Two-Round Secure Multiparty Computation Minimizing Public Key Operations

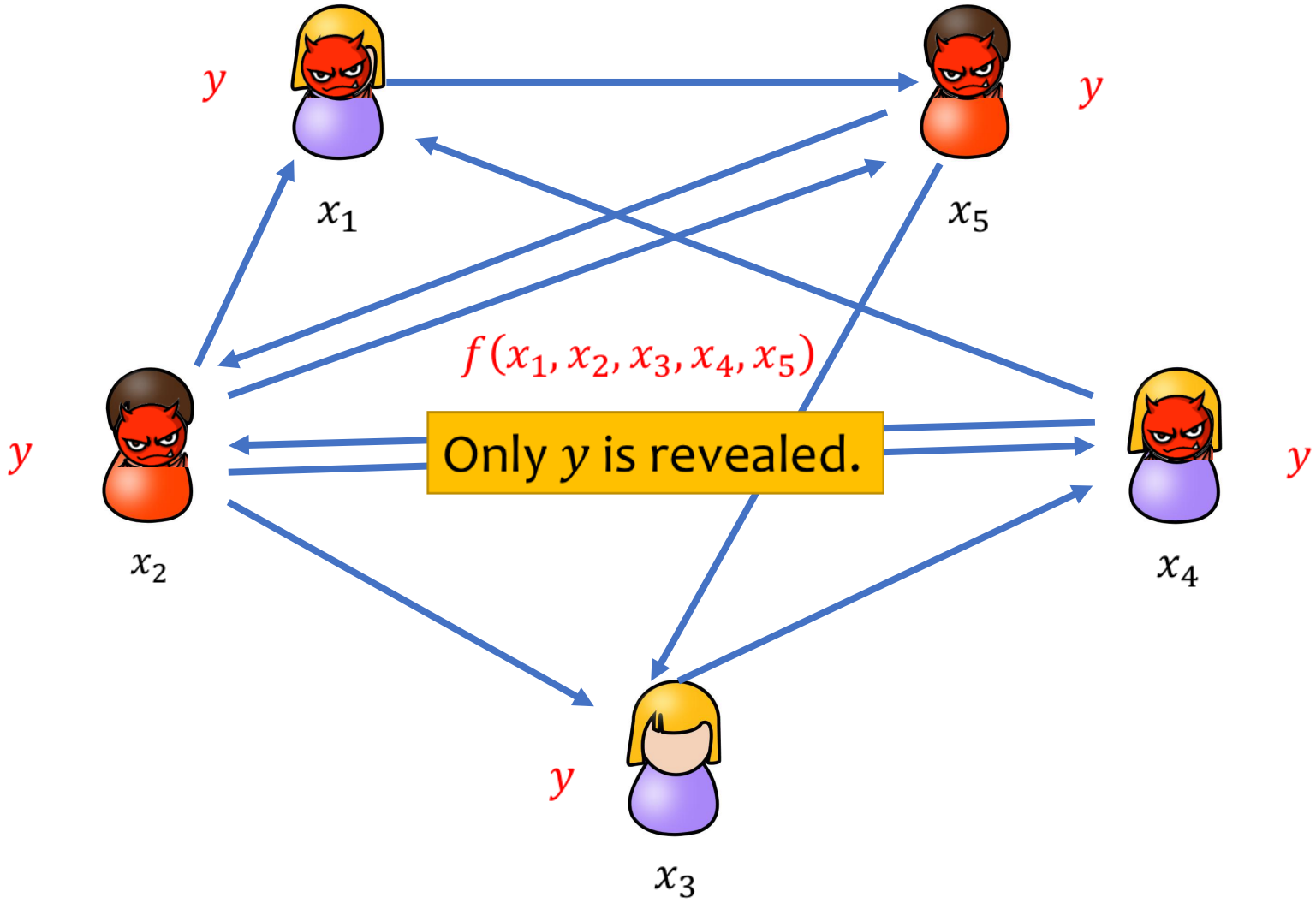
Sanjam Garg Peihan Miao Akshayaram Srinivasan

What did we achieve?

Two-Round Secure Multiparty Computation Minimizing Public Key Operations

Sanjam Garg Peihan Miao Akshayaram Srinivasan

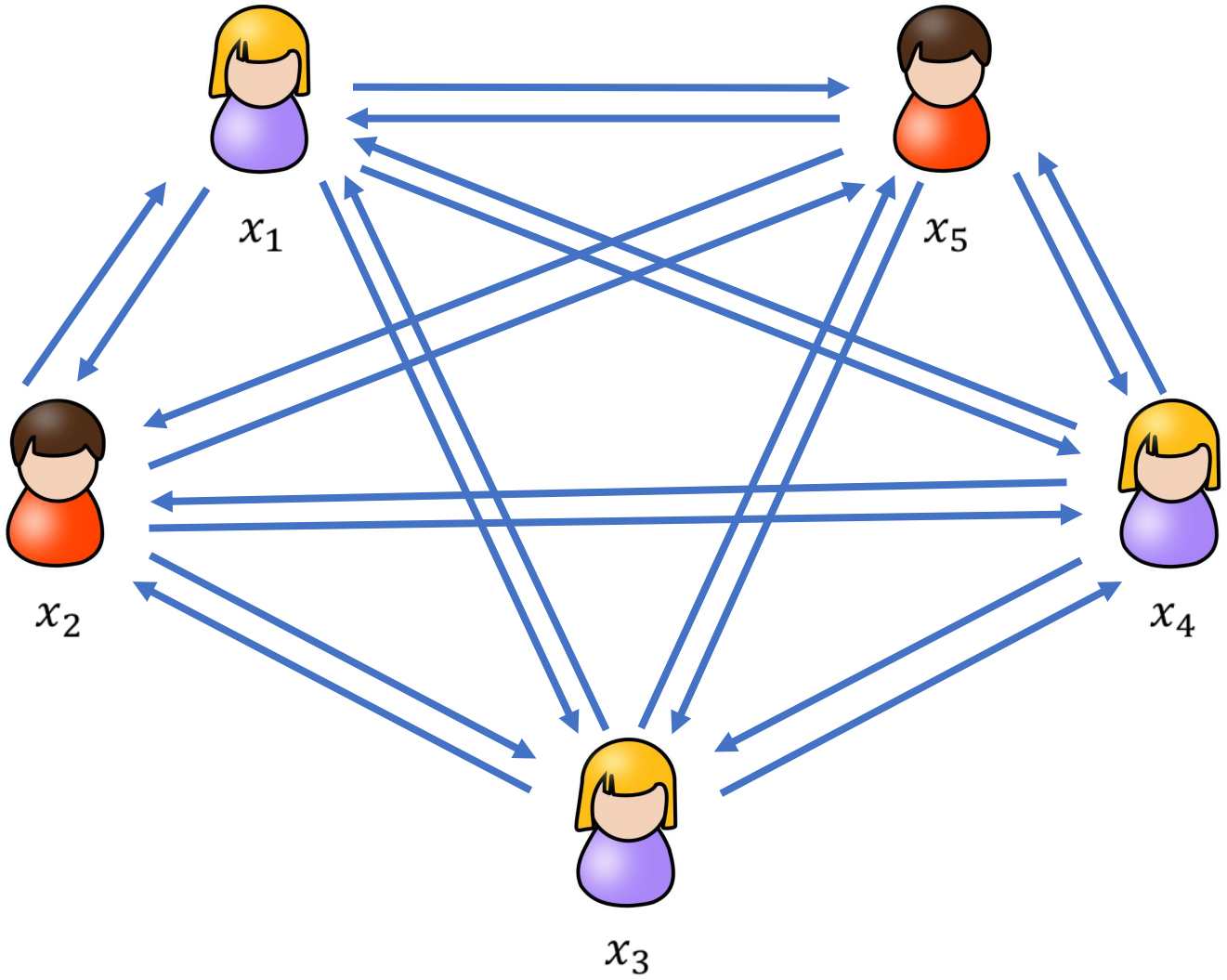
Secure Multiparty Computation (MPC)



