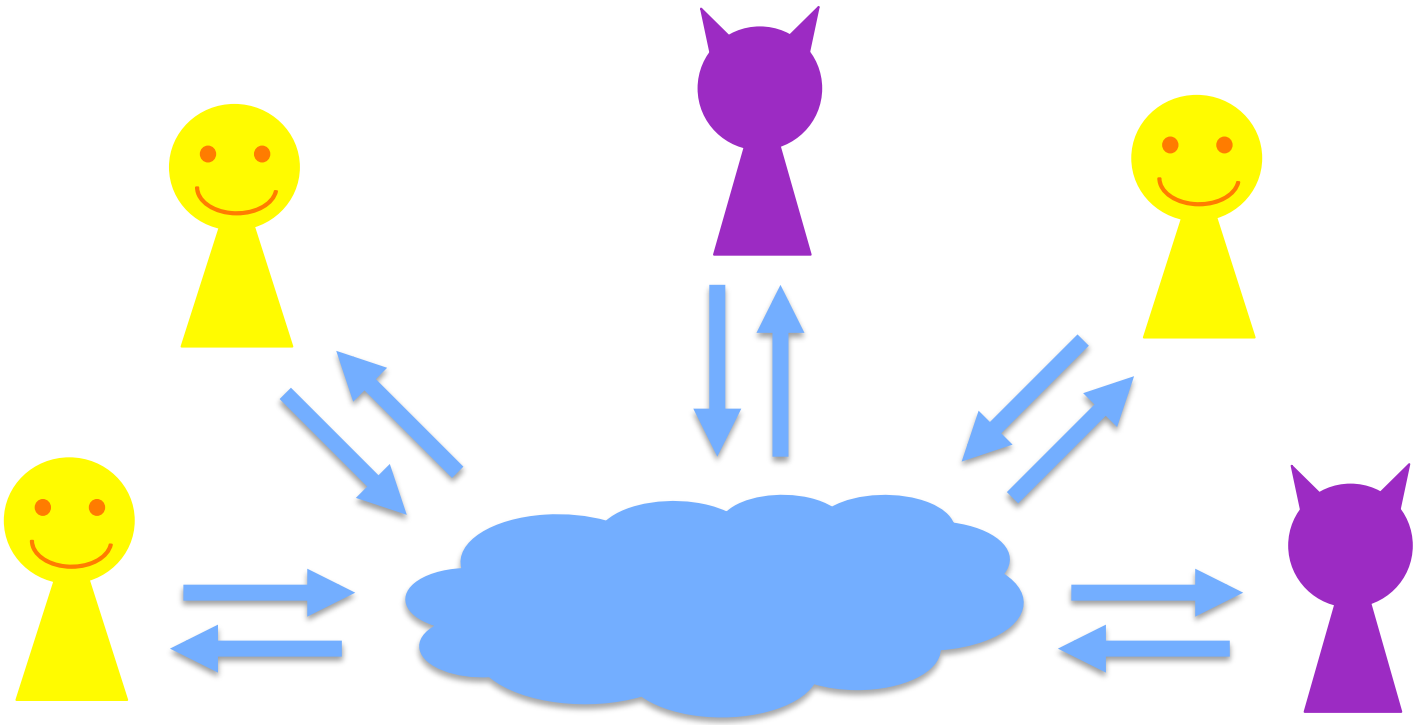
非同時通信路における合理的秘密分散

河内亮周（東工大） 岡本吉央（電通大）
田中圭介（東工大） 安永憲司（九州先端研）

暗号プロトコル

- 正直者と悪者が存在
- 悪者がいたとしても、プロトコルに従えば、正直者は目的を達成



プレイヤーに対する仮定

- 正直者は、常にプロトコルに従う
- 悪者は、可能な限りの邪魔をする

プレイヤーに対する仮定

- 正直者は、常にプロトコルに従う
- 悪者は、可能な限りの邪魔をする

- 極端すぎて現実的でないかも？
  - 正直者も、自分の利益のためなら、プロトコルに従わないかもしれない
  - 悪者も、目的を持って行動しているはず

プレイヤーに対する仮定

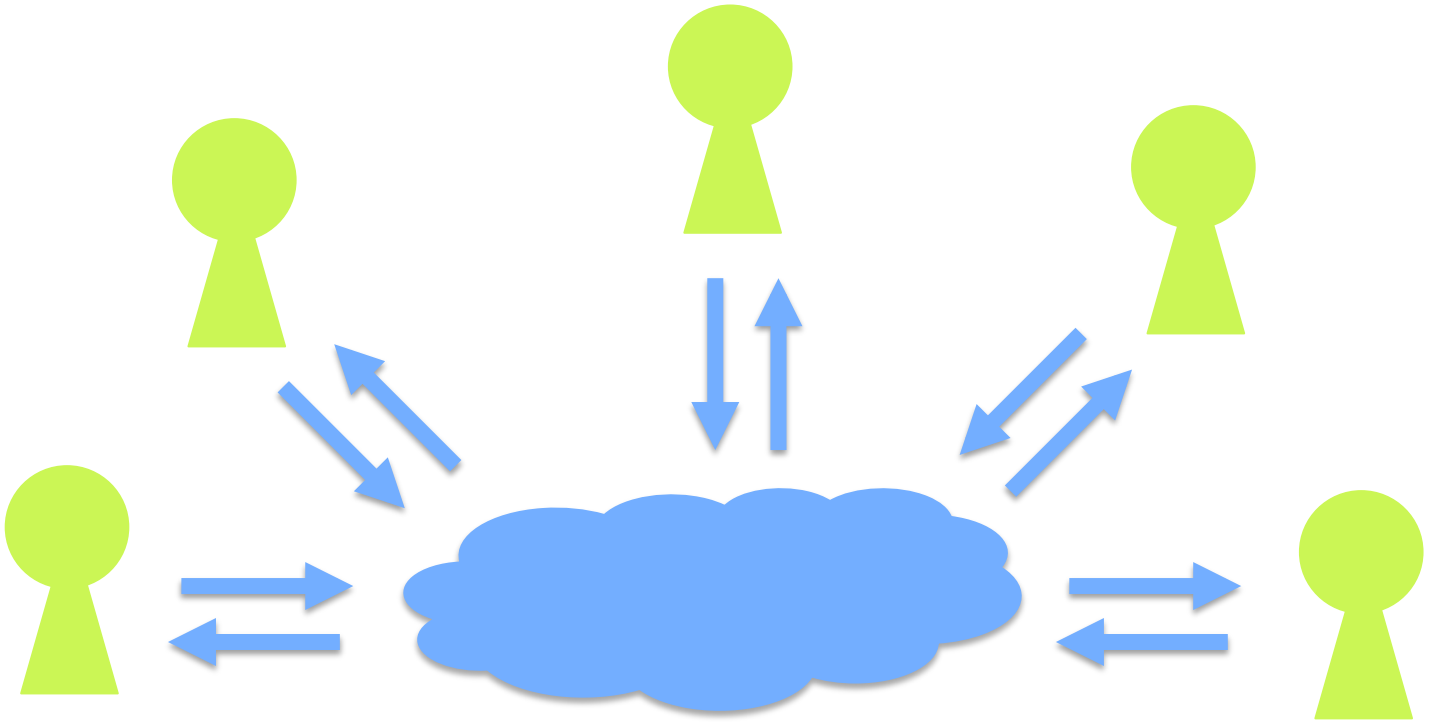
- 正直者は、常にプロトコルに従う
- 悪者は、可能な限りの邪魔をする

- 極端すぎて現実的でないかも？
  - 正直者も、自分の利益のためなら、プロトコルに従わないかもしれない
  - 悪者も、目的を持って行動しているはず

合理的なプレイヤー

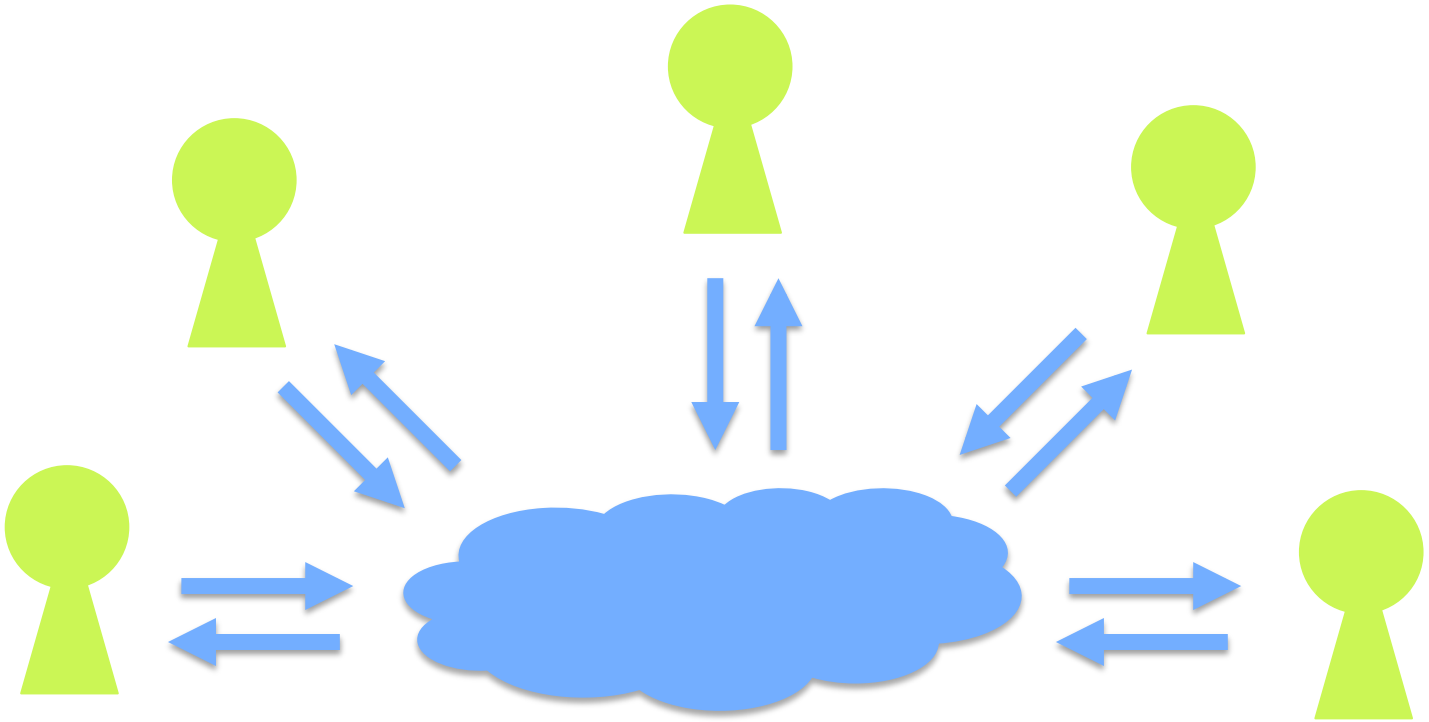
合理的なプレイヤー

- 自分の利得を最大化するために行動



合理的なプレイヤー

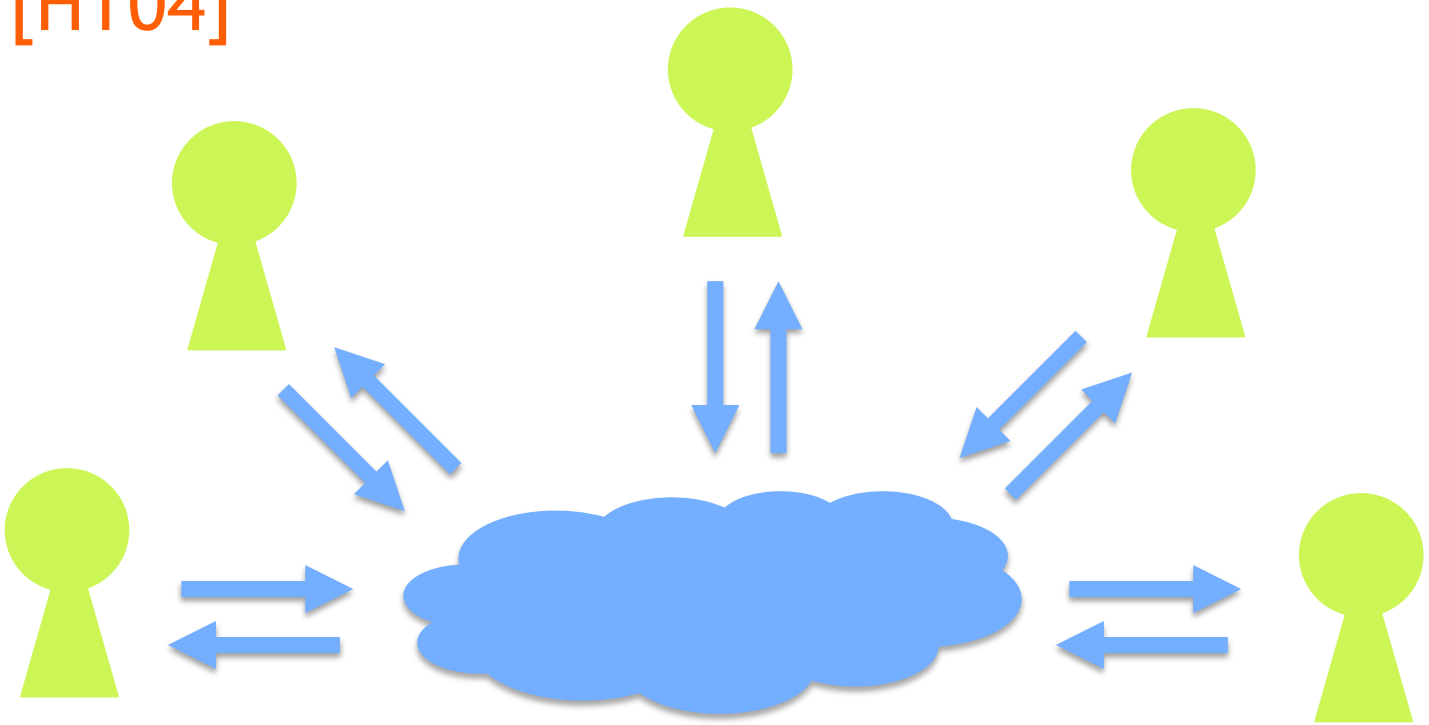
- 自分の利得を最大化するために行動
- 既存のプロトコルは正しく実行されるか？



合理的なプレイヤー

- 自分の利得を最大化するために行動
- 既存のプロトコルは正しく実行されるか？

→ Shamir の秘密分散は正しく実行されない [HT04]



秘密分散

- 参加者：ディーラー１人とプレイヤー n 人
- ２フェーズから構成
  - 分散フェーズ：
    ディーラーが、秘密からシェアを作り、
    各プレイヤーに配る
  - 復元フェーズ：
    シェアを出し合うことで秘密を復元
- (m, n) しきい値型秘密分散
  - m 個のシェアから秘密を復元でき
    m 個未満からは秘密について情報がもれない

[Halpern, Teague 2004]

[Halpern, Teague 2004]

- プレイヤーの利得関数

1. 秘密を復元したい
2. より少ない人数で復元したい

[Halpern, Teague 2004]

- プレイヤーの利得関数

1. 秘密を復元したい
2. より少ない人数で復元したい

Shamir の秘密分散では
復元フェーズが正しく実行されない

[Halpern, Teague 2004]

- プレイヤーの利得関数

1. 秘密を復元したい
2. より少ない人数で復元したい

Shamir の秘密分散では
復元フェーズが正しく実行されない

→ ゲーム理論による分析

戦略と Nash 均衡

- プレイヤー i の戦略 σ_i
  - どの状況でどの行動を取るかを記述したもの

- 戦略の組 $\sigma = (\sigma_1, \ldots, \sigma_n)$ が Nash 均衡

$\Leftrightarrow$ $\forall i, \forall \sigma_i', U_i(\sigma_i', \sigma_{-i}) \leq U_i(\sigma)$,

