FDTC 2012

An Efficient Countermeasure against Fault Sensitivity Analysis Using Configurable Delay Blocks

Sho Endo*, Yang Li†, Naofumi Homma*,
Kazuo Sakiyama†, Kazuo Ohta†, Takafumi Aoki*

*Tohoku University, Japan

†University of Electro-Communications, Japan

Outline

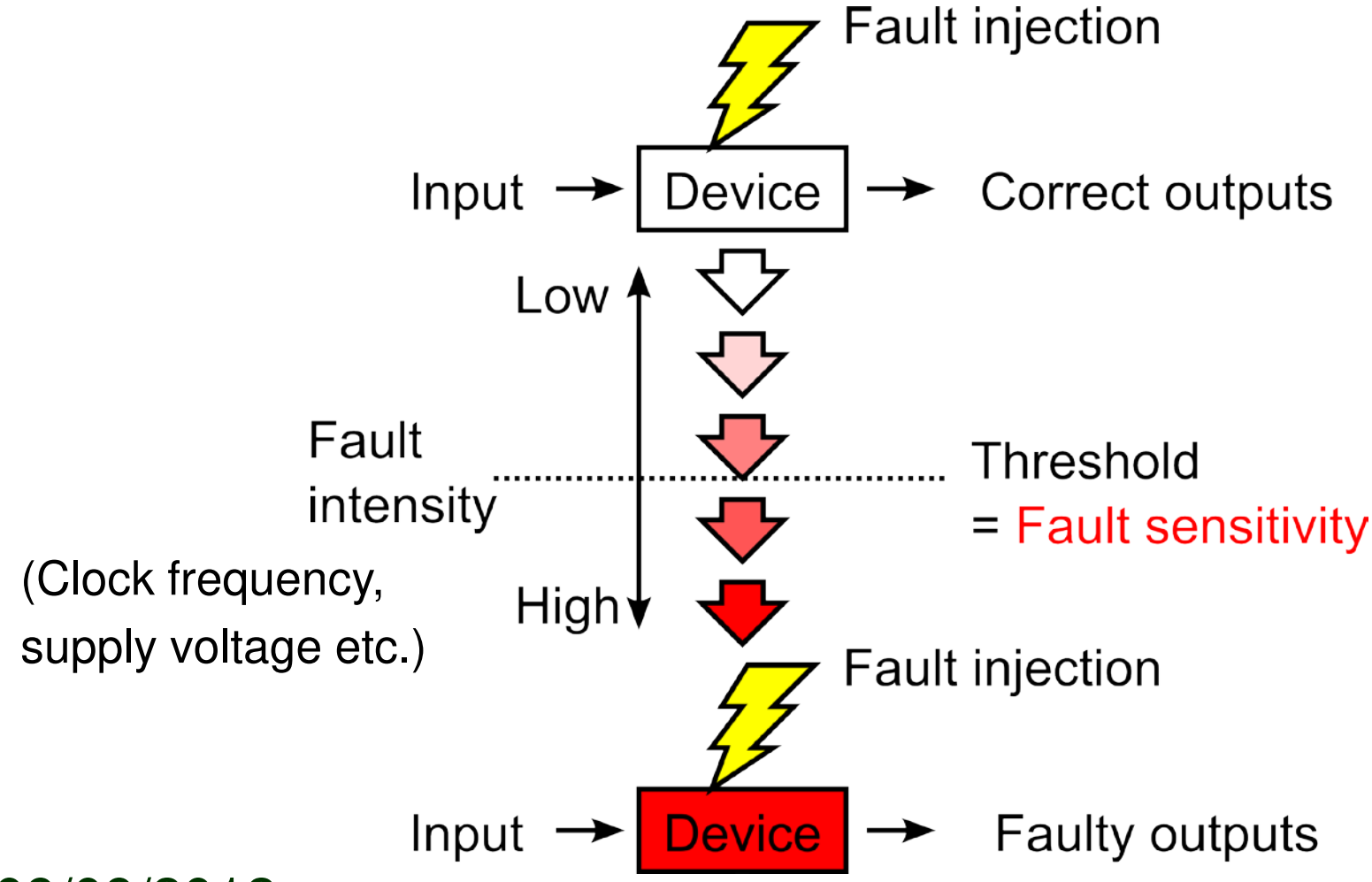
- Introduction
- Proposed countermeasure using Configurable Delay Blocks (CDBs)
- Evaluation
  - Validation of CDB function
  - Area overhead based on standard cell library (SCL) based design
- Conclusion and future works

Introduction

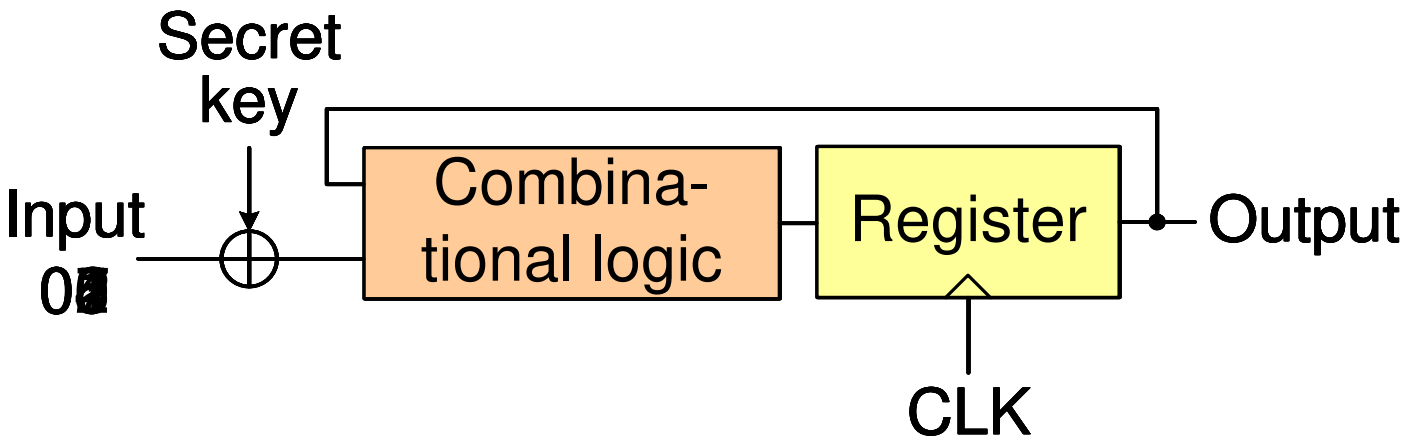
- Fault Sensitivity Analysis (FSA) [Li 2010]
  - Exploits new side-channel called fault sensitivity (FS)
  - FS depends on intermediate value in crypto circuits
- FSA defeated conventional countermeasures against physical attacks
  - Masked AND-OR [Moradi 2011]
  - RSL [Moradi 2011]
  - WDDL [Li 2012] etc.
- No implementation of countermeasure against FSA exists

