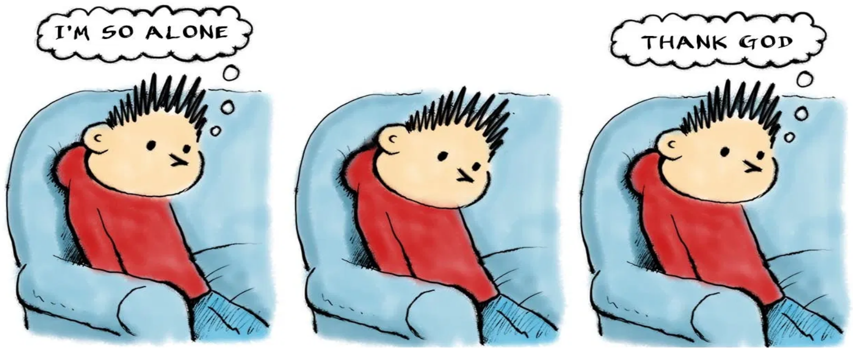
On the Round Complexity of Fully Secure Solitary MPC with Honest Majority

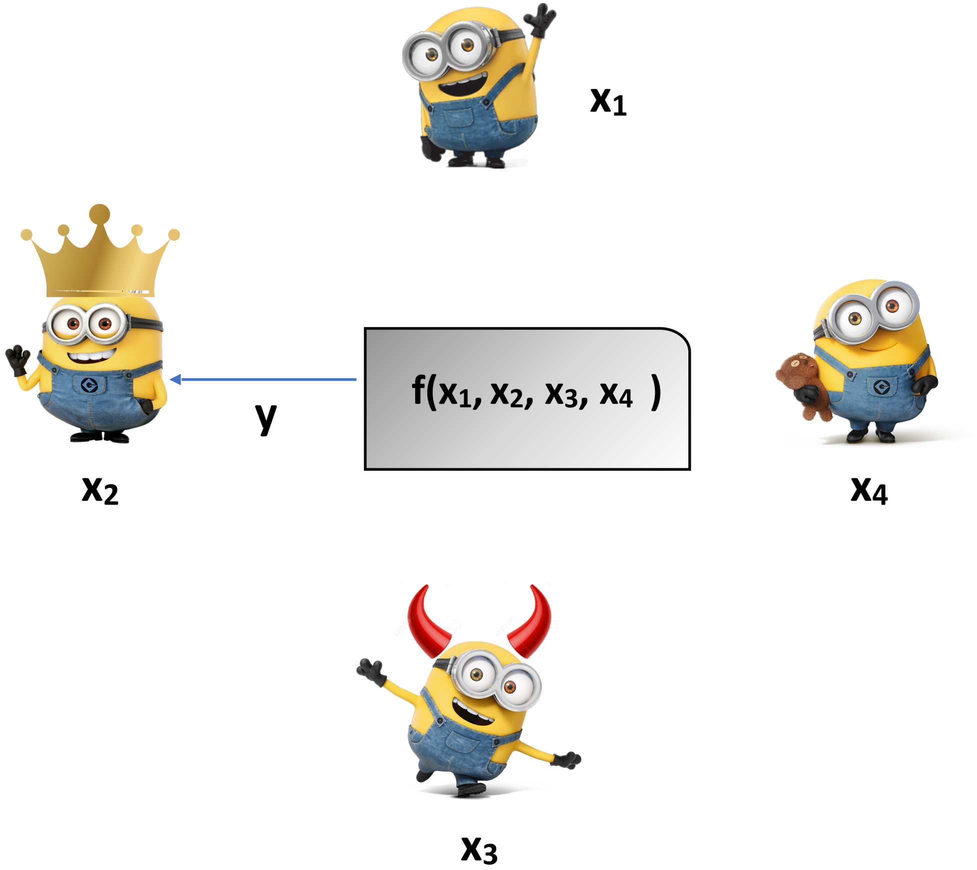
Saikrishna Badrinarayanan, Peihan Miao, Pratyay Mukherjee and **Divya Ravi**

TCC 2023

in BROWN SUPRA ORACLES UNIVERSITY OF AMSTERDAM

Solitary MPC





x_1

x_2

y

$f(x_1, x_2, x_3, x_4\ )$

x_4

x_3

MPC: allows group of parties to securely compute joint function on private inputs

Solitary MPC: only a *single* designated party obtains output

Standard MPC vs Solitary MPC

Standard MPC vs Solitary MPC

Full Security (G.O.D) in dishonest majority	Impossible [Cleve 86]	Impossible [HIKMR19]

	Standard MPC vs	Solitary MPC
Full Security (G.O.D) in dishonest majority	Impossible [Cleve 86]	Impossible [HIKMR19]

G.O.D in Honest Majority: [HIKMR19, FGMO05]
Need to assume either broadcast or PKI

Standard MPC vs Solitary MPC

	Standard MPC	Solitary MPC
Full Security (G.O.D) in dishonest majority	Impossible [Cleve 86]	Impossible [HIKMR19]
G.O.D with PKI and Broadcast	2 rounds [HLP11, GLS15]	2 rounds [HLP11, GLS15]

G.O.D in Honest Majority: [HIKMR19, FGMO05]
Need to assume either broadcast or PKI

Standard MPC vs Solitary MPC

	Standard MPC	Solitary MPC
Full Security (G.O.D) in dishonest majority	Impossible [Cleve 86]	Impossible [HIKMR19]
G.O.D with PKI and Broadcast	2 rounds [HLP11, GLS15]	2 rounds [HLP11, GLS15]
G.O.D with Broadcast (no PKI)		

G.O.D in Honest Majority: [HIKMR19, FGMO05]
Need to assume either broadcast or PKI

Standard MPC vs Solitary MPC

Full Security (G.O.D) in dishonest majority	Impossible [Cleve 86]	Impossible [HIKMR19]
G.O.D with PKI and Broadcast	2 rounds [HLP11, GLS15]	2 rounds [HLP11, GLS15]
G.O.D with Broadcast (no PKI)	3 rounds [GIKR02, GLS15, PR18, BJMS18, ACGJ18]	

G.O.D in Honest Majority: [HIKMR19, FGMO05]
Need to assume either broadcast or PKI

Standard MPC vs Solitary MPC

	Standard MPC	Solitary MPC
Full Security (G.O.D) in dishonest majority	Impossible [Cleve 86]	Impossible [HIKMR19]
	G.O.D in Honest Majority: [HIKMR19, FGMO05] Need to assume either broadcast or PKI	
G.O.D with PKI and Broadcast	2 rounds [HLP11, GLS15]	2 rounds [HLP11, GLS15]
G.O.D with Broadcast (no PKI)	3 rounds [GIKR02, GLS15, PR18, BJMS18, ACGJ18]	3 rounds [**This Work**, BJMS18, ACGJ18]

Standard MPC vs Solitary MPC

Full Security (G.O.D) in dishonest majority	Impossible [Cleve 86]	Impossible [HIKMR19]

G.O.D in Honest Majority: [HIKMR19, FGMO05]
Need to assume either broadcast or PKI

G.O.D with PKI and Broadcast	2 rounds [HLP11, GLS15]	2 rounds [HLP11, GLS15]
G.O.D with Broadcast (no PKI)	3 rounds [GIKR02, GLS15, PR18, BJMS18, ACGJ18]	3 rounds [This W BJMS18, A

Broadcast is necessary in first and second round

Standard MPC vs Solitary MPC

	Standard MPC	Solitary MPC
Full Security (G.O.D) in dishonest majority	Impossible [Cleve 86]	Impossible [HIKMR19]
	G.O.D in Honest Majority: [HIKMR19, FGMO05] Need to assume either broadcast or PKI	
G.O.D with PKI and Broadcast	2 rounds [HLP11, GLS15]	2 rounds [HLP11, GLS15]
G.O.D with Broadcast (no PKI)	3 rounds [GIKR02, GLS15, PR18, BJMS18, ACGJ18]	3 rounds [**This Work**, BJMS18, ACGJ18]

Standard MPC vs Solitary MPC

	Standard MPC	Solitary MPC
Full Security (G.O.D) in dishonest majority	Impossible [Cleve 86]	Impossible [HIKMR19]
	G.O.D in Honest Majority: [HIKMR19, FGMO05] Need to assume either broadcast or PKI	
G.O.D with PKI and Broadcast	2 rounds [HLP11, GLS15]	2 rounds [HLP11, GLS15]
G.O.D with Broadcast (no PKI)	3 rounds [GIKR02, GLS15, PR18, BJMS18, ACGJ18]	3 rounds [**This Work**, BJMS18, ACGJ18]
G.O.D with PKI (no broadcast)		

Standard MPC vs Solitary MPC

Full Security (G.O.D) in dishonest majority	Impossible [Cleve 86]	Impossible [HIKMR19]
G.O.D with PKI and Broadcast	2 rounds [HLP11, GLS15]	2 rounds [HLP11, GLS15]
G.O.D with Broadcast (no PKI)	3 rounds [GIKR02, GLS15, PR18, BJMS18, ACGJ18]	3 rounds [**This Work**, BJMS18, ACGJ18]
G.O.D with PKI (no broadcast)	Ω (t) rounds [DS83]	

G.O.D in Honest Majority: [HIKMR19, FGMO05]
Need to assume either broadcast or PKI

Standard MPC vs Solitary MPC

	Standard MPC	Solitary MPC
Full Security (G.O.D) in dishonest majority	Impossible [Cleve 86]	Impossible [HIKMR19]

G.O.D in Honest Majority: [HIKMR19, FGMO05]
Need to assume either broadcast or PKI

	Standard MPC	Solitary MPC
G.O.D with PKI and Broadcast	2 rounds [HLP11, GLS15]	2 rounds [HLP11, GLS15]
G.O.D with Broadcast (no PKI)	3 rounds [GIKR02, GLS15, PR18, BJMS18, ACGJ18]	3 rounds [**This Work**, BJMS18, ACGJ18]
G.O.D with PKI (no broadcast)	Ω (t) rounds [DS83]	4 rounds necessary 5 rounds sufficient [**This Work**]

Standard MPC vs Solitary MPC

	Standard MPC	Solitary MPC
Full Security (G.O.D) in dishonest majority	Impossible [Cleve 86]	Impossible [HIKMR19]
G.O.D with PKI and Broadcast	2 rounds [HLP11, GLS15]	2 rounds [HLP11, GLS15]
G.O.D with Broadcast (no PKI)	3 rounds [GIKR02, GLS15, PR18, BJMS18, ACGJ18]	3 rounds [This Work BJMS18, AC
G.O.D with PKI (no broadcast)	Ω (t) rounds [DS83]	4 rounds neces 5 rounds suffici [This Work]

G.O.D in Honest Majority: [HIKMR19, FGMO05]
Need to assume either broadcast or PKI

t >= 3

Study special cases
t = 1, 2

5-Round upper bound with PKI (no broadcast)

5-Round upper bound with PKI (no broadcast)

[GLS15] 2-round (non-solitary) G.O.D protocol using PKI and Broadcast

5-Round upper bound with PKI (no broadcast)

[GLS15] 2-round (non-solitary) G.O.D protocol using PKI and Broadcast

n = 3, t = 1

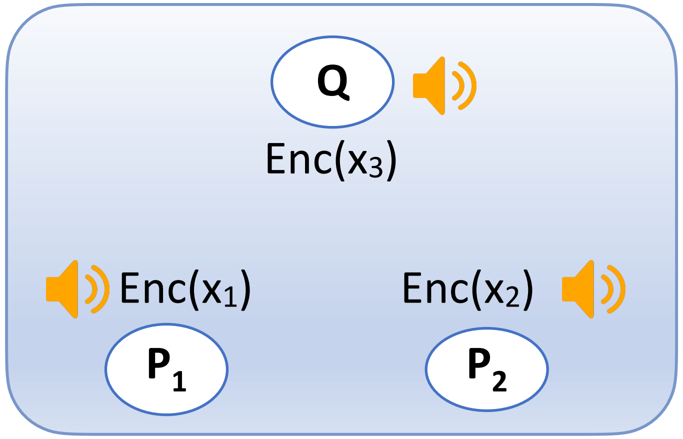
Decentralized threshold FHE Setup:

pk, sk_1 , sk_2 , sk_3

5-Round upper bound with PKI (no broadcast)

