OPTIMAL COMPRESSOR OF TEST RESPONSES*

M. Karpovsky and P. Nagvajara

Department of Electrical, Computer and System Engineering

Boston University

Mailing Address:

M. Karpovsky and P. Nagvajara

Department of Electrical, Computer, and System Engineering

College of Engineering,

Boston University,

110 Cummington St.,

Boston, MA 02215.

(617) 353-9592.

---

*This work was supported by the National Science Foundation under Grant DCR-8317763.

OPTIMUM COMPRESSION OF TEST RESPONSES

M. Karpovsky and P. Nagvajara

Department of Electrical, Computer and System Engineering

Boston University.

Abstract.

An alternative technique in test-response compression is presented. The proposed quadratic compression scheme is based on a quadratic function in an extension of the finite field of two elements, {0,1}. The problem of test-response compression is analogous to the one for error-detecting codes. A test response is tampered by an error sequence that is a manifestation of a fault. An error-detection capability of a compression scheme is given by means of a probabilistic approach. An error is masked (undetected) if and only if a test response is compressed into the reference signature (precomputed for a given circuit and a test sequence). With the assumption that a fault-free response (sequence) and an error sequence are statistically independent with uniformly distributed probabilities, a quadratic compression scheme is shown to be optimal with respect to the total error-masking probability, the maximum value of the conditional error-masking probability given an error sequence, and the maximum value of the conditional error-masking probability given a fault-free sequence. An implementation of the quadratic compression scheme requires slightly more hardware than a parallel signature analyzer. (Two designs of a quadratic compressor are considered.) However, the conditional error-masking probability given an error sequence, $Q(\tau)$, of a quadratic scheme is shown

to be constant (for the case of signature analysis, $Q(\tau)$ is either 0 or 1, for different τ, independent of the statistics of fault free-sequences, which implies an equal protection against all error sequences. In other words, the total error-masking probability, $Q_{total} = \sum_{\tau} Q(\tau)Pr[\tau \mid \tau \neq 0]$, of quadratic schemes is independent of the statistics of error sequences.

1. Introduction.

Signature analysis techniques, based on linear-feedback-shift registers (LFSR), are widely used for compression of test responses [2-7]. Since signature analysis is, in fact, equivalent to a decoding procedure for a linear error-detecting code (the LFSR is a decoder for this code), it only guarantees a detection of an unexpected observed test response, such that a number of distorted bits in an output of a device-under-test is less than the minimum distance of the code. However, if the number of erroneous bits is greater than the minimum distance, detection probabilities for different patterns of distorted bits, called error patterns or error sequences, are 0 or 1. (An error pattern is masked if and only if it belongs to the code.) For communication channels a distortion of a single bit in a message is more likely to occur than a distortion of two or more bits , hence, the notion of a minimum distance in determining the error-detection capability (in a probabilistic sense) of a linear coder is justified. However, in the case of testing, multiple errors (distorted bits) at outputs of devices-under-test may be as probable as single ones.

An alternative compression technique, based on quadratic functions, will be shown, by probabilistic approach, to be optimal and provide for an equal error-detection capability for all patterns of erroneous symbols in the observed test-response.

1.1 Data Compression of Test Responses.

The major problem in testing of Very-Large-Scale-Integration circuits is related to an excessive size of the reference data to be stored. For reducing the storage size, required for the reference data, test responses are compressed into a k-bit word called "signature". A block-diagram for data compression of test responses is given by Figure 1. The test response in Figure 1 is considered to be a stream of binary digits, which may correspond to "scan-out" data for a scan-testable design.

