16th Asia and South Pacific Design Automation Conference (ASP-DAC 2011), pp.818-823, Jan. 2011.

Secure Scan Design Using Shift Register Equivalents against Differential Behavior Attack

Hideo Fujiwara[1], Katsuya Fujiwara[2] and Hideo Tamamoto[2]

[1] Graduate School of Information Science
Nara Institute of Science and Technology
Nara 630-0192, JAPAN
fujiwara@is.naist.jp

[2] Faculty of Engineering and Resource Science
Akita University
Akita, 010-8502, JAPAN
{fujiwara, tamamoto}@ie.akita-u.ac.jp

Abstract - There is a need for an efficient design-for-testability to satisfy both testability and security of digital circuits. In our previous work, we reported a secure and testable scan design approach by using extended shift registers that are functionally equivalent but not structurally equivalent to shift registers, and showed a security level by clarifying the cardinality of those classes of shift register equivalents (SR equivalents). However, SR equivalents are not always secure for scan-based side-channel attacks. In this paper, we consider a scan-based side-channel attack called differential-behavior attack and propose several classes of SR-equivalent scan circuits using dummy flip-flops in order to protect the scan-based differential-behavior attack. To show the security level of those extended scan circuits, we introduce differential-behavior equivalent relation, and clarify the number of SR-equivalent extended scan circuits, the number of differential-behavior equivalent classes and the cardinality of those equivalent classes.

I. Introduction

Scan registers or scan chains are proven to be effective in improving the testability of digital circuits [1], [2]. However, its effect on the circuit, which makes its registers easily accessible from primary inputs and outputs, allows attackers to exploit this opportunity to extract key streams, copy intellectual property (IP), and even manipulate the circuit. This makes it difficult for scan chains to be used especially in special cryptographic circuits where secret key streams are stored in internal registers. However, sacrificing testability for security will degrade/affect product quality of these circuits, which conflicts with the high demand of reliable secure systems [3]. Fundamentally, the problem lies on the inherent contradiction between testability and security for digital circuits. Hence, there's a need for an efficient solution such that both testability and security are satisfied.

To solve this challenging problem, different approaches have been proposed. In [4], [5], a scan-chain design based on scrambling was proposed, where flip-flops are dynamically reordered in a scan chain. An alternative is given in [6], [7]. In this method, a secure scan-chain architecture with mirror key register (MKR) was introduced. Any crypto chip with the proposed architecture can be switched between test/normal mode (insecure) and normal mode only (secure). A similar scheme using insecure and secure modes is the lock & key security technique proposed in [8], [9]. It uses a test security controller (TSC) to switch between secure and insecure modes. This method divides the scan chain into smaller subchains of equal length. Moreover, Paul et al. in [10] claims to provide a superior technique compared to the ones mentioned. It is a Vlm-Scan that utilizes some flip-flops in a scan chain for authentication to move to test mode. The circuit can proceed to test mode only if the proper sequence of test keys are scanned in to the used flip-flops. The test controller can be tested, which is an advantage compared to the others, however, a long test key sequence is still needed. All of the proposed techniques [4 – 12] add extra hardware outside of the scan chain. This entails several disadvantages such as high area overhead, timing overhead or performance degradation, increased complexity of testing, and limited security for the registers part among others.

Sengar et al. discussed a model called secured flipped-scan-chain in [13], which works as conventional scan chains do except that it uses inverters in the scan path to flip part of the register content for protection. There are no additional test keys or clock cycles in the method. Testing the architecture can be done the same way with scan chains, only with additional NOT gates. However, Sengar's approach [13] has not considered the possibility of resetting (to zero) of all flip-flops in the scan chain. In this case, the positions of all inverters, despite a sufficient number, can still be determined by simply scanning out after reset. Thus, the internal state can be identified and the security is breached.

In [14], we proposed a secure and testable scan design approach by using extended shift registers that are functionally equivalent but not structurally equivalent to shift registers. The proposed approach is only to replace the original scan register with a modified scan register that requires little area overhead and no performance overhead with respect to normal operation. To show the security level for the proposed approach, we clarified the cardinality of those classes of shift register equivalents (*SR-equivalents*) [15]. However, SR-equivalents are not always secure for scan-based side-channel attacks. In this paper, we consider a scan-based side-channel attack called *differential-behavior attack* and propose several classes of SR-equivalent scan circuits using dummy flip-flops in order to protect the scan-based differential-behavior attack. To show the security level of those extended scan circuits, we introduce *differential-behavior equivalent relation,* and clarify the number of SR-equivalent extended scan circuits, the number of differential-behavior equivalent classes and the cardinality of those equivalent classes for several linear structure circuits.

