ゲーム理論と暗号

安永憲司

金沢大学

暗号理論秋学校@河口湖セントビレッヂ 2014.9.9-12

お知らせ

- 数学セミナー 2014年10月号
  - 特集＝ゲーム理論の数理
    - ゲーム理論入門／「ゲーム理論」は数学か？——渡辺隆裕
    - ゲームによって予測不可能性を捉える——宮部賢志＋竹村彰通
    - 離散凸解析とゲーム理論——田村明久
    - 暗号とゲーム理論——安永憲司
    - 組合せゲーム理論——坂井 公
    - ギャンブルと確率論——藤田岳彦
    - [座談会]ゲーム理論で変わる社会——船木由喜彦＋坂井豊貴＋横尾真＋岡本吉央
- 経済セミナー 2014年10・11月号
  - 特集＝入門 ゲーム理論
    - 『数学セミナー』2014年10月号の特集「ゲーム理論の数理」と同時期にゲーム理論特集を組む。経セミでは、社会現象、人間行動分析への応用の視点から、具体例を挙げつつゲーム理論の取り組みを解説する。

ゲーム理論とは何か

- 複数の意思決定者が相互作用する状況（ゲーム的状況）を研究する理論
  - 自分の利益が他者の行動に依存する状況
  - 一人での意思決定は（あまり）考えない
  - 意思決定を行うとき、
    相手がどう行動するかを考えないといけない

ゲームの例（秋学校の争い）

- A 秋学校と K 秋学校は毎年9月第４週に開催
  - 過去２年は、A が 9/24-27、K が 9/24-26
- 両秋学校とも参加者を増やしたい
- 日程が重ならない場合、
  参加者の３割がもう１つの秋学校にも参加
- 第４週以外では、両秋学校とも第２週が候補
- 第２週の場合、調整のためのコストがかかる

➡ 今年はどのように開催されるだろうか？

ゲームの例（秋学校の争い）

- 利得
  - A の期待参加者数 → 30（3割は 9）
  - K の期待参加者数 → 40（3割は 12）
  - 第２週開催の調整コスト → - 10

(第4, 第4) = (30, 40),　　(第4, 第2) = (30+12, 40+9-10)
(第2, 第4) = (30+12-10, 40+9),　(第2, 第2) = (30-10, 40-10)

利得行列

A 秋学校 \ K 秋学校	第４週	第２週
第４週	(30, 40)	(42, 39)
第２週	(32, 49)	(20, 30)

ゲームの例（秋学校の争い）

A 秋学校 \ K 秋学校	第４週	第２週
第４週	(30, 40)	(42, 39)
第２週	(32, 49)	(20, 30)

- 行動分析
  - K 秋学校は、A 秋学校 の選択によらず、「第４週」の方が高利得
  - A 秋学校 は、K が「第４週」をすれば「第２週」の方が高利得

  → （A, K）＝（第２週、第４週）が選択される

ゲーム理論の用語

- プレイヤー：意思決定を行う主体
- 行動（戦略）：プレイヤーのとりうる選択肢
- 利得（効用）：ゲームの結果に対する好みを表す数値
  （大きいほうが望ましい）
- 利得関数（効用関数）：ゲームの結果を利得（効用）
  に対応させる関数
- ゲームの解：ゲームにおいて予想される結果

ゲームのバリエーション

- 戦略型ゲームと展開型ゲーム
  - 戦略型：各プレイヤーが同時に（１回だけ）行動を選択（標準型とも呼ばれる）
  - 展開型：それ以外
- 完備情報ゲームと不完備情報ゲーム
  - 完備情報：ゲームの情報（プレイヤー・利得・行動の候補）に不確実性がないもの
- 完全情報ゲームと不完全情報ゲーム
  - 完全情報：自分以前のプレイヤーの行動選択がわかるとき
- その他：繰り返しゲーム・協力ゲーム

戦略型ゲームの定式化

- 戦略型ゲーム $\Gamma = (N, \{S_i\}_{i \in N}, \{u_i\}_{i \in N})$
  - プレイヤー集合 $N = \{1, \ldots, n\}$
  - 戦略集合 S_i, $i \in N$
  - 利得関数 $u_i : S_1 \times \cdots \times S_n \rightarrow \mathbf{R}$, $i \in N$

- ゲーム理論でよく使われる記法
  - 戦略の組 $s = (s_1, \ldots, s_n)$ に対して、

$$s_{-i} := (s_1, \ldots, s_{i-1}, s_{i+1}, \ldots, s_n)$$

$$(s^*_i, s_{-i}) := (s_1, \ldots, s_{i-1}, s^*_i, s_{i+1}, \ldots, s_n)$$

解の見つけ方（その１）

- 支配戦略を探す
  - あるプレイヤーのある戦略が支配戦略
    ⇔ 他のプレイヤーがどの戦略をとろうとも、
    他のどの戦略よりもよい戦略

  - 戦略 s_i がプレイヤー i の支配戦略
    ⇔ $\forall s^*_i \in S_i \setminus \{s_i\}$, $\forall s^*_{-i} \in S_{-i}$,
    $u_i(s_i, s^*_{-i}) > u_i(s^*_i, s^*_{-i})$

ゲームの例（気の進まない共同研究）

- 大学教授のＡとＢは、個人で行う研究とは別に、（大学に言われて仕方なく）共同研究をスタート
- ２人とも協力的な場合、個別研究の進捗はやや遅れるが、共同研究は進む
- １人だけ協力的な場合、共同研究の進捗はほどほどだが、協力的でない教授の個別研究は進む
- ２人とも協力的でない場合、個別研究だけが進む

２人はどのように研究を進めるだろうか？

ゲームの例（気の進まない共同研究）

- 行動 = {協力, 非協力}
- 利得
  - 個別研究の進捗は、共同研究に協力的だと 30、非協力的だと 50
  - 共同研究の進捗は、ともに協力的だと 30、片方だけ協力的だと 15、ともに非協力的だと 5

教授 A \ 教授 B	協力	非協力
協力	(60, 60)	(45, 65)
非協力	(65, 45)	(55, 55)

ゲームの例（気の進まない共同研究）

A 教授 \ B 教授	協力	非協力
協力	(60, 60)	(45, 65)
非協力	(65, 45)	(55, 55)

- 行動分析
  - 教授 A にとっては「非協力」が支配戦略
  - 教授 B にとっても「非協力」が支配戦略

    → （非協力, 非協力）が選択される

協力したほうが良いと考え大学側が設計しても、
気の進まない共同研究は進まない

囚人のジレンマ

囚人１＼囚人２	黙秘	自白
黙秘	(5, 5)	(-4, 6)
自白	(6, -4)	(-3, -3)

- ２人の囚人にとっては、（黙秘, 黙秘）が望ましいが、（自白, 自白）を選択
  → 個人合理的な戦略
- ２人にとって（自白, 自白）より（黙秘, 黙秘）の方が望ましい
  → 集団合理的な戦略
- 集団合理性に関する概念 → パレート最適性
- 無限繰り返しゲームでは、（黙秘, 黙秘）を達成可能

解の見つけ方（その２）

- 最適反応戦略を考える
  - 最適反応戦略：他のプレイヤーの戦略に対し、自分の利得を最大化する戦略
  - 戦略 s_i が戦略の組 s_{-i} の最適反応
    $\Leftrightarrow \forall s^*_i \in S_i \setminus \{s_i\}, u_i(s_i, s_{-i}) \geq u_i(s^*_i, s_{-i})$

ゲームの例（卒業研究のテーマ決め）

- M 教授の研究室に、
  研究モチベーションの高い4年生 N 君が配属
- M 教授は、N 君に行って欲しい研究テーマがある
- N 君は、やりたい研究テーマがあり、M 教授のテーマをするくらいなら大学を辞めた方がましだと考えている
- お互いに主張を譲らないことも考えられるが、各テーマを半分ずつという妥協案も考えられる

N 君の今後はどうなるだろうか？

ゲームの例（卒業研究のテーマ決め）

- 行動 = {強硬, 妥協}
- 行動の結果
  - 一方が妥協すると、強硬した方のテーマ
  - 両者とも妥協すると、両テーマを半分ずつ
  - 両者とも強硬すると、N 君は大学を辞める

M ＼ N	強硬	妥協
強硬	N 君退学	M テーマ
妥協	N テーマ	半々

M ＼ N	強硬	妥協
強硬	(0, 10)	(30, 0)
妥協	(10, 100)	(20, 50)

ゲームの例（卒業研究のテーマ決め）

M ＼ N	強硬	妥協
強硬	N 君退学	M テーマ
妥協	N テーマ	半々

M ＼ N	強硬	妥協
強硬	(0, 10)	(30, 0)
妥協	(10, 100)	(20, 50)

