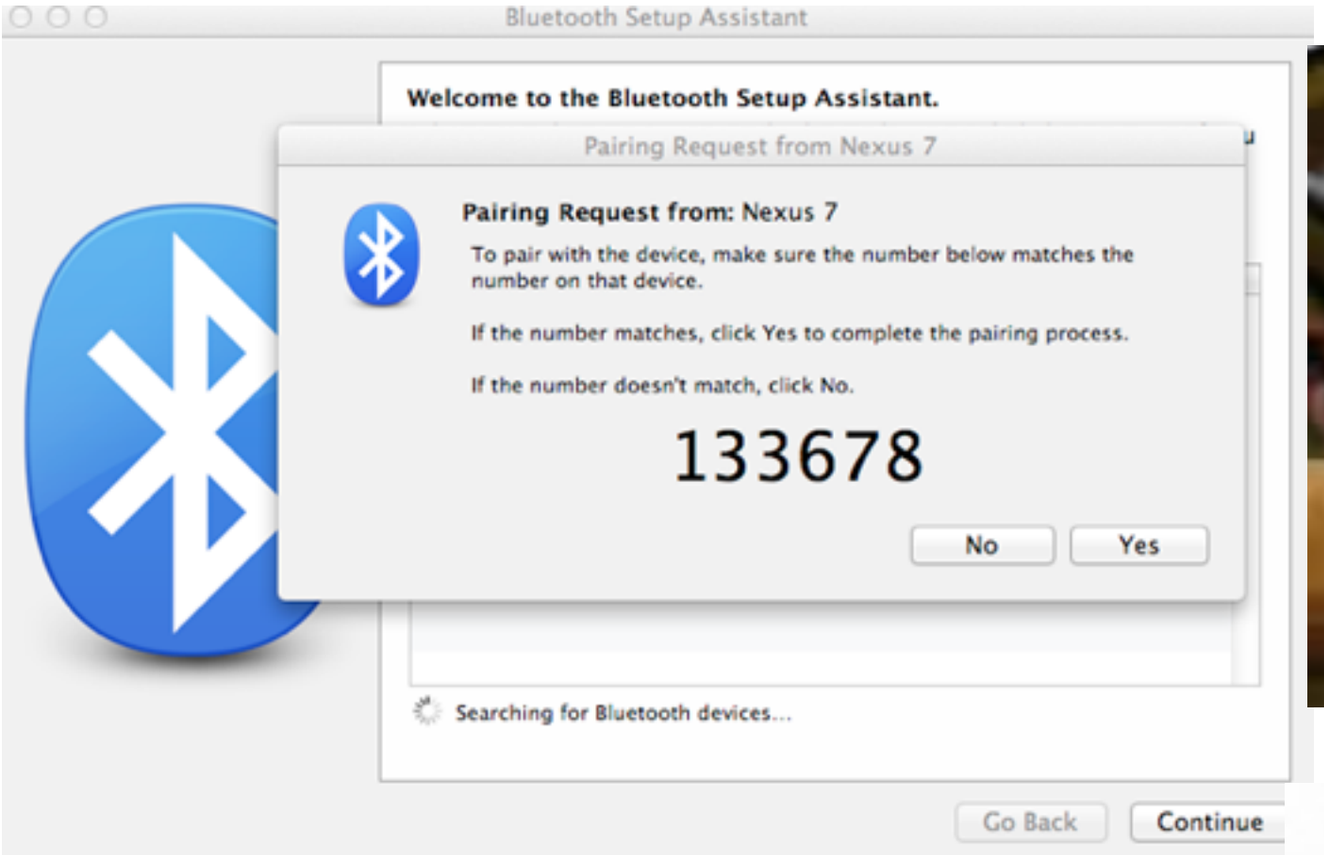
BANDANA - Body Area Network Device-to-device Authentication Using Natural Gait

Dominik Schürmann, Arne Brüsch,
Stephan Sigg and Lars Wolf

presented by William Xie

Pairing protocols

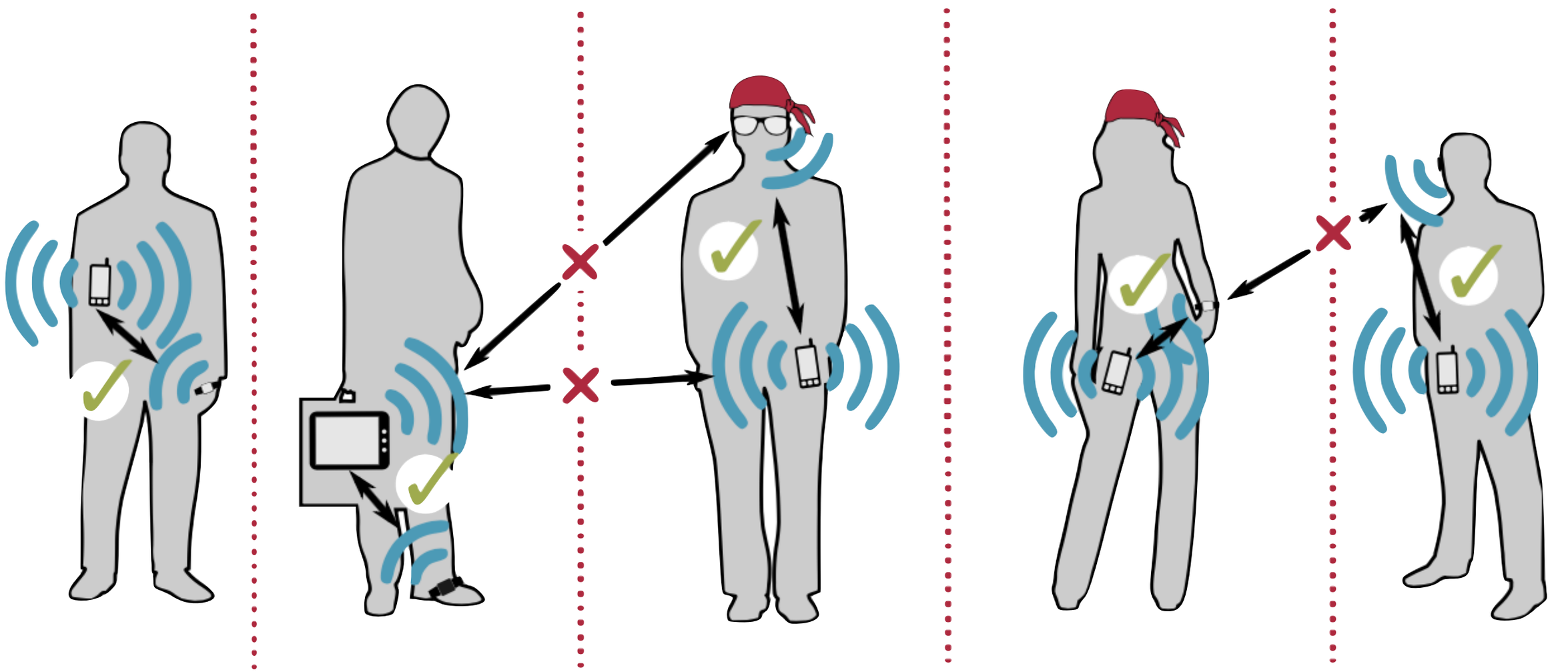


Drawbacks

- Good for one-time paring for limited devices
- Non-scalable large number of devices
- Cannot frequently change identity
- Not seamless

BANDANA

- Secure pairing scheme among on-body devices based on common movement patterns due to co-location on the same body[1]



Paper contributions

- BANDANA pairing protocol
- verification based on large-scale datasets
- security analysis

