Hardware Security Project

*Boyou Zhou**

*Boston Univeristy, MA

Created on Oct 4 2014, Modified on November 20, 2014

Outline

Outline

Oct 8 , 2014

Three Parts of Work

- *Sheng Wei*
  - The main point of the paper is to develop an one-gate trojan trigger circuit. The attack circuitry is on TrustHub. TrustHub has various kinds of attacking circtuits' verilog codes.
  - Sheng works on only a small part of the project for developing triggers. He can help us develop the trigger but not the attacking circtuit.
  - Leakage power analysis has been applied for detecting trojans that are off at first and then turned on later. For example, trigger can comes from a counter.

Three Parts of Work

- *Sheng Wei*
  - The main point of the paper is to develop an one-gate trojan trigger circuit. The attack circuitry is on TrustHub. TrustHub has various kinds of attacking circtuits' verilog codes.
  - Sheng works on only a small part of the project for developing triggers. He can help us develop the trigger but not the attacking circtuit.
  - Leakage power analysis has been applied for detecting trojans that are off at first and then turned on later. For example, trigger can comes from a counter.

Three Parts of Work

- *Sheng Wei*
  - The main point of the paper is to develop an one-gate trojan trigger circuit. The attack circuitry is on TrustHub. TrustHub has various kinds of attacking circtuits' verilog codes.
  - Sheng works on only a small part of the project for developing triggers. He can help us develop the trigger but not the attacking circtuit.
  - Leakage power analysis has been applied for detecting trojans that are off at first and then turned on later. For example, trigger can comes from a counter.

Three Parts of Work

- *Sheng Wei*
  - The main point of the paper is to develop an one-gate trojan trigger circuit. The attack circuitry is on TrustHub. TrustHub has various kinds of attacking circtuits' verilog codes.
  - Sheng works on only a small part of the project for developing triggers. He can help us develop the trigger but not the attacking circtuit.
  - Leakage power analysis has been applied for detecting trojans that are off at first and then turned on later. For example, trigger can comes from a counter.

Second part

- *Ronen*
  - The whole circuit's photonics response is simulated by adding up single gate response. **Gate-to-gate wires are excluded.**
  - There is a space issue with the single gate design. The attenuation for the reflected signal is too small. The way to solve this problem is to change the layout to bring more open space for Ronen.
  - One good way to solve the signal attenuation is to utilize the open space for antenna design. My idea is to fill the antenna with the rest of the circuit. Ronen agrees that it will bring the reflected back signal much stronger.
  - Ronen needs a month after I handling him the standard cells. So that will push my work's deadline to the end of Oct.

Second part

- *Ronen*
  - The whole circuit's photonics response is simulated by adding up single gate response. **Gate-to-gate wires are excluded.**
  - There is a space issue with the single gate design. The attenuation for the reflected signal is too small. The way to solve this problem is to change the layout to bring more open space for Ronen.
  - One good way to solve the signal attenuation is to utilize the open space for antenna design. My idea is to fill the antenna with the rest of the circuit. Ronen agrees that it will bring the reflected back signal much stronger.
  - Ronen needs a month after I handling him the standard cells. So that will push my work's deadline to the end of Oct.

Second part

- *Ronen*
  - The whole circuit's photonics response is simulated by adding up single gate response. **Gate-to-gate wires are excluded.**
  - There is a space issue with the single gate design. The attenuation for the reflected signal is too small. The way to solve this problem is to change the layout to bring more open space for Ronen.
  - One good way to solve the signal attenuation is to utilize the open space for antenna design. My idea is to fill the antenna with the rest of the circuit. Ronen agrees that it will bring the reflected back signal much stronger.
  - Ronen needs a month after I handling him the standard cells. So that will push my work's deadline to the end of Oct.

