[4-31]

$x^m + x^n + 1$ $(n \le m/2)$의 기약 다항식을 가지는 $GF(2^m)$에서의 Hybrid 곱셈기 구현

최용제, 장구영, 홍도원, 조현숙
한국전자통신연구원
choiyj@etri.re.kr

Implementation of a hybrid multiplier for $GF(2^m)$ with an irreducible trinomial $x^m + x^n + 1$ $(n \le m/2)$

YongJe Choi, KuYoung Chang, DoWon Hong, HyunSook Cho
Eletronics and Telecommunications Research Institute

요 약

$GF(2^m)$연산에 대한 효율적인 하드웨어 구현을 위해서는 면적과 성능에 대한 적절한 trade-off 가 고려되어야 한다. 본 논문은 이러한 trade-off 를 고려할 수 있는 hybrid 곱셈기에 대한 것으로, 기약 다항식이 $x^m + x^n + 1$ $(n \le m/2)$로 정의되는 $GF(2^m)$에서의 hybrid 곱셈기를 구현하였다. $k \le \lceil m/2 \rceil$을 만족하는 k에 대하여 구현된 hybrid 곱셈기는 km AND 게이트와 $km + 2k - 1$ XOR 게이트를 필요로 하며, 총 연산 시간은 $T_X + \lceil m/k \rceil (\max\{T_A, T_X\} + \lceil \log_2(k-1) \rceil) T_X$ 이다.

I. 서론

$GF(2^m)$에서의 연산은 통신 시스템이나 공개키 암호 시스템에서 널리 사용된다. 통신 시스템에서의 $GF(2^m)$연산은 정보의 신뢰성을 높이기 위해 사용되며, 신뢰성을 보장할 데이터 량에 따라서 m이 결정된다. m은 연산을 위한 하드웨어 크기와 밀접한 관계가 있으며, 통신 시스템의 경우 보통 8~32 정도의 m이 사용되며, 이를 위한 덧셈기, 곱셈기, 역승산기등의 연산기들은 비교적 쉽게 구현된다. 반면에 공개키 암호 시스템에서는 보장하는 안전성에 따라서 m이 결정되며, 타원곡선 암호 시스템의 경우 충분한 안전성을 보장하기 위해서 160 이상의 m 을 사용하도록 권고하고 있다. 이와 같이 큰 m 에 대해서는 연산을 위한 하드웨어의 성능뿐 아니라 면적도 동시에 고려되어야 한다. 특히 공개키 암호 시스템 연산의 주요한 부분을 차지하는 곱셈기의 경우 구현 방법에 따라 성능과 면적의 차이가 크게 나며, 이에 따라 전체 시스템의 성능도 큰 차이를 보이게 된다.

$GF(2^m)$에서의 곱셈기는 bit-serial 방법[1, 4]과 bit-parallel 방법[2, 3, 5] 등에 의해 설계할 수 있다. Bit-serial 방법은 작은 하드웨어로 구현할 수 있는 이점이 있지만, m 번 이상을 반복 수행하여야 하므로 연산 시간이 커져 시스템 성능을 저하시킬 수 있다. 반면 bit-parallel 방법은 빠른 성능을 기대할 수 있지만, m이 커짐에 따라 하드웨어 면적은 제곱배로 커져 m 값이 큰 시스템의 경우 구현에 어려움이 있다. 실제로 [2]의 경우 120 비트 안전성을 유지하기 위한 233 비트 곱셈기를 구현하기 위해서는 54,288 개의 XOR 게이트와 54,289 개의 AND 게이트가 필요하며, 이는 일반적인 상용 FPGA 에서 구현하기에는 어려움이 있다.

이에 본 논문에서는 기약 다항식이 $x^m + x^n + 1$ $(n \le m/2)$ 로 정의되는 $GF(2^m)$에서 면적과 성능에 대한 trade-off 를 할 수 있는 hybrid 곱셈기를 제안하였다. 조건 $n \le m/2$은 SEC, WTLS, ISO, NIST, FIPS 등의 표준에서 추천하는 기약 다항식의 형태로서 본 논문의 결과는 이들 표준 문서의 타원곡선 암호 시스템 구현에 유용하게 사용될 수 있다.

II. $GF(2^m)$에서의 부분곱 연산

Sunar 와 Koc[2]은 Mastrovito 곱셈기[1]를 이용하여 3 항 기약 다항식(irreducible trinomial)에 의해 정의된 $GF(2^m)$에서의 bit-parallel 곱셈기를 제안하였다. 본 논문에서는 이러한 곱셈기를 면적과 성능에 따라 달리 구현할 수 있도록 하는 hybrid 형태의 곱셈기를 제안하고 이를 구현하고자 한다.

$f(x) = x^m + x^n + 1$ $(1 \le n \le m/2)$ 을 $GF(2^m)$ 에서의 기약 다항식이라고 하자. 그러면, $GF(2^m)$의 임의의 원소 $a(x)$는 $\sum_{i=0}^{m-1} a_i x^i$, $a_i \in GF(2)$ 로 표현할 수 있다. $a(x) = \sum_{i=0}^{m-1} a_i x^i$ 라 하고, $b(x) = \sum_{i=0}^{k-1} b_i x^i$ 라 하자. m 비트 $a(x)$와 임의의 k 비트 $b(x)$에 대한 부분곱 연산을 고려하자.