2003년도 대한전기학회 하계학술대회 논문집 2003.7.21-23

초고속 전력선 통신을 위한 오류정정 부호화기 설계

최성수, 박해수, 이재조, 이원태, 김관호
한국전기연구원, 서울전기시험연구소, 전기정보망기술연구그룹

Design of Error Correction Encoder for High-Speed PLC Systems

Sungsoo Choi, Haesoo Park, Jaejo Lee, Wontae Lee, Kwanho Kim
Korea Electrotechnology Research Institute, Power Telecommunication Network Reaearch Group

Abstract - 본 논문은 전력선통신시스템 (Power Line Communications)을 위한 초고속 오류정정 부호화기 회로에 관한 설계방법론과 회로의 동작속도, 회로복잡성과 레이턴시에 직접적으로 기여하는 핵심 GF (Galois Field) 연산기들의 역할 및 이들의 설계결과에 관해 설명한다. 특히, 이러한 설계방법에 충실한 오류정정 부호화기회로는 입출력 병렬구조의 세미-시스톨릭 (Semi-systolic) 아키텍처를 갖는 고속의 내부 핵심 GF 연산기 회로들을 채택함으로써 고속 연산을 가능토록 한다. 최적화된 GF곱셈연산기를 기반으로 설계되어진 리드-솔로몬 (Reed-Solomon) 오류정정 부호화기는 전력선 채널상에서 데이터를 전송 시 발생되는 연집오류들을 효과적으로 복원하도록 하는 대표적인 부호화기로 이미 존재하는 다른 회로들에 비해 동작속도, 회로의 복잡성, 및 레이턴시 측면에서 그 성능이 월등히 뛰어나므로, 실제 초고속 전력선 통신시스템의 설계 및 구현 시 효과적으로 이용될 수 있다.

1. 서 론

전력선 통신시스템은 전력선 채널의 특성상 무선채널에 비해 감쇄, 다중경로문제와 페이딩왜곡이 심하다. 이러한 전력선 채널환경에서 단지 단순한 변복조 신호처리에 의한 정확한 정보전달은 어려우며, 이에 대한 충분한 신뢰성보장을 위해서는 오류정정 부호라는 다양한 신호처리 기술들이 필요하다. 이들 중 리드-솔로몬부호는 전력선에서 임의로 발생되는 군집오류들을 궤환 신호처리없이 효과적으로 복호해 낼 수 있는 강력한 전방향 오류정정 부호 (Forward Error Correction Code)로 알려져 있다 [13]. 이러한 리드-솔로몬부호는 전력선 통신시스템은 물론 CD 플레이어, 우주탐사선에 이르기까지 그 응용분야가 다양하다. 또한 최근 유무선 통신을 통해 대용량의 고속 동영상 정보 전달이 크게 요구되어지고 있으며, 이러한 서비스를 성공적으로 이끌기 위한 통신시스템의 고속화는 필수적 이라 할 수 있다. 이러한 고속 통신시스템 회로설계의 경우, 상위레벨의 기능적 모듈별에서부터 게이트레벨, 또는 회로레벨 등 각 레벨별 아키텍처 신호전달의 병목현상을 해소시킴으로써 해결되어질 수 있다. 그러나 현재의 일반적인 통신설계기술들은 낮은 속도에서 동작되는 통신응용에 관련되어 있어서, 결과적으로 고속에 관련된 응용 서비스들을 제공하기에는 어려움이 따른다. 그러므로 비록 설계하고자 하는 아키텍처가 동일한 알고리듬을 이용한다고 하더라도, 시스템 전체의 성능을 결정하는 기본 GF (Galois-Field) 산술연산기들 [1-10]부터 최적화된 새로운 회로의 고집적화 기술 아키텍처로 설계할 필요가 있다.

본 논문에서는 먼저 산술연산레벨에 대해서 게이트레벨의 파이프라이닝, 병렬처리 아키텍처기술을 효과적으로 사용하는 설계방법을 설명한다. 제안된 GF 산술연산기를 리드-솔로몬 오류정정 부호화기에 채택함으로 하여 신호처리의 병목현상을 근원적으로 해결함과 동시에 리드-솔로몬 오류정정부호화기 자체의 아키텍처 또한 낮은 복잡도의 특성을 갖도록 설계하는 방법에 대해 설명한다.

