On the Diffie-Hellman problem over GL_n

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

January 27, 2005

Abstract

This paper considers the Diffie-Hellman problem (DHP) over the matrix group GL_n over finite fields and shows that for matrices A and exponents k, l satisfying certain conditions called the *modulus conditions*, the problem can be solved without solving the discrete logarithm problem (DLP) involving only polynomial number of operations in n. A specialization of this result to DHP on $\mathbb{F}_{p^m}^*$ shows that there exists a class of session triples of a DH scheme for which the DHP can be solved in time polynomial in m by operations over $\mathbb{F}_p$ without solving the DLP. The private keys of such triples are termed *weak*. A sample of weak keys is computed and it is observed that their number is not too insignificant to be ignored. Next a specialization of the analysis is carried out for pairing based DH schemes on supersingular elliptic curves 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 embedding degree. A list of weak parameters of the DH scheme is developed on the basis of this analysis.

Key Words : Discrete logarithms, General linear group, Extension fields, Elliptic curves, Diffie Hellman scheme.

1 Introduction

A key exchange scheme over public channels based on discrete logarithms over finite cyclic groups was proposed by Diffie and Hellman in [1]. Known as the Diffie Hellman (DH) scheme, this scheme was a major advance in cryptography since it resolved both, the problem of key agreement by two users over a public channel and that of authentication. For the DH scheme to be secure the complexity of computation of the discrete logarithms over the group concerned should necessarily be high. On nonzero elements of finite fields $\mathbb{F}_{p^m}^*$ best known algorithms for computation of the discrete logarithm are of sub-exponential time complexity while on a generic class of cyclic subgroups of order n of elliptic curves these are of the order $O(\sqrt{\pi n/2})$ group operations [14]. Apart from the case of discrete logarithms over supersingular elliptic curves no sub-exponential time algorithm is known for their computations on general elliptic curves. Elliptic curves with cyclic subgroups of very large orders can be constructed on finite fields by well known methods. These groups are thus found useful for practical implementation of the DH scheme.

There is however the (as yet unfalsified) DH conjecture (or the DH assumption) which is also of equal importance in providing security to the DH scheme. According to this conjecture, the shared key in the DH scheme can be computed by a passive adversary only by solving the (hard) discrete logarithm problem (or a problem of equivalent complexity). Such should be the case for a generic class of parameters of the DH session over the concerned group for the scheme to be secure. Although the conjecture remains unresolved, it is widely believed to be true. It is nevertheless important to identify exceptions to the DH conjecture in order to make the DH scheme truly secure.

The purpose of this paper is to show existence of special cases of session parameters which are exceptions to the Diffie Hellman assumption and thus should be excluded from the DH schemes over groups such as the GL_n over finite fields, $\mathbb{F}_{p^m}^*$ and the supersingular elliptic curves. We show that in these special cases of session parameters, the shared key can be computed in polynomial time proportional to the matrix size (n in case of the matrix group GL_n or m in the case of $\mathbb{F}_{p^m}^*$) and further this computation can be performed without solving the discrete logarithms. For this reason we call private keys associated with such parameters, *weak keys* of the DH scheme over the respective groups. A generalization of such weak keys is then proposed for the DH scheme over elliptic curves E over $\mathbb{F}_p$ and it is shown that the image of the shared key in an extension field $\mathbb{F}_{p^m}$ provided by a paring on the curve can be computed in time polynomial in m given the public data in $\mathbb{F}_{p^m}$. Such weak keys are of significance to some of the paring based schemes on supersingular elliptic curves [15, 16, 18]. Currently a complete characterization of these weak keys is not known. However a sample of computations shown in this paper reveals that the density of such weak keys depends on several parameters and can be sometimes significant among the set of all permissible keys. This signifies the cryptographic relevance of this class of weak keys in practical DH schemes wherein more constraints need to be specified in the selection of private keys in order to exclude the weak keys.

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). This describes in brief our notation for the DH key exchange scheme and the two problems DHP and the DLP.

1.2 The Diffie Hellman conjecture

The DH conjecture (or the DH assumption on the key exchange scheme) is often found stated independent of computational complexities. It is by and large well known that the DHP is at least as difficult to solve as the DLP [9, 13]. We consider below a statement using above terminology

Conjecture 1 (Diffie Hellman conjecture). 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).

