ADVANCES IN CYBER-PHYSICAL SYSTEMS

Vol. 1, No. 2, 2016

EXTENDED FINITE FIELDS IN CRYPTOGRAPHIC INFORMATION PROTECTION

Roman Popovych

Lviv Polytechnic National University, 12, Bandera Str., Lviv, 79013, Ukraine
Author's e-mail: rombp07@gmail.com

Submitted on 21.11.2016

Abstrac. **The use of extended finite fields for cryptographic information protection is focused on. In particular, explicit construction in finite fields elements of high multiplicative order is described. The obtained correspondent lower bounds on the order are provided.**

Index Terms – information protection, algebraic structure, finite field, multiplicative order, lower bound.

I. INTRODUCTION

Ensuring the confidentiality, integrity and authenticity of information, cryptographic protection of information links between components of cyber-physical systems is an urgent problem.

In this paper we consider one aspect of information protection related to the use of certain algebraic structures called finite fields or Galois fields [5, 7].

F_q is the finite field [5, 7] with q elements, where q is the power of prime number p. F_{q^n} is the degree n extension of F_q. Generators of the multiplicative group $F_{q^n}^*$ are called primitive elements.

The following question still remains open: to find an efficient algorithm for constructing primitive elements in finite fields. An algorithm is efficient if it is polynomial, that is: its running time is $\log(q^n)^{O(1)}$ arithmetic operations in F_{q^n}. At present the problem of effective construction of a primitive element for a given finite field is computationally difficult.

The relaxation to the primitive element problem is as follows. Elements with high multiplicative order are often needed in several applications using finite fields [6, 7]. Ideally we want to have a possibility to obtain a primitive element for any finite field. However, if we have no factorization of the order of finite field multiplicative group, it is not known how to reach the goal. Therefore, a less ambitious question is being considered: to construct an element with the provably high order. Definition of Gao [4]: by "high orders" of elements in F_{q^n}, we mean that the orders of elements must be larger than every polynomial in $\log(q^n)$ when q^n tends to infinity. We do not need to compute the exact order of the element. It is sufficient in this case to obtain a lower bound of the order.

You can draw a parallel between classification of algorithms related to their computational complexity and division of finite element field into elements of the high order and elements of the order which is not high. In the case of algorithms, we have exponential and polynomial algorithms. The estimate of the computational complexity for the former ones is larger than any polynomial of input data volume (i.e. logarithm of the input data). The estimate for the latter is restricted by some polynomial. The concept of a high order element is similar to the concept of exponential algorithm. It is possible to compare an element which is not of high order with polynomial algorithm.

II. POSSIBLE FINITE CYCLIC GROUPS

The multiplicative order $\operatorname{ord} b$ of element $b \in F_q^*$ is the smallest positive integer u such that $b^u = 1$.

Typical possible applications of high order elements in finite fields are as follows:

– cryptography (Diffie-Hellman key exchange protocol, public key ElGamal cryptosystem);

– coding theory (in particular, for definition of error-correcting BCH-codes);

– pseudo-random numbers generators (different powers of high order element can be considered as a sequence of pseudo-random numbers);

– primality proving (elements of high order are used in the AKS algorithm of primality proving suggested by Agrawal, Kayal and Saxena [1]).

The use of high multiplicative order elements in cryptography is based on the so called discrete logarithm problem in a finite cyclic group [6].

Let G be a finite cyclic group that has q elements, with a generator g (which is also often called a primitive element). By using sequential squaring, one can quickly (in polynomial time) calculate $Y = g^X$ for any integer $1 \le X \le q-1$. It is considered that, possessing Y it is computationally difficult (impossible for modern supercomputers to do in a reasonable amount of time) to find discrete logarithm of it in the base g, that is the number X. In other words, the function $f(X)=g^X$ is a one way function. However, a proof of this is not known at present.

Bearing in mind the discrete logarithm problem, the following two cryptographic schemes are mostly considered.

A. Diffie-Hellman Key Exchange

How can two users agree on a secret key (used perhaps for a private key cryptosystem) over a public channel?

