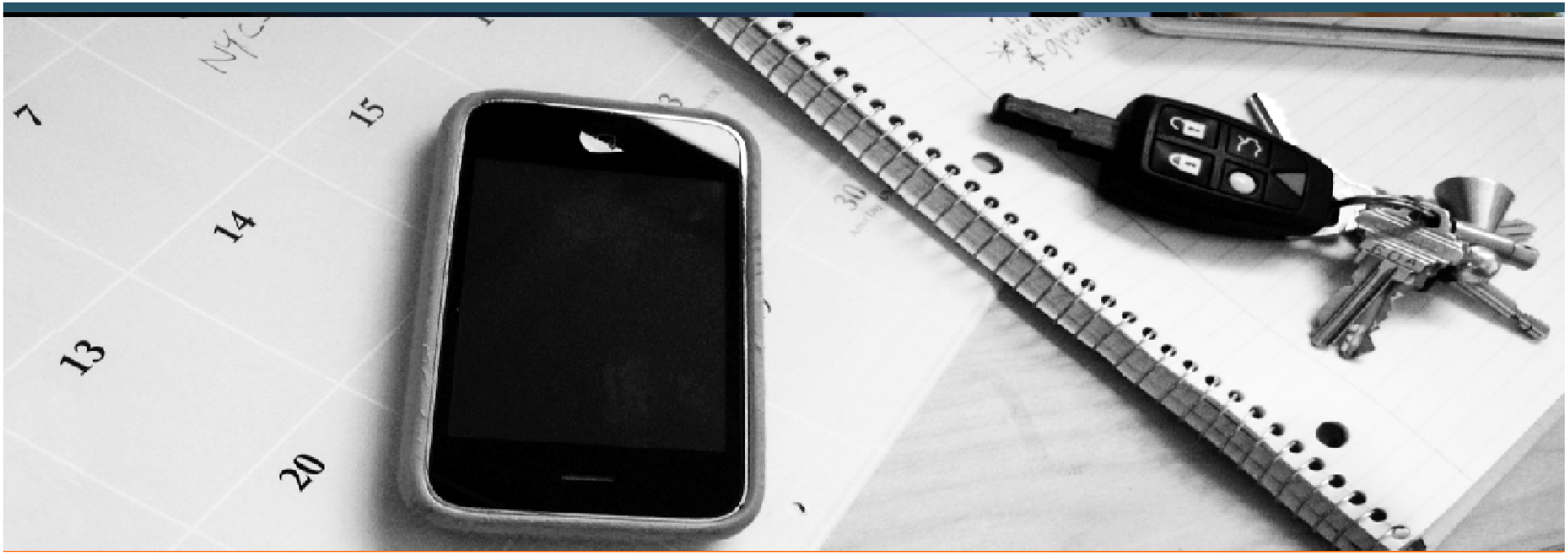
parc
A Xerox Company

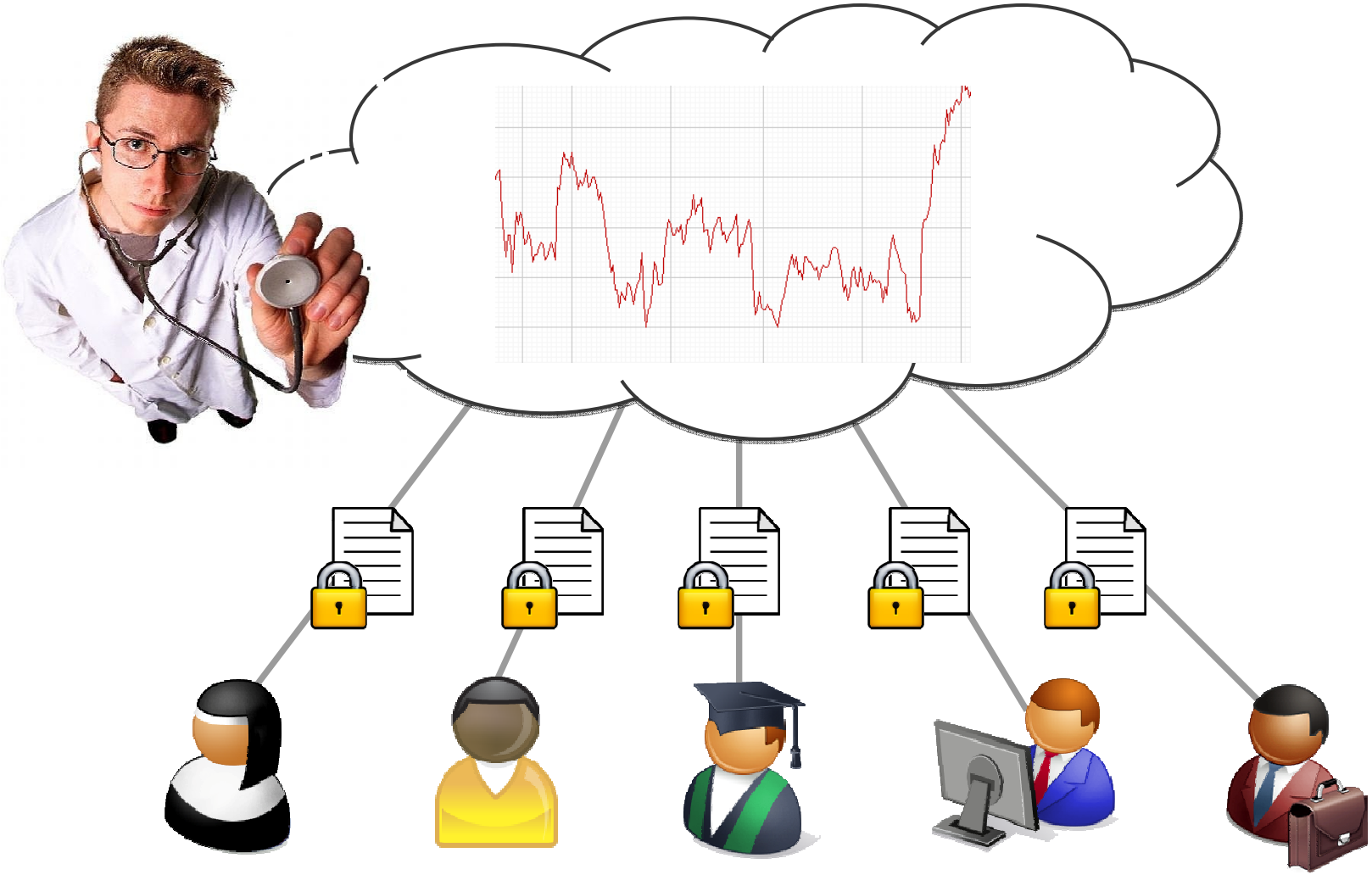
Privacy-Preserving Stream Aggregation

Elaine Shi (PARC/UC Berkeley), T-H. Hubert Chan (HKU),
Eleanor Rieffel (FXPal), Richard Chow (PARC), Dawn Song (UC Berkeley)



Privacy in Smart Grids

Privacy in Population Surveys



How can we allow a data aggregator to perform data analytics, while preserving individual privacy?

