Fast Irreducibility Testing for XTR Using a Gaussian Normal Basis of Low Complexity

Soonhak Kwon[1], Chang Hoon Kim[2], and Chun Pyo Hong[2]

[1] Inst. of Basic Science and Dept. of Mathematics, Sungkyunkwan University, Suwon 440-746, Korea
shkwon@skku.edu
[2] Dept. of Computer and Information Engineering, Daegu University, Kyungsan 712-714, Korea
chkim@dsp.taegu.ac.kr, cphong@daegu.ac.kr

Abstract. XTR appeared in 2000 is a very promising alternative to elliptic curve cryptosystem. Though the basic idea behind XTR is very elegant and universal, one needs to restrict the primes p such as $p \equiv 2 \pmod 3$ for optimal normal bases since it involves many multiplications in $GF(p^2)$. Moreover the restriction $p \equiv 2 \pmod 3$ is consistently used to improve the time complexity for irreducibility testing for XTR polynomials. In this paper, we propose that a Gaussian normal basis of type $(2, k)$ for small k can also be used for efficient field arithmetic for XTR when $p \not\equiv 2 \pmod 3$. Furthermore we give a new algorithm for fast irreducibility testing and finding a generator of XTR group when $p \equiv 1 \pmod 3$. Also we present an explicit generator of XTR group which does not need any irreducibility testing when there is a Gaussian normal basis of type $(2, 3)$ in $GF(p^2)$. We show that our algorithms are simple to implement and the time complexity of our methods are comparable to the best ones proposed so far.

Keywords: XTR cryptosystem, Gauss period, normal basis, roots of unity, cubic residue.

1 Introduction

XTR public key cryptosystem is introduced by Lenstra and Verheul [1], where it is shown that 170-bit XTR realizes a security of 1024-bit RSA. Therefore it is comparable to 160-bit ECC. In a series of paper, Lenstra and Verheul [2,3], and Stam and Lenstra [4,5] discuss various ideas and techniques to speed up XTR implementation where the condition $p \equiv 2 \pmod 3$ is used for a faster arithmetic. The crucial steps of XTR are to test whether a given XTR polynomial over $GF(p^2)$ is irreducible or not and to compute a suitable trace of a zero of the polynomial to verify that the root is indeed a generator of XTR group. Stam and Lenstra [5] showed that, when $p \equiv 3 \pmod 4$, one can also compute the trace of

H. Handschuh and A. Hasan (Eds.): SAC 2004, LNCS 3357, pp. 144–158, 2005.

the root as effectively as when $p \equiv 2 \pmod 3$. However for a fast irreducibility testing, the condition $p \equiv 2 \pmod 3$ is consistently used in [2,3,4].

Our aim in this paper is to give some evidence that the basic idea of XTR implementation is not so dependent on the choice of primes p. That is, by providing a few alternative bases for different primes p, we show that the field arithmetic in $GF(p^2)$ is as equally fast as the type I optimal normal basis which was originally proposed. Furthermore we present an algorithm for fast irreducibility testing which can be used when $p \equiv 1 \pmod 3$ and show that our algorithm performs as fast as the one proposed in [3,4]. Also we propose a method of finding a generator of XTR group without any irreducibility testing by using a Gaussian normal basis of type $(2, 3)$ in $GF(p^2)$. Consequently one has much freedom to choose a prime p for fast XTR implementation. Also some possible known or unknown attacks (for example, variants of Number Field Sieve) which exploit properties of special primes p may be avoided because we can choose either $p \equiv 1 \pmod 3$ or $p \equiv 2 \pmod 3$.

This paper is organized as follows. In section 2, we study basic properties of XTR and Gauss periods. In section 3, We show that efficient field arithmetic can be obtained using a low complexity Gaussian normal basis. In section 4, we suggest a new irreducibility testing with Gauss period technique which can be used when $p \equiv 1 \pmod 3$ and show that our irreducibility testing is significantly faster than the irreducibility testings in [3,4]. In section 5, we propose an algorithm for finding an explicit generator of XTR group which does not need any irreducibility testing when there exists a type $(2, 3)$ Gaussian normal basis. In section 6, we compare our methods with previously proposed algorithms. Finally, in section 7, we give concluding remarks.

2 Overview of XTR and Gaussian Normal Basis in $GF(p^n)$

2.1 XTR Cryptosystem

Let p be a prime. For $c \in GF(p^2)$, define a cubic polynomial $F(c, X) = x^3 - cX^2 + c^pX - 1$. It is well known [1] that $F(c, X)$ is irreducible over $GF(p^2)$ if and only if all zeros of $F(c, X)$ have order dividing $p^2 - p + 1$ and > 3. When $F(c, X)$ is irreducible, letting $h \in GF(p^6)$ be any zero of $F(c, X)$, we define c_n for any n as the trace of h^n over $GF(p^2)$, i.e. $c_n = Tr(h^n) = h^n + h^{np^2} + h^{np^4} = h^n + h^{n(p-1)} + h^{-np}$. Then the roots of $F(c_n, X)$ are h^n, h^{np^2}, h^{np^4}, and for any i and j, one has the following recurrence relation,

$$c_{i+j} = c_i c_j - c_j^p c_{i-j} + c_{i-2j}. \tag{1}$$

Let q be a prime such that q divides p^2-p+1. To realize a security comparable to 1024 bit RSA, it is suggested to choose primes $p, q \approx 170$ bit with $p \geq q$. Then $GF(p^6)$ has a unique multiplicative subgroup G of order q such that G is not contained in any proper subfield of $GF(p^6)$. XTR cryptosystem is based on the assumption that if $g \in GF(p^6)$ is a generator of G where both p and q are

sufficiently large, solving $Tr(g^n) = c$ for unknown n is very difficult. It is shown [1] that finding such n is as difficult as solving a discrete logarithm problem in $GF(p^6)$. On the other hand, basic manipulations such as choosing a key of XTR are effectively done. Moreover one easily computes $Tr(g^n)$ for given $Tr(g)$ and n using the recurrence relation (1). Therefore efficient multiplication in $GF(p^2)$ is a core of XTR speed up. When one chooses $p \equiv 2 \pmod 3$, there exists a type I ONB (optimal normal basis) for $GF(p^2)$ over $GF(p)$ and using this basis, one has the time complexity for the field arithmetic in $GF(p^2)$ as follows [4].

