TAMED: Transitional Approaches for LFI Resilient State Machine Encoding

Muhtadi Choudhury*, Minyan Gao*, Shahin Tajik‡, and Domenic Forte*
* University of Florida, Gainesville, FL, USA
‡ Worcetser Polytechnic Institute, Worcester, MA, USA

***Abstract*—Finite state machines (FSMs) control the behavior of sequential circuits, including access to privileged states and sensitive information. Laser-based fault injection (LFI) is a precise method where an adversary breaks the chip security by altering the values of individual flip-flops (FFs) with a laser beam. To understand LFI, different laser models, e.g., bit flip, bit set, and bit reset, have been developed. Existing countermeasures can improve FSM resiliency, but either generate multiple LFI resilient encodings applicable only to certain models, or are too conservative, thus incurring significant overhead. In this paper, we introduce the transition-based encoding CAD framework (TAMED), which offers greater flexibility by precisely generating a single optimized FSM encoding that is resilient to multiple LFI models. Predicated on linear programming, TAMED introduces Transitional Vulnerability Metrics that can quantify susceptibility of FSMs based on the bit flip model and the set-reset models. TAMED is demonstrated on 5 benchmarks and outperforms other FSM encoding schemes in terms of security and overhead.**

I. Introduction

Laser fault injection (LFI) is the most effective technique for inducing precise faults at high resolution (a byte or even a bit) [1]. Unlike other fault attacks, LFI enables effectuating an accurate fault for a specific duration maintaining both spatial and temporal accuracy [2], [3], [4]. Experiments on LFI demonstrate data dependent and data independent fault models, i.e., bit reset-set models and bit flip model, respectively. A bit reset (resp. a bit-set) models a fault that transitions the target bit from 1 to 0 (resp. from 0 to 1). However, if the current state of the bit is already at 0 (resp. 1 for bit-set) there is no effect. A bit-flip corresponds to a fault irrespective of the current state of the faulted bit. Contemporary research highlights *laser-sensitive areas* of a D flip-flop (DFF) showing that the validity of data-dependent bit-set/reset as well data-independent bit-flip fault models [5], [6]. In addition, the well defined laser-sensitive areas can be utilized by attackers for more integrated technology nodes [6]. It is thus extremely important to incorporate precise sensitive areas of the fault models when devising countermeasures for LFI as it has also been shown that even hitting a few transistors with a relaxed (imprecise) spot size can inflict useful faults – and that there is no intrinsic protection against LFI even at nanoscale technology nodes [3].

Existing countermeasures against LFI such as hardware irradiation sensors [4] provide relief but their expensive manufacturing steps make logical circuit-based approaches more appealing. In contrast, CAD tools can automatically incorporate logical approaches (e.g., FSM redundancy or security-aware encoding [7], [8]) to secure the FSM. A similar direction adopts *state exploration* with coding theory- based techniques where each of the FSM states is regarded as a linear or nonlinear codes, and standard error correction/detection improves FSM resiliency; however, state exploration leads to significant overhead in terms of chip area, power consumption, and performance penalties as this assumes *all the states* need uniform protection. More efficient state exploration techniques engendering LFI resistant encoding for arbitrary FSM sizes and number of lasers have recently been put forward in the literature, namely PATRON and SPARSE [9], [10]. These approaches in contrast to coding theory-based are less conservative, i.e., they only protect security-critical states in the FSM. However, they cannot *automatically* incorporate the precise laser sensitive areas to differentiate between the data-dependent bit-set/reset as well data-independent bit-flip fault models, where the direction of the FSM transition is secured rather than a state.

An ingenious attacker can always utilize the laser sensitive areas in a design to compromise the security of these complex SoCs, particularly if there is no resiliency in the design. Hence, considering all the contrasting design requirements of low power usage, high performance, diminished area, while maintaining proper security, we introduce TAMED (Transitional Approaches for LFI Resilient State Machine EncoDing) which makes the FSM inherently tolerant to precise LFI sensitive areas. TAMED employs Linear Programming (LP) to automatically generate an optimized encoding that protects only the critical transitions in the FSM (in contrast to the conservative state exploration schemes). Particularly, our contributions are:

- TAMED provides completely *automated* generation of LFI-resistant state encoding. Through the use of LP, TAMED can identify a single, LFI-resistant encoding *without any manual input.*
- TAMED's LP also offers flexibility to incorporate customized security criteria. To demonstrate this, a mechanism to *protect critical transitions from both the data dependent and data independent models* is added.
- Through LP, TAMED allows for additional overhead and/or security related optimizations. Specifically, the LP objective function *minimizes switching activity* and hence the FSM's dynamic power consumption [11].
- TAMED is demonstrated on 5 controller benchmarks and we compare its security and overhead to other state encoding schemes including PATRON. The *Transitional Vulnerability Metrics* (*TVM*) are also proposed to distinguish TAMED with the state exploration approaches in terms of vulnerability exposure to faults based on data dependent and independent models.

An outline for the rest of the paper is as follows. In the next section, we discuss basic notation and common terms, FSMs, and a motivating example of fault injection on an FSM. In Section III, the LFI fundamentals and flip-flop sensitivity are described and used to constitute a realistic threat model and to explain precision of transitional approaches. One of our proposed metrics is also introduced. Section IV provides the TAMED methodology which incorporates the description of the precise model, salient parameters and types of transitions along with another proposed metric leading to the comprehensive encoding framework and associated optimization procedures. Results are presented and discussed in Section V. Finally, conclusions and future work are given.

II. Background and Related Work

A. Basic Notation and Common Terms

We use blackboard bold fonts with upper case letters, e.g., $\mathbb{S}$, to represent sets. Upper case and italic font with one or no subscripts denote an element of a set, e.g., S_i or S. Vectors are denoted by lower case with arrow, e.g., $\vec{v}$, while elements of a vector are written in lower case with a subscript, e.g., v_i. The shorthand notation for a subset of elements i to j of a vector $\vec{v}$ is $\vec{v}_{i:j}$. A difference or relationship between the ith and jth elements is denoted with a subscript ij. The operator $|\cdot|$ denotes the cardinality of a set or vector. Scalar variables may be upper case or lower case with italic fonts.

B. FSM and Encoding

An FSM is defined as a 5-tuple $(\mathbb{S}, \mathbb{I}, \mathbb{O}, \varphi, \lambda)$, where $\mathbb{S}$ is a finite set of states, $\mathbb{I}$ is a finite set of input symbols, $\mathbb{O}$ is a finite set of output symbols, φ is the next-state function and λ is the output function. $|\mathbb{S}|$ is the total number of states in the FSM. Typically, an FSM is depicted as a directed graph $\mathcal{G} = (\mathbb{S}, \mathbb{T})$ where each state $S \in \mathbb{S}$ represents a vertex and each edge $T_{ij} \in \mathbb{T}$ represents a transition or edge from state S_i to the state S_j.

In the FSM, each state should only be accessed from its *accessible set of states*, i.e., $A(S_j) = \{S_i \mid T_{ij} \in \mathbb{T}\}$. In [7], a designer specifies a set $\mathbb{P}$ of *protected states* and a set $\mathbb{AU}$ of *authorized states*. A transition from state $S \in \mathbb{AU}$ that is allowed access to $\mathbb{P}$, such that $A(\mathbb{AU}) = \{P \mid P \in \mathbb{P}\}$ is referred to as an *authorized transition* ($\mathbb{AT}$) in this paper. In other words, authorized transitions can only occur when the current state is an authorized state and the next state is the protected state; the direction of the edge in AT is always from $\mathbb{AU}$ to the $\mathbb{P}$. In recent work relating to LFI resilient FSMs that consider only bit flip model [9], [10], a state exploration scheme is chosen where *all normal states* ($\mathbb{NS}$) are secure from the *sensitive states* ($\mathbb{SS}$) defined as $\mathbb{NS} = \{S \in \mathbb{S} \mid s \notin \mathbb{AU} \cup \mathbb{P}\}$, $\mathbb{SS} = \{S \in \mathbb{S} \mid s \in \mathbb{AU} \cup \mathbb{P}\}$, respectively. In other words, $\mathbb{NS}$ is extraneous as far as $\mathbb{AT}$ is concerned.

