Interactive Physical Zero-Knowledge Proof for Norinori

Jean-Guillaume Dumas[1] Pascal Lafourcade[2] ○**Daiki Miyahara**[3,4]
Takaaki Mizuki[3] Tatsuya Sasaki[3] Hideaki Sone[3]

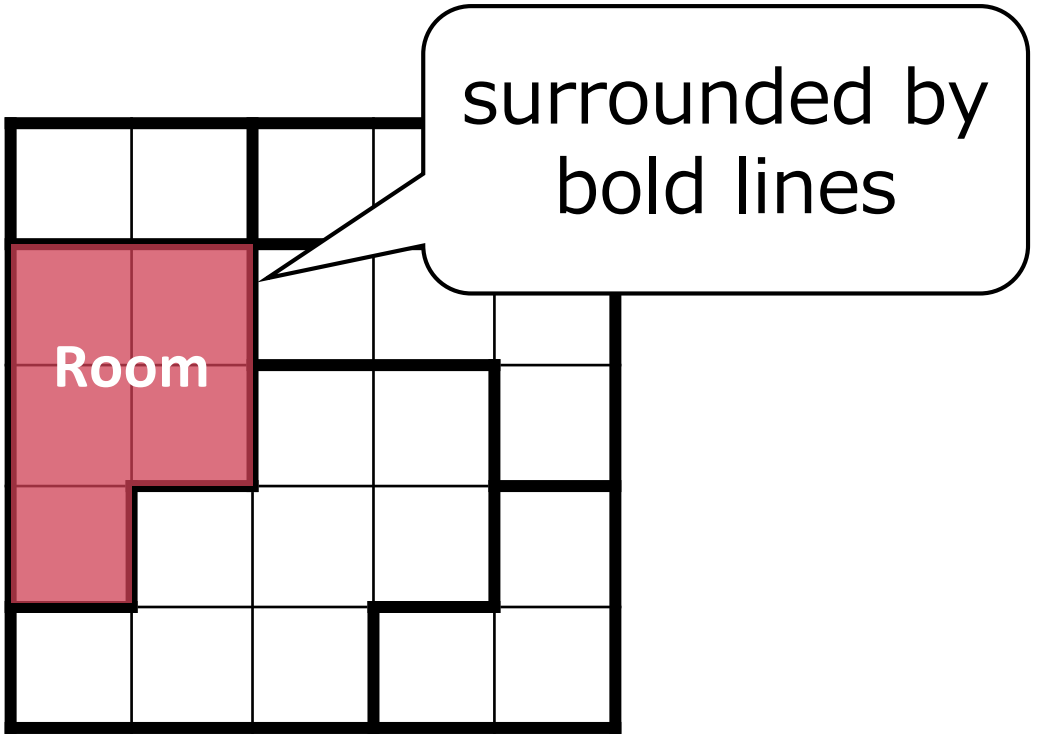
1. Univ. Grenoble Alpes 2. Univ. Clermont Auvergne
3. Tohoku Univ. 4. National Institute of Advanced Industrial Science and Technology

Outline

1. Background
    - Norinori
    - Scenario
    - Contribution
2. Idea
3. Our Construction
4. Conclusion

What is *Norinori*?

✓One of the most ***famous*** puzzles published by Nikori.

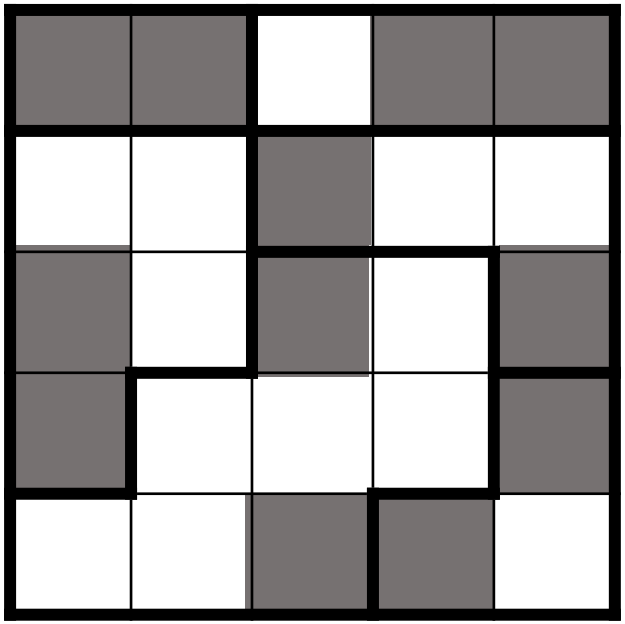


An example of a challenge of Norinori.

https://www.nikoli.co.jp/en/puzzles/norinori.html

What is *Norinori*?

✓**Goal**: Make some of empty cells become black so that:



An example of a challenge of Norinori.

Rules.

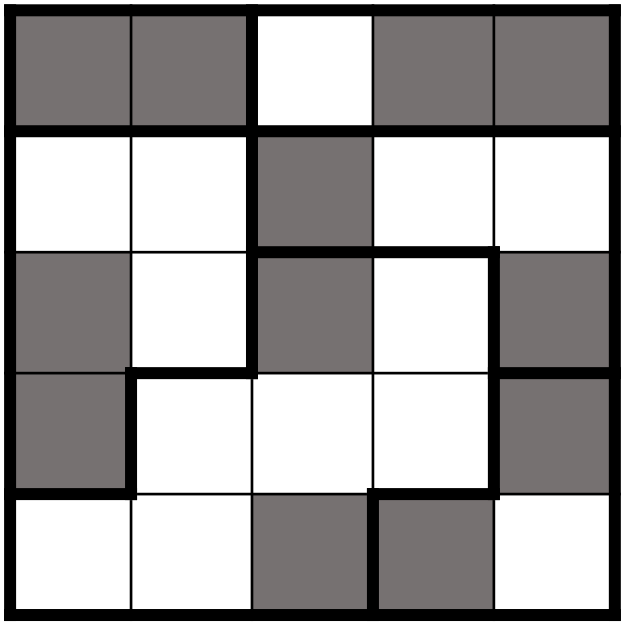
Room condition. Each room must contain exactly ***two*** black cells.

Pair condition. Each black cell must be adjacent to ***exactly one*** other black cell.

https://www.nikoli.co.jp/en/puzzles/norinori.html

What is *Norinori*?

✓**Goal**: Make some of empty cells become black so that:



A solution of the challenge.

Rules.

Room condition. Each room must contain exactly ***two*** black cells.

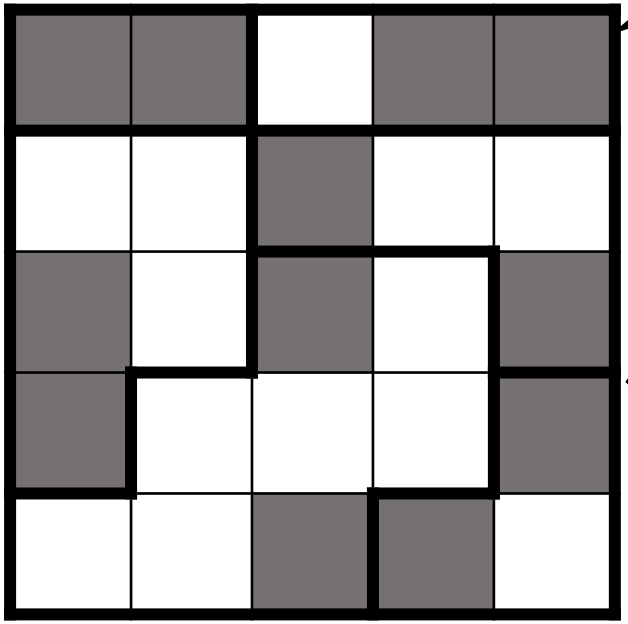
Pair condition. Each black cell must be adjacent to ***exactly one*** other black cell.

✓Solving Norinori was shown to be NP-complete.[BS17]

[BS17] M. Biro and C. Schmidt, ``Computational complexity and bounds for Norinori and LITS,'' EuroCG 2017.

What is *Norinori*?

✓We can **easily** confirm [illegible]atisfied.



A solution of the challenge.

Room: exactly two

Pair: exactly one

Rules.

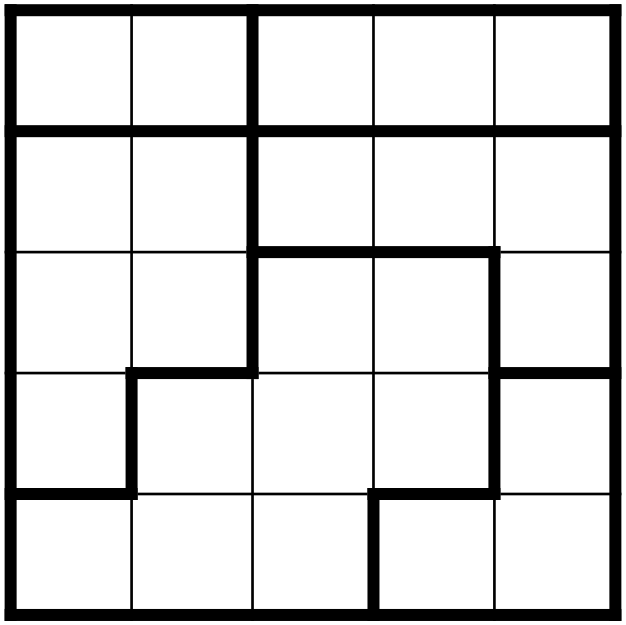
Room condition. Each room must contain exactly ***two*** black cells.

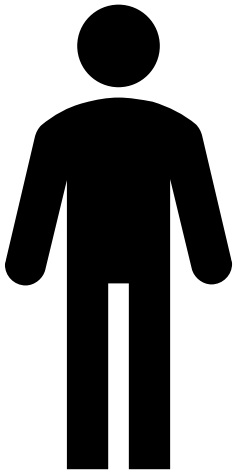
[illegible]ck

[illegible]cell.

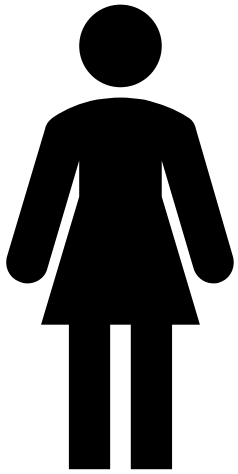
Consider two players, P and V.

✓P has brought a challenge of Norinori to V.





