Regular Paper

Secure and Testable Scan Design Utilizing Shift Register Quasi-equivalents

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

Abstract: Scan design makes digital circuits easily testable, however, it can also be exploited to be used for hacking the chip. We have reported a secure and testable scan design approach by using extended shift registers called "SR-equivalents" that are functionally equivalent but not structurally equivalent to shift registers [14], [15], [16], [17], [18]. In this paper, to further extend the class of SR-equivalents we introduce a wider class of circuits called "SR-quasi-equivalents" which still satisfy the testability and security similar to SR-equivalents. To estimate the security level, we clarify the cardinality of each equivalent class in SR-quasi-equivalents for several linear structural circuits, and also present the actual number of SR-quasi-equivalents obtained by the enhanced program SREEP.

Keywords: design-for-testability, scan design, shift register quasi-equivalents, security, scan-based side-channel attack

1. Introduction

Both testability and security of a chip has become primordial to ensure its reliability and protection from invasion to access important information. However, both may have conflicting requirements for designers. To guarantee quality, designers use design for testability (DFT) methods to make digital circuits easily testable for faults. Scan design is a powerful DFT technique that warrants high controllability and observability over a chip and yields high fault coverage [1], [2]. However, this also accommodates reverse engineering, which contradicts security. For secure chip designers, there is a demand to protect secret data from side-channel attacks and other hacking schemes [3]. Nevertheless, with improved control and access to the chip through DFT, the chip becomes more vulnerable to attacks. Scan chains can be used to steal important information such as intellectual property (IP) and secret keys of cryptographic chips [4], [6]. Despite all these, security chips can be made more susceptible to errors, and thus, not secure, if they are faulty. Therefore, testability is as important as security for secure IC designers to guarantee the quality of security and functionality of the chip. Hence, there is a need for an efficient solution to satisfy both testability and security of digital circuits.

To solve this challenging problem, different approaches have been proposed [4], [5], [6], [7], [8], [9], [10], [11], [12], [13]. All the approaches except Ref. [13] add extra hardware outside of the scan chain. Disadvantages of this are high area overhead, timing overhead or performance degradation, increased complexity of testing, and limited security for the registers part among others. The approach of Ref. [13] which inserts inverters in scan chains has a disadvantage such that the positions of inserted inverters can be determined by simply scanning out after resetting (to zero) all the flip-flops in the scan chain. Thus, internal state can be identified and the security is breached. To resolve those disadvantages of previous works, we have reported a secure and testable scan design approach by using extended shift registers called "*SR-equivalents*" that are functionally equivalent but not structurally equivalent to shift registers [14], [15], [16], [17], [18]. The proposed approach is only to replace part of the original scan chains to SR-equivalents, which satisfy both testability and security of digital circuits. This method requires very little area overhead and no performance overhead. Moreover, no additional keys and controller circuits outside of the scan chain are needed, thus making the scheme low-cost and efficient.

In this paper, to further extend the class of SR-equivalents we introduce a wider class of circuits called "*SR-quasi-equivalents*" which still satisfy the testability and security similar to SR-equivalents. The class of SR-equivalents is a specific subclass of SR-quasi-equivalents. The proposed approach in this paper is the same as Refs. [14], [15], [16], [17], i.e., it is only to replace part of the original scan chains to SR-quasi-equivalents in place of SR-equivalents. Using SR-quasi-equivalents in place of SR-equivalents has several advantages. The class of SR-quasi-equivalents is wider than that of SR-equivalents, and hence it has more choices or is more flexible to select modified scan registers not only for security and testability but also for other purpose such as low power testing. The security level of the secure scan architecture based on those SR-quasi-equivalents is determined by the probability that an attacker can identify or guess right the configuration of the SR-quasi-equivalent used in the circuit, and hence the attack probability approximates to the reciprocal of the cardinality of the class of SR-quasi-equivalents. We clarify the cardinality of each equivalent class in SR-quasi-equivalents for several

1   Akita University, Akita 010–8502, Japan
2   Osaka Gakuin University, Suita, Osaka 564–8511, Japan
a)   fujiwara@ie.akita-u.ac.jp

linear structured circuits, and also present the actual number of SR-quasi-equivalents obtained by the program SREEP [20].

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.

