Logic Design and Design for Security, Fall 2018

Project 2: SAT-based attack

0756023 周煥然

Build: make

Run: ./solver [Encrypted circuit] [Original circuit] [Output file] [SatAttackExe] [N]

Implementation:

我針對加密後的電路找出以下兩種 gate:

Type 1: 其中一個 input pin 為 primary input 或是 primary input 經由 Buf 或是 Not gate 接到該 input pin。

Type 2: 其中一個 input pin 為 key input 或是 key input 經由 Buf 或是 Not gate 接到該 input pin。

接著以每個 key input 為起點 traverse 電路(BFS)，終點則 primary output 或是 type 1 的 gate，因為當遇到 type 1 gate 時，可以藉由控制 primary input，mute 掉該 key input 的效果。

而每一個 type 2 gate 代表一個 key input，並根據以下幾點判斷該 key input 的重要性:

1.該 key input 可到達的 primary output 數量。

2.每一條從 key input 到 primary output 的 path 中，所經過 type 2 gate 的數量。

3.每一個 type 2 gate 會被幾條從 key input 到 primary output 的 path 所經過。

將這些數值標準化並做排序來決定最後的 output。