Light ~~Lightweight~~ Cryptography

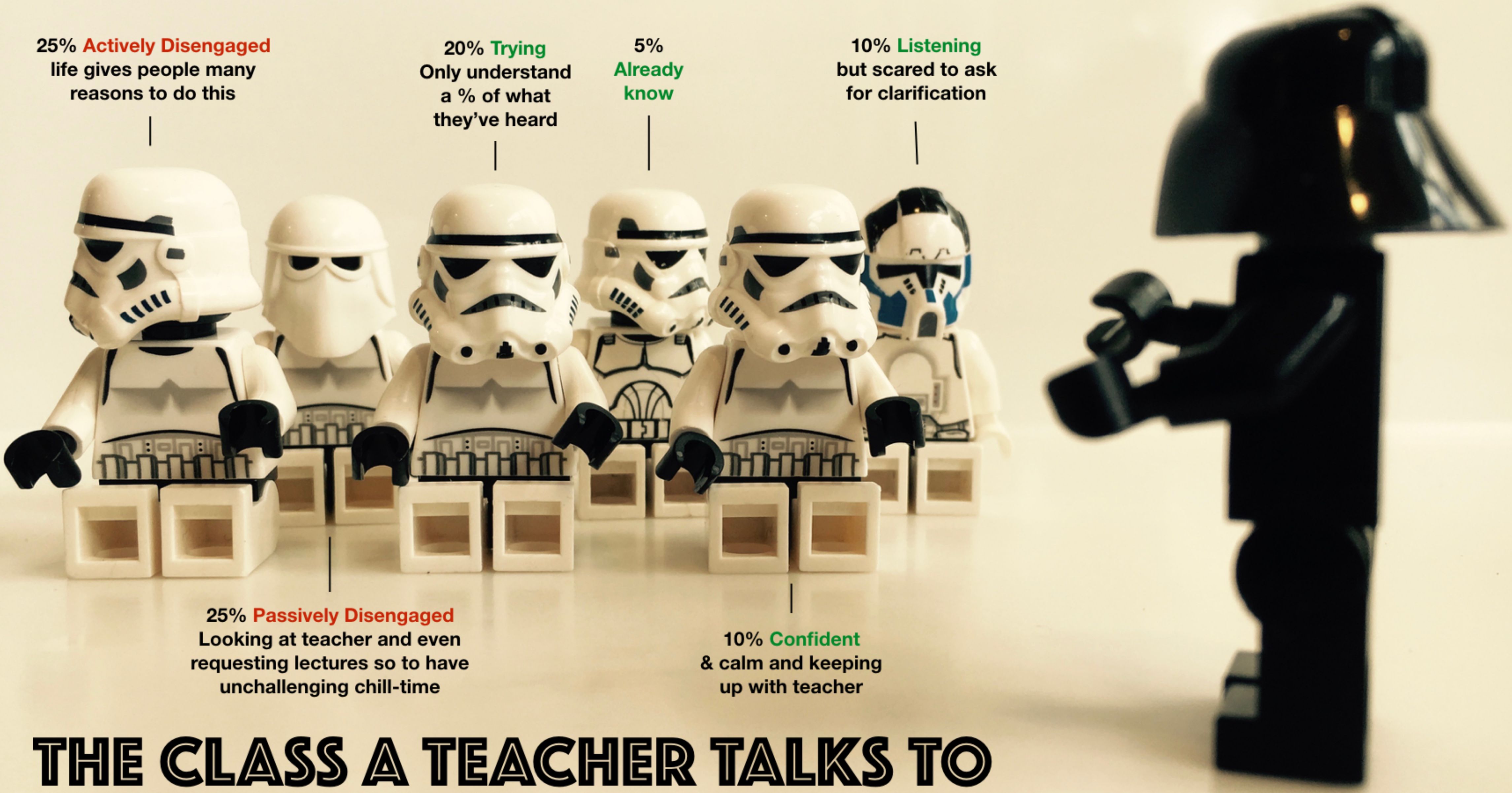
Pascal Lafourcade (LIMOS, France)

Takaaki Mizuki (Tohoku University, Japan)

Atsuki Nagao (Ochanomizu University, Japan)

Kazumasa Shinagawa (Tokyo Tech / AIST, Japan)

darkside



25% Actively Disengaged
life gives people many
reasons to do this

20% Trying
Only understand
a % of what
they've heard

5%
Already
know

10% Listening
but scared to ask
for clarification

25% Passively Disengaged
Looking at teacher and even
requesting lectures so to have
unchallenging chill-time

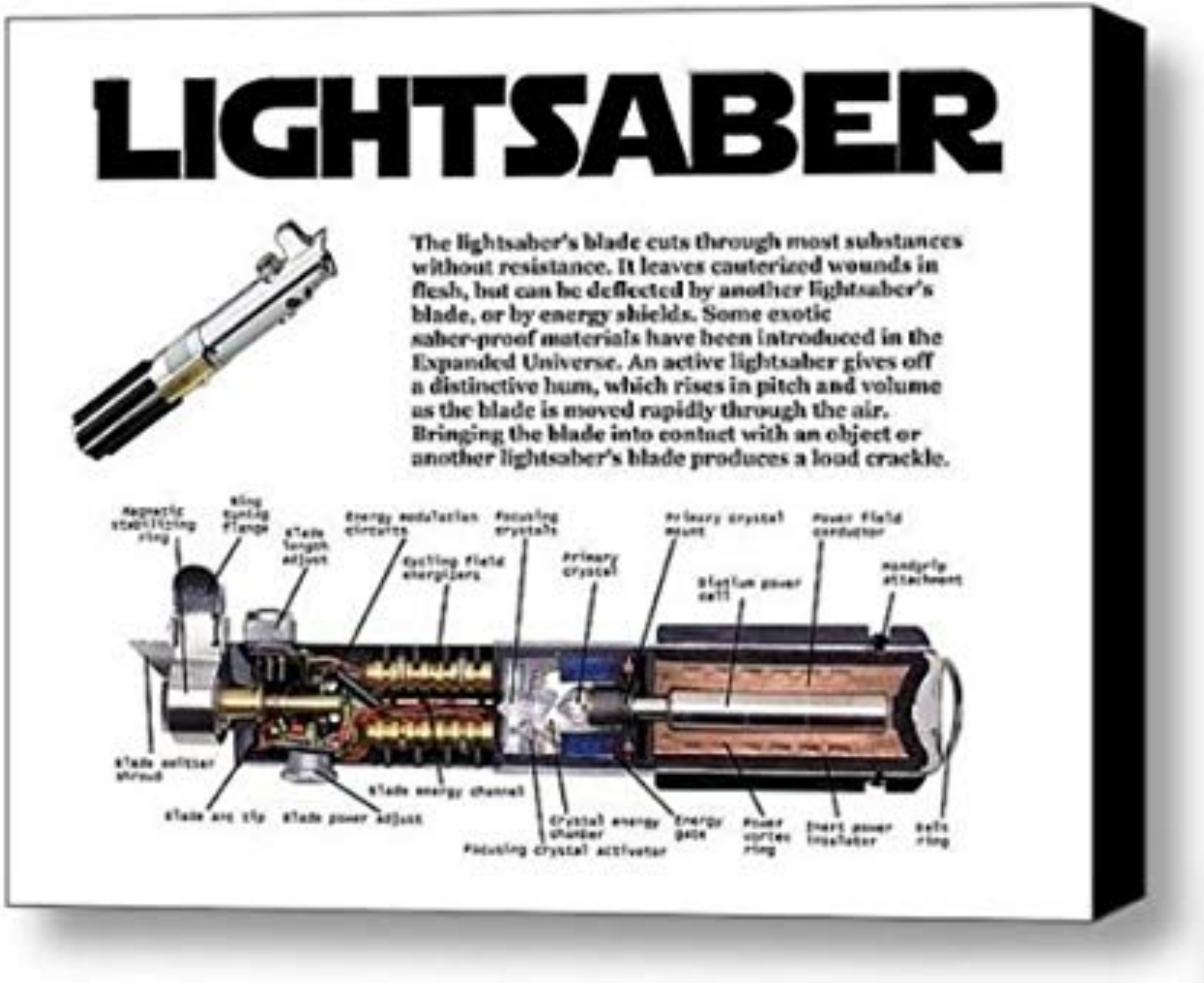
10% Confident
& calm and keeping
up with teacher