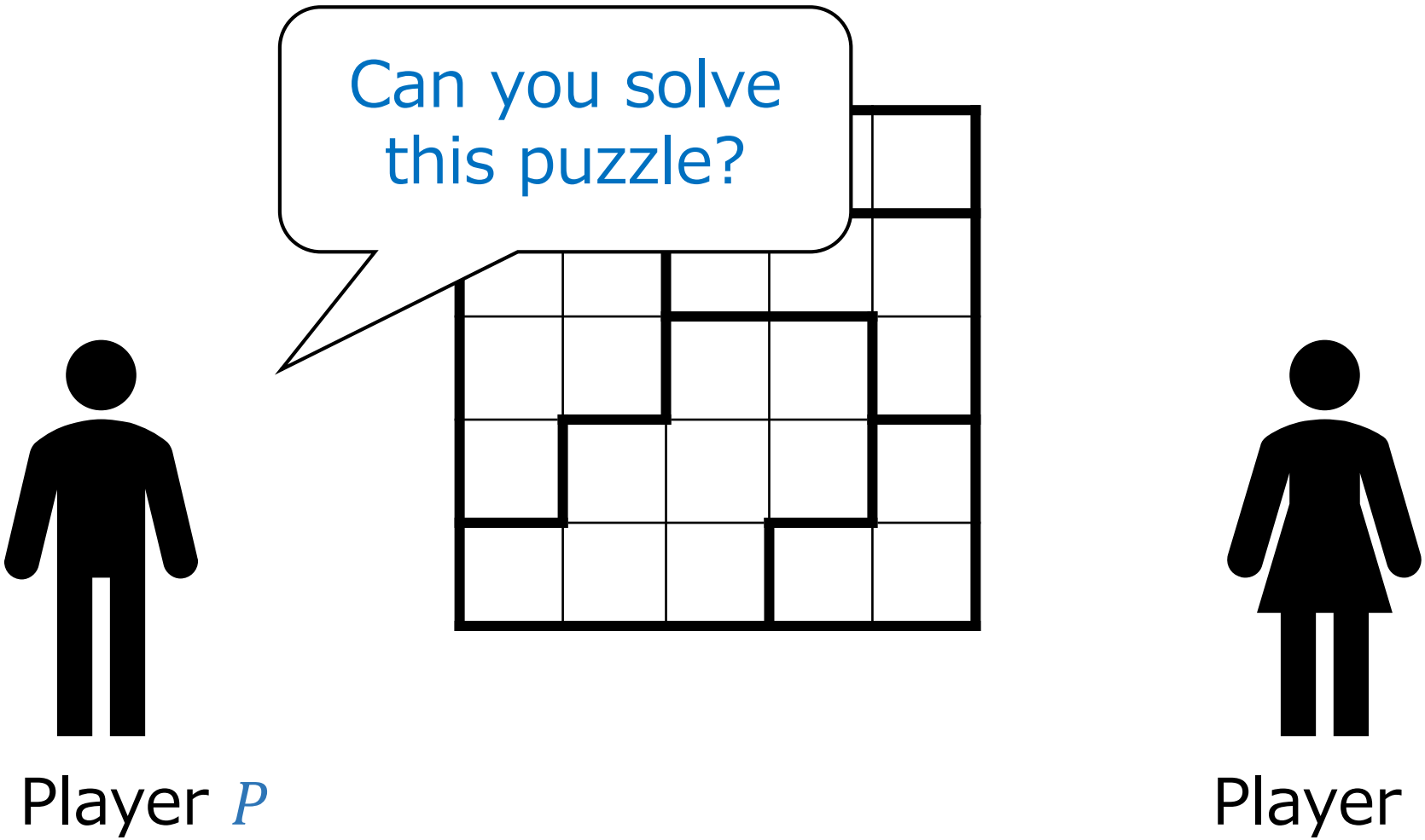
Player P



Player V

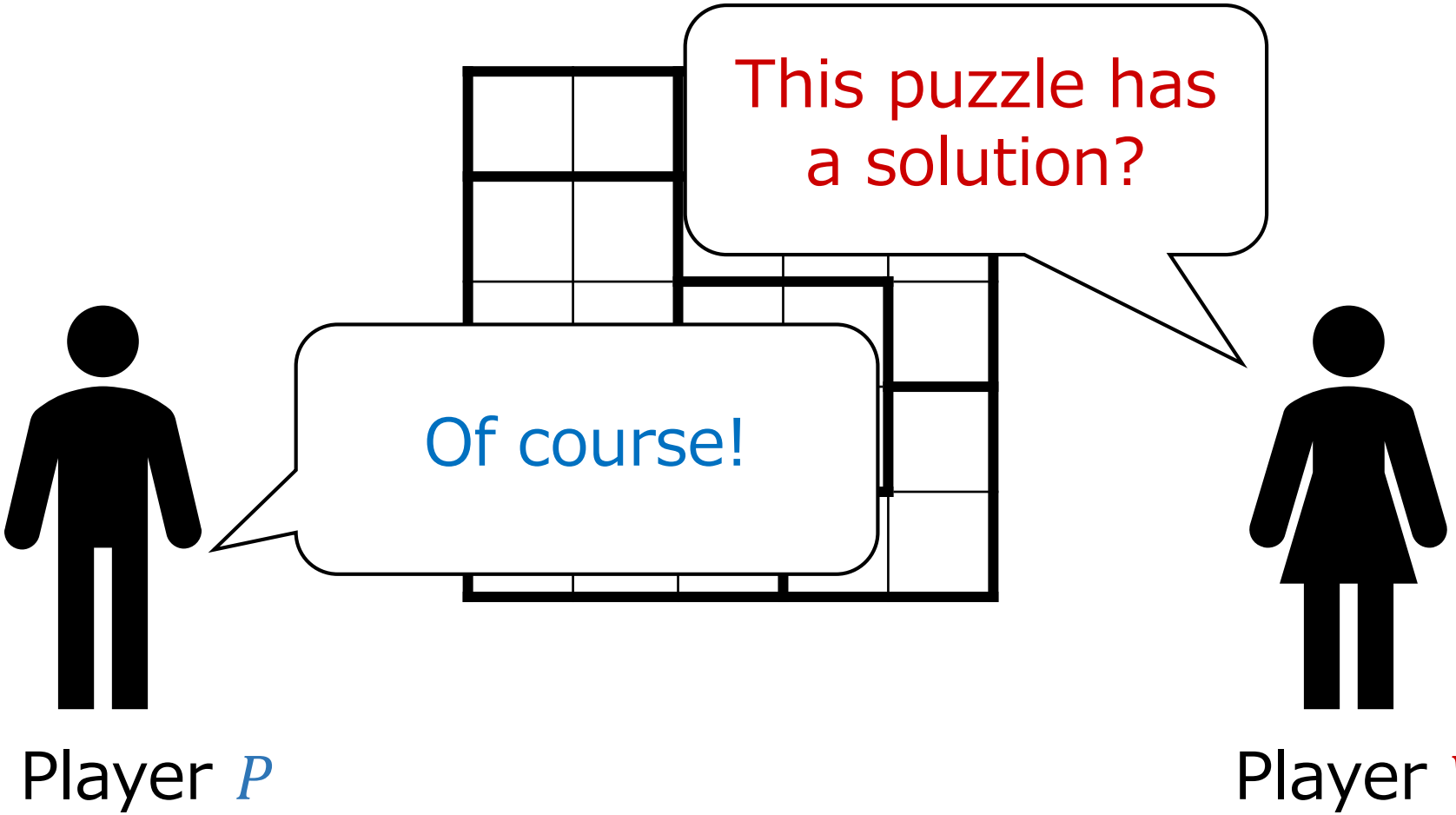
Consider two players, P and V.

✓P has brought a challenge of Norinori to V.



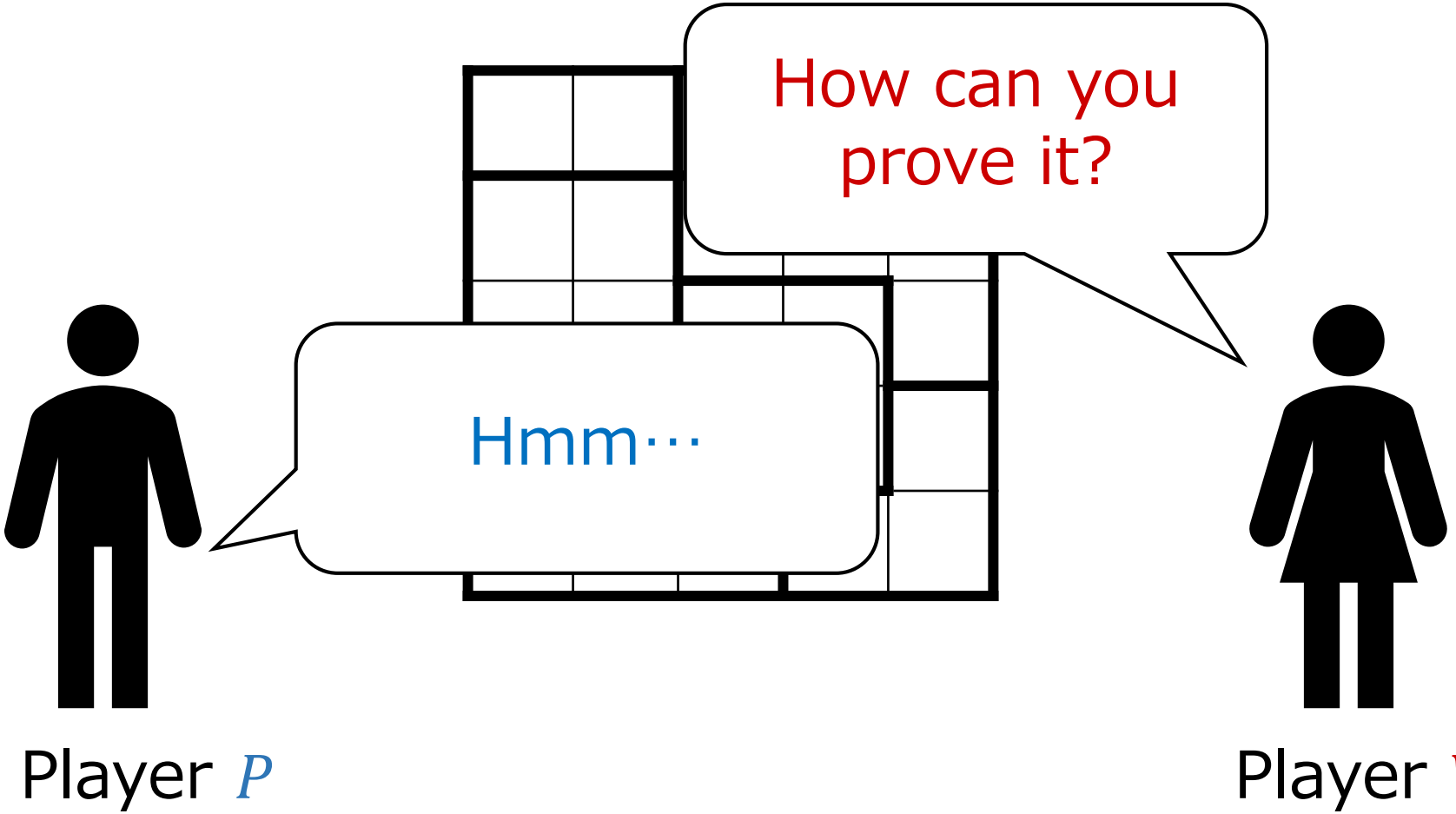
Consider two players, P and V.

- ✓But V can't solve this, so V wonders if this puzzle really has a solution.

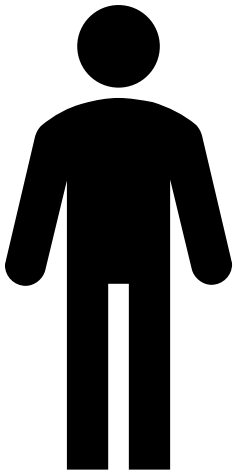


Consider two players, P and V.

✓***Dilemma***: P wants to convince V but does not want to reveal the solution.



The scenario

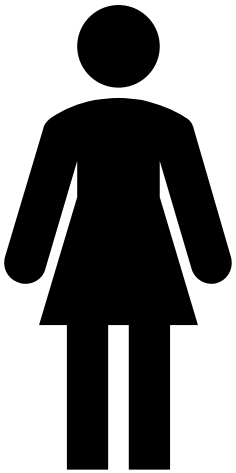


Player P

- ✓ Convince V that the problem has a solution **without** revealing it.

Restrictions:

- ✓ Use everyday objects.
- ✓ Prove it manually.

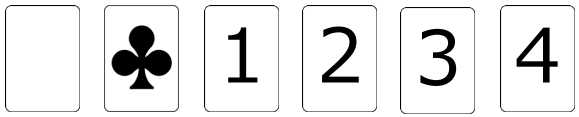


Player V

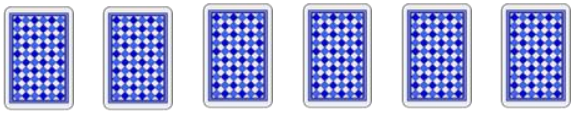
Physical Zero-Knowledge Proof (ZKP)!

Contribution

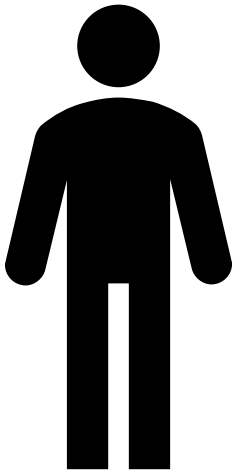
✓Design *a physical ZKP protocol* for Norinori using cards and envelopes.



