Pairing inversion for finding discrete logarithms

Cherepniy M.A.

supported by grant от м2 13-01-12420
email: cherepniy@gmail.com

This topic explains inversion algorithm for pairings. This technique may be utilized for breaking Diffie-Hellman Protocol on the elliptic curves [1] and for solving discrete logarithm problem on some curves, that satisfy GOST P.34.10-2012.

1 Introduction

Let utilized cyclic group $< P >$ on some elliptic curve has prime order $p$. Let $p - 1 = \prod_{i=1}^{t} q_i^{a_i}$. GOST P34.10-2012 does not impose any restrictions on such expansion, so we will consider it as ordinary. So, if

$$\psi(x, y) = \#\{1 \leq n \leq x \mid \text{ for every prime divisor } q \text{ of } n \text{ we have } q < y\},$$

then for fixed $u \geq 3, x \geq 1$ ([3] Theorem 3.1)

$$\psi(x, \sqrt{x}) \geq \frac{x}{u^{n(1+o(1))}}. \quad (1)$$

So, we have $q_i \leq \sqrt[y]{x}$ for fixed $u$ with constant probability.

For group of points on elliptic curve $E[\mathbb{F}_r]$ over finite field $\mathbb{F}_r$, where $r$ is prime, let’s denote a sum of $n$ points $P$ as $[n]P$.

Let two knowing points $Q, P \in E[\mathbb{F}_r]$ satisfy

$$Q = [n]P,$$

and we must obtain $n$, that is defined modulo $p = \text{ord}P$. We will denote the complexity of this problem as $\text{DLE}(r, p)$, and the complexity of calculation $[n_1n_2]P$ by pair $([n_1]P, [n_2]P)$ we will denote $\text{DHE}(r, p)$. We assume that the last problem harder than one operation on elliptic curve $E[\mathbb{F}_r]$. Let’s denote logarithm with some fixed base, that will be some effective constant as $\log$.

**Theorem 1** $\text{DLE}(r, p) \leq \text{DHE}(r, p)\log p \sum_{i=1}^{t} q_i^{a_i}$. 
Proof. It’s evident, that \( n \equiv 0 \pmod{p} \) if and only if \( Q \) is an infinity. Otherwise \( n \equiv g^h \pmod{p} \), where \( g \) is a primitive root mod \( p \), and \( h \) defined \( \pmod{p-1} \). Further we will look for \( h \) instead of \( n \).

Note, that point set \([n]P, n \not\equiv 0 \pmod{p} \) forms a cyclic group with order \( p-1 \) with respect to the operation

\[
[n_1]P \ast [n_2]P = [n_1n_2]P,
\]

that we will denote as \( G \).

Let \( q \mid p-1 \). We will look over \( j_0', j''_0 \in \{1, \ldots, \frac{p-1}{q} \} \) and check, if there exists such \( i \in \{0,1,\ldots,q-1\} \), that

\[
[g^{j_0'}]Q = [g^{j''_0}][g^{\frac{p-1}{q}i}]P,
\]

If yes, than

\[
n \equiv g^{j''_0}g^{p-1-\frac{2}{q}j''_0}(modp),
\]

or

\[
h \equiv j''_0 - j'_0 + \frac{p-1}{q}i(mod(p-1)),
\]

or

\[
h \equiv j''_0 - j'_0 \pmod{\frac{p-1}{q}}.
\]

For construction

\[
[g^{j_0'}]Q, [g^{j''_0}]P
\]

we need \( 4\log_2p \leq \log p \) additional operations on the elliptic curve.

According to the known birth day paradox theorem [4], the mean number of pairs \((j_0', j''_0, j_0'), j''_0 \in \{1, \ldots, \frac{p-1}{q} \}, \) that we must check before it will be obtained the situation when \( i \) exist, is equal to \((\sqrt{\frac{p-1}{q}} + O(1))^2 \). \( j''_0 \) and \( j''_0 \) pass some random independent subsets in \( \{1, \ldots, \frac{p-1}{q} \} \) with cardinality \( \sqrt{\frac{p-1}{q}} + O(1) \). Note, that, instead of random passing we may consider \( j''_0 = 0, j_0' \in \{1, \ldots, \frac{p-1}{q} \}, \) that will raise the cardinality of corresponding sets, but won’t change the number of checks.

