

MB-OFDM UWB 를 위한 RS 복호기 설계

최성우 *, 신철호*, 최상성*
 ETRI 디지털홈연구단 무선홈네트워크연구팀
 csw9908, chshin, sschoi@etri.re.kr

A Design of RS Decoder for MB-OFDM UWB

Sung-Woo Choi *, Cheol-Ho Shin, Sang-Sung Choi *
 Wireless Home Network Research Team, ETRI

Abstract — UWB is the most spotlighted wireless technology that transmits data at very high rates using low power over a wide spectrum of frequency band. UWB technology makes it possible to transmit data at rate over 100Mbps within 10 meters. To preserve important header information, MB-OFDM UWB adopts Reed-Solomon(23,17) code. In receiver, RS decoder needs high speed and low latency using efficient hardware. In this paper, we suggest the architecture of RS decoder for MB-OFDM UWB. We adopts Modified-Euclidean algorithm for key equation solver block which is most complex in area. We suggest pipelined processing cell for this block and show the detailed architecture of syndrome, Chien search and Forney algorithm block. At last, we show the hardware implementation results of RS decoder for ASIC implementation.

Keywords — UWB, Reed-Solomon, Channel code

1. 서론

UWB는 수 GHz 대 초광대역을 사용하는 초고속 데이터 무선 전송 기술을 말한다. UWB 는 기존 기술에 비해 상당히 저 전력으로 10m 내 근거리에서 100Mbps 급 전송이 가능한 기술이다. 따라서 근거리에서 고속 통신을 요구하는 홈네트워크에 적합한 무선 통신 기술이다. UWB 는 IEEE 802.15.3a 에서 표준화가 이루어지고 있으며, DS-UWB 와 MB-OFDM UWB의 경쟁이 치열한 상황이다. 따라서 시장을 선점하기 위하여 두가지 방식 모두 칩을 제작하고 상용화에 노력하고 있다. 본 논문은 두 방식 가운데 MB-OFDM UWB에 대하여 프레임 전송율을 높이기 위해 추가된 Reed-Solomon 부호의 구현에 중점을 둔다.

MB-OFDM UWB의 데이터 프레임은 PLCP 프리앰블, PLCP 헤더 그리고 PSDU 로 구성된다. 수신단은 PLCP 프리앰블과 헤더를 사용하여 신호를 감지하고 복조를 시작한다. PLCP 헤더는 PHY 와 MAC 이 데이터를 복조하는데 필수적인 정보를 포함하고 있다. 다음 그림은 PLCP 헤더를 나타낸다. [1]

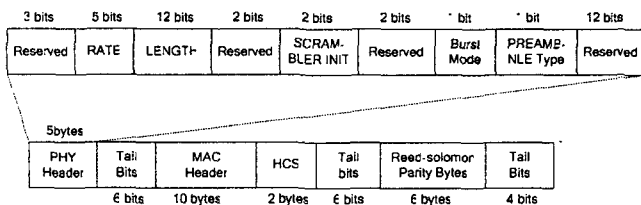


Fig. 1. PLCP Header structure

PLCP 헤더의 중요 정보가 전송 도중에 손상되는 것을 막기 위해서 송신단은 외부 코드로 Reed-Solomon 부호를 사용하도록 하였다. 그림 1에서 PHY 헤더와 MAC 헤더 그리고 HCS 의 총 17byte 정보는 scrambler를 통과한 후, Reed-Solomon (23,17) 부호를 사용하여 인코딩 되고 6 byte 의 패리티가 부가 되어 전송 된다. 이 코드는 패리티 byte를 포함하여 최대 3 bytes 의 에러를 정정 할 수 있다.

