Secure Scan Design using Shift Register Equivalents against Differential Behavior Attack

Hideo Fujiwara**, Katsuya Fujiwara*, and Hideo Tamamoto*

* Akita University

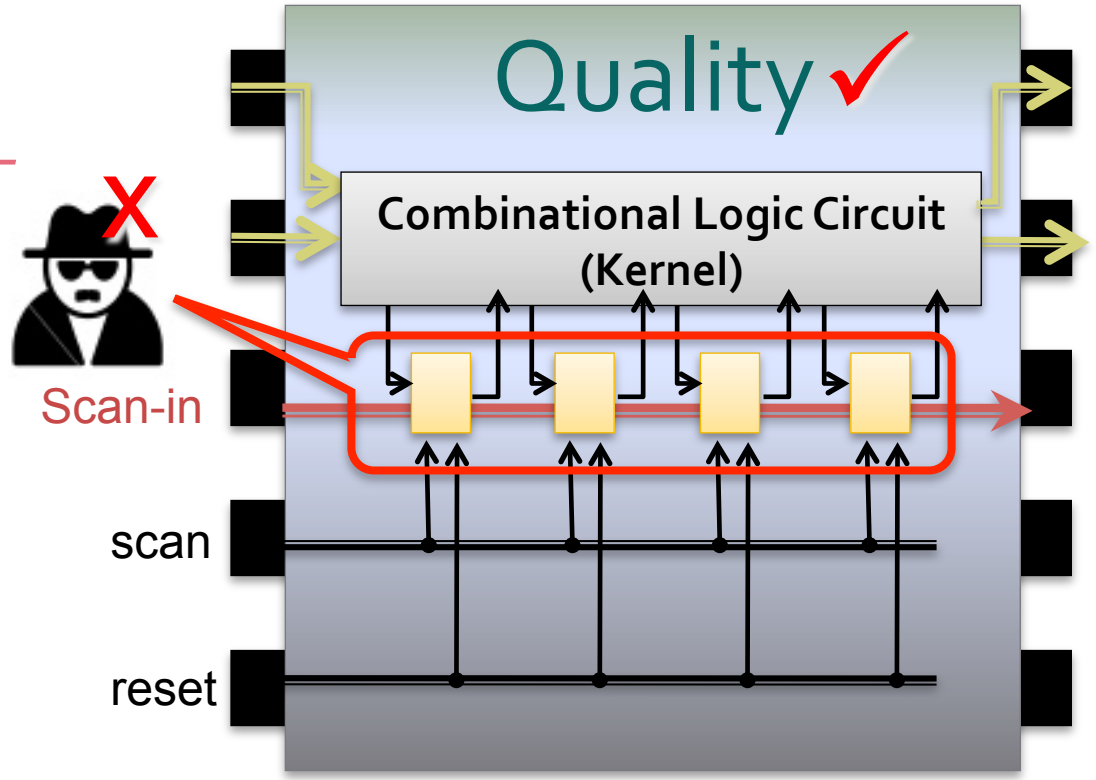
** Nara Institute of Science and Technology (NAIST)

Outline

1. Background and Motivation
2. Previous Works
3. Objective of the Study
4. Proposed Secure Scan Design
   - 4.1 SR-Equivalent Circuits
   - 4.2 How to Design/Control/Observe SR-Equivalent Circuits
   - 4.4 Application to Scan Design
5. Differential Behavior Attack
   - 5.1 Differential Behavior Equivalent
   - 5.2 Identification of Scan Structure
   - 5.3 Cardinality of Differential Behavior Equivalents
6. Conclusion

Background and Motivation

- Reliability
  → *Scan Design: most popular DFT*
- Protection of information
  → *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
  - U. Chandran, et al. 2009 –

- 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

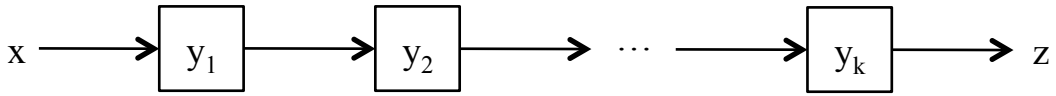
Objective of the Study

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

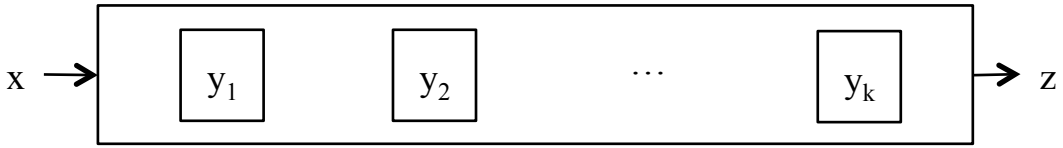
  Which leads to:
  - Little area overhead
  - No performance overhead

- Introduce SR-equivalent scan circuits
  - How to design/control/observe SR-equivalents
  - How to apply it to scan design
- Consider scan-based differential-behavior attack
  - Propose SR-equivalent scan circuits with dummy FFs to protect differential-behavior attack
- Consider security level
  - Cardinality of d-behavior equivalents

SR-Equivalent Circuits



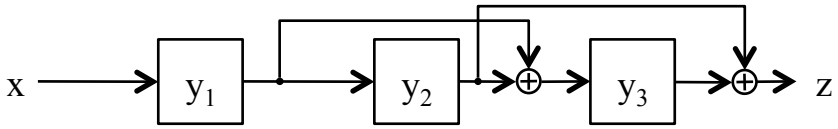
k-stage shift register, SR



k-stage SR-equivalent circuit, C

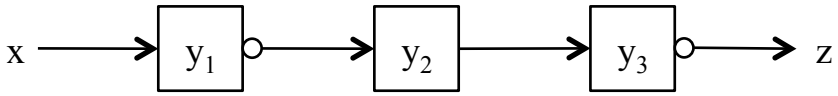
A circuit C with a single input x, a single output z, and k flip-flops is called *functionally equivalent* to a k-stage shift register
(or *SR-equivalent*)
if the input value applied to x at any time t appears at z after k clock cycles, i.e., z(t+k) = x(t) for any time t.

Example: SR-equivalent circuit R_1

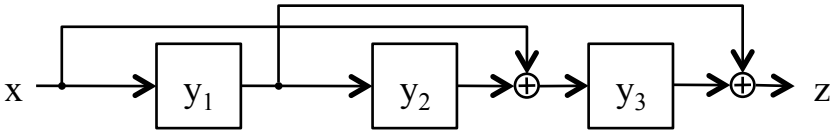


x	y_1	y_2	y_3	z
$x(0)$	$y_1(0)$	$y_2(0)$	$y_3(0)$	$z(0) = y_2(0) \oplus y_3(0)$
$x(1)$	$x(0)$	$y_1(0)$	$y_1(0) \oplus y_2(0)$	$z(1) = y_2(0)$
$x(2)$	$x(1)$	$x(0)$	$x(0) \oplus y_1(0)$	$z(2) = y_1(0)$
	$x(2)$	$x(1)$	$x(1) \oplus x(0)$	$z(3) = x(0)$

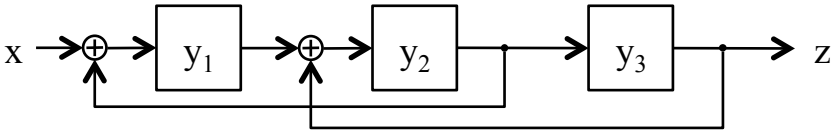
Five Types of Linear Circuits



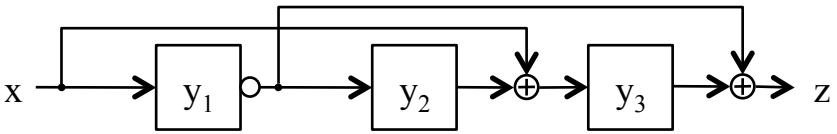
Inversion-Inserted SR (I^2SR)