THE CLASS A TEACHER TALKS TO

Based on over 2000 high school student responses to how they felt with each of their teachers

By Richard Wells @EduWells

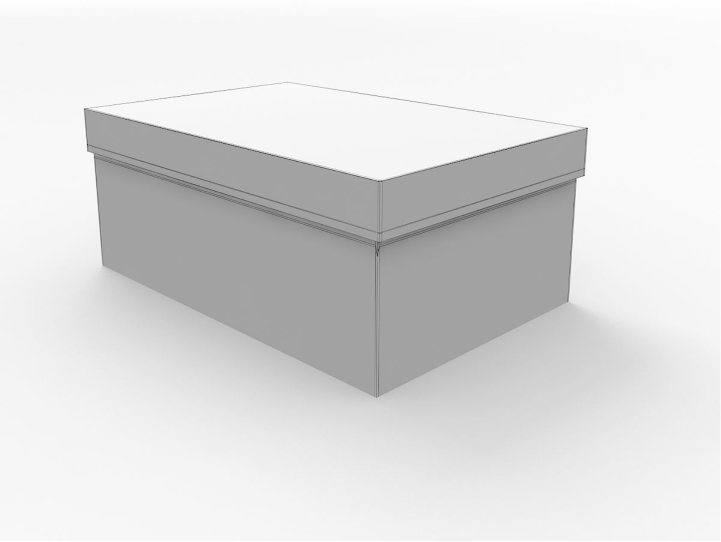
more at EduWells.com



LIGHTSABER

The lightsaber's blade cuts through most substances without resistance. It leaves cauterized wounds in flesh, but can be deflected by another lightsaber's blade, or by energy shields. Some exotic saber-proof materials have been introduced in the Expanded Universe. An active lightsaber gives off a distinctive hum, which rises in pitch and volume as the blade is moved rapidly through the air. Bringing the blade into contact with an object or another lightsaber's blade produces a loud crackle.

Material



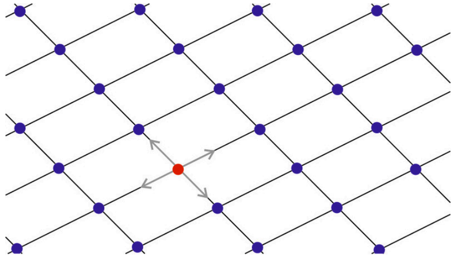
Agenda

1. Introduction
   - Physical cryptography
   - Related works
2. Light cryptography
   - Model
   - Set-Intersection protocol
   - Min/Max protocol
   - Addition protocol
3. Conclusion

Agenda

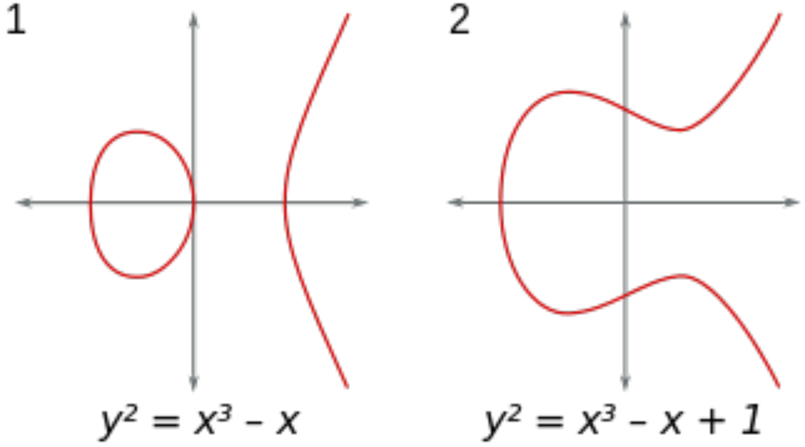
1. Introduction
   - Physical cryptography
   - Related works
2. Light cryptography
   - Model
   - Set-Intersection protocol
   - Min/Max protocol
   - Addition protocol
3. Conclusion

Background



- Modern cryptography is more and more used and complex

- Teaching cryptography is hard
  - Complex algorithm
  - Security
  - Deep mathematics
  - Not visualized



OUR GOAL : a good educational tool for cryptography

Physical cryptography

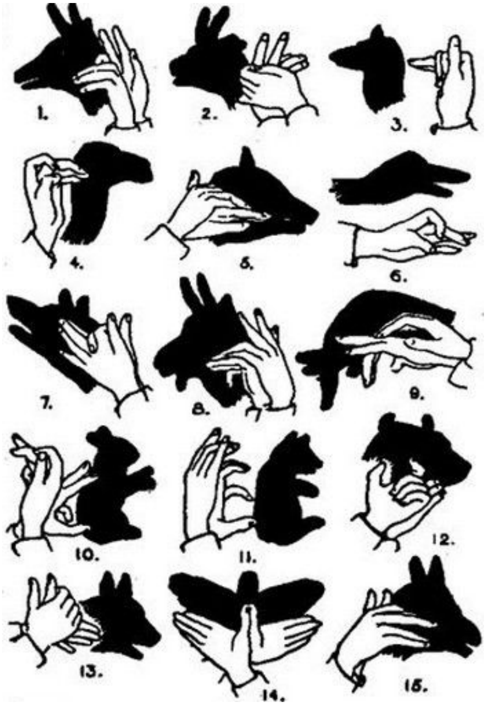
- Cryptography using physical objects (e.g. playing cards)

- Suitable for education
  - Good visualization
  - Concrete
  - Introduction to cryptographic concepts
  - No need of mathematics knowledge

Light cryptography

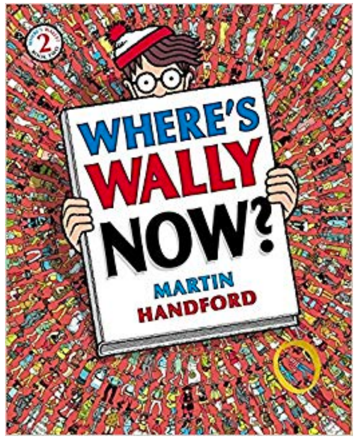
New model of physical cryptography

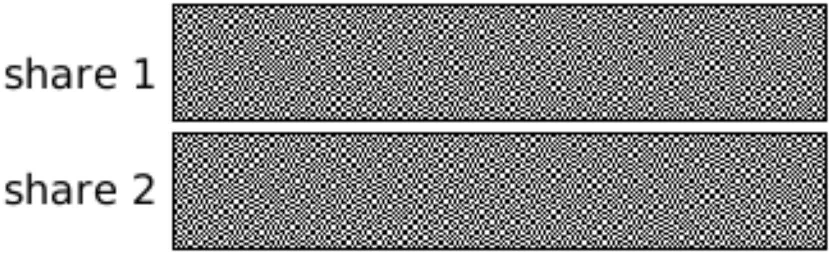
- Computation based on light and shadows
- Easy to understand
- Secure



Related works

- Zero-knowledge proof for “Where’s Wally” [1]
  - Proof that “I know Wally’s position” without revealing the position
- Visual secret sharing [2]
  - Secret image is reconstructed by stacking two transparent sheets
- Card-based protocols [3]
  - Secure computation protocol using a deck of cards (like playing cards)





[1] Naor, Naor, and Reingold, “Applied Kid Cryptography or How To Convince Your Children You Are Not Cheating”, EUROCRYPT 1999.

[2] Naor and Shamir, “Visual Cryptography”, EUROCRYPT 1994.