Definition 1. 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, $z(t+3) = x(t)$, 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 $(x(t), x(t+1), x(t+2))$ which transfers SR to the state $(y_1(t+3), y_2(t+3), y_3(t+3))$ is $(x(t), x(t+1), x(t+2)) = (y_3(t+3), y_2(t+3), y_1(t+3))$. The initial state $(y_1(t), y_2(t), y_3(t))$ can be identified as $(y_1(t), y_2(t), y_3(t)) =$
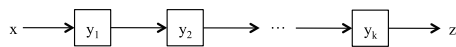
$(z(t+2), z(t+1), z(t))$ from the output sequence $(z(t), z(t+1), z(t+2))$. However, for the SR-equivalent circuit R_1, the input sequence which transfers R_1 to the state $(y_1(t+3), y_2(t+3), y_3(t+3))$ is $(x(t), x(t+1), x(t+2)) = (y_3(t+3) \oplus y_2(t+3), y_2(t+3), y_1(t+3))$ from Fig. 3, and the initial state $(y_1(t), y_2(t), y_3(t))$ can be identified as $(y_1(t), y_2(t), y_3(t)) = (z(t+2), z(t+1), z(t) \oplus z(t+1))$ 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 general circuits.

In Ref. [15], we showed the number of k-stage SR-equivalent circuits for each type of circuits. They are summarized in **Table 1**. From those cardinalities of SR-equivalents, the complexity or the difficulty of identifying the structure of SR-equivalent circuits increases more than exponentially as the stage of SR increases. Hence, very high security can be realized by using SR-equivalent circuits.

3.   SR-quasi-equivalent Circuits

For an 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*.

Definition 2. A circuit C with a single input, a single output, and k flip-flops is called to be *scan-controllable* if for any internal state of C a transfer sequence (of length k) to the state (final state) can be generated only from the connection information of C, independently of the initial state.

Definition 3. A circuit C with a single input, a single output, and k flip-flops is called to be *scan-observable* if any present state (initial state) of C can be identified only from the output sequence

Fig. 1 k-stage shift register SR.
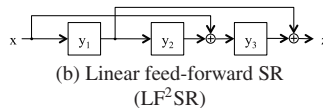

Fig. 2 k-stage SR-equivalent circuit C.

(a) SR-equivalent circuit R_1

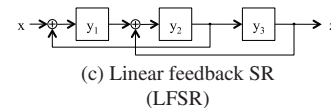| x	y_1	y_2	y_3	z
$x(t)$	$y_1(t)$	$y_2(t)$	$y_3(t)$	$z(t) = y_2(t) \oplus y_3(t)$
$x(t+1)$	$x(t)$	$y_1(t)$	$y_1(t) \oplus y_2(t)$	$z(t+1) = y_2(t)$
$x(t+2)$	$x(t+1)$	$x(t)$	$x(t) \oplus y_1(t)$	$z(t+2) = y_1(t)$
$x(t+3)$	$x(t+2)$	$x(t+1)$	$x(t) \oplus x(t+1)$	$z(t+3) = x(t)$

(b) Behavior of R_1 by symbolic simulation

Fig. 3   Example of SR-equivalent circuit.

Table 1   Cardinality of each class.

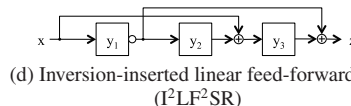|	# of circuits in the class	# of SR-equivalents in the class
I^2SR	$2^{k+1} - 1$	$2^k - 1$
LFSR	$2^{k(k+1)/2} - 1$	$2^{k(k-1)/2} - 1$
LF^{2}SR	$2^{k(k+1)/2} - 1$	$2^{k(k-1)/2} - 1$
I^2LFSR	$(2^{k(k+1)/2} - 1)(2^{k+1} - 1)$	$(2^{k(k-1)/2} - 1)(2^k - 1)$
I^2LF^{2}SR	$(2^{k(k+1)/2} - 1)(2^{k+1} - 1)$	$(2^{k(k-1)/2} - 1)(2^k - 1)$

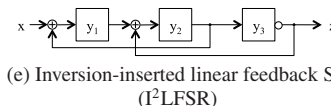(a) Inversion-inserted SR (I^2SR)

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

(c) Linear feedback SR (LFSR)

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

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

Fig. 4   Five types of linear structured circuits.

