Constructing high order elements through subspace polynomials

Qi Cheng* Shuhong Gao† Daqing Wan‡

Abstract

Every finite field has many multiplicative generators. However, finding one in polynomial time is an important open problem. In fact, even finding elements of high order has not been solved satisfactorily. In this paper, we present an algorithm that for any positive integer c and prime power q, finding an element of order $\exp(\Omega(\sqrt{q^c}))$ in the finite field $\mathbb{F}_{q^{(q^c-1)/(q-1)}}$ in deterministic time $(q^c)^{O(1)}$. We also show that there are $\exp(\Omega(\sqrt{q^c}))$ many weak keys for the discrete logarithm problems in those fields with respect to certain bases.

1 Introduction

It is an important property of a finite field that for every prime power q, there is a generator for the group $\mathbb{F}_q^* = \mathbb{F}_q - \{0\}$. In fact, there are as many as $\phi(q-1) = \Omega(q/\log\log q)$ [10, Chapter 1, Theorem 5.1] generators, where ϕ is Euler's phi function. Hence if we randomly select an element in the field, with a non negligible probability, the element has order $q-1$. Nevertheless, no polynomial time algorithm is known to find an element of that order. The main difficulty lies in proving the order of an element, for which all the known approaches require the complete factorization of $q-1$. It is widely believed that factoring integers is difficult. We comment that this problem bears some similarities with many hard explicit construction problems in computer science. In those problems, we want to construct an object satisfying certain property, which holds by a randomly chosen object with high probability. It is however hard to certify that a given object has the property, thus one can not design a fast algorithm to construct such an element, even allowing randomness.

Another related question is on weak keys of discrete logarithms in finite fields. The discrete logarithm problem in a finite field $\mathbb{F}_q$ is, given $\alpha, \beta \in \mathbb{F}_q$, find an integer x so that $\alpha^x = \beta$ (such x is known to exist in applications). In practice, α is often a primitive element or of high order, and α is fixed but β varies in $\mathbb{F}_q$. For most q, the discrete logarithm problem is believed to be hard, hence form the security foundation of several public key cryptosystems. In those cryptosystems, x is often a secret key. Even though the discrete logarithm problem could be hard in $\mathbb{F}_q$ (for a fixed α), the integer x could be easily computed for some $\beta \in \mathbb{F}_q$, so such x are called weak keys for α. These weak keys should certainly be avoided as being used as secret keys. Hence it is important in practice to know how many weak keys there are.

1.1 Previous work

Given the difficulty of finding an element of full order, researchers begin to study the problem of finding an element of sufficiently high order. The attentions focus on the following problem: Fix a prime power q, finding high order elements in the extension $\mathbb{F}_{q^n}$ of $\mathbb{F}_q$. If no constraint is put in the extension degree n, very few results are known. In [7], Gao presented an efficient algorithm which constructs an element of order $\exp((\log n)^2/\log\log n))$. His algorithm assumes some reasonable but unproved conjecture. Voloch [11] proposed a method which

*School of Computer Science, University of Oklahoma, Norman, OK 73019, USA. Email: qcheng@cs.ou.edu. Partially supported by NSF under grants CCF-0830522 and CCF-0830524 and by Project 973 (no: 2007CB807903)

†Department of Mathematical Sciences, Clemson University, Clemson, SC 29634, USA. Email: sgao@clemson.edu. Partially supported by National Science Foundation under Grants DMS-1005369 and CCF-0830481.

‡Department of Mathematics, University of California, Irvine, CA 92697, USA. Email: dwan@math.uci.edu. Partially supported by NSF.

constructs an element of order $\exp(\Omega((\log n)^2))$.

If we are allowed to choose degrees of extensions, then we can construct elements of considerably higher order. One approach to construct elements of high order is through the Gauss period [8, 13, 14, 1].

PROPOSITION 1.1. *Let q be a prime power. Let r be a prime such that q is a primitive root modulo r. Let β be a primitive r-th root of unity in $\mathbb{F}_{q^{r-1}}$. Denote $(r-1)/2$ by n. Then the Gauss period $\alpha = \beta + \beta^{-1} \in \mathbb{F}_{q^n}$ has order $\exp(\Omega(\sqrt{n}))$.*

To prove that the construction works for infinitely many n, one needs to assume that the Artin conjecture holds for q. The Artin conjecture claims that if an integer a is neither -1 nor a perfect square, then there are infinitely many primes p such that a is a primitive root modulo p. It has not been proven for any a. The following proposition summarizes another approach based on the Kummer and Artin-Schreier polynomials [5].

