# A Small Subgroup Attack for Recovering Ephemeral Keys in Chang and Chang Password Key Exchange Protocol

R. Padmavathy
Department of Computer Science and Engineering, National Institute of Technology, Warangal, India
Email: r_padma3@rediffmail.com
Chakravarthy Bhagvati
Department of Computer and Information Sciences, University of Hyderabad, Hyderabad, India
Email: chakcs@uohyd.ernet.in

***Abstract*— Three-party authenticated key exchange protocol is an important cryptographic technique in the secure communication areas. Recently Chang and Chang proposed a novel three party simple key exchange protocol and claimed the protocol is secure, efficient and practical. Unless their claim, a key recovery attack is proposed on the above protocol by recovering the ephemeral keys. One way of recovering the ephemeral key is to solve the mathematical hard Discrete Logarithm Problem (DLP). The DLP is solved by using a popular Pohlig-Hellman method in the above key recovery attack. In the present study, a new method based on the small subgroup attack to solve the DLP is discussed to recover the ephemeral keys. Computation of DLP is carried out by two stages, such as the prior-computation and DLP computation. The prior-computation is performed on off-line and the DLP computation is performed on on-line. The method is analyzed on a comprehensive set of experiments and the ephemeral keys are recovered in reduced time. Also, the key recovery attack on Chang and Chang password key exchange protocol is implemented by using the new method to recover the ephemeral key.**

***Index Terms*— Ephemeral key, Key recovery attack, Chang and Chang password key exchange protocol.**

## I. INTRODUCTION

The key exchange protocol is one of the most elegant ways of establishing secure communication between pair of users by using a session key. The session key, which is exchanged between two users assures the secure communication for later sessions. The first practical key exchange protocol is proposed by Diffie-Hellman. Since the introduction of key exchange protocol by Diffie-Hellman, various versions and improvements in key exchange protocol have been developed. In the line of key exchange protocol development, password based key exchange mechanism achieved attention due to its simplicity and wide range of applicability, as it requires the users to remember the easily remembrable password. Even though the protocol is simple and efficient, according to Ding and Horster [4], it should not be vulnerable to any type of off line, undetectable or detectable on line password guessing attacks, since the passwords are of low-entropy.

In general the password guessing attacks can be divided into three classes and they are listed below:

- Detectable on-line password guessing attacks : An attacker attempts to use a guessed password in an on-line transaction. He/She verifies the correctness of his/her guess using the response from server. A failed guess can be detected and logged by the server.

- Undetectable on-line password guessing attacks : Similar to an attacker tries to verify a password guess in an on-line transaction. However, a failed guess can not be detected and logged by server, as server is not able to distinguish an honest request from a malicious one.

- Off-line password guessing attacks : An attacker guesses a password and verifies his/her guess off-line. No participation of server is required, so the server does not notice the attack.

Since the first proposal of Bellovin and Merrit (PAKE) [2], many efficient key exchange protocols based on password have been developed. Recently these two party key exchange protocols are extended to three party, in which, the two parties initially communicates the passwords with the trusted server securely. Later the server authenticates the clients when they want to agree upon a session key. The 3-party protocol is introduced by Steiner et al [18]. Subsequently Ding and Hoster published on line and off line guessing attacks on Stener's protocol [4]. Later lin et al. proposed two versions of improved three party protocol [7], one with server's public key and another without. Recently Chang and Chang [3] proposed a novel three party encrypted key exchange protocol without server public key and claimed the protocol is secure, efficient and practical. Unlike their claims Yoon and Yoo [19] pointed out an Undetectable password guessing attack on their protocol, in which one party is able to know the other party's password and furthermore they presented an improved version of it to avoid the above attack. In the similar line Lu and Cao [8] extended the Adbella and Pointcheval protocol (SPAKE) [1] and proposed a simple


doi:10.4304/jcp.6.4.805-811

three party key exchange protocol (S-3PARTY). More recently Phan et al. [15] pointed out the Unknown key share attack and Undetectable password guessing attack on S-3PAKE and Guo et al. [5] proposed man in the middle attack and Undetectable on line dictionary attack. They also presented an improved version of S-3PAKE protocol to resist the above attack.

