SIGNATURE ANALYSIS BY QUADRATIC COMPRESSORS[1]

P. Nagvajara and M.G. Karpovsky
Research Laboratory for Design and Testing of
Computer and Communication Systems
Department of Electrical, Computer and System Engineering
Boston University,
44 Cummington Street, Boston, Massachusetts 02215
(617) 353-9592

Abstract

An alternative compression of test responses technique (signature analysis) for a built-in-self-test (BIST) VLSI design is presented. With the assumption that a fault-free response is uniformly distributed, the proposed quadratic compression scheme is shown to be optimal with respect to the lower bound on the maxima conditional error-masking probability Q(e) given error e (e≠0). An implementation of the quadratic compression scheme requires slightly more hardware than a parallel signature analyzer by linear-feedback shift Registers, LFSRs. However, the advantage of a quadratic compression technique over linear compression techniques (by LFSRs) is that, the conditional error-masking probability, Q(e), given an error sequence e (e≠0) for a quadratic scheme is constant, which implies an equal protection against all error patterns. In other words, quadratic compressors are robust with respect to a statistics of errors, since the total error-masking probability $Q_{total} = \sum_{e \neq 0} Q(e) Pr[\, e \,|\, e \neq 0 \,]$ is independent on the distribution $Pr[\, e \,|\, e \neq 0 \,]$.

1 Introduction

Compression of test responses (signature analysis) is the essential conpect in the built-in-self-test (BIST) design for VLSI devices [1-8]. Since the difficulty in testing VLSI circuits is related to an excessive among of reference data to be stored. To reduce the storage size of the reference data, test responses are compressed into a k-bit word called "signature". A block diagram of a BIST design for VLSI device is given in Fig. 1. The test response in Fig. 1 is considered to be a stream of {0,1} which corresponds to the "scan-out" data for a scan design.

---

[1]This work was supported by the National Science Foundation under Grant DCR-8317763.

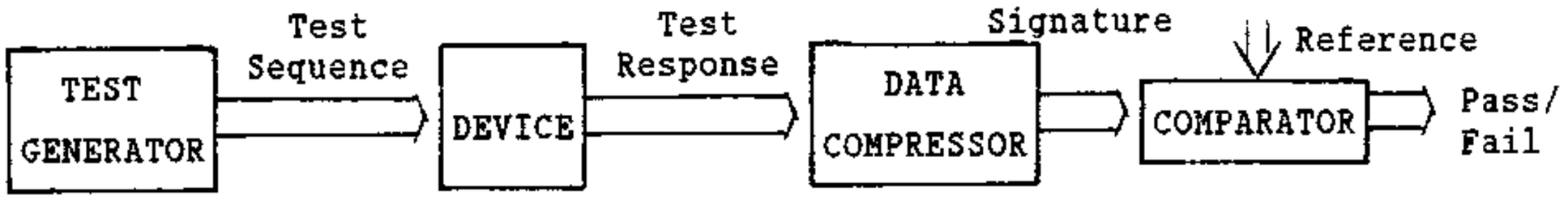

Fig. 1. BIST Design for VLSI Device

An alternative compression technique based on a quadratic function is presented. The proposed quadratic compressors provide for an equal error-detection capability for all patterns of erroneous symbols in the observed test response. Hence, quadratic compressors offer a reliable estimation of fault coverages when the distribution of errors is unknown.

2 Quadratic Compressors

The concept of quadratic compressor is based on the quadratic nonrepetitive function of 2T variables over a finite field of q elements, GF(q), $q=2^k$ [9],

$$y(\tilde{z}) = \tilde{z}_0\tilde{z}_1 \oplus \tilde{z}_2\tilde{z}_3 \oplus \ldots \oplus \tilde{z}_{2T-2}\tilde{z}_{2T-1},\ \tilde{z} \in V_{2T} \text{ over } GF(q),\ \tilde{z}_t \in GF(q). \qquad (1)$$

Let $\tilde{z}$ be a sequence of test responses consists of N=2kT bits. Rather, we consider $\tilde{z}$ as a sequence of k-bit symbols $\{z_t, t=0,1,\ldots,2T-1\}$ (see (1)). The quadratic signature $y(\tilde{z})$ is computed by multiplying two k-bit blocks $\tilde{z}_t\tilde{z}_{t+1}$ and accumulating the sum. Note that, multiplication of symbols from $GF(2^k)$ is a multiplication of polynomials degree less that k modulo an irreducible polynomial degree k, over {0,1}, and the addition, $\oplus$, is a polynomial (vector) addition modulo 2. The following theorem states that a quadratic compressor is optimal with respect to the lower bound on the maxima conditional error-masking probability Q(e) given error e ($e \neq 0$) which implies equal protection against all error patterns.

