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

Dake Chen, Member, IEEE, Chunxiao Lin, Peter A. Beerel, Senior Member, IEEE

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, the attack times are about one hundredth of state-of-the-art SAT based attacks on the same defense. 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]–[5].

The state of the art defenses involve applying dynamic keys to obfuscate the scan chain [6]–[8]. They leverage a linear feedback shift register (LFSR) that controls XOR gates along the scan chain to pseudo-randomly invert the scan chain sequence. The pseudo-random sequence is dependent on the seed of the LFSR which must remain secret to ensure security. Recently, some SAT based attacks [9], [10] were proposed to unveil the seed by converting the scan flip-flops to pseudo input and outputs and thereby modeling the sequential circuit and LFSR as a combinational circuit that can be analyzed through well-known SAT attacks. The work [8] 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 [11]. Here all flip-flops on scan chain are reset to 0 and the attack examines the initial sequence of scan out bits. Because 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 [7], [6] 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-based attacks [9], [10] 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 crypto-analysis [12], including attacks on LFSRs [13], and automatic test pattern generation [14], [15]. 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 scales as a low-degree polynomial, recovering the key that is as long as 500 bits in less than 7 seconds. The attack times are about one hundredth of state-of-the-art SAT based attacks on the same defense.

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). Because MISRs also consists of XOR gates and FFs they can be modeled, analyzed, and thus included in our attack. To the best of our knowledge, this is the first attack on obfuscated scan chains that considers the impact of test compression logic. Although slower with MISRs, we demonstrate our attack times remain manageable.

The remainder of this paper is organized as follows. 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 a pseudo-random number generator in many cryptographic and secure systems because of its lightweight, low overhead and high throughput [16], [17].

The generic structure of an LFSR is shown in Figure 1 where \( \lambda \) denotes its length and the Binary values \( c_0 \) to \( c_{\lambda-1} \) determine its feedback structure. The next state equation \( f_{i+1} \) can be represented as

\[
f_{i+1}^t = f_{i+1}^t, \quad \text{for } i \in [0, \lambda - 1]
\]

\[
f_{\lambda-1}^t = \sum_{j=0}^{\lambda-1} c_j f_j^t
\]
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 \( \text{GF}(2) \).

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 \( \lambda \) is \( 2^\lambda - 1 \) \[18\]. 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-based attacks \[9\] on static scan chain obfuscation techniques \[19\], state-of-the-art secure chains dynamically obscure scan chains using XORs that are driven by an LFSR \[6\]–\[8\] and pseudorandomly invert the scan sequence. The basic structure of these schemes is shown in Figure 1 where \( \lambda \) 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. 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) \[20\] illustrated in Figure 3.

Because 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-based attacks \[9\], \[10\]. 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.

1MUXes can also be used to selectively invert the scan bit by muxing between the \( Q \) and \( \overline{Q} \) outputs of the scan FFs \[6\].

### 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 \[10\], 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 $o$. This is known as flushing the scan chain [9]. 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

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

(3)

where, $t$ and $t + 1$ represent the current and next cycle, respectively. We will refer to this transition matrix as $T$. The state at any time step $t'$ can then be derived from the LFSR seed and $T$ as follows

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

(4)

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

$$f^{t+1} = T * f^t$$

(5)

$$f^{t'} = T^{t'} * s$$

(6)

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

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

(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 $o_m$ correspond to the scan output associated with the $m$th scan input. We then have

$$o_m = (T^m s)[0] + (T^{m+b} s)[1] + (T^{m+2b} s)[2] + \ldots + (T^{m+(\lambda-1)b} s)[\lambda - 1]$$

(8)

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

$$o_m = r_0 T^m + r_1 T^{m+b} + r_2 T^{m+2b} + \ldots + r_{\lambda-1} T^{m+(\lambda-1)b} s$$

(9)

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

$$A s = o$$

(10)

where $A$ consists of $\lambda$ $a$’s and $o$ 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 $A$ is full-rank, the solution yields the unique secret seed vector $s$. Otherwise, the solution yields a set of potential seed vectors characterized by a particular solution of $A s = o$ along with the null space of $A$. More precisely, when the rank is $k$ less than $\lambda$, 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 $\lambda$ clock cycles [5]. Because 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 $\lambda$ scan outputs to compose the matrix $A$.

C. Attack on 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 the MISR thwarts the direct access to scan outputs $i_m$. Importantly, the $h$ XOR gates in MISR are locking gates which corrupt the scan outputs $i_m$ 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 sequence of logic 0s into scan chain, after $2N$ cycles, the MISR forms the signature outs $D_i^{2N}$ which we can read out.
In following equations, all superscripts denote the time stamps. First of all, we derive the scan outputs \( im_i \) from the LFSR keys \( f \):

\[
im_i^t = \sum_{r=0}^{N-1} f_{r+iN}^t + r
\]

where \( im_i^t \) denotes the scan output of \( i^{th} \) chain at cycle \( t \), the sum is addition in GF(2), and all \( f \) can be obtained using Equation 6. Then, we can derive \( D_i^t \) as follows:

\[
D_0^t = im_0^{t-1} + d_0 * D_{h-1}^{t-1}
\]

\[
D_i^t = im_i^{t-1} + D_{i-1}^{t-1} + d_i * D_{h-1}^{t-1} \text{ for } i > 0
\]

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:

\[
signature out_i = D_i^{2N}
\]

where every signature out is an equation with respect to seed bits, thus we obtain \( h \) such equations in each round of test.

