Mental Jinro を支える暗号技術

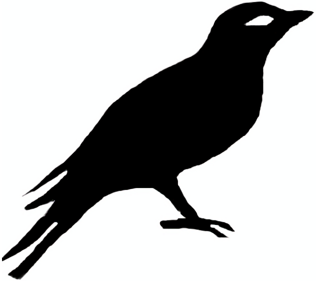
Tsukuba.pm #3

吉村 優

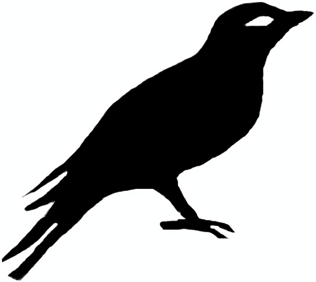
https://twitter.com/_yyu_
http://qiita.com/yyu
https://github.com/y-yu

May 14, 2016

自己紹介

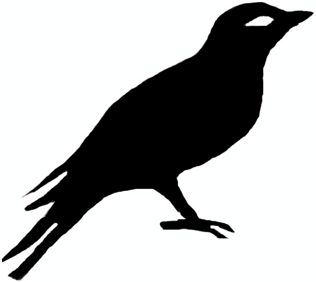


自己紹介



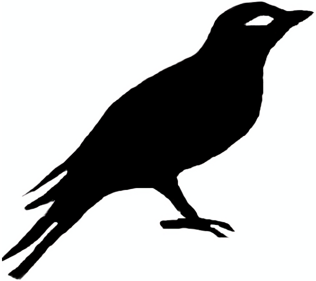
- 筑波大学 情報科学類 学士（COINS11）

自己紹介



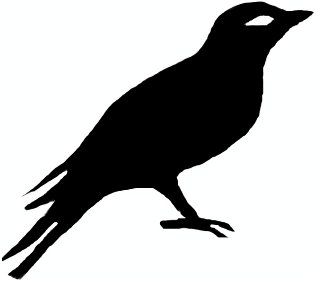
- 筑波大学 情報科学類 学士（COINS11）
- WORD 編集部 OB

自己紹介



- 筑波大学 情報科学類 学士（COINS11）
- WORD 編集部 OB
- プログラム論理研究室 OB

自己紹介



- 筑波大学 情報科学類 学士（COINS11）
- WORD 編集部 OB
- プログラム論理研究室 OB
- 現在は Scala を書く仕事に従事

Mental Jinro とは？

Mental Jinro とは？

> “ *Mental Jinro* は人狼からゲームマスターを排除したゲームである ”

Mental Jinro とは？

> *Mental Jinro* は人狼からゲームマスターを排除したゲームである

ゲームマスターとは何か？

Mental Jinro とは？

> *Mental Jinro* は人狼からゲームマスターを排除したゲームである

ゲームマスターとは何か？

そもそも人狼とは何か？

人狼とは？

人狼 *

“

”

Wikipedia —— 汝は人狼なりや？

* 人狼には様々なルールがあるが、このスライドではこのルールを用いる

人狼とは？

人狼 *

“

- プレイヤーはそれぞれが**村人**と村人に化けた**人狼**となり、自分自身の正体がばれないように他のプレイヤーと交渉して正体を探る

”

Wikipedia —— 汝は人狼なりや？

* 人狼には様々なルールがあるが、このスライドではこのルールを用いる

人狼とは？

人狼 *

- プレイヤーはそれぞれが**村人**と村人に化けた**人狼**となり、自分自身の正体がばれないように他のプレイヤーと交渉して正体を探る
- ゲームは半日単位で進行し、昼には全プレイヤーの投票により決まった人狼容疑者の**処刑**が、夜には人狼による村人の**襲撃**が行われる