- N 君にとっては「強硬」が支配戦略
- N 君の「強硬」に対し、M 教授の「妥協」が最適反応

  → N 君のテーマが採用される

学生という弱い立場であっても、
「強硬」が支配戦略であることを相手に知らせば
自分のやりたい研究ができる

Nash 均衡

- 戦略の組 $s = (s_1, \ldots, s_n)$ が Nash 均衡

  $\Leftrightarrow$ すべてのプレイヤーにとって、
  最適反応戦略であるとき

  $\Leftrightarrow \forall\, i, \forall\, s^*_i \in S_i \setminus \{s_i\},\ u_i(s_i, s_{-i}) \geq u_i(s^*_i, s_{-i})$

戦略型ゲームの解は Nash 均衡であるべき
（ただし、十分であるとは考えられていない）

戦略の弱支配関係

- 戦略 s_i が戦略 s^*_i を弱支配

  ⇔　他のプレイヤーの戦略に関わらず、
  s_i が s^*_i より悪くなることはなく、かつ
  他のプレイヤーのある戦略において、
  s_i が s^*_i より真によい

  ⇔ (1) $\forall\, s_{-i} \in S_{-i},\ u_i(s_i, s_{-i}) \geq u_i(s^*_i, s_{-i})$
  (2) $\exists\, s_{-i} \in S_{-i},\ u_i(s_i, s_{-i}) > u_i(s^*_i, s_{-i})$

合理的なプレイヤーは
弱支配される戦略を選択しないと考えられる

Nash 均衡に関する事実

- Nash 均衡は複数存在することがある
- Nash 均衡は弱支配されることがある

→ 弱支配されない Nash 均衡が解であるべき

1 \ 2	x	y
a	(2, 10)	(3, 0)
b	(1, 0)	(3, 10)

- (a, x) と (b, y) が Nash 均衡
- しかし、戦略 b は戦略 a に弱支配
  → (b, y) は解ではないと考えられる

Nash 均衡に関する事実（続き）

- 純粋戦略 Nash 均衡は存在するとは限らない
  - 純粋戦略：行動が確定的
  - 混合戦略：行動が確率的

例．マッチングペニー

1 \ 2	表	裏
表	(1, -1)	(-1, 1)
裏	(-1, 1)	(1, -1)

- 任意の有限戦略型ゲームにおいて、
  混合戦略を含めれば Nash 均衡は存在

展開型ゲーム

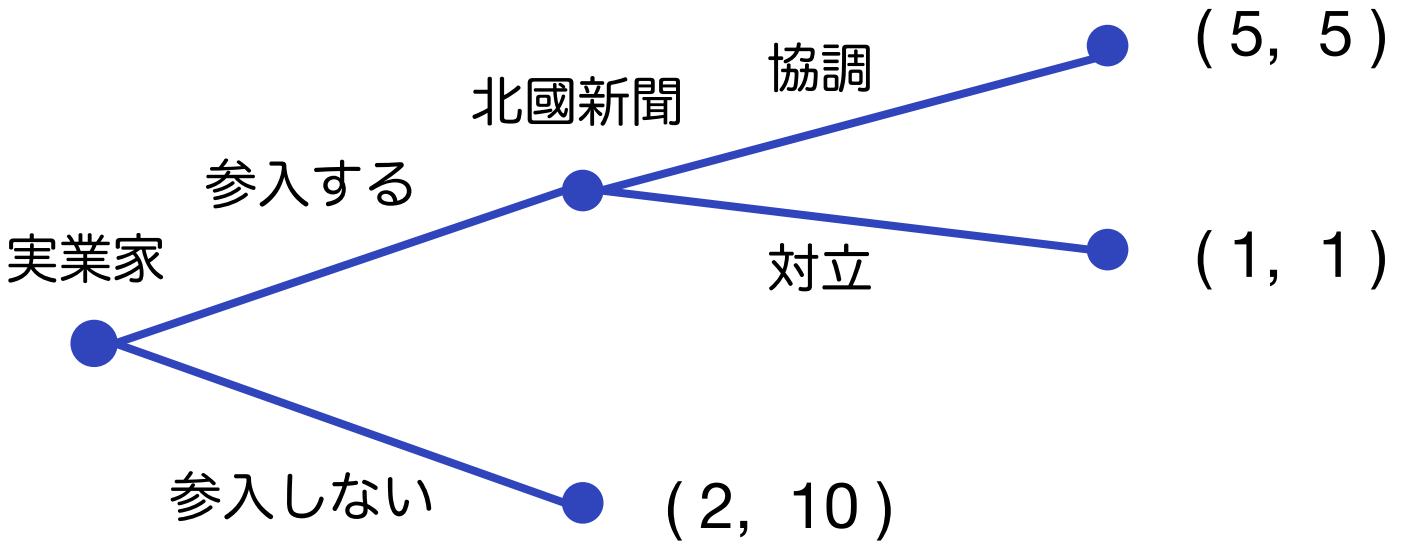
- すべてのプレイヤーが同時に行動するとは限らないゲーム
  - ゲームは逐次的に行われる
- プレイヤーの戦略は、履歴を行動に対応させる関数
  - 戦略型では、一度決めるだけ
- 利得関数は、終着履歴（ゲームの結果）から数値への関数
  - 戦略型でも、ゲームの結果から数値への関数

ゲームの例（おくやみ情報業界への参入）

- 北國新聞は、石川県内シェア７割を誇る地方新聞
  - 特に記事が優れているわけではない（らしい）
  - おくやみ欄が充実しているため、必要に迫られて購読している（らしい）
- ある実業家は、金沢市内のおくやみ情報をウェブで安価に提供する事業への参入を検討中
- 参入しなければ、お互い現状維持
- 参入した場合、北國新聞がその事業者と「協調」すれば利益を分けあえるが、「対立」した場合、おくやみ情報価格（北國新聞の場合は購読料）の値下げ競争が行われ、両者とも利益がなくなる