From a computational point of view the DH conjecture amounts to stating that the DHP cannot be solved in time complexity lower than that required for solving the associated DLP. In this paper we establish existence of a special class of session triples (a, k, l) and consequently the private keys k, l called weak keys for which the DHP can be solved in polynomial time without solving the DLP in the groups GL_n and $\mathbb{F}_{p^m}^*$. We then show that these results also lead to a polynomial time computation of the shared key of a DH session over certain elliptic curves in a suitable extension of the field of definition. Hence such weak keys can be considered as exceptions to the DH conjecture and must be avoided in practice.

There are other well known statements of the DH conjecture and results regarding the relationship between the two problems DHP and the DLP. For instance, 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].

1.3 Importance of solving the DHP over rings

One striking feature of the solution of the DHP in special cases over $GL_n(K)$ presented in this paper is that although the powers A^k of A involved are in the group $GL_n(K)$, the algorithm used for solving the DHP makes use of the embedding $GL_n(K) \subset M_n(K)$ where $M_n(K)$ is the algebra of $n \times n$ matrices over K. The DLP and DHP are originally posed without such an identification of the cyclic subgroup of G into a cyclic subgroup of $GL_n(K)$ for some K. Hence it is worthwhile to determine solutions of these problems over rings and examine whether there exist special cases defying the DH assumption after utilizing the additional structure of an algebra. In other words, these problems should be analyzed over cyclic subgroups of the group of units of a ring. This suggests that the the cryptanalysis of the DH scheme over different groups need be carried out using representations of these groups. Similar ideas have been proposed as "isomorphism attacks" on elliptic curve cryptography [14].

The generalization of the DLP over matrices 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 show that the DH exchange is fatally insecure for a special class of pairs of exponents owing to the fact that the DHP in these special cases can be solved in time polynomial in the matrix size. We then adapt the solution technique of the matrix case to finite fields $\mathbb{F}_{p^m}$ and derive analogous special cases leading to *weak keys*. We again show how for these weak keys the DHP gets resolved in polynomial time. For the DH schemes based on pairings over supersingular elliptic curves $E/\mathbb{F}_p$ we show that this method allows computation of the image of the shared key in an extension field $\mathbb{F}_{p^m}$ in time polynomial in m for an analogous class of session triples. Such an image of the shared key of a DH scheme on elliptic curves is utilized in multiparty and identity based key exchange schemes [15, 16, 18]. Hence the security of these schemes is compromised if the session triples fall into this class of special triples since the associated DHP has an inexpensive solution. Further analysis of these schemes and computation of weak keys of the triparty DH scheme shall be a topic of future research.

2 Modulus conditions and solution of the DHP in matrix case

In this section we develop some of the preliminary 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 that of solving for 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. 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

$$\begin{aligned} B &= f(A) && (1) \\ C^k &= f(C) && (2) \end{aligned}$$

and

$$\begin{aligned} C &= g(A) && (3) \\ B^l &= g(B) && (4) \end{aligned}$$

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 1. 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 (1), (3) 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 1 (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 1. The following statements hold

1. There exists a polynomial $f(x)$ with $\deg f(x) < \deg h(A, x)$ which satisfies (1) and (2) 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 (3) and (4) 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 2. 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.

2.1 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 2. 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.

2.2 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 1. 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, $\ldots$, 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 3. 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 3. 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".

2.3 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 2. 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 4. 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 (1) 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 2. 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.

2.4 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 1. 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 2. 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 3. 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 $6x = x^7 \bmod h(A,x) = x^7 \bmod h(C,x)$.

In the next section we show ways to extend results of this section to other groups such as $\mathbb{F}_{p^m}^*$ and groups of elliptic curves over $\mathbb{F}_p$ which lead to the solution of the DHP for an analogous class of triples such as those satisfying the modulus condition and for the conjugate class above.

3 Weak keys of the DH scheme over finite fields

The groups such as the nonzero elements of finite fields $\mathbb{F}_{p^m}^*$ are among the common examples of groups over which the DH scheme has been implemented. These form special cases of the matrix case of the DH scheme discussed above. This is because elements of $\mathbb{F}_{p^m}^*$ under multiplication act as linear operators in the field $\mathbb{F}_{p^m}$ which is an m dimensional vector space over $\mathbb{F}_p$. Hence under a fixed basis of $\mathbb{F}_{p^m}$ the group $\mathbb{F}_{p^m}^*$ is identified with a commutative subgroup of $GL_m(\mathbb{F}_p)$. We now develop the special cases of session triples of the DH scheme over $\mathbb{F}_{p^m}^*$ for which the DHP can be solved in polynomial time without solving the associated DLP.

