Appl. Num. Anal. Comp. Math. **2**, No. 1, 100 – 107 (2005) / **DOI** 10.1002/anac.200410027

Aitken and Neville Inverse Interpolation Methods over Finite Fields

E.C. Laskari[*1,3], **G.C. Meletiou**[**2,3], and **M.N. Vrahatis**[***1,3]

[1] Computational Intelligence Laboratory, Dept. of Mathematics, University of Patras, GR-26110 Patras, Greece
[2] A.T.E.I. of Epirus, Arta, Greece, P.O. Box 110, GR–47100 Arta, Greece
[3] University of Patras Artificial Intelligence Research Center (UPAIRC), University of Patras, GR-26110 Patras, Greece

Received 31 October 2004, revised 21 March 2005, accepted 21 March 2005
Published online 22 April 2005

In this contribution the application of two inverse interpolation methods over finite fields is studied. More specifically, we consider the Aitken and Neville inverse interpolation methods for a "shifted" discrete exponential function. The results indicate that the computational cost of finding the discrete logarithm through this approach remains high, however interesting features regarding the degree of the resulting interpolation polynomials are reported.

1 Introduction

Public key cryptography is intimately related to a number of hard and complex mathematical problems from the fields of computational algebra, number theory, probability theory, mathematical logic, Diophantine's complexity and algebraic geometry. Such problems are the factorization [1], the discrete logarithm [2, 3, 4] and others [5]. Cryptosystems rely on the assumption that these problems are computationally intractable, in the sense that their computation cannot be completed in polynomial time.

The *Discrete Logarithm Problem* (DLP) [2, 3, 4] amounts to the development of an efficient algorithm for the computation of an integer x that satisfies the relation:

$$\alpha^x = \beta,$$

where α is a fixed primitive element of a finite field $\mathbb{F}_q$ (i.e., α is a generator of the multiplicative group $\mathbb{F}_q^*$ of $\mathbb{F}_q$) and β is a non–zero element of the field. We assume that x is the smallest nonnegative integer with $\alpha^x = \beta$. Then, x is called the *index* or the *discrete logarithm* of β. In the special case of a finite field $\mathbb{Z}_p$ of prime order p, a primitive root g modulo p is selected. If u is the smallest nonnegative integer with $g^u \equiv h \pmod{p}$, then u is called the *index* or the *discrete logarithm* of h.

The security of various public and private key cryptosystems [2, 3, 4, 6, 7, 8, 9, 10, 11, 12, 13] relies on the assumption that DLP is computationally intractable. Specifically, we refer to:

(1) the *Diffie–Hellman exchange protocol* [14],
(2) the *El Gamal public key cryptosystem* as well as *the El Gamal digital signature scheme* [13].

The *Diffie–Hellman key Problem* (DHP) [6, 10, 15] is defined as follows. Let α be a fixed primitive element of a finite field $\mathbb{F}_q$; x, y, satisfying, $0 \leqslant x, y \leqslant q-2$, denote the private keys of two users; and $\beta = \alpha^x$, $\gamma = \alpha^y$ represent the corresponding public keys. Then, the problem amounts to computing α^{xy} from β and γ, where α^{xy} is the symmetric key for secret communication between the two users.

* e-mail: elena@math.upatras.gr, Phone: +30 2610 997 348
** e-mail: gmelet@teiep.gr, Phone: +30 26810 76941
*** e-mail: vrahatis@math.upatras.gr, Phone: +30 2610 997 374

Consider the special case of the DHP, where $\beta = \gamma$. The term *Diffie–Hellman Mapping* refers to the mapping:

$$\beta = \alpha^x \longmapsto \alpha^{x^2}.$$

The definition of the *Diffie–Hellman Mapping Problem* (DHMP) follows naturally from the aforementioned definition of DHP. The two problems, DHMP and DHP, are computationally equivalent, since the following relation holds:

$$\alpha^{x^2}\alpha^{y^2}\alpha^{2xy} = \alpha^{(x+y)^2},$$

and the computation of α^{xy} from α^{2xy} is feasible (square roots over finite fields).

