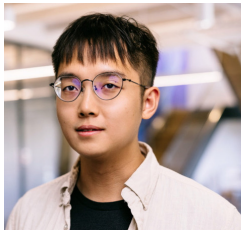
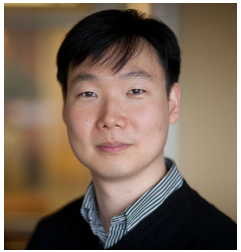
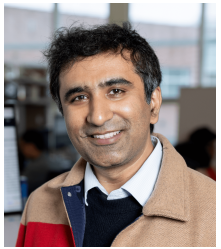
Privatar

Enabling Privacy-preserving Real-time Multi-user VR through Secure Outsourcing



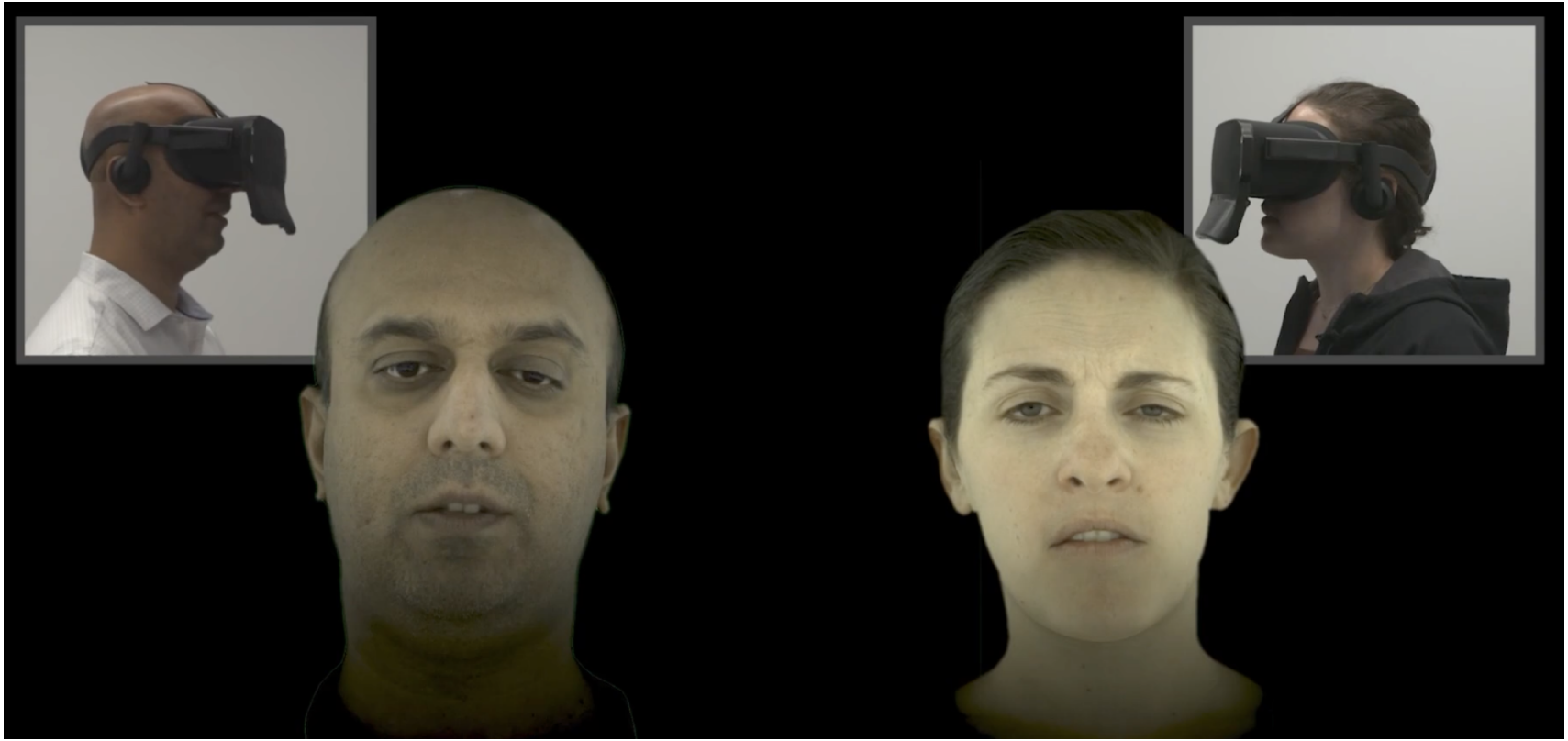




Jianming Tong†, Hanshen Xiao*, Krishnakumar Nair+, Hao Kang†, Ziqi Zhang-
Ashish Sirasao&, G. Edward Suh‡ and **Tushar Krishna†**
MIT(*), Google(+), UIUC(-), AMD(&), Cornell University/NVIDIA(‡)
Georgia Institute of Technology(†)
jianming.tong@gatech.edu

Outlines

- Background and Motivation
- Challenge
- Privatar: Secure Avatar Reconstruction Offloading
- Evaluation
- Conclusion

Application: VR Enables Photorealistic Chat

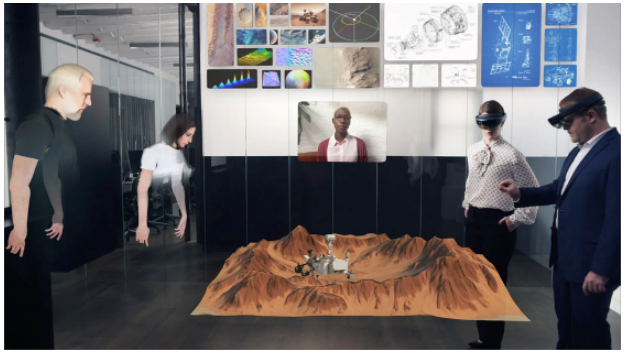


VR Enables Geographically Disjointed Users to communicate.