User A and user B agree on some finite cyclic group G with q elements and a generating element g o f this group G. (This is usually done long before the rest of the protocol; g is assumed to be known by all attackers.) We will write the group G multiplicatively. Both G, and g, are public.

User A: chooses a secret number $1 \le a \le q-1$, counts g^a and sends g^a to user B.

User B: chooses a secret number $1 \le b \le q-1$, counts g^b and sends g^b to user A.

Both user A and user B are now in possession of the group element $(g^a)^b=(g^b)^a=g^{ab}$, which can serve as the shared secret key.

B. The ElGamal cryptosystem (public key cryptosystem)

Let G is a finite cyclic group that has q elements with a generator g. Both G, and g, are public.

Every user U: chooses a random number $1 \le a \le q-1$ – the secret key for encryption. Then counts g^a and publishes it. This is the public key of the user. To send a private message P one chooses a random number k, then computes and sends the pair $b_1=g^k$, $b_2=P(g^a)^k$.

The user U performs the decryption according to the expression $P=b_2(b_1)^{-a}$.

Note, that g is not necessarily a generator of the group G. The first and second described cryptographic schemes work for any random element g. At the same time their resistance to cracking depends on the multiplicative order of the element g. The order of this element in chosen finite cyclic group must be big enough.

It is possible to use the following finite cyclic groups as G in cryptography:

1) Multiplicative group of a prime field $F_p^*=\{1,...,p-1\}$, that is the multiplicative group of integers modulo p, where p is prime, and g is a primitive root modulo p.

2) Elliptic curve $E(F_q)$ over a finite field F_q. It is usually written not in the multiplicative form, but in the additive form. Such curve is a set of pairs (x,y) of elements of the chosen field, which satisfies the affine equation of elliptic curve in, say, Weierstrass form

$$y^2=x^3+Ax^2+B,$$

where $A,B \in F_q$, $B \ne 0$, along with a distinguished point at infinity denoted O. The pair (x,y) of elements of the base field is called affine coordinates of elliptic curve point. The distinguished point O has no affine coordinates. Elements A,B of the base field are called coefficients of elliptic curve equation. This set together with the group operation of elliptic curves is an Abelian group, with the point at infinity as an identity element.

While an elliptic curve is not necessarily cyclic, it can always be generated by two elements. Thus, an elliptic curve does not necessarily possess a primitive element. But if such an element exists, the results about its explicit construction are unknown at present.

3) Multiplicative group of the extended finite field $F_{q^n}=F_q[x]/f(x)$, where $f(x)$ is irreducible over F_q polynomial of degree n.

All known strategies of primitive element search [3] consist of two stages:

1. Find a 'small' set $A \subseteq F_q$ guaranteed to contain a primitive root of F_q.

2. Test all elements of the set A for primitivity.

In many cases, we have polynomial algorithms for the first stage, especially if one assumes the Extended Riemann Hypothesis (ERH) [3].

One should divide the problem of finding a small set containing a primitive element: separately for prime fields and separately for extended fields. Usually we start the consideration from prime fields with a small number of elements. Determining the upper bound of the smallest primitive element is always an important problem in algebra and number theory. Wang showed in his classical paper [3] that the least primitive element for prime finite field F_p is bounded by $p^{1/4+e}$. Assuming ERH, Wang showed that the smallest primitive root in prime finite field F_p is bounded by the value $O(w^6(p-1)\log^2 p)$, where w is the map sending a positive integer to the number of its distinct prime divisors. It is proved that $w(n)=O(\log n/\log\log n)$. Shoup improved the bound to $\tilde{O}(w^4(p-1)\log^2 p)$. Here $\tilde{O}(f(n))$ means $O(f(n)\log^c f(n))$ for a certain constant c.

Hence if ERH is true, one can generate a set containing a primitive element by enumerating all the numbers less than Shoup's bound, which is polynomial on the size of the input. Bach showed how to construct a set of cardinality $O(\log^4 p)$ which contains at least one primitive element assuming ERH. Instead of using only small numbers, his set is composed of larger elements, which are a product of small primes.

