Ravencoin 及其核心 X16R 硬體加速可行性評估

Hardware acceleration in Ravencoin and its core X16R algorithm: A feasibility study

組員：潘逸軒、林宗暐

指導教授：黃之浩

Abstract

Ravencoin is one of open-source cryptocurrencies with X16R as its key algorithm. Ravencoin is well known as conducting irregular hard-fork to strengthen its anti-ASIC capability in terms of preventing hardware acceleration. With this merit, the price of Ravencoin has drastically soared in the first half of 2019, in which Ravencoin represents a great future potential in continuous development. Ravencoin adopts PoW, and consequently, individual hash rate will have a decisive impact on miners' long-term remuneration. In this research, both Ravencoin's computing efficiency and feasibility of hardware acceleration will be evaluated through analyzing Ravencoin process and X16Rv2 algorithm.

In this studies, the first conclusion is the difficulty in hardware implementation due to several factors, including Ravencoin's highly complicated main program, largely usage of high-level language with portion of functions incomplete. Secondly, there are several relatively slow algorithms under current speed tests and those could be potentially accelerated based on current studies. X16Rv2 algorithm is found to be feasible in speeding up either by adopting parallel programing or instruction pipeline. Therefore, Ravencoin could be hardware accelerated by incorporating computer and FPGA; the former is responsible for main program while the latter is designated for X16R computing.

Introduction

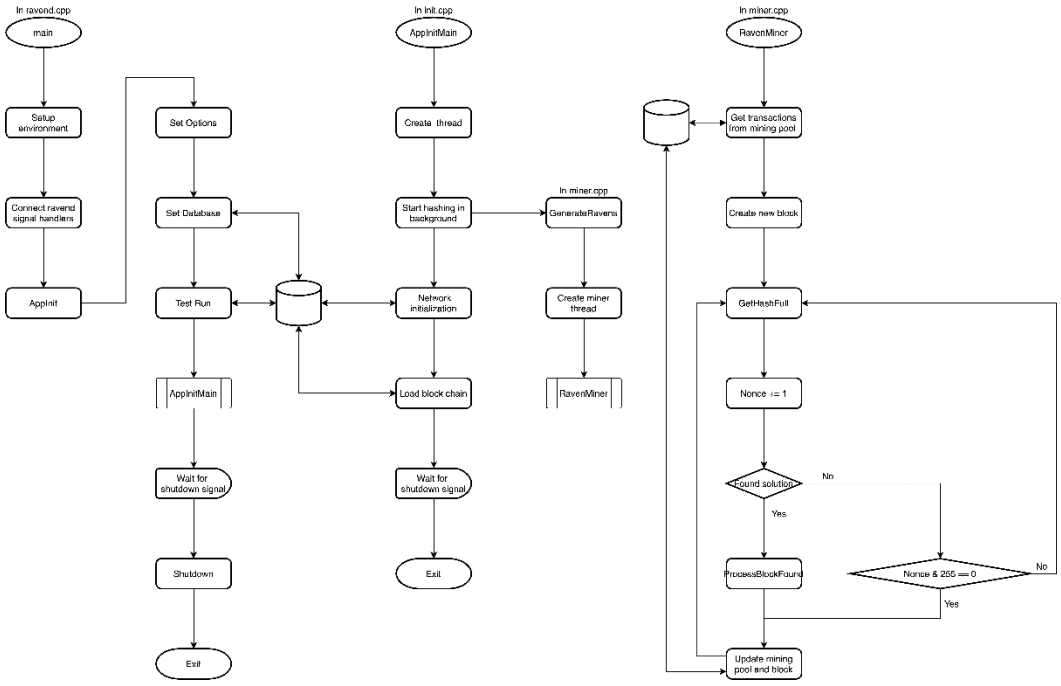
本專題研究主要專注在 Ravencoin 的架構研究及 Ravencoin 所使用的 X16Rv2 演算法分析。我們對 Ravencoin 的主程式及其挖礦流程進行結構分析，並將 Ravencoin 挖礦運算核心 X16Rv2 進行測速實驗。根據實驗結果，我們剖析數個速度較慢演算法的運算流程，進行 X16Rv2 演算法實作至硬體上的可行性評估，並嘗試以 TPS-1525 測試。

Research Process and Results

1. Ravencoin 主程式架構分析

研究發現，Ravencoin 區塊結構於比特幣基本一致，以 MerkleRoot 連結區塊頭與交易內容，與上一區塊的 hash 值一同 hash，構成區塊鏈。其挖礦流程主要依序經過：AppInit()、AppInitMain()、GenerateRavens()、RavenMiner()、GetHashFull()等函式，分別隸屬於多份文件。

