Round-optimal Honest-majority MPC in Minicrypt and with Everlasting Security

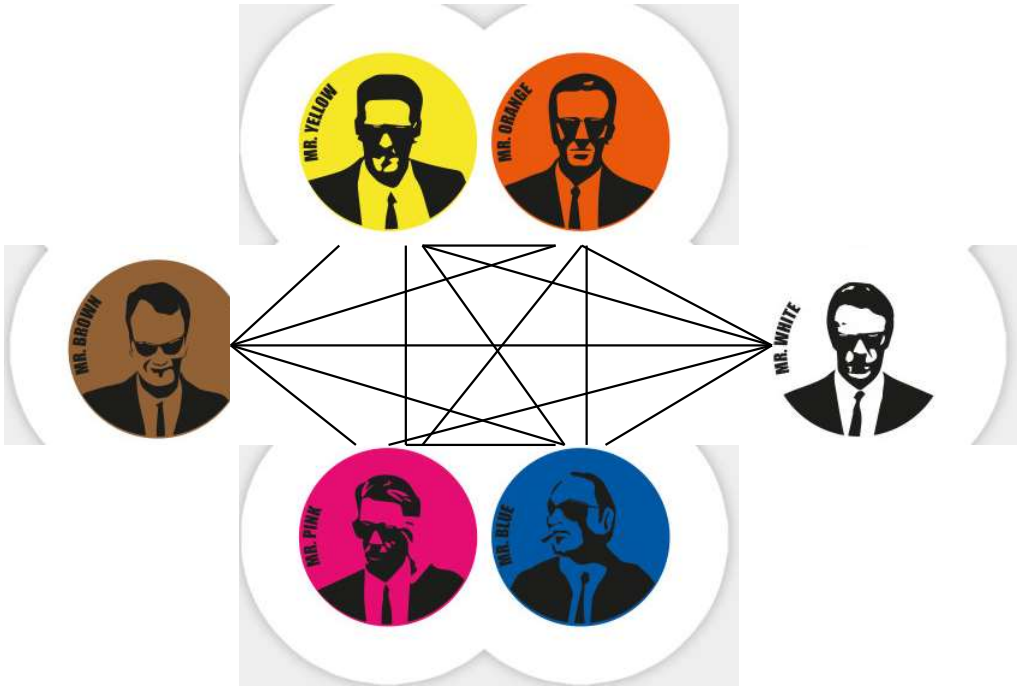
Benny Applebaum

Eliran Kachlon

Arpita Patra

Multiparty Computation

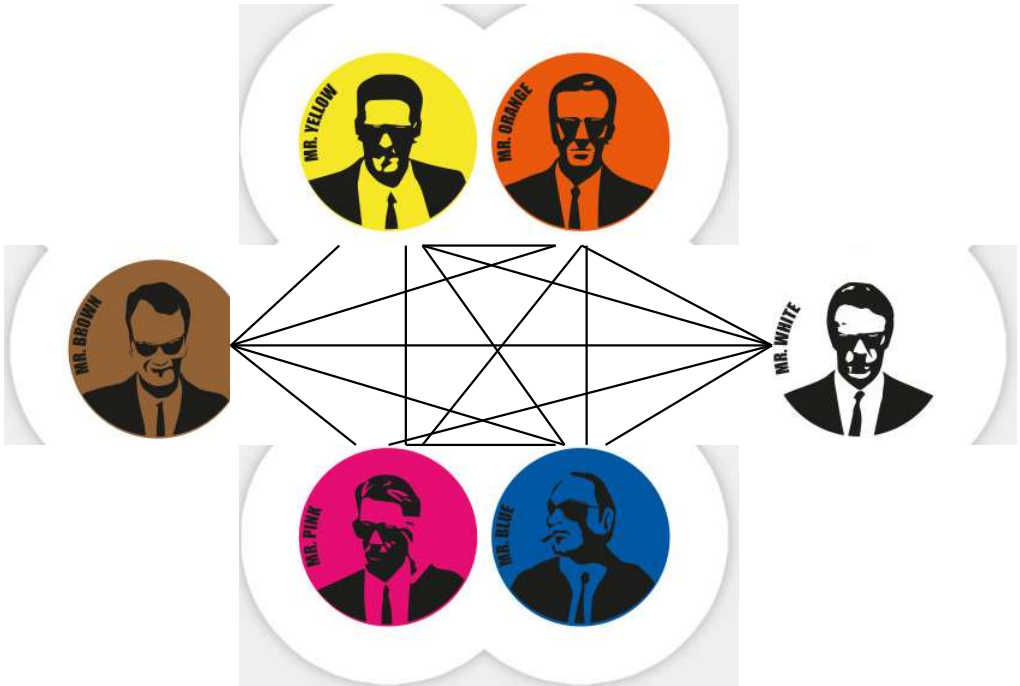
The model:



Multiparty Computation

The model:

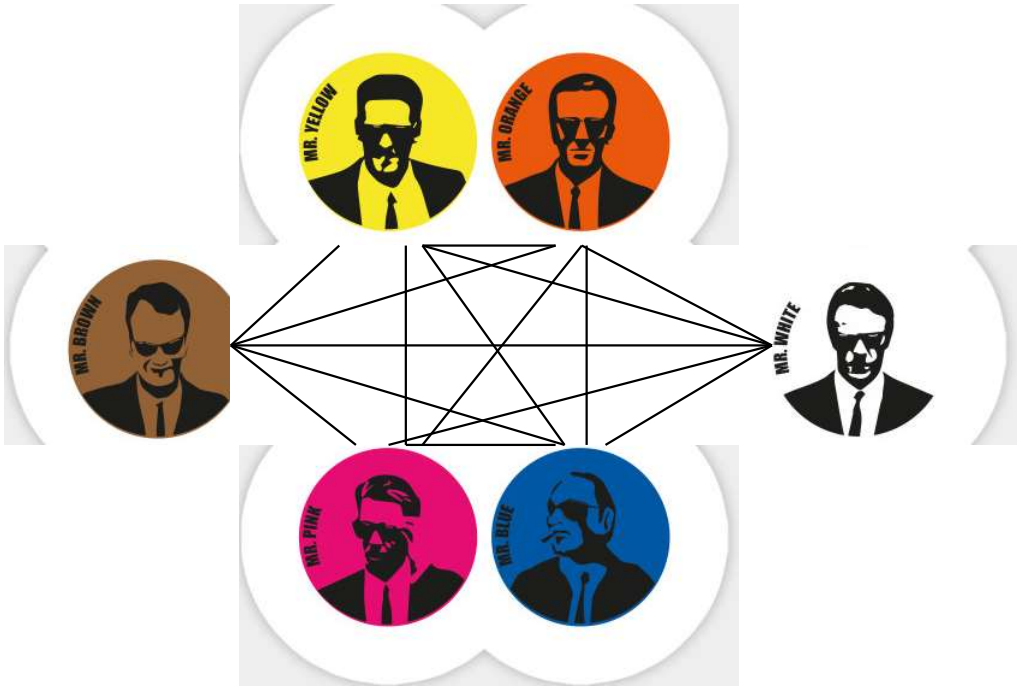
- N parties



Multiparty Computation

The model:

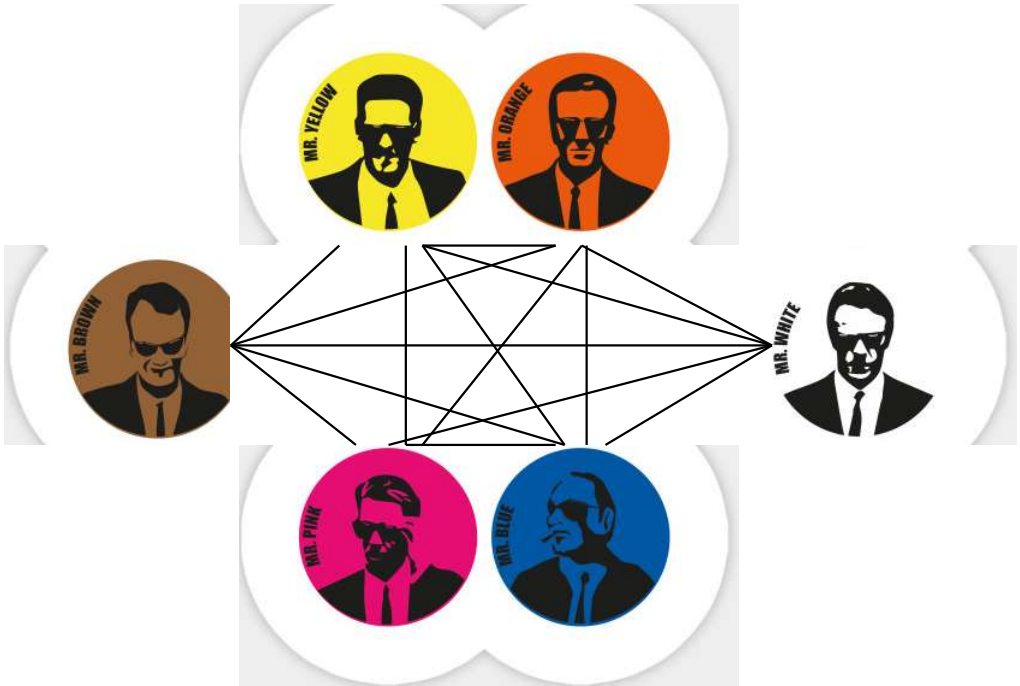
- N parties
- point-to-point private channels



Multiparty Computation

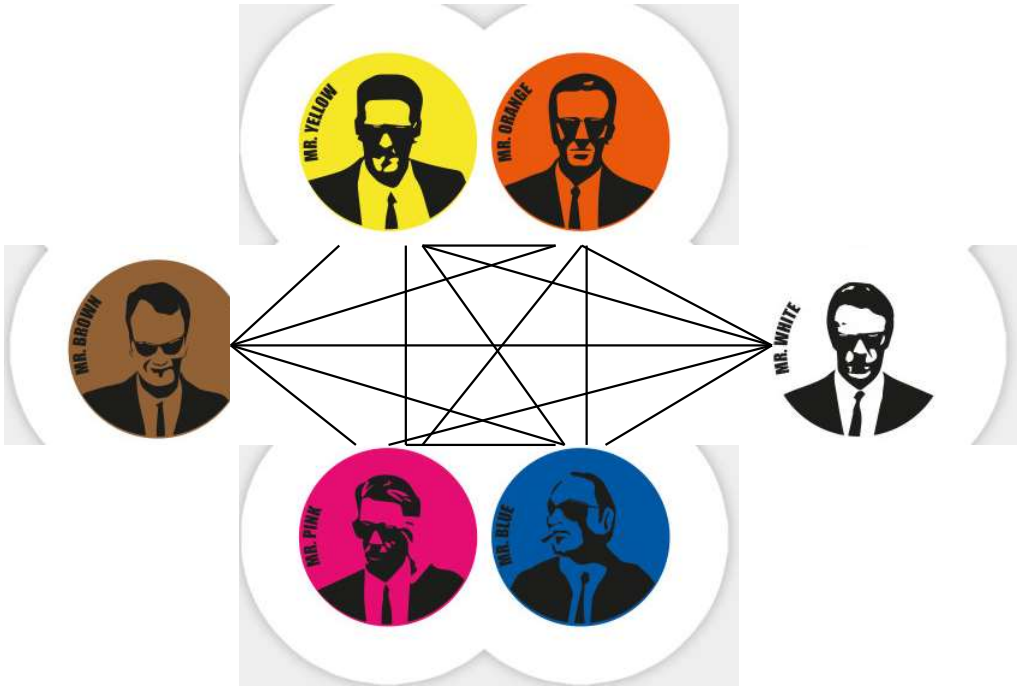
The model:

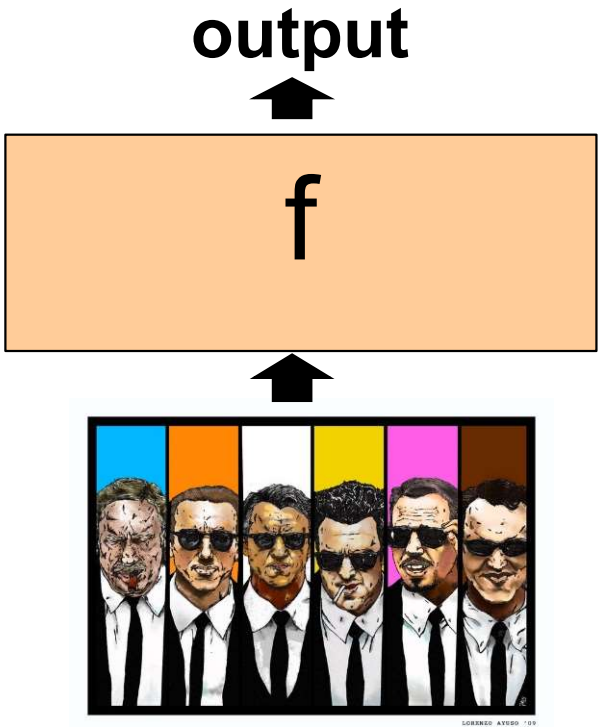
- N parties
- point-to-point private channels
- Broadcast



Multiparty Computation

Computational security:

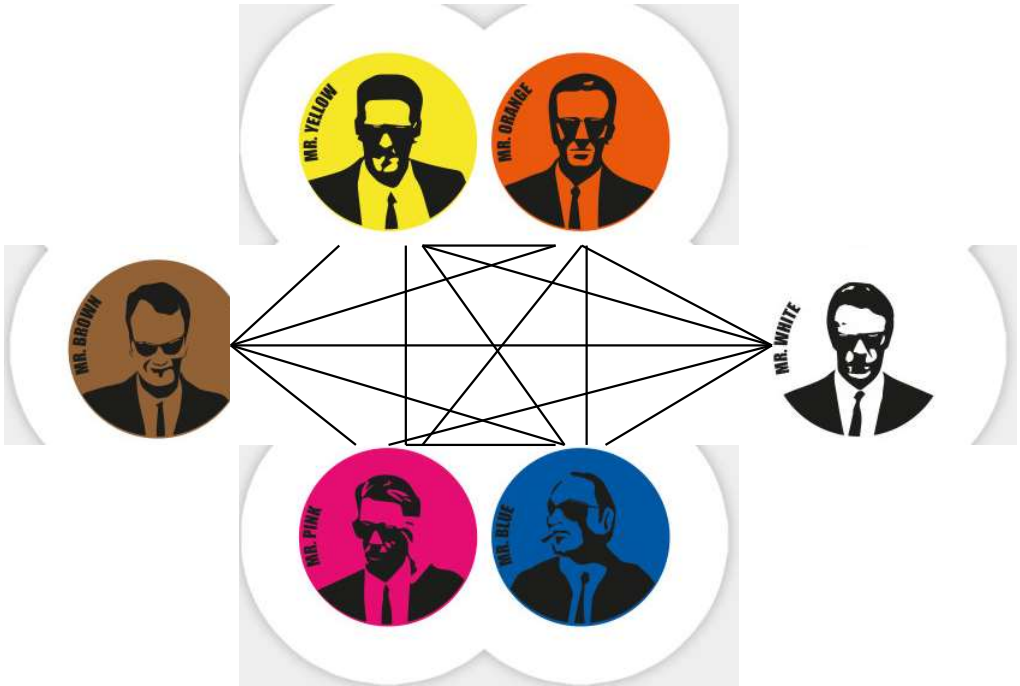


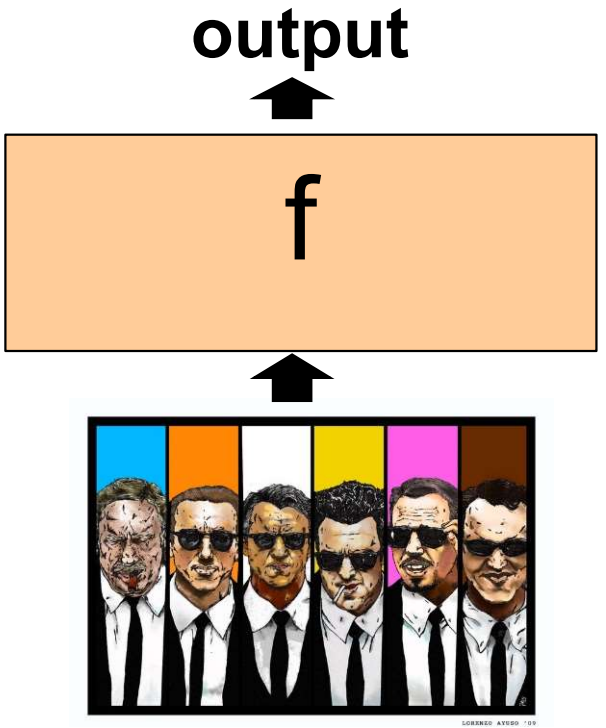


Multiparty Computation

Computational security:

- computationally-bounded adversary

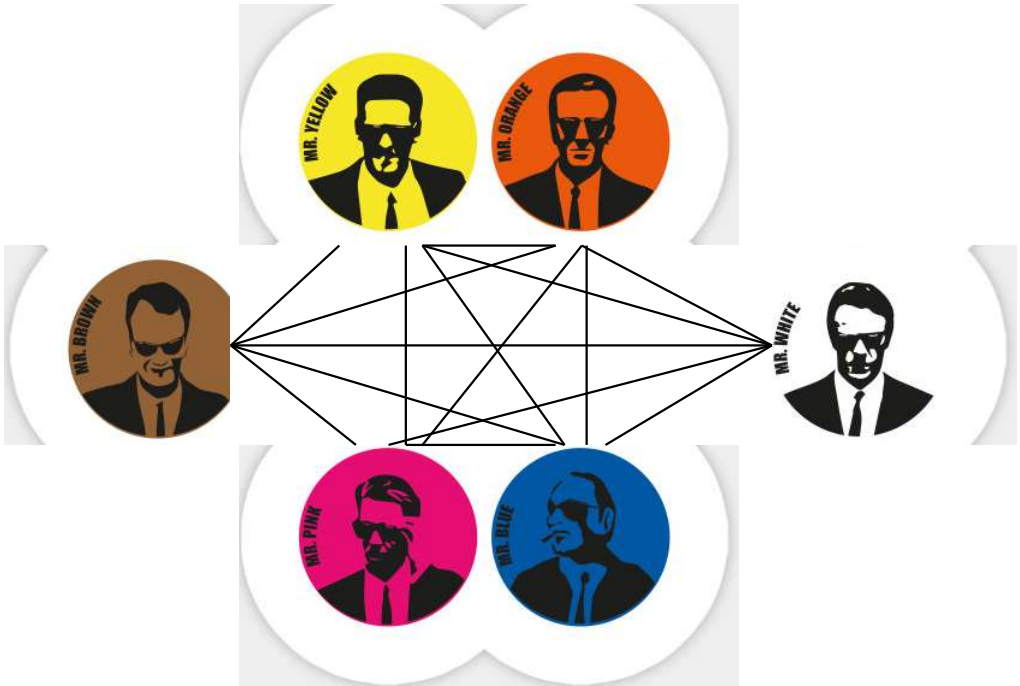


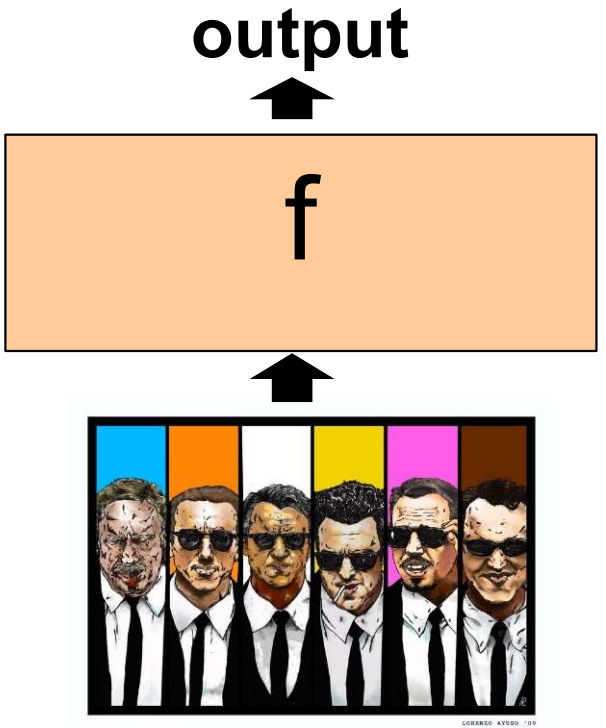


Multiparty Computation

Computational security:

- computationally-bounded adversary
- controls up to T<N/2 parties

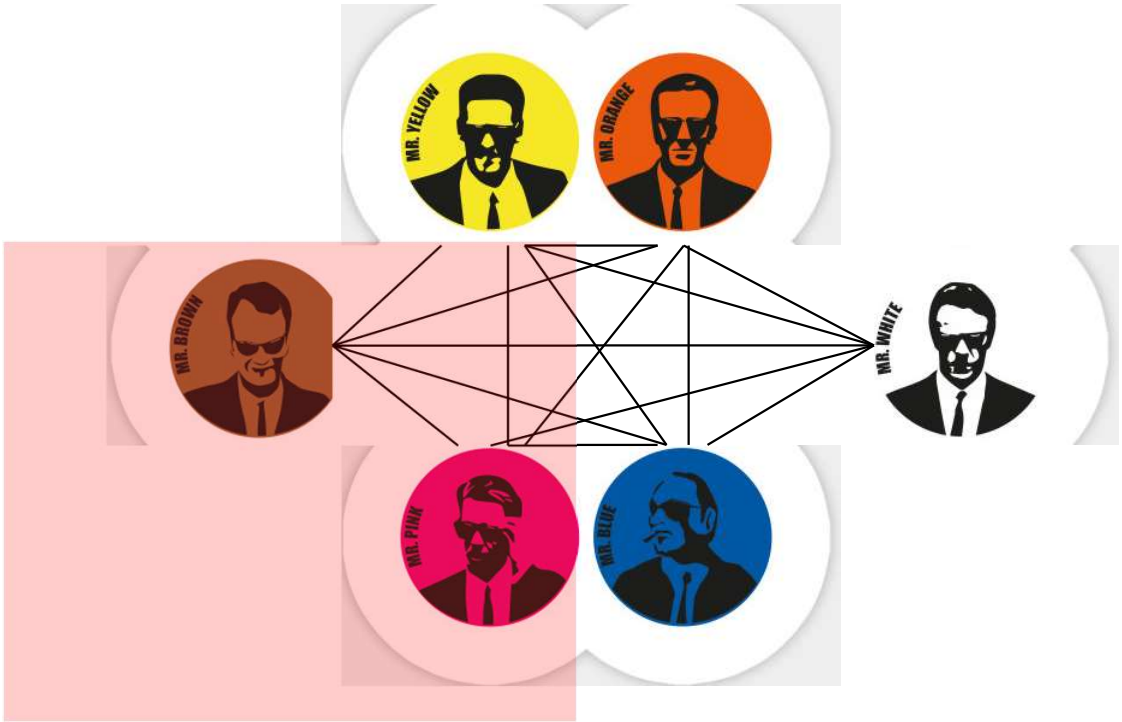


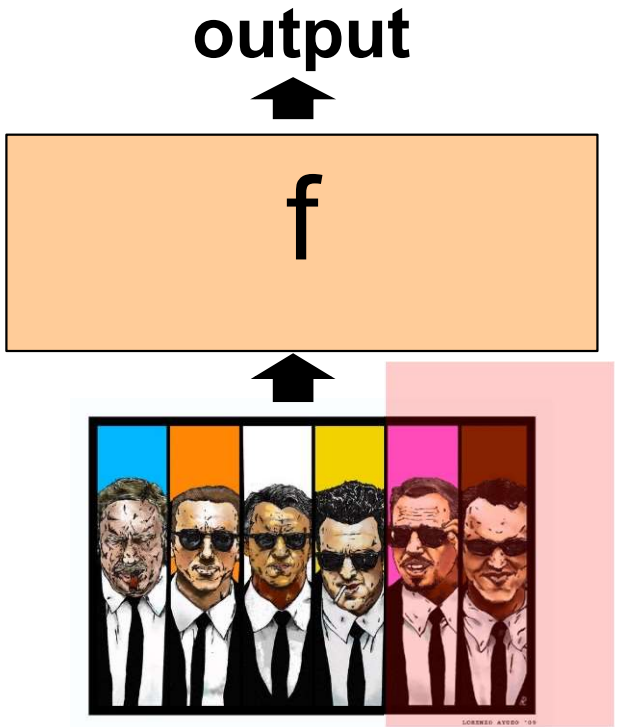


Multiparty Computation

Computational security:

- computationally-bounded adversary
- controls up to T<N/2 parties

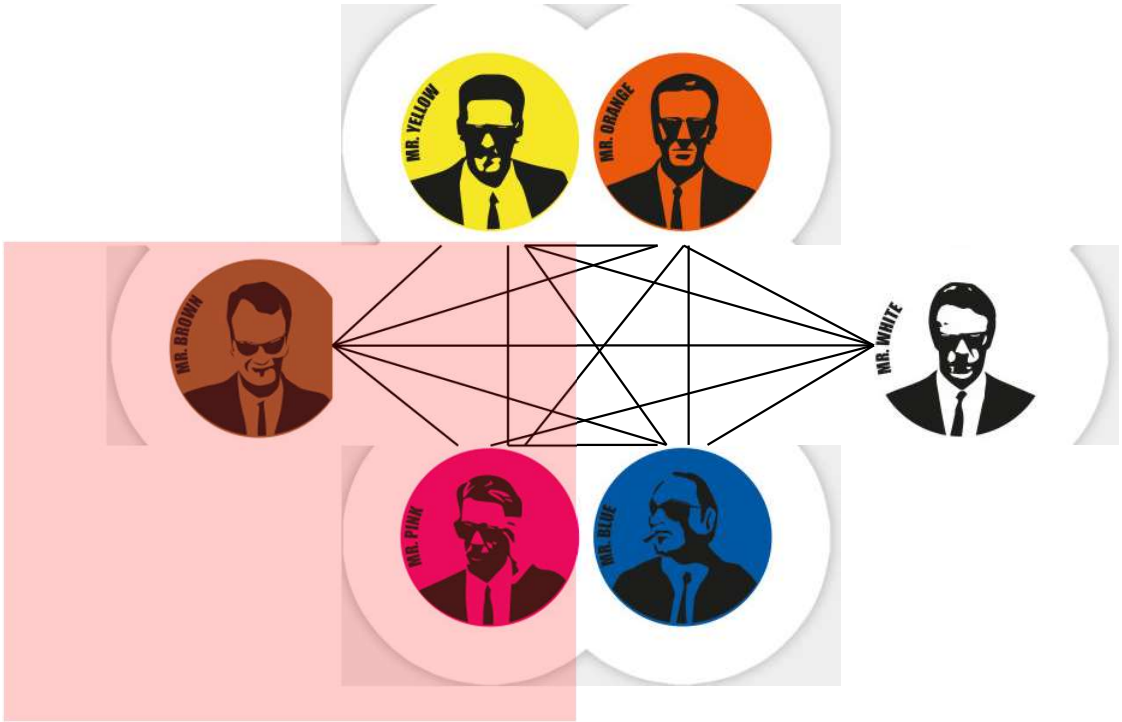


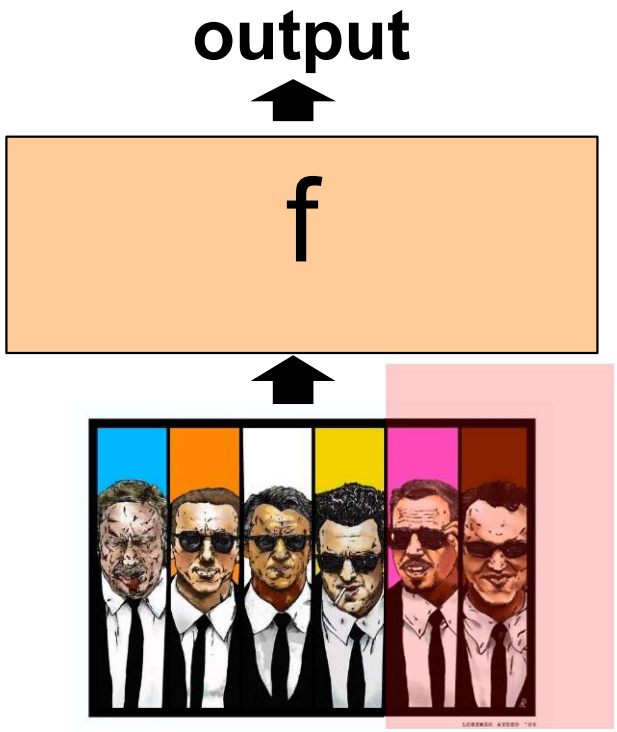


Multiparty Computation

Computational security:

- computationally-bounded adversary
- controls up to T<N/2 parties
- active (Byzantine)

