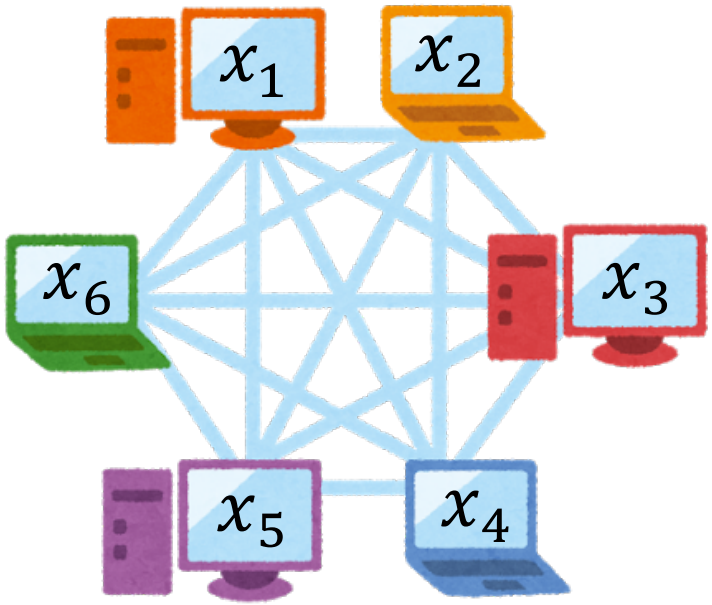
Size-Hiding Computation for Multiple Parties

Kazumasa Shinagawa[1,2]
Koji Nuida[2,3]
Takashi Nishide[1]
Goichiro Hanaoka[2]
Eiji Okamoto[1]

1: University of Tsukuba, 2: AIST, 3: JST PRESTO

Secure Multiparty Computation

- Each party P_i has some private input x_i
- The parties wish to compute a function $y = f(x_1, \cdots, x_n)$ without revealing the inputs
- Consider the single output, semi-honest, $n - 1$ corruption



Size-Hiding Computation

- can hide some of input/output-sizes from some of parties
- Each private size can be hidden from different set of parties
- It is known that some of size-hiding is impossible in general
- Which type of size-hiding is possible in general?

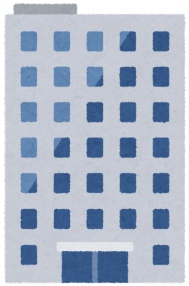
This Talk

complete characterization for the feasibility
(assuming the existence of FHE)

Set Intersection

- Police has a list of terrorists X
- Company has a list of customers Y
- Police wants to compute $X \cap Y$ without revealing $|X|$
- Naïve approach: Padding
- Padding is inefficient

X

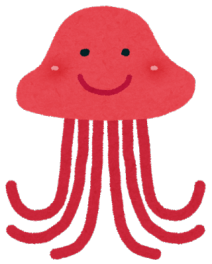


Y

Compute $X \cap Y$

Millionaire Problem

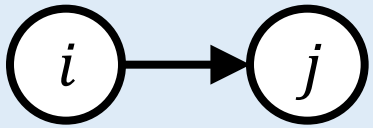
- Aliens: “Which planet has the largest population?”
- The population is related to the military power
- The input-size is also related to the military power
- Padding doesn’t work
  ∵ The largest population in the universe is too large




Outline

- NEW Notations
- Classification for two-party [LNO13]
- NEW Classification for multiparty
  - Almost all sizes cannot be hidden
- NEW Strong secure channel (SSC) model
  - It is implementable by steganography
- NEW Classification for multiparty in SSC model
  - Many sizes can be hidden in SSC model

