Low Complexity Cubing and Cube Root Computation over $\mathbb{F}_{3^m}$ in Standard Basis

Omran Ahmadi[1] and Francisco Rodríguez-Henríquez[2]

[1] Claude Shannon Institute, School of Mathematical Sciences

University College Dublin, Ireland

omran.ahmadi@ucd.ie

[2] Computer Science Department

Centro de Investigación y de Estudios Avanzados del IPN, México

francisco@cs.cinvestav.mx

Abstract

We present low complexity formulae for the computation of cubing and cube root over $\mathbb{F}_{3^m}$ constructed using special classes of trinomials, tetranomials and pentanomials. We show that for all those special classes of polynomials, cube root operation has the same area and time complexity as field cubing when implemented in hardware or software platforms.

keyword: Finite field arithmetic; cubing; cube root; cryptography

I. Introduction

Arithmetic over ternary extension fields $\mathbb{F}_{3^m}$ has gained an increasing importance in several relevant cryptographic applications, particularly in (hyper) elliptic curve cryptography. It has been shown that supersingular elliptic curves over $\mathbb{F}_{3^m}$ are excellent choices for the implementation of pairing-based cryptographic protocols [1]. Furthermore, some of the fastest algorithms known for pairing computations on these supersingular elliptic curves [2]–[5], require the efficient computation of the basic arithmetic finite field operations such as field addition, subtraction, multiplication, division, and exponentiation, cubing and cube root computation. In particular, cube root computation has become an important building block in the design of bilinear pairings [3]–[5].

The efficiency of finite field arithmetic implemented in hardware can be measured in terms of associated design space and time complexities. The space complexity is defined as the total amount of hardware resources needed to implement the circuit, i.e. the total number of logic gates required by the design. Time complexity, on the other hand, is simply defined as the total gate delay or critical path of the circuit, frequently formulated using gate delay units.

Let $P(x)$ be an irreducible polynomial of degree m over $\mathbb{F}_3$. Then, the ternary extension field $\mathbb{F}_{3^m}$ can be defined as,

$$\mathbb{F}_{3^m} \cong \mathbb{F}_3[x]/\left(P(x)\right).$$

The field cubing and cube root operation can be defined as follows. Let A be an arbitrary element in the field $\mathbb{F}_{3^m}$ as described above. Then, the field cubing of A, denoted as A^3, is the element $C \in \mathbb{F}_{3^m}$ such that $C = A^3$, holds. Similarly, the field cube root of A, denoted as $A^{\frac{1}{3}}$, or simply, $\sqrt[3]{A}$, is the element $D \in \mathbb{F}_{3^m}$ such that $D^3 = A$.

In 2004, Barreto in [6] published an extension of a method previously used for square root computations in binary fields to compute cube roots in ternary fields. Both approaches in the cases of binary and ternary fields are especially efficient when the finite field has been generated by a special class of irreducible trinomials.

Let us consider the ternary field $\mathbb{F}_{3^m}$ generated by the irreducible polynomial $P(x)$, with an extension degree $m = 3u + r$, where $u \geq 1$ and $r \in \{0, 1, 2\}$. Let A be an arbitrary element of the field $\mathbb{F}_{3^m}$, that in canonical basis can be written as,

$$A = \sum_{i=0}^{m-1} a_i x^i = \sum_{i=0}^{u-s} a_{3i} x^{3i} + x \cdot \sum_{i=0}^{u+r-2} a_{3i+1} x^{3i} + x^2 \cdot \sum_{i=0}^{u-1} a_{3i+2} x^{3i}.$$

where $s = 1$ if $r = 0$, and $s = 0$, otherwise. Then, the field cube root $\sqrt[3]{A}$, can be computed as [6], [1]

$$\sqrt[3]{A} = \sum_{i=0}^{u-s} a_{3i} x^i + x^{1/3} \cdot \sum_{i=0}^{u+r-2} a_{3i+1} x^i + x^{2/3} \cdot \sum_{i=0}^{u-1} a_{3i+2} x^i \bmod P(x). \quad (1)$$

Using (1) one can compute a cube root by performing two third-length polynomial multiplications with the per-field constants $x^{\frac{1}{3}}$ and $x^{\frac{2}{3}}$, that can be calculated offline. In the case that the Hamming weight

[1] There is a typo in the first equation of Subsection 2.2 of [6], since the upper limit of the third summatory should not be u but $u - 1$.

of $x^{\frac{1}{3}}$ and $x^{\frac{2}{3}}$ is low, those two multiplications are simple to compute. Barreto showed in [6], that low Hamming weights for $x^{\frac{1}{3}}$ and $x^{\frac{2}{3}}$ can be obtained if one uses $P(x) = x^m + ax^k + b$, with $a, b \in \mathbb{F}_3$, and $m \equiv k \equiv r \bmod 3$, with $r \neq 0$. It is worth to stress that this is a strong restriction as those trinomials do not exist for every extension degree m.[2] We also note that if the degree of the constants $x^{\frac{1}{3}}$ and $x^{\frac{2}{3}}$ is strictly less than $2u + r - 1$, then the computation of (1) does not require a reduction process modulo $P(x)$.

In [7], Ahmadi et al. studied the Hamming weight of $x^{\frac{1}{3}}$ and $x^{\frac{2}{3}}$ in the general case of irreducible trinomials where m is not congruent with k modulo 3. Authors in [7] showed that general irreducible trinomials can lead to high Hamming weights for the constants $x^{\frac{1}{3}}$ and $x^{\frac{2}{3}}$, thus making the computation of Eq. (1) expensive and therefore, less attractive.[3] In [4], and more recently in [5], several cube root friendly irreducible pentanomials for the extension degree $m = 509$ were reported. In [5], the pentanomials $P_1(x) = x^{509} - x^{477} + x^{445} + x^{32} - 1$ and $P_2(x) = x^{509} - x^{318} - x^{191} + x^{127} + 1$, were used. Those polynomials were then successfully utilized within a software library for computing bilinear pairings efficiently. However authors in [4], [5] did not elaborate further in the search criteria used for finding cube root friendly pentanomials.

In this paper, we present a study of the computational efforts associated to field cubing and cube root calculation in ternary extension fields. We also give a result useful for classifying trinomials that happen to be irreducible over $\mathbb{F}_3$. Furthermore, we present an extended version of Barreto method, that is useful for finding cube root friendly irreducible trinomials, tetranomials and pentanomials. We give a careful complexity analysis of the field cubing computation and report a list of irreducible polynomials with prime extension degrees m in the range $m \in [47, 541]$, that lead to efficient computations of the cube root operation. Finally, we discuss how the technique of mapping to a ring can be useful for speeding-up the cube root computation in certain ternary fields.

The rest of this paper is organized as follows. In Section II, we give a short summary of the main results published in the open literature for computing field squaring and square roots. In Section III, we present a lemma that allows the classification of irreducible trinomial for odd extension degrees. We

[2]In ternary fields $\mathbb{F}_{3^m}$, there exist 381 m values less than 1000 where at least one irreducible trinomial of degree m can be found. However, irreducible trinomials of the form $P(x) = x^m + ax^k + b$, with the property, $m \equiv k \equiv r \bmod 3$, are available in just 74 values out of the total of 168 prime numbers less than 1000 (about 44% of the cases).

[3]An almost worst case is reported in [4] for $m = 163$, where there exist an irreducible trinomial that yields $x^{\frac{1}{3}}$ with a Hamming weight of 162 nonzero terms.

also give the computational cost of the field cubing operation when $P(x)$ happens to be a trinomial or a tetranomial. Then, in Section IV, we analyze the computational cost of the cube root operation when $P(x)$ is a special class of trinomial, tetranomial, pentanomial and/or equally-spaced polynomial. In Section V, we show how the ring mapping idea can be used to accelerate the cube root computation in some ternary fields. Section VI presents a list of reduction polynomials that yield low cost cubings and cube roots for supersingular elliptic curves with large r-torsion subgroups over $\mathbb{F}_{3^m}$. Finally, in Section VII some concluding remarks are drawn.

II. Previous Work on Field Squaring and Square Roots in Binary Fields

Since many techniques used in binary arithmetic can be extended to ternary arithmetic, we will recount in the rest of this section the different approaches proposed across the years for computing field squaring and square root over binary fields.