2. 리드-솔로몬 오류정정 부호화기

2.1 GF 연산기

GF (Galois Field) 연산은 유한체이론[13]에 기본을 두고 있으며 암호화 프로토콜 및 통신의 부호화기에 직접적으로 이용되는 기본 연산 방식이다. GF 연산기들 중 덧셈기와 곱셈연산은 응용시스템의 기초연산으로 필수사항이다. 특히 GF덧셈연산이 단순히 각 입력다항식의 계수간 XOR연산인 반면, GF곱셈연산은 다소 복잡한 구조로 전체 시스템 동작의 병목부분이 되어진다. 이러한 병목부분을 해결한 표준기저형 (Standard-Basis Type) 고속 GF곱셈 연산기는 병렬구조의 세미-시스톨릭 아키텍처로 설계되어 질 수 있다. 최 성수 외2명[14]에 의해 설계되어진 고정상수 값을 갖는 고속 GF 세미-시스톨릭 곱셈 연산기는 그림 1과 같이 m x m 의 일반화된 곱셈기셀(GMC)들로 이루어져 있으며, 각 곱셈기셀들은 GF (2^m)를 구성하는 원시다항식 $F(x)$에 의해 단순화된 두 개의 고정된 곱셈기셀 (FMC)들로 설계되어져 곱셈기의 복잡도에 관한한 그림 2에 보인 바와 같이 그 성능이 향상됨을 알 수 있다. 실제, 0.25 μm의 표준형 셀합성 VLSI (고집적회로)테크날리지를 이용하여 GF(256) 곱셈기를 합성할 경우, 레이턴시 9의 최악의 조건에서 580 MHz의 동작속도를 갖는다. GF 곱셈기의 연산은 곱셈다항식 $P(x)$, 입력다항식 $A(x)$와 $B(x)$ 그리고 원시다항식 $F(x)$ 변수들에 의해서 병렬 반복 및 순차적으로 계산되어진다.

그러므로 GF곱셈은 $P(x) = A(x)B(x) \bmod F(x)$에 의해 계산되어진다. 여기서 각 다항식을 표준기저형 유한체 변수로 표현할 경우, 다음과 같이 쓸 수 있다.

$$P(x) = \sum_{i=0}^{m-1} p_i\alpha^i, A(x) = \sum_{i=0}^{m-1} a_i\alpha^i, B(x) = \sum_{i=0}^{m-1} b_i\alpha^i,$$

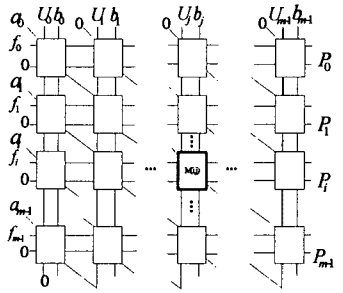

그림 1: 곱셈기셀 M(i,j)로 구성된 고속 GF 세미-시스톨릭 곱셈 연산기 구조.

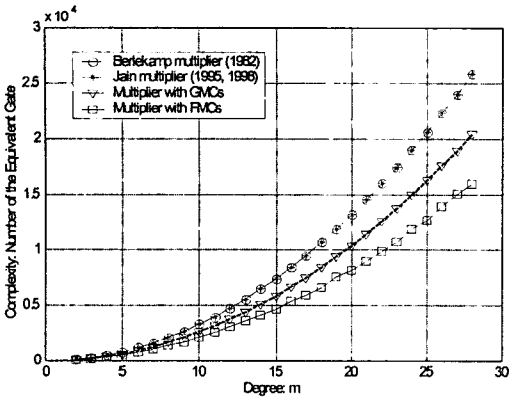

그림 2: 일반화된 곱셈기셀(GMC)로 구성된 곱셈기, 고정화된 곱셈기셀(FMC)로 구성된 곱셈기와 대표적인 다른 곱셈기들 간의 하드웨어 복잡성.

그리고 $F(x) = f_m + \sum_{i=0}^{m-1} f_i$ 이다.