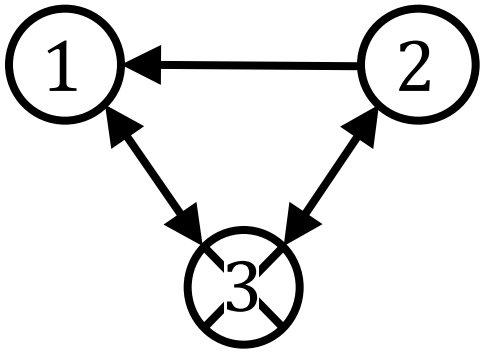
Notations



: P_j can know $|x_i|$

: who must not know the output size

- **A size-hiding class**



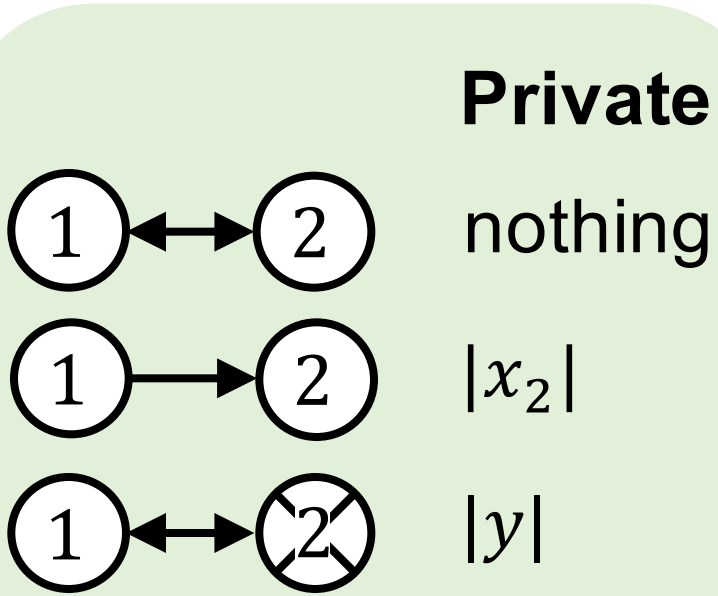
✓ P_2 must not know $|x_1|$

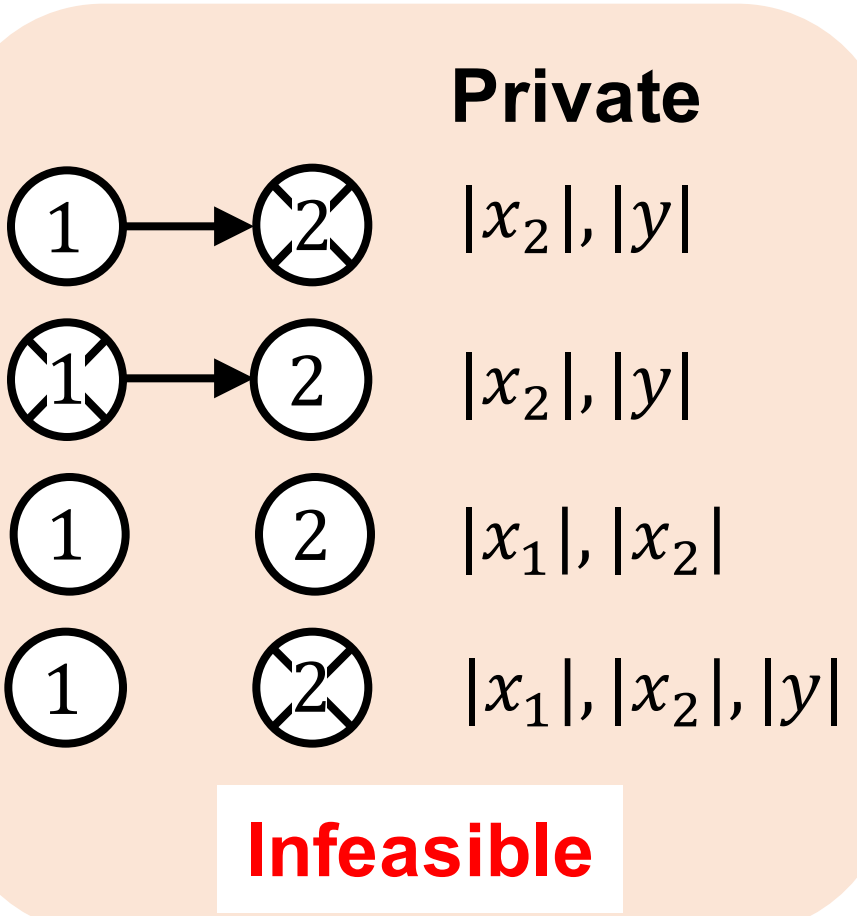
✓ P_3 must not know the output-size

Def. A class is feasible if general MPC is possible

Two-party Cases [LNO13]

