REFINED BOUNDS ON SIGNATURE ANALYSIS ALIASING FOR RANDOM TESTING

Nirmal R. Saxena, Piero Franco and Edward J. McCluskey

Center for Reliable Computing
ERL 460, Computer Systems Laboratory
Departments of Electrical Engineering and Computer Science
Stanford University, Stanford, California 94305-4055

ABSTRACT

In previous work a simple bound, $\frac{2}{L+2}$, on the aliasing probability in serial signature analysis for a random test pattern of length L was derived. This simple bound is sharpened here by almost a factor of two. For serial signature analysis, it is shown that the aliasing probability is bounded above by $\frac{1+\varepsilon}{L} \approx \frac{1}{L}$ (ε small for large L) for test lengths L less than the period, L_C, of the signature polynomial. The simple bounds derived are compared with exact as well as experimentally measured aliasing probability values. It is conjectured that L^{-1} is the best monotonic bound on the aliasing probability for serial signature analysis.

1. INTRODUCTION

This paper is a continuation of the work reported in [Saxena 91, Franco 91]. In [Saxena 91], simple bounds on the aliasing probability are derived after demonstrating that the exact calculation of the aliasing probability is impractical for realistic design parameters. These simple bounds avoid the exponential complexity of calculating the exact aliasing probability. A discussion of test data compaction issues is presented in [McCluskey 91].

The aliasing probability measure requires the assumption of an underlying error model. In the past, equally likely errors, single bit errors, and burst errors [Benowitz 75] [Frohwerk 77] were some of the error characteristics that have been assumed. In particular cases, it may be possible to justify the use of these models; however, the general applicability of these models for error characteristics in VLSI circuits, seems questionable. The bernoulli error model has been widely used by several researchers [Shedletsky 77] [Gupta 88] [McCluskey 88] [Damiani 89] [Ivanov 89] [Williams 88] [Iwasaki 90]. This model is reasonable for combinational circuits with the restriction that random test patterns are applied, and the faults are combinational. Faults that preserve the combinational nature of a circuit are called *combinational faults*. In the *bernoulli error model*, output errors are assumed to occur with probability p in the presence of a fault, and these output errors are independent events. The simulation results presented in Sec. 4 not only compare the aliasing probability bounds with the exact and experimental values, but also indirectly validate the bernoulli model. For a given circuit, the magnitude of p depends on the detectability [McCluskey 88] of the fault. The *detectability* k of a fault is the number of patterns that detect this fault. The value of p for any given detectable fault can be anywhere in the range $0<p\leq 1$ [Saxena 91].

Throughout this paper it is assumed that the signature register is a linear finite state machine (for example, linear feedback shift register or linear cellular automaton) described by the characteristic polynomial $U(X)$. In [Saxena 91], it is proved that all linear finite state machine signature analysis implementations having the same characteristic polynomial are equivalent with respect to the aliasing behavior. Also, it is assumed that the polynomial $U(X)$ does not have X as a factor. The application of the simple bounds to signature analysis based on polynomial $U(X)$ that has X as a factor is considered in [Saxena 91]. Comparison of the simple bounds, in [Saxena 91], with experimentally as well as theoretically computed aliasing probability values, suggests that there is room for further refinement. In this work, these simple bounds have been improved by almost a factor of 2. It is shown that for serial signature analysis the aliasing probability is bounded above by $\frac{1+\varepsilon}{L} \approx \frac{1}{L}$ (ε small, for large L) for test lengths L less than the period, L_C, of the signature polynomial. For example when L=80,000 , ε=1.8 x 10^{-4}. For test lengths L equal to integral multiples of L_C (called *period-multiple lengths*), there is no room for further refinement of the simple bound. This is because for period-multiple lengths, the aliasing probability can be as high as one. For test lengths L greater than L_C and not a multiple of L_C (called *non-period-multiple lengths*), there is opportunity to improve the simple bound, $\frac{2}{L_C+1}$, derived in [Saxena 91] by almost a factor of two; however, because of the limited length of this paper this improvement is not presented in this paper. Figure 1 illustrates this simple monotonic bound for three signature polynomials with three different periods. For

example, a polynomial with period 2^{20} will guarantee the aliasing probability bound to fall monotonically as L increases up to test length 2^{20} after which the aliasing probability bound does not improve with increasing test lengths. In Fig. 1 the points corresponding to the period-multiple lengths are not shown and this is denoted by the hatched lines. The practical importance of these simple bounds is that there is no significant improvement in the aliasing probability for test lengths L greater than or equal to L_C, in fact there is a danger of increasing aliasing probability (at period-multiple lengths). Exact and experimental aliasing probability values presented in Sec. 4 demonstrate this.

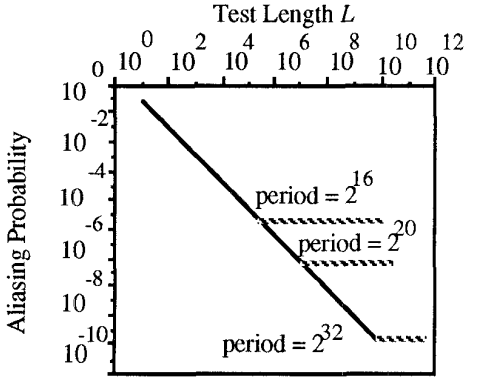


Figure 1. Aliasing Probability Bound as a Function of Test Length

2. DEFINITIONS

Definition 1: The *period* L_C of a polynomial $U(X)$ (without X as a factor) of degree r is the smallest positive integer, L_C, such that $U(X)$ divides $X^{L_C}+1$. If $U(X)$ has X as a factor then the *period* L_C of this polynomial is the period of the largest degree factor $U_1(X)$ (without X as a factor) of $U(X)$. If $U(X)$ is primitive then $L_C = 2^r-1$. If $U(X)$ is non-primitive then $L_C<2^r-1$.

Definition 2: $N(L,w,\alpha, U(X))$ is the number of weight w binary sequences of length L that have signature α with respect to $U(X)$. The *weight* w is the number of ones in the binary sequence. The *signature* α is the remainder after polynomial division of the binary sequence by modular LFSR implementation of $U(X)$. For all other implementations, the signature α is the final contents of the signature register.