The *factorization problem* is related to the RSA cryptosystem [1]. The security of this cryptosystem relies on the computational intractability of the factorization of a positive integer $N = pq$, where p and q are two distinct odd primes [16]. The factorization of N is equivalent to determining $\phi(N)$ from N, where $\phi(N) = (p-1)(q-1)$ [1].

Numerous techniques, including algebraic, number theoretic, soft computing and interpolation methods, have been proposed to tackle the aforementioned problems [2, 3, 4, 6, 7, 8, 9, 10, 11, 12, 15, 17, 18, 19]. We focus on interpolation techniques over finite fields. In particular, we consider the Aitken and the Neville inverse polynomial interpolation methods applied on a "shifted" discrete exponential function.

The rest of the paper is organized as follows. In Section 2, we briefly present previous work on interpolation methods over finite fields and describe the Aitken and Neville interpolation methods. In Section 3, the proposed approach for inverse interpolation over finite fields is described and results for a "shifted" exponential function are reported. The paper closes with a synopsis in Section 4.

2 Background Material

This section is devoted to a brief description of interpolation methods over finite fields and also presents the Aitken and Neville interpolation methods.

2.1 Interpolation Methods over Finite Fields

In a finite field $\mathbb{F}_q$, where $q = p^n$, with p prime and n a positive integer, every function can be represented as a polynomial through Lagrangian interpolation. For every function, $f : \mathbb{F}_q \to \mathbb{F}_q$, there exists a unique polynomial $p(x)$ of degree at most $(q-1)$ that coincides with f. Interpolation is computationally attractive only in the case of a polynomial with small number of non–zero coefficients (low sparsity). Since encryption and decryption functions are defined as functions over finite fields, it is natural to attempt to express them as polynomials.

Regarding the discrete logarithm function, the well–known formula due to Wells [20] exists:

$$\log_a(x) = \sum_{i=1}^{p-2} \frac{x^i}{1-a^i},$$

where $x \neq 0$, $a, x \in \mathbb{Z}_p$, and a is a generator of $\mathbb{Z}_p^*$. This formula can be generalized for the case of a field $\mathbb{F}_q$ of prime power order and moreover, for the case of a not being a generator of the multiplicative group of the field [7, 8, 11]. A discrete Fourier transformation can also be used [7]:

$$\log_a(x) = (1, 2, \ldots, p-1) \underset{1 \leqslant i,j \leqslant p-1}{(a^{-ij})} \begin{pmatrix} x \\ x^2 \\ \vdots \\ x^{p-1} \end{pmatrix}.$$

For the Diffie–Hellman mapping, the following formula has been proposed [10]:

$$K(x,y) = -\sum_{1 \leqslant i,j \leqslant p-1} x^i y^j a^{-ij}.$$

This expression can be represented through a discrete Fourier transformation as follows:

$$K(x,y) = (y, y^2, \ldots, y^{p-1}) \underset{1\leqslant i,j\leqslant p-1}{(-a^{-ij})} \begin{pmatrix} x \\ x^2 \\ \vdots \\ x^{p-1} \end{pmatrix}.$$

The Diffie–Hellman key exchange is based on the fact that there is no simple representation of the Diffie–Hellman mapping $F(g^u, g^v) = g^{uv}$, with $0 < u, v < d$. It can be easily verified that the polynomial [10]:

$$F(x,y) = e \sum_{i,j=0}^{d-1} g^{-ij} x^i y^j, \quad ed \equiv 1 \pmod{p},$$

represents the Diffie–Hellman key function in the field $\mathbb{F}_q$, where $q = p^n$.

The polynomial F can be of degree at most $2(d-1)$, while the largest number of non–zero coefficients of F is d^2. Recently, lower bounds for the degree of a two–variable polynomial have been identified [10].