Data cleanup

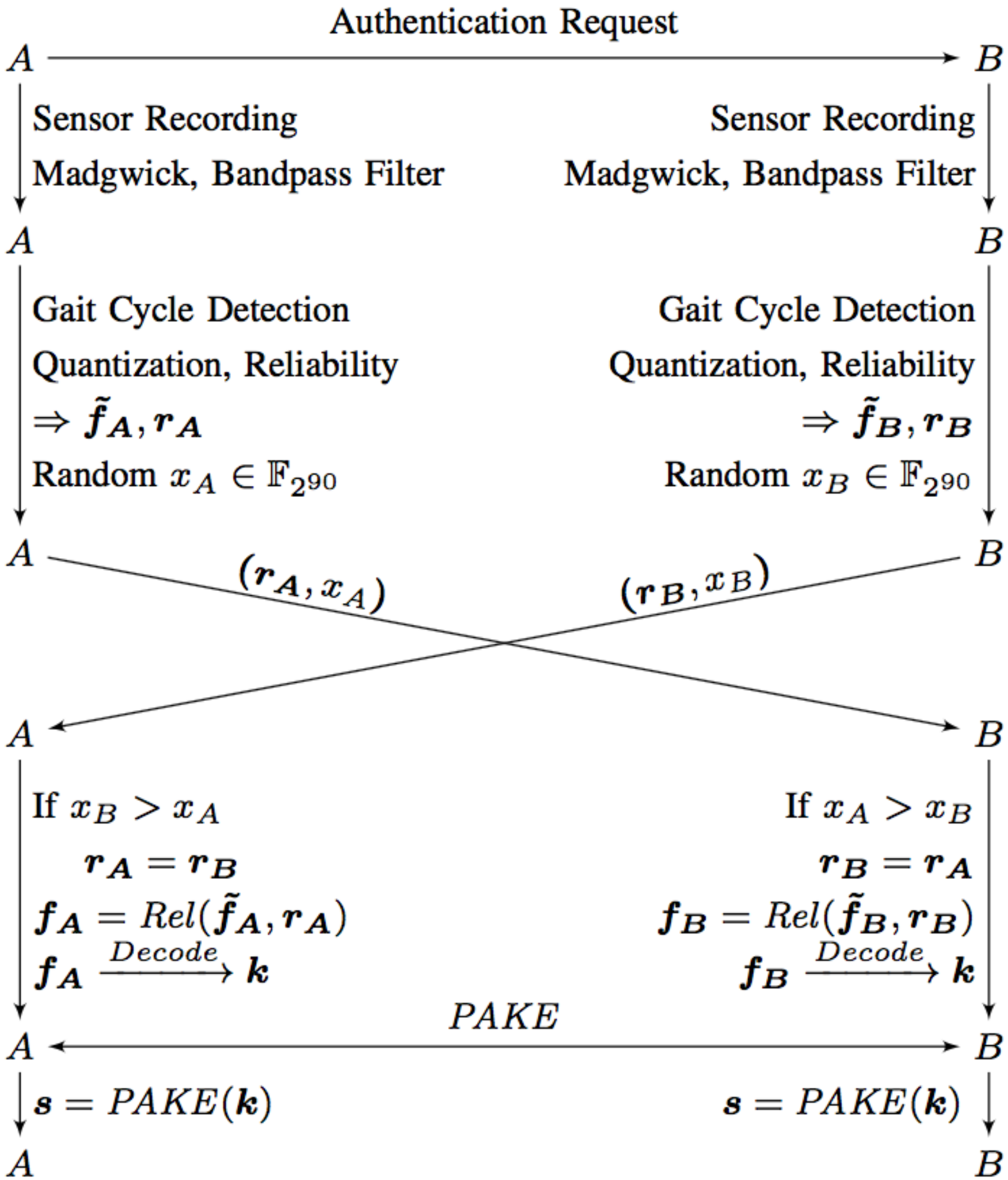
Gait cycle detection

Quantization

Transfer reliability vector

Error correction

Authentication



Data cleanup

- Sensor data: 3-axis accelerometer and gyroscope
- Madgwick's algorithm z-axis normalization
  - Keep only z-axis
- Bandpass filter (Type II Chebyshev)

