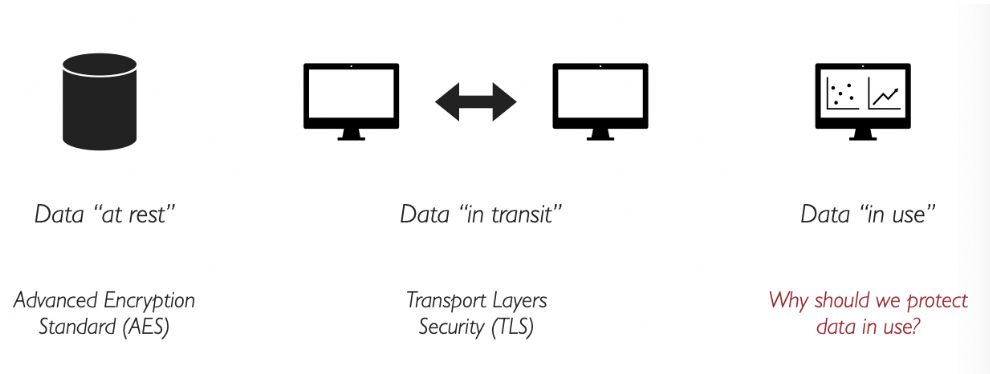
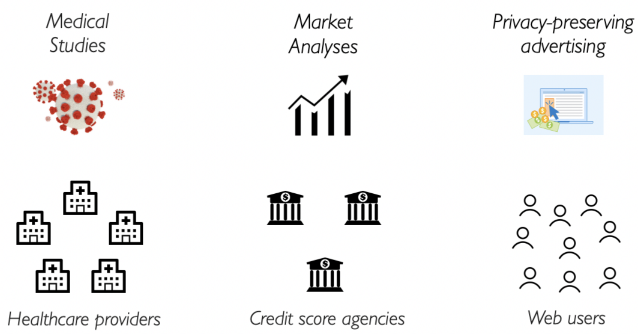
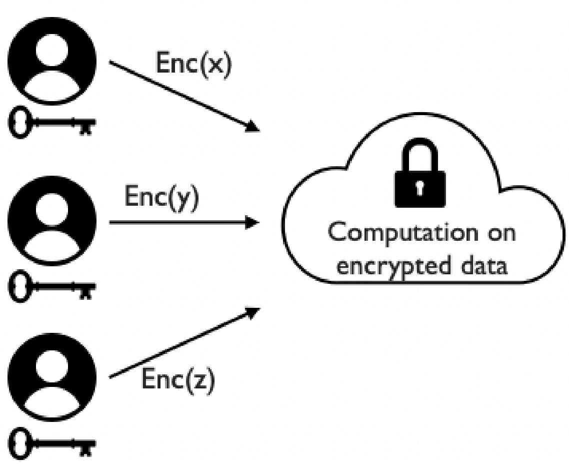
CAS CS 350
Lec 25

Systems for Secure Computation

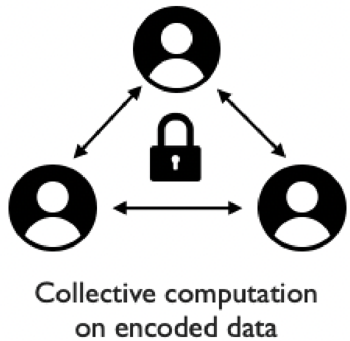
1. End-To-End Data protection
    a. 

2. Use Cases: Secure Collaborative Analytics
    a. 

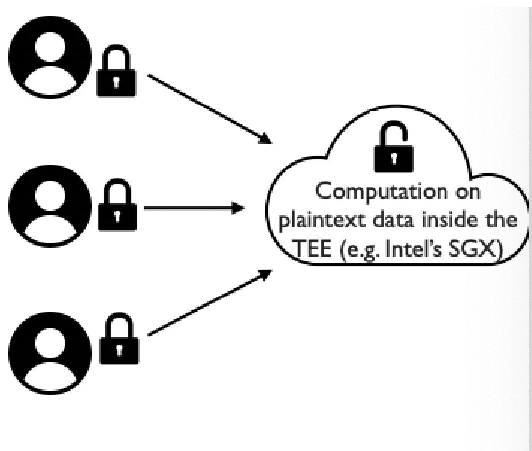
3. Approaches to secure Collaborative analytics
    a. Fully Homomorphic Encryption (FHE)
    b. 

    c. Security via homomorphic encryption (very high computational cost)

d. Secure Multi-Party Computation (MPC)