[GLS15] 2-round (non-solitary) G.O.D protocol using PKI and Broadcast

$n = 3, t = 1$



Q

Enc(x_3)

Enc(x_1)

Enc(x_2)

P_1

P_2

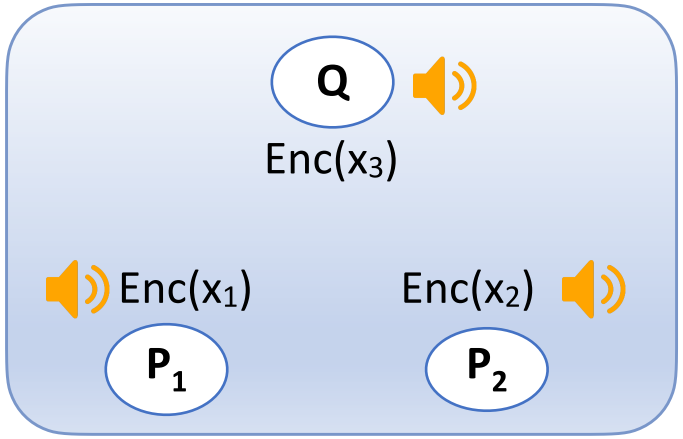
Decentralized threshold FHE Setup:

pk, sk_1, sk_2, sk_3

5-Round upper bound with PKI (no broadcast)

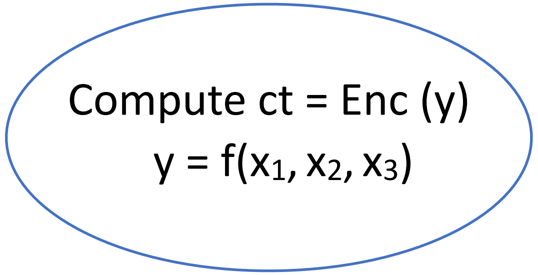
[GLS15] 2-round (non-solitary) G.O.D protocol using PKI and Broadcast

n = 3, t = 1



Decentralized threshold FHE Setup:

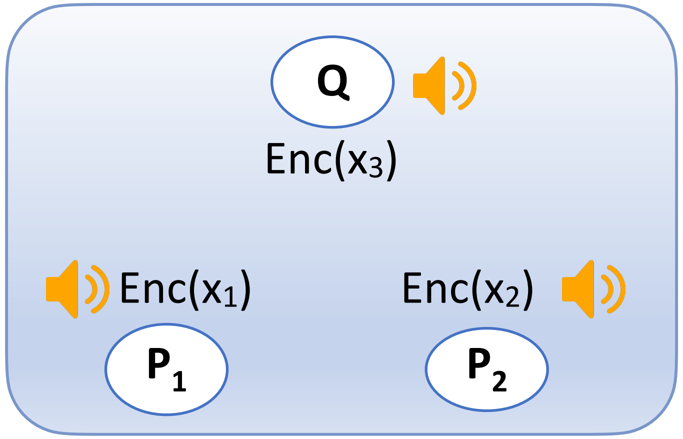
pk, sk_1 , sk_2 , sk_3



5-Round upper bound with PKI (no broadcast)

[GLS15] 2-round (non-solitary) G.O.D protocol using PKI and Broadcast

n = 3, t = 1

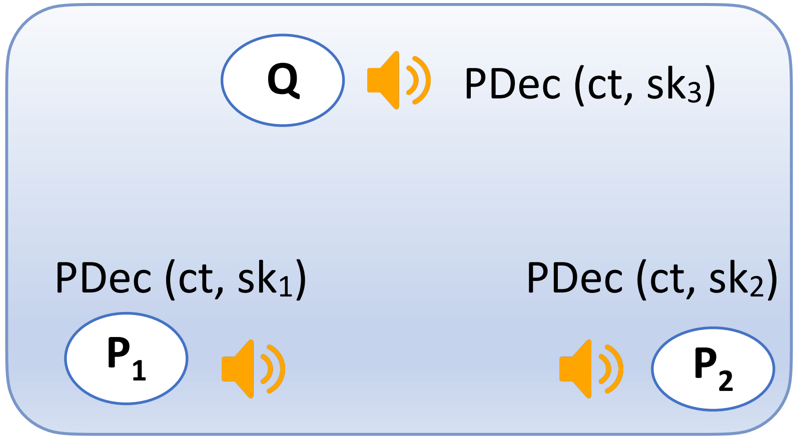


Decentralized threshold FHE Setup:

pk, sk_1 , sk_2 , sk_3

Compute ct = Enc (y)

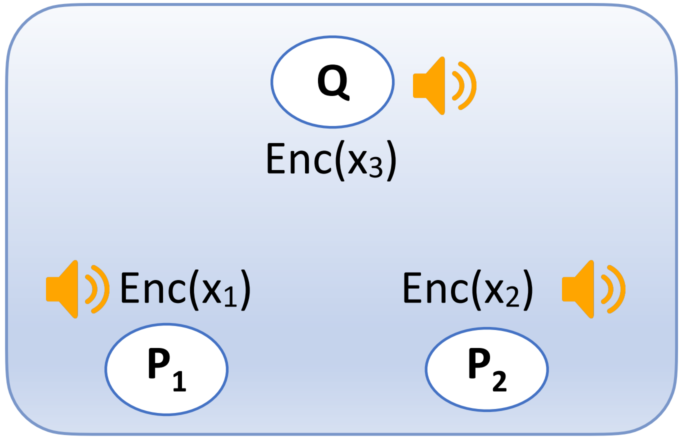
y = f(x_1, x_2, x_3)



5-Round upper bound with PKI (no broadcast)

[GLS15] 2-round (non-solitary) G.O.D protocol using PKI and Broadcast

$n = 3, t = 1$



Q

$\text{Enc}(x_3)$

$\text{Enc}(x_1)$

$\text{Enc}(x_2)$

P_1

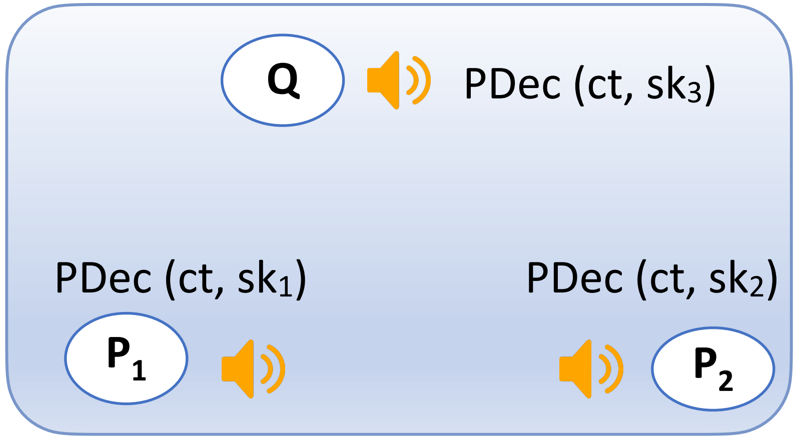
P_2

Decentralized threshold FHE Setup:

pk, sk_1, sk_2, sk_3

Compute $ct = \text{Enc}(y)$

$y = f(x_1, x_2, x_3)$



Q

PDec (ct, sk_3)

PDec (ct, sk_1)

PDec (ct, sk_2)

P_1

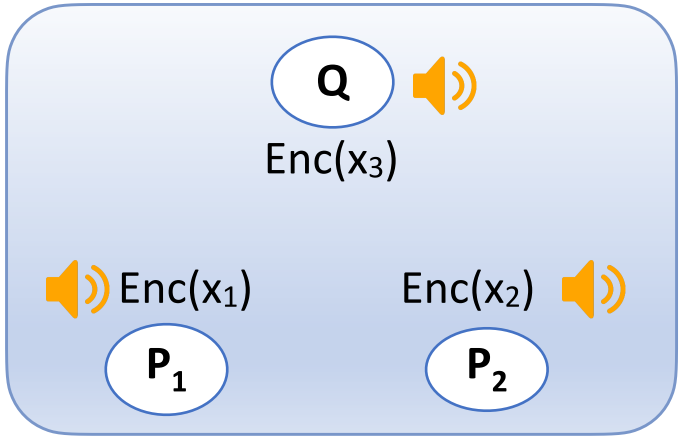
P_2

$(t + 1)$ partial decryptions can be combined to get output

5-Round upper bound with PKI (no broadcast)

[GLS15] 2-round (non-solitary) G.O.D protocol using PKI and Broadcast

n = 3, t = 1



Q

Enc(x_3)

Enc(x_1)

Enc(x_2)

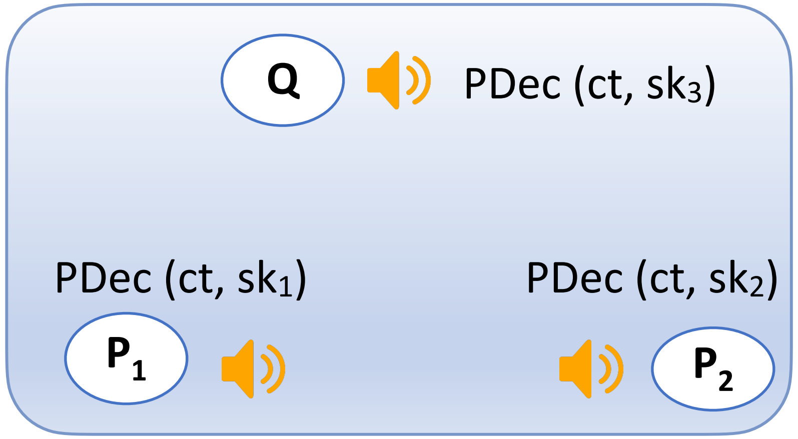
P_1

P_2

Decentralized threshold FHE Setup:

pk, sk_1 , sk_2 , sk_3

Compute ct = Enc (y)
y = f(x_1, x_2, x_3)



Q

PDec (ct, sk_3)

PDec (ct, sk_1)

PDec (ct, sk_2)

P_1

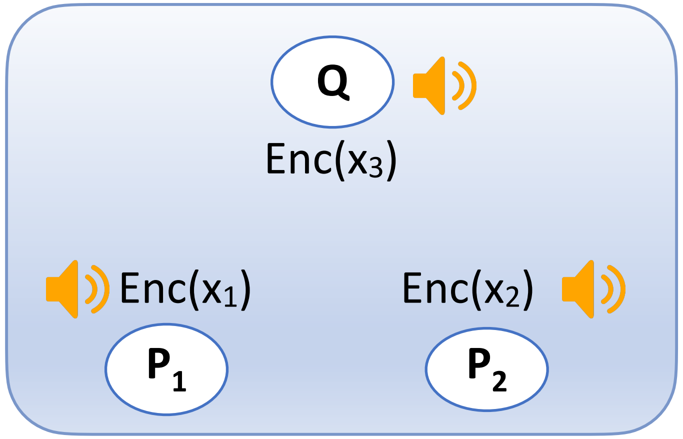
P_2

(t + 1) partial decryptions
can be combined to get output

5-Round upper bound with PKI (no broadcast)

[GLS15] 2-round (non-solitary) G.O.D protocol using PKI and Broadcast

n = 3, t = 1



Q

Enc(x_3)

Enc(x_1)

Enc(x_2)

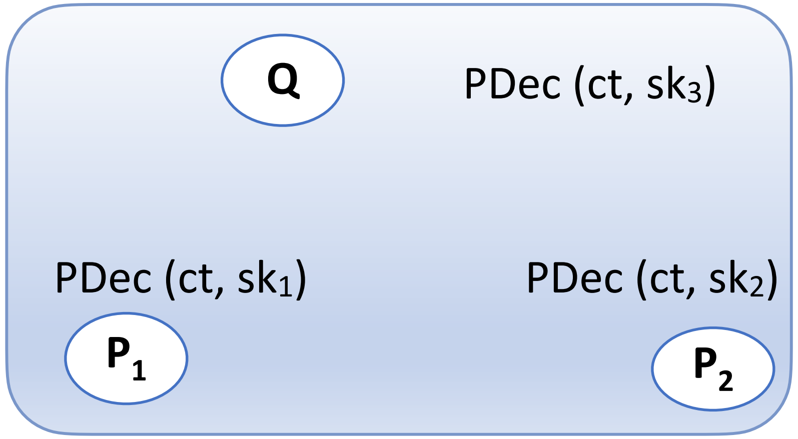
P_1

P_2

Decentralized threshold FHE Setup:

pk, sk_1 , sk_2 , sk_3

Compute ct = Enc (y)
y = f(x_1, x_2, x_3)



