合理的な秘密分散における不可能性とその回避方法

安永 憲司

九州先端科学技術研究所

コンピュータセキュリティシンポジウム 2012 @ 松江

暗号理論とゲーム理論

- 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（既存研究）

- 暗号理論をゲーム理論に利用
  - 信頼できる仲介者を暗号技術で実現 [DHR06, ADGH06, LMPS04, ILM05, ILM08]
- 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
    - 秘密分散 [HT04, ADGH06, LT06, GK06, KN08a, KN08b, MS09, OPRV09, AL09, FKN10, PS11]
    - リーダー選出，ランダムサンプリング [Gra10]
    - ビザンチン合意 [GKTZ12]
    - 公開鍵暗号 [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る安全性特徴付け[ACH11, GK12]

暗号理論とゲーム理論（既存研究）

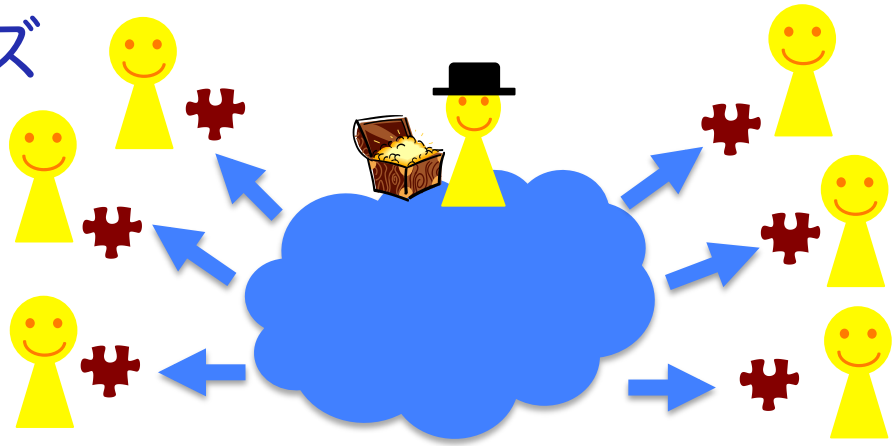
- 暗号理論をゲーム理論に利用
  - 信頼できる仲介者を暗号技術で実現 [DHR06, ADGH06, LMPS04, ILM05, ILM08]
- ゲーム理論を暗号理論へ適用
  - 合理的なプレイヤーが暗号プロトコルを実行
    - 秘密分散 [HT04, ADGH06, LT06, GK06, KN08a, KN08b, MS09, OPRV09, AL09, FKN10, PS11]
    - リーダー選出，ランダムサンプリング [Gra10]
    - ビザンチン合意 [GKTZ12]
    - 公開鍵暗号 [Y12]

本研究

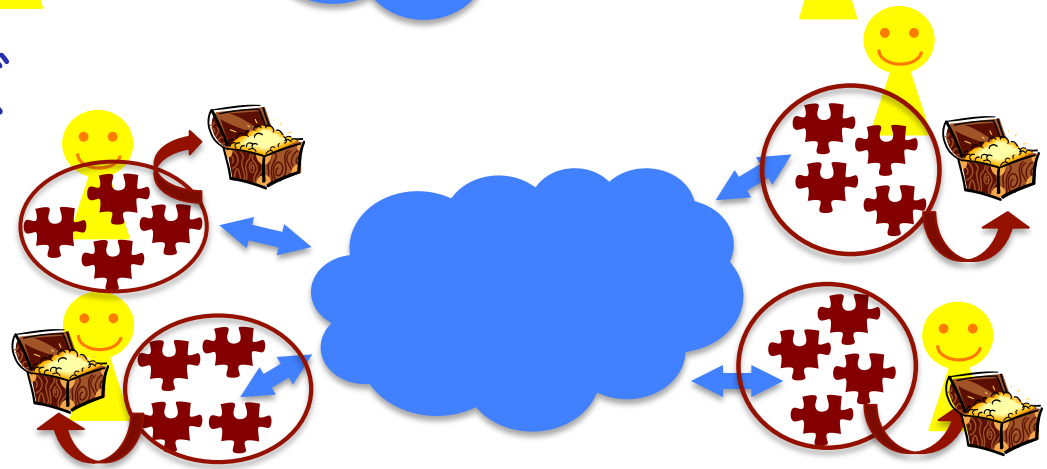
- ゲーム理論と暗号理論の概念間の関係
  - 暗号理論向けのゲーム理論の概念 [HP10, GLV10, PS11]
  - ゲーム理論の概念による安全性特徴付け[ACH11, GK12]

