Asian Journal of Information Technology 6 (10): 1041-1045, 2007
ISSN: 1682-3915

On Mega Series of Two Distinct Types of Discrete Logarithms in Free Groups and Public Key Cryptosystem

Sunil Kumar Kashyap, Birendra Kumar Sharma and Amitabh Banerjee
School of Studies in Mathematics, PT. Ravishankar Shukla University,
Raipur, Chhattisgarh-492010, India

Abstract: In this study, we define the mega series of 2 distinct types of discrete logarithms in the free groups and design a public key cryptosystem, whose security is based on the difficulty of solving not only the 1 or 2 or 3 or ... any number of discrete logarithms, but the mega series of 2 distinct types of discrete logarithms in the free groups. Thus the proposed public key cryptosystem becomes mega secured. Mathematics Subject Classification Number: 94A60.

Key words: Discrete logarithms, free groups, public key, cryptosystem

INTRODUCTION

We propose the mega series of the 2 distinct types of discrete logarithms in the free groups with the help of our Theorem 1. Then after, we design a public key cryptosystem, whose security is based on the proposed problem that is solving the difficulty of the mega series of the two distinct types of discrete logarithms in the free groups. It means, our public key cryptosystem providing the mega security, because its security is based on the mega series of 2 distinct types of discrete logarithms in the free groups.

In concise, our main proposed research of this study is following;

- To define the mega series of the two distinct types of discrete logarithms in the free groups with the help of our Theorem 1.
- To design the mega secure public key cryptosystem based on the above proposed problems.

PRELIMINARIES

The examples of discrete logarithms: Discrete logarithms are perhaps simplest to understand in the group $(Z_p)^\times$. This is the set of integers {1, ..., p-1} under multiplication modulo the prime p.

If we want to find the kth power of one of the numbers in this group, we can do so by finding its kth power as an integer and then finding the remainder after division by p.

This process is called discrete exponentiation. For example, consider $(Z17)^\times$. To compute 3^4 in this group, we first compute $3^4 = 81$ and then we divide 81 by 17, obtaining a remainder of 13. Thus $3^4 = 13$ in the group $(Z17)^\times$.

Discrete logarithm is just the inverse operation: Given that $3^k = 13 \pmod{17}$, what is the k that makes this true? Actually, there are infinitely many answers, due to the modular nature of the problem; we typically seek the least nonnegative answer, which is k = 4.

The definition of discrete logarithms: G be a finite cyclic groups with n elements. We assume that the group is written multiplicatively. Let b be a generator of G; then every element g of G can be written in the form $g = b^k$ for some integer k. Furthermore, any 2 such integers representing g will be congruent modulo n. We can thus define a function,

$$\log_b: G \rightarrow Z_n$$

(Where, Z_n denotes the ring of integers modulo n) by assigning to g the congruence class of k modulo n. This function is a group isomorphism, called the discrete logarithm to the base b.

The familiar base change formula for ordinary logarithms remains valid: If c is another generator of G, then we have,

$$\log_c (g) = \log_c (b). \log_b (g)$$

No efficient algorithm for computing general discrete logarithms) $\log_b (g)$ is known. The naive algorithm is to

Corresponding Author: Sunil Kumar Kashyap, School of Studies in Mathematics, Pt. Ravishankar Shukla University, Raipur, Chhattisgarh-492010, India

raise b to higher and higher powers k until the desired g is found; this is sometimes called trial multiplication. This algorithm requires running time linear in the size of the group G and thus exponential in the number of digits in the size of the group.

More sophisticated algorithms exist, usually inspired by similar algorithms for integer factorization. These algorithms run faster than the naive algorithm, but none of them runs in polyomial time. The following are the most popular and effiecient algorithms;

- Baby-step giant-step algorithm.
- Pollard's rho algorithm for lorarithms.
- Pohlig-Hellman algorithm.
- Index calculus algorothm.
- Numberfield sieve.
- Function field sieve.

Computing discrete logarithms is apparently difficult (no efficient algorithm is known), while the inverse problem of discrete exponentiation is not (it can be computed efficiently using exponentiation by squaring, for example). This asymmetry is analogous to the one between integer factorization and integer multiplication. Both asymmetries have been exploited in the construction of cryptographic systems.

