12th IEEE Workshop on RTL and High Level Testing (WRTLT'11), pp. 77-82, Nov. 2011.

SR-Quasi-Equivalents: Yet Another Approach to Secure and Testable Scan Design

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

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

[2] Faculty of Informatics
Osaka Gakuin University
Osaka, 564-8511, JAPAN
fujiwara@ogu.ac.jp

***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 [14-17]. 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 equivalents; 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 [4-13]. All the approaches except [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. In [14 - 17], 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. 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 security level of the secure scan architecture based on those SR-quasi-equivalents is determined by the probability that an attacker can identify 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 linear structured circuits, and also present the actual number of SR-quasi-equivalents obtained by the program SREEP [18].

2. SR-EQUIVALENT CIRCUITS

Consider a k-stage shift register shown in Figure 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 Figure 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.

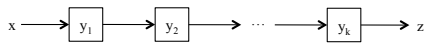
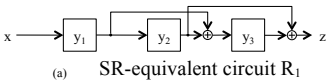


Figure 1. k-stage shift register SR

Figure 2. k-stage SR-equivalent circuit C

Figure 3 illustrates an example of 3-stage SR-equivalent circuit R_1. The table in Figure 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)⊕y_2(t+3), y_2(t+3), y_1(t+3)) from Figure 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)⊕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*.



(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)⊕y_3(t)
x(t+1)	x(t)	y_1(t)	y_1(t)⊕y_2(t)	z(t+1) = y_2(t)
x(t+2)	x(t+1)	x(t)	x(t)⊕y_1(t)	z(t+2) = y_1(t)
x(t+3)	x(t+2)	x(t+1)	x(t+1)⊕x(t)	z(t+3) = x(t)

(b) Behavior of R_1 by symbolic simulation

Figure 3. Example of SR-equivalent circuit

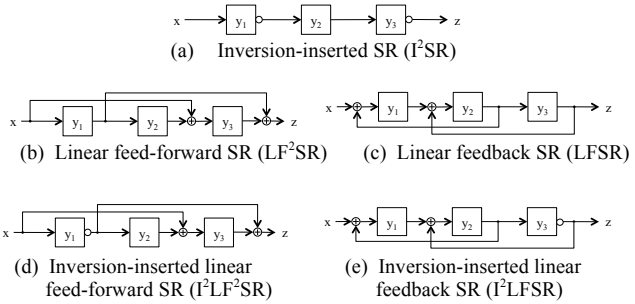


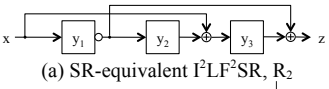
Figure 4. Five types of linear structured circuits

The SR-equivalent circuit shown in Figure 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 Figure 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 [15], we showed the number of k-stage SR-equivalent circuits for each type of circuits. They are summarized in Table I. 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.

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
LF^2SR	$2^{k(k+1)/2}$ - 1	$2^{k(k-1)/2}$ - 1
LFSR		
I^2LF^2SR	$(2^{k(k+1)/2}-1)(2^{k+1}-1)$	$(2^{k(k-1)/2}-1)(2^k-1)$
I^2LFSR		



(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⊕y_1(t)⊕y_3(t)
x(t+1)	x(t)	1⊕y_1(t)	x(t)⊕y_2(t)	z(t+1)=1⊕y_2(t)
x(t+2)	x(t+1)	1⊕x(t)	x(t+1)⊕1⊕y_1(t)	z(t+2)=y_1(t)
x(t+3)	x(t+2) =y_1(t+3)	1⊕x(t+1) =y_2(t+3)	x(t+2)⊕1⊕x(t) =y_3(t+3)	z(t+3)= x(t)

x(t) = 1⊕y_1(t+3)⊕y_3(t+3)
x(t+1) = 1⊕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⊕y_1(t)⊕y_3(t)
x(t+1)	x(t)	1⊕y_1(t)	x(t)⊕y_2(t)	z(t+1)=1⊕y_2(t)
x(t+2)	x(t+1)	1⊕x(t)	x(t+1)⊕1⊕y_1(t)	z(t+2)=y_1(t)
x(t+3)	x(t+2)	1⊕x(t+1)	x(t+2)⊕1⊕x(t)	z(t+3)= x(t)

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

(c) Equations for state-observation

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

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.***

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.

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

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

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 Figure 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 Figure 5(b). Similarly, as illustrated in Figure 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.