Theorem 1

Let $g(\tilde{Z})$ be a system of r Boolean functions,

$$g(\tilde{Z}) = \{g_0(\tilde{Z}), g_1(\tilde{Z}), \ldots, g_{r-1}(\tilde{Z})\}, \qquad (2)$$

arbitrarily chosen from the system

$$F(\tilde{Z}) = \{f_0(\tilde{Z}), f_1(\tilde{Z}), \ldots, f_{k-1}(\tilde{Z})\}, \quad k \geq r, \qquad (3)$$

where $F(\tilde{Z})$ is constructed by

$$y(\tilde{Z}) = \tilde{Z}_0\tilde{Z}_1 \oplus \tilde{Z}_2\tilde{Z}_3 \oplus \ldots \oplus \tilde{Z}_{2T-2}\tilde{Z}_{2T-1} = f_{k-1}(\tilde{Z})x^{k-1} \oplus f_{k-2}(\tilde{Z})x^{k-2} \oplus \ldots \oplus f_0(\tilde{Z}), \qquad (4)$$

and $\tilde{Z} \in V_{2T}$ over GF(q), $\tilde{Z}_i \in GF(q)$. Then the compressor $g(\tilde{Z})$ is optimal with

$$Q(e) = |\{(Z,e) \mid y(\tilde{Z})=y(z),\ \tilde{z}=z \oplus e\}|\ 2^{-N} \qquad (5)$$

$$= 2^{-r}, \text{ for all } e \neq 0 \qquad \square$$

From (5) one can see that error events $(\tilde{Z},Z)$ (ordered pairs of fault-free response and error) is masked if and only if the signature $y(\tilde{Z})$ $(\tilde{Z}=Z\oplus e)$ is equal to the reference $y(Z)$ in which the number of error events for any given $e\neq 0$, in the case of quadratic compressors, is equal to 2^{N-r} where r is the size of signature.

In the case of linear compressor by LFSRs which can be characterized by a linear transformation H, the linear signature is given by

$$S(\tilde{Z}) = \tilde{z}\ H^T = Z\ H^T \oplus e\ H^T, \tag{6}$$

and error e is masked if and only if $e\ H^T=0$, hence, for the linear compressor Q(e) is either zero or one. Therefore, linear compressor is the worst compressor with respect to the lower bound on the maxima of Q(e).

Example 1. As the first example, consider linear and quadratic compressions of test responses for exhaustive pseudorandom testing of the circuit shown in Fig. 2. For the test sequence (0000, 1111, 1110, ..., 0111) (generated by an LFSR with $p(x)=x^4\oplus x\oplus 1$ as a feedback polynomial) test response sequences (binary sequence of length 16) are compressed into four-bit signatures (N=16, k=4). Two signatures are obtained—one by LFSR with feedback polynomial $p(x) = x^4 \oplus x \oplus 1$ and another by the quadratic compressor.

