Error Detection in Polynomial Basis Multipliers over Binary Extension Fields

Arash Reyhani-Masoleh

&

Anwar Hasan

Centre for Applied Cryptographic Research,

University of Waterloo, Waterloo, Ontario, Canada

E-mails: areyhani@math.uwaterloo.ca

&

ahasan@ece.uwaterloo.ca

Outline

- Introduction
- PB Representation and multiplication over $GF(2^m)$
- Error Detection Strategy
- Parity Prediction Functions
- Error Detection in Bit-Parallel PB multiplier
- Error Detection in Bit-Serial PB Multiplier
- Conclusions

Introduction

- Finite field multiplier (FFM) is time consuming and costly
- FFM is extensively used in many cryptosystems
- There are different types of bases: polynomial basis (PB), normal basis, dual Basis, triangular basis
- The importance of detecting errors in cryptographic computations has been pointed out in some recent articles
- Previous research [Fenn 98] addresses only special case of AOP

PB Representation over $GF(2^m)$

- Let $F(z) = z^m + \sum_{i=0}^{m-1} f_i z^i$ be a monic irreducible polynomial over $GF(2)$
- Let $\alpha \in GF(2^m)$ be a root of $F(z)$, *i.e.*, $F(\alpha) = 0$.
- Then $\{1, \alpha, \alpha^2, \cdots, \alpha^{m-1}\}$ is known as PB
- Each element $A \in GF(2^m)$ can be written as

$$A = \sum_{i=0}^{m-1} a_i \alpha^i, \; a_i \in \{0, \; 1\}.$$

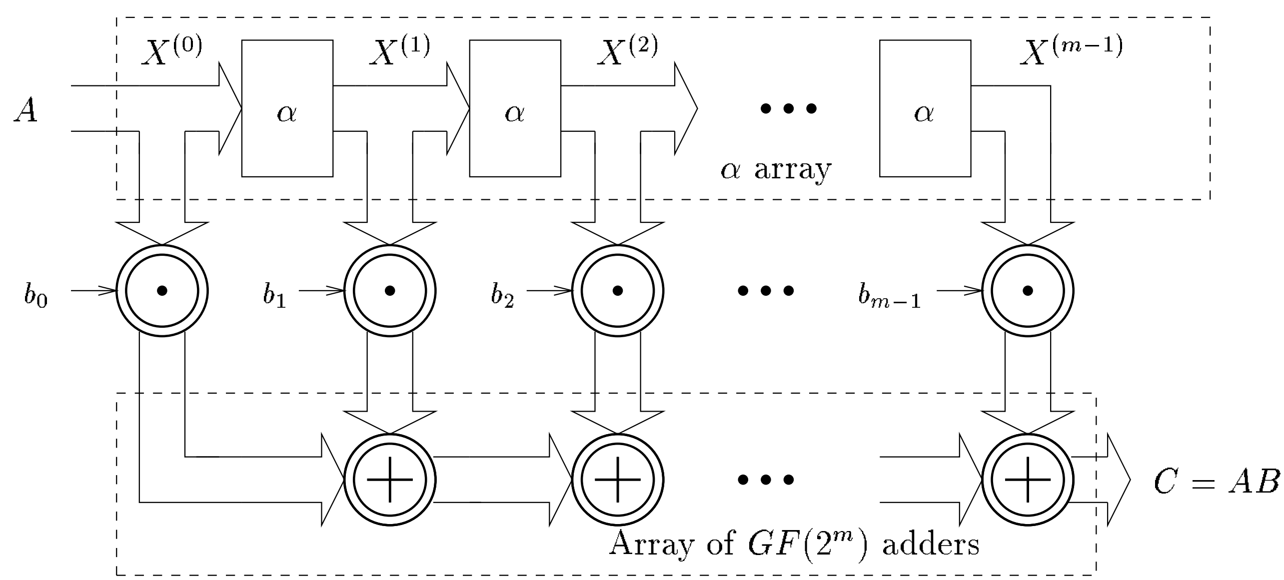
Multiplication Using PB

Let $A, B \in GF(2^m)$

$$
\begin{aligned}
C &= A \cdot B \mod F(\alpha) \\
&= \sum_{i=0}^{m-1} b_i \cdot ((A\alpha^i) \mod F(\alpha)) \\
&= \sum_{i=0}^{m-1} b_i \cdot X^{(i)},
\end{aligned}
$$