If instead of \( q \) we utilize such \( \tilde{q}_j \), that satisfy \( \text{HOK} \left[ \frac{p-1}{\tilde{q}} \right] = p-1 \), using the Chinese remainder theorem, then we will obtain \( h(mod(p-1)) \). So, the mean number of checks is
\[ O(\sum_j \pi^{p-1}_{q_j}), \]

that in case of \( \tilde{q}_j = \frac{p-1}{q_j}, j = 1, \ldots, t \), gives

\[ O(\sum_{i=1}^t q_i^{a_i}). \] (4)

Equality (2) means that

\[ Q_{j_0+p-1-j_0'} = [g_{j_0+p-1-j_0'}]Q \in G_{0, \frac{p-1}{q}} = \{ [g_\frac{p-1}{q}]P \mid i = 0, 1, \ldots, q - 1 \}. \] (5)

The calculation of \( Q_{j_0+p-1-j_0'} \) when \( j_0, j_0' \) are known, according to quadratic algorithm requires no more than \( 2\log_2 p \) multiplications \((mod p)\) and \( 2\log_2 p \) additions on elliptic curve, that are more complicated (corresponding formulas require 5 multiplications in the field per one addition on elliptic curve).

Note, that \( G_{0, \frac{p-1}{q}} \) is a cyclic subgroup of \( G \) and its order is \( q \). Let’s denote, that [13]

\[ k \cdot [n]P = \underbrace{[n]P \ast \cdots \ast [n]P}_{k} = [n^k]P. \]

Now the question about including (5) is the question about solvability of discrete logarithm problem in cyclic group \( G \). As far as subgroup of order \( q \) is unique in that group, this including exists if and only if when

\[ \underbrace{Q_{j_0+p-1-j_0'} \ast \cdots \ast Q_{j_0+p-1-j_0'}}_q = [1]P = P, \] (6)

that can be checked with complexity \( 2DHE(r, p) \log_2 q \). The end.

In general case [13]

\[ DLE(r, p) \leq O(s(p)\log^2 p(DHE(r, p))^{s(p)}), \]

where \( s(p) \) is the length of the longest branch of Pratt tree [2], for which we have only trivial bound \( s(p) \leq \log_2 p \) (today see some more in [9]).
2 Calculation and utilization of pairings and their inversions

2.1 The utilization of pairings for solving Diffie-Hellman problem

**Definition.**[1] Let $G_1, G_2, G_T$ be cyclic groups. Pairing is the map

$$e : G_1 \times G_2 \to G_T.$$  

We will consider bilinear with respect to group operations nondegenerate pairings.  

Let $f_1, f_2, f_T$ be the unique elements of the corresponding groups $G_1, G_2, G_T$. Then $e(f_1, G_2) = e(G_1, f_2) = f_T$ by definition. Let’s consider the case when $|G_1| = |G_2| = |G_T| = p$ is prime. In this case pairing $e$ is non-degenerate if and only if there exist such $g_1, g_2, g_T$ in the corresponding sets $G_1 \setminus f_1, G_2 \setminus f_2, G_T \setminus f_T$, that $e(g_1, g_2) = g_T$. For arbitrary $h_1 \in G_1, h_T \in G_T$ there exists such a $h_2 \in G_2$, and for arbitrary $h_2 \in G_2, h_T \in G_T$ there exist such a $h_1 \in G_1$, that $e(h_1, h_2) = h_T$.

Let’s consider the following problems[1]:

\[ FAPI - 1 : D_1 \in G_1, z \in G_T \to D_2 \in G_2 : e(D_1, D_2) = z, \]

\[ FAPI - 2 : D_2 \in G_2, z \in G_T \to D_1 \in G_1 : e(D_1, D_2) = z, \]

\[ GPI - 2 : z \in G_T \to D_1 \in G_1, D_2 \in G_2 : e(D_1, D_2) = z. \]

Let’s denote the corresponding complexities of these problems $I_1, I_2, I_T$. Let’s denote the corresponding oracles $O_1, O_2, O_T$, and complexity of pairing calculation we’ll denote $C$. As far as $p$ is prime and $e$ is nondegenerate, the solution of $FAPI - i$ is unique. Let’s denote $DH(G_i)$ the complexity of solving Diffie-Hellman problem in $G_i$.

