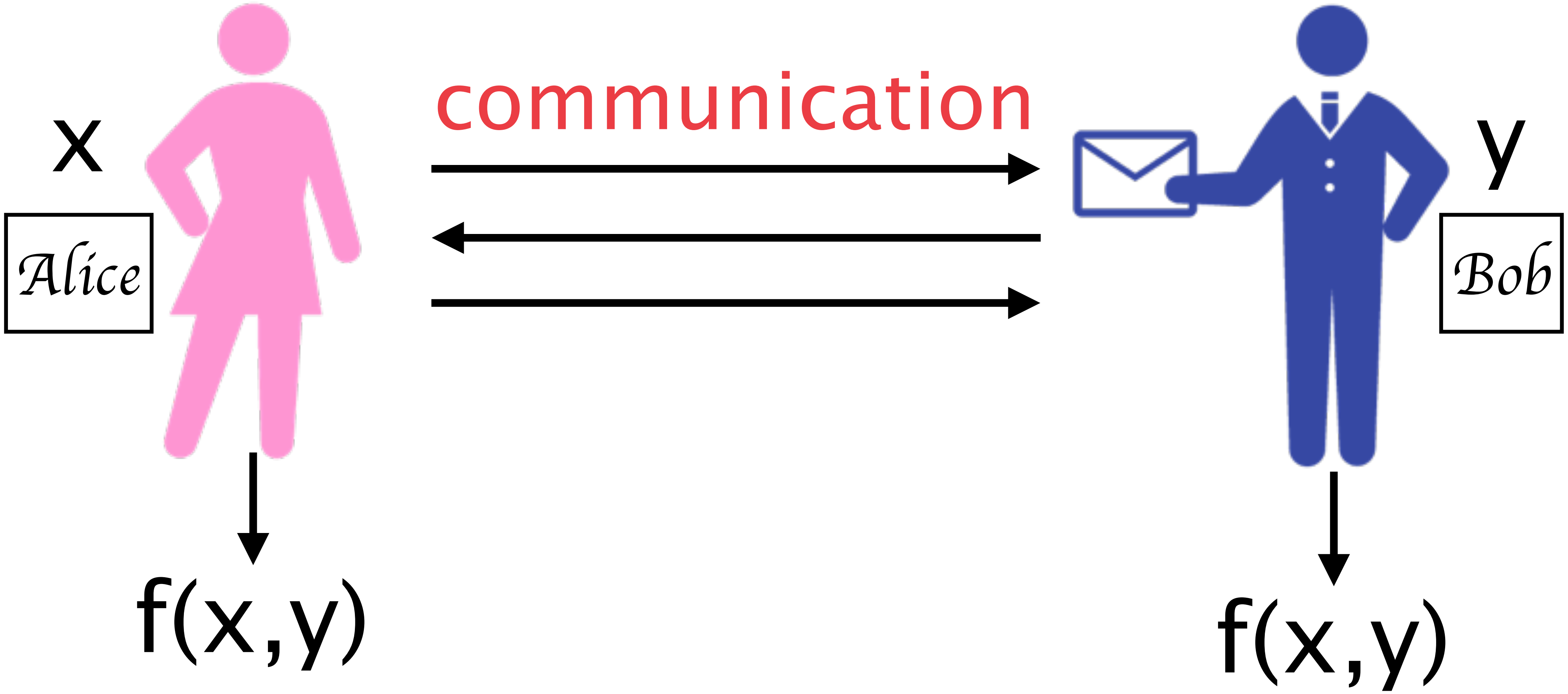
Multi-Party Computation with Small Shuffle Complexity Using Regular Polygon Cards

Kazumasa Shinagawa (Univ. Tsukuba)
Jacob Schuldt (AIST)
Naoki Kanayama (Univ. Tsukuba)
Goichiro Hanaoka (AIST)
Takaaki Mizuki (Tohoku Univ.)
Koji Nuida (AIST)
Takashi Nishide (Univ. Tsukuba)
Eiji Okamoto (Univ. Tsukuba)

