TURKISH
AVIATION
ACADEMY

İTÜ

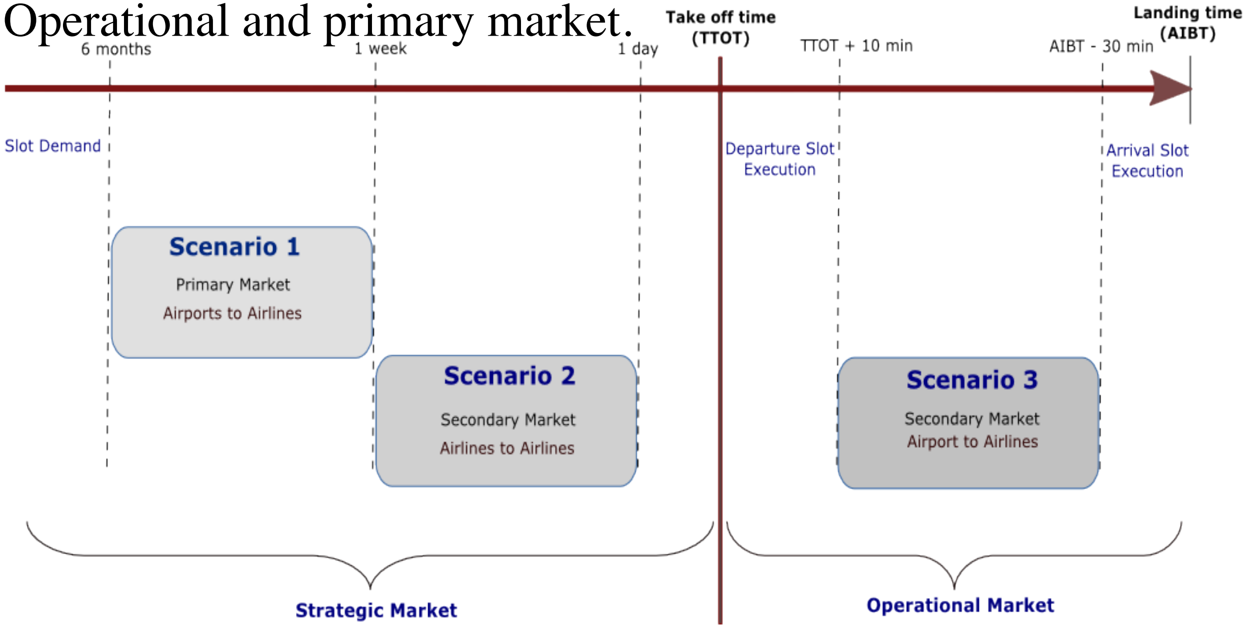
SECURE MULTIPARTY COMPUTATION

DR. EMRE KOYUNCU (ISTANBUL TECHNICAL UNIVERSITY)

Istanbul Technical University
Air Transportation Management
M.Sc. Program

Advanced Information Systems
6 June 2015

- Case scenarios:
  - **Scenario 1:** N airlines try to buy slots from an airport.
    Strategic and primary market.
  - **Scenario 2:** N airlines try to buy slots from another airline.
    Strategic and secondary market.
  - **Scenario 3:** N airlines try to buy a priority approach from an airport.
    Operational and primary market.



Take off time (TTOT)

Landing time (AIBT)

6 months

1 week

1 day

TTOT + 10 min

AIBT - 30 min

Slot Demand

Departure Slot Execution

Arrival Slot Execution

Scenario 1
Primary Market
Airports to Airlines

Scenario 2
Secondary Market
Airlines to Airlines

Scenario 3
Secondary Market
Airport to Airlines

Strategic Market

Operational Market

- General architecture

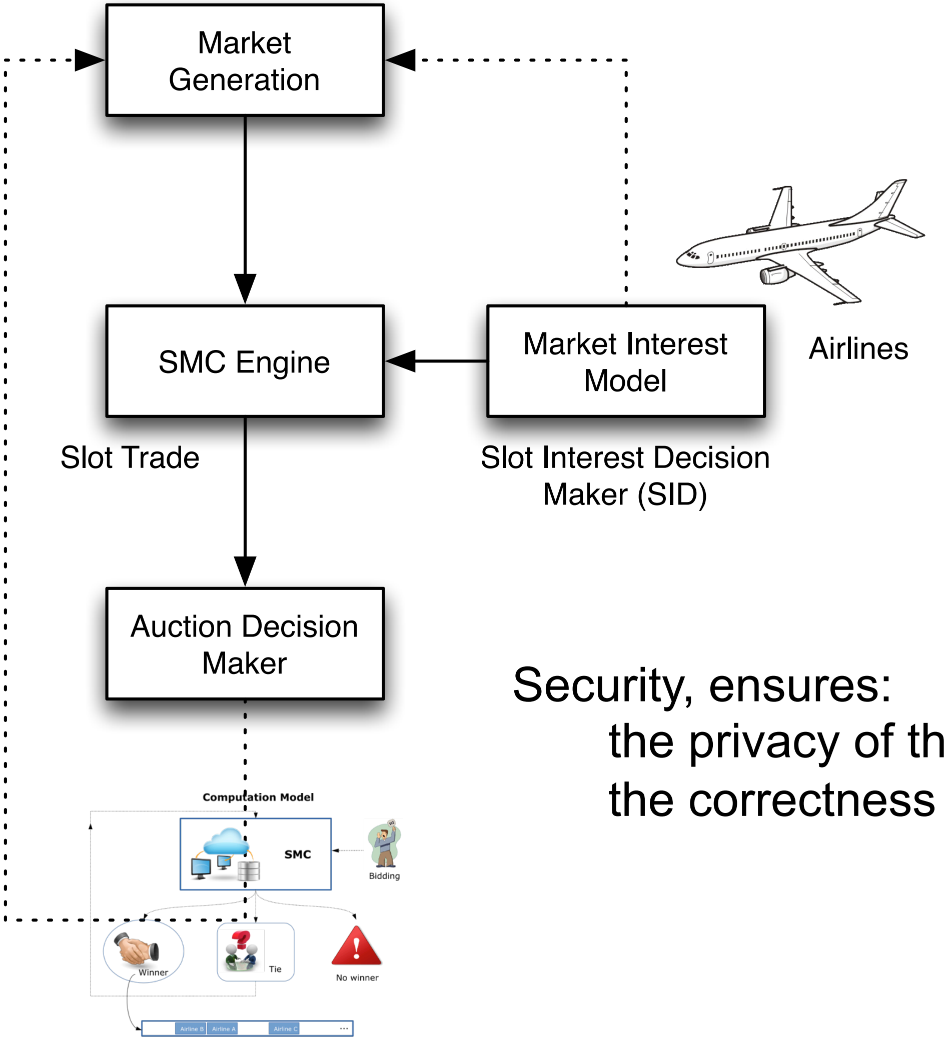


Figure 6. Auction decision cycle

Security, ensures:

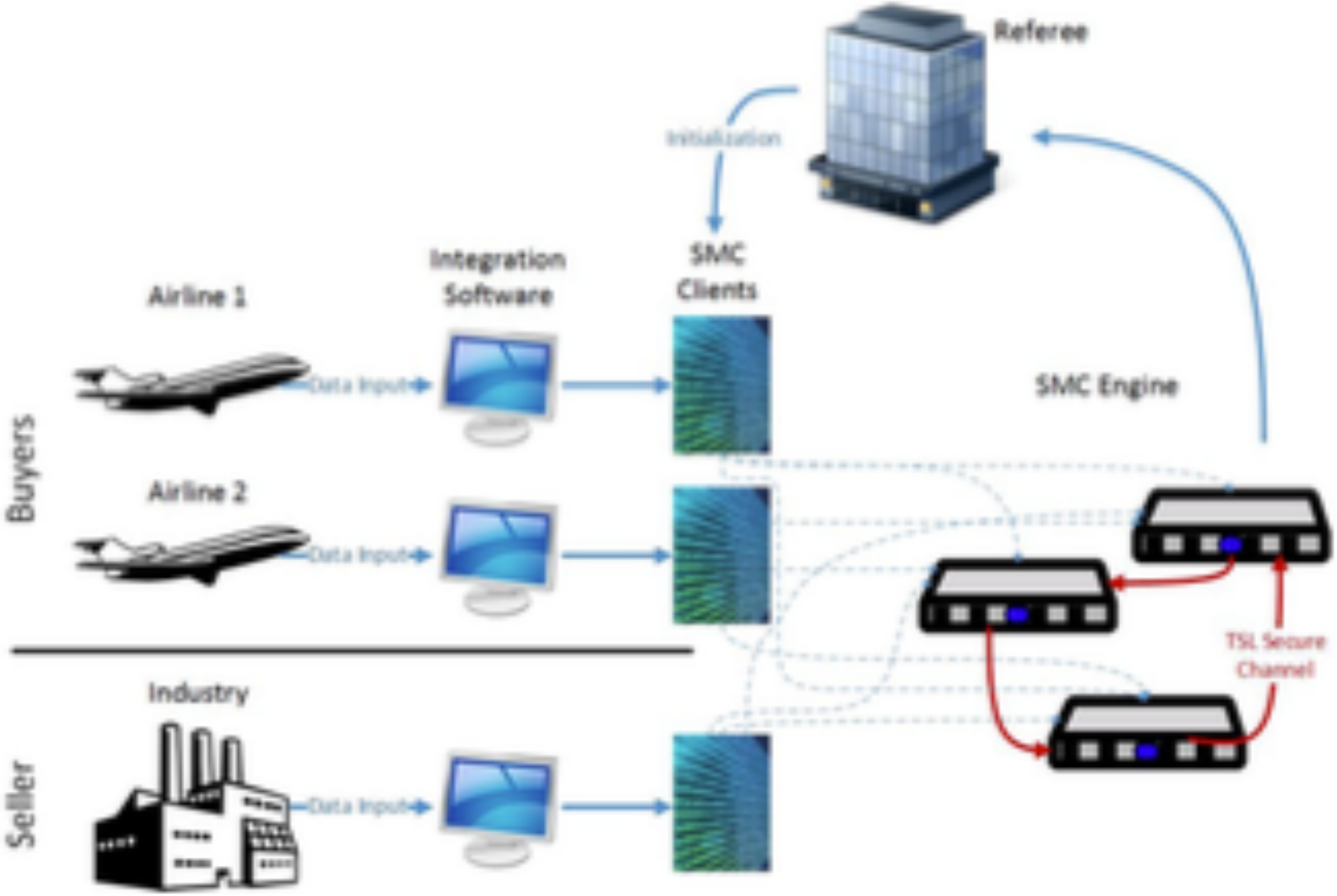
the privacy of the bidders' input and

the correctness of the computation

Slot Trading & Dynamic Landing Queues

Scenario 1

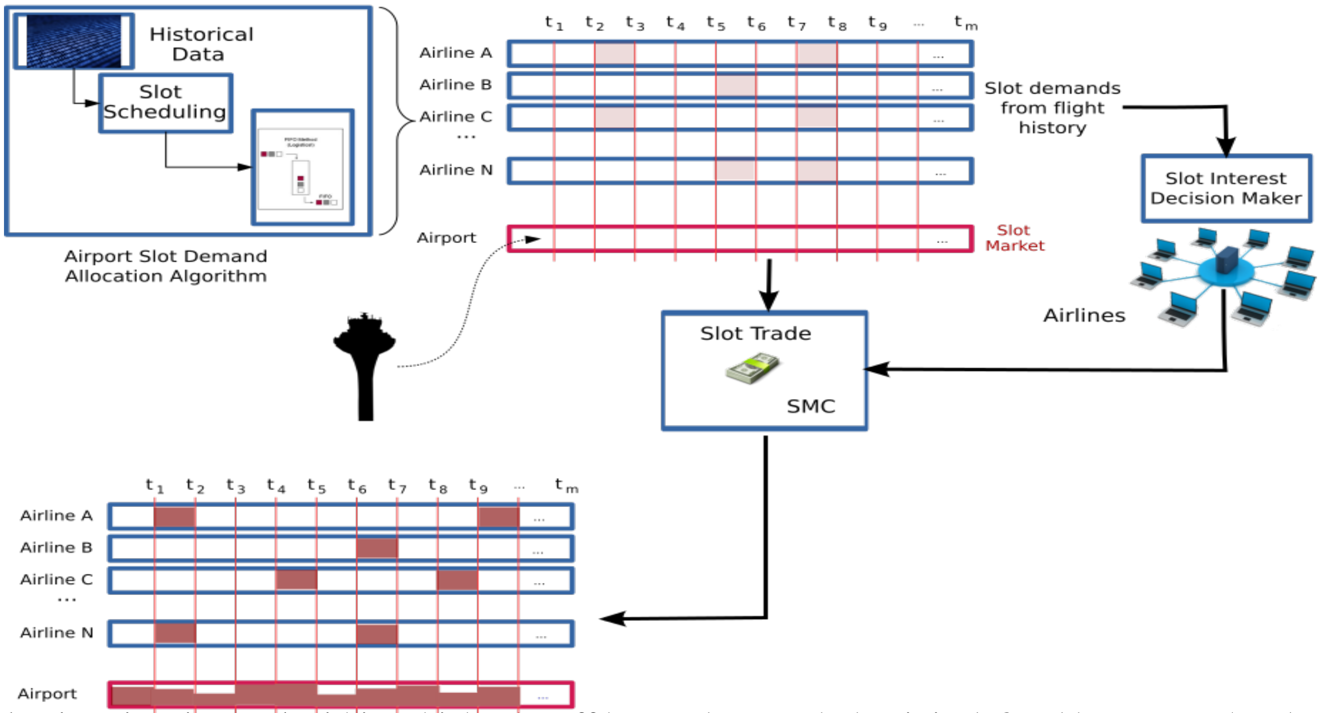
SCENARIO 1 FOR SLOT TRADING



Scenario 1 for Slot Trading

Scenario 1 focuses on initial slot trade from the airports for a long term (6 months before)

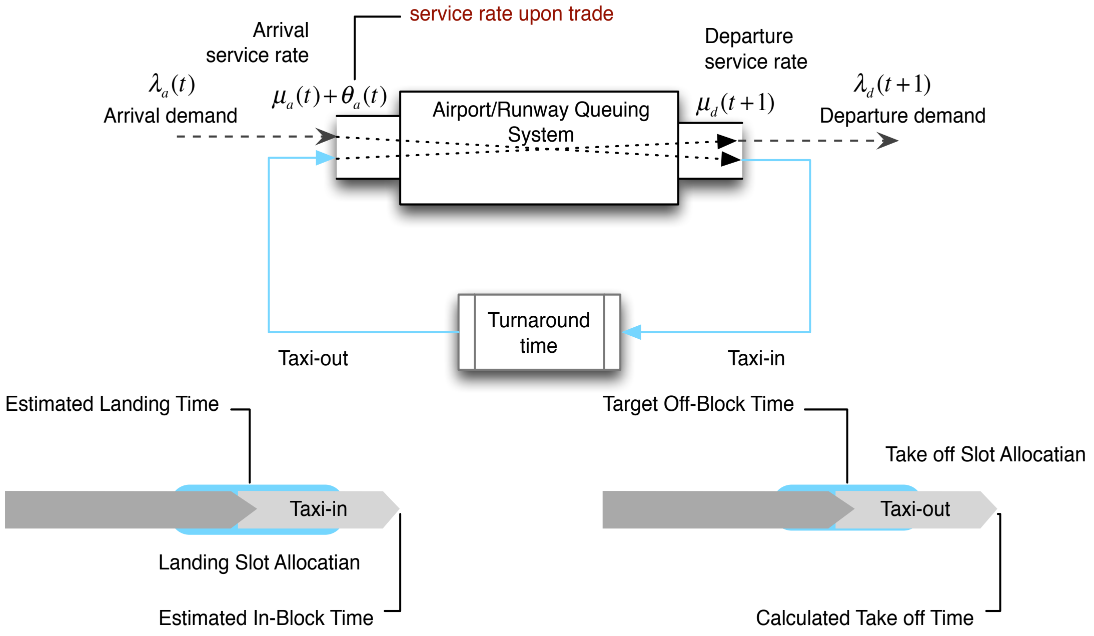
Simulation Model for Scenario #1


Historical Data
Slot Scheduling
Airport Slot Demand Allocation Algorithm
t1 t2 t3 t4 t5 t6 t7 t8 t9 ... tm
Airline A
Airline B
Airline C
...
Airline N
Airport
Slot demands from flight history
Slot Interest Decision Maker
Slot Market
Airlines
Slot Trade
SMC
t1 t2 t3 t4 t5 t6 t7 t8 t9 ... tm
Airline A
Airline B
Airline C
...
Airline N
Airport

slot; is a time interval within which take off has to done such that it is defined between −5 and + 10 minutes from *Calculated Take of Time* – CTOT in Europe (EUROCONTROL 2015).

Slot Demand Allocation Model (SAM)