이 RS(23,17) 코드는 RS(255,249) 코드의 shortend 형태를 갖는다. RS(255,249) 의 생성 다항식은 다음과 같다.

$$g(x) = \prod_{i=1}^6 (x - \alpha^i) = x^6 + 126x^5 + 4x^4 + 158x^3 + 58x^2 + 49x + 117 \quad (1)$$

송신 코드워드 다항식 $c(x)$ 는 메시지 다항식 $m(x)$, 생성 다항식 $g(x)$ 와 다음의 관계를 지닌다.

$$c(x) = x^{N-k}m(x) + [x^{N-k}m(x) \bmod g(x)] = q(x)g(x) \quad (2)$$

MB-OFDM UWB 는 RS 부호의 systematic 특성을 이용하여, 송신단에서는 필수적으로 지정하였으나, 수신단은 optional 로 RS 복호기를 사용하였다. 따라서 수신단에서의 RS 복호기의 면적이나 추가 지연등의 분석이 필요하다. 이에 본 논문은 MB-OFDM에서 추가 제안한 Reed-Solomon 부호에 대하여 적합한 알고리즘을 소개하고, 하드웨어 구현에 필요한 구조를 제시하고자 한다.

2. Modified Euclidean 알고리즘

이 장에서는 RS 복호기의 디코딩 알고리즘을 설명한다. [2] 먼저, $GF(2^m)$ 을 2^m 개의 원소로 구성된 Galois 유한 필드라 정의한다. $GF(2^m)$ 을 기반으로 하는 RS(N, k) 부호에서, $N = 2^m - 1$ 은 한 심볼이 m-bit로 구성된 RS(N,k) 코드의 길이를 나타내고, $k = N - (d - 1)$ 은 m-bit 정보의 길이를 나타낸다. 여기서 d는 $GF(2^m)$ 의 design distance 이며, 정정 가능한 에러의 수가 t 일 때, $d = 2t + 1$ 이다.

전송하려는 정보를 나타내는 다항식을 $c(x)$, 수신단에서 수신된 신호를 나타내는 다항식을 $r(x)$, 발생한 에러를 나타내는 다항식을 $e(x)$ 라 하자. 만약 전송 중에 v개의 에러가 발생 했다면, 에러 위치 다항식은 다음 식과 같다.

$$\Lambda(x) = \prod_{i=1}^v (1 + xX_i) = \lambda_0 + \lambda_1x + \dots + \lambda_vx^v \quad (3)$$

그리고 에러 크기 다항식 $\Omega(x)$ 는 다음 식과 같다.

$$\Omega(x) = \omega_0 + \omega_1 x^1 + \dots + \omega_{v-1} x^{v-1} \quad (4)$$

RS 디코딩은 신드롬 계산 단계, key equation 해석 단계, 에러 위치와 에러크기 연산의 3단계로 이루어진다.

먼저 receiver 에 수신된 신호에 대하여 신드롬을 계산한다. 신드롬 다항식 $S(x)$ 의 계수는 수신된 $r(x)$ 에 생성다항식의 근을 대입하여 다음 식과 같이 구한다.

$$S_j = r(\alpha^j) = \sum_{i=0}^{N-1} r_i (\alpha^j)^i, \quad 1 \leq j \leq 2t \quad (5)$$

위 식(5)에서 송신 코드워드 다항식 $c(x)$ 는 생성 다항식 $g(x)$ 과 $q(x)$ 의 곱이므로, $g(x)$ 의 근인 α^j 를 대입하면 제로이다. 따라서 다음의 관계가 성립한다.

$$S_j = r(\alpha^j) = c(\alpha^j) + e(\alpha^j) = e(\alpha^j) \quad (6)$$

즉, 신드롬 다항식이 제로가 아니면 수신 신호에 에러가 있음을 나타내며, 신드롬 값이 에러의 위치와 크기를 찾는데 사용된다. 계산된 신드롬과 에러 위치 다항식 $\Lambda(x)$, 에러 크기 다항식 $\Omega(x)$ 은 다음과 같은 관계를 가지며, 이를 key equation 이라 한다.

$$S(x) \cdot \Lambda(x) = \Omega(x) \text{ mod } x^{2t} \quad (7)$$

위 key equation 을 풀어내기 위하여 Berlekamp-Massey 알고리즘 (BM)[3], Euclidean 알고리즘[4]이 사용된다. Euclidean 알고리즘은 다항식의 나눗셈이 필요하여 연산이 복잡하므로, 이를 개선한 modified-euclidean 알고리즘(ME)이 제안되었다.[5][6] ME는 다항식끼리의 나눗셈을 없애고, 한 심볼에 대해서 나눗셈이 하나만 필요한 방법으로써, 나눗셈을 위한 inverse rom 만 있으면 된다.