FSM state encoding assigns a distinct binary pattern $\in \{0,1\}^n$ for each state where n is the number of state flip-flops (FFs). There are two traditional encoding techniques, which are both vulnerable to LFI [7]. In *binary encoding*, states are assigned in a binary sequence starting from 0. In *one-hot encoding*, only one bit of the state variable is allowed to be '1' while all others are set at '0' for every state in the FSM. For this scheme, $n = |\mathbb{S}|$, where the total number of state FFs is understandably greater than that of binary encoding.

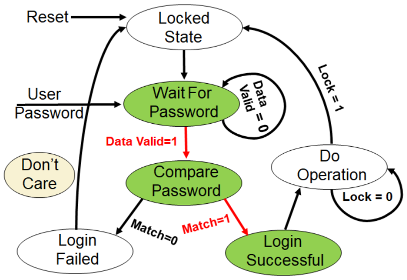


Fig. 1: A password checking FSM where the fault causes an incorrect password to be accepted.

C. Fault Injection Against FSMs

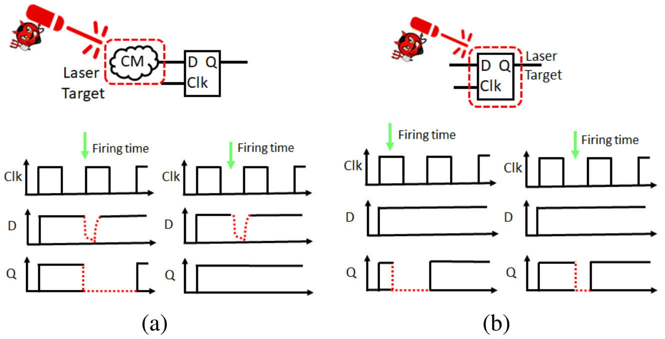
The potency of fault injection attacks is illustrated using a simple state transition diagram of a password authentication FSM in Fig. 1. The FSM constitutes 6 states: 'Locked State', 'Compare Password', 'Wait For Password', 'Login Failed', 'Login Successful' and 'Do Operation'. After reset, the system commences in Locked State. In the next clock rising edge, the system transitions to Wait For Password and remains there until the user inputs a password. Compare Password compares the user password with the system password. The assumption is that only authorized users know the correct password. If passwords mismatch, the FSM transitions to Login Failed and later returns to Locked State. If passwords match, the user can successfully log into the system and transition to Do Operation. The user can later return the FSM to Locked State.

In this FSM, the primary goal is to not let any malicious user bypass the password comparison protocol and transition to Login Successful, whereby system access is granted. Hence, the most critical transition for the FSM designer is the transition corresponding to 'Match=1'. The designer must also make sure the FSM transitions to Compare Password for every user to validate their inputs; bypassing this transition can also lead one step closer to illegal/unauthenticated system access. Hence, any fault injection leading to successful execution of these two transitions would allow the adversary to bypass the authentication mechanism provided by the protocol.

III. Threat Model and LFI Fundamentals

A. Proposed Threat Model

The scope of our threat model is detailed using the extensive definitions and updated fault models from recent work [12], [13]. Circuits can be divided into combinational logic (CM) gates $\eth_{cm}$ and state elements $\eth_s = \{FF\}$. All the relevant valid gates then becomes, $\eth = \eth_{cm} \cap \eth_s$, expressed in one set. An attacker is represented by a function $\zeta(f, t, l)$ where f is the total number of fault events (spatial and temporal components), t describes the fault types (bit flip, reset, and set), and l denotes the fault location(s) in a digital logic circuit. A net in the circuit suffers from a bit set (or bit reset) if it can be changed only from state 0 to state 1 (or state 1 to state 0) whereas the bit flip model inverts the net's value regardless of its current state. When considering f, any fault injection might be limited in spatial or temporal dimensions (*univariate* or *multivariate*). Spatially, the attacker may be limited in the number of fault injections that can occur simultaneously in the same clock cycle. Univariate fault



(a) (b)

Fig. 2: LFI on (a) combinational (CM) and (b) flip flop (FF). Regardless of the LFI time or input combination set, direct target of FF is more likely to induce a fault.

injections only consider fault events occurring in the same clock cycle, whereas multivariate fault injections occur in different clock cycles.

The two possible ways in which lasers can engender faults in state elements are *Single Event Transient (SET)* and *Single Event Upset (SEU)* as shown in Fig. 2. In SET, the laser is aimed in the combinational logic part of the design and a fault transient propagates to the memory cell within the memorization time window. For SEU, the logical value is instantaneously flipped; the laser directly hits the memory cell and there is no time delay involved for the bit-flip. *Multiple bit upsets* occur when a single laser beam overturns several state FFs simultaneously – the predominant reason can be attributed to *uncontrolled* laser strikes to peripheral circuits on the memory chip or circuit miniaturization [14].

A pertinent concept related to faults in state elements is *masking* [15], [16]. Masking can be simply defined as the set of components that control the success rate of transient faults, i.e., fault propagation through combinational logic. The masking types are electrical, logical, and latching-window masking that can impede the fault propagation to the FF inputs. *Electrical masking* is predicated on the fault characteristics (i.e., amplitude, duration, and time of strike) and the features of the gates that the fault is propagating through. By the time the fault is at the input of the memory element, fault attenuation may have resulted in waning of the fault duration and amplitude such that its features are not significant anymore to effectuate a bit fault. The effect of process variations on error rate is also increasing with miniaturization and thus they substantially impact glitch attenuation and hence electrical masking [17], [18]. *Logical masking* impedes the transient fault propagation if there is a controlling value at the other input of the gate. Finally, *latching-window or timing masking* is contributed in the circuit due to the *memorization* time window component as the fault can *only* be latched in a memory cell or an element if it satisfies the setup and hold time constraints.

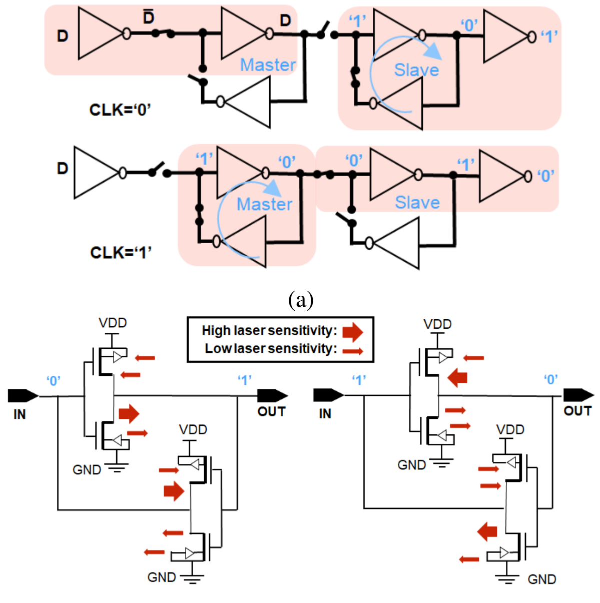
As it can be seen form the above discussion, Fig. 2(b) is resistant to all these masking factors. Thus, in this paper, we focus on direct memory units as targets so our threat model does not suffer from a level of uncertainty determined primarily by the unpredictable nature of these masking probabilities. Further, our threat model is regarded as one of a strong attacker who has physical access to the device and a high-precision LFI setup. Typically, in a laser attack, the attacker can maneuver the beam's diameter, wavelength, impact coordinates, amount of emitted energy and the duration of exposure. Additional controllable options include: moment of impact (synchronizing hit with respect to certain clock cycle), V_{cc}, target clock frequency, and temperature. More precisely, the assumptions are summarized below:

1) *Targets and knowledge of FSM:* In our threat model, we restrict the target set to state elements, i.e., $\eth = \eth_s = \{FF\}$ because they are more probable to be successful according to Fig. 2. Overturning a FF by direct strike does not depend on successful propagation along its fan-in and/or timing of the laser within a clock cycle. Also it is assumed that the attacker is well informed of the FSM features and the state encoding. It is possible to obtain all this intelligence through reverse-engineering or an insider.
2) *Bi/Unidirectionality of bit flips:* For at least a few experimental settings, errors are seen to be unidirectional [19]. This implies that certain bits in the design may not be of the same probability to fault to either of the logic ('0' vs. '1'). Such experimental observations lead to the accurate models referred to as "bit set" or "bit reset." In this paper, both unidirectional and bidirectional models have been considered. Hence, our countermeasures can protect faults in either direction or both directions.
3) *Number of concurrent faults and their locations:* We assume without the loss of generality that the adversary can accurately and concurrently overturn up to x number of state FFs in single clock cycle. In reality, x is contingent upon the number of lasers in the LFI setup and the relative FF locations in the IC layout [1]. This underscores the feasibility to precisely and reproducibly alter even the single memory cells like pointers, counters, flags, etc., that can potentially steer the program control flow. Hence, our threat model is generalized so it can be applied to more constrained conditions.
4) *Temporal dimensions:* Following the above notation, the attacker model $\zeta(f, \tau_{set-reset/bf}, \eth)$ [13] represent any number of fault(s) in *univariate*, set-reset or bit-flip model on any FF locations in the circuit design.

