SCFI: State Machine Control-Flow Hardening Against Fault Attacks

Pascal Nasahl
pascal.nasahl@iaik.tugraz.at
Graz University of Technology
Graz, Austria

Martin Unterguggenberger
martin.unterguggenberger@lamarr.at
Graz University of Technology,
Lamarr Security Research
Graz, Austria

Robert Schilling
robert.schilling@iaik.tugraz.at
Graz University of Technology
Graz, Austria

David Schrammel
david.schrammel@iaik.tugraz.at
Graz University of Technology
Graz, Austria

Rishub Nagpal
rishub.nagpal@lamarr.at
Graz University of Technology,
Lamarr Security Research
Graz, Austria

Stefan Mangard
stefan.mangard@iaik.tugraz.at
Graz University of Technology,
Lamarr Security Research
Graz, Austria

ABSTRACT
Fault injection (FI) is a powerful attack methodology allowing an adversary to entirely break the security of a target device. As finite-state machines (FSMs) are fundamental hardware building blocks responsible for controlling systems, inducing faults into these controllers enables an adversary to hijack the execution of the integrated circuit. A common defense strategy mitigating these attacks is to manually instantiate FSMs multiple times and detect faults using a majority voting logic. However, as each additional FSM instance only provides security against one additional induced fault, this approach scales poorly in a multi-fault attack scenario.

In this paper, we present SCFI: a strong, probabilistic FSM protection mechanism ensuring that control-flow deviations from the intended control-flow are detected even in the presence of multiple faults. At its core, SCFI consists of a hardened next-state function absorbing the execution history as well as the FSM’s control signals to derive the next state. When either the absorbed inputs, the state registers, or the function itself are affected by faults, SCFI triggers an error with no detection latency. We integrate SCFI into a synthesis tool capable of automatically hardening arbitrary unprotected FSMs without user interaction and open-source the tool. Our evaluation shows that SCFI provides strong protection guarantees with a better area-time product than FSMs protected using classical redundancy-based approaches. Finally, we formally verify the resilience of the protected state machines using a pre-silicon fault analysis tool.

CCS CONCEPTS
• Security and privacy → Hardware attacks and countermeasures.

KEYWORDS
Fault Attacks, Finite-State Machines, Control-Flow Integrity

1 INTRODUCTION
Fault attacks are active, physical attacks that allow an adversary to manipulate the execution of a digital circuit. In these attacks, one or multiple faults are injected into certain gates, wires, or registers of a logical hardware block. The effects of these faults, which comprise transient bit-flips or permanent stuck-at effects, manipulate the execution of the hardware block and an adversary can exploit this malfunctional behavior [23]. Finite-state machines (FSMs) are lucrative fault targets, as these fundamental hardware blocks are responsible for controlling systems and their datapaths. By hijacking the execution flow of the FSM using faults, an adversary can manipulate the FSM to enter states which cannot be reached from the current state. Hence, due to the severity of these attacks, security-sensitive state machines need dedicated protection against faults.

A common fault defense strategy is to encode the FSM states such that they are separated with a certain Hamming Distance [1, 4, 12]. However, this can only mitigate attackers aiming to induce faults into the state registers. Other defense strategies [6] introduce monitors which check whether the conducted state transition is in the list of valid state transitions. Leveugle et al. [11] dynamically verifies that the state transitions stay within the intended execution flow, which is determined during synthesis using the control-flow graph (CFG) of the FSM. There, on each state transition, a signature is derived, and a monitor checks whether the signature matches the predetermined signature of the CFG. However, faults induced either into the next-state logic or into the FSM’s control signals still enable adversaries to redirect the control-flow within the bounds of the CFG. Moreover, the fault detection latency of monitor-based schemes is high and the error coverage is often insufficient [18].

Redundantly instantiating the next-state logic and comparing the resulting states typically requires manual effort by the RTL designer. Moreover, this approach requires an additional redundant next-state logic for each additional fault protection layer. Hence, the area overhead of redundancy-based protection mechanisms scales poorly, especially when considering multi-fault attacks, e.g., quadruple laser fault injection [2].