3. BOUNDS AS A FUNCTION OF L, p, AND $U(X)$

The simple bounds presented in [Saxena 91] are refined by using the following approach. First, upper bounds are derived on the aliasing probability, $P_{al}(L,p,U(X))$, as a function of the detection probability p, the test length L, and the signature polynomial $U(X)$. Second, these bounds combined with an upper bound in [Ivanov 89] are used to obtain a tight simple upper bound. The *detection probability*, p, for a combinational fault in a circuit is the probability that a random test pattern produces an error in the output. In this section, two closed-form upper bounds on $P_{al}(L,p,U(X))$ are derived. These two bounds are compared with Ivanov's bounds for various test lengths L, output error probabilities p, and signature polynomials $U(X)$.

Theorem 1: Given

1. a polynomial $U(X)$ without X as a factor (in other words, all of the signature register stages participate in the feedback function), with period L_C, and
2. a single output response corresponding to a random pattern test length L,

then for $L<L_C$,

$$P_{al}(L,p,U(X)) \le f_1(L,p) =$$

$$\frac{1-p^{L+1}}{(L+1)(1-p)} - \frac{(1-p)^L}{(L+1)} - \frac{Lp^2(1-p)^{L-2}}{2} - p(1-p)^{L-1} - p^L \quad (1)$$

Proof: In order to compute $P_{al}(L,p,U(X))$, we need only consider *error polynomials*, $E(X)$, corresponding to length L error sequences. Aliasing occurs if $E(X)$ is a multiple of $U(X)$. The serial signature, α, is 0 for all $E(X)$ which are multiples of $U(X)$.

Lemma: If $E(X)$ is a multiple of $U(X)$ and $L<L_C$ then the weight of $E(X)$ cannot be 2 or L.

Proof of Lemma: Since the period L_C is greater than L the weight of $E(X)$ cannot be 2. The proof is by contradiction. Assume that $E(X)$ has weight 2. This implies the existence of non-negative integers s and t, such that $s<t<L$ and $E(X) = X^s+X^t = X^s(1+X^{t-s})$. Since $E(X)$ is a multiple of $U(X)$, $U(X)$ divides $X^s(1+X^{t-s})$. We are given that X is not a factor of $U(X)$ therefore $U(X)$ divides $1+X^{t-s}$. This leads to a contradiction because the period L_C is greater than $t-s$. Similarly we prove that the weight of $E(X)$ cannot be L. Assume $E(X)$ *mod* $U(X) = 0$ and weight of $E(X)$ is L. Given that $E(X)$ has weight L we have $E(X) = X^{L-1}+X^{L-2}+ \ldots +1$ and $U(X)$ divides $E(X)$. It follows that $U(X)$ also divides $(X+1)E(X)$. However $(X+1)E(X) = X^L+1$, this implies that the period L_C of $U(X)$ is less than or equal to L. This is a contradiction because we are given $L<L_C$.

The probability of a specific weight-w length-L error sequence is $p^w(1-p)^{L-w}$. This corresponds to a weight w polynomial $E(X)$. From [Saxena 91], the number of weight w polynomials having signature

α=0 for polynomials $U(X)$, without X as a factor, is bounded above by

$$\frac{1}{L-w+1}\binom{L}{w}$$

Since there are no weight-1†, weight-2, or weight-L error sequences having zero signature

$$P_{al}(L,p,U(X)) \le \sum_{w=3}^{L-1} \frac{1}{L-w+1}\binom{L}{w} p^w(1-p)^{L-w}$$

This sum can be expressed in a closed-form by deriving a closed-form for the following expression:

$$\sum_{w=0}^{L} \frac{1}{L-w+1}\binom{L}{w} p^w(1-p)^{L-w}$$

$$= \frac{p^{L+1}}{1-p} \sum_{w=0}^{L} \frac{1}{L-w+1}\binom{L}{w}\left(\frac{1-p}{p}\right)^{L-w+1}$$

Now substitute $y=\frac{1-p}{p}$, in the above expression. We have

$$\sum_{w=0}^{L} \frac{1}{L-w+1}\binom{L}{w}\left(\frac{1-p}{p}\right)^{L-w+1}$$

$$= \sum_{w=0}^{L} \frac{1}{L-w+1}\binom{L}{w} y^{L-w+1}$$

$$= \sum_{w=0}^{L} \int_0^y \binom{L}{w} y^{L-w} dy = \int_0^y \sum_{w=0}^{L} \binom{L}{w} y^{L-w}\, dy$$

$$= \int_0^y (1+y)^L\, dy = \frac{(1+y)^{L+1}-1}{L+1}$$

The above closed-form expression for $y=\frac{1-p}{p}$ is a summation for the range w=0 to w=L; excluding the terms for w=0, 1, 2 and L we have for $L<Lc$

$$P_{al}(L,p,U(X))$$

$$\le \frac{1-p^{L+1}}{(L+1)(1-p)} - \frac{(1-p)^L}{(L+1)} - \frac{Lp^2(1-p)^{L-2}}{2} - p(1-p)^{L-1} - p^L$$

Q.E.D

In Theorem 2, another upper bound on $P_{al}(L,p,U(X))$ is derived.

Theorem 2: Given

1. a polynomial $U(X)$ without X as a factor (in other words, all of the signature register stages participate in the feedback function), with period L_C and
2. a single output response corresponding to a random pattern test length L, then for $L < L_C$,

$$P_{al}(L,p,U(X)) \le f_2(L,p) =$$

$$\frac{1-(1-p)^{L+1}}{(L+1)p} - \frac{p^L}{(L+1)} - \frac{Lp(1-p)^{L-1}}{2} - \frac{L(L-1)p^2(1-p)^{L-2}}{6} - (1-p)^L \qquad (2)$$

Proof: The proof is similar to that in Theorem 1; however the bound, $\frac{1}{w+1}\binom{L}{w}$, on the number of weight w polynomials having signature α=0 for polynomials $U(X)$ is used. This bound has been derived in [Saxena 91]. Following the reasoning developed in the proof of Theorem 1 we have for $L < Lc$,

$$P_{al}(L,p,U(X)) \le \sum_{w=3}^{L-1} \frac{1}{w+1}\binom{L}{w} p^w(1-p)^{L-w}$$

