A Study on Hardware Trojan Insertion into Asynchronous NoC Router

Koutaro Inaba*, Tomohiro Yoneda**, Masashi Imai*
*Hirosaki University
**National Institute of Informatics
Japan

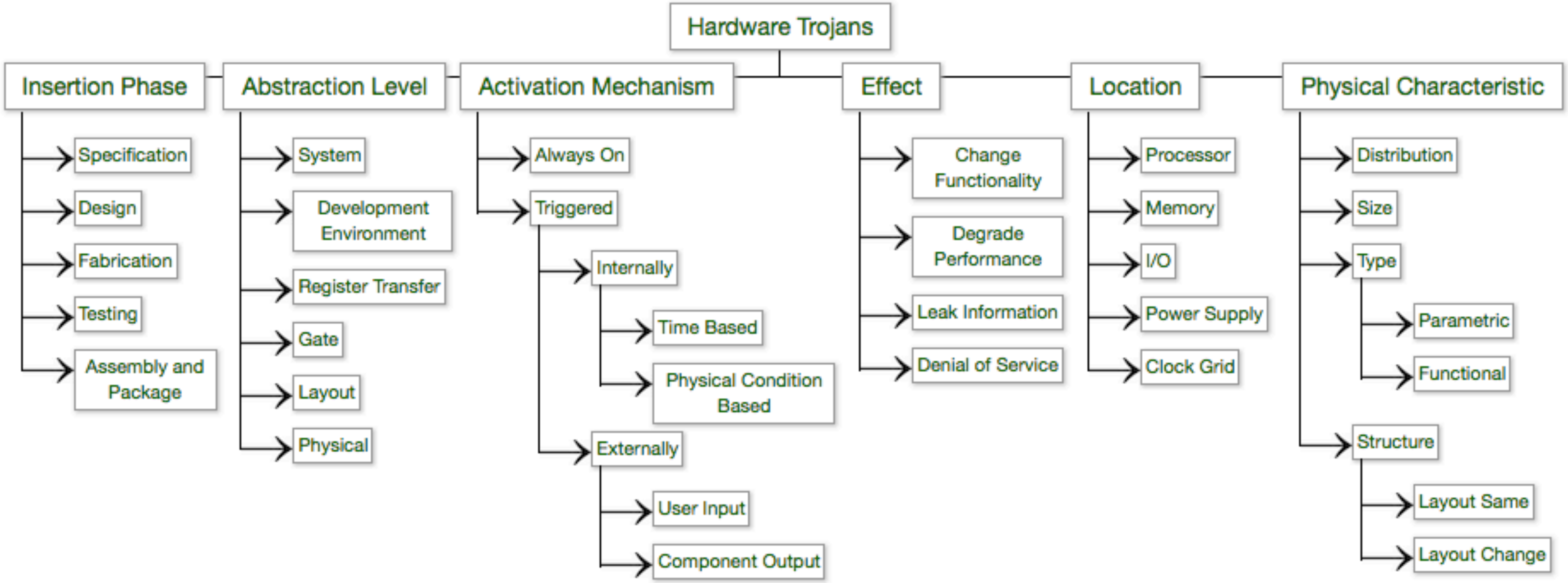
Background

- MPSoCs (Multi-Processor System-on-a-Chips) have been developed and used
  - MPSoCs integrate third party IP cores
  - Designers may use outsourcing developers
- The number of fabless companies is nowadays increasing

Hardware Trojan threats caused by adversaries and untrusted foundries have become one of the serious issues

Background

- Hardware Trojan: malicious modification of the target integrated circuits
  - Trojan taxonomy example [1]



- Hardware Trojans
  - Insertion Phase
    - Specification
    - Design
    - Fabrication
    - Testing
    - Assembly and Package
  - Abstraction Level
    - System
    - Development Environment
    - Register Transfer
    - Gate
    - Layout
    - Physical
  - Activation Mechanism
    - Always On
    - Triggered
      - Internally
        - Time Based
        - Physical Condition Based
      - Externally
        - User Input
        - Component Output
  - Effect
    - Change Functionality
    - Degrade Performance
    - Leak Information
    - Denial of Service
  - Location
    - Processor
    - Memory
    - I/O
    - Power Supply
    - Clock Grid
  - Physical Characteristic
    - Distribution
    - Size
    - Type
      - Parametric
      - Functional
    - Structure
      - Layout Same
      - Layout Change

[1] https://www.trust-hub.org/

Motivation

- Trojan device: correctly work until its Trojan trigger is activated
  - Adversaries should have deep knowledge about the target devices
- It is relatively difficult to insert hardware Trojans into asynchronous circuits
  - Asynchronous design styles have not yet been popular

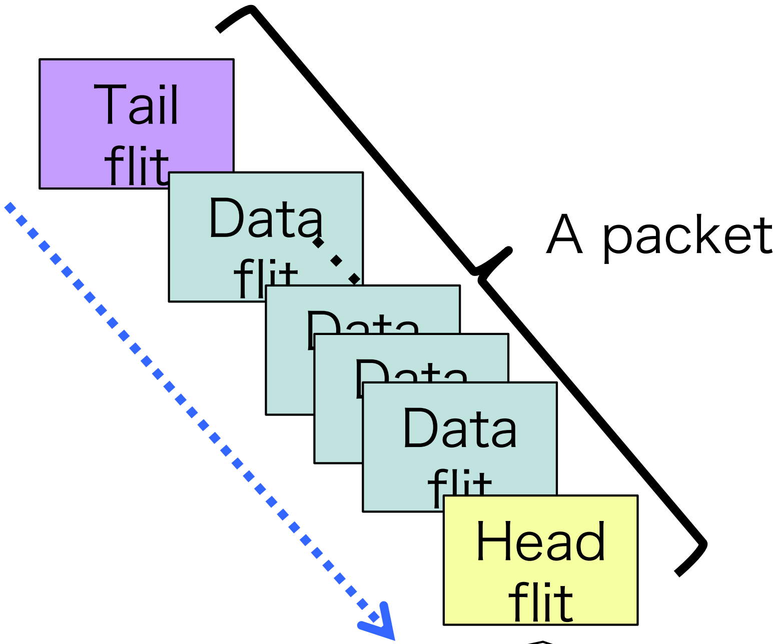
Questions:

- How difficult to insert a hardware Trojan into an asynchronous circuit?
- What is difference between synchronous circuit and asynchronous circuit?

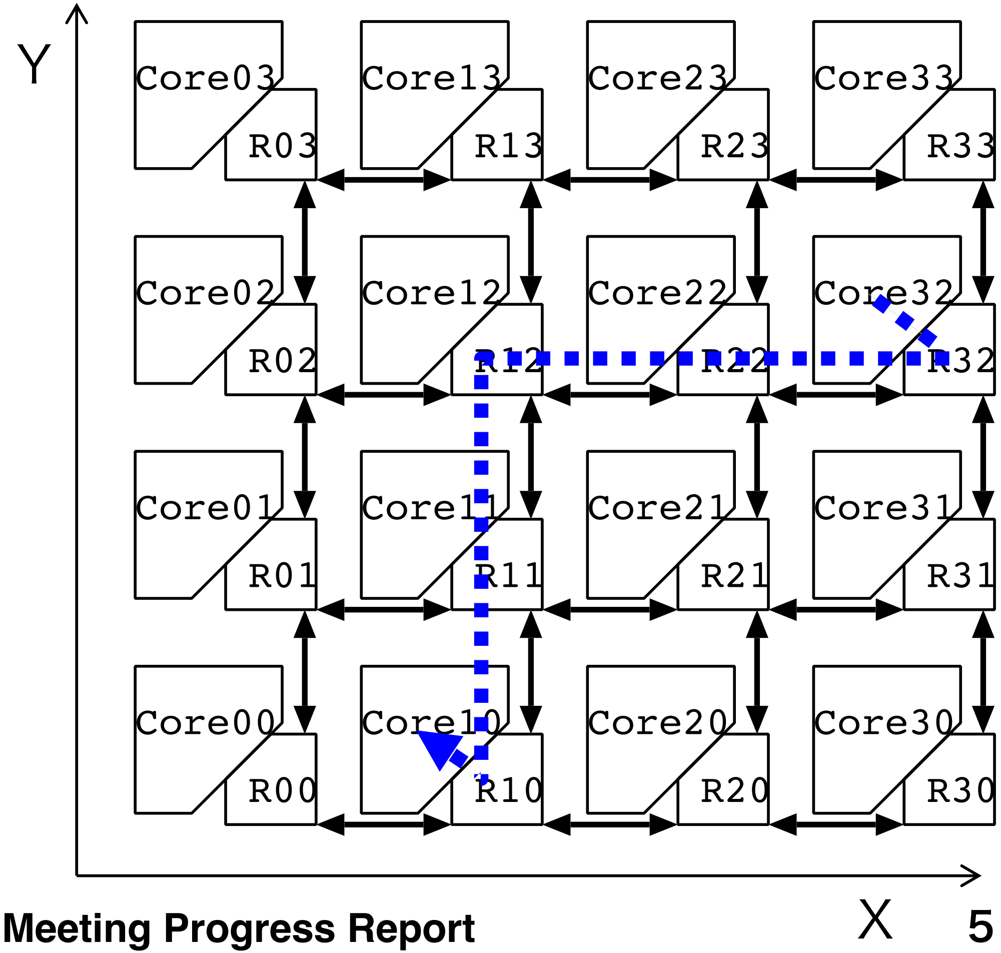
NoC router

Simple NoC router structure is chosen to show the fundamental influence of hardware Trojan

- The network topology is 2D-mesh
- The Flow control is wormhole switching
- The routing algorithm is dimension-order algorithm



- Head flit has the destination information.

