Weak keys of the Diffie-Hellman key exchange I

A. A. Kalele
kalele@ee.iitb.ac.in

V. R. Sule
vrs@ee.iitb.ac.in

Department of Electrical Engineering
Indian Institute of Technology Bombay
Powai, Mumbai 400076

September 28, 2005

Abstract

This paper investigates the Diffie-Hellman key exchange scheme over the group $\mathbb{F}_{p^m}^*$ of nonzero elements of finite fields and shows that there exist exponents k, l satisfying certain conditions called the *modulus conditions*, for which the Diffie Hellman Problem (DHP) can be solved in polynomial number of operations in m without solving the discrete logarithm problem (DLP). These special private keys of the scheme are termed *weak* and depend also on the generator a of the cyclic group. More generally the triples (a, k, l) with generator a and one of private keys k, l weak, are called *weak triples.* A sample of weak keys is computed and it is observed that their number may not be insignificant to be ignored in general. Next, an extension of the analysis and weak triples is carried out for the Diffie Hellman scheme over the matrix group GL_n and it is shown that for an analogous class of session triples, the DHP can be solved without solving the DLP in polynomial number of operations in the matrix size n. A revised Diffie Hellman assumption is stated, taking into account the above exceptions.

Key Words : Discrete logarithms, Diffie Hellman key exchange, Finite fields, General linear group.

1 Introduction

In this paper we analyze the Diffie Hellman (DH) key exchange scheme [1] on two groups $\mathbb{F}_{p^m}^*$, the group of nonzero elements of a finite field and GL_n the group of $n \times n$ matrices over a finite field. Since the public keys and the secret key exchanged between two parties in this scheme are obtained by integral exponentiations in a group, it is necessary for the security of this scheme that the discrete logarithms be not solvable inexpensively in the group. This condition is not sufficient to ensure security unless an assumption made by Diffie Hellman holds, according to which there is no alternative efficient way to recover the shared key other than computing the discrete logarithms. On multiplicative groups of finite fields such as $\mathbb{F}_p^*$ best known algorithms for computing the discrete logarithms require sub-exponential time complexity. Hence this assumption is vital for security of the DH scheme (as well as the El Gammal and other schemes based on the discrete exponentiation) over such groups. In general discrete logarithms over cyclic groups of order n are known to require $O(\sqrt{n})$ group operations [9, 15]. It is apparent therefore that the study of exceptions to this assumption or its proof are of great importance to secure practice of these schemes.

1.1 The Diffie Hellman problem

Consider a finite group G and let $< a > \subset G$ be a cyclic subgroup. In the DH scheme two users select positive integers k, l called *private keys* modulo the order n of a independently. Then declaring the *public keys* $b = a^k$, $c = a^l$ results in their sharing the element $s = b^l = c^k = a^{kl}$ called the *shared key*. The Diffie Hellman Problem (DHP) is to determine the shared key s from the knowledge of the triple (a, b, c) called the *public data* of the DH session. We call the triple (a, k, l) the *session triple*. The problem of computing k (or l) given b (or c) is the Discrete Logarithm Problem (DLP).

The DH assumption (also known as the as yet unfalsified DH conjecture) above precludes solving the DHP without solving the DLP. This is stated informally in many texts as follows. Let (a, k, l) be a session triple of a DH key exchange scheme with public data (a, b, c). Then, the DHP cannot be solved (or the shared key s cannot be computed) without solving the DLP (or computing one of k or l). Such a statement is however imprecise from a computational point of view until the complexities of solving the two problems are clarified. Moreover for the DH scheme to be secure it is necessary from the complexity viewpoint that the DHP be not solvable in polynomial time. Hence we restate the DH assumption as

Conjecture 1 (Diffie Hellman conjecture)**.** Consider the public data (a, b, c) of a DH session with session triple (a, k, l) with a of order n in a group G and k, l in $\mathbb{Z}_n$. Then,

1. Any algorithm which computes the shared key $s = a^{kl}$ cannot accomplish this task in polynomial time depending on the public data and
2. Whenever an algorithm computes s the computation also yields one of k or l.

In the above statement the problem of efficient computation of s and computational equivalence of the two problems DHP and DLP are formulated distinctly. Precise statements of the DH conjecture are well known using complexity theoretic arguments in [2, 3, 4] and using probabilistic arguments as in [17, 13]. From a probabilistic viewpoint the DH assumption can also be stated as follows.

> If $s = \mathcal{A}(a, b, c)$ is a an algorithm running in polynomial time with the public data as the input then the probability of its success giving s as the shared key of the session is negligible

It is shown in [2] that whenever the DHP is solvable in sub-exponential time complexity so is the DLP. This supports the equivalence of the two problems. It is however not established whether the same implication is true with respect to the polynomial time complexity. That the two problem DLP and DHP are computationally equivalent for finite fields and finite groups satisfying certain conditions is also well known [3, 4]. To the best of the knowledge of the authors, nontrivial exceptions (private keys and generators) for which the shared key can be computed in polynomial time do not seem to have appeared in published literature so far. This paper also defines an index called Insecurity Factor which gives an alternative way to examine the DH assumption from a probabilistic viewpoint. The sample computations of the insecurity factor for small fields indicates that the probabilistic statement of the DH assumption may not hold universally. It is not only from a theoretical viewpoint that it appears worthwhile to know a characterization of these exceptions, such a characterization would be necessary to make the DH scheme provably secure. This paper initiates first steps in this direction.

In this paper we explore the above exceptions and show that there exist exceptional private keys for which the DHP can be solved in polynomial time for these special cases without solving the DLP. Such exceptional private keys are called *weak keys* of the DH scheme. An application of these weak keys for paring based DH schemes over elliptic curves is reported in the second part of this paper. The present part is devoted to establishing the weak keys of the DH scheme over $\mathbb{F}_{p^m}^*$ and GL_n and explore their implications.

Currently a complete characterization of these weak keys is not known. However a sample of computations over $\mathbb{F}_{p^m}^*$ shown in this paper reveals that the density of such weak keys depends on many factors such as the field characteristic, the minimal polynomial of the generator and private key of the other user. The examples show that the percentage of weak keys can be sometimes significant among the set of all permissible keys which a user can choose. Since weakness of the private keys is interdependent, random choice of private keys by two parties in a DH scheme is not secure in the key exchange protocol. This fact is of importance in practical DH schemes wherein more constraints need to be specified in the selection of private keys in order to exclude the weak keys. We however show that detecting weakness of the private key by the second user having received the public key of the first user is inexpensive and helps to avoid choice of weak private key.

1.2 DH scheme over the matrix group

Generalization of the DLP over $GL_n(K)$ was proposed in [8]. In [6, 7] it was shown that no extra security was gained in the matrix case since the DLP for matrices could be translated in polynomial time to a DLP over an extension field of K. In this paper we analyze the DH exchange scheme over GL_n and show that there exists a special class of exponents and session triples for which the DHP can be solved in time which is polynomial in the matrix size. This special class in the matrix case follows from the analogy of weak keys in the finite fields case. A full characterization weak keys in the matrix case however shall require much further analysis and should have fruitful applications. These problems shall be left for future research.

1.3 Organization of the paper

Next section of this paper develops the special cases of the DH scheme over the group $\mathbb{F}_{p^m}^*$. These are defined in terms of sets of private keys and it is shown subsequently that the DHP for these special cases can be solved in polynomial time without solving the DLP. The section is concluded with illustrative examples of weak keys over different cases of $\mathbb{F}_{p^m}^*$. In section 3 the definitions and analysis is extended to the matrix case over finite fields K and analogous results are proved. This section is also concluded with illustrative examples. In section 4 the DH conjecture is restated in view of these developments and some open problems are highlighted. Finally, concluding remarks summerize the importance of results to practice of the DH scheme.

