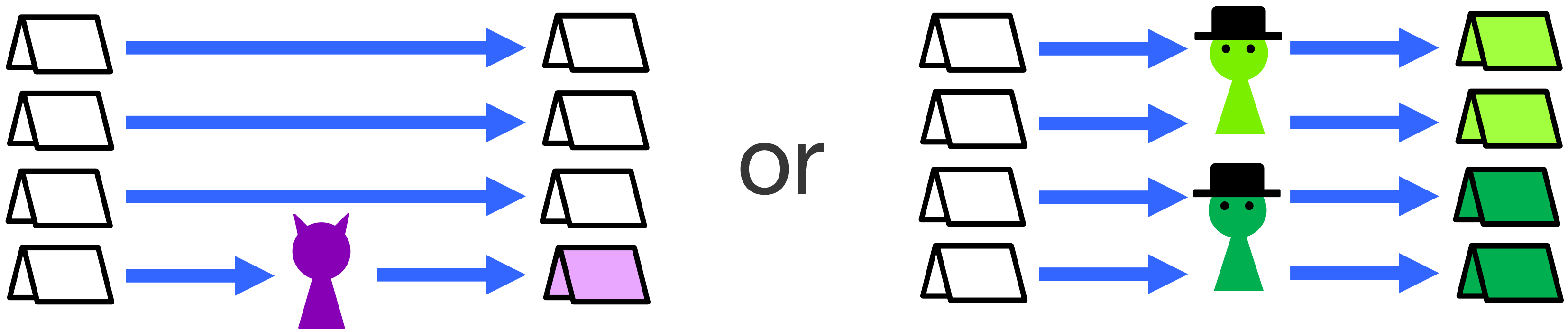
すべての通信路が敵に支配されても ゲーム理論的には安全な通信ができる

Game-Theoretically Secure Message Transmission against Adversaries who Corrupt All Channels

