Journal of Knowledge Information Technology and Systems

ISSN 1975-7700

http://www.kkits.or.kr

Design of Low-Complexity Decoder for Triple Error Correcting BCH Codes

Yong-Suk Cho, Yong-Dal Shin*

Department of IT & Securities, U1 University

ABSTRACT

The Bose-Chaudhuri-Hocquenghem (BCH) codes are a class of powerful multiple-error-correcting cyclic codes. Due to its powerful error-correction performance and reasonable hardware costs, the binary BCH codes have been widely used in data communications and storage systems for error control. In this paper, a design method of low-complexity decoder for triple error correcting binary BCH codes is presented, which is modified Peterson's direct solution method. In this method, all division operations over finite field $GF(2^m)$ are eliminated from the computations of the error locator polynomial. BCH codes are defined over finite field $GF(2^m)$ and all arithmetic operations are performed over this fields. Inversion in a finite field is time consuming and requires relatively complex circuitry. In conventional decoding algorithm of BCH codes are required finite field inversion. In this paper, inversionless decoder for triple error correcting BCH codes is proposed. The decoder comprises a syndrome computation circuit, a error locator polynomial computation circuit and a error location searching circuit, which can be implemented by linear feedback shift registers and logical gates. The attractive feature of this decoder is its remarkable simplicity from the point of view of hardware implementation. Futhermore, the proposed decoder has very simple control circuit and short decoding delay. Therefore this decoder can be implemented by simple hardware and also save buffer memory which stores received sequence.

KEYWORDS: Error correction codes, BCH codes, Peterson's algorithm, Galois fields, Finite fields inversion

ARTICLE INFO: Received 2 May 2018, Revised 28 May 2018, Accepted 8 June 2018.

*Corresponding author is with the Department of IT & Securities, U1 University, 52-70 Yeonamsan-ro Eumbong-myeon Asan-si Chungcheong nam-do KOREA.
E-mail address: ydshin@u1.ac.kr

1. 서 론

BCH(Bose Chaudhuri Hocquenghem) 부호는 오류정정 개수를 비교적 자유롭게 선택할 수 있고 정보비트 수에 비해 검사비트(parity-check bit)의 수가 비교적 작은 매우 효율적인 다중 오류정정 부호로 데이터통신과 데이터 저장 시스템 등에 널리 사용되고 있는 부호이다[1-4].

BCH 부호의 복호는 한 블럭 내에서 발생한 오류의 위치를 찾아내서 그 위치의 비트를 0이면 1로, 1이면 0으로 바꾸는 것이다. 일반적으로 BCH 부호의 복호는, 수신 시퀀스로부터 오증(誤症 : syndrome)을 계산하고, 이 오증을 이용하여 오류위치다항식(error locator polynomial)을 구성한 다음, 오류위치다항식의 근(root)을 구하여 오류위치(error location number)를 찾고 그 위치의 비트를 반전시킴으로써 오류를 정정한다[5, 6].

이와 같은 복호 과정 중에서 오증으로부터 오류위치다항식을 계산하는 과정이 가장 어렵고 복잡한 과정이다. Peterson의 복호법[7]은 오증으로부터 오류위치다항식의 계수를 직접 계산하는 방법이며, Berlekamp-Massey 복호법[8, 9]과 Euclid 복호법[10]은 반복 알고리즘을 사용하여 구하는 방법이다. Peterson 복호법은 복호지연(decoding delay)이 짧은 고속 복호에 적합한 반면 오류정정능력 t가 커지면 회로가 복잡해진다. 일반적으로 t가 6 또는 7보다 크면 Berlekamp-Massey 복호법이나 Euclid 복호법이 더 효율적인 반면, 반복 알고리즘으로 인한 복호지연이 불가피해지는 단점이 있다[11].