Lemma 1. *Let $p \equiv 2 \pmod 3$ and let $\{\alpha, \alpha^p\}$ be a type I ONB (optimal normal basis) over $GF(p)$ where α is a zero of $X^2 + X + 1$. Then*

1. *Squaring in $GF(p^2)$ costs two multiplications in $GF(p)$.*
2. *Computing $xy \in GF(p^2)$ costs 2.5 multiplications in $GF(p)$.*
3. *Computing $xz - z^p y \in GF(p^2)$ costs 3 multiplications in $GF(p)$.*

We assumed in the above lemma that small number of additions in $GF(p^2)$ is free. Also it is assumed that the cost of one multiplication without reduction of two $x, y \approx p$ and one reduction of $x \approx p^2 \pmod p$ are roughly the same.

2.2 Gauss Periods of Type (n, k) in $GF(p^n)$

The theory of Gauss periods has been studied by S. Gao, J. von zur Gathen, D. Panario, I. Shparlinski, S. Vanstone, and many other people. We will briefly review the theory of Gauss periods and the corresponding Gaussian normal bases [16,17]. Let n, k be positive integers such that $r = nk + 1$ is a prime different from p. Let $K = \langle \tau \rangle$ be a unique subgroup of order k in $GF(r)^\times$. Let β be a primitive rth root of unity in $GF(p^{nk})$. The following element

$$\alpha = \sum_{j=0}^{k-1} \beta^{\tau^j} \tag{2}$$

is called a Gauss period of type (n, k) or k in $GF(p^n)$. Let $ord_r p$ be the order of $p \pmod r$ and assume $gcd(nk/ord_r p, n) = 1$. Then it is well known that α is a normal element in $GF(p^n)$. That is, letting $\alpha_i = \alpha^{p^i}$ for $0 \le i \le n-1$, $\{\alpha_0, \alpha_1, \alpha_2, \cdots, \alpha_{n-1}\}$ is a basis for $GF(p^n)$ over $GF(p)$. It is usually called a Gaussian normal basis of type (n, k) or k in $GF(p^n)$. Since $K = \langle \tau \rangle$ is a subgroup of order k in $GF(r)^\times$, a cyclic group of order nk, the quotient group $GF(r)^\times / K$ is also a cyclic group of order n and the generator of the group is pK. Therefore we have a coset decomposition of $GF(r)^\times$ as a disjoint union,

$$GF(r)^\times = K_0 \cup K_1 \cup K_2 \cdots \cup K_{n-1}, \tag{3}$$

where $K_i = p^i K, 0 \le i \le n-1$. Note that any element in $GF(r)^\times$ is uniquely written as $\tau^s p^t$ for some $0 \le s \le k-1$ and $0 \le t \le n-1$.

Now for each $0 \le i \le n-1$, we have

$$\begin{aligned}\alpha\alpha_i &= \sum_{s=0}^{k-1} \beta^{\tau^s} \sum_{t=0}^{k-1} \beta^{\tau^t p^i} \\ &= \sum_{s=0}^{k-1}\sum_{t=0}^{k-1} \beta^{\tau^s(1+\tau^{t-s}p^i)} = \sum_{s=0}^{k-1}\sum_{t=0}^{k-1} \beta^{\tau^s(1+\tau^t p^i)}.\end{aligned} \tag{4}$$

There are unique $0 \le u \le k-1$ and $0 \le v \le n-1$ such that $1+\tau^u p^v = 0 \in GF(r)$, that is, $-1 = \tau^u p^v \in K_v$. If $t \ne u$ or $i \ne v$, then we have $1 + \tau^t p^i \in K_{\sigma(t,i)}$ for some $0 \le \sigma(t,i) \le n-1$ depending on t and i, and we may write $1 + \tau^t p^i = \tau^{t'} p^{\sigma(t,i)}$ for some t'. Therefore when $i \ne v$,

$$\begin{aligned}\alpha\alpha_i &= \sum_{s=0}^{k-1}\sum_{t=0}^{k-1} \beta^{\tau^s(1+\tau^t p^i)} = \sum_{s=0}^{k-1}\sum_{t=0}^{k-1} \beta^{\tau^s(\tau^{t'} p^{\sigma(t,i)})} \\ &= \sum_{t=0}^{k-1}\sum_{s=0}^{k-1} \beta^{\tau^{s+t'} p^{\sigma(t,i)}} = \sum_{t=0}^{k-1} \alpha^{p^{\sigma(t,i)}} = \sum_{t=0}^{k-1} \alpha_{\sigma(t,i)}.\end{aligned} \tag{5}$$

Also when $i = v$,

$$\begin{aligned}\alpha\alpha_v &= \sum_{s=0}^{k-1}\sum_{t=0}^{k-1} \beta^{\tau^s(1+\tau^t p^v)} \\ &= \sum_{t\ne u}\sum_{s=0}^{k-1} \beta^{\tau^s(\tau^{t'} p^{\sigma(t,v)})} + \sum_{s=0}^{k-1} \beta^{\tau^s(1+\tau^u p^v)} \\ &= \sum_{t\ne u}\sum_{s=0}^{k-1} \beta^{\tau^{s+t'} p^{\sigma(t,v)}} + \sum_{s=0}^{k-1} 1 \\ &= \sum_{t\ne u} \alpha^{p^{\sigma(t,v)}} + k = \sum_{t\ne u} \alpha_{\sigma(t,v)} + k.\end{aligned} \tag{6}$$

Thus $\alpha\alpha_i$ is computed by the sum of at most k basis elements in $\{\alpha_0, \alpha_1, \cdots, \alpha_{n-1}\}$ for $i \ne v$ and $\alpha\alpha_v$ is computed by the sum of at most $k-1$ basis elements and the constant term $k \in GF(p)$.

3 Efficient Field Arithmetic in $GF(p^2)$ with Gaussian Normal Basis

XTR cryptosystem involves many multiplications in $GF(p^2)$. Consequently, an appropriate choice of a basis for $GF(p^2)$ over $GF(p)$ is necessary. Our purpose is to show that a Gaussian normal basis of type $(2,k)$ for small k can be used for a fast arithmetic of XTR. Recall that a type $(2,1)$ Gauss period is used in [1] where the corresponding irreducible polynomial is $X^2 + X + 1$, and such basis exists

if and only if $p \equiv 2 \pmod 3$. Similar statements can be derived for any Gauss period of type $(2, k)$. In other words, a necessary and sufficient condition for the existence of such basis will be determined and the corresponding irreducible polynomial will also be given.