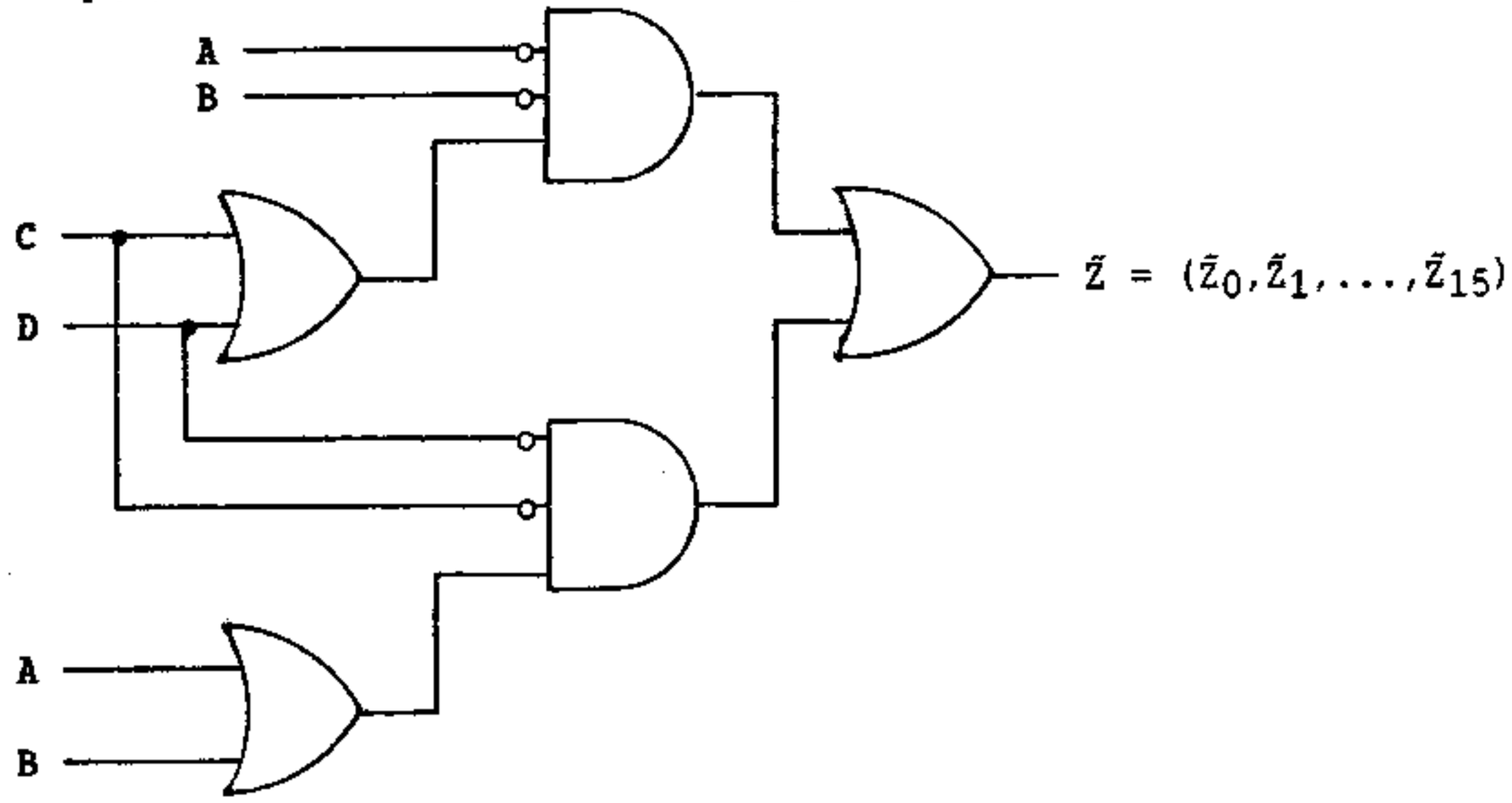

Fig. 2. Circuit Diagram— an Example Illustrating Advantages of Quadratic Compressors Over LFSR Compressors.

The quadratic compressor in this example can be described as follows. Let $\tilde{z} = (\tilde{z}_0,\tilde{z}_1,\ldots,\tilde{z}_{15})$ denote an observed test-response sequence. Then quadratic signature is computed by

$$y(\tilde{z}) = (\tilde{z}_0\oplus\tilde{z}_1x\oplus\ldots\oplus\tilde{z}_3x^3)\cdot(\tilde{z}_4\oplus\tilde{z}_5x\oplus\ldots\oplus\tilde{z}_7x^3)\ \oplus$$

$$(\tilde{z}_8\oplus\tilde{z}_9x\oplus\ldots\oplus\tilde{z}_{11}x^3)\cdot(\tilde{z}_{12}\oplus\tilde{z}_{13}\oplus\ldots\tilde{z}_{15}x^3)\ \text{modulo}\ x^4\oplus x\oplus 1. \tag{7}$$

In other words,

$$y(\tilde{z}) = u_0 v_0 \oplus u_1 v_1,\ u_i, v_i \in GF(2^4). \tag{8}$$

The fault coverages of both compression techniques are obtained from the number of single-stuck-at faults such that the observed signatures are equal to the correct signature divided by a total number of single-stuck-at faults in the circuit of Fig. 2. The fault coverage of the LSFR scheme is 56%, whereas the fault coverage of the quadratic-scheme is 100%. The reason that the LSFR compressor attains only 56% fault coverage (fails to detect 15 out of 34 faults) is that several faults in the circuit of Fig. 2 manisfest themselves as error patterns which are divisible by the feedback polynomial of the LFSR.

Example 2 The second example compares fault coverages of the quadratic compressor based on the function

$$y(\tilde{z}) = (\tilde{z}_0 \oplus \tilde{z}_1 x \oplus \tilde{z}_2 x^2)(\tilde{z}_3 \oplus \tilde{z}_4 x \oplus \tilde{z}_5 x^2) \text{ modulo } x^3 \oplus x \oplus 1, \tag{9}$$

that is,

$$y(\tilde{z}) = uv,\ u=(\tilde{Z}_0, \tilde{Z}_1, \tilde{Z}_2), v=(\tilde{Z}_3, \tilde{Z}_4, \tilde{Z}_5) \in GF(2^3) \text{(see Fig. 3)}, \tag{10}$$

with a linear Hamming (6,3) decoder given by

$$\begin{aligned} S_0 &= \tilde{z}_2 \oplus \tilde{z}_4 \oplus \tilde{z}_5, \\ S_1 &= \tilde{z}_1 \oplus \tilde{z}_3 \oplus \tilde{z}_5, \\ S_2 &= \tilde{z}_0 \oplus \tilde{z}_3 \oplus \tilde{z}_4. \end{aligned} \tag{11}$$

(These linear compressors have been used in [6-8]. A hardware realization of the quadratic compressor (9) is given in Section 3.2, Fig. 6).

