CSF 2021, June 22, Session 4, 15:00–15:45

Cooking Cryptographers: Secure Multiparty Computation Based on Balls and Bags

Daiki Miyahara[1,2]   Yuichi Komano[3]
Takaaki Mizuki[1,2]   Hideaki Sone[1]

1. Tohoku University, Email: daiki.miyahara.q4[at]alumni.tohoku.ac.jp
2. National Institute of Advanced Industrial Science and Technology (AIST)
3. Toshiba Corporation

Outline

1. Introduction: Cooking Cryptographers Problem
2. Our Proposed Protocol
3. Changing the Settings
4. Contribution
5. Conclusion

Outline

1. Introduction: Cooking Cryptographers Problem

2. Our Proposed Protocol

3. Changing the Settings

4. Contribution

5. Conclusion

What is Cooking Cryptographers Problem?

Analog of the Dining Cryptographers problem[1]

✓Assume that Alice and Bob are cooking Borscht soup

Alice

Borscht soup

Bob

[1] D. Chaum, The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability, Journal of Cryptology, vol. 1, pp. 65–75, 1988

What is Cooking Cryptographers Problem?

Analog of the Dining Cryptographers problem[1]

✓Assume that Alice and Bob are cooking Borscht soup

Alice

🥕 🧅 🧅

Borscht soup

Bob

🥕 🧅 🧅

✓Prepared ingredients either paid out of *pockets* or funded by *NFSA*‡

[1] D. Chaum, The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability, Journal of Cryptology, vol. 1, pp. 65–75, 1988

‡ National Fictional Security Agency

What is Cooking Cryptographers Problem?

Analog of the Dining Cryptographers problem[1]

✓Assume that Alice and Bob are cooking Borscht soup

Alice
Borscht soup
Bob

✓Prepared ingredients either paid out of *pockets* or funded by *NFSA*‡

✓Respect each other’s ideology to have a relation to NFSA, but…

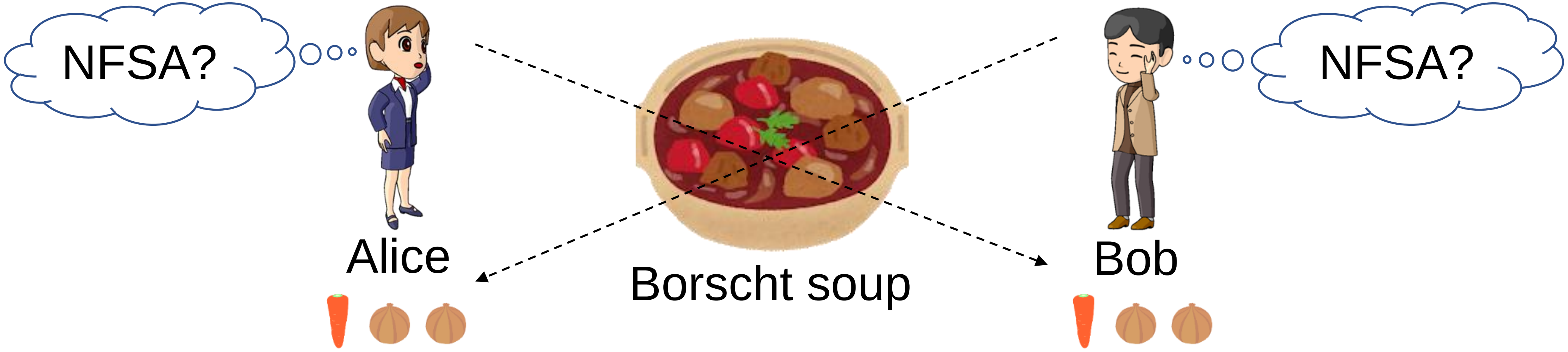
[1] D. Chaum, The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability, Journal of Cryptology, vol. 1, pp. 65–75, 1988

‡ National Fictional Security Agency

What is Cooking Cryptographers Problem?

Analog of the Dining Cryptographers problem[1]

✓Assume that Alice and Bob are cooking Borscht soup



✓Prepared ingredients either paid out of *pockets* or funded by *NFSA*‡

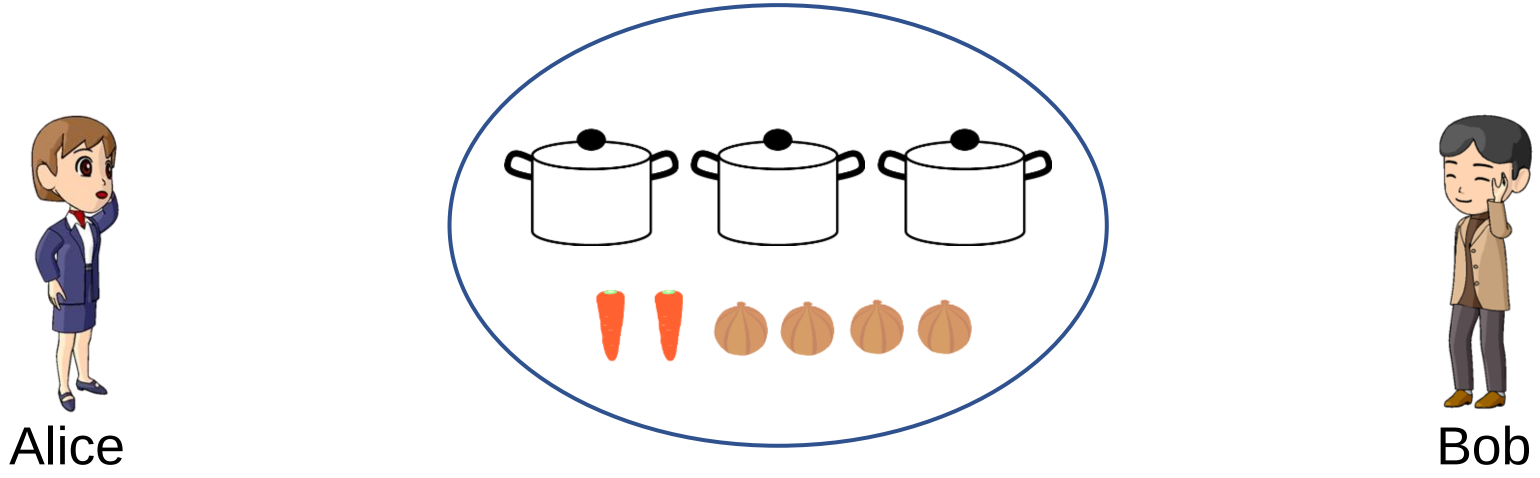
✓Respect each other's ideology to have a relation to NFSA, but…

✓Wonder if they eat food funded by NFSA

[1] D. Chaum, The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability, Journal of Cryptology, vol. 1, pp. 65–75, 1988

