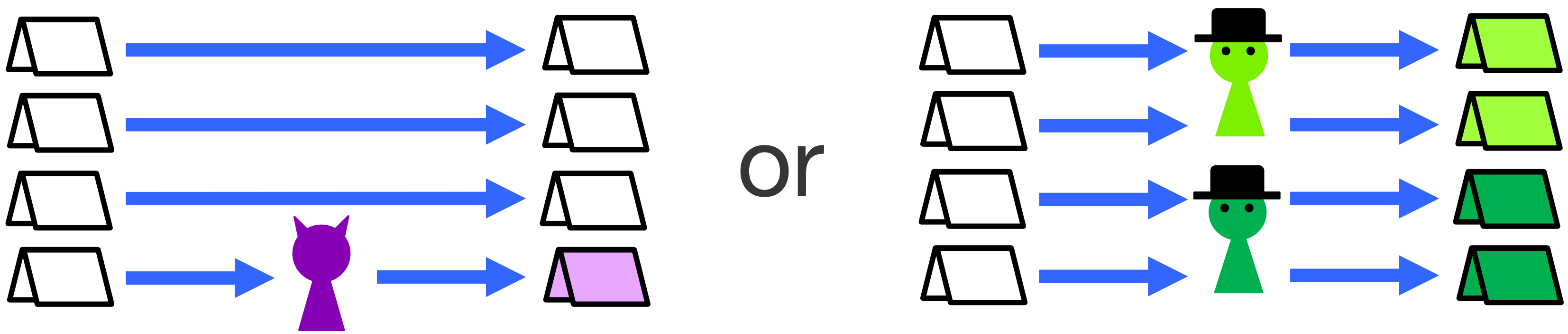
Perfectly Secure Message Transmission against Independent Rational Adversaries



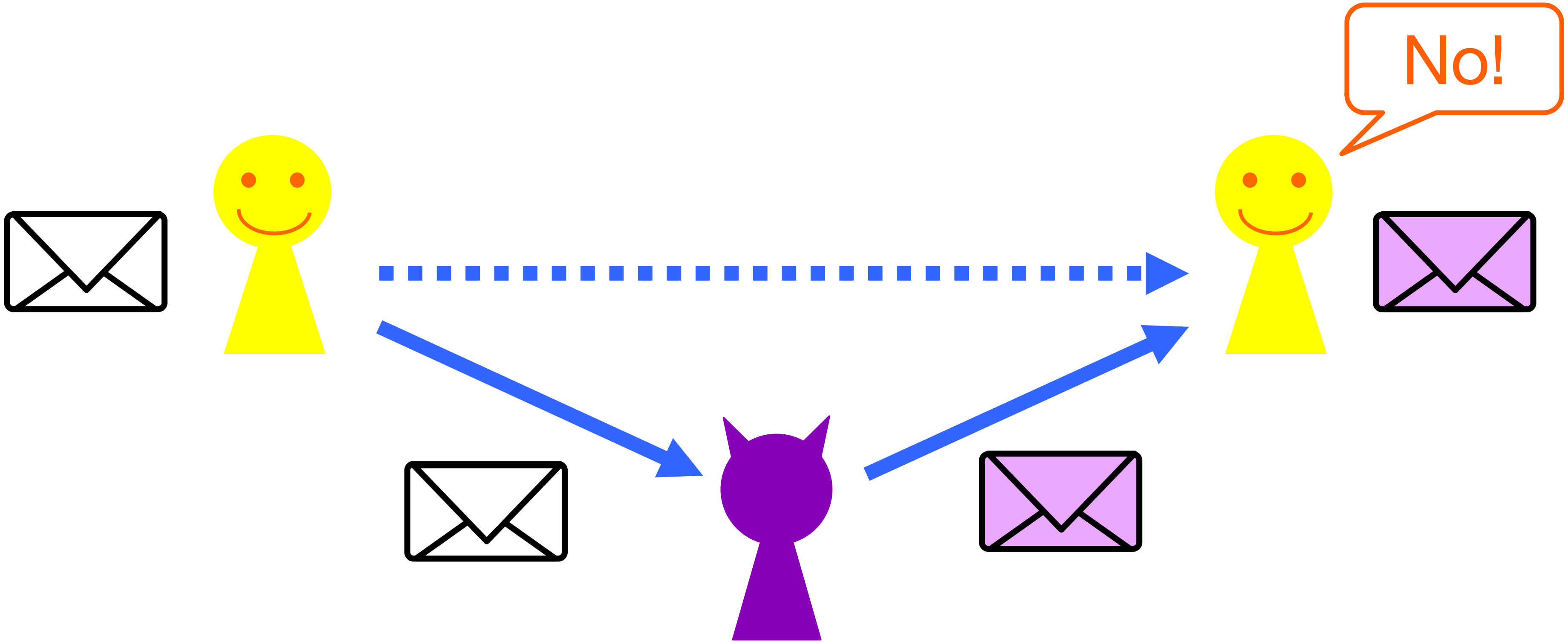
Kenji Yasunaga (Osaka University, Japan)

Takeshi Koshiba (Waseda University, Japan)

