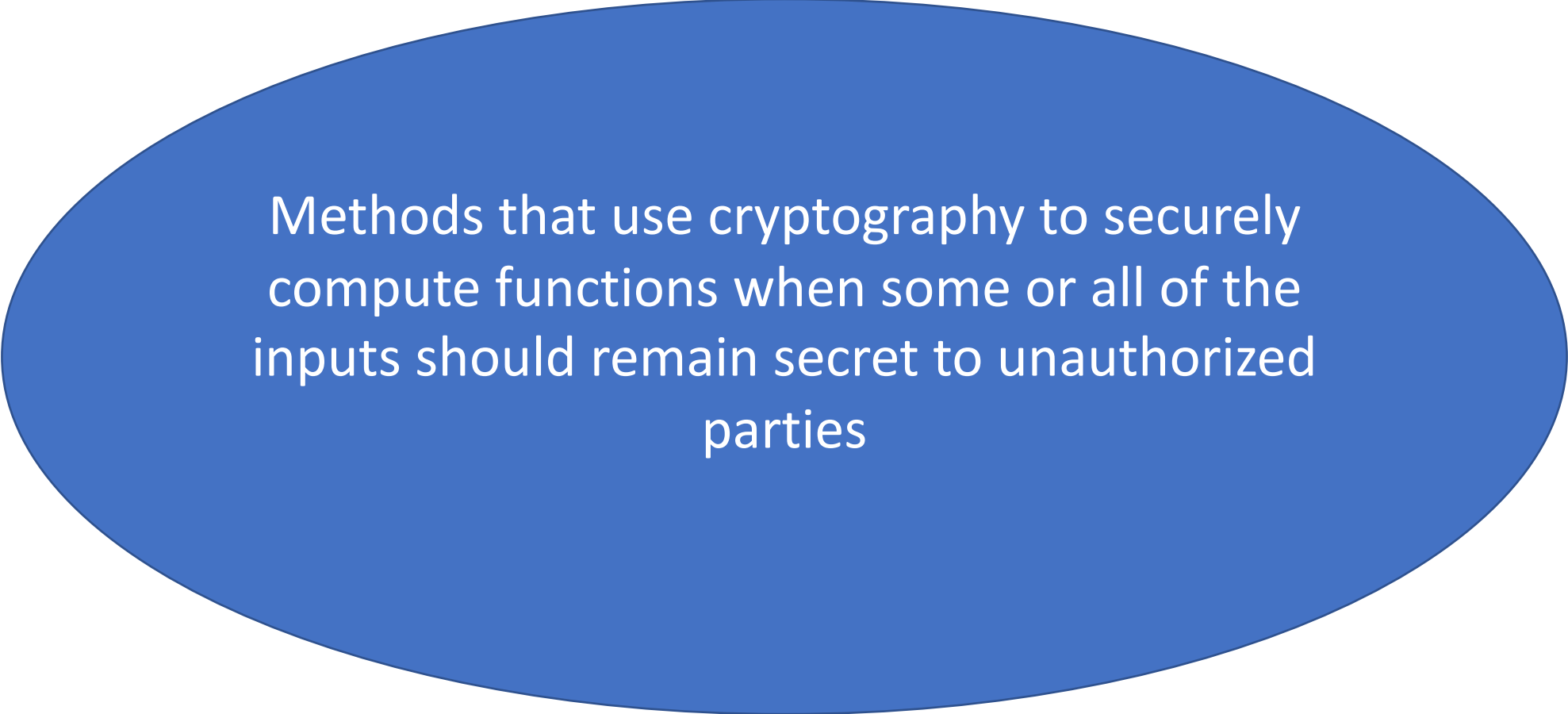


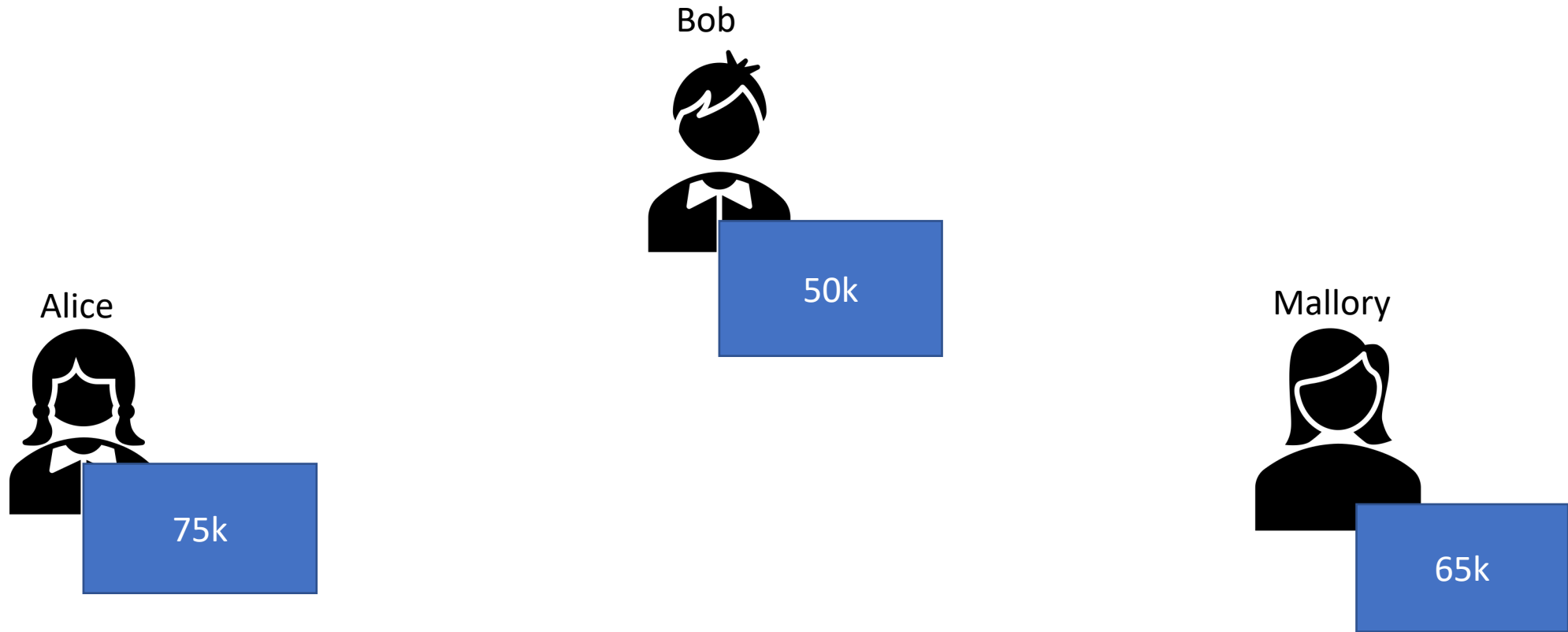
- Secure Computation Techniques
- Data Provenance for Secure Computation
- Provenance Policies