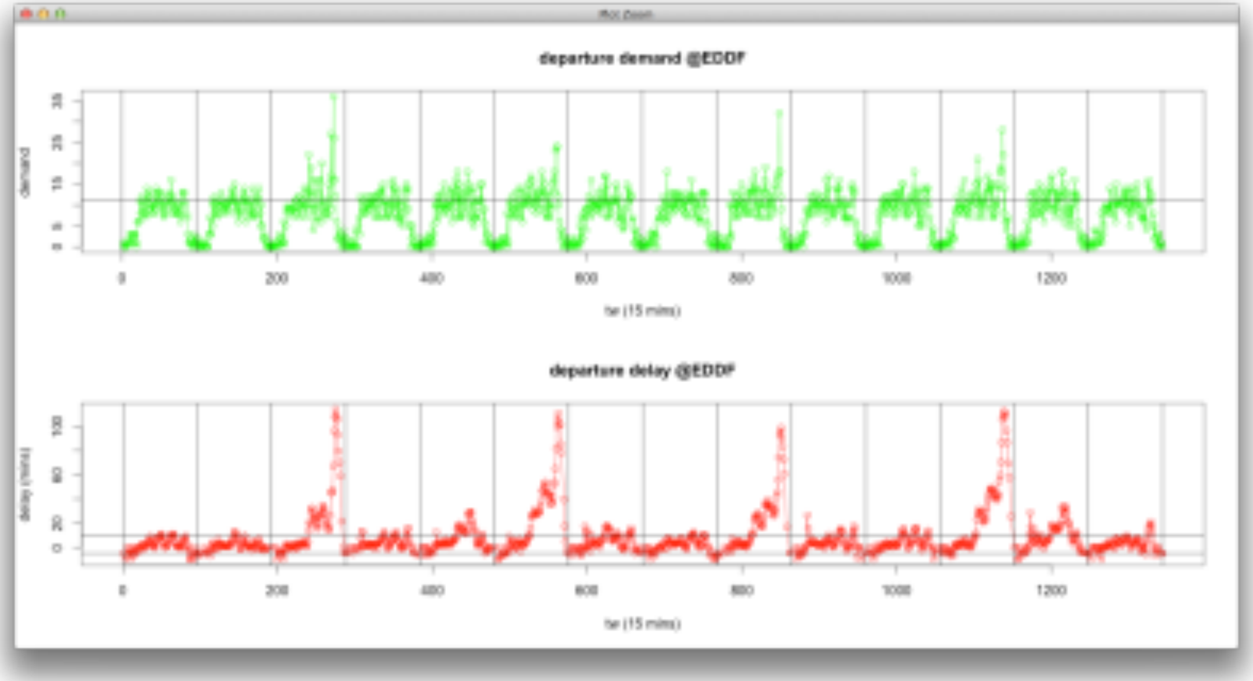
- Airport Queuing Model



– Static/Dynamics distribution of $\mu_a(t)$ to demand $\lambda_a(t)$

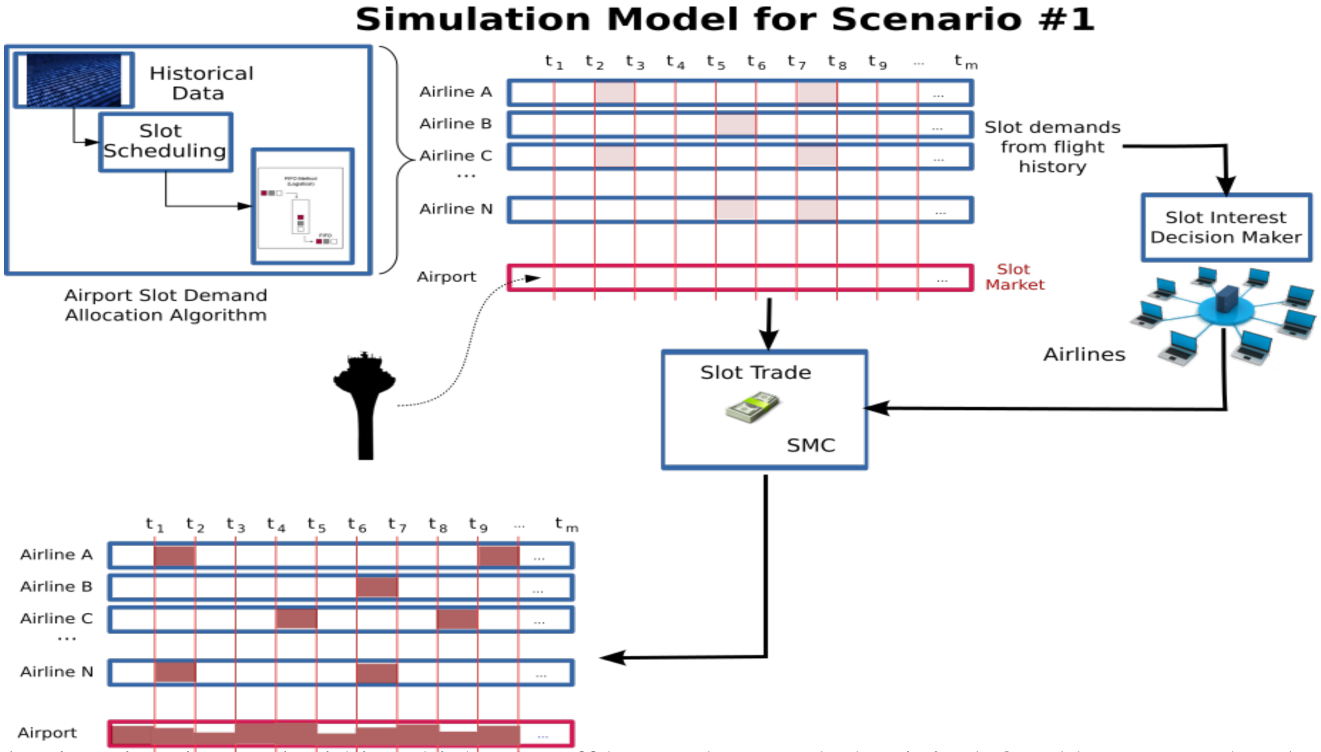
SLOT DEMAND ALLOCATION MODEL (SAM)

- Fill rates of all available slots vary quite a bit across airports
- Current slot capacities are based on the declared arrival and departure capacities



Scenario 1 for Slot Trading

Scenario 1 focuses on initial slot trade from the airports for a long term (6 months before)

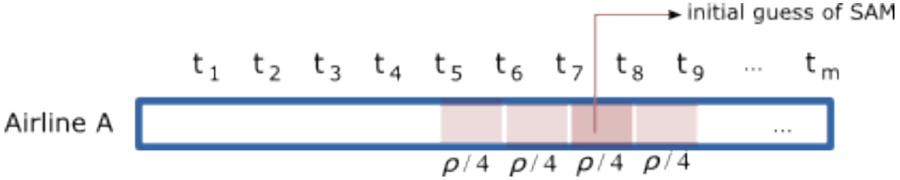

Simulation Model for Scenario #1

Historical Data
Slot Scheduling
Airport Slot Demand Allocation Algorithm
t_1 t_2 t_3 t_4 t_5 t_6 t_7 t_8 t_9 ... t_m
Airline A
Airline B
Airline C
...
Airline N
Airport
Slot demands from flight history
Slot Interest Decision Maker
Slot Market
Airlines
Slot Trade
SMC
t_1 t_2 t_3 t_4 t_5 t_6 t_7 t_8 t_9 ... t_m
Airline A
Airline B
Airline C
...
Airline N
Airport

slot; is a time interval within which take off has to done such that it is defined between −5 and + 10 minutes from *Calculated Take of Time* – CTOT in Europe (EUROCONTROL 2015).

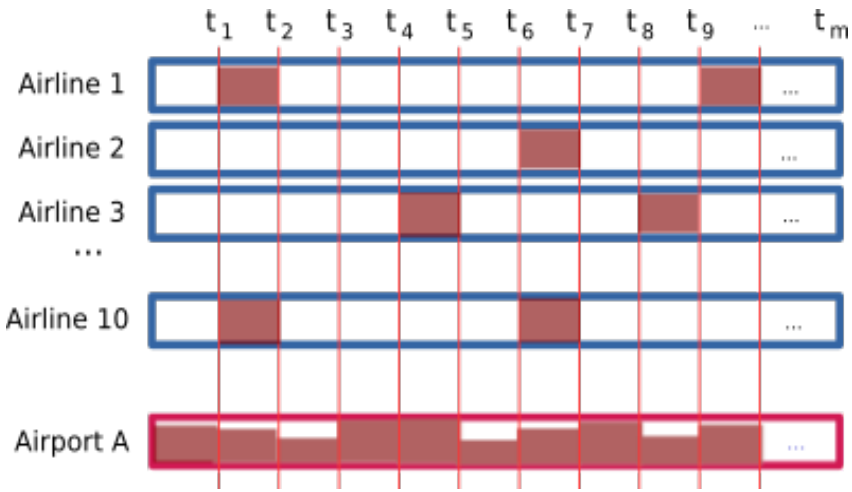
SLOT INTEREST DECISION MAKER (SID)

- *Slot Demand Allocation Model (SAM)* builds schedules for the interest of the airlines.
- Competition begins when at least two airlines want to get same slot exceeding its capacity.


initial guess of SAM
t_1 t_2 t_3 t_4 t_5 t_6 t_7 t_8 t_9 ... t_m
Airline A
...
$\rho/4$ $\rho/4$ $\rho/4$ $\rho/4$

SMC BID COMPARISON

- SMC Engine collects offers.
  - If the result is a tie between two or more participants, the referee provides a notification to the participants and creates a new secure auction.
  - If the minimum price that the seller asks for has not been reached, participants are informed about this.
- Winning price and the winner is disclosed to all participants

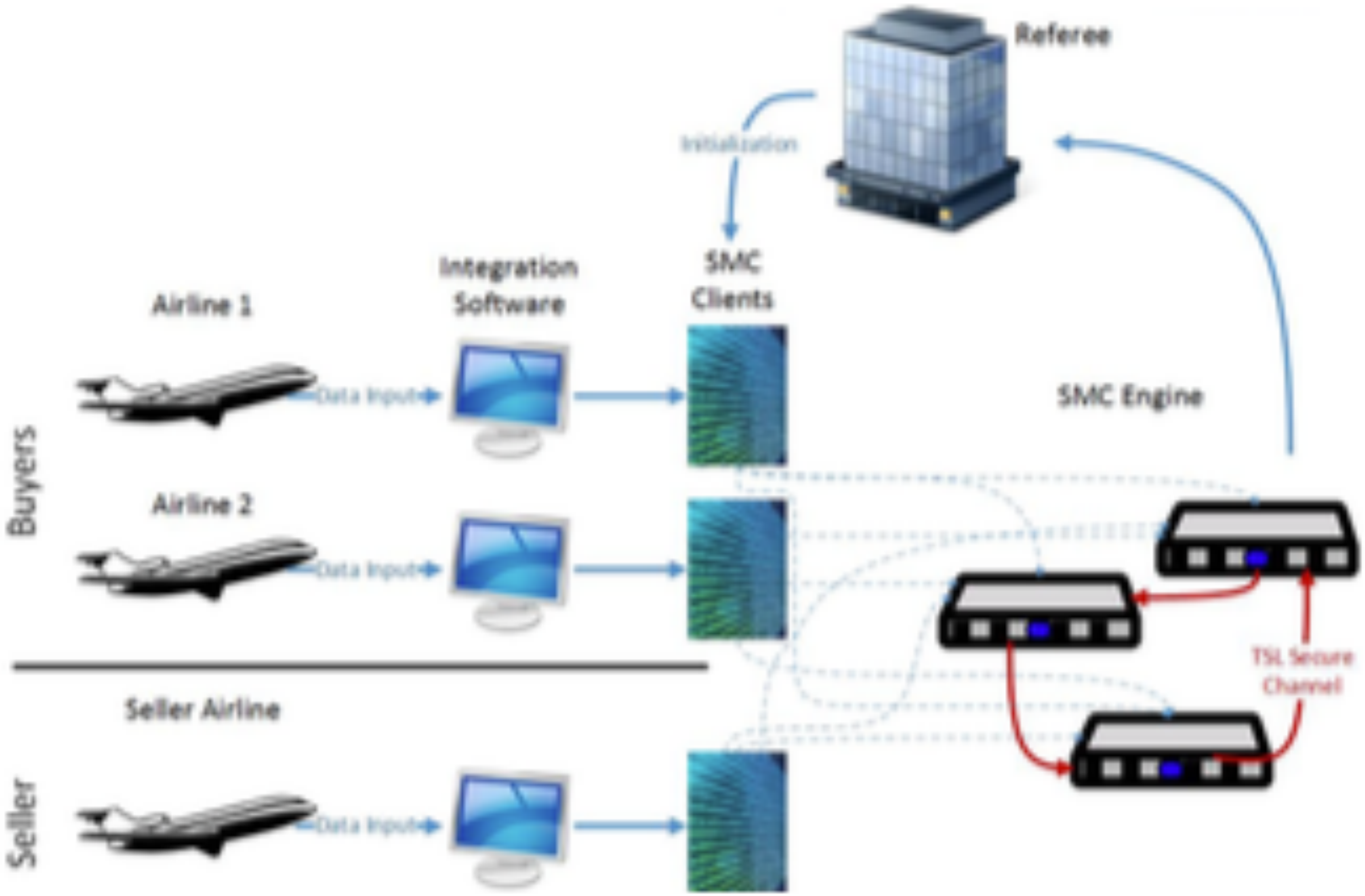


t_1 t_2 t_3 t_4 t_5 t_6 t_7 t_8 t_9 ... t_m
Airline 1
Airline 2
Airline 3
...
Airline 10
Airport A