GameSec2019@Stockholm

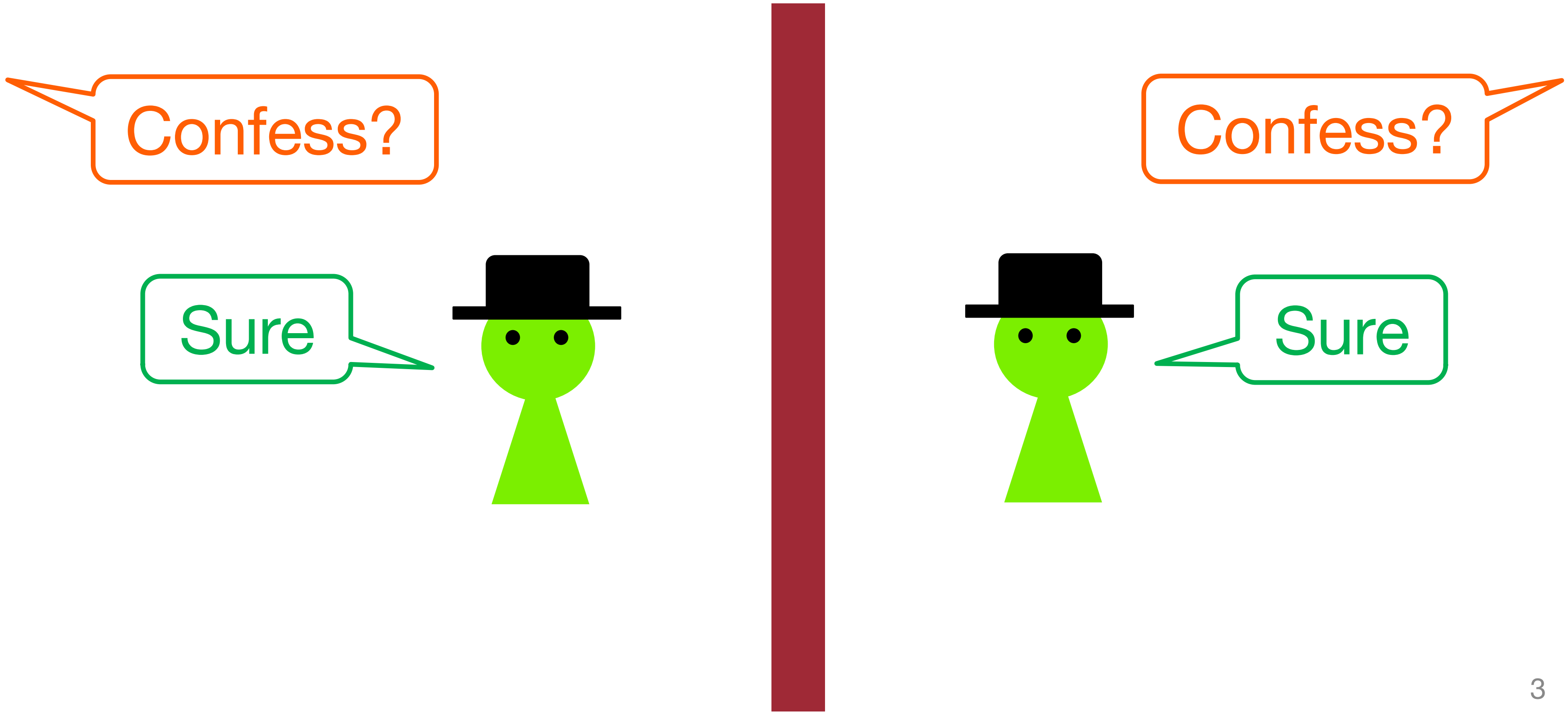
Cryptography

- Theory of protocols for protecting honest users from malicious adversaries



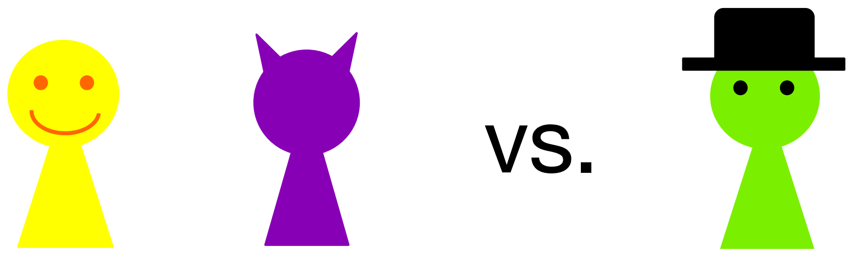
Game Theory

- Theory for analyzing behavior of rational players

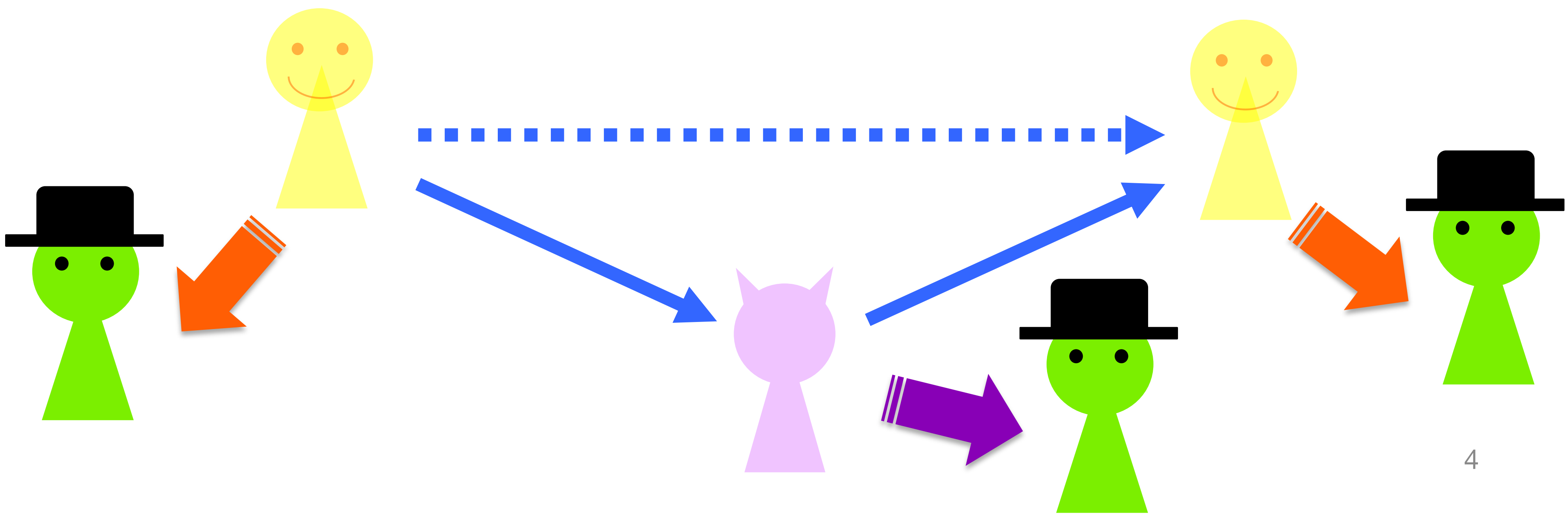


Game Theory in Cryptography

- Both crypto and GT analyze behavior of "players"

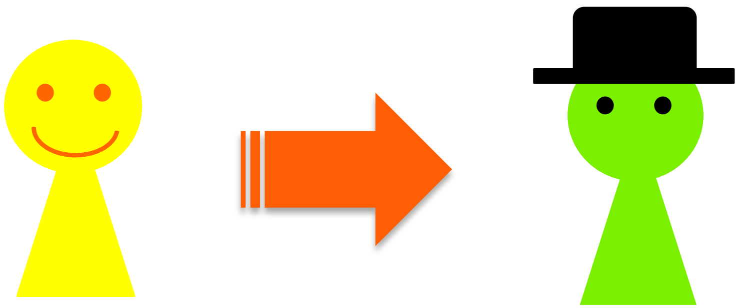


- Q. What if players behave rationally in protocols?



