On Discrete Logarithm Problem based on Algebraic Varieties over Finite Field and Public Key Cryptosystem

Sunil Kumar Kashyap[1], Ashutosh Pandey[2], Birendra Kumar Sharma[2]
Department of Mathematics, School of Advance Sciences, Vellore Institute of Technology University, Vellore, Tamil Nadu-632014, India
[1]Department of Mathematics, Kalinga University, Raipur, Chhattisgarh-492001, India
[2]School of Studies in Mathematics, Pandit Ravishankar Shukla University, Raipur, Chhattisgarh-492010, India

***Abstract* - We propose discrete logarithm problem (DLP) in algebraic varieties over finite field and then design public key cryptosystem (PKC).**

***Keywords* - DLP, PKC.**

Introduction

In this paper, Cardon and Murty's [8, 9] work is restudied in the context of DLP. We propose DLP in algebraic varieties over finite field. We extended to this result to design the PKC. First, we go to preliminaries as start as from here:

Materials and Method

1. Finite Field

A finite field is a field with a finite field order (i.e., number of elements), also called a Galois field. The order of a finite field is always a prime *(p)*or a power of a prime*(p)* [BirMac1996]. For each prime power, there exists exactly one up to an isomorphism finite field $GF(p)$, often written as F_{p^n}, if $q = p^n$ then F_q in current usage. For a finite set X, $|X|$ denotes its cardinality. By $f \ll g$ for $x \in X$, or $f = O(g)$ for $x \in X$, where X is an arbitrary set on which f is defined, we mean synonymously that there exists a constant $C \geq 0$ such that $|f(x)| \leq Cg(x)$ for all $x \in X$. The "implied constant" is any admissible value of C. It may depend on the set X which is always specified or clear in the context. We use elementary scheme-theoretic language for our algebraic geometry.

2. Algebraic Variety over Finite Field

In particular, an algebraic variety over a field F or over Z is simply a separated scheme of finite type over F or Z, and in fact only affine schemes will occur, so a variety is not necessarily reduced or irreducible. We write either V_A or V/A to indicate that a scheme is defined over a ring A. *R*= $\mathrm{F}_q[T]$ is the polynomial ring with coefficients in F_q over the indeterminate T and the function field $\mathrm{F}_q(T)$ is the field of fractions of *R*. We will assume that *g* is an odd integer that is relatively prime to *q*.

3. Polynomials in Finite Field

The symbol p will always represent a monic irreducible polynomial in *R*= $\mathrm{F}_q[T]$.The symbols n and m will also be monic (but not necessarily irreducible) polynomials in R of degrees j and k respectively. The expression $\prod_m f(m)$ would mean to product $f(m)$ over all monic polynomials m of fixed degree k. If a and b are elements of R, then (a,b) represents the greatest common (monic) divisor of a and b. If a and b are ordinary integers then (a,b) will denote the greatest common divisor in the usual sense.

4. Finite Extension Field

A field F_q is said to be an extension field (or field extension, or extension), denoted by K/F_q of a field if F_q is a subfield of *K*. For example, the complex numbers are an extension field of the real numbers, and the real numbers are an extension field of the rational numbers.

5. Exponential Subfield

An exponential subfield is a subfield *F* equipped with a homomorphism $\exp_F$ from its additive group to its multiplicative group. The exponent subfield is associated to extension field degree (or relative degree, or index) of an extension field K/F_q, denoted by $[K:F_q]$, is the dimension of *K* as a vector space over F_q, i.e. (1)

$[K : F_q] = \dim_{F_q} K.$

6. Variety of Extension Fields

Given a field F_q, there are a couple of ways to define an extension field. If F_q is contained in a larger field, $F_q \subset F_q'$. Then by picking some elements $\alpha_i \in F_q'$ not in F_q, one defines $F_q(\alpha_i)$ to be the smallest subfield of F_q' containing F_q and the α_i. For instance, the rationals can be extended by the complex number ζ, yielding $Q(\zeta)$. If there is only one new element, the extension is called a simple extension. The process of adding a new element is called "adjoining." Since elements can be adjoined in any order, it suffices to understand simple extensions. Because α_i is contained in a larger field, its algebraic operations, such as multiplication and addition, are defined with elements in F_q. Hence,

$$F_q(\alpha) = \left\{ \frac{f(\alpha)}{g(\alpha)} : f, g \in F_q, g(\alpha) \neq 0 \in F_q' \right\}. \tag{2}$$

The expression above shows that the polynomials with *p (α) = 0* are important. In fact, there are two possibilities.