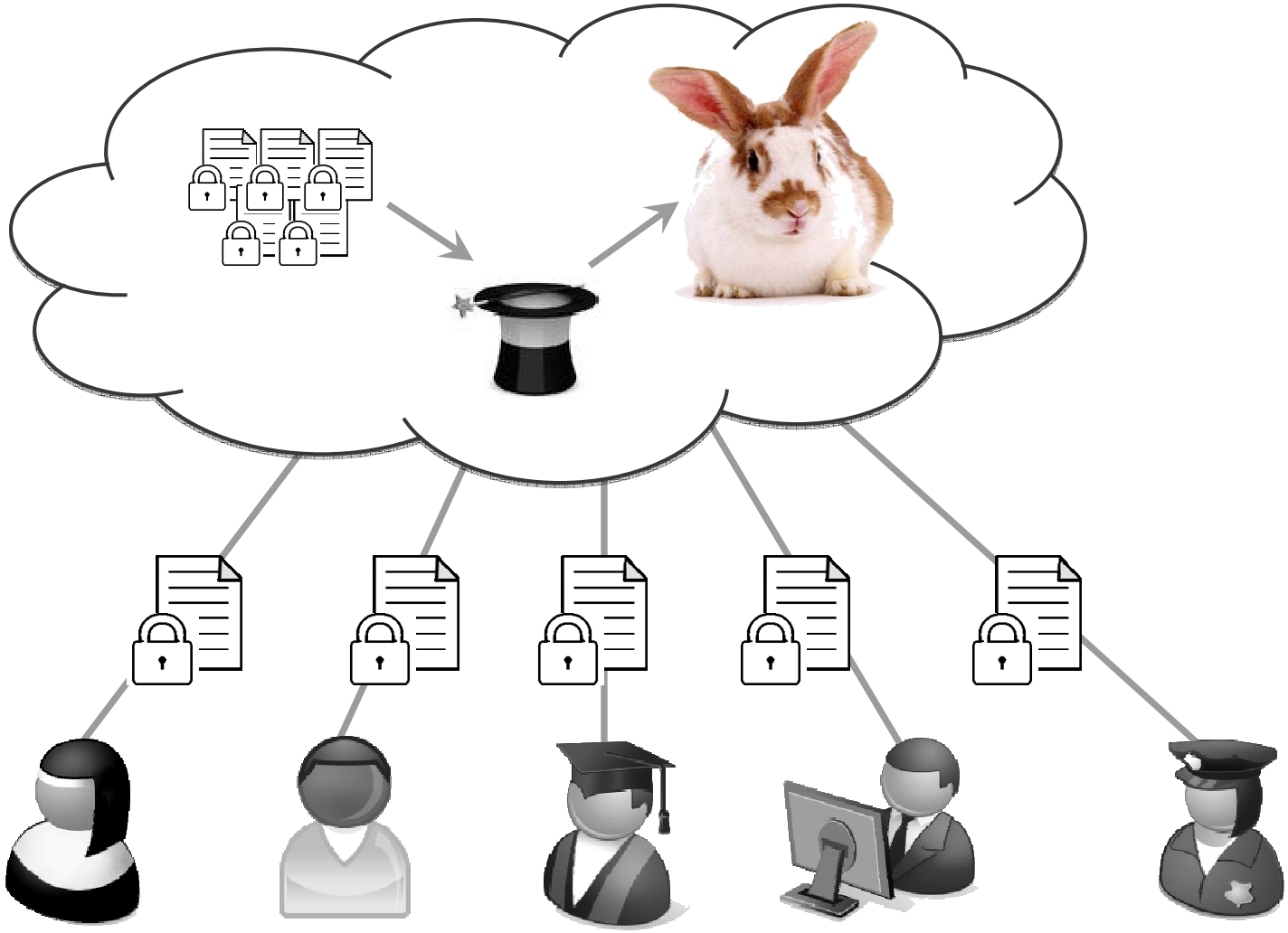
Our Results – Privacy Notion

Encryption Scheme → Aggregator Obliviousness

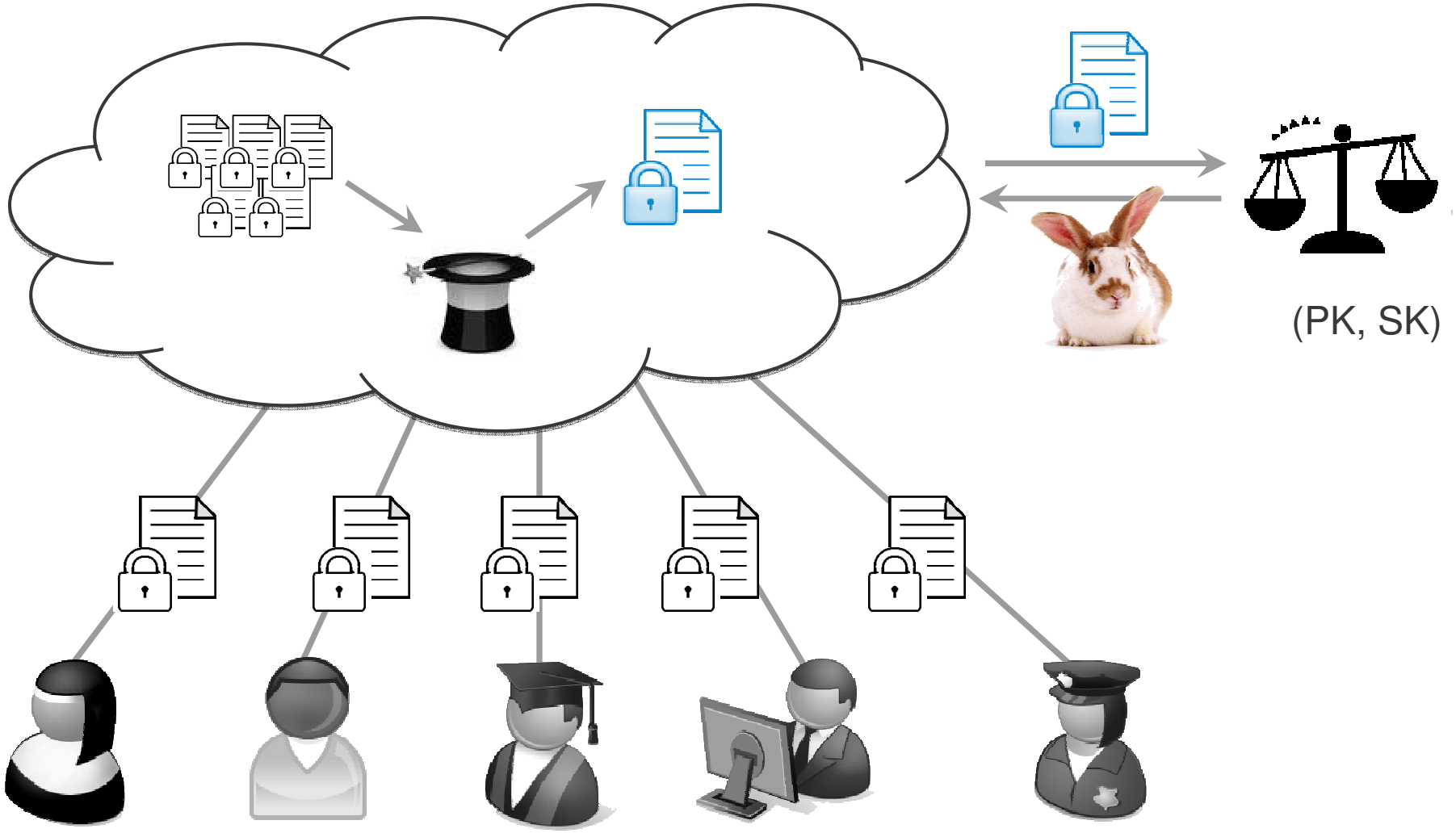
(Aggregator learns only desired statistic, and nothing else)

Distributed Noise Generation → Differential privacy against an untrusted aggregator