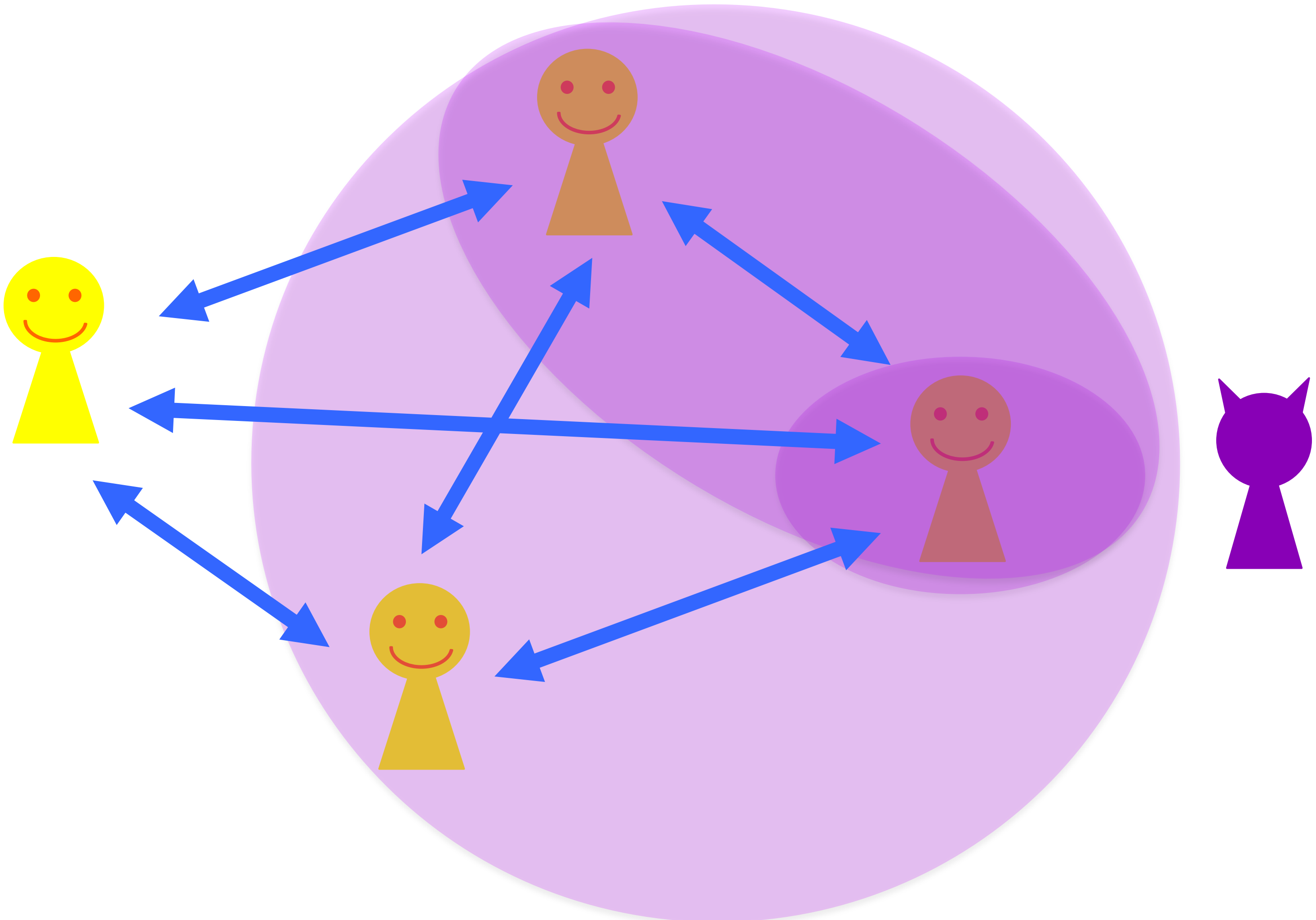


安永 憲司（大阪大学）　小柴 健史（早稲田大学）

冬のLAシンポジウム@京都大学数理解析研究所 2020.2.5

Cryptography

- Protect honest users from malicious adversaries



Cryptography

Q. What security is achieved
if t out of n resources are corrupted?

- Resources = Parties / Channels / etc.

Ex) Typical Results of Crypto Protocols

Resilience	Achieved Security
$t < n/3$	Perfect
$t < n/2$	Almost Perfect
$t < n$	Moderate

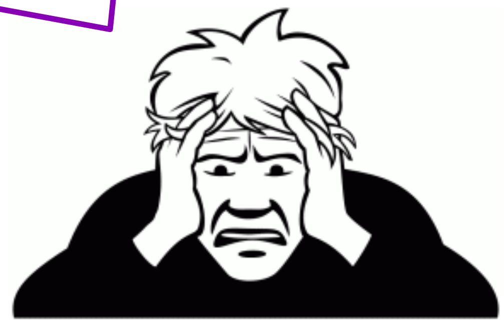
Impression of the Results

Resilience	Achieved Security
t < n	Moderate

Secure even if t = n – 1. Optimal!

How to guarantee one resource is NEVER corrupted?

Protocol Designer



System Manager

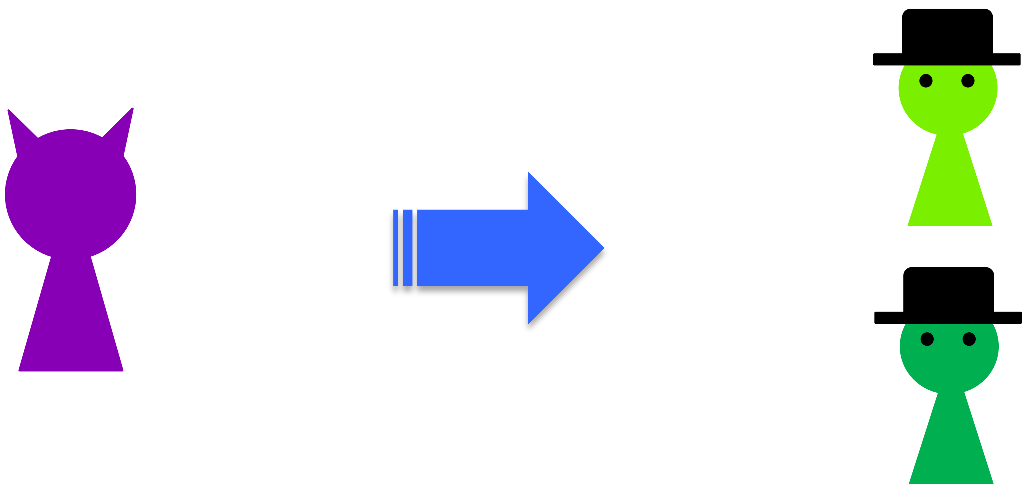
Research Question

Resilience	Achieved Security
$t < n/3$	Perfect
$t < n/2$	Almost perfect
$t < n$	Moderate
$t = n$	No security (?)

Can we achieve non-trivial security when $t = n$?