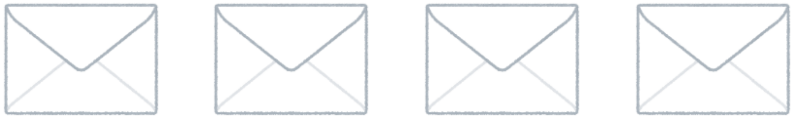
Face side



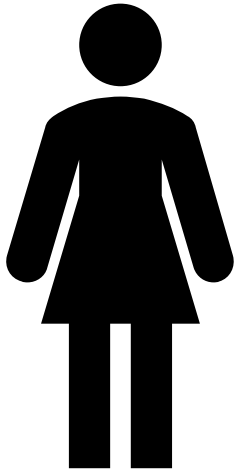
Back side



Player P



Envelopes

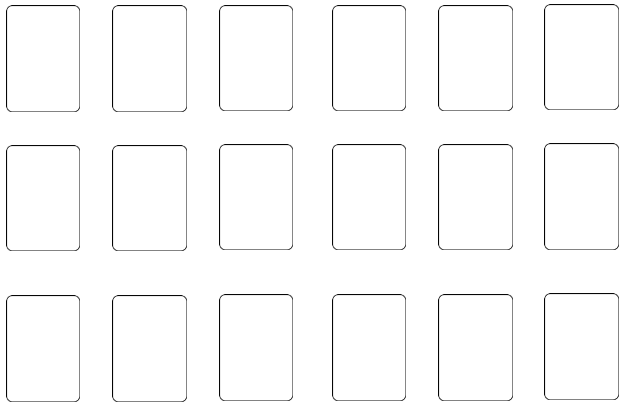


Player V

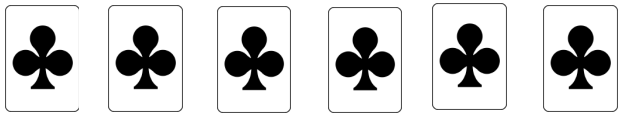
Outline

1. Background
   - Norinori
   - Scenario
   - Contribution
2. Idea
3. Our Construction
4. Conclusion

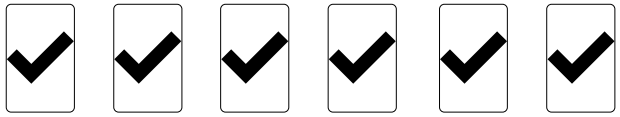
A deck of cards used in our protocol



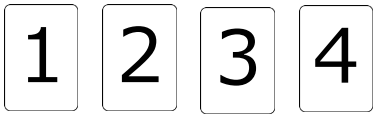
White cards



Black cards



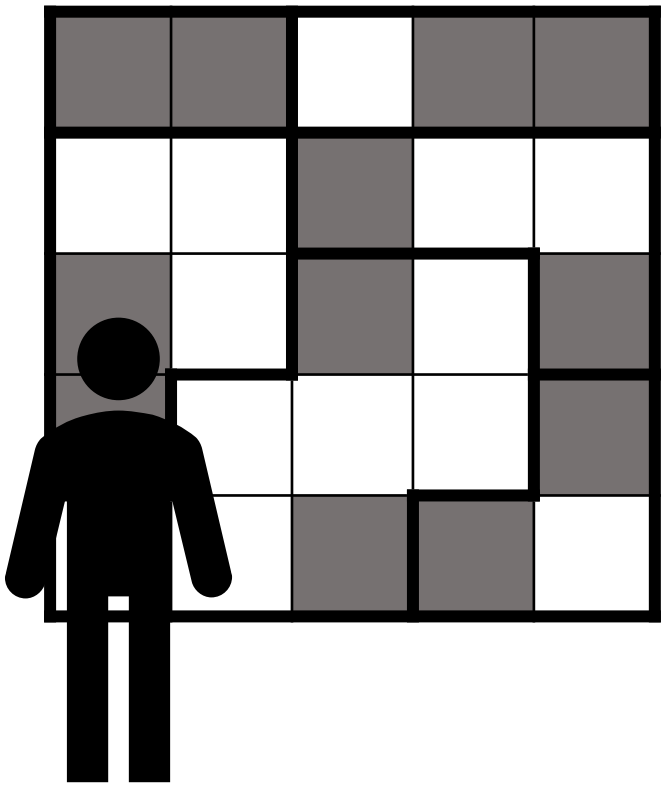
Marker cards



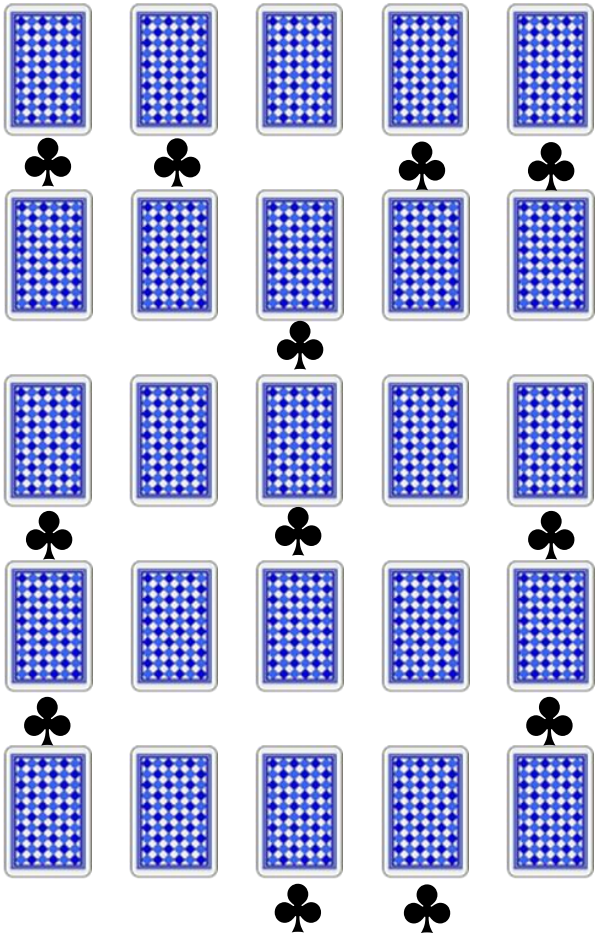
Number cards

Basic Idea

✓**Setup**: P puts one face-down card on each cell according to the solution.

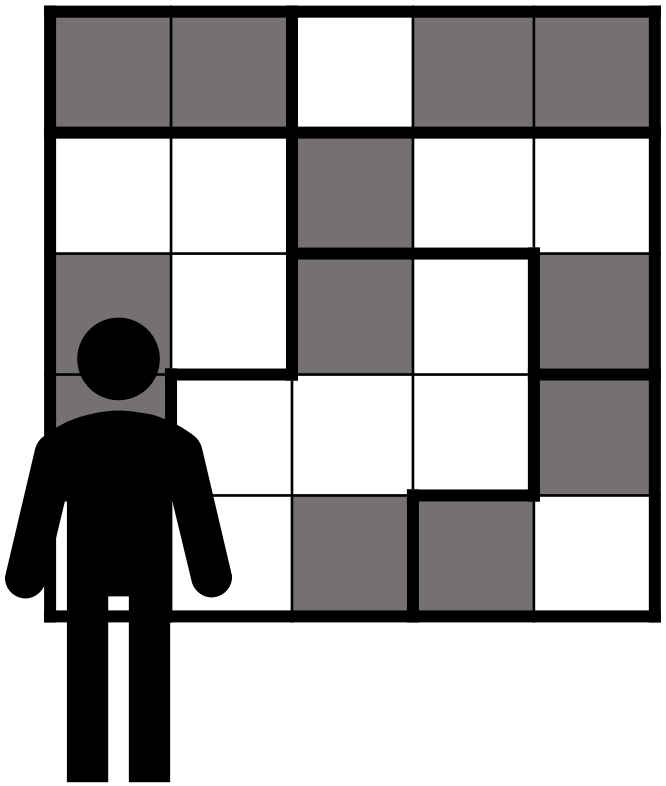


Player P

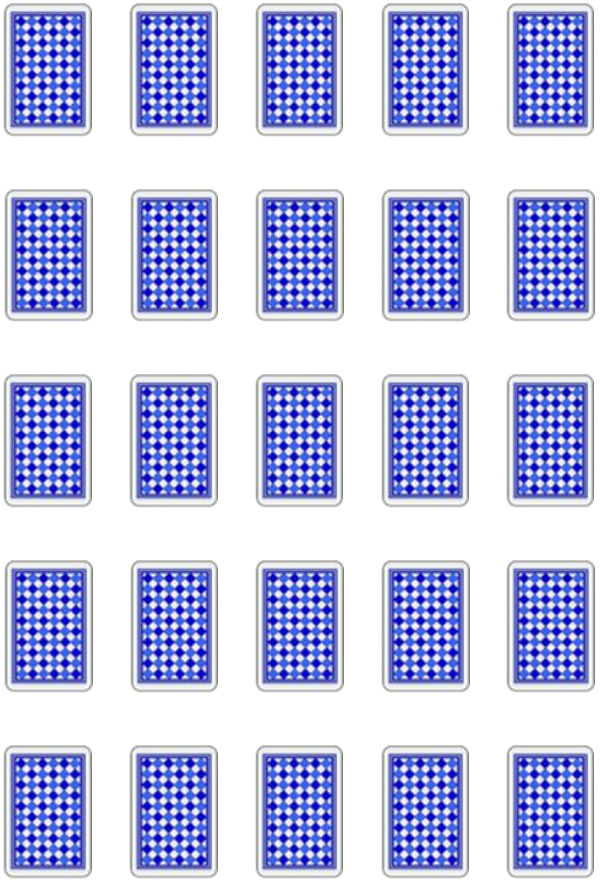


Basic Idea

✓Then, the Room condition can be ***easily*** verified.