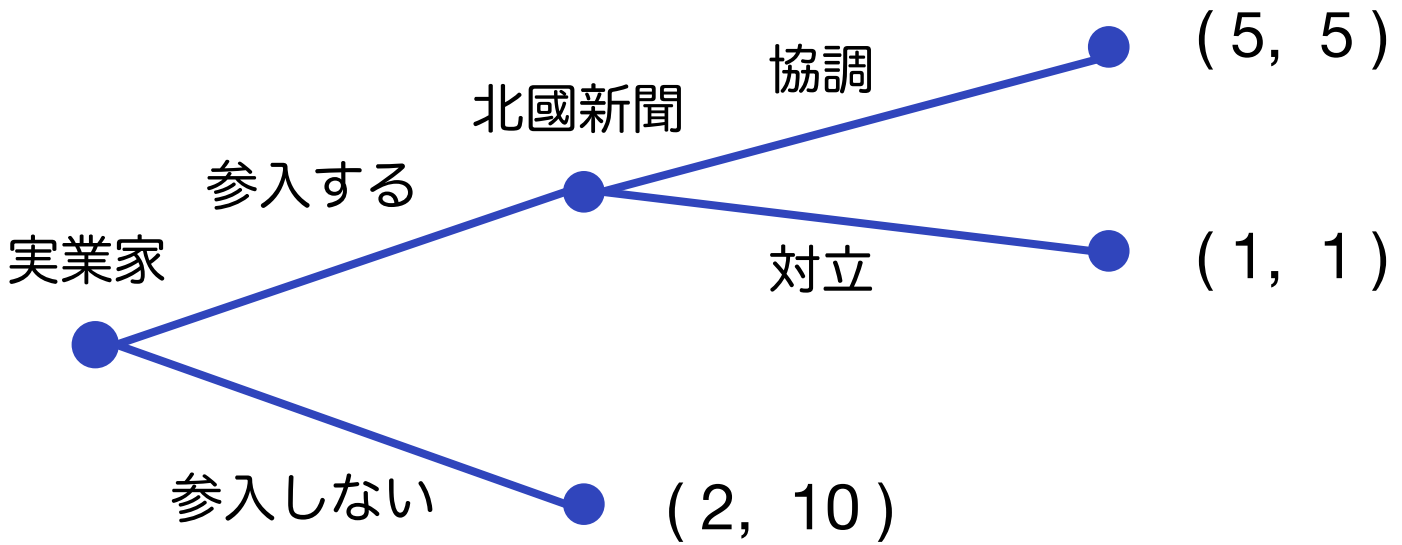
ゲームの例（おくやみ情報業界への参入）

- ゲームは木で表現



ゲームの解は何か？

展開型ゲームでの解の見つけ方



- 先読みをする
  - 「参入する」場合、北國新聞は「協調」
  - 「参入する」→「協調」であるため、実業家は「参入する」

ただし、完全情報ゲームでないと求められない

戦略型ゲームとしての展開型ゲーム

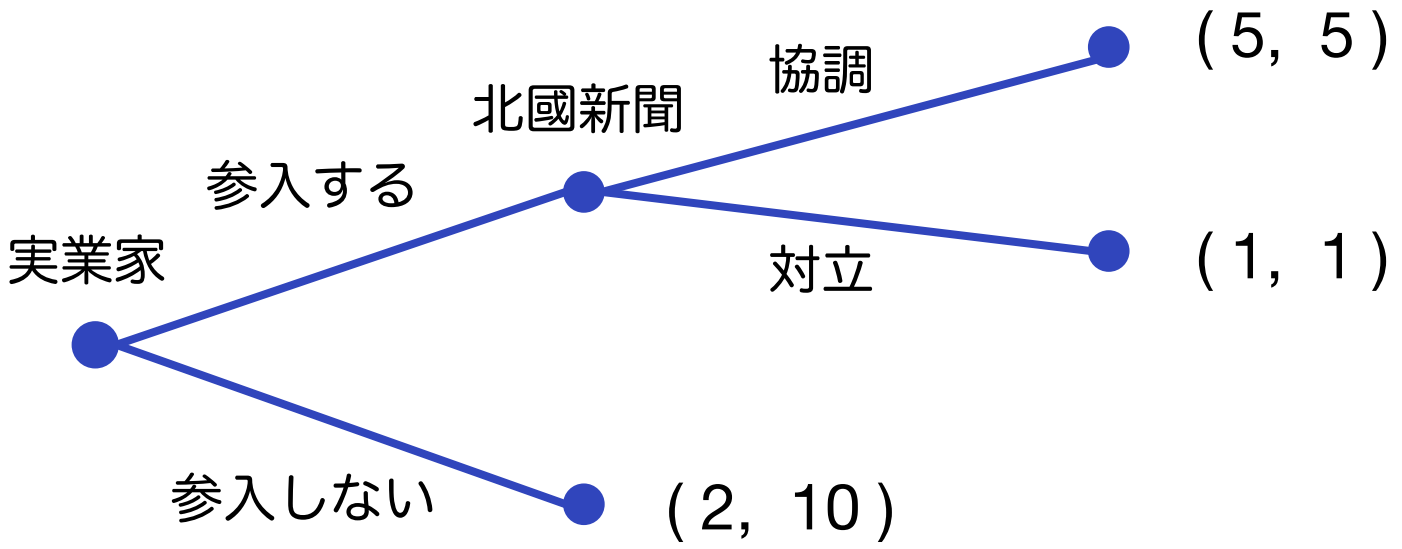
- 戦略型ゲームとしても表現可能

実業家 \ 北國新聞	協調	対立
参入する	(5, 5)	(1, 1)
参入しない	(2, 10)	(2, 10)

- ゲームの解として、Nash 均衡も同様に使える！

→ しかし、このゲームには２つの Nash 均衡

展開型ゲームにおける Nash 均衡の問題点



- （参入する, 協調）は Nash 均衡
- （参入しない, 対立）も Nash 均衡
- しかし、実業家が「参入する」を選んだとき、北國新聞が「対立」を選ぶとは考えにくい

→ 信憑性のない脅し

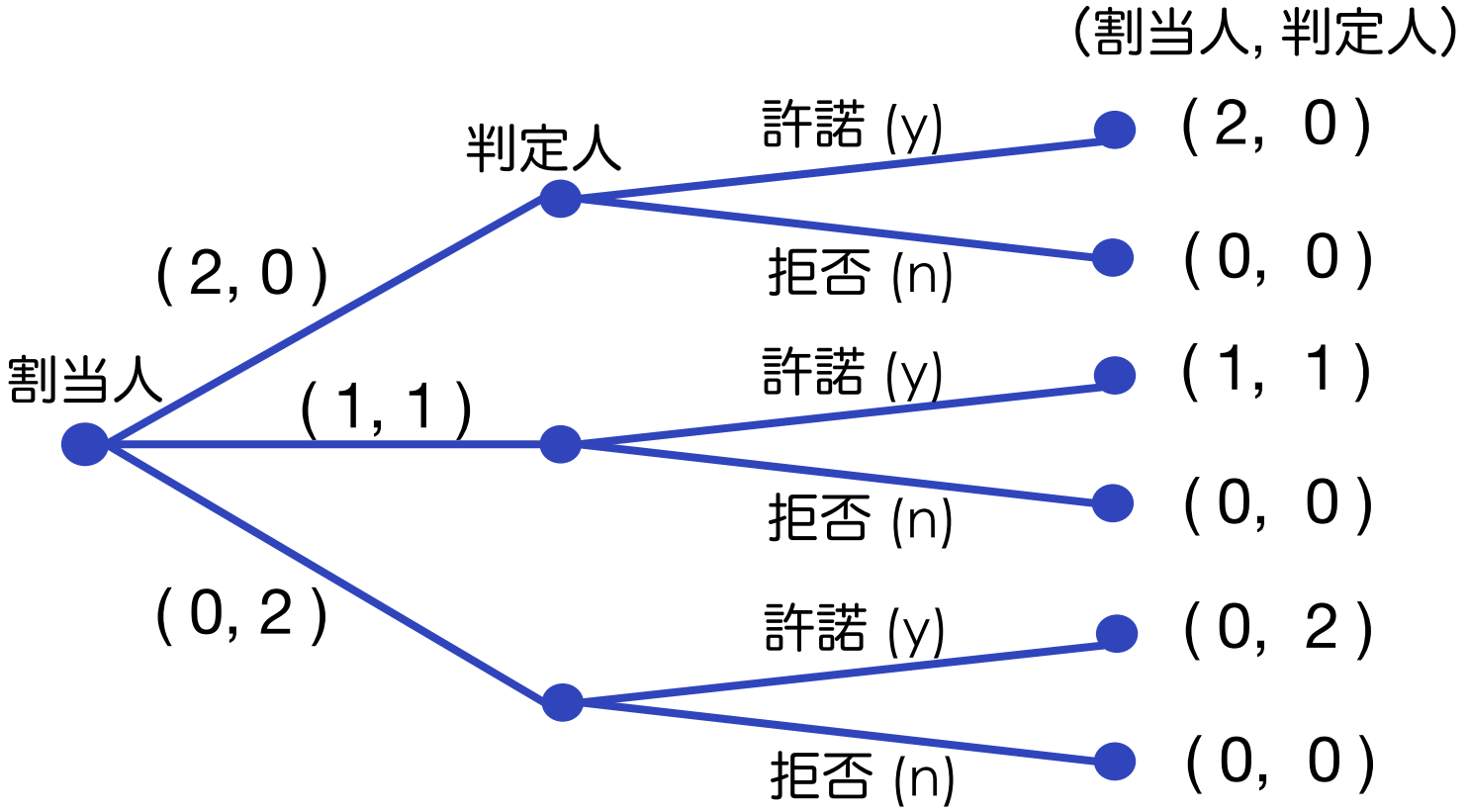
なぜ信憑性のない脅しが生じるのか？

- Nash 均衡は、最適反応戦略の組であり、
  自分以外の戦略は変わらないことを前提に議論
  - しかし、展開型ゲームでは、自分の行動が
    変われば、相手の行動が変わるのが自然
  - そして、Nash 均衡では実現パス以外のパスに
    おける均衡を考えない

  → 部分ゲーム完全均衡でこの問題を解決

- 戦略の組が部分ゲーム完全均衡
  ⇔ その戦略が、すべての「部分ゲーム」において
  Nash 均衡であるとき

ゲームの例（割り当てゲーム）



- Nash 均衡は、((2,0),yyy), ((2,0), yyn), ((2,0), yny), ((1,1), nyy), ((1,1), nyn), ((0,2), nny), (2,0), nny), ((2,0), nnn)
- 部分ゲーム完全均衡は、((2,0), yyy), ((1,1), nyy)

不完備・不完全ゲームとハルサニ変換

- 完備情報ゲームと不完備情報ゲーム
  - 完備情報：ゲームの情報（プレイヤー・利得・行動の候補）に不確実性がないもの
  - 不完備の例：オークション（他者の利得が不明）
- 完全情報ゲームと不完全情報ゲーム
  - 完全情報：自分以前のプレイヤーの行動選択がわかるとき
- ハルサニ変換
  - 「不完備情報ゲーム → 不完全情報ゲーム」への変換
  - ゲームの最初に、（不完全情報の）偶然手番を追加

ベイジアンゲーム（戦略型不完備情報ゲーム）

- 自然 (nature) が状態 $\omega \in \Omega$ を確率的に選択
- 各プレイヤー i は、タイプ $\tau_i(\omega) \in T_i$ を受け取る
  - τ_i : シグナル関数、T_i : タイプ集合
  - 各 i は、$\{\tau_j\}_{j \in N}$ および ω の事前確率を知っている
  - 他のプレイヤーのタイプ $\{\tau_i(\omega)\}_{i \in N \setminus \{i\}}$ に対する事後確率（信念）をベイズルールにより更新
- 各プレイヤーは、戦略・利得関数・自然状態を考慮した上で、行動を選択する

ゲーム開始時にプレイヤー毎に与えられる個別情報は、「タイプ」と呼ばれている

相関均衡

例．男女の争い (battle of the sexes, Bach or Stravinsky)

1 \ 2	Bach	Stravinsky
Bach	(2, 1)	(0, 0)
Stravinsky	(0, 0)	(1, 2)

