Generating Large Instances of the Gong-Harn Cryptosystem

Kenneth J. Giuliani and Guang Gong

Centre for Applied Cryptographic Research
University of Waterloo
Waterloo, Ontario, Canada, N2L 3G1
{kjgiulia, ggong}@cacr.math.uwaterloo.ca

Abstract. In 1999, Gong and Harn proposed a new cryptosystem based on third-order characteristic sequences over finite fields. This paper gives an efficient method to generate instances of this cryptosystem over large finite fields. The method first finds a "good" prime p to work with and then constructs the sequence to ensure that it has the desired period. This method has been implemented in C++ using NTL [7] and so timing results are presented.

1 Introduction

In 1998 and 1999, Gong and Harn proposed a new public-key cryptosystem (PKC) based on third-order characteristic sequences of period q^2+q+1 over $\mathbb{F}_q$ where q is a power of a prime, published in ChinaCrypt'98 [1] and in the IEEE Transactions on Information Theory [2], respectively. The security of the PKC is based on the difficulty of solving the discrete logarithm (DL) in $\mathbb{F}_{q^3}$. In 2000, Lenstra and Verheul [3] proposed the XTR public-key cryptosystem at the Crypto'2000, which is based on the third-order characteristic sequences with period p^2-p+1 by taking $q=p^2$. However, for large values of p where $q=p^r$, it seems to be difficult to check whether or not a sequence has the correct period q^2+q^2+1 in the GH-PKC. In this paper, we give a method for constructing such instances which are assured to have the desired properties for the case $q=p^2$. The more general case $q=p^r$ will appear in the full paper.

2 Third-Order Characteristic Sequences and the Gong-Harn Cryptosystem

In this section, we present a review for 3rd-order characteristic sequences over finite fields and the GH Diffie-Hellman key agreement protocol.

2.1 3rd-Order Characteristic Sequences

Let

$$f(x) = x^3 - ax^2 + bx - 1, a, b \in \mathbb{F}_q \tag{1}$$

be an irreducible polynomial over $\mathbb{F}_q$ and α be a root of $f(x)$ in the extension field $\mathbb{F}_{q^3}$. A sequence $\{s_i\}$ is said to be a 3rd-order characteristic sequence generated by $f(x)$ if the initial state of $\{s_i\}$ is given by

$$s_0 = 3, s_1 = a, \text{ and } s_2 = a^2 - 2b$$

and

$$s_{k+3} = as_{k+2} - bs_{k+1} + s_k, k = 0, 1, \cdots.$$

In this case, the trace representation of $\{s_i\}$ is as follows:

$$s_k = Tr(\alpha^k) = \alpha^k + \alpha^{kq} + \alpha^{kq^2}, k = 0, 1, 2, \cdots.$$

In the following, we write $s_k = s_k(a, b)$ or $s_k(f)$ to indicate the generating polynomial. Let $f^{-1}(x) = x^3 - bx^2 + ax - 1$, which is the reciprocal polynomial of $f(x)$. Let $\{s_k(b, a)\}$ be the characteristic sequence of $f^{-1}(x)$, called *the reciprocal sequence of* $\{s_k(a, b)\}_{k \geq 0}$. Then we have $s_{-k}(a, b) = s_k(b, a), k = 1, 2, \cdots$.

2.2 The GH Diffie-Hellman Key Agreement Protocol

Note that in [2], the GH-DH was presented in $\mathbb{F}_p$. However, these results are also true in $\mathbb{F}_q$ where q is a power of a prime.

GH-DH Key Agreement Protocol (Gong and Harn, 1999) [2] :

System parameters: p is a prime number, $q = p^r$ and $f(x) = x^3 - ax^2 + bx - 1$ which is an irreducible polynomial over $\mathbb{F}_q$ with period $Q = q^2 + q + 1$.