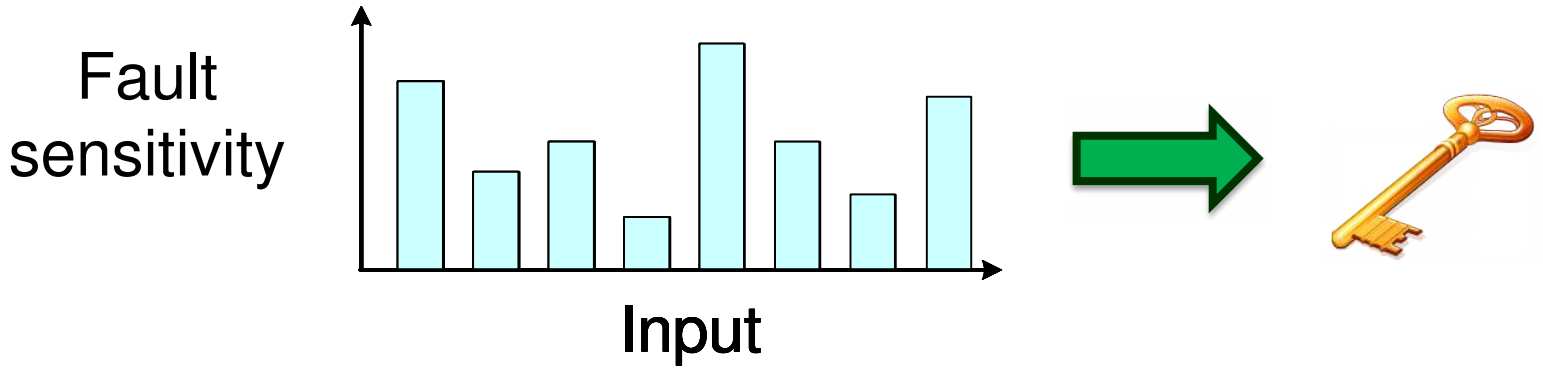
Fault Sensitivity Analysis (FSA)

- Observing fault sensitivity



Fault Sensitivity Analysis (FSA)



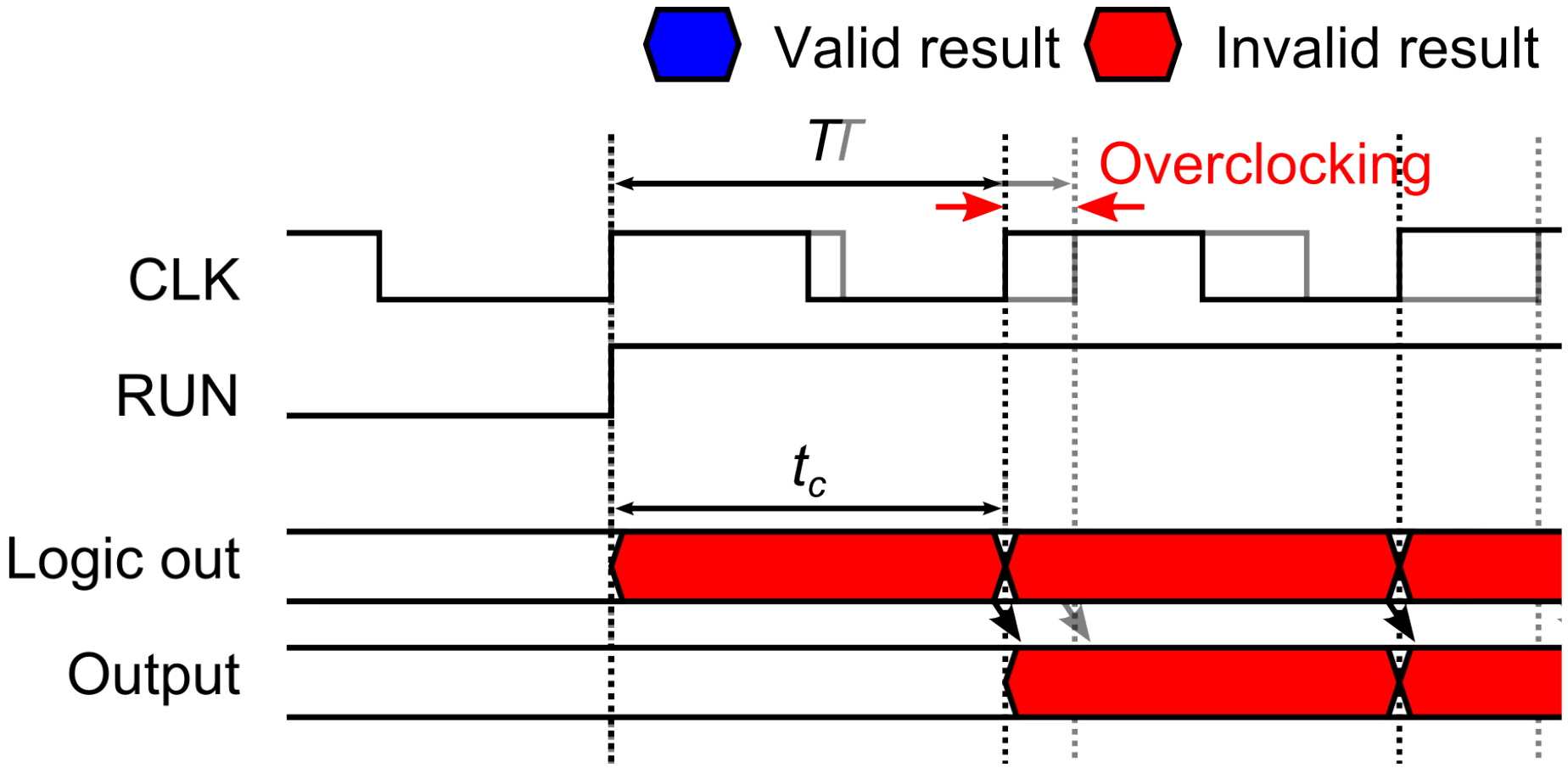


- Methods that recover intermediate value
  - Hamming weight in PPRM S-box, collision FSA