B. LFI Sensitivity of Flip-Flops

1) D Flip-Flop Operation: The most common approach for constructing an edge-triggered D flip-flop (FF) is to use a master-slave latch configuration [20] as shown in Fig. 3(a). When the clock signal is low ($CLK = 0$), the master latch is "transparent" and allows the input D to pass to its output. At the same time, the slave latch is in "hold" mode, keeping its previous value at the output of the FF (Q) using positive feedback. When the clock transitions to logic high ($CLK = 1$), the master and slave latches switch to hold and transparent modes, respectively. The value at the FF output Q becomes the last value of input D before the rising edge of the clock.

2) SEU Sensitive Regions of Flip-Flop: A laser strike to a reverse-biased PN junction, induces a parasitic current, known as a *photocurrent* [5]. Fig. 3(b) shows a basic latch design maintaining logic '1' and '0' on the left and right, respectively, while in hold mode. It also shows the PN junctions



(a)

(b)

Fig. 3: (a) D flip-flop operation for logic low and high clock signal. Orange regions highlight the active circuits and blue semi-circle indicates a latch in hold mode; (b) Laser sensitive areas (large red arrows) in master/slave latches that can lead to SEUs when latch outputs are logic '1' and '0'.

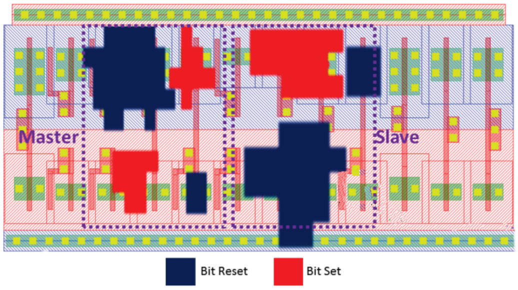


Fig. 4: Experimental results showing the sensitivity map on a D Flip-Flop with laser stimulation [5].

of the cross-coupled inverter pairs within these master/slave latches that are most sensitive to laser strikes. Arrow direction indicates the direction of photocurrent between drain/source and bulk while thicker arrow indicates larger photocurrent. On the left, a laser strike on the NMOS drain of the top inverter or on the PMOS drain of the bottom inverter can cause the FF state to invert from '0' to '1' at the output. On the righthand side of Fig. 3(b), it is the PMOS drain of the top inverter or on the NMOS drain of the bottom inverter that are more sensitive to laser strikes. Note that a SEU occurrence ultimately depends on many parameters of the attack including laser spot size, power, pulse duration, the focus of the laser beam, spatial parameters (location, geometry, wafer thickness), and the PN junction voltage biasing. The most updated electrical model considering very short laser pulse durations with a thin spatial accuracy to identify sensitive areas for a recent CMOS technology is presented in [5]. The sensitive areas are revealed by cartographies measurement and confirmed by proper electrical simulations that take into account the topology of the target as shown in Fig. 4. We elaborate on the topological sensitivity map at the beginning of the next section.

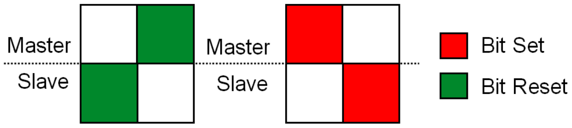


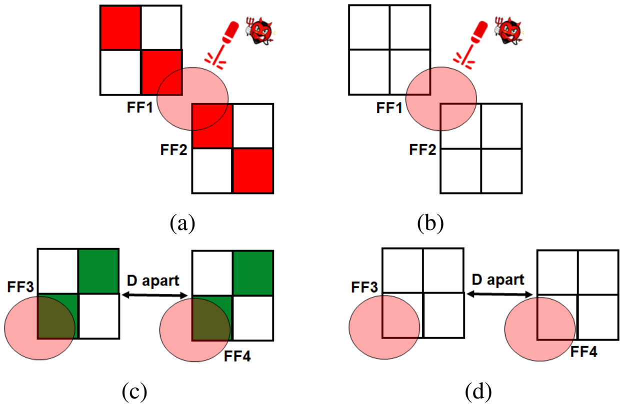
Fig. 5: Simplified representation of sensitive areas in a D Flip-Flop (DFF). Master and slave portion in the area are segregated to appreciate the relative orientation in the latches. Sensitive areas for a bit reset (left) and for a bit set (right).

C. Transitional Approaches and FSM vulnerability

In this section, we begin by introducing the bit set and bit reset models and then comparing *transitional* FSM protection approaches to the *state*-based FSM protection approaches. Transitional approaches refer to the countermeasure developed precisely for $\mathbb{AT}$ considering the different sensitive regions of FF, i.e., bit set and bit reset models whereas state-based approaches correspond to the countermeasure developed with state exploration schemes considering $\mathbb{SS}$ and the bit flip model. We illustrate the need for transitional approaches by showing how the security can be affected when only the latter approach is considered. Then, we describe a subset of the types of transitions that can be efficiently handled by TAMED along with encoding examples. Finally, a novel metric named Transitional Vulnerability Metric (TVM) is proposed. From this point forward, we refer to the bit set or the bit reset as the set-reset model.

1) Bit Set and Bit Reset: The topological sensitivity results of laser stimulation experiment on a D Flip-Flop (DFF) [5], is represented in this paper in Fig. 5 for simplicity. The sensitivity map for bit reset and bit set depict approximate sensitive regions in the master and slave latches. This means that only through the precise laser beam, incident on the bit reset (bit set) sensitive regions on the DFF, an instantaneous '1' to '0' ('0' to '1') SEU may be achieved. This however implies that the assumption of the instantaneous overturning of the states '1' and '0' in the bit flip model on any portion of the FF layout may not be always correct as we see below.

2) Precision of Transition-based Approaches vs. Bit Flip Model: A few recent papers propose countermeasures against LFT considering the bit flip model [9], [10]. It is important to incorporate the localization of the sensitive regions on the DFF layout as assuming general bit flip model when devising countermeasures against LFI may result in consequential error. Fig. 6 illustrates possible scenarios in which consideration of the more precise set-reset model than the bit flip model becomes crucial. For Fig. 6(a) and (b), let's assume that the protected state set $\mathbb{P} = \{11\}$ and the transition from the state $\{01\}$ to $\mathbb{P}$ is authorized. Considering the current state for $FF_{1:2}$ as $\{01\}$ under set-reset model, the next state is $\{11\}$ which is in $\mathbb{P}$. However, under bit flip model the next state comes to $\{10\}$, as each of the state in $FF_{1:2}$ is overturned. If the FSM has a security mechanism to detect the AT to the P, it can be inferred that only the set-reset model can precisely recognize $\mathbb{AT}$ and bit flip model does not. For Fig. 6(c) and (d), let's assume that $\mathbb{P} = \{11\}$ and the transition from the state $\{00\}$ to $\mathbb{P}$ is authorized, i.e., $\mathbb{AU} = \{00\}$. The $FF_{3:4}$



(a) (b) (c) (d)

Fig. 6: Comparison between set-reset and bit flip models under the same attack setting. (a) Set-reset model showing a laser is incident on the bit set sensitive regions of $FF_{1:2}$; (b) Bit flip model for the same attack setting as (a); (c) Set-reset model showing two laser beams incident on the bit reset sensitive regions of $FF_{3:4}$ slave latches respectively; (d) Bit flip model for the same attack setting as (c).

are assumed at an interdistance, D as required by possible countermeasures against LFI [10]. Considering the current state for $FF_{3:4}$ as $\{00\}$, under set-reset model the next state remains at $\{00\}$. However, under bit flip model the next state comes to $\{11\}$, which is the $\mathbb{P}$. In this case, it is observed that the bit flip model is providing false positives, i.e., claiming an AT has occurred, where in reality no transition has occurred. All of these scenarios can pose grave security risk, e.g., FSM from an encryption module. In light of these examples, it can be understood that the order of nodes in the $\mathbb{AT}$ is critical to develop precise countermeasure for set reset model something that is lacking in the state exploration approach where direction of edges is overlooked. However, security analysis of bit flip model has been included in this paper as it is shown to be relevant in some cases and it can still be induced along with primarily the precise bit set and bit reset faults [21].