$U_i(\sigma)$：戦略 σ に従ったときの期待利得

どのプレイヤーも、他のプレイヤーが σ に従う限り、
戦略 σ から逸脱しても、利得は増えない

Shamir の (m, n) 秘密分散の問題点

- 復元フェーズで、
  全員がシェアを出すという戦略はよくない

- 認証つき秘密分散を仮定すると
  プレイヤーの選択肢は実質的に２つ
  - シェアを「出す」
  - シェアを「出さない」

Shamir の (m, n) 秘密分散の問題点

- m = n のとき
  - 「出す」　　→ n 人で復元
  - 「出さない」 → 1 人で復元

Nash 均衡ではない

- m < n のとき
  - シェアを出しても出さなくても n 人で復元
  - 「出さない」が「出す」より悪い状況はなく、また、ある状況では真に良い

弱支配される Nash 均衡

既存研究

文献	通信路	その他の仮定	MPC	ラウンド数	解概念	連携耐性
[HT04]	同時同報	秘密通信路	✔	O(1/β)	IEWDS	
[ADGH06]	同時同報		✔	2	IEWDS	n/2 − 1
[GK06]	同時同報		✔	O(1/β)	IEWDS	n − 1
[KN08a]	同時同報	M/M Enc.	✔	O(1/β)	IEWDS	
[KN08b]	同時同報			O(1/β)	strict NE	1
[OPRV09]	同報	正直者		2	THPE	
[AL09]	同時同報	[GK06] 等		2	IEWDS	n/2 − 1
[FKN10]	P2P	VRF		O(1/β)	strict NE	n − 1

IEWDS = 弱支配戦略の連続的削除
strict NE = strict Nash 均衡
THPE = 摂動完全均衡

β：利得に依存する十分小さな値

既存研究

文献	通信路	その他の仮定	MPC	ラウンド数	解概念	連携耐性
[HT04]	同時同報	秘密通信路	✔	O(1/β)	IEWDS	
[ADGH06]	同時同報		✔	2	IEWDS	n/2 − 1
[GK06]	同時同報		✔	O(1/β)	IEWDS	n − 1
[KN08a]	同時同報	M/M Enc.	✔	O(1/β)	IEWDS	
[KN08b]	同時同報			O(1/β)	strict NE	1
[OPRV09]	同報	正直者		2	THPE	
[AL09]	同時同報	[GK06] 等		2	IEWDS	n/2 − 1
[FKN10]	P2P	VRF		O(1/β)	strict NE	n − 1

IEWDS = 弱支配戦略の連続的削除
strict NE = strict Nash 均衡
THPE = 摂動完全均衡

β：利得に依存する十分小さな値

strict Nash 均衡と連携耐性

- 戦略の組 $\sigma = (\sigma_1, \ldots, \sigma_n)$ が strict Nash 均衡

$\Leftrightarrow$ $\forall i, \forall \sigma_i' \neq \sigma_i, \exists \delta > 0, U_i(\sigma_i', \sigma_{-i}) \leq U_i(\sigma) - \delta,$

σ 以外の戦略を取ると、利得が真に下がる

- 戦略の組 σ が連携耐性 r の Nash 均衡

$\Leftrightarrow$ $\forall$ 連携 $C \subseteq \{1, 2, \ldots, n\}$ s.t. $|C| \leq r$,
$\forall \sigma_C', \ U_C(\sigma_C', \sigma_{-C}) \leq U_C(\sigma_C, \sigma_{-C})$

  - 連携耐性 1 の Nash 均衡 =（通常の）Nash 均衡
  - 提携耐性 r の strict Nash 均衡 も同様に定義

r 人が連携しても、 σ は Nash 均衡

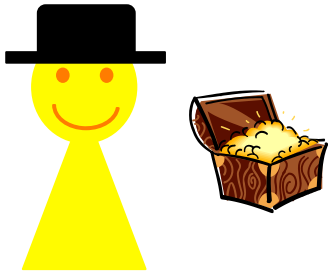
本研究の成果

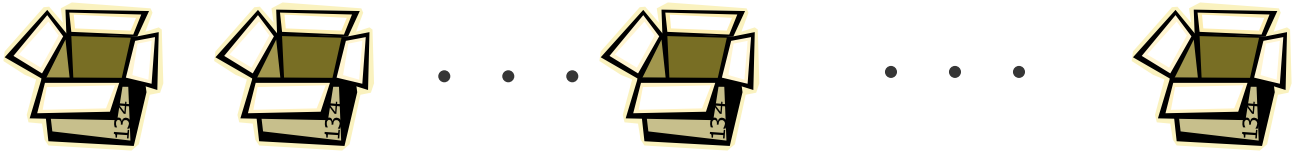
- 合理的秘密分散 (RSS) の一般的変換法の提案
  - 任意の RSS を（ブラックボックス的に使い）平均 2 ラウンドで復元する RSS に変換
  - 連携耐性 n/2 – 1 の strict Nash 均衡を保つ
    - 定数ラウンド復元 RSS で最適な連携耐性 [AL09]
  - （非同時）同報通信路を仮定
    - 同時同報通信路の場合、平均 1 ラウンドで復元

既存研究との比較

文献	通信路	その他の仮定	MPC	ラウンド数	解概念	連携耐性
[HT04]	同時同報	秘密通信路	✔	O(1/β)	IEWDS	
[ADGH06]	同時同報		✔	2	IEWDS	n/2 – 1
[GK06]	同時同報		✔	O(1/β)	IEWDS	n – 1
[KN08a]	同時同報	M/M Enc.	✔	O(1/β)	IEWDS	
[KN08b]	同時同報			O(1/β)	strict NE	1
[OPRV09]	同報	正直者		2	THPE	
[AL09]	同時同報	[GK06] 等		2	IEWDS	n/2 – 1
[FKN10]	P2P	VRF		O(1/β)	strict NE	n – 1
本研究	同報	既存の RSS		2	strict NE	n/2 – 1