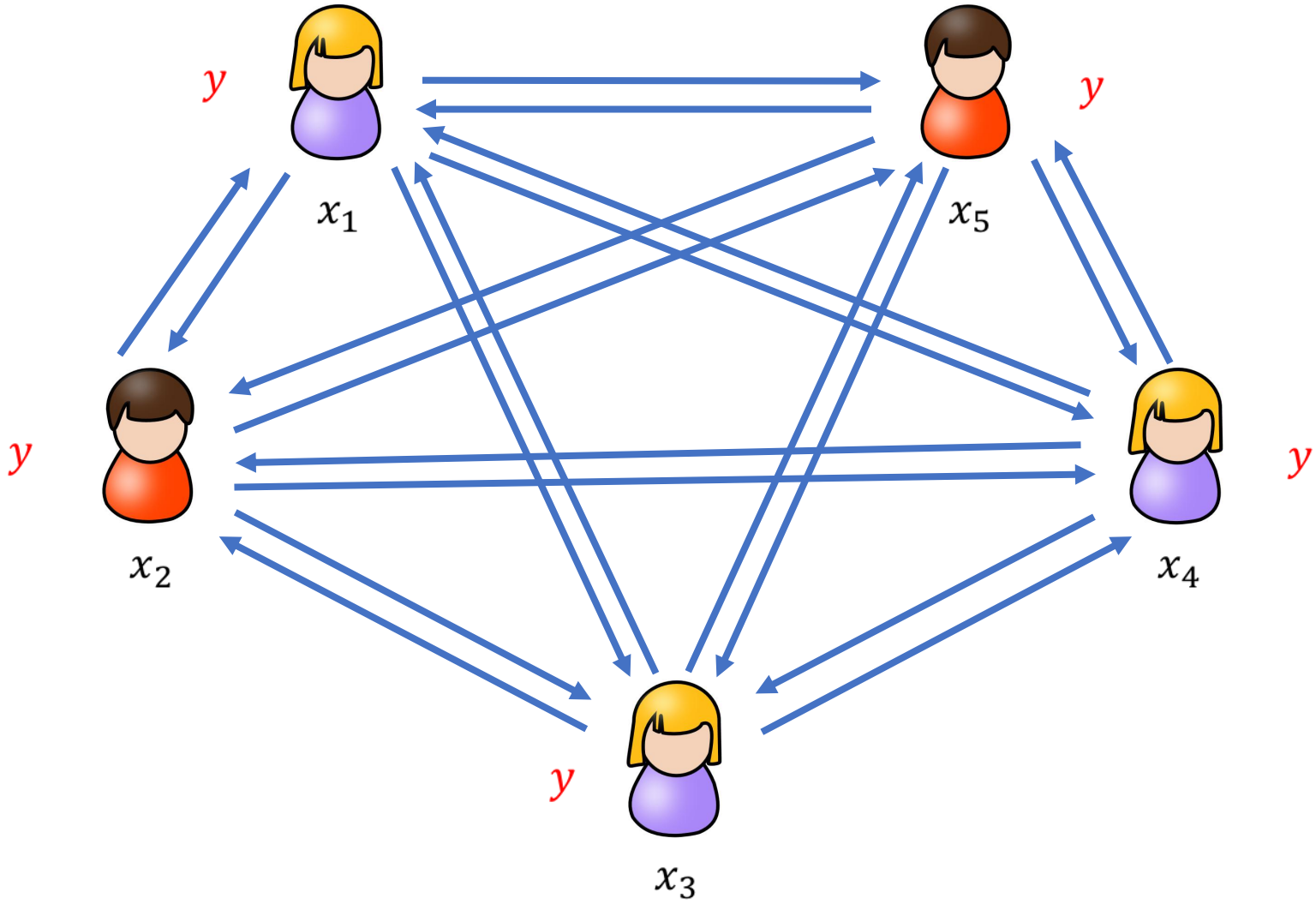
What does Two-Round mean?

The MPC protocol has two rounds.

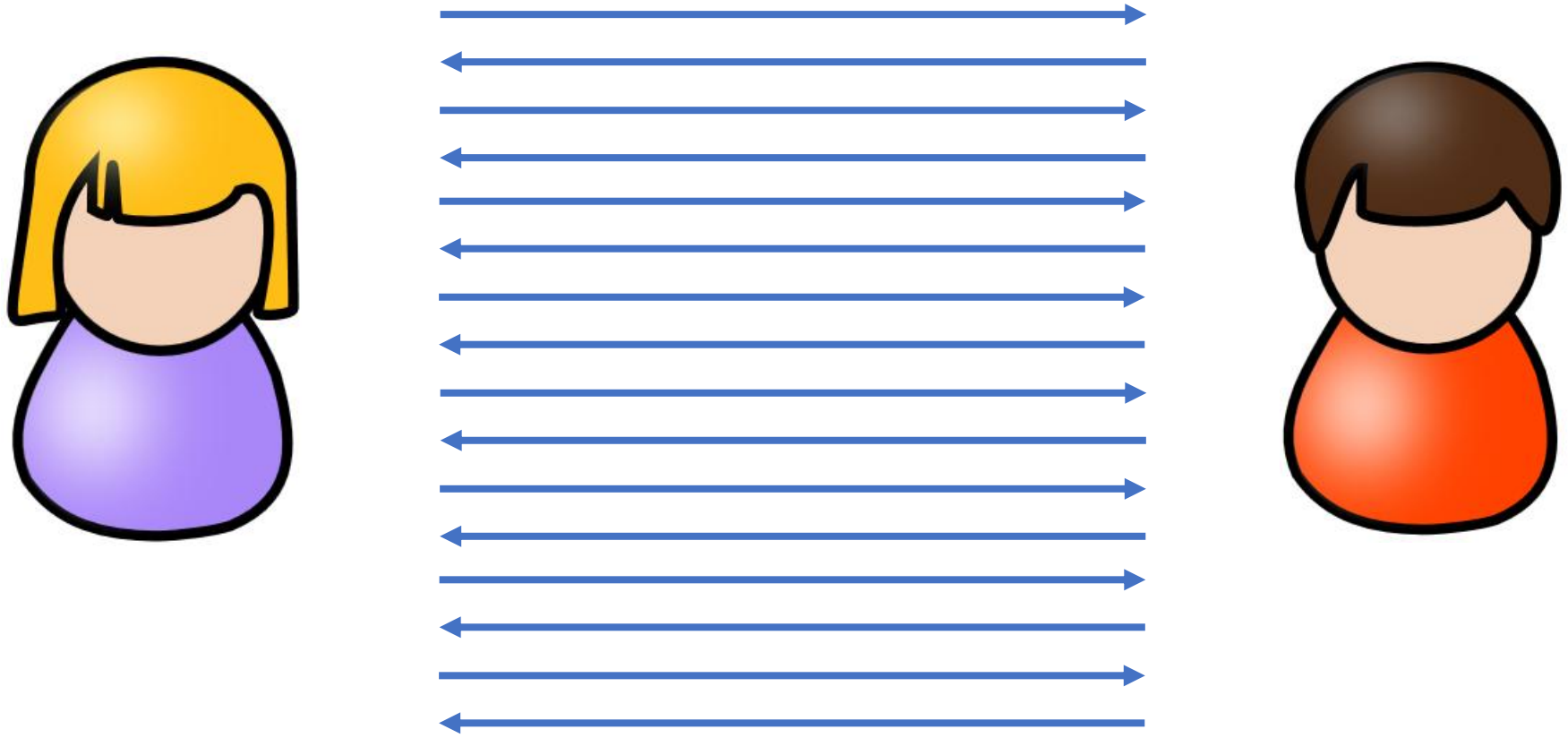
Two-Round MPC



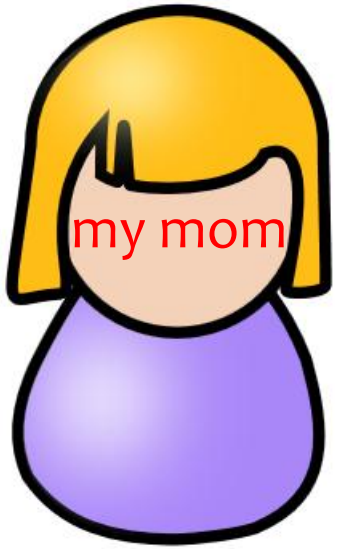
Two-Round MPC

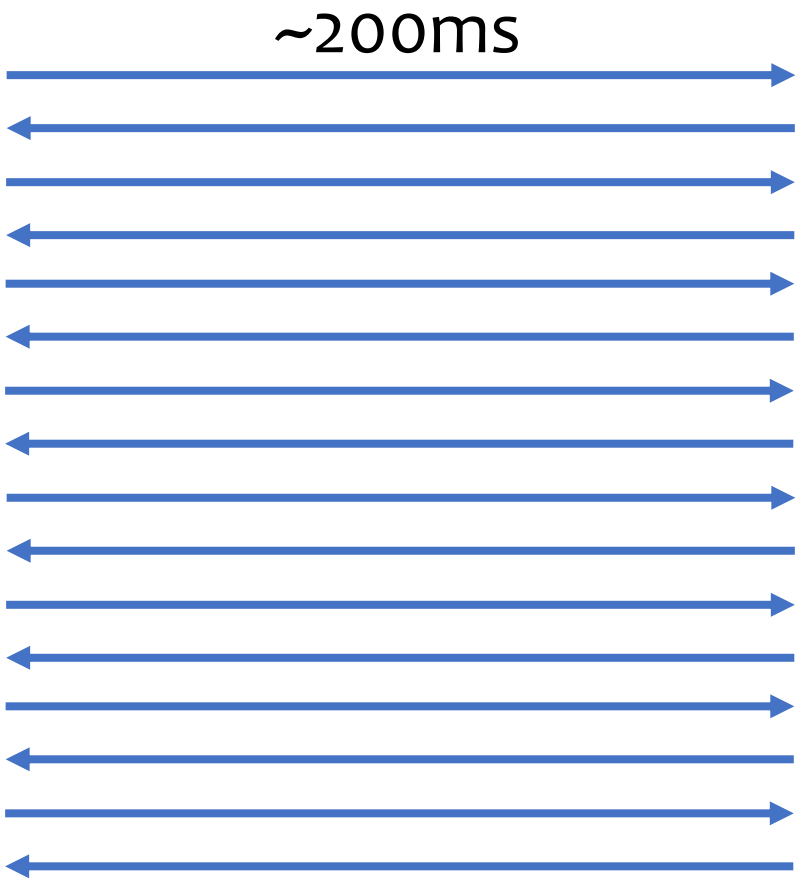


Why is round complexity important?



Why is round complexity important?





Why not one round?

Because it’s impossible! [HLP’11]

Two-Round MPC?

- [Yao'86, GMW'87]: any function, round = depth of C
- [BMR'90]: constant rounds
- 2 rounds from various assumptions
  - Indistinguishability Obfuscation (iO) [GGHR'14]
  - Witness Encryption [GLS'15]
  - Learning With Errors (LWE) [MW'16, BP'16, PS'16]
  - Bilinear Maps [GS'17]
  - 2-Round Oblivious Transfer (OT) [BL'18, GS'18]
- 2-round MPC $\Leftrightarrow$ 2-round OT

Can we implement it?