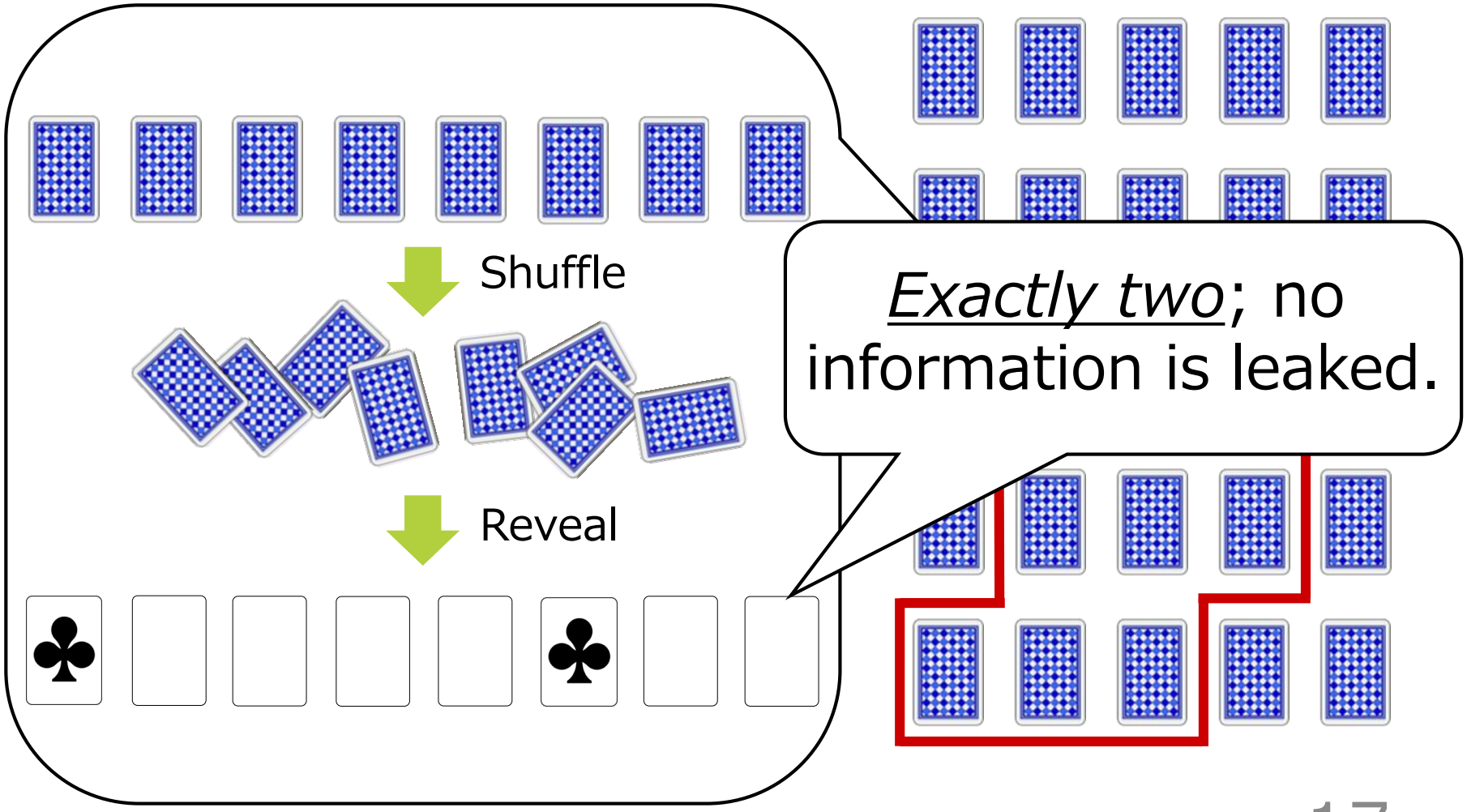


Player P



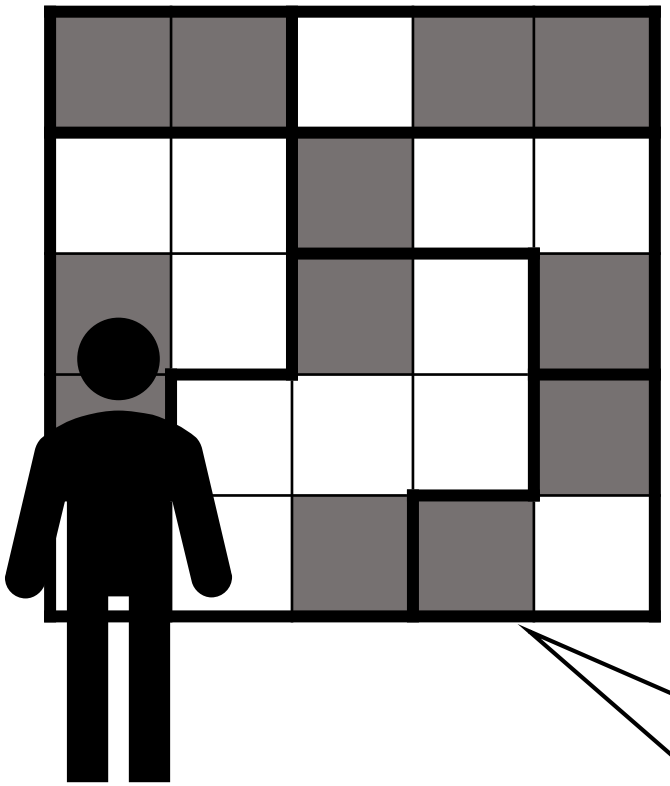
Basic Idea

✓Then, the Room condition can be ***easily*** verified.

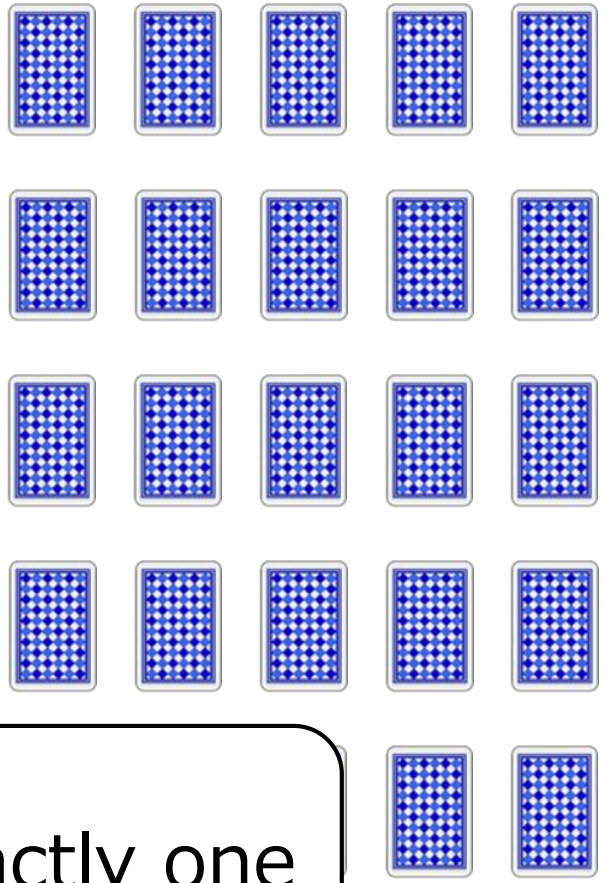


Basic Idea

✓Then, how we verify the Pair condition?



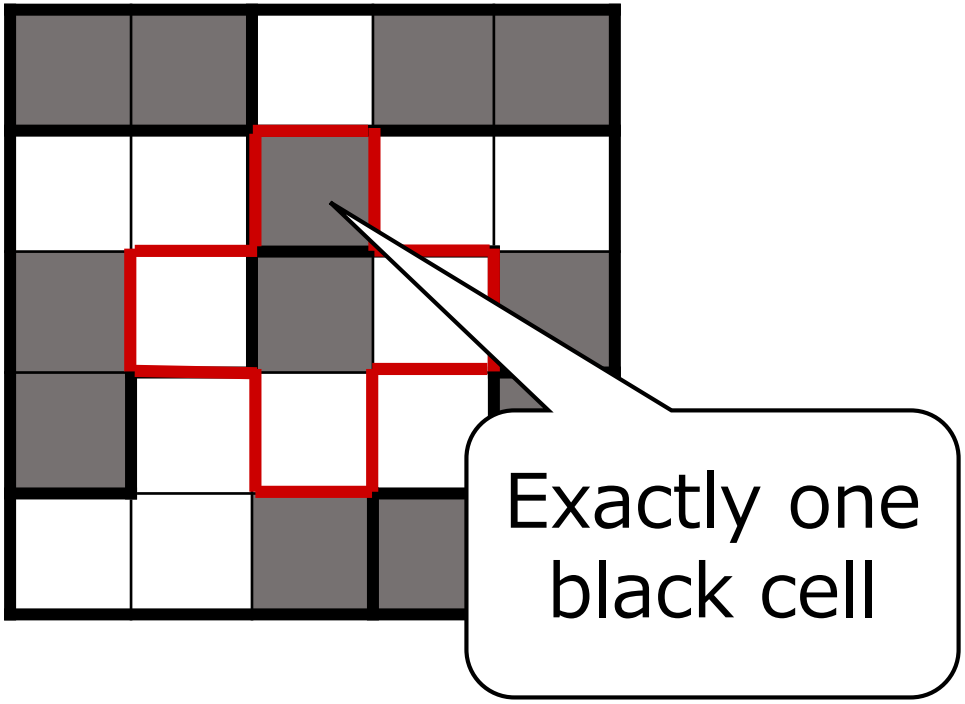
Player P

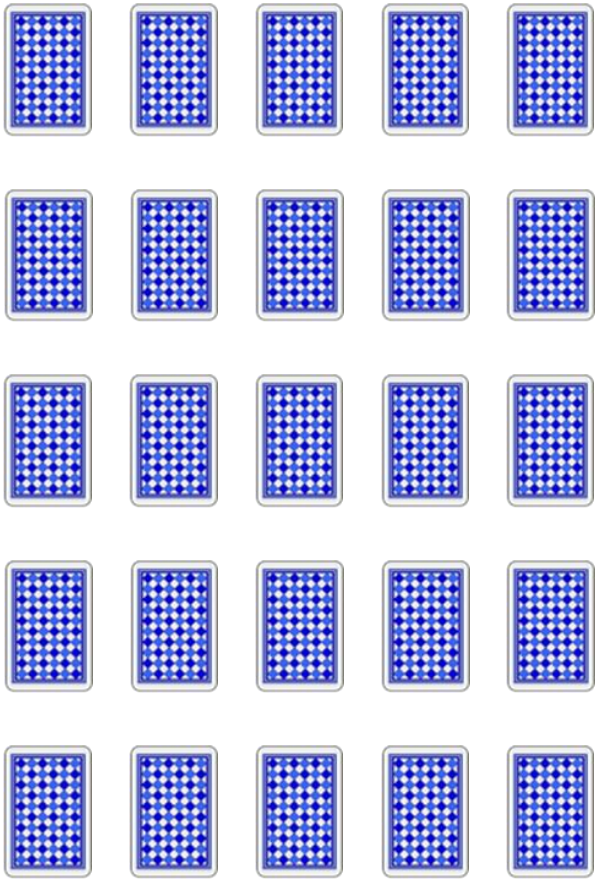


Pair: exactly one

Basic Idea

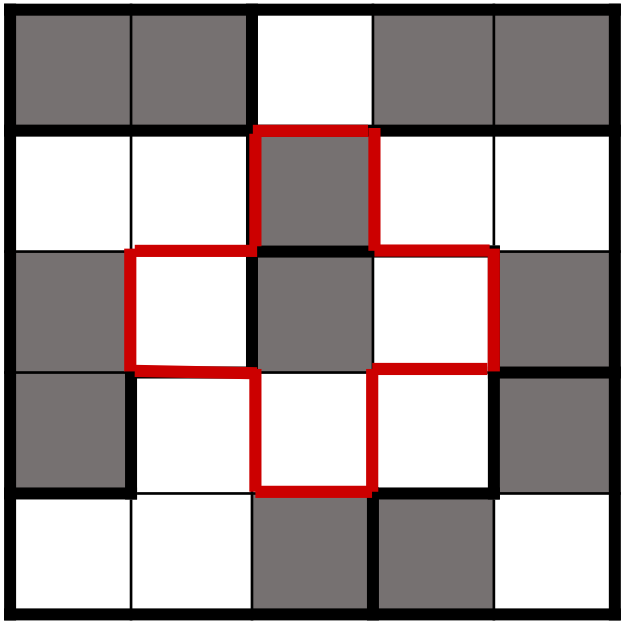
✓Exactly one black cell exists among ***four adjacent cells*** of each black one.

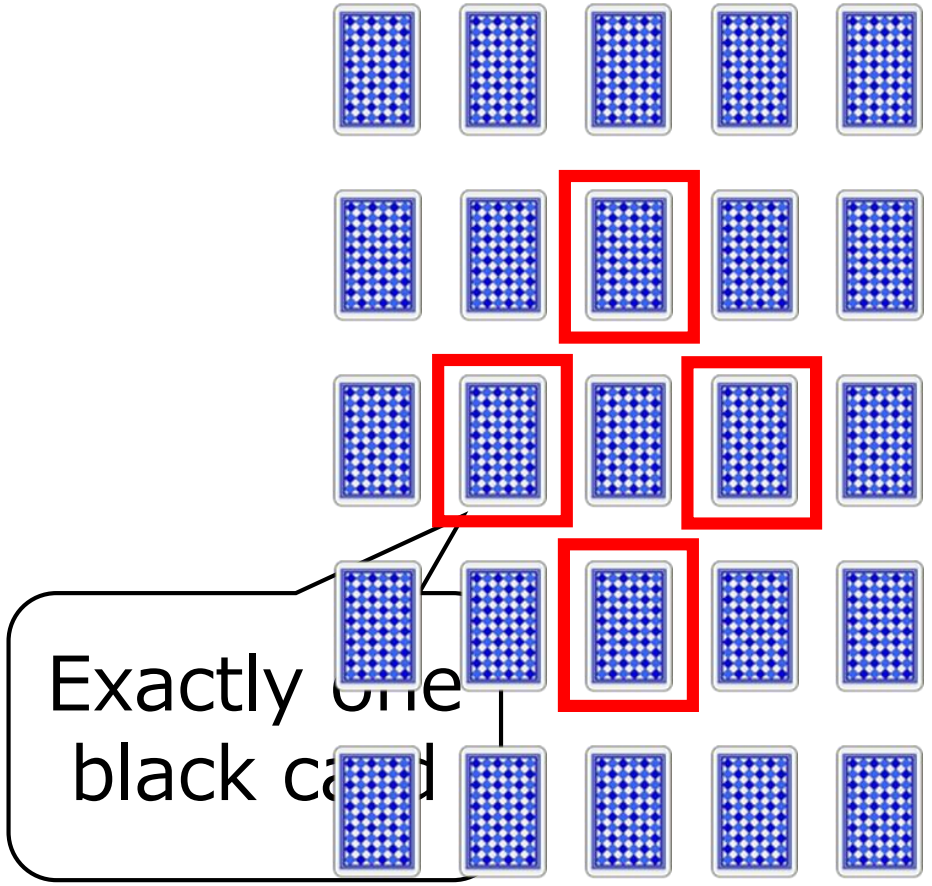




Basic Idea

✓Exactly one black cell exists among ***four adjacent cells*** of each black one.

