International Journal of Mathematics And its Applications
Volume 4, Issue 4 (2016), 91–100.
ISSN: 2347-1557
Available Online: http://ijmaa.in/

International Journal of Mathematics And its Applications

Extended Diffie-Hellmann Protocol Based on Lucas Actions

Research Article

P.Anuradha Kameswari[1]*, S.Uma Devi[2] and T.Surendra[3]

1 Department of Mathematics, Andhra University, Visakhapatnam, India.

2 Department of Engineering Mathematics, AUCE(A), Andhra University, Visakhapatnam (A.P), India.

3 Department of Mathematics, GITAM University, Visakhapatnam, India.

Abstract: Discrete log problem (DLP) is a special case of semigroup action problem (SAP) that leads to generalized DLP. The cryptographic protocols like Diffie-Helman/ Elgamal based on DLP may be extended using semigroup action problem (SAP). The effect of square root attacks like Pollard Rho, Shanks baby step - giant step on these extensions with group actions, led to the study of a square root attacks on the generalized DLP, in the cases when, the semigroup has a large sub group and with Matrix action on abelian groups. We propose to extend the study of square root attack, Shank's Baby-step Giant-step on the generalized DLP considering the special case of LUCAS actions on abelian groups.

Keywords: Lucas group actions, Lucas Semigroup actions, Generalized discrete log problems, Extended Diffie-Hellmann protocol.

1. Introduction

In 1976, Whitfield Diffie and Martin Hellman published the paper "New Directions in Cryptography" [5]. This paper made several groundbreaking contributions to public key encryption.Diffie-Hellmann protocol (DHP) is a public key distribution method called Diffie-Hellmann key exchange, based on the assumption that the discrete log problem (DLP) is difficult to solve, the computational difficulty of discrete logarithm problem (DLP) depends on the choice of the underlying group for discrete logarithm problem.The groups most oftenly used for which the Diffie-Hellmann problem (DHP) been hard and used securely are the multiplicative group $\mathbb{F}_q^*$ of a finite field $\mathbb{F}_q$ of order q [6], for which there is a sub exponential time algorithm called index calculus alogithm and number field sieve in case q = p a prime but with no polynomial time algorithm and the other group is the group of rational points on an elliptic curve over a finite field and the best known algorithm to solve discrete log is Pollard rho algorithm [16]. The expected running time is $O(\sqrt{n})$ where n is the order of the group. The group operations on Elliptic curve are rather expensive relative to the operations of addition and multiplication in finite field as it required to find the inversions in the finite field. For breaking the Diffie-Hellmann protocol (DHP), solving the underlying discrete logarithm problem (DLP) is required. P.J. Smith and M.J.J.Lennon [17] in 1993 proposed public key cryptography based on Lucas sequences which were similar to idea of using Dickson polynomial in cryptography by Muller and Nobauer in 1981. Henceforth Lucas sequences were widely used in cryptography and there are applications like LUCELG-PK, public key cryptosystem, LUCDS. Digital signature algorithm, LUC pseudo random bit generator, Williams p+1 factorization

* *E-mail: panuradhakameswari@yahoo.in*

algorithm, that are based on Lucas sequences [8, 10].

In this paper the ideas of generalised discrete log with group actions and semigroup actions with Lucas sequences are described. We refer to the introduction of Lucas sequences and some properties on Lucas sequences in our papers [2, 3, 8]. In this paper we describe operations to obtain a group $(L(\triangle, N), \star)$, semigroup $(L(\triangle, N), \circ)$ with Lucas sequences and study the possibilities of generalised discrete logarithm with Lucas actions, one with Lucas group action and other with Lucas semigroup action which give rise to the Lucas group action problem and Lucas semigroup action problem and extended the Shanks Baby-step Giant-step method to solve both the problem by employing the group action with $(L(\triangle, N), \star)$ and semigroup action with $(L(\triangle, N), \circ)$.

2. Diffie-Hellmann Key Exchange Based on Group Actions Implemented with Group of Lucas Sequences

Definition 2.1. *Let a and b be two integers and α a root of the polynomial $x^2 - ax + b$ in $\mathbf{Q}(\sqrt{\boldsymbol{\Delta}})$ for $\Delta = a^2 - 4b$ a non square, writing $\alpha = \frac{a+\sqrt{\Delta}}{2}$ and its conjugate $\beta = \frac{a-\sqrt{\Delta}}{2}$ we have $\alpha + \beta = a, \alpha\beta = b, \alpha - \beta = \sqrt{\Delta}$ and the Lucas sequences $\{V_n(a,b)\}$ and $\{U_n(a,b)\}$, $n \geq 0$ are defined as*

$$\begin{cases} V_n(a,b) = \alpha^n + \beta^n \\ U_n(a,b) = \frac{\alpha^n - \beta^n}{\alpha - \beta} \end{cases}$$

Lucas sequences satisfy the following relations:

