|  |
| --- |
|  |
| **Zero-Knowledge Proof：以 Schnorr Protocol 為核心的可驗證身份驗證系統** |
| 課程名稱：密碼學  系所：電機工程研究所  組別：資訊安全組  組員：r13921a13 林伯叡  d13921c02黃杬霆 |

****

**目錄**

[**前言** 1](#_Toc197954916)

[**一、** **專題背景與動機** 2](#_Toc197954917)

[**二、** **專題目標** 3](#_Toc197954918)

[**三、** **系統設計** 4](#_Toc197954919)

[**四、** **專題成果** 5](#_Toc197954920)

[**五、** **結論** 6](#_Toc197954921)

[**六、** **未來展望** 7](#_Toc197954922)

[**七、** **參考文獻** 8](#_Toc197954923)

[**八、** **○○○ (此處為各標題供複製使用，最後報告完成要刪除)** 9](#_Toc197954924)

[**(一)** **○○○** 9](#_Toc197954925)

**前言**

○○○：

* ○○○**：**○○○○

1. **背景介紹與動機說明**
2. **背景介紹**

在早期的驗證系統中欲達成登入驗證，通常只能透過使用端直接揭露部分或全部資訊來讓目標端驗證，例如：輸入密碼、提交文件、或洩露原始資料…等方式，雖能達到驗證目的，但容易造成機密洩漏、重放攻擊，或讓未經授權的第三方竊取重要資訊。在高度依賴網路傳輸與重視資訊安全的現代，這類型作法已難以滿足對安全性及隱私性的雙重需求。為了解決這些問題，密碼學家 Shafi Goldwasser、Silvio Micali 與 Charles Rackoff 在 1985 年提出了**零知識證明**（**Zero-Knowledge Proof**， **ZKP**）的概念 [1]。他們設計了一種互動式的證明方法，讓「證明者」能在不揭露秘密本身的情況下，說服「驗證者」其確實知道某個秘密。這項技術徹底顛覆了傳統「揭露才能驗證」的模式，為密碼學、身分驗證與區塊鏈等未來領域帶來了全新的解決方案，以下為相關數學理論基礎及基本性質：

* + - 1. 數學理論基礎：
    1. 選用的難題：採數學上難解的問題—**離散對數問題**（**Discrete Logarithm Problem**，**DLP**）作為整個方法的核心基礎，駭客若想入侵則必須破解該議題。
    2. 數學背景：在一個有限域中 ，給定一個生成元（generator） 及任意元素 ，欲找到一個，使得：，則稱為相對於 的離散對數**（）**。
       1. 基本性質：

1. **可靠性**（**Soundness**）：若陳述為假，不存在一個可證明策略，使證明者（Prover）說服驗證者（Verifier）相信。

例如：假設有人提出證明：「1 + 1 = 3」，證明系統應要求這種錯誤的證明不該存在。

1. **完整性**（**Completeness**）：若陳述為真，證明者（Prover）應該能找到一個可證明策略使驗證者（Verifier）相信。

例如：如果「1 + 1 = 2」是真的，那證明系統應該可以證明，而非找不到證明。

1. **零知識性**（**Zero-Knowledge**）：證明者（Prover）欲向驗證者（Verifier）證明知道「秘密（Security）」，必須在不直接揭露該秘密的情況下，僅能透過一些「陳述（Statement）」的交換，讓驗證者相信其知道該秘密，例如：證明者可以向驗證者證明自己知道密碼，而不需要直接告訴驗證者密碼。
2. **動機說明**

依據前述傳統驗證機制（無論是密碼式或生物特徵式）普遍仰賴資訊的直接揭露，導致使用者在追求安全驗證的同時，卻又必須承擔機密洩漏、重放攻擊、甚至嚴重的隱私外洩風險…等，此外，ZKP所提供的「不揭露秘密亦能驗證」，正好回應了當今資訊安全與隱私保護的雙重需求。本專題正是基於這樣的基礎，進一步探究 ZKP 的相關原理及成效。

1. **專題目標**

本專題旨在循序探討ZKP技術的發展脈絡，從基本架構出發，逐步導入實作效率與交互性的改善技術，藉由改善互動傳輸成本，最終達成兼顧安全性與可實用性的「非互動式驗證機制」，目標分為以下三階段：