만약, erasure 에 대한 고려를 하지 않는다면, ME 알고리즘은 다음과 같다.

먼저 $i=0$ 일 때의 다항식의 초기값을 설정한다.

$$\begin{aligned} R_0(x) &= x^{2t} & Q_0(x) &= S(x) \\ L_0(x) &= 0 & U_0(x) &= 1 \end{aligned} \quad (8)$$

초기값을 설정한 후, $i \geq 1$ 인 경우에는 새로운 다항식을 다음과 같이 계산한다.

$$\begin{aligned} R_i(x) &= [\sigma_{i-1} b_{i-1} R_{i-1}(x) + \bar{\sigma}_{i-1} a_{i-1} Q_{i-1}(x) \\ &\quad - x^{l_{i-1}} [\sigma_{i-1} a_{i-1} Q_{i-1}(x) + \bar{\sigma}_{i-1} b_{i-1} R_{i-1}(x)] \\ Q_i(x) &= \sigma_{i-1} Q_{i-1}(x) + \bar{\sigma}_{i-1} R_{i-1}(x) \\ L_i(x) &= [\sigma_{i-1} b_{i-1} L_{i-1}(x) + \bar{\sigma}_{i-1} a_{i-1} U_{i-1}(x) \\ &\quad - x^{l_{i-1}} [\sigma_{i-1} a_{i-1} U_{i-1}(x) + \bar{\sigma}_{i-1} b_{i-1} L_{i-1}(x)] \\ U_i(x) &= \sigma_{i-1} U_{i-1}(x) + \bar{\sigma}_{i-1} L_{i-1}(x) \end{aligned} \quad (9)$$

여기서,

$$\begin{aligned} l_{i-1} &= \deg(R_{i-1}(x)) - \deg(Q_{i-1}(x)) \\ \sigma_{i-1} &= 1 & l_{i-1} < 0 \\ \sigma_{i-1} &= 0 & l_{i-1} \geq 0 \end{aligned} \quad (10)$$

이고, a_{i-1} , b_{i-1} 은 각각 $R_{i-1}(x)$ 과 $Q_{i-1}(x)$ 의 최고차항의 계수이다. 이 알고리즘은 $\deg(R_{i-1}(x)) < t$ 이면 반복을 중지한다. 그리하면, 에러 위치다항식과 에러 크기 다항식은 다음과 같다.

$$\Lambda(x) = L_i(x), \quad \Omega(x) = R_i(x) \quad (11)$$

에러 위치 다항식 $\Lambda(x)$ 의 근을 구하면 에러의 위치를 찾을 수 있다. 이 때 사용하는 알고리즘이 Chien search 알고리즘이다. Chien search 알고리즘은 에러 위치 다항식에 생성다항식의 근 α^i 을 차례대로 입력하여, $\Lambda(\alpha^i) = 0$ 이면, $X_i = \alpha^{-i}$ 이 에러의 위치이다.

에러의 크기는 Forney 알고리즘을 계산하면 된다. Forney 알고리즘에 의한 에러의 크기는 다음과 같이 계산한다.

$$Y_i = \frac{\Omega(x)}{\Lambda'(x)} \Big|_{x=\alpha^i} \quad (12)$$

여기서 $\Lambda'(x)$ 는 $\Lambda(x)$ 의 미분 다항식이다. 디코더는 $x = \alpha^i$, ($1 \leq i \leq N$)를 Chien search 알고리즘과 Forney 알고리즘에 입력하여, 에러의 위치를 찾고 에러값을 찾는다.

이상의 RS 디코더의 블록도는 다음 그림과 같다.