II. Extended Shift Registers

Figure 1 illustrates a 3-stage shift register and the state transition graph. Based from this, we define extended shift registers and shift register equivalent circuits (SR-equivalents) as follows.

Extended Shift Register. A circuit whose state transition graph is isomorphic to that of k-stage shift register is called a *k-stage extended shift register.*

Shift Register Equivalent. A circuit C is called *functionally equivalent* to a k-stage shift register (or *SR-equivalent)* if the state transition graph of C is isomorphic to that of the shift register and the input/output assignment is the same as that of the shift register. The state assignment is not necessarily the same as that of the shift register.

Figure 2(a)-(b) illustrates examples of 3-stage extended shift registers; an extended shift register which is not SR-equivalent and an extended shift register which is SR-equivalent. Underlined symbols indicate differences from the state transition graph shown in Figure 1. Here, we consider the following five types of linear circuits that can realize extended shift registers; inversion-inserted shift registers (I^2SR), linear feed-forward shift registers (LF^2SR), linear feedback shift registers (LFSR), inversion-inserted linear feed-forward shift registers (I^2 LF^2SR), and inversion-inserted linear feedback shift registers (I^2LFSR). Figure 3 shows those examples.

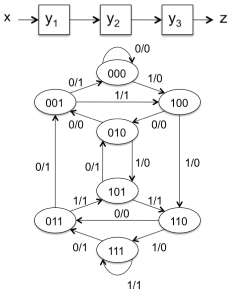
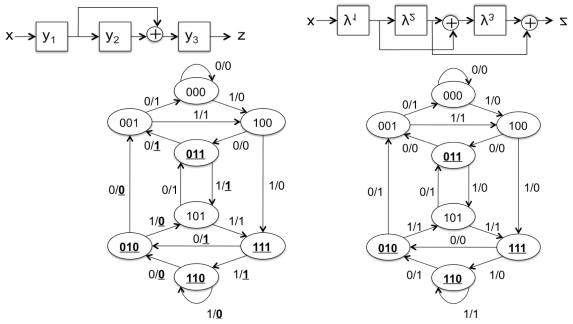
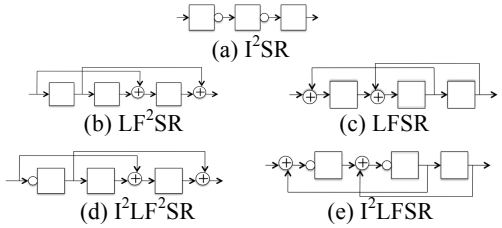


Figure 1. Shift register



(a) Not SR-equivalent (b) SR-equivalent

Figure 2. Extended shift registers



(a) I^2SR

(b) LF^2SR (c) LFSR

(d) I^2LF^2SR (e) I^2LFSR

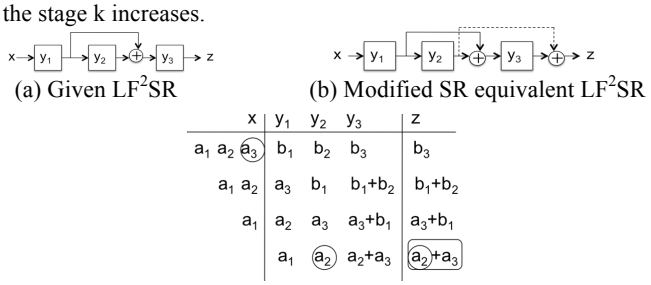
Figure 3. Five types of linear circuits

A. *How to Design SR-Equivalents*

Let us consider how to adapt the design of proposed SR-equivalents in DFT flow that generally needs to conform to some requirements and constraints. Let the constraint be the power consumption during scan operation. First, we insert NOT and feed-forward XOR gates into a scan chain to minimize power consumption during scan operation by using the method of [16]. Next, we check if the augmented scan register or extended shift register is SR-equivalent or not. If not, we augment it to SR-equivalent with minimal modification.

We have presented how to modify a given extended SR into SR-equivalent in [14], [15]. A k-stage LF^2SR given in Figure 4(a) is used as an example to demonstrate how a modification to SR equivalent is done. Here, k=3. By symbolic simulation illustrated in Figure 4(c), the output z at time k+1=4 becomes a_2+a_3 after applying an input sequence a_3 a_2 a_1 to x, where x(1)= a_3, x(2)= a_2, and x(3)= a_1. To change a_2+a_3 into a_3, we add another value a_2 to the output z, i.e., $a_2+a_3+a_2= a_3$. To do so, we modify the circuit by adding a feed-forward from y_2 to z as shown in Figure 4(b). Then the modified circuit becomes SR-equivalent. In this way, for a k-stage LF^2SR, the additional feed-forward line is uniquely determined from the output expression at time k+1 obtained by symbolic simulation.

