Efficient Serial Gaussian Normal Basis Multipliers over Binary Extension Fields

Yong-tae Kim*

This paper was partially supported by Gwangju National University of Education 2007

요 약

부호이론이나 암호학의 응용분야에 유한체는 매우 중요한 내용이고, 컴퓨터에서의 구현시에는 종규기저를 사용하는 것이 효과적이다. 본 논문에서는 유한체 타입 I 최적정규기저를 가지는 $GF(2^{mk})$는 $GF(2^m)$의 확대체가 된다는 사실을 이용하여 지금까지 알려진 가장 효율적인 Reyhani-Masoleh and Hasan의 곱셈기보다 25%정도 빠른 곱셈기를 소개하려고 한다.

ABSTRACT

Finite field arithmetic is very important in the area of cryptographic applications and coding theory, and it is efficient to use normal bases in hardware implementation. Using the fact that $GF(2^{mk})$ having a type-I optimal normal basis becomes the extension field of $GF(2^m)$, we, in this paper, propose a new serial multiplier which reduce the critical XOR path delay of the best known Reyhani-Masoleh and Hasan's serial multiplier by 25% and the number of XOR gates of Kwon et al.'s multiplier by 2 based on the Reyhani-Masoleh and Hasan's serial multiplier for type-I optimal normal basis.

키워드

Finite fields, Massey-Omura multiplier, Sequential multiplier, Gaussian normal basis, Critical path delay, ECC.

I. Introduction

In 1986, Massey-Omura[1] invented the serial multiplier which has a long path delay with parallel input and serial output. Agnew et al.[2] proposed a Sequential Multiplier with Parallel Output(SMPO) by improving Massey-Omura's serial multiplier. Recently, Reyhani-Masoleh and Hasan[3,4] proposed a SMPO with lower area complexity and path delay than that of Agnew et al. In 2004, Kwon et al.[5] proposed a SMPO improving that of Agnew et al. whose path delay is unchanged and area complexity is equal to or higher than that of Reyhani-Masoleh and Hasan according to type-II or otherwise. On the other hand, Yang et al.[6] proposed a SMPO which has the same path delay as that of Kwon et al. by reconstructing the multiplication matrix of Reyhani-Masoleh and Hasan over type-II optimal normal basis. It is well known that if 8 is not a divisor of m and $GF(2^m)$ has a type-k Gaussian normal basis, where m odd, then there is a Gaussian normal basis of type-k in $GF(2^m)$ and especially if $GF(2^m)$ is of

* 광주교육대학교 수학교육학과
심사완료일자 : 2009. 08. 27
접수일자 : 2009. 07. 10

type k, then $GF(4m+1)^*$ =<2>[7]. And many of the finite fields $GF(2^m)$, m $\leq$ 2000, having Gaussian normal bases of type-II, VI, X or XII satisfy the condition $GF(mk+1)^*$ =<2> according to Standard P1363[5], ANSI X9.63[8] if m is odd. The multipliers for many of finite fields $GF(2^m)$ thus can be constructed by using the multipliers for the extension field $GF(2^{mk})$ with type-I optimal normal basis based on Reyhani-Masoleh and Hasan. In 2005, Kim et al.[7] proposed a serial multiplier for type-IV Gaussian normal basis by embedding $GF(2^m)$ into the extension field $GF(2^{mk})$ with type-I optimal normal basis. Moreover, most of cryptographical applications including ECC are mainly implemented over $GF(2^m)$ for odd prime m. Therefore, in this paper, m is regarded as odd because of the facts above, and using the fact that $GF(2^m)$ having type-k Gaussian normal basis is a subfield of $GF(2^{mk})$ having a type-I optimal normal basis if $GF(mk+1)^*$ =<2> and m odd, we propose a new architecture for SMPO which transforms the Gaussian normal basis multiplication in $GF(2^m)$ into the type-I optimal normal basis multiplication in $GF(2^{mk})$ based on Reyhani-Masoleh and Hasan's SMPO over $GF(2^m)$ having a type-k Gaussian normal basis. Our SMPO reduce the XOR critical path delay of the serial multiplier of Reyhani-Masoleh and Hasan by 25% and has the same critical path delay as that of Kwon et al. if k=4, and reduce the XOR critical path delay of those of Reyhani-Masoleh and Hasan and Kwon et al. by 20% if k=10.

