# CS6132 Advanced Logic Synthesis

## Homework 2 Report

111062584 王領崧

- 實驗流程:
  此次作業使用 SAT attack tool 來檢視三種不同 logic encryption algorithms。透過實驗比較不同 logic encyption 與不同 benchmarks 搭配的加密效果，藉此分析表現比較好的組合的特性。
  測量的數據有 #PIs, #Key Inputs, #POs, #Gates, #SAT iterations, CPU time。

- 實驗設定:
  實驗機器為 cad server 上面的 ic51，有 64 CPUs & 128GB memory。
  **rnd, dac12** 加密的 benchmark 有 21 個，每個 benchmark 各有 4 個 encryption area overhead 的版本，分別為 5%, 10%, 25%, 50%。
  **sarlock/dac12** 加密的 benchmark 有 11 個，每個 benchmark 各有 3 個 encryption area overhead 的版本，分別為 5%, 10%, 25%。
  SAT attack tool 解密的時限為 2 小時，超過 2 小時即為解密失敗 (fail)。

- 實驗結果和分析:
  1. rnd encryption results
     這裡為攻擊 rnd encryption locked benchmark 的結果。在 21 個 benchmark 中，17 個 benchmark 所有 encryption area 版本都能在時限內被解密，4 個 benchmark 有部分版本會解密失敗，分別是 c2670 (enc25, enc50)、c7552 (enc50)、dalu (enc50)、des (enc50)。Chart 1 是全部被解密 benchmark 的執行時間，Chart 2 是部分解密 benchmark 的執行時間。
     實驗結果顯示，大部分的 testcases 都能在 **12** 分鐘內被破解。全部解密和部分解密的 benchmark，隨著 encryption area 提升，執行時間皆以類指數型的成長(25 -> 50 成長幅度最大)。意外的是部分解密的 benchmark 在 enc 5%, 10% 的執行時間並沒有和全部解密的相差太多。

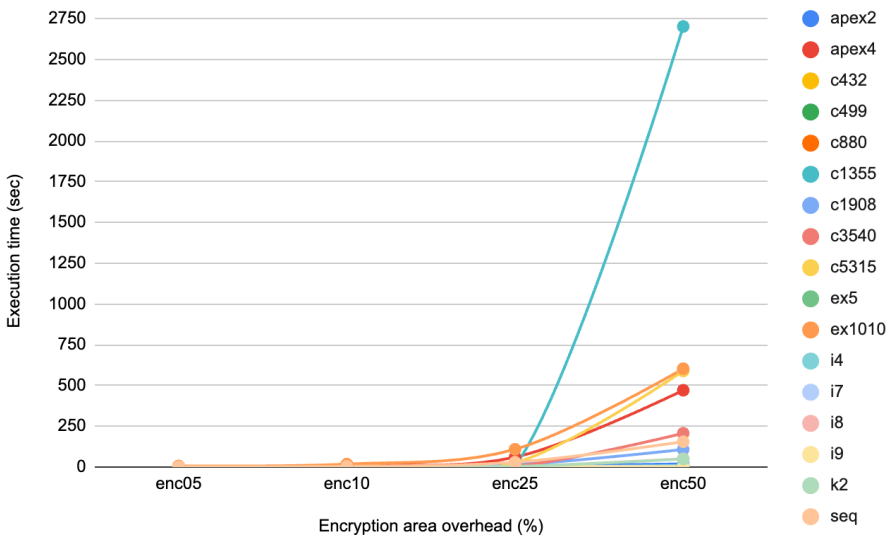


**Chart 1: Runtime of complete decrypted benchmark (rnd encryption)**

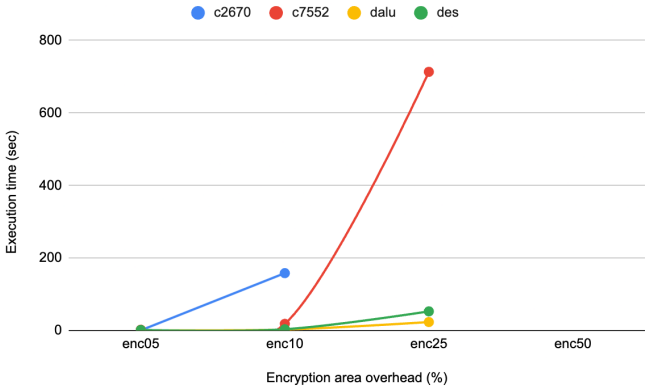


**Chart 2: Runtime of partial decrypted benchmark (rnd encryption)**

2. dac12 encryption results

這裡為攻擊 dac12 encryption locked benchmark 的結果。在 21 個 benchmark 中，16 個 benchmark 都能在時限內被解密，5 個 benchmark 有部分版本會解密失敗，分別是 c2670 (全部)、c5315 (25%, 50%)、c7552 (10%, 25%, 50%)、dalu (50%)、des (10%, 25%, 50%)。Chart 3 是全部被解密 benchmark 的執行時間，Chart 4 是部分解密 benchmark 的執行時間。