The case of small characteristic extended fields seems easier. Shoup, and independently Shparlinski shows unconditionally that one can deterministically construct a set of size $(np)^{O(1)}$, which contains at least one primitive element in the field F_{p^n} .

Unfortunately, at the current state of the art, the second stage requires the integer factorization of $q-1$ (a is primitive if and only if, then $a^{(q-1)/d} \neq 1$ for every prime number $d \mid q-1$), which is not known to be obtainable in polynomial time. The difficulty does not lie in the scarcity of primitive elements.

This implies that if we select a random element, we are highly likely to get a primitive element. Equally, if we select a list of $(\log\log q)^{1+e}$ many random elements with probability $1+o(1)$, there is a primitive element in the list. However, it is very hard to decide which element is primitive.

There should be also mentioned results about existence of primitive elements of some (quite simple) form.

The problem of high multiplicative order elements construction is considered both for general and for special finite fields. For special finite fields, it is possible to construct elements which can be proved to have much higher orders. A review of the obtained in this area results is provided in [7, section 4.4] (the section is written by Voloch).

III. LOWER BOUNDS ON MULTIPLICATIVE ORDER OF ELEMENTS IN EXTENDED FINITE FIELDS

We are considering below the obtained lower bounds on multiplicative order of elements for different classes of extended finite fields.

From the computational point of view, a finite field extension is nothing but a polynomial ring over a prime finite field modulo an irreducible polynomial. Let us assume that the field is given as $F_q[x]/f(x)$, where $f(x)$ is an irreducible polynomial over F_q.

All the constructions follow a similar scheme. The target element b is so designed that we can find a set U of large cardinality consisting of integers between 1 and q^n-1, which satisfies:

1. For any $i \in U$, b^i has a simple representation of degree less than n, y $F_p[a]$ (usually we get the representation using linearity of the p-th power);

2. For any $i, j \in U$, if $i \neq j$, then $b^i \neq b^j$. Since the power of b has small degree representation, we can lift the element to the polynomial ring $F_q[x]$, where it is easier to prove the distinctness of two elements.

If we can prove these two statements, we have shown that the cardinality of U is the lower bound of the order of the element b .

Thus, the combinatorial approach dominates in the construction of elements of large order. As element b some binomial of the variable x *is* usually taken (as a rule, linear, that is a binomial of degree one) and constructs products of elements conjugated with the element b . One uses both linear and non-linear conjugates. It is possible to involve both positive and negative powers of these conjugates.

A. Elements of high order in finite fields based on cyclotomic polynomials

We consider finite fields of the form

$$F_q(q) = F_{q^{r-1}} = F_q[x]/(x^{r-1}+\ldots+x+1) .$$

Let q be a power of a prime number p, r be an odd prime number coprime with q. Condition under which the given factor-ring is a field is as follows: q is a primitive root modulo r, a be any non-zero element in the finite field F_q. We obtain an estimation for the order of elements of the form $b = q + q^{-1} = q^{-1}(q^2+1)$ in cyclotomic extensions of finite fields. Such elements are called gauss periods analogously to extensions of the field of rational numbers.

We improve and generalize the result from the paper [2] for elements of the form more general than gauss period. The method, which is used in obtaining results, is to replace an element with its automorphic image. This gave an answer to the open question posed by these authors.

As an additional bonus in many cases the corresponding large order elements are generators of normal bases as well.

Such extensions are considered in our papers [8, 10]. Lower bound on the order of elements equals to $5^{\sqrt{(r-2)/2}-2}$ if the field characteristic $p \geq 5$.

B. Elements of high order in finite fields based on Kummer polynomials

Extension based on the Kummer polynomial is particularly used in pairing based cryptography. We consider further finite fields of the form $F_q(q) =_q [x]/(x^m - a)$. The numbers q, m and the element a from the initial field F_q are supposed to be such ones that the extension $F_q[x]/(x^m - a)$ exists.