This sum can be expressed in a closed form by deriving a closed form for the following expression:

$$\sum_{w=0}^{L} \frac{1}{w+1}\binom{L}{w} p^w(1-p)^{L-w}$$

$$= \frac{(1-p)^{L+1}}{p} \sum_{w=0}^{L} \frac{1}{w+1}\binom{L}{w}\left(\frac{p}{1-p}\right)^{w+1}$$

Now substitute $y=\frac{p}{1-p}$, in the above expression. We have

$$\sum_{w=0}^{L} \frac{1}{w+1}\binom{L}{w}\left(\frac{p}{1-p}\right)^{w+1}$$

$$= \sum_{w=0}^{L} \frac{1}{w+1}\binom{L}{w} y^{w+1}$$

$$= \sum_{w=0}^{L} \int_0^y \binom{L}{w} y^w dy = \int_0^y \sum_{w=0}^{L} \binom{L}{w} y^w dy$$

$$= \int_0^y (1+y)^L\, dy = \frac{(1+y)^{L+1}-1}{L+1}$$

The forgoing closed-form expression for $y=\frac{p}{1-p}$ is a summation for the range w=0 to w=L; excluding the terms for w=0, 1, 2 and L we have $P_{al}(L,p,U(X))$

$$\le \frac{1-(1-p)^{L+1}}{(L+1)p} - \frac{p^L}{(L+1)} - \frac{Lp(1-p)^{L-1}}{2} - \frac{L(L-1)p^2(1-p)^{L-2}}{6} - (1-p)^L \text{ for } L<Lc$$

Q.E.D

$f_1(L,p)$ and $f_2(L,p)$ define two closed-form upper bounds on $P_{al}(L,p,U(X))$. For p close to zero, $f_1(L,p)$ is tighter than $f_2(L,p)$; however, for p close to one,

† Weight-0 sequence is excluded because it corresponds to error escape situation and is separately quantified by escape probability [McCluskey 88].

$f_2(L,p)$ provides a tighter bound on $P_{al}(L,p)$. This is illustrated in Fig. 2.

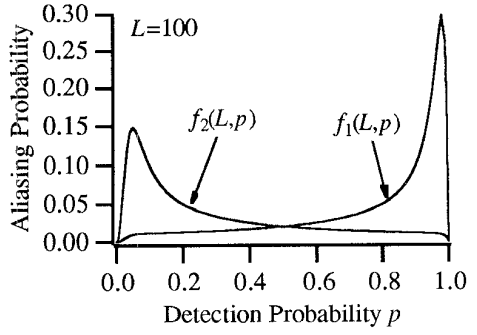


Figure 2. Plot of Bounds $f_1(L,p)$ and $f_2(L,p)$ as a Function of p.

The plots in Fig. 2 are for test length $L=100$. Although $L=100$ is a small test length it does illustrate the nature of $f_1(L,p)$ and $f_2(L,p)$ as a function of p. A closed-form upper bound on $P_{al}(L,p,U(X))$ is $min\{f_1(L,p),f_2(L,p)\}$. A bound tighter than this is

$$\sum_{w=3}^{L-1} min\left\{\frac{1}{w+1},\frac{1}{L-w+1}\right\}\binom{L}{w}p^w(1-p)^{L-w}$$

unfortunately, there is no simple way of expressing this in a closed-form.

3.1 Comparison With Previously Published Bounds

In [Ivanov 89] the following bound on the aliasing probability for degree r primitive polynomials was proved: $P_{al}(L,p,U(X)) \le f_3(L,p) =$

$$2^{-r}\left(1+|1-2p|^{\lfloor L/r \rfloor}\right)^r-(1-p)^L \qquad (3)$$

Let us denote Ivanov's bound (eq. (3)) by $f_3(L,p)$. Figures 3 and 4 compare bounds developed in this paper and $f_3(L,p)$. In Figures 3 and 4, the graph is plotted with output error probability p as the independent variable. From these graphs it can be seen that Ivanov's bound is sharper than the upper bound derived in this paper for values of p in the mid-region. However, for p close to zero or one bounds developed in this paper are sharper. For example, as $p \to 1$, bound $f_3(L,p) \to 1$. For low and high values of p the bounds developed in this paper are tighter than Ivanov's bound. There are cut-off points where one bound gets tighter than the other. Two cut-off points p_{small} and p_{large} are defined (Figures 3 and 4) such that:

$f_1(L,p) \le f_3(L,p)$ for $p \le p_{small}$ and

$f_2(L,p) \le f_3(L,p)$ for $p \ge p_{large}$.

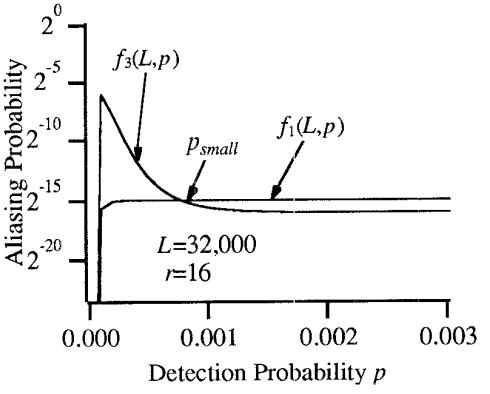


Figure 3. Comparison of Bounds as a Function of p

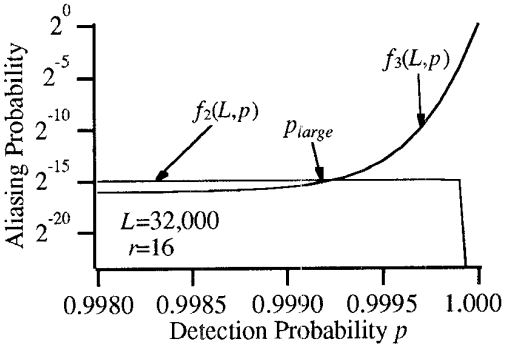


Figure 4. Comparison of Bounds as a Function of p

The upper bounds can be further sharpened by taking the minimum of $f_1(L,p)$, $f_2(L,p)$, and $f_3(L,p)$.

Throughout this section the emphasis has been on the derivation of closed-formed bounds on $P_{al}(L,p,U(X))$. The reason for this is that closed-form bounds are useful in deriving a simple bound on $P_{al}(L,p,U(X))$, which does not depend on p. At design time, the system designer has the freedom to choose the signature polynomial $U(X)$, the signature register size r, and the test length L; however, the designer has no choice or has complete uncertainty about the faults that occur in the circuit (hence, uncertainty about the range of p). Therefore, what the system designer needs is a bound on the aliasing probability which is true for all values of p. Bounds that only depend on the test length L and the signature polynomial $U(X)$ are called *simple bounds*.