For XTR, We have $n = 2$ and $2k + 1 = r$ is a prime. Thus the possible choices of k are $k = 1, 2, 3, 5, 6, 8, 9, 11, \cdots$. From the formula (3), the coset decomposition of $GF(r)^\times$ is $GF(r)^\times = K \cup pK$ where $K = \langle \tau \rangle$ is a unique subgroup of $GF(r)^\times$ of order k.

Lemma 2. *Let $2k+1 = r$ be a prime. Then a Gaussian normal basis $\{\alpha, \alpha^p\}$ of type $(2, k)$ exists in $GF(p^2)$ if and only if p is a quadratic nonresidue $\pmod r$. We have $\alpha + \alpha^p = -1$ and $\alpha\alpha^p = \frac{k+1}{2}$ if k is odd, $-\frac{k}{2}$ if k is even. That is, the corresponding irreducible polynomial of α is $X^2 + X + \frac{k+1}{2}$ if k is odd and $X^2 + X - \frac{k}{2}$ if k is even.*

Proof. It is easy to show that the given Gauss period forms a normal basis if and only if $gcd(2k/ord_r p, 2) = 1$. This condition is equivalent to say that p is an odd power of a primitive root $\pmod r$, i.e. p is a quadratic nonresidue $\pmod r$. Recall that $K = \langle \tau \rangle$ is a unique subgroup of order k in $GF(r)^\times$ and $GF(r)^\times = K \cup pK$ is a disjoint union. In particular $p \notin K$. Also from $\alpha = \sum_{j=0}^{k-1} \beta^{\tau^j}$ where β is a primitive rth root of unity over $GF(p)$, we have

$$\alpha + \alpha^p = \sum_{j=0}^{k-1} \beta^{\tau^j} + \sum_{j=0}^{k-1} \beta^{p\tau^j} = \sum_{t \in GF(r)^\times} \beta^t = \frac{\beta^r - 1}{\beta - 1} - 1 = -1. \tag{7}$$

Now from the formulas (5) and (6), we have the followings depending on whether $-1 \in K$ or $-1 \in pK$,

$$\alpha\alpha^p = \sum_{t=0}^{k-1} \alpha_{\sigma(t,1)} \quad or \quad \alpha\alpha^p = \sum_{t \neq u} \alpha_{\sigma(t,1)} + k, \tag{8}$$

where $\alpha_0 = \alpha, \alpha_1 = \alpha^p$, and $1 + \tau^t p \in p^{\sigma(t,1)} K$ with $\sigma(t, 1) = 0$ or 1. Let us consider the case $k = odd$ first. In this case, we have $-1 \in pK$ and $u \pmod k$ in the second equation of (8) is a unique value satisfying $1 + \tau^u p = 0$ in $GF(r)$. Using this, we have the following for any $j \not\equiv 0 \pmod k$,

$$\frac{1 + \tau^{u-j} p}{1 + \tau^{u+j} p} = \frac{1 - \tau^{-j}}{1 - \tau^j} = -\tau^{-j} = \tau^{u-j} p \in pK. \tag{9}$$

In other words, $1 + \tau^{u-j} p$ and $1 + \tau^{u+j} p$ are in different cosets for any $j \not\equiv 0 \pmod k$. Since $\{1 + \tau^{u+j} p | -\frac{k-1}{2} \leq j \leq \frac{k-1}{2}\} = \{1 + \tau^i p | 0 \leq i \leq k-1\}$, we find

$$\alpha\alpha^p = \frac{k-1}{2}(\alpha + \alpha^p) + k = \frac{-k+1}{2} + k = \frac{k+1}{2}. \tag{10}$$

Now suppose that $k = even$. Then $-1 \in K$ and $1 + \tau^j p \neq 0 \in GF(r)$ for any j. Also we have

$$1 + \tau^j p = \tau^j p(1 + \tau^{i-j} p), \tag{11}$$

where $i \pmod k$ is a unique value satisfying $p^2 = \tau^{-i} \in K$. In particular we have $j \not\equiv i - j \pmod k$. Thus $1 + \tau^j p$ and $1 + \tau^{i-j} p$ are in different cosets for any j. By observing the residue system $\pmod k$ can be written as a disjoint union

$$\{0, 1, 2, \cdots, k-1\} = \{j_1, i - j_1\} \cup \{j_2, i - j_2\} \cup \cdots \cup \{j_{\frac{k}{2}}, i - j_{\frac{k}{2}}\}, \tag{12}$$

we easily deduce

$$\alpha\alpha^p = \frac{k}{2}(\alpha + \alpha^p) = -\frac{k}{2}. \tag{13}$$

□

The case $k = 1$ is used in original XTR where a type I ONB exists if and only if $p \equiv 2 \pmod 3$ with the corresponding irreducible polynomial $X^2 + X + 1$. Using a Gaussian normal basis $\{\alpha, \alpha^p\}$ of type $(2, k)$ where p is a quadratic nonresidue $\pmod r$ with $r = 2k + 1$, we have roughly the same computational complexity of the field arithmetic in $GF(p^2)$. That is,

Lemma 3. *If a Gaussian normal basis of type* $(2, k)$ *is used for small* k*, Lemma 1 is also true.*

Proof. This is a straightforward computation using Lemma 2. For example, letting $x = x_0\alpha + x_1\alpha^p$ and $y = y_0\alpha + y_1\alpha^p$ in $GF(p^2)$, the multiplication of xy is as follows when $k = odd$

$$xy = \{(x_0 - x_1)(y_0 - y_1)\frac{k+1}{2} - x_0y_0\}\alpha + \{(x_0 - x_1)(y_0 - y_1)\frac{k+1}{2} - x_1y_1\}\alpha^p, \tag{14}$$

and when $k = even$

$$xy = -\{(x_0 - x_1)(y_0 - y_1)\frac{k}{2} + x_0y_0\}\alpha - \{(x_0 - x_1)(y_0 - y_1)\frac{k}{2} + x_1y_1\}\alpha^p. \tag{15}$$