Application: Realistic VR requires many users!

VR Concert

VR Football Game



Virtual Meeting

Render (>10) Multiple Avatars

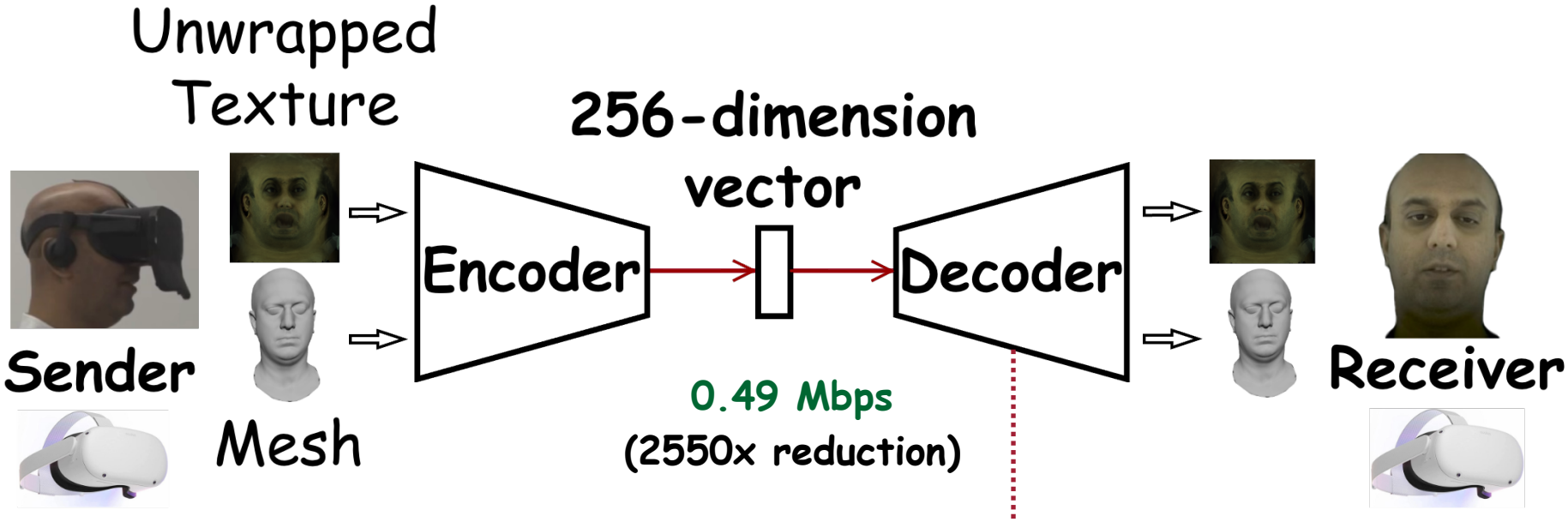
Exceed the Compute Capacity of a single VR headset

This Talk: Secure Avatar Reconstruction Outsourcing!

Outlines

- Background and Motivation
- Challenge
- Privatar: Secure Avatar Reconstruction Offloading
- Evaluation
- Conclusion

Problem: Limited Compute for Multi-user VR



Compute Bottleneck: 364 GFlops per user

902 GFlops Max Throughput

Problem: only Support <= 2 Users

How to securely outsource avatar reconstruction other devices?

Challenge: Private Data Needs Secure Outsourcing

Unwrapped Texture

Sender

Mesh

Private Data

User Identity, Expression and Emotion

Directly Outsourcing leaks privacy

Challenge 1: Where to outsource?