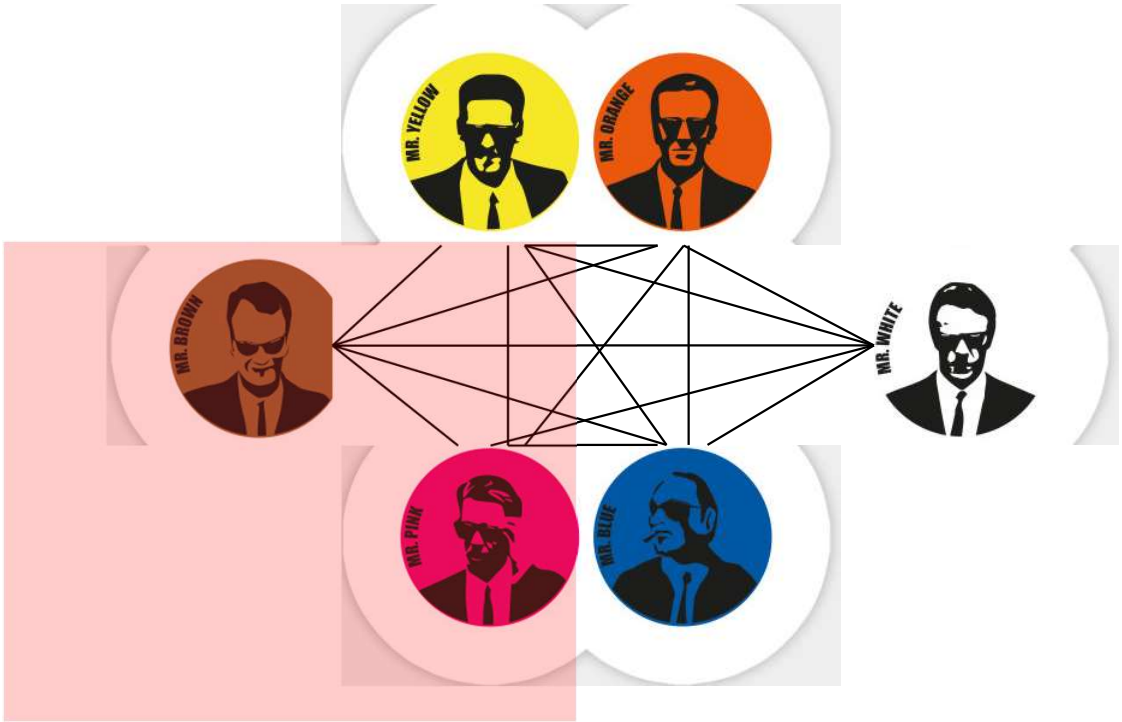


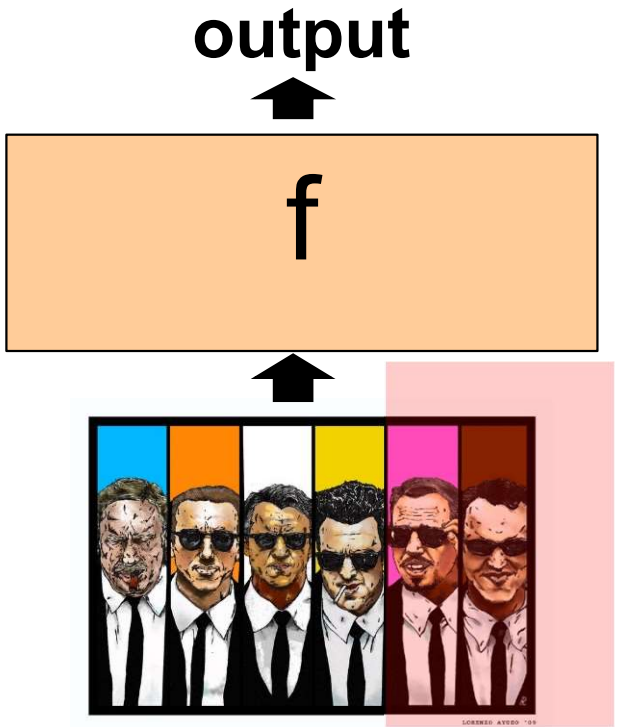


Multiparty Computation

Computational security:

- computationally-bounded adversary
- controls up to T<N/2 parties
- active (Byzantine)
- Full security (including GOD)





Round Complexity

How many rounds of interaction are required?

Round Complexity

How many rounds of interaction are required?

Lower Bound [GIKR02]:

No 2-round protocol for general MPC.

[Gennaro, Ishai, Kushilevitz, Rabin]

Round Complexity

How many rounds of interaction are required?

Lower Bound [GIKR02]:

No 2-round protocol for general MPC.

Upper Bounds:

3 rounds	CRS	Threshold FHE (LWE)	[GLS15]

[Gordon, Liu, Shi]

Round Complexity

How many rounds of interaction are required?

Lower Bound [GIKR02]:

No 2-round protocol for general MPC.

Upper Bounds:

3 rounds	CRS	Threshold FHE (LWE)	[GLS15]
3 rounds	plain	Threshold FHE (LWE)	[BJMS20]

[Badrinarayanan, Jain, Manohar, Sahai]

Round Complexity

How many rounds of interaction are required?

Lower Bound [GIKR02]:

No 2-round protocol for general MPC.

Upper Bounds:

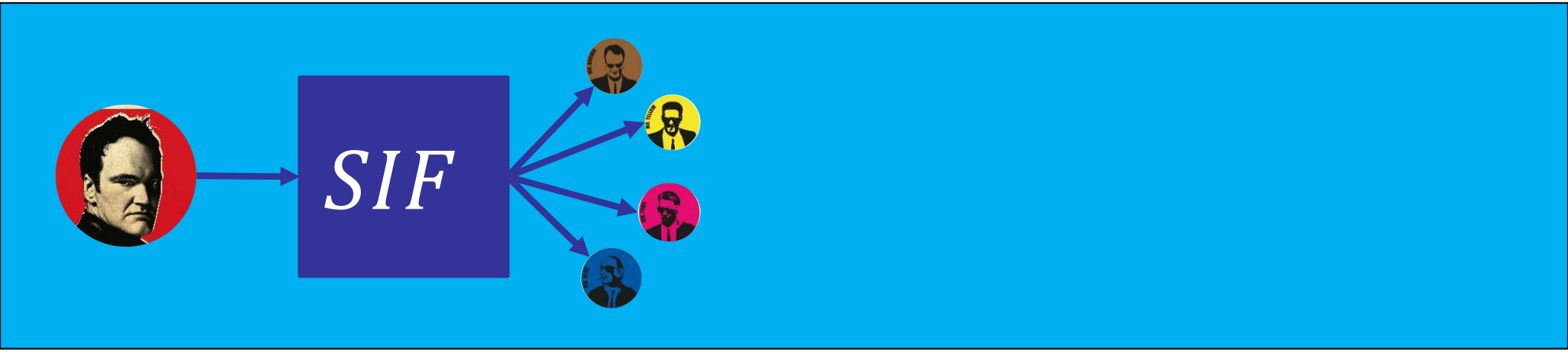
3 rounds	CRS	Threshold FHE (LWE)	[GLS15]
3 rounds	plain	Threshold FHE (LWE)	[BJMS20]
3 rounds	plain	PKE+NIZK	[ACGJ18]

[Ananth, Choudhuri, Goel, Jain]

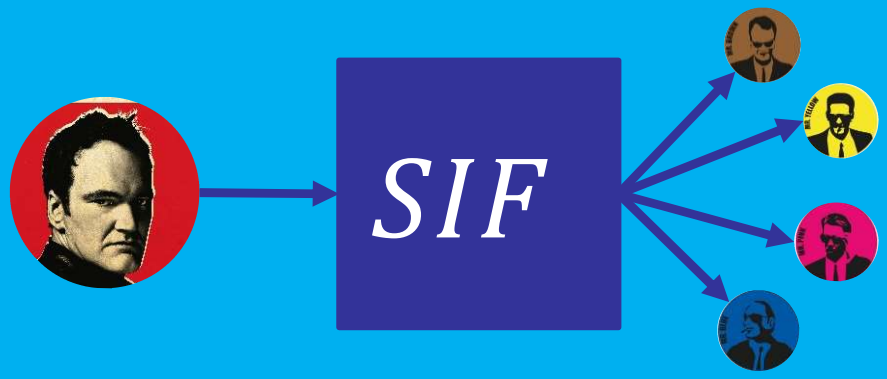
Round Complexity

Round-optimal MPC from **Minicrypt**-type assumptions?

Main Result: Compiler



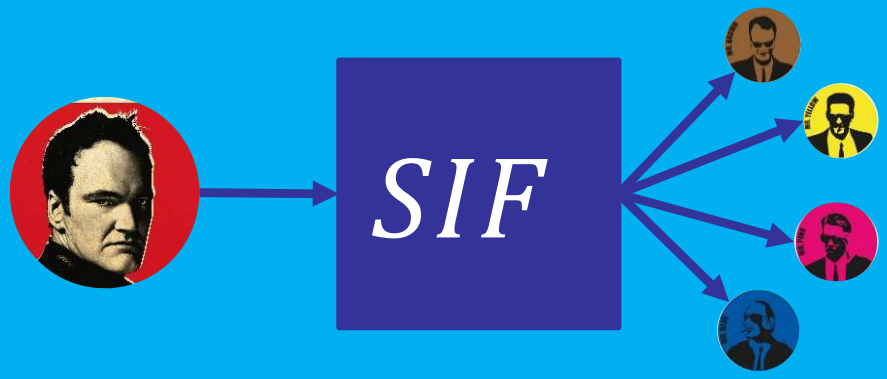
Main Result: Compiler



2-round protocol:

- 1 offline round
- 1 online round

Main Result: Compiler

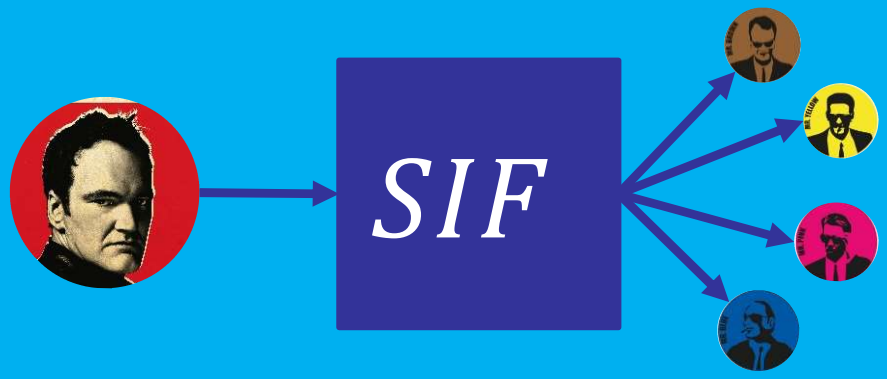


2-round protocol:

- 1 offline round
- 1 online round

Non-interactive commitments

Main Result: Compiler



2-round protocol:

- 1 offline round
- 1 online round

Non-interactive commitments

3 round general MPC protocol

Compilation

Assuming **non-interactive commitments*** [AKP22]

2-round SIF (online/offline)

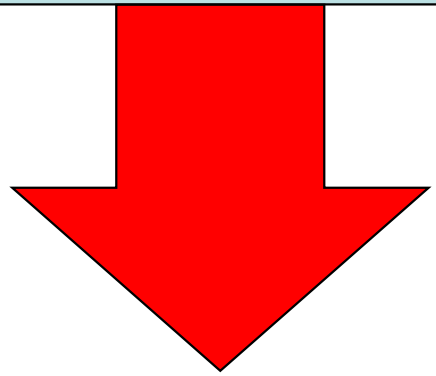
- Constant #parties – honest majority $t < \frac{1}{2}n$.
- Polynomial #parties – almost honest majority $t < 0.499n$.

Compilation

Assuming **non-interactive commitments*** [AKP22]

2-round SIF (online/offline)

- Constant #parties – honest majority $t < \frac{1}{2}n$.
- Polynomial #parties – almost honest majority $t < 0.499n$.



Assuming **non-interactive commitments***

3-round general MPC

- Constant #parties – honest majority $t < \frac{1}{2}n$.
- Polynomial #parties – almost honest majority $t < 0.499n$.

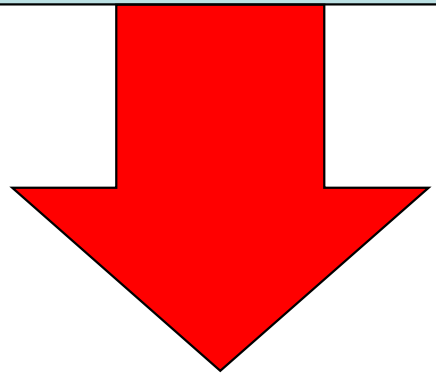
Compilation

Assuming **non-interactive commitments*** [AKP22]

2-round SIF (online/offline)

Constant #parties – honest majority $t < \frac{1}{2}n$.

Polynomial #parties – almost honest majority $t < 0.499n$.



Assuming **non-interactive commitments***

3-round general MPC

Constant #parties – honest majority $t < \frac{1}{2}n$.

Polynomial #parties – almost honest majority $t < 0.499n$.

Computationally-hiding NICOM

[A**K**P22] requires security against selective-opening attacks.

Computationally-hiding NICOM

[A**K**P22] requires security against selective-opening attacks.

Can be based on Minicrypt-type assumptions:

- 1-1 OWFs with sub-exp hardness [Blum81, Yao82, GL89]
- OWFs with sub-exp hardness + CRS [Naor91]
- OWFs with sub-exp hardness + derand. assumptions [BOV03]

Statistically-hiding NICOM

Statistically-hiding NICOM

Provide **everlasting security** for $NC1$ circuits**:**

Adversary is bounded during the execution

but computationally *unbounded* after the execution

Statistically-hiding NICOM

Provide **everlasting security** for $NC1$ circuits**:**

Adversary is bounded during the execution

but computationally *unbounded* after the execution

Based on **collision-resistant hash-function** [HM96, DPP98]

Statistically-hiding NICOM

Provide **everlasting security** for $NC1$ circuits**:**

Adversary is bounded during the execution

but computationally *unbounded* after the execution

Based on **collision-resistant hash-function** [HM96, DPP98]

How to select the hash function?

Statistically-hiding NICOM

Provide **everlasting security** for $NC1$ circuits**:**

Adversary is bounded during the execution

but computationally *unbounded* after the execution

Based on **collision-resistant hash-function** [HM96, DPP98]

How to select the hash function?

- Common random string

Statistically-hiding NICOM

Provide **everlasting security** for $NC1$ circuits**:**

Adversary is bounded during the execution

but computationally *unbounded* after the execution

Based on **collision-resistant hash-function** [HM96, DPP98]

How to select the hash function?

- Common random string
- Additional offline round

Statistically-hiding NICOM

Provide **everlasting security** for $NC1$ circuits**:**

Adversary is bounded during the execution

but computationally *unbounded* after the execution

Based on **collision-resistant hash-function** [HM96, DPP98]

How to select the hash function?

- Common random string
- Additional offline round
- Fixed function for uniform adversary

The Construction

Outline

Outline

- 2-round semi-malicious for general MPC.

Outline

- 2-round semi-malicious for general MPC.
  - Play honestly, can choose input and rand.

Outline

- 2-round semi-malicious for general MPC.
  - Play honestly, can choose input and rand.
- 3-round fail-stop.

Outline

- 2-round semi-malicious for general MPC.
  - Play honestly, can choose input and rand.
- 3-round fail-stop.
  - Play honestly, can abort at any time.

