本文描述了一種可重構密碼芯片，用於加速 DES、3DES 和 AES 計算，這些計算需要高性能和靈活性以適應大量與異構客戶端的安全連接。為了獲得高吞吐量，我們分析了高速度可重構設計的可行性，並找出了影響吞吐量的關鍵參數。隨後，我們提出了相應的設計方案，包括算法的重構分析、可重構處理單元的設計以及基於流水線和並行結構的新型可重構架構。實現結果顯示，操作頻率為 110 MHz，吞吐量為 DES 提供 7 Gbps、3DES 提供 2.3 Gbps、AES 提供 1.4 Gbps。與現有的類似實現相比，我們的設計可以實現更高的性能。

1. 引言

對於當前網絡或其他安全系統的需求，密碼芯片被期望支持多算法，並且靈活性變得越來越重要。大多數密碼算法具有相似的基本操作，可以設計成可重構處理單元（RPUs）。通過控制一些可控節點，RPUs 可以被重構以構建不同的電路，並且可以快速便捷地實現不同的功能以匹配不同的算法。基於 RPUs，一個可重構密碼芯片（RCC）可以取代許多特定用途的芯片，從而降低開發和製造成本。因此，已經有多種方法嘗試將可重構硬件應用於密碼學領域 [1~2]。

現代密碼學面臨的最大問題之一是數據吞吐量，特別是用於數據加密的對稱算法。對稱算法的較小帶寬會導致通信瓶頸。DES、3DES 和 AES 是最廣泛使用的對稱算法，雖然 DES 已被 AES 算法取代，但由於遺留需求，它在未來幾年內仍將保留在公共領域。因此，如何為這些算法設計一個高速的可重構密碼芯片（RCC）成為了一個挑戰。

在需要加密或解密大量數據的應用中，吞吐量決定了總加密或解密時間，因此是衡量密碼速度的最佳指標。通常，加密和解密的吞吐量是相等的，因此僅報告一個參數。要分析高速可重構設計的可行性，我們必須分析加密吞吐量的計算，並找出影響 RCC 速度的主要因素。加密吞吐量

𝑉

V 定義為單位時間內加密的位數，可以量化如下：



其中，L 是數據的塊長度，f 是系統時鐘頻率，k 是處理一個塊所需的時鐘週期數，而 f/k 是加密一個明文塊所需的時間。由於我們可以為不同算法的硬件實現選擇固定的塊長度，因此影響 V 的主要參數是 f 和 k。

最大系統時鐘頻率 𝑓maxfmax​ 由最小時鐘週期決定，這取決於組合邏輯中延遲最長的部分。設 𝑡𝑖ti​ 為組合邏輯 𝑖i 的延遲，𝑚m 為組合邏輯的數量。因此，𝑓maxfmax​ 的方程可以表示為：



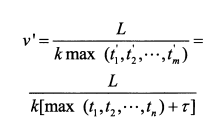
將 𝑓maxfmax​ 代入公式 (1)，我們得到



由於重構技術可以在電路中設置一些可控節點，以針對不同的算法改變 RPUs 和電路結構，因此 RPUs 和架構的重構會增加組合邏輯的延遲。設

𝜏

τ 為增加的最壞情況延遲，則可重構電路的吞吐量為：



其中 t 和 t 是可重組電路和無需重新配置的電路的組合邏輯延遲。

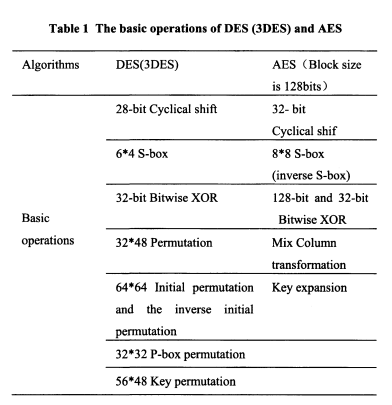
根據上述分析，可以認為k和τ是決定RCC速度的關鍵參數。為了提高吞吐量，我們必須減少k和τ。眾所周知，k可以通過使用流水線和並行結構來減少。τ的值與RPUs的結構有關。由於RPUs的內部結構是可變的，結構的複雜性會直接影響其延遲。此外，它還會影響數據傳播路徑的延遲。因此，可以通過設計面積小且性能高的RPUs來減少τ。