A. Squaring

Let $\mathbb{F}_{2^m}$ be a binary extension field generated by an irreducible polynomial $P(x)$, and let A be an arbitrary element of that field. Then, the element A can be written in canonical basis as, $A = \sum_0^{m-1} a_i x^i$, with $a_i \in \mathbb{F}_2$ for $i = 0, 1 \ldots, m-1$. Let us also assume that the extension degree m can be expressed as, $m = 2u + 1$, with $u \geq 1$. Then, the polynomial squaring operation can be obtained as,

$$\begin{aligned} A^2 &= \left(\sum_{i=0}^{m-1} a_i x^i\right)^2 = \sum_{i=0}^{m-1} a_i x^{2i} = \sum_{i=0}^{u} a_i x^{2i} + \sum_{i=u+1}^{2u} a_i x^{2i} \\ &= \sum_{i=0}^{u} a_i x^{2i} + x^{2u+1} \sum_{i=1}^{u} a_{u+i} x^{2i-1} = \sum_{i=0}^{u} a_i x^{2i} + x^m \sum_{i=1}^{u} a_{u+i} x^{2i-1}. \end{aligned}$$

Hence, we can compute the field squaring operation defined as $C = A^2 \bmod P(x)$ as,

$$C = A^2 \bmod P(x) = \sum_{i=0}^{u} a_i x^{2i} + x^m \sum_{i=1}^{u} a_{u+i} x^{2i-1} \bmod P(x) \tag{2}$$

It is possible to implement efficiently Eq. (2) in software by extracting the two half-length vectors $A^L = (a_u, a_{u-1}, \cdots, a_1, a_0)$ and $A^H = (a_{2u}, a_{2u-1}, \cdots, a_{u+2}, a_{u+1})$, followed by one field multiplication of length $m/2$ bits by the per-field constant x^m. In the case that the irreducible polynomial $P(x)$

is a trinomial of the form, $P(x) = x^m + x^k + 1$, then $x^m = x^k + 1$ has a Hamming weight of 2. We stress that the reduction process modulo P(x) stipulated in Eq. (2), must be always carried out. [4]

B. Square Root

One straightforward method for computing p-th roots in prime extension fields is based on Fermat's Little Theorem which establishes that for any element $A \in \mathbb{F}_{p^m}$, the identity $A^{p^m} = A$ holds. Therefore, $\sqrt[p]{A}$ may be computed as $D = A^{p^{m-1}}$ with a computational cost of $m-1$ field exponentiations to the power p. [5]

A potentially much more efficient approach for computing square roots over binary extension fields, was presented by Fong et al. in [9] based on the following observation. Let A be an arbitrary element in $\mathbb{F}_{2^m}$ represented in the polynomial basis as $A = \sum_0^{m-1} a_i x^i, i = 0, 1 \ldots, m-1$. Then, $\sqrt{A}$ can be expressed in terms of the square root of x as,

$$A^{\frac{1}{2}} = \sum_{i=0}^{\lfloor \frac{m-1}{2} \rfloor} a_{2i} x^i + x^{\frac{1}{2}} \sum_{i=0}^{\lfloor \frac{m-3}{2} \rfloor} a_{2i+1} x^i \bmod P(x). \tag{3}$$

It is possible to implement efficiently Eq. (3) in software by extracting the two half-length vectors $A_{even} = (a_{m-1}, a_{m-3}, \cdots, a_2, a_0)$ and $A_{odd} = (a_{m-2}, a_{m-4}, \cdots, a_3, a_1)$, followed by one field multiplication of length $m/2$ bits by the pre-computed constant $x^{\frac{1}{2}}$. However, in the case that the irreducible polynomial $P(x)$ is a trinomial, $P(x) = x^m + x^n + 1$ with m an odd prime number, then the square root of an arbitrary element $A \in \mathbb{F}_{2^m}$ can be obtained at a very low price: the computation of some few additions and shift operations [9].[6] Furthermore, Rodríguez-Henríquez et al. showed in [10] that for all practical cases, the cost of computing in hardware the square root over binary fields generated with irreducible trinomials, is not more expensive than the computational effort required for computing field squarings.

Based on the technique used for trinomials, Avanzi in [11], [12] published a method that can find irreducible polynomials, other than trinomials, that lead to low-weight constants $x^{\frac{1}{2}}$. His method can be

[4]The only exception would be if $P(x)$ is an irreducible trinomial of the form, $P(x) = x^m + x + 1$.

[5]This is the method suggested in [8], for computing square roots over binary extension fields.

[6]It is noticed that there exist 545 values of m less than 1000 for which at least one irreducible trinomial of degree m over $\mathbb{F}_2$ can be found. Restricting ourselves to extension degrees where m is a prime number, from the total of 168 prime numbers less than 1000, irreducible trinomials can be found for just 82 values (nearly in 48% of the cases).

summarized as follows. Let us assume that there exists an m-degree polynomial, irreducible over $\mathbb{F}_2$, that can be written as $P(x) = x \cdot U(x)^2 + 1$, where $U(x)$ is an $\frac{m-1}{2}$-degree polynomial of even weight. Then, it follows that the per-field constant $x^{\frac{1}{2}}$ will be given by, $x^{\frac{1}{2}} = xU(x)$.

Using the above approach to guide his search of irreducible polynomials, Avanzi was able to find a rich family of square root friendly irreducible pentanomials and heptanomials that produce constants $x^{\frac{1}{2}}$ with low Hamming weight. By virtue of Eq. (3), this implies that one can calculate the field square root operation with a computational effort comparable to that required by irreducible trinomials. Avanzi's square root friendly polynomials became a good option for binary extension fields with degree extensions m where no irreducible trinomial can be found.

Other pentanomials that lead to fast computation of the square root over $\mathbb{F}_{2^m}$, were published independently by Ahmadi et al. in [13], where two square root friendly irreducible pentanomials for the extension degrees $m = 163, 283$, and one irreducible trinomial for $m = 233$, were used with advantage for speeding-up the computation of the scalar multiplication on Koblitz curves. Furthermore, in [14], Scott proposed to use irreducible pentanomials that can assure both, fast modular reductions and square root computations in software implementations. To this end, he suggested to work with m-degree irreducible pentanomials of the form $P(x) = x^m + x^{k_1} + x^{k_2} + x^{k_3} + 1$, such that $m - k_1 \equiv m - k_2 \equiv m - k_3 \equiv 0 \bmod w$, where w is the word length of the target processor and m is a prime number. These irreducible pentanomials not always can be found for a given extension degree m. However, less efficient alternatives were also suggested in [14]. Finally Panairo and Thompson studied in [15] the computation of p-th roots in finite fields of odd characteristic p, with $p \geq 5$, where irreducible binomials can be found.

III. Field Cubing Computation

Let us consider the ternary field $\mathbb{F}_{3^m}$ generated by the irreducible polynomial $P(x)$, and let A be an arbitrary element of that field. Then, the element A can be written in canonical basis as, $A = \sum_{i=0}^{m-1} a_i x^i$, $a_i \in \mathbb{F}_3$, where the extension degree m can be written as, $m = 3u + r$, with $u \geq 1$ and $r \in \{0, 1, 2\}$.

Then, the polynomial cubing A^3, can be computed as,

$$\begin{aligned} A^3 &= \left(\sum_{i=0}^{m-1} a_i x^i\right)^3 = \sum_{i=0}^{m-1} a_i x^{3i} \\ &= \sum_{i=0}^{u} a_i x^{3i} + \sum_{i=u+1}^{2u+r-1} a_i x^{3i} + \sum_{i=2u+r}^{3u+r-1} a_i x^{3i} \\ &= C_0 + x^{3u+r} C_1 + x^{6u+2r} C_2. \end{aligned}$$

where,

$$C_0 = \sum_{i=0}^{u} a_i x^{3i}, \quad C_1 = \sum_{i=1}^{u+r-1} a_{i+u} x^{3i-r}, \quad C_2 = \sum_{i=r}^{u+r-1} a_{i+2u} x^{3i-2r}. \tag{4}$$

We can compute the field cubing operation defined as $C = A^3 \bmod P(x)$ by performing,

$$\begin{aligned} C = A^3 \bmod P(x) &= C_0 + x^{3u+r} C_1 + x^{6u+2r} C_2 \bmod P(x) \\ &= C_0 + x^m C_1 + x^{2m} C_2 \bmod P(x). \end{aligned} \tag{5}$$

Eq. (5) states that the cubing operation can be computed by determining the constants x^m and x^{2m}, which are per-field constants, and therefore they can be pre-computed offline. In the rest of this Section we will study several classes of trinomials and tetranomials, and we will give closed formulae for the field cubing operation.

A. Irreducible Trinomials

1) Classification of Ternary Trinomials: Let us consider ternary extension fields constructed using irreducible trinomials of the form $P(x) = x^m + ax^k + b$, with $m \geq 2$ and $a, b \in \mathbb{F}_3$. Then, the following results are useful.

Theorem III.1. *Let $m > 2$ be an odd number. Then, if k is odd we have that, $P_1(x) = x^m + x^k - 1$ is always reducible over $\mathbb{F}_3$ and $P_3(x) = x^m - x^k + 1$ is irreducible if and only if $P_2(x) = x^m - x^k - 1$ is irreducible over $\mathbb{F}_3$.*
If k is even, then $P_2(x) = x^m - x^k - 1$ is always reducible over $\mathbb{F}_3$ and $P_3(x)$ is irreducible if and only if $P_1(x) = x^m + x^k - 1$ is irreducible.

Proof: If m and k are odd numbers, then $P_1(-1) = 0$ and hence $P_1(x)$ is reducible over $\mathbb{F}_3$. On

the other hand $P_3(x)$ is irreducible over $\mathbb{F}_3$ if and only if $P_3(-x)$ is irreducible and hence if and only if $-P_3(-x) = P_2(x) = x^m - x^k - 1$ is irreducible. If k is an even number, then $P_2(-1) = 0$ and thus $P_2(x)$ is reducible over $\mathbb{F}_3$. The rest of the proof is similar to the previous case.

Hence, we will study in the rest of this subsection, without loss of generality, irreducible trinomials of the form, $P(x) = x^m - x^k + 1$.

