2021 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT) | 978-1-6654-1609-2/21/$31.00 ©2021 IEEE | DOI: 10.1109/DFT52944.2021.9568356

GF-Flush: A GF(2) Algebraic Attack on Dynamically Secured Scan Chains

Dake Chen, Chunxiao Lin and Peter A. Beerel
University of Southern California
Los Angeles, CA, United States
{dakechen, chunxiao, pabeerel}@usc.edu

***Abstract*—Scan chains provide increased controllability and observability for testing digital circuits. The increased testability, however, can also be a source of information leakage for sensitive designs. The state-of-the-art defenses to secure scan chains apply dynamic keys to pseudo-randomly invert the scan vectors. In this paper, we pinpoint an algebraic vulnerability of these dynamic defenses that involves creating and solving a system of linear equations over the finite field GF(2). In particular, we propose a novel GF(2)-based flush attack that breaks even the most rigorous version of state-of-the-art dynamic defenses. Our experimental results demonstrate that our attack recovers the key as long as 500 bits in less than 7 seconds. Our attack times are, on average, over 4300x faster than state-of-the-art SAT based attacks on the same defenses and circumvent any obfuscation on the combinational logic portions of the design. We then demonstrate how our attacks can be extended to scan chains compressed with Multiple-Input Signature Registers (MISRs).**

***Index Terms*—Hardware Security, Logic Locking, Dynamic Obfuscated Scan Chain, GF(2) Analysis, Algebraic Attack**

I. Introduction

The decentralized supply chain of modern integrated circuit (IC) design and manufacturing raises significant concern related to threats that include intellectual property (IP) piracy [1] and Trojan insertion [2]. For many designs, the scan chain used in manufacturing testing presents a significant threat vector as it provides extensive controllability and observability of chip internals to the attacker [3]–[8].

Many of the state-of-the-art defenses include dynamic keys to obfuscate the scan chain [9]–[11]. They leverage a linear feedback shift register (LFSR) that controls XOR gates along the scan chain to psuedo-randomly invert the scan chain sequence. The psuedo-random sequence is dependent on the seed of the LFSR which must remain secret to ensure security. Recently, [12], [13] proposed SAT attacks to unveil the seed by converting the scan flip-flops to psuedo input and outputs which effectively models the sequential circuit and LFSR as a combinational circuit that can be analyzed through well-known SAT attacks. The work [11] points out that this conversion from sequential to combinational logic increases the number of SAT literals and clauses, increasing the complexity and associated run-times of SAT attacks.

In contrast, a simple flush and reset attack was proposed in [14]. Here all flip-flops on scan chain are reset to 0 and the attack examines the initial sequence of scan out bits. Since the attacker can also reverse engineer the location of the locking gates, they are able to reveal the key input values from the scan out patterns. One recent dynamic obfuscation design [10], [11] resists this reset attack by adding a shadow chain between the LFSR and scan chain. Due to the presence of the shadow chain which has the same length as LFSR, the initial scan out patterns remain zero and leak no information about the secret seed.

In this paper, we propose a more comprehensive flush attack based on GF(2) algebra that unveils the secret key of the dynamic scan locking defenses even when protected by a shadow chain. In contrast to SAT attacks [12], [13] which attack the scan chain coupled with locked combinational logic, our attack isolates the scan chain, enabling the use of more computationally scalable algebraic techniques used in cryptoanalysis [15], including attacks on LFSRs [16], and automatic test pattern generation [17], [18]. In particular, the attack involves solving a system of linear equations over the finite field GF(2) whose size scales linearly with the size of the key. We empirically validate that the complexity of our attack is computationally tractable, recovering keys as long as 500 bits in less than 7 seconds. Our attack times are, on average, over 4300x faster than the comparable state-of-the-art SAT attack.

We further consider the case when the only access to the scan chain outputs is through test compression logic, such as a Multiple-Input Signature Registers (MISR). Since MISRs also consist of XOR gates and FFs they can be modeled, analyzed, and thus considered in our attack. To the best of our knowledge, this is the first attack on obfuscated scan chains that considers MISRs. One prior attack [12] considered XOR gates for compression but these are less complex than MISRs and offer lower compression rates. Another prior attack on an AES cipher [19] analyzed its feasibility when its outputs were accessible only after an MISR. For our attack, even if with MISRs, the attack times are manageable.

The remainder of this paper is organized as follows.

This material is based on research sponsored by the Air Force Research Labs (AFRL) and the Defense Advanced Research Projects Agency (DARPA) under agreement number #FA8650-18-1-7817. The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright notation thereon. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the U.S. Government.

