PAPER

Differential Behavior Equivalent Classes of Shift Register Equivalents for Secure and Testable Scan Design

Katsuya FUJIWARA[†a)], *Member*, **Hideo FUJIWARA**[††], *Fellow*, *and* **Hideo TAMAMOTO**[†], *Member*

SUMMARY It is important to find an efficient design-for-testability methodology that satisfies both security and testability, although there exists an inherent contradiction between security and testability for 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 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 SR-equivalent scan circuits, we introduce a differential-behavior equivalent relation and clarify the number of SR-equivalent scan circuits, the number of differential-behavior equivalent classes and the cardinality of those equivalent classes.

key words: *design-for-testability, scan design, shift register equivalents, security, scan-based side-channel attack*

1. Introduction

Scan registers or scan chains are proven to be effective in improving the testability of digital circuits [1], [2]. However, their 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 for reliable secure systems [3]. Fundamentally, the problem lies in 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. 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. To resolve such a reset-based attack, Agrawal et al. [14] introduced an XOR-scan-chain architecture for secure scan design. However, the XOR-scan-chain is required to be reset before feeding in a test pattern, and hence the test response in the scan chain must be scanned out before feeding in the next test pattern, i.e., scanning in a test pattern and scanning out a test response cannot be performed simultaneously, which doubles the test application time compared to the standard scan testing.

In [16], [18], 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 extended shift registers include flipped-scan chain of [13] and XOR-scan chain of [14] as special cases. Further, our secure scan architecture can protect reset-based attack by adding one extra flip-flop [16], [18], and hence thanks to this extra flip-flop and

Manuscript received September 17, 2010.
Manuscript revised March 2, 2011.

[†]The authors are with the Graduate School of Engineering and Resource Science, Akita University, Akita-shi, 010–8502 Japan.
[††]The author is with the Graduate School of Information Science, Nara Institute of Science and Technology, Ikoma-shi, 630–0192 Japan.
a) E-mail: fujiwara@ie.akita-u.ac.jp

DOI: 10.1587/transinf.E94.D.1430

the shift-register equivalence of modified scan chains, scanning in a test pattern and scanning out a test response can be performed simultaneously, in the same way as the standard scan testing. 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. As for the security, the objective application is mainly to use it for cryptographic circuits though it can be used for IP protection and other purposes. To show the security level for the proposed approach, we clarified the cardinality of those classes of shift register equivalents (*SR-equivalents*) [17], [18]. However, SR-equivalents are not always secure for scan-based side-channel attacks like differential behavior attack of [6].

In this paper, we consider a scan-based side-channel attack called *differential-behavior attack* which is an extension of the differential-behavior attack of [6], 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 SR-equivalent scan circuits, we introduce *differential-behavior equivalent relation*, and clarify the number of SR-equivalent scan circuits, the number of differential-behavior equivalent classes and the cardinality of those equivalent classes for several linear structure circuits.

2. SR-Equivalent Circuits

Consider a k-stage shift register shown in Fig. 1. For the k-stage shift register, the input value applied to x appears at z after k clock cycles. Suppose a circuit C with a single input x, a single output z, and k flip-flops as shown in Fig. 2. If the input value applied to x of C appears at the output z of C after k clock cycles, the circuit C behaves as if it is a k-stage shift register.

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.

Figure 3 illustrates an example of 3-stage SR-equivalent circuit R_1. The table in Fig. 3 can be obtained easily by symbolic simulation. As shown in the table, $z(3) = x(0)$, i.e., the input value applied to x appears at z after $k = 3$ clock cycles, and hence the circuit is SR-equivalent. Although the input/output behavior of R_1 is the same as that of the 3-stage shift register, the internal state behavior of R_1 is different from the shift register. For the shift register SR, the input sequence $(x(0), x(1), x(2))$ which transfers SR to the state $(y_1(2), y_2(2), y_3(2))$ is $(x(0), x(1), x(2)) = (y_3(2), y_2(2), y_1(2))$. The initial state $(y_1(0), y_2(0), y_3(0))$ can be identified as $(y_1(0), y_2(0), y_3(0)) = (z(2), z(1), z(0))$ from the output sequence $(z(0), z(1), z(2))$. However, for the SR-equivalent circuit R_1, the input sequence which transfers R_1 to the state $(y_1(2), y_2(2), y_3(2))$ is $(x(0), x(1), x(2)) = (y_3(2) \oplus y_2(2), y_2(2), y_1(2))$ from Fig. 3, and the initial state $(y_1(0), y_2(0), y_3(0))$ can be identified as $(y_1(0), y_2(0), y_3(0)) = (z(2), z(1), z(0) \oplus z(1))$ from the output sequence. Therefore, without the information on the structure of R_1 one cannot control/observe the internal state of R_1. From this observation, replacing the shift register with an SR-equivalent circuit makes the scan circuit *secure*.