4. SHARPENED SIMPLE BOUNDS

In [Saxena 91], a simple bound, $\frac{2}{L+2}$, was derived for test lengths L less than the period L_C of the signature polynomial. This bound is sharpened by

almost a factor of two in this section. This sharpened simple bound is derived by taking the maxima of the function $min\{f_1(L,p), f_2(L,p), f_3(L,p)\}$.

For a given L the function $f_3(L,p)$ behaves [see Figures 3 and 4] as follows:

1. at p=0 it is 0
2. for some small p>0 attains a maximum value and falls rapidly as p approaches 0.5.
3. as p approaches 1: this function remains almost flat; rapidly increases in the neighborhood of one and attains value 1 at p=1.

For a given $L<L_C$ the function $f_1(L,p)$ behaves [see Fig. 2] as follows:

1. at p=0 it is 0
2. it increases slowly as p approaches 1
3. it attains a maximum value in the neighborhood of 1, then falls rapidly and attains value zero at p=1.

For a given $L<L_C$ the function $f_2(L,p)$ behaves [see Fig. 2] as follows:

1. at p=0 it is zero
2. it attains a maximum value in the neighborhood of 0
3. as p further increases, it falls rapidly and attains value 0 at p=1.

For small values of p, the min function is dominated by $f_1(L,p)$ and $f_3(L,p)$. For mid-values of p, $f_3(L,p)$ dominates the min function. Function $f_2(L,p)$ dominates the min function for large values of p. There exist[††] p_{small} and p_{large} (as illustrated in Figures 3 and 4) $0<p_{small}<p_{large}<1$, such that:

1. $f_1(L,p) \le f_3(L,p)$, for $p \le p_{small}$
2. $f_3(L,p) < f_1(L,p)$, and $f_3(L,p) < f_2(L,p)$, for $p_{small} < p < p_{large}$
3. $f_2(L,p) \le f_3(L,p)$, for $p \ge p_{large}$

The values p_{small} and p_{large} can be calculated by solving equations $f_1(L,p) = f_3(L,p)$ and $f_2(L,p) = f_3(L,p)$ respectively. It follows from the behavior of these functions that a simple bound on the aliasing probability is the maximum of $f_1(L,p_{small})$ and $f_2(L,p_{large})$. Solving for the exact values of p_{small} and p_{large} is a difficult problem. However, in order to derive simple bounds on the aliasing probability it is sufficient to derive an upper-bound on p_{small} and a lower bound on p_{large}. This is because from equations (1) and (2) it follows that:

$$f_1(L, p_{small}) \le \frac{1}{(L+1)(1-p_{small})}$$

and

$$f_2(L, p_{large}) \le \frac{1}{(L+1)p_{large}}$$

Using standard numerical analysis techniques the required bounds on p_{small} and p_{large} can be derived by incurring only $O(1)$ complexity. That is, for a given test length L and signature register size r, the bounds on p_{small} and p_{large} can be derived by incurring only a constant complexity. Clearly, the bounds on p_{small} and p_{large} depend on L and r. Let us define $\varepsilon(L,r) = max\{(1-p_{small})^{-1}, (p_{large})^{-1}\}-1$. $\varepsilon(L,r)$ is small for large values of test length L and signature register size r. Figures 5 illustrates this. The values in this figure were obtained by using a simple numerical analysis root finding program. It follows from the definition of $\varepsilon(L,r)$ that

$$1+\varepsilon(L,r) = max\{(1-p_{small})^{-1}, (p_{large})^{-1}\}$$

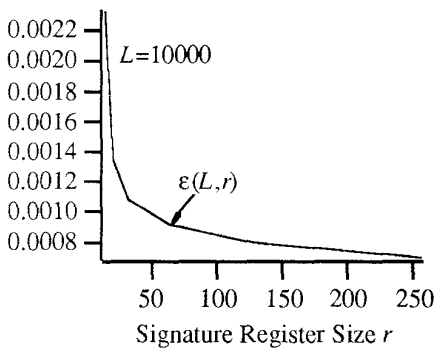


Figure 5. Plot of ε as a Function of r

It was already shown that a simple bound on the aliasing probability is $max\{f_1(L, p_{small}), f_2(L, p_{large})\} \le max\{(1-p_{small})^{-1}, (p_{large})^{-1}\} \frac{1}{(L+1)} = \frac{1+\varepsilon(L,r)}{(L+1)}$. This is almost $\frac{1}{L}$. This refined simple bound holds good for test lengths L less than L_C.

The derivation of the simple bound relies on the correctness of Ivanov's bound for all polynomials without X as a factor. In [Ivanov 89], the bound was proved for primitive polynomials. This bound also holds good for non-primitive polynomials. A proof is presented in the Appendix.

In Fig. 6, the sharpened simple bound is compared with the exact aliasing probability for the signature polynomial X^8+X^3+1. The exact values for the

[††] The existence of p_{small} and p_{large} can be formally proved by considering the monotonic properties (in restricted regions of p) and the continuity properties of functions f_1, f_2, and f_3.

aliasing probability is calculated for a fault with p=0.992. The period L_C of this polynomial is 217. The simple bound L^{-1} is used in Fig. 6. It is interesting to note that the simple bound L^{-1} in Fig. 6 is almost a monotonic envelope for the exact aliasing probability. We conjecture that L^{-1} is the best monotonic bound on the aliasing probability in serial signature analysis for test lengths $L<L_C$. For period-multiple test lengths L, there is no opportunity to refine the simple bounds because the aliasing probability can go as high as one. For non-period-multiple test lengths $L>L_C$, there is opportunity to improve the simple bounds by a factor of two; however, there is not much practical value in carrying out this refinement. This is because at test length $L=L_C-1$, the simple bound on the aliasing probability is almost $\frac{1}{L_C-1}$. For primitive polynomials, this is very close to the asymptotic aliasing probability value 2^{-r}.