PROPOSITION 1.2. *Let α be an element of degree d over $\mathbb{F}_q$. If it satisfies*

$$x^q + ax + b = 0,$$

where $a \in \mathbb{F}_q^*$ and $b \in \mathbb{F}_q^*$ are nonzero, then it has order greater than 2^d.

In fact, if $a = -1$ and q is a prime, then $x^q + ax + b = 0$ is irreducible over $\mathbb{F}_q$, it becomes the Artin-Schreier polynomial. If $a \neq -1$, replace x by $y - \frac{b}{a+1}$, we get $y^q - ay = 0$, which is the case of the Kummer polynomial. Note that y will have small order, but x has very large order.

COROLLARY 1.1. *Given a prime power q and a prime p such that p does not divide q, we can construct an element in $\mathbb{F}_{q^{p(p-1)}}$ with order $\exp(\Omega(p))$ in randomized time $(p \log q)^{O(1)}$ or deterministic time $(pq)^{O(1)}$.*

The above corollary provides an algorithm which constructs elements of order $\exp(\Omega(\sqrt{n}))$ in $\mathbb{F}_{q^n}$ for infinitely many n without assuming any conjecture. However the approach is based on the subfield structure. For a fixed prime q, $n = p(p-1)$ can not be prime when $p > 2$.

1.2 Our results In this paper, we contribute in two ways. We first present a new way to construct elements of high order. It is based on subspace polynomials (also called q-linearized polynomials) [9]. Subspace polynomials have found many applications in theoretical computer science [4, 2, 3], especially in explicit construction problems. Our approach can be thought as a generalization of Proposition 1.2. Our main theorem is as follows:

THEOREM 1.1. *Assume that $c \geq 2$ and $x^c + a_1 x^{c-1} + \cdots + a_c \in \mathbb{F}_q[x]$ is primitive. Let α be a root of the polynomial*

$$x^{\frac{q^c-1}{q-1}} + a_1 x^{\frac{q^{c-1}-1}{q-1}} + a_2 x^{\frac{q^{c-2}-1}{q-1}} + \cdots + a_c.$$

Then α has degree $d = (q^c-1)/(q-1)$ over $\mathbb{F}_q$ and α has order greater than $\exp(\Omega(\sqrt{q^c}))$.

COROLLARY 1.2. *Given a prime power q and a positive integer c, we can construct in time polynomial in q^c an element in $\mathbb{F}_{q^{\frac{q^c-1}{q-1}}}$ of order $\exp(\Omega(\sqrt{q^c}))$.*

Proof. We can search for a primitive polynomial over $\mathbb{F}_q$ of degree c in time $(q^c)^{O(1)}$.

Our approach constructs an element of order $\exp(\Omega(\sqrt{n}))$ in $\mathbb{F}_{q^n}$ for infinite many n without assuming any conjecture, and it is not based on subfield structures of $\mathbb{F}_{q^n}$, since both q and $(q^c-1)/(q-1)$ can be prime.

For the α constructed in Theorem 1.1, we show that the number of weak keys is at least $\exp(\Omega(\sqrt{n}))$. Those weak keys have small sum-of-digits in base q representations. See [6] for the discussion on the advantage and disadvantage of using exponents of small sum-of-digits in the discrete logarithm problem.

2 High order elements

We begin with a weaker result which generalizes Proposition 1.2. The proof of this simpler result illustrates some of the main ideas used in our later stronger result.

THEOREM 2.1. *Let c be a positive integer and let α be an element of degree $d > q^{c-1}$ over $\mathbb{F}_q$. If α satisfies*

$$x^{q^c} = a_1 x^{q^{c-1}} + a_2 x^{q^{c-2}} + \cdots + a_c x,$$

where $a_1, a_2, \cdots, a_c$ are in $\mathbb{F}_q$, then $\alpha+1$ has order greater than

$$\binom{d+\lfloor\frac{d-1}{q^{c-1}}\rfloor}{d}.$$

Proof. It is easy to see that for any $1 \le i \le d$, we have

$$(\alpha+1)^{q^i} = a_{i,1}\alpha^{q^{c-1}} + a_{i,2}\alpha^{q^{c-2}} + \cdots + a_{i,c}\alpha + 1,$$

where $(a_{i,1}, a_{i,2}, \cdots, a_{i,c}) \in \mathbb{F}_q^c$ and for any i, j, $1 \le i < j \le d$, we have

$$(a_{i,1}, a_{i,2}, \cdots, a_{i,c}) \neq (a_{j,1}, a_{j,2}, \cdots, a_{j,c}).$$