Second part

- *Ronen*
  - The whole circuit's photonics response is simulated by adding up single gate response. **Gate-to-gate wires are excluded.**
  - There is a space issue with the single gate design. The attenuation for the reflected signal is too small. The way to solve this problem is to change the layout to bring more open space for Ronen.
  - One good way to solve the signal attenuation is to utilize the open space for antenna design. My idea is to fill the antenna with the rest of the circuit. Ronen agrees that it will bring the reflected back signal much stronger.
  - Ronen needs a month after I handling him the standard cells. So that will push my work's deadline to the end of Oct.

Second part

- *Ronen*
  - The whole circuit's photonics response is simulated by adding up single gate response. **Gate-to-gate wires are excluded.**
  - There is a space issue with the single gate design. The attenuation for the reflected signal is too small. The way to solve this problem is to change the layout to bring more open space for Ronen.
  - One good way to solve the signal attenuation is to utilize the open space for antenna design. My idea is to fill the antenna with the rest of the circuit. Ronen agrees that it will bring the reflected back signal much stronger.
  - Ronen needs a month after I handling him the standard cells. So that will push my work's deadline to the end of Oct.

Third Part

- *CAD tools*
  - I can see the layout, but the bindkeys have not been set. So I can not change anything. Once I get that done, I will contact Ronen for single gate simulation.
  - 130nm Design rules have not been found for Ronen's design. I will also get this part as fast as possible.
  - Jamie can not help and I can not get help from Cadence. So his help from Cadence will be lagged for a long time.

Third Part

- *CAD tools*
  - I can see the layout, but the bindkeys have not been set. So I can not change anything. Once I get that done, I will contact Ronen for single gate simulation.
  - 130nm Design rules have not been found for Ronen's design. I will also get this part as fast as possible.
  - Jamie can not help and I can not get help from Cadence. So his help from Cadence will be lagged for a long time.

Third Part

- *CAD tools*
  - I can see the layout, but the bindkeys have not been set. So I can not change anything. Once I get that done, I will contact Ronen for single gate simulation.
  - 130nm Design rules have not been found for Ronen's design. I will also get this part as fast as possible.
  - Jamie can not help and I can not get help from Cadence. So his help from Cadence will be lagged for a long time.

Third Part

- *CAD tools*
  - I can see the layout, but the bindkeys have not been set. So I can not change anything. Once I get that done, I will contact Ronen for single gate simulation.
  - 130nm Design rules have not been found for Ronen's design. I will also get this part as fast as possible.
  - Jamie can not help and I can not get help from Cadence. So his help from Cadence will be lagged for a long time.

Outline

- **CAD tools** Currently, we will work on the Nangate technology instead of 130nm. Current known ways to do the power simulation is to use encounter to simulate the vcd file from modelsim, which is not accurate. The accurate simulation needs extraction from layout.
- **Testbench** Testbench can be downloaded from Trusthub. We need to find a testbench that makes sense in terms of area, leakage power and layout.

- **CAD tools** Currently, we will work on the Nangate technology instead of 130nm. Current known ways to do the power simulation is to use encounter to simulate the vcd file from modelsim, which is not accurate. The accurate simulation needs extraction from layout.
- **Testbench** Testbench can be downloaded from Trusthub. We need to find a testbench that makes sense in terms of area, leakage power and layout.

- **CAD tools** Currently, we will work on the Nangate technology instead of 130nm. Current known ways to do the power simulation is to use encounter to simulate the vcd file from modelsim, which is not accurate. The accurate simulation needs extraction from layout.
- **Testbench** Testbench can be downloaded from Trusthub. We need to find a testbench that makes sense in terms of area, leakage power and layout.

Time Stamp

Oct 15 , 2014

Outline

A *'Good Trojan'* in Information Leakage

Size

The area of added circuit must be small due to extra energy consumption and die size.

Side-Channel Leakage

In order to leak information, the circuit must consume more energy for secret info transmitting. A *'good Trojan'* must consume energy as small as possible but leak information as much as possible.

Trigger

The attacker must be hard to be triggered. This is due to extensive functional testing.

A *'Good Trojan'* in Information Leakage

Size

The area of added circuit must be small due to extra energy consumption and die size.

