SREEP: Shift Register Equivalents Enumeration and Synthesis Program for Secure Scan Design

Katsuya Fujiwara¹, Hideo Fujiwara², Marie Engeline J. Obien² and Hideo Tamamoto¹

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

² Graduate School of Information Science
   Nara Institute of Science and Technology
   Nara 630-0192, JAPAN
   {fujiwara, obien-j}@is.naist.jp

Abstract—We reported a secure scan design approach using extended shift registers that are functionally equivalent but not structurally equivalent to shift registers. The security level of the secure scan architecture based on those shift register equivalents is determined by the probability that an attacker can identify the configuration of the shift register equivalent used in the circuit, and hence the attack probability approximates to the reciprocal of the cardinality of the class of shift register equivalents. In this paper, we clarify the cardinality of each class of shift register equivalents from several linear structured circuits and the cardinality of the whole class of shift register equivalents. We also consider the enumeration problem of shift register equivalents and the synthesis problem of desired shift register equivalents. A program called SREEP (Shift Register Equivalents Enumeration and Synthesis Program) is presented to solve those problems.

Keywords - scan design; shift register equivalents; security; testability; cardinality; enumeration.

I. INTRODUCTION

Both testability and security of a chip have 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 [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 [3-11]. All the approaches except [8,11] add extra hardware outside of the registers.

In [11], we reported a secure and testable scan design approach by using extended shift registers that are functionally equivalent but not structurally equivalent to shift registers. This approach is only to replace the original scan registers with the modified extended scan register, and hence requires little area overhead and no performance overhead with respect to normal operation. The security level of the secure scan architecture based on those shift register equivalents is determined by the probability that an attacker can identify the configuration of the shift register equivalent used in the circuit, and hence the attack probability approximates to the reciprocal of the cardinality of the class of shift register equivalents. In this paper, we clarify the cardinality of each class of shift register equivalents from several linear structured circuits and the cardinality of the whole class of shift register equivalents. We also consider the enumeration problem of shift register equivalents and the synthesis problem of desired shift register equivalent. A program called SREEP (Shift Register Equivalents Enumeration and Synthesis Program) is presented to solve those problems.

II. SHIFT REGISTER EQUIVALENTS

Definition 1: A circuit whose state transition graph is isomorphic to that of a k-stage shift register is called a k-stage extended shift register.

Definition 2: A circuit C is called functionally equivalent to a k-stage shift register (or SR-equivalent) if the state transition graph of C is isomorphic to that of the shift register and the input/output assignment is the same as that of the shift register. The state assignment is not necessarily the same as that of the shift register. (see Fig. 1(b)).

In the next section, we consider the following seven types of linear circuits that can realize extended shift registers: inversion inserted shift registers (I'SR), linear feed-forward shift registers (LF'SR), linear feedback shift registers (LFSR), linear feed-forward shift registers with inversion (LF'SR+I'SR), linear feedback shift registers with inversion (LFSR+I'SR), shift registers with linear feed-forward and feedback (LF²SR+LFSR), and shift registers with linear feed-forward, linear feedback and inversion (LF²SR+LFSR+I'SR) (see Fig. 2).
The total number of k-stage SRs is \(2^{k(k+1)/2}\). The cardinality of the class of k-stage LF\(^2\)SRs (LFSRs) is \(2^{k(k+1)/2}\). The cardinality of the class of k-stage LF\(^2\)SRs (LFSRs) that are SR-equivalent is \(2^{k(k+1)/2}\).

C. LF\(^2\)SR+I\(^2\)SR and LFSR+I\(^2\)SR

Similar to Theorems 2 and 3, we have the following theorems.

Theorem 5: Any LF\(^2\)SR+I\(^2\)SR can be modified to an LF\(^2\)SR+I\(^2\)SR that is SR-equivalent to the k-stage shift register by manipulating the linear sum of the output and by adding inverters.

Theorem 6: Any LFSR+I\(^2\)SR can be modified to an LFSR+I\(^2\)SR that is SR-equivalent to the k-stage shift register by manipulating the linear sum of the input and by adding inverters.

Regarding the cardinality of linear sum of the input and linear sum of the output.

Theorem 7: The cardinality of the class of k-stage LF\(^2\)SR+I\(^2\)SRs (LFSR+I\(^2\)SRs) is \(2^{k(k+1)/2} - 1\). The cardinality of the class of k-stage LF\(^2\)SR+I\(^2\)SRs (LFSR+I\(^2\)SRs) that are SR-equivalent is \(2^{k(k+1)/2} - 1\).

D. LF\(^2\)SR+LFSR and LFSR+LFSR+I\(^2\)SR

Theorem 8: The cardinality of the class of k-stage LF\(^2\)SR+LFSR that is SR-equivalent to the k-stage shift register by manipulating the linear sum of the output and by adding inverters.

Similarly, the following theorem for LFSR holds.

Theorem 3: Any LFSR can be modified to an LFSR that is SR-equivalent to the k-stage shift register by manipulating the linear sum of the input.

