

## Introduction:

A hardware Trojan is now considered as a possible threat to integrated circuits when they are produced in an un-trusted foundry. What we are looking for is the possibility of adding Trojans in *design houses* rather than foundries. This requires not only the low possibility to trigger the Trojan, but also obfuscated communication channels that cannot be detected by logic analysis and simulation.

We investigate a 'content & timing' based Trojan trigger and two methods of obfuscated communication of the trigger signal to the Trojan: 'thermal communication', and 'feedback'.

1. 'content & timing' based Trojan trigger extremely decreases the probability of triggering a Trojan;
2. 'Thermal communication' makes use of temperature to transfer trigger signal to activate a Trojan;
3. 'Feedback' requires the VGA peripheral as a part of the communication channel.

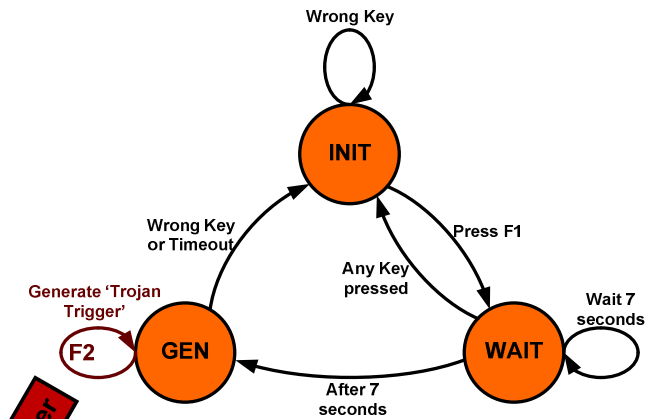
We call the second and third one as covert communication channels, as shown in the center figure.

## Feedback:

- An existing electrical connection exists on the board between RED1 and RED2.
- RED1 and RED2 are defined as "input" but only used as "output".
- Output a 'HIGH' on RED2 and simultaneously configure RED1 from "output" to "input".
- With the VGA peripheral, signal on RED2 can be sampled by RED1.
- An obfuscated communication channel is created.
- Without the VGA peripheral, there is no signal into port RED1 and hence the Trojan will never be triggered.
- A Trojan that is triggered by a signal using this path is only complete when the FPGA is plugged into the board.
- The Trojan cannot be triggered during the simulation and analysis stage.

## Content and Timing:

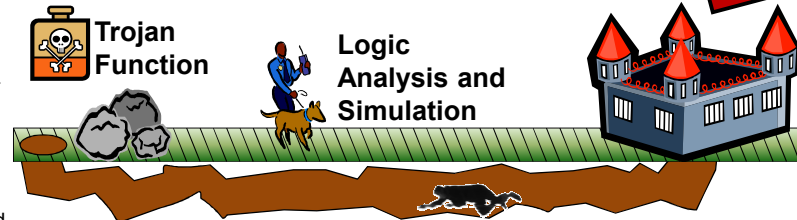
- A typical keyboard input sequence .
- Precise time delay between two key presses needed for trigger.
  - Any press in between means start over.
- Extremely low probability of trigger
  - Example: Trigger pattern of F1 and F2
    - 10 seconds gap with trigger failure if any key is pressed in between.
    - Probability of a tester finding such pattern by brute force is - once is  $3^{*1035}$  years.
- Almost impossible to simulate and detect such key press sequence with time dimension.



## Thermal Communication:

Temperature is an invisible covert communication channel to logic analysis and simulation. Trojans with this technique added in the design houses will only appear after implementation.

- We use heat to transfer information in integrated circuits.
1. Generate different amounts of heat according the 'input' with a set of ring oscillators enabled by the 'input';
  2. Sense the temperature with another 2 ring oscillators.
  3. Post-process the frequencies of the 2 ring oscillators and get the 'output' which equals to 'input'.



## Covert Communication Channel

