Round-Optimal Black-Box Multiparty Computation from Polynomial-Time Assumptions

Michele Ciampi

The University of Edinburgh

Rafail Ostrovsky

University of California, Los Angeles

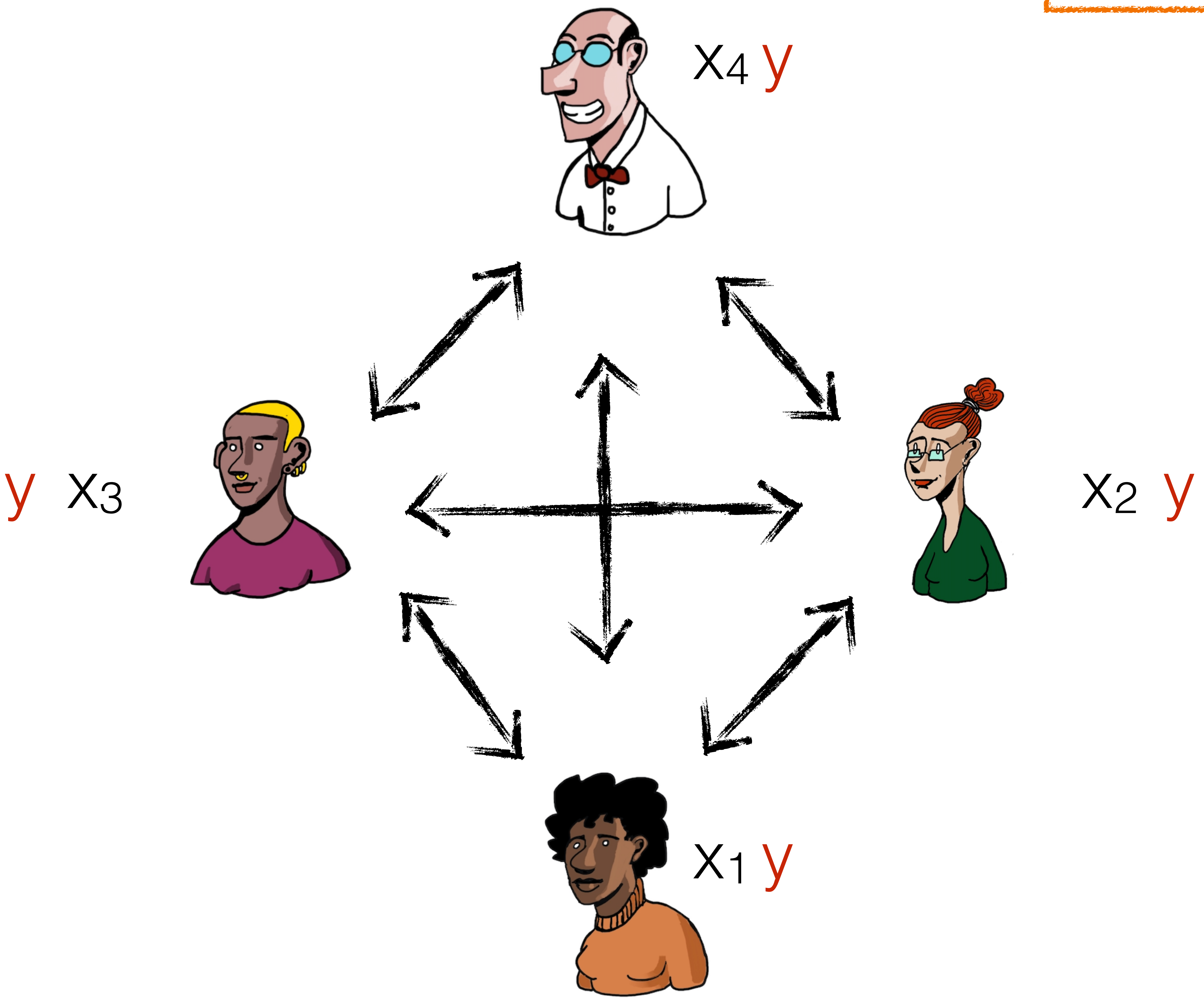
Luisa Siniscalchi

Technical University of Denmark

Hendrik Waldner

Multi-Party Computation (MPC)

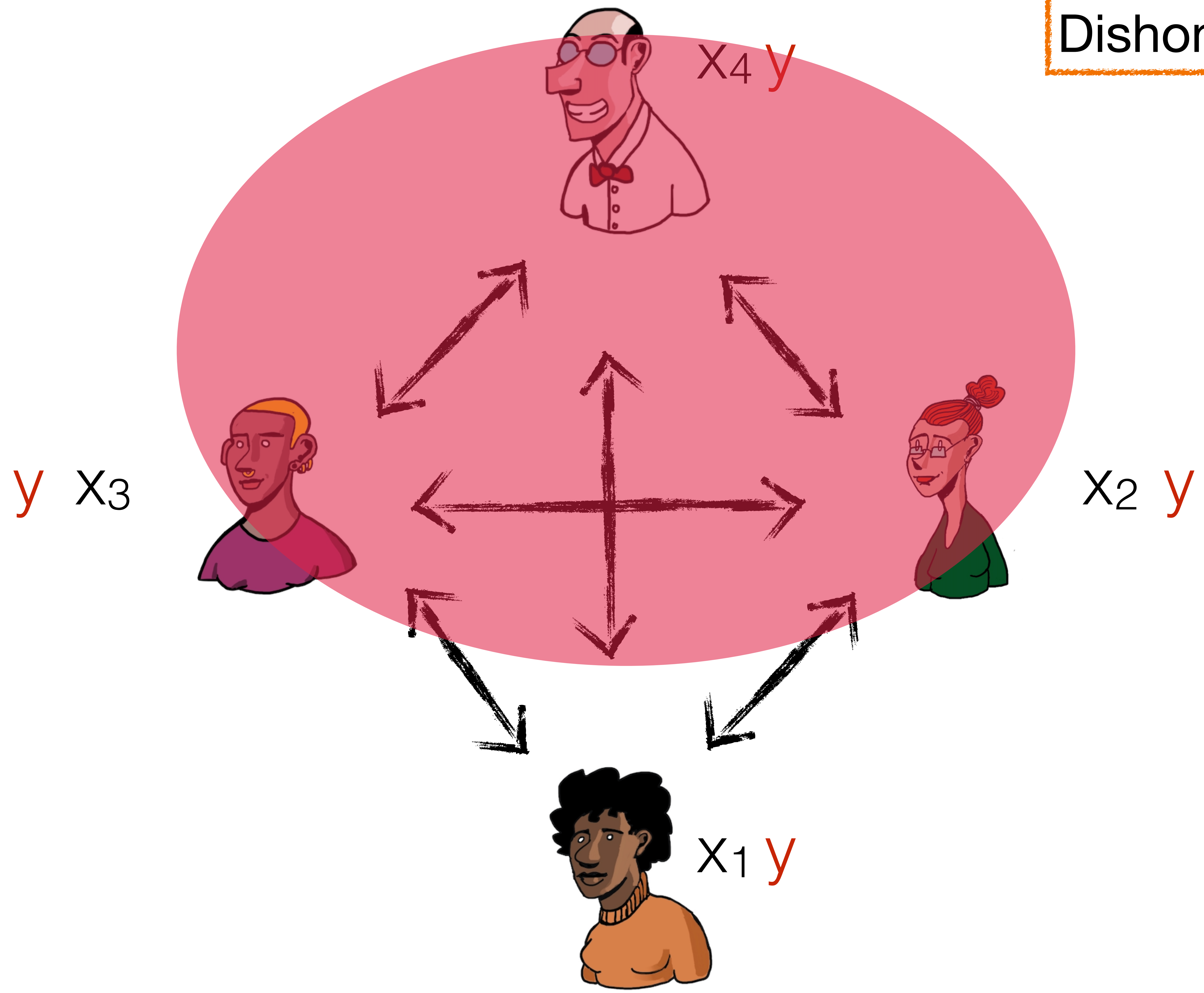
Plain model (no RO, no setup)



$y=f(x_1,x_2,x_3,x_4)$

Multi-Party Computation (MPC)

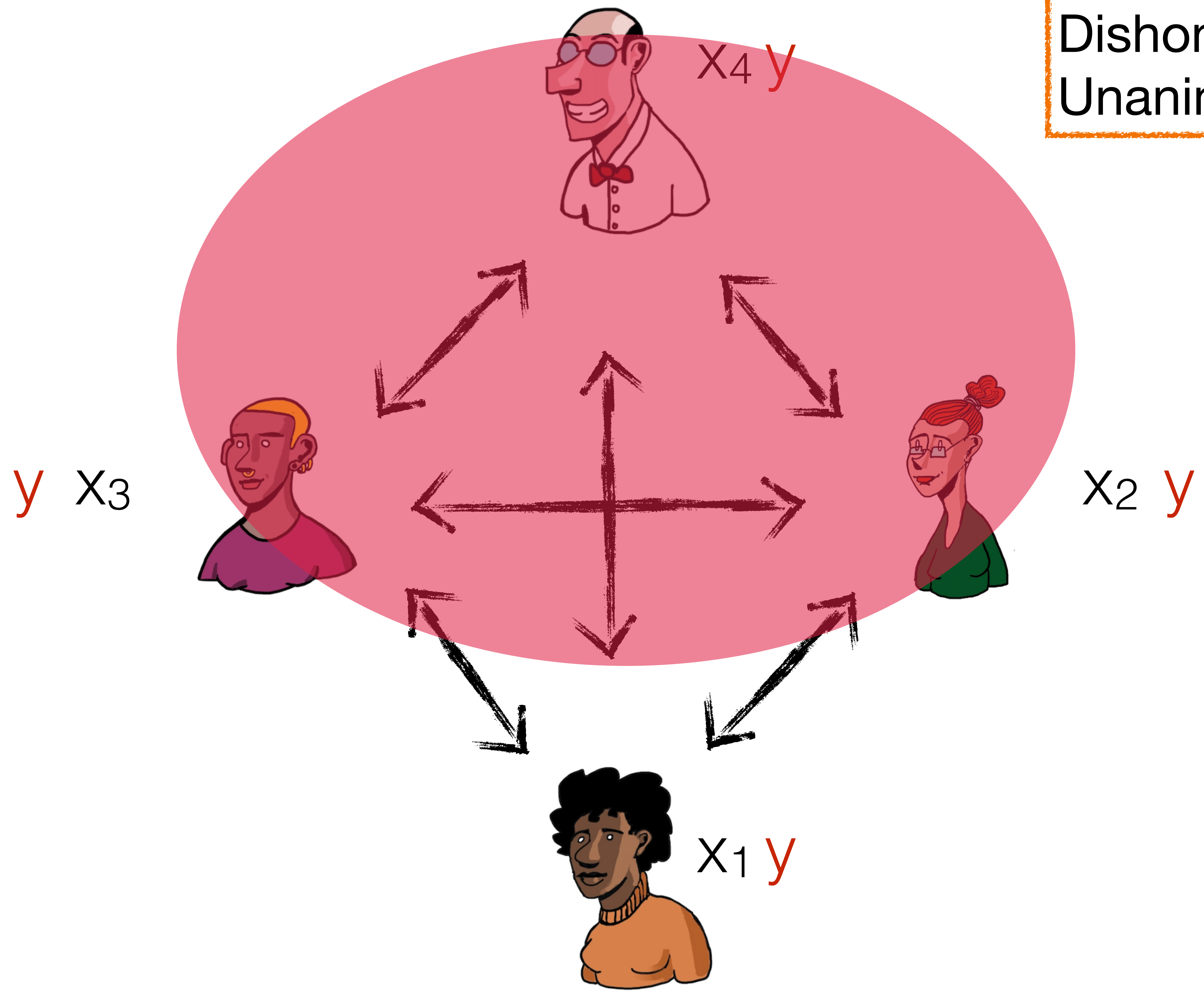
Plain model (no RO, no setup)
Dishonest majority



$y=f(x_1,x_2,x_3,x_4)$

Multi-Party Computation (MPC)

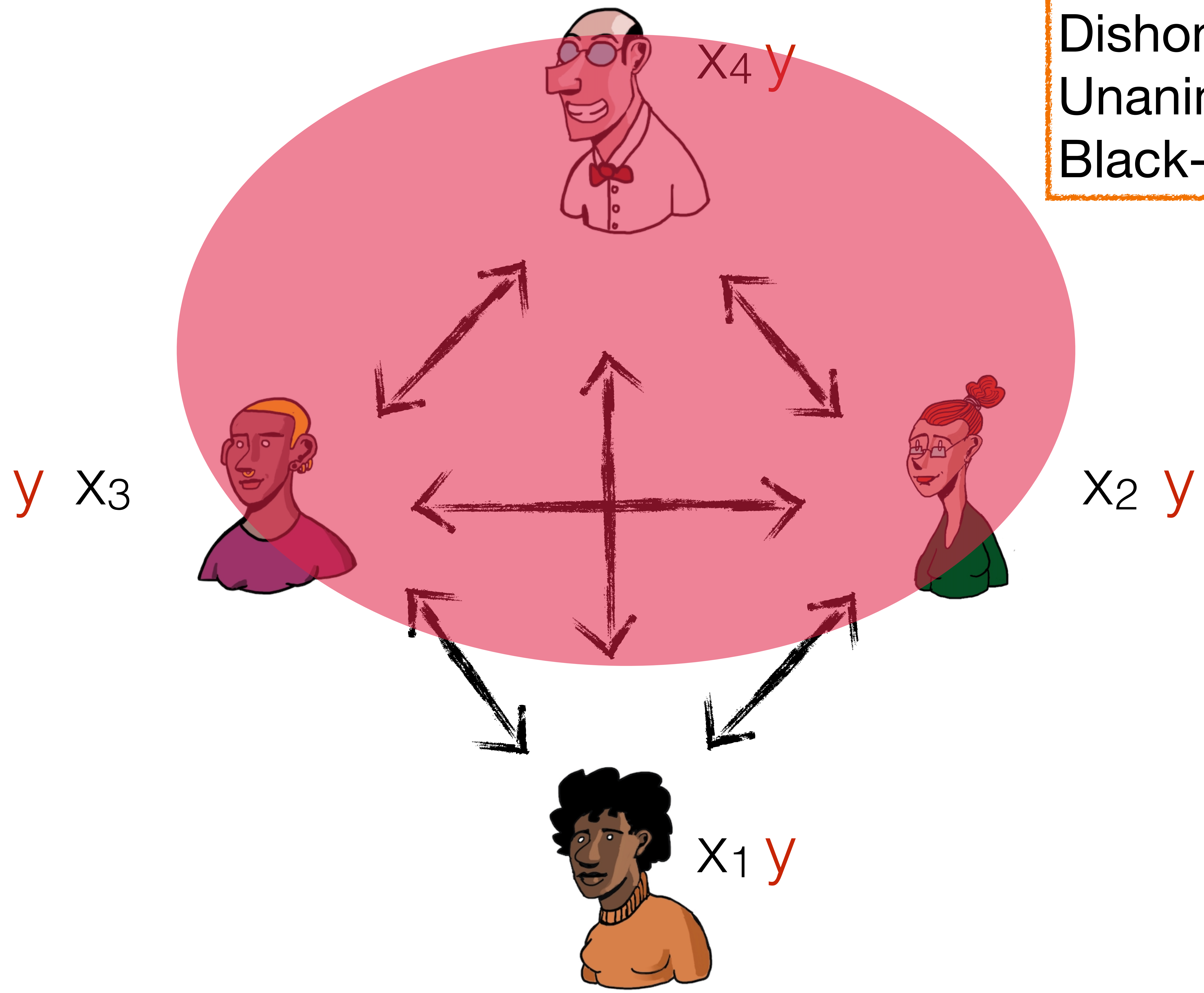
Plain model (no RO, no setup)
Dishonest majority
Unanimous abort



$y=f(x_1,x_2,x_3,x_4)$

Multi-Party Computation (MPC)

Plain model (no RO, no setup)
Dishonest majority
Unanimous abort
Black-box simulation



$y=f(x_1,x_2,x_3,x_4)$

Multi-Party Computation (MPC)

Plain model (no RO, no setup)
Dishonest majority
Unanimous abort
Black-box simulation

Multi-Party Computation (MPC)

Plain model (no RO, no setup)
Dishonest majority
Unanimous abort
Black-box simulation

What is the exact round complexity?

The State of the Art on Round Optimal MPC

Plain model
Dishonest majority
Unanimous abort
Black-box simulation

Optimal round complexity: 4-round [GK90, KO04, GMPP16]

[GK90] O. Goldreich and H. Krawczyk. On the Composition of Zero-Knowledge Proof Systems. In SIAM J. Computing 1990
[KO04]J. Katz and R. Ostrovsky. Round-optimal secure two-party computation. In CRYPTO 2004.
[GMPP16] S. Garg, P. Mukherjee, O. Pandey, and A. Polychroniadou. The exact round complexity of secure computation. In EUROCRYPT 2016.

The State of the Art on Round Optimal MPC

Optimal round complexity: 4-round [GK90, KO04, GMPP16]

Plain model
Dishonest majority
Unanimous abort
Black-box simulation

. . .

