Fault Detection Structures for the Montgomery Multiplication over Binary Extension Fields

Arash Hariri and Arash Reyhani Masoleh

Department of Electrical and Computer Engineering
Faculty of Engineering
The University of Western Ontario
London, Ontario, Canada N6A 5B9

Outline

- Background
- Previous Work
- Time Redundancy Based Fault Detection in Montgomery Multiplication
- Parity-Based Fault Detection in the Bit-Serial Montgomery Multiplication
- Discussion and Comparison
- Conclusions

Background

The binary extension field $\mathrm{GF}(2^m)$:

- contains 2^m elements
- is an extension of *GF*(2)={0,1}
- is associated with an irreducible polynomial

$$F(z) = z^m + f_{m-1}z^{m-1} + \cdots + f_1 z + 1,$$
$$f_i \in \{0,1\} \text{ for } i = 1 \text{ to } m-1$$

Background

- Assuming x is a root of $F(z)$, i.e., $F(x) = 0$ each element of $\mathrm{GF}(2^m)$ can be represented as a polynomial of degree $m-1$

$$A \in GF(2^m) \Leftrightarrow A = a_{m-1}x^{m-1} + \cdots + a_1 x + a_0,$$

$$a_i \in \{0,1\} \text{ for } i = 0 \text{ to } m-1$$

This representation is called the polynomial basis representation.

Background

- Assuming A and B are two elements of the binary extension field and $r = x^m$ the Montgomery factor satisfying

$$\gcd(r, F(x)) = 1$$

- The Montgomery multiplication over binary extension fields is defined as

$$C = A \cdot B \cdot r^{-1} \bmod F(x),$$

$$r \cdot r^{-1} = 1 \bmod F(x).$$

Previous Work

- Time redundancy based concurrent error detection scheme for semi-systolic implementation of the Montgomery multiplication algorithm
- Based on performing two different multiplications: the polynomial basis multiplication and the Montgomery multiplication

Previous Work

- Assuming $A, B \in \mathrm{GF}(2^m)$, $\overline{A}$ and $\overline{B}$ are the Montgomery residues computed by $A \cdot x^m \bmod F(x)$ and $B \cdot x^m \bmod F(x)$ respectively, then

$$C = A \cdot B \bmod F(x)$$
$$\overline{C} = \overline{A} \cdot \overline{B} \cdot x^{-m} \bmod F(x)$$

$$\begin{aligned}\overline{C} = \overline{A} \cdot \overline{B} \cdot x^{-m} \bmod F(x) &= (A \cdot x^m) \cdot (B \cdot x^m) \cdot x^{-m} \bmod F(x)\\ &= A \cdot B \cdot x^m \bmod F(x) = C \cdot x^m \bmod F(x).\end{aligned}$$

Arash Hariri and Arash Reyhani Masoleh
The University of Western Ontario, London, Ontario, Canada