(1). $V_{2n}(a,b) = (V_n(a,b))^2 - 2b^n$

(2). $V_{2n-1}(a,b) = V_n(a,b)V_{n-1}(a,b) - ab^{n-1}$

(3). $V_{2n+1}(a,b) = aV_n^2(a,b) - bV_n(a,b)V_{n-1}(a,b) - ab^n$

(4). $V_n^2(a,b) = \Delta U_n^2(a,b) + 4b^n$

(5). $V_{km}(a,b) = V_k(V_m(a,b), b^k)$

(6). $U_{km}(a,b) = U_k(V_m(a,b), b^k)U_m(a,b)$

(7). $V_{k+m}(a,b) = \frac{1}{2}\left(V_k(a,b)V_m(a,b) + \Delta U_k(a,b)U_m(a,b)\right)$

(8). $U_{k+m}(a,b) = \frac{1}{2}\left(U_k(a,b)V_m(a,b) + U_m(a,b)V_k(a,b)\right)$

2.1. Modular Computations with the Lucas Sequences

Definition 2.2 ([8, 11]). *Let $N = p_1^{e_1} \dots p_r^{e_r}$, p_i's odd primes and define the function $S(N) = lcm\left\{p_i^{e_i - 1}\left(p_i - (\frac{\Delta}{p_i})\right)\right\}_{i=1}^{r}$.*

Theorem 2.3. *For $N = p_1^{e_1}.....p_r^{e_r}$ and $p_i \nmid \Delta$. Then*

$$\begin{cases} U_{S(N)t}(a,b) \equiv 0 \bmod N \\ V_{S(N)t}(a,b) \equiv 2 \bmod N \text{ for some integer } t \text{ and } p_i \nmid 2\Delta. \end{cases}$$

For $\triangle = a^2 - 4$ such that $(\triangle,N) = 1$, the set of Lucas sequences $L(\triangle, N)$ modulo N is the set $L(\triangle, N) = \{(V_m(a,1), U_m(a,1)) \bmod N,\ 0 \leq m \leq S(N)\}$ forms a group with respect to the operation $\star$ given as

$$(V_m(a,1),U_m(a,1))\star(V_k(a,1),U_k(a,1))=(V_{m+k}(a,1),U_{m+k}(a,1)).$$

In this section we consider the generalised discrete logarithm with a group action on a group G implemented with the group of Lucas sequences $L(\triangle, N)$ we first describe an action of L($\triangle, N$) on a group G in the following theorem:

Theorem 2.4. *Let G be a cyclic group of order N and let $*$: L($\triangle$, N)$\times G \to G$, be a mapping defined as for any $g \in G$, ($V_m(a,1)$,$U_m(a,1)$) $\in$ L($\triangle$, N) and*

$$(V_m(a,1),U_m(a,1)) * g = g^{(\frac{V_m(a,1)+\sqrt{\triangle}U_m(a,1)}{2})}$$

then $*$ is an action of L($\triangle$, N) on G.

Proof. We need to verify the two action properties of L($\triangle$, N) on the given group G.

(i) For any ($V_m(a,1)$,$U_m(a,1)$),($V_k(a,1)$,$U_k(a,1)$)$\in$L($\triangle$, N) we have by definition

$$\begin{aligned}(V_m(a,1),U_m(a,1)) * (V_k(a,1),U_k(a,1)) * g &= (V_m(a,1),U_m(a,1)) * g^{(\frac{V_k(a,1)+\sqrt{\triangle}U_k(a,1)}{2})}\\ &= (V_m(a,1),U_m(a,1)) * x, \quad for \;\; x = g^{(\frac{V_k(a,1)+\sqrt{\triangle}U_k(a,1)}{2})}\\ &= x^{(\frac{V_m(a,1)+\sqrt{\triangle}U_m(a,1)}{2})}\\ &= g^{(\frac{V_k(a,1)+\sqrt{\triangle}U_k(a,1)}{2})(\frac{V_m(a,1)+\sqrt{\triangle}U_m(a,1)}{2})}\\ &= g^{(\frac{V_{k+m}(a,1)+\sqrt{\triangle}U_{k+m}(a,1)}{2})}\\ &= (V_{m+k}(a,1),U_{m+k}(a,1)) * g\end{aligned}$$

Therefore, (($V_m(a,1)$,$U_m(a,1)$)$\star$($V_k(a,1)$,$U_k(a,1)$))$*$g = ($V_{m+k}(a,1)$,$U_{m+k}(a,1)$))$*$g.

(ii) Now for the identity element ($V_0(a,1)$, $U_0(a,1)$) $\in$ L($\triangle$, N), we have

$$\begin{aligned}(V_0(a,1),U_0(a,1)) * g &= g^{(\frac{V_0(a,1)+\sqrt{\triangle}U_0(a,1)}{2})}\\ &= g^{(\frac{2+\sqrt{\triangle}0}{2})}\\ &= g^{\frac{2}{2}}\\ &= g\end{aligned}$$

therefore, ($V_0(a,1)$,$U_0(a,1)$)$*$g = g. Therefore, $*$ is an action of the group $(L(\triangle, N), \star)$ on group G. □

Remark 2.5. *The orbits of each element x$\in$G under the above action are given as O(x)=$\{(V_i(a,1),U_i(a,1)) * x \;\forall i = 0,1,2,...S(N)\}$.*

