SCIENCE CHINA
Information Sciences

• RESEARCH PAPER •

September 2024, Vol. 67, Iss. 9, 192203:1–192203:12
https://doi.org/10.1007/s11432-023-4044-8

Nonsingularity of grain-like cascade feedback shift registers subject to fault attacks

Haitao LI*, Zhaoqi LIU & Wenrong LI

School of Mathematics and Statistics, Shandong Normal University, Jinan 250014*, China*

Received 6 November 2023/Revised 12 March 2024/Accepted 3 May 2024/Published online 12 August 2024

Abstract Feedback shift registers (FSRs) are pivotal in generating pseudorandom sequences for stream ciphers and play a crucial role in error detection and code correction. This paper investigates the resilience of grain-like cascade FSRs (GLC-FSRs) against two types of fault attacks: hard and soft. First, we introduce a new criterion for assessing the nonsingularity of GLC-FSRs using the structure matrices of feedback functions, which enable the measurement of the number of nonsingular GLC-FSRs. Second, we demonstrate that GLC-FSRs subject to hard fault attacks become singular as determined by this new criterion. Ultimately, by constructing a soft fault bit set, we discuss the resilience of GLC-FSRs to soft fault attacks. Results demonstrate that singular GLC-FSRs remain singular after being injected by soft fault attacks. Conversely, for nonsingular GLC-FSRs, suitable soft fault attacks are designed to maintain their nonsingular status.

Keywords grain-like cascade feedback shift register, fault attack, nonsingularity, semi-tensor product

1 Introduction

Stream cipher is an important cryptographic mechanism and has several advantages, including high encryption and decryption efficiency, simple implementation, and prohibition of error propagation [1]. Its widespread application spans fields such as communications [2, 3] and medicine [4, 5]. Side-channel attacks, such as power analysis, fault attack, and timing analysis, pose significant threats to cipher implementation [6]. The idea of fault attack was introduced by Biham and Shamir [7], and two types of fault attacks are identified currently: hard fault attacks, where certain bits are fixed at 0, and soft fault attacks, which allow attackers to modify the bit values at a certain moment [8]. Obtaining all or part of the secret information by analyzing the differences between faulty and normal outputs triggered by the fault attacks is possible. Correspondingly, it is shown in [6] that the attack model is successful for stream and block ciphers.

Feedback shift registers (FSRs) are fundamental components in stream ciphers, generating pseudorandom bit sequences used as the key streams for encryption. FSRs can be classified into two types based on the feedback mechanisms: linear (LFSRs) and nonlinear (NFSRs) feedback shift registers. LFSRs are integral to many classical stream ciphers owing to their fast speed and efficient hardware implementation [9]. However, the main drawback of n-stage LFSRs is its inability to determine the structure of LFSRs by checking 2^n consecutive bits of the output sequence [10]. Thus, NFSRs have garnered significant attention in stream cipher research [11–13]. In particular, the fault attacks against FSRs also have realistic applications. Hu et al. [8] developed several algorithms to analyze Trivium cascade FSRs subject to hard fault attacks and simplify the cipher. The security of ACORN cascade FSRs under fault attacks was analyzed using a fault location identification algorithm in [6]. Roy et al. [14] conducted the security analysis on Kreyvium cascade FSRs subject to fault attacks based on the key scheduling algorithm. Although several efficient algorithms were developed to analyze the FSRs subject to fault attacks, a theoretical framework is still lacking.

Grain is a typical algorithm among stream ciphers based on NFSRs [15] and is a hardware-oriented finalist for the eSTREAM Stream Cipher Project [16]. In a grain-like cascade FSR (GLC-FSR), an NFSR

*Corresponding author (email: lihaitao_sdu@163.com) is serially connected to an LFSR using the logical operator $\oplus$, where the LFSR output is regarded as an NFSR input. In the last few decades, several significant analyses have been conducted on GLC-FSRs. The periodicity of GLC-FSRs was examined in [17]. Jiang [18] investigated grain-like structures that generate at least one sequence with a minimum period. A basic requirement in sequential cipher design — the nonsingularity of GLC-FSRs — has also been investigated. Lu et al. [19] showed that the nonsingularity of GLC-FSRs correlates with those of state transition matrices. Wang et al. [20] used the state refresh transformations to explore the relationship between the nonsingular GLC-FSR configurations and their feedback functions. To the best of our knowledge, research focusing on the impact of fault attacks on the nonsingularity of GLC-FSRs is limited.

The semi-tensor product (STP) of matrices is a useful mathematical tool for analyzing logical operations [21]. Using this approach, a Boolean function can be equivalently converted into an algebraic form [22–24], facilitating the discussions around Boolean networks (BNs) [25–27]. Recent studies have also focused on attacks on BNs. Zhu et al. [28] used the algebraic state space representation approach to investigate undetectable attacks in BNs. The output feedback control stabilization of hidden Markov Boolean control networks under shifting attacks was studied in [24]. Particularly, STP has greatly promoted the development of FSRs in recent years [29–32]. A linear representation of FSRs utilizing the STP was given in [33]. In [34], an innovative approach was introduced for studying the relationship between Galois NFSRs and Fibonacci NFSRs. In [35], a method was put forward for reconstructing the period of NFSR with a single input. Furthermore, STP explored the observability of Galois NFSRs over finite fields [36] and the nonsingularity of multivalued FSRs [37].

Herein, we discuss the nonsingularity of GLC-FSRs subject to fault attacks. The main contributions of this article are summarized below:

(i) We introduce a new criterion for the nonsingularity of GLC-FSRs. Unlike previous criteria, which relied on the state transition matrix of the whole FSR [19], our criterion depends solely on the structure matrices of feedback functions and has a lower computational load. Furthermore, we derive the number of nonsingular GLC-FSRs using this new criterion.

(ii) We construct the algebraic form of GLC-FSRs subject to fault attacks using the STP framework. Diverging from specific algorithms in [6, 14], the algebraic form provides a theoretical framework for analyzing FSRs subject to fault attacks. Based on the algebraic form, we prove that GLC-FSRs subject to hard fault attacks are always singular. Moreover, we propose the soft fault bit set and establish a criterion for the nonsingularity of GLC-FSRs subject to soft fault attacks.

We organize the rest of this article as follows. In Section 2, we provide some background information on GLC-FSRs. In Section 3, we explore the number of nonsingular GLC-FSRs. In Section 4, we examine the impact of fault attacks on the nonsingularity of GLC-FSRs. In Section 5, we summarize the main conclusion provided.

Notations. "$\otimes$", "$*$", and "$\ltimes$" denote Kronecker product, Khatri-Rao product, and semi-tensor product of matrices [21], respectively. "$\oplus$" represents modulo 2 addition. All $\alpha \times \beta$ real matrices form the set $\mathcal{M}_{\alpha\times\beta}$. Given $\mathcal{P} \in \mathcal{M}_{\alpha\times\beta}$, $\mathrm{Col}(\mathcal{P})$ is the set of columns and $\mathrm{Col}_k(\mathcal{P})$ is the k-th column. $\delta_n^i := \mathrm{Col}_i(I_n)$, where I_n is the n-dimensional identity matrix. Matrix $G = [\delta_\alpha^{i_1}\ \delta_\alpha^{i_2}\ \cdots\ \delta_\alpha^{i_\beta}] \in \mathcal{M}_{\alpha\times\beta}$ is called a logical matrix, if $\mathrm{Col}(L) \subseteq \mathrm{Col}(I_\alpha)$. G is simply represented as $G = \delta_\alpha[i_1, i_2, \ldots, i_\beta]$. The set of $\alpha \times \beta$ logical matrices is denoted by $\mathcal{G}_{\alpha\times\beta}$. $\Delta_2 := \mathrm{Col}(I_2)$. $\mathcal{D} := \{0, 1\}$. $\mathbf{1}_n := [\underbrace{1, 1, \ldots, 1}_{n}]^{\mathrm{T}}$. The symbol $\ltimes$ can be removed without creating any confusion.

2 Preliminaries

Given two positive integers $p, q \geqslant 2$, the diagram of a $(p+q)$-stage GLC-FSR is shown in Figure 1, which contains a p-stage NFSR and a q-stage LFSR. The p-stage NFSR and q-stage LFSR are cascaded by the operation $\oplus$. Each square in the figure is called a bit, which represents a binary storage device. The states of p-stage NFSR, q-stage LFSR and $(p+q)$-stage GLC-FSR are represented by $X = (x_1, \ldots, x_p) \in \mathcal{D}^p$, $Z = (z_1, \ldots, z_q) \in \mathcal{D}^q$ and $W = (x_1, \ldots, x_p, z_1, \ldots, z_q) \in \mathcal{D}^{p+q}$, respectively.