User Alice chooses $e, 0 < e < Q$, with $gcd(e, Q) = 1$ as her private key and computes (s_e, s_{-e}) as her public key. Similarly, user Bob has $r, 0 < r < Q$, with $gcd(r, Q) = 1$ as his private key and (s_r, s_{-r}) as his public key. In the key distribution phase, Alice uses Bob's public key to form a polynomial:

$$g(x) = x^3 - s_r x^2 + s_{-r} x - 1$$

and then computes the eth terms of a pair of reciprocal char-sequences generated by $g(x)$. I.e., Alice computes

$$s_e(s_r, s_{-r}) \text{ and } s_{-e}(s_r, s_{-r}).$$

Similarly, Bob computes

$$s_r(s_e, s_{-e}) \text{ and } s_{-r}(s_e, s_{-e}).$$

They share the common secret key as (s_{er}, s_{-er}).

Remark 1. The XTR [3] uses the characteristic sequences generated by an irreducible polynomial of the form $f(x) = x^3 - ax^2 + a^p x - 1$ over $\mathbb{F}_{p^2}$ with period $p^2 - p + 1$. Thus, XTR uses one characteristic sequence instead of a pair of reciprocal characteristic sequences, since in this case $s_{-k} = s_k^p$. Hence the two terms s_k and s_{-k} are dependent. For $q = p^2$, the two schemes have the same efficiency when they are applied to the DH key agreement protocol, because the GH-DH computes a pair of elements over $\mathbb{F}_{p^2}$ and shares a pair of elements over $\mathbb{F}_{p^2}$, while the XTR-DH computes one element over $\mathbb{F}_{p^2}$ and shares one element over $\mathbb{F}_{p^2}$.

3 The Approach

One approach to generating sequences of a given period is to randomly select fields and sequence polynomials and check to see if it has the desired period. However, determining the order of a sequence may be very difficult, and it may require many attempts before a good sequence is found. We give a more systematic approach to generating instances based on the following proposition (see [5] for a proof).

Proposition 1. *Let f be an irreducible polynomial of degree 3 over $GF(q)$ and t be a positive integer. The following are equivalent:*

1. *The sequence generated by f has period t.*
2. *t is the smallest integer such that f divides $x^t - 1$.*
3. *A root α of f has order t in the extension field $GF(q^3)$ of $GF(q)$ generated by f.*

Thus, if we can find an element of order $q^2 + q + 1$ in the extension field $GF(q^3)$, we can construct a polynomial whose sequence is of the desired period. Note that the multiplicative group of $GF(q^3)$ is cyclic. The following lemma helps us determine whether an element in a cyclic group has a given order.

Lemma 1. *Let G be a cyclic group of order n and let t be a number dividing n whose prime factorization is $t = p_1^{e_1} \cdots p_r^{e_r}$. Then an element $g \in G$ has order exactly t if and only if $g^t = 1_G$ and $g^{t/p_i} \neq 1_G$ for all $i = 1, \ldots, r$ where 1_G denotes the identity element of G.*

Thus, if we knew the factorization of $q^2 + q + 1$, we could easily determine whether or not an element has this order. The problem we immediately encounter is that the factorization of large numbers is a very difficult problem. One way to circumvent this problem is to choose primes p for which this factorization is much simpler.

4 Choosing "Good" Primes p

We define a prime p to be *good* if the factorization of q^2+q+1 is known where $q=p^2$. We have the following factorization

$$q^2+q+1 = p^4+p^2+1 = (p^2+p+1)(p^2-p+1)$$

Let $p^+ = p^2+p+1$ and $p^- = p^2-p+1$. Let us now derive conditions for when a prime l divides either p^+ or p^-.

First, observe that neither 2 nor p are divisors since q^2+q+1 is odd and congruent to 1 modulo p. Next, note that no prime l divides both p^+ and p^-, for then it would also have to divide $p^+ - p^- = 2p$.