We claim that if $(y_1, y_2, \cdots, y_d)$ and $(z_1, z_2, \cdots, z_d)$ are different non-negative integer vectors with weights $\sum_i y_i$ and $\sum_i z_i$ bounded by $\lfloor\frac{d-1}{q^{c-1}}\rfloor$, then

$$\prod_{i=1}^{d}(\alpha+1)^{y_i q^i} \neq \prod_{i=1}^{d}(\alpha+1)^{z_i q^i}.$$

To prove it, we need to show

$$\begin{aligned}&\prod_{i=1}^{d}(a_{i,1}\alpha^{q^{c-1}} + a_{i,2}\alpha^{q^{c-2}} + \cdots + a_{i,c}\alpha + 1)^{y_i}\\ \neq\ &\prod_{i=1}^{d}(a_{i,1}\alpha^{q^{c-1}} + a_{i,2}\alpha^{q^{c-2}} + \cdots + a_{i,c}\alpha + 1)^{z_i}.\end{aligned}$$

Since α has degree d which is greater than

$$\max(\sum_i y_i, \sum_i z_i)q^{c-1},$$

it is equivalent to show

$$\begin{aligned}&\prod_{i=1}^{d}(a_{i,1}x^{q^{c-1}} + a_{i,2}x^{q^{c-2}} + \cdots + a_{i,c}x + 1)^{y_i}\\ \neq\ &\prod_{i=1}^{d}(a_{i,1}x^{q^{c-1}} + a_{i,2}x^{q^{c-2}} + \cdots + a_{i,c}x + 1)^{z_i}\end{aligned}$$

in $\mathbb{F}_q[x]$. Since the non-negative integer vectors $(y_1, \cdots, y_d)$ and $(z_1, \cdots, z_d)$ have weights at most $(d-1)/q^{c-1} < q^c/q^{c-1} = q$, we deduce that he desired non-identity is equivalent to the following non-identity

$$\begin{aligned}&\prod_{i=1}^{d}(a_{i,1}x_{c-1} + a_{i,2}x_{c-2} + \cdots + a_{i,c}x_0 + 1)^{y_i}\\ \neq\ &\prod_{i=1}^{d}(a_{i,1}x_{c-1} + a_{i,2}x_{c-2} + \cdots + a_{i,c}x_0 + 1)^{z_i}\end{aligned}$$

in $\mathbb{F}_q[x_0, x_1, \cdots, x_{c-1}]$, which is true because of the unique factorization in $\mathbb{F}_q[x_0, x_1, \cdots, x_{c-1}]$. The order of $\alpha+1$ is thus greater than the number of non-negative integer vectors of length d and weight at most $\lfloor\frac{d-1}{q^{c-1}}\rfloor$.

If $d = q^c - 1$, then the above result can be greatly improved. First there is a well-known fact about subspace polynomials.

LEMMA 2.1. *The q-polynomial $(a_0x + a_1x^q + a_2x^{q^2} + \cdots + a_kx^{q^k})/x \in \mathbb{F}_q[x]$ is irreducible if and only if $a_0 + a_1x + \cdots + a_kx^k$ is a primitive polynomial in $\mathbb{F}_q[x]$.*

For a q-polynomial $r(x) = a_0x + a_1x^q + \cdots + a_kx^{q^k}$ over $\mathbb{F}_q$, the quotient