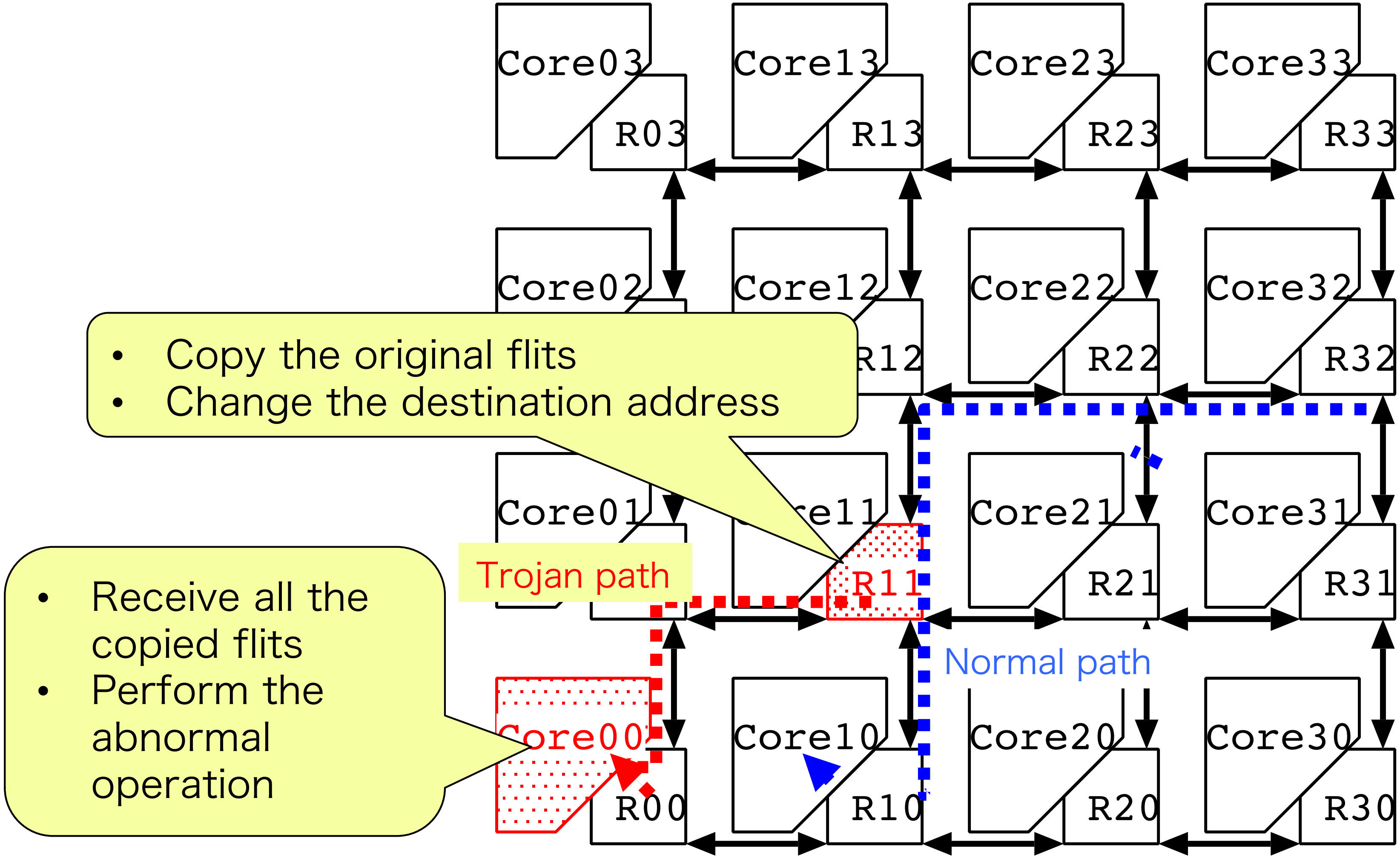


Trojan NoC router

- Aim: to leak the confidential information from NoC chip
- Assumptions:
  - Only one router is changed to the Trojan router in order to avoid large area and power overhead due to hardware Trojan insertion
  - The software in a specified core is also changed
    - Out of scope in this work
- Trojan trigger:
  - The Trojan router receives the specified data flit from the specified core
- Trojan behavior:
  - Copy the original flits and change the destination of the copied head flit to the specified address