Outline

- 2-round semi-malicious for general MPC.
  - Play honestly, can choose input and rand.
- 3-round fail-stop.
  - Play honestly, can abort at any time.
- 3-round active.

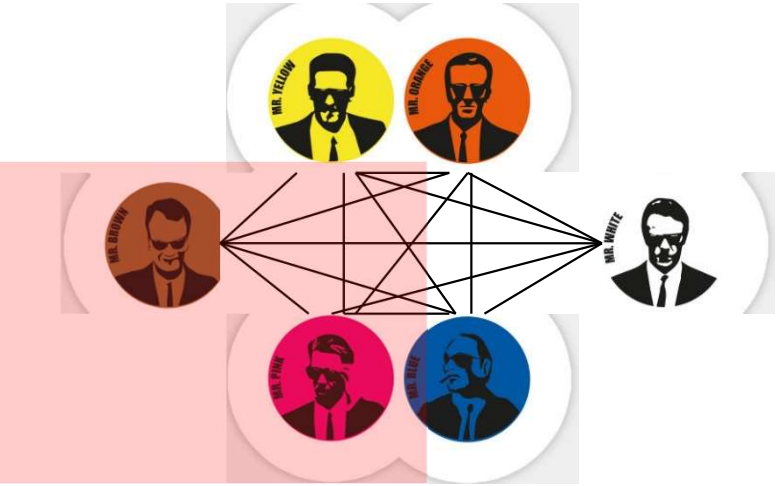
Outline

- 2-round semi-malicious for general MPC.
  - Play honestly, can choose input and rand.
- 3-round fail-stop.
  - Play honestly, can abort at any time.
- 3-round active.

- IT variant of [ACGJ18]

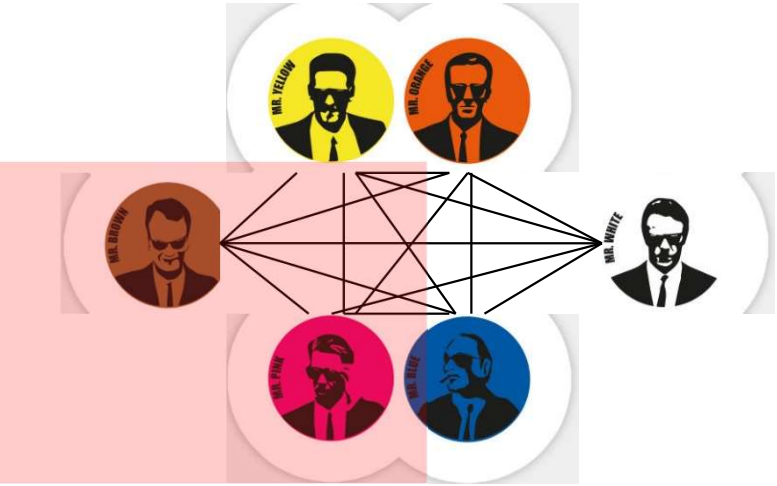
2-round Semi malicious

Round 1:
private channels

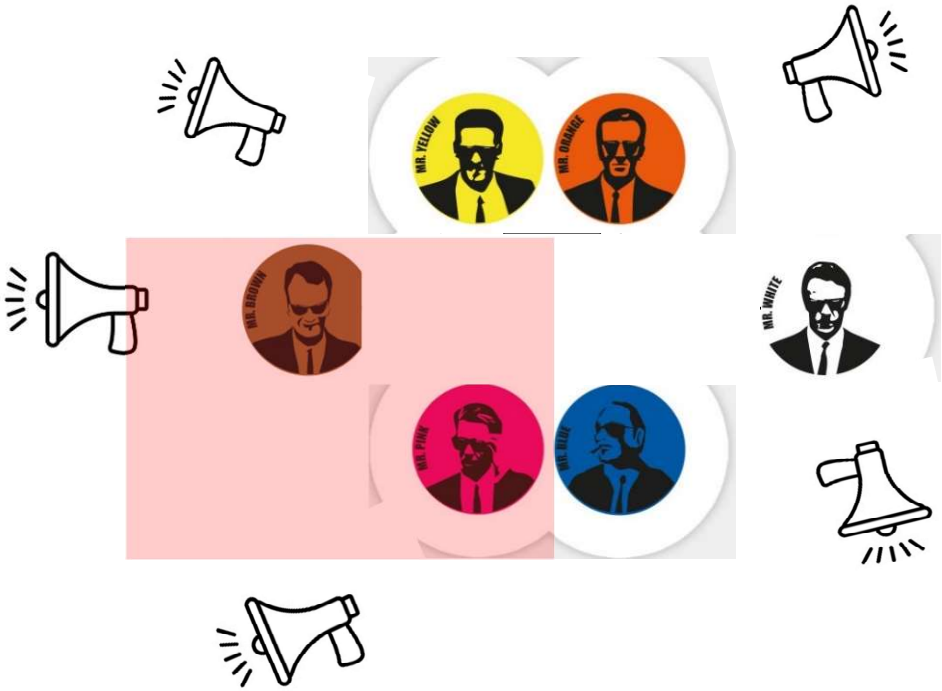


2-round Semi malicious

Round 1:
private channels



Round 2:
Broadcast channel

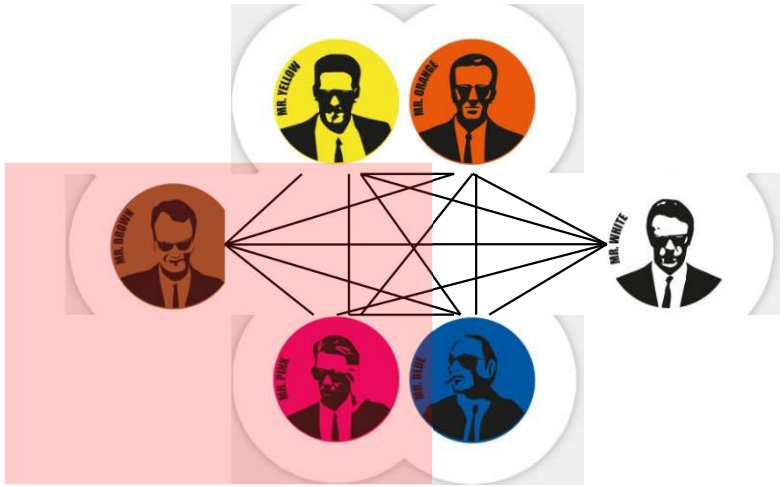


Outline

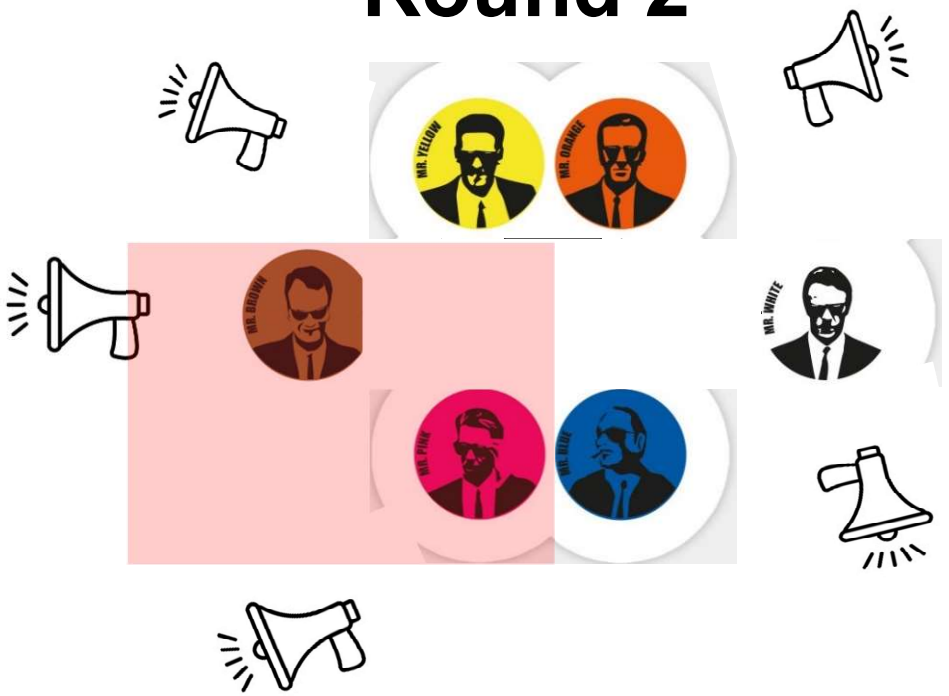
- ~~2-round semi-malicious.~~
- 3-round fail-stop.
- 3-round active.

