타원 곡선 암호 프로세서용 GF(2^m) Inversion, Division 회로 설계 및 구현

현 주 대, 최 병 윤
동의대학교 컴퓨터 공학과
전화 : 051-890-1704 / 핸드폰 : 016-579-0463

VLSI Design and Implementation of Inversion and Division over GF(2^m) for Elliptic Curve Cryptographic System

Ju-Dai Hyun, Byeong-Yoon Choi
Dept. of Computer engineering, Dongeui University
E-mail : highfreq@dongeui.ac.kr

Abstract

In this paper, we designed GF(2^m) inversion and division processor for Elliptic Curve Cryptographic system. The processor that has 191 by m value designed using Modified Euclid Algorithm. The processor is designed using 0.35 μm CMOS technology and consists of about 14,000 gates and consumes 370 mW. From timing simulation results, it is verified that the processor can operate under 367 Mhz clock frequency due to 2.72 ns critical path delay. Therefore, the designed processor can be applied to Elliptic Curve Cryptographic system.

I. 서론

통신 당사자가 각각의 비밀키를 보유하고 이를 통해 데이터의 암, 복호화만 수행하면 안전한 통신이 보장되는 대칭키 암호 방식에 비해 불특정 다수와 안전한 통신을 위해서는 효율적인 키 관리와 분배기법 필요하다. 작은 길이의 키로 다수의 상대방과 안전한 통신을 가능하게 하고 전자서명 용도로도 활용할 수 있는 효율적 암호기법이 공개키 방식이다. 지금까지의 대부분의 공개키 암호 방식은 RSA가 주도 해왔다. 그러나 RSA를 이용한 공개키 암호시스템은 높은 신뢰성을 위해서 더욱 큰 길이의 키가 필요하고, 키 길이의 증가는 더 많은 연산량과 더 많은 하드웨어 면적을 필요로 한다. 이 문제의 대처 방안으로 1985년 Neal Koblitz[1]와 Victor Miller[2]에 의해 개발된 타원 곡선 암호 시스템이 주목되고 있다. 키 길이가 1백60비트인 타원 곡선 암호 시스템은 1024비트인 RSA암호와 유사한 안전성을 가진다. 키 길이가 시스템의 성능과 면적에 직결되는 점을 감안하면 RSA에 비해 더욱 효율적이라는 결론을 얻을 수 있다. 타원 곡선 암호 시스템의 활용도가 증가함에 따라 본 논문에서 타원 곡선 암호 시스템의 핵심 구성요소인 역원 및 제산 회로의 설계 방안을 제시 한다.

GF(2^m) 상의 제산 회로를 구현하는 방식은 Fermat 방식, Modified Euclid Algorithm, 그리고 Almost Inversion Algorithm등 다양한 방식이 있다[3]. 본 연구에서는 modified Euclid algorithm 방식을 채택하여 역원, 제산 회로를 설계하였다.

본 논문의 구성은 2장에서 Modified Euclid Algorithm에 대해 소개하고, 3장에서 GF(2^m) 역원 및 제산 회로의 설계를 기술하고 4장에서 설계된 회로의 검증과 성능 분석을 기술하고, 5장에서 결론 및 향후 연구 방향을 제시하였다.

II. Modified Euclid Algorithm

2.1 Euclid Algorithm

GF(2^m)상의 역원을 구현하는 다양한 방식이 제안되고 있다. 이러한 방식은 사용하는 기저에 따라 정규 기저(normal basis)에 바탕을 둔 방식과 다항식 기저(polynomial basis)에 바탕을 둔 방식이 있다. 정규 기저 방식을 사용할 경우 제곱 동작이 단순한 이동 동작으로 구현 할 수 있어, 역원 계산이 상대적으로 고속으로 이루어질 수 있으나 이 방식은 동일 하드웨어로 다양한 크기의 필드로 확장이 어렵다는 결점이 있다.

역원 계산의 방식으로는 반복적인 곱셈 동작으로 역원을 계산하는 Fermat 방식, Modified Euclid algorithm, 그리고 almost inversion algorithm이 있다. 본 연구에서는 Modified Euclid Algorithm 방식을 채택하여 역원, 제산 회로를 설계하였다. Euclid Algorithm은 다음과 같다.