[BGJ+18]
[HHPV18]

4 ROUND
Num. ass.

[CCG+20]

4 ROUND
OT

[GK90] O. Goldreich and H. Krawczyk. On the Composition of Zero-Knowledge Proof Systems. In SIAM J. Computing 1990
[KO04]J. Katz and R. Ostrovsky. Round-optimal secure two-party computation. In CRYPTO 2004.
[GMPP16] S. Garg, P. Mukherjee, O. Pandey, and A. Polychroniadou. The exact round complexity of secure computation. In EUROCRYPT 2016.
[HHPV18]. S. Halevi, C. Hazay, A. Polychroniadou, and M. Venkitasubramaniam. Round-optimal secure multi-party computation. In CRYPTO 2018.
[BGJ+18] S. Badrinarayanan, V. Goyal, A. Jain, Y. T. Kalai, D. Khurana, and A. Sahai. Promise zero knowledge and its applications to round optimal MPC. In CRYPTO 2018.
[CCG+20] A. R. Choudhuri, M. Ciampi, V. Goyal, A. Jain, and R. Ostrovsky. Round optimal secure multiparty computation from minimal assumptions. In TCC 2020.

The State of the Art on Round Optimal MPC

Optimal round complexity: 4-round [GK90, KO04, GMPP16]

Plain model
Dishonest majority
Unanimous abort
Black-box simulation

[GK90] O. Goldreich and H. Krawczyk. On the Composition of Zero-Knowledge Proof Systems. In SIAM J. Computing 1990
[KO04]J. Katz and R. Ostrovsky. Round-optimal secure two-party computation. In CRYPTO 2004.
[GMPP16] S. Garg, P. Mukherjee, O. Pandey, and A. Polychroniadou. The exact round complexity of secure computation. In EUROCRYPT 2016.
[HHPV18]. S. Halevi, C. Hazay, A. Polychroniadou, and M. Venkitasubramaniam. Round-optimal secure multi-party computation. In CRYPTO 2018.
[BGJ+18] S. Badrinarayanan, V. Goyal, A. Jain, Y. T. Kalai, D. Khurana, and A. Sahai. Promise zero knowledge and its applications to round optimal MPC. In CRYPTO 2018.
[CCG+20] A. R. Choudhuri, M. Ciampi, V. Goyal, A. Jain, and R. Ostrovsky. Round optimal secure multiparty computation from minimal assumptions. In TCC 2020.

The State of the Art on Round Optimal MPC

Optimal round complexity: 4-round [GK90, KO04, GMPP16]

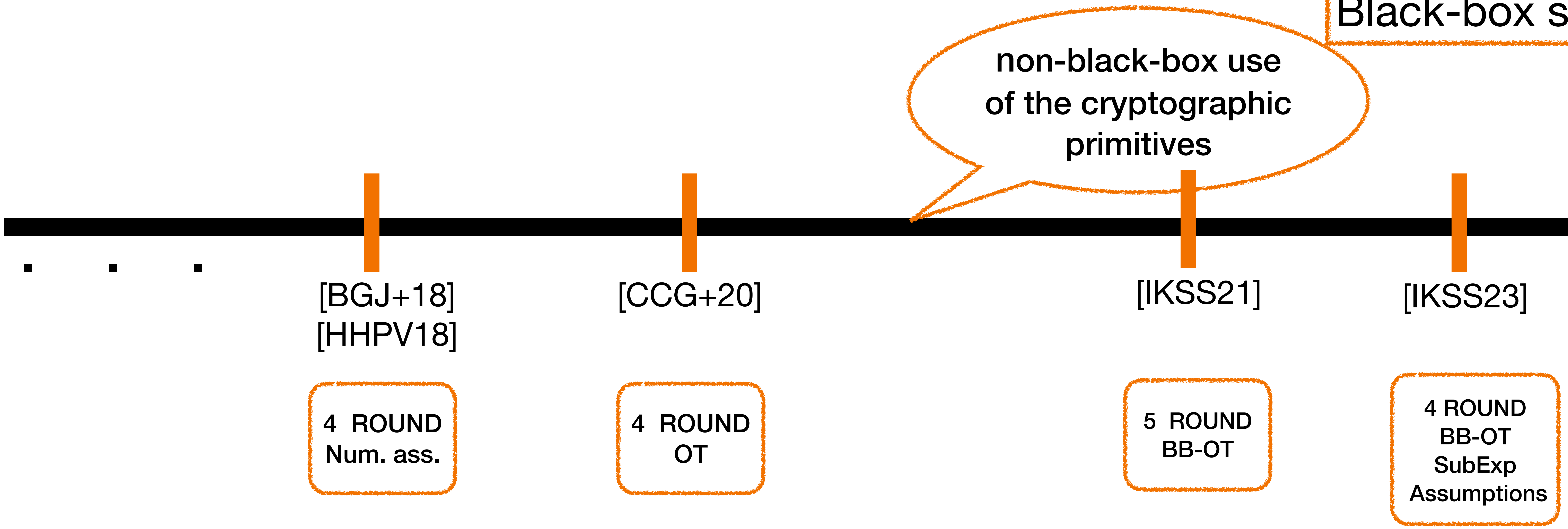
Plain model
Dishonest majority
Unanimous abort
Black-box simulation

[GK90] O. Goldreich and H. Krawczyk. On the Composition of Zero-Knowledge Proof Systems. In SIAM J. Computing 1990
[KO04]J. Katz and R. Ostrovsky. Round-optimal secure two-party computation. In CRYPTO 2004.
[GMPP16] S. Garg, P. Mukherjee, O. Pandey, and A. Polychroniadou. The exact round complexity of secure computation. In EUROCRYPT 2016.
[HHPV18]. S. Halevi, C. Hazay, A. Polychroniadou, and M. Venkitasubramaniam. Round-optimal secure multi-party computation. In CRYPTO 2018.
[BGJ+18] S. Badrinarayanan, V. Goyal, A. Jain, Y. T. Kalai, D. Khurana, and A. Sahai. Promise zero knowledge and its applications to round optimal MPC. In CRYPTO 2018.
[CCG+20] A. R. Choudhuri, M. Ciampi, V. Goyal, A. Jain, and R. Ostrovsky. Round optimal secure multiparty computation from minimal assumptions. In TCC 2020.
[IKSS21] Y. Ishai, D. Khurana, A. Sahai, and A. Srinivasan. On the round complexity of black-box secure MPC. In CRYPTO 2021.
[IKSS23] Y. Ishai, D. Khurana, A. Sahai, and A. Srinivasan. Round-optimal black-box MPC in the plain model. In CRYPTO 2023
[COSW23] M. Ciampi, R. Ostrovsky, L. Siniscalchi, and H. Waldner. List oblivious transfer and applications to round-optimal black-box multiparty coin tossing.CRYPTO2023.

The State of the Art on Round Optimal MPC

Optimal round complexity: 4-round [GK90, KO04, GMPP16]

Plain model
Dishonest majority
Unanimous abort
Black-box simulation



[GK90] O. Goldreich and H. Krawczyk. On the Composition of Zero-Knowledge Proof Systems. In SIAM J. Computing 1990
[KO04]J. Katz and R. Ostrovsky. Round-optimal secure two-party computation. In CRYPTO 2004.
[GMPP16] S. Garg, P. Mukherjee, O. Pandey, and A. Polychroniadou. The exact round complexity of secure computation. In EUROCRYPT 2016.
[HHPV18]. S. Halevi, C. Hazay, A. Polychroniadou, and M. Venkitasubramaniam. Round-optimal secure multi-party computation. In CRYPTO 2018.
[BGJ+18] S. Badrinarayanan, V. Goyal, A. Jain, Y. T. Kalai, D. Khurana, and A. Sahai. Promise zero knowledge and its applications to round optimal MPC. In CRYPTO 2018.
[CCG+20] A. R. Choudhuri, M. Ciampi, V. Goyal, A. Jain, and R. Ostrovsky. Round optimal secure multiparty computation from minimal assumptions. In TCC 2020.
[IKSS21] Y. Ishai, D. Khurana, A. Sahai, and A. Srinivasan. On the round complexity of black-box secure MPC. In CRYPTO 2021.
[IKSS23] Y. Ishai, D. Khurana, A. Sahai, and A. Srinivasan. Round-optimal black-box MPC in the plain model. In CRYPTO 2023
[COSW23] M. Ciampi, R. Ostrovsky, L. Siniscalchi, and H. Waldner. List oblivious transfer and applications to round-optimal black-box multiparty coin tossing.CRYPTO2023.

The State of the Art on Round Optimal MPC

Optimal round complexity: 4-round [GK90, KO04, GMPP16]

Plain model
Dishonest majority
Unanimous abort
Black-box simulation

non-black-box use of the cryptographic primitives

. . .

[BGJ+18]
[HHPV18]

4 ROUND
Num. ass.

[CCG+20]

4 ROUND
OT

[IKSS21]

5 ROUND
BB-OT

[IKSS23]

4 ROUND
BB-OT
SubExp
Assumptions

[COSW23]

4 ROUND
BB-OT
Inputless-functionalities

[GK90] O. Goldreich and H. Krawczyk. On the Composition of Zero-Knowledge Proof Systems. In SIAM J. Computing 1990
[KO04]J. Katz and R. Ostrovsky. Round-optimal secure two-party computation. In CRYPTO 2004.
[GMPP16] S. Garg, P. Mukherjee, O. Pandey, and A. Polychroniadou. The exact round complexity of secure computation. In EUROCRYPT 2016.
[HHPV18]. S. Halevi, C. Hazay, A. Polychroniadou, and M. Venkitasubramaniam. Round-optimal secure multi-party computation. In CRYPTO 2018.
[BGJ+18] S. Badrinarayanan, V. Goyal, A. Jain, Y. T. Kalai, D. Khurana, and A. Sahai. Promise zero knowledge and its applications to round optimal MPC. In CRYPTO 2018.
[CCG+20] A. R. Choudhuri, M. Ciampi, V. Goyal, A. Jain, and R. Ostrovsky. Round optimal secure multiparty computation from minimal assumptions. In TCC 2020.
[IKSS21] Y. Ishai, D. Khurana, A. Sahai, and A. Srinivasan. On the round complexity of black-box secure MPC. In CRYPTO 2021.
[IKSS23] Y. Ishai, D. Khurana, A. Sahai, and A. Srinivasan. Round-optimal black-box MPC in the plain model. In CRYPTO 2023
[COSW23] M. Ciampi, R. Ostrovsky, L. Siniscalchi, and H. Waldner. List oblivious transfer and applications to round-optimal black-box multiparty coin tossing.CRYPTO2023.

The State of the Art on Round Optimal MPC

Optimal round complexity: 4-round [GK90, KO04, GMPP16]

Plain model
Dishonest majority
Unanimous abort
Black-box simulation

[GK90] O. Goldreich and H. Krawczyk. On the Composition of Zero-Knowledge Proof Systems. In SIAM J. Computing 1990
[KO04]J. Katz and R. Ostrovsky. Round-optimal secure two-party computation. In CRYPTO 2004.
[GMPP16] S. Garg, P. Mukherjee, O. Pandey, and A. Polychroniadou. The exact round complexity of secure computation. In EUROCRYPT 2016.
[HHPV18]. S. Halevi, C. Hazay, A. Polychroniadou, and M. Venkitasubramaniam. Round-optimal secure multi-party computation. In CRYPTO 2018.
[BGJ+18] S. Badrinarayanan, V. Goyal, A. Jain, Y. T. Kalai, D. Khurana, and A. Sahai. Promise zero knowledge and its applications to round optimal MPC. In CRYPTO 2018.
[CCG+20] A. R. Choudhuri, M. Ciampi, V. Goyal, A. Jain, and R. Ostrovsky. Round optimal secure multiparty computation from minimal assumptions. In TCC 2020.
[IKSS21] Y. Ishai, D. Khurana, A. Sahai, and A. Srinivasan. On the round complexity of black-box secure MPC. In CRYPTO 2021.
[IKSS23] Y. Ishai, D. Khurana, A. Sahai, and A. Srinivasan. Round-optimal black-box MPC in the plain model. In CRYPTO 2023
[COSW23] M. Ciampi, R. Ostrovsky, L. Siniscalchi, and H. Waldner. List oblivious transfer and applications to round-optimal black-box multiparty coin tossing.CRYPTO2023.

Can we close the gap?

[IPS08] Compiler

OUTER PROTOCOL

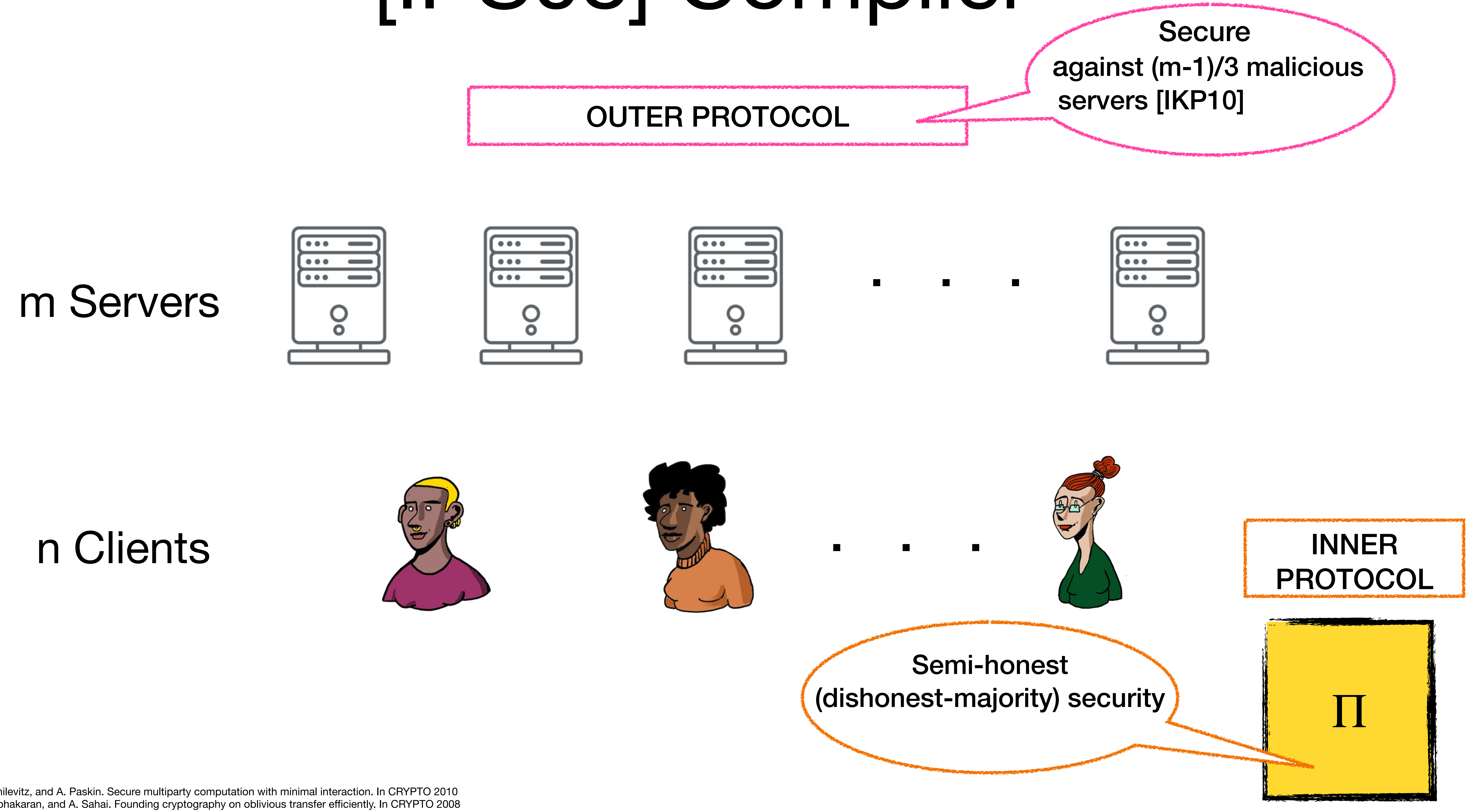
Secure against (m-1)/3 malicious servers [IKP10]

m Servers

n Clients

[IKP10]Y. Ishai, E. Kushilevitz, and A. Paskin. Secure multiparty computation with minimal interaction. In CRYPTO 2010
[IPS08]Y. Ishai, M. Prabhakaran, and A. Sahai. Founding cryptography on oblivious transfer - efficiently. In CRYPTO 2008

[IPS08] Compiler



[IKP10]Y. Ishai, E. Kushilevitz, and A. Paskin. Secure multiparty computation with minimal interaction. In CRYPTO 2010
[IPS08]Y. Ishai, M. Prabhakaran, and A. Sahai. Founding cryptography on oblivious transfer efficiently. In CRYPTO 2008

