

# s38417-T300

## 🔑 Trojan description

- 🔑 The Trojan trigger is a comparator with activation probability of  $1.6616e-44$ . The Trojan payload leaks the value of a specific net through side-channel signals (ring-oscillator with 29 stages).

## 🔑 Trojan taxonomy

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

# s38417-T300

// Trigger -----

```
NOR2X0 Trojan1 (.IN1(n4037), .IN2(n4043), .QN(Tj_OUT1));
NOR2X0 Trojan2 (.IN1(n4034), .IN2(n4033), .QN(Tj_OUT2));
NOR2X0 Trojan3 (.IN1(n4046), .IN2(n4038), .QN(Tj_OUT3));
NOR2X0 Trojan4 (.IN1(n2568), .IN2(n3457), .QN(Tj_OUT4));
NOR4X0 Trojan1234_NOT (.IN1(Tj_OUT1), .IN2(Tj_OUT1), .IN3(Tj_OUT3), .IN4(Tj_OUT4), .QN(Tj_OUT1234));
NOR2X0 Trojan5 (.IN1(n3478), .IN2(n3469), .QN(Tj_OUT5));
NOR2X0 Trojan6 (.IN1(n3445), .IN2(n3212), .QN(Tj_OUT6));
NOR2X0 Trojan7 (.IN1(n3237), .IN2(n3225), .QN(Tj_OUT7));
NOR2X0 Trojan8 (.IN1(n3196), .IN2(n3417), .QN(Tj_OUT8));
NOR4X0 Trojan5678_NOT (.IN1(Tj_OUT5), .IN2(Tj_OUT6), .IN3(Tj_OUT7), .IN4(Tj_OUT8), .QN(Tj_OUT5678));
AND2X1 Trojan_CLK_NOT (.IN1(Tj_OUT1234), .IN2(Tj_OUT5678), .Q(Tj_Trigger) );
```

// Payload -----

```
DFFX2 Trojan_Payload1 (.CLK(Tj_Trigger), .D(1'b1), .Q(RingOscENable1));
DFFX2 Trojan_Payload2 (.CLK(Tj_Trigger), .D(1'b0), .QN(RingOscENable2));
DFFX2 Trojan_Payload3 (.CLK(Tj_Trigger), .D(1'b1), .Q(RingOscENable3));
AND3X4 Trojan_Payload (.IN1(RingOscENable1), .IN2(RingOscENable2), .IN3(RingOscENable3), .Q(RingOscENable));
```

**Please send your concerns/questions to**

**Dr. Hassan Salmani at [SalmaniHSN@gmail.com](mailto:SalmaniHSN@gmail.com)**

**Administrator at [admin@trust-hub.com](mailto:admin@trust-hub.com)**