2.2 The Aitken and Neville Interpolation Methods

A Lagrangian type interpolation achieves the desirable accuracy using the smallest possible number of interpolation points. However, the proper number of interpolation points is not a priori known. Typically, a number of interpolation points are initially considered and, if they are not sufficient, new points are added iteratively until the desired accuracy is achieved. The addition of a new interpolation point in the case of Lagrangian interpolation cannot be performed directly, because the interpolation polynomial changes and, thus, all computations need to be performed from the beginning.

The Aitken and Neville interpolation methods are well–known and they are considered as the state-of-the-art for the interpolation of functions over real numbers [21]. Furthermore, Aitken and Neville interpolation methods are constructive in a way that permits the addition of a new interpolation point with low computational cost. This advantage of the aforementioned methods over the Lagrangian interpolation method and the fact that their interpolation formulae can be applied in any field, has motivated our investigation of their performance over finite fields.

Let $f(x)$ be a function defined on a field $\mathbb{F}$, $x_i \in \mathbb{F}$, $i = 0, \ldots, n$, be mutually different interpolation points, and $f_i = f(x_i)$. Then, the Aitken polynomial is defined as:

$$P_{0,1,\ldots,m,i}(x) = \frac{1}{(x_i - x_m)} \begin{vmatrix} P_{0,1,\ldots,m}(x) & x_m - x \\ P_{0,1,\ldots,m-1,i}(x) & x_i - x \end{vmatrix}, \qquad \text{for} \begin{cases} m = 0, \ldots, n-1, \\ i = (m+1), \ldots, n, \end{cases}$$

where, in general, $P_{0,1,\ldots,k}$ denotes the Aitken polynomial that interpolates all points $x_0, x_1, \ldots, x_k$.

The corresponding Neville interpolation formula is:

$$P_{i,i+1,\ldots,i+m}(x) = \frac{1}{(x_{i+m} - x_i)} \begin{vmatrix} P_{i,i+1,\ldots,i+m-1}(x) & x_i - x \\ P_{i+1,i+2,\ldots,i+m}(x) & x_{i+m} - x \end{vmatrix}, \qquad \text{for} \begin{cases} m = 1, \ldots, n, \\ i = 0, \ldots, (n-m), \end{cases}$$

where, in general, $P_{i,i+1,\ldots,i+k}$ denotes the Neville polynomial that interpolates all points $x_i, x_{i+1}, \ldots, x_{i+k}$.

In several applications, the values f_i, $i = 0, \ldots, n$, of a function $y = f(x)$ at the corresponding points x_i, $i = 0, \ldots, n$, are given, and the point x^*, such that $f(x^*) = y^*$, is required. This is the inverse interpolation problem for the function f. Both Aitken and Neville interpolation methods can be applied for the inverse interpolation problem by simply exchanging x_i and $y_i = f_i$ in the corresponding formulae [21]. Thus, the formula of the inverse Aitken interpolation method is:

$$P_{0,1,\ldots,m,i}(y) = \frac{1}{(y_i - y_m)} \begin{vmatrix} P_{0,1,\ldots,m}(y) & y_m - y \\ P_{0,1,\ldots,m-1,i}(y) & y_i - y \end{vmatrix}, \qquad \text{for} \begin{cases} m = 0, \ldots, n-1, \\ i = (m+1), \ldots, n, \end{cases}$$

while the corresponding inverse Neville interpolation formula is:

$$P_{i,i+1,\ldots,i+m}(y) = \frac{1}{(y_{i+m} - y_i)} \begin{vmatrix} P_{i,i+1,\ldots,i+m-1}(y) & y_i - y \\ P_{i+1,i+2,\ldots,i+m}(y) & y_{i+m} - y \end{vmatrix}, \qquad \text{for} \begin{cases} m = 1, \ldots, n, \\ i = 0, \ldots, (n-m). \end{cases}$$

Table 1 Instances of test problems used.