**Theorem 2** ([1, Theorem 1])

$$DH(G_i) \leq I_1 + I_2 + 2C, i \in \{1, 2\}. \quad (7)$$
Below we will consider the case, when \( G_2 \) is a finite group with not prime order, but it has a prime \( p \) as a universal exponent. The complexity of solving \( FAPI - 2 \) in this case (finding at least one solution) we will denote as \( \tilde{I}_2 \).

Analogous to proof of Theorem 2, we obtain some similar bound. Let \((P, aP, bP)\) be the elements of \( G_1 \), that are, at the same time, arguments of Diffie-Hellman problem in \( G_1 \). Let \( z = e(aP, Q) = e(P, aQ) \) for arbitrary argument \( Q \in G_2 \), for which \( z \neq f_T \). Let \( O_1(P, z) = \tilde{Q} : e(P, \tilde{Q}) = e(aP, Q) \), then \( \tilde{z}' = e(bP, \tilde{Q}) = e(abP, Q) \). So \( O_2(\tilde{z}', Q) = abP \). So, we obtain the bound for complexity \( DH(G_1) \) of Diffie-Hellman problem in \( G_1 \):

\[
DH(G_1) \leq I_1 + \tilde{I}_2 + 2C, i \in \{1, 2\}.
\]

By theorem 1 we obtain

\[
DLE(r, p) \leq \log p(I_1 + \tilde{I}_2 + 2C) \sum_{i=1}^{I} q_i^{a_i}.
\]

Let’s consider the function \( f_{s, Q} \) for arbitrary integer \( s \), defined by equation

\[
div(f_{s, Q}) = s(Q) - (sQ) - (s - 1)(\infty).
\]  \hspace{1cm} \hspace{1cm} (8)

According to [5, Corollary III.3.5.], such function exists. Pairing is often [10, 11] defined by formula

\[
f_{s, Q}(D_2) = \prod_{P \in \text{Supp} D_2} f_{s, Q}(P)^{\nu_{P}(D_2)}.
\]

Let \( u \) be the uniformization parameter at infinity, \( \nu_{\infty}(f) \) is an order of function \( f \) at infinity, then denote \( \nu_{\infty}(f) = (u^{-\nu_{\infty}(f)})/(\infty) \). Denote \( f^{\text{norm}} = (\nu_{\infty}(f))^{-1}f \). To obtain uniqueness in definition \( f_{s, Q}(D_2) \), we replace \( f \) by \( f^{\text{norm}} \).

Values \( f_{s, Q}(D_2) \) and corresponding pairings may be calculated with the help of algorithm of Davenport [6] - Miller [7] and its generalizations [8]. This algorithm is linear relating to length of argument. For example, the calculation of Weil pairing demands \( O(k\log r) \) operations in the field \( \mathbb{F}_q, q = r^k \), or \( O(k^3 \log^3 r) \) bit operations.

Let us have base-2 representation \( s = \sigma_{l-1} \ldots \sigma_0; \sigma_{l-1} = 1 \), and points \( P = (x_1, y_1) \in E(\mathbb{F}_r)[p], Q = (x_2, y_2) \in E(\mathbb{F}_q) \). Miller algorithm:

1. \( T \leftarrow P, f_1 \leftarrow 1, f_2 \leftarrow 1 \)
2. for $i = l - 2$ to 0
3. $T \leftarrow [2]T \quad (T = (x_3, y_3))$
4. $\lambda \leftarrow$ the slope of the tangent of $E$ at $T$.
5. $f_1 \leftarrow f_1^2(y_2 - \lambda(x_2 - x_3) - y_3)$
6. $f_2 \leftarrow f_2^2(x_2 + (x_1 + x_3) - \lambda^2)$
7. if $\sigma_i = 1$ then
8. $T \leftarrow T \oplus P$
9. $\lambda \leftarrow$ the slope of the line through $T$ and $P$
10. $f_1 \leftarrow f_1(y_2 - \lambda(x_2 - x_3) - y_3)$
11. $f_2 \leftarrow f_2(x_2 + (x_1 + x_3) - \lambda^2)$, and for
12. return $f_{s,P}(Q) = \frac{f_1}{f_2}$

Mention, that $\lambda$ doesn’t depend on $Q$. So when $P$ is known, we have $\text{deg}_{x_2} f_1, \text{deg}_{y_2} f_1, \text{deg}_{x_2} f_2, \text{deg}_{y_2} f_2 \leq s$ as polynomials. For fixed $Q$, according to the double formulas, we obtain

$$\text{deg}_{y_1} y_3 = 2, \text{deg}_{x_1} y_3 = 3, \text{deg}_{y_1} x_3 = 2, \text{deg}_{x_1} x_3 = 4, \text{deg}_{y_3} \lambda = 2, \text{deg}_{x_3} \lambda = 1.$$ 