More recently R.Padmavathy and Chakravarthy [11] discussed a key recovery attack on Chang and Chang protocol by recovering the ephemeral keys. The ephemeral keys are recovered by solving a mathematical hard Discrete Logarithm Problem (DLP). The following paragraph discusses the DLP.

Let a group ($G$, *) consist of a set $G$ and a binary operation *. The order of an element, say $a$, of a finite group $G$ is defined to be with the smallest value $t$ such that $a^t = 1$. Some of the well known groups used in the cryptography are the set with multiplication mod p (p is a prime), the multiplication group of the field and the addition group formed by the collection of points defined by an elliptic curve over finite field. For a given prime $p$, a generator $g$ and an element $y$, the problem of finding $x$, in the range of $0 \leq x \leq p-2$, such that $g^x = y$, is known as the DLP.

Apart from the Exhaustive search to solve DLP a well known deterministic algorithm is Shanks baby step - giant step algorithm. It requires $O(\sqrt{n})$ group operations and space [6], where $n$ is the order of the generator. Pollard Rho method, which is a probabilistic one, has similar square root running time but avoids large space requirements [16]. Pohlig -Hellman method [17] reduces the DLP in a field to small subgroups. For example if $p-1$ is a product of small factors, namely $q_i$, which are relatively prime to each other. Then the method reduces the discrete logarithm $x$ mod $p$ to $x_i$ mod $q_i$, computes $x_i$ mod $q_i$ in each $q_i$ and finally combines the results using Chinese remainder theorem.

The DLP can be computed in the sub exponential time using Index calculus method, if there is more structure to the group beyond the set of elements and the group operation. Specifically, certain group elements can be labeled as smooth, when it can be factored into a product of group elements from some relatively small factor base. The index calculus method uses a fixed small set called the factor base $B$ and tries to write elements as a product of members of the factor base $B$ [9]. The base consists of objects which are small and irreducible.

The ephemeral keys are solved by using Pohlig-Hellman method in [11] and other efficient methods to recover ephemeral keys are discussed in [12], [13]. In the present study, the DLP is solved to recover ephemeral keys by using a new method based on small subgroup attack. Ephemeral keys are dynamic and change for every session [10]. Since the underlying group and the generator is common for all sessions and the ephemeral keys are computed for each session, the partial computation of solving the DLP for ephemeral key may be computed off-line and the remaining computation can be done on on-line. This is the technique followed in the new method proposed in the present study. The method involves two phases, such as a prior computation step and DLP computation step. In the first step, the information regarding the DLP of $y$ is gathered using the underlying group and the generator. The second step is the step for finding the DLP of $y$.

The following section describes the Chang and Chang password key exchange protocol and the key recovery attack. Section 3 discusses the new method to solve DLP for ephemeral key. Section 4 presents the experimental results and concluding remarks are given in Section 5.

## II. A Key Recovery Attack on Chang and Chang Password Key Exchange Protocol

This section briefly explains the key recovery attack on Chang and Chang novel three party key exchange protocol proposed by R.Padmavathy and Chakravarthy Bhagvati [11]. The notations used in this protocol are listed below:

$A, B$ : two communication parties.
$S$: the trusted server.
$ID_A, ID_B, ID_S$: the identities of A,B and S, respectively.
$PW_A, PW_B$: the passwords securely shared by A with S and B.
$E_{PW}(.)$:a symmetric encryption scheme with a password $PW$.
$r_A, r_B$: the random numbers chosen by A and B, respectively.
$p$ a large prime.
$g$ a generator of order $p-1$.
$R_A, R_B, R_S$: the random exponents chosen by A,B and S, respectively.
$N_A, N_B$ : $N_A = g^{R_A} \ mod \ p$ and $N_B = g^{R_B} \ mod \ p$.
$F_S(.)$: the one-way trapdoor hash function (TDF) where only S knows the trapdoor.
$f_K(.)$: the pseudo-random hash function (PRF) indexed by a key K.
$K_{AS}, K_{AS}$: a one time strong keys shared by A with S and B with S, respectively.

