



(19)대한민국특허청(KR)
(12) 등록특허공보(B1)

(51) 。 Int. Cl. G06F 7/52 (2006.01)	(45) 공고일자 (11) 등록번호 (24) 등록일자	2007년02월28일 10-0653358 2006년11월27일
--	-------------------------------------	--

(21) 출원번호 (22) 출원일자 심사청구일자	10-2005-0090141 2005년09월27일 2005년09월27일	(65) 공개번호 (43) 공개일자
----------------------------------	---	------------------------

(73) 특허권자 고려대학교 산학협력단
 서울 성북구 안암동5가1 고려대학교 내

(72) 발명자 임종인
 서울 종로구 내수동 95 파크펠리스 101-901

 김창한
 서울 서초구 반포동 20-9 주공아파트 328-402호

 장남수
 서울 마포구 성산2동 200-84

 김소선
 서울 성북구 안암동5가 103-149 208호

(74) 대리인 현종철

(56) 선행기술조사문헌 KR1020010068349 A US5272661 A 논문 * 심사관에 의하여 인용된 문헌	KR1020040055523 A US6925479 B2
--	-----------------------------------

심사관 : 한선경

전체 청구항 수 : 총 10 항

(54) 유한체의 병렬곱셈 연산장치

(57) 요약

유한체의 병렬곱셈 연산장치가 개시된다. 그 연산장치는 유한체의 병렬 곱셈 연산장치는, 유한체 $GF(2^m)$ 이 타입 k 인 가우스 시안 정규기저를 가지며, $GF(n+1)^* = \langle 2 \rangle$ 이고 $n=mk$ 인 조건을 만족하는 입력 $A, B(A, B$ 는 벡터)에 대해, $A_i * B_i$ 에 의해 A, B 를 AB곱셈부; 입력 A, B 에 대해 수학적식 2에 의해 연산되는 x 함수부; x 함수부의 결과값을 입력으로 하여 $S1 = x^{2^{(m-k)}}$ 에 따라 오른쪽 순환이동(right cyclic shift) 수행하는 S1함수부; AB곱셈부의 결과값과 S1함수부의 결과값을 최종 출력의 각 자리에 맵핑시켜 더하는 BTX1 연산부를 포함함을 특징으로 한다.

[수학식 2]

$$x_{j,i_0} = (A_j \cdot B_{((i_0+j))}) \oplus (A_{((i_0+j))} \cdot B_j)$$

여기서, $1 \leq i_0 \leq u = (m-1)/2$, $0 \leq j < m-1$.

본 발명에 의하면, 암호학적으로 많이 응용되는 유한체인 타입 $k=2,4,6$ 에 적용하면, 가장 효율적인 Reyhani-Masoleh와 Hasan의 곱셈기와 동일한 공간 및 시간 복잡도를 갖는다. 따라서 암호관련 응용분야의 하드웨어 구현에 유용하게 적용할 수 있다.

대표도

도 1

특허청구의 범위

청구항 1.

유한체 $GF(2^m)$ 이 타입 k 인 가우시안 정규기저를 가지며, $GF(n+1)^* = \langle 2 \rangle$ 이고 $n=mk$ 인 조건을 만족하는 입력 A, B (A, B 는 벡터)에 대해,

$A_i * B_i$ 에 의해 A, B 를 수학식 1에 의해 곱하는 AB곱셈부;

[수학식 1]

$$A * B = A_i * B_i$$

입력 A, B 에 대해 수학식 2에 의해 연산되는 x 함수부;

[수학식 2]

$$x_{j,i_0} = (A_j \cdot B_{((i_0+j))}) \oplus (A_{((i_0+j))} \cdot B_j)$$

여기서, $1 \leq i_0 \leq u = (m-1)/2$, $0 \leq j < m-1$.

상기 x 함수부의 결과값을 입력으로 하여 수학식 3에 따라 오른쪽 순환이동(right cyclic shift) 수행하는 S1함수부;

[수학식 3]

$$S1 = x^{2^{(m-1)}}$$

상기 AB곱셈부의 결과값과 상기 S1함수부의 결과값을 최종 출력의 각 자리에 수학식 4에 의해

[수학식 4]

$$C = \sum_{j=0}^{m-1} A_j B_j \beta^{2^j} + \sum_{i_0=1}^u \sum_{w=0}^{k/2-1} \left(\sum_{j=0}^{m-1} x_{j,i_0} \beta^{2^j} \right)^{2^{(m+i_0+w)}} + \sum_{w=1}^{k/2} \left(\sum_{j=0}^{m-1} x_{j,i_0} \beta^{2^j} \right)^{2^{(m+i_0+w)}},$$

$$x_{j,i_0} = (A_j \cdot B_{((i_0+j))}) \oplus (A_{((i_0+j))} \cdot B_j), 1 \leq i_0 \leq u = (m-1)/2, 0 \leq j < m-1.$$

맵핑시켜 더하는 BTX1 연산부를 포함함을 특징으로 하는 유한체의 병렬곱셈 연산장치.

청구항 2.

제1항에 있어서, 상기 AB곱셈부는

입력 A와 입력 B를 논리곱연산하며, 유한체 $GF(2^m)$ 에서의 m 에 해당하는 개수만큼의 AND게이트로 이루어짐을 특징으로 하는 유한체의 병렬곱셈 연산 장치.

청구항 3.

제1항에 있어서, 상기 x함수부는

$u = (m-1)/2$ 개의 그룹으로 이루어지고,

상기 그룹은 m 개의 서브그룹으로 이루어지고,

상기 서브그룹은

A_j 와 $B_{((i0+j))}$ 를 논리곱 연산하는 제1AND게이트;

(여기서 $((a+b))$ 는 $((a+b)) = (a+b) \bmod m$ 이다.)

$A_{((i0+j))}$ 와 B_j 를 논리곱 연산하는 제2AND게이트; 및

상기 제1AND게이트 및 제2AND게이트의 출력을 배타논리합하는 XOR게이트를 구비하여 이루어짐을 특징으로 하는 유한체의 병렬 곱셈 연산 장치.

청구항 4.

제3항에 있어서, 상기 S1함수부는

x 함수부의 서브그룹 개수(u 개)에 해당하는 S1함수 맵핑그룹으로 이루어지고,

상기 S1함수 맵핑그룹은 k 개의 단위맵핑부로 이루어지고,

상기 단위맵핑부는 상기 x 함수부의 서브그룹에서 출력되는 m 비트의 데이터를 입력으로 하여 수학식 5와 같은 ζ 함수에 의해

[수학식 5]

$$\zeta_i = \begin{cases} k_i \bmod m, & i \equiv i_0 \bmod m \\ k_i + i_0 \bmod m, & i \equiv -i_0 \bmod m \end{cases}$$

m 개의 출력으로 오른쪽 순환이동 매핑함을 특징으로 하는 유한체의 병렬 곱셈 연산 장치.

청구항 5.

제4항에 있어서, 상기 BTX1 연산부는

m 개의 서브BTX1 연산부로 이루어지고,

상기 서브BTX1 연산부는

상기 AB곱셈부의 결과값과 상기 S1함수부의 단위매핑부의 결과값에 대해 상기 수학식 4에 의해 결정되는 입력값을 배타 논리합 연산하는 XOR 게이트가 이진트리로 구성됨을 특징으로 하는 유한체의 병렬 곱셈 연산 장치.

청구항 6.

유한체 $GF(2^m)$ 이 타입 k인 가우시안 정규기저를 가지며, $GF(n+1)^* = \langle 2 \rangle$ 이고 $n=mk$ 인 조건을 만족하는 입력 A, B(A, B는 벡터)에 대해,

$A_i * B_i$ 에 의해 A, B를 수학식 1에 의해 곱하는 AB곱셈부;

[수학식 1]

$$A * B = A_i * B_i$$

입력 A, B에 대해 수학식 6에 의해 연산되는 y 함수부;

[수학식 6]

$$y_{j,i_0} = (A_j \oplus A_{((i_0+j))}) \cdot (B_{((i_0+j))} \oplus B_j)$$

여기서, $1 \leq i_0 \leq u, 0 \leq j \leq m-1$

상기 y 함수부의 결과값을 입력으로 하여 수학식 7에 따라 오른쪽 순환이동(right cyclic shift) 수행하는 S2함수부;

[수학식 7]

$$S2 = y^{2^{i_0}}$$

상기 AB곱셈부의 결과값과 상기 S2함수부의 결과값을 최종 출력의 각 자리에 수학식 4에 의해

[수학식 8]

$$C = \sum_{j=0}^{m-1} A_j B_j \beta^{2^j} + \sum_{i_0=1}^u \sum_{j=0}^{k/2-1} \left(\sum_{j=0}^{m-1} y_{j,i_0} \beta^{2^j} \right) 2^{i_0} + \sum_{j=1}^{k/2} \left(\sum_{j=0}^{m-1} y_{j,i_0} \beta^{2^j} \right) 2^{i_0},$$

여기서, $y_{j,i_0} = (A_j \oplus A_{((i_0+j))}) \cdot (B_{((i_0+j))} \oplus B_j), 1 \leq i_0 \leq u, 0 \leq j \leq m-1$

맵핑시켜 더하는 BTX2 연산부를 포함함을 특징으로 하는 유한체의 병렬곱셈 연산장치.

청구항 7.

제6항에 있어서, 상기 AB곱셈부는

입력 A와 입력 B를 논리곱연산하며, 유한체 $GF(2^m)$ 에서의 m 에 해당하는 개수만큼의 AND게이트로 이루어짐을 특징으로 하는 유한체의 병렬곱셈 연산 장치.

청구항 8.