3) Transitional Vulnerability Metric (Bit Flip Model): Consider an authorized transition between states s_i and s_j which are encoded to binary values of i and j, respectively. Let $HD(a, b)$ denote the Hamming distance between two binary strings a and b. In our threat model, if $HD(i, j) \leq x$, $s_i \in \mathbb{AU}$, and $s_j \in \mathbb{P}$, then the FSM may be exploitable by LFI in one clock cycle. Note that although the order of states in the transition is unimportant for bit flip model, symbols $\mathbb{AU}$ and $\mathbb{P}$ still represent the originating node and terminal node in order to maintain uniformity with the set-reset model. We define a subset of transitions $\mathbb{VT}_{x_{bf}} \subseteq \mathbb{T}$ as

$$\mathbb{VT}_{x_{bf}} = \{(s_i, s_j \in \mathbb{T}) |\ s_i \in \mathbb{AU}\ , HD(i, j) \leq x,\ s_j \in \mathbb{P}\} \quad (1)$$

where $\mathbb{VT}_{x_{bf}}$ represents the set of transitions vulnerable to x faults due to the bit flip model. Clearly, the goal for our fault tolerant scheme should be $|\mathbb{VT}_{x_{bf}}| = 0$. For instance, if $|\mathbb{SS}| = 3$ for an FSM with $x = 1$, $s_i = \{000\}$, $s_j = \{001\}$, and $s \notin (s_i \cup s_j) = \{010\}$, then the AT between s_i and s_j is not secure as $HD(i, j) \leq x$. However, if under the same attack setting, $s_i = \{010\}$, $s_j = \{001\}$, and $s \notin (s_i \cup s_j) = \{000\}$, then AT is secure and $|\mathbb{VT}_{x_{bf}}| = 0$.

To aid our security analysis, a novel metric named *Transitional Vulnerability Metric* (TVM) is proposed in this paper. In this case, $TVM_{bf}(x)$ denotes sensitivity of the metric to only the bit flip model.

$$TVM_{bf}(x) = \frac{|\mathbb{VT}_{x_{bf}}|}{|\mathbb{T}|}. \quad (2)$$

where $0 \leq TVM_{bf}(x) \leq 1$. The desired value of $TVM_{bf}(x) = 0$, which means there are no vulnerable transitions due to bit flip in the FSM. Intuitively, $TVM_{bf}(x)$ is the percentage of transitions where x bit flip faults can lead to states in $\mathbb{P}$ not being accessed from states in $\mathbb{AU}$. Note that a transitional vulnerability metric for the bit set-reset models will be introduced in Section IV-C.

IV. TAMED Methodology

A. Precise Set-Reset Model

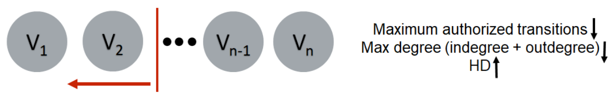
In this section, we will illustrate the protection scheme in TAMED which originates from secure bit transitions according to FF orientation and arrangement and leads to the countermeasure safeguarding an FSM's AT for the precise set-reset model. It is important to note that the *order* of the states in the transition matter in this model, i.e., the direction of the edge is always from $\mathbb{AU}$ to $\mathbb{P}$ in the authorized transitions.

Security FFs: The TAMED methodology for set-reset model requires that $\mathbb{AU}$ and $\mathbb{P}$ states generation follow specific procedures. If Fig. 6(a) is considered as the current attack scenario, then precisely the bit set portions of the $FF_{1,2}$ are only targeted. This essentially means that transitioning to other states from the possible current state, say $\mathbb{AU} = \{00\}$ can be possible with LFI. If the corresponding P is any of the states in the set $\{01, 10, 11\}$ then $TVM \geq 0$ and a vulnerability exists in the FSM. It can be interpreted from the above example that, if the laser is on the set sensitive portion on a DFF, a current state bit '0' under the set-reset model in $\mathbb{AU}$ can be utilized by the attacker to get to a state P. Hence, a current state of $\mathbb{AU} = \{11\}$ and $\mathbb{P} = \{00\}$ in this case $(x = 1)$ can be considered secure as it prevents any FF overturning of the states due to the LFI attack. In the same way, had it been the individual bit reset portions of the $FF_{1,2}$ that were targeted with the same laser setting $(x = 1)$ then any of the states in $\{01, 10\}$ as the current state, $\mathbb{AU}$ can be made vulnerable $(\mathbb{P} = \{00\})$. Specifically, if the laser is on the reset sensitive portion on a DFF a current state bit '1' in $\mathbb{AU}$ can be utilized by the attacker to get to a P. Hence, an $\mathbb{AU} = \{00\}$ and $P = \{11\}$ in this case $(x = 1)$ can be considered secure.

In summary, the basis of security in the TAMED methodology comes from the bit transitions from AU to P respectively, i.e., a requirement of $1 \rightarrow 0$ for bit set model and a requirement of $0 \rightarrow 1$ for bit reset model. In this paper, we refer to these security bits in the encoding that correspond to satisfying the secure bit transitions constraint as *security bits* and the corresponding FF set as *security FFs* ($\mathbb{SFF}$). For each of the AT considered in TAMED, the $HD \geq x$ constraint is ensured on these $\mathbb{SFF}$ for appropriate protection.

B. Salient Parameters in TAMED and Types of Transitions

Parameters: From Section II-B, an FSM is represented by vertices and edges. Let $n = |\mathbb{S}|$ and each state in $\mathbb{S}$ be represented by a vector of length n: $[v_1, v_2, \ldots v_n]$, $v_i \in \{0, 1\} \forall i$,



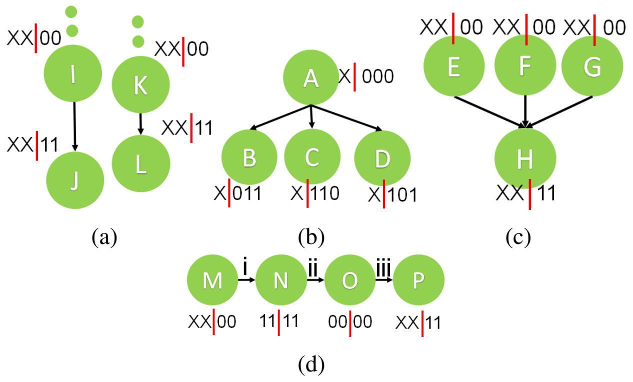
V1
V2
Vn-1
Vn
Maximum authorized transitions↓
Max degree (indegree + outdegree)↓
HD↑

Fig. 7: Relationship between salient parameters of transitional approach with the increase of security bits/FFs.

where v_i represents the variable associated with the i^{th} FF in the FSM. As a convention (without loss of generality), we assume that $m = |\mathbb{SFF}|$ rightmost bit positions of the vectors correspond to $\mathbb{SFF}$, unless otherwise stated. For example, the $\mathbb{SFF}$ correspond to $[v_{n-m+1}, \ldots, v_n]$ (shorthand, $\vec{v}_{n-m+1:n}$) for states in $\mathbb{S}$. These variables are illustrated in Fig. 7 along with the different salient parameters for encoding optimization in the TAMED methodology.