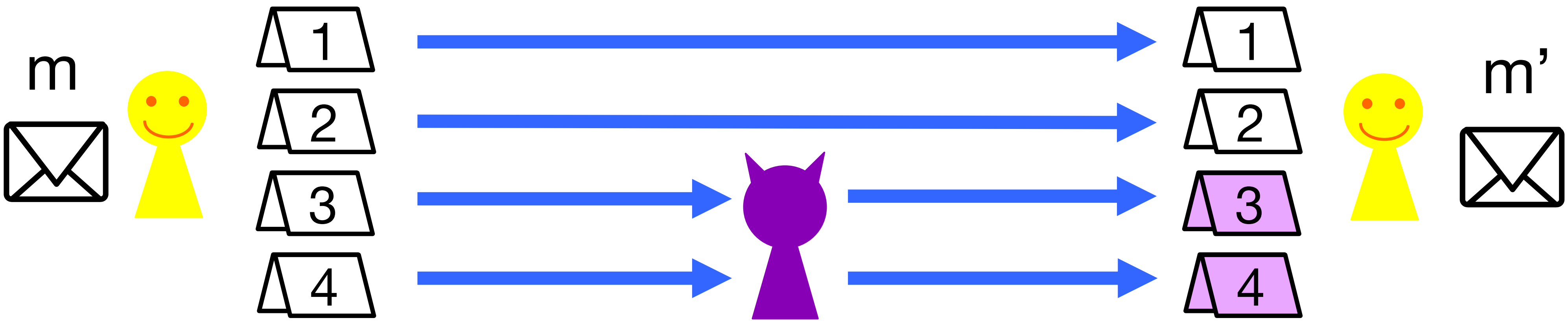
Our Results — Overview

- Achieve game-theoretic security when t = n
  - Target: Secure Message Transmission (SMT)
  - Assumption: There are multiple adversaries who are rational



Secure Message Transmission (SMT)

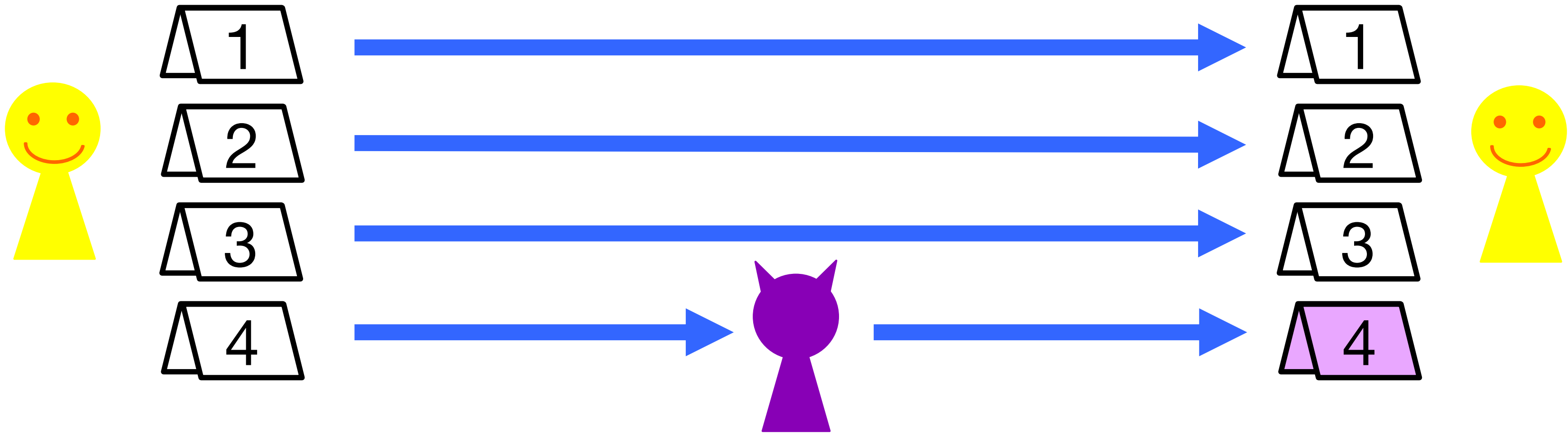
- Send messages "securely" and "reliably" through n channels
  - Adversary corrupts t channels