Let us now consider the case $l=3$. If $p \equiv 1 \pmod 3$, then $p^+ \equiv 0 \pmod 3$. On the other hand, if $p \equiv 2 \pmod 3$, then $p^- \equiv 0 \pmod 3$. Thus, q^2+q+1 will always be divisible by 3.

For all other primes l, we see that l will divide p^+ (respectively p^-) if and only if p is a root of the polynomial x^2+x+1 (respectively x^2-x+1) in $\mathbb{F}_l$. Observe that any root of x^2+x+1 (respectively x^2-x+1) has order 3 (respectively order 6) in the multiplicative group $\mathbb{F}_l^*$. This will occur only if $l \equiv 1 \pmod 3$. The converse to this assertion, namely that if $l \equiv 1 \pmod 3$ then x^2+x+1 (respectively x^2-x+1) is reducible, is easily seen. Thus, the condition $l \equiv 1 \pmod 3$ is necessary for l to divide p^+ or p^-, and so we only need to consider small primes l of this type.

If $l \equiv 1 \pmod 3$, we can determine the roots of these polynomials over $\mathbb{F}_l$ using the quadratic formula. The roots of x^2+x+1 are $2^{-1}(-1 \pm \sqrt{-3})$, and the roots of x^2-x+1 are $2^{-1}(1 \pm \sqrt{-3})$, where the inverse is taken modulo l. Let $r = 2^{-1}(-1+\sqrt{-3})$ be one of the roots of x^2+x+1. Then, $-r-1$ is the other root. In addition, we see that $r+1$ and $-r$ are the roots of x^2-x+1. Hence, l divides p^+ if and only if $p \equiv r, -r-1 \pmod l$, while l divides p^- if and only if $p \equiv r+1, -r \pmod l$. Note that $r, -r-1, r+1, -r$ are easily computable given l, and independent of the value of p.

We now have a strategy for finding a *good* prime p. We select a bound B and a random prime p and attempt trial division of p^+ and p^- by all primes $< B$. We then perform a primality test on the remaining large factors of p^+ and p^-. If both are prime then we have found a desirable p. Otherwise we try again with another random p.

Note that we need not attempt trial division by those primes l for which $l \equiv 2 \pmod 3$. Moreover, we can determine if l divides by p^+ and p^- by simply checking if the much smaller value p matches one of $r, -r-1, r+1, -r$ modulo l. Since these numbers are independent of p, they can be precomputed once for all primes p to be tested. This enables us to determine divisibility by calculating p modulo l instead of working with the much larger numbers p^+ and p^-.

If desired, one also may use some more advanced factorization methods on p^+ and p^- such as Pollard's $(p-1)$-method [6] or the elliptic curve method [4]. Regardless, the goal is to obtain a value p for which the factorizations of p^+ and p^- are known.

5 Finding Elements of Order $q^2 + q + 1$

Now that we have a prime p for which the factorization of q^2+q+1 is known, we would like to use this information to find an element of this order. Suppose we have the factorization $q^2+q+1 = p_1^{e_1} \cdots p_r^{e_r}$. We know that $\mathbb{F}_{q^3}^*$ is a cyclic group of order $q^3 - 1$. Let $G \subseteq \mathbb{F}_{q^3}^*$ be the unique cyclic subgroup of order $q^2 + q + 1$. The map

$$\begin{aligned} \psi : \mathbb{F}_{q^3}^* &\rightarrow G \\ \alpha &\mapsto \alpha^{q-1} \end{aligned}$$

is a group homomorphism onto G. Thus, if $\alpha \in \mathbb{F}_{q^3}^*$ is selected at random, then $\beta = \alpha^{q-1}$ is a random element in G. We know that β has order dividing q^2+q+1. We can now use the lemma to determine if β is indeed an element of this order.