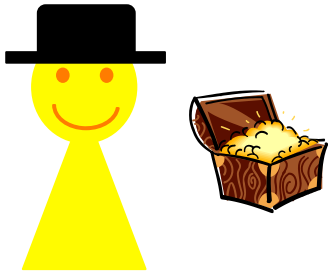
提案プロトコル （分散フェーズ）

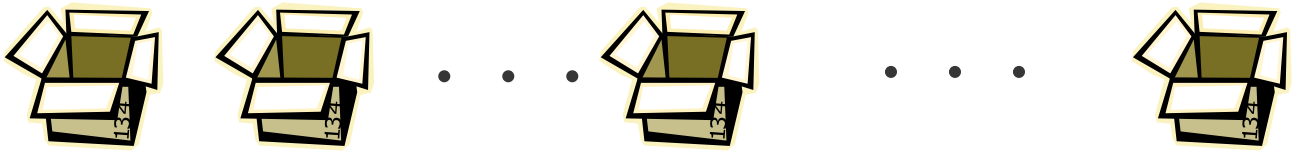




提案プロトコル （分散フェーズ）

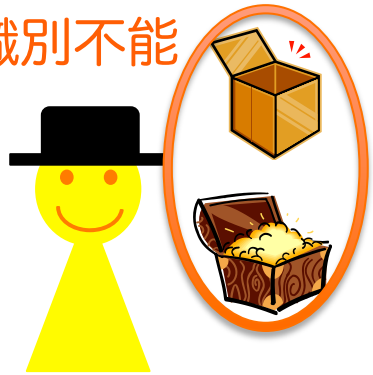
1. 通常の SS S_1

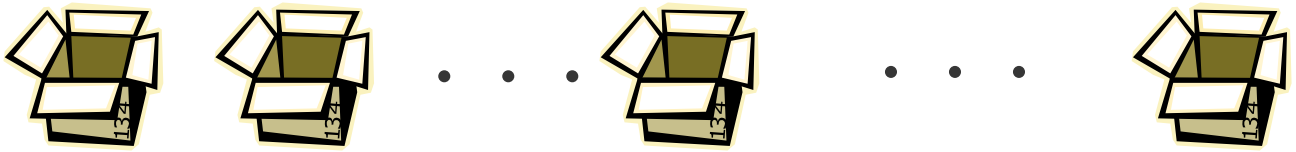




提案プロトコル （分散フェーズ）

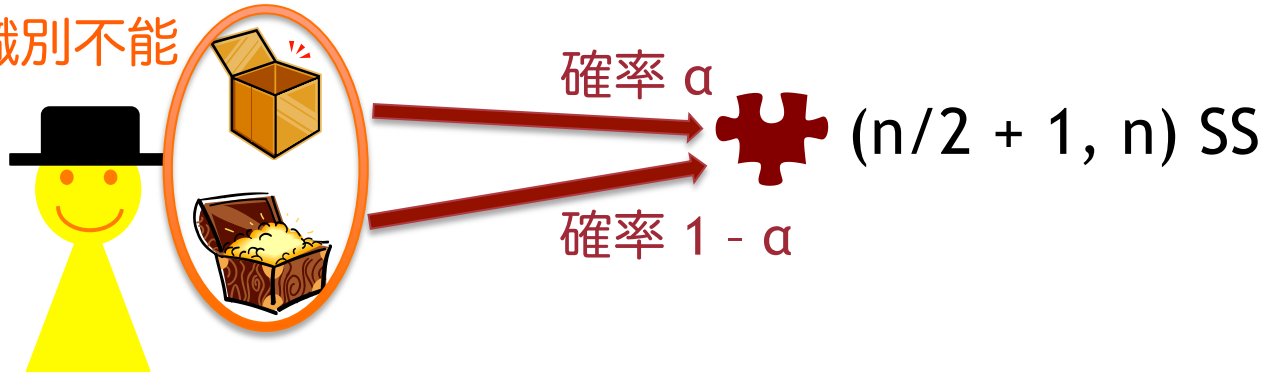
1. 通常の SS S_1

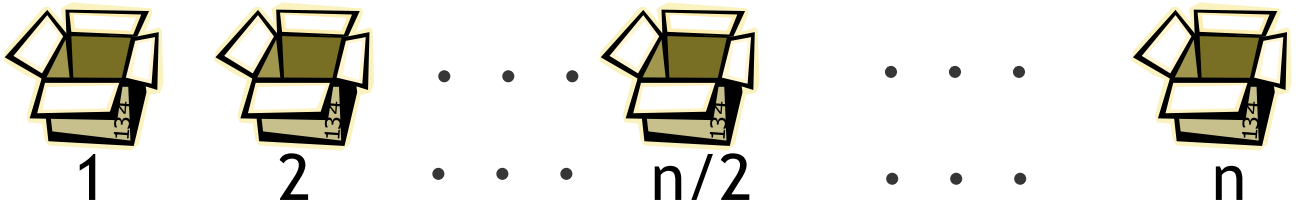




提案プロトコル （分散フェーズ）

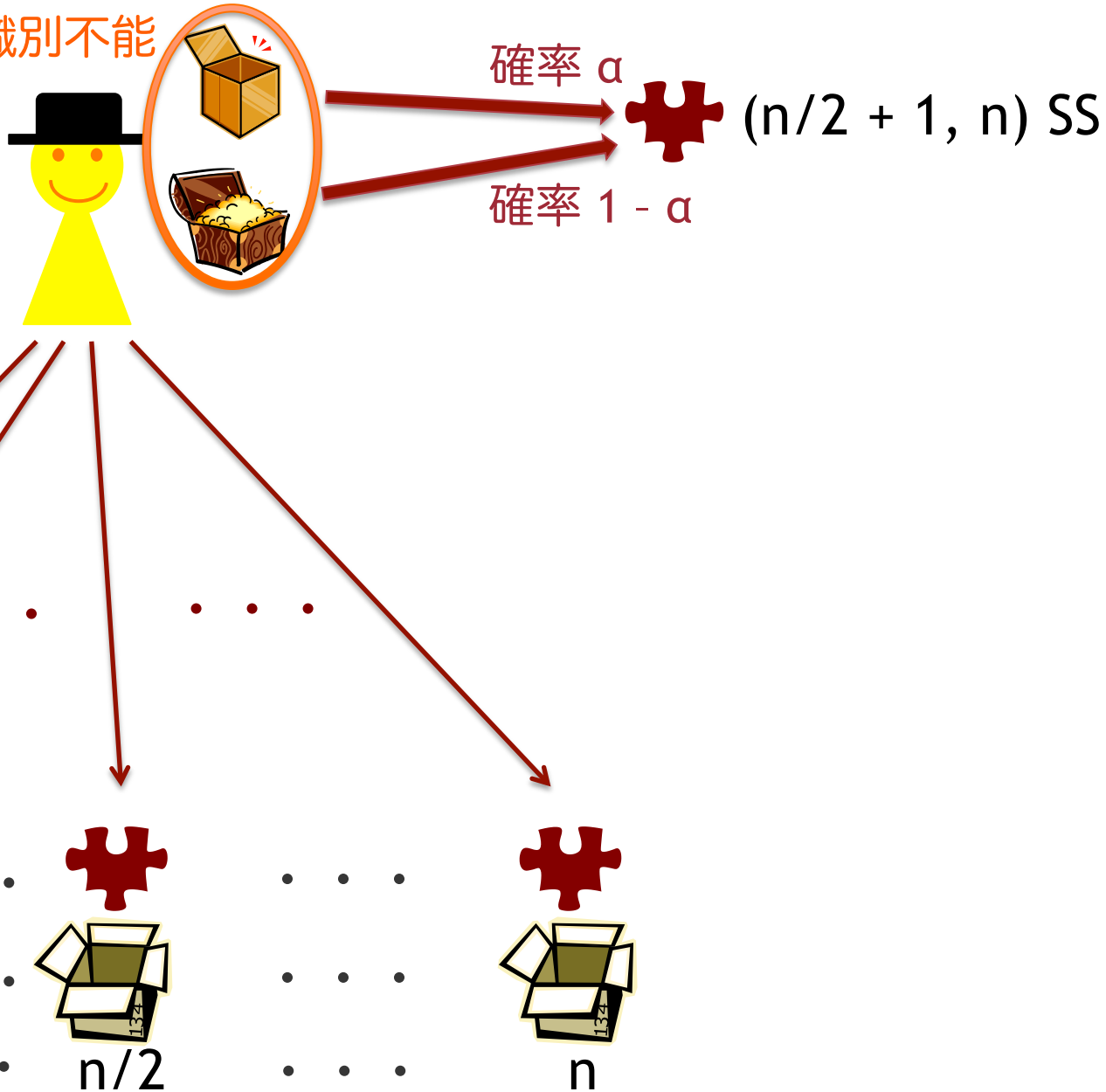
1. 通常の SS S_1





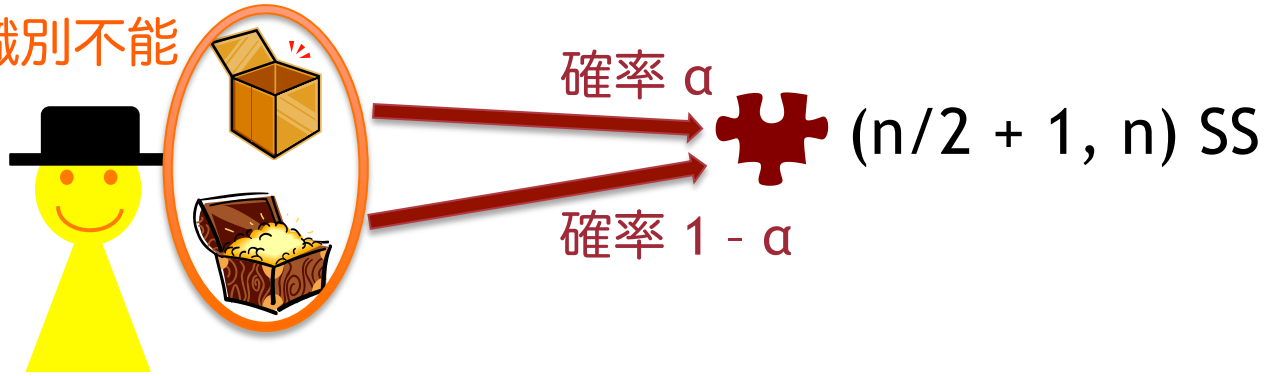
提案プロトコル （分散フェーズ）

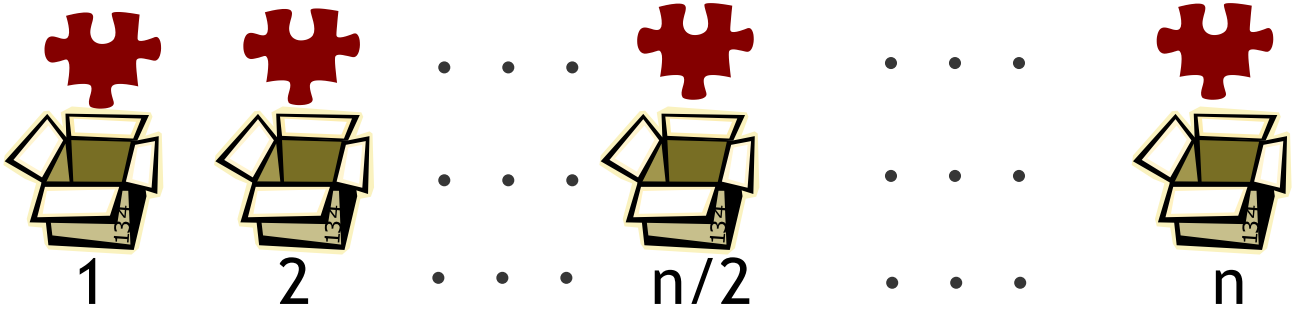
1. 通常の SS S_1



提案プロトコル （分散フェーズ）

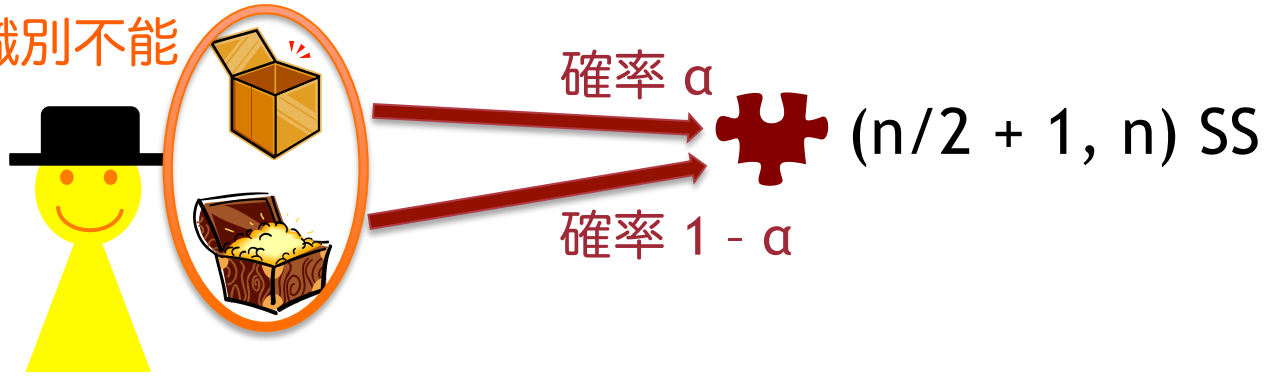
1. 通常の SS S_1

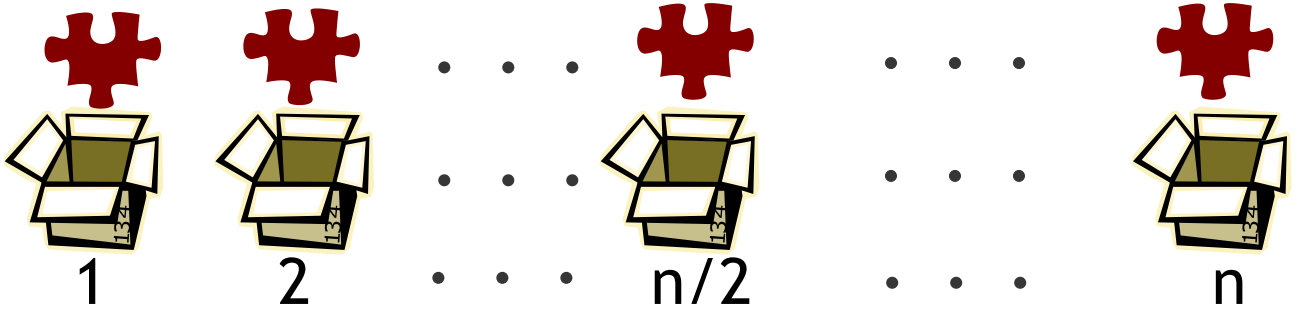




提案プロトコル （分散フェーズ）

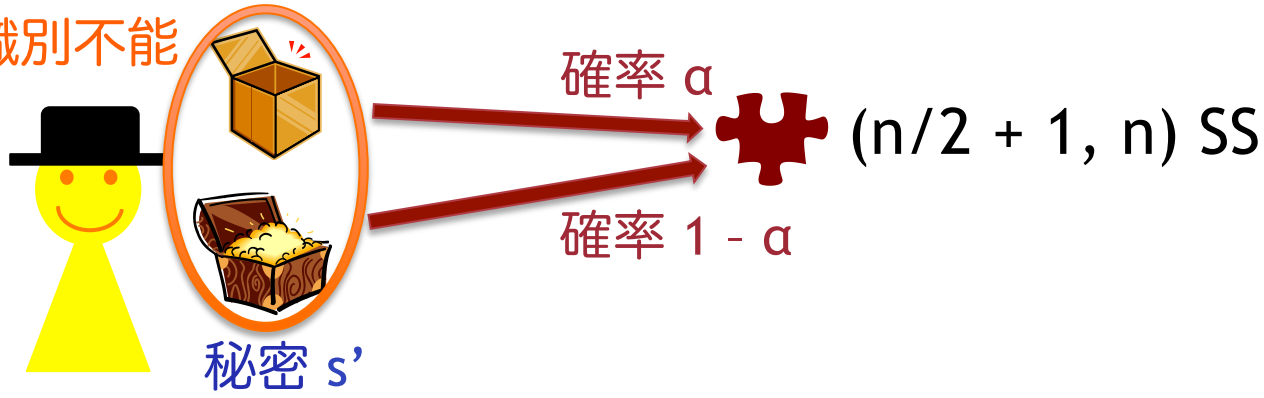
1. 通常の SS S_1
2. 通常の SS S_2





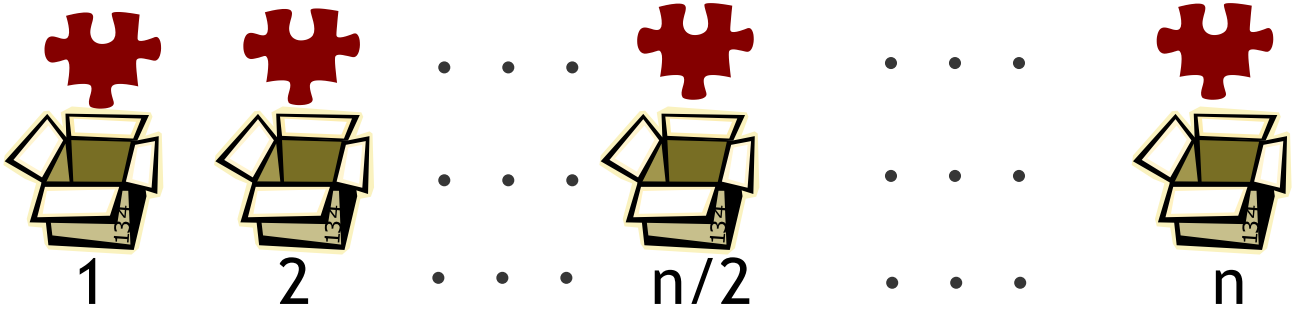
提案プロトコル （分散フェーズ）

1. 通常の SS S_1
2. 通常の SS S_2



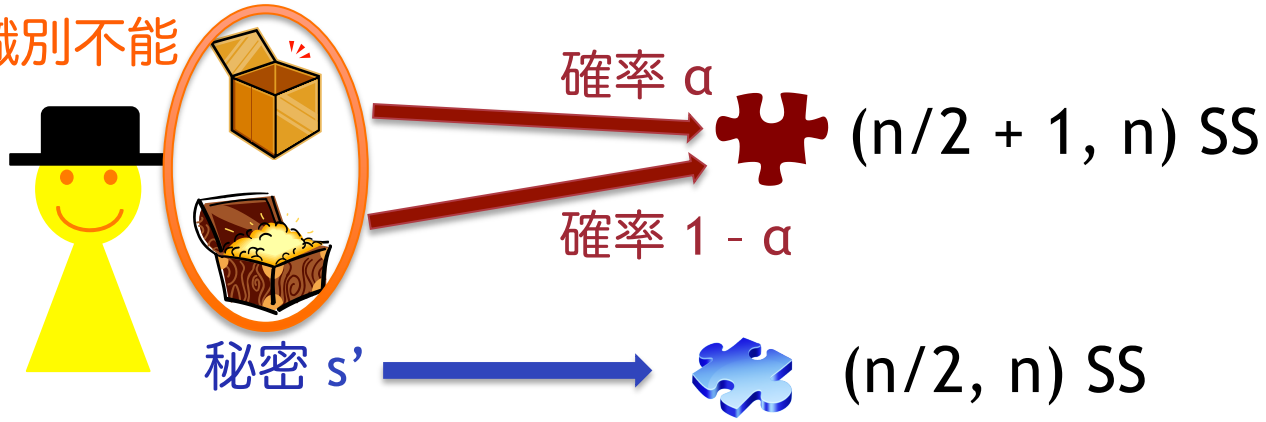
秘密 s’

$$= \begin{cases} 1\ (S_1 \text{ で本物}) \\ 0\ (S_1 \text{ で偽物}) \end{cases}$$



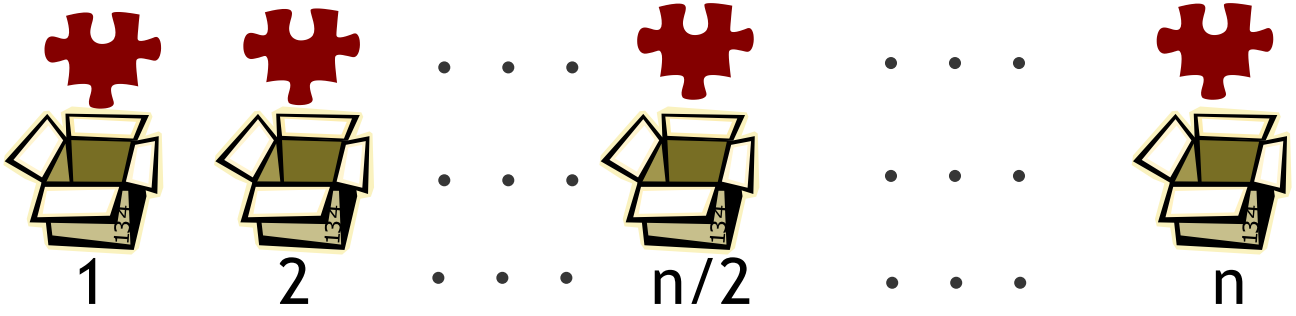
提案プロトコル （分散フェーズ）

1. 通常の SS S_1
2. 通常の SS S_2



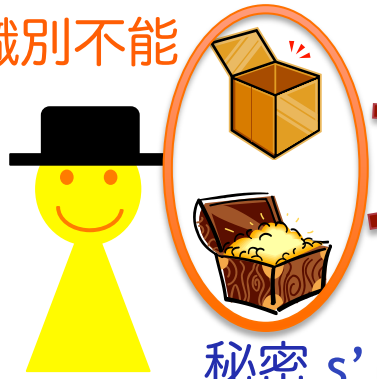
秘密 s’

$$= \begin{cases} 1\ (S_1 \text{ で本物}) \\ 0\ (S_1 \text{ で偽物}) \end{cases}$$



提案プロトコル （分散フェーズ）

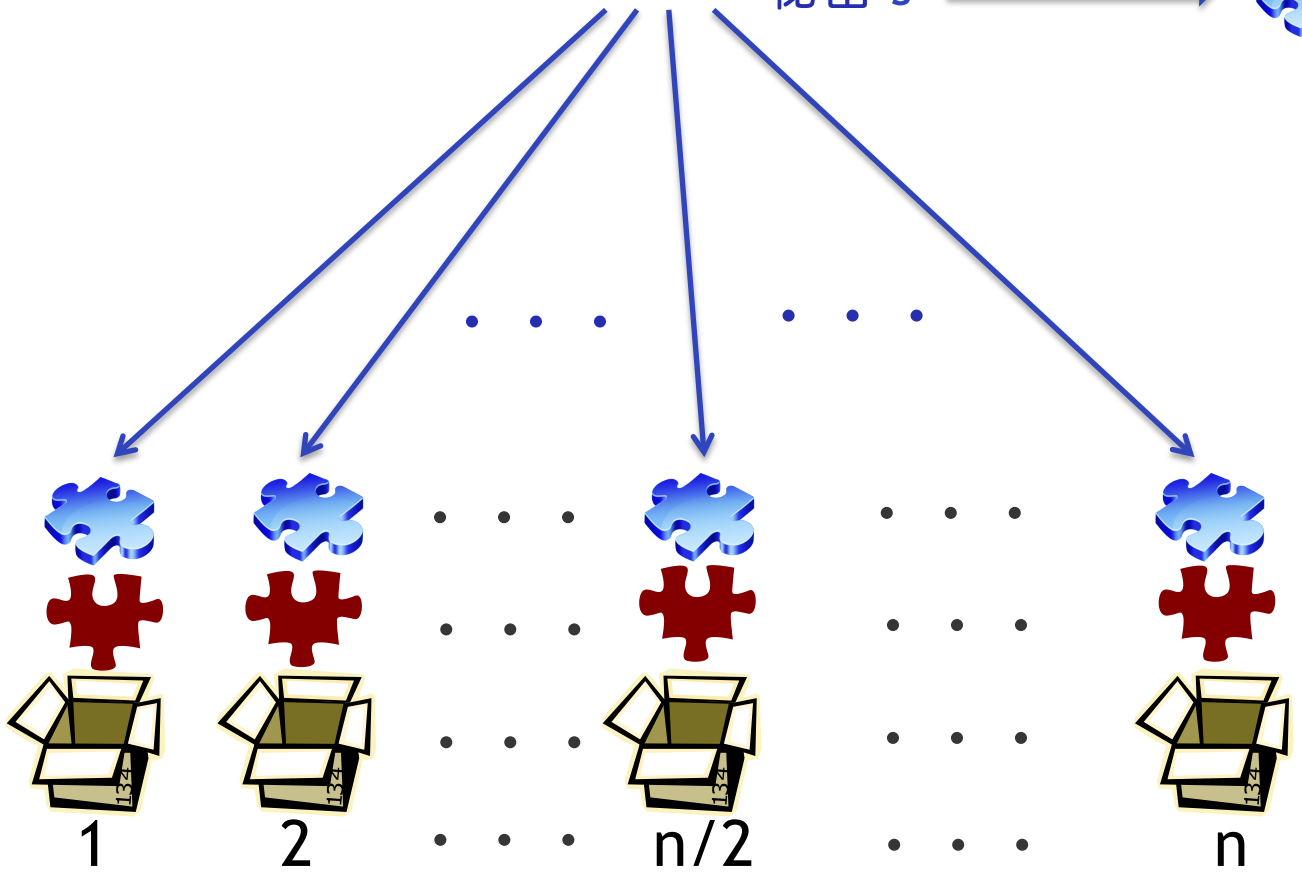
1. 通常の SS S_1
2. 通常の SS S_2



確率 α → (n/2 + 1, n) SS

確率 1 - α

秘密 s’ → (n/2, n) SS

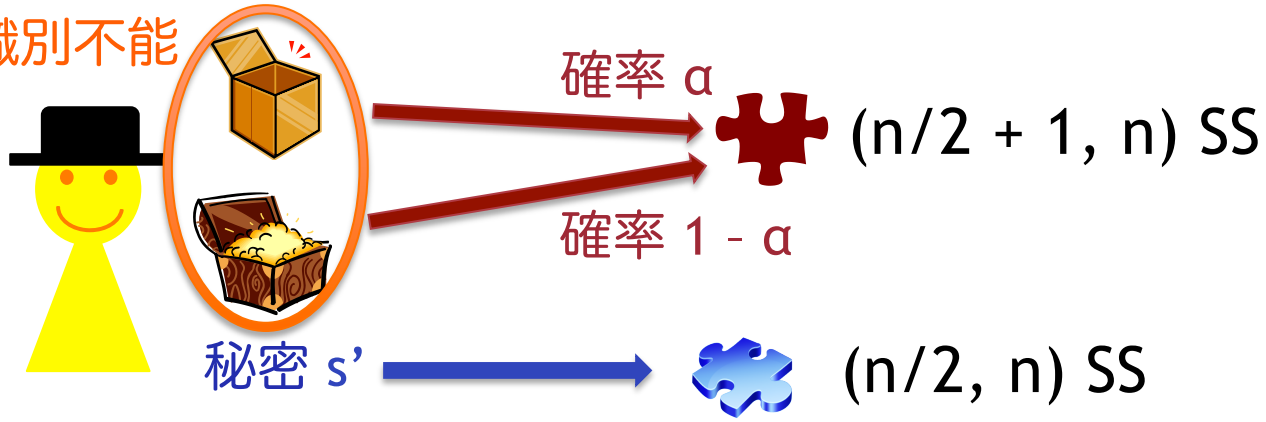


秘密 s’

