CERIAS

the center for education and research in information assurance and security

Third-Party Grid-Data Integrity Verification

Mikhail J. Atallah, YounSun Cho, Ashish Kundu

Goal

Design a data authentication server

- ❖ **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

Approach1

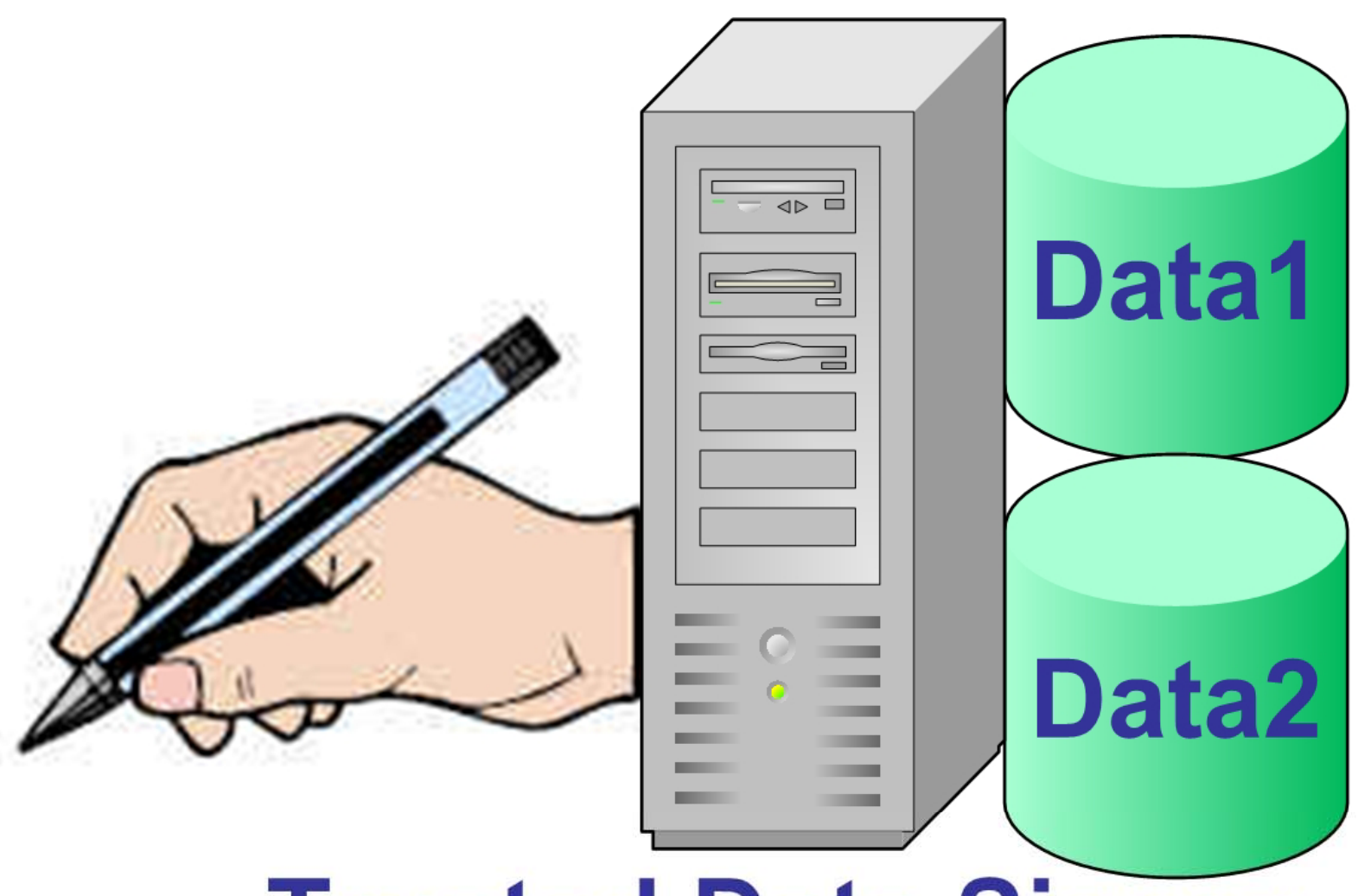
- ❖ **Store signatures of a linear number of judiciously chosen "canonical" subsets of the data,**
  - ◆ such that any of the n^2 possible user ranges consists of the union of a small number of canonical subsets of the n-cell grid.