Wikipedia —— 汝は人狼なりや？

* 人狼には様々なルールがあるが、このスライドではこのルールを用いる

人狼とは？

人狼 *

“

- プレイヤーはそれぞれが**村人**と村人に化けた**人狼**となり、自分自身の正体がばれないように他のプレイヤーと交渉して正体を探る
- ゲームは半日単位で進行し、昼には全プレイヤーの投票により決まった人狼容疑者の**処刑**が、夜には人狼による村人の**襲撃**が行われる
-
  - 全ての人狼を処刑することができれば村人チームの勝ち

”

Wikipedia —— 汝は人狼なりや？

* 人狼には様々なルールがあるが、このスライドではこのルールを用いる

人狼とは？

人狼 *

“

- プレイヤーはそれぞれが**村人**と村人に化けた**人狼**となり、自分自身の正体がばれないように他のプレイヤーと交渉して正体を探る
- ゲームは半日単位で進行し、昼には全プレイヤーの投票により決まった人狼容疑者の**処刑**が、夜には人狼による村人の**襲撃**が行われる
-
    - 全ての人狼を処刑することができれば村人チームの勝ち
    - 人狼と同じ数まで村人を減らすことができれば人狼チームの勝ち

”

Wikipedia —— 汝は人狼なりや？

---

* 人狼には様々なルールがあるが、このスライドではこのルールを用いる

人狼の役職

人狼に必要な役職

参加者を次の役職に分ける必要がある

人狼の役職

人狼に必要な役職

参加者を次の役職に分ける必要がある

- 村人

人狼の役職

人狼に必要な役職

参加者を次の役職に分ける必要がある

- 村人
- 人狼

人狼の役職

人狼に必要な役職

参加者を次の役職に分ける必要がある

- 村人
- 人狼
- ゲームマスター

人狼の役職

人狼に必要な役職

参加者を次の役職に分ける必要がある

- 村人
- 人狼
- ゲームマスター

ゲームマスターとは何か？

ゲームマスターと公平性

ゲームマスターの役割

ゲームマスターと公平性

ゲームマスターの役割

- 人狼と村人のチーム分けをする

ゲームマスターと公平性

ゲームマスターの役割

- 人狼と村人のチーム分けをする
- 人狼に襲撃された村人を村人チームに宣告する

ゲームマスターと公平性

ゲームマスターの役割

- 人狼と村人のチーム分けをする
- 人狼に襲撃された村人を村人チームに宣告する
- 人狼と村人の数を管理し、どちらかのチームが勝利した時それを宣言する

ゲームマスターと公平性

ゲームマスターの役割

- 人狼と村人のチーム分けをする
- 人狼に襲撃された村人を村人チームに宣告する
- 人狼と村人の数を管理し、どちらかのチームが勝利した時それを宣言する

ゲームマスターとは審判

ゲームマスターと公平性

ゲームマスターの役割

- 人狼と村人のチーム分けをする
- 人狼に襲撃された村人を村人チームに宣告する
- 人狼と村人の数を管理し、どちらかのチームが勝利した時それを宣言する

ゲームマスターとは審判

ゲームマスターが不公平だったら？

ゲームマスターと公平性

ゲームマスターの役割

- 人狼と村人のチーム分けをする
- 人狼に襲撃された村人を村人チームに宣告する
- 人狼と村人の数を管理し、どちらかのチームが勝利した時それを宣言する

ゲームマスターとは審判

ゲームマスターが不公平だったら？

大問題！

Mental Jinro

ゲームマスターを消そう！

Mental Jinro

ゲームマスターを消そう！

ゲームマスターが消えると……

Mental Jinro

ゲームマスターを消そう！

ゲームマスターが消えると……

- チーム分けはどうする？

Mental Jinro

ゲームマスターを消そう！

ゲームマスターが消えると……

- チーム分けはどうする？
- 襲撃された村人の情報をどう伝える？

ゲームマスターを消そう！

ゲームマスターが消えると……

- チーム分けはどうする？
- 襲撃された村人の情報をどう伝える？
- 勝敗は誰が判断する？

Mental Jinro を支える暗号技術

Mental Jinroを支える暗号技術
コミットメント

コイントスゲーム

アリスとボブの二人がいるとする

コイントスゲーム