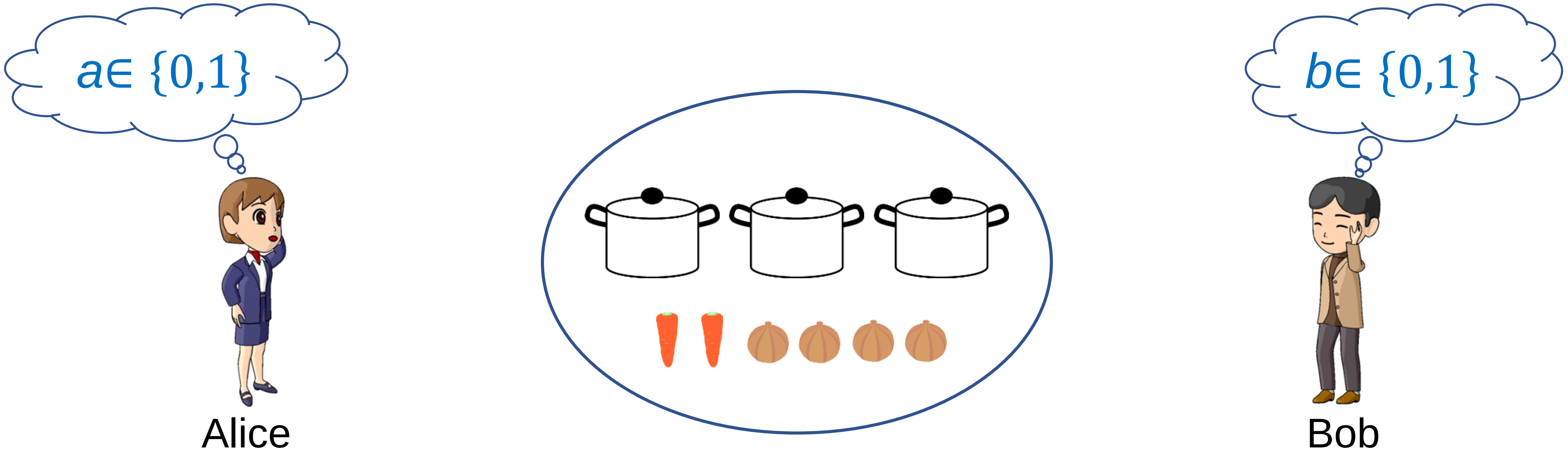
‡ National Fictional Security Agency

Cooking Cryptographers Problem: Secure AND Computation



✓They are in the kitchen, and there are the ingredients and saucepans

Cooking Cryptographers Problem: Secure AND Computation

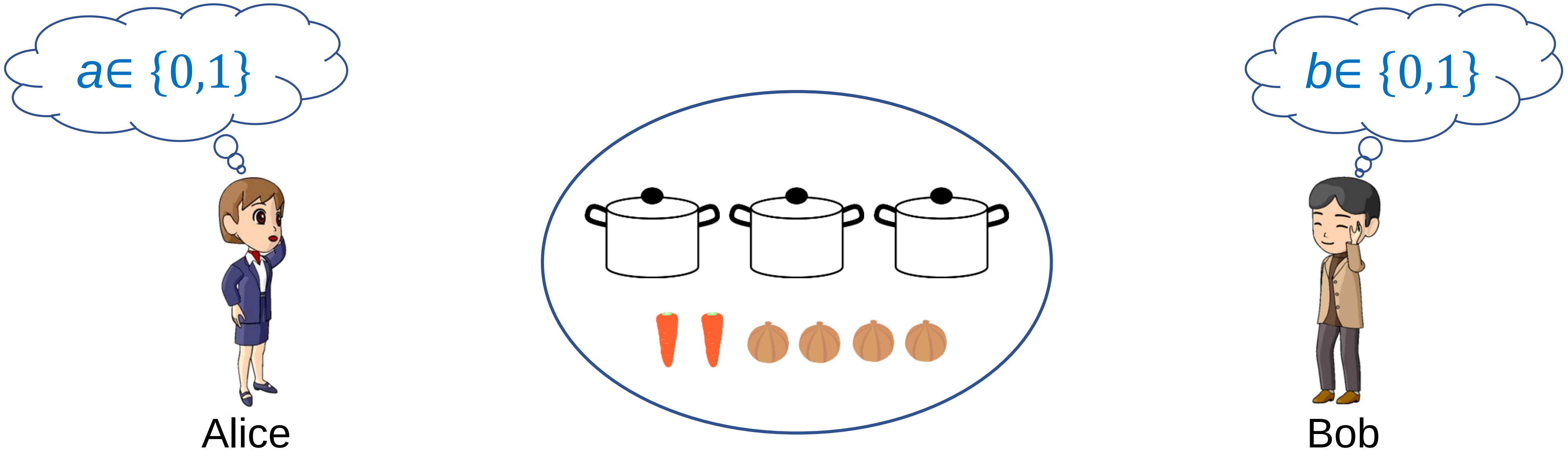


✓They are in the kitchen, and there are the ingredients and saucepans

✓Each of them has their private bit:

Funded by NFSA = 0, Paid out of pocket = 1

Cooking Cryptographers Problem: Secure AND Computation

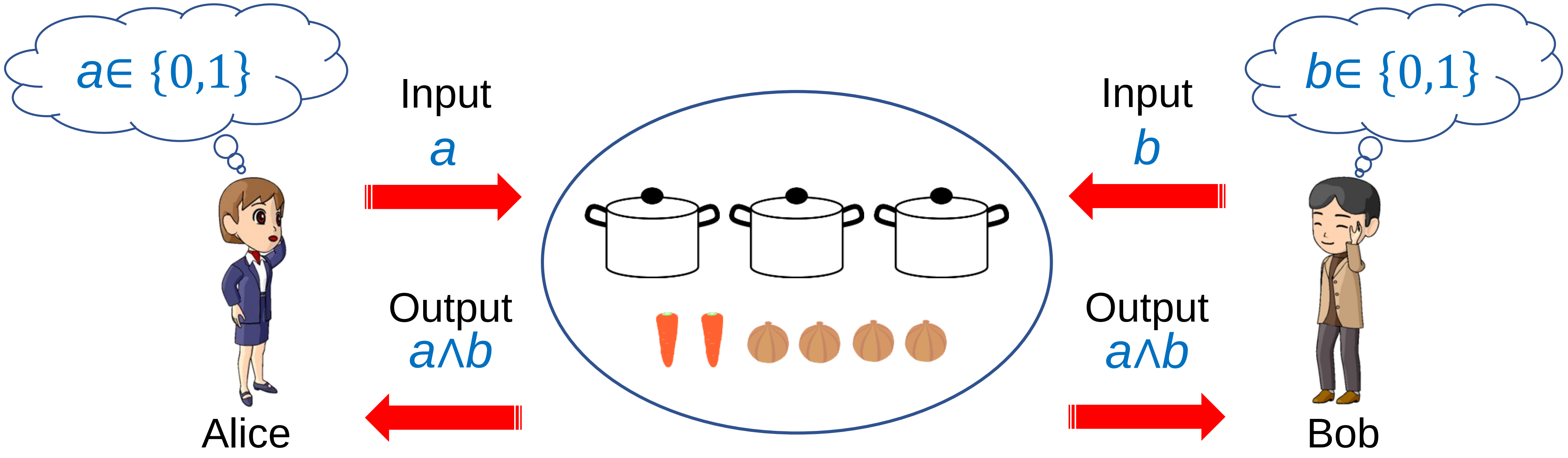


✓They are in the kitchen, and there are the ingredients and saucepans

✓Each of them has their private bit:
Funded by NFSA = 0, Paid out of pocket = 1

✓The goal: obtain $a \wedge b$ without revealing any information about a and b

Cooking Cryptographers Problem: Secure AND Computation



$a \in \{0,1\}$

Input a

Output $a \wedge b$

Alice

$b \in \{0,1\}$

Input b

Output $a \wedge b$

Bob

✓They are in the kitchen, and there are the ingredients and saucepans

✓Each of them has their private bit:
Funded by NFSA = 0, Paid out of pocket = 1

✓The goal: obtain $a \wedge b$ without revealing any information about a and b

Outline

1. Introduction: Cooking Cryptographers Problem

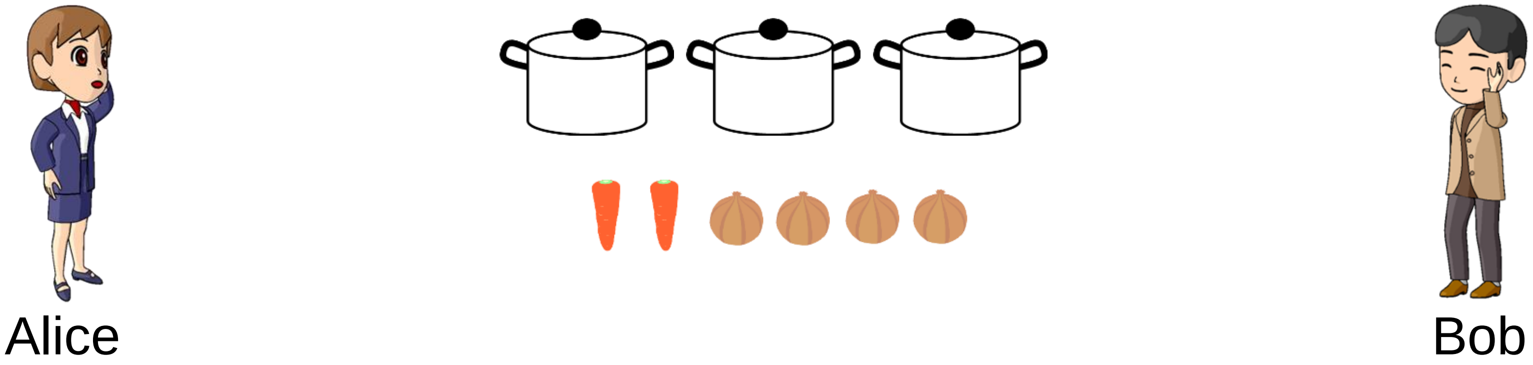
2. Our Proposed Protocol

3. Changing the Settings

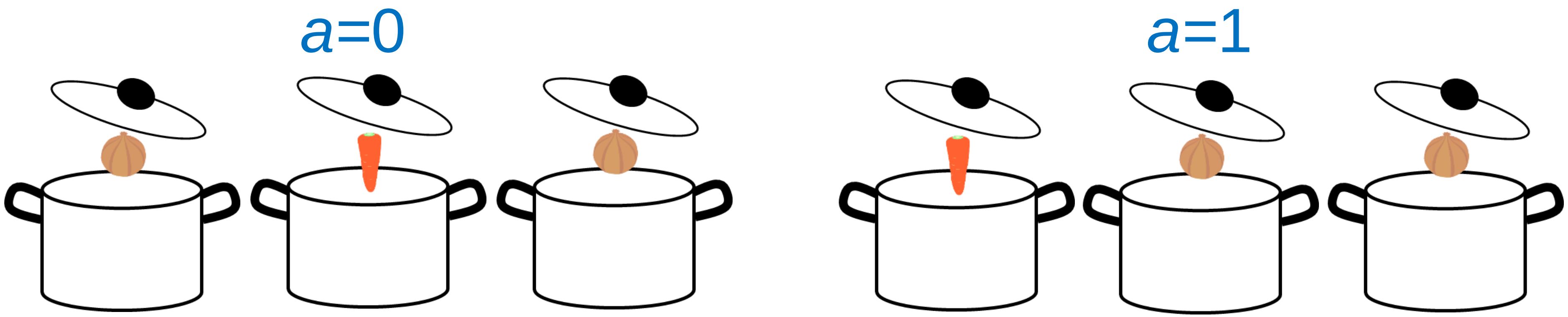
4. Contribution

5. Conclusion

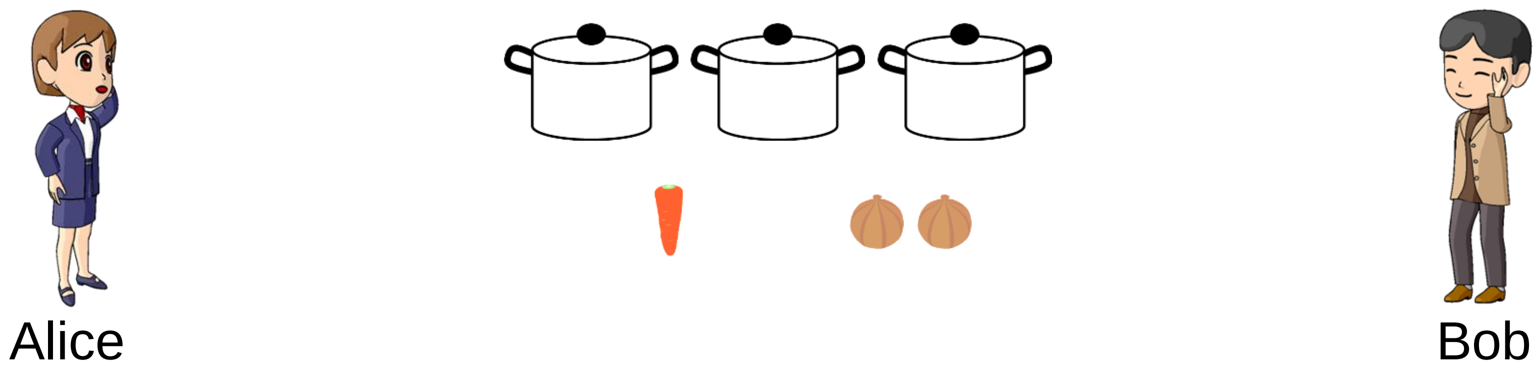
Our Proposed Protocol Performing Secure AND Computation