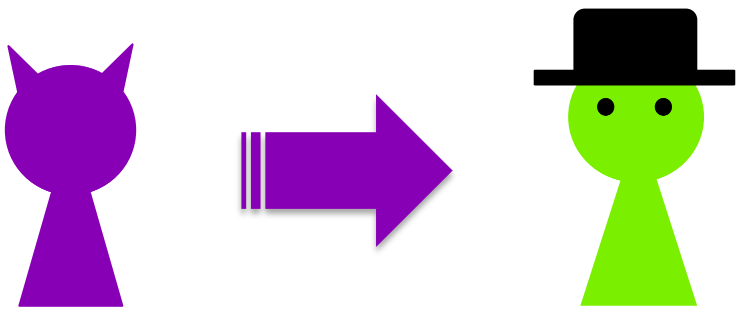
Game Theory in Cryptography

- Direction 1: Honest → Rational



Resolve potential problems

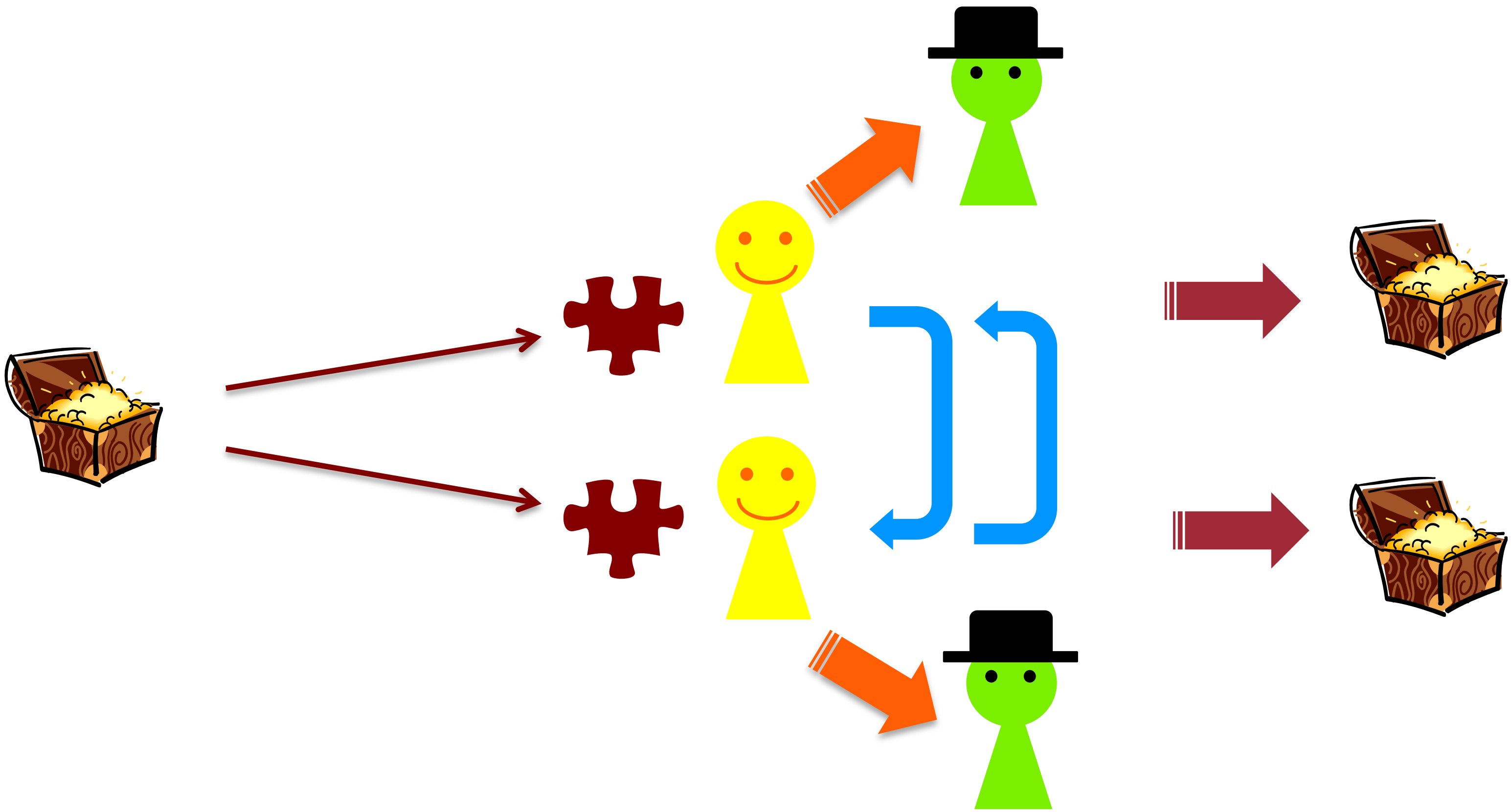
- Direction 2: Malicious → Rational



Overcome existing barriers

Halpern and Teague (STOC'04)

- Target: Secret Sharing
- Direction: Honest → Rational



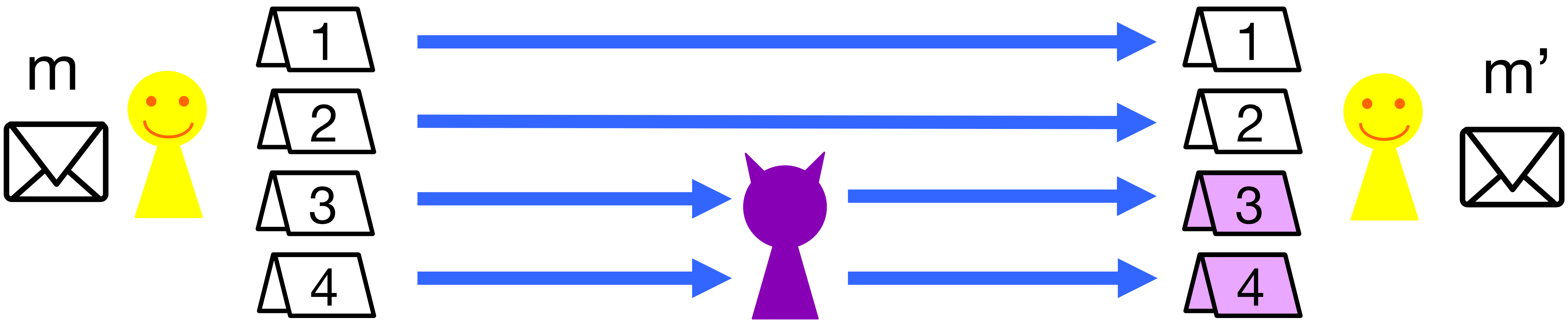
Following Work

Target	Direction	References
Secret Sharing	Honest → Rational	[HT04, GK06, ADGH06, KN08, OPRV09, FKN10, AL11, KOTY17, etc.]
Leader Election	Honest → Rational	[Gra10, ADH13, AGFS14]
Public-Key Encryption	Honest → Rational	[Y16, YY17]
Byzantine Agreement	Malicious → Rational	[GKTZ12]
Multiparty Computation	Malicious → Rational	[ACH16, GK12]
Protocol Design	Malicious → Rational	[GKMTZ13]
Delegated Computation	Malicious → Rational	[AM13,GHRV14,GHRV16]
Secure Message Transmission	Malicious → Rational	[FYK18]

Our Target & Direction

Secure Message Transmission (SMT)

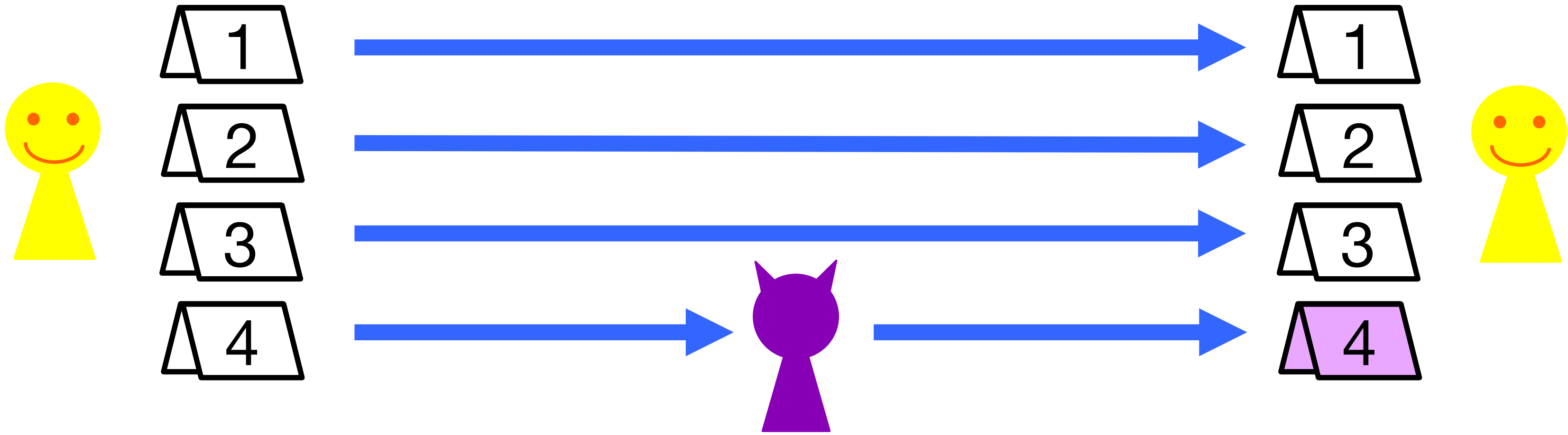
- Send messages “securely” and “reliably” through n channels
  - Adversary corrupts t channels



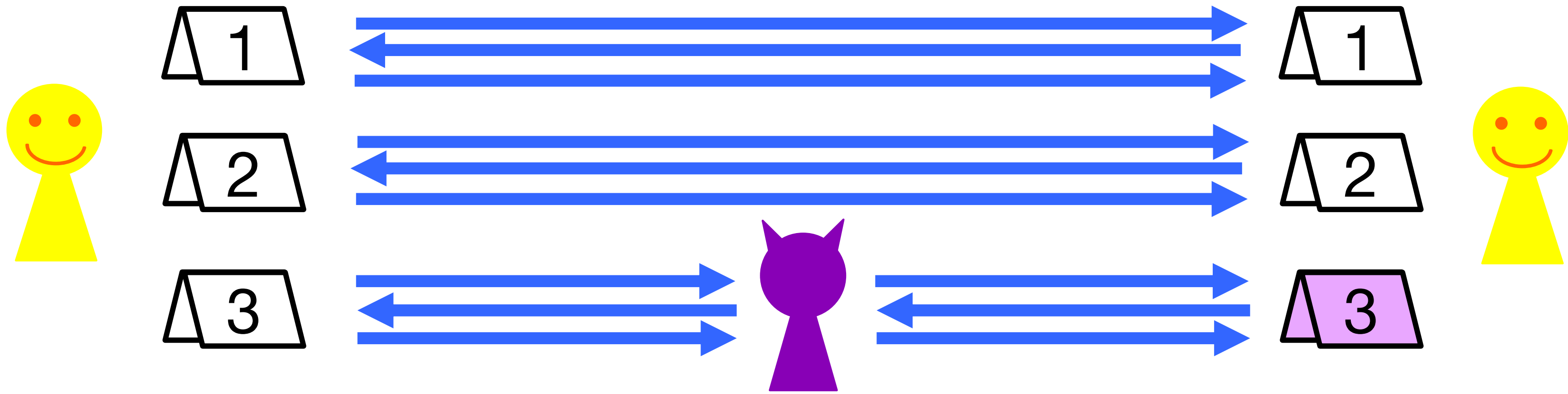
  - Secrecy: m is hidden from Adversary
  - Reliability: m’ = m
- Perfect SMT ⇔ Perfect Secrecy & Reliability