So, on the $i$-step of the algorithm we have

$$\text{deg}_{y_1} y_3, \text{deg}_{y_1} x_3 = 2 \leq 2^i, \text{deg}_{x_1} y_3 \leq \text{deg}_{x_1} x_3 \leq 4^i.$$ 

All degrees are bounded by $4^i$, and according to Miller’s algorithm, on $i$-step we have:

$$\text{deg}_{x_1} \frac{f_1}{f_2} \rightarrow 2\text{deg}_{x_1} \frac{f_1}{f_2} + 8 \cdot 4^i,$$

$$\text{deg}_{y_1} \frac{f_1}{f_2} \rightarrow 2\text{deg}_{y_1} \frac{f_1}{f_2} + 8 \cdot 2^i,$$

and at the end of algorithm we obtain:
\[
\text{deg}_{x_1} \frac{f_1}{f_2} \leq 2 \cdot 4^{\log_2 s + 1} = 8s^2,
\]
\[
\text{deg}_{y_1} \frac{f_1}{f_2} \leq 2 \cdot 2^{\log_2 s + 2} = 8s.
\]

Let \( \mathbb{F}_r \) be a finite field with \( r \) elements, where \( r \) is a prime number. Let \( E \) be an elliptic curve defined over \( \mathbb{F}_r \) and \( (\infty) \) denotes the infinity point. The order of \( \mathbb{F}_r \) points group \( E(\mathbb{F}_r) \) is denoted as \( \#E(\mathbb{F}_r) \), \( p \) is a large prime factor of \( \#E(\mathbb{F}_r) \), and \( k \in \mathbb{N} \), is minimal satisfies \( p \mid r^k - 1 \).

Let \( P \in G_1 = E[p] \cap \text{Ker}(\pi_r - [1]) \) and \( Q \in G_2 = E[p] \cap \text{Ker}(\pi_r - [r]) \). Let \( f_{s, Q} \) be a rational function on \( E \) with divisor (8) for the each integer \( s \).

Let \( s = r^i (\text{mod}p) \) for some integer \( i \). Let \( D \) be a divisor, which is equivalent to \((P) - (\infty)\) with its support, which disjoints from \( \text{Supp}(f_{s, Q}) \). Then [12][Theorem 1] (reduced) generalized Ate pairing

\[
e(Q, P) = f_{s, Q}(D) = \prod_{R \in \text{Supp}D} f_{s, Q}(R)^{v_R(D)},
\]

is a nondegenerate bilinear map from \( G_2 \times G_1 \) to subgroup of \( p \) roots of unit in \( \mathbb{F}_{r^k}^* \), if

\[
\gamma_p(s^{\text{ord}_p s} - 1) \leq \gamma_p(r^k - 1),
\]

where \( \gamma_p(x) \) is a degree of \( p \) in multiplicative representation of \( x \), and \( \text{ord}_p \) is the order (\( \text{mod}p \)).

We will consider nonreduced generalized Ate pairing

\[
\tilde{e}(P, Q) = f_{s, Q}(D),
\]
as a map from \( G_1 \times E(\mathbb{F}_{r^k}) \) to \( \mathbb{F}_{r^k}^*/(\mathbb{F}_{r^k}^*)^p \). This map is correctly defined, because \( \tilde{e}([p]P, E(\mathbb{F}_{r^k})) \in (\mathbb{F}_{r^k}^*)^p \), i.e. it is a unit of factor group. \( \tilde{e}(P, (\infty)) = 1 \) by definition. As for arbitrary \( s \) the divisor (8) is the main divisor, this map is a homomorphism. So,

\[
\tilde{e} : G_1 \times E(\mathbb{F}_{r^k})/[p]E(\mathbb{F}_{r^k}) \longrightarrow \mathbb{F}_{r^k}^*/(\mathbb{F}_{r^k}^*)^p.
\]

In the case when (9) is held, this homomorphism is nondegenerate too by theorem [12][Theorem 1].