Let us consider the cardinality of the classes of LF\(^2\)SRs and LFSRs together with their SR-equivalents. The total number of k-stage LF\(^2\)SRs is \(2^{k(k+1)/2} - 1\). Similarly, the total number of k-stage LFSRs is \(2^{k(k+1)/2} - 1\).

For each (k-1)-stage LF\(^2\)SR, add one flip-flop to the right end and make it k-stage LF\(^2\)SR. Since this k-stage LF\(^2\)SR is not always SR-equivalent, modify it to be SR-equivalent by using Theorem 2. The number of such augmented k-stage SR-equivalent LF\(^2\)SRs is equal to the total number of (k-1)-stage LF\(^2\)SRs, and hence \(2^{k(k-1)/2} - 1\). Therefore, the total number of k-stage LF\(^2\)SRs that are SR-equivalent is \(2^{k(k-1)/2} - 1\). Similarly the total number of LFSRs that are SR-equivalent is \(2^{k(k-1)/2} - 1\).

Theorem 4: The cardinality of the class of k-stage LF\(^2\)SRs (LFSRs) is \(2^{k(k+1)/2} - 1\). The cardinality of the class of k-stage LF\(^2\)SRs (LFSRs) that are SR-equivalent is \(2^{k(k+1)/2} - 1\).

A. I\(^2\)SR

An inversion inserted shift register (I\(^2\)SR) is obtained by inserting some inversions in a shift register.

Theorem 1: Any k-stage I\(^2\)SR with even number of inversions is functionally equivalent to the k-stage shift register.

The total number of k-stage I\(^2\)SRs is \(2^{k+1}-1\). On the other hand, the total number of k-stage I\(^2\)SRs that are SR-equivalent is \(2^k-1\) from Theorem 1.

B. LF\(^2\)SR and LFSR

Theorem 2: Any LF\(^2\)SR can be modified to an LF\(^2\)SR that is SR-equivalent to the k-stage shift register by manipulating the linear sum of the output.

Consider the circuit shown in Figure 3(a), the output assignment is different from that of the shift register only when state transition occurs from states (011), (010), (110), and (111), i.e., only when \(y_2 = 1\). Hence, as shown in Figure 3(b), by adding an XOR at the output with inputs from \(y_3\) and \(y_2\) that is indicated by the broken line arrow, the output assignment of the modified LF\(^2\)SR becomes the same as that of the shift register of Figure 1(a). With this, only the state assignment is different while the input and output assignments remain the same, thus making it SR-equivalent.

Similarly, the following theorem for LFSR holds.

III. CARDINALITY OF SR-EQUIVALENTS
E. Cardinality of Whole SR-equivalents

The cardinality of each class is summarized in Table I. The covering relation among seven classes is illustrated in Figure 4. Let N(k) be the number of all k-stage SR-equivalents. SR-equivalent circuits are the circuits whose state graphs are the same as that of SR except state assignment. The number of states is $2^k$ and the number of state values is $2^k$, where k is the number of flip-flops. So, the total number of different SR-equivalent state graphs is the number of permutations to assign $2^k$ values to $2^k$ states, which is $2^{2k}$. Further, the size of each permutation (of state variables) equivalents is $k!$. Hence, the number of permutation equivalents is $2^{2k}/k!$. Therefore, we have

$$N(k) = 2^{2k}/k! - 1.$$  

Table I shows the cardinality of each class and the cardinality of SR-equivalents in each class for k-stage circuits. Table II shows the computed values. From Table II, for each class ($I^2SR$, $LF^2SR$, $LSFR$, $LF^2SR+I^2SR$ and $LSFR+I^2SR$), we can observe that the cardinality of k-stage circuits in the class is equal to the cardinality of $(k+1)$-stage SR-equivalents in the class as shown in Theorems 4 and 7.

![Image](image-url)

Figure 4. Covering relation among classes

IV. SREEP

We made a program called SREEP (Shift Register Equivalents Enumeration and Synthesis Program) to solve the enumeration and synthesis problems for SR-equivalents [13]. SREEP adopts GUI (graphical user interface) for expressing outcome by circuit diagram and table. SR-ID code is introduced to represent the structure of each extended SR uniquely. Fig. 5 shows an example of outcome by SREEP.

![Image](image-url)

V. ENUMERATION PROBLEM FOR SR-EQUIVALENTS

For each class ($I^2SR$, $LF^2SR$, $LSFR$, $LF^2SR+I^2SR$, $LSFR+I^2SR$, $LF^2SR+LSFR$, and $LF^2SR+LF^2SR+I^2SR$), we enumerated all k-stage extended SRs and identified SR-equivalents for $k=1, 2, \ldots$ and 6, in order to obtain the real number of SR-equivalents for each class.

