

暗号プロトコル

情報セキュリティ7, 8章
秘密分散, マルチパーティプロトコル

CONTENTS

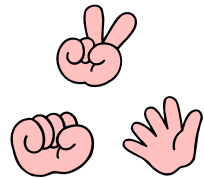
- 暗号プロトコル
- 秘密分散 (7.1)
 - 満場一致法
 - しきい値法
- マルチパーティプロトコル (7.2)
 - 電子投票 (8.3)
 - 足し算のマルチパーティプロトコル

暗号プロトコルとは？

- 基本機能
 - 互いに信頼できないプレイヤーが合意できる計算を実行すること
 - プレーヤーの行動を検証する技術(内部不正の防止)
- 例
 - 億万長者問題(A. Yao, 1982)
 - NSAランチ問題(D. Chaum, CACM, 1985)
 - 電子選挙・電子マネー・電子オークション
 - 匿名内部告発プロトコル(Rivest, Shamir & Tauman, 2000)

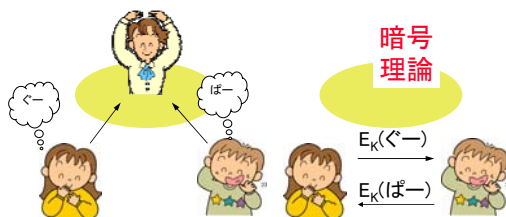
問題1. ネットでじゃんけん

- チャットで
 - A> じゃや〜んけん
 - B> ぼん!
 - A> ぐー
 - B> ぱー
 - B> じゃあ僕の勝ちだね!
 - A> (...)
- 問題点
 - 1. _____アタック (公平性)
 - 2. 判定を誰がどうやって (検証性)



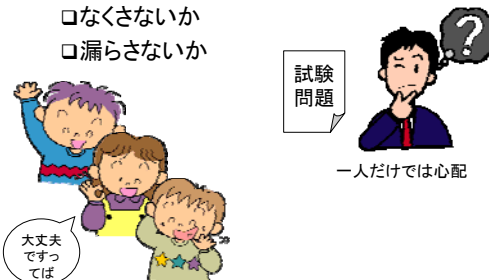
解決策

- 信頼できる第三者
_____(Trusted Third Party)
- 暗号プロトコル



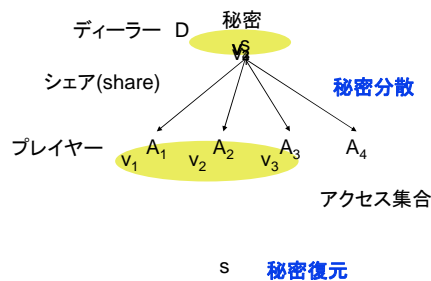
問題2. 試験問題の管理

- 試験問題をTAに渡しても大丈夫か？
 - なくさないか
 - 漏らさないか



法 (Secret Sharing Scheme)

■ 秘密を分散するプロトコル



満場一致法

■ 秘密復元に全員のシェアを要する

$$\square s = v_1 + v_2 + v_3 \pmod{p}$$

□例)

$$s = 7, p = 13$$

$$v_1 = 3, v_2 = 6 \quad (\text{ランダム})$$

$$v_3 = s - 3 - 6 = \quad (\text{mod } 13) \quad (\text{方程式})$$

法

■ シヤミアの(t,n)しきい値法

□ Shamir, A, "How to share a secret", CACM, Vol.22, No.11, pp.612-613, 1979

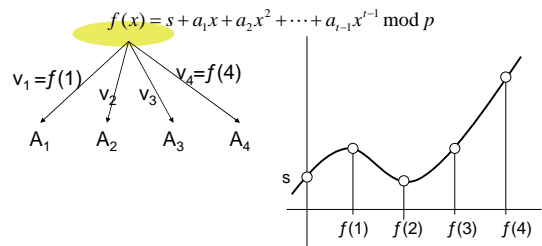
1. n人中のt人が集まると秘密sを復元できる
2. t-1人の集まりからはsについて全くわからない

■ 満場一致法

□ $n = t$ の場合

1. 秘密分散

D 秘密のt-1次多項式



2. 復元 (方程式の解き方1)

■ 連立方程式を代数的に解く

$$f(x) = s + ax + bx^2 \pmod{11}$$

$$f(1) = 0$$

$$f(2) = 1$$

$$f(3) = 6$$

■ 例

$$f(2) - 2f(1) = -s + 2b =$$

$$f(3) - 3f(1) = -2s + 6b =$$

$$+3s + -2s = -3 + 6 =$$

2. 復元 (方程式の解き方2)