Algorithm 1: Euclid Algorithm

Input : A(α), B(α), G(α)
Output : C(α) = A(α) / B(α) mod G(α)

```
R = B(α); S = G(α); U = A(α); V = 0;
while R ≠ 0, do
   Q = S DIV R;
   temp = S - Q • R; S = R; R = temp;
   temp = V - Q • U; V = U; U = temp;
end
(U = C(α))
```

이 알고리즘은 반복의 횟수가 정해져 있지 않기 때문에 하드웨어로 설계시 단점이 될 수 있다.

2.2 Modified Euclid Algorithm

이전에 언급한 Euclid Algorithm의 단점을 보완하기 위해 Modified Euclid Algorithm이 제안 되었다[4]. 다음의 알고리즘과 같이 Modified Euclid Algorithm은 GF(2^m)상의 역원과 제산 연산을 수행하기 위해 항상 2m의 반복회수를 가진다.

Algorithm 2: Modified Euclid Algorithm

Input : A(α), B(α), G(α)
Output : C(α) = A(α) / B(α) mod G(α)

```
R = B(α); S = G(α); U = A(α); V = 0;
count = 0;
for i = 1 to 2m do
   if r_m == 0 then
      R = α • R; U = α • U mod G;
      count = count + 1;
   else
      if s_m == 1 then
         S = S + R; V = V + U;
      end
      S = α • S;
      if count == 0 then
         R <-> S; U <-> v;
         U = α • U mod G;
         count = count - 1;
      end
   end
end
```

III. Modified Euclid Algorithm의 VLSI 설계

본 논문의 역원 • 제산 회로의 사양은 다음과 같다.
$F(2^{191}) = x^{191} + x^9 + 1$
$E : y^2 + xy = x^3 + ax^2 + b$
a=2866537b676752636a68f56554e12640276b649ef7526267
b=2e45ef571f00786f67b0081b9495a3d95462f5de0aa185ec

설계된 GF(2^m)상의 역원 및 제산 회로의 전체 구조는 그림 1에 나타난 것과 같이 각각의 연산을 담당하는 R, S, U, V 레지스터로 구성된 데이터 이를 제어하기 위한 제어 유닛으로 구성되어있다.

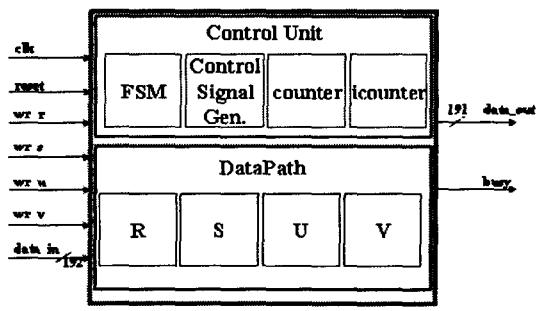

그림 1. 전체 구조.

3.1 Datapath 설계

데이터 패스의 전체 구조는 그림 2와 같이 αR 및 α S 모듈, 가산 모듈, U/α mod G 모듈과 αU mod G 모

듈로 구성된다.

GF(2^m)상에서의 가산 연산은 동일한 차수의 계수들 사이의 합에 Mod 2를 취하므로 xor로 구성할 수 있다. R 레지스터와 S 레지스터의 차수를 증가시키는 αR 모듈과 αS 모듈은 shift 연산으로 구성된다. 그리고 U/α mod G 모듈과 αU mod G 모듈은 그림 3, 4와 같이 LSFR(linear feedback shift register)로 구성하였다.

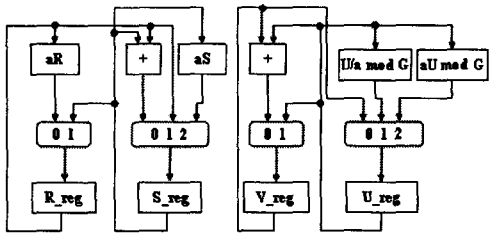

그림 2. 데이터 패스 구조.