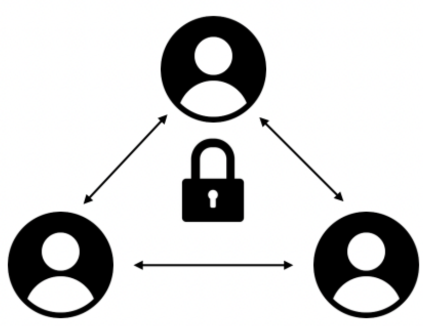


e.
f. Security via decentralized trust (high communication cost)
g. Trusted Execution Environments (TEEs)

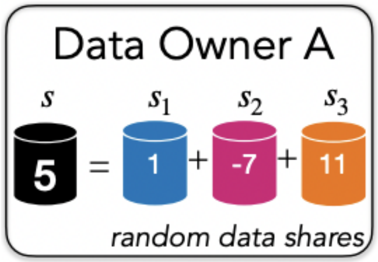


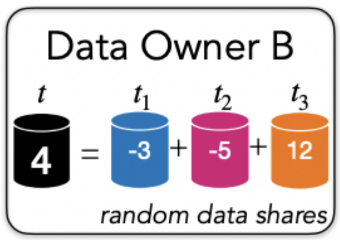
h.
i. Security via physically protected HW (prone to side-channel attacks)

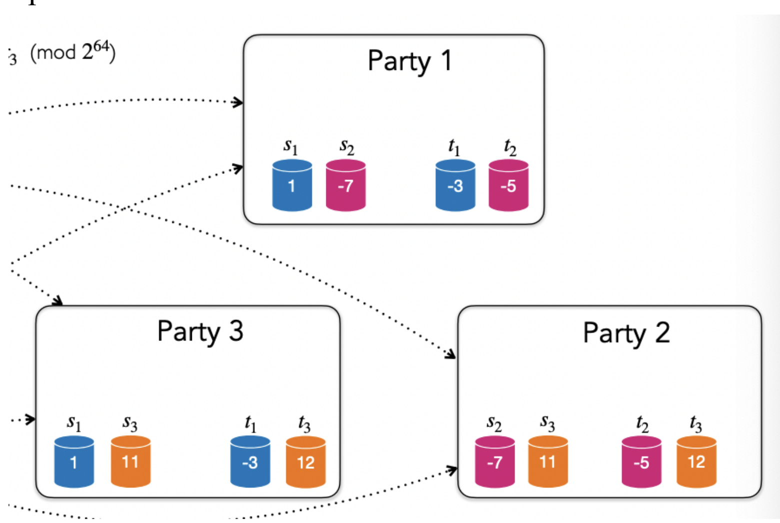
4. Secure Multi-party Computation (MPC)