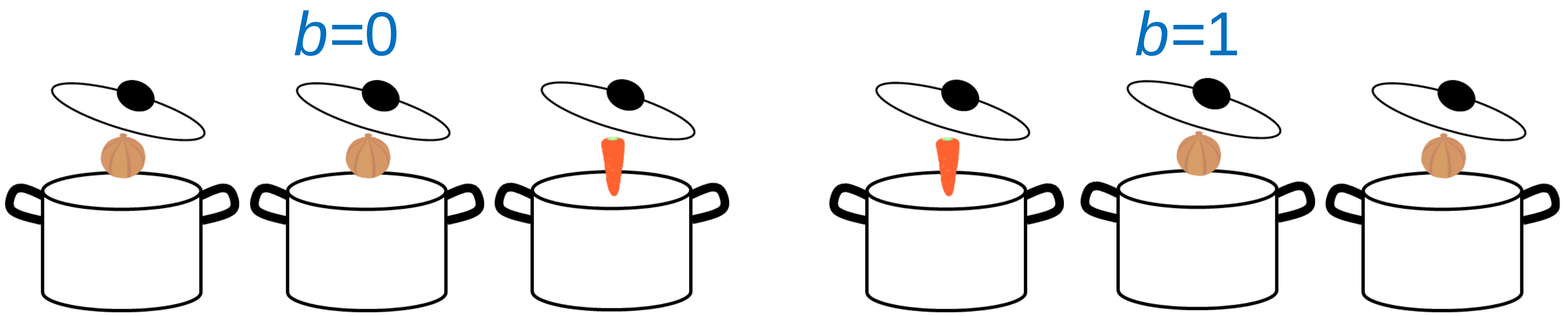
1. Alice puts ingredients into saucepans depending on the value of *a* (so that Bob cannot see them):



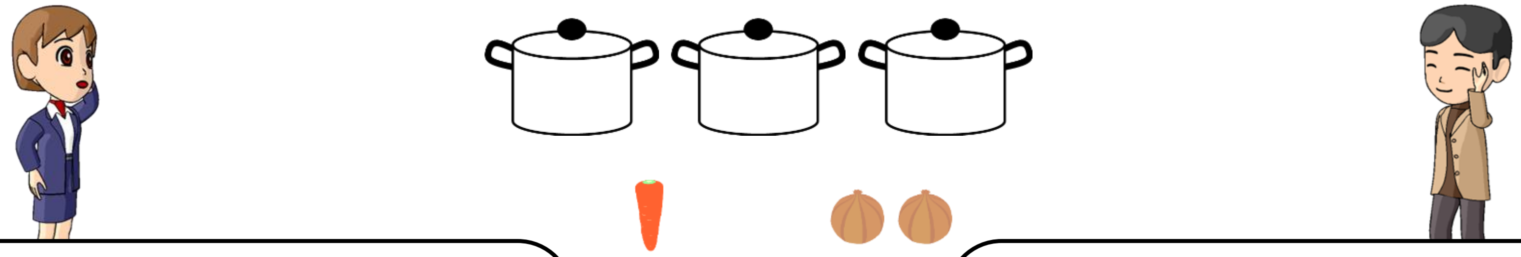
Our Proposed Protocol Performing Secure AND Computation



2. Bob puts ingredients into saucepans depending on the value of *b* (so that Alice cannot see them):



Our Proposed Protocol Performing Secure AND Computation



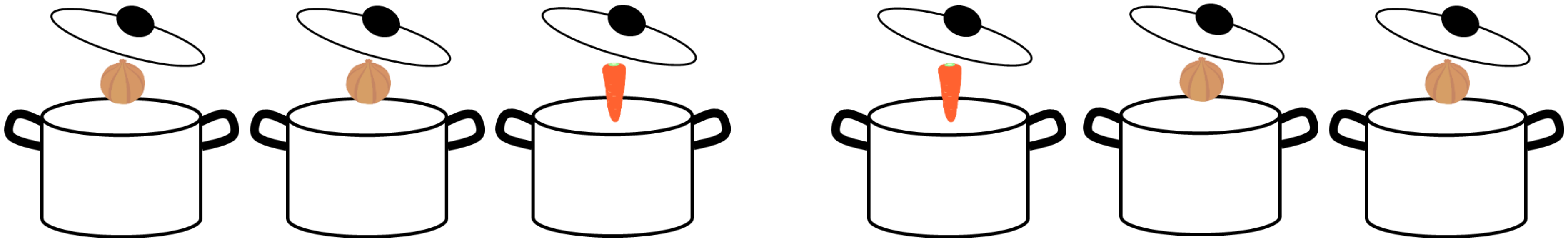
2. Bob p aucepans de of *b*
(so th em):

The position is *different* to Alice

The position is the *same* to Alice

b=0

b=1



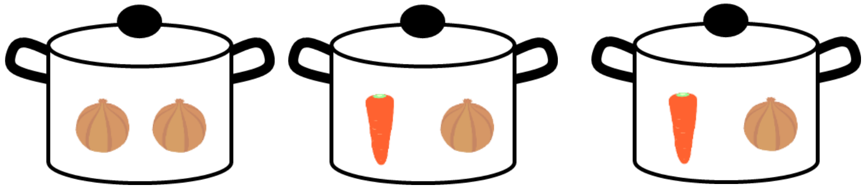
Our Proposed Protocol Performing Secure AND Computation

✓Consider the breakdown of ingredients in the three saucepans:

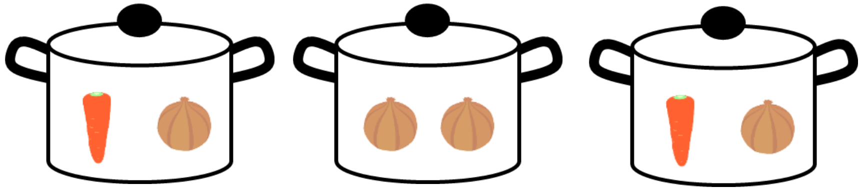
Our Proposed Protocol Performing Secure AND Computation

✓Consider the breakdown of ingredients in the three saucepans:

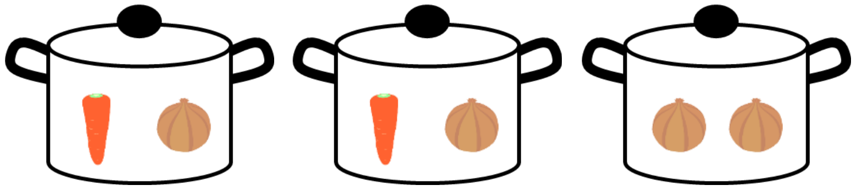
a=0/*b*=0



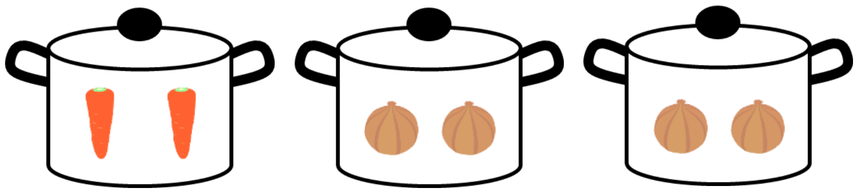
a=1/*b*=0



a=0/*b*=1

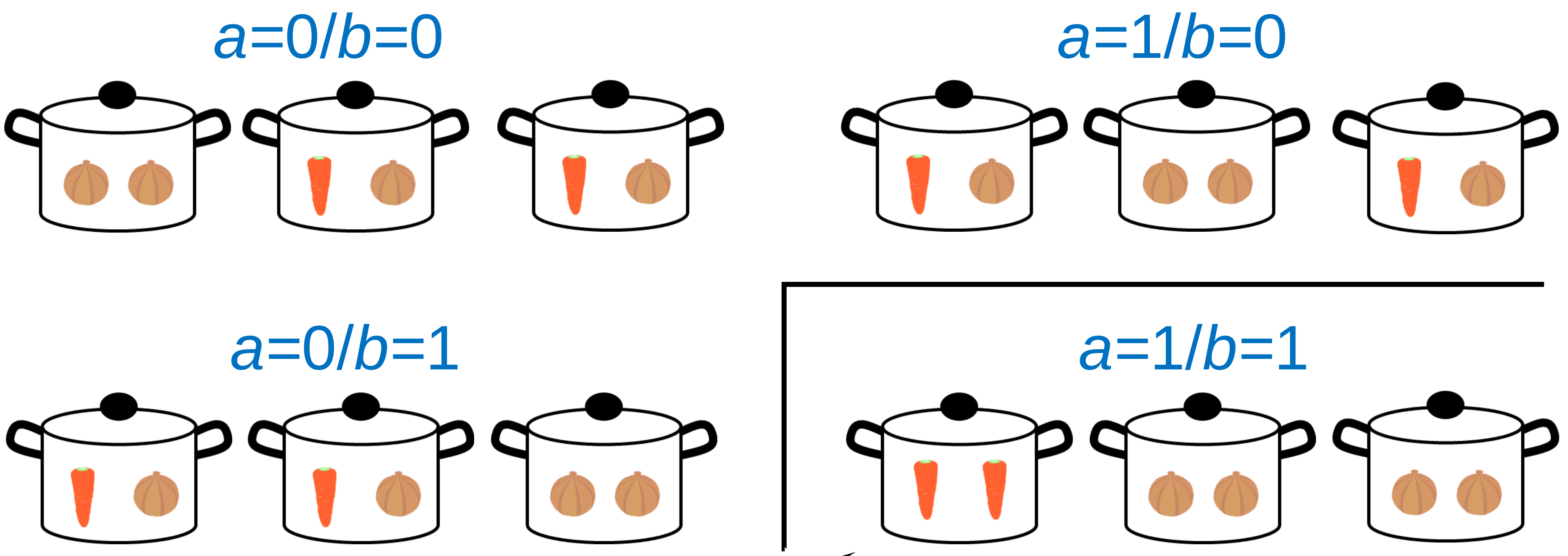


a=1/*b*=1



Our Proposed Protocol Performing Secure AND Computation

✓Consider the breakdown of ingredients in the three saucepans:



$a=0/b=0$

$a=1/b=0$

$a=0/b=1$

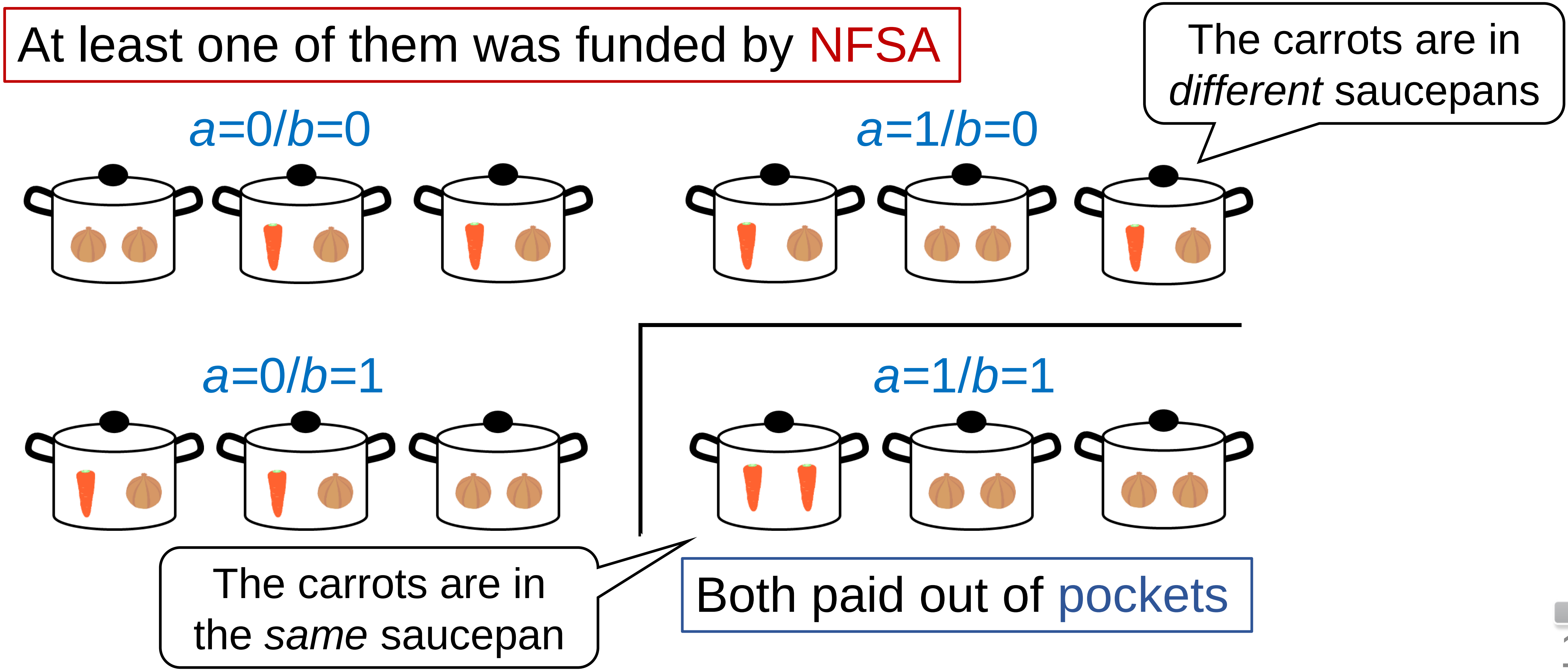
$a=1/b=1$

The carrots are in the *same* saucepan

Both paid out of pockets

Our Proposed Protocol Performing Secure AND Computation

✓Consider the breakdown of ingredients in the three saucepans:



At least one of them was funded by NFSA

The carrots are in *different* saucepans

a=0/*b*=0

a=1/*b*=0

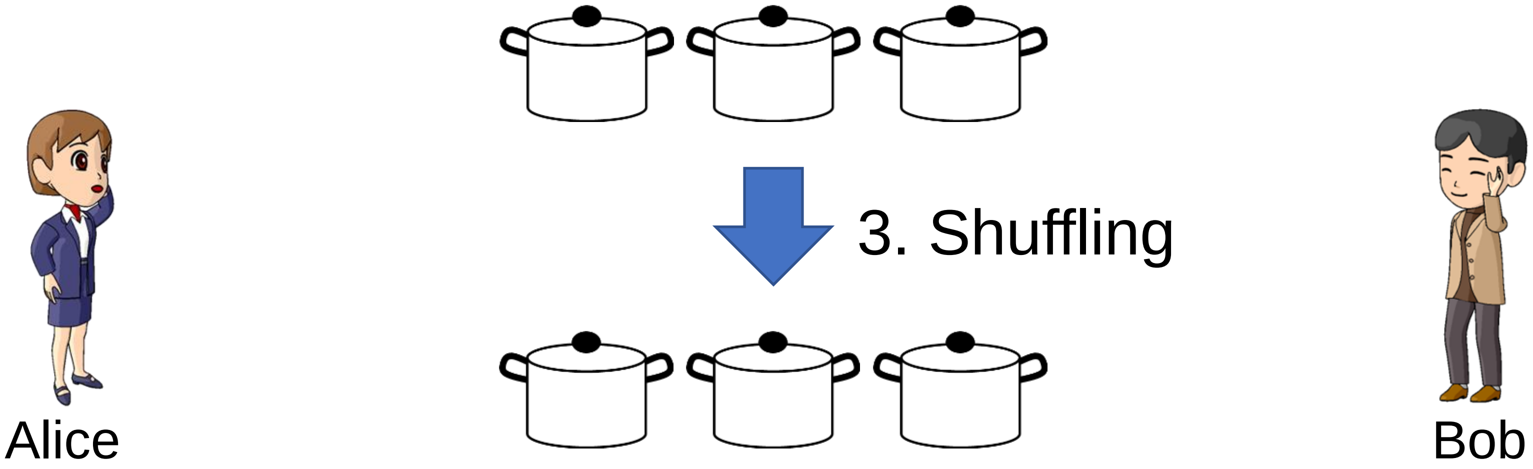
a=0/*b*=1

a=1/*b*=1

The carrots are in the *same* saucepan

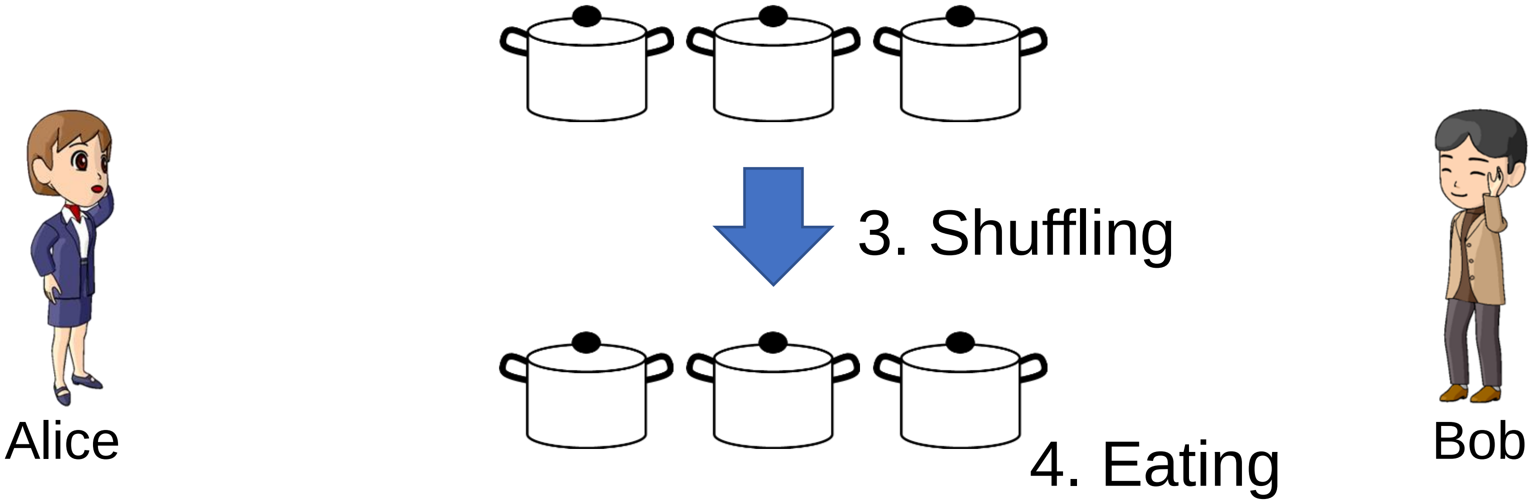
Both paid out of pockets

Our Proposed Protocol Performing Secure AND Computation



3. Shuffle the order of the three saucepans

Our Proposed Protocol Performing Secure AND Computation



Alice

3. Shuffling

4. Eating

Bob

3. Shuffle the order of the three saucepans
4. Enjoy eating the cooked Borscht soup:
   If there is a saucepan only with carrots, then $a \wedge b=1$ (pockets);
   otherwise, $a \wedge b=0$ (NFSA)