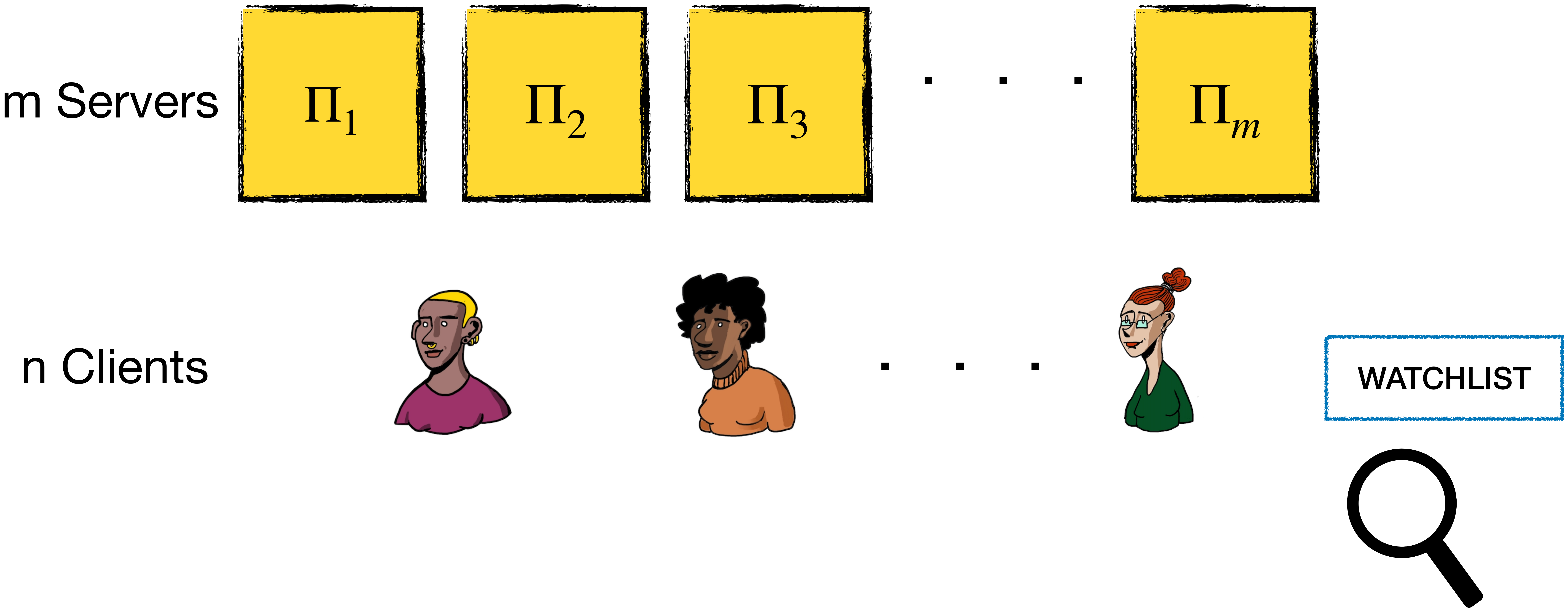
[IPS08] Compiler

m Servers Π_1 Π_2 Π_3 . . . Π_m

n Clients

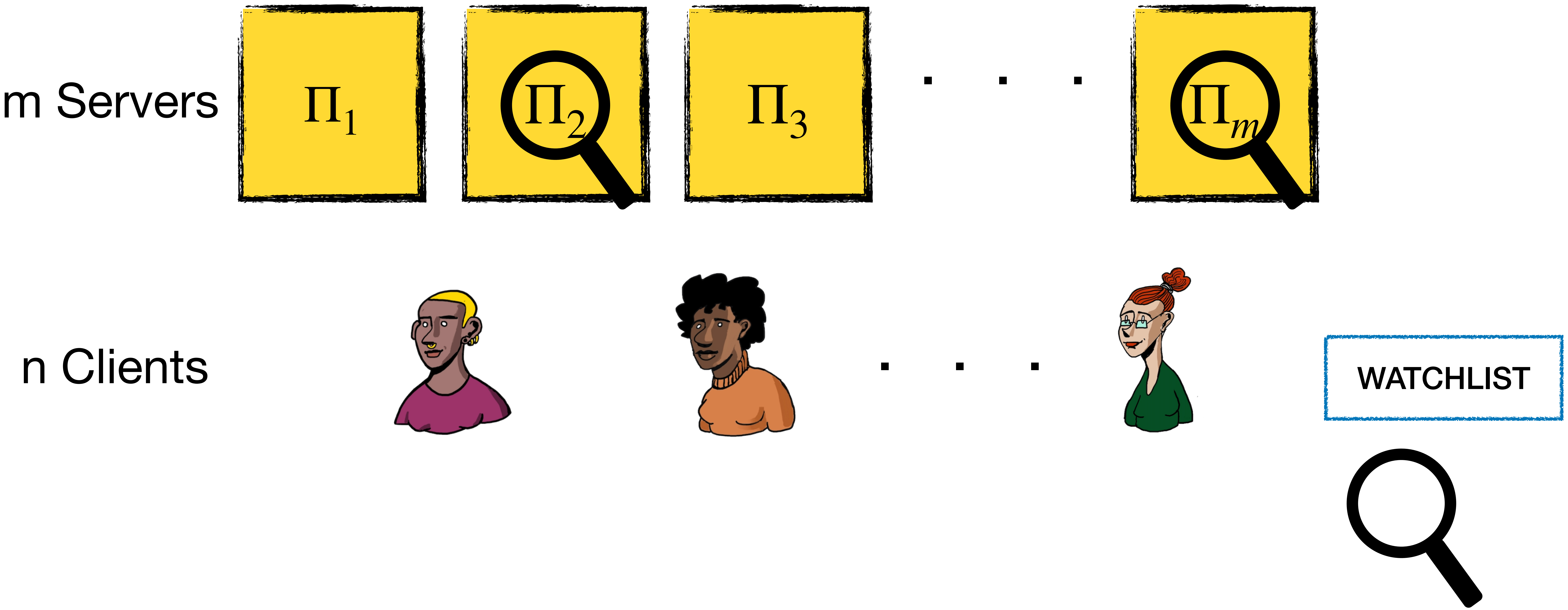
[IPS08]Y. Ishai, M. Prabhakaran, and A. Sahai. Founding cryptography on oblivious transfer - efficiently. In CRYPTO 2008

[IPS08] Compiler



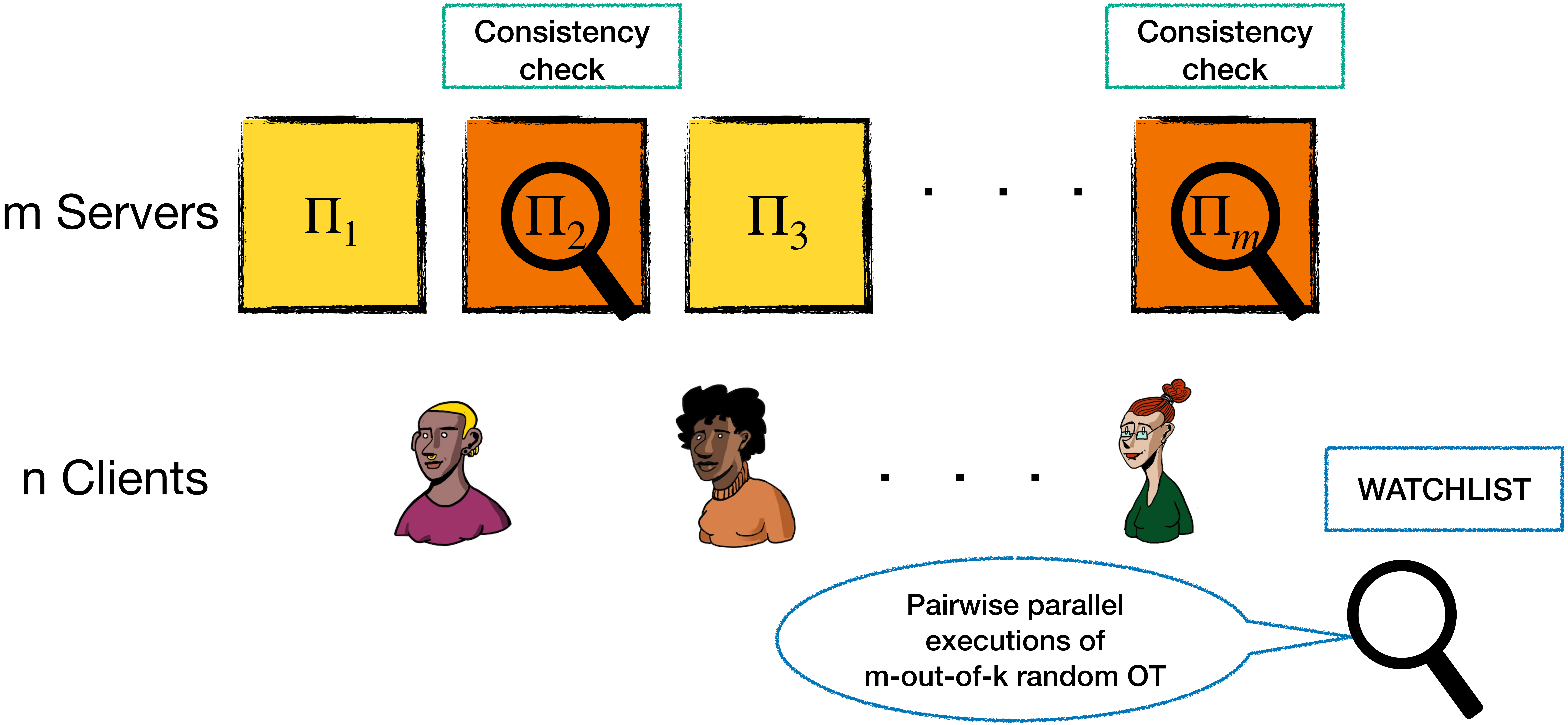
[IPS08]Y. Ishai, M. Prabhakaran, and A. Sahai. Founding cryptography on oblivious transfer - efficiently. In CRYPTO 2008

[IPS08] Compiler



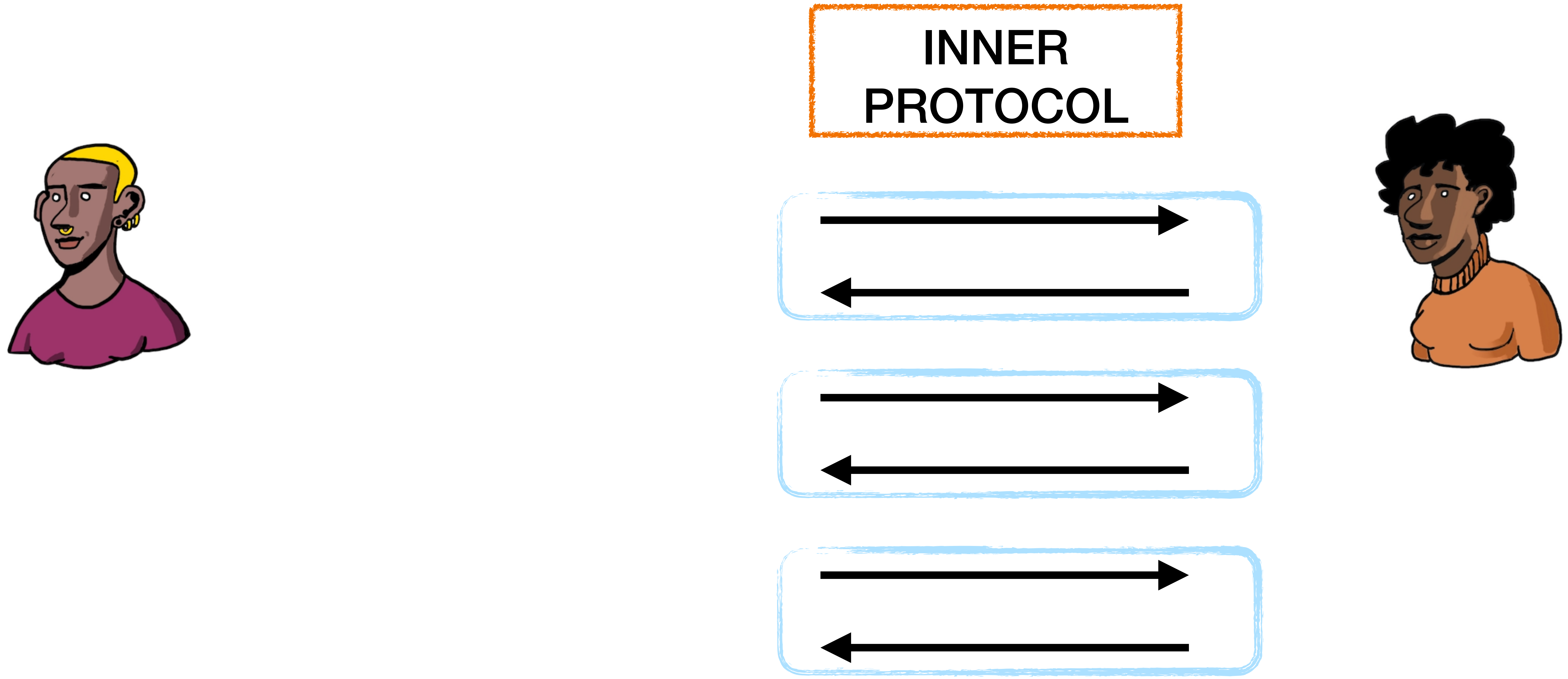
[IPS08]Y. Ishai, M. Prabhakaran, and A. Sahai. Founding cryptography on oblivious transfer - efficiently. In CRYPTO 2008

[IPS08] Compiler



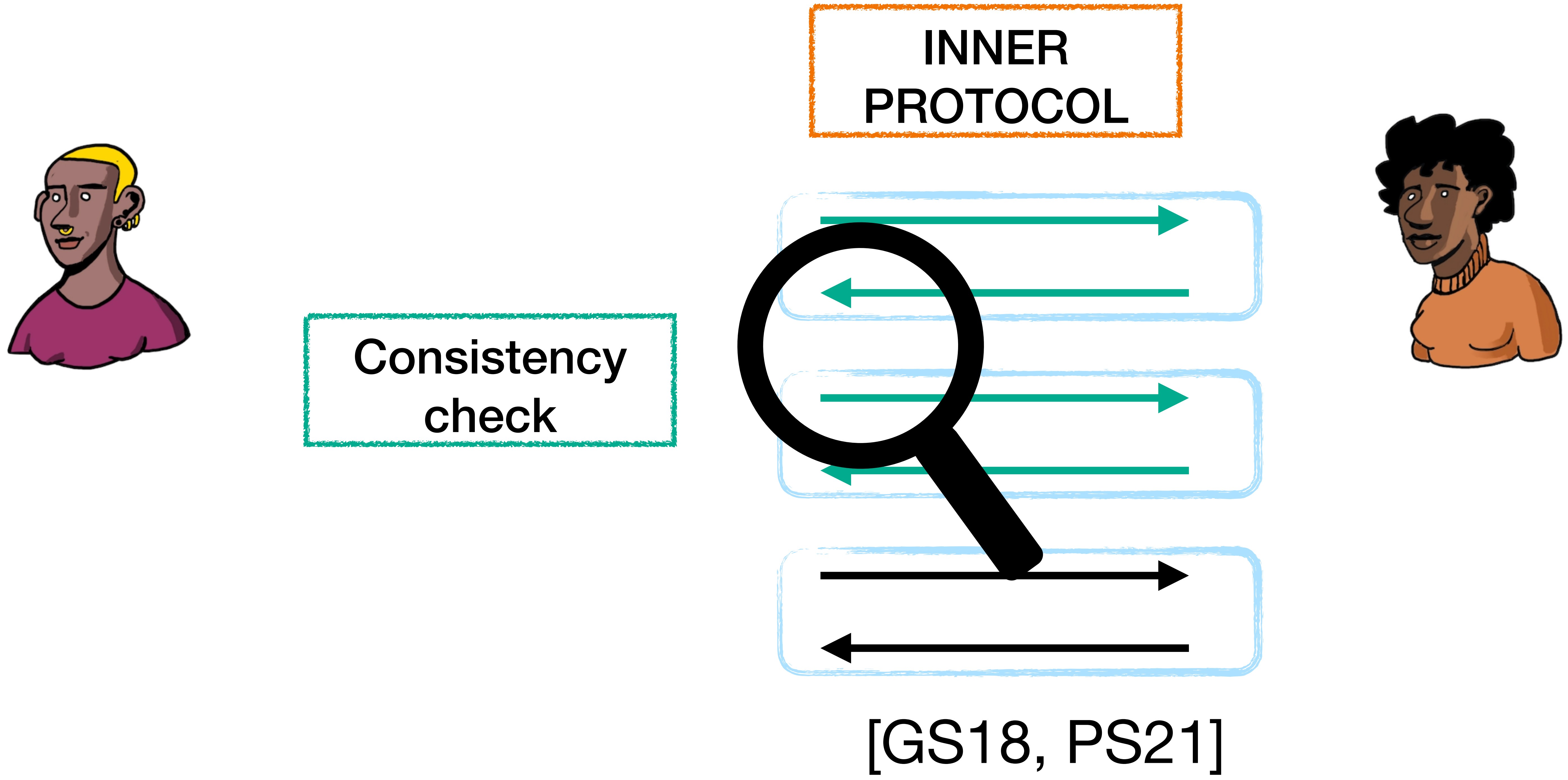
[IPS08]Y. Ishai, M. Prabhakaran, and A. Sahai. Founding cryptography on oblivious transfer - efficiently. In CRYPTO 2008