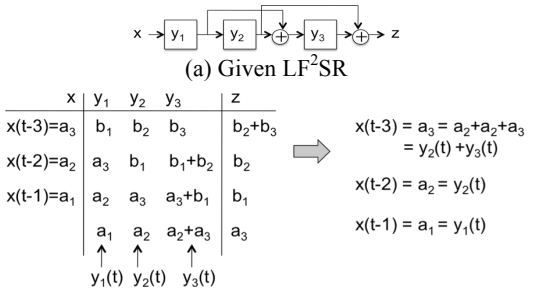
Symbolic simulation is very fast, and hence it is not so hard to construct a long stage of SR-equivalent by modification shown in Figure 4. However, the additional hardware might increase as the stage k increases.



(a) Given LF^2SR (b) Modified SR equivalent LF^2SR

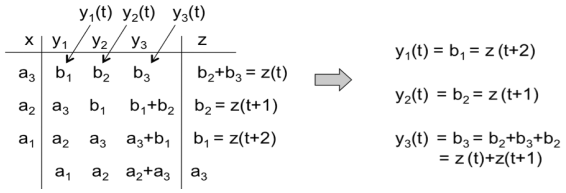
(c) Symbolic simulation

Figure 4. Modification to SR-equivalent



(a) Given LF^2SR

(b) Obtain state-justification sequence from final state



(c) Determine initial state from output sequence

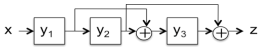
Figure 5. State-justification and state-observation

B. *How to Control/Observe SR-Equivalents*

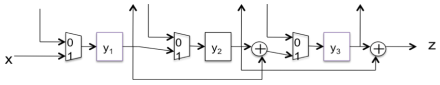
For a synthesized SR-equivalent circuit, the following two problems are important in order to utilize the SR-equivalent circuit as a scan shift register in testing. One problem is to generate an input sequence to transfer the circuit into a given desired state. This is called *state-justification problem.* The other problem is to determine the initial state by observing the output sequence from the state. This is called *state-observation problem*. In [14], we showed that for any SR-equivalent circuit, those problems can be solved uniquely similar to SR. That is, for any desired state, a transfer sequence to the state can be uniquely generated, independently of the initial state, and any present state (initial state) can be uniquely identified only from the output sequence.

Consider a 3-stage LF^2SR given in Figure 5(a). This LF^2SR is SR-equivalent. By using symbolic simulation, we can obtain an input sequence (x(t-3), x(t-2), x(t-1)) that transfers the circuit from any state to the desired final state (y_1(t), y_2 (t), y_3 (t)) as illustrated in Figure 5(b). Similarly, as illustrated in Figure 5(c), we can determine the initial state (y_1(t), y_2 (t), y_3 (t)) from the output sequence (z(t), z(t+1), z(t+2)). For other type of

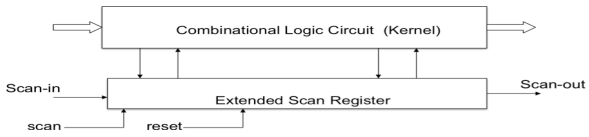
SR-equivalent structures, we can obtain those equations similarly and easily from symbolic simulation.



(a) Extended shift register R_1



(b) Extended scan register S_1



(c) Kernel with extended scan register

Figure 6. Scan design with extended scan register

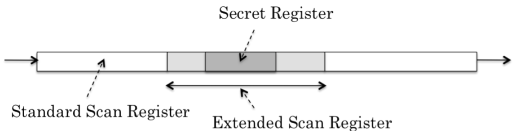


Figure 7. Long secure scan chain

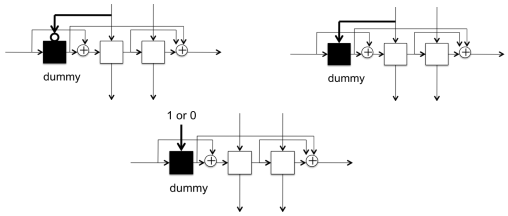


Figure 8. Extended scan circuits with dummy FF

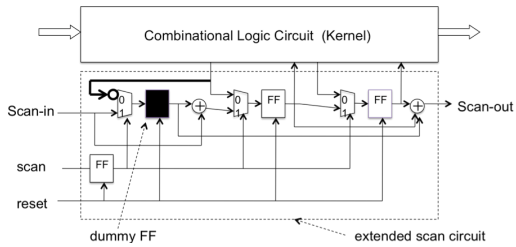


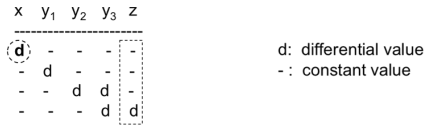
Figure 9. Scan design with extended scan circuit

III. Extended Scan Circuits

A scan-designed circuit consists of a single or multiple scan registers or scan chains and the remaining combinational logic circuit (*kernel*). A scan register is regarded as a shift register with multiplexers that select the normal data from the combinational logic circuit and the shifting data from the preceding flip-flop. Here, we replace the shift register with an *extended shift register*. The scan register with the extended shift register as shown in Figure 6 is called the *extended scan register (ESR)*.