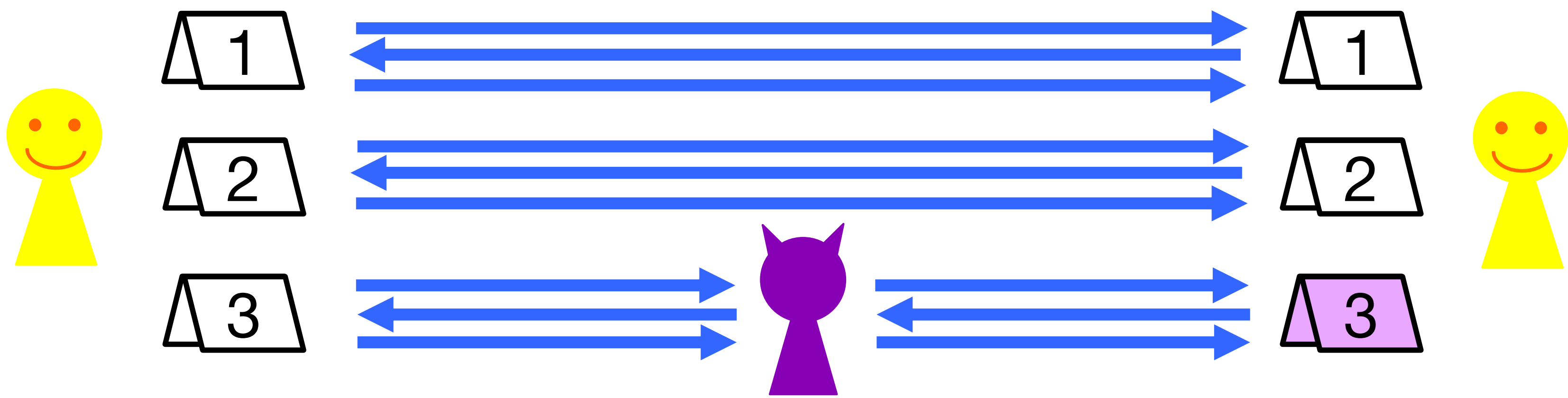
  - Secrecy: m is hidden from Adversary
  - Reliability: m' = m
- Perfect SMT ⇔ Perfect Secrecy & Reliability

Known Facts of Perfect SMT (PSMT)