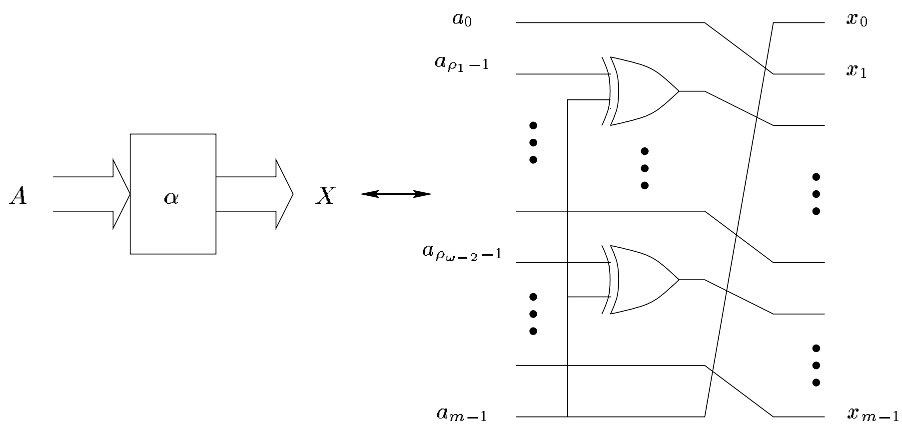
where $X^{(i)} = \alpha \cdot X^{(i-1)} \mod F(\alpha), \quad 1 \le i \le m-1$,

$X^{(0)} = A$.