제6항에 있어서, 상기 y함수부는

m개의 그룹으로 이루어지고,

상기 그룹은 $u = (m-1)/2$ 개의 서브그룹으로 이루어지고,

상기 서브그룹은

A_j 와 $A_{((i0+j))}$ 를 배타논리합 연산하는 제1XOR게이트;

(여기서 $((a+b))$ 는 $((a+b)) = (a+b) \bmod m$ 이다.)

B_j 와 $B_{((i0+j))}$ 를 배타논리합 연산하는 제2XOR게이트; 및

상기 제1XOR게이트 및 제2XOR게이트의 출력을 논리곱연산하는 AND게이트를 구비하여 이루어짐을 특징으로 하는 유한체의 병렬 곱셈 연산 장치.

청구항 9.

제8항에 있어서, 상기 S2함수부는

y 함수부의 서브그룹 개수(u개)에 해당하는 S2함수 맵핑그룹로 이루어지고,

상기 S2함수 맵핑그룹은 k 개의 단위맵핑부로 이루어지고,

상기 단위맵핑부는 상기 y 함수부의 서브그룹에서 출력되는 m 비트의 데이터를 입력으로 하여 수학식 5와 같은 ζ 함수에 의해

[수학식 5]

$$\zeta_i = \begin{cases} k_i \bmod m, & i \equiv i_0 \bmod m \\ k_i + i_0 \bmod m, & i \equiv -i_0 \bmod m \end{cases}$$

m 개의 출력으로 오른쪽 순환이동 매핑함을 특징으로 하는 유한체의 병렬 곱셈 연산 장치.

청구항 10.

제9항에 있어서, 상기 BTX2 연산부는

m 개의 서브BTX2 연산부로 이루어지고,

상기 서브BTX2 연산부는

상기 AB곱셈부의 결과값과 상기 S2함수부의 단위매핑부의 결과값에 대해 상기 수학식 8에 의해 결정되는 입력값을 배타 논리합 연산하는 XOR 게이트가 이진트리로 구성됨을 특징으로 하는 유한체의 병렬 곱셈 연산 장치.

명세서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 곱셈장치에 관한 것으로서, 특히 유한체의 병렬곱셈 장치에 관한 것이다.

유한체는 암호학과 코딩 이론 등에서 응용되고 있으며 최근 공개키 암호인 타원곡선암호(ECC), XTR, ElGamal 타입 암호 등의 관련 응용 분야에서 활발하게 사용되고 있다. 특히 유한체 $GF(2^m)$ 은 2^m 개의 원소들을 포함하는 수 체계이고, 유한체의 각 원소가 n비트로 표현될 수 있으므로 에러정정 코드 및 암호 시스템의 하드웨어 구현과 같은 응용에 많이 이용된다. 이들은 기본적으로 유한체 연산을 포함하고 있으며 이 연산에 따라 암호 시스템의 효율성이 결정된다. 따라서 유한체에서 정의된 연산의 고속화는 매우 중요하며 많은 연구의 대상이 되고 있다.

유한체의 연산은 표현 방법에 따라 달라지며 대표적으로 다항식기저, 정규기저 등이 있고, Nonconvention 기저를 사용한다. 특히 정규기저를 이용하는 경우 제곱연산이 순환이동(Cyclic shift)으로 이루어지는 등 많은 장점을 가지고 있어 하드웨어 구현에 이용된다. 이 중 기약 AOP(All one polynomial)에 의해 생성되는 타입 I 최적 정규기저를 가지는 유한체가 가장 높은 효율성을 보인다. 이에 대한 공간 및 시간 복잡도에서 우수한 유한체의 곱셈 연산장치가 요구되고 있다.

발명이 이루고자 하는 기술적 과제

본 발명이 이루고자 하는 기술적 과제는 타입 I 최적 정규기저를 가지는 유한체 $GF(2^m)$ 의 부분체이고 타입 (m,k)인 가우스 주기를 가지는 유한체 $GF(2^m)$ 을 기반으로 하며, 타원곡선암호를 비롯한 암호 시스템 응용에서 소수인 m을 주로 사용하므로 m이 홀수인 경우만 고려하여, 유한체 $GF(2^{mk})$ 에서 병렬 곱셈 연산기인 Reyhani-Masoleh과 Hasan의 타입 I 연산기를 활용하여 유한체 $GF(2^m)$ 에서 곱셈을 수행하는 유한체의 병렬 곱셈 연산장치를 제공하는 것이다.

발명의 구성

상기 기술적 과제를 이루기 위한 본 발명에 의한 유한체의 병렬 곱셈 연산장치는, 유한체 $GF(2^m)$ 이 타입 k인 가우시안 정규기저를 가지며, $GF(n+1)^* = \langle 2 \rangle$ 이고 $n=mk$ 인 조건을 만족하는 입력 A, B(A, B는 벡터)에 대해, $A_i * B_i$ 에 의해 A, B를 수학식 1에 의해 곱하는 AB곱셈부; 입력 A, B에 대해 수학식 2에 의해 연산되는 x 함수부; 상기 x 함수부의 결과값을 입력으로 하여 수학식 3에 따라 오른쪽 순환이동(right cyclic shift) 수행하는 S1함수부; 상기 AB곱셈부의 결과값과 상기 S1함수부의 결과값을 최종 출력의 각 자리에 수학식 4에 의해 맵핑시켜 더하는 BTX1 연산부를 포함함을 특징으로 한다.

[수학식 1]

$$A * B = A_i * B_i$$

[수학식 2]

$$x_{j,i_0} = (A_j \cdot B_{((i_0+j))}) \oplus (A_{((i_0+j))} \cdot B_j)$$

여기서, $1 \leq i_0 \leq u = (m-1)/2$, $0 \leq j < m-1$.

[수학식 3]

$$S1 = x^{2^{c_{m-1}}}$$

[수학식 4]

$$C = \sum_{j=0}^{m-1} A_j B_j \beta^{2^j} + \sum_{i_0=1}^u \sum_{w=0}^{k/2-1} \left(\sum_{j=0}^{m-1} x_{j,i_0} \beta^{2^j} \right)^{2^{c_{m-1}+w}} + \sum_{w=1}^{k/2} \left(\sum_{j=0}^{m-1} x_{j,i_0} \beta^{2^j} \right)^{2^{c_{m-1}+w}},$$

$$x_{j,i_0} = (A_j \cdot B_{((i_0+j))}) \oplus (A_{((i_0+j))} \cdot B_j), 1 \leq i_0 \leq u = (m-1)/2, 0 \leq j < m-1.$$

[수학식 5]

$$\xi_i = \begin{cases} k_i \bmod m, & i \equiv i_0 \bmod m \\ k_i + i_0 \bmod m, & i \equiv -i_0 \bmod m \end{cases}$$

상기 AB곱셈부는 입력 A와 입력 B를 논리곱연산하며, 유한체 GF(2^m)에서의 m에 해당하는 개수만큼의 AND게이트로 이루어짐이 바람직하다. 상기 x함수부는 u = (m-1)/2개의 그룹으로 이루어지고, 상기 그룹은 m개의 서브그룹으로 이루어지고, 상기 서브그룹은 A_j와 B_{((i₀+j))}를 논리곱 연산하는 제1AND게이트; A_{((i₀+j))}와 B_j를 논리곱 연산하는 제2AND게이트; 및 상기 제1AND게이트 및 제2AND게이트의 출력을 배타논리합하는 XOR게이트를 구비하여 이루어짐이 바람직하다. 여기서 ((a+b))는 ((a+b)) = (a+b) mod m이다.

상기 S1함수부는 x함수부의 서브그룹 개수(u개)에 해당하는 S1함수 맵핑그룹으로 이루어지고, 상기 S1함수 맵핑그룹은 k개의 단위맵핑부로 이루어지고, 상기 단위맵핑부는 상기 x함수부의 서브그룹에서 출력되는 m비트의 데이터를 입력으로 하여 수학식 5와 같은 ξ함수에 의해 m개의 출력으로 오른쪽 순환이동 맵핑함이 바람직하다.

상기 BTX1 연산부는 m개의 서브BTX1 연산부로 이루어지고, 상기 서브BTX1 연산부는 상기 AB곱셈부의 결과값과 상기 S1함수부의 단위맵핑부의 결과값에 대해 상기 수학식 4에 의해 결정되는 입력값을 배타논리합 연산하는 XOR게이트가 이진트리로 구성됨이 바람직하다.

상기 기술적 과제를 이루기 위한 본 발명에 의한 유한체의 병렬 곱셈 연산장치는, 유한체 GF(2^m)이 타입 k인 가우시안 정규기저를 가지며, GF(n+1)* = <2> 이고 n=mk인 조건을 만족하는 입력 A, B(A, B는 벡터)에 대해, A_i * B_i에 의해 A, B를 수학식 1에 의해 곱하는 AB곱셈부; 입력 A, B에 대해 수학식 6에 의해 연산되는 y함수부; 상기 y함수부의 결과값을 입력으로 하여 수학식 7에 따라 오른쪽 순환이동(right cyclic shift) 수행하는 S2함수부; 상기 AB곱셈부의 결과값과 상기 S2함수부의 결과값을 최종 출력의 각 자리에 수학식 4에 의해 맵핑시켜 더하는 BTX2 연산부를 포함함을 특징으로 한다.