본 논문에서는 Peterson 복호법을 개선하여 기존의 복호기보다 하드웨어적으로 훨씬 더 간단한 3중 오류정정 BCH 부호의 복호기를 설계한다. 설계된 복호기의 특징은 기존의 Peterson 복호법에서 유한체 상의 나눗셈을 생략하는 것으로, 이 방법을 사용하면 Peterson 복호법의 문제점인 복잡한 회로 규모를 대폭 축소시킬 수 있다.

나눗셈은 유한체 $GF(2^m)$의 연산 중에서 가장 어렵고 복잡한 연산이다. 기존의 Peterson 복호법에서는 오류위치다항식을 구하는 과정에서 나눗셈이 필요하게 된다. 나눗셈은 일반적으로 한 원소의 역원(inverse element)에 다른 원소를 곱하는 것으로, 나눗셈기는 역원기와 곱셈기로 구현할 수 있다. 역원기는 장치화가 복잡하고 어렵기 때문에 이를 효과적으로 구현하는 것이 복호기 전체 회로의 간단화 및 고속화의 관건이 된다[12, 13].

본 몬문에서는 기존의 오류위치다항식을 변형한 새로운 오류위치다항식을 사용하여 나눗셈 자체를 생략할 수 있는 3중 오류정정 BCH 복호기를 설계한다. 먼저 2.에서 BCH 복호법을 분석하고, 3.에서 3중 오류정정 BCH 부호의 저복잡도 복호기를 설계한다. 그리고 4.에서 결론을 맺는다.

2. BCH 부호의 복호법

한 블럭 내에서 발생한 t개 이하의 모든 오류를 정정할 수 있는 t중 오류정정 BCH 부호는, 입력비트를 다항식(polynomial)으로 표현한 정보다항식(information polynomial) $d(x)$와 특수한 구조를 갖는 생성다항식(generator polynomial) $g(x)$의 곱으로 구성된다[14].

$$c(x) = d(x) \cdot g(x) \tag{1}$$

유한체(finite field) $GF(2^m)$의 원시원(primitive element)을 α라 하면, 생성다항식 $g(x)$는 α, α^3, α^5, ……, α^{2t-1}를 근(root)으로 갖는 다항식으로 정의된다. 그러므로 식 (1)에 α^j (j=1, 3, 5, ……, $2t-1$)를 대입하면 $g(\alpha^j)$가 0이므로 다음과 같이 쓸 수 있다.

$$c(\alpha^j) = d(\alpha^j) \cdot g(\alpha^j) = 0 \quad (2)$$

수신다항식 $r(x)$는 다음과 같이 부호다항식 $c(x)$에 오류다항식 $e(x)$가 더해진 것이므로, α^j (j = 1, 3, 5, ……, $2t-1$)를 대입하면

$$r(\alpha^j) = c(\alpha^j) + e(\alpha^j) = e(\alpha^j) \quad (3)$$

가 된다. 식 (3)은 오류가 발생하지 않으면 0이 되고 오류가 발생하면 0이 되지 않는다. 그러므로 이 식을 다음과 같이 오증으로 정의할 수 있다.

$$S_j \equiv r(\alpha^j) = e(\alpha^j) \quad (4)$$

만약 $u(1 \le u \le t)$개의 오류가 i_1, i_2, ……, i_u ($i_1 < i_2 < \cdots\cdots < i_u$) 위치에 발생하였다고 가정하면 오류다항식은 다음과 같이 쓸 수 있다.

$$e(x) = x^{i_1} + x^{i_2} + \cdots\cdots + x^{i_u} \quad (5)$$

따라서 오증 S_j는 식 (5)에 α^j를 대입하면

$$S_j = (\alpha^{i_1})^j + (\alpha^{i_2})^j + \cdots\cdots + (\alpha^{i_u})^j \quad (6)$$

가 되고, 여기에서 α^{i_k}를 오류위치 X_k로 표기하면 다음과 같이 정리할 수 있다.

