Secure and Testable Scan Design Using Extended de Bruijn Graphs

Hideo Fujiwara and Marie Engelene J. Obien

Nara Institute of Science and Technology, Japan

ASP-DAC 2010

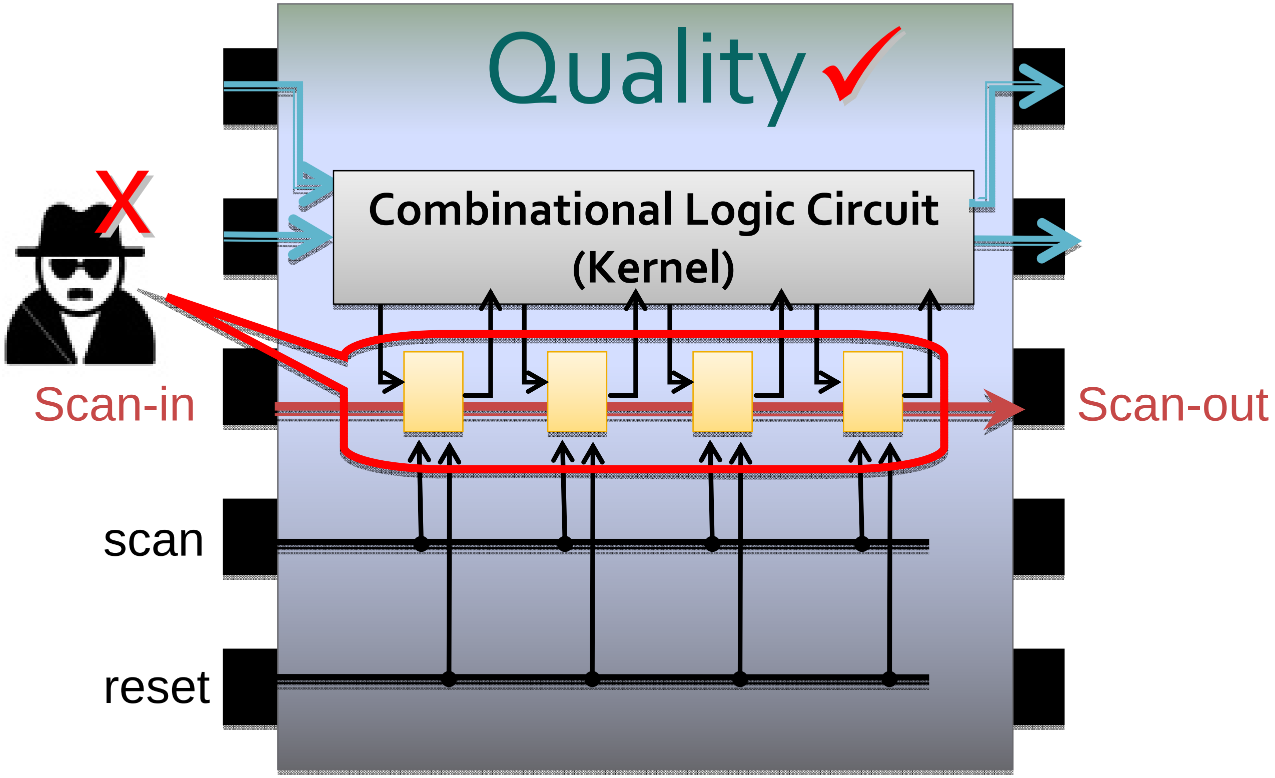
Outline

1. Background and Motivation
2. Previous Works
3. Objective of the Study
4. Proposed Design
    - Extended de Bruijn Graph
    - Extended Shift Registers
    - Proposed Secure Scan Design
        - Scan-Testability
        - Scan-Security
    - Cardinality and Area Cost
5. Conclusion

Digital Circuits Need...

- Reliability due to increasing complexities in VLSI design
  → *Scan Design: most popular DFT*

- Protection of information: esp. in crypto chips
  → *Scan Design: increases vulnerability of chip*



Contradiction between Testability and Security → **Solution?**

Previous Works

- Recent works focus on secure scan design:
  - D. Hely, et al. 2004, 2007 – scrambling
  - B. Yang, et al. 2004, 2006 – MKR
  - J. Lee, et al. 2006, 2007 – lock & key
  - S. Paul, et al. 2007 – Vlm-scan
  - G. Sengar, et al. 2007 – flipped-scan-chain
  - M. Inoue, et al. 2009 – partial scan based on balanced structure
  - U. Chandran, et al. 2009 – multi-level security authorization

- All approaches (*except Sengar*) add extra hardware outside of scan registers.

  Which means:
  - high area overhead
  - timing overhead or performance degradation
  - increased complexity of testing
  - limited security for the registers part

Objective of the Study

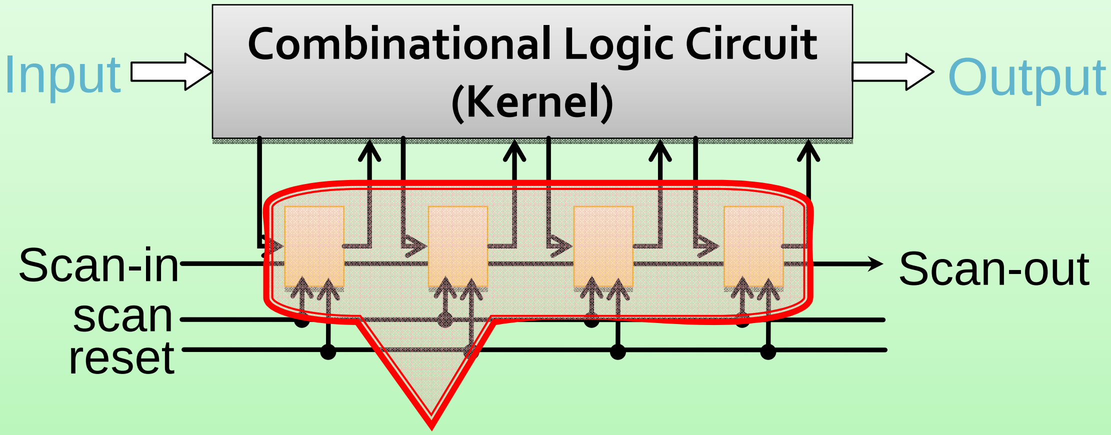
- Propose a **secure scan design approach**
  - Satisfies both scan-testability and scan-security
  - Replaces original scan registers with modified scan registers only

  Which leads to:
  - Little area overhead
  - No performance overhead

- Introduce Extended de Bruijn Graph
  - Extended scan register (ESR) types
- Introduce new concepts
  - Scan-testability
  - Scan-security

Introduction: de Bruijn Graph

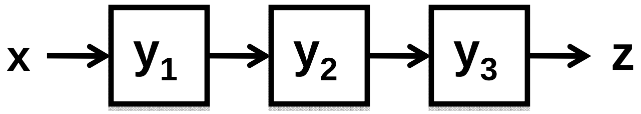
Problem:

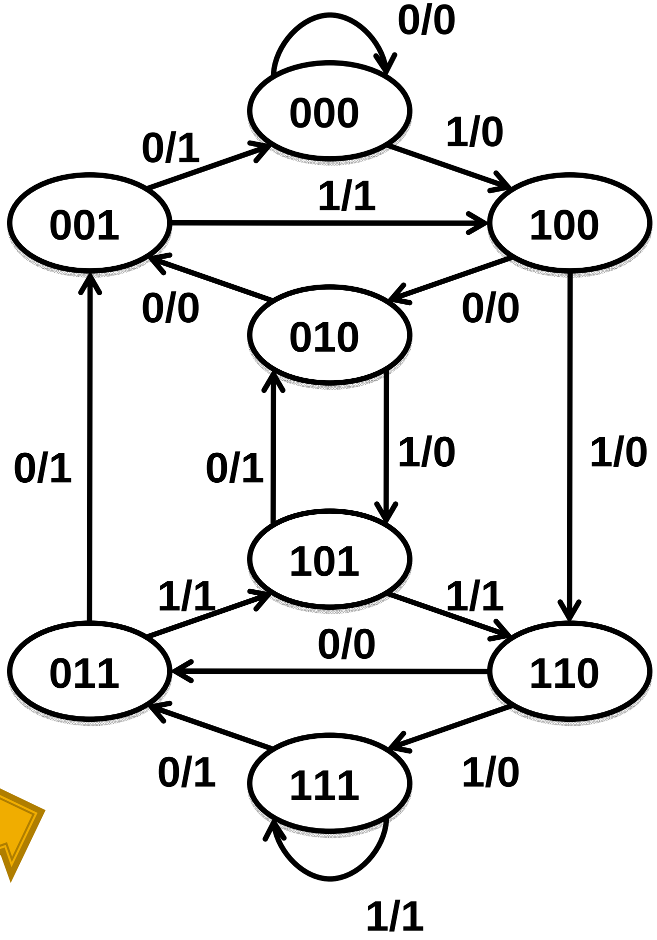


Shift register → not secure!