Side-Channel Leakage

In order to leak information, the circuit must consume more energy for secret info transmitting. A *'good Trojan'* must consume energy as small as possible but leak information as much as possible.

Trigger

The attacker must be hard to be triggered. This is due to extensive functional testing.

A *'Good Trojan'* in Information Leakage

Size

The area of added circuit must be small due to extra energy consumption and die size.

Side-Channel Leakage

In order to leak information, the circuit must consume more energy for secret info transmitting. A *'good Trojan'* must consume energy as small as possible but leak information as much as possible.

Trigger

The attacker must be hard to be triggered. This is due to extensive functional testing.

A *'Good Trojan'* in Information Leakage

Size

The area of added circuit must be small due to extra energy consumption and die size.

Side-Channel Leakage

In order to leak information, the circuit must consume more energy for secret info transmitting. A *'good Trojan'* must consume energy as small as possible but leak information as much as possible.

Trigger

The attacker must be hard to be triggered. This is due to extensive functional testing.

Outline

AES-T100 Explanation

- *Side Channel Attack* This method is implemented with power side channel attack. It leaks the secret information through CDMA channel.
- *CDMA Leakage* The attacking circuit consists of a PRNG for spread spectrum. In this way, the leakage information will be distributed through many cycles so that the leakage power analysis can not detect the information
- *Demo from Paper* It is implemented with FPGA. The author used 8 flipflops to mimic a huge capacitor.

AES-T100 Explanation

- *Side Channel Attack* This method is implemented with power side channel attack. It leaks the secret information through CDMA channel.
- *CDMA Leakage* The attacking circuit consists of a PRNG for spread spectrum. In this way, the leakage information will be distributed through many cycles so that the leakage power analysis can not detect the information
- *Demo from Paper* It is implemented with FPGA. The author used 8 flipflops to mimic a huge capacitor.

AES-T100 Explanation

- *Side Channel Attack* This method is implemented with power side channel attack. It leaks the secret information through CDMA channel.
- *CDMA Leakage* The attacking circuit consists of a PRNG for spread spectrum. In this way, the leakage information will be distributed through many cycles so that the leakage power analysis can not detect the information
- *Demo from Paper* It is implemented with FPGA. The author used 8 flipflops to mimic a huge capacitor.

AES-T100 Explanation

- *Side Channel Attack* This method is implemented with power side channel attack. It leaks the secret information through CDMA channel.
- *CDMA Leakage* The attacking circuit consists of a PRNG for spread spectrum. In this way, the leakage information will be distributed through many cycles so that the leakage power analysis can not detect the information
- *Demo from Paper* It is implemented with FPGA. The author used 8 flipflops to mimic a huge capacitor.

AES-T100

- **Functionality** Leaks the keys of AES.
- **Trigger Condition** Always on.
- **Location** Highlighted.

AES-T100

- **Functionality** Leaks the keys of AES.
- **Trigger Condition** Always on.
- **Location** Highlighted.

AES-T100

- **Functionality** Leaks the keys of AES.
- **Trigger Condition** Always on.
- **Location** Highlighted.

AES-T100

- **Functionality** Leaks the keys of AES.
- **Trigger Condition** Always on.
- **Location** Highlighted.