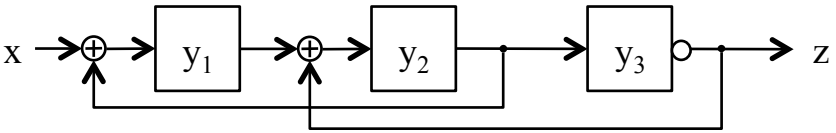
Linear Feed-Forward SR (LF^2SR)



Linear Feedback SR (LFSR)

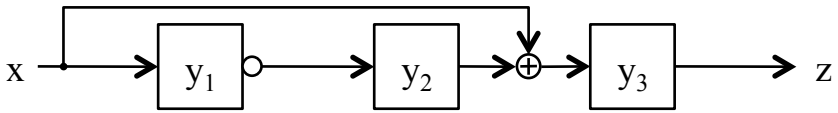


Inversion-Inserted Linear Feed-Forward SR (I^2LF^2SR)



Inversion-InsertedLinear Feedback SR (I^2LFSR)

How to Design SR-Equivalent Circuits 1/2

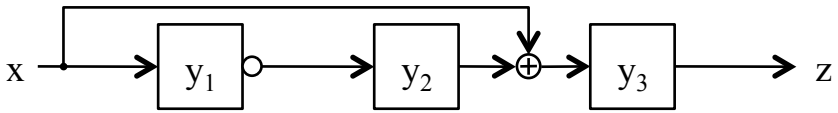


Given I^2LF^2SR

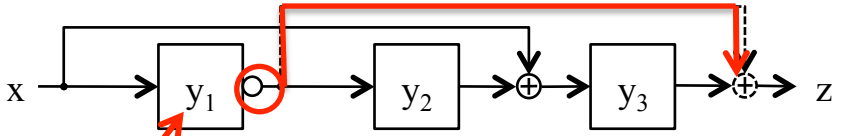
x	y_1	y_2	y_3	z
$x(0)$	$y_1(0)$	$y_2(0)$	$y_3(0)$	$z(0)=y_3(0)$
$x(1)$	$x(0)$	$1\oplus y_1(0)$	$x(0)\oplus y_2(0)$	$z(1)=x(0)\oplus y_2(0)$
$x(2)$	$x(1)$	$1\oplus x(0)$	$x(1)\oplus 1\oplus y_1(0)$	$z(2)=x(1)\oplus 1\oplus y_1(0)$
	$x(2)$	$1\oplus x(1)$	$x(2)\oplus 1\oplus x(0)$	$z(3)=x(2)\oplus 1\oplus x(0)$

Symbolic simulation

How to Design SR-Equivalent Circuits 2/2



Given I²LF²SR

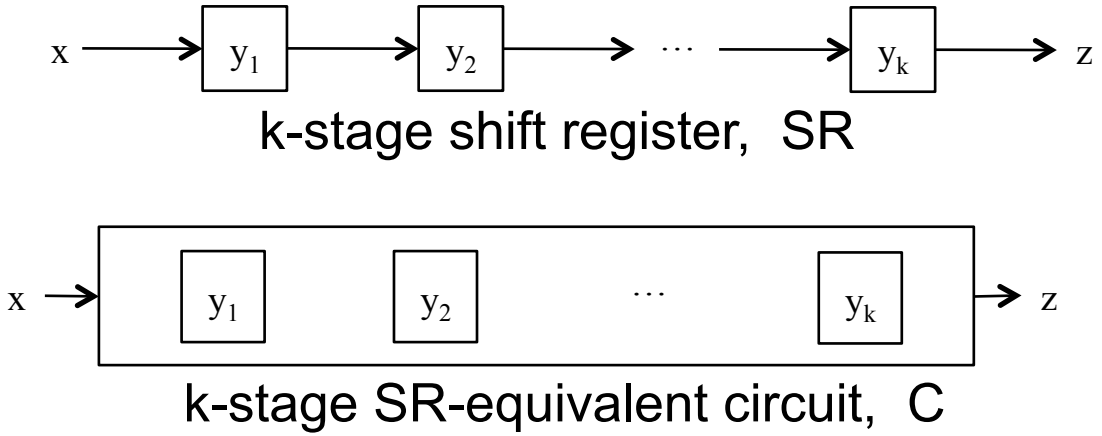


Modified SR-equivalent I²LF²SR

x	y_1	y_2	y_3	z
$x(0)$	$y_1(0)$	$y_2(0)$	$y_3(0)$	$z(0)=y_3(0)$
$x(1)$	$x(0)$	$1 \oplus y_1(0)$	$x(0) \oplus y_2(0)$	$z(1)=x(0) \oplus y_2(0)$
$x(2)$	$x(1)$	$1 \oplus x(0)$	$x(1) \oplus 1 \oplus y_1(0)$	$z(2)=x(1) \oplus 1 \oplus y_1(0)$
	$x(2)$	$1 \oplus x(1)$	$x(2) \oplus 1 \oplus x(0)$	$z(3)=x(2) \oplus 1 \oplus x(0)$

Symbolic simulation

How to Control/Observe SR-Equivalents



To utilize the SR-equivalent circuit C as a shift register SR, we need to consider the following two problems.

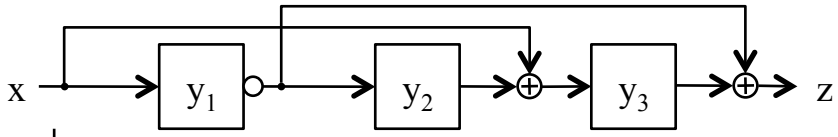
State-Justification: (Scan-in)

To generate an input sequence to transfer the circuit C into a given desired state, independently of the initial state.

State-Observation: (Scan-out)

To identify the initial state by observing the output sequence from the state, independently of the input sequence.

How to Control SR-Equivalent Circuits, R_2



SR-equivalent I^2LF^2SR, R_2

x	y_1	y_2	y_3	z
$x(0)$	$y_1(0)$	$y_2(0)$	$y_3(0)$	$z(0)=1\oplus y_1(0)\oplus y_3(0)$
$x(1)$	$x(0)$	$1\oplus y_1(0)$	$x(0)\oplus y_2(0)$	$z(1)=1\oplus y_2(0)$
$x(2)$	$x(1)$	$1\oplus x(0)$	$x(1)\oplus 1\oplus y_1(0)$	$z(2)=y_1(0)$
	$x(2)$ $=y_1(3)$	$1\oplus x(1)$ $=y_2(3)$	$x(2)\oplus 1\oplus x(0)$ $=y_3(3)$	$z(3)=x(0)$

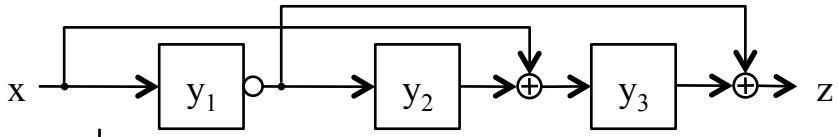
$$x(0) = 1\oplus y_1(3)\oplus y_3(3)$$

$$x(1) = 1\oplus y_2(3)$$

$$x(2) = y_1(3)$$

Transfer sequence x(0),x(1),x(2) for final state $y_1(3)$,$y_2(3)$,$y_3(3)$ is expressed by final state only, independently of initial state.