Thus the computation $xy \in GF(p^2)$ needs 3 multiplications (without reduction) of integers $\approx p$ and 2 reductions $\pmod p$ of integers $\approx p^2$. Therefore the total cost is 2.5 multiplications in $GF(p)$. Here we assumed that k is small and a small number of additions in $GF(p)$ is negligible compared with one multiplication in $GF(p)$. Also letting $z = z_0\alpha + z_1\alpha^p \in GF(p^2)$, we have the value of $xz - yz^p$ as

$$\{(s\frac{k+1}{2} - x_0)z_0 - (s\frac{k+1}{2} - y_0)z_1\}\alpha + \{(s\frac{k+1}{2} + y_1)z_0 - (s\frac{k+1}{2} + x_1)z_1\}\alpha^p, \tag{16}$$

when $k = odd$, and we have

$$\{(s\frac{k}{2} + y_0)z_1 - (s\frac{k}{2} + x_0)z_0\}\alpha + \{(s\frac{k}{2} - x_1)z_1 - (s\frac{k}{2} - y_1)z_0\}\alpha^p, \tag{17}$$

when $k = even$, where $s = x_0 - x_1 + y_0 - y_1$. Thus the cost of $xz - yz^p \in GF(p^2)$ is 4 integer multiplications plus 2 reductions $\pmod p$, which is approximately 3 multiplications in $GF(p)$. □

It is not difficult to see that, with a Gaussian normal basis of type k, the number of necessary additions for each of the basic operations increases roughly in proportion to $\log_2 \frac{k+1}{2}$ or $\log_2 \frac{k}{2}$ depending on whether $k = odd$ or $k = even$. The exact number of necessary additions with a type k Gaussian normal basis is shown in Table 1 in section 6.

Note that so far we have only considered classical Gauss periods and their implications. However one may repeat the same arguments as in Lemma 2 and 3 based on the more general Gauss periods [20] successfully developed by S. Feisel, J. von zur Gathen, and M. Shokrollahi. Since the irreducible polynomial of the (classical or general) Gauss period in $GF(p^2)$ is of the form $X^2 + aX + b$ and since the linear coefficient a contributes twice of a computational cost of the constant term b, one may not have a significant advantage of general Gauss periods over classical Gauss periods in this case.

4 New Irreducibility Testing and Finding a Generator of XTR Group

For a proper implementation of XTR, we need to find a generator of XTR group. That is, an element g of prime order q with $q|p^2 - p + 1$ should be determined. This g is a zero of the polynomial $F(c, X) = X^3 - cX^2 + c^pX - 1$ where $c = g + g^{p^2} + g^{p^4}$ and it can be found as follows. First one randomly chooses $c \in GF(p^2)$ until one finds $F(c, X)$ which is irreducible over $GF(p^2)$. Here we need a fast irreducibility testing. Next, from an irreducible $F(c, X)$, one computes $c_{(p^2-p+1)/q}$ using the recurrence relation (1). Here we need an efficient field arithmetic such as Lemma 1 or 3. If $c_{(p^2-p+1)/q} \neq 3$ (which is very probable), then the roots of $F(c_{(p^2-p+1)/q}, X)$ have order q.

In section 3, we showed that, with Gaussian normal bases of low weight, the computation of $c_{(p^2-p+1)/q}$ or c_i for any i can be done as equally fast as with the optimal normal basis of type I in [3,4]. On the other hand, the best of a few irreducibility testings of $F(c, X)$ is related to an irreducibility testing of a certain cubic polynomial over $GF(p)$ [3]. And the condition $p \equiv 2 \pmod 3$ is wisely used to determine whether a given cubic polynomial over $GF(p)$ is irreducible or not. If one follows the method in [3] in the case of $p \equiv 1 \pmod 3$, one instantly encounters with the problem of determining whether an element of the form $\frac{-f_0 \pm \sqrt{\Delta}}{2}$ is a cubic residue in $GF(p^2)$ or not, where Δ and f_0 are certain integers determined from the coefficients of the cubic polynomial and Δ is a quadratic residue $\pmod p$. It seems that the computational cost of determining whether $\frac{-f_0 \pm \sqrt{\Delta}}{2}$ is a cubic residue in $GF(p^2)$ when Δ is a quadratic residue $\pmod p$ is not so cheap compared with the computational cost of determining whether $\frac{-f_0 \pm \sqrt{\Delta}}{2}$ is a cubic residue in $GF(p^2)$ when Δ is a quadratic nonresidue $\pmod p$ (See [3].). So we devise another method which combines the idea of cubic residue $\pmod p$ and the idea [2] of presenting an explicit generator of XTR group without irreducibility testing.

Let us consider the following two irreducible polynomials over $GF(p)$,

$$X^2+X+a=(X-\alpha)(X-\alpha^p) \quad \text{and} \quad X^3-b=(X-\gamma)(X-\gamma^p)(X-\gamma^{p^2}), \tag{18}$$

where α and γ are zeros the corresponding polynomials. A necessary condition for the irreducibility of X^3-b is $p\equiv 1 \pmod 3$. So throughout this section we assume $p\equiv 1 \pmod 3$.

Lemma 4. *Let $s\neq 0\in GF(p)$ and let $g=(s+\alpha\gamma)^{\frac{p^6-1}{p^2-p+1}}$. Then $X^3-Tr(g)X^2+Tr(g)^pX-1$ is irreducible over $GF(p^2)$, where $Tr(g)=g+g^{p^2}+g^{p^4}$ is the trace of g over $GF(p^2)$. Moreover letting $w\equiv b^{\frac{p-1}{3}} \pmod p$, $Tr(g)$ has the following expression*

$$\frac{-3}{P(-s)}\{(s^6+b\{w(4a-1)-a\}s^3+a^3b)\alpha + (s^6-b\{w(4a-1)+5a-1\}s^3+a^3b)\alpha^p\},$$

where $P(X)=X^6+b(1-3a)X^3+a^3b^2$.