Modern technique in the famous primality proving AKS algorithm and its further improvements [1] is to use polynomials of degree one to generate a large multiplicative subgroup of a finite field multiplicative group. Cheng [3] discovered a connection to the special finite field high order element problem and applied this idea to obtain a new solution of this problem. It is shown in [3] how to construct high order element in such extensions with the condition $q \equiv 1 (\bmod m)$. The lower bound 5.8^m is obtained in this case. High order elements are constructed for extensions of the form $F_q[x]/(x^{2^t}-a)$ and $F_q[x]/(x^{3^t}-a)$ without the divisibility condition. Lower bounds on multiplicative orders are equal to $\exp((\log m)^2)$, where $m=2^t$ and $m=3^t$ correspondingly. We improve and generalize this result in [9]. For any degree m of an extension, we drop the condition of divisibility of the number $q-1$ by m. We showed in the key lemma that the number m is a product of two numbers m_1 and m_2, where m_1 is a divisor of $q-1$, a m_2 is the order of the element q modulo m.

We consider an arbitrary extension of the form $F_q[x]/(x^m-a)$ and construct explicitly in it elements of multiplicative order at least $2^{\lfloor\sqrt[3]{2m}\rfloor}$. The idea is as follows. If the number $q-1$ has big divisor m_1, then we use for construction the method, analogous to the method for Kummer extensions. If the number $q-1$ has no big divisor m_1, then the number m_2 is large, and we use for construction the method, analogous to the method for extensions on a base of cyclotomic polynomials.

The algorithm of high order element construction is as follows. Let us find, using direct computations, $m_2=\mathrm{ord}_m q$ and $m_1=\dfrac{m}{m_2}$. Then compare m_1 and $\lfloor\sqrt{2m_2}\rfloor$. If $m_1\le\lfloor\sqrt{2m_2}\rfloor$, then the target element is equal to $q+b$ for any element b from F_q. If $m_1>\lfloor\sqrt{2m_2}\rfloor$, then the desired element is equal to $q^{m_2}+b$. The lower bound on the order of considered above elements equals to $2^{\lfloor\sqrt[3]{2m}\rfloor}$.

C. Elements of high order in finite fields based on Artin-Schreier polynomials

We consider finite fields of the form $F_p(q)=F_{p^p}=F_p[x]/(x^p-x-a)$.

For any prime number p, Artin-Shreier extension of the finite field F_p is the field F_{p^p}. It is known that the polynomial x^p-x-a is irreducible over F_p for any non-zero element a in F_p, and we may take $F_{p^p}=F_p[x]/(x^p-x-a)$.

Lower bound on the order of $q+b$ for any element b from F_p is obtained in [12] and equals to 4^p. For this class of fields is known, but not proven, the conjecture about the explicit form of primitive elements (Wagstaff's conjecture).

We obtained using computer calculations an explicit construction of some primitive elements [12]. Namely: if a is primitive in F_p, then the element $a(q+i)$ ($i=0,\ldots,p-1$) is primitive for $p<126$ and $p=137,163,167,173$. Note that a can be find by direct computations.

D. Elements of high order in recursive finite fields

It is of special interest to construct elements of high order in recursive extensions of finite fields. From the point of view of applications such a construction is very attractive, since we can perform operations with finite field elements recursively, and therefore effectively.

We obtained a lower bound on the multiplicative order of some elements in towers of finite fields of characteristic two defined by Wiedemann. Our bound does not depend on any unknown constant unlike the previous result due to Voloch. For this class of fields is posed, but not proven, the conjecture about the explicit form of some primitive elements (Wiedemann's conjecture).

We also get the bound on the order of elements in towers of finite fields of characteristic two defined by Conway. Previously any nontrivial lower bounds were not known on the order of elements in these towers. We described as well some primitive elements for the first twelve fields in the tower. More over, a condition is obtained, under which elements of this form are primitive for all fields in the tower.

We obtained a lower bound on the multiplicative order of some elements in towers of finite fields of characteristic larger than two. Previously any nontrivial lower bounds were not known on the order of elements in this case.