Yes, but it's too slow…

Why?

Too many public key operations…

Why is it bad?

Because public key operation is VERY slow!

- Symmetric key operations (AES) ~100M/sec
- Public (asymmetric) key operations ~10K/sec

Our Main Result

- 2-round MPC from 2-round OT (minimal assumption)
- State of the art: $\mathrm{poly}(n, \lambda, |C|)$ OTs (public key operations)
- We improve it to: $\mathrm{poly}(n, \lambda)$ OTs (public key operations) + $\mathrm{poly}(n, \lambda, |C|)$ symmetric key operations
  - Semi-honest from 2-round semi-honest OT
  - Malicious from 2-round malicious OT in the CRS model

How did we achieve it?

2-round MPC with $\mathrm{poly}(n, \lambda, |C|)$ OTs

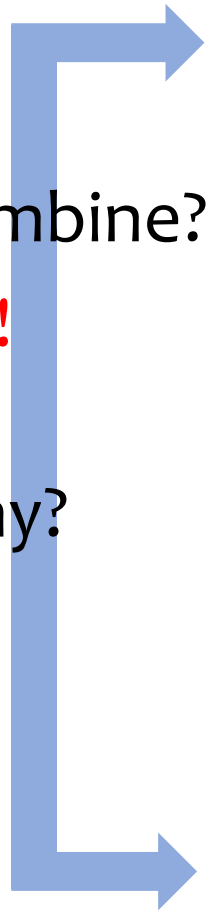
How to reduce OTs (public key operations) ?

OT extension!

- $\mathrm{poly}(n, \lambda, |C|)$ OTs
- Minimize public key operations

2-round OT extension?

Yes! [Beaver'96]



2-round MPC with $\mathrm{poly}(n, \lambda, |C|)$ OTs

Combine?

No!

How to reduce OTs (public key operations) ?

OT extension!

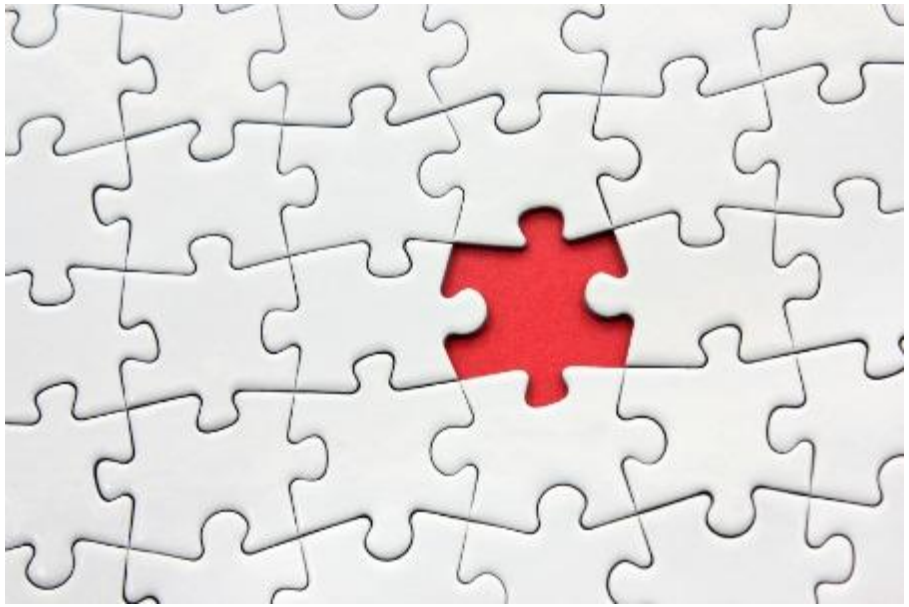
Why?

- $\mathrm{poly}(n, \lambda, |C|)$ OTs
- Minimize public key operations

2-round OT extension?

Yes! [Beaver'96]

2-round MPC with $\mathrm{poly}(n, \lambda, |C|)$ OTs

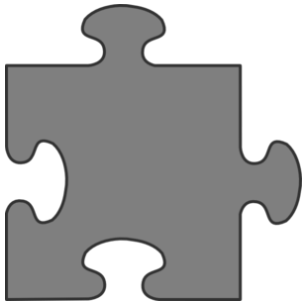


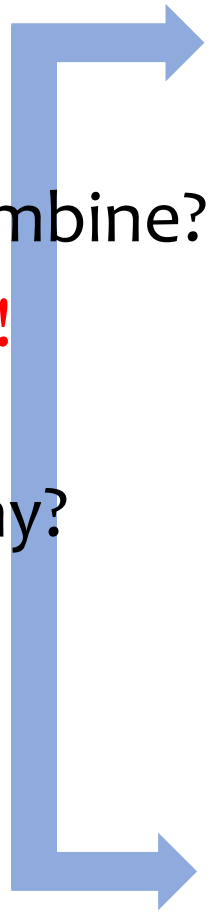
Combine?

No!

Why?

2-round OT extension?





Combine?

No!

Why?

2-round MPC with $\mathrm{poly}(n, \lambda, |C|)$ OTs

- ☑ $\mathrm{poly}(n, \lambda, |C|)$ OTs
- ☑ Special properties needed from OTs

How to solve it?

2-round OT extension?

- ☑ $\mathrm{poly}(n, \lambda, |C|)$ OTs
- ☒ Special properties needed from OTs

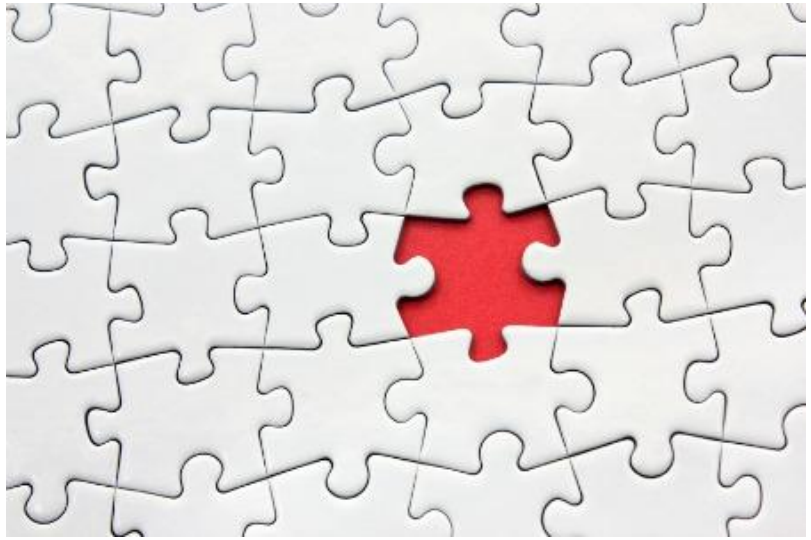
2-round MPC with $\mathrm{poly}(n, \lambda, |C|)$ OTs

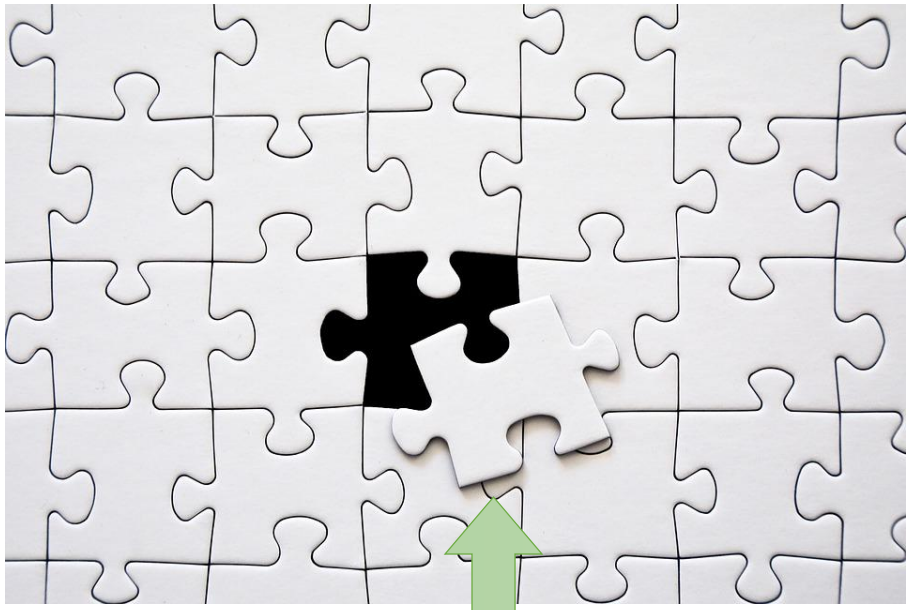
Combine?

No!

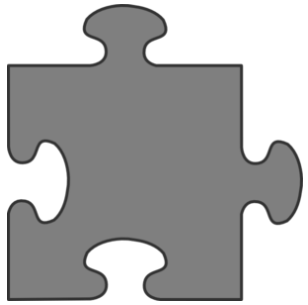
Why?

How to solve it?





2-round OT extension?



2-round MPC with $\mathrm{poly}(n, \lambda, |C|)$ OTs

Combine?

No!

- ☑ $\mathrm{poly}(n, \lambda, |C|)$ OTs
- ☑ Weakened special properties needed from OTs

Why?

How to solve it?

2-round OT extension?

- ☑ $\mathrm{poly}(n, \lambda, |C|)$ OTs
- ☑ Weakened special properties needed from OTs

Technical Overview (semi-honest)

- Building blocks
  - Yao's garbled circuit (symmetric key)
  - two-round OT (public key)

- Two-Round MPC [BL'18, GS'18]
  - What are the special properties needed from OT?
  - Why are they needed?