How to Observe SR-Equivalent Circuits, R_2



SR-equivalent I^2LF^2SR, R_2

x	y_1	y_2	y_3	z
$x(0)$	$y_1(0)$	$y_2(0)$	$y_3(0)$	$z(0)=1\oplus y_1(0)\oplus y_3(0)$
$x(1)$	$x(0)$	$1\oplus y_1(0)$	$x(0)\oplus y_2(0)$	$z(1)=1\oplus y_2(0)$
$x(2)$	$x(1)$	$1\oplus x(0)$	$x(1)\oplus 1\oplus y_1(0)$	$z(2)=y_1(0)$
	$x(2)$	$1\oplus x(1)$	$x(2)\oplus 1\oplus x(0)$	$z(3)=x(0)$

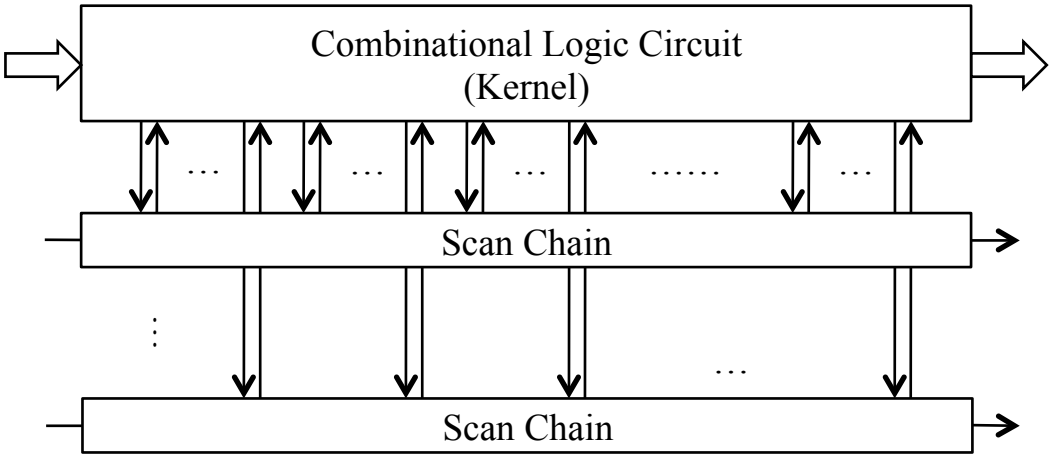
Initial state ($y_1(0)$,$y_2(0)$,$y_3(0)$) is identified from output sequence z(0),z(1),z(2) only, independently of the input sequence.

