

A Study on Constructing the Inverse Element Generator over $GF(3^m)$

Chun-Myoung Park, *Member, KIMICS*

Abstract—This paper presents an algorithm generating inverse element over finite fields $GF(3^m)$, and constructing method of inverse element generator based on inverse element generating algorithm. An inverse computing method of an element over $GF(3^m)$ which corresponds to a polynomial over $GF(3^m)$ with order less than equal to $m-1$. Here, the computation is based on multiplication, square and cube method derived from the mathematics properties over finite fields.

Index Terms— finite fields, irreducible polynomial, arithmetic operation, inverse element.

I. INTRODUCTION

In recently, many digital logic system and computer systems are required to process more data and high efficiency.^[1-4] Specially arithmetic relation is require more high speed and efficiency. The advanced arithmetic operation is analyzed easily using by finite fields.^[5-8]

In this paper, we propose the high efficiency inverse element generator over finite fields.

This paper's organization is as following. In Section 2, we propose the multiplication, square and cube algorithm based on finite field mathematical properties. In section 3, we discuss of inverse element generation algorithm over $GF(3^m)$. And in section 4, we construct an inverse element generator based on section 3's algorithm. Finally in section 5, we summary our inverse element generator over finite fields, also we prospect future research fields.

II. MULTIPLICATION, SQUARE AND CUBE ALGORITHM OVER FINITE FIELDS

2.1. Mathematical Properties of Finite Fields

In this section, we review the important mathematical properties of finite fields, these mathematical properties used in build up this paper.

Any other mathematical properties except these mathematical properties refer to references^[9-12].

Finite fields is defined by any prime number P and integer m , namely $GF(P^m)$. In generally finite fields is organized by 5-tuple $\{S, +, \cdot, 0, 1\}$, where S is set of elements, $+$ and \cdot are binary operation over S , 0 and 1 are each identity element for addition and multiplication arithmetic operation.

Also finite fields are classified into ground fields $GF(P)$ and extension fields $GF(P^m)$.

The number of elements over ground fields $GF(P)$, P is the prime number more than 1, are $\{0, 1, 2, \dots, P-1\}$.

The important mathematical properties over finite fields are as following.

[MP1] for $\alpha \in GF(P^m)$, $\alpha^\psi = \alpha$ and $\alpha^{\psi-1} = 1$ ($\psi = P^m$) in case of $\alpha \neq 1$.

[MP2] for $\alpha, \beta \in GF(P^m)$ and arbitrary integer m , $(\alpha \pm \beta)^\mu = \alpha^\mu \pm \beta^\mu$ ($\mu = P^m$)

[MP3] for $\alpha \in GF(P^m)$, $\alpha^i \bullet \alpha^j = \alpha^{i+j(\text{mod } \psi-1)}$ ($\psi = P^m$)

[MP4] The elements in $GF(P^m)$ are represented by

$$F(\alpha) = \sum_{i=0}^{m-1} a_i \alpha^i, \text{ where } \alpha \text{ is root, that is, } \alpha \text{ have coefficient}$$

that have element for integer field Z_p that have mod P , where m degree primitive irreducible polynomial $F(X) = X^m + f_{m-1}X^{m-1} + f_{m-2}X^{m-2} + \dots + f_1X + f_0$, $a_i \in Z_p (i=0, 1, 2, \dots, m-1)$ and $f_0 \neq 0$.

2.2. Algorithm of multiplication and square over $GF(3^m)$

$GF(3^m)$ have 3^m elements and we represented this with set is as following expression (1).

$$GF(3^m) = \{0, \alpha, \alpha^2, \dots, \alpha^{\psi-2} = \alpha^{-1}, \alpha^{\psi-1} = 1\} \quad (1)$$

where, $\psi = 3^m$.

Then, for more than m degree term, we can represent degree $m-1$ polynomial using mod $F(X)$ arithmetic that used by primitive polynomial $F(X)$.

Therefore arbitrary element over $GF(3^m)$ can represent as following.

$$F(X) = a_{m-1}X^{m-1} + a_{m-2}X^{m-2} + \dots + a_1X + a_0 = \sum_{i=0}^{m-1} a_i X^i \quad (2)$$

where, $a_i \in GF(3)$ and $i=0, 1, 2, \dots, m-1$.

