Realization of SR-Equivalents Using Generalized Shift Registers for Secure Scan Design

Hideo FUJIWARA††, Fellow and Katsuya FUJIWARA††, Member

SUMMARY We reported a secure scan design approach using shift register equivalents (SR-equivalents, for short) that are functionally equivalent but not structurally equivalent to shift registers [10] and also introduced generalized shift registers (GSRs, for short) to apply them to secure scan design [11]–[13]. In this paper, we combine both concepts of SR-equivalents and GSRs and consider the synthesis problem of SR-equivalent GSRs, i.e., how to modify a given GSR to an SR-equivalent GSR. We also consider the enumeration problem of SR-equivalent GFSRs, i.e., the cardinality of the class of SR-equivalent GFSRs 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

Both testability and security of a chip have become fundamental to ensuring its reliability and protection from invasion to access important information. 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 provides high controllability and observability over a chip and yields high fault coverage [1]. However, it also allows reverse engineering, which contradicts security. There is a demand to protect secret data from side-channel attacks and other hacking schemes [2]. 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 [3]–[9]. 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 [10], where 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 (GF²SRs, for short) [11], [12] and generalized feedback shift registers (GFSRs, for short) [13], to consider their application to secure scan design.

As for testability, the class of SR-equivalents is better than GSRs. On the other hand, as for security, the class of GSRs is better than SR-equivalents. In this paper, combining both concepts of SR-equivalents and GSRs, we propose the class of SR-equivalent GSRs for secure and testable scan design. We consider the synthesis problem of SR-equivalent GSRs (GF²SRs and GFSRs), i.e., how to modify a given GSR to an SR-equivalent GSR. We also clarify the cardinality of each class of SR-equivalent GF²SRs and GFSRs to estimate the security level.

2. SR-Equivalents and GSRs

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 $z$ after $k$ clock cycles, the circuit $C$ behaves as if it is a $k$-stage shift register.

A circuit $C$ with a single input $x$, a single output $z$, and $k$ flip-flops is called functionally equivalent to a $k$-stage shift register (or SR-equivalent) if the input value applied to $x$ at any time $t$ appears at $z$ after $k$ clock cycles, i.e., $z(t+k) = x(t)$ for any time $t$.

Figure 3(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 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.

In [11], [12], we introduced a class of generalized shift registers called generalized feed-forward shift registers...
3. Synthesis Problem for SR-Equivalent GSRs

Let us consider the problem of modifying a given GSR (GF<sup>2</sup>SR or GFSR) into an SR-equivalent. First, consider a k-stage GF<sup>2</sup>SR shown in Fig. 4 (a). By symbolic simulation, we can obtain the output \( z \) at time \( t + k \) behaves in accordance with the following equation.

\[
 z(t + k) = x(t) \oplus f(x(t + 1), x(t + 2), \ldots, x(t + k))
\]

Consider a 3-stage GF<sup>2</sup>SR, \( R_3 \), given in Fig. 4 (c). By using symbolic simulation, we can obtain the output \( z(t + 3) = x(t) \oplus y_1(t) y_2(t) \) as shown in Fig. 5.

In [13], we introduced another class of \textit{generalized shift registers called generalized feedback shift registers (GFSR)}, shown in Fig. 6 (a). Figures 6 (b) and (c) show examples of 3-stage GFSRs, \( R_4 \) and \( R_5 \). In [13], we also proposed \textit{strongly secure GFSR}. \( R_5 \) is strongly secure. The difference between GFSR and GF<sup>2</sup>SR is whether the structure is feedback type or feed-forward type. From the feedback structure of Fig. 6 (a), we can see that for any GFSR with \( k \) flip-flops, the output \( z \) at time \( t + k \) behaves in accordance with the following equation.

\[
 z(t + k) = x(t) \oplus f(y_1(t), y_2(t), \ldots, y_k(t))
\]

Consider a 3-stage GFSR, \( R_5 \), given in Fig. 6 (c). By using symbolic simulation, we can obtain the output \( z(t + 3) = x(t) \oplus y_1(t) y_2(t) \) as shown in Fig. 7.
To realize this modification on the given GF 2SR, we need to express the added logic function \( g \) by a logic function \( f \) of variables \( x(t+k), y_1(t+k), y_2(t+k), \ldots, y_k(t+k) \) as follows.

\[
f(x(t+1), x(t+2), \ldots, x(t+k)) = g(x(t+k), y_1(t+k), y_2(t+k), \ldots, y_k(t+k))
\]

This can be obtained from the outcome of symbolic simulation. Then, we add the feed-forward logic \( f \) to the output \( z \) of the circuit. The modified GF 2SR becomes SR-equivalent. Note that if the given GF 2SR has only one feedback logic to the output \( z \), the logic function is equal to \( g(x, y_1, y_2, \ldots, y_k) \) and hence the modified GF 2SR becomes a \( k \)-stage shift register. We have the following theorem.

**Theorem 1:** Any \( k \)-stage GF 2SR can be modified to a GF 2SR that is SR-equivalent by adding a feed-forward logic function to the output.