Known Facts of Perfect SMT (PSMT)

- Fact 1. ∃1-round PSMT ⇔ $t < n/3$

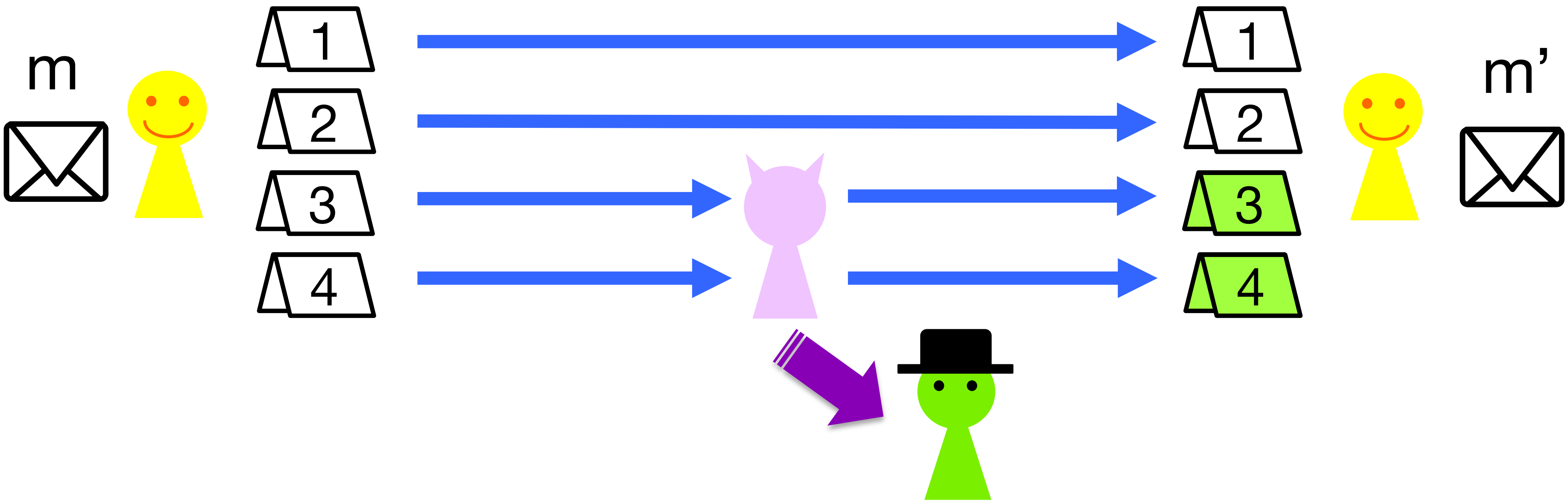


- Fact 2. ∃multi-round PSMT ⇔ $t < n/2$



Our Work & Direction

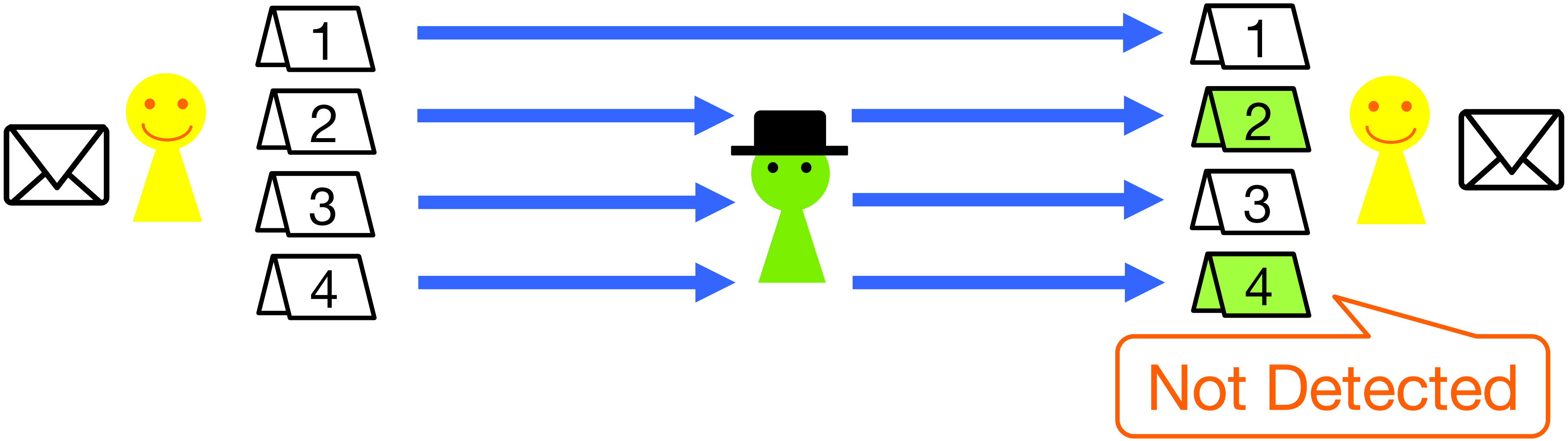
- PSMT against rational adversaries
  - Direction: Malicious → Rational



- Q. Can we overcome the existing barriers?

Previous Work

- Fujita, Yasunaga, Koshiba (GameSec 2018)
  - “Timid” adversary, who avoid being detected



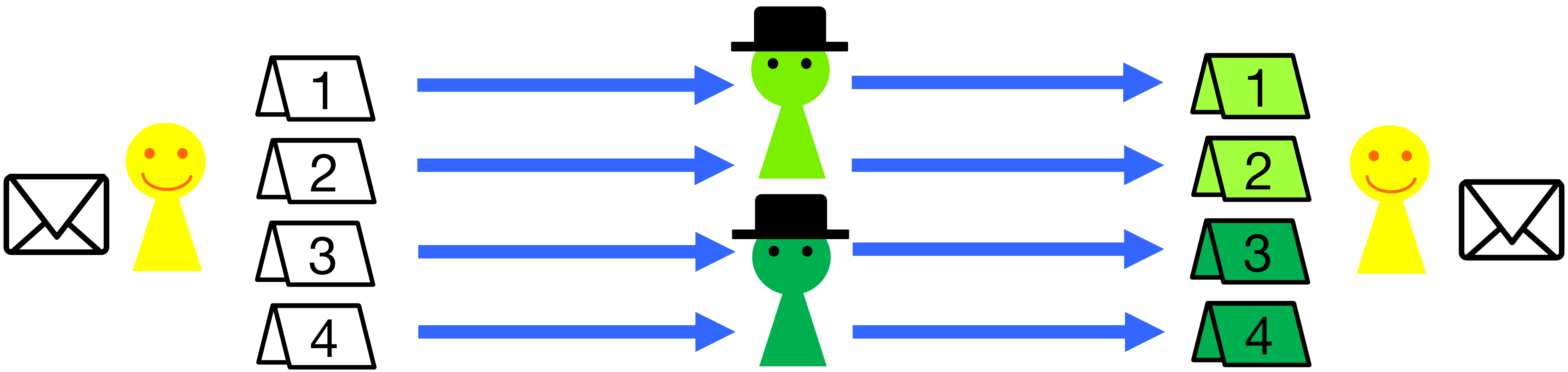
  - Construct PSMT against a timid adversary corrupting $t < n$ channels

Overcome the PSMT barrier $t < n/2$

This Work

- PSMT against “multiple” timid adversaries
- All channels can be corrupted

Impossible for malicious adversaries



Our Results

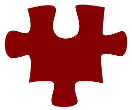
- Construct four PSMT protocols P_1, P_2, P_3, P_4