Outline

1. Introduction: Cooking Cryptographers Problem

2. Our Proposed Protocol

3. Changing the Settings

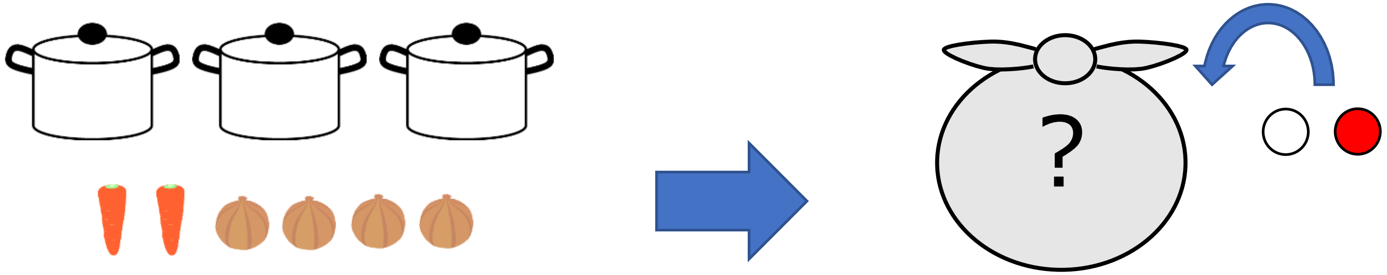
4. Contribution

5. Conclusion

Change the Settings from Kitchen to Using Balls and Bags

✓Replace: ingredients ↦ balls, saucepans ↦ bags

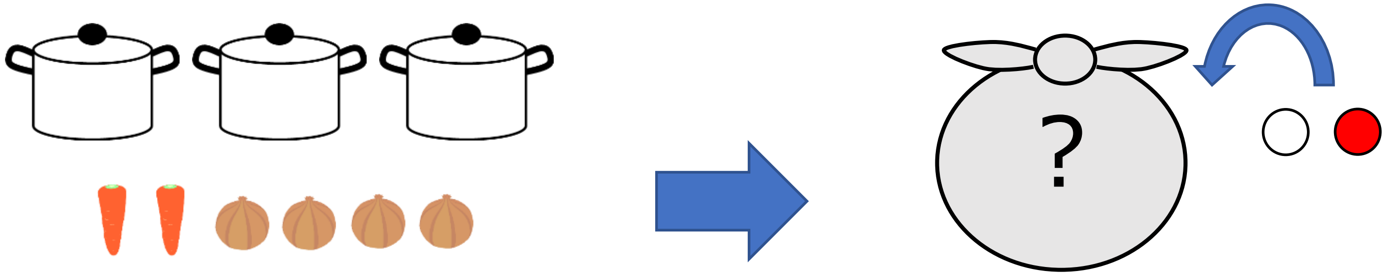
Cooking every time to perform secure computations is difficult…



Change the Settings from Kitchen to Using Balls and Bags

✓Replace: ingredients ↦ balls, saucepans ↦ bags

Cooking every time to perform secure computations is difficult…

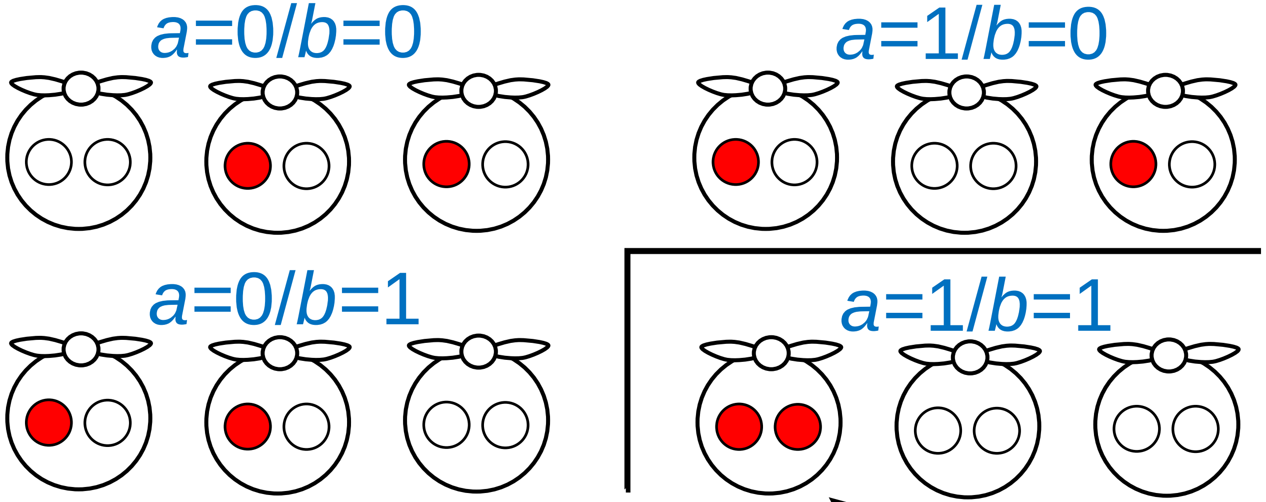


✓ Balls and bags are easy to prepare, and they are also familiar tools for learning Probability in high school

Change the Settings from Kitchen to Using Balls and Bags

✓It also *performs* the secure computation if we replace ingredients and saucepans with balls and bags, respectively