### A. The attack

A malicious party $B$ guesses the password of $A$ using Undetectable password guessing attack as proposed by Yoon and Yoo. $B$ uses the password of $A$ for obtaining the session key between $A$ and $C$, when $A$ and $C$ wants to communicate. The following procedure presents the attack in detail.
Step 1:

$A \rightarrow C : \{ID_A, ID_B, ID_S, E_{PWA}(N_A), F_S(r_A), f_{K_{AS}}(N_A)\}$
User A chooses a random integer number $r_A$ and a random exponent $R_A \in_R Z_p^*$, and then computes $N_A = g^{R_A}$ and $K_{AS} = N_A^{R_A}$. Then, A encrypts $N_A$ by using his/her password

$PW_A$ like $E_{PW_A},(N_A)$ and computes two hash values $F_S(r_A)$ and $f_{K_{AS}}(N_A)$. Finally, $A$ sends $\{ID_A, ID_B, ID_S, E_{PWA}(N_A), F_S(r_A), f_{K_{AS}}(N_A)\ \}$ to C.

Step2:

$B$ gets $\{ID_A, ID_B, ID_S, E_{PWA}(N_A), F_S(r_A), f_{K_{AS}}(N_A)\}$ and from $E_{PWA}(N_A)$ decrypts $N_A$, since password is known and solves the ephemeral key $R_A$ from $N_A$ using the popular Pohlig-Hellman method or index calculus method as discussed in the following section. This is achieved, since the order of the generator used in the protocol is p-1. When the factorization of p-1 is known and small, the exponent can be solved in reduced time, even in polynomial time when the factors of p-1 is in the form of $2^n p1^m$, where $p_1$ is small and $n, m$ are very large.

Step4:

$C \rightarrow S$: $\{ID_A, ID_C, ID_S, E_{PWA}(N_A), F_S(r_A), f_{K_{AS}}(N_A)$ $E_{PWC}(N_C), F_S(r_C), f_{K_{CS}}(N_C)\}$. User C chooses a random integer $r_C$ and a random exponent $R_C \in_R Z_p^*$, and then computes $N_C = g^{R_C}$ and $K_{CS} = N_C^{R_C}$. Then, C encrypts $N_C$ by using his/her password $PWC$ like $E_{PWC},(N_C)$ and computes two hash values $F_S(r_C)$ and $f_{K_{CS}}(N_C)$. Finally, $C$ sends $\{ID_A, ID_C, ID_S, E_{PWA}(N_A), F_S(r_A), f_{K_{AS}}(N_A)$ $E_{PWC}(N_C), F_S(r_C), f_{K_{CS}}(N_C)\}$ to $S$.

Step5:

$S \rightarrow C$:$\{\ N_C^{R_S}, f_{K_{AS}}(ID_A, ID_C, K_{AS}, N_C^{R_S}), N_A^{R_S},$ $f_{CS}(ID_A, ID_C, K_{CS}, N_A^{R_S})\}$ Server S decrypts $E_{PWA}(N_A)$ and $E_{PWC}(N_C)$ by using $PW_A$ and $PW_C$ to get $N_A$ and $N_C$,respectively. Then, $S$ gets $r_A$ and $r_C$ from $F_S(r_A)$ and $F_S(r_C)$ by using a trap door, respectively. To authenticate A and B, S computes $K_{AS} = N_A^{r_A}$ and $K_{CS} = N_C^{r_C}$ and then verifies $f_{K_{AS}}(N_A)$ and $f_{K_{CS}}(N_C)$, respectively. If successful, S chooses a random exponent $R_S \in_R Z_p^*$ and then computes ,$N_A^{R_S}$ and ,$N_C^{R_S}$, respectively. Finally, S computes two hash values $f_{K_{AS}}(ID_A, ID_C, K_{AS}, N_C^{R_S})$ $f_{K_{CS}}(ID_A, ID_C, K_{CS},, N_A^{R_S})$, and sends $\{$ $N_C^{R_S}, f_{K_{AS}}(ID_A, ID_C, K_{AS}, N_C^{R_S}), N_A^{R_S},$ $f_{CS}(ID_A, ID_C, K_{CS}, N_A^{R_S})\}$ to B.