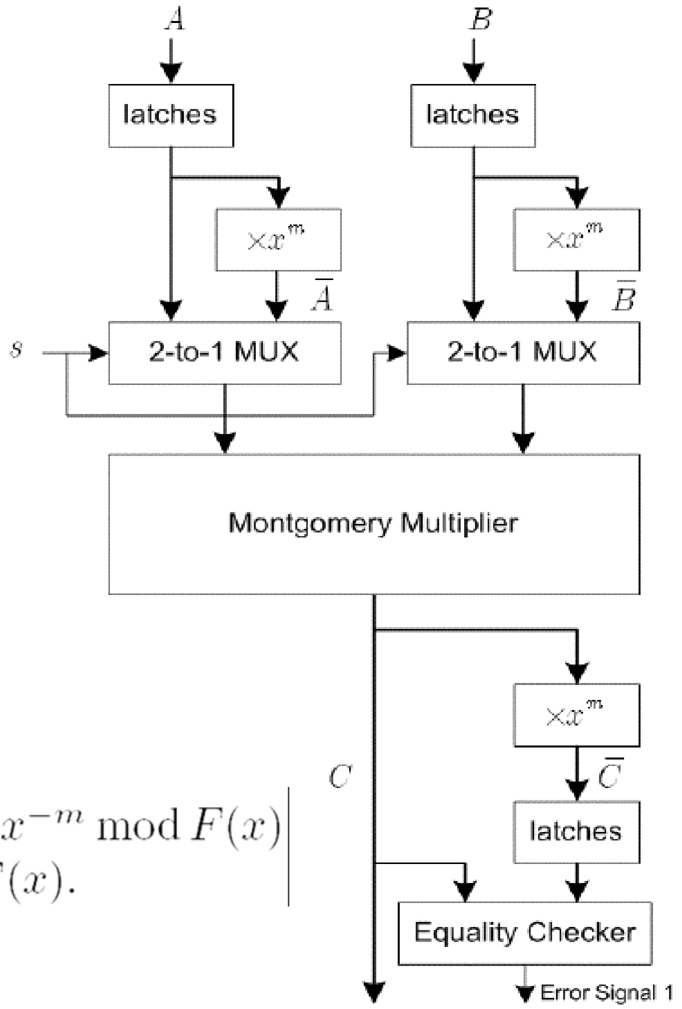
Previous Work

- Error detection flowchart using the time redundancy

$$A \cdot x^m \bmod F(x) \quad B \cdot x^m \bmod F(x)$$

$$C = A \cdot B \bmod F(x)$$

$$\overline{C} = \overline{A} \cdot \overline{B} \cdot x^{-m} \bmod F(x)$$



$$\begin{aligned}\overline{C} = \overline{A} \cdot \overline{B} \cdot x^{-m} \bmod F(x) &= (A \cdot x^m) \cdot (B \cdot x^m) \cdot x^{-m} \bmod F(x) \\ &= A \cdot B \cdot x^m \bmod F(x) = C \cdot x^m \bmod F(x).\end{aligned}$$

*By C.W. Chiou et al 2006

New Time Redundancy Based Fault Detection Scheme

- Now, we choose $r = x^{m-1}$ as the Montgomery factor, so

$$A' = A \cdot x^{-1} \bmod F(x), \ \ B' = B \cdot x^{-1} \bmod F(x) = \sum_{i=0}^{m-1} b'_i x^i$$

- So we consider two Montgomery multiplications:

$$C = A \cdot B \cdot x^{-m} \bmod F(x),$$

$$C' = A' \cdot B' \cdot x^{-(m-1)} \bmod F(x)$$

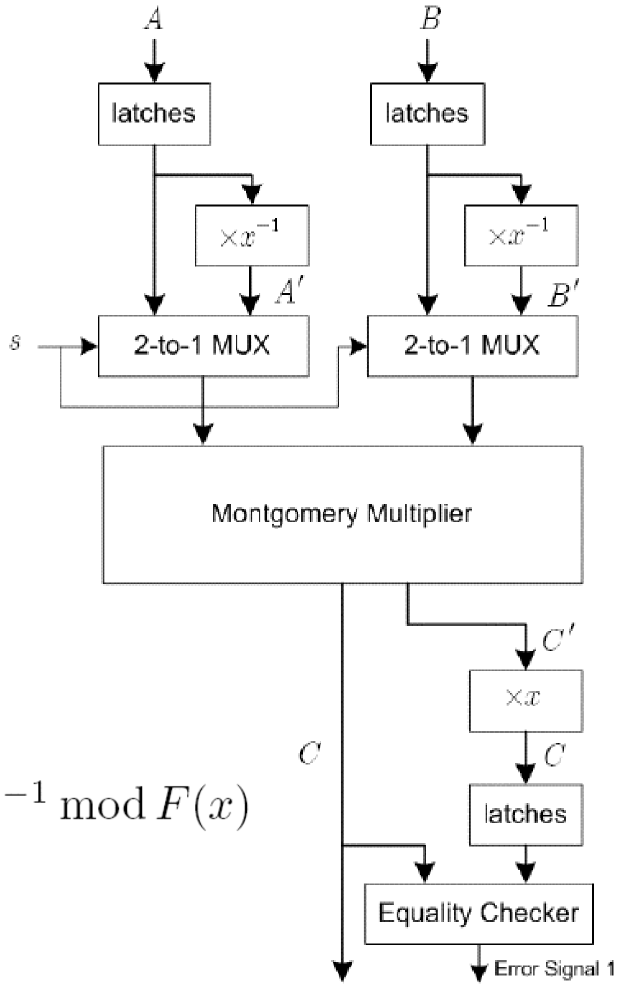
$$C' = (A \cdot x^{-1}) \cdot (B \cdot x^{-1}) \cdot x^{-(m-1)} \bmod F(x) = C \cdot x^{-1} \bmod F(x)$$