Trojan Free Layout

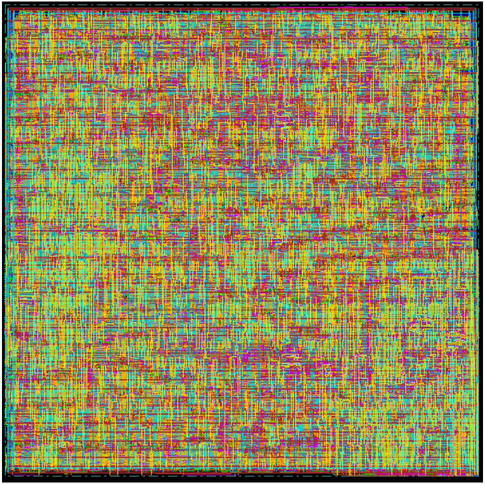

Figure: AES-T100 Trojan Free Circuit

Trojan Free Layout Without Filler Cells

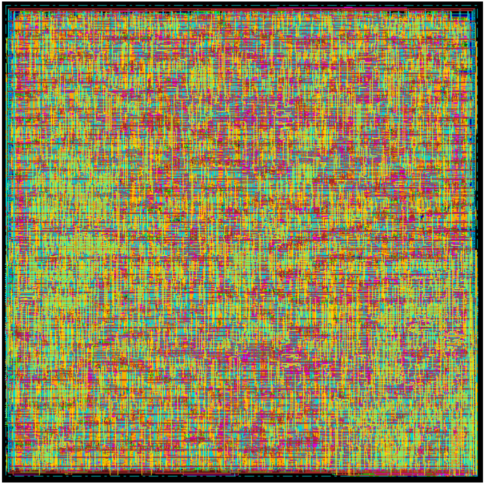

Figure: AES-T100 Trojan Free Circuit without Filler Cells

Trojan In Layout

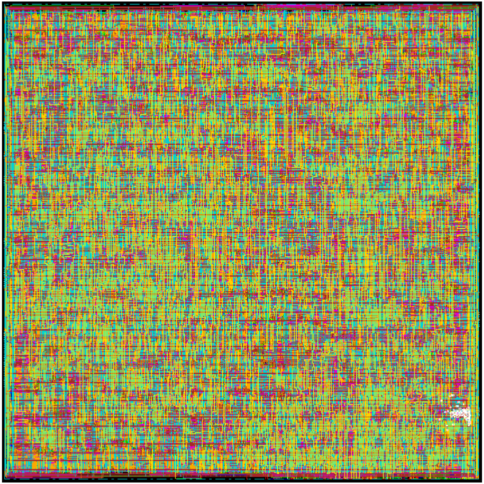

Figure: AES-T100 Trojan Inserted Circuit

Trojan Free Layout Without Filler Cells

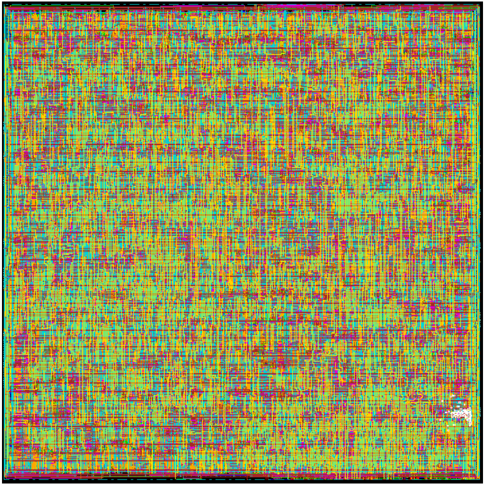

Figure: AES-T100 Trojan Inserted Circuit without Filler Cells

Outline

1. Preparation Work
   - Contacting People
   - Conclusion
2. **Layout of Hardware Trojan Circuits**
   - Specs for Hidding HT
   - HT insertion AES-T100
   - Dummy Trojan
3. Results
   - Single Gate Simulation
   - Multiple Gates Simulation
   - Real Circuit Simulation
   - Power Analysis Results

b15-T100

- **Functionality** Slows down part of the cicuit by reducing the clock frequency by half.
- **Trigger Condition** Observes 0xFF for the address bus for bits 8-15.
- **Location** Tightly placed at the bottom left section of the layout.
- *P&R* **Problem** I did not finish place and route due to ec535 hw due.....

b15-T100

- **Functionality** Slows down part of the cicuit by reducing the clock frequency by half.
- **Trigger Condition** Observes 0xFF for the address bus for bits 8-15.
- **Location** Tightly placed at the bottom left section of the layout.
- *P&R* **Problem** I did not finish place and route due to ec535 hw due.....