First, For some positive integer *n*, the *n*th power α^n can be written as a (finite) linear combination,

$$\alpha^n = \sum_{i=0}^{n-1} c_i \alpha^i, \tag{3}$$

with $c_i \in F_q$ and $powers(\alpha) < n.$ In this case, α is called an algebraic number over F_q and $F_q(\alpha)$ is an algebraic extension. The extension field degree of the extension is the smallest integer *n* satisfying the above and the polynomial $p(x) = x^n - \sum_{i=0}^{n-1}$ is called the extension field minimal polynomial. Otherwise, there is no such integer *n* as in the first case. Then α is a transcendental number over F_q and $F_q(\alpha)$ is a transcendental extension of transcendental degree 1.

7. Algebraic Extension Field

Note that in the case of an algebraic extension, the extension field can be written as;

$$F_q(\alpha) = F_q[\alpha] = \{ f(\alpha) : f \in F_q \ \& \deg ree(f) < n \}. \tag{4}$$

2. Unlike the similar expression above, it is not immediately obvious that the ring $F_q[\alpha]$ is a field. The following argument shows how to divide in this ring. Because no polynomial *f* of degree less than *n* can divide the extension field minimal polynomial *p*, any such polynomial *f* is relatively prime. That is, there exist polynomials *a* and *b* such that, $af + bp = 1,$ or rather,

$a(x) f(x) \equiv 1 (\mathrm{mod}\, p(x)).$

And $a(\alpha)$ is the multiplicative inverse of $f(\alpha).$ (5)

8. Number Field

A number field is a finite algebraic extension of the rational numbers. Mathematicians have been using number fields for hundreds of years to solve equations like $x^2 - 2y^2 = k$ where all the variables are integers, because they try to factor the equation in the extension $Q(\sqrt{2})$. For instance, it is easy to see that the only integer solutions to $(x^2 - y^2) = (x + y)(x - y) = 5$ be $(\pm 3, \pm 2)$ since there are four ways to write 5 as the product of integers as:

$5 = 5 \times 1 = 1 \times 5 = -1 \times -5 = -5 \times -1.$

Hence, it became necessary to understand what a prime number field is. In fact, it led to some confusion because unique factorization does not always hold. The lack of unioque factorization is measured by the class group, and the class number. (6)

It can be shown that any number field can be written $Q(\zeta)$ for some ζ ,that is every number field is a simple extension of the rationals. Naturally, the choice of ζ is not unique, e.g.

$Q(\zeta) = Q(2 + \zeta) = Q(-\zeta) = \ldots$

9. Product Operator type Representations of Finite Extension Fields

Let, a basic type of any product can be expressed mathematically with the product operation (pie, $\prod$) symbolic notation as follows:

(1) $$P_f(M, N) = \prod_{M \le n < M+N} e(f(n)),$$

Where $e(z) = e^{2i\pi z}$ and f is some real-valued function.Here we give some basics about the product operation, because we broadly use this operation as a major tool to represent DLPs over extension fields from the exponent subfields.

10. Product Operator

The product operator ($\prod$) {Greek letter, capital *pie*} is an instruction to product over a series of values. For instance, if we have the set of values for the variable, $X = \{X_1, X_2, X_3, X_4, X_5\}$, then

$$\prod_{i=1}^{n=5} X_i = X_1 \times X_2 \times X_3 \times X_4 \times X_5.$$

10.1. Example

Literally, the expression, $\prod_{i=1}^{n=5} X_i$, says: beginning with i=1 and ending with i=5, product over the *variables* X_i.