2) Irreducible Trinomials $P(x) = x^m - x^k + 1$, with $m \equiv k \equiv r \mod 3$: Let us consider the ternary field $\mathbb{F}_{3^m}$ generated by the trinomial $P(x) = x^m - x^k + 1$, irreducible over $\mathbb{F}_3$, where the extension degree m can be expressed as, $m = 3u + r$, $1 \leq u$ and $k = 3v + r$, $0 \leq v$, with $m \equiv k \equiv r \bmod 3$, $r \neq 0$ and $u - 2v \geq 1$. Then, we can write $x^m = x^k - 1$ and $x^{2m} = \left(x^k - 1\right)^2 = x^{2k} + x^k + 1$. Using Eq. (5), we can compute the field cubing as,

$$C^3 = C_0 + x^m C_1 + x^{2m} C_2 = C_0 - C_1 + C_2 + x^k(C_1 + C_2) + x^{2k} C_2 \bmod P(x).$$

In order to further expand the above result, it becomes useful to define $C_1^L, C_1^H, C_2^L, C_2^H$ as,

$$\begin{aligned} C_1 &= \sum_{i=1}^{u+r-1} a_{i+u} x^{3i-r} = \sum_{i=1}^{u-v} a_{i+u} x^{3i-r} + x^{3(u-v)} \sum_{i=1}^{v+r-1} a_{i+2u-v} x^{3i-r} \\ &= C_1^L + x^{3(u-v)} C_1^H. \end{aligned}$$

$$\begin{aligned} C_2 &= \sum_{i=r}^{u+r-1} a_{i+2u} x^{3i-2r} = \sum_{i=r}^{u-v+r-1} a_{i+2u} x^{3i-2r} + x^{3(u-v)} \sum_{i=r}^{v+r-1} a_{i+3u-v} x^{3i-2r} \\ &= C_2^L + x^{3(u-v)} C_2^H. \end{aligned}$$

We also define C_2^{LL}, C_2^{HH} as follows,

$$\begin{aligned} C_2 &= \sum_{i=r}^{u+r-1} a_{i+2u} x^{3i-2r} = \sum_{i=r}^{u-2v} a_{i+2u} x^{3i-2r} + x^{3(u-2v)-r} \sum_{i=1}^{2v+r-1} a_{i+3u-2v} x^{3i-r} \\ &= C_2^{LL} + x^{3(u-2v)-r} C_2^{HH}. \end{aligned}$$

Notice that $3(u-v) = m-k$, $3(u-2v)-r = m-2k$. Thus, we have

$$\begin{aligned} C^3 &= C_0 - C_1 + C_2 + x^k(C_1 + C_2) + x^{2k}C_2 \bmod P(x) \qquad (6)\\ &= C_0 - C_1 + C_2 + x^k(C_1^L + x^{m-k}C_1^H + C_2^L + x^{m-k}C_2^H) + x^{2k}(C_2^{LL} + x^{m-2k}C_2^{HH}) \\ &= C_0 - C_1 + C_2 - (C_1^H + C_2^H + C_2^{HH}) + x^k(C_1^L + C_1^H + C_2^L + C_2^H + C_2^{HH}) + x^{2k}C_2^{LL}. \end{aligned}$$

3) An Example: Let $\mathbb{F}_{3^{13}}$ be a field generated with the irreducible trinomial, $P(x) = x^{13} - x^4 + 1$, with $m = 3u+1 = 3\cdot 4+1 = 13$, $r = 1$ and $k = 3v+1 = 3\cdot 1+1 = 4$. Let $A = \sum_{i=0}^{12} a_i x^i$ be an arbitrary element of that field. Then according with the definitions given above, we have:

$$\begin{aligned} C_0 &= \textstyle\sum_{i=0}^{4} a_i x^{3i} &&= a_0 + a_1x^3 + a_2x^6 + a_3x^9 + a_4x^{12} \\ C_1 &= \textstyle\sum_{i=1}^{4} a_{4+i} x^{3i-1} &&= a_5x^2 + a_6x^5 + a_7x^8 + a_8x^{11} \\ C_2 &= \textstyle\sum_{i=1}^{4} a_{8+i} x^{3i-2} &&= a_9x + a_{10}x^4 + a_{11}x^7 + a_{12}x^{10} \end{aligned}$$

and,

$$\begin{aligned} C_1^L &= \sum_{i=1}^{u-v} a_{i+u}x^{3i-r} = \sum_{i=1}^{3} a_{4+i}x^{3i-1} = a_5x^2 + a_6x^5 + a_7x^8. \\ C_1^H &= \sum_{i=1}^{v+r-1} a_{i+2u-v}x^{3i-r} = \sum_{i=1}^{1} a_{7+i}x^{3i-1} = a_8x^2. \\ C_2^L &= \sum_{i=r}^{u-v+r-1} a_{i+2u}x^{3i-2r} = \sum_{i=1}^{3} a_{8+i}x^{3i-2} = a_9x + a_{10}x^4 + a_{11}x^7. \\ C_2^H &= \sum_{i=r}^{v+r-1} a_{i+3u-v}x^{3i-2r} = \sum_{i=1}^{1} a_{11+i}x^{3i-2} = a_{12}x; \\ C_2^{LL} &= \sum_{i=r}^{u-2v} a_{i+2u}x^{3i-2r} = \sum_{i=1}^{2} a_{8+i}x^{3i-2} = a_9x + a_{10}x^4; \\ C_2^{HH} &= \sum_{i=1}^{2v+r-1} a_{i+3u-2v}x^{3i-r} = \sum_{i=1}^{2} a_{10+i}x^{3i-2} = a_{11}x^2 + a_{12}x^5; \end{aligned}$$

Thus,

$$\begin{aligned} C = A^3 &= C_0 - C_1 + C_2 - (C_1^H + C_2^H + C_2^{HH}) + x^k(C_1^L + C_1^H + C_2^L + C_2^H + C_2^{HH}) + x^{2k}C_2^{LL} \\ &= a_0 + (a_9 - a_{12})x + (-a_5 - a_8 - a_{11})x^2 + a_1x^3 + a_{10}x^4 + \\ &\quad +(-a_6 + a_9)x^5 + (a_2 + a_5 + a_8 + a_{11})x^6 + a_{11}x^7 + (-a_7 + a_{10})x^8 + \\ &\quad +(a_3 + a_6 + a_9 + a_{12})x^9 + a_{12}x^{10} + (-a_8 + a_{11})x^{11} + (a_4 + a_7 + a_{10})x^{12} \end{aligned}$$

4) Complexity Analysis: In the following we will assume that the field addition and field subtraction operations can be computed at the same cost in the base field $\mathbb{F}_3$.

The area complexity cost of the field cubing operation can be directly deduced from (6), along with the definitions of $C_1^L, C_1^H, C_2^L, C_2^H, C_2^{LL}$ and C_2^{HH}, as described next.

We first notice from (4) that each one of the m coefficients of the words C_0, C_1 and C_2 are associated with different powers x^i, for $i = 0, \ldots, m-1$. Hence, the term $C_0 - C_1 + C_2$ of (6) is free of overlaps, and consequently, it can be implemented without cost in hardware, i.e., with no addition/subtraction operations. Furthermore, it can be noticed that the words C_1^L, C_2^L, C_2^{LL} and C_1^H, C_2^H, C_2^{HH} appear in (6) once and twice, respectively.

Therefore, the total number of $\mathbb{F}_3$ field adder/subtracter required for computing (6) is upper bounded by, [7]

$$\begin{aligned} \text{\# of adder blocks} &\leq |C_1^L| + |C_2^L| + |C_2^{LL}| + 2\left[|C_1^H| + |C_2^H| + |C_2^{HH}|\right] \\ &= (u - v) + (u - v) + (u - 2v - r + 1) + \\ &\quad +2\left[(v + r - 1) + v + (2v + r - 1)\right] \\ &= 3u + 4v + 3r - 3 = m + \frac{2}{3}(2k + r) - 3. \end{aligned}$$

Table I shows prime extension degrees $m \in [47, 541]$, for which there exist preferred irreducible trinomials. In that table we have selected the irreducible trinomials of the form $P(x) = x^m - x^k + 1$, with the smallest possible middle term degree k. In the interval $[47, 541]$ there are a total of 86 prime numbers, but only for 42 of them, a preferred irreducible trinomial can be found.

[7] In the following, the operator $|\cdot|$ represents the length in trits of the term being computed.

B. *Irreducible Tetranomials* $P(x) = x^m + ax^{k_1} + bx^{k_2} + c$, *with* $m \equiv k_1 \equiv k_2 \equiv r \bmod 3$

Besides trinomials, the next simple option in $\mathbb{F}_3$ would be to try to find irreducible tetranomials of the form, $P(x) = x^m + ax^{k_1} + bx^{k_2} + c$, with $a, b, c \in \mathbb{F}_3$. Table II shows some extensions where there exist no irreducible trinomials and thus, the only option is to work with irreducible tetranomials or pentanomials.

Let us write the extension degree m as, $m = 3u + r$, $u \geq 1$ and $k_1 = 3v + r$, $k_2 = 3w + r$, with $0 \leq w < v < u$, with $m \equiv k_1 \equiv k_2 \equiv r \bmod 3$, $r \neq 0$ and $u - 2v \geq 1$.