Contribution
In this paper, we introduce SCFI, a scalable mitigation approach probabilistically protecting the control-flow of finite-state machines against multi-fault attacks. SCFI ensures that any control-flow deviation from the intended control-flow is detected with a high probability by substituting the unprotected next-state logic of the controller with a fault-hardened next-state logic. Internally, this hardened logic absorbs the control signals and the execution history and only generates a valid next state when these inputs are not
tampered by faults. When either the control signals, the current state (i.e., the execution history), or the next-state logic itself is targeted by faults, the logic ensures that these faults corrupt the next state output to a degree which can be detected. To ensure this behavior, SCFI uses a lightweight diffusion layer, which is based on a maximum distance separable (MDS) matrix multiplication. We integrate SCFI into the Yosys synthesis suite to automatically protect arbitrary FSMS against fault attacks without any user interaction and open-source the modified toolchain. In order to evaluate the area and timing overhead, we synthesized several FSMS used in an industry-driven open-source project with our modified synthesis suite. Our comparison with a redundancy-based protection approach of the FSM’s next-state logic shows that SCFI scales better in terms of area-time product for different fault protection levels than classical redundancy-based protection approaches. Finally, we utilize a pre-silicon fault analysis tool to formally verify the fault resiliency of the hardened FSMS.

2 BACKGROUND

This section provides fundamental background on fault attacks and finite-state machines required for the subsequent chapters.

2.1 Fault Attacks

Fault attacks are commonly used to break the security of embedded devices. In these physical attacks, one or multiple faults are induced into the circuit, causing several side effects at the electrical level. These electrical effects comprise timing violations and other disturbances [17] and they influence the execution of the target. By exploiting the effects of a fault, an adversary is capable of hijacking the control-flow of software [15, 20, 21], bypassing security measures, such as secure-boot [5, 22], or extracting secret keys used by cryptographic primitives [3, 7].

Originally, fault attacks were pure physical attacks requiring an adversary to have physical access to the target device. To induce a fault, attackers interrupt the supply voltage or the clock signal, decapsulate the chip and shoot with a laser directly into the die, or use electromagnetic pulses [10]. However, recent publications, such as Plundervolt [13], CLKSCREW [19], or VoltJockey [16], demonstrated that faults also could be induced remotely in software, increasing the attack surface of fault attacks even more.

In general, a fault \( f \in F \) is described using the set \( K = \{ e, s, t \} \), where \( e \) is the effect of a fault, \( s \) the spatial, and \( t \) the temporal dimension of the fault. Typically, the fault effect \( e \) comprises transient, i.e., bit-flips, or stuck-at effects. The spatial \( s \) and temporal \( t \) dimensions of a fault describe where (which gate or wire) and when (which clock cycle) a fault is induced. The set \( F \) consists of all possible fault combinations and an adversary typically can inject up to a certain number of faults into the circuit.

2.2 Finite-State Machines

Finite-state machines (FSMs) are sequential circuits responsible for controlling systems and their datapaths. Internally, an FSM maintains a finite set of states, and a state-transition into the next state that is controlled by the input signals, i.e., the control signals and the current state. The outputs of a Mealy-type FSM are defined by the current state and the input signals, and the outputs of a Moore-type FSM only depend on the current state.

As depicted in Figure 1, an FSM is described using the 5-tuple \( \{ S, X, Y, \phi, \lambda \} \). The \( |S| \) states of an FSM are represented as a \( s \)-bit symbol \( S \), where the size \( s \) needs to be at least \( s = \lfloor \log_2(|S|) \rfloor \) bits to comprise the entire state space. Furthermore, the FSM consists of \( n \)-bit control signals \( X \) and \( m \)-bit output signals \( Y \). The FSM uses the next-state function \( S_N = \phi(X, S_C) \) to derive the next state \( S_N \) from the current state \( S_C \) and the control signals \( X \). For a Mealy machine, the output \( Y \) depends on the current state \( S_C \) and the input signals \( X \) and is described using the output function \( Y = \lambda(X, S_C) \).

As depicted in Figure 1, an FSM is described using the 5-tuple \( \{ S, X, Y, \phi, \lambda \} \). The \( |S| \) states of an FSM are represented as a \( s \)-bit symbol \( S \), where the size \( s \) needs to be at least \( s = \lfloor \log_2(|S|) \rfloor \) bits to comprise the entire state space. Furthermore, the FSM consists of \( n \)-bit control signals \( X \) and \( m \)-bit output signals \( Y \). The FSM uses the next-state function \( S_N = \phi(X, S_C) \) to derive the next state \( S_N \) from the current state \( S_C \) and the control signals \( X \). For a Mealy machine, the output \( Y \) depends on the current state \( S_C \) and the input signals \( X \) and is described using the output function \( Y = \lambda(X, S_C) \).