Let

$X_1 = 8$, $X_2 = 10$, X3 = 11, $X_4 = 15$, $X_5 = 16$.

Then $n = 5$ {the number of *cases*}, and

$$\prod_{i=1}^{n=5} X_i = 8 \times 10 \times 11 \times 15 \times 16 = 211200.$$

11. Characteristics of Product Operator

In many contexts, it is clear that the product is over all cases and we do not need the superscript over the product operator. Furthermore, in most contexts it is assumed that the product begins with $i = 1$. Hence, the notation, $\prod_i X_i$ is taken to imply $\prod_{i=1}^{n=5} X_i$. In most situations, where the variable has only one subscript, as in X_i, the subscript can be omitted. In these situations, $\prod X$ implies $\prod_{i=1}^{n=5} X_i$.

12. Product operators for two subscripts

In other contexts, the variable X may have more than one subscript, e.g., X_{ij}. This occurs, for instance, when individual belongs to two or more subgroupings or cross-classifications. We might have a situation as shown below in Table 1.

Table 1

Group 1	Group 2	Group 3
X_{11}, X_{21}, X_{31}, X_{41}	X_{12}, X_{22}, X_{32}, X_{42}, X_{52}, X_{62}	X_{13}, X_{23}, X_{33}, X_{43}, X_{53}

Here we have three groups, each with a different number of cases. We denote the *i*th case in the *j*th group with the symbol, X_{ij}. To sum all the cases, over all three groups, we would use the following, double product operator,

$$\prod_{j}^{3} \prod_{i}^{n_j} X_{ij}.,$$

12.1. Example

Here, the above instructs us to product over the three groups (j=1, 2, and 3) and, within each group, sum over the number of cases in the group (i=1, 2, 3, 4 for Group 1; i=1, 2, 3, 4, 5, 6 for Group 2; i=1, 2, 3, 4, 5 for Group 3). For simplicity, we often write the product expression as,

$$\prod\prod X_{ij},$$

where it is assumed that we are to product over all groups and all cases within each group. For example, let's substitute the following numbers for the symbolic values given above.

Table 2

Group 1	Group 2	Group 3
10, 8, 12, 13	6, 11, 8, 10, 8, 12	14, 6, 6, 10, 9

Then,

$$\prod\prod X_{ij} = \prod\left[\prod X_{ij}\right]$$
$$= [10\times 8\times 12\times 13]\times[6\times 11\times 8\times 10\times 8\times 12]\times[14\times 6\times 6\times 10\times 9]$$
$$= [12480]\times[506880]\times[45360]$$
$$= 286941118464000.$$

A more complex situation occurs when cases are grouped into cross-classifications. Table 3 represents a situation where cases are cross-classified by some common properties.

Table 3

	1	2	3
I	X_{111}, X_{211}, X_{311}, X_{411}	X_{112}, X_{212}, X_{312}, X_{412}	X_{113}, X_{213}, X_{313}, X_{413}
II	X_{121}, X_{221}, X_{321}, X_{421}	X_{122}, X_{222}, X_{322}, X_{422}	X_{123}, X_{223}, X_{323}, X_{423}

To indicate product over all the cases in the above table, we would use the notation,

$$\prod_k \prod_j \prod_i X_{ijk}.$$

where it is assumed that the product is over all *N* cases, *i*, over all *J* rows, *j*, and all *K* columns, *k*.