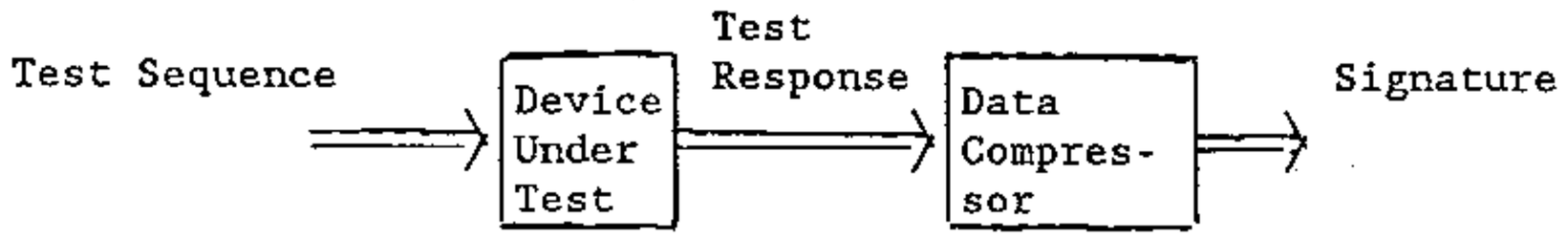
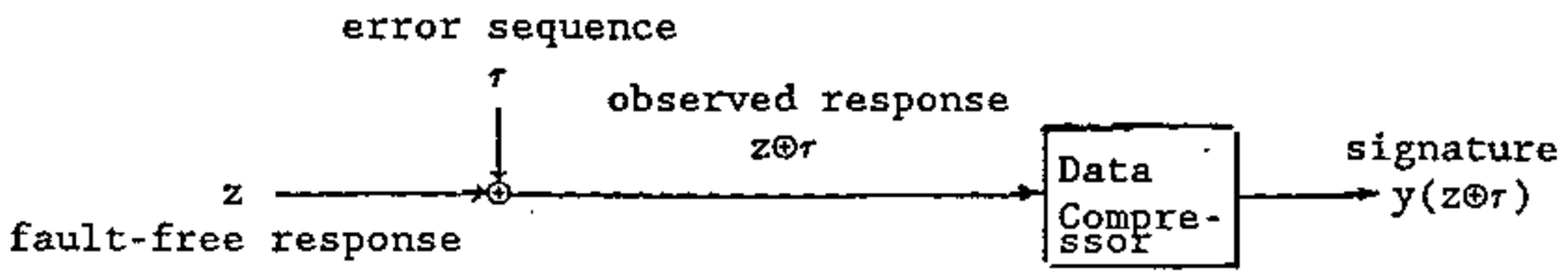


Figure 1: Data Compression of Test Responses

1.2 Signal-Analysis Description of Faults.

Let us suppose that, a fault-free response (reference data), z, is a string of N binary digits, that is $z \in V^N$, where V^N is an N-dimensional vector space over (0,1); the error sequence τ (manifestation of a fault) is added modulo 2 to form the observed response, $z \oplus \tau$ (see Figure 2).



$z, \tau \in V^N$, $y(z \oplus \tau) \in V^k$ over (0,1), (V^N denotes N-dimensinal vector space).

Figure 2: Signal-Analysis Description of Faults.

The data compressor implements mapping $y: V^N \rightarrow V^k$ over (0,1), that is $z \oplus \tau \in V^N$ is mapped into a signature, $y(z \oplus \tau) \in V^k$, and compared to the reference signature y(z). The advantage is that only a k-bit reference data is required, instead of an N-bit of the fault-free response (eg. $N=2^{12}$, k=16).

The major limitation of data compression techniques is related to a difficulty of predicting probabilities of errors $\tau \neq 0$ such that an observed signature is equal to the reference one, $y(z \oplus \tau) = y(z)$.

1.3 Probabilistic Model.

Since a compressor is to be used for an ensemble of devices and test-generation techniques, a fault-free response, z, of a device-under-test is considered to be a random variable. Note that, even for the case when a device-under-test is given (one circuit in an ensemble), if it is tested by a random test, z is a random variable. Another random variable is an error sequence, τ, which is the manifestation of fault(s) occuring in a device-under-test. Moreover, z, τ are assumed to be statistically independent with the uniformly distributed probabilities:

$$\Pr[z] = 2^{-N}, \text{ and } \Pr[\tau \mid \tau \neq 0] = (2^N - 1)^{-1}, \quad z, \tau \in V^N \text{ over } (0,1),$$

where $\Pr[\tau \mid \tau \neq 0]$ is a conditional probability that error pattern τ will appear at the output of a device-under-test, condition that, there is a fault in the device.

1.4 Performance Measures.

A quantitative measure describing an error- detecting capability of a compressor can be given in terms of the following probabilities:

- The total probability of the event (z, τ), such that $y(z) = y(z \oplus \tau)$,

is defined as "the total error-masking probability", denoted by Q_{total}.

⊙ The conditional probability, given τ ($\tau \neq 0$), that $y(z) = y(z \oplus \tau)$, called "the conditional error-masking probability given τ", denoted by $Q(\tau)$.

⊙ The conditional probability, given z, that $y(z) = y(z \oplus \tau)$, $\tau \neq 0$, called "the conditional error-masking probability given z", denoted by $Q(z)$.