Q

PDec (ct, sk_3)

PDec (ct, sk_1)

PDec (ct, sk_2)

P_1

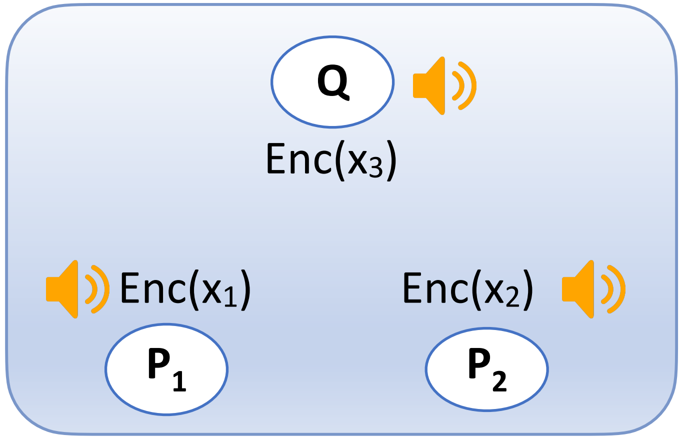
P_2

(t + 1) partial decryptions
can be combined to get output

5-Round upper bound with PKI (no broadcast)

[GLS15] 2-round (non-solitary) G.O.D protocol using PKI and Broadcast

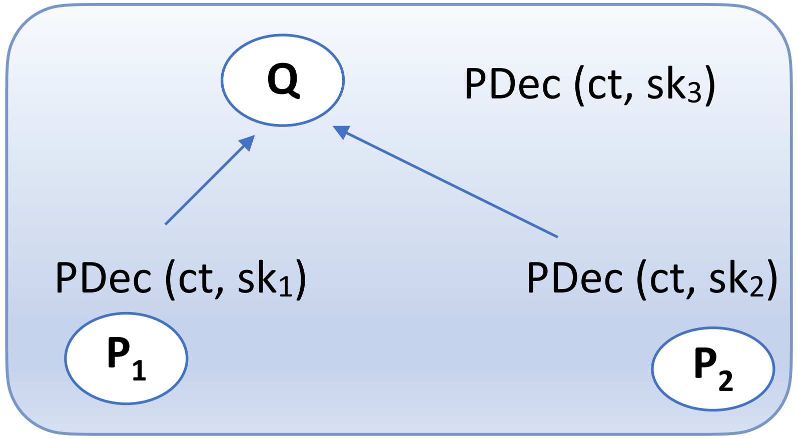
n = 3, t = 1



Decentralized threshold FHE Setup:

pk, sk_1 , sk_2 , sk_3

Compute ct = Enc (y)
y = f(x_1, x_2, x_3)

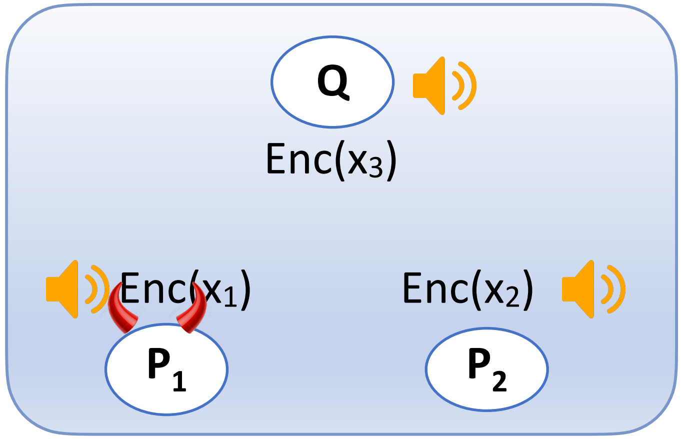


(t + 1) partial decryptions
can be combined to get output

5-Round upper bound with PKI (no broadcast)

[GLS15] 2-round (non-solitary) G.O.D protocol using PKI and Broadcast

n = 3, t = 1



Q

Enc(x_3)

Enc(x_1)

Enc(x_2)

P_1

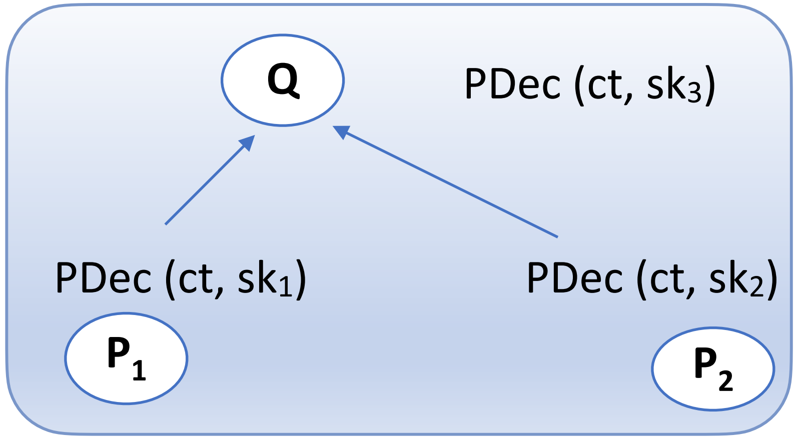
P_2

Decentralized threshold FHE Setup:

pk, sk_1 , sk_2 , sk_3

Compute ct = Enc (y)

y = f(x_1, x_2, x_3)



Q

PDec (ct, sk_3)

PDec (ct, sk_1)

PDec (ct, sk_2)

P_1

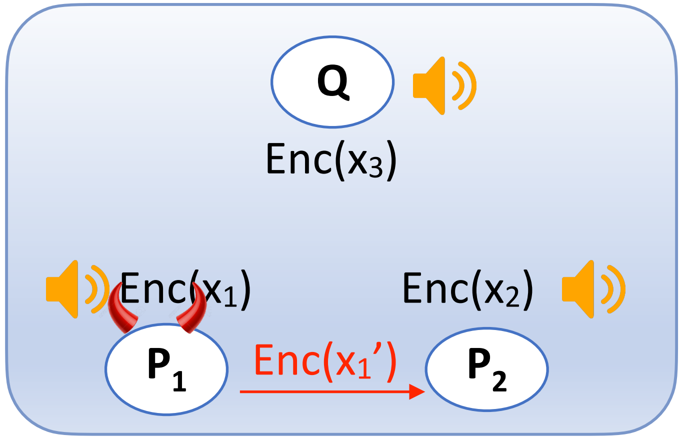
P_2

(t + 1) partial decryptions
can be combined to get output

5-Round upper bound with PKI (no broadcast)

[GLS15] 2-round (non-solitary) G.O.D protocol using PKI and Broadcast

n = 3, t = 1



Q

Enc(x_3)

Enc(x_1)

Enc(x_2)

P_1

Enc(x_1')

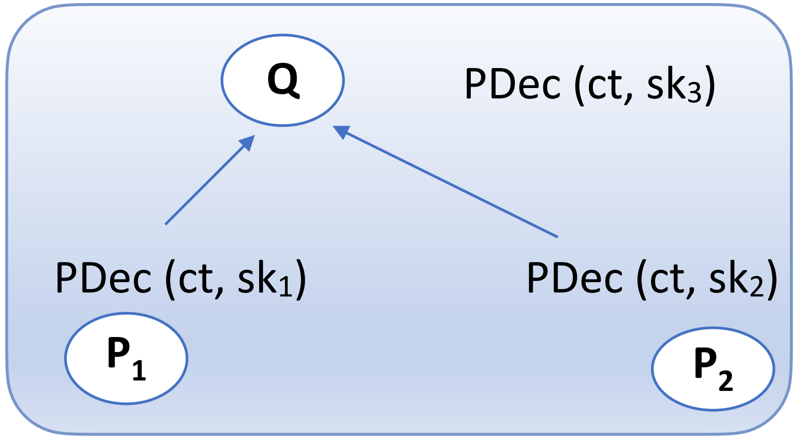
P_2

Decentralized threshold FHE Setup:

pk, sk_1 , sk_2 , sk_3

Compute ct = Enc (y)

y = f(x_1, x_2, x_3)



Q

PDec (ct, sk_3)

PDec (ct, sk_1)

PDec (ct, sk_2)

P_1

P_2

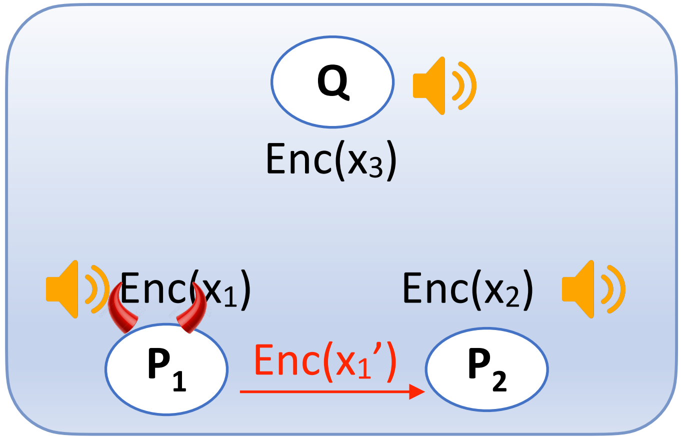
(t + 1) partial decryptions

can be combined to get output

5-Round upper bound with PKI (no broadcast)

[GLS15] 2-round (non-solitary) G.O.D protocol using PKI and Broadcast

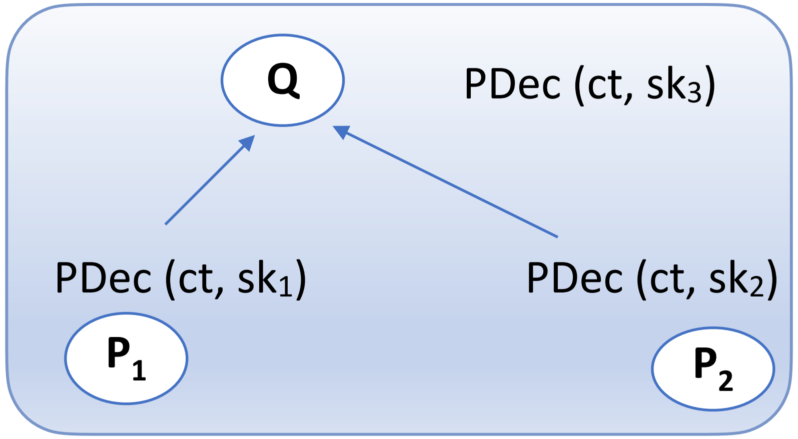
n = 3, t = 1



Decentralized threshold FHE Setup:

pk, sk_1, sk_2, sk_3

Compute ct = Enc (y)
$y = f(x_1, x_2, x_3)$



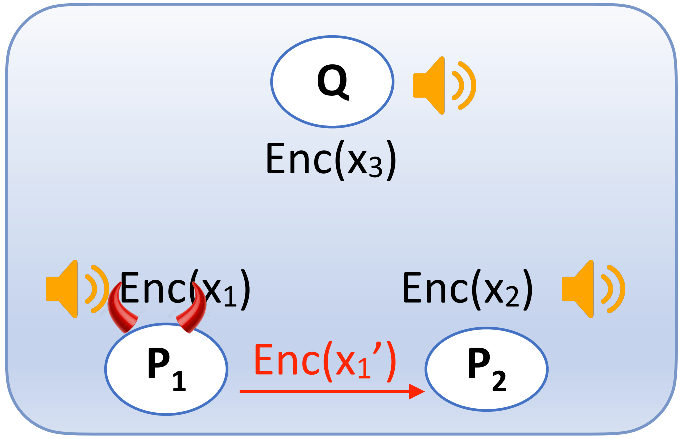
Need to agree!