Section II reviews the background leveraged in this paper. Section III describes the proposed attack. Section IV details experimental results of our attack. Some conclusions and opportunities for future work are discussed in the last section.

II. Background

A. A Linear Feedback Shift Register (LFSR)

A Linear Feedback Shift Register (LFSR) is often used as pseudo-random number generator in many cryptographic and secure systems because of its lightweight, low overhead and high throughput [20], [21].

The generic structure of an LFSR is shown in Figure 1, where λ denotes its length and the Binary values c_0 to $c_{\lambda-1}$ determine its feedback structure. The next state equation f_i^{t+1} can be represented as

$$f_i^{t+1} = f_{i+1}^t, \text{ for } i \in [0, \lambda - 1) \tag{1}$$

$$f_{\lambda-1}^{t+1} = \sum_{j=0}^{\lambda-1} c_j f_j^t \tag{2}$$

where t and $t+1$ represent the current and next state, respectively, f_i^t denotes the value of stage i of LFSR at time t, and all operations are in GF(2).

The sequence generated by an LFSR is periodic and the period depends on the values of c_i and the initial state, or *seed* of the LFSR. The maximum period of an LFSR of length λ is $2^\lambda - 1$ [22]. The sequences generated by LFSRs with maximum period are referred to as PN-sequences and these are desired for secure systems as they are more difficult to break than LFSRs with small periods.

B. Dynamically Obfuscated Scan Chains

Due to the effectiveness of SAT attacks [12] on static scan chain obfuscation techniques [23], state-of-the-art secure chains dynamically obscure scan chains using XORs that are driven by an LFSR [9]–[11] and psuedo-randomly invert the scan sequence.[1] The basic structure of these schemes is shown in Figure 1, where λ represents the length of the LFSR and key, N denotes the length of scan chain, and b represents the spacing of locking gates throughout the chain. Besides inserted with fixed distance b, the locking gates can also be randomly inserted between scan flip-flops. The most secure version of these methods updates the LFSR every clock cycle, applying new key bits to the scan locking gates every cycle.

C. MISR

As the size of chips and number of scanned FFs increase, the latency and memory requirements to shift out and process their stored values during test grows. For this reason test compression techniques, involving both a decompressor and compressor, have become an essential part of the design. The decompressor expands one scanned-in sequence into many parallel scan chain segments and the compressor compresses the outputs of many parallel scan segments into one. The most commonly used compressor is a Multiple-Input Signature Register (MISR) [24] illustrated in Figure 3,

Since the MISR can prohibit direct access to the scan outputs, it has significant impact on all HW security attacks that rely on scan chain access, including previous SAT attacks [12], [13]. Interestingly, as the MISR uses XOR gates that are commonly used to obfuscate combinational logic, one might think the MISR effectively encrypts the scan outputs.

D. Algebraic Analysis

LFSRs are commonly used in built-in-self-test structures and algebraic analysis [17], [18] has been used to find seeds and characteristic polynomials that lead to high test coverage. Moreover, algebraic cryptanalysis or algebraic attack [15], [16] has been widely used for attacking various ciphers. These attacks first find low degree equations to approximate the function of feedback shift registers (FSR) or algorithms based on their features, then leverage the XL algorithm [25] to solve the system of multivariate polynomial equations, thereby acquire the key bits. These algebraic techniques, however, have never been applied in scan-chain locking. Considering all operations in the LFSR, scan-chain locking gates and MISR are effectively XOR operations, we hypothesize that an algebraic attack over GF(2) can be very efficient.

III. GF-Flush: A GF(2) Algebraic Attack

A. Algebraic Foundations of the Attack

The basic flow of our proposed attack is illustrated in Figure 2. Similar to previous attacks on the same defenses [13], we assume that the netlist is reverse-engineered and thus the structural information about the LFSR c_i, the length of the scan chain N, and the location of XOR gates b are known to the attacker. We also assume the attacker has access to an oracle, which in this case amounts to a working scan-chain with the correct seed programmed in the LFSR.