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

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

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

(b) Equations for state-justification

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

$$y_1(t) = z(t+2)$$
$$y_2(t) = 1 \oplus z(t+1)$$
$$y_3(t) = 1 \oplus z(t) \oplus z(t+2)$$
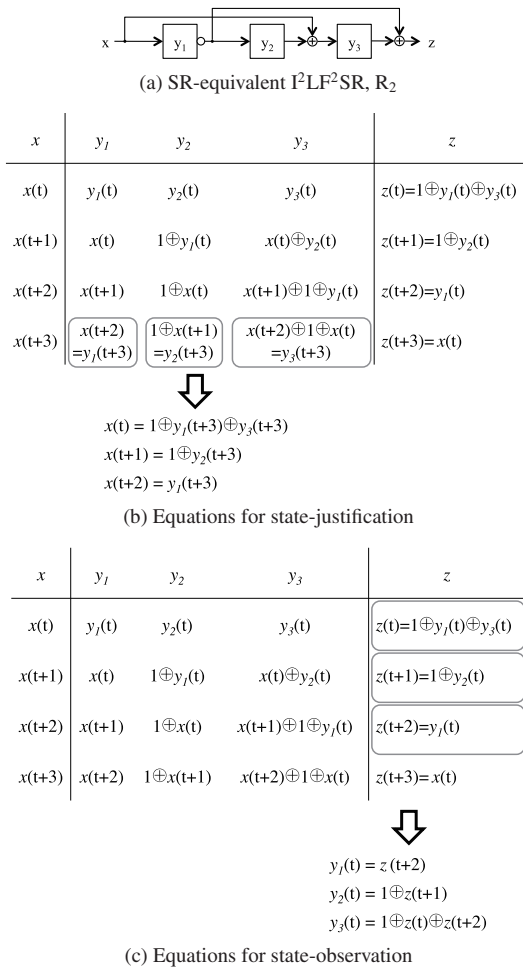
(c) Equations for state-observation

Fig. 5   State-justification and state-observation for R_2.

(of length k) and the connection information of C, independently of the initial state and the input sequence.

Definition 4. A circuit C is called to be *scan-testable* if C is scan-controllable and scan-observable.

In Ref. [14] we showed that any SR-equivalent circuit is scan-testable.

Theorem 1. [14]   *Any SR-equivalent circuit is scan-controllable and scan-observable, and hence scan-testable.*

Consider a 3-stage I^2LF^2SR, R_2, given in **Fig. 5** (a). This I^2LF^2SR is SR-equivalent. By using symbolic simulation, we can derive equations to obtain an input sequence $(x(t), x(t+1), x(t+2))$ that transfers R_2 from any state to the desired final state $(y_1(t+3), y_2(t+3), y_3(t+3))$ as illustrated in Fig. 5 (b). Similarly, as illustrated in Fig. 5 (c), we can derive equations to determine uniquely the initial state $(y_1(t), y_2(t), y_3(t))$ from the output sequence. Hence, R_2 is scan-testable.

Next, let us try to relax the definition of scan-testability. First, suppose to relax the scan-controllability by removing "independence of the initial state" as follows.

Definition 5. A circuit C is called to be *quasi-scan-controllable* if for any internal state of C a transfer sequence of length k to the final state can be generated from a given initial state and the connection information of C.

However, this quasi-scan-controllability does not make the state-justification easy because of the dependence of initial state.

So, we don't adopt this relaxation. Next, let us relax the definition of scan-observability as follows.

Definition 6. A circuit C is called to be *quasi-scan-observable* if any present state (initial state) of C can be identified from the output sequence with respect to any applied input sequence (of length k) and the connection information of C.

In this case, since it is easy to apply any input sequence to C, this quasi-scan-observability makes state-observation easy. So, we adopt this relaxation and extend scan-testability as follows.

Definition 7. A circuit C is called to be *quasi-scan-testable* if C is scan-controllable and quasi-scan-observable.

Based on the above new concept of "quasi-scan-testability," we introduce a new class of circuits as follows.

Definition 8. A circuit C with a single input x, a single output z, and k flip-flops is called *functionally quasi-equivalent* to a k-stage shift register (or *SR-quasi-equivalent*) if the input value applied to x at any time t appears at z after k clock cycles with exclusive-OR of some inputs and/or constant 1, i.e.,

$$z(t + k) = x(t) \oplus c_0 \oplus c_1 x(t + 1) \oplus c_2 x(t + 2) \oplus \ldots \oplus c_k x(t + k)$$

where $c_0, c_1, c_2, ..., c_k$ are 0 or 1. The ordered set of coefficients $(c_0, c_1, c_2, ..., c_k)$ is called the *characteristic coefficient* of the SR-quasi-equivalent circuit C.

We can prove that any SR-quasi-equivalent circuit C satisfies the following two properties: (1) for any internal state of C a transfer sequence (of length k) to the state (final state) can be generated only from the connection information of C, independently of the initial state, i.e., C is scan-controllable; (2) any present state (initial state) of C can be identified from the input-output sequence (of length k) and the connection information of C, i.e., C is quasi-scan-observable, where k is the number of flip-flops. Hence, we have the following.