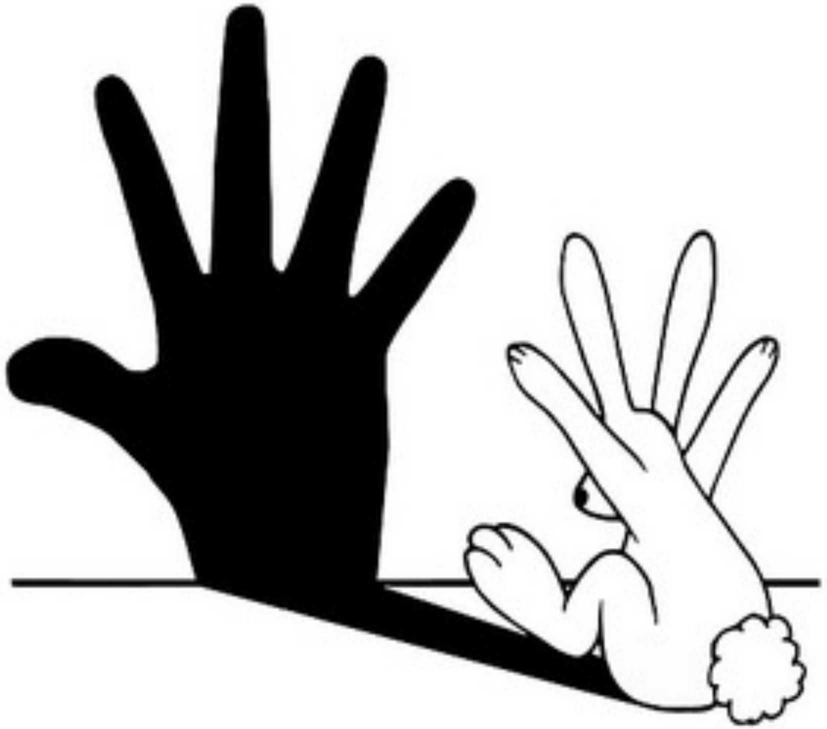
[3] den Boer, “More Efficient Match-Making and Satisfiability The Five Card Trick”, EUROCRYPT 1989.

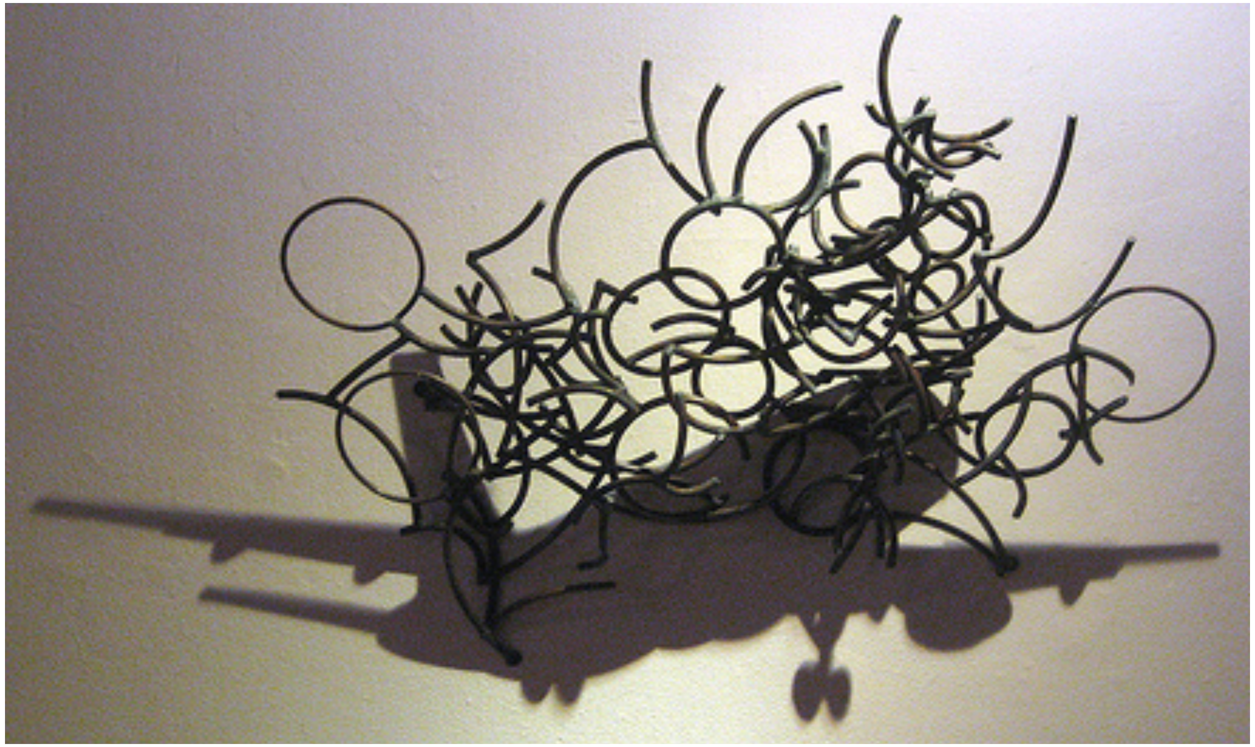
Agenda

1. Introduction
   - Physical cryptography
   - Related works
2. Light cryptography
   - Model
   - Set-Intersection protocol
   - Min/Max protocol
   - Addition protocol
3. Conclusion

Properties of shadows

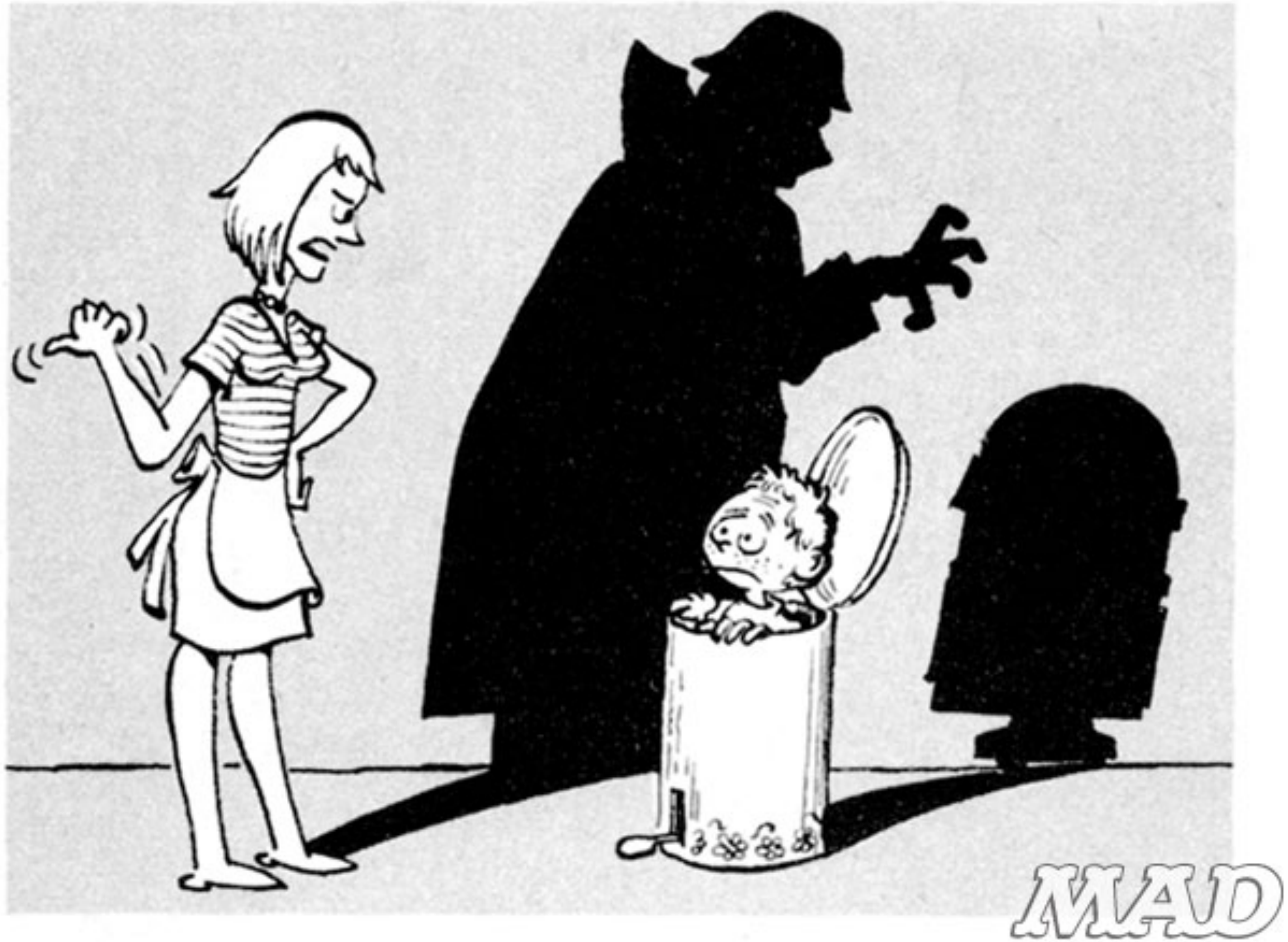
- It is sometimes hard to imagine its original shape from shadows





Who knows what evils lurk in the hearts of men?