Hiding two or more sizes is infeasible in two-party case





Outline

- NEW Notations
- Classification for two-party [LNO13]
- NEW **Classification for multiparty**
  - Almost all sizes cannot be hidden
- NEW Strong secure channel (SSC) model
  - It is implementable by steganography
- NEW Classification for multiparty in SSC model
  - Many sizes can be hidden in SSC model

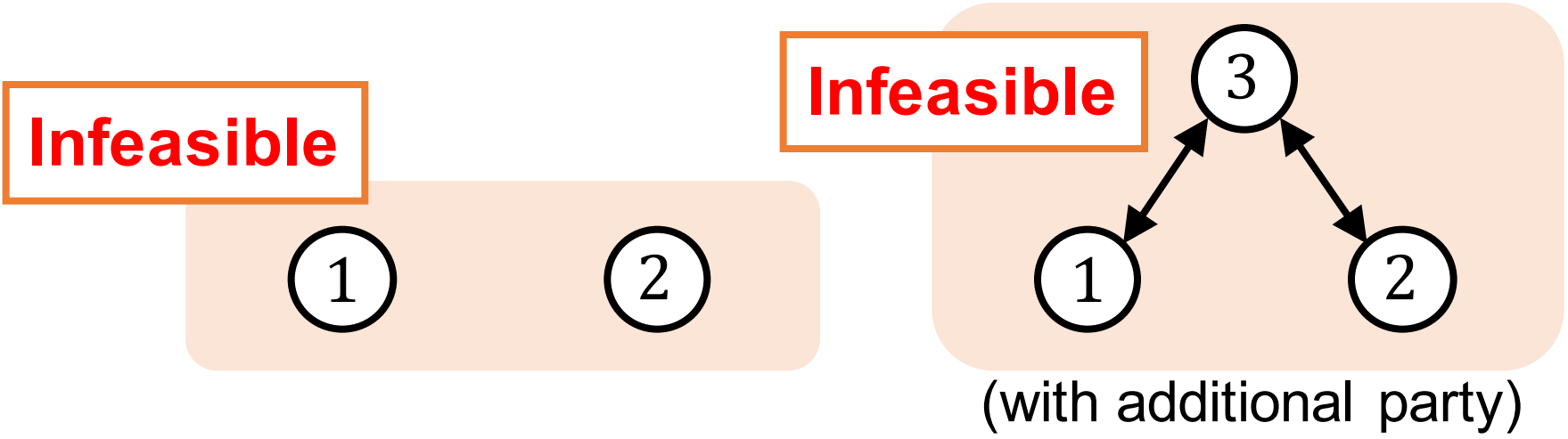
Multiparty Cases (Our Result)

Our result in standard model

Even in MPC, it is infeasible to hide two sizes

- The infeasibility is proven by techniques of [LNO13]
- The protocol for hiding $|x_1|$
  - The parties invoke KeyGen for threshold FHE
  - Each party P_i sends $Enc(x_i)$ to P_1
  - P_1 computes $[y]$ and broadcast it
  - They invoke Decryption