アリスとボブの二人がいるとする

1. アリスがコインの "表" または "裏" を紙に書き、紙を封筒に入れる

コイントスゲーム

アリスとボブの二人がいるとする

1. アリスがコインの“表” または “裏” を紙に書き、紙を封筒に入れる
2. ボブはコインを投げる

コイントスゲーム

アリスとボブの二人がいるとする

1. アリスがコインの “表” または “裏” を紙に書き、紙を封筒に入れる
2. ボブはコインを投げる
3. 封筒から紙を取り出し、
   - アリスの予想とコインの結果が同じなら、アリスの勝利
   - アリスの予想とコインの結果が違えば、ボブの勝利

コイントスゲーム

アリスとボブの二人がいるとする

1. アリスがコインの"表"または"裏"を紙に書き、紙を封筒に入れる
2. ボブはコインを投げる
3. 封筒から紙を取り出し、
    - アリスの予想とコインの結果が同じなら、アリスの勝利
    - アリスの予想とコインの結果が違えば、ボブの勝利
4. このゲームは電話上で行う

コイントスゲーム

アリスとボブの二人がいるとする

1. アリスがコインの“表”または“裏”を紙に書き、紙を封筒に入れる
2. ボブはコインを投げる
3. 封筒から紙を取り出し、
   - アリスの予想とコインの結果が同じなら、アリスの勝利
   - アリスの予想とコインの結果が違えば、ボブの勝利
4. このゲームは電話上で行う

アリスが予想を反故にする？

コイントスゲーム

アリスとボブの二人がいるとする

1. アリスがコインの “表” または “裏” を紙に書き、紙を**封筒**に入れる
2. ボブはコインを投げる
3. 封筒から紙を取り出し、
   - アリスの予想とコインの結果が同じなら、アリスの勝利
   - アリスの予想とコインの結果が違えば、ボブの勝利
4. このゲームは**電話上**で行う

アリスが予想を**反故**にする？

封筒をどうやって実現する？

コイントスゲーム

プロトコル

†整数 $x \bmod p$ かつ $xy \equiv 1 \pmod{p}$ となる逆元 y が存在する x の集合である

‡後述する

コイントスゲーム

プロトコル

1. ボブは $p = 2q + 1$ となる大きな素数 p, q をランダムに生成して、$\mathbb{Z}_p^{*}$[†] の位数 q の部分群 G から**生成元**[‡] g, v をランダムに選択して p, q, g, v をアリスへ送信する

[†] 整数 $x \bmod p$ かつ $xy \equiv 1 \pmod p$ となる逆元 y が存在する x の集合である

[‡] 後述する

コイントスゲーム

プロトコル

1. ボブは $p = 2q + 1$ となる大きな素数 p, q をランダムに生成して、$\mathbb{Z}_p^{*}$[†] の位数 q の部分群 G から**生成元**[‡] g, v をランダムに選択して p, q, g, v をアリスへ送信する
2. アリスは p, q, g, v を検証し、表と予想するなら $m := 1$ を選択し、裏と予想するなら $m := q - 1$ を選択し、乱数 $r \in \{1, \ldots, q-1\}$ を用いて $c := g^r v^m \bmod p$ 計算し c をボブへ送信する

[†] 整数 $x \bmod p$ かつ $xy \equiv 1 \pmod{p}$ となる逆元 y が存在する x の集合である

[‡] 後述する

コイントスゲーム

プロトコル

1. ボブは $p = 2q + 1$ となる大きな素数 p, q をランダムに生成して、$\mathbb{Z}_p^{*}$[†] の位数 q の部分群 G から**生成元**[‡] g, v をランダムに選択して p, q, g, v をアリスへ送信する
2. アリスは p, q, g, v を検証し、表と予想するなら $m := 1$ を選択し、裏と予想するなら $m := q - 1$ を選択し、乱数 $r \in \{1, \ldots, q - 1\}$ を用いて $c := g^r v^m \bmod p$ 計算し c をボブへ送信する
3. ボブはコイントスをして、結果をアリスへ送信する