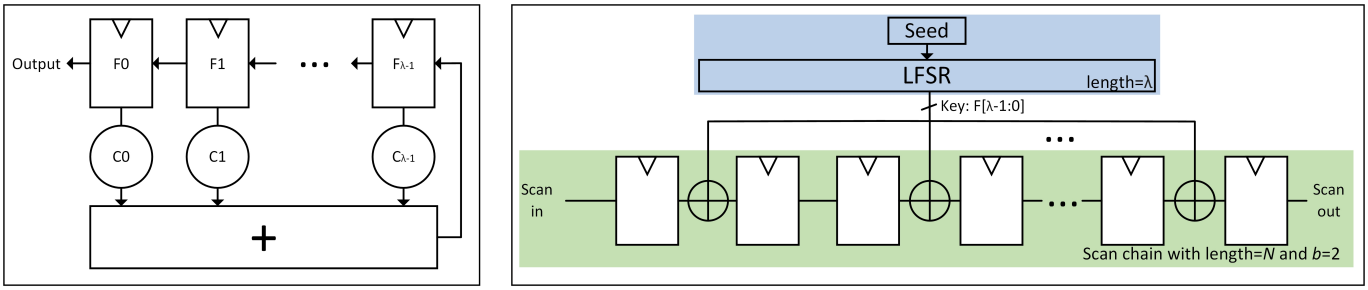
To obtain enough algebraic expressions, our attack shifts in sequence of logic 0s into the oracle scan chain obfuscated by the LFSR and captures the corresponding scan outputs $\boldsymbol{o}$. This is known as *flushing* the scan chain [12]. As we show below, choosing logic 0s to scan in instead of random bits simplifies the algebraic expression of the scan output and corresponding final system of equations.

In particular, we can derive an algebraic representation of the secure scan chain. The matrix representation of the LFSR states reveals many properties and can be derived from Equation 2 as follows

$$\begin{pmatrix} f_0^{t+1} \\ \vdots \\ f_{\lambda-2}^{t+1} \\ f_{\lambda-1}^{t+1} \end{pmatrix} = \begin{pmatrix} 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \\ c_0 & c_1 & \cdots & c_{\lambda-1} \end{pmatrix} \begin{pmatrix} f_0^t \\ \vdots \\ f_{\lambda-2}^t \\ f_{\lambda-1}^t \end{pmatrix} \tag{3}$$

where, t and $t+1$ represent the current and next cycle, respectively, and f_i^t denotes the state value of F_i at time step t. We will refer to this transition matrix as $\boldsymbol{T}$. The state at any

[1] MUXes can also be used to selectively invert the scan bit by muxing between the Q and Q_{bar} outputs of the scan FFs [9].



(a) LFSR (b) dynamically secured scan chain

Fig. 1: LFSR and basic structure of a dynamically secured scan chain

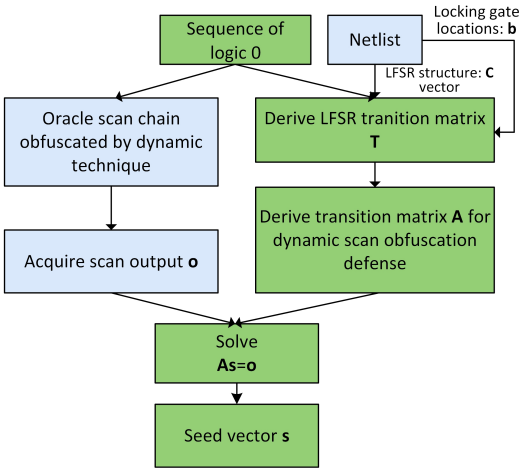


Fig. 2: Flow of the proposed attack

time step t' can then be derived from the LFSR seed and $\boldsymbol{T}$ as follows

$$\begin{pmatrix} f_0^{t'} \\ \vdots \\ f_{\lambda-2}^{t'} \\ f_{\lambda-1}^{t'} \end{pmatrix} = \begin{pmatrix} 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \\ c_0 & c_1 & \cdots & c_{\lambda-1} \end{pmatrix}^{t'} \begin{pmatrix} s_0 \\ \vdots \\ s_{\lambda-2} \\ s_{\lambda-1} \end{pmatrix} \tag{4}$$

To simplify this representation, we use the matrix and vector forms as follows

$$\boldsymbol{f}^{t+1} = \boldsymbol{T} * \boldsymbol{f}^{t} \tag{5}$$

$$\boldsymbol{f}^{t'} = \boldsymbol{T}^{t'} * \boldsymbol{s} \tag{6}$$

Using Equation 6, we can symbolically represent the key input of any locking gate driven by the ith stage of the LFSR at time step t':

$$f_i^{t'} = (\boldsymbol{T}^{t'} * \boldsymbol{s})[i] \tag{7}$$

We observe that when logic 0s go through the scan chain, they are simply XOR with keys $f_i^{t'}$. We can thus derive the symbolic expression for the expected values of the scan out signal. Let $\boldsymbol{o_m}$ correspond to the scan output associated with the mth scan input. We then have

$$\begin{aligned} \boldsymbol{o_m} =& (\boldsymbol{T}^m \boldsymbol{s})[0] + (\boldsymbol{T}^{m+b} \boldsymbol{s})[1] + (\boldsymbol{T}^{m+2b} \boldsymbol{s})[2] \\ &+ ... + (\boldsymbol{T}^{m+(\lambda-1)b} \boldsymbol{s})[\lambda-1] \end{aligned} \tag{8}$$