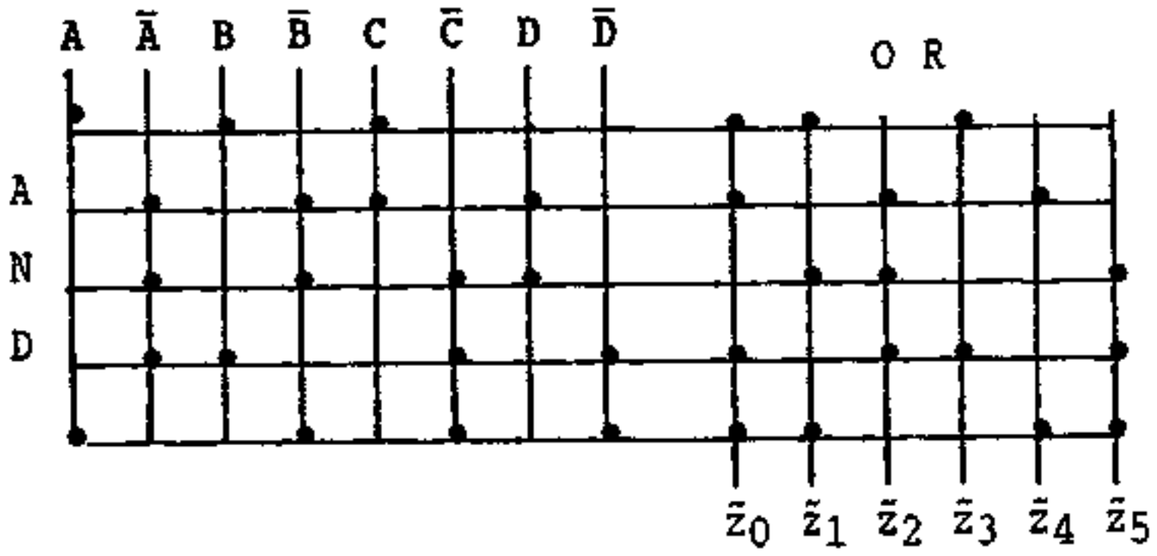

Fig. 3. Circuit Example where Faults are Masked when using a Linear Compression Scheme

The test procedure for the circuit given in Fig. 3 consists of the exhaustive test where every output pattern $(\tilde{z}_0, \tilde{z}_1, \tilde{z}_2, \tilde{z}_3, \tilde{z}_4, \tilde{z}_5)$ is compressed via a combinational circuit into a three-bit signature (N=6, k=3). The fault-free signatures corresponding to the compressed correct output

patterns for all 16 possible input combinations are kept as references.

The fault coverage for single-stuck-at faults of the linear single-error-correcting Hamming (6,3) decoder is 46% (fails to detect 40 out of 74 faults) which is unexceptable, whereas the quadratic compressor attains 100% fault coverage. This second example also brings up the point that the performance of linear compressors can be catastrophic when no imformation on possible error patterns is available.

3 Hardware Implementations and Complexities of Quadratic Compressors

Consider the following implementation of a quadratic compressor (Fig. 4).