$$S_j = X_1^j + X_2^j + \cdots + X_u^j \quad (7)$$

식 (7)을 j = 1, 3, 5, ……, $2t-1$에 대하여 풀어 쓰면 다음과 같은 t개의 방정식이 된다.

$$\begin{aligned} S_1 &= X_1 + X_2 + \cdots + X_u \\ S_3 &= X_1^3 + X_2^3 + \cdots + X_u^3 \\ S_5 &= X_1^5 + X_2^5 + \cdots + X_u^5 \\ &\vdots \quad\quad \vdots \quad\quad \vdots \quad\quad\quad \vdots \\ S_{2t-1} &= X_1^{2t-1} + X_2^{2t-1} + \cdots + X_u^{2t-1} \end{aligned} \quad (8)$$

BCH 부호의 복호는 이 t개의 방정식으로부터 u개의 미지수 X_1, X_2, ……, X_u를 구하는 것이다. 그러나 이 방정식은 비선형(nonlinear)이므로 직접 해를 구하는 것은 매우 어렵다. Peterson은 다음과 같은 오류위치다항식을 도입하여 위와 같은 비선형 방정식을 푸는 방법을 처음 제안하였다[7].

$$\begin{aligned} \sigma(x) &= (1 + X_1 x)(1 + X_2 x) \cdots (1 + X_u x) \\ &= 1 + \sigma_1 x + \sigma_2 x + \cdots + \sigma_u x \end{aligned} \quad (9)$$

식 (9)와 같이 오류위치다항식 $\sigma(x)$는 오류위치의 역수를 근으로 갖는 다항식이다. 이와 같이 정의한 오류위치다항식의 계수 σ_i와 오증 S_j와의 관계는 Newton의 항등식에 의하여 다음과 같이 된다[11]. 여기에서 $S_{2j} = (S_j)^2$ 이다.

$$\underbrace{\begin{bmatrix} 1 & 0 & \cdots & 0 \\ S_2 & S_1 & \cdots & 0 \\ S_4 & S_3 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ S_{2u-2} & S_{2u-3} & \cdots & S_{u-1} \end{bmatrix}}_{\mathbf{A}^{(u)}} \underbrace{\begin{bmatrix} \sigma_1^{(u)} \\ \sigma_2^{(u)} \\ \sigma_3^{(u)} \\ \vdots \\ \sigma_u^{(u)} \end{bmatrix}}_{\boldsymbol{\sigma}^{(u)}} = \underbrace{\begin{bmatrix} S_1 \\ S_3 \\ S_5 \\ \vdots \\ S_{2u-1} \end{bmatrix}}_{\mathbf{B}^{(u)}} \quad (10)$$

이 방정식은 선형방정식이므로 비교적 쉽게 오류위치다항식을 구할 수 있다. 오증으로부터 오류위치다항식의 계수를 구하는 것은 BCH 부호의 복호과정 중 가장 어렵고 복잡한 과정으로 이에 대한 해법이 BCH 부호의 복호에서 가장 핵심이 되는 부분이다.

Peterson은 오류가 u 또는 $u-1$개 발생하였을

때 식 (10)의 행렬식(determinant) $|\mathbf{A}^{(u)}|$ 가 0이 아니며(non singular), $u-2$개 이하가 발생하였을 경우 0이 됨을 증명하였다[7]. 그러므로 행렬식 $|\mathbf{A}^{(u)}|$ 를 계산하면 실제 발생한 오류의 개수를 찾을 수 있다.

따라서 복호는 먼저 수신다항식 $r(x)$로부터 오증 S_j를 계산하고 이 오증으로부터 행렬식 $|\mathbf{A}^{(u)}|$ 를 계산한다. 행렬식 $|\mathbf{A}^{(u)}|$ 의 값이 영이 아니면 식 (10)을 이용하여 오류위치다항식 $\sigma^{(u)}(x)$를 구한다. 오류위치는 오류위치다항식의 근의 역수이므로, 방정식 $\sigma^{(u)}(x)=0$을 풀어서 근을 구하고 그것의 역수를 구하여 그 위치의 수신 비트를 반전시키면 오류가 정정된다.

