On Low Complexity Bit Parallel Polynomial Basis Multipliers

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 over $GF(2^m)$
- Mastrovito multiplier over $GF(2^m)$
- New architecture based on reduction matrix
- Special cases (ESP, trinomial, pentanomial)
- Complexities and comparison
- 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

PB Representation over $GF(2^m)$

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

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

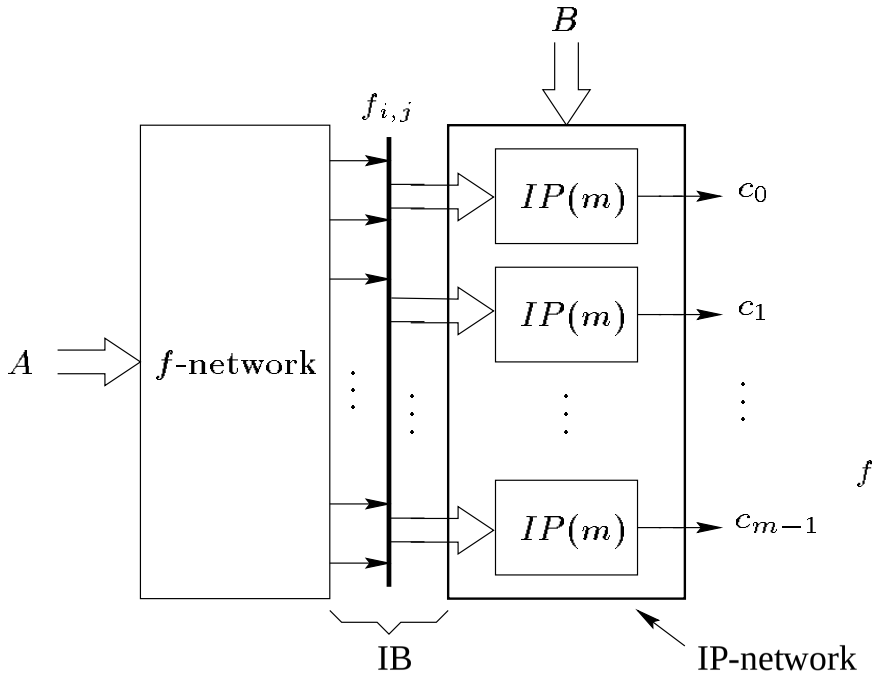
Mastrovito Multiplier over $GF(2^m)$

- The coordinates of the product $C = AB$ are calculated using

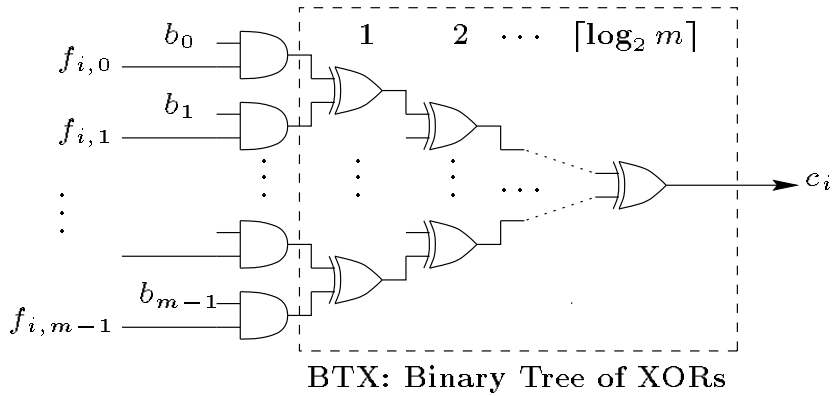
$$\mathbf{c} = \mathbf{F}\mathbf{b},$$

where $\mathbf{b} = [b_0, b_1, \cdots, b_{m-1}]^T$, $\mathbf{c} = [c_0, c_1, \cdots, c_{m-1}]^T$, and $\mathbf{F} = [f_{i,j}]_{i,j=0}^{m-1}$, $f_{i,j} \in GF(2)$

- The entries of $[f_{i,j}]$ depend on A and $P(x)$



(a)