# Problem	p	α	b
1	101	2	30
2	599	7	200
3	1759	6	500
4	2003	5	100
5	2411	6	700
6	2801	3	300
7	3001	14	100
8	3313	10	400
9	3631	15	3600
10	4001	3	1000
11	4441	21	500
12	4751	19	4500
13	5003	2	1000
14	5209	17	300
15	5881	31	3000
16	6007	3	2000
17	6841	22	4000
18	7001	3	500
19	7841	12	3500
20	8011	14	40
21	8761	23	6000
22	8929	11	3000
23	9001	7	200
24	10007	5	1000

3 Inverse Interpolation over Finite Fields

We study the inverse Aitken and the inverse Neville interpolation methods over finite fields. In particular, we investigate the inverse interpolation approach on the values of the "shifted" discrete exponential function:

$$f(x) = \alpha^x - b \pmod{p},$$

over $\mathbb{Z}_p$ with p a prime number and α a primitive element of $\mathbb{Z}_p$. This function is a bijection, since α is a primitive element.

Since the considered methods are constructive, not all the elements of the range of the function are used as interpolation points, but rather, as many points as necessary to construct a polynomial that interpolates the function value $f(x^*) = 0 \pmod{p}$. The procedure begins by interpolating two function values of the function $f(x)$ for two random values of x. The resulting polynomial is evaluated at zero and, unless the obtained value is the discrete logarithm of b over α modulo p, its function value becomes a new interpolation point.

The capability and the characteristics of the considered inverse interpolation methods over finite fields of prime order were tested for different primes, p, and values of b. The instances of the test problems are reported in Table 1. The results over 100 independent experiments for these problems are reported in Table 2. This table reports the number of verifications (# Verifications), the number of points used (# Points Used), and the degree of the resulting polynomials (Pol. Degree). Verifications refers to the number of times that a polynomial evaluation at zero is performed, to verify whether the outcome equals the value of the discrete logarithm. Each verification requires one evaluation of the "shifted" exponential function, f, for a specific value of x. Points Used refers to the number of interpolation points, $y = f(x)$, employed by the procedure (and, thus, evaluated) until the proper interpolation polynomial is found. Note that not all of these points are necessarily interpolated by the final polynomial. Finally, the third quantity (Pol. Degree) corresponds to the degree of the resulting polynomial that interpolates the value of the discrete logarithm. The number of interpolation points that are used to construct this polynomial is (Pol. Degree+1). For each experiment, the two initial interpolation points are chosen randomly

in the range $[1, p-1]$. For each of the three quantities, the mean value (Mean), the median (Med), the standard deviation (StD), as well as, the minimum (Min) and maximum (Max) values are reported.

The results indicate that the computational cost, with respect to the required verifications, for tackling the discrete logarithm problem is high for both methods. However, the relatively low degree of the resulting polynomials is an interesting finding as it indicates that in most cases a polynomial with low degree that interpolates the discrete logarithm exists. Therefore, finding the proper interpolation points is critical for reducing the computational cost.

Another attractive finding is the high frequency with which, low degree polynomials appear in the conducted experiments for each instance of the problem. This conclusion is derived by the low median values of the degree of the obtained polynomial reported in Table 2, in contrast to the corresponding maximum values that are rarely observed. The frequency of appearance of different degrees of polynomials over all tested problems for both methods is depicted in Figure 1. Regarding the ability of each method to find a proper polynomial, Aitken's method was slightly better than the Neville's method in most cases.

The performance of the methods was also investigated for several instances of b, while keeping the value of p constant. Table 3 reports results for this setting. Overall, the behavior of both methods is quite stable with respect to this parameter.

4 Synopsis

The performance of two inverse interpolation methods, namely the Aitken and Neville interpolation methods, was studied on a "shifted" discrete exponential function over finite fields. The results indicate that the computational cost for tackling the problem of the discrete logarithm through both methods is high. Overall, Aitken's method proved slightly better than the Neville's method. It is important to observe that the resulting polynomials were most often of low degree. This finding implies that in most cases there exists a low degree polynomial that interpolates the discrete logarithm. Therefore, finding the proper interpolation points is crucial to reduce the computational cost of this approach and it will be the subject of future work.