3.1 Modulus conditions and conjugate classes

In the present field case a matrix representation of elements is in fact not necessary. We shall thus write analogous definitions in this case following those of the matrix case above. Consider a session triple (a, k, l) being used by two users where a is an element of K^* of order n. 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 $\mathbb{F}_p[x]$. Let $h_c(x) = \operatorname{lcm}(h(a, x), h(c, x))$ and $h_b(x) = \operatorname{lcm}(h(a, x), h(b, x))$.

Definition 3 (Modulus conditions). The triple (a, k, l) is said to satisfy the modulus condition C1 if

$$x^k \bmod h(a, x) = x^k \bmod h_c(x) \tag{5}$$

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

$$x^l \bmod h(a, x) = x^l \bmod h_b(x) \tag{6}$$

Next we define the conjugate class of session triples.

Definition 4 (Conjugate class). The 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 $h(a, x) = h(c, x)$).

In order to exhibit the weak private keys k, l of the DH scheme which are associated with weak session triples (a, k, l) we make following definitions.

Definition 5. Let a in $\mathbb{F}_{p^m}$ be fixed of order n. Define

1. 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 are weak keys since the DHP can be solved in polynomial time for session triples (a, k, l) whenever either k or l lie in any one of the above 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.

3.2 Conditions for solving the DHP

The following theorems give necessary and sufficient conditions under which the DHP can be solved in a special way in that 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 5. 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

$$\begin{array}{rcl} b & = & f(a) \\ s & = & f(c) \end{array} \tag{7}$$

   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

$$\begin{array}{rcl} c & = & g(a) \\ s & = & g(b) \end{array} \tag{8}$$

   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 4. 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 $g(b)$.

Above theorem is essentially identical to theorem 1. As an analogous counterpart of the above theorem the following theorem gives conditions of weakness for the private key l.

Theorem 6. 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

$$\begin{aligned} c &= f(a) \\ s &= f(b) \end{aligned} \tag{9}$$

   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

$$\begin{aligned} b &= g(a) \\ s &= g(c) \end{aligned} \tag{10}$$

   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 7. $h(a, x) = h(a^k, x)$ 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 [17], $a^k = a^{p^r}$ 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 above properties we call the set $C(n)$ the set of fatally weak keys. 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 $p^r \bmod n$. We provide instances of this situation in examples.

3.3 The scalar case

We now discuss the case of DH session where the generator a is chosen from $\mathbb{F}_p$. 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. 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 formulae.

3.4 Solving the DHP without solving DLP

We now investigate the problem of solving the DHP over $\mathbb{F}_{p^m}^*$ when either of the keys k, l are weak. The results of the matrix case above when specialized by considering the generator a in the present case as an element of $GL_m(\mathbb{F}_p)$, are also applicable for the present case. Hence it follows that when either of the private keys are weak, the DHP can be solved in time complexity polynomial in m without solving the DLP. We shall however establish this result without resorting to the matrix case.

Theorem 5 above gives criteria in terms of equations (7), (8) for the private key k to belong to sets $W_1(a,l)$, $W_2(a,l)$ respectively. Equations (7) and (8) 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 these sets. In such situations an adversary can compute $f(c)$ and $g(b)$ from public data and succeeds in attacking the DH scheme.

Theorem 8. Consider a session triple (a,k,l) in which either k belongs to $W_1(a,l) \cup W_2(a,l)$ or l belongs to $W_1(a,k) \cup W_2(a,k)$. 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 (7) 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 (8). Next the shared key s equals one or both of $f(c)$ or $g(b)$ by theorems 5, 6. 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 5. The above theorem shows that the DHP is solvable in polynomial time whenever the session triples satisfy one of the modulus conditions. However the theorem gives no idea of the complexity of solving the DLP for these special class of triples. This shall be left as an open problem 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 as in the matrix case. Due to the above theorem we call the session triples (a, k, l) weak whenever any one of the modulus conditions are satisfied.

3.4.1 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. For convenience 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 5 in terms of equations (7), (8) 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 2. (This algorithm checks whether a choice of k belongs to $W_1(a, l) \cup W_2(a, l)$ for a given l).

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 basis $1, a, a^2, \ldots, a^{(m-1)}$ of $\mathbb{F}_{p^m}$. These are precisely coefficients of f and g.)

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. (Key k is weak if $X = 1$).