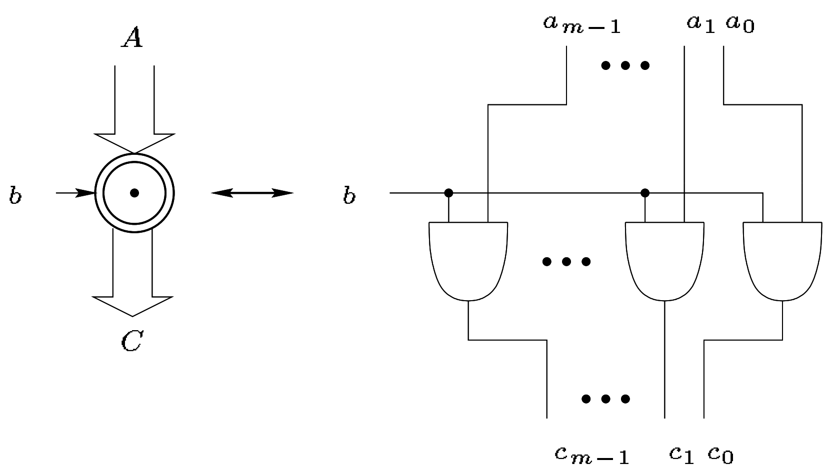


Three modules of the multiplier structure

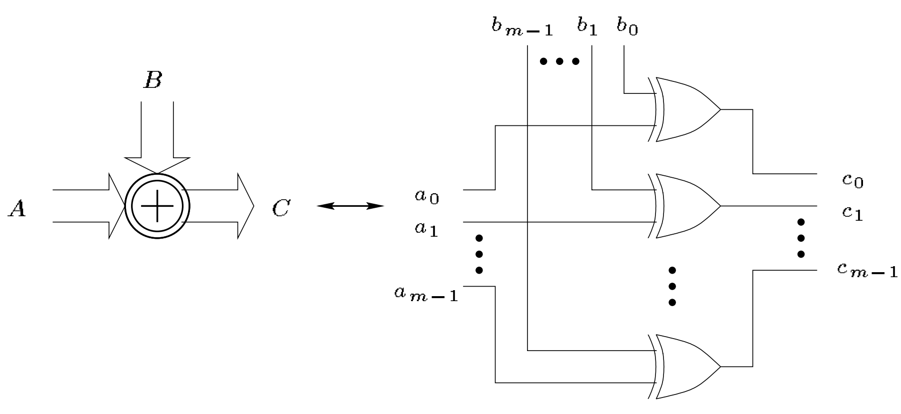
- α module



- Pass-thru module

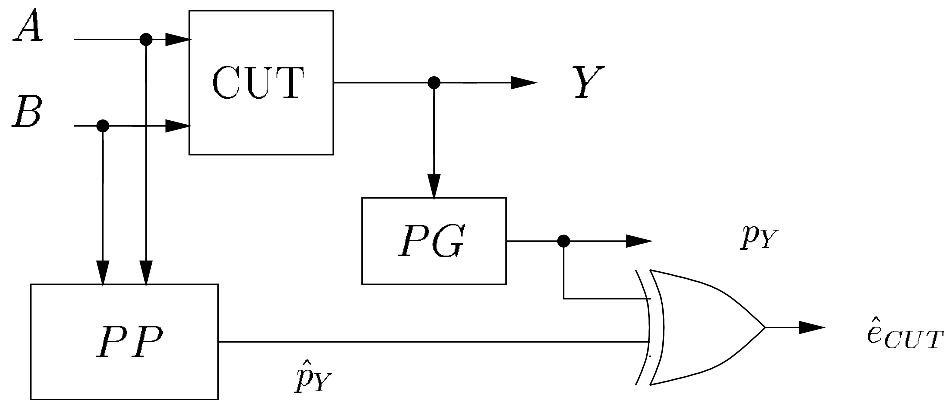


- Sum module



Error Detection Strategy

- Parity prediction (PP) method is used



- PP block predicts the parity of Y using a PP function $\hat{p}_Y = \Gamma_{\text{CUT}}(A, B)$.

- PG block generates the actual parity of Y, i.e., $p_Y = \sum_{i=0}^{m-1} y_i$

- p_Y and $\hat{p}_Y$ are compared, $\hat{e}_{\text{CUT}} = \begin{cases} 1 & \text{if error} \\ 0 & \text{otherwise} \end{cases}$

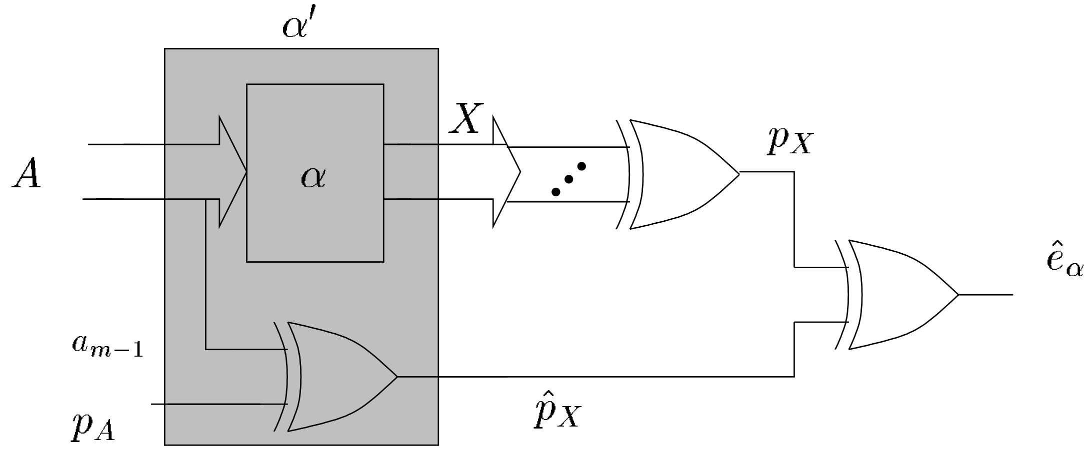
- Assumptions:
  - p_A and p_B are available
  - PP and PG blocks can be made fault free or detectable
  - A single stuck at fault model is used

Parity Predictions of Individual Modules

- **α module:**

$$\hat{p}_X = \Gamma_\alpha = p_A + a_{m-1}$$

where $X \triangleq A \cdot \alpha \bmod F(\alpha)$ is the output, $p_A \in GF(2)$