Acknowledgements We acknowledge the partial support by the "Archimedes" research programme awarded by the Greek Ministry of Education and Religious Affairs and the European Union.

References

[1] R. Rivest, A. Shamir, L. Adlemann, A method for obtaining digital signatures and public-key cryptosystems, Commun. ACM, **21**, 120–126, (1978).
[2] L. Adleman, A subexponential algorithm for discrete logarithm problem with applications to cryptography, 20th FOCS, 55–60, (1979).
[3] A. M. Odlyzko, Discrete logarithms: the past and the future, Des. Codes Cryptog., **19**, 129–145, (2000).
[4] S. C. Pohlig, M. Hellman, An improved algorithm for computing logarithms over $\mathrm{GF}(p)$ and its cryptographic significance, IEEE Trans. Inf. Theory, **24**, 106–110, (1978).
[5] R. C. Merkle, M. E. Hellman, Hiding information and signatures in trapdoor knapsacks, IEEE Trans. Inf. Theory, **24**, 525–530, (1978).
[6] D. Coppersmith, I. Shparlinski, On polynomial approximation of the discrete logarithm and the Diffie–Hellman mapping, J. Cryptology, **13**, 339–360, (2000).
[7] G. C. Meletiou, G. L. Mullen, A note on discrete logarithms in finite fields, Appl. Algebra Engrg. Comm. Comput., **3**, No. 1, 75–79, 1992.
[8] G. L. Mullen, D. White, A polynomial representation for logarithms in $\mathrm{GF}(q)$, Acta Arith., **47**, 255–261, (1986).
[9] H. Niederreiter, A short proof for explicit formulas for discrete logarithms in finite fields, Appl. Algebra Engrg. Comm. Comput., **1**, 55–57, (1990).
[10] A. Winterhof, A note on the interpolation of the Diffie-Hellman mapping, Bull. Australian Math. Soc., **64**, No. 3, 475–477, (2001).
[11] G. C. Meletiou, Explicit form for the discrete logarithm over the field $\mathrm{GF}(p, k)$, Arch. Math. (Brno), **29**, No. 1–2, 25–28, (1993).
[12] A. Winterhof, Polynomial interpolation of the discrete logarithm, Des. Codes Cryptogr., **25**, No. 1, 63–72, (2002).
[13] T. El Gamal, A public key cryptosystem and a signature scheme based on discrete logarithms, IEEE Trans. Inf. Theory, **31**, 469–472, (1985).

Table 2 Results of the inverse Aitken and inverse Neville methods over 100 independent experiments.