Now for N = 13 and a = 4 then $\triangle = a^2 - 4 = 16 - 4 = 12$ for $\sqrt{\triangle}$=5 mod 13 and S(N)= 13-1= 12, the elements in L($\triangle$, N) are given as {(2,0),(4,1),(1,4),(0,2),(12,4),(9,1),(11,0),(9,12),(12,9),(0,11),(1,9),(4,12)}. Let M=$(Z_{13^2})^*$, the multiplicative group of (Z_{13^2}), M is of order $\phi(13^2)$=13×12 then there is g$\in$M such that O(g)=13 taking G=$\langle g\rangle$ the subgroup generated by g, we have a group G of order 13 inparticular note g= 27 $\in$ M is of order 13. Now taking G = $\langle 27\rangle$ we have $*$:L($\triangle$, N)×G$\to$ G a group action and for ($V_4(a,1)$,$U_4(a,1)$)= (12,4) $\in$ L($\triangle$, N) we have the orbits of g = 27 and h=($V_4(a,1)$,$U_4(a,1)$)$*$27= $27^{\frac{V_4(a,1)+\sqrt{\triangle}U_4(a,1)}{2}} = 27^{\frac{12+5\times4}{2}}$=79 in L($\triangle, N$)given as

$$O(g) = O(27) = \{(V_i(a,1),U_i(a,1)) * 27 \;\forall\; i = 0,1,2...12\}$$

$$O(h) = O(79) = \{(V_i(a,1),U_i(a,1)) * 79 \;\forall\; i = 0,1,2...12\}$$

$$O(g) = \{27, 118, 105, 131, 79, 14, 144, 53, 66, 40, 92, 157, 27\}$$

$$O(h) = \{79, 14, 144, 53, 66, 40, 92, 157, 27, 118, 105, 131, 79\}$$

Now we have the generalised discrete logarithm problem in L($\triangle, N$) with the Lucas group action on group G of order N, this problem is also called as Lucas group action problem and is defined as follows:

Definition 2.6. Let L($\triangle, N$) be the group of Lucas sequences acting on cyclic group G of order N then if g be the generator of G and h any given element in G then Lucas group action problem is to find $0 \leq$ m $\leq$S(N) such that $(V_m(a,1),U_m(a,1))*g$ = h.

Extended Diffie-Hellmann protocol with Lucas group action:

For any generator of G, the key exchange protocol between A and B is as follows:

1. **A** chooses private key m and takes $(V_m(a,1),U_m(a,1))$ in L($\triangle$, N) and computes $(V_m(a,1),\ U_m(a,1))*g = g^{\frac{V_m(a,1)+\sqrt{\triangle}U_m(a,1)}{2}} = \alpha$ (*say*) then makes (a, g, α) public.
2. **B** chooses private key k and takes $(V_k(a,1),U_k(a,1))$ and computes $(V_k(a,1),\ U_k(a,1))*$g $= g^{\frac{V_k(a,1)+\sqrt{\triangle}U_k(a,1)}{2}} = \beta$ (*say*) then makes (a, g, β) public.
3. Then the shared secret key is taken as $(V_{k+m}(a,1),U_{k+m}(a,1))*g = g^{\frac{V_{k+m}(a,1)+\sqrt{\triangle}U_{k+m}(a,1)}{2}}$.
4. **A** computes this shared secret key from β as $(V_m(a,1),U_m(a,1))*\beta$, similarly **B** computes shared secret key from α as $(V_k(a,1),U_k(a,1))*\alpha$.

Example 2.7. *Let $N = 13$ and $a = 4$ then $\triangle = a^2 - 4$ and S(N)=13 -1= 12, take G=$\langle 27\rangle$ subgroup of order 13 in $(Z_{13^2})^*$ then for L($\triangle$, N)={(2,0),(4,1),(1,4),(0,2),(12,4),(9,1),(11,0),(9,12),(12,9),(0,11),(1,9),(4,12)}, the protocol is as follows:*

1. ***A** chooses private key m = 4 and takes $(V_4(a,1),U_4(a,1))$ and computes $\alpha = (V_4(a,1),U_4(a,1)) * 27$=$(12,4) * 27$*
$$= 27^{\frac{12+5\times 4}{2}}$$
$$= 27^{16}$$
$$= 27^3 (\text{mod } 169)$$
$$= 79$$
and makes (a, 27, α) public.
2. ***B** chooses private key m=7 and takes $(V_7(a,1),U_7(a,1))$ and computes β=$(V_7(a,1),U_7(a,1)) * 27$=$(9,12) * 27$*
$$=27^{\frac{9+5\times 12}{2}}$$
$$= 27^{483}$$
$$=27^2 (\text{mod } 169)$$
$$= 53$$
and makes (a, 27, β) public.
3. ***A** computes secret key as $\beta^{\frac{V_4(a,1)+\sqrt{\triangle}U_4(a,1)}{2}} = 53^{\frac{12+5X4}{2}} = 53^3 (\text{mod } 169) = 157$.*
4. ***B** computes secret key as $\alpha^{\frac{V_7(a,1)+\sqrt{\triangle}U_7(a,1)}{2}} = 79^{\frac{9+5X12}{2}} = 79^2 (\text{mod } 169) = 157$.*