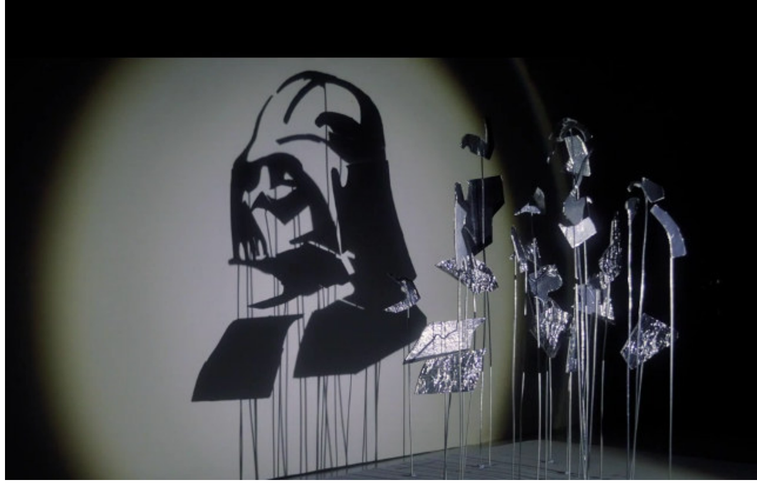
THE SHADOW KNOWS



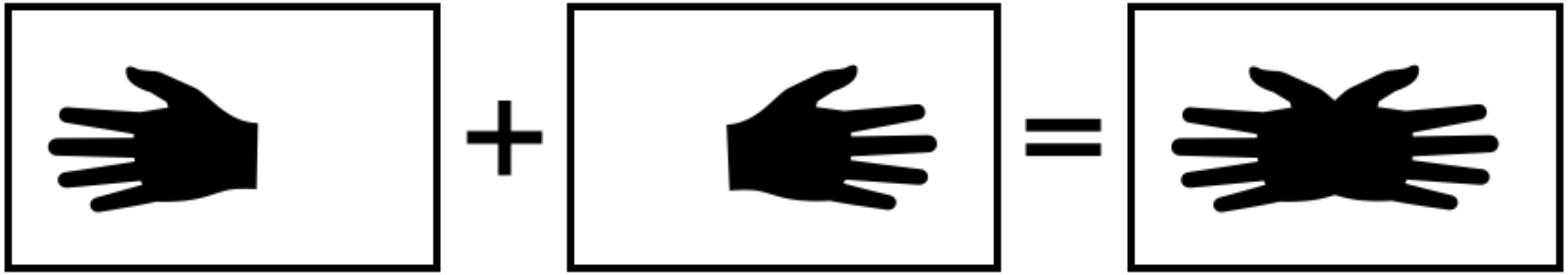
MAD

madmagazine.com

Properties of shadows



The resulting shadow is the union of shadows

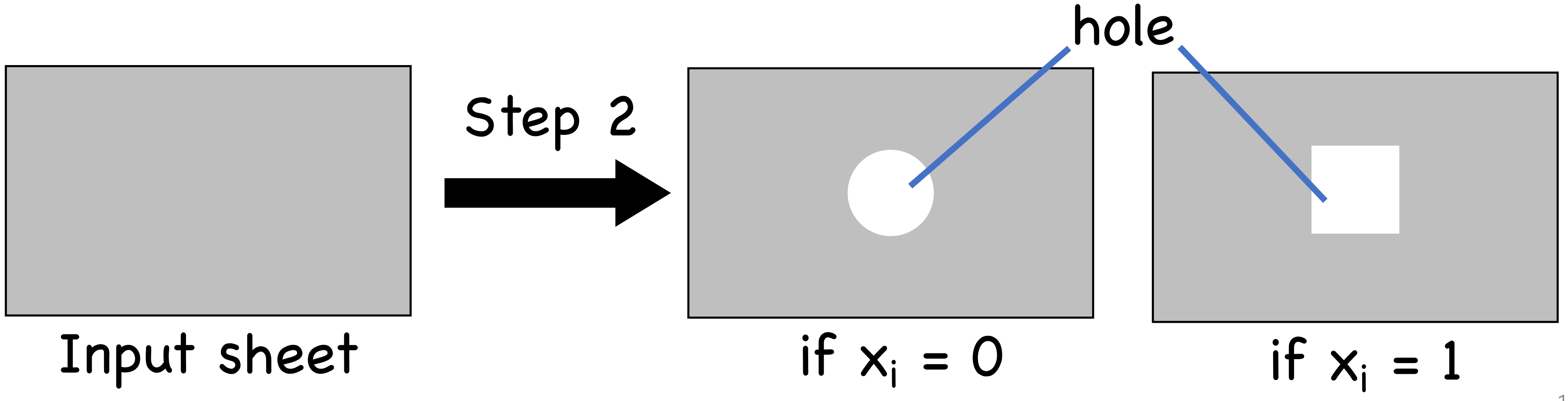


Shadow *addition*

Protocols of Light Cryptography

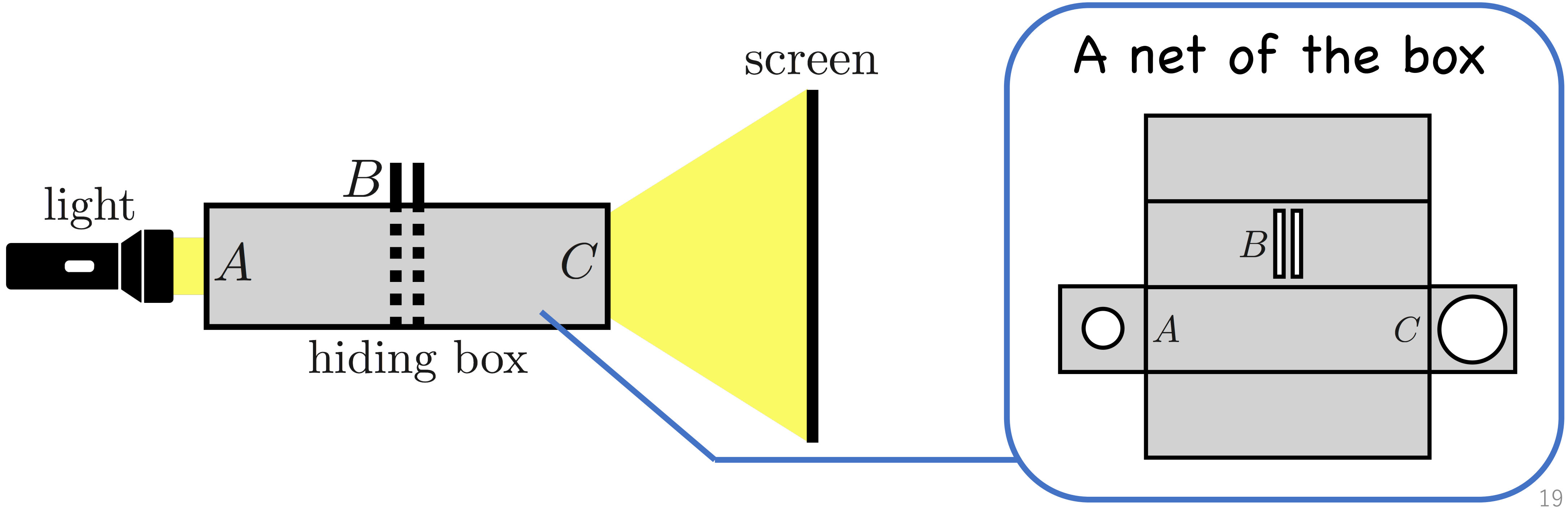
- Start: Each party has a secret input x_i
- Goal: Compute a joint function $f(x_1, x_2, \ldots, x_n)$ with hiding secrets