[†] 整数 $x \bmod p$ かつ $xy \equiv 1 \pmod{p}$ となる逆元 y が存在する x の集合である

[‡] 後述する

コイントスゲーム

プロトコル

1. ボブは $p = 2q + 1$ となる大きな素数 p, q をランダムに生成して、$\mathbb{Z}_p^{*}$[†] の位数 q の部分群 G から**生成元**[‡] g, v をランダムに選択して p, q, g, v をアリスへ送信する
2. アリスは p, q, g, v を検証し、表と予想するなら $m := 1$ を選択し、裏と予想するなら $m := q - 1$ を選択し、乱数 $r \in \{1, \ldots, q-1\}$ を用いて $c := g^r v^m \bmod p$ 計算し c をボブへ送信する
3. ボブはコイントスをして、結果をアリスへ送信する
4. アリスは r, m を公開する

[†] 整数 $x \bmod p$ かつ $xy \equiv 1 \pmod p$ となる逆元 y が存在する x の集合である

[‡] 後述する

コイントスゲーム

プロトコル

1. ボブは $p = 2q + 1$ となる大きな素数 p, q をランダムに生成して、$\mathbb{Z}_p^{*}$[†] の位数 q の部分群 G から**生成元**[‡] g, v をランダムに選択して p, q, g, v をアリスへ送信する
2. アリスは p, q, g, v を検証し、表と予想するなら $m := 1$ を選択し、裏と予想するなら $m := q - 1$ を選択し、乱数 $r \in \{1, \ldots, q-1\}$ を用いて $c := g^r v^m \bmod p$ 計算し c をボブへ送信する
3. ボブはコイントスをして、結果をアリスへ送信する
4. アリスは r, m を公開する
5. ボブは $c \equiv g^r v^m \pmod p$ を検証する

[†]整数 $x \bmod p$ かつ $xy \equiv 1 \pmod p$ となる逆元 y が存在する x の集合である

[‡]後述する

コイントスゲームの検証

コイントスゲームの検証

アリスが予想を**反故**にする？

コイントスゲームの検証

アリスが予想を**反故**にする？

アリスは m をコミットした後で、$m'(m' \neq m)$ と偽れる

$\Downarrow$ ならば

コイントスゲームの検証

アリスが予想を反故にする？

アリスは m をコミットした後で、$m'(m' \neq m)$ と偽れる

$\Downarrow$ ならば

アリスは $g^r v^m = g^{r'} v^{m'}$ となる r' を計算できる

$\Downarrow$ ならば

コイントスゲームの検証

アリスが予想を**反故**にする？

アリスは m をコミットした後で、$m'(m' \neq m)$ と偽れる

$\Downarrow$ ならば

アリスは $g^r v^m = g^{r'} v^{m'}$ となる r' を計算できる

$\Downarrow$ ならば

アリスは g を何乗したら v となるかという**離散対数**が求められる

$$
\begin{aligned}
g^r v^m &\equiv g^{r'} v^{m'} && \pmod{p} \\
v^{m-m'} &\equiv g^{r'-r} && \pmod{p} \\
\log_g \left(v^{m-m'}\right) &\equiv r' - r && \pmod{q} \\
\log_g v &\equiv (r'-r)/(m-m') && \pmod{q}
\end{aligned}
$$

離散対数問題

離散対数問題

“次の条件を満す $g, p, y (y = g^x \bmod p)$ が与えられたとき、x を求める問題のことである”

クラウドを支えるこれからの暗号技術 *[2]*

§このような g のことを**生成元**と言い、生成元は全ての $i = 1, \ldots, q-1$ と $j = 1, \ldots, q-1$ について、$i \neq j$ ならば $g^i \not\equiv g^j \pmod p$ となる

