

Fast, precise and repeatable positioning of EM-probes for local Side-Channel Attacks

Matthias Probst^{*}, Alexander Wiesent^{*}, Michael Gruber[†], Georg Sigl^{*†}

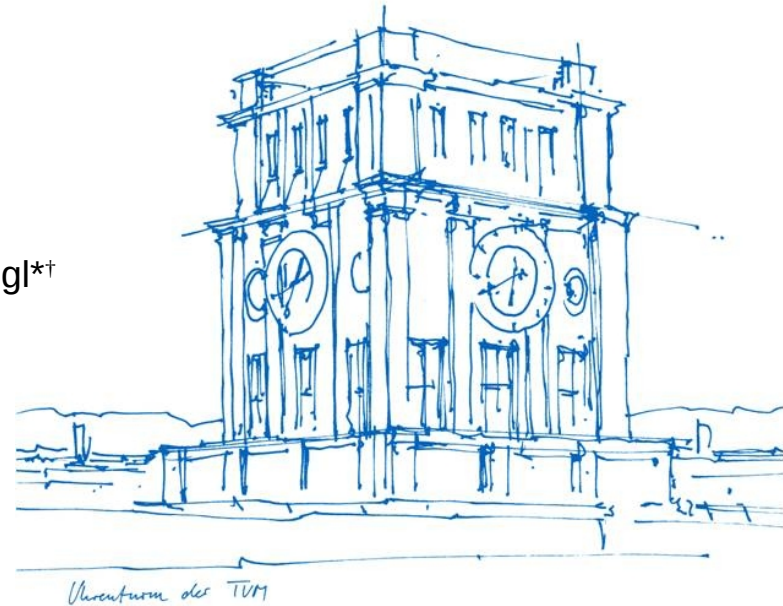
^{*}Technical University of Munich

TUM School of Computation, Information and Technology

Chair of Security in Information Technology

[†]Fraunhofer Institute for Applied and Integrated Security (AISEC)

Munich, Germany

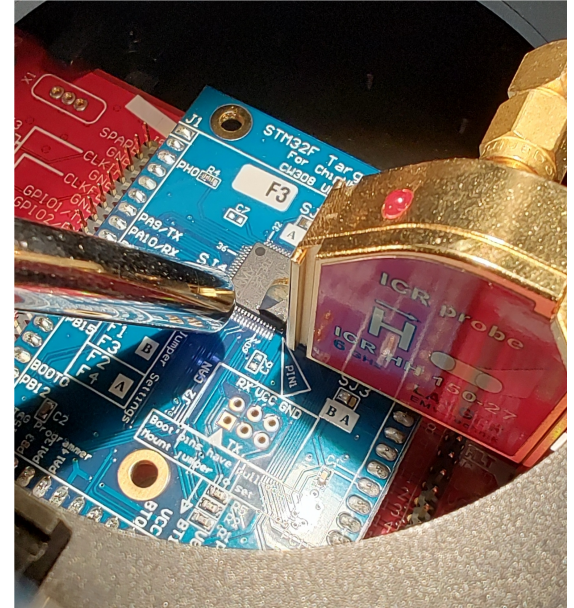


Why care about repositioning?

Repositioning is important for:

- Profiled Attack Scenario
- Attacking the same position again
 - Labs are typically limited by the amount of x-y-z tables
 - Leveraging the same attack position for a different attack
- Extending Machine Learning Datasets
- Reproducibility of results across different research groups

→ Consistently placing a local probe is required with high accuracy



Related Topics & Contribution

For **finding** a suitable attack location:

- Iyer and Yilmaz: An adaptive acquisition approach to localize electromagnetic information leakage from cryptographic modules, 2019
 - Greedy acquisition approach
- Jiang and Pavlidis: A Probe Placement Method for efficient Electromagnetic Attacks, 2021
 - Local maximum of SNR
- Iyer and Yilmaz: Rapid Pre-Characterization of fine-grained EM Side-Channel (In)vulnerability of AES Modules, 2022
 - → F-Statistic based approach
- ...