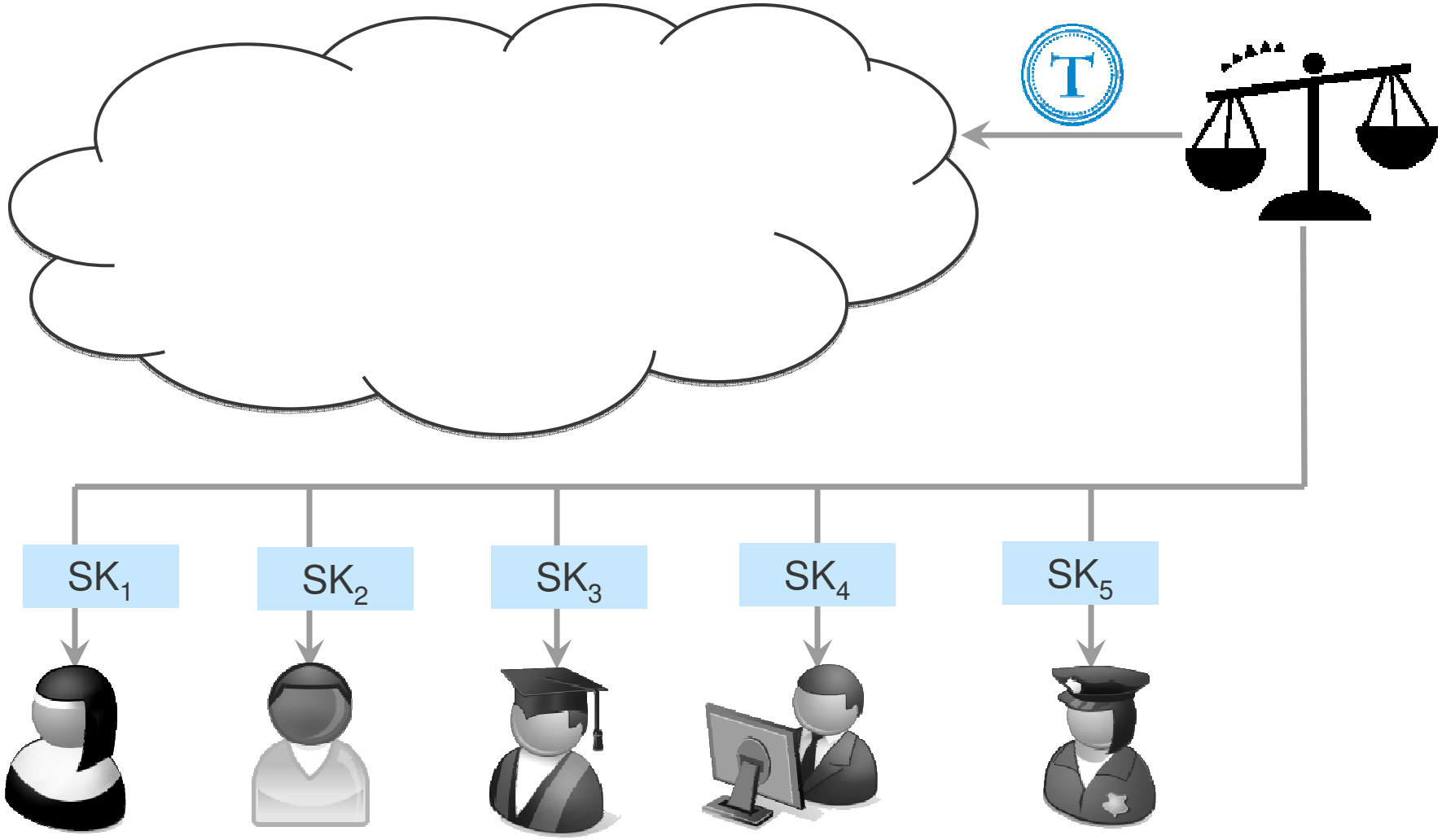
Computing on Multiple Users' Encrypted Data



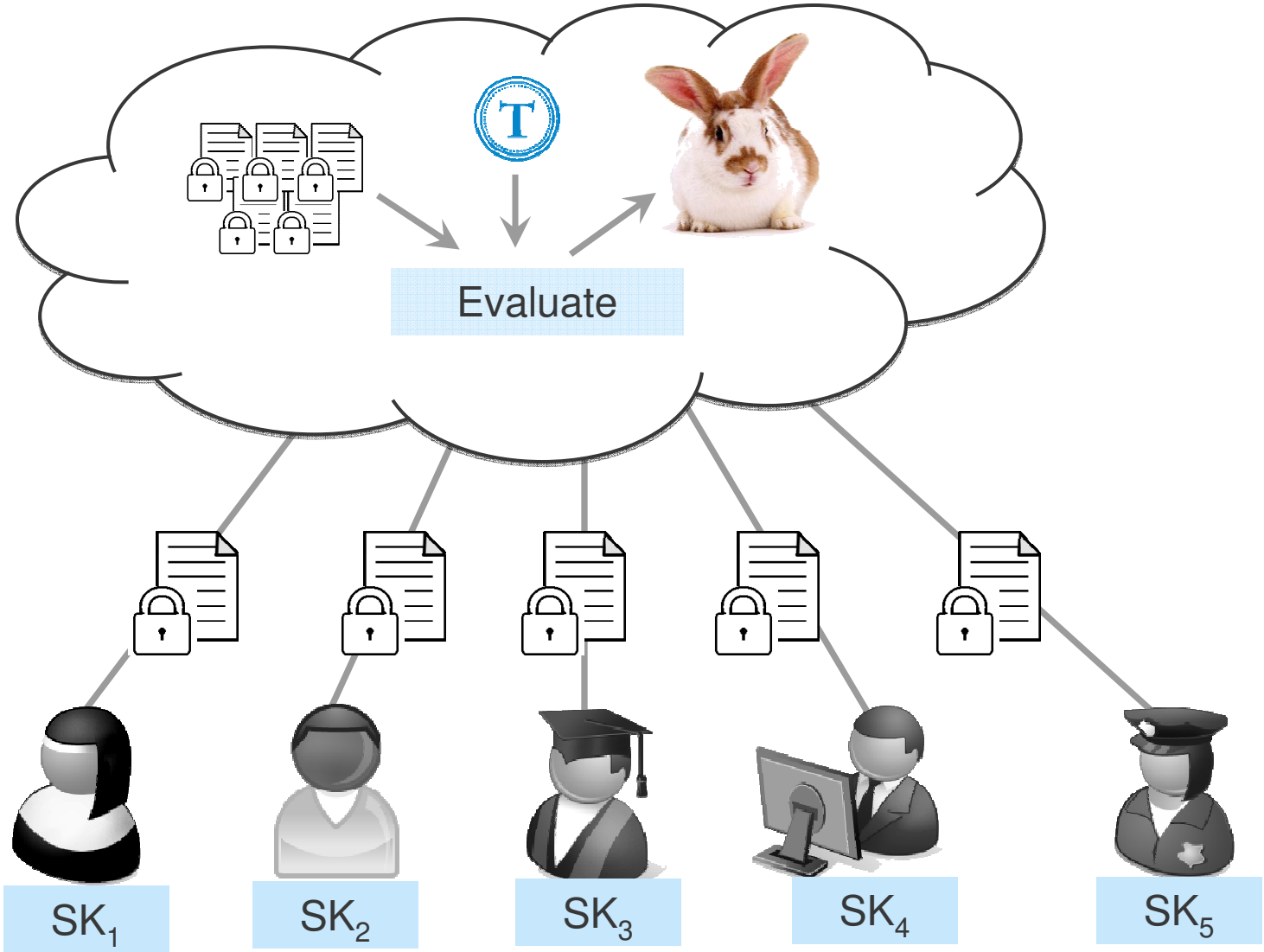
Homomorphic Encryption?