Trojan NoC router

- Trojan router: R11
- Abnormal SW core: Core00

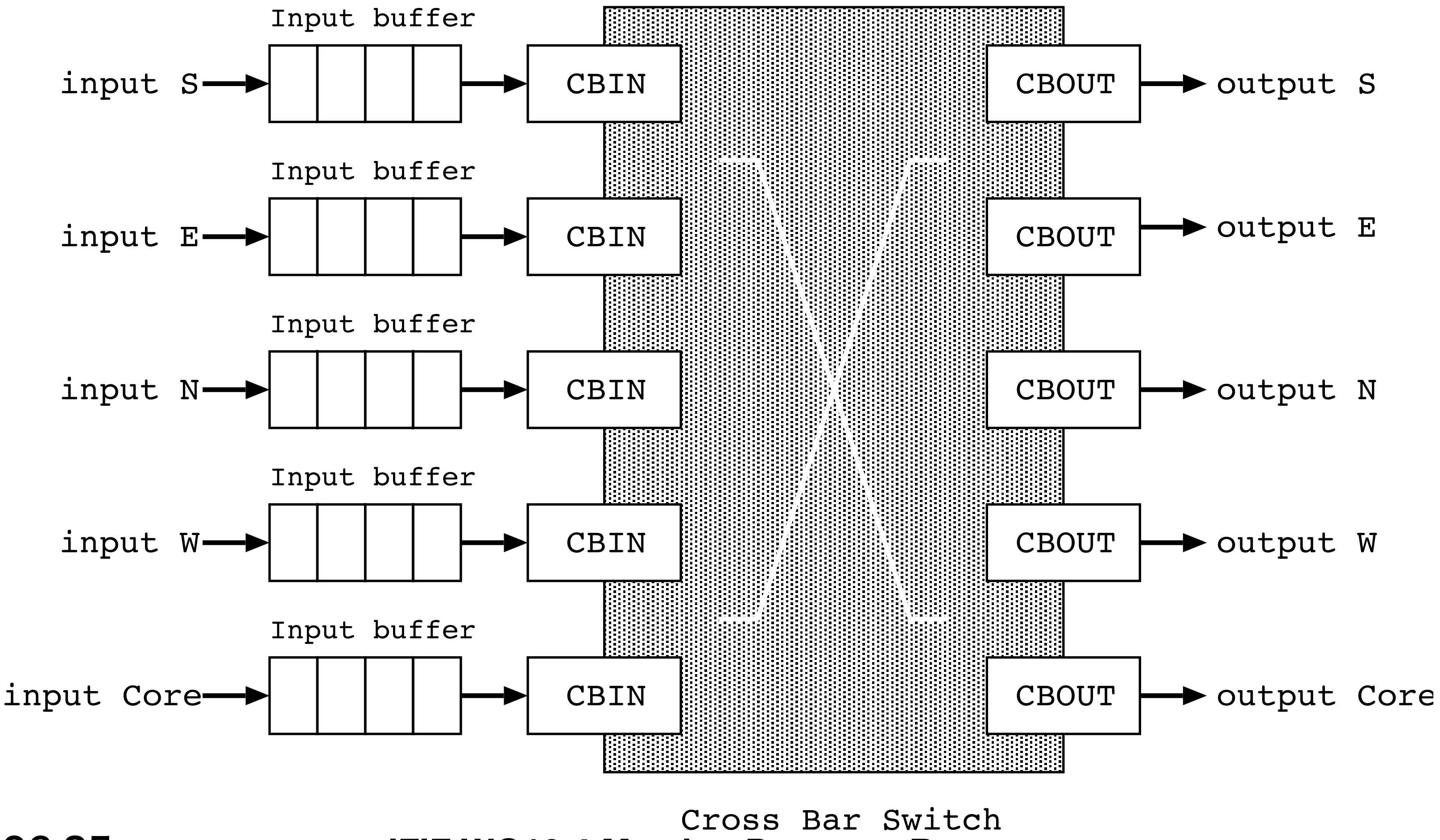


- Copy the original flits
- Change the destination address

- Receive all the copied flits
- Perform the abnormal operation

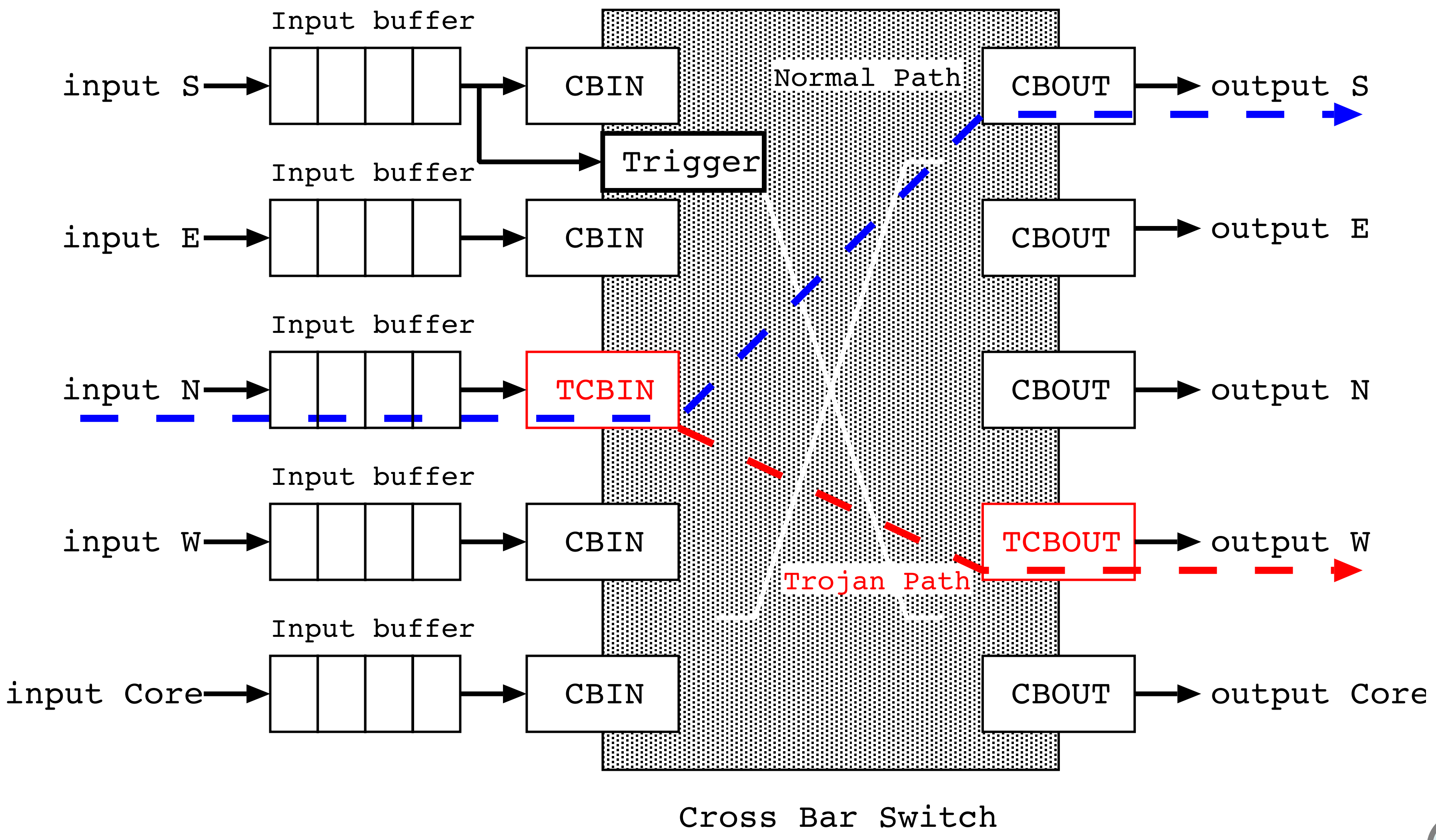
Normal NoC router architecuture

- Five input buffer units
- Cross bar switch unit
  - CBIN (Cross Bar INput)
  - CBOUT (Cross Bar OUTput)