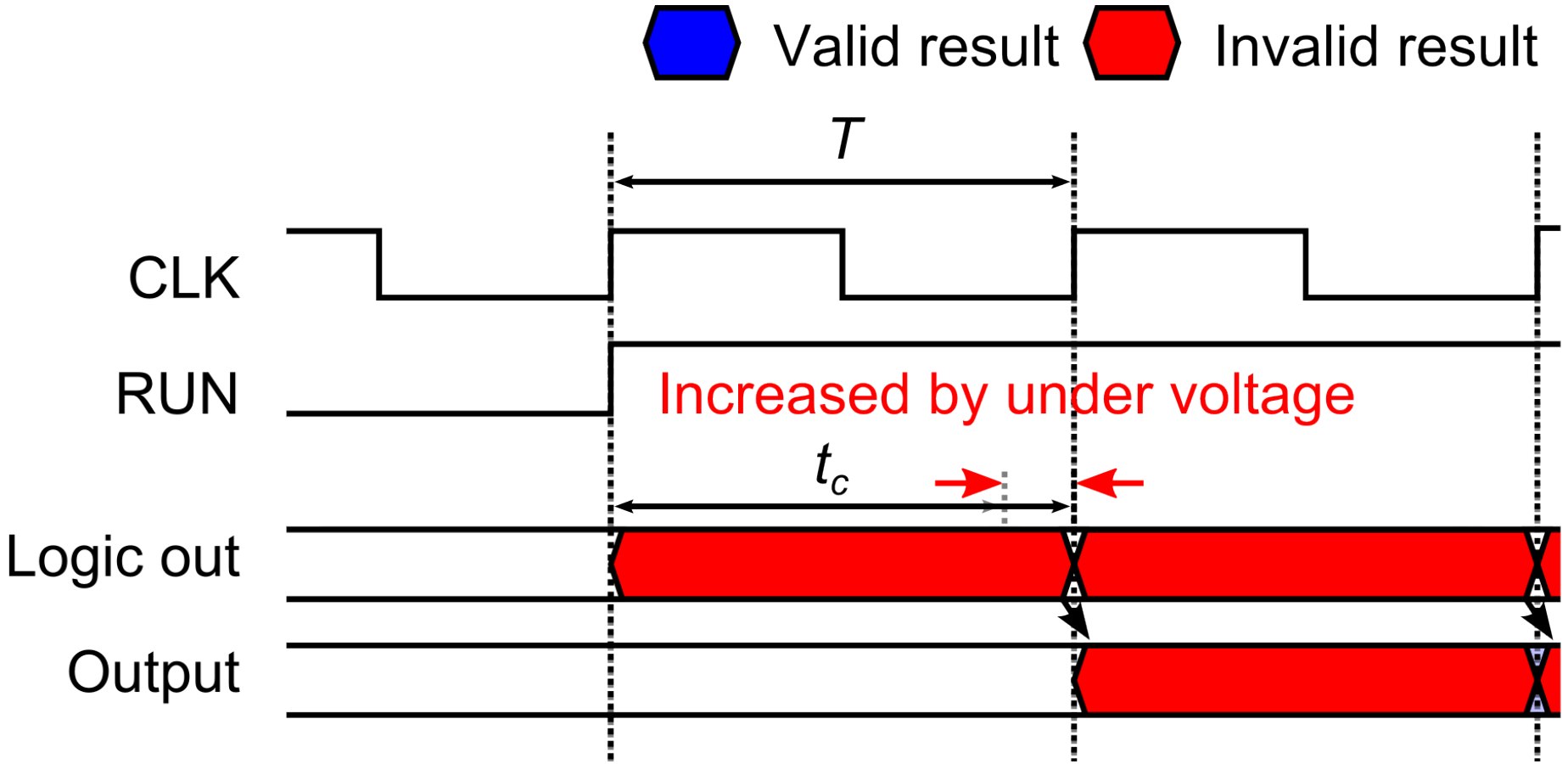
Fault injection techniques for FSA

- Means of fault injection on general fault attacks
  - Exposure to laser/light , excessive temperature, overclocking, under voltage etc.
- Overclocking, under voltage are often used for FSA
  - Inducing setup time violation faults
  - Advantages
    - Depackaging is not required
    - Timely fault injection into the target operation

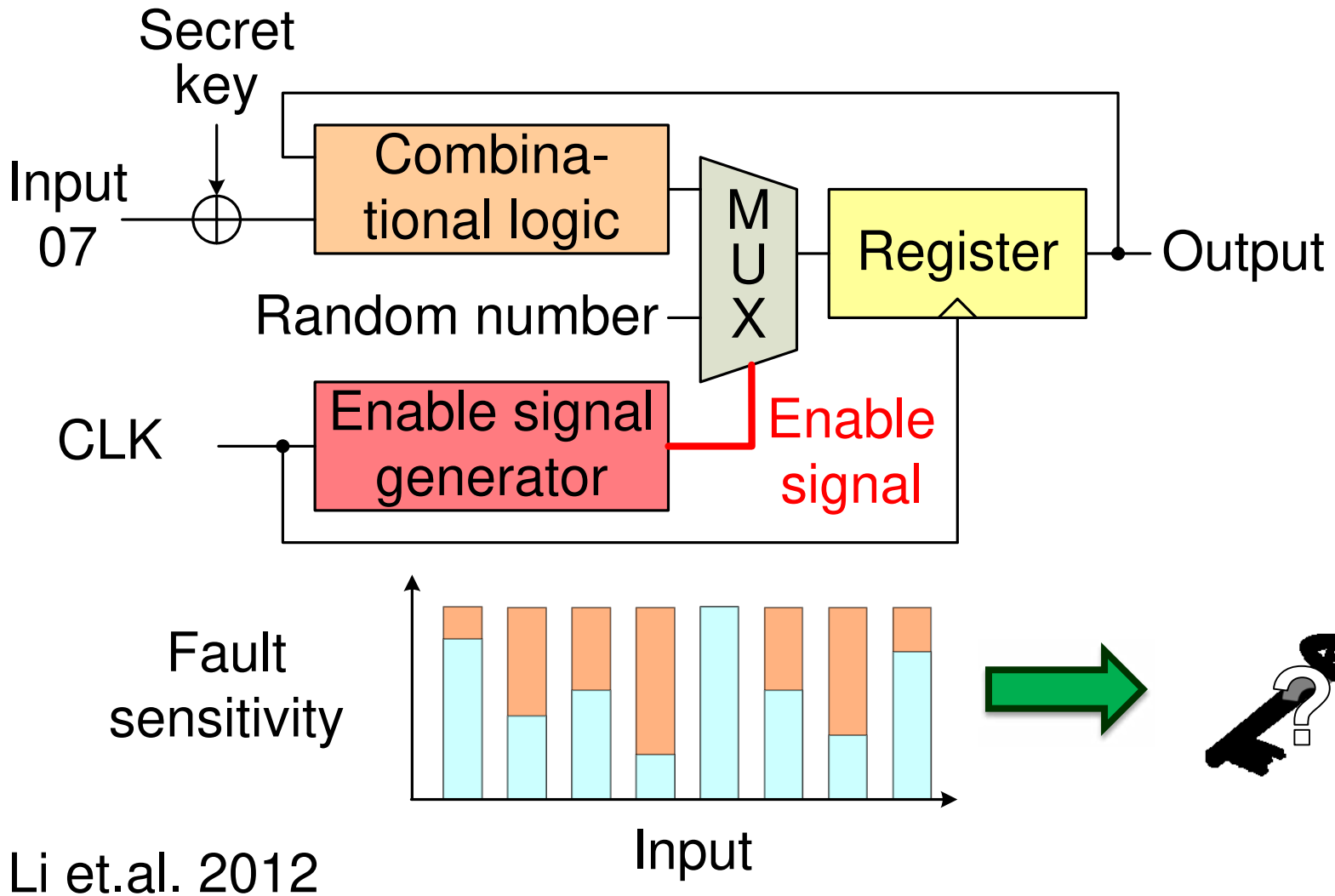
FSA with overclocking



FSA with under voltage



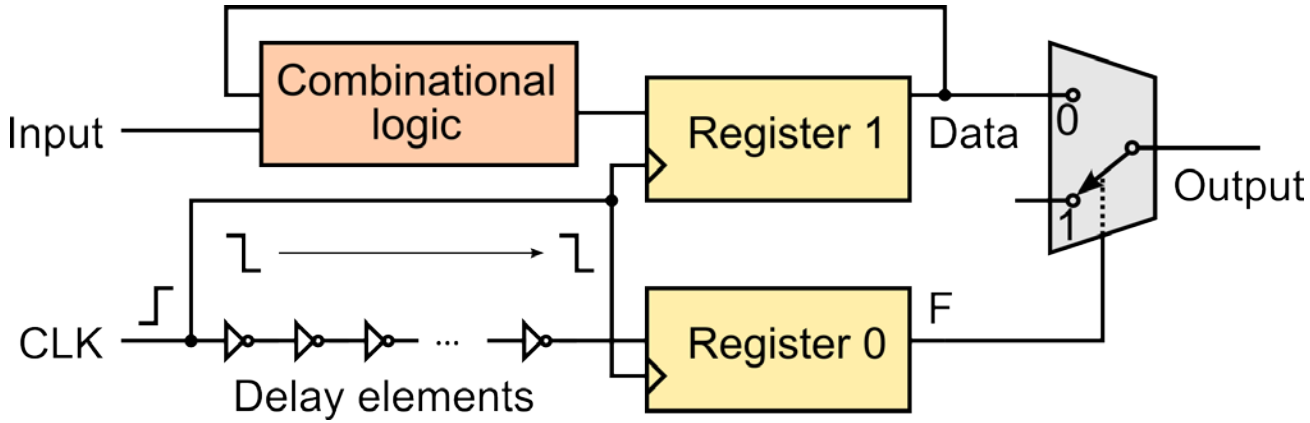
Concept of countermeasure against FSA



- Li et.al. 2012

Related work: countermeasure using delay elements

- Attack detection method using sequential delay elements [Selmane 2009]
  - Attack detection signal F is asserted when the clock signal rises before the signal passes through the delay elements