- Fact 1. ∃1-round PSMT ⇔ $t < n/3$

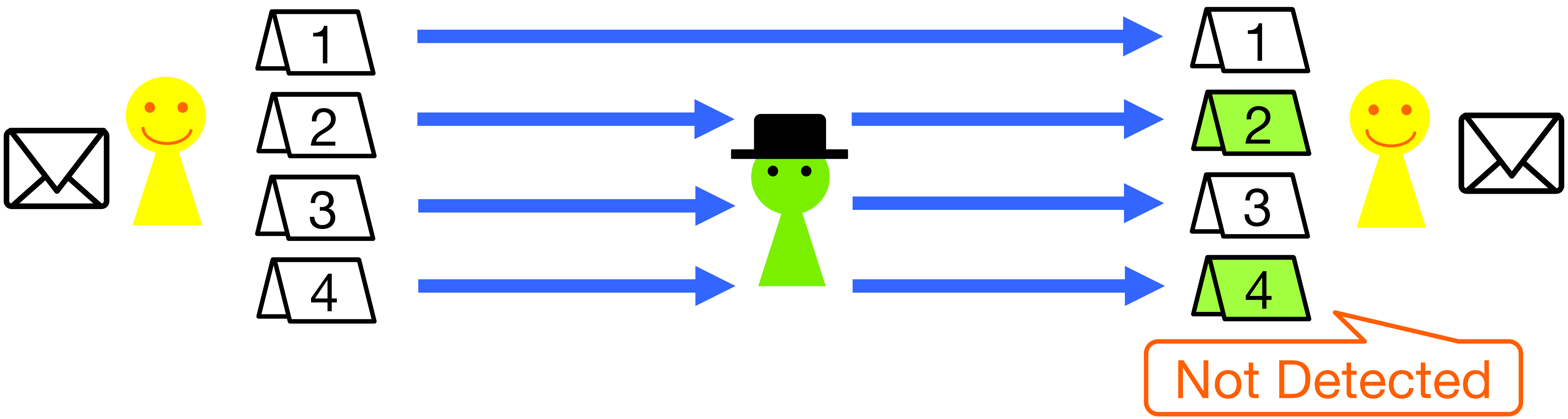


- Fact 2. ∃multi-round PSMT ⇔ $t < n/2$



Previous Work on GT security of PSMT

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

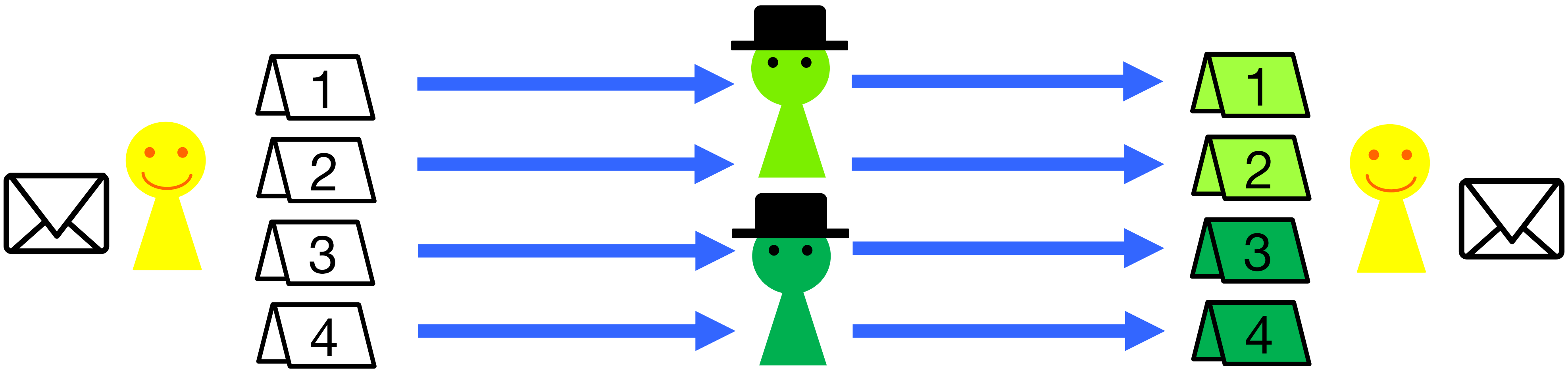


  - Construct PSMT against a timid adversary corrupting $t < n$ channels

This Work

- PSMT against multiple timid adversaries
  - Each adversary does not cooperate
  - All channels can be corrupted

Impossible against a single adversary



Our Results

- Construct three PSMT protocols π_1, π_2, π_3

	Additional Assumption	t	# round	Construction Idea
π_1	—	$< n/2$	1	CISS of [Hayashi,Koshiba (2018)]
π_2	Strictly-timid adversaries	$< n$	1	π_1 & Punishment
π_3	Mixing of rational/malicious	$< n/6$	1	π_1 & Error Correction