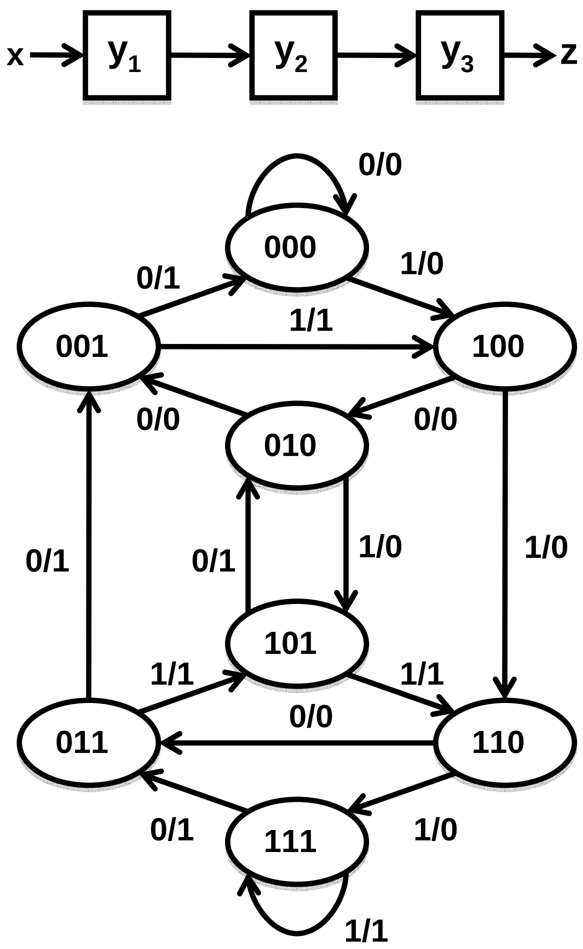
Solution: Change the shift register.

A de Bruijn graph represents
a state transition graph of a shift register.