[IKKS21]'s Approach: Compress IPS



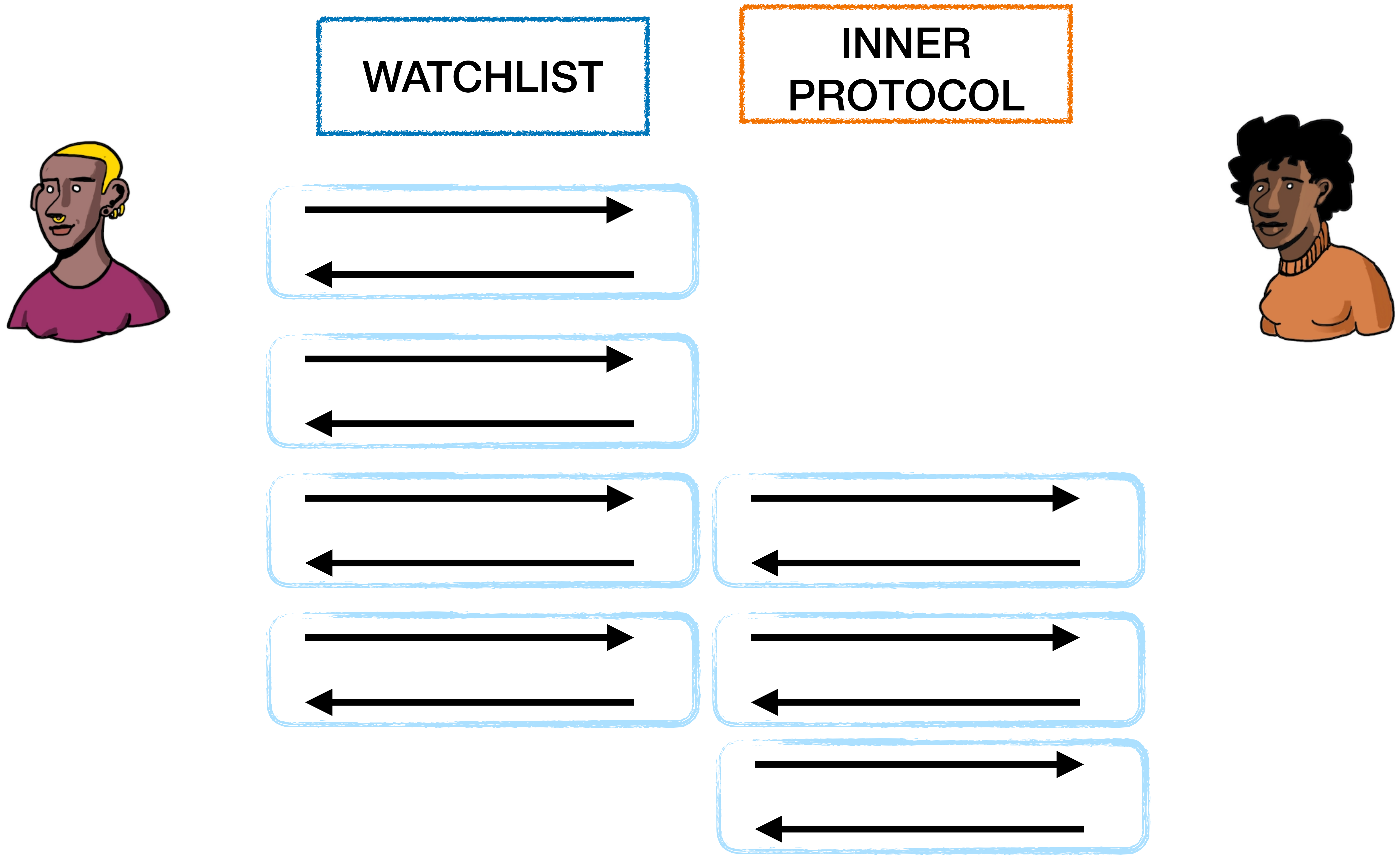
[IKSS21] Y. Ishai, D. Khurana, A. Sahai, and A. Srinivasan. On the round complexity of black-box secure MPC. In CRYPTO 2021

[IKKS21]'s Approach: Compress IPS



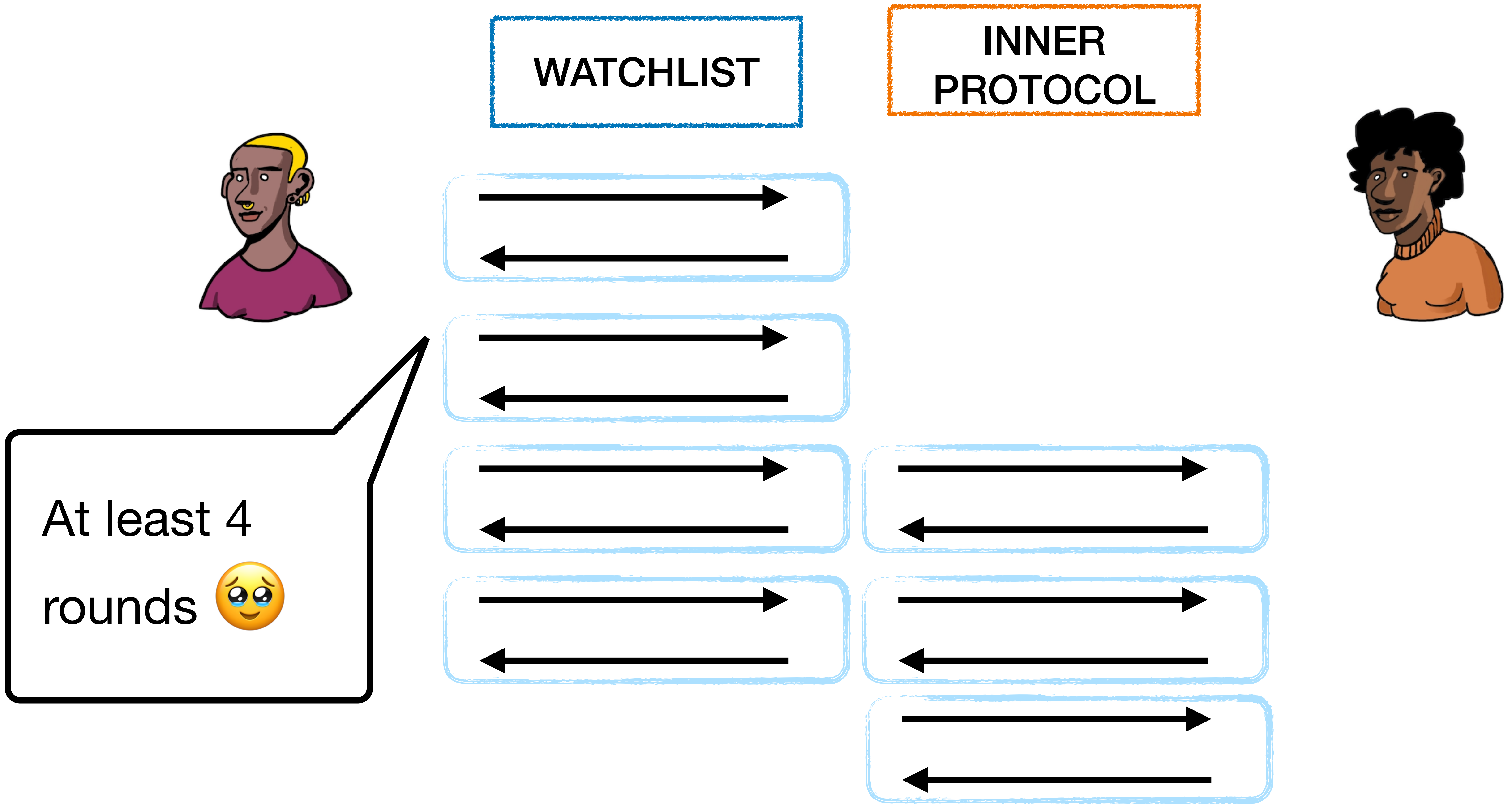
[GS18] S. Garg and A. Srinivasan. Two-round multiparty secure computation from minimal assumptions. In EUROCRYPT 2018
[PS21] A. Patra and A. Srinivasan. Three-round secure multiparty computation from black-box two-round oblivious transfer. In CRYPTO2021
[IKSS21] Y. Ishai, D. Khurana, A. Sahai, and A. Srinivasan. On the round complexity of black-box secure MPC. In CRYPTO 2021

[IKKS21]'s Approach: Compress IPS



[KO04]J. Katz and R. Ostrovsky. Round-optimal secure two-party computation. In CRYPTO 2004.
[IKSS21] Y. Ishai, D. Khurana, A. Sahai, and A. Srinivasan. On the round complexity of black-box secure MPC. In CRYPTO 2021

[IKKS21]'s Approach: Compress IPS



[KO04]J. Katz and R. Ostrovsky. Round-optimal secure two-party computation. In CRYPTO 2004.
[IKSS21] Y. Ishai, D. Khurana, A. Sahai, and A. Srinivasan. On the round complexity of black-box secure MPC. In CRYPTO 2021

[COSW23]'s Approach: Relax Watchlist Requirements

[COSW23] M. Ciampi, R. Ostrovsky, L. Siniscalchi, and H. Waldner. List oblivious transfer and applications to round-optimal black-box multiparty coin tossing.CRYPTO2023.

[COSW23]'s Approach:
Relax Watchlist Requirements

Sometimes aborting adversaries

[COSW23] M. Ciampi, R. Ostrovsky, L. Siniscalchi, and H. Waldner. List oblivious transfer and applications to round-optimal black-box multiparty coin tossing.CRYPTO2023.

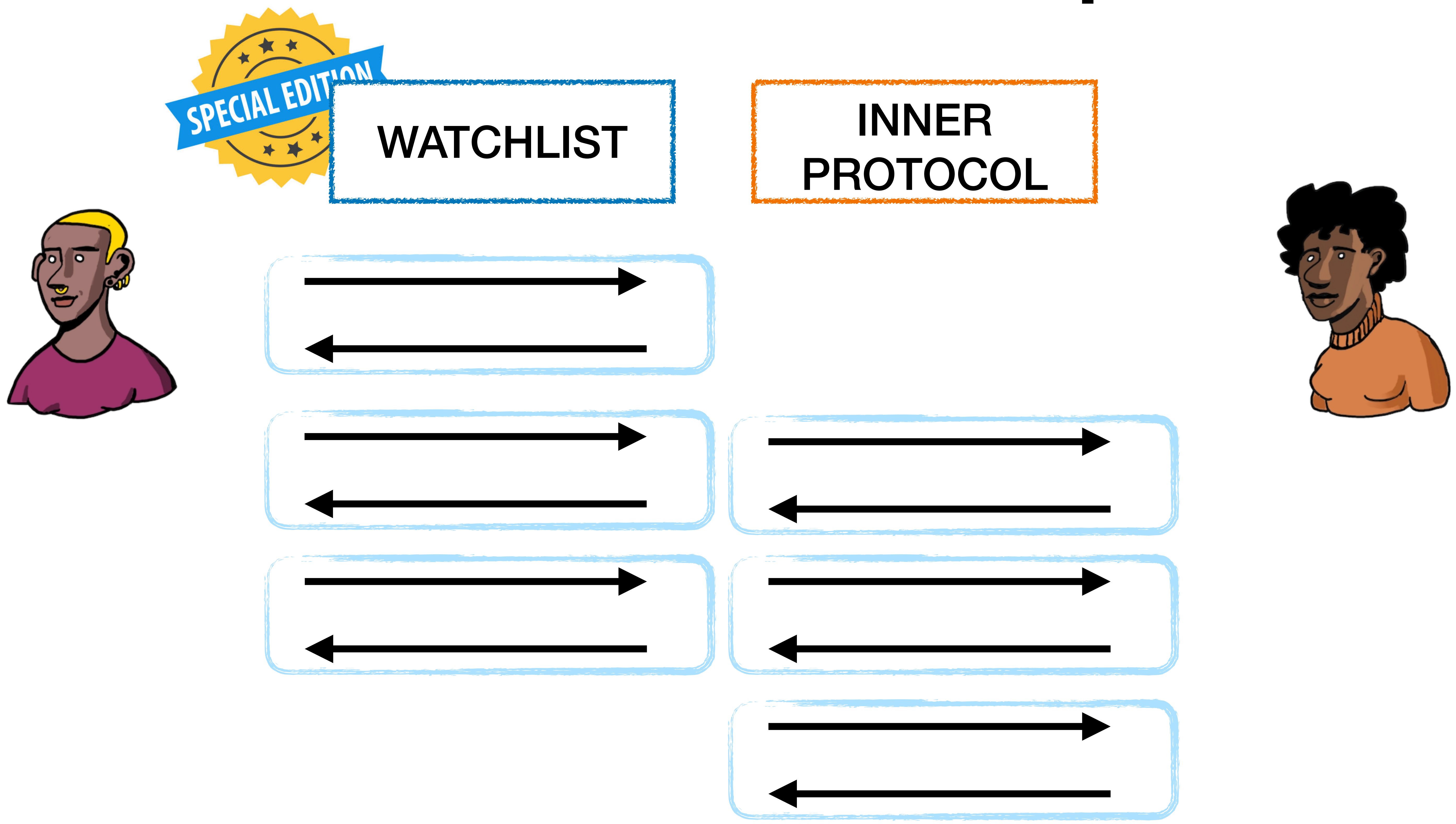
[COSW23]'s Approach: Relax Watchlist Requirements

Sometimes aborting adversaries

[COSW23] M. Ciampi, R. Ostrovsky, L. Siniscalchi, and H. Waldner. List oblivious transfer and applications to round-optimal black-box multiparty coin tossing.CRYPTO2023.

[COSW23]'s Approach: Relax Watchlist Requirements

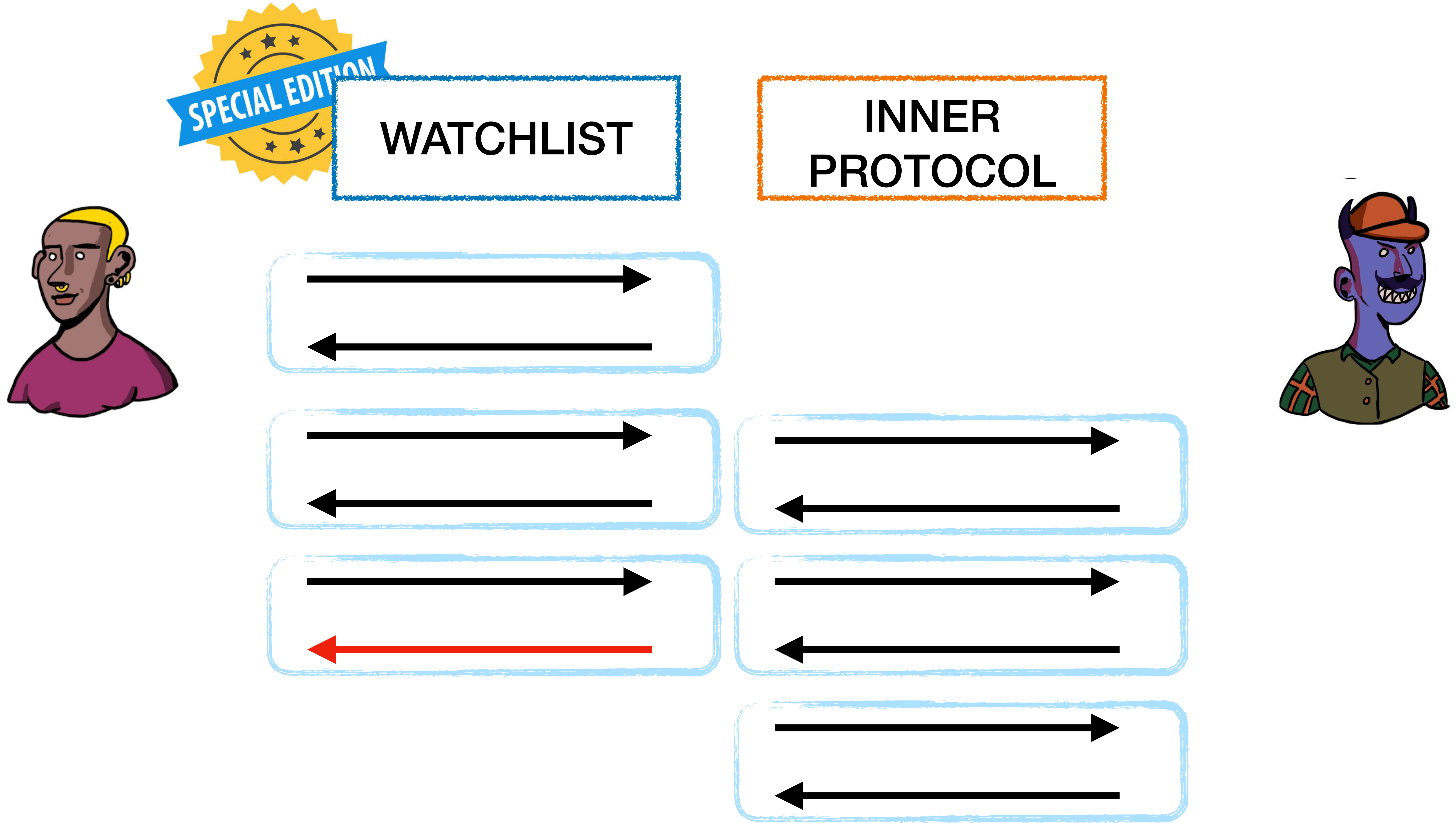
Sometimes aborting adversaries



[COSW23] M. Ciampi, R. Ostrovsky, L. Siniscalchi, and H. Waldner. List oblivious transfer and applications to round-optimal black-box multiparty coin tossing.CRYPTO2023.