The SR-equivalent circuit shown in Fig. 3 is a linear feed-forward shift register. SR-equivalent circuits can also be realized by a linear feedback shift register and/or by inserting inverters as shown in Fig. 4. SR-equivalent circuits can be realized not only by linear feed-forward/feedback shift registers with/without inverters but also by more gen-

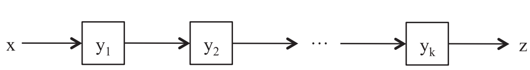


Fig. 1 k-stage shift register SR.

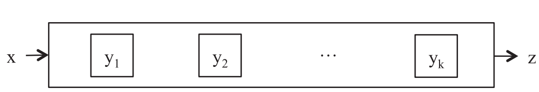
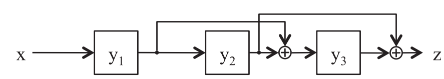


Fig. 2 k-stage SR-equivalent circuit C.

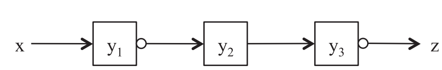


(a) SR-equivalent circuit R_1

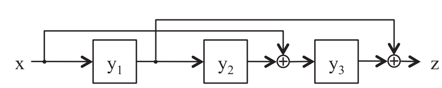
x	y_1	y_2	y_3	z
$x(0)$	$y_1(0)$	$y_2(0)$	$y_3(0)$	$z(0) = y_2(0) \oplus y_3(0)$
$x(1)$	$x(0)$	$y_1(0)$	$y_1(0) \oplus y_2(0)$	$z(1) = y_2(0)$
$x(2)$	$x(1)$	$x(0)$	$x(0) \oplus y_1(0)$	$z(2) = y_1(0)$
	$x(2)$	$x(1)$	$x(1) \oplus x(0)$	$z(3) = x(0)$

(b) Behavior of R_1 by symbolic simulation

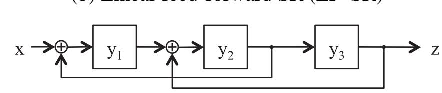
Fig. 3 Example of SR-equivalent circuit.



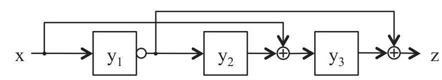
(a) Inversion-inserted SR (I^2SR)



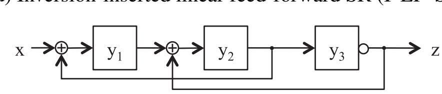
(b) Linear feed-forward SR (LF^2SR)



(c) Linear feedback SR (LFSR)

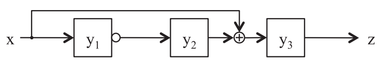


(d) Inversion-inserted linear feed-forward SR (I^2LF^2SR)

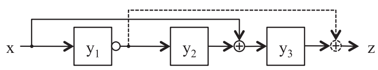


(e) Inversion-inserted linear feedback SR (I^2LFSR)

Fig. 4 Five types of linear circuits.



(a) Given I^2LF^2SR

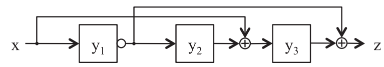


(b) Modified SR-equivalent I^2LF^2SR

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

(c) Symbolic simulation

Fig. 5 Modification to SR-equivalent I^2LF^2SR.



(a) SR-equivalent I^2LF^2SR, R_2

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

$\Downarrow$

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

(b) Equations for state-justification

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

$\Downarrow$

$y_1(t-3) = z(t-1)$
$y_2(t-3) = 1\oplus z(t-2)$
$y_3(t-3) = 1\oplus z(t-3)\oplus z(t-1)$

(c) Equations for state-observation

Fig. 6 State-justification and state-observation for R_2.

eral circuits.