秘密分散

- 分散フェーズ



- 復元フェーズ



- (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

合理的な秘密分散

- 単純な設定では、各プレイヤーは正直者と仮定

合理的な秘密分散

- 単純な設定では、各プレイヤーは正直者と仮定
- Halpern, Teague (STOC '04)
  - プレイヤーが自分の利益のため行動すると？

合理的な秘密分散

- 単純な設定では、各プレイヤーは正直者と仮定
- Halpern, Teague (STOC '04)
  - プレイヤーが自分の利益のため行動すると？

    → Shamir の秘密分散は正しく実行されない

合理的な秘密分散

- 単純な設定では、各プレイヤーは正直者と仮定
- Halpern, Teague (STOC '04)
  - プレイヤーが自分の利益のため行動すると？

    → Shamir の秘密分散は正しく実行されない
  - 自分の利益のために行動するプレイヤー

    → 合理的なプレイヤー

合理的な秘密分散

- 単純な設定では、各プレイヤーは正直者と仮定
- Halpern, Teague (STOC '04)
  - プレイヤーが自分の利益のため行動すると？

    → Shamir の秘密分散は正しく実行されない
  - 自分の利益のために行動するプレイヤー

    → 合理的なプレイヤー
  - 合理的なプレイヤーが正しく実行可能

    → 合理的な秘密分散

Halpern, Teague (STOC ’04)

Halpern, Teague (STOC ’04)

- 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 (STOC ’04)

- 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
- (n, n) 秘密分散の復元フェーズを考える

Halpern, Teague (STOC '04)

- 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
- (n, n) 秘密分散の復元フェーズを考える
  - プレイヤーは正直にシェアを出すだろうか？

Halpern, Teague (STOC '04)

- 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
- (n, n) 秘密分散の復元フェーズを考える
  - プレイヤーは正直にシェアを出すだろうか？
  - 他プレイヤーがシェアを出すと仮定したとき

Halpern, Teague (STOC '04)

- 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
- (n, n) 秘密分散の復元フェーズを考える
  - プレイヤーは正直にシェアを出すだろうか？
  - 他プレイヤーがシェアを出すと仮定したとき
    - 自分がシェアを出せば、 n 人全員が秘密を復元

Halpern, Teague (STOC '04)

- 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
- (n, n) 秘密分散の復元フェーズを考える
  - プレイヤーは正直にシェアを出すだろうか？
  - 他プレイヤーがシェアを出すと仮定したとき
    - 自分がシェアを出せば、 n 人全員が秘密を復元
    - 自分がシェアを出さなければ、自分 1 人が復元

Halpern, Teague (STOC '04)

- 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
- (n, n) 秘密分散の復元フェーズを考える
  - プレイヤーは正直にシェアを出すだろうか？
  - 他プレイヤーがシェアを出すと仮定したとき
    - 自分がシェアを出せば、 n 人全員が秘密を復元
    - 自分がシェアを出さなければ、自分 1 人が復元

  → シェアを出さない方が利得が高い
  （シェアを出すことは Nash 均衡でない）

Nash 均衡と結託耐性

- Nash 均衡

  どのプレイヤーも、
  他のプレイヤーがプロトコルに従うとき、
  プロトコルから逸脱しても利得は増えない

  - 逸脱したときに利得が減る → 狭義 Nash 均衡

- 結託耐性 r の Nash 均衡

  r 人が結託して逸脱しても Nash 均衡

不可能性に関する既知結果

- Asharov, Lindell (Crypto '09)
  - n = 2 のとき、
    定数ラウンド復元プロトコルは存在しない
    - 解概念として Nash 均衡を考える場合
    - 復元ラウンド数が利得の値に依存することを証明
  - 結託耐性 n/2 を達成する
    定数ラウンド復元プロトコルは存在しない
    - n = 2 の場合に帰着して証明