$$= \begin{cases} 1\ (S_1 \text{ で本物}) \\ 0\ (S_1 \text{ で偽物}) \end{cases}$$

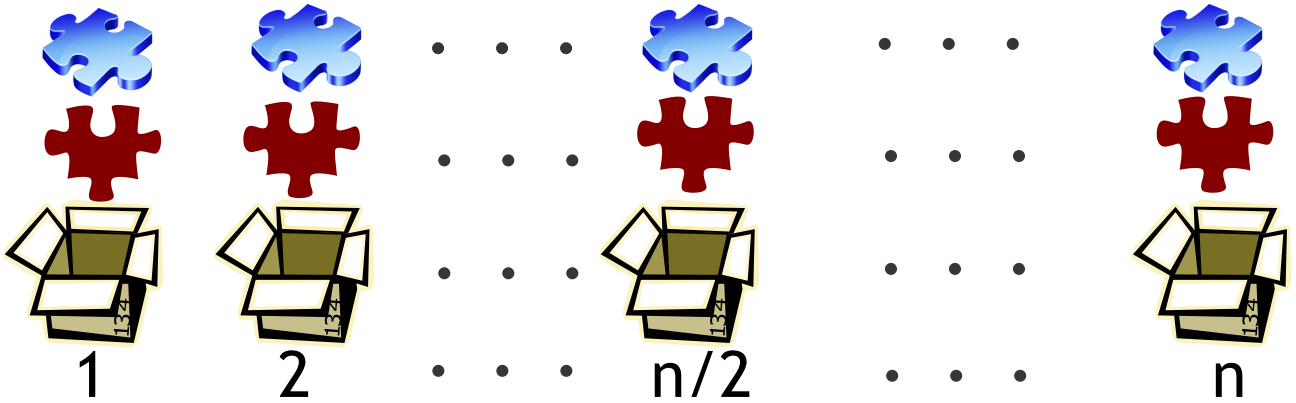
提案プロトコル （分散フェーズ）

1. 通常の SS S_1
2. 通常の SS S_2



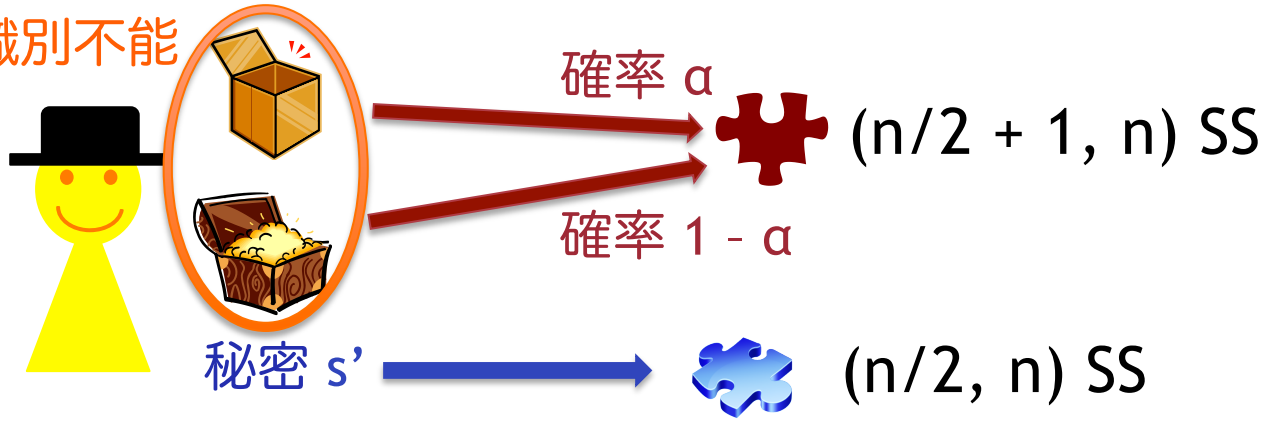
秘密 s’

$$= \begin{cases} 1\ (S_1 \text{ で本物}) \\ 0\ (S_1 \text{ で偽物}) \end{cases}$$



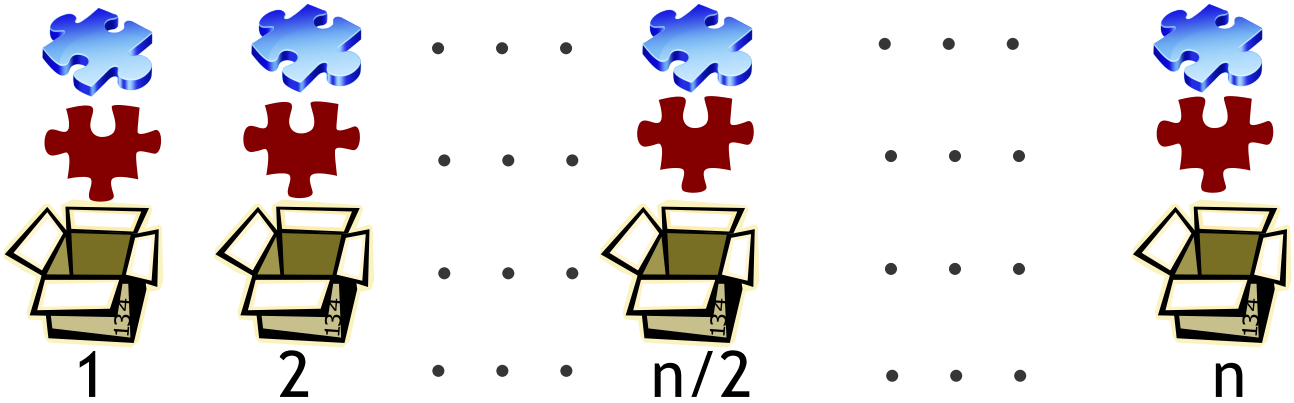
提案プロトコル （分散フェーズ）

1. 通常の SS S_1
2. 通常の SS S_2
3. RSS S_3



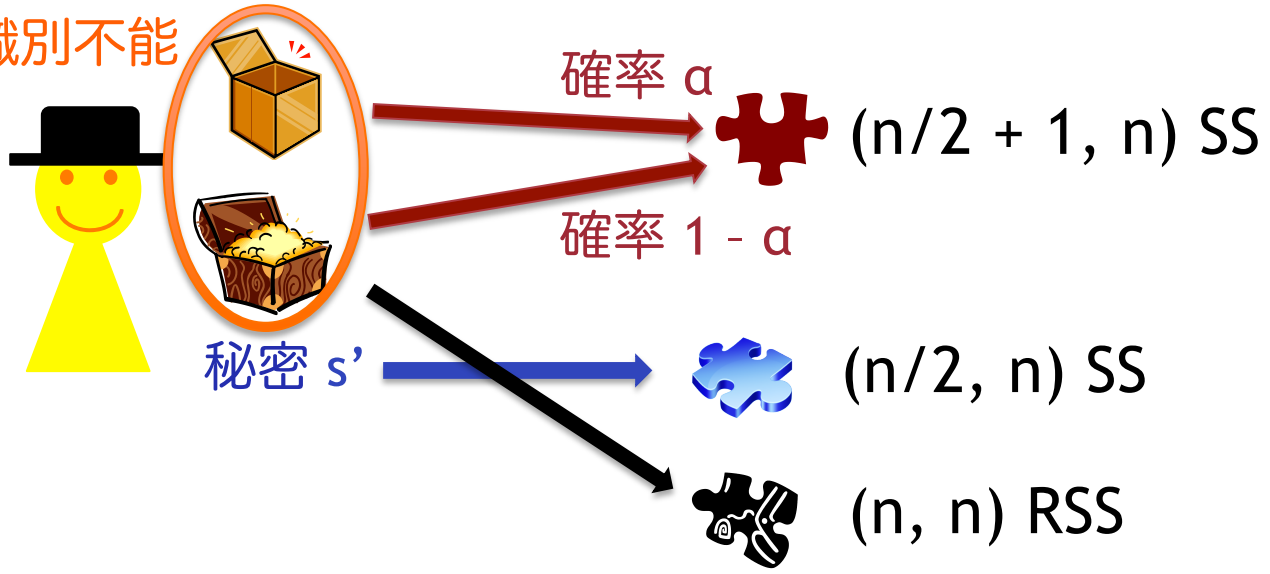
秘密 s’

$$= \begin{cases} 1\ (S_1 \text{ で本物}) \\ 0\ (S_1 \text{ で偽物}) \end{cases}$$



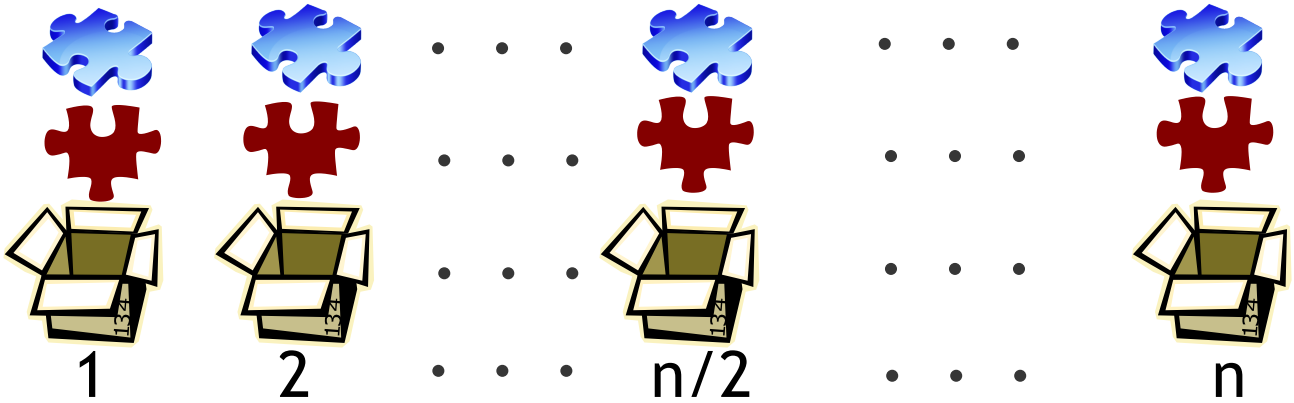
提案プロトコル （分散フェーズ）

1. 通常の SS S_1
2. 通常の SS S_2
3. RSS S_3



秘密 s’

$$= \begin{cases} 1\ (S_1 \text{ で本物}) \\ 0\ (S_1 \text{ で偽物}) \end{cases}$$



提案プロトコル （分散フェーズ）

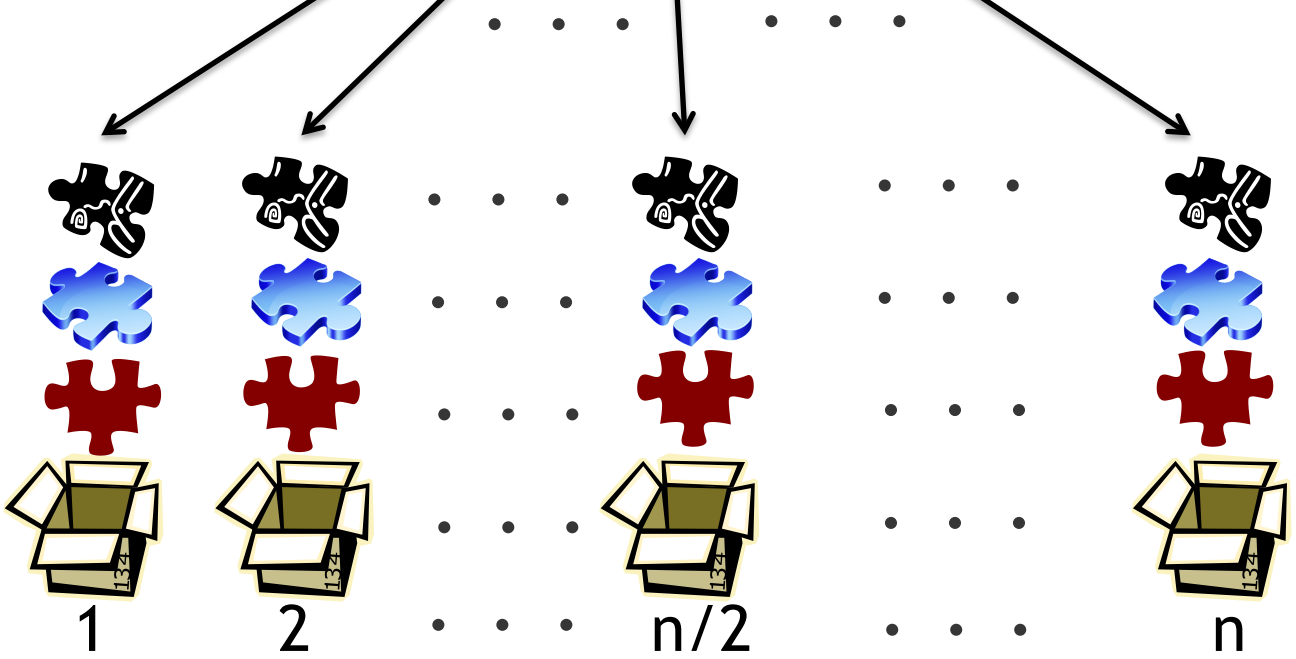
1. 通常の SS S_1
2. 通常の SS S_2
3. RSS S_3

確率 α → (n/2 + 1, n) SS

確率 1 - α

秘密 s’ → (n/2, n) SS

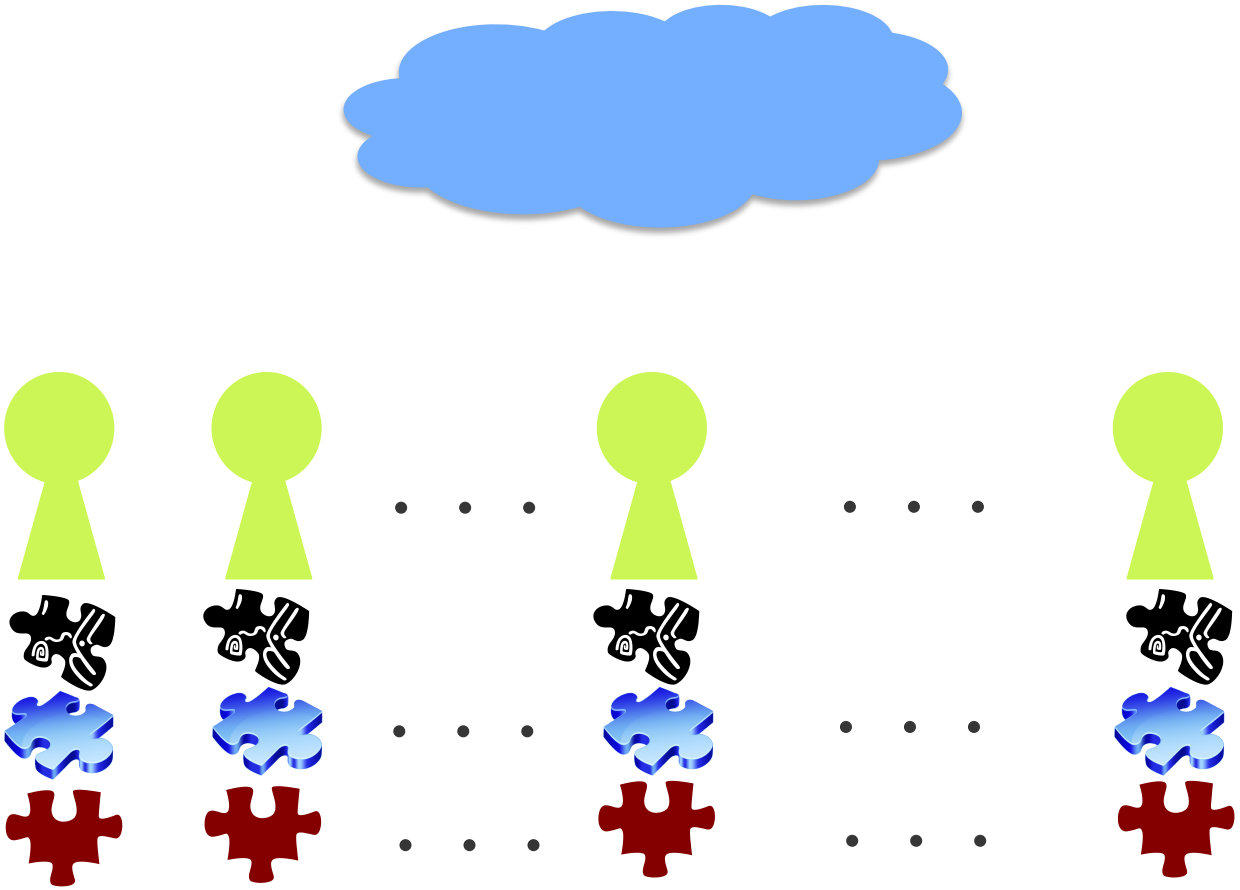
(n, n) RSS



秘密 s’