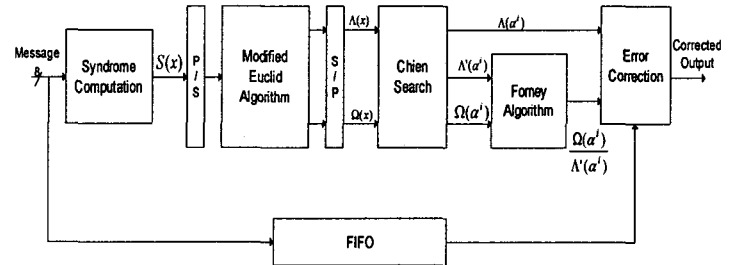


Fig. 2. RS decoder architecture

3. Reed-Solomon 복호기 구조

MB-OFDM UWB 를 위하여 제안된 RS 복호기는 가장 큰 부분을 차지하는 Key equation 해석 부분을 위해서 ME 알고리즘을 사용한 구조를 채택하였다. ME 알고리즘은 다항식 나눗셈이 필요없어 회로가 간단하고 고속 전송을 위한 파이프라인 삽입이 간단한 systolic array 구조로 설계가 용이하다. 본 장은 ME 블록을 포함한 주요 블록의 구조를 설명한다.

3.1 신드롬 계산

RS(23, 17) 부호를 사용하여 수신된 총 23 bytes 의 신드롬 계산 블록의 입력 신호열을 다음 식으로 정의한다.

$$v(x) = v_{22}x^{22} + v_{21}x^{21} + v_{20}x^{20} + \dots + v_1x + v_0 \quad (13)$$

신드롬 회로는, 생성 다항식의 근, $\alpha^i (i=1, 2, \dots, 2t)$ 을 사용하여 식(14)의 계산을 수행한다.

$$\begin{aligned} S_1 &= v(\alpha) \\ S_2 &= v(\alpha^2) \\ &\dots \\ S_6 &= v(\alpha^6) \end{aligned} \quad (14)$$

그림 3 은 신드롬 계산 셀을 나타내고, 그림 4 는 이 신드롬 계산 셀을 이용한 신드롬 계산 블록의 구조를 나타낸다.

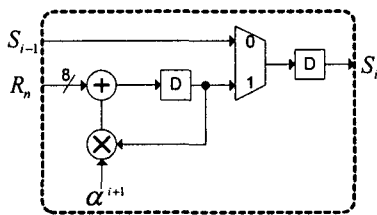


Fig. 3. 신드롬 계산 셀

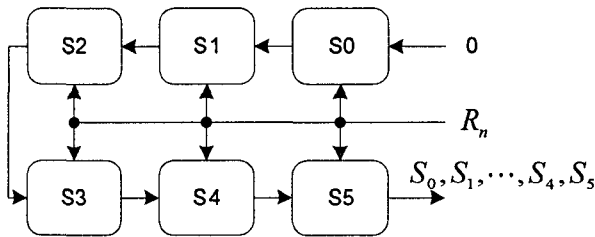


Fig. 4. 신드롬 계산 블록

각 셀은 GF(2⁸) constant 곱셈기와 덧셈기, Multiplexer 로 구성되며, 입력신호 길이 23 bytes 동안 연산을 하고, 계산이 끝나면 S5 셀에 저장된 값부터 차례 대로 ME 블록으로 출력한다.

3.2 ME 블록

비교적 많은 숫자의 에러 정정이 필요한 RS 복호기에서 key equation 해석 블록은 전체 RS 복호기 하드웨어의 60~70 % 를 차지한다. 그러나 본 시스템이 사용하는 RS(23,17) 코드는 3 byte의 에러정정이 필요하므로 다른 시스템에 비해서 적은 key equation 해석 블록이 필요하다. 따라서 본 MB-OFDM UWB 시스템은 고속 동작을 위한 in-out throughput 딜레이가 중요한 고려 사항이 된다.

위 장에서 설명한 ME 알고리즘 연산을 위한 하드웨어 구조는 systolic array 형태로 연산셀을 연결한 구조가 파이프 라인 삽입이 용이하여 고속 통신에 적합하므로 선택하였다. 본 시스템이 정정 가능 에러수가 3 이므로 총 6개의 ME 연산 셀 을 가지며, 전체 ME 블록의 구조는 다음 그림과 같다.

