I486S 演習問題 (CMP プロトコル)

- Commitment Multiplication Protocol (CMP) は、Dealer D が、秘密 a, b を、$[a]_D$, $[b]_D$, $[c]_D$ と秘密分散したあと、$c = ab$ であると参加者に証明するプロトコル。
- 一般の $[[a]]_\emptyset = ([a_1]_1, \ldots, [a_n]_n)$, $[[b]]_\emptyset = ([b_1]_1, \ldots, [b_n]_n)$ の状態から、$[ab] = \sum \lambda_{i,n}[a_i b_i]$ の状態に正しく秘密分散するためのサッププロトコルとして必要。
- 各秘密分散プロトコル $P_i : a \to [a]_D$ と復元プロトコル $P_i : a \leftarrow [a]$ は実際は VSS や誤り訂正符号を使って強制的に正しく行わせる。

以下、秘密分散は有限体 $\mathbb{F}_7$ の上で行われる。

$$\lambda_{i,n} = \prod_{j \neq i}^{1 \leq j \leq n} \frac{j}{j-i}.$$

$\lambda_{1,4} = 4$, $\lambda_{2,4} = 1$, $\lambda_{3,4} = 4$, $\lambda_{4,4} = 6$.

$t = 1, n = 4$ とする。$[a] = (0, 4, 1, 5)$ としこの秘密分散に使った多項式を $f(X) = a + f_1 X$ とする。$[b] = (5, 1, 4, 0)$ としこの秘密分散に使った多項式を $g(X) = b + g_1 X$ とする。$[c] = (2, 5, 1, 4)$ である。

1. D は、$h(X) = f(X)g(X) = c + h_1 X + h_2 X^2$ を計算する。
2. D は、$f_1 \to [f_1] = (6, 1, 3, 5)$, $g_1 \to [g_1] = (1, 6, 4, 2)$, $f_1 \to [f_1] = (6, 1, 3, 5)$, $h_1 \to [h_1] = (2, 1, 0, 6)$, $h_2 \to [h_2] = (1, 4, 0, 3)$ を実行する。
3. 参加者は、協力して $P_i : f(i) \leftarrow [f(i)] = [a] + i[f_1]$, $P_i : g(i) \leftarrow [g(i)] = [b] + i[g_1]$, $P_i : h(i) \leftarrow [h(i)] = [c] + i[h_1] + i^2[h_2]$ を実行する。
4. 各 P_i は、$h(i) = f(i)g(i)$ が成立するか検証する（成立しない場合は D を accuse）。
5. accuse 数が t 以下ならプロトコルを受理する。

問題 1　各 $f(i), g(i), h(i)$ を求め、$f(i) = g(i)h(i)$ が成立するか検証せよ。

問題 2　a, b, c の値を求めよ。