Now, an element $\beta \in G$ has order exactly q^2+q+1 if and only if it generates G. For a randomly chosen element, this happens with probability $\frac{\phi(q^2+q+1)}{q^2+q+1}$ where ϕ is the Euler ϕ-function. Given the factorization above, this works out to

$$\frac{\phi(q^2+q+1)}{q^2+q+1} = \frac{\phi(p_1^{e_1})}{p_1^{e_1}} \cdots \frac{\phi(p_r^{e_r})}{p_r^{e_r}} = \frac{p_1 - 1}{p_1} \cdots \frac{p_r - 1}{p_r}$$

If, for example we take $B = 2^{16} = 65536$, then in the worst case, this probability would work out to

$$\frac{2}{3} \cdot \frac{6}{7} \cdot \cdots \cdot \frac{65520}{65521} \cdot \frac{q^+ - 1}{q^+} \cdot \frac{q^- - 1}{q^-} > 0.28$$

where q^+ and q^- are the large leftover factors respectively of p^+ and p^-. Thus, one can find such an element β with very high probability after only a few tries.

6 Constructing the Sequence

Suppose that we have an element $\beta \in \mathbb{F}_{p^6}$ of order $p^4 + p^2 + 1$. Let

$$f(x) = (x - \beta)(x - \beta^{p^2})(x - \beta^{p^4}) = x^3 - ax^2 + bx - 1$$

where $a = \beta + \beta^{p^2} + \beta^{p^4}$ and $b = \beta^{-1} + \beta^{-p^2} + \beta^{-p^4}$. Then we have the following result [5].

Lemma 2. *f is an irreducible polynomials of degree 3 over $\mathbb{F}_{p^2}$.*

Corollary 1. *f generates a sequence of period $p^4 + p^2 + 1 = q^2 + q + 1$ over $\mathbb{F}_{p^2} = \mathbb{F}_q$.*

Proof. This follows immediately from the preceding lemma 2 and proposition 1. □

7 Obtaining a Representation for the Coefficients

There is one detail remaining. The representation that we currently have for a and b are as elements in $\mathbb{F}_{p^6}$. We need to have some sort of representation for them in $\mathbb{F}_{p^2}$.

7.1 A General Method

One method to do so is as follows. Suppose $g(x) = x^2 + c_1 x + c_0$ is an irreducible polynomial over $\mathbb{F}_p$ such that the degree 6 polynomial $h(x) = x^6 + c_1 x^3 + c_0$ is also irreducible over $\mathbb{F}_p$. Consider the field extensions to $\mathbb{F}_{p^2}$ and $\mathbb{F}_{p^6}$ given by these two respective polynomials. Then we have the injective field homomorphism

$$\begin{array}{ccc} \mathbb{F}_{p^2} & \to & \mathbb{F}_{p^6} \\ u_1 x + u_0 & \mapsto & u_1 x^3 + u_0 \end{array}$$

Suppose that we had used h as our representation of $\mathbb{F}_{p^6}$. Then a and b must be of the form $a = u_1 x^3 + u_0$ and $b = v_1 x^3 + v_0$ in $\mathbb{F}_{p^6}$. Thus, we have the explicit representation of the sequence over $\mathbb{F}_{p^2}$ as $a = u_1 x + u_0$ and $b = v_1 x + v_0$ where the extension to the field $\mathbb{F}_{p^2}$ is given by g.

This method will suffice if one is not constrained with regards to the extension polynomial to be used. One can simply search for a polynomial of the form given by h which is also irreducible, from which one obtains the irreducible polynomial g. In addition, this method will work if one has a specific extension polynomial $g(x) = x^2 + c_1 x + c_0$ in mind, as long as $h(x) = x^6 + c_1 x^3 + c_0$ is also irreducible over $\mathbb{F}_p$. Note that is not always true.

7.2 A Method for a Specific Polynomial Representation

Suppose that one would like to use a specific polynomial representation given by $g(x) = x^2 + c_1 x + c_0$. If $x^6 + c_1 x^3 + c_0$ were not irreducible over $\mathbb{F}_p$, then one could not use the method given in the previous subsection. This subsection lists another method for doing so.