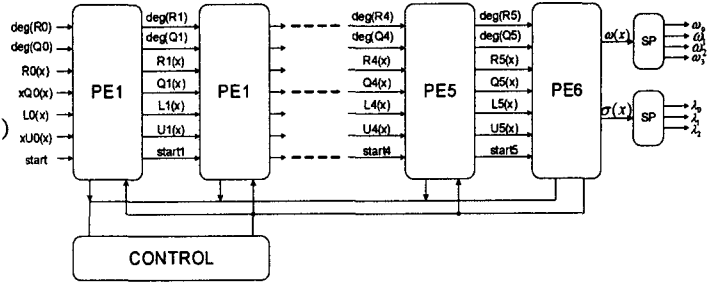


Fig. 5. ME processing block

본 논문은 파이프라인된, low latency ME 알고리즘 연산 셀을 제안하였다. 제안된 연산 셀은 degree computation 블록과 processing arithmetic 블록으로 구성된다[7]. Degree computation 블록은 입력된 다항식의 차수를 비교하여 교환 신호를 발생하고, 차수가 t 보다 적으면, 알고리즘의 연산을 중지하도록 stop 신호를 뒤에 연결된 셀에 내보낸다.

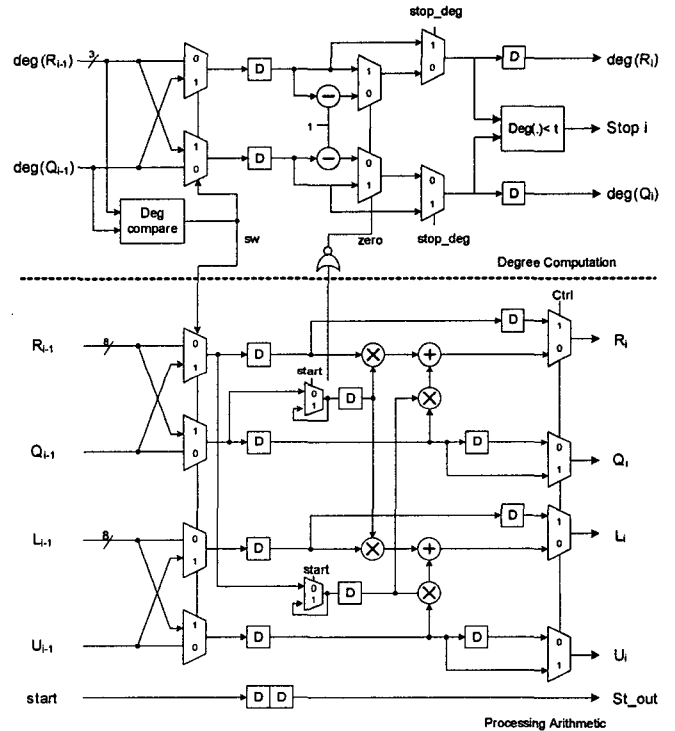


Fig. 6. ME 연산 element

ME 연산 element 에서 입력된 신호는 2단의 D flip-flop 을 거쳐 출력 신호를 내보낸다. 각 element는 2개의 딜레이 를 가지므로 ME 연산 블록은 12개의 지연 후에 출력을 내보 낸다. 그림 5의 제어회로는 각 element 에서 오는 중지 신호 를 검사하여, ME 연산이 끝나면 출력 버퍼에 저장된 에러 위치 다항식과 에러 크기 다항식을 병렬적으로 출력한다.

3.3 Chien search 및 Forney 블록

Chien search 블록은 ME 블록에서 입력된 에러 위치 다항식의 계수를 초기값으로 설정하고, 다항식에 $\alpha^{233}, \alpha^{234}, \dots, \alpha^{254}, \alpha^{255} = 1$ 을 대입하여 $\Lambda(\alpha^n) = 0$ 인 n 을 찾으

α^{-n} 에 에러가 존재한다. $\alpha^{-n} = \alpha^{(N-n) \bmod N}$ 이므로 RS 디코더 입력이 FIFO를 통과한 후의 값에 대응한다. α^{233} 을 대입하였을 때 계산값이 제로이면 인코딩 정보의 첫 번째 심볼인 v_{22} 에 에러가 있고, α^{255} 를 대입하였을 때 제로이면 v_0 에 에러가 있음을 의미한다.