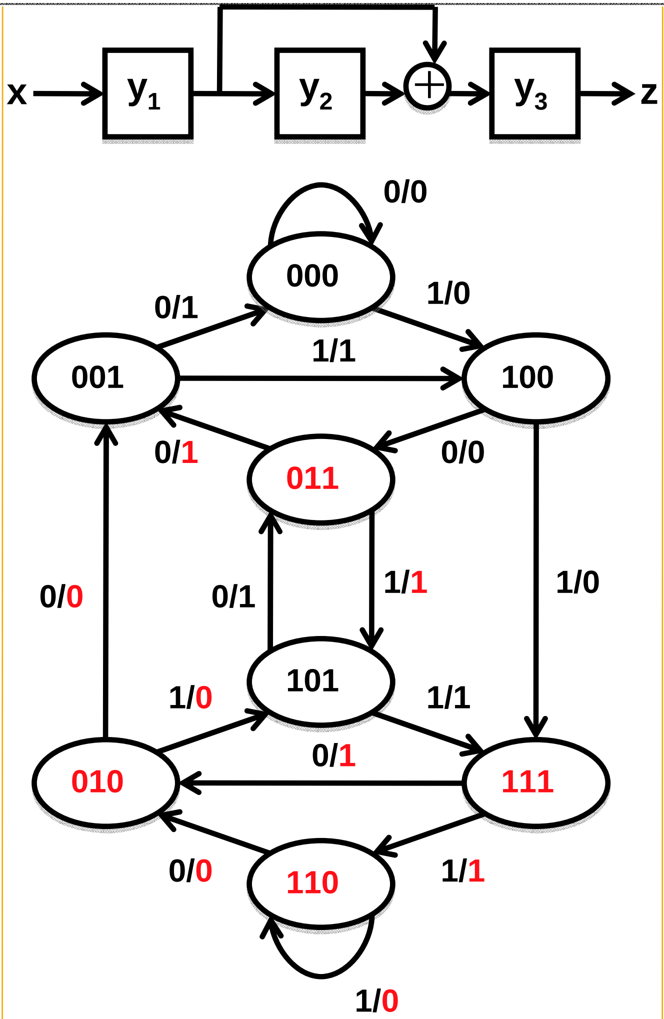




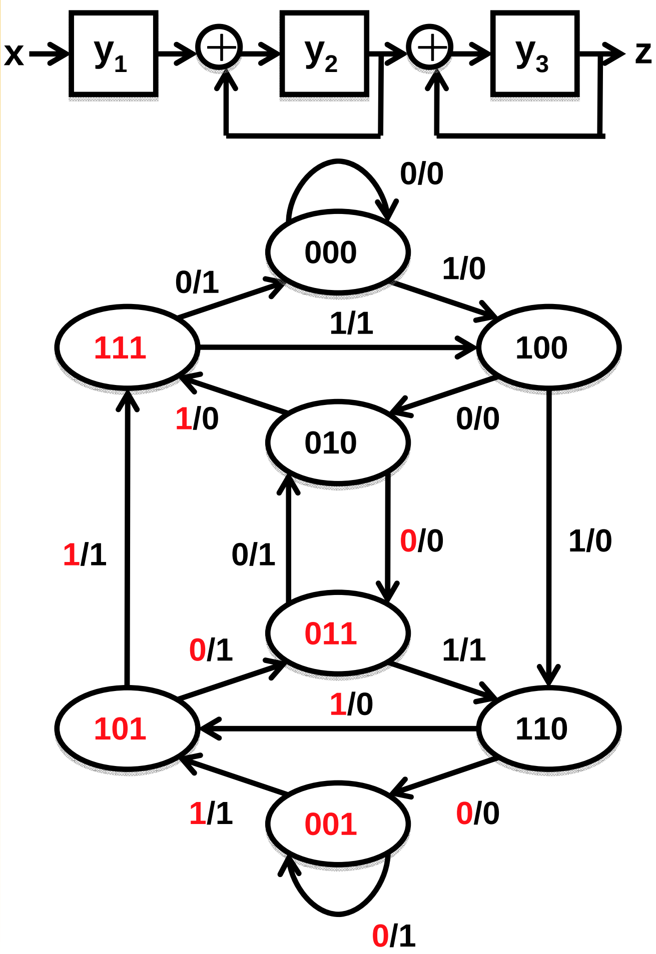
Definition: Extended de Bruijn Graph 1



de Bruijn Graph

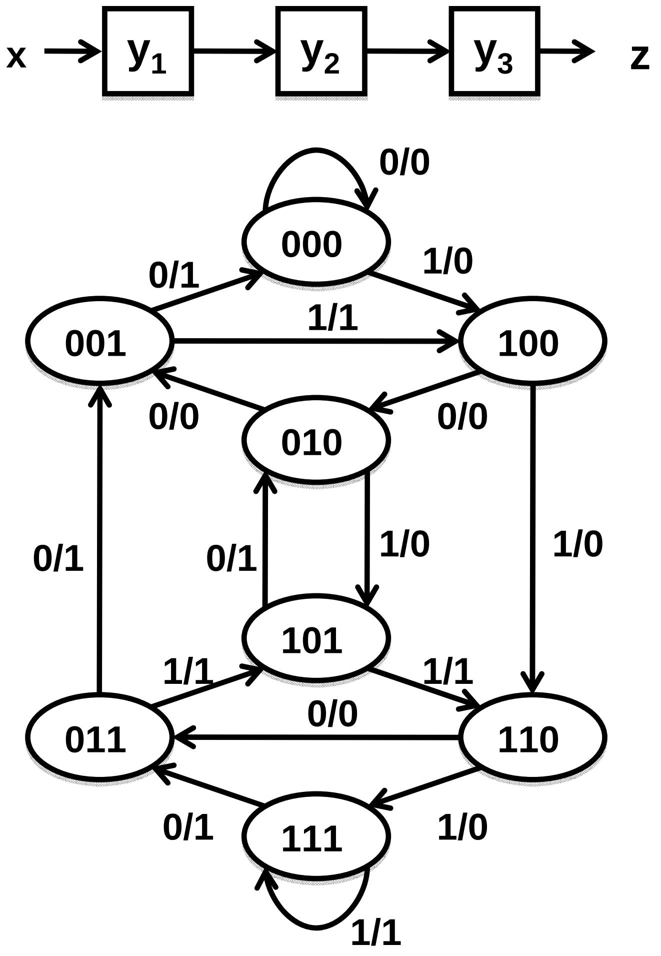


Input-equivalence

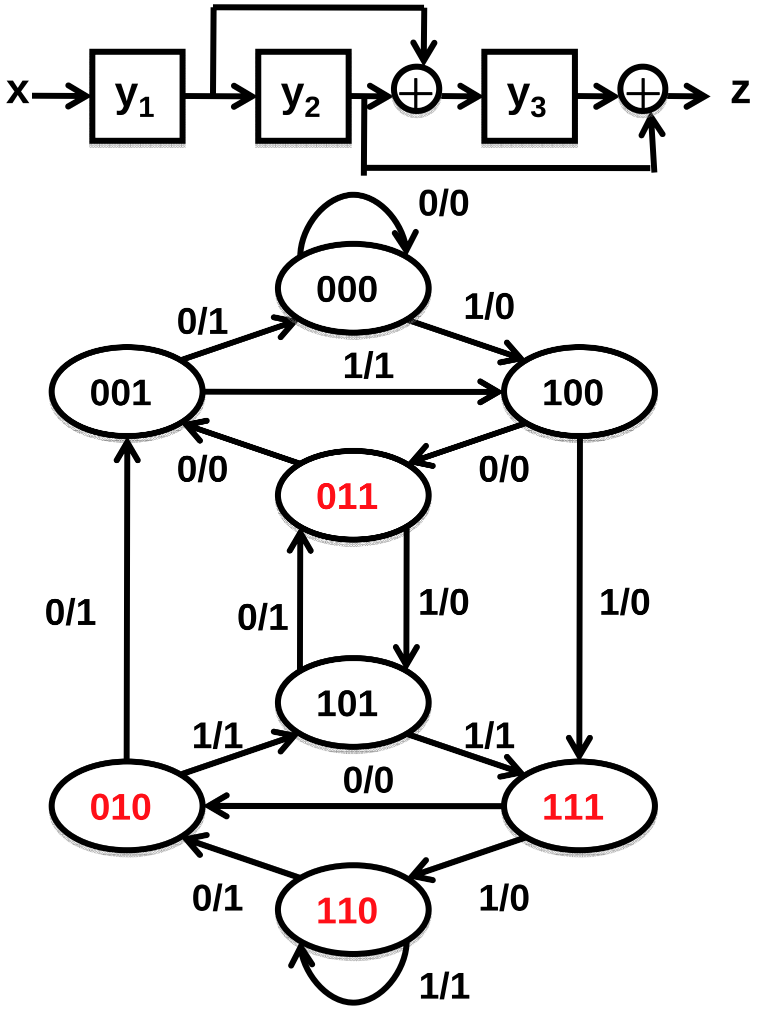


Output-Equivalence

Definition: Extended de Bruijn Graph 2



de Bruijn Graph



Functional equivalence

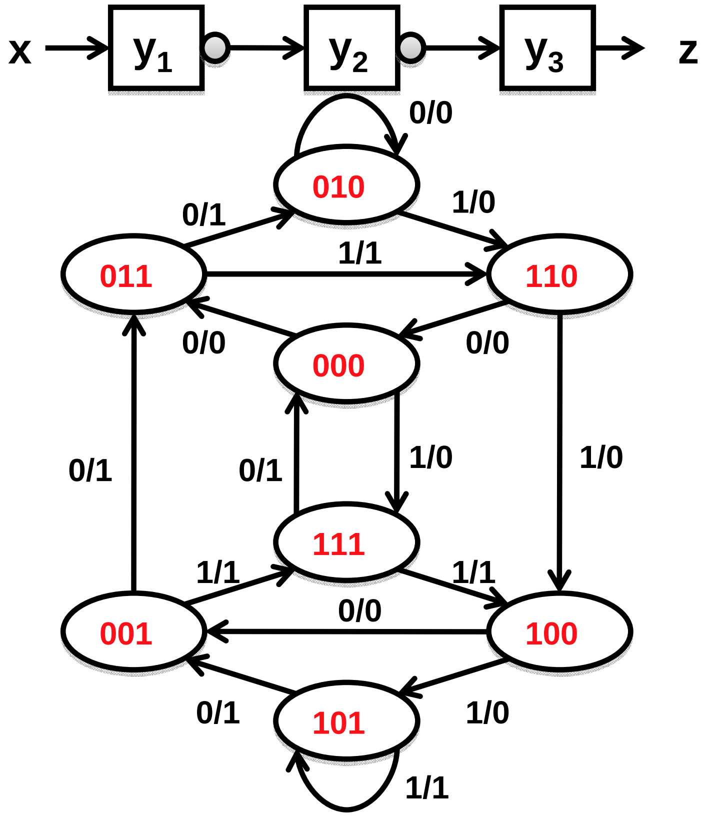
Realization: Extended Shift Registers

Models:

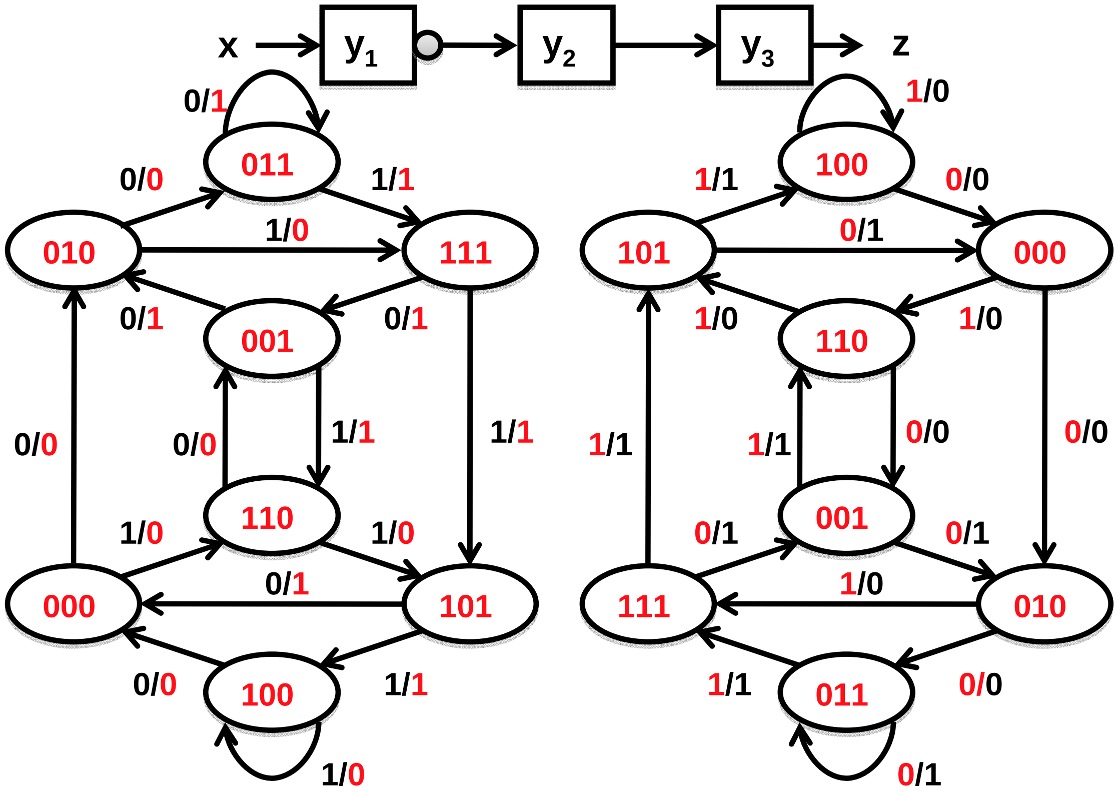
1. Inversion Inserted SR (I^2SR)
2. Linear Feed-Forward SR (LF^2SR)
3. Linear Feedback SR (LFSR)

- General sequential circuit structure – other structure realization

Inversion Inserted SR



Any k-stage I²SR with ***even*** number of inversions is *functionally equivalent* to the k-stage SR.