(t + 1) partial decryptions
can be combined to get output

5-Round upper bound with PKI (no broadcast)

[GLS15] 2-round (non-solitary) G.O.D protocol using PKI and Broadcast

$n = 3, t = 1$

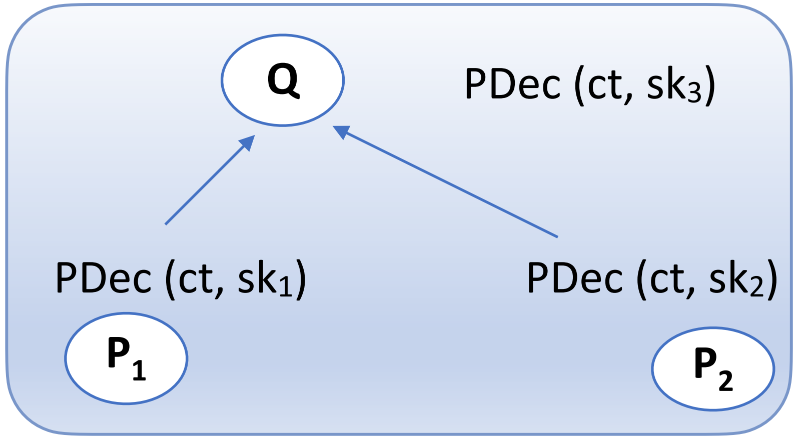


Decentralized threshold FHE Setup:

pk, sk_1 , sk_2 , sk_3

Compute ct = Enc (y)

$y = f(x_1, x_2, x_3)$



(t + 1) partial decryptions can be combined to get output

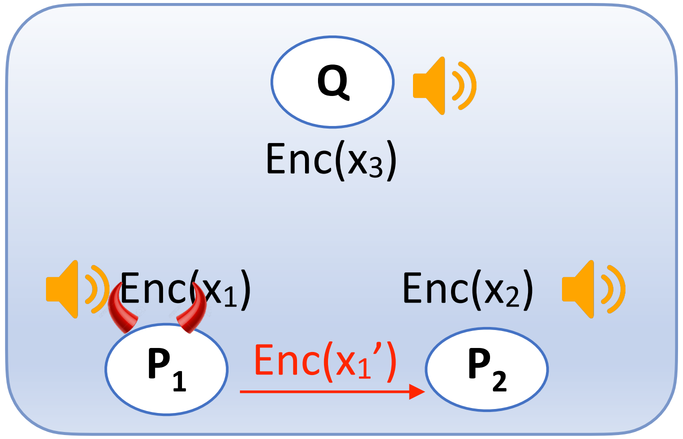
Need to agree!

Broadcast would need t + 1 rounds

5-Round upper bound with PKI (no broadcast)

[GLS15] 2-round (non-solitary) G.O.D protocol using PKI and Broadcast

n = 3, t = 1

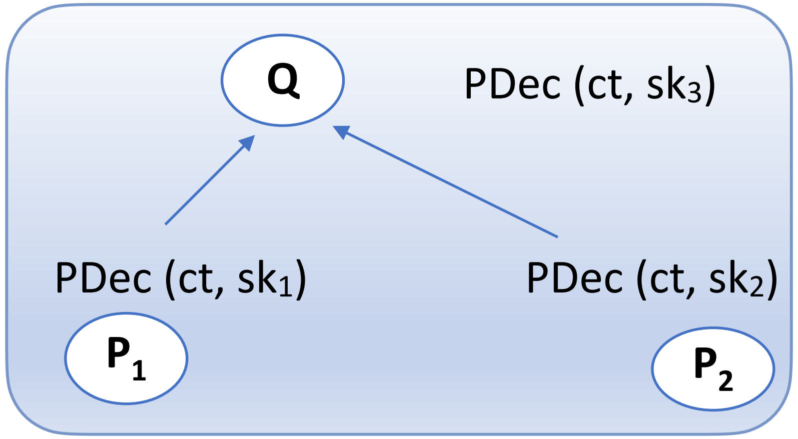


Decentralized threshold FHE Setup:

pk, sk_1 , sk_2 , sk_3

Compute ct = Enc (y)

y = f(x_1, x_2, x_3)



(t + 1) partial decryptions can be combined to get output

Need to agree!

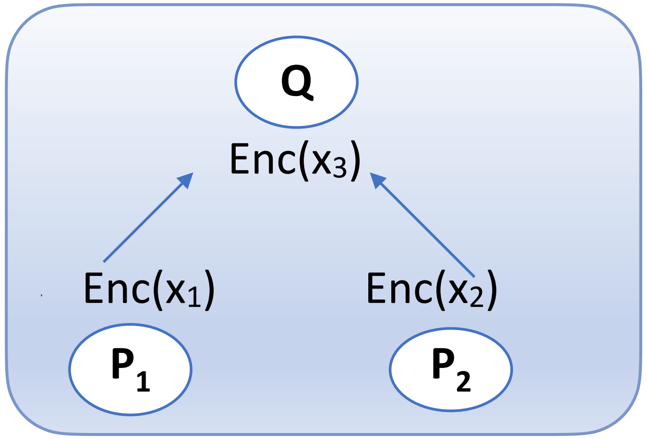
Broadcast would need t + 1 rounds

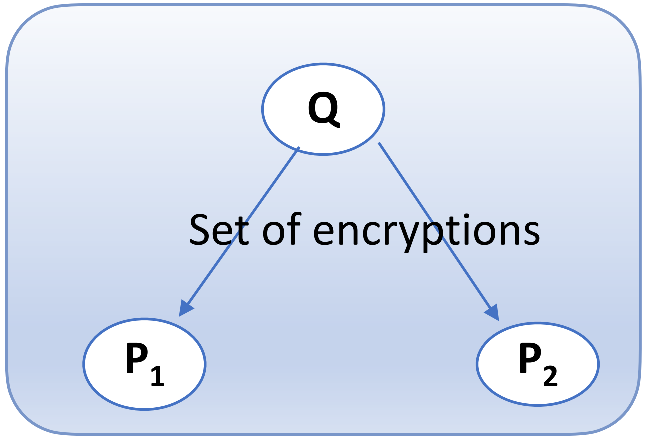
We only need to agree if Q is honest

5-Round upper bound with PKI (no broadcast)

Decentralized threshold FHE Setup: pk, sk_1 , sk_2 , sk_3

n = 3, t = 1

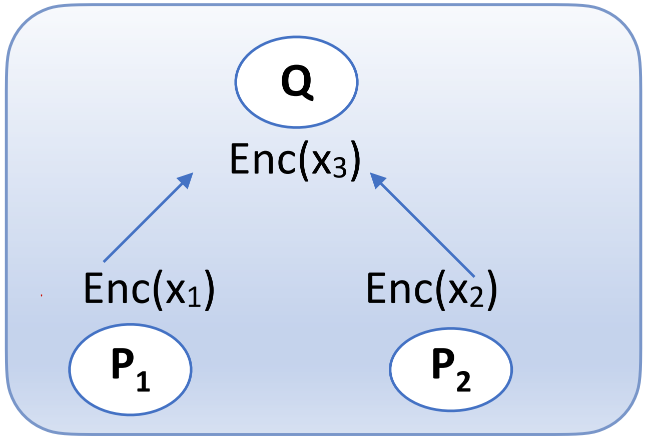


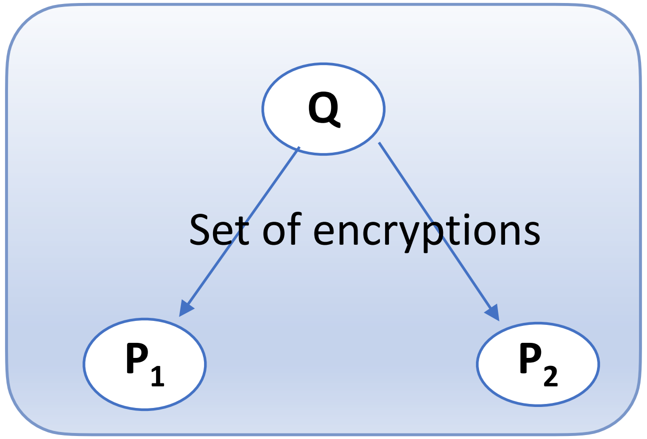


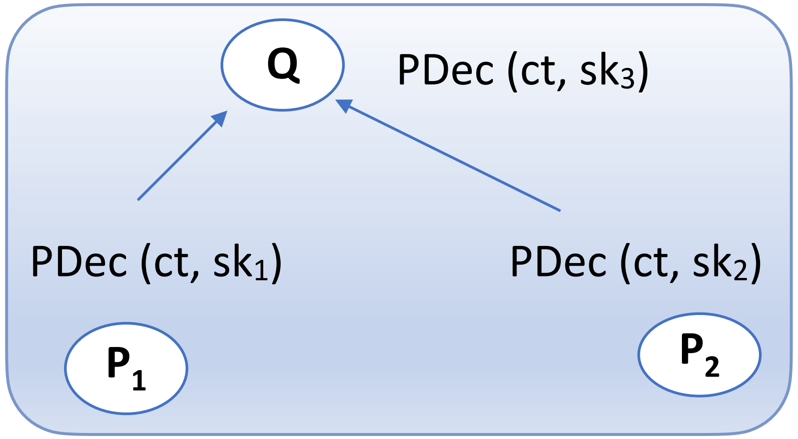
5-Round upper bound with PKI (no broadcast)

Decentralized threshold FHE Setup: pk, sk_1 , sk_2 , sk_3

n = 3, t = 1



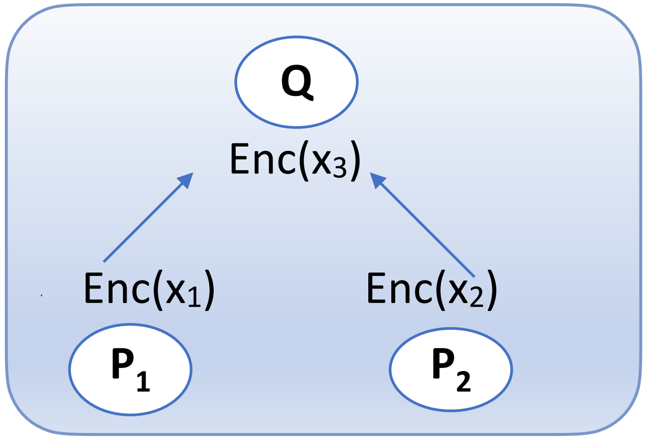


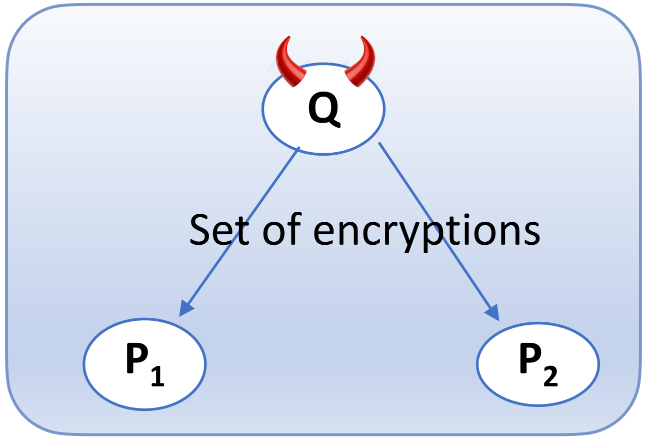


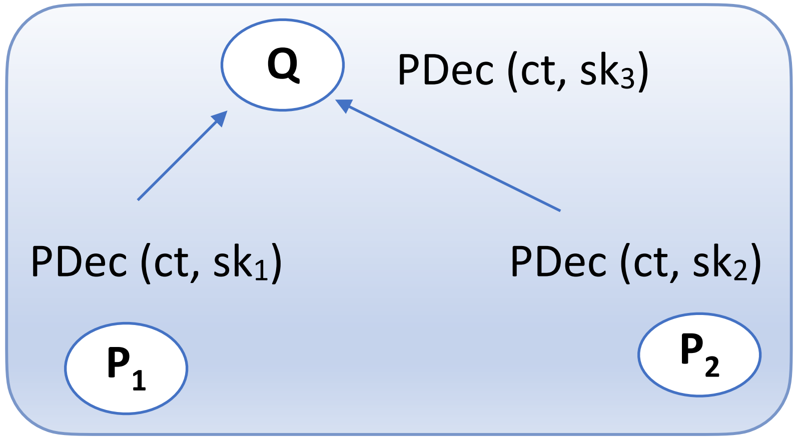
5-Round upper bound with PKI (no broadcast)