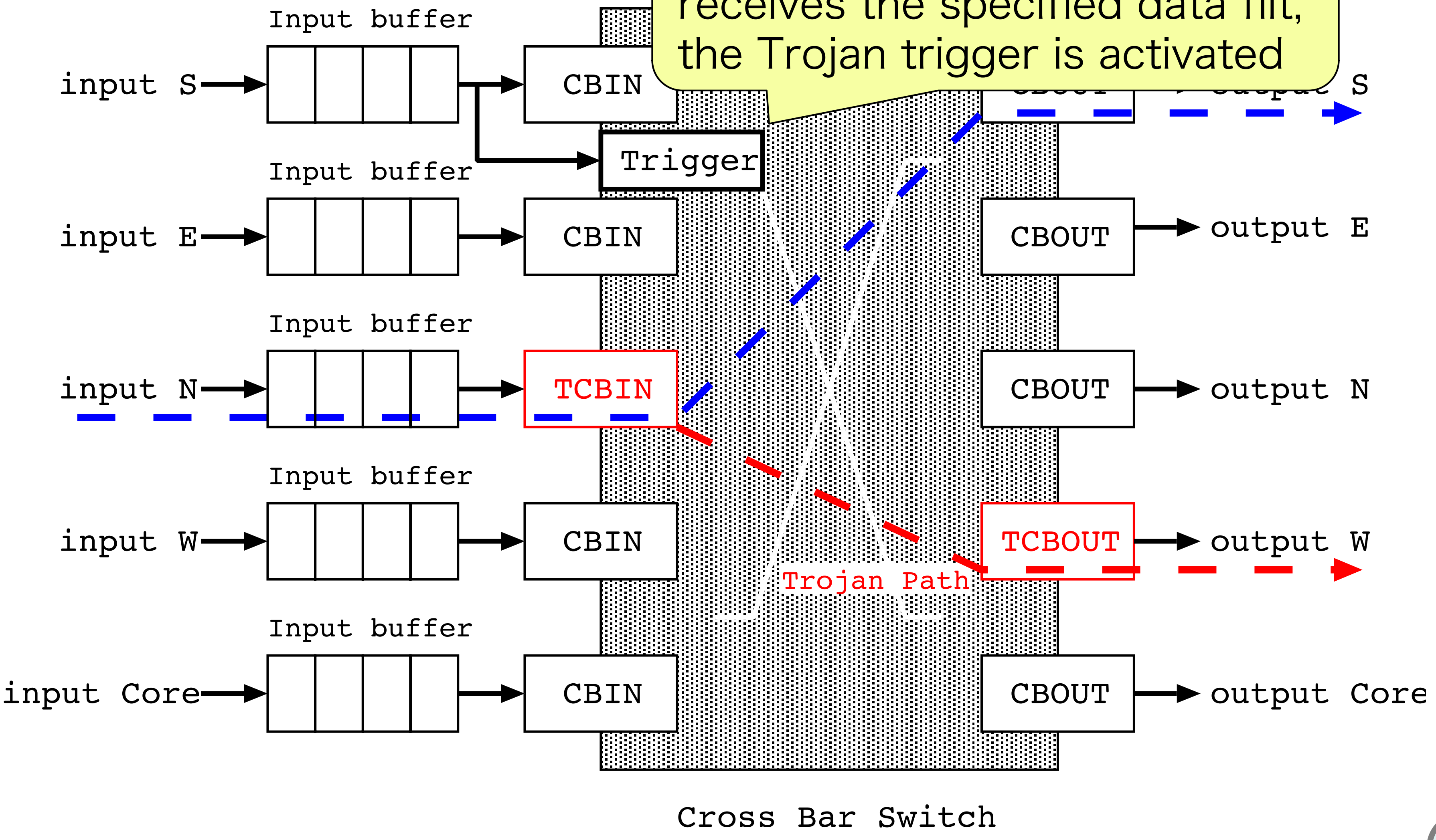
Trojan NoC router architecture

- Trojan router R11



Trojan NoC router architecture

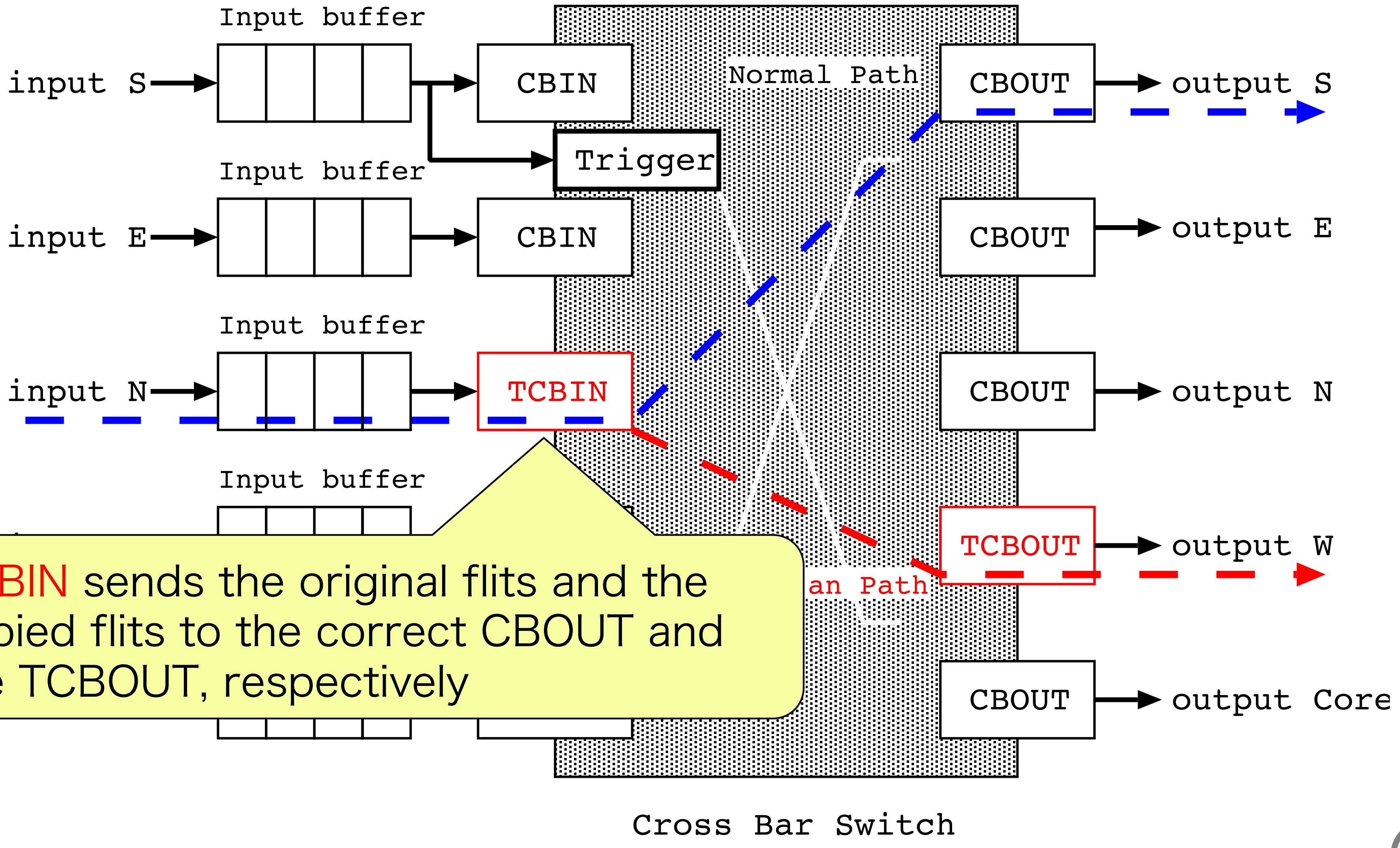
- Trojan router R11



When the trigger circuit receives the specified data flit, the Trojan trigger is activated

Trojan NoC router architecture

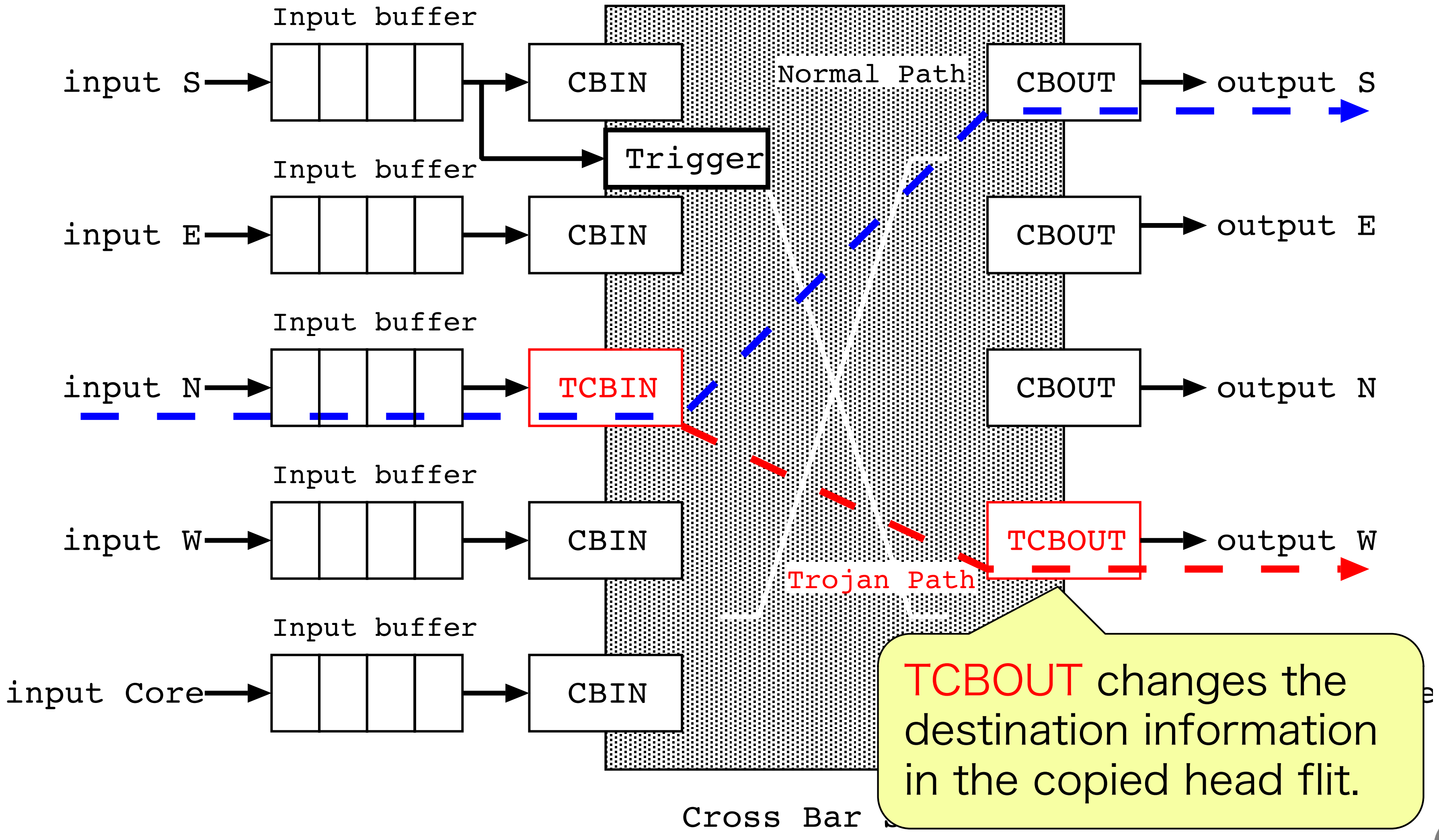
- Trojan router R11



TCBIN sends the original flits and the copied flits to the correct CBOUT and the TCBOUT, respectively