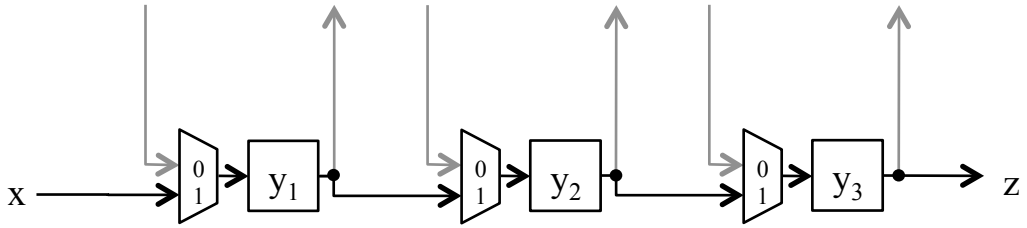
$$y_1(0) = z(2)$$

$$y_2(0) = 1\oplus z(1)$$

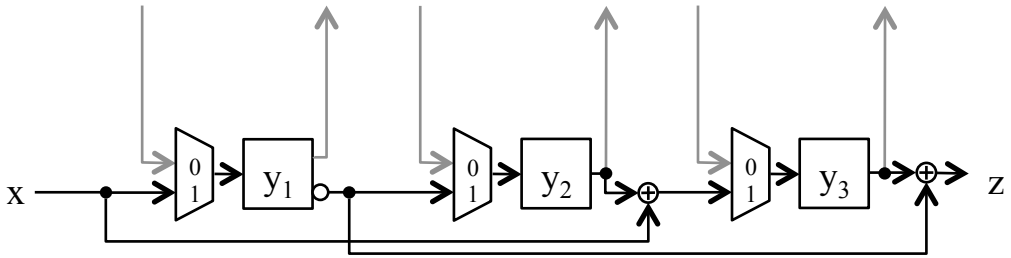
$$y_3(0) = 1\oplus z(0)\oplus z(2)$$

Application to Scan Design 1/3



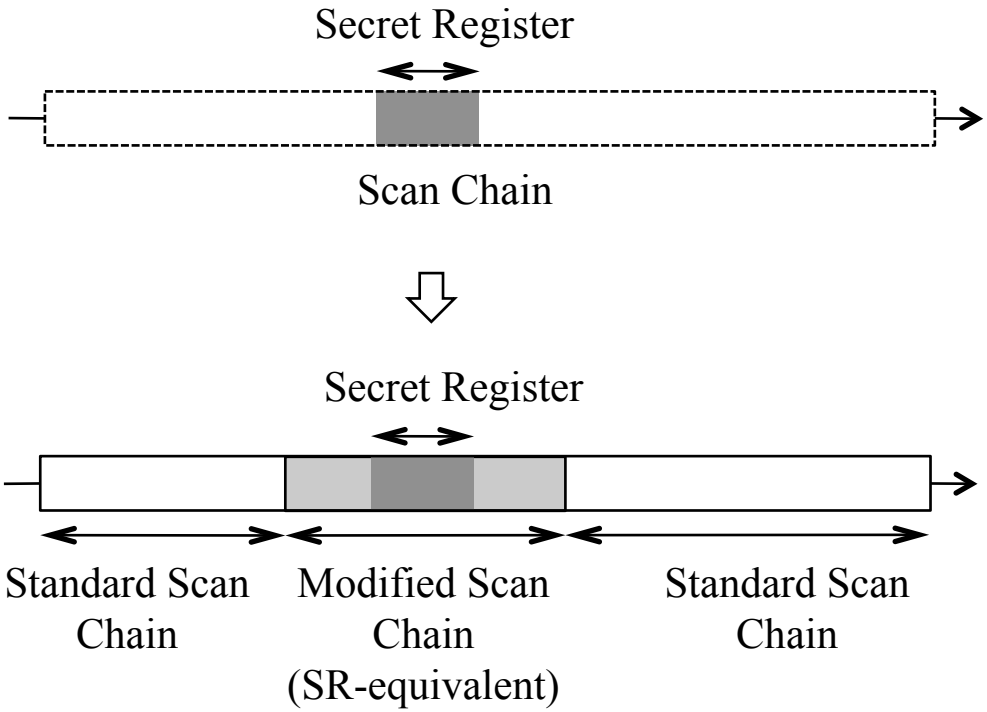


Standard scan register



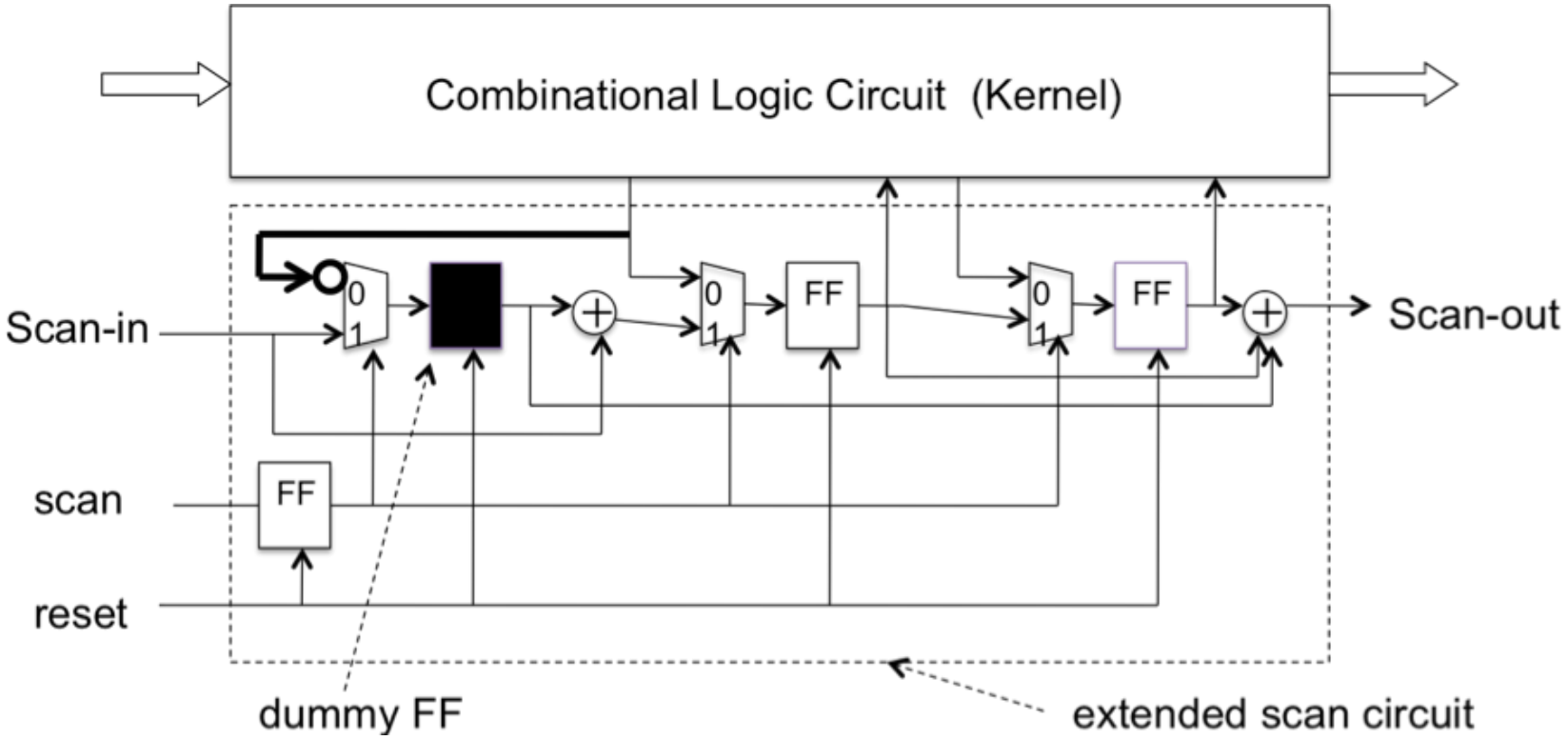
Modified scan register
(SR-equivalent)

Application to Scan Design 2/3



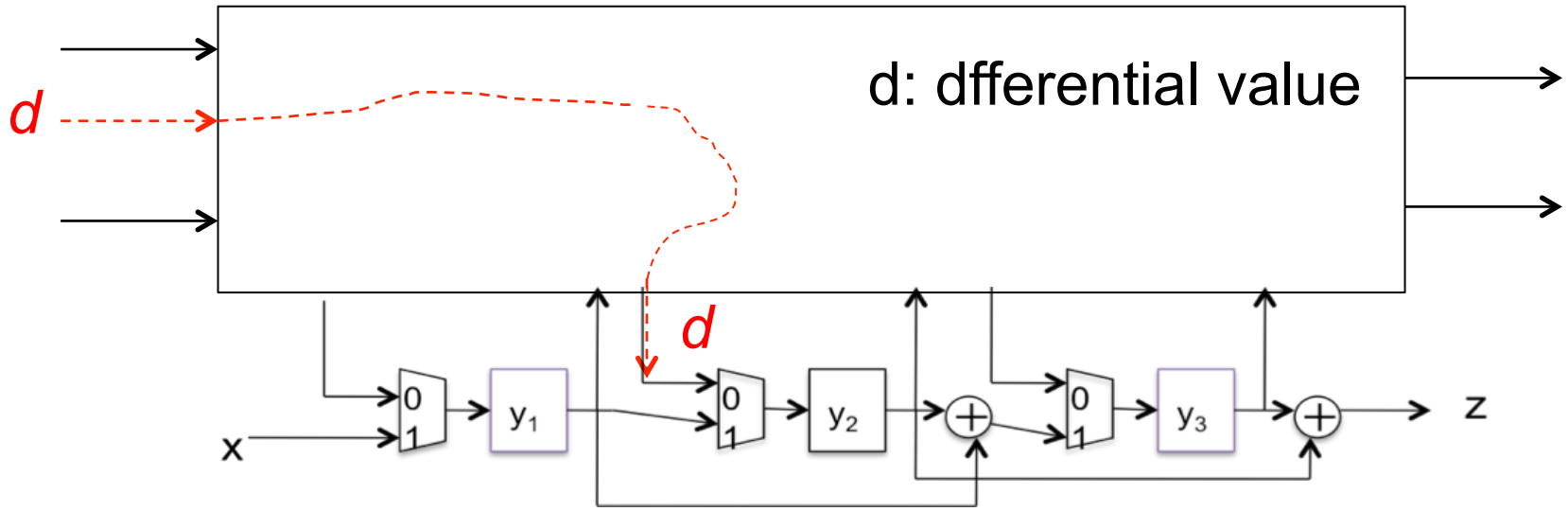
Replacement of scan chain by modified scan chain

Application to Scan Design 3/3



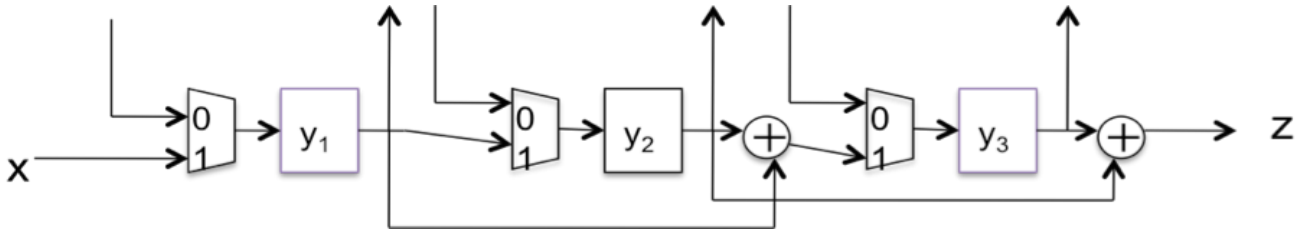
Scan design with SR-equivalent scan circuit

Differential Behavior (d-behavior)



- First, the circuit under test is reset and then run in normal mode.
- Next, it is switched to scan mode to scan out the contents of scan registers.
- These steps are repeated using another input sequence that is slightly different from the first input sequence.