For GLC-FSRs, the transition from the current state to the next state occurs on each clock pulse. According to Figure 1, the state transition from time $t \in \mathbb{N}$ to time $t+1$ satisfies the following group of

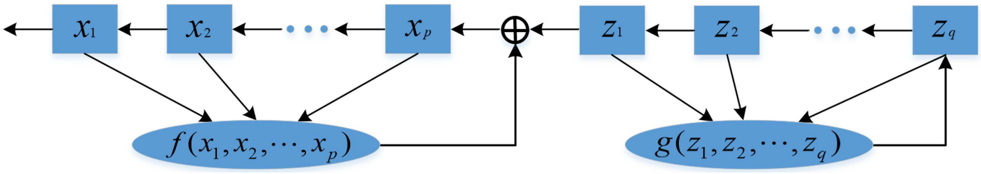

Figure 1 (Color online) Diagram of a $(p+q)$-stage GLC-FSR.

equations:

$$\begin{cases} x_1(t+1) = \psi_1\big(x_1(t),\dots,z_q(t)\big), \\ \quad\vdots \\ x_{p-1}(t+1) = \psi_{p-1}\big(x_1(t),\dots,z_q(t)\big), \\ x_p(t+1) = \psi_p\big(x_1(t),\dots,z_q(t)\big), \\ z_1(t+1) = \phi_1\big(x_1(t),\dots,z_q(t)\big), \\ \quad\vdots \\ z_{q-1}(t+1) = \phi_{q-1}\big(x_1(t),\dots,z_q(t)\big), \\ z_q(t+1) = \phi_q\big(x_1(t),\dots,z_q(t)\big), \end{cases} \tag{1}$$

where $\psi_i(x_1,\dots,z_q) = x_{i+1}$, $i = 1,\dots,p-1$, $\phi_j(x_1,\dots,z_q) = z_{j+1}$, $j = 1,\dots,q-1$, $\psi_p(x_1,\dots,z_q) = f(x_1,\dots,x_p)\oplus z_1$, $\phi_q(x_1,\dots,z_q) = g(z_1,\dots,z_q)$, $f:\mathcal{D}^p\to\mathcal{D}$ and $g:\mathcal{D}^q\to\mathcal{D}$ are feedback functions of NFSR and LFSR, respectively.

STP is a useful tool to derive the equivalent algebraic form of FSRs [33]. Actually, FSR (1) is determined by some Boolean functions. By expressing the Boolean values 0 and 1 to vectors δ_2^2 and δ_2^1, respectively. Any Boolean function $\varphi:\mathcal{D}^n\to\mathcal{D}$ can be uniquely expressed as $\varphi(x_1,\dots,x_n) = M_\varphi\ltimes x_1\ltimes\cdots\ltimes x_n$, where $x_i\in\Delta_2$, $i=1,\dots,n$, and $M_\varphi\in\mathcal{G}_{2\times 2^n}$ is called the structure matrix of φ.

In the following, we introduce the proposition about the deleting operator.

Proposition 1 ([21])**.** Let $X\in\mathcal{G}_{m\times 1}$, $Y\in\mathcal{G}_{n\times 1}$ and $Z\in\mathcal{G}_{r\times 1}$. The deleting operator $\mathcal{P} = \mathbf{1}_m^{\mathrm{T}}\otimes I_n\otimes\mathbf{1}_r^{\mathrm{T}}$ satisfies

$$\mathcal{P}\ltimes XYZ = Y,$$

where $\otimes$ denotes the Kronecker product, I_n is the n-dimensional identity matrix, $\mathbf{1}_m^{\mathrm{T}} = [\underbrace{1,1,\dots,1}_{m}]$ and $\mathbf{1}_r^{\mathrm{T}} = [\underbrace{1,1,\dots,1}_{r}]$.

Using the deleting operator, the structure matrices of Boolean functions $\psi_1,\dots,\psi_{p-1}$ are calculated as

$$\begin{aligned} &\Psi_1 = \mathbf{1}_{2^0}^{\mathrm{T}}\otimes I_2\otimes\mathbf{1}_{2^{p+q-1}}^{\mathrm{T}} = \delta_2\Big[\underbrace{1,\ 1,\dots,\ 1}_{2^{p+q-2}},\underbrace{2,\ 2,\dots,\ 2}_{2^{p+q-2}},\underbrace{1,\ 1,\dots,\ 1}_{2^{p+q-2}},\underbrace{2,\ 2,\dots,\ 2}_{2^{p+q-2}}\Big], \\ &\qquad\vdots \\ &\Psi_{p-1} = \mathbf{1}_{2^{p-2}}^{\mathrm{T}}\otimes I_2\otimes\mathbf{1}_{2^{q+1}}^{\mathrm{T}} = \delta_2\Big[\underbrace{1,\ 1,\dots,\ 1}_{2^q},\underbrace{2,\ 2,\dots,\ 2}_{2^q},\dots,\underbrace{1,\ 1,\dots,\ 1}_{2^q},\underbrace{2,\ 2,\dots,\ 2}_{2^q}\Big], \end{aligned} \tag{2}$$

respectively. Similarly, the structure matrices of Boolean functions $\phi_1,\dots,\phi_{q-1}$ are derived as

$$\begin{aligned} &\Phi_1 = \mathbf{1}_{2^p}^{\mathrm{T}}\otimes I_2\otimes\mathbf{1}_{2^{q-1}}^{\mathrm{T}} = \delta_2\Big[\underbrace{1,\ 1,\dots,\ 1}_{2^{q-2}},\underbrace{2,\ 2,\dots,\ 2}_{2^{q-2}},\underbrace{1,\ 1,\dots,\ 1}_{2^{q-2}},\underbrace{2,\ 2,\dots,\ 2}_{2^{q-2}}\Big], \\ &\qquad\vdots \\ &\Phi_{q-1} = \mathbf{1}_{2^{p+q-2}}^{\mathrm{T}}\otimes I_2\otimes\mathbf{1}_2^{\mathrm{T}} = \delta_2\left[1,\ 2,\ 1,\ 2,\dots,\ 1,\ 2,\ 1,\ 2\right], \end{aligned} \tag{3}$$

respectively.

One can see from (1) that the structure matrices of ψ_p and ϕ_q are related to the feedback functions f and g, which will be calculated in Proposition 2.

Therefore, FSR (1) can be converted to the following form:

$$\begin{cases} x_1(t+1) = \Psi_1 x_1(t)\cdots x_p(t)z_1(t)\cdots z_q(t),\\ \qquad \vdots \\ x_p(t+1) = \Psi_p x_1(t)\cdots x_p(t)z_1(t)\cdots z_q(t),\\ z_1(t+1) = \Phi_1 x_1(t)\cdots x_p(t)z_1(t)\cdots z_q(t),\\ \qquad \vdots \\ z_q(t+1) = \Phi_q x_1(t)\cdots x_p(t)z_1(t)\cdots z_q(t), \end{cases} \tag{4}$$

where $\Psi_k \in \mathcal{G}_{2\times 2^{p+q}}$, $k=1,\dots,p$ and $\Phi_s \in \mathcal{G}_{2\times 2^{p+q}}$, $s=1,\dots,q$. Letting $w = \ltimes_{k=1}^{p} x_k \ltimes_{s=1}^{q} z_s \in (\Delta_2)^{p+q}$, FSR (1) has an equivalent algebraic form as

$$w(t+1) = Lw(t), \tag{5}$$

where $L = \Psi_1 * \cdots * \Psi_p * \Phi_1 * \cdots * \Phi_q \in \mathcal{G}_{2^{p+q}\times 2^{p+q}}$ is the state transition matrix.

Suppose that the structure matrices of feedback functions f, g are

$$\begin{aligned} M_f &= \delta_2\,[\alpha_1,\ \alpha_2,\dots,\ \alpha_{2^p}] \in \mathcal{G}_{2\times 2^p},\\ M_g &= \delta_2\,[\beta_1,\ \beta_2,\dots,\ \beta_{2^q}] \in \mathcal{G}_{2\times 2^q}. \end{aligned} \tag{6}$$

For $\alpha \in \{1,2\}$, we define

$$\bar{\alpha} = \begin{cases} 2, & \text{if } \alpha = 1,\\ 1, & \text{if } \alpha = 2. \end{cases} \tag{7}$$

Then, the relations between Ψ_p, Φ_q and M_f, M_g can be obtained below.

