PDA: Semantically Secure Time-Series Data Analytics with Dynamic Subgroups

- Background & previous works
  - various needs for sharing data, which contains sensitive info
  - previous works focus on data anonymization
  - restrict the usage of published data
- Design goals
  - Time-series data, Communication & Computation overhead
  - Channel security
  - Privacy-requirement independent accuracy
- this paper, a cryptographic tool PDA:
  - capable for any data analysis based on **polynomial**
  - secure against CPA in Dolev-Yao network model
  - small communication overhead, comparable with the peer works who present ah-hoc solutions specifically.

Preliminaries & Definitions & Achieving

- k-DDH problem, N-th residue, discrete logarithm $\log_{1+N} \pmod{N^2}$, DCR problem
- Lemm2: DDH$\leq_P$ k-DDH
- Setup -> KeyGen -> Encode -> Aggregate
- Correctness of PDA: formalized with prob.
- Security of PDA: Data publishing game
- Construction (more details in the paper)
- **Dynamic User Group**, Examples

Correctness & Security

- **Indistinguishable**: Lemma 6-8
- Theorem 2
- κ controls the actual size of encode value, which didn't explained aforementioned

Related work

- Secure Multi-party Computation
- Perturbation
- Secret-shared Keys
- Secure Multivariate Polynomial Evaluation

Questions & Notes:

- IND-CPA is equivalent to the semantic security under CPA, paper