Secure Computation Techniques

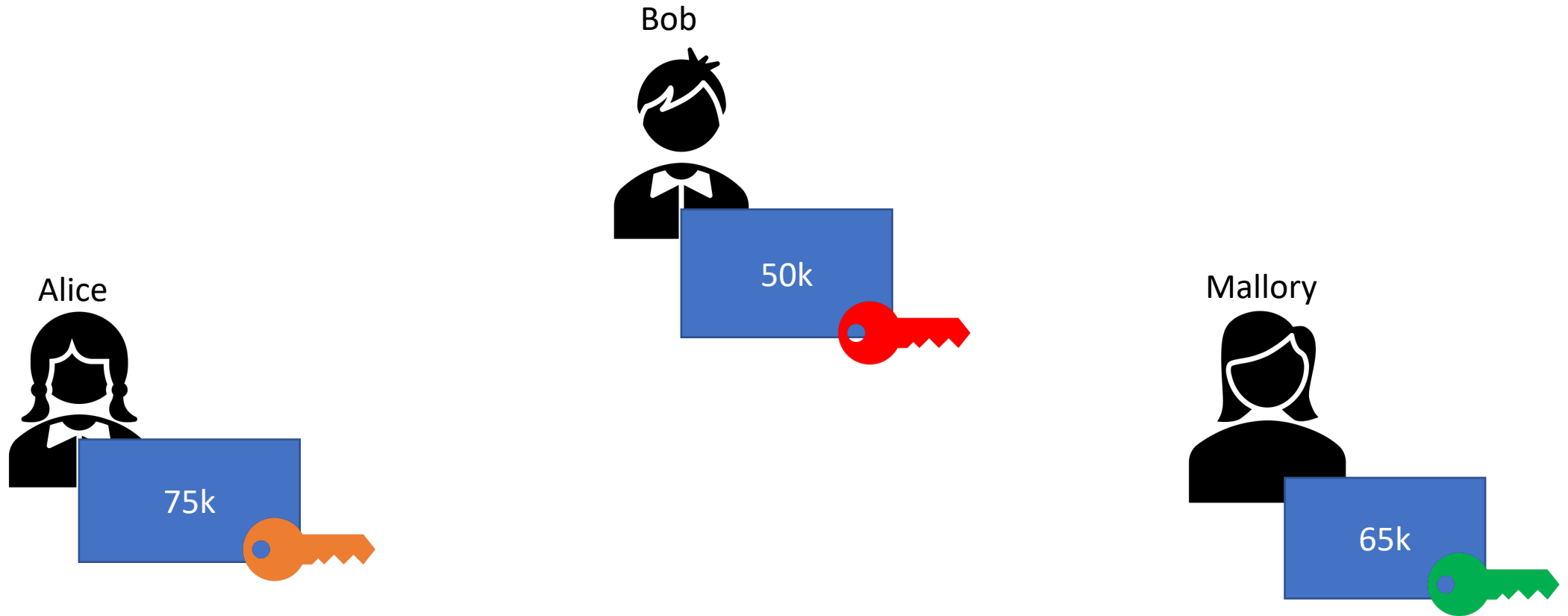


Methods that use cryptography to securely compute functions when some or all of the inputs should remain secret to unauthorized parties