Single-bit-change d-behavior for S_1



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

d: differential value
- : constant value

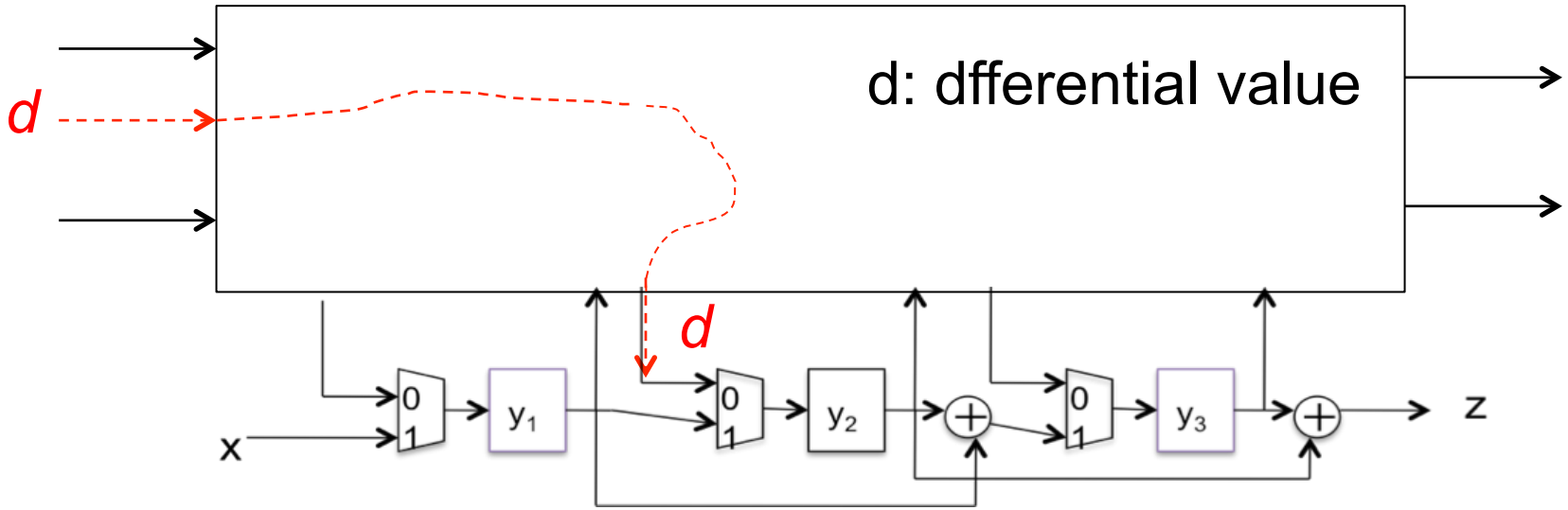
x	y_1	y_2	y_3	z
-	**d**	-	-	-
-	-	d	d	-
-	-	-	d	d
-	-	-	-	-

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

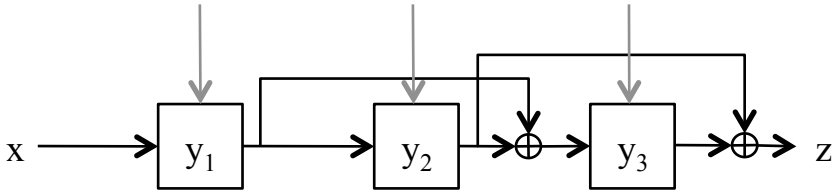
x	y_1	y_2	y_3	z
-	-	-	**d**	d
-	-	-	-	-
-	-	-	-	-
-	-	-	-	-

Differential-behavior Attack

The attack that inserts differential values into extended scan registers in normal mode and observes the differential behaviors in scan mode is called a *differential-behavior attack*.



Differential-behavior set



Extended scan circuit, S_1

-	-	d	d	...	d
-	-	d	d		-
-	d	d	-		-
d	d	-	-		-

Differential-behavior set
(*d-behavior set*, for short) :
The set of all d-behaviors for S_1

-	-	d	d
-	-	d	-
-	d	-	-
d	-	-	-

Fundamental differential-behavior set
(*fundamental d-behavior set*, for short) :
The set of all *single-bit-change* d-behaviors for S_1

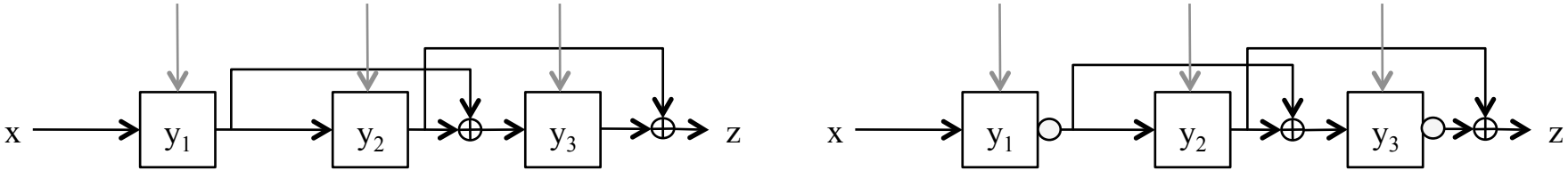
Differential-behavior equivalent relation

Let S_1 and S_2 be extended scan circuits.

S_1 and S_2 are said to be *differential-behavior equivalent* (or *d-behavior equivalent*, for short) if the d-behavior sets of S_1 and S_2 are the same.