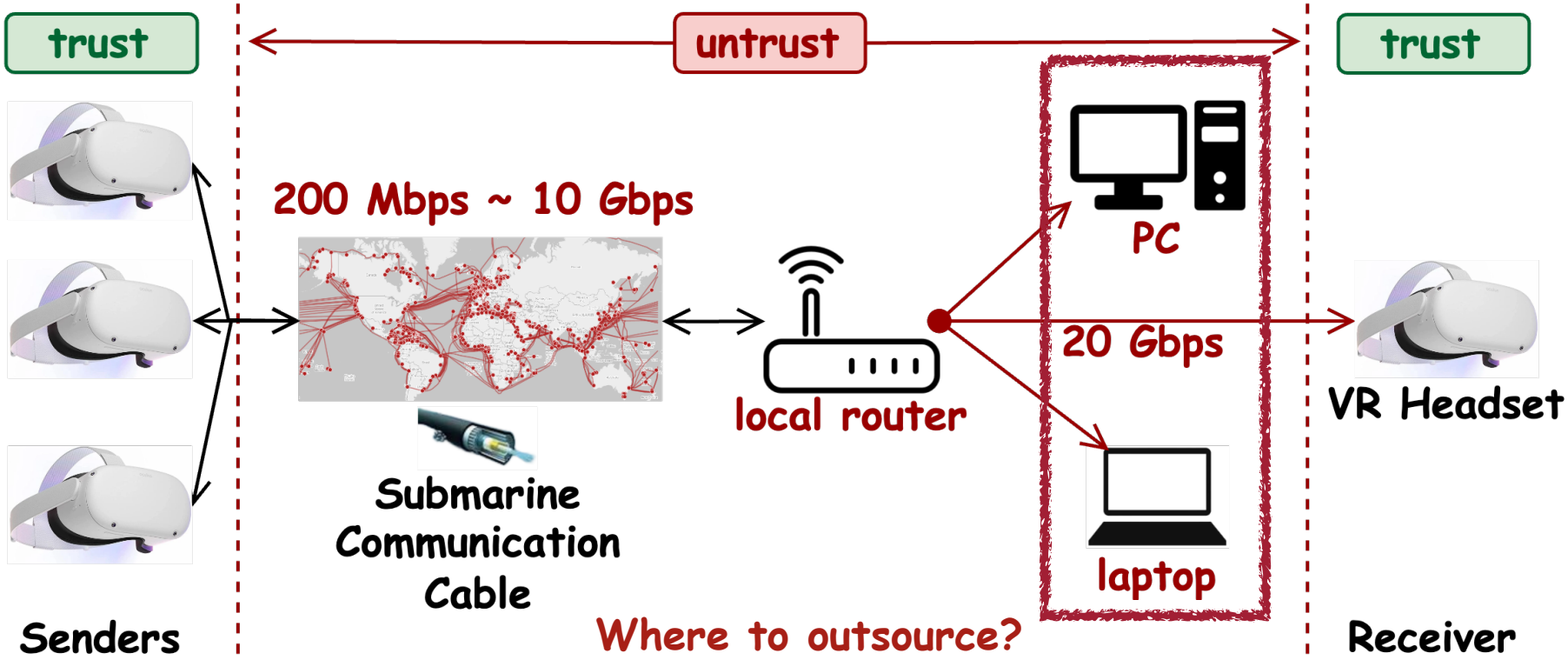
Challenge 2: What data to outsource?

Challenge 3: How to ensure privacy?

Outlines

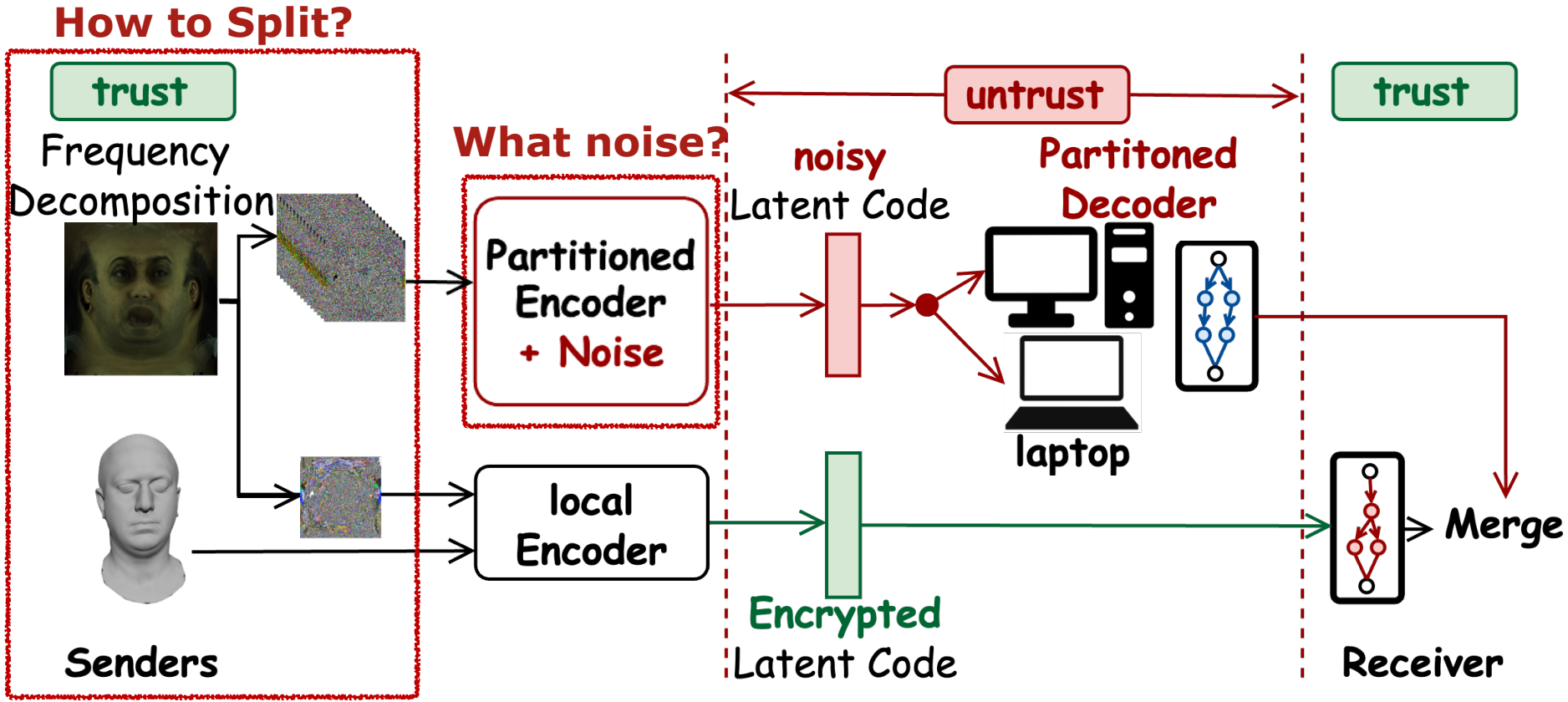
- Background and Motivation
- Challenge
- Privatar: Secure Avatar Reconstruction Offloading
  - Overview: Partially Outsource to Untrusted Devices
  - How to Split Data? Horizontal Partitioning
  - What Noise? Distribution-Aware Minimal Perturbation
- Evaluation
- Conclusion