Proposition 2. Consider the algebraic form of FSR (1). The structure matrices Ψ_p and Φ_q satisfy

$$\begin{aligned} \Psi_p &= \delta_2\Bigg[\underbrace{\bar{\alpha}_1,\dots,\ \bar{\alpha}_1}_{2^{q-1}},\ \underbrace{\alpha_1,\dots,\ \alpha_1}_{2^{q-1}},\dots,\underbrace{\bar{\alpha}_{2^p},\dots,\ \bar{\alpha}_{2^p}}_{2^{q-1}},\ \underbrace{\alpha_{2^p},\dots,\ \alpha_{2^p}}_{2^{q-1}}\Bigg],\\ \Phi_q &= \delta_2[\beta_1,\ \beta_2,\dots,\ \beta_{2^q},\ \beta_1,\ \beta_2,\dots,\ \beta_{2^q},\dots,\beta_1,\ \beta_2,\dots,\ \beta_{2^q}]. \end{aligned} \tag{8}$$

Proof. According to FSR (1), the dynamics of bits x_p and z_q satisfy $x_p(t+1) = f\big(x_1(t),\dots,x_p(t)\big) \oplus z_1(t)$ and $z_q(t+1) = g\big(z_1(t),\dots,z_q(t)\big)$, respectively. Using the deleting operator, the dynamics of bits x_p and z_q are expressed as

$$\begin{aligned} x_p(t+1) &= f\big(x_1(t),\dots,x_p(t)\big) \oplus z_1(t)\\ &= M_\oplus M_f x_1(t)\cdots x_p(t)z_1(t)\\ &= \delta_2[2,\ 1,\ 1,\ 2]\delta_2[\alpha_1,\ \alpha_2,\dots,\ \alpha_{2^p}]x_1(t)\cdots x_p(t)z_1(t)\\ &= \delta_2[\bar{\alpha}_1,\ \alpha_1,\ \bar{\alpha}_2,\ \alpha_2,\dots,\ \bar{\alpha}_{2^p},\ \alpha_{2^p}](I_{2^{p+1}} \otimes \mathbf{1}^{\mathrm{T}}_{2^{q-1}})x_1(t)\cdots x_p(t)z_1(t)\cdots z_q(t)\\ &= \delta_2[\bar{\alpha}_1,\dots,\ \bar{\alpha}_1,\ \alpha_1,\dots,\ \alpha_1,\dots,\bar{\alpha}_{2^p},\dots,\ \bar{\alpha}_{2^p},\ \alpha_{2^p},\dots,\ \alpha_{2^p}]w(t)\\ &= \Psi_p w(t),\\ z_q(t+1) &= g\big(z_1(t),\dots,z_q(t)\big)\\ &= M_g z_1(t)\cdots z_q(t)\\ &= \delta_2[\beta_1,\ \beta_2,\dots,\ \beta_{2^q}](\mathbf{1}^{\mathrm{T}}_{2^p} \otimes I_{2^q})x_1(t)\cdots x_p(t)z_1(t)\cdots z_q(t)\\ &= \delta_2[\beta_1,\dots,\ \beta_{2^q},\beta_1,\dots,\ \beta_{2^q},\dots,\beta_1,\dots,\ \beta_{2^q}]w(t)\\ &= \Phi_q w(t), \end{aligned}$$

where $M_\oplus = \delta_2[2,\ 1,\ 1,\ 2]$ is the structure matrix of operation $\oplus$. This completes the proof.

In this paper, we devote to further exploring the nonsingularity of FSR (1) and the number of nonsingular GLC-FSRs by using the equivalent algebraic form. Moreover, considering the effect of fault attacks on FSRs, we also investigate the nonsingularity of GLC-FSRs subject to fault attacks.

3 Further results on nonsingularity of GLC-FSRs

Nonsingularity is a basic requirement for FSRs in cryptographic design. By ensuring the nonsingularity of FSRs, the equivalent secret key can be avoided effectively, and the reliability of the system can be improved. Therefore, when designing nonsingular FSRs, special attention should be paid to the selection of feedback functions. In this section, we obtain two criteria for the nonsingularity of GLC-FSRs by analyzing the feedback functions f and g. Then, the number of nonsingular GLC-FSRs is calculated based on these criteria.

The state transition diagram of FSR (1) has 2^{p+q} nodes and 2^{p+q} directed edges. Each state of FSR (1) is represented by a node. For two states W_1, $W_2 \in \mathcal{D}^{p+q}$, W_1 is said to be a successor state of W_2 if there exists an directed edge from W_2 to W_1. Equivalently, W_2 is said to be a predecessor state of W_1. Based on the state transition diagram, the definition of nonsingular GLC-FSRs is shown below.

Definition 1 ([38])**.** FSR (1) is said to be nonsingular if its state transition diagram contains only cycles.

We observe that there exist two different states with identical successor states if an FSR is singular. In this case, an equivalent secret key is likely to emerge. Therefore, the nonsingularity of FSRs is necessary for developing stream ciphers [19].

As was shown in [19], FSR (1) is nonsingular iff its state transition matrix L is nonsingular. Notice that the nonsingularity of GLC-FSR is determined by the feedback functions f and g. Therefore, we use the structure matrices M_f and M_g which are given in (6) to further explore the nonsingularity of FSR (1), and put forward the following new criterion.

Lemma 1. FSR (1) is nonsingular iff M_f and M_g satisfy

$$\alpha_{i+2^{p-1}} = \bar{\alpha}_i,\ \beta_{j+2^{q-1}} = \bar{\beta}_j, \tag{9}$$

where $i = 1, 2, \dots, 2^{p-1}$, $j = 1, 2, \dots, 2^{q-1}$.

Proof. From Definition 1, FSR (1) is nonsingular iff any state has only one predecessor state and only one successor state. Denote the state transition matrix in (5) as $L = \delta_{2^{p+q}}[\eta_1,\ \eta_2, \dots,\ \eta_{2^{p+q}}]$, then state $\delta_{2^{p+q}}^{\tau}$ has only one successor state $L\delta_{2^{p+q}}^{\tau} = \delta_{2^{p+q}}^{\eta_\tau}$, where $\tau = 1, 2, \dots, 2^{p+q}$. Moreover, the uniqueness of the predecessor state for each state is equivalent to $\eta_c \neq \eta_v$, $\forall\ c \neq v$. Therefore, FSR (1) is nonsingular iff $\eta_c \neq \eta_v$, $\forall\ c \neq v$. In the following, we prove that $\eta_c \neq \eta_v$, $\forall\ c \neq v$ iff (9) is true.

According to (5), it holds that $L = \Psi_1 * \cdots * \Psi_p * \Phi_1 * \cdots * \Phi_q$. Hence, we get

$$\mathrm{Col}_\rho(L) = \mathrm{Col}_\rho(\Psi_1) \ltimes \cdots \ltimes \mathrm{Col}_\rho(\Psi_p) \ltimes \mathrm{Col}_\rho(\Phi_1) \ltimes \cdots \ltimes \mathrm{Col}_\rho(\Phi_q). \tag{10}$$

Then, we define disjoint sets

$$\begin{aligned}
&\Lambda_1 = \{r_{i,j}^1 \mid r_{i,j}^1 = j + (i-1)2^q, i = 1, 2, \dots, 2^{p-1},\ j = 1, 2, \dots, 2^{q-1}\},\\
&\Lambda_2 = \{r_{i,j}^2 \mid r_{i,j}^2 = r_{i,j}^1 + 2^{q-1},\ r_{i,j}^1 \in \Lambda_1, i = 1, 2, \dots, 2^{p-1},\ j = 1, 2, \dots, 2^{q-1}\},\\
&\Lambda_3 = \{r_{i,j}^3 \mid r_{i,j}^3 = r_{i,j}^1 + 2^{p+q-1},\ r_{i,j}^1 \in \Lambda_1,\ i = 1, 2, \dots, 2^{p-1},\ j = 1, 2, \dots, 2^{q-1}\},\\
&\Lambda_4 = \{r_{i,j}^4 \mid r_{i,j}^4 = r_{i,j}^1 + 2^{q-1} + 2^{p+q-1},\ r_{i,j}^1 \in \Lambda_1, i = 1, 2, \dots, 2^{p-1},\ j = 1, 2, \dots, 2^{q-1}\}.
\end{aligned} \tag{11}$$

Then $\bigcup_{k=1}^4 \Lambda_k = \{1, 2, \dots, 2^{p+q}\}$ and $|\Lambda_k| = 2^{p+q-2}$, $k = 1, \dots, 4$. Arbitrarily chosen $r_{u,v}^1 \in \Lambda_1$, it can be obtained from (10) and (11) that

$$\begin{aligned}
&\mathrm{Col}_{r_{u,v}^1}(L) = \delta_{2^{p-1}}^u \delta_2^{\bar{\alpha}_u} \delta_{2^{q-1}}^v \delta_2^{\beta_v} = \delta_{2^{p+q}}^{\eta_{r_{u,v}^1}},\\
&\mathrm{Col}_{r_{u,v}^2}(L) = \delta_{2^{p-1}}^u \delta_2^{\alpha_u} \delta_{2^{q-1}}^v \delta_2^{\beta_{v+2^{q-1}}} = \delta_{2^{p+q}}^{\eta_{r_{u,v}^2}},\\
&\mathrm{Col}_{r_{u,v}^3}(L) = \delta_{2^{p-1}}^u \delta_2^{\bar{\alpha}_{u+2^{p-1}}} \delta_{2^{q-1}}^v \delta_2^{\beta_v} = \delta_{2^{p+q}}^{\eta_{r_{u,v}^3}},\\
&\mathrm{Col}_{r_{u,v}^4}(L) = \delta_{2^{p-1}}^u \delta_2^{\alpha_{u+2^{p-1}}} \delta_{2^{q-1}}^v \delta_2^{\beta_{v+2^{q-1}}} = \delta_{2^{p+q}}^{\eta_{r_{u,v}^4}}.
\end{aligned} \tag{12}$$

From (12), for any $r_{u_1,v_1}^1 \neq r_{u_2,v_2}^1$, one has $\{r_{u_1,v_1}^1, r_{u_1,v_1}^2, r_{u_1,v_1}^3, r_{u_1,v_1}^4\} \cap \{r_{u_2,v_2}^1, r_{u_2,v_2}^2, r_{u_2,v_2}^3, r_{u_2,v_2}^4\} = \emptyset$. Therefore, it is necessary to prove that $\eta_{r_{u,v}^1}$, $\eta_{r_{u,v}^2}$, $\eta_{r_{u,v}^3}$ and $\eta_{r_{u,v}^4}$ are different from each other iff $\alpha_{u+2^{p-1}} = \bar{\alpha}_u$ and $\beta_{v+2^{q-1}} = \bar{\beta}_v$.