- Two-Round OT Extension [Beaver'96]
  - Why not satisfying the special properties needed from OT?

- How to solve the problems?

Technical Overview (semi-honest)

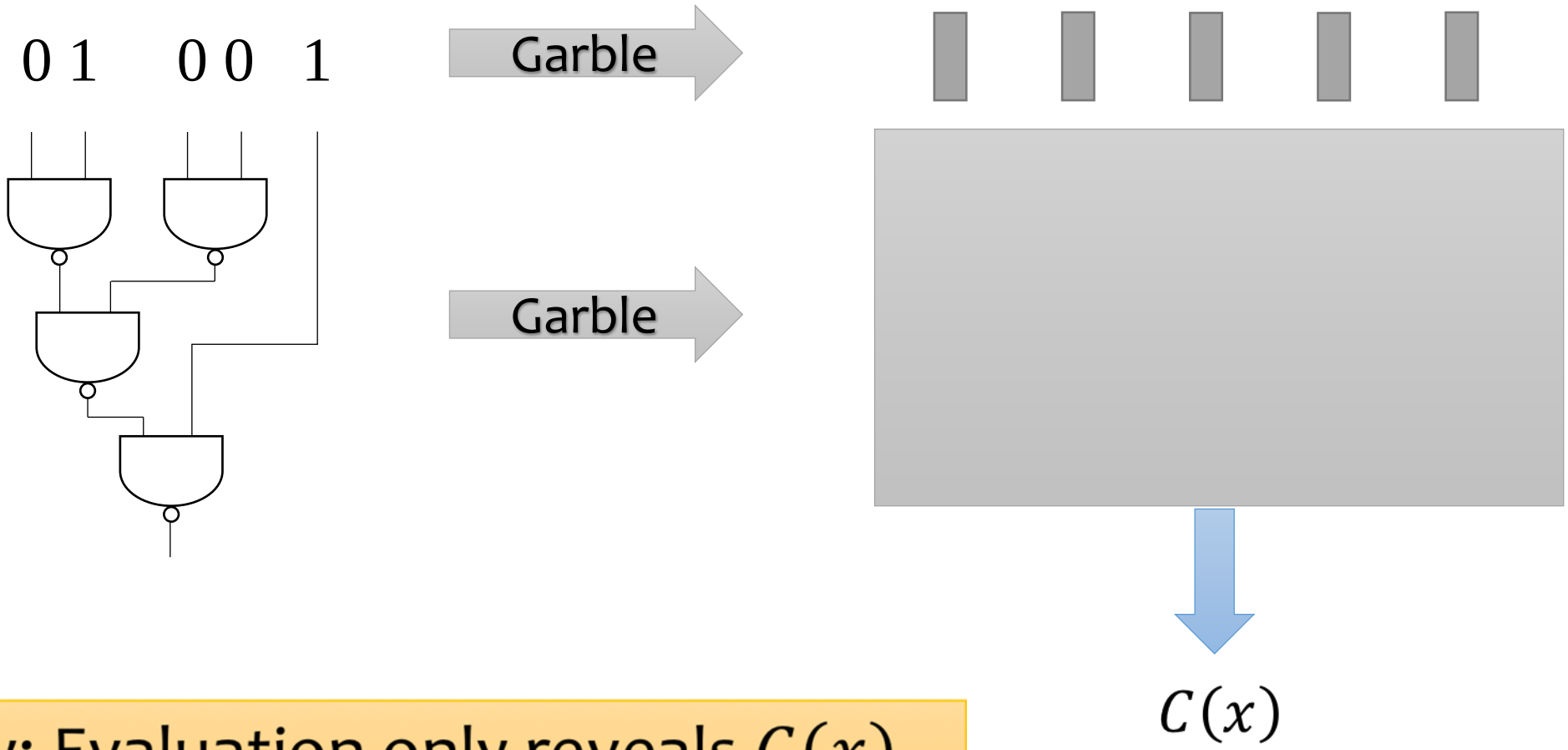
- Building blocks
  - Yao's garbled circuit (symmetric key)
  - two-round OT (public key)

- Two-Round MPC [BL'18, GS'18]
  - What are the special properties needed from OT?
  - Why are they needed?

- Two-Round OT Extension [Beaver'96]
  - Why not satisfying the special properties needed from OT?

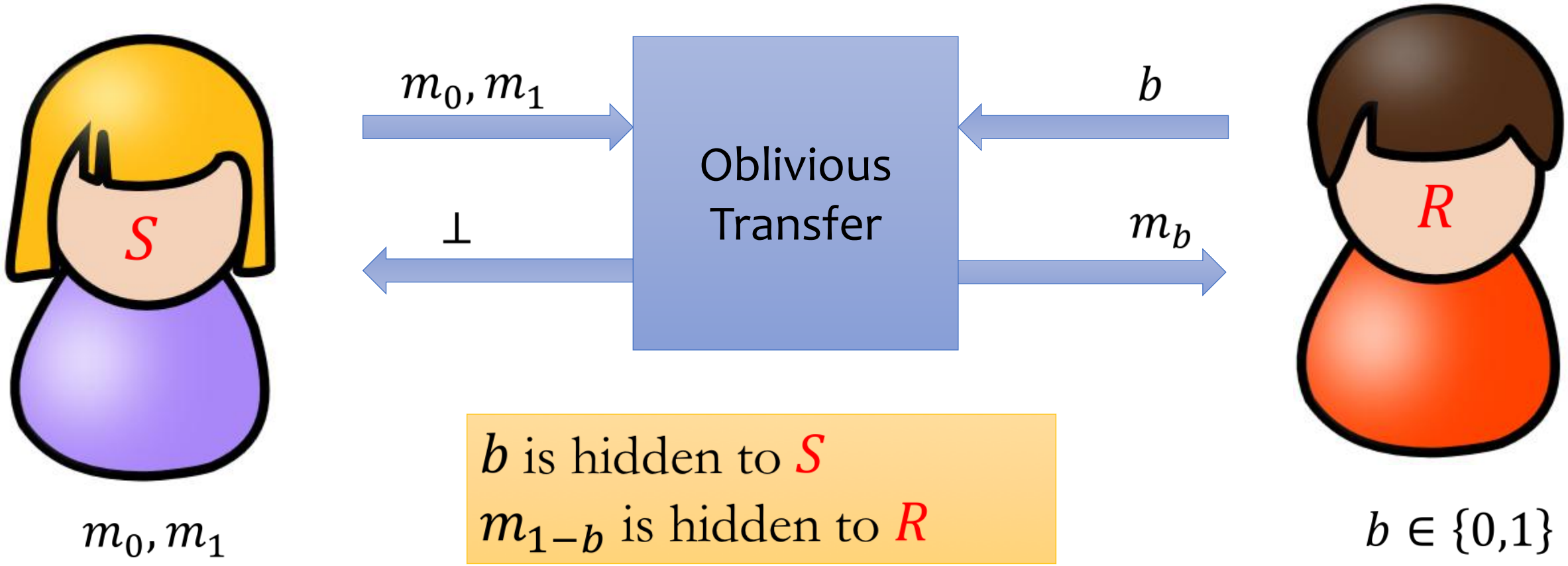
- How to solve the problems?

Yao's garbled circuit [Yao'86]



Security: Evaluation only reveals $C(x)$

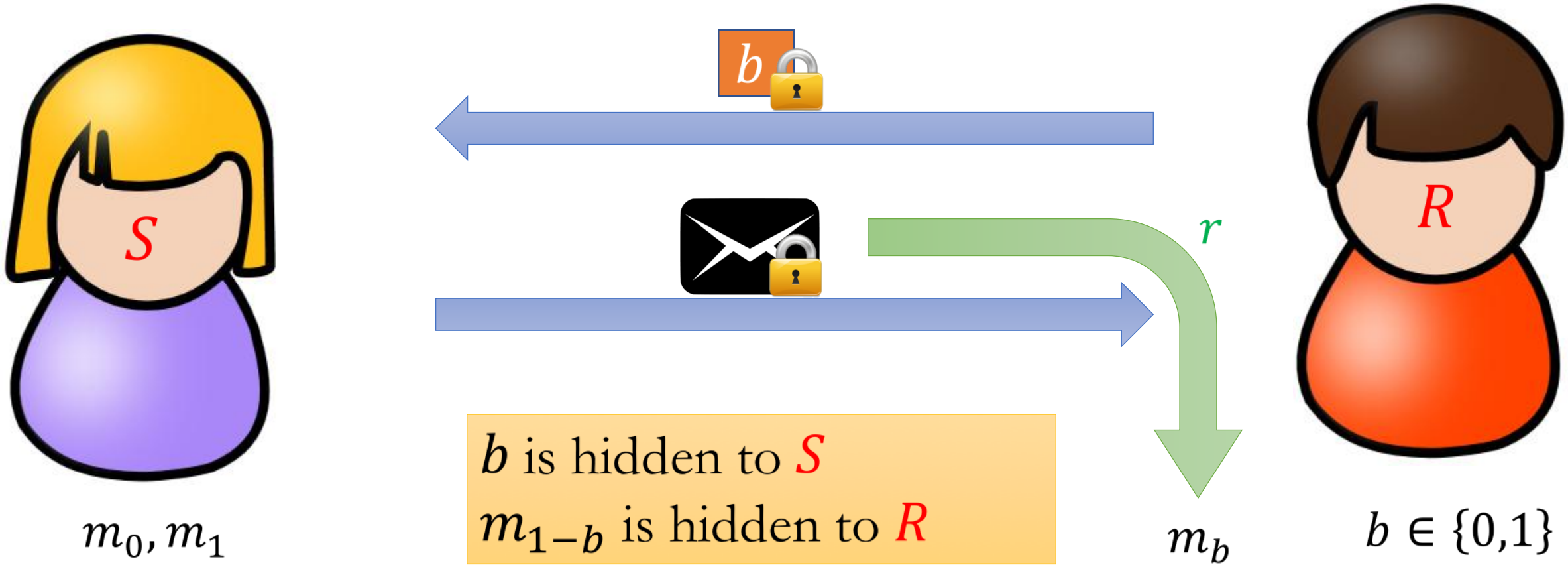
Oblivious Transfer (OT) [Rab'81, EGL'85, BCR'86, Kil'88]



b is hidden to S

m_{1-b} is hidden to R

Two-Round OT [AIR'01, NP'01, HK'12]