- Delay elements could be used for enable signal generation in Li's countermeasure

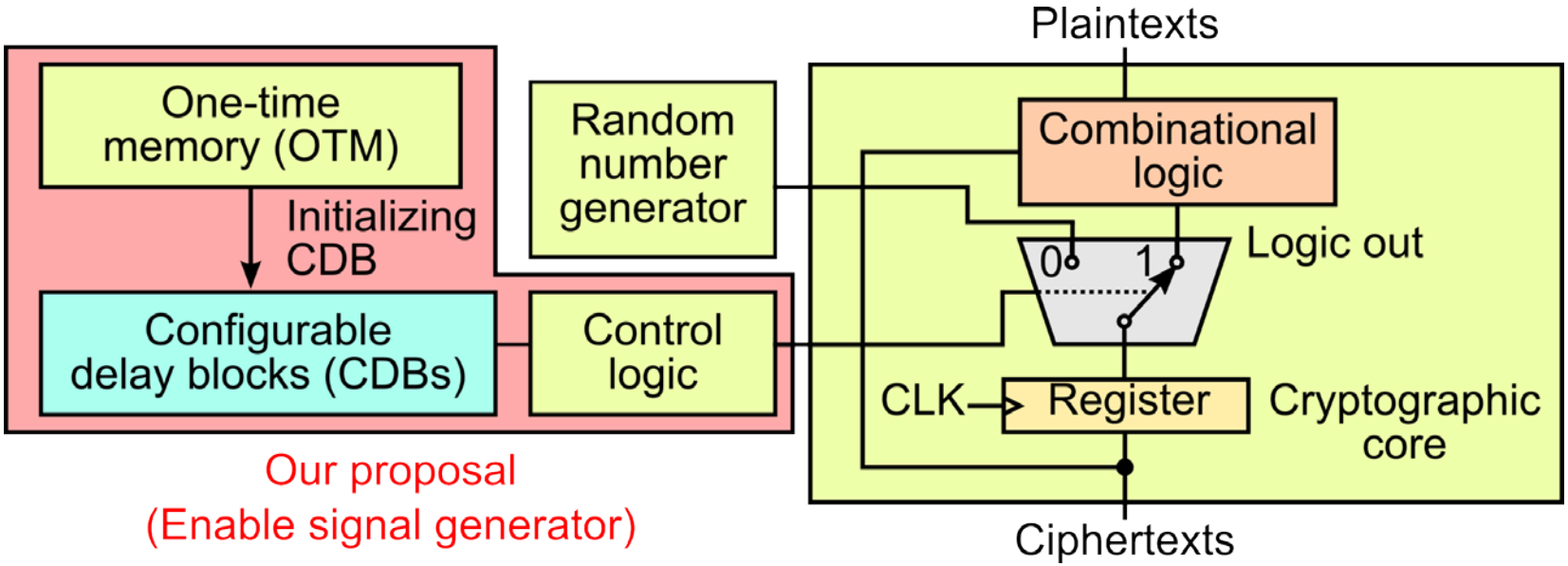
Goal of this work

- Implementation of a countermeasure against FSA
- Our contributions
  - First concrete implementation of Li's countermeasure
    - "Enable signal" generation method
  - Configurable Delay Blocks (CDBs)
    - Can be adjusted after manufacture
    - Provide fine delay-time tuning
    - Efficient countermeasure with low overheads

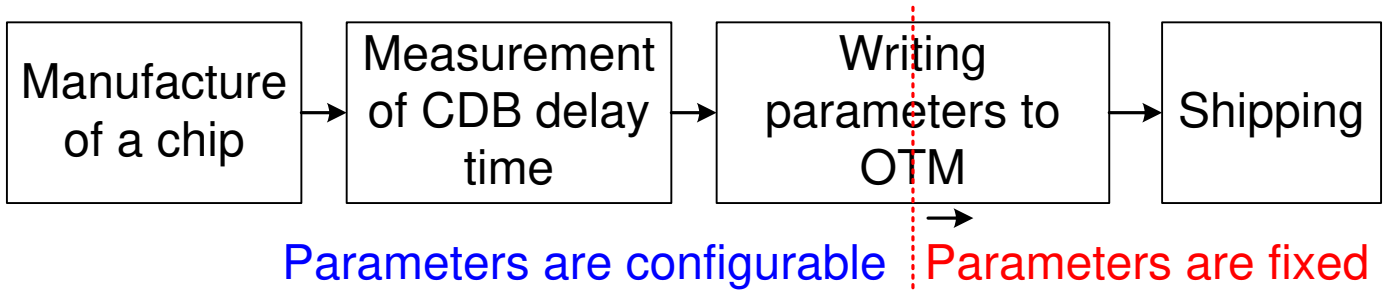
Outline

- Introduction
- Proposed countermeasure using Configurable Delay Blocks (CDBs)
- Evaluation
  - Validation of CDB function
  - Area overhead based on standard cell library (SCL) based design
- Conclusion and future works