離散対数問題

離散対数問題

“次の条件を満す $g, p, y (y = g^x \bmod p)$ が与えられたとき、x を求める問題のことである”

クラウドを支えるこれからの暗号技術 *[2]*

g, p が次を満すとき、離散対数問題を解くことは困難

§このような g のことを**生成元**と言い、生成元は全ての $i = 1, \ldots, q-1$ と $j = 1, \ldots, q-1$ について、$i \neq j$ ならば $g^i \not\equiv g^j \pmod p$ となる

離散対数問題

離散対数問題

“ 次の条件を満す $g, p, y (y = g^x \bmod p)$ が与えられたとき、x を求める問題のことである ”

クラウドを支えるこれからの暗号技術 *[2]*

g, p が次を満すとき、離散対数問題を解くことは困難

- p は巨大な素数

§このような g のことを**生成元**と言い、生成元は全ての $i = 1, \ldots, q-1$ と $j = 1, \ldots, q-1$ について、$i \neq j$ ならば $g^i \not\equiv g^j \pmod{p}$ となる

離散対数問題

離散対数問題

“ 次の条件を満す $g, p, y (y = g^x \bmod p)$ が与えられたとき、x を求める問題のことである ”

クラウドを支えるこれからの暗号技術 *[2]*

g, p が次を満すとき、離散対数問題を解くことは困難

- p は巨大な素数
- $p-1$ の約数の中に、巨大な素数 q が含まれている

§このような g のことを**生成元**と言い、生成元は全ての $i = 1, \ldots, q-1$ と $j = 1, \ldots, q-1$ について、$i \neq j$ ならば $g^i \not\equiv g^j \pmod{p}$ となる

離散対数問題

離散対数問題

> 次の条件を満す $g, p, y (y = g^x \bmod p)$ が与えられたとき、x を求める問題のことである
>
> クラウドを支えるこれからの暗号技術 *[2]*

g, p が次を満すとき、離散対数問題を解くことは困難

- p は巨大な素数
- $p - 1$ の約数の中に、巨大な素数 q が含まれている
- g は全ての $i = 1, \ldots, q-1$ について、$g^i \not\equiv 1 \pmod p$ となる §

---

§このような g のことを**生成元**と言い、生成元は全ての $i = 1, \ldots, q-1$ と $j = 1, \ldots, q-1$ について、$i \neq j$ ならば $g^i \not\equiv g^j \pmod p$ となる

コイントスゲーム

プロトコル

1. ボブは $p = 2q + 1$ となる大きな素数 p, q をランダムに生成して、$\mathbb{Z}_p^{*}$[†] の位数 q の部分群 G から**生成元**[‡] g, v をランダムに選択して p, q, g, v をアリスへ送信する
2. アリスは p, q, g, v を検証し、表と予想するなら $m := 1$ を選択し、裏と予想するなら $m := q - 1$ を選択し、乱数 $r \in \{1, \ldots, q - 1\}$ を用いて $c := g^r v^m \bmod p$ 計算し c をボブへ送信する
3. ボブはコイントスをして、結果をアリスへ送信する
4. アリスは r, m を公開する
5. ボブは $c \equiv g^r v^m \pmod p$ を検証する

[†] 整数 $x \bmod p$ かつ $xy \equiv 1 \pmod p$ となる逆元 y が存在する x の集合である

[‡] 後述する

コイントスゲームの検証

アリスが予想を反故にする？

アリスは m をコミットした後で、$m'(m' \neq m)$ と偽れる

$\Downarrow$ ならば

アリスは $g^r v^m = g^{r'} v^{m'}$ となる r' を計算できる

$\Downarrow$ ならば

アリスは g を何乗したら v となるかという離散対数が求められる

$$
\begin{aligned}
g^r v^m &\equiv g^{r'} v^{m'} && \pmod p \\
v^{m-m'} &\equiv g^{r'-r} && \pmod p \\
\log_g (v^{m-m'}) &\equiv r' - r && \pmod q \\
\log_g v &\equiv (r' - r)/(m - m') && \pmod q
\end{aligned}
$$