By introducing an identity matrix $\boldsymbol{R}$ with shape $\lambda * \lambda$ and factoring out $\boldsymbol{s}$, we can further simplify this expression as follows

$$\begin{aligned} \boldsymbol{o_m} =& [\boldsymbol{r_0} \boldsymbol{T}^m + \boldsymbol{r_1} \boldsymbol{T}^{m+b} + \boldsymbol{r_2} \boldsymbol{T}^{m+2b} \\ &+ ... + \boldsymbol{r_{\lambda-1}} \boldsymbol{T}^{m+(\lambda-1)b}] \boldsymbol{s} \end{aligned} \tag{9}$$

where $\boldsymbol{r_i}$ is the ith row of $\boldsymbol{R}$. The size of the first term $\boldsymbol{a} = \boldsymbol{r_0} \boldsymbol{T}^m + ... + \boldsymbol{r_{\lambda-1}} \boldsymbol{T}^{m+(\lambda-1)b}$ is $1 * \lambda$. Using the above o_m symbolic equation repeatedly for λ clock cycles and extracting their first term a, we can compose a system of linear equations in GF(2)

$$\boldsymbol{A} \boldsymbol{s} = \boldsymbol{o} \tag{10}$$

where $\boldsymbol{A}$ consists of λ $\boldsymbol{a}$'s and $\boldsymbol{o}$ is the corresponding captured scan outputs. Our attack completes by solving this system of equations in GF(2).

B. Analysis of the Proposed Attack

Since the system of linear equations in Eq. 10 is based on the physical structure of the circuit, it is guaranteed to be solvable. If $\boldsymbol{A}$ is full-rank, the solution yields the unique secret seed vector $\boldsymbol{s}$. Otherwise, the solution yields a set of potential seed vectors characterized by a particular solution of $\boldsymbol{A}\boldsymbol{s} = \boldsymbol{o}$ along with the null space of $\boldsymbol{A}$. More precisely, when the rank is k less than λ, there are 2^k possible seeds. These seeds can be used in further analysis, such as brute-force or SAT attacks, possibly in conjunction with attacking the combinational logic.

State-of-the-art secure chains are protected by a shadow chain which prevents the scan chain from being influenced by the LFSR for first λ clock cycles [11]. Since the scan chain is longer than the LFSR, the first o fully affected by the LFSR will be scanned out at cycle $N+1$. Interestingly, our attack can circumvent this defense by simply skipping the first N scan outputs and collecting the next λ scan outputs to compose the matrix $\boldsymbol{A}$.

C. Attack on a MISR

Figure 3 shows the structure of dynamically secured scan chain with a MISR, where the length of every chain is N, the Boolean values d_i define the structure of the MISR, and D_i represent the internal Boolean state of MISR that is available for reading after every round of tests. We can observe that

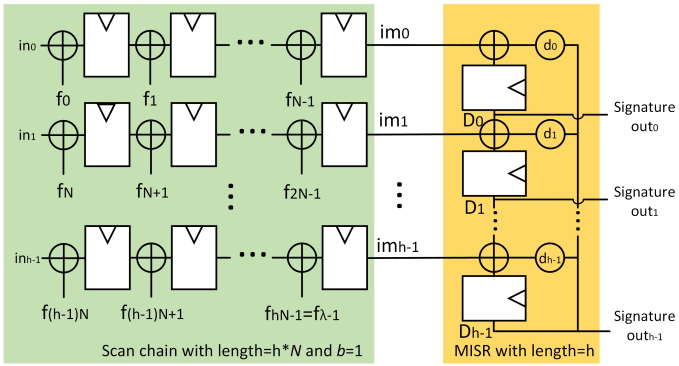


Fig. 3: Structure of a secured scan chain with MISR

the MISR thwarts the direct access to scan outputs im_i. Importantly, the h XOR gates in MISR are locking gates which corrupt the scan outputs im and make attacks that demand direct access to scan outputs ineffective. Therefore, it is important to integrate the MISR into our algebraic model.