In the proposed *secure scan design*, not all scan registers are replaced with ESRs. As shown in Figure 7, only the scan registers necessary to be secure are replaced with ESRs that cover the secrete registers and the size of ESRs is large enough to make them secure. So, the area overhead can be low. The delay overhead due to additional XOR gates influences only scan operation, and hence there is no delay overhead for normal operation.

In the following section, we consider a *differential behavior attack* as a scan-based side-channel attack. To protect the attack, we introduce a *dummy* flip-flop as shown in Figure 8. A circuit consisting of an extended shift register and a dummy FF is called an *extended scan circuit*. Figure 8 illustrates three extended scan circuits with three types of dummy flip-flops. Figure 9 shows scan design with the extended scan circuit.



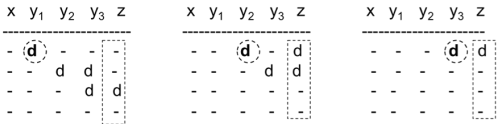


Figure 10. Fundamental d-behaviors for S_1

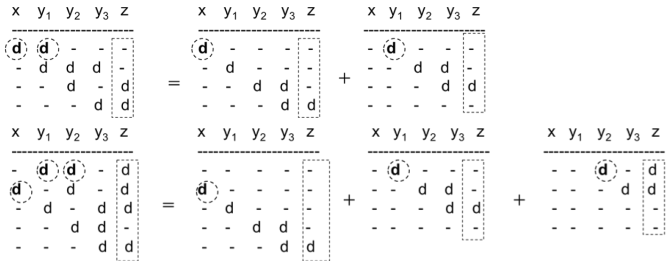


Figure 11. XOR-superposition of fundamental d-behaviors

IV. Differential Behavior

Let us consider the following scan-based attack. 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. By applying such two input sequences that are slightly different from each other, the contents of scan registers have a single bit or multiple bit difference between two input sequences, i.e., one can insert different values (referred to *differential value*) into a single or multiple flip-flops between two input sequences (or a pair of input sequences) and observe the differences between the pair of output sequences by scan operation. Such a pair of two scan-out sequences including differential values is called *a differential behavior* (or *d-behavior,* for short). Figure 10 shows four d-behaviors for the extended scan register S_1 of Figure 6 (b). A single differential value is inserted into x, y_1, y_2, y_3, and y_4, respectively.

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.* For the differential-behavior attack, we consider the possibility of the worst case such that arbitrary number of differential values can be inserted into any flip-flops except dummy flip-flops though the inserted positions are unknown, and that differential values can also be inserted simultaneously from scan-input at any time again and again.

Differential-behavior set. A set of all d-behaviors for an extended scan circuit S is called the *differential-behavior set* of S (or *d-behavior set* of S, for short). A set of all *single-bit* d-behaviors for S is called the *fundamental differential-behavior set* of S (or *fundamental d-behavior set* of S, for short). Figure 10 shows the fundamental d-behavior set of S_1 of Figure 6 (b).

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.

XOR operation of differential value (d) and constant (-) is as follows. (d)+(d)=(-), (d)+(-)=(d), (-)+(-)=(-). Then, the following theorem holds.

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

Figure 11 illustrates two examples of Theorem 1. From Theorem 1, we see that two extended scan circuits can be identified to be d-behavior equivalent or not, only by checking their fundamental behavior sets are the same.

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.

V. Identification of Scan Structure

The extended shift register R_1 of Figure 6(a) is SR-equivalent. The total number of SR-equivalent circuits with 3 flip-flops is $N(3)=2^3!/3! - 1 = 6{,}719$. Since they are all functionally equivalent to the 3-stage shift register, their input/output relations are the same for all of them. Therefore, the probability that an attacker can identify it to be R_1 by guessing is 1/6719. The number of 3-stage SR-equivalent LF^{2}SR-type circuits is $2^{k(k-1)/2}-1 = 7$, and hence the guessing probability is one seventh. However, the guessing probability approaches to zero as the number of flip-flops increases. In the above discussion, we considered only attacks via scan operation for extended scan registers. However, if we target extended scan circuits, we need to consider differential-behavior attacks.