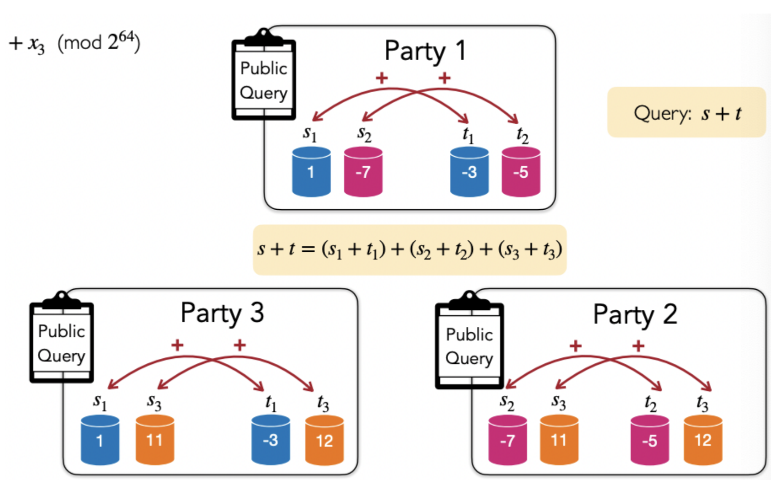


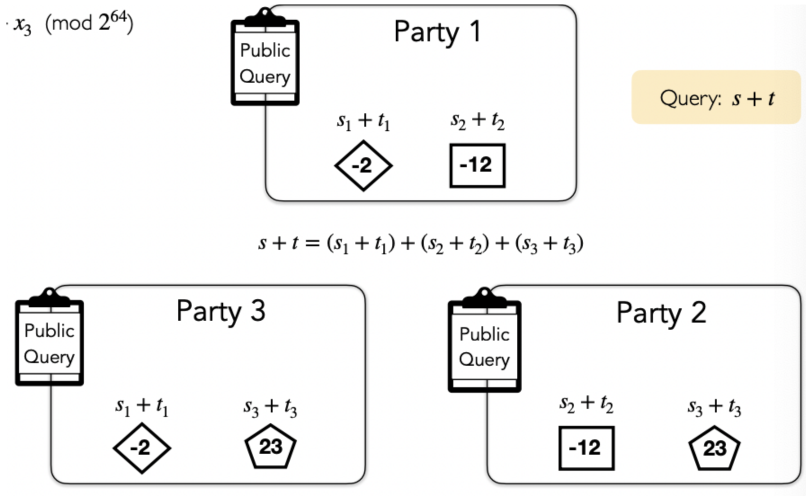
a.
b. Any number of parties
c. Protection against external adversaries
d. Protection against malicious parties
e. Arbitrary computations
f. Easy to explain
    i. But not easy to make it practical

5. Example: Secure Addition
    a. Arithmetic sharing: x = x1 + x2 + x3 (mod 2^64)
    b. 

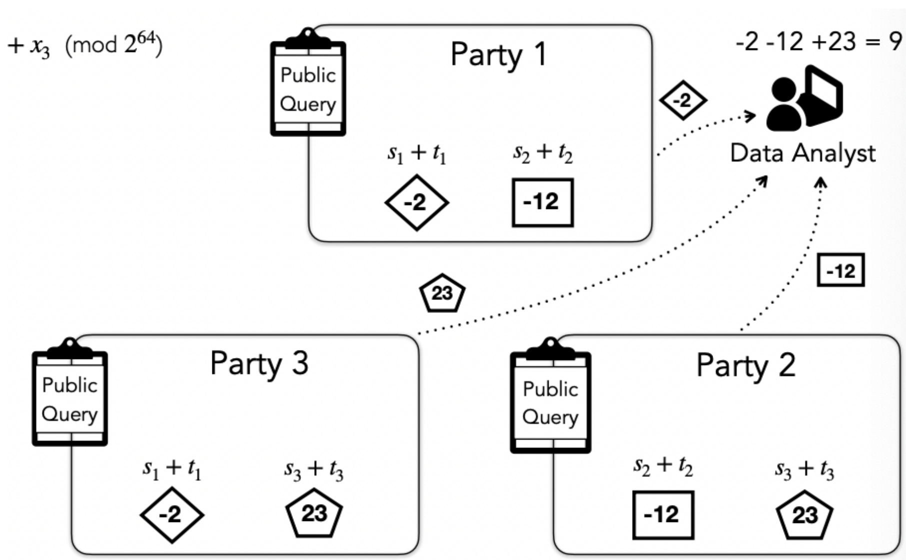
    c. 

    d. 3 parties
    e. 

    f. 

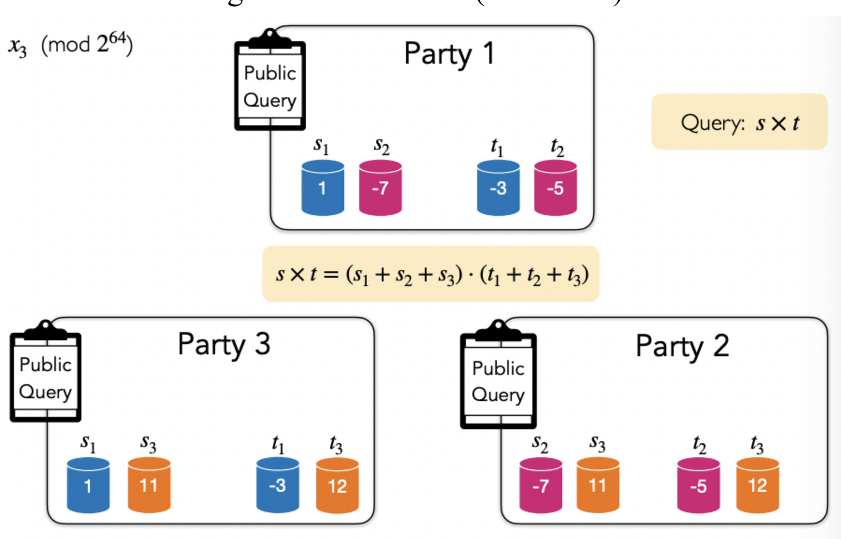


g.