In our attack on scan chains with a MISR, we still shift in a sequence of logic 0s into the scan chain. After $2N$ cycles, the MISR forms the signature outputs D_i^{2N} which we read out. First, we derive the scan outputs im_i from the LFSR keys f:

$$im_i^t = \sum_{r=0}^{N-1} f_{r+iN}^{t-N+r} \tag{11}$$

where im_i^t denotes the scan output of i^{th} chain at cycle t, the sum is addition in GF(2), and all f's are be obtained using Equation 6. Then, we derive D_i^t as follows

$$D_0^t = im_0^{t-1} + d_0 * D_{h-1}^{t-1} \tag{12}$$

$$D_i^t = im_i^{t-1} + D_{i-1}^{t-1} + d_i * D_{h-1}^{t-1} \quad for\ i > 0 \tag{13}$$

where D_i^t represents the internal values of the MISR stage i at cycle t and the initial D_i^0 are reset to 0. After $2N$ cycles, the signature outs are formed and available for reading:

$$signature\ out_i = D_i^{2N} \tag{14}$$

where every signature out is an equation in terms of seed bits. Thus we obtain h such equations in each round of testing.

We do not reset the LFSR but, as is typical, we reset the MISR at the beginning of every test sequence. Hence we require $\lambda/h = h*N/h = N$ tests, each generating h equations, to obtain a sufficient number of equations to recover the secret seed. Similar to the analysis in Section III-B, a unique seed vector s is acquired in the case that these equations are full-rank, otherwise, we acquire a set of potential seed vectors.

IV. Experimental Results

A. Experiment Setup

Our experiments in Sections IV-B and IV-D compare our algebraic attack to SAT attacks on scan chains and thus excludes a MISR.[2] Both experiments demonstrate results for different key lengths. Since our attack isolates the scan chain, LFSR, and MISR, there is no need to model the combinational logic driven by the scan chain. For experiments in Sections IV-B and IV-C, we assume the key length λ equals the scan chain length (N without a MISR and hN with a MISR), i.e., we set $b = 1$, and the update of the LFSR is synchronized to the scan clock, which is also presumed to be the most secure defense. In addition, we assumed the existence of a shadow chain of length λ. We used MATLAB to generate the LFSR transition matrix $\boldsymbol{T}$, transition matrix of the secure scan chain $\boldsymbol{A}$ and MISR signature out recursively. We then utilized the MATLAB function *gflineq*() and, when necessary, *gf2null*() to identify all the solutions over GF(2). For each key length, we randomly chose 10 configuration vectors c, constrained to have $c_0 = 1$, made all $d_i = 1$, and measured the average run-time including the generation of matrix $\boldsymbol{A}$ and $\boldsymbol{T}$ and the solving of the system of linear equations.

For experiments in Section IV-D, we incorporated dynamically secured scan chain into the ISCAS-89 benchmarks [26] in Verilog and perform the proposed attack on them. We added scan chains to circuits and randomly inserted key gates according to various tested key lengths, then extracted the key positions and applied the proposed attack. All experiments were run on an Intel i7-8700 CPU running at 3.20 GHz with 16-GB RAM.

B. Analysis of Basic Obfuscated Scan Chains

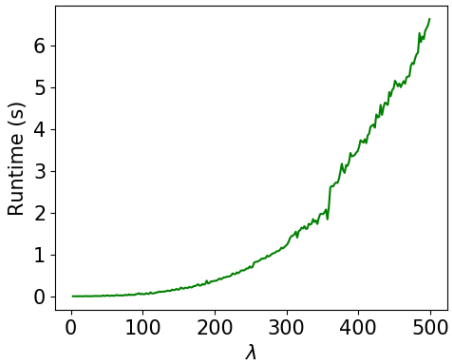


Fig. 4: Average attack run-times vs. number of key bits λ

Figure 4 plots the average attack run-time on the defense without MISR as the number of key bits λ ranging from 3 to 500. Even with 500 key bits, the attack on average took less than 7 second. The run-time trend suggests the complexity of our attack scales as no more than a low-degree polynomial. This is expected because solving a system of linear equations has complexity no worse than $O(\lambda^3)$. To further show the scalability of our proposed attack, we also tried $\lambda = 1000$ and the attack took 66 seconds.

Interestingly, 87% of the random configurations led to a unique seed, however, the average number of seeds is influenced by a few extreme cases and is 43.8. We further experimented with $\lambda = 500$ and explored 1000 different random configurations of c. The average number of seeds of 2.5 with the vast majority cases yielding a unique seed. We

[2]In practice, there often exists a bypass signal to circumvent the MISR. This analysis considers the case the attacker has access to such a signal.