II Type -k Gaussian Normal Bases Multipliers

It is well known that there is always a normal basis for the finite field $GF(2^m)$ over $GF(2)$ for any positive integer l[5,9]. Multiplications in finite fields are explicitly discussed in [10] and the method for representing an element of $GF(2^m)$ as an element of $GF(2)$, where n=mk is introduced in [7]. We, in this section, propose a new multiplier modifying the Reyhani-Masoleh and Hasan [3,4]'s multiplier. We use two notations ((i))$\equiv$i mod m and <<i>>$\equiv$ I mod n from now on. Let $GF(2^n)$ be a finite field generated by a AOP and γ

be a root of the AOP $x^n+x^{n-1}+\cdots+x+1$, then γ generates the type-I optimal normal basis. In this case, n becomes even and $\delta_i = \gamma^{1+2i}$, where i=1,2, $\cdots$, v=n/2, since $\beta=\gamma$. We then have the following lemma since γ is a root of the AOP.

Lemma 1(Confer [11])

$$\delta_i = \begin{cases} \gamma^{2^{k_i}}, 1 \leq \frac{n}{2}-1, \\ 1=\sum_{j=0}^{n-1} \gamma^{2^j}, v=n/2, \end{cases}$$

where k_i satisfies the congruence $2^i+1 \equiv 2^{k_i}$ mod n+1.

Reyhani-Masoleh and Hasan[12] proved the following lemma by substituting all the entries of the multiplication matrix M=($\beta^{2^i+2^j}$) by the elements of the form β^{2^j}, 0 $\leq$j $\leq$n-1.

Lemma 2(Confer [4])

Let $GF(2^n)$ be a finite field having a type-I optimal normal basis, γ a generator of the optimal normal basis, A,B in $GF(2^n)$, C=AB and g $\in${0,1 }. Then

$$C=\sum_{j=0}^{n-1} a_{<<j-g>>} b_{\ll j-g \gg} \gamma^{2^j} + \sum_{i=1}^{v-1} \left(\sum_{j=0}^{n-1} x_{j,i} \gamma^{2^j}\right)^{2^{k_i}} + \sum_{j=0}^{n-1} \left(\sum_{i=1}^{v-1} x_{i,v}\right) \gamma^{2^j}, \quad v=n/2,$$

where

$$x_{j,i}=\begin{cases}a_jb_{<<i+j>>}+a_{<<i+j>>}b_j & \text{if } g=1\\ (a_j+a_{<<i+j>>})(b_j+b_{<<i+j>>} & \text{if } g=0.\end{cases}$$

III. A New Serial Architecture for the Type k Gaussian Normal Basis Multiplier

Let m,k be positive integers, n=mk, n+1 prime such that $GF(n+1)^*$= <2>. Since m is odd, k should be even. Now, We like to extend the elements A,B $\in GF(2^m)$ to the elements in $GF(2^n)$ with respect to type-I optimal basis and then construct a new multiplier for the finite subfield $GF(2^m)$ to calculate C=AB modifying Reyhani-Masoleh and Hasan multiplier described in section 2. For the later, we now define an exponent.

Definition 1. Suppose that n=mk, n+1 prime, $GF(n+1)^*$= <2> and k_i is the

exponent defined in Lemma 1. For 1 $\le i_0 \le$ u=(m-1)/2 and i $\in\{i_0,$ m-i_0, m+i_0, $\cdots$, km/2 -$i_0\}$, we will define θ_i as follows.

$$\theta_i=\begin{cases}((k_i)), i\equiv i_0 \bmod n,\\ ((k_i+i_0)), i\equiv -i_0 \bmod m.\end{cases}$$

Then we have the following.