If every possible \( s \) is large, utilization of pairing \( f_{s, h, Q}(P) \) from [10] may be effective.
From Miller algorithm [7], we obtain \( f_{s,Q}(x,y) \) or \( f_{s,(x,y)}(P) \) as rational functions

\[
\frac{f_1(x,y)}{f_2(x,y)}, \text{deg}_x(f_1/f_2), \text{deg}_y(f_1/f_2) \leq 8s^2.
\]

For fixed \( P \in G_1 \) we have \( x,y \in \mathbb{F}_r^k \) and \( f_1(x,y), f_2(x,y) \in \mathbb{F}_r(x,y) \). For fixed \( Q \in G_2 \) we have \( x,y \in \mathbb{F}_r \) and \( f_1(x,y), f_2(x,y) \in \mathbb{F}_r(x,y) \). Without loss of generality, we may assume that \( \text{deg}_x f_i(x,y) = O(s^2), \text{deg}_y f_i(x,y) = 1 \).

For solving \( e(Q, (x,y)) = z \) we obtain equation

\[
\left( \frac{f_1(x,y)}{f_2(x,y)} \right)^{\frac{e^k-1}{p^r}} = z.
\]  \hspace{1cm} (10)

Let \( \frac{e^k-1}{p^r} = \alpha_{k-1} r^{k-1} + \cdots + \alpha_0, \alpha_i \in \{0,1,\ldots,r-1\} \). Then

\[
\prod_{i=0}^{k-1} \left( \frac{f_1(x,y)}{f_2(x,y)} \right)^{\alpha_i} = z^r^j, j = 0,1,\ldots,k-1,
\]

where \( i - j \text{ (modk) } \) is a least positive residue \( \text{ (modk) } \). Let’s consider

\[
\left( \frac{f_1(x,y)}{f_2(x,y)} \right)^{e^i}, i = 0,\ldots,k-1, \text{ as a new multiplicative variables. The degrees of these variables will form a circulant matrix } C \text{ in } \mathbb{Z}_{r^{k-1}}^k. \text{ We want to obtain a vector } \vec{v} \in \mathbb{Z}_{r^{k-1}}^k, \text{ for which } \vec{v} C = (a_1,\ldots,a_k), a_i \in \mathbb{Z}, \text{ where } \sum_{i=1}^{k} |a_i| \leq |\vec{a}| = a \text{ with a small } a \in \mathbb{N}. \text{ With the help of LLL algorithm [14][Theorem 7.11] we can obtain vector } (a_1,\ldots,a_k) \text{ as a smallest in a lattice of rows of } C \text{ by } O(k^4 \log r) \text{ operations with not big integers (with absolute values smaller than } O(k \log r)). \text{ According to the [14][Theorem 7.7], we obtain [18]}

\[
a \leq 2^{(k-1)/4} (\det C)^{\frac{1}{2}}, \det C = \prod_{j=0}^{k-1} \sum_{t=0}^{k-1} \alpha_t e^{2\pi i j t}.
\]

The similar considerations in [15] lead to the same lattice. Direct computer calculations with 5-digit primes show, that small vectors \( a \) don’t exist.
Most coordinates of minimal vector are 5-digit. This situation doesn’t significantly change, if we obtain to the lattice vectors of powers, that give roots of the unit with not very big degree. One may examine such roots item-by-item in the end.

Let’s consider nonreduced generalized Ate pairing in the case when it is nondegenerate. Values of such pairing are in factor group $\mathbb{F}_{p_k}^*/(\mathbb{F}_{p_k}^*)^p$. So inversion of such pairing may be contracted to the solving an equality:

$$\frac{f_1(x, y)}{f_2(x, y)} = z(\tilde{z})^p, \tilde{z} \in \mathbb{F}_{p_k}^*.$$  \hspace{1cm} (11)

To make the power in the right hand side of this equality lower, let’s consider $i : r^i \equiv s (mod p)$. We propose, that $s$ is small, and (9) is true. Let us $t = \frac{r^i - s}{p}, (t, \frac{r^k - 1}{p}) = 1$ too. If this condition is not true, we can consider $t = \frac{\sum \alpha_r r^i}{p} \in \mathbb{Z}$, that satisfies this condition and has $| \alpha_i | \leq s^2$. If residues $\sum \alpha_i r^i (mod p)$, and $\frac{\sum \alpha_r r^i}{p} (mod \frac{r^k - 1}{p})$, when $\frac{\sum \alpha_r r^i}{p} \in \mathbb{Z}$, are random, then our condition is satisfied with good probability, when $(2s^2)^k > 2p \ln \ln \frac{r^k - 1}{p}$, or when

$$s^k > p.$$  \hspace{1cm} (12)