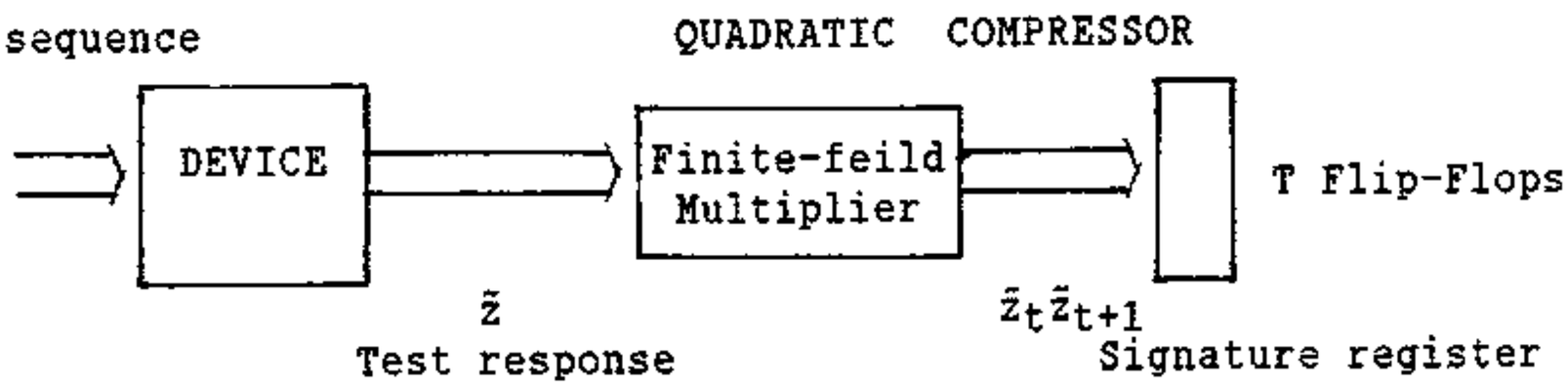

Fig. 4. Hardware Implementation of Quadratic Compressor

3.1 Sequential Quadratic Compressor

If the observed response, $\tilde{z}=z\oplus e$, is processed in a serial fashion, based on the quadratic function over $GF(2^k)$, $y(\tilde{z})= \tilde{z}_0\tilde{z}_1\oplus\tilde{z}_2\tilde{z}_3\oplus\ldots\oplus\tilde{z}_{2T-2}\tilde{z}_{2T-1}$, where $\tilde{z}$ is a binary sequence of length $N = 2kT$ and $\tilde{z}_t$, $\tilde{z}_{t+1}$ are blocks of length k, $t=0,2,4,\ldots,2T-2$. The product $\tilde{z}_t\tilde{z}_{t+1}$, is computed when the two k-bit blocks of the test response, $\tilde{z}_t$ and $\tilde{z}_{t+1}$, are available. (A 2k-bit register may be required to store the two operands $\tilde{z}_t$ and $\tilde{z}_{t+1}$ for the multiplier, however, the already existing output-register of a circuit-under-test may be sufficient for storing $\tilde{z}_t$ and $\tilde{z}_{t+1}$).

Next, we will consider a sequential realization of a multiplier.

The sequential finite field multiplication can be computed using an LFSR with the feedback taps corresponding to the modulo polynomial p(x). The multiplication of two polynomials $\tilde{z}_t = a_{k-1}x^{k-1} \oplus a_{k-2}x^{k-2} \oplus \ldots \oplus a_0$, and $\tilde{z}_{t+1} = b_{k-1}x^{k-1} \oplus b_{k-2}x^{k-2} \oplus \ldots \oplus b_0$, modulo primitive polynomial p(x) (see Fig. 5) is obtained by loading the coefficients of $\tilde{z}_t$, $\{a_i,\ i=0,..,k-1\}$, into the feedforward-taps register where the feedback taps have been connected according to the coefficients of p(x). The coefficients of the second polynomial $\tilde{z}_{t+1}$ are shifted in, starting from b_0. After k shifts, the contents of the LFSR (starting from the left most D flip-flop) are the coefficients of the product $\tilde{z}_t\tilde{z}_{t+1} = c_0 \oplus c_1x \oplus \ldots \oplus c_{k-1}x^{k-1}$ modulo a primitive polynomial p(x) of degree k. (Note, that the order of the coefficients of the two operands, taken from the two k-bit blocks of data, is immaterial with respect to the data compression process).

Example 3. Let $k = 32$, $q = 2^{32}$, $p(x) = x^{32} \oplus x^{20} \oplus x^2 \oplus x \oplus 1$, and $\tilde{z}_t$, $\tilde{z}_{t+1}$ are two operands (two 16-bit blocks). The sequential circuit computing

$\tilde{z}_t\tilde{z}_{t+1}$ modulo p(x) is presented in Fig. 5 (a control circuit for loading data and shifting is not shown).