Slot Trading & Dynamic Landing Queues

Scenario 2

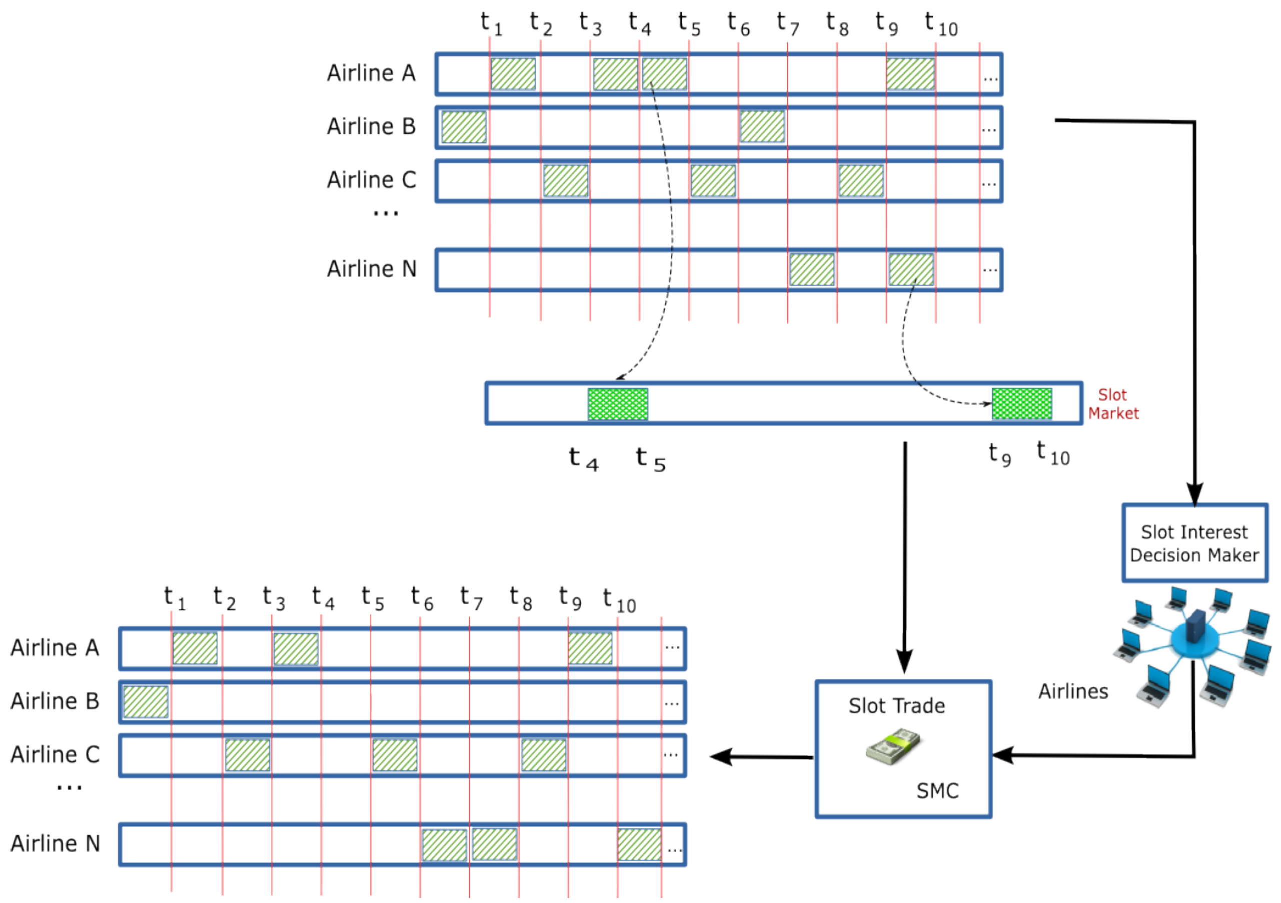
Scenario 2 in Slot Trading



SCENARIO 2 IN SLOT TRADING

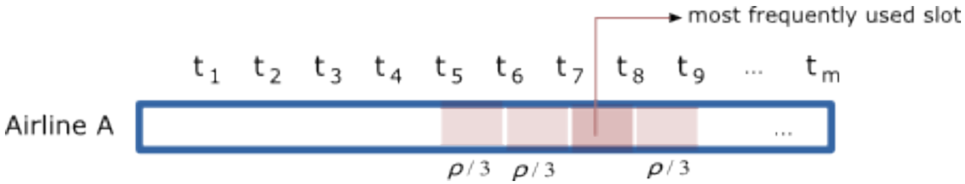
- Scenario 2 focuses on secondary strategic market in which airlines trades their slot between them.

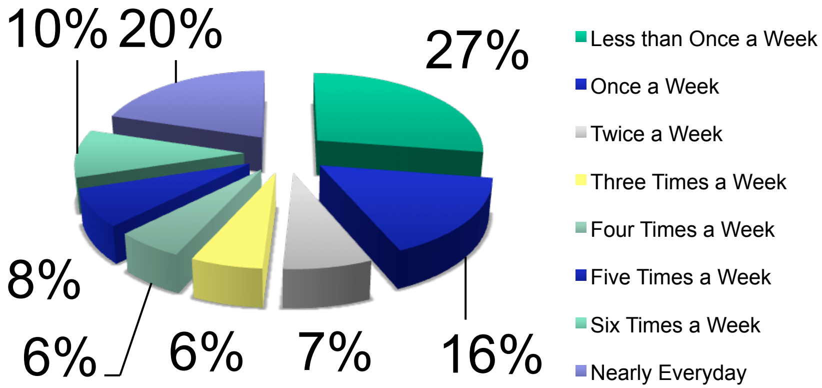
Simulation Model for Scenario #2


t_1 t_2 t_3 t_4 t_5 t_6 t_7 t_8 t_9 t_{10}
Airline A
Airline B
Airline C
...
Airline N
Slot Market
t_4 t_5
t_9 t_{10}
Slot Interest Decision Maker
Airlines
Slot Trade
SMC
t_1 t_2 t_3 t_4 t_5 t_6 t_7 t_8 t_9 t_{10}
Airline A
Airline B
Airline C
...
Airline N

Slot Interest Decision Maker (SID)

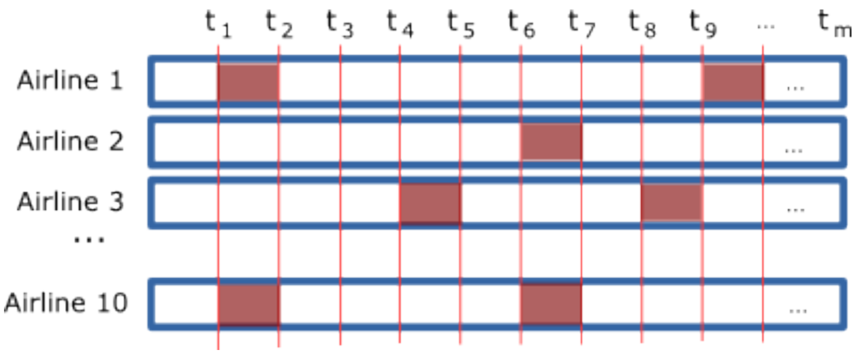
- *Slot Interest Decision Maker (SID)*, hypothetically generates the market and the traders by utilizing flight frequencies
  - The idea behind the concept model is that
    - airlines are interested in selling non-scheduled or least frequently used slots
    - airlines are interested in buying the slots around their most frequently used slots


most frequently used slot
t_1 t_2 t_3 t_4 t_5 t_6 t_7 t_8 t_9 ... t_m
Airline A
...
$\rho/3$ $\rho/3$ $\rho/3$



SMC BID COMPARISON

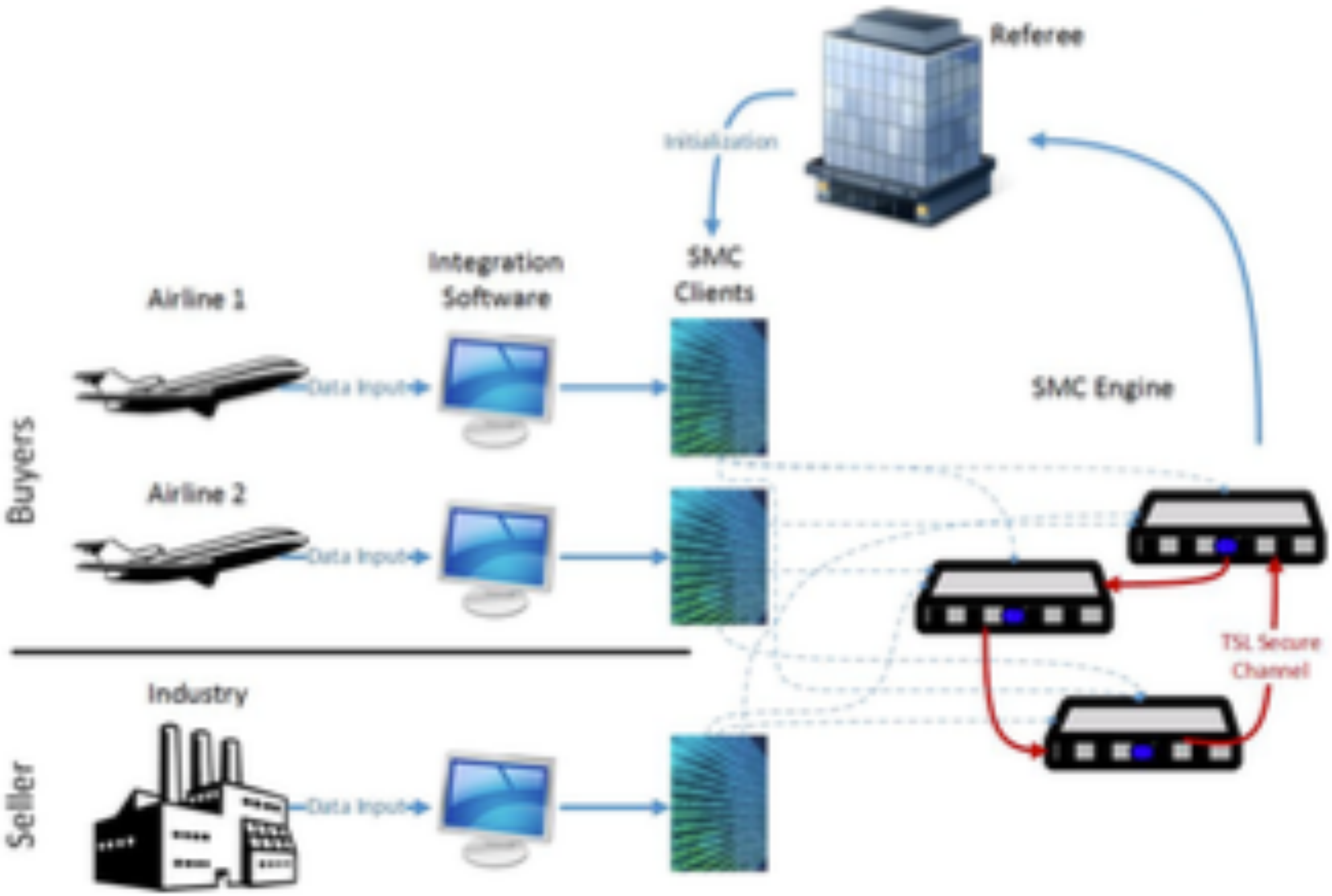
- SMC Engine collects offers.
  - If the result is a tie between two or more participants, the referee provides a notification to the participants and creates a new secure auction.
  - If the minimum price that the seller asks for has not been reached, participants are informed about this.
- Winning price and the winner is disclosed to all participants