On the other hand, α is a root of primitive polynomial, therefore α^m is equal to following equation (3), where $+$ is

Manuscript received May 14, 2010; revised May 16, 2010; accepted May 31, 2010.

Chun-Myoung Park is with the Department of Computer Engineering, Chungju National University, Chungju, 380-702, Korea (Email: cmpark@cju.ac.kr)

mod3.

$$\begin{aligned} \alpha^m + a_{m-1}\alpha^{m-1} + \dots + a_1\alpha + a_0 &= 0 \\ \alpha^m &= -a_{m-1}\alpha^{m-1} - a_{m-2}\alpha^{m-2} - \dots - a_1\alpha - a_0 \\ \alpha^m &= (3 - a_{m-1})\alpha^{m-1} + (3 - a_{m-2})\alpha^{m-2} + \dots + (3 - a_1)\alpha + (3 - a_0) \end{aligned} \tag{3}$$

Therefore, we can represent element over GF(3^m) into polynomial α of maximum m-1 degree, it is as following.

$$\text{GF}(3^m) = \{a_{m-1}\alpha^{m-1} + a_{m-2}\alpha^{m-2} + \dots + a_1\alpha + a_0\}$$

where, $a_i \in \text{GF}(3)$ and $i=0,1,2, \dots, m-1$.

$$\text{For two elements over GF}(3^m), e_1 = \sum_{i=0}^{m-1} a_i \alpha^i, e_2 = \sum_{i=0}^{m-1} b_i \alpha^i,$$

$e_1 \bullet e_2$ is represented as following.

$$e_1 \bullet e_2 = \sum_{i=m-1}^0 P_i \alpha^i + \sum_{i=2m-2}^m P_i \alpha^i \tag{4}$$

We consecutive multiply expression (4), generate maximum degree α^{2m-2} , we mod F(X) from α^{2m-2} to α^m , we can obtain following expression.

$$e_1 \bullet e_2 = \sum_{i=m-1}^0 R_i \alpha^i \tag{5}$$

where, multiplication and addition are mod3 product and mod3 addition.

In case of square, e_1 equal e_2 , expression (5) is represented by expression (6).

$$e_1^2 = e_1 \bullet e_1 = e_1 \bullet e_2 = \sum_{i=0}^{m-1} R_i \alpha^i \tag{6}$$

Therefore, we can use construct the square generator using multiplier.

2.3. Method of cube multiplication over GF(3^m)

According to mathematical properties [MP2], $(a+b)^3 = a^3 + b^3$, and $a^3 = a, b^3 = b$.

Therefore, cube for anyone element e over GF(3^m) is represented by equation (7)

$$e^3 = e = \sum_{j=3m-3}^0 P_j \alpha^j \tag{7}$$

where, $P_j = a_j$ in case of $j=3i, P_j=0$ in case of $j=3i+1$ and $j=3i+2$, and $i=0,1, \dots, m-1$.

That reason is as following.

$$\begin{aligned} e^3 &= e = (a_{m-1}\alpha^{m-1} + a_{m-2}\alpha^{m-2} + \dots + a_1\alpha + a_0)^3 \\ &= a_{m-1}^3 \alpha^{3m-3} + a_{m-2}^3 \alpha^{3m-6} + \dots + a_1^3 \alpha^3 + a_0^3 \\ &= a_{m-1} \alpha^{3m-3} + a_{m-2} \alpha^{3m-6} + \dots + a_1 \alpha^3 + a_0 \end{aligned}$$

For example, we obtain cube for any element over GF(3⁴). Let any element over GF(3⁴) is e, we can represent it as following.

$$e = a_3 \alpha^3 + a_2 \alpha^2 + a_1 \alpha + a_0$$

where, $a_i \in \text{GF}(3)$ and $i=0,1,2$

Next, we select $F(X) = X^4 + X + 2$ for polynomial F(X). And, we obtain cube as following.

