카라추바 알고리즘

https://youtu.be/bbNtp6zN2Sc

장경배

한성대학교
HANSUNG UNIVERSITY

CryptoCraft LAB
https://crypto.modoo.at

Paper

Quantum Inf Process (2015) 14:2373–2386
DOI 10.1007/s11128-015-0993-1

CrossMark

Quantum circuits for $\mathbb{F}_{2^n}$-multiplication with subquadratic gate count

Shane Kepley[1] · **Rainer Steinwandt**[1]

Received: 10 December 2014 / Accepted: 8 April 2015 / Published online: 12 May 2015

Abstract One of the most cost-critical operations when applying Shor's algorithm to binary elliptic curves is the underlying field arithmetic. Here, we consider binary fields $\mathbb{F}_{2^n}$ in polynomial basis representation, targeting especially field sizes as used in elliptic curve cryptography. Building on Karatsuba's algorithm, our software implementation automatically synthesizes a multiplication circuit with the number of T-gates being bounded by $7 \cdot n^{\log_2(3)}$ for any given reduction polynomial of degree $n = 2^N$. If an irreducible trinomial of degree n exists, then a multiplication circuit with a total gate count of $\mathcal{O}(n^{\log_2(3)})$ is available.

Karatsuba’s multiplication algorithm

- 큰 수에 대한 효과적인 곱셈 알고리즘
- 1960년 수학 문제들에 대한 계산 복잡도 이론 세미나가 열린 적이 있는데,
  그 후 1주 만에 23살 학생 카라추바가 이 알고리즘을 발견

Karatsuba's multiplication algorithm

- **기본 단계**

x 와 y 는 B진법의 n 자리수, n 보다 작은 양수 m 에 대하여 다음과 같이 x, y 를 쪼갤 수 있음

$$x = x_1 B^m + x_0$$
$$y = y_1 B^m + y_0$$

ex) 12 34 = 12 × 10^2 + 34

56 78 = 56 × 10^2 + 78

$$z_2 = x_1 y_1$$
$$z_1 = x_1 y_0 + x_0 y_1$$
$$z_0 = x_0 y_0$$

라고 할 때, x 와 y의 곱은 $xy = (x_1 B^m + x_0)(y_1 B^m + y_0)$

$$= z_2 B^{2m} + z_1 B^m + z_0$$

이 방법은 4번의 곱셈이 필요

Karatsuba's multiplication algorithm

기존방법

$$z_2 = x_1y_1$$

$$z_1 = x_1y_0 + x_0y_1$$

$$z_0 = x_0y_0$$

카라추바

$$z_2 = x_1y_1$$

$$z_0 = x_0y_0$$

$$z_1 = (x_1y_1 + x_1y_0 + x_0y_1 + x_0y_0) - x_1y_1 - x_0y_0 = x_1y_0 + x_0y_1$$

이므로

$$z_1 = (x_1 + x_0)(y_1 + y_0) - z_2 - z_0$$

덧셈을 몇 번 함으로써 3번의 곱셈만으로 xy 를 구할 수 있음

$$\boxed{\begin{aligned} xy &= (x_1B^m + x_0)(y_1B^m + y_0) \\ &= z_2 B^{2m} + z_1 B^m + z_0 \end{aligned}}$$

Example 1

Problem. 1234 x 5678

$$z_2 = x_1 y_1$$
$$z_0 = x_0 y_0$$
$$z_1 = (x_1 + x_0)(y_1 + y_0) - z_2 - z_0$$
$$xy = (x_1 B^m + x_0)(y_1 B^m + y_0)$$
$$= z_2\, B^{2m} + z_1\, B^m + z_0$$

$$12\ 34 = 12 \times 10^2 + 34$$
$$56\ 78 = 56 \times 10^2 + 78$$
$$z_2 = 12 \times 56 = 672$$
$$z_0 = 34 \times 78 = 2652$$
$$z_1 = (12 + 34)(56 + 78) - z_2 - z_0 = 46 \times 134 - 672 - 2652 = 2840$$