b15-T100

- **Functionality** Slows down part of the cicuit by reducing the clock frequency by half.
- **Trigger Condition** Observes 0xFF for the address bus for bits 8-15.
- **Location** Tightly placed at the bottom left section of the layout.
- *P&R* **Problem** I did not finish place and route due to ec535 hw due.....

b15-T100

- **Functionality** Slows down part of the cicuit by reducing the clock frequency by half.
- **Trigger Condition** Observes 0xFF for the address bus for bits 8-15.
- **Location** Tightly placed at the bottom left section of the layout.
- *P&R* **Problem** I did not finish place and route due to ec535 hw due.....

b15-T100

- **Functionality** Slows down part of the cicuit by reducing the clock frequency by half.
- **Trigger Condition** Observes 0xFF for the address bus for bits 8-15.
- **Location** Tightly placed at the bottom left section of the layout.
- *P&R* **Problem** I did not finish place and route due to ec535 hw due.....

Outline

Single Gate Simulation

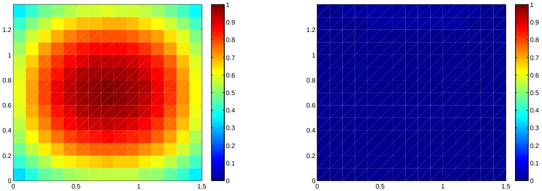

Figure: Single Gate Simulation Comparison

Outline

Circuit with Trojans Response

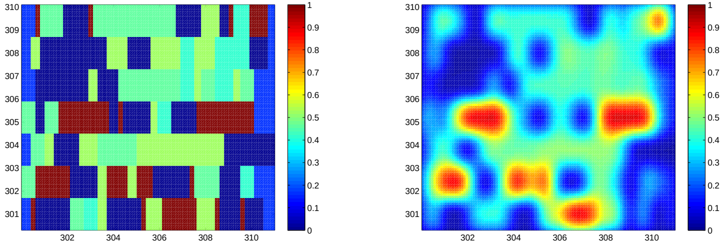

Figure: Circuit with Trojans

Circuit without Trojans

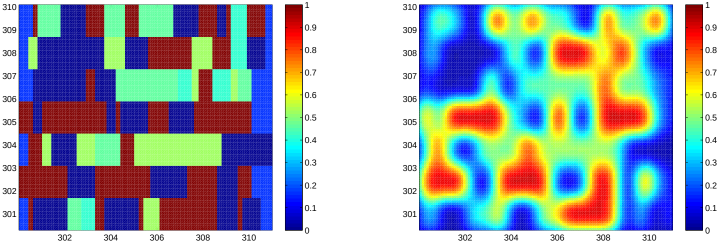

Figure: Circuit without Trojans

Response Comparison

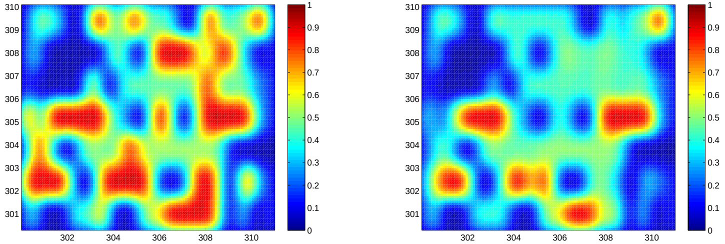

Figure: Response Comparison

Error Rate of False Alarm