Technical Overview (semi-honest)

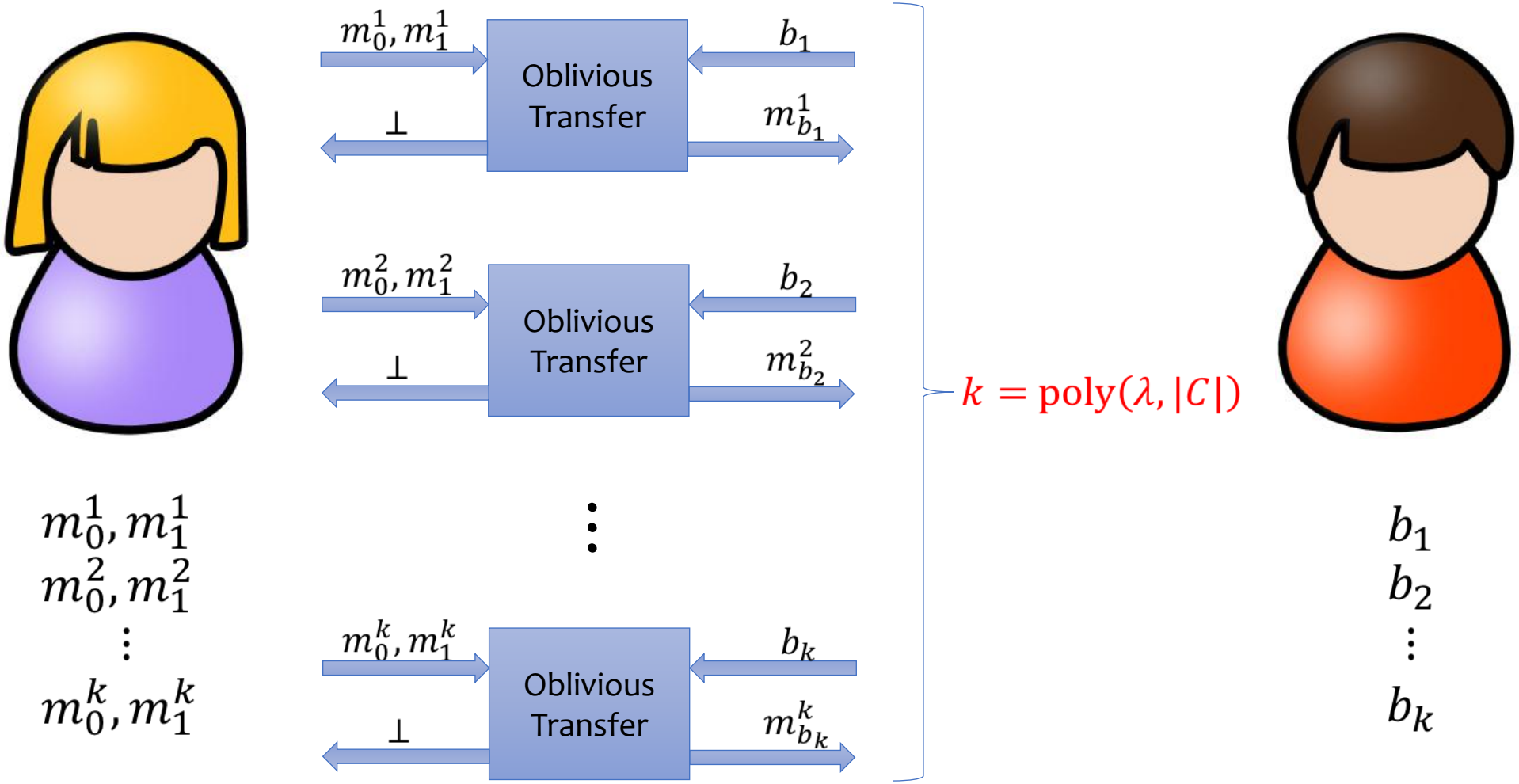
- Building blocks
  - Yao's garbled circuit (symmetric key)
  - two-round OT (public key)

- Two-Round MPC [BL'18, GS'18]
  - What are the special properties needed from OT?
  - Why are they needed?

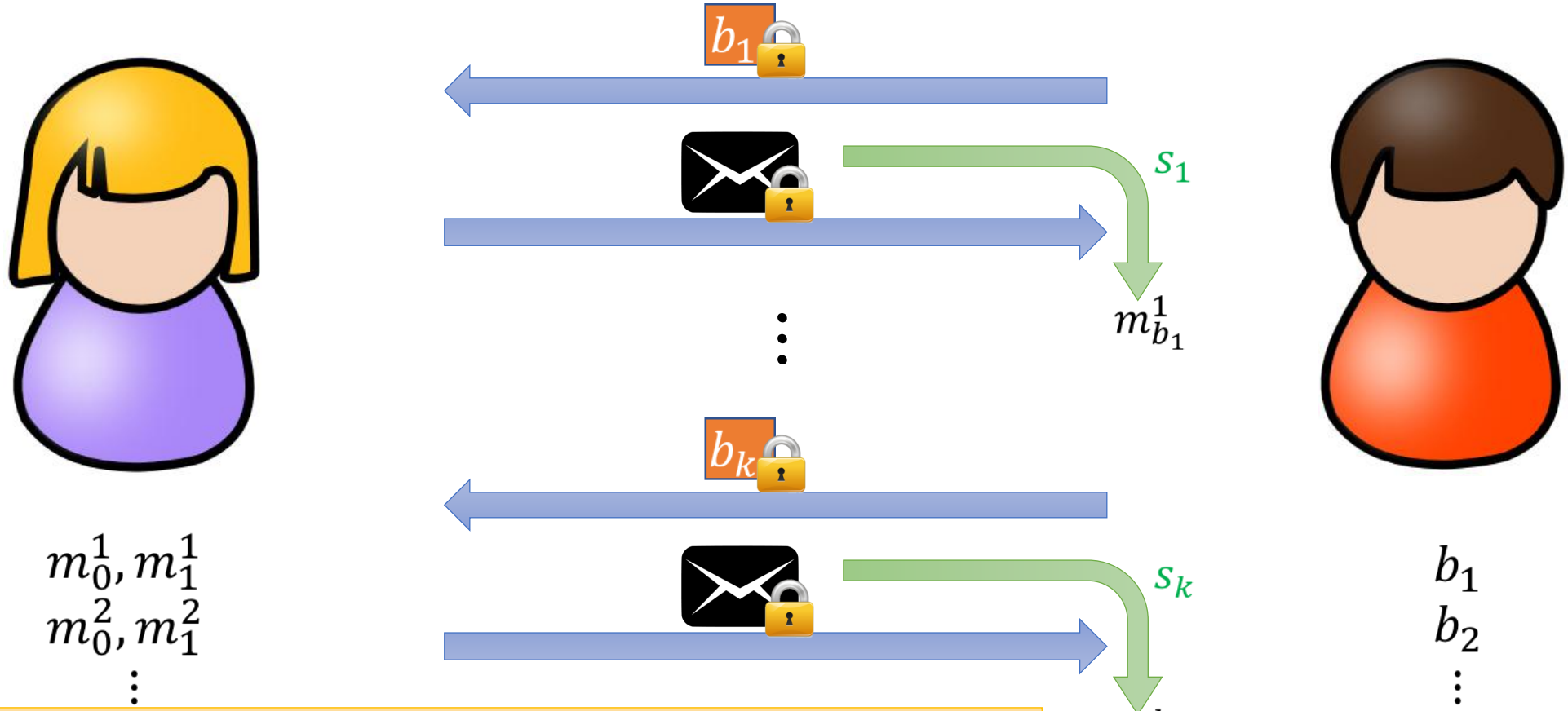
- Two-Round OT Extension [Beaver'96]
  - Why not satisfying the special properties needed from OT?

- How to solve the problems?