Example of d-behavior equivalence

S_1 and S_2 are *d-behavior equivalent.*



d-behavior set of S_1

-	-	d	d		d
-	-	d	d	...	-
-	d	d	-		-
d	d	-	-		-

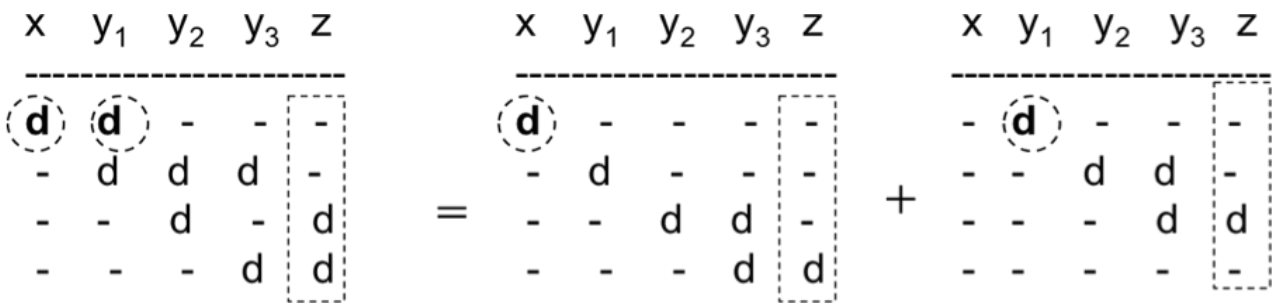
same

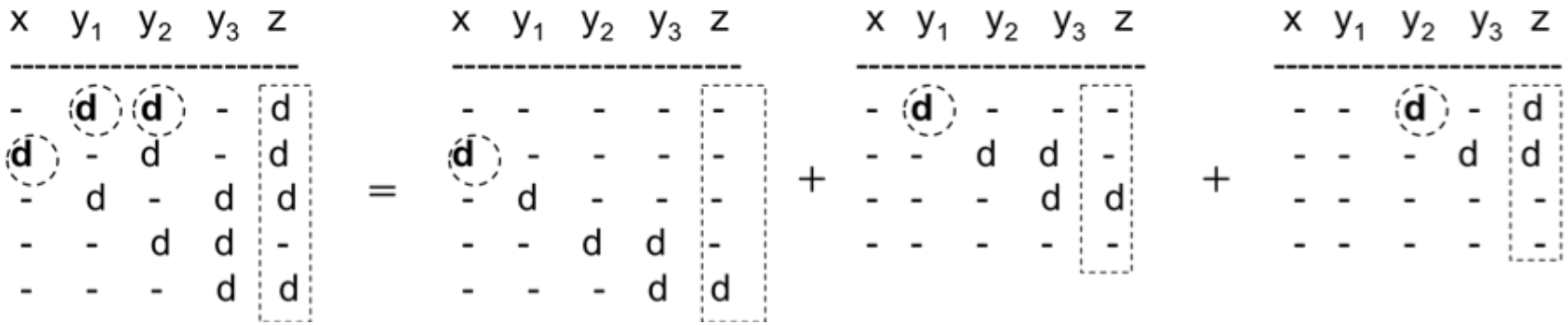
d-behavior set of S_2

-	-	d	d		d
-	-	d	d	...	-
-	d	d	-		-
d	d	-	-		-

d : differential value
- : constant value

XOR-superposition of fundamental d-behaviors





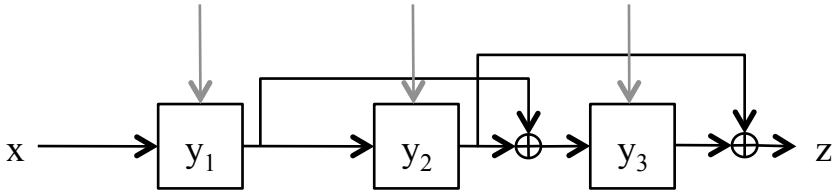
Any differential behavior can be uniquely expressed by XOR-superposition of fundamental d-behaviors only.

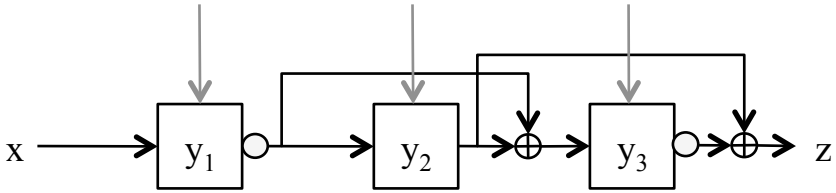
Theorems

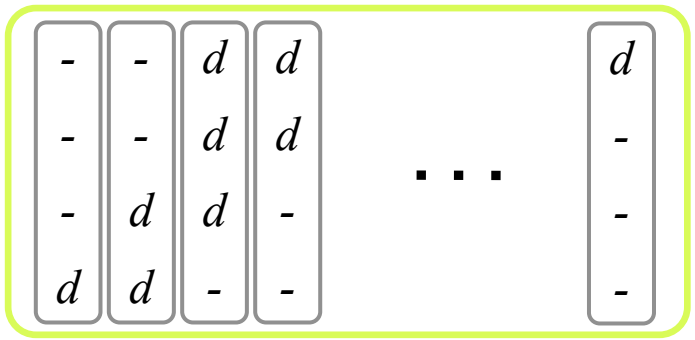
Theorem 1:
Any differential behavior can be uniquely expressed by XOR-superposition of fundamental d-behaviors only.

Theorem 2:
Let S_1 and S_2 be extended scan circuits.
S_1 and S_2 are d-behavior equivalent if and only if fundamental d-behavior sets of S_1 and S_2 are the same.

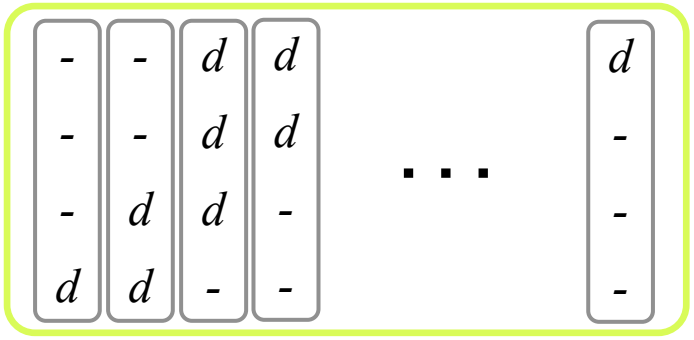
Example of d-behavior equivalent relation







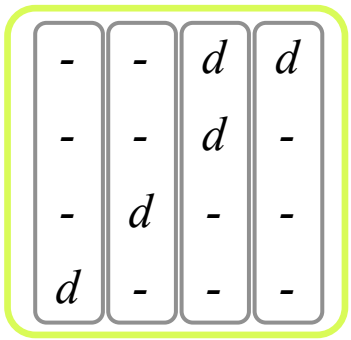
=



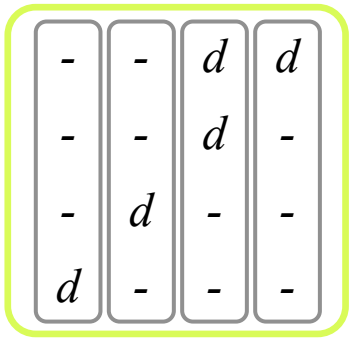
d-behavior set of S_1

iff

d-behavior set of S_2



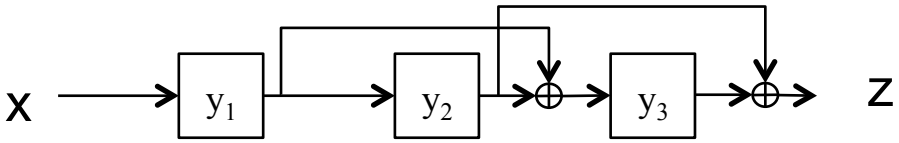
=



Fundamental d-behavior set of S_1

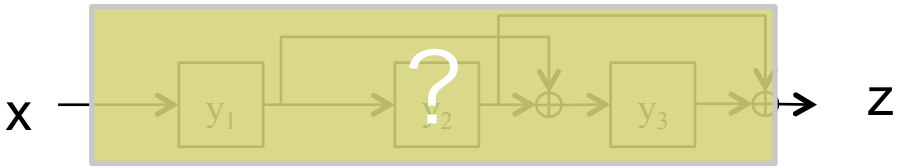
Fundamental d-behavior set of S_2

Identification of Scan Structure



This circuit R_1 is an 3-stage SR-equivalent LF^2SR.