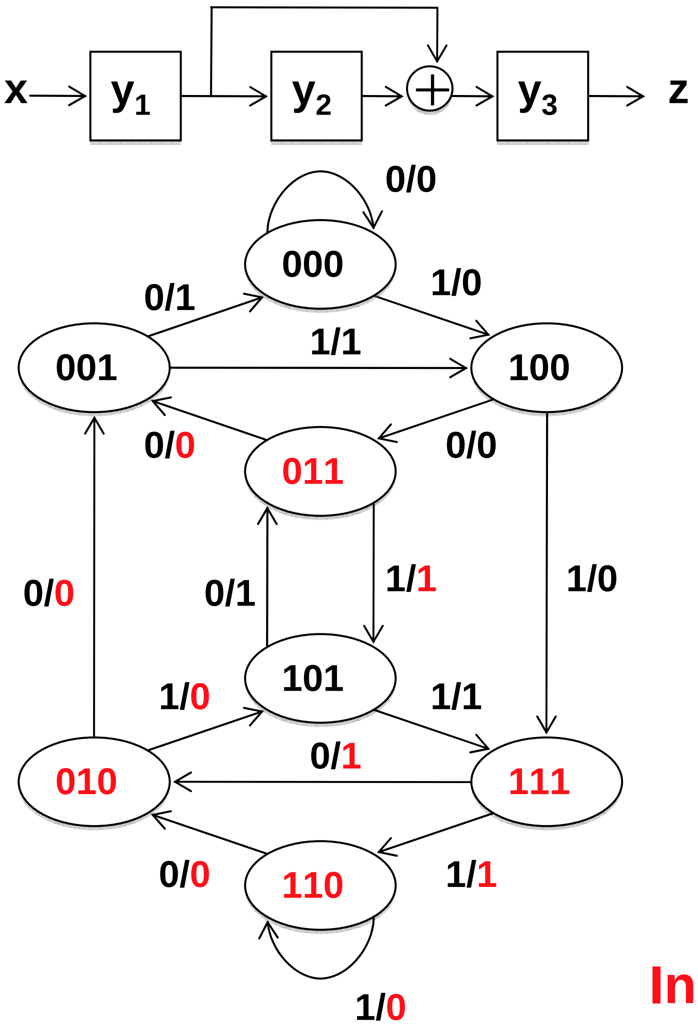


Input-equivalent

Output-equivalent

Any I²SR with ***odd*** number of inversions is *input-equivalent* and *output-equivalent* to SR but *not simultaneously*, thus ***not** functionally equivalent* to SR.

Linear Feed-Forward SR (LF²SR)

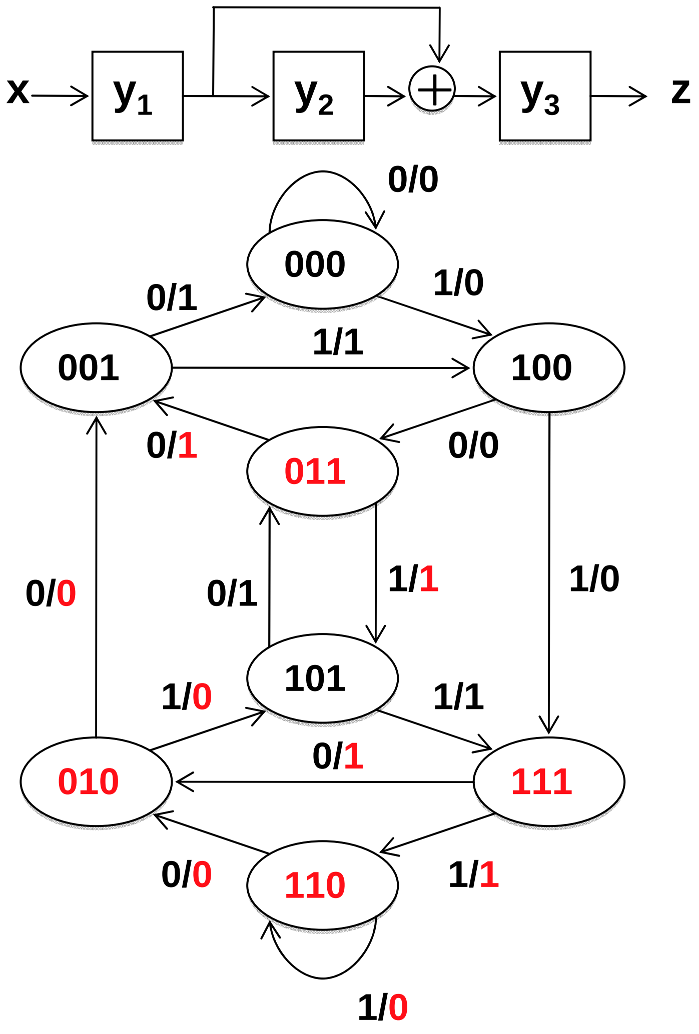


Any k-stage LF²SR is *input-equivalent* to a k-stage SR.

Can be **modified** to be output-equivalent (and hence functionally equivalent) to the k-stage SR, by **manipulating the linear sum of the output**.

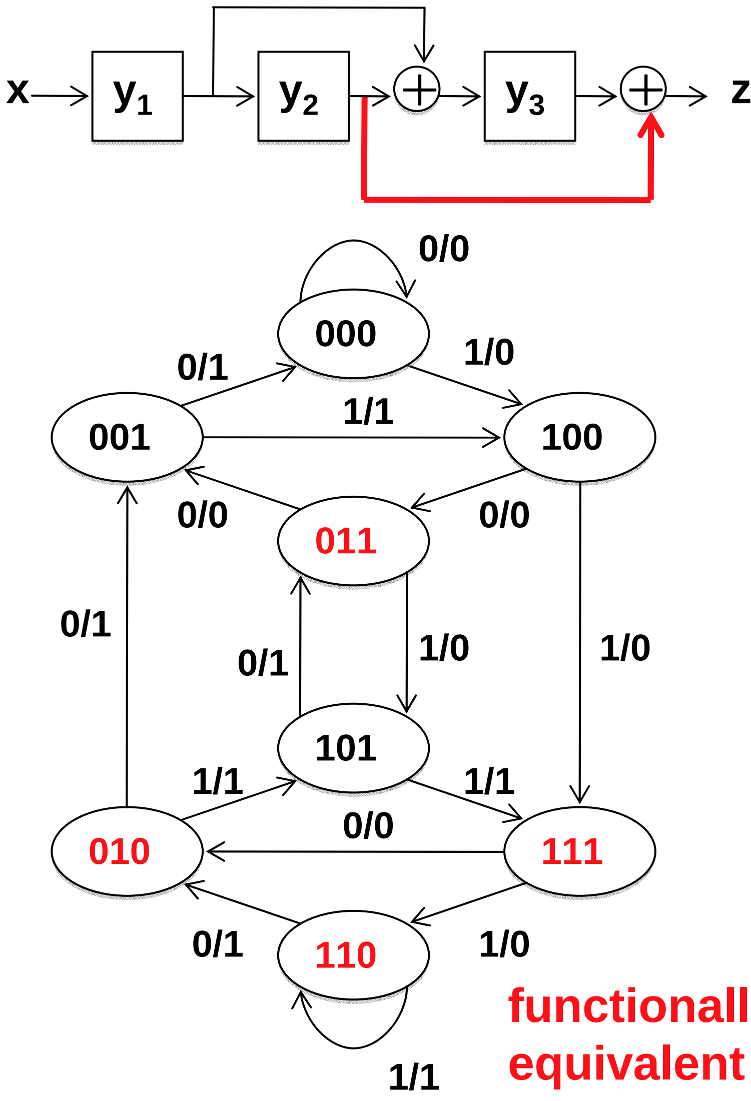
Input-equivalent but not output-equivalent