Note that the above algorithm can be executed in polynomial time (in m) as already shown in the proof of the above theorem.

3.5 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 one user. In fact we call 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 $W_1(a,l) \cup W_2(a,l)$ 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 $\mathbb{Z}_n$. Although $C(n)$ itself is not large for primitive elements, if the generator chosen has a prime order n such that p is a primitive element of $\mathbb{Z}_n^*$ then all the keys are weak. Hence such generators must be avoided at all costs as fatally weak parameters. 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.

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% appears to be practically noteworthy while the number L denotes the percentage of weak cases for choice of the second private key.

Example 4. Weak keys in the field $\mathbb{F}_{p^m}$ for $p = 2$, $m = 7$. Generator polynomial $h(x) = x^7 + x + 1$. $\operatorname{ord} a = 127$. $L = 17/119$. See figure 1.

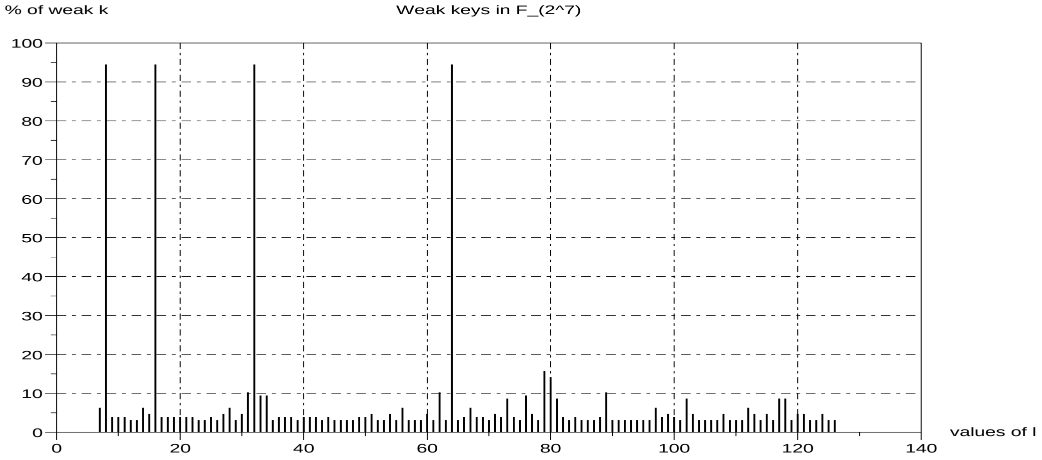

Figure 1: Weak keys for the field $\mathbb{F}_{2^7}$

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

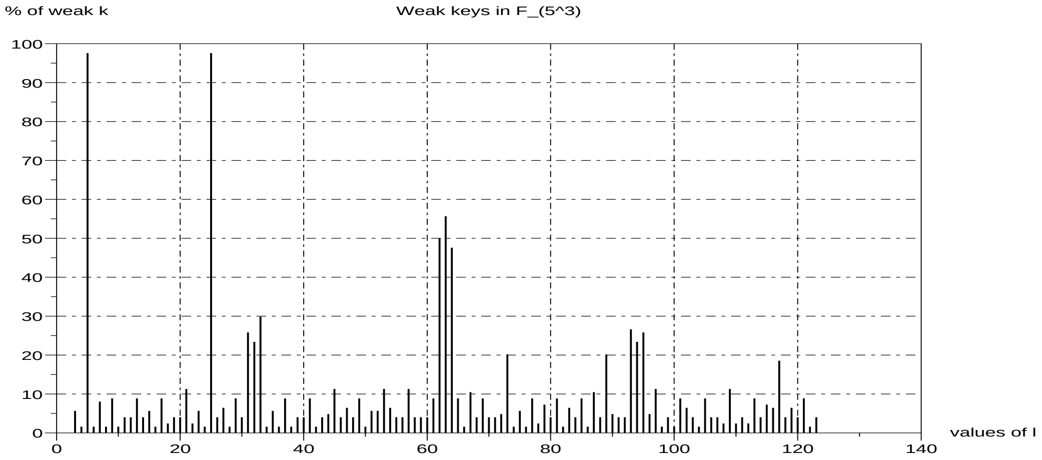

Figure 2: Weak keys for the field $\mathbb{F}_{5^3}$

Example 6. Weak keys in the field $\mathbb{F}_{p^m}$ for $p = 11$, $m = 2$. Generator polynomial $h(x) = x^2 + 4x + 7$. $\operatorname{ord} a = 120$. $L = 31/117$. See figure 3. This plot also shows higher average of weak keys.