Theorem 1. Assume that $GF(2^m)$ has a Gaussian normal basis of type k, n=mk, $GF(n+1)^*$ =<2>, g $\in\{0,1\}$ and u=(m-1)/2. If A,B are belong to $GF(2^m)$ and C is the product of A and B, then

$$C=\sum_{j=0}^{m-1}A_{((j-g))}B_{((j-g))}\beta^{2^j}+\sum_{j=0}^{m-1}\Big(\sum_{i_0=0}^{u}x_{j,i_0}\Big(\sum_{w=0}^{k/2-1}\beta^{2^{\theta_{wm+i_0}}}+\sum_{w=1}^{k/2}\beta^{2^{\theta_{wm-i_0}}}\Big)\Big)^{2^j},$$

where

$$x_{j,i}=\begin{cases}A_jB_{((i+j))}+A_{((i+j))}B_j & \text{if } g=1,\\ (A_j+A_{((i+j))})(B_j+B_{((i+j))}) & \text{if } g=0.\end{cases}$$

proof) Without loss of generality, we prove the theorem for g=1. Let A,B $\in GF(2^m)\subset GF(2^n)$. Then

$$C=AB=\sum_{j=0}^{n-1}a_{<<j-1>>}b<<j-1>>\gamma^{2^j}+\sum_{i=1}^{v-1}\Big(\sum_{j=0}^{n-1}x_{j,i}$$

$\gamma^{2^j})^{2^{k_i}}$, $v=(k/2)m$ and

$a_j=A_{((j))}, b_j=B_{((j))}, 0\le j\le n-1$. Therefore we calculate only A_iB_i for i=0,1,2, $\cdots$, m-1. Next, if i=wm, 1 $\le$w $\le$ k/2, then

$x_{j,i}=a_jb_{<<i+j>>}+a_{<<j+i>>}b_j=A_{((j))}B_{((i+j))}+A_{((i+j))}B_{((j))}=0.$

Lastly,

$x_{j,i}=a_jb_{<<i+j>>}+a_{<<j+i>>}b_j=A_jB_{((i+j))}+A_{((i+j))}B_j=x_{((j)),((i))}.$

Therefore, for 1 $\le$ i $\le$(m-1)/2,

$$\sum_{j=0}^{n-1}x_{j,i}\gamma^{2^j}=\sum_{t=0}^{k-1}\sum_{j_0=0}^{m-1}\gamma^{2^{j_0}})^{2^{tm}}=\sum_{j_0=0}^{m-1}x_{j_0,i}\beta^{2^{j_0}}.$$

Thus,

$$\sum_{i=1}^{v-1}\Big(\sum_{j=0}^{n-1}x_{j,i}\gamma^{2^j}\Big)^{2^{k_i}}=\sum_{i=1}^{v-1}\Big(\sum_{j_0=0}^{m-1}x_{j_0,i}\beta^{2^{j_0}}\Big)^{2^{k_i}}$$

$$=\sum_{j_0=0}^{m-1}\sum_{i=10}^{v-1}x_{j_0,i}\beta^{2^{k_i}})^{2^{j_0}}.$$

For 1 $\le i_0\le$u=(m-1)/2, we divide is into two classes as follows.

(1) i= wm + i_0, 0$\le$w$\le$k/2 -1,

(2) i= wm - i_0, 0$\le$w$\le$k/2 ,

For (1),

$$\begin{aligned}x_{j,i}&=x_{j,wm+i_0}\\ &=a_jb_{<<j+wm+i_0>>}+a_{<<j+wm+i_0>>}b_j\\ &=A_{((j))}B_{((j+i_0))}+A_{((j+i_0))}B_{((j))}\\ &=x_{((j)),i_0}.\end{aligned}$$

For (2),

$$\begin{aligned}x_{j,i}&=x_{j,wm-i_0}\\ &=a_jb_{<<j+wm-i_0>>}+a_{<<j+wm-i_0>>}b_j\\ &=A_{((j))}B_{((j-i_0))}+A_{((j-i_0))}B_{((j))}\end{aligned}$$

$=x_{((j-i_0)),i_0}$.