$$\frac{r(x)}{x} = a_0 + a_1x^{q-1} + \cdots + a_kx^{q^k-1}$$

is called quasi-irreducible if

$$r^*(x) = a_0 + a_1x^{\frac{q-1}{q-1}} + \cdots + a_kx^{\frac{q^k-1}{q-1}}$$

is irreducible over $\mathbb{F}_q$ and $r^*(x) \neq x$. Note that

$$\frac{r(x)}{x} = r^*(x^{q-1}).$$

Thus, if $r(x)/x$ is irreducible, then it is quasi-irreducible. The converse may not be true. Furthermore, if $(r_1^*(x), r_2^*(x)) = 1$, then there exists polynomials $\alpha_1(x)$ and $\alpha_2(x)$ such that $r_1^*(x)\alpha_1(x) + r_2^*(x)\alpha_2(x) = 1$. So $r_1^*(x^{q-1})\alpha_1(x^{q-1}) + r_2^*(x^{q-1})\alpha_2(x^{q-1}) = 1$, which implies

$$(\frac{r_1(x)}{x}, \frac{r_2(x)}{x}) = 1.$$

For a prime power q and a positive integer k, define

$$\begin{aligned}R(q,k) \ =\ &\big\{r(x) \in \mathbb{F}_q[x] | r(x) \text{ is a monic } q-\text{polynomial of}\\ &\text{degree } q^k \text{ and } r(x)/x \text{ is quasi} - \text{irreducible}\big\}.\end{aligned}$$

Certainly $|R(q,k)| \le q^k$. The above lemma shows that

$$|R(q,k)| \ge \phi(q^k - 1)/k.$$

THEOREM 2.2. *Let $c \ge 2$ be a positive integer and let $x^c + a_1x^{c-1} + \cdots + a_c \in \mathbb{F}_q[x]$ be a primitive*

polynomial. Let α be a non-zero root of the q-polynomial

$$x^{q^c} + a_1 x^{q^{c-1}} + a_2 x^{q^{c-2}} + \cdots + a_c x.$$

Then α has degree $d = q^c - 1$ over $\mathbb{F}_q$ and α has order greater than

$$\binom{|R(q, \lfloor c/2 \rfloor)| + \frac{q^c-1}{q^{\lfloor c/2 \rfloor}}}{|R(q, \lfloor c/2 \rfloor)|} = \exp(\Omega(\sqrt{q^c}))$$

Proof. The primitive polynomial assumption and the lemma imply that α has degree $d = q^c - 1$. It is then easy to see that for any $0 \le j \le d-1$, we can write

$$\alpha^{q^j} = a_{j,1}\alpha^{q^{c-1}} + a_{j,2}\alpha^{q^{c-2}} + \cdots + a_{j,c}\alpha,$$

where $(a_{j,1}, a_{j,2}, \cdots, a_{j,c}) \in \mathbb{F}_q^c - \{0\}^c$ and for $0 \le j \le d-1$, $(a_{j,1}, a_{j,2}, \cdots, a_{j,c})$ runs over all the element in $\mathbb{F}_q^c - \{0\}^c$, since α has $q^c - 1$ conjugates over $\mathbb{F}_q$.

Denote $|R(q, \lfloor c/2 \rfloor)|$ by m. For $1 \le i \le m$, let $r_i(x) \in \mathbb{F}_q[x]$ be an enumeration of polynomials in $R(q, \lfloor c/2 \rfloor)$, and j_i be the corresponding integer such that $\alpha^{q^{j_i}} = r_i(\alpha)$. In particular, $r_i^*(x) \ne x$. We claim that if $(y_1, y_2, \cdots, y_m)$ and $(z_1, z_2, \cdots, z_m)$ are different in $(\mathbb{Z}_{\ge 0})^m$ with

$$\max(\sum_{i=1}^m y_i, \sum_{i=1}^m z_i) < \frac{q^c - 1}{q^{\lfloor c/2 \rfloor}},$$

then

$$\prod_{i=1}^m (\alpha)^{y_i q^{j_i}} \ne \prod_{i=1}^m (\alpha)^{z_i q^{j_i}}.$$

To prove it, we need to show

$$\prod_{i=1}^m (r_i(\alpha))^{y_i} \ne \prod_{i=1}^m (r_i(\alpha))^{z_i}.$$

Since

$$\max(\sum_{i=1}^m y_i, \sum_{i=1}^m z_i) q^{\lfloor c/2 \rfloor} < q^c - 1 = d,$$

it is equivalent to showing

$$\prod_{i=1}^m (r_i(x))^{y_i} \ne \prod_{i=1}^m (r_i(x))^{z_i},$$

that is,

$$x^{\sum_i y_i - \sum_i z_i} \prod_{i=1}^m (r_i(x)/x)^{y_i} \ne \prod_{i=1}^m (r_i(x)/x)^{z_i}.$$

This is true by unique factorization. Thus the order of α is greater than or equal to the number of non negative integer solutions of

$$\sum_{i=1}^m y_i < \frac{q^c - 1}{q^{\lfloor c/2 \rfloor}}.$$

This concludes the proof.