For this class of irreducible tetranomials, we have,

$$\begin{aligned} x^m &= -ax^{k_1} - bx^{k_2} - c; \\ x^{2m} &= \left(-ax^{k_1} - bx^{k_2} - c\right)^2 = x^{2k_1} - acx^{k_1} + 1 + x^{2k_2} - abx^{(k_1+k_2)} - cbx^{k_2} \end{aligned}$$

Once again, we can use Eq. (5) for computing the field cubing operation.

which implies,

$$\begin{aligned} C^3 &= C_0 + x^m C_1 + x^{2m} C_2 \\ &= C_0 - cC_1 + C_2 - ax^{k_1}(C_1 + cC_2) - bx^{k_2}(C_1 + cC_2) + \\ &\quad + x^{2k_1} C_2 + x^{2k_2} C_2 - abx^{k_1+k_2} C_2 \bmod P(x). \end{aligned}$$

TABLE I

CANDIDATE REDUCTION TRINOMIALS FOR $\mathbb{F}_{3^m}$, $P(x) = x^m - x^n + 1$ OF DEGREE $m \in [47, 541]$ ENCODED AS $m(n)$, WITH m A PRIME NUMBER

$m(n)$	$m(n)$	$m(n)$	$m(n)$
47(32)	167(71)	277(97)	431(365)
59(17)	179(59)	313(187)	433(262)
61(7)	181(37)	337(25)	443(188)
71(20)	191(71)	347(65)	457(67)
73(1)	193(64)	349(223)	467(92)
83(32)	227(11)	359(122)	479(221)
97(16)	229(79)	373(25)	491(11)
107(11)	239(5)	383(80)	503(35)
109(13)	241(88)	409(136)	541(145)
131(47)	251(26)	419(26)	
157(22)	263(104))	421(13)	

Using the same approach utilized in Subsection III-A.4, the computational complexity of the above formula can be estimated as,

$$\begin{aligned}\#\text{ of adders} \;\leq\;& (u-v)+(u-v)+(u-2v-r+1)+3\left[(v+r-1)+v+(2v+r-1)\right]+\\ &+(u-w)+(u-w)+(u-2w-r+1)+3\left[(w+r-1)+w+(2w+r-1)\right]+\\ &+(u-v-w-r+1)+3\left[v+w+r-1\right]\\ =\;& 7u+10v+10w+12r-12=2m+3(k_1+k_2)+u+v+w+4r-12.\end{aligned}$$

IV. Formulae for Cube Root Computation

A. Irreducible Trinomials $P(x) = x^m - x^k + 1$, with $m \equiv k \equiv r \mod 3$

Let us consider the ternary field $\mathbb{F}_{3^m}$ generated by the trinomial $P(x) = x^m - x^k + 1$, irreducible over $\mathbb{F}_3$, where the extension degree m can be expressed as, $m = 3u + r$, $u \geq 1$ and $k = 3v + r$, $0 \leq v < u$, with $m \equiv k \equiv r \bmod 3$ and $r \in [1, 2]$. In [6] it was found that for $r = 1$ we have,

$$x^{2/3} = -x^{u+1} + x^{v+1}; \quad x^{1/3} = x^{2u+1} + x^{u+v+1} + x^{2v+1}.$$

whereas for $r = 2$ we have,

$$x^{1/3} = -x^{u+1} + x^{v+1}; \quad x^{2/3} = x^{2u+2} + x^{u+v+2} + x^{2v+2}.$$

From above results, it follows that when dealing with irreducible trinomials of this kind, we do not need to perform the reduction modulo P(x) indicated in Eq.(1).

In the following we will apply Barreto's trick to the case of irreducible tetranomials.

B. Tetranomials

Let $\mathbb{F}(3^m)$ be a ternary field generated by the tetranomial $P(x) = x^m + ax^{k_1} + bx^{k_2} + c$ irreducible over $\mathbb{F}_3$, where the extension degree m can be expressed as, $m = 3u + r$, $u \geq 1$ and $k_1 = 3v + r$, $k_2 = 3w + r$, with $0 \leq w < v < u$, and $m \equiv k_1 \equiv k_2 \equiv r \bmod 3$, $r \neq 0$. Once again, using (1) one can compute a cube root by finding the per-field constants $x^{1/3}$ and $x^{2/3}$.

1) case $r = 1$: For $r = 1$, we observe that $-c = x^m + ax^{k_1} + bx^{k_2}$, which implies,

$$-cx^2 = x^2(x^m + ax^{k_1} + bx^{k_2}) = x^{3(u+1)} + ax^{3(v+1)} + bx^{3(w+1)}$$

TABLE II

REDUCTION POLYNOMIALS FOR $\mathbb{F}_{3^m}$, GIVING LOW COST CUBINGS AND/OR CUBE ROOTS. THE VALUE $N(M)$ IS LISTED WHERE N IS THE TOTAL NUMBER OF ADDERS/SUBTRACTERS OVER $\mathbb{F}_3$ REQUIRED AND M IS THE NUMBER OF ADDER DELAYS NEEDED FOR COMPUTING THE OPERATION. PTR=PREFERRED TRINOMIALS. PP= PREFERRED PENTANOMIALS. PT= PREFERRED TETRANOMIALS. EST= EQUALLY SPACED TETRANOMIALS

Reduction polynomial	**Type**	$\sqrt[3]{x}$	$\sqrt[3]{x^2}$	$N(M)$ c^3	$N(M)$ $\sqrt[3]{c}$
$x^{37}-x^{13}+1$	PTr	$x^{25}+x^{17}+x^9$	$-x^{13}+x^5$	44(2)	36(2)
$x^{41}+x^{24}-x^{17}+$ x^7-1	PP	$x^{39}+x^{31}+x^{23}+$ $x^{22}-x^{14}+x^5$	$-x^{20}+x^{12}+x^3$	125(3)	92(3)
$x^{43}+x^{30}+x^{17}-$ $x^{13}-1$	PP	$-x^{19}+x^9+x^6$	$x^{38}+x^{28}+x^{25}+$ $x^{18}-x^{15}+x^{12}$	126(3)	89(3)
$x^{49}+x^{13}+x^4-1$	PT	$x^{33}-x^{21}-x^{18}+$ $x^9-x^6+x^3$	$x^{17}+x^5+x^2$	131(3)	112(3)
$x^{59}-x^{17}+1$	PTr	$-x^{20}+x^6$	$x^{40}+x^{26}+x^{12}$	70(2)	58(2)
$x^{92}+x^{29}+x^5-1$	PT	$x^{31}+x^{10}+x^2$	$x^{62}-x^{41}+x^{20}+$ $x^4-x^{33}-x^{12}$	261(3)	212(3)
$x^{163}-x^{99}+x^{35}+x^{64}-1$	PP	$x^{76}+x^{43}+x^{12}$	$x^{152}-x^{119}-x^{88}+$ $x^{86}-x^{55}+x^{24}$	490(3)	355(3)
$x^{193}-x^{64}+1$	PTr	$x^{129}+x^{86}+x^{43}$	$-x^{65}+x^{22}$	234(2)	192(2)
$x^{233}-x^{141}+x^{49}+x^{92}-1$	PP	$x^{217}-x^{170}-x^{125}+$ $x^{123}-x^{78}+x^{33}$	$x^{109}+x^{62}+x^{17}$	709(3)	512(3)
$x^{337}-x^{25}+1$	PTr	$x^{225}+x^{121}+x^{17}$	$-x^{113}+x^9$	352(2)	336(2)
$x^{507}+x^{338}+x^{169}-1$	EST	$x^{451}-x^{282}+x^{113}$	$-x^{57}-x^{226}$	451(2)	394(2)

Hence, $x^{2/3} = -cx^{u+1} - acx^{v+1} - bcx^{w+1}$. From this we deduce that

$$x^{4/3} = x^{2(u+1)} - ax^{u+v+2} + x^{2(v+1)} + x^{2(w+1)} - bx^{u+w+2} - abx^{v+w+2},$$

and thus dividing both sides of the above equation by x we get

$$x^{1/3} = x^{2u+1} - ax^{u+v+1} - bx^{u+w+1} + x^{2v+1} + x^{2w+1} - abx^{v+w+1}.$$

2) case $r = 2$: For $r = 2$, we observe that $-c = x^m + ax^{k_1} + bx^{k_2}$, which implies,

$$-cx = x(x^m + ax^{k_1} + bx^{k_2}) = x^{3(u+1)} + ax^{3(v+1)} + bx^{3(w+1)}$$

Hence, $x^{1/3} = -cx^{u+1} - acx^{v+1} - bcx^{w+1}$. We can directly obtain $x^{2/3}$ by computing,

$$\begin{aligned} x^{2/3} = (x^{1/3})^2 &= (-cx^{u+1} - acx^{v+1} - bcx^{w+1})^2 \\ &= x^{2(u+1)} - ax^{u+v+2} + x^{2(v+1)} + x^{2(w+1)} - bx^{u+w+2} - abx^{v+w+2}. \end{aligned}$$

From the above results, it turns out that for this class of tetranomials, we do not need to carry out the

reduction process indicated in Eq.(1).