(b)

$$[c_0,\, c_1,\, \cdots,\, c_{m-1}]^T = [f_{i,j}][b_0,\, b_1,\, \cdots,\, b_{m-1}]^T,$$

PB Multiplication over $GF(2^m)$

- Multiplication of any two elements A and B over $GF(2^m)$:
  - Polynomial multiplication

$$S = A \cdot B = \left(\sum_{i=0}^{m-1} a_i \alpha^i \right) \cdot \left(\sum_{j=0}^{m-1} b_j \alpha^j \right) = \sum_{k=0}^{m-1} d_k \alpha^k + \sum_{k=0}^{m-2} e_k \alpha^{m+k},$$

  - Modular reduction

$$C = \sum_{i=0}^{m-1} c_i \alpha^i \equiv S \mod P(\alpha).$$

New Formulation for PB Multiplication over $GF(2^m)$

Theorem: Let C be the product of A and $B \in GF(2^m)$. Then

$$\mathbf{c} = [c_0, c_1, \cdots, c_{m-1}]^T = \mathbf{d} + \mathbf{Q}^T \mathbf{e},$$

where $\mathbf{d} = [d_0, d_1, \cdots, d_{m-1}]^T$, $\mathbf{e} = [e_0, e_1, \cdots, e_{m-2}]^T$,

and the $m-1 \times m$ *reduction matrix* $\mathbf{Q} = [q_{i,j}]$, $q_{i,j} \in \{0, 1\}$, is

$$\begin{bmatrix} \alpha^m \\ \alpha^{m+1} \\ \vdots \\ \alpha^{2m-2} \end{bmatrix} \equiv \mathbf{Q} \begin{bmatrix} 1 \\ \alpha \\ \vdots \\ \alpha^{m-1} \end{bmatrix} \pmod{P(\alpha)}.$$

New Architecture of PB Multiplier over $GF(2^m)$

- IP-network:

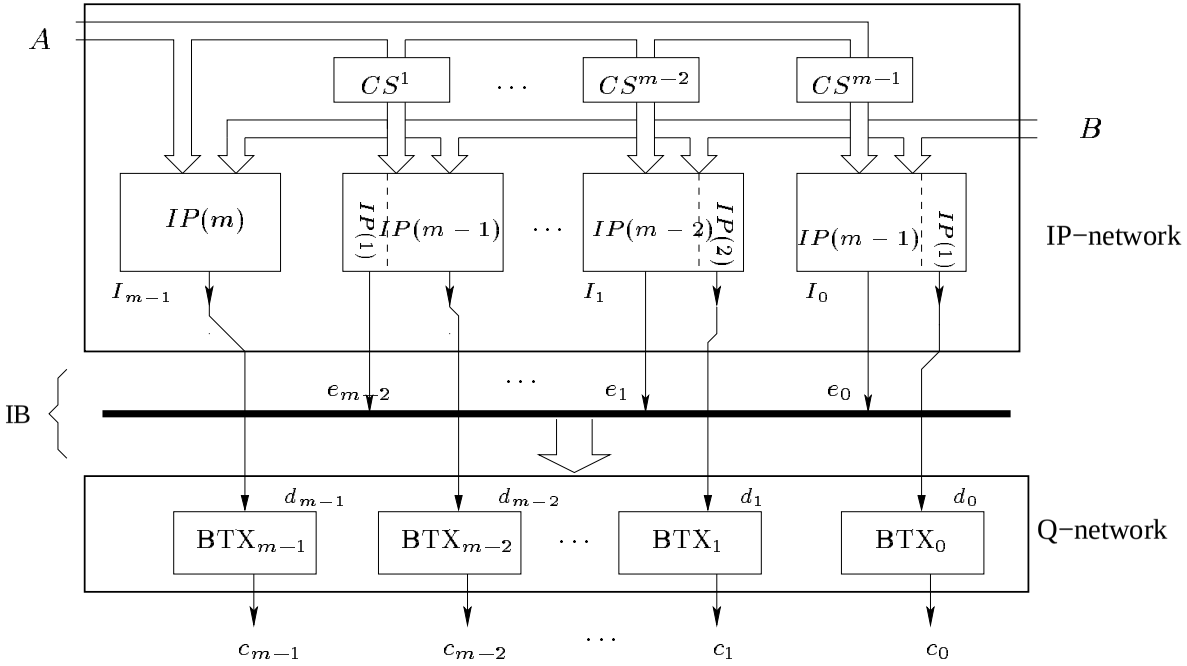
  m^2 AND gates &

  $(m-1)^2$ XOR gates

- $\mathbf{Q}-$network:

  at most

  $H(\mathbf{Q})$ XOR gates

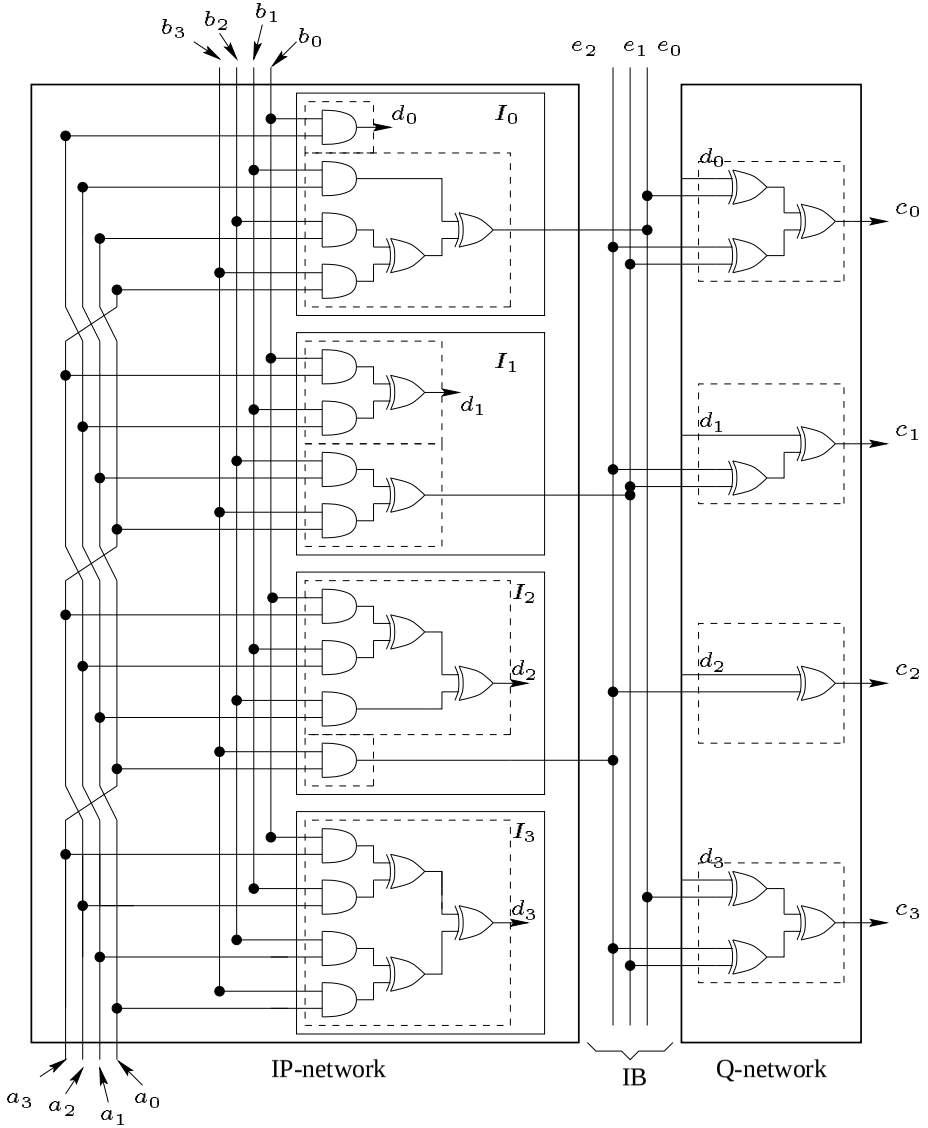


- $IP(i)$, $1 \leq i \leq m$, is the inner product of two vectors with i elements
- BTX_j, $0 \leq j \leq m-1$, is the binary tree of XOR gates corresponds to $j-$th colomn of $\mathbf{Q}$