Suppose the extended scan register R_1 and the scan circuit S_1 in Figure 6. S_1 consists of R_1. The fundamental d-behavior set of S1 is shown in Figure 10. As explained later in Section VI.B, every class of differential behavior equivalents for LF^{2}SR-type extended scan circuits consists of one element or singleton, i.e., the cardinality of every d-behavior equivalent class is 1. Hence, we can see any extended scan circuit that has the same fundamental d-behavior set as that of S_1 is only S_1 itself. Therefore, we can uniquely identify S_1 from the d-behavior set, and hence the structure of S_1 is identified and S_1 is not secure.

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, for each type of extended scan circuits we clarify the total number of SR-equivalent extended scan circuits in the class, the number of d-equivalent classes, and the cardinality of those equivalent classes in the following sections.

VI. Cardinality of Differential Behavior Equivalents

From Theorem 2, we see that two extended scan circuits can be identified to be d-behavior equivalent or not, only by checking their fundamental behavior sets are the same. Therefore, we consider only fundamental behaviors from now on.

A. *I^{2}SR without Dummy FF*

Consider an SR-equivalent k-stage I^{2}SR-type scan circuit without dummy FF. If a differential value is inserted into the j-th FF y_j, the d-behavior becomes (- , …. , - , d , - , … , -) of length k+1. Therefore, the following k+1 d-behaviors are obtained.

(- , … , - , d), (-, … , - , d, -), … , (d , - , … , -)

Therefore, the total number of SR-equivalent k-stage I^{2}SR-type scan circuits is $2^k - 1$.

They are all d-behavior equivalent each other. Hence, the number of d-behavior equivalent classes is 1. The cardinality of the unique equivalent class is $2^k - 1$.

B. *LF^{2}SR and LFSR without Dummy FF*

Consider an SR-equivalent k-stage LF^{2}SR-type scan circuit without dummy FF. If a differential value is inserted into the j-th FF y_j, the d-behavior becomes (z_1 , z_2, ... , z_{k-1} , d , - , … , -) of length k+1 where z_1 , z_2, ... , z_{k-1} are either (-) or (d). The number of total such different patterns are 2^{k-j}.

Since a differential value can be inserted in y_1 , y_2, ... , and y_k , the number of different d-behavior sets (the number of equivalent classes) including SR becomes

$$\prod_{j=1}^{k} 2^{k-j} = \prod_{i=1}^{k-1} 2^{i} = 2^{\frac{k(k-1)}{2}}$$

The total number of SR-equivalent k-stage LF^{2}SR-type scan circuits including SR is $2^{k(k-1)/2} - 1$. Hence, the cardinality of every equivalent class is 1, i.e., singleton.

As for SR-equivalent k-stage LFSR-type scan circuits, we can obtain similarly, i.e., the number of extended scan circuits, the number of d-behavior equivalent classes, and the cardinality of those equivalent classes are the same as those of LF^{2}SR-type scan circuits.

C. *I^{2}LF^{2}SR and I^{2}LFSR without Dummy FF*

Consider an SR-equivalent k-stage I^{2}LF^{2}SR-type scan circuit without dummy FF. By considering the superposition of I^{2}SR and LF^{2}SR, the total number of SR-equivalent k-stage I^{2}LF^{2}SR-type scan circuits is

$$\left(2^{\frac{k(k-1)}{2}} - 1\right)\left(2^k - 1\right)$$

The total number of d-equivalent classes is $2^{k(k-1)/2} - 1$. Hence, there exists an equivalent class whose cardinality is at least $2^k - 1$.

As for SR-equivalent k-stage I^{2}LFSR-type scan circuits without dummy FF, we can obtain similarly, i.e., the number of extended scan circuits, the number of d-behavior equivalent classes, and the cardinality of those equivalent classes are the same as those of I^{2}LF^{2}SR-type scan circuits without dummy FF.

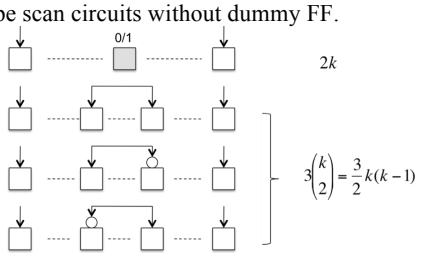


Figure 12. Total number of patterns with one dummy FF

D. *I^{2}SR with One Dummy FF*

Consider SR-equivalent k-stage I^{2}SR-type scan circuits with one dummy FF. The total number of SR-equivalent k-stage I^{2}SRs is $2^k - 1$.