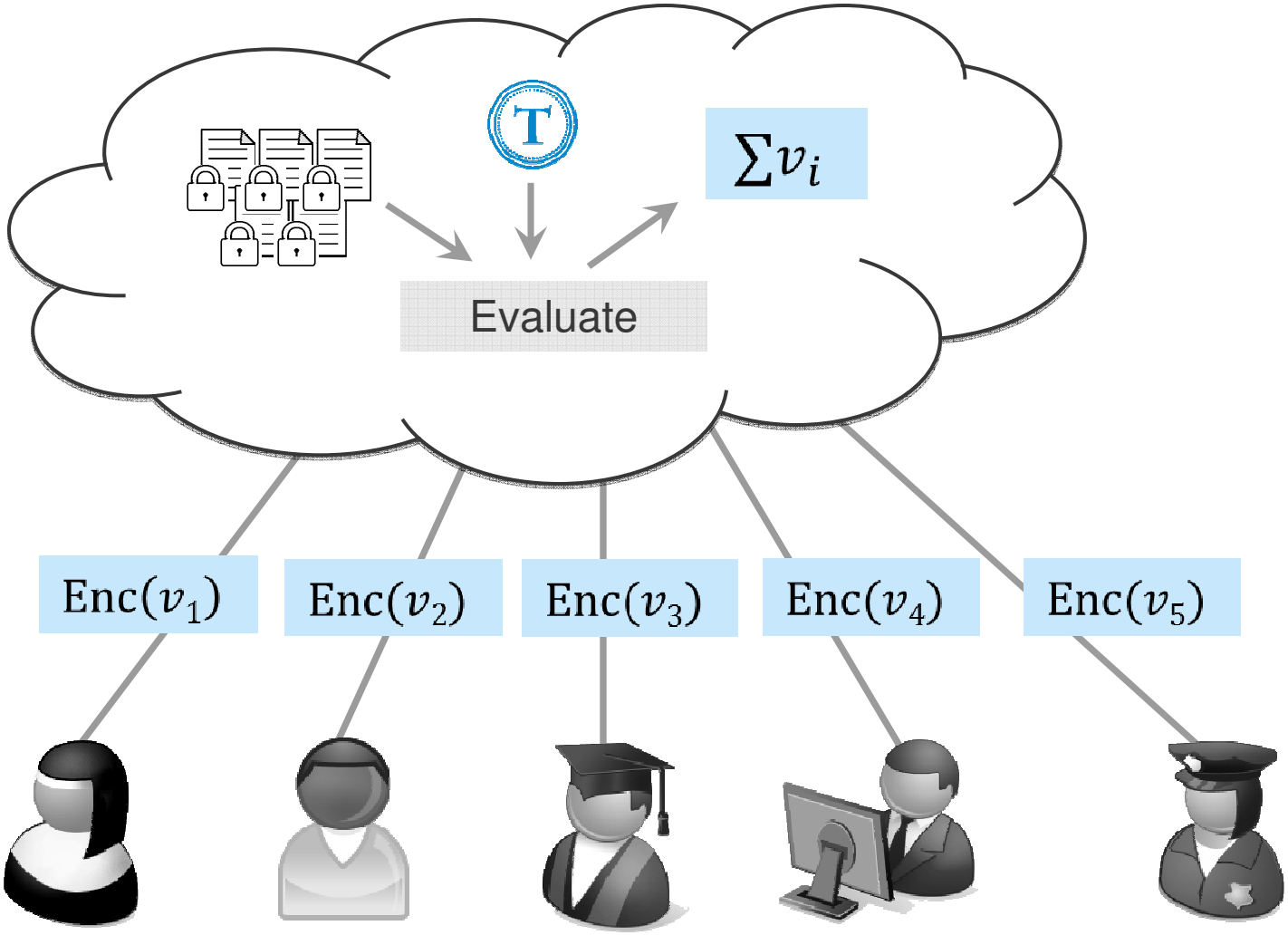
New Paradigm



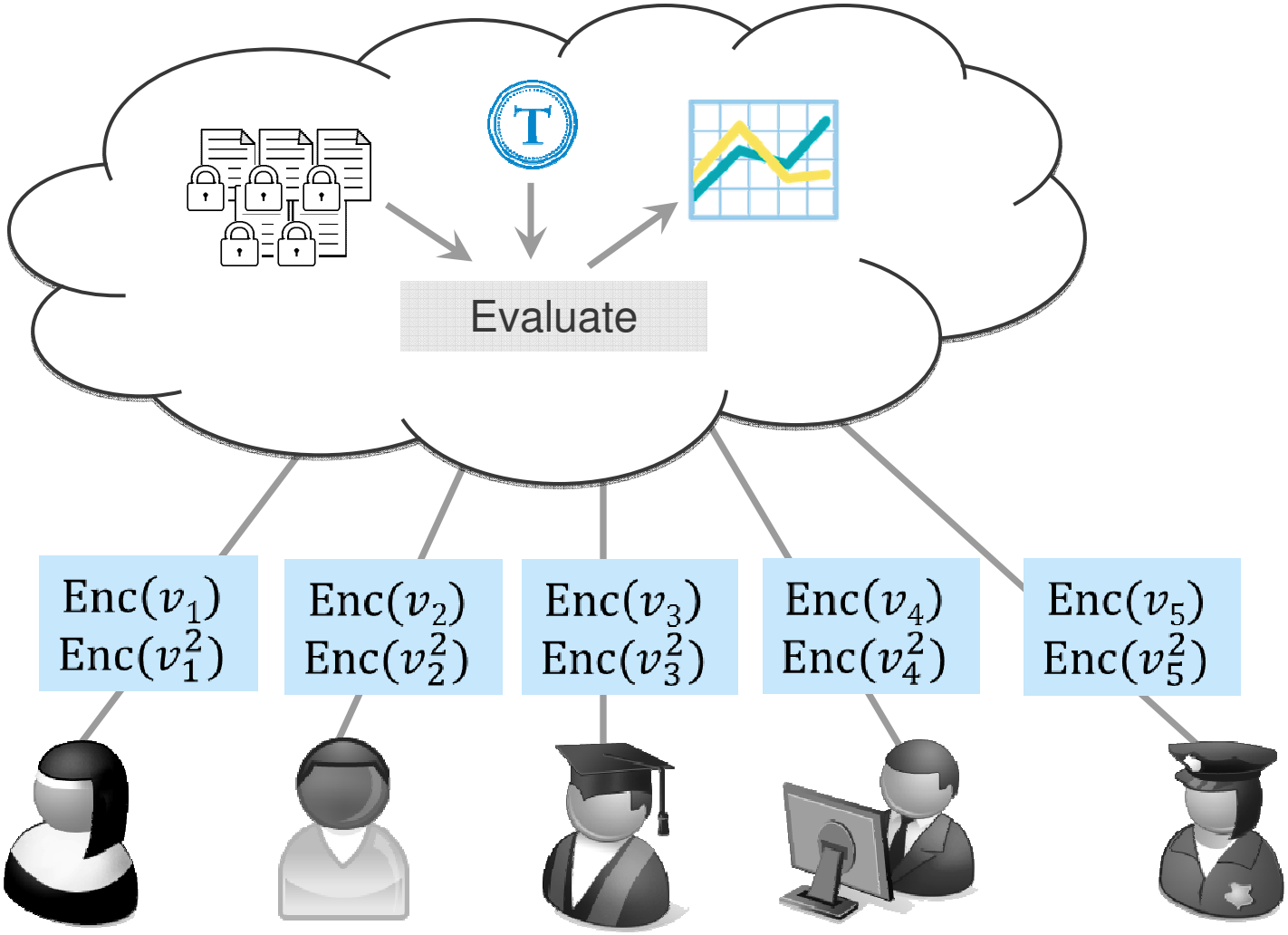
New Paradigm



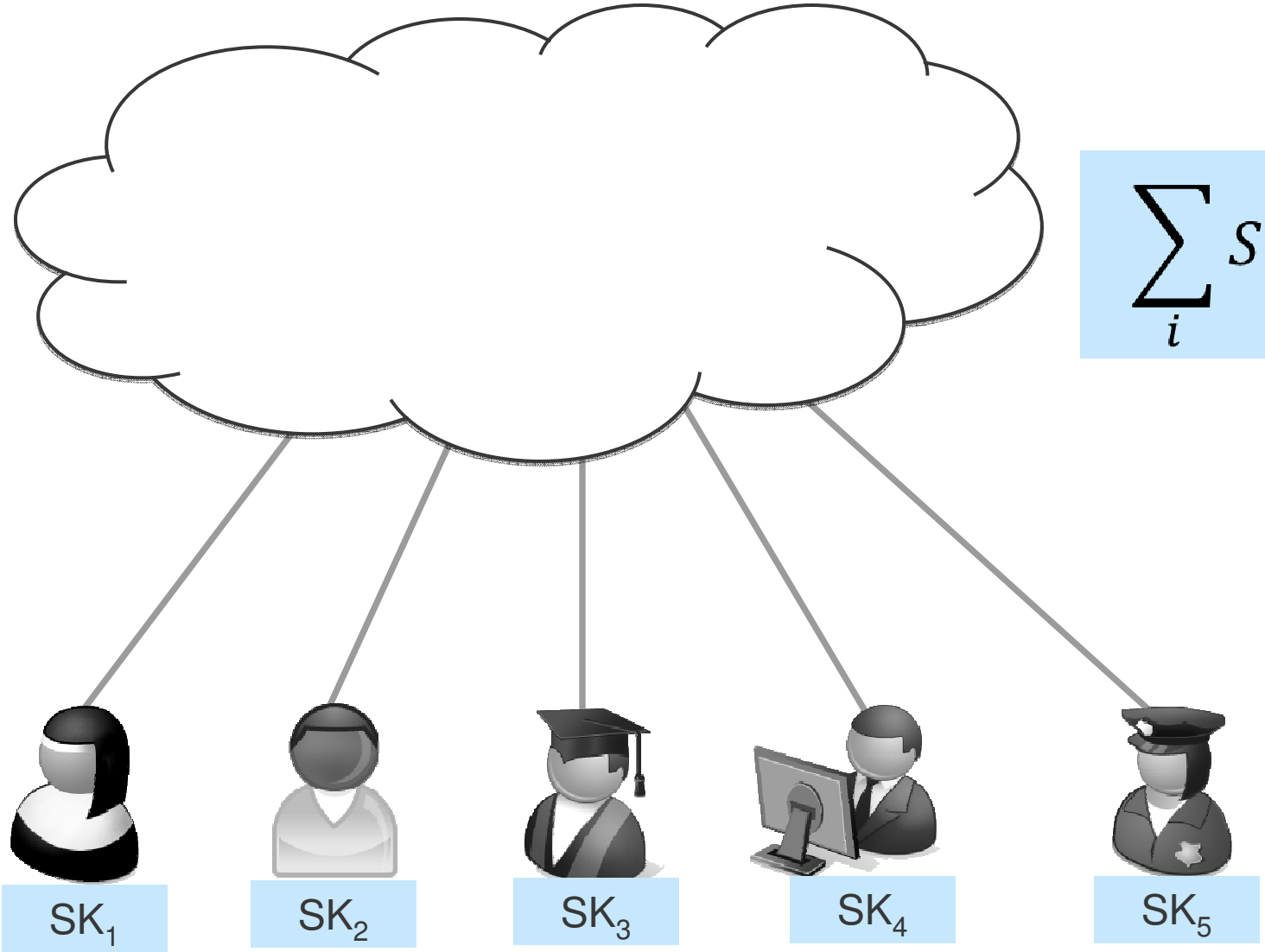
Expressiveness: Summation