1. Each party has an input sheet
2. Depending on own input, each party makes holes in the sheet



Protocols of Light Cryptography

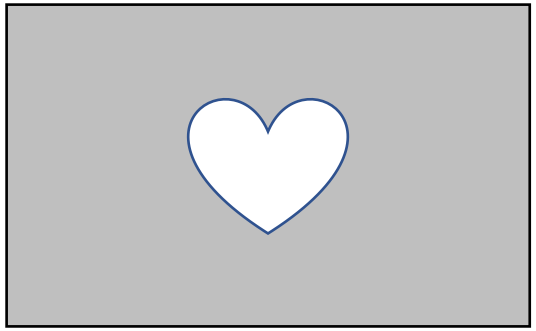
3. Each party inserts own input sheet in the hiding box (B)
4. (A) is illuminating by the light
5. The result image is printed on the screen



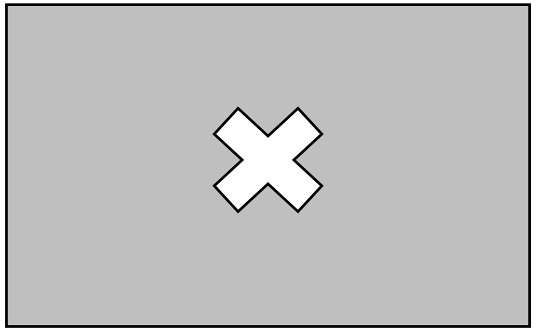
How to “securely” have an agreement

Alice	Bob	
Yes	Yes	→ agreement
Yes	No	→ disagreement
No	Yes	
No	No	

Determine the current situation without revealing inputs directly



if Yes



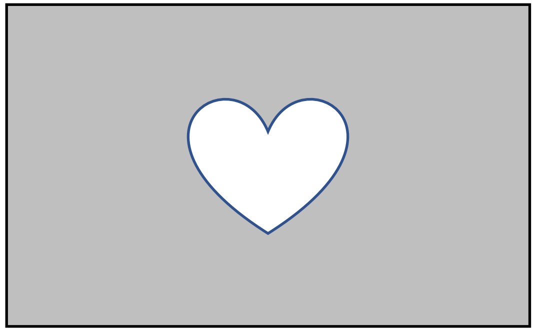
if No

How to “securely” have an agreement

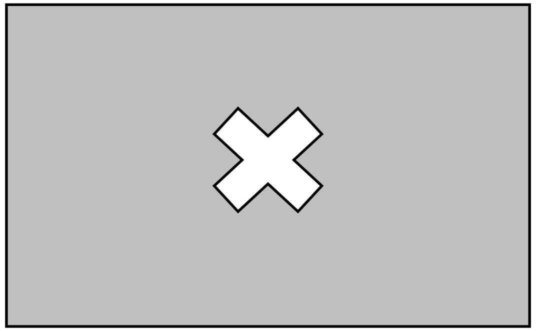
Alice	Bob	
Yes	Yes	→ agreement
Yes	No	→ disagreement
No	Yes	
No	No	

Determine the current situation without revealing inputs directly

Computation of an AND



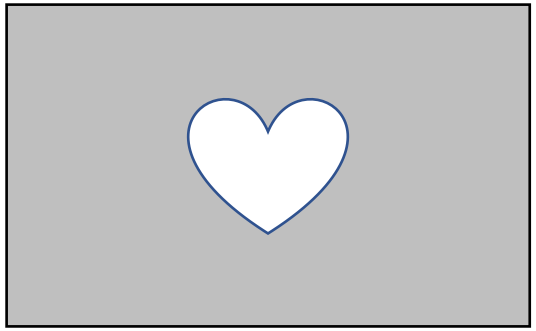
if Yes



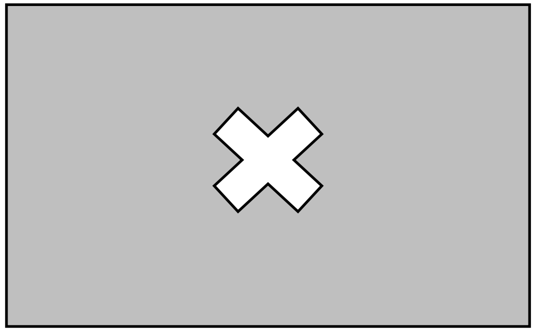
if No

How to “securely” have an agreement

Alice	Bob	
Yes	Yes	→ agreement
Yes	No	→ disagreement
No	Yes	
No	No	



if Yes



if No

Determine the current situation without revealing inputs directly

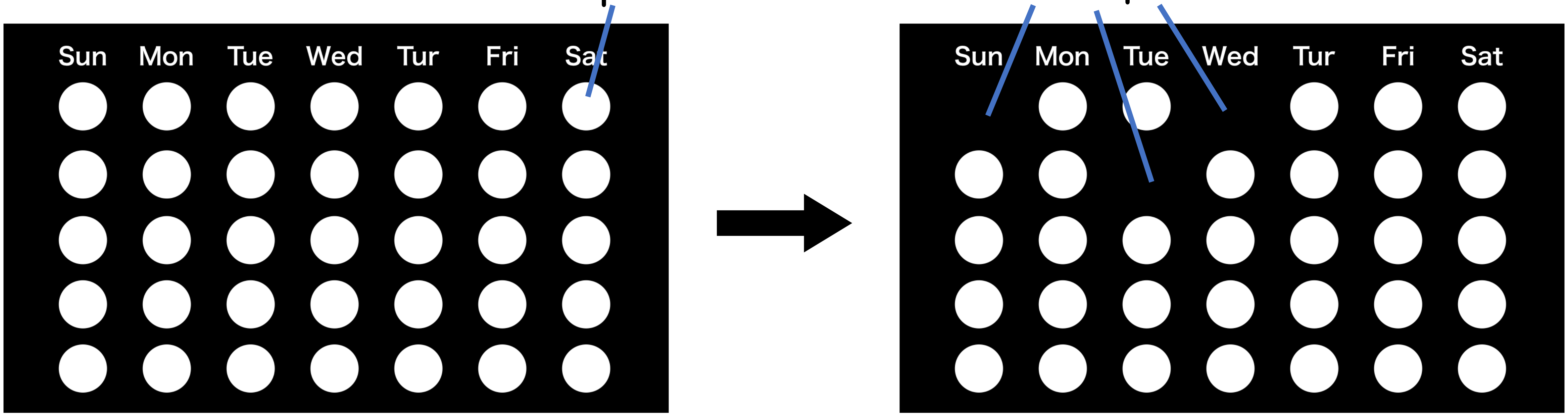
Computation of an AND

NOBODY LEARNS OTHER CHOICE

Schedule a meeting for next month?

Transparent sheets

- Input sheets also can be implemented by transparent sheets
- Each party fills it by a black pen or a black-colored seals



transparent

black pen

The black image is printed on transparent sheets

Depending on input, some circles are filled by a black pen

Scheduling (set-intersection)

Input sheet

Sun	Mon	Tue	Wed	Tur	Fri	Sat
○	○	○	○	○	○	○
○	○	○	○	○	○	○
○	○	○	○	○	○	○
○	○	○	○	○	○	○
○	○	○	○	○	○	○

Alice's schedule

Sun	Mon	Tue	Wed	Tur	Fri	Sat
○	○	○	○			○
○	○	○			○	○
○	○			○	○	○
○			○	○	○	○
		○	○	○	○	○