On one hand, if $\alpha_{u+2^{p-1}} = \bar{\alpha}_u$ and $\beta_{v+2^{q-1}} = \bar{\beta}_v$, one can derive from (7) that

$$\alpha_u = \bar{\alpha}_{u+2^{p-1}} \neq \alpha_{u+2^{p-1}} = \bar{\alpha}_u,\ \beta_v = \bar{\beta}_{v+2^{q-1}} \neq \beta_{v+2^{q-1}} = \bar{\beta}_v.$$

Based on (12), $\eta_{r^1_{u,v}}$, $\eta_{r^2_{u,v}}$, $\eta_{r^3_{u,v}}$ and $\eta_{r^4_{u,v}}$ are different from each other.

On the other hand, assume that $\eta_{r^1_{u,v}}$, $\eta_{r^2_{u,v}}$, $\eta_{r^3_{u,v}}$ and $\eta_{r^4_{u,v}}$ are different from each other. From $\eta_{r^2_{u,v}} \neq \eta_{r^4_{u,v}}$, we get

$$\delta^u_{2^{p-1}}\delta_2^{\alpha_u}\delta^v_{2^{q-1}}\delta_2^{\beta_{v+2^{q-1}}} \neq \delta^u_{2^{p-1}}\delta_2^{\alpha_{u+2^{p-1}}}\delta^v_{2^{q-1}}\delta_2^{\beta_{v+2^{q-1}}},$$

that is, $\alpha_u \neq \alpha_{u+2^{p-1}}$, $\bar{\alpha}_u = \alpha_{u+2^{p-1}}$. Then from $\bar{\alpha}_u = \alpha_{u+2^{p-1}}$ and $\eta^1_{u,v} \neq \eta^4_{u,v}$, we conclude

$$\delta^u_{2^{p-1}}\delta_2^{\alpha_{u+2^{p-1}}}\delta^v_{2^{q-1}}\delta_2^{\beta_v} \neq \delta^u_{2^{p-1}}\delta_2^{\alpha_{u+2^{p-1}}}\delta^v_{2^{q-1}}\delta_2^{\beta_{v+2^{q-1}}},$$

that is, $\beta_v \neq \beta_{v+2^{q-1}}$, $\bar{\beta}_v = \beta_{v+2^{q-1}}$. Hence, the structure matrices M_f and M_g satisfy $\bar{\alpha}_u = \alpha_{u+2^{p-1}}$ and $\bar{\beta}_v = \beta_{v+2^{q-1}}$ if FSR (1) is nonsingular.

By the arbitrariness of $r^1_{u,v}$, we conclude that FSR (1) is nonsingular iff $\alpha_{i+2^{p-1}} = \bar{\alpha}_i$ and $\beta_{j+2^{q-1}} = \bar{\beta}_j$, where $i = 1, 2, \dots, 2^{p-1}$, $j = 1, 2, \dots, 2^{q-1}$.

Remark 1. The nonsingularity of GLC-FSRs was investigated in [19] by using the whole state transition matrix $L \in \mathcal{G}_{2^{p+q}\times 2^{p+q}}$, and the computational complexity is $O(2^{p+q})$. Compared with [19], the criterion of checking the nonsingularity of GLC-FSRs in Lemma 1 is based on the structure matrices M_f and M_g, whose computational complexity, $O(2^p + 2^q)$, is much lower.

From (9), we derive the characteristics of structure matrices M_f and M_g when the GLC-FSRs are nonsingular. In the following, based on the features of the structural matrix M_f and M_g, we present the properties of feedback functions f and g.

Lemma 2. FSR (1) is nonsingular iff its feedback functions satisfy

(i) $f(x_1, \dots, x_p) = \neg x_1 \oplus f_1(x_2, \dots, x_p)$ or $f(x_1, \dots, x_p) = x_1 \oplus f_2(x_2, \dots, x_p)$;

(ii) $g(z_1, \dots, z_q) = z_1 \oplus g_2(z_2, \dots, z_q)$.

Proof. (Sufficiency) Here we only prove the case of $f(x_1, \dots, x_p) = \neg x_1 \oplus f_1(x_2, \dots, x_p)$ and $g(z_1, \dots, z_q) = z_1 \oplus g_2(z_2, \dots, z_q)$. The proof for the case of $f(x_1, \dots, x_p) = x_1 \oplus f_2(x_2, \dots, x_p)$ and $g(z_1, \dots, z_q) = z_1 \oplus g_2(z_2, \dots, z_q)$ is similar.

Suppose that $f = \neg x_1 \oplus f_1(x_2, \dots, x_p)$, $g = z_1 \oplus g_2(z_2, \dots, z_q)$, and the structure matrices of f_1, g_2 are $M_{f_1} = \delta_2[\alpha_1,\ \alpha_2, \dots,\ \alpha_{2^{p-1}}] \in \mathcal{G}_{2\times 2^{p-1}}$, $M_{g_2} = \delta_2[\beta_1,\ \beta_2, \dots,\ \beta_{2^{q-1}}] \in \mathcal{G}_{2\times 2^{q-1}}$. Using STP, we obtain that

$$\begin{aligned} f(x_1, \dots, x_p) &= M_\oplus M_\neg x_1 M_{f_1} x_2 \cdots x_p \\ &= M_\oplus M_\neg (I_2 \otimes M_{f_1}) x_1 x_2 \cdots x_p \\ &= M_f x_1 x_2 \cdots x_p, \\ g(z_1, \dots, z_q) &= M_\oplus z_1 M_{g_2} z_2 \cdots z_q \\ &= M_\oplus (I_2 \otimes M_{g_2}) z_1 z_2 \cdots z_q \\ &= M_g x_1 x_2 \cdots x_p, \end{aligned}$$

where $M_\neg = \delta_2[2,\ 1]$ is the structure matrix of operation $\neg$. Hence, the structure matrices M_f and M_g are

$$\begin{aligned} M_f &= \delta_2[2,\ 1,\ 1,\ 2]\delta_2[2,\ 1]\delta_4[\alpha_1,\ \alpha_2, \dots,\ \alpha_{2^{p-1}}, 2+\alpha_1, 2+\alpha_2, \dots,\ 2+\alpha_{2^{p-1}}] \\ &= \delta_2[1,\ 2,\ 2,\ 1]\delta_4[\alpha_1,\ \alpha_2, \dots,\ \alpha_{2^{p-1}}, 2+\alpha_1, 2+\alpha_2, \dots,\ 2+\alpha_{2^{p-1}}] \\ &= \delta_2[\alpha_1,\ \alpha_2, \dots,\ \alpha_{2^{p-1}},\ \bar{\alpha}_1,\ \bar{\alpha}_2, \dots,\ \bar{\alpha}_{2^{p-1}}] \in \mathcal{G}_{2\times 2^p}, \\ M_g &= \delta_2[2,\ 1,\ 1,\ 2]\delta_4[\beta_1,\ \beta_2, \dots,\ \beta_{2^{p-1}}, 2+\beta_1, 2+\beta_2, \dots,\ 2+\beta_{2^{p-1}}] \\ &= \delta_2[\bar{\beta}_1,\ \bar{\beta}_2, \dots,\ \bar{\beta}_{2^{p-1}},\ \beta_1,\ \beta_2, \dots,\ \beta_{2^{p-1}}] \in \mathcal{G}_{2\times 2^q}. \end{aligned}$$

According to Lemma 1, FSR (1) is nonsingular.