- Nash 均衡は、純粋戦略 (B, B), (S, S) と
  混合戦略 ((2/3, 1/3), (1/3, 2/3)) であり、
  それぞれの期待利得は、(2,1), (1,2), (2/3, 2/3)
- 公開されたコイン投げ（暗号理論ではCRS）を使い、
  表なら (B,B), 裏なら (S, S) に従うことにすれば、
  期待利得は (3/2, 3/2)
- このようにして達成可能な均衡を相関均衡と呼ぶ
  - 「おすすめ戦略」をタイプとして知らせている

これまでのまとめ

- ゲーム的状況 = 複数の意思決定者が相互作用する状況
- 戦略型ゲーム
  - すべてのプレイヤーが同時に行動
  - 解の見つけ方

    1. 支配戦略を見つける 2. 最適反応戦略を考える
  - Nash 均衡の問題点: 弱支配される可能性
- 展開型ゲーム
  - プレイヤーの行動が逐次的
  - 解の見つけ方 → 先読みをする（完全情報ゲーム）
  - Nash 均衡の問題点: 信憑性のない脅しの可能性
    → 部分ゲーム完全均衡
- 不完備情報ゲーム・相関均衡

以降の内容

- 暗号理論におけるゲーム理論
  - 既存研究・暗号理論へ応用する際の難しさ
  - 暗号プロトコルの安全性と Nash 均衡
  - 秘密分散とゲーム理論

暗号理論におけるゲーム理論

暗号理論 vs ゲーム理論

- ともにプレイヤー間の相互作用に関する研究

- 暗号理論
  - プレイヤーは正直者 or 悪者
  - 正直者をどのように守るか？

- ゲーム理論
  - プレイヤーは合理的
  - 合理的なプレイヤーはどう振る舞うか？

暗号理論とゲーム理論に関する研究

- 暗号理論をゲーム理論に利用
  - 信頼できる仲介者（相関均衡）を暗号技術で実現 [DHR00, ADGH06, LMPS04, ILM05, IML05, ASV08, ADH08, ILM08, AKL+09, ILM11, AKMZ12, CV12]
- ゲーム理論を暗号理論へ適用
  - 合理的なプレイヤーが暗号プロトコルを実行 [HT04, ADGH06, LT06, GK06, KN08a, KN08b, MS09, OPRV09, AL09, Gra10, FKN10, PS11, GKTZ12, Y12]
- ゲーム理論と暗号理論の概念間の関係
  - 暗号理論向けのゲーム理論の概念 [HP10, GLV10, PS11]
  - ゲーム理論の概念によって安全性を特徴付け [ACH11, GK12, HTYY12, HTY13]

ゲーム理論を応用する際の難しさ

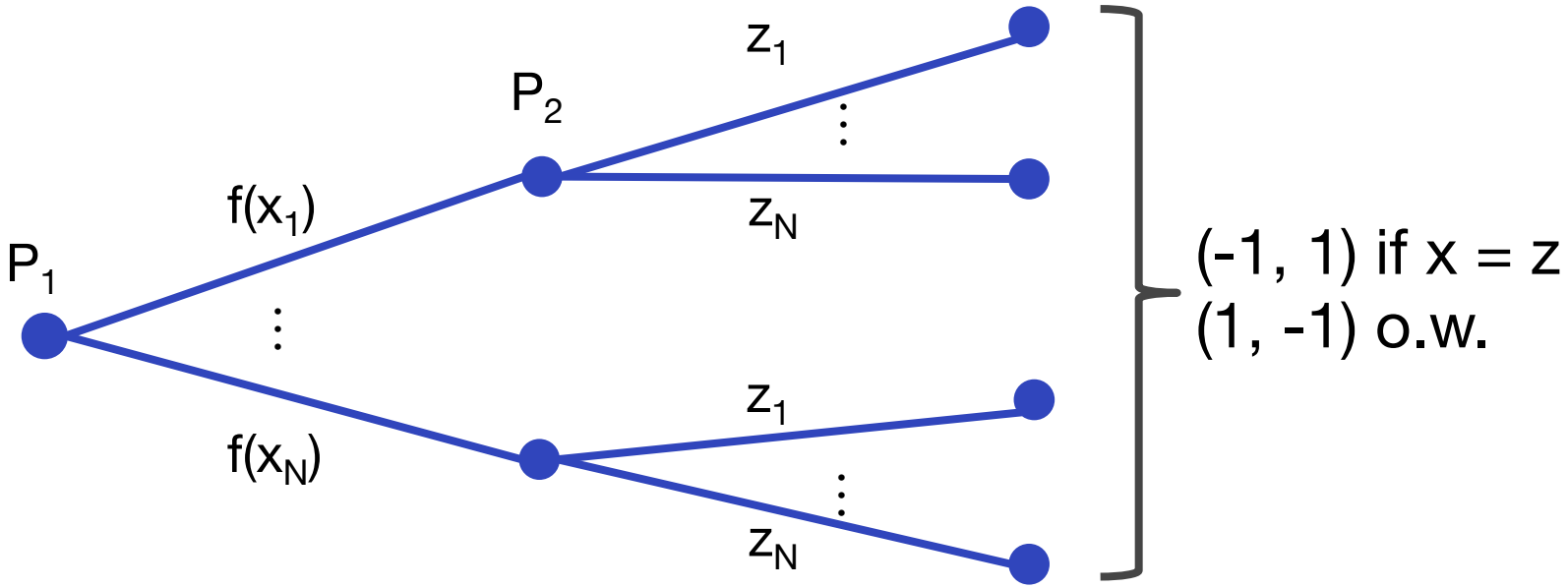
- 一方向性置換ゲーム（零和ゲーム）

  1. P_1 が $x \in_R \{0,1\}^n$ を選び $f(x)$ を P_2 に送る
  2. P_2 が $z \in \{0,1\}^n$ を P_1 に送る
  3. P_2 は $z = x$ のときに利得 1, それ以外で -1

  - 通常のゲーム理論では、P_2 が常に勝つ
  - 直観的には、両者ランダムに選択することが Nash 均衡になるべき

→ 計算量的 Nash 均衡

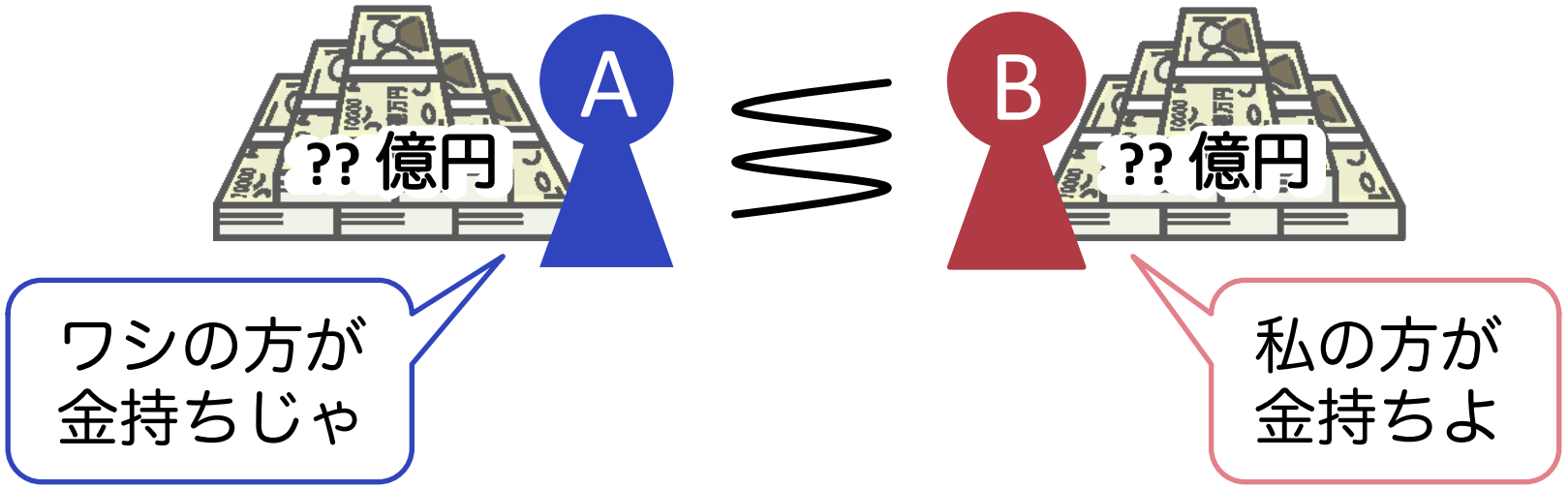
ゲーム理論を応用する際の難しさ



- 部分ゲーム完全均衡は？
  - P_2 が f(x) を受け取ったという条件下での部分ゲームを考えると、f(z) = f(x) なる z を選ぶのが最適な戦略
    - 与えられた１つの戦略（マシン）では、部分ゲームにおいて異なる複数のマシンすべてには勝てない