2 Modulus conditions and conjugate classes over $\mathbb{F}_{p^m}^*$

In this section we describe weak keys of the DH scheme over the group $\mathbb{F}_{p^m}^*$ of nonzero elements of the finite field $\mathbb{F}_{p^m}$. Consider a session triple (a, k, l) being used by two users where a be an element of $\mathbb{F}_{p^m}^*$ of order n. (In most cases a will be a primitive element of $\mathbb{F}_{p^m}^*$ hence $n = p^m - 1$). The private keys k, l are in $\mathbb{Z}_n$. Let $(a, b, c) = (a, a^k, a^l)$ denote the public data of the session and $s = a^{kl}$ denote the shared key. For any a in $\mathbb{F}_{p^m}$ denote by $h(a, x)$ the minimal polynomial of a over $\mathbb{F}_p[x]$ (when a is primitive $\deg h = m$). Denote

$$\begin{aligned} h_c(x) &= \operatorname{lcm}(h(a, x), h(c, x)) \\ h_b(x) &= \operatorname{lcm}(h(a, x), h(b, x)) \end{aligned}$$

Following conditions define sets of private keys of central importance to this paper.

Definition 1 (Modulus conditions)**.** A session triple (a, k, l) is said to satisfy the modulus condition C1 if

$$x^k \bmod h(a, x) = x^k \bmod h_c(x) \tag{1}$$

while the triple (a, k, l) is said to satisfy modulus condition C2 if

$$x^l \bmod h(a, x) = x^l \bmod h_b(x) \tag{2}$$

Consider next another class of session triples.

Definition 2 (Conjugate class)**.** A session triple (a, k, l) is said to belong to the *conjugate class* relative to k (respectively l) if $h(a, x) = h(b, x)$ (respectively if $h(a, x) = h(c, x)$).

Thus (a, k, l) is in conjugate class relative to k if the public key b and generator a are conjugates. Further, in order to describe the weak private keys k, l of the DH scheme which are associated with weak session triples (a, k, l) we define following subsets of $\mathbb{Z}_n$.

Definition 3. Let a in $\mathbb{F}_{p^m}$ be fixed of order n. Define

1. Set of keys of the Conjugate class

$$C(n) = \{t \in \mathbb{Z}_n | t = p^r \bmod n, \text{ for some } 0 \leq r \in \mathbb{Z}\}$$

2. Keys satisfying modulus condition C1. Given $l \in \mathbb{Z}_n$

$$W_1(a, l) = \{k \in \mathbb{Z}_n | x^k \bmod h(a, x) = x^k \bmod h_c(x)\}$$

3. Keys satisfying modulus condition C2. Given $l \in \mathbb{Z}_n$

$$W_2(a, l) = \{k \in \mathbb{Z}_n | x^l \bmod h(a, x) = x^l \bmod h_b(x)\}$$

We show in what follows that the above sets $C(n)$ and $W_i(a, .)$ are weak keys of the DH scheme as the DHP can be solved in polynomial time for session triples (a, k, l) whenever either k or l lie in any one of these sets. In short we shall show that the set $W(a, l)$ denoting $W_1(a, l) \cup W_2(a, l)$ is a set of weak keys. By definition the sets W_1, W_2 depend on a and l. Hence $W(a, l)$ also depends on a and l.

2.1 Conditions for solving the DHP

The following theorems give necessary and sufficient conditions under which the shared key can be computed from the public data uniquely and can be expressed as a polynomial in the public data. These conditions are also useful for individual users of a DH scheme to determine whether or not their private keys are weak by looking at the public keys of the other user.

Theorem 1. The following statements hold

1. There exists a polynomial f in $\mathbb{F}_p[x]$ such that

   (a) $\deg f < \deg h(a,x)$

   (b) The following equations hold

   $$\begin{aligned} b &= f(a) \\ s &= f(c) \end{aligned} \tag{3}$$

   iff k belongs to $W_1(a,l)$.

   Moreover, f is the unique such polynomial satisfying the above two conditions

2. There exists a polynomial g in $\mathbb{F}_p[x]$ such that

   (a) $\deg g < \deg h(a,x)$

   (b) The following equations hold

   $$\begin{aligned} c &= g(a) \\ s &= g(b) \end{aligned} \tag{4}$$

   iff k belongs to $W_2(a,l)$.

   Moreover, g is the unique such polynomial satisfying the above two conditions.

Proof. Let f in $\mathbb{F}_p[x]$ exists satisfying the conditions (a), (b) above. Then $F(x) = x^k - f(x)$ belongs to $\mathbb{F}_p[x]$ and has roots a and c. Hence $F(x)$ is divisible by the minimal polynomials $h(a,x)$ and $h(c,x)$ hence also by $h_c(x)$ their lcm. Since $\deg h(a,x) \leq \deg h_c(x)$, $\deg f$ is less than the degrees of both of these polynomials. It follows that $f(x) = x^k \bmod h(a,x) = x^k \bmod h_c(x)$. Further, f is the unique such polynomial of required degree which must then satisfy (a),(b). This proves necessity of item 1 and uniqueness of f.

Conversely let $f(x) = x^k \bmod h(a,x) = x^k \bmod h_c(x)$. Then (a) and (b) hold. This proves sufficiency of item 1. Item 2 can be proved on similar lines. □

Remark 1. Computation of polynomial f (respectively g) in the above theorem from public data is a problem of solving linear systems $b = f(a)$ (respectively $c = g(a)$) for coefficients of f (resp. g) which are polynomials in $\mathbb{F}_p[x]$ of degree less than degree of $h(a,x)$. Further, if k belongs to one of the sets claimed then the shared key s can be computed as either $f(c)$ or $g(b)$.

As an analogous counterpart of the above theorem the following theorem gives conditions of weakness for the private key l.

Theorem 2. The following statements hold

1. There exists a polynomial f in $\mathbb{F}_p[x]$ such that
   (a) $\deg f < \deg h(a,x)$
   (b) The following equations hold

$$\begin{array}{rcl} c & = & f(a) \\ s & = & f(b) \end{array} \tag{5}$$

   iff l belongs to $W_1(a,k)$.

   Moreover, f is the unique such polynomial satisfying the above two conditions

2. There exists a polynomial g in $\mathbb{F}_p[x]$ such that
   (a) $\deg g < \deg h(a,x)$
   (b) The following equations hold

$$\begin{array}{rcl} b & = & g(a) \\ s & = & g(c) \end{array} \tag{6}$$

   iff l belongs to $W_2(a,k)$.

   Moreover, g is the unique such polynomial satisfying the above two conditions.

We omit the proof as it follows on similar lines as that of the proof of the earlier theorem.

One obvious class of keys k (respectively l) which is contained in $W_2(a,l)$ for any l (respectively contained in $W_2(a,k)$ for any k) are those for which the minimal polynomials satisfy $h(a,x) = h(b,x)$ (respectively $h(a,x) = h(c,x)$). Following theorem shows that this is precisely the conjugate class.

Theorem 3. $h(a,x) = h(a^k, x)$ iff k belongs to $C(n)$. Moreover $C(n) \subset W_2(a,k)$ for any k in $\mathbb{Z}_n$.

Proof. Elements a and a^k have the same minimal polynomial over $\mathbb{F}_p$ iff a^k is a root of the irreducible polynomial $h(a,x)$. By the well known characterization of roots of irreducible polynomials [18], $a^k = a^{p^r}$ for $r = 0,1,2,\ldots,(d-1)$ where $d = \deg h(a,x) \leq m$. However, in the splitting field $\mathbb{F}_{p^d}$ of $h(a,x)$ we have $a^{p^d} = a$. Hence $a^k = a^{p^r}$ for any $r > 0$. Hence $k = p^r \bmod n$. Thus without loss of generality we can assume $m = d$. Other statement is obvious. □

An important relationship between the conjugate class keys $C(n)$ and the set W_1 defined above is given by

Corollary 1. $W_1(a,r) = \mathbb{Z}_n$ iff $r \in C(n)$

Proof. Let r be in $C(n)$. Then $h(a,x) = h(a^r,x)$. Hence any t in $\mathbb{Z}_n$ belongs to $W_1(a,r)$. This proves sufficiency.