2.1 Proof of Theorem 1.1

THEOREM 2.3. *Assume that $c \ge 2$ and $x^c + a_1 x^{c-1} + \cdots + a_c \in \mathbb{F}_q[x]$ is primitive. Let e be a positive divisor of $q-1$. Let β be a root of the polynomial*

$$f_e(x) = x^{\frac{q^c-1}{e}} + a_1 x^{\frac{q^{c-1}-1}{e}} + a_2 x^{\frac{q^{c-2}-1}{e}} + \cdots + a_c.$$

Then β has degree $d = (q^c - 1)/e$ and β has order greater than $\exp(\Omega(\sqrt{q^c}))$.

Proof. Write $\beta = \alpha^e$. Then, α is a non-zero root of the q-polynomial

$$x^{q^c} + a_1 x^{q^{c-1}} + \cdots + a_c x,$$

and

$$\mathrm{ord}(\beta) = \frac{1}{e}\mathrm{ord}(\alpha).$$

If $f_e(x)$ were reducible, then $f(x^e) = (x^{q^c} + a_1 x^{q^{c-1}} + a_2 x^{q^{c-2}} + \cdots + a_c x)/x$ would be reducible, which is a contradiction. We can now apply the previous theorem.

The case $e = 1$ is just Theorem 2.2. Taking $e = q - 1$, we obtain Theorem 1.1.

2.2 The case of $c = 2$ In the case $c = 2$, the order can be significantly improved.

THEOREM 2.4. *Assume that α is an element of degree d over $\mathbb{F}_q$ and it satisfies*

$$\alpha^{q+1} - a_1\alpha - b_1 = 0$$

The order of α is at least 5.8^d.

Proof. We define an iterative sequence:

$$\begin{aligned} a_{i+1} &= a_i a_1 + b_i \\ b_{i+1} &= a_i b_1 \end{aligned}$$

Or equivalently

$$\begin{pmatrix} a_{i+1} \\ b_{i+1} \end{pmatrix} = \begin{pmatrix} a_1 & 1 \\ b_1 & 0 \end{pmatrix} \begin{pmatrix} a_i \\ b_i \end{pmatrix}$$

Note that

$$\begin{aligned}\alpha^q &= \frac{a_1\alpha+b_1}{\alpha}\\ \alpha^{q^2} &= \frac{a_2\alpha+b_2}{a_1\alpha+b_1}\\ &\vdots\\ \alpha^{q^{d-1}} &= \frac{b_{d-1}}{a_{d-2}\alpha+b_{d-2}}\\ \alpha^{q^d} &= \alpha.\end{aligned}$$

Also note that the condition $\alpha^{q^d}=\alpha$ implies that $a_{d-1}=b_d=0$ and $a_d=b_{d-1}$. We may assume that $a_0=1, b_0=0$. We claim that if we view (a_i,b_i), $0\le i\le d-1$ as points on the projective line $P^1(\mathbb{F}_q)$, then they are distinct. Otherwise for some $0\le i<j\le d-1$, we have $(a_i,b_i)=(a_j,b_j)$ and

$$\alpha^{(q-1)(q^{i+1}+\cdots+q^j)}=(\frac{a_j\alpha+b_j}{a_i\alpha+b_i})^{q-1}=1.$$

This implies that $\alpha^{q^{j-i}}=\alpha$. Since α has degree d over F_q, we must have $d|(j-i)$. The distinctness of these projective points implies that $a_ib_i\neq 0$ for $1\le i\le d-2$.