Linear Feed-Forward SR (LF²SR)



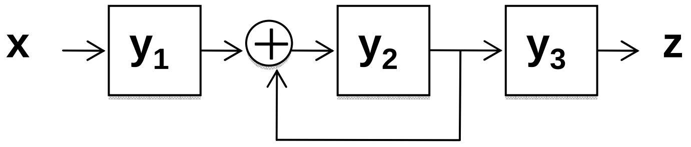
010
011
110
111

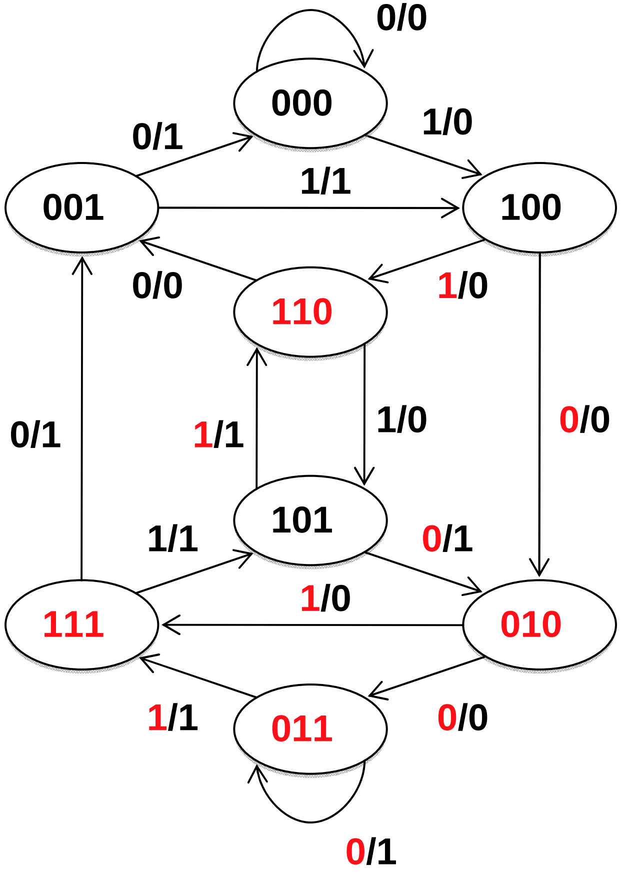
y_2



functionally equivalent

Linear Feedback SR (LFSR)



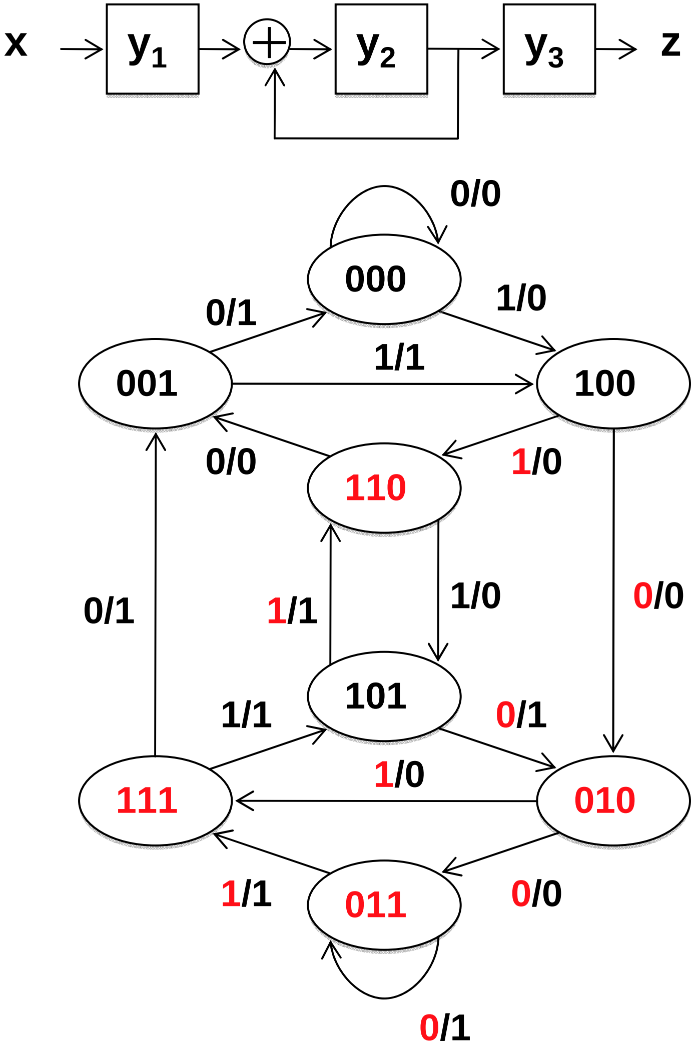


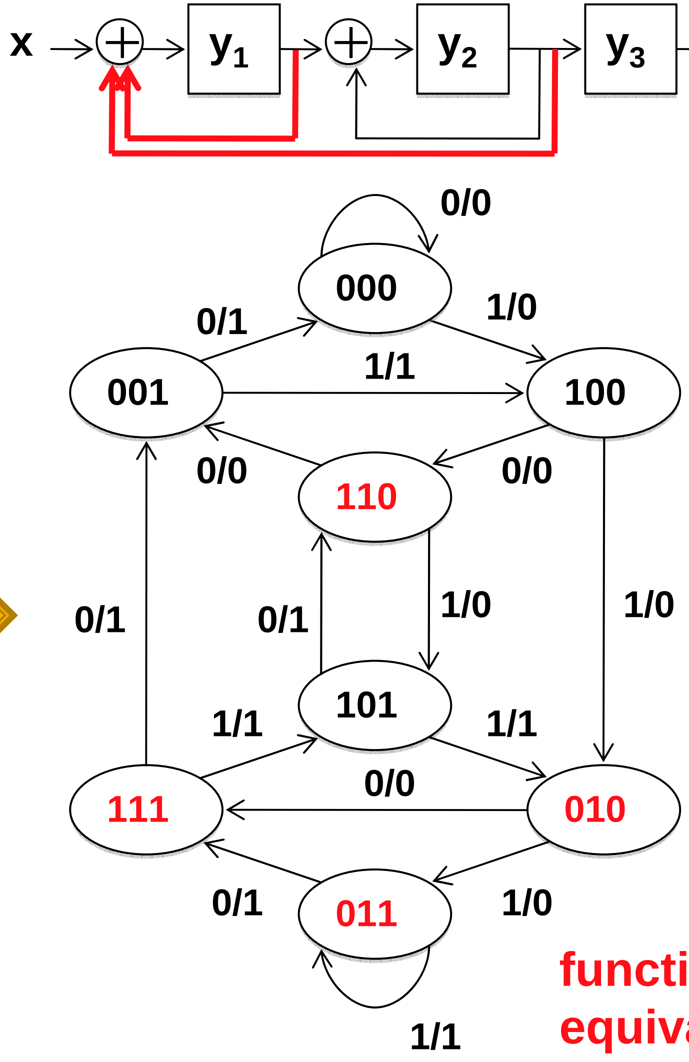
Any k-stage LFSR is *output-equivalent* to a k-stage SR.

Can be **modified** to be input-equivalent (and hence functionally equivalent) to the k-stage SR, by **manipulating the linear sum of the input**.