Popular choices for the group G in discrete logarithm cryptography are the cyclic groups $(Zp)_{\times}$; see Elgamal encryption, Diffie-Hellman key exchange and the Digital signature scheme. Newer cryptography applications use discrete logarithms in cyclic subgroups of elliptic curves over finite fields; see elliptic curve cryptography.

Free groups, free products, generators and relations: In this study, we show that free objects (free groups) exist in the (concrete) category of groups and we shall use these to develop a method of describing groups in terms of "generators and relations". In addition, we indicate how to construct coproducts (free products) in the categary of groups.

Given a set X we shall construct a group F that is free on the set X. If $X = \Phi$, F is the trivial group $\langle e \rangle$ If $X \neq \Phi$, let X^{-1} be a set disjoint from X such that $|X| = |X^{-1}|$. Choose a bijection $X \rightarrow X^{-1}$ and denote the image of $x \varepsilon X$ by x^{-1}. Finally choose a set that is disjoint from $X \cup X^{-1}$ and has exactly one element; denote this element by 1. A word on X is a sequence $(a_1, a_2, \ldots)$ with $a_i \varepsilon X \cup X^{-1} \cup \{1\}$ such that for some $n \varepsilon N^*$, $a_k = 1$ for all $k \geq n$. The constant sequence $(1,1,\ldots)$ is called the empty word and is denoted 1. A word $(a_1, a_2, \ldots)$ on X is said to be reduced provided that,

- For all $x \varepsilon X$, x and x^{-1} are not adjacent (that is $a_i = x \Rightarrow a_{i+1} = x$ for all $(i \varepsilon N^*, x \varepsilon X)$ and
- $a_k = 1$ implies $a_i = 1$ for all $I \geq k$

In particular, the empty word 1 is reduced.

Every nonempty reduced word is of the form, $(x_1^{\lambda 1}, x_2^{\lambda 2}, \ldots, x_n^{\lambda n}, 1,1,\ldots)$, where $n \varepsilon N^*$, $x_i \varepsilon X$ and $\lambda_i = \pm 1$. Hereafter we shall denote this word by $x_1^{\lambda 1}, x_2^{\lambda 2} \ldots, x_n^{\lambda n}$. This new notation is both more tractable and more suggestive. Observe that the definition of equality of sequences shows that 2 reduced words $x_1^{\lambda 1} \ldots, x_m^{\lambda m}$ and $y_1^{\delta n} \ldots y_1^{\delta n}$ $(x_i, y_j \varepsilon X; \lambda_i, \delta_j = \pm 1)$ are equal if and only if both are 1 or $m = n$ and $x_i = x_i$, $\lambda_i = \delta_i$, for each $i = 1,2,\ldots,n$. Consequently the map from X into the set F(X) of all reduced words on X given by $x \mapsto x^1 = x$ a is injective. We shall identify X with its image and consider X to be a subset of F(X).

Next we define a binary operation on the set F = F(X) of all reduced words on X. The empty word 1 is to act as an identity element (w1 = 1w = w for all $w \varepsilon F$). In formally, we would like to have the product of non empty reduced words to be given by juxtaposition, that is,

$$(x_1^{\lambda 1} \ldots x_m^{\lambda m})(y_1^{\delta 1} \ldots y_n^{\delta n}) = x_1^{\lambda 1} \ldots x_m^{\lambda m} y_1^{\delta 1} \ldots y_n^{\delta n}$$

Unfortunately the word on the right side of the equation may not be reduced. Therefore, we define the product to be given by juxtaposition and (if necessary) cancellation of adjacent terms of the form $xx^{-1} = x^{-1}x$; More precisely, if $x_1^{\gamma 1} \ldots x_m^{\gamma m}$ and $y_1^{\delta 1} \ldots y_n^{\delta m}$ are non empty reduced words on X with n, m let k be the largest integer $(0 \leq k \leq m)$ such that

$$x_{m-j}^{\lambda_{m-j}} = x_{m+j}^{\delta_{m+j}} \text{ for } j=,1,\ldots,k-1$$