Bob's schedule

Sun	Mon	Tue	Wed	Tur	Fri	Sat
		○	○	○	○	○
○			○	○	○	○
○	○			○	○	○
○	○	○			○	○
○	○	○	○			○

result

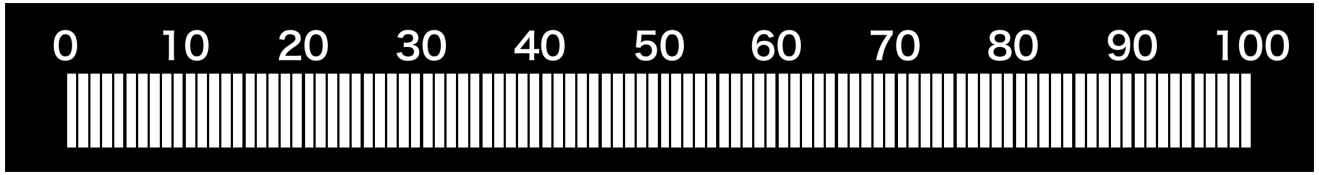
Sun	Mon	Tue	Wed	Tur	Fri	Sat
		○	○			○
○					○	○
○	○			○	○	○
○					○	○
		○	○			○

NOBODY LEARNS OTHER CHOICE

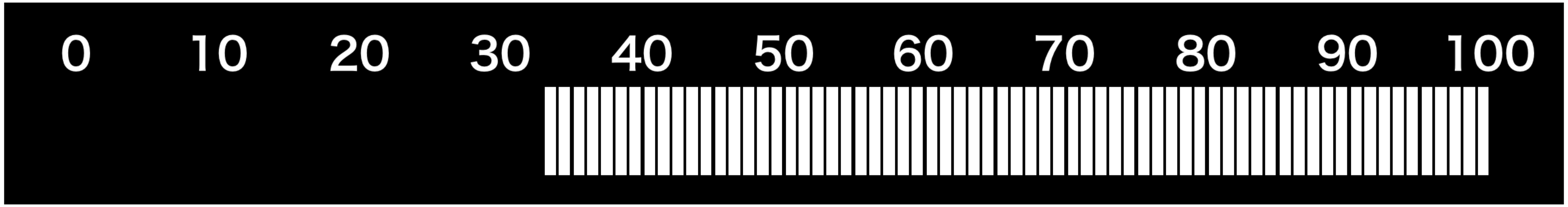
Compute the maximum of salaries ?

Max protocol

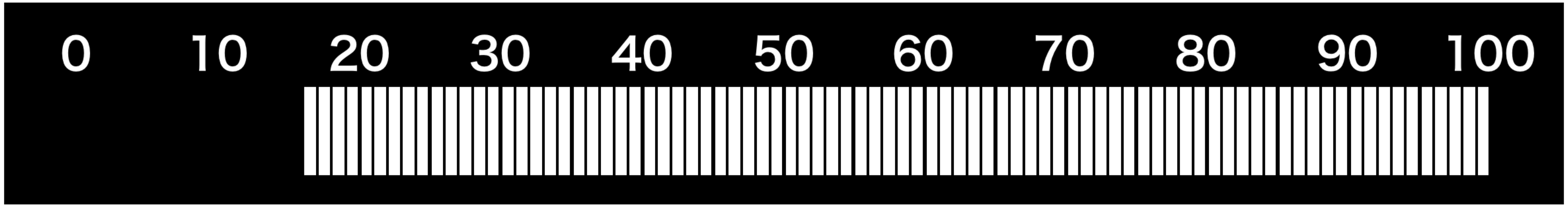
Input sheet



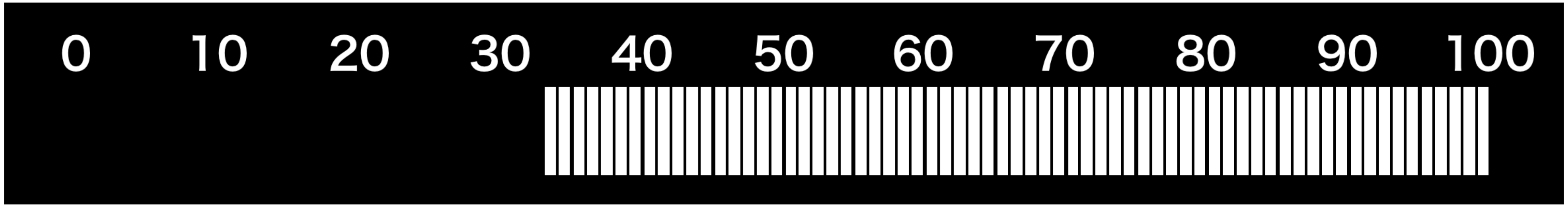
Alice's
input = 33



Bob's
input = 16



result = 33

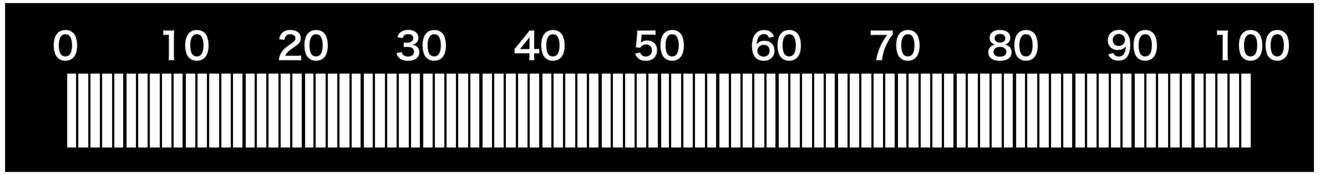


NOBODY LEARNS OTHER CHOICE

Compute the minimum of salaries ?