Theorem 2. *Any SR-quasi-equivalent circuit is scan-controllable and quasi-scan-observable, and hence quasi-scan-testable.*

Proof. Let C be a SR-quasi-equivalent circuit with a single input x, a single output z, and k flip-flops. Since C is SR-quasi-equivalent, the output z at time $t + k$ is $z(t+k) = x(t) \oplus c_0 \oplus c_1 x(t+1) \oplus c_2 x(t+2) \oplus \ldots \oplus c_k x(t+k)$, where $(c_0, c_1, c_2, \ldots, c_k)$ is the characteristic coefficient of C. That is, the input value $x(t)$ flows through k flip-flops to the output z. Without loss of generality, we can suppose $x(t)$ propagates $y_1(t + 1), y_2(t + 2), \ldots, y_k(t + k)$, and $z(t + k)$. The value of $x(t)$ propagates through $y_1(t + 1), y_2(t + 2), \ldots, y_k(t + k)$, and $z(t + k)$. Further, $z(t + k)$ can be expressed as $z(t+k) = x(t) \oplus c_0 \oplus c_1 x(t+1) \oplus \ldots \oplus c_k x(t+k)$, i.e., $z(t+k) = x(t) \oplus f_0$, where $f_0 = c_0 \oplus c_1 x(t+1) \oplus \ldots \oplus c_k x(t+k)$. Similarly, the value of $y_1(t)$ propagates through $y_2(t + 1), y_3(t + 2), \ldots, y_k(t + k - 1)$, and $z(t + k - 1)$. Hence, $z(t + k - 1)$ can be expressed as $z(t + k - 1) = y_1(t) \oplus f_1$. In the same way, $z(t+k-2), z(t+k-3), \ldots$, and $z(t)$ are also expressed as $z(t+k-2) = y_2(t) \oplus f_2, z(t+k-3) = y_3(t) \oplus f_3, \ldots$, and $z(t) = y_k(t) \oplus f_k$, respectively, where $f_1, f_2, \ldots$, and f_k are the linear functions of $y_1(t), y_2(t), \ldots, y_k(t), x(t), x(t + 1), \ldots$, and $x(t + k - 1)$. From these k equations, $y_1(t), y_2(t), \ldots$, and $y_k(t)$ are expressed only by $x(t), x(t+1), \ldots, x(t+k-1), z(t), z(t+1), \ldots, z(t+ k - 1)$. Therefore, the initial state of k flip-flops can be identified from the input-output sequence (of length k) and the connection information of C, i.e., C is quasi-scan-observable.
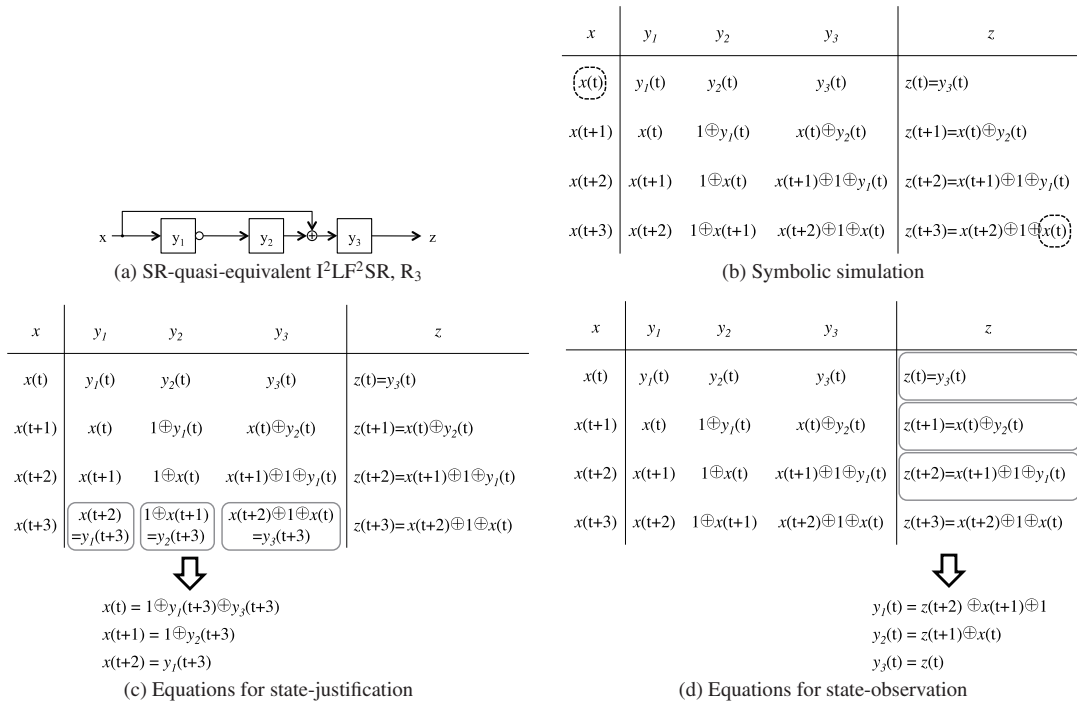
(b) Symbolic simulation

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

(a) SR-quasi-equivalent I²LF²SR, R₃

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

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

(c) Equations for state-justification

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

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

(d) Equations for state-observation

Fig. 6   Example of SR-quasi-equivalent circuit.