Two-Round MPC [BL'18, GS'18]



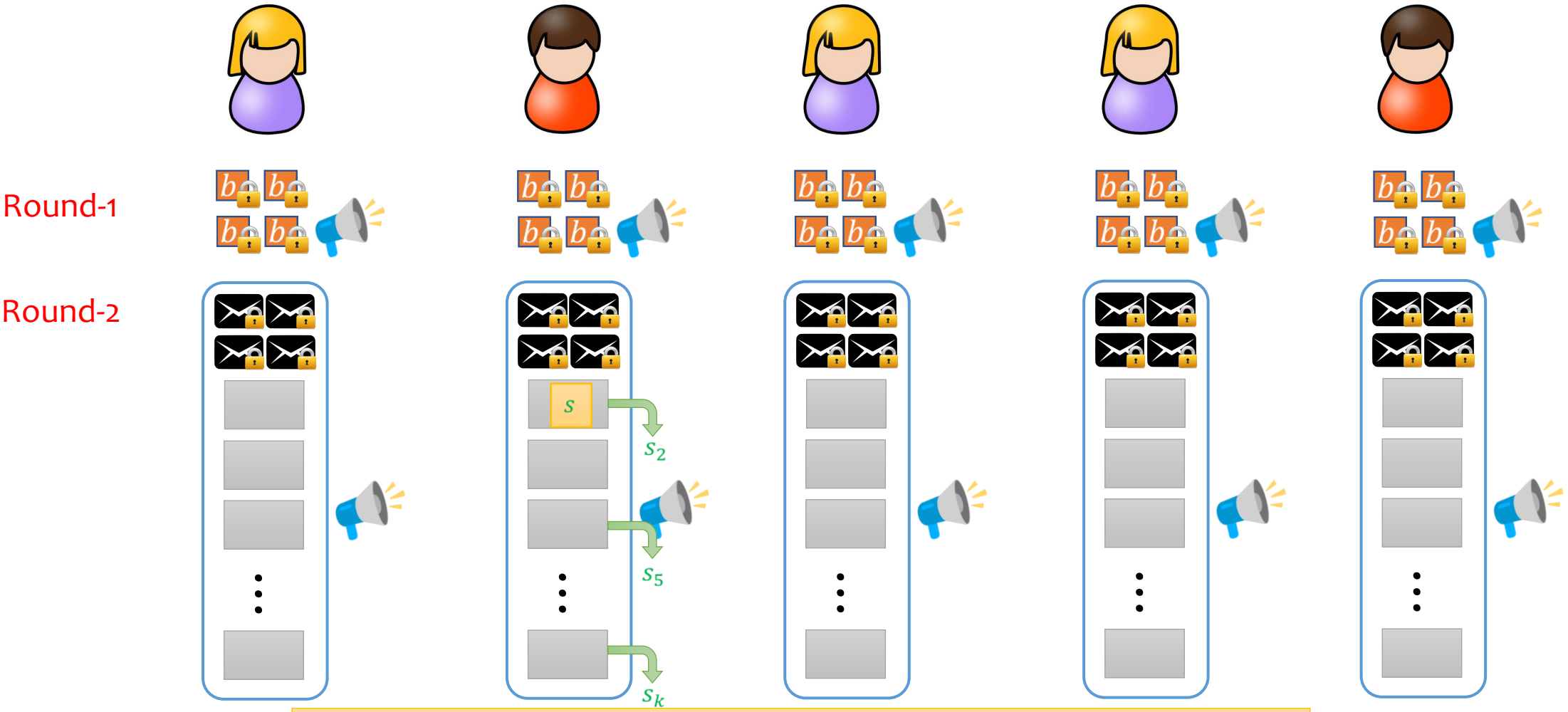
Two-Round MPC [BL'18, GS'18]



- Decryption secrets are known by Receiver before Round-2
- Decryption secrets are independent

Why?

Two-Round MPC [BL'18, GS'18]



- Decryption secrets are known by Receiver before Round-2
- Decryption secrets are independent

Technical Overview (semi-honest)

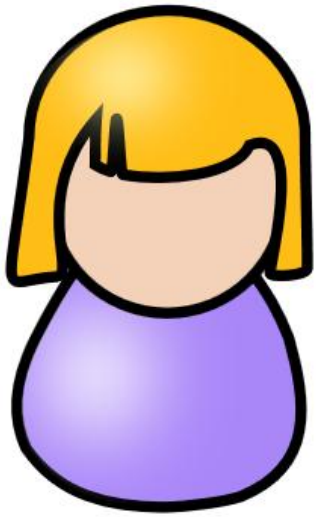
- Building blocks
  - Yao's garbled circuit (symmetric key)
  - two-round OT (public key)

- Two-Round MPC [BL'18, GS'18]
  - What are the special properties needed from OT?
  - Why are they needed?

- Two-Round OT Extension [Beaver'96]
  - Why not satisfying the special properties needed from OT?

- How to solve the problems?

OT Extension [Beaver'96]



m_0^1, m_1^1
m_0^2, m_1^2
$\vdots$
m_0^k, m_1^k

h_0^1, h_1^1 — Oblivious Transfer — c_1 / $\perp$ / $h_{c_1}^1$

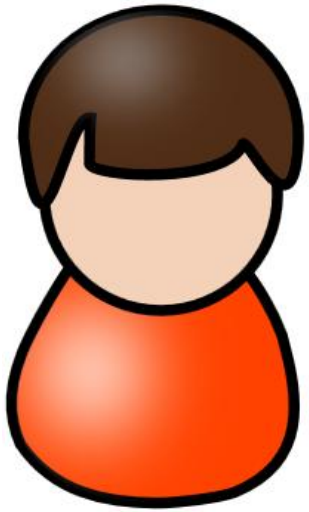
h_0^2, h_1^2 — Oblivious Transfer — c_2 / $\perp$ / $h_{c_2}^2$

