Classic McEliece 密碼系統之公鑰生成演算法之現場可程式化邏輯閘陣列實作

本院覽號

32T-1110224

公告日期

智財權狀態

know-how

摘要

1. 加密的公鑰密碼系統，為了達到「前向保密」，其公私鑰需定期更換。更換的頻率越快速，前向保密的效果就越強，因此本發明的目的是讓公鑰的產生更有效率。
2. 本發明藉由實現三種具「提前停止」效果的演算法來加速公鑰生成。本發明的硬體架構基礎是Wang, Szefer, Niederhagen 等人所設計的架構，我們更動了原有的架構，並加入額外的模組以實現三種演算法的效果。
3. 本發明主要是基於 Wang, Szefer, Niederhagen 等人的論文完成，但這些論文並沒有使用「提前停止」。

技術優勢

我們的技術加快了 Classic McEliece公鑰的生成，可稍微加強「前向保密」的強度

應用範圍

可用於需要使用 Classic McEliece 密碼系統進行金鑰交換的應用。

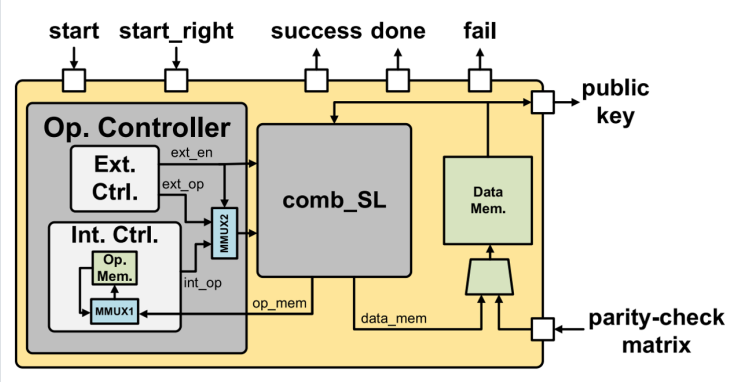

圖1.上圖為我們的硬體設計中主要的模組。其中 comb_SL 是一個二維的計算器陣列，是主要的運算單位。 \

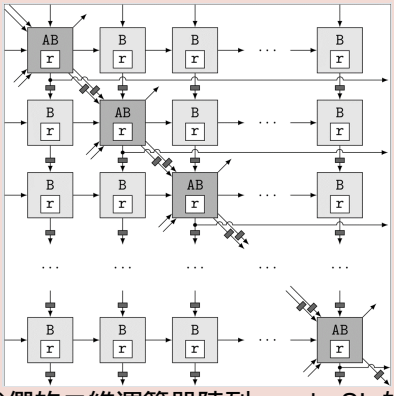

圖2.我們的二維運算器陣列 comb_SL 的架構

創作人

周彤、Ruben Niederhagen、陳博仁、Jakub Szefer、Wen Wang

中央研究院
ACADEMIA SINICA