3. RCC的設計

RCC的設計是一個包括劃分和重構的過程。劃分是分析密碼算法的重構性，找到可以設計為RPUs的相似操作。重構包括RPUs設計和可重構架構設計。從第2部分的高速可重構設計的可行性分析中可以看出，影響加密吞吐量的主要因素是k和τ。為了實現高速RCC，我們必須在RPUs設計和可重構架構設計中找到解決方案，以減少k和τ。

3.1 重新配置分析

為了分析 DES、3DES 和 AES 的重新配置，我們必須分析這些算法之間的相似操作。表 1 列出了 DES（3DES）[3] 和 AES[4] 的基本操作。3DES 本質上是順序的，因此是 DES 的一個邏輯延伸。因此，3DES 的操作與 DES 相同。



從表 1 中，我們可以看到這些算法的相似操作是循環移位、S-box 和按位 XOR。S-box 通常被實現為 ROM，是許多算法中唯一的非線性組件，決定了整個算法的安全強度；預期將其設計為可以更新以增強這些算法安全性的 RPU。正如我們所知，AES 的 S-box 和逆 S-box 使用不同的查找表（LUT）。當操作從加密變為解密或反之時，RPU 可以在重置後加載相應的表。因此，它不僅應該實現 DES S-box 和 AES S-box 的重新配置，還應該實現 AES S-box 和 AES 逆 S-box 的重新配置。其設計對於設計可重組架構非常重要。

這些算法中的循環移位操作是固定的，可以通過排列簡單實現，無需設計為 RPUs。按位 XOR 在加密學中非常常見。預期將其設計為可以增強邏輯電路可擴展性的 RPU。

3.2 RPU 設計

為了滿足不同算法的需求，RPUs 必須靈活地改變其結構。然而，靈活性的增加可能會導致 τ 的增加。因此，RPUs 的設計者總是面臨性能和靈活性之間的折衷。根據第 3.1 節的分析，可以說 DES（3DES）和 AES 之間的相似操作是 S-box 查找表和 XOR 運算。因此，S-box 和 XOR 可以分別設計為可以命名為可重組 S-box（RC-S）和可重組 XOR（RC-XOR）的 RPUs。由於我們可以通過添加 MUX 實現對不同輸入的 XOR 運算，因此實現 RC-XOR 是很容易的。

設計 RC-S 是困難的，因為它不僅需要實現 DES 和 3DES 的 48X32 LUT，還需要實現 AES 的 8X8 LUT。我們設計了一個 RC-S，由八個並行的 64 X 4 RAM 和兩個 4 到 1 的 MUX 組成。圖 1 顯示了 RC-S 的內部結構。MUX 是可控制的節點，可以通過改變結構 RC-S 來實現不同的 S-box 操作。RC-S 的輸入信號包括地址信號、用於 RAM 寫入使能的 wen 信號、用於 RAM 啟用的 cen 信號和用於節點控制的 ctrls 信號。為了實現 DES 和 3DES，RC-S 具有 48 位地址（DES\_A），每個 RAM 具有不同的地址信號。為了實現 AES，RC-S 具有 8 位地址（AESA），並且整個八個 RAM 具有相同的 6 位地址。如圖 1 所示，可以看出 RC-S 的結構是簡單的。與一般的 S-box 相比，RC-S 的延遲增加了一個 MUX 的延遲用於 DES，以及兩個 MUX 的延遲用於 AES。因此，RC-S 的設計對 S-box 操作的延遲影響很小，有利於減少 τ。