It can be seen that the vertical red demarcation line divides the $\mathbb{SFF}$ from the rest of the FFs. As previously mentioned, the convention is to assume that the requirement of the $HD \geq x$ is to be satisfied with the $\mathbb{SFF}$. For the lefthand side, the convention is to assume don't care bits (denoted by X), unless otherwise stated. Due to our desired switching activity (dynamic power consumption) minimization procedure of the FI-resistant FSM, it is important to incorporate as many Xs in the state encoding as possible so there is more room for optimization. As the demarcation line moves from right to left, intuitively the maximum number of authorized transitions that can be incorporated into the FSM will decrease. One way to visualize this is as the number of Xs decrease, there's less possible ways in which the encoding can be varied with 0 or 1. For example, the $|\mathbb{AT}|$ achievable in '$XX00 \longrightarrow XX11$' is more than '$X000 \longrightarrow X111$' for an LFI capability $x = 1$. The HD capability will also increase with more $|\mathbb{SFF}|$, simply because the number of the security bits increases. The parameters *indegree* and *outdegree* are important as they may require higher n for certain HD requirement in $\mathbb{AT}$. For a vertex, the number of head ends into the vertex is called the indegree and the number of tail ends from the vertex is its outdegree. Naturally, the capacity to incorporate higher degrees (indegree and outdegree) of a vertex is expected with more Xs. This shall be shown by specific examples below.

Transition types and examples: Fig. 8 illustrates a subset of AT along with examples of corresponding state encodings that TAMED can incorporate. It should be noted that as for all these examples $x = 1$ is considered, a minimum $HD = 2$ between any of the transitions ensure security, i.e, a $HD = 2$ between the security bits in each transition. The two transitions in Fig. 8(a) are part of the same FSM and it can be seen that there is room for optimization with Xs for $n = 4$ and a constant $HD = 2$ in the security bits. A shift of the demarcation line for the outdegree of vertex A in Fig. 8(b) means less Xs for the same HD in the security bits and hence less combinations of the transitions possible, e.g., $0000 \longrightarrow \{0011, 0110, 0101\}$ is a qualifying example. Another shift of the line to the original position is necessary for the indegree of vertex H in Fig. 8(c), which satisfies the HD requirement of the security bits as well as enough combinations of the vertices, E, F, G, e.g., $\{0000, 0100, 1000\} \longrightarrow 0011$ is a qualifying example. Fig. 8(d) shows a series of consecutive authorized transitions (i, ii, and iii) originating from the same ending vertex. We refer to this type of FSM as *directed rooted tree FSM* in this paper. Here, the security bits are extended to the leftmost two bits due to the $1 \longrightarrow 0$ transition requirement in the AT (ii). Although the number of don't cares is further reduced, n is maintained at 4 to conserve area and power. In this case, the left hand side bits follow the bit set model under the set-reset model so security comes from the '$1' \longrightarrow$ '$0'$ transition in the FFs. The security bits on the right hand side follow the usual bit reset model in the FFs. As the security bits corresponding to the specific bits incorporate both types of transitions for security we refer to this methodology as set-reset approach under set-reset model. TAMED can also incorporate set only (only $1 \longrightarrow 0$ transition), and reset only (only $0 \longrightarrow 1$ transition) approaches under set-reset model. In this paper, set-reset approach under set-reset model has been specifically chosen for analysis as it provides security for both types of transitions.



(a)

(b)

(c)

(d)

Fig. 8: A subset of different $\mathbb{AT}$ that can be constructed by TAMED. All examples consider an LFI capability of $x = 1$. X represents a don't care state in the encoding and the red demarcation line on the encoding separates the don't care bits from the security bits in (a)-(c). All bits that are not X are security bits. (a) $I \longrightarrow J, K \longrightarrow L$ are transitions of the same FSM. (b)(c)(d) have 3 transitions each.

C. Transitional Vulnerability Metric (Set-Reset Model)

In order to aid the corresponding security analysis for set-reset approach, the metric named *Transitional Vulnerability Metric* $TVM_{sr}(x)$ is proposed. Note that, to ensure proper security for the TAMED methodology a requirement of '$1 \longrightarrow 0$' (bit set) or '$0 \longrightarrow 1$' (bit reset) is required and the HD constraint is desired only on $\mathbb{SFF}$ bit positions. This can be expressed as $HD(\mathbb{AU}_{n-m+1:n}, \mathbb{P}_{n-m+1:n}) > x$. In addition to that, depending on the bit set or bit reset model of the $\mathbb{SFF}$, $\mathbb{AU}_{n-m+1:n} \in \{1\}^m$ or $\mathbb{AU}_{n-m+1:n} \in \{0\}^m$, respectively, where $m = |\mathbb{SFF}|$. To this end, we define a subset of transitions $\mathbb{VT}_{sr}(x) \subseteq \mathbb{T}$ as

$$\mathbb{VT}_{sr}(x) = \{(s_i, s_j \in \mathbb{T}) | \; s_i \in \mathbb{AU}, \\ HD(s_{i_{n-m+1:n}}, s_{j_{n-m+1:n}}) \leq x, \; s_j \in \mathbb{P}\} \quad (3)$$

where $\mathbb{VT}_{sr}(x)$ represents the set of transitions vulnerable to x faults due to the set-reset model. Clearly, the goal of our fault tolerant scheme should be $|\mathbb{VT}_{sr}(x)| = 0$.

If $x = 1$, and the required $|AT| = 1$ for the example in Fig. 6(a), where current state is $\{01\}$ and $\mathbb{P} = \{11\}$ then $|\mathbb{VT}_{sr}(1)| > 0$. Only if $\mathbb{AU} = \{00\}$ is AT secured. This means that generally for set-reset model FFs, there are two components to the $\mathbb{VT}_{sr}(x)$: *bidirectional* transitions or all '0'

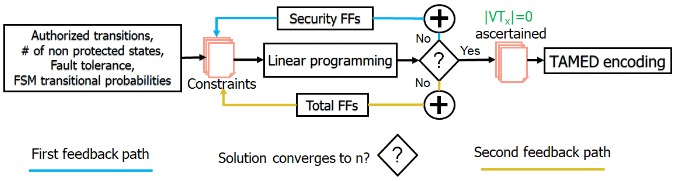


Fig. 9: Block diagram of TAMED.

Algorithm 1 Generation of TAMED encoding

```
procedure
Input: Authorized Transitions, # of non protected states (|$NS$|), $HD$, FSM transitional probabilities, The model assumed
Output: TAMED encoding
    $n = log_2|S|$                                  ▷ initial estimation
    while $n$ does not converge do
        construct all common linear constraints
        for (all range of security FFs) do
            construct model specific constraints
            implement objective function
            try to converge $n$
        end for
        if ($n$ does not converge) then
            $n = n + 1$
        end if
        if ($n$ converges) then
            ensure $|VT_x| = 0$                      ▷ validates security
        end if
    end while
end procedure
```

and all ‘1’ in $\mathbb{AU}$ corresponding to $\mathbb{SFF}$ that does not provide minimum HD. These two components are captured by:

$$\mathbb{VT}_{sr}(x) = \begin{cases} |\{(u,v) \in AT|(u_i \leq v_i)||(u_j \geq v_j)\}||\ \{(u_i > v_i)\}| \\ \quad {\scriptstyle \forall i,j=1+(n-m)\cdots n,\ where\ m=reset\ |\mathbb{SFF}|} \\ |\{(u,v) \in AT|(u_i \leq v_i)||(u_j \geq v_j)\}||\ \{(u_i < v_i)\}| \\ \quad {\scriptstyle \forall i,j=1+(n-m)\cdots n,\ where\ m=set\ |\mathbb{SFF}|} \end{cases} \tag{4}$$

where, the current state is u, the next state is v, the total number of security FFs is $|SFF|$, and i^{th} FF of u is represented with u_i. Intuitively, $\mathbb{VT}_{sr}(x)$ captures the total number of vulnerable transitions in the AT, where individual fault types (bit set and bit reset on security bits) considered exclusively can lead to any $\mathbb{P}$. To capture the FSM’s degree of susceptibility to the precise x set or reset faults in one clock cycle,

$$TVM_{sr}(x) = \frac{|\mathbb{VT}_{sr}(x)|}{|\mathbb{T}|}. \tag{5}$$

where, $0 \leq TVM_{sr}(x) \leq 1$. In other words, $TVM_{sr}(x)$ is the percentage of transitions where x bit flip faults can lead to a $\mathbb{P}$ from $\mathbb{AU}$. The desired value of $TVM_{sr}(x) = 0$, which means there are no vulnerable transitions due to set or reset models in the FSM.