First, choose an irreducible degree 3 polynomial $\hat{g}(y) = y^3 + d_2 y^2 + d_1 y + d_0$. We can extend to the field $\mathbb{F}_{p^2}$ by using the representation

$$\mathbb{F}_{p^2} = \frac{\mathbb{F}_p[x]}{(g(x))}$$

We can then consider $\hat{g}$ as a polynomial over $\mathbb{F}_{p^2}$ and extend the field once more. Note that since $\hat{g}$ is irreducible over $\mathbb{F}_p$ and its degree is coprime to that of g, it is also irreducible over $\mathbb{F}_{p^2}$. Thus we have the extension

$$\mathbb{F}_{p^6} = \frac{\mathbb{F}_{p^2}[y]}{(\hat{g}(y))}$$

Note that the subfield $\mathbb{F}_{p_2}$ corresponds to those elements with no y-term associated to it. Thus, it would be easy to obtain a and b using the representation of g.

The problem we encounter with this method is that it is somewhat tedious to do a double field extension. In fact, certain software packages such as NTL [7] allow single extensions but do not support multiple field extensions. It would be much simpler if we could use only a single field extension. To this end, we now show a method to interpolate the the polynomials g and $\hat{g}$ into an irreducible degree 6 polynomial h.

Let γ and η be roots of g and $\hat{g}_2$ respectively. Thus, we have that

$$g(x) = x^2 + c_1x + c_2 = (x - \gamma)(x - \gamma^p)$$

and

$$\hat{g}(y) = y^3 + d_2y^2 + d_1y + d_0 = (y - \eta)(y - \eta^p)(y - \eta^{p^2})$$

We construct the polynomial h to be the minimal polynomial of the element $\zeta = \gamma\eta$. Since $\gamma \in \mathbb{F}_{p^2}\backslash\mathbb{F}_p$ and $\eta \in \mathbb{F}_{p^3}\backslash\mathbb{F}_p$, we see that this polynomial must be of degree 6 and is explicitly given as

$$\begin{aligned}
h(z) &= z^6 + e_5z^5 + e_4z^4 + e_3z^3 + e_2z^2 + e_1z + e_0 \\
&= (z - \zeta)(z - \zeta^p)(z - \zeta^{p^2})(z - \zeta^{p^3})(z - \zeta^{p^4})(z - \zeta^{p^5}) \\
&= (z - \gamma\eta)(z - \gamma^p\eta^p)(z - \gamma\eta^{p^2})(z - \gamma^p\eta)(z - \gamma\eta^p)(z - \gamma^p\eta^{p^2})
\end{aligned}$$

where we have used the relations $\gamma^{p^2} = \gamma$ and $\eta^{p^3} = \eta$.

It turns out that we can derive the coefficients of h directly from the coefficients of g and $\hat{g}$. With some work, it is easily seen that we have the following relations

$$\begin{aligned}
e_5 &= -c_1d_2 \\
e_4 &= c_1^2d_1 + c_0d_2^2 - 2c_0d_1 \\
e_3 &= 3c_0c_1d_0 - c_1^3d_0 - c_0c_1d_1d_2 \\
e_2 &= c_0c_1^2d_0d_2 - 2c_0^2d_0d_2 + c_0^2d_1^2 \\
e_1 &= -c_0^2c_1d_0d_1 \\
e_0 &= c_0^3d_0^2
\end{aligned}$$

Elements in $\mathbb{F}_{p^6}$ in this polynomial representation have the form (replacing z with ζ)

$$\begin{aligned}
&u_0 + u_1\zeta + u_2\zeta^2 + u_3\zeta^3 + u_4\zeta^4 + u_5\zeta^5 \\
&= u_0 + u_1(\gamma\eta) + u_2(\gamma^2\eta^2) + u_3(\gamma^3\eta^3) + u_4(\gamma^4\eta^4) + u_5(\gamma^5\eta^5)
\end{aligned}$$

Using the relations $\gamma^2 = -c_1\gamma - c_2$ and $\eta^3 = -d_2\eta^2 - d_1\eta - d_0$, we can reduce to a representation of the form

$$v_0 + v_1\gamma + v_2\eta + v_3\gamma\eta + v_4\eta^2 + \gamma\eta^2$$

Note that the subfield $\mathbb{F}_{p^2}$ consists of those elements with no η-term. We can use this to determine a and b in the representation using g.