2.1 How to Design SR-Equivalent Circuits

For the class of I^2SRs, any k-stage I^2SR with even number of inverters is SR-equivalent. For the classes of LF^2SR and I^2LF^2SR, any k-stage LF^2SR and I^2LF^2SR can be modified to be SR-equivalent by manipulating the linear sum of the output. For the classes of LFSR and I^2LFSR, any k-stage LFSR and I^2LFSR can be modified to be SR-equivalent by manipulating the linear sum of the input.

To illustrate an example, consider a k-stage I^2LF^2SR given in Fig. 5 (a). Here, $k = 3$. By symbolic simulation illustrated in Fig. 5 (c), the output $z(3)$ becomes $x(2)\oplus 1\oplus x(0)$. To change $x(2)\oplus 1\oplus x(0)$ into $x(0)$, we add extra value $x(2)\oplus 1$ to the output z, i.e., $x(2)\oplus 1\oplus x(0)\oplus x(2)\oplus 1 = x(0)$. To do so, we modify the circuit by adding extra feed-forward from y_1 with inverter to z as shown in Fig. 5 (b). Then, the modified circuit becomes SR-equivalent.

2.2 How to Control/Observe SR-Equivalents

For a synthesized SR-equivalent circuits, 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*.

Consider a 3-stage I^2LF^2SR, R_2, given in Fig. 6 (a). This I^2LF^2SR is SR-equivalent. Figure 6 illustrates how to solve state-justification and state-observation problem. By using symbolic simulation, we can derive equations to obtain an input sequence $(x(t-3), x(t-2), x(t-1))$ that transfers R_2 from any state to the desired final state $(y_1(t), y_2(t), y_3(t))$ as illustrated in Fig. 6 (b). Similarly, as illustrated in Fig. 6 (c), we can derive equations to determine uniquely the initial state $(y_1(t-3), y_2(t-3), y_3(t-3))$ from the output sequence $(z(t-3), z(t-2), z(t-1))$.

3. SR-Equivalent Scan Circuits

A scan-designed circuit consists of a single or multiple scan chains and the remaining combinational logic circuit (*kernel*) as illustrated in Fig. 7. A scan chain is regarded as a circuit consisting of 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 SR-equivalent register. The modified scan register is called the *SR-equivalent scan register*. For example, SR-equivalent scan register S_1 is obtained from SR-equivalent register R_1 as shown in Fig. 8.

In the proposed *secure scan design*, to reduce the area overhead as much as possible, not all scan chains are replaced with modified scan registers. As shown in Fig. 9, only parts of scan chains necessary to be secure are replaced with modified SR-equivalent scan chains that cover secret registers to be protected, and the size of the modified scan chains is large enough to make it secure. Regarding the performance overhead, the delay overhead due to additional

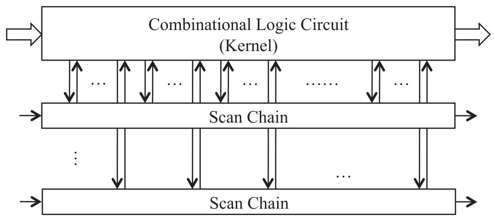
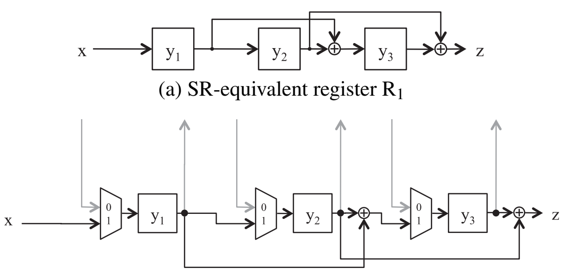


Fig. 7 Scan-designed circuit.



(a) SR-equivalent register R_1

(b) SR-equivalent scan register S_1

Fig. 8 Modified scan register. (SR-equivalent)

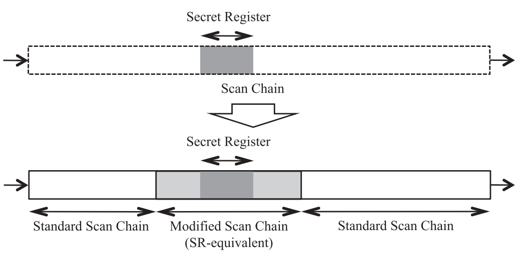


Fig. 9 Replacement of scan chain by modified scan chain.