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 involving \( h \) equations with respect to seed bits, to obtain a sufficient number of equations to recover the secret seed. Similar to the analysis in Section III-B, a unique seed vector \( s \) would be acquired in the case that these equations are full-rank, otherwise, we are able to acquire a set of potential seed vectors.

IV. EXPERIMENTAL RESULTS

A. Experiment Setup

Our first experiment compares our algebraic attack to SAT-based attacks on scan chains and thus excludes a MISR. 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. We assume the key length \( \lambda \) equals the scan chain length \( (N \text{ without a MISR and } h\*N \text{ with a MISR}) \), i.e., we set \( h = 1 \). 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 \( \lambda \).

We used MATLAB to generate the LFSR transition matrix \( T \), transition matrix of the secure scan chain \( A \) 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 \( A \) and \( T \) and the solving of the system of linear equations. All experiments were run on Intel i7-8700 CPU running at 3.20 GHz with 16-GB RAM.

B. Analysis of Basic Obfuscated Scan Chains

Figure 4 plots the average attack run-time on the defense without MISR as the number of key bits \( \lambda \) 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 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 LFSR length \( \lambda \) 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.
powers of \( T \) parallelized across multiple processors by pre-computing increasingly larger matrices. This becomes an important and interesting area of future work. However, their attack assumed the combinational logic was not logic locked, in contrast to what is advocated in [3]. This is an important limitation because several combinational logic techniques are known to be SAT-resistant [10], [11], which would complicate this type of attack. Furthermore, the SAT-based attacks rely on the access to scan outputs. The presence of a MISR may restrict this access and should not be neglected.

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 also unlock the combinational logic. Moreover, because it leverages the algebraic nature of the problem it can integrate the MISR into the model for attacking, and for the same defenses without MISR, it recovers the set of potential seeds orders of magnitude faster than equivalent SAT-based attacks.

D. Comparison to Other Attacks

State-of-the-art attacks on dynamically secured scan chains are based on SAT attacks [9], [10]. In particular, [9] observed that the LFSR logic can be unrolled and combined with the associated combinational logic circuit and then attacked with SAT. They tested their attack framework with various ISCAS benchmarks and demonstrated that even with 368 key bits they can successfully uncover the LFSR seed in less than one hour. However, their attack assumed the combinational logic was not logic locked, in contrast to what is advocated in [8]. This is an important limitation because several combinational logic techniques are known to be SAT-resistant [10], [11], which would complicate this type of attack. Furthermore, the SAT-based attacks rely on the access to scan outputs. The presence of a MISR may restrict this access and should not be neglected.

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 also unlock the combinational logic. Moreover, because it leverages the algebraic nature of the problem it can integrate the MISR into the model for attacking, and for the same defenses without MISR, it recovers the set of potential seeds orders of magnitude faster than equivalent SAT-based attacks.

V. CONCLUSIONS AND DISCUSSION

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 significantly 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 LFSR-\( N \) 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. Tehraniipoor 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, “Scannable-Based Attack against Elliptic Curve Cryptosystems,” in 15th ASP-DAC, 2010.

[5] J. DaRoit, A. Das, G. Natale, M. Flottes, B. Rouayheb, and J. Verbauwhede, “A New Scan Attack on RSA in Presence of Industrial Countermeasures,” in COSADE, 2012.

[6] R. Karmanak, S. Chattopadhyay, and R. Kapur, “A Scan Obfuscation Guided Design-for-Security Approach for Sequential Circuits,” IEEE Trans. Circuits Syst. I, Exp. Briefs, vol. 67, no. 3, pp. 546–550, 2020.

[7] X. Wang, D. Zhang, M. He, D. Su, and M. Tehraniipoor, “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.

[8] M. M. Rahman, A. Nahiyan, S. Mir, F. Rahman, F. Farahmandi, D. Forte, and M. Tehraniipoor, “Dynamically Obfuscated Scan Chain To Resist Oracle-Guided Attacks On Logic Locked Design,” IACR Cryptol. ePrint Arch., vol. 2019, p. 946, 2019.

[9] N. Alrahis, M. Yasin, N. Limaye, H. Saleh, B. Mohammad, M. Alquatry, and O. Sinanoglu, “ScanSAT: Unlocking Static and Dynamic Scan Obfuscation,” IEEE Transactions on Emerging Topics in Computing, pp. 1–1, 2019.

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

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] H. Wunderlich, “Self test using unequiplorable random patterns,” in Proc. IEEE 17th InternationalSymposium on Fault-Tolerant Computing, FTCS-17, 1987.

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

[17] J. Meliá-Seguí, J. García-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.

[18] Wardlaw, “A Matrix Model for the Linear Feedback Shift Register,” Naval Research Lab, Tech. Rep., Jul. 1989.

[19] R. Courtois, S. Chattopadhyay, and R. Kapur, “Encrypt Flip-Flop: A Novel Logic Encryption Technique For Sequential Circuits,” ArXiv, vol. abs/1801.04961, 2018.

[20] F. Elguibaly and M. W. El-Kharashi, “Multiple-input signature registers: an improved design,” in PACTIM., vol. 2, 1997, pp. 519–522 vol.2.

[21] 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.

[22] K. N. Devika and R. Bhaktavatchalal, “Programmable MISR modules for logic BIST based VLSI testing,” in ICCIICC, 2016, pp. 699–703.

[23] 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.

[24] 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.

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

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