Refinding this location again:

- Richter et al.: Automated Probe Repositioning for on-die EM-Measurements, 2019
 - Machine Learning Based Approach with average accuracy of 30 μm

Related Topics & Contribution

Richter et al.: Automated Probe Repositioning for on-die EM-Measurements, 2019:

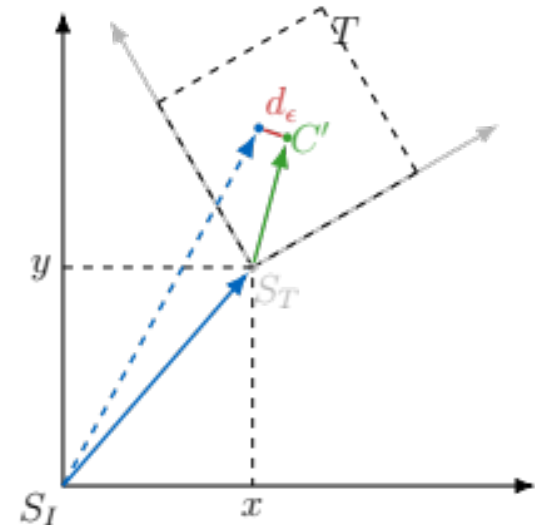
- Machine-Learning based
- **200** trace per position required, point of interest search, leakage from AES
- Accuracy of 30 μm on average (dep. on Position)

This work:

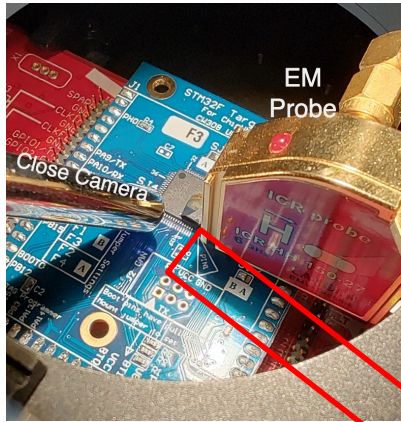
- Image positioning based
- Only **one** trace per position required for repositioning
- Accuracy of 30 μm Guaranteed

1. Profile the **profiling** chip with a detailed **map I** (full chip area and 20um step size)
2. Record the map of the **testing** chip **map T** (not necessary to cover the full chip area)
3. Identify the difference (x,y,angle) between **T** and **I** with one of our positioning algorithms
 - Correlation Coefficient (CC)
 - Particle Filter (PF)
 - Oriented Fast and rotated Brief (ORB)
4. Use parameters to precisely position probe on testing chip

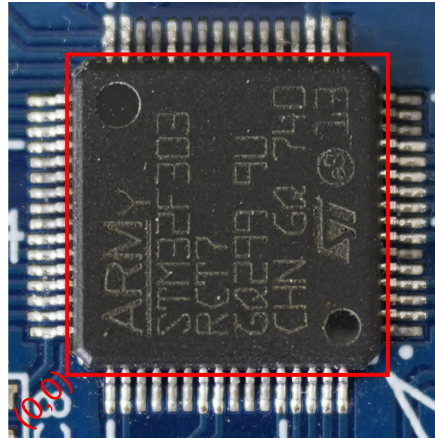
In our experiments, the error is given as d_ϵ as difference from the center of **map T**