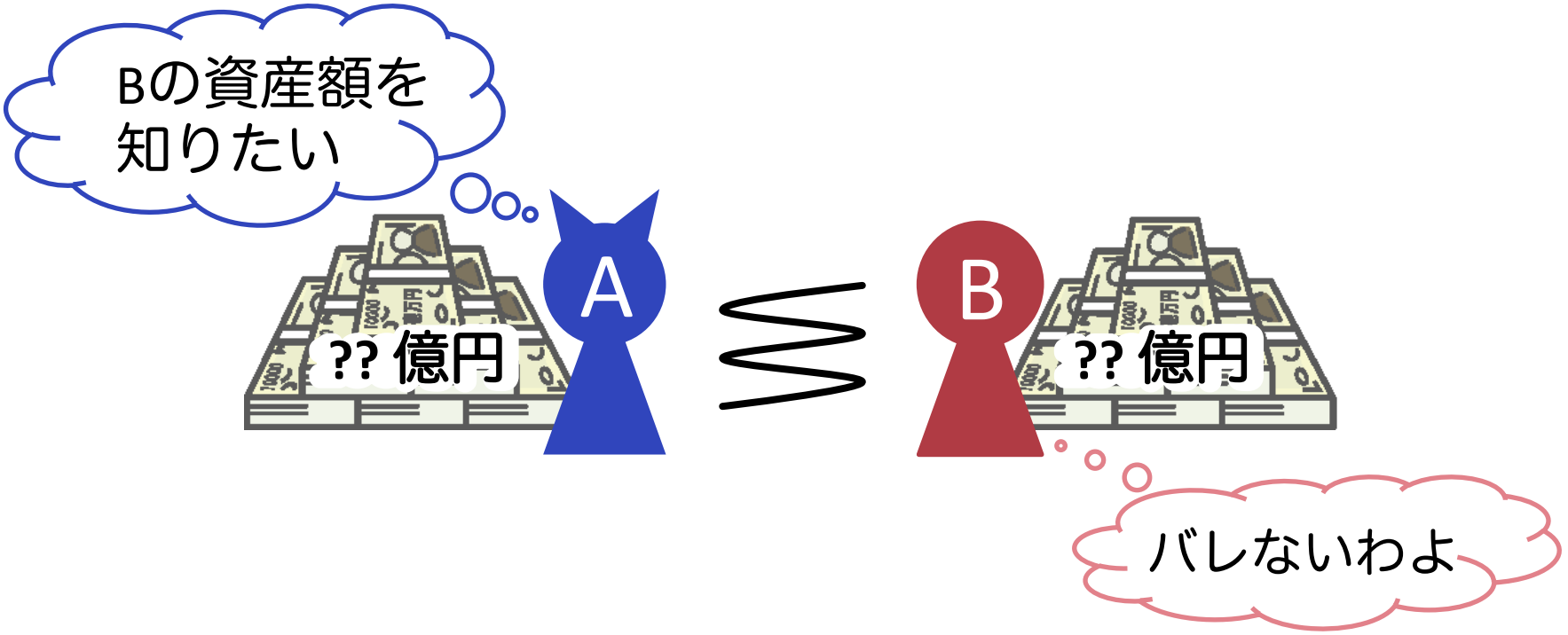
暗号プロトコルの安全性と Nash 均衡

億万長者ゲーム



- どちらが金持ちか知りたい
- 自分の資産額は知られたくない

暗号理論的な安全性



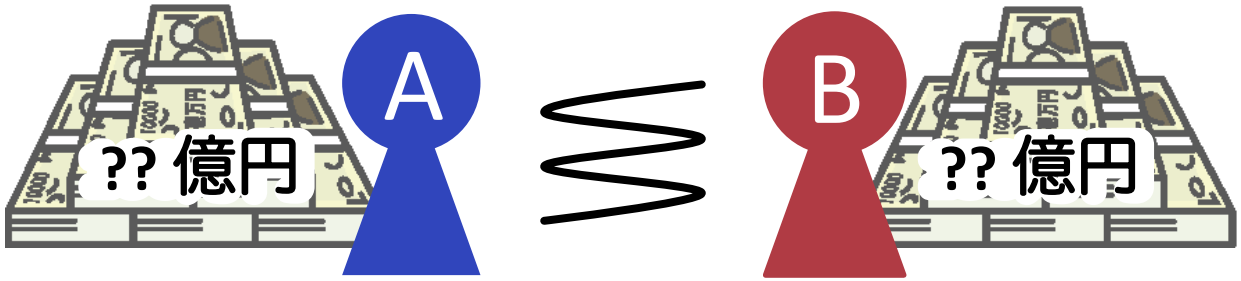
どんな攻撃者も相手の資産額を
知ることが出来ない

暗号理論的な安全性

- A と B がプロトコルに従えば、どちらが金持ちであるかを両者知ることができる（正当性）
- A がプロトコルに従う限り、B がどのようにプロトコルから逸脱したとしても、B は A の資産額に関する情報を得られない（A の安全性）
- B がプロトコルに従う限りA がどのようにプロトコルから逸脱したとしても、A は B の資産額に関する情報を得られない（B の安全性）

「ゲーム理論的な」安全性を考えてみる

「暗号プロトコルの実行 = ゲームの実行」と考える



利得

- どちらが金持ちか知りたい
- 自分の資産額は知られたくない
- 相手の資産額を知りたい　　など

プロトコルに従うという戦略がゲームの解
（プロトコルに従うことが合理的）

ゲーム理論的な安全性

- プロトコル (π_A, π_B) を実行したときの
  A の利得関数 $u_A(\pi_A, \pi_B)$ のとる値を以下のように定義
  - どちらが金持ちか知ることが出来た → 1
  - 相手の資産額を知ることが出来た → 2
- B の利得関数 u_B も同様に定義
- 暗号理論的な安全性は以下のように書き直せる
  - $\forall \pi^*_B \in S_B, u_B(\pi_A, \pi^*_B) \leq u_B(\pi_A, \pi_B)$（A の安全性）
  - $\forall \pi^*_A \in S_A, u_A(\pi^*_A, \pi_B) \leq u_A(\pi_A, \pi_B)$（B の安全性）

戦略組 (π_A, π_B) が Nash 均衡であることの定義に一致！

より一般的に

- 暗号理論的な安全性
  - 正直者がプロトコルに従う限り、
    他のプレイヤーがどのように振る舞っても
    正直者の安全性は保たれる
- Nash 均衡によるゲーム理論的な安全性
  - プロトコルからどのように逸脱しても、
    自分の利得を上げることは出来ない

「自分が高利得 ⇔ 相手の安全性を破る」
ならば、両者は一致

暗号理論的な安全性の限界 (1/2)

- 暗号理論的な安全性
  ＝ ゲーム理論的な安全性の特殊な場合

→ 暗号理論的な安全性が捉えてない部分が明らかに

1. 「自分が低利得 ⇔ 自分の安全性が破られる」という利得は考えていない
   - 自分の安全性を保てる範囲内で、相手の安全性を破るために逸脱するプレイヤーは想定外
   - 暗号理論の安全性は、自分の安全性が最大限に脅かされる状況を考えている

暗号理論的な安全性の限界 (2/2)

2. すべてのプレイヤーがプロトコルから逸脱する状況は考えてない
   - 暗号理論では、一方は必ず正直者
   - 部分ゲーム完全均衡のような保証はない

3. 複数の性質（安全性）を同時には考えていない
   - 複数の性質間のトレードオフを考慮するプレイヤーは想定外
   - ただし、性質を１つずつ考えことは、より高い安全性を考えることになる

