IEICE TRANS. INF. & SYST., VOL.E100–D, NO.9 SEPTEMBER 2017

LETTER

Synthesis and Enumeration of Generalized Shift Registers for Strongly Secure SR-Equivalents

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

SUMMARY In our previous work, we introduced new concepts of secure scan design; *shift register equivalent circuits* (*SR-equivalents*, for short) and *strongly secure circuits*, and also introduced *generalized shift registers* (*GSRs*, for short) to apply them to secure scan design. In this paper, we combine both concepts of SR-equivalents and strongly secure circuits and apply them to GSRs, and consider the synthesis problem of strongly secure SR-equivalents using GSRs. We also consider the enumeration problem of GSRs that are strongly secure and SR-equivalent, i.e., the cardinality of the class of strongly secure SR-equivalent GSRs to clarify the security level of the secure scan architecture.

key words: *design-for-testability, scan design, generalized feedback/feed-forward shift registers, security, scan-based side-channel attack*

1. Introduction

Scan design is a powerful design-for-testability (DFT) technique that warrants high controllability and observability over a chip and yields high fault coverage [1]. However, this also accommodates reverse engineering, which contradicts security. There is a demand to protect secrete data from side-channel attacks and other hacking schemes. Hence, it is important to find an efficient DFT approach that satisfies both security and testability. Various approaches to secure scan design have been reported [2]. 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 [3], [4]. In [4], we considered a scan-based side-channel attack with reset called *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 [3], [4], linear structured circuits were considered. We then expanded them into non-linear structured circuits and introduced two classes of *generalized shift registers* (*GSRs*, for short) which are *generalized feed-forward shift registers* (*GF*^{2}*SRs*, for short) [5], [6] and *generalized feedback shift registers* (*GFSRs*, for short) [7], to consider their application to secure scan design.

In [6], we introduced a more secure concept called *strong security* such that no internal state of strongly secure circuits leaks out, and presented how to design such strongly secure GSRs (GF^{2}SRs [6] and GFSRs [7]). In [8], we considered the synthesis problem of SR-equivalent GSRs (GF^{2}SRs and GFSRs), i.e., how to modify a given GSR to an SR-equivalent GSR. We also clarified the cardinality of each class of SR-equivalent GF^{2}SRs and GFSRs to estimate the security level [8].

SR-equivalent circuits have the property suited for scan chains, i.e., the input sequence applied to a k-stage SR-equivalent circuit appears at the output after k clock cycles, and hence any test sequence can be easily propagated through the SR-equivalent circuit to other parts of scan chains without modifying the sequence [3], [4]. So, it is important to consider such circuits that are both strongly secure and SR-equivalent in order to design secure and testable scan chains. In this paper, combining both concepts of SR-equivalents and strongly secure circuits, we apply them to GSRs (GF^{2}SRs and GFSRs), and consider the synthesis problem of GF^{2}SRs and GFSRs that are strongly secure and SR-equivalent. We also consider the enumeration problem of GSRs (GF^{2}SRs and GFSRs) that are strongly secure and SR-equivalent. We clarify the cardinality of each class of strongly secure and SR-equivalent GF^{2}SRs/GFSRs to clarify the security level of each secure scan architecture.

2. SR-Equivalents and Generalized Shift Registers

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. C 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 (a) illustrates an example of 3-stage SR-equivalent circuit R_1. The table in Fig. 3 (b) 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

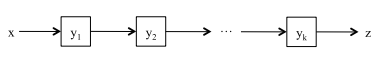


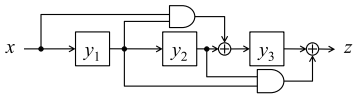
Fig. 1 k-stage shift register SR.

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

Manuscript received April 15, 2017.
Manuscript revised May 11, 2017.
Manuscript publicized May 26, 2017.