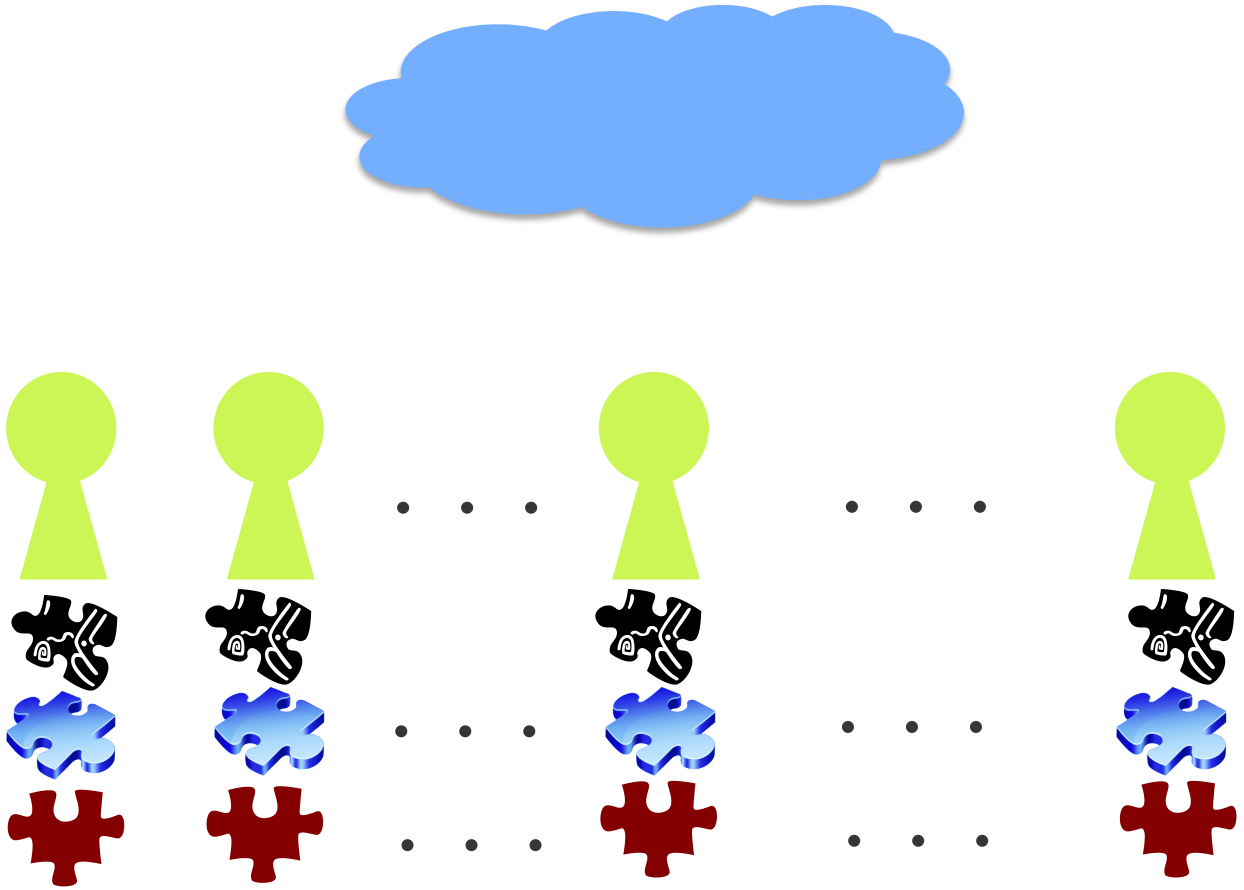
$$= \begin{cases} 1\ (S_1 \text{ で本物}) \\ 0\ (S_1 \text{ で偽物}) \end{cases}$$