For a list of integers $(n_0,n_1,\cdots,n_{d-1})$ we have

$$\begin{aligned}&\alpha^{n_0+n_1q+n_2q^2+\cdots+n_{d-1}q^{d-1}}\\ =\;&\alpha^{n_0-n_1}(a_1\alpha+b_1)^{n_1-n_2}\cdots\\ &(a_{d-2}\alpha+b_{d-2})^{n_{d-2}-n_{d-1}}b_{d-1}^{n_{d-1}}.\end{aligned}$$

Consider the set of integer lists:

$$\begin{aligned}S = \big\{&(n_0,n_1,\cdots,n_{d-1})\in\mathbb{Z}^d\big|n_{d-1}=0,\\ &\sum_{n_i-n_{i-1}\ge 0} n_i-n_{i-1}\le (d-1)/2,\\ &\sum_{n_i-n_{i-1}<0} n_{i-1}-n_i\le (d-1)/2\big\},\end{aligned}$$

It follows from the unique factorization property of $\mathbb{F}_q[x]$ that as $(n_0,n_1,\cdots,n_{d-1})$ runs over the elements of S, the elements

$$\alpha^{n_0+n_1q+n_2q^2+\cdots+n_{d-1}q^{d-1}}$$

are distinct. So the order of α is greater than or equal to the cardinality of S, which is equal to the cardinality

$$\begin{aligned}T = \big\{&(m_0,m_1,\cdots,m_{d-2})\in\mathbb{Z}^{d-1}\big|\\ &\sum_{m_i\ge 0} m_i\le (d-1)/2\\ &\sum_{m_i<0}|m_i|\le (d-1)/2\big\}.\end{aligned}$$

The following set is a subset of T:

$$\left\{(m_0,m_1,\cdots,m_{d-2})\in\mathbb{Z}^{d-1}\Big|\begin{array}{r}\sum_{m_i\ge 0} m_i=\lfloor(d-1)/2\rfloor\\ \sum_{m_i<0}|m_i|=\lfloor(d-1)/2\rfloor\\ \sum_{m_i<0}1=d_-\end{array}\right\},$$

whose cardinality is

$$\binom{d-1}{d_-}\binom{\lfloor(d-1)/2\rfloor}{d_-}\binom{\lfloor(d-1)/2\rfloor+(d-1-d_-)-1}{d-1-d_-},$$

which is at least 5.8^d if we set $d_-=0.292d$.

COROLLARY 2.1. *Given a prime power q and an integer $t|q+1$, we can construct an element in $\mathbb{F}_{q^t}$ with order $\exp(\Omega(t))$ in deterministic time $q^{O(1)}$, or randomized time $(t\log q)^{O(1)}$.*

COROLLARY 2.2. *Given a prime power q and a prime p such that p does not divide q, we can construct an element in $\mathbb{F}_{q^{p(p-1)/2}}$ with order $\exp(\Omega(p))$ in randomized time $(p\log q)^{O(1)}$ and deterministic time $(pq)^{O(1)}$.*

Proof. Since $p|q^{p-1}-1=(q^{(p-1)/2}-1)(q^{(p-1)/2}+1)$. Either $p|q^{(p-1)/2}-1$ or $p|q^{(p-1)/2}+1$.

3 Weak keys for the discrete logarithm problem

In this section, we show that the discrete logarithm problem using generators arising from our larger order construction has a large number of weaker keys. The following lemma was proved in [12]:

LEMMA 3.1. *There exists an algorithm, that given $h(x)\in\mathbb{F}_q[x]$ of degree d and $f(x)\in\mathbb{F}_q[x]$ of degree less than d, finds two polynomials $f_1(x)$ and $f_2(x)$ of degree less than or equal to $\lfloor(d-1)/2\rfloor$ such that*

$$f(x)f_1(x)\equiv f_2(x)\pmod{h(x)},$$

and the algorithm runs in time $O((d\log q)^{O(1)})$.

THEOREM 3.1. *Assume that α is an element of degree d over $\mathbb{F}_q$ and it satisfies*

$$\alpha^{q+1} - a_1\alpha - b_1 = 0.$$

Let $(n_0, n_1, \cdots, n_{d-1})$ be a list of integers in

$$\begin{aligned} S &= \big\{(n_0, n_1, \cdots, n_{d-1}) \in \mathbb{Z}^d \big| n_{d-1} = 0, \\ &\quad \sum_{n_i - n_{i-1} \geq 0} n_i - n_{i-1} \leq (d-1)/2, \\ &\quad \sum_{n_i - n_{i-1} < 0} n_{i-1} - n_i \leq (d-1)/2\big\}, \end{aligned}$$

Then there is a polynomial time algorithm that given $f(x) \in \mathbb{F}_q[x]$ such that $f(\alpha) = \alpha^{n_0+n_1q+n_2q^2+\cdots+n_{d-1}q^{d-1}}$ computes $(n_0, n_1, \cdots, n_{d-1})$.