Slot Trading & Dynamic Landing Queues

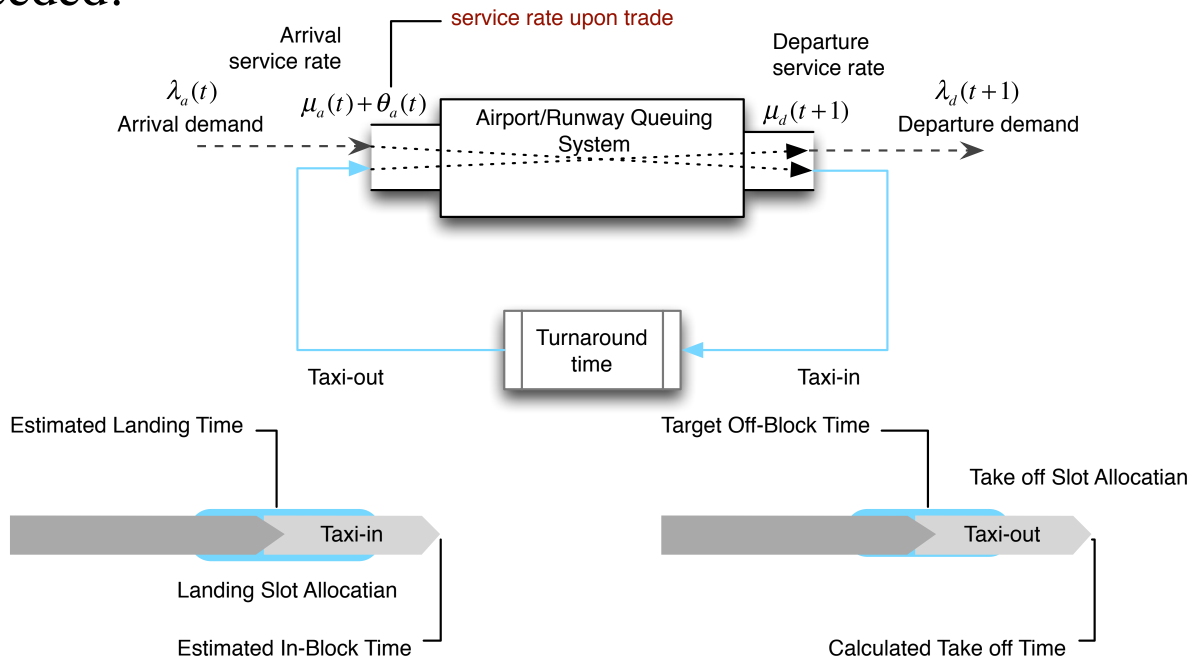
Scenario 3

Scenario 3 for Slot Trading



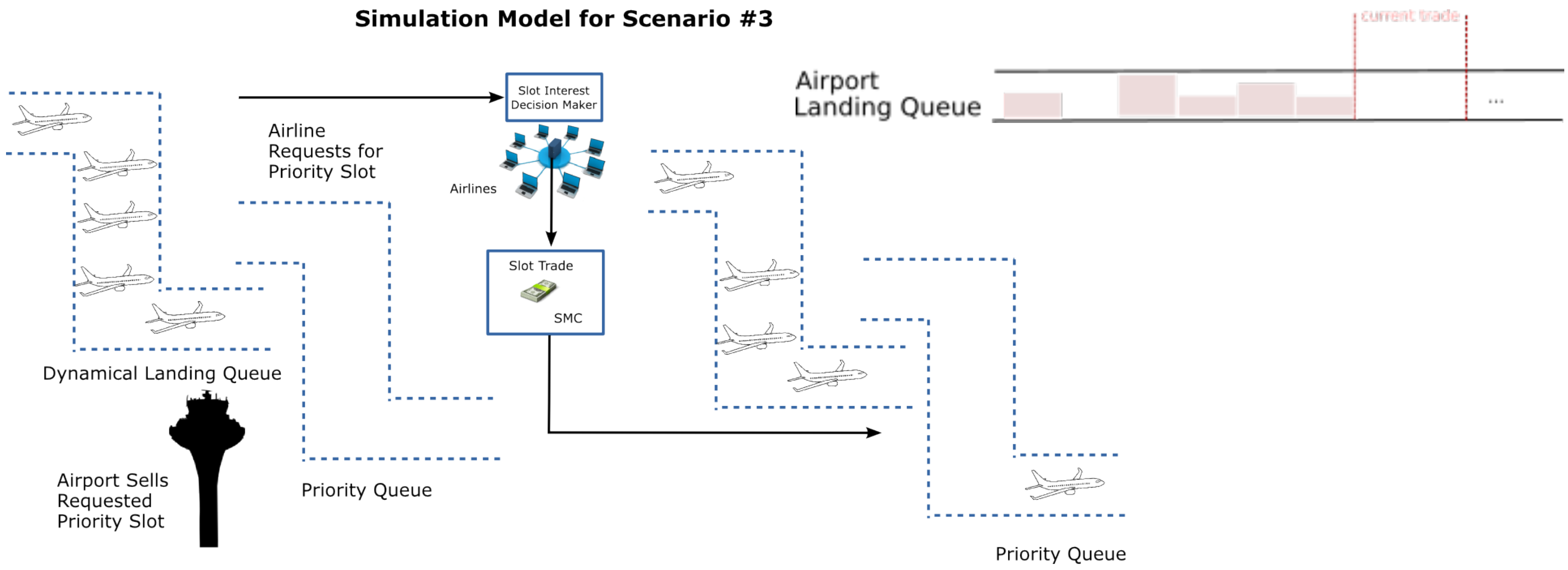
SCENARIO 3

- Scenario 3 focuses on buying a priority landing slot from an airport during approach.
  - Suppose that the airport has an additional runway with capacity $\theta_a(t)$ which is open to trade
  - This particular runway can be utilized in normal operations, however bid customers can have priority utilizing this capacity as needed.

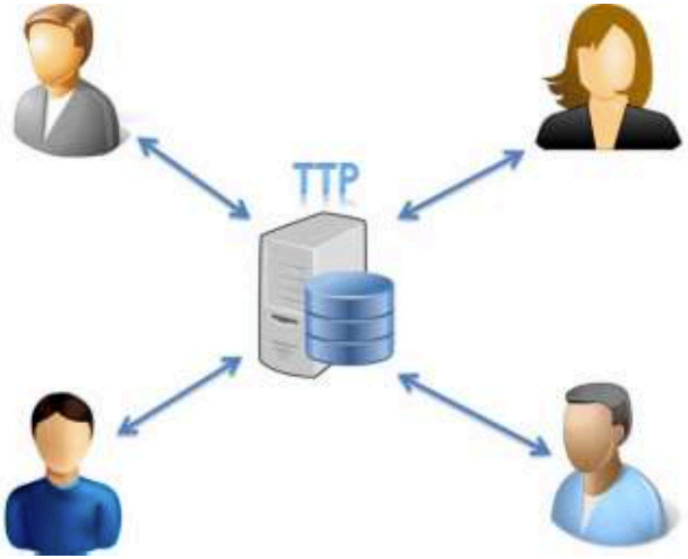


Slot Interest Decision Maker (SID)

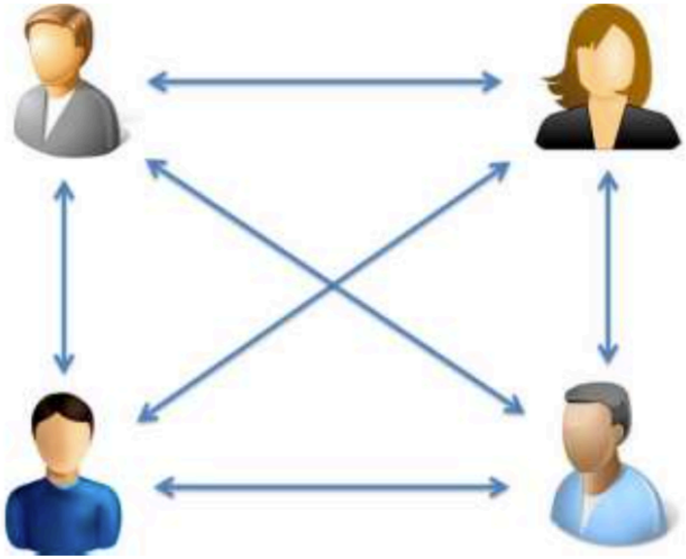
- *Slot Interest Decision Maker (SID)* utilizes current delay
  - Evaluate en-route delays for each landing aircraft.
  - If it is more than 30 minutes, airline is interested in buying a priority slot.


Simulation Model for Scenario #3
current trade
Airport Landing Queue
...
Slot Interest Decision Maker
Airline Requests for Priority Slot
Airlines
Slot Trade
SMC
Dynamical Landing Queue
Airport Sells Requested Priority Slot
Priority Queue
Priority Queue

SECURE MULTIPARTY COMPUTATION



Trusted Third Party (TTP),
Traditional Model



Secure Multiparty Computation
(SMC)

SECURE SHARING?

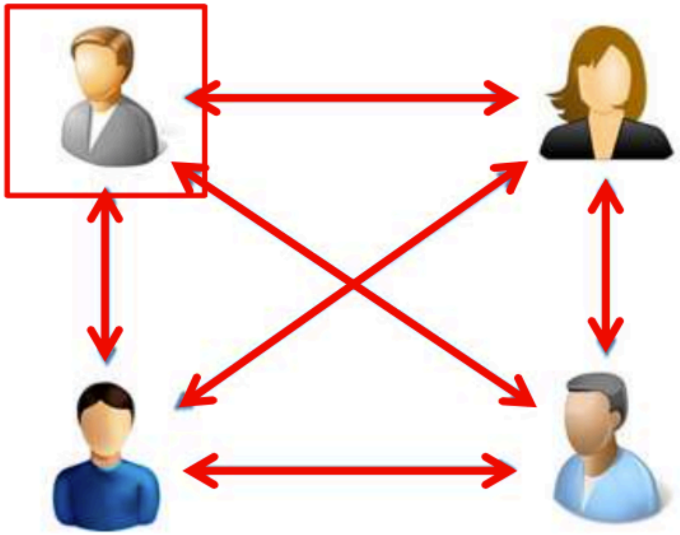
Subfield of cryptography

- Term coined by Yao (1982) in the "Millionaire problem":

  "Two millionaires wish to know who is richer; however, none of them wants the other to find out how much his fortune is worth. How can they know who's the richest?"