An Example over $GF(2^4)$

- $P(x) = x^4 + x^3 + 1$
- $\mathbf{Q} = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix}$
- $\mathbf{c} = \mathbf{d} + \mathbf{Q}^T\mathbf{e}$

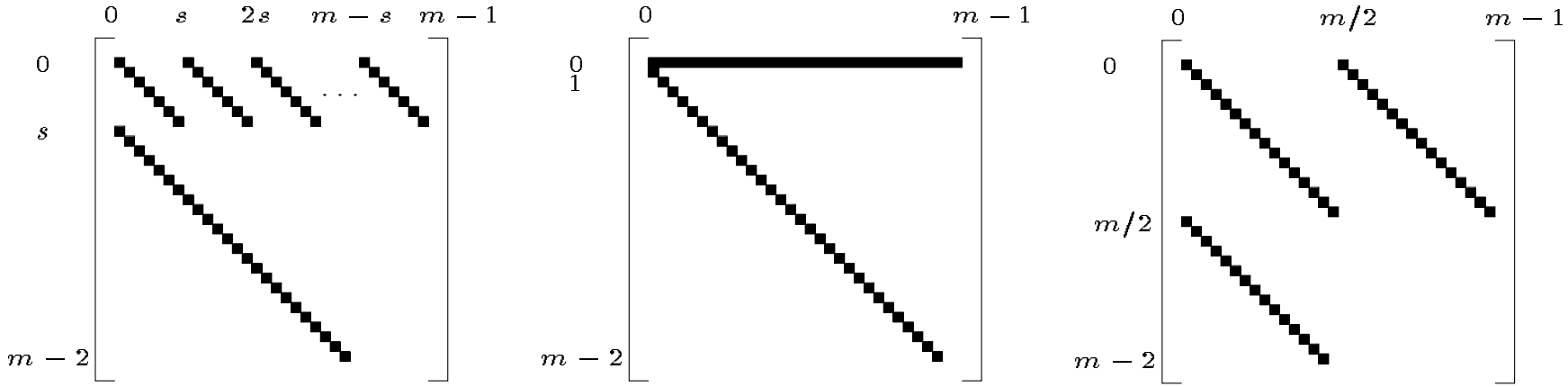
$$
\begin{aligned}
c_0 &= d_0 + [e_0 + (e_1 + e_2)] \\
c_1 &= d_1 + (e_1 + e_2) \\
c_2 &= d_2 + e_2 \\
c_3 &= d_3 + [e_0 + (e_1 + e_2)]
\end{aligned}
$$



- # XOR gates in $\mathbf{Q}-$network can be reduced by reusing common terms

Reduction Matrix for Equally-Spaced Polynomials

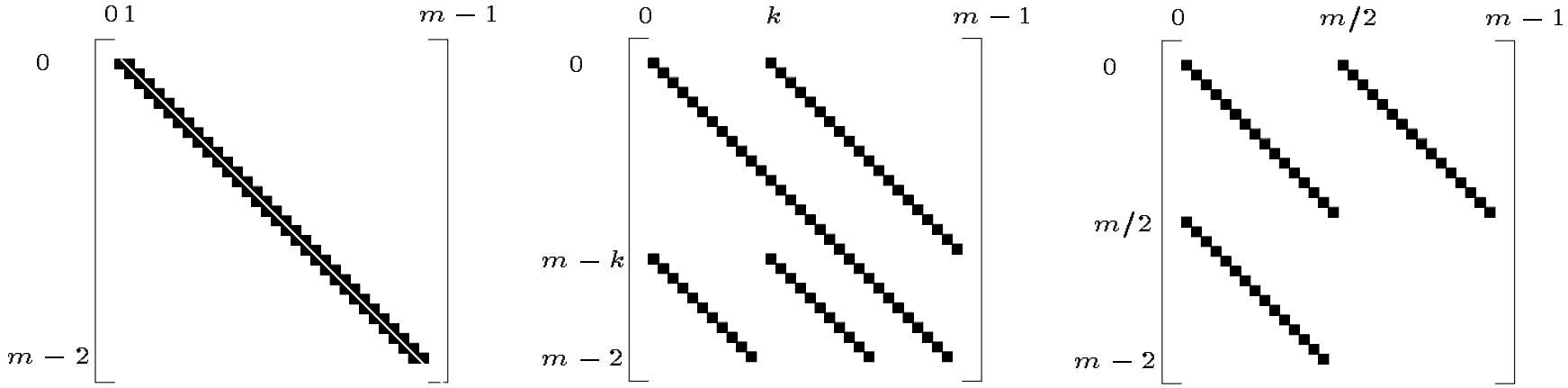
- A polynomial $P(x) = x^{ns} + x^{(n-1)s} + \cdots + x^s + 1$, over $GF(2)$, with $ns = m$, is called s-ESP of degree m.