Data cleanup

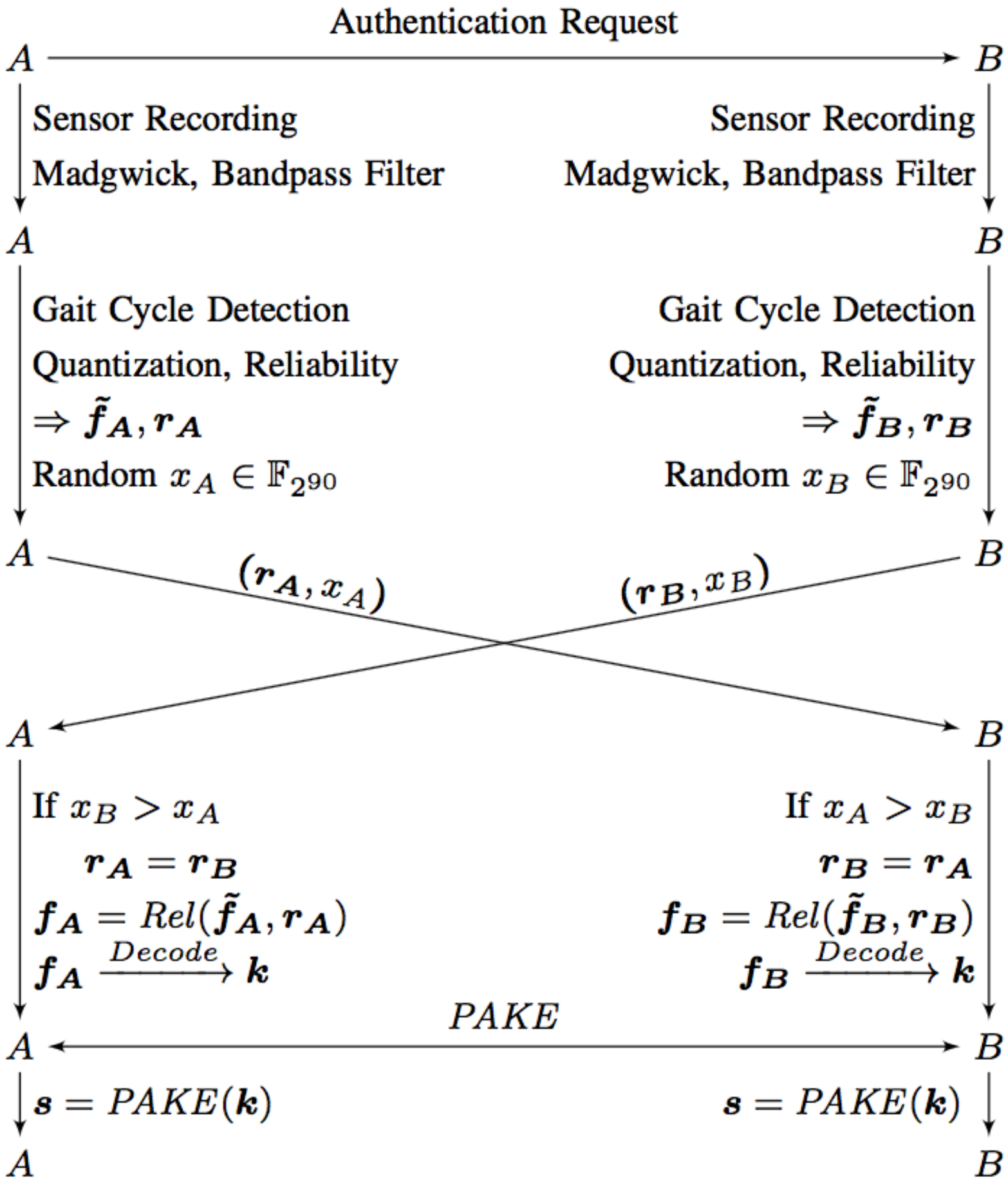
Gait cycle detection

Quantization

Transfer reliability vector

Error correction

Authentication



Gait cycle detection

- Find auto correlation

$$\boldsymbol{a} = (a_1, \ldots a_k, \ldots a_n)$$

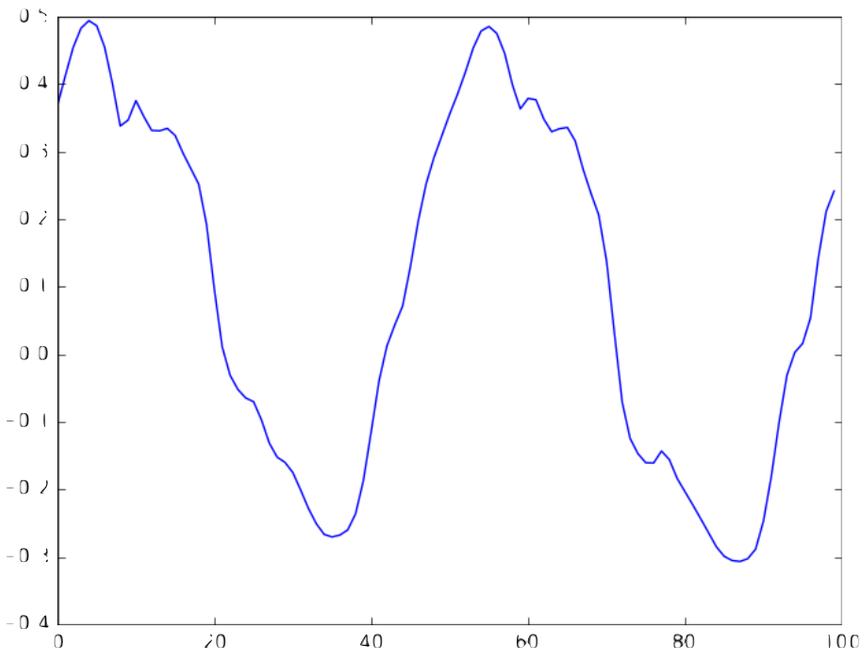
$$a_k = \frac{1}{(n-k)\sigma^2} \sum_{t=1}^{n-k} z_{t+k}.\overline{z_t}$$