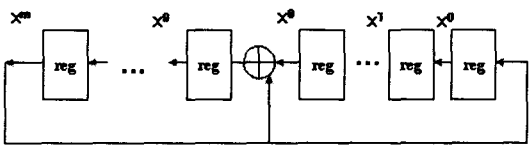

그림 3. αU mod G 모듈.

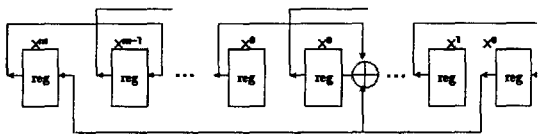

그림 4. U/α mod G 모듈.

3.2 제어 유닛 설계

제어 유닛의 구성은 그림 5와 같이 상태를 지시하는 FSM(Finite State Machine)과 Modified Euclid Algorithm에서 사용하는 i 와 count의 값을 가지는 icnt, cnt 모듈 그리고 데이터 패스의 제어신호를 생성하는 Control Signal Generator 모듈로 구성된다.

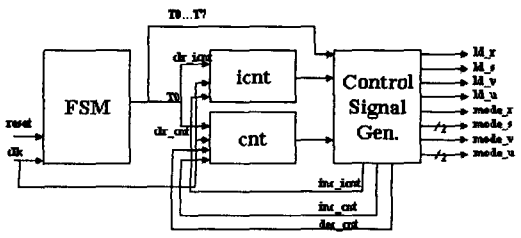

그림 5. 제어 유닛 구조.

Modified Euclid Algorithm을 ASM 챠트로 표현하면 그림 6과 같다. 그림 6에 나타난 것과 같이 Modified Euclid Algorithm은 R 레지스터와 S 레지스터의 MSB값에 의해 역원 혹은 제산 연산시 필요한 클럭의 수는 가변적이다.

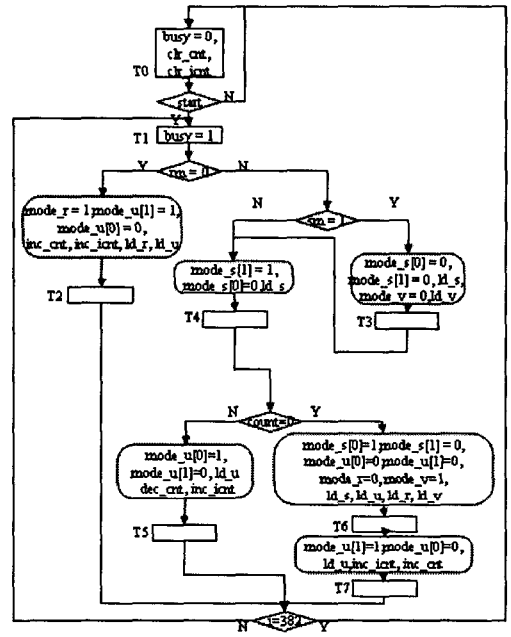

그림 6. Modified Euclid Algorithm의 FSM

Ⅳ. 검증 및 성능 분석

본 연구에서 설계한 역원 및 제산 회로는 Verilog-HDL 언어로 구현하고, Synopsys Design Analyzer[5]로 합성한 후, Cadence Verilog-XL[6] 시뮬레이터로 올바른 동작이 이루어지는지 검증하였다.

설계된 역원 및 제산회로는 0.35μm CMOS 셀 라이브러리로 합성한 결과, 최대 전파 지연시간이 약 2.72 ns이므로, 최대 동작 주파수는 약 367 MHz 임을 확인하였고, 전체 게이트 수는 약 14,000 이고, 소비전력은 약 370 mW 임을 확인 하였다.

Ⅴ. 결론

본 논문에서는 성능과 면적측면에서 효율적인 타원곡선 암호 프로세서용 GF(2^m)상의 역원 및 제산 회로를 설계 하였다. 다항식 기저의 역원 및 제산회로는 다양한 알고리즘이 제시되고 있다. 본 논문은 Modified Euclid Algorithm을 이용하여 설계하였다. 설계된 회로

의 합성결과, 0.35μm 공정에서 약 14,000개의 게이트 수와, 267 MHz의 최대 동작 주파수를 가진다. 따라서 본 논문에서 설계한 역원 및 제산회로는 타원 곡선 암호 시스템이나 RS-Code 등에서 활용될 수 있을 것으로 판단된다.