Then define the following relation,

$$(x_1^{\lambda 1} \ldots x_m^{\lambda m})(y_1^{\delta 1} \ldots y_n^{\delta n}) = \begin{cases} x_1^{\lambda 1} \ldots x_{m-k}^{\lambda m-k} y_{k+1}^{\delta k+1} \\ \ldots y_n^{\delta n}, \text{if}, k < m; \\ y_{m+1}^{\delta m+1} \ldots y_n^{\delta n}, \text{if}, k = m < n; \\ 1, \text{if}, k = m = n. \end{cases}$$

If m > n, the product is defined analogously. The definition insures that the product of reduced words is a reduced word.

The definition of free groups: If X is a non empty set and F = F(X) is the set of all reduced words on X, then F is a groups under the defined binary operation and F = ⟨X⟩.

The group F = F(X) is called the free group on the set X. The terminology "free" is explained as follows.

Let F be the free group on a set X and τ: X →F the inclusion map. If G is a group and f: X→ga map of sets, then there exixts a unique homomorphism of groups such $\overline{f}$: F → G that $\overline{f}\,\tau$ = f. In other words, Fis free objects on the set X in the categary of groups.

THE MEGA SERIES OF TWO DISTINCT TYPES OF DISCRETE LOGARITHMS IN FREE GROUPS

In this study, we define the mega series of 2 distinct types of discrete logarithms in free groups, with the help of the following important theorem;

Theorem 1: If, the following relations is defined in the free group F,

$$(x_1^{\lambda 1}\ldots x_m^{\lambda m})(y_1^{\delta 1}\ldots y_n^{\delta n})=\begin{cases} x_1^{\lambda 1}\ldots x_{m-k}^{\lambda m-k}\, y_{k+1}^{\delta k+1} \\ \ldots y_n^{\delta n}, \text{if}, k<m; \\ y_{m+1}^{\delta m+1}\ldots y_n^{\delta n}, \text{if}, k=m<n; \\ 1, \text{if}, k=m=n. \end{cases}$$

then, the mega series of the 2 distinct types of discrete logarithms are defined as follows;

- To compute the values of l1, l2,…, lm is the mega series of first type of the discrete logarithms.
- To compute the values of d1, d2,…, dn is the mega series of second type of the discrete loarithms.

Proof: We know that, the following relations are defined in the free groups,

$$(x_1^{\lambda 1}\ldots x_m^{\lambda m})(y_1^{\delta 1}\ldots y_n^{\delta n})=\begin{cases} x_1^{\lambda 1}\ldots x_{m-k}^{\lambda m-k}\, y_{k+1}^{\delta k+1} \\ \ldots y_n^{\delta n}, \text{if}, k<m; \\ y_{m+1}^{\delta m+1}\ldots y_n^{\delta n}, \text{if}, k=m<n; \\ 1, \text{if}, k=m=n. \end{cases}$$

Now, we study the following three individual cases, which are related to the above relations,

Case 1:
If, k<m;
Then,

$$(x_1^{\lambda 1}\ldots x_m^{\lambda m})(y_1^{\delta 1}\ldots y_n^{\delta n})= x_1^{\lambda 1}\ldots x_{m-k}^{\lambda m-k}\, y_{k+1}^{\delta k+1}\ldots y_n^{\delta n},$$

$$\Rightarrow (x_1^{\lambda 1}\ldots x_m^{\lambda m})=\frac{x_1^{\lambda 1}\ldots x_{m-k}^{\lambda m-k}\, y_{k+1}^{\delta k+1}\ldots y_n^{\delta n}}{(y_1^{\delta 1}\ldots y_m^{\delta m})}$$

$$\Rightarrow x_1^{\lambda 1}=\frac{x_1^{\lambda 1}\ldots x_{m-k}^{\lambda m-k}\, y_{k+1}^{\delta k+1}\ldots y_n^{\delta n}}{(y_1^{\delta 1}\ldots y_n^{\delta n})(x_m^{\lambda m})}$$

.
.
.

$$\Rightarrow x_m^{\lambda n}=\frac{x_1^{\lambda 1}\ldots x_{m-k}^{\lambda m-k}\, y_{k+1}^{\delta k+1}\ldots y_n^{\delta n}}{(y_1^{\delta 1}\ldots y_n^{\delta n})(x_1^{\lambda 1})}$$

Above, we find the mega series of first type of discrete logarithms, which can be represent as follows;

"To compute the values of $\lambda_1, \lambda_2,\ldots, \lambda_m$ is the mega series of first type of discrete logarithms".