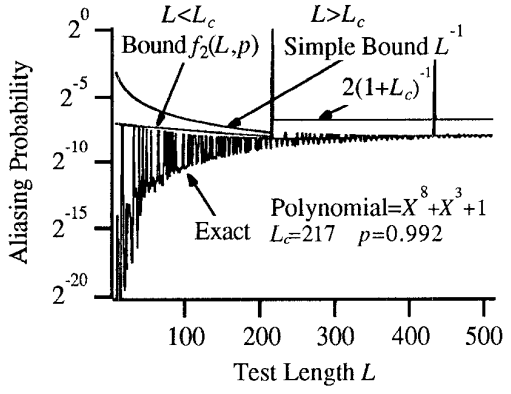


Figure 6. Comparison of Exact Values and the Simple Bound

4.1 Experimental Results

In Fig. 6, the refined bound is compared with the theoretically calculated exact aliasing probability values. Some simulation experiments were performed to compare experimentally measured aliasing probability values with the bounds derived in this paper. Figure 7 presents the results of one such experiment. The experimental results in Fig. 7 track the values predicted by the exact (derived analytically) aliasing probability values. Therefore these simulations not only provide comparison of the simple bounds and the experimental aliasing probability estimates but also provide a validation of the bernoulli model. The circuits simulated in these experiments were the ALU181 (Fig. 8) and a 7-bit Comparator (Figs. 7).

For each of the plots in Fig. 7 and Fig. 8, the experimental aliasing probability as a function of test length L was obtained as follows. A single output of the corresponding circuit was chosen for response compaction by serial signature analysis for each experiment. Each experiment had 50,000 trials. The trials were different in that different random test patterns of length 511 were used and other parameters were constant. For each trial and at every test length $L \leq 511$, the signature of the faulty circuit was compared with the fault-free signature at that length to record the aliasing information. The probability of aliasing was calculated after 50,000 different trials. The experimental error in estimating aliasing probability based on 50,000 trails is within ±20%.

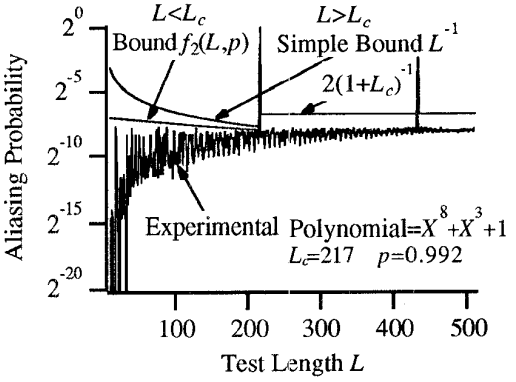


Figure 7. Experimental Validation for Serial Signature Analysis (7-Bit Comparator)

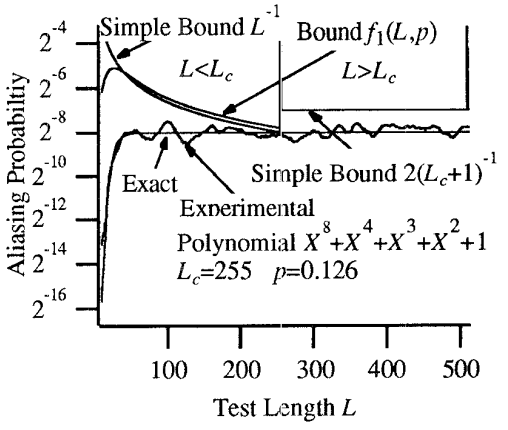


Figure 8. Comparison of Exact Values, Experimental Values and the Simple Bound (ALU181)

The nature of simulation experiments described by Figures 7 and 8 is that a particular fault was fixed and the parameter of variation was random test patterns. Since the simple bounds apply to any combinational fault, the expected number of combinational faults that alias is also bounded above by the product of the simple bound and the total number of combinational

faults. In other words, the expected fraction of combinational faults that alias is bounded above by the simple bound on aliasing probability. Fig. 9 illustrates this. If there are n_f combinational faults in a sample and the set $\{g_1, g_2, ..., g_v\}$ denotes all the distinguishing faults in this sample; where each fault g_i is a representative from an equivalent class of b_i equivalent faults, $1 \le i \le v$. Clearly, $\Sigma b_i = n_f$. For a test length L, the expected number of faults that alias, E[aliasing faults], is given by

$$E[\text{aliasing faults}] = \sum_{i=1}^{v} b_i \text{Prob}\{\text{fault } g_i \text{ aliases}\}$$

Since the simple bounds on the aliasing probability apply to any combinational fault, we have

$$E[\text{aliasing faults}] \le \sum_{i=1}^{v} b_i \text{ (Simple Bound)}$$

$$= \text{(Simple Bound)} \sum_{i=1}^{v} b_i$$

$$= \text{(Simple Bound)}\ n_f$$

The simulation experiments reported in Fig. 9 were done on the ALU181 circuit. A total of 1.4 million triple stuck-at faults were simulated. For each of these faults, the random test pattern was fixed. For this experiment the statistical estimation error is hard to quantify because it requires knowledge about the distribution, b_i, of the equivalent faults in the 1.4 million fault sample. It is interesting to note that the fraction of aliased faults (Fig. 9) peaks at test length $L=L_c=255$.

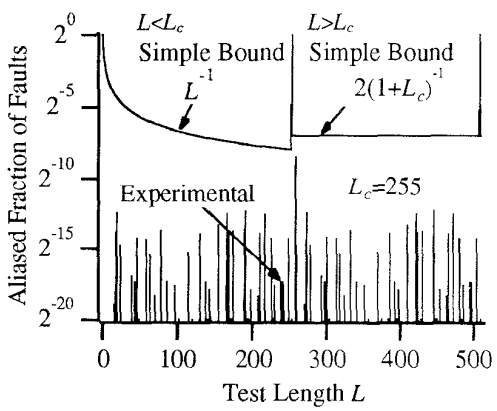


Figure 9. Simple Bounds and Expected Fraction of Aliased Faults (ALU181)

5. CONCLUSIONS

We conjecture that the best monotonic bound on the aliasing probability for serial signature analysis is L^{-1} for test lengths L less than L_C. Simple bounds on the aliasing probability for serial signature analysis are refined by almost a factor of two. Exact values sometime attain values close to that predicted by the simple bound (Fig. 6, for example). These bounds provide a useful design guideline of using a signature polynomial with period greater than the test length. For example, with random test length $L=10^6$, a primitive polynomial with degree greater than or equal to 20 guarantees the aliasing probability to be less than or equal to 0.0001%.