2.2. To Extend Shank's Baby-step Giant-step attack on Discrete Logarithm Problem with Lucas group action

In the Diffie-Hellmann protocol, the shared secret key $(V_{k+m}(a,1),U_{k+m}(a,1))*$g may be evaluated from given public keys if the Lucas action problem is solved. In this section we describe the procedure to solve Lucas action problem by extending the Shanks Baby-step and Giant-step method, emphasising that $(L(\triangle, N), \star)$ is a group. As the orbits of g & α are same sets the Lucas action problem may be solved by employing Shank's Baby-step Giant-step as follows:

Shank's Baby-step Giant-step method can be employed on the basis of collision as the Baby-step and Giant-step are the orbits of same element of G, hence lie in the same orbit. Let G be a cyclic group of order N and g be the generator of G given $\alpha = (V_k(a,1), U_k(a,1)) * g$ to find a 't' such that $(V_t(a,1), U_t(a,1))$=$(V_k(a,1), U_k(a,1))$. Let m = $\sqrt{S(N)}$, then for k=mq+r, we compute the baby step B given as

$$\text{Baby step, } \mathbf{B} = \{(V_r(a,1), U_r(a,1))^{-1} * \alpha : 0 \leq r < m\},$$

note this is possible as for each $(V_r(a,1), U_r(a,1)) \in L(\triangle, N)$, we have $(V_r(a,1), U_r(a,1))^{-1} \in L(\triangle, N)$ as $L(\triangle, N)$ is a group. For some r, with $0 \leq r < m$ if we have $(V_r(a,1), U_r(a,1))^{-1}$*$\alpha$=g then we have $(V_r(a,1), U_r(a,1))$*$(V_r(a,1), U_r(a,1))^{-1}$*$\alpha$ = $(V_r(a,1), U_r(a,1)) * g \Rightarrow (V_0(a,1), U_0(a,1)) * \alpha = (V_r(a,1), U_r(a,1)) * g \Rightarrow \alpha = (V_r(a,1), U_r(a,1)) * g$, therefore in the baby step

$$\mathbf{B}=\{((V_r(a,1), U_r(a,1))^{-1} * \alpha, r) : 0 \leq r < m\}$$

if we find the pair (g, r) in B i.e. for some r, $(V_r(a,1), U_r(a,1))^{-1}$*$\alpha$=g, then we have $(V_k(a,1), U_k(a,1))$ for that r, if such (g, r) is not found for any r in B then take δ=$(V_m(a,1), U_m(a,1))$*g and compute the Giant step members for

$$\text{Giant step, } \mathbf{G} = \{(V_{mq}(a,1), U_{mq}(a,1)) * g : 0 \leq q < m\},$$

where

$$\begin{aligned}(V_{mq}(a,1), U_{mq}(a,1)) * g &= (V_m(a,1), U_m(a,1)) * (V_m(a,1), U_m(a,1)) * ... * (V_m(a,1), U_m(a,1))(q \ times) * g \\ &= ((V_m(a,1), U_m(a,1)) \star (V_m(a,1), U_m(a,1)) \star ... \star (V_m(a,1), U_m(a,1)))(q-1 \ times) * \delta.\end{aligned}$$

Then if for some q, $((V_{mq}(a,1), U_{mq}(a,1)) * g), r)$ is a pair in B for some r, then we have

$$\begin{aligned}(V_{mq}(a,1), U_{mq}(a,1)) * g &= (V_r(a,1), U_r(a,1))^{-1} * \alpha \\ \Rightarrow (V_r(a,1), U_r(a,1)) * (V_{mq}(a,1), U_{mq}(a,1)) * g &= \alpha \\ \Rightarrow (V_{mq+r}(a,1), U_{mq+r}(a,1)) * g &= \alpha\end{aligned}$$

Now as m, q, r are known quantities $(V_{mq+r}(a,1), U_{mq+r}(a,1)) * g$ can be evaluated, therefore we have for t= mq+r,

$$(V_t(a,1), U_t(a,1)) * g = g^{\frac{V_t(a,1)+\sqrt{\triangle}U_t(a,1)}{2}} = \alpha$$

and then we may compute the shared secret from the public key β as

$$\begin{aligned}\beta^{\frac{V_t(a,1)+\sqrt{\triangle}U_t(a,1)}{2}} &= (g^{\frac{V_k(a,1)+\sqrt{\triangle}U_k(a,1)}{2}})^{\frac{V_t(a,1)+\sqrt{\triangle}U_t(a,1)}{2}} \\ &= (g^{\frac{V_t(a,1)+\sqrt{\triangle}U_t(a,1)}{2}})^{\frac{V_k(a,1)+\sqrt{\triangle}U_k(a,1)}{2}} \\ &= (\alpha)^{\frac{V_k(a,1)+\sqrt{\triangle}U_k(a,1)}{2}} \\ &= (g^{\frac{V_m(a,1)+\sqrt{\triangle}U_m(a,1)}{2}})^{\frac{V_k(a,1)+\sqrt{\triangle}U_k(a,1)}{2}} \\ &= g^{\frac{V_{k+m}(a,1)+\sqrt{\triangle}U_{k+m}(a,1)}{2}} \\ &= (V_{k+m}(a,1), U_{k+m}(a,1)) * g\end{aligned}$$

