Proceedings of the 5th WSEAS Int. Conf. on Electronics, Hardware, Wireless and Optical Communications, Madrid, Spain, February 15-17, 2006 (pp187-192)

Special Polynomial Families for Generating More Suitable Pairing-Friendly Elliptic Curves

Pu Duan, Shi Cui, Choong Wah Chan
School of Electrical and Electronic Engineering
Nanyang Technological University
S2, B3b-10, Workstation Resource Lab
Singapore

Abstract: - Constructing non-supersingular elliptic curves for pairing-based cryptosystems have attracted much attention in recent years. The best previous technique builds curves with $\rho = \lg(q) / \lg(r) \approx 1$ ($k = 12$) and $\rho = \lg(q) / \lg(r) \approx 1.25$ ($k = 24$). When $k > 12$, most of the previous works address the question by representing $r(x)$ as a cyclotomic polynomial. In this paper, we propose a method to find more pairing-friendly elliptic curves by various forms of irreducible polynomial $r(x)$. In addition, we propose a equation to illustrate how to obtain small values of ρ by choosing appropriate forms of discriminant D and trace t. Numerous parameters of certain pairing-friendly elliptic curves are presented with support for the theoretical conclusions.

Key-Words: - pairing-friendly elliptic curves, special polynomial families, cyclotomic polynomials

1 Introduction

After the propositions of identity-based encryption scheme [12] and short signature scheme [13], paring-based cryptography has attracted significant attention in modern public-key cryptography. Over pairing-based cryptosystems, Elliptic Curve Discrete Logarithm Problem (ECDLP) on supersingular elliptic curves is reduced to Discrete Logarithm Problem (DLP) over an extension field by Weil Pairing [10] or Tate Paring [15]. Although supersingular elliptic curves provides high efficiency for pairing-based cryptosystems [19, 20], researchers have explored other forms of elliptic curves (e.g. non-supersingular elliptic curves) since supersingular elliptic curves only can be built when embedding degree $k \leq 6$ [11].

In 2001, Miyaji, Nakabayashi and Takano [8] first proposed a method to find suitable non-supersingular elliptic curves for pairing-based cryptosystems. They discussed the problem from the point of view of tract t. Scott and Barreto [1] extended the method of Miyaji et al. and found more suitable non-supersingular elliptic curves when $k \in [3, 4, 6]$. Gallbraith, Mckee and Valenca [3] summarized the methods proposed by the early researchers and presented some appropriate families of group orders for such elliptic curves when embedding degree $k \leq 6$. Duan, Cui and Chan [5] extended the work of Gallbraith et al. by proposing the idea of effective polynomial families of pairing-friendly elliptic curves.

For larger values of embedding degree k, Brezing and Weng proposed an efficient method to find these curves [7]. They used $t - 1$ as a kth root of unity modulo prime r. They generated the curves with the best performance so far as $\lg(q) / \lg(r) = 1.25$ ($k = 24$). Barreto, Lynn and Scott [21] also proposed an efficient algorithm as for finding the suitable polynomial families of pairing-friendly elliptic curves when the value of k is large. They presented several polynomial families in their paper, which can be implemented to generate plenty of elliptic curves. For arbitrary values of embedding degree k, Dupont, Enge and Morain [16] proposed another method for finding the suitable curves. Most of the curves they found had $\lg(q) / \lg(r) \approx 2$. Barreto and Naehrig [17] generated non-supersingular elliptic curves with $\lg(q) / \lg(r) = 1$ when embedding degree $k = 12$. They presented the best curves with prime group order known so far. Their work was generated by a special polynomial family of $q(x)$, $t(x)$ and $r(x)$, where $4q(x) - t^2(x)$ can be factorized as one square polynomial multiplying with one constant number. In the most recent work, Murphy and Fitzpatrick [4] extended the work of Brezing et al. [7] and generated pairing-friendly elliptic curves over prime fields with discriminant $D > 4$ for arbitrary values of k.

In this paper we propose a different method for finding more pairing-friendly elliptic curves.

Compared to the previous works, the irreducible polynomial r(x) is not restricted as a standard cyclotomic polynomial in our method. More pairing-friendly elliptic curves are found by various representations of r(x). We also illustrate the relation to obtain small values of ρ by choosing appropriate forms of discriminant D and trace t.