t = # corrupted channels per adversary

CISS = Cheater-Identifiable Secret Sharing

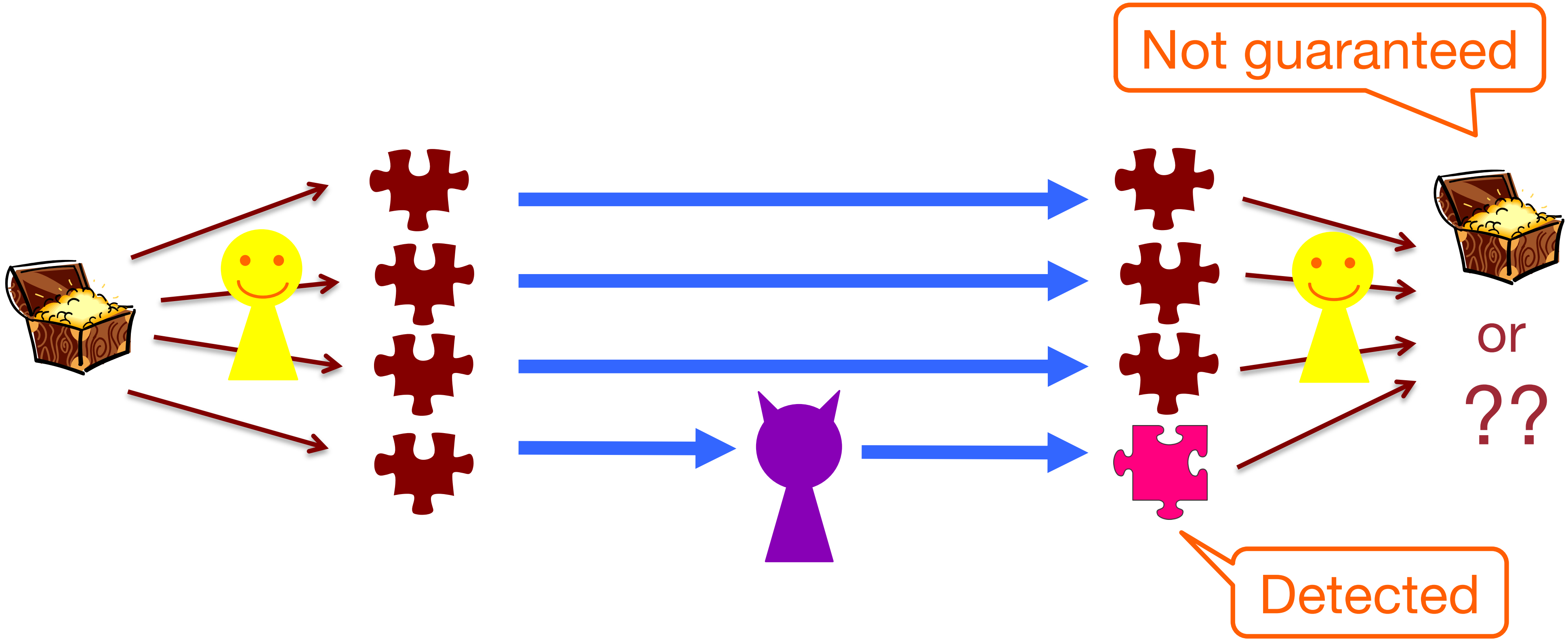
GT Security & Adversary’s Utility

- Game-Theoretic Security:
  - Define SMT game G for rational adversaries
  - Protocol π is GT secure
    ⇔ To “do nothing” is a Nash equilibrium in G

- Utility: Timid adversaries want
  1. to violate the security requirements of SMT
  2. their actions to be undetected by π
  3. other adversaries’ actions to be detected

(t, n) Secret Sharing and CISS

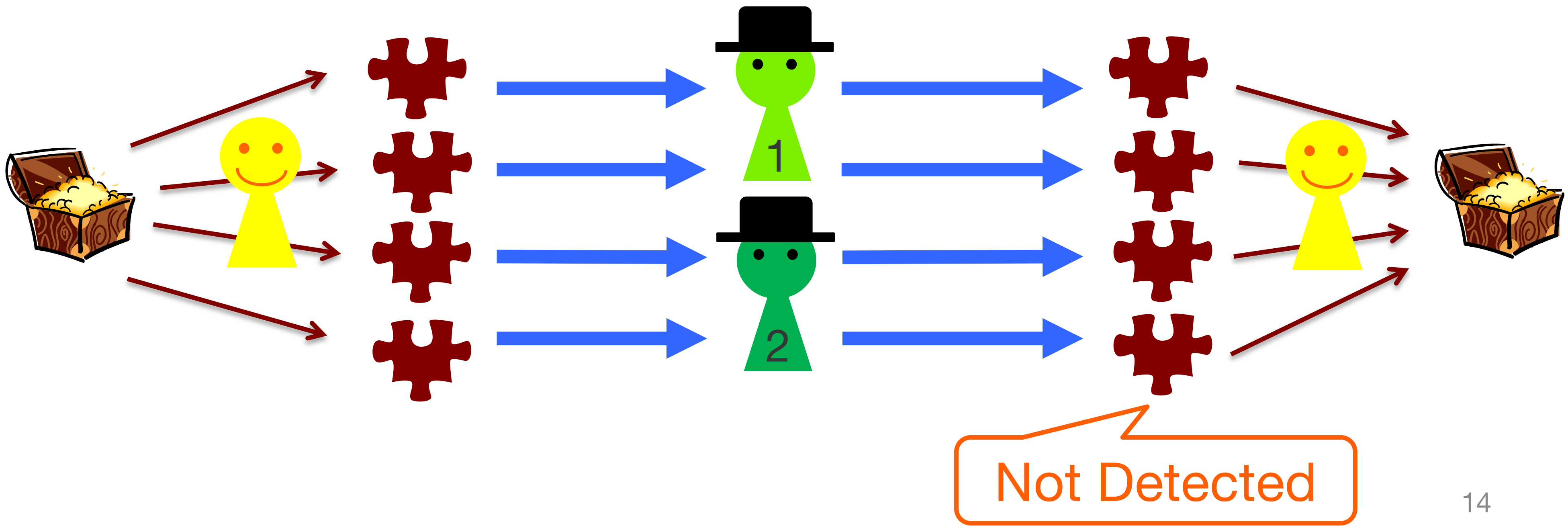
- (t, n) Secret Sharing: $\leq$ t shares reveal no info. on 
- CISS: SS that can identify the cheated shares