As depicted in Figure 1, an FSM is described using the 5-tuple \( \{ S, X, Y, \phi, \lambda \} \). The \( |S| \) states of an FSM are represented as a \( s \)-bit symbol \( S \), where the size \( s \) needs to be at least \( s = \lfloor \log_2(|S|) \rfloor \) bits to comprise the entire state space. Furthermore, the FSM consists of \( n \)-bit control signals \( X \) and \( m \)-bit output signals \( Y \). The FSM uses the next-state function \( S_N = \phi(X, S_C) \) to derive the next state \( S_N \) from the current state \( S_C \) and the control signals \( X \). For a Mealy machine, the output \( Y \) depends on the current state \( S_C \) and the input signals \( X \) and is described using the output function \( Y = \lambda(X, S_C) \).
the general description of a state machine provided in Section 2.2. the adversary can achieve this goal by inducing faults into the next-state logic. A fault into the next-state logic allows an adversary to hijack the execution flow of the FSM and to indirectly change the output signals. This fault target can be modeled using the modified next-state logic 

FT1 State Registers: A fault into the state registers allows the adversary to arbitrarily redirect the control-flow of the FSM inside \( t \in \text{CFG} \) or outside \( t \notin \text{CFG} \) the control-flow graph. For the CFG in Figure 2, the adversary could flip bits in the state registers to directly jump from \( S_0 \) to \( S_1 \).

FT2 Control Signals: By inducing bit-flips into the control signals, the adversary can manipulate the control-flow of the FSM within the borders of the CFG. For example, a fault into the control signal \( x_0 \) or into the comparison logic can hijack the execution \( S_0 \rightarrow S_1 \) to \( S_0 \rightarrow S_2 \) in Figure 2.

FT3 Next-State Logic: When directly targeting the logic of the next-state function, the adversary can arbitrarily redirect the control-flow of the FSM within or outside the bounds of the CFG.

3.2 Goal - Fault Secure FSM

In order to comprehensively protect the control-flow of finite-state machines against fault attacks, dedicated fault countermeasures must consider all fault targets FT1, FT2, and FT3. The goal is that a fault-protected controller FSMF influenced by faults detects any control-flow deviations from the control-flow of an identical copy FSMF which is not affected by faults, i.e., \( \phi_F(S,X,F_N) =? \phi_F(S,X,0) \).

4 DESIGN

To comprehensively protect finite-state machines against control-flow hijacks, with SCFI, we maintain the integrity of the control-flow by introducing a fault-hardened next-state logic \( \phi_{FH} \). This hardened next-state logic prevents that a fault into FT1, FT2, or FT3 enables the adversary to redirect the control-flow inside or outside the boundaries of the CFG. This function \( \phi_{FH} \) is internally constructed using a multi-input signature register (MISR) and it links the entire execution history in a compressed format to detect control-flow deviations. To enter the next valid state, the execution history as well as the control signals need to be genuine. As shown in Figure 3, \( \phi_{FH} \) maps a valid tuple \( \{X,SC\} \), which includes the execution history in \( SC \), into a valid next state \( SN \). When an adversary induces faults into FT1...FT3, i.e., either into the tuple \( \{X,SC\} \) or into the \( \phi_{FH} \) logic, \( \phi_{FH} \) forces the FSM into a non-escapable terminal error state. Figure 4 depicts the transformation of an unprotected next-state logic of an example FSM.
4.1 Selection of the Hardened Next-State Function

In SCFI, we utilize a lightweight diffusion function used in cryptographic primitives for the hardened next-state function $\phi_{FH}$. The properties of this function imply that any fault at the input or within the logic maximally affect the output, thereby substantially decreasing probability of a successful fault attack. Figure 5 depicts the structure of $\phi_{FH}$ mapping the input space $\{S_{Ce}, X_e, Mod\}$ to a next encoded state $S_{Ne}$.