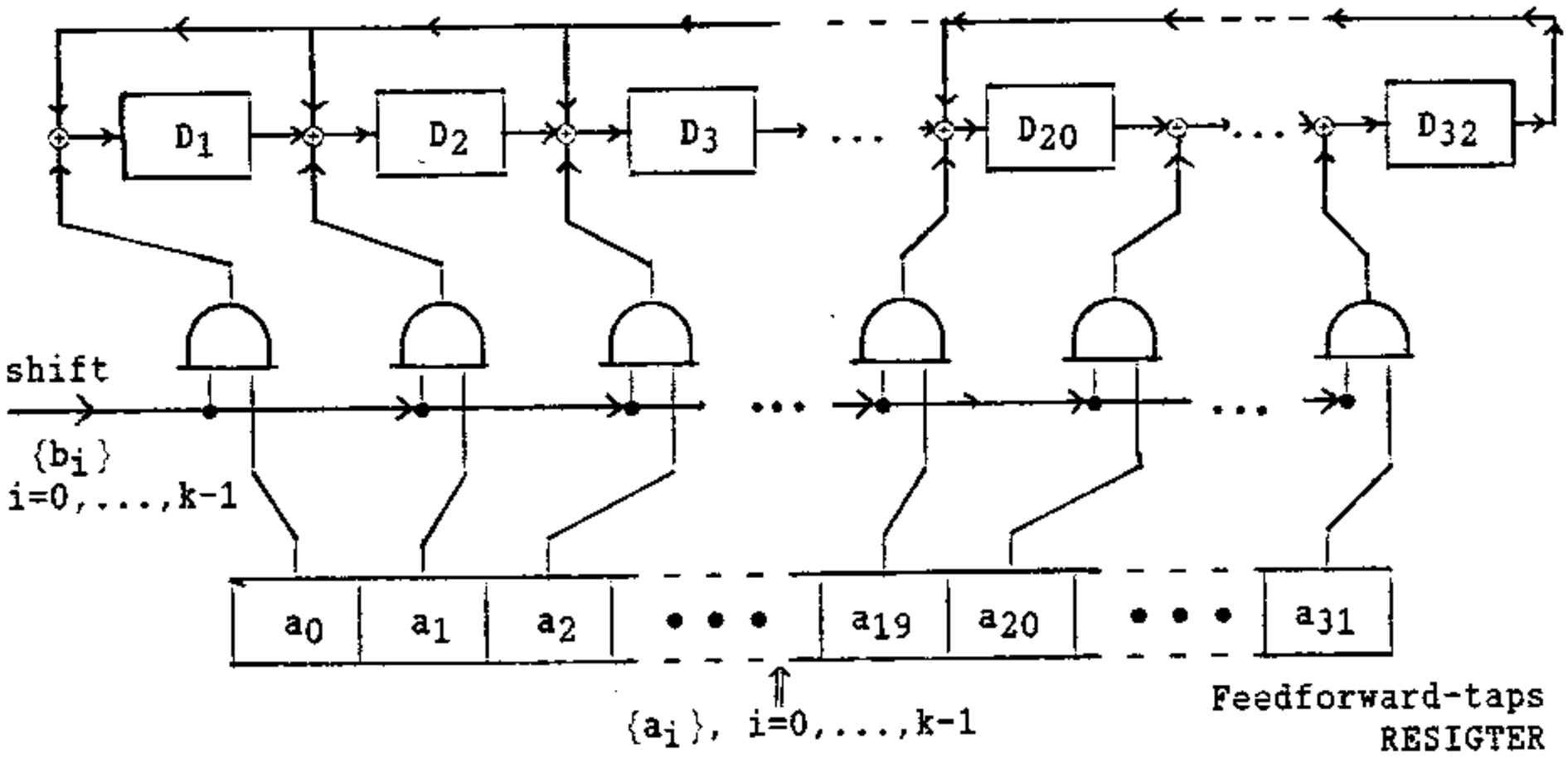

Fig. 5. Sequential Finite-Field Multiplier.

A sequential quadratic compressor can be implemented using three k-bit registers (linear feedback register with internal XOR gates, feedforward-taps register, and T flip-flop register), k two-input AND gates and a control circuit. One can see that, for VLSI testing the hardware overhead for linear and quadratic compression schemes is of the same order.

3.2 Combinational Quadratic Compressor

Combinational quadratic compressor is a combinational circuit performs a multiplication of two polynomials degree less than k, $\tilde{z}_t = a_{k-1}x^{k-1} \oplus a_{k-2}x^{k-2} \oplus \ldots \oplus a_0$ and $\tilde{z}_{t+1} = b_{k-1}x^{k-1} \oplus b_{k-2}x^{k-2} \oplus \ldots \oplus b_0$ (recall that, $\tilde{z}_t$ and $\tilde{z}_{t+1}$ are elements in $GF(2^k)$ where $(a_{k-1}, a_{k-2}, \ldots, a_0)$ and $(b_{k-1}, b_{k-2}, \ldots, b_0)$ are two k-bit blocks which are multiplier's operands). The product, $\tilde{z}_t\tilde{z}_{t+1} = c_{2k-2}x^{2k-2} \oplus c_{2k-3}x^{2k-3} \oplus \ldots \oplus c_0$, is obtained by a two-level (AND,XOR) circuit (Fig. 6), which requires k^2 two-input AND gates and $(k-1)^2$ two-input XOR gates.

The final step is reduction of $\tilde{z}_t\tilde{z}_{t+1} \equiv f_{k-1}x^{k-1} \oplus f_{k-2}x^{k-2} \oplus \ldots \oplus f_0$ modulo p(x), where p(x) is the irreducible polynomial of degree k.The coeffients $\{f_{k-1}, f_{k-2}, \ldots, f_0\}$ is obtained by the second XOR-network with inputs $\{c_{2k-2}, \ldots, c_0\}$ from the first XOR-network (see Fig. 6). Numbers of two-input XOR gates required for the reduction circuit are listed in Table 1 for different degrees of irreducible polynomials.