- CISS does not imply PSMT

Our Idea for Protocol π_1

- CISS works as PSMT against timid adversaries
  - To do nothing is a Nash equilibrium
  - Use CISS of [HK18] w/ stronger hash functions



Protocol π_1

- $(s_1, \ldots, s_n)$: shares of $((n-1)/2, n)$-secret sharing for $m \in \{0,1\}^s$
- $H = \{ h_i : \{0,1\}^s \rightarrow \{0,1\}^k \}$: a family of pairwise ind. hash func. h_i
  - $h_i(s_j)$: 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

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

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

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

Majority voting on L_i

Final failure list L

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

Security Proof of π_1

> Theorem 1. π_1 is PSMT against multiple timid adversaries, each corrupting $< n/2$ channels by choosing sufficiently large k

Proof sketch:

- Suppose there exist two adversaries A_1 & A_2
- u^* = Utility when doing nothing
- To get higher utility than u^*, A_1 needs either
  1. Violating reliability
     → Detected w.h.p. on majority ($\geq 1 - t$) lists L_i
  2. Cheating detection of A_2
     → Impossible due to majority voting & $t < n/2$

Our Idea for Protocol π_2

- Fact: CISS exists ⇔ $t < n/2$
- CISS can work as PSMT even for $t \geq n/2$ against strictly timid adversaries

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 π_2

- $(s_1, \ldots, s_n)$: 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 π_1
- 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 $T_{1,j}$

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

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

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

$L = L_1 \cup L_2 \cup L_3$

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

Security Proof of π_2

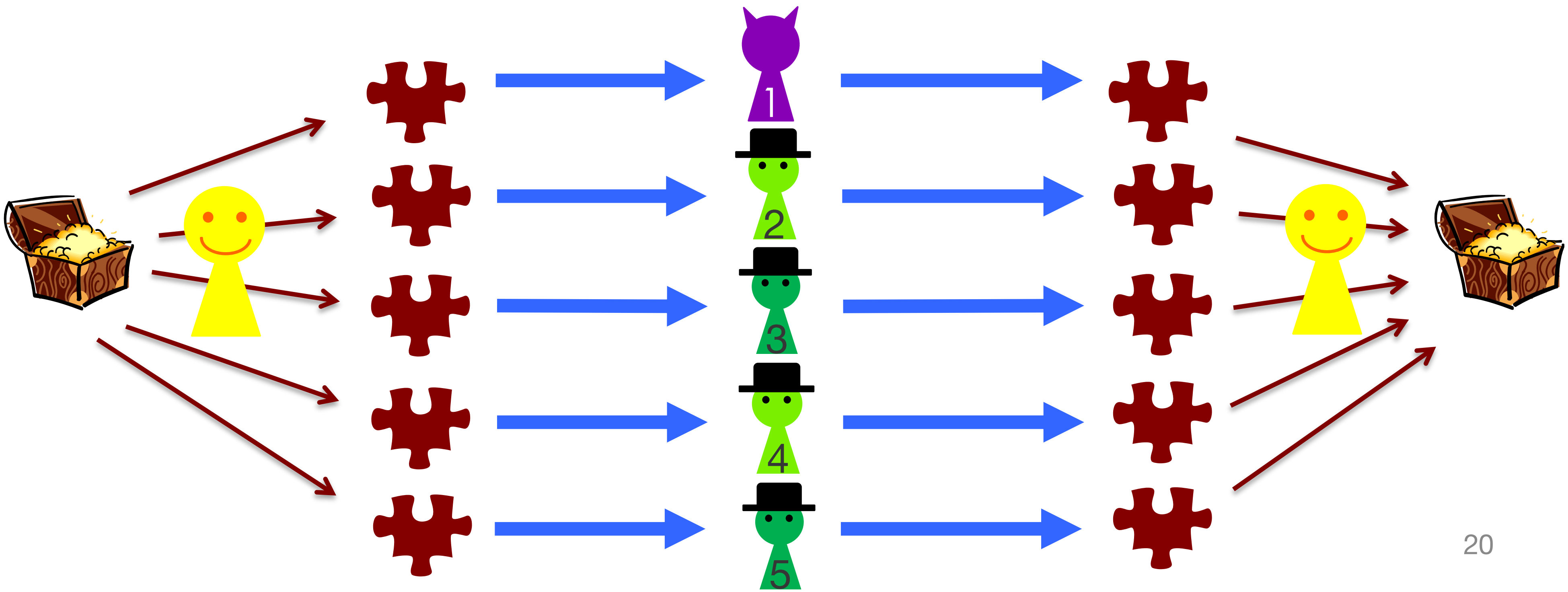
> Theorem 2. π_2 is PSMT against strictly-timid adversaries, each corrupting $< n$ channels by choosing sufficiently large k