Fail-stop Adversary

Round 1



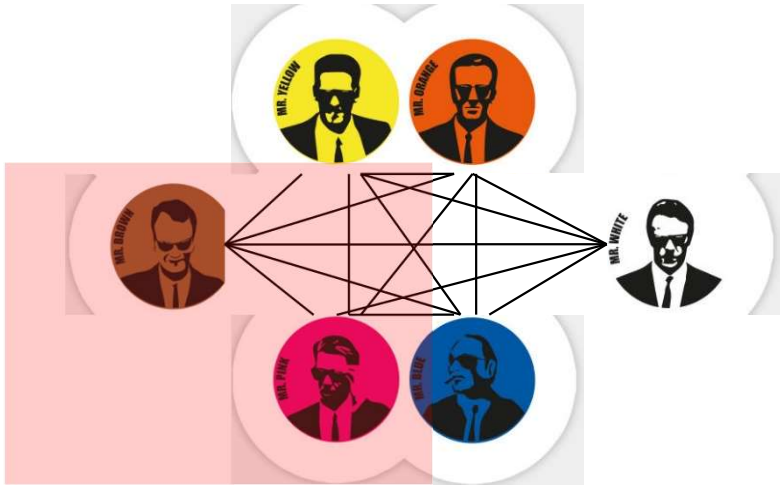
Round 2



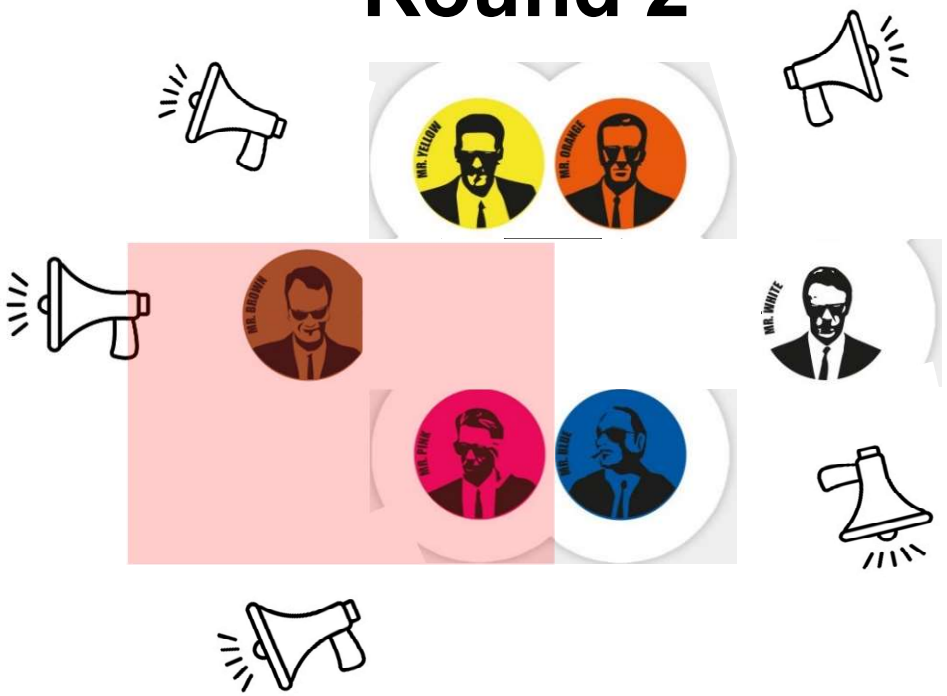
Fail-stop Adversary

- First-round aborts

Round 1



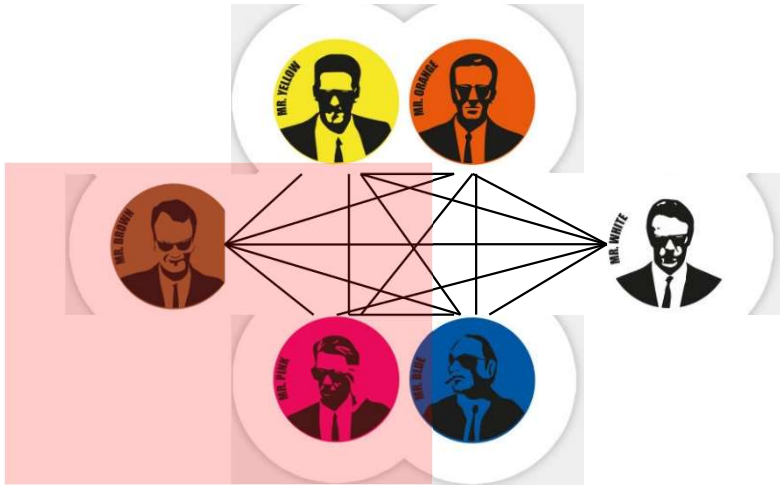
Round 2



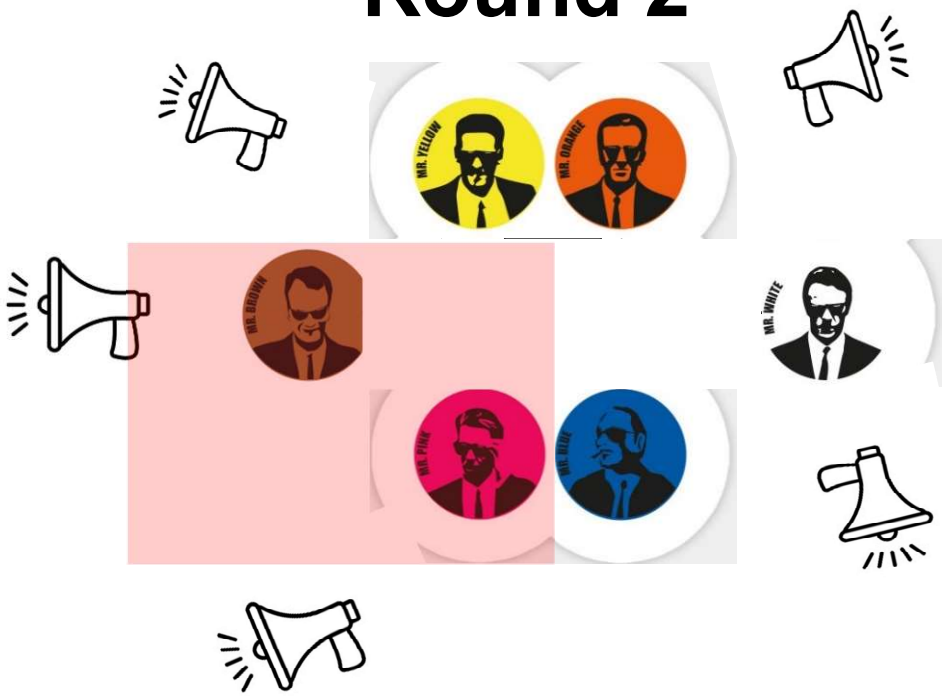
Fail-stop Adversary

- First-round aborts
- Second-round aborts

Round 1



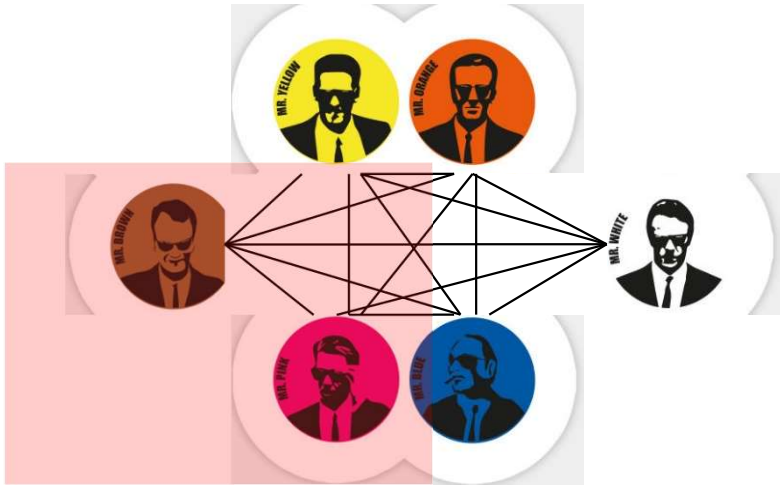
Round 2



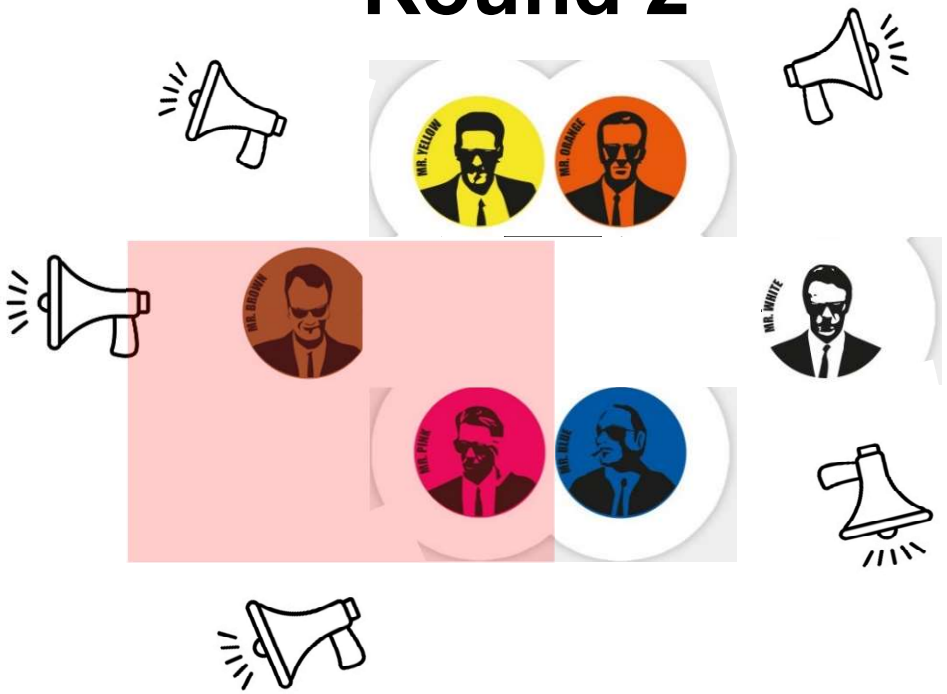
Fail-stop Adversary

- ~~First-round aborts~~
- Second-round aborts

Round 1



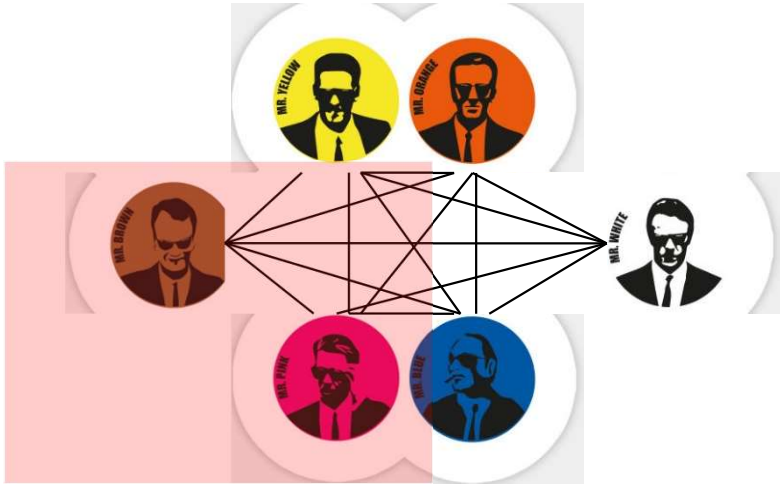
Round 2



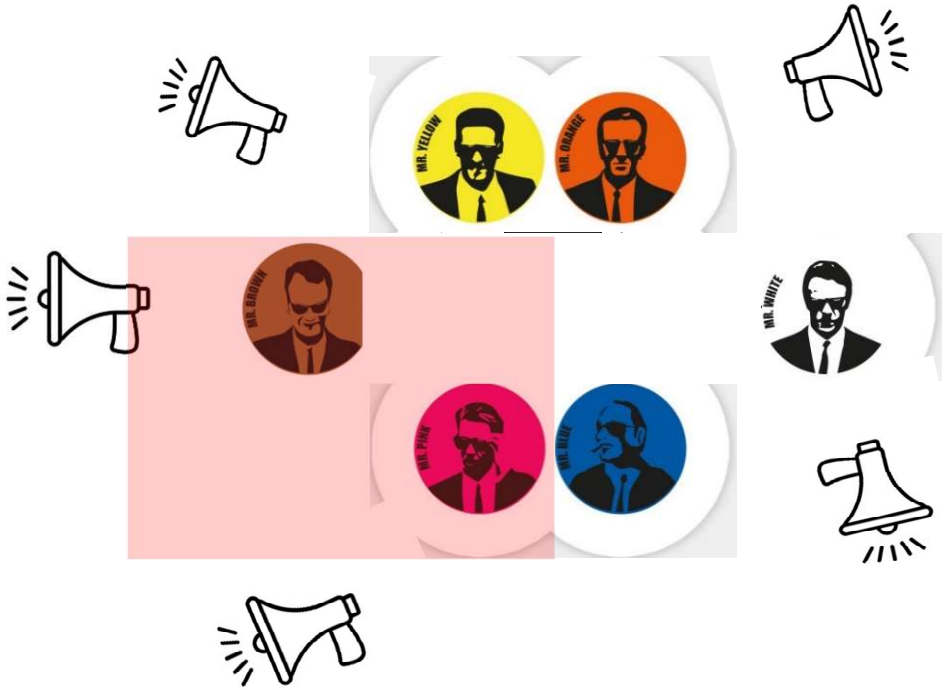
Second-round Fail-stop

Second-round Fail-stop

Round 1

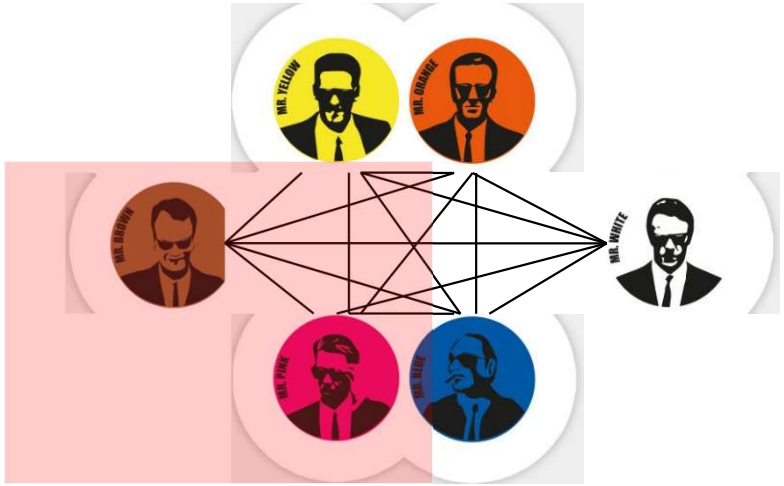


Round 2

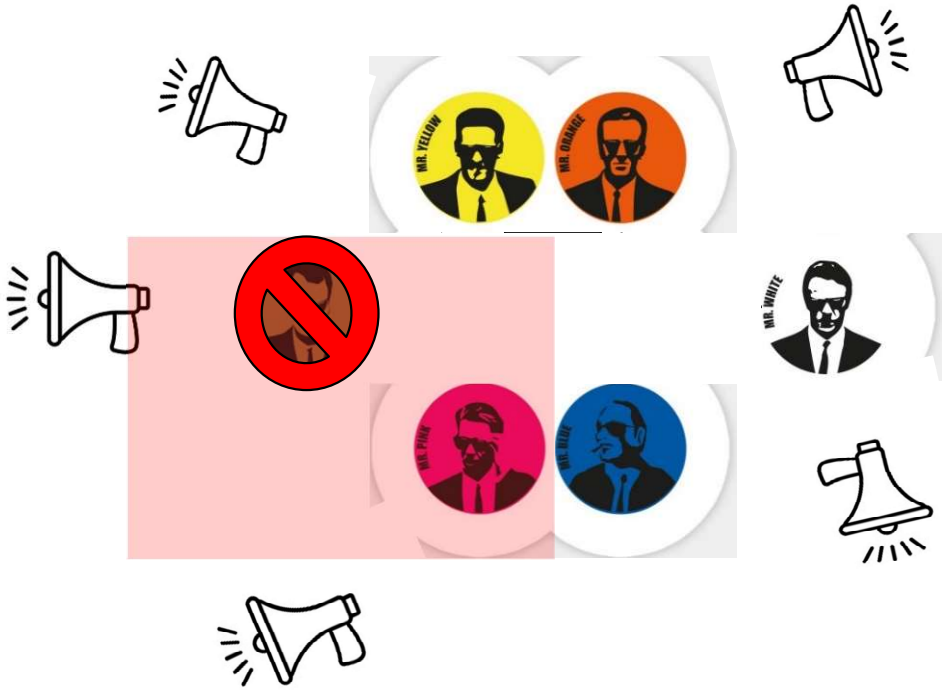


Second-round Fail-stop

Round 1



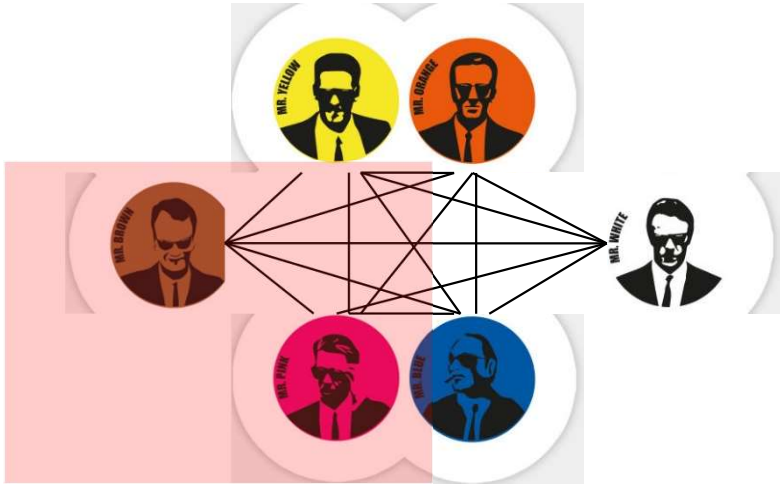
Round 2



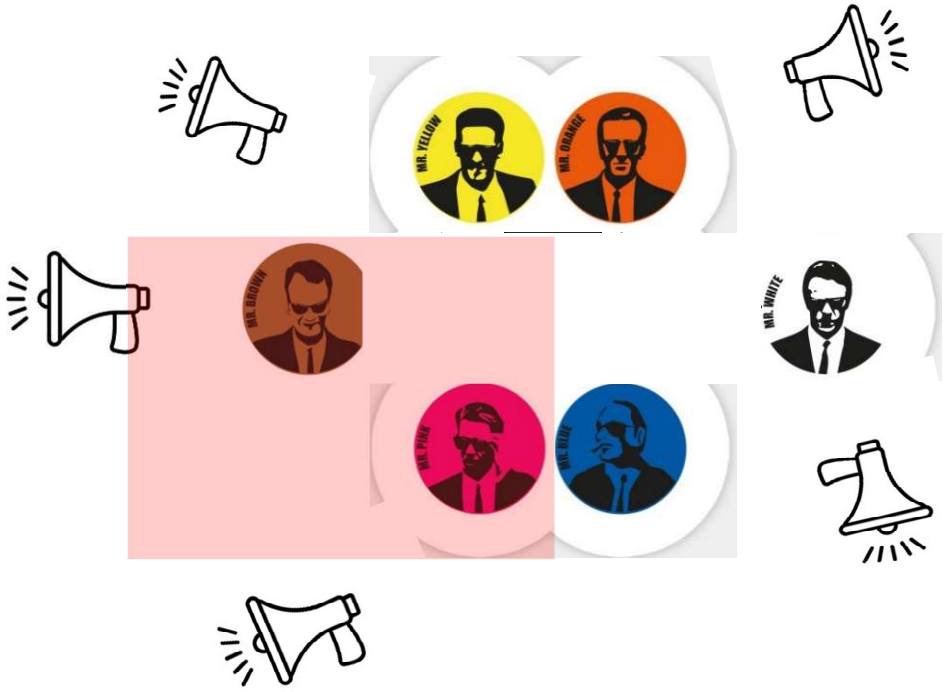
Second-round Fail-stop

Step I: public communication.