본 연구에서 설계한 $GF(2^m)$ 상의 역원 및 제산회로의 m 값은 192로 고정되어 있다. 고정된 유한체상의 연산은 성능상의 이점이 있으나, 다양한 암호시스템 적용하기에 제한이 있다. 따라서 가변적 유한체상에서의 역원 및 제산회로의 연구가 요구된다.

표 1. 설계된 회로의 전기적 특성

사용 알고리즘	Modified Euclid Algorithm
사용 field	$F(2^{191}) = x^{191} + x^9 + 1$
사용 곡선	$E : y^2 + xy = x^3 + ax^2 + b$
최대 동작 주파수	367 MHz
최소 요구 클럭 수	382
최대 요구 클럭 수	1,528
면적	14,000
소비 전력	370 mW

감사의 글

본 논문은 회로 구현에 IDEC 지원 장비를 사용하였습니다.

참고문헌

[1] N. Koblitz, "Elliptic curve Cryptosystem", Mathematics of Computation, vol. 48, pp. 203 - 209, 1987.

[2] V. Miller, "Use of elliptic curves in cryptography", Advances in Cryptology, Crypto '85, LNCS 218, pp. 417 - 426, 1986.

[3] 최병윤, 암호 프로세서용 제어기 설계에 관한 연구, 한국 전자 통신 연구원 위탁 과제 최종 연구 보고서, 1999.11.

[4] H. runner, A. Curiger, and M. Hofstetter, "On computing multiplicative inverses in $GF(2^m)$, IEEE Trans. Comput., vol. 42, pp. 1010-1015, 1993.8.

[5] IDEC, "Synopsys tools 교육", 1999.4

[6] CADENCE, Verilog-XL Reference Manual volume 1-2, 1991.3.

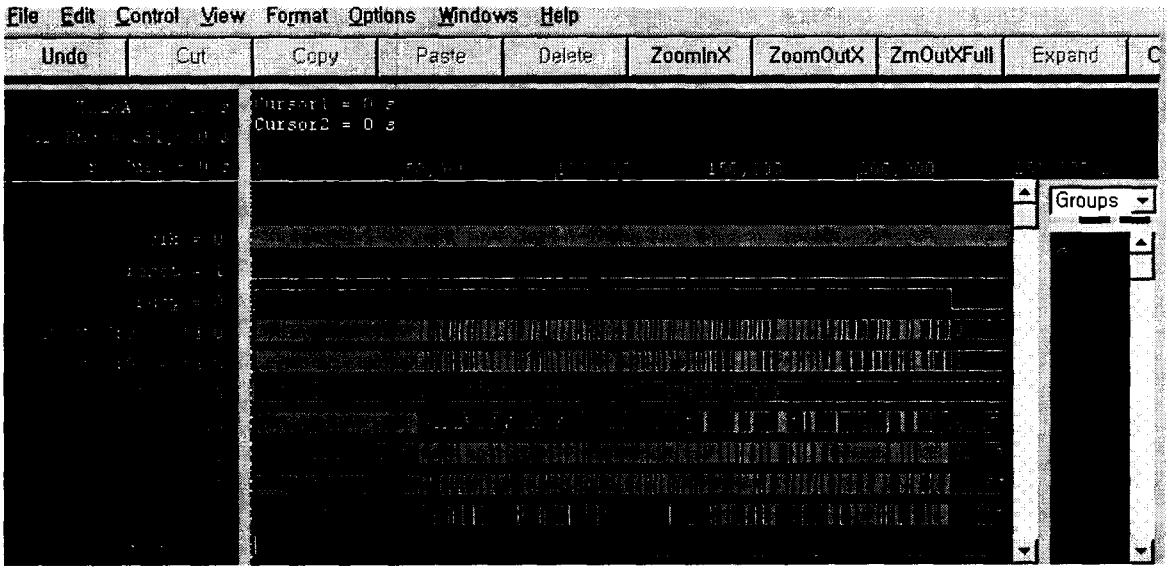

그림 7. 설계된 회로의 시뮬레이션 파형