本研究

- KOTY プロトコルの問題点の指摘

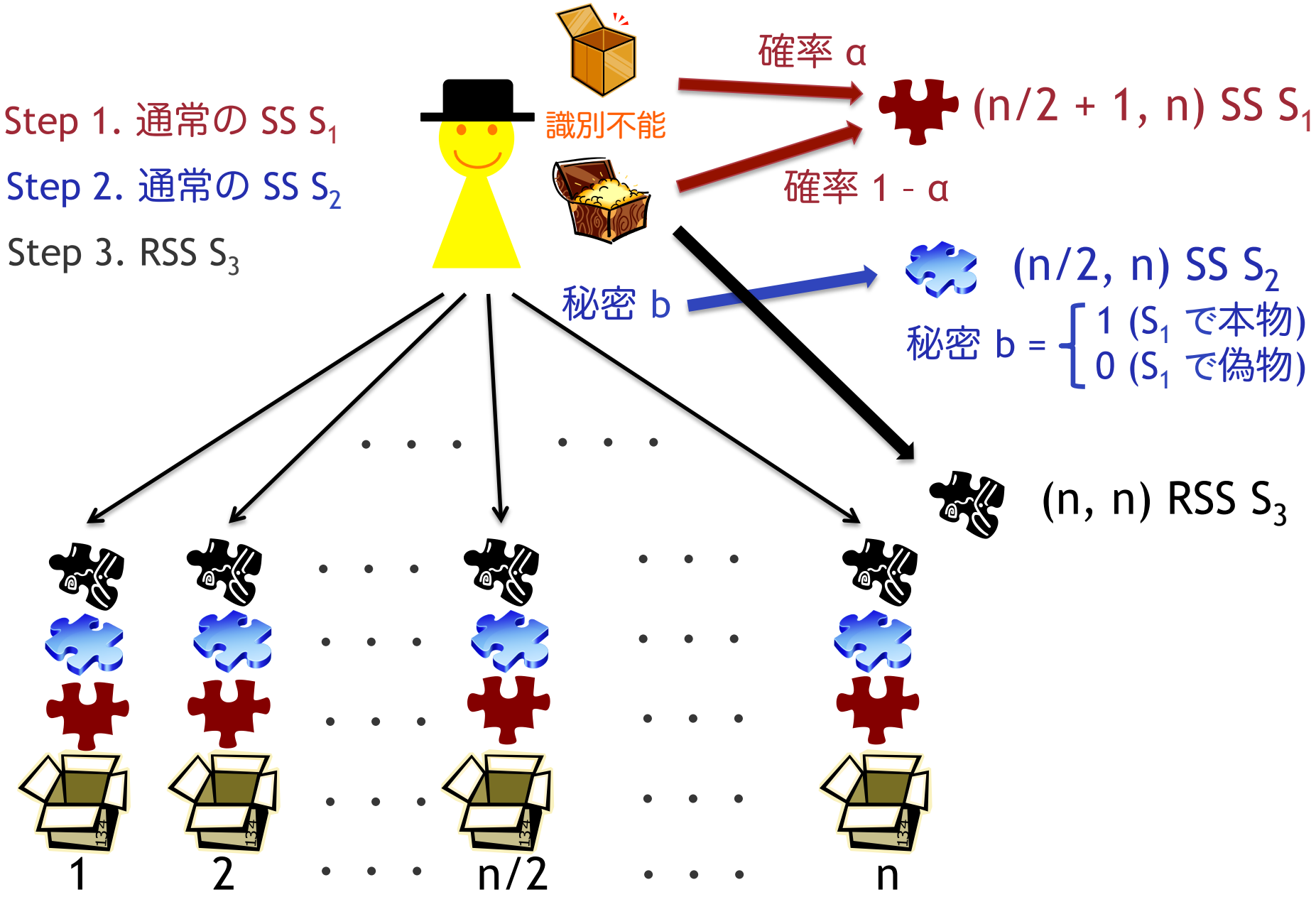
  [KOTY12]
  A. Kawachi, Y. Okamoto, K. Tanaka, K. Yasunaga.
  Rational secret sharing for non-simultaneous channels.
  IEICE Technical Report, 2012

- 回避方法の提案
  - 不可能性の回避につながる

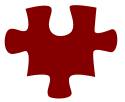
KOTY プロトコル

- ブロードキャスト通信路を仮定
  - １人ずつ順番にブロードキャスト
- 定数ラウンド復元
  - 高い確率で 2 ラウンド
- 結託耐性 n/2 - 1 の狭義 Nash 均衡
  - 定数ラウンド復元では最適な結託耐性