Step 6:

$B$ gets $\{\ N_C^{R_S}, f_{K_{AS}}(ID_A, ID_C, K_{AS}, N_C^{R_S}), N_A^{R_S},$ $f_{CS}(ID_A, ID_C, K_{CS}, N_A^{R_S}\ \}$ and from $N_C^{R_S}$ he computes the session key $(N_C^{R_S})^{R_A}$ is nothing but a session key between A and C $g^{R_A R_S R_C}$

Step 7:

$C \rightarrow A$: $\{\ N_C^{R_S}, f_{K_{AS}}(ID_A, ID_C, K_{AS}, N_C^{R_S}),$ $f_K(ID_C, K)\}$ By using $K_{CS} = N_C^{r_C}$, C authenticates S by checking $f_{CS}(ID_A, ID_C, K_{CS}, N_A^{R_S})$. If successful, C computes the session key $K = (N_A^{R_S})^{R_C} = g^{R_S R_A R_C}$ and hash value $f_K(ID_C, K)$, and then sends $\{$ $N_C^{R_S}, f_{K_{AS}}(ID_A, ID_C, K_{AS}, N_C^{R_S}), f_K(ID_C, K)\}$ to A.

Step8:

$A \rightarrow C$:$\{f_K(ID_A, K)\}$ By using $K_{AS} = N_A^{r_A}$, A authenticates S by checking $f_{K_{AS}}(ID_A, ID_C, K_{AS}, N_C^{R_S})$. If successful A computes the session key $K = (N_C^{R_S})^{R_A} = g^{R_S R_A R_B}$, and authenticates C by checking $f_K(ID_C, K)$. If authenticates is passed, A computes and sends $f_K(ID_A, K)$

Step 9:

$C$ authenticates A by checking $f_K(ID_A, K)$. If successful, C confirms A's knowledge of the session key $K = g^{R_S R_A R_C}$.

## III. Solving Discrete Logarithm problem (DLP) for ephemeral keys

From the discussion of key recovery attack on Chang-Chang protocol, it is observed that the computation of $R_A$ from $N_A$ is the key issue. This leads to recover the session key by the malicious party $B$.

### A. New method based on small subgroup attack

In this section, a new method based on small subgroup attack to solve the DLP for ephemeral keys ($N_A$ and $N_B$) used in the key recovery attack is discussed. The DLP is solved by using the Pohlig-Hellman method in [11]. In the password key exchange protocol, such as Chang and Chang, the underlying group and the generator of order $p-1$ are common for all sessions and the ephemeral key, say $y$, is computed for every session. This motivated to propose a new technique for the computation of DLP of $y$. The proposed method comprises two phases. The first phase performs the partial computation of DLP of $y$ on off-line and the second phase is for computing the remaining computation on on-line. The technique is based on the property of field elements of prime say $p$ of the form $p-1 = 2X$, where $X$ is a prime or product of primes

*1) Property of field elements:*

*Theorem 1:* Let $p$ be a prime with $p-1 = 2X$, where $X$ is a prime or product of primes and let an element $y \in Z_p^*$ . In such a case, If the order of $y$ is $q$ then the order of $-y$ is $2q$, vice-versa, where $q$ is a prime and the factor of $X$.

*Proof:*

1) Let $y \in Z_p^*$ be an element of $O(q)$ Then,

$$y^q \equiv 1; -y^{2q} \equiv -y^{q^2} \equiv 1$$

That is, $-y$ is a generator for $O(2q)$.

2) Let $y \in Z_p^*$ be an element of $O(2q)$. Then,

$$y^{\frac{2q}{2}} \equiv -1; -y^{\frac{2q}{2}} \equiv 1$$

It shows that $-y$ is an element of $O(q)$.
From (1) and (2), it may be seen that if $y$ is of order $q$ then $-y$ is of $2q$, vice-versa.

Also, the discrete logarithm of $y$ and $-y$ are related as follows:-

$$x = q \pm 2i \bmod p-1; \text{ when y is of order } 2q \quad (1)$$
$$i = (x \pm q)/2 \bmod q; \text{when y is of order } q \quad (2)$$

[14] where $x$ is the discrete logarithm of $y$ or $-y$, $i$ is the discrete logarithm of $-y$ or $y$ with respect to $q$ and $q$ is the order of the subgroup. Based on the above theorem a new technique is developed and discussed below.