Secure Protocol (without Cards)



x

Alice

communication

y

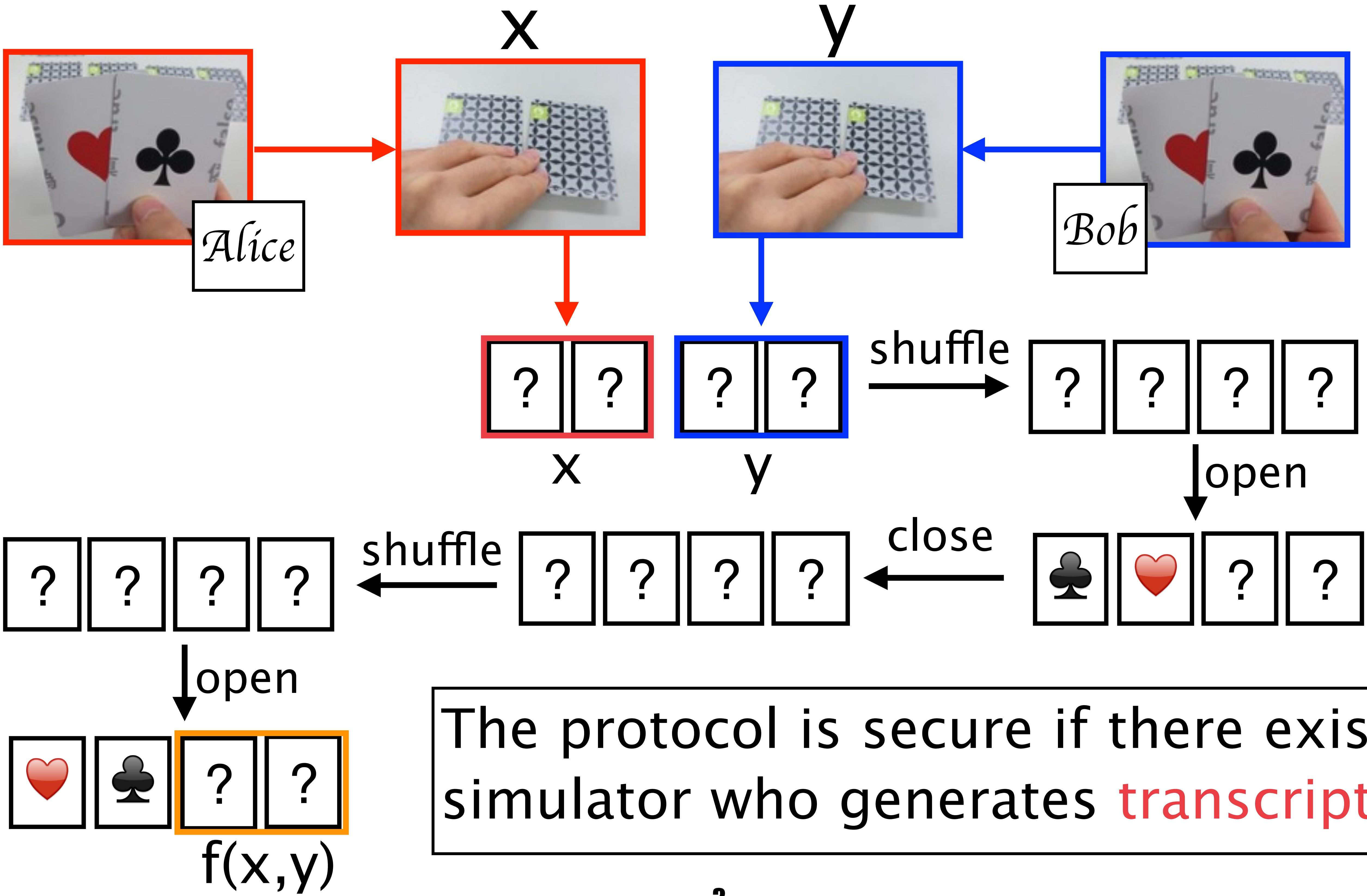
Bob

f(x,y)

f(x,y)

The protocol is secure if there exists a simulator that can generates transcripts

Card-based Protocol



x

y

Alice

Bob

? ? ? ?

x y

shuffle

? ? ? ?

open

♣ ♥ ? ?

close

? ? ? ?

shuffle

? ? ? ?

open

♥ ♣ ? ?

f(x,y)

The protocol is secure if there exists simulator who generates transcripts

Previous Works

- All previous works focus on boolean circuits

How to deal with arithmetic circuits?