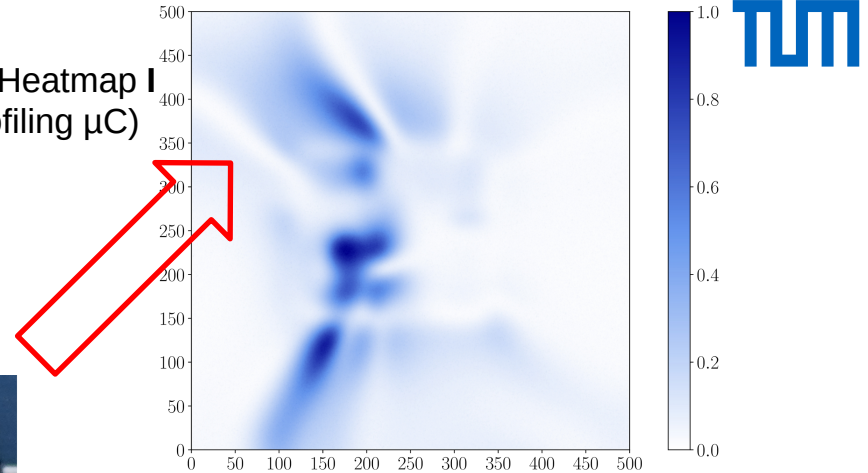
Map Recording



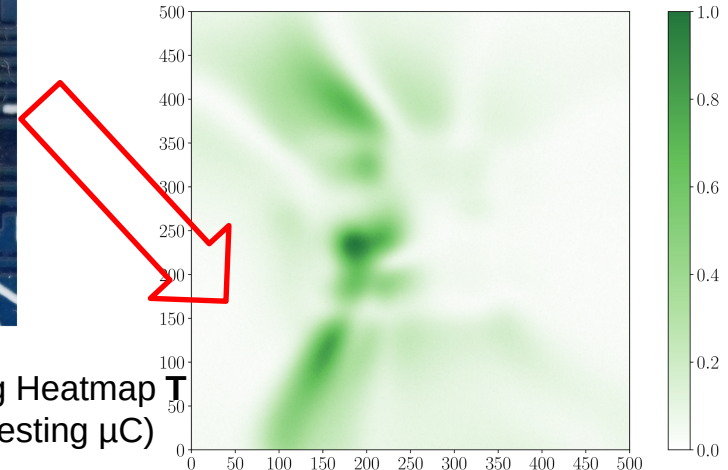
Scan the area with 20 μ m step size



Profiling Heatmap **I**
(form profiling μ C)



Testing Heatmap **T**
(form testing μ C)

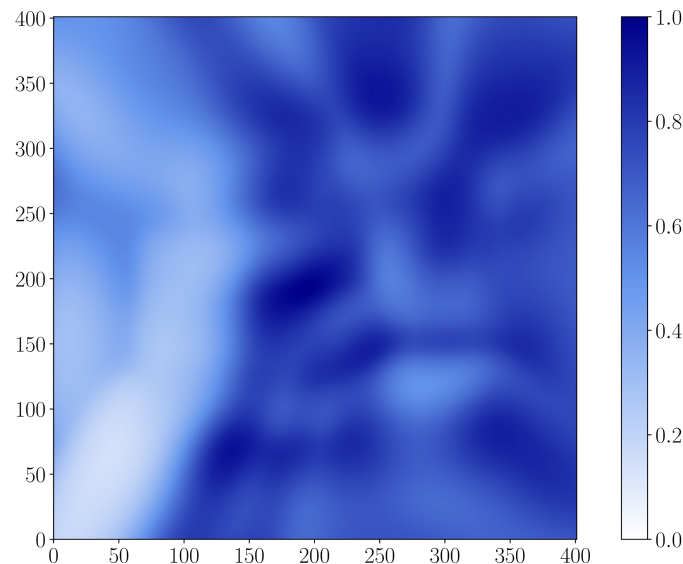


Correlation Coefficient (CC)

The cross correlation between **T** and **I** for each possible position and with different rotation **angles** with:

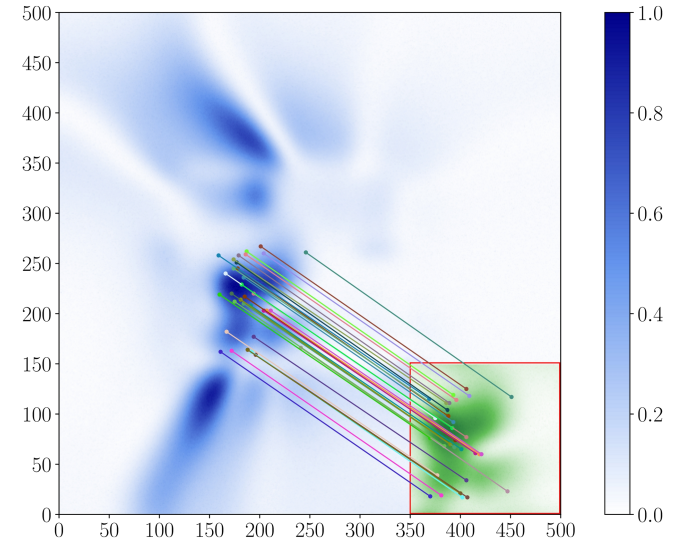
$$R(x, y) = \frac{\sum_{x', y'} \bar{T}(x', y') \cdot \bar{I}(x + x', y + y')}{\sqrt{\sum_{x', y'} \bar{T}(x', y')^2 \cdot \sum_{x', y'} \bar{I}(x + x', y + y')^2}}$$