This paper is organized as the following sections. In Sections 2 we give a description of the mathematics background. In Section 3 we present our method and discuss the difference when it is compared with the previous works. In Section 4 certain special polynomial families of pairing-friendly elliptic curves with various forms of r(x) are presented. We draw the conclusion in Section 5. The parameters of certain pairing-friendly elliptic curves, based on the proposed polynomial families, are presented in Appendix.

2 Mathematics Background

To find suitable elliptic curves for pairing-based cryptosystems, we need to solve certain equations. Assume the cofactor h is an integer, r is the order of a point as a big prime number and t is the trace of an elliptic curve. We want to find an elliptic curve over $\mathbf{F}_q$, where q = p is a prime number (we only consider the prime fields in this paper). ECDLP on such elliptic curves can be reduced to DLP over $\mathbf{F}_{q^k}$, where k is the smallest integer satisfying certain conditions, defined as the embedding degree [1]. The following equations determine whether such an elliptic curve exists or not. Details of elliptic curves for pairing-based cryptosystems can be found in [1, 21].

In a strict sense, to find the suitable elliptic curves for pairing-based cryptosystems [10], we need

$$r \mid q^k - 1 \quad (1)$$

However, under a mild condition [6], we just consider q as a kth root of unity modulo r [7]. Meanwhile, since k is the smallest integer satisfying $r \mid q^k - 1$, equation (1) should be presented as $r \mid q^k - 1$ and $q^i - 1$ is not divisible by r when $0 < i < k$. From [14] we have

$$dr = \Phi_k(q) \quad (2)$$

where d is an integer and $\Phi_k(q)$ is a cyclotomic polynomial of q with embedding degree k and

$$d'r \neq \Phi_i(q),\ 0 < i < k \quad (3)$$

Besides these conditions, we need

$$hr = q + 1 - t \quad (4)$$

where h is an integer. Combining equation (2) and (4) together, we obtain

$$sr = \Phi_k(t - 1) \quad (5)$$

where s is also an integer [1]. Since k is the smallest integer, we have

$$s'r \neq \Phi_i(t - 1),\ 0 < i < k \quad (6)$$

By Hasse's bound we have

$$|t| \leq 2q^{1/2} \quad (7)$$

With all the above equations, we compute the elliptic curve by solving

$$DV^2 = 4q - t^2 \quad (8)$$

In equation (8) D is chosen by certain conditions [2].

All the above equations aim for finding suitable elliptic curves for pairing-based cryptosystems in integer fields. But it is impossible to search the whole integer fields to obtain the suitable solutions. We should transfer the problem into polynomial fields. When analyzing in polynomial fields, we assume q, t, r, h, d, s, D and V as q(x), t(x), r(x), h(x), d(x), s(x), D(x) and V(x). Duan et al. [5] proposed a lemma which illustrates the fact that in polynomial fields, equation (2) and (5) are already both sufficient and necessary conditions. Thus for finding pairing-friendly elliptic curves in polynomial fields, only equations (2, 4, 5, 7, 8) are required and they can be rewritten as:

$$d(x)r(x) = \Phi_k(q(x)) \quad (9)$$

$$h(x)r(x) = q(x) + 1 - t(x) \quad (10)$$

$$s(x)r(x) = \Phi_k(t(x) - 1) \quad (11)$$

$$|t(x)| < 2q(x)^{1/2} \quad (12)$$

$$D(x)V(x)^2 = 4q(x) - t^2(x) \quad (13)$$

How to build pairing-friendly elliptic curves by finding polynomial families satisfying equation (9) to (13) were presented in [1, 3, 5, 8, 17]. Most of the works concentrated on the cases when embedding degree $k \leq 6$. Only one special polynomial family was found by Barreto et al. [17] when k = 12, which built the best curves with prime group order known so far.