Chien search 블록은 $\Lambda(\alpha^i)$ 를 계산하여 에러 정정부에 내보내고, 그 미분값인 $\Lambda'(\alpha^i)$ 를 구하여 Forney 블록으로 serial 하게 보낸다. 각 계수의 초기값을 로딩하고 α^i 곱하는 동작을 하는 Chien search 셀은 그림 7과 같으며, 이 셀을 사용한 Chien search 블록은 그림 8에 나타내었다.

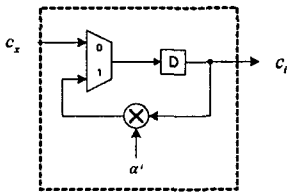


Fig. 7. Chien search cell

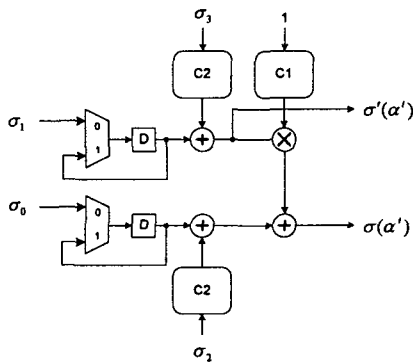


Fig. 8. Chien search 블록

Galois 필드에서 짝수 차 항은 미분하면 제로가 된다. 즉 $\Lambda(x) = \Lambda_{\text{even}}(x) + \Lambda_{\text{odd}}(x)$ 일 때, $\Lambda_{\text{odd}}(x) = x \cdot \Lambda'(x)$ 이다. 따라서 그림 8과 같이 $\Lambda_{\text{even}}(x)$, $\Lambda_{\text{odd}}(x)$ 를 구하고 나서 $\Lambda(x)$ 를 구하면, 따로 $\Lambda(\alpha^i)$ 를 계산하는 회로가 필요 없게 된다. [6]

Forney 블록은 ME 블록으로부터 에러 위치 다항식 $\Omega(x)$ 를 입력받아 그림 7과 같은 셀에 저장하고, 다항식에 α^{233} , α^{234} , ..., α^{254} , $\alpha^{255} = 1$ 을 대입하여 $\Omega(\alpha^i)$ 를 생성한다. Forney 블록은 에러의 크기를 생성하는데, 에러의 크기는 식 (12)로 구한다. 여기 포함된 나눗셈을 실행하기 위해 8 bits 255 word 로 구성된 ROM 에 $GF(2^8)$ 의 inverse 값을 저장한다. ROM은 입력된 $\Lambda(\alpha^i)$ 에 따라 그 inverse 값을 multiplier 로 출력하여 $\Omega(\alpha^i)$ 와 곱셈을 수행한다. 연산된 에러크기는 Chien search 출력과 AND 연산 되고, FIFO를 거친 출력과 xor 되어 에러를 정정한다.

Forney 블록은 Chien search 블록에 사용되었던 같은 셀을 사용한다. Forney 블록과 에러 정정 블록의 관계는 다음 그림과 같다.

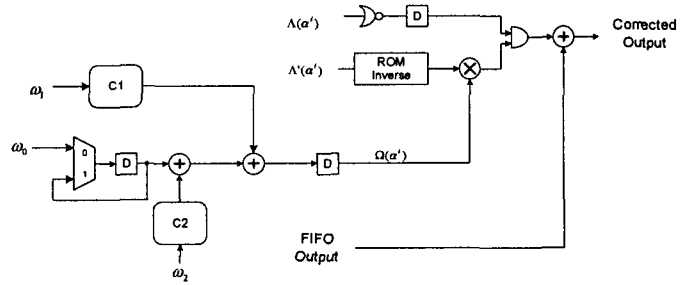


Fig. 9. Forney 블록과 에러 정정 블록

4. Hardware implementation result

제안된 구조를 이용한 RS 복호기를 UWB 칩 제작에 활용하기 위하여 verilog 코딩 후, TSMC 0.18um 라이브러리를 사용하여 합성 하였다.