New Time Redundancy Based Fault Detection Scheme

- The Modified flowchart

$$C = A \cdot B \bmod F(x)$$

$$C' = A' \cdot B' \cdot x^{-(m-1)} \bmod F(x)$$



$$C' = (A \cdot x^{-1}) \cdot (B \cdot x^{-1}) \cdot x^{-(m-1)} \bmod F(x) = C \cdot x^{-1} \bmod F(x)$$

- The Montgomery multiplication can be implemented by using a semi-systolic architecture.
- Using the new Montgomery factor, the latency of the architecture is m, equal to the latency of the polynomial basis multiplication.

New Parity-Based Fault Detection Scheme

Algorithm 1 Bit-level Montgomery multiplication over GF(2^m)

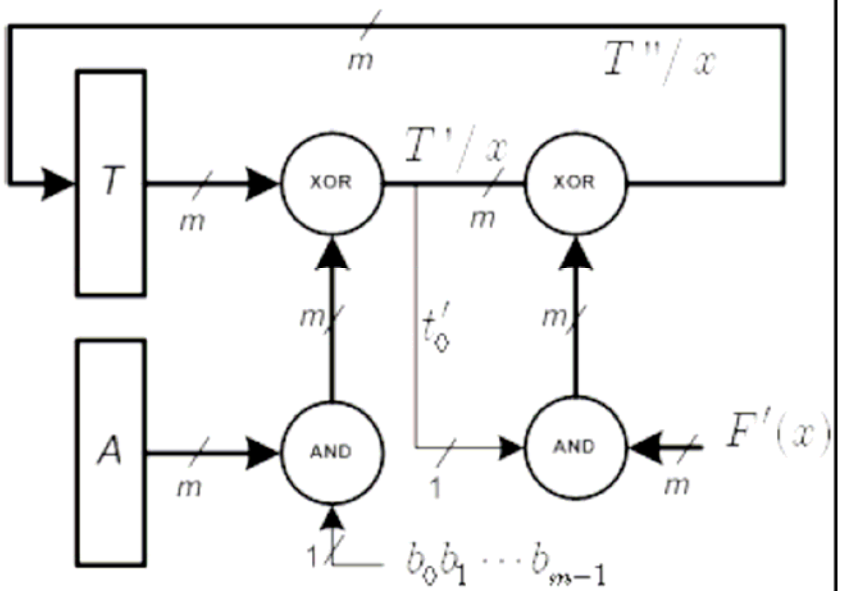
Inputs: $A, B, F(x)$
Output: $C = A \cdot B \cdot r^{-1} \bmod F(x)$
Step 1: $T := 0$
Step 2: For $i := 0$ to $m - 1$
Step 3: $T' := T + b_i A$
Step 4: $T'' := T' + t'_0 F(x)$
Step 5: $T := T''/x$
Step 6: $C := T$

*By CK Koc and T Acar 1998

New Parity-Based Fault Detection Scheme

Algorithm 1 Bit-level Montgomery multiplication over GF(2^m)

Inputs: $A, B, F(x)$
Output: $C = A \cdot B \cdot r^{-1} \bmod F(x)$
Step 1: $T := 0$
Step 2: For $i := 0$ to $m-1$
Step 3: $T' := T + b_i A$
Step 4: $T'' := T' + t'_0 F(x)$
Step 5: $T := T''/x$
Step 6: $C := T$