오류위치다항식으로부터 오류위치를 구하여 오류를 정정하는 과정은 일반적으로 Chien의 방법을 가장 많이 사용한다[15]. 행렬식 $|\mathbf{A}^{(u)}|$ 가 영이면, 행렬 $\mathbf{A}^{(u)}$에서 가장 아래의 두 행과 가장 왼쪽의 두 열을 제거한 행렬 $\mathbf{A}^{(u-2)}$를 구성하여 같은 과정을 반복한다.

식 (9)와 같은 오류위치다항식의 정의에 따라 오류위치는 오류위치다항식의 근의 역수이므로 오류위치를 구하기 위해서는 먼저 방정식 $\sigma^{(u)}(x)=0$의 해를 구하여야 한다. 식 (10)에서 행렬식 $|\mathbf{A}^{(u)}|$ 가 0이 아닐 경우, 행렬 $\mathbf{A}^{(u)}$의 역행렬이 존재하므로 다음과 같이 쓸 수 있다.

$$\boldsymbol{\sigma}^{(u)} = \{\mathbf{A}^{(u)}\}^{-1} \cdot \mathbf{B}^{(u)} \tag{11}$$

여기에서 행렬 $\mathbf{A}^{(u)}$의 여인자(cofactor)를 $A_{i,k}^{(u)}$라 하면 식 (11)은 다음과 같이 정리할 수 있다.

$$\sigma_k^{(u)} = \frac{1}{|\mathbf{A}^{(u)}|}\sum_{i=1}^{u} S_{2i-1}\, A_{i,k}^{(u)} \qquad k=1, 2, \cdots, u \tag{12}$$

식 (9)의 오류위치다항식을 다시 쓰면

$$\sigma^{(u)}(x) = 1 + \sum_{k=1}^{u} \sigma_k^{(u)} x^k \tag{13}$$

가 되고 여기에 식 (12)를 대입하여 방정식 $\sigma^{(u)}(x)=0$를 구성하면 다음과 같이 된다.

$$1 + \sum_{k=1}^{u}\left\{\frac{1}{|\mathbf{A}^{(u)}|}\sum_{i=1}^{u} S_{2i-1} A_{i,k}^{(u)}\right\} x^k = 0 \tag{14}$$

여기에서 $|\mathbf{A}^{(u)}|$ 는 k와 무관하고 0이 아니라고 가정하였으므로 $|\mathbf{A}^{(u)}|$ 를 양변에 곱하면

$$|\mathbf{A}^{(u)}| + \sum_{k=1}^{u}\left\{\sum_{i=1}^{u} S_{2i-1} A_{i,k}^{(u)}\right\} x^k = 0 \tag{15}$$

가 된다. 따라서 식 (15)의 해를 구하여 역수를 취하면 오류위치를 구할 수 있다. 변형된 오류위치다항식을 $\Lambda^{(u)}(x)$로 표기하면

$$\Lambda^{(u)}(x) = |\mathbf{A}^{(u)}| + \sum_{k=1}^{u} \Lambda_k^{(u)} x^k \tag{16}$$

가 되므로, 식 (16)과 같은 변형된 오류위치다항식을 사용하면 오증으로부터 오류위치다항식을 구할 때 유한체 상의 나눗셈을 생략할 수 있다.

3. 3중 오류정정 BCH 부호의 저복잡도 복호기 설계

본 논문에서는 BCH 복호기를 그림 1과 같이 오증 계산회로, 오류위치다항식 계산회로, 오류위치 탐지회로의 3부분으로 나누어 설계한다.