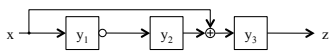
Next, let us first try to relax the definition of scan-testability. First, suppose to relax the scan-controllability by removing "independence of the initial state" as follows. A circuit C is called to be ***quasi-scan-controllable*** if for any internal state of C a transfer sequence of length k to 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 try to relax the definition of scan-observability as follows. A circuit C is called to be ***quasi-scan-observable*** if any present state (initial state) of C can be identified from the *input-output 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. 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.

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.,

$$z(t+k) = x(t) \oplus c_0 \oplus c_1x(t+1) \oplus c_2x(t+2) \oplus \ldots \oplus c_kx(t+k)$$

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.



(a) SR-quasi-equivalent I^2LF^2SR, R_3

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

(b) Symbolic simulation

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

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

(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

Figure 6. Example of SR-quasi-equivalent circuit

We can easily see 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.

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

Consider a 3-stage I^2LF^2SR, R_3, given in Figure 6(a). This I^2LF^2SR 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 Figure 6(b). Therefore, R_3 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 R_3 from any state to the desired final state ($y_1(t+3)$, $y_2(t+3)$, $y_3(t+3)$) as illustrated in Figure 6(c). Similarly, as illustrated in Figure 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.

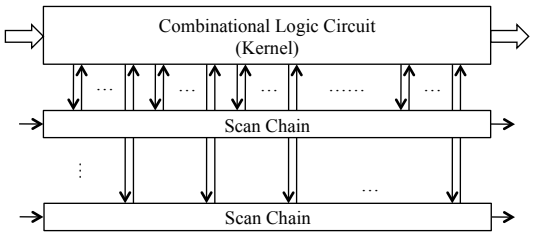
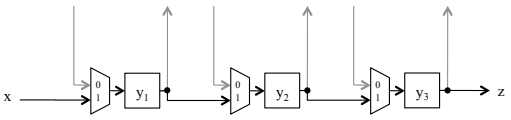
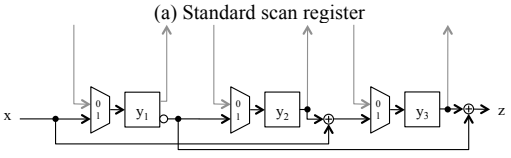


Figure 7. Scan-designed circuit



(a) Standard scan register



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

Figure 8. Standard and modified scan registers

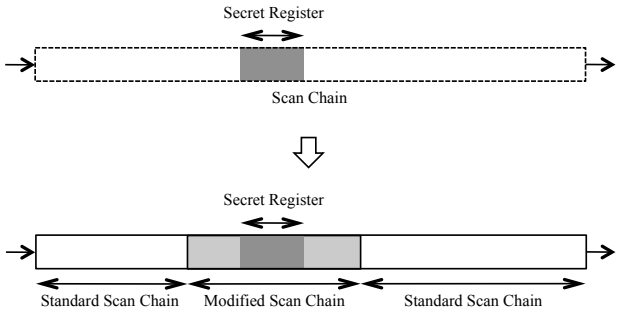


Figure 9. Replacement of scan chain by modified scan chain

4. APPLICATION TO SCAN DESIGN

A scan-designed circuit consists of a single or multiple scan chains and the remaining combinational logic circuit (*kernel*) as illustrated in Figure 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 Figure 8(a). Here, we replace the shift register with a modified SR-quasi-equivalent scan register as shown in Figure 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 Figure 9, only parts of scan chains necessary to be secure are replaced with modified SR-quasi-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. The size of modified scan chain can 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.

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.

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.

Consider two SR-quasi-equivalent circuits C_1 and C_2. We can easily see that *C_1 and C_2 have the same characteristic coefficient if and only if they are functionally equivalent.* Suppose that C_1 and C_2 have different structures but the same characteristic coefficient. Then, we cannot distinguish C_1 and C_2 merely from the input/output relation because they are functionally equivalent. Therefore, 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 (though it might be time-consuming and the complexity increases exponentially in the worst case).

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.

TABLE II. CARDINALITY OF EACH EQUIVALENT CLASS IN SR-QUASI-EQUIVALENTS OBTAINED BY ANALYSIS

EQUIVALENT CLASS	I^2SR	LF^2SR	I^2LF^2SR	I^2LFSR	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 ~ 01…11	0 ~ 0	$2^{K(K-1)/2}$ ~ $2^{K(K-1)/2}$	$2^{K(K-1)/2}(2^K-1)$ ~ $2^{K(K-1)/2}(2^K-1)$	0 ~ 0	0 ~ 0	$2^{K(K+1)/2}$ ~ $2^{K(K+1)/2}$
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 ~ 11…11	0 ~ 0	0 ~ 0	$2^{K(K-1)/2}2^K$ ~ $2^{K(K-1)/2}2^K$	0 ~ 0	0 ~ 0	$2^{K(K+1)/2}$ ~ $2^{K(K+1)/2}$
TOTAL	$2^{K+1}-1$	$2^{K(K+1)/2}-1$	$(2^{K(K+1)/2}-1)(2^{K+1}-1)$	$(2^{K(K-1)/2}-1)(2^{K+1}-1)$	$2^{K(K-1)/2}-1$	

The security level of the secure scan architecture based on those SR-quasi-equivalents is determined by the probability that an attacker can identify 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 identify 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.