Proof. Note that $g=(s+\alpha\gamma)^{\frac{p^6-1}{p^2-p+1}}=(s+\alpha\gamma)^{p^4+p^3-p-1}$. Clearly the order of g divides p^2-p+1. It is well known [1] that g has an order >3 and dividing p^2-p+1 if and only if the corresponding cubic polynomial is irreducible over $GF(p^2)$. Therefore to prove the irreducibility of $X^3-Tr(g)X^2+Tr(g)^pX-1$, it is enough to show that g has an order >3. Suppose that g has an order ≤ 3. Then since $p\equiv 1 \pmod 3$, we have $g^p=g$. Thus

$$(s+\alpha\gamma)^{p^5+p^4-p^2-p}=(s+\alpha\gamma)^{p^4+p^3-p-1}, \tag{19}$$

which can be written as

$$(s+\alpha^p\gamma^{p^2})(s+\alpha\gamma)=(s+\alpha^p\gamma)(s+\alpha\gamma^{p^2}). \tag{20}$$

Cancelling common terms of both sides of (20) and since $s\not\equiv 0 \pmod p$, we get

$$(\alpha-\alpha^p)(\gamma-\gamma^{p^2})=0, \tag{21}$$

which is a contradiction because the polynomials in (18) are irreducible over $GF(p)$. Now let us calculate $Tr(g)$. Let

$$P(X)=\prod_{j=0}^{5}(X-(\alpha\gamma)^{p^j})=X^6+b(1-3a)X^3+a^3b^2 \tag{22}$$

be the irreducible polynomial of $\alpha\gamma$ over $GF(p)$. From this one easily get

$$\begin{aligned}(s+\alpha\gamma)^{-p-1}=&\frac{1}{P(-s)}(s+\alpha\gamma^p)(s+\alpha\gamma^{p^2})(s+\alpha^p\gamma)(s+\alpha^p\gamma^{p^2})\\ =&\frac{1}{P(-s)}\{s^4-(\alpha\gamma+\alpha^p\gamma^p)s^3+(\alpha^{2p}\gamma^{1+p^2}+\alpha^2\gamma^{p+p^2}+a\gamma^{1+p})s^2\\ &-a(\alpha^p\gamma^{2+p^2}+\alpha\gamma^{2p+p^2})s+a^2b\gamma^{p^2}\}.\end{aligned} \tag{23}$$

Also we have

$$(s+\alpha\gamma)^{p^4+p^3} = (s+\alpha\gamma^p)(s+\alpha^p\gamma) = s^2 + (\alpha\gamma^p + \alpha^p\gamma)s + a\gamma^{1+p}. \tag{24}$$

On the other hand, from the equation $X^3 - b = 0$ in (18), we get $Tr(\gamma^j) = 0$ for any $j \not\equiv 0 \pmod 3$. This is obvious from the third order linear recurrence relation arising from the equation or one may directly show as follows. Letting $j = 3j' + j''$ with $j'' = 1, 2$, we have $Tr(\gamma^j) = Tr(\gamma^{3j'}\gamma^{j''}) = b^{j'}Tr(\gamma^{j''}) = 0$ since γ is a zero of the irreducible polynomial $X^3 - b$. From (23) and (24), though the complete expression of $(s+\alpha\gamma)^{p^4+p^3-p-1}$ is a little bit complicated, it is easy to see that the coefficients of s, s^2, s^4 and s^5 of $(s+\alpha\gamma)^{p^4+p^3-p-1}$ are polynomials of γ where each of the exponents of γ is not divisible by 3. For example, the coefficient of s^5 is $\alpha\gamma^p + \alpha^p\gamma - \alpha\gamma - \alpha^p\gamma^p$. Therefore the trace of these terms are 0 by the previous remark. Now since $w = b^{\frac{p-1}{3}} \in GF(p)$ and using

$$\gamma^{2+p} = \gamma^{2p+p^2} = bw, \quad \gamma^{1+2p} = \gamma^{2+p^2} = bw^2 \tag{25}$$

in the expression of the multiplication of the equations (23) and (24), we find that the coefficient of s^3 of $(s+\alpha\gamma)^{p^4+p^3-p-1}$ is

$$b\{w(-4a+1)+a\}\alpha + b\{w(4a-1)+5a-1\}\alpha^p. \tag{26}$$

Therefore the trace of $g = (s+\alpha\gamma)^{p^4+p^3-p-1}$ over $GF(p^2)$ is

$$\begin{aligned}\frac{-3}{P(-s)}\{&(s^6 + b\{w(4a-1)-a\}s^3 + a^3b)\alpha \\ &+ (s^6 - b\{w(4a-1)+5a-1\}s^3 + a^3b)\alpha^p\}.\end{aligned} \tag{27}$$

□

Lemma 4 implies that, if the irreducible polynomials $X^2 + X + a$ and $X^3 - b$ are given, one can find an element $Tr(g)$ where g is of order > 3 and dividing $p^2 - p + 1$. In view of Lemma 2, we may take $a = \frac{k+1}{2}$ if $k = odd$ and $a = -\frac{k}{2}$ if $k = even$. A Gaussian normal basis of type $(2, k)$, or simply of type k, in $GF(p^2)$ exists if and only if p is a quadratic nonresidue $\pmod{2k+1}$. For example, there exists a Gaussian normal basis of type 2 if and only if $p \equiv 2, 3 \pmod 5$, type 3 if and only if $p \equiv 3, 5, 6 \pmod 7$, type 5 if and only if $p \equiv 2, 6, 7, 8, 10 \pmod{11}$, etc. On the other hand, $X^3 - b$ is irreducible over $GF(p)$ if and only if b is a cubic nonresidue $\pmod p$, that is, $b^{\frac{p-1}{3}} \not\equiv 1 \pmod p$. The cost of computing $b^{\frac{p-1}{3}}$ is $1.8\log_2 p$ multiplications in $GF(p)$ if one use a square and multiply method using the same assumption in [3,4] saying that the cost of one squaring is roughly 80 percent of the cost of one multiplication. Note that one can reduce the cost of computation if one use more sophisticated argument on addition chains. For a simple example, let $\frac{p-1}{3} = \sum_{i=0}^{l-1} s_i 4^i$ be a 4-ary expansion of $\frac{p-1}{3}$ with $l = \lfloor \log_4 \frac{p-1}{3} \rfloor + 1$. Then a 4-ary window method says that

$$b^{\frac{p-1}{3}} = b^{\sum_{i=0}^{l-1} s_i 4^i} = (\cdots(((b^{s_{l-1}})^4 b^{s_{l-2}})^4 b^{s_{l-3}})^4 \cdots)^4 b^{s_0} \tag{28}$$

can be computed with $2.6\log_4 p = 1.3\log_2 p$ multiplications in $GF(p)$ using the precomputed values of b^2 and b^3. Please refer to [18,19] for more advanced window techniques and tricks of additions chains. Since one thirds of integers b are cubic residues $\pmod p$, using the above mentioned 4-ary window method, it is expected that after $1.95\log_2 p$ multiplications one finds a cubic nonresidue b $\pmod p$ and an element g of order dividing p^2-p+1 with the irreducible polynomial $X^3 - Tr(g)X + Tr(g)^p X - 1$ over $GF(p^2)$. Now let q be a prime dividing p^2-p+1. Then $g^{\frac{p^2-p+1}{q}}$ is an element of order q if and only if $Tr(g^{\frac{p^2-p+1}{q}}) \neq 3$. One may use the recurrence relation (1) to compute the trace value and in view of Lemma 3, the computational cost is $7\log_2(\frac{p^2-p+1}{q})$ multiplications in $GF(p)$.