提案プロトコル（復元フェーズ）



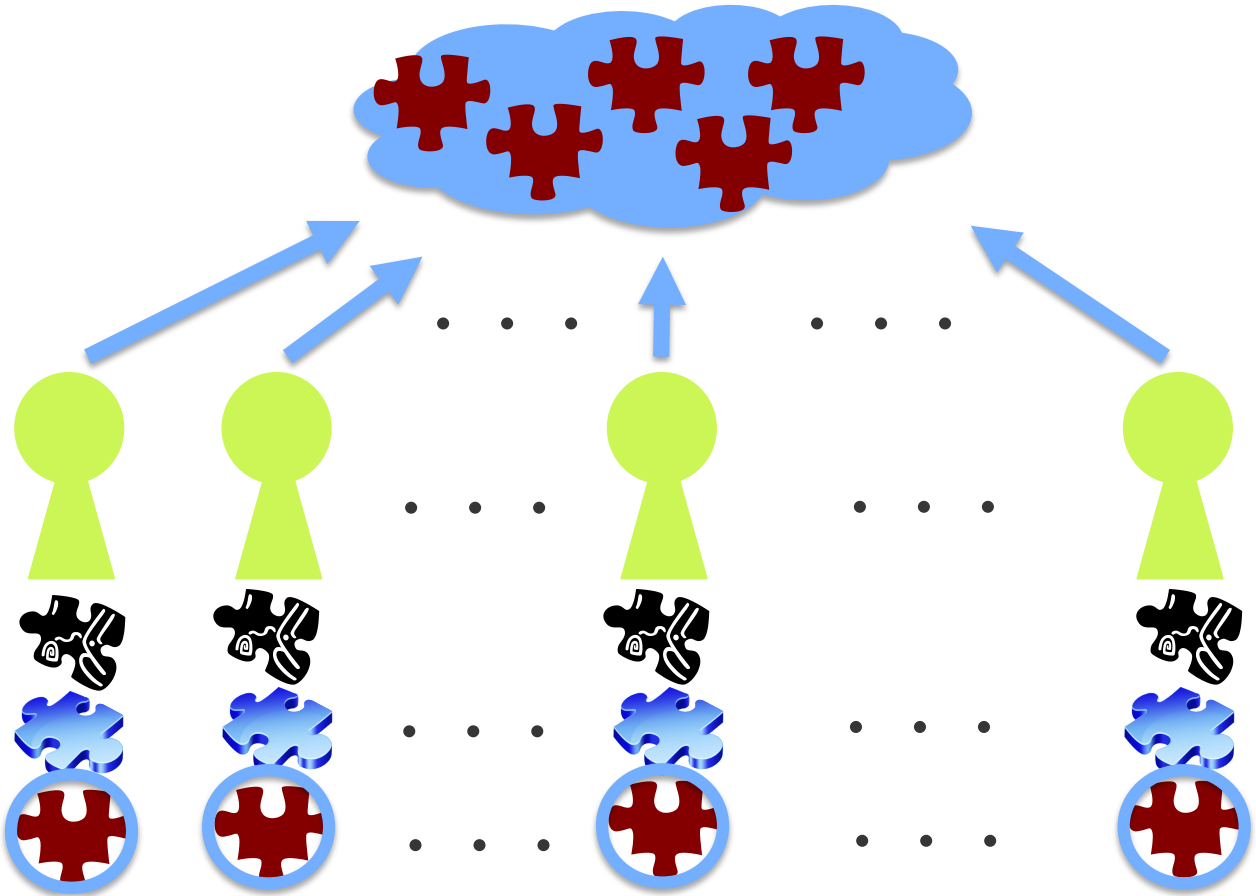
提案プロトコル（復元フェーズ）

Step 1. (n/2 + 1, n) SS S_1 のシェアを出す



提案プロトコル（復元フェーズ）

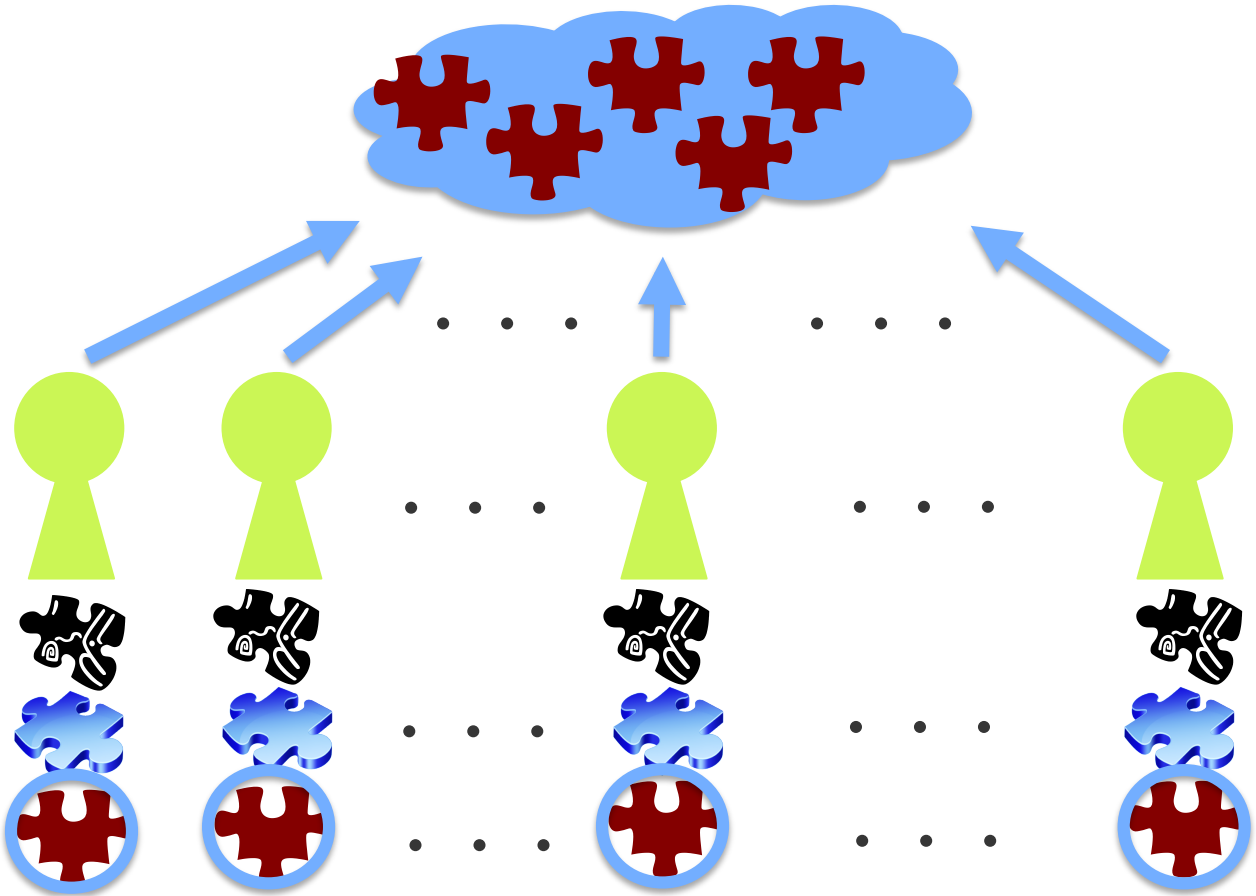
Step 1. (n/2 + 1, n) SS S_1 のシェアを出す



提案プロトコル（復元フェーズ）

Step 1. $(n/2 + 1, n)$ SS S_1 のシェアを出す

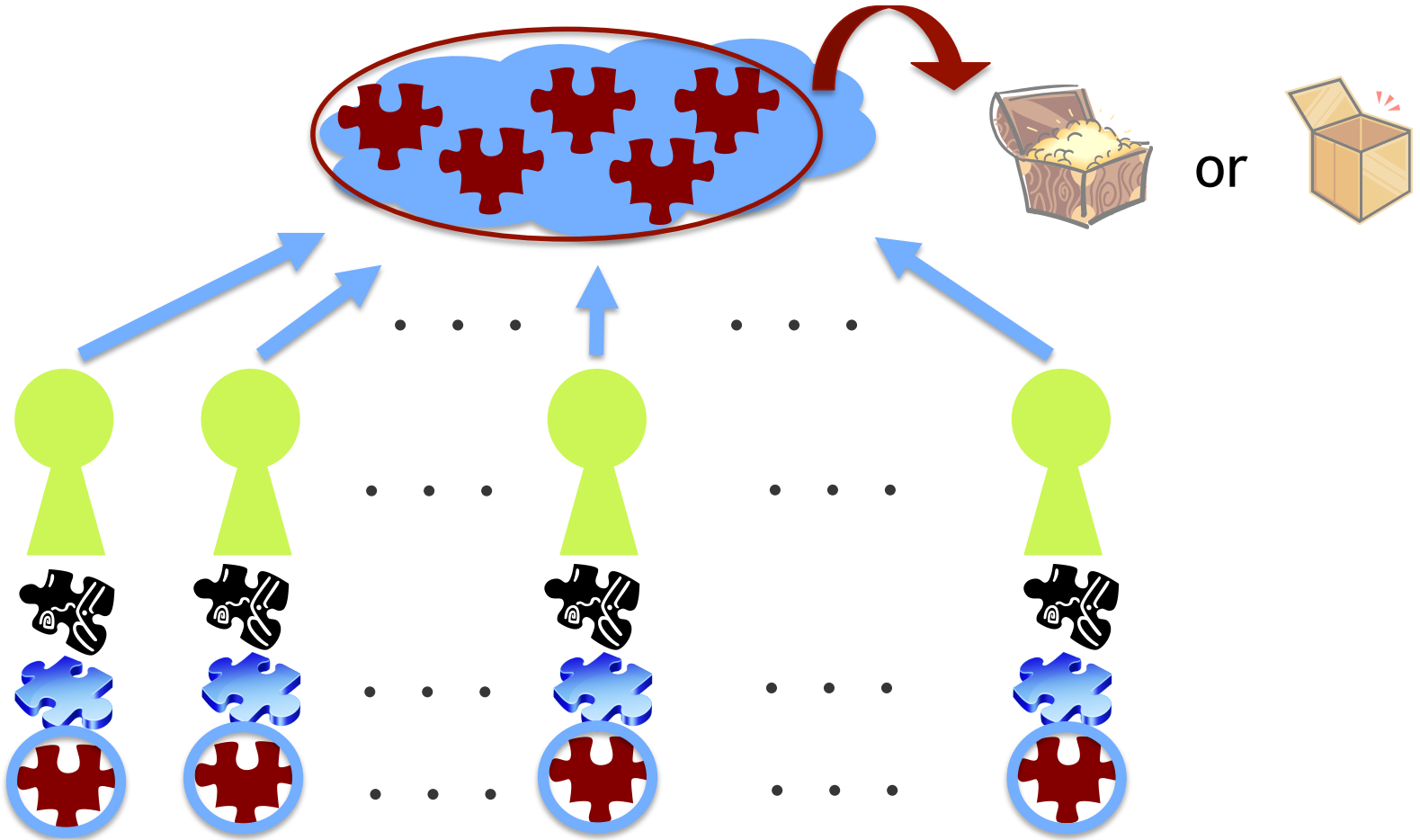
正しいシェアの数 $\geq n/2 + 1$ → 秘密 s を復元



提案プロトコル（復元フェーズ）

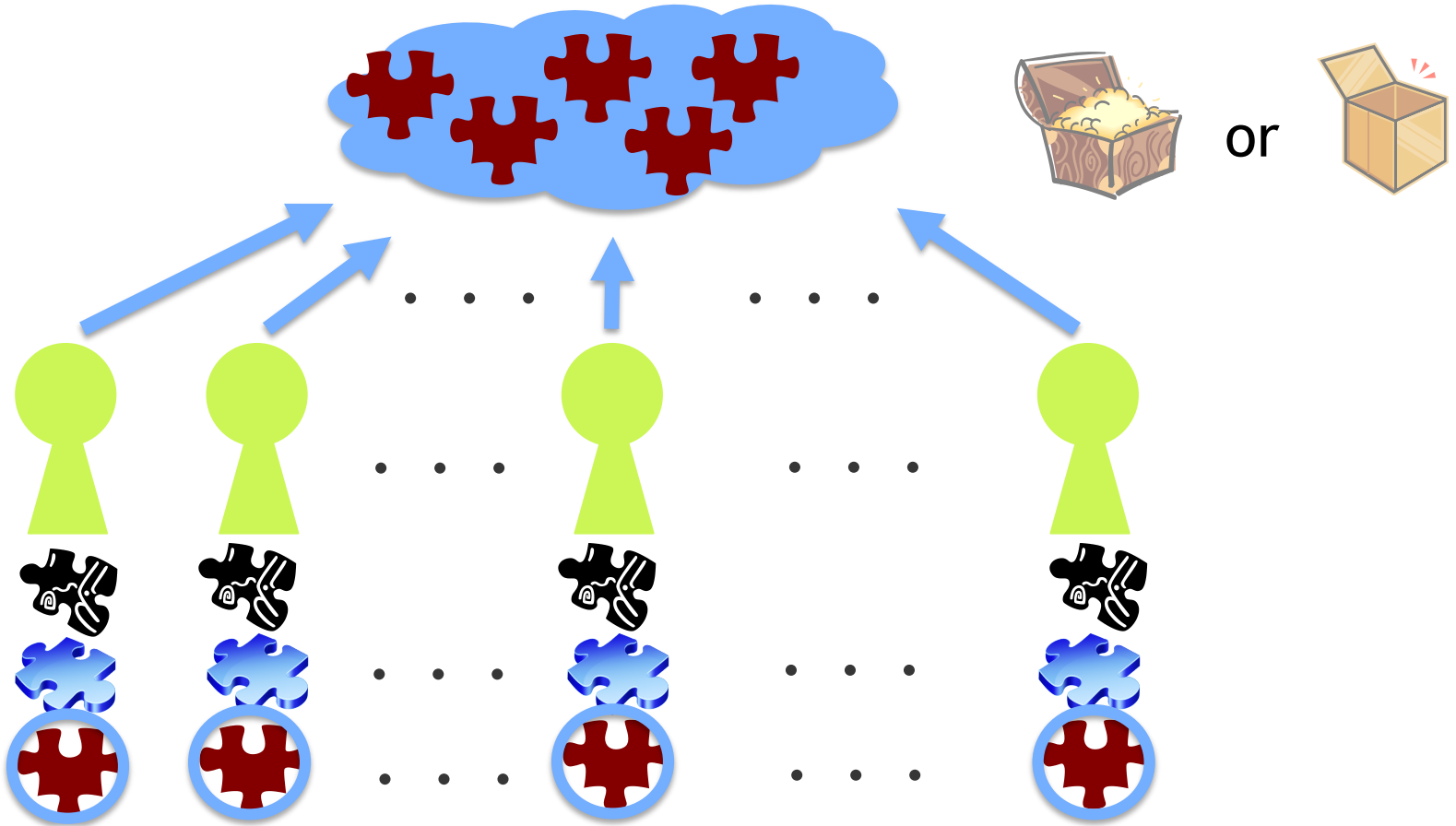
Step 1. (n/2 + 1, n) SS S_1 のシェアを出す

正しいシェアの数 ≥ n/2 + 1 → 秘密 s を復元



提案プロトコル（復元フェーズ）

Step 1. (n/2 + 1, n) SS S_1 のシェアを出す

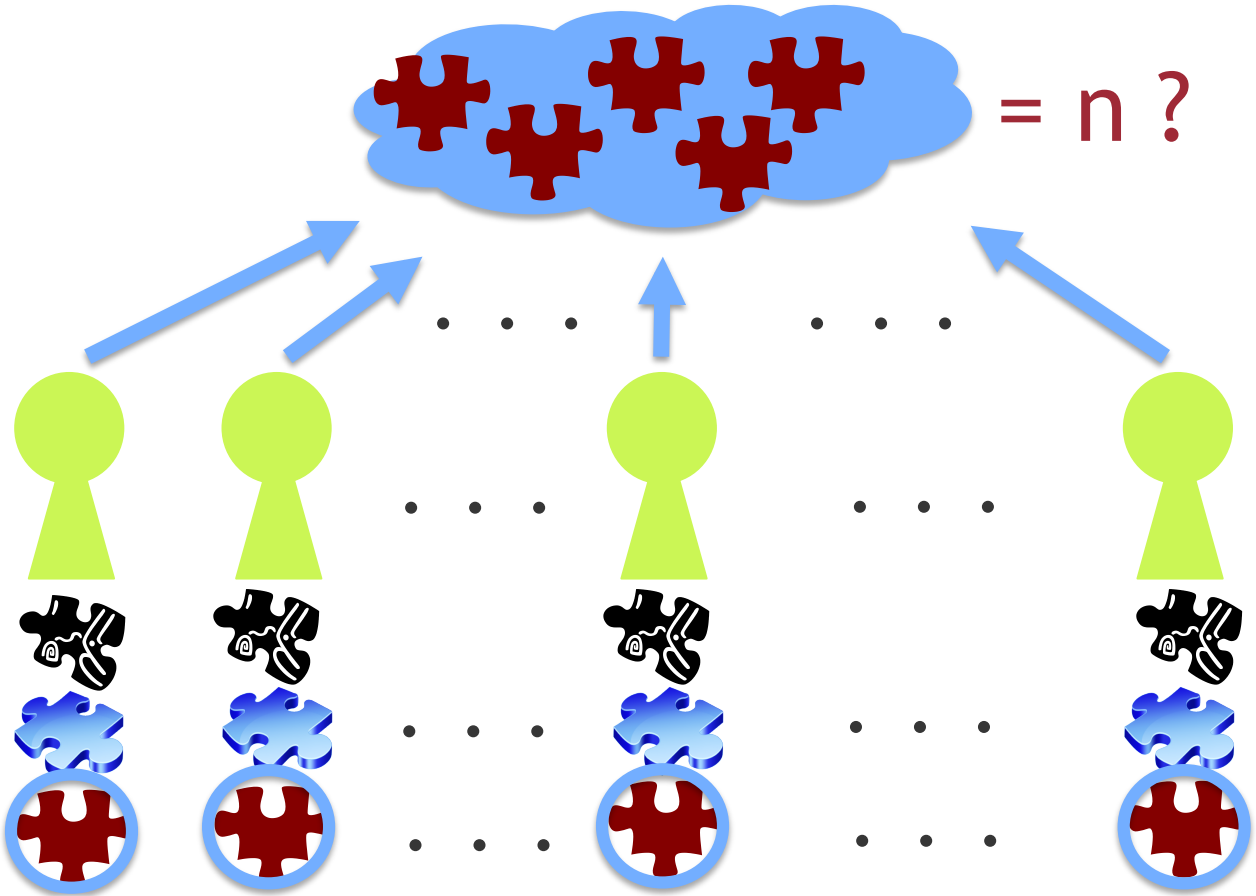


提案プロトコル（復元フェーズ）

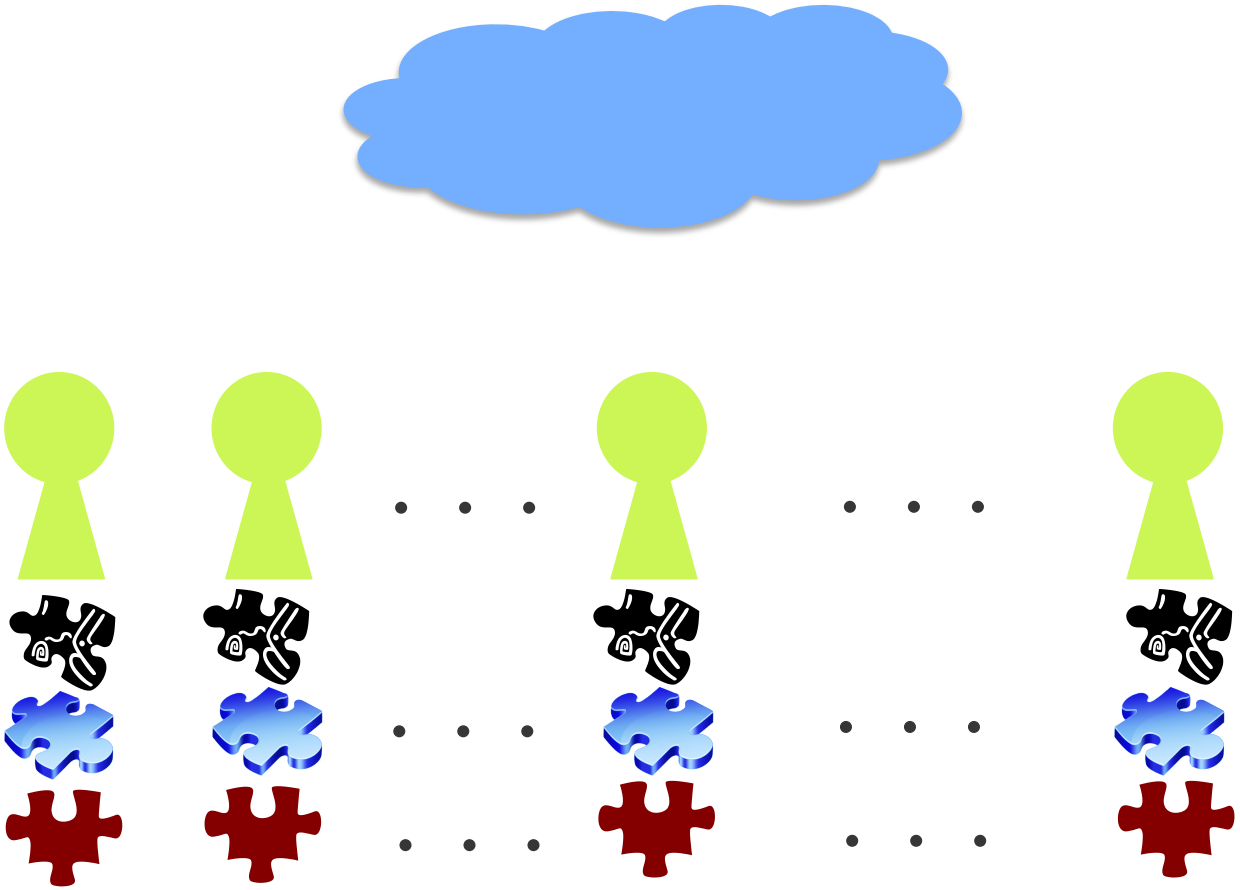
Step 1. (n/2 + 1, n) SS S_1 のシェアを出す

正しいシェアの数 < n → 終了（s を秘密として出力）

= n → 次のラウンドへ

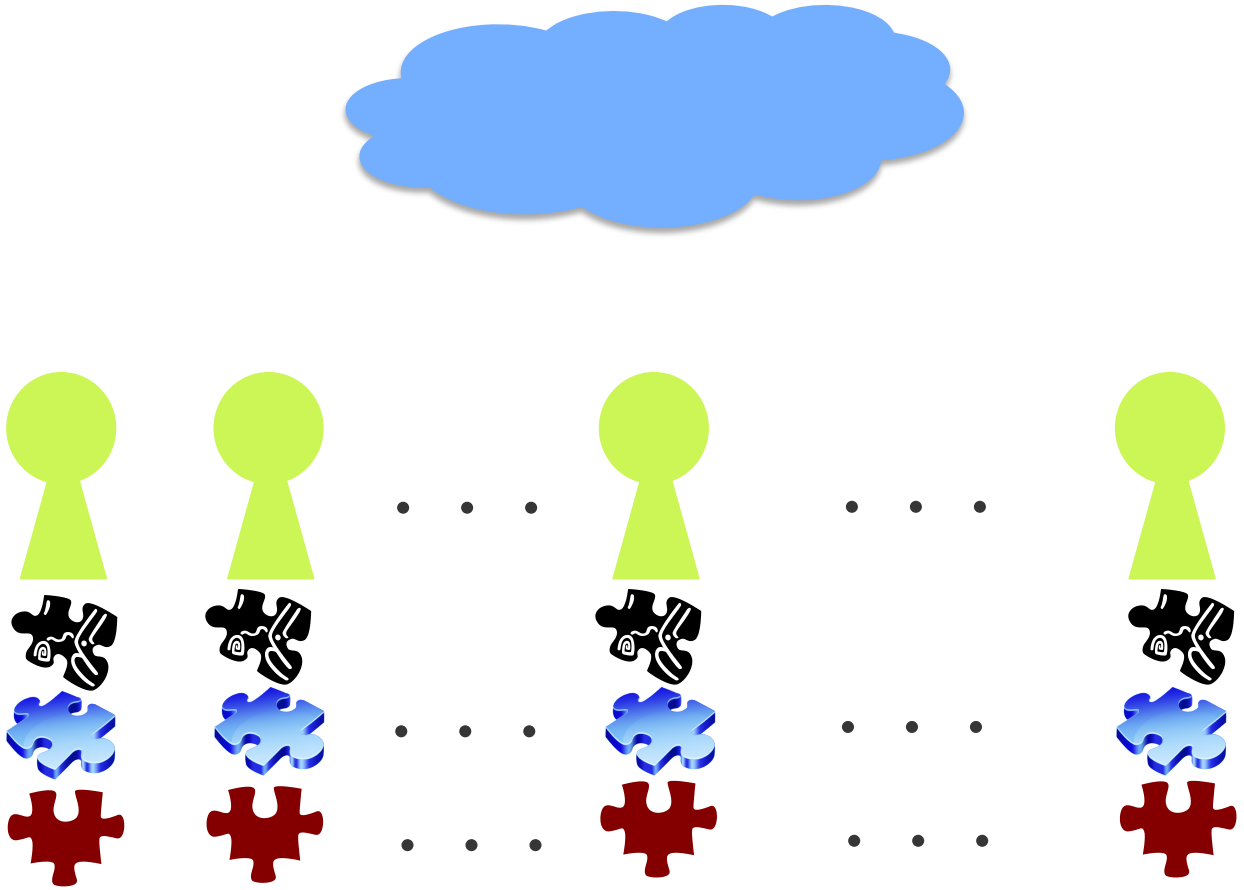


提案プロトコル（復元フェーズ）



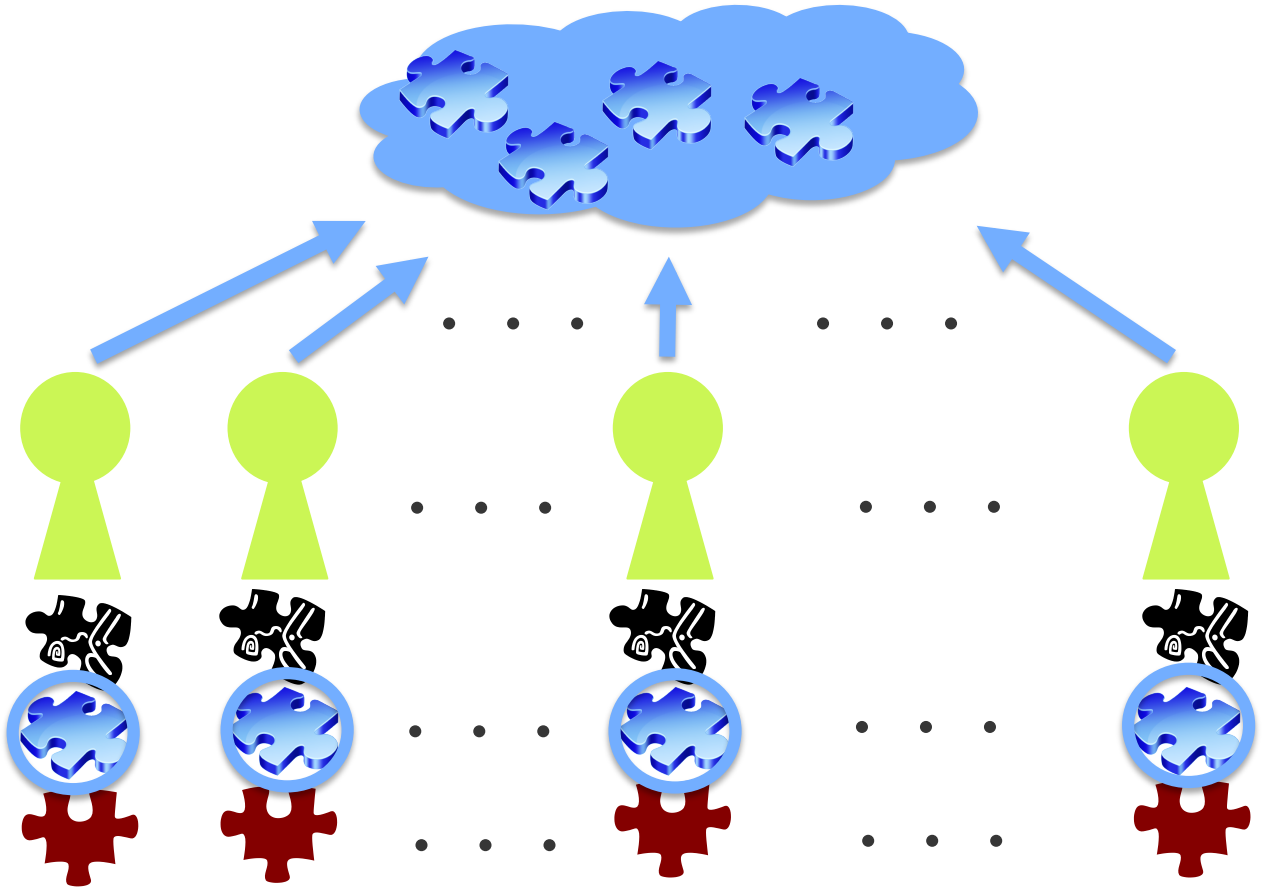
提案プロトコル（復元フェーズ）

Step 2. (n/2, n) SS S_2 のシェアを出す



提案プロトコル（復元フェーズ）

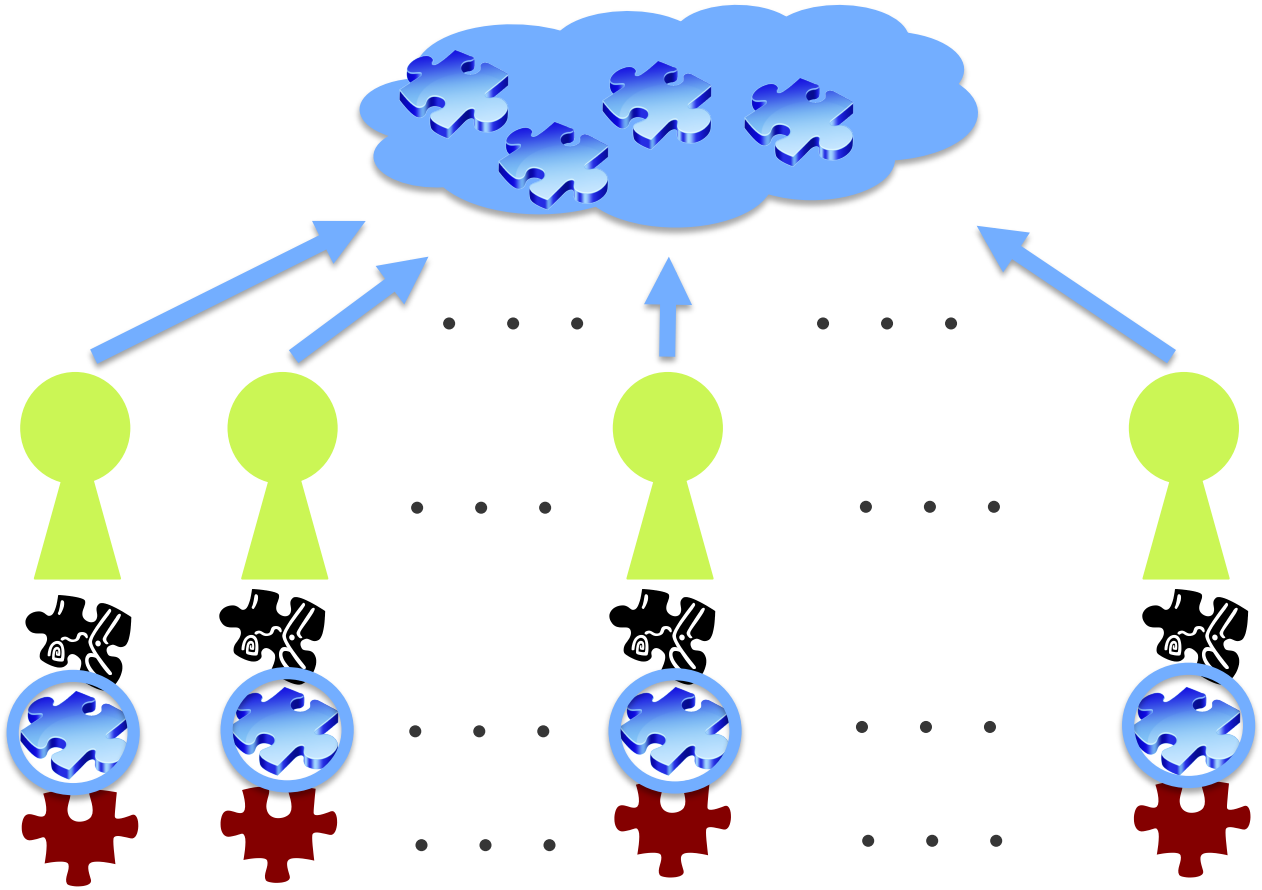
Step 2. (n/2, n) SS S_2 のシェアを出す



提案プロトコル（復元フェーズ）

Step 2. (n/2, n) SS S_2 のシェアを出す

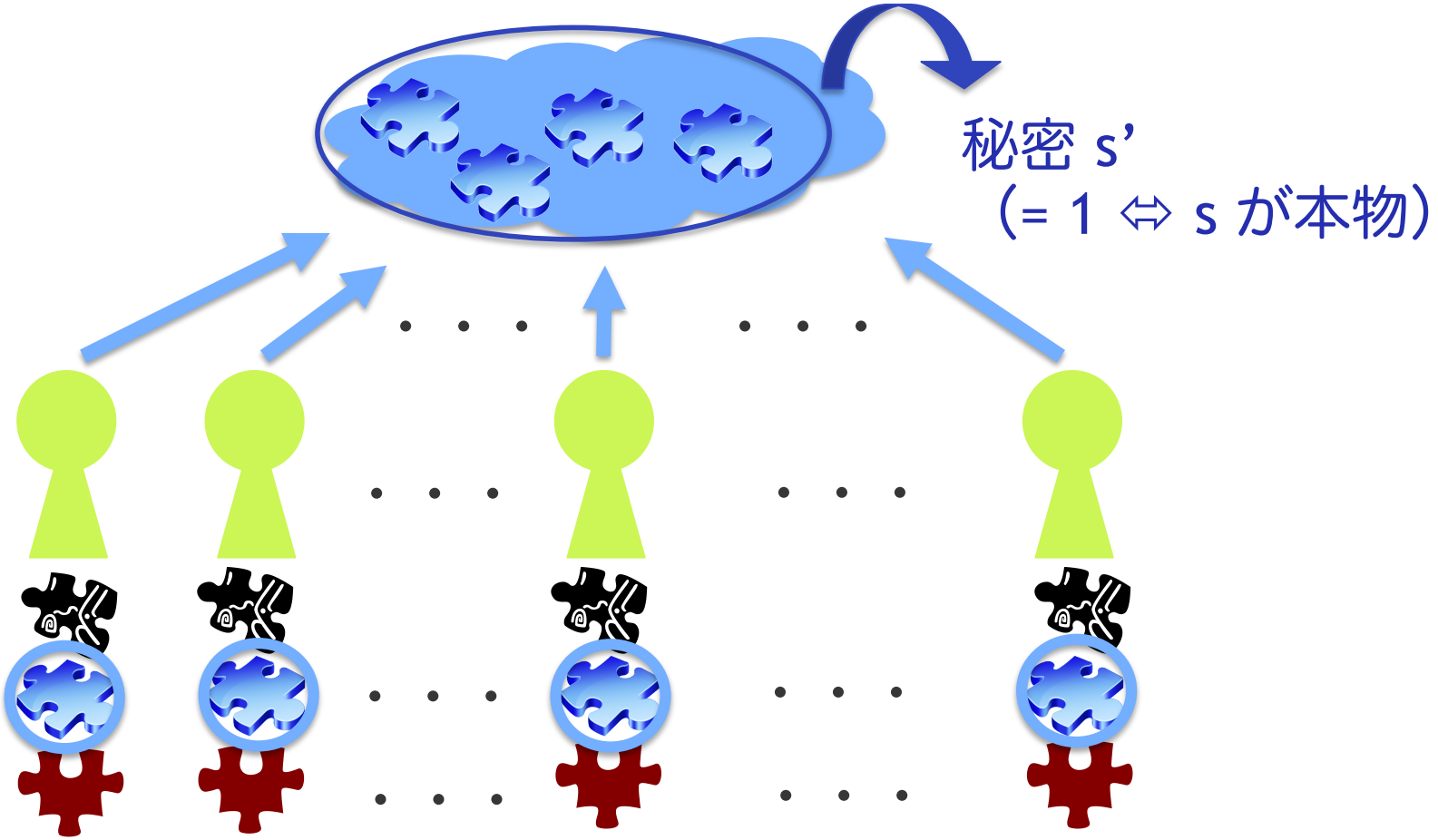
正しいシェアの数 ≥ n/2 → 秘密 s’ を復元



提案プロトコル（復元フェーズ）

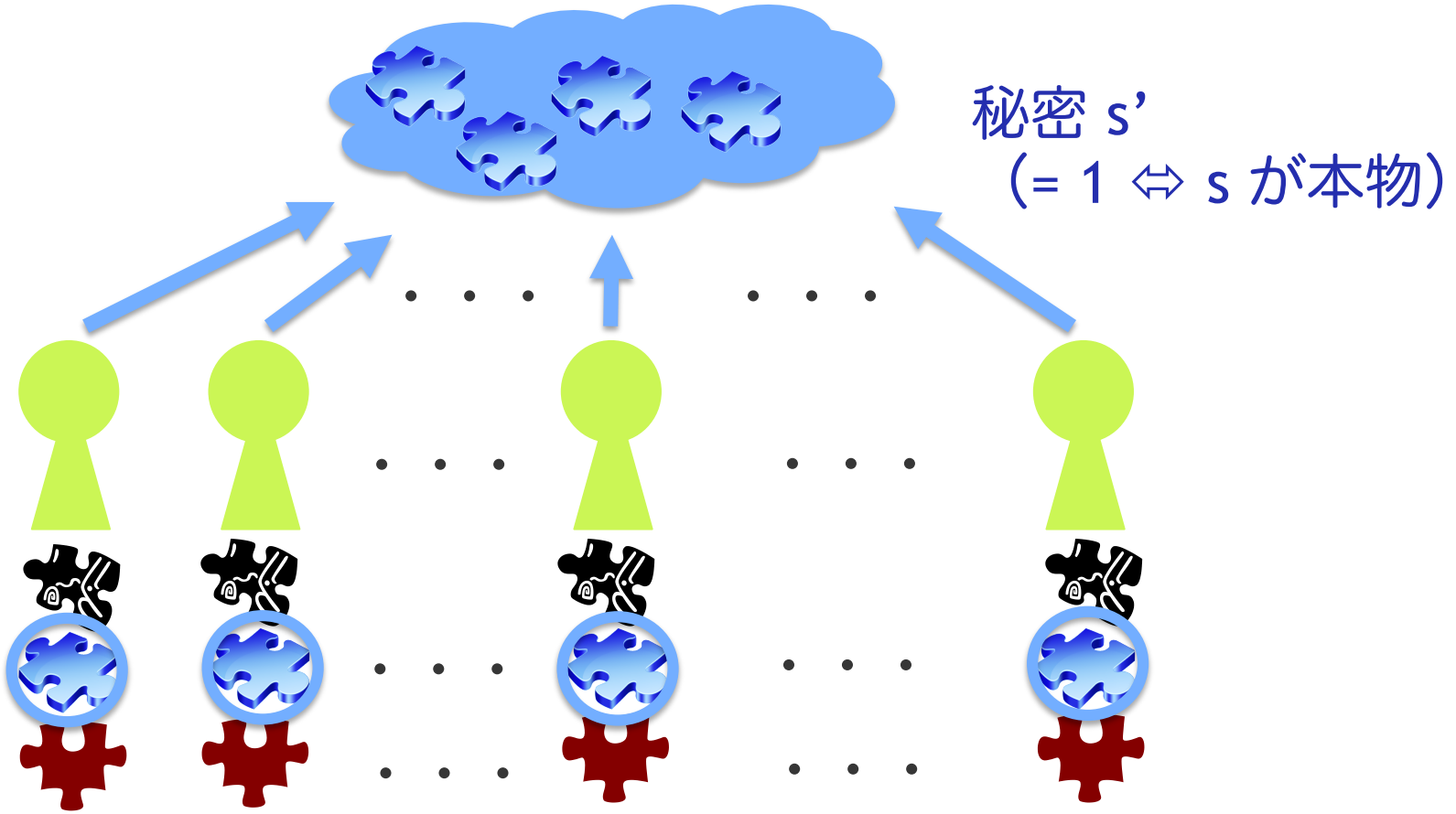