[†]The author is with Osaka Gakuin University, Suita-shi, 564–8511 Japan.
[††]The author is with Akita University, Akita-shi, 010–8502 Japan.
a) E-mail: fujiwara@ogu.ac.jp

DOI: 10.1587/transinf.2017EDL8081

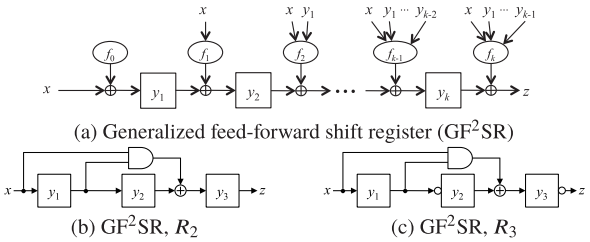


(a) SR-equivalent circuit R_1.

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

(b) Behavior of R_1 by symbolic simulation.

Fig. 3 Example of SR-equivalent circuit.



(a) Generalized feed-forward shift register (GF^{2}SR)

(b) GF^{2}SR, R_2 (c) GF^{2}SR, R_3

Fig. 4 Generalized feed-forward shift register (GF^{2}SR).

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

Fig. 5 Symbolic simulation of R_3.

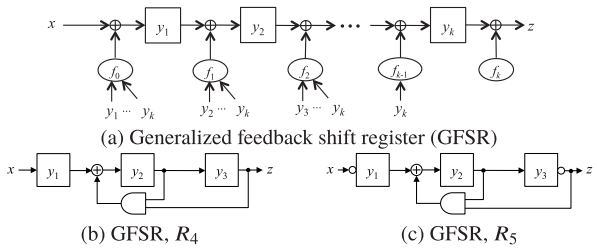
at z after $k = 3$ clock cycles, and hence the circuit is SR-equivalent. Although the input/output behavior of R_1 is the same as that of the 3-stage shift register, the internal state behavior of R_1 is different from the shift register. Therefore, without the information on the structure of R_1 one 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*.

Figure 4 (a) shows a class of *generalized shift registers* (*GSR*) called *generalized feed-forward shift registers* (*GF^{2}SR*). In this figure, $f_0, f_1, \cdots, f_k$ are arbitrary logic functions. Figures 4 (b) and (c) show examples of 3-stage GF^{2}SRs, R_2 and R_3. Generally, for any GF^{2}SR with k flip-flops, the output z at time $t + k$ behaves in accordance with the following equation.

$$z(t+k) = x(t) \oplus f(x(t+1), x(t+2), \cdots, x(t+k))$$

Consider a 3-stage GF^{2}SR, R_3, given in Fig. 4 (c). By using symbolic simulation, we can obtain the output $z(t + 3) = x(t) \oplus x(t + 2)x(t + 1)$ as shown in Fig. 5.

Figure 6 (a) shows another class of generalized shift registers called *generalized feedback shift registers* (*GFSR*). Figures 6 (b) and (c) show examples of 3-stage GFSRs, R_4 and R_5.



(a) Generalized feedback shift register (GFSR)

(b) GFSR, R_4 (c) GFSR, R_5

Fig. 6 Generalized feedback shift register (GFSR).

3. Security of Generalized Shift Registers

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 extended scan chains.* Based on this assumption, we consider the security to prevent scan-based attacks.

In [5]–[7], we introduced a concept called *scan-secure* as follows. 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. The security level of the secure scan architecture based on those GSRs is determined by the probability that an attacker can identify the structure of the GSR used in the circuit, and hence the attack probability approximates to the reciprocal of the cardinality of the class of GSRs.

Although the structure of a GSR is hard to be identified, it may not be secure if part of the contents of the GSR leak out. To avoid such leakage, we consider more secure scan registers whose contents never leak out. First, we define several concepts in the following. Consider a circuit C with a single input, a single output, and k flip-flops. C is called to be *scan-in secure* 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, such that the transfer sequence is always different from that of a k-stage shift register. C is called to be *scan-out secure* if any present state (initial state) of C can be identified only from the *input-output sequence* (of length k) and the connection information of C, such that the output sequence is always different from that of a k-stage shift register. C is called to be *strongly secure* if C is scan-in secure and scan-out secure.