(Necessity) Assume that FSR (1) is nonsingular. According to (9), we denote the structure matrix of f as

$$\begin{aligned} M_f &= \delta_2[\alpha_1, \alpha_2, \dots, \alpha_{2^{p-1}}, \alpha_{2^{p-1}+1}, \alpha_{2^{p-1}+2}, \dots, \alpha_{2^p}] \\ &= \delta_2[\alpha_1, \alpha_2, \dots, \alpha_{2^{p-1}}, \bar{\alpha}_1, \bar{\alpha}_2, \dots, \bar{\alpha}_{2^{p-1}}]. \end{aligned}$$

Let $M_{f_1} = \delta_2[\alpha_1,\ \alpha_2, \dots,\ \alpha_{2^{p-1}}]$, $M_{f_2} = \delta_2[\bar{\alpha}_1,\ \bar{\alpha}_2, \dots,\ \bar{\alpha}_{2^{p-1}}]$. From (7), it holds that

$$M_{f_2} = \delta_2[2,\ 1]\delta_2[\alpha_1,\ \alpha_2, \dots,\ \alpha_{2^{p-1}}] = M_\neg M_{f_1}.$$

Hence, function f can be expressed as

$$\begin{aligned}
f(x_1,x_2,\ldots,x_p) =&[M_{f_1} \quad M_{\neg}M_{f_1}]x_1x_2\cdots x_p\\
=&[I_2 \quad M_{\neg}]\begin{bmatrix} M_{f_1} & \mathbf{0}\\ \mathbf{0} & M_{f_1}\end{bmatrix}x_1x_2\cdots x_p\\
=&M_{\oplus}M_{\neg}(I_2\otimes M_{f_1})x_1x_2\cdots x_p\\
=&M_{\oplus}M_{\neg}x_1M_{f_1}x_2\cdots x_p\\
=&\neg x_1\oplus f_1(x_2,\ldots,x_p),
\end{aligned}$$

or

$$\begin{aligned}
f(x_1,x_2,\ldots,x_p) =&[M_{f_1} \quad M_{\neg}M_{f_1}]x_1x_2\cdots x_p\\
=&[M_{\neg} \quad I_2]\begin{bmatrix} M_{\neg}M_{f_1} & \mathbf{0}\\ \mathbf{0} & M_{\neg}M_{f_1}\end{bmatrix}x_1x_2\cdots x_p\\
=&M_{\oplus}(I_2\oplus M_{\neg}M_{f_1})x_1x_2\cdots x_p\\
=&M_{\oplus}x_1M_{\neg}M_{f_1}x_2\cdots x_p\\
=&x_1\oplus f_2(x_2,\ldots,x_p).
\end{aligned}$$

Similar to f, the feedback function g satisfies $g=\neg z_1\oplus g_1(z_2,\ldots,z_q)$ or $g=z_1\oplus g_2(z_2,\ldots,z_q)$. Since g is a linear function, it holds that $g=z_1\oplus g_2(z_2,\ldots,z_q)$.

Based on Lemmas 1 and 2, we finally calculate the number of nonsingular GLC-FSRs.

Theorem 1. The number of nonsingular GLC-FSRs composed of p-stage NFSRs and q-stage LFSRs is $2^{q-1+2^{p-1}}-2^{p+q-2}$.

Proof. According to Lemmas 1 and 2, a GLC-FSR is nonsingular iff the linear feedback function g satisfies $g=z_1\oplus g_2(z_2,\ldots,z_q)$ and the structure matrix of the nonlinear feedback function f satisfies $\alpha_{i+2^{p-1}}=\bar{\alpha}_i$, $i=1,2,\ldots,2^{p-1}$.

On one hand, since g is linear, then $g_2=\alpha_2z_2\oplus\cdots\oplus\alpha_qz_q$, where $\alpha_2,\ldots,\alpha_q\in\mathcal{D}$. Hence, there exist 2^{q-1} linear functions which satisfy the requirement of the linear feedback function g in the nonsingular GLC-FSRs.

On the other hand, since the Boolean function has a one-to-one correspondence with its structure matrix, then there exist $2^{2^{p-1}}$ Boolean functions whose structure matrices satisfy $\alpha_{i+2^{p-1}}=\bar{\alpha}_i$. Moreover, these $2^{2^{p-1}}$ Boolean functions contain 2^{p-1} linear functions. Hence, there exist $2^{2^{p-1}}-2^{p-1}$ nonlinear functions which satisfy the requirement of the nonlinear feedback function f in the nonsingular GLC-FSRs.

To sum up, the number of nonsingular GLC-FSRs composed of p-stage NFSRs and q-stage LFSRs is $2^{q-1}(2^{2^{p-1}}-2^{p-1})=2^{q-1+2^{p-1}}-2^{p+q-2}$.

Remark 2. The proof of Lemma 2 combines the structure matrices and the refresh transformations of feedback functions. In this way, the number of nonsingular GLC-FSRs can be obtained. Moreover, Lemma 1 facilitates the exploration of fault attack on the nonsingularity of GLC-FSRs.

To illustrate Theorem 1, we finally provide an example.

Example 1. Consider the GLC-FSRs composed of 2-stage NFSRs and 2-stage LFSRs.

From Lemma 1, the structure matrix M_f in nonsingular GLC-FSRs satisfies

$$M_f=\delta_2[1,\ 1,\ 2,\ 2] \text{ or } M_f=\delta_2[1,\ 2,\ 2,\ 1] \text{ or } M_f=\delta_2[2,\ 1,\ 1,\ 2] \text{ or } M_f=\delta_2[2,\ 2,\ 1,\ 1].$$

Hence, feedback function f satisfies $f=x_1$ or $f=\neg x_1\oplus x_2$ or $f=x_1\oplus x_2$ or $f=\neg x_1$. Since f is a nonlinear function, we further derive

$$f=\neg x_1\oplus x_2 \text{ or } f=\neg x_1.$$

From Lemma 2, the linear feedback function g of nonsingular GLC-FSRs satisfies

$$g=z_1 \text{ or } g=z_1\oplus z_2.$$

Hence, the number of nonsingular GLC-FSRs composed of 2-stage NFSRs and 2-stage LFSRs is 4, which is consistent with $2^{2-1+2}-2^{4-2}=4$ in Theorem 1.

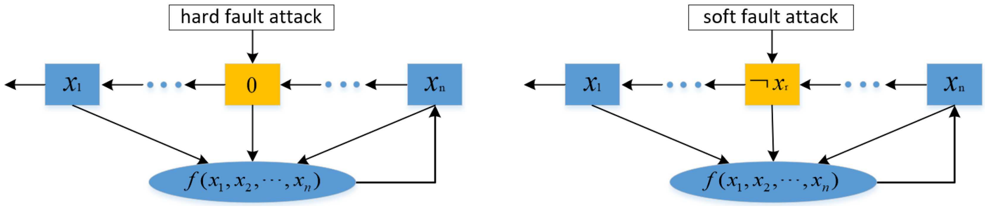

Figure 2 (Color online) FSR under fault attack which injects only one bit.

4 Nonsingularity of GLC-FSRs subject to fault attacks

The fault attack is a feasible way to achieve the side-channel attacks in cryptography. The attacker can destroy the normal operation of the cryptosystem through fault attacks, which may cause the cryptosystem to produce the wrong output. Then, the attacker can analyze the fault information and deduce the key or plaintext information. In this section, we establish the algebraic form of GLC-FSRs subject to fault attacks under the STP framework, and then explore the effect of fault attacks on the nonsingularity of GLC-FSRs.

In this article, we discuss two types of fault attacks [8]: hard fault attack and soft fault attack. Hard fault attack indicates that the attacker permanently fixes some random bits to 0. Thus, the bits injected by hard fault will always be read out as 0, but will never be written in. Besides, hard fault attack is destructive, and thus it can only be injected once. Soft fault attack indicates that the attacker will change the value of some random bits in FSRs and has the power to reset the register. Hence, soft fault attack can be injected multiple times. Figure 2 shows these two kinds of fault attacks on FSRs, where the injection position is x_r.

Firstly, we investigate the nonsingularity of GLC-FSRs which are attacked by a hard fault. Since all hard fault attacks are destructive, we only need to consider the case that a single bit is attacked and make Assumption 1.

Assumption 1. The hard fault attack is injected into a single bit of FSR (1).

According to the structure matrices of GLC-FSRs, we come to the following conclusion.

Theorem 2. Under Assumption 1, FSR (1) subject to the hard fault attack is singular.

Proof. Here we only prove the situation where the hard fault attack is injected into the NFSR of FSR (1). The proof for the situation where the hard fault attack is injected into the LFSR of FSR (1) is similar.