まとめ（暗号プロトコルの安全性と Nash 均衡）

- ゲーム理論的な安全性
  - 「プロトコルの実行 = ゲームの実行」
  - プロトコルに従うという戦略がゲームの解

- Nash 均衡によるゲーム理論的な安全性は、暗号理論的な安全性と等価
- より強い均衡概念を考えると、より強い安全性が得られる

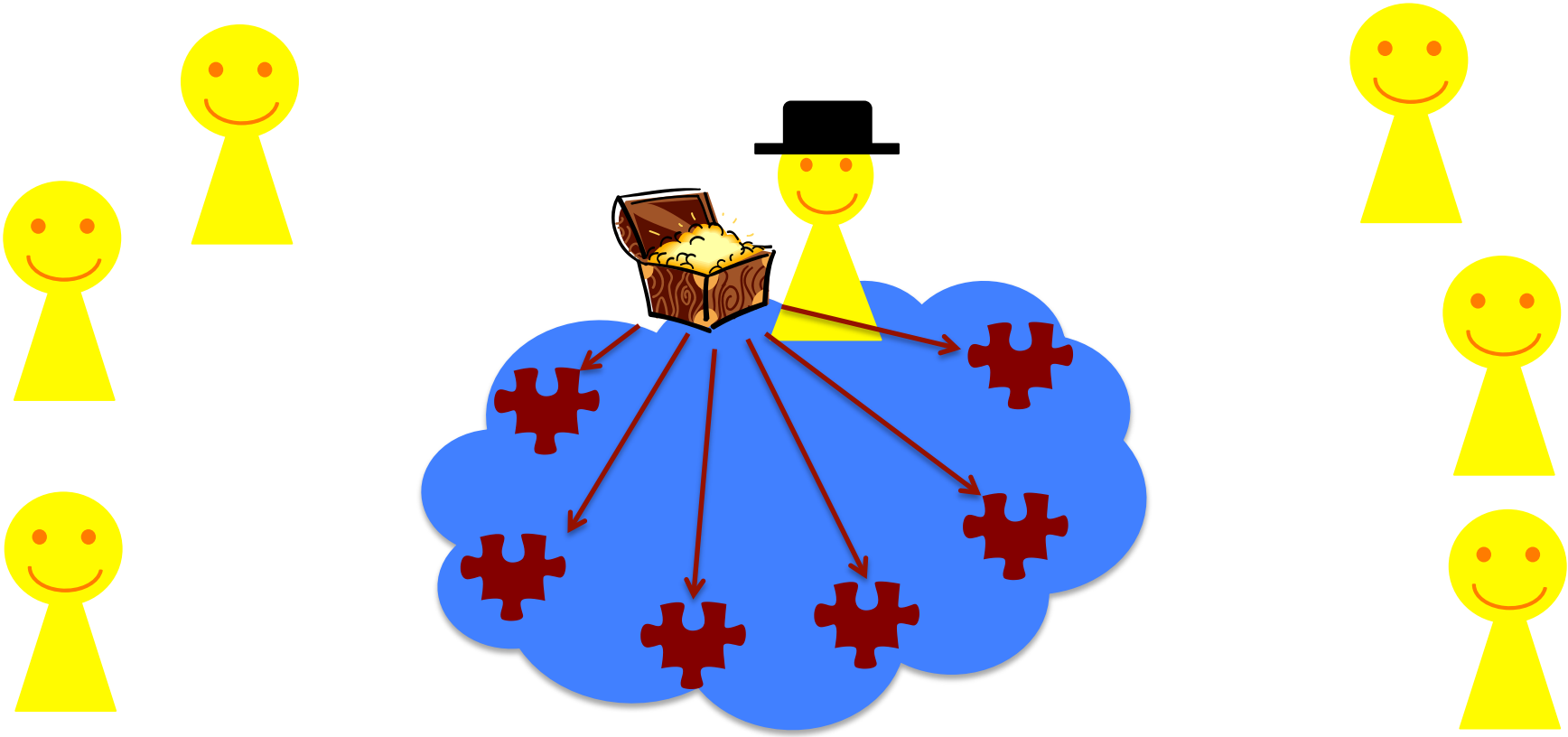
秘密分散とゲーム理論

秘密分散

- 参加者： ディーラー１人とプレイヤー n 人

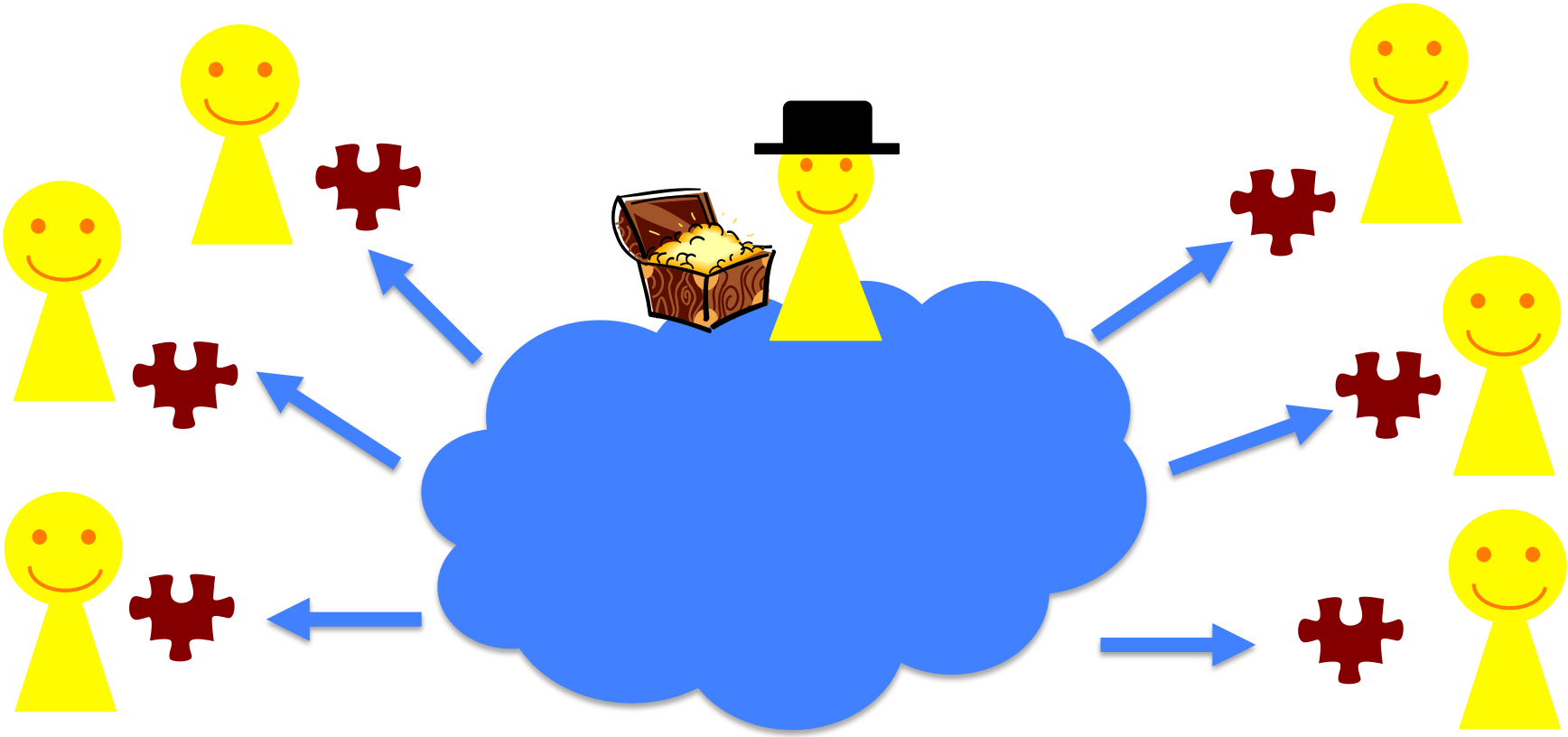
秘密分散

- 分散フェーズ：
  ディーラーは、秘密からシェアを作り、
  各プレイヤーにを配る



秘密分散

- 分散フェーズ：
  ディーラーは、秘密からシェアを作り、
  各プレイヤーにを配る



秘密分散

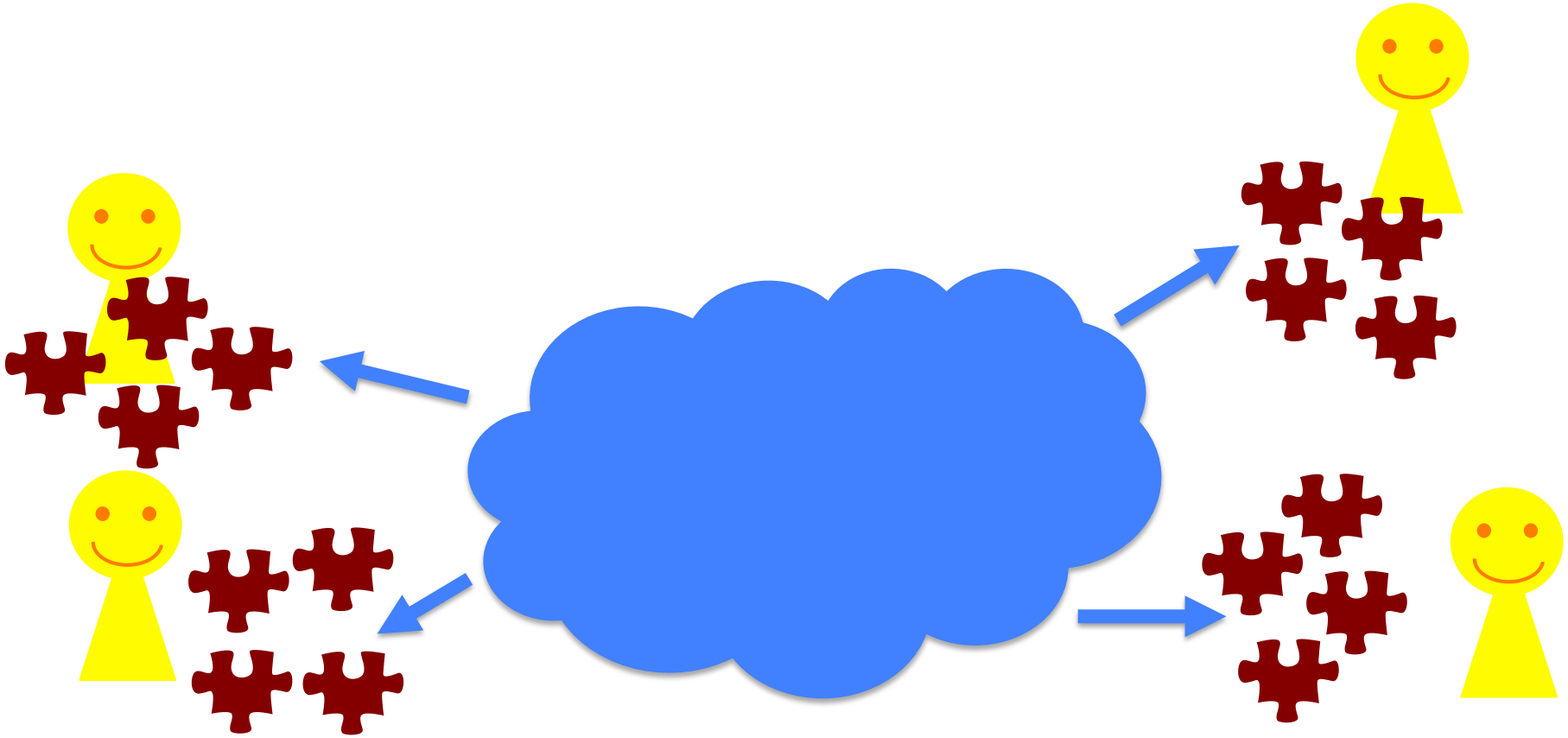
- 復元フェーズ：
  一定人数のプレイヤーがそろったとき、
  シェアを出し合うことで秘密を復元