Proof sketch:

- Suppose there exist two adversaries A_1 & A_2
- u^* = Utility when doing nothing
- To get higher utility than u^*, A_1 needs either
  1. Violating reliability
     → Detected w.h.p., implying cheating detection of A_1
  2. Cheating detection of A_2
     → Also cause tampering detection of A_1

Our Idea for Protocol π_3

- What if a malicious adversary exists?
  - PSMT for $t < n/3$: SS with error correction
- Protocol π_1 works as PSMT against malicious A_1 and timid A_i's if $t_1, t_i < n/3$, $t_1 + t_i < n/2$



Protocol π_3 and Security Proof

Protocol π_3

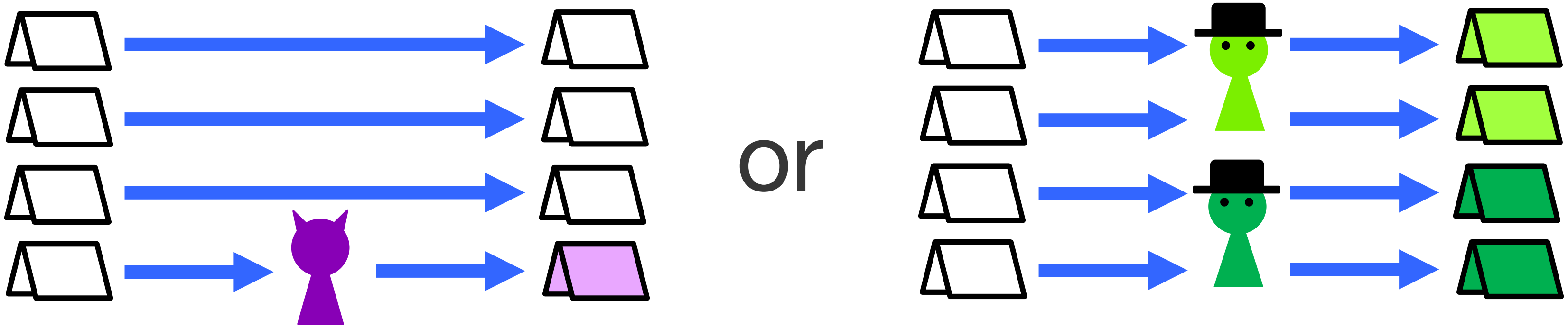
- $(s_1, \ldots, s_n)$: shares of $((n - 1)/3, n)$-SS with error correction
  - Secret recovery even if $< (n - 1)/3$ shares are erroneous
- Other parts are the same as π_1

Theorem 3. π_3 is PSMT against malicious adversary A_1 and timid adversaries A_i, each corrupting t_1 and t_i channels, where $t_1, t_i < n/3$, $t_1 + t_i < n/2$

Proof sketch:

- To get higher utility, timid adversary A_i need either
  1. Violating reliability
     → Detected w.h.p. on majority ($\geq 1 - (t_1 + t_i)$) lists L_i
  2. Cheating detection of A_2
     → Impossible due to majority voting & $t_1 + t_i < n/2$

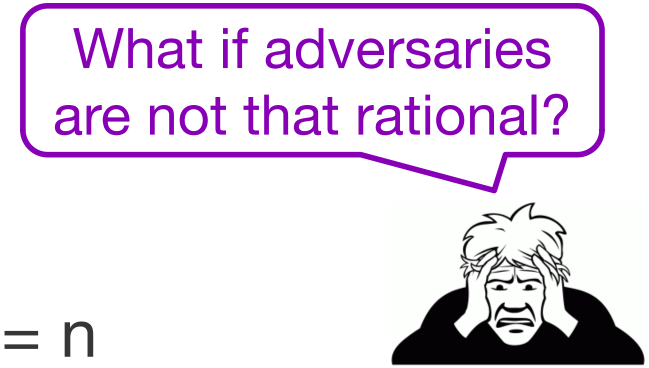
Conclusions



This Work

- GT security of PSMT when t = n
- Assumption: ∃multiple timid adversaries
- See [Yasunaga, Koshiba (GameSec 2019)] for details

Future Work



- Stronger GT security (e.g., unique NE)
- GT security of other protocols when t = n