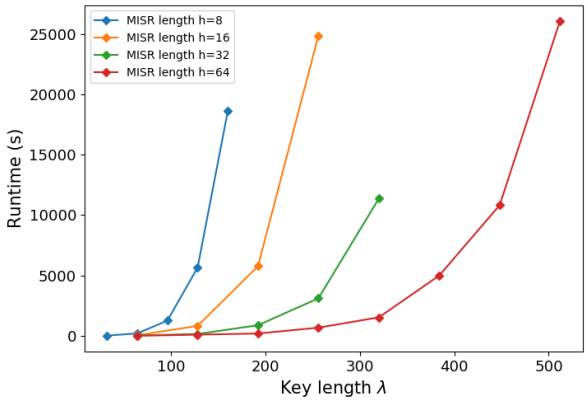


Fig. 5: Average attack run-times with different size MISRs

should emphasize however that for configurations where we could verify that the characteristic polynomial of the LFSR is primitive, a unique seed was always unveiled.

C. Analysis of Impact of MISRs

Figure 5 demonstrates the average attack run-times on the dynamically secured scan chain with different lengths of MISRs h as a function of varying key length λ constrained by the relationship $\lambda = h * N$. The experiments with $\lambda > 300$ timed-out after 8 hours for smaller values of h. This is because with a MISR, we obtain only h equations every test round (i.e., $2N$ cycles) compared to the case without a MISR which produces roughly one equation every cycle. For practical MISR lengths that are typically greater than 16 [27], the attack run-time remains under 8 hours for key lengths of under 250. In all cases, the run-time is dominated by the computation of the various powers of the system matrix T.[3]

D. Comparison to Other Attacks

State-of-the-art attacks on dynamically secured scan chains are based on SAT attacks [12], [13]. In particular, [13] observed that the LFSR logic can be unrolled and combined with the associated combinational logic circuit and then attacked by SAT. They tested their attack framework with various ISCAS benchmarks and demonstrated that even with 368 key bits they could successfully uncover the LFSR seed in less than 23 hours. However, their attack assumed the combinational logic was not logic locked, in contrast to what is advocated in [11]. This is an important limitation because several combinational obfuscation techniques are known to be SAT resistant [28], [29] which would hamper the effectiveness SAT attacks. Furthermore, the SAT attacks rely on the access to scan outputs and thus should consider the impact of a MISR.

In contrast, our proposed attack isolates the scan chain and in particular does not involve modeling or attacking the combinational logic and thus circumvents any effort to obfuscate the combinational logic. Moreover, since it leverages

[3]Although not experimentally tested, we note that this computation can be parallelized across multiple processors by pre-computing increasingly larger powers of T via iterative squaring.

TABLE I: Comparison of SAT and proposed attacks

Benchmark	Key bits	SAT attack run-times (secs)	Proposed attack run-times (secs)	Improv. ratio
s5378	10	12.98	0.04	325
	20	29.39	0.05	588
	30	66.84	0.03	2228
	40	1823.79	0.04	45595
s9234	10	15.48	0.01	1548
	20	37.87	0.05	757
	30	95.75	0.06	1596
	40	4071.83	0.04	101796
s15850	10	39.31	0.01	3931
	20	90.13	0.01	9013
	30	151.08	0.05	3022
	40	2352.71	0.04	58818
s13207	10	46.09	0.03	1536
	20	107.52	0.01	10752
	30	214.45	0.03	7148
	40	5680.52	0.02	284026
Average improvement				33292
Benchmark	Key bits	SAT attack run-times [13] (secs)	Proposed attack run-times (secs)	Improv. ratio
s38584	144	925	0.54	1713
	160	557	0.65	857
	176	1175	0.73	1610
	192	872	1.00	872
	208	4897	1.17	4185
	224	4792	1.28	3744
	240	2880	1.44	2000
	256	9219	1.74	5298
	272	2831	1.92	1474
	288	15025	2.10	7155
	304	6465	2.39	2705
	320	12745	2.48	5139
	336	10678	2.55	4187
	352	11502	2.73	4213
	368	11173	3.90	2865
s38417	144	862	0.73	1181
	160	583	0.92	634
	176	1711	1.48	1156
	192	945	1.12	844
	208	1947	1.34	1453
	224	1999	1.42	1408
	240	2252	1.53	1472
	256	16220	1.90	8537
	272	14603	2.10	6954
	288	24546	2.28	10766
	304	33591	2.63	12772
	320	62135	2.79	22271
	336	81504	2.90	28105
	352	74140	3.03	24469
	368	70591	4.51	15652
s35932	144	281	0.77	365
	160	634	0.69	919
	176	372	1.26	295
	192	618	1.18	524
	208	597	1.38	433
	224	1007	2.06	489
	240	810	2.24	362
	256	832	2.71	307
	272	1364	3.00	455
	288	2657	3.41	779
	304	1881	2.87	655
	320	2992	3.02	991
	336	2008	4.78	420
	352	2270	5.14	442
	368	3231	4.79	675
Average improvement				4307

the algebraic nature of the problem it can integrate the MISR into the attack.