$$\begin{aligned} e &= (a_3 \alpha^3 + a_2 \alpha^2 + a_1 \alpha + a_0)^3 \\ &= a_3 \alpha^9 + a_2 \alpha^6 + a_1 \alpha^3 + a_0 \end{aligned}$$

On the other hand, $F(\alpha) = \alpha^4 + \alpha + 2$, therefore $\alpha^4 = \alpha + 2$, then $\alpha^6 = 2\alpha^3 + \alpha^2$ and $\alpha^9 = \alpha^3 + \alpha^2 + \alpha$. Finally, we represent e as following.

$$e = (a_3 + 2a_2 + a_1)\alpha^3 + (a_0 + a_2 + a_1)\alpha^2 + a_3\alpha + a_0$$

III. ALGORITHM OF INVERSE ELEMENT GENERATION

In this section, we discuss algorithm of inverse element generation over GF(3^m).

Let e is any one element over GF(3^m), then its inverse element e⁻¹ is as following equation(1).

$$e^{-1} = e^{\Psi-2} \tag{1}$$

where, $\Psi = a^m$

Also, above inverse element is represented by triple product of 3.

$$e^{-1} = e \bullet (e^2)^{\Omega_1} \bullet (e^2)^{\Omega_2} \bullet (e^2)^{\Omega_3} \bullet \dots \bullet (e^2)^{\Omega_{m-1}}$$

where, $\Omega_1=3, \Omega_2=3^2, \Omega_3=3^3, \dots, \Omega_{m-1}=3^{m-1}$

The following is algorithm of inverse element generation over GF(3^m), and the fig. 3-1 depicted algorithm.

[Algorithm]

- STEP 1 : Accept any element e over GF(3^m).
- STEP 2 : Obtain result for power of element e.
- STEP 3 : Cube product result after Step2 or Step 5.
- STEP 4 : If it (m-1) times triple product do, go to Step 6.
- STEP 5 : Product result of Step 3 with e, then go to Step 3.
- STEP 6 : Product result of Step 4 with e.
- STEP 7 : The inverse element e⁻¹ is result of Step 6.