E. Elements of high order in general finite fields

Gao [4] gave an algorithm constructing high order elements for many (conjecturally all) general extensions F_{q^n} of finite field F_q with lower bound on the order $\exp((\log m)^2/\log\log m)$. The Gao's approach is based on the proposed by him, but not yet proved, conjecture. We improved [11] Gao method and its modification by Conflitti due to a successful definition of the set that allows to construct pair-wise different powers of the element q, which sets the extension of the initial field.

We also get some bounds that do not rely on any unproved assumptions.

IV. CONCLUSIONS

In the paper the use of three different finite cyclic groups for cryptographic information protection has been considered. The implementation of cryptographic primitives in multiplicative group of extended finite fields has been proposed. Explicit construction of high multiplicative order elements is described both for special classes of finite fields (extensions based on cyclotomic polynomials, extensions based on Kummer polynomials, extensions based on Artin-Schreier polynomials, recursive extensions (binary by Wiedemann or

Conway; non-binary), and for general finite fields. The obtained correspondent lower bounds on the order have been provided.

REFERENCES

[1] M. Agrawal, N. Kayal, N. Saxena, PRIMES is in P, Annals of Mathematics, vol. 160, no. 2, pp. 781–793, 2004.

[2] O. Ahmadi, I. E. Shparlinski, J. F. Voloch, Multiplicative order of Gauss periods, Int. J. Number Theory, vol. 6, no. 4, pp. 877–882, 2010.

[3] Q. Cheng, On the construction of finite field elements of large order, Finite Fields Appl., vol. 11, no. 3, pp. 358–366, 2005.

[4] S. Gao, Elements of provable high orders in finite fields, Proc. Amer. Math. Soc., vol. 127, no. 6, pp. 1615-1623, 1999.

[5] R. Lidl, H. Niederreiter, Finite Fields. Cambridge University Press, 1997, 755 p.

[6] A. Menezes, P. Van Oorschot, S. Vanstone. Handbook of Applied Cryptography, London, CRC Press, 1996, 794 p.

[7] G.L. Mullen, D. Panario, Handbook of finite Fields. Boca Raton: CRC Press, 2013, 1068 p.

[8] R. Popovych, Elements of high order in finite fields of the form $F_q[x]/\Phi_r(x)$, Finite Fields Appl.,. vol. 18, no. 4, pp. 700–710, 2012.

[9] R. Popovych, Elements of high order in finite fields of the form $F_q[x]/(x^m - a)$, Finite Fields Appl., vol. 19, no. 1, pp. 86-92, 2013.

[10] R. Popovych, Sharpening of explicit lower bounds on elements order for finite field extensions based on cyclotomic polynomials, Ukr. Math. Journ., vol. 66, no. 6, pp. 815-825, 2014.

[11] R. Popovych On elements of high order in general finite fields, Algebra and Discrete Mathematics, vol. 18, no.2, pp. 295-300, 2014.

[12] R. B. Popovych, Some primitive elements for the Artin–Schreier extensions of finite fields, Journal of Mathematical Sciences, vol. 210, no. 1, pp. 67–75, 2015.

R. Popovych was born in Lviv, Ukraine, in 1957. He received an engineering degree in electronic computing machines from Lviv Polytechnic University, Ukraine, in 1979 and Ph.D. degree in information and measurement systems from Physics-Mechanics Institute of the Academy of Sciences of Ukraine, Lviv, in 1988.

From 1979 to 1982 he was an Engineer with the Institute for Applied Problems of Mechanics and Mathematics of the Academy of Sciences of Ukraine. From 1982 to 1990 he did a postgraduate degree and was a Research Assistant with the Physics-Mechanics Institute of the Academy of Sciences of Ukraine. From 1990 to 1998 he was a Senior Researcher with the Research Institute of Consumer Electronics. Since 1999, he has been an Assistant Professor with the Department of Computer Engineering in National University “Lviv Polytechnic”, Lviv, Ukraine. He is the author of one book and more than 100 articles. His research interests include algebra, number theory and applications, cryptography, digital signal processing.

ACKNOWLEDGMENT

The scientific results, presented in this paper, were obtained within the frame of research project number 0115U000446, 01.01.2015 – 31.12.2017, financially supported by the Ministry of Education and Science of Ukraine