Therefore,

$$C=\sum_{j=0}^{m-1}A_{((j-g))}B_{((j-g))}\beta^{2^j}+\sum_{j=0}^{m-1}(\sum_{i_0=0}^{u}x_{j,i_0}(\sum_{w=0}^{k/2-1}\beta^{2^{\theta_{wm+i_0}}}+\sum_{w=1}^{k/2}\beta^{2^{\theta_{wm-i_0}}}))^{2^j}.$$

This completes the proof.

From Theorem 1, if

$$G_j(A,B)=A_{((j-g))}B_{((j-g))}\beta+\sum_{i_0=0}^{u}(\sum_{w=0}^{k/2-1}\beta^{2^{\theta_{wm+i_0}}}+\sum_{w=1}^{k/2}\beta^{2^{\theta_{wm-i_0}}},$$

then

$C=((G_{m-1}^2+G_{m-2})^2+\cdots+G_1)^2+G_0,$

where $G_{m-t}(A,B)=G_{m-1}(A^{2^{t-1}},B^{2^{t-1}})$.

Moreover, since β^{2^j} appears k times for each j, there can occur at most ku+1 terms. However, that β^{2^j} appears twice for each i_0 means the same value is added twice. Therefore such terms can be neglected. Consequently, the number of XOR gates of the serial multiplier is

$$M=|\{\beta\}|+\sum_{i_0=1}^{u}|\{\beta^{2^{\theta_{i_0}}},\beta^{2^{\theta_{wm-i_0}}},\cdots,\beta^{2^{\theta_{(k/2)m-i_0}}}\}|+\epsilon u,$$

where

$$\epsilon=\begin{cases}1 \text{ if } g=1,\\ 2 \text{ if } g=0.\end{cases}$$

And if we set $l=Max\,M_j+1, j=0,\cdots,m-1,$ where

$$M_j=|\{wm+i_0|\theta_{wm+i_0}=j,0\le w\le k/2|+|\{wm-i_0|\theta_{wm-i_0}=j,1\le w\le k/2\}|+t, \text{ where}$$

$$t=\begin{cases}1 \text{ if } j=0,\\ 0 \text{ if } j\ne 0,\end{cases}$$

then l determines the critical path delay of the XOR gates. To reduce the value of l, we need the following.

Corollary 1. Assume that $GF(2^m)$ has a type-k Gaussian normal basis and n=mk,

$GF(n+1)^*$=<2>. If A,B $\in GF(2^m)\subset GF(2^n)$ then

$$C=\sum_{j=0}^{m-1}(A_{((j+j_0-g))}B_{((j+j_0-g))}\beta^{2^{j_0}})^{2^j}+\sum_{j=0}^{m-1}(\sum_{i_0=1}^{u}x_{((j+j_{i_0})),i_0}(\sum_{w=0}^{k/2-1}\beta^{2^{\theta_{wm+i_0}+j_{i_0}}}+(\sum_{w=0}^{k/2-1}\beta^{2^{\theta_{wm-i_0}+j_{i_0}}})^{2^j},$$

where

$$x_{i,j}=\begin{cases}A_jB_{((i+j))}+A_{((i+j))}B_j \text{ if } g=1\\ (A_j+A_{((i+j))})(B_jB_{((i+j))}) \text{ if } g=0.\end{cases}$$

proof) If we perform j_{i_0}-fold right cyclic shift on each basic element β^{2^j} appeared in C in Theorem 1 for each i_0, then

$$C=\sum_{j=0}^{m-1}(A_{((j-g))}B_{((j-g))}\beta^{2^{j_0}})^{2^{j-j_0}}+\sum_{j=0}^{m-1}(\sum_{i_0=0}^{u}x_{j,i_0}(\sum_{w=0}^{k/2-1}\beta^{2^{\theta_{wm+i_0}+j_{i_0}}}+\sum_{w=0}^{k/2}\beta^{2^{\theta_{wm-i_0}+j_{i_0}}}))^{2^{j-j_0}}.$$

Substitute the value of β which has earlier derived and matches the bits, then we obtain the result.