Table I compares the SAT and proposed attack run-times. We reproduced the SAT attack and successfully applied them to four moderate-sized ISCAS circuits with key sizes between 10 and 40 bits. On larger circuits our implementation timed out after 2 days and we thus also compare to run-times reported from [13]. The disparity of performance is likely because [13] used a tailored rather than off-the-shelf SAT solver and used a more powerful computer. In both cases, however, the proposed attack recovers the set of potential seeds are always over two orders of magnitude faster than the equivalent SAT attack and on average over 4300x faster. Again, this run-time benefit would be even larger if the combinational circuits were also locked.[4]

V. Summary and Conclusions

This paper presents a scalable GF(2) algebraic attack on scan chains that are obfuscated by dynamic keys generated by an LFSR. The experimental results demonstrate that the defenses with 500 key bits can be cracked in 7 seconds. The power of the proposed attack stems from the observation that all operations in the defensive circuitry can be modeled in GF(2). The results highlight that while SAT attacks are powerful, algebraic attacks should not be overlooked as they can be dramatically more efficient.

The results lead to several ideas of improving secure scan chains to protect against such algebraic attacks. For example, obfuscating the structure of the LFSR or using non-linear LFSRs [30], [31] may make anticipating the scan output vectors more challenging. Studying whether such additional defenses can be circumvented with more sophisticated algebraic attacks becomes an important and interesting area of future work.

References

[1] J. A. Roy, F. Koushanfar, and I. L. Markov, "Ending Piracy of Integrated Circuits," *Computer*, vol. 43, no. 10, pp. 30–38, 2010.

[2] M. Tehranipoor and F. Koushanfar, "A Survey of Hardware Trojan Taxonomy and Detection," *IEEE Des. Test. Comput.*, vol. 27, no. 1, pp. 10–25, 2010.

[3] B. Yang, K. Wu, and R. Karri, "Secure Scan: A Design-for-Test Architecture for Crypto Chips," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 25, no. 10, pp. 2287–2293, 2006.

[4] R. Nara, N. Togawa, M. Yanagisawa, and T. Ohtsuki, "Scan-based Attack against Elliptic Curve Cryptosystems," in *15th ASP-DAC*, 2010.

[5] J. DaRolt, A. Das, G. Natale, M. Flottes, B. Rouzeyre, and I. Verbauwhede, "A New Scan Attack on RSA in Presence of Industrial Countermeasures," in *COSADE*, 2012.

[6] S. Potluri, A. Aysu, and A. Kumar, "SeqL: Secure Scan-Locking for IP Protection," in *2020 21st International Symposium on Quality Electronic Design (ISQED)*, 2020, pp. 7–13.

[7] M. Portolan, V. Reynaud, P. Maistri, and R. Leveugle, "Dynamic Authentication-Based Secure Access to Test Infrastructure," in *2020 IEEE European Test Symposium (ETS)*, 2020, pp. 1–6.

[8] E. Valea, M. Da Silva, M.-L. Flottes, G. Di Natale, and B. Rouzeyre, "Stream vs block ciphers for scan encryption," *Microelectronics Journal*, vol. 86, pp. 65–76, 2019.

[9] R. Karmakar, S. Chattopadhyay, and R. Kapur, "A Scan Obfuscation Guided Design-for-Security Approach for Sequential Circuits," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 67, no. 3, pp. 546–550, 2020.

[10] X. Wang, D. Zhang, M. He, D. Su, and M. Tehranipoor, "Secure Scan and Test Using Obfuscation Throughout Supply Chain," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst*, vol. 37, no. 9, pp. 1867–1880, 2018.

[11] M. M. Rahman, A. Nahiyan, S. Amir, F. Rahman, F. Farahmandi, D. Forte, and M. Tehranipoor, "Dynamically Obfuscated Scan Chain To Resist Oracle-Guided Attacks On Logic Locked Design," *IACR Cryptol. ePrint Arch.*, vol. 2019, p. 946, 2019.