Decentralized threshold FHE Setup: pk, sk_1 , sk_2 , sk_3

n = 3, t = 1



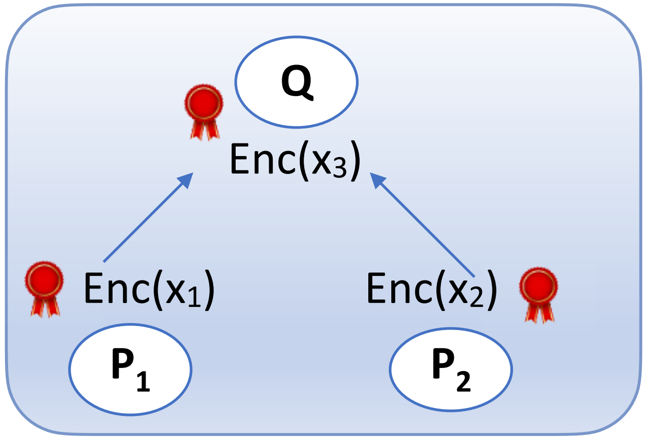


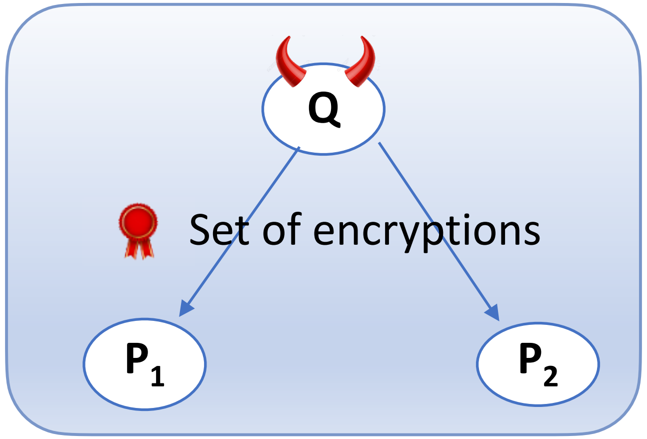


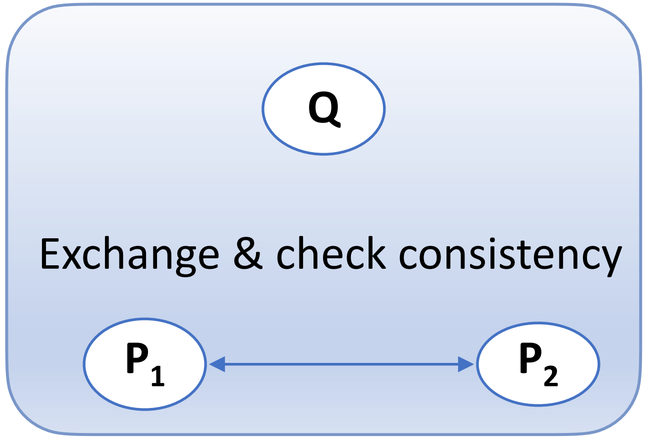
5-Round upper bound with PKI (no broadcast)

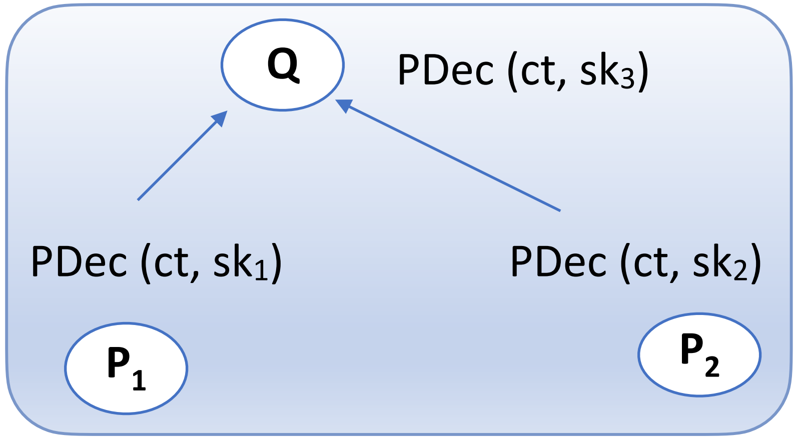
Decentralized threshold FHE Setup: pk, sk_1 , sk_2 , sk_3

n = 3, t = 1





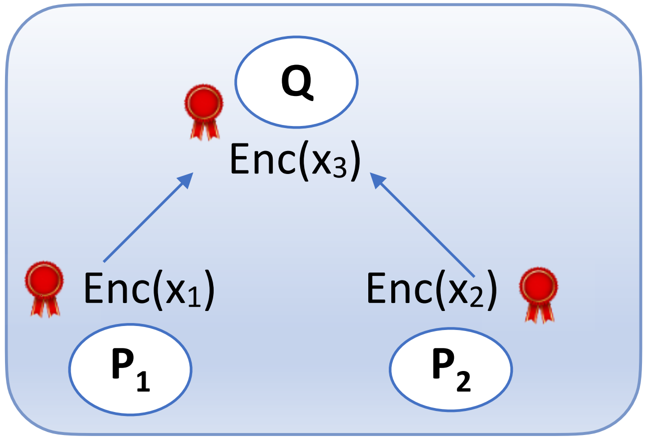


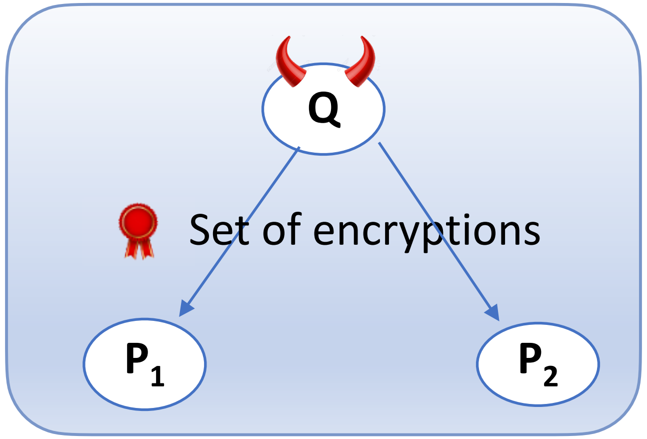


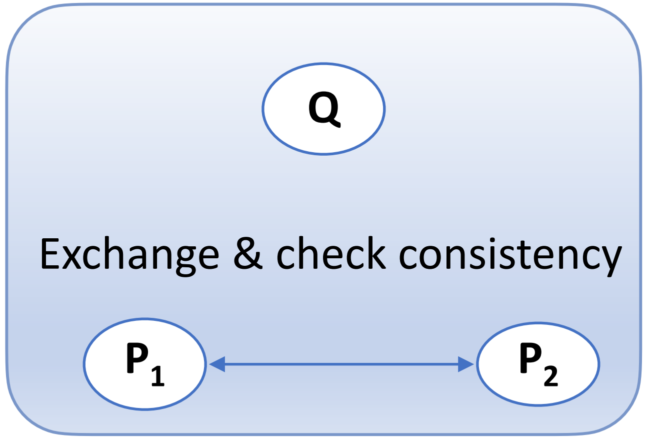
5-Round upper bound with PKI (no broadcast)

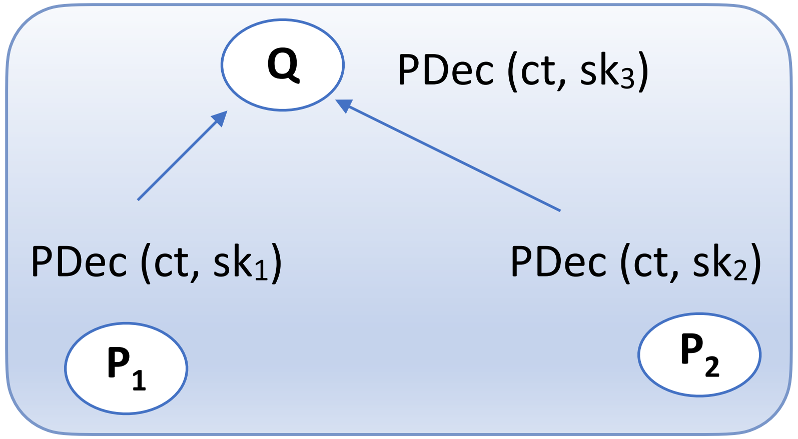
Decentralized threshold FHE Setup: pk, sk_1 , sk_2 , sk_3

n = 3, t = 1





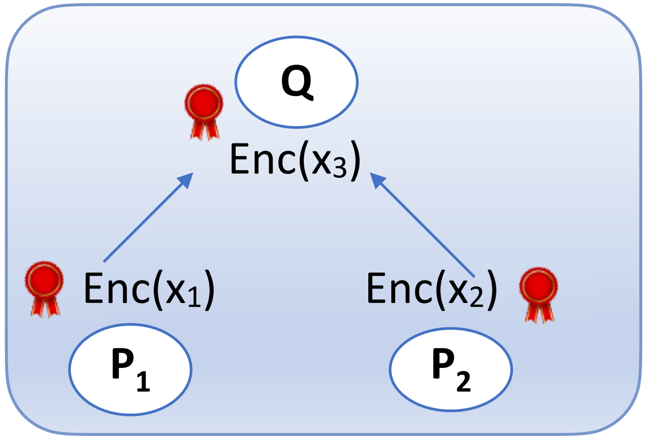




5-Round upper bound with PKI (no broadcast)

Decentralized threshold FHE Setup: pk, sk_1 , sk_2 , sk_3

n = 3, t = 1



Q

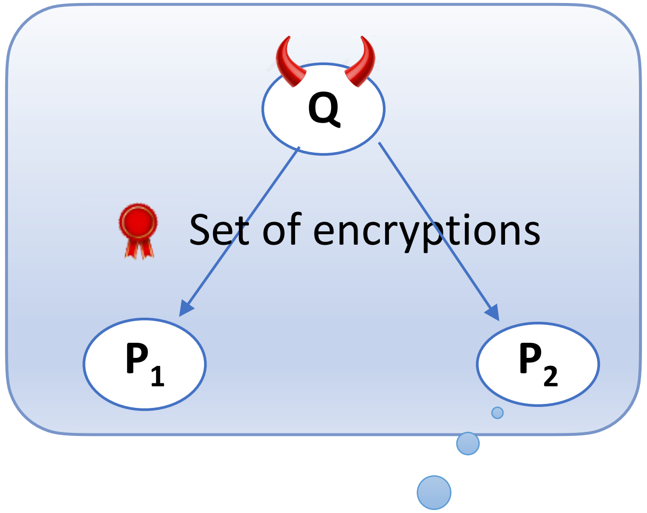
Enc(x_3)

Enc(x_1)

Enc(x_2)

P_1

P_2



Q

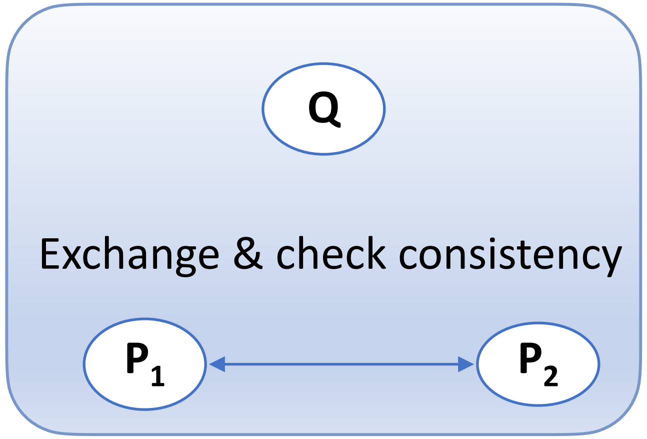
Set of encryptions

P_1

P_2

Q says P_1 did not send anything.

Is Q corrupt or P_1?