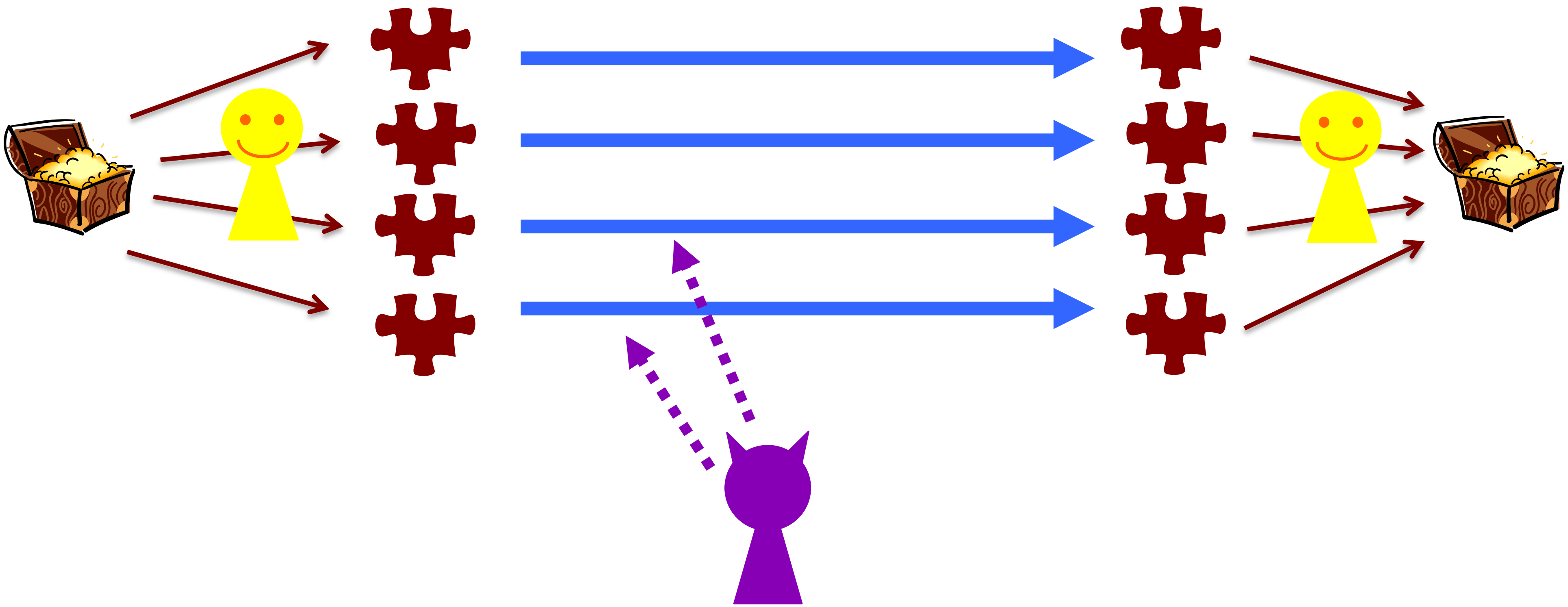
	Additional Assumption	t	# round	Construction Idea
P_1	Public channel	$< n$	3	PSMT of [SJST11]
P_2	—	$< n/2$	1	CISS of [HK18]
P_3	Strictly-timid adversaries	$< n$	1	P_2 & Punishment
P_4	Mixing of rational/malicious	$< n/6$	1	P_2 & Error Correction

t = # corrupted channels per adversary

CISS = Cheater-Identifiable Secret Sharing

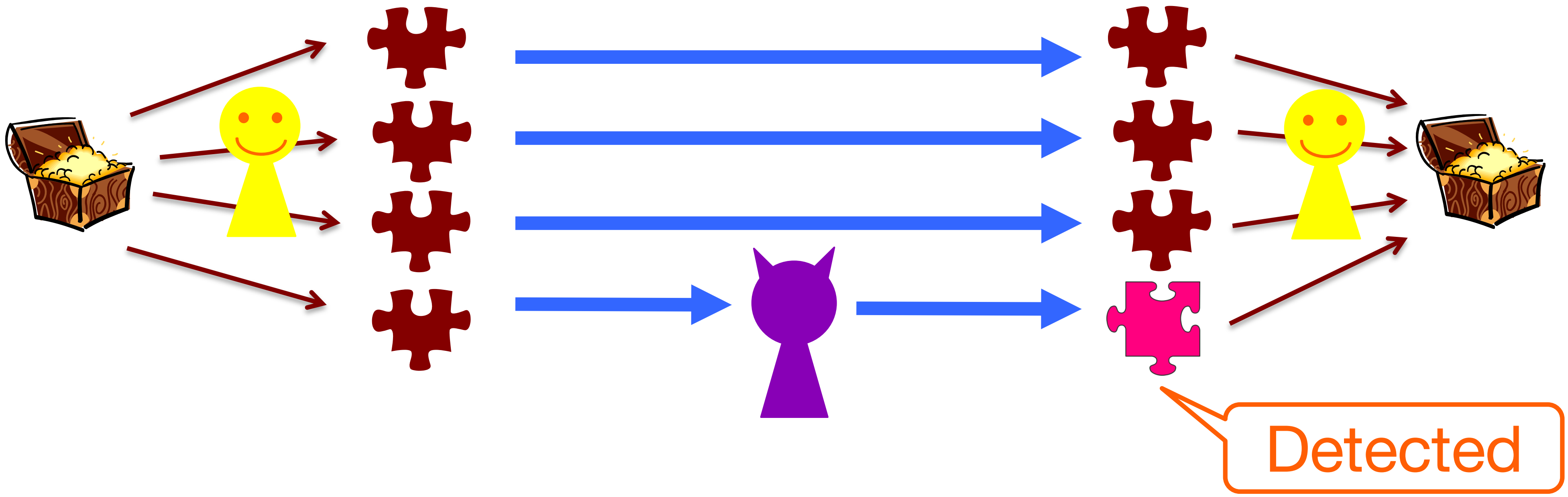
(t, n) Secret Sharing

- Generate n shares  from  such that ≤ t shares reveal no information on 



Cheater-Identifiable Secret Sharing (CISS)

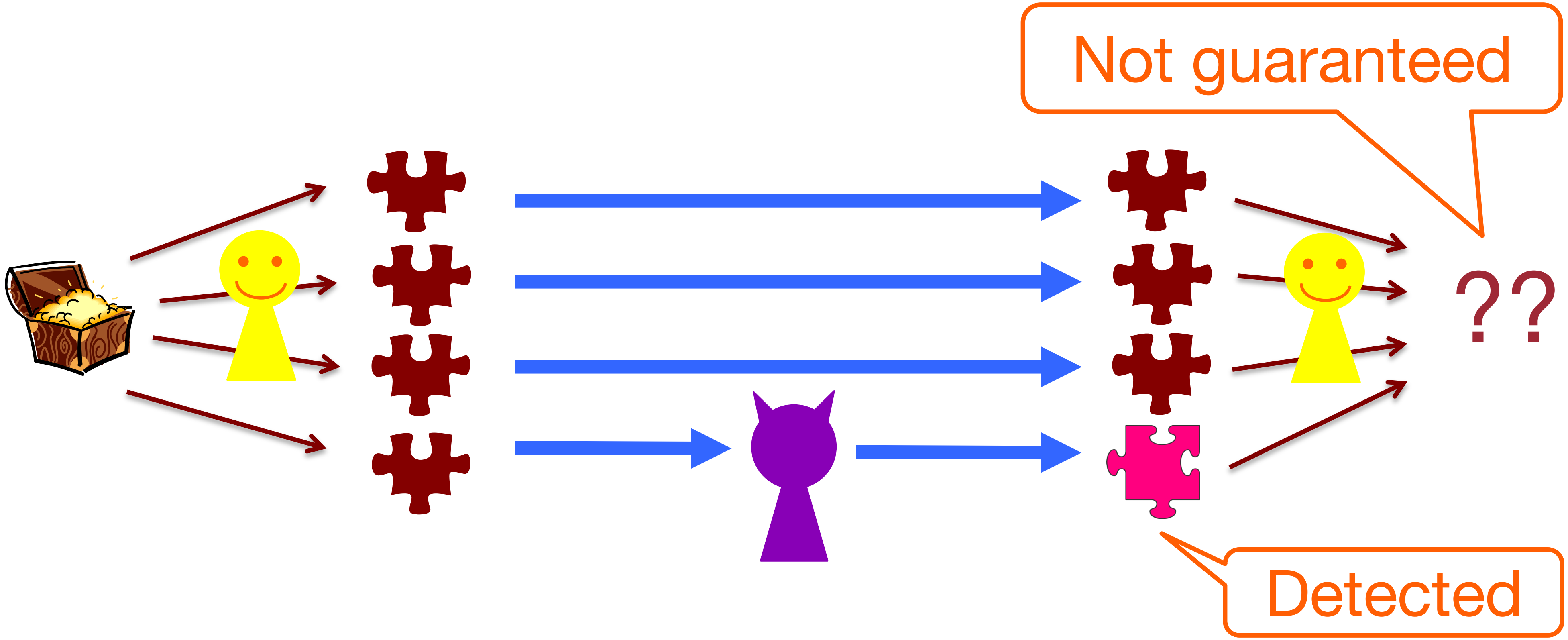
- Identify the cheated shares



- Q. Is CISS a complete solution of PSMT?