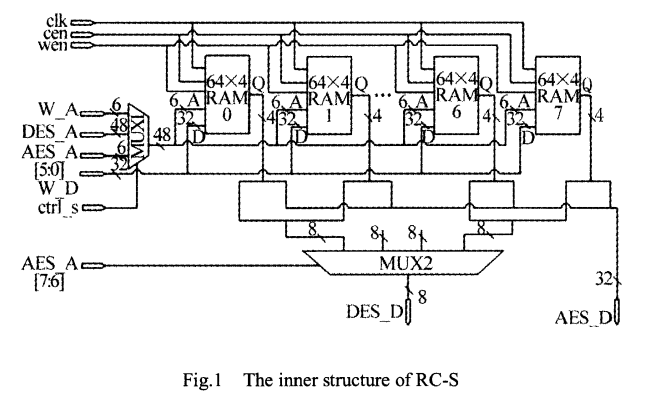


圖1 RC-S內部結構

3.3 可重組架構設計

在本節中，我們提出了一種基於管道、並行處理和重新配置技術的可重組架構，以降低 k。有三個需要解決的問題如下：

(1) 面積限制，這意味著如何在面積和性能之間取得平衡。

(2) 需要決定 RPU 的數量，主要挑戰在於如何在最大化加密吞吐量的同時最小化面積消耗。

(3) RPUs 之間的連接，不同的算法具有不同的管道和並行架構，在這一點上，如何改變 RPUs 之間的連接以匹配不同的架構。

區塊算法的迭代性質使它們非常適合進行流水線處理。但這並不意味著流水線處理可以在不考慮面積消耗的情況下應用於任何算法。由於 DES 輪轉換的規模相對較小，大多數 DES 硬件實現都將 16 個 DES 輪展開並進行流水線處理以提高速度。例如，Ihn Kim 在 0.35 微米 CMOS 技術中製作了一個完全流水線處理的自定義 VLSI 芯片，能夠以 5.6 Gbps 的吞吐量在 87.5 MHz 下進行 DES 加/解密。聖地亞哥國家實驗室（SNL）宣布了它們最快的 DES 自定義 ASIC，速度達到 9.28 Gbps。

由於 AES 輪中存在相當大的並行性，輪的所有轉換可以對區塊的字節、行或列進行並行處理，並且並行架構被廣泛應用於 AES 硬件實現中。由於 AES 輪的規模相對較大，通常不會使用流水線處理。因此，在我們的設計中，DES（3DES）的實現中使用了 16 級流水線，而對於 AES 則使用了並行結構。

基於上述分析，設計了一個新的可重組架構，如圖 2 所示。圖 2 顯示了 RPU 陣列擁有十六個 RPUs，由 RC-S 和 RC-XOR 組成。通過控制節點 A 和 B，這些 RPUs 之間的連接可以更改，以實現兩種不同的架構。一種是 16 級流水線架構，另一種是並行架構。對於 DES，該架構可以通過 RPU 陣列的串行連接形成 16 級流水線結構。它從初始置換開始，進行十六輪加密，然後進行初始置換的逆操作。內部數據路徑都是 64 位。每個輪次是一個流水線階段，在一個時鐘周期內執行。因此，該電路可以在每個時鐘周期內完成一個 DES 的區塊加密/解密。