ACKNOWLEDGEMENTS

This paper was supported in part by the Hewlett-Packard Resident Fellowship, in part by the National Science Foundation under Grant No. MIP-8709128, and in part by the Innovative Science and Technology Office of the Strategic Defense Initiative Organization administered through the Office of Naval Research under contract No. N00014-85-K-0600.

REFERENCES

[Damiani 89] Damiani, M., *et al.*, "An Analytical Model for the Aliasing Probability in Signature Analysis Testing," *IEEE Trans. CAD,* Vol. 8, No. 11, pp. 1133-1144, Nov. 1989.

[Franco 91] P. Franco, N.R. Saxena, and E.J. McCluskey, "Relating Signature Analysis Aliasing to Test Length and Register Design," *Proc. ISCAS-91*, pp. 1889-1892, June 1991.

[Gupta 88] Gupta, S.K and D.K. Pradhan, "A New Framework for Designing and Analyzing BIST Techniques: Computation of Exact Aliasing Probability," *Dig. 1988 IEEE Test Conf.*, pp. 329-342, Sep. 1988

[Ivanov 89] Ivanov, A. and V.K. Agarwal, "An Analysis of the Probabilistic Behavior of Linear Feedback Signature Registers," *IEEE Trans. CAD,* Vol. 8, No. 10, pp. 1074-1088, Oct. 1989.

[Iwasaki 90] Iwasaki, K. and N. Yamaguchi, "Design of Signature Circuits Based on Weight Distribution of Error-Correcting Codes," *Proc. ITC*, pp. 779-785, Sep. 1990.

[McCluskey 91] McCluskey, E.J., "Techniques for Test Output Response Analysis," *Proc. ISCAS-91*, pp. 1869-1872, June 1991.

[McCluskey 88] McCluskey, E.J., *et al.*, "Probability Models for Pseudorandom Test Sequences," *IEEE Trans. CAD,* Vol. 7, No. 1, pp. 68-74, Jan. 1988.

[Peterson 84] Peterson, W.W. and E.J. Weldon Jr., *Error-Correcting Codes*, 2nd ed., Cambridge, MA: M.I.T. Press, 1984.

[Shedletsky 77] Shedletsky, J.J., "Random Testing: Practicality vs. Verified Effectiveness," in *Proc. FTCS-7*, pp. 175-179, June 1977.

[Saxena 91] Saxena, N.R., P. Franco, and E.J. McCluskey, "Bounds on Signature Analysis

Aliasing for Random Testing," *Proc. FTCS-21*, pp. 104-111, June 1991.

[Williams 88] Williams, T.W., *et al.*, "Bounds and Analysis of Aliasing Errors in Linear Feedback Shift Registers," *IEEE Trans. CAD*, Vol. 7, No. 1, pp. 75-83, Jan. 1988.

APPENDIX

The following theorem proves that Ivanov's bound is true for all signature polynomials $U(X)$ without X as a factor. In proving Ivanov's bound, a particular implmentation of signature analyzer is used. It follows from the results in [Saxena 91] that any linear finite state machine implementation of signature analysis with $U(X)$ as the characteristic polynomial will also satisfy this bound.

Theorem A-1: For test length L; with degree-r signature polynomial $U(X)$ without X as a factor; and, a fault with detection probability p; the aliasing probability, $P_{al}(L,p,U(X))$, is bounded above by

$$2^{-r}\left(1+|1-2p|^{\lfloor L/r \rfloor}\right)^r - (1-p)^L.$$

Proof: Without any loss in generality we assume that the signature is computed using an implementation corresponding to Fig. A-1. For the purpose of computing aliasing probability we need only consider error sequences. This is because of the linearity property of signature analysis. Let us denote the error sequence for a test length L by $e_1, e_2, ..., e_L$. Aliasing occurs if the signature of this error sequence is all-zero.

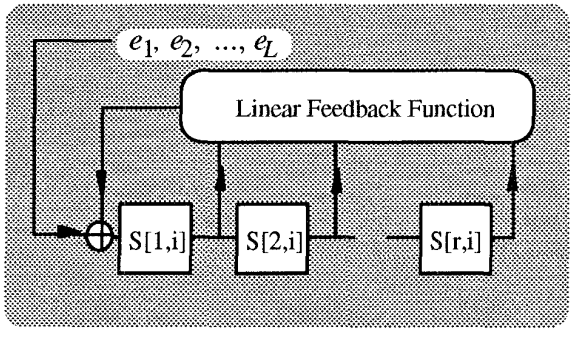


Figure A-1. An Implementation of Serial Signature Computation

By the nature of signature computation in Fig. A-1, it is easy to infer that the binary value in each of the r signature stages is a linear sum of some subset of terms in the error sequence $e_1, e_2, ..., e_L$. The binary value in each of the r signature register stages is uniquely represented by r corresponding subsets. These subsets change as a function of the number of sequence terms applied and the nature of the linear feedback function. Let us denote these subsets by $S[1,i]$, $S[2,i]$, ..., $S[r,i]$ for the length i error sequence $e_1, e_2, ..., e_i$. The linear feedback function simply consists of *exclusive-or* gates. Any *exclusive-or* operation of the binary values of some stages corresponds to the set *symmetric difference* operation of the sets of these stages.

The subsets $S[1,i+1]$, $S[2,i+1]$, ..., $S[r,i+1]$ corresponding to the length $i+1$ error sequence, $e_1, e_2, ..., e_{i+1}$, are recursively obtained as

$$S[j,i+1] = S[j-1,i] \text{ for } 2 \le j \le r$$

$$S[1,i+1] = \{e_{i+1}\} \nabla (S[1,i] \cap U[1]) \nabla (S[2,i] \cap U[2]) \nabla ... (S[r-1,i] \cap U[r]) \nabla S[r,i]$$

The symbol ∇ denotes the symmetric difference. The set $U[j]$, $1 \le j \le r-1$, is a universal set (i.e., includes set $S[j,i]$ in the symmetric difference) if there is a feedback connection from stage j, else the set $U[j]$ is a null set (i.e., it does not include the set $S[j,i]$ in the symmetric difference). Set $\{e_{i+1}\}$ is the singleton set which includes the error sequence term e_{i+1} for the $(i+1)$'th error sequence input. Since the term is not present in the sets $S[1,i]$, $S[2,i]$, ..., $S[r,i]$, by the symmetric difference operation it is included in the set $S[1,i+1]$ without cancellation.