Step 2. (n/2, n) SS S_2 のシェアを出す

正しいシェアの数 ≥ n/2 → 秘密 s’ を復元



提案プロトコル（復元フェーズ）

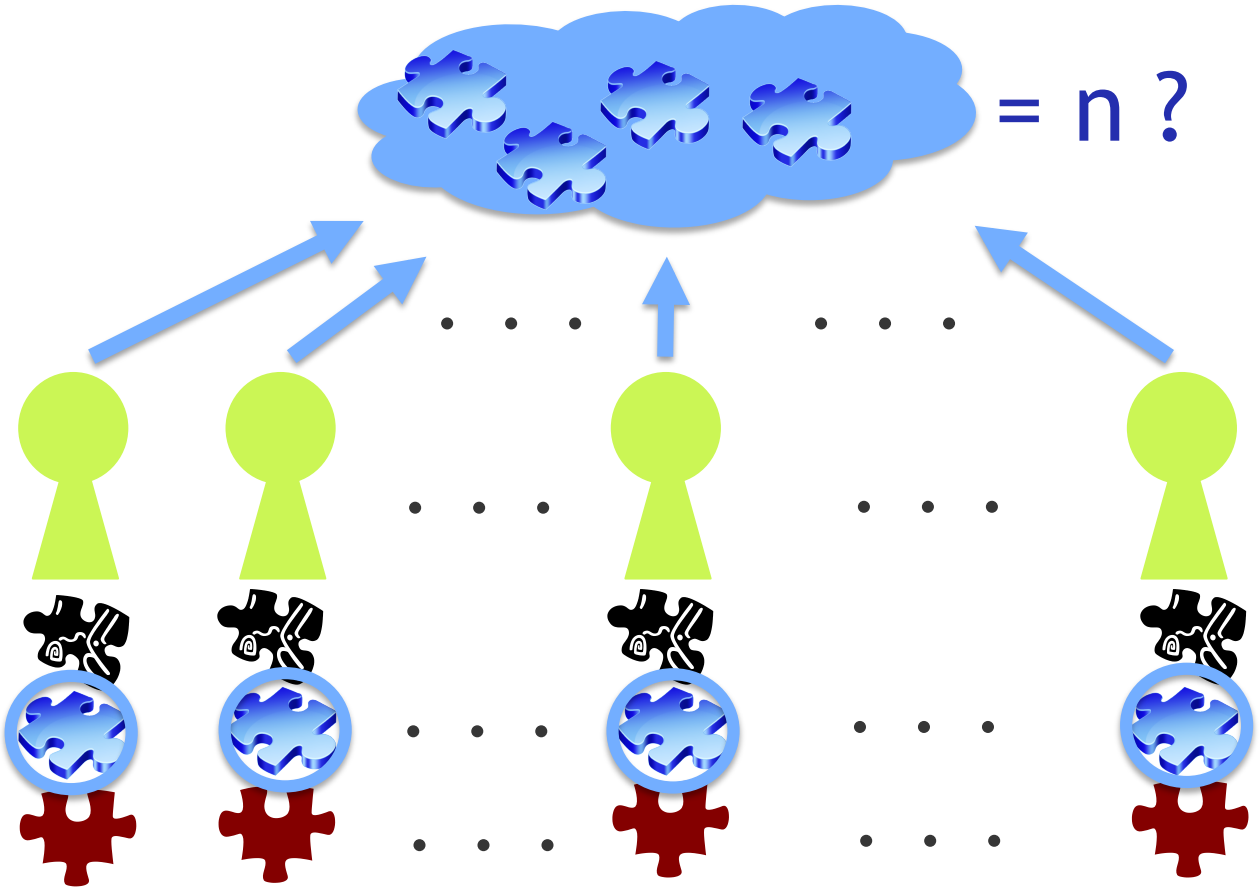
Step 2. (n/2, n) SS S_2 のシェアを出す



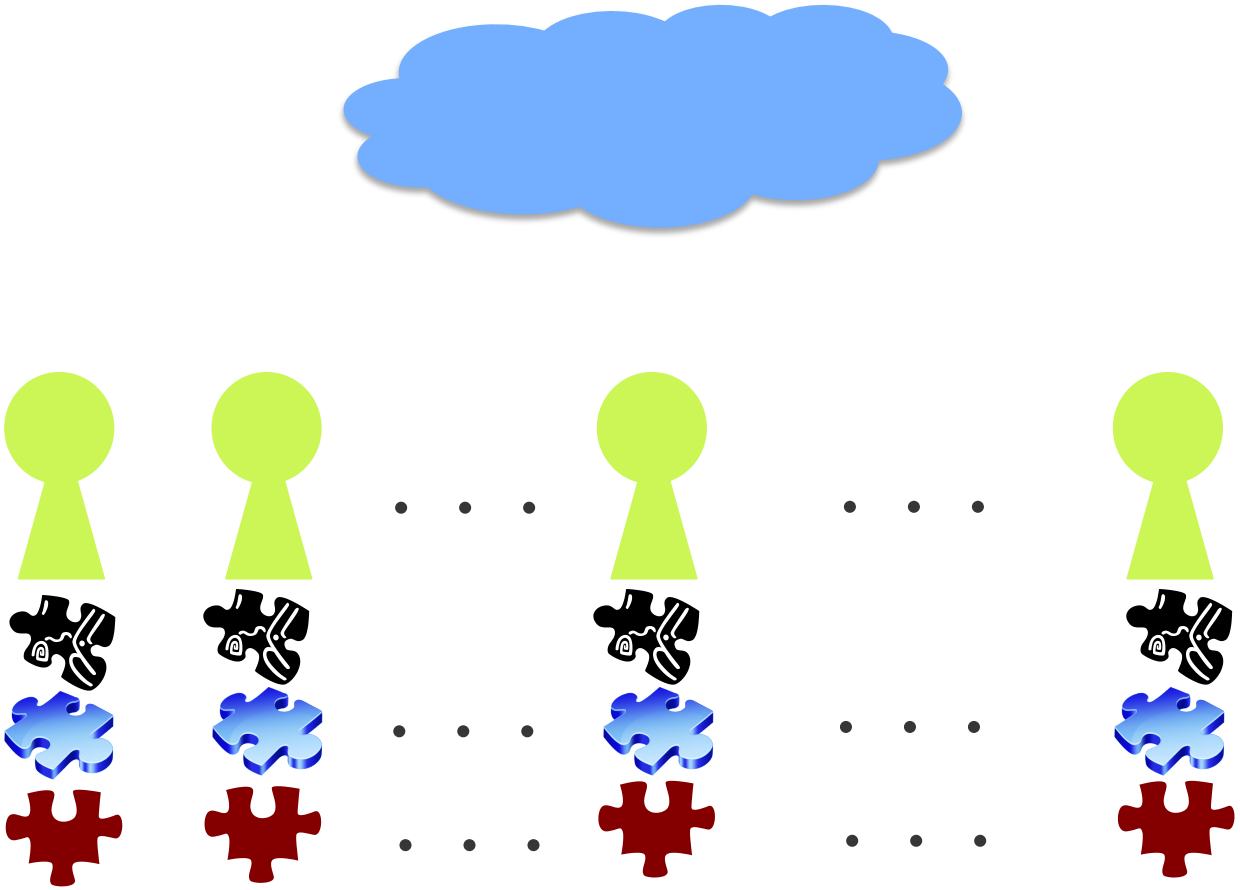
提案プロトコル（復元フェーズ）

Step 2. (n/2, n) SS S_2 のシェアを出す

正しいシェアの数 = n かつ s’ = 0 → 次のラウンドへ
それ以外 → 終了（s を出力）

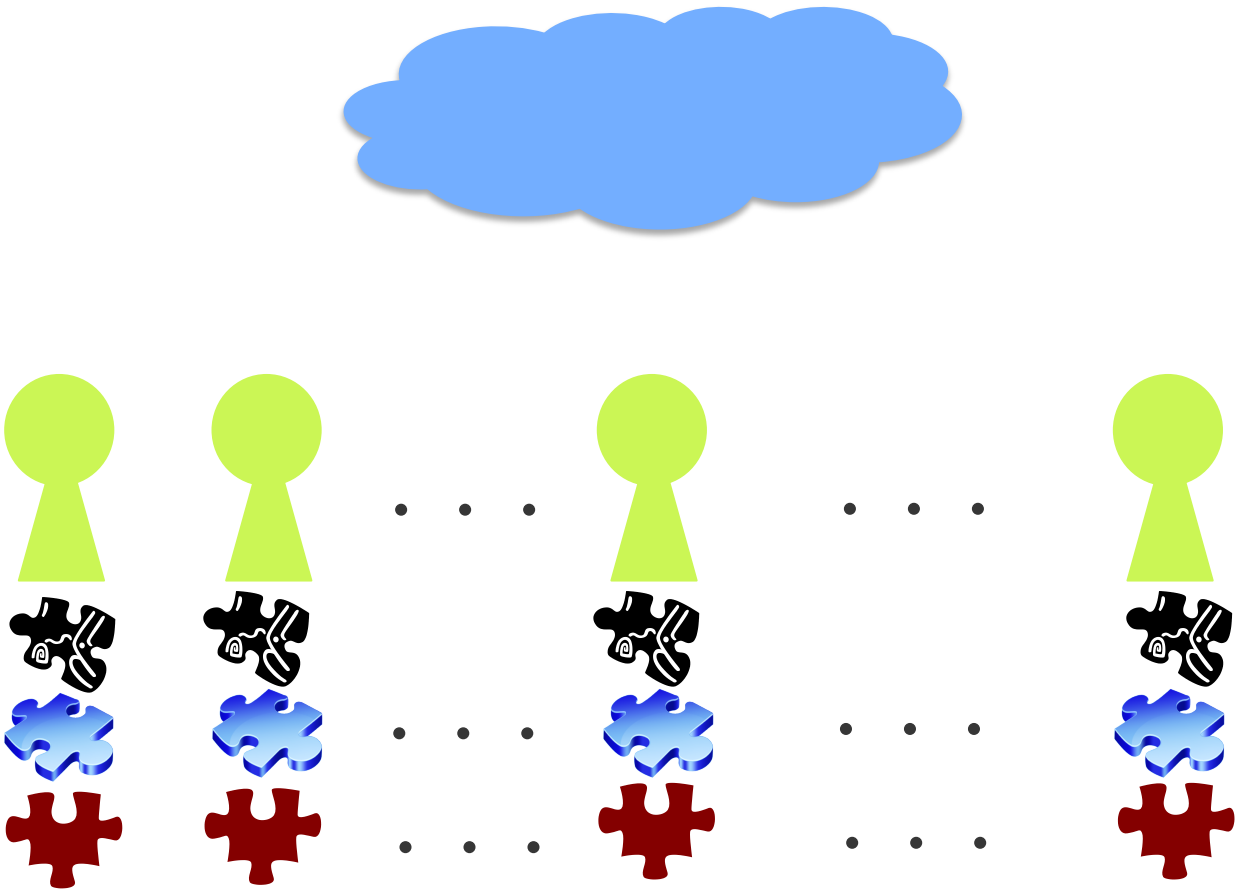


提案プロトコル（復元フェーズ）



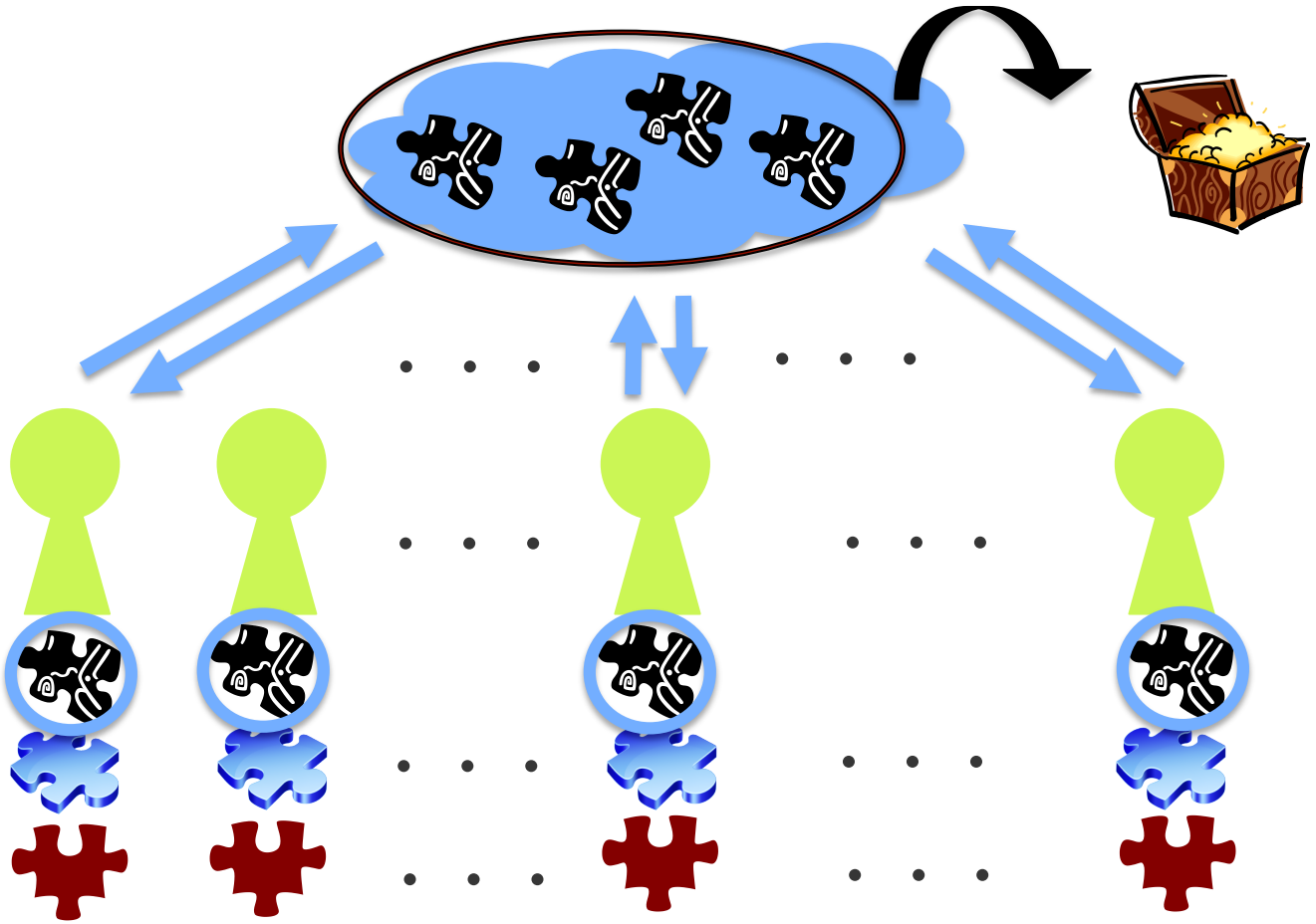
提案プロトコル（復元フェーズ）

Step 3. (n, n) RSS S_3 のシェアを使って秘密を復元
（RSS が正しく動作すれば秘密を復元）



提案プロトコル（復元フェーズ）

Step 3. (n, n) RSS S_3 のシェアを使って秘密を復元
（RSS が正しく動作すれば秘密を復元）



提案プロトコルの分析

- 連携耐性 n/2 – 1 の strict Nash 均衡
  - サイズ n/2 – 1 以下の連携 C
  - C 以外の n/2 + 1 人が従うと仮定し、
    C が従わないと利得が下がることを示す

- C のプレイヤーがプロトコルに従うとき
  → 全員が秘密を復元

提案プロトコルの分析

- Step 1
  - C 以外は従うので正しいシェアは n/2 + 1 以上
    → (n/2 + 1, n) SS なので必ず s は復元
    - ただし、確率 α で s は偽物
  - C のプレイヤーが「出さない」とき
    Step 2 に進まずプロトコル終了

    → 確率 α で偽物であるため、利得は下がる
    - この時点で、C は s が本物かどうかわからない
      - 本物と偽物は識別不能
      - s’ は (n/2, n) SS S_2 で秘密分散

提案プロトコルの分析

- Step 2
  - C のプレイヤーが「出さない」とき

    確率 α で s’ = 0（s は偽物）の場合、
    Step 3 に進まずプロトコル終了

    → 確率 α で利得は下がる
- Step 3
  - 連携耐性 (n/2 – 1) の strict Nash 均衡なので