Limitation of standard channel



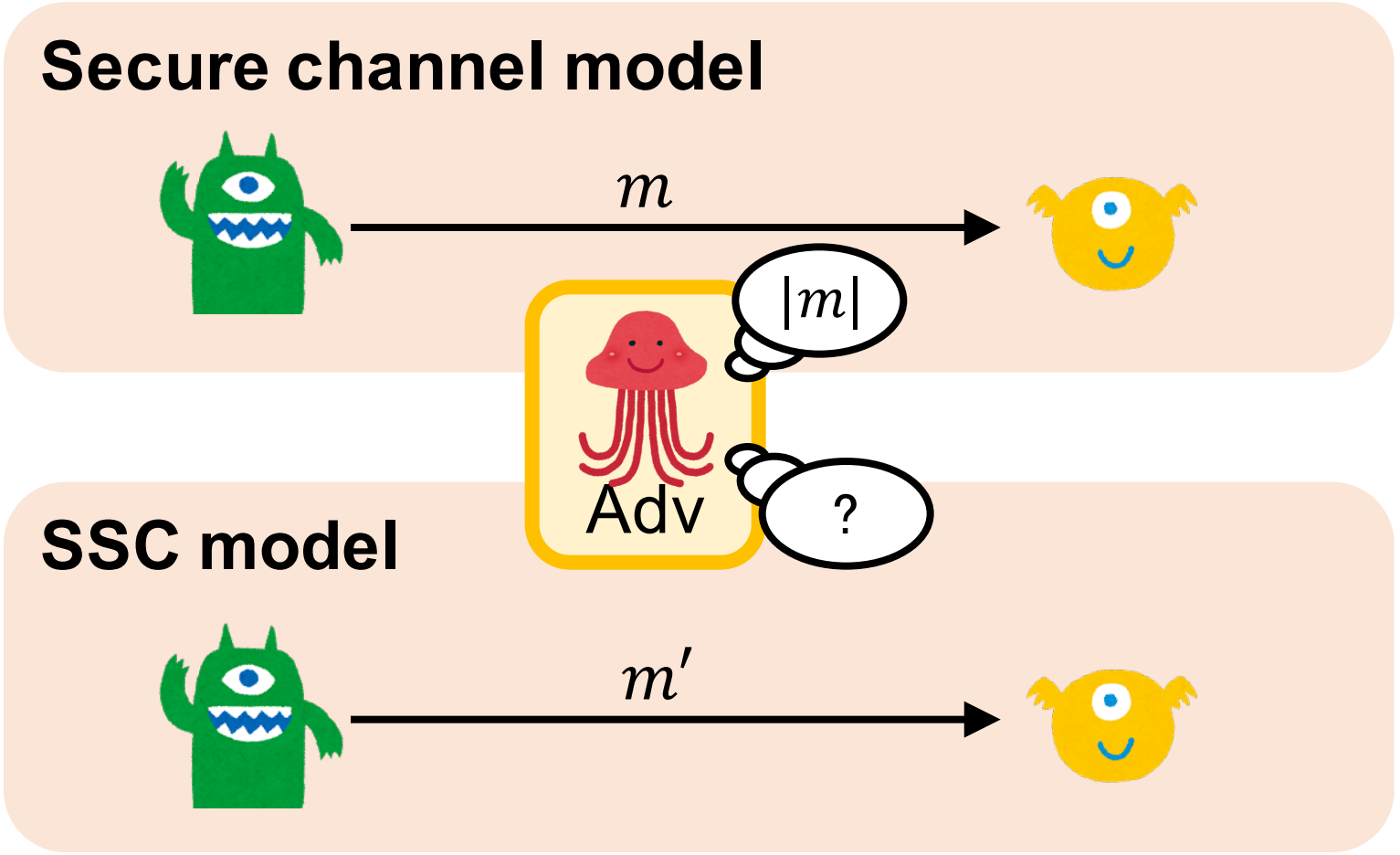
P_3 can know $|x_1|$ and $|x_2|$ but

P_1 cannot send $Enc(x_1)$

P_2 cannot send $Enc(x_2)$

$\because$ channel may leak the number of communication bits

Strong Secure Channel (SSC)



- It is implementable by steganography

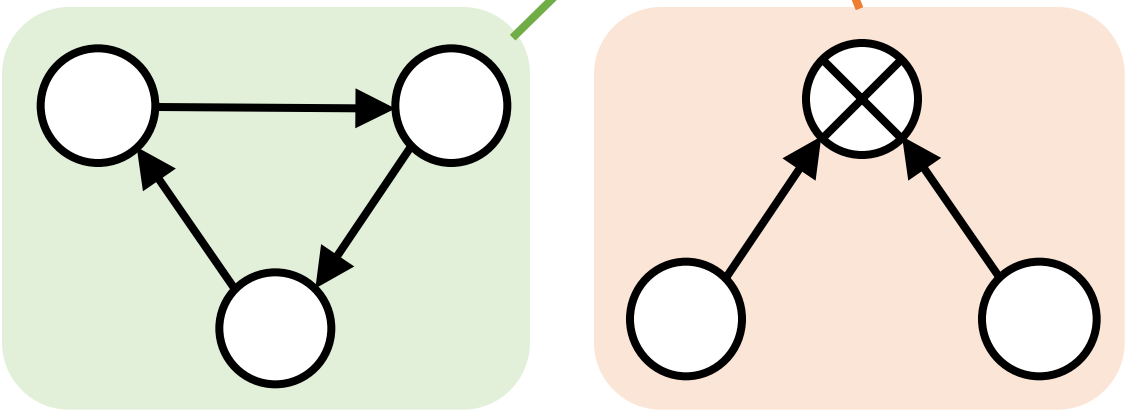
Outline

- NEW Notations
- Classification for two-party [LNO13]
- NEW Classification for multiparty
  - Almost all sizes cannot be hidden
- NEW Strong secure channel (SSC) model
  - It is implementable by steganography
- NEW **Classification for multiparty in SSC model**
  - Many sizes can be hidden in SSC model