[수학식 6]

$$y_{j,i_0} = (A_j \oplus A_{((i_0+j))}) \cdot (B_{((i_0+j))} \oplus B_j)$$

여기서, $1 \leq i_0 \leq u$, $0 \leq j \leq m-1$

[수학식 7]

$$S2 = y^{2^{c_{m-1}}}$$

[수학식 8]

$$C = \sum_{j=0}^{m-1} A_j B_j \beta^{2^j} + \sum_{i_0=1}^u \sum_{j=0}^{k/2-1} \left(\sum_{i=0}^{m-1} y_{j,i_0} \beta^{2^i} \right) 2^{c_{i_0} i} + \sum_{j=1}^{k/2} \left(\sum_{i=0}^{m-1} y_{j,i_0} \beta^{2^i} \right) 2^{c_{i_0} i},$$

여기서, $y_{j,i_0} = (A_j \oplus A_{((i_0+j))}) \cdot (B_{((i_0+j))} \oplus B_j)$, $1 \leq i_0 \leq u$, $0 \leq j \leq m-1$

상기 AB곱셈부는 입력 A와 입력 B를 논리곱연산하며, 유한체 GF(2^m)에서의 m에 해당하는 개수만큼의 AND게이트로 이루어짐이 바람직하다. 상기 y함수부는 m개의 그룹으로 이루어지고, 상기 그룹은 u = (m-1)/2 개의 서브그룹으로 이루어지고, 상기 서브그룹은 A_j와 A_{((i₀+j))}를 배타논리합 연산하는 제1XOR게이트; (여기서 ((a+b))는 ((a+b)) = (a+b) mod m이다.) B_j와 B_{((i₀+j))}를 배타논리합 연산하는 제2XOR게이트; 및 상기 제1XOR게이트 및 제2XOR게이트의 출력을 논리곱연산하는 AND게이트를 구비하여 이루어짐이 바람직하다.

상기 S2함수부는 y함수부의 서브그룹 개수(u개)에 해당하는 S2함수 맵핑그룹으로 이루어지고, 상기 S2함수 맵핑그룹은 k개의 단위맵핑부로 이루어지고, 상기 단위맵핑부는 상기 y함수부의 서브그룹에서 출력되는 m비트의 데이터를 입력으로 하여 수학식 5와 같은 ζ함수에 의해 m개의 출력으로 오른쪽 순환이동 매핑함이 바람직하다.

상기 BTX2 연산부는 m개의 서브BTX2 연산부로 이루어지고, 상기 서브BTX2 연산부는 상기 AB곱셈부의 결과값과 상기 S2함수부의 단위매핑부의 결과값에 대해 상기 수학식 8에 의해 결정되는 입력값을 배타논리합 연산하는 XOR 게이트가 이진트리로 구성됨이 바람직하다.

이하, 첨부된 도면들을 참조하여 본 발명에 따른 유한체의 병렬 곱셈 연산장치에 대해 상세히 설명한다.

먼저, 본 발명을 위한 기본적인 수학적 배경을 기술하기로 한다. 양의 정수 m에 대해 유한체 GF(2) 위에서 GF(2^m)의 정규기저가 존재한다. 즉 $\beta \in GF(2^m)$ 가 존재하여 $N = \beta, \beta^2, \dots, \beta^{2^{m-1}}$ 이 GF(2) 위에서 GF(2^m)의 기저 (Basis)일 때 N을 정규기저라 하고, β를 정규기저 생성자라 한다. 따라서 $A \in GF(2^m)$ 에 대하여 $A = \sum_{i=0}^{m-1} a_i \beta^{2^i}$, $a_i \in GF(2)$ 로 표현되며 좌표로 $A = (a_0, a_1, \dots, a_{m-1})$ 와 같이 나타낸다. 또한 벡터 (행렬)표현으로 다음과 나타내며 T는 행렬의 치환 (Transpose)을 나타낸다.

$$A = \bar{a} \times \bar{\beta}^T = \bar{a} \times \bar{a}^T, \quad \bar{a} = (a_0, a_1, \dots, a_{m-1}), \quad \bar{\beta} = (\beta_0, \beta_1, \dots, \beta_{m-1})$$

임의의 원소 $A \in GF(2^m)$ 에 대해 A^2 은 좌표로 표현하면 $A^2 = (a_{m-1}, a_0, \dots, a_{m-2})$ 이고, 이는 오른쪽 순환이동 (Right cyclic shift, RCS)로 수행이 된다.

m, k는 양수이고 p = mk + 1 ≠ 2는 소수, 유한체 GF(p)*에서 2의 위수 (Order)를 e이며 GCD(mk/e, m) = 1이라고 한다. 유한체 GF(2ⁿ), n = mk에서 p의 원시근 (A primitive nth root of unity)을 γ, kth root of unity를 τ이고, $\beta = \gamma + \gamma^\tau + \gamma^{\tau^2} + \dots + \gamma^{\tau^{k-1}}$ 이라고 하면 β는 유한체 GF(2^m)의 정규기저 생성자이다. 즉 $\beta, \beta^2, \beta^{2^2}, \dots, \beta^{2^{m-1}}$ 은 유한체 GF(2) 위에서 GF(2^m)의 정규기저로, 이 때 β를 유한체 GF(2) 위에서 타입 (m, k)인 가우스 주기 (Gauss period of type (m, k))라 한다. 본 발명에서는 유한체 GF(2^m)이 타입 (m, k)인 가우스 주기를 가지는 경우 유한체 GF(2^m)를 타입 k라고 한다. 또한 모든 계수가 1인 다항식인 $x^m + x^{m-1} + \dots + x + 1$ 을 All one polynomial (AOP)라 한다. 이 때 k=1인 경우 타입 I 최적 정규기저라고 하며, k=2인 경우 타입 II 최적 정규기저라고 한다. 또한 n = mk인 경우 유한체 GF(2^m)은 GF(2ⁿ)의 부분체이다.

정리 1. (타입 I 최적 정규기저)

유한체 GF(2) 위에서 GF(2ⁿ)이 타입 I의 최적 정규기저를 가지기 위한 필요충분조건은 (n+1)이 소수이고 GF(n+1)*=<2>이다. 또는 n차의 AOP인 $x^n + x^{n-1} + \dots + x + 1$ 가 유한체 GF(2) 위에서 기약다항식인 경우 AOP의 근은 최적 정규기저의 생성자이다.

정리 2. (타입 II의 최적 정규기저)

유한체 GF(2) 위에서 GF(2ⁿ)이 타입 II의 최적 정규기저를 가지기 위한 필요충분조건은 (2m+1)이 소수이고, GF(2m+1)*=<2>이나 2m+1≡3 mod 4 이고, GF(2m+1)*=<-1,2> 이면 $\beta = \gamma + \gamma^{-1}$ 는 유한체 GF(2)위에서 GF(2^m)의 최적 정규기저 생성자이다. 여기서 γ 는 (2m+1)의 원시근이다.

본 발명에서는 m은 홀수이고, n=mk, (n+1)은 소수이며 GF(n+1)*=<2>인 경우를 고려한다. 즉 γ 이 (n+1)의 원시근이면, 정리 1에 의해 γ 는 유한체 GF(2ⁿ)의 타입 I 최적 정규기저 생성자이다. 또한, e=mk, τ=2^m이므로, (m,k)는 가우스 주기이며, $\beta = \gamma + \gamma^{2^m} + \gamma^{2^{2m}} + \dots + \gamma^{2^{m(k-1)}}$ 는 유한체 GF(2)위에서 GF(2^m)의 정규기저 생성자이다. 따라서 임의의 원소 A∈GF(2^m)는

$A = A_0\beta + A_1\beta^2 + A_2\beta^{2^2} + \dots + A_{m-1}\beta^{2^{m-1}}$, $A_i \in GF(2)$ 와 같이 표현된다. 유한체 GF(2^m)는 GF(2ⁿ)의 부분체이므로, A∈GF(2ⁿ) 이고,

$$\begin{aligned} A &= A_0\gamma + A_1\gamma^2 + A_2\gamma^{2^2} + \dots + A_{m-1}\gamma^{2^{m-1}} \\ &+ A_0\gamma^{2^m} + A_1\gamma^{2^{m+1}} + \dots + A_{m-1}\gamma^{2^{2m-1}} + \dots \\ &+ A_0\gamma^{2^{m(k-1)}} + A_1\gamma^{2^{m(k-1)+1}} + \dots + A_{m-1}\gamma^{2^{mk-1}} \end{aligned}$$

이다. 임의의 원소

$$A = a_0\gamma + a_1\gamma^2 + a_2\gamma^{2^2} + \dots + a_{mk-1}\gamma^{2^{mk-1}} \in GF(2^n) \text{ 이면}$$

[수학식 1]

$$a_{i+mj} = A_i, 0 \leq i \leq m-1, 0 \leq j \leq k-1$$

이다.

$$B = B_0\beta + B_1\beta^2 + B_2\beta^{2^2} + \dots + B_{m-1}\beta^{2^{m-1}} \in GF(2^n) \text{ 이고}$$

$$B = b_0\gamma + b_1\gamma^2 + b_2\gamma^{2^2} + \dots + b_{mk-1}\gamma^{2^{mk-1}} \in GF(2^n) \text{ 이면}$$

수학식 1과 같은 성질을 만족한다.

(2) Reyhani-Masoleh과 Hasan의 AOP를 이용한 타입 I 연산기

유한체 GF(2^m)에서 임의의 두 원소를 A,B에 대해 C=AB이라 하면 곱의 결과인 C는 다음과 같이 표현한다.

[수학식 2]

$$C = (\bar{a} \times \bar{b}^T)(\bar{b} \times \bar{b}^T) = \bar{a}M\bar{b}, \quad M = \bar{b}^T\bar{b} = (\beta^{2^i+2^j}), \quad 0 \leq i, j \leq m-1$$

즉 기저 N을 이용하여 $\beta^{2^i+2^j}$ 을 구성하며 수식식 2에서 곱의 행렬 M을 다음과 같이 다시 표현한다.

$$M = M_0\beta + M_1\beta^2 + \dots + M_{m-1}\beta^{2^{m-1}}, \quad M_i \in \text{Mat}_{m \times m}(GF(2))$$

제곱 연산이 순환이동연산으로 이루어진다는 것을 이용하면 곱 $C=AB=(c_0, c_1, \dots, c_{m-1})$ 은 다음과 같이 표현된다.

$$C = \bar{a}M_i\bar{b}^T = \bar{a}^{(i)}M_0\bar{b}^{(i)}, \quad \bar{a}^{(i)} = (a_0, a_{i+1}, \dots, a_{i-1}), \quad \bar{b}^{(i)} = (b_0, b_{i+1}, \dots, b_{i-1})$$

따라서 각 i에 대하여 행렬 M_i 의 1의 개수는 모두 같음을 알 수 있으며 이 때 M_0 의 1의 개수를 정규기저 B의 복잡도라 하고 C_N 으로 표시한다. 또한 Gao 등은 $C_N \geq 2m-1$ 임을 증명하였다. 만약 $C_N=2m-1$ 일 때 정규기저 N을 최적 정규기저 (Optimal normal basis, ONB)라고 한다.