Threat Model and VR System Setup



Untrusted Devices Connected to Local Router (PC, Laptop)

Secure Offloading Partitioned Model and Input



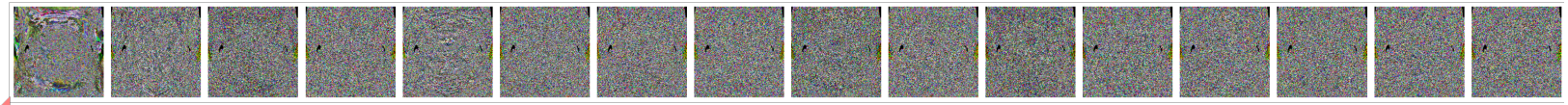
Horizontally Partitions Input and Model and Offloaded One Part

Outlines

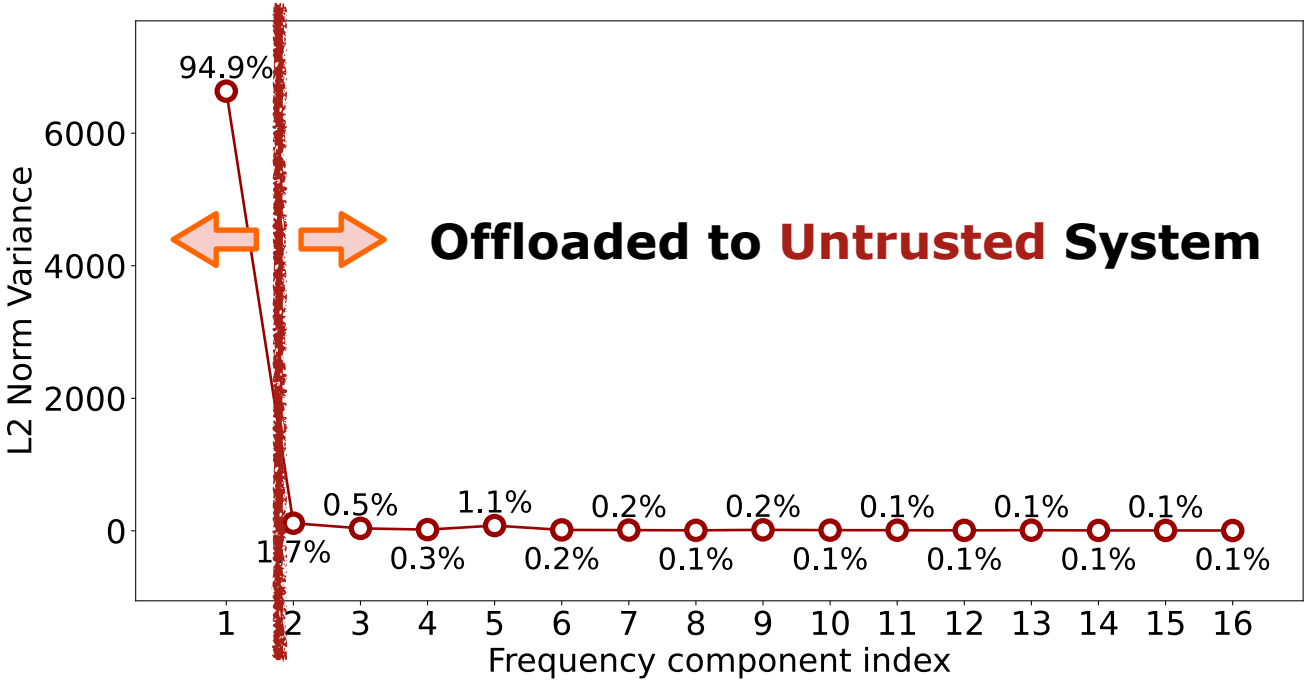
- Background and Motivation
- Challenge
- Privatar: Secure Avatar Reconstruction Offloading
  - Overview: Partially Outsource to Untrusted Device
  - How to Split Data? Horizontal Partitioning
  - What Noise? Distribution-Aware Minimal Perturbation
- Evaluation
- Conclusion

Frequency Splitter: Energy based Partition

Unwrapped Texture (X)