4. Synthesis Problem for Strongly Secure SR-Equivalent GSRs

In our previous work, we presented a method for making a given GSR strongly secure [6], [7], and a method for making it SR-equivalent [8].

Here let us now consider the problem of modifying a

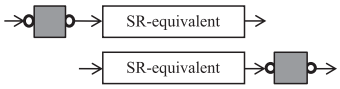


Fig. 7 Adding a dummy FF with two NOT gates.

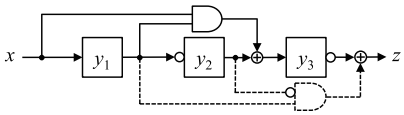


Fig. 8 Modified SR-equivalent GF^{2}SR, R_6.

given GSR (GF^{2}SR or GFSR) into a strongly secure SR-equivalent one. We can consider two approaches. One approach (Method A) is to make a given GSR SR-equivalent first and then to make it strongly secure. The other approach (Method B) is to make a given GSR strongly secure first and then to make it SR-equivalent.

The first approach (Method A) consists of the following three steps.

Method A: (1) Check if a given GSR is SR-equivalent or not, by symbolic simulation. If it is not SR-equivalent, make it SR-equivalent by adding feed-forward or feedback logic (using the method in [8]).
(2) Check if the modified GSR is strongly secure or not. If it is not strongly secure, make it strongly secure (scan-in secure and scan-out secure) by adding NOT gates and a dummy FF if necessary (using the method in [6], [7]).
(3) Check if the modified GSR is still SR-equivalent. If it is not SR-equivalent, make it SR-equivalent without losing strong security by adding NOT gates and a dummy FF if necessary.

Note that step (3) is necessary because it may happen that the modified GSR is not SR-equivalent anymore due to the addition of NOT gates at step (2).

However, there is a straightforward method for making an SR-equivalent GSR strongly secure without violating the SR-equivalence so that step (3) can be skipped. At step (2), we add a dummy FF with two NOT gates to the input or the output of the SR-equivalent GSR as illustrated in Fig. 7. Obviously, the dummy FF with two NOT gates makes the circuit strongly secure, and the whole circuit is still SR-equivalent.

Next, let us consider the second approach (Method B) which consists of the following two steps.

Method B: (1) Check if a given GSR is strongly secure or not, by symbolic simulation. If it is not strongly secure, make it strongly secure (scan-in secure and scan-out secure) by adding NOT gates and a dummy FF if necessary (using the method in [6], [7]).
(2) Check if the modified GSR is SR-equivalent or not, by symbolic simulation. If it is not SR-equivalent, make it SR-equivalent by adding feed-forward or feedback logic (using the method in [8]).

Here, note that the modified SR-equivalent GSR after step (2) is still strongly secure. To see this, let us consider the following.

Consider an SR-equivalent circuit C with a single input x, a single output z, and k flip-flops $y_1, y_2, \cdots, y_k$. Let $x(t)$ and $z(t)$ be the input value and the output value at time t, and let $(y_1(t), y_2(t), \cdots, y_k(t))$ be the state of FFs at time t. Suppose an input sequence $x(t), x(t+1), \cdots, x(t+k-1)$ is applied to C. After this input sequence is applied, the state of FFs becomes $(y_1(t+k), y_2(t+k), \cdots, y_k(t+k))$. The output sequence of length k after time $t+k$ are $z(t+k), z(t+k+1), \cdots, z(t+2k-1)$, where $z(t+k) = x(t), z(t+k+1) = x(t+1), \cdots, z(t+2k-1) = x(t+k-1)$ because C is SR-equivalent.

If C is not scan-in secure, there exists an input sequence $x(t), x(t+1), \cdots, x(t+k-1)$ such that $x(t) = y_k(t+k), \cdots, x(t+k-1) = y_1(t+k)$. Hence, $z(t+k) = y_k(t+k), \cdots, z(t+2k-1) = y_1(t+k)$ which implies C is not scan-out secure. Similarly, we can see that if C is not scan-out secure, C is not scan-in secure. Then, we have the following theorem.