Instead of (11) we will consider analogous:

$$\frac{f_1(x, y)}{f_2(x, y)} = z(\tilde{z})^{pt}, \tilde{z} \in \mathbb{F}_{p_k}^*.$$  \hspace{1cm} (13)

As far as $pt \equiv r^i - s (mod r^k - 1)$, we obtain

$$\frac{f_1(x, y)}{f_2(x, y)} = z(\tilde{z})^{r^i - s}.$$  \hspace{1cm} (13)

In the case of fixed $Q$ we have $x, y \in \mathbb{F}_r$, $n \deg \left( \frac{f_1(x, y)}{f_2(x, y)} \right) = O(s^2)$.

Element $\tilde{z} \in \mathbb{F}_{r_k}$ may be represented in normal bases ([17])

$$\tilde{z} = z_1 \theta^{r^0} + z_2 \theta^{r^1} + \ldots + z_k \theta^{r^{k-1}}, z_i \in \mathbb{F}_r,$$

$$\tilde{z}^{r^i} = z_1^{r^{i (mod k)}} \theta^{r^0} + \ldots + z_k^{r^{i (mod k)}} \theta^{r^{k-1}}.$$  

Production of such elements can be written in the same form with coefficients, that are quadratic forms from initial coefficients. Multiplying by the denominator, we obtain
\[ \Phi(x, y, z_1, \ldots, z_k) = 0, \Phi \in \mathbb{F}_{r^k}[x, y], \deg \Phi = O(s^2). \]

In the case when \( \#E(\mathbb{F}_r) = p \) every solution of the system of this equation with the equation of considered elliptic curve gives point in \( < P > \).

In the case of fixed \( P \), in (13) we have \( x, y \in \mathbb{F}_{r^k} \), which may be represented in normal bases as above:

\[
\begin{align*}
x &= x_1 \theta^{r_0} + x_2 \theta^{r_1} + \ldots + x_k \theta^{r_{k-1}}, x_i \in \mathbb{F}_r, \\
y &= y_1 \theta^{r_0} + y_2 \theta^{r_1} + \ldots + y_k \theta^{r_{k-1}}, y_i \in \mathbb{F}_r.
\end{align*}
\]

So in the both cases when we represent \( z, \bar{z} \) and coefficients of polynomials, that are in \( \mathbb{F}_{r^2} \), in normal bases, and gather coefficients at \( \theta^{r_i} \) by \( O(s^2k^2) \) arithmetic operations in \( \mathbb{F}_r \), we may represent equation (13) as a system of \( k \) equations of degree \( O(s^2) \) over \( \mathbb{F}_r \) on variables \( x, y, z_1, \ldots, z_k \) or \( x_1, \ldots, x_k; y_1, \ldots, y_k; z_1, \ldots, z_k \), that are in \( \mathbb{F}_r \). Curve equation \( y^2 = x^3 + ax + \beta \) upends one or \( k \) equations over \( \mathbb{F}_r \) respectively. The system of this equations may be solved by Groebner bases methods or by some other methods of solving polynomial systems, when \( s, k \) are not very big. The complexity bound of \( F5 \) algorithm in this case (number of variables is more, than the number of equations) is [19]

\[ O(k(s^2)^{3/2k}), \]

that is evidently the complexity bound of the whole inverting algorithm.

As was mentioned in [16], when \( p \) is prime and \( d = \text{ord}_p s \), \( s \equiv r^i \pmod{p} \), then \( p \) divides the value of cyclotomic polynomial \( Q_d(s) \). So \( s \geq p^{\frac{i}{2}} \geq p^{\frac{i}{6}} \).

In this case condition (12) is held, but by substitution in (14) we obtain too much complexity bound. On the other hand, when the considered polynomial system is not semi-regular [20], as in the case \( HFE \), the same algorithms may solve it in a shorter time.

The considered polynomial system may be complemented with the equations obtained from \( \bar{e}(mP, Q) = z^m(\bar{z}_1)p, \bar{e}(P, [m]Q) = z^m(\bar{z}_2)p, \bar{z}_1, \bar{z}_2 \in \mathbb{F}_{r^k}^* \).

Normal bases may be replaced with any other bases. Frobenius map acts in it as linear operator.
References