    プロトコルに従わないとき、利得は下がる

提案プロトコルの性質

- RSS S_3 が連携耐性 $(n/2 - 1)$ の strict Nash 均衡のとき、提案プロトコルも連携耐性 $(n/2 - 1)$ の strict Nash 均衡
  - [FKN10] プロトコルを S_3 として利用可能
    - 連携耐性 $(n - 1)$ の strict Nash 均衡を達成
  - 復元に必要なラウンド数は、S_3 が T のとき、提案プロトコルは $2(1 - \alpha) + \alpha T$
    - α を十分小さくとれば、平均 2 以下
  - 定数ラウンドプロトコルにおいて、連携耐性 $(n/2 - 1)$ は（Nash 均衡であっても）最適（[AL09]）
  - 定数ラウンドで strict Nash 均衡達成は初めて
  - RSS S_3 は高い確率で実行しない → 持っているだけ！

今後の研究の方向性

- 連携耐性 n/2 – 1 の strict Nash 均衡では不十分？
  - 提案プロトコルの復元フェーズ Step 1 で、n/2 + 1 人目のプレイヤーはシェアを出すのか？
    - すでに n/2 個のシェアがあるので、自分で復元可能
    - もし n/2 + 1 人目以降がすべて出さないと、最初の n/2 人は秘密を復元できない！
      - 確率 α で偽物であるが、より少ない人数（n/2 人）で復元しているので、利得は上がる可能性
    - この考察は n/2 人がプロトコルから逸脱する状況
- 連携耐性 n/2 – 1 を超える方法の考案
  - 間違った秘密を出力したときの利得が非常に小さいとすれば回避可能（かも）

既存研究との比較

文献	通信路	その他の仮定	MPC	ラウンド数	解概念	連携耐性
[HT04]	同時同報	秘密通信路	✔	O(1/β)	IEWDS	
[ADGH06]	同時同報		✔	2	IEWDS	n/2 – 1
[GK06]	同時同報		✔	O(1/β)	IEWDS	n – 1
[KN08a]	同時同報	M/M Enc.	✔	O(1/β)	IEWDS	
[KN08b]	同時同報			O(1/β)	strict NE	1
[OPRV09]	同報	正直者		2	THPE	
[AL09]	同時同報	[GK06] 等		2	IEWDS	n/2 – 1
[FKN10]	P2P	VRF		O(1/β)	strict NE	n – 1
本研究	同報	既存の RSS		2	strict NE	n/2 – 1