- N players wish to securely compute a given function
  - No one learns anything else than its private input and the result of the computation
- Security ensures:
  - the privacy of the player's input
  - The correctness of the computation

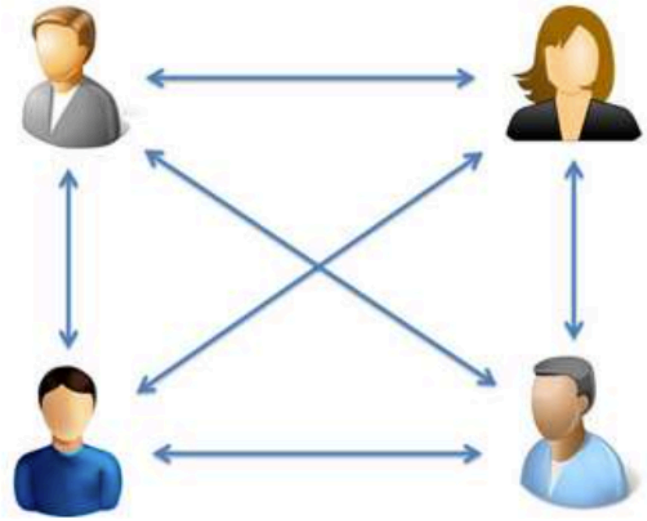
MULTIPARTY?



Party: A **participant** in the secure computation, also called a **player**.

Protocol: In general terms, it describes **how the algorithms should be used, how the players interact.**

SEMI-HONEST PARTY?



Semi-honest party (honest but curious party):

- **parties** in the computation are **corrupted** by a **passive adversary**
- **parties** will always **follow** the **protocol correctly**
- **parties** will try to learn the others private data by examining all the data they get
- the **outcome** of the **computation won't be affected**

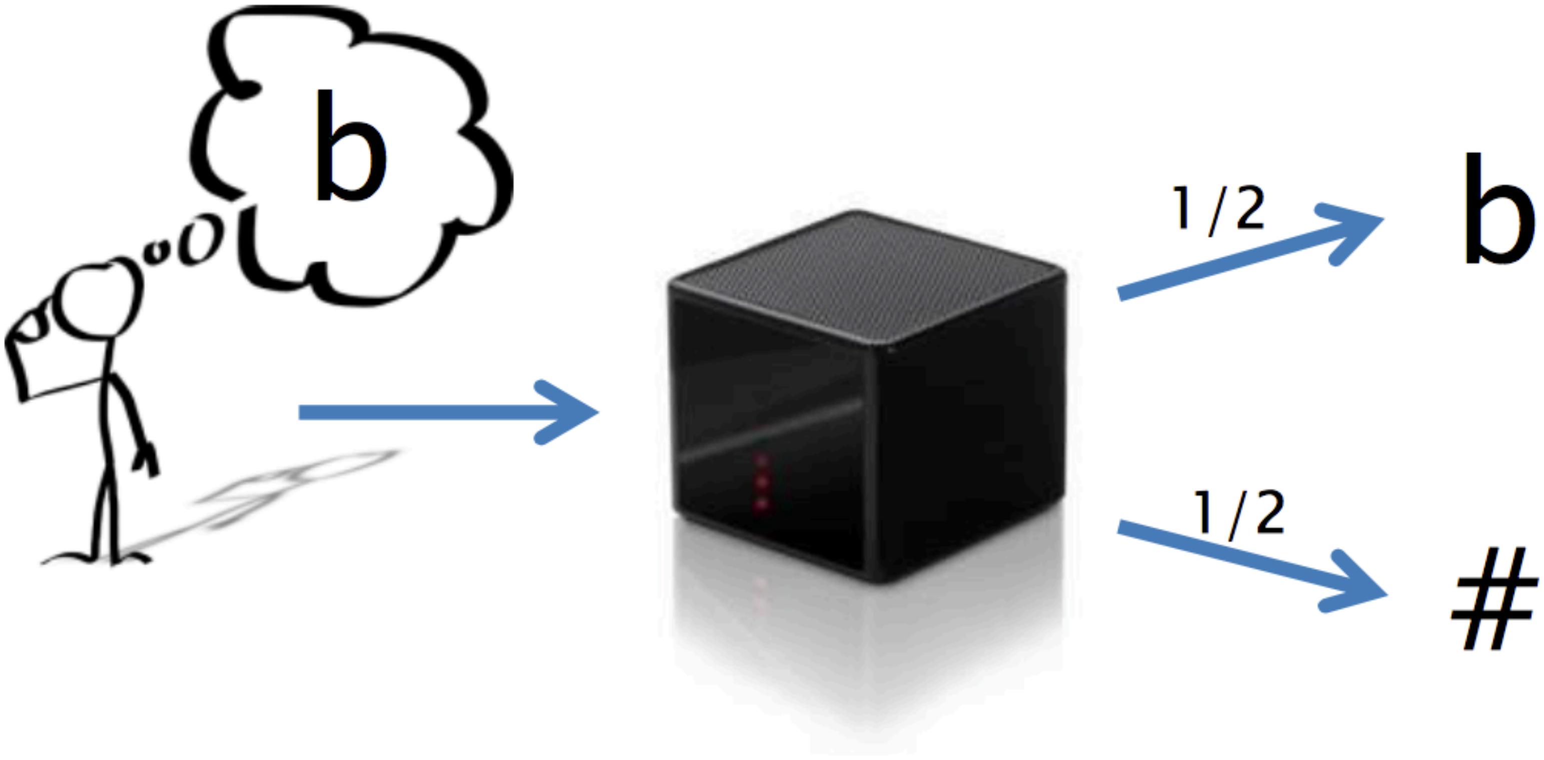
SMC Primitives

Primitive	Remarks	Usage
Oblivious Transfer (OT)	• Sends data with a ½ probability of delivery • Used as an arithmetic black box	Usually used in two-party computations
Secret Sharing (SS)	• Split the private data into shares • Unbreakable without the needed number of shares	Most widely used primitive in the construction of SMC protocols
Homomorphic Encryption (HE)	• Doesn't need to generate shares, it can perform the computation over the encrypted data directly • Very powerful, but complex to implement	Theoretical approach, too costly and complex to implement

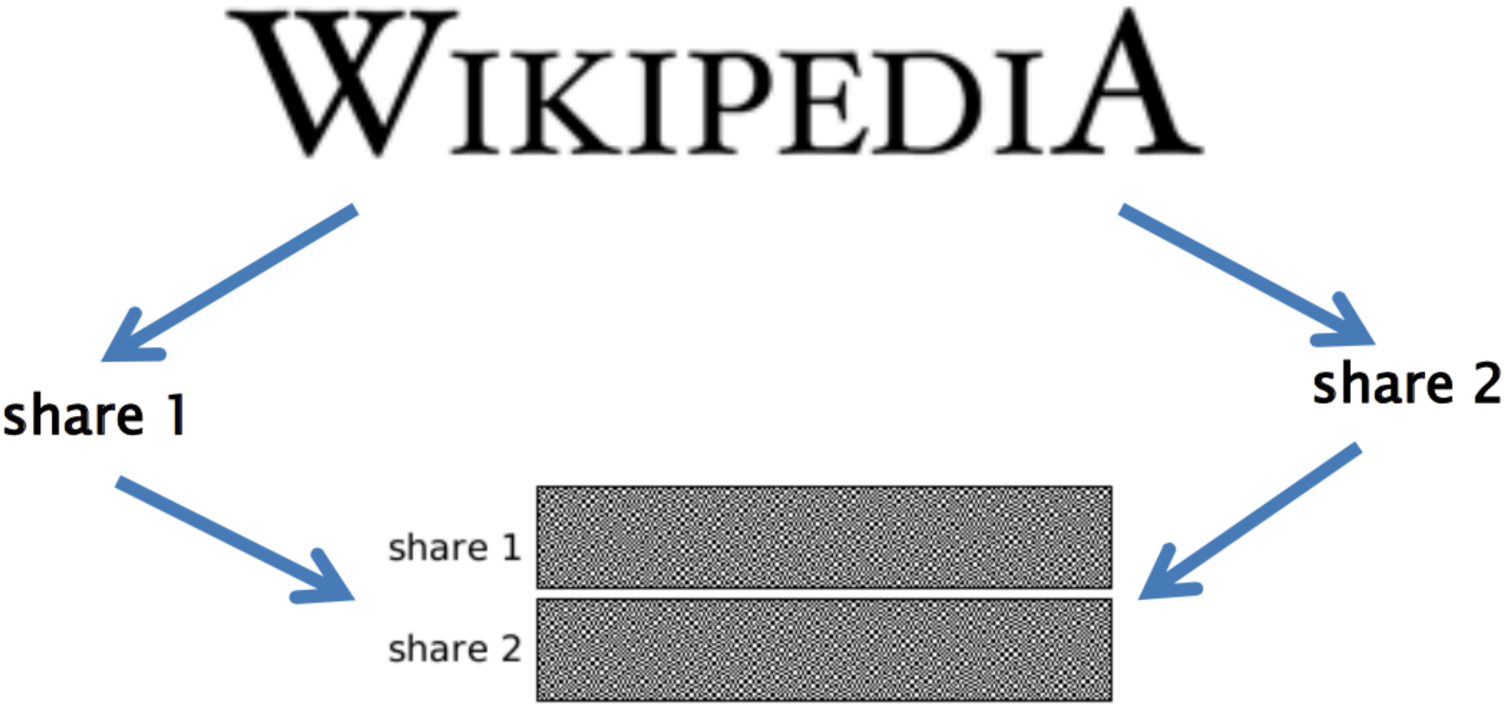
Oblivious Transfer

Rabin's oblivious transfer is kind of formalization of "noisy wire" communication