For each SR-equivalent k-stage I^{2}SR, there exist the following number of different patterns of placing one dummy FF as shown in Figure 12. In the case that a constant 0 or 1 is connected to the normal input of one dummy FF, there are 2k cases. In the case that a normal input of other FF is connected to the normal input of one dummy FF, there are 3k(k-1)/2 cases. Therefore, the total number of SR-equivalent k-stage I^{2}SR-type scan circuits with one dummy FF is

$$\left(2k + \frac{3}{2}k(k-1)\right)\left(2^k - 1\right) = \left(\frac{3k^2 + k}{2}\right)\left(2^k - 1\right)$$

Inserting a differential value becomes either inserting a

differential value into a FF or inserting two differential values into two FFs. Therefore, the total number of d-equivalent classes is

$$\binom{k}{1}+\binom{k}{2}=k+\frac{k(k-1)}{2}=\frac{k(k+1)}{2}$$

Hence, there exists an equivalent class whose cardinality is at least

$$\left\lfloor \frac{\left(\frac{3k^2+k}{2}\right)\left(2^k-1\right)}{\frac{k(k+1)}{2}} \right\rfloor = \frac{3k+1}{k+1}\left(2^k-1\right) \approx 3\left(2^k-1\right)$$

E. LF²SR and LFSR with One Dummy FF

Consider SR-equivalent k-stage LF²SR-type scan circuits with one dummy FF. The total number of SR-equivalent k-stage LF²SRs is $2^{k(k-1)/2}-1$.

For each SR-equivalent k-stage I²SR, there exist the following number of different patterns of placing one dummy FF as shown in Figure 12. In the case that a constant 0 or 1 is connected to the normal input of one dummy FF, there are 2k cases. In the case that a normal input of other FF is connected to the normal input of one dummy FF, there are 3k(k-1)/2 cases. Therefore, the total number of SR-equivalent k-stage LF²SR-type scan circuits with one dummy FF is

$$\left(2k+\frac{3}{2}k(k-1)\right)\left(2^{\frac{k(k-1)}{2}}-1\right)=\left(\frac{3k^2+k}{2}\right)\left(2^{\frac{k(k-1)}{2}}-1\right)$$

Similar to the discussion of Section VI.*D*, inserting a differential value becomes either inserting a differential value into a FF or inserting two differential values into two FFs. Therefore, the total number of d-equivalent classes is

$$\frac{\prod_{j=1}^{k}2^{k-j}}{2^{k-1}}+\frac{\prod_{j=1}^{k}2^{k-j}}{2^{k-2}}+\ldots+\frac{\prod_{j=1}^{k}2^{k-j}}{2^{0}}=2^{\frac{k^2-3k+2}{2}}\left(2^k-1\right)$$

On the other hand, the number of scan circuits is

$$\left(\frac{3k^2+k}{2}\right)\left(2^{\frac{k(k-1)}{2}}-1\right)$$

Therefore, there exists an equivalent class whose cardinality is at least

$$\left\lfloor \frac{\left(\frac{3k^2+k}{2}\right)\left(2^{\frac{k(k-1)}{2}}-1\right)}{2^{\frac{k^2-3k+2}{2}}\left(2^k-1\right)} \right\rfloor \approx O(k^2)$$

F. I²LF²SR and I²LFSR with One Dummy FF

Consider an SR-equivalent k-stage I²LF²SR-type scan circuit with one dummy FF. By considering the superposition of I²SR and LF²SR, the total number of SR-equivalent k-stage I²LF²SR-type scan circuits is

$$\left(\frac{3k^2+k}{2}\right)\left(2^{\frac{k(k-1)}{2}}-1\right)\left(2^k-1\right)$$

The total number of d-equivalent classes is

$$2^{\frac{k^2-3k+2}{2}}\left(2^k-1\right)$$

Therefore, there exists an equivalent class whose cardinality is at least

$$\left\lfloor \frac{\left(\frac{3k^2+k}{2}\right)\left(2^{\frac{k(k-1)}{2}}-1\right)}{2^{\frac{k^2-3k+2}{2}}} \right\rfloor \approx O(k^2 2^k)$$

As for SR-equivalent k-stage I²LFSR-type scan circuits with one dummy FF, we can obtain similarly, i.e., the number of extended scan circuits, the number of d-behavior equivalent classes, and the cardinality of those equivalent classes are the same as those of I²LF²SR-type scan circuits with one dummy FF.