Example 1. Suppose $p \equiv 3 \pmod 4$. Then $g(x) = x^2 + 1$ is irreducible over $\mathbb{F}_p$. Let $\hat{g}(y) = y^3 - y - k$ be irreducible for some $k \in \mathbb{F}_p$. Then $h(z) = z^6 + 2z^4 + z^2 + k^2$. An element can be represented as

$$\begin{aligned}
&u_0 + u_1\zeta + u_2\zeta^2 + u_3\zeta^3 + u_4\zeta^4 + u_5\zeta^5 \\
&= u_0 + u_1(\gamma\eta) + u_2(\gamma^2\eta^2) + u_3(\gamma^3\eta^3) + u_4(\gamma^4\eta^4) + u_5(\gamma^5\eta^5) \\
&= u_0 + k(u_5 - u_3)\gamma + ku_4\eta + (u_1 - u_3 - ku_5)\gamma\eta + (u_4 - u_2)\eta^2 + ka_5\gamma\eta^2
\end{aligned}$$

If this element were in the subfield $\mathbb{F}_{p^2}$, then the coefficients of the terms with an η must be 0. This yields the relations $u_2 = u_4 = u_5 = 0$ and $u_1 = u_3$. Thus, such an element can be represented as $u_0 - ku_1x$ in the field $\mathbb{F}_{p^2}$ where $g(x) = x^2 + 1$ was used as the extension polynomial.

Example 2. Suppose $p \equiv 2 \pmod 3$. Then $g(x) = x^2 + x + 1$ is irreducible over $\mathbb{F}_p$. Let $\hat{g}(y) = y^3 - y - k$ be irreducible for some $k \in \mathbb{F}_p$. Then $h(z) = z^6 + z^4 - 2kz^3 + z^2 - kz + k^2$. An element can be represented as

$$\begin{aligned}
&u_0 + u_1\zeta + u_2\zeta^2 + u_3\zeta^3 + u_4\zeta^4 + u_5\zeta^5 \\
&= u_0 + u_1(\gamma\eta) + u_2(\gamma^2\eta^2) + u_3(\gamma^3\eta^3) + u_4(\gamma^4\eta^4) + u_5(\gamma^5\eta^5) \\
&= u_0 + k(u_3 - u_5) - ku_5\gamma + (u_3 - u_5)\eta + (u_1 - u_5 + ku_4)\gamma\eta \\
&\quad + (-u_2 - ku_5)\eta^2 + (u_4 - u_2 - ku_5)\gamma\eta^2
\end{aligned}$$

If this element were in the subfield $\mathbb{F}_{p^2}$, then the coefficients of the terms with an η must be 0. This yields the relations $u_4 = 0$ and $u_1 = u_3 = u_5 = -k^{-1}u_2$. Thus, such an element can be represented as $u_0 - ku_1x$ in the field $\mathbb{F}_{p^2}$ where $g(x) = x^2 + x + 1$ was used as the extension polynomial.

8 The Algorithm

The method is summarized here in algorithmic form.