- Many works aims to reduce the number of cards
  - n-ary function: 2n+6 cards [Nishida et al. 15]
- No results to reduce the number of shuffles

How to reduce the number of shuffles?

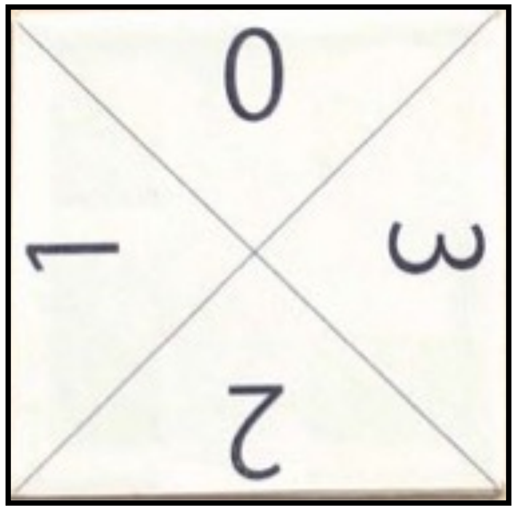
Our Contribution

- New cards for arithmetic circuits
  - Regular polygon cards

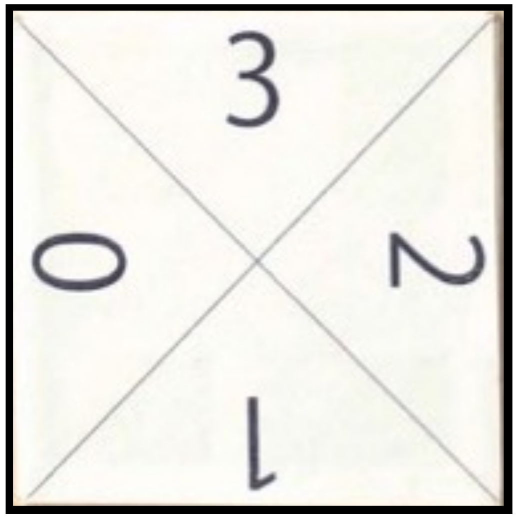
- New technique for reducing Num. of shuffles

Regular Polygon Card:

- polygon shaped
- 3-sided, 4-sided, 5-sided, and so on.