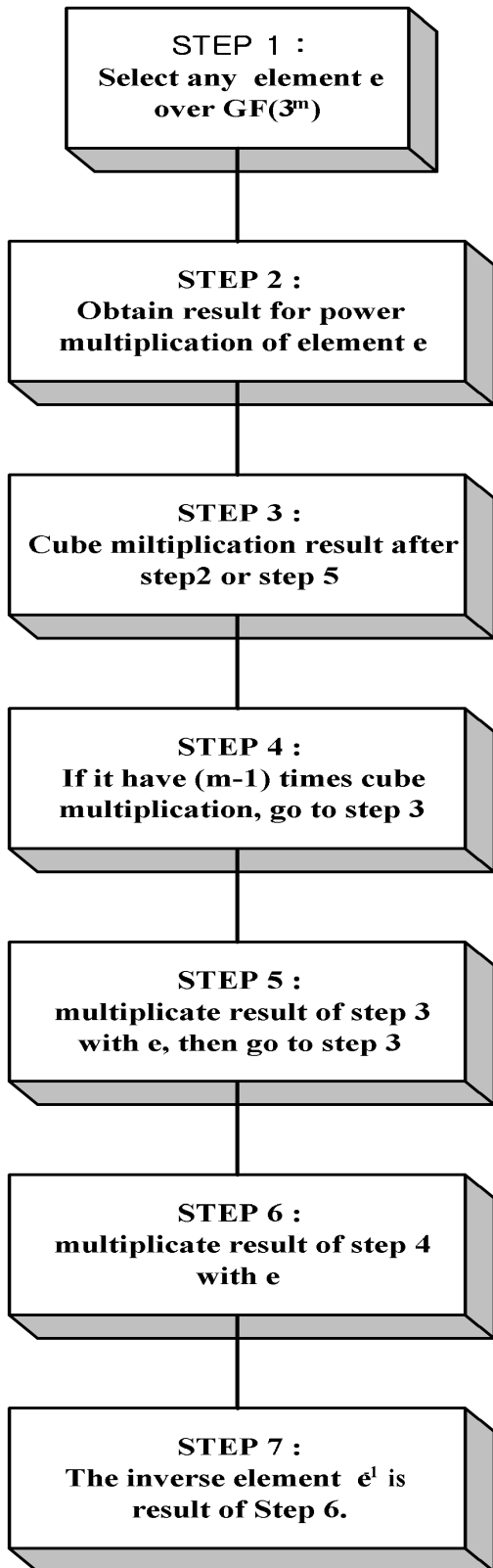


Fig. 1. The block diagram of Inverse element generation over $GF(3^m)$

IV. UNIVERSAL INVERSE ELEMENT GENERATOR

In this section, we discuss constructing the universal inverse element generator over $GF(3^m)$.

The block diagram of universal inverse element generator over $GF(3^m)$ is as following fig. 1.

As shown fig. 2, the universal inverse element generator was constructed with multiplier, square multiplier, cube multiplier.

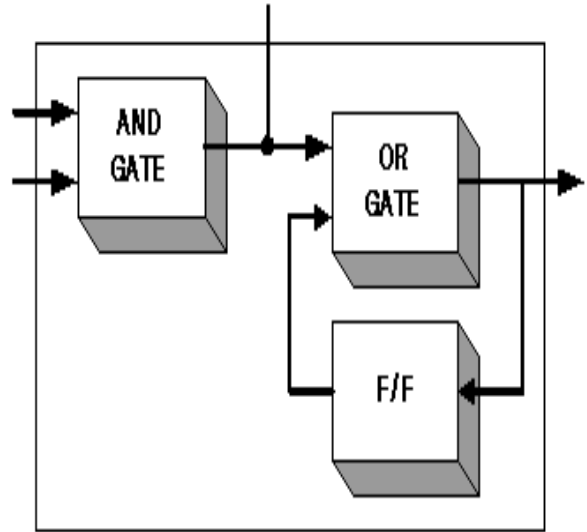
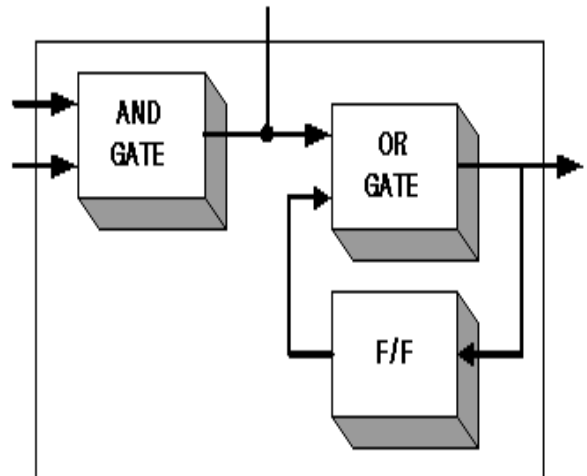
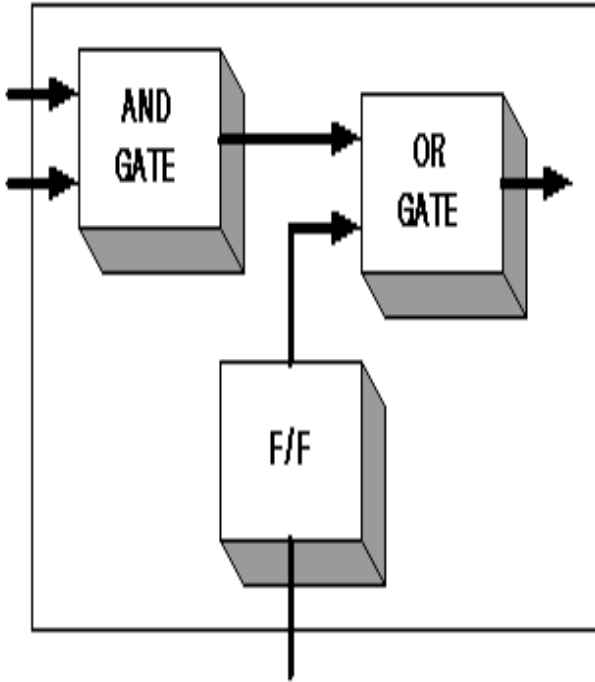