KOTY プロトコル （分散フェーズ）



KOTY プロトコル （復元フェーズ）

Step 1. (n/2 + 1, n) S_1 のシェア  を順に出す

- 全員正しいシェア → 次のラウンド
  それ以外 → 終了

Step 2. (n/2, n) S_2 のシェア  を順に出す

- 全員正しいシェア ∧ b = 0 → 次のラウンド
  それ以外 → 終了

Step 3. (n, n) S_3 のシェア  を使って秘密 s を復元

- 結託耐性 n/2 - 1 の狭義 Nash である直観的理由
  - Step 1 で逸脱 → 偽物の可能性が残る
  - Step 2 で逸脱 → Step 3 に進めない

KOTY プロトコルの性質

- 定理
  S_3 が結託耐性 n/2 - 1 の狭義 Nash であるとき、
  KOTY も結託耐性 n/2 - 1 の狭義 Nash
  復元ラウンド数 = $2(1 - \alpha) + T_3 \cdot \alpha$
  - T_3 は S_3 の復元ラウンド数
  - α を十分小さくとれば復元ラウンド数 ≈ 2

KOTY プロトコルの問題点

KOTY プロトコルの問題点

- より望ましく見える戦略が存在

KOTY プロトコルの問題点

- より望ましく見える戦略が存在
  - Step 1 で、n/2 個のシェアが出た後、
    自分のシェアとあわせて秘密を復元して終了

KOTY プロトコルの問題点

- より望ましく見える戦略が存在
  - Step 1 で、n/2 個のシェアが出た後、
    自分のシェアとあわせて秘密を復元して終了
    - 最初の n/2 人のプレイヤーは秘密を復元できない
    - 残りの n/2 人は確率 1 - α で本物の秘密を復元

    少ない人数で復元 → 利得が高くなる可能性

KOTY プロトコルの問題点

- より望ましく見える戦略が存在
  - Step 1 で、n/2 個のシェアが出た後、
    自分のシェアとあわせて秘密を復元して終了
    - 最初の n/2 人のプレイヤーは秘密を復元できない
    - 残りの n/2 人は確率 1 - α で本物の秘密を復元

    少ない人数で復元 → 利得が高くなる可能性
- 結託耐性 n/2 - 1 の狭義 Nash に矛盾？

KOTY プロトコルの問題点

- より望ましく見える戦略が存在
  - Step 1 で、n/2 個のシェアが出た後、
    自分のシェアとあわせて秘密を復元して終了
    - 最初の n/2 人のプレイヤーは秘密を復元できない
    - 残りの n/2 人は確率 1 - α で本物の秘密を復元

    少ない人数で復元 → 利得が高くなる可能性
- 結託耐性 n/2 - 1 の狭義 Nash に矛盾？
  → 矛盾しない
  - 上記の議論では n/2 人が逸脱する必要

何が問題なのか？

何が問題なのか？

- 結託耐性が n/2 - 1 しかないこと
  - 結託耐性が n - 1 なら問題は生じない

何が問題なのか？

- 結託耐性が n/2 - 1 しかないこと
  - 結託耐性が n - 1 なら問題は生じない

- しかし、不可能性の結果 [AL 11] から、
  定数ラウンドプロトコルの結託耐性 ≤ n/2 - 1

何が問題なのか？

- 結託耐性が n/2 - 1 しかないこと
  - 結託耐性が n - 1 なら問題は生じない

- しかし、不可能性の結果 [AL 11] から、
  定数ラウンドプロトコルの結託耐性 ≤ n/2 - 1

  → 不可能性を回避する必要

不可能性の回避方法

不可能性の回避方法

- 利得関数に仮定を追加
  「偽物の秘密を復元することを嫌がる」

不可能性の回避方法

- 利得関数に仮定を追加
  「偽物の秘密を復元することを嫌がる」

- 先ほどの問題は回避可能
  - 偽物の可能性があれば、逸脱しない

不可能性の回避方法

- 利得関数に仮定を追加
  「偽物の秘密を復元することを嫌がる」

- 先ほどの問題は回避可能
  - 偽物の可能性があれば、逸脱しない

- 定理
  上記仮定のもと、修正版 KOTY プロトコルは
  結託耐性 n - 1 の狭義 Nash を達成
  - S_1 と S_2 をともに (n, n) 秘密分散に変更

まとめ

- KOTY プロトコルの問題点
  - より望ましい戦略が存在

  → 結託耐性が小さいことが問題

- 不可能性の回避
  - 利得関数に仮定を追加

    「偽物の秘密を復元することを嫌がる」

  → 結託耐性 n - 1 を達成可能に