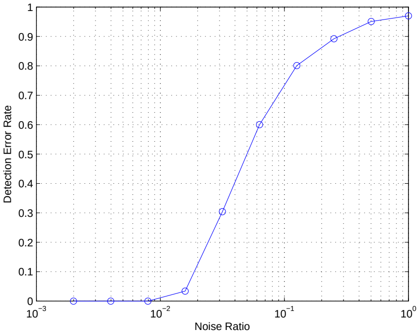

Figure: Error Rate of False Alarm

Error Rate of Miss Test

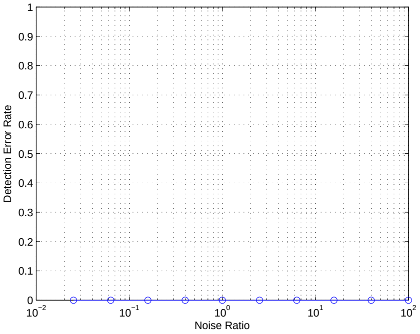

Figure: Error Rate of Miss Test

Outline

Trojan Free Response

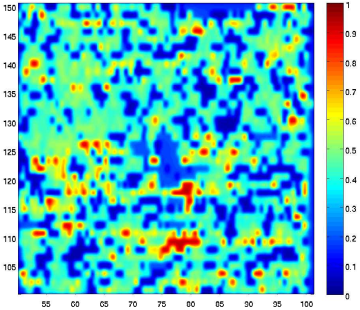

Figure: Trojan Free Response

Trojan In Response

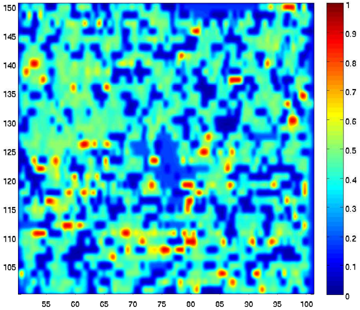

Figure: Trojan In Response

Error Rate of False Alarm

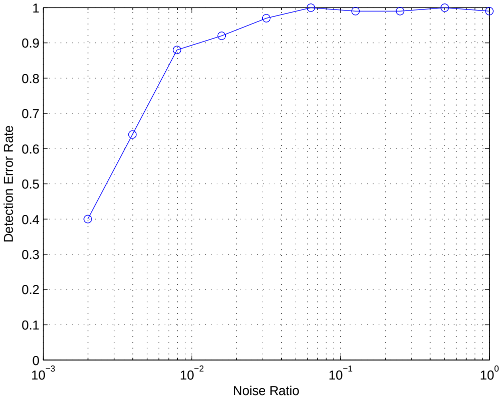

Figure: Error Rate of False Alarm

Error Rate of Miss Test

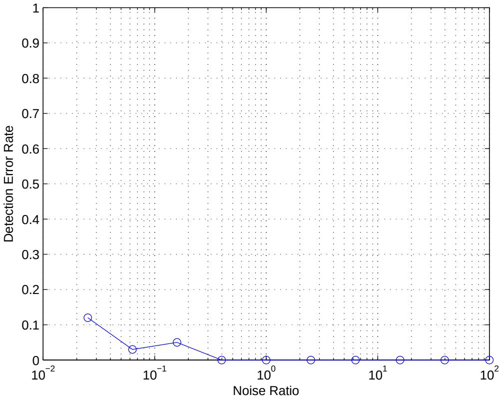

Figure: Error Rate of Miss Test

Outline

1. Preparation Work
    - Contacting People
    - Conclusion
2. Layout of Hardware Trojan Circuits
    - Specs for Hidding HT
    - HT insertion AES-T100
    - Dummy Trojan
3. **Results**
    - Single Gate Simulation
    - Multiple Gates Simulation
    - Real Circuit Simulation
    - **Power Analysis Results**

Power Analysis Results

Type of Circuit	Power with Trojan	Internal	Dynamic	Leakage	Power without Trojan	Internal	Dynamic	Leakage
AES100	175.4	60.75	111.8	2.857	172.2	59.8	109.6	2.813
AES200	171	59.49	108.7	2.796	172.2	59.8	109.6	2.813
AES1000	174	61.39	109.7	2.859	172.2	59.8	109.6	2.813
PIC100	0.68	0.428	0.2103	0.04196	0.5248	0.3727	0.114	0.03811
PIC200	0.4797	0.2617	0.1844	0.0336	0.5248	0.3727	0.114	0.03811
PIC300	0.264	0.09332	0.136	0.03472	0.5248	0.3727	0.114	0.03811

Table A Brief Summary of Power Analysis Results (Units : 1mW)