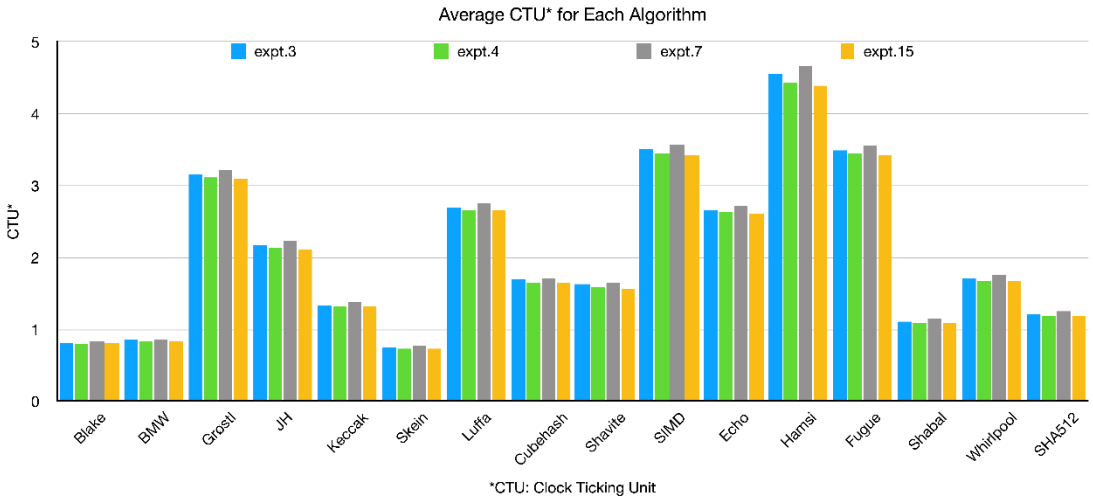
分析 Ravencoin 程式架構後，我們確認其源代碼 30 餘萬行，部分功能仍屬開發狀態，大量使用高階語言特性，且文件結構複雜，難以將完整程式以硬體實作進行加速。而其核心 X16Rv2 則相對獨立，可望由電腦與 FPGA 共同運作實現加速。



圖一、 Ravencoin 簡要挖礦流程

2. X16Rv2 演算法速度測試

因此，我們對 X16Rv2 及其子文件改寫，使 X16Rv2 可獨立編譯運行，以進行測速實驗。重複運行千萬次後，我們得出屬於 X16Rv2 的數個演算法，平均運行時間顯著並且穩定的較長，所得數據趨勢與 X16R 原始論文接近。