與 rnd encryption 的實驗結果相似，大部分的 testcases 都能在 **10** 分鐘內被破解，執行時間皆以類指數型的成長，部分解密的執行時間並沒有和全部解密的相差太多。

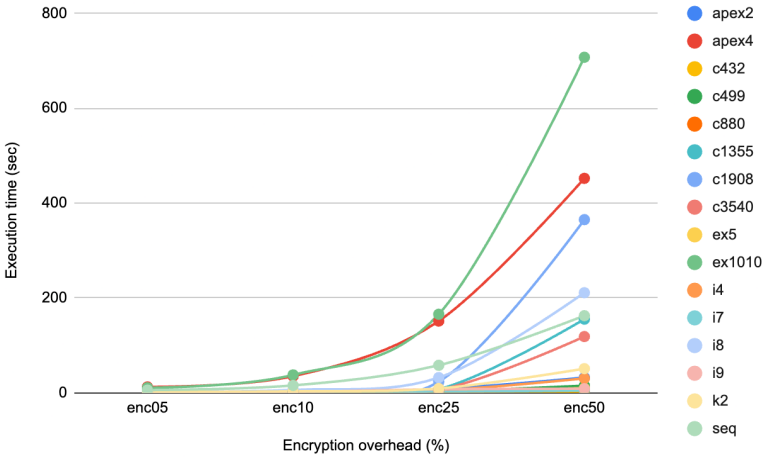


**Chart 3: Runtime of complete decrypted benchmark (dac12 encryption)**

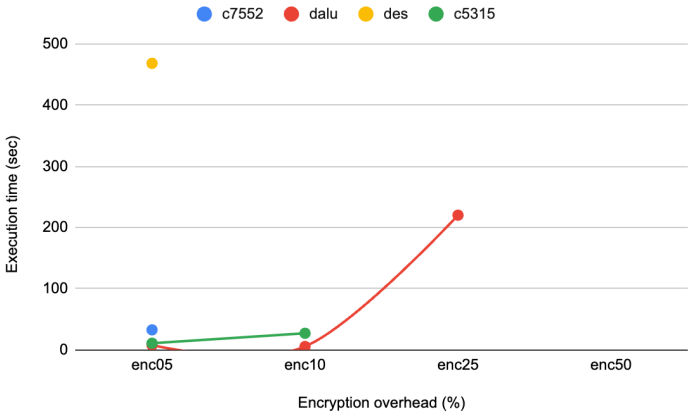


**Chart 4: Runtime of partial decrypted benchmark (dac12 encryption)**

3. sarlock/dac12 encryption results
   這裡為攻擊 sarlock/dac12 encryption locked benchmark 的結果。由於 sarlock 是 anti-SAT，所以在 11 個 benchmark 中，僅有 2 個 benchmark 能在時限內被解密，其餘 9 個所有版本都會解密失敗。Table 1 為成功解密的 benchmark 的實驗數據。
   實驗結果顯示，隨著 encryption area 提升，#Key inputs 大約是 2 倍的速度在增加，執行時間也呈現指數型增加。有趣的是，相同測資需要的 SAT iterations 數量都相同。

| Name | #PIs | #Key Inputs | #POs | #Gates | #SAT iterations | CPU time |
|---|---|---|---|---|---|---|
| apex4 (5%) | 10 | 278 | 19 | 5675 | 1023 | 336.592 |
| apex4 (10%) | 10 | 546 | 19 | 5943 | 1023 | 383.401 |
| apex4 (25%) | 10 | 1350 | 19 | 6747 | 1023 | 1437.71 |
| ex5 (5%) | 8 | 61 | 63 | 1191 | 255 | 4.882 |
| ex5 (10%) | 8 | 114 | 63 | 1247 | 255 | 6.761 |
| ex5 (25%) | 8 | 272 | 63 | 1406 | 255 | 13.305 |

**Table 1: Results of complete decrypted benchmark (sarlock/dac12 encryption)**

4. rnd & dac12 results comparison
   這裡為比較 rnd & dac12 加密的效果，使用的測資是都有解密成功的 9 個 enc_50 的 testcases (有些執行時間 < 10s 就不列入表格)，參考的數據有 #KIs, #Gates, #SAT iterations, CPU time。Table 2 為比較的表格，使用 rnd 作為 baseline 比較，最後結果用 % 呈現。
   實驗結果顯示，兩者數據差異非常小，基本上都在正負 0.5% 以內，只有兩個測資的 CPU time 相差到 2~3 %，顯示兩個 encryption algorithm 的效果差不多。

| Name | #Key Inputs | #Gates | #SAT iterations | CPU time |
|---|---|---|---|---|
| apex2 | 0 | -0.004 | -0.076 | 0.743 |
| apex4 | 0 | 0.001 | 0.008 | -0.039 |
| c1355 | 0 | 0.015 | -0.306 | -0.943 |
| c1908 | 0 | 0.007 | 0.521 | 2.407 |
| c3540 | 0 | 0.001 | 0.199 | -0.426 |
| ex1010 | 0 | 0.001 | -0.094 | 0.175 |
| i8 | 0 | -0.002 | 0.461 | 3.205 |
| k2 | 0 | -0.003 | -0.032 | 0.043 |
| seq | 0 | 0.002 | -0.023 | 0.051 |