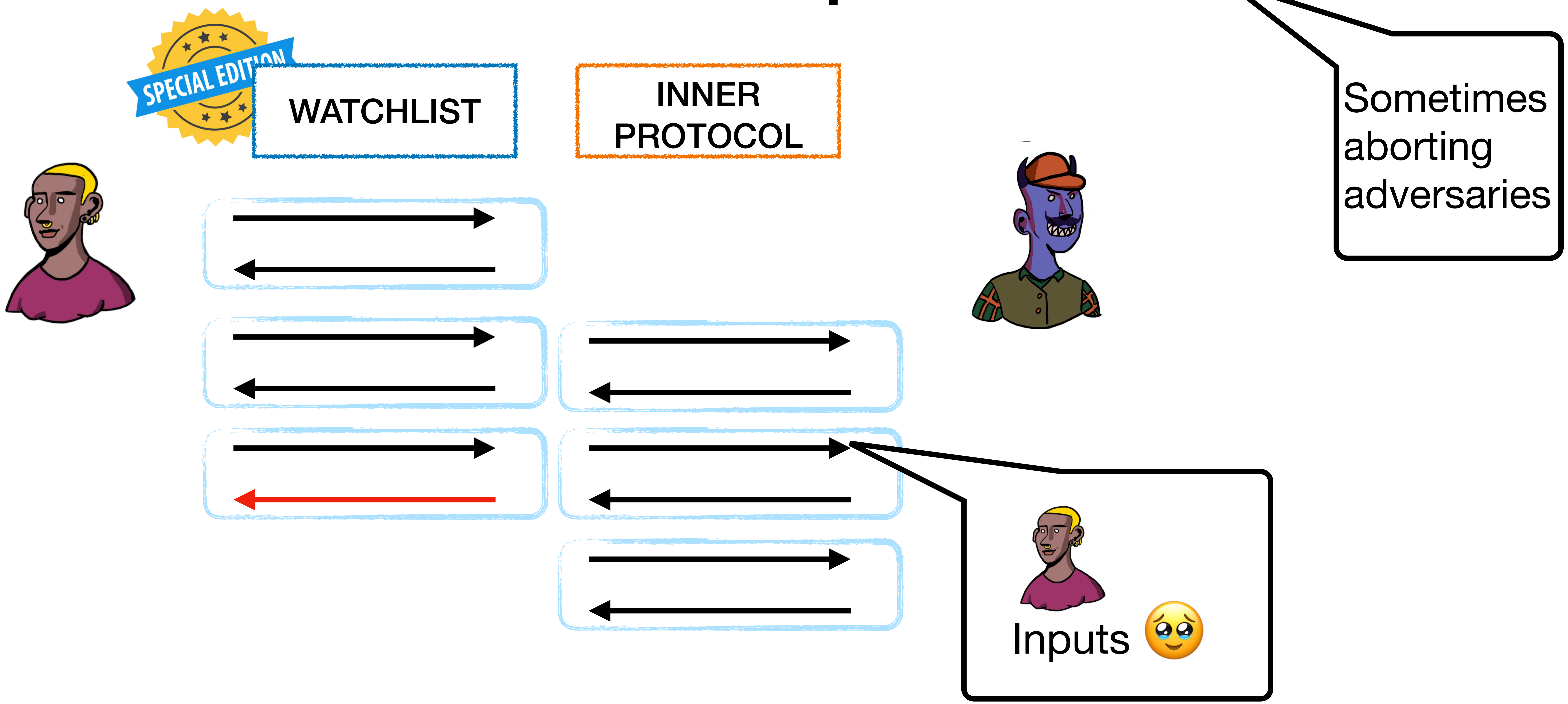
[COSW23]'s Approach: Relax Watchlist Requirements

Sometimes aborting adversaries



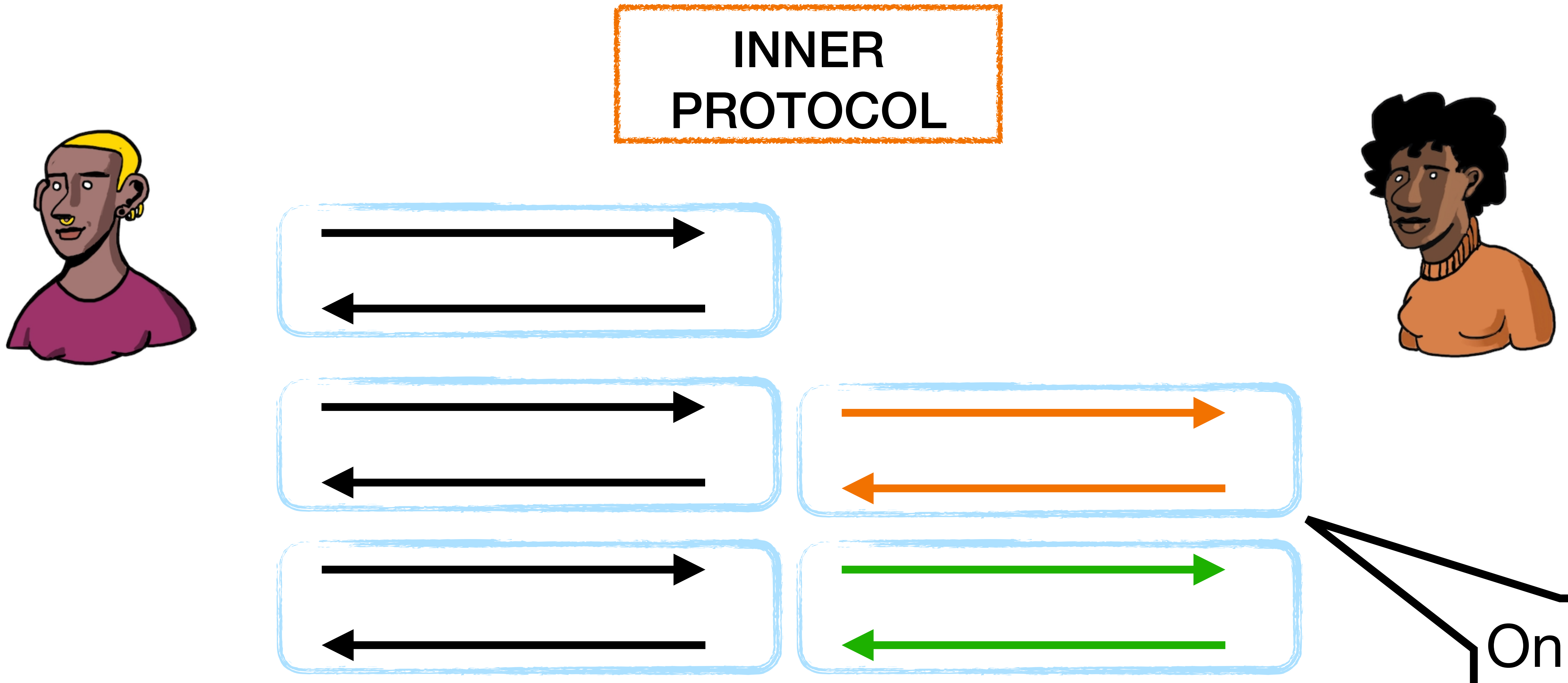
[COSW23] M. Ciampi, R. Ostrovsky, L. Siniscalchi, and H. Waldner. List oblivious transfer and applications to round-optimal black-box multiparty coin tossing.CRYPTO2023.

[COSW23]'s Approach: Relax Watchlist Requirements



[COSW23] M. Ciampi, R. Ostrovsky, L. Siniscalchi, and H. Waldner. List oblivious transfer and applications to round-optimal black-box multiparty coin tossing.CRYPTO2023.

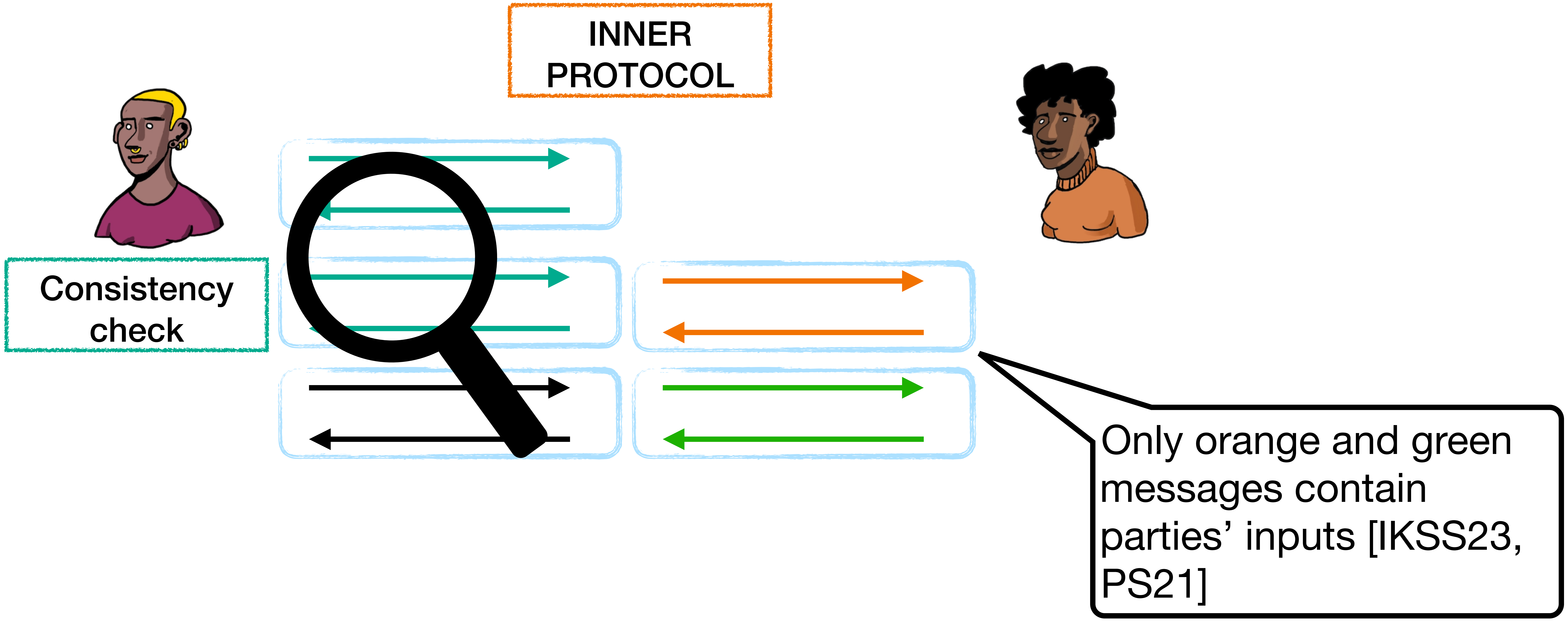
Our Approach: Split Inner Protocol



Only orange and green messages contain parties' inputs [IKSS23, PS21]

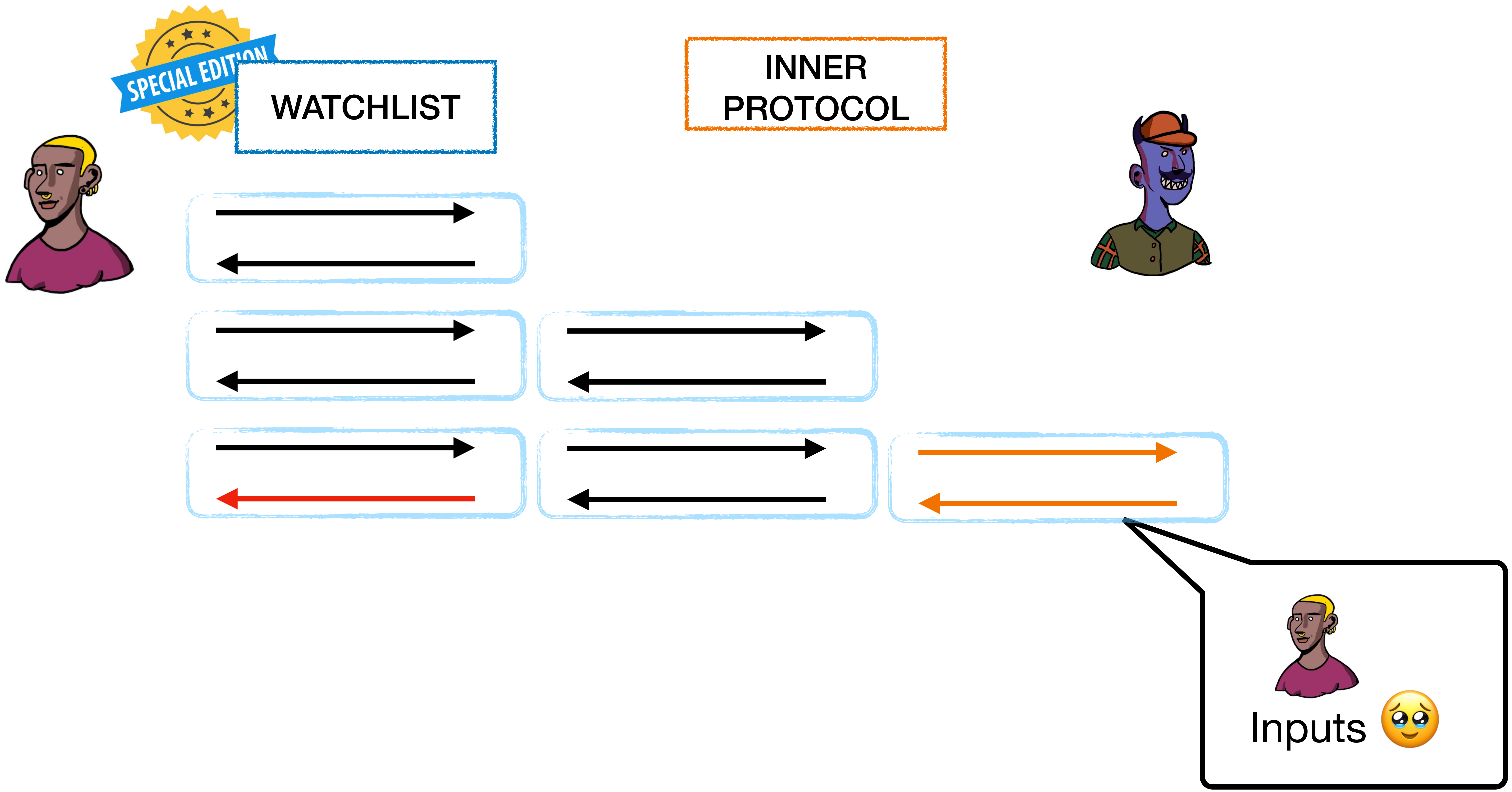
[COSW23] M. Ciampi, R. Ostrovsky, L. Siniscalchi, and H. Waldner. List oblivious transfer and applications to round-optimal black-box multiparty coin tossing .In CRYPTO2023.
[PS21]A. Patra and A. Srinivasan. Three-round secure multiparty computation from black-box two-round oblivious transfer. In CRYPTO2021
[IKSS23] Y. Ishai, D. Khurana, A. Sahai, and A. Srinivasan. Round-optimal black-box MPC in the plain model. In CRYPTO 2023

Our Approach: Split Inner Protocol

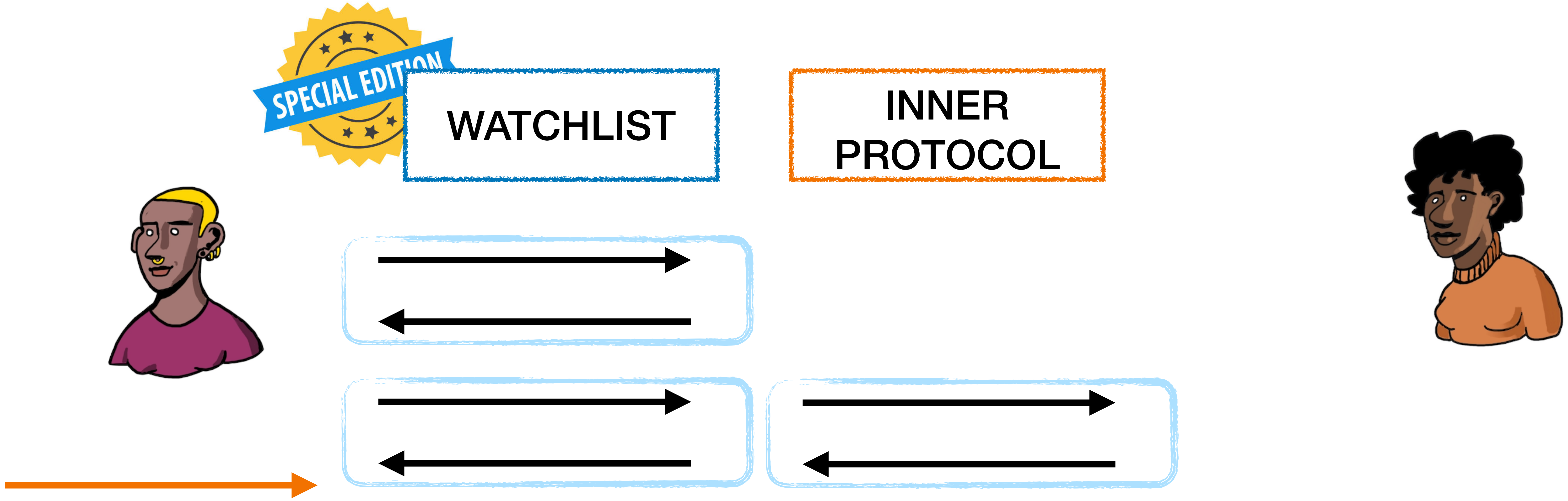


[COSW23] M. Ciampi, R. Ostrovsky, L. Siniscalchi, and H. Waldner. List oblivious transfer and applications to round-optimal black-box multiparty coin tossing .In CRYPTO2023.
[PS21]A. Patra and A. Srinivasan. Three-round secure multiparty computation from black-box two-round oblivious transfer. In CRYPTO2021
[IKSS23] Y. Ishai, D. Khurana, A. Sahai, and A. Srinivasan. Round-optimal black-box MPC in the plain model. In CRYPTO 2023