Suppose that the hard fault attack is injected into bit x_k, where $k \in \{1,2,\ldots,p\}$. Correspondingly, the attacked bit is denoted as x_k^F and the dynamics of x_k^F becomes $x_k^F(t+1)=0$. Hence, the structure matrix of x_k^F satisfies $\Psi_k^F=\delta_2[2,\ 2,\ldots,2]\in\mathcal{G}_{2\times 2^{p+q}}$. The state transition matrix of FSR (1) subject to this type of hard fault is represented as $L^F=\delta_{2^{p+q}}[\eta_1^F,\ \eta_2^F,\ldots,\ \eta_{2^{p+q}}^F]\in\mathcal{G}_{2^{p+q}\times 2^{p+q}}$. Then

$$\mathrm{Col}_\tau(L^F)=\mathrm{Col}_\tau(\Psi_1)\ltimes\cdots\ltimes\mathrm{Col}_\tau(\Psi_{k-1})\ltimes\mathrm{Col}_\tau(\Psi_k^F)\ltimes\mathrm{Col}_\tau(\Psi_{k+1})\ltimes\cdots\mathrm{Col}_\tau(\Phi_q)=\delta_{2^{p+q}}^{\eta_\tau^F}, \tag{13}$$

where $\tau=1,2,\ldots,2^{p+q}$.

Without losing generality, let $\delta_{2^{p+q}}^{\eta_\tau^F}=\delta_{2^{k-1}}^{\mu}\delta_2^2\delta_{2^{p+q-k}}^{\nu}$. Using STP, we obtain that

$$\delta_{2^{p+q}}^{\eta_\tau^F}=\delta_{2^{k-1}}^{\mu}\delta_2^2\delta_{2^{p+q-k}}^{\nu}=\delta_{2^k}^{2(\mu-1)+2}\delta_{2^{p+q-k}}^{\nu}=\delta_{2^k}^{2\mu}\delta_{2^{p+q-k}}^{\nu}=\delta_{2^{p+q}}^{2^{p+q-k}(2\mu-1)+\nu}.$$

Noticing that $\mu\in\{1,2,\ldots,2^{k-1}\}$ and $\nu\in\{1,2,\ldots,\ 2^{p+q-k}\}$, it holds that

$$\begin{aligned}2^{p+q-k}(2\mu-1)+\nu\in\Big\{\ & 2^{p+q-k}+1,\ldots,2^{p+q-k}+2^{p+q-k},\\ & 3\cdot 2^{p+q-k}+1,\ldots,3\cdot 2^{p+q-k}+2^{p+q-k},\ldots,\\ & (2^k-1)\cdot 2^{p+q-k}+1,\ldots,2^k-1\cdot 2^{p+q-k}+2^{p+q-k}\ \Big\}=\Omega_k,\end{aligned}$$

where $|\Omega_k|=2^{p+q-1}$. Since the state transition matrix L^F has 2^{p+q} columns and the set Ω_k has 2^{p+q-1} elements, there must exist identical columns in matrix L^F. According to Lemma 1, FSR (1) subject to the hard fault is singular.

Remark 3. Similar to the proof of Theorem 2, the state transition matrix L^F has at most $2^{p+q-\omega}$ different columns when the hard fault attack is injected into ω bits, where $\omega = 2, 3, \ldots, p+q$. Hence, FSR (1) subject to any hard fault attack becomes singular.

Next, we investigate the nonsingularity of GLC-FSRs subject to soft fault attacks. For the convenience of the following discussion under the framework of STP, we give some necessary preliminaries. Let $\Re = \{x_{k_1}, \ldots, x_{k_\iota}, z_{s_1}, \ldots, z_{s_\sigma}\}$ be the soft fault bit set, where $k_1 < \cdots < k_\iota$, $s_1 < \cdots < s_\sigma$. Based on the definition of soft fault attack, the soft fault function with respect to $\Re$ is described as

$$S_{\Re}(W) = (x_1^*, \ldots, x_p^*, z_1^*, \ldots, z_q^*), \tag{14}$$

where $W = (x_1, \ldots, x_p, z_1, \ldots, z_q)$ and

$$\begin{cases} x_k^* = \neg x_k, & \text{if } x_k \in \Re; \\ z_s^* = \neg z_s, & \text{if } z_s \in \Re; \\ x_k^* = x_k, & \text{if } x_k \notin \Re; \\ z_s^* = z_s, & \text{if } z_s \notin \Re. \end{cases}$$

By converting W and $S_{\Re}(W)$ into vector forms as $W = x_1 \cdots x_p z_1 \cdots z_q$ and $S_{\Re}(W) = x_1^* \cdots x_p^* z_1^* \cdots z_q^*$, respectively, the soft fault function $S_{\Re}$ can expressed as

$$S_{\Re}(W) = x_1^* \cdots x_p^* z_1^* \cdots z_q^* = M_{S_{\Re}} x_1 \cdots x_p z_1 \cdots z_q, \tag{15}$$

where $M_{S_{\Re}} = [\ltimes_{i=1}^{\iota}(I_{2^{k_i-1}} \otimes M_\neg)][\ltimes_{j=1}^{\sigma}(I_{2^{p+s_j-1}} \otimes M_\neg)] \ltimes I_{2^{p+q}} \in \mathcal{G}_{2^{p+q} \times 2^{p+q}}$.

Since the attacker has the ability to inject the soft fault at any random bit, we denote the power set of $\{x_1, \ldots, x_p, z_1, \ldots, z_q\}$ as $\Upsilon = \{\Re_1,\ \Re_2, \ldots,\ \Re_{2^{p+q}}\}$, where $\Re_1, \Re_2, \ldots, \Re_{2^{p+q}}$ are all possible soft fault bit sets. For example, for a GLC-FSR consisting of a 3-stage NFSR and a 2-stage LFSR, the soft fault bit sets are

$$\begin{aligned} &\Re_1 = \emptyset,\ \Re_2 = \{x_1\},\ \Re_3 = \{x_2\},\ \Re_4 = \{x_3\},\ \Re_5 = \{z_1\},\ \Re_6 = \{z_2\}, \\ &\Re_7 = \{x_1,\ x_2\},\ \Re_8 = \{x_1,\ x_3\},\ \Re_9 = \{x_1,\ z_1\},\ \Re_{10} = \{x_1,\ z_2\}, \\ &\cdots,\ \Re_{31} = \{x_2,\ x_3,\ z_1,\ z_2\},\ \Re_{32} = \{x_1,\ x_2,\ x_3,\ z_1,\ z_2\}, \end{aligned}$$

where $\Re_1$ indicates that the GLC-FSR is not attacked by the soft fault, and $\Re_{32}$ indicates that all bits are attacked by the soft fault. Since soft fault attack can be injected multiple time, we make the following natural assumption.

Assumption 2. The attacker can inject the soft fault attack $\Re(t)$ with respect to the state $w(t)$ of FSR (1) at time t, where $\Re(t) \in \{\Re_1, \Re_2, \ldots, \Re_{2^{p+q}}\}$.

Soft fault attacks mean that the attacker can modify the values of one or more random bits and has the ability to reset FSRs. Thus, the soft fault attack can be injected into x_p and z_q. When the soft fault attack is injected into only one bit at each time, say x_r, we only need to consider the impact of Φ_{r-1} on the state transition matrix L. However, the more general case is that the soft fault attacks are injected into several bits at different times. Therefore, we use the soft fault bit sets to analyze the state transition of GLC-FSRs subject to soft fault attacks.

Similar to (14) and (15), we obtain the soft fault functions and the corresponding structure matrices with respect $\Re_1,\ \Re_2, \ldots, \Re_{2^{p+q}}$, which are denoted as

$$S_{\Re_1},\ S_{\Re_2}, \ldots,\ S_{\Re_{2^{p+q}}} \quad \text{and} \quad M_{S_{\Re_1}},\ M_{S_{\Re_2}}, \ldots,\ M_{S_{\Re_{2^{p+q}}}} \in \mathcal{G}_{2^{p+q} \times 2^{p+q}}. \tag{16}$$

Moreover, we convert all the soft fault bit sets into vector forms below:

$$\Re_1 \sim \delta_{2^{p+q}}^1,\ \Re_2 \sim \delta_{2^{p+q}}^2, \ldots,\ \Re_{2^{p+q}} \sim \delta_{2^{p+q}}^{2^{p+q}}. \tag{17}$$

Now, based on Assumption 2, the soft fault attack depending on the state can be represented as

$$\Re(t) = Hw(t), \tag{18}$$

where $H = \delta_{2^{p+q}}[h_1,\ h_2, \ldots,\ h_{2^{p+q}}] \in \mathcal{G}_{2^{p+q} \times 2^{p+q}}$.

Since the structure matrix corresponding to the soft fault attack $\Re(t)$ can be represented as $[M_{S_{\Re_1}}\ M_{S_{\Re_2}}\ \cdots\ M_{S_{\Re_{2^{p+q}}}}]\Re(t)$, the state of FSR (1) with the soft fault attack (18) is

$$\begin{aligned}\widetilde{w}(t) &= [M_{S_{\Re_1}}\ M_{S_{\Re_2}}\ \cdots\ M_{S_{\Re_{2^{p+q}}}}]\Re(t)w(t)\\ &= [M_{S_{\Re_1}}\ M_{S_{\Re_2}}\ \cdots\ M_{S_{\Re_{2^{p+q}}}}]Hw(t)w(t).\end{aligned}$$

Given $w(t)=\delta^{\lambda}_{2^{p+q}}$, $\lambda\in\{1,2,\ldots,2^{p+q}\}$, using STP, we get $w(t)w(t)=\delta^{\lambda}_{2^{p+q}}\delta^{\lambda}_{2^{p+q}}=\delta^{(\lambda-1)2^{p+q}+\lambda}_{2^{2p+2q}}$. Hence, we construct the power-reducing matrix $J=\delta_{2^{2p+2q}}[1, 2^{p+q}+2, \ldots, 2^{2p+2q}]\in\mathcal{G}_{2^{2p+2q}\times 2^{p+q}}$, which satisfies $Jw(t)=w(t)w(t)$.