**First Phase:-(off-line)**

For a random prime $Z_p^*$, Compute the generators with order of factors of $p-1$ and the logarithms of subgroup generators with respect to the generator of order p-1.

**Second Phase:- (on-line)**

If the order of $y$ is small and $q$, then the DLP of $y$ with respect to order $q$ ($\log y_q$) is computed by using any exponential time algorithm such as Shanks baby step and giant step or Pollard Rho. The logarithm of $y$ with respect to order $p-1$ is calculated as $\log y = \log g_q \times \log y_q$.

Similarly, if the order of $y$ is small and $2q$, then the logarithm of $y$ with respect to order $p-1$ is calculated as $\log y = \log g_{2q} \times \log y_{2q}$. To find the logarithm of $y$ with respect to order $2q$ ($y_{2q}$), the generator of order $2q$ ($g_{2q}$) is needed. The generator of order $2q$ ($g_{2q}$) is obtained from the generator of order $q$ ($g_q$) by computing $-g_q$ ($g_{2q}$), and the logarithm of $g_{2q}$ is obtained from the logarithm of $g_q$ by using the equation (1) with the assumption of $i$ is $\log_q$ and $x$ is $\log_{2q}$. After obtaining the logarithm of $g_{2q}$, the logarithm of $y$ with respect to order $2q$ is computed by using the pollard Rho algorithm by using the generator of order $2q$ ($g_{2q}$). Finally the logarithm of $y$ is calculated.

**Algorithm 1** Off-line Computation
INPUT : Problem of size $p$, factors of $p-1$.
OUTPUT: logarithm of generators of each factor of $p-1$.

1: **for** every $q$ of $p-1$ **do**
2: Find the generator as follows:- $g_q \equiv g^{\frac{p-1}{q}}$
3: Find the logarithm of generators as follows:- $\log g_q = \frac{p-1}{q}$
4: **end for**

The **Algorithm-1** is for prior computation and **Algorithm-2** is for computation of DLP of $y$. The variable $q$ represents one of the factor of $p-1$ and

**Algorithm 2** On-line Computation
INPUT: Problem of size $p$,factors of $p-1$ and the logarithms of generators of each factor of $p-1$.
OUTPUT: logarithm of $y$.

1: Find the order of $y$
2: **if** $y$ is of order $q$ **then**
3: Find the logarithm of $y_q$ using Pollard Rho
4: $\log y = \log g_q \times \log y_q$
5: **else**
6: **if** $y$ is of order $2q$ **then**
7: Compute $-g_q$
8: Find the $\log y_{2q}$ using Pollard Rho with $-g_q$ as generator
9: $\log y = \log y_{2q} \times (q + 2 \log g_q)$
10: **end if**
11: **end if**

$\log g_q, \log y_q, \log y_{2q}, \log -g_q$ represent logarithm of generator of order $q$, logarithm of $y$ with respect to $q$, logarithm of $y$ with respect to $2q$ respectively.

## IV. Experimental Results

We implemented the method discussed above for problems of different size and conducted experiments using an appropriate database. This is generated for the purpose of ensuring the performance of the method to solve the DLP, which is discussed in the previous section. In this section we describe these experiments and give a representative selection of our experimental results. The purpose of our experiments is to produce the data on which we can base reliable statements about the expected running time of the proposed method to solve the DLP. Let us describe clearly, First we generated a database of approximately 100 problems along with the necessary information to carry out the experiments.

- $A$ data file is produced with 4-tuple ($p$, $g$, $y$, $F$) with the following properties:
- $p$ is the prime to be tested of size between 100 to 1024 bits.
- $g$ is the generator
- $y$ is the ephemeral key for which the DLP to be solved .
- $F$ is an array of factors of $p-1$.

The following algorithm is used to produce the database.
**Algorithm-3**

- Select $k$ between 100 to 1024bits.
- Select a set of primes.
- Compute the product of primes ($X$)
- Check $2X+1$ is a prime using probabilistic primality test algorithm and the size of the prime is $k$ bits.
- Find the generator $g$ of order $p-1$.
- Create a 4-tuple as $(p, g, y, F)$.