Therefore if we define

$$G_j'(A,B)=A_{((j+j_0-g))}B_{((j+j_0-g}))\beta^{2^{j_0}}+\sum_{i_0}^{u}x_{((j+j_0)),i_0}(\sum_{w=0}^{k/2-1}\beta^{2^{\theta_{wm+i_0}+j_{i_0}}}+\sum_{w=0}^{k/2-1}\beta^{2^{\theta_{wm-i_0}+j_{i_0}}}),$$

then

$C=((G_{m-1}'^2+G_{m-2}')^2+\cdots+G_1')^2+G_0',$

where $G'_{m-t}(A,B) = G'_{m-1}A^{2^{t-1}}, B^{2^{t-1}})$ by Corollary 1.

Let $l' = Max M'_j + 1, j = 0, \cdots, m-1$, where
$M'_j = |\{wm + i_0 | \theta_{wm+i_0} + j_{i_0} = j, 0 \le w < k/2\}| +$
$|\{wm - i_0 | \theta_{wm-i_0} = j_{i_0}, 1 \le w \le k/2\}|$.

Then the process of calculating C in Corollary 1 is as follows. Firstly, for each i_0, we seek for j_{j_0} such that l'

becomes to be optimal and choose j_0 being different from l'. Next, $G_j(A,B)$ is obtained by j_0 -fold and j_{i_0}-fold right shift of the first term and the second term respectively in the equation of defining $G_j(A,B)$. Lastly, C is calculated by G_j's and thus XOR path delay for calculating C can be reduced to $\lceil \log_2 l' \rceil$. Therefore the critical path delay is

determined by l'.

IV. Optimization

In implementing our proposed multiplier, for a fixed $1 \le i_0 \le$u=(m-1)/2 if some

θ_i, i=i_0, $m - i_0, m + i_0, \cdots$, km/2-i_0, in Theorem 1 are the same, then so are the outputs of $\beta^{2^{\theta_i}}$. Therefore the result is not changed if we discard them. So we can reduce the number of XOR gates and path delay. In this regard, the number of XOR gates and path delay can be reduced by confirming whether the values of θ_is coincide for some i. In some special type of Gaussian normal basis, we have the following notable result.

Lemma 3(Confer [7], Lemma 4)

Assume that m odd, 4m+1 prime and $GF(4m+1)^*$=<2>. Then one of $k_1 = k_2 + u$ mod m or $k_1 = k_2 + u$ mod m

holds for u=(m-1)/2 if, in $GF(4m+1)^*$=<2>, $\begin{cases} 2^u + 1 = 2^{k_1} \\ 2^{m-u} + 1 = 2^{k_2} \end{cases}$ or

$$\begin{cases} 2^{m+u} + 1 = 2^{k_3} \\ 2^{2m-u} + 1 = 2^{k_4} \end{cases}.$$

On the other hand, if $GF(2^m)$ have a type-IV Gaussian normal basis and m is odd, then either $\theta_u = \theta_{m-u}$ or θ_{m+u}=θ_{2m-u} for u=(m-1)/2 (confer [7]).

Therefore, if $GF(2^m)$ have a type-IV Gaussian normal basis and m be odd, then for u=(m-1)/2, either $\theta_u = \theta_{m-u}$ or $\theta_{m+u} = \theta_{2m-u}$ by Lemma 3. So, for g=1, there need M=(5m-7)/2 XOR gates and thus there needs M=(7m-13)/2 XOR gates for type-VI Gaussian normal basis.

V. Complexity

In this chapter, we calculate the complexities of the serial multiplier constructed in Theorem 1 and Corollary 1 of section 3.