Again,
If, k<m;

$$(x_1^{\lambda 1}\ldots x_m^{\lambda m})(y_1^{\delta 1}\ldots y_n^{\delta n})= x_1^{\lambda 1}\ldots x_{m-k}^{\lambda m-k}\, y_{k+1}^{\delta k+1}\ldots y_n^{\delta n},$$

$$\Rightarrow (y_1^{\delta 1}\ldots y_n^{\delta n})=\frac{x_1^{\lambda 1}\ldots x_{m-k}^{\lambda m-k}\, y_{k+1}^{\delta k+1}\ldots y_n^{\delta n}}{(x_1^{\lambda 1}\ldots x_n^{\lambda n})}$$

$$\Rightarrow y_1^{\delta 1}=\frac{x_1^{\lambda 1}\ldots x_{m-k}^{\lambda m-k}\, y_{k+1}^{\delta k+1}\ldots y_n^{\delta n}}{(x_1^{\lambda 1}\ldots x_m^{\lambda n})(y_n^{\delta n})}$$

.
.
.

$$\Rightarrow y_n^{\delta m}=\frac{x_1^{\lambda 1}\ldots x_{m-k}^{\lambda m-k}\, y_{k+1}^{\delta k+1}\ldots y_n^{\delta n}}{(y_1^{\delta 1}\ldots y_n^{\delta n})(y_1^{\delta 1})}$$

Above, we find the mega series of first type of discrete logarithms, which can be represent as follows;

"To compute the values of $\delta_1, \delta_2,\ldots, \delta_n$ is the mega series of second type of discrete loarithms".

Case 2:
If, k<m;
Then,

$$(x_1^{\lambda 1}\ldots x_m^{\lambda m})(y_1^{\delta 1}\ldots y_n^{\delta n})= y_{m+1}^{\delta m+1}\ldots y_n^{\delta n},$$

$$\Rightarrow (x_1^{\lambda 1}\ldots x_m^{\lambda m})=\frac{y_{m+1}^{\delta m+1}\ldots y_n^{\delta n}}{(y_1^{\delta 1}\ldots y_n^{\delta n})}$$

$$\Rightarrow x_1^{\delta 1}=\frac{y_{m+1}^{\delta m+1}\ldots y_n^{\delta n}}{(y_1^{\delta 1}\ldots y_n^{\delta n})(x_m^{\lambda m})}$$

.
.
.

$$\Rightarrow x_m^{\lambda m}=\frac{y_{m+1}^{\delta m+1}\ldots y_n^{\delta n}}{(y_1^{\delta 1}\ldots y_n^{\delta n})(x_1^{\lambda 1})}$$

Above, we find the mega series of first type of discrete logarithms, which can be represent as follows;
"To compute the values of $\lambda_1, \lambda_2, \ldots, \lambda_m$, is the mega series of first type of discrete logarithms".
Again,
If, k = m <n;
Then,

$$(x_1^{\lambda 1}\ldots x_m^{\lambda m})(y_1^{\delta 1}\ldots y_n^{\delta n}) = y_{m+1}^{\delta m+1}\ldots y_n^{\delta n},$$
$$\Rightarrow (y_1^{\delta 1}\ldots y_n^{\delta n}) = \frac{y_{m+1}^{\delta m+1}\ldots y_n^{\delta n}}{(x_1^{\lambda 1}\ldots x_m^{\lambda m})},$$
$$\Rightarrow y_1^{\delta 1} = \frac{y_{m+1}^{\delta m+1}\ldots y_n^{\delta n}}{(x_1^{\lambda 1}\ldots x_m^{\lambda m})(y_n^{\delta n})},$$
$$\vdots$$
$$\Rightarrow y_n^{\delta n} = \frac{y_{m+1}^{\delta m+1}\ldots y_n^{\delta n}}{(x_1^{\lambda 1}\ldots x_m^{\lambda m})(y_1^{\delta 1})}$$

Above, we find the mega series of second type of discrete logarithms, which can be represent as follows;
"To compute the values of $\delta_1, \delta_2, \ldots, \delta_n$ is the mega series of second type of discrete logarithms".