① Reyhani-Masoleh 와 Hasan의 AOP를 이용한 곱셈기

Reyhani-Masoleh 와 Hasan은 유한체의 곱의 행렬 $M = (\beta^{2^i+2^j})$ 을 다음과 같이 분리하였다.

$$M = U + U^T + D,$$

$$D = \begin{pmatrix} \beta^2 & 0 & \dots & 0 & 0 \\ 0 & \beta^{2^2} & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & \beta^{2^{i-1}} & 0 \\ 0 & 0 & \dots & 0 & \beta \end{pmatrix}, \quad U = \begin{pmatrix} 0 & \beta^{1+2^m} & \dots & \beta^{1+2^{m-2}} & \beta^{1+2^{m-1}} \\ 0 & 0 & \dots & \beta^{2+2^{m-2}} & \beta^{2+2^{m-1}} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 0 & \beta^{2^{m-2}+2^{m-1}} \\ 0 & 0 & \dots & 0 & 0 \end{pmatrix}$$

만약 $\delta_i = \beta^{1+2^i}$, $i=1, 2, \dots$, $v=|m/2|$ 이면 U의 모든 원소는 $\delta_i^{2^j}$, $j=0, 1, \dots, m-1$ 로 표현되므로 다음과 같은 정리를 제시하였다.

정리 3. $A, B \in GF(2^m)$ 이면 $C=AB$ 는 다음과 같다.

$$C = \begin{cases} \sum_{j=0}^{m-1} a_j \cdot b_j \beta^{2^{j+1}} + \sum_{i=1}^v \sum_{j=0}^{m-1} x_{j,i} \delta_i^{2^j}, & \text{for } m \text{ odd} \\ \sum_{j=0}^{m/2-1} a_j \cdot b_j \beta^{2^{j+1}} + \sum_{i=1}^{v-1} \sum_{j=0}^{m-1} x_{j,i} \delta_i^{2^j} + \sum_{j=0}^{v-1} x_{j,v} \delta_v^{2^j}, & \text{for } m \text{ even} \end{cases}$$

여기서 a_j, b_j 는 A, B의 좌표이며 $x_{j,i} = (a_j \cdot b_{i+j}) \oplus (b_j \cdot a_{i+j})$ 이다. $\oplus$ 는 XOR 연산자이고, $\cdot$ 는 AND 연산자이며 모든 색인은 모듈러 m값이다.

유한체 $GF(2^n)$ 가 기약다항식 AOP $x^n + x^{n-1} + \dots + x + 1$ 에 의해 생성되고, AOP의 근을 γ 라 하자. 이 때 γ 는 유한체 $GF(2^n)$ 의 타입 I 최적 정규기저를 생성하며, 정리 3을 정리 4와 같이 적용할 수 있다. 여기서 $\langle\langle i+j \rangle\rangle$ 는 $i+j \bmod n$ 을 의미한다.

정리 4. 유한체 이 타입 I 최적 정규기저를 가지며 γ 는 이 정규기저의 생성자이라고 하자. 임의의 원소 이면 는 다음과 같다.

$$C = \sum_{j=0}^{n-1} a_j \cdot b_j \gamma^{2^{\langle\langle j+1 \rangle\rangle}} + \sum_{i=1}^{v-1} \left(\sum_{j=0}^{n-1} x_{j,i} \gamma^{2^j} \right)^{2^{k_i}} + \sum_{j=0}^{n-1} \left(\sum_{i=1}^{v-1} x_{i,v} \right) \gamma^{2^j}, \quad v=n/2,$$

$$x_{j,i} = (a_j \cdot b_{\ll i+j \gg}) \oplus (a_{\ll i+j \gg} \cdot b_j)$$

② Reyhani-Masoleh 와 Hasan의 AND 연산을 감소시킨 곱셈기

2003년에 Reyhani-Masoleh 와 Hasan은 곱인 정리 5를 기반으로 AND연산을 감소시키는 병렬 곱셈 알고리즘을 제안하였다,

정리 5. 임의의 원소 $A, B \in GF(2^m)$ 이면 $C=AB$ 는 다음과 같다.

$$C = \begin{cases} \sum_{j=0}^{m-1} a_j \cdot b_j \delta_0^{2^{j-1}} + \sum_{j=0}^{m-1} \sum_{i=1}^v y_{j,i} \delta_i^{2^j} & \text{for } m \text{ odd} \\ \sum_{j=0}^{ml-1} a_j \cdot b_j \delta_0^{2^{j-1}} + \sum_{j=0}^{m-1} \sum_{i=1}^{v-1} y_{j,i} \delta_i^{2^j} + \sum_{j=0}^{v-1} y_{j,v} \delta_u^{2^j} & \text{for } m \text{ even,} \end{cases}$$

$y_{j,i} = (a_j \oplus a_{i+j}) \cdot (b_j \oplus b_{i+j})$, $1 \leq i \leq v$, $0 \leq j \leq m-1$ 이고 모든 색인은 모듈러 m 값이다.

(3) 본 발명에 의한 병렬 곱셈기의 구성

본 발명에서는 유한체 $GF(2^m)$ 가 타입 k인 가우시안 정규기저를 가지며 $GF(n+1)^* = \langle 2 \rangle$ 이고 $n=mk$ 인 경우를 고려한다. 본 발명은 유한체 $GF(2^n)$ 에서 병렬 곱셈 연산기인 Reyhani-Masoleh과 Hasan의 타입 I 연산기를 활용하여 유한체 $GF(2^m)$ 에서 곱셈을 수행하는 새로운 병렬 곱셈 연산기를 제안한 것이다. 즉 임의의 원소 $A, B \in GF(2^m) \subset GF(2^n)$ 일 때 2002년과 2003년에 각각 제안된 Reyhani-Masoleh과 Hasan의 기본 타입 I 연산기를 활용하여 새로운 병렬 곱셈 연산 $C=AB$ 를 수행하는 연산기를 구성한다. 본 발명에서 이용할 ξ_i 는 다음과 같이 정의한다.

정의 1. $n=mk$, $(n+1)$ 은 소수, $GF(n+1)^* = \langle 2 \rangle$ 이며 k_i 는 $2^i + 1 \equiv 2^{k_i} \pmod{n+1}$ 이라 하자. 이 때

$1 \leq i_0 \leq u = (m-1)/2$ 에 대해 $i \in \{i_0, m-i_0, , m+i_0, \dots, km/2-i_0\}$ 인 경우 다음과 같이 ξ_i 를 정의한다.

$$\xi_i = \begin{cases} k_i \pmod{m}, & i \equiv i_0 \pmod{m} \\ k_{i+i_0} \pmod{m}, & i \equiv -i_0 \pmod{m} \end{cases}$$

① Reyhani-Masoleh과 Hasan의 곱셈기를 이용한 본 발명에 의한 유한체 $GF(2^m)$ 에서의 병렬 곱셈기

본 발명은 유한체 $GF(2^m)$ 의 원소 A,B를 타입 I의 최적 정규기저를 가지는 확대체 $GF(2^n)$ 의 원소로 생각하여 병렬 곱셈기를 구성한다. 2002년 제안된 Reyhani-Masoleh과 Hasan의 연산기에서 $a_i \cdot b_i = A_{((i))} \cdot B_{((i))}$, $0 \leq i \leq n-1$ 이므로 n개의 계산이 필요하다. 그러나 본 발명에서는 $A_{((i))} \cdot B_{((i))}$, $0 \leq i \leq m-1$ 는 m개만 계산한다. 또한 $x_{j,i} = (a_j \cdot b_{\ll i+j \gg}) \oplus (a_{\ll i+j \gg} \cdot b_j)$ 은 식 (1)에 의해 $a_{\ll i \gg} = a_{((i))} = A_{((i))}$ 임을 이용하여 연산한다.

Reyhani-Masoleh와 Hasan의 곱셈기에서 $1 \leq i < v = n/2$ 에 대하여 B_i 통과한 후 S_i 에서의 연산은 $2^i + 1 \equiv 2^{k_i} \pmod{n+1}$ 을 만족하는 k_i 에 따라 오른쪽 순환이동(RCS)에 의하여 수행된다. 한편

$A, B \in GF(2^m) \subset GF(2^n)$ 이므로 m 개의 좌표가 k 번 반복하여 표현되며 $AB \in GF(2^m)$ 이므로 0부터 $m-1$ 까지의 좌표만 고려한다. 따라서 $0 \leq i_0 \leq u$ 에 대해 $B_i, i \in \{i_0, m-i_0, m+i_0, \dots, km/2-i_0\}$ 경우 B_{i_0} 로부터 S_i 의 출력값은 앞에 정의한 ξ_i 에 의한 RCS에 의하여 주어진다.