D. TAMED Encoding Framework

In this section, we propose our encoding scheme framework called TAMED (Transitional Approaches for LFI Resilient State Machine EncoDing) which makes the FSM inherently tolerant to precise laser fault injection under transition-based models. TAMED employs integer linear programming (ILP) to achieve the goal of finding a flexible and switching activity optimized encoding along with optimal n and $|\mathbb{VT}| = 0$ for security, according to the FSM design specifications and other user inputs. The block diagram for TAMED is shown in Fig. 9. We refer to ‘non-protected states’ ($\mathbb{NS}$), as the states that are not incorporated into any of the authorized transitions. The user inputs for TAMED are the *FSM design specification* (FSM states, transitions, and transitional probabilities for optimization of switching activity), *FSM security specification* (e.g., authorized transitions, # of non-protected states, and the *attacker’s expected capability* (e.g., number of laser faults x). The type of transitional approach (bit flip or set-reset in this paper) can be a supplementary input.

In addition to the block diagram, Algorithm 1 depicts TAMED’s steps. All transitional information is inputted using adjacency list where the order of the transition is important by default. After the inputs are provided the corresponding linear constraints for $n = log_2|\mathbb{S}|$ are initialized. Subsequently, an iteration commences which tries to find if any solution converges with the current n FFs. Concurrently, for each n it is made sure that the demarcation line moves from right to left first (i.e., $|\mathbb{SFF}|$ is increased) and the corresponding linear constraints updated according to the model to check if the FSM design specification is met. If not met, then n is increased by 1 as TAMED explores the second feedback path; the iteration repeats until the ILP process converges to a fitting n and the optimized state encoding is generated. Finally, TAMED encoding is obtained upon checking for the appropriate $VT_x = 0$ depending on the fault model, preventing any AT not measuring up to the security constraint.

ILP Problem Formulation: Our goal is to construct a framework that can incorporate any transitional approach model (set-reset, bit flip) with proper ILP constraints appropriately designed for an LFI-resistant FSM. The objective function corresponds to the total switching activity of the FSM which is minimized for dynamic power minimization. Details of the different constraints and objective function are elaborated below. Set-reset constraints share the same constraints as bit flip constraints.

For each state encoding y_i, where $i = 1, \ldots, f$, of an f-state FSM, our objective function for the linear optimization problem can be expressed as finding a code, $[y_{i,1}, y_{i,2}, \ldots y_{i,n}]$, such that:

$$\begin{aligned} &\min_{y} f(y)\ where \\ &f(y) = \sum_{1 \leq i < j \leq f} p_{i,j} \sum_{l=1}^{n} \left| y_{il} - y_{jl} \right|, i \neq j \\ &\forall y_{il} \in \{\ f - state\ encoding\ \}, \\ &subject\,to \begin{cases} Constraints \\ y\ (0\ -1)\ integer \end{cases} \end{aligned} \tag{6}$$

where n is the number of FFs in the FSM design; $p_{i,j}$ represents the total transitional probability between states y_{il} and y_{jl}, where l represents the number of bits in the state encoding. Here, the dimension i corresponds to each of the state encoding. Optimization constraints for each of the model are elaborated upon below.

1) Bit Flip Model:

- The first constraint enforces the design requirement in the authorized transitions ($\mathbb{AT}$), i.e., between the $\mathbb{AU}$ and the $\mathbb{P}$. Given the attacker's LFI capability of x, all states $\in \mathbb{AU}$ need to be a minimum of HD of $x+1$ away from all states $\in \mathbb{P}$. This is expressed as:

$$\sum_{l=1}^{n} |y_{AUl} - y_{Pl}| > x \qquad (7)$$

- Assuming no self transitions, the total number of maximum possible combinations of transitions in an FSM can be calculated by $|\mathbb{S}|C_2$ in an FSM, where C refers to the combination function. All possible combinations of transitions, apart from the ones in $\mathbb{AT}$, i.e., $(|\mathbb{S}|C_2 - |\mathbb{AT}|)$ must be at least unit HD away. This may include the combination of transitions not existing in $\mathbb{T}$ in the FSM, i.e., $\sum_{l=1}^{n} \left|y_{AU_al} - y_{AU_bl}\right| \geq 1$, $\sum_{l=1}^{n} \left|y_{P_al} - y_{P_bl}\right| \geq 1$, $\sum_{l=1}^{n} \left|y_{NS_al} - y_{NS_bl}\right| \geq 1$, $\sum_{l=1}^{n} |y_{NSl} - y_{AUl}| \geq 1$, and $\sum_{l=1}^{n} |y_{NSl} - y_{Pl}| \geq 1$, where $a \neq b$. Hence, this constraint ensures that each of the state in $\mathbb{T}$ is distinct in the FSM.

2) Set-Reset Model: Just to reiterate, for set-reset model we have assumed a convention of reset model in the rightmost security bits and if need be, set model in the leftmost security bits. Along with all the common constraints of the bit flip model, some additional constraints are necessary to realize the set-reset model which are itemized below.

- Staying with the convention, during each iteration, a range of security bits may be required to specifically transition from 0 bits to 1 bits due to security requirement, while attempting to converge to the optimum n. The constraints in Equations (8) and (9) enforce this. Given the attacker's LFI capability of x, all of the the rightmost ($h = |\mathbb{SFF}|$) security bits of AU may be needed to start off with at least $(x+1)$ '0' bits. The number of security bits is varied in the expression:

$$\sum_{l=1}^{h} y_{AUl} \leq h - (x+1) \qquad (8)$$

  Also, it should be noted that if the security bit in AU is '0' then the corresponding bit in P must be '1' among the h security bits. However, if the bit in AU is '1', the corresponding bit in P could be either '0' or '1'. This is captured by:

$$y_{Pl} \geq 1 - y_{AUl}, \; where \; \forall l = 1, \ldots, h \qquad (9)$$

- If alternatively, $1 \longrightarrow 0$ transition is required to reflect the bit set model in the leftmost security bits for FSMs like Fig. 8(d), the above constraints are adjusted to:

$$\sum_{l=1}^{h} 1 - hy_{AUl} \leq h - (x+1) \qquad (10)$$

$$y_{Pl} \leq 1 - y_{AUl}, \; where \; \forall l = 1, \ldots, h \qquad (11)$$

The overall problem can thus be represented as an ILP problem. There are numerous commercial and free tools available in order to solve the ILP for a TAMED encoding.

		AES			SHA-256			RSA			FSM Controller			PCI (System Controller)		
	x	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3
TAMED (Bit Flip)	PDP	1.1	1.2	1.2	1	1	1	1	1.2	1.7	0.9	1.2	1.4	1	1	1
	VM	0.2	0.4	0.4	0.6	0.6	0.6	0.1	0.3	0.3	0.3	0.4	0.4	0.1	0.2	0.2
	TVM_{bf}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	TVM_{sr}	0.2	0.2	0	0.1	0.1	0.1	0	0	0	0.1	0	0.1	0.2	0	0
	Area	1	1.1	1.4	1	1.2	1.3	0.9	1.2	1.4	1	1.3	1.4	1	1	1.01
TAMED (S & R)	PDP	1.3	1.6	1.9	0.9	1	1.1	1.3	1.8	2.1	1.3	1.6	1.8	1	1	1
	VM	0.2	0.4	0.4	0.3	0.4	0.4	0.1	0.3	0.3	0.1	0.1	0.1	0.1	0.2	0.2
	TVM_{bf}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	TVM_{sr}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Area	1.2	1.5	1.8	1.2	1.4	1.6	1.1	1.6	1.9	1.1	1.4	1.6	1	1	1.01
PATRON	PDP	1.3	1.8	1.9	1.1	1.3	1.3	1.3	2	2.5	1.4	1.7	1.8	1	1.1	1.1
	VM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	TVM_{bf}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	TVM_{sr}	0.01	0	0.02	0	0	0.03	0	0.04	0	0.01	0.01	0.02	0	0.02	0
	Area	1.2	1.4	1.7	1.2	1.5	1.6	1.2	1.6	1.9	1.2	1.5	1.8	1.03	1.06	1.07
Codetables	PDP	1.4	1.9	2.1	1.1	1.5	1.6	1.4	2	2.6	1.2	1.7	2.2	1	1.1	1.2
	VM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	TVM_{bf}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	TVM_{sr}	0.02	0.02	0	0	0	0.06	0	0	0	0	0	0.03	0.02	0	0.06
	Area	1.2	1.6	1.7	1.2	1.5	1.7	1.2	1.7	1.9	1.3	1.7	1.9	1.01	1.08	1.08

TABLE I: Power-delay product (PDP), vulnerability metrics (VM, TVM_{bf},TVM_{sr}), and area analysis for different encoding schemes. All PDP and area values are **normalized** by PDP and area of Binary Encoding. Average of 5 values are taken for PATRON, and Codetables. Red and green denote vulnerable and non-vulnerable FSMs, respectively. '(S & R)' means 'Set and Reset'.