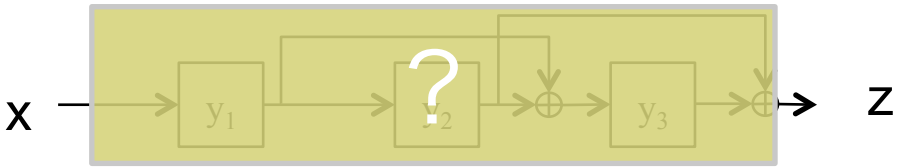
Identification of Scan Structure



# of 3-stage SR-equivalents = $2^k!/k! - 1 = 6{,}719$

# of 3-stage SR-equivalent LF^{2}SR = $2^{k(k1-)/2} - 1 = 7$

Identification of Scan Structure

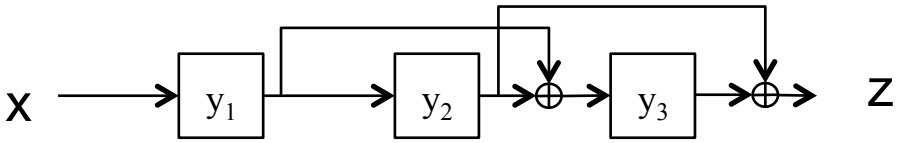


# of 3-stage SR-equivalents = $2^k!/k! - 1 = 6{,}719$
# of 3-stage SR-equivalent LF²SR = $2^{k(k1-)/2} - 1 = 7$

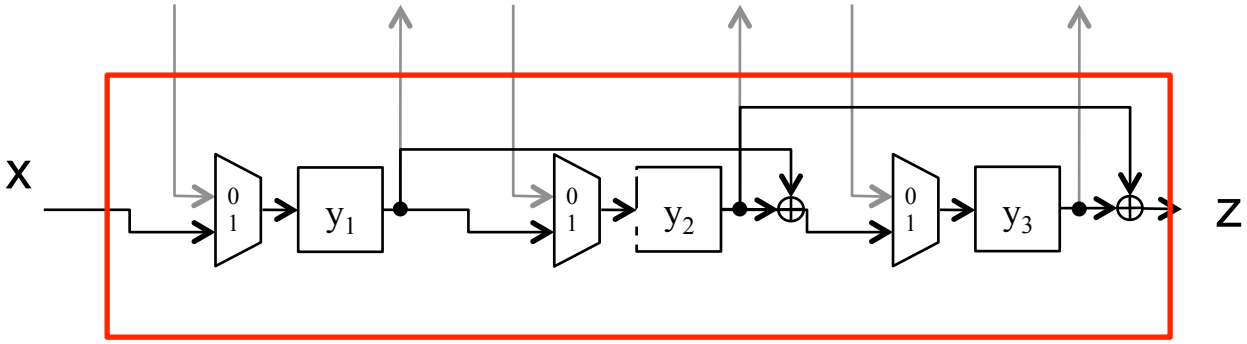
Probability to identify the configuration =
Reciprocal of the cardinality of SR-equivalents

For 3-stage SR-equivalents: 1/6719
For 3-stage SR-equivalent LF²SR: 1/7

Identification of Scan Structure

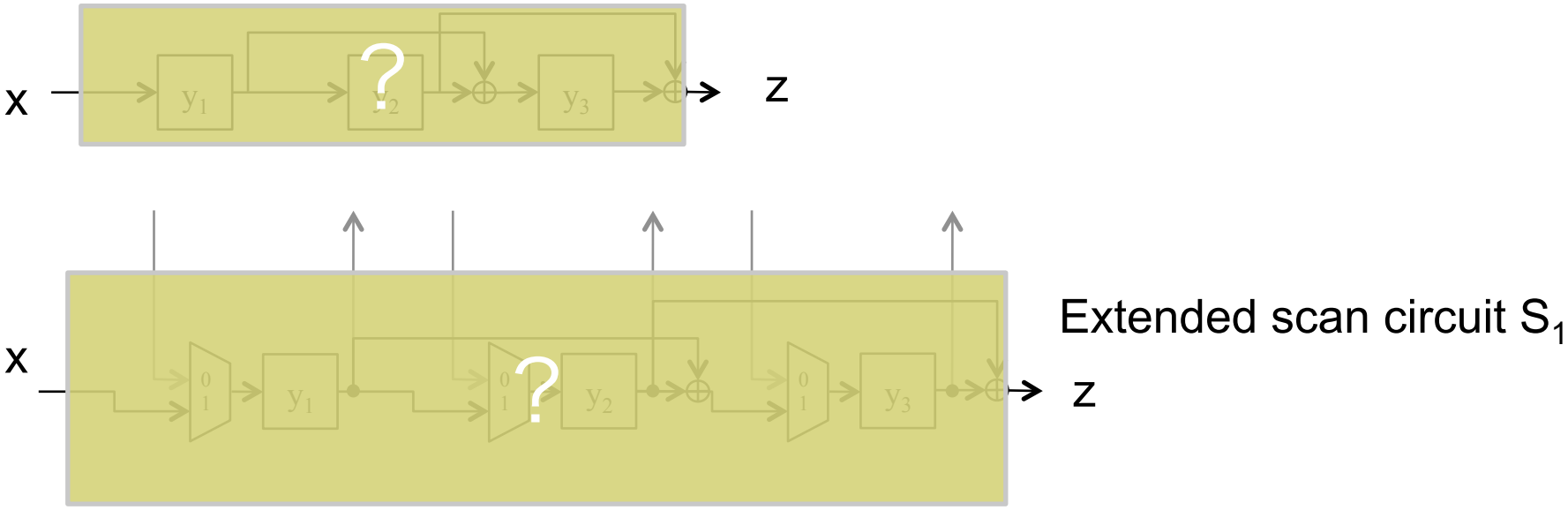


Extended shift register R_1



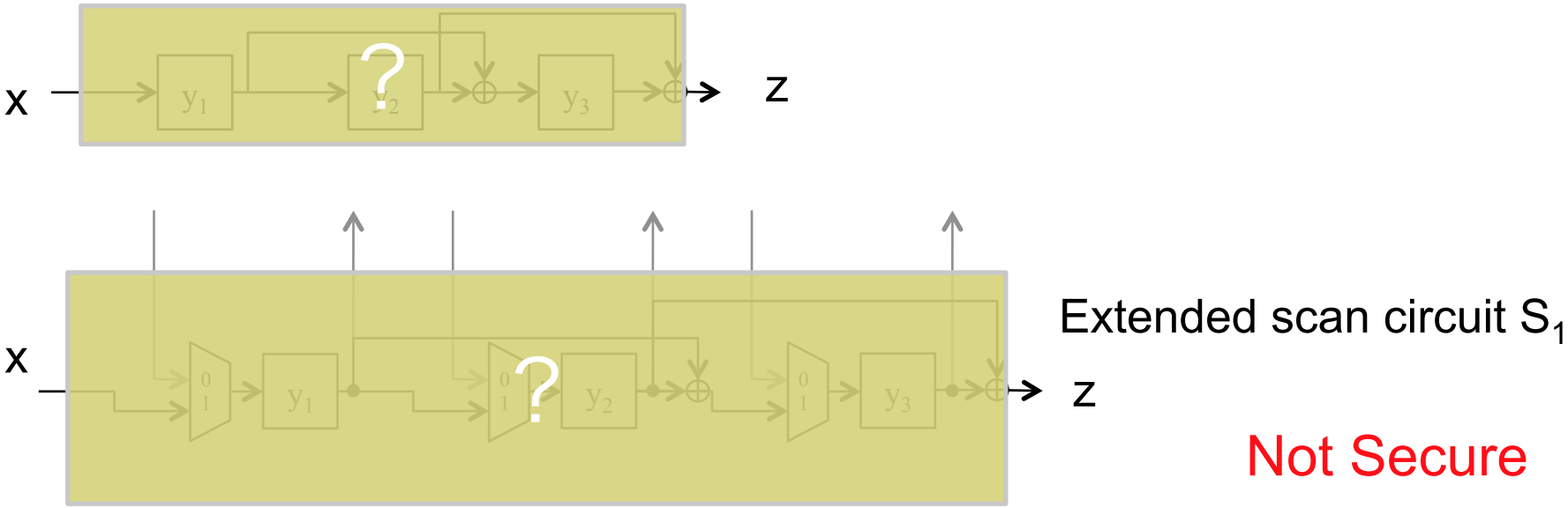
Extended scan circuit S_1

Identification of Scan Structure



# of 3-stage d-behavior equivalent LF²SR = 1

Identification of Scan Structure



Extended scan circuit S_1

Not Secure

# of 3-stage d-behavior equivalent LF^2SR = 1

Probability to identify the configuration =
Reciprocal of the cardinality of d-behavior equivalents

Identification of Scan Structure

The probability that an attacker can identify the configuration of an extended scan circuit S approximates to the reciprocal of the cardinality of the class of extended scan circuits that are d-behavior equivalent to S.