Our Result in SSC model

- Complete classification in SSC model
- Maximum number of private sizes is n

# of private sizes	1	2	3	4	…
Secure channel	✔	✘	✘	✘	…
SSC model	✔	✔/✘	✔ ✘	✔/✘	…



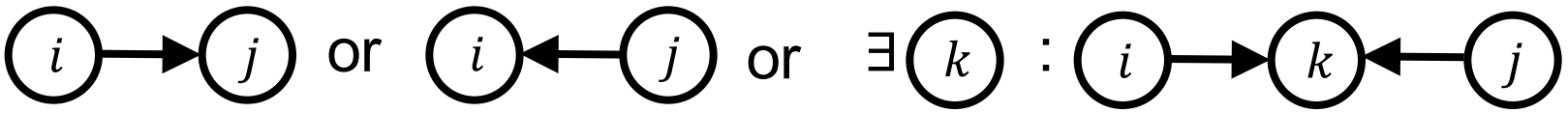
Case 1

When the output-size is public

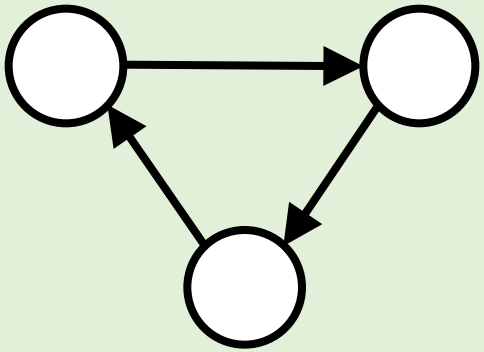
Case 1 (public output-size)

- Suppose the output-size is **public**
- Size-hiding computation is feasible in SSC model

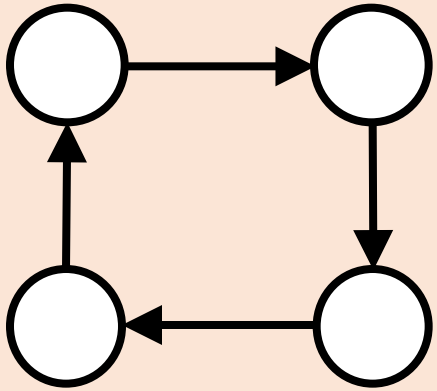
  $\Leftrightarrow$ for every i and j



Feasible!



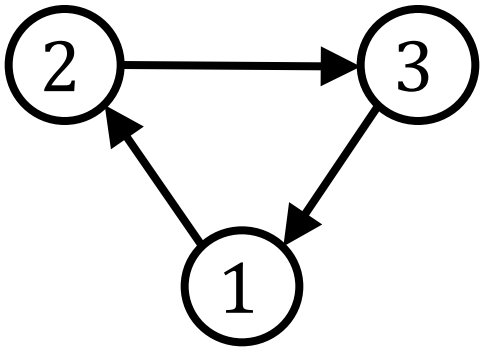
Infeasible



Main Idea for Construction

- Invoke Sharing Protocols for P_1, P_2, P_3

$[x]$: FHE ciphertext



Longest input

Sharing Protocol for P_1:

P_3 sends to P_1:

$[1\ x_3]$

P_2 sends to P_1:

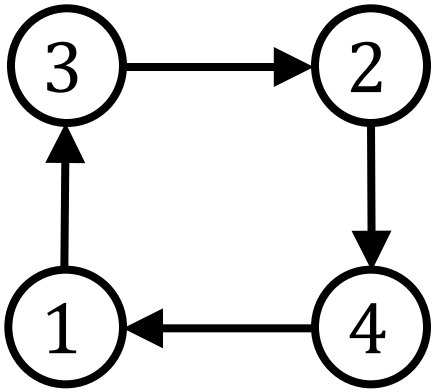
If $|x_1| \geq |x_2|$ $[1\ 0^{|x_1|-|x_2|}\ x_2]$