V. Results and Discussion

Experiments: In this section, we evaluate the proposed TAMED encoding and compare it to the other FF encoding schemes. The post-synthesis results mention Power Delay Product (PDP) normalized by the PDP of a binary encoded FSM. Despite the corresponding PDPs correlation with area, normalized area values for each x are included separately as well. A recently published state exploration scheme against LFI known as PATRON [9], which protects *all SS* from the *NS* proposes a relevant metric named Vulnerability Metric (VM). VM is the percentage of states where x faults can lead to a SS. VM is utilised in this section to realize the overlap/divide with the proposed transition based vulnerability metrics (TVM_{bf} and TVM_{sr}). Specifically, TAMED is investigated on five controller benchmark circuits, namely AES, SHA, RSA, FSM Controller, and PCI (System Controller) in terms of PDP, area, VM, TVM_{bf}, and TVM_{sr} with increasing x. All benchmark circuits are collected from OpenCores [22] with the exception of the synthetic benchmark named 'FSM Controller' and synthesized using Synopsys Design Compiler (DC) with 32-nm library. Although, the number of simultaneous laser faults is typically restricted to two (i.e., $x \leq 2$) today, we include results for $x = 3$ to demonstrate the generality of our threat model and the capability to handle LFI in current as well as future attack scenarios [23].

State Encoding Approaches and Benchmarks: TAMED is compared with PATRON scheme that can assume *only* the bit flip model for the power consumption adjusted encoding [9]. As PATRON encoding generation is manually exhaustive, multiple possible encodings that meet the same FSM design

	AES	SHA-256	RSA	FSM Controller	PCI (System Controller)
$\lvert\mathbb{S}\rvert$	5	7	7	7	6
$\lvert\mathbb{T}\rvert$	10	11	9	9	5
$\lvert\mathbb{SS}\rvert$	3	3	4	5	3
$\lvert\mathbb{AT}\rvert$	2	2	3	3	2

TABLE II: The corresponding values of the total number of states ($|\mathbb{S}|$), total number of transitions ($|\mathbb{T}|$), total number of sensitive states ($|\mathbb{SS}|$), and total number of authorized transitions ($|\mathbb{AT}|$) for each benchmark.

constraint are possible. Hence, all the compared metrics are average of 5 different values for each x in PATRON.

The linear codes referred to as Codetables is also compared with TAMED as these codes are readily proven to be effective against LFI. An $[n, k, d]$ linear code represents k bit messages in n bit codewords where two distinct codewords differ in at least d bits. The codetable represents bounds and construction of the linear code $[n, k, d]$ over Galois Field of q [24]. As we are considering only Boolean values $q = 2$, i.e., only *binary code* is examined. For Codetables, all T transitions in the FSM are considered AT as there is no flexibility within this approach *to separate AT from the rest of the transitions*. Note that with this approach, the applicability for all the popular linear encoding such as Hamming (7,4), Extended Hamming, Binary Golay, Extended Binary Golay, etc. that could be designed for the specific benchmarks parameters are also inherently examined. Also, as Codetables assume a uniform HD of $(x+1)$ between the codewords, the average of 5 different values are taken for this approach too.

Discussion on other relevant error detection-based approaches such as non-linear codes is important because of their proven effect of improving reliability against LFI and to realize/appreciate the contrast with TAMED encoding. With regard to nonlinear codes, robust and partially robust codes can be assuring [25], [26]. However, both these codes have minimum HD of 1. As HD flexibility is of utmost importance in the context of LFI, this property/attribute by itself makes them inapplicable. Most of these codes also have relatively low code rate (a measure of inefficiency) [27]. Hence, because of their inadequacy to LFI nonlinear codes are disregarded here.

Most cryptographic algorithms tend to have small number of states. For AES, the authorized transitions are regarded from “Initial Round” to “Do Round” and “Do Round” to “Final Round”. For SHA-256 the transitions from “Block next” to “Data input”, and “Valid” are regarded as in the authorized transitions [8]. For RSA, the consecutive transitions between “Load2”, “Multiply”, “Result”, and “Square” are regarded as in AT. It is important to note that for each of the benchmark, AT is selected so as to incorporate all the different types of transitions as in Fig. 8. Compared to the proposed TAMED approach, PATRON [9] and Codetables [24] consider states for the solution set(s) instead of the AT. Furthermore, TAMED incorporates flexibility to consider all T transitions in the FSM as AT, if intended by the designer.

PDP and Area Overhead Comparison: Table I shows a comprehensive comparison of TAMED with the other *model-unaware* approaches. Relevant information for each of the benchmark is presented in Table II. As the PDP and area values are normalized with binary encoding, Codetables and PATRON generate encoding that are not power optimized as they have no selection criteria of the optimum encoding meeting the specific FSM design specification. As expected, linear encoding from the Codetables achieve the highest PDP on average since their solution is only guided by the HD, rather than the other important FSM design parameters, i.e., transitional probabilities, and NS. The approach with the next highest PDP is PATRON. For the PATRON approach, a contributing factor to different PDPs is in how the designer encode the sensitive states. Added to that, PATRON protects *all SS* from its NS choices, as well as each state within SS, which contributes to redundant protection mechanism in design. The TAMED approaches are seen to have better PDPs because of the power optimization step and the flexibility in the TAMED process to generate the one encoding solution to precisely match the FSM design parameters based on different models. The bit flip model, and the more precise set and reset model have better PDPs compared to the model-unaware approaches. In terms of area, TAMED also has the lowest overall average overhead compared to the other model-unaware approaches, likely because it attempts to minimize the number of FFs needed in its optimization flow. On average, compared to the state-based approaches the TAMED approaches are seen to be less by 13.09% in PDP and 8.33% in area.

FSM Security Resilience Comparison: For security analysis, VM, TVM_{bf}, and TVM_{sr} are explored with increasing x. Except TAMED, all the approaches deliver encoding that have $VM = 0$ by design. For TAMED, all encodings have $VM(x) > 0$, indicating susceptibility of certain transitions to LFI but not the specific $\mathbb{AT}$ due to the corresponding $TVM_{bf} = 0$. For example, TAMED (AES, $x = 1$) generate a secure encoding for all the AT in the FSM, although $VM > 0$. In other words, VM is a conservative metric as for it to provide a sense of security (i.e., a value of 0), some of the non-security critical state transitions may have to be regarded as critical. It is confirmed from considering Codetable and PATRON schemes, where $TVM_{bf} = 0$ and $VM = 0$ signifies that not only all the AT are secure, but all the T between the SS and the NS are *conservatively* secure. Hence, the metric TVM_{bf} can be concluded as a more precise metric than VM as it considers protection of only the specific $\mathbb{AT}$ unlike VM. In order to calculate TVM_{sr}, $|\mathbb{SFF}|$ for PATRON and Codetables is assumed to contain $(x+1)$ security bits for the corresponding x. This assumption is practically demonstrated and is based on security grounds as the attacker may inflict an additional fault from a fixed number of lasers, if the layout is not security adjusted [3], [21], [10]. Note that for TAMED the security bits can be more than the $(x + 1)$ bits to accommodate the necessary HD so $|\mathbb{SFF}| = (x + 1)$ bits is the minimum value for each x.