0

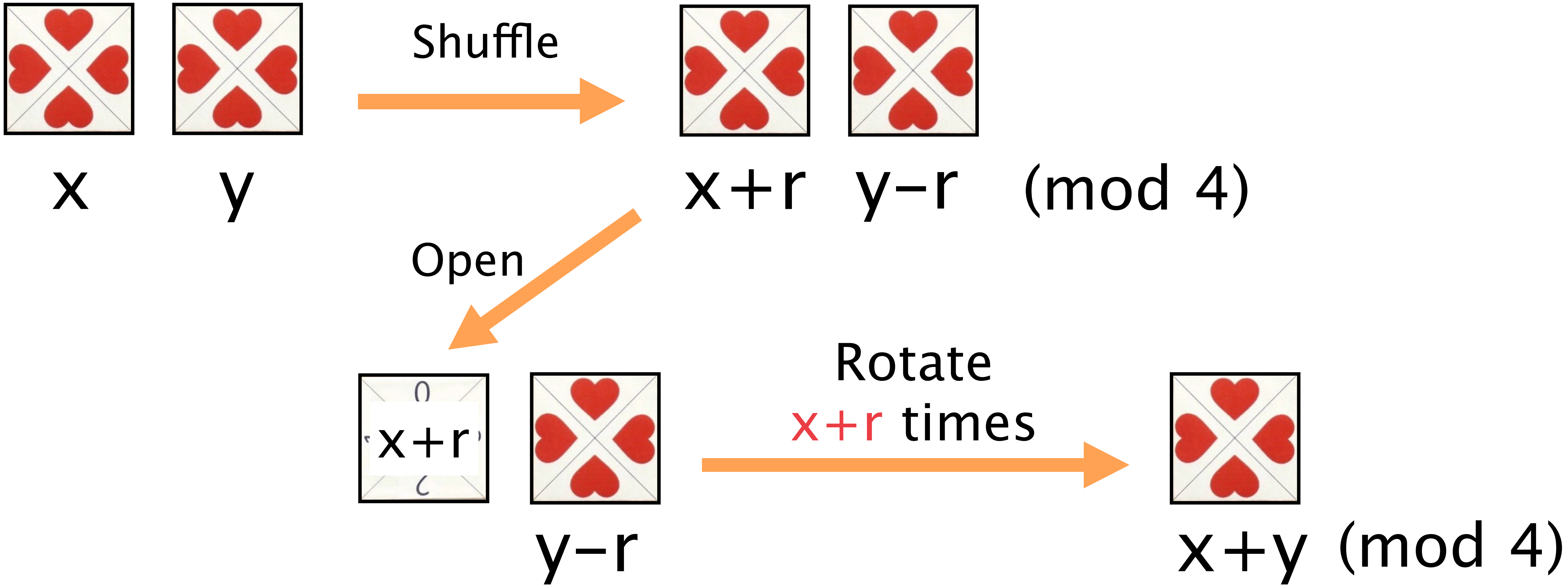


3

- back side has rotational symmetric pattern

Addition Protocol

Rotate two cards “r”–times (“r” is hidden to parties)



x y

Shuffle

x+r y−r (mod 4)

Open

x+r y−r

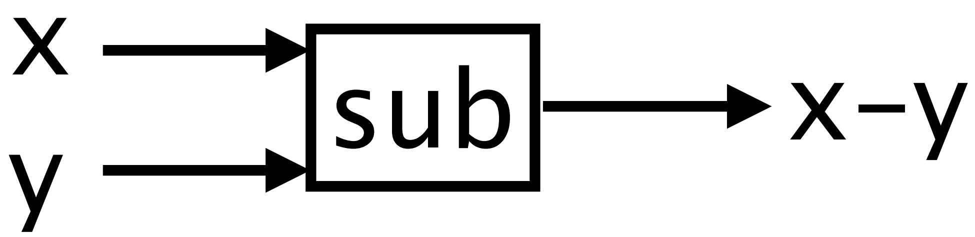
Rotate
x+r times

x+y (mod 4)

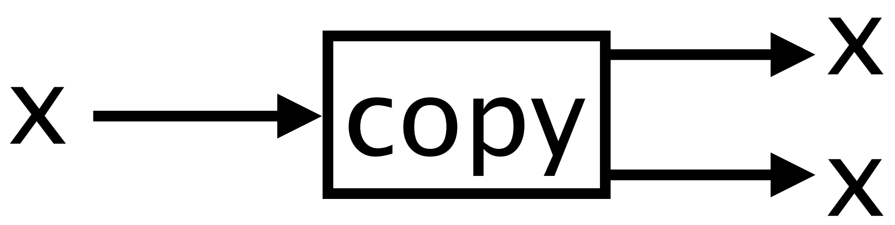
Note: “x+r” does not reveal any secret information
since nobody knows the random value “r”.