Example 2.8. *Let N=13 and a=4 then* $\triangle = a^2 - 4 = 4^2 - 4 = 12$ *and S(N)=13-1=12. In* $L(\triangle, N)$ *given h=66 to find the discrete log of 66 to the base 4. We have m=*$\sqrt{S(N)} = \sqrt{12} = 4$ *and by division algorithm* $k = mq+r$, $0 \leq r < m$ *i.e.*

$k = 4q + r; r = 0, 1, 2$ or 3, using $(V_r(a,1), V_r(a,1))^{-1} = (V_{(S(N)-1)r}(a,1), U_{(S(N)-1)r}(a,1))$ and also we have group action as $(V_m(a,1), U_m(a,1)) * g = g^{\frac{V_m(a,1)+\sqrt{\triangle}U_m(a,1)}{2}}$, we compute the Baby step pairs in B as

$$\begin{aligned}
\boldsymbol{B} &= \{(V_r(a,1), U_r(a,1))^{-1} * \alpha, r) : 0 \leq r < m\} \\
&= \{(V_r(a,1), U_r(a,1))^{-1} * 66, r) : 0 \leq r < 4\} \\
&= \{((V_0(a,1), U_0(a,1))^{-1} * 66, 0), ((V_1(a,1), U_1(a,1))^{-1} * 66, 1), ((V_2(a,1), U_2(a,1))^{-1} * 66, 2), ((V_3(a,1), U_3(a,1))^{-1} * 66, 3)\} \\
&= \{((V_0(a,1), U_0(a,1)) * 66, 0), ((V_{11}(a,1), U_{11}(a,1)) * 66, 1), ((V_{10}(a,1), U_{10}(a,1)) * 66, 2), ((V_9(a,1), U_9(a,1)) * 66, 3)\} \\
&= \{((2,0) * 66, 0), ((4,12) * 66, 1), ((1,9) * 66, 2), ((0,11) * 66, 3)\} \\
&= \{(66, 0), (53, 1), (144, 2), (14, 3)\},
\end{aligned}$$

none of the elements in the Baby-step coincide with the pair (g, r)=(27, r) for r=0,1,2 or 3. So we need to compute Giant steps for a $\delta = (V_m(a,1), U_m(a,1)) * g$ and

$$\begin{aligned}
\delta^q &= (V_{mq}(a,1), U_{mq}(a,1)) * g \quad for\ q = 1, 2, 3, ... \\
&= (V_{4q}(a,1), U_{4q}(a,1)) * 27
\end{aligned}$$

For $q = 1$,

$$\begin{aligned}
\delta^q &= (V_4(a,1), U_4(a,1)) * 27 \\
&= (12, 4) * 27 = 27^{\frac{12+5\times4}{2}} \\
&= 27^{16} = 27^3 (mod\ 169) = 79;
\end{aligned}$$

For $q = 2$,

$$\begin{aligned}
\delta^q &= (V_8(a,1), U_8(a,1)) * 27 \\
&= (12, 9) * 27 = 27^{\frac{12+5\times9}{2}} \\
&= 27^{399} = 27^9 (mod\ 169) = 66;
\end{aligned}$$

Here $\delta^2 = 66$ is the first element in the pairs of B for r= 0. For q= 2, (66, 0) is in B, $\therefore$ for r=0, m=4 and q=2, we have t=mq+r=4×2+0=8 and $(V_8(a,1), U_8(a,1)) * 27 = 66 = \alpha$; using t, the shared secret key can be computed with the help of the public key β.

3. Diffie-Hellmann Key exchange Based on Semi-group Actions Implemented with Semigroup of Lucas Sequences

Semigroup action problem: For the semigroup action we consider the semigroup L($\triangle$, N)={$(V_m(a,1), U_m(a,1))$mod N, 0≤m≤S(N)} with the operation $\circ$ given as $(V_m(a,1), U_m(a,1)) \circ (V_k(a,1), U_k(a,1)) = (V_{km}(a,1), U_{km}(a,1))$ with $(V_1(a,1), U_1(a,1))$=(a,1) as identity.

Theorem 3.1. *For any $0 < k, m < S(N)$ such that (k, S(N))=1 if $0 < m < S(N)$ is such that $km \equiv 1$ mod S(N) then $(V_k(a,1), U_k(a,1)) \circ (V_m(a,1), U_m(a,1)) = (V_1(a,1), U_1(a,1))$, i.e. $(V_m(a,1), U_m(a,1))$ is inverse of $(V_k(a,1), U_k(a,1))$ in L($\triangle$, N), with respect to '$\circ$' on L($\triangle$, N).*

In this section we now consider the Generalised discrete logarithm with a semigroup action on a subset of a mapping G implemented with Lucas sequences L(△, N) we first look at the following action of L(△, N).

Theorem 3.2. *Let G be a cyclic group of order N generated by g then the set* $G'=\{g^r : r = u_t(a,1) : 0 \leq t \leq S(N)\}$, *then the mapping* $* : L(\triangle, N) \times G' \to G'$ *given as for any h*$\in G'$ *and* $(V_m(a,1), U_m(a,1))$ *in L(*△, *N) if* $h = g^{U_k(a,1)}$, $(V_m(a,1), U_m(a,1)) * h = g^{U_{km}(a,1)}$, *then* $*$ *is a semi-group action of L(*△, *N) on* G'.