Conversely, let for some r, $W_1(a,r) = \mathbb{Z}_n$. Since $\operatorname{ord} a^r \leq \operatorname{ord} a$ and hence also $t = \deg h(a^r,x) \leq h(a,x) = d \leq n$. Let $h(a,x) = x^d + \phi(x)$ and $h(a^r,x) = x^t + \psi(x)$. If $t = d = n$ then both polynomials must be equal to $x^n - 1$. Hence assume $t \leq d < n$. If $t < d$ then $x^t \bmod h(a,x) = x^t$ while $x^t \bmod h(a^r,x)$ is polynomial of degree less or equal to $t-1$ which would give a contradiction. Hence $t = d$. On the hand, $\phi(x) = -x^d \bmod h(a,x)$ while $\psi(x) = -x^d \bmod h(a^r,x)$. Hence $\phi(x) = \psi(x)$. This proves necessity. □

In view of the fact proved below that the set $W(a,l)$ is a set of weak keys k, the above properties show that the set $C(n)$ is the set of fatally weak keys since l belongs to $C(n)$ implies all keys k in $\mathbb{Z}_n$ are weak. Further we have

Corollary 2. $C(n)$ is a multiplicative subgroup of $\mathbb{Z}_n^*$.

The proof follows from the fact that $C(n) =< p >$ (cyclic multiplicative monoide) in $\mathbb{Z}_n$ but since n is the order of a, n is coprime to p hence p has inverse in $\mathbb{Z}_n$. Note that the set $C(n)$ may not be small. For instance when p is a primitive root of the multiplicative group $\mathbb{Z}_n$ then every k in $\mathbb{Z}_n$ is of the form $p^r \bmod n$. However when p is not primitive in $\mathbb{Z}_n$ the cardinality of $C(n)$ is equal to the number of conjugates of a which is equal to m when the generator a is primitive in $\mathbb{F}_{p^m}$. In this case $C(n)$ has the smallest cardinality.

2.2 The scalar case

We now discuss the case of DH session where the generator a is chosen from $\mathbb{F}_p$ itself. Thus $m = 1$ and $h(a,x) = (x - a)$. In this case we have

Corollary 3.
1. $C(n) = \{1\}$.
2. $W_1(a,l) = \{k | k(l-1) \bmod n = 0\}$.
3. $W_2(a,l) = \{k | l(k-1) \bmod n = 0\}$.

Proof. In this case t is in $C(n)$ iff $(x - a) = (x - a^t)$ i.e. $a = a^t$. Since t is by definition in $\mathbb{Z}_n$, $t = 1$. Next, the modulus condition C1 holds for k given a fixed l iff $x^k \bmod (x - a) = x^k \bmod (x - c)$ which is equivalent to $a^k = c^k = a^{kl}$. Hence $k(l-1) \bmod n = 0$. Similarly k is in $W_2(a,l)$ iff $a^l = a^{kl}$ from which the claim follows. □

Finally, consider a to be the generator of $\mathbb{F}_p^*$ i.e. a primitive element. Then the order of a equals $p - 1$. Hence we get $W_1(a,l) = \{k | k(l-1) \bmod (p-1) = 0\}$. Similarly $W_2(a,l) = \{k | l(k-1) \bmod (p-1) = 0\}$ and also $C(n) = \{1\}$. Alternatively this implies that weak keys k satisfy one of the equations $c^k = c$ or $b^l = b$. Since the shared key is $s = c^k = b^l$, k is weak iff $s = c = b$. This is the classical setting for DH key exchange with a large prime p. In this setting the conjugate class is smallest. Further, if the order n of a is prime then the only weak k are $l^{-1} \bmod n$ which means the second user should not choose k such that b is an inverse of c modulo p. This description also shows that the field $\mathbb{F}_p$ is safest for DH key exchange with a primitive since weak keys are completely characterized by the above formulas.

2.3 Solving the DHP without solving DLP

We now investigate the problem of solving the DHP over $\mathbb{F}_{p^m}^*$ when either k is in $W(a,l)$ or l is in $W(a,k)$. Theorem 1 above gives criteria in terms of equations (3), (4) for the private key k to belong to set $W(a,l)$. Equations (3) and (4) are linear in coefficients of polynomials f and g whose solutions give the shared key s as either $f(c)$ or $g(b)$ whenever k or l are members of the sets $W(a,l)$, $W(a,k)$ respectively. In such situations an adversary can compute $f(c)$ and $g(b)$ from public data and succeeds in attacking the DH scheme.

Theorem 4. *Consider a session triple (a,k,l) in which either k belongs to $W(a,l)$ or l belongs to $W(a,k)$. Then the DHP can be solved in number of operations which grows at most as a polynomial in m over the field $\mathbb{F}_p$. The shared key computed is either $f(c)$ or $g(b)$. Moreover for $k,l \geq m$ this computation does not yield any of k, l.*

Proof. Since b and c both belong to the field $\mathbb{F}_p(a)$ we can assume without loss of generality that the degree of $h(a,x)$ is equal to m and that $\mathbb{F}_{p^m} = \mathbb{F}_p(a)$. The equation (3) then is an expression of b in the basis $1, a, a^2, \ldots, a^{m-1}$. The coefficients in this expression are the coefficients of the polynomial f. Hence computation of f is equivalent to change of basis expression for b in $\mathbb{F}_{p^m}$. This involves number of operations in $\mathbb{F}_p$ which is a polynomial in m. Similar conclusion holds for computation of g from the equation (4). Next the shared key s equals one or both of $f(c)$ or $g(b)$ by theorems 1, 2. This computation involves linear combination of the basis elements of $\mathbb{F}_{p^m}$ over $\mathbb{F}_p$ and is equivalent to a multiplication of an $m \times m$ matrix over $\mathbb{F}_p$ by an m-tuple. This proves the claim on number of operations.

Next we show that computation of polynomials f or g above does not yield k or l. Since f is computed from the equation $b = f(a)$ the data is independent of l. Also for $k \geq m$, $f(x) \neq x^k$ being a reminder of division by $h(a,x)$. Let $q(x)$ be the quotient. Then

$$x^k = q(x)h(a,x) + f(x)$$

The equation $b = f(a)$ is thus identical to

$$b = q(a)h(a,a) + f(a)$$

However $h(a,a) = 0$. Hence solution of f from $b = f(a)$ gives no information on $q(x)$. Since k and $q(x)$ are known simultaneously, this computation does not yield k. Similar reasoning shows that computation of g also does not yield l. That the shared key s equals $f(c)$ or $g(b)$ is proved above. □

Remark 2. The above theorem shows that the DHP is solvable in polynomial time whenever the session triples satisfy one of the modulus conditions without solving the DLP. We thus call the set $W(a,l)$, $W(a,k)$ the sets of weak keys and session triples (a,k,l) weak triples whenever one of the modulus conditions is satisfied. However the theorem gives no idea of the complexity of solving the DLP for these special class of triples. This is an open problem which shall be left for future work.

Given the generator a of a DH session the computation of f and g above depends on the knowledge of m the degree of the minimal polynomial $h(a,x)$ in $\mathbb{F}_p[x]$. However this one time computation can also be carried out in polynomial number of operations in m. In many practical cases, a shall be a root of the irreducible polynomial of the field extension $(\mathbb{F}_{p^m} : \mathbb{F}_p)$. Hence a polynomial basis of $\mathbb{F}_{p^m}$ shall be available.

2.3.1 Weak keys, weak session triples and a computational check

We close this section with an algorithm which provides a computational check on session triple (a, k, l) to verify the conditions of the above theorem. Recall that we denote the sets $W_1(a, l) \cup W_2(a, l)$ simply as $W(a, l)$. Thus by this notation, a session triple (a, k, l) is weak (i.e. satisfies any one of the modulus conditions C1 or C2) iff either $k \in W(a, l)$ or $l \in W(a, k)$. This algorithm builds from the criteria of theorem 1 in terms of equations (3), (4) for the private key k to belong to sets $W_1(a, l)$, $W_2(a, l)$ respectively. Consider a DH session in which the generator a and the public key c of the second user is known i.e. the private key l is already chosen.

Algorithm 1. (This algorithm checks whether a choice of k belongs to $W_1(a, l) \cup W_2(a, l)$ for a given public key c of the first user which leaves l fixed).
Input Generator a a primitive element in the field $\mathbb{F}_{p^m}$, order n of a and the public key c.