Output-equivalent but not input-equivalent

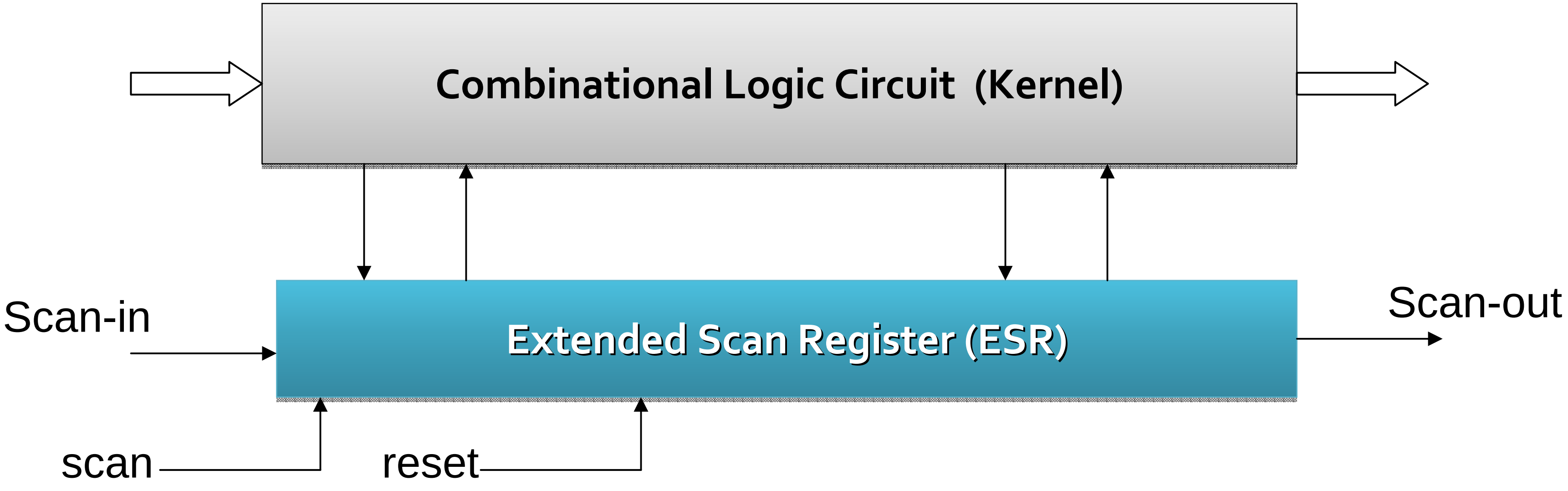
Linear Feedback SR (LFSR)





functionally equivalent

Proposed Secure Scan Design


Combinational Logic Circuit (Kernel)
Scan-in
Extended Scan Register (ESR)
Scan-out
scan
reset

Proposed scan design with ESR

Satisfies both Scan-Testability and Scan-Security

Scan-Controllability/Observability

- An ESR is *scan-controllable*
  - if for any internal state of R a transfer sequence (of length k) to the state (final state) can be generated only from the connection information of R

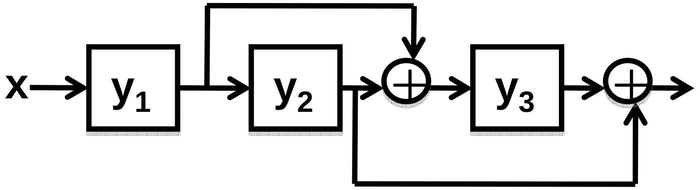
    → independently of the initial state (where k is the size of R)

- An ESR is *scan-observable*
  - if any present state (initial state) of R can be identified only from the output sequence (of length k) and the connection information of R

    → independently of the initial state and the input sequence (where k is the size of R)

Scan-Testability Illustrated (LF²SR)

$y_1(t) = x(t-1)$
$y_2(t) = y_1(t-1)$
$y_3(t) = y_1(t-1) + y_2(t-1)$
$z(t) = y_2(t) + y_3(t)$



$x(t-3) = y_1(t)$
$x(t-2) = y_2(t)$
$x(t-1) = y_2(t) + y_3(t)$

The transfer sequence to state ($y_1(t)$, $y_2(t)$, $y_3(t)$)
is uniquely obtained only from the destination state,
independently of the initial state.

Scan-controllable

$y_1(t) = z(t+2)$
$y_2(t) = z(t+1)$
$y_3(t) = z(t) + z(t+1)$

The initial state ($y_1(t)$, $y_2(t)$, $y_3(t)$)
can be identified only from
the output sequence of length 3.

Scan-observable

Scan-Testability of Secure Scan Design

- An extended shift register is *scan-testable* if R is scan-controllable and scan-observable.

- A circuit with ESR is called to be *scan-testable* if the ESR is scan-testable.

Any extended shift register that is functionally equivalent to a shift register is scan-testable.

How to make ESR scan-testable?

- I^2SR – can be functionally equivalent by even number of inversions
- LF^2SR and LFSR – can be functionally equivalent by output and input manipulations, resp.

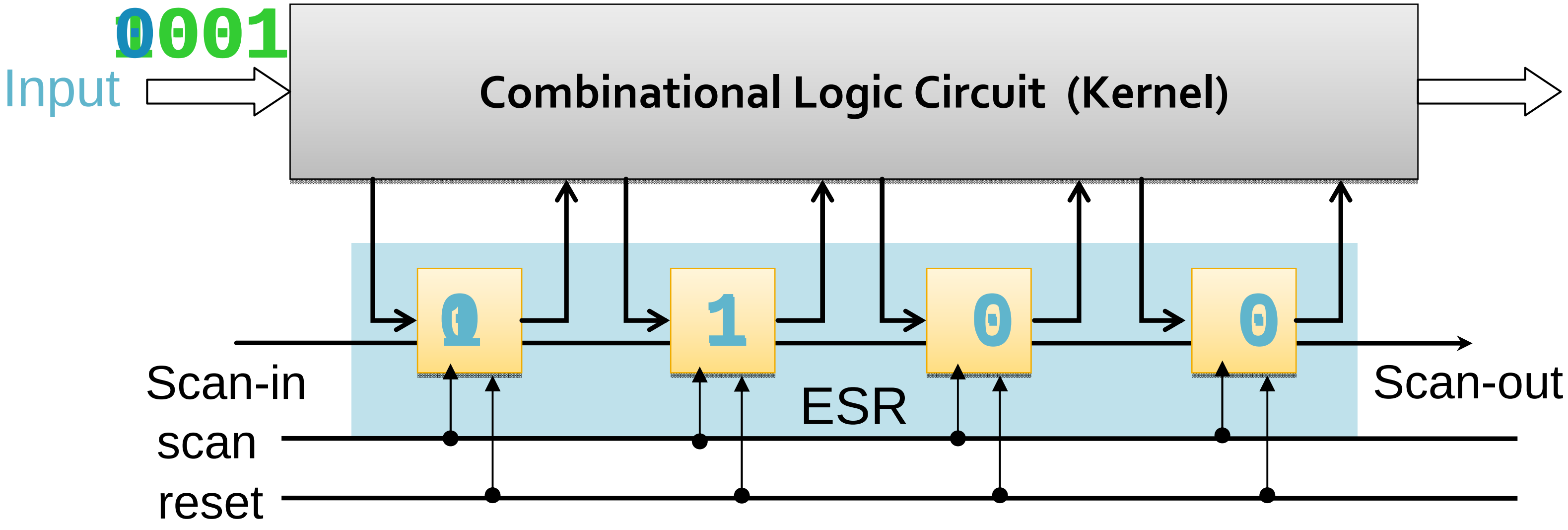
Scan-Security

A circuit with ESR is *scan-secure* if the attacker cannot determine the structure of the ESR.

Attacker Assumptions:

1. Knows NOT the detailed information in the gate-level design.
2. Knows the cryptographic algorithm/general implementation structure at high level.
   - Can make bit-change insertion attack or differential values attack.
3. Knows the presence of test pins and scan chains, but NOT the structure of ESR.

Single-bit Change Insertion Attack



Input Sequence A: 1 0 0 1 OUT : 1 1 0 0

Input Sequence B: 0 0 0 1 OUT : 0 1 0 0

- Parallel inputs from kernel can be used to make bit-change insertion attack/differential values attack.

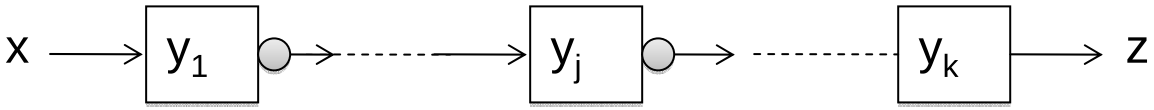
Scan-Security of Secure Scan Design

A circuit with ESR is *scan-secure* if the attacker cannot uniquely determine the structure of the ESR.