2.1.1 오류부호화기 내 $2t$개의 GF 곱셈연산기 설계

리드-솔로몬 부호화기에 응용되어질 GF 곱셈 연산기는 부호화기의 구조상 $2t$개의 GF 곱셈연산기들이 반드시 필요하게 된다. 여기서 t는 부호화기의 오류정정능력지수를 나타내는 값으로 (255,239) 리드-솔로몬 부호의 경우 $t=8$, 즉 8바이트의 군집오류를 정정할 수 있다. 만약 16개의 GF 곱셈기들을 아래 수식과 같이 반복하여 사용할 경우 부호화기의 복잡도는 기본 곱셈연산기의 16배로 증가되어진다.

$$P_0 = AB_0 = \sum_{n=0}^{m-1} (A\alpha^n) b_n^{(0)},$$

$$P_1 = AB_1 = \sum_{n=0}^{m-1} (A\alpha^n) b_n^{(1)}, \ ...,$$

$$P_{15} = AB_{15} = \sum_{n=0}^{m-1} (A\alpha^n) b_n^{(15)},$$

하지만 위 식의 $(A\alpha^n)$이 GF 곱셈 연산내 공통부분으로 들어가 있다는 사실을 주의한다면 16개의 GF곱셈기들을 또 다른 하나의 GF 곱셈기꼴의 연산기로 설계할 수 있다. 이렇게 설계되어진 단순화된 GF곱셈기셀의 구조는 그림 3과 같다. 이전 절에 소개되었던 고정화된 곱셈기셀 (FMC)구조와 같이 원시다항식의 계수값에 의해 (a)와 (b) 두개의 곱셈기셀들로 설계되어질 수 있다.

더욱이 오류부호화기 내 GF 곱셈 연산기들의 입력 다항식 B들이 항상 고정된 값을 갖는 점을 주의하면 단순화된 GF 곱셈꼴 연산기를 그림 4와 같이 최적화 할 수 있다.

2.2 고속 리드-솔로몬 오류정정 부호화기

일반적으로, 이미 알려진 (255,239)리드-솔로몬 오류정정 부호화기는 그 동작속도가 75 MHz아래로 제한되어 있으며, 그 복잡성 또한 크다. 이러한 시간-하드웨어 복잡성 문제를 해결하기위해서는 고속 동작과 회로의 복잡도가 낮도록 회로를 설계하여 자체 아키텍처를 향상시켜야 함은 물론 내부의 가장 핵심이 되는 모듈들을 최적화 시켜야 한다. 특히, 2.1절에서 언급된 회로 내 가장 기본이

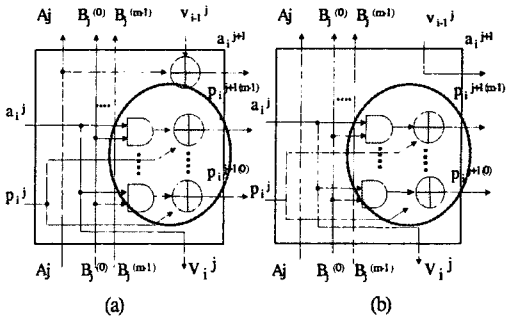

그림 3: m개의 GF 곱셈기를 대신하는 단순화된 GF 곱셈기 셀; (a) $f_i=1$ (b) $f_i=0$.

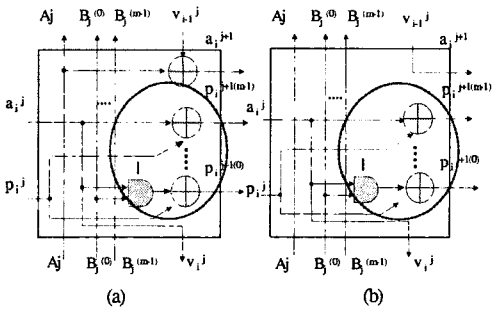

그림 4: m개의 GF 곱셈기를 대신하는 고정입력에 대한 단순화된 GF 곱셈기 셀; (a) $f_i=1$ (b) $f_i=0$.

되는 GF 고속 연산기를 위한 최적화는 시스템 내 어떤 알고리듬의 변경 없이도 아키텍처의 성능향상을 보장시킬 수 있다.

