I486S 演習問題 (BGW VSS)

Alice, Bob, Charlie, David, Eve, Flora, George の 7 人はマルチパーティ計算をして結果を共有したいと思っているが、この中に不正者（能動的攻撃者）が 2 人いる可能性がある。不正者に対しても安全なマルチパーティ計算をするため、BGW の VSS を使って、各自が Dealer 役になり、自分の秘密を全員の間で秘密分散した。幸いなことに最終的に全ての VSS プロトコルは受理されたが、各プロトコルの最中次のようなことが起きた。

- Bob が Dealer のとき、David と Flora の間で dispute が起きた。dispute を受けて Bob が broadcast した値に対して、David と Flore は両者とも Bob を accuse した。
- Charlie が Dealer のとき、Alice と David の間で dispute が起きた。dispute を受けて Charlie が broadcast した値に対して、Alice は Charlie を accuse した。
- David が Dealer のとき、Alice と Bob の間で dispute が起きた。dispute を受けて David が broadcast した値に対して、Bob は David を accuse した。

問題 1　最大 2 人信用出来ない人物がいるので、BGW VSS の二変数対称多項式の X,Y の次数（$\deg_X(F) = \deg_Y(F)$) は幾つに設定すべきか。

問題 2　全ての VSS プロトコル実行の結果、不正者の可能性がある人物の集合を全部書き下せ。ただし、正直な参加者は計算間違いをしないと仮定して良く、不正者は 2 人以下である。

次のステップで、再び各参加者のローカルなシェアの秘密分散を BGW の VSS で行った。Flora が Dealer のとき、Charlie と George の間で dispute が起こった。Flore が値を broadcast した後、Charlie も George も Flore を accuse せず、VSS プロトコルは受理され終了した。

問題 3　　不正者は誰か。

問題 4　不正者の数を 2 人以下と特定しない場合、不正者の可能性のある集合は？ただし、上記の行動の中で不正行為を働かなかった参加者は不正者に数えない。VSS は不正者 2 人と想定して実行されたとする。