1. Choose k in $\mathbb{Z}_n$ randomly.
2. Compute $b = a^k$.
3. Compute polynomials $f(x)$, $g(x)$ in $\mathbb{F}_p[x]$ of degrees less than m such that

$$\begin{aligned} b &= f(a) \\ c &= g(a) \end{aligned}$$

(Alternatively, compute the coefficients in the expressions of b and c in terms of the polynomial basis $1, a, a^2, \ldots, a^{(m-1)}$ of $\mathbb{F}_{p^m}$. These are precisely coefficients of f and g. When h is the minimal polynomial of the extension $\mathbb{F}_{p^m}$ the co-efficients are available in the presentation of b and c).

4. Compute $s = c^k$.
5. Set boolean variable $X = 1$ if $(s - f(c))(s - g(b)) = 0$ else $X = 0$.

Output k, X, s. (Key k is weak if $X = 1$ and in that case s is the shared key).

Note that the above algorithm can be executed in polynomial time (in m) as already shown in the proof of the above theorem. The above algorithm computes weakness of the private key k and the subsequent shared key s. For computing weakness of the private key l and the corresponding shared key s we can execute an identical algorithm given below.

Algorithm 2. (This algorithm checks whether a choice of l belongs to $W_1(a, k) \cup W_2(a, k)$ for a given public key b of the first user which leaves k fixed).
Input Generator a a primitive element in the field $\mathbb{F}_{p^m}$, order n of a and the public key b.

1. Choose l in $\mathbb{Z}_n$ randomly.
2. Compute $c = a^l$.

3. Compute polynomials $f(x)$, $g(x)$ in $\mathbb{F}_p[x]$ of degrees less than m such that

$$\begin{aligned} b &= f(a) \\ c &= g(a) \end{aligned}$$

   (Alternatively, compute the coefficients in the expressions of c and b in terms of the polynomial basis $1, a, a^2, \dots, a^{(m-1)}$ of $\mathbb{F}_{p^m}$. These are precisely coefficients of f and g. When h is the minimal polynomial of the extension $\mathbb{F}_{p^m}$ the co-efficients are available in the presentation of b and c).

4. Compute $s = b^l$.

5. Set boolean variable $X = 1$ if $(s - f(c))(s - g(b)) = 0$ else $X = 0$.

Output l, X, s. (Key l is weak if $X = 1$ and in that case s is the shared key).

2.4 Existence and examples of weak keys

From the above development we can legitimately call the sets $W(a, r)$ as the sets of weak keys for given private keys r and a. The algorithm of the last section gives a computational check for these sets in terms of a and the public key of the first user. In fact we called the set $C(n)$ as fatally weak. Such weak keys must necessarily be avoided in a DH scheme. There now remains the question of existence and cardinalities of the sets $W(a, l)$ of weak keys as functions of a and l (respectively k). Existence of weak keys in $\mathbb{F}_{p^m}$ is immediate since the set of conjugate class keys $C(n) =< p >$ as shown above, where $< p >$ is the multiplicative group of units of $\mathbb{Z}_n$ and further $C(n) \subset W_{a,r}$ for any r in $\mathbb{Z}_n$. However $C(n)$ by itself is not large for primitive elements. A complete characterization of the sets $W(a, r)$ has not yet been found. However we provide a collection of samples of these sets in different fields $\mathbb{F}_{p^m}$ computed numerically. The number of weak keys as functions of parameters p, m, n does not appear to be negligible in general. At the same time it is difficult from these examples to quantify in general the number of weak cases with respect to the field parameters. The problem of fuller characterization of $W(a, r)$ shall be left for further work.

2.5 The Insecurity Factor

In the following examples, the percentages of weak k's for each of the l in the range $d \leq l < \operatorname{ord}(a) - 1$ are plotted for different finite fields of approximately same orders. Let L denote the ratio N_1/N_2 where N_1 = number of l for which there are approximately 10% or higher number of weak k, and $N_2 = \operatorname{ord} a - (d + 1)$. Percentage of weak keys of the order of 10% is practically noteworthy hence we choose this as a lower limit. On the other hand the number L denotes the percentage of weak cases for choice of the second private key. Let an *Insecurity Factor* denoted I be defined as the percentage of first key choice (say choice of l) for which at least 10% of the the second key choice (keys k) is weak. Then in terms of the above numbers $I = N_2 \times 100$. In practice this means that I% of the private keys chosen first are likely to be insecure.

Example 1. Weak keys in the field $\mathbb{F}_{p^m}$ for $p = 2$, $m = 7$. Generator polynomial $h(x) = x^7 + x + 1$. $\operatorname{ord} a = 127$. $L = 17/119 = 0.14$. See figure 1.

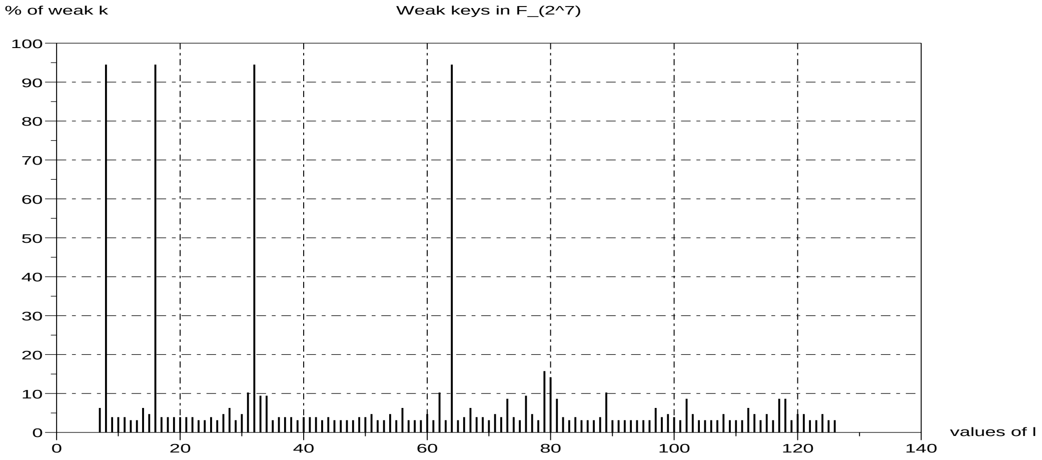

Figure 1: Weak keys for field characteristics p=2

In this example there is 14% chance for the choice of the first private key for which at least 10% of the second key choice is weak. Hence the insecurity factor is $I = 14\%$.

Example 2. Weak keys in the field $\mathbb{F}_{p^m}$ for $p = 5$, $m = 3$. Generator polynomial $h(x) = x^3 + 3x + 2$. $\operatorname{ord} a = 124$. $L = 39/120 = 0.33$. See figure 2.

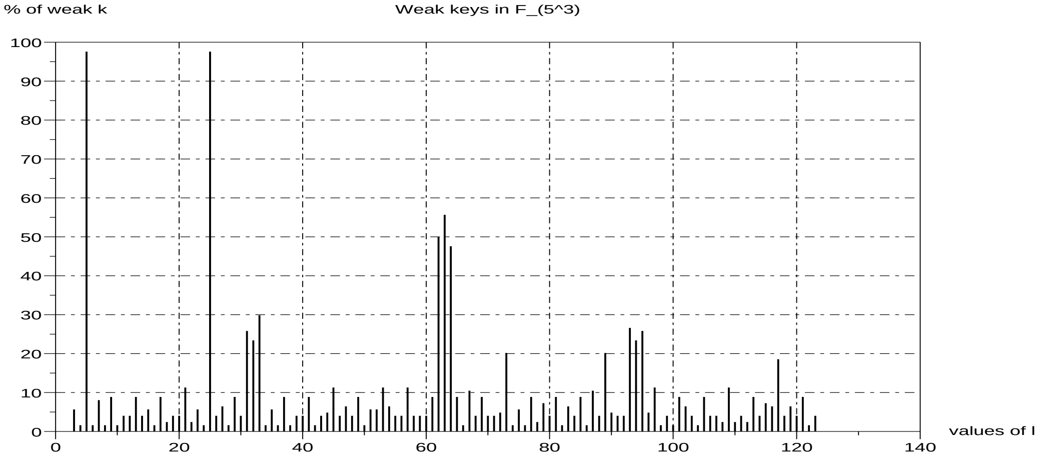

Figure 2: Weak keys for field characteristics p=5

Insecurity factor $I = 33\%$.