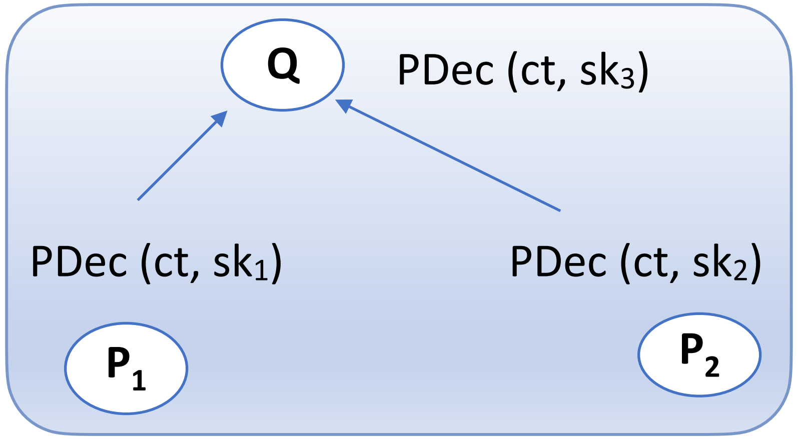


Q

Exchange & check consistency

P_1

P_2



Q

PDec (ct, sk_3)

PDec (ct, sk_1)

PDec (ct, sk_2)

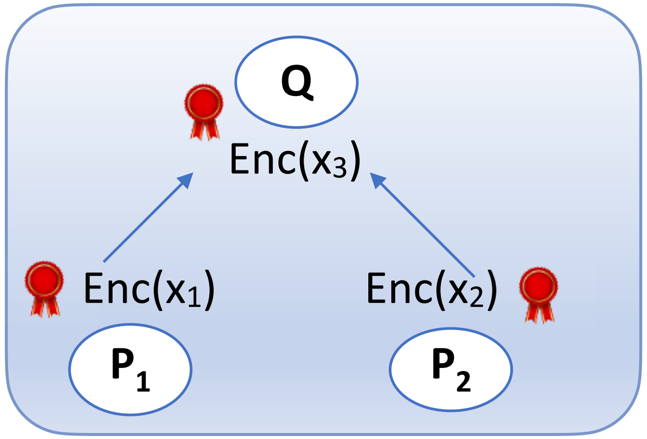
P_1

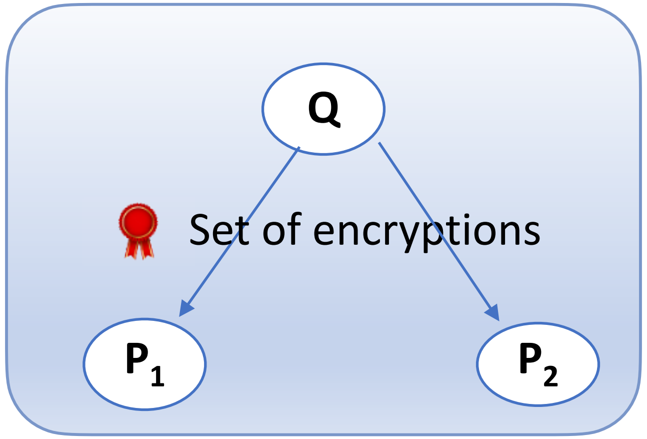
P_2

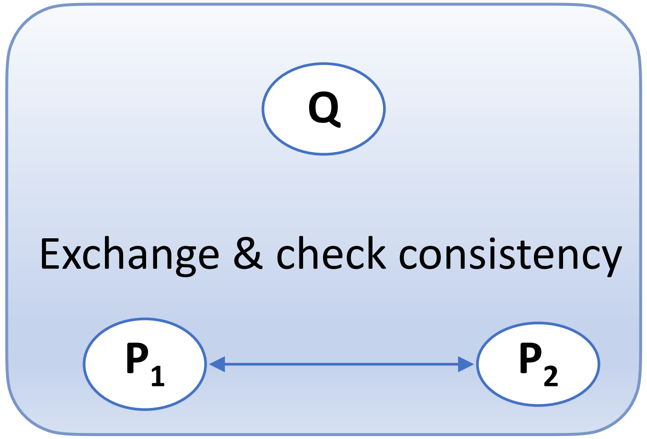
5-Round upper bound with PKI (no broadcast)

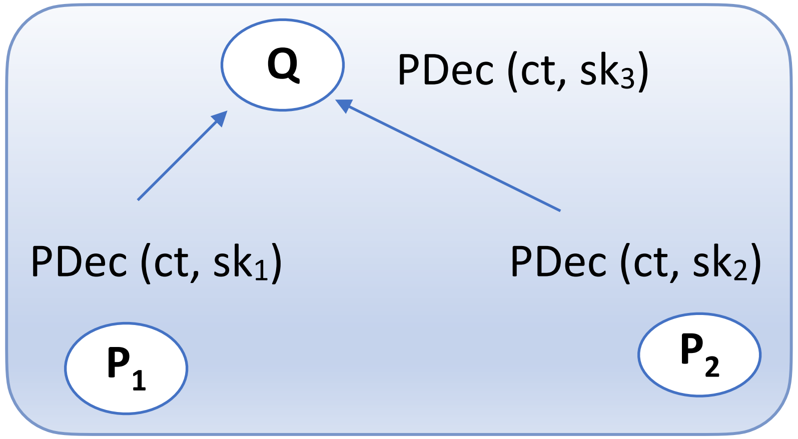
Decentralized threshold FHE Setup: pk, sk_1, sk_2, sk_3

n = 3, t = 1





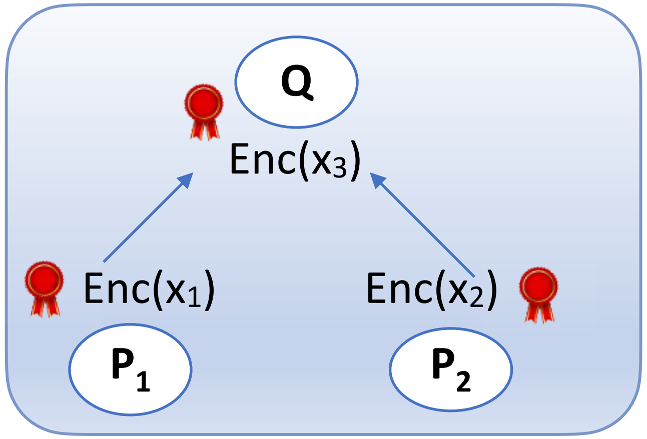


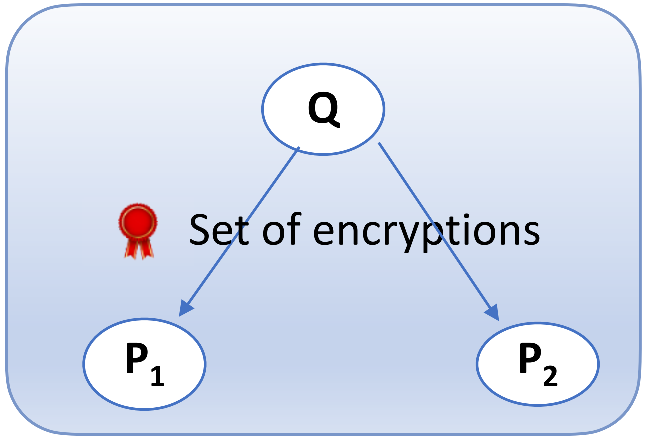


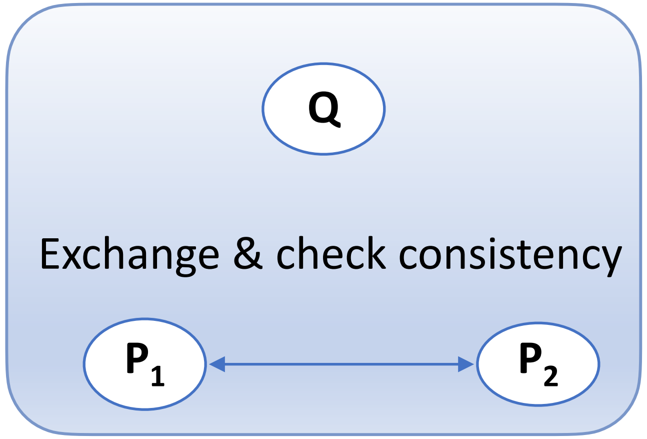
5-Round upper bound with PKI (no broadcast)

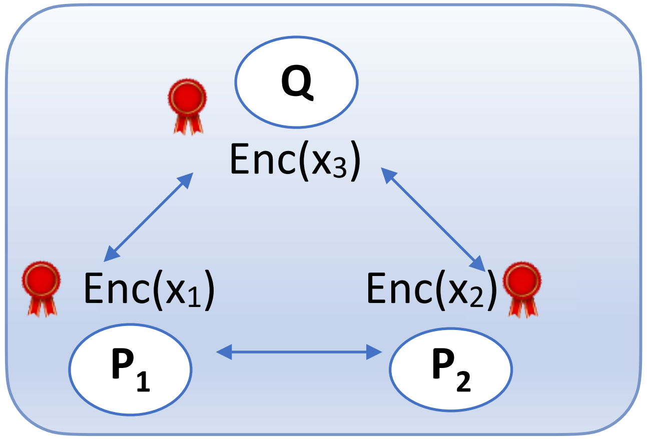
Decentralized threshold FHE Setup: pk, sk_1 , sk_2 , sk_3

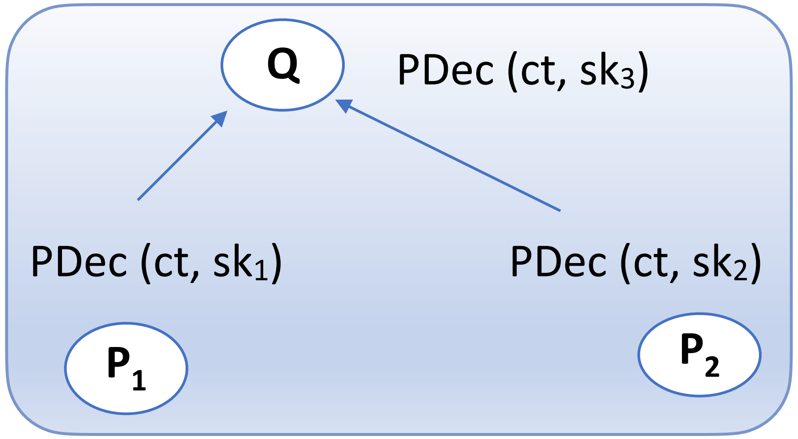
n = 3, t = 1







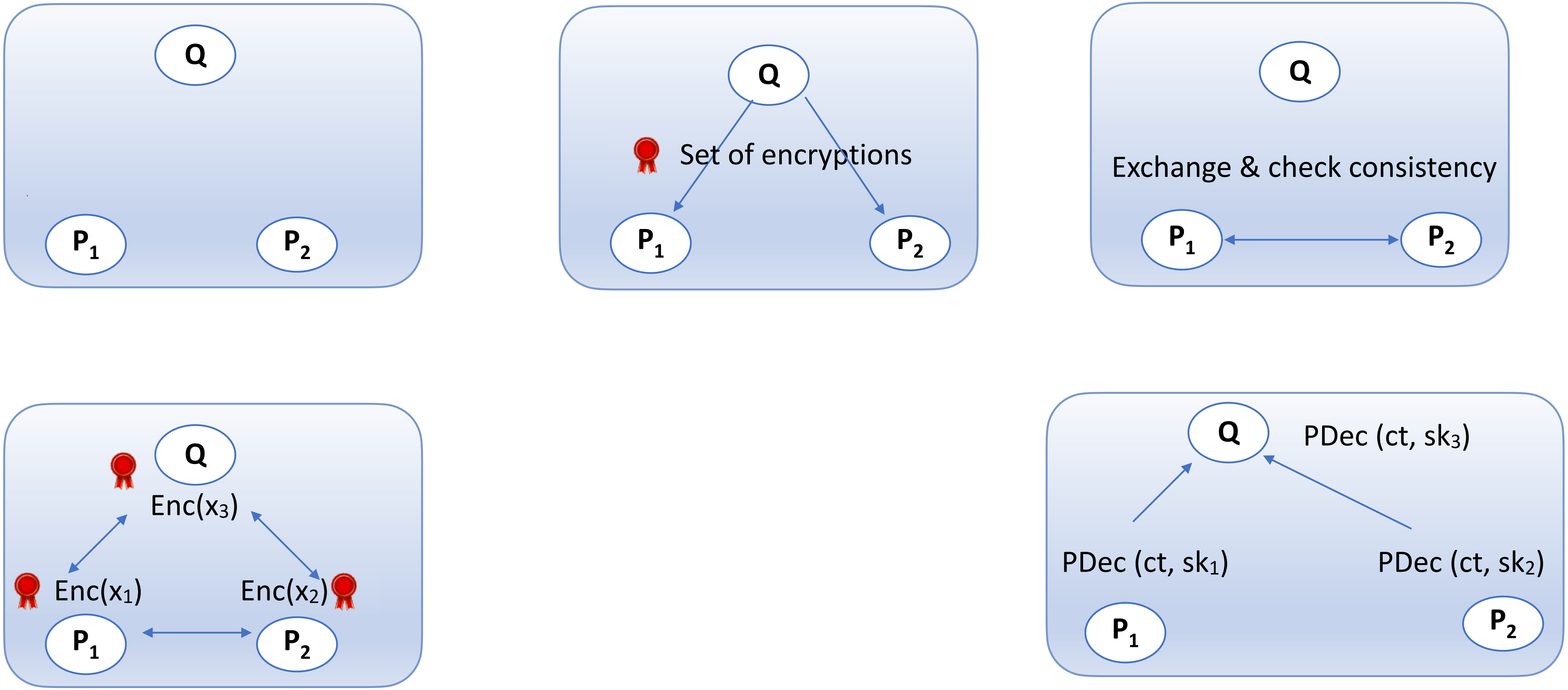




5-Round upper bound with PKI (no broadcast)