Otherwise $[0\ 0^{|x_1|}]$

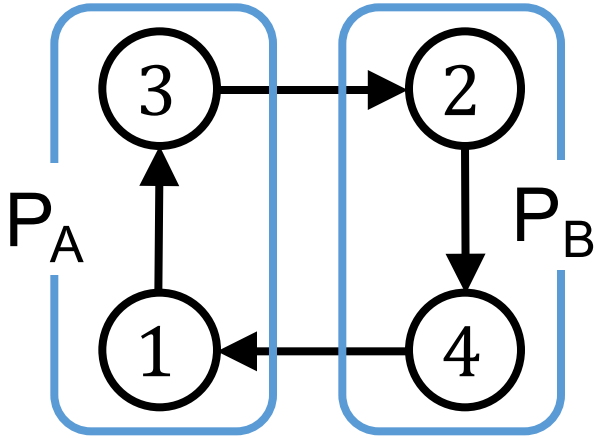
One of them can obtain all flagged ciphertexts!

$\rightarrow [f(x_1, x_2, x_3)]$ can be computed

Infeasibility (Reduced to [LNO13])



$F(x_1, x_2, x_3, x_4)$



- Suppose the class is feasible
- Let $F(x_1, x_2, x_3, x_4) = f(x_1, x_2)$
- Two private sizes (in two-party) is feasible
- It contradicts [LNO13]

Case 2

When the output-size is private

Case 2 (private output-size)

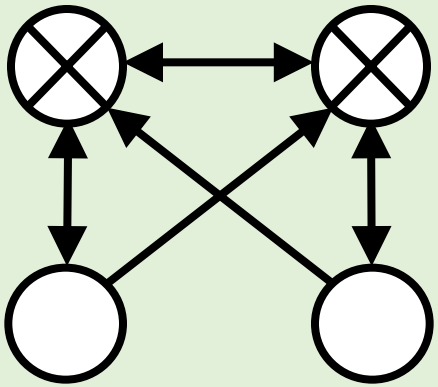
- Suppose the output-size is **private**
- Size-hiding computation is feasible in SSC model

  ⇔ for every ⊗

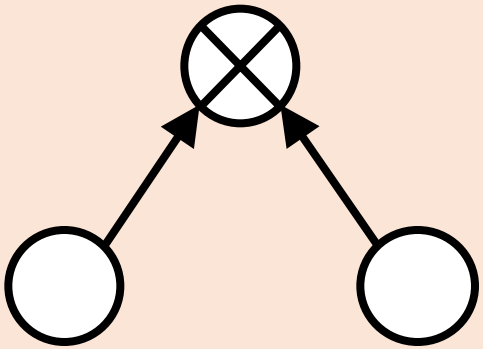
  ✓ The party can know all input-sizes; and

  ✓ ∃○ : ⊗→○

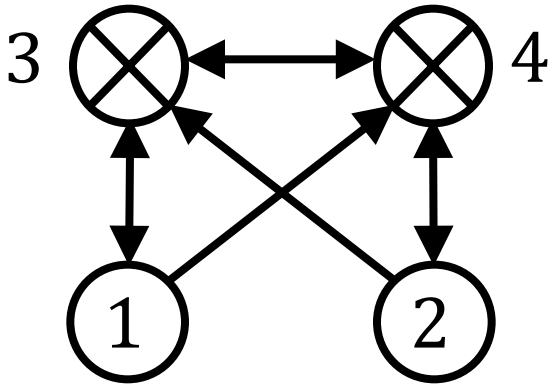
Feasible!



Infeasible



Main Idea for Construction (1)



FHE + MPC

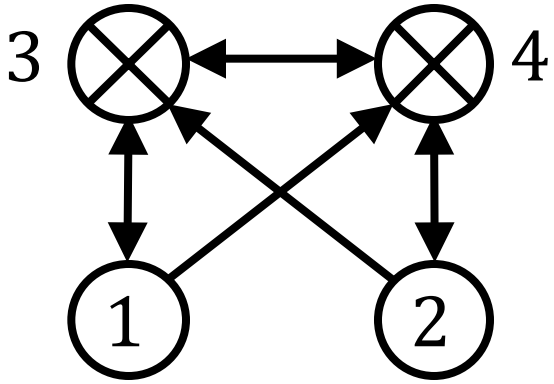
- P_3, P_4 are not involved in **KeyGen**