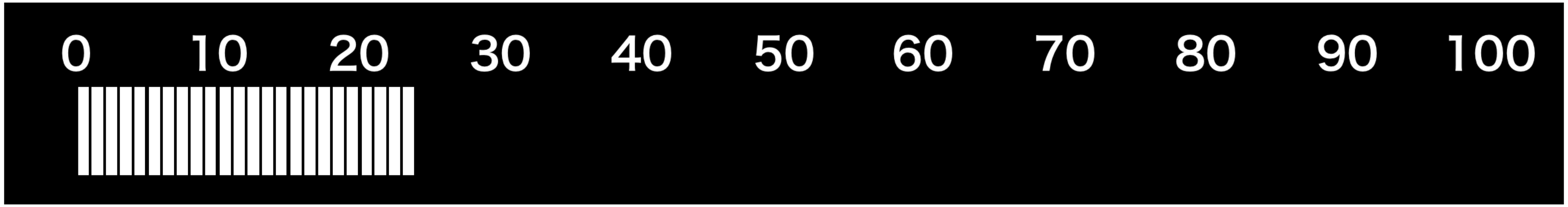
Min protocol

Input sheet



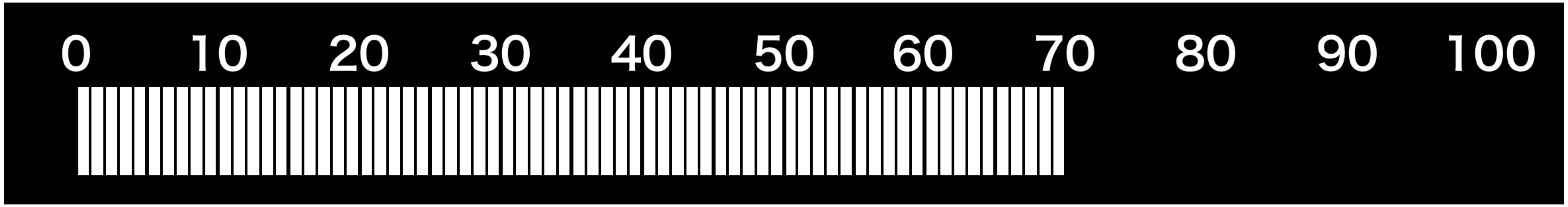
Alice's

input = 24

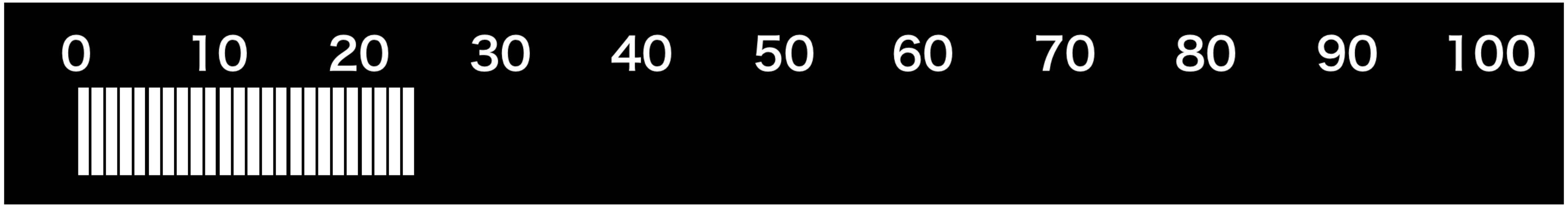


Bob's

input = 70



result = 24

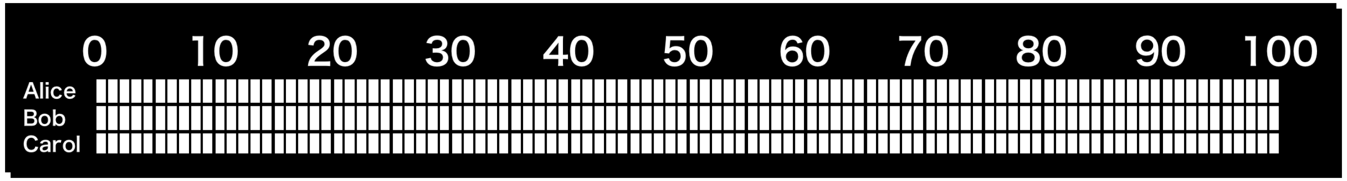


NOBODY LEARNS OTHER CHOICE

Compute who is the millionaire?

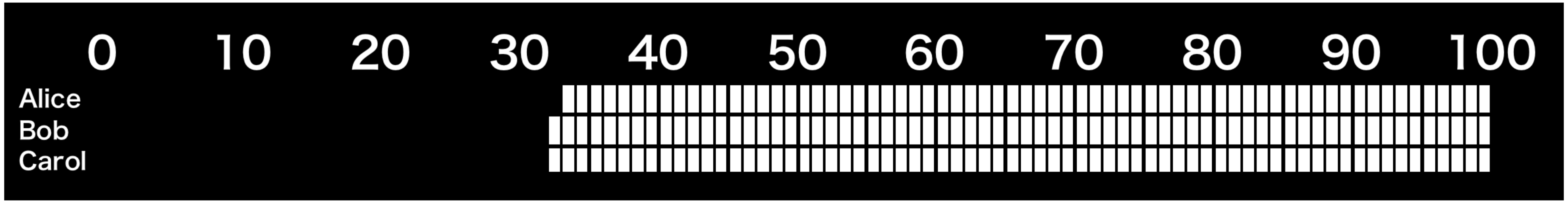
Max with name

Input sheet



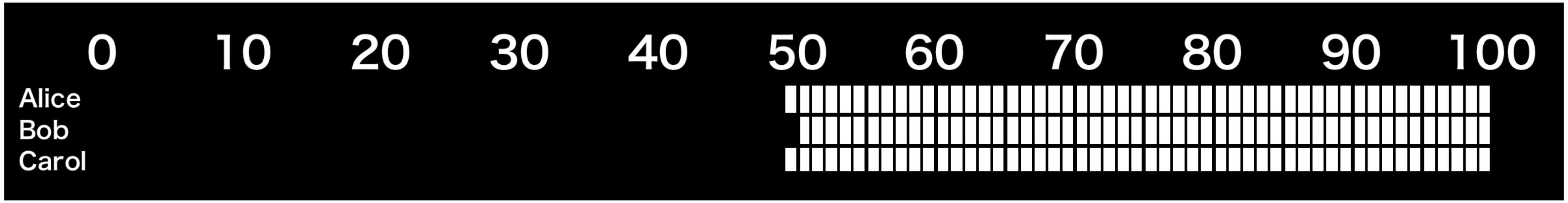
Alice's

input = 33



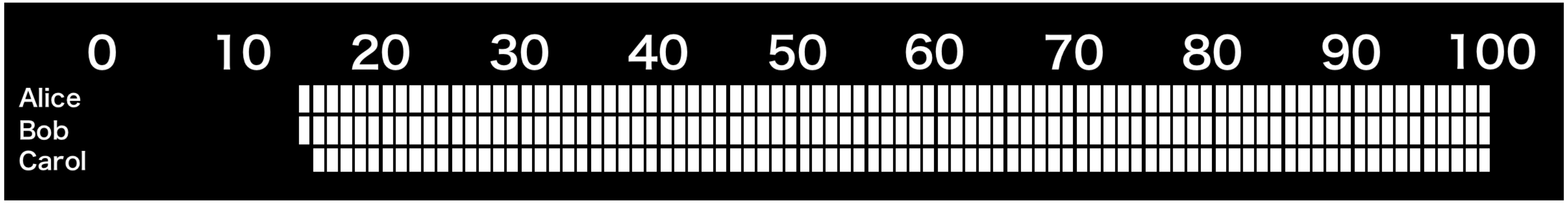
Bob's

input = 50



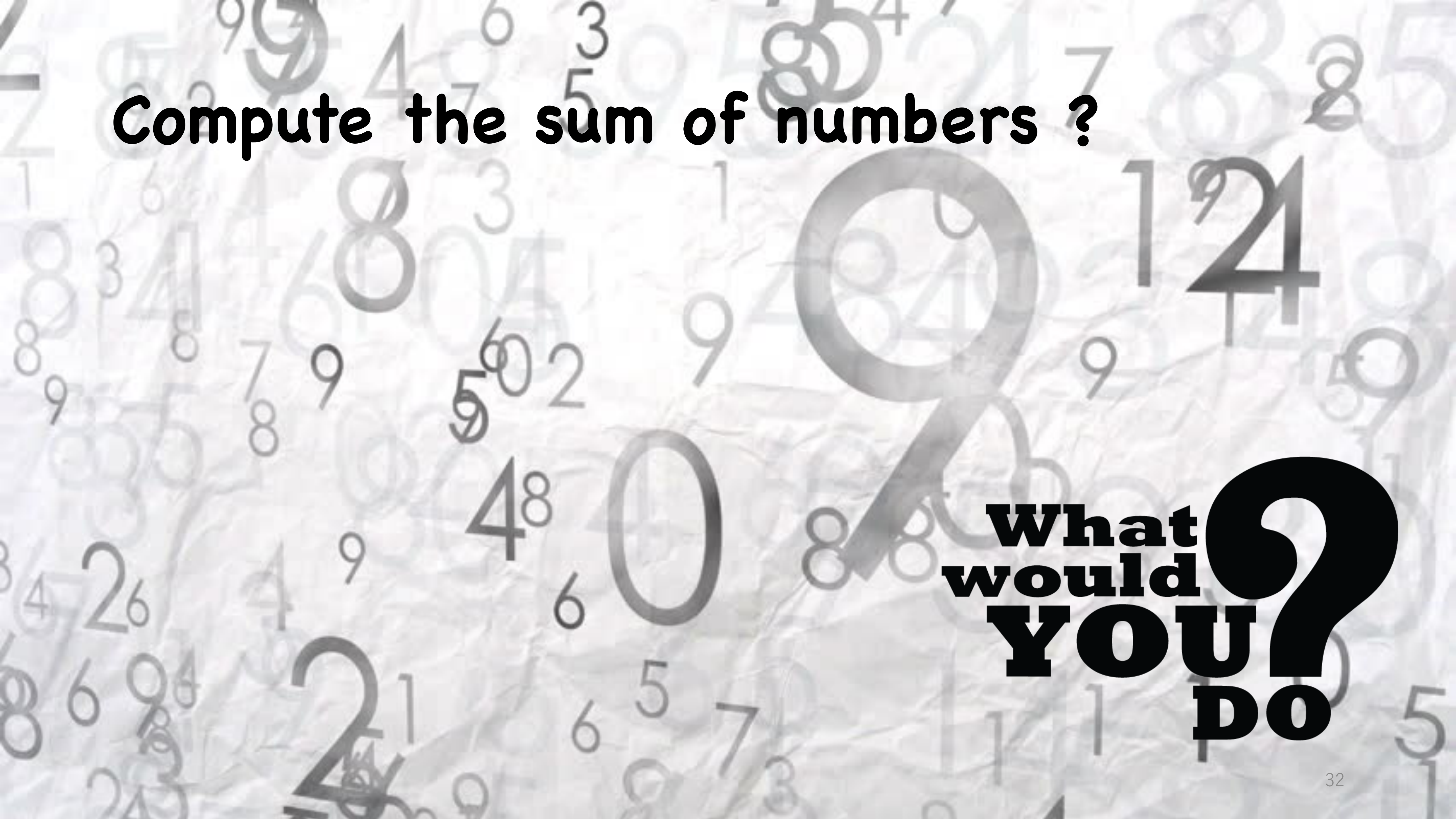
Carol's

input = 50



NOBODY LEARNS OTHER CHOICE

Compute the sum of numbers ?