$\vdots$

h_0^λ, h_1^λ — Oblivious Transfer — c_λ / $\perp$ / $h_{c_\lambda}^\lambda$

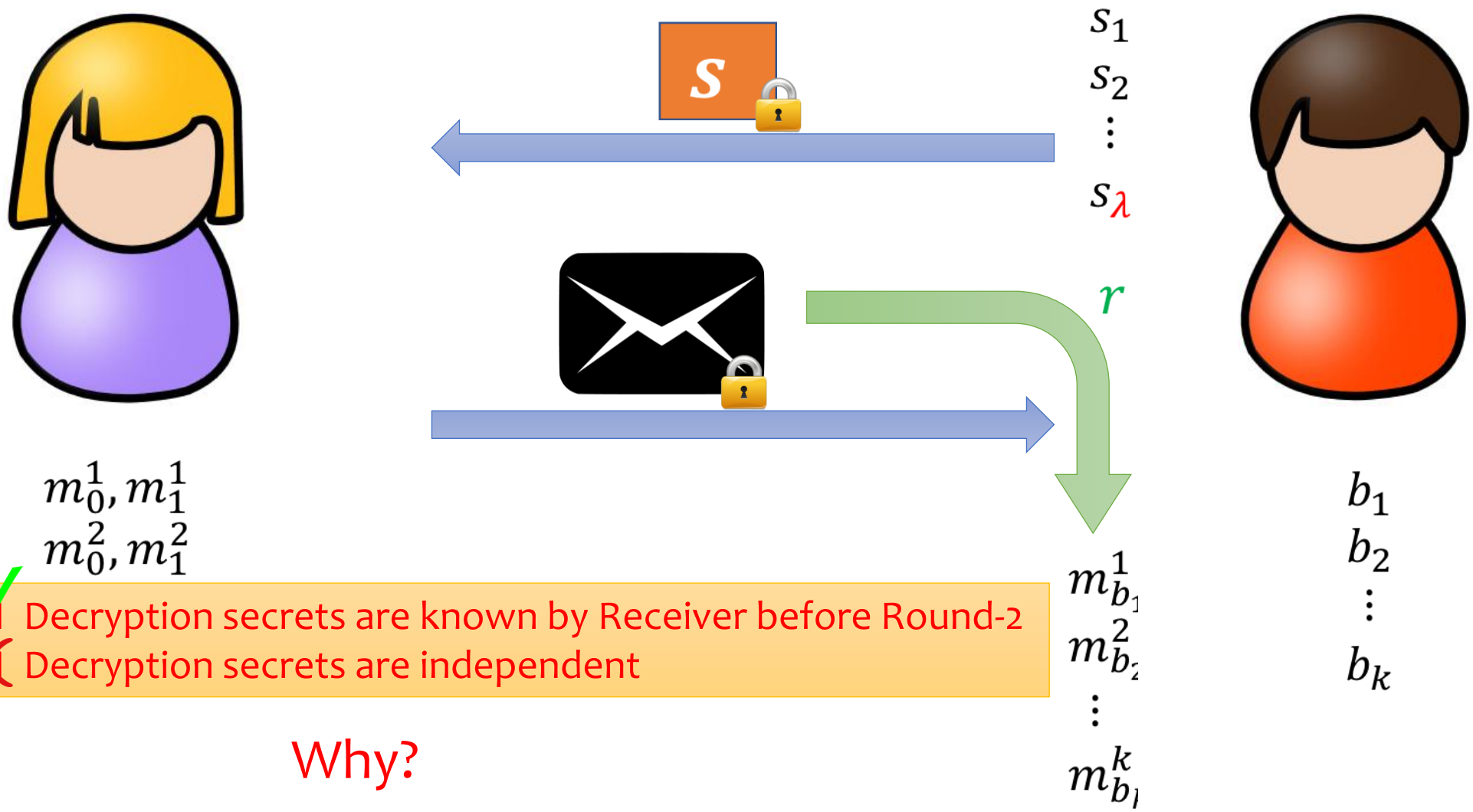
λ

$+\text{poly}(\lambda, |C|)$ symmetric key operations



b_1
b_2
$\vdots$
b_k

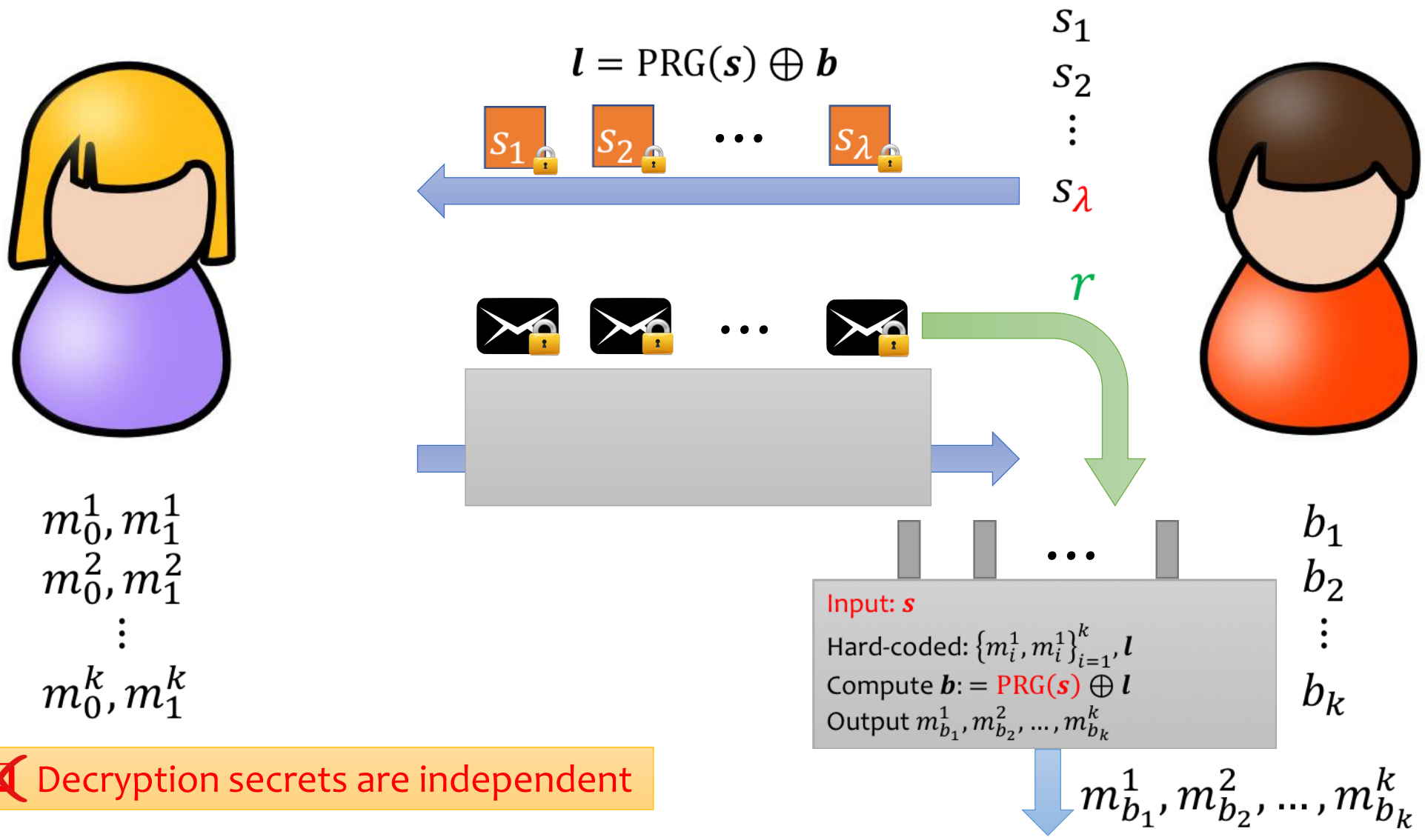
Two-Round OT Extension [Beaver'96]



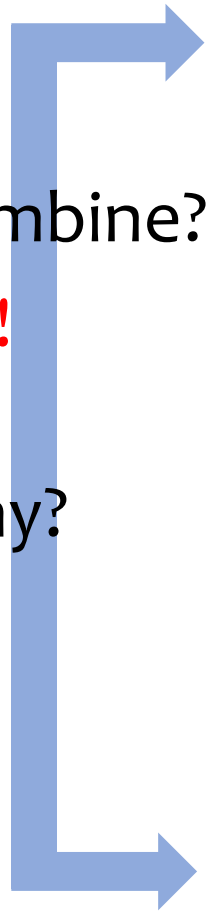
- ☑ Decryption secrets are known by Receiver before Round-2
- ☒ Decryption secrets are independent

Why?

Two-Round OT Extension [Beaver'96]



Decryption secrets are independent



Combine?

No!

Why?

2-round MPC with $\mathrm{poly}(n, \lambda, |C|)$ OTs

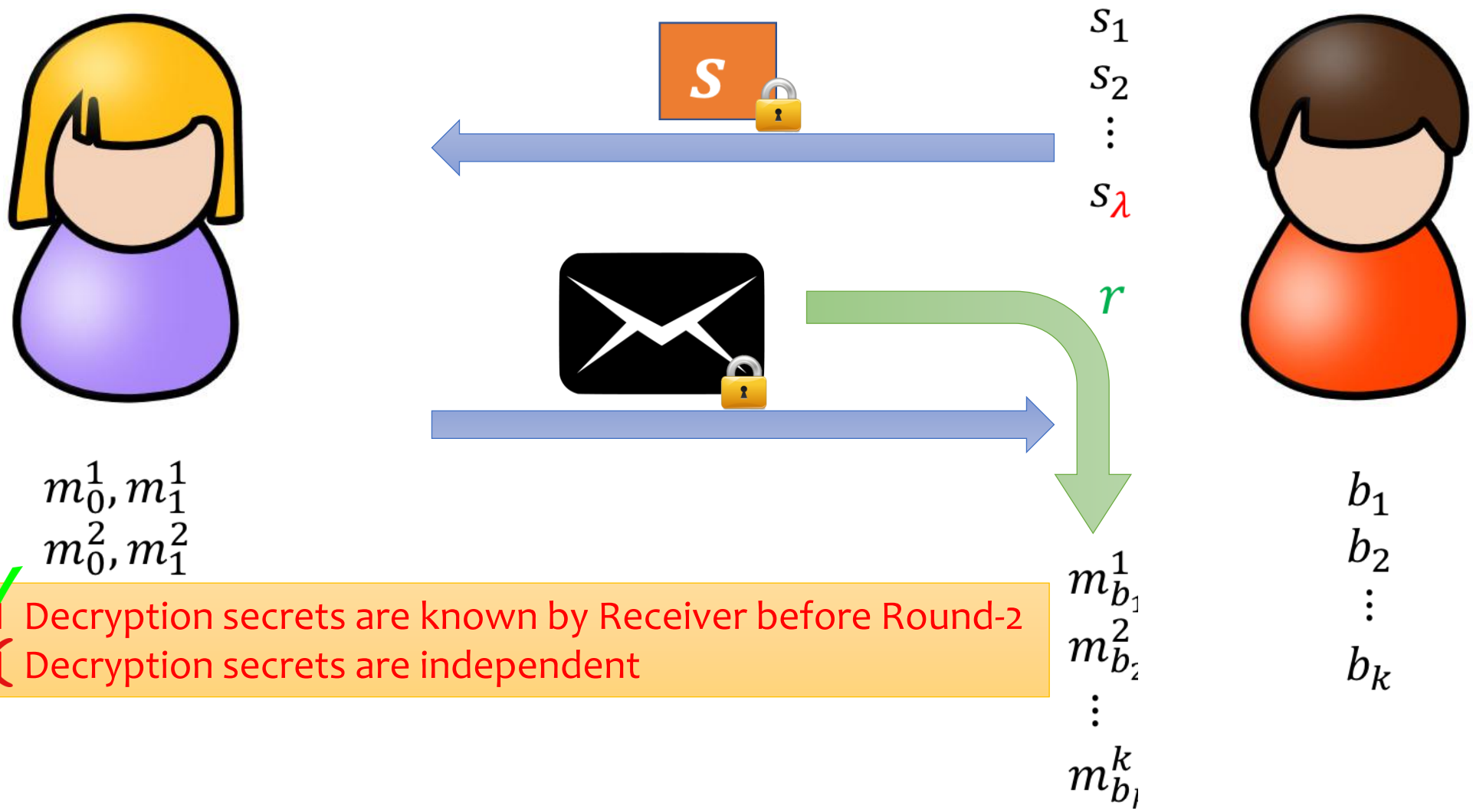
- ☑ $\mathrm{poly}(n, \lambda, |C|)$ OTs
- ☑ Special properties needed from OTs

How to solve it?

2-round OT extension?