Round 1



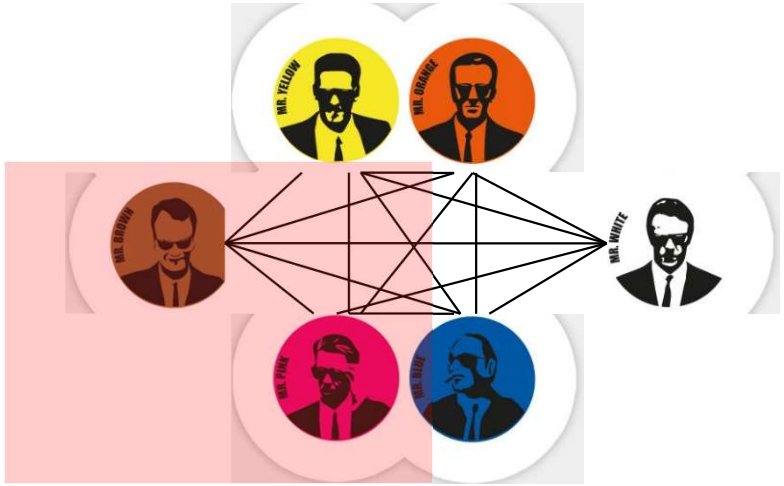
Round 2



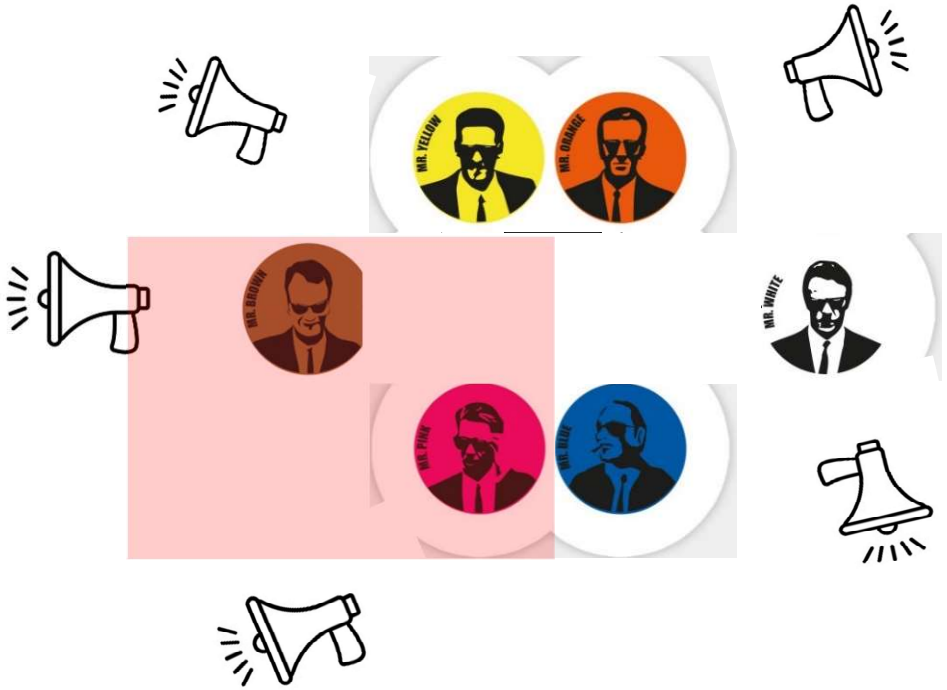
Second-round Fail-stop

Step I: public communication.
Step II: Forcing broadcast.

Round 1



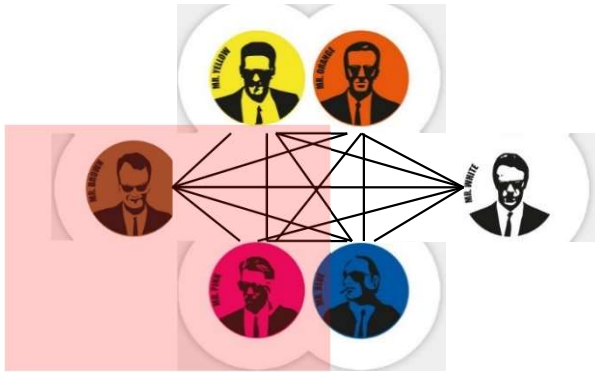
Round 2



Second-round Fail-stop

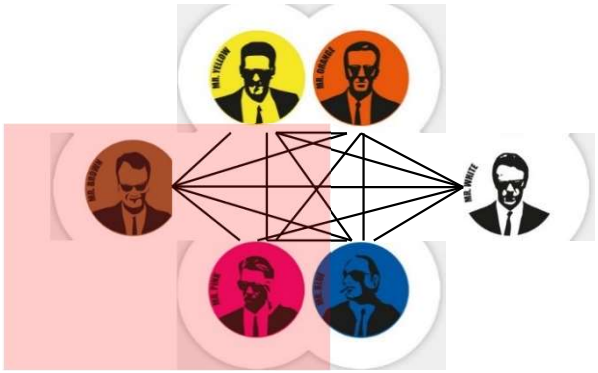
Step I: public communication.

Round 0

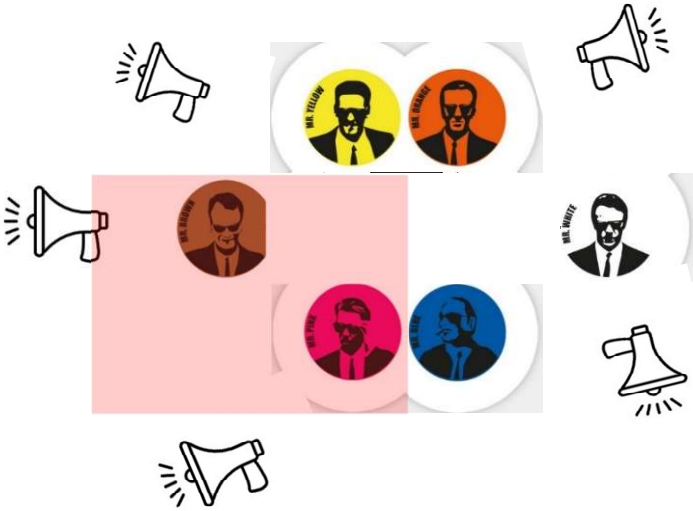


Exchange one-time pads

Round 1



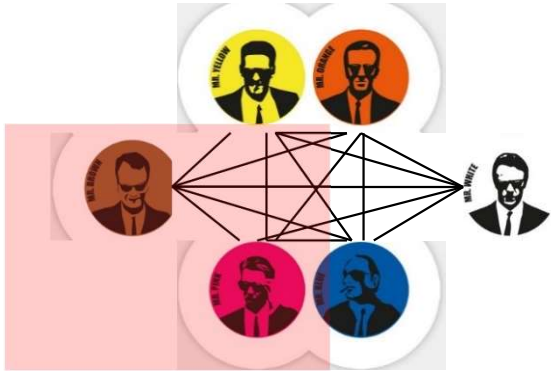
Round 2



Second-round Fail-stop

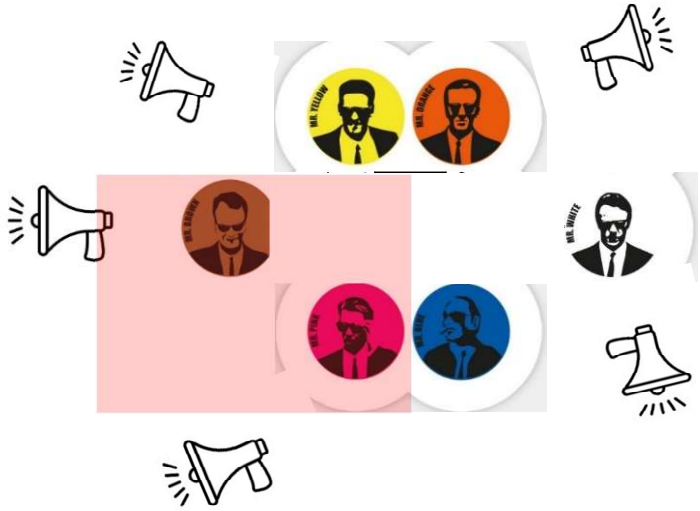
Step I: public communication.

Round 0

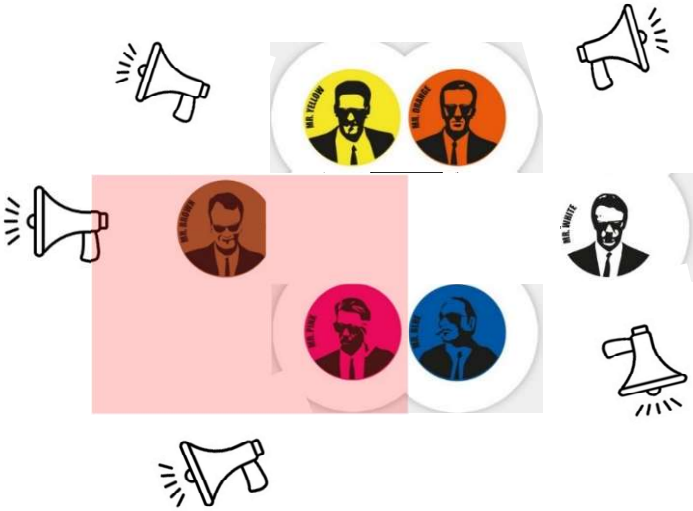


Exchange one-time pads

Round 1



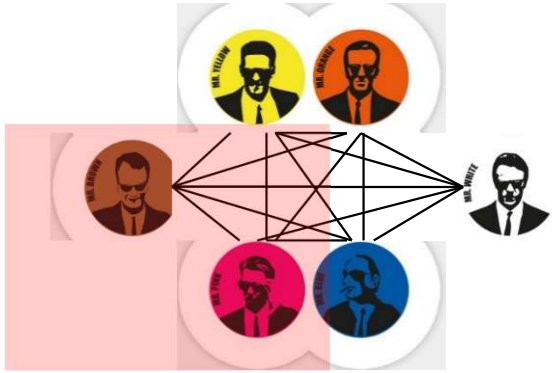
Round 2



Second-round Fail-stop

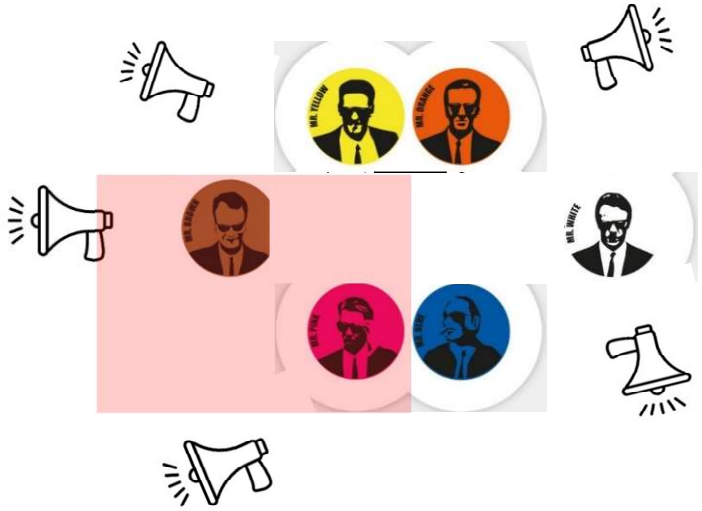
Step I: public communication.

Round 0

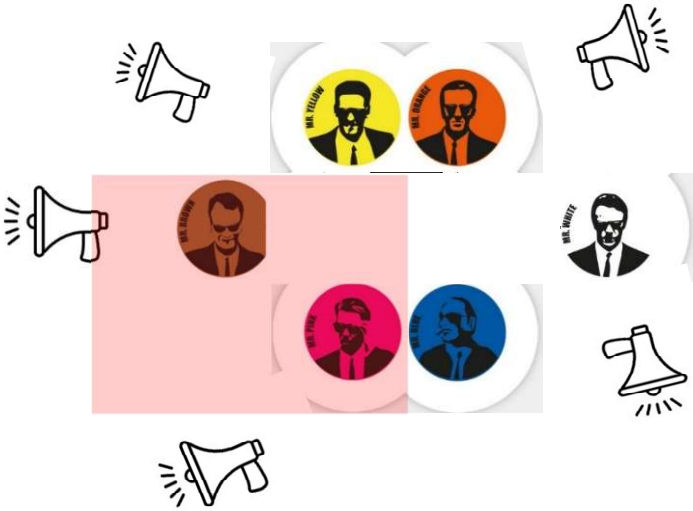


Exchange one-time pads

Round 1



Round 2



Previous works: public-key encryption.

Second-round Fail-stop

Step II: Forcing broadcast

Second-round Fail-stop

Step II: Forcing broadcast

Second-round Fail-stop

Step II: Forcing broadcast

- BC of Mr Brown is a function G_i of $\left(x_i, r_i, (\rho_{i,j})_j, (A_{j,i})_j\right)$

Second-round Fail-stop

Step II: Forcing broadcast

- BC of Mr Brown is a function $\boldsymbol{G_i}$ of $\left(x_i, r_i, (\rho_{i,j})_j, (A_{j,i})_j\right)$
- In Round 1, Mr. Brown generates a GC of $\boldsymbol{G_i}$.

Second-round Fail-stop

Step II: Forcing broadcast

- BC of Mr Brown is a function $\boldsymbol{G_i}$ of $\left(x_i, r_i, (\rho_{i,j})_j, (A_{j,i})_j\right)$
- In Round 1, Mr. Brown generates a GC of $\boldsymbol{G_i}$.
  - Labels of $(x_i, r_i, (\rho_{i,j})_j)$ are known in Round 1.

Second-round Fail-stop

Step II: Forcing broadcast

- BC of Mr Brown is a function $\boldsymbol{G_i}$ of $\left(x_i, r_i, (\rho_{i,j})_j, (A_{j,i})_j\right)$
- In Round 1, Mr. Brown generates a GC of $\boldsymbol{G_i}$.
  - Labels of $(x_i, r_i, (\rho_{i,j})_j)$ are known in Round 1.
  - Mr. Brown shares the labels of $(A_{j,i})_j$.

Second-round Fail-stop

Step II: Forcing broadcast

- BC of Mr Brown is a function G_i of $\left(x_i, r_i, (\rho_{i,j})_j, (A_{j,i})_j\right)$
- In Round 1, Mr. Brown generates a GC of G_i.
  - Labels of $(x_i, r_i, (\rho_{i,j})_j)$ are known in Round 1
  - Mr. Brown shares the labels of $(A_{j,i})_j$.
  - Correct labels of $(A_{j,i})_j$ recovered in Round 2.

Outline

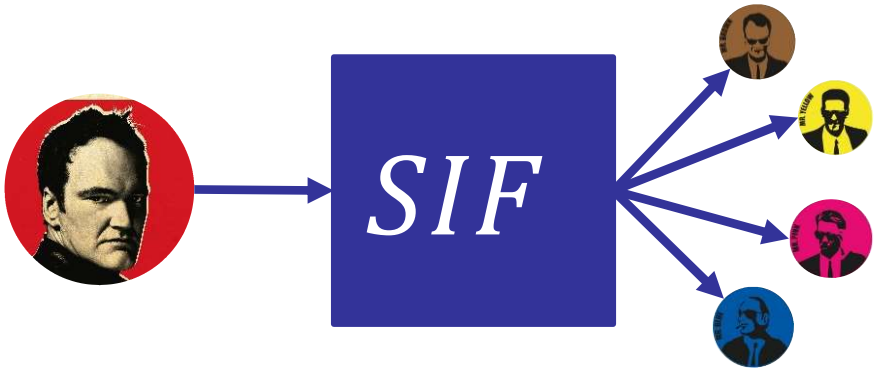
- ~~2-round semi-malicious.~~
- ~~3-round fail-stop.~~
- 3-round active.