Proof. The two action properties to be verified are for $(V_m(a,1),U_m(a,1)),(V_k(a,1),U_k(a,1))$ in L(△, N), we have

$$\begin{aligned}(V_k(a,1),U_k(a,1)) * (V_m(a,1),U_m(a,1)) * h &= (V_k(a,1),U_k(a,1)) * g^{U_{mr}(a,1)}, \quad for \;\; h = g^{U_r(a,1)} \\ &= g^{U_{mr}(a,1)U_k(V_{mr}(a,1))} \\ &= g^{U_{mkr}(a,1)} \\ &= (V_{mk}(a,1),U_{mk}(a,1)) * g^{u_r(a,1)} \\ &= (V_{mk}(a,1),U_{mk}(a,1)) * h \\ &= (V_m(a,1),U_m(a,1)) \circ (V_k(a,1),U_k(a,1)) * h\end{aligned}$$

and as $(V_1(a,1),U_1(a,1))$ is the identity of the semi-group, we have $(V_1(a,1),U_1(a,1))*g^{U_r(a,1)} = g^{U_r(a,1)}$. Therefore, $*$ is a semi-group action of Lucas sequences on G'. □

Remark 3.3. *The orbit of the generator g and any h*$\in G'$ *given as* $h=(V_m(a,1),U_m(a,1)) * g$, *the orbit O(h) of h is proper subset of O(g).*

Now for $N = 13$ and $a = 4$ then $\triangle=a^2-4$ and S(N)=13-1=12. The elements in L(△, N) given by the set

$$\{(2,0),(4,1),(1,4),(0,2),(12,4),(9,1),(11,0),(9,12),(12,9),(0,11),(1,9),(4,12)\}$$

is a Lucas group. Let $M=(Z_{13^2})^*$, then there exist $g\in M$ such that $O(g)=13$ and $G=\langle g\rangle$ is of order 13, taking $g=27\in G$ we have $G=\langle 27\rangle$ a group of order 13 . The mapping $* : L(\triangle, N) \times G' \to G'$ given as $(V_m(a,1),U_m(a,1))*g = g^{U_m(a,1)}$, for $G' =\{27^0, 27^1, 27^2, 27^4, 27^9, 27^{11}, 27^{12}\}$, is a semigroup action. We have for $g = 27$ and for $(V_4(a,1), U_4(a,1))=(12,4)$ in L(△, N)

$$\begin{aligned}h &= (V_4(a,1),U_4(a,1)) * 27 \\ &= 27^{U_4(a,1)} \\ &= 27^4 (\text{mod } 169) \\ &= 105 \in G', \quad \text{we have} \\ O(g) &= \{(V_i(a,1),U_i(a,1)) * g : i = 1,2,...12\} \\ O(h) &= \{(V_i(a,1),U_i(a,1)) * h : i = 1,2,...12\} \\ &= \{(V_{4i}(a,1),U_{4i}(a,1)) * g : i = 1,2,...12\} \;\; for \;\; h = (V_4(a,1),U_4(a,1)) * g. \\ O(g) &= \{27, \mathbf{105}, 53, 105, 27, \mathbf{1}, 144, \mathbf{66}, 118, 144, 1\} \\ O(h) &= \{105, 66, 1, 105, 66, 1, 105, 66, 1, 105, 66, 1\}\end{aligned}$$

Now we have the Generalised discrete logarithm problem (GDLP) with the L(△, N), the Lucas semigroup action and this problem is also called as Lucas Lucas semigroup action problem and is defined as follows.

Definition 3.4. *Let $L(\triangle, N)$ be the semigroup of Lucas sequences acting on a subset of a group order N, let g be the generator of G and h=$(V_k(a,1), U_k(a,1)) * g \in G$ then Lucas semigroup action problem is to find $0 < m < S(N)$ such that ($V_m(a,1)$,$U_m(a,1)$)$*$ g=h.*

Extended Diffie-Hellmann protocol with Lucas semi-group action: For any g a generator of G, the key exchange protocol between A and B is as follows:

1. **A** chooses private key m such that $0 < m < S(N)$ and computes ($V_m(a,1)$,$U_m(a,1)$) and $g^{U_m(a,1)}$ and makes {a, g, $V_m(a,1)$, $h_A = g^{U_m(a,1)}$} public.
2. **B** chooses private key k such that $0 < m < S(N)$ and computes ($V_k(a,1)$,$U_k(a,1)$) and $g^{U_k(a,1)}$ makes {a, g, $V_k(a,1)$, $h_B = g^{U_k(a,1)}$ } public.
3. Then the shared secret key is $g^{U_{km}(a,1)}$=$g^{U_k(a,1)U_m(V_k(a,1))}$.
4. **A** computes shared secret key from h_B of $V_k(a,1)$ as ($V_m(a,1)$,$U_m(a,1)$)$*h_B = (h_B)^{U_m(V_k(a,1))}$.
5. Similarly **B** computes shared secret key from h_A of $V_m(a,1)$ as ($V_k(a,1)$,$U_k(a,1)$)$*h_A = (h_A)^{U_k(V_m(a,1))}$.