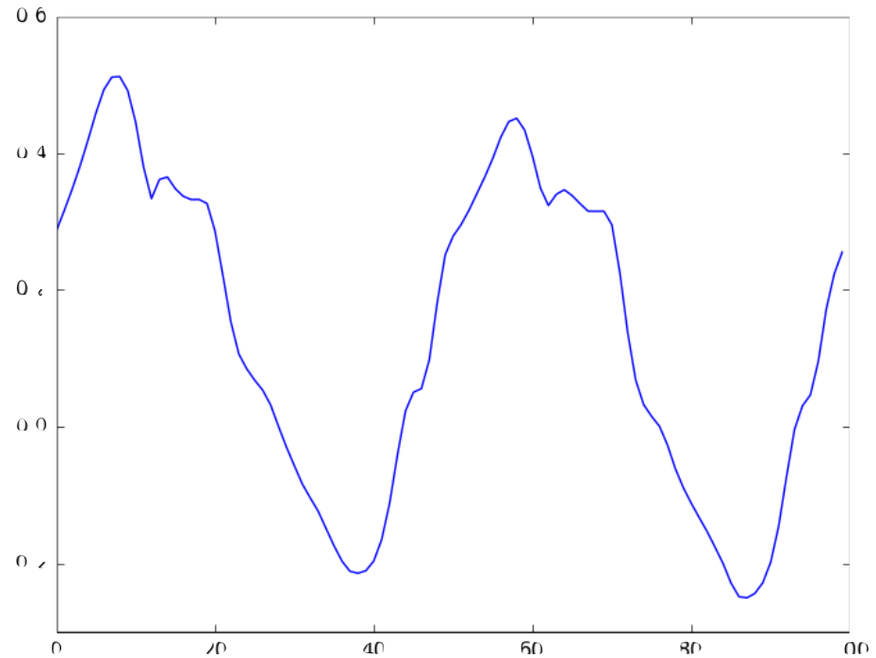
Gait cycle detection

- Find auto correlation

$$\boldsymbol{a} = (a_1, \ldots a_k, \ldots a_n)$$

$$a_k = \frac{1}{(n-k)\sigma^2} \sum_{t=1}^{n-k} z_{t+k} . \overline{z_t}$$





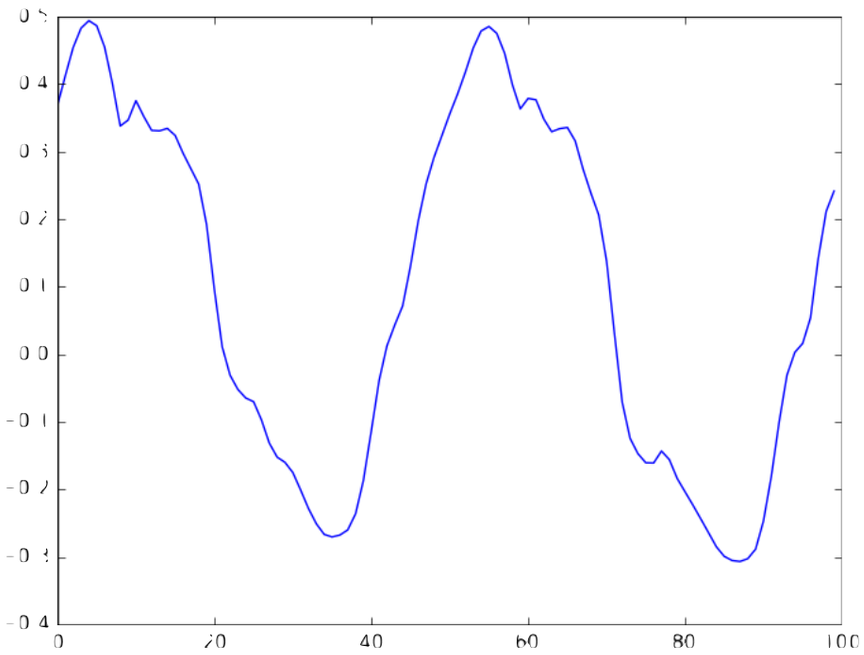
High correlation

Gait cycle detection

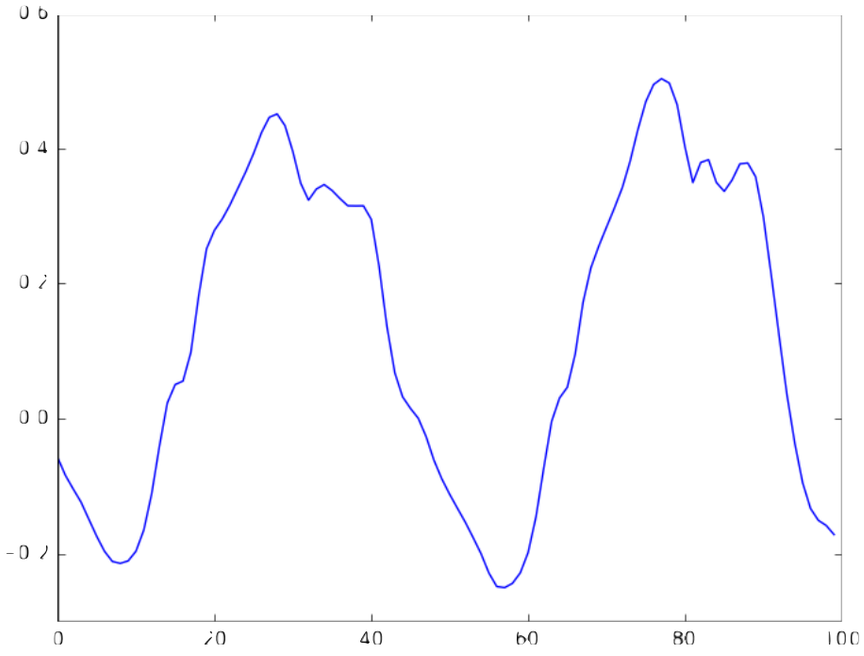
- Find auto correlation

$$\boldsymbol{a} = (a_1, \ldots a_k, \ldots a_n)$$

$$a_k = \frac{1}{(n-k)\sigma^2} \sum_{t=1}^{n-k} z_{t+k} . \overline{z_t}$$



Low correlation



Gait cycle detection

- Find local argmax $\boldsymbol{a}$

$$\boldsymbol{\zeta} = \{\zeta_1, \ldots, \zeta_i, \ldots \zeta_m\}.$$

They represent a collection of time shift k which yields the highest correlations

$$\delta_{mean} = \left\lceil \frac{\sum_{i=1}^{m-1} \zeta_{i+1} - \zeta_i}{m-1} \right\rceil$$

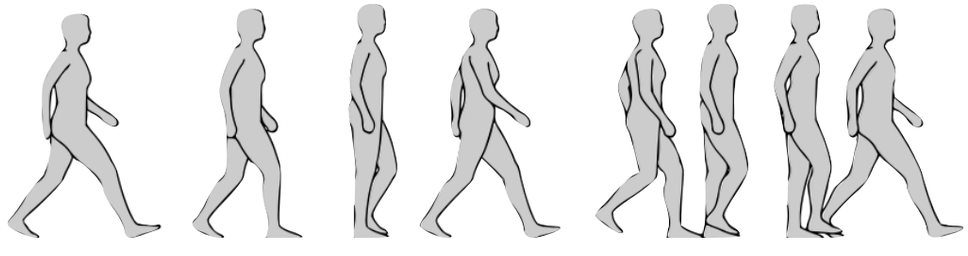
Gait cycle detection

- Look for minimum in each period with deviation τ

$$\boldsymbol{\mu} = \{\mu_1, \ldots, \mu_i, \ldots, \mu_{m-1}\};$$
$$\mu_i = \arg\min\left(z_{\zeta_i-\tau}, z_{\zeta_i-\tau+1}, \ldots, z_{\zeta_i+\delta_{mean}+\tau}\right).$$

- Split input into gait cycles (2 period)

$$\boldsymbol{Z} = \{Z_1, ..., Z_i, ..., Z_q\}$$
$$Z_i = (z_{\mu_{i-1}}, \ldots, z_{\mu_i}, \ldots, z_{\mu_{i+1}-1});$$
$$i = \{1, 3, \ldots, q\}$$