Example 3. Weak keys in the field $\mathbb{F}_{p^m}$ for $p = 11$, $m = 2$. Generator polynomial $h(x) = x^2 + 4x + 7$. $\operatorname{ord} a = 120$. $L = 31/117 = 0.26$. See figure 3. This plot also shows higher average of weak keys.

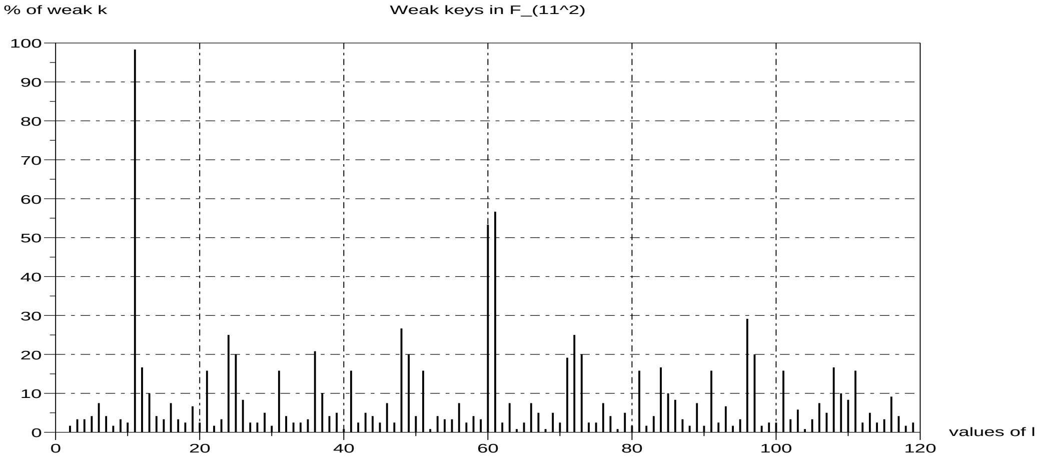

Figure 3: Weak keys for field characteristics p=11

Insecurity factor $I = 26\%$

Example 4. Weak keys in the field $\mathbb{F}_{p^m}$ for $p = 13$, $m = 2$. Generator polynomial $h(x) = x^2 + x + 2$. $\operatorname{ord} a = 168$. $L = 34/165 = 0.21$. See figure 4.

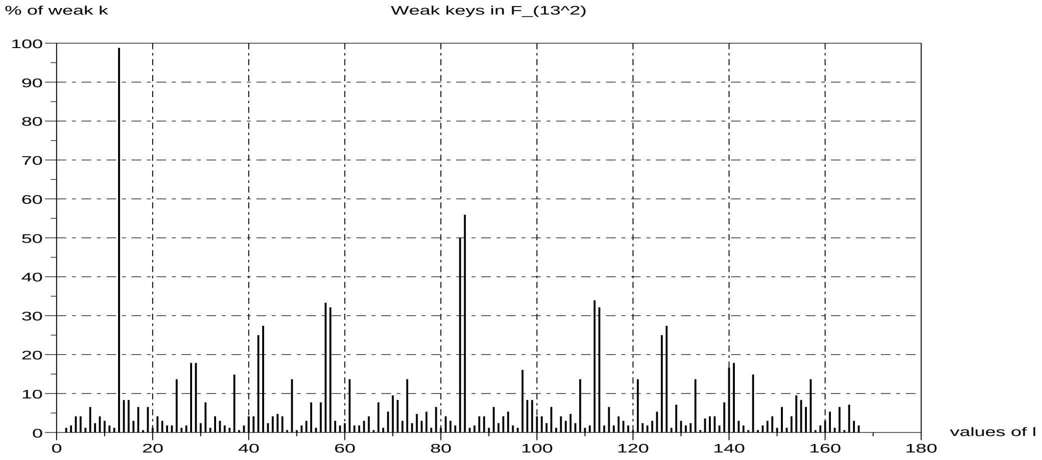

Figure 4: Weak keys for field characteristics p=13

Insecurity factor $I = 21\%$.

Example 5. Weak keys in the field $\mathbb{F}_{p^m}$ for $p = 11$, $m = 2$, $\operatorname{ord} a = 120$. Generator polynomial $h_1(x) = x^2 + 3x + 6$ with $L = 28/117 =$ and $h_2(x) = x^2 + 3x + 8$. $L = 31/117$. See figure 5.

Insecurity factor $I = 24\%$.

Example 6. In this example we present an instance of weak triple in a relatively large field, since a complete list by enumeration, as provided in previous examples is not feasible in reasonable time for such a large field. Let $\mathbb{F}_{11^{35}}$ be the finite field constructed with an irreducible polynomial $f(x) = x^{35} + 10x^{10} + 3$ over $\mathbb{F}_{11}$. Let a be a root of this polynomial. Consider a triple (a, k, l) with $(k, l) = (13244084834273, 10100)$. Now the public data (b, c) for this choice of k, l is $(b, c) = (9a^3, a^{30} + 8a^{25} + 6a^{20} + 10a^{15} + 2a^{10} + 10a^5 + 5)$. The shared key $s = a^{kl} = 9a^{25} + 2a^{20} + 7a^{15} + 5a^{10} + 3a^5 + 4$. Now the polynomial f such that $b = f(a)$ is $f(x) = 9x^3$. The shared key s can be computed as $f(c)$. Now we consider another triple (a, k, l) with $(k, l) = (39732254502817, 13567)$. The public data (b, c) for this choice of k, l is $(b, c) = (3a^7, 7a^{32} + 9a^{27} + a^{22} + 4a^{17} + 4a^{12} + a^7 + 7a^2)$. The shared key $s = a^{kl} = 2a^{34} + 4a^{29} + 6a^{24} + a^{19} + 10a^{14} + a^9 + 6a^4$. The polynomial f such that $b = f(a)$ is $f(x) = 3x^7$. The shared key s can be computed as $f(c)$.

2.6 Justification for evaluation of weakness

It might appear that even if one of the private keys of the users satisfies modulus condition it will not give an advantage to an adversary who cannot verify whether the shared key computed is indeed the actual shared key except in the case when one of the keys belongs

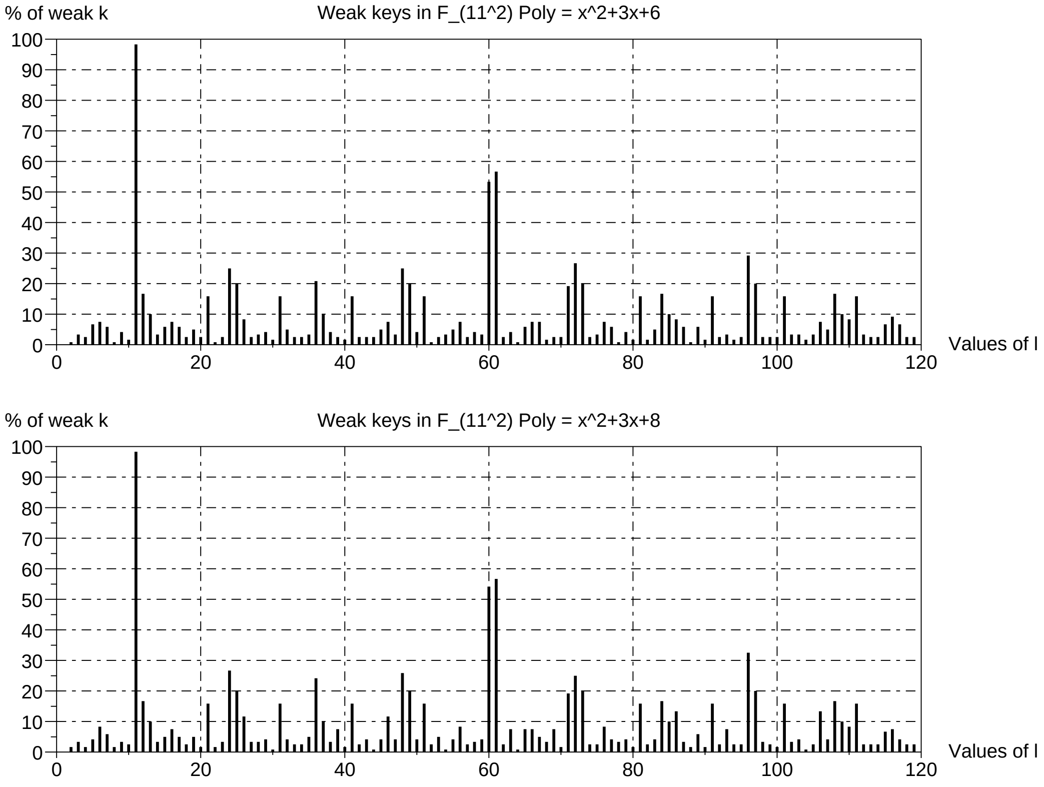

Figure 5: Weak keys for field characteristics $p = 11$ with different polynomials

to the conjugate class. However there are two issues here which are both relevant for secure implementation of the DH scheme.