Also the probability that $g^{\frac{p^2-p+1}{q}} = (s+\alpha\gamma)^{\frac{p^6-1}{q}}$ is an element of order q, for a randomly chosen s, is expected to $(p^6-1)(1-\frac{1}{q})/(p^6-1) = \frac{q-1}{q}$. Of course, this is not really correct unless we assume that the choice of $s+\alpha\gamma$ is random in $GF(p^6)^\times$. Since q is very large, the (error) probability that $g^{\frac{p^2-p+1}{q}} = 1$ is extremely small from a practical point of view as is already explained in [2]. Therefore we have the following result.

Theorem 5. *Let $p \equiv 1 \pmod 3$ and suppose that a Gaussian normal basis of type $(2,k)$ is given in $GF(p^2)$ for small k. Then one can find a generator of the XTR group, a trace of an element of order q, using approximately $1.95\log_2 p + 7\log_2(\frac{p^2-p+1}{q})$ multiplications in $GF(p)$ on average.*

Note that, compared with previous results, the computational cost of our algorithm has been improved from $2.7\log_2 p + 7\log_2(\frac{p^2-p+1}{q})$ in [3,4] to $1.95\log_2 p + 7\log_2(\frac{p^2-p+1}{q})$. This is because the methods in [3,4] have no other choice but to use the trace map $GF(p^2) \to GF(p)$ to avoid an exponentiation in $GF(p^2)$ with the condition $p \equiv 2 \pmod 3$ during the irreducibility testing, while our method needs an exponentiation in $GF(p)$ not in $GF(p^2)$. It should be mentioned that our factor 1.95 can be improved further if we use more refined window techniques. Another good point (or the difference) is that our algorithm is applied to the primes p with $p \equiv 1 \pmod 3$, whereas only the case $p \equiv 2 \pmod 3$ is dealt in [3,4].

5 Gaussian Normal Basis of Type (2, 3) and an Explicit Generator of XTR Group Without Irreducibility Testing

In section 4, assuming $p \equiv 1 \pmod 3$, we explained how one can find a generator of XTR group where an explicit value of $b^{\frac{p-1}{3}}$ and the irreducibility of $X^3 - b$ need to be determined. However, as is already mentioned in [2], an irreducibility testing may be omitted if one has an explicit irreducible polynomial of degree 6 over $GF(p)$ with corresponding roots of low multiplicative order. For example, Lenstra and Verheul [2] used a primitive 9th root of unity with the irreducible

polynomial $X^6 - X^3 + 1$ and a type I ONB. A necessary and sufficient condition for the irreducibility of $X^6 - X^3 + 1$ over $GF(p)$ is $p \equiv 2, 5 \pmod 9$, or equivalently $ord_9 p = 6$. In this section, we show that a similar argument also works if we use a primitive 7th root of unity with a Gaussian normal basis of type $(2, 3)$ over $GF(p)$. Our method is applicable when $p \equiv 3, 5 \pmod 7$ and no restriction of $p \pmod 3$ is necessary.

Let $\{\alpha, \alpha^p\}$ be a Gaussian normal basis of type $(2, 3)$, or more simply type 3, in $GF(p^2)$. That is, $\alpha = \beta + \beta^2 + \beta^4$ where β is a primitive 7th root of unity over $GF(p)$ and $\langle 2 \rangle$ is a unique multiplicative subgroup of order 3 in $GF(7)^\times$. Such basis exists if and only if p is a quadratic nonresidue $\pmod 7$, i.e. $p \equiv 3, 5, 6 \pmod 7$. Note that β is a zero of the polynomial

$$P(X) = \frac{X^7 - 1}{X - 1} = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1. \tag{29}$$

The above polynomial is irreducible over $GF(p)$ if and only if p is a primitive root $\pmod 7$, i.e. $p \equiv 3, 5 \pmod 7$. Therefore from now on, we assume $p \equiv 3, 5 \pmod 7$ to use the irreducibility of the polynomial in (29). Then using the relation

$$\{1, p^2, p^4\} \equiv \{1, 2, 4\} \pmod 7, \qquad \{p, p^3, p^5\} \equiv \{3, 5, 6\} \pmod 7, \tag{30}$$

we get

$$\alpha = \beta + \beta^2 + \beta^4 = \beta + \beta^{p^2} + \beta^{p^4} = Tr(\beta), \tag{31}$$

and

$$\alpha^p = \beta^3 + \beta^5 + \beta^6 = \beta^{p^3} + \beta^{p^5} + \beta^{p^6} = Tr(\beta^p). \tag{32}$$

Lemma 6. *Let $s \neq 0, \pm 1 \in GF(p)$ and let $g = (s + \beta)^{\frac{p^6 - 1}{p^2 - p + 1}}$. Then $X^3 - Tr(g)X^2 + Tr(g)^p X - 1$ is irreducible over $GF(p^2)$, where $Tr(g) = g + g^{p^2} + g^{p^4}$ is the trace of g over $GF(p^2)$. Moreover $Tr(g)$ has the following expression if $p \equiv 3 \pmod 7$,*

$$Tr(g) = \frac{-1}{P(-s)}\{(s^3 - s)(3s^3 - 3s^2 - s - 2)\alpha + ((s^2 - s)(3s^4 - 4s^2 - 4s - 6) - 1)\alpha^p\},$$

and if $p \equiv 5 \pmod 7$,

$$Tr(g) = \frac{-1}{P(-s)}\{(s^3 - s)(3s^3 - 3s^2 - s - 2)\alpha^p + ((s^2 - s)(3s^4 - 4s^2 - 4s - 6) - 1)\alpha\}.$$