The red balls are in *different* bags



The red balls are in the *same* bag

Outline

1. Introduction: Cooking Cryptographers Problem

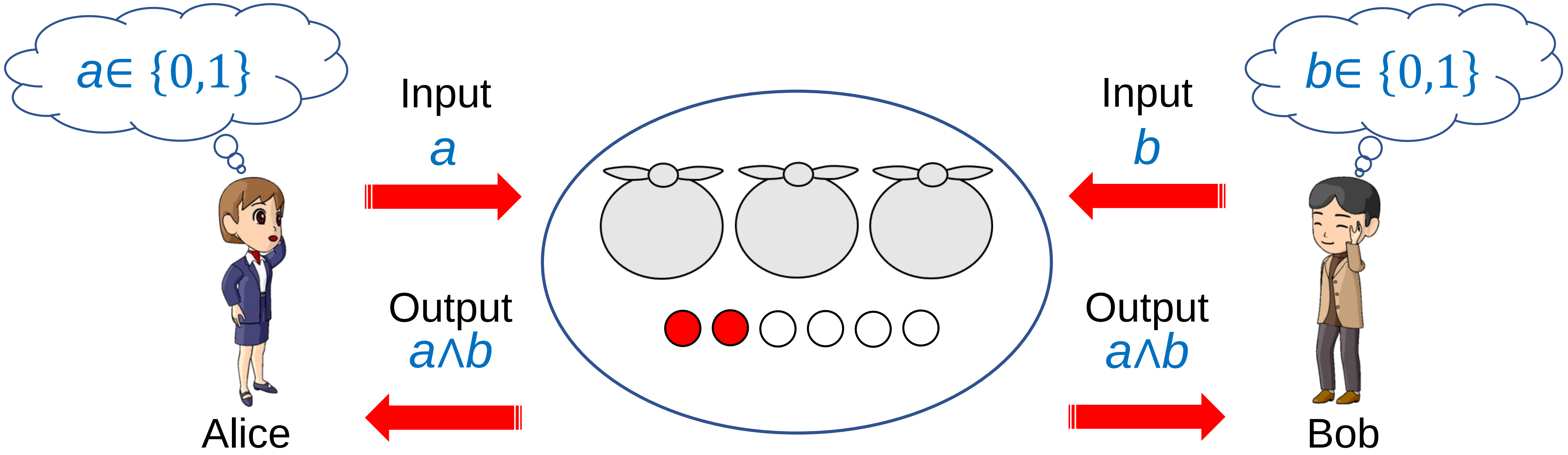
2. Our Proposed Protocol

3. Changing the Settings

4. Contribution

5. Conclusion

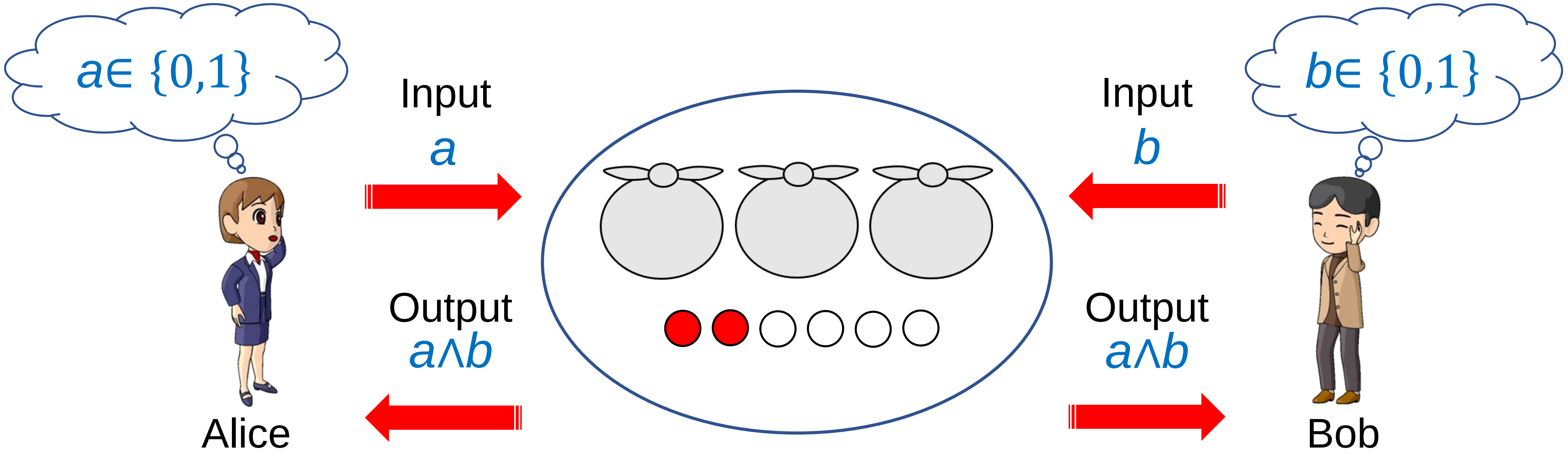
Contribution: Secure computations using balls and bags



✓Employ a property that the order of balls in a bag is disordered

✓Extend our two-input AND to the *multi-input* AND

Contribution: Secure computations using balls and bags



✓Employ a property that the order of balls in a bag is disordered

✓Extend our two-input AND to the *multi-input* AND

✓Formalize secure computation using balls and bags

✓Construct a protocol for *any* Boolean function

Outline

1. Introduction: Cooking Cryptographers Problem

2. Our Proposed Protocol

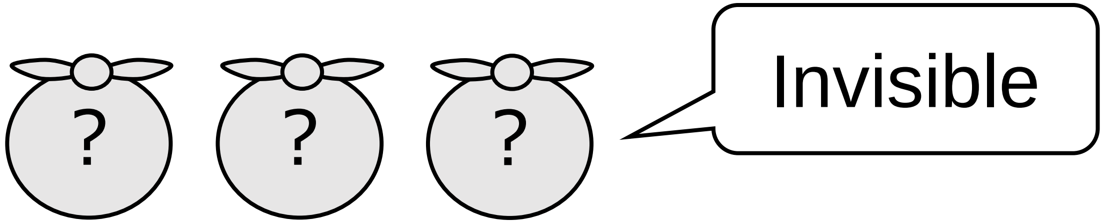
3. Changing the Settings

4. Contribution

5. Conclusion

Merits of cryptographic protocols using physical objects

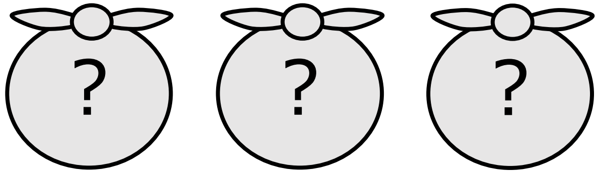
- ✓Employ physical properties that can be intuitively understood[2]
  - ✓Correctness and security are clear even for non-experts
  - ✓The notion of secure multiparty computations can be illustrated[3,4]



[2] T. Moran et al., Polling with Physical Envelopes: A Rigorous Analysis of a Human-Centric Protocol, EUROCRYPT 2006, vol. 4004, pp. 88–108, 2006
[3] A. Marcedone et al., Secure Dating with Four or Fewer Cards, Cryptology ePrint Archive, Report 2015/1031, 2015
[4] R. Pass et al., A Course in Cryptography, 2010
[5] S. Izmalkov et al., Rational Secure Computation and Ideal Mechanism Design, FOCS 2005, pp. 585–594, 2005
[6] M. Lepinksi et al., Collusion-free protocols, STOC 2005, pp. 543–552, 2005

Merits of cryptographic protocols using physical objects

- ✓Employ physical properties that can be intuitively understood[2]
  - ✓Correctness and security are clear even for non-experts
  - ✓The notion of secure multiparty computations can be illustrated[3,4]



Invisible

- ✓Implement stronger cryptographic notions
  - ✓Ballot boxes can be used to implement *rational* secure computations[5]
  - ✓The use of envelopes is essential to realize *collusion-free* protocols[6]

[2] T. Moran et al., Polling with Physical Envelopes: A Rigorous Analysis of a Human-Centric Protocol, EUROCRYPT 2006, vol. 4004, pp. 88–108, 2006
[3] A. Marcedone et al., Secure Dating with Four or Fewer Cards, Cryptology ePrint Archive, Report 2015/1031, 2015
[4] R. Pass et al., A Course in Cryptography, 2010
[5] S. Izmalkov et al., Rational Secure Computation and Ideal Mechanism Design, FOCS 2005, pp. 585–594, 2005
[6] M. Lepinksi et al., Collusion-free protocols, STOC 2005, pp. 543–552, 2005