Decentralized threshold FHE Setup: pk, sk_1, sk_2, sk_3

n = 3, t = 1



Set of encryptions

Exchange & check consistency

Enc(x_3)

Enc(x_1)

Enc(x_2)

PDec (ct, sk_3)

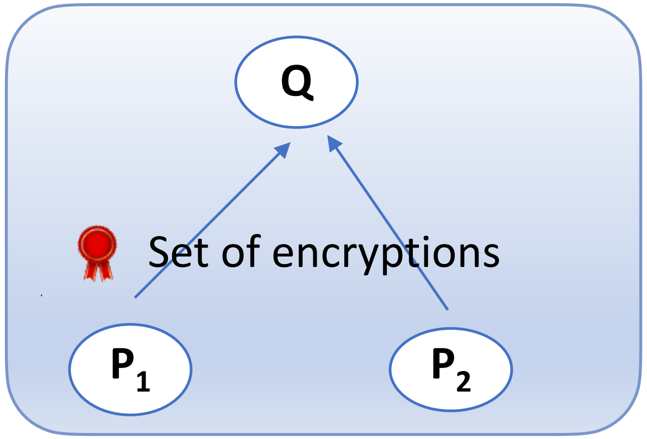
PDec (ct, sk_1)

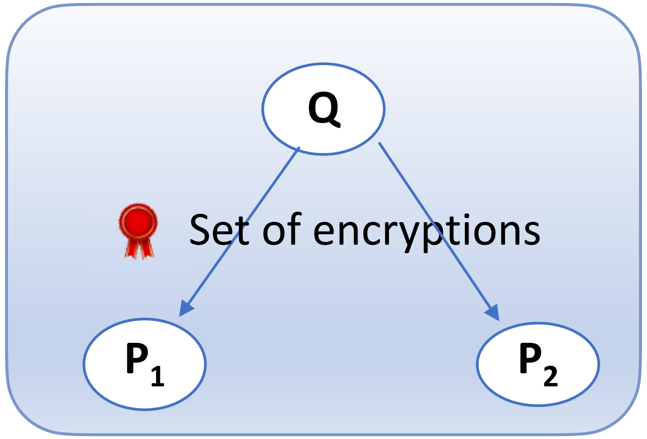
PDec (ct, sk_2)

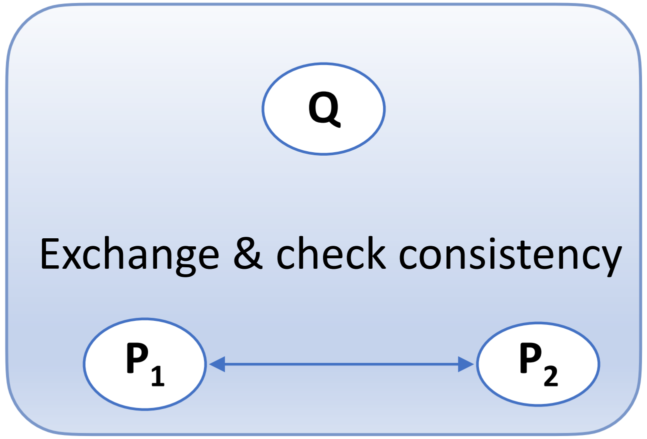
5-Round upper bound with PKI (no broadcast)

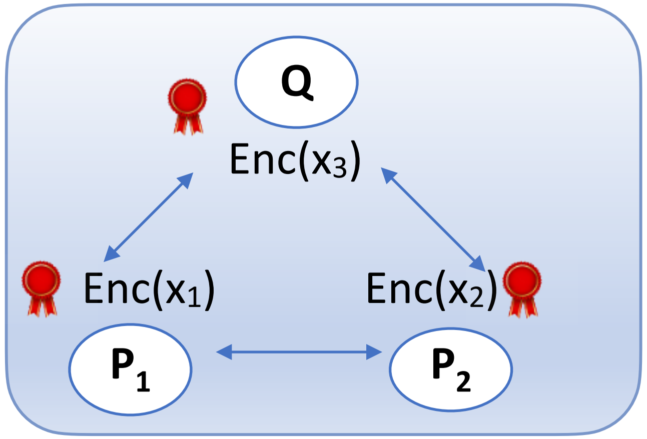
Decentralized threshold FHE Setup: pk, sk_1 , sk_2 , sk_3

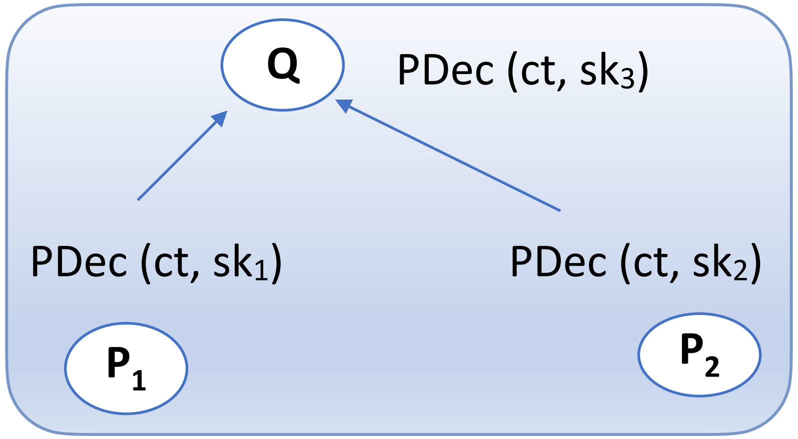
n = 3, t = 1







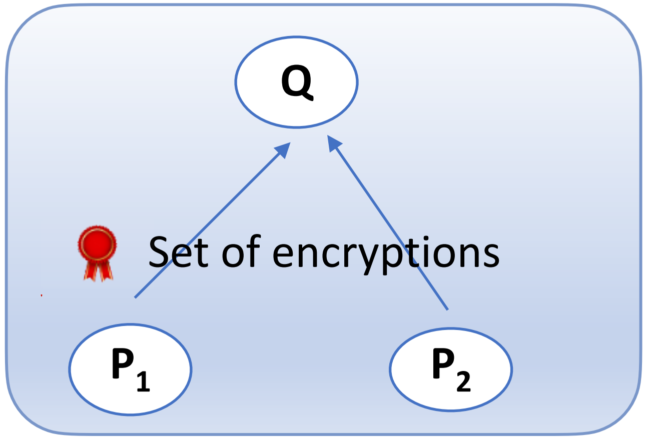


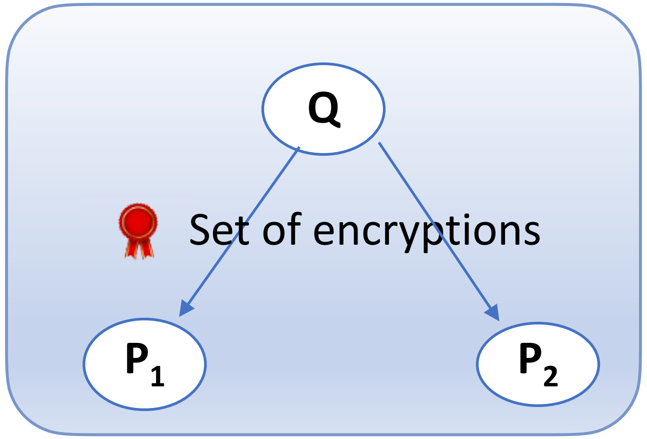


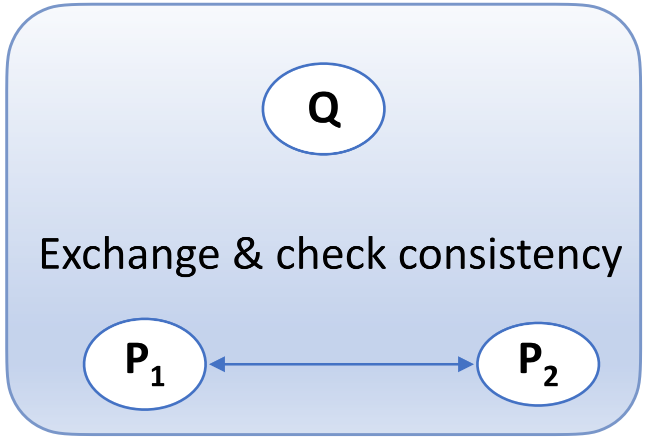
5-Round upper bound with PKI (no broadcast)

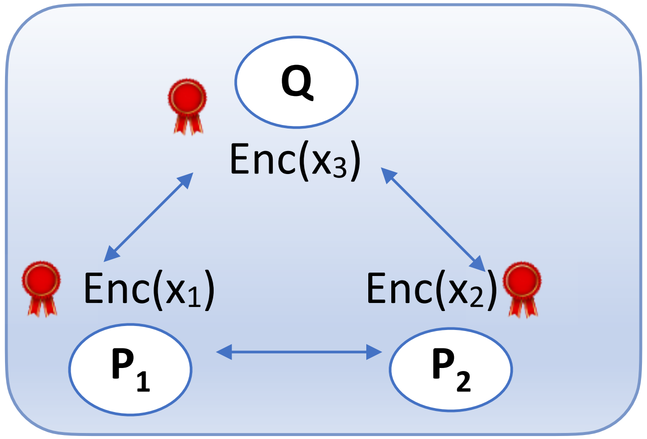
Decentralized threshold FHE Setup: pk, sk_1 , sk_2 , sk_3

n = 3, t = 1



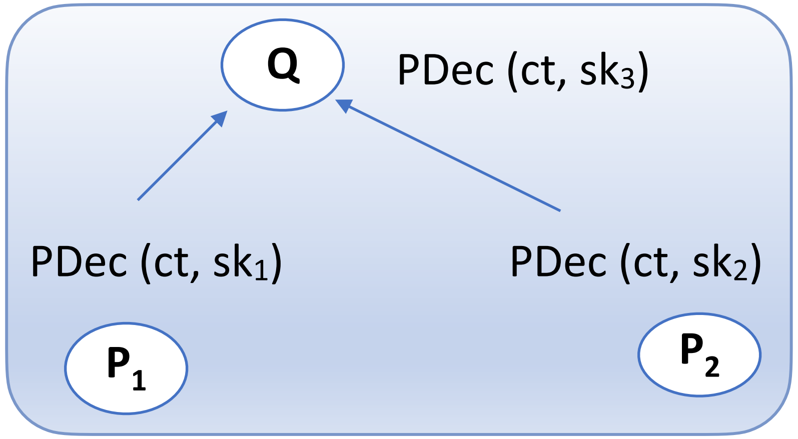






Q must include a cipher text from party

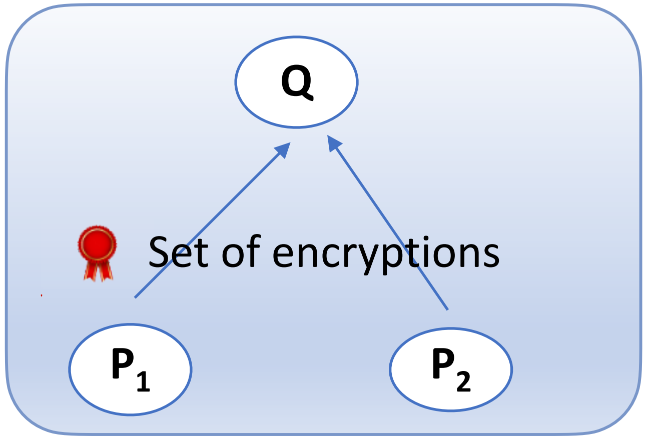
- received directly in round 1
- Via different party in round 2