Having built up the database the method is tested. The table-1 represents average running time to solve the DLP of $y$, when the order of $y$ is $q$ or $2q$. The average running time is listed based on the order of $q$. Table-2 shows

TABLE I.
AVERAGE RUNNING TIME OF OFF-LINE AND ON-LINE COMPUTATIONS

| Problem size in bits | Off-line Running time in $\mu$s | On-line Running time | | |
|---|---|---|---|---|
| – | – | $q \approx 2^{20}$ | $q \approx 2^{30}$ | $q \approx 2^{40}$ |
| 100 | 6897 | 100ms | 1s | 1s |
| 256 | 52418 | .75s | 9m | 4h |
| 512 | 109932 | 1.25s | 15m | 6h |
| 1024 | 819460 | 2.5s | 40m | 16h |

TABLE II.
SELECTED LIST OF PROBLEMS SOLVED

| Problem | Generator of subgroup $q$ | Logarithm of generator of subgroup $q$ | Generator of subgroup $2q$ | Ephemeral key $y$ | Logarithm (DLP) of $y$ |
|---|---|---|---|---|---|
| 19100099015936 | 42692746481915 | 11790184577738 | 14830824367744 | 1211016537175 | 1143647904040 |
| 50473786381403 | 05214682255939 | 58317152087286 | 99952318155809 | 9097783526253 | 6425676375246 |
| 54882802383987 | 21054541511202 | 14125186656782 | 62777348232866 | 6978350794809 | 6755701431057 |
| 02779486862596 | 64571907141726 | 11592275841109 | 76322296148424 | 5477010726884 | 0786524450756 |
| 73707683 | 9428709 | 0969610 | 04278974 | 525830293195 | 587582405217 |
| 34153293653803 | 31587995096258 | 89615056234469 | 25652985575452 | 1163730026953 | 1837108652806 |
| 39960388006815 | 17294434969352 | 56164283399806 | 26659530374621 | 5041669059925 | 6260136780969 |
| 17632109811572 | 99981172548703 | 58509909126574 | 76509372628683 | 4470121156541 | 6034994531370 |
| 28235674675229 | 97550725955774 | 501810705764 | 0684948719455 | 1001401151800 2766 | 9477728711946 8162 |
| 87590417430723 | 60453296155989 | 81102238361781 | 27137121274734 | 5894300008847 | 4703929824983 |
| 51011323449493 | 09684323098160 | 02788262453234 | 41327000351333 | 7801691794326 | 2996171922228 |
| 7116028209 | 4484127257 | 9181507600 | 2631900952 | 893882218071 | 762525274408 |
| 35527136788005 | 26108246390031 | 28421709430404 | 94188903979734 | 2269138558123 | 1890043677121 |
| 00929355621337 | 54817614236277 | 00743484497070 | 61117413850604 | 2393128598320 | 8664944171905 |
| 89062501 | 46201616 | 3125000 | 2860885 | 2435037754 | 5175781250 |
| 20602102921755 | 23762623821497 | 16278204777683 | 18225840539605 | 1751600492338 | 2543469496512 |
| 07490794709453 | 14729187618463 | 02214948906234 | 36017875947607 | 7606476165568 | 9722108576659 |
| 5687 | 626 | 9184 | 2061 | 432268 | 92060 |
| 56843418860808 | 39317167198025 | 51386450650170 | 17526251662782 | 5067635044821 | 3115019353572 |
| 01486968994140 | 45843434887577 | 44544219970703 | 55643534106563 | 4788109827879 | 2792148590087 |
| 6251 | 4468 | 1250 | 1783 | 442170 | 890625 |
| 84782316550432 | 47665829597026 | 72221973357775 | 37116486953405 | 37116486953405 | 2983081508255 |
| 40702858886640 3 | 65498460979461 5 | 75413546458989 8 | 75204397907178 8 | 75204397907178 8 | 9550621170156 697 |
| 31400857981641 | 22743099941158 | 13205436289289 | 86577580404829 | 27328216955331 | 1725108864423 |
| 63223281069127 | 66323984131388 | 9249391400638 | 6899296937739 | 93650109216281 | 5217708149083 47 |
| 11629947400608 | 20792696017529 | 10194151425224 | 95506777988550 | 57310051114185 | 6389292090457 |
| 0119380780339 | 179501213815 | 3067605375358 | 939879566524 | 187206051185 | 4880400552161 |
| 10000000000000 | 19201683683819 | 33333333333333 | 80798316316180 | 19201683683819 | 1666666666666 |
| 00000000000000 | 70000326718251 | 33333333333333 | 29999673281748 | 70000326718251 | 6666666666666 |
| 000000000327 | 71002465659 | 33333333442 | 28997534668 | 71002465660 | 6666666666721 |
| 10000000000000 | 49843318580590 | 14135694182737 | 84437207871939 | 50156681419409 | 5000014135694 |
| 00000000000000 | 22833786641626 | 77297792428639 | 97244553522994 | 77166213358373 | 1827377729779 |
| 000000004219 | 83011830037 | 481842 | 35584981464 | 16988174182 | 2428639483951 |
| 10000000000000 | 2208360907695 | 13844854559802 | 77916390923045 | 52615691210493 | 5000415345636 |
| 00000000000000 | 4610490338659 | 84927106840742 | 38950966134091 | 71999435166308 | 7940854781320 |
| 00000103 | 086559838 | 638 | 3440265 | 1777183 | 522227965 |
| 10000000000000 | 3072102722306 | 20594789888864 | 69278972776931 | 24396954182402 | 5000035011142 |
| 00000000000000 | 8212214213860 | 33532272138729 8 | 78778578613993 | 98790528416272 | 8110693700486 |
| 00082549 | 065813499 | | 4193408 | 8572710 | 263587519 |
| 10000000000000 | 7384419687517 | 27408892157247 | 26155803124826 | 15245806559296 | 5002738148326 |
| 00000000000000 | 3532229528238 | 00701749865902 | 46777047176152 | 38972550552515 | 5089760010481 |
| 0017803 | 47402210 | | 615593 | 421826 | 16044999 |
| 10000000000000 | 7967748588439 | 53331342296554 | 20322514115609 | 31722507820841 | 5002613235772 |
| 00000000000000 | 0744258607918 | 26197421962913 4 | 25574139208137 | 33876937946337 | 5311588367367 |
| 0028939 | 62145582 | | 883357 | 767461 | 61842035 |