The hardware complexity (number of equivalent two-input gates) of the k-bit combinational finite feild multiplier is the sum of k^2 two-input AND gates, $(k-1)^2$ two-inputs XOR gates, and the complexity of the reduction circuit (Table 1).

k	p(x)	L_{XOR}
8	$x^8 \oplus x^4 \oplus x^3 \oplus x^2 \oplus 1$	28
12	$x^{12} \oplus x^6 \oplus x^4 \oplus x \oplus 1$	52
16	$x^{16} \oplus x^{12} \oplus x^3 \oplus x \oplus 1$	116
24	$x^{24} \oplus x^2 \oplus x \oplus 1$	111
32	$x^{32} \oplus x^{20} \oplus x^2 \oplus x \oplus 1$	205

k: Degrees of irreducible polynomials, p(x): Irreducible polynomials, and L_{XOR}: Number of two-input XOR gates.

Table 1. Hardware Complexities of Reduction Circuits for Combinational Quadratic Compressor

Example 4. Let $k = 3$, $q = 2^3$, $p(x) = x^3 \oplus x \oplus 1$. Then

$$\tilde{z}_t\tilde{z}_{t+1} = (a_2x^2 \oplus a_1x \oplus a_0)(b_2x^2 \oplus b_1x \oplus b_0)$$

$$= (a_2b_2)x^4 \oplus (a_1b_2 \oplus a_2b_1)x^3 \oplus (a_0b_2 \oplus a_1b_1 \oplus a_2b_0)x^2 \oplus (a_0b_1 \oplus a_1b_0)x \oplus a_0b_0$$

$$= c_4x^4 \oplus c_3x^3 \oplus c_2x^2 \oplus c_1 \oplus c_0.$$

Substituting, $x^3 = x \oplus 1$ and $x^4 = x^2 \oplus x$, we have

$$\tilde{Z}_t\tilde{Z}_{t+1} \equiv (c_4 \oplus c_2)x^2 \oplus (c_4 \oplus c_3 \oplus c_1)x \oplus (c_3 \oplus c_0) \text{ modulo } p(x).$$

Thus, $f_2 = a_2b_2 \oplus a_0b_2 \oplus a_1b_1 \oplus a_2b_0$, $f_1 = a_2b_2 \oplus a_1b_2 \oplus a_2b_1 \oplus a_0b_1 \oplus a_1b_0$ and $f_0 = a_1b_2 \oplus a_2b_1 \oplus a_0b_0$. Note also that f_2, f_1, and f_0 are quadratic repetitive Boolean functions of $\{a_2, a_1, a_0, b_2, b_1, b_0\}$.