AITKEN															
Problem	# Verifications					# Points Used					Pol. Degree				
	Mean	Med	StD	Min	Max	Mean	Med	StD	Min	Max	Mean	Med	StD	Min	Max
1	51.06	49.50	27.24	4.00	98.00	12.36	11.50	6.15	2.00	27.00	6.27	5.00	4.44	1.00	25.00
2	304.34	298.50	190.44	9.00	598.00	31.95	29.00	19.01	4.00	96.00	16.19	11.00	14.25	1.00	80.00
3	845.33	776.50	505.70	52.00	1741.00	50.97	44.50	27.15	10.00	126.00	23.82	18.00	20.77	1.00	113.00
4	885.76	858.50	577.26	4.00	1978.00	50.15	47.00	28.76	2.00	138.00	26.62	19.50	23.10	1.00	113.00
5	1185.38	1233.50	698.64	6.00	2385.00	59.90	58.00	31.35	3.00	147.00	30.07	21.00	28.41	1.00	125.00
6	1251.48	1225.00	813.69	39.00	2800.00	60.21	56.50	35.48	9.00	220.00	33.38	24.50	28.74	1.00	121.00
7	1490.59	1434.00	871.58	7.00	2996.00	68.81	62.50	36.85	3.00	190.00	29.91	25.00	24.50	1.00	116.00
8	1727.81	1689.50	886.54	80.00	3280.00	74.44	68.00	35.10	12.00	170.00	37.70	32.00	25.80	2.00	123.00
9	1701.35	1536.50	1109.06	29.00	3578.00	72.75	63.00	43.54	7.00	176.00	38.66	31.50	34.32	1.00	143.00
10	1953.68	1758.00	1228.28	41.00	3996.00	79.38	68.50	45.88	9.00	224.00	39.24	29.00	35.27	2.00	168.00
11	2297.73	2430.00	1298.40	18.00	4438.00	86.37	84.50	45.71	6.00	272.00	47.17	35.50	34.66	1.00	127.00
12	2092.47	1744.00	1452.38	6.00	4613.00	78.01	66.00	44.95	3.00	181.00	35.35	25.00	36.91	1.00	174.00
13	2569.09	2992.00	1450.74	48.00	4875.00	88.88	95.50	43.22	10.00	193.00	43.37	36.00	34.83	1.00	130.00
14	2538.64	2831.00	1437.81	44.00	5203.00	87.19	90.00	44.47	9.00	284.00	44.20	35.00	38.53	3.00	282.00
15	3140.46	3172.50	1686.20	116.00	5730.00	100.56	96.00	48.11	15.00	210.00	54.73	44.00	44.67	1.00	180.00
16	3227.38	3088.50	1684.70	38.00	5993.00	103.76	93.00	50.98	9.00	269.00	45.27	36.00	36.94	1.00	173.00
17	3725.76	4058.00	2022.05	184.00	6838.00	113.78	111.00	60.69	19.00	343.00	55.38	40.00	45.02	1.00	218.00
18	3238.45	2996.50	2019.04	60.00	6926.00	98.18	88.50	52.63	11.00	252.00	48.93	38.50	43.07	1.00	212.00
19	3794.16	3498.00	2256.09	98.00	7831.00	108.69	96.50	59.65	14.00	329.00	53.68	44.00	44.84	1.00	192.00
20	3801.96	3979.50	2289.30	10.00	7989.00	107.27	105.00	58.25	4.00	312.00	54.72	38.50	48.85	1.00	242.00
21	4253.92	4782.00	2463.25	146.00	8704.00	112.20	117.50	56.97	17.00	299.00	59.54	42.00	55.87	1.00	296.00
22	4823.47	5221.00	2403.39	57.00	8916.00	125.86	124.00	59.34	10.00	353.00	63.53	51.50	54.91	2.00	259.00
23	4350.66	4492.00	2364.91	104.00	8919.00	113.89	111.50	56.05	14.00	290.00	56.89	43.50	51.90	3.00	288.00
24	4927.91	5450.50	2932.47	92.00	9734.00	121.69	125.50	62.27	13.00	268.00	64.41	51.50	50.12	2.00	222.00