- + Low computational effort
- + Accurate results for similar maps
- Noise and image difference can degrade accuracy



Oriented Fast and rotated Brief (ORB)

- Pyramid level detection scheme
 - Keypoints are first identified in **T** and **I** and matched later
 - Parameters (size of features, number of classification levels, number of level elements, etc.) are automatically tuned in our algorithm
 - Position is determined by the highest number of matches
- + Rotation and scale agnostic
- + More resistant to noise
- Complexity due to parameter space may lead to local optima



Particle Filter (PF)

Probabilistic iterative approach

1. n particles with features (position, direction) are randomly spread over the feature map (i.e. I) representing possible state based on T
2. Particles are weighted based on how close they match I
3. Higher weights = better match
4. Low weight particles are discarded
5. New particles are randomly resampled around high weight particles
6. Process runs again from 2.

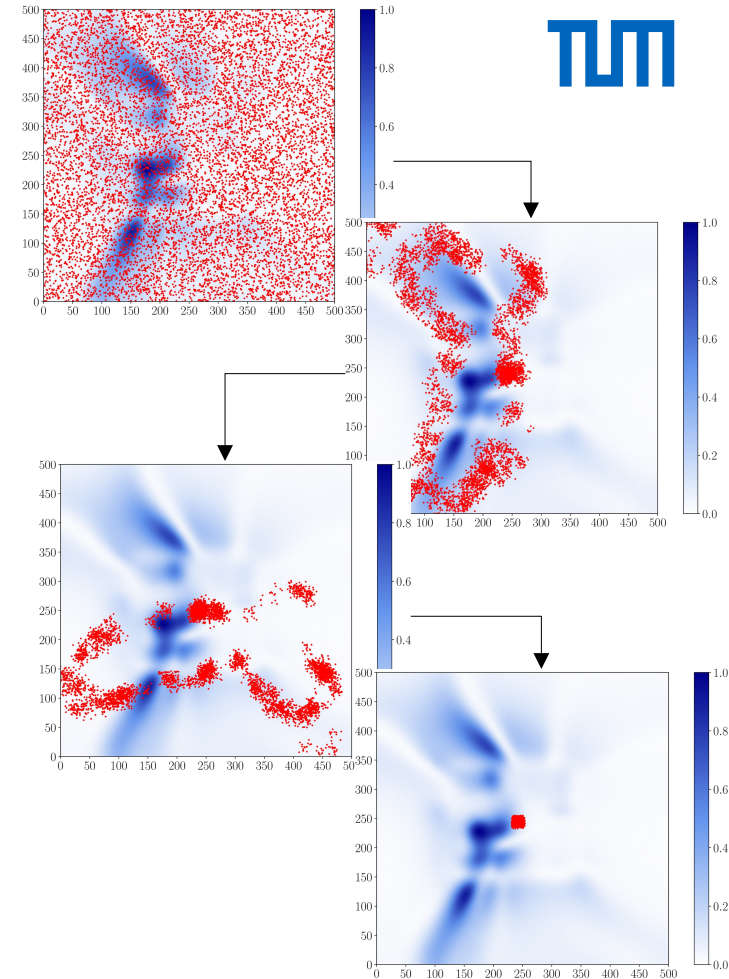
+ Multivariate Input space

+ Noise resistance

- Probabilistic

- Scalability

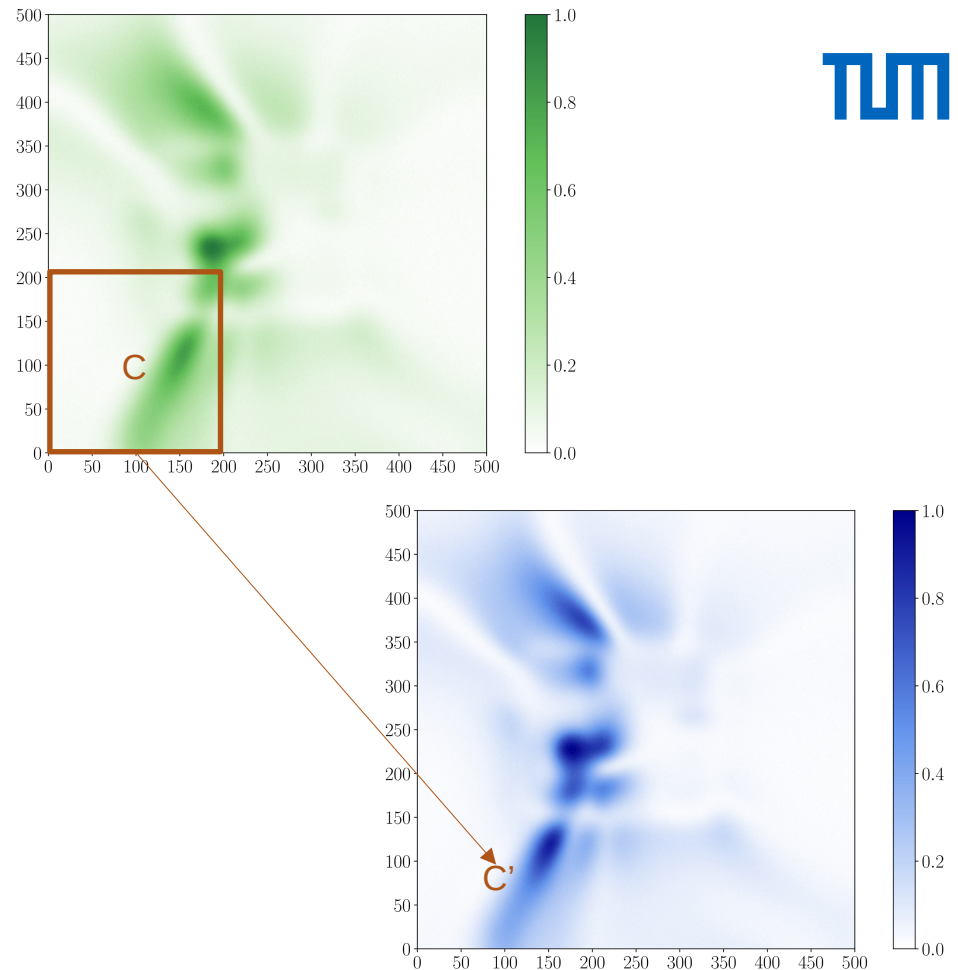
Matthias Probst - Fast and precise repositioning



Experiment Description

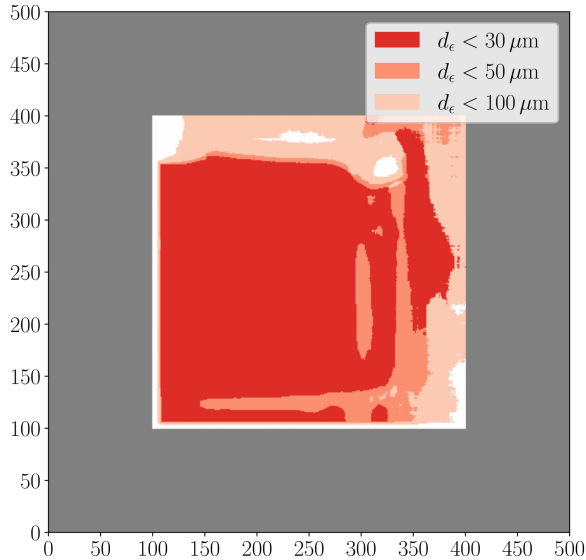
Testing every possible 200x200 rectangle of **I**:

- Accuracy is plotted based on the error of Center point C
- For each probe and method, we run 90601 test (= number of possible choice of 200x200 sized **I**)