Data cleanup

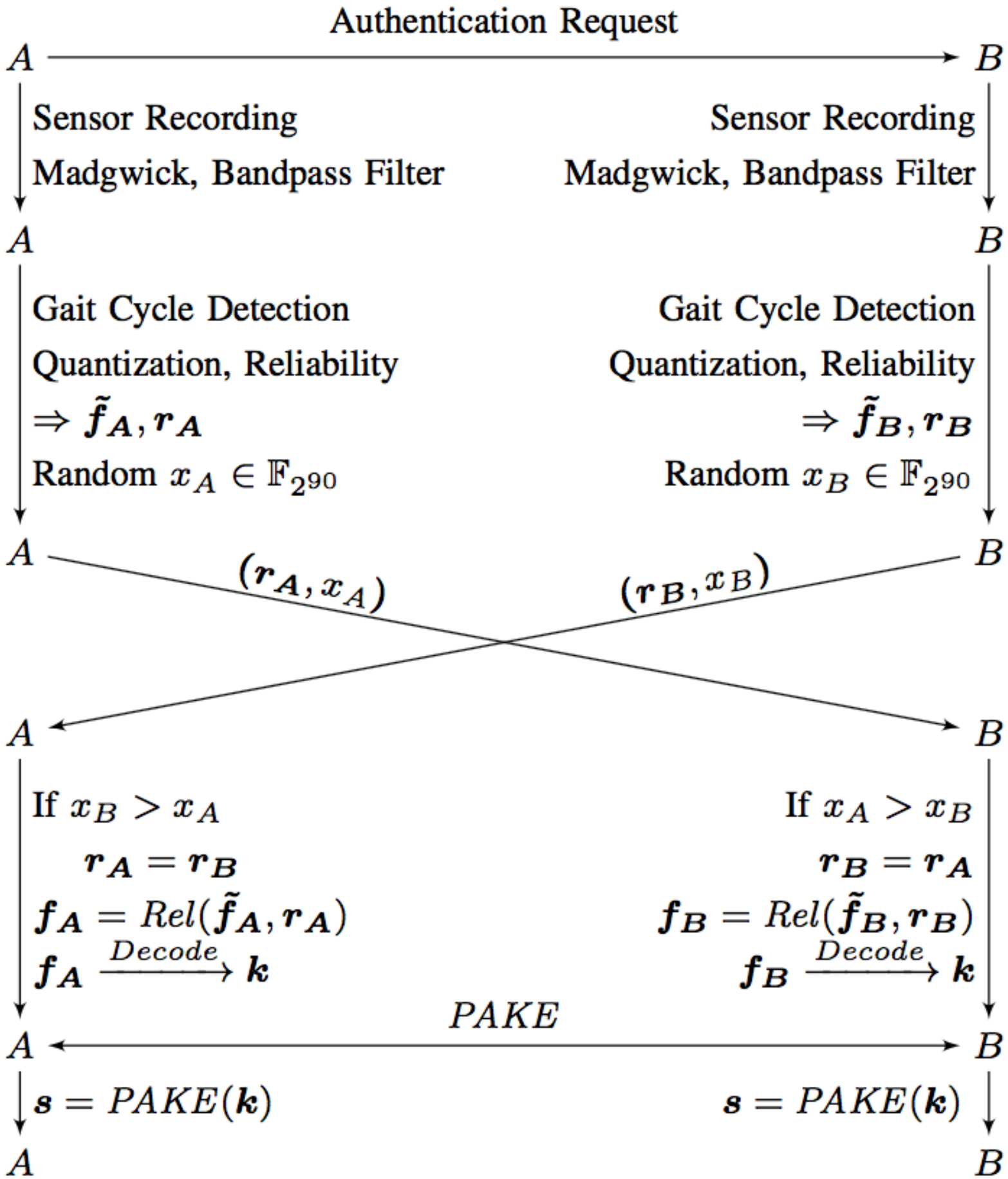
Gait cycle detection

Quantization

Transfer reliability vector

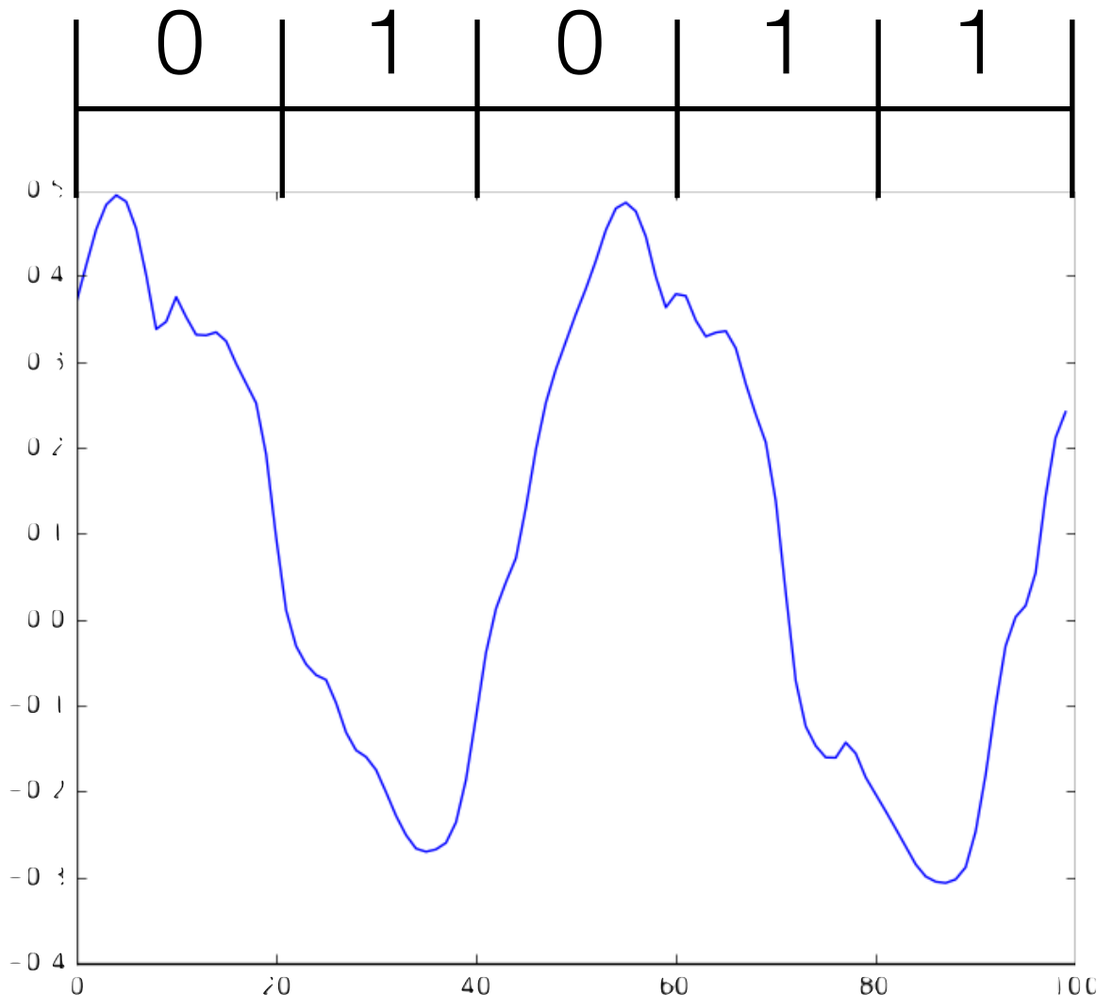
Error correction

Authentication



Quantization

- Energy difference between Z_i and average $\boldsymbol{Z}$



$$\widetilde{f} = \begin{cases} 1, & \text{if } \sum A - Z > 0 \\ 0, & \text{otherwise} \end{cases}$$

Reliability vector:
$\boldsymbol{r} \propto$ energy difference

Data cleanup

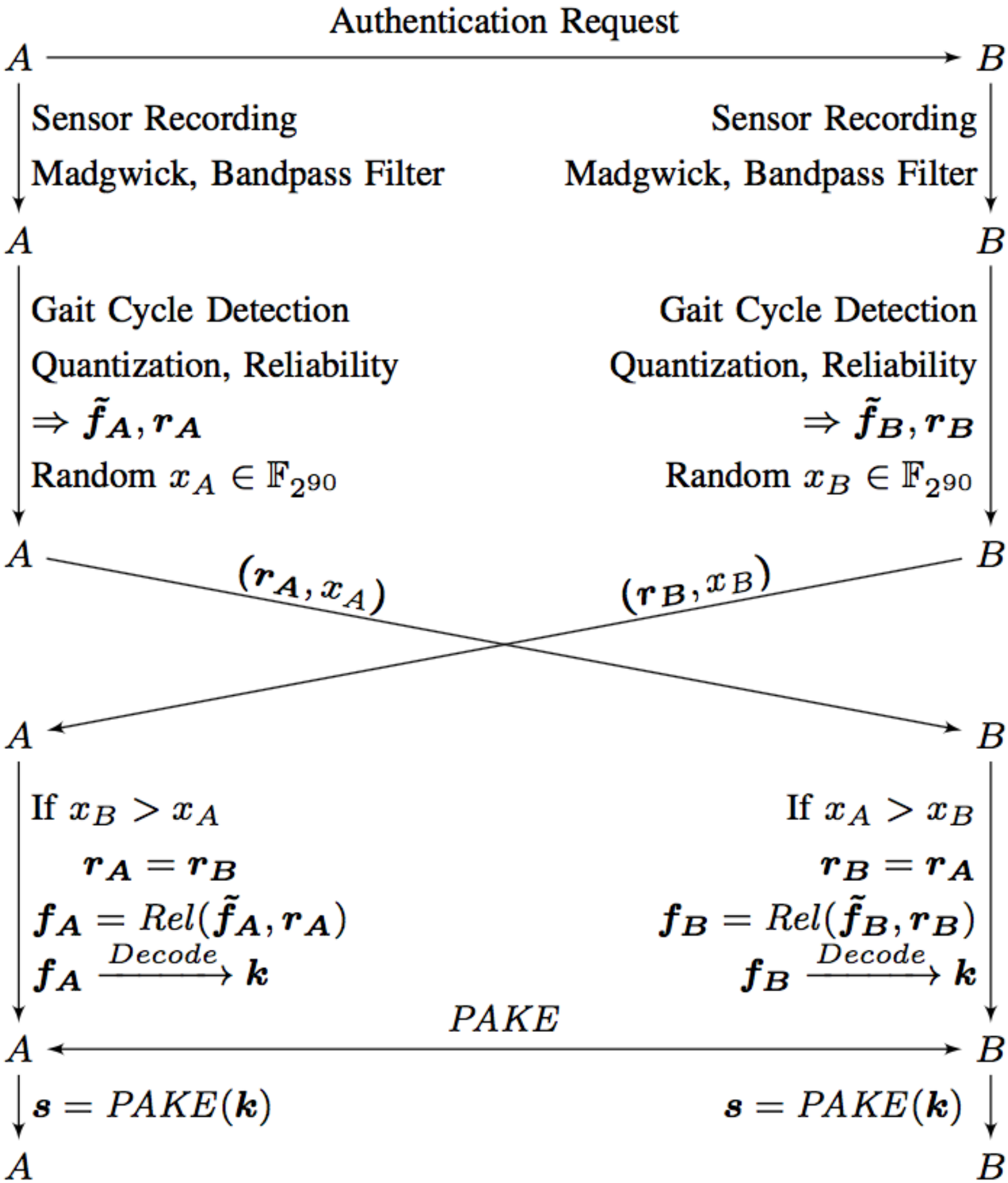
Gait cycle detection

Quantization

Transfer reliability vector

Error correction

Authentication



Transfer reliability vector

- with a random value to a pairing device.
- Compare it against received random value so both devices uses the identical $\boldsymbol{r}$
- Sort $\widetilde{\boldsymbol{f}}$ with ordering of $\boldsymbol{r}$