13. Product Operator Representation as DLP

Let α be some constant value. Then, $\prod_{i=1}^{x} \alpha = \alpha^x = \beta.$

In other words, this direct operation is also referred as the exponent expression (and the inverse operation as the DLP), producing constant *x* times is the same as powering the constant by *x*. Hence, if $\alpha = 5$, then

$$\prod_{i=1}^{3} \alpha = 5^3 = 5\times 5\times 5 = 125..$$

This rule can be extended to double product operation. Thus,

$$\prod\prod = \prod_j^j \left[\prod_i^{n_j} \alpha\right] = \prod_j^j \alpha^{n_j}.$$

13.1. Example

Let us consider, the situation involving the three groups given earlier in Table 2. If all cases, in all groups, have the constant value, 10, then

$$\prod_{j}^{3}\prod_{i}^{n_j}10$$
$$=\prod_{j}^{3}\left[\prod_{i}^{n_j}10\right]$$
$$=\left[10\times10\times10\times10\right]$$
$$\times\left[10\times10\times10\times10\times10\times10\right]$$
$$\times\left[10\times10\times10\times10\times10\right]$$
$$=\left[10^{4}\right]\times\left[10^{6}\right]\times\left[10^{5}\right]$$
$$=\left[10^{4+5+6}\right]$$
$$=\left[10^{15}\right]$$
$$=1000000000000000.$$

14. Product Operator Representation over the Finite Extension Field

These tend to arise naturally in any asymptotic counting problem, as ways to express the secondary terms after isolating a "main term" and the basic goal is to establish some form of cancellation, of the type

(2) $$\prod_{M\le n<M+N} e(f(n)) \ll N\theta(N)^{-1},$$

where the saving $\theta(N)$ from the trivial bound N is a positive increasing function with $\theta(N)\to+\infty$ as $N\to+\infty$. Evidently, it must be the case that f varies "fast enough" for such an estimate to hold.

Various highly ingenious methods have been developed to deal with the distinct possible types of phase functions f; the names of Weyl, van der Corput and Vinogradowv in particular are attached to the most classical ideas. It was however discovered that this type of analytic questions could sometimes be attacked using highly involved algebraic tools: if the interval of product operation is of the type $0\le n<p$, where p is prime, and if $f(n)=g(n)/p$, where g be a polynomial or a rational is function, the best general results come from an interpretation as an exponential product over the finite field $Z/pZ.$

Indeed, one introduces the "companion" products

$$P_v=\prod_{x\in \mathrm{F}_{p^v}} e\left(\frac{Tr\, f(x))}{p}\right),$$

For $v\ge1$, where F_{p^v} is a field with p^v elements, Tr: $\mathrm{F}_{p^v}\to\mathrm{F}_p=\mathrm{Z}/p\mathrm{Z}$ being the trace map. Although $P_v, v\ge2$, never (?) has any interpretation in analytic number theory, it is the properties of the generating function

$$Z(T)=\exp\left(\prod_{v\ge1}\frac{P_v}{v}T^v\right)$$

In this context, this was first recognized and developed by A. Weil, who proved for instance that for a fixed (non-constant) function $g\in \mathrm{Z}[X]$ one has

$$P_v(p) \ll p^{v/2}$$

For all primes p and $v\ge1$(with possibly few well-understood exceptions), with an implied constant depending only on g. See e.g. [IK] for a description of the elementary approach of Stepanov and [IK, 11.11] for a first survey of the more advanced cohomological methods of Grothendieck, Deligne, Kaatz and others.

Results and Discussion

1. Proposed Results

In this chapter, we propose new DLPs for exponential subfield as a base field and extension of this base field by the product operators over finite fields which combine quite efficiently the cohomological methods (black-box) and some results and techniques of logic to give estimates where the product set in the finite field is much more general than the algebraic sets that are usually considered. We hope that this added flexibility will make it suitable for applications to analytic number theory; also the statement is, in itself, quite elementary with very few conditions.