Input (bit size b, bound $B > 3$)

<u>Precomputation:</u>

for each prime $l \equiv 1 \pmod 3$, $3 < l < B$
  compute $r = 2^{-1}(1 + \sqrt{-3}) \pmod l$
  store the pair (l, r) in table A
end for

Prime Generation:

```
loop
    generate a random prime p of b bits
    calculate p+ and p-
    set q+ = p+ and q- = p-
    if p ≡ 1 (mod 3)
        let s be the highest power of 3 dividing q+
        divide q+ by 3^s
        store (l, s) in table B
    else
        let s be the highest power of 3 dividing q-
        divide q- by 3^s
        store (l, s) in table C
    end if
    for each entry (l, r) in table A
        compute m = p (mod l)
        if m = r or m = l - r - 1
            let s be the highest power of l dividing q+
            divide q+ by l^s
            store (l, s) in table B
        else if m = r + 1 or m = l - r
            let s be the highest power of l dividing q-
            divide q- by l^s
            store (l, s) in table C
        end if
    end for
    do primality tests on both q+ and q-
    if both q+ and q- are prime
        exit the loop
    else
        clear tables B and C
    end if
    return to the top of the loop
end loop
```

Constructing the Sequence:

```
select an irreducible polynomial h of degree 6 over F_p using one of the methods in section 7
loop
    choose a random element α ∈ F_{p^6}
    compute β = α^(p^2 - 1)
    for i = 3, q+, q-, each prime l in tables B and C
        if β^((p^4 + p^2 + 1)/i) = 1
            return to top of loop
        end if
```

end for
exit loop
end loop
compute $a' = \beta + \beta^{p^2} + \beta^{p^4}$
compute $b' = \beta^{-1} + \beta^{-p^2} + \beta^{-p^4}$
derive the irreducible degree 2 polynomial g from h using the appropriate method from section 7
derive a and b from a' and b' respectively using the appropriate method from section 7

Output (p, g, a, b)

A Implementation and Timing Analysis

The algorithm listed in the previous section was implemented in C++ on a UNIX server using the NTL [7] number theory library. The dominant step of the algorithm was, by far, prime generation. As a result, timing analysis was performed on this portion of the algorithm with the results listed in table 1 and table 2.

The bounds $B = 2^{10}$ and $B = 2^{16}$ were both tested. 10 instances were generated for each bound and for each bit size from 160 to 320 by 8 bits. The number of primes searched before the candidate was found, the CPU time, and the bit sizes of the largest prime factors q^+ and q^- respectively of p^+ and p^- were recorded. The class of instances with bound $B = 2^{16}$ were, on average generated much faster than those with bound $B = 2^{10}$, especially for the larger bit sizes. The bit sizes of q^+ and q^- were only marginally larger with the bound $B = 2^{10}$.

In addition, attempts were made to generate instances with the bound $B = 4$. This was attempted for bit sizes 160 to 240 by 8. The average CPU time using this bound was substantially longer than with the other two bounds. Thus, for some bit sizes, fewer than 10 instances were generated. Results for this bound are listed in table 3.

B Example Instances

This section lists some example instances.

Example 3. The prime p listed here has 160 bits.
$p = 1276593311082943972800140646397807976959837132709$
$p^+ = 1629690481901714162735730680725186288280728823955302744324479689642812431700906503271994314811391$
$p^- = (3)5432301606339047209119102269083954294269096079842498525674379338990707168027036291060248801819991$
$g(x) = x^2 + x + 1$
$a = [852223667913003644390015513849147072549735623 35]x + [1209115664825072234387309339396575750110393685169]$

Table 1. Timing results for prime generation with bound $B = 2^{10}$.

bits	# searched	time (sec)	q^+	q^-
160	139.9	19	309.5	310.2
168	529.5	79.6	327.5	326.8
176	318.9	47.6	342.4	343
184	184.9	33.9	358.7	358.3
192	388.2	90	375.9	374.6
200	441.5	90.6	391.7	390.9
208	432.2	93.5	407	406.1
216	395.5	127.1	420.3	426.4
224	445	117.4	439.7	441
232	295.9	83.4	455.7	457
240	418.5	118.9	467.8	472.2
248	847.8	304	488.1	489.3
256	1098.4	396.8	499.7	503.5
264	582.2	235.2	516.4	518.6
272	796.4	350.9	535.3	533.5
280	1233.2	579	550.8	552.9
288	1299.4	645.6	567.8	563.5
296	1144.1	590.1	584.5	581.1
304	1320.8	781.4	595	596.8
312	467.6	288.8	615.4	614.2
320	885.3	585.3	634.1	634.2