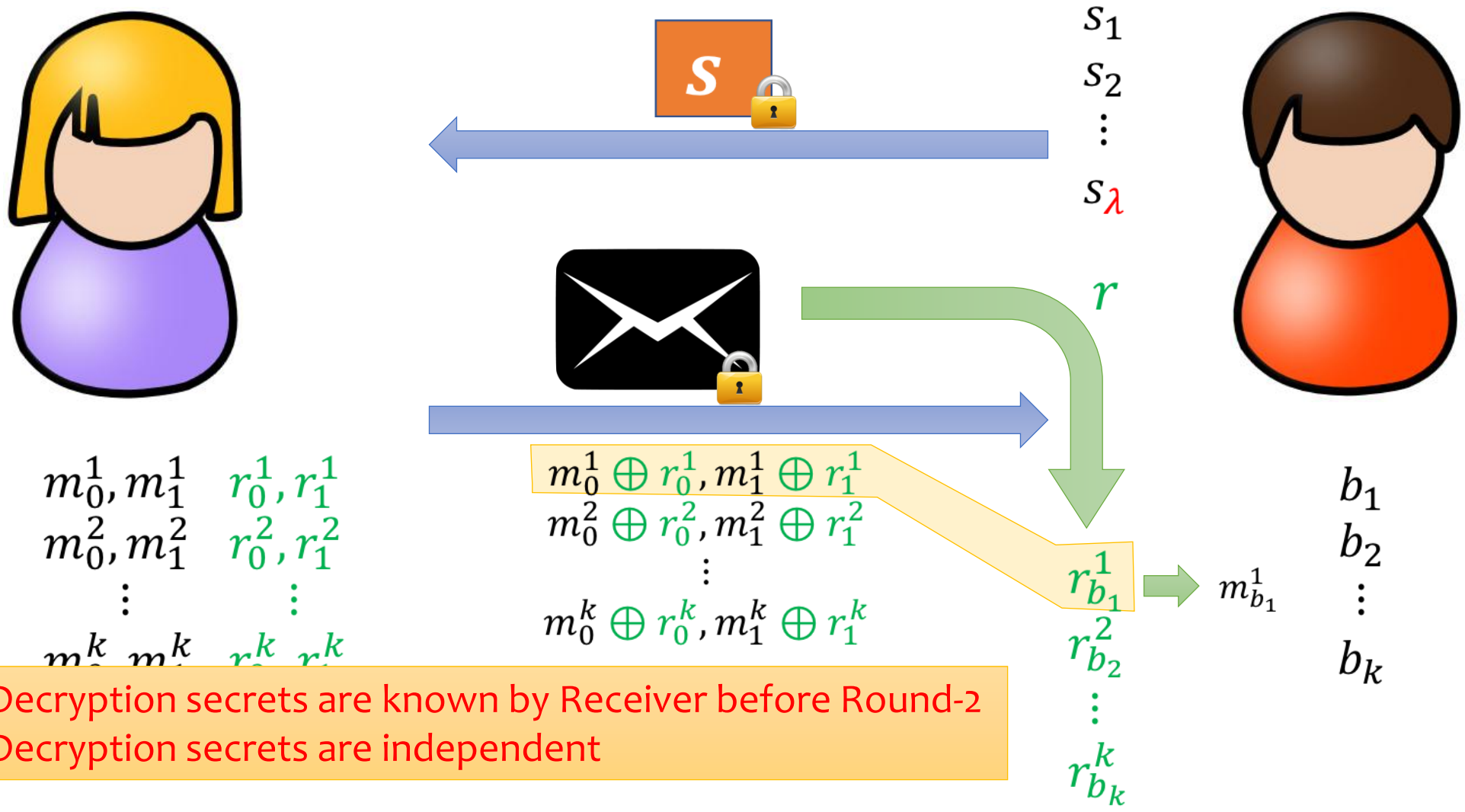
- ☑ $\mathrm{poly}(n, \lambda, |C|)$ OTs
- ☒ Special properties needed from OTs

Two-Round OT Extension [Beaver'96]



- ☑ Decryption secrets are known by Receiver before Round-2
- ☒ Decryption secrets are independent

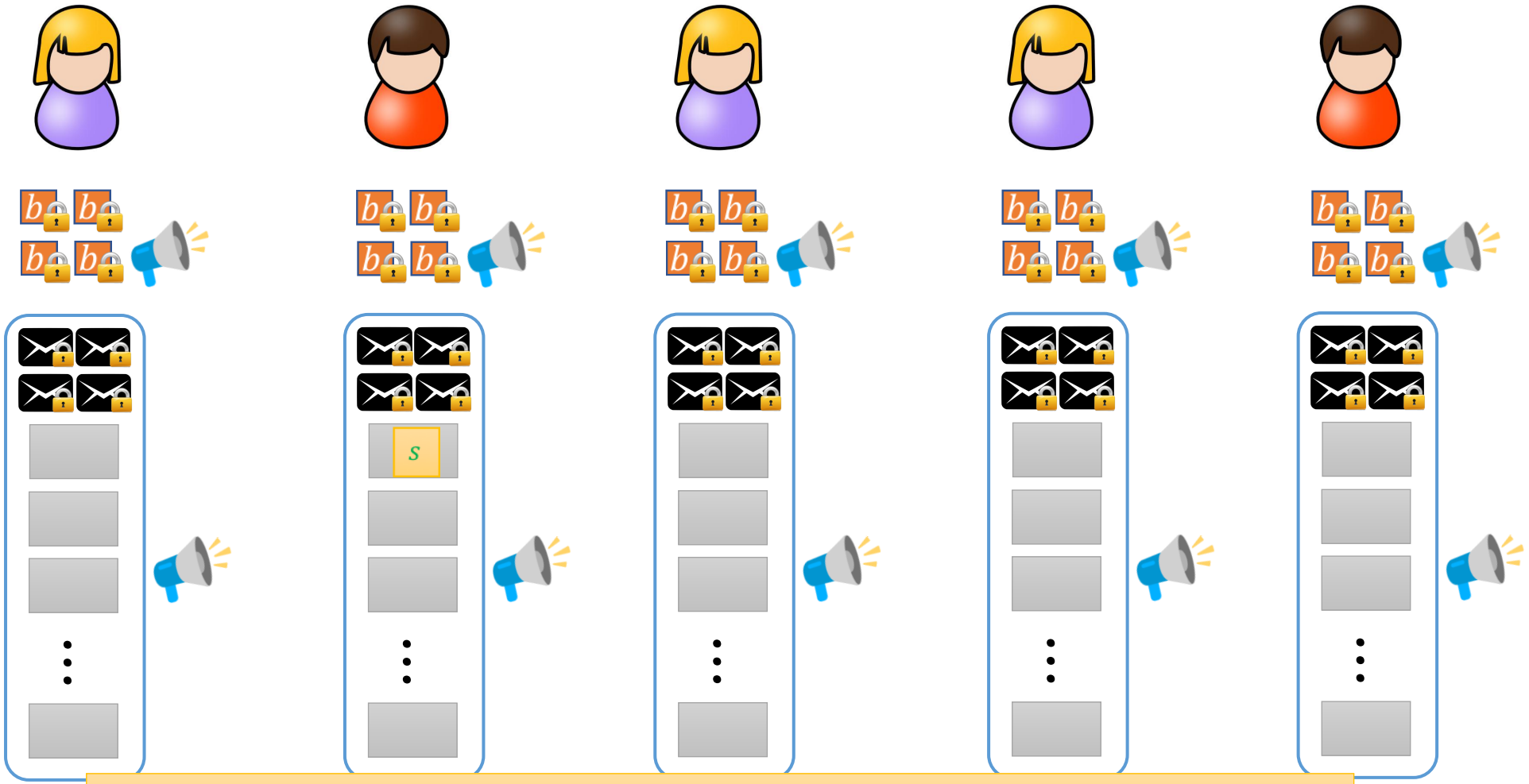
First Attempt: Modify Two-Round OT Extension



☒ Decryption secrets are known by Receiver before Round-2

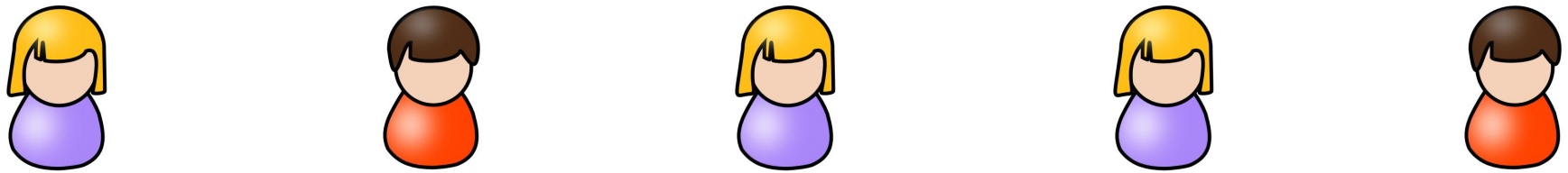
☑ Decryption secrets are independent

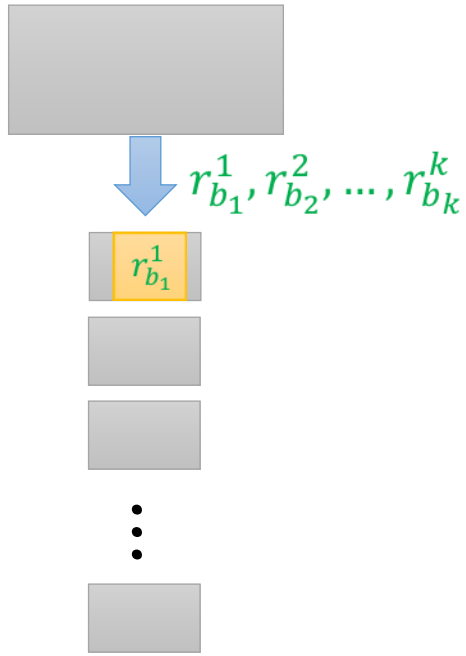
Two-Round MPC [BL'18, GS'18]



~~Decryption secrets are hard-coded in the garbled circuits;~~
~~So they should be known before Round 2!~~

Second Attempt: Weaken Special Properties





Weakened property: Decryption secrets can be computed and fed into the garbled circuits after Round-2.

Summary

- What did we achieve?
  - 2-round MPC from 2-round OT using $\mathrm{poly}(n, \lambda)$ OTs (public key operations) + $\mathrm{poly}(n, \lambda, |C|)$ symmetric key operations
- Combine 2-round MPC with 2-round OT extension
  - Mismatch in the special properties!
  - Weaken special properties and modify protocols
- More challenges and new tools in malicious setting
  - Somewhere Adaptive Garbled Circuit
  - Special Purpose Zero-Knowledge Proof

Future Work

- How to make it more practical?

- Making black-box use of crypto operations?
- Impossible for 2 rounds! [GMMM'18] talk tomorrow morning :)
- Black-box but 3 rounds?
  - Combining with black-box OT extension [IKNP'03]

- Concrete optimization for implementation

Thanks!