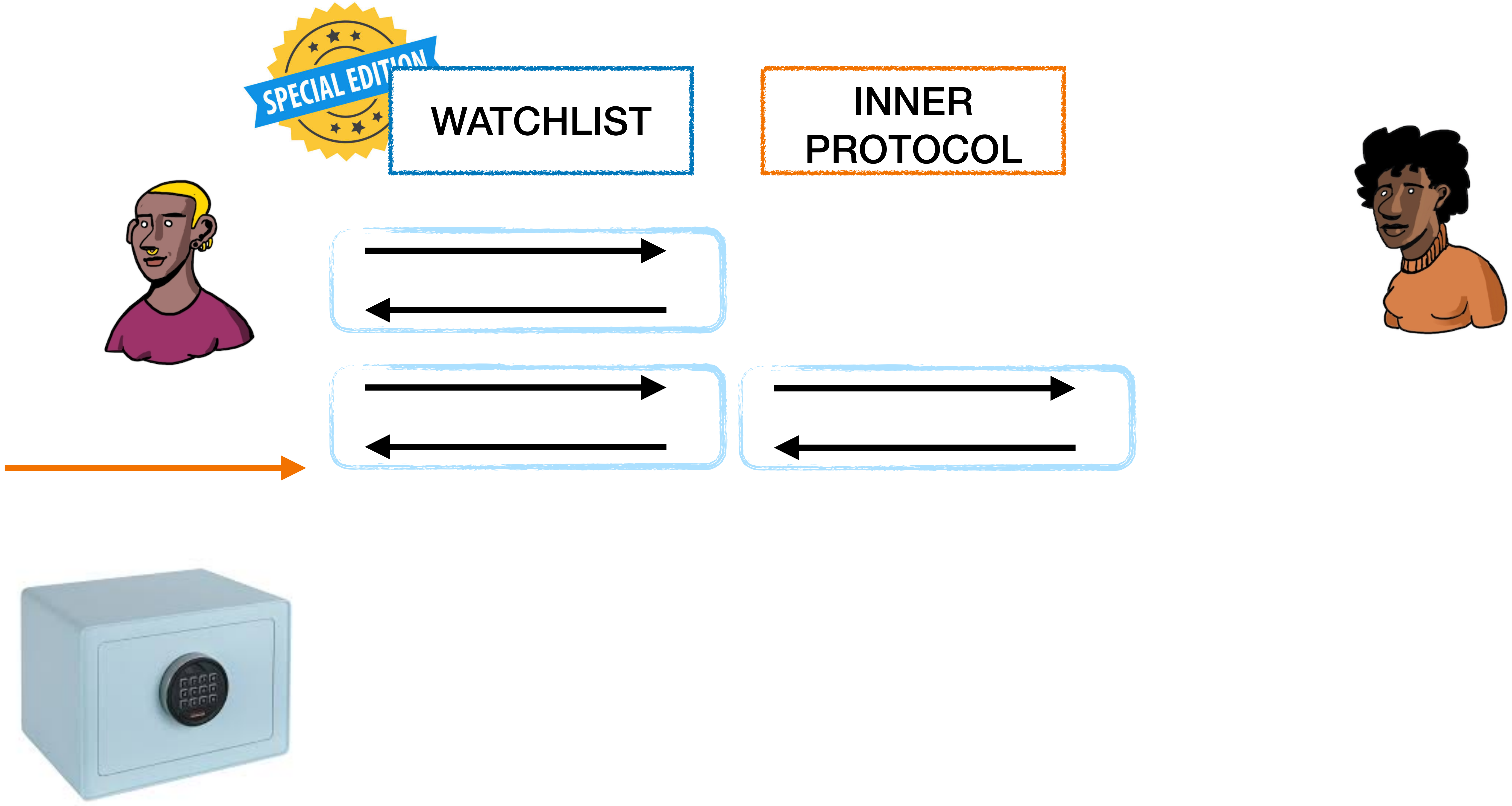
Our Approach:
Split Inner Protocol



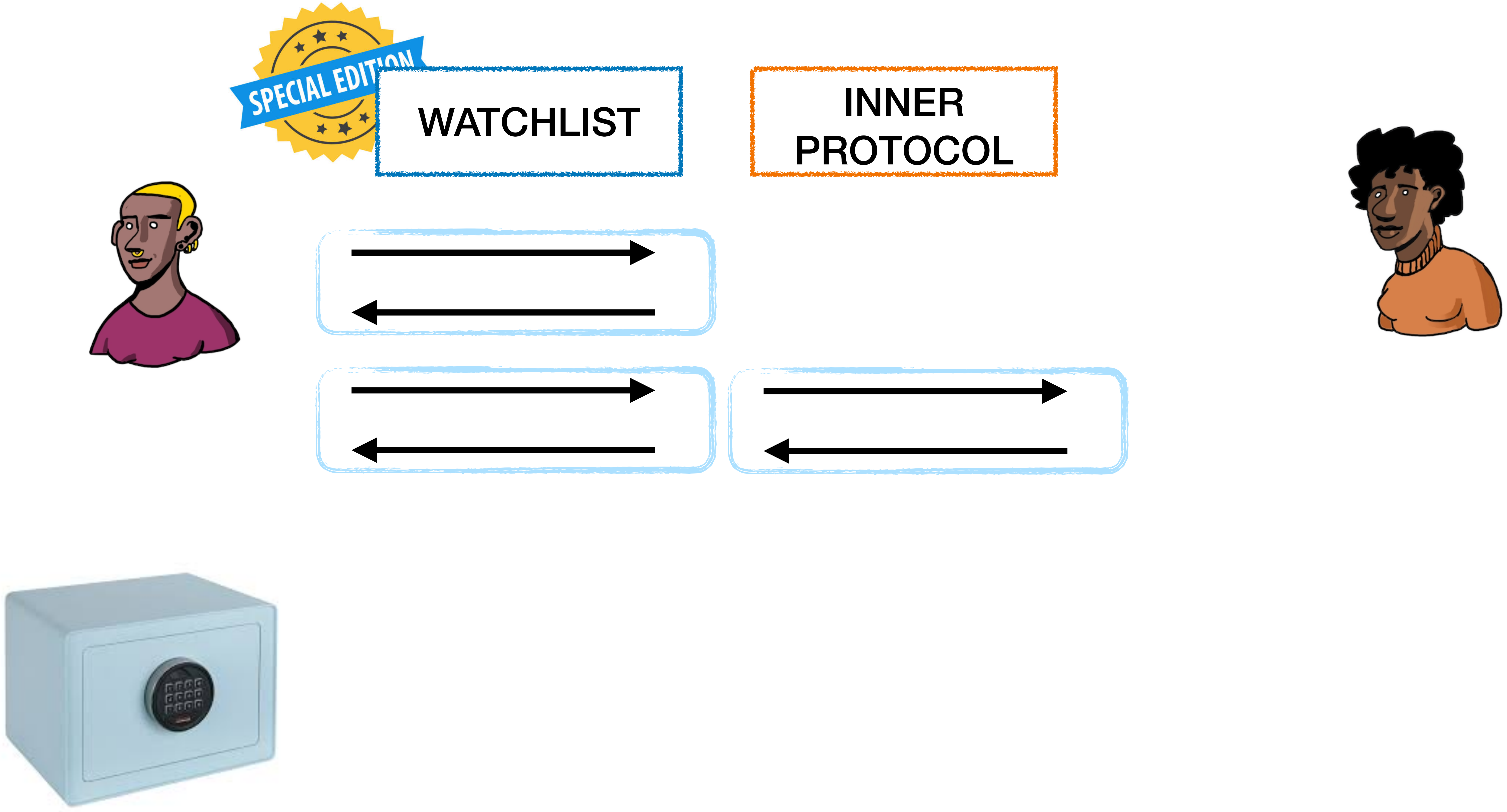
Our Approach: Conditional Disclosure of Secrets



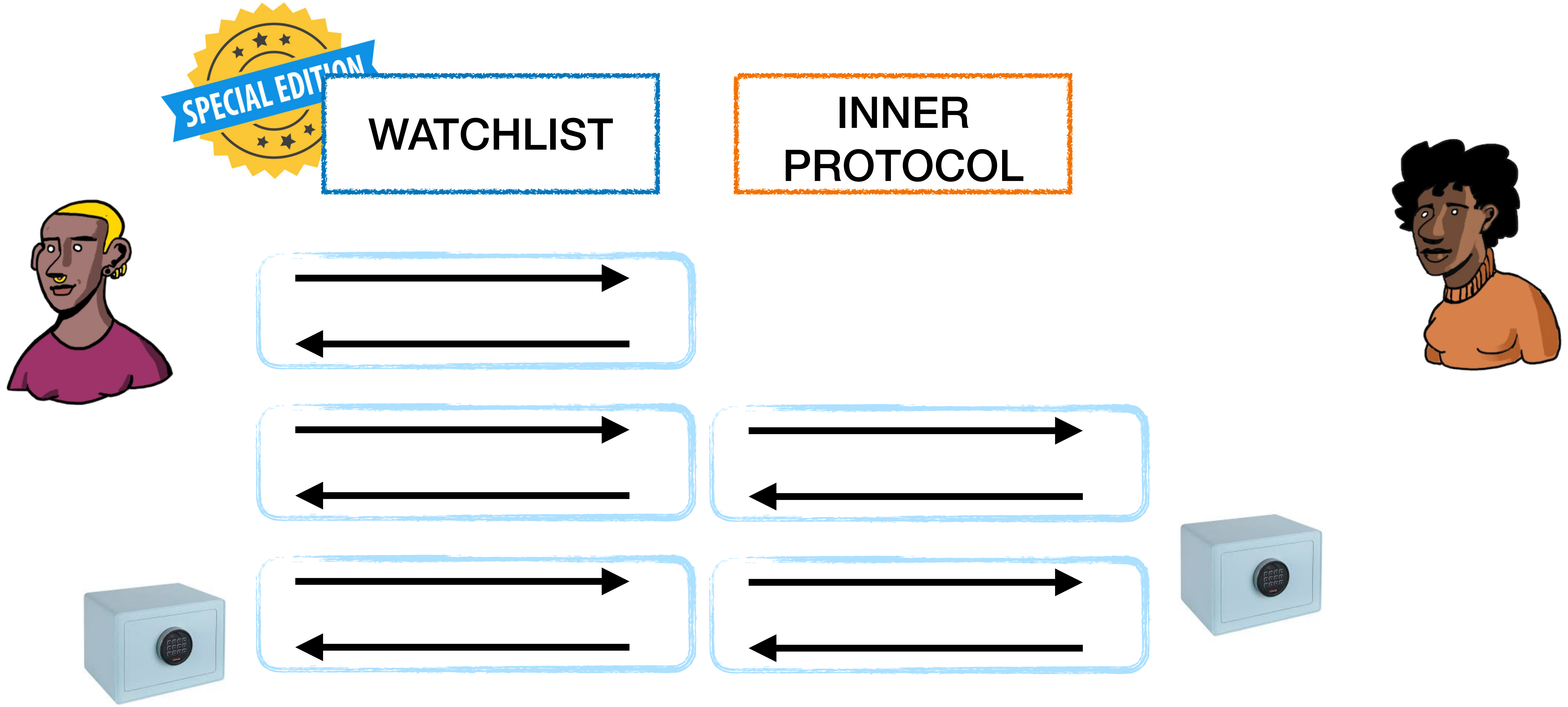
Our Approach:
Conditional Disclosure of Secrets



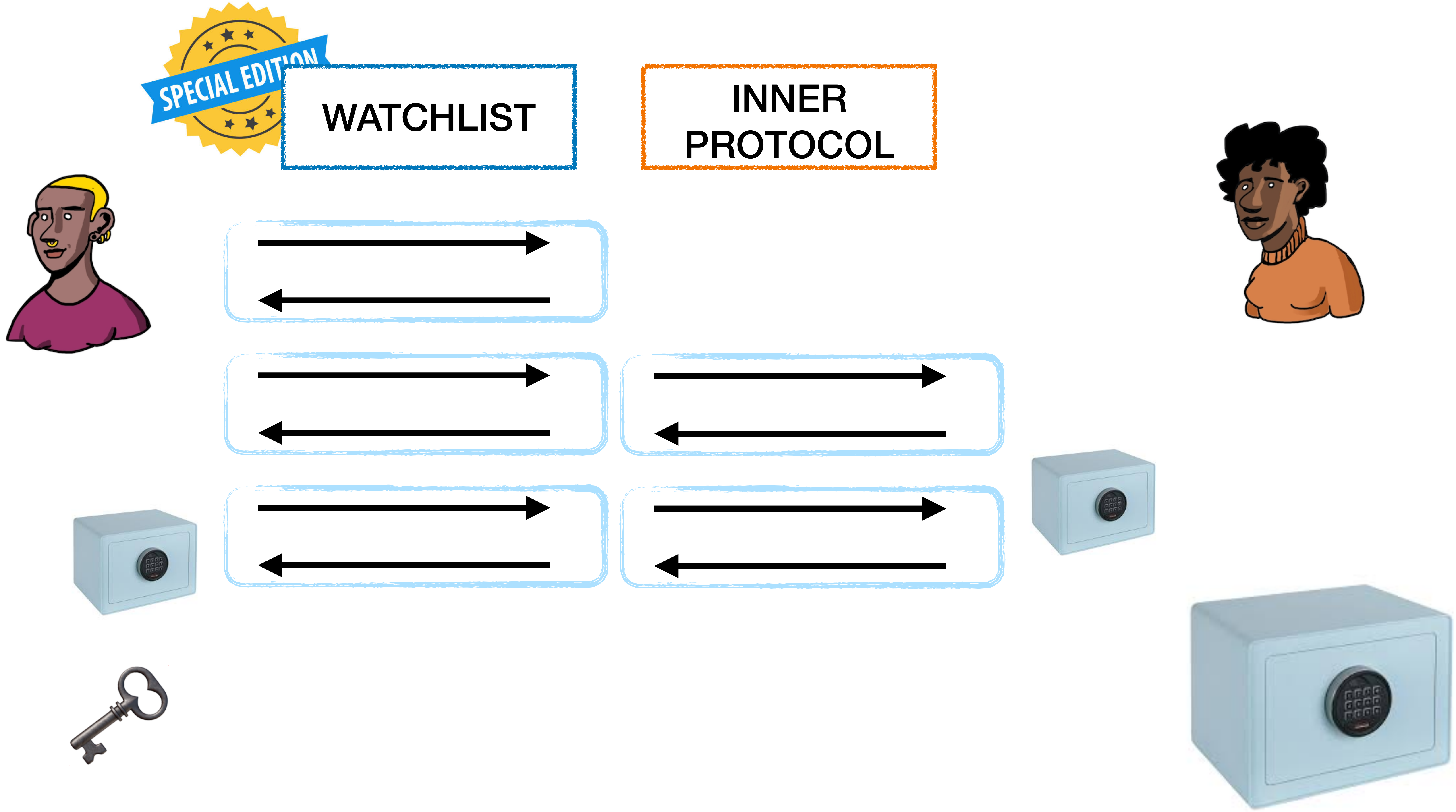
Our Approach:
Conditional Disclosure of Secrets