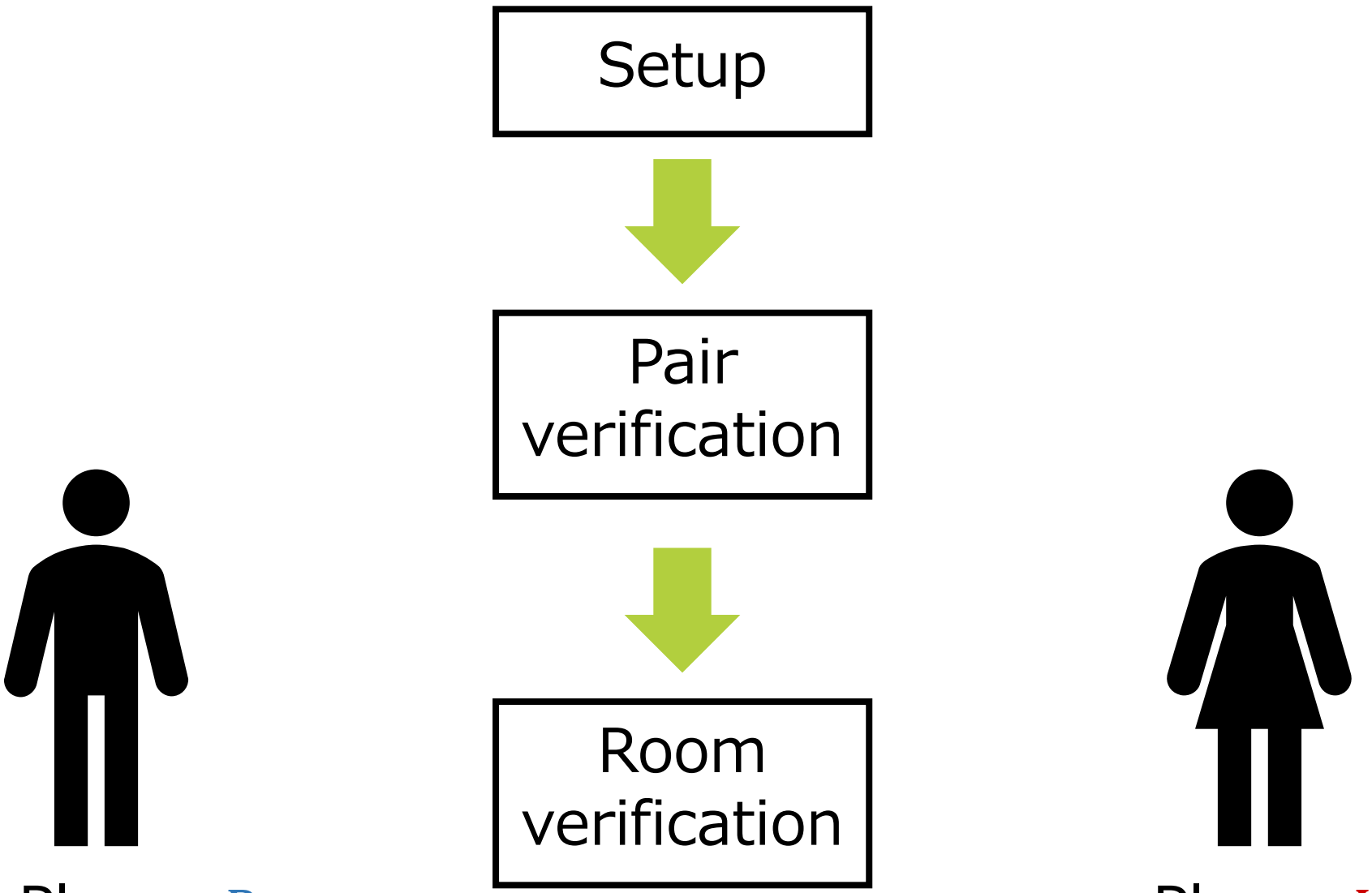




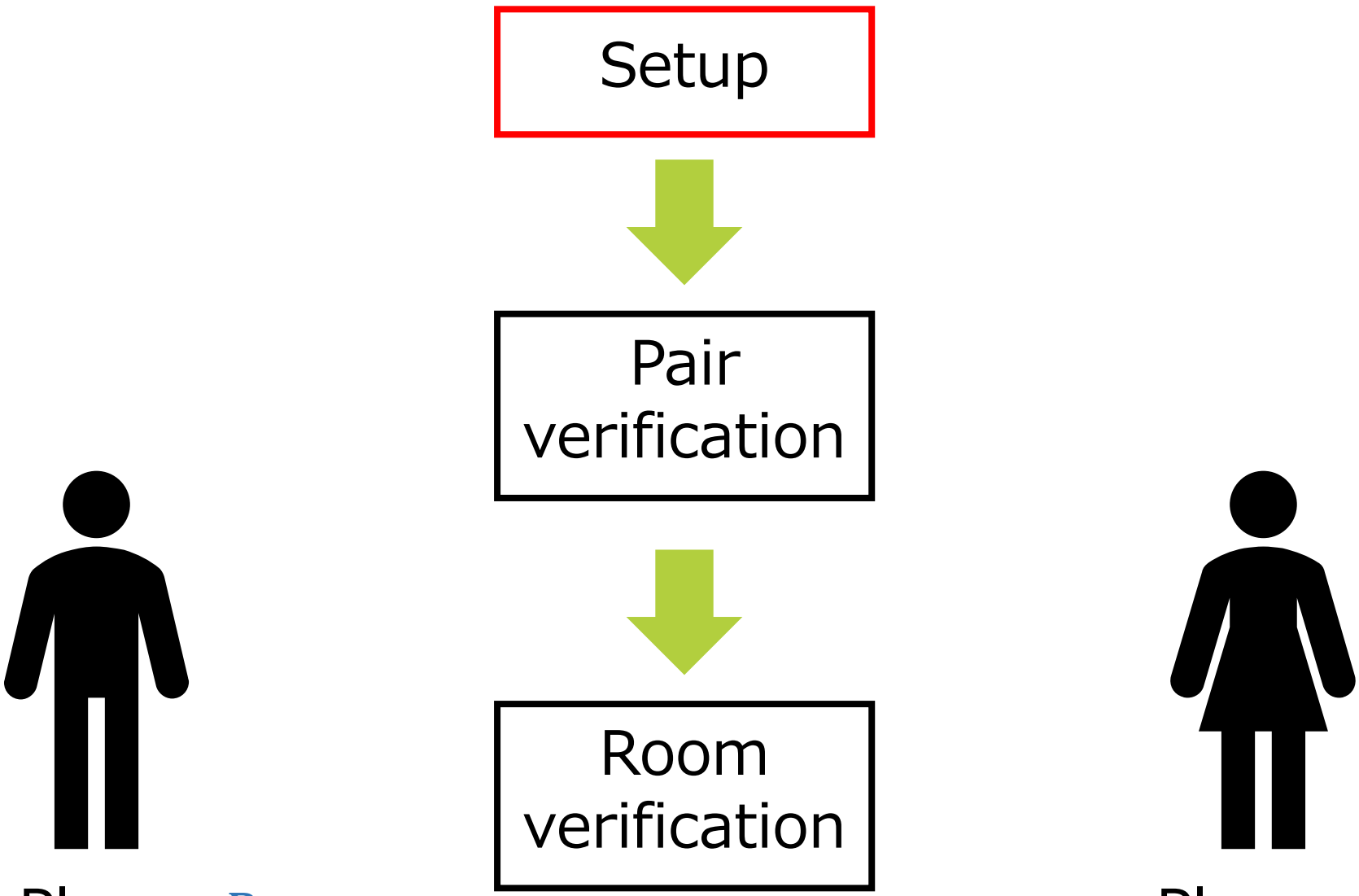
Outline

1. Background
   - Norinori
   - Scenario
   - Contribution
2. Idea
3. Our Construction
4. Conclusion

Our construction

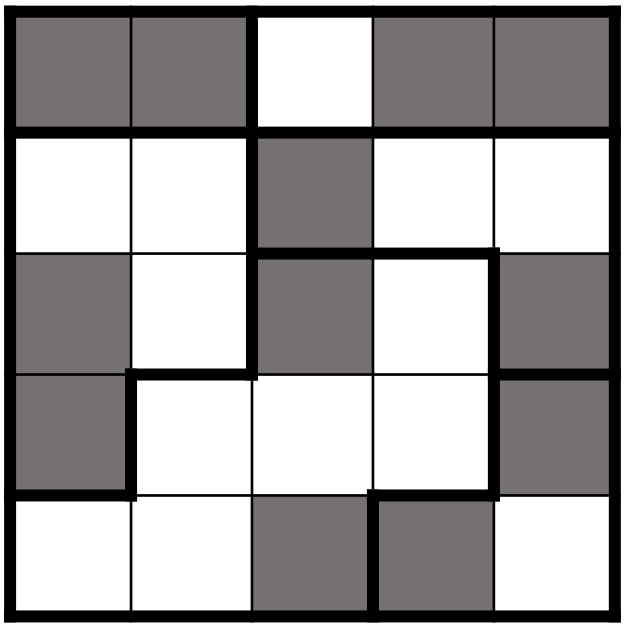


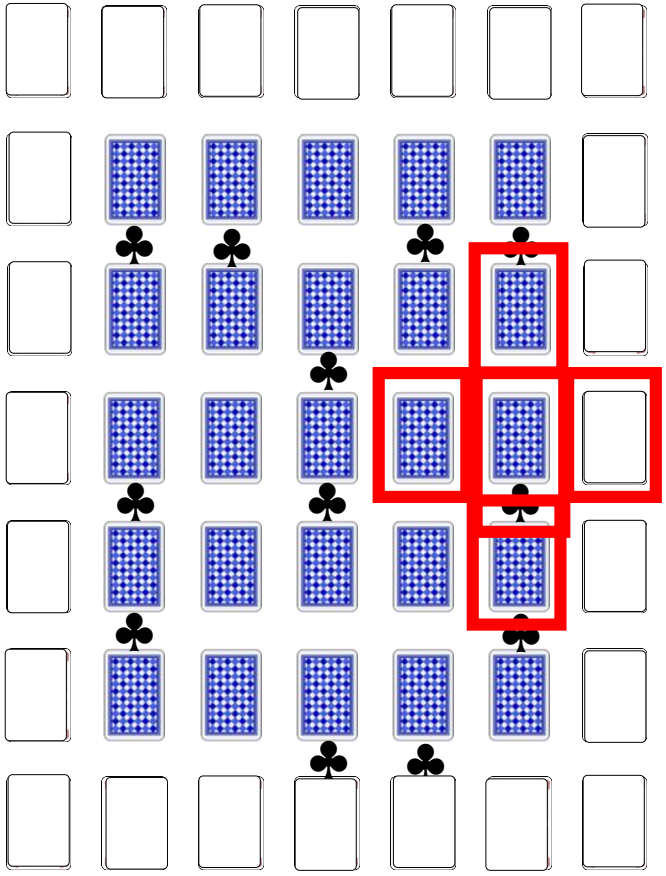
Our construction



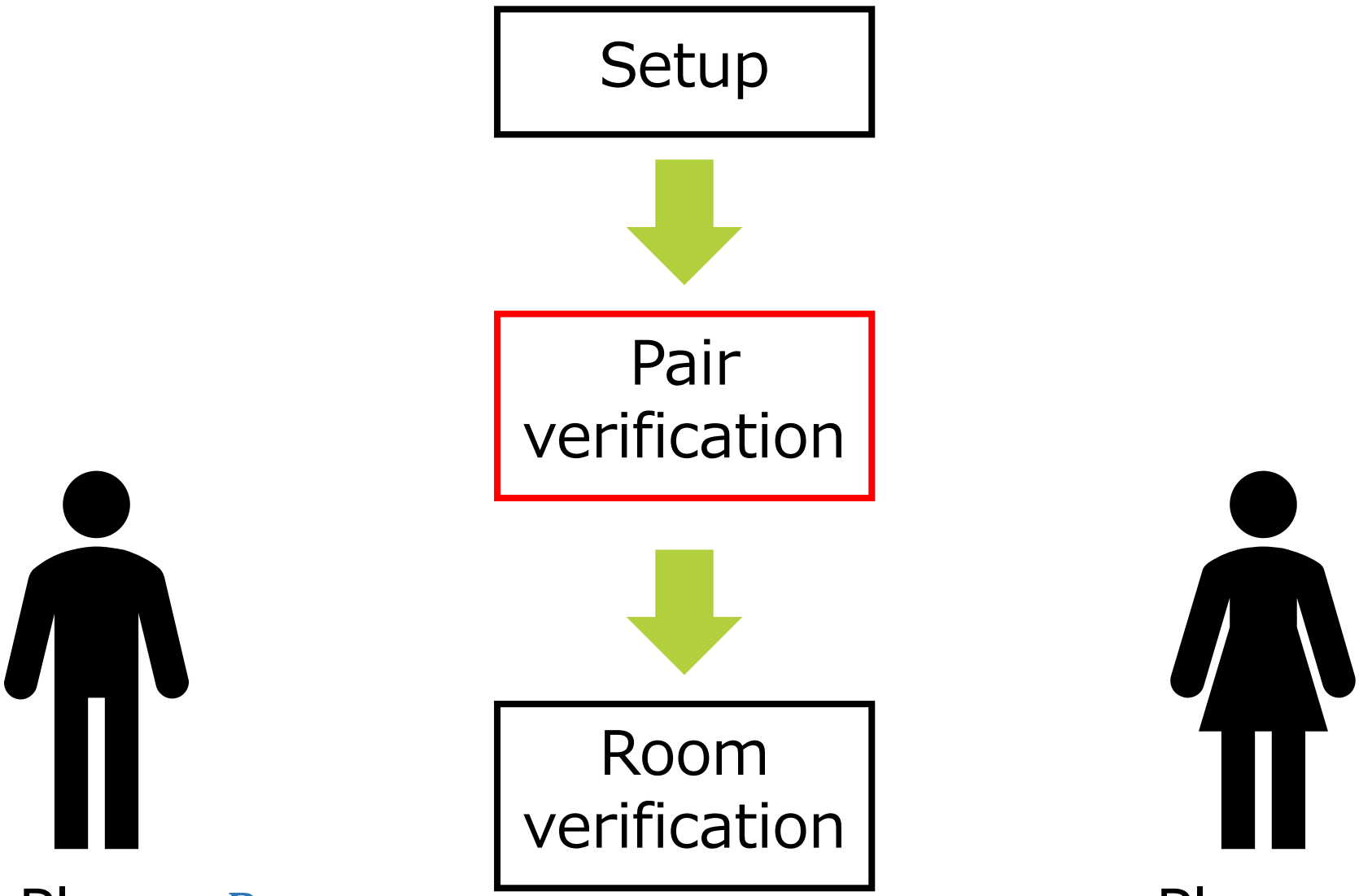
Setup

- ✓P puts one face-down card on each cell according to the solution.
- ✓They put additional white cards for the Pair verification.





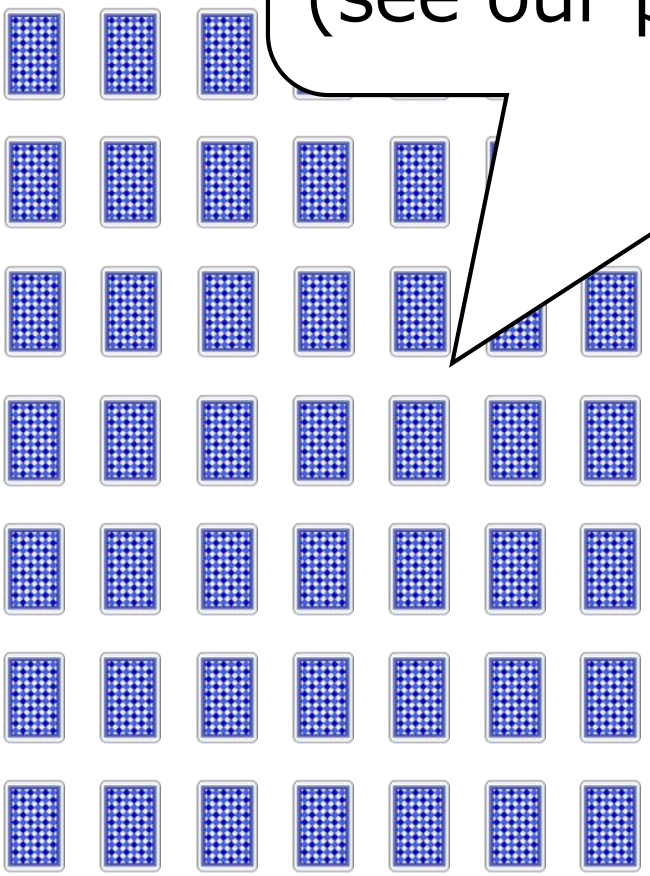
Our construction

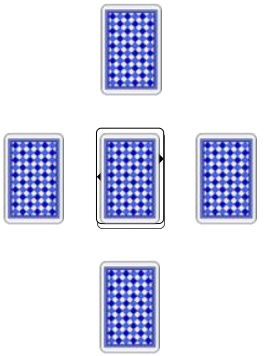


Pair verification

1. P pic
of it
Then