Fig. 2. Block diagram of universal inverse element generator over $GF(3^m)$

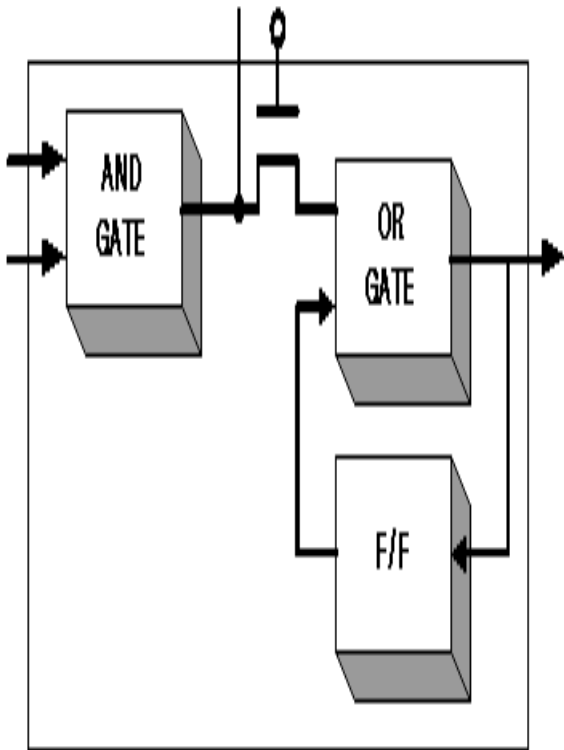
Also, the cell of multiplier, square multiplier and cube multiplier are fig.3 (a), fig.3 (b) and fig. 3 (c).



(a) Cell of multiplier



(b) Cell of square multiplier



(c) Cell of cube multiplier

The multiplier over $GF(3^m)$ is shown in fig. 4.