According to (16)–(18), the algebraic form of FSR (1) subject to the soft fault attack (18) is represented as

$$w(t+1)=L\widetilde{w}(t)=L^SHJw(t), \tag{19}$$

where $L^S=L[M_{S_{\Re_1}}\ M_{S_{\Re_2}}\ \cdots\ M_{S_{\Re_{2^{p+q}}}}]\in\mathcal{G}_{2^{p+q}\times 2^{2p+2q}}$.

Similar to Definition 1, FSR (1) subject to the soft fault attack (18) is nonsingular if the state transition diagram of system (19) contains only cycles. The following result shows that singular FSR (1) is still singular when a soft fault attack occurs.

Theorem 3. FSR (1) subject to the soft fault attack (18) is singular, if FSR (1) is singular.

Proof. Since FSR (1) is singular, according to the proof of Lemma 1, we get $\mathrm{Col}(L)\subsetneqq(\Delta_2)^{p+q}$. Then there exists $\lambda\in\{1,2,\ldots,2^{p+q}\}$ such that $\delta^{\lambda}_{2^{p+q}}\notin\mathrm{Col}(L)$.

Arbitrarily choose the state $w(t)=\delta^{\tau}_{2^{p+q}}$ of system (19). Then, the successor state of $\delta^{\tau}_{2^{p+q}}$ is

$$\begin{aligned}w(t+1)&=L[M_{S_{\Re_1}}\ M_{S_{\Re_2}}\ \cdots\ M_{S_{\Re_{2^{p+q}}}}]\delta_{2^{p+q}}[h_1,\ h_2,\ldots,\ h_{2^{p+q}}]\delta^{\tau}_{2^{p+q}}\delta^{\tau}_{2^{p+q}}\\ &=L[M_{S_{\Re_1}}\ M_{S_{\Re_2}}\ \cdots\ M_{S_{\Re_{2^{p+q}}}}]\delta^{h_\tau}_{2^{p+q}}\delta^{\tau}_{2^{p+q}}\\ &=LM_{S_{\Re_{h_\tau}}}\delta^{\tau}_{2^{p+q}}=L\mathrm{Col}_\tau(M_{S_{\Re_{h_\tau}}}).\end{aligned}$$

Since $\delta^{\lambda}_{2^{p+q}}\notin\mathrm{Col}(L)$, we get $L\mathrm{Col}_\tau(M_{S_{\Re_\zeta}})\neq\delta^{\lambda}_{2^{p+q}}$, that is, $\delta^{\tau}_{2^{p+q}}$ is not a predecessor state of $\delta^{\lambda}_{2^{p+q}}$. By the arbitrariness of $\delta^{\tau}_{2^{p+q}}$, we conclude that $\delta^{\lambda}_{2^{p+q}}$ has no predecessor state in system (19). Hence, FSR (1) subject to the soft fault attack (18) is singular.

The following presents a necessary and sufficient condition for the nonsingularity of FSR (1) subject to the soft fault attack (18).

Theorem 4. FSR (1) subject to the soft fault attack (18) is nonsingular iff

$$\mathrm{Col}(L^SHJ)=(\Delta_2)^{p+q}. \tag{20}$$

Proof. (Sufficiency) Arbitrarily chosen state $w(t)=\delta^{\vartheta}_{2^{p+q}}$ of system (19), the successor state of $\delta^{\vartheta}_{2^{p+q}}$ is

$$w(t+1)=L^SHJ\delta^{\vartheta}_{2^{p+q}}=\mathrm{Col}_\vartheta(L^SHJ).$$

According to (20), there exists only one state $\delta^{\zeta}_{2^{p+q}}$ which satisfies

$$L^SHJ\delta^{\zeta}_{2^{p+q}}=\mathrm{Col}_\zeta(L^SHJ)=\delta^{\vartheta}_{2^{p+q}},$$

that is, $\delta^{\vartheta}_{2^{p+q}}$ has only one predecessor state $\delta^{\zeta}_{2^{p+q}}$.

By the arbitrariness of $\delta^{\vartheta}_{2^{p+q}}$, we conclude that any state of system (19) has the unique predecessor state and the unique successor state. Therefore, there exist only cycles in the state transition diagram of system (19), which implies that FSR (1) subject to the soft attack (18) is nonsingular.

(Necessity) We prove the necessity by a reduction to absurdity. Suppose that

$$\mathrm{Col}(L^SHJ)\subsetneqq(\Delta_2)^{p+q}.$$

Hence, there must exist identical columns in matrix L^SHJ. Without loss of generality, we denote $\mathrm{Col}_\vartheta(L^SHJ)=\mathrm{Col}_\zeta(L^SHJ)=\delta^{\varphi}_{2^{p+q}}$. Then, it holds that

$$L^SHJ\delta^{\vartheta}_{2^{p+q}}=L^SHJ\delta^{\zeta}_{2^{p+q}}=\delta^{\varphi}_{2^{p+q}},$$

that is, $\delta_{2^{p+q}}^{\varphi}$ has two different predecessor states, which contradicts the fact that FSR (1) subject to the soft fault attack (18) is nonsingular.

According to Theorems 3 and 4, we conclude that singular GLC-FSRs remain singular after soft fault attacks, and nonsingular GLC-FSRs remain nonsingular after the specific soft fault attacks satisfying (20).

At last, an illustrative example is used to interpret Theorems 2 and 4.

Example 2. Consider a GLC-FSR below:

$$\begin{cases} x_1(t+1) = x_2(t), \\ x_2(t+1) = x_3(t), \\ x_3(t+1) = \big[x_1(t) \oplus \big(\neg x_2(t) \wedge x_3(t)\big)\big] \oplus z_1(t), \\ z_1(t+1) = z_2(t), \\ z_2(t+1) = z_1(t) \oplus z_2(t), \end{cases} \tag{21}$$

where $x_k,\ z_s \in \mathcal{D},\ k = 1,2,3,\ s = 1,2.$

Firstly, we analyze the nonsingularity of FSR (21). The feedback functions of FSR (21) are $f(x_1,x_2,x_3) = x_1 \oplus (\neg x_2 \wedge x_3)$ and $g(z_1,z_2) = z_1 \oplus z_2$. Using STP, we obtain the structure matrices of f, g below:

$$M_f = \delta_2[1,\ 1,\ 2,\ 1,\ 2,\ 2,\ 1,\ 2],\ M_g = \delta_2[2,\ 1,\ 1,\ 2].$$

According to Lemma 1, FSR (21) is nonsingular. To verify our result, the algebraic form of FSR (21) is derived from (2), (3) and Proposition 2, which is shown below:

$$w(t+1) = Lw(t),$$

where

$$\begin{aligned} L = \delta_{32}[&6,\ 7,\ 1,\ 4,\ 14,\ 15,\ 9,\ 12, 18,\ 19,\ 21,\ 24,\ 30,\ 31,\ 25,\ 28, \\ &2,\ 3,\ 5,\ 8,\ 10,\ 11,\ 13,\ 16, 22,\ 23,\ 17,\ 20,\ 26,\ 27,\ 29,\ 32]. \end{aligned}$$

Based on L, there exist only four cycles in the state transition diagram of FSR (21): $\delta_{32}^4 \to \delta_{32}^4$, $\delta_{32}^{32} \to \delta_{32}^{32}$, $\delta_{32}^8 \to \delta_{32}^{12} \to \delta_{32}^{24} \to \delta_{32}^{16} \to \delta_{32}^{28} \to \delta_{32}^{20} \to \delta_{32}^8$ and $\delta_{32}^1 \to \delta_{32}^6 \to \delta_{32}^{15} \to \delta_{32}^{25} \to \delta_{32}^{22} \to \delta_{32}^{11} \to \delta_{32}^{21} \to \delta_{32}^{10} \to \delta_{32}^{19} \to \delta_{32}^5 \to \delta_{32}^{14} \to \delta_{32}^{31} \to \delta_{32}^{29} \to \delta_{32}^{26} \to \delta_{32}^{23} \to \delta_{32}^{13} \to \delta_{32}^{30} \to \delta_{32}^{27} \to \delta_{32}^{17} \to \delta_{32}^2 \to \delta_{32}^7 \to \delta_{32}^9 \to \delta_{32}^{18} \to \delta_{32}^3 \to \delta_{32}^1$. Hence, FSR (21) is nonsingular, which is consistent with Lemma 1.