- **Pass-thru module:**

$$\hat{p}_G = \Gamma_{pass} = b \cdot p_A$$

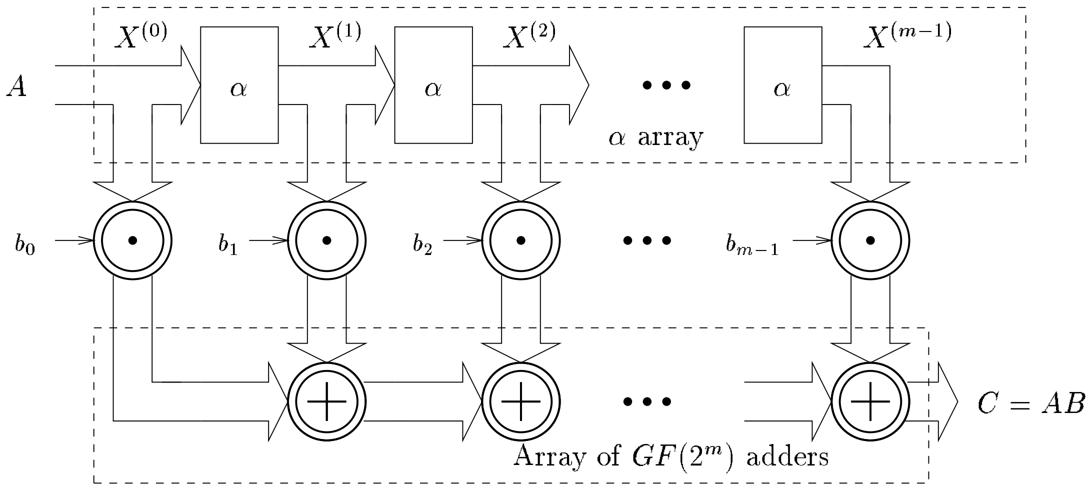
where $G = bA$, $b \in GF(2)$

- **Sum module:**

$$\hat{p}_D = \Gamma_{sum} = p_A + p_B$$

where $D = A + B$, and $p_A = \sum_{i=0}^{m-1} a_i$ is the parity bit for A

Parity Prediction of the PB multiplication



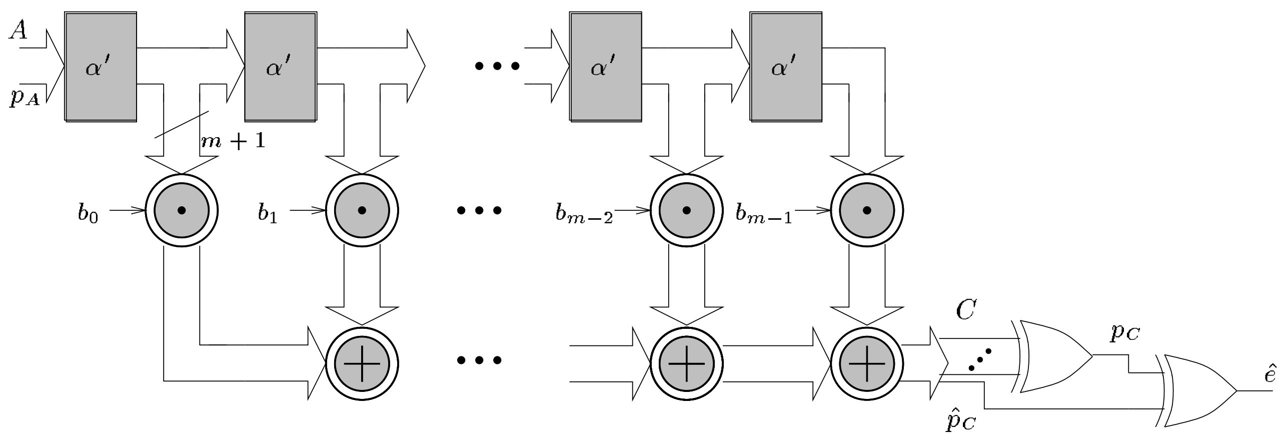
- Lemma: Let $x_{m-1}^{(j)}$ be the $(m-1)$-th coordinate of $X^{(j)} = A\alpha^j \mod F(\alpha)$

$$\hat{p}_{X^{(j)}} = p_A + \sum_{k=0}^{j-1} x_{m-1}^{(k)}, \qquad j = 1, 2, \cdots, m-1.$$

- Theorem: Let C be the product of two arbitrary elements A and B of $GF(2^m)$. Then

$$\hat{p}_C = \sum_{j=0}^{m-1} b_j \hat{p}_{X^{(j)}}.$$

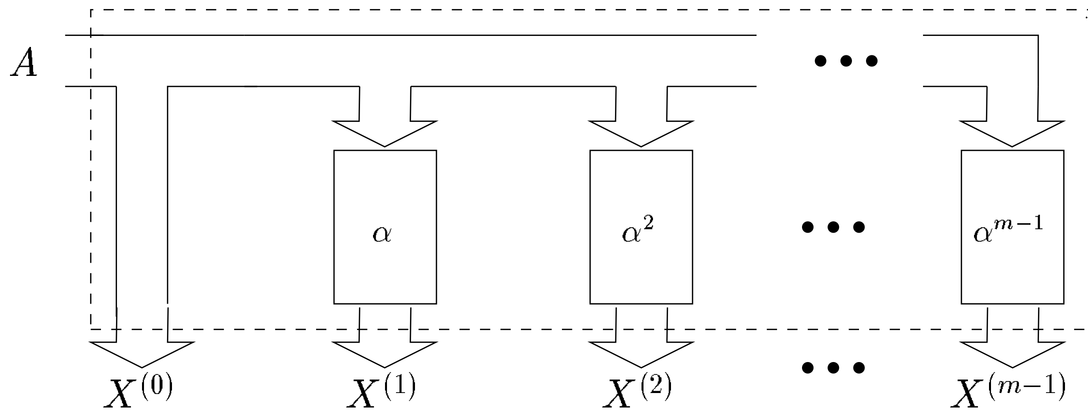
Error Detection in Bit-Parallel PB multiplier