The number of weak keys is at least 5.8^d, better than previous result 5.17^d.

Let $c \geq 2$ be a positive integer and let $x^c + a_1x^{c-1} + \cdots + a_c \in \mathbb{F}_q[x]$ be a primitive polynomial. Let α be a non-zero root of the q-polynomial

$$x^{q^c} + a_1x^{q^{c-1}} + a_2x^{q^{c-2}} + \cdots + a_cx.$$

Define

$$\begin{aligned} J &= \big\{j | \exists r(x) \in R(q, \lfloor c/2 \rfloor) \\ &\quad \text{such that } \alpha^{q^j} = r(\alpha)\big\} \end{aligned}$$

Let $d = q^c - 1$. Define

$$\begin{aligned} S &= \big\{(n_0, n_1, \cdots, n_{d-1}) \in \mathbb{Z}^d_{\geq 0} \big| \\ &\quad \sum_j n_j < \frac{q^c - 1}{q^{\lfloor c/2 \rfloor}} \\ &\quad n_j = 0 \text{ if } j \notin J\big\}. \end{aligned}$$

THEOREM 3.2. *There is a polynomial time algorithm that given $f(x) \in \mathbb{F}_q[x]$ of degree no more than $q^c - 1$ such that $f(\alpha) = \alpha^{n_0+n_1q+n_2q^2+\cdots+n_{d-1}q^{d-1}}$ computes $(n_0, n_1, \cdots, n_{d-1})$.*

The number of weak keys is at least

$$\binom{|R(q, \lfloor c/2 \rfloor)| + \frac{q^c-1}{q^{\lfloor c/2 \rfloor}}}{|R(q, \lfloor c/2 \rfloor)|} = \exp(\Omega(\sqrt{q^c}))$$

Proof. For $1 \leq i \leq |R(q, \lfloor c/2 \rfloor)|$, let $r_i(x)$ be an enumeration of polynomials in $R(q, \lfloor c/2 \rfloor)$ and let $j_i \in J$ be the corresponding integer such that such that $\alpha^{q^{j_i}} = r_i(\alpha)$. We have the equality

$$f(x) = \prod_{i=1}^{m} r_i(x)^{n_{j_i}}$$

over $\mathbb{F}_q[x]$. List all the polynomials $r_1(x), \cdots, r_m(x)$ in a table. This can be done in polynomial time. Try the maximal power of $r_i(x)$ which divides $f(x)$. This recovers all n_j.

Similarly, we have

THEOREM 3.3. *Let e be a divisor of $q-1$. Let β be a root of the irreducible polynomial*

$$x^{\frac{q^c-1}{e}} + a_1x^{\frac{q^{c-1}-1}{e}} + a_2x^{\frac{q^{c-2}-1}{e}} + \cdots + a_c.$$

Let $d = (q^c - 1)$ (this is NOT the degree of β now) and let $(n_0, n_1, \cdots, n_{d-1})$ be a vector in

$$\begin{aligned} S' &= \big\{(n_0, n_1, \cdots, n_{d-1}) \in \mathbb{Z}^d_{\geq 0} \big| \\ &\quad \sum_j n_j \equiv 0 \ (\mod e), \ \sum_j n_j < \frac{q^c - 1}{q^{\lfloor c/2 \rfloor}} \\ &\quad n_j = 0 \text{ if } j \notin J\big\}. \end{aligned}$$

Then there is a polynomial time algorithm that given $f(x) \in \mathbb{F}_q[x]$ such that

$$f(\beta) = \beta^{\frac{n_0+n_1q+\cdots+n_{d-1}q^{d-1}}{e}}$$

computes $(n_0, n_1, \cdots, n_{d-1})$.

Proof. Note that the exponent $\frac{n_0+n_1q+\cdots+n_{d-1}q^{d-1}}{e}$ is an integer since $\sum_j n_j$ is divisible by e. W.l.o.g, assume that $\beta = \alpha^e$. By the previous theorem, the exponent of α in

$$\alpha^{n_0+n_1q+n_2q^2+\cdots+n_{d-1}q^{d-1}} = \beta^{\frac{n_0+n_1q+\cdots+n_{d-1}q^{d-1}}{e}}$$

can be found in polynomial time.