1.5 Optimal Data-Compressor for Test Response.

A data compressor is (asymptotically) optimal if and only if the probabilities Q_{total}, $Q(\tau)$, and $Q(z)$, (asymptotically) satify the following bounds, respectively:

1.5.1 Lower Bound on Total Error-Masking Probability.

$$Q_{total} = \sum_{(z,\tau)\,|\,y(z)=y(z\oplus\tau)} \Pr\left[(z,\tau)\,|\;\tau\neq 0\right] \geq \frac{2^{N-k}-1}{2^{N}-1} \qquad (1).$$

and $Q_{total} \simeq 2^{-k}$ ($N \to \infty$, k fixed).

The proof of (1) can be found in [1,4].

The following two lower bounds are easy to prove.

1.5.2 Lower Bound on The Maximum Value of $Q(\tau)$.

$$\min_{\{y\}} \max_{\tau} Q(\tau) \geq \frac{2^{N-k}-1}{2^{N}-1}\;; \qquad \min_{\{y\}} \max_{\tau} Q(\tau) \simeq 2^{-k} \qquad (2).$$

where $\{y\}$ denotes a set of all possible compressors, that is,

mappings $y: z \to i$, $z \in V^N$, $i \in V^k$.

1.5.3 Lower Bound on The Maximum Value of Q(z).

$$\min_{\{y\}} \max_{z} Q(z) \geq \frac{2^{N-k} - 1}{2^N - 1}\ ; \qquad \min_{\{y\}} \max_{z} Q(z) = 2^{-k} \qquad (3).$$

The equalities in the above bounds hold if and only if mapping y partition V^N into equal-cardinality equivalent classes (a,b belong to the same class if and only if y(a) = y(b); in this case y is said to be a uniform mapping). A linear mapping is uniform; however, the converse is not true.

In the next section, optimum compressors, which asymptotically satify the above bounds (1)-(3) are presented.

2. Quadratic Compressor.

The concept of a quadratic compressor is based on the quadratic nonrepetitive function of 2m variables over the field GF(q) of q elements [1]:

$$y(z) = z_0z_1 \oplus z_2z_3 \oplus \ldots \oplus z_{2m-2}z_{2m-1},\ z \in V^{2m} \text{ over } GF(q),\ z_i \in GF(q) \qquad (4).$$

Let $q=2^k$, and for z being a string of N bits, z_0 in (4) is the first k-bit block in z, and z_i is the ith k-bit block, i =0,1,...,2m-1 (provided that, N/k = 2m). The signature, $y(z \oplus r)$, can be computed by multiplying two k-bit blocks z_tz_{t+1} (t even) and updating (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 (sum), $\oplus$, is a polynomial (vector) addition modulo 2 (componentwise mod 2 sum). In Section 3 hardware realizations and complexity analysis for quadratic compressors are presented.

The following theorem states, that $Q(\tau)$, for a quadratic compressor described above, asymptotically satisfies the lower bound (2) on the maximum

value of $Q(\tau)$. Moreover, it is shown that $Q(\tau) = q^{-1} = 2^{-k}$; hence, the total error-masking probability Q_{total} for a quadratic compressor asymptotically satisfies (1); $Q_{total} \geq (2^{N-k}-1)/(2^{N}-1) = 2^{-k}$.

Theorem 1.

Let $y(z)$ be a quadratic nonrepetitive function $y(z) = z_0z_1 \oplus z_2z_3 \oplus \ldots \oplus z_{2m-2}z_{2m-1}$, where $z \in V^{2m}$ over GF(q), $z_i \in GF(q)$, and $Pr[z]$, $Pr[\tau \mid \tau \neq 0]$ are uniformly distributed. Then, we have for conditional probability $Q(\tau) = Prob[y(z) = y(z \oplus \tau) \mid \tau]$ for a given $\tau \neq 0$, $Q(\tau) = q^{-1} = 2^{-k}$.

Proof.

Denote $z_{\odot} = (z_0z_2 \ldots z_{2m-2})$, $z_{\circledcirc} = (z_1z_3 \ldots z_{2m-1})$, that is $z_{\odot}, z_{\circledcirc} \in V^{m}$ over GF(q); consider a fixed τ, $\tau \neq 0$, with $\tau_{\odot}, \tau_{\circledcirc}$ defined similar to $z_{\odot}, z_{\circledcirc}$. Then, $y(z) = y(z \oplus \tau)$ can be writen as $\langle z_{\odot}, z_{\circledcirc} \rangle = \langle (z_{\odot} \oplus \tau_{\odot}), (z_{\odot} \oplus \tau_{\circledcirc}) \rangle$, where $\langle\ \rangle$ denotes inner-product defined in V^{m} over GF(q). It follows that

$$y(z)=y(z \oplus \tau) \Leftrightarrow \langle \tau_{\odot}, z_{\odot} \rangle \oplus \langle \tau_{\odot}, z_{\circledcirc} \rangle \oplus \langle \tau_{\circledcirc}, \tau_{\circledcirc} \rangle = 0. \qquad (5).$$