3.1. To Extend Shank's Baby-step Giant-step Attack on Discrete Logarithm Problem with Lucas Semi-group Action

In this implementation note the discrete log of Lucas action on semigroup may be solved as the Generalised discrete log problem on group of Lucas sequences in Chapter 4, when we solve for m given V=$V_m(a,1)$, but note as the exact suffice 'm' should be considered, we verify if $g^{U_m(a,1)}$ coincides with the public value h_A for the obtained 'm', if we go for another collision. We employ Shanks Baby-step Giant-step method. Note as this is a semigroup action such that the orbit O(h) is representation of some elements in O(g) i.e. in Baby-step we compute O(g) and look at the collisions. Let $h = (V_k(a,1), U_k(a,1)) * g$; to solve the discrete logarithm of h, compute the Baby-step B is given as

$$\mathbf{B}=\{(V_r(a,1), U_r(a,1)) * h \text{ for } (\mathrm{V_r(a,1)}, \mathrm{U_r(a,1)}) \in \mathrm{L}^*\}.$$

If for some r, $(V_r(a,1), U_r(a,1)) * \alpha$=g we are through. As $h = (V_r(a,1), U_r(a,1))^{-1} * g$ and if $(V_r(a,1), U_r(a,1))^{-1} = (V_x(a,1), U_x(a,1))$ we may take k=x if $V_x(a,1) = V_k(a,1)$ given as in public key. If not we compute giant steps as follows:

$$\mathbf{G}=\{(V_q(a,1), U_q(a,1)) * g \ \forall q = 1, 2, 3, ...\},$$

if for some q, $(V_q(a,1), U_q(a,1)) * g$=$(V_r(a,1), U_r(a,1)) * h$ in B then $h = (V_r(a,1), U_r(a,1))^{-1} * (V_q(a,1), U_q(a,1)) * g$ then if we have $(V_r(a,1), U_r(a,1))^{-1}$=$(V_x(a,1), U_x(a,1))$ for some $0 < x < S(N)$ then for k= rx if $V_{rx}(a,1)$=$V_k(a,1)$ as public key, if not proceed for the next q.

Example 3.5. *Let N=13 and a=4 then $\triangle = a^2 - 4 = 4^2 - 4 = 12$ and S(N) = 13-($\frac{\triangle}{13}$)= 13-1 = 12. The multiplicative group $L^*(\triangle, N)$={(4,1),(9,1),(9,12),(4,12)} given h=66, we find the discrete log of 144 to the base 27 as follows: we compute the Baby step pairs in B with the public key given as (4, 27,9,144), we have*

$$\mathbf{B}=\{(\mathrm{V_r(a,1)}, \mathrm{U_r(a,1)}) * \mathrm{h}, \mathrm{r}) \text{ for } (\mathrm{V_r(a,1)}, \mathrm{U_r(a,1)}) \in \mathrm{L}^*(\triangle, \mathrm{N})\}.$$

As $L^*(\triangle, N)$={(4,1), (9,1), (9,12), (4,12)} we have

$$\begin{aligned}\mathbf{B} &= \{(4,1) * (66,1), (9,1) * 66, 5), ((9,12) * 66, 7), ((4,12) * 66, 11)\} \\ &= \{(66,1), (105,5), (66,7), (105,11)\}.\end{aligned}$$

Note in B we do not find r such that $(V_r(a,1), U_r(a,1)) * 66$=27 for r=1,5,7,11. So we have to go for finding of Giant step, we have

$$\mathbf{G} = \{(V_1(a,1), U_1(a,1)) * 27, (V_2(a,1), U_2(a,1)) * 27, (V_3(a,1), U_3(a,1)) * 27, (V_4(a,1), U_4(a,1)) * 27, ...\}$$

take $\delta^q = (\mathrm{V_q(a,1), U_q(a,1)}) * \mathrm{g}$ for q=1,2,3,...

$= (\mathrm{V_q(a,1), U_q(a,1)}) * 27$ for q=1,2,3,...

for q=1, $\delta^q = (\mathrm{V_1(a,1), U_1(a,1)}) * 27 = (4,1) * 27 = 27 (\mathrm{mod}\ 169)$=27;

q=2, $\delta^q = (\mathrm{V_2(a,1), U_2(a,1)}) * 27 = (9,4) * 27 = 27^4 (\mathrm{mod}\ 169)$=105.

Note for q=2, δ^q coincides with (105, 5) and (105, 11) in B, therefore we have

$$(\mathrm{V_q(a,1), U_q(a,1)}) * \mathrm{g} = (\mathrm{V_r(a,1), U_r(a,1)}) * \mathrm{h} \text{ in B}$$

$\Rightarrow (\mathrm{V_2(a,1), U_2(a,1)}) * 27 = (\mathrm{V_5(a,1), U_5(a,1)}) * \mathrm{h}$ for r=5 & 11, if $(\mathrm{V_r(a,1), U_r(a,1)})^{-1} = (\mathrm{V_x(a,1), U_x(a,1)})$ we have

$$k = rx = \begin{cases} 2 \times 5 & \text{for } x = 5 \\ 2 \times 11 & \text{for } x = 11 \end{cases}$$