For larger values of k, the polynomial families of q(x), t(x) and r(x) will not satisfy all the conditions as equations (9) to (13). Only some of the parameters will maintain the polynomial relations and the other ones will only be valid for certain x as x_0. Brezing and Weng [7] proposed a method to find these curves. In their method, t(x) and r(x) will satisfy equation (11) by representing t(x) – 1 as a kth root of unity modulo r(x) in polynomial fields. The irreducible polynomial r(x) is always set as a cyclotomic polynomial. q and DV^2 will not have the polynomial relations. They can not be represented as polynomials in cyclotomic fields. But all the parameters are satisfying equations (9) - (13) for a specific x_0. Barreto, Lynn and Scott [21] also proposed a similar algorithm. Their method found the suitable curves by implementing certain polynomial families of pairing-friendly elliptic curves when embedding degree k is arbitrary. In their

work, r(x) was also fixed as a cyclotomic polynomial and t(x) was fixed as x + 1.

In the next section, we will present a new method for finding more pairing-friendly elliptic curves with arbitrary embedding degree k by some special polynomial families. The new method allows r(x) to be an irreducible polynomial with different forms.

3 A New Method for Producing More Pairing - Friendly Elliptic Curves with Special Polynomial Families

By the algorithms presented in [1, 3, 5, 8, 17], polynomial families of q(x), t(x) and r(x) are implemented to generate various pairing-friendly elliptic curves by choosing different values of x. But when embedding degree k > 12, polynomial families are hard to be found satisfying all the pairing-friendly conditions (equation (9) to (13)). Then there is a possibility that only parts of the parameters maintain the polynomial relations while the other ones are only valid for certain values of x as x_0. Thus different approaches should be implemented for finding these effective polynomial families. We will analyze the question in the following paragraphs.

First we assume that parameters r and t maintain the pairing-friendly conditions in polynomial fields; but parameters q, D and V do not have the pairing-friendly conditions in polynomial forms. All the conditions are satisfied only for certain values of x as x_0 is given to all the parameters. For r and t we have

$$s(x)r(x) = \Phi_k(t(x) - 1)$$

This can be viewed as

$$r(x) \mid \Phi_k(t(x) - 1) \quad (14)$$

Represented in polynomial fields, for a specific x_0, equation (13) can be rewritten as

$$DV^2(x_0) = 4h(x_0)r(x_0) - (t(x_0) - 2)^2 \quad (15)$$

Dividing D from both sides of equation (15) we have

$$V^2(x_0) = [4h(x_0)r(x_0) / D] - [t(x_0) - 2]^2/D \quad (16)$$

Assuming $[t(x_0) - 2]^2 \mid 4Dh(x_0)$, equation (16) can be rewritten as

$$V^2(x_0) = \{[t(x_0) - 2]^2 / D^2\}\{[4Dh(x_0)r(x_0) / (t(x_0) - 2)^2] - D\} \quad (17)$$

Here we use a technique to consider $4Dh(x_0) / (t(x_0) - 2)^2$ as a polynomial h'(x) for certain x_0. This means for a specific x_0, $4Dh(x_0)$ is divided by $[t(x_0) - 2]^2$ and it can be represented in polynomial fields as a polynomial h'(x). Then equation (17) is represented as

$$V^2(x_0) = \{[t(x_0) - 2]^2 / D^2\}\{h'(x)r(x) - D\} \quad (18)$$

Thus if h'(x)r(x) – D can be regarded as a square polynomial $S^2(x)$, all parameters in equation (18) have square forms. Assuming $h'(x)r(x) - D = S^2(x)$, for any suitable x_0, equation (18) is written as

$$V^2(x_0) = \{[t(x_0) - 2]^2 / D^2\}S^2(x) \quad (19)$$

This equation represents a modified polynomial family. For the specific x_0, we have

$$DV^2(x_0) = \{[t(x_0) - 2]^2 /D\}S^2(x_0) \quad (20)$$

Representing equation (20) into equation (8), we obtain

$$q = [t^2(x_0) + DV^2(x_0)] / 4 \quad (21)$$

We choose a suitable x_0 to satisfy that $r(x_0)$ is a prime integer. Then for the specific x_0, if $q = [t^2(x_0) + DV^2(x_0)] / 4$ is also a prime integer, we find all the suitable parameters with satisfaction to a pairing-friendly elliptic curve.