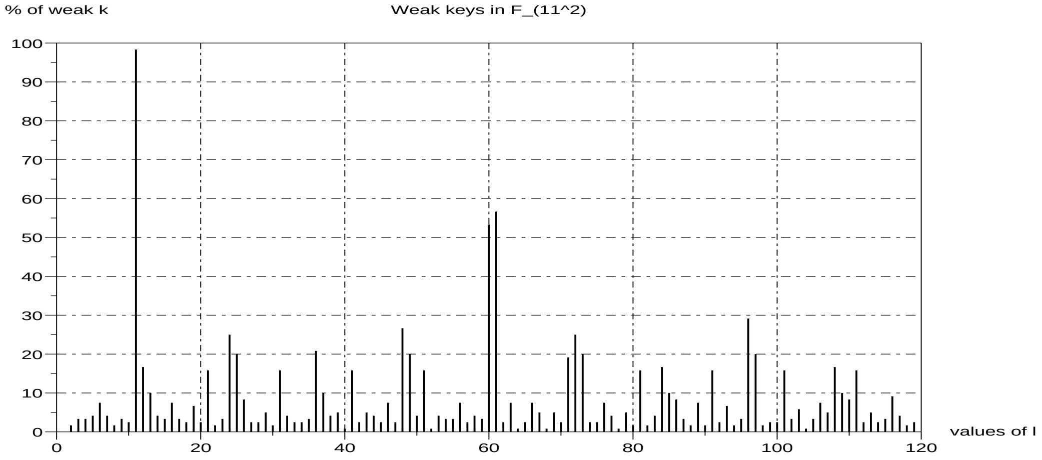

Figure 3: Weak keys for the field $\mathbb{F}_{11^2}$

Example 7. Weak keys in the field $\mathbb{F}_{p^m}$ for $p = 13$, $m = 2$. Generator polynomial $h(x) = x^2 + x + 2$. $\operatorname{ord} a = 168$. $L = 34/165$. See figure 4.

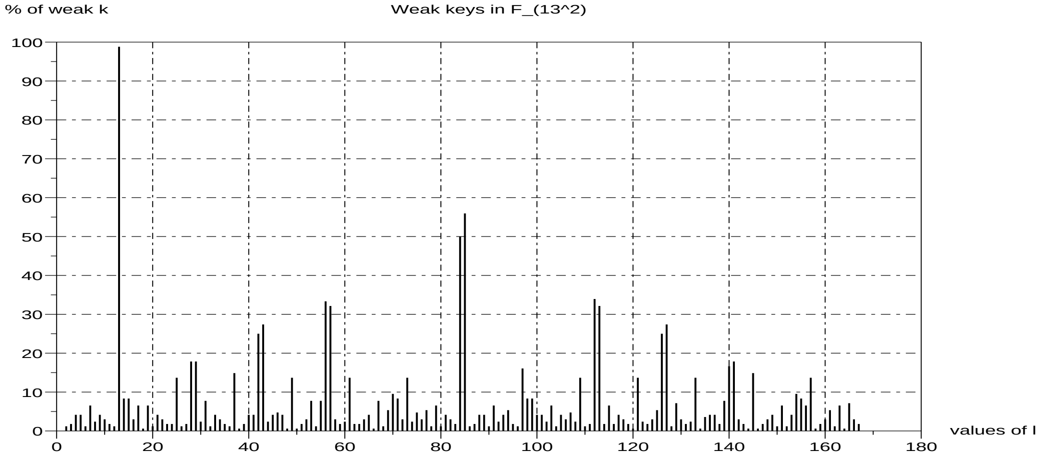

Figure 4: Weak keys for the field $\mathbb{F}_{13^2}$

Example 8. 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.

4 DHP over elliptic curves

In this section we consider the DHP defined over an elliptic curve E over a finite field $\mathbb{F}_p$ for some prime p. Use of elliptic curves for DH scheme was proposed in [10, 11] and has since then become among the most important of algorithms. The reader is referred to [14, 15] for modern developments of cryptography based on elliptic curves. Of principal interest in this paper is the well known reduction of [5] known as the MOV attack based on the Weil pairing which provides an isomorphism of a cyclic subgroup $< P >$ in E of order n with that of the group μ_n of n^{th} roots of unity in an extension field of $\mathbb{F}_p$. The notations of this construction are quite well known and may be referred from the above references.