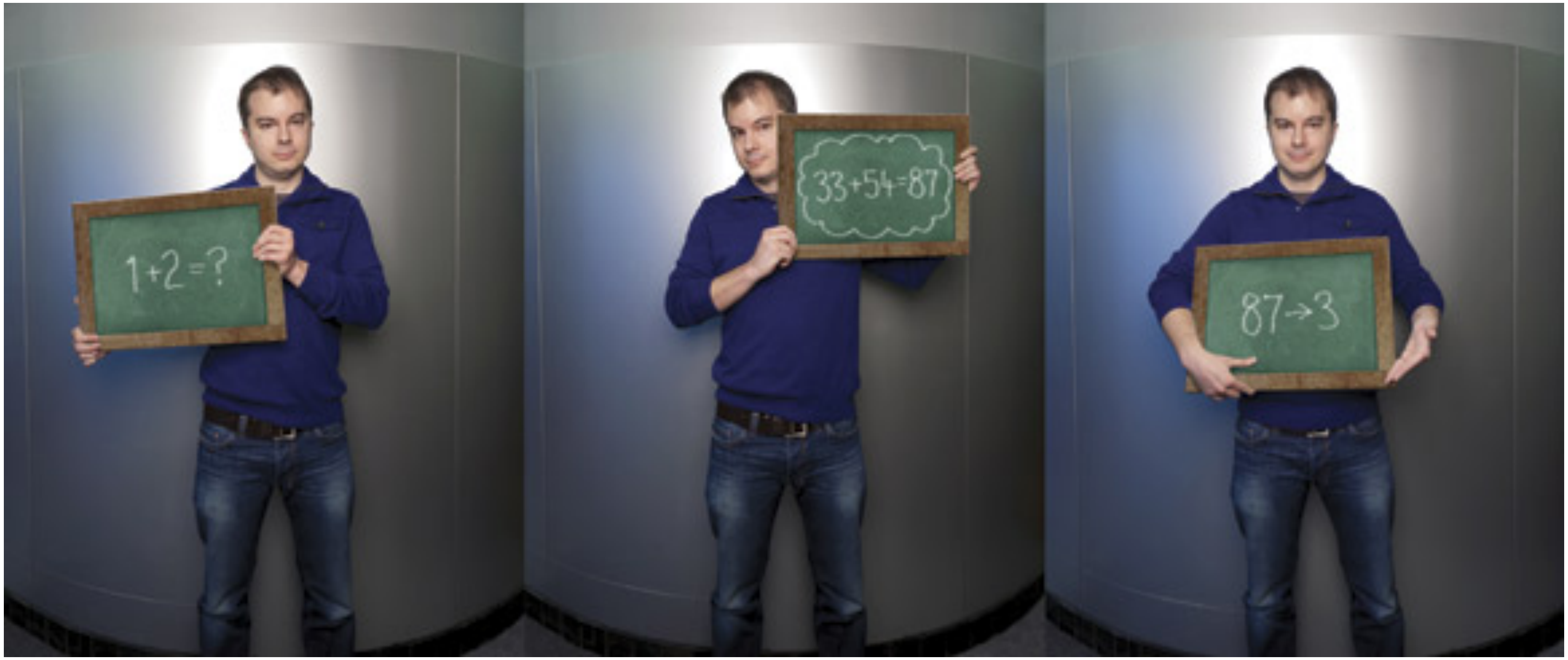
- Sender sends bit b into OT machine
- Machine then flips the coin, and with probability 1/2 sends b to receiver.
- Sender does not know which output receiver received



Secret Sharing

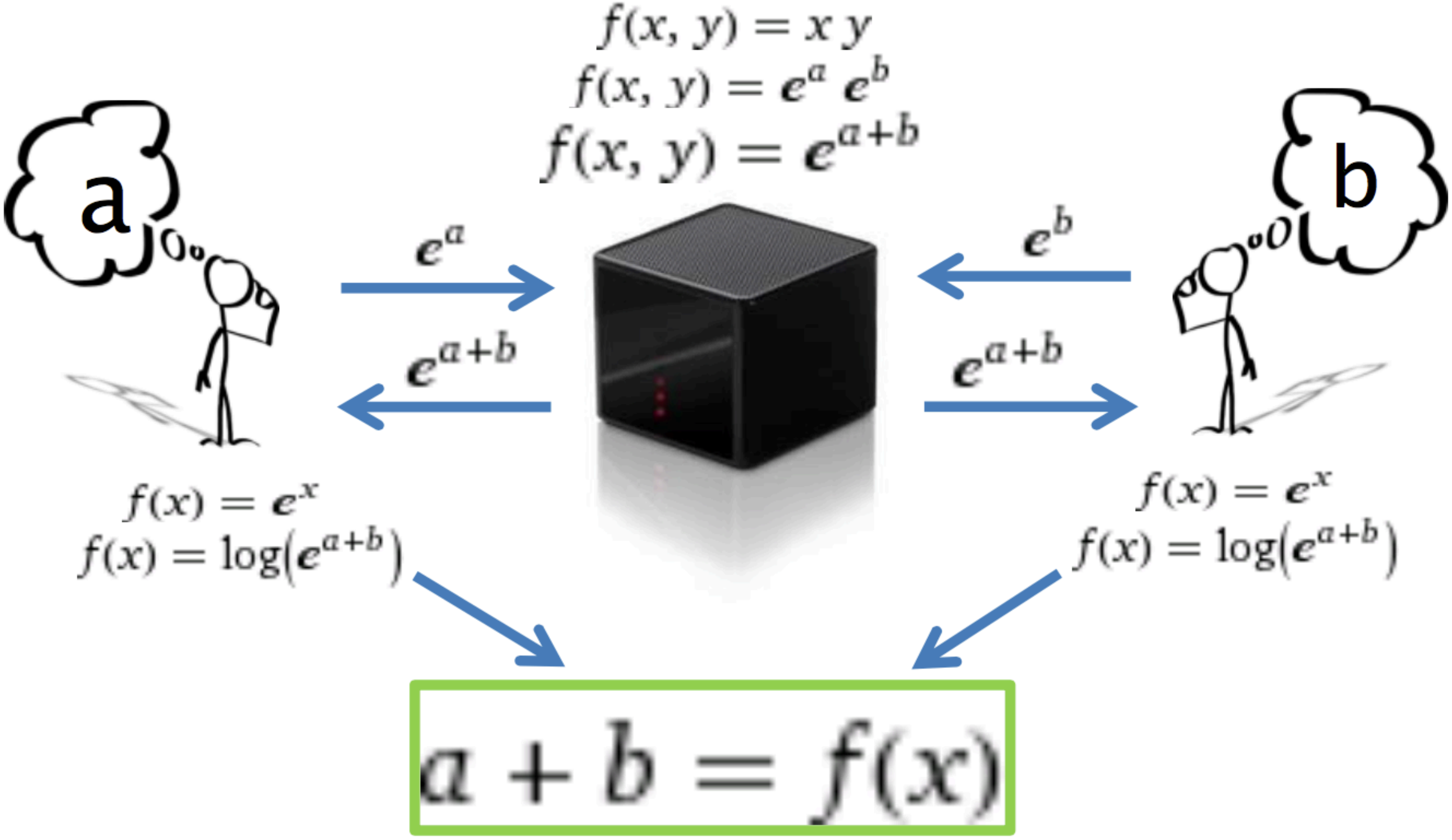


Homomorphic Encryption



Let’s calculate a + b!

$\exp(x+y) = (\exp x)(\exp y)$



$f(x, y) = x\,y$

$f(x, y) = e^a\, e^b$

$f(x, y) = e^{a+b}$

e^a

e^{a+b}

e^b

e^{a+b}

$f(x) = e^x$

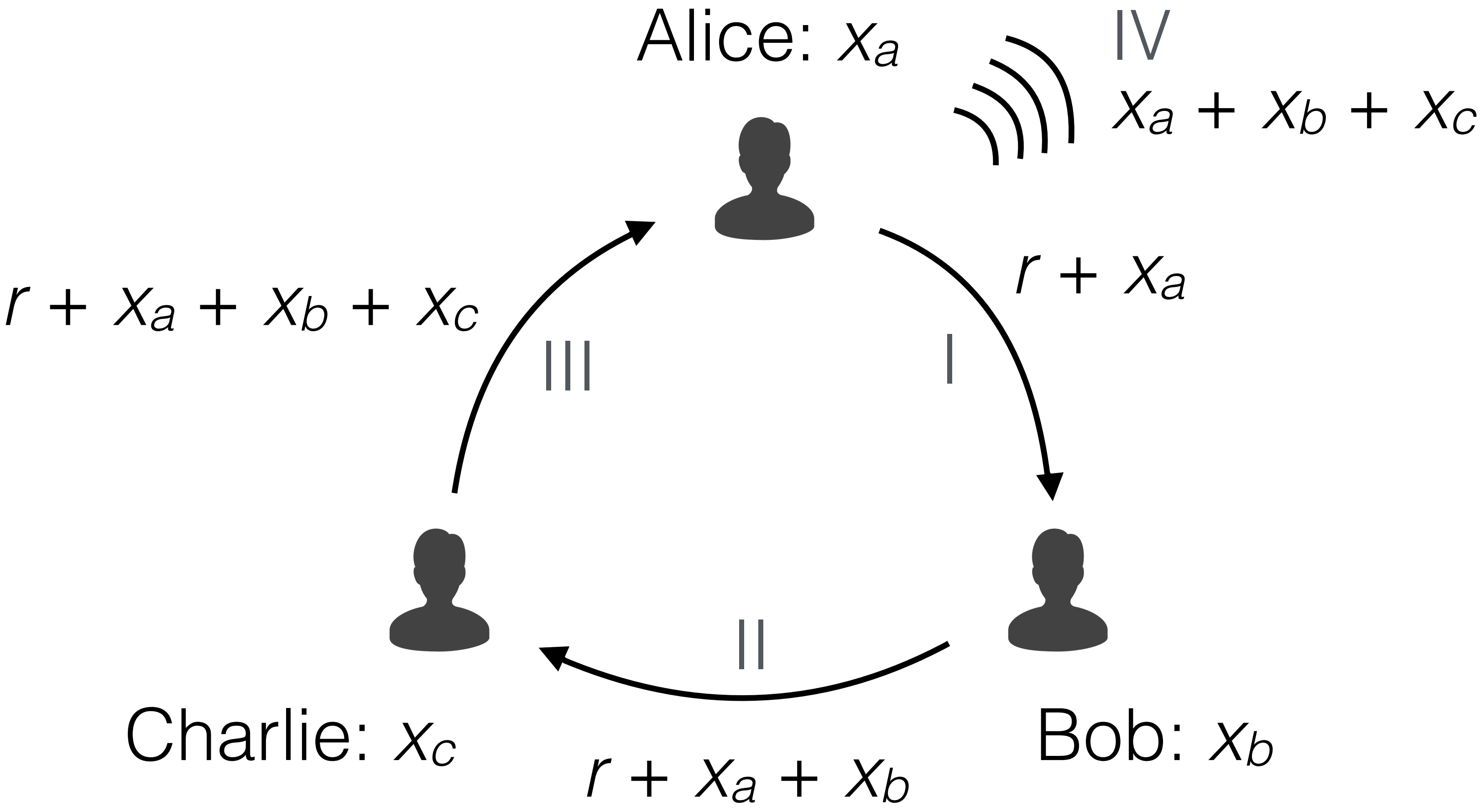
$f(x) = \log(e^{a+b})$

$f(x) = e^x$

$f(x) = \log(e^{a+b})$

$$\boxed{a + b = f(x)}$$

Secret Sharing (I)