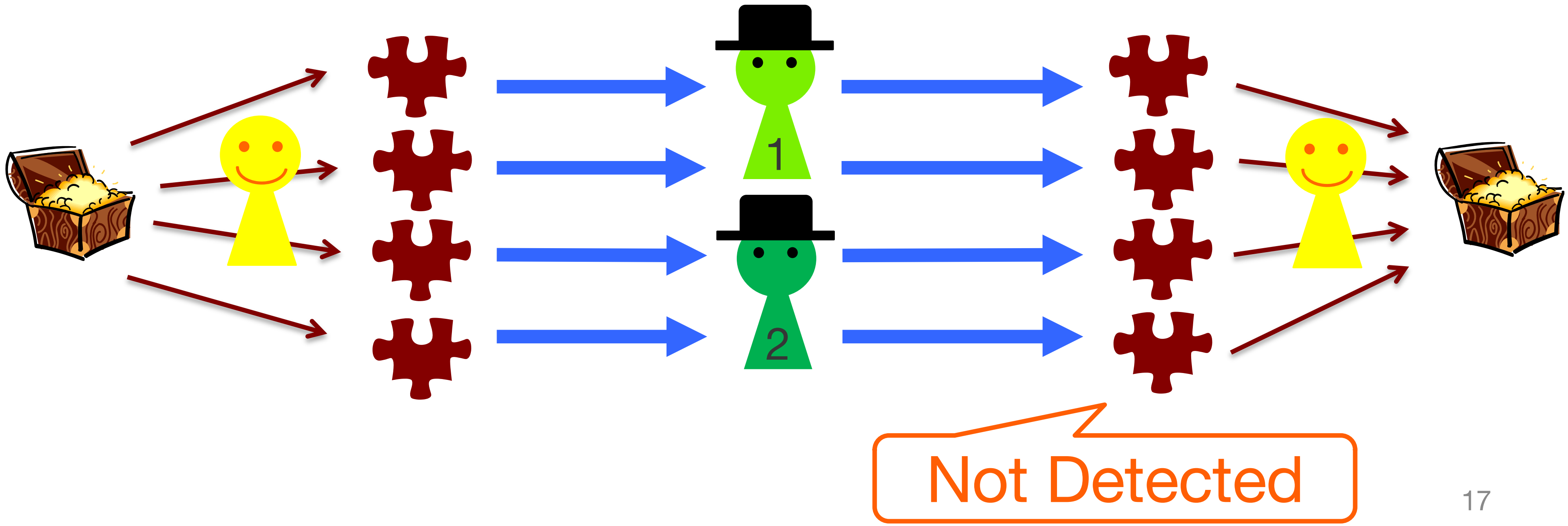
Q. Is CISS a complete solution of PSMT?

- A. No.
  - CISS only guarantees cheater identification
  - PSMT requires recovering the message



Our Idea for Protocol P_2

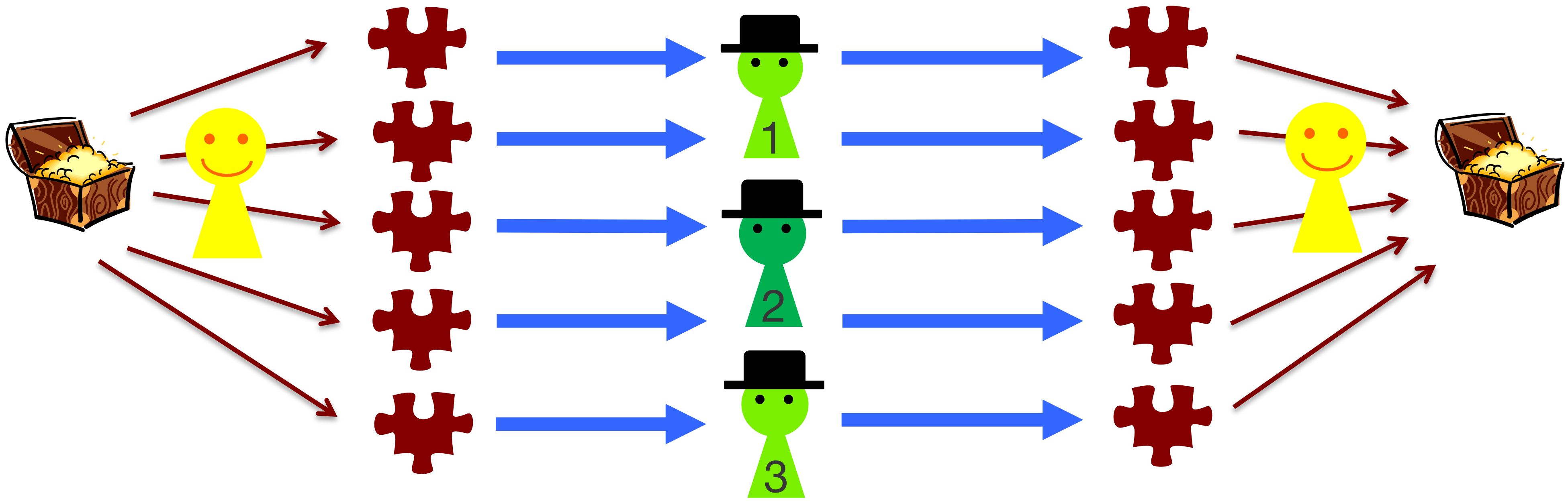
- CISS can work as PSMT
  if adversaries avoid being detected
  - Being silent is rational (a Nash equilibrium)
  - Use CISS of [HK18] w/ stronger hash functions



Protocol P_2

- Theorem: P_2 is PSMT against multiple timid adversaries, each corrupting $t < n/2$ channels

$\exists$CISS $\Leftrightarrow$ $t < n/2$



- Q. Can we overcome this barrier?

Our Idea for Protocol P_3

- A. Yes.
  - CISS with $t \geq n/2$ works as PSMT if adversaries strongly dislike being detected

Avoiding detection is the most important

  - Construct $(n - 1, n)$-type CISS such that if cheating is detected at channel i for share s_j, then both i & j are punished (regarded cheating)

Strictly timid adversaries will not cheat

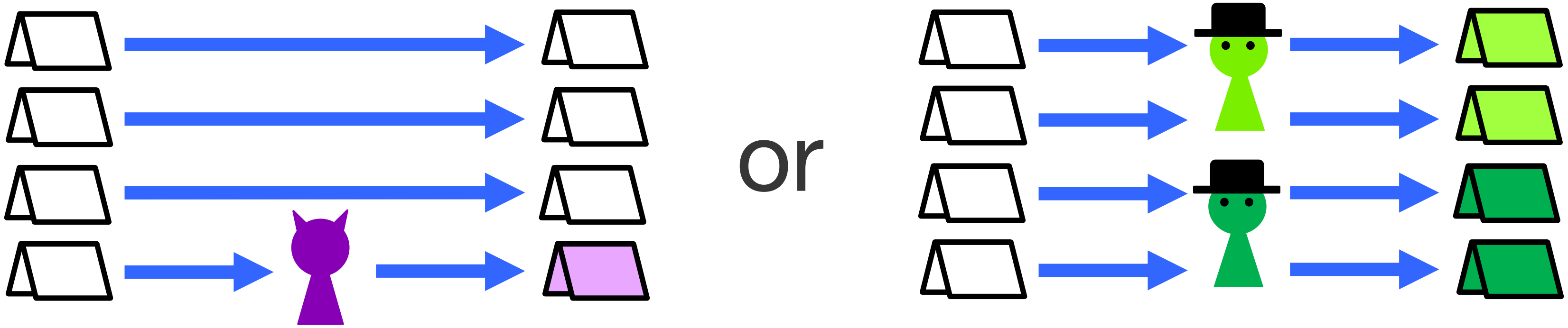
Protocol P_3

- Theorem: P_3 is PSMT against multiple strictly-timid adversaries, each corrupting $t < n$ channels

Summary of Our Results

	Additional Assumption	t	# round	Construction Idea
P_1	Public channel	$< n$	3	PSMT of [SJST11]
P_2	—	$< n/2$	1	CISS of [HK18]
P_3	Strictly-timid adversaries	$< n$	1	P_2 & Punishment
P_4	Mixing of rational/malicious	$< n/6$	1	P_2 & Error Correction

Conclusions



This Work

- Target: PSMT
- Direction: Malicious → Rational
- Feature: All channels can be corrupted

Future Work

- Further study on mixing rational & malicious
- "Malicious → Rational" for other protocols

References (1/2)

[ADGH06] Abraham, Dolev, Gonen, Halpern. Distributed computing meets game theory: robust mechanisms for rational secret sharing and multiparty computation. PODC 2006.