**Table 2: rnd & dac12 results comparison (rnd is the baseline)**

5. #Key input & CPU time
   這裡為 key input 數量和 CPU time 的關係圖，資料為此次作業所有成功解密的 testcases。Chart 5 為兩者關係的分布圖。
   由實驗結果得知，key input 數量和 CPU time 呈現正相關，但是沒有非常明顯。並且當 encryption area 越大，key input 的數量會越多，執行時間也比較久。(enc5 和 enc10 因為都分布於左下角，所以被蓋住了不易看見)

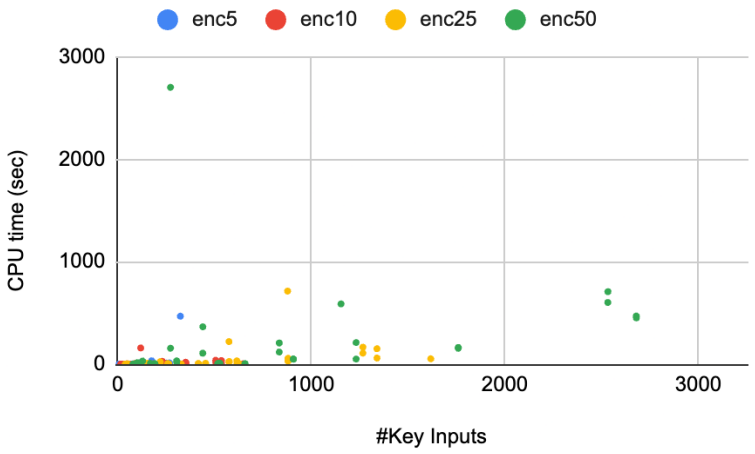


**Chart 5: Relation of #Key inputs and CPU time (All decrypted benchmarks)**

6. #Gates & CPU time

   這裡為探討 gates 數量和 CPU time 的關係，因為第 5. 已經討論 encryption area 和 CPU time 關係，所以這邊直接使用 rnd encryption area 50% 的 testcase 來做比較分析，Chart 6 為 #gates 和 CPU time 的關係圖，testcase 的順序是由 #gates 由小到大排序。因為執行時間分佈較懸殊，所以採用對數刻度來表示，並且解密失敗的 testcase 用粉紅色來表示。

   實驗結果顯示，對於成功解密的測資，#gates 數量和 CPU time 並沒有很直接的關聯，因為後面的 runtime 都在 2 次方的量級內，但第五個測資是在 3 次方。不過無法在時間內成功解密的測資，#gates 越大確實看起來機會比較大。

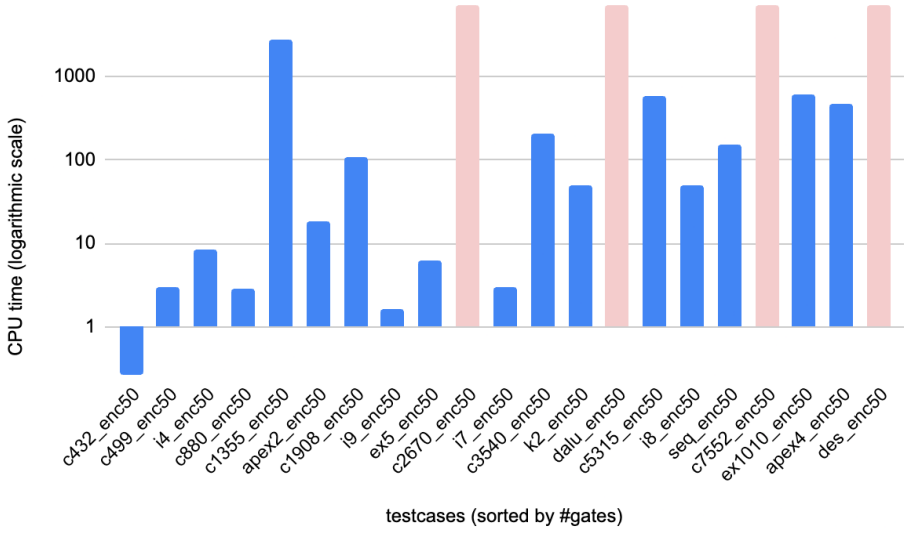


**Chart 6: Relation of #Gates and CPU time (Decrypted rnd benchmarks)**

7. Conclusion
   a. rnd & dac12 encryption 的效果差不多，有 17(16)/21 的 testcases 可以成功解密，剩餘的 testcases 部分版本可以成功解密，不過大部分都在 12 分鐘內就可以被 SAT 破解，加密的效果並不理想。
   b. 由於 sarlock 是 anti-SAT，所以僅有 2/11 的 testcases 被成功解密。
   c. SAT attack tool 解密的時間會以類似指數型態成長，encryption area overhead 從 25% -> 50% 的成長幅度為最大。