Trojan NoC router architecture

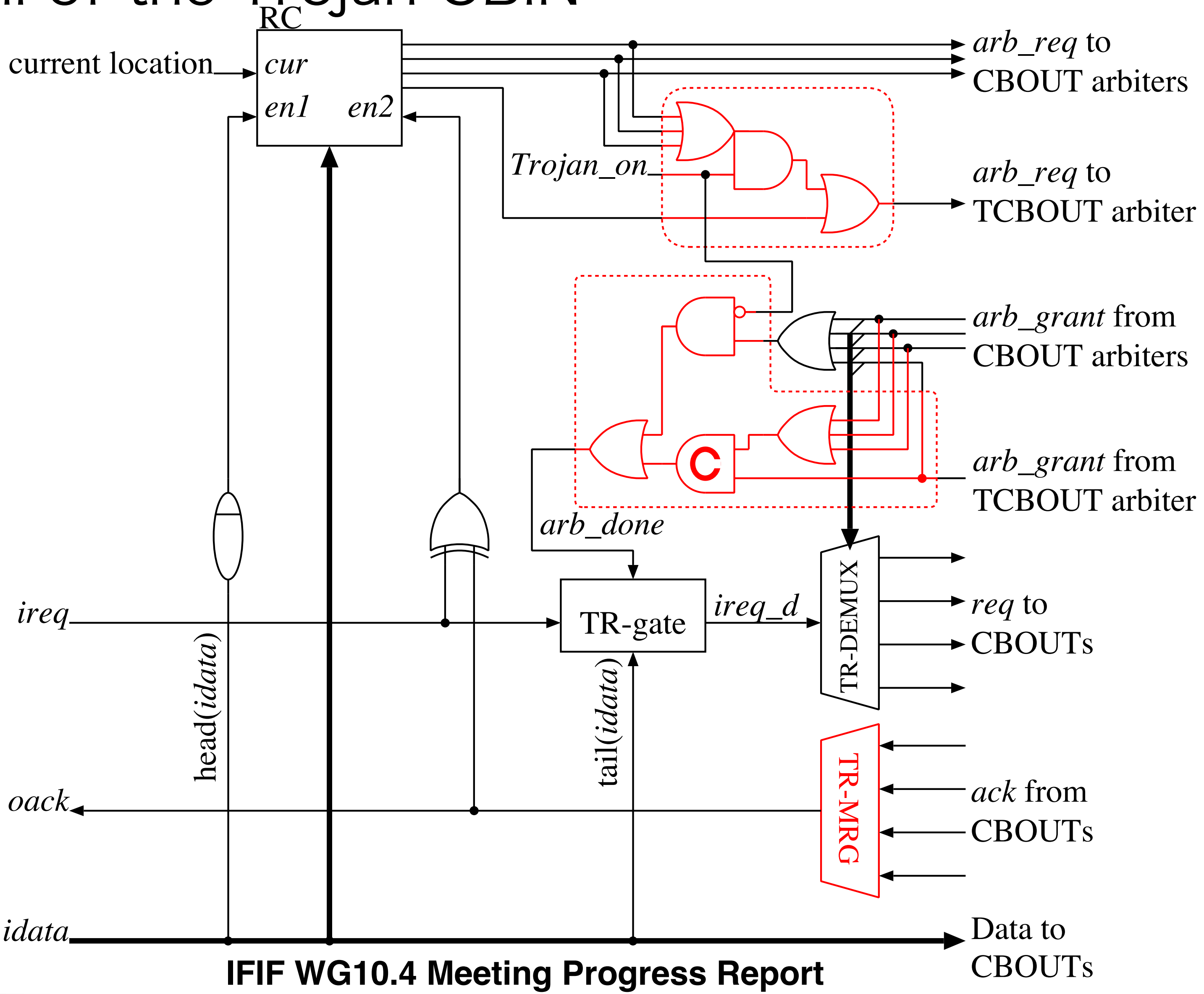
- Trojan router R11



TCBOUT changes the destination information in the copied head flit.

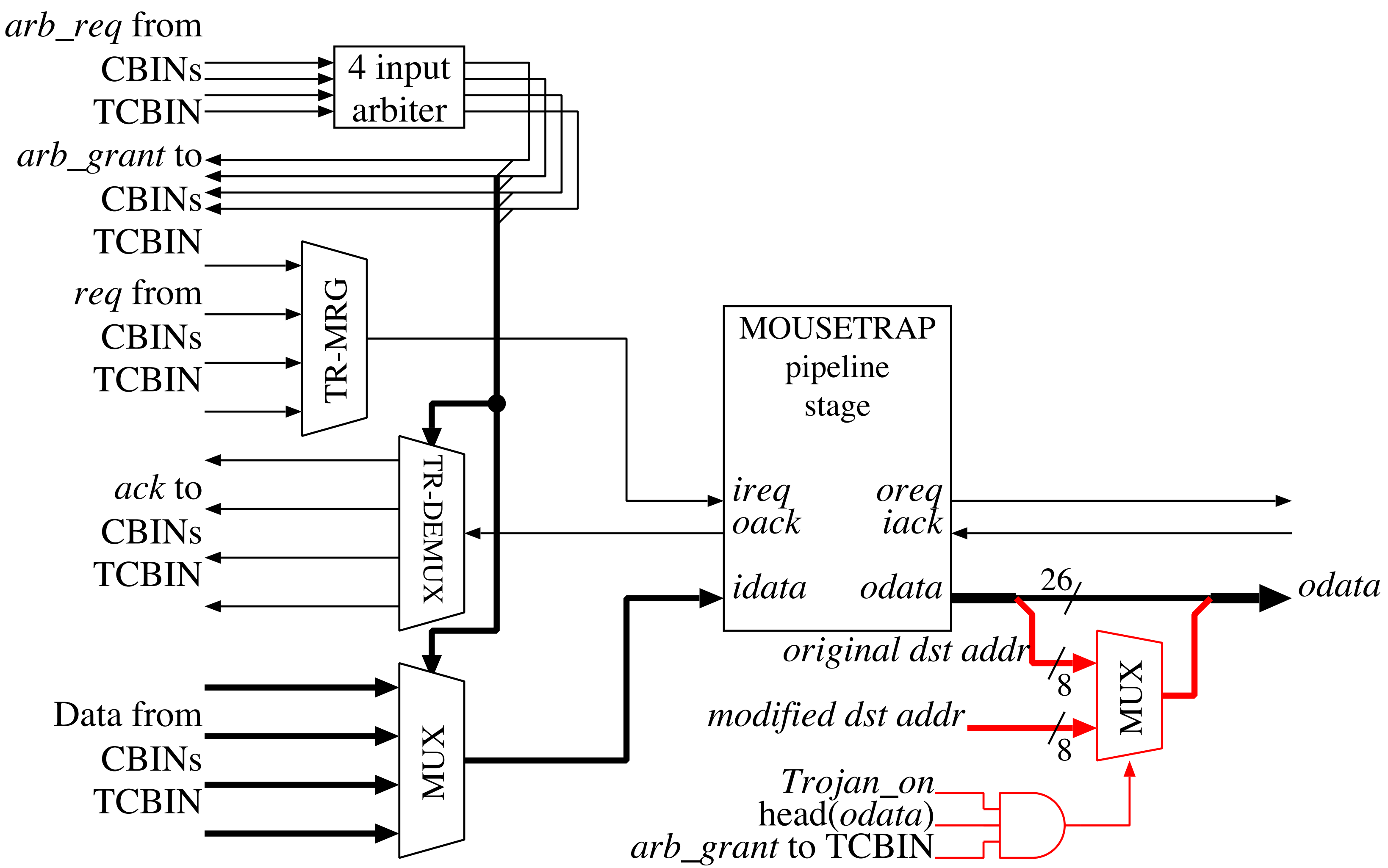
Trojan-CBIN(TCBIN)