1. **傳統ZKP（互動式驗證機制）**

初期的零知識證明為互動式機制，由證明者與驗證者透過多次隨機挑戰與回應的方式達成驗證。在理論上這種架構能確保完整性、可靠性與零知識性；然而，在實務應用上此類 ZKP 通常需多輪互動、傳輸成本高，不利於一對多、非同步或網路不穩定的環境中。為解決該問題，本專題進一步探討如何降低相關傳輸所造成的不穩定。

1. **Schnorr Protocol（簡化版互動式驗證機制）[2]**

Schnorr在結構上延續傳統互動式 ZKP 的安全性設計，但引入更簡潔的數學結構：**承諾（commit）**、**挑戰（challenge）**及**回應（response）**，大幅降低計算與通訊成本，並具有實作上的簡便性，並使其成為多種密碼學應用（如電子簽章）中的基礎原型。然而，Schnorr 協定仍屬於互動式協定，需證明者與驗證者同時在線互動，這在分散式系統或無法同步傳輸的場景中仍有侷限。因此，我們接續探討如何將其轉化為非互動式形式。

1. **Fiat–Shamir Heuristic（非互動式驗證機制）[3]**

Fiat–Shamir 方法利用 hash 函數將互動式協定中的隨機挑戰值，改為由證明者本地端自行計算產生，實現 ZKP 的「非互動化」。它將原本需由驗證者提出的挑戰，改為自行產生 **hash** 值： ，消除雙方互動需求。

上述變更成功解決 Schnorr 協定的互動性限制，使得零知識證明可應用於區塊鏈（需支援**非互動式證明**的去中心化架構）、電子身份（如一次性提交的**非互動式驗證**流程）、無人監督驗證等場景，這些應用場域皆對**非互動性有高度依賴**，因此Fiat–Shamir 方法成為現代 ZKP 實作中的關鍵技術。

1. **系統設計**
2. **傳統ZKP**
3. **Schnorr Protocol**

屬於**簡化版互動式零知識證明**，以**離散對數之難度**作為核心，***Prover*** 知道一個秘密私鑰，計算，並提供 ***Verifier*** 公鑰，***Prover*** 欲在不透漏的情況下，讓 ***Verifier*** 相信其知道秘密 ，以下為參數設定：

質數**：**：隨機挑選的大質數

：

生成元（）**：**

私鑰**： （隨機挑選）**

公鑰**：**

* + - 1. **承諾（commit）：**

1. ***Prover*** 隨機選擇一個 ephemeral key ，使得
2. 計算承諾值 ： 。
3. 傳送 給 ***verifier***。
   * + 1. **挑戰（Challenge）：**
4. Verifier 產生一個隨機的挑戰值 ，使得
5. 傳送 給 Prover。
   * + 1. **回應（Response）：**
6. Prover 計算： 。
7. 傳送 給 Verifier。
8. Verifier 驗證：

（成立 → 接受；不成立 → 拒絕）

1. **Fiat–Shamir Heuristic**
2. **專題成果**
3. **結論**
4. **未來展望**
5. **參考文獻**
6. Goldwasser, S., Micali, S., & Rackoff, C. (1985). The knowledge complexity of interactive proof-systems. *SIAM Journal on Computing*, *18*(1), 186–208. https://doi.org/10.1137/0218012
7. Schnorr, C. P. (1990). Efficient identification and signatures for smart cards. In G. Brassard (Ed.), Advances in Cryptology – CRYPTO ’89 (Lecture Notes in Computer Science, Vol. 435, pp. 239–252). Springer. https://doi.org/10.1007/0-387-34805-0\_21
8. Fiat, A., & Shamir, A. (1987). How to prove yourself: Practical solutions to identification and signature problems. In A. M. Odlyzko (Ed.), Advances in Cryptology – CRYPTO ’86 (Lecture Notes in Computer Science, Vol. 263, pp. 186–194). Springer. https://doi.org/10.1007/3-540-47721-7\_12
9. **○○○ (此處為各標題供複製使用，最後報告完成要刪除)**
10. **○○○**
    * + 1. ○○○：
11. ○○○：
    * 1. ○○○：

○○○：

○○○：