

# 論文ゼミ

情報学科4年

G99p0283 岡部吉彦

# 題材

G98p054-5相良鉄兵氏の  
「電子入札方式における  
同点落札問題の一方方向性関数を用いた解決法」

# 封印式オークション

- 入札は一人一回のみ
- 入札値は、開札まで主催者によって秘密に保持される
- 開札時に一斉に入札値の集計を行い落札者を決定する

# 同点落札問題

- 複数の入札者が同じ価格を入札し、その価格が最高入札価格になった場合、落札者が数名存在する問題

# 解決法

- ・再度オークションを行う
  - しかし、効率性、個人情報漏洩などにより不適切
- ・「入札時刻」を設定し、一番早い入札者を最終落札者とする

# システム設定

- 入札者  $b_i$  ( $i = 1 \dots I$ )
- 入札価格幅  $V = \{v_1, v_2 \dots v_L\}$  ( $x = 1, 2 \dots L$ )
- 暗号関数族  $\{E_v\}$ 、復号関数族  $\{D_v\}$   $M_v$  の生成、公開
- 鍵の作成

- 入札者  $b$

- ID 暗号化の為の公開鍵  $p_b$ 、秘密鍵  $s_b$

- オークションサーバ  $a$

- ID 暗号化、入札時刻  $t$  の為の公開鍵  $p_a$ 、秘密鍵  $s_a$

# 手順1 (入札フェーズ)

1. 個人情報・入札情報の暗号化、入札
  - ・入札者  $b$  は、一方向性関数  $H$  を作成
  - ・入札者  $b$  は個人IDを暗号化する
    - $E_a(\text{ID})$  { オークションサーバ  $a$  の公開鍵  $p_a$  による暗号化 }
    - $E_b(\text{ID})$  { 入札者  $b$  の秘密鍵  $s_b$  による暗号化 }
  - ・入札価格を決定 ( $V_k$  とする)

# 手順2

- ・暗号化、付加

$$K_b = E_{v_k}(M_{v_k}) \parallel E_a(\text{ID}) \parallel E_b(\text{ID})$$

- ・一方向性Hash関数Hをかける

$$F_b = H [ E_{v_k}(M_{v_k}) \parallel E_a(\text{ID}) \parallel E_b(\text{ID}) ]$$

- ・オークションサーバに送信

# 手順3

## 2. 入札情報の受信、入札時刻 $t$ の通知

- ・オークションサーバ $a$ は、受諾時刻 $t$ を記録
- ・自身の秘密鍵で $t$ を暗号化

$$E_t(t)$$

- ・入札者に、受信時刻と受信情報を通知

$$N_a = E_t(t) \parallel H [ E_{v_k}(M_{v_k}) \parallel E_a(\text{ID}) \parallel E_b(\text{ID}) ]$$

# 手順4

## 3、 $t$ の確認、Hash関数、入札情報の送信

- ・入札者 $b$ は、公開鍵で時刻情報 $E_t(t)$ を復号化
- ・不正がないことを確認
- ・自らが生成した一方向性Hash関数 $H$ と  $K_b$ を送信

# 手順5

## 4. 入札情報の復号化

- ・オークションサーバは、ハッシュ化を行う

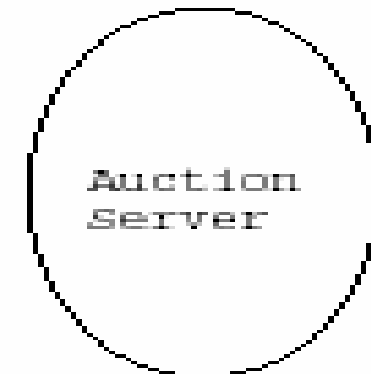
$$G_b = H [ E_{v_k}(M_{v_k}) \parallel E_a(\text{ID}) \parallel E_b(\text{ID}) ]$$

- ・  $G_b = F_b$  で正当性を確認
- ・ データ連結を外し、入札データとして受諾

$$E_{v_k}(M_{v_k}) \parallel E_a(\text{ID}) \parallel E_b(\text{ID}) \rightarrow E_{v_k}(M_{v_k}), E_a(\text{ID}), E_b(\text{ID})$$

# 手順6 (掲示板への書き込み)

```
27.Jan 15:30:40 E_a(ID)
27.Jan 15:33:54 E_a(ID)
.
.
.
.
.
27.Jan 16:05:22 E_a(ID)
27.Jan 16:21:34 E_a(ID)
```



## 手順7 (開札フェーズ)

- ・ 最大値  $v_L$  に対する  $D_{v_L}$  で  $E_{v_L}(M_v)$  を復号
- ・ 復号結果が予め決められた  $M_{v_L}$  に等しければ、 $v_L$  が落札値となる
- ・ そうでなければ、 $D_{v_L-1}$  で試み、一致するまで続ける
- ・ 同点落札が生じた場合は、一番早い人を最終落札者とする

# 今後の課題

- 同時刻、同価格の場合の落札者の決定
- 匿名性に対して、若干弱い