- The output of any gate of the shaded pass-thru and sum modules in multiplier is connected to only one gate in the next stage
- The single stuck fault at any gate of two modules in multiplier changes only one coordinate of the output
- This multiplier however cannot detect a single stuck-at fault in α modules
- To overcome this problem, two methods are proposed.

Error Detection in α Modules

- New architecture of α array



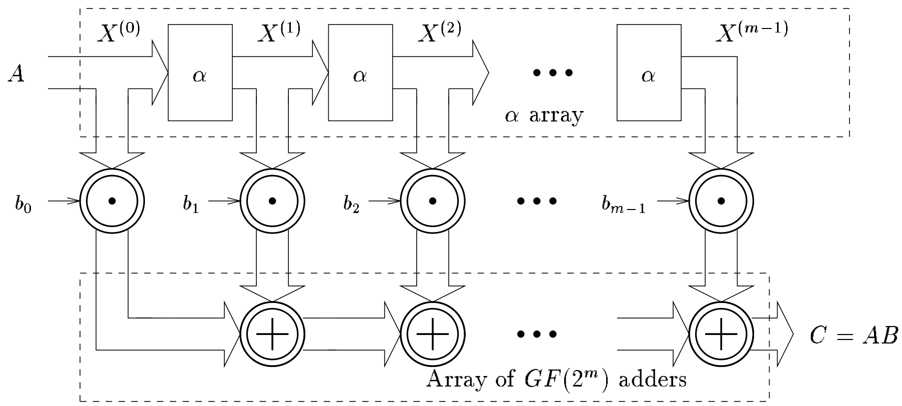
$$\mathbf{x}^{(i)} = \mathbf{G}^i \cdot \mathbf{a},\ 1 \le i \le m-1, \text{ where } \mathbf{G} = \begin{bmatrix} 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & \cdots & 0 & f_1 \\ 0 & 1 & \cdots & 0 & f_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & f_{m-1} \end{bmatrix}$$

- Error detection circuit of α array

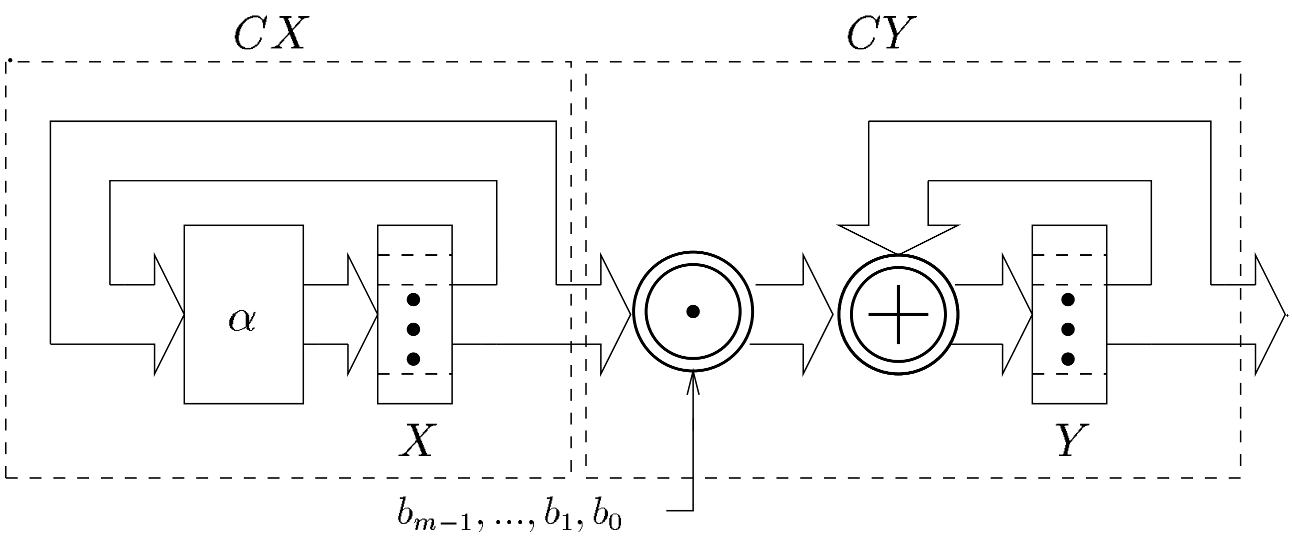
$$\hat{p}_{X^{(m-1)}} = p_A + \sum_{k=0}^{m-2} x_{m-1}^{(k)}.$$