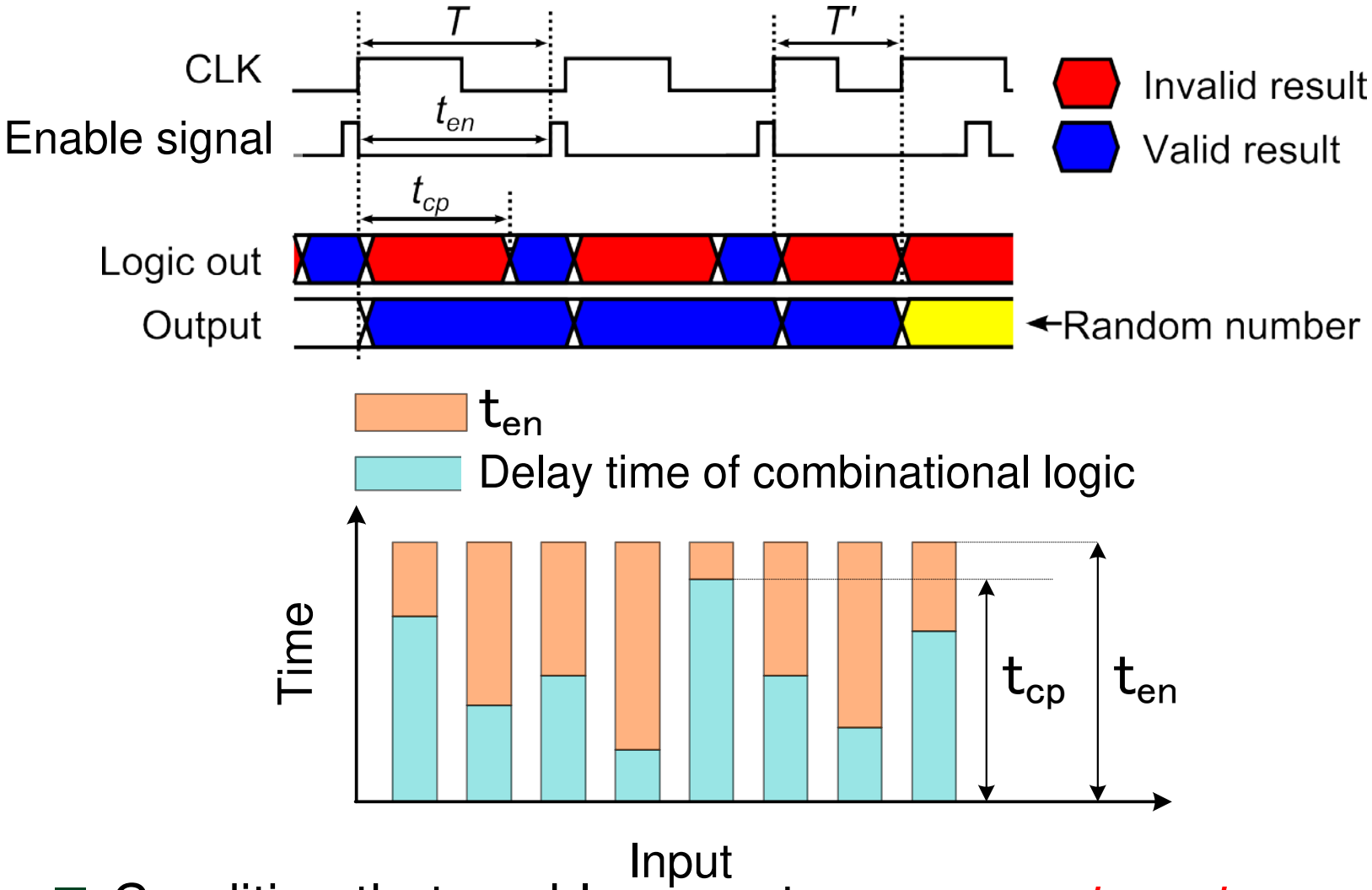
Overview of proposed countermeasure



Block diagram of countermeasure

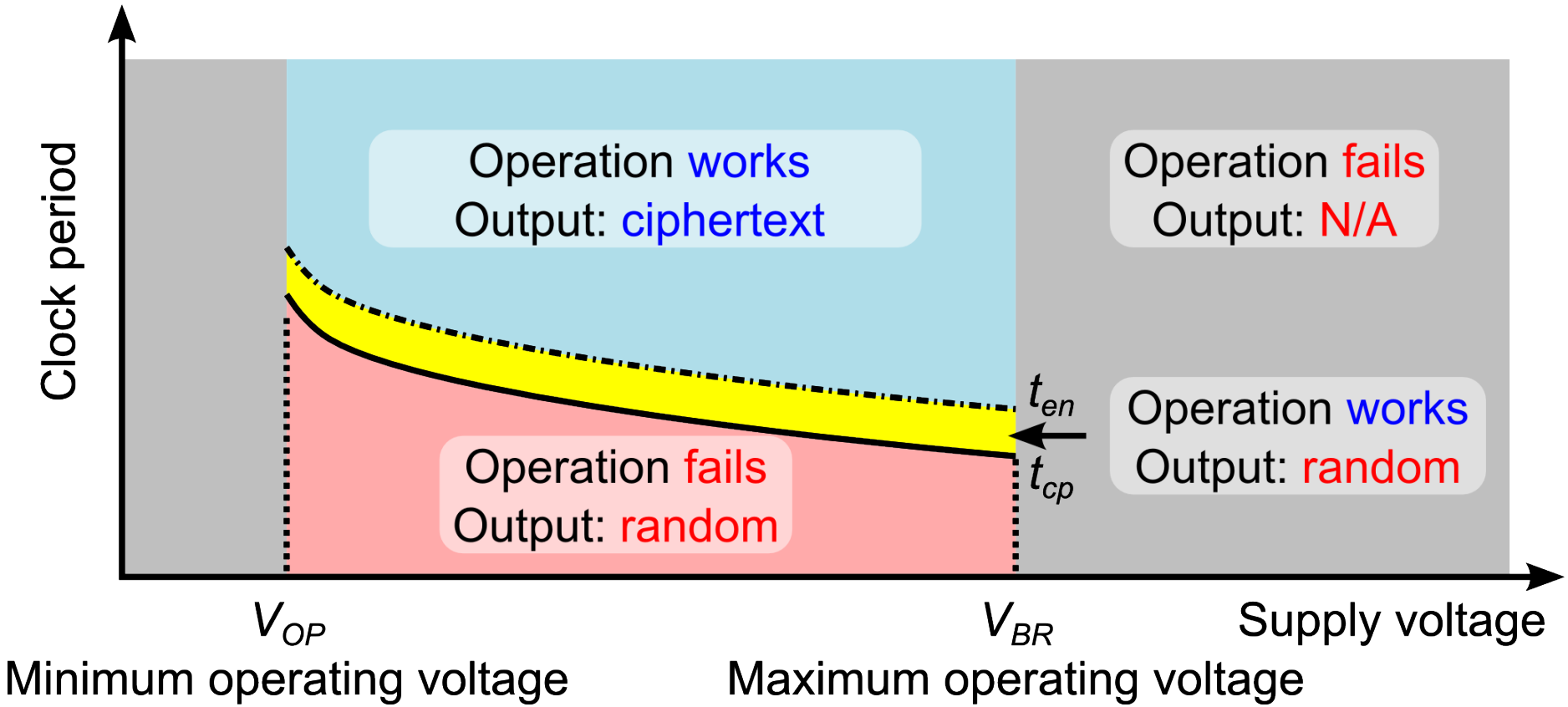


Timing chart of enable signal

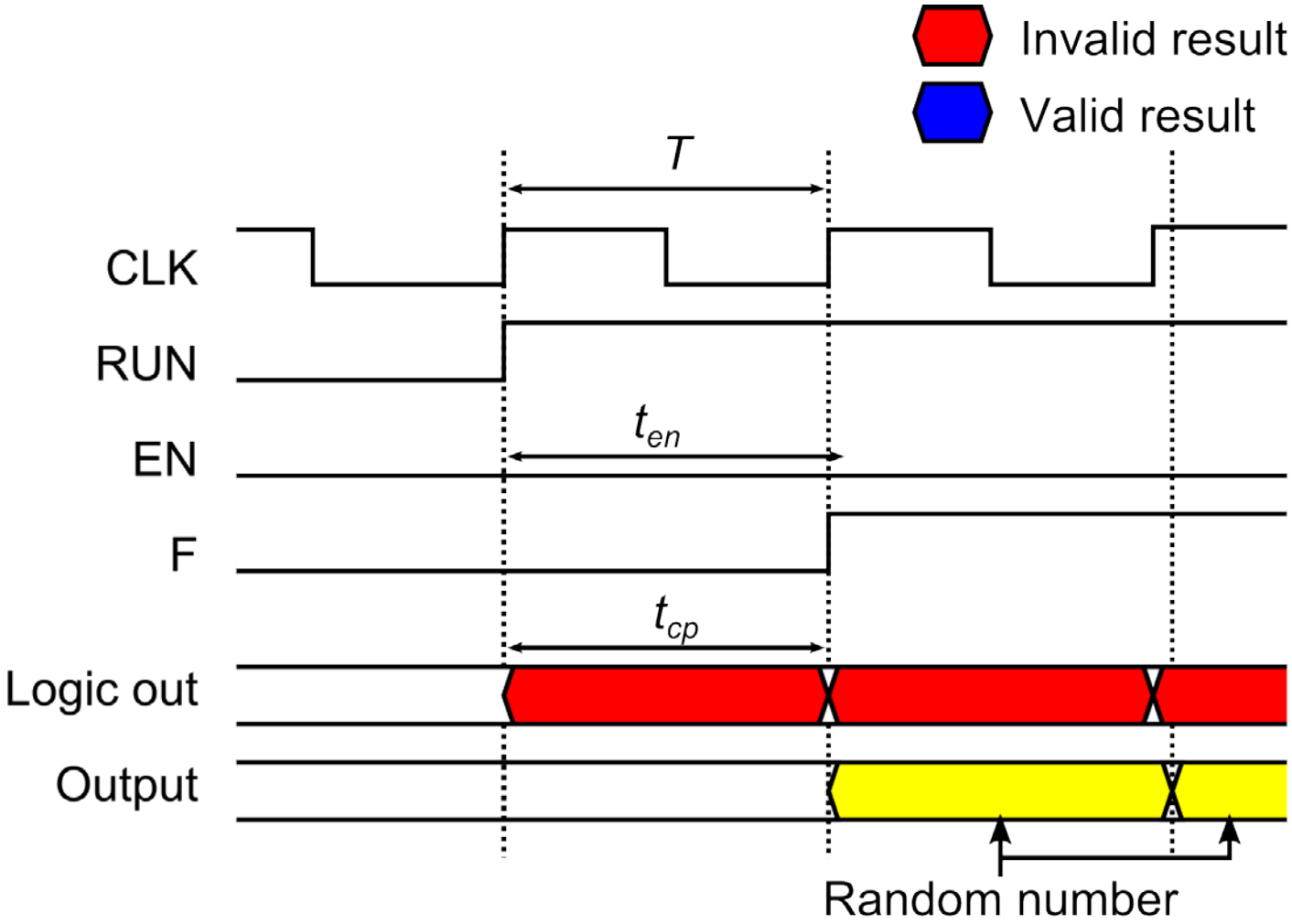


- Condition that enables countermeasure: $t_{en} > t_{cp}$

Ideal configuration of t_{en}

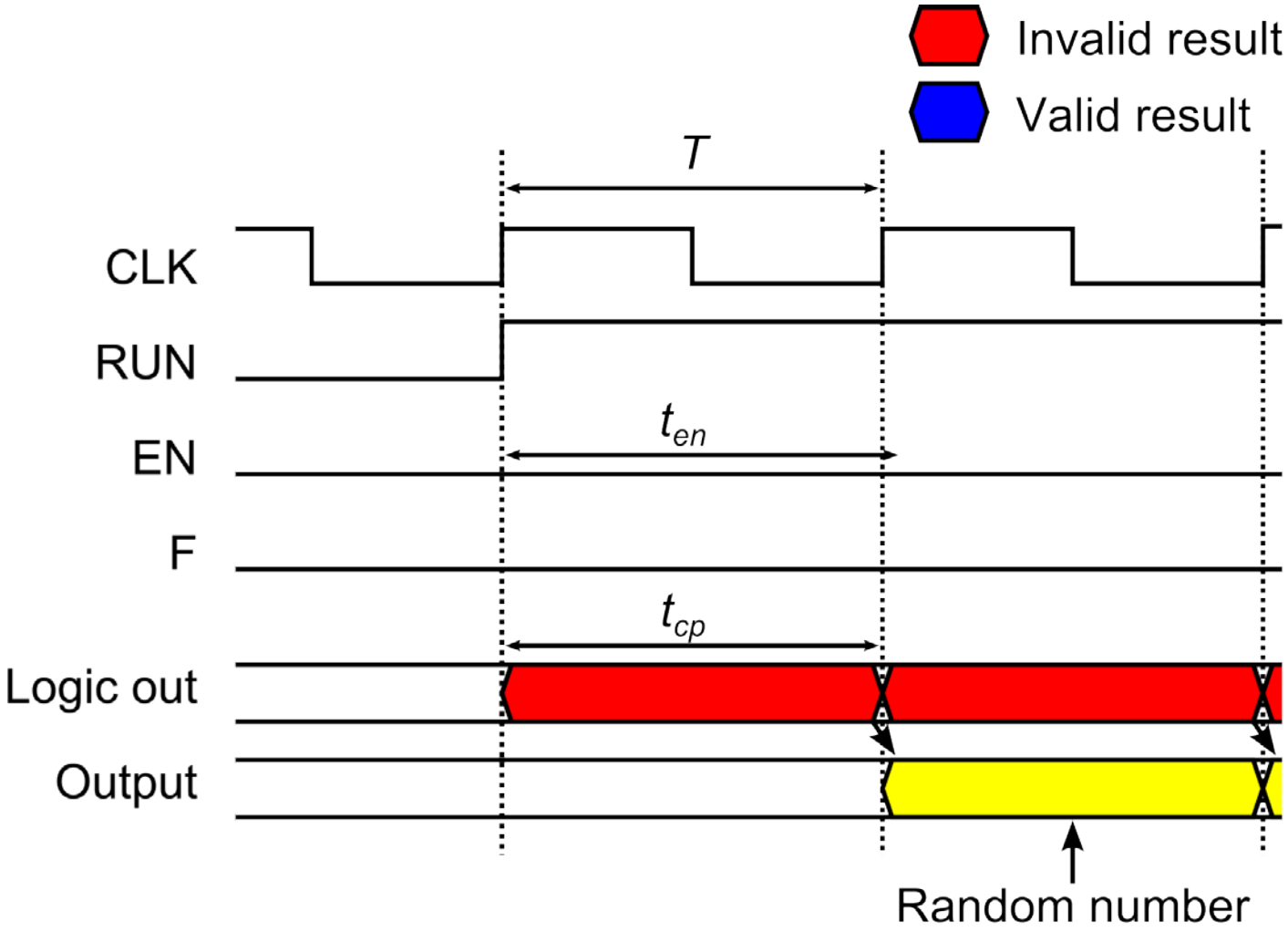


Behavior of countermeasure (1/2)



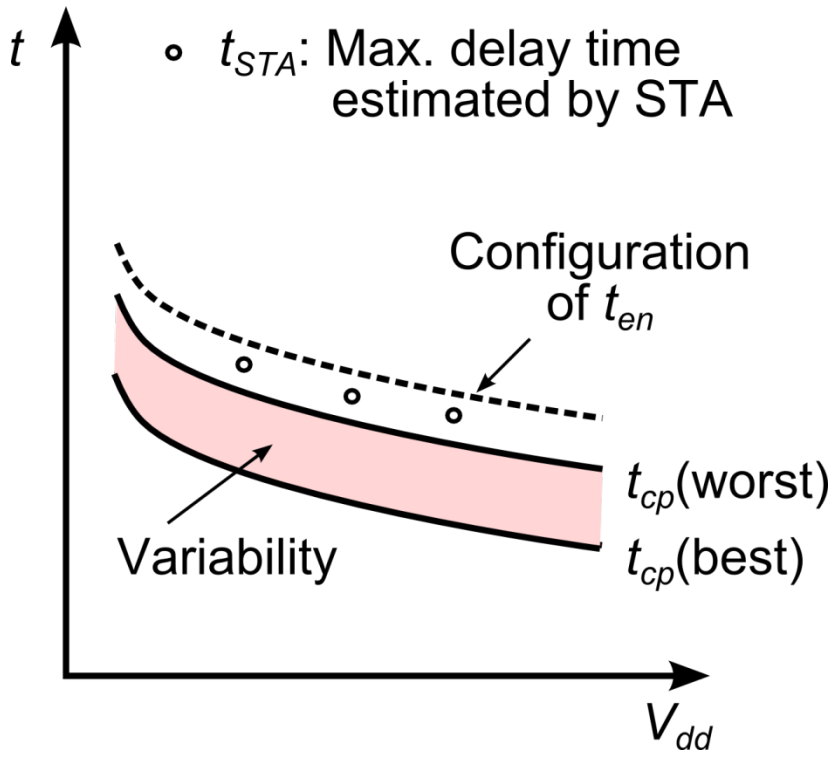
- When clock period is shortened

Behavior of countermeasure (2/2)



- When supply voltage was lowered

Configuration of t_{en} based on STA



- Configuration method based on delay time estimation by Static Timing Analysis (STA)
- t_{STA} is always larger than t_{cp}
  - t_{STA} is the longest delay time estimated by maximum gate chain
- We can prevent leakage of FS when we set $t_{en} > t_{STA}$