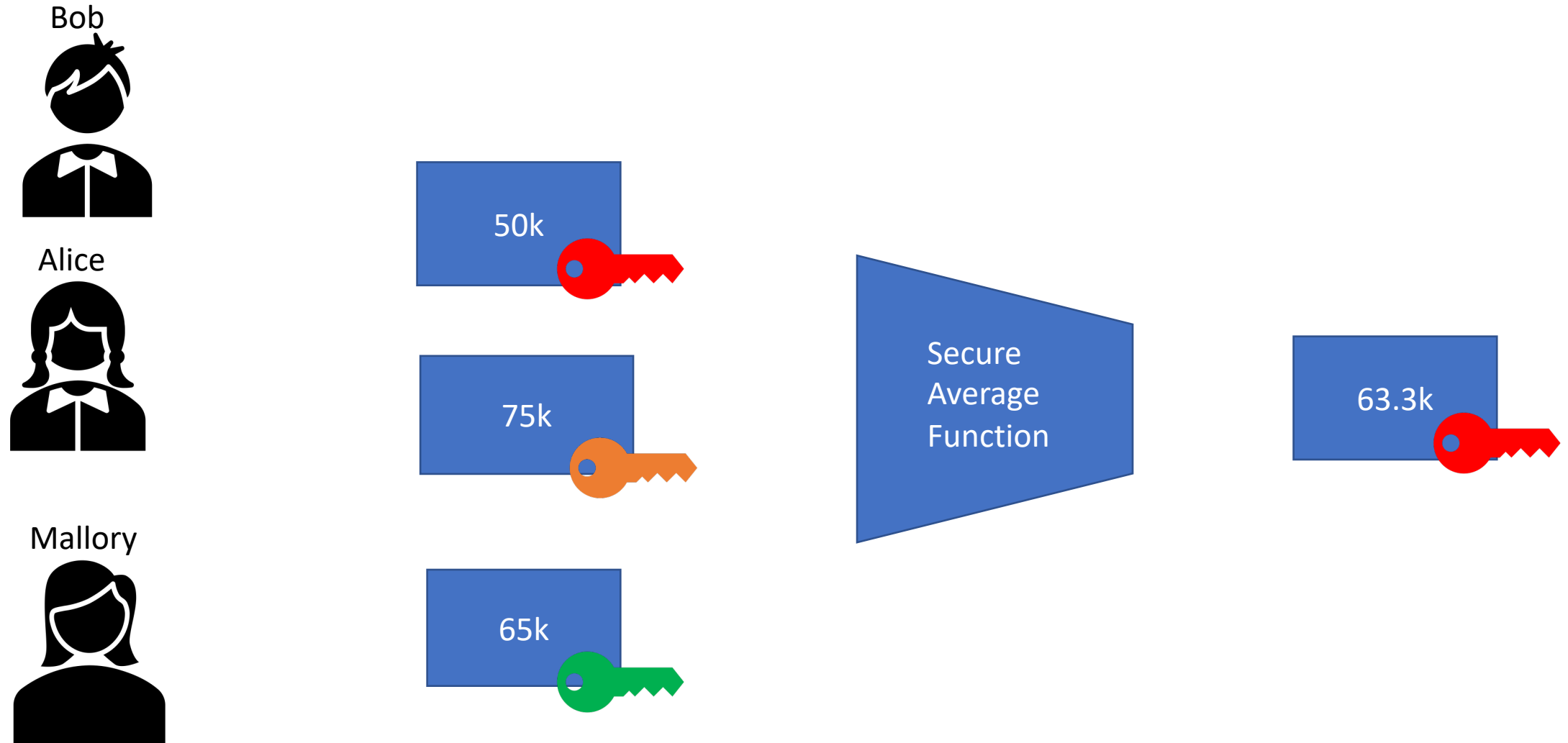
Secure Computation Example



Secure Computation Example



Secure Computation Example



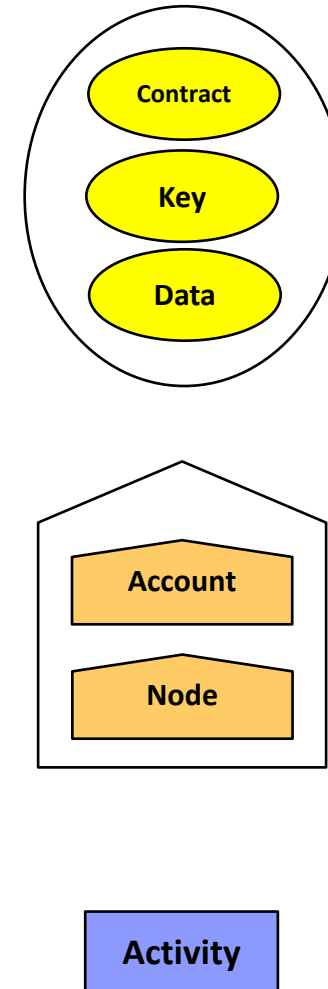
Data Provenance for Secure Computation

Data Provenance

- Documentation describing the history of data from its inception to its latest state
 - Can be used to assess the integrity of data
- Represented as a labeled directed acyclic graph
- Nodes
 - Entities: Contract, Key, or Data
 - Agents: Account or Node
 - Activities
- Labeled edges
 - WasAttributedTo, WasDerivedFrom, Used, ActedOnBehalfOf, WasAssociatedWith, and WasGeneratedBy

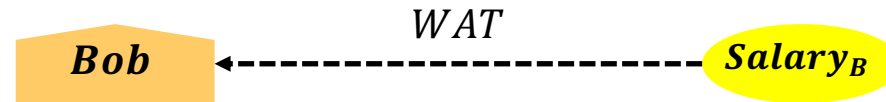
Secure Computation Provenance Nodes

- Contract entity represents the logic that defines a function
- Key entity represents a cryptographic key
- All other data is represented by data entities
- Account agent represents a user or organization
- Node agent represents secure computation engine
- Activity represents a function



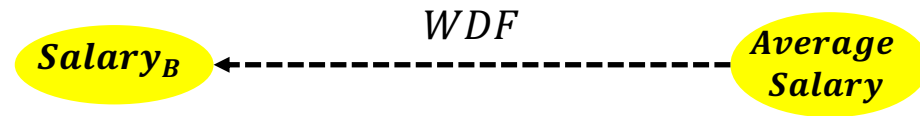
Secure Computation Provenance Edges

- WasAttributedTo (WAT)
 - Source node type: Entity
 - Destination node type: Agent



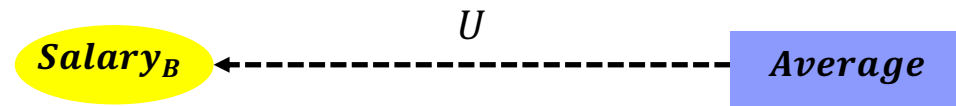
Secure Computation Provenance Edges

- WasDerivedFrom (WDF)
 - Source node type: Entity
 - Destination node type: Entity