2.2.1 (255, 239) 리드-솔로몬 부호화기 설계

리드-솔로몬부호는 비이진 블록부호로 강력한 채널부호들 중 하나로 알려져 있다. 수신된 데이터 중에 8개의 오류바이트를 정정할 수 있는 (255, 239) 리드-솔로몬부호의 생성다항식 $G(x)$은 다음과 같다.

$$G(x) = (x-\alpha^{15})(x-\alpha^{14}) \cdots (x-1),$$

여기서 α 는 원시다항식 $F(x) = x^8 + x^4 + x^3 + x^2 + 1$의 근으로 GF(256)원소의 베이스이다.

$U(x)$를 정보데이터 다항식이라고 하자. 계통적 리드-솔로몬 부호화절차는 다음 수식에 따른다.

$$C(x) = U(x)x^{16} + < U(x)x^{16} >_{G(x)},$$

여기서 $< \cdot >_{G(x)}$는 $G(x)$로 나눈 나머지 다항식을 의미한다. (255,239) 리드-솔로몬 부호화기는 그림 5와 같이 선형 궤환구조를 갖는 쉬프트레지스터인 RS BASE로 설계되어진다. 제안된 리드-솔로몬 부호화기는 이처럼 RS 베이스모듈, 하나의 GF 곱셈기꼴의 연산기, 제어모듈, 2개의 램과 컨퍼터로 구성된다. 하나의 GF 곱셈기꼴의 연산기는 이전 절에서 제안한 하나의 고정입력에 대한 단순화된 곱셈기를 채택하고 있으며, 마치 16개의 GF 곱셈 연산을 수행하는 것과 동일한 계산을 한다. 그림 6은 입력 비정수배의 CLK신호들에 따라 입력 정보데이터신호의 연속적 데이터들을 실시간으로 부호화할 수 있도록 제어신호 S1과 S2를 생성하여 2개의 램에 번갈아 가며 읽고 쓰는 동작 타이밍도를 나타낸 것이다. 여기서 C는 부호화된 redundancy 신호다. 그림 7은 제안된 리드-솔로몬 부호화기의 최상위 스케메틱을 나타낸

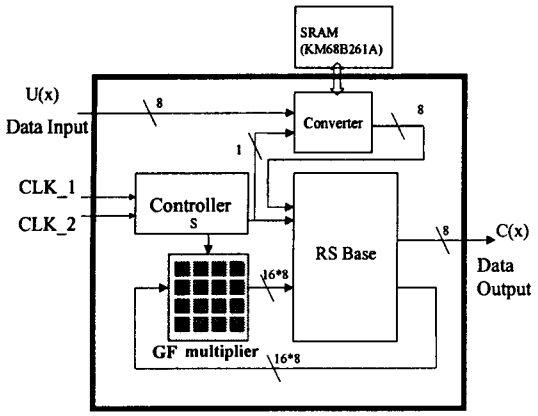

그림 5 : 제안된 (255,239) 리드-솔로몬 부호화기 구조.

것으로 고속의 디지털 신호전달을 위한 클록스큐(clock skew) 현상을 보정한 회로를 보여주고 있다.

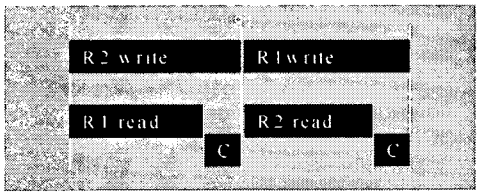

그림 6 : 제어신호에 의한 실시간 부호화기 동작 타이밍도.

3. 결 론

본 논문은 초고속 전력선 통신시스템을 위한 리드-솔로몬 부호화기의 설계에 대한 방법론적 측면과 오류부호화기 내 고속용 GF 곱셈연산기의 최적화 설계 방법을 설명하였다. 실제, 제안된 리드-솔로몬 부호화기를 0.25 μm의 표준 셀방식의 VLSI 테크날리지로 합성구현 할 경우, GF 곱셈 연산기의 병렬 및 파이프라이닝 세미-시스톨릭구조에 의해 580 MHz의 동작속도를 낼 수 있으며, 100%의 데이터 처리율과 9 싸이클의 레이턴시를 갖는다. 비록 설계의 구조적 특성에 따라 다소 전력소모가 큰 단점은 있지만, 전력선을 통한 안정된 전기공급과 시스템 전체의 성능향상으로 초고속 서비스를 지원하는 전력선 통신시스템 설계 시 적합하다.