$1 < s < \frac{m}{2}$ $\qquad$ $s = 1$ (AOP) $\qquad$ $s = \frac{m}{2}$ (Trinomial)

- There is no common term in $\mathbf{Q}$ and $H(\mathbf{Q}) = 2m - s - 1$
- Thus, #XOR gates$=(m-1)^2 + H(\mathbf{Q}) = m^2 - s$

Reduction Matrix for Trinomial $P(x) = x^m + x^k + 1$

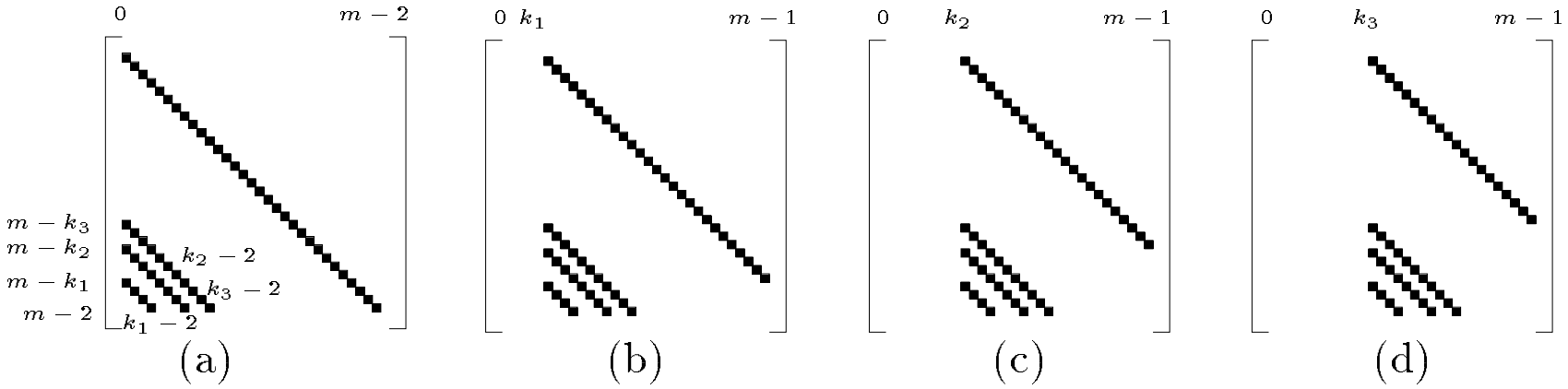


$k = 1$ $\qquad$ $1 < k < \frac{m}{2}$ $\qquad$ $k = \frac{m}{2}$

- There is no common term in $\mathbf{Q}$ for $k = 1$ $(H(\mathbf{Q}) = 2m - 1)$ and $k = \frac{m}{2}$ $(H(\mathbf{Q}) = 1.5m - 1)$
- There are common terms in $\mathbf{Q}$ for $1 < k < \frac{m}{2}$

Class 1-Pentanomial

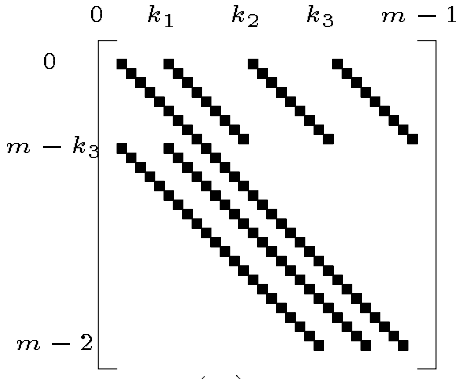
- $P(x) = x^m + x^{k_3} + x^{k_2} + x^{k_1} + 1, 1 \leq k_1 < k_2 < k_3 \leq \frac{m}{2}$
- $\mathbf{Q} = \mathbf{Q}_a + \mathbf{Q}_b + \mathbf{Q}_c + \mathbf{Q}_d$, $\mathbf{c} = \mathbf{d} + \mathbf{Q}^T\mathbf{e}$