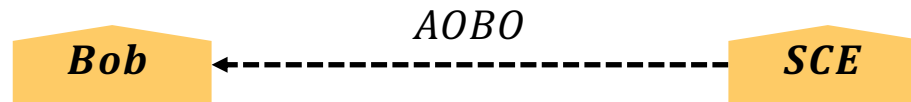
Secure Computation Provenance Edges

- Used (U)
 - Source node type: Activity
 - Destination node type: Entity



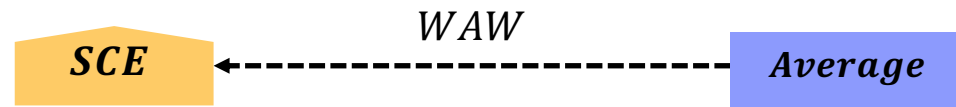
Secure Computation Provenance Edges

- **ActedOnBehalfOf(AOBO)**
 - Source node type: Node Agent
 - Destination node type: Account Agent



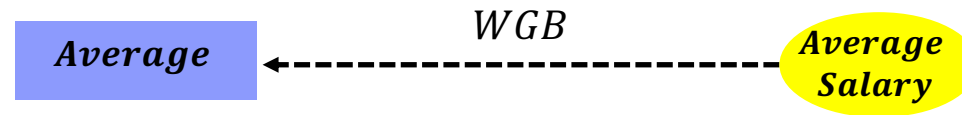
Secure Computation Provenance Edges

- WasAssociatedWith(WAW)
 - Source node type: Activity
 - Destination node type: Node Agent