TABLE III.
SELECTED LIST OF ORDER OF $q$ AND $2q$ SOLVED

| Problem | Order of subgroup $q$ | Order of subgroup $2q$ |
|---|---|---|
| 341532936538033996038800681517632109811572282356746752 29 | 343 | 686 |
| 3552713678800500929355621337890625 01 | 125 | 250 |
| 1000000000000000000000000000000000000000327 | 3 | 6 |
| 1000000000000000000000000000000000000004219 | 707429 | 1414858 |
| 1000000000000000000000000000000000 00103 | 72229 | 144458 |
| 1000000000000000000000000000000000 82549 | 4855597 | 9711194 |
| 1000000000000000000000000000000001 7803 | 3648451 | 7296902 |
| 1000000000000000000000000000000002 8939 | 187507 | 375014 |

the selected list of problems solved by using the method proposed in the present study. The method is efficient when the order of $y$ is small. Since the most efficient method to solve the DLP on prime order subgroup i.e., (the subgroup of $p-1$ is a prime($q$)) is Pollard Rho, the method is used to solve the DLP with respect to $q$ in the proposed technique. Table-3 presents a selected list of the order of $q$ and $2q$ solved through the proposed method.

Further, the Chang and Chang password key exchange protocol is implemented and the session key is recovered by using the key recovery attack through the new method based on small subgroup attack is proposed in the present study. For example a problem of given $p = 12354138214723269403533485216332053524660110994963094785247378545048606590980187022168408637245590534058400097769951339145176552219627304115752702394091713106183405557203514035791158676147460937 51$ is solved in fraction seconds.

## V. CONCLUSION

A new method based on small subgroup attack to solve the DLP for ephemeral key is proposed in the present study. Specifically, the ephemeral keys are recovered for successful attempt of key recovery attack on Chang and Chang password password key exchange protocol. The property of field elements of prime of the form $p-1 = 2X$, where $X$ is a prime or product of primes motivated to develop a new method. The method consists of two steps, such as the computation to be performed on off-line and the computation on on-line. This leads to recover the ephemeral key in reduced time and the experimental results assures the claim made in the present study. The method can be applicable with some more additional steps for primes of other forms.