We must point out that Barreto, Lynn and Scott [21] proposed a similar method as the above approach. In their work, several polynomial families were presented for finding suitable elliptic curves with arbitrary values of embedding degree k. But r(x) was fixed as a standard cyclotomic polynomial and t(x) was fixed as x + 1 in their paper. In our method, r(x) are taken as different irreducible polynomials satisfying $r(x) \mid \Phi_k(t(x) - 1)$. More pairing-friendly elliptic curves exist when r(x) is not presented as a standard cyclotomic polynomial.

The main idea of our method can be presented as the following procedures. First we choose a specific r(x) and trace polynomial t(x) with $r(x) \mid \Phi_k(t(x) - 1)$. Here we should consider r(x) as any irreducible polynomials. Then after choosing a suitable discriminant D, we find polynomial families h'(x) which satisfies $h'(x)r(x) - D = S^2(x)$. In the following steps, we choose a suitable x_0 when $r(x_0)$ is a prime integer and test whether $q = \{t^2(x_0) + [(t(x_0) - 2)^2 / D]S(x_0)\} / 4$ is also a prime integer. Is q satisfies the condition, we have found the suitable parameters of a pairing-friendly elliptic curve. In our method, $4Dh(x_0) / (t(x_0) - 2)^2 = h'(x)$ is a hidden condition since we represent h'(x) as a polynomial.

Based on the above analysis, we propose an algorithm for finding the suitable pairing-friendly elliptic curves.

Algorithm 1

Input: embedding degree k, $q^k \geq 2^{1024}$ and $r \geq 2^{160}$

Output: x_0, $q(x_0)$, $t(x_0)$, $r(x_0)$, $DV^2(x_0)$

1. Choose an irreducible polynomial r(x).
2. Compute trace polynomial t(x) by $\Phi_k(t(x) - 1) \equiv 0 \bmod r(x)$.
3. Choose a polynomial family h'(x) and a suitable discriminant D with $h'(x)r(x) - D = S^2(x)$ where $S^2(x)$ is a square

polynomial.

4. Find a specific x_0 when $r(x_0)$ is a prime integer and $q = \{t^2(x_0) + S^2(x_0) [(t(x_0) - 2)^2 / D] \} / 4$ is also a prime integer.
5. Output x_0, $q(x_0)$, $t(x_0)$, $r(x_0)$, $DV^2(x_0)$.
6. Establish the elliptic curve by CM method with the above parameters.
7. If no suitable parameters are found, repeat from step 1.

When finding the suitable polynomials t(x) with arbitrary forms of r(x), a much simpler way is to choose an arbitrary t(x) first and then factorize $\Phi_k(t(x) - 1)$. The meaningful factor can be regarded as a valid r(x). This simple technique allows us to find more pairing-friendly elliptic curves by various forms of r(x).

Because the key procedure of the new method is to find special polynomial families h'(x), r(x) and $S^2(x)$, in the next section we will list some polynomial families with different embedding degree k, ρ (lg(q) / lg(r)) and r(x).

4 Special Polynomial Families for Producing More Pairing-Friendly Elliptic Curves

In this section we will present some special polynomial families obtained by our method. These families can be used to generate more pairing-friendly elliptic curves with different forms of r(x), small values of ρ and arbitrary values of embedding degree k.

Although Barreto et al. [21] proposed a similar deduction, they did not explain how elliptic curves with small ρ can be found by different forms of h'(x), t(x) and r(x). The new method indicates that the value of ρ is related to the choice of r(x), t(x) and h'(x). It is because $\rho = \lg(q) / \lg(r) = \text{degree}(q(x)) / \text{degree}(r(x))$. Since $DV^2(x_0) = \{[t(x_0) - 2]^2 / D\}\{h'(x)r(x) - D\}$, we have $\text{degree}(q(x)) = \text{degree}(DV^2(x)) \approx 2\text{degree}(t(x)) + \text{degree}(h'(x)) + \text{degree}(r(x))$. Thus the value of $\rho = \text{degree}(q(x)) / \text{degree}(r(x)) = [2\text{degree}(t(x)) + \text{degree}(h'(x)) + \text{degree}(r(x))] / \text{degree}(r(x)) = 1 + [2\text{degree}(t(x)) + \text{degree}(h'(x))] / \text{degree}(r(x))$. It is to say that ρ will always be larger than 1. This can also be deduced from the conditions used in our method. Since we assume $[t(x_0) - 2]^2 \mid 4Dh(x_0)$ in the algorithm, h(x) will be a constant integer as h when ρ = 1. Then $[t(x_0) - 2]^2 \mid 4Dh$ will not be satisfied since $|t^2(x_0)| > 4Dh$. When the degree of h'(x) is 0 (h'(x) is a constant number), ρ has the smallest values as $1 + 2\text{degree}(t(x)) / \text{degree}(r(x))$. Thus for finding ρ close to 1, h'(x) should be chosen as a constant number and t(x) should be chosen with the smallest degrees.