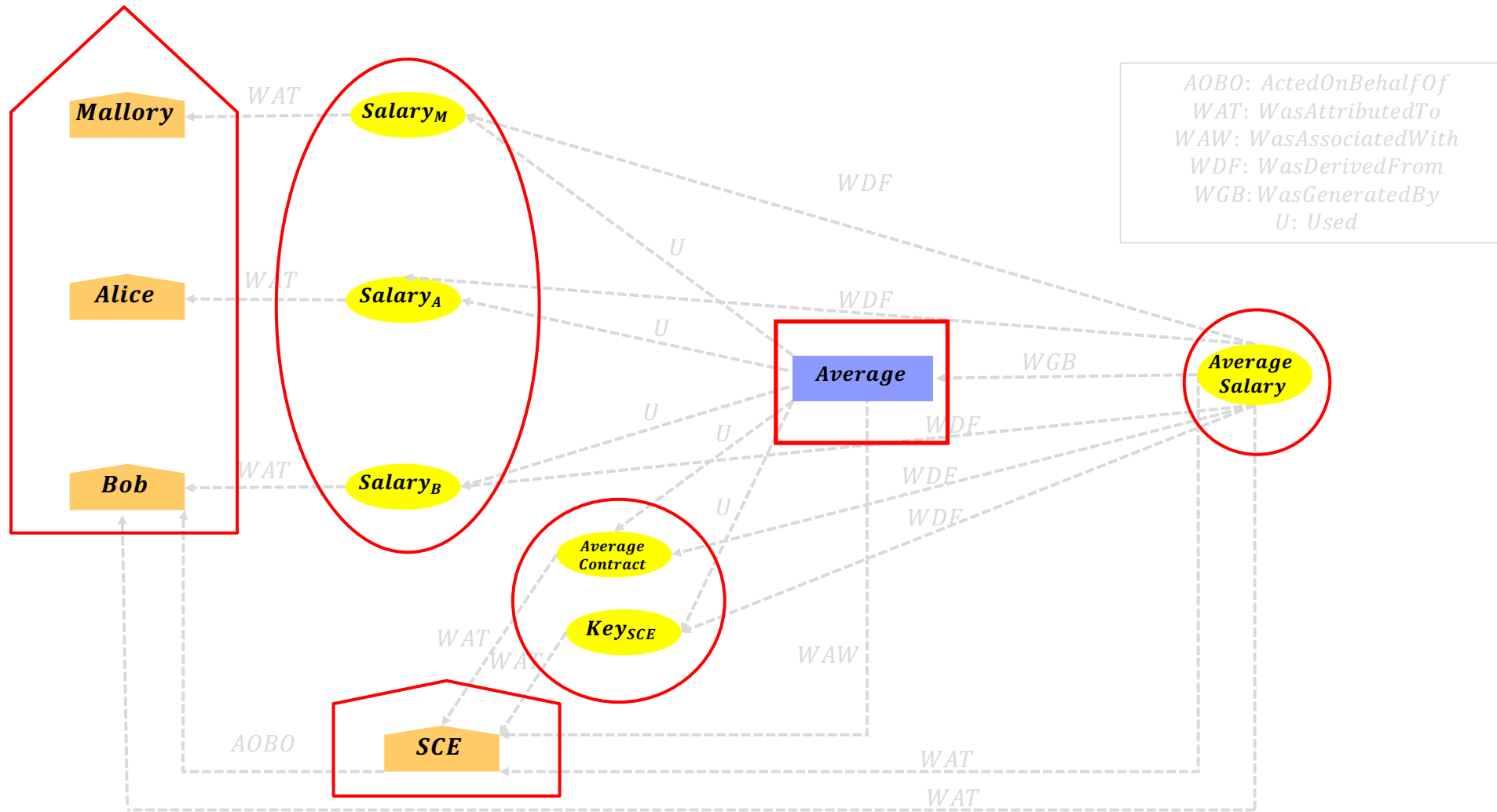


Secure Computation Provenance Edges

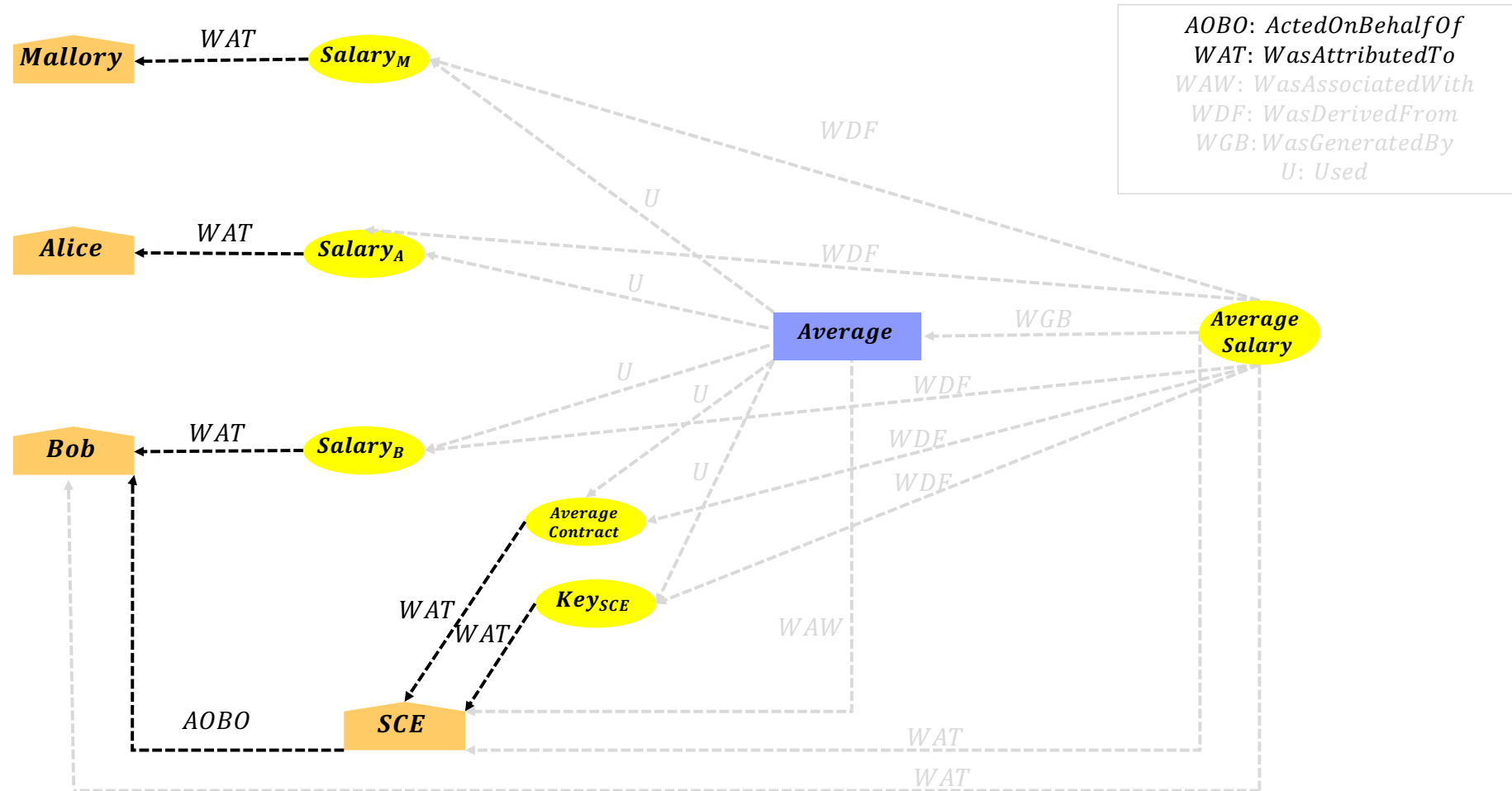
- WasGeneratedBy(WGB)
 - Source node type: Entity
 - Destination node type: Activity