임의의 원소 $A, B \in GF(2^m) \subset GF(2^n)$ 에 대해 본 발명에서 제안하는 $C=AB$ 는 다음과 같다.

$$C = \sum_{j=0}^{m-1} A_j B_j \beta^{2^j} + \sum_{i_0=1}^u \sum_{w=0}^{k/2-1} \left(\sum_{j=0}^{m-1} x_{j,i_0} \beta^{2^j} \right) 2^{i_0 \cdot 2^w} + \sum_{w=1}^{k/2} \left(\sum_{j=0}^{m-1} x_{j,i_0} \beta^{2^j} \right) 2^{i_0 \cdot 2^w},$$

$$x_{j,i_0} = (A_j \cdot B_{((i_0+j))}) \oplus (A_{((i_0+j))} \cdot B_j), 1 \leq i_0 \leq u = (m-1)/2, 0 \leq j < m-1$$

도 1은 본 발명에 의한 유한체의 병렬곱셈 장치의 구성을 블록도로 도시한 것으로서, 그 병렬곱셈장치는 AB곱셈부(100), x함수부(110), S1함수부(120) 및 BTX1연산부(130)를 포함하여 이루어진다.

상기 AB곱셈부(100)는 유한체 $GF(2^m)$ 이 타입 k 인 가우시안 정규기저를 가지며, $GF(n+1)^* = \langle 2 \rangle$ 이고 $n=mk$ 인 조건을 만족하는 입력 A, B (A, B 는 벡터)에 대해, $A_i * B_i$ 에 의해 A, B 를 수학식 1에 의해 곱한다.

$$\text{수학식 1}$$

$$A * B = A_i * B_i$$

상기 AB곱셈부(100)는 입력 A 와 입력 B 를 논리곱연산하며, 유한체 $GF(2^m)$ 에서의 m 에 해당하는 개수만큼의 AND게이트로 이루어짐이 바람직하다.

상기 x함수부(110)는 입력 A, B 에 대해 수학식 2에 의해 연산된다.

$$\text{수학식 2}$$

$$x_{j,i_0} = (A_j \cdot B_{((i_0+j))}) \oplus (A_{((i_0+j))} \cdot B_j)$$

여기서, $1 \leq i_0 \leq u = (m-1)/2, 0 \leq j < m-1$.

도 2는 상기 x함수부(110)의 보다 상세한 구성을 블록도로 도시한 것으로서, $u = (m-1)/2$ 개의 그룹으로 이루어지고, 상기 그룹은 m 개의 서브그룹으로 이루어진다.

도 3은 상기 서브그룹의 보다 상세한 구성을 블록도로 도시한 것으로서, 상기 서브그룹은 A_j 와 $B_{((i_0+j))}$ 를 논리곱 연산하는 제1AND게이트(300), $A_{((i_0+j))}$ 와 B_j 를 논리곱 연산하는 제2AND게이트(320) 및 상기 제1AND게이트(300) 및 제2AND게이트(320)의 출력을 배타논리합하는 XOR게이트(340)를 구비하여 이루어진다. 여기서 $((a+b))$ 는 $((a+b)) = (a+b) \bmod m$ 이다.

상기 S1함수부(120)는 상기 x함수부(110)의 결과값을 입력으로 하여 수학식 3에 따라 오른쪽 순환이동(right cyclic shift) 수행한다.

$$\text{수학식 3}$$

$$S1 = x^{2^{i_0 \cdot 2^w}}$$

상기 S1함수부(130)는 x함수부의 서브그룹 개수(u 개)에 해당하는 S1함수 맵핑그룹으로 이루어지고, 상기 S1함수 맵핑그룹은 k 개의 단위맵핑부로 이루어진다. 상기 단위맵핑부는 상기 x함수부의 서브그룹에서 출력되는 m 비트의 데이터를 입력으로 하여 수학식 5와 같은 ζ 함수에 의해

수학식 5

$$\xi_i = \begin{cases} k_i \bmod m, & i \equiv i_0 \bmod m \\ k_i + i_0 \bmod m, & i \equiv -i_0 \bmod m \end{cases}$$

m 개의 출력으로 오른쪽 순환이동 매핑한다.

상기 BTX1 연산부(130)는 상기 AB곱셈부(100)의 결과값과 상기 S1함수부(120)의 결과값을 최종 출력의 각 자리에 수학식 4에 의해 맵핑시켜 더한다.

수학식 4

$$C = \sum_{j=0}^{m-1} A_j B_j \beta^{2^j} + \sum_{i_0=1}^u \sum_{w=0}^{k/2-1} \left(\sum_{j=0}^{m-1} x_{j,i_0} \beta^{2^j} \right) 2^{c_{w,i_0}} + \sum_{w=1}^{k/2} \left(\sum_{j=0}^{m-1} x_{j,i_0} \beta^{2^j} \right) 2^{c_{w,i_0}},$$

$$x_{j,i_0} = (A_j \cdot B_{((i_0+j))}) \oplus (A_{((i_0+j))} \cdot B_j), 1 \leq i_0 \leq u = (m-1)/2, 0 \leq j < m-1.$$

도 4는 상기 BTX1 연산부(130)의 보다 상세한 구성을 블록도로 도시한 것으로서, 상기 BTX1 연산부는 m 개의 서브 BTX1 연산부(400, 410, 420)로 이루어진다.

도 5는 상기 서브BTX1 연산부(400)의 보다 상세한 구성을 도시한 것으로서, 상기 AB곱셈부(100)의 결과값과 상기 S1함수부(120)의 단위매핑부의 결과값에 대해 상기 수학식 4에 의해 결정되는 입력값을 배타논리합 연산하는 XOR 게이트가 이진트리로 구성된다.

도 6은 본 발명에 의한 병렬곱셈장치의 개념을 블록도로 도시한 것이다.

도 7은 본 발명의 실시예에 해당하는, AOP를 이용한 병렬곱셈기의 구체적인 블록도를 도시한 것이다.

② Reyhani-Masoleh 와 Hasan의 곱셈기를 이용한 본 발명에 의한 유한체 GF(2^m)에서의 병렬 곱셈기

본 발명은 2003년에 Reyhani-Masoleh 와 Hasan이 제안한 AND연산을 감소시키는 연산기를 이용하여 유한체 GF(2^m)에서 곱셈을 수행하는 새로운 병렬 곱셈 연산기를 구성한다. 즉 유한체 GF(2ⁿ)가 타입 I의 최적 정규기저를 가지며 γ 가 이 정규기저의 생성자라고 하고, 임의의 원소 $A, B \in GF(2^m) \subset GF(2^n)$ 이면 C=AB는 다음과 같다.

$$C = \sum_{j=0}^{m-1} A_j B_j \beta^{2^j} + \sum_{i_0=1}^u \sum_{w=0}^{k/2-1} \left(\sum_{j=0}^{m-1} y_{j,i_0} \beta^{2^j} \right) 2^{c_{w,i_0}} + \sum_{w=1}^{k/2} \left(\sum_{j=0}^{m-1} y_{j,i_0} \beta^{2^j} \right) 2^{c_{w,i_0}},$$

$$y_{j,i_0} = (A_j \oplus A_{((i_0+j))}) \cdot (B_{((i_0+j))} \oplus B_j), 1 \leq i_0 \leq u, 0 \leq j \leq m-1.$$

기존의 곱셈기에서는 $a_i \cdot b_i = A_{((i))} \cdot B_{((i))} \quad 0 \leq i \leq n-1$ 를 계산해야 한다. 그러나 본 발명에서는 수학식 1에 의하여 $A_i \cdot B_i, 0 \leq i \leq m-1$ 만 계산하면 된다. 따라서 m개의 AND연산이 주어진다. 또한,

$y_{j,i} = (a_j \oplus a_{\ll i+j \gg}) \cdot (b_j \oplus b_{\ll i+j \gg}), 1 \leq i \leq v = n/2, 0 \leq j \leq n-1$ 를 계산하기 위해 수학식 1이 성립하므로, 다음이 성립한다.

$$A_i = a_{i+mj}, 0 \leq i \leq m-1, 0 \leq j \leq k-1, B_i = b_{i+mj}, 0 \leq i \leq m-1, 0 \leq j \leq k-1$$

또한 $i = i_0 + tm, 1 \leq j_0 \leq m-1, 0 \leq w \leq k/2-1$ 과

$j = j_0 + tm, 0 \leq j_0 \leq m-1, 0 \leq t \leq k-1$ 일 때 다음과 같다.

$$\begin{aligned}
 y_{j,i} &= (a_j \oplus a_{\ll i+j \gg}) \cdot (b_j \oplus b_{\ll i+j \gg}) \\
 &= (a_{j_0+tm} \oplus a_{\ll i_0+wm+j_0+tm \gg}) \cdot (b_{j_0+tm} \oplus b_{\ll i_0+wm+j_0+tm \gg}) \\
 &= (a_{j_0} \oplus a_{\ll (i_0+j_0) \gg}) \cdot (b_{j_0} \oplus b_{\ll (i_0+j_0) \gg}) \\
 &= (A_{j_0} \oplus A_{\ll (i_0+j_0) \gg}) \cdot (B_{j_0} \oplus B_{\ll (i_0+j_0) \gg})
 \end{aligned}$$

만약, $i = u + s, u = \lfloor m/2 \rfloor, 1 \leq s \leq u$ 인 경우 $i_0 = m - i$ 라 하면 $1 \leq i_0 \leq u$ 이며 다음과 같다.

$$\begin{aligned}
 y_{j,i} &= (a_j \oplus a_{\ll j+u+s \gg}) \cdot (b_j \oplus b_{\ll j+u+s \gg}) \\
 &= (a_{\ll j+u+s \gg} \oplus a_j) \cdot (b_{\ll j+u+s \gg} \oplus b_j) \\
 &= (A_{\ll (j+u+s) \gg} \oplus A_{\ll (j) \gg}) \cdot (B_{\ll (j+u+s) \gg} \oplus B_{\ll (j) \gg}) \\
 &= y_{\ll (j+u+s) \gg, \ll (m-(u+s)) \gg} = y_{\ll (j+i) \gg, i_0}
 \end{aligned}$$

$i = m, 2m, \dots, v = mk/2$ 인 경우 다음이 성립한다.