For five classes of $I^2SR$, $LF^2SR$, $LSFR$, $LF^2SR+I^2SR$, and $LSFR+I^2SR$, the real number of SR-equivalents for $k=1, 2, \ldots$ and 6 obtained by SREEP is the same as the cardinality of SR-equivalents shown in Table II. For other two classes of $LF^2SR+LSFR$ and $LF^2SR+LF^2SR+I^2SR$ by SREEP, $k=1, 2, \ldots$ and 6 obtained by SREEP is the same as the cardinality of SR-equivalents shown in Table II. For other two classes of $LF^2SR+LSFR$ and $LF^2SR+LF^2SR+I^2SR$, Table III shows the real number of SR-equivalents and the total number of extended SRs for $k=1, 2, \ldots$ and 6 obtained by SREEP.

SREEP can generate all SR-equivalents that satisfy the given desired parameters or constraints such as type of circuit

![Image](image-url)

Figure 5. Outcome example by SREEP

### Table I. Cardinality of each class

<table>
<thead>
<tr>
<th>Class</th>
<th># of circuits in the class</th>
<th># of SR equivalents in the class</th>
</tr>
</thead>
<tbody>
<tr>
<td>$I^2SR$</td>
<td>$2^{2k} - 1$</td>
<td>$2^{2k} - 1$</td>
</tr>
<tr>
<td>$LF^2SR$</td>
<td>$2^{2k+1} - 1$</td>
<td>$2^{2k+1} - 1$</td>
</tr>
<tr>
<td>$LF^2SR+I^2SR$</td>
<td>$(2^{2k+1} - 1)(2^{2k+1} - 1)$</td>
<td>$(2^{2k+1} - 1)(2^{2k+1} - 1)$</td>
</tr>
<tr>
<td>$LSFR+I^2SR$</td>
<td>$(2^{2k+1} - 1)^2$</td>
<td>?</td>
</tr>
<tr>
<td>$LF^2SR+LSFR$</td>
<td>$(2^{2k+1} - 1)^2$</td>
<td>?</td>
</tr>
</tbody>
</table>

### Table II. Cardinality of SR-equivalents / extended SRs for $I^2SR$, $LF^2SR$, $LSFR$, $LF^2SR+I^2SR$, and $LSFR+I^2SR$

<table>
<thead>
<tr>
<th>k</th>
<th>$I^2SR$</th>
<th>$LF^2SR$</th>
<th>$LSFR$</th>
<th>$LF^2SR+I^2SR$</th>
<th>$LSFR+I^2SR$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1 / 3</td>
<td>0 / 1</td>
<td>0 / 3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>3 / 7</td>
<td>1 / 7</td>
<td>3 / 49</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>7 / 15</td>
<td>7 / 63</td>
<td>49 / 945</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>15 / 31</td>
<td>63 / 1,023</td>
<td>945 / 31,713</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>31 / 63</td>
<td>1,023 / 32,767</td>
<td>31,713 / 2,064,321</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>63 / 127</td>
<td>32,767 / 2,097,151</td>
<td>2,064,321 / 266,338,177</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Table III. Cardinality of SR-equivalents / extended SRs for $LF^2SR+LSFR$ and $LF^2SR+LF^2SR+I^2SR$ by SREEP

<table>
<thead>
<tr>
<th>k</th>
<th>$LF^2SR+LSFR$</th>
<th>$LF^2SR+LF^2SR+I^2SR$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0 / 1</td>
<td>0 / 3</td>
</tr>
<tr>
<td>2</td>
<td>0 / 49</td>
<td>0 / 343</td>
</tr>
<tr>
<td>3</td>
<td>12 / 3,969</td>
<td>84 / 59,535</td>
</tr>
<tr>
<td>4</td>
<td>905 / 1,046,529</td>
<td>13,575 / 32,442,399</td>
</tr>
<tr>
<td>5</td>
<td>198,505 / 1,073,676,289</td>
<td>6,153,655 / 67,641,606,207</td>
</tr>
<tr>
<td>6</td>
<td>180,038,401 / 4,398,042,316,801</td>
<td>11,342,419,263 / 558,551,374,233,727</td>
</tr>
</tbody>
</table>
structure, number of stages, upper and lower limits of the number of feed-forwards/feedbacks, etc.

![Diagram of scan chain](image)

### Figure 6. Long scan chain

For \( LF^2SR + 1^2SR \) or \( LFSR + 1^2SR \), not only feed-forwards or feedbacks are added but also a NOT gate to \( z \) or \( x \), if necessary.

### VII. CONCLUSIONS

The security level for the secure scan design based on SR-equivalents is related to the attack probability which approximates to the reciprocal of the cardinality of the class of SR-equivalents. In this paper, we clarified the cardinality of each class of SR-equivalents from several linear structured circuits and the cardinality of the whole class of SR-equivalents, and presented the real number of SR-equivalents by enumeration for up to 6-stage SR-equivalents. We also considered the enumeration problem of SR-equivalents and the synthesis problem of desired SR-equivalents. A program called SREEP (Shift Register Equivalents Enumeration and Synthesis Program) was presented to solve those problems.

### REFERENCES