**Mix Layer.** In this layer, the input triple is split into $k$ $l$-bit vectors $L$. For this, the encoded current state, the encoded control signals, and the modifier are split into $k$ shares and each share is placed into the vectors, as shown in Figure 5.

**Diffusion Layer.** Then, in the diffusion layer, the vectors $L$ are absorbed by $k$ diffusion functions. These functions conduct a linear transformation $D(L) = M \cdot L$ which is a matrix multiplication of vector $L$ with matrix $M$ in a specific field. This transformation, depending on the choice of matrix $M$, yields a strong diffusion. Ideal choices of this matrix are called maximum distance separable (MDS) matrices, maximizing the diffusion property.

**Unmix Layer.** The output of the diffusion layer is stored into $k$ $l$-bit vectors. The concatenation of the first $k$-bits of each output vector results in the encoded next state $S_{Ne}$. As the size $k \cdot l$ of the output space is larger than the size $s_e$ of the encoded state, $k \cdot l - s_e$ bits are free. SCFI uses, depending on the required fault security, the topmost bits of each output vector as error detection bits $E$. Here, by choosing a corresponding modifier $Mod$, $\phi_{FH}$ sets these bits to a predefined value, i.e., 1. In the error logic, the logical AND of $S_{Ne}$ and $E$ infects the next state when a fault-induced error happens.

5 IMPLEMENTATION

We open-source a modified version of the Yosys [24] open synthesis suite capable of automatically protecting arbitrary FSMs with SCFI. The protection can be enabled globally or selectively for the unprotected FSMs in the design flow with a certain fault protection level $N$. Our implementation adds a new Yosys pass to the suite operating in between of other optimization passes before the design is mapped to the logic gate level. Note that the RTL designer only needs to manually encode the control signals with a Hamming Distance of $N$-bits in the modules driving these signals.

5.1 Next-State Logic

First, our custom FSM protection pass identifies the unprotected FSM by utilizing the existing Yosys FSM passes. Then, the FSM’s state variables are re-encoded so that the Hamming Distance between these variables is $N$. Afterwards, our pass extracts the CFG of the FSM and stores the current state, the next state, and the control signals for each control-flow edge. With this information, the modifier $Mod$ for state transition is determined, satisfying the equation $MDS(S_{Ce}, X_e, Mod) = S_{Ne}$.

For the MDS diffusion function, we use a lightweight construction with a minimal gate count proposed by Duval et al. [8]. As shown in Figure 6, this function splits the 32-bit input space into 4 8-bit chunks, performs the matrix multiplication, and returns 4 8-bit vectors which form the 32-bit output. In SCFI, we selected the $M^{8,3}$ [8] MDS matrix operating in the field $\mathbb{F}_2[\alpha]$ with $\alpha = X^8 + X^2 + 1$. This particular matrix has a low XOR count with a slightly larger logical depth compared to other matrices in the $4 \times 4$ category. We note that the choice of MDS matrix can be changed according to design requirements, i.e., area or timing constraints.

Having the modifiers, our pass describes the logic of the next-state function in the internal Yosys register-transfer level intermediate language (RTLIL). As depicted in Figure 7, first the active control signal $X_{active}$ is determined by performing a pattern match of the control signal and the current state $S_{Ce}$. Then, using this signal and $S_{Ce}$, the modifier for this input is selected. In the mix layer, the wires of the triple $\{S_{Ce}, X_{active}, Mod_{active}\}$ are distributed to the $k$ 32-bit input MDS diffusion functions. These
lightweight diffusion functions consist of only XOR gates. In the unmix layer, the next state \( S_{Ne} \) is concatenated and the error bits \( E \) are selected. By connecting \( S_{Ne} \) and \( E \) using AND gates, a fault infectively destroys the next state.

**6 EVALUATION**

To evaluate the effectiveness of SCFI in terms of area, timing, and security when protecting security-sensitive FSMs of an industry-driven project, we integrate our custom Yosys pass into the design flow of the OpenTitan [9] secure element. This chip, which is entirely open-source, acts as a secure root-of-trust and provides a key storage and cryptographic accelerators.