NEVILLE															
Problem	# Verifications					# Points Used					Pol. Degree				
	Mean	Med	StD	Min	Max	Mean	Med	StD	Min	Max	Mean	Med	StD	Min	Max
1	53.57	54.50	26.47	5.00	100.00	12.78	12.00	5.93	2.00	30.00	7.61	6.50	5.39	1.00	29.00
2	313.76	308.00	168.96	11.00	593.00	31.43	29.00	15.31	4.00	72.00	16.92	13.00	12.02	1.00	49.00
3	961.97	960.00	502.37	32.00	1748.00	57.22	53.00	28.57	8.00	134.00	29.43	22.50	24.09	1.00	109.00
4	1030.32	1076.00	544.13	113.00	1970.00	56.97	55.50	26.52	15.00	124.00	29.95	22.50	22.53	1.00	95.00
5	1076.98	1060.50	626.18	6.00	2352.00	55.07	53.00	27.40	3.00	135.00	26.16	19.00	22.84	1.00	121.00
6	1406.53	1362.00	789.02	18.00	2742.00	65.74	61.00	31.44	6.00	145.00	32.41	25.00	27.40	1.00	111.00
7	1472.15	1438.00	893.62	8.00	2979.00	67.51	62.00	36.23	3.00	172.00	33.91	26.00	27.82	1.00	112.00
8	1682.65	1556.50	978.54	42.00	3206.00	72.76	64.50	37.08	9.00	150.00	31.71	23.00	26.33	1.00	115.00
9	1830.08	1894.00	1040.59	5.00	3625.00	75.23	73.50	39.30	2.00	216.00	40.04	34.00	32.91	1.00	135.00
10	2134.41	2023.00	1191.16	14.00	3994.00	86.02	75.00	46.77	5.00	233.00	43.19	42.00	33.19	1.00	177.00
11	2197.55	2415.00	1265.07	17.00	4370.00	81.52	83.50	41.62	5.00	195.00	35.95	26.00	29.54	1.00	128.00
12	2451.19	2322.00	1361.64	27.00	4625.00	87.62	80.50	42.45	7.00	189.00	44.07	34.00	34.27	2.00	143.00
13	2681.18	2864.00	1461.67	28.00	4916.00	94.79	91.50	48.01	7.00	202.00	45.92	35.00	38.28	1.00	145.00
14	2485.72	2675.50	1511.98	109.00	5192.00	88.97	86.00	51.54	15.00	252.00	44.92	31.50	38.03	1.00	211.00
15	2936.12	2825.50	1826.41	28.00	5861.00	98.40	88.50	56.98	7.00	264.00	49.17	38.00	44.79	1.00	209.00
16	3139.66	2867.00	1757.40	45.00	5988.00	102.50	88.50	54.64	9.00	265.00	54.55	49.50	43.29	1.00	190.00
17	3429.21	3255.00	1932.10	158.00	6805.00	103.87	94.00	52.77	18.00	265.00	53.58	39.00	48.15	1.00	230.00
18	3177.59	3110.00	1939.81	9.00	6990.00	95.84	90.50	52.48	4.00	301.00	52.54	46.50	40.90	1.00	196.00
19	3697.39	3648.50	2259.73	181.00	7796.00	105.62	100.00	57.46	19.00	281.00	46.34	34.50	39.05	1.00	168.00
20	4025.00	4266.50	2322.49	94.00	7985.00	112.37	110.50	59.54	14.00	303.00	61.39	45.50	53.68	2.00	288.00
21	4592.02	5090.50	2732.54	115.00	8611.00	121.49	122.50	63.21	15.00	266.00	67.06	56.50	50.40	1.00	200.00
22	4463.26	4737.00	2378.70	7.00	8723.00	115.79	116.50	53.26	3.00	261.00	62.33	52.00	46.77	1.00	209.00
23	4719.24	4997.00	2690.34	58.00	8878.00	123.24	120.50	64.18	11.00	280.00	60.18	51.50	48.67	1.00	202.00
24	4932.99	4711.50	2988.91	58.00	9963.00	123.68	113.00	66.22	11.00	332.00	56.21	42.50	54.51	1.00	258.00