How to make ESR scan-secure?

- I^{2}SR – with reset is not secure!
  - So, add an extra control flip-flop to prevent scan operation after reset.
- LF^{2}SR and LFSR – can be attacked with single-bit change
  - So, insert dummy flip-flop to make ESR indistinguishable.

Scan-Security: I²SR

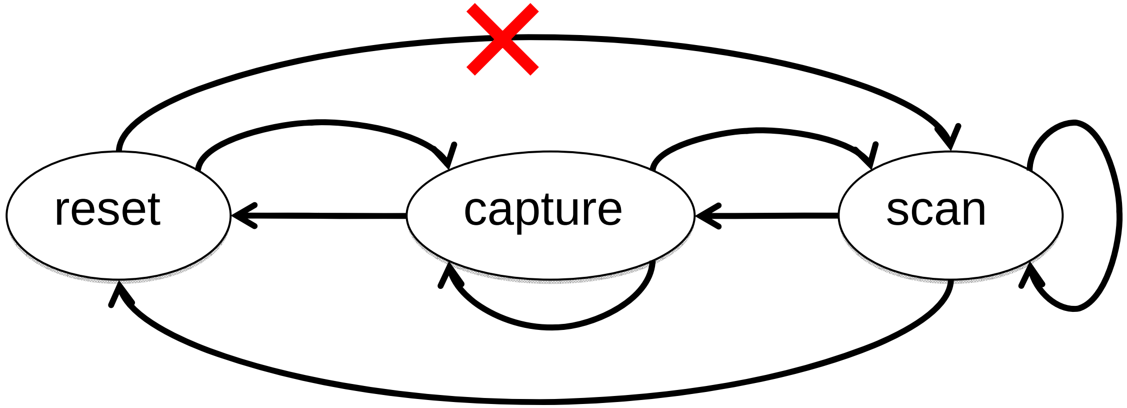


- *Single-bit change insertion attack:*
  - The sequential depth of each flip-flop can be identified.
  - The locations of NOT gate cannot be identified.

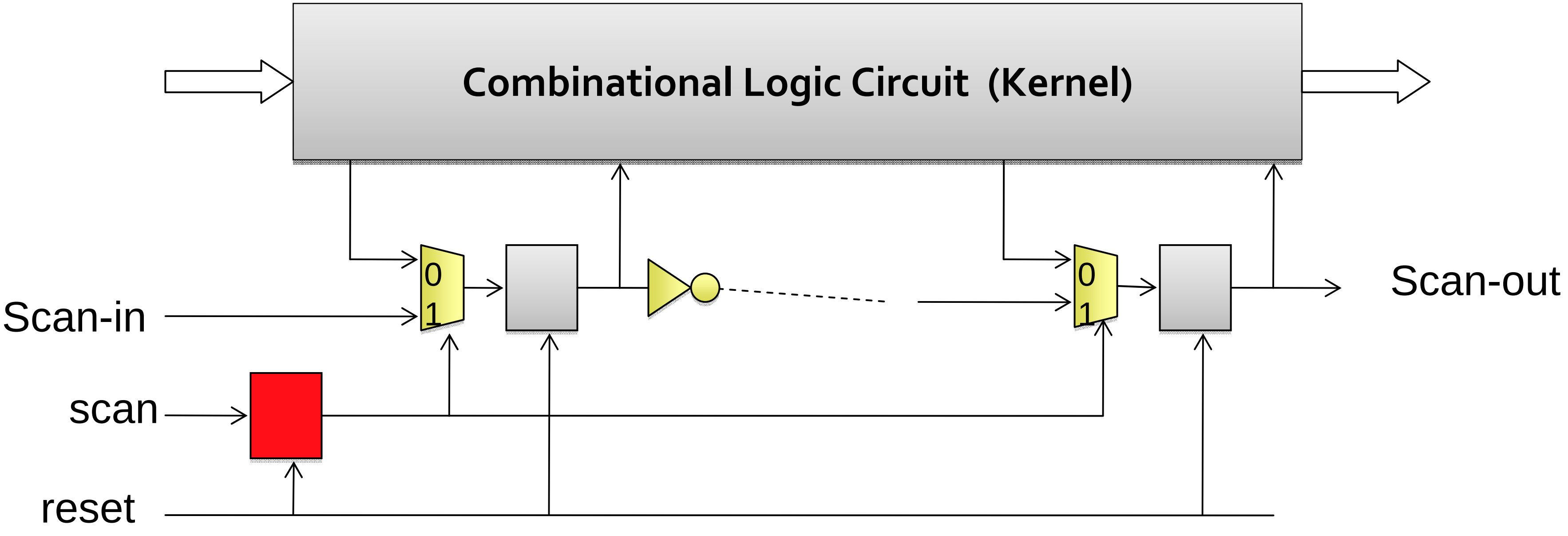
BUT! With reset, all the locations of NOT gate
are identified by scanning after reset (to all zero).
The internal state can be identified.

  - So, for the I²SR with reset, the following technique is necessary to guarantee the security.

Scan-Secure I²SR

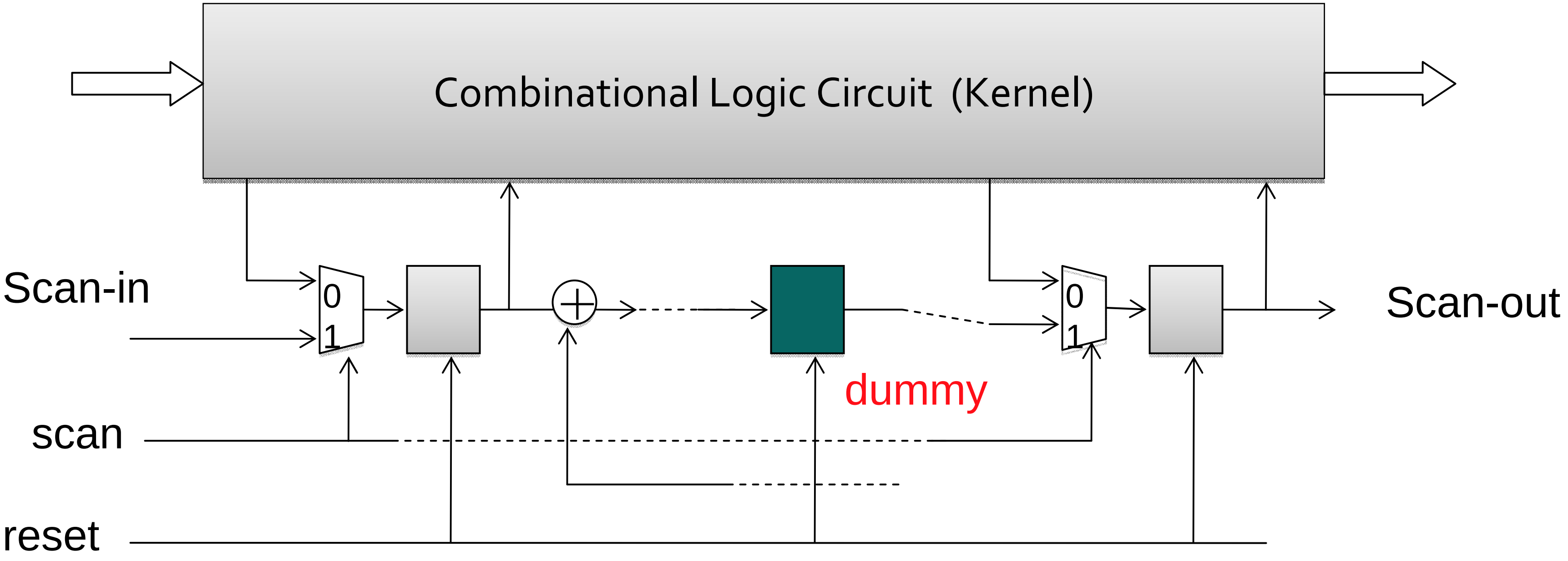


I²SR with control FF is scan-secure

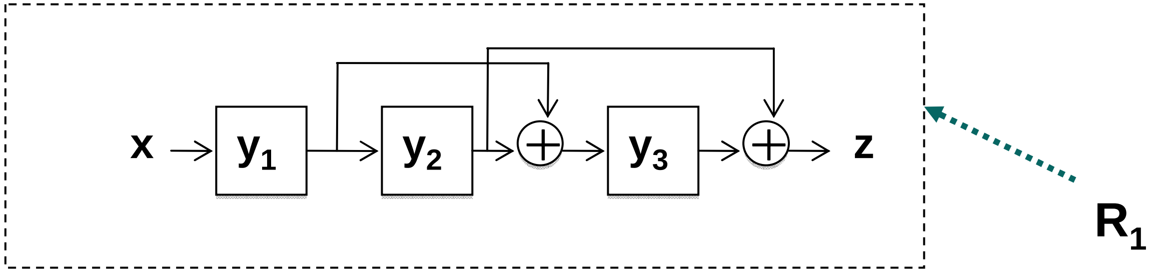


Scan-Secure LF²SR and LFSR

Any *scan-testable* LF²SR and LFSR can be *scan-secure* by inserting *dummy* flip-flops or by disconnecting flip-flops from the kernel (making them *dummy*).