Notice that, $|\{z \mid y(z)=y(z \oplus \tau)\}|$ equals to the number of solutions $(z_{\odot}, z_{\circledcirc})$ of (5). Thus, if $(\tau_{\odot}, \tau_{\circledcirc}) \neq 0$, then, $|\{z \mid y(z)=y(z \oplus \tau)\}| = q^{m}\, q^{m-1}$. Therefore, $Q(\tau) = Pr[z] \cdot |\{z \mid y(z)=y(z \oplus \tau)\}| = q^{-1} = 2^{-k}$. □

In Theorem 2 the conditional error-masking probability given z, $Q(z)$, is derived for quadratic compressors and shown to be asymptotically satifying the bound given in 1.5.3.

Theorem 2.

Consider a quadratic nonrepetitive function $y(z) = \langle z_{\oplus}, z_{\oplus} \rangle$, $z \in V^{2m}$, $z_{\oplus}, z_{\oplus} \in V^{m}$ over GF(q) $(q=2^k)$, and $Pr[\tau \mid \tau \neq 0] = q^{2m}-1$ (uniform distribution). Then, $Q(z) = q^{-1} = 2^{-k}$.

Proof.

For a given z, suppose $y(z) = i$ and $|\{\tau \mid y(z)=y(z\oplus\tau),\ \tau\neq 0\}| = A_i - 1$. Then, $Q(z) = (A_i-1)/(q^{2m}-1)$, where A_i is a number solutions for the following equation

$$\langle z_{\oplus}, z_{\oplus} \rangle = z_0z_1 \oplus z_2z_3 \oplus \ldots \oplus z_{2m-2}z_{2m-1} = i, \quad i \in GF(q) \qquad (6)$$

First, let i=0, then $A_0 = q^m + q^{m-1}(q^m-1)$, since for any choice of $z_{\oplus}\neq 0$, there are q^{m-1} values of $z_{\oplus}$ satifying (6); and for $z_{\oplus} = 0$ all q^m possible values of $z_{\oplus}$ are solutions of (6). Similarly, $A_i = q^{m-1}(q^m-1)$ for $i\neq 0$. Therefore, as $2m\to\infty$ and k is finite, $A_i \simeq q^{2m-1}$, and

$$Q(z) = (A_i-1)/(q^{2m}-1) \simeq q^{-1} = 2^{-k}. \qquad \square$$

3. Hardware Implementations and Complexities for Quadratic Compressors

Consider the following implementation of a quadratic compressor (Figure 3):

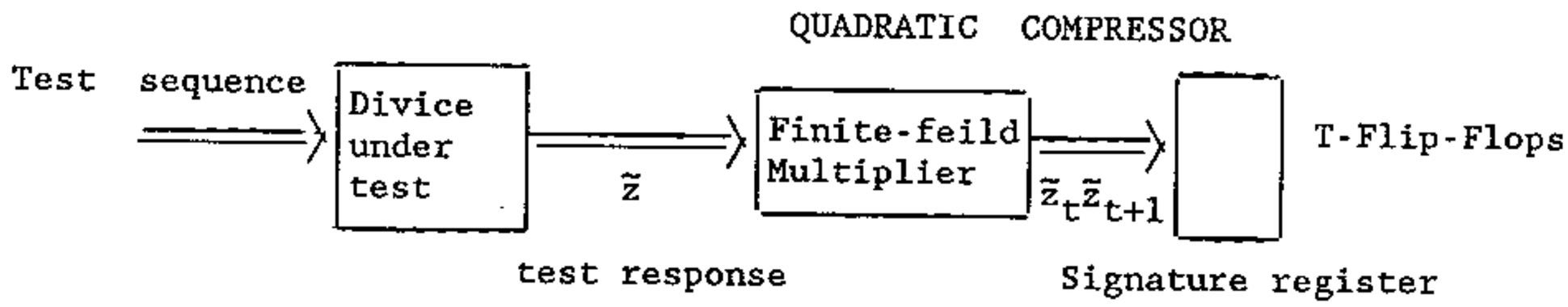


Figure 3: Hardware Implementation of a Quadratic Compressor.