Next, let us prove that the values $y_1(t + k), y_2(t + k), \ldots$, and $y_k(t + k)$ are expressed only by $x(t), x(t + 1), \ldots, x(t + k - 1)$, independently of the initial values $y_1(t), y_2(t), \ldots$, and $y_k(t)$.

Let us prove it by contradiction. Assume it does not hold. Then, there exists a flip-flop y_a such that $y_a(t + k)$ includes $y_b(t)$. Assign $y_1(t) = 0, y_2(t) = 0, \ldots, y_b(t) = 1, \ldots, y_k(t) = 0$, and $x(t) = x(t + 1) = \ldots = x(t + k - 1) = 0$. Since $y_a(t + k)$ includes $y_b(t)$, $y_a(t + k) = 1$. This value is propagated to z at some time, i.e., $z(t + k + j) = 1$ for some $j < k$. On the other hand, $x(t) = x(t + 1) = \ldots = x(t + k - 1) = 0$ implies $z(t + k) = z(t + k + 1) = \ldots = z(t + 2k - 1) = 0$ since this circuit C is SR-quasi-equivalent. This is inconsistent with $z(t + k + j) = 1$ for some $j < k$. Therefore, the values $y_1(t + k), y_2(t + k), \ldots$, and $y_k(t + k)$ can be expressed only by $x(t), x(t + 1), \ldots, x(t + k - 1)$, independently of the initial values $y_1(t), y_2(t), \ldots$, and $y_k(t)$. This means that for any internal state of C a transfer sequence (of length k) to the final state can be generated only from the connection information of C, independently of the initial state, i.e., C is scan-controllable. □

Consider a 3-stage I²LF²SR, R₃, given in **Fig. 6** (a). This I²LF²SR is SR-quasi-equivalent. By using symbolic simulation, we can obtain an output sequence $(z(t), z(t + 1), z(t + 2), z(t + 3))$ and the output $z(t + 3) = x(t) \oplus 1 \oplus x(t + 2)$ as shown in Fig. 6 (b). Therefore, R₃ is SR-quasi-equivalent. By using symbolic simulation, we can derive equations to obtain an input sequence $(x(t), x(t + 1), x(t + 2))$ that transfers R₃ from any state to the desired final state $(y_1(t + 3), y_2(t + 3), y_3(t + 3))$ as illustrated in Fig. 6 (c). Similarly, as illustrated in Fig. 6 (d), we can derive equations to determine uniquely the initial state $(y_1(t), y_2(t), y_3(t))$ from the input/output sequence.

4.   Application to Scan Design
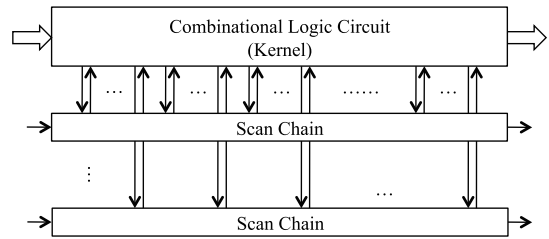
A scan-designed circuit consists of a single or multiple scan

Fig. 7   Scan-designed circuit.

(a) Standard scan register

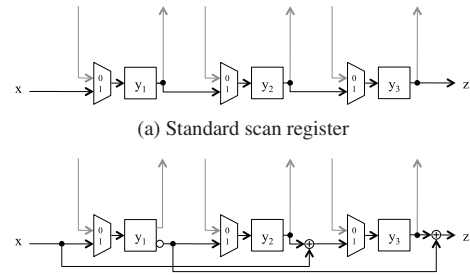(b) Modified scan register (SR-quasi-equivalent)

Fig. 8   Standard and modified scan registers.

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 as shown in **Fig. 8** (a). Here, we replace the shift register with a modified SR-quasi-equivalent scan register as shown in Fig. 8 (b).

However, to reduce the area overhead as much as possible, not all scan chains are replaced with modified scan chains. As shown in **Fig. 9**, only parts of scan chains necessary to be secure are replaced with modified scan chains that cover secret registers to be protected, and the size of the modified scan chains is large enough to make it secure. The size of modified scan chain can

Table 2   Cardinality of each equivalent class in SR-quasi-equivalents obtained by analysis.