Single-bit Change Insertion Attack (LF²SR)



Differential value injected from x

Differential value injected from y_1

time

x	y_1	y_2	y_3	z
d	-	-	-	-
-	d	-	-	-
-	-	d	d	-
-	-	-	d	d
-	-	-	-	-

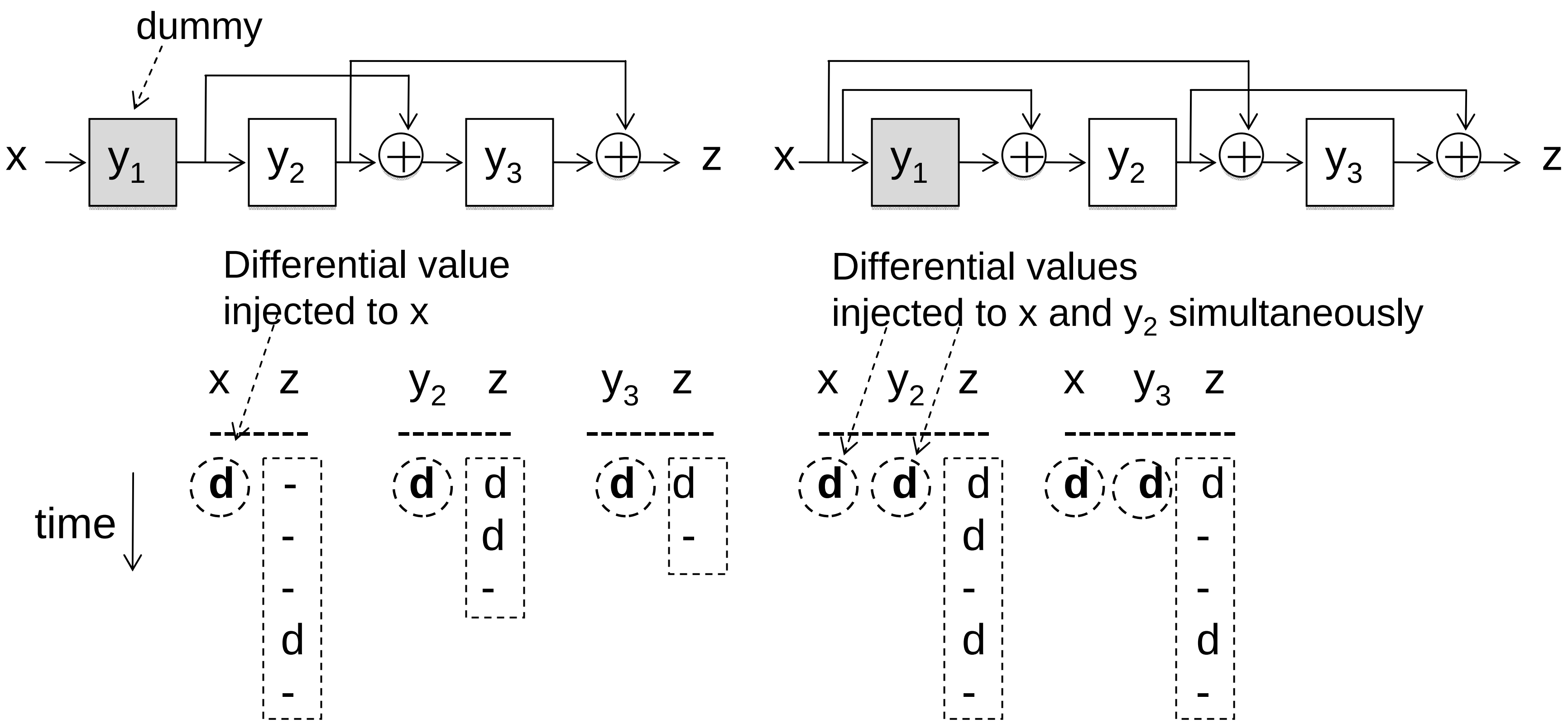
y_1	y_2	y_3	z
d	-	-	-
-	d	d	-
-	-	d	d
-	-	-	-

y_1	y_2	y_3	z
-	**d**	-	d
-	-	d	d
-	-	-	-

y_1	y_2	y_3	z
-	-	**d**	d
-	-	-	-

The LF²SR that behaves like the above is *uniquely identified* to be R_1, therefore, this is not scan-secure.

Indistinguishable LF²SRs with dummy FF



Differential value injected to x

x	z
d	-
	-
	-
	d
	-

y_2	z
d	d
	d
	-

y_3	z
d	d
	-

Differential values injected to x and y_2 simultaneously

x	y_2	z
d	**d**	d
		d
		-
		d
		-

x	y_3	z
d	**d**	d
		-
		-
		d
		-

Both LF²SRs generate the same responses by single-bit change insertion, and hence cannot be distinguished from each other.

Both scan-secure

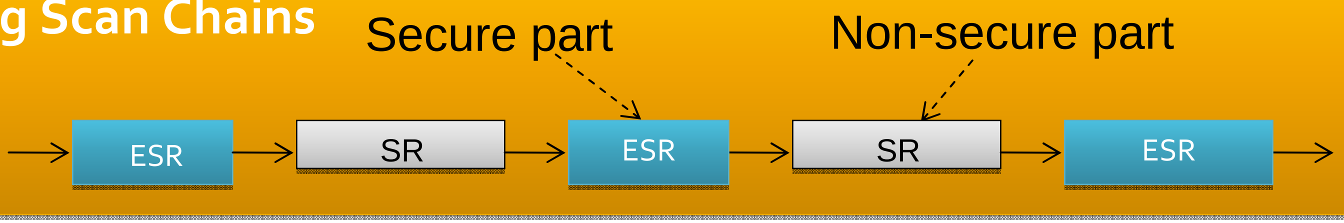
Cardinality of Indistinguishable Extended SRs and Area Cost

A cascade of any two extended scan registers (ESR) that are scan-secure and scan-testable is also scan-secure and scan-testable.

- **I²SR:**
  - $2^k - 1$ → $\Theta(2^k)$ where Θ = asymptotically tight bound
  - Less area overhead
- **LF²SR and LFSR:**
  - $2^{k(k+1)/2} - 1$ → $\Omega(2^k)$ where Ω = asymptotic lower bound
  - Inferior to I²SR in terms of area overhead

# of Indistinguishable LF²SR and LFSR grows exponentially (k) → very high security

For Long Scan Chains



Conclusion

1. Introduced a new secure scan design approach.

2. Presented three types of *scan-testable* and *scan-secure extended scan registers* (I^2SR, LF^2SR, and LFSR).
   - Done by adding extra control flip-flop, adjusting input/output, and introducing dummy flip-flops.

3. The proposed secure scan design requires little area overhead and no performance overhead for normal operation. No additional keystreams involved.

Future Work

1. Cardinality of each class of shift register equivalents.
2. Synthesis problem for desired shift register equivalents without using state diagrams.
3. State justification/observation problem for shift register equivalents without using state diagrams.
4. Scan security for multiple bit change attacks.