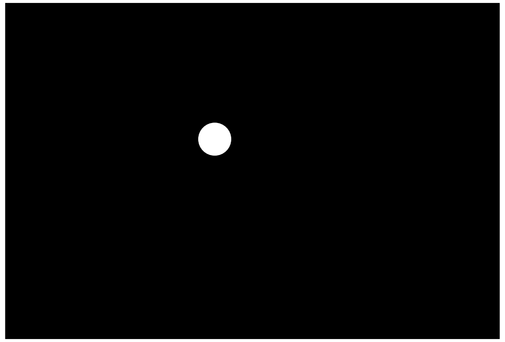


Addition protocol 0

Input sheet:

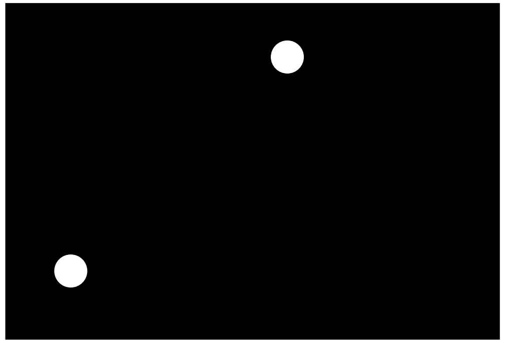
Alice's

input = 1



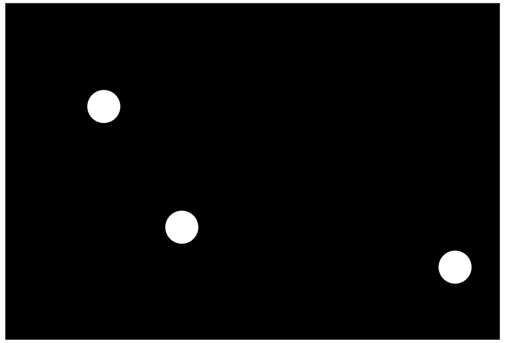
Bob's

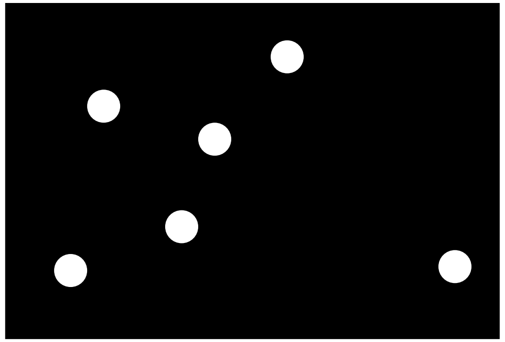
input = 2



Carol's

input = 3

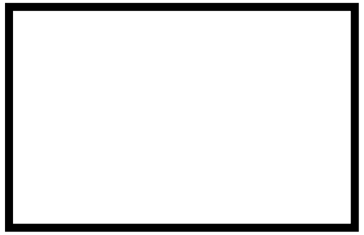




- The output image is randomized
- If two circles are collude, the output is not correct

Addition protocol 1

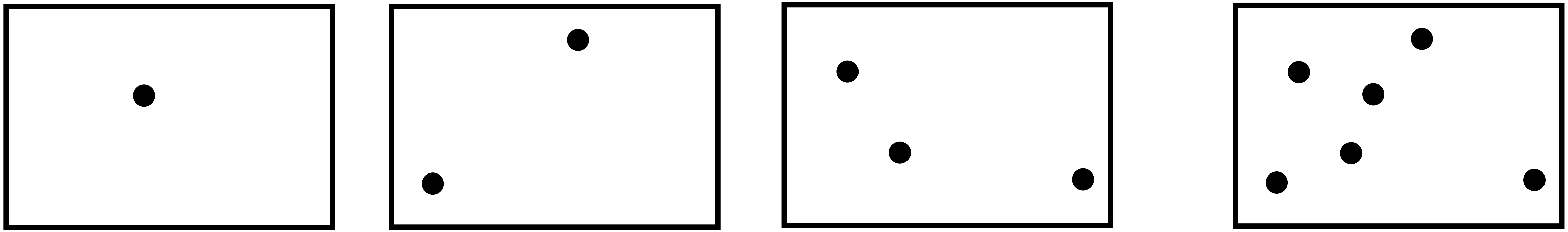
Input sheet:



Alice's input = 1

Bob's input = 2

Carol's input = 3



- The output image is randomized
- If two circles are collude, the output is not correct

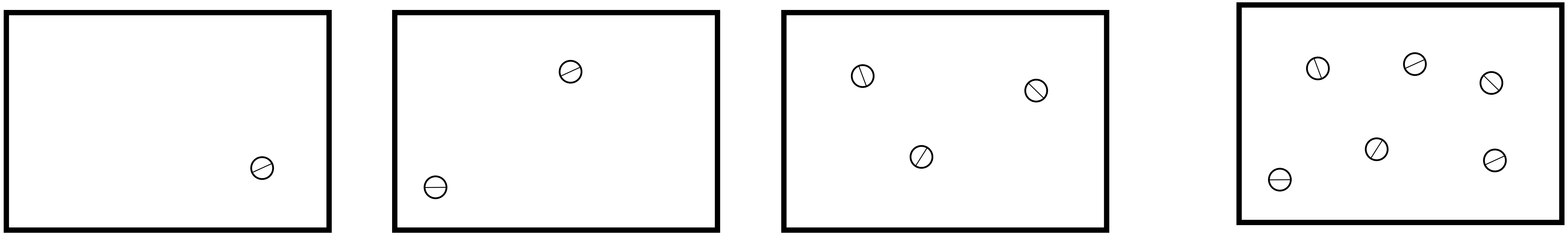
Addition protocol 2

Input sheet:

Alice's
input = 1

Bob's
input = 2

Carol's
input = 3



- Use ⊖ instead of ●
- The collision probability is reduced

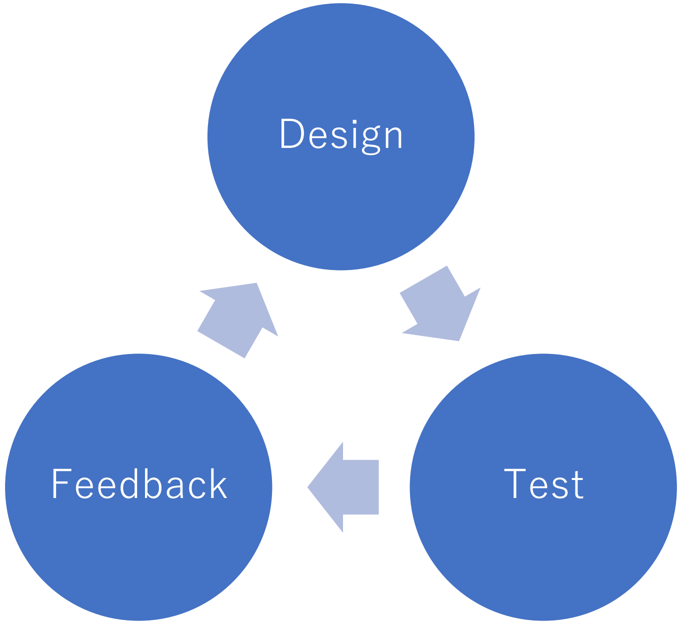
Conclusion

CONTRIBUTIONS:

- Light cryptography is a new model of physical cryptography
- Secure computation based on light and shadows :
  - Max/Minimum
  - Addition
  - Schedule

Future directions

- Use it in cryptography courses



- Designe more protocols : Subtraction ? Multiplication ?
- Study more about physical cryptography

Questions ?