Mikhail J. Atallah, YounSun Cho, Ashish Kundu

**Goal**

- Design a data authentication server

**Approach**

- **Approach 1**
  - **Purpose of server** is to let users authenticate data organized as an n-cell grid
    - GIS, image, scientific, etc
  - **Server does not have signature key**
    - What the server stores is pre-signed by trusted data owner
    - Hence no compromise of key if server suffers a break-in
  - **Performance metrics**
    - How many signatures are stored in the server *(we achieve O(n))*
    - How many signatures are sent to a user for data authentication *(we achieve O(1))*
    - Time for user to verify signature (~ the number of grid cells in its range)

- **Approach 2**
  - User query is a range of data the user wishes to authenticate
    - User has copy of its range of data only (nothing outside it)
    - Signature cannot involve a cell outside user's range
    - But: for an n-cell grid there are n² possible ranges
    - Too many: cannot afford to pre-store a signature for each

**The signer previously distributed integrity verification (IV) items to the untrusted data authentication server**

**Request IV of a subset of data**

**IV corresponding to the requested subset of data**