Outline

- Introduction
- Proposed countermeasure using Configurable Delay Blocks (CDBs)
- Evaluation
  - Validation of CDB function
  - Area overhead based on standard cell library (SCL) based design
- Conclusion and future works

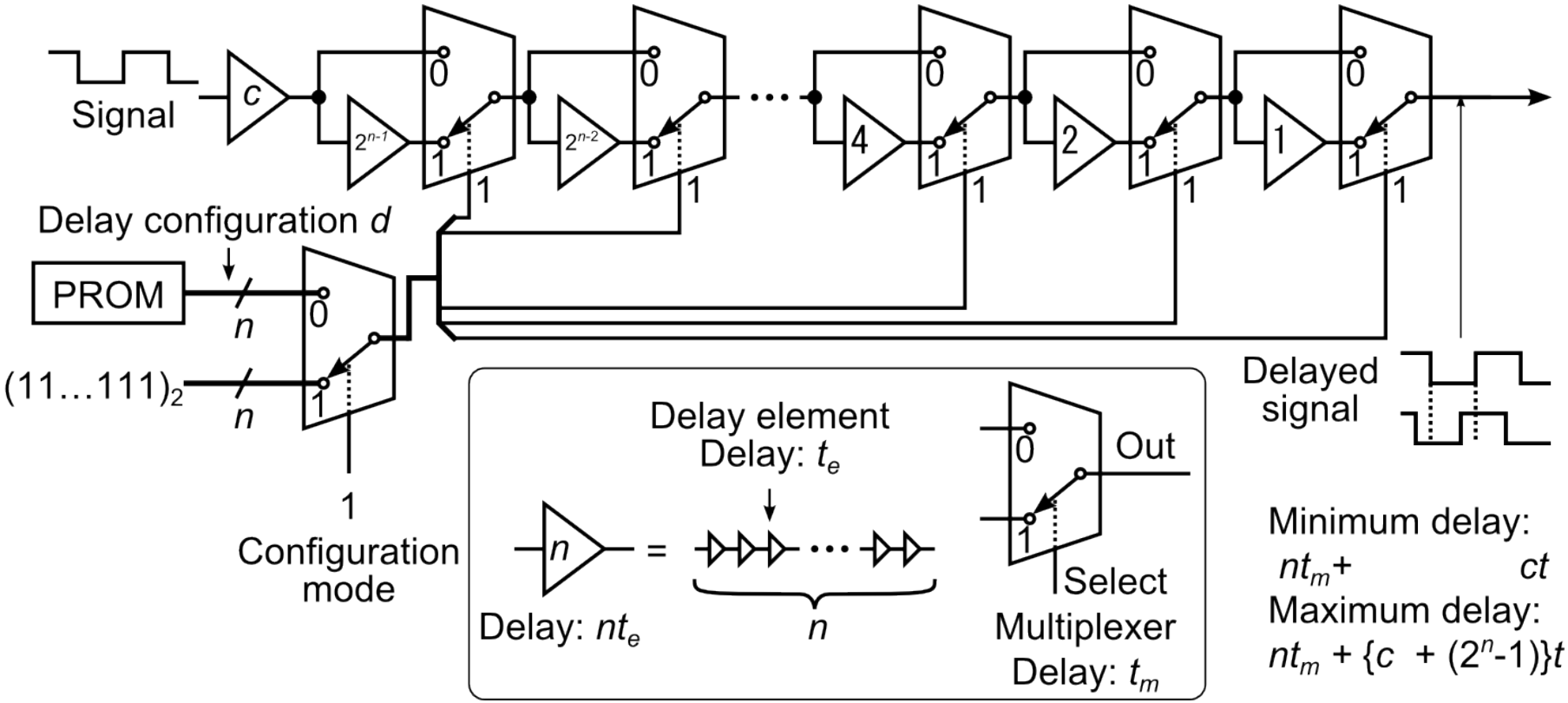
Evaluation of proposed countermeasure

- Implementation of AES module with proposed countermeasure
- Validation of CDB function on FPGA prototype
- Estimation of area overhead based on Static Cell Library (SCL) design