[참 고 문 헌]

[1] S. Wei, "VLSI Architectures for Computing Exponentiations, Multiplicative Inverses, and Divisions in GF(2^m)," *IEEE Transation on the VLSI Systems*, vol. 44, pp. 847-855, Oct. 1997.

[2] S. W. Wei, "A Systolic Power-Sum Circuit for GF(2^m)," *IEEE Trans. on Computers*, vol. 43, pp. 226-229, Feb. 1994.

[3] T. C. Bartee and D. I. Schneider, "Computation with Finite Fields," *Jounal of the Information and Computers*, vol. 6, pp. 79-98, Mar. 1963.

[4] J. L. Massey and J. K. Omura, "Computational Method and Apparatus for Finite Field Arithmetic," U.S. Patent US04587627, May 1986.

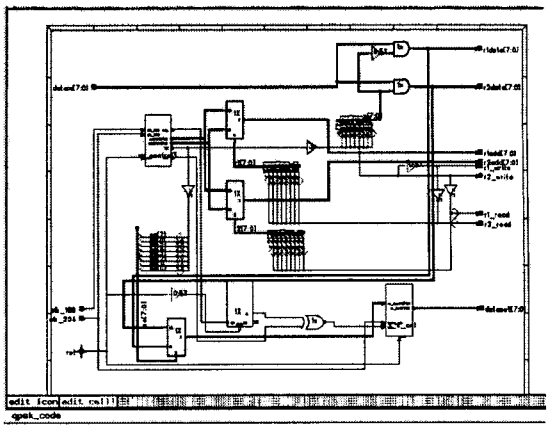

그림 7 : 설계된 (255,239) 리드-솔로몬 부호화기의 배선도.

[5] C. S. Yeh, I. S. Reed, and T. K. Truong, "Systolic Multipliers for Finite Fields GF(2^m)," *IEEE Trans. on Computers*, vol. C-33, pp. 357-360, Apr. 1984.

[6] I. S. Hsu, T. K. Truong, L. J. Deutsch, and I. S. Reed, "A Comparison of VLSI Architecture of Finite Field Multipliers Using Dual, Normal, or Standard Bases," *IEEE Trans. on Computers*, vol. 37, pp. 735-739, Apr. 1988.

[7] M. A. Hasan and V. K. Bhargava, "Multiplication and Inversion over a Class of GF(2^m)," *Proc. IEEE Pacific Rim Conf. on Commu., Computers and Signal Processing*, pp. 211-213, May 9-10. 1991.

[8] C. L. Wang and J. L. Lin, "Systolic Array Implementation of Multipliers for Finite Field GF(2^m)," *IEEE Trans. on Circuits and Systems*, vol. 38, pp. 796-800, July 1991.

[9] S. K. Jain and K. K. Parhi, "Low Latency Standard Basis GF(2^m) Multiplier and Squarer Architectures," *Proc. IEEE ICASSP*, Detroit, MI, pp.2747-2750, 1995.

[10] S. K. Jain, L. Song and K. K. Parhi, "Efficient Semisystolic Architectures for Finite-Field Arithmetic," *IEEE Transation on the VLSI Systems*, vol. 6, pp. 101-113, Mar. 1998.

[11] E. R. Berlekamp, "Bit-Serial Reed-Solomon Encoder," *IEEE Trans. on Information Theory*, vol. IT-28, pp. 869-874, Nov. 1982.

[12] S. Choi, Y. Lee, and K. Kim, "A High-Speed Coded QPSK Transmitter LSI for DAVIC-Compliant Digital Communications," *Proc. Int. Conf. on WPMC'00*, Bangkok, Tailand, vol. 2, pp.810-814 Nov. 2000.

[13] S. Lin and D. J. Costello, *Error Control Coding: Fundamentals and Applications*, Prentice-Hall, Inc., Englewood Cliffs, 1983.

[14] S. Choi, Y. Lee, and K. Kim, "Architecture for a High-Speed Standard-Basis GF(2^m) Multiplier with a Constant Primitive Coefficient Set", *Int. Journal of Electronics*, vol. 89, no. 10, pp.801-810, 2002