Brezing et al. [7] successfully found pairing-friendly elliptic curves with arbitrary embedding degree. Similar work was achieved by Barreto et al. [21]. But the limitation of their work was that r(x) was only represented as the standard cyclotomic polynomial. They did not provide any explanations to the circumstances when r(x) was not a cyclotomic polynomial. The work of Murphy and Fitzpatrick [4] was also based on the standard representations of r(x) as $\Phi_k(x)$.

Our method ignores the limitation imposed on the forms of r(x) since we only need to find h'(x) and D with $h'(x)r(x) - D = S^2(x)$. For this point, r(x) can be any irreducible polynomials satisfying $r(x) \mid \Phi_k(t(x) - 1)$. This allows us to find much more elliptic curves by various representations of r(x).

Table 1 tabulates some special polynomial families with different r(x) (including the case when r(x) is a cyclotomic polynomial) when k is taken different values from 8 to 32. The trace t(x) is taken with degree as small as possible to obtain desired values of ρ. In Appendix, we generate the parameters of certain pairing-friendly elliptic curves when k = 14, 15, 28 by the polynomial families of Table 1.

k	r(x)	h'(x)	t(x)	D	ρ
8	$x^{16} - x^{12} + x^8 - x^4 + 1$	$x^4 + 1$	$x^5 + 1$	1	1.87
8	$x^{16} - 4x^{14} + 9x^{12} - 12x^{10} + 10x^8 - 4x^6 + 1$	$x^4 + 1$	$x^5 - x^3$	1	1.87
14	$x^{12} + x^{11} - x^9 - x^8 + x^6 + x + 1$	$4x^2 - 4x + 4$	$x^3 + 1$	3	1.67
15	$81x^8 - 81x^7 + 54x^6 - 27x^5 + 9x^4 - 9x^3 + 6x^2 - 3x + 1$	$36x^2 + 36x + 12$	$-3x^2 +$	3	1.75
16	$x^{32} - x^{24} + x^{16} - x^8 + 1$	$x^8 + 1$	$x^5 + 1$	1	1.56
28	$x^{24} + x^{22} - x^{18} - x^{16} + x^{12} - x^8 - x^6 + x^2 + 1$	$4x^4 - 4x^2 + 4$	$x^3 + 1$	3	1.42
32	$x^{64} - x^{48} + x^{32} - x^{16} + 1$	$x^{16} + 1$	$x^5 + 1$	1	1.41

Table 1: More special polynomial families with different r(x)

When the irreducible polynomial r(x) is not limited as a cyclotomic polynomial, more values of the discriminant D will be suitable for generating pairing-friendly elliptic curves. Appendix presents parameters of curves with D = 3 when embedding degree k = 14, 15, 28. Such curves and their related polynomial families in Table 1 are not proposed by any relative works before. These new polynomial families will be implemented for finding much more pairing-friendly elliptic curves. It is no way to list all the special polynomial families with various values of embedding degree k.