Approach2

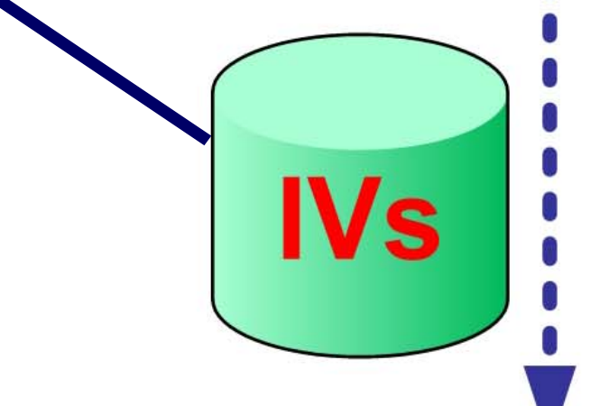
- ❖ **Use bilinear maps and aggregate signatures**.
  - ◆ Aggregation of existing signatures done by server

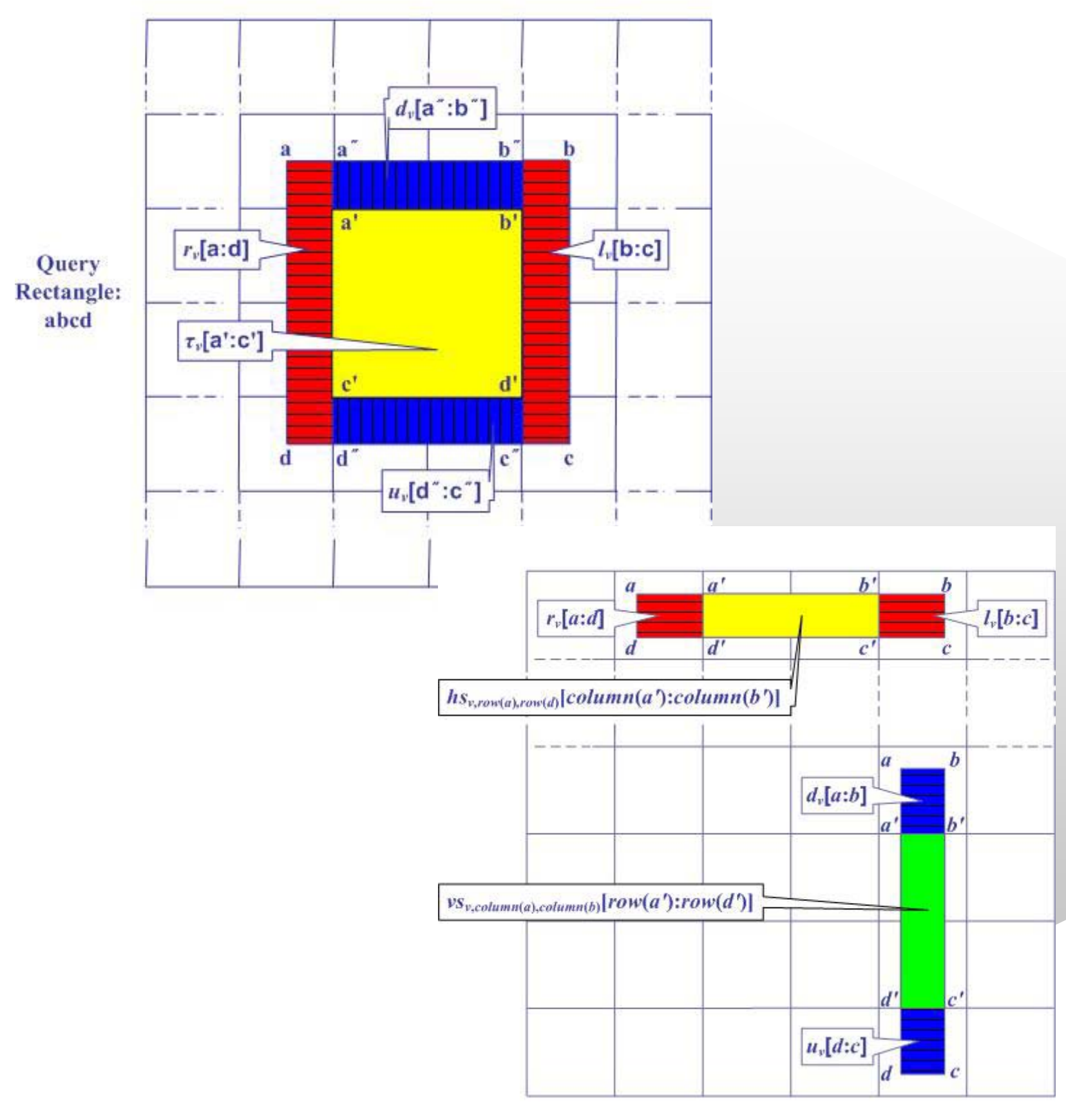
- ❖ **User query is a range of data the user wishes to authenticate**
  - ◆ User has copy of its range of data only (nothing outside it)
    - • Signature cannot involve a cell outside user's range
  - ◆ **But**: for an n-cell grid there are n^2 possible ranges
    - • Too many: cannot afford to pre-store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