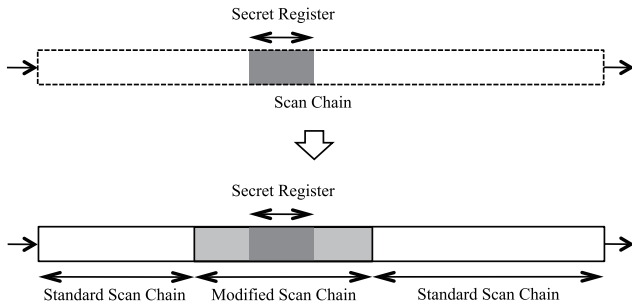| Equivalent class	I²SR	LF²SR	I²LF²SR	I²LFSR	LFSR	Total
00...00	$2^k - 1$	$2^{k(k-1)/2} - 1$	$(2^{k(k-1)/2} - 1)(2^k - 1)$	$(2^{k(k-1)/2} - 1)(2^k - 1)$	$2^{k(k-1)/2} - 1$	$2(2^{k(k+1)/2}) - 2^k - 1$
00...01	0	$2^{k(k-1)/2}$	$2^{k(k-1)/2}(2^k - 1)$	0	0	$2^{k(k+1)/2}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
01...11	0	$2^{k(k-1)/2}$	$2^{k(k-1)/2}(2^k - 1)$	0	0	$2^{k(k+1)/2}$
10...00	2^k	0	$(2^{k(k-1)/2} - 1)2^k$	$(2^{k(k-1)/2} - 1)2^k$	0	$2(2^{k(k+1)/2}) - 2^k$
10...01	0	0	$2^{k(k-1)/2}2^k$	0	0	$2^{k(k+1)/2}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
11...11	0	0	$2^{k(k-1)/2}2^k$	0	0	$2^{k(k+1)/2}$
Total	$2^{k+1} - 1$	$2^{k(k+1)/2} - 1$	$(2^{k(k+1)/2} - 1)(2^{k+1} - 1)$	$(2^{k(k-1)/2} - 1)(2^{k+1} - 1)$	$2^{k(k-1)/2} - 1$	

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

be determined by the expected security level computed from the cardinality of SR-quasi-equivalent circuits that will be described in the following section. The delay overhead due to additional Exclusive-OR gates influences only scan operation, and hence there is no delay overhead for normal operation.

Since the modified scan register is scan-testable, any input sequence can be applied to the modified scan register during state-observation. Hence, both state-justification and state-observation can be performed simultaneously, i.e., both scan-in and scan-out operations can be overlapped in the same way as the standard scan testing. Therefore, the test sequence for the modified scan design is of the same length as the standard scan design.

5.   Cardinality of SR-quasi-equivalents

When we consider a secure scan design, we need to assume what the attacker knows and how he can potentially make the attack. Here, we assume that the attacker does not know the detailed information in the gate-level design, and that the attacker knows the presence of test pins (scan in/out, scan, and reset) and modified scan chains. However, he does not know the structure of modified scan chains (the connection information, position of XOR and NOT, and the size).

Based on the above assumption, we consider the security to prevent scan-based attacks.

Definition 9. A circuit C with a single input x, a single output z, and k flip-flops is called scan-secure if the attacker cannot determine the structure of C.

First, let us consider reset-based attack. For the type of I²SR, the positions of inverters can be determined by simply scanning out after resetting (to zero) all the flip-flops in the scan chain. In our previous work [14], [18], we showed such reset-based attack can be protected by adding one extra flip-flop which disables scan operation right after reset. Here, we assume our proposed

scheme of modified scan registers adopts such an extra flip-flop introduced in Refs. [14], [18] to prohibit scan-after-reset operation so that an attacker cannot initialize the register by resetting.

Next, consider two SR-quasi-equivalents C_1 and C_2. Suppose that C_1 and C_2 have different structures but the same characteristic coefficient. Then, for any input sequence, the output sequences of C_1 and C_2 are the same after k clock cycles, independently of their initial states. There also exist states s_1 and s_2 for C_1 and C_2, respectively, such that the output sequences of C_1 and C_2 starting from states s_1 and s_2 are the same. Hence, we cannot distinguish C_1 with s_1 and C_2 with s_2 merely from the input/output relation. Suppose an SR-quasi-equivalent C is given which is either C_1 or C_2. Since scan-after-reset attack cannot be performed, we cannot reset C. Further, unless we know the structure of C, we cannot determine the initial state merely from input/output relation, and hence we cannot initialize C. Without knowing the internal state of C, we cannot identify if C is C_1 or C_2. Therefore, an attacker cannot determine the structure of C, and hence C_1 and C_2 are scan-secure.

The characteristic coefficient of any SR-quasi-equivalent circuit C can be identified by applying input sequences to C and observing the output responses from C.

Here, we partition the whole set of SR-quasi-equivalent circuits with k flip-flops into equivalent classes based on characteristic coefficient. Since the size of coefficient is $k + 1$, the number of equivalent classes is 2^{k+1}. The first equivalent class of the characteristic coefficient, 00...0, is the set of SR-equivalent circuits.