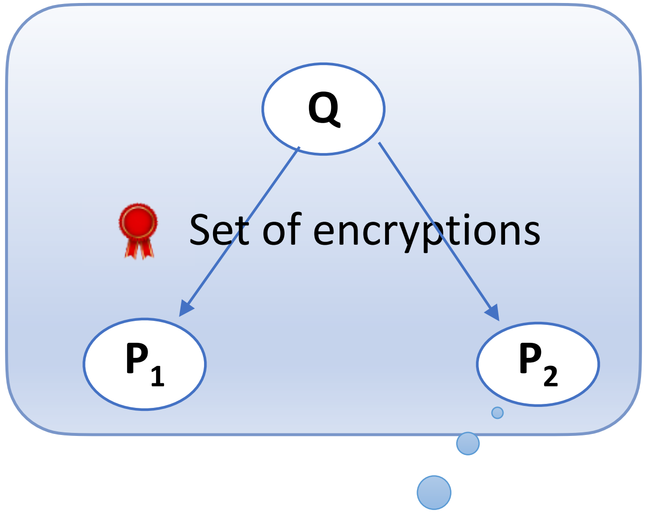
5-Round upper bound with PKI (no broadcast)

Decentralized threshold FHE Setup: pk, sk_1 , sk_2 , sk_3

n = 3, t = 1

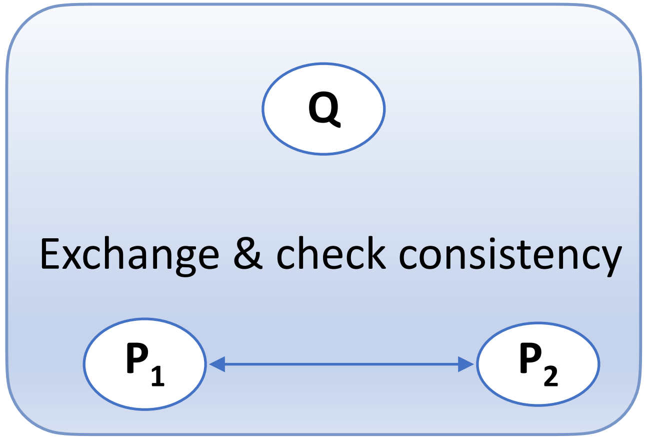


Set of encryptions

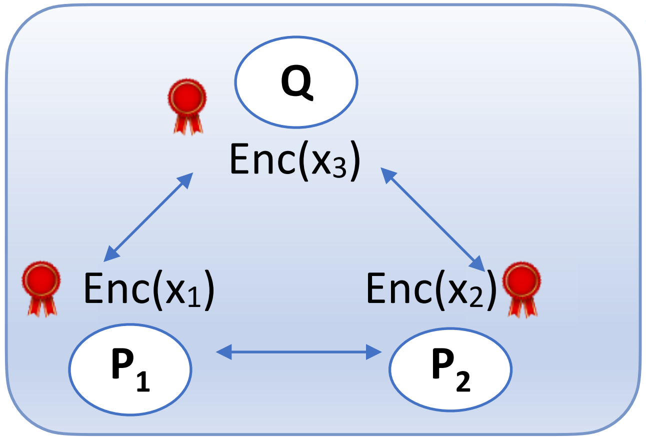


Set of encryptions

Q must include a cipher text for P_1 since I sent him one!



Exchange & check consistency



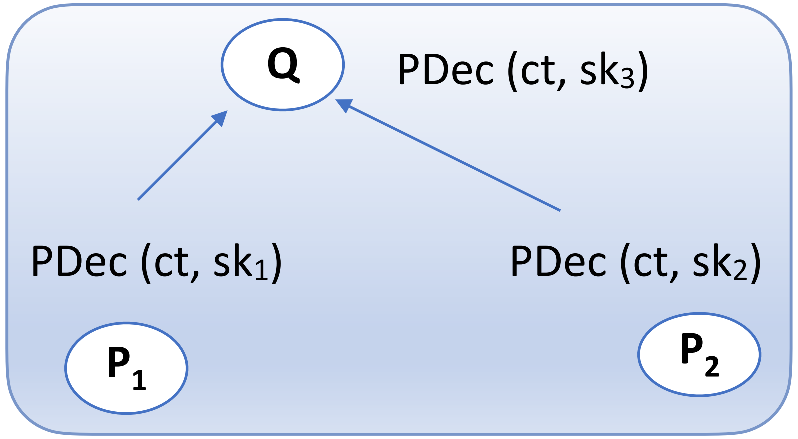
$Enc(x_3)$

$Enc(x_1)$

$Enc(x_2)$

Q must include a cipher text from party

- received directly in round 1
- Via different party in round 2



PDec (ct, sk_3)

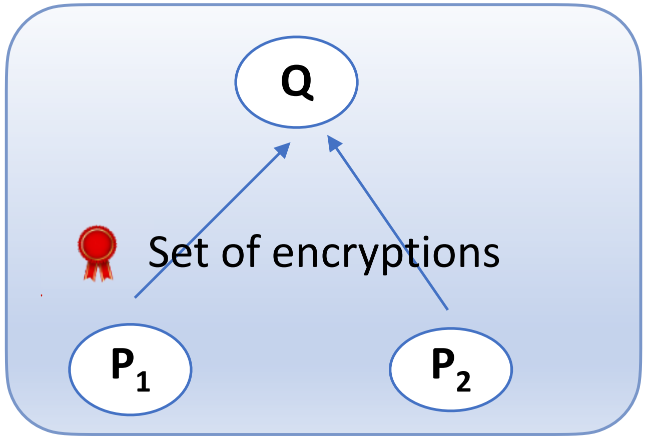
PDec (ct, sk_1)

PDec (ct, sk_2)

5-Round upper bound with PKI (no broadcast)

Decentralized threshold FHE Setup: pk, sk_1, sk_2, sk_3

n = 3, t = 1



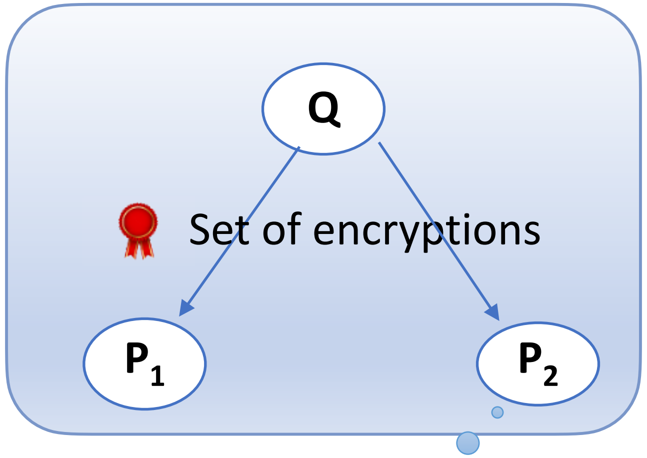
Q

Set of encryptions

P_1

P_2

Round 2



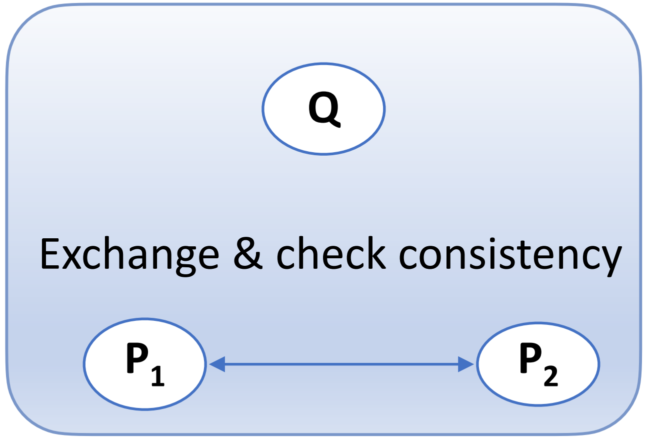
Q

Set of encryptions

P_1

P_2

Round 3



Q

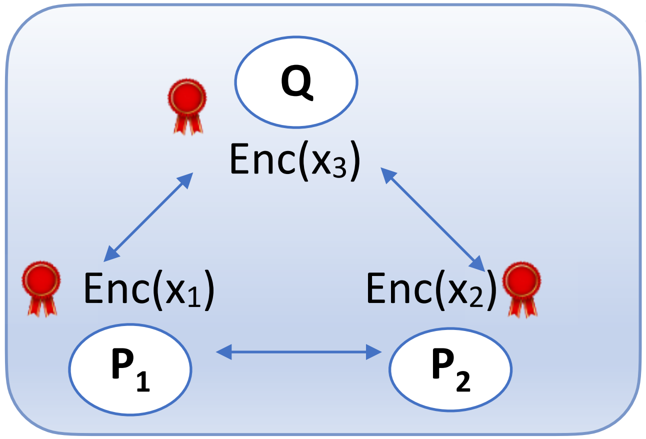
Exchange & check consistency

P_1

P_2

Round 4

Q must include a cipher text for P_1 since I sent him one!



Q

Enc(x_3)

Enc(x_1)

Enc(x_2)

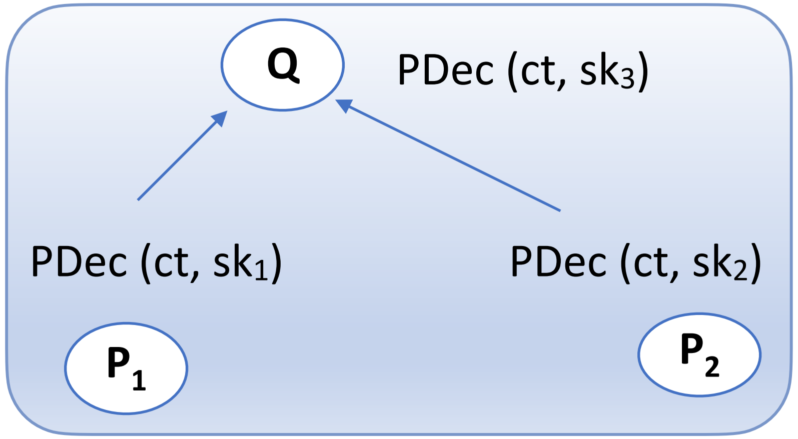
P_1

P_2

Round 1

Q must include a cipher text from party

- received directly in round 1
- Via different party in round 2



Q

PDec (ct, sk_3)

PDec (ct, sk_1)

PDec (ct, sk_2)

P_1

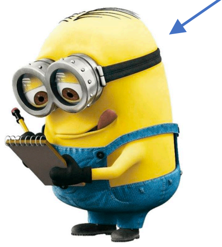
P_2

Round 5

Round Complexity of Solitary MPC with G.O.D

- Need to assume either broadcast or PKI [HIKMR19, FGMO05]

Broadcast	PKI	Threshold	Lower Bound	Upper Bound
✔	✔	t < n/2	2 [HLP11]	2 [GLS15]
✔	✖	t < n/2	3 [This work]	3 [ACGJ18, BJMS18]
✖	✔	n/2 > t >=3	4 [This work]	5 [This Work]



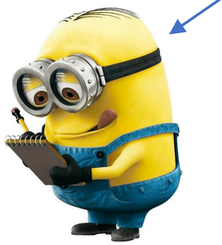
Additional Results:

- Optimal use of broadcast
- Special cases t = 1 & t = 2

Round Complexity of Solitary MPC with G.O.D

- Need to assume either broadcast or PKI [HIKMR19, FGMO05]

Broadcast	PKI	Threshold	Lower Bound	Upper Bound
✓	✓	t < n/2	2 [HLP11]	2 [GLS15]
✓	✖	t < n/2	3 [This work]	3 [ACGJ18, BJMS18]
✖	✓	n/2 > t >=3	4 [This work]	5 [This Work]



Additional Results:
- Optimal use of broadcast
- Special cases t = 1 & t = 2