電路標準化運用於零知識證明決策樹模型中之實作與實用性研究

專題編號:114-1-CSIE-S023
執行期限:113年第1學期至114年第1學期
指導教授:陳昱圻
專題參與人員: 111820001 賴文琪
111820009 范姜芷妤
111820019 黃子臻

一、摘要

零知識證明 (ZKP) 是一種密碼學技術，允許證明者在不洩漏輸入或中間過程的情況下，向驗證者證明某項運算已正確執行。本專題聚焦於 ZKP 在決策樹模型推論驗證中的應用，旨在透過電路標準化（Constraint Normalization）技術來優化其運算效能。

在 ZKP 系統中，計算會被轉換為 R1CS (Rank-1 Constraint System) 約束，其數量直接影響證明生成與驗證的效率。我們利用 Circom 撰寫決策樹邏輯，並設計腳本將多變數電路自動轉換為單變數形式，以探討此方法是否能有效減少 R1CS 約束。最終，簡化後的電路使用 SnarkJS 搭配高效的 Groth16 協議完成 ZKP 的生成與驗證。

關鍵詞:零知識證明、Circom、SnarkJS、Groth16 協議、約束正規化

二、緣由與目的

隨著資料驅動應用的興起，隱私與安全需求日益提升。零知識證明（ZKP）生成與驗證證明更為耗時。

決策樹結構清楚但具分支複雜性，是 ZKP 應用效能測試的良好起點。但傳統上將決策樹轉換為 ZKP 電路的做法，因包含大量的比較與布林邏輯，會產生大量冗餘約束，造成約束系統（R1CS）電路標準化（Constraint Normalization）一致化的約束結構。此方法理論上能有效減少約束條件，透過提升編譯器（如高斯消去）的優化效果，從而降低 ZKP 的計算負擔並維持運算正確性。

三、研究範圍

本研究聚焦於零知識證明（ZKP）技術，旨在證明使用者可依據決策樹模型完成推論運算過程，保障結果來源正確、無法偽造，並保護使用者輸入數據的隱私。核心探討電路標準化（Constraint Normalization）減少 R1CS 約束數量，從而降低 ZKP 的計算負擔。為進行系統化評估，我們選用 Wine、Olivetti Faces、Breast Cancer 與 Digits 等多個具有代表性的資料集進行模型訓練與測試，並以 Groth16 協議與 Circom 工具為主要開發平台。研究範圍涵蓋:決策樹模型訓練與規則提取、ZKP 電路設計與簡化、證明生成與驗證流程，以及標準化前後的電路效能比較。

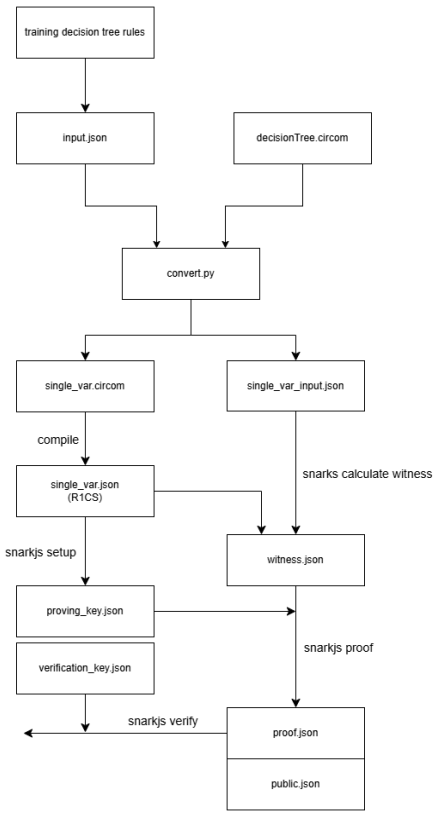
四、使用技術方法

本研究使用 Circom 作為零知識電路設計工具，撰寫決策樹邏輯的電路模板，定義節點的閾值比較與路徑決策規則。為降低電路複雜度，我們設計 Python 腳本進行標準化，將多變數輸入簡化為單變數結構，以減少電路中的約束數量，進一

步優化後續計算效能。

在證明協定方面，採用效率優異的 Groth16，並搭配 SnarkJS 套件完成電路的 witness 計算、參數初始化、證明生成與驗證等工作流程。SnarkJS 支援 Circom 產出的 R1CS 與 .wasm 檔案，並能處理 proof.json 與 public.json 等中介資料，實現完整的 ZKP 驗證流程。

五、架構流程



1.資料選定與模型訓練

本專題採用 Wine、Olivetti Faces、Breast Cancer 與 Digits 等多個公開資料集進行模型訓練。透過 PyTorch 訓練建立決策樹模型，將模型結構化為規則檔案，整合成包含節點閾值、邏輯條件與預測結果的 input.json。

2.決策樹電路建構與簡化

使用 Circom 編寫決策樹電路模板，模擬節點比較與路徑選擇機制。為提升電路效率，設計 convert.py 腳本，將多變數電路轉換為單變數版本（即套用約束標準化），以降低電路複雜度。最終產出簡化版電路 single_var.circom 及對應輸入檔案。

3.編譯電路與生成證明

使用 Circom 編譯簡化後的電路，得到 R1CS 約束系統及必要的輔助檔案（如 .wasm）。接著使用 SnarkJS 計算 witness，並採用 Groth16 協議依序執行三個步驟：Setup 階段產出證明與驗證金鑰，Prove 階段使用 witness 與 proving key 生成 ZKP 證明，最後於 Verify 階段使用 verifying key 驗證該證明，確認推論正確且無洩漏任何資訊。

六、實驗結果

經由對多變數邏輯電路進行標準化處理後，雖然在一般電路架構中可觀察到一定程度的優化效果，然而在應用於決策樹結構的電路時，其所對應的 R1CS 約束數量反而有略為增加的情形。進一步分析後發現，此效能下降的主因來自於 Circom 中之比較邏輯需依賴位元分解（bit decomposition）進行實作。由於位元分解後所引入的位元層級約束無法被原始數值層級的約束所取代，導致整體約束數量上升，進而影響電路效能，未如預期地達成優化效果。

七、結論

據實驗結果，本研究雖提出以電路標準化簡化決策樹在 ZKP 中的表示方式，然而實測顯示該方法在決策樹電路上未如預期有效減少 R1CS 約束。主因在於 Circom 的比較邏輯需依賴位元分解，使得標準化後引入的位元層級約束無法以原始數值約束取代，因此是否採用標準化仍須依據電路類型進行判斷。

八、參考文獻

[1] 曾竣羿 (2024). 基於參數向量的快速 R1CS 標準化方法. 國立台灣科技大學資訊工程系碩士學位論文.