the latency of m clock cycles

delay of $2(T_A + T_X)$

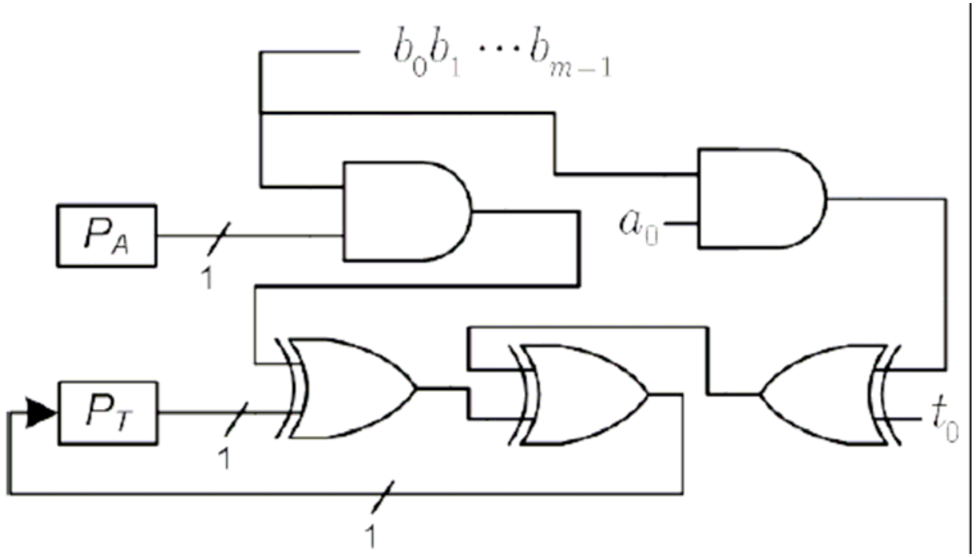
$2m-1$ AND gates and $2m-1$ XOR

New Parity-Based Fault Detection Scheme

Lemma 1: The parity of $T^{(i)}$ equals $P_{T^{(i-1)}} + b_i \cdot P_A + \mathrm{t}_0^{(\mathrm{i}-1)} + b_i \cdot a_0$, where $P_{T^{(i-1)}}$ is the parity of $T^{(i-1)}$, P_A is the parity of A, and $\mathrm{t}_0^{(\mathrm{i}-1)}$ is the LSB of $T^{(i-1)}$.

New Parity-Based Fault Detection Scheme

$$P_{T(i-1)} + b_i \cdot P_A + \mathrm{t}_0^{(\mathrm{i}-1)} + b_i \cdot a_0$$



delay of $T_A + 2T_X$

the latency of m

Arash Hariri and Arash Reyhani Masoleh
The University of Western Ontario, London, Ontario, Canada

Discussion and Comparison

- The time redundancy based scheme:
  - The original scheme

$$H \cdot x^m \bmod F(x).$$

taking into account that

$$x^m = f_{m-1}x^{m-1} + \cdots + f_1 x + 1$$

We have

$$H \cdot x^m = (h_{m-1}x^{m-1} + \cdots + h_1 x + h_0) \cdot (f_{m-1}x^{m-1} + \cdots + f_1 x + 1) \bmod F(x).$$

The area complexity of $O(m^2)$
The time complexity of $O(\log_2 m)$

Arash Hariri and Arash Reyhani Masoleh
The University of Western Ontario, London, Ontario, Canada

Discussion and Comparison

- Time redundancy based scheme:
  - The modified scheme

$$H \cdot x^{-1} = (h_{m-1}x^{m-1} + \cdots + h_1 x + h_0) \cdot x^{-1} \bmod F(x),$$

taking into account that

$$x^{-1} = x^{m-1} + f_{m-1}x^{m-2} \cdots + f_1,$$

We have

$$H \cdot x^{-1} = (h_0)\, x^{m-1} + (h_0 f_{m-1} + h_{m-1})\, x^{m-2} + \cdots + (h_0 \cdot f_1 + h_1)$$

The area complexity of $O(m)$

The constant time complexity of $T_A + T_X$

Discussion and Comparison

- Time parity based scheme:
  - The critical path delay $T_A + 2T_X$
  - The latency of m
    - ➢ Concurrent parity prediction
  - Three XOR gate and two AND gates (Constant)
  - Final XOR tree
    - The time complexity of $\lceil \log_2(m+1) \rceil \cdot T_X$
    - The area complexity of *m* XOR gates

Conclusions

- Two error detection schemes have been introduced:
  - Modification of an existing time redundancy based scheme for semi-systolic implementation of the Montgomery multiplication.
  - A new parity based scheme for the bit-serial Montgomery
- The time and complexity of the previous time redundancy based scheme is significantly improved. While it has the same error detection capability.
- The parity based scheme is capable of obtaining the parity of the intermediate and the final result without any time overhead and with a constant hardware overhead.

Thanks!