Local Processing



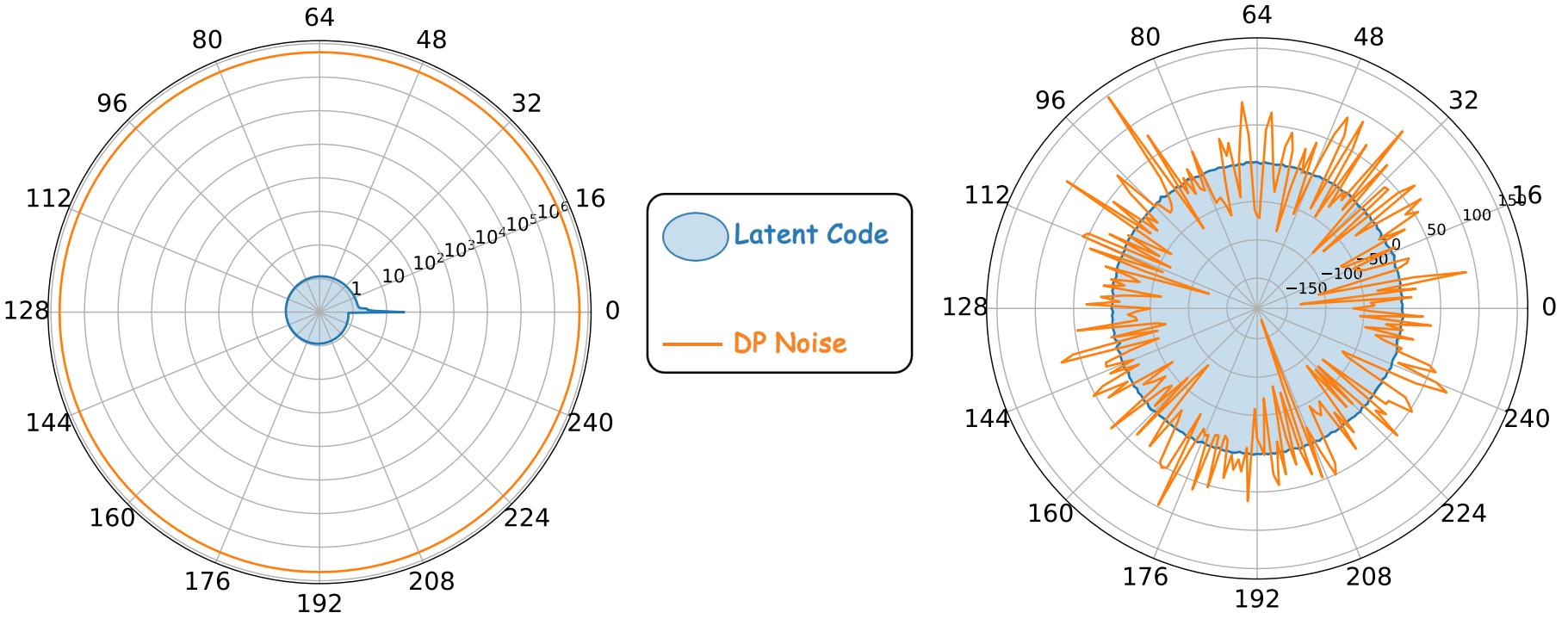
Offloaded to Untrusted System

Outlines

- Background and Motivation
- Challenge
- Privatar: Secure Avatar Reconstruction Offloading
  - Overview: Partially Outsource to Untrusted Device
  - How to Split Data? Horizontal Partitioning
  - What Noise? Distribution-Aware Minimal Perturbation
- Evaluation
- Conclusion

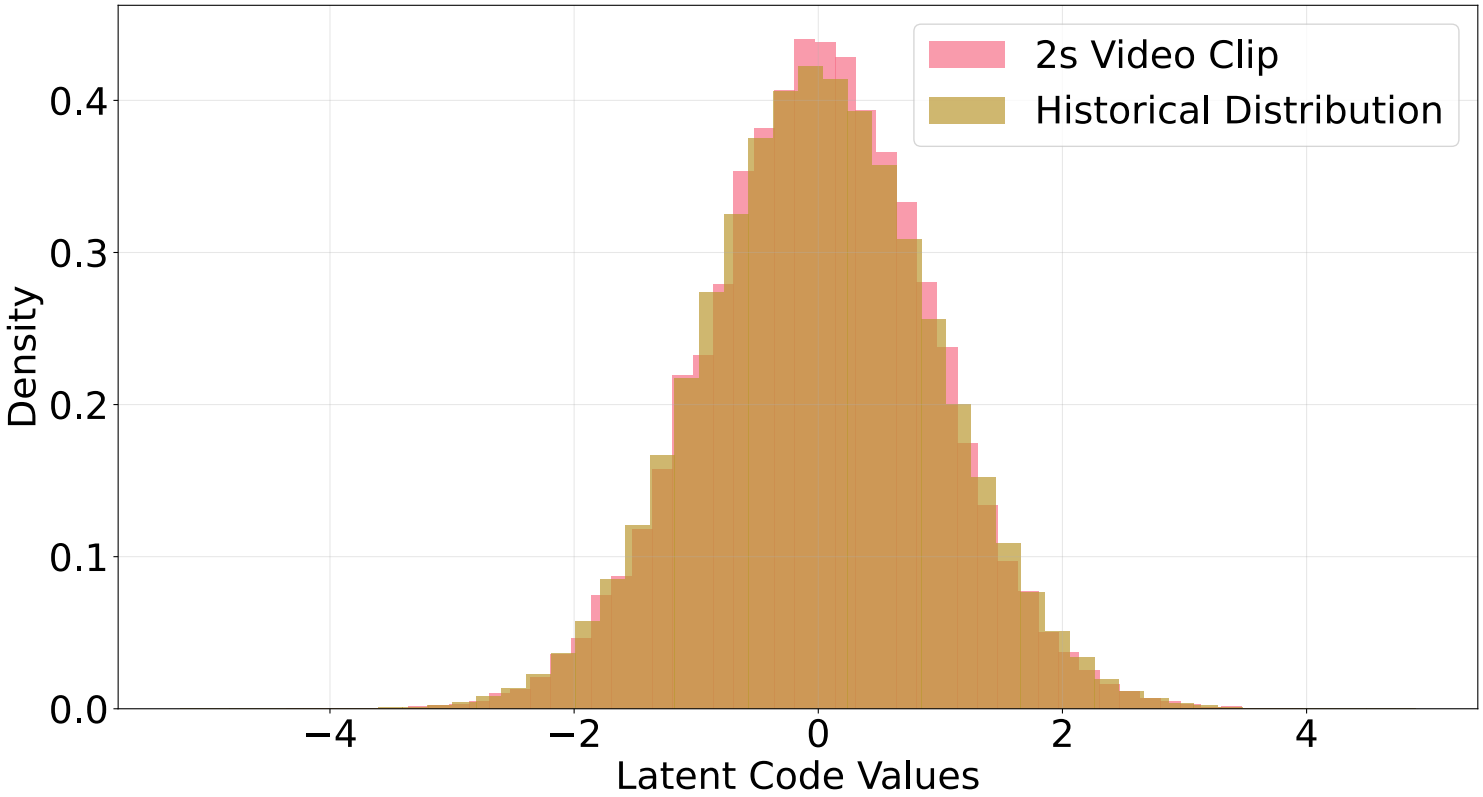
Adding Noise for Provable Privacy Guarantee

