s15850-T100

- Trojan description
  - The Trojan trigger consists of two comparators and one flip-flop at the output of each comparator. The comparators drive the clock inputs of the flip-flops. The data input of the first flip-flop is '1' and the output of the first flip-flop is connected to the data input of the second flip-flop. The output of the second flip-flop is gated by the inverted test enable signal to ensure Trojan activation only in the functional mode. The Trojan payload is a MUX on an output port. Unless the Trojan gets activated, the output port functions as normal; otherwise, the output port leaks an internal signal.

- Trojan taxonomy
  - Insertion phase: Design
  - Abstraction level: gate level
  - Activation mechanism: Internally conditionally triggered
  - Effects: Denial of Service, Change functionality
  - Location: Processor
  - Physical characteristics: Functional

s15850-T100

```
// Trojan trigger ----------------
 // Comparator 1
 AND2X2 Tg1_Trojan1 (.IN1(g6179), .IN2(n519), .Q(Tg1_OUT1));
 AND2X2 Tg1_Trojan2 (.IN1(n1202), .IN2(n1132), .Q(Tg1_OUT2));
 AND2X2 Tg1_Trojan3 (.IN1(n1226), .IN2(n1858), .Q(Tg1_OUT3));
 AND2X2 Tg1_Trojan4 (.IN1(g5556), .IN2(n898), .Q(Tg1_OUT4));
 AND4X1 Tg1_Trojan1234 (.IN1(Tg1_OUT1), .IN2(Tg1_OUT2), .IN3(Tg1_OUT3), .IN4(Tg1_OUT4), .Q(Tg1_OUT1234));
 NOR2X0 Tg1_Trojan5 (.IN1(n1391), .IN2(n931), .QN(Tg1_OUT5));
 NOR2X0 Tg1_Trojan6 (.IN1(n857), .IN2(n902), .QN(Tg1_OUT6));
 NOR2X0 Tg1_Trojan7 (.IN1(n1889), .IN2(n1890), .QN(Tg1_OUT7));
 NOR2X0 Tg1_Trojan8 (.IN1(n1055), .IN2(n1016), .QN(Tg1_OUT8));
 AND4X1 Tg1_Trojan5678 (.IN1(Tg1_OUT5), .IN2(Tg1_OUT6), .IN3(Tg1_OUT7), .IN4(Tg1_OUT8), .Q(Tg1_OUT5678));
 AND2X2 Tg1_Tj_Trigger ( .IN1(Tg1_OUT1234), .IN2(Tg1_OUT5678), .Q(Tg1_Trigger1) );
 DFFNX2 Tg1_Trigger ( .CLK(Tg1_Trigger1), .D(1'b1), .Q(Tg1) );
```

s15850-T100

```
// Trojan trigger ----------------
 // Comparator 2
 AND2X2 Tg2_Trojan1 (.IN1(n938), .IN2(n1917), .Q(Tg2_OUT1));
 AND2X2 Tg2_Trojan2 (.IN1(n1921), .IN2(n1911), .Q(Tg2_OUT2));
 AND2X2 Tg2_Trojan3 (.IN1(n1918), .IN2(n1913), .Q(Tg2_OUT3));
 AND2X2 Tg2_Trojan4 (.IN1(n1916), .IN2(n1910), .Q(Tg2_OUT4));
 AND4X1 Tg2_Trojan1234 (.IN1(Tg2_OUT1), .IN2(Tg2_OUT2), .IN3(Tg2_OUT3), .IN4(Tg2_OUT4), .Q(Tg2_OUT1234));
 AND2X2 Tg2_Trojan5 (.IN1(n1161), .IN2(n1154), .Q(Tg2_OUT5));
 AND2X2 Tg2_Trojan6 (.IN1(n1116), .IN2(n1162), .Q(Tg2_OUT6));
 AND2X2 Tg2_Trojan7 (.IN1(n1155), .IN2(n1107), .Q(Tg2_OUT7));
 AND2X2 Tg2_Trojan8 (.IN1(n929), .IN2(n554), .Q(Tg2_OUT8));
 AND4X1 Tg2_Trojan5678 (.IN1(Tg2_OUT5), .IN2(Tg2_OUT6), .IN3(Tg2_OUT7), .IN4(Tg2_OUT8), .Q(Tg2_OUT5678));
 AND2X2 Tg2_Tj_Trigger ( .IN1(Tg2_OUT1234), .IN2(Tg2_OUT5678), .Q(Tg2_Trigger2) );
 DFFNX2 Tg2_Trigger ( .CLK(Tg2_Trigger2), .D(Tg1), .Q(Tg2) );

 INVX0 INVtest_se ( .IN(test_se), .QN(test_se_NOT) );
 AND2X2 Trojan_Trigger (.IN1(Tg2), .IN2(test_se_NOT), .Q(Trigger_select) );

 // Trojan payload ----------------
 MUX21X2 Trojan_Paylaod ( .IN1(g4207_Payload), .IN2(n1936), .S(Trigger_select), .Q(g4207) );
```

Please send your concerns/questions to

Dr. Hassan Salmani at SalmaniHSN@gmail.com

Administrator at admin@trust-hub.com