Note that the number of weak keys is simply the number of elements in S'. The most interesting case is when $e = q - 1$. We obtain

COROLLARY 3.1. *Let β be a root of the irreducible polynomial*

$$x^{\frac{q^c-1}{q-1}} + a_1x^{\frac{q^{c-1}-1}{q-1}} + a_2x^{\frac{q^{c-2}-1}{q-1}} + \cdots + a_c.$$

Let $d = (q^c - 1)$ (this is NOT the degree of β now) and let $(n_0, n_1, \cdots, n_{d-1})$ be a vector in

$$\begin{aligned} S' \quad = \quad & \Big\{(n_0, n_1, \cdots, n_{d-1}) \in \mathbb{Z}_{\geq 0}^d \Big| \\ & \sum_j n_j \equiv 0 \ (\mod q-1), \ \sum_j n_j < \frac{q^c - 1}{q^{\lfloor c/2 \rfloor}} \\ & n_j = 0 \text{ if } j \notin J \Big\}. \end{aligned}$$

Then there is a polynomial time algorithm that given $f(x) \in \mathbb{F}_q[x]$ such that

$$f(\beta) = \beta^{\frac{n_0 + n_1 q + \cdots + n_{d-1} q^{d-1}}{q-1}}$$

computes $(n_0, n_1, \cdots, n_{d-1})$.

4 Open problems

Many important problems about constructing high order element remain open:

1. Given a prime power q and a positive integer t, construct an element in $\mathbb{F}_{q^t}$ with order $\exp(\Omega(t))$ in randomized time $(qt)^{O(1)}$.

2. Given a prime p, finds an element of order $\exp(\Omega((\log p)^c))$ in $\mathbb{F}_p$ in time $(\log p)^{O(1)}$, for some positive constant $c \leq 1$.

References

[1] Omran Ahmadi, Igor Shparlinski, and Jose Felipe Voloch. Multiplicative order of gauss periods. *International Journal of Number Theory*, 6(4):877–882, 2010.

[2] Eli Ben-Sasson, Oded Goldreich, Prahladh Harsha, Madhu Sudan, and Salil Vadhan. Robust pcps of proximity, shorter pcps and applications to coding. In *STOC 2004*, 2004.

[3] Eli Ben-Sasson and Swastik Kopparty. Affine dispersers from subspace polynomials. In *The 41st ACM Symposium on Theory of Computing (STOC 2009)*, 2009.

[4] Eli Ben-Sasson, Swastik Kopparty, and Jaikumar Radhakrishnan. Subspace polynomials and list decoding of Reed-Solomon codes. In *47th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 207–216, 2006.

[5] Qi Cheng. Constructing finite field extensions with large order elements. In *ACM-SIAM Symposium on Discrete Algorithms (SODA)*, pages 1123–1124, 2004.

[6] Qi Cheng. On the bounded sum-of-digits discrete logarithm problem in finite fields. *SIAM Journal on Computing*, 34(6):1432–1442, 2005.

[7] Shuhong Gao. Elements of provable high orders in finite fields. *Proc. American Mathematical Society*, 127:1615–1623, 1999.

[8] Shuhong Gao and Scott A. Vanstone. On orders of optimal normal basis generators. *Mathematics of Computation*, 64:1227–1233, 1995.

[9] Rudolf Lidl and Harald Niederreiter. *Finite Fields (2nd ed.)*. Cambridge University Press, 1997.

[10] Karl Prachar. *Primzahlverteilung*. Springer-Verlag, 1957.

[11] Jose F. Voloch. On the order of points on curves over finite fields. *Integers*, 7, 2004.

[12] Joachim von zur Gathen and Jürgen Gerhard. *Modern Computer Algebra*, volume 3. Springer-Verlag, 1999.

[13] Joachim von zur Gathen and Igor Shparlinski. Orders of Gauss periods in finite fields. In *Proc. 6th Intern. Symp. on Algorithms and Computation*, volume 1004 of *Lecture Notes in Computer Science*. Springer-Verlag, 1995. Also appeared as Orders of Gauss periods in finite fields. Applicable Algebra in Engineering, Communication and Computing, **9** (1998), 15–24.

[14] Joachim von zur Gathen and Igor Shparlinski. Gauss periods in finite fields. In *Proc. 5th Conference of Finite Fields and their Applications*, pages 162–177. Springer-Verlag, 1999.