秘密分散

- 復元フェーズ：
  一定人数のプレイヤーがそろったとき、
  シェアを出し合うことで秘密を復元

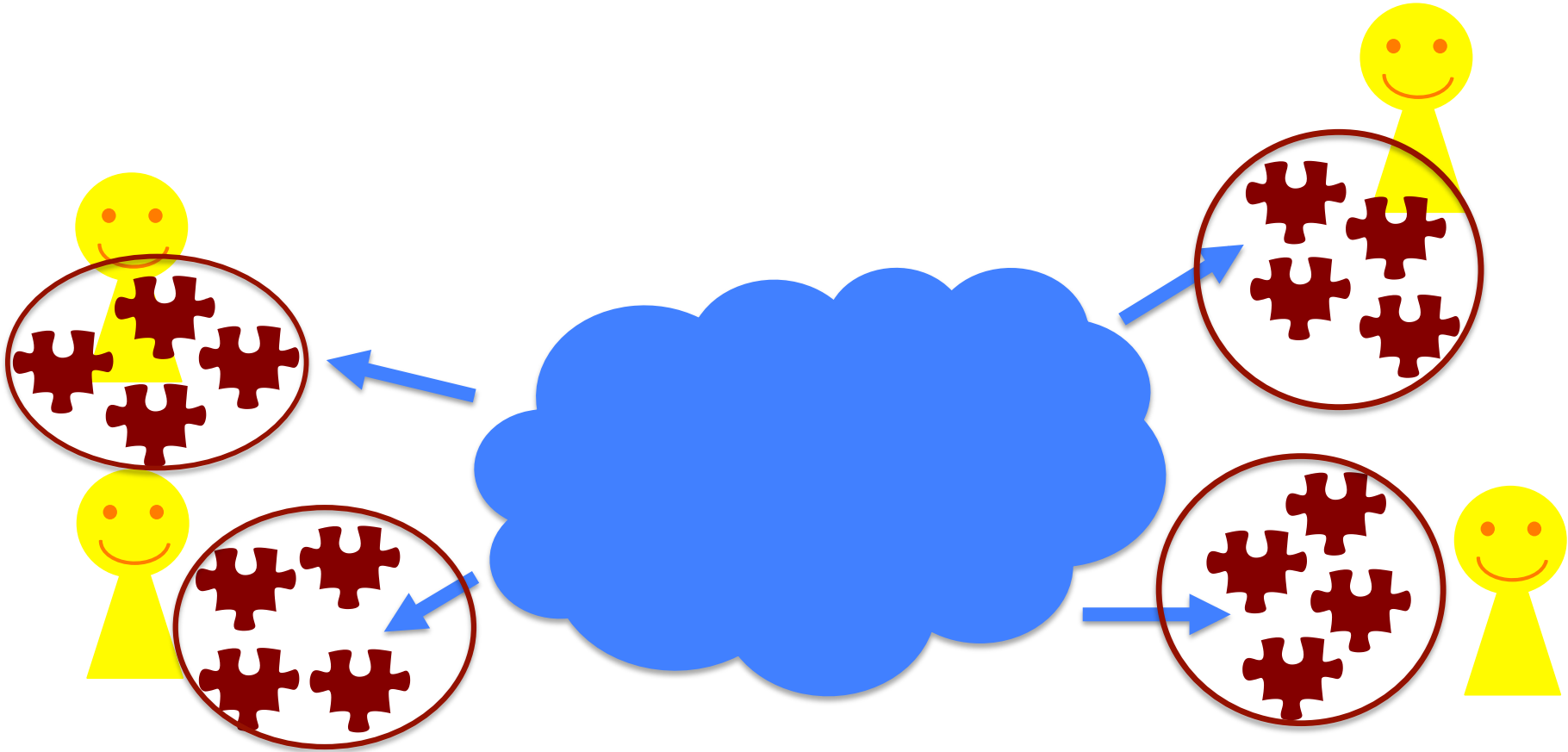
秘密分散

- 復元フェーズ：
  一定人数のプレイヤーがそろったとき、
  シェアを出し合うことで秘密を復元



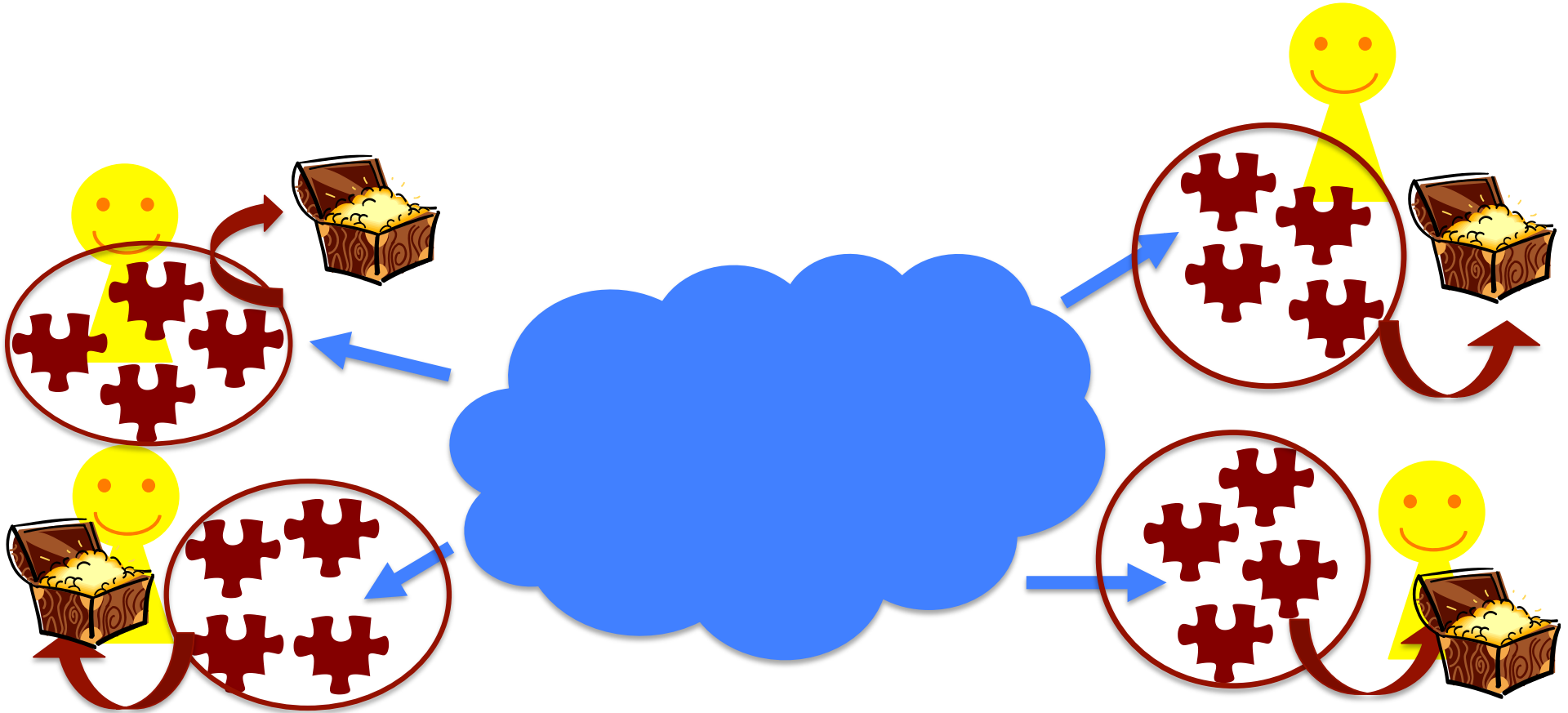
秘密分散

- 復元フェーズ：
  一定人数のプレイヤーがそろったとき、
  シェアを出し合うことで秘密を復元



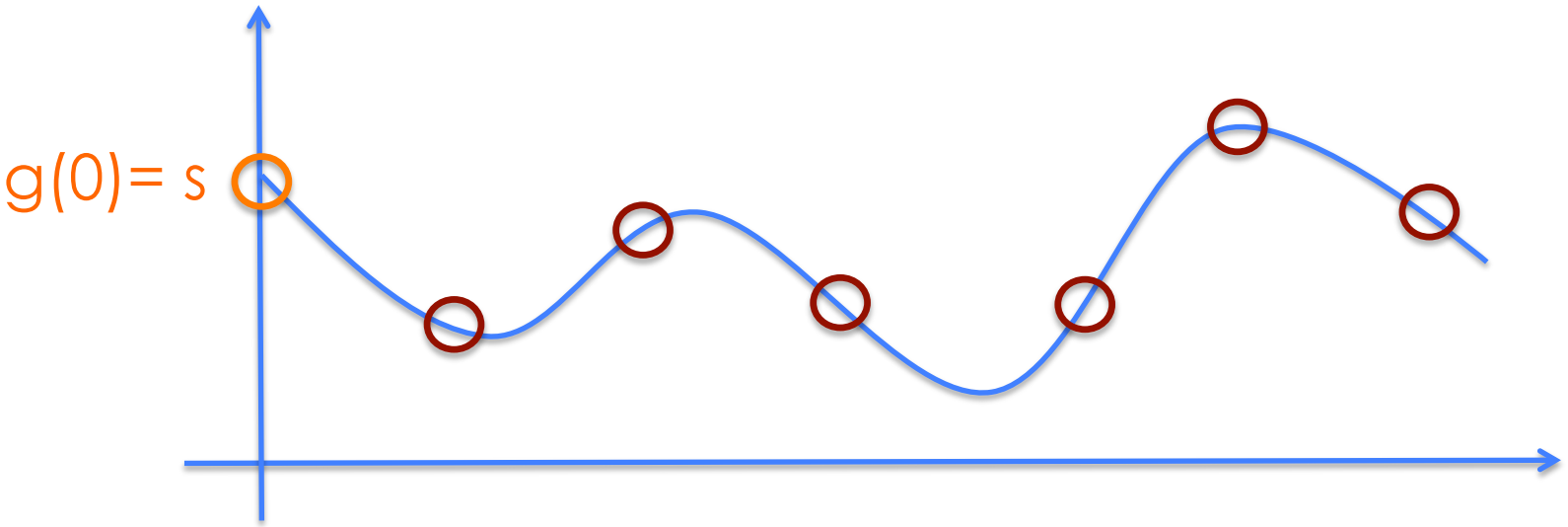
秘密分散

- 復元フェーズ：
  一定人数のプレイヤーがそろったとき、
  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 個以上のシェアから秘密を復元でき、
  m 個未満では秘密についてわからない

- Shamir の秘密分散
  ランダム (m - 1) 次多項式 g s.t. g(0)= s を選び、
  g(1), …, g(n) をシェアとし、多項式補間で復元



[Halpern, Teague 2004]

- プレイヤーの利得

1. 秘密を復元したい
2. より少ない人数で復元したい

Shamir の秘密分散プロトコルは
正しく実行されない

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がよくない

- 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

[Gordon, Katz 08] のプロトコル

- (2, 2) 秘密分散の場合を考える

- プレイヤー P_i の利得
  - P_i だけが復元 → U^+
  - ２人とも復元 → U
  - どちらも復元しない → U^-
  - $U^+ > U > U^-$

GK08 プロトコルのアイディア

- ディーラーは P_1, P_2 それぞれに、
  無限個のシェア $(a_1, a_2, \ldots)$, $(b_1, b_2, \ldots)$を用意
  - 各 i について（独立に）
    - 確率 δ で $a_i + b_i = s$（本物の秘密）
    - 確率 $1 - \delta$ で $a_i + b_i = \perp$（偽物）
- 各ラウンド i において
  - 両プレイヤーはシェア a_i, b_i を同時に出す
  - $a_i + b_i = s$ なら終了
  - $a_i + b_i = \perp$ なら次のラウンドへ
  - もし一人がシェアを出さなかったら終了

GK08 プロトコルの分析

- P_1 が逸脱することを考える
  - Nash 均衡を考えるので P_2 は従うと仮定
- P_1 がシェアを出さないとき、
  P_1 は確率 δ で U^+ を、確率 $1-\delta$ で U^- を得る
  → 期待利得は $\delta U^+ + (1-\delta) U^-$
- P_1 がシェアを出すとき、利得は U
- ここで、$\delta U^+ + (1-\delta) U^- < U$ ならば
  シェアを出すことは、弱支配ではない
- ただし、同時にシェアを出すことに強く依存

実際のプロトコル

- 無限個のシェアを用意することはできない
- ディーラーは $a + b = s$ となるシェアを用意
- 各ラウンド i において
  - P_1 と P_2 は安全なプロトコル(MPC)を利用して a_i と b_i を a と b から生成