Proof. It is enough to show that g has an order > 3 to show the irreducibility of the cubic polynomial because g has an order dividing $p^2 - p + 1$. Recall that, from (29),

$$P(X) = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1 \tag{33}$$

is irreducible over $GF(p)$ if and only if $p \equiv 3, 5 \pmod 7$. If the order of g is ≤ 3, then using $g^{p^2 - 1} = 1$, we get

$$(s + \beta)^{p^6 + p^5 - p^3 - p^2} = (s + \beta)^{p^4 + p^3 - p - 1}, \tag{34}$$

which is reexpressed as

$$(s+\beta)^{p^5+p+2} = (s+\beta)^{p^4+2p^3+p^2}. \tag{35}$$

Using $\beta^7 = 1$ and $p \equiv 3, 5 \pmod 7$, we may express both sides of the above equations as polynomials of β of degree < 7. Comparing the coefficients of β^j, $0 \le j \le 6$, we get a contradiction. Now let us calculate the trace value of $g = (s+\beta)^{p^4+p^3-p-1}$. The element g can be expressed as follows depending on whether $p \equiv 3 \pmod 7$ or $p \equiv 5 \pmod 7$,

$$g_0 = \frac{(s+\beta^4)(s+\beta^6)}{(s+\beta^3)(s+\beta)}, \quad or \quad g_1 = \frac{(s+\beta^2)(s+\beta^6)}{(s+\beta^5)(s+\beta)}. \tag{36}$$

Since it is trivial to show $Tr(g_0^p) = Tr(g_1)$ and $Tr(g_1^p) = Tr(g_0)$ regardless of the choice of $p \equiv 3, 5 \pmod 7$, we only need to find the trace in the case $p \equiv 3 \pmod 7$. One easily get

$$\begin{aligned}(s+\beta)^{-p-1} &= \frac{1}{P(-s)}(s+\beta^2)(s+\beta^4)(s+\beta^5)(s+\beta^6) \\ &= \frac{1}{P(-s)}\{s^4 - (1+\beta+\beta^3)s^3 - \beta^5 s^2 - (1+\beta^2+\beta^3)s + \beta^3\}.\end{aligned} \tag{37}$$

Also we have

$$(s+\beta)^{p^4+p^3} = (s+\beta^4)(s+\beta^6) = s^2 + (\beta^4+\beta^6)s + \beta^3. \tag{38}$$

Therefore g can be written as

$$\begin{aligned}g &= (s+\beta)^{\frac{p^6-1}{p^2-p+1}} = (s+\beta)^{p^4+p^3-p-1} \\ &= \frac{1}{P(-s)}\{s^6 + (\beta^2+2\beta^4+\beta^5+2\beta^6)s^5 \\ &\qquad + (-1+\beta+2\beta^3-\beta^5)s^4 + (1+2\beta+2\beta^5+\beta^6)s^3 \\ &\qquad + (-\beta+2\beta^3+\beta^5-\beta^6)s^2 + (2+\beta+2\beta^2+\beta^4)s + \beta^6\}.\end{aligned} \tag{39}$$

Taking the trace of g and using the relation (31) and (32), we get

$$\begin{aligned}Tr(g) = \frac{-1}{P(-s)}\{&(s^3-s)(3s^3-3s^2-s-2)\alpha \\ &+ ((s^2-s)(3s^4-4s^2-4s-6)-1)\alpha^p\}.\end{aligned} \tag{40}$$

□

The condition $s \neq 0, \pm 1$ is necessary in view of the equation (40) for non obvious choices of g, since when $s = 0, \pm 1$, the trace value is α or α^p and, from the equations in (36), the corresponding g is of order 7, i.e. $g \in \langle\beta\rangle$. Note that one has the similar restriction on s in [2]. Since the irreducibility testing is not necessary in this case, we have

Theorem 7. *Let $p \equiv 3, 5 \pmod 7$. Then using a Gaussian normal basis of type 3 in $GF(p^2)$, one can find a generator of the XTR group, a trace of an element of order q, using approximately $7\log_2(\frac{p^2-p+1}{q})$ multiplications in $GF(p)$ on average.*

6 Comparison with Previous Results

In section 3, we claimed that one can obtain equally fast arithmetic using a Gaussian normal basis of type k for small k. This is true if one can really ignore the cost of small number of additions of integers of bit size $\approx \log_2 p$. In fact, our method of Gaussian normal basis of type $k \geq 2$ slightly increases the number of necessary additions for each of the basic operations. Let A (resp. B) be the cost of one addition (resp. one doubling) of integers of bit size $\approx \log_2 p$ without reduction for each of the operations $x^2, xy, xz - yz^p$ in $GF(p^2)$. From the equations (14)–(17) in Lemma 3, the number of necessary additions and doublings with a Gaussian normal basis of type k can be computed easily and they are shown in Table 1.

Table 1. The number of necessary additions and doublings

Type k	1	2	3	5	6	8	9	11
x^2	$3A$	$5A+B$	$5A+2B$	$6A+2B$	$6A+2B$	$5A+3B$	$6A+3B$	$6A+3B$
xy	$3A$	$4A$	$4A+B$	$5A+B$	$5A+B$	$4A+2B$	$5A+2B$	$5A+2B$
$xz - yz^p$	$8A$	$9A$	$9A+B$	$10A+B$	$10A+B$	$9A+2B$	$10A+2B$	$10A+2B$

For example, compared with the original XTR (i.e. $k = 1$) in [3,4], the computation of xy needs one more addition of two integers of bit size $\approx \log_2 p$ with a Gaussian normal basis of type 2, and needs one more addition and a doubling with a Gaussian normal basis of type 3.

Typically, the cost of one addition (with or without reduction) is of linear complexity $O(\log_2 p)$ and the cost of one multiplication in $GF(p)$ is of $O({\log_2}^2 p)$. Thus the cost of one addition is negligible compared with the cost of one multiplication in this point of view. The cost of computing $Tr(g^m)$ with g the generator of XTR group is $7\log_2 m$ multiplications in $GF(p)$, where the constant 7 comes from the fact that two of x^2 and one of $xz - yz^p$ are computed for every iteration of the trace computation. Therefore compared with [3,4], our basis requires $c\log_2 m$ more additions for the computation of $Tr(g^m)$ where c is a small constant depending on k. For example, we have $c = 7$ (resp. $c = 10$) if we use a Gaussian normal basis of type 2 (resp. 3). Since the cost of $c\log_2 m$ (with $m < q \approx p$) additions is roughly equivalent to the cost of c multiplications in $GF(p)$, we conclude that c more multiplications in $GF(p)$ is needed for the computation of $Tr(g^m)$ compared with the original XTR with a type I ONB. This constant c is negligible compared with the total delay time of XTR implementation including parameter set up and irreducibility testing, since the worst case in Table 1 with a type 11 Gaussian normal basis requires only $c = 16$ more multiplications in $GF(p)$ for the computation of the trace value. Moreover Theorem 5 says that our method can find a generator of XTR group in $1.95\log_2 p + 7\log_2(\frac{p^2-p+1}{q})$ $GF(p)$-multiplications while the methods in [3,4] need $2.7\log_2 p + 7\log_2(\frac{p^2-p+1}{q})$ $GF(p)$-multiplications to find a generator. Thus $0.75\log_2 p$ $GF(p)$-multiplications is saved using our method and this is a huge saving compared with c multiplications in $GF(p)$.