Table I. Cardinality of d-behavior equivalent classes (without dummy FF)

	# of SR-Equivalent Scan Circuits	# of Equivalent Classes	Guaranteed Cardinality
I²SR	2^k-1	1	2^k-1
LF²SR (LFSR)	$2^{k(k-1)/2}-1$	$2^{k(k-1)/2}-1$	1
I²LF²SR (I²LFSR)	$(2^{k(k-1)/2}-1)(2^k-1)$	$2^{k(k-1)/2}-1$	2^k-1

Table II. Cardinality of d-behavior equivalent classes (with one dummy FF)

	# of SR-Equivalent Scan Circuits	# of Equivalent Classes	Guaranteed Cardinality
I²SR	$(3k^2+k)(2^k-1)/2$	k(k+1)/2	$3(2^k-1)$
LF²SR (LFSR)	$(3k^2+k)(2^{k(k-1)/2}-1)/2$	$(2^{(k-1)(k-2)/2})(2^k-1)$	$O(k^2)$
I²LF²SR (I²LFSR)	$(3k^2+k)(2^{k(k-1)/2}-1)(2^k-1)/2$	$(2^{(k-1)(k-2)/2})(2^k-1)$	$O(k^2 2^k)$

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

	# FFs	# of Scan Circuits	# of Equivalent Classes	Guaranteed Cardinality	Range of Cardinality
I²SR	k=3 k=4 k=5	7 15 31	1 1 1	7 15 31	7~7 15~15 31~31
LF²SR (LFSR)	k=3 k=4 k=5	7 63 1023	7 63 1023	1 1 1	1~1 1~1 1~1
I²LF²SR (I²LFSR)	k=3 k=4 k=5	49 945 31713	7 63 1023	7 15 31	7~7 15~15 31~31

Table IV. Cardinality of d-behavior equivalent classes (with one dummy FF) by SREEP-2

	# FFs	# of Scan Circuits	# of Equivalent Classes	Guaranteed Cardinality	Range of Cardinality
I²SR	k=3 k=4 k=5	105 390 1240	6 10 15	17 39 82	14~21 30~45 62~93
LF²SR (LFSR)	k=3 k=4 k=5	105 1638 40920	14 120 1984	7 13 20	5~10 8~20 11~40
I²LF²SR (I²LFSR)	k=3 k=4 k=5	735 24570 1268520	14 120 1984	52 204 639	35~70 120~300 341~1240

VI. Enumeration Results by SREEP-2

In the previous sections, for each type of extended scan circuits with/without dummy FF, we have clarified the total number of SR-equivalent extended scan circuits in the class, the number of d-equivalent classes, and the cardinality of those equivalent classes. Regarding the cardinality of d-equivalent classes, we showed the existence of an equivalent class whose cardinality is at least of the size. Table I and II show the summary. From Table I, two classes of LF²SR and LFSR are not secure because their guaranteed cardinality is 1. However, all other classes in Table I and Table II

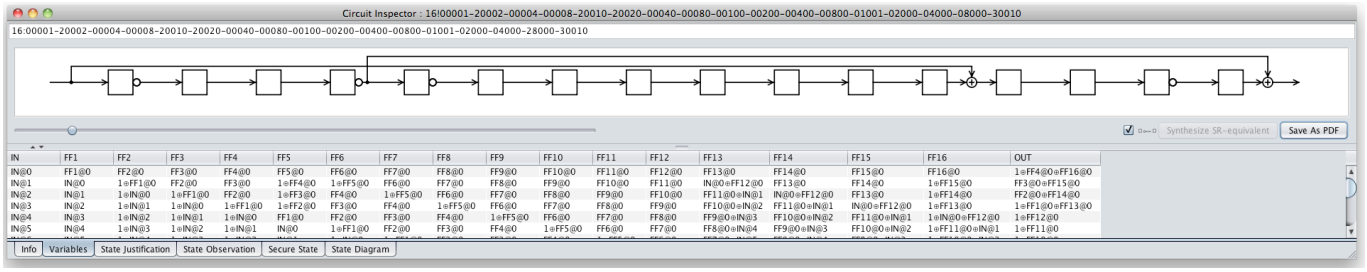


Figure 13. Outcome of SR-equivalent extended scan register by SREEP-2

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

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 Table III and Table IV, respectively. The third column shows the number of SR-equivalent scan circuits in each class of extended scan circuits. The fourth column shows the number of d-equivalent classes. The fifth column shows the guaranteed cardinality, i.e., there exists an equivalent class whose cardinality is at least the guaranteed one. The sixth column shows the range of cardinality, i.e., the minimal cardinality to the maximal cardinality.

As for the number of SR-equivalent scan circuits and the number of d-equivalent classes, theoretical values computed from the expressions in Section VI coincide with the actual values obtained from SREEP-2. As for the guaranteed cardinalities, they are all exactly within the range of cardinality. Hence, it is indeed guaranteed that there exist equivalent classes whose cardinality is larger than the guaranteed cardinality.