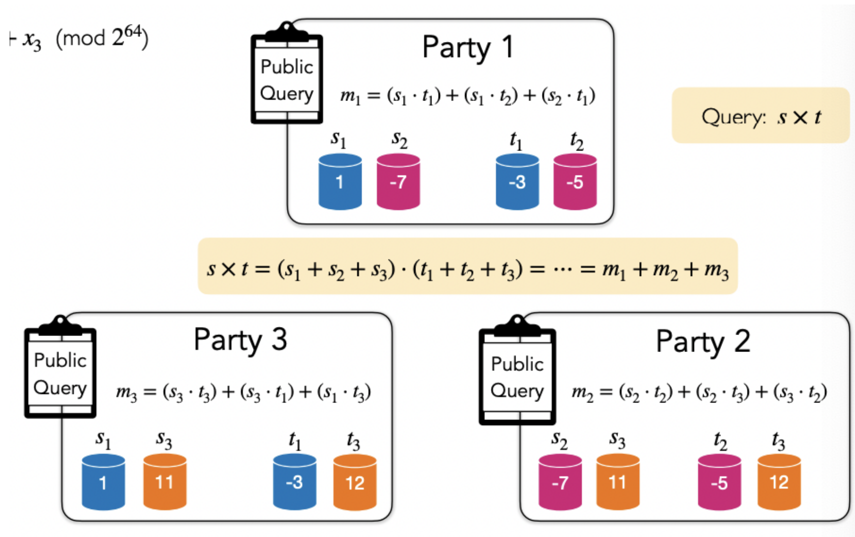


h.

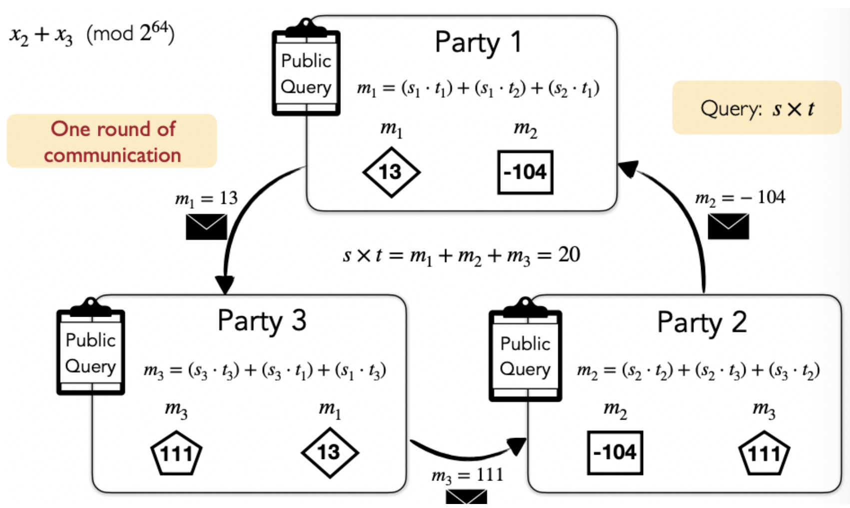
6. Example: Secure multiplication
   a. Arithmetic sharing: x = x1 + x2 +x3 (mod 2^64)



b.

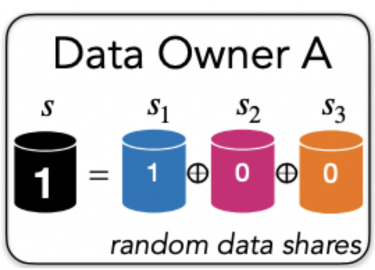


c.

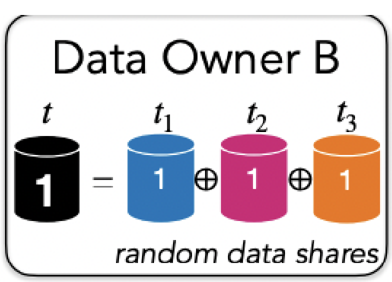


d.