Let $e : E[n] \times E[n] \to \bar{K}$ denote the Weil paring on the group $E[n]$ of n-torsion points of $E(\bar{K})$ where $\bar{K}$ is the algebraic closure of $\mathbb{F}_p$. For the point P of order n (relatively prime to p) there exists a point $\tilde{Q}$ in $E[n]$ such that $\alpha = e(P, \tilde{Q})$ is an element of $\mathbb{F}_{p^m}$ for some m. A smallest of such integers m is chosen. Then $e([k]P, \tilde{Q}) = \alpha^k$ gives the isomorphism of the two groups $< P >$ and μ_n.

4.1 Associated DHP in the extension field and weak keys

Consider the DH scheme with session triple (P, k, l), k, l in $\mathbb{Z}_n$ and public data (P, Q, R) where $Q = [k]P$ and $R = [l]P$. There is thus an associated DHP over $\mathbb{F}_{p^m}$ with session

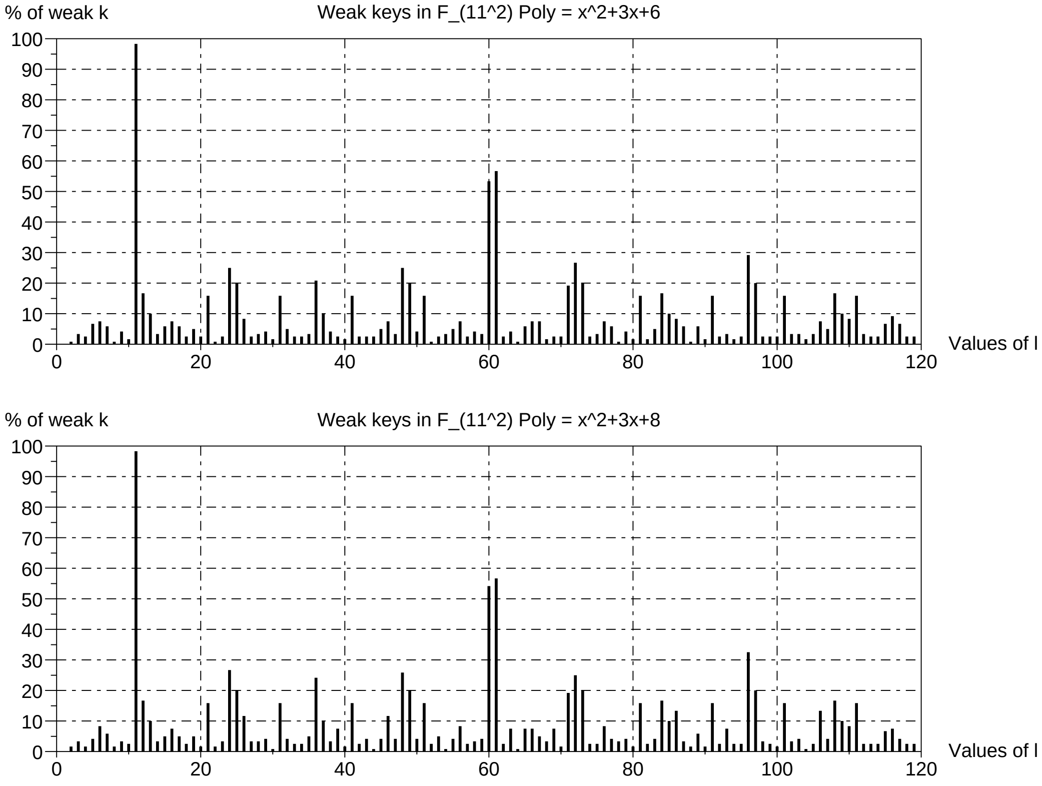

Figure 5: Weak keys for the field $\mathbb{F}_{11^2}$ with different polynomials

triple (α, k, l) and public data (α, β, γ) where $\beta = \alpha^k$ and $\gamma = \alpha^l$. Let S be the shared key of the DH session in E. Then from the properties of the Weil pairing it follows that $\psi \overset{\text{def}}{=} e(S, \tilde{Q}) = \alpha^{kl}$ is the shared key of the DH session in $\mathbb{F}_{p^m}$. We call ψ the *image* in $\mathbb{F}_{p^m}$ of the shared key S of the DH session over E. Conversely if ψ is the shared key of the DH session in $\mathbb{F}_{p^m}$ with (α, k, l) as the session triple then due to the above isomorphism there exists a unique point S in E which is the shared key of the DH session over E such that $\psi = e(S, \tilde{Q})$. Let T be any point in $< P >$ and $\theta = e(T, \tilde{Q})$. We call the minimal polynomial $h(\theta, x)$ of θ over $\mathbb{F}_p[x]$ as the *minimal polynomial of* T *over* $\mathbb{F}_p$ and denote this as $h(T, x)$. Let $h_q(x) = \operatorname{lcm}(h(P, x), h(Q, x))$ while $h_r(x) = \operatorname{lcm}(h(P, x), h(R, x))$. Define the analogous modulus conditions relative to the public data (P, Q, R) as follows.

Definition 6 (Modulus conditions). The triple (P, k, l) is said to satisfy the modulus condition C1 if

$$x^k \bmod h(P, x) = x^k \bmod h_r(x) \tag{11}$$

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

$$x^l \bmod h(P, x) = x^l \bmod h_q(x) \tag{12}$$

Also define the analogous conjugate class of session triples as

Definition 7 (Conjugate class). The triple (P, k, l) is said to belong to the conjugate class relative to k (respectively l) if $h(P, x) = h(Q, x)$ (respectively if $h(a, x) = h(R, x)$).

Lemma 1. A session triple (P, k, l) satisfies modulus condition C1 (respectively C2) iff the triple (α, k, l) satisfies modulus condition C1 (respectively C2). The triple (P, k, l) is in the conjugate class relative to k (respectively l) iff (α, k, l) is in the conjugate class relative to k (respectively l).