XOR gates influences only scan operation, and hence there is no delay overhead for normal operation.

We have considered a scan-designed circuit consists of multiple scan chains as shown in Fig. 7. However, we may consider a scan-designed circuit with stimulus decomposition circuit and test response compactor. Even for such scan-designed circuits, SR-equivalent scan circuits can be applied to make the circuits more secure. Suppose a circuit under test that includes two registers A and B such that A can be easily controlled by primary inputs during normal operation and B can be easily observed by primary output during normal operation. Then, part of scan chain between A and B can be scanned in thru A from primary inputs and can be scanned out thru B to primary outputs by using normal and scan operations, even if the scan-designed circuit has scan stimulus decompression circuit and test response compactor. Hence, the circuit under test is not secure. However, if we replace the scan chain between A and B by an SR-equivalent scan chain, then this part of scan chain becomes secure independently of other part, i.e., even if the circuit under test has stimulus decompression circuit and test response compactor.

There have been reported several scan-based attacks such as reset-based attack [14], differential behavior attack [6] and discriminator-based attack [15]. In our previous work [16], [18], we showed that our secure scan architecture protects the reset-based attack of [14] by adding one extra flip-flop to prohibit scan-after-reset (see Fig. 11). The set of differential behaviors used in the differential behavior attack of [6] is a subset of the differential-behavior set defined in the following section. Hence, if it is secure for the differential-behavior attack defined in this paper, it is also secure for the differential behavior attack of [6]. In our proposed secure scan architecture, the scanned-out data from a scan register is not the same as the content of the scan register. Therefore, the attacker cannot obtain the content of the scan register and hence the existing scan-based attacks [6], [14], [15] that depend on calculation from scanned data will fail, unless the attacker can identify the configuration of the extended scan register.

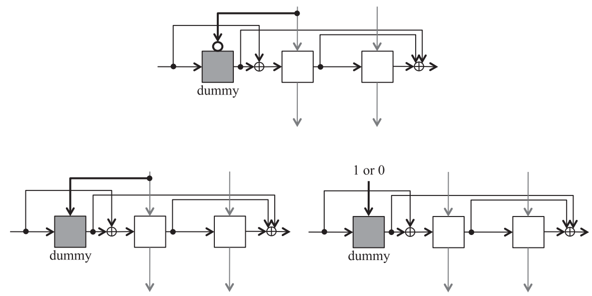


Fig. 10 SR-equivalent scan circuits with dummy FF.

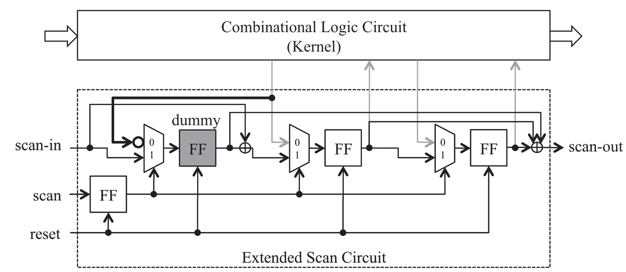


Fig. 11 Scan design with SR-equivalent scan circuit.

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 Fig. 10. A dummy flip-flop is an extra flip-flop which is inserted in a scan chain but is not used in the original circuit. A circuit consisting of an SR-equivalent scan register and a dummy FF is called an *SR-equivalent scan circuit*. Figure 10 illustrates three SR-equivalent scan circuits with three types of dummy flip-flops. Figure 11 shows scan design with the SR-equivalent scan circuit.

4. 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 se-

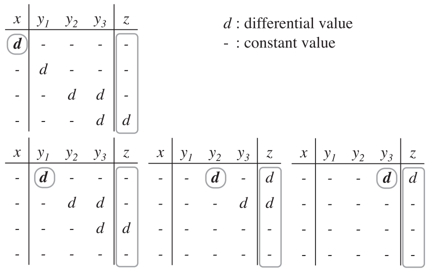


Fig. 12 Fundamental d-behaviors for S_1.