In fact, when r is allowed to contain a small factor s as r = s × n (n is a prime larger than 2^{160}), more suitable elliptic curves can be found. The same technique has been used in [1] when embedding degree k ≤ 6. When r = s × n, n should be a large prime bigger than 2^{160} [9] and the cofactor h will be multiplied with a small factor s. Brezing et al. [7] and Barreto et al. [21] only implemented r as a large prime in their methods. By our method it is easy to find that the condition of prime r(x) can be loosed to r = s × n without effecting the values of ρ heavily. Thus more elliptic curves different with the previous works are found in this paper. The value of ρ will not increase much if s is carefully chosen. The simplest situation is that r(x) = sr'(x), where s is a small integer and r'(x) is an irreducible polynomial. In such circumstances, more suitable polynomial families for pairing-friendly elliptic curves are found with different k. Table 2 presents two examples of such polynomial families when k = 12, 14. In Appendix, we generate the parameters of certain elliptic curves by the following polynomial families.

k	r'(x)	s	t(x)
12	$2197x^4 - 1352x^3 + 299x^2 - 28x + 1$	13	13x – 1
14	$20511149x^6 - 30413083x^5 + 18803919x^4 - 6205739x^3 + 1153069x^2 - 114381x + 4733$	19	29x – 6

Table 2: More polynomial families with r(x) = sr'(x)

5 Conclusion

In this paper, we propose a new method to find more pairing-friendly elliptic curves with arbitrary embedding degree k by certain special polynomial families. This method allows us to obtain new families of pairing-friendly elliptic curves by representing r(x) with various forms. In addition, we propose the technique to let prime r contain a small factor s for finding more pairing-friendly elliptic curves. Numerous parameters of new pairing-friendly elliptic curves are found with the proposed method.

References:

[1] M. Scott and P. S. L. M. Barreto. Generating more MNT elliptic curves. Cryptology ePrint Archive, Report 2004/058, 2004.

[2] IEEE Computer Society, New York, USA. IEEE Standard Specifications for Public Key Cryptography-IEEE Std 1363-2000, 2000.

[3] S. D. Galbraith, J. Mckee and P. Valenca. Ordinary abelian varieties having small embedding degree. Cryptology ePrint Archive, Report 2004/365, 2004.

[4] A. Murphy and N. Fitzpatrick. Elliptic curves for pairing applications. Cryptology ePrint Archive, Report 2005/302, 2005.

[5] P. Duan, S. Cui and C. W. Chan. Effective polynomial families for generating more pairing-friendly elliptic curves. Cryptology ePrint Archive, Report 2005/236, 2005.

[6]R. Balasubramanian and N. Koblitz. The improbability that an elliptic curve has subexponential discrete log problem under the Menezes-Okamoto-Vanstone algorithm. Journal of Cryptology, vol. 11, pp. 141-145, 1998.

[7] F. Brezing and A. Weng. Elliptic curves suitable for pairing based cryptography. Cryptology ePrint Archive, Report 2003/143, 2003.

[8] A. Miyaji, M. Nakabayashi, and S. Takano. New explicit conditions of elliptic curve traces for FR-reduction. IEICE Transactions on Fundamentals, E84-A(5):1234-1243, 2001.

[9] A. M. Odlyzko. Discrete logarithms: the past and the future. Design, Codes and Cryptography, 19:129-145, 2000.

[10] A. Menezes, T. Okamoto, and S. Vanstone. Reducing elliptic curve logarithms to logarithms in a finite field. Proc.22nd Annual ACM Symposium on the Theory of Computing, pp. 80-89, 1991.

[11]D. Page, N. P. Smart and F. Vercauteren. A comparison of MNT curves and supersingular curves. Cryptology ePrint Archive, Report 2004/165, 2004.

[12] D. Boneh and M. Franklin. Identity based encryption from the Weil pairing. SIAM Journal. of Computing, vol. 32, no.3, pp. 586-615, 2003.

[13] D. Boneh, B. Lynn and H. Shacham. Short signatures from the Weil pairing. Advances in Cryptology – Asiacrypt'2001, volume 2248 of Lecture Notes in Computer Science, page 514-532, Springer-Verlag, 2002.

[14]P. S. L. M. Barreto, B. Lynn, and M. Scott. Constructing elliptic curves with prescribed embedding degrees. In Security in Communication Networks – SCN'2002, volume 2576 of Lecture Notes in Computer Science, pages 263 – 273. Springer-Verlag, 2002.

[15] G. Frey, M. Muller and H. G Ruck. The Tate Pairing and the Discrete Logarithm Applied to Elliptic Curve Cryptosystems. IEEE Transactions on Information Theory, Vol 45, 1999.