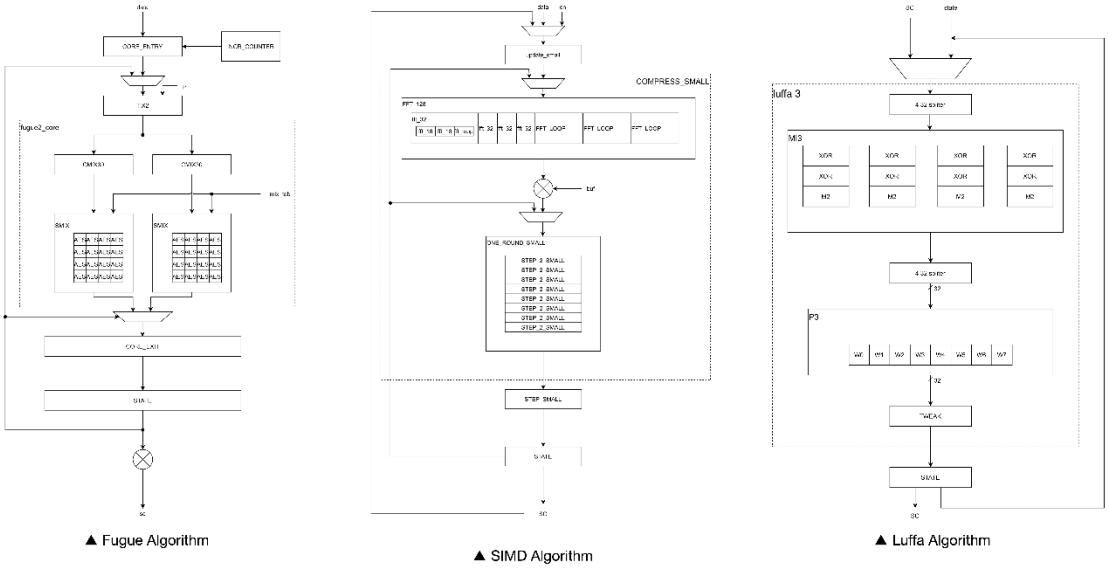
圖二、平均速度測試結果

3. X16Rv2 演算法在 FPGA 上加速可行性分析

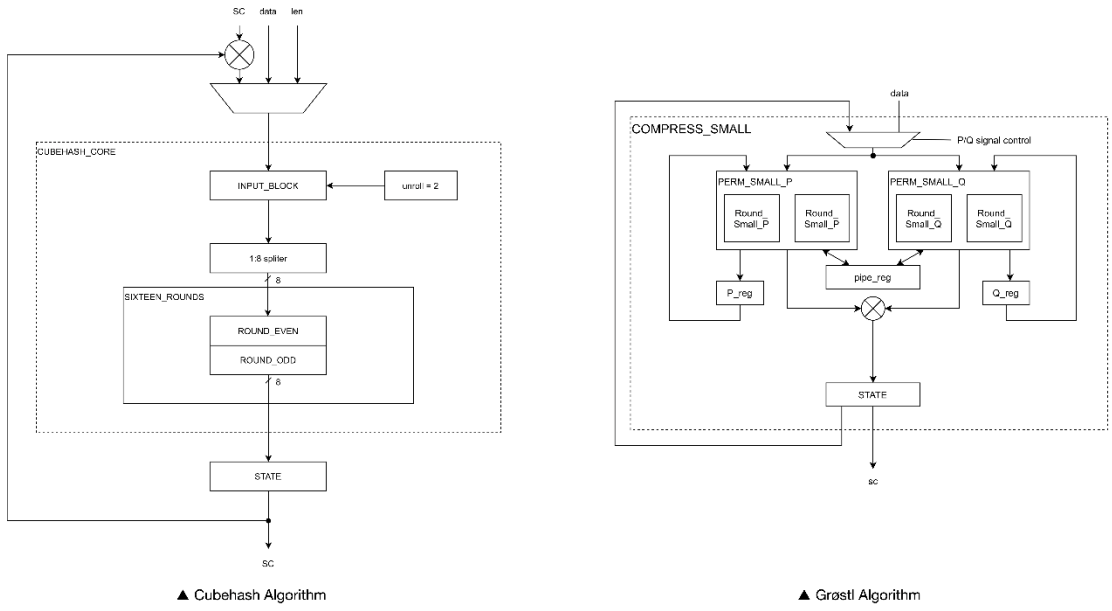
根據 X16Rv2 測速實驗結果，我們針對 7 個速度較慢的演算法進行分析，分別為 Hamsi、Grøstl、Fugue、SIMD、Echo、Luffa 以及 Cubehash。我們分析其源代碼，研究各演算法的運作流程。我們逐一追查重複進行的函式，並由演算法之原理，逐個分析有無可使用平行運算或指令管線化，達成硬體加速的可能。

我們發現，上述 7 個演算法中，都有部分函式具有硬體加速的潛力，甚至部分為演算法的核心架構。針對這些可加速的流程，我們研究其可加速的方法，並繪製成硬體流程圖，闡述可平行運算或指令管線化之處。