Expressiveness: Distributions

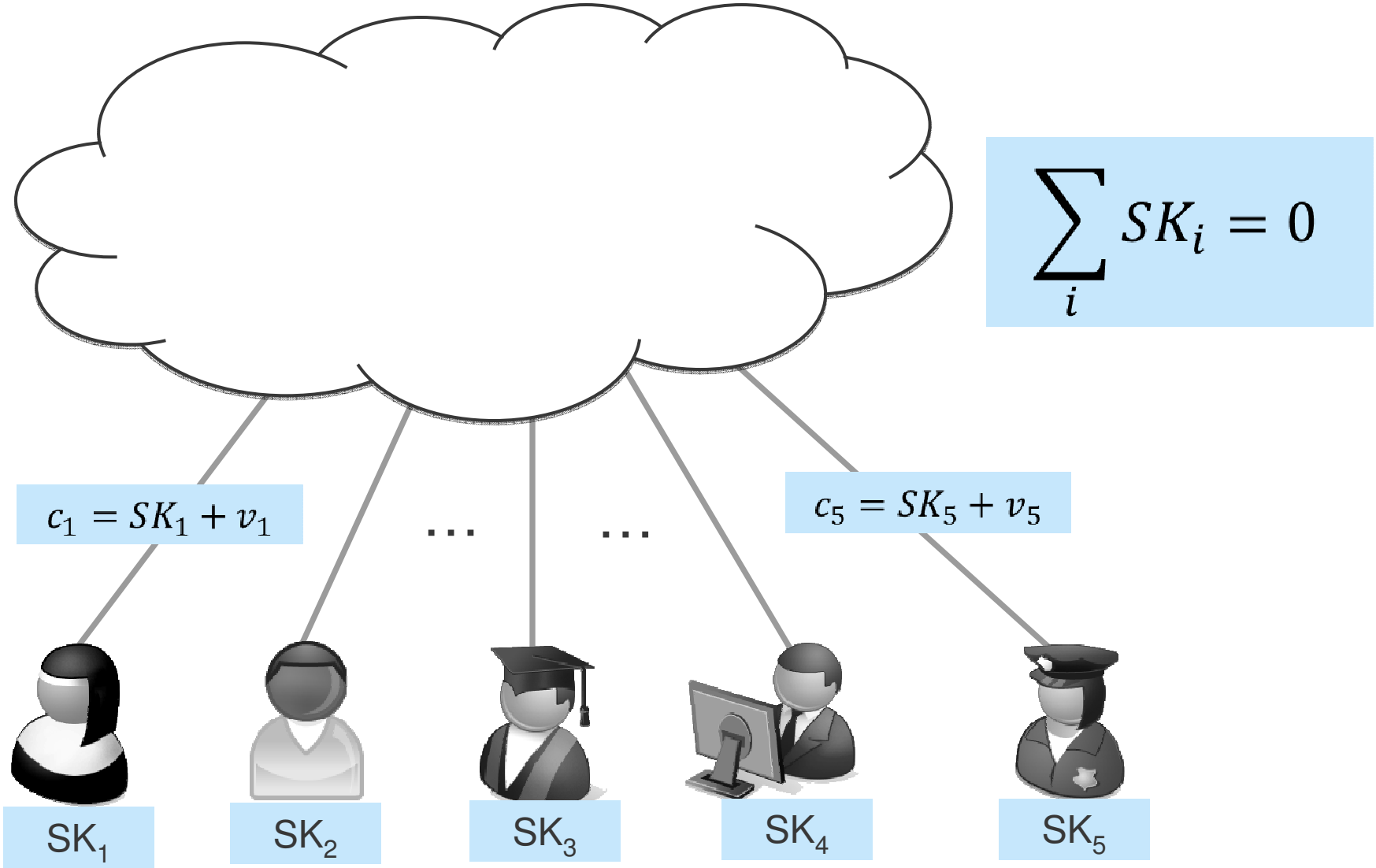


Aggregate Once: Simple Construction

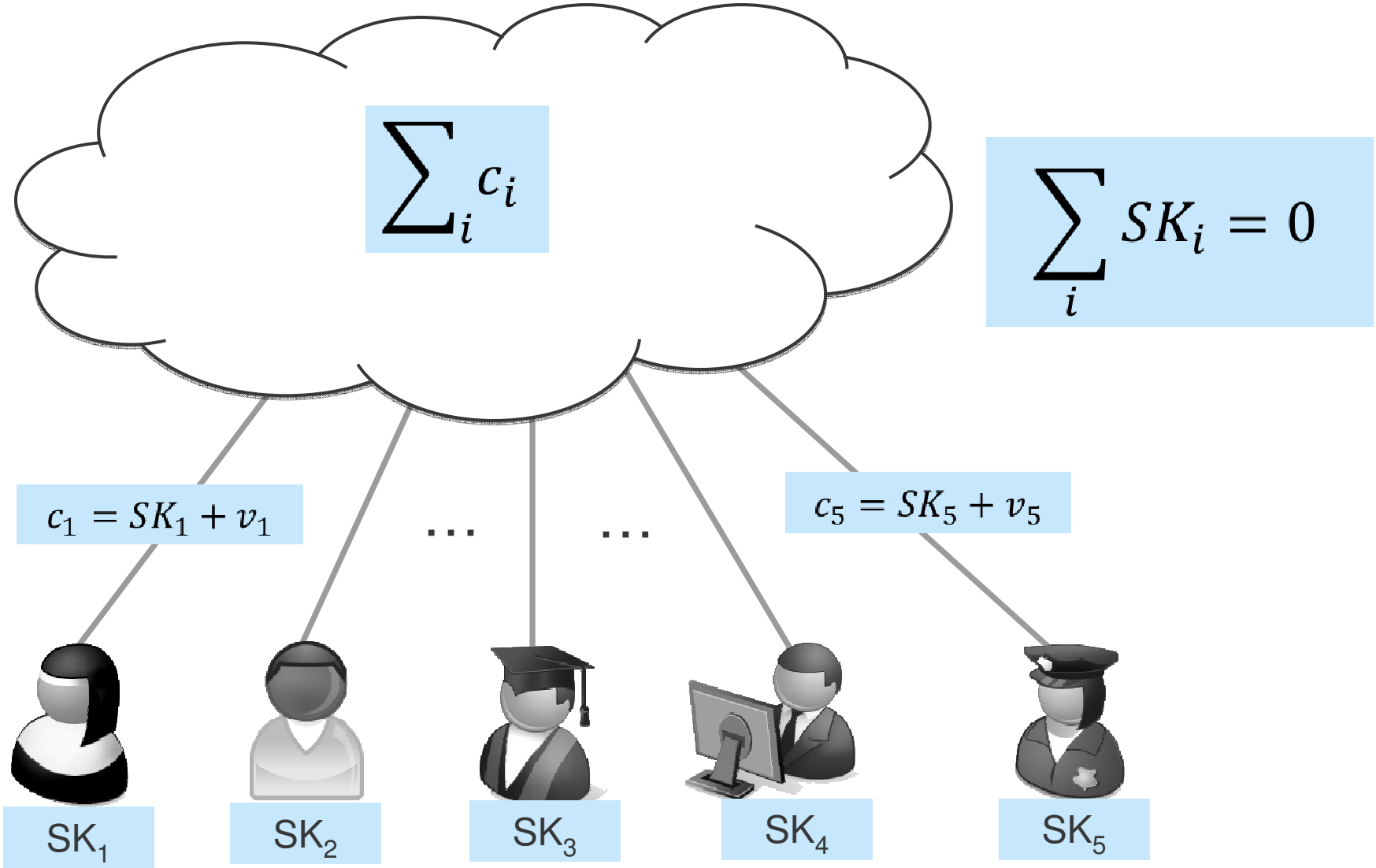


$$\sum_i SK_i = 0$$

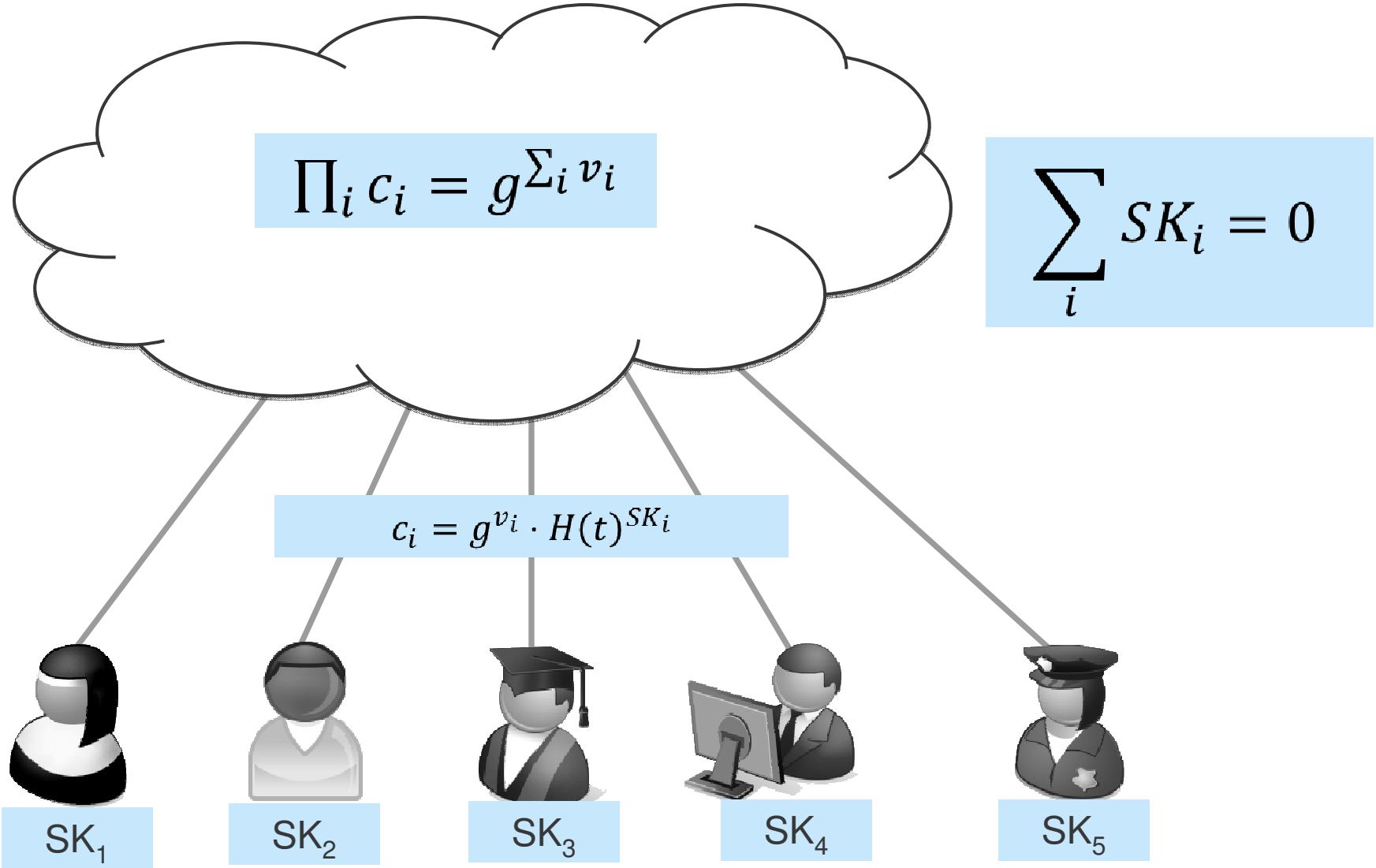