[12] L. Alrahis, M. Yasin, N. Limaye, H. Saleh, B. Mohammad, M. Alqutayri, and O. Sinanoglu, "ScanSAT: Unlocking Static and Dynamic Scan Obfuscation," *IEEE Transactions on Emerging Topics in Computing*, pp. 1–1, 2019.

[13] N. Limaye and O. Sinanoglu, "DynUnlock: Unlocking Scan Chains Obfuscated using Dynamic Keys," in *DATE*, 2020, pp. 270–273.

[14] G. Sengar, D. Mukhopadhyay, and D. R. Chowdhury, "Secured Flipped Scan-Chain Model for Crypto-Architecture," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 26, no. 11, pp. 2080–2084, 2007.

[15] N. T. Courtois and G. V. Bard, "Algebraic Cryptanalysis of the Data Encryption Standard," in *IMA International Conference on Cryptography and Coding*. Springer, 2007, pp. 152–169.

[16] N. T. Courtois and W. Meier, "Algebraic Attacks on Stream Ciphers with Linear Feedback," in *Advances in Cryptology — EUROCRYPT*, E. Biham, Ed. Springer, 2003, pp. 345–359.

[17] Li-Ren Huang, Jing-Yang Jou, and Sy-Yen Kuo, "Gauss-elimination-based generation of multiple seed-polynomial pairs for LFSR," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 16, no. 9, pp. 1015–1024, 1997.

[18] H. Wunderlich, "Self test using unequiprobable random patterns," in *Proc. IEEE 17th InternationalSymposium on Fault-Tolerant Computing, FTCS-17*, 1987.

[19] J. Da Rolt, G. Di Natale, M.-L. Flottes, and B. Rouzeyre, "Are advanced DfT structures sufficient for preventing scan-attacks?" in *2012 IEEE 30th VLSI Test Symposium (VTS)*, 2012, pp. 246–251.

[20] R. Shiva Prasad, A. Siripagada, S. Selvaraj, and N. Mohankumar, *Random Seeding LFSR-Based TRNG for Hardware Security Applications*. Springer, 2019, pp. 427–434.

[21] J. Melià-Seguí, J. Garcia-Alfaro, and J. Herrera-Joancomartí, "Multiple-polynomial LFSR based pseudorandom number generator for EPC Gen2 RFID tags," in *IECON 2011 - 37th Annual Conference of the IEEE Industrial Electronics Society*, 2011, pp. 3820–3825.

[22] W. Wardlaw, "A Matrix Model for the Linear Feedback Shift Register," Naval Research Lab, Tech. Rep., July 1989.

[23] R. Karmakar, S. Chattopadhyay, and R. Kapur, "Encrypt Flip-Flop: A Novel Logic Encryption Technique For Sequential Circuits," *ArXiv*, vol. abs/1801.04961, 2018.

[24] F. Elguibaly and M. W. El-Kharashi, "Multiple-input signature registers: an improved design," in *PACRIM.*, vol. 2, 1997, pp. 519–522 vol.2.

[25] N. Courtois, A. Klimov, J. Patarin, and A. Shamir, "Efficient Algorithms for Solving Overdefined Systems of Multivariate Polynomial Equations," in *Advances in Cryptology — EUROCRYPT*, B. Preneel, Ed. Berlin, Heidelberg: Springer, 2000, pp. 392–407.

[26] F. Brglez, D. Bryan, and K. Kozminski, "Combinational profiles of sequential benchmark circuits," in *IEEE International Symposium on Circuits and Systems,*, 1989, pp. 1929–1934 vol.3.

[27] K. N. Devika and R. Bhakthavatchalu, "Programmable MISR modules for logic BIST based VLSI testing," in *ICCICCT*, 2016, pp. 699–703.

[28] M. Yasin, A. Sengupta, M. T. Nabeel, M. Ashraf, J. Rajendran, and O. Sinanoglu, "Provably-secure Logic Locking: From Theory to Practice," in *ACM CCS*, 2017, pp. 1601–1618.

[29] K. Shamsi, T. Meade, M. Li, D. Z. Pan, and Y. Jin, "On the Approximation Resiliency of Logic Locking and IC Camouflaging Schemes," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 2, pp. 347–359, 2019.

[30] M. Hell, T. Johansson, A. Maximov, and W. Meier, *The Grain Family of Stream Ciphers*. Springer, 2008, pp. 179–190.

[31] S. W. Golomb *et al.*, *Shift Register Sequences*. Aegean Park Press, 1967.

[4]We have posted the code of our attack to assist other researchers to reproduce our method. https://github.com/Charles-lin-2020/GF-Flush-Attack.git