For 256D Tensor, Differential Privacy (DP) gives Worst-Case Protection



Ignores Dimensional Differences — But VR Data Not Hit Worst Case

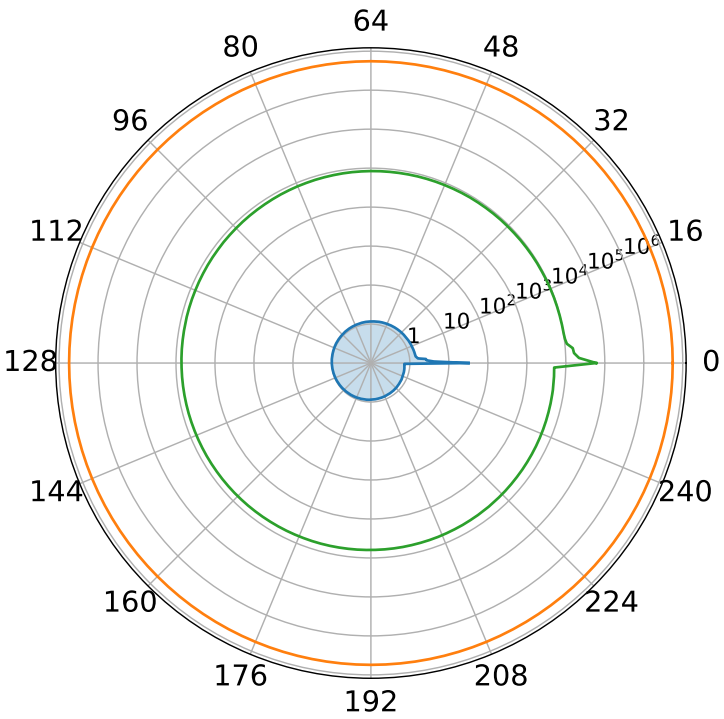
Observation: Slow Statistical Distribution Drifting

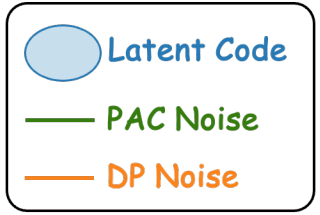


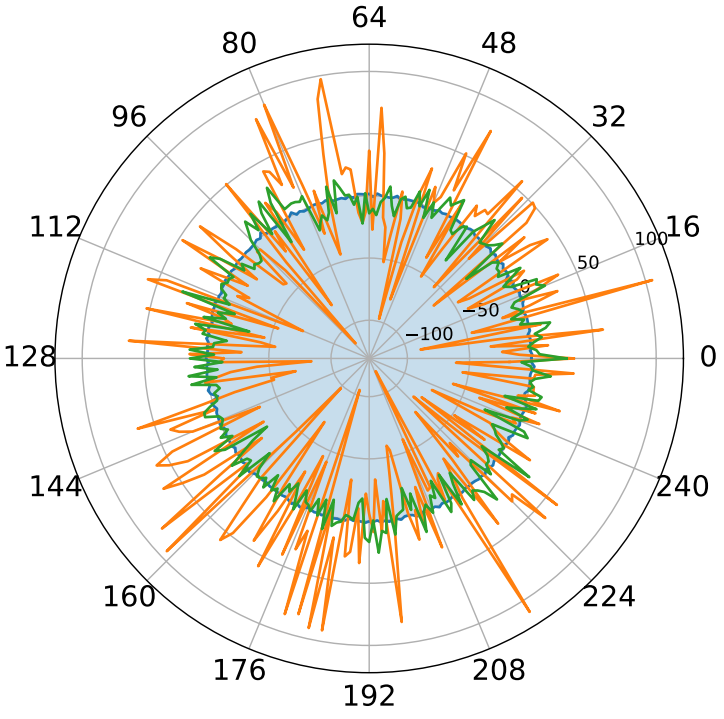
We Could Add Statistical Distribution into Noise Determination!