Data cleanup

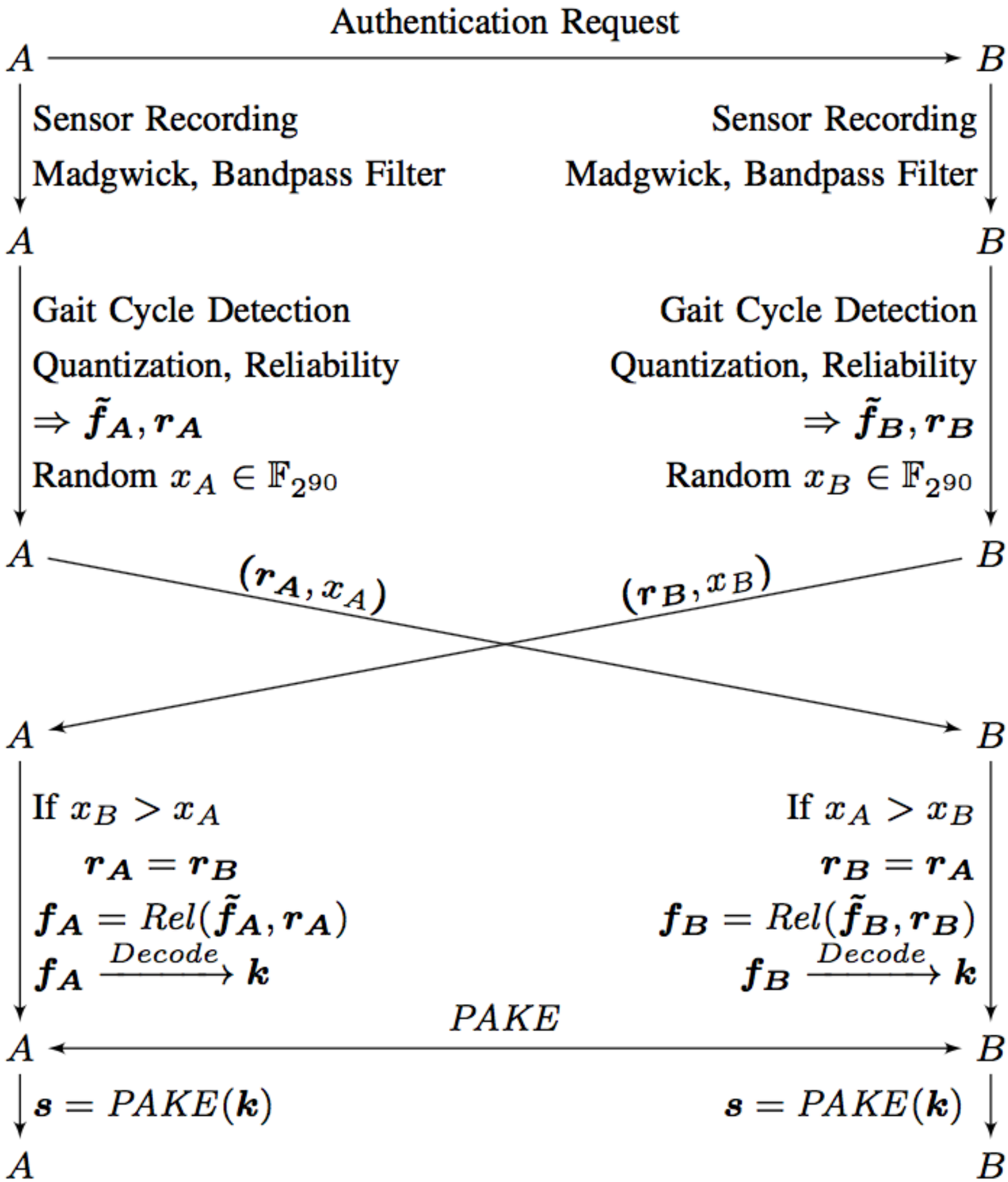
Gait cycle detection

Quantization

Transfer reliability vector

Error correction

Authentication



Error correction and Authentication

- using BCH code with user defined bit errors
- J-PAKE to generate shared secret

Data cleanup

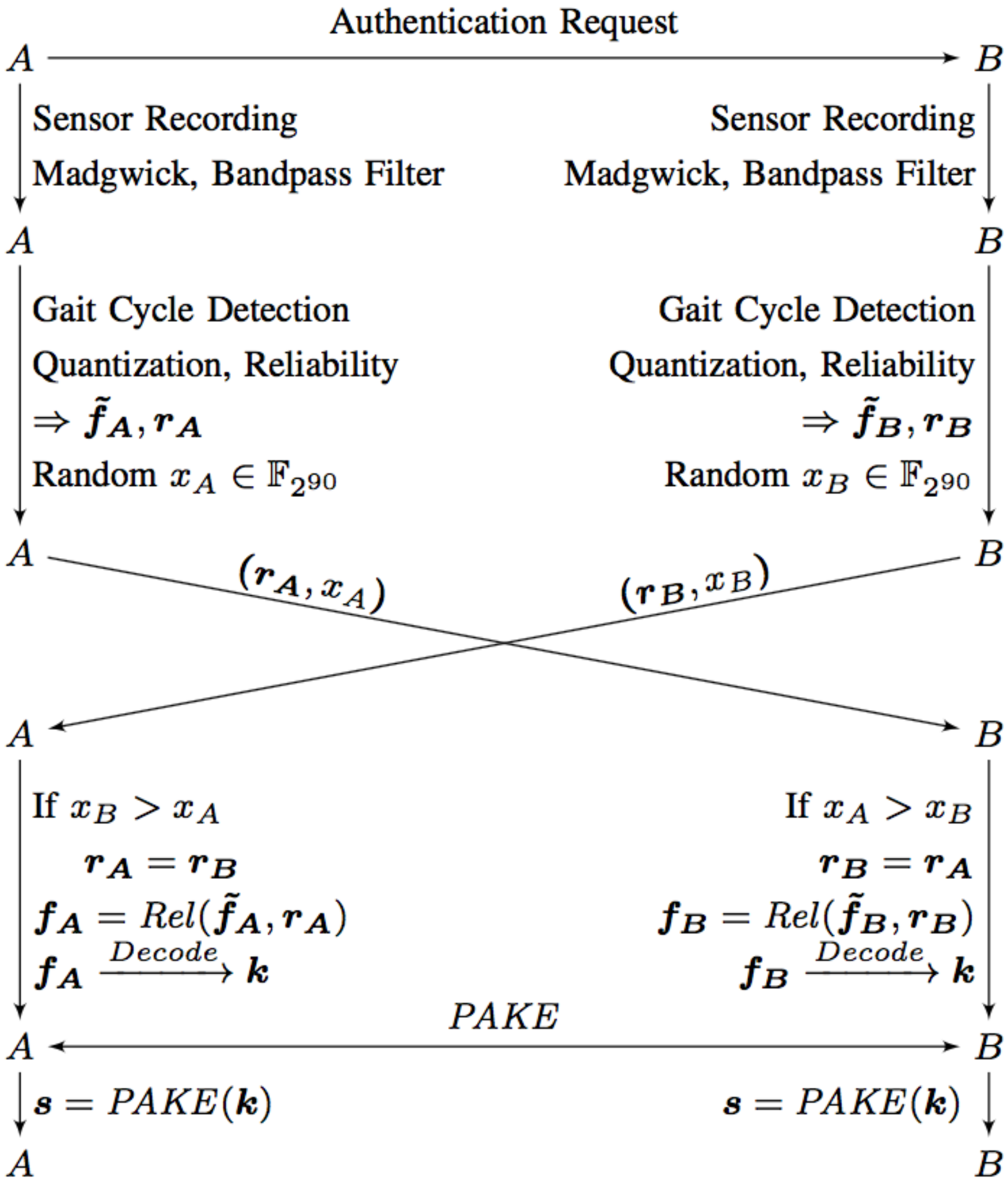