Our main focus on this results for the cryptographic applications to analytic number theory, it is clear that the potential of the more advanced results has not yet been fully exploited; there are a number of reasons for this, not only the complexity of the algebraic geometry involved (although that is certainly a factor), but also the difficulty of bringing a natural problem to a position

where the Riemann Hypothesis for varieties over finite fields can be applied successfully. We need only look at the proof of the Burgess estimate for short character products (see e.g. [IK] to see what ingenuity may be required; also the comments in [IK] explain how the question of uniformity in parameters and "flexibility" in the shape of the products can be crucial matters. The following theorem represents the rational functions as the exponential subfield by the product oprator with the multiplicative character conditions:

1.1. **Theorem [8, 9]:** *Let* $\varphi(x)$ *be a first-order formula in the language* $(0,1,+,-,\cdot)$ *of rings. For every ring A, let* $\varphi(A)=\{x\in A\,|\,\varphi(x)\,holds\}$.

Let $f,g\in \mathrm{Q}(X)$ *be rational functions with* f *non-constant. Let* $N\geq 1$ *be the product of primes* p *such that* f *modulo* p *is constant. Then there exists a constant* $C\geq 0$, *depending only on* φ *and the degree of the numerator and denominator of* f *and* g *such that for any prime* p *and any multiplicative character* χ *modulo* p *we have*

$$\left|\prod_{\substack{x\in\varphi(\mathrm{Z}/p\mathrm{Z})\\ f(x),g(x)\,defined}}\chi(g(x))e\left(\frac{f(x)}{p}\right)\right|\leq C(p,N)^{1/2}\sqrt{p}. \tag{3}$$

Compared to the classical products above, the point is that the product condition can be quite complicated, involving arbitrary entanglements of quantifiers (in first-order predicates, i.e., applied to elements of the field). One may also wonder if in fact the bound is really non-trivial (what if the number of points is usually of size $p^{1/4}$, for instance ?), but in fact, as proved in [CDM] and as we will explain again in detail below, the number of points of summation is either $\leq$ or or $\geq cp$, for some $A\geq 1$ and $c>0$ depending only on the formula φ. And one should keep in mind that if this were applied to a problem of analytic number theory, whether this is efficient or not would most often is obvious from the final result anyway. The proposed DLP is given below by theorem 17.1.

15. DLP

15.1. **Theorem:** *The number of square free elements of the form* n^2-am^g *with* $\deg(n)=j$ *and* $\deg(m)=k$ *that are representable in more than one way is DLP for the value of g under the order* $o(q^{j+k})$.

Proof: Let S be the collection of pairs (m,n) of monic polynomials m and n with $\deg(n)=j$ and $\deg(m)=k$ such that n^2-am^g is representable in more than one way. We will determine an upper bound for $|S|$ thereby proving the lemma. Let m_1 and m_2 be fixed unequal polynomials such that

$n_1^2-am_1^g=n_2^2-am_2^g$

For some n_1 and n_2. Then

$a(m_1^g-m_2^g)=n_1^2-n_2^2=(n_1-n_2)(n_1+n_2)$

Which shows that the choices for n_1 and n_2 are determined by the divisors of $a(m_1^g-m_2^g)$. Since $\deg(m_1^g-m_2^g)<gk$, the orst possible case is when $a(m_1^g-m_2^g)$ is divisible by $gk-1$ distinct monic linear factors. In this worst case the number of (not necessarily monic) divisors is

$$(q-1)\prod_{v=0}^{gk-1}\binom{gk-1}{v}=(q-1)2^{gk-1}.$$

Notice that q is fixed but we vary k. So, this is a very crude upper bound on the number of divisors when k is large relative to q. Here the problem of computing the value of *g* is DLP.

There are q^k choices for m_1. Given m_1, the number of choices for n_1 is bounded by the number of choices for m_2 times the number of divisors of $m_1^g-m_2^g$. Thus the set S contains $O(q^{2k}2^{gk})$ pairs. Since $j=\lfloor gk/2\rfloor$ or $\lfloor gk/2\rfloor-1$ and $q\geq 5$, we obtain $|S|=O(q^{2k}2^{gk})=o(q^{j+k})$.