Adding Noise for Provable Privacy Guarantee

Leverage Statistic Data Distribution to Provable Minimize Noise





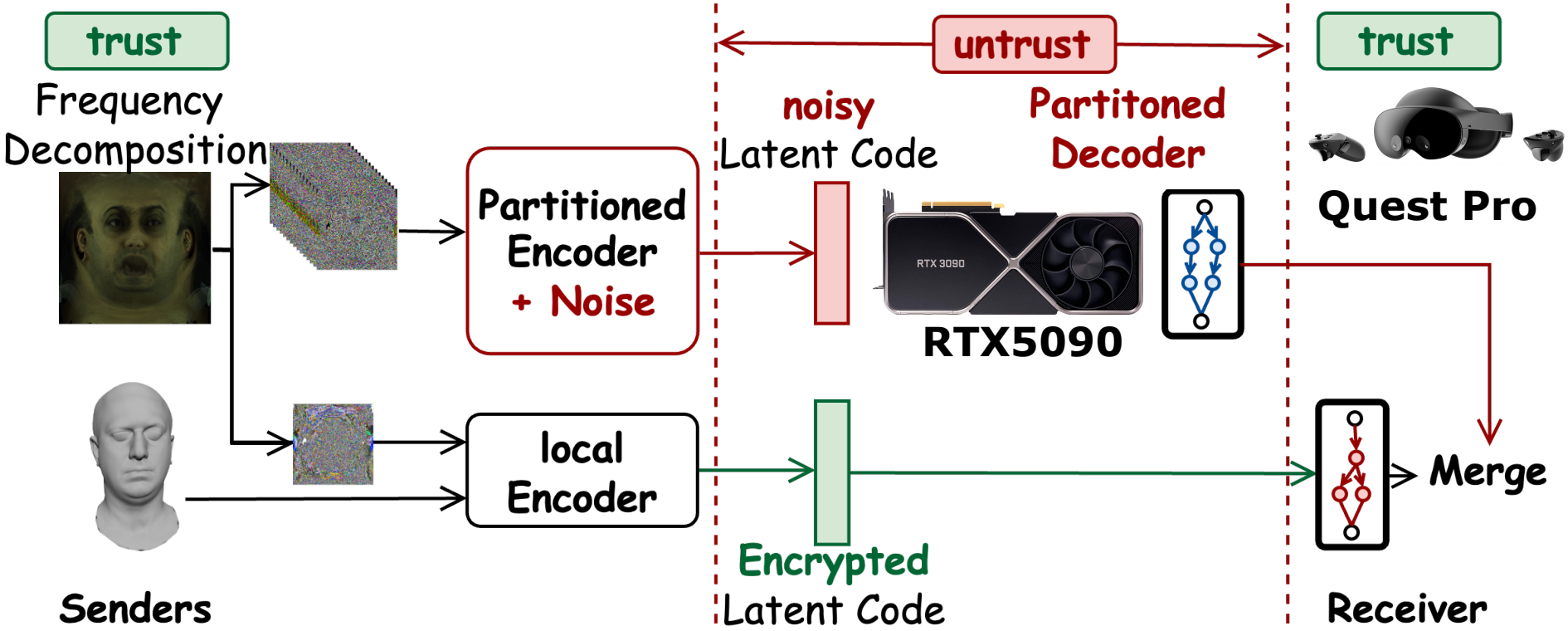


Statistical Distribution **Random One Data Sample**

Outlines

- Background and Motivation
- Challenge
- Privatar: Secure Avatar Reconstruction Offloading
  - Overview: Partially Outsource to Untrusted Device
  - How to Split Data? Horizontal Partitioning
  - What Noise? Distribution-Aware Minimal Perturbation
- Evaluation
- Conclusion