Detail of the Trojan CBIN



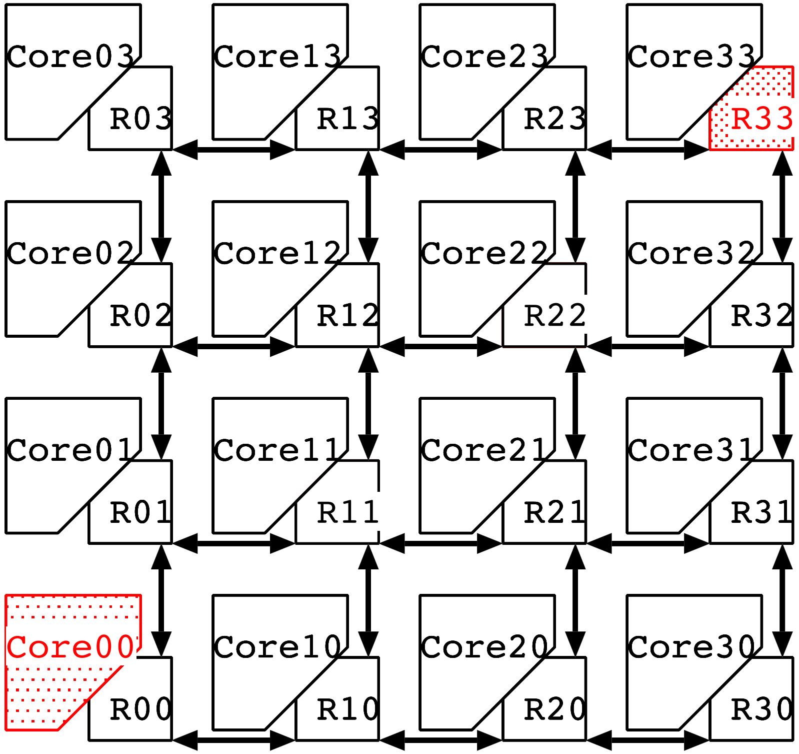
Trojan-CBOUT (TCBOUT)

Detail of the Trojan-CBOUT



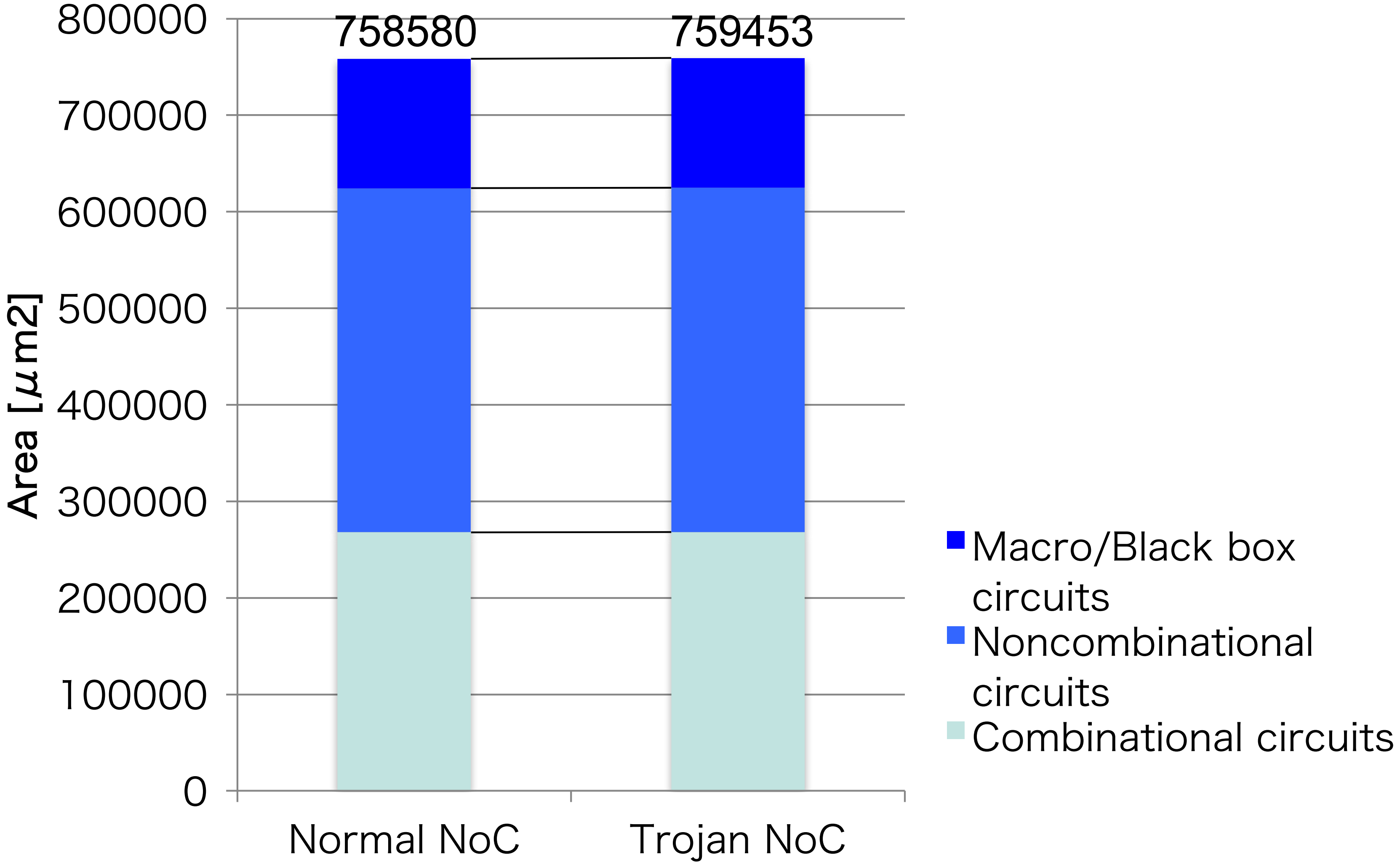
Evaluation

- Hardware Trojan asynchronous NoC routers are designed and evaluated using the 130nm bulk CMOS technology
- The evaluation for comparison is done based on the simulations of synthesized 4 * 4 NoC netlist
  - Uniform random traffics
  - The position of the hardware Trojan is (tx, ty) = (1, 1), (2, 2), or (3, 3)
  - The position of the abnormal SW core is (sx, sy) = (0, 0)
  - Trigger data flit is 34'h3aaaaaaaa