### 6.1 Area Overhead

In order to evaluate the area overhead introduced by SCFI, we analyzed unprotected (i), manually protected (ii), and automatically protected (iii) FSMs. As the reference (i) for our evaluation, we selected several FSMs of OpenTitan and synthesized the entire corresponding module with Yosys using the open-source Nangate45 standard cell library. For the manually protected (ii) FSMs, we encoded the control signals with a Hamming Distance of \( N \) bits and instantiated the next-state logic of the FSM \( N \) times. To detect control-flow hijacks triggered by faults, we designed a small error logic monitoring the state registers of the redundant FSMs and raising an error signal when one or more state values mismatch. Finally, we automatically protected (iii) the reference (i) FSMs by calling the SCFI Yosys pass in the design flow. Similar to the manually protected (ii) FSMs, we encoded the control signals with a HD of \( N \) bits and configured SCFI that at least \( N \) faults are required to hijack the FSM. Table 1 illustrates the area overheads for the three configurations for different FSMs and different protection levels \( N \) ranging from 2 to 4. For the manual redundancy approach, the geometric mean of the area overhead is 17.5 \% for \( N = 2 \), 42.9 \% for \( N = 3 \), and 67.6 \% for \( N = 4 \). In comparison, the geometric mean area overhead for the FSMs protected with SCFI is 9.6 \% for \( N = 2 \), 21.8 \% for \( N = 3 \), and 27.1 \% for \( N = 4 \). Note that for smaller input spaces \( \{ S_{Ce}, X_{Ce}, Mod \} \) the area overhead for SCFI could be higher than for a redundancy approach (cf. otbn_controller in Table 1) as SCFI needs to instantiate a MDS matrix with a 32-bit input.

**Table 1: Area overhead for protecting different FSMs using redundancy or SCFI.**

<table>
<thead>
<tr>
<th>Protection Level</th>
<th>Unprotected Area [GE]</th>
<th>Redundancy Area [%]</th>
<th>SCFI Area [%]</th>
</tr>
</thead>
<tbody>
<tr>
<td>adc_ctrl_fsm</td>
<td>1019</td>
<td>38</td>
<td>2</td>
</tr>
<tr>
<td>aes_control</td>
<td>632</td>
<td>38</td>
<td>2</td>
</tr>
<tr>
<td>ibex_fsm</td>
<td>2729</td>
<td>38</td>
<td>2</td>
</tr>
<tr>
<td>ibex_controller</td>
<td>537</td>
<td>38</td>
<td>2</td>
</tr>
<tr>
<td>ibex_lsu</td>
<td>933</td>
<td>38</td>
<td>2</td>
</tr>
<tr>
<td>otbn_controller</td>
<td>2857</td>
<td>38</td>
<td>2</td>
</tr>
<tr>
<td>pwrmgr_fsm</td>
<td>301</td>
<td>38</td>
<td>2</td>
</tr>
<tr>
<td>Geometric Mean</td>
<td>17.5</td>
<td>42.9</td>
<td>21.8</td>
</tr>
</tbody>
</table>

![Figure 8: Area-time product for the adc_ctrl fsm module in different configurations.](image)

### 6.2 Timing Overhead

SCFI affects the timing of the next-state logic by introducing the fault-hardened next-state function \( \hat{\phi}_{FH} \). However, the timing overhead is minimal, as the logical depth of \( \hat{\phi}_{FH} \) comprises four XOR layers for the MDS multiplication and an AND layer for the error masking. We successfully synthesized all modules in all configurations depicted in Table 1 for OpenTitan’s target frequency of 125 MHz with Yosys and the open-source standard cell library.

Figure 8 illustrates the area-time (AT) product for the unmodified, the redundancy-protected, and the SCFI-hardened adc_ctrl fsm module. In this plot, we increased the clock period from 3200 ps to 6000 ps and measured the area in kGE of the design synthesized by Cadence Genus and a proprietary cell library. For this experiment, we switched from Yosys to the Cadence synthesis suite as Yosys and the internally utilized yosys-abc tool only provides basic area and time optimization functionality. As shown in Figure 8, Cadence was able to meet the timing for a maximum frequency of 312 MHz for the base design, 308 MHz for the design using redundancy, and 294 MHz for SCFI. However, this slightly decreased frequency is typically not problematic, as the critical path of a design is usually not in an FSM. Moreover, as depicted, SCFI achieves a better AT product for protecting the next-state logic of the FSM in the adc_ctrl fsm module than the redundancy approach.