Demo.
Addition Protocol

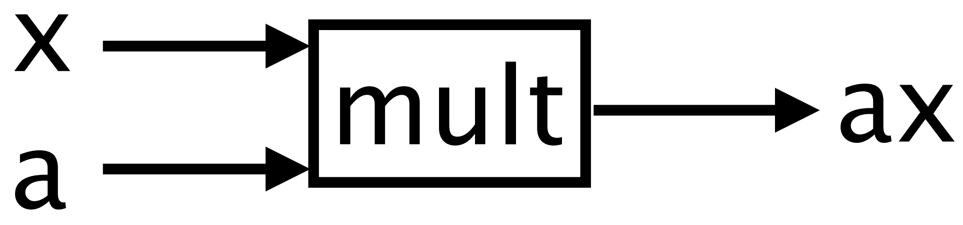
Subtraction Protocol

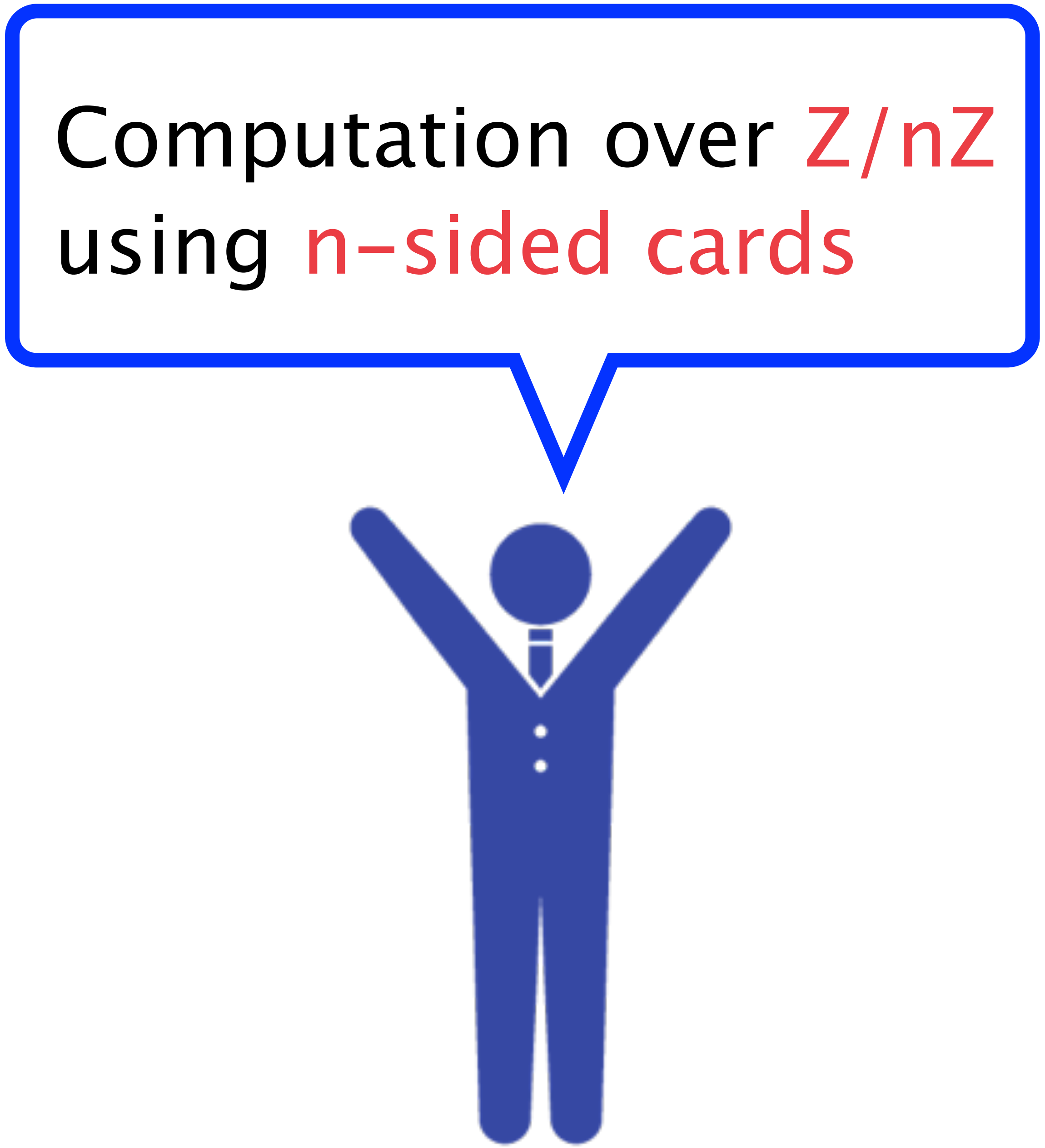


Copy Protocol



Multiplication Protocol





Computation over Z/nZ using n−sided cards

Demo.
Evaluation of f(x)

Shuffle-Efficient Protocols

Any 1-ary function f(x)	2 shuffles
Any 2-ary function f(x,y)	4 shuffles
:	
Any n-ary function	2n shuffles

Nishida et al.

$O(2^n)$ shuffles
2n+6 cards

⇔ trade-off

Our work

2n shuffles
$O(2^n)$ cards

Summary

- New cards for arithmetic circuits
  - Regular polygon cards
  - Protocols for Linear Function (Add/Sub/…)

- New technique for reducing Num. of shuffles
  - Any n-ary function with 2n shuffles