$$\begin{aligned}
 y_{j,i} &= (a_j \oplus a_{\ll tm+j \gg}) \cdot (b_j \oplus b_{\ll tm+j \gg}) \\
 &= (A_{\ll (j) \gg} \oplus A_{\ll (j) \gg}) \cdot (B_{\ll (j) \gg} \oplus B_{\ll (j) \gg}) = 0
 \end{aligned}$$

따라서 $y_{j,i}$ 는, $0 \leq j \leq m-1, 1 \leq i \leq u = (m-1)/2$ 인 경우만 계산하며, $i = m, 2m, \dots, m(k/2-1)$ 의 계산은 할 필요가 없음을 알 수 있다. 유한체 $GF(2^m)$ 은 $GF(2^n)$ 의 부분체이므로 부분체의 성질에 의하여 $GF(2^n)$ 에서 m 개의 좌표를 수행한다. 따라서 타입 k 인 유한체 $GF(2^m)$ 에서 $n = mk, GF(n+1)^* = \langle 2 \rangle$ 라 하고, 임의의 원소

$A, B \in GF(2^m) \subset GF(2^n)$ 이면 $C = AB$ 는 다음과 같다.

$$C = \sum_{j=0}^{m-1} A_j B_j \beta^{2^j} + \sum_{i_0=1}^u \sum_{w=0}^{k/2-1} \left(\sum_{j=0}^{m-1} y_{j,i_0} \beta^{2^j} \right) 2^{t_{w,i_0}} + \sum_{w=1}^{k/2} \left(\sum_{j=0}^{m-1} y_{j,i_0} \beta^{2^j} \right) 2^{t_{w,i_0}},$$

$$y_{j,i_0} = (A_j \oplus A_{\ll (i_0+j) \gg}) \cdot (B_{\ll (i_0+j) \gg} \oplus B_j), 1 \leq i_0 \leq u, 0 \leq j \leq m-1.$$

본 발명에서 제안하는 병렬 곱셈기는 B_i 의 출력이 $y_{j,i}$ 가 되도록 입력을 $A_j, A_{\ll (j+i) \gg}, B_j, B_{\ll (j+i) \gg}$ 로 바꾸어 다시 구성하면 도 8과 같다. 또한 $A_j \cdot B_j$ 값이 BTX의 j 번째 좌표의 입력값이 되도록 조정한다.

상술한 Reyhani-Masoleh 와 Hasan의 곱셈기를 이용한 본 발명에 의한 유한체 $GF(2^m)$ 에서의 병렬 곱셈기는, AB곱셈부, y 함수부, S2함수부, BTX2 연산부를 포함하여 이루어진다.

상기 AB곱셈부는 유한체 $GF(2^m)$ 이 타입 k 인 가우시안 정규기저를 가지며, $GF(n+1)^* = \langle 2 \rangle$ 이고 $n = mk$ 인 조건을 만족하는 입력 A, B (A, B 는 벡터)에 대해, $A_i * B_i$ 에 의해 A, B 를 수학식 1에 의해 곱한다.

상기 AB곱셈부는 입력 A 와 입력 B 를 논리곱연산하며, 유한체 $GF(2^m)$ 에서의 m 에 해당하는 개수만큼의 AND게이트로 이루어진다.

상기 y 함수부는 입력 A, B 에 대해 수학식 6에 의해 연산된다.

수학식 6

$$y_{j,i_0} = (A_j \oplus A_{((i_0+j))}) \cdot (B_{((i_0+j))} \oplus B_j)$$

여기서, $1 \leq i_0 \leq u$, $0 \leq j \leq m-1$

상기 y함수부는 m개의 그룹으로 이루어지고, 상기 그룹은 $u = (m-1)/2$ 개의 서브그룹으로 이루어진다. 상기 서브그룹은 A_j 와 $A_{((i_0+j))}$ 를 배타논리합 연산하는 제1XOR게이트와, B_j 와 $B_{((i_0+j))}$ 를 배타논리합 연산하는 제2XOR게이트와, 상기 제1XOR게이트 및 제2XOR게이트의 출력을 논리곱연산하는 AND게이트를 구비하여 이루어진다. 여기서 $((a+b))$ 는 $((a+b)) = (a+b) \bmod m$ 이다.

상기 S2함수부는 상기 y 함수부의 결과값을 입력으로 하여 수학식 7에 따라 오른쪽 순환이동(right cyclic shift) 수행한다.

수학식 7

$$S2 = y^{2^{c_{m-i}}}$$

상기 S2함수부는 y 함수부의 서브그룹 개수(u개)에 해당하는 S2함수 맵핑그룹으로 이루어지고, 상기 S2함수 맵핑그룹은 k 개의 단위맵핑부로 이루어진다. 상기 단위맵핑부는 상기 y 함수부의 서브그룹에서 출력되는 m 비트의 데이터를 입력으로 하여 수학식 5와 같은 ξ 함수에 의해 m 개의 출력으로 오른쪽 순환이동 매핑한다.

[수학식 5]

$$\xi_i = \begin{cases} k_i \bmod m, & i \equiv i_0 \bmod m \\ k_i + i_0 \bmod m, & i \equiv -i_0 \bmod m \end{cases}$$

상기 BTX2연산부는 상기 AB곱셈부의 결과값과 상기 S2함수부의 결과값을 최종 출력의 각 자리에 수학식 4에 의해 맵핑시켜 더한다.

수학식 8

$$C = \sum_{j=0}^{m-1} A_j B_j \beta^{2^j} + \sum_{i_0=1}^u \sum_{j=0}^{k/2-1} \left(\sum_{j=0}^{m-1} y_{j,i_0} \beta^{2^j} \right) 2^{c_{m+i_0}} + \sum_{j=1}^{k/2} \left(\sum_{j=0}^{m-1} y_{j,i_0} \beta^{2^j} \right) 2^{c_{u+i_0}},$$

여기서, $y_{j,i_0} = (A_j \oplus A_{((i_0+j))}) \cdot (B_{((i_0+j))} \oplus B_j)$, $1 \leq i_0 \leq u$, $0 \leq j \leq m-1$

상기 BTX2 연산부는 m 개의 서브BTX2 연산부로 이루어지고, 상기 서브BTX2 연산부는 상기 AB곱셈부의 결과값과 상기 S2함수부의 단위매핑부의 결과값에 대해 상기 수학식 8에 의해 결정되는 입력값을 배타논리합 연산하는 XOR 게이트가 이진트리로 구성된다.

도 9는 타입IV의 가우시안 정규기저를 갖는 유한체 $GF(2^7)$ 의 병렬곱셈 연산기의 일실시예를 도시한 것이다.

본 발명은 컴퓨터로 읽을 수 있는 기록 매체에 컴퓨터(정보 처리 기능을 갖는 장치를 모두 포함한다)가 읽을 수 있는 코드로서 구현하는 것이 가능하다. 컴퓨터가 읽을 수 있는 기록 매체는 컴퓨터 시스템에 의하여 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기록 장치를 포함한다. 컴퓨터가 읽을 수 있는 기록 장치의 예로는 ROM, RAM, CD-ROM, 자기 테이프, 플로피 디스크, 광데이터 저장장치 등이 있다.

본 발명은 도면에 도시된 실시예를 참고로 설명되었으나 이는 예시적인 것에 불과하며, 본 기술 분야의 통상의 지식을 가진 자라면 이로부터 다양한 변형 및 균등한 타 실시예가 가능하다는 점을 이해할 것이다. 따라서, 본 발명의 진정한 기술적 보호 범위는 첨부된 등록청구범위의 기술적 사상에 의해 정해져야 할 것이다.

발명의 효과

상술한 바와 같이 본 발명에 의하면, 암호학적으로 많이 응용되는 유한체인 타입 $k=2,4,6$ 에 본 발명을 적용하면, 가장 효율적인 Reyhani-Masoleh와 Hasan의 곱셈기와 동일한 공간 및 시간 복잡도를 갖는다. 따라서 암호관련 응용분야의 하드웨어 구현에 유용하게 적용할 수 있다.

그리고 본 발명에 의한 병렬곱셈장치에 대한 성능평가를 한 결과 다음과 같다.

① 성능

가. 타입 $k=4$ 인 경우

m 이 홀수, $p=4m+1$ 은 소수, $GF(p)^*=\langle 2 \rangle$ 이고 예 $u=(m-1)/2$ 대하여, Z_p^* 에서

$$\begin{cases} 2^u+1=2^{k_1}, & 2^{m-u}+1=2^{k_2}, \\ 2^{m+u}+1=2^{k_3}, & 2^{2m-u}+1=2^{k_4} \end{cases}$$

이라고 하자. m 이 2000이하의 경우에 대하여 $u=(m-1)/2$ 또는 $k_3=k_4+u \pmod m$ 중 하나가 성립함을 확인하였다. 따라서 타입 IV의 경우는 $2m$ 개의 XOR gate수를 줄일 수 있다. 예를 들어 타입 IV인 권장 타원곡선인 $m=163$ 인 경우, $i=163+81, 2*163-81$ 일 때 $\xi_i=81$ 로 같다. $m=409$ 인 경우, $i=409+204, 2*409-204$ 일 때 $\xi_i=204$ 로 같다.

나. 타입 $k=6$ 인 경우

타입 $k=6$ 을 만족하는 1000이하에 m 에 대하여 i 에 대한 ξ_i 가 같은 쌍으로 4개 나타난다. 즉 $m=103$ 인 경우, $i=2*103-1, 2*103+1$ 일 때, $\xi_i=89$ 이고, $i=14, 103-14$ 일 때 14, $i=2*103+14, 2*103-14$ 일 때 15, $i=15, 103-15$ 일 때 14이다. 만약 m 이 홀수, $p=6m+1$ 은 소수, $GF(p)^*=\langle 2 \rangle$ 라 하면 이를 이용하여 $1 \leq i_0 \leq u=(m-1)/2$ 에 대해 $i=i_0, m-i_0, m+i_0, \dots, km/2-i_0$ 일 때 ξ_i 의 같은 쌍이 4개 존재한다. 따라서 타입 VI의 경우는 XOR gate를 8m 개를 감소시킬 수 있다는 것을 알 수 있다.