  $\because$ P_3, P_4 must not join threshold **Decryption of** $[y]$

- P_3, P_4 do **Evaluation**, and obtain $[y]$ with zero paddings

  Thanks to the padding, they can do this without knowing $|y|$

Main Idea for Construction (2)



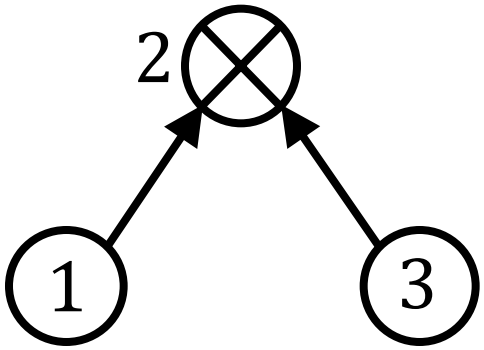
- P_1, P_2 do KeyGen
- P_3, P_4 get encrypted input-shares
- P_3, P_4 do Evaluate using MPC
- P_1, P_2 do threshold Decryption

If P_1, P_2 are corrupted
FHE does not work → P_3 or P_4 is honest
Security by MPC

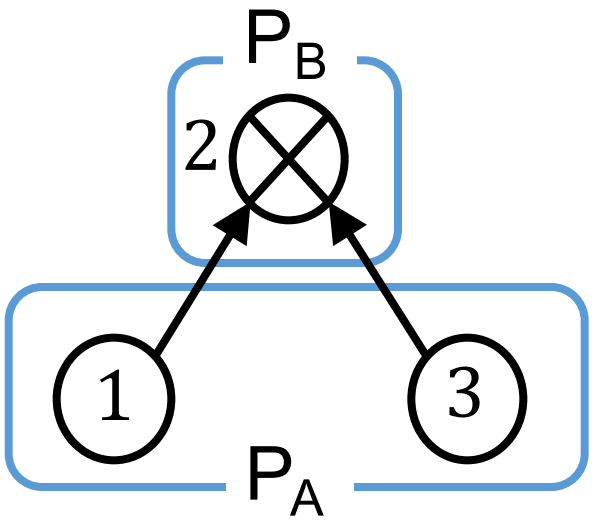
If P_3, P_4 are corrupted
MPC does not work → P_1 or P_2 is honest
Security by FHE

FHE or MPC guarantee the security!

Infeasibility (Reduced to [LNO13])



$F(x_1, x_2, x_3)$



- Suppose the class is feasible
- Let $F(x_1, x_2, x_3) = f(x_1, x_2)$
- Two private sizes (in two-party) is feasible
- It contradicts [LNO13]

Conclusion

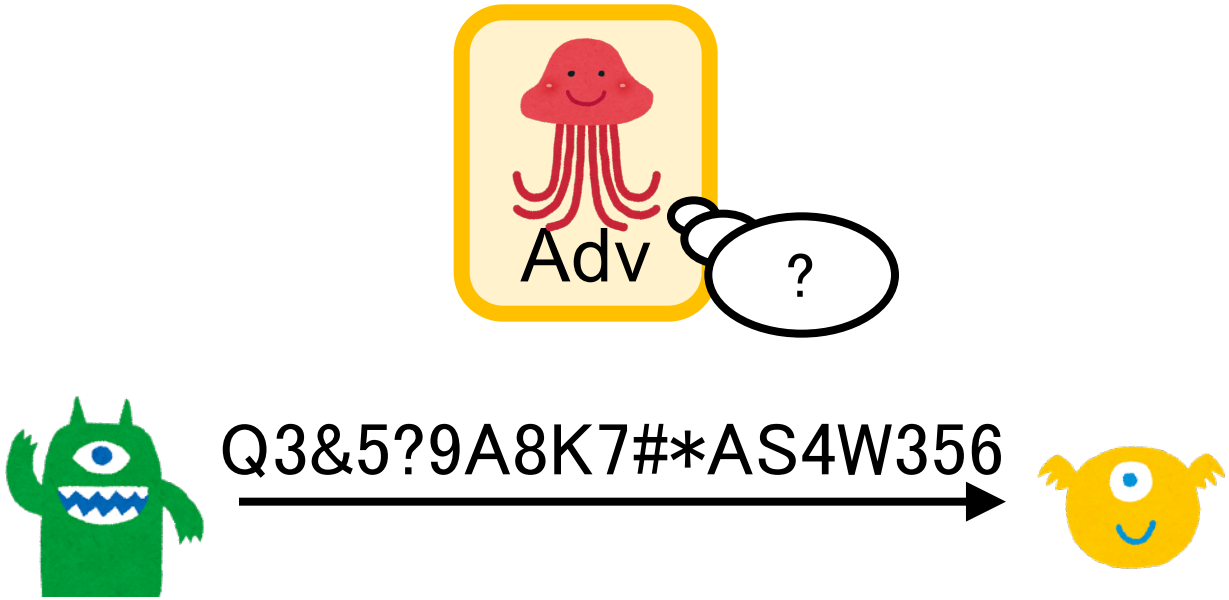
- Hiding two is infeasible (standard model)