1. The adversary can always compute the polynomials f, g from the public data and compute $s_1 = f(c)$ and $s_2 = g(b)$. If one of k, l is weak then one of these is the shared key. In practice shared keys are seeds for encryption algorithms on which chosen plain text attacks can be mounted. Hence having a probable seed compromises the encryption process since it is not any randomly chosen seed being tried. Hence it is assumed that being able compute the shared key compromises the key exchange even if the associated DH decision problem is not solved since in this case information outside of the DH session is being utilized.

2. Whether or not the a random private key chosen by a user is weak can be determined inexpensively by the user who selects the key after the first user has declared her public key. Hence since randomly chosen private keys can turn out weak it will be safer to carry out the check for weakness rather than take the randomly chosen private key which may be weak. Hence incorporating the algorithm for verifying weakness of the private key is not only inexpensive but provides safety.

These reasons amply justify evaluation of weakness of private keys of a DH session and shows that the weak keys proposed here are cryptographically relevant.

3 Modulus conditions and solution of the DHP in matrix case

In this section we develop an extension of some of the previous results over the matrix case. We shall denote the general linear group and the algebra of $n \times n$ matrices over a finite field K as $GL_n(K)$ and $M_n(K)$ or simply as GL_n and M_n respectively, whenever the field is known from the context. The minimal polynomial of a matrix A shall be denoted as $h(A, x)$. This is a monic polynomial $f(x)$ in $K[x]$ of least degree such that $f(A) = 0$. For completeness we pose the DHP below in the notation of the DH scheme introduced in the beginning.

Problem 1 (DHP over GL_n)**.** A matrix A in GL_n and matrices $B = A^k$ and $C = A^l$ are given for some unknown positive integers $k, l < \operatorname{ord} A$. Determine the matrix $A^{kl} = B^l = C^k$. The matrix A^{kl} is the shared key of the DH key exchange session. The triple (A, k, l) is called the session triple while (A, B, C) the public data of the DHP

The DLP is concerned with solving k from B (or that of l from C) and is analyzed in [7]. Clearly, solution of the DLP leads to the solution of the DHP above. Following the development of the last section we propose a special class of session triples (A, k, l) for which the DHP can be solved by an inexpensive computation and without solving the logarithms. Denote

$$\begin{aligned} h_c(x) &= \operatorname{lcm}(h(A,x), h(C,x)) \\ h_b(x) &= \operatorname{lcm}(h(A,x), h(B,x)) \end{aligned}$$

Proposition 1. There exist polynomials $f(x)$, $g(x)$ with $\deg f < \deg h_c$, $\deg g < \deg h_b$ such that

$$\begin{aligned} B &= f(A) \qquad (7) \\ C^k &= f(C) \qquad (8) \end{aligned}$$

and

$$\begin{aligned} C &= g(A) \qquad (9) \\ B^l &= g(B) \qquad (10) \end{aligned}$$

Conversely if any polynomials f, g satisfy above conditions then $f(x) = x^k \bmod h_c(x)$ and $g(x) = x^l \bmod h_b(x)$.

Proof. Let $f(x) = x^k \bmod h_c(x)$ and $g(x) = x^l \bmod h_b(x)$. Then these polynomials satisfy the above properties. Conversely, if $B = f(A)$ and $C^k = f(C)$ (respectively $C = g(A)$ and $B^l = g(B)$) then $x^k - f(x)$ (resp. $x^l - g(x)$) is an annihilating polynomial of both A and C and hence is divisible by $h_c(x)$. Clearly, since $\deg f < \deg h_c$ it follows that $f(x) = x^k \bmod h_c(x)$. Case for g can be proved similarly. □

Remark 3. Above proposition gives existence of polynomials f, g in $K[x]$ which can express the shared key $S = B^l = C^k$ in terms of the public data of any session triple (A, k, l).

An adversary of a DH key exchange session does not have the private keys k, l and hence cannot compute f, g above as residues of x^k, x^l. However the adversary can compute f, g from the equations (7), (9) respectively. These are linear equations in coefficients of f, g whose solutions are not necessarily unique. A special class of session triples (A, k, l) for which these solutions are unique facilitate solution of the DHP directly. These special triples are defined by

Definition 4 (The modulus conditions)**.** A session triple (A, k, l) with A in $GL_n(K)$ and is said to satisfy the *modulus condition* C1 if

$$x^k \bmod h(A, x) \quad = \quad x^k \bmod h_c(x)$$

while it is said satisfy *modulus condition* C2 if

$$x^l \bmod h(A, x) \quad = \quad x^l \bmod h_b(x)$$

Theorem 5. The following statements hold

1. There exists a polynomial $f(x)$ with $\deg f(x) < \deg h(A, x)$ which satisfies (7) and (8) iff (A, k, l) satisfies the modulus condition C1. Such a polynomial is unique.

2. There exists a polynomial $g(x)$ with $\deg g(x) < \deg h(A, x)$ which satisfies (9) and (10) iff (A, k, l) satisfies the modulus condition C2. Such a polynomial is unique.

Proof. Only the first item is proved as the second item follows by similar reasoning. Let (A, k, l) satisfy condition C1 and choose $f(x) = x^k \bmod h(A, x) = x^k \bmod h_c(x)$. Then f satisfies the required conditions. This proves sufficiency.

Conversely, let f be a polynomial of $\deg f < \deg h(A, x)$ which satisfies $B = f(A)$ and $C^k = f(C)$. Then $x^k - f(x)$ is annihilating for both A and C, hence divisible by their minimal polynomials. Hence $x^k - f(x)$ is also divisible by $h_c(x)$. Hence f is the unique polynomial which equals $x^k \bmod h(A, x) = x^k \bmod h_c(x)$ since $\deg f(x) < \deg h(A, x) \leq \deg h_c(x)$. This proves the necessity. □

Remark 4. Note that the equation $B = f(A)$ (resp. $C = g(A)$) always has a unique solution f (resp. g) of degree less than that of $h(A, x)$ given any public data (A, B, C) of a DH session. These equations are linear systems over the field K and have fixed size n^2 equations in d unknowns where d is the degree of $h(A, x)$ for any k (resp. l). The shared key C^k (resp. B^l) is then obtained as $f(C)$ (resp. $g(B)$) for triples (A, k, l) satisfying the modulus condition C1 (resp. C2) .

The modulus conditions also hold under following restricted conditions which is stated for completeness.

Proposition 2. 1. The triple (A, k, l) satisfies the modulus condition C1 if $x^k \bmod h(A, x) = x^k \bmod h(C, x)$

2. The triple (A, k, l) satisfies the modulus condition C2 if $x^l \bmod h(A, x) = x^l \bmod h(B, x)$

Proof. If (A, k, l) satisfies condition of the first item then there exist polynomials $q(A, x)$, $q(C, x)$ such that for $f = x^k \bmod h(A, x)$, $x^k - f = q(A, x)h(A, x) = q(C, x)h(C, x)$. Hence $x^k - f$ is a multiple of both $h(A, x)$ and $h(C, x)$ hence there exists a polynomial q such that $x^k - f = qh_c$. Since $\deg f < \deg h(A, x) \leq \deg h_c$ it follows that $f = x^k \bmod h_c$. The second condition can be proved similarly. □

It can be shown that the above conditions are equivalent to C1, C2 respectively when the field K has zero characteristics while in finite fields they are in general strictly sufficient. We omit further discussion of this fact.