다. 타입 $k=10$ 인 경우

타입 $k=10$ 을 만족하는 1000이하에 m 에 대해 i 에 대한 ξ_i 의 같은 쌍이 16개 나타난다. 먼저 i_0 에 대하여 수식 4의 예 대한 ξ_i 가 같을 때를 $\{i_0, i_1, i_2, \xi_i\}$ 로 표현하면 $m=337$ 인 경우는 다음과 같다.

$\{6, m-6, 2*m+6, 278\}, \{7, 7, m+7, 116\}, \{7, m-7, 2*m+7, 0\}, \{51, m+51, 2*m+51, 51\}, \{51, 2*m-51, 5*m-51, 272\}, \{52, m+52, 2*m+51, 109\}, \{57, m-57, 5*m-57, 285\}, \{58, m-58, 5*m-58, 0\}, \{58, 2*m-58, 4*m-58, 58\}, \{59, 2*m-59, 4*m-59, 65\}, \{65, 65, 5*m-65, 59\}, \{65, 2*m+65, 3*m+65, 116\}, \{109, m+109, 4*m-109, 52\}, \{109, 2*m+109, 5*m-109, 330\}, \{116, 116, 2*m-116, 65\}, \{116, 2*m+116, 4*m-116, 7\}.$

만약 m 이 홀수, $p=10m+1$ 또는 $12m+1$ 이 소수, $GF(p)^*=\langle 2 \rangle$ 이면 $1 \leq i_0 \leq u=(m-1)/2$ 에 대해 $i=i_0, m-i_0, m+i_0, \dots, km/2-i_0$ 일 때 ξ_i 가 같은 쌍이 $k=10$ 이면 16개, $k=12$ 이면 25개 존재한다. 따라서 타입 X의 경우 32m개, XII의 경우 50개의 XOR gate 수를 줄일 수 있다.

한편, 본 발명은 Reyhani-Masoleh과 Hasan의 곱셈기를 이용한 유한체 GF(2^m)에서의 병렬 곱셈기인 경우 최대 복잡도는 다음과 같다. 여기서 T_A는 AND delay, T_X는 XOR Delay 이다.

a) m² AND gate.

b) (k+1)m(m-1)/2 XOR gate.

c) $T_A + \lceil \log_2 \{k(m-1) + 2\} \rceil T_X$

또한 타입 II의 최적 정규기저를 가지는 유한체 GF(2^m)에서 본 발명의 복잡도는 다음과 같다.

a) m² AND gate, $\frac{3}{2} m(m-1)$ XOR gate

b) $T_A + (1 + \lceil \log_2 m \rceil) T_X$

타입 IV의 최적 정규기저를 가지는 유한체 GF(2^m)에서 본 발명의 복잡도는 다음과 같다.

a) m² AND gate, $m(7m-23)/2$ XOR gate

b) $T_A + \lceil \log_2 (4m-6) \rceil T_X = T_A + \lceil \log_2 C_N \rceil T_X$

타입 VI의 최적 정규기저를 갖는 유한체 에서 본 발명의 복잡도는 다음과 같다.

a) m² AND gate, $m(7m-23)/2$ XOR gate.

b) $T_A + \lceil \log_2 (6m-20) \rceil T_X = T_A + \lceil \log_2 C_N \rceil T_X$

본 발명은 2003년에 제안된 Reyhani-Masoleh 와 Hasan의 곱셈기를 이용한 유한체 GF(2^m)에서의 병렬 곱셈기인 경우 최대 복잡도는 다음과 같다. 여기서 T_A는 AND delay, T_X는 XOR Delay 이다.

a) m(m+1)/2 AND gate.

b) (k+2)m(m-1)/2 XOR gate.

c) $T_A + \lceil \log_2 \{k(m-1) + 2\} \rceil T_X$

또한 타입 II의 최적 정규 기저를 갖는 유한체 GF(2^m)에서 본 발명의 복잡도는 다음과 같다.

a) m(m+1) AND gate.

b) 2m(m-1) XOR gate.

c) $T_A + \lceil \log_2 C_N \rceil T_X$

타입 IV의 최적 정규기저를 갖는 유한체 에서 본 발명의 복잡도는 다음과 같다.

a) $m(m+1)/2$ AND gate.

b) $m(3m-5)$ XOR gate.

$$c) T_A + \lceil \log_2 C_N \rceil T_X$$

타입 VI의 최적 정규기저를 갖는 유한체 $GF(2^m)$ 에서 본 발명의 복잡도는 다음과 같다.

a) m^2 AND gate.

b) $4m(m-3)$ XOR gate.

$$c) T_A + \lceil \log_2 C_N \rceil T_X$$

타입 (m,10) 또는 (m,12)인 가우스 주기를 갖는 유한체에서의 연산기는 16, 25쌍의 ξ_i 가 각각 일치하므로, 최대 복잡도에서 32m, 50m개의 XOR gate를 빼며 그에 따른 T_X 값도 줄어드는 것이다.

Multipliers		#AND	#XOR	Time Delay
2002년에 제안된 Reyhani-Masoleh과 Hasan의 곱셈기를 이용한 유한체 $GF(2^m)$ 에서의 병렬 곱셈기	General	m^2	$(k+1)m(m-1)/2$	$\leq T_A + \lceil \log_2\{k(m-1)+2\}T_X \rceil$
	Type IV	m^2	$m(5m-9)/2$	$T_A + \lceil \log_2(4m-7) \rceil T_X$
	Type VI	m^2	$m(7m-23)/2$	$T_A + \lceil \log_2(6m-21) \rceil T_X$
2003년에 제안된 Reyhani-Masoleh과 Hasan의 곱셈기를 이용한 유한체 $GF(2^m)$ 에서의 병렬 곱셈기	General	$m(m+1)$	$\leq (k+2)m(m-1)$	$\leq T_A + \lceil \log_2\{k(m-1)+2\}T_X \rceil$
	Type IV	$m(m+1)$	$m(3m-5)$	$T_A + \lceil \log_2(4m-7) \rceil T_X$
	Type VI		$4m(m-3)$	$T_A + \lceil \log_2(6m-21) \rceil T_X$

② 예제

$m=7, k=4$ 이면, $n=29, p=29$ 이므로 $GF(29)^* = \langle 2 \rangle$ 이다. 각 i 에 대한 k_i 와 ξ_i 의 값을 $\{i, k_i, \xi_i\}$ 와 같이 표현하면 다음과 같다.

$\{1, 5, 5\}, \{7-1, 12, 6\}, \{7+1, 16, 2\}, \{2*7-1, 27, 0\}, \{2, 22, 1\}, \{7-2, 2, 4\}, \{7+2, 24, 3\}, \{2*7-2, 3, 5\}, \{3, 10, 3\}, \{7-3, 21, 3\}, \{7+3, 23, 2\}, \{2*7-3, 9, 5\}.$

따라서, $i=i_0=3, i=7-i_0=4$ 에서 $\xi_i=3$ 이 동일한 값이므로 S_3, S_4 는 삭제하여도 된다.

도면의 간단한 설명

도 1은 본 발명에 의한 유한체의 병렬곱셈 장치의 구성을 블록도로 도시한 것이다.

도 2는 도 1의 x함수부의 보다 상세한 구성을 블록도로 도시한 것이다.

도 3은 도 2의 서브그룹의 보다 상세한 구성을 블록도로 도시한 것이다.

도 4는 도 1의 BTX1 연산부의 보다 상세한 구성을 블록도로 도시한 것이다.

도 5는 도 4의 서브BTX1 연산부의 보다 상세한 구성을 도시한 것이다.

도 6은 본 발명에 의한 병렬곱셈장치의 개념을 블록도로 도시한 것이다.

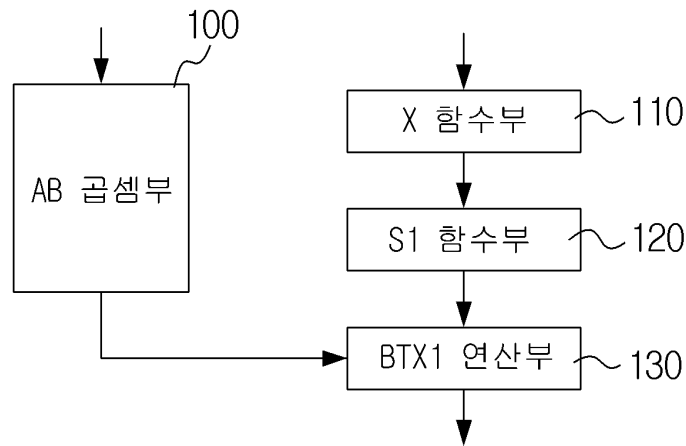
도 7은 본 발명의 실시예에 해당하는, AOP를 이용한 병렬곱셈기의 구체적인 블록도를 도시한 것이다.

도 8은 $y_{j,i}$ 연산을 위한 블록을 게이트로 도시한 것이다.