To evaluate the security level against d-behavior attacks, we clarify the cardinality of each equivalent class.

Cardinality of d-behavior equivalent classes

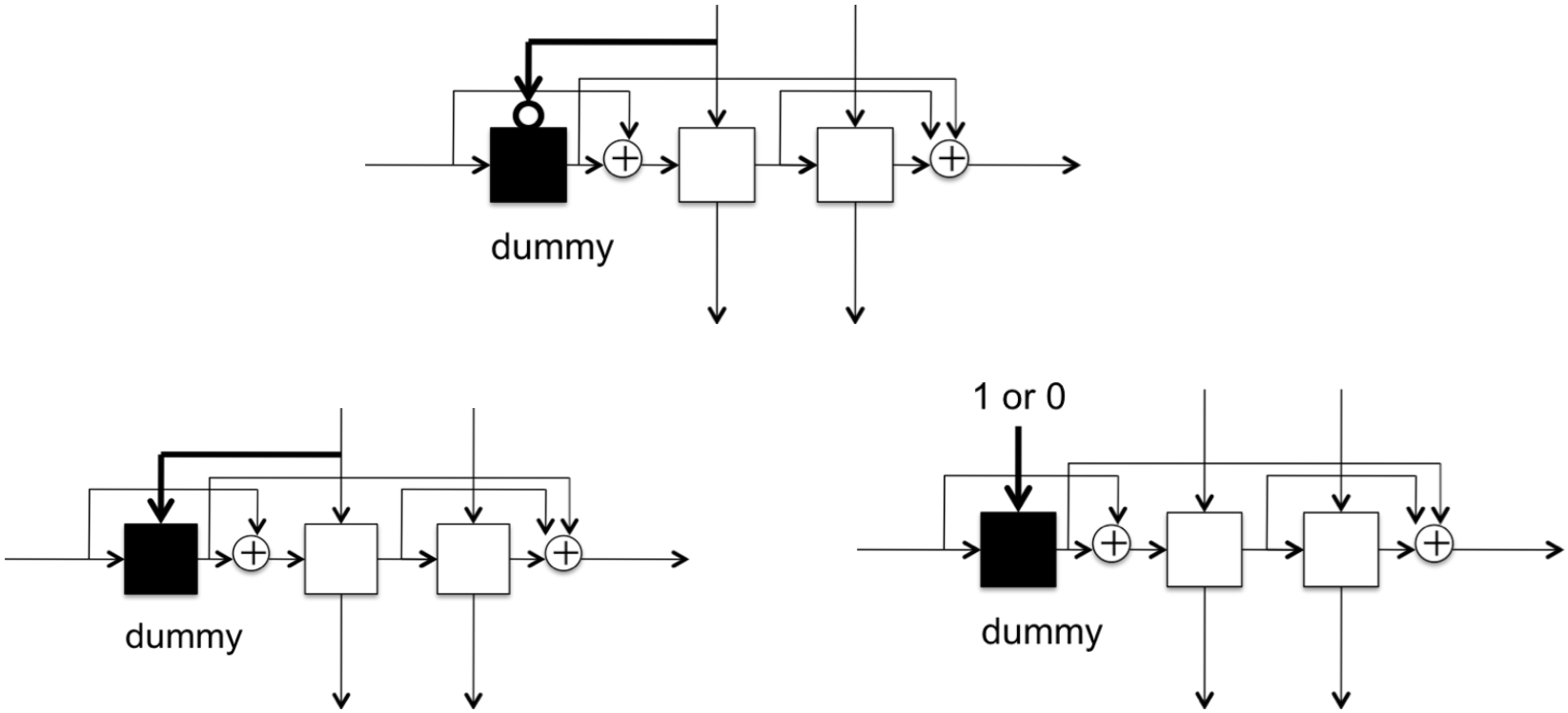
(without dummy FF)

	# of SR-Equivalent Scan Circuits	# of Equivalent Classes	Guaranteed Cardinality
I^2SR	$2^k - 1$	1	$2^k - 1$
LF^2SR (LFSR)	$2^{k(k-1)/2} - 1$	$2^{k(k-1)/2} - 1$	1
I^2LF^2SR (I^2LFSR)	$(2^{k(k-1)/2}-1)(2^k-1)$	$2^{k(k-1)/2} - 1$	$2^k - 1$

Two classes of LF^2SR and LFSR are not secure because their guaranteed cardinality is 1.

However, all other classes are secure.

SR-equivalent scan circuits with dummy FF



SR-equivalent scan circuits with dummy FF

Cardinality of d-behavior equivalent classes

(with dummy FF)

	# of SR-Equivalent Scan Circuits	# of Equivalent Classes	Guarantee Cardinality
I^2SR	$(3k^2+k)(2^k-1)/2$	$k(k+1)/2$	$3(2^k-1)$
LF^2SR (LFSR)	$(3k^2+k)(2^{k(k-1)/2}-1)/2$	$(2^{(k-1)(k-2)/2})(2^k-1)$	$O(k^2)$
I^2LF^2SR (I^2LFSR)	$(3k^2+k)(2^{k(k-1)/2}-1)(2^k-1)/2$	$(2^{(k-1)(k-2)/2})(2^k-1)$	$O(k^2 2^k)$

$O(k^2)$

$O(k^2 2^k)$

All classes with dummy FF are secure.

Especially the classes of I^2LF^2SR and I^2LFSR with dummy FF are the most secure thanks to high cardinality.

Enumeration Results by SREEP-2

To examine the actual cardinalities of d-equivalent classes for each type of extended scan circuits, we made a program called *SREEP-2 (Shift Register Equivalents Enumeration and Synthesis Program -2)*.

The enumeration results for extended scan circuits without and with dummy FF are shown in the following slides.

Cardinality of d-behavior equivalent classes (without dummy FF) by SREEP-2

	# FFs	# of Scan Circuits	# of Equivalent Classes	Guaranteed Cardinality	Range of Cardinality
I^2SR	k=3 k=4 k=5	7 15 31	1 1 1	7 15 31	7~7 15~15 31~31
LF^2SR (LFSR)	k=3 k=4 k=5	7 63 1023	7 63 1023	1 1 1	1~1 1~1 1~1
I^2LF^2SR (I^2LFSR)	k=3 k=4 k=5	49 945 31713	7 63 1023	7 15 31	7~7 15~15 31~31

Not Secure

Cardinality of d-behavior equivalent classes (with dummy FF) by SREEP-2

	# FFs	# of Scan Circuits	# of Equivalent Classes	Guaranteed Cardinality	Range of Cardinality
I^2SR	k=3	105	6	17	14~21
	k=4	390	10	39	30~45
	k=5	1240	15	82	62~93
LF^2SR (LFSR)	k=3	105	14	7	5~10
	k=4	1638	120	13	8~20
	k=5	40920	1984	20	11~40
I^2LF^2SR (I^2LFSR)	k=3	735	14	52	35~70
	k=4	24570	120	204	120~300
	k=5	1268520	1984	639	341~1240

Increased thanks to dummy FF

Most secure

Conclusions

- Considered a scan-based differential-behavior attack and proposed several classes of SR-equivalent scan circuits using dummy flip-flops in order to protect the scan-based differential-behavior attack.

- Introduced differential-behavior equivalent relation, and clarified the cardinality of differential-behavior equivalent classes.

- The proposed extended scan design is very secure as well as easily testable, the normal delay or performance overhead is zero, and the area overhead can be very low.

Thank you