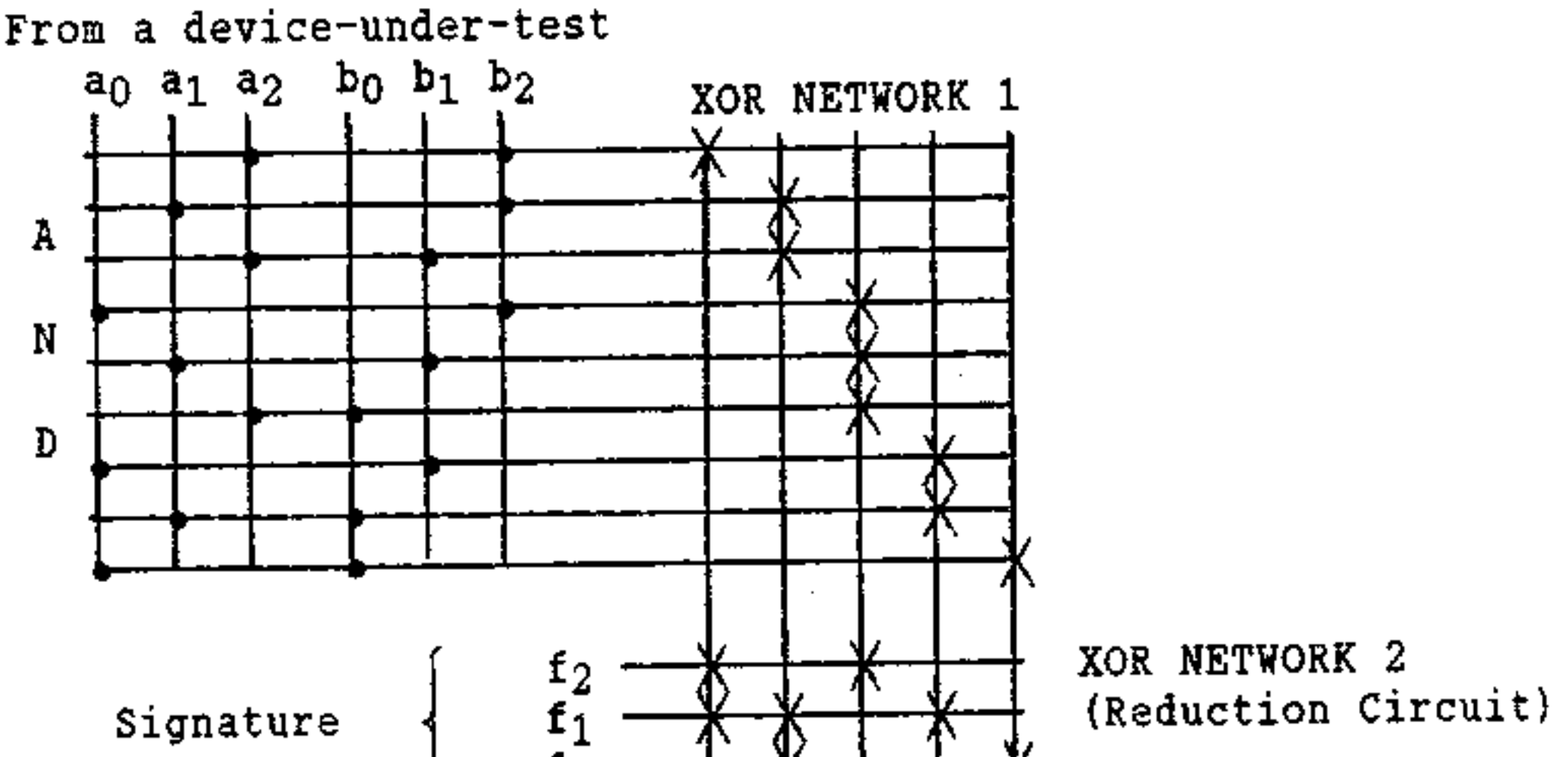

Fig 6. Combinational Quadratic Compressor

Example 5. Combinational quadratic compressors can be used for BIST design for a ROM. For example, a design of BIST 512x64K ROM based on a quadratic compressor to compute 32-bit signatures for every cell. These precomputed signatures are stored in a the 32x64K shadow-memory. Assuming that errors occur either in cells of the 512x64K ROM or in 32x64K shadow-memory, the probability that errors are masked is 2^{-32}. (Note that, this technique also provides for location of faulty cells, since signatures are stored in the shadow-memory for every cell of the original 64K ROM).

4 Conclusions

An alternative technique for data compression of test responses which is based on a quadratic function in a finite field of 2^k elements was presented. The proposed quadratic compressors are optimal from the points of veiw of the lower bound on the maxima conditional error-masking probability Q(e) given an error e (e≠0).

While a quadratic compressor requires slightly more hardware than an LFSR compressor, it can provide for a minimum of $\max_{e\neq 0} Q(e)$, in constrast with the case of a signature analysis by LSFRs, when Q(e) is either 0 or 1 for a given e≠0. Hence, quadratic compressors are "robust" with respect to the distribution of errors $Pr[e|e\neq 0]$, that is, the total error-masking probability $Q_{total} = \sum_{e\neq 0} Q(e) Pr[e|e\neq 0] = 2^{-r}$, (r-bit signature), is indepedent on $Pr[e|e\neq 0]$.

References

[1] E.J. McCluskey and S. Bozorgui-Nesbat, "Design for autonomous test," IEEE Trans. on Comput. vol. C-30, pp. 866-875, 1981.

[2] H. Fujiwara, Logic Testing and Design for Testability, MIT Press, 1985

[3] J.E. Smith, "Measure of effectiveness of fault signature analysis," IEEE Trans. on Compt., June 1980.

[4] J.P. Robinson and N.R. Saxena, "A unified view of test compression method," IEEE Trans. on Compt., April 1984.

[5] P.K. Bhavsar and B. Krishnamurthy, "Can we eliminate fault escape in self testing by polynomial division (signature analysis)," Proc., ITC-1984, pp. 134-139.

[6] K.K. Saluja and M.G. Karpovsky, "Testing computer hardware through data compression in space and time," Proc. ITC-1983, pp. 83-88.

[7] S.R. Reddy, K.K. Suluja and M.G. Karpovsky, "A data compression technique for built-in self test," Proc. FTCS, 1985.

[8] ——, "A data compression technique for test responses," to appear in IEEE Trans. on Compt., 1988.

[9] M.G. Karpovsky, Finite Orthogonal Series in The Design of Digital Devices, Halsted Press, John Wiley & Sons, Inc., 1976.

[10] M.G. Karpovsky and P. Nagvajara, "Optimal time and space compression of test responses for VLSI devices," Proc. IEEE, ITC-1988, pp. 523-529.

[11] ——, "Functions with flat autocorrelations and their generalizations," Proc. IEEE, IWST-1988, FGR.