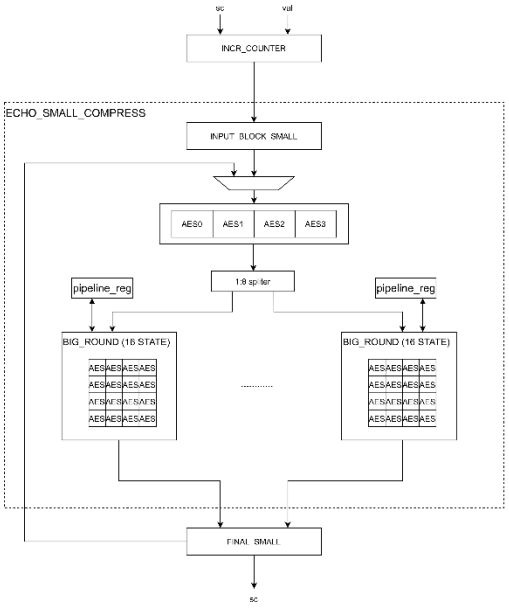
以下為我們的分析成果：



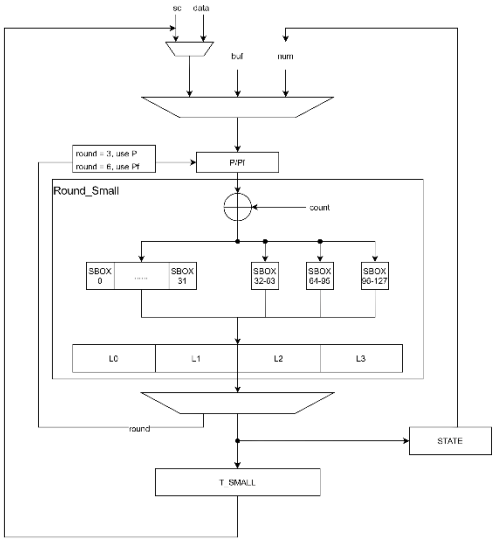
圖三、Fugue、SIMD、Luffa 硬體實作構想



圖四、Cubehash、Grøstl 硬體實作構想



▲ Echo Algorithm



▲ Hamsi Algorithm

圖五、Echo、Hamsi 硬體實作構想

Conclusions

據上述研究，我們認為 Ravencoin 之核心 X16Rv2 以硬體加速甚為可行，雖 Ravencoin 主程式難以完整硬體實作，然透過電腦與 FPGA 合作運行，仍可實現 Ravencoin 挖礦的硬體加速。

Review

一開始在考量專題題目時，出於我們皆對金融科技相當感興趣，並且知悉之浩老師開設「抗 ASIC 加密貨幣之硬體加速」，在初步了解區塊鏈的技術與運作後，我們向老師進一步請益，並與老師討論目標。之後，在老師的引導下，我們便由兩個面向著手進行，一為 Ravencoin 的主架構分析，探討挖礦過程是否有加速的可能性；二為 Ravencoin 運算核心 X16Rv2 的分析，我們想找到可以加速的部分，或是重複運算的函式，嘗試利用硬體將之加速。

在一開始的研究中，理解主程式架構是一大挑戰。一來 Ravencoin 是個很大型的專案，而官方並無提供指引，甚至源代碼內幾乎沒有註釋。二來從核心 X16R 循線向上追尋中，找到非常多並非挖礦用的函式，會使用、測試 X16R。因此，理解整個主程式花費相當多的時間，不過也從中學習到許多大型專案的

要點，以及程式設計的技巧。同時，我們也在研讀 X16Rv2 每一演算法的原理，為未來的研究做準備。

此後，在分析 X16Rv2 速度時，遇到許多編譯上的困難，不斷查詢資料後才一一解決。而實驗時，測得數據也非一開始就合理，直到使用正確的資料長度與格式，才成功測出 X16Rv2 的各演算法速度。

有了各演算法的速度數據後，我們進行 X16Rv2 的分析及硬體實作構想，並嘗試在 TPS-1525 上運作。因為 X16Rv2 演算法每一個都相當複雜，故我們選擇了數個運作較慢的進行操作及分析。然而，其複雜程度仍超過我們想像，分析與整理就花費許多時間。我們在第二學期期中，開始嘗試 TPS-1525 的使用，但對於機器的使用並不熟悉，且受限於時間，僅完成用於測試的 Bitstreams 生成。

在完成專題的過程中，我們學到許多，包含大型專案的文件、程式技巧、演算法的設計、硬體加速的要點等。從一開始有興趣，到能獨立完成研究，必須感謝老師提供給我們的幫助及資源，在兩周一次的面談，教導我們許多關於加密貨幣的知識，也會講一些有趣的故事，讓我們大家在輕鬆但不隨便的氛圍中完成專題。也感謝專題伙伴間的相互配合及努力不懈。

Reference

Ravencoin, www.ravencoin.org

RavonProject/Ravencoin on Github, www.github.com/RavenProject/Ravencoin

Tillich et al. High-Speed Hardware Implementations of
BLAKE, Blue Midnight Wish, CubeHash, ECHO, Fugue, Grøstl, Hamsi, JH, Keccak, Luffa, Shabal, SHAvite-3, SIMD, and Skein, 2009,
https://eprint.iacr.org/2009/510.pdf.

Vivado Design Suite User Guide, High-Level Synthesis,
www.xilinx.com/support/documentation/sw_manuals/xilinx2019_2/ug902-vivado-high-level-synthesis.pdf

TPS-1525 Specification: www.talentpros.com.tw/tps-1525