It should be mentioned that an explicit example of XTR polynomial is given in [12] using the assumption of $p \equiv 3, 5 \pmod 7$. However the given XTR polynomial needs another condition $p \equiv 3 \pmod 4$ to be irreducible over $GF(p^2)$. On the other hand, only the assumption $p \equiv 3, 5 \pmod 7$ is needed in our Theorem 7 and no further restriction (such as $p \equiv 2 \pmod 3$ or $p \equiv 3 \pmod 4$) is needed. Moreover our theorem of using a Gaussian normal basis of type 3 presents a method of finding a generator of XTR group whereas no explicit generator (nor the method of finding it) of XTR group is given in [12].

7 Conclusions

In this paper, we showed that an efficient implementation of XTR is not so dependent on the choice of prime p. Using a Gaussian normal basis of type $(2, k)$ for small k, we find that the field arithmetic for XTR is as efficient as that of the type I ONB used in [1]. Moreover, with the condition $p \equiv 1 \pmod 3$, we presented an algorithm which combines an efficient irreducibility testing and finding a generator of XTR group, and showed that our irreducibility testing is significantly faster than the methods in [3,4]. Also we proposed an efficient algorithm, with a Gaussian normal basis of type $(2, 3)$, which determines a generator of XTR group without any irreducibility testing. The time complexity of these algorithms are comparable to the best algorithms [3,4,5] proposed so far. Since the generality of the idea behind XTR does not restrict the choice of particular primes p and since no possible cryptographic weakness or strongness of choosing special $p \equiv 1$ or $2 \pmod 3$ is known at this moment, our result provides a meaningful improvement over the existing XTR implementations.

Acknowledgements. The authors would like to thank anonymous referees and Prof. J. von zur Gathen who made valuable suggestions on the preliminary version of this paper. Also, this work was supported by Korea Research Foundation Grant (KRF-2004-015-C00004).

References

1. A.K. Lenstra and E.R. Verheul, "The XTR public key system," *Crypto 2000, Lecture Notes in Computer Science*, vol. 1880, pp. 1–19, 2000.
2. A.K. Lenstra and E.R. Verheul, "Key improvements to XTR," *Asiacrypt 2000, Lecture Notes in Computer Science*, vol. 1976, pp. 220–233, 2000.
3. A.K. Lenstra and E.R. Verheul, "Fast irreducibility and subgroup membership testing in XTR," *PKC 2001, Lecture Notes in Computer Science*, vol. 1992, pp. 73–86, 2001.
4. M. Stam and A.K. Lenstra, "Speeding up XTR," *Asiacrypt 2001, Lecture Notes in Computer Science*, vol. 2248, pp. 125–143, 2001.
5. M. Stam and A.K. Lenstra, "Efficient subgroup exponentiation in quadratic and sixth degree extensions," *CHES 2002, Lecture Notes in Computer Science*, vol. 2523, pp. 318–332, 2003.

6. W. Bosma, J. Hutton, and E.R. Verheul, "Looking beyond XTR," *Asiacrypt 2002, Lecture Notes in Computer Science*, vol. 2501, pp. 46–63, 2002.
7. A.E. Brouwer, R. Pellikaan, and E.R. Verheul, "Doing more with fewer bits," *Asiacrypt 1999, Lecture Notes in Computer Science*, vol. 1716, pp. 321–332, 1999.
8. E.R. Verheul, "Evidence that XTR is more secure than supersingular elliptic curve cryptosystems," *Eurocrypt 2001, Lecture Notes in Computer Science*, vol. 2045, pp. 195–210, 2001.
9. G. Gong and L. Harn, "Public key cryptosystems based on cubic finite field extensions," *IEEE Trans. Information Theory*, vol. 45, pp. 2601–2605, 1999.
10. G. Gong, L. Harn, and H. Wu, "The GH Public key cryptosystem," *SAC 2001, Lecture Notes in Computer Science*, vol. 2259, pp. 284–300, 2001.
11. S. Lim, S. Kim, I. Yie, J. Kim, and H. Lee, "XTR extended to $GF(p^{6m})$," *SAC 2001, Lecture Notes in Computer Science*, vol. 2259, pp. 301–312, 2001.
12. J. Kim, I. Yie, S. Oh, H. Kim, and J. Ryu, "Fast generation of cubic irreducible polynomials for XTR," *Indocrypt 2001, Lecture Notes in Computer Science*, vol. 2247, pp. 73–78, 2001.
13. D. Han, K. Yoon, Y. Park, C. Kim, and J. Lim, "Optimal extension fields for XTR," *SAC 2002, Lecture Notes in Computer Science*, vol. 2595, pp. 369–384, 2002.
14. W.W. Li, M. Naslund, and I. Shparlinski "Hidden number problem with the trace and bit security of XTR and LUC," *Crypto 2002, Lecture Notes in Computer Science*, vol. 2442, pp. 433–448, 2002.
15. I. Shparlinski "On the generalized hidden number problem and bit security of XTR," *AAECC 2001, Lecture Notes in Computer Science*, vol. 2227, pp. 268–277, 2001.
16. A.J. Menezes, I.F. Blake, S. Gao, R.C. Mullin, S.A. Vanstone, and T. Yaghoobian, *Applications of Finite Fields*, Kluwer Academic Publisher, 1993.
17. S. Gao, J. von zur Gathen, and D. Panario, "Gauss periods and fast exponentiation in finite fields," *Latin 1995, Lecture Notes in Computer Science*, vol. 911, pp. 311–322, 1995.
18. D.E. Knuth, "The Art of Computer Programming, Third Edition," *Vol. 2, Seminumerical Algorithms*, Addison Wesley, 1997.
19. D.M. Gordon, "A survey of fast exponentiation methods," *J. of Algorithms*, vol. 27, pp. 129–146, 1998.
20. S. Feisel, J. von zur Gathen, M. Shokrollahi, "Normal bases via general Gauss periods," *Math. Comp.*, vol. 68, pp. 271–290, 1999.