C. Pentanomials

Let $\mathbb{F}_{3^m}$ be a ternary field generated by an irreducible pentanomial of the form, $p(x) = x^m - ax^{m-d} + x^{m-2d} + ax^d - 1$, with $a \neq 0$, and where m is an odd prime number that can be written as, $m = 3u + r$, where $m \equiv r \bmod 3$ $r \neq 0$, and $d = 3v + r$ is a positive integer so that $d < \lceil \frac{m}{2} \rceil$. Then, $x^m = ax^{m-d} - x^{m-2d} - ax^d + 1$, which implies,

$$\begin{aligned} x^{m+d} &= ax^m - x^{m-d} - ax^{2d} + x^d \\ &= x^{m-d} - ax^{m-2d} - x^d + a - x^{m-d} - ax^{2d} + x^d = -ax^{m-2d} - ax^{2d} + a; \\ x^{m+d+1} &= -ax^{2d+1} - ax^{m-2d+1} + ax; \\ x^{m+d+2} &= -ax^{2d+2} - ax^{m-2d+2} + ax^2. \end{aligned} \tag{7}$$

It is noticed that, $m + d \equiv 2d \equiv m - 2d \equiv -r \bmod 3$. In the following, we distinguish two cases.

1) case $r = 1$: If $r = 1$, from Eq. (7) we can write, $\sqrt[3]{x} = ax^{\frac{m+d+1}{3}} + x^{\frac{2d+1}{3}} + x^{\frac{m-2d+1}{3}}$, which implies,

$$\begin{aligned} \sqrt[3]{x^2} &= \left(ax^{\frac{m+d+1}{3}} + x^{\frac{2d+1}{3}} + x^{\frac{m-2d+1}{3}}\right)^2 \\ &= x^{2\frac{m+d+1}{3}} + x^{2\frac{2d+1}{3}} + x^{2\frac{m-2d+1}{3}} - ax^{\frac{m+3d+2}{3}} - ax^{\frac{2m-d+2}{3}} - x^{\frac{m+2}{3}}. \end{aligned}$$

2) case $r = 2$: If $r = 2$, from Eq. (7) we can write, $\sqrt[3]{x^2} = ax^{\frac{m+d+2}{3}} + x^{\frac{2d+2}{3}} + x^{\frac{m-2d+2}{3}}$. Furthermore, we have,

$$\begin{aligned} \sqrt[3]{x} &= \sqrt[3]{x^2}\left(x^{\frac{m+d-1}{3}} + x^{\frac{2d-1}{3}} + x^{\frac{m-2d-1}{3}}\right) \\ &= (ax^{\frac{m+d+2}{3}} + x^{a\frac{2d+2}{3}} + x^{\frac{m-2d+2}{3}})(x^{\frac{m+d-1}{3}} + x^{\frac{2d-1}{3}} + x^{\frac{m-2d-1}{3}}) \\ &= x^{\frac{2m+2d+1}{3}} - ax^{\frac{m+3*d+1}{3}} - ax^{\frac{2m-d+1}{3}} + x^{\frac{4d+1}{3}} - x^{\frac{m+1}{3}} + x^{\frac{2m-4d+1}{3}}. \end{aligned}$$

We stress that the polynomial degrees of the constants $x^{\frac{1}{3}}$ and $x^{\frac{2}{3}}$ associated to this class of pentanomials, force us to carry out the reduction process post-computation indicated in (1).

D. Equally Spaced Polynomials

Irreducible Equally-Spaced Polynomials (ESPs) have the same space separation between two consecutive non-zero coefficients. They can be defined as

$$p(x) = x^m + p_{(k-1)d}x^{(k-1)d} + \cdots + p_{2d}x^{2d} + p_d x^d + p_0 \ , \tag{8}$$

where $m = kd$ and $p_{id} \in \mathbb{F}_3^*$ for $i = 0, 1, 2, \ldots, k-1$. The ESP specializes to the all-one-polynomials (AOPs) when $d = 1$, i.e., $p(x) = x^m + p_{m-1}x^{m-1} + \cdots + p_1 x + p_0$, and to the equally-spaced trinomials when $d = \frac{m}{2}$, i.e., $p(x) = x^m + p_{\frac{m}{2}}x^{\frac{m}{2}} + p_0$.

1) Equally Spaced Tetranomials: Let $\mathbb{F}_{3^m}$ be a ternary field generated by an irreducible equally spaced tetranomial of the form, $p(x) = x^m + x^{2d} + x^d - 1$, where $m = 3d$, and where d is a positive integer such that $d \equiv 1 \bmod 3$. Then, we have that $x^m = -x^{2d} - x^d + 1$, which implies,

$$\begin{aligned} x^{m+d} &= -x^{3d} - x^{2d} + x^d \\ &= x^{2d} + x^d - 1 - x^{2d} + x^d = -x^d - 1; \\ x^{m+d+1} &= -x^{d+1} - x; \\ x^{m+d+2} &= -x^{d+2} - x^2. \end{aligned}$$

From last equality above, we have, $x^2 = -x^{d+2} - x^{m+d+2}$, and since $d \equiv 1 \bmod 3$, we have, $m+d+2 \equiv 4d+2 \equiv 0 \bmod 3$, and $d+2 \equiv 0 \bmod 3$. Therefore, we can write, $\sqrt[3]{x^2} = -(x^{\frac{d+2}{3}} + x^{\frac{4d+2}{3}})$. Moreover, since $x = -x^{d+1} - x^{4d+1}$, it implies that,

$$\sqrt[3]{x} = -\sqrt[3]{x^2}(x^{\frac{d-1}{3}} + x^{\frac{4d-1}{3}}) = (x^{\frac{d+2}{3}} + x^{\frac{4d+2}{3}})(x^{\frac{d-1}{3}} + x^{\frac{4d-1}{3}}).$$

However, we stress that irreducible equally spaced tetranomials are extremely rare. For extension degrees $m < 1000$, it can be only found three of them, for $m = 3, 39, 507$. Notice that by definition, this kind of tetranomials only exist for extension degree m, multiple of three. Furthermore, the polynomial degrees of the constants $x^{\frac{1}{3}}$ and $x^{\frac{2}{3}}$ associated to equally spaced tetranomials, force us to have a reduction process post-computation. Concrete examples of irreducible equally spaced tetranomials can be found in Table II.

2) Equally Spaced Pentanomials: Let $\mathbb{F}_{3^m}$ be a ternary field generated by an irreducible equally spaced pentanomial of the form, $p(x) = x^m + x^{3d} + x^{2d} - x^d - 1$, where $m = 4d$ and where d is a positive integer not a multiple of 3. Then, $x^m = -x^{3d} - x^{2d} + x^d + 1$, which implies,

$$\begin{aligned} x^{m+d} &= -x^{4d} - x^{3d} + x^{2d} + x^d \\ &= x^{3d} + x^{2d} - x^d - 1 - x^{3d} - x^{2d} + x^d = -x^{2d} - 1; \\ x^{m+d+1} &= -x^{2d+1} - x; \\ x^{m+d+2} &= -x^{2d+2} - x^2. \end{aligned} \tag{9}$$

It is noticed that $m + d = 5d \equiv 2d \bmod 3$. In the following, we distinguish two cases.

Case $d \equiv 1 \bmod 3$

If $d \equiv 1 \bmod 3$, then from the second last equality of Eq. (9), we have, $x = -x^{2d+1} - x^{m+d+1}$. Therefore, $\sqrt[3]{x} = -x^{\frac{2d+1}{3}} - x^{\frac{5d+1}{3}}$ and,

$$\sqrt[3]{x^2} = (-x^{\frac{2d+1}{3}} - x^{\frac{5d+1}{3}})^2 = x^{2\frac{2d+1}{3}} - x^{\frac{7d+2}{3}} + x^{2\frac{5d+1}{3}}.$$

Case $d \equiv 2 \bmod 3$

If $d \equiv 2 \bmod 3$, then from the last equality of Eq. (9), we have, $x^2 = -x^{2d+2} - x^{m+d+2}$. Therefore, $\sqrt[3]{x^2} = -x^{\frac{2d+2}{3}} - x^{\frac{5d+2}{3}}$, whereas,

$$\begin{aligned} \sqrt[3]{x} &= \sqrt[3]{x^2}(-x^{\frac{2d-1}{3}} - x^{\frac{5d-1}{3}}) \\ &= (-x^{\frac{2d+2}{3}} - x^{\frac{5d+2}{3}})(-x^{\frac{2d-1}{3}} - x^{\frac{5d-1}{3}}) \\ &= x^{\frac{4d+1}{3}} - x^{\frac{7d+1}{3}} + x^{\frac{10d+1}{3}}. \end{aligned}$$

Unfortunately, although irreducible equally spaced pentanomials are more abundant than their tetranomials counterpart, they are still very rare. For extension degrees $m < 1000$, there are only 20 of them. Concrete examples of irreducible equally spaced pentanomials can be found in Table II. It is noted that the polynomial degrees of the constants $x^{\frac{1}{3}}$ and $x^{\frac{2}{3}}$ associated to this class of pentanomials, force us to have a reduction process post-computation indicated in (1).