Table 2. Timing results for prime generation with bound $B = 2^{16}$.

bits	# searched	time (sec)	q^+	q^-
160	106.3	19.8	307.6	306.3
168	108.2	21.8	322.2	328.1
176	115.4	23.4	335.6	334.5
184	78.9	18.9	354.6	353
192	221.4	57.9	375.2	371.7
200	162.2	43	388.4	387.7
208	236.8	66.7	397.7	398.4
216	240	76.8	421.1	399.2
224	158.9	53.6	437.9	427.2
232	224	78.3	444	448.6
240	106.5	41.1	460.8	468.3
248	433	184.2	481.6	479.1
256	327.4	141.8	493.7	498.9
264	160.7	75.3	510.7	511.9
272	331.8	186.5	533	530
280	300.9	162.4	544	547.9
288	405	230.7	560.8	560.2
296	803	476.9	584.2	575
304	604	398.7	592.5	592.6
312	291.8	202.9	611.1	608.2
320	319.4	264.8	624.3	625.7

Table 3. Timing results for prime generation with bound $B = 4$.

bits	# searched	time (sec)	q^+	q^-	# instances
160	3721.5	383.5	319.5	319.5	2
168	11727.29	1383.29	335	334.29	7
176	17520.5	2114.5	350	352	2
184	8214.8	1215.6	366.6	367.3	10
192	23773	3751	384	383	1
200	17927	2918.5	400	398	2
208	13146	2203	413	415	1
216	21012	4238	431	430	1
224	6769.5	1412	447	446.5	2
236	10056	2254	462.5	463	2
240	30651	6889	477	479	1

$b = [246868582389120965340698690747362673995248240017]x$
$\quad + [893048047568985860793458252220232059855756667683]$

Example 4. The prime p listed here has 160 bits.
$p = 1353081569040243787002953026589849378107407355807$
$p^+ = (3)6102765774921360046408448466984410943175577269572070036269642 6$
$\quad 1429092268344297821850519634659019$
$p^- = 18308297324764080139225345400953232829526731808689148477428122967$
$\quad 1327089897971376679534408926 5443$
$g(x) = x^2 + 1$
$a = [965913929992835996699498327367567768167816904081]x$
$\quad + [114439484991500531161708001866868463982927203984]$
$b = [499746686903428250077058835004207585322076077588]x$
$\quad + [241440714372014101653045391345358648608519166355]$

References

1. G. Gong and L. Harn, "A new approach on public-key distribution", *ChinaCRYPT '98*, pp 50-55, May, 1998, China.
2. G. Gong and L. Harn, "Public-key cryptosystems based on cubic finite field extensions", *IEEE IT* vol 45, no 7, pp 2601-2605, Nov. 1999.
3. A. K. Lenstra and E. R. Verheul, "The XTR public key system", *Advances in Cryptology, Proceedings of Crypto'2000*, pp. 1-19, Lecture Notes in Computer Science, Vol. 1880, Springer-Verlag, 2000.
4. H. W. Lenstra Jr., "Factoring Integers with Elliptic Curves", *Ann. of Math.* vol 126, no 2, pp 649-673, 1987.
5. R. Lidl and H. Niederreiter, *Finite Fields*, Addison-Wesley Publishing Company, Reading, MA, 1983.
6. J. M. Pollard, "Theorems on Factorization and Primality Testing", *Proc. Cambridge Philos. Soc.* vol 76, pp 521-528, 1974.
7. V. Shoup, "NTL: A Library for doing Number Theory", *http://shoup.net/ntl*.