[ADH13] Abraham, Dolev, Halpern. Distributed protocols for leader election: A game-theoretic perspective. DISC 2013.

[AGFS14] Afek, Ginzberg, Feibish, Sulamy. Distributed computing building blocks for rational agents. PODC 2014.

[AL11] Asharov, Lindell. Utility dependence in correct and fair rational secret sharing. J. Cryptology, 2011.

[AM13] Azar, Micali. Super-efficient rational proofs. EC '13.

[HT04] Halpern, Teague. Rational secret sharing and multiparty computation: extended abstract. STOC 2004.

[FKN10] Fuchsbauer, Katz, Naccache. Efficient rational secret sharing in standard communication networks. TCC 2010.

[FYK18] Fujita, Yasunaga, Koshiba. Perfectly secure message transmission against rational timid adversaries. GameSec 2018.

[GHRV14] Guo, Hubácek, Rosen, Vald. Rational arguments: single round delegation with sublinear verification. ITCS 2014.

[GHRV16] Guo, Hubácek, Rosen, Vald. Rational sumchecks. TCC (A2) 2016.

References (2/2)

[GK06] Gordon, Katz. Rational secret sharing, Revisited. SCN 2006.

[GKMTZ13] Garay, Katz, Maurer, Tackmann, Zikas. Rational protocol design: Cryptography against incentive-driven adversaries. FOCS 2013.

[GKTZ12] Groce, Katz, Thiruvengadam, Zikas. Byzantine agreement with a rational adversary. ICALP 2012.

[Gra10] Gradwohl. Rationality in the full-information model. TCC 2010.

[HK18] Hayashi, Koshiba. Universal construction of cheater-identifiable secret sharing against rushing cheaters based on message authentication. ISIT 2018.

[KN08] Kol, Naor. Games for exchanging information. STOC 2008

[KOTY17] Kawachi, Okamoto, Tanaka, Yasunaga. General constructions of rational secret sharing with expected constant-round reconstruction. Comput. J., 2017.

[OPRV09] Ong, Parkes, Rosen, Vadhan. Fairness with an Honest Minority and a Rational Majority. TCC 2009

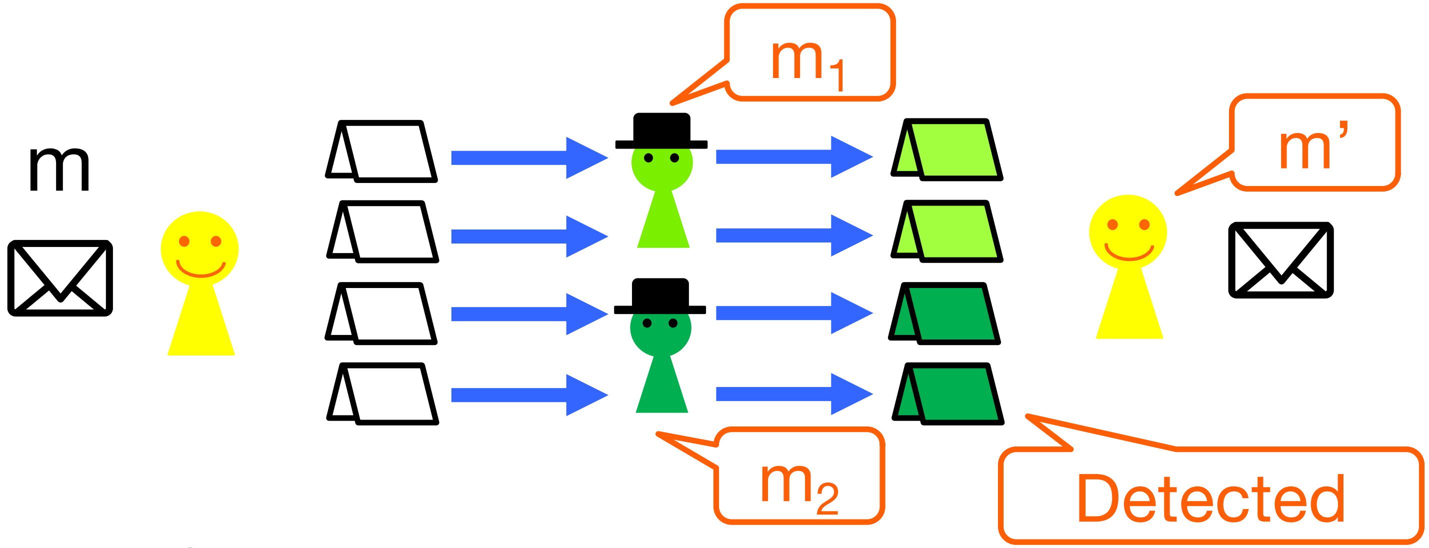
[SJST11] Shi, Jiang, Safavi-Naini, Tuhin. On optimal secure message transmission by public discussion. IEEE Trans. Information Theory, 2011.

[Y16] Yasunaga. Public-key encryption with lazy parties. IEICE Transactions, 2016.

[YY17] Yasunaga, Yuzawa. Repeated games for generating randomness in encryption. IEICE Transactions, 2018.

SMT Game (for Two Adversaries A_1, A_2)

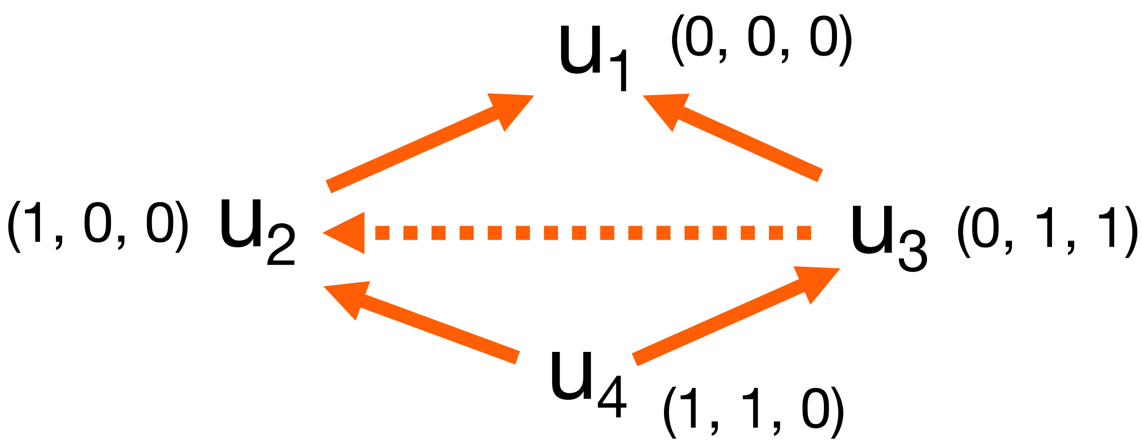
1. Set suc = guess_1 = guess_2 = detect_1 = detect_2 = 0.
2. Run the SMT protocol for random message m



3. Set
   - suc = 1 if the receiver outputs m
   - guess_1 = 1 if A_1 outputs m
   - guess_2 = 1 if A_2 outputs m
   - detect_1 = 1 if the protocol detects deviation of A_1
   - detect_2 = 1 if the protocol detects deviation of A_2

Utility of Timid Adversaries

- For outcome (suc, $guess_1$, $guess_2$, $detect_1$, $detect_2$), adversary A_1 gets higher utility if either
  - suc = 0 (rather than suc = 1), — Reliability fails
  - $guess_1 = 1$ (rather than $guess_1 = 0$), — Secrecy fails
  - $detect_1 = 0$ (rather than $detect_1 = 1$), or — Not detected
  - $detect_2 = 1$ (rather than $detect_2 = 0$) — A_2 detected
- "Strictly" timid adversary A_1 gets higher utility if
  - suc = 1 rather than $detect_1 = 1$



	suc	$detect_1$	$detect_2$
u_1	0	0	0
u_2	1	0	0
u_3	0	1	1
u_4	1	1	0

Security Definition

Protocol π is PSMT against (t_1, t_2)-adversaries

$\Leftrightarrow$

$\exists B_1, B_2$ corrupting t_1, t_2 channels, resp. such that

1. Perfect security: π is PSMT against (B_1, B_2)
2. Nash equilibrium of (B_1, B_2):
   $\forall A_1, A_2$ corrupting the same channels as B_1, B_2,

   $U_1(A_1, B_2) \leq U_1(B_1, B_2)$ and $U_2(B_1, A_2) \leq U_2(B_1, B_2)$

Adversaries have no incentive to deviate from (B_1, B_2)

Our Protocols

- Suppose A_1, A_2 corrupts t_1, t_2 channels, resp.