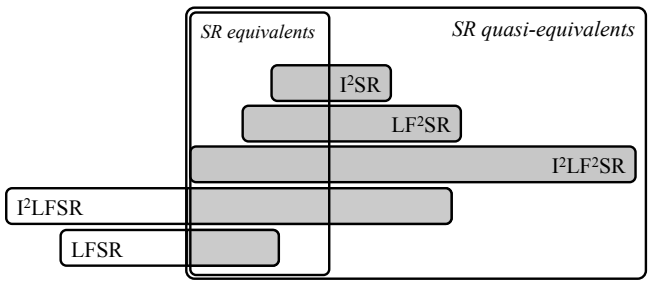


Figure 10. Covering relation among classes

The cardinality of each equivalent class in five types of linear structured circuits (I^2SR, LF^2SR, I^2LF^2SR, I^2LFSR, LFSR) is summarized in Table II. The second row is the equivalent class of the characteristic coefficient 00…00, and this is the same as the SR-equivalents (see Table I). 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 I^2SR, LF^2SR, and I^2LF^2SR (see Table I). This means any circuit of type I^2SR, LF^2SR, and I^2LF^2SR is SR-quasi-equivalent. On the other hand, as for I^2LFSR 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 [15, 16], we reported a program called SREEP (Shift Register Equivalents Enumeration and Synthesis Program).

TABLE III. CARDINALITY OF EACH EQUIVALENT CLASS FOR K=4 OBTAINED BY SREEP

	I^2SR	LF^2SR	I^2LF^2SR	I^2LFSR	LFSR	TOTAL
00000	15	63	945	945	63	2,031
00001 ~ 01111	0 ~ 0	64 ~ 64	960 ~ 960	0 ~ 0	0 ~ 0	1,024 ~ 1,024
10000	16	0	1,008	1,008	0	2,032
10001 ~ 11111	0 ~ 0	0 ~ 0	1,024 ~ 1,024	0 ~ 0	0 ~ 0	1,024 ~ 1,024
TOTAL	31	1023	31,713	1,953	63	

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 III shows the results obtained by SREEP. The theoretical values obtained by substituting 4 for k for Table II coincides with the actual values in Table III obtained by SREEP [18].

The probability that an attacker can identify the structure of an SR-quasi-equivalent circuit in an equivalent class approximates to the reciprocal of the cardinality of the class. In Table II, they are $O((2^k)^2)$ except $O(2^k)$ for I^2SR. Hence, the number of indistinguishable SR-quasi-equivalent circuits grows much more rapidly than exponentially and hence they are very secure.

From Tables I and II, for each class of linear structured circuits (I^2SR, LF^2SR, I^2LF^2SR, I^2LFSR, LFSR), we have Table IV 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 Tables II and IV, we have the covering relation among five classes of linear structured circuits (I^2SR, LF^2SR, I^2LF^2SR, I^2LFSR, LFSR), and SR-equivalents and SR-quasi-equivalents as illustrated in Figure 10.

From Figure 10, we can see all the circuits in I^2SR, LF^2SR, and I^2LF^2SR 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.

TABLE IV. 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
I^2SR	$2^{K+1}-1$	$2^{K}-1$	$2^{K+1}-1$
LF^2SR	$2^{K(K+1)/2}-1$	$2^{K(K-1)/2}-1$	$2^{K(K+1)/2}-1$
I^2LF^2SR	$(2^{K(K+1)/2}-1)(2^{K+1}-1)$	$(2^{K(K-1)/2}-1)(2^{K}-1)$	$(2^{K(K+1)/2}-1)(2^{K+1}-1)$
I^2LFSR	$(2^{K(K+1)/2}-1)(2^{K+1}-1)$	$(2^{K(K-1)/2}-1)(2^{K}-1)$	$(2^{K(K-1)/2}-1)(2^{K+1}-1)$
LFSR	$2^{K(K+1)/2}-1$	$2^{K(K-1)/2}-1$	$2^{K(K-1)/2}-1$

6. CONCLUSION

In our previous work [14-17], 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 [18].

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] 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.

[17] 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.

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