V. RING MAPPING AND ROOT COMPUTATION

One approach proposed in the literature for carrying out the arithmetic of the finite field $\mathbb{F}_{p^m}$ is the embedding of $\mathbb{F}_{p^m}$ in a proper ring and performing all the arithmetic operations in the ring and projecting the result back to the original field. If ring is chosen properly, then field arithmetic can be sped up. This idea is known as the ring mapping. In the following example taken from [16] we briefly explain this technique in the context of squaring and square-root taking in the binary fields. (The author in [16] credits this example to Ito and Tsujii [17])

Suppose for some m, $P(x) = x^m + x^{m-1} + \ldots + x + 1$ is irreducible over $\mathbb{F}_2$. Then we have $\mathbb{F}_{2^m} = \mathbb{F}_2[x]/(P(x))$. Now $x^{m+1} + 1 = (x+1)P(x)$. This implies that

$$R_2 = \frac{F_2[x]}{(x^{m+1}+1)} \cong \mathbb{F}_{2^m} \times \mathbb{F}_2.$$

Regarding $\mathbb{F}_{2^m}$ and R_2 as vector spaces over the binary field $\mathbb{F}_2$,

$$\{1, x, x^2, \ldots, x^{m-1}\}$$

and

$$\{1, x, x^2, \ldots, x^{m-1}, x^m\}$$

are standard bases for $\mathbb{F}_{2^m}$ and R_2 over $\mathbb{F}_2$, respectively. Squaring and square-root taking are very simple in R_2. If $b = a_m x^m + \ldots + a_2 x^2 + a_1 x + a_0$ is an element of R_2, then from Eq. (3) and the fact that $x^{m+1} = 1$ in R_2 it follows that

$$b^2 = a_{m/2}x^m + a_n x^{m-1} + a_{m/2-1}x^{m-2} + a_{m-1}x^{m-3} + \ldots + a_2 x^4 + a_{m/2+2}x^3 + a_1 x^2 + a_{m/2+1}x + a_0.$$

Since square-root taking is just the inverse operation of squaring, thus one can take the square of an element easily too. Further information on how this can be used to square or take the square root of an element of $\mathbb{F}_{2^m}$ can be found in [16].

In [16], it has been mentioned that the above idea can be generalized to other finite fields. Here we show the details of applying the above idea to cubing and cube-root taking.

Now suppose for some m, $P(x) = x^m + x^{m-1} + \ldots + x + 1$ is irreducible over $\mathbb{F}_3$ (this implies that

$m \neq 2 \pmod 3$ (see [16])). Then $\mathbb{F}_{3^m} = \mathbb{F}_3[x]/(P(x))$. We have $x^{m+1} - 1 = (x-1)P(x)$. Thus

$$R_3 = \frac{F_3[x]}{(x^{m+1}-1)} \cong \mathbb{F}_{3^m} \times \mathbb{F}_3.$$

The same as before $\{1, x, x^2, \ldots, x^{m-1}\}$ and $\{1, x, x^2, \ldots, x^{m-1}, x^m\}$ are standard bases for $\mathbb{F}_{3^m}$ and R_3 over $\mathbb{F}_3$, respectively. Now if we assume that $m \equiv 1 \pmod 3$, then from $x^{m+1} = 1$ in R_3, it follows that $x^{1/3} = x^{(m+1)/3}$ and $x^{2/3} = x^{(2m+2)/3}$. Thus if $b = a_m x^m + \ldots + a_2 x^2 + a_1 x + a_0$ is an element of R_3, then from (1), it follows that

$$\begin{aligned} b^{1/3} = \quad & a_{m-2}x^m + a_{m-5}x^{m-1} + a_{m-8}x^{m-2} + \ldots + a_2 x^{(2m+4)/3} \\ + \quad & a_m x^{(2m+1)/3} + + a_{m-3}x^{(2m-2)/3} + \ldots + a_1 x^{(m+2)/3} \\ + \quad & a_{m-1}x^{(m-1)/3} + \ldots + a_3 x + a_0. \end{aligned}$$

Similar formula can be obtained for the case when m is divisible by 3. For how one can move back and forth from $\mathbb{F}_{3^m}$ to R_3 see [16]. Notice that one drawback of the above method is that the embedding mentioned above works just for composite m while most of the times we are interested in prime m. One possible alternative strategy when m is such that the above method does not work and there is no preferred irreducible trinomial of degree m, is to look for trinomials or tetranomials of preferred shape which have degrees higher than m and are divisible by an irreducible polynomial of degree m. If such a trinomial or tetranomial exists, then one can use the idea of ring mapping to accelerate the root computation.

VI. Applications to Pairing-Based Cryptography

As it was mentioned in the Introduction Section, field cubing and field cube root are crucial arithmetic operations required by several pairing algorithms working on supersingular elliptic curves defined over ternary fields $\mathbb{F}_{3^m}$. Let E be a supersingular elliptic curve defined by the equation $y^2 = x^3 - x + b$, with $b \in \{-1, 1\}$. Given a prime integer m, the number of rational points of E over the finite field $\mathbb{F}_{3^m}$ is given by [2],

TABLE III

REDUCTION POLYNOMIALS THAT YIELD LOW COST CUBINGS AND/OR CUBE ROOTS FOR SUPERSINGULAR ELLIPTIC CURVES DEFINED BY THE EQUATION $y^2 = x^3 - x + b$, WITH LARGE r-TORSION SUBGROUPS OVER $\mathbb{F}_{3^m}$, WITH m A PRIME NUMBER IN THE RANGE $[47, 541]$

m	b	μ	$\#E(\mathbb{F}_{3^m})$	r	recommended reduction polynomial
47	-1	1	$283r$	$\left(3^{47} - 3^{24} + 1\right)/283$	$x^{47} - x^{32} + 1$
53	-1	-1	$48973r$	$\left(3^{53} + 3^{27} + 1\right)/48973$	$x^{53} + x^{42} + x^{31} - x^{11} - 1$
79	-1	-1	r	$\left(3^{79} + 3^{40} + 1\right)$	$x^{79} - x^{51} + x^{28} + x^{23} - 1$
97	1	1	$7r$	$\left(3^{97} + 3^{49} + 1\right)/7$	$x^{97} - x^{16} + 1$
163	-1	-1	r	$\left(3^{163} + 3^{82} + 1\right)$	$x^{163} - x^{99} + x^{64} + x^{35} - 1$
167	1	1	$7r$	$\left(3^{167} + 3^{84} + 1\right)/7$	$x^{167} - x^{71} + 1$
193	-1	1	r	$\left(3^{193} - 3^{97} + 1\right)$	$x^{193} - x^{64} + 1$
239	-1	1	r	$\left(3^{239} - 3^{120} + 1\right)$	$x^{239} - x^{5} + 1$
317	-1	-1	r	$\left(3^{317} + 3^{159} + 1\right)$	$x^{317} - x^{267} + x^{217} + x^{50} - 1$
353	-1	-1	r	$\left(3^{353} + 3^{177} + 1\right)$	$x^{353} - x^{249} + x^{145} + x^{104} - 1$
509	1	-1	$7r$	$\left(3^{509} - 3^{255} + 1\right)/7$	$x^{509} + x^{294} - x^{215} + x^{79} - 1$

$N = 3^m + 1 + \mu b 3^{(m+1)/2}$, with

$$\mu = \begin{cases} +1 & \text{if } m \equiv 1,\ 11 \pmod{12}, \\ -1 & \text{if } m \equiv 5,\ 7 \pmod{12}. \end{cases}$$

Let r be the largest prime factor of N. Then, we can write $N = i \cdot r$, where i is a small positive integer. Now if P is a rational point, $[i]P$ belongs to the r-torsion subgroup. Hence, a design problem consists of finding extension degrees m where N has large prime factors r. Table III shows a selection of prime extension degrees $m \in [47, 541]$ that enjoy large r-torsion subgroups along with the corresponding reduction polynomials associated to them.

VII. CONCLUSION

In this paper we investigated the computational cost associated with field cubing and cube root computation in ternary extension fields, $\mathbb{F}_{3^m}$ generated by special classes of irreducible polynomials. We presented cube-root friendly families of irreducible trinomials, tetranomials and pentanomials that exist for most prime extension degrees m, which are the cases of interest in modern cryptographic applications. More specifically, in the range $[47, 541]$, there exist a total of 86 prime numbers. Using the irreducible trinomials, tetranomials and pentanomials discussed in Section IV, we are able to propose

a reduction polynomial for all the 86 instances except for $m = 89, 149, 151, 283, 449, 463, 521$. The proposed polynomials are listed in Appendix A, along with the corresponding values of the constants $x^{\frac{1}{3}}$ and $x^{\frac{2}{3}}$ associated to them.

ACKNOWLEDGMENT

The authors would like to thank Darrel Hankerson and Jean-Luc Beuchat for their valuable comments that help to improve the presentation of this paper. The second author acknowledges support from CONACyT through the CONACyT project number 60240.

REFERENCES

[1] P. Barreto, H. Kim, B. Lynn, and M. Scott, "Efficient algorithms for pairing-based cryptosystems," in *Advances in Cryptology – CRYPTO 2002*, ser. Lecture Notes in Computer Science, M. Yung, Ed., no. 2442. Springer, 2002, pp. 354–368.