3.1 Solution of the DHP without solving the DLP

We now show that for triples (A, k, l) satisfying the modulus conditions C1 or C2 the computation of the shared key A^{kl} by computing either f or g does not yield k or l. In the following we present the analysis only with respect to the modulus condition C1. The other case relating to condition C2 can be analyzed on identical lines.

Theorem 6. Let the triple (A, k, l) satisfy condition C1 and $k \geq \deg h(A, x)$. Then computation of $f(x)$ from the equation $B = f(A)$ such that $\deg f(x) < \deg h(A, x)$, solves the DHP with the shared key $S = f(C)$ but does not yield either of k or l.

Proof. Clearly the equation $B = f(A)$ does not involve l. Hence its solution is independent of l. Next, since (A, k, l) satisfies C1, it follows from theorem 1 that $S = C^k = f(C)$ (thereby solving the DHP) and that there exist a unique polynomial $q(x)$ such that

$$x^k = q(x)h(A, x) + f(x)$$

Since $q(x)$ is the quotient and f the reminder when x^k is divided by $h(A, x)$, it follows that given the reminder f and divisor $h(A, x)$, both the dividend x^k and the quotient $q(x)$ are known simultaneously i.e. knowledge of k yields that of $q(x)$ and conversely. Since $k \geq \deg h(A, x)$, $f(x) \neq x^k$. Now as $h(A, x)$ is the minimal polynomial of A, $h(A, A) = 0$. The equation $B = f(A)$ is thus identical to

$$A^k = q(A)h(A, A) + f(A)$$

Hence $q(A)$ cannot be known from the knowledge of f as $h(A, A) = 0$. This implies solution of f from the equation $B = f(A)$ does not yield k. □

In general there is no unique k for a given reminder f in the above equation. For, if k and $k' > k$ both give same reminder f for quotients q, q' then, $x^{k'} - x^k$ is divisible by h. Hence assuming f nonzero, $x^{k'-k} - 1$ is divisible by h. This shows that $k' = k + m \operatorname{ord} h$, where $\operatorname{ord} h$ is the order of the polynomial h in $K[x]$. The following example shows two such exponents. Consider the finite field $\mathbb{F}_3$. $h(x) = x^3 + x^2 + 2x + 1$, this polynomial has order 26 equal to that of its companion matrix in $GL_3(\mathbb{F}_3)$. let $f(x) = 2x^2$. Then for both $k = 15$ and $k = 41$, $x^k - f(x)$ can be shown to be divisible by $h(x)$.

This theorem shows that for triples (A, k, l) satisfying the modulus condition and with k sufficiently large, it is possible to compute the shared key A^{kl} without computing k or l. In the next section we discuss such a computation in more detail.

3.2 Polynomial time solution of the DHP

For session triples satisfying either of the modulus conditions C1, C2 it is shown above that the DHP is solved by computing the polynomials $f(x)$, $g(x)$ respectively. Following algorithm can be used to compute the shared key.

Algorithm 3. Input: Public data (A, B, C) of a DH session and the degree m of the minimal polynomial $h(A, x)$.

1. Compute $f(x)$ with $\deg f < m$ from the equation $B = f(A)$.
2. Compute $g(x)$ with $\deg g < m$ from the equation $C = g(A)$.
3. Compute $S_1 = f(C)$.
4. Compute $S_2 = g(B)$.
5. Output: Shared key $S = S_1$ if (A, k, l) satisfies C1.
6. Output: Shared key $S = S_2$ if (A, k, l) satisfies C2.

Note that computation of $h_c(x)$ respectively $h_b(x)$ is not required for computing S_1, S_2. Computation of the degree m of $h(A, x)$ is a one time operation in the task of solving the DHP for the scheme in which the generator A is fixed. Moreover it is well known that the degree of the minimal polynomial of a matrix over a field K can be computed in time polynomial in the matrix size. (This is equivalent to checking linear independence of the the matrices I, A, ..., A^{q-1} for $q \leq n$ over K in the algebra $K^{n \times n}$ where n is the matrix size). It is also useful for users to have an algorithm for verifying whether the keys chosen satisfy the modulus conditions. Such an algorithm is presented in the next section in the case of fields.

Theorem 7. If the session triple (A, k, l) satisfies any one of the modulus conditions C1 or C2, then given $m = \deg h(A, x)$ the DHP can be solved in number of operations in the field K of entries of A which grows at most as a polynomial in n. However it is not clear how much complex it is to solve the DLP for such triples.

Proof. Above algorithm shows that computation of polynomials f and g solves the DHP when the triple (A, k, l) satisfies any one of the conditions C1, C2. Hence the theorem is proved if it is shown that solutions of these polynomials can be computed in time polynomial in n. The coefficients of polynomial f and g are the unique solutions of the linear systems of equations $B = f(A)$ and $C = g(A)$ over the field K. These systems have fixed size, n^2 equations in m unknowns. Since $m \leq n$ the number of operations required for solving these equations in K by the Gaussian algorithm is at most $2n^3$. □

Remark 5. Note that the theorem does not give an indication of how complex it is to solve the DLP in the special cases of triples (A, k, l) satisfying the modulus conditions.

In view of the above result we shall state briefly that, for session triples satisfying any one of the modulus conditions C1, C2, "the DHP is solvable in polynomial time".

3.3 Conjugate class session triples

Consider the public data (A, B, C) of the DH scheme. The problem to be addressed now is to decide whether or not the triple (A, k, l) satisfies the modulus condition, purely from the public data. This is possible in a special class of triples defined below.

Definition 5. A triple (A, k, l) is said to belong to the *conjugate class* relative to k if $h(A, x) = h(B, x)$ and relative to l if $h(A, x) = h(C, x)$.

Theorem 8. For session triples (A, k, l) belonging to the conjugate classes relative to any one of k or l the DHP is solvable from the public data in polynomial time without solving the DLP.

Proof. Consider the public data (A, B, C) of the DHP. If the triple (A, k, l) belongs to the conjugate class relative to l, then it clearly satisfies the modulus condition C1. The knowledge that this is so is obtained only from A and C which belong to the public data. The polynomial f is now solved from the equation (7) and the shared key equals $C^k = f(C)$. Hence the shared key is computed purely from the public data. The computation of f moreover does not imply computation of k or l due to theorem 6. Thus the DHP is solvable without solving the DLP for these special class of triples. The statement about solvability in polynomial time is proved above. The case of conjugate class relative to k follows similarly. □

In view of the above theorem it follows that the session triples belonging to the conjugate classes relative to either k or l must be excluded from the DH conjecture as obvious exceptions. However since for the triples satisfying the modulus conditions the DHP is solvable in polynomial time, these triples are weak cases of the DH scheme. Finally, there is also the question of existence of weak triples (A, k, l) which remains to be answered for matrices A in GL_n. While such existence can be easily shown, we shall skip this question in the interest of brevity and also owing to the importance of the field case treated in the next section where we establish the existence of weak triples in detail. We conclude this section however with illustrative examples.

3.4 Examples

In this section we present examples which illustrate the above theory for solving the DHP for matrices. The parameters used in these problems are of very small sizes and by no means realistic.

Example 7. Consider the field be $\mathbb{F}_{53}$ and A in GL_2 given by

$$A = \begin{bmatrix} 1 & 51 \\ 1 & 1 \end{bmatrix}$$

Let $k = 3$, $l = 53$ then

$$A^3 = B = \begin{bmatrix} 48 & 51 \\ 1 & 48 \end{bmatrix} \qquad C = A^{53} = \begin{bmatrix} 1 & 2 \\ 52 & 1 \end{bmatrix}$$

The shared key is

$$A^{53\times 3} = \begin{bmatrix} 48 & 2 \\ 52 & 48 \end{bmatrix}$$

The minimal polynomials are $h(A,x) = h(C,x) = x^2 + 51x + 3$. Now the polynomial Solution of the linear system $B = f(A)$ gives $f(x) = x + 47$. It is easy to see that $A^{53\times 3} = f(C)$. In this example the exponent $l = 53$ is of the form p^j for $j = 1$. Where p is the field characteristic.