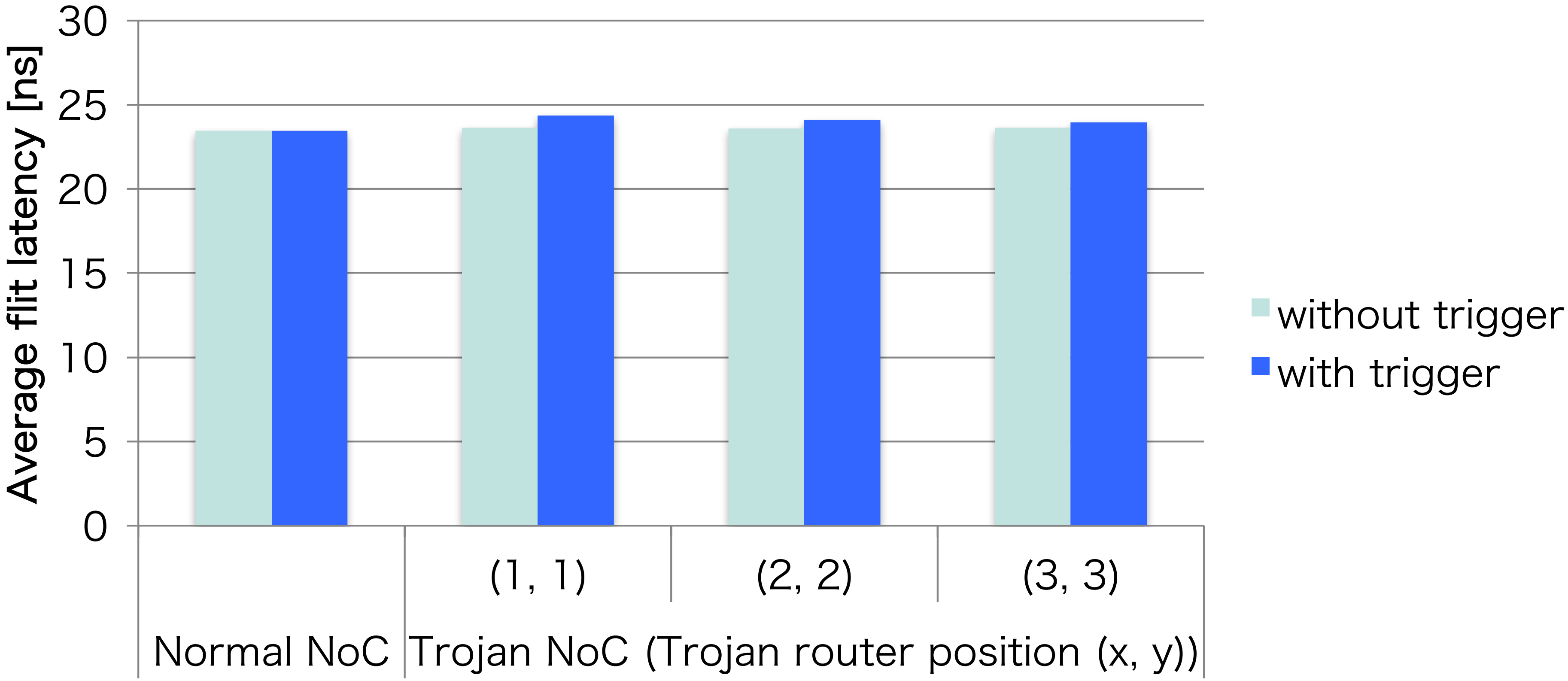
Area comparison of 4 * 4 NoC

- The area overhead is about 0.12%



Average flit latency comparison

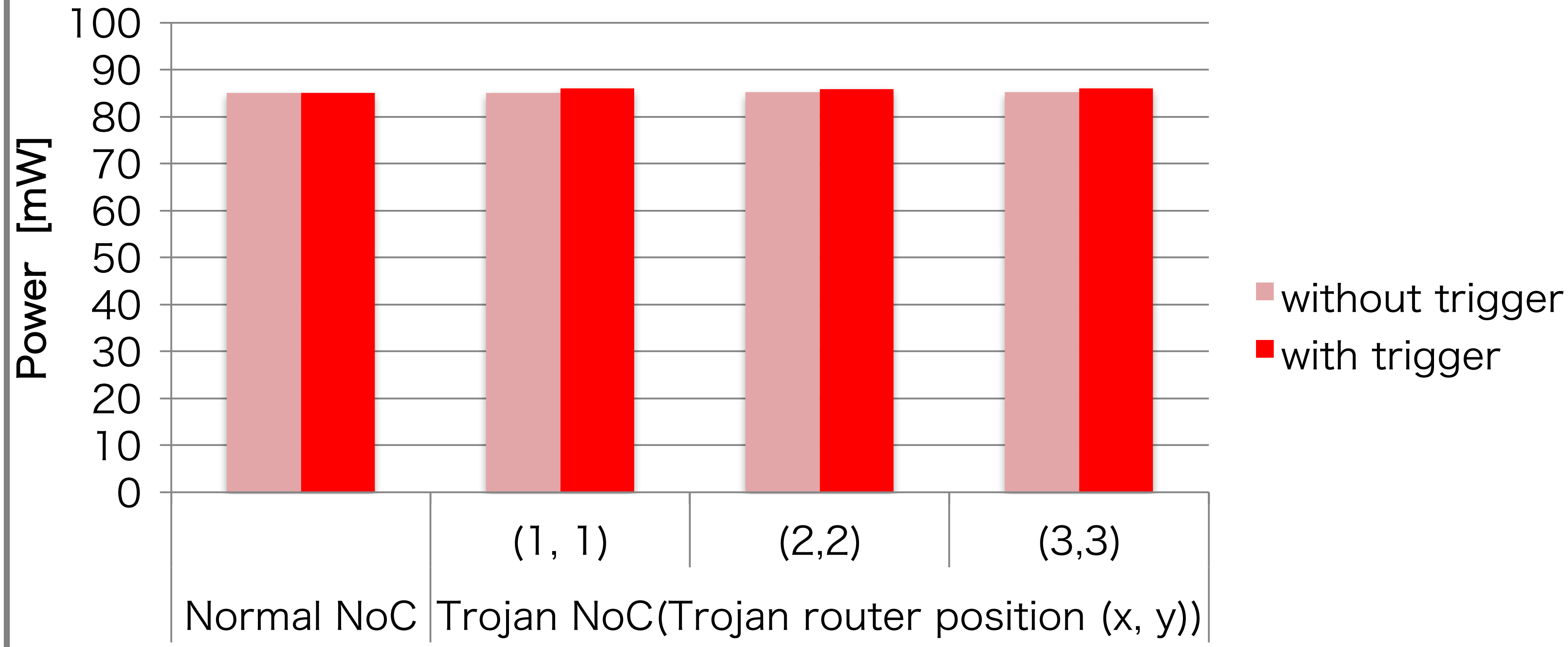
- The average flit latency is calculated based on latencies of all the flits generated during the measurement phase



- The latency are almost the same when the Trojan trigger is not activated
- When Trojan trigger is activated, the latency increases about from 2.0% to 3.8%

Total power comparison of the NoC

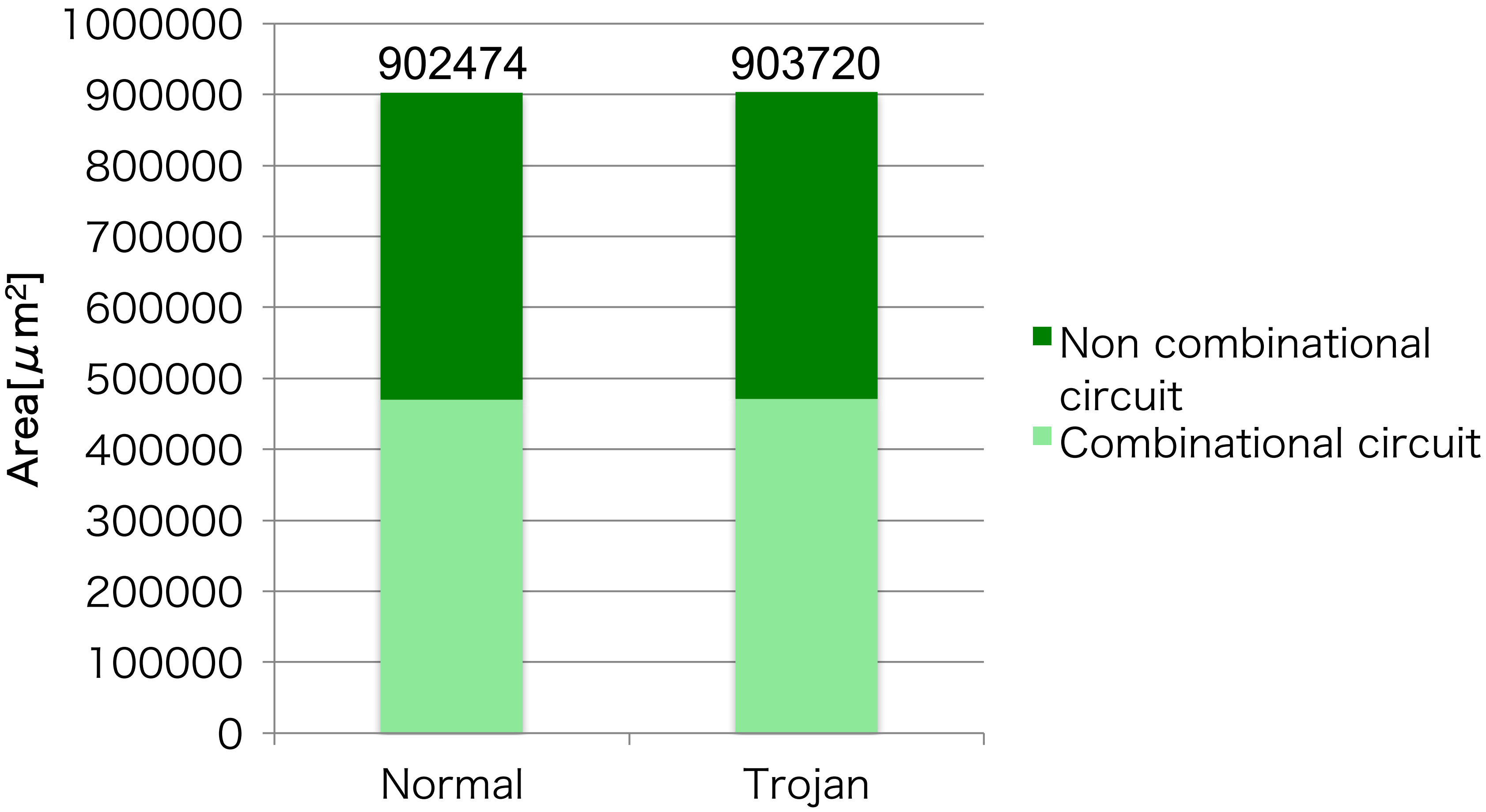
- SAIF(Switching Activity Interchange Format) is used to calculate the power of the hardware Trojan NoC



- The power is almost the same when the Trojan trigger is not activated
- When Trojan trigger is activated, power incleases about from 0.87% to 0.99%