As an example, consider a 3-stage GF 2SR, \( R_3 \), given in Fig. 4 (c). By symbolic simulation illustrated in Fig. 5, we obtain \( z(t+3) = x(t) \oplus x(t+2) x(t+1) \). We also get \( x(t+2) = y_1(t+3) \) and \( x(t+1) = y_2(t+3) \). Hence, we can see

\[
z(t+3) = x(t) \oplus x(t+2) x(t+1) = x(t) \oplus y_1(t+3) y_2(t+3)
\]

Then, we add the feed-forward logic \( g(y_1, y_2) = y_1 y_2 \) to the output \( z \) of the circuit as shown in Fig. 8. The modified circuit \( R_4 \) is SR equivalent.

Next, let us consider a \( k \)-stage GFSR shown in Fig. 6 (a). By symbolic simulation, we can get the output \( z \) at time \( t+k \) as follows.

\[
z(t+k) = x(t) \oplus f(y_1(t), y_2(t), \ldots, y_k(t))
\]

To change this equation into \( z(t+k) = x(t) \), we add function \( f(y_1(t), y_2(t), \ldots, y_k(t)) \) to this equation as follows.

\[
z(t+k) = x(t) \oplus f(y_1(t), y_2(t), \ldots, y_k(t)) \oplus f(y_1(t), y_2(t), \ldots, y_k(t)) = x(t)
\]

To do so, we modify the circuit by adding the feedback logic \( f(y_1, y_2, \ldots, y_k) \) to the input \( x \). The modified GFSR is SR-equivalent. Note that if the given GFSR has only one feedback logic to the input \( x \), the logic function is equal to \( f(y_1(t), y_2(t), \ldots, y_k(t)) \) and hence the modified GFSR becomes a \( k \)-stage shift register. We have the following theorem.

**Theorem 2:** Any \( k \)-stage GFSR can be modified to a GFSR that is SR-equivalent by adding a feedback logic function to the input.

As an example, consider a 3-stage GFSR, \( R_5 \), given in Fig. 6 (c). By symbolic simulation illustrated in Fig. 7, we get \( z(t+3) = x(t) \oplus y_1(t)y_2(t) \). Then, we modify \( R_5 \) by adding the feedback logic \( y_1y_2 \), to the input \( x \) as shown in Fig. 9. The modified circuit \( R_7 \) is SR equivalent.

**4. Security of SR-Equivalent GF 2SR/GFSR**

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 input, 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.

A circuit \( C \) with a single input, a single output, and \( k \) flip-flops is called scan-secure if the attacker cannot determine the structure of \( C \).

We have already reported that SR-equivalents, GF 2SRs, and GFSRs are scan-secure in [10]–[12], and [13], respectively. The security level of the secure scan architecture based on a class of extended 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 extended shift registers.

In [11] and [13], we clarified the cardinality of each class of GF 2SRs and GFSRs.

**Theorem 3** [11]: The cardinality of the class of \( k \)-stage GF 2SRs is \( 2^{2^k - 1} - 1 \).

**Theorem 4** [13]: The cardinality of the class of \( k \)-stage GFSRs is \( 2^{2^k - 1} - 1 \).

Here, let us consider the cardinality of each class of \( k \)-stage GF 2SRs and GFSRs that are SR-equivalent. First, we have the following theorem for GF 2SRs.

**Theorem 5**: The total number of \( k \)-stage GF 2SRs that are SR-equivalent is equal to the total number of \((k-1)\)-stage GF 2SRs.
Proof: For each \((k-1)\)-stage GF\(^2\)SR, add one flip-flop to the right end and make it \(k\)-stage GF\(^2\)SR. If this \(k\)-stage GF\(^2\)SR is not SR-equivalent, modify it to be SR-equivalent by using Theorem 1, i.e., 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. Therefore, the number of generated \(k\)-stage GF\(^2\)SRs that are SR-equivalent is equal to the total number of \((k-1)\)-stage GF\(^2\)SRs.

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

From Theorems 3 and 5, we can see that the following theorem holds.

**Theorem 6:** The cardinality of the class of \(k\)-stage SR-equivalent GF\(^2\)SRs is \(2^{(2^{(k-1)}-1)}\).

Similarly, we have the following theorem for GFSRs.

**Theorem 7:** The total number of \(k\)-stage GFSRs that are SR-equivalent is equal to the total number of \((k-1)\)-stage GF-SRs.

From Theorems 4 and 7, we can see that the following theorem holds.

**Theorem 8:** The cardinality of the class of \(k\)-stage SR-equivalent GFSRs is \(2^{(2^{(k-1)}-1)}\).

## 5. Conclusion

In our previous work, we reported a secure and testable scan design approach by using SR-equivalents [10], *generalized feed-forward shift registers* (GF\(^2\)SRs) [11], [12], and *generalized feedback shift registers* (GFSRs) [13]. In this paper, combining both concepts of SR-equivalents and generalized shift registers (GSRs), we proposed the class of SR-equivalent GSRs for secure and testable scan design. 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.

**References**