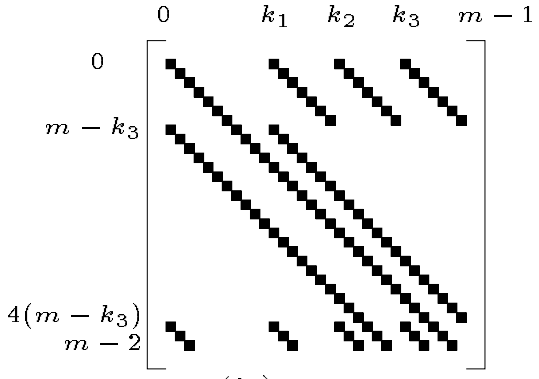
- $\mathbf{Q}_a^T\mathbf{e}$ can be reused to obtain $\mathbf{Q}_b^T\mathbf{e}$, $\mathbf{Q}_c^T\mathbf{e}$, and $\mathbf{Q}_d^T\mathbf{e}$
- If $k_1 = k_3 - k_2$, then $(\mathbf{Q}_c + \mathbf{Q}_d)^T\mathbf{e}$ can also be obtained from $(\mathbf{Q}_a + \mathbf{Q}_b)^T\mathbf{e}$

Class 2-Pentanomial

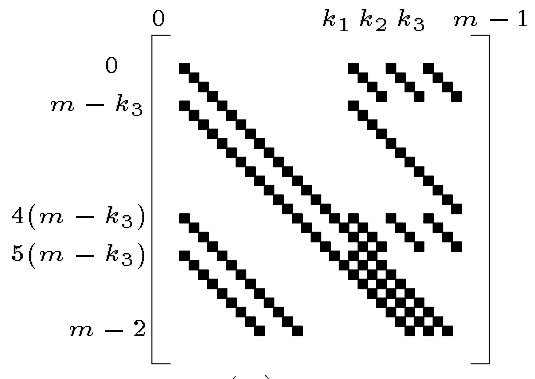
- $P(x) = x^m + x^{m-s} + x^{m-2s} + x^{m-3s} + 1,$



(a)



(b)



(c)

$\frac{m-1}{4} \leq s \leq \frac{m-1}{3}$ $\quad$ $\frac{m-1}{5} \leq s < \frac{m-1}{4}$ $\quad$ $\frac{m-1}{8} \leq s < \frac{m-1}{5}$

- $k_1 = m - 3s$, $k_2 = m - 2s$, and $k_3 = m - 3s$

Comparison in Term of # XOR and delay

Reference	Special Case	#XOR	Time delay
$P(x) = x^m + x^{k_3} + x^{k_2} + x^{k_1} + 1,\ 1 < k_1 < k_2 < k_3 \leq \frac{m}{2}$			
[11]	$k_1 \geq 1$	$m^2 + 2m - 3$	$T_A + (6 + \lceil \log_2 m \rceil)\, T_X$
This paper	$k_1 > 1$	$m^2 + 2m - 3$	$T_A + (4 + \lceil \log_2 (m-1) \rceil)\, T_X$
This paper	$k_1 = 1$	$m^2 + 2m - 3$	$T_A + (3 + \lceil \log_2 (m-1) \rceil)\, T_X$
This paper	$k_3 - k_2 = k_1$	$m^2 + m + k_1 - 2$	$T_A + (4 + \lceil \log_2 (m-1) \rceil)\, T_X$
[7]	$k_3 - k_2 = k_1 = 1$	$m^2 + m + 2k_2$	$T_A + (3 + \lceil \log_2 (m-1) \rceil)\, T_X$
This paper	$k_3 - k_2 = k_1 = 1$	$m^2 + m$	$T_A + (3 + \lceil \log_2 (m-1) \rceil)\, T_X$
This paper,[7]	$k_i = i$	$m^2 + m$	$T_A + (3 + \lceil \log_2 (m-1) \rceil)\, T_X$
$P(x) = x^m + x^{m-s} + x^{m-2s} + x^{m-3s} + 1$			
[11]	$1 \leq s \leq \frac{m-1}{3}$	$m^2 + 4m - 5s - 5$	$T_A + \left(\lfloor \frac{d}{4} \rfloor + 4 + \lceil \log_2 (m-1) \rceil \right) T_X$
[11]	$s \leq \frac{m-1}{3}$	$\geq m^2 + 2.33m - 7$	$\geq T_A + (4 + \lceil \log_2 (m-1) \rceil)\, T_X$
This paper	$\frac{m-1}{8} \leq s \leq \frac{m-1}{3}$	$\leq m^2 + m$	$\leq T_A + (4 + \lceil \log_2 (m-1) \rceil)\, T_X$