We have now shown that there are $\square\ q^{j+k}$ distinct values of $D=n^2-am^g$. Since $j=\lfloor gk/2\rfloor$ or $j=\lfloor gk/2\rfloor-1$ there are $\square\ q^{gk(\frac{1}{2}+\frac{1}{g})}$ distinct values of D. Therefore there are $\square\ q^{l(\frac{1}{2}+\frac{1}{g})}$ quadratic extensions $\mathrm{F}_q(T,\sqrt{D})$ of $\mathrm{F}_q(T)$ such that $\deg(D)\leq l$.

This completes the proof.

Although, we have given the four DLPs, but for the cryptographic applications, we care about some conditions, which associated to the number theory. We already defined the exponential subfields by the product operator representation, but, still we are facing the following questions,

Q1. The proposed DLPs can be used to design PKC?
Q2. The proposed DLP how distinct to the basic DLP?
Q3. The proposed DLP only require the number theoretic studies?

These series of the questions can be listed long, but we present the three fundamental questions, which plays the key role to design the real and practical PKCs. In the next section, we not only study the proposed results in the term of number theory but also we study the results under the logical parameters. In below, we give the PKC,

16. PKC

16.1. Key Generation Algorithm

1. *The number of squarefree elements of the form of DLP(g),* $D = n^2 - am^g$,
2. *The step 1 is defined with* $\deg(n) = j$ *and* $\deg(m) = k$,
3. *The step 2 are representable in more than one way under the order* $o(q^{j+k})$.
4. *The public key is (n^2, a, m, D),*
5. *The private key is (g).*

16.2. Encryption

$$Ciphertext = C = [c_1, c_2] = \left[c_1 = m(D^g)^k, c_2 = (D^k)\right].$$

16.3. Decryption

$$Plaintext = m = (c_1)(c_2)^{-g}.$$

Conclusion

17. PKC

17.1. Key Generation Algorithm

6. *The number of squarefree elements of the form of DLP(g),* $D = n^2 - am^g$,
7. *The step 1 is defined with* $\deg(n) = j$ *and* $\deg(m) = k$,
8. *The step 2 are representable in more than one way under the order* $o(q^{j+k})$.
9. *The public key is (n^2, a, m, D),*
10. *The private key is (g).*

17.2. Encryption

$$Ciphertext = C = [c_1, c_2] = \left[c_1 = m(D^g)^k, c_2 = (D^k)\right].$$

17.3. Decryption

$$Plaintext = m = (c_1)(c_2)^{-g}.$$

Acknowledgement
Thanks to the reviewer for their significant comments.

References

[1] N. Ankeny and S. Chowla, On the divisibility of the class numbers of quadratic fields, Pacific Journal of Math., 5 (1955) p. 321-324.
[2] H. Cohen and H.W. Lenstra Jr., Heuristics on class groups of number fields, Springer Lecture Notes, 1068 in Number Theory Noordwijkerhout 1983 Proceedings.
[3] H. Davenport and H. Heilbronn, On the density of discriminants of cubic fields, II, Proc. Royal Soc., A 322 (1971), p. 405-420.
[4] Eduardo Friedman and Lawrence C. Washington, On the distribution of divisor classgroups of curves over finite fields, in Th´eorie des nombres (Quebec, PQ 1987), p. 227-239, de Gruyter, Berlin, 1989.
[5] Christian Friesen, Class number divisibility in real quadratic function fields, Canad. Math. Bull., Vol. 35(3), 1992, p. 361-370.
[6] P. Hartung, Proof of the existence of infinitely many imaginary quadratic fields whose class number is not divisible by 3, J. Number Theory, 6 (1974), 276-278.
[7] T. Honda, A few remarks on class numbers of imaginary quadratic fields, Osaka J. Math., 12 (1975), 19-21.
[8] M. Ram Murty, The ABC conjecture and exponents of class groups of quadratic fields,Contemporary Mathematics, Volume 210, 1998, pages 85-95.
[9] M. Ram Murty, Exponents of class groups of quadratic fields, Topics in Number Theory (University Park, PA, 1997), 229-239, Math. Appl., 467, Kluwer Acad. Publ.,

Dordrecht, 1999.