コイントスゲームの検証

アリスは m をコミットした後で、$m'(m' \neq m)$ と偽れる

$$\Downarrow \text{ならば}$$

アリスは g を何乗したら v となるかという**離散対数**が求められる

コイントスゲームの検証

アリスは m をコミットした後で、$m'(m' \neq m)$ と偽れる

$\Downarrow$ ならば

アリスは g を何乗したら v となるかという**離散対数**が求められる

離散対数問題を解くことは困難であるということに矛盾する

コイントスゲームの検証

アリスは m をコミットした後で、$m'(m' \neq m)$ と偽れる

$$\Downarrow \text{ならば}$$

アリスは g を何乗したら v となるかという**離散対数**が求められる

離散対数問題を解くことは困難であるということに矛盾する

アリスは m をコミットした後で m' と偽ることは困難である

コイントスゲームの検証

封筒をどうやって実現する？

コイントスゲームの検証

封筒をどうやって実現する？

ボブは $g^r v^m$ から m を特定できる

$\downarrow$ しかし

コイントスゲームの検証

封筒をどうやって実現する？

ボブは $g^r v^m$ から m を特定できる

$\downarrow$ しかし

g, v は**生成元**である

$\Downarrow$ 従って

$g^r \bmod p$ は $1, \ldots, p-1$ の全ての値を取る

$\Downarrow$ つまり

コイントスゲームの検証

封筒をどうやって実現する？

ボブは $g^r v^m$ から m を特定できる

$\downarrow$ しかし

g, v は**生成元**である

$\Downarrow$ 従って

$g^r \bmod p$ は $1, \ldots, p-1$ の全ての値を取る

$\Downarrow$ つまり

全ての m' には $g^r v^m = g^{r'} v^{m'}$ となる r' が存在する

$\Downarrow$ つまり

コイントスゲームの検証

封筒をどうやって実現する？

ボブは $g^r v^m$ から m を特定できる

$\downarrow$ しかし

g, v は生成元である

$\Downarrow$ 従って

$g^r \bmod p$ は $1, \ldots, p-1$ の全ての値を取る

$\Downarrow$ つまり

全ての m' には $g^r v^m = g^{r'} v^{m'}$ となる r' が存在する

$\Downarrow$ つまり

ボブは正しい m を区別することができない

まとめ

まとめ

- Mental Jinro はゲームマスターを排除した人狼である

まとめ

- Mental Jinro はゲームマスターを排除した人狼である
- コミットメントを利用することで、コミットした情報を反故にしたり、コミットメントからコミットした情報を特定されることを防げる

まとめ

- Mental Jinro はゲームマスターを排除した人狼である
- コミットメントを利用することで、コミットした情報を反故にしたり、コミットメントからコミットした情報を特定されることを防げる
- Mental Jinro はこのコミットメントによって成り立っている

まとめ

- Mental Jinro はゲームマスターを排除した人狼である
- コミットメントを利用することで、コミットした情報を反故にしたり、コミットメントからコミットした情報を特定されることを防げる
- Mental Jinro はこのコミットメントによって成り立っている
- Mental Jinro の詳細は Qiita の記事を参照のこと

目次

参考文献

H. デルフス, H. クネーブル.
暗号と確率的アルゴリズム入門 — 数学理論と応用.
シュプリンガーフェアラーク東京, 12 2003.

光成滋生.
クラウドを支えるこれからの暗号技術.
秀和システム, 6 2015.

余談

このスライドはLuaLaTeXとBeamerにより作成され、Travis CIによる自動コンパイルが行われている

ソースコード
: https://github.com/y-yu/mental-jinro-slide

PDF（アニメーションあり）
: https://y-yu.github.io/mental-jinro-slide/mental_jinro.pdf

PDF（アニメーションなし）
: https://y-yu.github.io/mental-jinro-slide/mental_jinro_without_animation.pdf

Thank you for listening!
Any question?