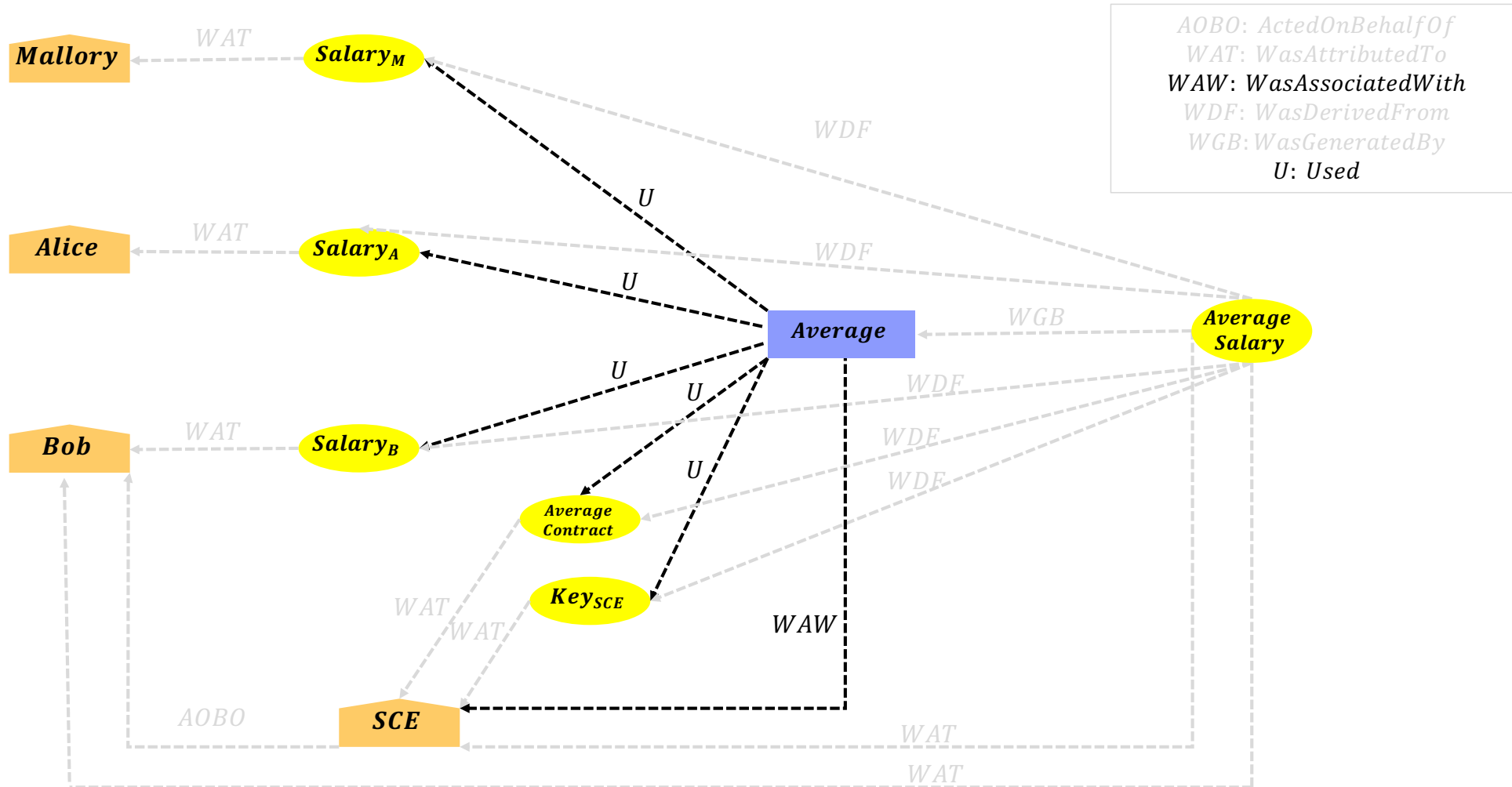
Example Provenance Graph



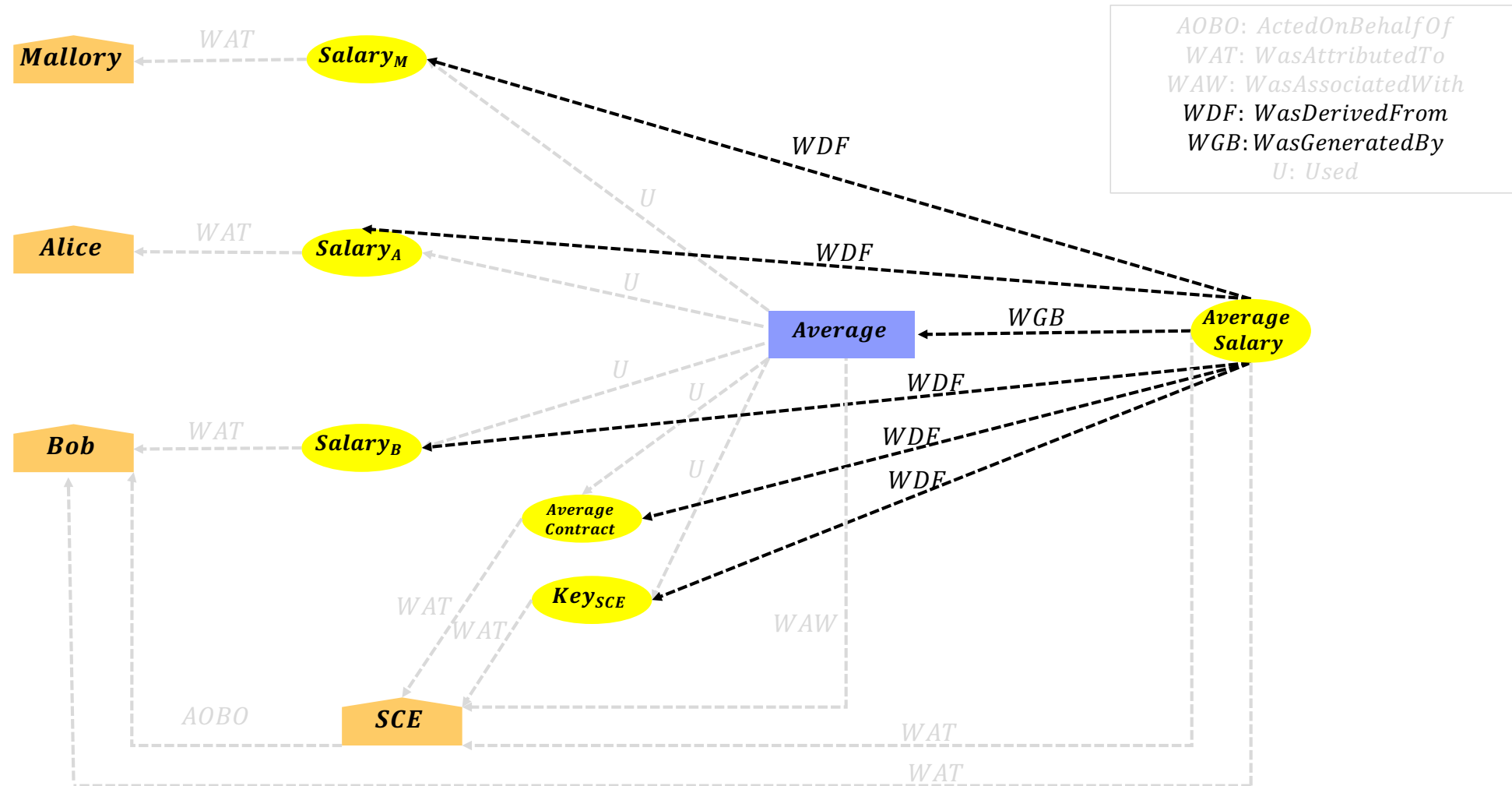
Example Provenance Graph



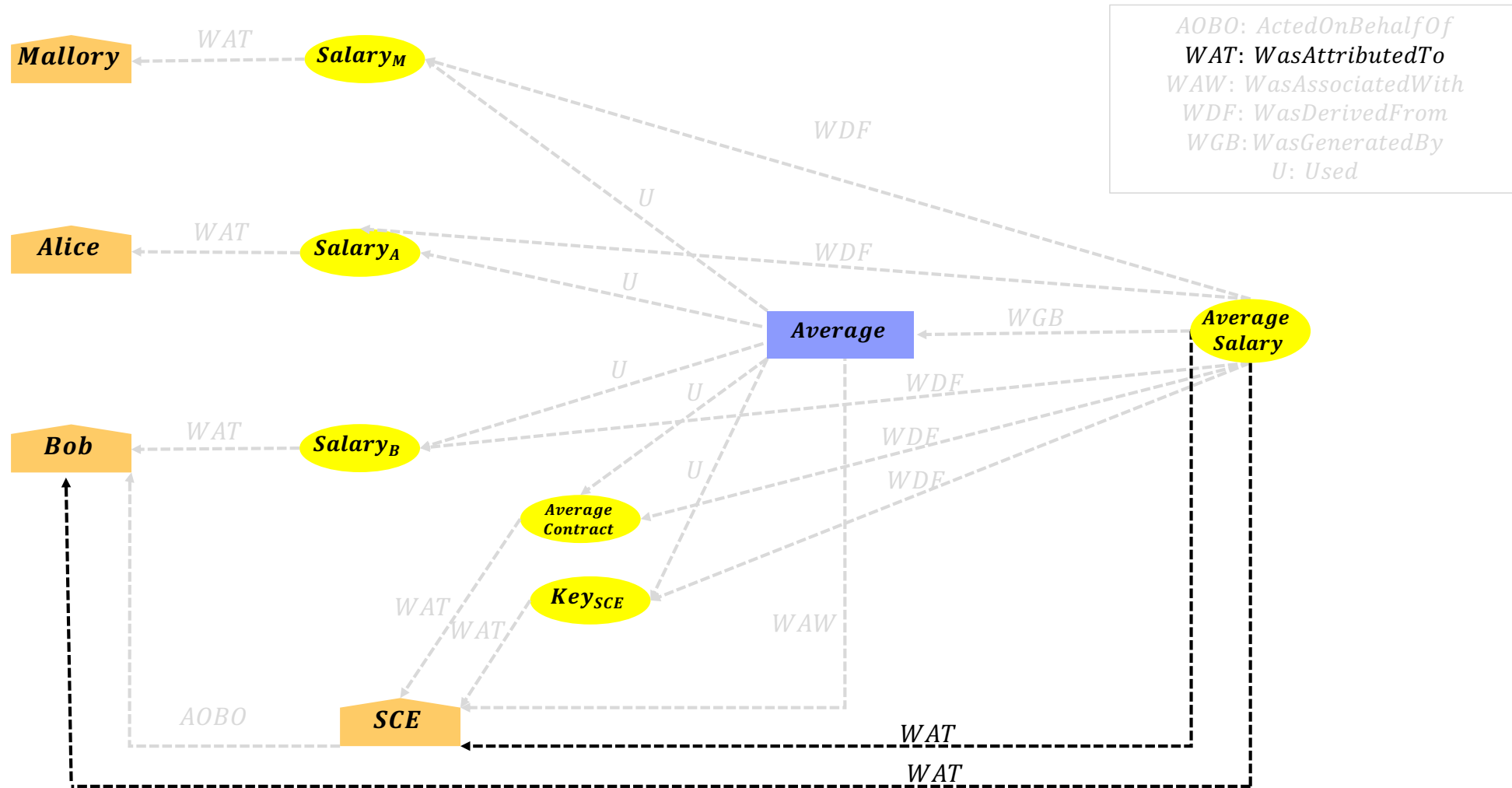
Example Provenance Graph



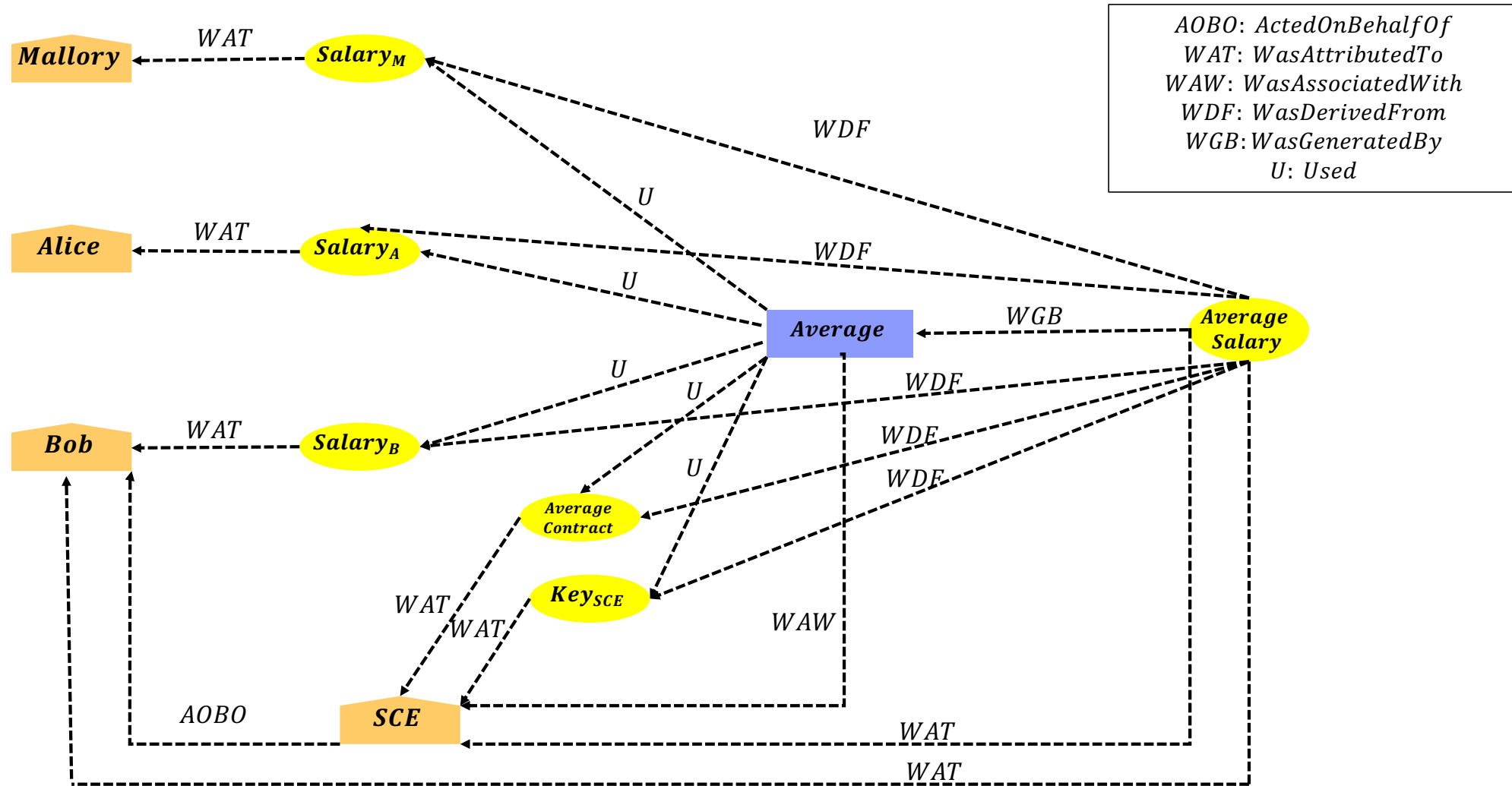
Example Provenance Graph



Example Provenance Graph



Example Provenance Graph