  - 残りは同様

[Fuchsbauer, Katz, Naccache 2010] プロトコル

- GK08 等のプロトコルはシェアを
  同時に出すことを必要

  → 同時ブロードキャスト通信路を仮定
- GK08 は MPC を毎ラウンド計算
  - 計算効率はよくない

- FKN10 では上記の問題点を解決し、
  かつ強い解概念をもつプロトコルを提案

FKN10 プロトコルのアイディア

- 基本アイディアは同じ：
  - 本物ラウンドと偽物ラウンドが存在
  - 本物である確率が十分小さいので、プレイヤーは正しくシェアを出し続ける
- 既存プロトコルと異なる点：
  - 既存：本物ラウンドであるかをすぐに認識
  - FKN10：本物ラウンドであるかは後で認識
- 検証可能ランダム関数 (VRF) を利用
  - 擬似ランダム関数であり、正しさを証明で検証可能。また、証明は１つしか存在しない

FKN10 プロトコル

- ディーラーは
  - 本物ラウンド r^* を選ぶ（幾何分布に従う）
  - VRF の鍵を２種類生成：$(pk_i, sk_i), (pk_i', sk_i'), i \in \{1,2\}$
  - P_1 に以下のシェアを渡す（P_2 も同様）
    $(sk_1, sk_1', pk_2, pk_2', shr_1 = F_{sk2}(r^*) + s, sig_1 = F_{sk2'}(r^*+1))$

- 各ラウンド r において（P_1 の立場）
  - $F_{sk1}(r), F_{sk1'}(r)$ とその証明を送る
  - $y^{(r)}$ と $z^{(r)}$ を受け取ったとき
    - $sig_1 = z^{(r)}$ なら $s^{(r-1)} = shr_1 + y^{(r-1)}$ を出力して終了
    - 相手が離脱 or 偽証明を送ったら $s^{(r-1)}$ を出力し終了
    - それ以外の場合、次のラウンドへ

FKN10 プロトコルの分析

- P_2 が従い、P_1 が逸脱することを考える
- 逸脱はラウンド $r = r^* + 1$ または $r < r^* + 1$ で可能
  - $r = r^* + 1$ で逸脱
    → P_2 も s を出力するので利得は U のまま
  - $r < r^* + 1$ で逸脱
    → $r = r^*$ であれば利得は U^+ の可能性があるが、
    本物ラウンドの確率は十分小さく、
    期待利得は U より小さい（ように設定）
- $r = r^* + 1$ での逸脱はプロトコル終了の印であり、逸脱でないとみなすと、逸脱は真に利得を下げる
  → 狭義 Nash 均衡（強い解概念）

FKN10 プロトコルの特徴

- 同時ブロードキャスト通信路を必要としない
  - P2P ネットワークで十分
- 計算効率がよい
  - VRF の部分は TDP で実現可能

- 秘密を見て秘密であることが確信できると問題
  - 秘密がパスワードで、正しさの確認ができる場合
  - この問題は非同時ブロードキャスト通信路では避けられない [Asharov, Lindell 2010]

まとめ（秘密分散とゲーム理論）

- 正直者に合理性を仮定すると
  プロトコルの実現がとても大変になった例
  - 秘密の復元を独占したいと考えるプレイヤーばかりだと、公平に復元することが大変
- 暗号理論として達成が困難（？）
  - 多くのプロトコルで同時ブロードキャスト
  - 非同時ブロードキャストだと
    秘密自体にエントロピーが必要

  → 妥当な仮定等をおいて簡単に実現できないか