Active Adversary

Main idea: Prove honest behaviour via zero-knowledge proofs

Active Adversary

Main idea: Prove honest behaviour via zero-knowledge proofs

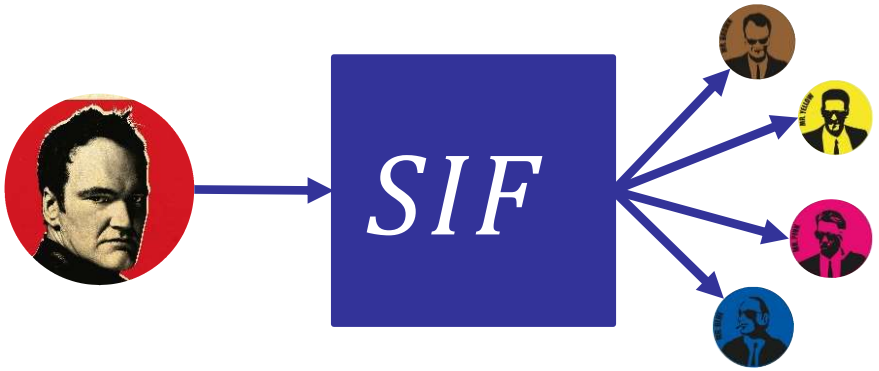


(x, w) $\quad if\ R(x, w) = 1 \quad Return\ (x, \text{true})$

$\quad\quad\quad\quad if\ R(x, w) = 0 \quad Return\ (x, \text{false})$

Active Adversary

Main idea: Prove honest behaviour via zero-knowledge proofs



(x, w) $\quad if\ R(x,w) = 1 \quad Return\ (x, \text{true})$

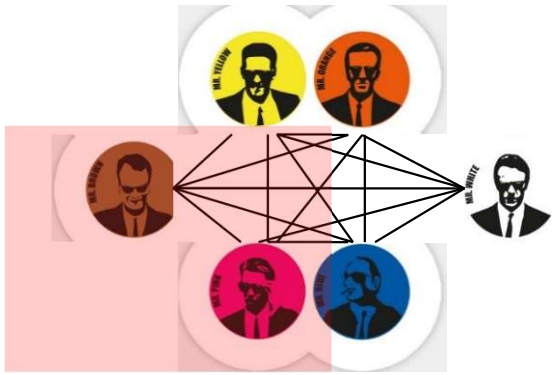
$\quad\quad\quad\quad if\ R(x,w) = 0 \quad Return\ (x, \text{false})$

2-round protocol:

- 1 offline round
- 1 online round

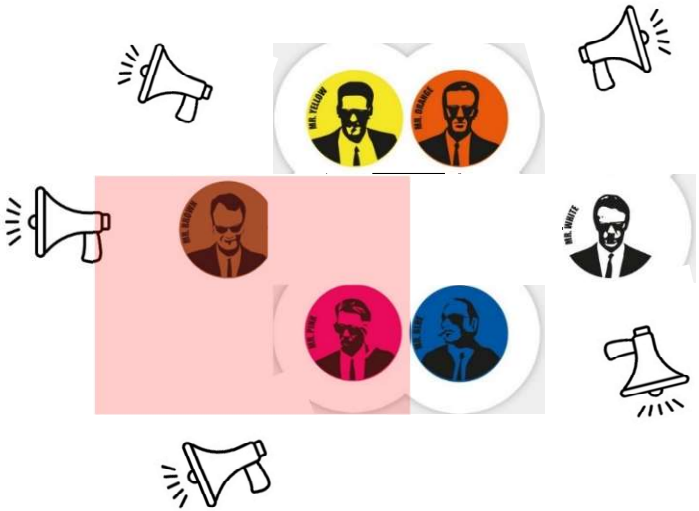
Active Adversary

Round 0

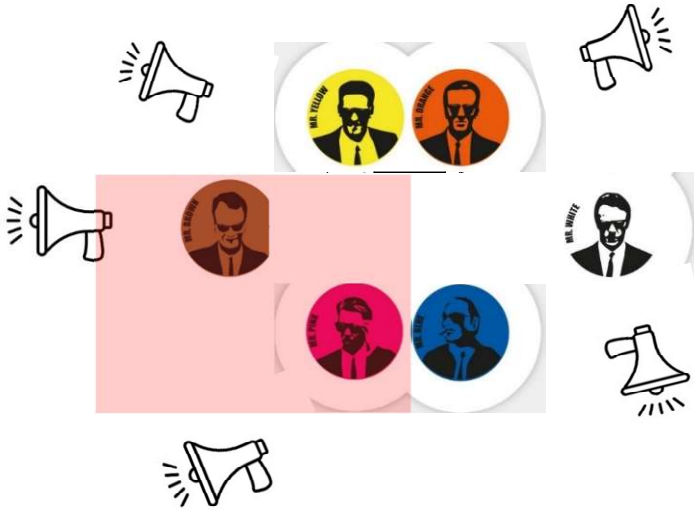


Exchange one-time pads

Round 1

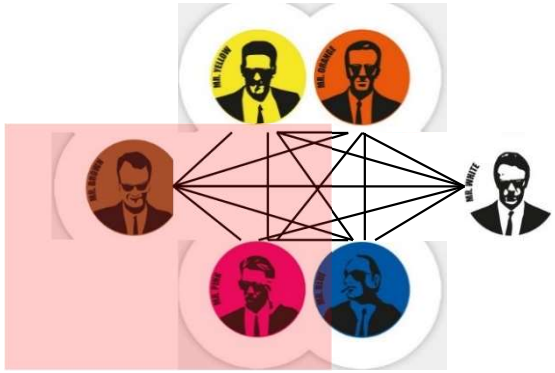


Round 2



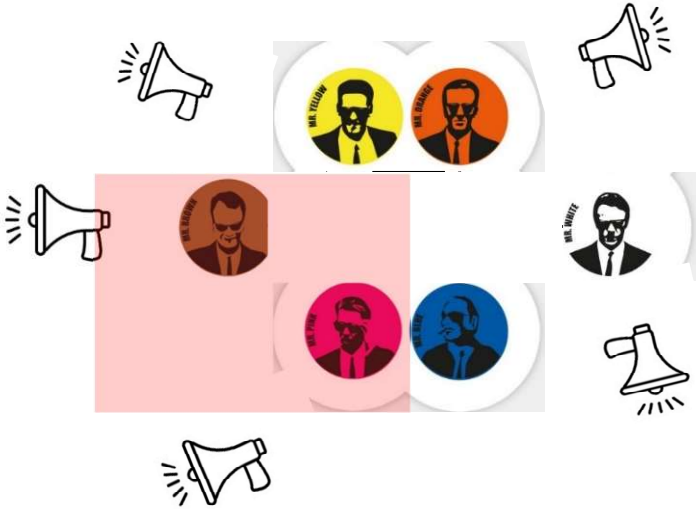
Active Adversary

Round 0



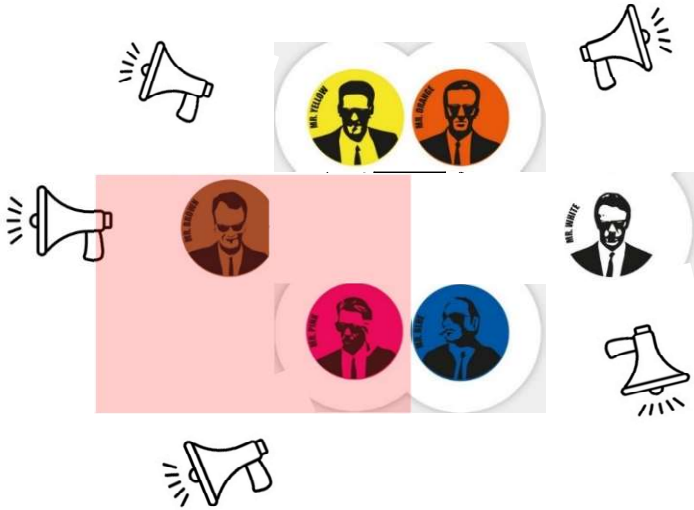
Exchange one-time pads

Round 1



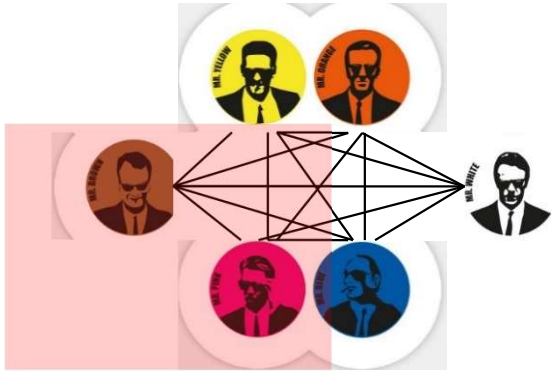
Offline round of SIF

Round 2



Active Adversary

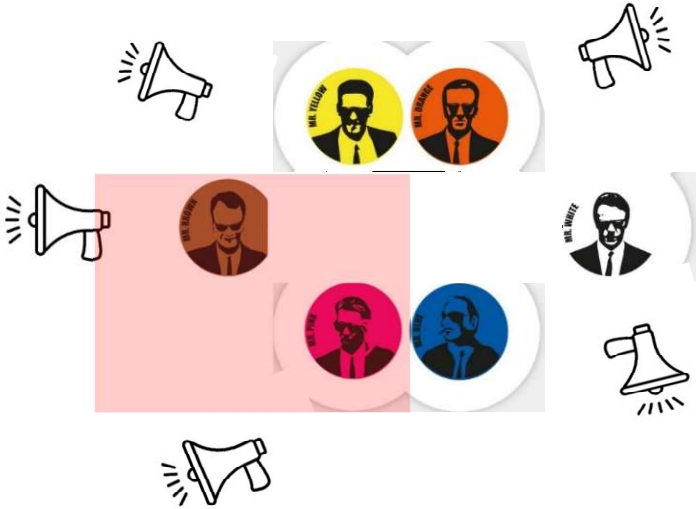
Round 0



Exchange one-time pads

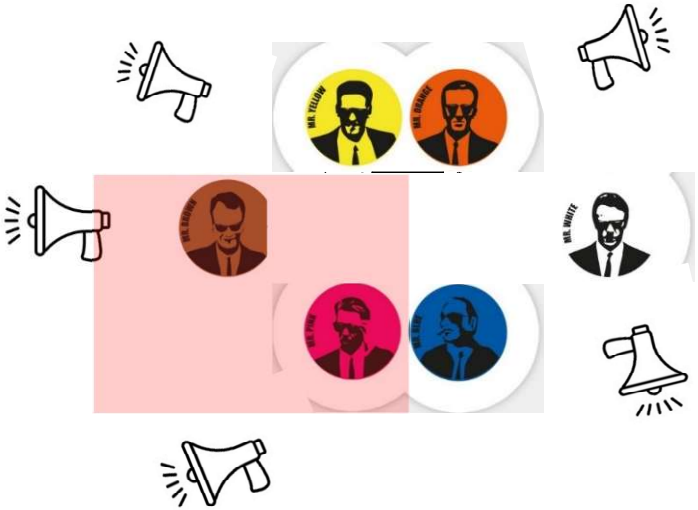
Offline round of SIF

Round 1



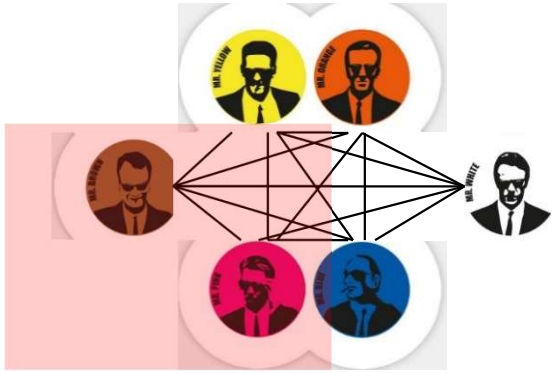
Prove honest behaviour in Rounds 0 and 1.

Round 2



Active Adversary

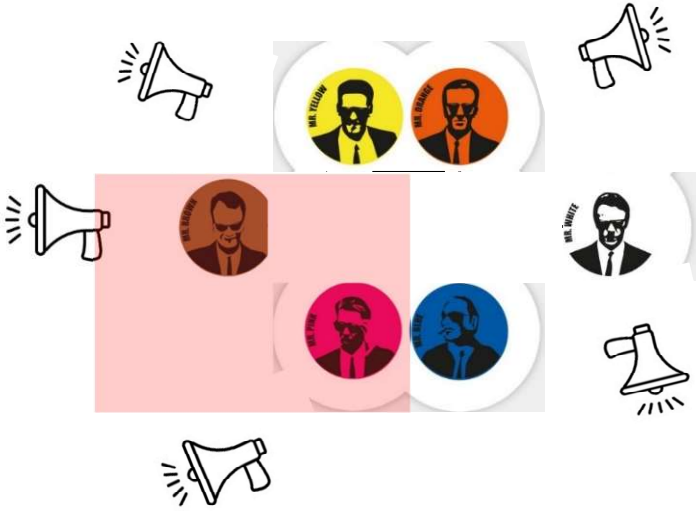
Round 0



Exchange one-time pads

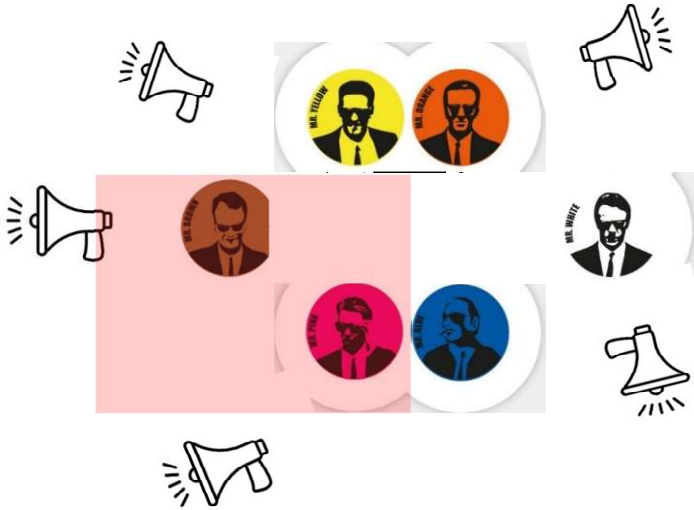
Offline round of SIF

Round 1



Prove honest behaviour in Rounds 0 and 1.