### 6.3 Security Evaluation

By encoding the control signals and the state variable, an adversary cannot hijack the state machine by inducing faults into fault targets \( FT1 \) and \( FT2 \). As the input pattern matching logic of \( \phi_{FH} \) operates on these encoded signals, the attacker needs to induce \( N \) faults into this block to manipulate the active, encoded control signal. While a fault into the modifier selection block \( \phi \), which consists of multiplexers, could select a different modifier, the attacker cannot exploit this injected fault. More specifically, a fault would yield a combination of control signal, state, and modifier which creates a non-valid next state. Internally, the mix layer consists of a rewiring of the encoded control signals, the state, as well as the modifier. Hence, this layer can resist up to \( N = 1 \) faults. The idea of the diffusion layer is that a small change at the input causes a significant change at the output, i.e., the avalanche effect. To achieve this property, SCFI internally uses MDS matrix multiplication yielding optimal diffusion guarantees. These MDS matrices propagate a bit-flip in a single input byte to all four output bytes, i.e., they have a branch number of 5. Hence, one or multiple bit-flips into the input triple \( \{ S_{Ce}, X_{active }, Mod_{active} \} \) propagate through this function affecting multiple output bits. By effecting
the next state $S_{C_{E}}$ or the error bits $E$, an invalid state is generated in the unmix; and error $E$ layer and the FSM enters the default error state. Precisely, there are only $|S_{C_{E}}| + |E|$ valid output states; an attacker who induces $N$ faults on the next-state function inputs, $(X, S_{C})$, would have a success probability of $P = \frac{|S_{C_{E}}| + |E|}{k^{2|S_{C_{E}}|+|E|}}$. However, considering that $|S_{C_{E}}| + |E| < \kappa \cdot 2^{32-\ell(S_{C_{E}}+|E|)}$, the success probability is very small. For attacks within the next-state function, the MDS property of the diffusion layer ensures that the success probability still remains quite low, albeit it is higher than the previous case. As shown in Figure 6 depicting the construction of the MDS matrix, faults in the first three XOR layers propagate to at least two output bytes. Although a fault at the last layer only affects one output byte, all valid output states $S_{O}$ are still encoded with a Hamming Distance of $N$, requiring that the adversary needs to induce $N$ bit-flips.

6.4 Formal Security Analysis

We formally analyzed the resilience of the diffusion layer consisting of the MDS matrix multiplication by utilizing SYNFI [14], a recently introduced pre-silicon fault analysis tool operating at the netlist. For the analysis, we synthesized an FSM with 14 state transitions and configured SCFI with a protection level of 2 bits (HD). We used SYNFI to analyze whether it is possible to hijack one of the state transitions and enter another next state using faults. In total, we injected 7644 single bit-flips exhaustively into all available gates in the MDS matrix multiplication and 32 (0.42 %) of these faults enable an adversary to hijack the execution-flow of the FSM.

Note that analyzing the resilience of FSMs against faults is also necessary when using other protection approaches. For example, when redundantly instantiating the next-state logic to mitigate faults, a synthesis tool aiming to meet timing and area constraints could weaken the security when optimizing the design.

7 LIMITATION & FUTURE WORK

A potential future work could extend SCFI to adapt the MDS matrix size to the size of the $(S_{C}, X, Mod)$ input triple to further improve the area-time product. In addition, the formal analysis could be integrated into the Yosys pass to increase security guarantees of SCFI. Finally, a future work could investigate how SCFI could be extended to also provide protection for the output logic.

A limitation of the current prototype implementation is that the selector signals of the MUXes used in the input pattern matching logic are 1-bit signals. This would allow an adversary to redirect the control-flow within the bounds of the CFG. To mitigate this attack vector, an updated version of the SCFI Yosys pass could introduce encoded selector signals.

8 CONCLUSION

In this paper, we presented SCFI, a methodology capable of protecting the control-flow of finite-state machines against fault attacks. SCFI substitutes the next-state logic of FSMs with a fault-hardened function only deriving a next valid state in a fault-free scenario. We integrated SCFI into the Yosys synthesis suite and open-sourced our modified toolchain. Our evaluation shows that the area overhead for FSMs protected with SCFI is lower than for traditional protection approaches.

ACKNOWLEDGMENTS

This project has received funding from the Austrian Research Promotion Agency (FFG) via the AWARE project (grant number 41091245).

REFERENCES