7. Example: Secure XOR
   a. Boolean Sharing: x = x1 XOR x2 XOR x3

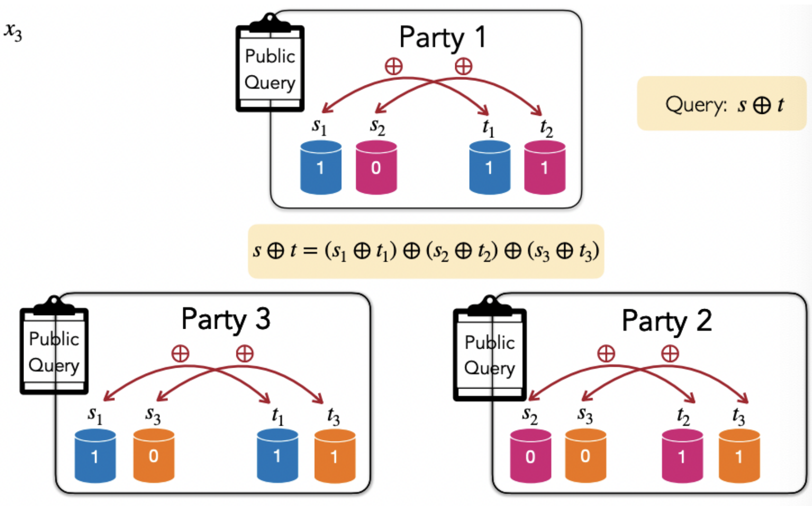


b.



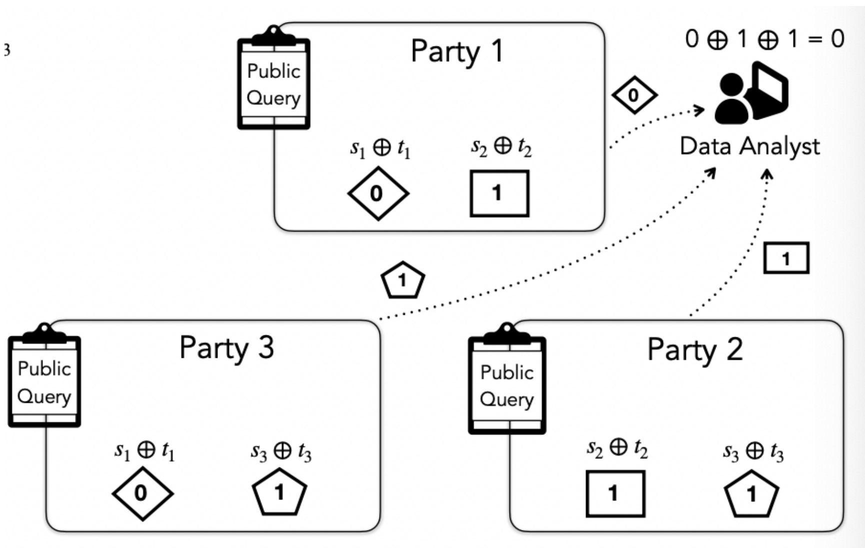
c.

x_3



d.

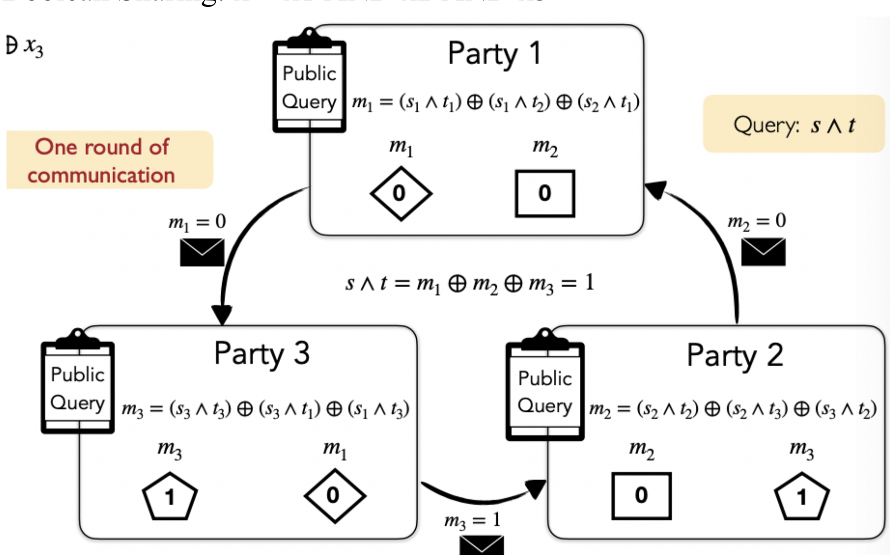
3



e.