In Figure 3 the observed response, $\tilde{z} = z\oplus\tau$, is processed in a serial fashion, based on the quadratic function over $GF(2^k)$, $y(\tilde{z}) = \tilde{z}_0\tilde{z}_1 \oplus \tilde{z}_2\tilde{z}_3 \oplus$

$\ldots \oplus \tilde{z}_{2m-2}\tilde{z}_{2m-1}$, where $\tilde{z}$ is a binary sequence length $N = 2mk$, and $\tilde{z}_t$, $\tilde{z}_{t+1}$, are blocks of length k, t=0,2,4,...,2m-2. The product, $\tilde{z}_t\tilde{z}_{t+1}$, is computed when the two k-bit blocks of a 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 exsisting output register of a circuit-under-test may be sufficient for storing $\tilde{z}_t$ and $\tilde{z}_{t+1}$.

We will consider now combinational and sequential implementations of multipliers.

3.1 Combinational Multiplier.

The finite field multiplier may be designed as a combinational circuit to speed up a testing procedure. The presented combinational circuit performs a multiplication of two polynomials degree less than k, $\tilde{z}_t = a_{k-1}x^{k-1} \oplus a_{k-2}x^{k-2} \oplus \ldots \oplus a_0$, $\tilde{z}_{t+1} = b_{k-1}x^{k-1} \oplus b_{k-2}x^{k-2} \oplus \ldots \oplus b_0$, (recall, that $\tilde{z}_t$, $\tilde{z}_{t+1}$ are elements in $GF(2^k)$, and $(a_{k-1}, a_{k-2}, \ldots, a_0)$ and $(b_{k-1}, b_{k-2}, \ldots, b_0)$ are two k-bit blocks (multiplier operands) mentioned earlier). The resulted 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 (Figure 4), which requires k^2 two-input AND gates and $(k-1)^2$ two-input XOR gates. The final step is reduction of $\tilde{z}_t\tilde{z}_{t+1} = f_{k-1}x^{k-1} \oplus f_{k-2}x^{k-2} \oplus \ldots \oplus f_0$ modulo $\alpha(x)$, where $\alpha(x)$ is the irreducible polynomial $\alpha(x)$ of degree k; $(f_{k-1}, f_{k-2}, \ldots, f_0)$ is obtained by an XOR-network with inputs $(c_{2k-2}, \ldots, c_0)$ from the first XOR plane (Figure 4). If $\alpha(x)$ is a trinomial, (which it is often the case), then the second XOR plane requires 2k-1 two-input XOR gates. In summary, the hardware complexity (number of two-input gates) of the k-bit combinational finite feild multiplier is approximately $2k^2$.

Example 1. Let $k = 3$, $q = 2^3$, $\alpha(x) = x^3 \oplus x \oplus 1$. Since $x^3 = x \oplus 1$ and $x^4 = x^2 \oplus x$, we have,

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

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

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

$$= (c_4 \oplus c_2)x^2 \oplus (c_4 \oplus c_3 \oplus c_1)x \oplus (c_3 \oplus c_0) \text{ modulo } \alpha(x)$$

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 $\{a_2, a_1, a_0, b_2, b_1, b_0\}$ [1].