Example 8. In this example $h(A,x) = h(C,x)$ is satisfied for exponents k, l which are not of the form p^j. Let the field be $\mathbb{F}_{13}$. The matrices A, B and C are given respectively as

$$A = \begin{bmatrix} 2 & 0 \\ 0 & 7 \end{bmatrix} \quad B = A^3 = \begin{bmatrix} 8 & 0 \\ 0 & 5 \end{bmatrix} \quad C = A^{11} = \begin{bmatrix} 7 & 0 \\ 0 & 2 \end{bmatrix}$$

The shared key A^{kl} is given by

$$A^{3\times 11} = \begin{bmatrix} 5 & 0 \\ 0 & 8 \end{bmatrix}$$

Now solving the linear system $B = f(A)$ gives the polynomial $f(x) = 2x + 4$. Then it can be seen that $f(C) = A^{kl}$.

Example 9. This example shows that modulus condition is satisfied even if $h(A,x) \neq h(C,x)$. Let the field be $\mathbb{F}_7$. The matrix A is chosen as

$$A = \begin{bmatrix} 0 & 5 \\ 1 & 0 \end{bmatrix}$$

Let $k = 7$ and $l = 3$. Then

$$B = \begin{bmatrix} 0 & 2 \\ 6 & 0 \end{bmatrix} \qquad C = \begin{bmatrix} 0 & 4 \\ 5 & 0 \end{bmatrix}$$

The shared key A^{kl} is

$$A^{7\times 3} = \begin{bmatrix} 0 & 3 \\ 2 & 0 \end{bmatrix}$$

Solving the linear system $B = f(A)$ gives $f(x) = 6x$. Then the shared key can be computed as $A^{21} = 6C$. Here $h(A,x) = x^2 + 2$ and $h(C,x) = x^2 + 1$. Since $k = 7$, we get $6x = x^7 \bmod h(A,x) = x^7 \bmod h(C,x)$.

4 Revised DH conjecture and open problems

The analysis of the DH scheme on $\mathbb{F}^*_{p^m}$ and GL_n above shows existence of special session triples for which the DHP can be solved by an adversary inexpensively without solving the DLP. Since such exceptions can be easily determined by the second user of the scheme from the knowledge of her own private key, a repeated choice of the private key along with such check should result in a strong session triple. Hence the security of the DH scheme depends on the non-solvability of the DHP outside the exceptional class of session triples satisfying the modulus conditions. However this also leads to an unanswered question. In view of the DH conjecture stated above we can thus make a revised conjecture as follows.

Conjecture 2 (Revised Diffie Hellman Conjecture)**.** The Diffie Hellman conjecture stated above is true for all session triples which do not satisfy any one of modulus conditions.

If the above statement is proved to be true, then the DH scheme shall be secure for sessions triples not satisfying the modulus conditions.

It has already been remarked above that although it was possible to prove that the DHP is solvable in polynomial time for the special class of triples which satisfy modulus conditions, no conclusion could be drawn regarding complexity of solving the DLP for these triples since the solution of the DHP did not yield the exponents. We state this as an open problem

Problem 2 (Open)**.** Determine the time complexity of solving the exponents k, l for any session triple (a, k, l) which satisfies one of the modulus conditions.

Next, it is shown above that for triples (a, k, l) satisfying one of the modulus conditions, the DHP is solvable in polynomial time. However whether polynomial time solvability characterizes the class of triples satisfying modulus conditions is not known. We state this as another open problem

Problem 3 (Open)**.** Show that if the DHP can be solved in polynomial time for a session triple (a, k, l) then the triple satifies one of the modulus conditions.

5 Concluding remarks

Special cases of session triples of the DH scheme over groups $\mathbb{F}_{p^m}^*$ and GL_n exist for which the DHP can be solved in polynomial time without solving the DLP. These are triples (a, k, l) which satisfy any one of the modulus conditions. Hence such special cases can be called weak cases of the DH scheme and must be excluded from use in this scheme. The analysis and examples of weak cases over finite fields show that the number of weak keys may not be insignificant to be ignored and depends on the generator a, the parameters of the field extension as well as the private key of the other user. A simple computational algorithm is proposed to determine the weak triples. This algorithm can be used in practice by the second user of the DH scheme (who has the public key of the first user) for choice of her private key by discarding keys which turn out weak. A complete characterization of weak keys as well as algorithms for avoiding them in practical implementations are desirable to make the DH key exchange secure from the simple algebraic attack proposed in this paper. Finally the question of complexity of solving the DLP for these special class of session triples remained unresolved. It should be worthwhile to know whether the DLP for these session triples can also be solved in polynomial time. The Diffie Hellman conjecture is restated in view of these exceptions and is conjectured to be true outside the exceptions reported as weak keys here. The second part of this paper shall report extension and application of the above weak keys of the DH scheme for pairing based DH schemes on elliptic curves.

Acknowledgements

The authors are grateful to Professor Balwant Singh for enlightening discussions and encouragement.

References

[1] W. Diffe and M. Hellman, “New directions in crptography”, IEEE Trans. on Information Theory, vol. 22, pp. 644-654, 1976.

[2] D. Boneh and R. Lipton, “Algorithms for black-box fields and their application to cryptography”, in Advances in Cryptology - Crypto’96, Lecture Notes in Comp. Sc., vol. 1109, pp. 283-297, Springer Verlag, 1996.

[3] B. den Boer, “Diffie Hellman is as strong as discrete logs for certain primes”, in Advances in cryptology - Crypto’88, Lecture Notes in Comp. Sc., vol. 403, pp. 530-539, Springer Verlag, 1988.

[4] U. Maurer, ”Towards the equivalence of breaking the Diffie Hellman protocol and computing discrete logarithms”, Advances in Cryptology - Crypto’94, Lecture Notes in Comp. Sc. vol. 839, pp. 271-281, 1994.

[5] A. J. Menezes, T. Okamoto and S. A. Vanstone, “Reducing elliptic curve logarithm to logarithms in finite fields”, IEEE Trans. on Information Theory, vol. 39, pp. 1639-1646, 1993.

[6] A. J. Menezes and S. Vanstone, “A note on cyclic groups, finite fields and the discrete logarithm problem”, Applicable Algebra in Engineering Communication and Computing, vol. 3, pp. 67-74, 1992.

[7] A. J. Menezes and Yi-Hong Wu, “The discrete logarithm problem in GL_n”, ARS Combinotoria, vol. 47 pp. 23-32, 1998.

[8] R. Odoni, V. Varadharajan and R. Sanders, “Public key distribution in matrix rings”, Electronic Letters, vol. 20, pp. 386-387, 1984.

[9] A. J. Menezes, P. C. van Oorschot and S. A. Vanstone, “The Handbook of Applied Cryptography” CRC Press, 1997.

[10] N. Koblitz, ”Elliptic curve cryptosystems”, Math. Computat. vol. 48, pp. 203-209, 1987.

[11] V. Miller, “Uses of elliptic curves in cryptography”, in Advances in Cryptology - Crypto’85, Lecture Notes in Comp. Sc. vol. 218, pp. 417-426, Springer Verlag, New York, 1986.

[12] T. ElGamal, ”A public key cryptosystem and a signature scheme based on discrete logarithms”, IEEE Trans. on Information Theory, vol. 31, pp. 469-472, 1985.

[13] D. Stinson, "Cryptography, Thoery and Practice", Chapman & Hall/CRC, 2002.

[14] D. Hankerson, A. Menezes, S. Vanstone, "Guide to elliptic curve cryptography", Springer, 2004.

[15] L. Washington, " Elliptic curves, number theory and cryptography", CRC press, 2003.

[16] A. Joux, " A one round protocol for tripartite Diffie Hellman", Proc. ANTS 4, Lecture Notes in Comp. Sc., vol. 1838, pp. 385-394, 2000.

[17] R. Dutta, R. Barua, P. Sarkar, "Pairing based cryptographic protocols: A survey", Cryptology ePrint Archive, 2004/64. http://eprint.iacr.org/2004/064.

[18] R. Lidl, H. Niederreiter, "Finite Fields", Ency. of Math. and Its Appln. Cambridge University Press, 1997.

[19] D. Boneh, M. Franklin, "Identity based encryption from the Weil pairing". In Advances in Cryptology, Crypto 2001. Lecture notes in Comp. Sc. vol. 2139, pp. 213-229, Springer Verlag.