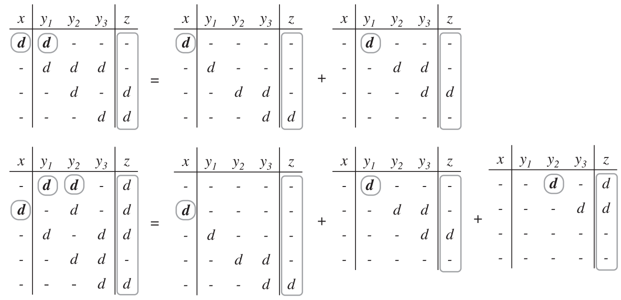


Fig. 13 XOR-superposition of fundamental d-behaviors.

quence 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 12 shows four d-behaviors for the SR-equivalent scan register S_1 of Fig. 8 (b). A single differential value is inserted into x, y_1, y_2, and y_3, respectively.

Differential-behavior attack. The attack that inserts differential values into SR-equivalent 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, 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 SR-equivalent 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 12 shows the fundamental d-behavior set of S_1 of Fig. 8 (b).

Differential-behavior equivalent relation. Let S_1 and S_2 be SR-equivalent 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. $(d) \oplus (d) = (-)$, $(d) \oplus (-) = (d)$, $(-) \oplus (-) = (-)$. Then, the following theorem holds.

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

Proof: Suppose n differential values (d-values) are inserted into the input $(x, y_1, y_2, \ldots, y_k)$ of a scan circuit S. The propagation of each inserted d-value can be generated individually in S, from which n fundamental d-behaviors are obtained uniquely. The superposition of two propagations can be performed by superposing two corresponding values in accordance with an operation op such that $(d)\ op\ (d) = (-)$, $(d)\ op\ (-) = (d)$, and $(-)\ op\ (-) = (-)$, i.e., this op is XOR operation. Hence, the simultaneous propagation of n inserted d-values can be generated by taking XOR of those n fundamental propagations. Therefore, the total propagation is obtained by XOR-superposition of n fundamental propagations. □

Figure 13 illustrates two examples of Theorem 1. From Theorem 1, we see that two SR-equivalent scan circuits can be identified to be d-behavior equivalent or not, only by checking whether their fundamental behavior sets are the same.

Theorem 2: Let S_1 and S_2 be SR-equivalent 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.

Proof: If fundamental d-behavior sets of S_1 and S_2 are the same, d-behavior sets of S_1 and S_2 are also the same from Theorem 1, and hence S_1 and S_2 are d-behavior equivalent. If fundamental d-behavior sets of S_1 and S_2 are not the same, d-behavior sets of S_1 and S_2 are not the same and hence S_1 and S_2 are not d-behavior equivalent. □

5. Identification of Scan Structure

In [17], [18], we showed the number of k-stage SR-equivalent circuits for each type of circuits and the total number of SR-equivalent circuits with k flip-flops. They are $2^k - 1$, $2^{k(k-1)/2} - 1$, $2^{k(k-1)/2} - 1$, $(2^{k(k-1)/2} - 1)(2^k - 1)$, and $(2^{k(k-1)/2} - 1)(2^k - 1)$, for I^2SR, LF^2SR, LFSR, I^2LF^2SR, and I^2LFSR, respectively, and the total number of SR-equivalent circuits with k flip-flops is $2^k!/k! - 1$.

Consider the circuit R_1 of Fig. 8 (a) that is SR-equivalent. The total number of SR-equivalent circuits with 3 flip-flops is $2^k!/k! - 1 = 2^3!/3! - 1 = 6{,}719$. 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^2SR-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 SR-equivalent scan registers. However, if we target SR-equivalent scan circuits, we need to consider differential-behavior attacks.

Suppose the S-equivalent scan register R_1 and the SR-equivalent scan circuit S_1 in Fig. 8. S_1 consists of R_1. The fundamental d-behavior set of S_1 is shown in Fig. 12. As explained later in Sect. 6.2, every class of differential behavior equivalents for LF^2SR-type SR-equivalent 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 SR-equivalent 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 SR-equivalent scan circuit S approximates to the reciprocal of the cardinality of the class of SR-equivalent scan circuits that are d-behavior equivalent to S. To evaluate the security level against d-behavior attacks, for each type of SR-equivalent scan circuits we clarify the total number of SR-equivalent scan circuits in the class, the number of d-equivalent classes, and the cardinality of those equivalent classes in the following sections.

6. Cardinality of Differential Behavior Equivalents

From Theorem 2, we see that two SR-equivalent 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.