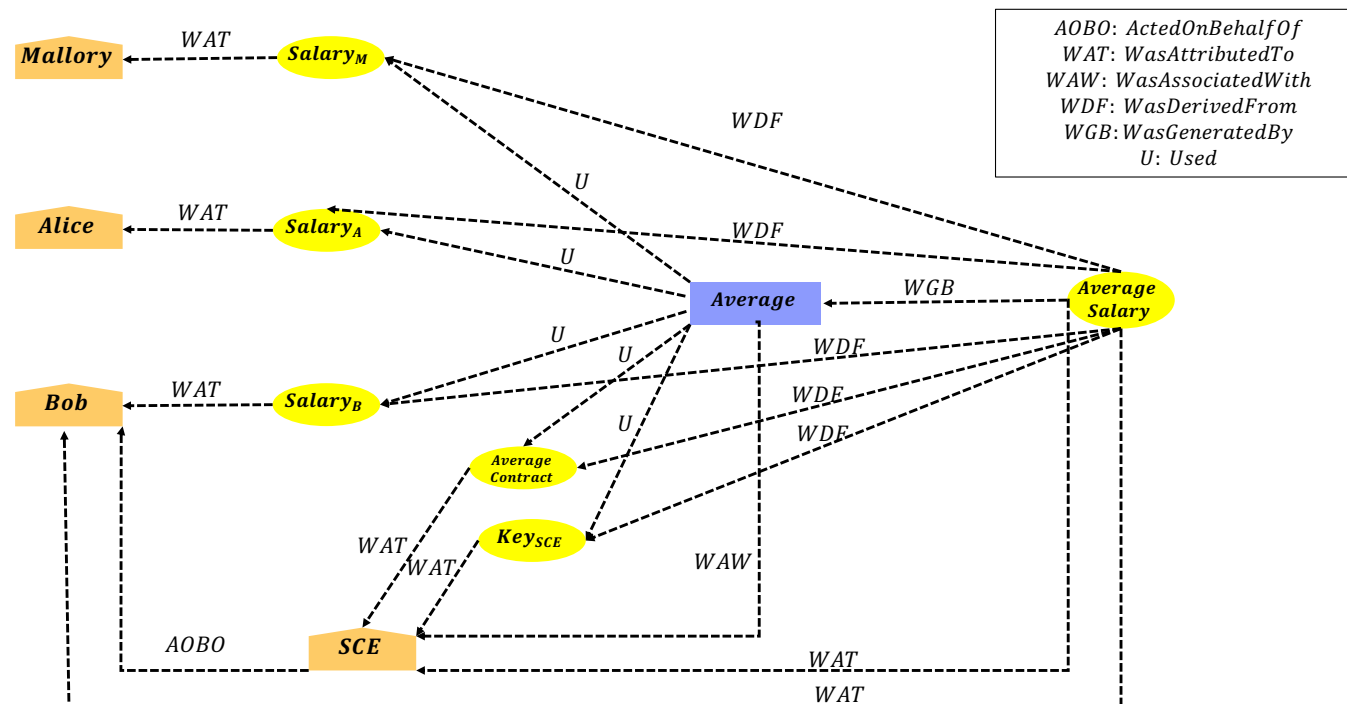
Provenance Policies

Provenance Policies

- Constraints placed on provenance graphs to either:
 1. Verify that data was generated as expected
 2. Detect when data was manipulated in an unexpected way
- Aim to prevent the consumption of untrusted data

Provenance policies

- Bob can verify that the average salary was generated as he expected by specifying a provenance policy that can be automatically evaluated on the provenance graph



Provenance Policies

- In this study you will use two languages and systems to specify provenance policies that will be evaluated on provenance graphs
 - ProProv
 - Rego