Aggregate Once: Simple Construction



Aggregate Once: Simple Construction



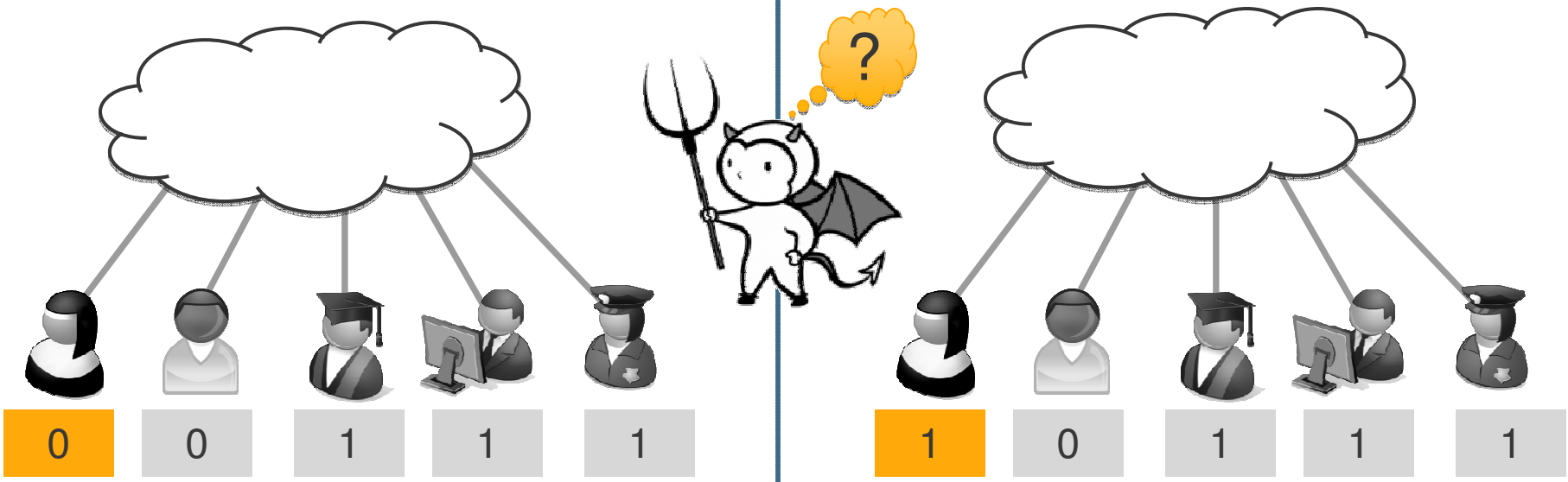
Multiple Time Steps



Differential Privacy against an Untrusted Aggregator