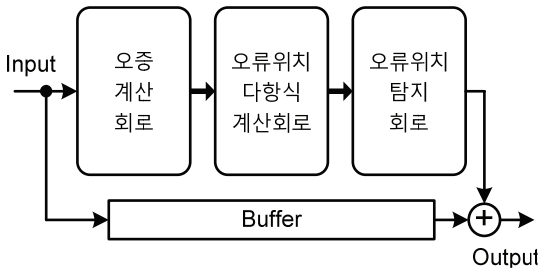

그림 1 BCH 복호기의 블록도
Figure 1. Block diagram of BCH decoder

오증은 식 (4)와 같이 수신다항식으로부터 구할 수 있다. 식 (4)를 다시 정리하면

$$S_j = r_0 + r_1(\alpha^j) + \cdots + r_{n-1}(\alpha^j)^{n-1} \quad (17)$$
$$= (\cdots((r_{n-1})\alpha^j + r_{n-2})\alpha^j + \cdots)\alpha^j + r_0$$
$$j = 1,\ 3,\ 5, \cdots\cdots, 2t-1$$

가 된다. 따라서 식 (17)을 이용하면 그림 2와 같이 오증계산회로를 설계할 수 있다.

그림 2에서 ⊕는 $GF(2^m)$ 상의 덧셈기로 m개의 2입력 Exclusive OR 게이트로 구현할 수 있다. 또한 □는 m비트 레지스터를, ⓐ는 α^j를 곱하는 상수곱셈기를 나타내고 있다.

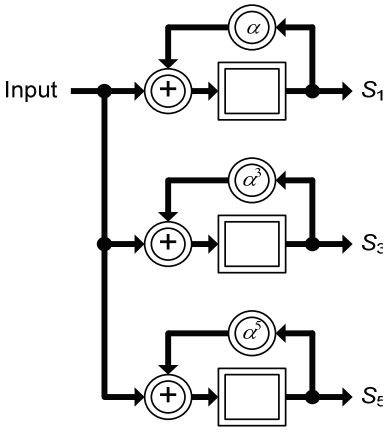

그림 2 오증계산회로
Figure 2. Syndrome computation circuit

3중 오류정정 BCH 부호의 오류위치다항식의 계수는 식 (16)에 $u = 3$을 대입하면 다음과 같이 구할 수 있다.

$$|\mathbf{A}^{(3)}| = S_1^3 + S_3$$
$$\Lambda_1^{(3)} = S_1(S_1^3 + S_3) \quad (18)$$
$$\Lambda_2^{(3)} = S_1^2 S_3 + S_5$$
$$\Lambda_3^{(3)} = (S_1^3 + S_3)^2 + S_1\Lambda_2^{(3)}$$

식 (18)을 이용하면 그림 3과 같이 오류위치다항식 계산회로를 설계할 수 있다. 그림 3에서 [X]와 [()²]는 $GF(2^m)$ 상의 곱셈기와 제곱기를 나타내고 있다.

행렬식 $|\mathbf{A}^{(3)}|$ 가 0이면 1개의 오류가 발생한 것이므로 오류위치 탐지회로는 그림 4와 같이 설계할 수 있다. 그림 4에서 [+1]는 최하위 비트를 반전시키는 회로로 NOT 게이트 한 개로, [=0]는 입력이 모두 0일 때에만 0을 출력하는 회로로 $m-1$개의 2입력 OR 게이트로 구성할 수 있다.