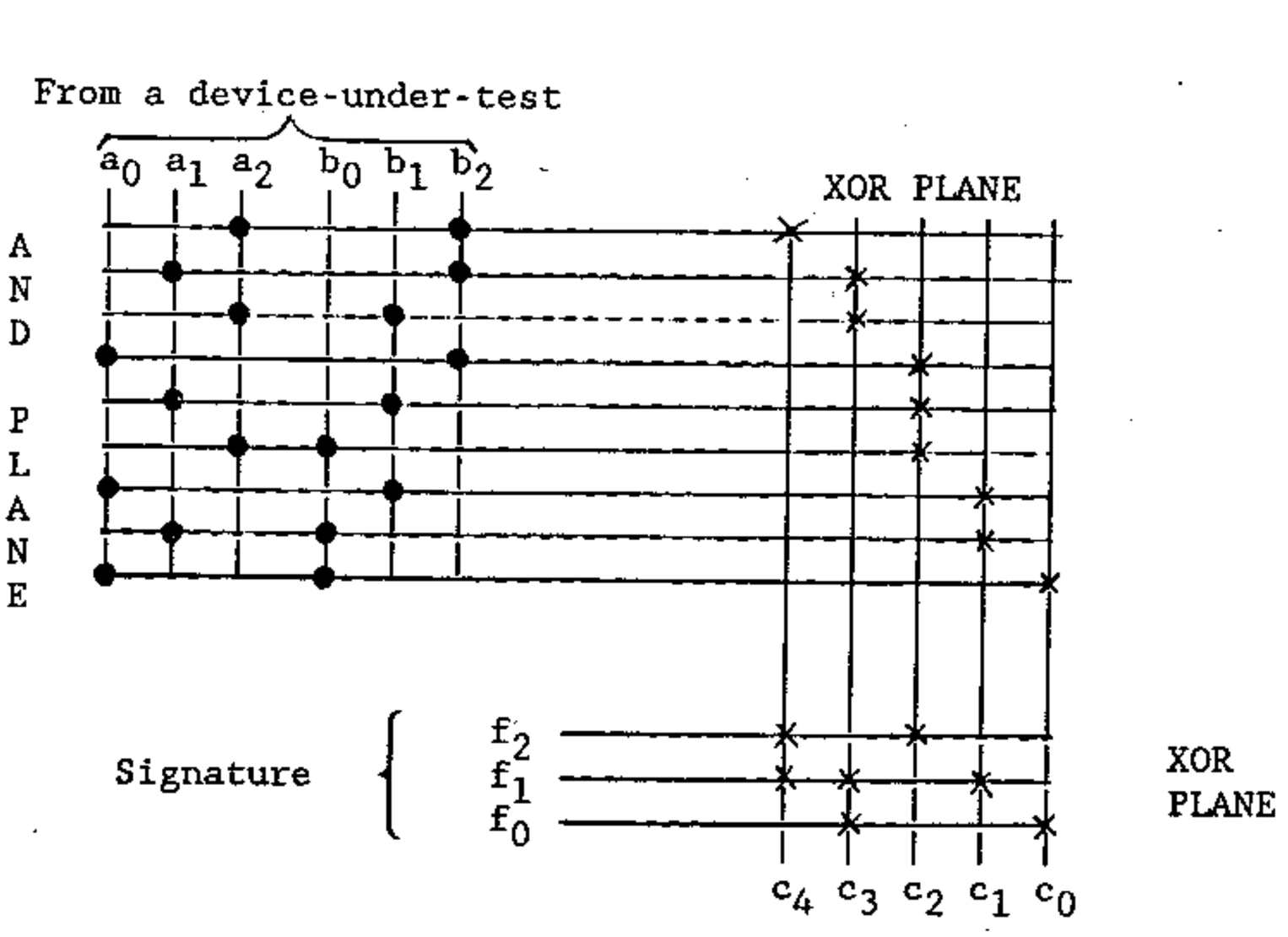


Figure 4: Combinational Finite Field Multiplier.

3.2 Sequential Multiplier.

Since the hardware complexity of a combinational multiplier is twice the square of k (for k-bit signature), an alternative implementation is considered. Sequential finite field multiplication can be reduce to the shift, Boolean multiplication, and modulo2 addition of product terms $\tilde{z}_t\tilde{z}_{t+1}$.

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

With $\tilde{z}_t\tilde{z}_{t+1}$ given in Example 1, the sequential circuit computing $\tilde{z}_t\tilde{z}_{t+1}$ modulo $\alpha(x)$ is presented in Figure 5.

