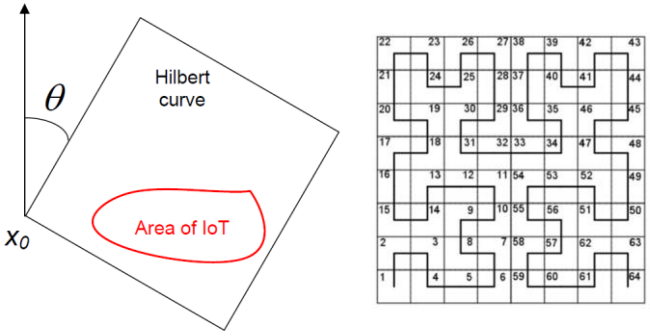
Enabling Privacy-Preserving Routing-on-Context in IoT

AUBURN UNIVERSITY

Challenge:

- In the IoT era, connectivity-based routing is not the best solution for context-oriented IoT traffic
- A new routing primitive that supports efficient IoT routing based on the targeted application context, rather than on connectivity.
- "secure-by-design" privacy preservation of the context information



One-way Hilbet Space Filling Curve Encryption for an IoT network.

Scientific Impact:

- Create better understanding on the security and privacy vulnerabilities of IoT
- Renovate Internet routing paradigm by creating "secure-by-design" context-oriented routing for IoT traffic
- Enable privacy-preserving context-aware computing in IoT

Solution:

- New privacy-preserving context-oriented routing technique based on Hilbert space-filling curve space encryption
- Probabilistic traffic mixer to counter context inference attack
- Federated learning to support privacy-preserving context-aware computing in IoT

Broader Impact and Broader Participation:

- Bring privacy protection to millions of IoT users
- "Secure-by-design" context-driven routing that better fits into tomorrow's IoT industry
- Outreach to under-represented groups
- New curriculum development, recruitment and training of graduate students

CNS-2006998, Auburn University, PI: Tao Shu (tshu@auburn.edu)