6.1 I^2SR without Dummy FF

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

$$(-,\dots,-,d),(-,\dots,-,d,-),\dots,(d,-,\dots,-)$$

Hence, the total number of SR-equivalent k-stage I^2SR-type scan circuits is 2^k-1.

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

6.2 LF^2SR and LFSR without Dummy FF

Consider an SR-equivalent k-stage LF^2SR-type scan circuit without dummy FF. If a differential value is inserted into the j-th FF y_j, the d-behavior becomes $(z_1,z_2,\dots,z_{j-1},d,-,\dots,-)$ 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

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

The total number of SR-equivalent k-stage LF^2SR-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 SR-equivalent scan circuits, the number of d-behavior equivalent classes, and the cardinality of those equivalent classes are the same as those of LF^2SR-type scan circuits.

6.3 I^2LF^2SR and I^2LFSR without Dummy FF

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

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

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

6.4 I^2SR with One Dummy FF

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

For each SR-equivalent k-stage I^2SR, there exist the following number of different patterns of placing one dummy FF as shown in Fig. 14. 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^2SR-type scan circuits with one dummy FF is

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

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

$$\binom{k}{1} + \binom{k}{2} = k + \frac{k(k-1)}{2} = \frac{k(k+1)}{2} \tag{4}$$

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

$$\left\lfloor \frac{\left(\frac{3k^2+k}{2}\right)\left(2^k - 1\right)}{\frac{k(k+1)}{2}} \right\rfloor = \frac{3k+1}{k+1}\left(2^k - 1\right) \approx 3\left(2^k - 1\right) \tag{5}$$

6.5 LF^{2}SR and LFSR with One Dummy FF

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

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 Fig. 14. 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 LF^{2}SR-type scan circuits with one dummy FF is

$$\left(2k + \tfrac{3}{2}k(k-1)\right)\left(2^{\frac{k(k-1)}{2}} - 1\right) = \left(\tfrac{3k^2+k}{2}\right)\left(2^{\frac{k(k-1)}{2}} - 1\right) \tag{6}$$

Similar to the discussion of Sect. 6.4, 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

$$\frac{\prod_{j=1}^{k} 2^{k-j}}{2^{k-1}} + \frac{\prod_{j=1}^{k} 2^{k-j}}{2^{k-2}} + \cdots + \frac{\prod_{j=1}^{k} 2^{k-j}}{2^{0}} = 2^{\frac{k^2-3k+2}{2}}\left(2^k - 1\right) \tag{7}$$

On the other hand, the number of scan circuits is

$$\left(\frac{3k^2+k}{2}\right)\left(2^{\frac{k(k-1)}{2}} - 1\right) \tag{8}$$

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

$$\left\lfloor \frac{\left(\frac{3k^2+k}{2}\right)\left(2^{\frac{k(k-1)}{2}} - 1\right)}{2^{\frac{k^2-3k+2}{2}}\left(2^k - 1\right)} \right\rfloor \approx O(k^2) \tag{9}$$

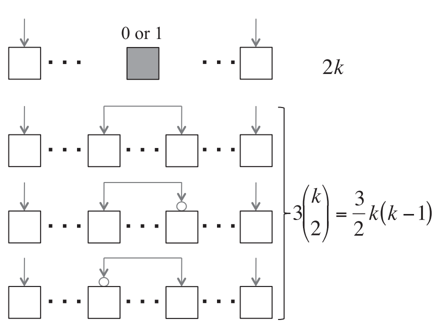


Fig. 14 Total number of patterns with one dummy FF.

6.6 I^{2}LF^{2}SR and I^{2}LFSR with One Dummy FF

Consider an SR-equivalent k-stage I^{2}LF^{2}SR-type scan circuit with one 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

$$\left(\frac{3k^2+k}{2}\right)\left(2^{\frac{k(k-1)}{2}} - 1\right)\left(2^k - 1\right) \tag{10}$$

The total number of d-equivalent classes is

$$2^{\frac{k^2-3k+2}{2}}\left(2^k - 1\right) \tag{11}$$

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

$$\left\lfloor \frac{\left(\frac{3k^2+k}{2}\right)\left(2^{\frac{k(k-1)}{2}} - 1\right)}{2^{\frac{k^2-3k+2}{2}}} \right\rfloor \approx O(k^2 2^k) \tag{12}$$

As for SR-equivalent k-stage I^{2}LFSR-type scan circuits with one dummy FF, we can obtain similarly, i.e., the number of SR-equivalent 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 with one dummy FF.