Case 3:
If, k = m = n;
Then,

$$(x_1^{\lambda 1}\ldots x_m^{\lambda m})(y_1^{\delta 1}\ldots y_n^{\delta n}) = 1,$$
$$\Rightarrow (x_1^{\lambda 1}\ldots x_m^{\lambda m})(y_1^{\delta 1}\ldots y_n^{\delta n}) = 1,$$
$$\Rightarrow (x_1^{\lambda 1}\ldots x_m^{\lambda m}) = \frac{1}{(y_1^{\delta 1}\ldots y_n^{\delta n})},$$
$$\Rightarrow x_1^{\lambda 1} = \frac{1}{(y_1^{\delta 1}\ldots y_n^{\delta n})(x_m^{\lambda m})},$$
$$\vdots$$
$$\Rightarrow x_m^{\lambda m} = \frac{1}{(y_1^{\delta 1}\ldots y_n^{\delta n})(x_1^{\lambda 1})}$$

Above, we find the mega series of first type of discrete logarithms, which can be represent as follows;
"To compute the values of $\lambda_1, \lambda_2, \ldots, \lambda_m$, is the mega series of first type of discrete logarithms".
Again,
If, k = m <n;
Then,

$$(x_1^{\lambda 1}\ldots x_m^{\lambda m})(y_1^{\delta 1}\ldots y_n^{\delta n}) = 1,$$
$$\Rightarrow (x_1^{\lambda 1}\ldots x_m^{\lambda m})(y_1^{\delta 1}\ldots y_n^{\delta n}) = 1,$$
$$\Rightarrow (x_1^{\lambda 1}\ldots x_m^{\lambda m}) = \frac{1}{(x_1^{\lambda 1}\ldots x_m^{\lambda m})},$$
$$\Rightarrow y_1^{\delta 1} = \frac{1}{(x_1^{\lambda 1}\ldots x_m^{\lambda m})(y_n^{\delta n})},$$
$$\vdots$$
$$\Rightarrow y_n^{\delta n} = \frac{1}{(x_1^{\lambda 1}\ldots x_m^{\lambda m})(y_1^{\delta 1})}$$

In above, we find the mega series of second type of discrete logarithms, which can be represent as follows;
"To compute the values of $\delta_1, \delta_2, \ldots, \delta_n$ is the mega series of second type of discrete logarithms".
Thus, we clearly see that,
If, the following relations is defined in the free group F,

$$(x_1^{\lambda 1}\ldots x_m^{\lambda m})(y_1^{\delta 1}\ldots y_n^{\delta n}) = \begin{cases} x_1^{\lambda 1}\ldots x_{m-k}^{\lambda m-k} y_{k+1}^{\delta k+1} \\ \ldots y_n^{\delta n}, \text{if}, k < m; \\ y_{m+1}^{\delta m+1}\ldots y_n^{\delta n}, \text{if}, k = m < n; \\ 1, \text{if}, k = m = n. \end{cases}$$

Then, there are the mega series of the two distinct types of discrete loarithms are involves in all the three cases individually, which can be represent as follows;

- To compute the values of $\lambda_1, \lambda_2, \ldots, \lambda_m$ is the mega series of first type of the discrete logarithms.
- To compute the values of $\delta_1, \delta_2, \ldots, \delta_n$ is the mega series of second type of the discrete logarithms.

This completes the proof.

