# 第七周區塊鏈課程筆記

姓名：胡樂麒　學號：B1228005

2025 年 12 月 3 日

## 1 HW1 解釋離散對數問題 (Discrete Logarithm Problem, DLP)

設 $G$ 一個有限循環群（cyclic group），生成元 $g$，群的階 $n$。**離散對數問題**是指給定 $g$ 與 $h \in G$，求出整數 $x$ 使得：

$$h = g^x.$$

若能找到關系式 $g^a h^b = 1_G$，則可得：

$$x = -a/b \pmod{n}.$$

### 1.1 Pollard's Rho 方法

Pollard 的 rho 方法是一種利用「碰撞 (collision)」來求解 DLP 的演算法。它透過定義一個接近隨機的函數 $f : G \to G$，反覆計算：

$$x_{i+1} = f(x_i),$$

直到出現重復（即碰撞）就停止。

定義函數：

$$f(x) = \begin{cases} hx & \text{若} x \in S_1, \\ x^2 & \text{若} x \in S_2, \\ gx & \text{若} x \in S_3. \end{cases}$$

若 $x_i = g^{a_i} h^{b_i}$，當出現碰撞 $x_{i_1} = x_{i_2}$ 時：

$$g^{a_1 - a_2} h^{b_1 - b_2} = 1_G,$$

即可解出 $x$。

### 1.2 偵測碰撞的方法

- **土法煉鋼：**將所有可能列表。
- **Naive：**儲存所有已出現的元素，記憶體需求高。
- **Floyd 龜兔算法：**使用「慢指標與快指標」trace 循環，節省記憶體。
- **Distinguished Points：**僅記特定條件的元素，方便平行化計算。

**範例：** 設 $G = (\mathbb{Z}/101\mathbb{Z})^\times$, $g = 2$, $h = 3$。

定義:

$$S_1 = \{x : x \equiv 1 \pmod 3\}, \quad S_2 = \{x : x \equiv 2 \pmod 3\}, \quad S_3 = \{x : x \equiv 0 \pmod 3\}.$$

根據 $f(x)$ 不斷迭代，直到出現碰撞，即可求得 DLP 解。

## 2 互動式證明與零知識證明 (ZKP)

在 **互動式證明系統 (Interactive Proof)** 中，有兩方:

$$P \leftrightarrow V$$

其中 $P$ 設「證明者 (Prover)」，$V$ 則是「驗證者 (Verifier)」。證明者希望證明驗證者某件事是真的，但不走漏任何秘密給 V。

### 2.1 零知識證明的三個性質

1. **完整性 (Completeness)：**若命題真，誠實的驗證者必定接受。
2. **可靠性 (Soundness)：**若命題假，欺騙的證明者無法使驗證者信服。
3. **零知識性 (Zero-Knowledge)：**驗證者不會學到任何額外資訊。

**例子:用粉筆色調檢測色盲** 老師以「徵兵確認色盲」當作例子,解釋 **non-transferability**。但是這個證明只有對證明者有用，P 跟 V 有可能事先講好，所以這個證明只對 V 有效色盲者讓對方信服分辨粉筆色彩，但無法向第三方證明這一點。這正是 ZKP 的特性:只能讓特定的驗證者認同。

—

# 3 Schnorr 的零知識證明 (ZKP) 用於 DLP

給定:

$$g \in G, \quad y = g^x, \quad \text{其中} x \text{ 秘密值。}$$

目標: 證明自己知道 $x$，但不泄漏 $x$ 的值。

## 3.1 協定步驟 (Protocol Steps)

1. **承諾 (Commitment):** 證明者 $P$ 選擇隨機 $k \in \mathbb{Z}_n$，計算:

$$r = g^k,$$

傳給驗證者 $V$。

2. **挑戰 (Challenge):** 驗證者選擇隨機 $e$，傳給 $P$。

3. **回應 (Response):** $P$ 計算:

$$s = k + xe \pmod{n},$$

回傳 $s$。

## 3.2 驗證步驟

驗證者檢查:

$$ry^e \stackrel{?}{=} g^s y^{-e}.$$

**證明:**

$$g^s y^{-e} = g^{k+xe} g^{-xe} = g^k$$

若成立，則驗證者確信 $P$ 了解 $x$，但無法得知其實際值。

## 3.3 Simulation

$$s \leftarrow \mathbb{Z}_n, \quad e \leftarrow \mathbb{Z}_n, \quad r = g^s y^{-e}.$$

—

# 4 課程總結

- **Pollard' s Rho 方法:** 用碰撞求解 DLP 的經典演算法。
- **零知識證明:** 讓驗證者相信命題真，但不透漏秘密。
- **Schnorr ZKP:** 對 DLP 的高效率互動式零知識證明。