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

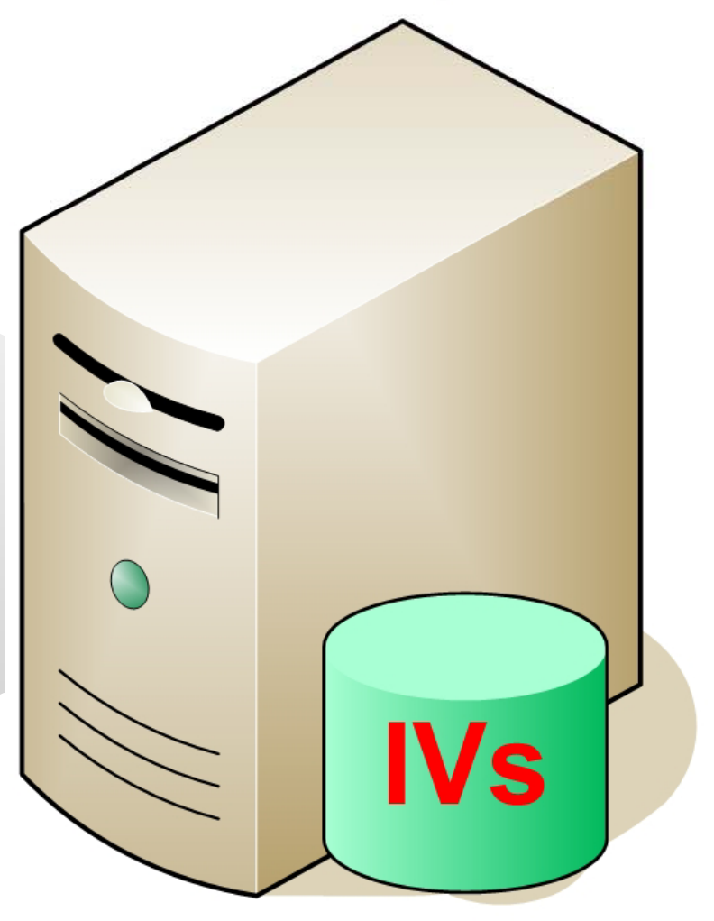


Trusted Data Signer





Query processing for 2D data structure



Untrusted Data Authentication Server

Request IV of a subset of data

IV correspoding to the resquested subset of data

User