

Hardware acceleration in RandomX algorithm of Monero: A feasibility study

門羅幣的RandomX演算法硬體加速可行性評估

組別：A26 指導教授：黃之浩 組員：廖宏儒、李旻珊

I. Abstract

加密貨幣是指利用區塊鏈技術，依靠礦工使用礦機尋找nonce以完整hash做交易運算的系統，本專題主題為近年熱門的加密貨幣演算法RandomX。使用RandomX的門羅幣具有獨特的隱私技術，我們從門羅幣學習加密貨幣挖礦流程和四大項隱私技術的實作原理。研究RandomX演算法後我們嘗試加速RandomX的運行速度，分為先找尋程式中可優化的函數和嘗試用可程式邏輯陣列(FPGA)加速，並從上述結果分別分析從軟體或硬體加速RandomX的可行性。

II. Monero

加密貨幣挖礦流程

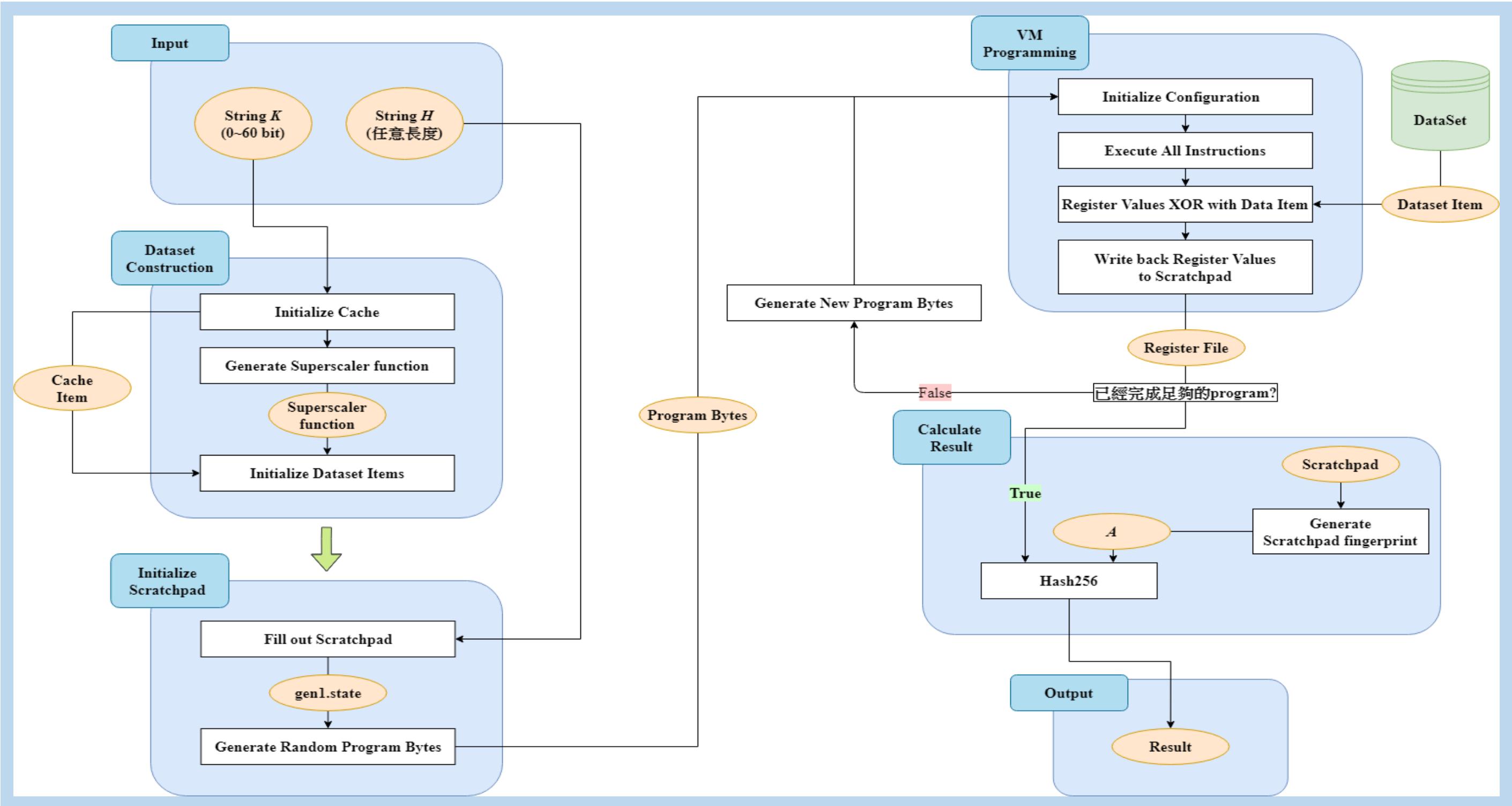
加密貨幣的交易要求放置於記憶池中，完整的block包含一組未完成的交易資訊、Hash、nonce，挖礦競爭即是比誰能最快找到完整block的nonce，完成的block才能嵌入最長的區塊鏈中(完成交易)，礦工能得到挖礦獎勵。而Monero另具備抗ASIC機制，避免用客製的礦機加入競爭，以專門機器和龐大記憶體優勢壟斷貨幣、破壞市場。