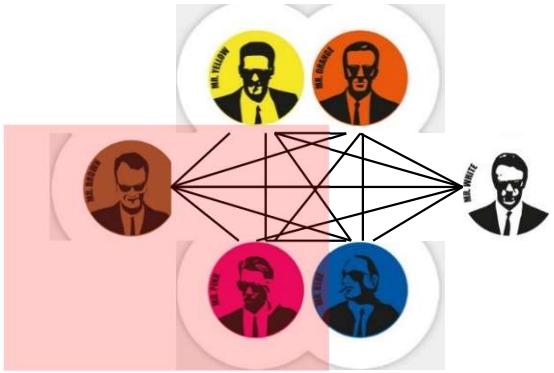
Round 2



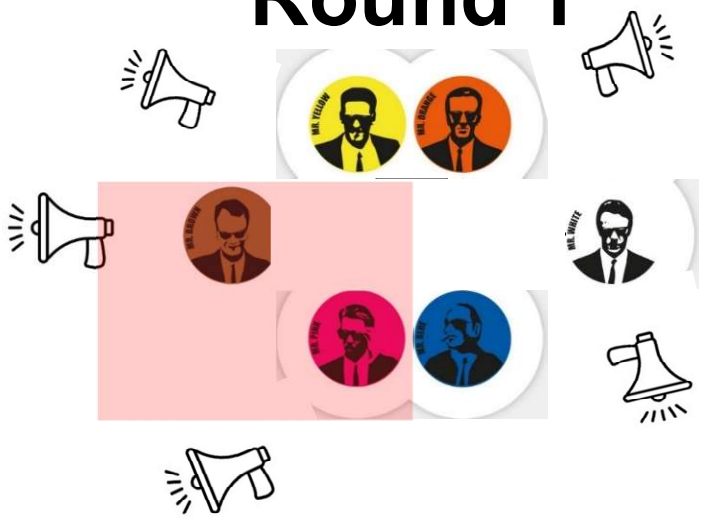
Prove honest behaviour in Round 2.

Active Adversary

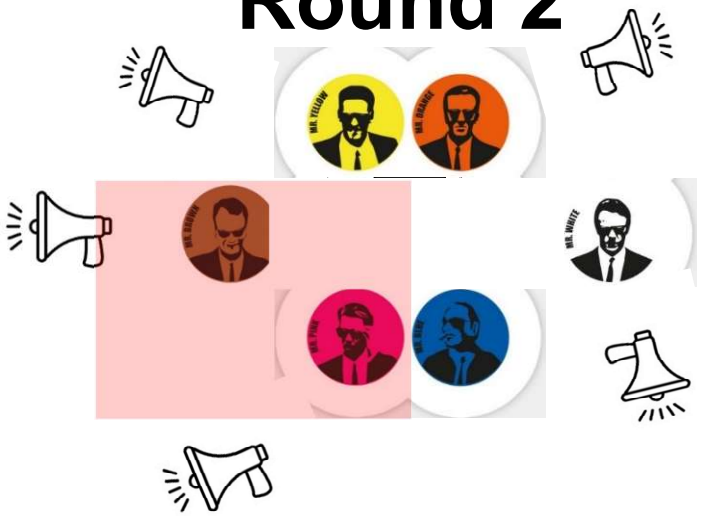
Round 0



Round 1



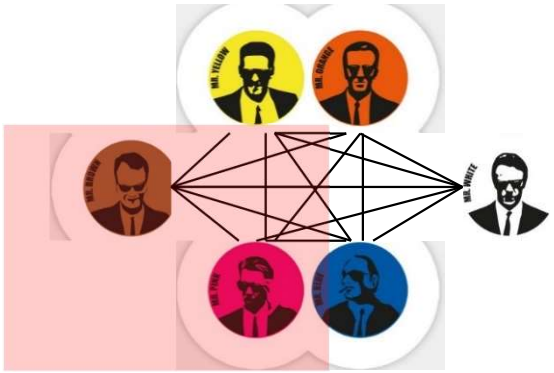
Round 2



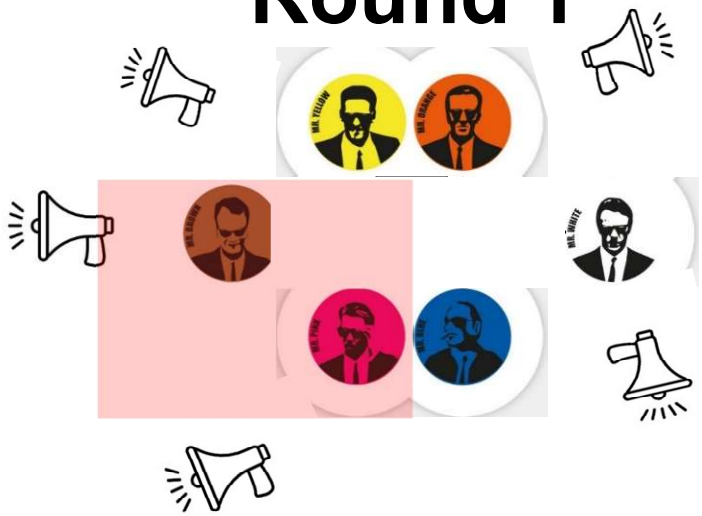
Problem: Round 0 has private communication.

Active Adversary

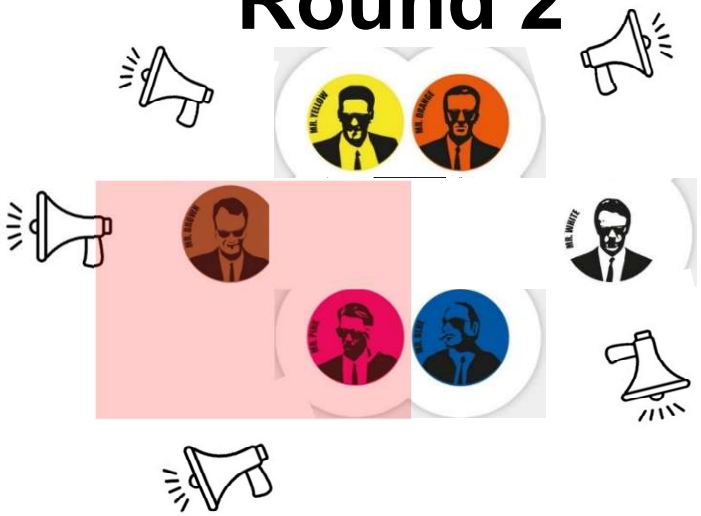
Round 0



Round 1



Round 2

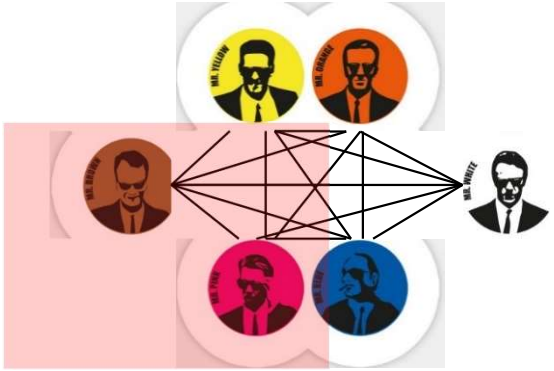


Problem: Round 0 has private communication.

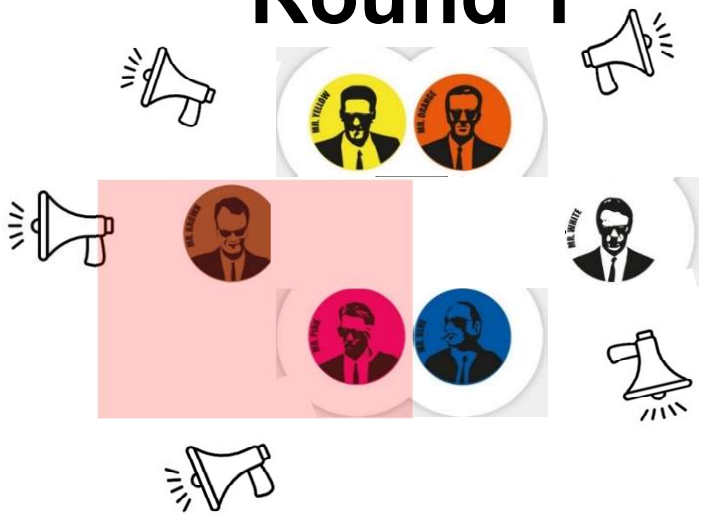
- How to prove correct use of OTP?

Active Adversary

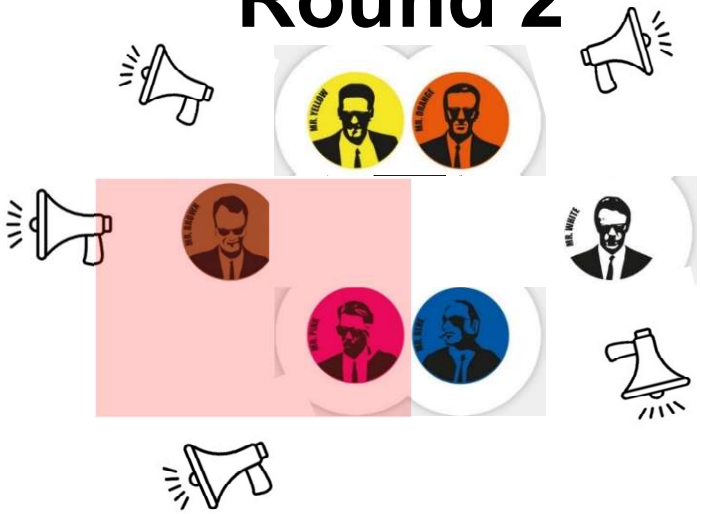
Round 0



Round 1



Round 2



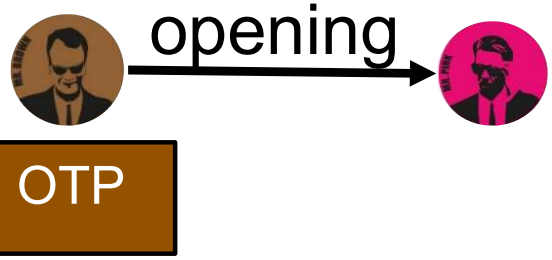
Problem: Round 0 has private communication.

- How to prove correct use of OTP?

Solution: Committed one-time pads.

Active Adversary

Round 0 **Round 1** **Round 2**



Problem: Round 0 has private communication.

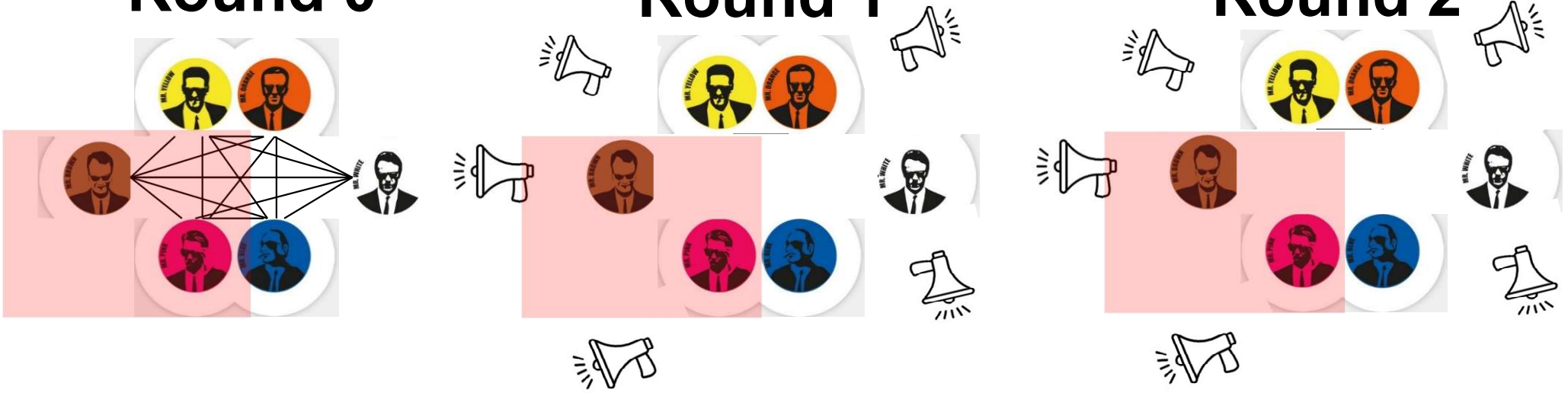
- How to prove correct use of OTP?

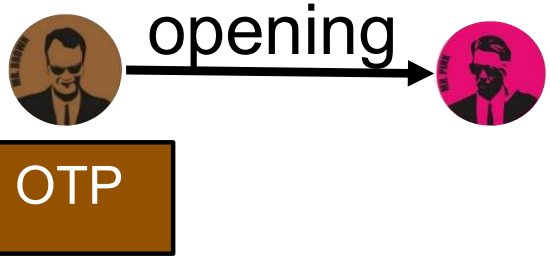
Solution: Committed one-time pads.

- Every party commits to its OTP and sends openings to commitments.

Active Adversary

Round 0 **Round 1** **Round 2**





Problem: Round 0 has private communication.

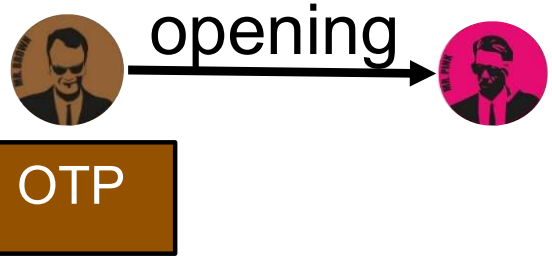
- How to prove correct use of OTP?

Solution: Committed one-time pads.

- Every party commits to its OTP and sends openings to commitments.
  - **Valid opening:** Prove consistency with committed OTP.

Active Adversary

Round 0 **Round 1** **Round 2**



Problem: Round 0 has private communication.

- How to prove correct use of OTP?

Solution: Committed one-time pads.

- Every party commits to its OTP and sends openings to commitments.
  - **Valid opening:** Prove consistency with committed OTP.
  - **Invalid opening:** broadcast plaintext message.

Summary

Summary

- 3-round protocol for general MPC

Summary

- 3-round protocol for general MPC
  - Full security

Summary

- 3-round protocol for general MPC
  - Full security
  - Minicrypt-type assumptions!

Summary

- 3-round protocol for general MPC
  - Full security
  - Minicrypt-type assumptions!
  - Everlasting security

Summary

- 3-round protocol for general MPC
  - Full security
  - Minicrypt-type assumptions!
  - Everlasting security

- GMW-type compiler for honest majority

Summary

- 3-round protocol for general MPC
  - Full security
  - Minicrypt-type assumptions!
  - Everlasting security

- GMW-type compiler for honest majority
  - PKE replaced by committed OTPs

Summary

- 3-round protocol for general MPC
  - Full security
  - Minicrypt-type assumptions!
  - Everlasting security

- GMW-type compiler for honest majority
  - PKE replaced by committed OTPs
  - Zero-knowledge proofs via SIF

Summary

- 3-round protocol for general MPC
  - Full security
  - Minicrypt-type assumptions!
  - Everlasting security

- GMW-type compiler for honest majority
  - PKE replaced by committed OTPs
  - Zero-knowledge proofs via SIF

Thank You!