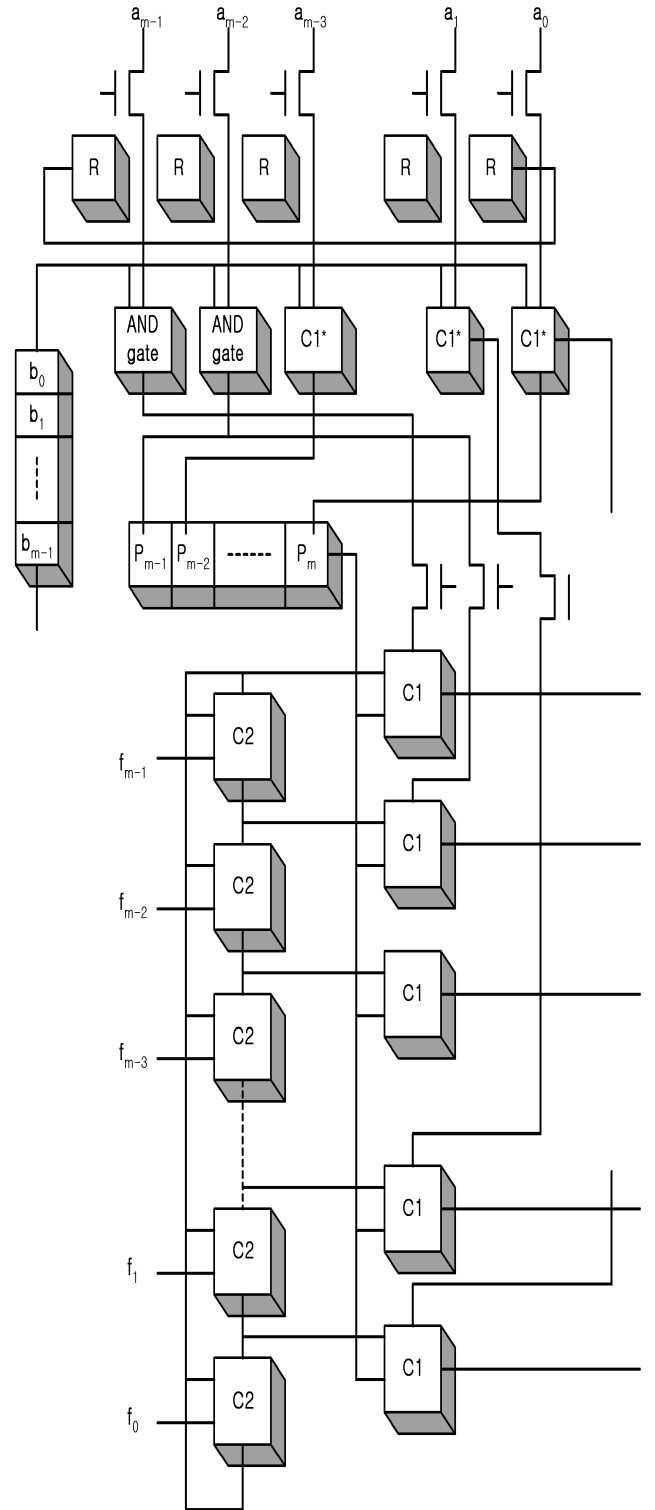


Fig. 4. Block diagram of multiplier over $GF(3^m)$

Fig. 3. Each cell of universal inverse element generator over $GF(3^m)$

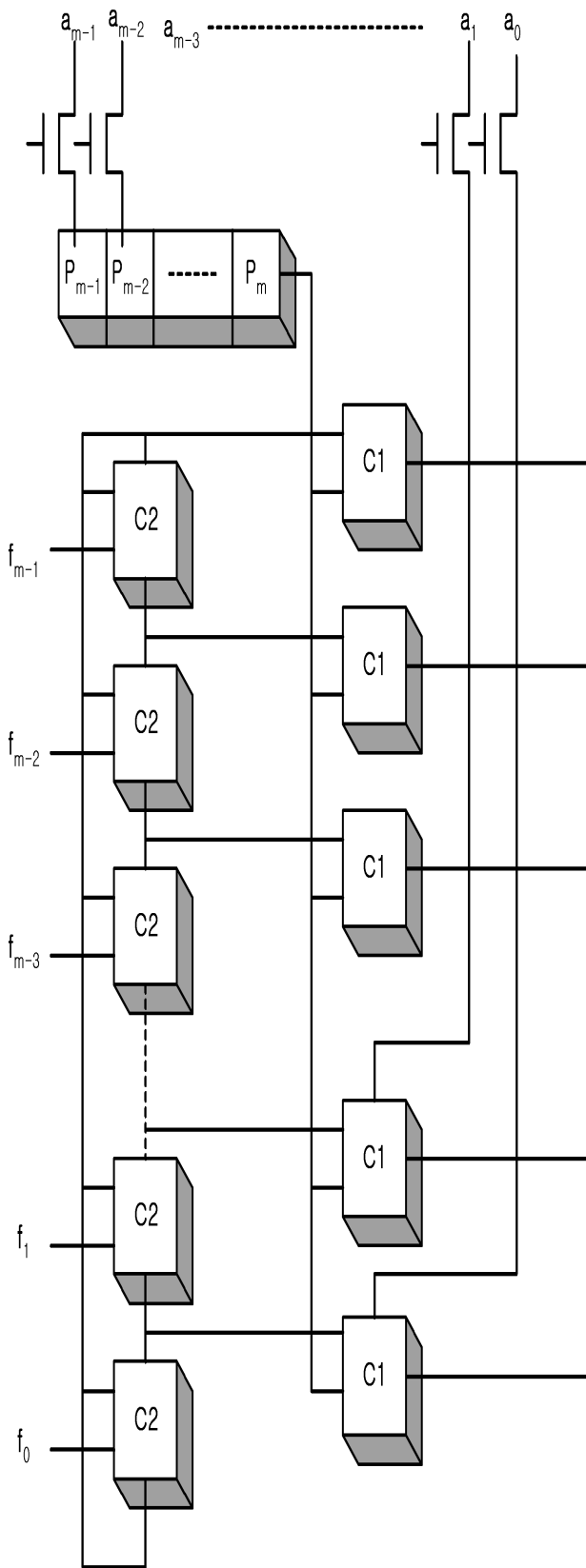


Fig. 5. Block diagram of cube multiplier over $GF(3^m)$

The multiplier's characteristics don't change according to increase m or changing irreducible polynomial.