Note: we use the existing technique[KW17] to hide the positions. (see our paper)

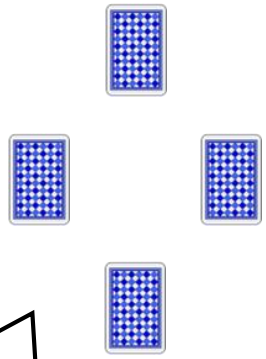




[KW17] A. Koch and S. Walzer, ``Foundations for actively secure card-based cryptography,'' IACR Cryptology ePrint Archive, 2017:423, 2017.

Pair verification

- ✓Now, we have the four adjacent cards.
- ✓We can verify the Pair condition by just revealing these four cards, but:

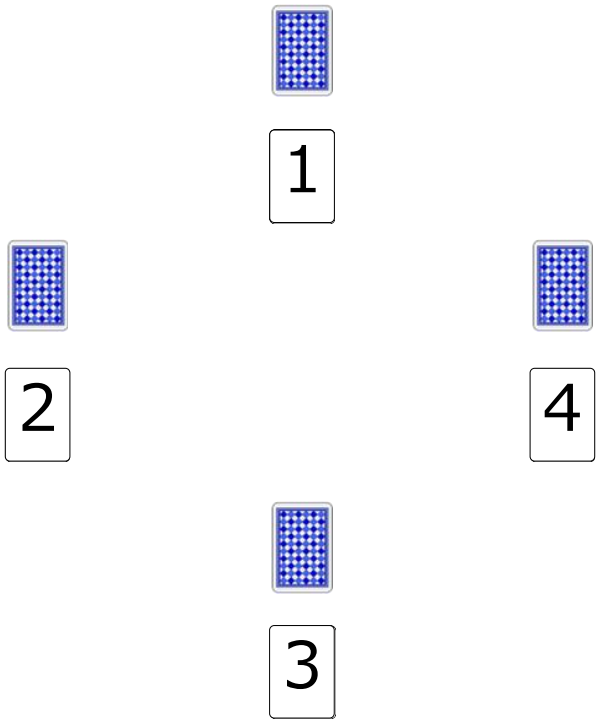


Just revealing them **leaks information**.

These are **necessary** for the next verifications.

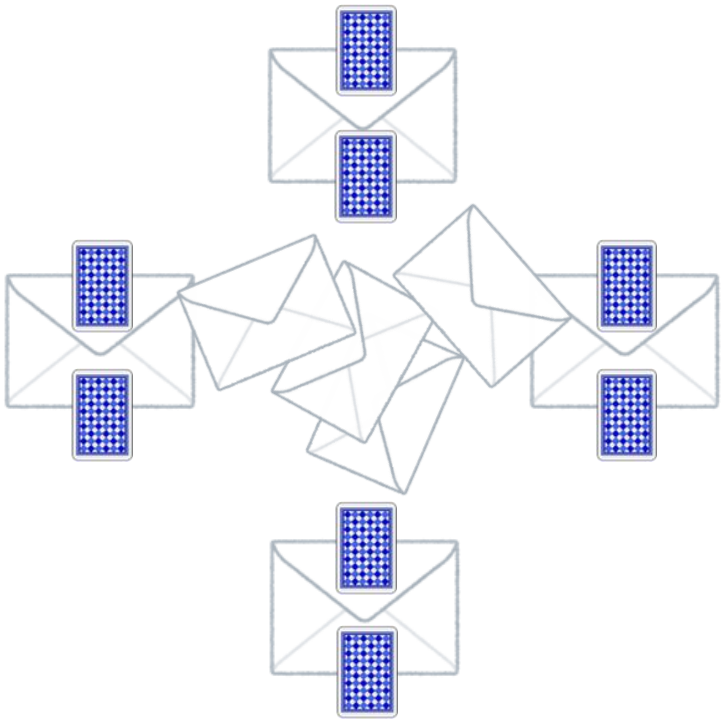
Pair verification

2. *V* puts number cards below the four adjacent cards, which specify the original positions (and then turn them over).