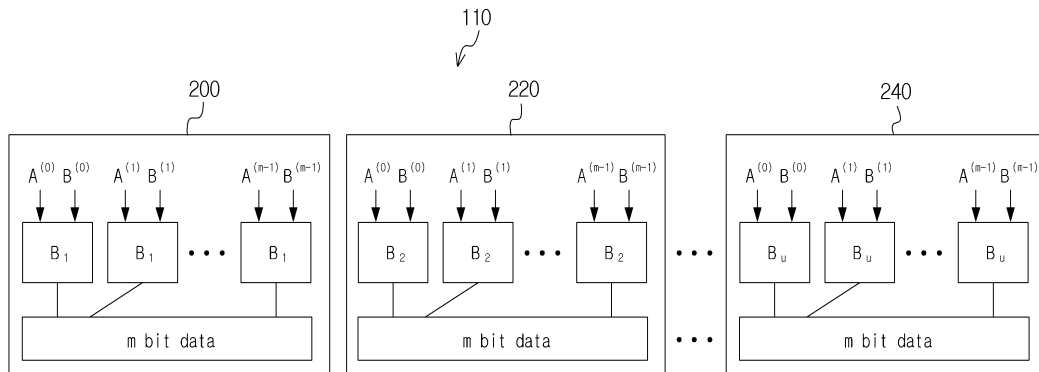
도 9는 타입IV의 가우시안 정규기저를 갖는 유한체 $GF(2^7)$ 의 병렬곱셈 연산기의 일실시예를 도시한 것이다.

도면

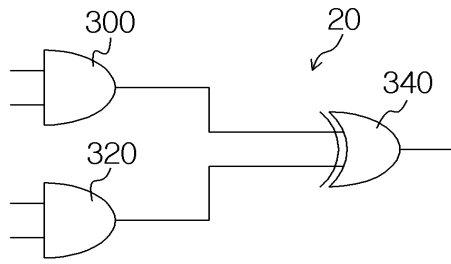
도면1



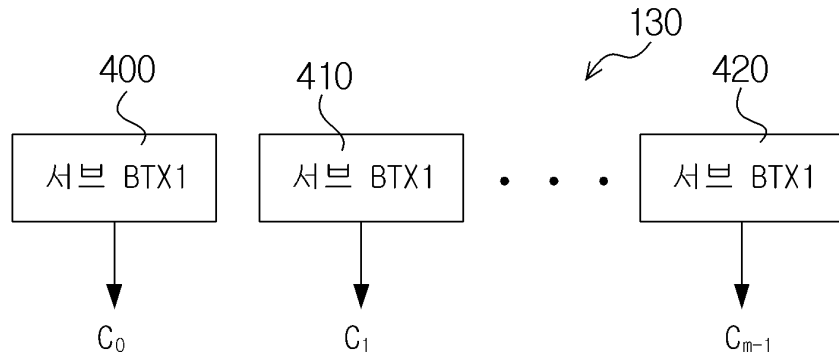
도면2



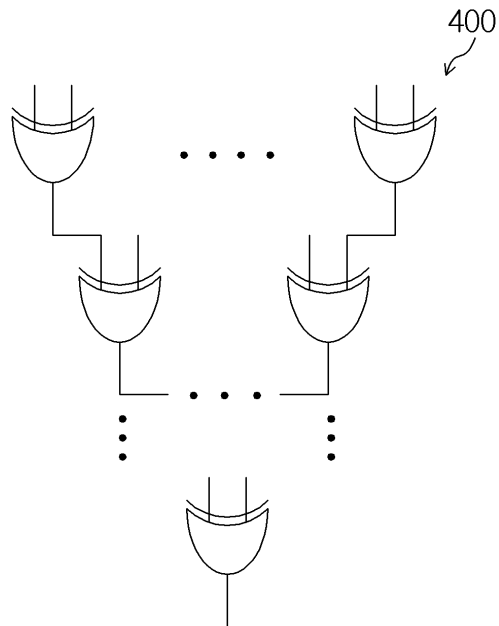
도면3



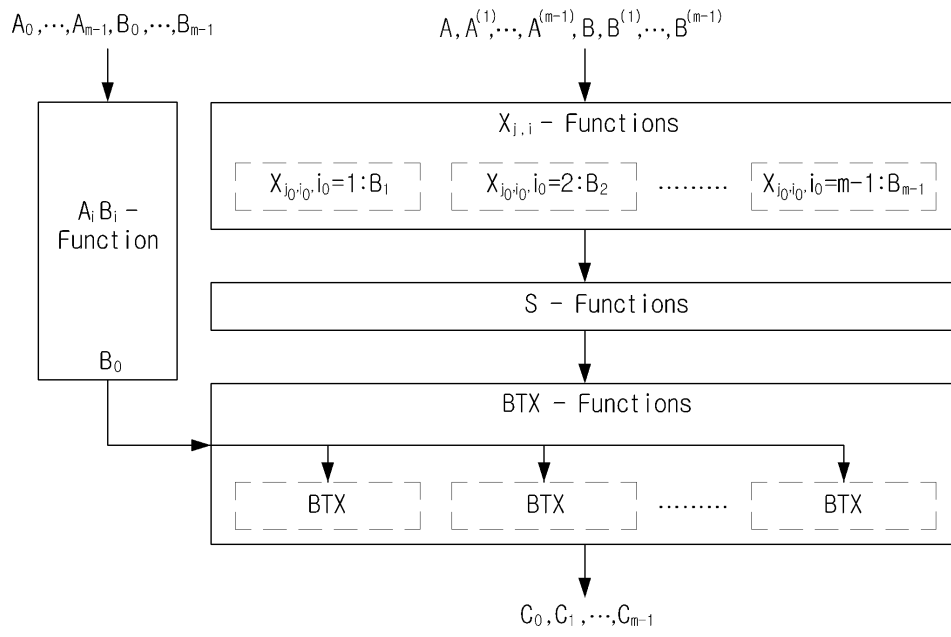
도면4



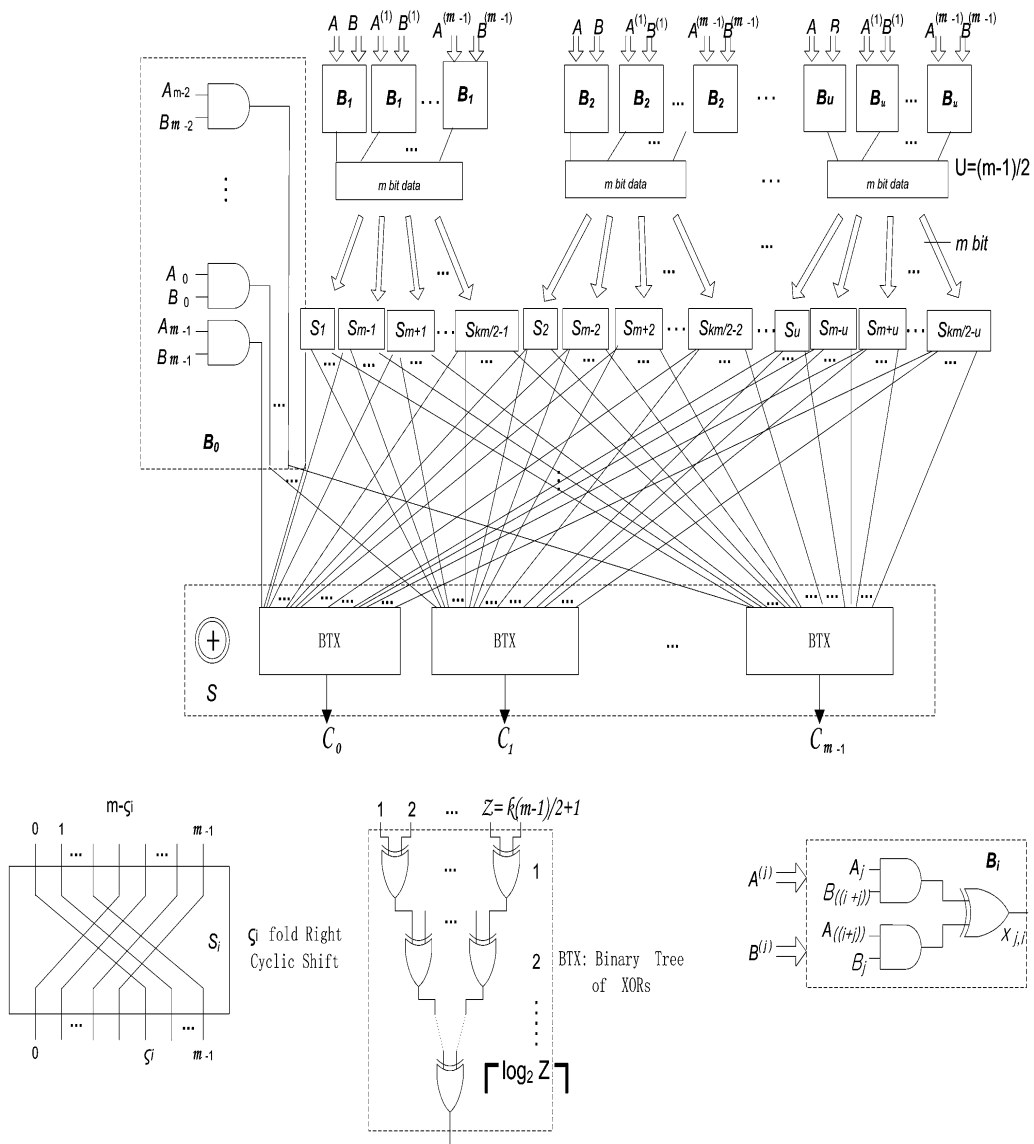
도면5



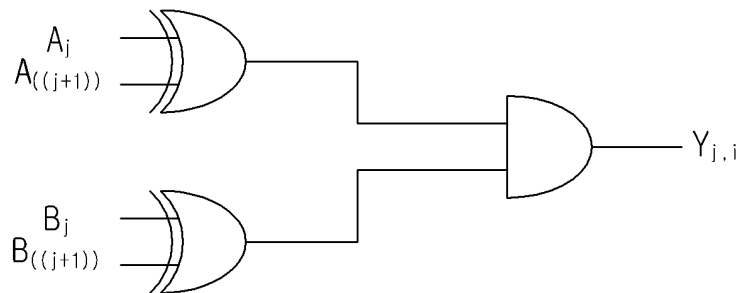
도면6



도면7



도면8



도면9