Theorem 1: For any SR-equivalent circuit C, C is scan-in secure if and only if C is scan-out secure.

For any GF^{2}SR, adding a feed-forward logic to the output z never violates the scan-in security. Similarly, for any GFSR, adding a feed-back logic to the input x never violates the scan-out security. Therefore, from this observation and Theorem 1, we can see that the modified SR-equivalent GSR after step (2) is still strongly secure.

As an example, consider a 3-stage GF^{2}SR, R_2, given in Fig. 4 (b). From symbolic simulation, we can see that R_2 is neither scan-in secure nor scan-out secure. So, we apply step (1) and get R_3 shown in Fig. 4 (c), which is strongly secure. From the symbolic simulation for R_3 illustrated in Fig. 5, we can see R_3 is not SR-equivalent. We then apply step (2), and get the modified circuit R_6 that is SR equivalent as shown in Fig. 8. R_6 is still strongly secure.

5. Enumeration Problem for Strongly Secure SR-Equivalent GSRs

The security level of the secure scan architecture based on a class of generalized shift registers is determined by the probability that an attacker can guess right the structure of the extended shift register used in the scan design, and hence the attack probability approximates to the reciprocal of the cardinality of the class of generalized shift registers.

In [5] and [7], we clarified the cardinality of each class of GF^{2}SRs and GFSRs.

Theorem 2 [5]: The cardinality of the class of k-stage GF^{2}SRs is $2^{(2^{(k+1)}-1)} - 1$.

Theorem 3 [7]: The cardinality of the class of k-stage GFSRs is $2^{(2^{(k+1)}-1)} - 1$.

In [8], we clarified the cardinality of each class of k-stage GF^{2}SRs and GFSRs that are SR-equivalent.

Theorem 4 [8]: The cardinality of the class of k-stage SR-equivalent GF^{2}SRs is $2^{(2^k-1)}-1$.
Theorem 5 [8]: The cardinality of the class of k-stage SR-equivalent GFSRs is $2^{(2^k-1)}-1$.

Here, let us consider the cardinality of each class of k-stage GF^{2}SRs and GFSRs that are SR-equivalent and strongly secure. First, we have the following lemma for GF^{2}SRs.

Lemma 1: The total number of k-stage scan-in secure GF^{2}SRs that are SR-equivalent is equal to the total number of $(k-1)$-stage scan-in secure GF^{2}SRs.

Proof: For each $(k-1)$-stage scan-in secure GF^{2}SR, add one flip-flop to the right end and make it k-stage scan-in secure GF^{2}SR. If this k-stage scan-in secure GF^{2}SR is not SR-equivalent, modify it to be SR-equivalent by adding a feed-forward logic function to the output of the GF^{2}SR. Note that the feed-forward logic function to be added is uniquely determined, because adding different feed-forward function implies different output function. Also, this addition does not violate scan-in security, i.e., the augmented GF^{2}SR is SR-equivalent and scan-in secure. Therefore, the number of generated k-stage scan-in secure GF^{2}SRs that are SR-equivalent is equal to the total number of $(k-1)$-stage scan-in secure GF^{2}SRs.

On the other hand, for any k-stage scan-in secure GF^{2}SR that is SR-equivalent, there exists a $(k-1)$-stage scan-in secure GF^{2}SR such that the k-stage scan-in secure GF^{2}SR is obtained by adding one flip-flop to the right end of the $(k-1)$-stage scan-in secure GF^{2}SR and by adding a feed-forward logic function if necessary. Therefore, the total number of k-stage scan-in secure GF^{2}SRs that are SR-equivalent is equal to the total number of $(k-1)$-stage scan-in secure GF^{2}SRs. □

Next, let us consider the total number of k-stage scan-in secure GF^{2}SRs.

Lemma 2: The total number of k-stage scan-in secure GF^{2}SRs is at least half of the total number of k-stage GF^{2}SRs.