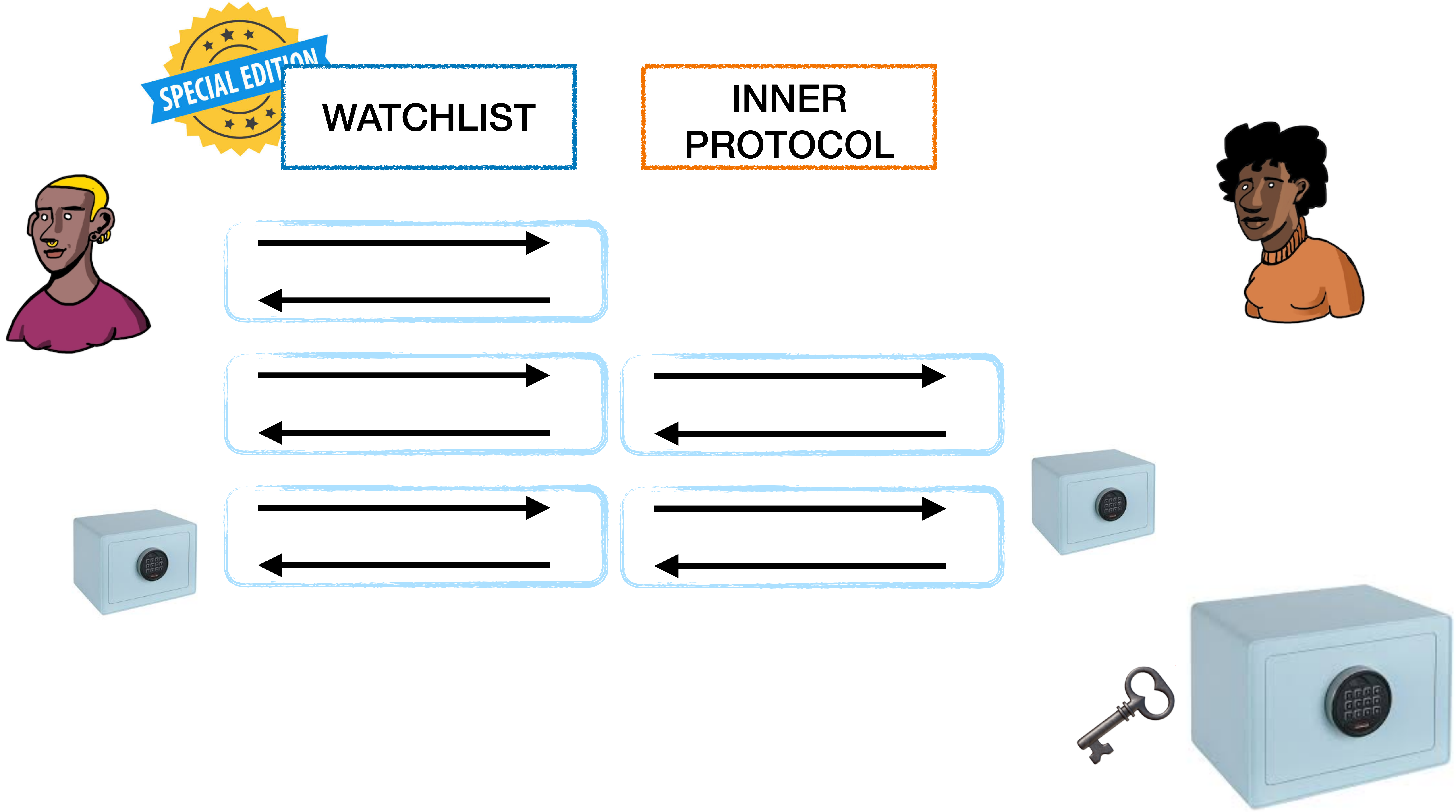
Our Approach:
Conditional Disclosure of Secrets



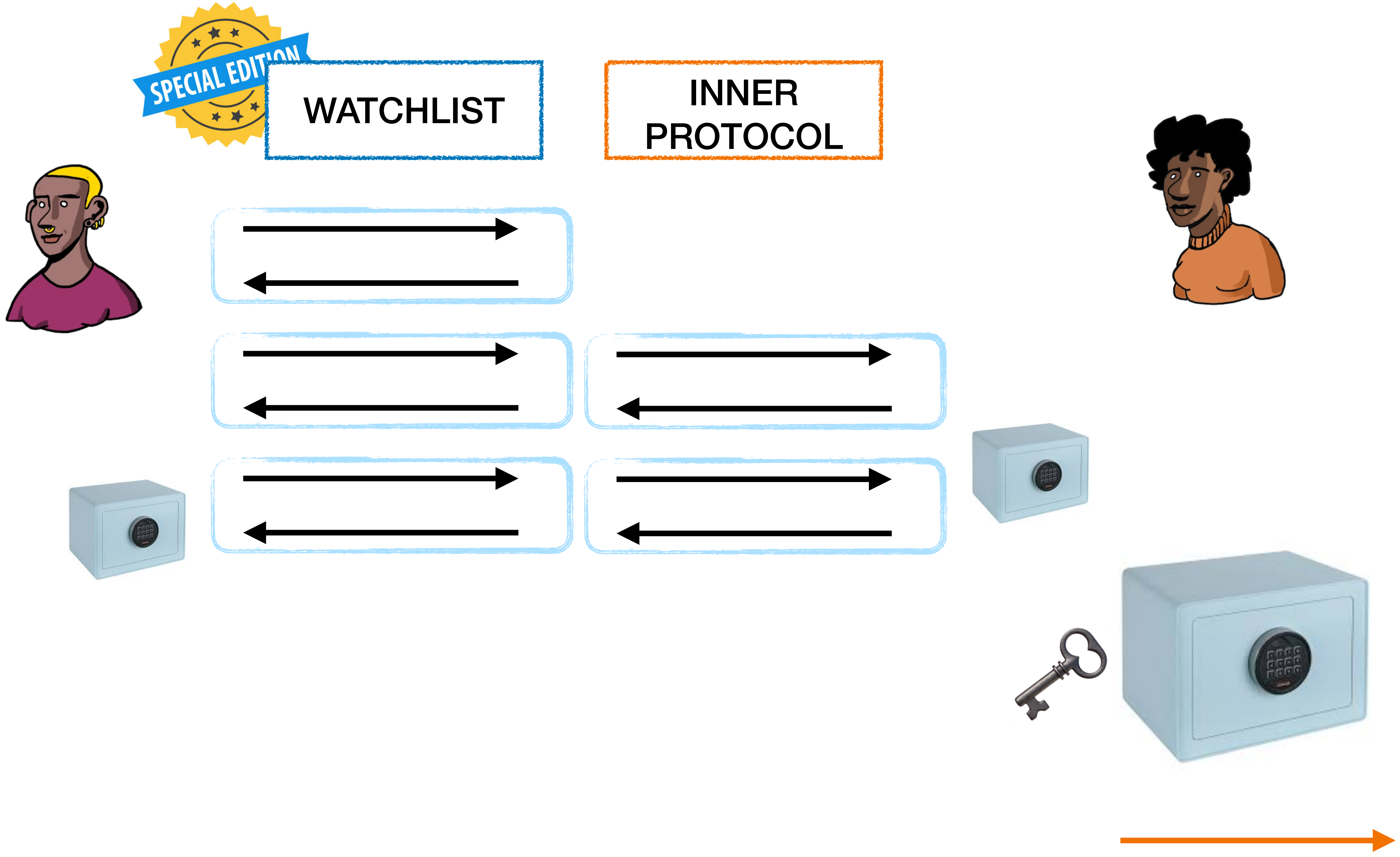
Our Approach:
Conditional Disclosure of Secrets



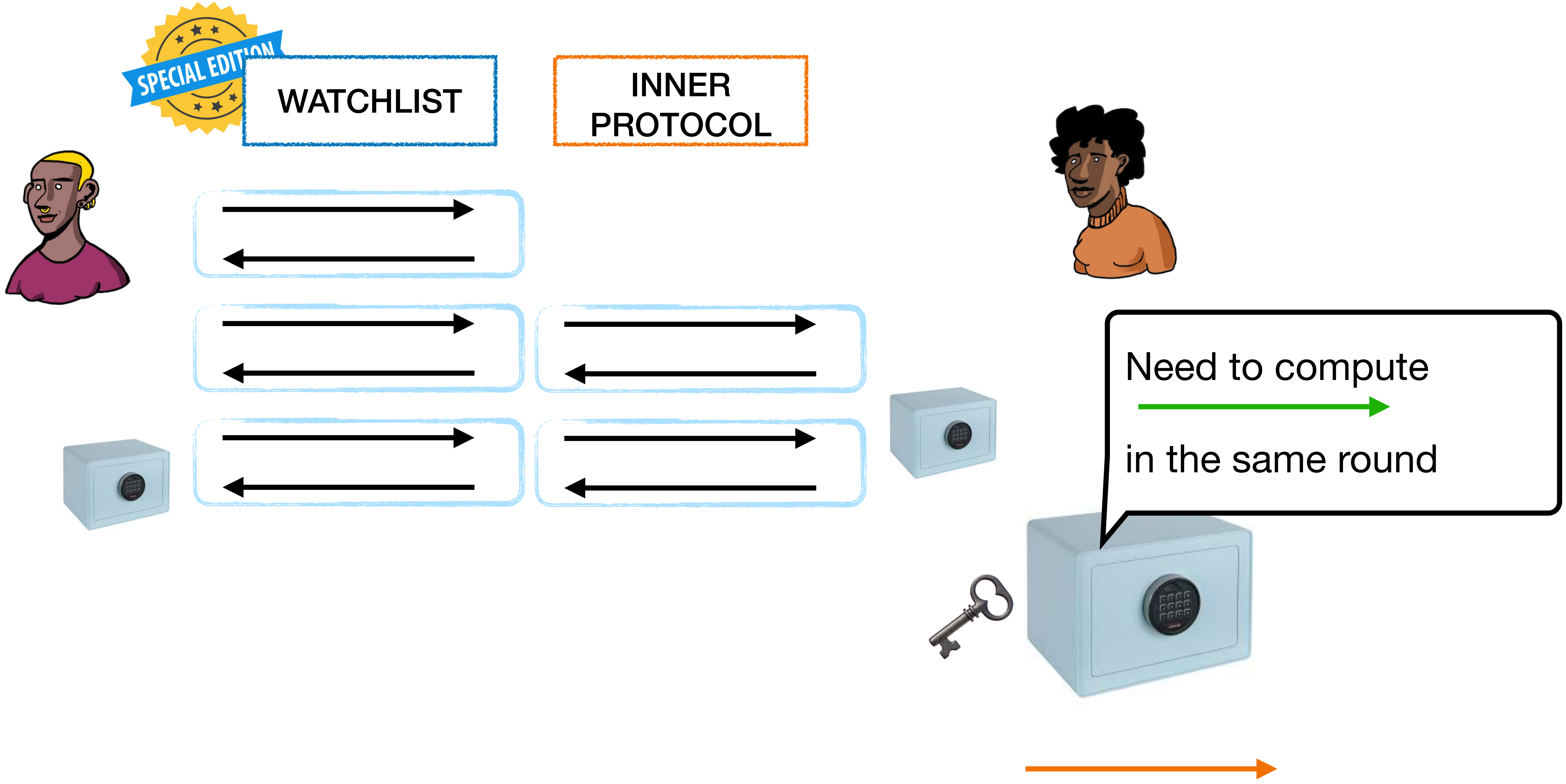
Our Approach:
Conditional Disclosure of Secrets



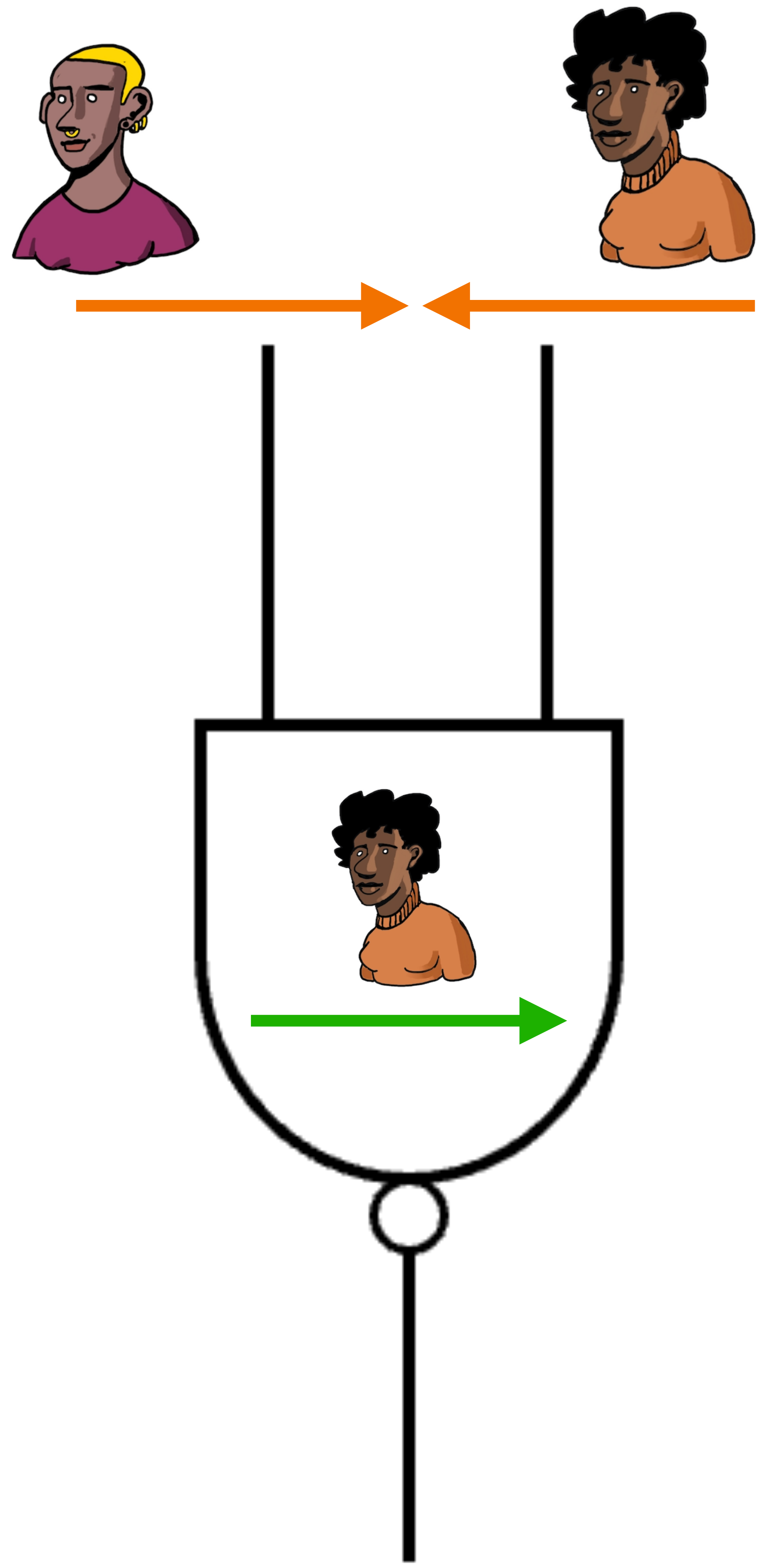
Our Approach:
Conditional Disclosure of Secrets



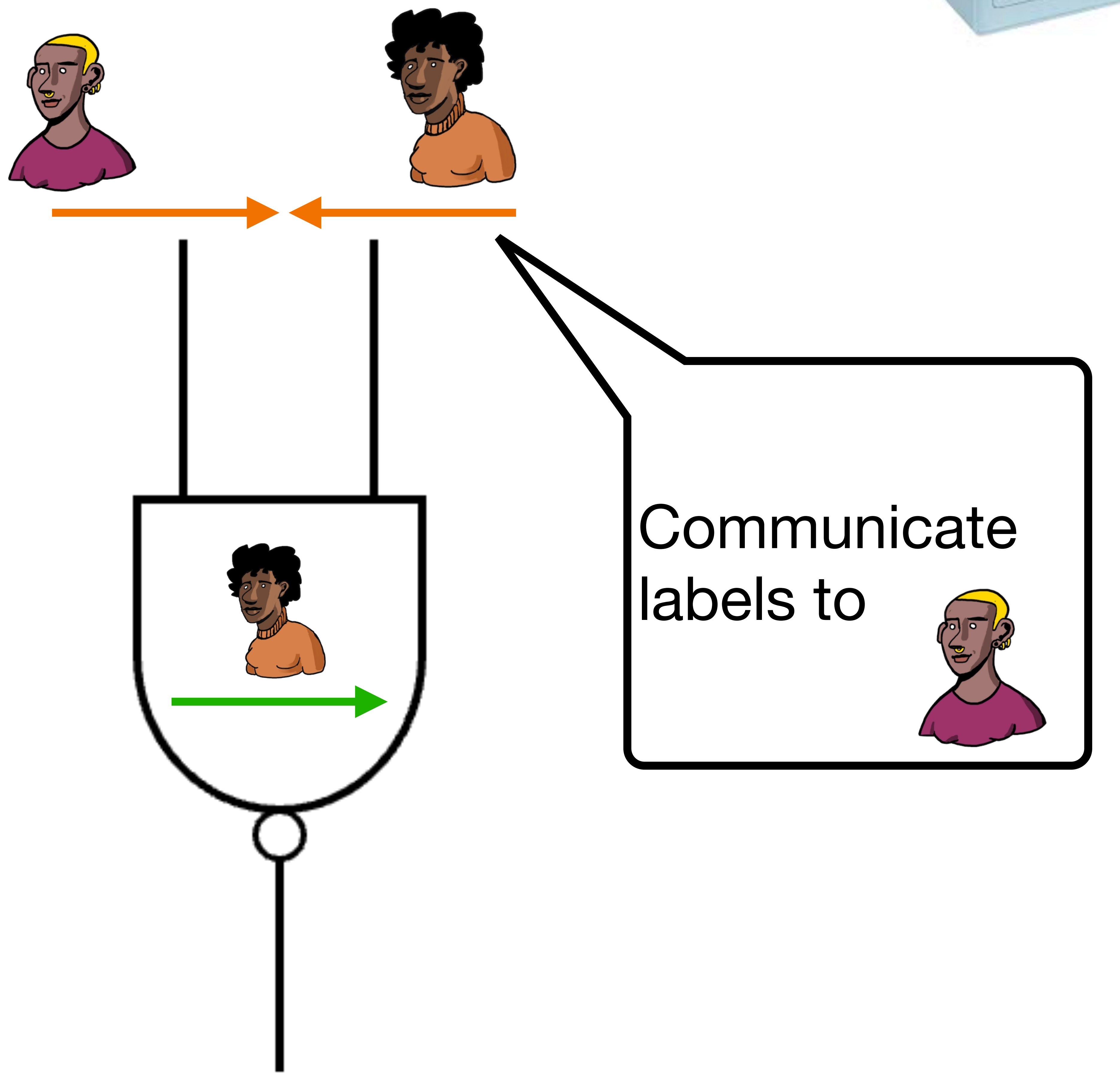
Our Approach:
Conditional Disclosure of Secrets



