總和驗證協議的運算與展現

專題編號：114-2-CSIE-S004
執行期限：114 年第 1 學期至 114 年第 2 學期
指導教授：陳昱圻
專題參與人員： 112820019 林哲丞
112820030 陳昱霖
112820032 何昕哲

摘要

針對雲端委託運算中算力不對等與隱私外洩的挑戰，本計畫實作並視覺化「零知識 GKR (ZK-GKR)」協議，以實現低成本且保護隱私的可驗證運算。本系統後端採用 C# 結合 mcl 函式庫，由底層建構算術電路、總和驗證協議與 KZG 多項式承諾等密碼學核心；前端以 Vue.js 3 打造互動式介面。透過將協議執行過程封裝為結構化事件流，本研究成功將複雜的底層數學運算與多輪通訊，轉化為直觀的動態電路圖與步驟指引。研究成果不僅驗證了 ZK-GKR 在資源受限場景下的實務可行性，更大幅降低該協議的學習與除錯門檻，未來具備推動去中心化技術(Web3)與零知識機器學習(zkML)等前沿領域應用的極大潛力。

關鍵詞：零知識證明、GKR 協議、可驗證運算、多項式承諾、互動式視覺化

緣由與目的

如今，將龐大的資料處理與模型推論外包給第三方伺服器已是常態。然而，這衍生出了嚴重的安全與信任問題。當運算能力極度不對等時，資源受限的終端設備該如何確認第三方回傳的運算結果是正確的？並且，如何在確認的過程中確保不外洩額外的隱私資料給第三方？基於上述挑戰，本計畫旨在實作並展示「ZK-GKR」協議。GKR 能讓終端設備以極低的運算成本驗證龐大的計算結果，結合零知識證明技術，確保驗證過程中的資料機密性。期望透過具體的展示，驗證 ZK-GKR 在解決算力不對等與隱私保護問題上的可行性與優勢。

相關技術背景與研究方法

一、GKR 協議概述

GKR 是由 Goldwasser、Kalai 與 Rothblum 於 2008 年提出的一種 Interactive Proof System [1]。其核心目標在於解決 Delegating Computation 中的信任問題，計算能力有限的 Verifier 將龐大的計算外包給運算力強大但不可信的 Prover，確保 Verifier 能以極低的運算成本驗證計算結果的正確性。在技術實作上，GKR 協議將計算過程化為 DAG 的算術電路。協議執行時，會透過 Sum-Check[2]，將電路從輸出層逐層遞迴至輸入層，將前一層的正確性聲明轉化為對下一層的聲明。隨著零知識證明技術的發展，現代的 GKR 變體（如 Libra 等協議 [3]）進一步透過多項式承諾 (Polynomial Commitments) [4] 確保安全性與資料的防篡改性。

二、研究方法與系統架構

為了將上述的密碼學理論具象化並驗證可行性，本計畫採用「理論實作化」與「互動視覺化」雙軌並行，具體分為以下三個核心階段：

（一）密碼學演算法實作

本計畫於後端使用 C# 語言，並整合高效能的 BLS12-381 雙線性配對密。

（二）前後端通訊架構設計

為呈現互動式證明的多輪通訊特性，系統採用 ASP.NET Core Web API 作為後端架構，將密碼學協議的執行過程封裝為結構化 JSON 事件流 (Event Stream)。前端採用 Vue.js 3 框架，搭配響應式狀態管理，協議執行密碼學函式庫 mcl［5］，由底層建構 GKR 的核心元件。模組包含：

1. 算術電路(Arithmetic Circuit)：

建構 DAG 電路結構，實作多線性擴展 (MLE) 與電路的求值邏輯。

2. 總和驗證協議(Sum-Check Protocol)：
依據 Lund 等人提出的代數方法［2］，模擬 Prover 與 Verifier 之間的多輪互動，執行隨機挑戰(Random Challenge)與多項式求值。

3. 多項式承諾(KZG Commitment)：

實作 Multilinear KZG［4］，透過可信設置生成 Structured Reference String 進行承諾計算，確保每一輪具備零知識與輸入層資料的防篡改特性、訊息傳遞與變數狀態，即時轉譯為對應 UI 元件，實現前後端高度解耦與資料同步。

（三）互動視覺化與防呆機制

本專題設計專屬的電路視覺化與互動對話框，將複雜的運算過程，轉化為直觀易懂的步驟。此外，為提升系統穩定性，後端層面導入了「電路結構檢查」與「資料校驗機制」，有效防止使用者輸入非法的電路結構而導致協議執行中斷，完善整體的系統體驗。

成果與討論

本系統成功實作了具備 KZG 承諾的 GKR 協議，驗證了在算力與資源不對等場景下，證明者 (Prover) 能夠產生正確的證明，而驗證者 (Verifier) 可透過協議有效確認運算結果的正確性，證實了本專題在密碼學實務上的可行性。本專題的核心價值在於產出一套直觀的視覺化工具，將晦澀的密碼學過程用電路圖的動態顯示參與運算的電路閘門 (Gate)，降低 GKR 協議的學習門檻。。並將 Prover 與 Verifier 之間巨大的數值傳遞，轉化為可按步驟點擊的對話氣泡，大幅降低了理解門檻。

參考文獻 (Reference)

[1] S. Goldwasser, Y. T. Kalai, and G. N. Rothblum, "Delegating computation: Interactive proofs for muggles," in *Proc. 40th Annu. ACM Symp. Theory Comput. (STOC)*, 2008, pp. 113–122.

[2] C. Lund, L. Fortnow, H. Karloff, and N. Nisan, "Algebraic methods for interactive proof systems," *Journal of the ACM (JACM)*, vol. 39, no. 4, pp. 859–868, Oct. 1992.

[3] T. Xie, J. Zhang, Y. Zhang, C. Papamanthou, and D. Song, "Libra: Succinct zero-knowledge proofs with optimal prover computation," in *Adv. Cryptology – CRYPTO 2019*, 2019, pp. 733–764.

[4] S. Lanlege, "Polynomial commitments," Polytope Research, 2023.[Online]. Available: https://research.polytope.technology/polynomial-commitments/?utm_source=chatgpt.com

[5] S. Mitsunari, "mcl: A portable and fast pairing-based cryptography library," GitHub repository, 2024. [Online]. Available: https://github.com/herumi/mcl