[2] J.-L. Beuchat, N. Brisebarre, J. Detrey, E. Okamoto, M. Shirase, and T. Takagi, "Algorithms and arithmetic operators for computing the η_T pairing in characteristic three," *IEEE Transactions on Computers*, vol. 57, no. 11, pp. 1454–1468, Nov. 2008.

[3] J.-L. Beuchat, N. Brisebarre, J. Detrey, E. Okamoto, and F. Rodríguez-Henríquez, "A comparison between hardware accelerators for the modified tate pairing over $\mathbb{F}_{2^m}$ and $\mathbb{F}_{3^m}$," in *Pairing 2008*, ser. Lecture Notes in Computer Science, S. Galbraith and K. Paterson, Eds., no. 5209. Springer, 2008, pp. 297–315.

[4] O. Ahmadi, D. Hankerson, and A. Menezes, "Software implementation of arithmetic in $\mathbb{F}_{3^{\mathrm{m}}}$," in *WAIFI*, ser. Lecture Notes in Computer Science, C. Carlet and B. Sunar, Eds., vol. 4547. Springer, 2007, pp. 85–102.

[5] D. Hankerson, A. Menezes, and M. Scott, *Software Implementation of Pairings*, ser. Cryptology and Information Security. IOS Press, to appear, ch. 12.

[6] P. S. L. M. Barreto, "A note on efficient computation of cube roots in characteristic 3," Cryptology ePrint Archive, Report 2004/305, 2004, http://eprint.iacr.org/.

[7] O. Ahmadi, D. Hankerson, and A. Menezes, "Formulas for cube roots in $\mathbb{F}_{3^{\mathrm{m}}}$," *Discrete Applied Mathematics*, vol. 155, no. 3, pp. 260–270, 2007.

[8] IEEE standards documents, *IEEE P1363: Standard specifications for public key cryptography. Draft Version D18*. IEEE, November 2004, http://grouper.ieee.org/groups/1363/.

[9] K. Fong, D. Hankerson, J. López, and A. Menezes, "Field inversion and point halving revisited." *IEEE Trans. Computers*, vol. 53, no. 8, pp. 1047–1059, 2004.

[10] F. Rodríguez-Henríquez, G. Morales-Luna, and J. López, "Low-complexity bit-parallel square root computation over GF(2^m) for all trinomials," *IEEE Trans. Computers*, vol. 57, no. 4, pp. 472–480, 2008.

[11] R. Avanzi, "Another look at square roots and traces (and quadratic equations) in fields of even characteristic," Cryptology ePrint Archive, Report 2007/103, 2007, http://eprint.iacr.org/.

[12] R. M. Avanzi, "Another look at square roots (and other less common operations) in fields of even characteristic," in *Selected Areas in Cryptography*, ser. Lecture Notes in Computer Science, C. M. Adams, A. Miri, and M. J. Wiener, Eds., vol. 4876. Springer, 2007, pp. 138–154.

[13] O. Ahmadi, D. Hankerson, and F. Rodríguez-Henríquez, "Parallel formulations of scalar multiplication on koblitz curves," *Special Issue on Cryptography in Computer System Security Journal of Universal Computer Science (JUCS)*, vol. 14, pp. 481–504, 2008.

[14] M. Scott, "Optimal irreducible polynomials for GF(2^m) arithmetic," Cryptology ePrint Archive, Report 2007/192, 2007, http://eprint.iacr.org/.

[15] D. Panairo and D. Thompson, "Efficient pth root computations in finite fields of characteristic p," *Designs, Codes and Cryptography*, To appear in 2009.

[16] J. H. Silverman, "Fast multiplication in finite fields GF(2^{n})," in *CHES*, ser. Lecture Notes in Computer Science, Çetin Kaya Koç and C. Paar, Eds., vol. 1717. Springer, 1999, pp. 122–134.

[17] B. Ito and S. Tsujii, "Structure of a parallel multipliers for a class of fields GF(2^m) using normal bases," *Information and Computers*, vol. 83, pp. 21–40, 1989.

APPENDIX A

In Tables IV and V we list the reduction polynomials for $\mathbb{F}_{3^m}$ yielding low cost cubings and/or cube roots, with m a prime number in the range $[47, 307]$ and $[311, 541]$, respectively. We also list the values of the constants $x^{\frac{1}{3}}$ and $x^{\frac{2}{3}}$ generated by the proposed polynomials.

In the range $[47, 541]$, there exist a total 86 prime numbers. Using the irreducible trinomials and pentanomials discussed in Section IV, we are able to propose a reduction polynomial for all the 86 instances, excepting for $m = 89, 149, 151, 283, 449, 463, 521$.

TABLE IV

REDUCTION POLYNOMIALS FOR $\mathbb{F}_{3^m}$, YIELDING LOW COST CUBINGS AND/OR CUBE ROOTS, WITH m A PRIME NUMBER IN THE RANGE $[47, 307]$

Reduction polynomial	$\sqrt[3]{x}$	$\sqrt[3]{x^2}$
$x^{47} - x^{32} + 1$	$-x^{16} + x^{11}$	$x^{32} + x^{27} + x^{22}$
$x^{53} + x^{42} + x^{31} - x^{11} - 1$	$x^{43} + x^{32} + x^{29} + x^{21} - x^{18} + x^{15}$	$-x^{22} + x^{11} + x^8$
$x^{59} - x^{17} + 1$	$-x^{20} + x^6$	$x^{40} + x^{26} + x^{12}$
$x^{61} - x^7 + 1$	$x^{41} + x^{23} + x^5$	$-x^{21} + x^3$
$x^{67} - x^{45} + x^{23} + x^{22} - 1$	$x^{30} + x^{15} + x^8$	$x^{60} - x^{45} - x^{38} + x^{30} - x^{23} + x^{16}$
$x^{71} - x^{20} + 1$	$-x^{24} + x^7$	$x^{48} + x^{31} + x^{14}$
$x^{73} - x + 1$	$x^{49} + x^{25} + x$	$-x^{25} + x$
$x^{79} - x^{51} + x^{28} + x^{23} - 1$	$x^{36} + x^{19} + x^8$	$x^{72} - x^{55} - x^{44} + x^{38} - x^{27} + x^{16}$
$x^{83} - x^{32} + 1$	$-x^{28} + x^{11}$	$x^{56} + x^{39} + x^{22}$
$x^{97} - x^{16} + 1$	$x^{65} + x^{38} + x^{11}$	$-x^{33} + x^6$
$x^{101} - x^{81} + x^{61} + x^{20} - 1$	$x^{81} - x^{61} - x^{54} + x^{41} - x^{34} + x^{27}$	$x^{41} + x^{21} + x^{14}$
$x^{103} + x^{54} - x^{49} + x^5 - 1$	$-x^{51} + x^{33} + x^2$	$x^{102} + x^{84} + x^{66} + x^{53} - x^{35} + x^4$
$x^{107} - x^{11} + 1$	$-x^{36} + x^4$	$x^{72} + x^{40} + x^8$
$x^{109} - x^{13} + 1$	$x^{73} + x^{41} + x^9$	$-x^{37} + x^5$
$x^{113} - x^{87} + x^{61} + x^{26} - 1$	$x^{93} - x^{67} - x^{64} + x^{41} - x^{38} + x^{35}$	$x^{47} + x^{21} + x^{18}$
$x^{127} - x^{111} + x^{95} + x^{16} - 1$	$x^{48} + x^{32} + x^{11}$	$x^{96} - x^{80} + x^{64} - x^{59} - x^{43} + x^{22}$
$x^{131} - x^{83} + 1$	$-x^{44} + x^{28}$	$x^{88} + x^{72} + x^{56}$
$x^{137} + x^{72} - x^{65} + x^7 - 1$	$x^{135} + x^{111} + x^{87} + x^{70} - x^{46} + x^5$	$-x^{68} + x^{44} + x^3$
$x^{139} + x^{120} + x^{101} - x^{19} - 1$	$-x^{53} + x^{34} + x^{13}$	$x^{106} + x^{87} + x^{68} + x^{66} - x^{47} + x^{26}$
$x^{157} - x^{22} + 1$	$x^{105} + x^{60} + x^{15}$	$-x^{53} + x^8$
$x^{163} - x^{99} + x^{64} + x^{35} - 1$	$x^{76} + x^{43} + x^{12}$	$x^{152} - x^{119} - x^{88} + x^{86} - x^{55} + x^{24}$
$x^{167} - x^{71} + 1$	$-x^{56} + x^{24}$	$x^{112} + x^{80} + x^{48}$
$x^{173} - x^{147} + x^{121} + x^{26} - 1$	$x^{133} - x^{107} - x^{84} + x^{81} - x^{58} + x^{35}$	$x^{67} + x^{41} + x^{18}$
$x^{179} - x^{59} + 1$	$-x^{60} + x^{20}$	$x^{120} + x^{80} + x^{40}$
$x^{181} - x^{37} + 1$	$x^{121} + x^{73} + x^{25}$	$-x^{61} + x^{13}$
$x^{191} - x^{71} + 1$	$-x^{64} + x^{24}$	$x^{128} + x^{88} + x^{48}$
$x^{193} - x^{64} + 1$	$x^{129} + x^{86} + x^{43}$	$-x^{65} + x^{22}$
$x^{197} - x^{117} + x^{80} + x^{37} - 1$	$x^{185} - x^{146} + x^{107} - x^{105} - x^{66} + x^{25}$	$x^{93} + x^{54} + x^{13}$
$x^{199} - x^{177} + x^{155} + x^{22} - 1$	$x^{74} + x^{52} + x^{15}$	$x^{148} - x^{126} + x^{104} - x^{89} - x^{67} + x^{30}$
$x^{211} - x^{189} + x^{167} + x^{22} - 1$	$x^{78} + x^{56} + x^{15}$	$x^{156} - x^{134} + x^{112} - x^{93} - x^{71} + x^{30}$
$x^{223} + x^{144} - x^{79} + x^{65} - 1$	$-x^{101} + x^{53} + x^{22}$	$x^{202} + x^{154} + x^{123} + x^{106} - x^{75} + x^{44}$
$x^{227} - x^{11} + 1$	$-x^{76} + x^4$	$x^{152} + x^{80} + x^8$
$x^{229} - x^{79} + 1$	$x^{153} + x^{103} + x^{53}$	$-x^{77} + x^{27}$
$x^{233} - x^{141} + x^{92} + x^{49} - 1$	$x^{217} - x^{170} - x^{125} + x^{123} - x^{78} + x^{33}$	$x^{109} + x^{62} + x^{17}$
$x^{239} - x^5 + 1$	$-x^{80} + x^2$	$x^{160} + x^{82} + x^4$
$x^{241} - x^{88} + 1$	$x^{161} + x^{110} + x^{59}$	$-x^{81} + x^{30}$
$x^{251} - x^{26} + 1$	$-x^{84} + x^9$	$x^{168} + x^{93} + x^{18}$
$x^{257} - x^{165} + x^{92} + x^{73} - 1$	$x^{233} - x^{178} - x^{141} + x^{123} - x^{86} + x^{49}$	$x^{117} + x^{62} + x^{25}$
$x^{263} - x^{104} + 1$	$-x^{88} + x^{35}$	$x^{176} + x^{123} + x^{70}$
$x^{269} + x^{150} - x^{119} + x^{31} - 1$	$x^{259} + x^{209} + x^{159} + x^{140} - x^{90} + x^{21}$	$-x^{130} + x^{80} + x^{11}$
$x^{271} + x^{246} + x^{221} - x^{25} - 1$	$-x^{99} + x^{74} + x^{17}$	$x^{198} + x^{173} + x^{148} + x^{116} - x^{91} + x^{34}$
$x^{277} - x^{97} + 1$	$x^{185} + x^{125} + x^{65}$	$-x^{93} + x^{33}$
$x^{281} - x^{231} + x^{181} + x^{50} - 1$	$x^{221} - x^{171} - x^{144} + x^{121} - x^{94} + x^{67}$	$x^{111} + x^{61} + x^{34}$
$x^{293} - x^{285} + x^{277} + x^8 - 1$	$x^{201} - x^{193} + x^{185} - x^{106} - x^{98} + x^{11}$	$x^{101} + x^{93} + x^6$
$x^{307} + x^{258} + x^{209} - x^{49} - 1$	$-x^{119} + x^{70} + x^{33}$	$x^{238} + x^{189} + x^{152} + x^{140} - x^{103} + x^{66}$