7. Enumeration Results by SREEP-2

In the previous sections, for each type of SR-equivalent scan circuits with/without dummy FF, we have clarified the total number of SR-equivalent 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. Tables 1 and 2 show the summary. From Table 1, two classes of LF^{2}SR

Table 1 Cardinality of d-behavior equivalent classes. (without dummy FF)

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

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

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

and LFSR are not secure because their guaranteed cardinality is 1. However, all other classes in Table 1 and Table 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 SR-equivalent scan circuits, we made a program called *SREEP-2* (*Shift Register Equivalents Enumeration and Synthesis Program-2*). The enumeration results for SR-equivalent scan circuits without and with dummy FF are shown in Table 3 and Table 4, respectively. The third column shows the number of SR-equivalent scan circuits in each class of SR-equivalent scan circuits. The fourth column shows the number of d-equivalent classes. The fifth column shows the guaranteed cardinality that is derived by dividing the value of third column by the value of fourth column. Hence, it is guaranteed there exists an equivalent class whose cardinality is larger than or equal to the guaranteed cardinality. Note that there might exist an equivalent class whose cardinality is smaller than the guaranteed one. The sixth column shows the range of cardinality that denotes the range from the minimum size to the maximum size among actual d-equivalent classes. The minimum size and the maximum size were obtained by enumerating all those d-behavior equivalent classes for SR-equivalent scan circuits by SREEP-2.

Table 3 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	7	1	7	7~7
	k=4	15	1	15	15~15
	k=5	31	1	31	31~31
LF^2SR	k=3	7	7	1	1~1
(LFSR)	k=4	63	63	1	1~1
	k=5	1023	1023	1	1~1
I^2LF^2SR	k=3	49	7	7	7~7
(I^2LFSR)	k=4	945	63	15	15~15
	k=5	31713	1023	31	31~31

Table 4 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
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	k=3	105	14	7	5~10
(LFSR)	k=4	1638	120	13	8~20
	k=5	40920	1984	20	11~40
I^2LF^2SR	k=3	735	14	52	35~70
(I^2LFSR)	k=4	24570	120	204	120~300
	k=5	1268520	1984	639	341~1240

As for the number of SR-equivalent scan circuits and the number of d-equivalent classes, theoretical values computed from the expressions in Sect. 6 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 Sect. 3, not all scan registers are replaced with SR-equivalent scan registers but only the registers necessary to be secure are replaced with SR-equivalent scan registers, as shown in Fig. 9. So, the area overhead of whole scan circuits is expected to be low. Further, the area overhead of each SR-equivalent scan register can be very low. Figure 15 shows an example of the outcome of an SR-equivalent 16-stage I^2LF^2SR-type 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.

8. 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 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.

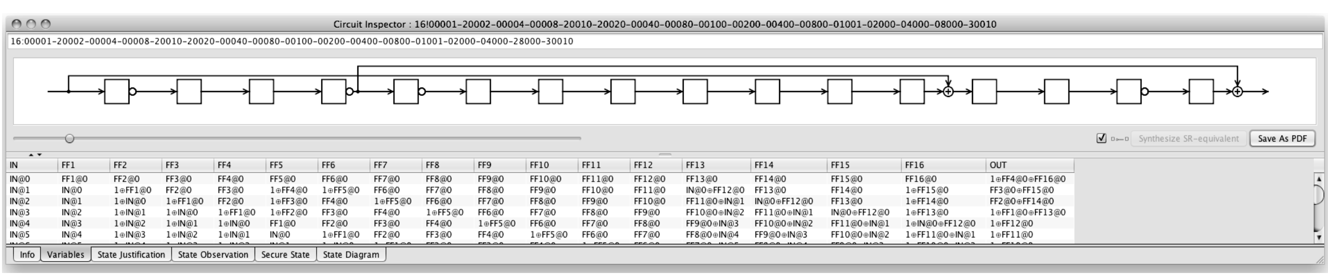


Fig. 15 Outcome of SR-equivalent extended scan register by SREEP-2.