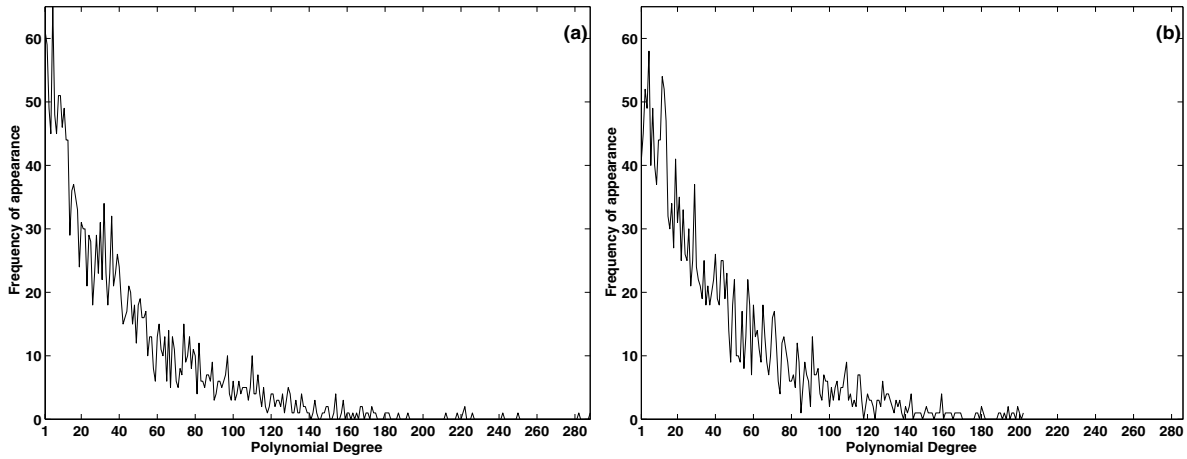

Fig. 1 Frequency of appearance of polynomial degrees over all problems with (a) Aitken method and (b) Neville method.

Table 3 Results over 100 independent experiments for $p = 2003$, $\alpha = 5$ and several instances of b.

Problem	measure (%)	# Points Used	Pol.Degree
	Mean	61.07	29.25
$p = 2003$	Median	60.00	25.00
$a = 5$	Min	5.00	1.00
$b = 9$	Max	142.00	112.00
	Mean	58.86	26.87
$p = 2003$	Median	57.00	19.00
$a = 5$	Min	13.00	1.00
$b = 100$	Max	180.00	140.00
	Mean	57.41	29.52
$p = 2003$	Median	51.00	21.00
$a = 5$	Min	10.00	1.00
$b = 600$	Max	153.00	108.00
	Mean	54.07	27.46
$p = 2003$	Median	51.00	21.00
$a = 5$	Min	8.00	2.00
$b = 900$	Max	110.00	78.00
	Mean	55.89	28.86
$p = 2003$	Median	49.00	20.00
$a = 5$	Min	8.00	1.00
$b = 1300$	Max	173.00	133.00
	Mean	55.48	28.09
$p = 2003$	Median	50.00	23.00
$a = 5$	Min	5.00	2.00
$b = 1550$	Max	145.00	123.00
	Mean	55.11	27.88
$p = 2003$	Median	51.00	23.00
$a = 5$	Min	9.00	2.00
$b = 1900$	Max	162.00	121.00
	Mean	52.23	23.82
$p = 2003$	Median	48.00	20.00
$a = 5$	Min	3.00	1.00
$b = 2000$	Max	138.00	100.00

[14] W. Diffie, M. Hellman, New directions in cryptography, IEEE Trans. Inf. Theory, **22**, 644–654, (1976).
[15] U. Maurer, S. Wolf, The relationship between breaking the Diffie-Hellman protocol and computing discrete logarithms, SIAM J. Computing, **28**, 1689–1721, (1999).
[16] A. Menezes, P. van Oorschot, S. Vanstone, Handbook of applied cryptography, CRC Press, (1996).
[17] I. Shparlinski, Cryptographic applications of analytic number theory: complexity lower bounds and pseudorandomness, Progress in Computer Science and Applied Logic, **22**, Birkhaüser Verlag, Basel, (2003).
[18] T. Lange, A. Winterhof, Incomplete character sums over finite fields and their application to the interpolation of the discrete logarithm by Boolean functions, Acta Arith., **101**, No. 3 223–229, (2002).
[19] G. C. Meletiou, A polynomial representation for exponents in $\mathbb{Z}_p$, Bull. Greek Math. Soc., **34**, 59–63, (1992).
[20] A. L. Wells, A polynomial form for logarithms modulo a prime, IEEE Trans. Inform. Theory, **IT-30**, 845–846, (1985).
[21] R. L. Burden, J. D. Faires, Numerical Analysis, Brooks/Cole Publishing Company, (1997).