Next, let us consider the overhead of SR-equivalent scan circuits. The performance or delay overhead for normal operation is zero. The delay overhead due to extra XOR gates influences only scan operation. Regarding the area overhead, as mentioned in Section III, not all scan registers are replaced with extended scan registers but only the registers necessary to be secure are replaced with extended scan registers, as shown in Figure 7. So, the area overhead of whole scan circuits is expected to be low. Further, the area overhead of each extended scan register can be very low. Figure 13 shows an example of the outcome of an SR-equivalent 16-stage I^2LF^2SR-type extended scan register without dummy FF obtained by SREEP-2 under the constraint of at most two XOR gates. Hence, the area overhead is very low.

VII. Conclusions

In this paper, we 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. In order to show the security level of those extended scan circuits, we introduced differential-behavior equivalent relation, and clarified the number of SR-equivalent extended scan circuits, the number of differential-behavior equivalent classes and the cardinality of those equivalent classes. It is shown that 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.

Acknowledgements

This work was supported in part by Japan Society for the Promotion of Science (JSPS) under Grants-in-Aid for Scientific Research (B) (No. 20300018).

References

[1] H. Fujiwara, Y. Nagao, T. Sasao, and K. Kinoshita, "Easily testable sequential machines with extra inputs," *IEEE Trans. on Computers,* Vol. C-24, No. 8, pp. 821-826, Aug. 1975.

[2] H. Fujiwara, *Logic Testing and Design for Testability*, *The MIT Press* 1985.

[3] K. Hafner, H. Ritter, T. Schwair, S. Wallstab, M. Deppermann, J. Gessner, S. Koesters, W. Moeller, and G. Sandweg, "Design and test of an integrated cryptochip," *IEEE Design and Test of Computers*, pp. 6-17, Dec. 1999.

[4] D. Hely, M.-L. Flottes, F. Bancel, B. Rouzeyre, and N. Berard. "Scan design and secure chip." *10th IEEE International On-Line Testing Symposium,* pp. 219–224, 2004.

[5] D. Hely, F. Bancel, M.L. Flottes, and B. Rouzeyre. "Securing scan control in crypto chips." *Journal of Electronic Testing - Theory and Applications*, Vol. 23, No. 5, pp. 457–464, Oct. 2007.

[6] B. Yang, K. Wu, and R. Karri. "Scan based side channel attack on dedicated hardware implementations of data encryptionstandard." *International Test Conference 2004*, pp. 339–344, 2004.

[7] B. Yang, K. Wu, and R. Karri. "Secure scan: A design-for-test architecture for crypto chips." *IEEE Trans. on Computer-Aided Design of Integrated Circuits and Systems*, Vol. 25, No.10, pp. 2287–2293, Oct. 2006.

[8] J. Lee, M. Tehranipoor, and J. Plusquellic, "A low-cost solution for protecting IPs against scan-based side-channel attacks," *24th IEEE VLSI Test Symposium,* pp. 94 - 99, 2006.

[9] J. Lee, M. Tehranipoor, C. Patel, and J. Plusquellic. "Securing designs against scan-based side-channel attacks." *IEEE Trans. on Dependable and Secure Computing*, Vol. 4, No. 4, pp. 325–336, Oct.-Dec. 2007.

[10] S. Paul, R. S. Chakraborty, and S. Bhunia. "VIm-Scan: A low overhead scan design approach for protection of secret key inscan-based secure chips." *25th IEEE VLSI Test Symposium*, pp. 455–460, 2007.

[11] M. Inoue, T. Yoneda, M. Hasegawa, and H. Fujiwara, "Partial scan approach for secret information protection," *14th IEEE European Test Symposium*, pp. 143-148, May 2009.

[12] U. Chandran and D. Zhao, "SS-KTC: A high-testability low-overhead scan architecture with multi-level security integration," *27th IEEE VLSI Test Symposium,* pp. 321-326, May 2009.

[13] G. Sengar, D. Mukhopadhyay, and D. R. Chowdhury. "Secured flipped scan-chain model for crypto-architecture." *IEEE Trans. on Computer-Aided Design of Integrated Circuits and Systems*, Vo. 26, No.11, pp. 2080-2084, November 2007.

[14] H. Fujiwara and M.E.J. Obien, "Secure and testable scan design using extended de Brujin graph," *15th Asia and South Pacific Design Automation Conference*, pp. 413-418, Jan. 2010.

[15] K. Fujiwara, H. Fujiwara, M.E.J. Obien, and H. Tamamoto, "SREEP: Shift register equivalents enumeration and synthesis program for secure scan design," *13th IEEE International Symposium on Design and Diagnosis of Electronic Circuits and Systems,* pp.193-196, April 2010.

[16] O. Sinanoglu and A. Orailoglu, "Modeling scan chain modifications for scan-in test power minimization," *International Test Conference 2003*, pp. 602-611, 2003.

[17] SREEP: http://sreep.fujiwaralab.net/.