[16] R. Dupont, A. Enge, and F. Morain. Building curves with arbitrary small MOV degree over finite prime fields. Journal of Cryptology, 18(2): 79-89, 2005.

[17] P. S. L. M. Barreto and M. Naehrig. Pairing-Friendly Elliptic Curves of Prime Order. Cryptology ePrint Archive, Report 2005/133, 2005.

[18]N. Koblitz and A. Menezes. Pairing-based cryptography at high security levels. Cryptography ePrint Archive, Report 2005/076, 2005.

[19]S. Galbraith, K. Harrison and D. Soldera. Implementing the Tate pairing. In Algorithm Number Theory Symposium – ANTS V, volume 2369 of

Lecture Notes in Computer Science, pages 324 – 337. Springer – Verlag, 2002.

[20] P. S. L. M. Barreto, H. Y. Kim, B. Lynn and M. Scott. Efficient algorithms for pairing-based cryptosystems. In Advances in Cryptology – Crypto' 2002, volume 2442 of Lecture Notes in Computer Science, pages 354-368. Springer-Verlag, 2002.

[21] P. S. L. M. Barreto, B. Lynn and M. Scott. Efficient implementation of pairing-based cryptosystems. Journal of Cryptology, 17(4): 321 – 334, 2004.

Appendix

(1) k = 14
$r(x) = x^{12} + x^{11} – x^9 – x^8 + x^6 – x^4 – x^3 + x + 1$, $t(x) = x^3 + 1$, $h'(x) = 4x^2 – 4x + 4$, D = 3
x = 15232
r = 155995361021362964986617313981716948403826318130049 (167 bits)
t = 3534034567169
q = 150666731193060465857318079463252879097159019829490149782649859359850965103446020059
$DV^2 = 3 \times 448206397683121677619022856321082709420715^2$
ρ ≈ 1. 63

(2) k = 15
$r(x) = 81x^8 – 81x^7 + 54x^6 – 27x^5 + 9x^4 – 9x^3 + 6x^2 – 3x + 1$, $t(x) = –3x^2 + 1$, $h'(x) = 36x^2 + 36x + 12$, D = 3
x = 555160
r = 730852224770217224873076079683665556267288264121 (160 bits)
t = – 924607876799
q = 577701004015093581229234435988592940930639047439215123641554855917032109322710916801
$DV^2 = 3 \times 877649135676357917704884356667981068923199^2$
ρ ≈ 1. 73

(3) k = 28
$r(x) = x^{24} + x^{22} – x^{18} – x^{16} + x^{12} – x^8 – x^6 + x^2 + 1$, $t(x) = x^3 + 1$, $h'(x) = 4x^4 – 4x^2 + 4$, D = 3
x = 4771
r = 193475517289794799472841019248011083439477940513443901124940403238863262235005661903714 41 (294 bits)
t = 108599606012
q = 394093170064435167699978967026027611768493458697157224906246478662523751222508742907233737715393478235512636680743001834871 1

$DV^2 = 3 \times 229228610798458916310214822643061578056488974455156650579939870^2$
ρ ≈ 1. 4

(4) k = 12
$r(x) = 2197x^4 – 1352x^3 + 299x^2 – 28x + 1$, $t(x) = 13x – 1$ D = 3
x = 137438953782
r = 783915802287873738784769281395853185119086316917 (160 bits)
t = 1786706399165
q = 108442095810496574020294539628275481997508664893174275858667282760415108 47
$DV^2 = 3 \times 380249209178220512303502913837721631 1^2$
ρ ≈ 1.5

(5) k = 14
$r(x) = 20511149x^6 – 30413083x^5 + 18803919x^4 – 6205739x^3 + 1153069x^2 – 114381x + 4733$, $t(x) = 29x – 6$, D = 7
x = 5936652
r = 897923694407722064866709188398349353035596592369 (160 bits)
t = 172162902
q = 326811759720835564714732775797503236447913111267853657917916780522421188688368290 1
$DV^2 = 7 \times 432145319288933879814785107185576180841002^2$
ρ ≈ 1.7