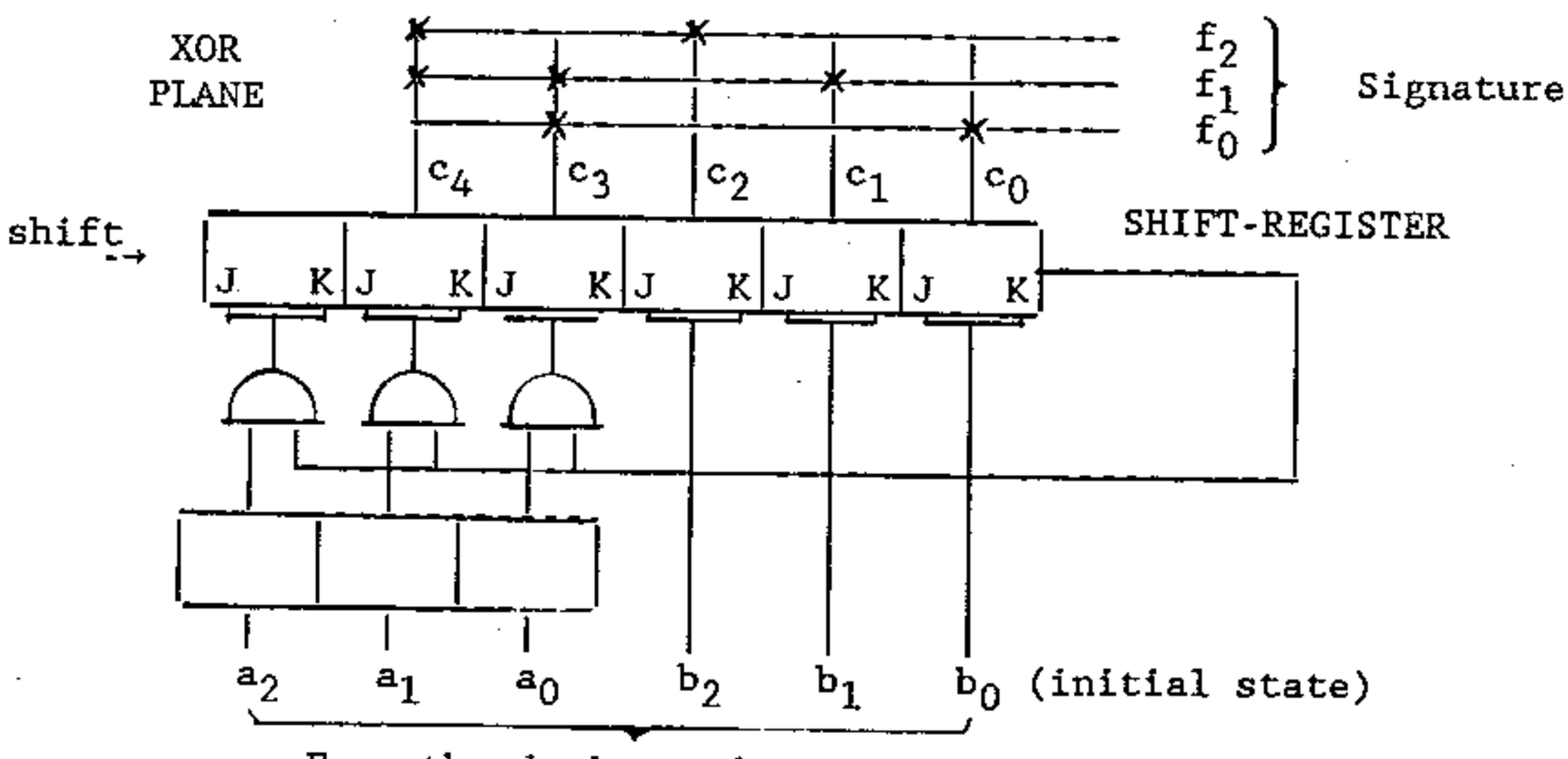


Figure 5: Sequential Finite Field Multiplier.

In general, the presented sequential finite field multiplier requires 3k-bit registers, k two-input AND gates and $(\gamma-1)(k-1)$ two-input XOR gates, where $\gamma+1$ is the number of coefficients in $\alpha(x)$, ($\gamma = 2$ for trinomials).

4. Quadratic Space Compression.

The general block diagram for space compression is shown in Figure 6 [5-7].

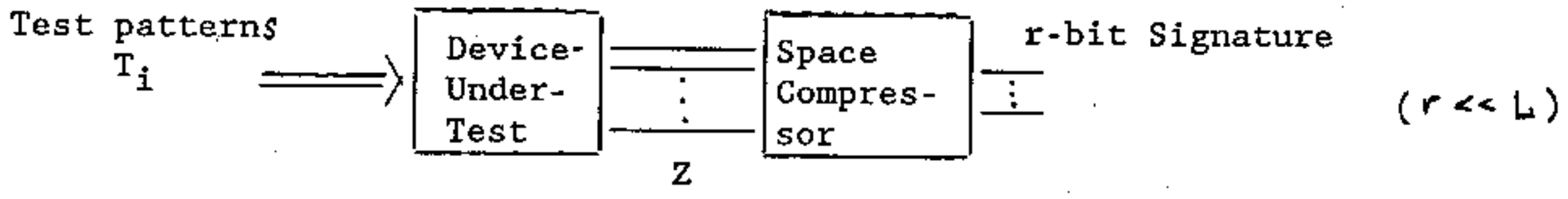


Figure 6: Space Compression Schematic Diagram

Since a quadratic space compressor is a system of quadratic Boolean functions, $y(Z) = (f_0(Z), f_1(Z), \ldots, f_{r-1}(Z))$, the number of outputs for a device-under-test is assumed to be even. The response pattern, Z, is a vector in 2L-dimensional space over (0,1), which to be mapped into an r-bit signature by a quadratic function over a finite field. For example, $r = L = k$, $y(Z) = Z_0Z_1$, where Z_0, Z_1 are k-bit vectors, that is, $Z \in V^2$ over $GF(2^k)$, $Z_0, Z_1 \in GF(2^k)$. Assuming that $Pr[Z]$ and $Pr[\tau \mid \tau \neq 0]$ are uniformly distributed, by Theorem 1, the space compressor, $y(Z) = Z_0Z_1$, is optimal.