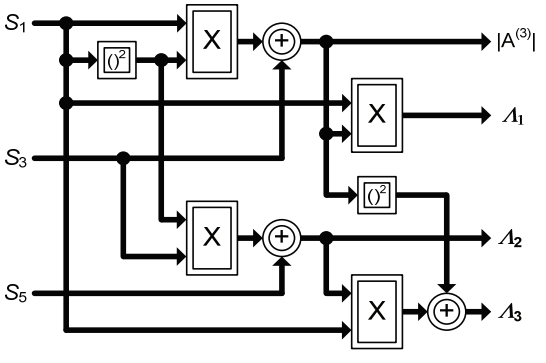

그림 3 오류위치다항식 계산 회로
Figure 3. Error location polynomial computation circuit

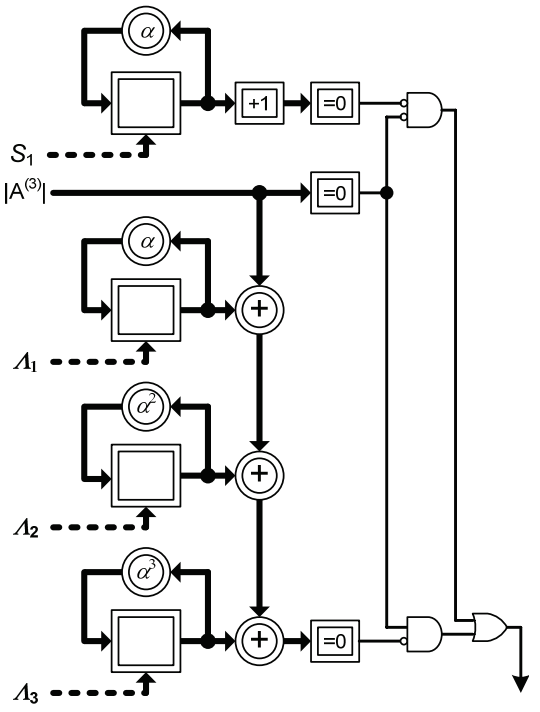

그림 4 오류위치 탐지회로
Figure 4. Error location searching circuit

4. 결 론

BCH 부호의 복호 과정 중에서, 기존의 Peterson 방법에서는 오증으로부터 오류위치다항식을 구할 때 유한체 $GF(2^m)$상의 나눗셈이 필요하였다. 유한체 $GF(2^m)$상의 임의의 두 원소 사이의 나눗셈은 일반적으로, 한 원소의 역원에 다른 원소를 곱하는 것으로, 곱셈기와 역원기를 포함하고 있는 것이다. 따라서 장치화가 대단히 복잡하고 어렵다.

본 논문에서는 기존의 오류위치다항식을 변형한 새로운 오류위치다항식을 사용하여, 나눗셈을 생략한 3중 오류정정 BCH 부호의 복호기를 설계하였다. 설계된 복호기는 기존의 Peterson 방법으로 장치화한 복호기보다 훨씬 간단한 하드웨어로 장치화 할 수 있다.

References

[1] Y. Lee, H. Yoo, I. Yoo, and I. C. Park, *High-throughput and low-complexity BCH decoding architecture for solid-state drives*, IEEE Transactions on Very Large Scale Integration Systems, Vol. 22, No. 5, pp. 1183-1187, 2014.

[2] C. H. Yang, T. Y. Huang, M. R. Li, and Y. L. Ueng, *A 5.4㎽ soft-decision BCH decoder for wireless body area networks*, IEEE Trans- actions on Circuits and Systems, Regular Papers, Vol. 61, No. 9, pp. 2721-2729, 2014.

[3] X. Zhang, and Z. Wang, *A low-complexity three-error-correcting BCH decoder for optical transport network*, IEEE Transactions on Circuits and Systems II, Express Briefs, Vol. 59, No. 10, pp. 663-667, 2012.

[4] Y. M. Lin, C. L. Chen, H. C. Chang, and C. Y. Lee, *A 26.9K 314.5 Mb/s soft (32400, 32208) BCH decoder chip for DVB-S2 system*, IEEE Journal of Solid-State Circuits, Vol. 45, No. 11, pp. 2330-2340, 2010.

[5] M. Y. Rhee, *Error-correcting coding theory*, McGraw-Hill, 1989.

[6] W. W. Peterson, and E. J. Weldon, *Error-correcting cods*, MIT Press, 1972.