For the length i error sequence $e_1, e_2, ..., e_i$, let us define sets $m[1,i]$, $m[2,i]$, ..., $m[r,i]$ with the following properties:

1. For $1 \le j \le r$ sets $m[j,i] \subseteq S[j,i]$. (*inclusion property*)
2. Sets $m[1,i]$, $m[2,i]$, ..., $m[r,i]$ are mutually disjoint; that is, for all $k \ne j$ such that $1 \le j \le r$ and $1 \le k \le r$, $m[j,i] \cap m[k,i] = \emptyset$. (*mutually disjoint property*)

Lemma: There exists a constructive procedure of selecting the sets $m[j,i]$ with the property that for every i the sets $m[j,i]$ have at least $\lfloor \frac{i}{r} \rfloor$ members for $1 \le j \le r$.

Proof of Lemma: The input sequence $e_1, e_2, ..., e_i$, can be decomposed into at least $\lfloor \frac{i}{r} \rfloor$ disjoint sequences each feeding into the signature register independently as shown below

Sequence q	Sequence
1	$e_1, e_2, ..., e_r, 0, ..., 0$
2	$0, 0, ..., 0, e_{r+1}, e_{r+2}, ..., e_{2r}, 0, ..., 0$
.	.
.	.
.	.
$a = \lfloor \frac{i}{r} \rfloor$	$0, ..., 0, e_{(a-1)r+1}, e_{(a-1)r+2}, ..., e_{ar}, 0, ..., 0$
$a+1$	(residual sequence if i not a multiple of r)

These sequences are disjoint in that they do not have any common symbol terms e_j between them. Let us denote sets $m_q[i,j]$, $1 \le q \le \lfloor \frac{i}{r} \rfloor$, with the inclusion and the disjoint properties for the corresponding disjoint sequences shown above. In order get a construction of sets $m[1,i]$, $m[2,i]$, ..., $m[r,i]$ each having at least $\lfloor \frac{i}{r} \rfloor$ members it is sufficient to show that each of the sets $m_q[1,i]$, $m_q[2,i]$, ..., $m_q[r,i]$, $1 \le q \le \lfloor \frac{i}{r} \rfloor$, have at least one member. This is because the sets $m[i,j]$ can be constructed by taking the union of the sets $m_q[i,j]$ for $1 \le q \le \lfloor \frac{i}{r} \rfloor$. This union operation is allowed because of the superposition property of the linear feedback shift register. If the sets $m_q[i,j]$ have at least one member then the set $m[i,j]$ will have at least $\lfloor \frac{i}{r} \rfloor$ members because it is derived from the union of $\lfloor \frac{i}{r} \rfloor$ mutually disjoint (disjoint because of disjoint sequences 1,2, ..., a) sets. Also by symmetry, it is sufficient to establish that the cardinality of $m_q[i,j]$ is at least one, just for q=1; because, all other sequences are shifted versions of Sequence 1 with different error symbols. As Sequence 1 is fed into the LFSR, after r steps the first stage in the LFSR will at least depend on error symbol e_r (because set S[1,r] will contain e_r) and the second stage will at least depend on e_{r-1} and so on ... After r steps we can pick sets $m_1[1,r] = \{e_r\}$, $m_1[2,r] = \{e_{r-1}\}$, ... , $m_1[r,r]=\{e_1\}$ satisfying inclusion, and mutually disjoint properties.

For Sequence 1 after r steps , all-zero symbols are fed into the LFSR; therefore, the contents in each of the r signature register stages will be some linear combination of error symbols e_1, ..., e_r. The fact that the signature polynomial chosen does not have X as a factor ensures that each of the r stages in the signature register are linearly independent. This is because the matrix defining the state transition graph of the signature register is *non-singular* (determinant non-zero). Linear independence formulated in terms of sets implies that the set corresponding to any one of the signature stages cannot be obtained by the symmetric difference of sets corresponding to any of the remaining stages. This linear independence always allows the construction of sets $m_1[1,r] = \{p_r\}$, $m_1[2,r] = \{p_{r-1}\}$, ..., $m_1[r,r]=\{p_1\}$, such that $\{p_1, p_2, ..., p_r\}$ is some permutation of $\{e_1, e_2, ..., e_r\}$. If such a construction is not possible then it implies that at least one of the signature register stages is linearly dependent on other stages (leads to a contradiction). The following paragraph proves this.

Let us assume that for some $h<r$, after having picked sets $m_1[1,r]=\{p_r\}$, $m_1[2,r]=\{p_{r-1}\}$, ..., $m_1[h,r] = \{p_{r-h+1}\}$ we cannot pick set $m_1[h+1,r]$ for any permutation of $\{p_{r-h+1}, p_{r-h}, ..., p_r\}$ of any h element subset of $\{e_1, e_2, ..., e_r\}$. This implies that the h+1 signature register stages are determined completely by h error symbols and therefore signature register stages 1 through h+1 are not linearly independent (a contradiction!).

This establishes that the cardinality of sets $m[j,i]$ is at least $\lfloor \frac{i}{r} \rfloor$ for $1 \le j \le r$. **(End of Lemma)**

For test length L, i=L. The number of members in sets $m[j,L]$ is at least $\lfloor \frac{L}{r} \rfloor$. A specific signature in the signature register is obtained if each of the stages assume a specific value. This means that sets $S[j,L]$ assume a specific parity. Since sets $m[j,L]$ are subsets of sets $S[j,L]$, a specific parity of set $S[j,L]$ is accomplished by the following compound events:

1) the parity of set $m[j,L]$ is even and the parity of the set $S[j,L]$-$m[j,L]$ is even, or
2) the parity of set $m[j,L]$ is odd and the parity of the set $S[j,L]$-$m[j,L]$ is odd.