THE PROPOSED MULTI-OPTIONAL SELECTION OF ANY DISCRETE LOGARITHMS FROM THE MEGA SERIES OF TWO DISTINCT TYPES OF DISCRETE LOGARITHMS BASED PUBLIC KEY CRYPTOSYSTEMS

In this study, we give the concept to design the mega secure public key cryptosystems. In this special idea, our proposed public key cryptosystems providing the mega security, because the security of our public key cryptosystem is based on the random selection of any discrete logarithms from the mega series of 2 distinct types of discrete logarithms in the free groups.

Thus, we proposed the multi-optional selection of any discrete logarithms from the mega series of the 2 distinct types of the discrete logarithms based public key cryptosystems, with the help of our Theorem 1.

The key generation:

- Select the free group,
- Select (any one or two or three or ... any numbers) the appropriate discrete logarithm problem (or problems) in the free groups by using our Theorem 1, for example;

First, we select the case-3, then after, we select the first discrete logarithms from the first series of discrete logarithms as,

$$x_m^{\lambda m} = \frac{1}{(y_1^{\delta 1} \ldots y_n^{\delta n})(x_1^{\lambda 1})}$$

We can again select the second discrete logarithms from the second series of discrete logarithms as,

$$y_n^{\delta n} = \frac{1}{(x_1^{\lambda 1} \ldots x_m^{\lambda m})(y_1^{\delta 1})}$$

- Select all keys, $\{x_1, x_m, y_1, y_n, \lambda_1, \lambda_m, \delta_1, \delta_n\}$.
- Select the public keys, $\{x_1, x_m, y_1, y_n, \lambda_1, \delta_1\}$
- Select the private keys, $\{\lambda_m, \delta_n\}$

The encryption

- Select the message, $[m = m_1 + m_2]$,
- The Ciphertext, $[c_1, c_2, c_3, c_4]$, where,

$$c_1 = (x_m)^k,$$
$$c_2 = (y_n)^l,$$
$$c_3 = m_1 \{(x_m^{\lambda m})^k\},$$
$$c_4 = m_2 \{(y_n^{\delta n})^l\},$$

The decryptin: The Plaintext, $[m = m_1 + m_2]$, where,

$m_1 = (c_3).(c_1)^{-\lambda m}$
$m_2 = (c_4).(c_2)^{-\delta n}$

CONCLUSION

In the year 2005, Petridis and Risager (2005) was given the concept of discrete logarithms in free groups, after a suitable re-normalization and restriction, the discrete logarithm is distributed according to a standard Gaussian distribution. Mainly in this study shows that, for the free group on n generators, they prove that the discrete logarithm is distributed according to the standard Gaussian when the logarithm is renormalized appropriately. We study also Hungerford (2004), Sharp (2001), Terras (1999) and Zassenhaus (1958).

We motivated to the above idea to develop the new fundamental concept of the discrete logarithms in the free groups, but using the different way, therefore our concept is exactly different to Petridis and Risager's concept, because we not only give the discrete logarithms in free groups but also give the two distinct and mega series of discrete logarithms in free groups, by using the fundamental idea of Free Groups, Free Products, Generators and Relations based our original Theorem 1. We also design a secure, practical and multi-optional public key cryptosystem based on the our concept. This public key cryptosystem providing the security of many public key cryptosystems in the only single public key cryptosystem, because the security of our public key cryptosystem is based on the not only depend on the one or two discrete logarithm problems but the mega series of discrete logarithm problems. It means the behaviour of our public key cryptosystem as "evergreen public key cryptosystem".

REFERENCES

Hungerford, T.W., 2004. Algebra, Springer-Verlag Publications, New York Inc.

Petridis, Y.N. and M.S. Risager, 2005. Discrete logarithms in free groups, Proceedinges of the American Mathematical Society, pages 1003-1012, S 0002-9939(05)08074-3, Article electronically Published, Vol. 134.

Sharp, R., 2001. Local limit theorems for free groups. J. Math. Ann., MR1872533 (2002k:20039), 321: 889-904.

Terras, A., 1999. Fourier analysis on finite groups and applications, Cambridge University Press, Cambridge, MR1695775 (2000d:11003).

Zassenhaus, H., 1958. The Theory of Groups, New York: Chelsea Publishing Company.