- SSC model is rich for size-hiding
- Some of them are still infeasible

Thank you for your attention!

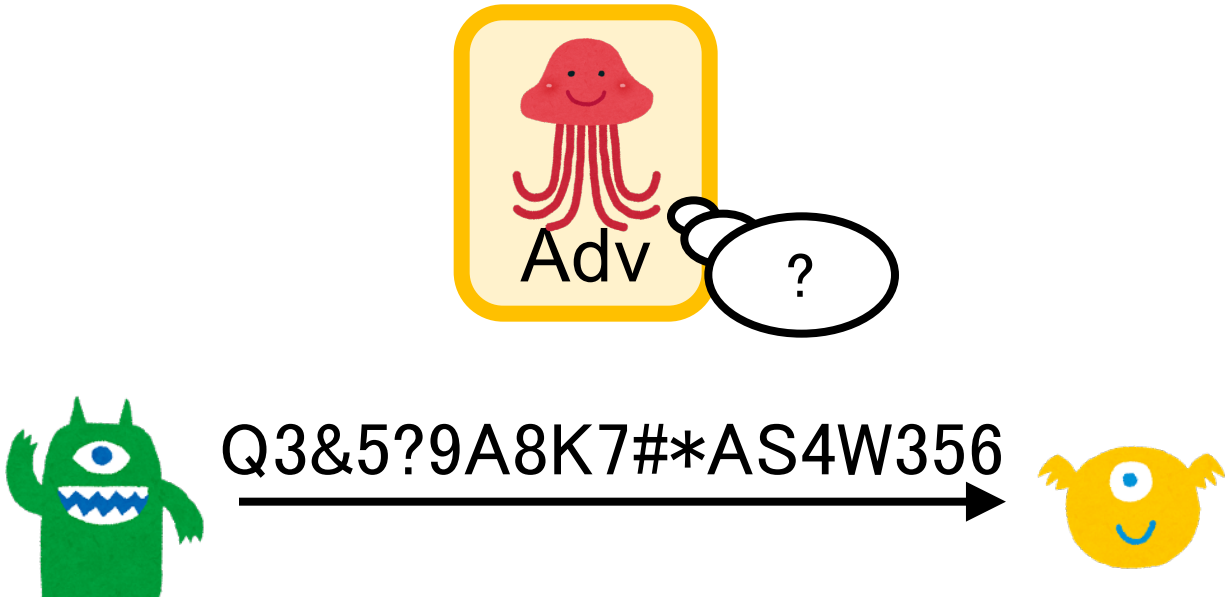
Q&A

- How to implement SSC by steganography?
  - A party can hide message of an arbitrary length



Q&A

- How to implement SSC by steganography?
  - A party can hide message of an arbitrary length



Conclusion

Background

- [LNO13] constructed size-hiding protocol for two parties
- They also proved the strong limitation

This work

- We introduce the strong secure channel (SSC) model
- We construct size-hiding protocols in the SSC model
- We also prove the (weaker) limitation for the SSC model

Thank you for your attention!

Set Intersection

- Police has a list of terrorists X
- Company has a list of customers Y
- Police wish to compute $X \cap Y$ without revealing

- Naïve approach, Padding, is inefficient

- **Millionaire Problem** (Population version)
  - Aliens: “Which planet has the largest population?”
  - The population is related to the military power
  - Its size is also related to the military power
  - Padding doesn’t work since the upper-bound is too large