Differential Privacy

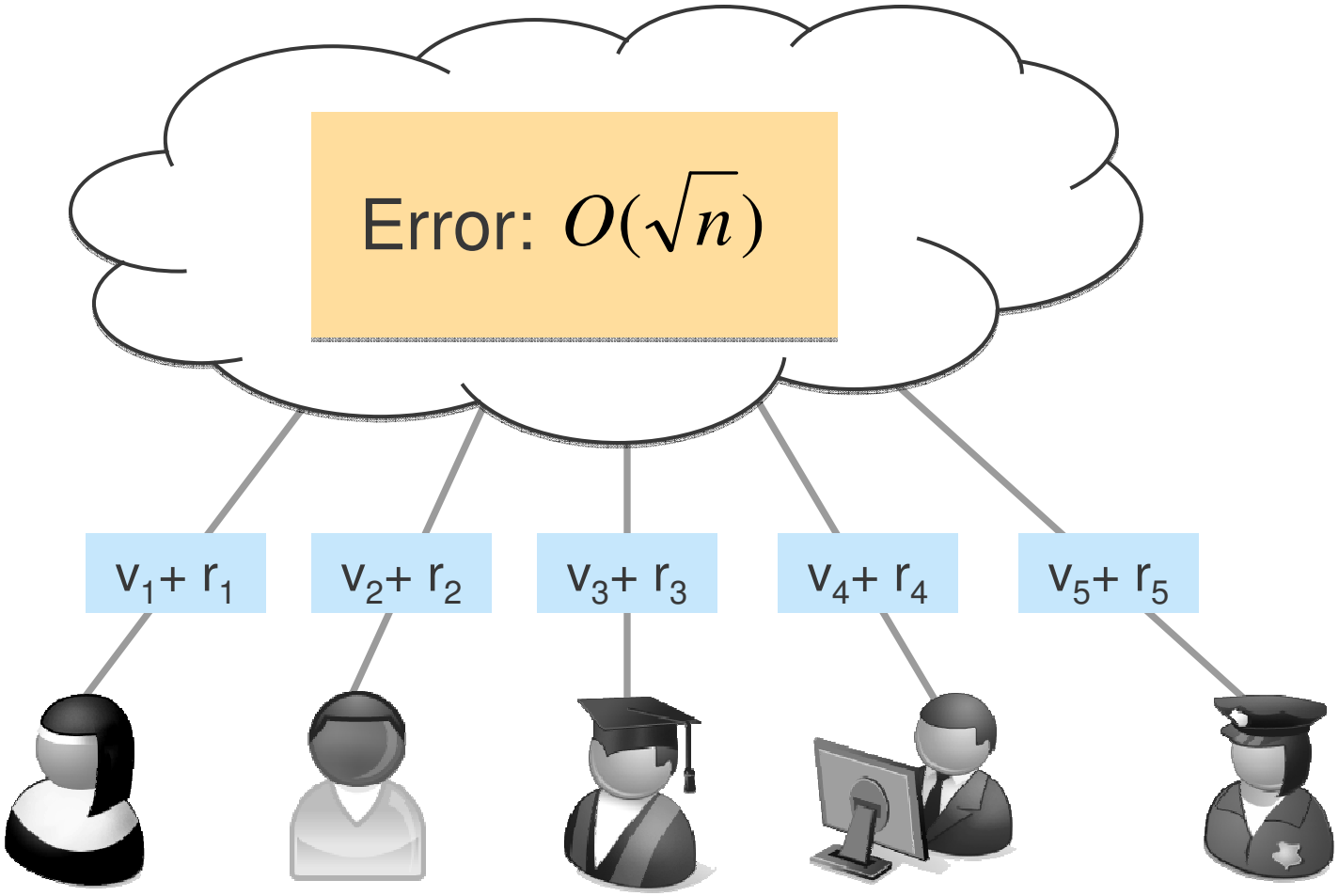
[Dwork06]



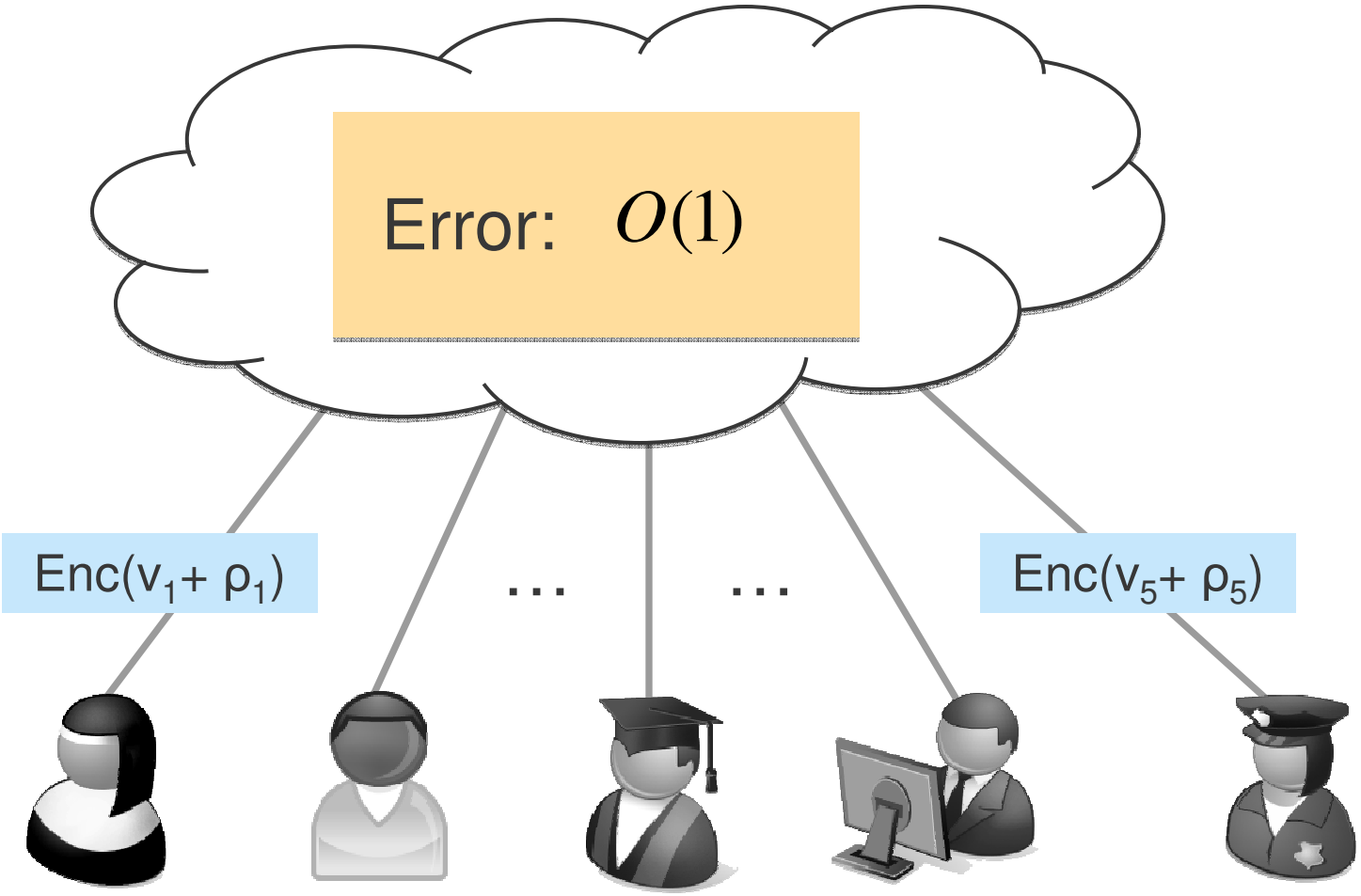
8 neighboring vectors **x** and **x′**, 8 sets of transcripts S:

$$\Pr[\pi(x) \in S] \leq \exp(\varepsilon) \cdot \Pr[\pi(x') \in S]$$

Naïve Scheme



Crypto + Differential Privacy



Open Problems and Future Work

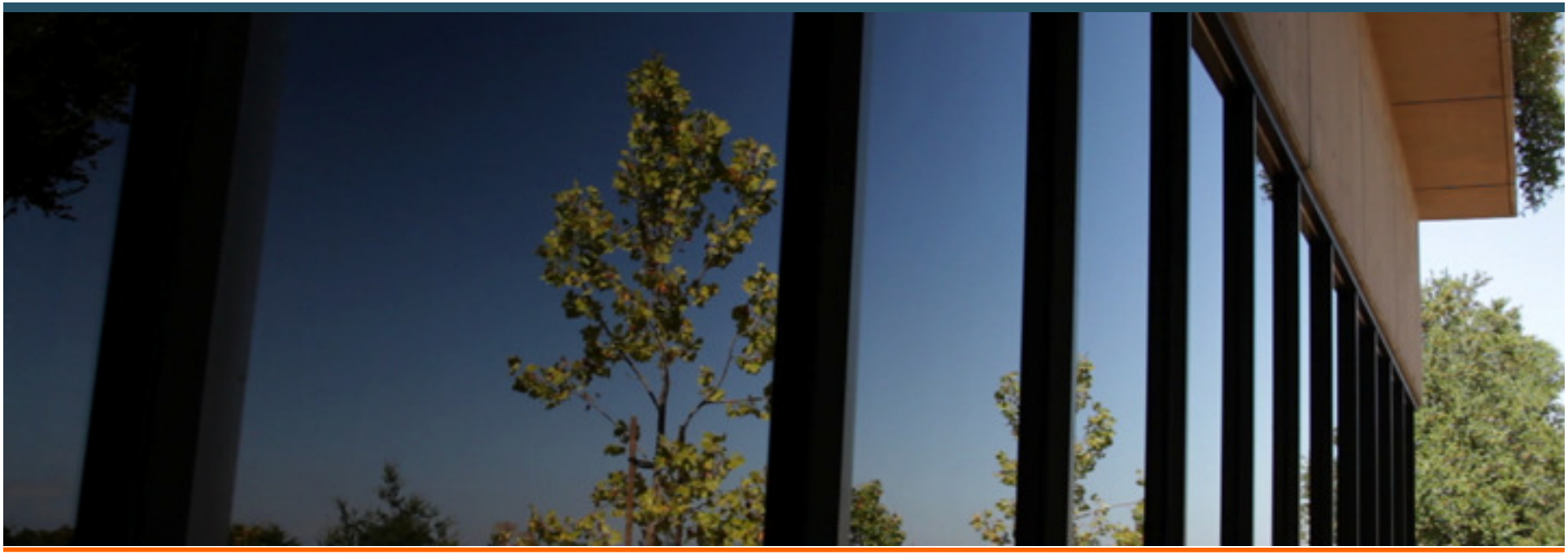
- More expressive queries
- Larger plaintext space
- Fault tolerance [CSS10]
- Reduce privacy loss over multiple time steps [CSS10]

Take-Home Messages

- Differential Privacy against an Untrusted Aggregator
- The Power of Combining Cryptography and Differential Privacy

parc
A Xerox Company

Thank you!



Our Results – Property

- Periodic aggregation
- Non-interactive
  - No interactions among users
  - Users upload ciphertext to aggregator, and no more communication needed

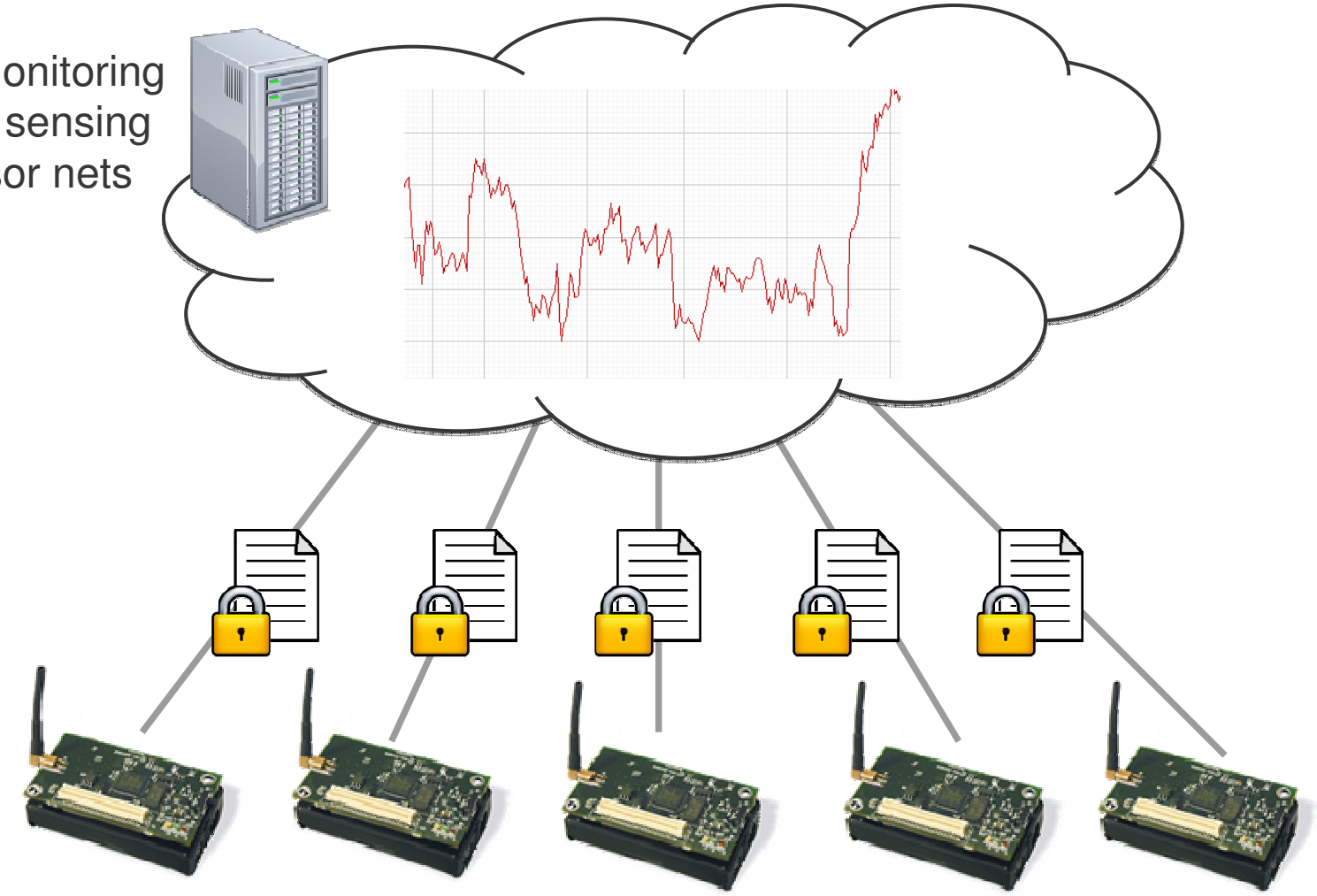
Power of Combining Crypto and Differential Privacy

Scheme	Error Bound
Differential Privacy	$\Omega(\sqrt{n})$ [CSS10]
Crypto + Differential Privacy	$O(1)$

Privacy in Sensor Networks

- Building monitoring
- Employee sensing
- Body sensor nets

…



Privacy in Market Research