Gait cycle detection

Quantization

Transfer reliability vector

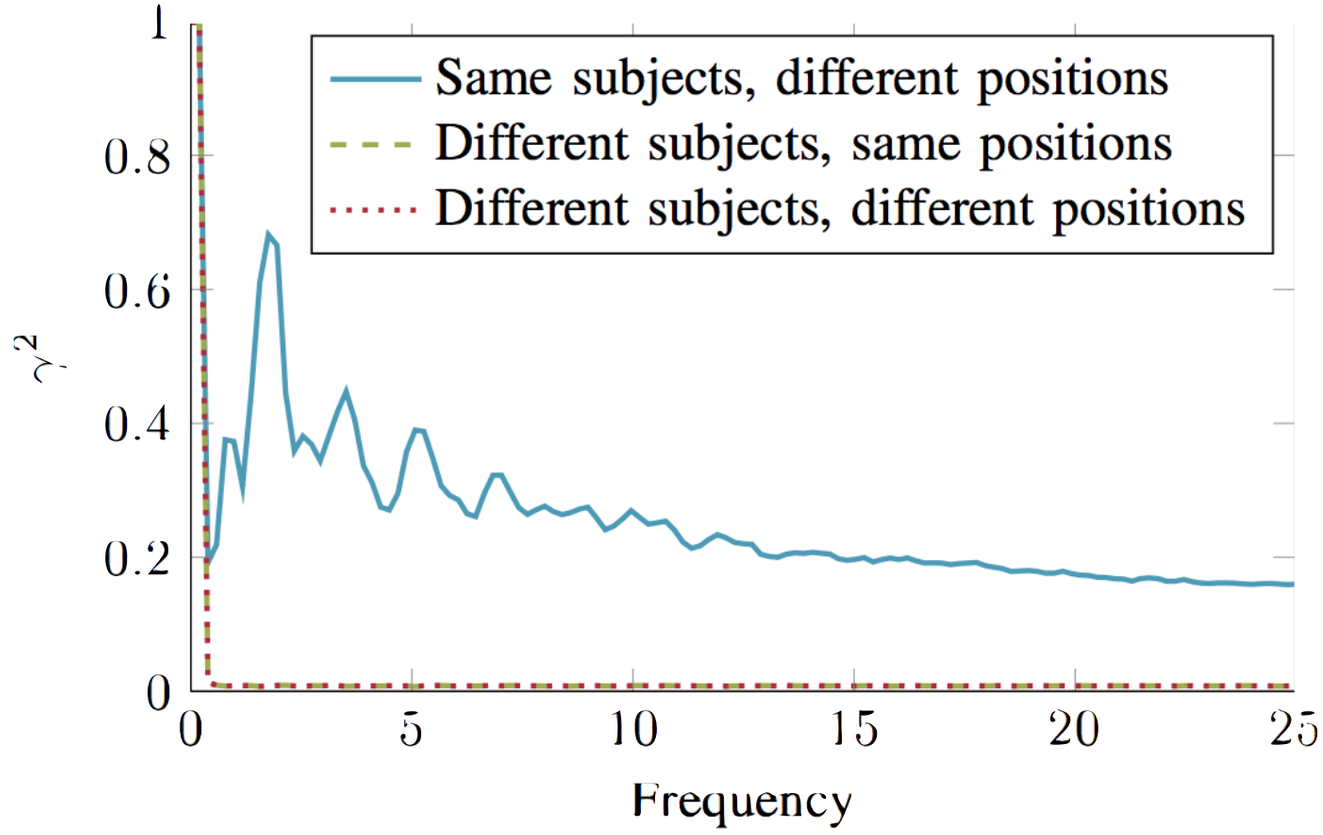
Error correction

Authentication



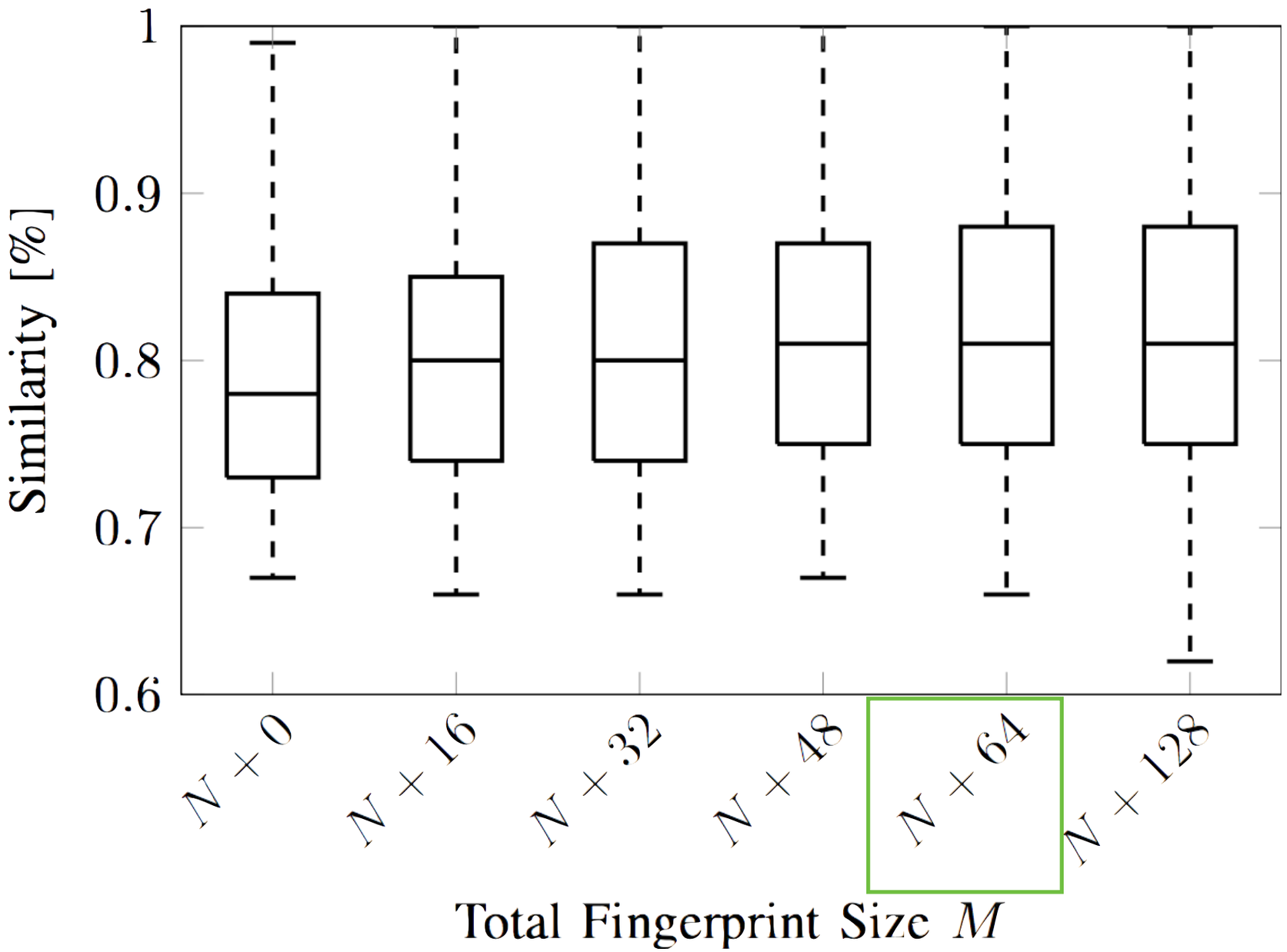
Analysis

- Normalized z-axis signals have **high** spectral coherence for **same** subjects, **low** for **different** subjects