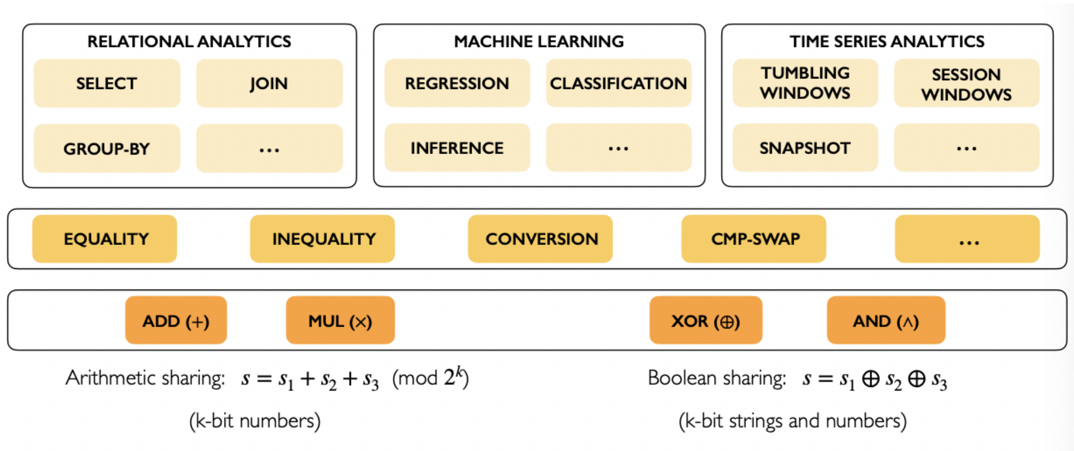
8. Example: Secure AND
   a. Boolean Sharing: x = x1 AND x2 AND x3

Ɖ x_3



b.

9. From Secure Primitives to Complex Computations

a. 

10. Oblivious Computation

   a. To prevent information leakage, the computing parties perform an identical computation that is data-independent
      i. Data access patterns do not depend on the actual shares
      ii. No conditionals (if-then-else)
      iii. No data reduction

b.

For 3-bit numbers: $a : a_2a_1a_0$ $\quad b : b_2b_1b_0$

If $(a > b)\ \{\dots\}$ ➡

$$\phi = a \overset{?}{>} b = (a_2 \oplus b_2) \wedge a_2$$
$$\oplus\ (a_2 \oplus b_2 \oplus 1) \wedge (a_1 \oplus b_1) \wedge a_1$$
$$\oplus\ (a_2 \oplus b_2 \oplus 1) \wedge (a_1 \oplus b_1 \oplus 1) \wedge ((b_0 \oplus 1) \wedge a_0)$$

"If the most significant bits are not the sam
then a is greater than b when a_2 is set"

Cleartext *Oblivious*

c.

nbers: $a : a_2a_1a_0$ $\quad b : b_2b_1b_0$

$$(a_2 \oplus b_2) \wedge a_2$$
$$\oplus\ (a_2 \oplus b_2 \oplus 1) \wedge (a_1 \oplus b_1) \wedge a_1$$

"Else, a is greater than b when the second most significant bits are not the same and a_1 is set"

d.

$$\phi = a \overset{?}{>} b = (a_2 \oplus b_2) \wedge a_2$$
$$\oplus\ (a_2 \oplus b_2 \oplus 1) \wedge (a_1 \oplus b_1) \wedge a_1$$
$$\oplus\ (a_2 \oplus b_2 \oplus 1) \wedge (a_1 \oplus b_1 \oplus 1) \wedge ((b_0 \oplus 1) \wedge a_0)$$

"Else, a is greater than b when a_0 is set and b_0 is not set"

e.

$\boldsymbol{R}$

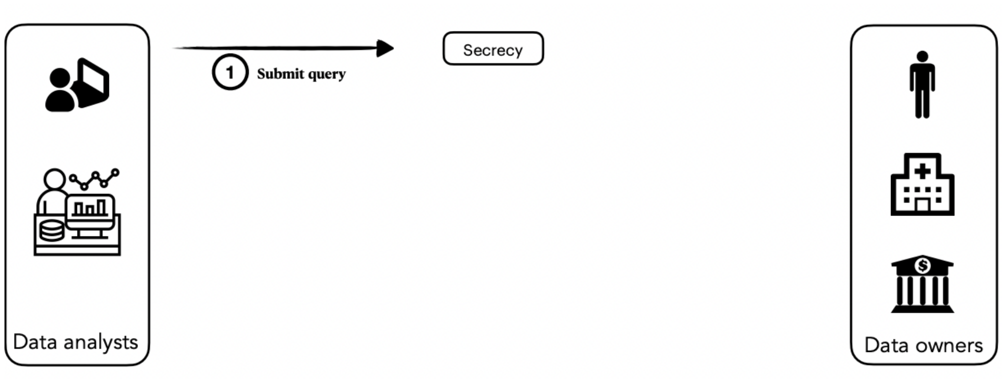
Employee	Salary
Kim	2000
Jane	1500
Alex	4500