Conclusions

- A new efficient architecture for PB multiplier over $GF(2^m)$ has been proposed.
- Also, we have considered time and space complexities of this architecture.
- Our results for the ESPs and trinomials ($k \neq 1$) match the corresponding best results available
- For trinomial $x^m + x + 1$, the multiplier has one additional XOR gate delay compared to the best one available in the literature
- For class 1 pentanomials, this multiplier is faster than the Mastrovito multiplier and has fewer XOR gates if the special case of $k_3 - k_2 = k_1$ is used.

- Also, for class 2 pentanomials, our multiplier is either faster or has the same gate delay and has at least $1.33m - 7$ fewer XOR gates
- Moreover, the architectures discussed here have fewer number of lines on the buses compared to the well known Mastrovito multiplier

References

[1] G. B. Agnew, R. C. Mullin, and S. A. Vanstone. "An Implementation of Elliptic Curve Cryptosystems Over $F_{2^{155}}$". *IEEE J. Selected Areas in Communications*, 11(5):804–813, June 1993.

[2] A. Halbutogullari and C. K. Koc. "Mastrovito Multiplier for General Irreducible Polynomials". *IEEE Transactions on Computers*, 49(5):503–518, May 2000.

[3] E. D. Mastrovito. "VLSI Designs for Multiplication over Finite Fields $GF(2^m)$". In *LNCS-357, Proc. AAECC-6*, pages 297–309, Rome, July 1988. Springer-Verlag.

[4] E. D. Mastrovito. *VLSI Architectures for Computation in Galois Fields*. PhD thesis, Linkoping Univ., Linkoping Sweden, 1991.

[5] A. J. Menezes, I. F. Blake, X. Gao, R. C. Mullin, S. A. Vanstone, and T. Yaghoobian. *Applications of Finite Fields*. Kluwer Academic Publishers, 1993.

[6] A. Reyhani-Masoleh and M. A. Hasan. "A New Efficient Architecture of Mastrovito Multiplier over $GF(2^m)$". In 20^{th} *Biennial Symposium on Communications*, pages 59–63, Kingston, Ontario, Canada, May 2000.

[7] F. Rodriguez-Henriquez and C. K. Koc. "Parallel Multipliers Based on Special Irreducible Pentanomials". *IEEE Transactions on Computers*, to appear, 2003, available at http://islab.oregonstate.edu/koc/Publications.html.

[8] L. Song and K. K. Parhi. "Low Complexity Modified Mastrovito Multipliers over Finite Fields $GF(2^M)$". In *ISCAS-99, Proc. IEEE International Symposium on Circuits and Systems*, pages 508–512, 1999.

[9] B. Sunar and C. K. Koc. "Mastrovito Multiplier for All Trinomials". *IEEE Transactions on Computers*, 48(5):522–527, May 1999.

[10] H. Wu. "Bit-Parallel Finite Field Multiplier and Squarer Using Polynomial Basis". *IEEE Transactions on Computers*, 51(7):750–758, July 2002.

[11] T. Zhang and K. K. Parhi. "Systematic Design of Original and Modified Mastrovito Multipliers for General Irreducible Polynomials". *IEEE Transactions on Computers*, 50(7):734–748, July 2001.