## REFERENCES


[1] M. Abdella and D. Pointcheval, "Simple password-based encrypted key exchange protocols", *CT-RSA 2005*, Springer-Verlag, p191-208, 2005.

[2] SM. Bellovin and M. Merrit, "Encrypted key exchange: password-based protocols secure against dictionary attacks", *IEEE symposium on research in security and privacy*, p72-84, 1992.

[3] CC. Chang and YF. Chang, "A novel three party encrypted key exchange protocol", *Computer Standards and Interfaces*, v26(5), p471-6, 2004.

[4] Y. Ding and P.Hoster, "Undetectable Online password guessing attacks", *ACM operating systems review*, v29(4), p77-86, 1995.

[5] H. Guo, Z. Li, Y. Mu and X. Zhang "Cryptanalysis of simple three-party key exchange protocol", *Computers and Security*, v27, p16-21, 2008.

[6] D. E Knuth, *The Art of computer programming,vol.3:Sorting and Searching*, Addison-Wesley, 1973.

[7] CL. Lin, HM. Sun, M. Steiner, T. Hwang "Three-party encrypted key exchange without server public keys" *IEEE Communications letters*, v5(12), p497-499, 2001.

[8] R. Lu and Z. Cao, "Simple three-party key exchange protocol", *Computers and Security*, v26, p94-97, 2007.

[9] McCurely, "The Discrete logarithm problem", *Cryptology and computational number theory proceeding of symposia in Applied Mathematics*, v42, pp 49-74.

[10] A. Menezes, and U. Berkant, "On Reusing Ephemeral Keys in Diffie-Hellman Key Agreement Protocols", preprint, 2008.

[11] R. Padmavathy, and Chakravarthy Bhagvati, "A Key Recovery Attack on Chang and Chang Password Key Exchange Protocol", *International Conference on Computer and Network Technology*, pp176-181, 2009.

[12] R. Padmavathy, and Chakravarthy Bhagvati, "Methods to Solve Discrete Logarithm Problem for Ephemeral Keys", *ARTCOM*, pp704-708, 2009.

[13] R. Padmavathy, and Chakravarthy Bhagvati, "Ephemeral Key Recovery using Index Calculus Method", *Journal of Discrete Mathematical Sciences and Cryptography*, v13(1), pp29-43, 2009.

[14] R. Padmavathy, and Chakravarthy Bhagvati, "Improved Random Method for Index Calculus Method", National Workshop on Cryptology, pp71-91, 2008.

[15] RCW. Phan, WC. Yau and BM. Goi "Cryptanalysis of simple three-party key exchange protocol (S-3PAKE)", *Information sciences*, v178(2), p849-856, 2008.

[16] J. M Pollard, "Monte Carlo methods for index computation (mod p)", *Mathematics of Computation.*, v32(143), pp.106-110, 1978.

[17] S. Pohlig, and M. Hellman, "An improved algorithm for computing logarithms over GF(p) and its cryptographic significance", *IEEE Transaction on Information Theory*, v24, pp 106-110, 1978.

[18] M. Steiner and G. Tsudik, M. Waidner "Refinement and extention of encrypted key exchange", *ACM Operating Systems Review*, v29(3), p22-30, 1995.

[19] EJ. Yoon and KY. Yoo, "Improving the novel three-party encrypted key exchange protocol", *Computer Standards and Interfaces*, v30 p309-314, 2008.

**R.Padmavathy** received her M.tech degree from Andhra University and a Ph.D from the University of Hyderabad, India. At present she is working as a faculty member at the National Institute of Technology, Warangal. Her research interests include Information security, Cryptology and Network Security.

**Chakkravarthy Bhagvati** received his Ph.D degree from RPI Newyork, USA . At present he is a professor at University of Hyderabad, Hyderabad, India. He published a number of papers in International Conferences and Journals. He chaired the National Workshop on Cryptology organized by the CRSI-Cryptology Research Society of India and an In- ternational Workshop on Computer Vision organized by IIIT-Hyderabad. His research interests include Image Processing, Computer Vision, Pattern Recognition, OCR for telugu and Cryptography.