[7] W. W. Peterson, *Encoding and Error correction procedure for Bose-Chaudhuri codes*, IRE Transaction on Information Theory, Vol. IT-6, pp. 459-470, 1960.

[8] E. R. Berlekamp, *Algebraic coding theory*, McGraw-Hill, 1968.

[9] J. L. Massey, *Shift register synthesis and BCH decoding*, IEEE Transactions on Information Theory, Vol. IT-15, pp. 125-127, 1969.

[10] Y. Sugiyama, Y. Kasahara, S. Hirasawa, and

T. Namekawa, *A method for solving key equation for goppa codes*, Information and Control, Vol. 27, pp. 87-99, 1975.

[11] S. B. Wicker, *Error control systems for digital communication and storage*, Prentice Hall, 1995.

[12] R. Lidl, and H. Niederreiter, *Introduction to finite fields and their applications*, Cambridge University Press, 1994.

[13] T. Itoh, and S. Tsujii, *A fast algorithm for computing multiplicative inverses in using normal bases*, Information and Computation, Vol. 78, No. 39, pp. 21-40, 1988.

[14] S. Lin, and D. Costello, *Error control coding: Fundamentals and applications*, Pearson, Prentice-Hall, 2004.

[15] R. T. Chien, *Cyclic decoding procedure for the bose chaudhuri hocquenghem codes*, IEEE Transactions on Information Theory, IT-10, pp. 357-363, 1964.

3중 오류정정 BCH 부호의 저복잡도 복호기 설계

조용석, 신용달

유원대학교 정보통신보안학과

요 약

BCH 부호는 순회부호의 일종으로 강력한 다중오류 정정 능력을 가지고 있다. 2진 BCH 부호는 강력한 오류정정 능력과 적당한 하드웨어 비용으로 인하여 데이터통신과 데이터 저장 시스템 등에 널리 사용되고 있다. 본 논문에서는 Peterson의 복호방법을 개선한 3중 오류정정 BCH 부호의 저복잡도 복호기 설계 방법을 제안한다. 제안된 복호기는 오류위치다항식을 계산하는데 있어서 유한체 $GF(2^m)$ 상의 모든 나눗셈을 제거한 것이다. BCH 부호는 유한체 $GF(2^m)$ 상에서 정의되며 모든 연산이 이 위에서 이루어진다. 유한체 $GF(2^m)$ 상의 연산 중에서 가장 어렵고 복잡한 것이 나눗셈이며, BCH 부호의 종래의 복호 방법에서는 나눗셈이 필요하였다. 본 논문에서는 나눗셈이 생략된 3중 오류정정 BCH 부호의 복호기를 설계한다. 설계된 복호기는 LFSR과 논리 게이트들로 구현되는 오증 계산회로, 오류위치다항식 계산회로, 오류위치 탐지회로로 구성된다. 본 복호기는 매우 간단한 하드웨어로 구현할 수 있는 장점을 가지고 있다. 또한 제어회로도 매우 간단하고, 복호지연도 오증계산에 걸리는 한 블록만큼만 소요되므로 수신 시퀀스를 저장하는 버퍼 메모리를 절약할 수 있다.

Yong-Suk Cho received the B.S., M.S., and Ph.D. degree in the Department of Electronic Communication Engineering from Hanyang University in 1986, 1988 and 1998, respectively. From 1989 to 1996, he was a researcher at Korea Telecom. He has been a professor in the Department of IT & Securities at U1 University since 1996. His current research interests include finite field arithmetic, cryptography, and error-control coding.

E-mail address: yscho@u1.ac.kr

Yong-Dal Shin received Ph.D. degree from Kyung-pook national university, Daegu Korea, 1994. He has been a professor in the Department of IT & Securities at U1 University since 1996. He research areas include multimedia security, digital watermarking, digital forensics.

E-mail address: ydshin@u1.ac.kr