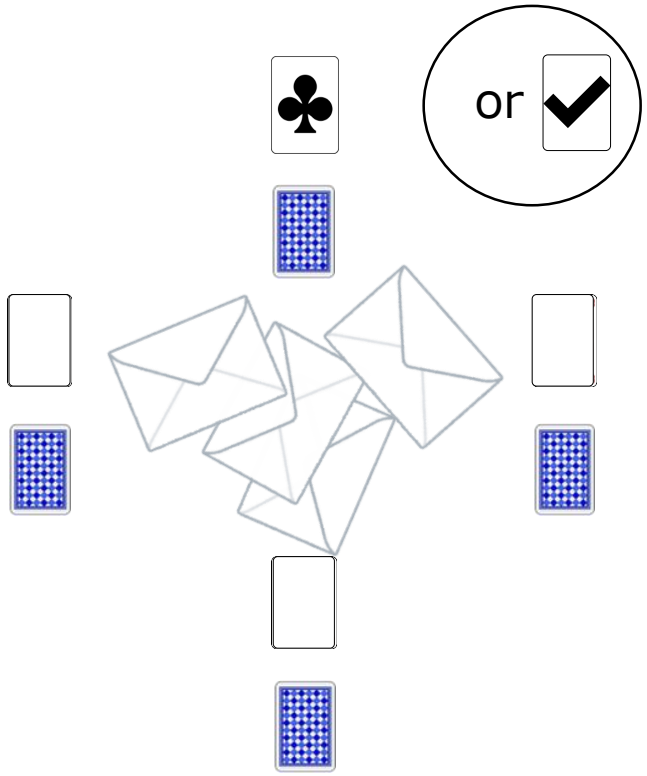
Pair verification

3. V puts each two cards into an envelope, and then shuffles them:



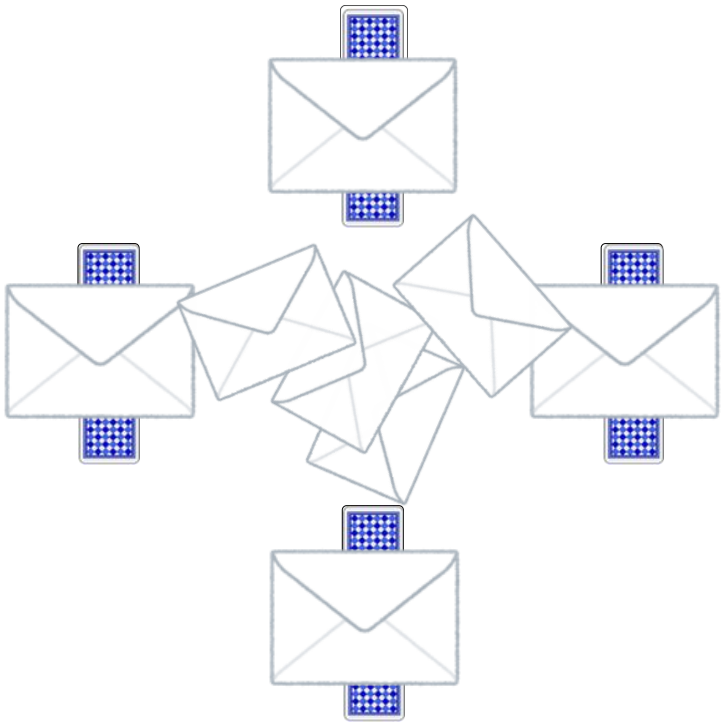
Pair verification

4. V reveals the four adjacent cards.
   Then, ***exactly one*** black or marker should appear.



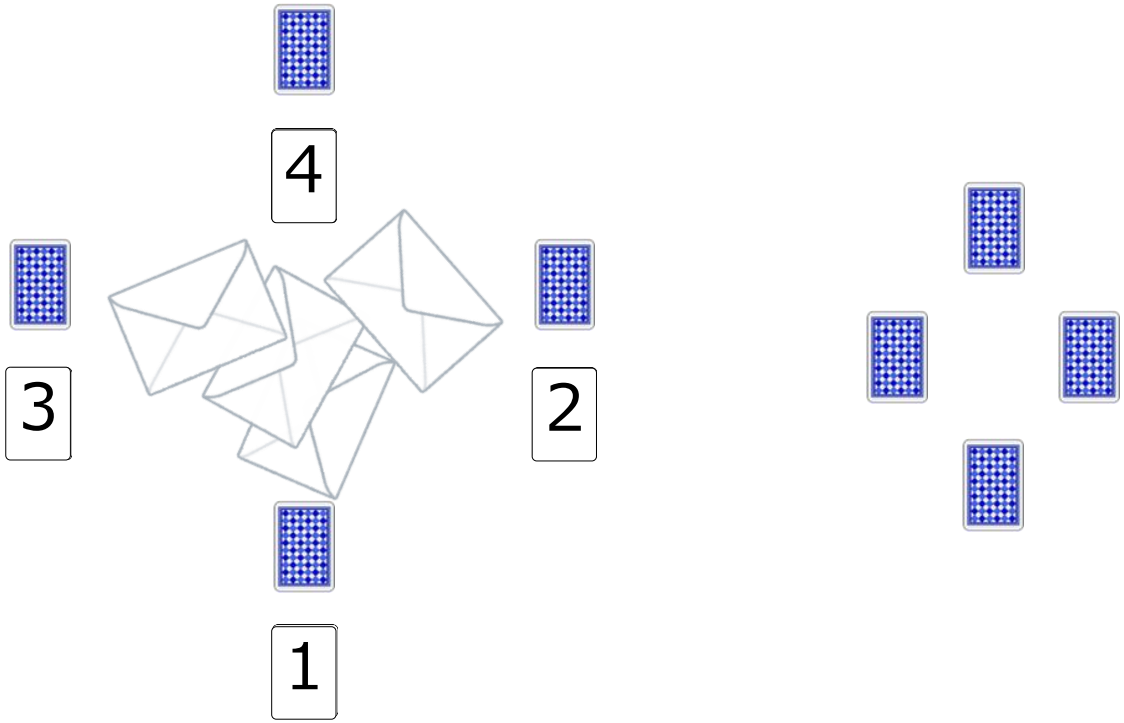
Pair verification

5. V turns them over, and then shuffles them as before.



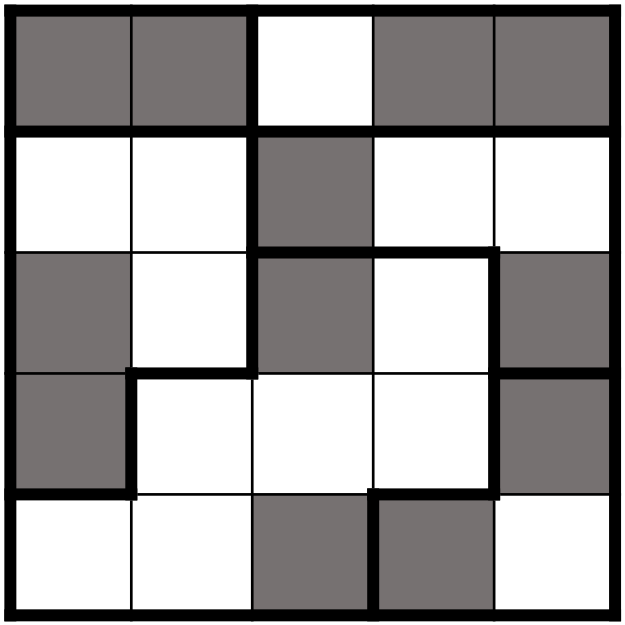
Pair verification

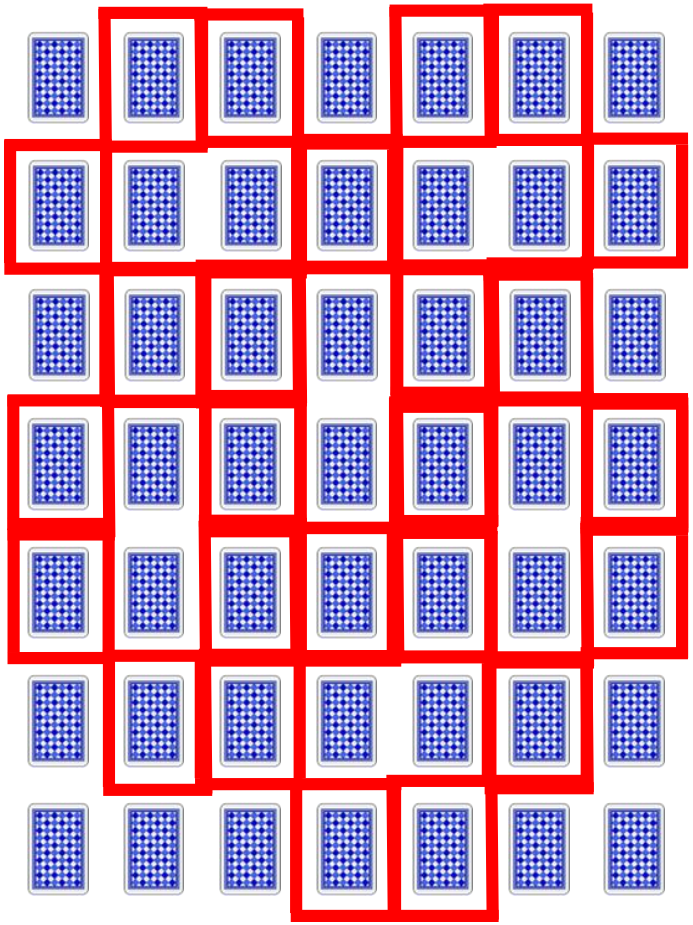
6. *V* reveals the four number cards.
   V can place the four adjacent cards in the original positions.



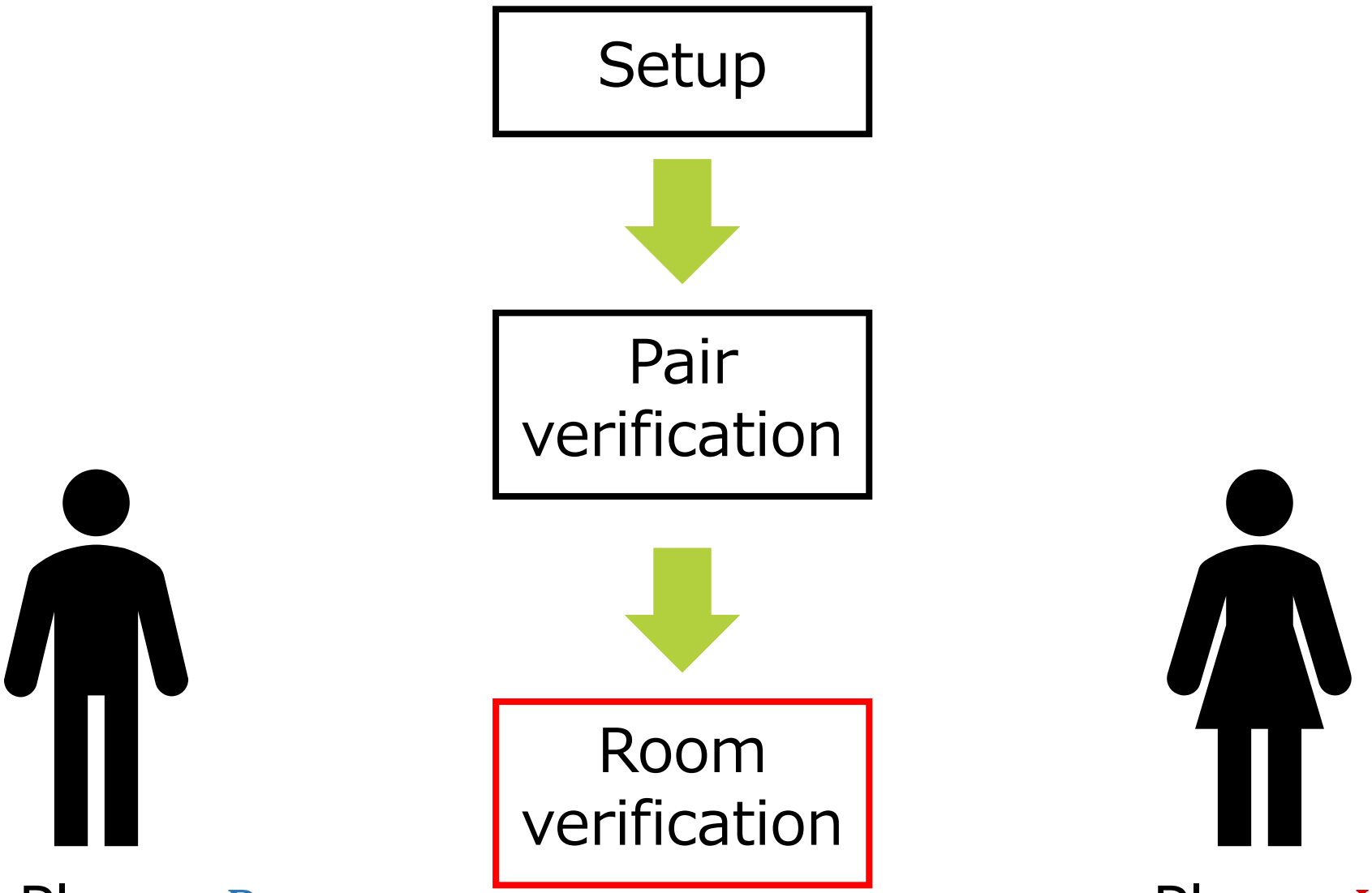
Pair verification

✓By repeating the previous steps twice as the number of rooms, V is convinced of the Pair condition.