The security level of the secure scan architecture based on those SR-quasi-equivalents is determined by the probability that an attacker can guess right the structure of the SR-quasi-equivalent circuit used in the circuit, and hence the attack probability approximates to the reciprocal of the cardinality of the class of SR-quasi-equivalents. Since the attacker can determine the characteristic coefficient of SR-quasi-equivalents, we need to clarify the cardinality of each equivalent class in SR-quasi-equivalents to estimate the attack probability.

The cardinality of each equivalent class in five types of linear structured circuits (I²SR, LF²SR, I²LF²SR, I²LFSR, LFSR) is summarized in **Table 2**. The second row is the equivalent class of the characteristic coefficient 00...00, and this is the same as the SR-equivalents (see Table 1). The fourth row is the equivalent class of 10...00 such that $z(t + k) = x(t) \oplus 1$. The last row is the total number of each type of linear structured circuit. They coincide with the total number of circuits in the class for I²SR,

Table 3   Cardinality of each equivalent class for $k = 4$ obtained by SREEP.

	I²SR	LF²SR	I²LF²SR	I²LFSR	LFSR	Total
00000	15	63	945	945	63	2,031
00001	0	64	960	0	0	1,024
⋮	⋮	⋮	⋮	⋮	⋮	⋮
01111	0	64	960	0	0	1,024
10000	16	0	1,008	1,008	0	2,032
10001	0	0	1,024	0	0	1,024
⋮	⋮	⋮	⋮	⋮	⋮	⋮
11111	0	0	1,024	0	0	1,024
Total	31	1,023	31,713	1,953	63	

Table 4   Cardinality of each class of SR-equivalents/quasi-equivalents.

Class	# of circuits in the class	# of SR-equivalents in the class	# of SR-quasi-equivalents in the class
I²SR	$2^{k+1}-1$	2^k-1	$2^{k+1}-1$
LF²SR	$2^{k(k+1)/2}-1$	$2^{k(k-1)/2}-1$	$2^{k(k+1)/2}-1$
I²LF²SR	$(2^{k(k+1)/2}-1)(2^{k+1}-1)$	$(2^{k(k-1)/2}-1)(2^k-1)$	$(2^{k(k+1)/2}-1)(2^{k+1}-1)$
I²LFSR	$(2^{k(k+1)/2}-1)(2^{k+1}-1)$	$(2^{k(k-1)/2}-1)(2^k-1)$	$(2^{k(k-1)/2}-1)(2^{k+1}-1)$
LFSR	$2^{k(k+1)/2}-1$	$2^{k(k-1)/2}-1$	$2^{k(k-1)/2}-1$

LF²SR, and I²LF²SR (see Table 1). This means any circuit of type I²SR, LF²SR, and I²LF²SR is SR-quasi-equivalent. On the other hand, as for I²LFSR only two equivalent classes (00...00 and 10...00) are SR-quasi-equivalents. As for LFSR, there is no SR-quasi-equivalent circuit except SR-equivalent circuits.

In Refs. [15], [16], we reported a program called SREEP (Shift Register Equivalents Enumeration and Synthesis Program). To examine the actual cardinalities of equivalent classes in SR-quasi-equivalents, we enhanced the program by adding several facilities in handling SR-quasi-equivalents and its equivalent classes. **Table 3** shows the results obtained by SREEP. The theoretical values obtained by substituting 4 for k for Table 2 coincides with the actual values in Table 3 obtained by SREEP [20].

The characteristic coefficient of any SR-quasi-equivalent circuit C can be determined by applying input sequences to C and observing the output responses from C. After knowing the characteristic coefficient, the probability that an attacker can further identify or guess right the structure of an SR-quasi-equivalent circuit approximates to the reciprocal of the cardinality of the coefficient's equivalent class. These cardinalities are shown in the right end column of Table 2. They are all similar to the cardinality of SR-equivalent circuits, i.e., the coefficient (00 . . . 00) class. They grow much more rapidly than exponentially and hence they are very secure.

From Table 1 and Table 2, for each class of linear structured circuits (I²SR, LF²SR, I²LF²SR, I²LFSR, LFSR), we have **Table 4** which illustrates the total number of circuits in the class, the number of SR-equivalents in the class, and the number of SR-quasi-equivalents in the class.

From Table 2 and Table 4, we have the covering relation among five classes of linear structured circuits (I²SR, LF²SR, I²LF²SR, I²LFSR, LFSR), and SR-equivalents and SR-quasi-equivalents as illustrated in **Fig. 10**.