Now, we discuss the nonsingularity of FSR (21) subject to the hard fault attack. Assume that the hard fault is injected into bit x_2 and the attacked bit is denoted as x_2^F. Then the structure matrix of x_2^F satisfies $\Psi_2^F = \delta_2[2,\ 2, \ldots,\ 2] \in \mathcal{G}_{2\times 32}$. Hence, the state transition matrix of the attacked FSR is

$$\begin{aligned} L^F = \delta_{32}[&14,\ 15,\ 9,\ 12,\ 14,\ 15,\ 9,\ 12, 26,\ 27,\ 29,\ 32,\ 30,\ 31,\ 25,\ 28, \\ &10,\ 11,\ 13,\ 16,\ 10,\ 11,\ 13,\ 16, 30,\ 31,\ 25,\ 28,\ 26,\ 27,\ 29,\ 32]. \end{aligned}$$

According to Lemma 1, FSR (21) subject to the hard fault attacks is singular, which is consistent with Theorem 2.

Finally, we analyze the nonsingularity of FSR (21) subject to soft fault attack. Assume that the soft fault attack is

$$\Re(t) = Hw(t), \tag{22}$$

where $H = I_{32}$. According to (15) and (17), we obtain

$$\begin{aligned} L^S HJ\delta_{32}^{14} = L^S H\delta_{32}^{14}\delta_{32}^{14} = LM_{S_{\Re_{14}}}\delta_{32}^{14} = L\mathrm{Col}_{14}(M_{S_{\Re_{14}}}) = L\delta_{32}^{12} = \delta_{32}^{24}, \\ L^S HJ\delta_{32}^{15} = L^S H\delta_{32}^{15}\delta_{32}^{15} = LM_{S_{\Re_{15}}}\delta_{32}^{15} = L\mathrm{Col}_{15}(M_{S_{\Re_{15}}}) = L\delta_{32}^{12} = \delta_{32}^{24}. \end{aligned}$$

Hence, it holds that

$$\mathrm{Col}(L^S HJ) \subsetneqq (\Delta_2)^5.$$

According to Theorem 4, GLC-FSR (21) subject to the soft fault attack (22) is singular.

5 Conclusion

We have derived the number of nonsingular GLC-FSRs by constructing the structure matrices of feedback functions. Next, we have demonstrated that any GLC-FSR is singular under hard fault attacks. Furthermore, we have analyzed the nonsingularity of GLC-FSRs subject to soft fault attacks, utilizing the soft fault function and soft fault bit set. Future research could explore the nonsingularity of other types of FSRs subject to fault attacks.

Acknowledgements This work was supported by National Natural Science Foundation of China (Grant No. 62073202) and Young Experts of Taishan Scholar Project (Grant No. tsqn201909076).

References

1 Jiao L, Hao Y L, Feng D G. Stream cipher designs: a review. Sci China Inf Sci, 2020, 63: 131101

2 Lee H, Moon S. Parallel stream cipher for secure high-speed communications. Signal Process, 2002, 82: 259–265

3 Dubrova E, Hell M. Espresso: a stream cipher for 5G wireless communication systems. Cryptogr Commun, 2017, 9: 273–289

4 Bouslimi D, Coatrieux G, Cozic M, et al. A joint encryption/watermarking system for verifying the reliability of medical images. IEEE Trans Inform Technol Biomed, 2012, 16: 891–899

5 Ding Y, Tan F, Qin Z, et al. DeepKeyGen: a deep learning-based stream cipher generator for medical image encryption and decryption. IEEE Trans Neural Netw Learn Syst, 2021, 33: 4915–4929

6 Dey P, Rohit R S, Adhikari A. Full key recovery of ACORN with a single fault. J Inf Security Appl, 2016, 29: 57–64

7 Biham E, Shamir A. Differential fault analysis of secret key cryptosystems. In: Proceedings of the 17th Annual International Cryptology Conference, 1997. 513–525

8 Hu Y, Zhang F, Zhang W. Hard fault analysis of Trivium. Inf Sci, 2013, 229: 142–158

9 Zhong J, Lin D. On minimum period of nonlinear feedback shift registers in grain-like structure. IEEE Trans Inform Theor, 2018, 64: 6429–6442

10 Massey J. Shift-register synthesis and BCH decoding. IEEE Trans Inform Theor, 1969, 15: 122–127

11 Zhang J M, Qi W F, Tian T, et al. Further results on the decomposition of an NFSR into the cascade connection of an NFSR into an LFSR. IEEE Trans Inform Theor, 2015, 61: 645–654

12 Zhang J M, Tian T, Qi W F, et al. A new method for finding affine sub-families of NFSR sequences. IEEE Trans Inform Theor, 2019, 65: 1249–1257

13 Wang X J, Tian T, Qi W F. A generic method for investigating nonsingular Galois NFSRs. Des Codes Cryptogr, 2022, 90: 387–408

14 Roy D, Bathe B, Maitra S. Differential fault attack on Kreyvium & FLIP. IEEE Trans Comput, 2020, 70: 2161–2167

15 Hell M, Johansson T, Meier W. Grain: a stream cipher for constrained environments. J Wireless Mobile Comput, 2007, 2: 86–93

16 Hell M, Johansson T, Maximov A, et al. The Grain family of stream ciphers. In: New Stream Cipher Designs: The eSTREAM Finalists. Berlin: Springer, 2008. 179–190

17 Hu H, Gong G. Periods on two kinds of nonlinear feedback shift registers with time varying feedback functions. Int J Found Comput Sci, 2011, 22: 1317–1329

18 Jiang Y. Weak grain-like structures. IEEE Trans Inform Theor, 2020, 66: 7717–7723

19 Lu J Q, Li M L, Liu Y, et al. Nonsingularity of Grain-like cascade FSRs via semi-tensor product. Sci China Inf Sci, 2018, 61: 010204

20 Wang Q, Jin C. Criteria for nonsingularity of Grain-like cascade feedback shift register (in Chinese). Comput Eng, 2014, 40: 167–170

21 Cheng D, Qi H, Li Z. Analysis and Control of Boolean Networks: A Semi-tensor Product Approach. London: Springer, 2011

22 Yu Y, Meng M, Feng J. Observability of Boolean networks via matrix equations. Automatica, 2020, 111: 108621

23 Yan Y Y, Cheng D Z, Feng J E, et al. Survey on applications of algebraic state space theory of logical systems to finite state machines. Sci China Inf Sci, 2023, 66: 111201

24 Wang L, Wu Z G, Lam J. Necessary and sufficient conditions for security of hidden Markov Boolean control networks under shifting attacks. IEEE Trans Netw Sci Eng, 2022, 10: 321–330

25 Guo Y, Gong P, Wu Y, et al. Stabilization of discrete-time switched systems with constraints by dynamic logic-based switching feedback. Automatica, 2023, 156: 111190

26 Wang S L, Li H T. Aggregation method to reachability and optimal control of large-size Boolean control networks. Sci China Inf Sci, 2023, 66: 179202

27 Wu J, Liu Y, Ruan Q, et al. Robust stability of Switched Boolean networks with function perturbation. Nonlinear Anal-Hybrid Syst, 2022, 46: 101216

28 Zhu S, Lu J, Cao J, et al. Undetectable attacks on Boolean networks. In: Proceedings of the 62nd IEEE Conference on Decision and Control, 2023. 1698–1703

29 Zhao D W, Peng H P, Li L X, et al. Novel way to research nonlinear feedback shift register. Sci China Inf Sci, 2014, 57: 1–14

30 Kong W H, Zhong J H, Lin D D. Observability of Galois nonlinear feedback shift registers. Sci China Inf Sci, 2022, 65: 192206

31 Gao Z, Feng J. Research status of nonlinear feedback shift register based on semi-tensor product. Mathematics, 2022, 10: 3538

32 Lu J Q, Li B W, Zhong J. A novel synthesis method for reliable feedback shift registers via Boolean networks. Sci China Inf Sci, 2021, 64: 152207

33 Qi H. On shift register via semi-tensor product approach. In: Proceedings of the 32nd Chinese Control Conference, 2013. 208–212

34 Lu J, Li M, Huang T, et al. The transformation between the Galois NLFSRs and the Fibonacci NLFSRs via semi-tensor product of matrices. Automatica, 2018, 96: 393–397

35 Gao B, Liu X, Lan Z, et al. A novel method for reconstructing period with single input in NFSR. Chaos Solitons Fractals, 2018, 109: 36–40

36 Gao Z, Feng J, Yu Y, et al. On observability of Galois nonlinear feedback shift registers over finite fields. Front Inform Technol Electron Eng, 2022, 23: 1533–1545

37 Liu Z, Wang Y, Cheng D. Nonsingularity of feedback shift registers. Automatica, 2015, 55: 247–253

38 Lai X J. Condition for the nonsingularity of a feedback shift-register over a general finite field. IEEE Trans Inform Theor, 1987, 33: 747–749