$$= 10\ (mod 12)\ \ for\ x = 5\ \&\ 11.$$

$\Rightarrow k = rx = 10$; but note $(V_{10}(a,1)) \neq (V_k(a,1))$ given public key. Therefore, we proceed for the next q; now for $q = 3$, $\delta^q = (\mathrm{V_3(a,1), U_3(a,1)}) * 27 = 27^2 = 53$, for q=4, $\delta^q = (\mathrm{V_4(a,1), U_4(a,1)}) * 27 = 27^4 = 105$. Therefore $(\mathrm{V_4(a,1), U_4(a,1)}) * 27$ coincides with (105, 5) and (105, 11) in B. Therefore $(\mathrm{V_4(a,1), U_4(a,1)}) * 27 = (\mathrm{V_r(a,1), U_r(a,1)}) * \mathrm{h}$, for r=5,11 and if $(\mathrm{V_r(a,1), U_r(a,1)})^{-1} = (\mathrm{V_x(a,1), U_x(a,1)})$ we have

$$k = qx = \begin{cases} 4 \times 5 & \text{for } x = 5 \\ 4 \times 11 & \text{for } x = 11 \end{cases}$$

$$= 8\ (mod\ 12)\ \ for\ \ x = 5\ \&\ 11.$$

Now note $\mathrm{V_8(a,1)}$ coincides with the given public key $\mathrm{V_m(a,1)}$, therefore m=8, this solves the Lucas semigroup action problem. In this paper we described the Lucas group action problem and Lucas semigroup action problem and extended the Shanks method to solve both the problem by employing the group action with $(L(\triangle, N), \star)$ and semigroup action with $(L(\triangle, N), \circ)$.

4. Conclusion

Generalized discrete logarithms with Lucas group action and Lucas semigroup action giving rise to Lucas group action problem and Lucas semigroup action problem are described and extended the Shanks method to solve both the problem by employing the group action with $(L(\triangle, N), \star)$ and semigroup action with $(L(\triangle, N), \circ)$. This study with Lucas sequences is intractable and this study implemented with Lucas sequences gives a wide cross sectional view in the similar study with much complicated structures like Dickson polynomial, Elliptic curves and Hyper elliptic curves.

References

[1] Z.M.Ali, M.Othman,M.R.M.Said and M.N.Sulaiman, *Two fast compuation algorithms for LUC cryptosystem*, International Conference on Electrical Engineering, (2007).

[2] P.Anuradha Kameswari, T.Surendra and B.Ravitheja, *Shanks Baby-Step Giant-Step Attack Extended To Discrete Log with Lucas Sequences*, IOSR 12(1)(2016), 09-16.

[3] P.Anuradha Kameswari and T.Surendra, *Pollard RHO algorithm implemented to Discrete Log with Lucas sequences*, IOSR 4(3)(2016), 226-231.

[4] J.Christopher and M.S.Monico, *Semirings and Semigroup Actions in Public-Key Cryptography*, Dissertation, Graduate School of the University of Notre Dame, (2002).

[5] W.Diffie and M.E.Hellman, *New directions in cryptography*, IEEE Trans. Information Theory, 22(6)(1976), 644-654.

[6] Gary L.Mullen and Carl Mummert, *Finite Fields and Applications*, Indian Edition, 41.

[7] B.S.Gerard Maze, *Algebraic Methods for Constructing One-way Trapdoor Functions*, Dissertation, Graduate School of the University of Notre Dame, (2003).

[8] D.H.Lehmer, *An Extendeds theory of Lucas functions*, Annals of Math., 31(1930), 419-448.

[9] Marc Gysin, *The Discrete Logarithm Problem for Lucas Sequences and a New Class of Weak RSA Moduli*, The University of Wollongong, NSW 2522.

[10] G.Maze, C.Monico and J.Rosenthal, *A public key cryptosystem based on actions by semigroups*, In the proceedings of the 2002 IEEE International Symposium on Information Theory, page XY, Lausanne, Switzerland, (2002).

[11] A.J.Menezes, P.C.Van Oorschot and S.A.Vanstone, *Hand book of Applied Cryptography*, CRC Press Series on Discrete Mathematics and its Applications, CRC Press, Boca Raton, FL, (1997).

[12] Neal Koblitz, *A course in number theory and cryptography*, ISBN 3-578071-8, SPIN 10893308.

[13] Neiderreiter and R.H.Lidl, *Finite Fields*, Encyclopaedia of Mathematics and its Applications vol. 20; Addison. Wesley, Reading, Massachusetts, (1983).

[14] I.Niven, H.S.Zuckerman and J.H.Silverman, *An Introduction to the Theory of Numbers*, 5th ed., John Wiley and Sons, New York, (1991).

[15] K.H.Rosen, *Elementary number theory and its applications*, Third eddition, Addison-Wesley.

[16] J.H.Silverman, *The Arithmetic of Elliptic Curves*, vol. 106 of Graduate Texts in Mathematics, Springer-Verlag, New York, (1986).

[17] P.J.Smith and G.J.J.Lennon, *LUC: a new public key cryptosystem*, Ninth IFIP Sympoiusm on Computer Science Security, Elsevier Science Publictions, (1993), 103-117.

[18] E.Teske, *On random walks for Pollard's method*, Mathematics of Comutations, 70(2000), 809-825.

[19] A.Yamamura, *Public-key cryptosystems using the modular group. In Public Key Cryptography*, Volume 1431 of Lecture Notes in Computer Science, pages 203-216. Springer, Berlin, (1998).