Although the security level of SR-quasi-equivalents is almost the same as that of SR-equivalents, there are several merits when
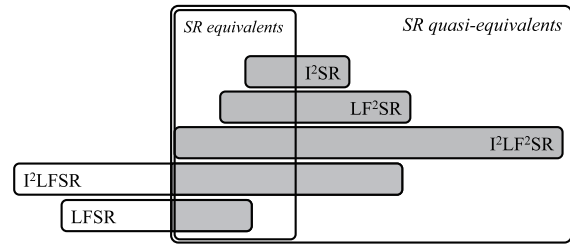

Fig. 10   Covering relation among classes.

applying SR-quasi-equivalents to the scan chain. One merit is as follows. From Fig. 10, we can see all the circuits in I²SR, LF²SR, and I²LF²SR are SR-quasi-equivalent, and hence we can use any of them to organize the secure and testable scan chains which means it is very easy to design an SR-quasi-equivalent circuit. Another merit is as follows. As for the influence on test power due to shift register modification, the insertion of inverters and/or XOR gates can reduce test power even more than standard scan design if they are inserted appropriately. However, such modified shift registers are not always SR-equivalent but mostly SR-quasi-equivalent. Hence, SR-quasi-equivalent circuits are useful to easily organize modified scan chains that satisfy low-power testing as well as security and testability similar to SR-equivalent circuits.

6.   Conclusion

In our previous work [14], [15], [16], [17], [18], we reported a secure and testable scan design approach by using extended shift registers called "SR-equivalents" that are functionally equivalent but not structurally equivalent to shift registers. In this paper, to extend the class of SR-equivalents we have introduced a wider class of circuits called "SR-quasi-equivalents" which still satisfy the testability and security similar to SR-equivalents.

The security level for the secure scan design based on SR-quasi-equivalents is related to the attack probability that approximates to the reciprocal of the cardinality of the class of SR-quasi-equivalents. In this paper, we clarified the cardinality of each equivalent class in SR-quasi-equivalents for several linear structured circuits, and also presented the actual number of SR-quasi-equivalents obtained by the program SREEP [20].

References

[1] Fujiwara, H., Nagao, Y., Sasao, T. and Kinoshita, K.: Easily testable sequential machines with extra inputs, *IEEE Trans. Comput.*, Vol.C-24, No.8, pp.821–826 (1975).

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

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

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

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

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

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

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

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

[10] Paul, S., Chakraborty, R.S. and Bhunia, S.: 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] Inoue, M., Yoneda, T., Hasegawa, M. and Fujiwara, H.: Partial scan approach for secret information protection, *14th IEEE European Test Symposium*, pp.143–148 (2009).

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

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

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

[15] Fujiwara, K., Fujiwara, H., Obien, M.E.J. and Tamamoto, H.: 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 (2010).

[16] Fujiwara, K., Fujiwara, H. and Tamamoto, H.: SREEP-2: SR-equivalent Generator for Secure and Testable Scan Design, *11th IEEE Workshop on RTL and High Level Testing*, pp.7–12 (2010).

[17] Fujiwara, K., Fujiwara, H., Obien, M.E.J. and Tamamoto, H.: Enumeration and Synthesis of Shift Register Equivalents for Secure Scan Design, *IEICE Trans. Inf. and Syst.*, Vol.J93-D, No.11, pp.2426–2436 (2010). (In Japanese)

[18] Fujiwara, K., Fujiwara, H. and Tamamoto, H.: Differential Behavior Equivalent Classes of Shift Register Equivalents for Secure and Testable Scan Design, *IEICE Trans. Inf. and Syst.*, Vol.E94-D, No.7, pp.1430–1439 (2011).

[19] Fujiwara, K., Fujiwara, H. and Tamamoto, H.: SR-Quasi-Equivalents: Yet Another Approach to Secure and Testable Scan Design, *12th IEEE Workshop on RTL and High Level Testing* (*WRTLT'11*), pp.77–82 (2011).

[20] SREEP: available from ⟨http://sreep.fujiwaralab.net/⟩ (accessed 2012-05-11).

Hideo Fujiwara received his 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, Meiji University from 1985 to 1993, Nara Institute of Science and Technology from 1993 to 2011, and joined Osaka Gakuin University in 1993. Presently he is a Professor Emeritus of Nara Institute of Science and Technology, and a Professor with Faculty of Informatics, Osaka Gakuin University. 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 390 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 IEEE Transactions on Computers, and Journal of Electronic Testing: Theory and Application, and as a guest editor of several special issues of IEICE Transactions of Information and Systems. Dr. Fujiwara is a life fellow of IEEE, a Golden Core member of IEEE Computer Society, a fellow of IEICE, and a fellow of IPSJ.

Katsuya Fujiwara received his B.E., M.E., and 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 an 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 IEICE, IPSJ, JSSST and IEEE Computer Society.

Hideo Tamamoto received his B.E. degree in Electronic Engineering, 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 IEICE, IPSJ, JSAI, SICE and IEEE.

(Recommended by Associate Editor: *Toshinori Hosokawa*)