제안된 RS 복호기의 총 latency 는 46 심볼 클럭이며, RS 복호기의 FIFO 도 같은 크기의 dual port RAM을 사용하여 구현하였다. 하드웨어 합성 결과 총 면적은 27k 게이트를 차지하였고, 동작 주파수는 232MHz 심볼 주파수로서, 최대 1.6Gbps 급 데이터 전송이 가능한 것이다. 이것은 적은 면적으로 RS 복호기가 구현이 가능함을 암시한다.

한편, MB-OFDM UWB 는 헤더 부분만 RS 부호를 사용하는 데, 이를 확장하여 데이터에도 사용하기 위해서 RS(255,239) 코드를 사용하고 본 논문에 제시한 RS 복호기의 구조를 사용하면, 면적은 78k gates 로 증가한다. 본 논문의 구조는 하나의 셀을 반복 사용하는 recursive 방법에 비하여, 면적은 증가하지만 latency 적고, high pipelined 방법에 비해 동작 속도는 낮지만, latency와 면적이 적은 장점이 있다.

5. 결론

본 논문은 MB-OFDM UWB 에서 헤더를 보호하기 위해서 추가한 RS(23,17)코드에 대해서 연구하였다. RS 코드의 구조를 제시하기 위하여, 적합한 알고리즘을 연구하였으며, 적은 하드웨어를 차지하며, 출력까지의 지연이 적은 구조를 연구하였다. 제안된 구조는 복잡성이 가장 높은 key equation 연산 블록을 위해서 modified-euclidean 알고리즘을 사용하였다. ME 블록을 위해서 내부 지연 단이 2인 pipelined 연산셀을 설계하였다. 설계된 연산셀은 구조가 간단한 systolic array 구조로써, 다른 RS 코드로 확장이 쉽다. 그리고 추가 파이프라인 삽입이 용이하므로, 고속 동작을 위한 critical path 단축이 쉬운 장점이 있다. 제안된 RS 복호기의 하드웨어 합성 결과에 따르면 면적은 27k gates 를 차지하였으며, 출력까지의 latency 는 46 클럭이다. 제안된 구조는 모듈 형태로 쉽게 확장할 수 있으며, 제안된 구조를 확장하여 전체 UWB 프레임에 RS 코드를 적용한다면 RS 복호기의 하드웨어가 약 3배 정도 증가함을 알 수 있었다.

REFERENCES

[1] <http://ftp.802wirelessworld.com/15/04/15-04-0268-03-003a-Multiband-OFDM-CFP-Doc>

- [2] S. B. Wicker, Error Control Coding : Fundamentals and Applications. Englewood Cliffs, NJ: Prentice-Hall, 1983.
- [3] H. M. Hsu, C. L. Wang, "An area-efficient pipelined VLSI architecture for decoding of Reed-Solomon codes based on a time-domain algorithm", IEEE Trans. Circuits Syst. Video Technol., vol. 7, pp. 864-871, Dec. 1997
- [4] T. K. Matsushima, T. Masuchima, and S. Hirasawa, "Parallel architecture for high-speed Reed-Solomon decoder," IEEE Trans. Comput., vol. C-34, pp. 393-403, May 1985
- [5] H. M. Shao, T. K. Truong, L. J. Deutsch, J. H. Yuen, and I. S. Reed, "A VLSI design of a pipelined Reed-Solomon decoder", IEEE Trans. Comput., vol. C-34, pp. 393-403, May 1985
- [6] H. M. Shao, I. S. Reed, "On the VLSI Design of Pipelined Reed-Solomon Decoder Using Systolic Arrays", IEEE Trans. Comput., vol 37, pp. 1273-1280, Oct. 1998
- [7] H. Lee, "High-speed VLSI architecture for Parallel Reed-Solomon Decoder", IEEE Trans. Very Large Scale (VLSI) Integr. Syst., vol. 11, no.2, pp. 288-294, Apr. 2003

M E M O