The proof is obvious from the above definitions. From the case of DHP over finite fields developed in the last section it now follows that the image ψ of the shared key S of the DHP on E can be solved in $\mathbb{F}_p$ operations which grow at most as a polynomial in d the degree of the minimal polynomial of P. We state this as the next theorem.

Theorem 9. Let the session triple (P, k, l) satisfy modulus condition C1 or C2 and $k, l \geq d$. Let S be the shared key of the DH session. Given the data (α, β, γ) of the associated DHP in $\mathbb{F}_{p^m}$, the image of the shared key $\psi = e(S, \tilde{Q})$ can be computed in number of operations in $\mathbb{F}_p$ which grow at most as a polynomial in d. There exist unique polynomials f, g in $\mathbb{F}_p$ of degrees at most $d - 1$ such that ψ equals one of $\psi_1 = f(e(R, \tilde{Q}))$ or $\psi_2 = g(e(Q, \tilde{Q}))$. The computation of f, g moreover does not yield k or l.

Proof. From the lemma above the triple (α, k, l) satisfies modulus condition C1 or C2 respectively where $\alpha = e(P, \tilde{Q})$ and has minimal polynomial of degree d in $\mathbb{F}_p[x]$. Hence from theorems 5, 6 there exist unique polynomials f, g for the DHP with public data (α, β, γ) which express the shared key ψ as either $\psi_1 = f(\gamma)$ or $\psi_2 = g(\beta)$. From theorem 8 it follows that computation of f or g can be accomplished in number of $\mathbb{F}_p$ operations which grow at most as a polynomial in d. Finally from the properties of the Weil pairing we have $\psi_1 = f(e(R, \tilde{Q})$, $\psi_2 = g(e(Q, \tilde{Q})$ and $\psi = e(S, \tilde{Q})$ where S is the shared key of the DH session on E with public data (P, Q, R). Also from theorem 8 it follows that this computation does not yield k or l. □

Above theorem shows that for session triples (P, k, l) satisfying either of the modulus conditions, the DHP can in principle be solved without solving the DLP on E. While this fact makes such session triples exceptions to be excluded from the DH conjecture from a theoretical standpoint, it by itself is not cryptographically significant unless the rest of the computations involved in computing the Weil pairings and inverse mapping from ψ to S also depend polynomially on the data. In the next section we discuss a possibility in which the image ψ of the shared key can be computed in polynomial time.

4.2 Application to pairing based key exchange

In this section we highlight key exchange schemes for which the above theorem is of cryptographic significance. These schemes are defined over elliptic curves which are supersingular on which the computation of pairings such as $e(Q, \tilde{Q})$ can be carried out in polynomial time in the embedding degree m. Hence the computation of the pairing can be achieved inexpensively. However the prime p is large enough so that the DLP in $\mathbb{F}_{p^m}$ is intractable being of sub exponential order. Pairing based schemes proposed by [16] and [18] on supersingular elliptic curves involve $m \leq 6$ and are important for triparty and identity based key exchange.