The probability of sets $S[j,L]$, $1 \le j \le r$, assuming a specific parity can be bounded above by the upper bound on the probability of sets $m[j,L]$, $1 \le j \le r$, assuming even or odd parities. From the bernoulli model it follows that the probability of any error symbol assuming a value 1 is p. The probability of set $m[j,L]$ assuming a specific parity (odd or even) is given by the expressions $2^{-1}\left(1 \pm (1-2p)^{\lfloor L/r \rfloor}\right)$. These expressions are obtained by summing the probability terms $\binom{\lfloor L/r \rfloor}{w} p^w (1-p)^{\lfloor L/r \rfloor - w}$ for even (odd) w in order to obtain even (odd) parity for sets $m[j,L]$, $1 \le j \le r$. The expressions, $2^{-1}\left(1 \pm (1-2p)^{\lfloor L/r \rfloor}\right)$, can be bounded above by

$$2^{-1}\left(1 + |1-2p|^{\lfloor L/r \rfloor}\right)$$

Therefore, the probability of all of the r sets $m[j,L]$, $1 \le j \le r$, having a specific parity is bounded above by

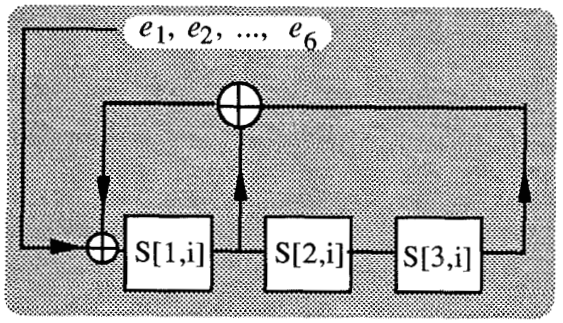
$$2^{-r}\left(1 + |1-2p|^{\lfloor L/r \rfloor}\right)^r$$

(statistical independence is assumed because sets $m[j,L]$ are disjoint for $1 \le j \le r$). Excluding the error-free case, we have the following bound on the aliasing probability

$$2^{-r}\left(1 + |1-2p|^{\lfloor L/r \rfloor}\right)^r - (1-p)^L \qquad \text{Q.E.D}$$

The following example illustrates the construction of sets $m[i,j]$.

Example: (r=3, L=6)



Time i=0: (no symbol enters the LFSR)

$S[1,0] = \emptyset$; $S[2,0] = \emptyset$; $S[3,0] = \emptyset$;

$m_1[1,0] = \emptyset$; $m_1[2,0] = \emptyset$; $m_1[3,0] = \emptyset$;

$m_2[1,0] = \emptyset$; $m_2[2,0] = \emptyset$; $m_2[3,0] = \emptyset$;

$m[1,0] = \emptyset$; $m[2,0] = \emptyset$; $m[3,0] = \emptyset$;

Time i=1: (e_1 symbol enters the LFSR)

$S[1,1] = \{e_1\}$; $S[2,1] = \emptyset$; $S[3,1] = \emptyset$;

$m_1[1,1] = \{e_1\}$; $m_1[2,1] = \emptyset$; $m_1[3,1] = \emptyset$;

$m_2[1,1] = \emptyset$; $m_2[2,1] = \emptyset$; $m_2[3,1] = \emptyset$;

$m[1,1] = \{e_1\}$; $m[2,1] = \emptyset$; $m[3,1] = \emptyset$;

Time i=2: (e_2 symbol enters the LFSR)

$S[1,2] = \{e_2,e_1\}$; $S[2,2] = \{e_1\}$; $S[3,2] = \emptyset$;

$m_1[1,2] = \{e_2\}$; $m_1[2,2] = \{e_1\}$; $m_1[3,2] = \emptyset$;

$m_2[1,2] = \emptyset$; $m_2[2,2] = \emptyset$; $m_2[3,2] = \emptyset$;

$m[1,2] = \{e_2\}$; $m[2,2] = \{e_1\}$; $m[3,2] = \emptyset$;

Time i=3: (e_3 symbol enters the LFSR)

$S[1,3] = \{e_3,e_2,e_1\}$; $S[2,3] = \{e_2,e_1\}$; $S[3,3] = \{e_1\}$;

$m_1[1,3] = \{e_3\}$; $m_1[2,3] = \{e_2\}$; $m_1[3,3] = \{e_1\}$;

$m_2[1,3] = \emptyset$; $m_2[2,3] = \emptyset$; $m_2[3,3] = \emptyset$;

$m[1,3] = \{e_3\}$; $m[2,3] = \{e_2\}$; $m[3,3] = \{e_1\}$;

Time i=4: (e_4 symbol enters the LFSR)

$S[1,4] = \{e_3,e_2,e_4\}$; $S[2,4] = \{e_3,e_2,e_1\}$;
$S[3,4] = \{e_2,e_1\}$;

$m_1[1,4] = \{e_3\}$; $m_1[2,4] = \{e_2\}$; $m_1[3,4] = \{e_1\}$;

$m_2[1,4] = \{e_4\}$; $m_2[2,4] = \emptyset$; $m_2[3,4] = \emptyset$;

$m[1,4] = \{e_3,e_4\}$; $m[2,4] = \{e_2\}$; $m[3,4] = \{e_1\}$;

Time i=5: (e_5 symbol enters the LFSR)

$S[1,5] = \{e_5,e_4,e_3,e_1\}$; $S[2,5] = \{e_3,e_2,e_4\}$;
$S[3,5] = \{e_3,e_2,e_1\}$;

$m_1[1,5] = \{e_3\}$; $m_1[2,5] = \{e_2\}$; $m_1[3,5] = \{e_1\}$;

$m_2[1,5] = \{e_5\}$; $m_2[2,5] = \{e_4\}$; $m_2[3,5] = \emptyset$;

$m[1,5] = \{e_3,e_5\}$; $m[2,5] = \{e_2,e_4\}$; $m[3,5] = \{e_1\}$;

Time i=6: (e_6 symbol enters the LFSR)

$S[1,6] = \{e_6,e_5,e_4,e_2\}$; $S[2,6] = \{e_5,e_4,e_3,e_1\}$;
$S[3,6] = \{e_3,e_2,e_4\}$;

$m_1[1,6] = \{e_2\}$; $m_1[2,6] = \{e_1\}$; $m_1[3,6] = \{e_3\}$;

$m_2[1,6] = \{e_6\}$; $m_2[2,6] = \{e_5\}$; $m_2[3,6] = \{e_4\}$;

$m[1,6] = \{e_2,e_6\}$; $m[2,6] = \{e_1,e_5\}$; $m[3,6] = \{e_3,e_4\}$