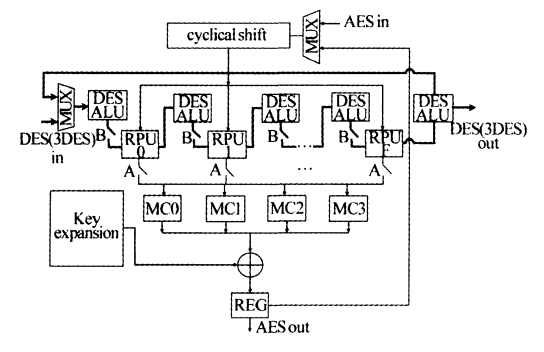


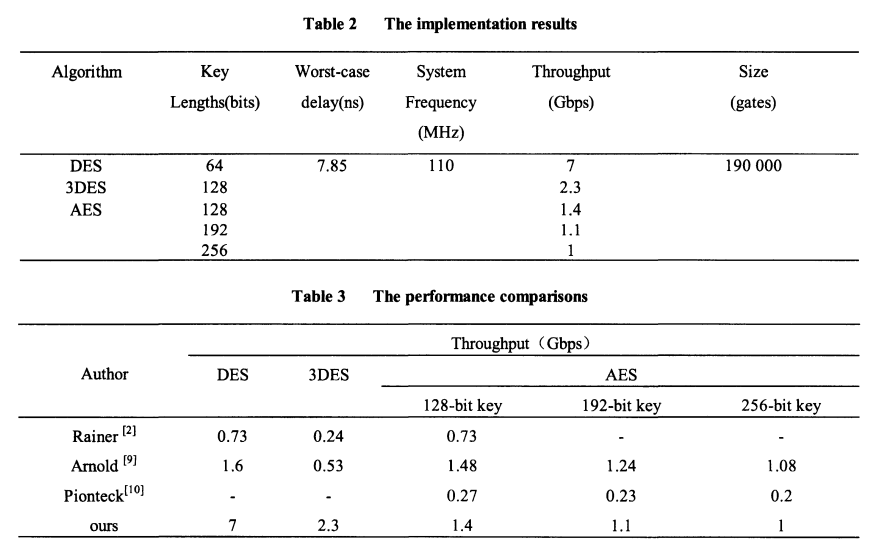
圖2 可重構架構的結構

3DES 算法僅由三個單獨的 DES 操作依序組成。因此，與 DES 和流水線化 DES 相關的大部分工作都直接或間接地適用於 3DES。如圖 2 所示，DES 電路被重復三次以實現 3DES。在前 16 個周期中，使用的加密金鑰是 3DES\_key1，接著是下一個 16 個周期的 3DES\_key2，最後是最後 16 個周期的 3DES\_key3。對於第一個和第二個 16 個周期，DES 加密/解密的結果被寫回到輸入寄存器。因此，對於 3DES，16 個區塊的加密/解密需要 48 個時鐘周期。

對於 AES，該架構可以通過 RPU 陣列的並行連接實現並行結構。如圖 2 所示，每個輪次由循環移位模塊、16 個 RPUs、4 個混合列模塊（MCs）和一個 128 位的 XOR 組成。為了提高吞吐量，循環移位操作可以通過排列簡單實現。密鑰擴展模塊負責生成輪密鑰。由於密鑰長度可以獨立選擇為 128、192 或 256 位，因此包含這些操作的輪數為 10、12 或 14 輪。輪次是使用組合邏輯實現的，其輸出被註冊為下一輪的輸入。因此，根據密鑰長度，一個區塊的加密/解密需要 10、12 或 14 個時鐘周期。

4.實現結果

該設計使用自頂向下的方法通過 Verilog HDL 描述，並使用 Cadence EDA 工具進行模擬。它通過使用 TSMC 0.25 μm 標準單元庫的 Cadence PKS 工具進行合成。實現結果如表 2 所示。我們的設計可以實現 DES、3DES 和 AES 的加密和解密，包含大約 190,000 個閘。而參考文獻 [7] 中設計的總閘數為 173,000，並且僅實現了 AES 的加密。表 3 顯示了我們的設計與其他解決方案之間的性能比較。如表 2 和表 3 所示，可以看出操作頻率為 100 MHz，DES 的吞吐率為 7 Gbps，3DES 為 2.3 Gbps，AES 為 1.4 Gbps。與類似的現有實現相比，我們的設計可以實現更高的性能。



實施結果

結論

我們設計的目標是開發一款針對 DES、3DES 和 AES 的高速可重組密碼芯片。通過分析高速可重組設計的可行性，我們發現時鐘周期數 k 和增加的最壞情況延遲 τ 是影響可重組密碼芯片吞吐量的關鍵參數。為了減少 τ，我們找到了一個具有小面積和高性能的 RPU 解決方案（RC-S），可以提高 S-box 和算法的靈活性和安全性。為了減少 k，我們提出了一種新穎的可重組架構，將重新配置與流水線和並行結構相結合。基於 TSMC 0.25 μm 技術，我們實現了 DES、3DES 和 AES 算法，模擬結果顯示，在 110 MHz 時鐘下，DES 的吞吐量為 7 Gbps，3DES 為 2.3 Gbps，AES 為 1.4 Gbps。與其他類似設計相比，我們的設計可以達到更高的性能，因此對於可重組密碼芯片的發展具有重要意義。