$\sigma(Salary > 3000)$ ➡

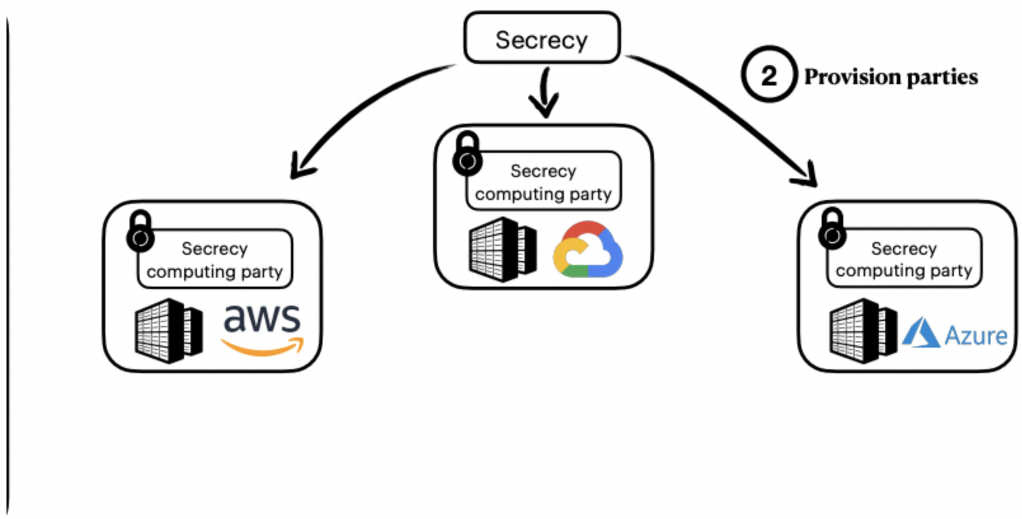
$\boldsymbol{R'}$

Employee	Salary	ϕ
Kim	2000	0
Jane	1500	0
Alex	4500	1

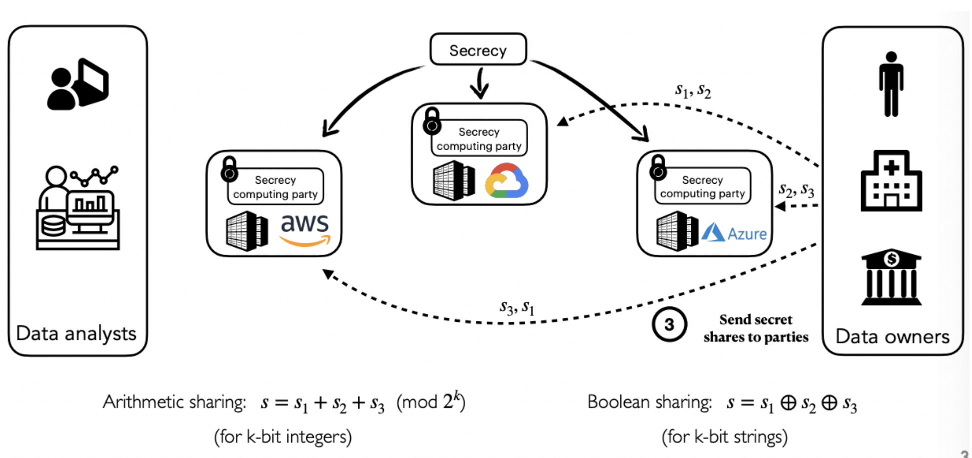
11. The Security project @BU - secrecy as a service