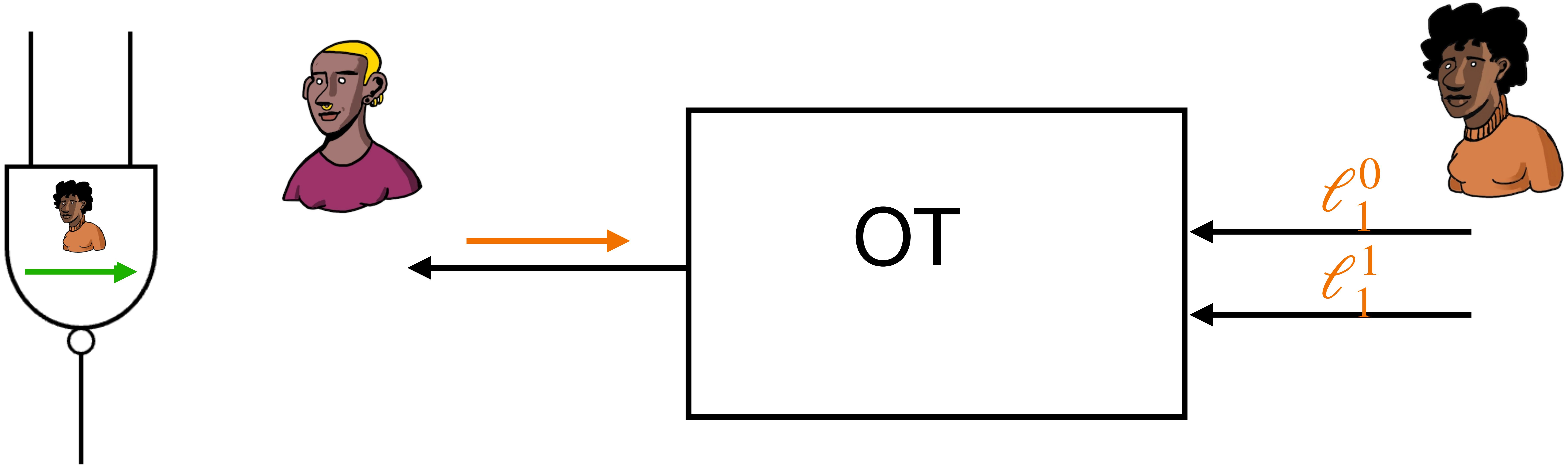
Our Approach: How to Build



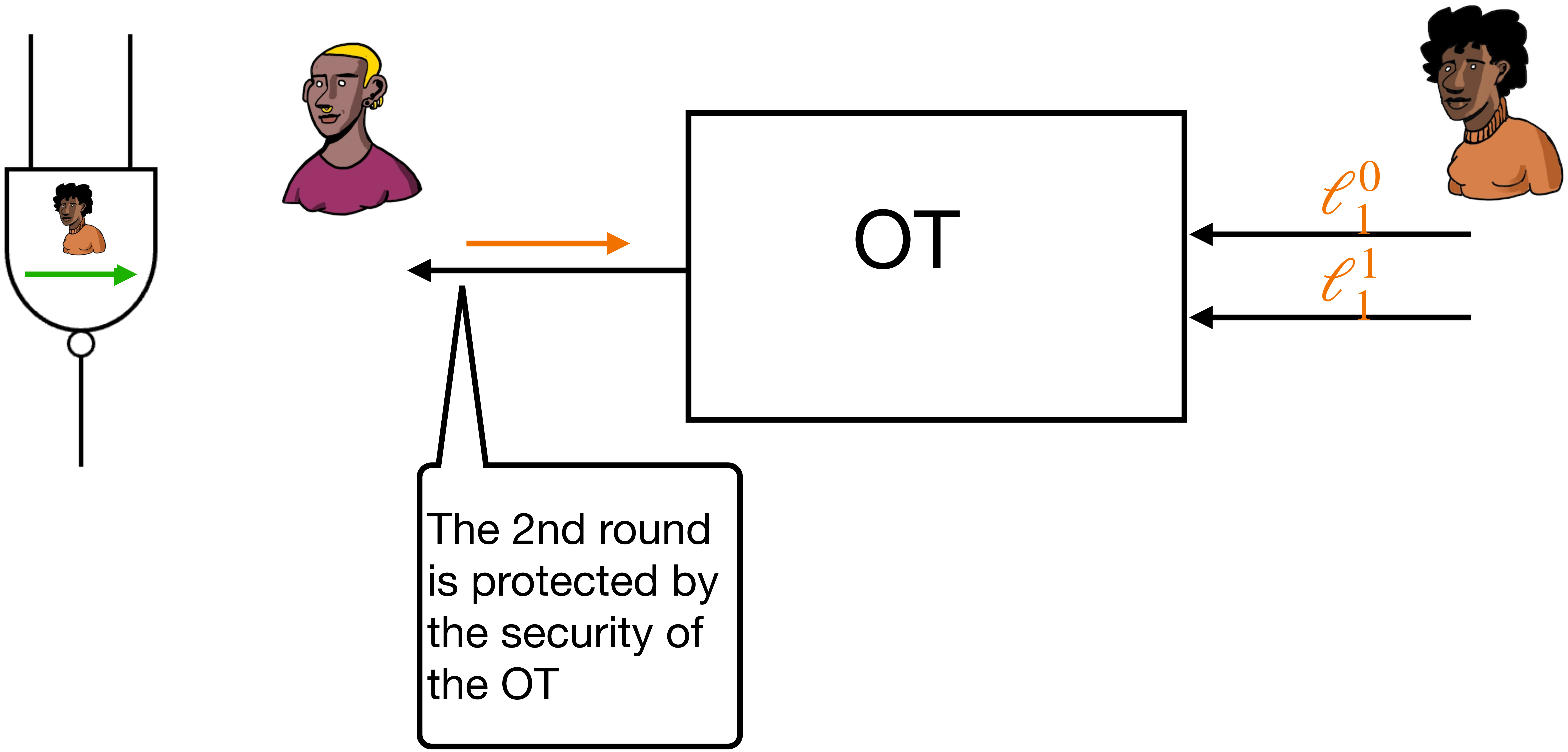
Our Approach: How to Build



Our Approach: How to Build

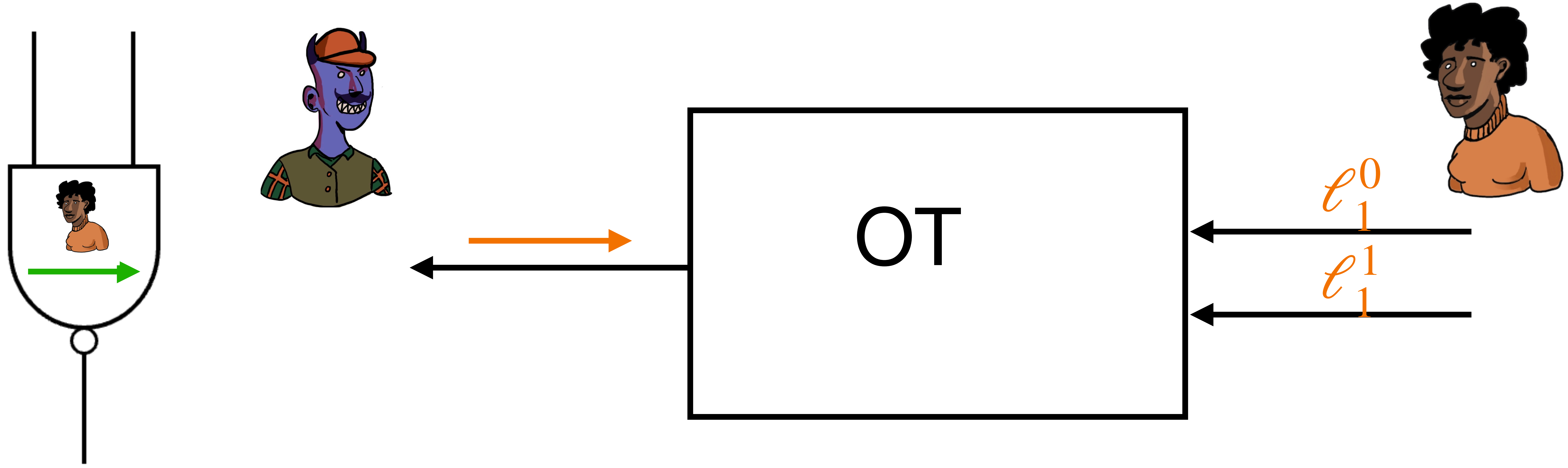


Our Approach: How to Build



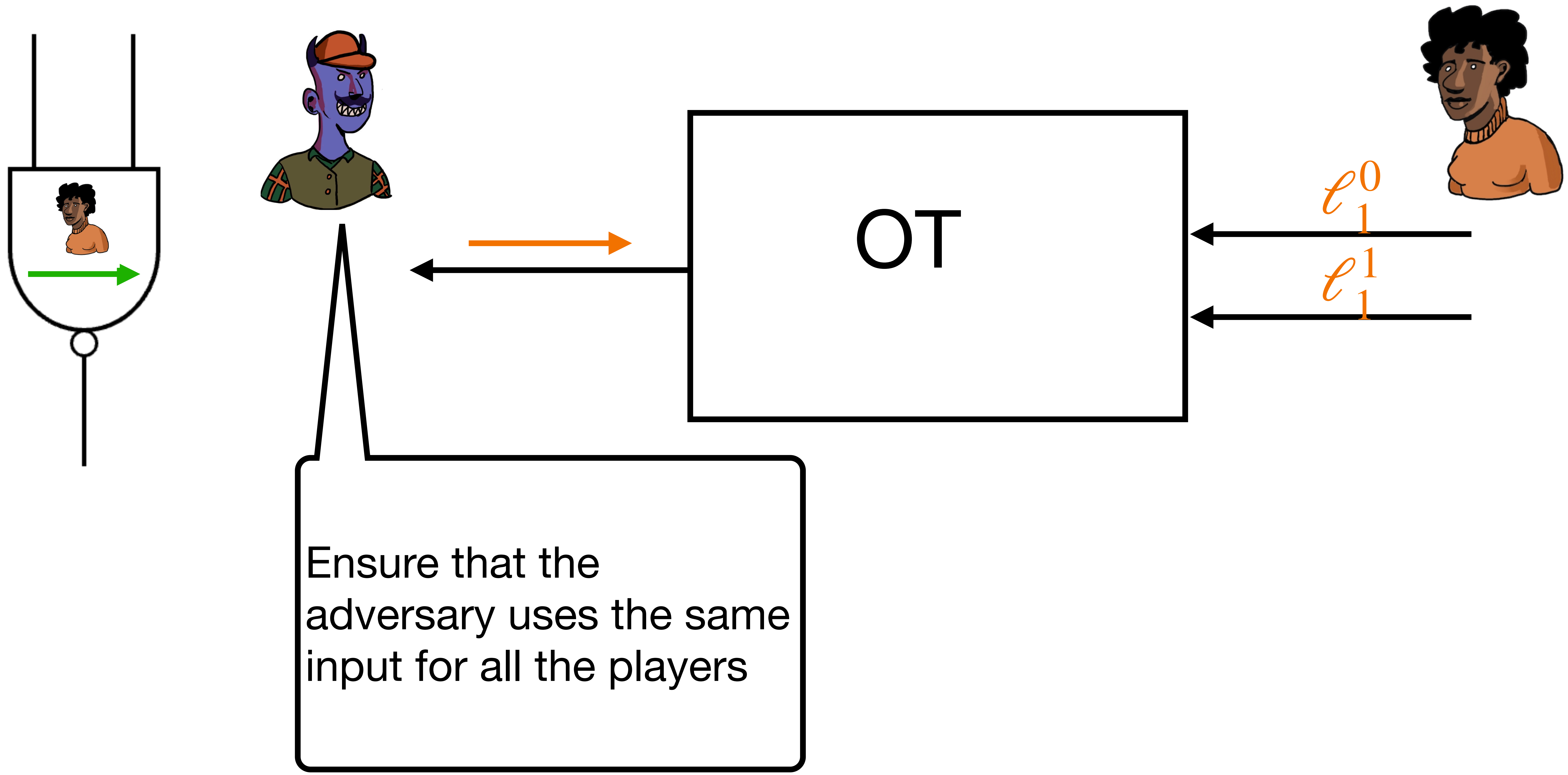
Our Approach: How to Build

Subtleties



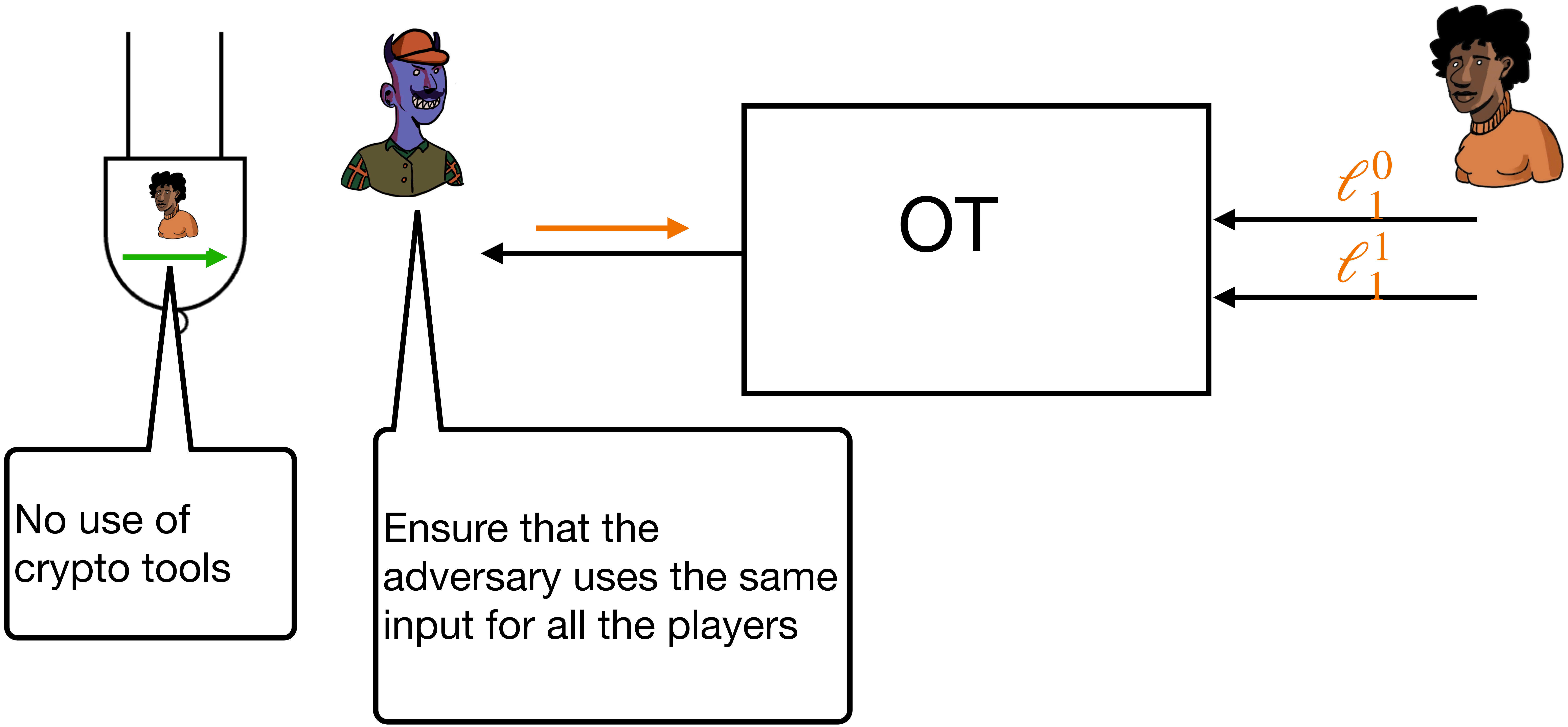
Our Approach: How to Build

Subtleties



Our Approach:
How to Build

Subtleties



Conclusion

We gave the first black-box round-optimal MPC protocol for any functionality assuming polynomial-time assumptions

Open questions

- Black box use of semi-honest OT? OR 4-round malicious OT
- What about identifiable abort?

Conclusion

We gave the first black-box round-optimal MPC protocol for any functionality assuming polynomial-time assumptions

Open questions

- Black box use of semi-honest OT? OR 4-round malicious OT
- What about identifiable abort?

THANKS!