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. Comput., vol.C-24, no.8, pp.821–826, Aug. 1975.
[2] H. Fujiwara, Logic Testing and Design for Testability, 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 Des. Test Comput., vol.8, no.4, 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," J. Electron. Test., Theory Appl., 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. Comput.-Aided Des. Integr. Circuits Syst., 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. 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. Comput.-Aided Des. Integr. Circuits Syst., vol.26, no.11, pp.2080–2084, Nov. 2007.
[14] M. Agrawal, S. Karmakar, D. Saha, and D. Mukhopadhyay, "Scan based side channel attacks on stream ciphers and their countermeasures," INDOCRYPT 2008, pp.226–238, 2008.
[15] R. Nara, N. Togawa, M. Yanagisawa, and T. Ohtsuki, "A scan-based attack based on discriminators for AES cryptosystems," IEICE Trans. Fundamentals, vol.E92-A, no.12, pp.3229–3237, Dec. 2009.
[16] 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.
[17] 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.
[18] K. Fujiwara, H. Fujiwara, M.E.J. Obien, and H. Tamamoto, "Enumeration and synthesis of shift register equivalents for secure scan design," IEICE Trans. Inf. & Syst. (Japanese Edition), vol.J93-D, no.11, pp.2426–2436, Nov. 2010.
[19] K. Fujiwara, H. Fujiwara, and H. Tamamoto, "SREEP-2: SR-equivalent generator for secure and testable scan design," 11th IEEE Workshop on RTL and High Level Testing, pp.7–12, Dec. 2010.
[20] H. Fujiwara, K. Fujiwara, and H. Tamamoto, "Secure scan design using shift register equivalents against differential behavior attack," 16th Asia and South Pacific Design Automation Conference, pp.818–823, Jan. 2011.
[21] O. Sinanoglu and A. Orailoglu, "Modeling scan chain modifications for scan-in test power minimization," International Test Conference 2003, pp.602–611, 2003.
[22] SREEP: http://sreep.fujiwaralab.net/

Katsuya Fujiwara received the B.E., the M.E., and the Ph.D. degrees in Engineering from Meiji University, Tokyo, Japan, in 1997, 1999, and 2002, respectively. He joined Akita University, Akita, Japan in 2002. Presently he is a Assistant Professor with the Department of Computer Science and Engineering, Akita University. His research interests are software engineering and network software. He is a member of the IPSJ, the JSSST and the IEEE Computer Society.

Hideo Fujiwara received the B.E., M.E., and Ph.D. degrees in electronic engineering from Osaka University, Osaka, Japan, in 1969, 1971, and 1974, respectively. He was with Osaka University from 1974 to 1985 and Meiji University from 1985 to 1993, and joined Nara Institute of Science and Technology, Nara, Japan in 1993. Presently he is a Professor with the Graduate School of Information Science, Nara Institute of Science and Technology, Nara Japan. His research interests are logic design, digital systems design and test, VLSI CAD and fault tolerant computing, including high-level/logic synthesis for testability, test synthesis, design for testability, built-in self-test, test pattern generation, parallel processing, and computational complexity. He has published over 380 papers in refereed journals and conferences, and nine books including the book from the MIT Press (1985) entitled Logic Testing and Design for Testability. He received many awards including the Okawa Prize for Publication, three IEEE CS (Computer Society) Certificate of Appreciation Awards, two IEEE CS Meritorious Service Awards, IEEE CS Continuing Service Award, and two IEEE CS Outstanding Contribution Awards. He has served as an editor and associate editors of several journals, including the IEEE Trans. on Computers, and Journal of Electronic Testing: Theory and Application, and as guest editor of several special issues of IEICE Transactions of Information and Systems. Dr. Fujiwara is a fellow of the IEEE, a Golden Core member of the IEEE Computer Society, and a fellow of the IPSJ.

Hideo Tamamoto received the B.E. degree in Electronic Engineering, the M.E. and D.E. degrees in Electrical Engineering from the University of Tokyo, Tokyo, Japan, in 1971, 1973 and 1976, respectively. In 1976, he joined the faculty of Akita University, Akita, Japan. Since 1993 he has been a professor in the Department of Computer Science and Engineering, Akita University. From 1996 to 1997, he was a visiting professor at the Electronic Engineering Department of Electrical Engineering, the University of Iowa, USA. His current research interests are testable design of logic circuits and current/thermal testing of CMOS logic circuits. He is a member of the IPSJ, the JSAI, the SICE and the IEEE.