■ (Lagrange)の補間法

$$f(x) = \sum_j \lambda_j(x) f(j)$$

$$\lambda_j(x) = \prod_{\ell \neq j} \frac{x - \ell}{j - \ell}$$

■ 例

$$f(0) = \sum_{j=1}^3 \lambda_j(0) f(j)$$

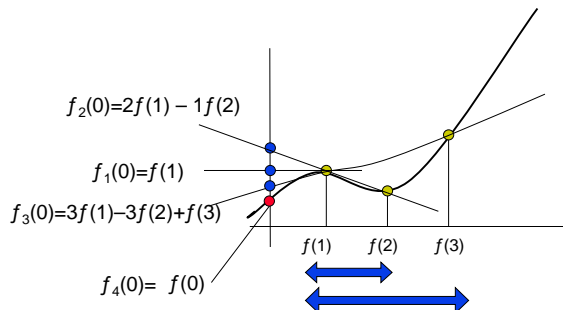
$$= \lambda_1(0) f(1) + \lambda_2(0) f(2) + \lambda_3(0) f(3)$$

$$= \frac{2}{2-1} \frac{3}{3-1} f(1) + f(2) + \frac{1}{1-3} \frac{2}{2-3} f(3)$$



http://etlab.mis.ous.ac.jp/info/sys_03/52/explain1.html

ラグランジェ補間法



問題3. 電子投票

- 2002年6月23日
岡山県新見市
 - 日本初の電子投票 (市長市議選挙)
 - 1万9千人有権者, 43投票所, 86%投票率
 - 開票時間25分 (不在者投票2時間)
 - 投票者の97%「投票しやすかった」



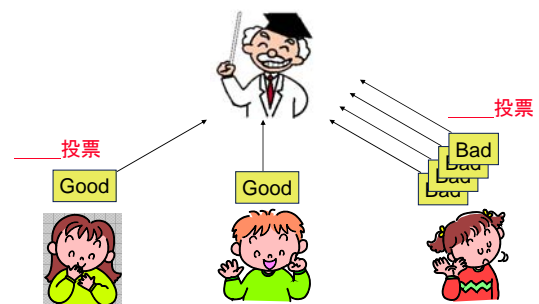
電磁記録的投票システム

<http://premium.nikkeibp.co.jp/biz/e-gov/>

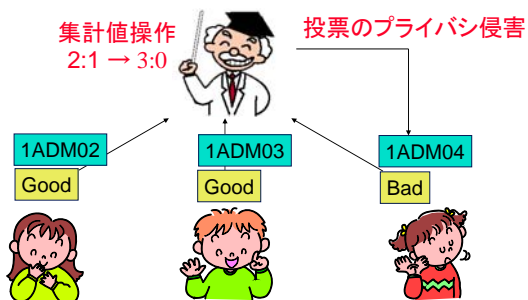
電子投票のメリット

- 開票の性
 - 人的計算ミスなし
- 即日開票
 - 迅速
- - 投票用紙印刷不要, 開票者数
- 投票者の利便性
 - 誤字脱字による無効票の削減
 - (体の不自由な人でも代筆が認められない)

悪い学生



悪い先生



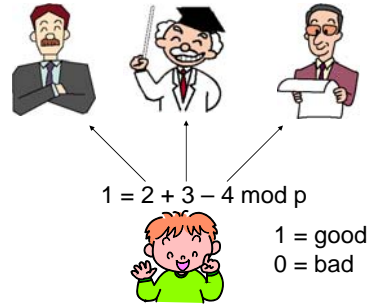
電子投票の問題点

- 投票者の不正
 - 投票
 - 投票用紙偽造
 - 集計者の不正
 - 投票用紙の改ざん, 水増し, 破棄
 - 性
- 先生一人だけでは信用できない.

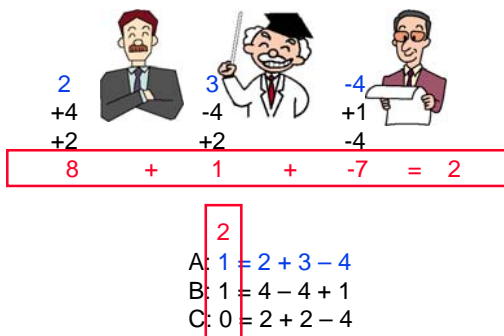
マルチパーティプロトコル

- 入力
 - プレイヤ A_1 , 秘密 s_1
 - プレイヤ A_2 , 秘密 s_2
 - プレイヤ A_3 , 秘密 s_3
- 出力
 - ある関数 $y = f(s_1, s_2, s_3)$ の計算
 - s_1, s_2, s_3 は秘密のまま
- f の例
 - 足し算: 選挙
 - 最大値: オークション (8.4節)
 - 署名: 分散署名 (7.2節2. RSA分散復号)

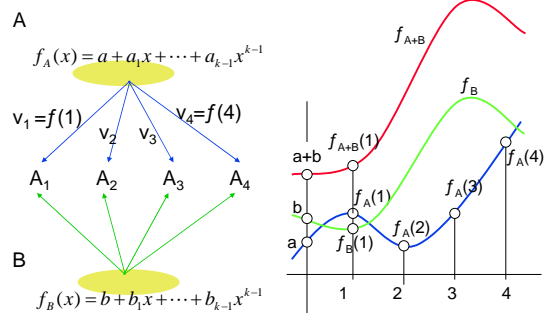
足し算プロトコル Step 1



足し算プロトコル Step 2



足し算のマルチパーティプロトコル



演習

- mod 11の上での二次の多項式 $f(x)$ がある。
 式の値が次の様に分かっているとき, 自分の学生番号から3つの数字を選び, ラグランジェ補間法により秘密を復元せよ. (例 1ADM1214ならば $f(1), f(2), f(4)$)

x	1	2	3	4	5	6	7	8	9	10
f(x)	1	1	7	8	4	6	3	6	4	8