Ttheorem 2. The maximum complexities of the multiplier of Theorem 1 and Corollary 1 are

a) m AND gates, (k+1)(m-1)/2 +1 XOR gates if g=1 and (m+1)/2 AND gates, (k+2)(m-1)/2 XOR gates if g=0 and

b) T_A + (1+ $\lceil \log_2 l' \rceil$) T_X path delay, where T_A, T_X are AND delay and XOR delay respectively.

proof)

For a), if g=1, then there need one AND gate in order to calculate $A_{j-1}B_{j-1}$, and the total number of AND gates to generate x_{j,i_0} is m-1 since, for each $1 \le i_0 \le$ u=(m-1)/2, there need two AND gates in order to calculate x_{j,i_0}. Therefore we need a total

number of m AND gates. Since the number of XOR gate to generate each x_{j,i_0} is 1 for

each $1 \leqq i \leqq u=(m-1)/2$, there need a total of (m-1)/2 XOR gates. There need 1+k(m-1)/2 to calculate $G_j(A,B)^2 + G_{j-1}(A,B)$ except x_{j,i_0}, and thus we need a total of (k+1)(m-1)/2+1 XOR gates. By the way, for $i_0 = u$, two θ_{i_0} coincide by Lemma 3. Therefore the optimized total number of XOR gates is (5m-7)/2. For g=0, there need (m-1)/2 and 1 AND gates to generate x_{j,i_0} and A_jB_j respectively, and thus we need a total of (m-1)/2 AND gates. Similarly, there need a total (k+2)(m-1)/2 XOR gates in total in case g=0.

For b), it is immediately that both of the number of path delay of AND gates and that of XOR gates for calculating x_{j,i_0} are equal to 1. Thus the critical XOR path delay is $1+\lceil \log_2 l' \rceil$ since the number of upper bound of the number of XOR gates to generate the basic element β^{2^j} in $G_j(A,B)^2 + G_{j-1}(A,B)$ except x_{j,i_0} is 1. This completes the proof.

VI. Conclusion

Using the fact that $GF(2^m)$ having type-k Gaussian normal basis is a subfield of $GF(2^{mk})$ having a type-I optimal normal basis if $GF(mk+1)^*$ =<2> and m odd, in this paper, we proposed a new architecture for SMPO, which transforms the Gaussian normal basis multiplication in $GF(2^m)$ into the type-I optimal normal basis multiplication in $GF(2^{mk})$ based on Reyhani-Masoleh and Hasan's SMPO over $GF(2^m)$ having a type-k Gaussian normal basis. We can confirm that our proposed SMPO reduce the XOR critical path delay of the serial multiplier of Reyhani-Masoleh and Hasan by 25% and has the same critical path delay as that of Kwon et al. if k=4, and reduce the XOR critical path delay of those of Reyhani-Masoleh and Hasan and Kwon et al. by 20% if k=10. We therefore expect our proposed serial multiplier will be efficiently applied to hardware implementations in the related application areas.

References

[1] J. L. Massey and J. K. Omura, "Computational method and apparatus for finite field arithmetic", US Patent, No. 4587627, 1986.

[2] G. B. Agnew, R. C. Mullin, I. Onyszchuk and S. A. Vanstone, "An implementation for a fast public key cryptosystem", J. Cryptography, Vol. 3, pp.63-79, 1991.

[3] A. Reyhani-Masoleh and M. H. Hasan, "Low complexity sequential normal basis multipliers over $GF(2^m)$", 16th IEEE Symposium on Computer Arithmetic, Vol. 16, pp.188-195, 2003.

[4] A. Reyhani-Masoleh and M. H. Hasan, "Low Complexity Word-Level Sequential Normal Basis Multipliers", IEEE Trans. Computers, Vol. 54, No. 2, pp.98-110, Feb. 2005.

[5] S. Kwon, K. Gaj, C. H. Kim and C. P. Hong, "Efficient Linear Array for Multiplication in $GF(2^m)$ Using a Normal Basis for Elliptic Curve Cryptography", CHES 2004, LNCS 3156, pp.76-91, 2004.

[6] H. Wu and M. A. Hasan, "Low Complexity bit-parallel multipliers for a class of finite fields", IEEE Trans., Vol. 47, No. 8, pp.883-887, Aug. 1998.

[7] C. H. Kim, Y. Kim, N. S. Chang and I. Park, " Modified Serial Multipliers for Type-IV Gaussian Normal Bases", Lecture Notes in Computer Science(Indocrypt 2005) 3797, pp.375-388, 2005.