Proof: The class of k-stage GF^{2}SRs can be partitioned into two equal parts; one is a set of GF^{2}SRs with NOT gate at the input side and the other is a set of GF^{2}SRs without NOT gate at the input side. Then, it is obvious that all the k-stage GF^{2}SRs with NOT gate at the input side are scan-in secure. Hence, the theorem holds. □

From Lemmas 1 and 2, we have the following theorem.

Theorem 6: The total number of k-stage scan-in secure GF^{2}SRs that are SR-equivalent is at least half of the total number of $(k-1)$-stage GF^{2}SRs.

From this theorem and Theorem 1, we have the following theorem.

Theorem 7: The total number of k-stage strongly secure GF^{2}SRs that are SR-equivalent is at least half of the total number of $(k-1)$-stage GF^{2}SRs.

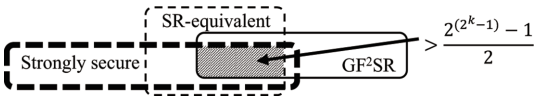


Fig. 9 Cover relation and cardinality.

From this theorem and Theorem 2, we have the following theorem.

Theorem 8: The cardinality of the class of k-stage GF^{2}SRs that are SR-equivalent and strongly secure is larger than $(2^{(2^k-1)}-1)/2$.

Figure 9 illustrates the cover relation and cardinality in Theorem 8.

So far, we have considered the class of GF^{2}SRs. Similarly to GF^{2}SR, we can prove the following lemmas and theorems for GFSRs.

Lemma 3: The total number of k-stage scan-out secure GFSRs that are SR-equivalent is equal to the total number of $(k-1)$-stage scan-out secure GFSRs.

Lemma 4: The total number of k-stage scan-out secure GFSRs is at least half of the total number of k-stage GFSRs.

Theorem 9: The total number of k-stage scan-out secure GFSRs that are SR-equivalent is at least half of the total number of $(k-1)$-stage GFSRs.

Theorem 10: The cardinality of the class of k-stage GFSRs that are SR-equivalent and strongly secure is larger than $(2^{(2^k-1)}-1)/2$.

6. Conclusion

In this paper, we considered the synthesis problem of GF^{2}SRs and GFSRs that are strongly secure and SR-equivalent, i.e., how to modify a given GSR to an SR-equivalent and strongly secure GSR. We also considered the enumeration problem of GSRs (GF^{2}SRs and GFSRs) that are strongly secure and SR-equivalent, and clarified the cardinality of each class of strongly secure and SR-equivalent GF^{2}SRs/GFSRs to estimate the security level of each secure scan architecture.

References

[1] H. Fujiwara, Logic Testing and Design for Testability, The MIT Press, 1985.
[2] J.D. Rolt, A. Das, G.D. Natale, M.-L. Flottes, B. Rouzeyre, and I. Verbauwhede, "Test versus security: Past and present," IEEE Trans. Emerg. Topics Comput., vol.2, no.1, pp.50–62, 2014.
[3] 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.
[4] K. Fujiwara, H. Fujiwara, and H. Tamamoto, "Differential behavior equivalent classes of shift register equivalents for secure and testable scan design," IEICE Trans. Inf. & Syst., vol.E94-D, no.7, pp.1430–1439, July 2011.

[5] K. Fujiwara and H. Fujiwara, "Generalized feed-forward shift registers and their application to secure scan design," IEICE Trans. Inf. & Syst. vol.E96-D, no.5, pp.1125–1133, May 2013.
[6] H. Fujiwara and K. Fujiwara, "Strongly secure scan design using generalized feed forward shift registers," IEICE Trans. Inf. & Syst., vol.E98-D, no.10, pp.1852–1855, Oct. 2015.
[7] H. Fujiwara and K. Fujiwara, "Properties of generalized feedback shift registers for secure scan design," IEICE Trans. Inf. & Syst., vol.E99-D, no.4, pp.1255–1258, April 2016.
[8] H. Fujiwara and K. Fujiwara, "Realization of SR-equivalents using generalized shift registers for secure scan design," IEICE Trans. Inf. & Syst., vol.E99-D, no.8, pp.2182–2185, Aug. 2016.