門羅幣隱私技術

- 1.RingCT — 藉由commitment(交易人私下提交金額)和range proof(檢驗提交金額是否合理)機制隱藏交易數額。
- 2.Ring Signatures — 將區塊鏈上不同支出的金鑰混雜，簽名中同時有本人的公開、私密金鑰和他人的公開金鑰，以隱藏交易人身分，但是會保留用來驗證本人身分的key image。
- 3.Stealth Address — 在公開地址加上隨機數據以保證每次交易都使用唯一的一次性地址。需要以私密金鑰進行運算後比對區塊鏈上的交易紀錄才能知道交易屬於誰。
- 4.Kovri — 在交易紀錄和交易人IP位址間創造隱密網路以切斷其聯繫。

III. RandomX Algorithm

RandomX是個proof of work (PoW) 演算法，目的在於盡可能消除CPU和專用硬體間的差距，而其核心就在於它模擬出一個虛擬CPU(Virtual Machine)，並藉由資料的依存性、隨機性和大量對資料的隨機操作，讓它難以被實作出專用的加速器來平行加速。RandomX的流程主要可以分為—Dataset Construction, Initialize Scratchpad, VM Programming, Calculate Result四個block。



圖一、RandomX流程圖

- 1.RandomX接受輸入值後由K進入Dataset Construction中生成資料集、H進入Initialize Scratchpad生成隨機程序的資訊。
- 2.每個隨機程序都有自己的初始值和指令，VM Programming會從中取得VM的配置，並在每完成一個程序後就與資料集中的特定項目進行XOR，並寫進Scratchpad。
- 3.在完成所有的隨機程序後，Calculate Result會將最後的Register值與Scratchpad fingerprint組合，組合結果通過Hash256就可得到最終輸出值。

IV. Optimization & FPGA

首先試著從軟體上優化，經過測速分析後聚焦在尋找耗時最久的Cache Initilization、運算Hash部份可加速的地方：但是RandomX中的迴圈幾乎都不獨立，無法改成平行運算。唯二獨立的迴圈第一個本身耗時極短，優化無法產生效果；第二個開發者已使用平行加速了，故我們認為從軟體上加速不可行。接著進行在FPGA上運行FPGA的研究。考量RandomX運算中需要大量記憶體存取資料，我們使用能支援64GB RAM FPGA 礦機 TPS-1525。我們選擇從RandomX中常使用的function—blake2b轉換。參考UART規格寫出UART介面後，將變數改變時間和改變值紀錄後另寫出always block來更新變數，並寫一個Finite State Machine的always block紀錄即時state位置。不過因為還無法正常在FPGA上運行，尚未能得知用硬體加速RandomX的效果。

V. Future

本次專題的評估結果，我們得出了從軟體上無法優化的結論，也側面驗證了RandomX本身資料的依存性。硬體方面，雖然還不能驗證RandomX本身，但是從將範例程式由C++轉為Verilog的成功經驗，我們認為若能在未來逐一排查錯誤，在FPGA上運行RandomX加速應是可行的。希望能在完成blake2b後，進一步檢測其他函式在FPGA上的加速成效。