Bit-Serial PB Multiplier

- Bit-Parallel:



- Bit-Serial:



- $X(0) = A$, $X(1) = X^{(1)} = \alpha A$, $X(m) = X^{(m)} = \alpha^m A$

- $Y(0) = 0$, $Y(1) = b_0 A$, ... $Y(m) = C = AB$

Error Detection in Bit-Serial PB Multiplier

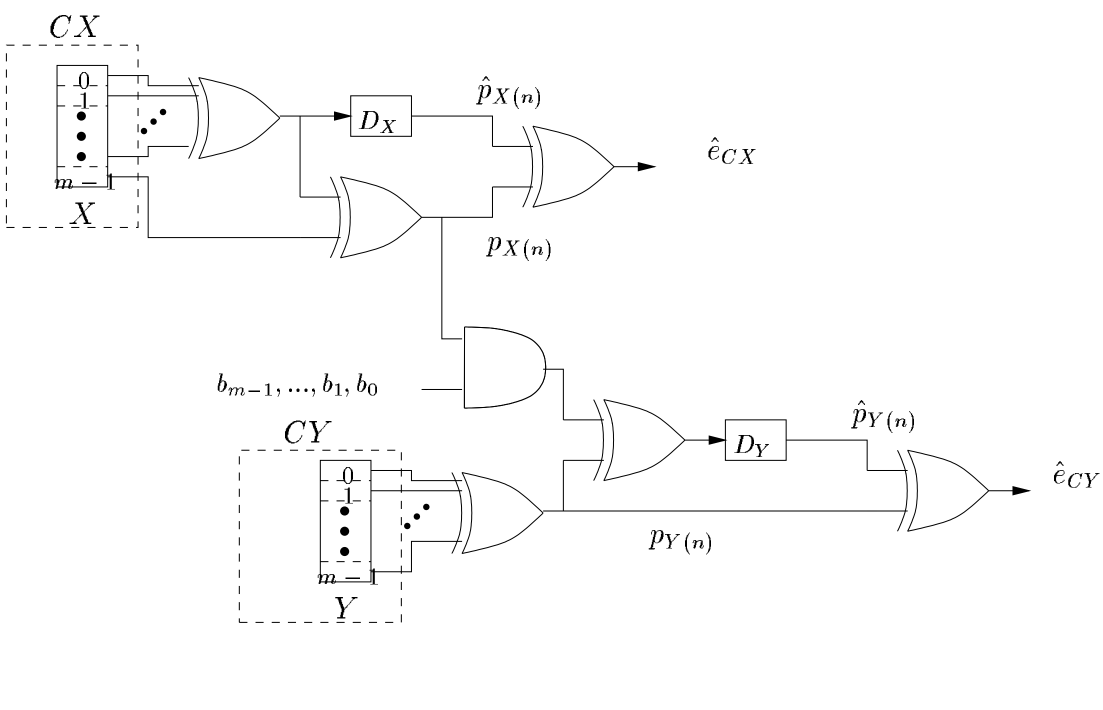
- PP method is used to check the contents of two registers in every clock cycle.
- For CX block:

$$\hat{p}_{X(n)} = \sum_{i=0}^{m-2} x_i(n-1),$$

where $x_i(n-1) \in GF(2)$ is the ith coordinate of $X(n-1)$.

- For CY block:

$$\hat{p}_{Y(n)} = p_{Y(n-1)} + b_{n-1} p_{X(n-1)}$$



- If there are no odd number of errors, after the first clock cycle, both $\hat{e}_{CX}$ and $\hat{e}_{CY}$ should be 0.

Conclusions

- Error detection in PB multipliers are considered
- A single stuck-at fault model is used
- The parity prediction functions of the individual modules and whole multiplier are obtained
- The work presented here is generic
- The probability of error detection of our bit-serial multiplier is about 100%
- More research is needed to reduce the overhead cost of the proposed multiplier.