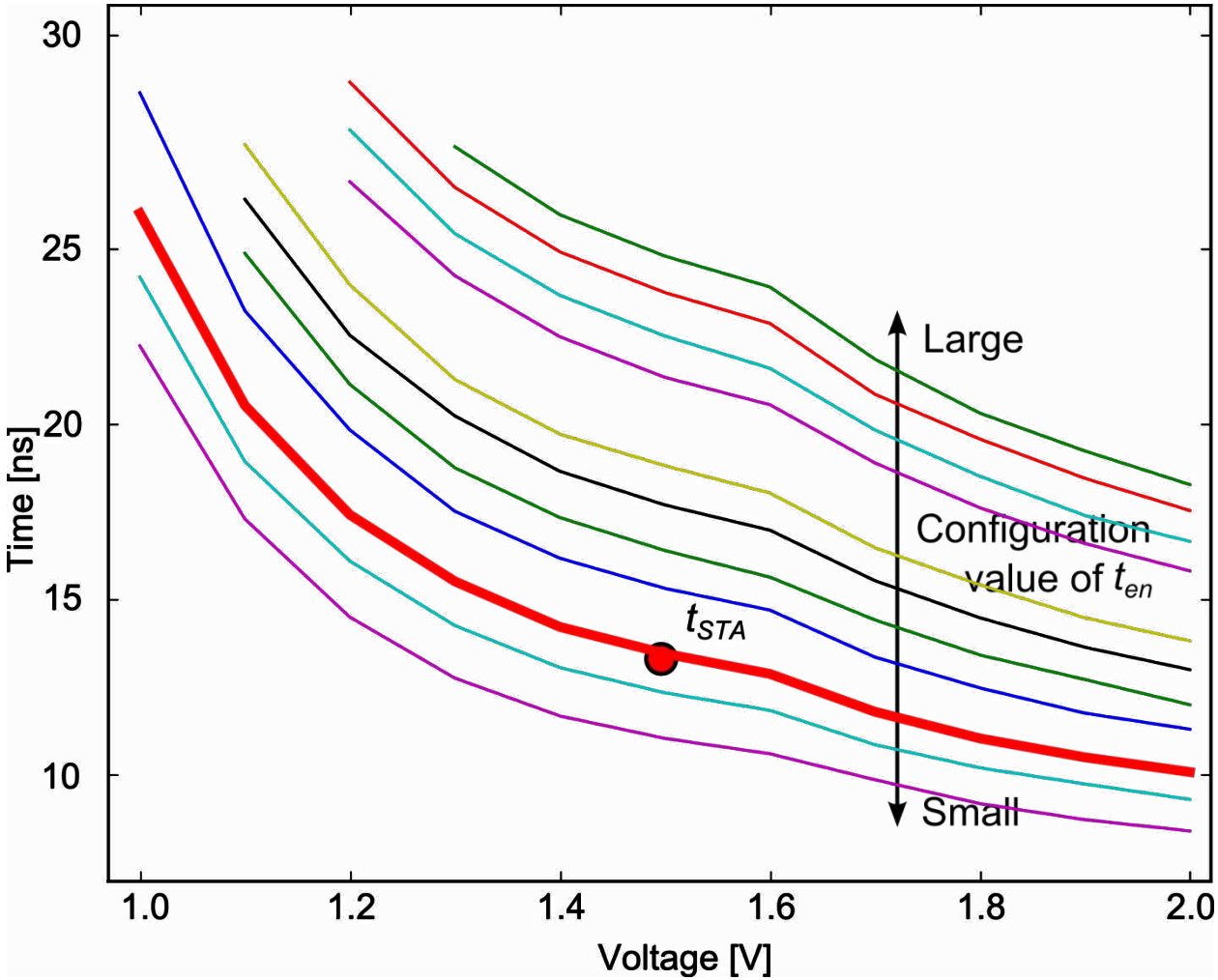
Experimental conditions

Platform	SASEBO-G
FPGA	Xilinx XC2VP7

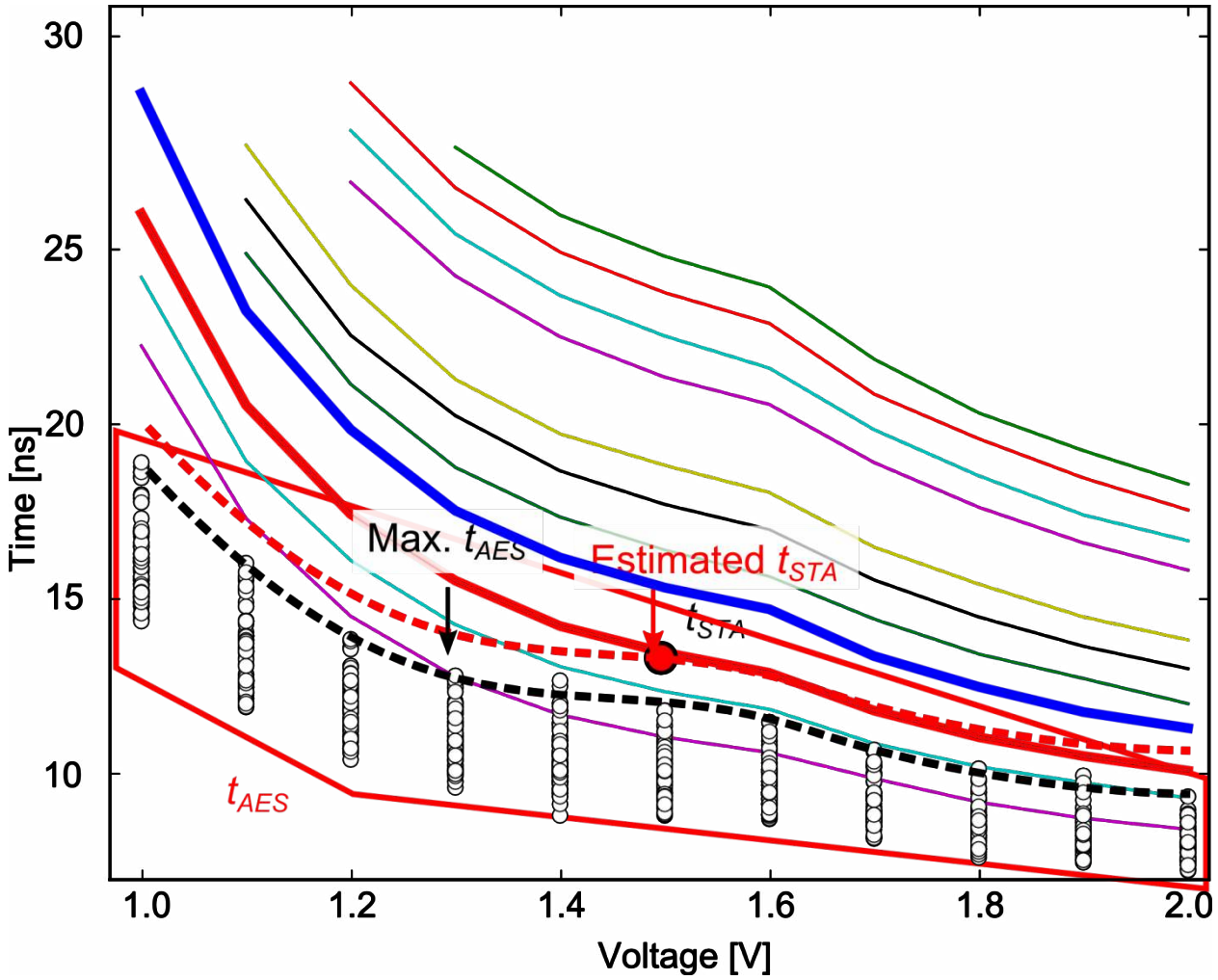
Implementation of CDB



Validation of CDB function



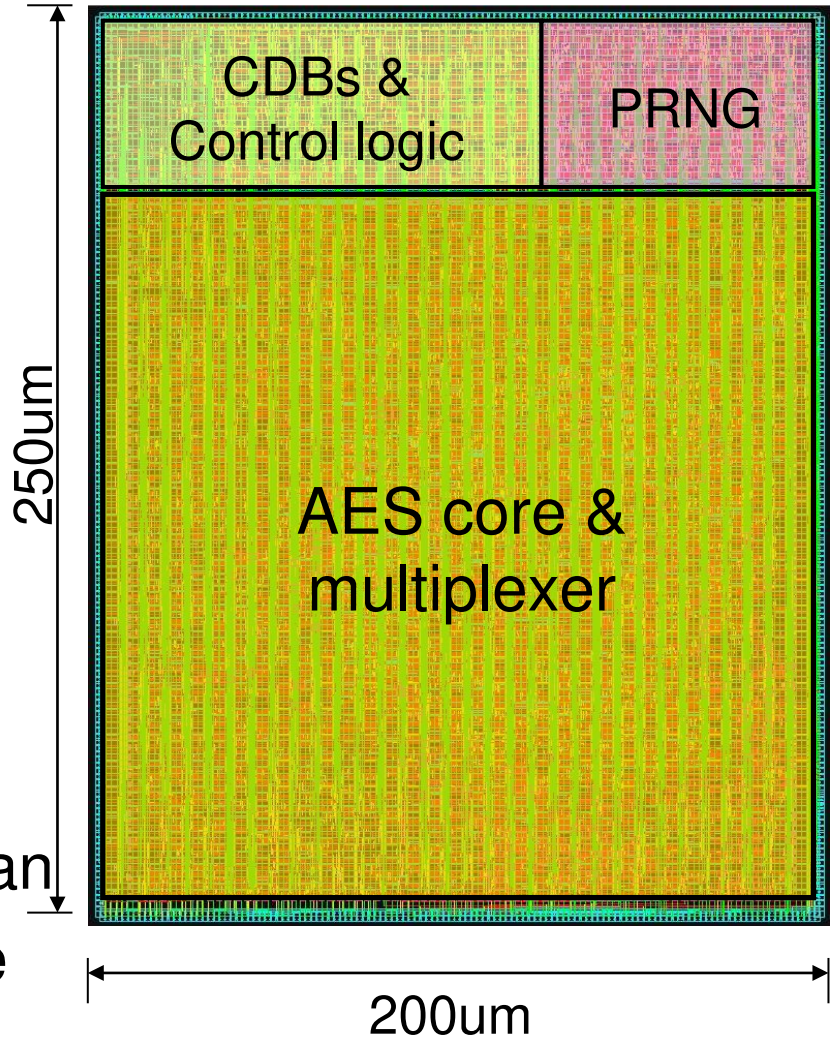
Validation of CDB function



Gate counts based on SCL design

Components	Gates	%
AES core	28702	100
Multiplexers	1882	6.56
CDBs	1068	3.72
Control logic	35	0.12
Total	31687	110.4

- TSMC 65nm cell library
- 8-stage CDB
- Overhead is much smaller than conventional countermeasure such as masking



Conclusion and future work

- Proposal of countermeasure against FSA using configurable delay blocks (CDBs)
  - Enable signal generation method
  - Post-manufacture configuration of CDB based on measurement of real chips
- Evaluation
  - Validation of CDB function on FPGA prototype
  - Area overhead of countermeasure
- Future work: evaluation of countermeasure on ASIC

Thank you!

Enable signal generator