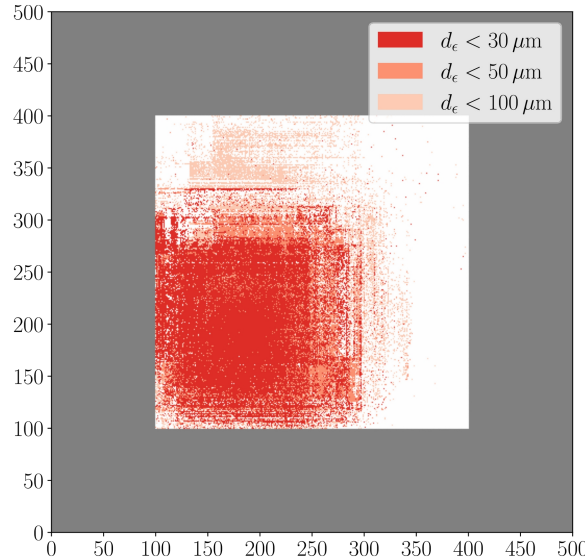


Results – Langer ICR HH 250-75

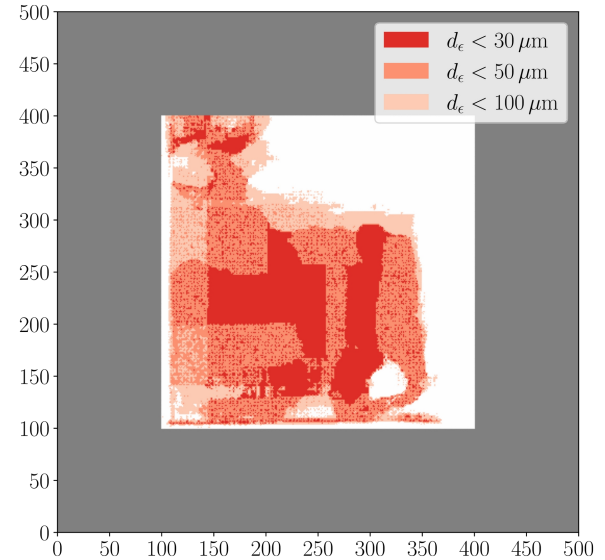
Size of I: 200x200 Positions



CC



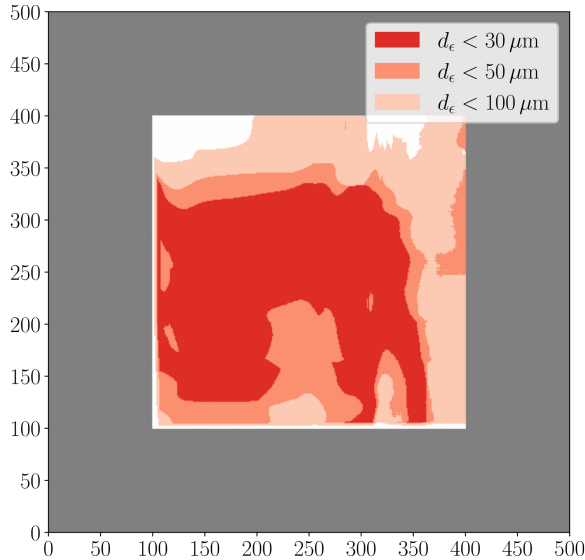
ORB



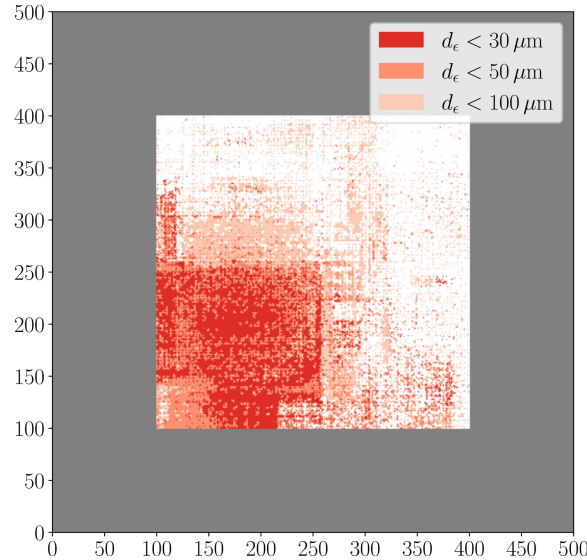
PF

Results – Langer ICR HH 150-75

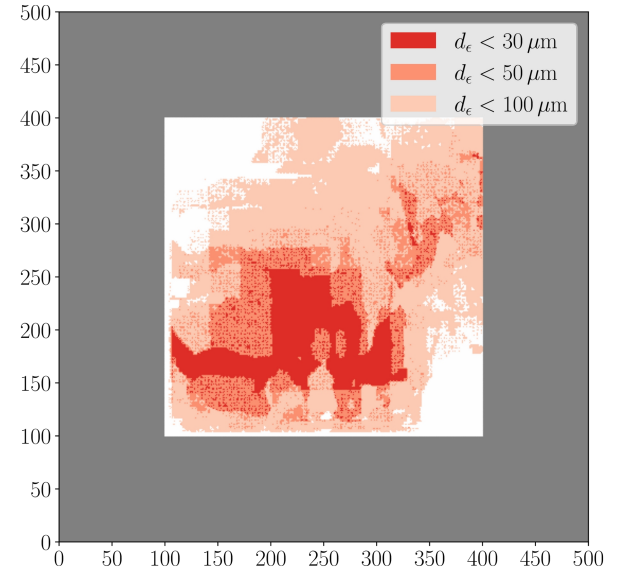
Size of I: 200x200 Positions



CC



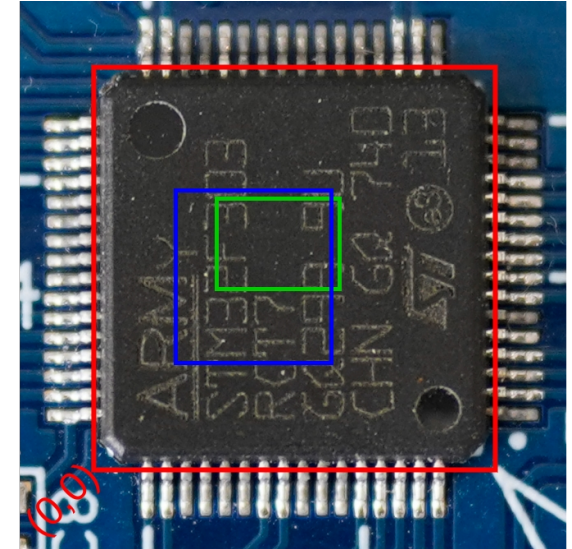
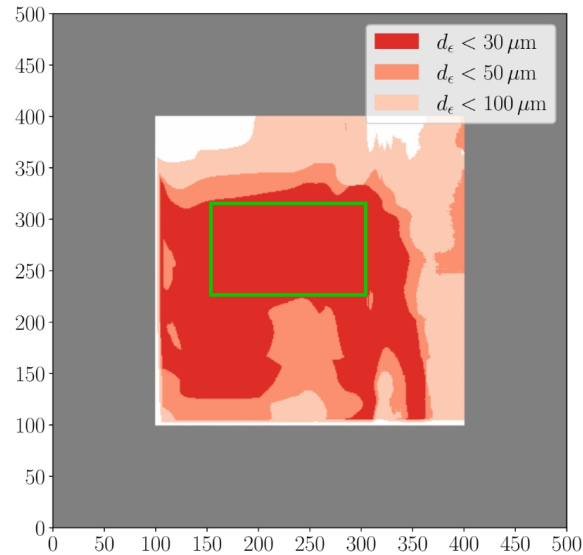
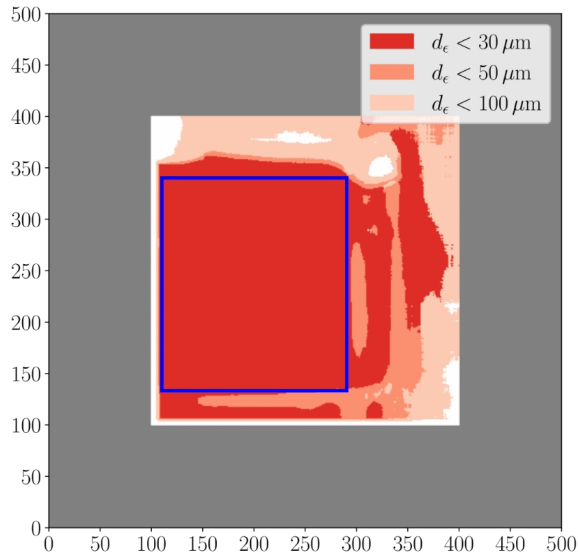
ORB



PF

Results – Conclusion

CC has highest overall accuracy → Best suitable



Conclusion

We present a fast and reliable repositioning methodology

- Precision at least **30 μ m or higher** in large areas for CC
- Compared to Richter et al., we gain a speed-up of about **x3** for initial repositioning (**x28** for each next positioning) with similar accuracy

The methodology is open for different positioning algorithms and is tested with multiple probes

Code available: <https://gitlab.lrz.de/tueisec/probenav>



Thank you for your Attention!

matthias.probst@tum.de

<https://www.sec.ei.tum.de>