[8] ANSI X 9.63, "Public key cryptography for the financial sevices industry: Elliptic curve key agreement and transport protocols", draft, 1998.

[9] C. K. Koc and B. Sunar, "Low-complexity bit-parallel canonical and normal basis multipliers for a class of finite fields", IEEE Trans. Computers, Vol. 47, No. 3, pp.353-356, Mar. 1998.

[10] Y. T. Kim, "Efficient Parallel Gaussian Normal Bases Multipliers over Finite Fields", Honam Math. J., Vol. 29, No. 3, pp.415-425, 2007.

[11] A. Reyhani-Masoleh and M. H. Hasan, "A new construction of Massey-Omura parallel multiplier over $GF(2^m)$", IEEE Trans. Computers, Vol. 51, No. 5, pp.512-520, May 2002.

[12] A. Reyhani-Masoleh and M. H. Hasan, "Efficient multiplication beyond optimal normal bases", IEEE Trans. Computers, Vol. 52, No. 4, pp.428-439, April 2003.

[13] S. Gao Jr. and H. W. Lenstra, "Optimal normal bases, Designs, Codes and Cryptography", Vol. 2, pp.315-323, 1992.

[14] M. A. Hasan, M. Z. Wang, and V. K. Bhargava, "A modified Massey-Omura parallel multiplier for a class of finite fields", IEEE Trans. Computers, Vol. 42, No. 10, pp.1278-1280, Oct. 1993.

[15] IEEE P1363, "Standard specifications for public key cryptography", Draft 13, 1999.

[16] T. Itoh and S. Tsujii, "Structure of parallel multipliers for a class of fields", Information and Computation, Vol. 83, pp.21-40, 1989.

[17] C. H. Kim, S. Oh, and J. Lim, "A new hardware architecture for operations in $GF(2^m)$", IEEE Trans. Computers, Vol. 51, No. 1, pp.90-92, Jan. 2002.

[18] R. Lidl and H. Niederreiter, "Introduction to finite fields and its applications", Cambridge Univ. Press, 1994.

[19] A. J. Menezes, I. F. Blake, X. Gao, R. C. Mullin, S. A. Vanstone, and T. Yaghoobian, "Applications of finite fields", Kluwer Academic, 1993.

[20] A. Reyhani-Masoleh and M. H. Hasan, "Efficient Digit-Serial Normal Basis Multipliers over Binary Extension Fields", ACM Trans. on Embedded Computing Systems(TECS), Special Issue on Embedded Systems and Security, Vol. 3, Issue 3, pp.575-592, August 2004.

[21] A. Reyhani-Masoleh, "Efficient Algorithms and Architecture for Fields Multiplication Using Gaussian Normal Bases", IEEE Trans. Computers, Vol. 55 No. 1, pp.34-47, Jan. 2006.

[22] C. C Wang, T. K. Truong, H. M. Shao, L. J. Deutsch, J. K. Omura, and I. S. Reed, "VLSI architectures for computing multiplications and inverses in $GF(2^n)$", 1998.

[23] H. Wu and M. A. Hasan, "Low Complexity bit-parallel multipliers for a class of finite fields", IEEE Trans., Vol. 47, No. 8, pp.883-887, Aug. 1998.

[24] D. J. Yang, C. H. Kim, Y. Park, Y. Kim and J. Lim, "Modified sequential Normal Basis Multipliers for Type II Optimal Normal Basis", ICCSA 2005, LNCS 3481, pp.647-656, 2005.

저자 소개

김용태(Yong-tae Kim)

1976년 2월 : 공주사범대학 수학교육과(이학사)
1986년 2월 : 고려대학교 대학원 수학과 (이학석사)
1991년 2월 : 고려대학교 대학원 수학과(이학박사)
2000년 8월 : 서울대학교 대학원 수학교육과(교육학석사)
2008년 2월 : 서울대학교 대학원 수학교육과(박사과정 수료)
1992년 3월 ~ 현재 : 광주교육대학교 수학교육과 교수
※관심분야 : ECC, 정수론적 암호학, 공개키암호학