TABLE V

REDUCTION POLYNOMIALS FOR $\mathbb{F}_{3^m}$, YIELDING LOW COST CUBINGS AND/OR CUBE ROOTS, WITH m A PRIME NUMBER IN THE RANGE $[311, 541]$

Reduction polynomial	$\sqrt[3]{x}$	$\sqrt[3]{x^2}$
$x^{311}+x^{17}+x^{11}+1$	$-x^{104}-x^{6}-x^{4}$	$x^{208}-x^{110}-x^{108}+x^{12}-x^{10}+x^{8}$
$x^{313}-x^{187}+1$	$x^{209}+x^{167}+x^{125}$	$-x^{105}+x^{63}$
$x^{317}-x^{267}+x^{217}+x^{50}-1$	$x^{245}-x^{195}-x^{156}+x^{145}-x^{106}+x^{67}$	$x^{123}+x^{73}+x^{34}$
$x^{331}+x^{246}+x^{161}-x^{85}-1$	$-x^{139}+x^{57}+x^{54}$	$x^{278}+x^{196}+x^{193}+x^{114}-x^{111}+x^{108}$
$x^{337}-x^{25}+1$	$x^{225}+x^{121}+x^{17}$	$-x^{113}+x^{9}$
$x^{347}-x^{65}+1$	$-x^{116}+x^{22}$	$x^{232}+x^{138}+x^{44}$
$x^{349}-x^{223}+1$	$x^{233}+x^{191}+x^{149}$	$-x^{117}+x^{75}$
$x^{353}-x^{249}+x^{145}+x^{104}-1$	$x^{305}-x^{222}-x^{201}+x^{139}-x^{118}+x^{97}$	$x^{153}+x^{70}+x^{49}$
$x^{359}-x^{122}+1$	$-x^{120}+x^{41}$	$x^{240}+x^{161}+x^{82}$
$x^{367}-x^{303}+x^{239}+x^{64}-1$	$x^{144}+x^{80}+x^{43}$	$x^{288}-x^{224}-x^{187}+x^{160}-x^{123}+x^{86}$
$x^{373}-x^{25}+1$	$x^{249}+x^{133}+x^{17}$	$-x^{125}+x^{9}$
$x^{379}+x^{264}+x^{149}-x^{115}-1$	$-x^{165}+x^{77}+x^{50}$	$x^{330}+x^{242}+x^{215}+x^{154}-x^{127}+x^{100}$
$x^{383}-x^{80}+1$	$-x^{128}+x^{27}$	$x^{256}+x^{155}+x^{54}$
$x^{389}-x^{249}+x^{140}+x^{109}-1$	$x^{353}-x^{270}-x^{213}+x^{187}-x^{130}+x^{73}$	$x^{177}+x^{94}+x^{37}$
$x^{397}+x^{31}+x^{25}+1$	$x^{265}-x^{143}-x^{141}+x^{21}-x^{1}9+x^{17}$	$-x^{133}-x^{11}-x^{9}$
$x^{401}+x^{210}-x^{191}+x^{19}-1$	$x^{395}+x^{325}+x^{255}+x^{204}-x^{134}+x^{13}$	$-x^{198}+x^{128}+x^{7}$
$x^{409}-x^{136}+1$	$x^{273}+x^{182}+x^{91}$	$-x^{137}+x^{46}$
$x^{419}-x^{136}+1$	$-x^{140}+x^{46}$	$x^{280}+x^{186}+x^{92}$
$x^{421}-x^{13}+1$	$x^{281}+x^{145}+x^{9}$	$-x^{141}+x^{5}$
$x^{431}-x^{365}+1$	$-x^{144}+x^{122}$	$x^{288}+x^{266}+x^{244}$
$x^{433}-x^{262}+1$	$x^{289}+x^{232}+x^{175}$	$-x^{145}+x^{88}$
$x^{439}-x^{231}+x^{208}+x^{23}-1$	$x^{216}+x^{139}+x^{8}$	$x^{432}-x^{355}+x^{278}-x^{224}-x^{147}+x^{16}$
$x^{443}-x^{188}+1$	$-x^{148}+x^{63}$	$x^{296}+x^{211}+x^{126}$
$x^{457}-x^{67}+1$	$x^{305}+x^{175}+x^{45}$	$-x^{153}+x^{23}$
$x^{461}+x^{432}+x^{403}-x^{29}-1$	$x^{327}+x^{298}+x^{269}+x^{183}-x^{154}+x^{39}$	$-x^{164}+x^{135}+x^{20}$
$x^{467}-x^{92}+1$	$-x^{156}+x^{31}$	$x^{312}+x^{187}+x^{62}$
$x^{479}-x^{221}+1$	$-x^{160}+x^{74}$	$x^{320}+x^{234}+x^{148}$
$x^{487}-x^{255}+x^{232}+x^{23}-1$	$x^{240}+x^{155}+x^{8}$	$x^{480}-x^{395}+x^{310}-x^{248}-x^{163}+x^{16}$
$x^{491}-x^{11}+1$	$-x^{164}+x^{4}$	$x^{328}+x^{168}+x^{8}$
$x^{499}-x^{327}+x^{172}+x^{155}-1$	$x^{224}+x^{115}+x^{52}$	$x^{448}-x^{339}-x^{276}+x^{230}-x^{167}+x^{104}$
$x^{503}-x^{35}+1$	$-x^{168}+x^{12}$	$x^{336}+x^{180}+x^{24}$
$x^{509}+x^{294}-x^{215}+x^{79}-1$	$x^{483}+x^{385}+x^{287}+x^{268}-x^{170}+x^{53}$	$-x^{242}+x^{144}+x^{27}$
$x^{523}+x^{414}+x^{305}-x^{109}-1$	$-x^{211}+x^{102}+x^{73}$	$x^{422}+x^{313}+x^{284}+x^{204}-x^{175}+x^{146}$
$x^{541}-x^{145}+1$	$x^{361}+x^{229}+x^{97}$	$-x^{181}+x^{49}$