The importance of the above theorem for the paring based schemes referred above is as follows. In these schemes the shared key actually utilized for various cryptographic tasks is the shared key ψ of the DHP in $\mathbb{F}_{p^m}$. This key is the image of S, the shared key of the DHP with session triple (P, k, l) on E and is computed from the pairing as $\psi = e(S, \tilde{Q})$. Thus whenever E is supersingular, the computation of the public data of the DHP in $\mathbb{F}_{p^m}$ is possible in polynomial time. Above theorem shows that when (P, k, l) satisfies one of the modulus conditions, ψ can be computed as a solution of the DHP in $\mathbb{F}_{p^m}$ with public data (α, β, γ) in $\mathbb{F}_p$ operations depending polynomially on d. The degree d of the minimal polynomial of P (same as that of α) is itself computable in at most polynomial number of operations in m. Hence for the pairing based schemes on supersingular curves the DHP can be solved in $\mathbb{F}_p$ operations which grow at most as a polynomial in m when the session triple (P, k, l) satisfies one of the modulus conditions.

4.3 Weak parameters of pairing based schemes

We shall formally call a DH scheme on an elliptic curve E to be paring based if there is a paring $\omega : E[n] \times E[n] \to \mathbb{F}_{p^m}$ and that the shared key used for encryption is a result of a DH scheme on $\mathbb{F}_{p^m}$. Multiparty DH scheme and the identity based scheme on elliptic curves referred above are examples of such schemes. As discussed above, when m is sufficiently small the polynomial time computation of the shared key ψ in $\mathbb{F}_{p^m}$ should turn out to be a powerful attack whenever the session triples satisfy modulus conditions. For instance when $m = 6$ the solution of the DHP in these special cases requires computation in $\mathbb{F}_p$ of at most a fixed order however nothing can be said about the DLP for these special cases. We shall leave this as an open question to be investigated in future. Similar conclusions can be drawn with respect to other well known pairing based problems such as the Bilinear DHP and the Decisional DHP. Detailed study of DHPs of these types is beyond the scope of this paper and shall be pursued in a separate article.

While the actual bounds on computation can be worked out for specific curves we mention that it would be important to avoid the following list of weak parameters on supersingular E over $\mathbb{F}_p$ for which the DHP can be solved in polynomial time in the embedding degree m.

1. Points P of order n such that $< p >= \mathbb{Z}_n^*$.
2. Given l, private keys k which belong to $W_1(\alpha, l) \cup W_2(\alpha, l)$. Similarly for l when k is given.
3. If l is the private key of the session chosen first, then those l for which number of weak k is larger than a certain fraction of $n - 2$ since $1 < l \leq (n - 1)$.

Thus the nature of weak keys k, l in the case of DH schemes on supersingular curves is the same as that in the field case $\mathbb{F}_{p^m}$ for an appropriate generator. Hence the existence of such weak keys follows from the existence of such keys in the field case treated above. The first item in the above list identifies generators for which α are not primitive elements of $\mathbb{F}_{p^m}$ but for which all numbers in $\mathbb{Z}_n$ are conjugate class keys. Such generators are fatally weak. This shows that increasing the order of P by itself does not make the session secure in pairing based schemes. Computational algorithms for identifying weak parameters over supersingular curves of realistic orders shall be necessary for future implementations of these schemes. These developments shall be reported separately.

5 Conclusions

Special cases of session triples of the DH scheme exist for which the DHP can be solved in polynomial time without solving the DLP. Hence such special cases must be excluded from use in the DH scheme. The method of analysis first identifies these special cases in the matrix group and then develops special cases by analogy over finite fields $\mathbb{F}_{p^m}$ as well as supersingular elliptic curves for pairing based schemes. These schemes on supersingular elliptic curves are of significance for identity based and triparty key exchange schemes. The analysis and examples over fields show that the number of weak keys is not insignificant to be ignored. A simple computational algorithm is proposed to determine the weak triples. Their characterization as well as algorithms for avoiding them in practical implementations is desirable. Orders of generators of DH sessions are also identified for which all private keys are weak making such sessions fatally weak. Such generators must therefore be strictly avoided. Avoiding these weak keys in practice should be 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.

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. Lidl, H. Niederreiter, ”Finite Fields”, Ency. of Math. and Its Appln. Cambridge University Press, 1997.

[18] 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.