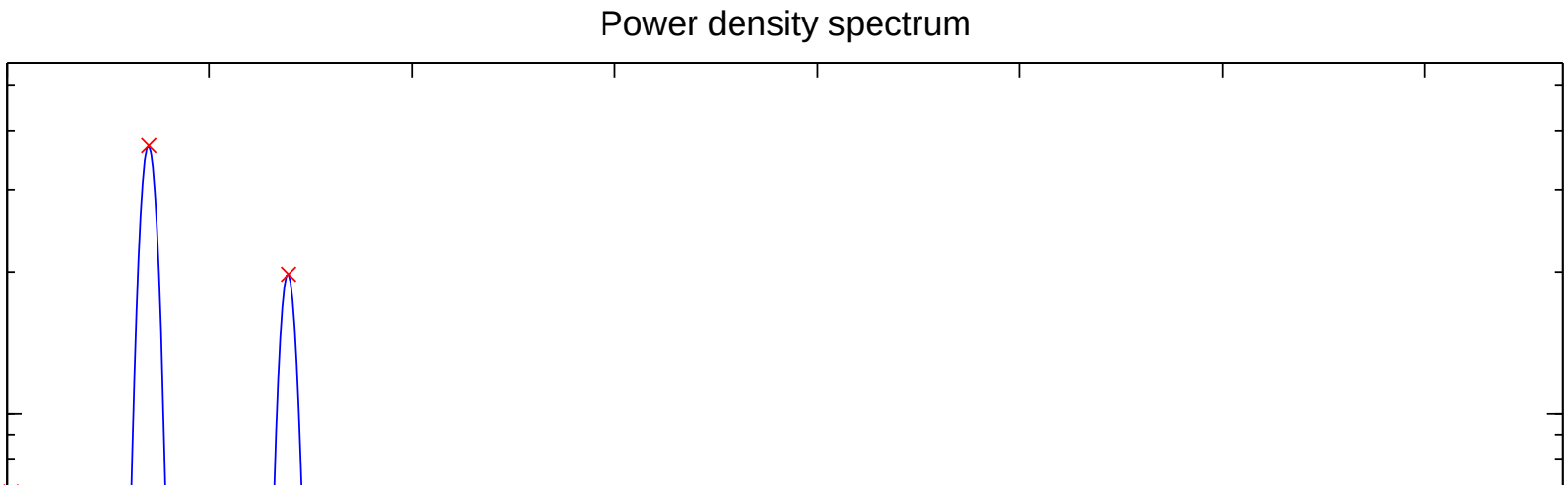
- Simplified demodulation
- Cross talking
- Redundancy for error correction
- Improved modulation scheme with multiple carriers

BER for Turbo Code

2/3 redundancy




Vertical cut
f(y)
y
0
50
100
150
200
0
100
200
300
400
500
600
700


Power density spectrum
10^3