Also, if two input of multiplier, then multiplier is square multiplier.

The cube multiplier is shown as fig.5.

In fig.5, the cube multiplier's basic type is same as multiplier, and then inputted element transferred into mod processing part without multiplication processing.

V. CONCLUSION

This paper propose a method of constructing the inverse element generation and inverse element generator over finite fields $GF(3^m)$.

The proposed inverse element generator was constructed by serial processing multiplier type.

A method computing inverse of an element over $GF(3^m)$ which corresponds to a polynomial over $GF(3^m)$ with order less than equal to $m-1$.

Here, the computation is based on multiplication, square and cube method derived from the mathematics properties over finite fields.

Future research was required to advanced inverse element generator, then we are able to constructing the divider over finite fields.

For the future, we prospect constructing four basic arithmetic operation unit systems(AOUS) over finite fields.

Then we obtain the arithmetic system that process the other future research is construct the logical unit that process the shift, rotate and complement and so on.

If above future research is establish, we implement the arithmetic and logical unit(ALU) of high efficiency computer ALU architecture based on embedded system

REFERENCES

- [1] D.L.Dietmeyer, Logic Design of Digital Systems, Allyn and Bacon, 1979.
- [2] K. Hwang, Computer Arithmetic principles, architecture, and design, John Wiley & Sons, 1979
- [3] M.D.Ercegovic and T.Lang, Digital Systems and Hardware Firmware Algorithms, Wiley, 1985.
- [4] E.J.McClusky, Logic Design Principles, Prentice-Hall, 1986.
- [5] D.Green, Modern Logic Design, Electronic Systems Engineer-ing Series, 1986.
- [6] Chen; Wen-Ching Lin; Hao-Hsuan Wu,"A New Algorithm for High-Speed Modular Multiplication Design," IEEE Trans. On Circuit and Systems, VOLUME 56, issue 9, pp. 2009-2019. Sep., 2009.
- [7] Nibouche, O.; Boussakta, S.; Darnell, M.," Pipeline Architectures for Radix-2 New Mersenne Number Transform," IEEE Trans. On Circuit and Systems, VOLUME 56, issue 8, pp. 1668-1680, Aug., 2009.
- [8] Meher, P.K.," Systolic and Super-Systolic Multipliers for Finite Field $GF(2^m)$ Based on Irreducible Trinomials, IEEE Trans. On Circuit and Systems, VOLUME 55, issue 4, pp. 1031-1040, Apr. 2008.

- [9] Tung-Chou Chen; Shyue-Win Wei; Hung-Jen Tsai," Arithmetic Unit for Finite Field $GF(2^m)$, IEEE Trans. On Circuit and Systems, VOLUME 55, issue 3, pp. 828-837, Mar., 2008.
- [10] Conway, T.," Galois field arithmetic over $GF(p^m)$ for high-speed/low-power error-control applications," IEEE Trans. On Circuit and Systems, VOLUME 51, issue 4, pp. 709- 717, Apr., 2004.
- [11] G.Drolet,"A new representation of elements of finite fields $GF(2^m)$ yields small complexity arithmetic circuits,' IEEE Trans. Comput.,vol.47.no.9,pp.938-946,Sep.1998.
- [12] R.J.McEliece, Finite Fields for Computer Science and Engineers, Kluwer Academic Publishers, 1987.



Chun-Myoung Park received the B.S, M.S and Ph.D. degree from electronic engineering, Inha University, Incheon, Korea, in 1983, 1986 and 1994 respectively. He joined the faculty at Chungju National University at 1995, where he is currently a professor in the Dept. of computer engineering. From 2002 to 2003, he was a visiting scholar at UCI in USA. His research interests include the next generation digital logic systems & computer architecture, embedded computer systems, ubiquitous computing systems, e(U)-Learning , IT application etc.