It can be concluded that Codetables and PATRON cannot take set-reset model into account, as $TVM_{sr} \neq 0$ for some values. This means that at least one of the 5 times the encoding choices did not fulfill the security requirements. The occasional $TVM_{sr} = 0$ in these approaches is derived from the lucky selection of security-compliant encoding choices, i.e., the current state and next state of each authorized transition follow the TAMED security constraints. However, there is no guarantee that TVM_{sr} will always be 0 in these approaches. Except for TAMED (Set and Reset), none of the approaches can reliably generate encoding with $TVM_{sr} = 0$. The model unaware approaches (PATRON and Codetables) cannot provide solution for the precise set-reset model but only the bit flip model even though all the states have a minimum HD of $(x+1)$ between the codewords. *The fact that* $VM \neq TVM_{sr} \neq TVM_{bf}$ *illustrates the need for TAMED which has the flexibility of protecting only the specific AT according to the design requirement and different models in estimating the FSM vulnerability to LFI.*

VI. Conclusion

In this paper, we introduced a transition-based LFI resilient encoding scheme that incorporates sensitive regions of a flip flop under bit set, reset, set-reset, and flip models to protecting any number and type of transition(s) in an FSM according to the designer's intent. Specifically, if the sensitive regions are accounted for in the threat model, critical errors result for the contemporary countermeasures. In contrast, TAMED's automated linear programming approach constitutes more flexibility as it can consider the FF sensitivity when generating a single power optimized encoding. The proposed transitional vulnerability metrics were also shown to be more precise than other state exploration approaches in terms of exposure to faults based on data dependent and independent models. TAMED outperformed other FSM encoding schemes in terms of security, PDP, or area and in many cases all three. For future work, we plan to investigate and extend TAMED on FPGAs. We also plan to co-optimize TAMED encoding and layout similar to SPARSE.

References

[1] M. Agoyan, J.-M. Dutertre, A.-P. Mirbaha, D. Naccache, A.-L. Ribotta, and A. Tria, "How to flip a bit?," in *2010 IEEE 16th International On-Line Testing Symposium*, pp. 235–239, IEEE, 2010.

[2] A. Barenghi, L. Breveglieri, I. Koren, and D. Naccache, "Fault injection attacks on cryptographic devices: Theory, practice, and countermeasures," *Proceedings of the IEEE*, vol. 100, no. 11, pp. 3056–3076, 2012.

[3] F. Schellenberg, M. Finkeldey, N. Gerhardt, M. Hofmann, A. Moradi, and C. Paar, "Large laser spots and fault sensitivity analysis," in *2016 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, pp. 203–208, IEEE, 2016.

[4] R. Leveugle, P. Maistri, P. Vanhauwaert, F. Lu, G. Di Natale, M.-L. Flottes, B. Rouzeyre, A. Papadimitriou, D. Hély, V. Beroulle, *et al.*, "Laser-induced fault effects in security-dedicated circuits," in *2014 22nd International Conference on Very Large Scale Integration (VLSI-SoC)*, pp. 1–6, IEEE, 2014.

[5] C. Champeix, N. Borrel, J.-M. Dutertre, B. Robisson, M. Lisart, and A. Sarafianos, "Seu sensitivity and modeling using pico-second pulsed laser stimulation of a d flip-flop in 40 nm cmos technology," in *2015 IEEE international symposium on defect and fault tolerance in VLSI and nanotechnology systems (DFTS)*, pp. 177–182, IEEE, 2015.

[6] J.-M. Dutertre, V. Beroulle, P. Candelier, L.-B. Faber, M.-L. Flottes, P. Gendrier, D. Hely, R. Leveugle, P. Maistri, G. Di Natale, *et al.*, "The case of using cmos fd-soi rather than cmos bulk to harden ics against laser attacks," in *2018 IEEE 24th International Symposium on On-Line Testing And Robust System Design (IOLTS)*, pp. 214–219, IEEE, 2018.

[7] A. Nahiyan, K. Xiao, K. Yang, Y. Jin, D. Forte, and M. Tehranipoor, "Avfsm: A framework for identifying and mitigating vulnerabilities in fsms," in *Proceedings of the 53rd Annual Design Automation Conference*, pp. 1–6, 2016.

[8] A. Nahiyan, F. Farahmandi, P. Mishra, D. Forte, and M. Tehranipoor, "Security-aware fsm design flow for identifying and mitigating vulnerabilities to fault attacks," *IEEE Transactions on Computer-aided design of integrated circuits and systems*, vol. 38, no. 6, pp. 1003–1016, 2018.

[9] M. Choudhury, D. Forte, and S. Tajik, "Patron: A pragmatic approach for encoding laser fault injection resistant fsms," in *2021 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, pp. 569–574, IEEE, 2021.

[10] M. Choudhury, S. Tajik, and D. Forte, "Sparse: Spatially aware lfi resilient state machine encoding," in *Proceedings of the 10th International Workshop on Hardware and Architectural Support for Security and Privacy*, pp. 1–8, 2021.

[11] L. Yuan, G. Qu, T. Villa, and A. Sangiovanni-Vincentelli, "Fsm re-engineering and its application in low power state encoding," in *Proceedings of the 2005 Asia and South Pacific Design Automation Conference*, pp. 254–259, 2005.

[12] J. Richter-Brockmann, A. R. Shahmirzadi, P. Sasdrich, A. Moradi, and T. Güneysu, "Fiver–robust verification of countermeasures against fault injections," *IACR Cryptographic Hardware and Embedded Systems*, 2021.

[13] J. Richter-Brockmann, P. Sasdrich, and T. Güneysu, "Revisiting fault adversary models-hardware faults in theory and practice.," *IACR Cryptol. ePrint Arch.*, vol. 2021, p. 296, 2021.

[14] S. Buchner, A. Campbell, T. Meehan, K. Clark, D. McMorrow, C. Dyer, C. Sanderson, C. Comber, and S. Kuboyama, "Investigation of single-ion multiple-bit upsets in memories on board a space experiment," in *1999 Fifth European Conference on Radiation and Its Effects on Components and Systems. RADECS 99 (Cat. No. 99TH8471)*, pp. 558–564, IEEE, 1999.

[15] N. Miskov-Zivanov and D. Marculescu, "Modeling and analysis of ser in combinational circuits," in *Workshop on Silicon Errors in Logic-System Effects (SELSE)*, 2010.

[16] P. Shivakumar, M. Kistler, S. W. Keckler, D. Burger, and L. Alvisi, "Modeling the effect of technology trends on the soft error rate of combinational logic," in *Proceedings International Conference on Dependable Systems and Networks*, pp. 389–398, IEEE, 2002.

[17] N. Miskov-Zivanov, K.-C. Wu, and D. Marculescu, "Process variability-aware transient fault modeling and analysis," in *2008 IEEE/ACM International Conference on Computer-Aided Design*, pp. 685–690, IEEE, 2008.

[18] H.-K. Peng, C. H.-P. Wen, and J. Bhadra, "On soft error rate analysis of scaled cmos designs: a statistical perspective," in *Proceedings of the 2009 International Conference on Computer-Aided Design*, pp. 157–163, 2009.

[19] C. Roscian, J.-M. Dutertre, and A. Tria, "Frontside laser fault injection on cryptosystems-application to the aes'last round," in *2013 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*, pp. 119–124, IEEE, 2013.

[20] J. M. Rabaey, A. P. Chandrakasan, and B. Nikolić, *Digital integrated circuits: a design perspective*, vol. 7. Pearson education Upper Saddle River, NJ, 2003.

[21] J.-M. Dutertre, V. Beroulle, P. Candelier, S. De Castro, L.-B. Faber, M.-L. Flottes, P. Gendrier, D. Hely, R. Leveugle, P. Maistri, *et al.*, "Laser fault injection at the cmos 28 nm technology node: an analysis of the fault model," in *2018 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC)*, pp. 1–6, IEEE, 2018.

[22] "Opencores https://opencores.org/."

[23] L. Bossuet, L. de Laulanié, and B. Chassagne, "Multi-spot laser fault injection setup: New possibilities for fault injection attacks," in *Smart Card Research and Advanced Applications: 20th International Conference, CARDIS 2021, Lübeck, Germany, November 11–12, 2021, Revised Selected Papers*, p. 151, Springer.

[24] M. Grassl, "Bounds on the minimum distance of linear codes and quantum codes." Online available at http://www.codetables.de, 2007.

[25] M. Karpovsky and A. Taubin, "New class of nonlinear systematic error detecting codes," *IEEE Transactions on Information Theory*, vol. 50, no. 8, pp. 1818–1819, 2004.

[26] Y. Neumeier and O. Keren, "Punctured karpovsky-taubin binary robust error detecting codes for cryptographic devices," in *2012 IEEE 18th International On-Line Testing Symposium (IOLTS)*, pp. 156–161, IEEE, 2012.

[27] K. J. Kulikowski, Z. Wang, and M. G. Karpovsky, "Comparative analysis of robust fault attack resistant architectures for public and private cryptosystems," in *2008 5th Workshop on Fault Diagnosis and Tolerance in Cryptography*, pp. 41–50, IEEE, 2008.