Evaluation Setup

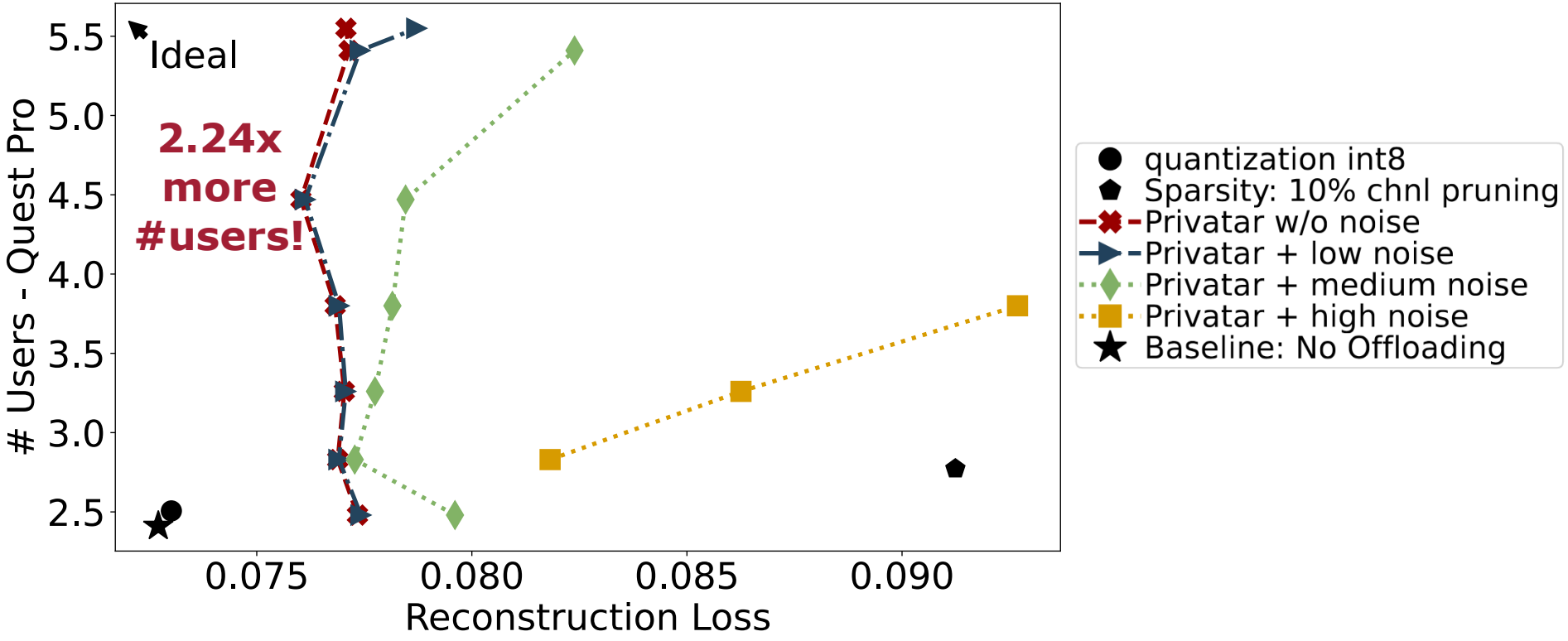


Real Deployed on RTX 5090 and Estimated on Quest Pro

Evaluation: Negligible Quality Loss from Truth

(a) Truth (b) Baseline (c) FO (d) Quantize (e) Sparsity (f) PRIVATAR

Privatar: SotA #user-Accuracy Pareto Frontier



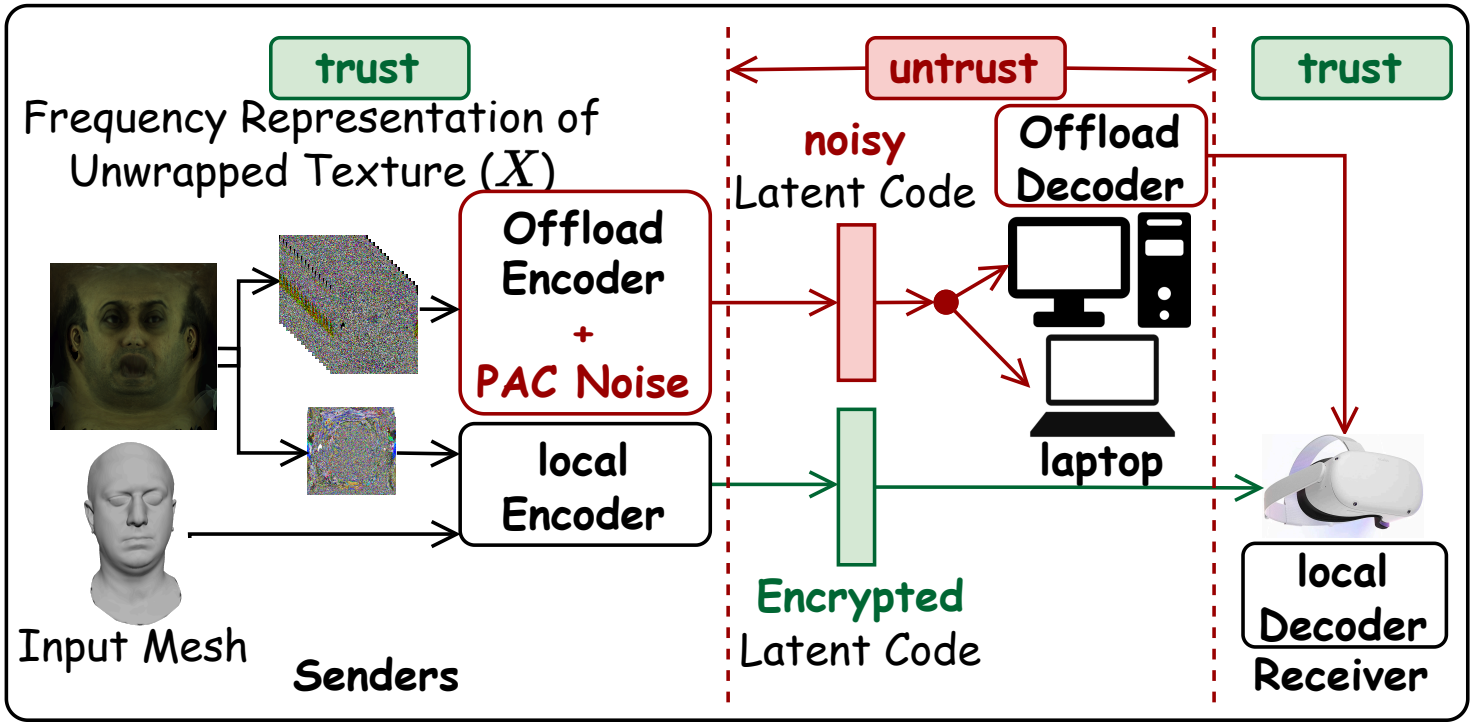
Privatar Offers SoTA #user-Accuracy Pareto-Frontier Curve

jianming.tong@gatech.edu

Outlines

- Background and Motivation
- Challenge
- Privatar: Secure Avatar Reconstruction Offloading
  - Overview: Partially Outsource to Untrusted Device
  - How to Split data? Horizontal Partitioning
  - What Noise? Distribution-Aware Minimal Perturbation
- Evaluation
- Conclusion

First Secure Outsourcing Avatar Ceconstruction



Paper

Code

What to split? Horizontal Partitioning

How to secure data? Distribution-Aware Minimal Noise