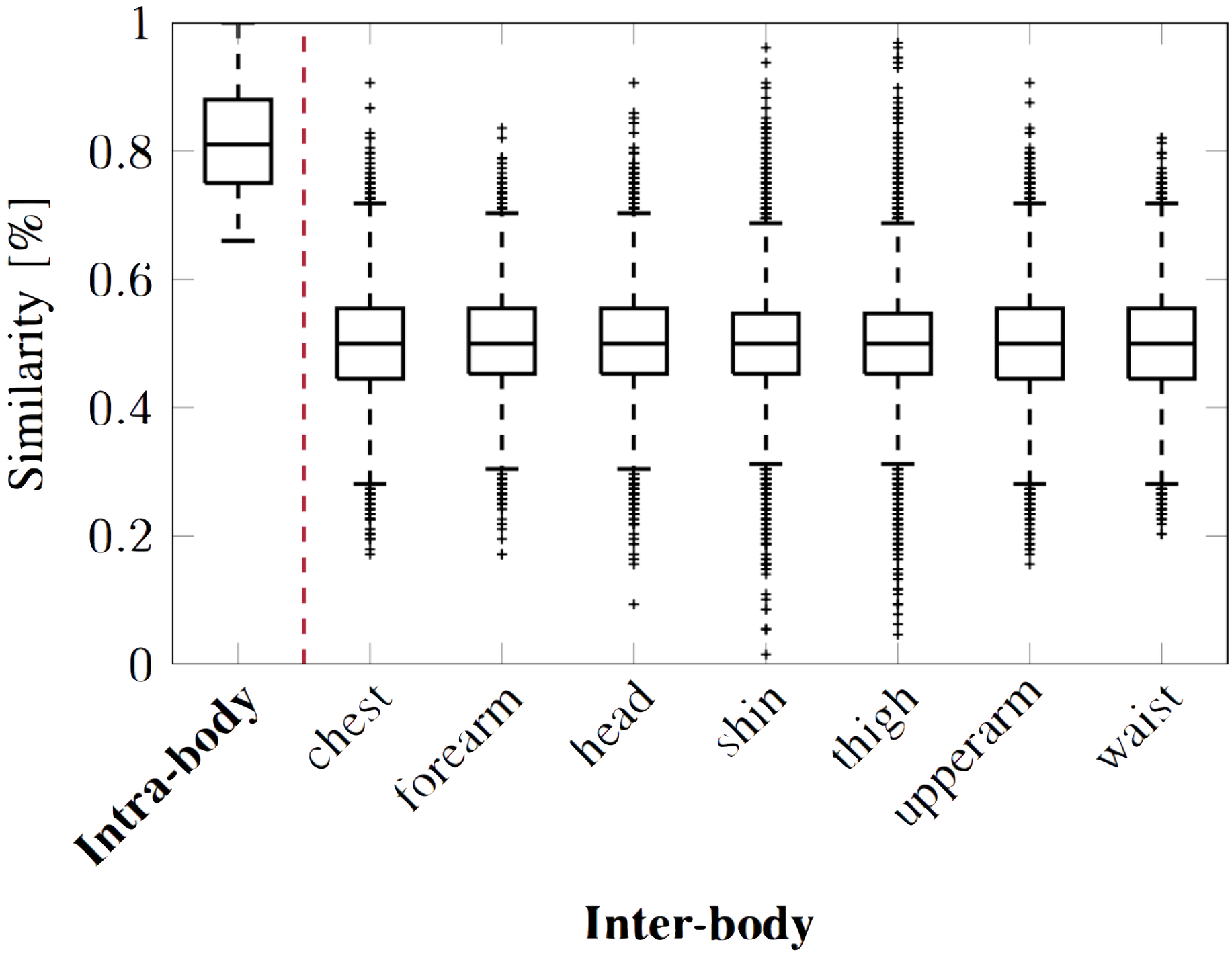


- Noise < 0.5 Hz and > 10 Hz [2]

Analysis


1
0.9
0.8
0.7
0.6
Similarity [%]
$N+0$
$N+16$
$N+32$
$N+48$
$N+64$
$N+128$
Total Fingerprint Size M

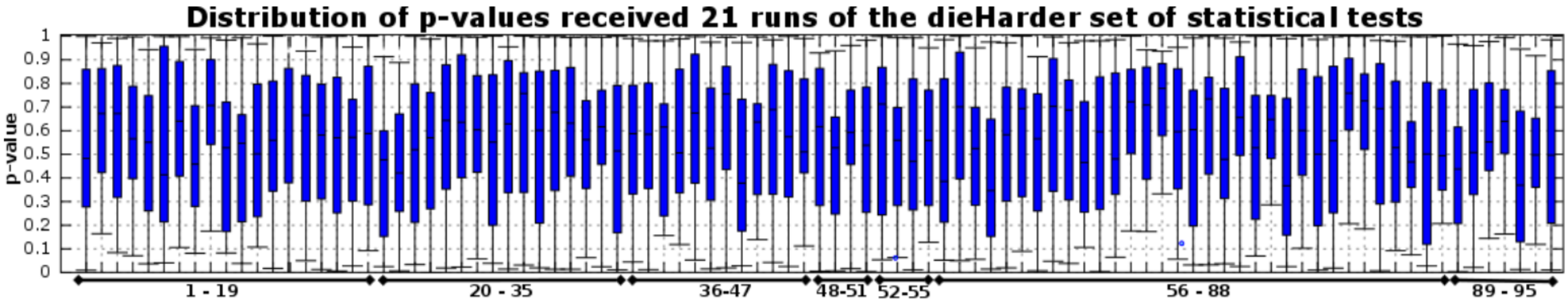
Analysis


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

Analysis

	chest	forearm	head	shin	thigh	upperarm	waist
chest	1.0	0.82	0.74	0.78	0.78	0.88	0.81
forearm	0.82	1.0	0.8	0.81	0.88	0.89	0.89
head	0.74	0.8	1.0	0.8	0.76	0.77	0.78
shin	0.78	0.81	0.8	1.0	0.77	0.78	0.8
thigh	0.78	0.88	0.76	0.77	1.0	0.85	0.84
upperarm	0.88	0.89	0.77	0.78	0.85	1.0	0.88
waist	0.81	0.89	0.78	0.8	0.84	0.88	1.0

Analysis


Distribution of p-values received 21 runs of the dieHarder set of statistical tests
p-value
1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
1 - 19
20 - 35
36-47
48-51
52-55
56 - 88
89 - 95
1: birthdays
2: operm5
3: rank32x32
4: rank6x8
5: bitstream
6: opso
7: oqso
8: dna
9: count1sstr
10: count1sbyt
11: parkinglot
12: 2dsphere
13: 3dsphere
14: squeeze
15: runs
16: craps
17: marsagliatsangcd
18: stsmonobit
19: stsruns
20-35: sts-serial (1-16)
36-47: rgb-bitdistribution (1-12)
48-51: rgb-minimum distance (2-5)
52-55: rgb-permutations (2-5)
56-88: rgb-lagged-sum (0-32)
89: rgb-kstest-test
90: dab-bytedistrib
91: dab-dct
92: dab-filltree 32
93-94: dab-filltree (0,1)
95: dab-monobit2 (12)

Analysis

Security:

- Mimic gait
- Brute force
- Video recording
- **Attach malicious device**

Discussions

- Dataset choices
- Why N = 128?
- Very long authentication time and tries per day
- 80% Threshold
- Different, non-periodic motion
- Not enough details on deliberate attacks

References

1. Schürmann, Dominik, et al. "BANDANA--Body Area Network Device-to-device Authentication using Natural gAit." arXiv preprint arXiv:1612.03472 (2016).

2. Lester, Jonathan, Blake Hannaford, and Gaetano Borriello. ""Are You with Me?"–Using Accelerometers to Determine If Two Devices Are Carried by the Same Person." International Conference on Pervasive Computing. Springer Berlin Heidelberg, 2004.