	Additional Assumption	t_1	t_2	# round	Construction Idea
P_1	Public channel	$< n$	$< n$	3	PSMT of [SJST11]
P_2	—	$< n/2$	$< n/2$	1	CISS of [HK18]
P_3	Strictly-timid adversaries	$< n$	$< n$	1	P_2 & Punishment
P_4	A_1 is malicious	$< n/3$	$< n/3$ $< n/2 - t_1$	1	P_2 & Error Correction

Protocol P_2

- $(s_1, \ldots, s_n)$: shares of $((n-1)/2, n)$-secret sharing for $m \in \{0,1\}^s$
- $h_i \in H$: family of pairwise ind. hash functions $h_i : \{0,1\}^s \rightarrow \{0,1\}^k$
  - $h_i(s_j)$: the authentication tag for s_j using h_i
- $r_{i,j} \in \{0,1\}^k$: random key for encrypting $h_i(s_j)$
  - $T_{i,j} = h_i(s_j) \oplus r_{i,j}$: encrypted tag for s_j

Tag for s_2 $= h_1(s_2) \oplus r_{1,2}$

Tag for s_3 $= h_1(s_3) \oplus r_{1,3}$

Keys for hiding s_1

Authentication failure list verified with h_1

$(s_1, h_1, T_{1,2}, T_{1,3}, r_{2,1}, r_{3,1}) \rightarrow L_1 = \{ j : h_1(s_j) \oplus r_{1,j} \neq T_{1,j} \}$

$(s_2, h_2, T_{2,1}, T_{2,3}, r_{1,2}, r_{3,2}) \rightarrow L_2 = \{ j : h_2(s_j) \oplus r_{2,j} \neq T_{2,j} \}$

$(s_3, h_3, T_{3,1}, T_{3,2}, r_{1,3}, r_{2,3}) \rightarrow L_3 = \{ j : h_3(s_j) \oplus r_{3,j} \neq T_{3,j} \}$

Majority voting on L_i

Final failure list L

Recover m using shares $\{ s_i : i \notin L \}$

Security Proof of P_2

Theorem. P_2 is PSMT against (t_1, t_2)-adversaries with $t_1, t_2 \in [1, (n-1)/2]$, $t_1 + t_2 \leq n$ if

$$k \geq \log_2((u_1 - u_4)/(u_2 - u_4)) + 2\log_2(n+1) - 1.$$

Proof:

- (B_1, B_2) be the strategy of doing nothing → $U_i(B_1, B_2) = u_2$
- P_2 is PSMT against (B_1, B_2)
- To get higher utility (than u_2), A_1 needs either
  1. suc = 0

     → Tampering is detected on majority ($\geq 1 - t_1$) lists L_i
  2. $detect_2 = 1$

     → Impossible due to majority voting & $t_1 < n/2$

Protocol P_3

- $(s_1, \ldots, s_n)$: shares of $(n-1, n)$-secret sharing for $m \in \{0,1\}^s$
- $h_i \in H$, $r_{i,j} \in \{0,1\}^k$, $T_{i,j} = h_i(s_j) \oplus r_{i,j}$ are the same as P_2
- If $T_{i,j}$ verification fails, L_i includes both i and j

i is also punished

Tag for s_2 $= h_1(s_2) \oplus r_{1,2}$

Tag for s_3 $= h_1(s_3) \oplus r_{1,3}$

Keys for hiding s_1

Authentication failure list verified with $T_{1,j}$

$(s_1, h_1, T_{1,2}, T_{1,3}, r_{2,1}, r_{3,1}) \rightarrow L_1 = \{\, 1, j : h_1(s_j) \oplus r_{1,j} \neq T_{1,j} \,\}$

$(s_2, h_2, T_{2,1}, T_{2,3}, r_{1,2}, r_{3,2}) \rightarrow L_2 = \{\, 2, j : h_2(s_j) \oplus r_{2,j} \neq T_{2,j} \,\}$

$(s_3, h_3, T_{3,1}, T_{3,2}, r_{1,3}, r_{2,3}) \rightarrow L_3 = \{\, 3, j : h_3(s_j) \oplus r_{3,j} \neq T_{3,j} \,\}$

Union of L_i's

$L = L_1 \cup L_2 \cup L_3$

If $L = \emptyset$, recover m
Otherwise, output $\perp$

Security Proof of P_3

Theorem. P_3 is PSMT against strictly-timid (t_1, t_2)-adversaries with $t_1, t_2 \in [1, n-1]$, $t_1 + t_2 \leq n$ if

$$k \geq \log_2((u_1 - u_3)/(u_2 - u_3)) - 1.$$

Proof:

- (B_1, B_2) be the strategy of doing nothing → $U_i(B_1, B_2) = u_2$
- P_2 is PSMT against (B_1, B_2)
- To get higher utility (than u_2), A_1 needs either
  1. suc = 0
     → Tampering is detected w.h.p., implying $\text{detect}_1 = 1$
  2. $\text{detect}_2 = 1$
     → Also cause $\text{detect}_1 = 1$, which A_1 should avoid

Protocol P_4

- $(s_1, \ldots, s_n)$: shares of $((n-1)/3, n)$-secret sharing for m with error-correcting property
    - Even if $(n-1)/3$ shares are erroneous, m is recoverable
- $h_i \in H$, $r_{i,j} \in \{0,1\}^k$, $T_{i,j} = h_i(s_j) \oplus r_{i,j}$ are the same as P_2

Tag for s_2 $= h_1(s_2) \oplus r_{1,2}$

Tag for s_3 $= h_1(s_3) \oplus r_{1,3}$

Keys for hiding s_1

Authentication failure list verified with h_1

$(s_1, h_1, T_{1,2}, T_{1,3}, r_{2,1}, r_{3,1}) \longrightarrow L_1 = \{ j : h_1(s_j) \oplus r_{1,j} \neq T_{1,j} \}$

$(s_2, h_2, T_{2,1}, T_{2,3}, r_{1,2}, r_{3,2}) \longrightarrow L_2 = \{ j : h_2(s_j) \oplus r_{2,j} \neq T_{2,j} \}$

$(s_3, h_3, T_{3,1}, T_{3,2}, r_{1,3}, r_{2,3}) \longrightarrow L_3 = \{ j : h_3(s_j) \oplus r_{3,j} \neq T_{3,j} \}$

Majority voting on L_i

Final failure list L

Recover m from the received shares

Security Proof of P_4

Theorem. P_3 is PSMT against (t_1, t_2)-adversaries with $t_1 \in [1, (n-1)/3]$, $t_2 \in [1, \min\{(n-1)/2 - t_1, (n-1)/3\}]$, $t_1 + t_2 \leq n$, where A_1 is a malicious adversary, if

$$k \geq \log_2((u_1 - u_4)/(u_2 - u_4)) - 1.$$

Proof:

- B_2 be the strategy of doing nothing
  - Even if A_1 malicious, m can be recovered → $U_2(A_1, B_2) = u_2$
- P_2 is PSMT against (A_1, B_2)
- To get higher utility (than u_2), A_2 needs either
  1. suc = 0

     → Tampering is detected on majority ($\geq 1 - (t_1 + t_2)$) lists L_i
  2. $detect_1 = 1$

     → Impossible due to majority voting & $t_1 + t_2 < n/2$