마지막으로 $z_2 \times 10^{2\times 2} + z_1 \times 10^2 + z_0 = 672 \times 10000 + 2840 \times 100 + 2652 = \mathbf{7006652}$

Example 2 (Binary)

$1010 = 10 \times 2^2 + 10$

$1111 = 11 \times 2^2 + 11$

$z_2 = 10 \times 11 = 110$

$z_0 = 10 \times 11 = 110$

$z_1 = (10 + 10)(11 + 11) - 110 - 110 = 1100$

$\therefore 110 \times 2^4 + 1100 \times 2^2 + 110 = 1001 0110$

$$
\begin{array}{r}
1100000 \\
110000 \\
110 \\
\hline
10010110
\end{array}
$$

$$z_2 = x_1 y_1$$

$$z_0 = x_0 y_0$$

$$z_1 = (x_1 + x_0)(y_1 + y_0) - z_2 - z_0$$

$$xy = (x_1 B^m + x_0)(y_1 B^m + y_0)$$

$$= z_2 B^{2m} + z_1 B^m + z_0$$

$$
\begin{array}{r}
1010 \\
\times\ 1111 \\
\hline
1010 \\
1010 \\
1010 \\
1010 \\
\hline
10010110
\end{array}
$$

Karatsuba’s multiplication algorithm

효율성 분석

- 카라추바 알고리즘 기본단계는 모든 *B*와 *m*에 대해 작동하지만, *m*이 *n*/2일 때 가장 효율적이다.

- 작은 *n*에 대하여는 추가적인 덧셈과 시프트 연산 때문에 고전적인 곱셈법보다 속도가 느려진다.
  그 경계는 컴퓨터의 플랫폼에 따라 달라진다.
  대략적으로 곱하는 수가 $2^{320} \approx 2 \times 10^{96}$ 이상일 때 카라추바 알고리즘이 더 빠르다.

Multiplication

2.1 Multiplying binary polynomials with Karatsuba's algorithm

In Sect. 3.3 we will discuss how to handle extension degrees that are not a power of 2, but for now assume that $n = 2^N$. Let

$$X = \sum_{k=0}^{n-1} x_k t^k, \quad Y = \sum_{k=0}^{n-1} y_k t^k, \quad Z = \sum_{k=0}^{2n-2} z_k t^k \in \mathbb{F}_2[t]$$

$1010 = 10 \times 2^2 + 10$

$1111 = 11 \times 2^2 + 11$

$X \cdot Y = Z$ 를 연산하기 위해

곱셈의 대상 다항식인 X 와 Y 를 나눈다.

$$X = X[2]t^{n/2} + X[0], \quad Y = Y[2]t^{n/2} + Y[0],$$

Multiplication

$$C[2]=X[2]\cdot Y[2],\quad C[0]=X[0]\cdot Y[0],\quad C[1]=\underbrace{(X[0]+X[2])}_{=X[1]}\cdot\underbrace{(Y[0]+Y[2])}_{=Y[1]},$$

X · Y 는 다음과 같이 완료됨

$$\left(X[2]t^{\frac{n}{2}}+X[0]\right)\cdot\left(Y[2]t^{\frac{n}{2}}+Y[0]\right)=C[2]t^{n}+(C[1]+C[2]+C[0])\,t^{\frac{n}{2}}+C[0].$$

$$z_2 = x_1 y_1$$

$$z_0 = x_0 y_0$$

$$z_1 = (x_1 + x_0)(y_1 + y_0) - z_2 - z_0$$

$$\begin{aligned} xy &= (x_1 B^m + x_0)(y_1 B^m + y_0) \\ &= z_2\, B^{2m} + z_1\, B^m + z_0 \end{aligned}$$