The generalization of this example is given by the following theorem.

Theorem 3.

Let $g(Z)$ be a system of r Boolean functions, $g(Z) = \{g_0(Z), g_1(Z), \ldots, g_{r-1}(Z)\}$, arbitrarily chosen from a set of k quadratic Boolean functions, $F = \{f_0(Z), f_1(Z), \ldots, f_{k-1}(Z)\}$. The set F is constructed by

$y(Z) = Z_0Z_1 \oplus Z_2Z_3 \oplus \ldots \oplus Z_{2m-2}Z_{2m-1} = f_0(Z)x^{k-1} \oplus f_1(Z)x^{k-2} \oplus \ldots \oplus f_{k-1}$ modulo $\alpha(x)$, where $Z \in V^{2m}$ over $GF(q)$, $Z_i \in GF(q)$, and $\alpha(x)$ is an irreducible polynomial used in constructing $GF(q)$ $(q = 2^k)$.

The compressor, $g(Z)$, is optimal, that is

Q_{total}, $Q(\tau)$, and $Q(Z) \approx 2^{-r}$. □

To illustrate the usefullness of Theorem 3, consider the following example. Let the number of output-lines $2L = 128$, the size of signature is r, and $k = L = 64$. Then, one can use the following function for data compression $y(Z) = Z_0Z_1 = f_{63}(Z)X^{63} \oplus f_{62}(Z)x^{62} \oplus \ldots \oplus f_0(Z)$ modulo $\alpha(x)$, where $\alpha(x)$ is an irreducible polynomial of degree 64 over {0,1}. A subset of $r \leq 64$, Boolean functions out of $\{f_0(Z), f_1(Z), \ldots, f_{63}(Z)\}$ forms an optimum compressor $g(Z)$, with the probability of masking any error being 2^{-r}.

5. Conclusions

A new technique for data compression of test responses which is based on quadratic functions in a finite field of 2^k elements was presented. The proposed quadratic compressors are optimal from the points of veiw of a total error-masking probability Q_{total}, maximum value of a conditional error-masking probability given an error sequence τ, $Q(\tau)$, and maximum value of a conditional error-masking propability given z, Q(z). (Widely used linear compression schemes, based on LFSRs, are optimal only from the points veiw of Q_{total} and Q(z).)

While a quadratic compressor requires slightly more hardware for data compression than a linear one, it can provide for a minimum of the maximum value of $Q(\tau)$, in contrast with the case of a signature analysis by LSFRs, when $Q(\tau)$ is either 0 or 1 for different τ. (With respect to the lower bound on the maximum value of $Q(\tau)$, signature analysis is the worst compressor.)

Another aspect related to the constant-$Q(\tau)$ property of the quadratic compression scheme is its "robustness" with respect to assumptions on a

statistics of errors, $Pr[\tau \mid \tau \neq 0]$, since the total error-masking probability, ($Q_{total} = \sum_{\tau} Q(\tau) Pr[\tau \mid \tau \neq 0]$ over all τ, $\tau \neq 0$), attained by the quadratic scheme, does not change its value due to variations in $Pr[\tau \mid \tau \neq 0]$. (However, for the case of a (linear) signature analysis, $Q(\tau)$ is either 0 or 1, hence, Q_{total} is sensitive to $Pr[\tau \mid \tau \neq 0]$.)

6. References.

1. Karpovsky, M. G., "Finite Orthogonal Series in The Design of Digital Devices," Halsted Press, John Wiley & Sons, Inc., 1976.
2. Smith, J. E., "Measure of Effectiveness of Fault Signature Analysis," IEEE Trans. Compt., June 1980.
3. Robinson J. P. and Saxena N. R., "A unified View of Test Compression Method," IEEE Trans. Compt., April 1984.
4. Bhavsar, D. K. and Krishnamurthy B., "Can we Eliminate Fault Escape in Self Testing by Polynomial Division (Signature Analysis)," IEEE Proc. Int'l. Test Conf., pp. 134-139, October 1984.
5. Saluja K. K., and Karpovsky, M. G. "Testing Computer Hardware Through Data Compression in Space and Time," IEEE Proc. Int'l. Test Conf., pp. 83-88, October 1983.
6. Reddy, S. R., Suluja K. K., and Karpovsky M. G., "A Data Compression Technique for Built-in Self Test," Proc. Fault-Tolerant Computing Symp., Ann Arbor, MI, 1985.
7. Reddy, S. R., Suluja K. K., and Karpovsky M. G., "A Data Compression Technique for Test Response," IEEE Trans. Compt., 1987 (to appear).