Alice: x_a

IV

$x_a + x_b + x_c$

$r + x_a$

I

$r + x_a + x_b + x_c$

III

II

Charlie: x_c

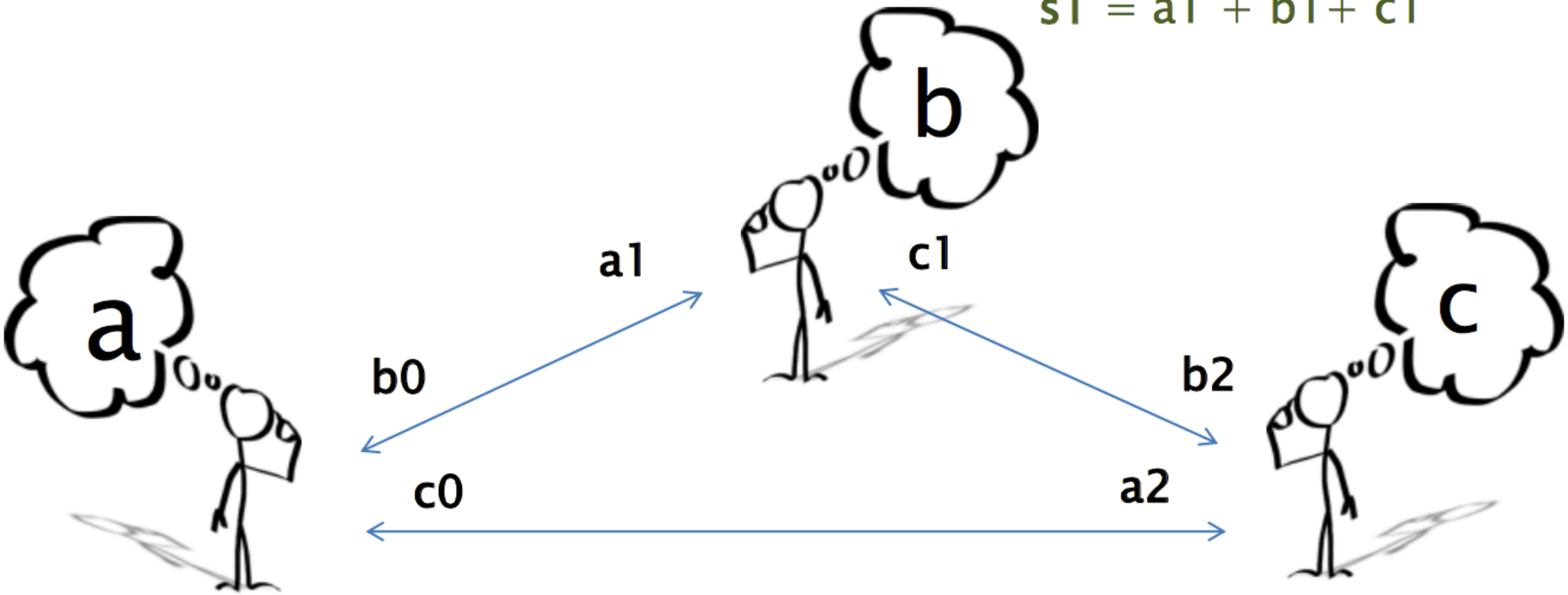
$r + x_a + x_b$

Bob: x_b

Secret Sharing (II)

Let's *securely* calculate a + b + c!

b = b0 + b1 + b2
s1 = a1 + b1 + c1

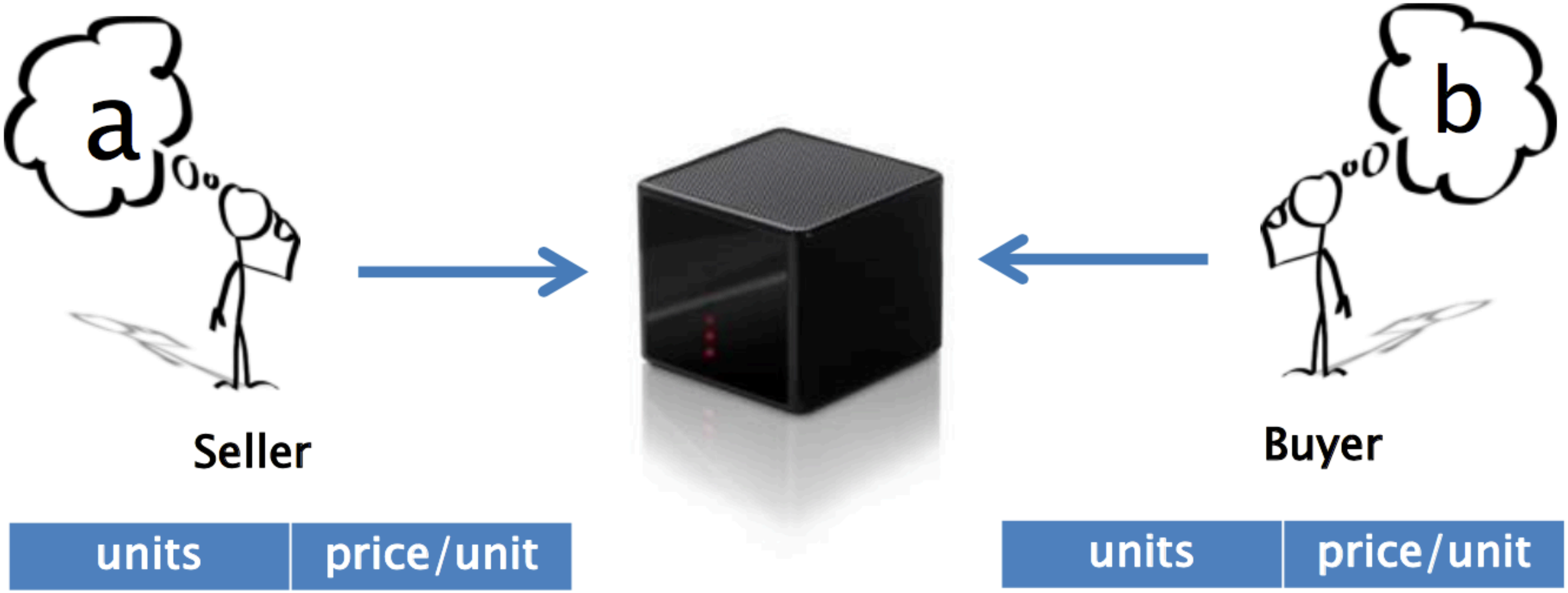


a = a0 + a1 + a2
s0 = a0 + b0 + c0

c = c0 + c1 + c2
s2 = a2 + b2 + c2

$$\boxed{s0 + s1 + s2 = a + b + c}$$

SECURE BIDDING

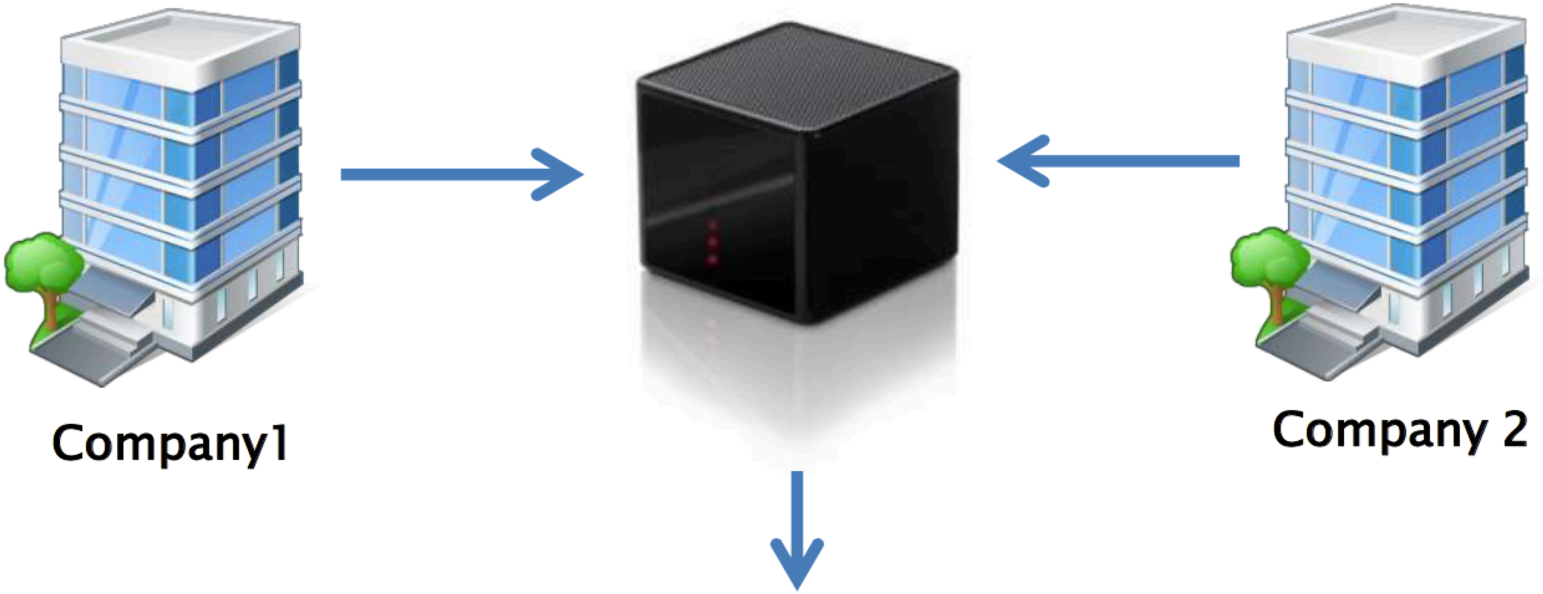


units	price/unit
1	20
2	9
3	5,5

Market clearance price

units	price/unit
1	18
2	9
3	5

Third Party SMC Engine



Sector benchmarking:

- Statistical Data
- Strategic Ranking
- Anonymity