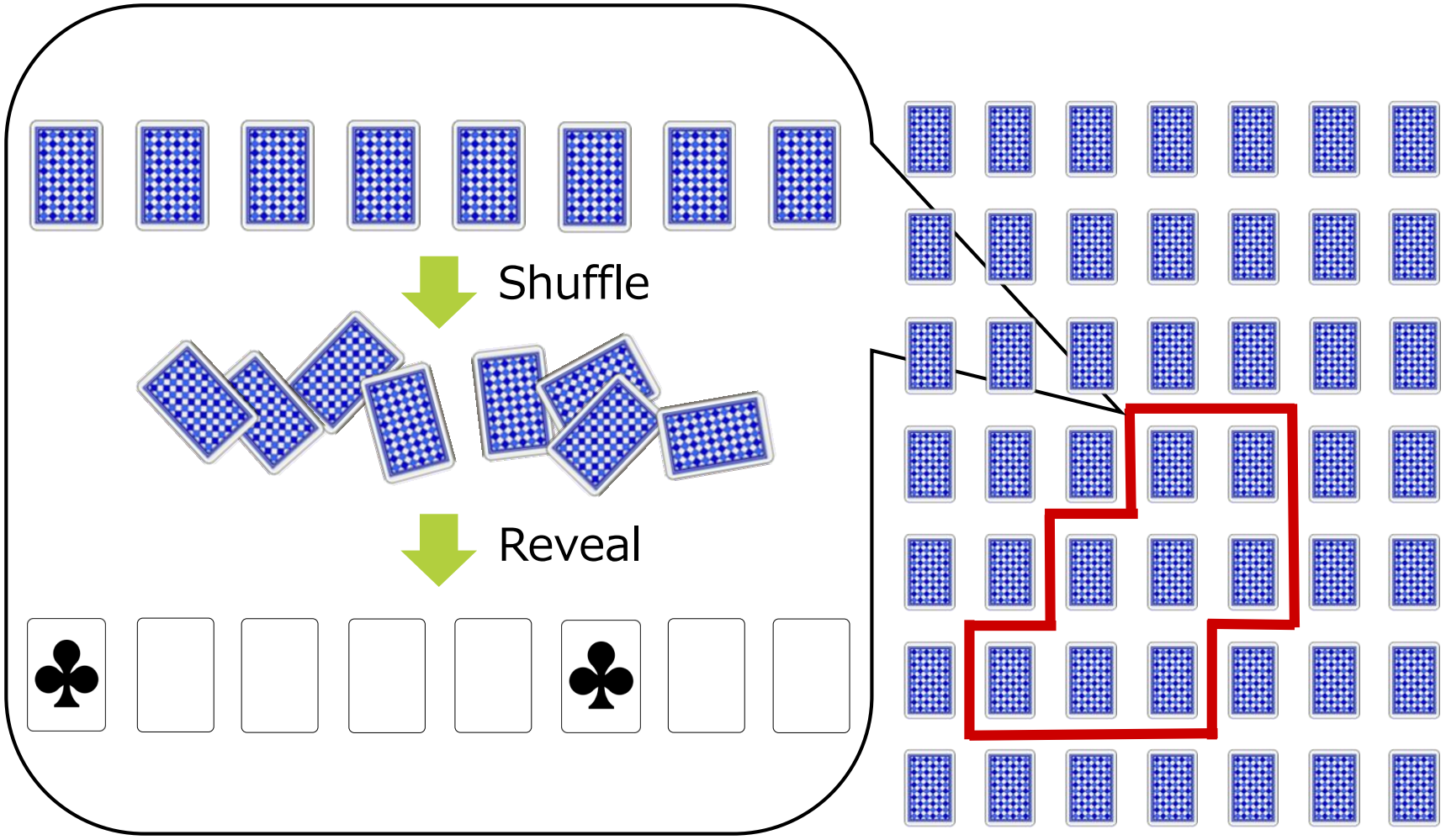


Our construction



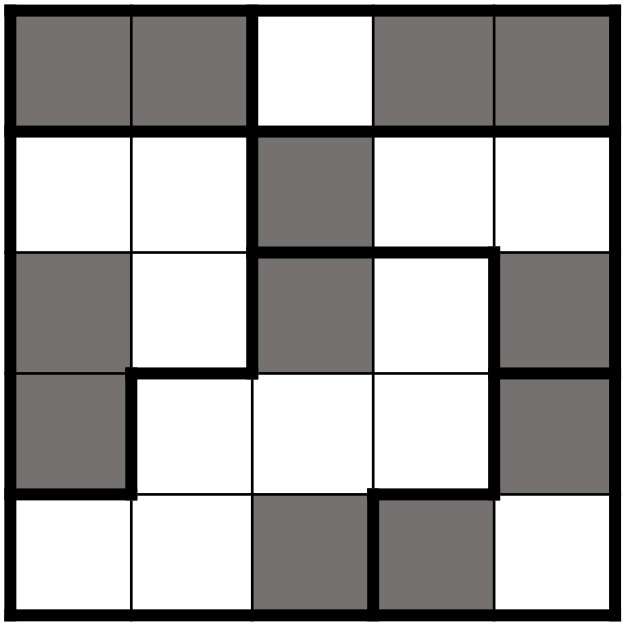
Room verification is easy

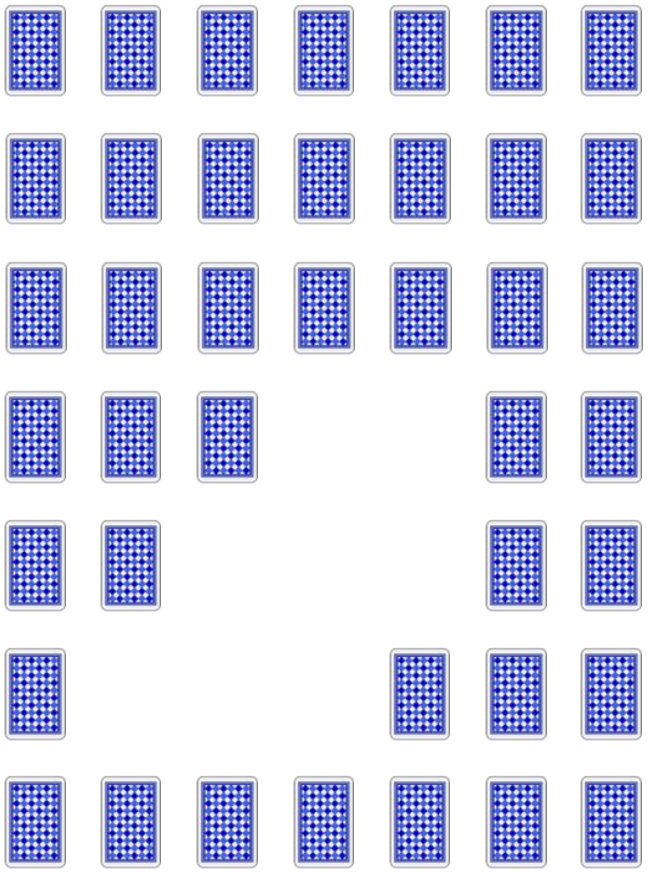
- ✓Shuffle the cards corresponding to each room and then reveal them.



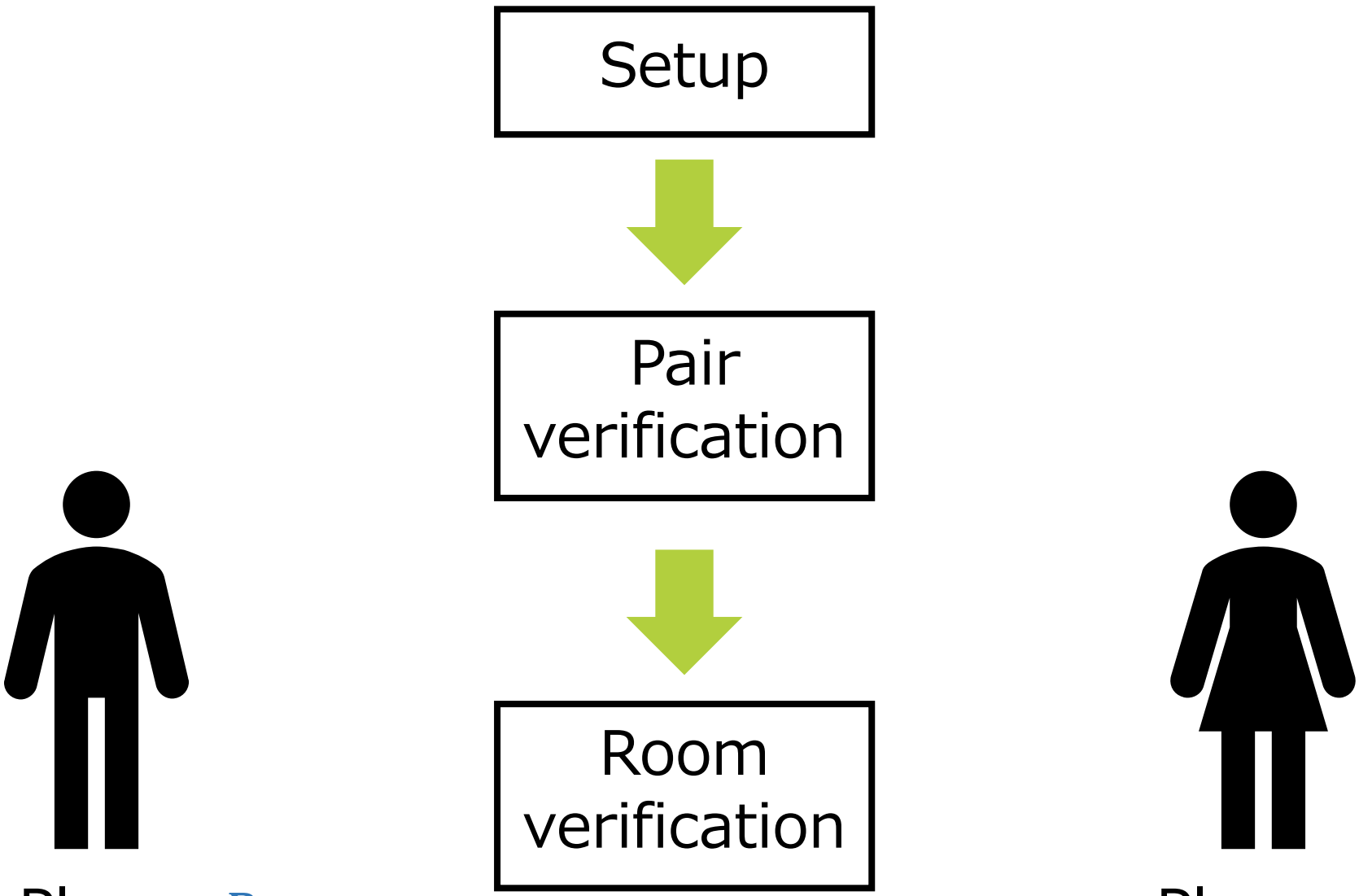
Room verification is easy

- ✓By repeating the previous step, V is convinced of the Room condition.





Our construction

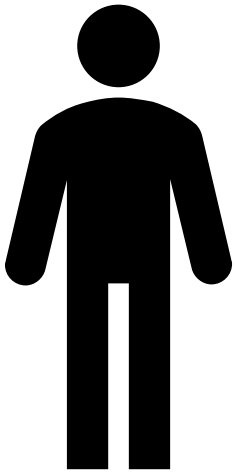


Outline

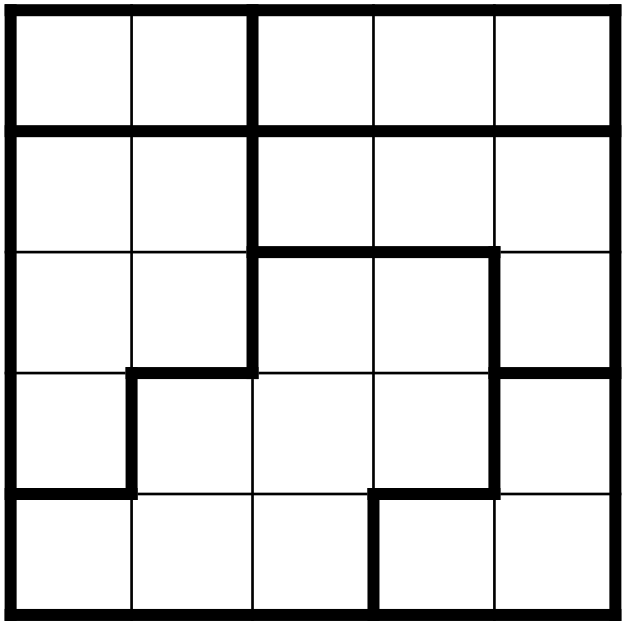
1. Background
   - Norinori
   - Scenario
   - Contribution
2. Idea
3. Our Construction
4. Conclusion

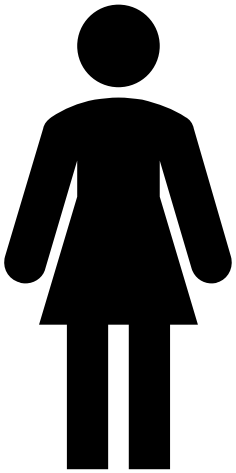
Conclusion

✓Designed *a physical ZKP protocol* for Norinori using cards and envelopes.



Player P





Player V