Multiplication circuit

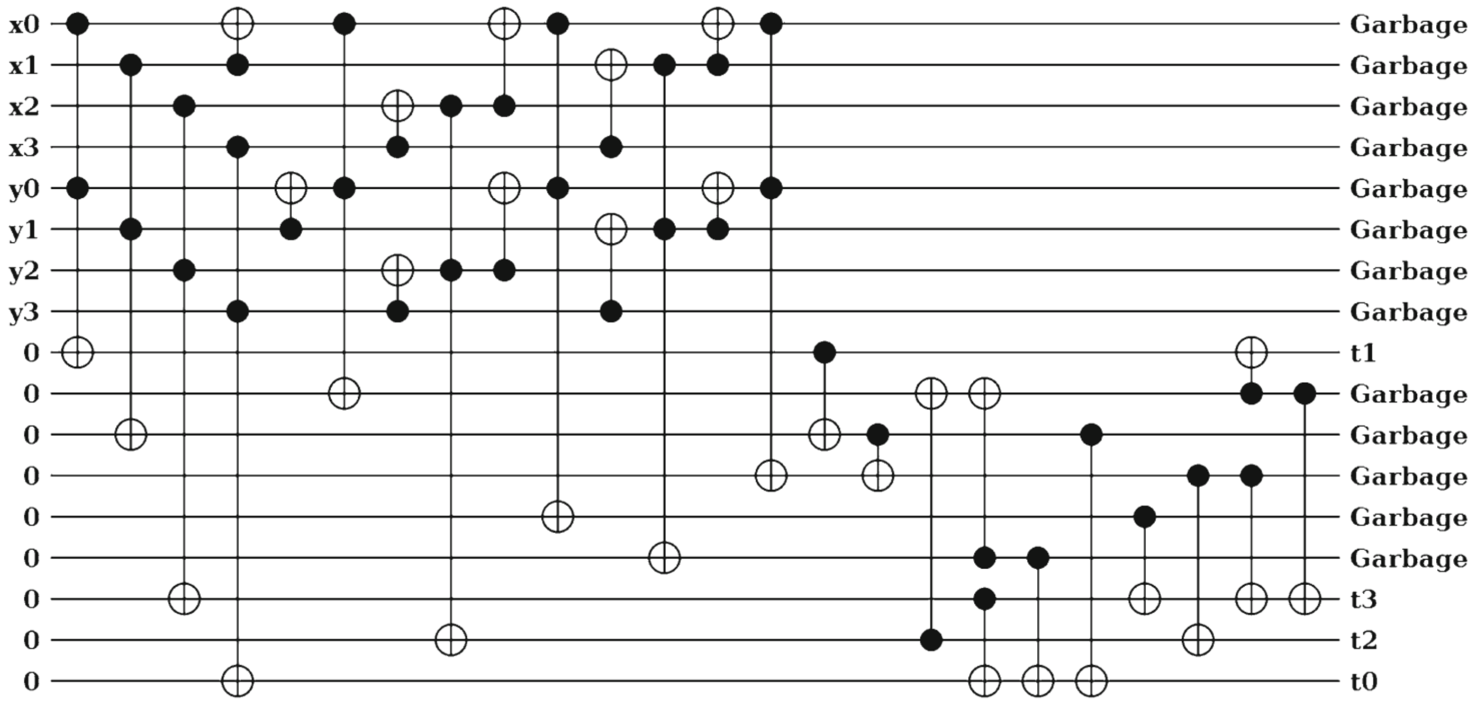

Fig. 2 Multiplication circuit for $\mathbb{F}_{16} = \mathbb{F}_2[t]/(t^4 + t + 1)$. The coefficients of the inputs X and Y are provided on the wires labeled x0,…,x3 and y0,…,y3, respectively. The coefficients of the product $X \cdot Y$ in $\mathbb{F}_{16}$ are available on the wires labeled t0,…,t3

감사합니다