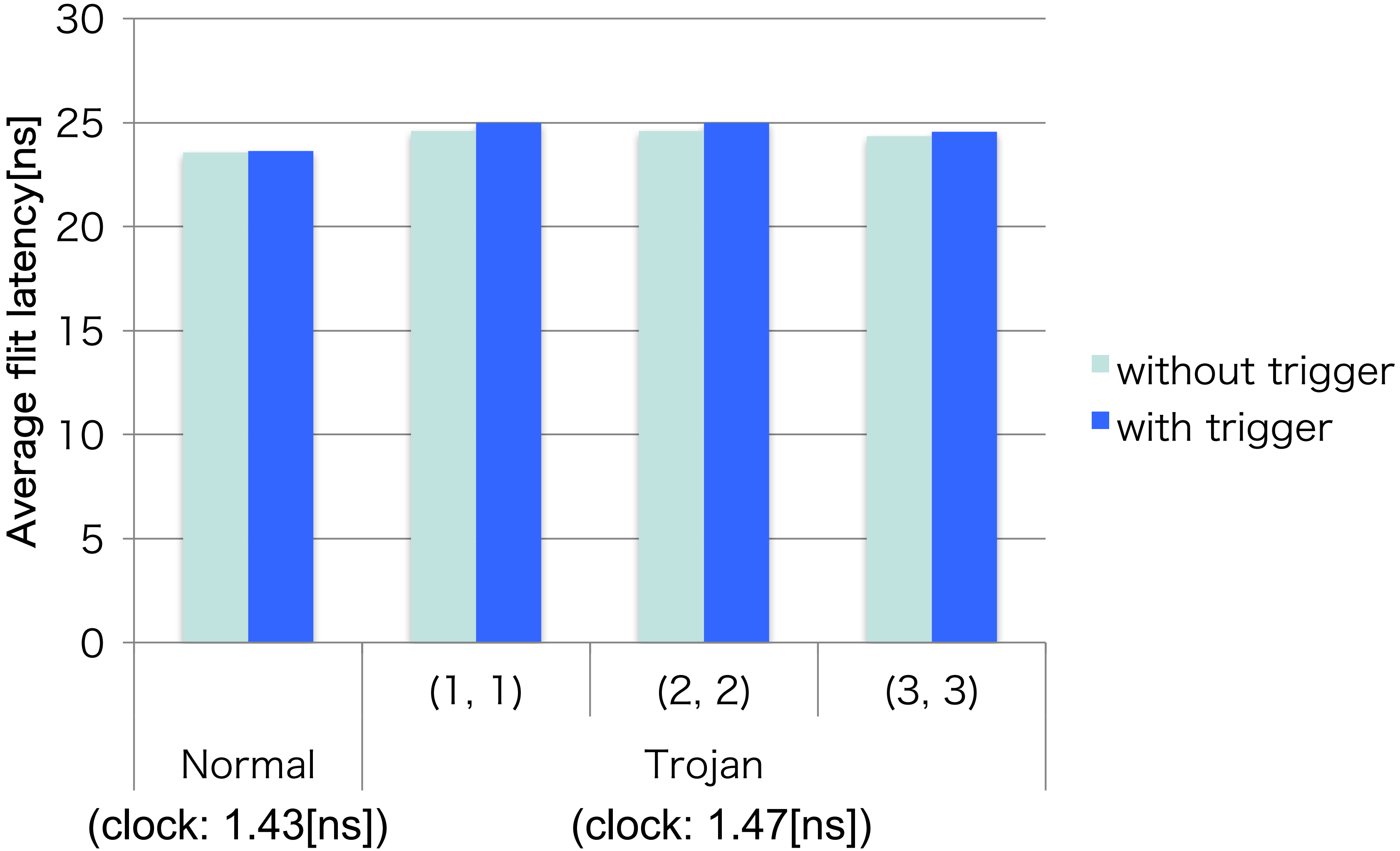
Area comparison of synchronous NoC

- The overhead is about 0.14%



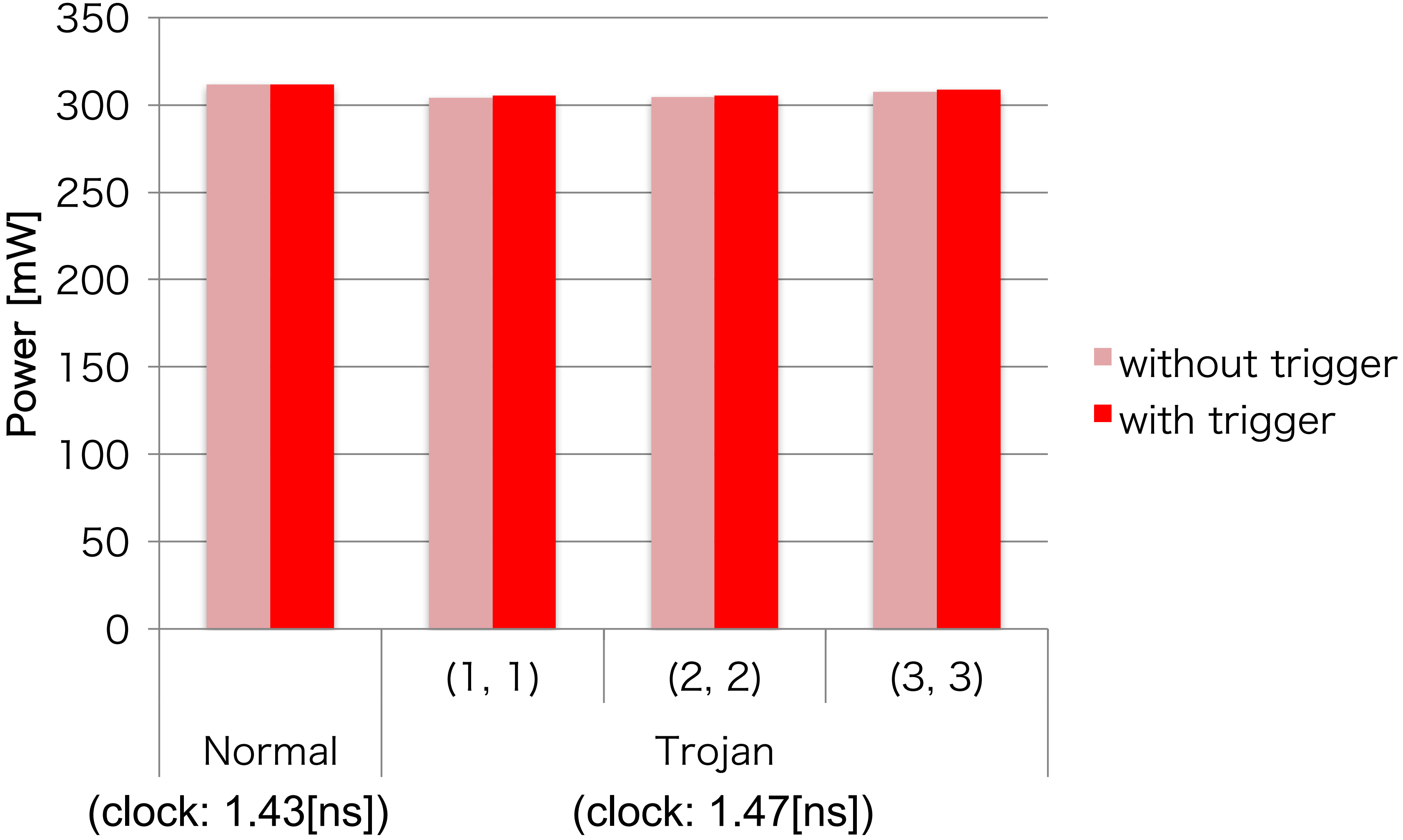
Average flit latency of synchronous NoC

- The average flit latency with trigger condition increases from 4.2% to 6.1%



Power comparison of synchronous NoC

- The power with trigger condition decreases from 1.1% to 2.2% since the clock cycle increases



Comparison between async vs. sync

- The critical path increases due to the Trojan insertion
  - The influence for asynchronous circuits is small
  - The influence for synchronous ones is relatively large

- Overhead comparison

	Asynchronous	Synchronous
Area	0.12%	0.14%
Average latency	2.0% ~ 3.8%	4.2% ~ 6.1%
Power	+0.87% ~ +0.99%	-1.1% ~ -2.2%

Conclusion

- Hardware Trojan threats have become one of the serious issues

- We have designed and evaluated hardware Trojan asynchronous NoC routers based on the MOUSETRAP pipeline templates using the 130nm CMOS technology

- As the result, it is concluded that the overhead of hardware Trojan insertion can be small

Future work

- It is in the scope of our future work to develop a detection method of hardware Trojan in asynchronous circuits and propose a counter method against hardware Trojan threats

Thank you for your kind attention