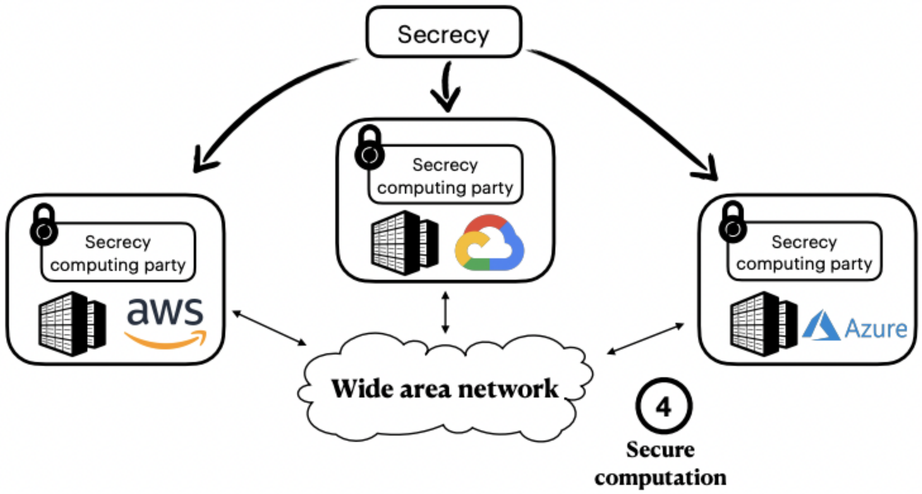
a.



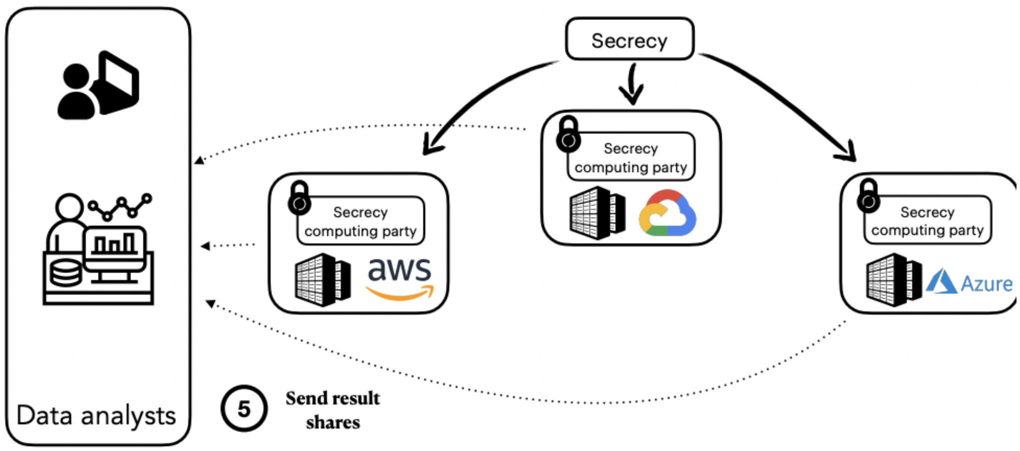
b.



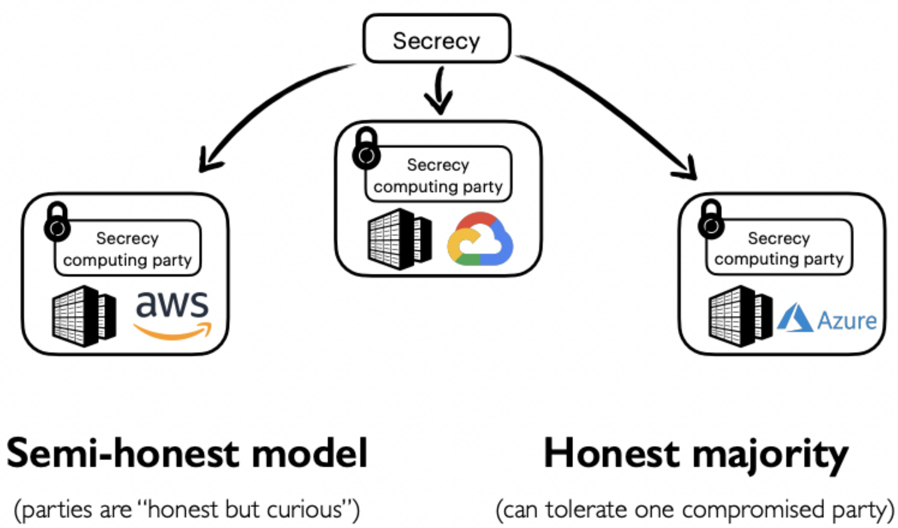
c.


Secrecy
Secrecy computing party
Secrecy computing party
aws
Secrecy computing party
Azure
Wide area network
4
Secure computation

d.


Data analysts
Secrecy
Secrecy computing party
Secrecy computing party
aws
Secrecy computing party
Azure
5
Send result shares

e.


Secrecy
Secrecy computing party
Secrecy computing party
aws
Secrecy computing party
Azure
Semi-honest model
(parties are "honest but curious")
Honest majority
(can tolerate one compromised party)

f.