

Weak keys of the Diffie Hellman key exchange II: Pairing based schemes on on elliptic curves

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

October 10, 2005

Abstract

This paper develops a cryptanalysis of the pairing based Diffie Hellman (DH) key exchange schemes which have found important applications as in the tripartite exchange scheme proposed in [1]. The analysis of *weak keys* of the standard DH scheme proposed in [2] is applied to show existence of weak sessions for tripartite schemes over super-singular curves. It is shown that for such sessions the associated Bilinear Diffie Hellman Problem (BDHP) is solvable in polynomial time, without computing the private keys i.e. without solving the discrete logarithms. Similar applications of the analysis to Decisional Diffie Hellman Problem (DDHP) and the Identity Based DH scheme (IBS) are also developed. The tripartite key exchange scheme is analyzed in detail and it is shown that the number of weak keys increases in this scheme as compared to the standard two party DH scheme. It is shown that the random choice of private keys by the users independent of each other's knowledge is insecure in these schemes. Algorithms are suggested for checking weakness of private keys based on an order of selection. A modified tripartite key exchange scheme is presented in which detection of weak keys is incorporated.

1 Introduction

This paper develops an analysis of the pairing based Diffie Hellman (DH) key exchange schemes on elliptic curves and shows existence of parameters of these schemes for which the shared key can be computed in polynomial time without solving the associated discrete logarithms. Hence private keys involved in such parameters are called weak keys of the scheme.

In this second part of a series of two part papers we presents developments arising from results of the first part [2]. The first part presents certain weak keys of the two party DH scheme over the groups $\mathbb{F}_{p^m}^*$ and GL_n over finite fields while this part is devoted to the development of analogous weak parameters of pairing based DH schemes over elliptic curves. These special parameters determine some of the weak keys of the tripartite key agreement scheme proposed in [1].

1.1 Pairing based DH schemes

Let P be a generator of a cyclic subgroup of G of order n . If A, B are users with *private keys* k, l in \mathbb{Z}_n , then a session in a two party DH key exchange scheme is said to have the *session triple* (P, k, l) with *public data* $(P, Q, R) = (P, P^k, P^l)$. The *shared key* of the session is $S = P^{kl}$. The problem of computing S in terms of the public data is the well known DH Problem (DHP). Now if $e : G \times G \rightarrow K$ is a pairing¹ with values in a finite field K , then for a fixed T in G such that $\omega = e(P, T)$ is not the identity of K , the above setup results in a DH key exchange scheme over K with session triple (ω, k, l) , public data $(\omega, \kappa, \lambda) = (\omega, \omega^k, \omega^l)$ and shared key $s = \omega^{kl} = e(S, T)$.

The DH scheme above on G is said to be a *paring based* scheme based on pairing e if the shared key computed by the users is s in K . In a pairing based scheme it is s that gets utilized for encryption purpose instead of S as in the standard DH scheme. Pairing based DH schemes arise from the Bilinear DH Problem (BDHP) in the tripartite single pass scheme referred above [1], the Identity based DH scheme [12] and the Decision DH Problem (DDHP) on groups where a paring is available.

The above extensions of the DH scheme are practically feasible when the paring $e(A, B)$ itself can be computed for elements A, B of G without much overhead. Such is the case for instance over super-singular and certain special elliptic curves [17]. Further, these schemes are secure from the well known MOV attack [5] when the algorithms for solving discrete logarithm problem (DLP) over K have sufficiently high time complexity such as when the characteristic of K is sufficiently large.

1.2 Weak keys of the DHP over fields

In [2] a class of weak keys of the DHP over groups $\mathbb{F}_{p^m}^*$ and GL_n are proposed. These comprise of session triples (a, k, l) for say a in $\mathbb{F}_{p^m}^*$ for which the DHP can be solved in polynomial time in m from the public data in \mathbb{F}_p operations without solving the DLP. In this paper we shall show how this analysis can be extended to prove existence of session triples (P, k, l) of the DHP arising in paring based DH schemes on super-singular elliptic curves for which the shared key s can be computed in polynomial time from the data $(\omega, \kappa, \lambda)$ without solving the associated DLP. Further, this paper shall also develop the above class of weak keys for the specialized situations of paring based DHPs such as the BDHP and the DDHP. This leads to determining some of the weak keys of the tripartite DH scheme, the Identity based DH scheme and that of the DDHP. We provide several examples of weak keys of the tripartite key exchange scheme for illustration.

2 Tripartite Diffie Hellman scheme and the bilinear DHP

Consider three users A, B, C who can choose integers a, b, c randomly in \mathbb{Z}_n as private keys. The single pass tripartite key exchange problem is concerned with creating a unique common shared key between the users which they can compute once all of them generate their individual public keys using a publicly known algorithm. The single pass term refers

¹A pairing is a bilinear non-degenerate map i.e. satisfies $e(a^n, b) = e(a, b)^n$, $e(a, b^n) = e(a, b)^n$ for a, b in G and n in \mathbb{Z} and $e(a, x) = 1$ for all x in G implies a is identity in G .

to the fact that no second stage computation requiring declared public keys of the users is necessary for computing the shared key.

In [1] such a scheme is proposed over an elliptic curve E defined over \mathbb{F}_p with the help of the Tate paring on this curve. Let $E[n]$ denote the set of n -torsion points of $E(K)$ over K the algebraic closure of \mathbb{F}_p where p is coprime to n . Let $e : E[n] \times E[n] \rightarrow K$ denote a paring on $E(K)$. Let P and Q be independent points in $E[n]$ where P has order n . Now each of the users A , B and C choose private keys a , b , c which are random integers modulo n and declare their public keys as pairs of points² $(AP, AQ) \stackrel{\text{def}}{=} (aP, aQ)$, $(BP, BQ) \stackrel{\text{def}}{=} (bP, bQ)$ and $(CP, CQ) \stackrel{\text{def}}{=} (cP, cQ)$ respectively on E . Then A , B and C can compute $e(aBP, CQ)$, $e(bCP, AQ)$ and $e(cAP, BQ)$ respectively all of which equal to $e(P, Q)^{abc}$ which is the shared key between them. Clearly, such a scheme is practically feasible only when the parings can be computed inexpensively. Hence such paring based schemes are feasible mainly on super-singular curves where the parings $e(P, Q)$ can be computed in polynomial time complexity in $\log p$. Here Q is chosen such that $e(P, Q)$ is not identity. An element Q in $E[n]$ independent of P serves this purpose when $e(\cdot, \cdot)$ is the Tate pairing. Consider now the Bilinear DHP (BDHP) associated with this scheme.

Definition 1 (Bilinear Diffie Hellman Problem). Let the pairing $e : E[n] \times E[n] \rightarrow K$ on E and P, Q be as above where E is super-singular. Given pairs of points $(AP, AQ) = (aP, aQ)$, $(BP, BQ) = (bP, bQ)$, $(CP, CQ) = (cP, cQ)$ on E determine the shared key $s = e(P, Q)^{abc}$. We call the pair (P, Q) along with the above pairs of points as the *public data* of the BDHP.

2.1 Weak keys of the BDHP

Since an adversary can compute $\omega = e(P, Q)$, $e(AP, Q) = \omega^a$, $e(BP, Q) = \omega^b$, $e(CP, Q) = \omega^c$, security of the above scheme presupposes practical infeasibility of computing the DLP in the field \mathbb{F}_{p^m} where ω belongs. For instance this can be achieved by starting with an elliptic curve E defined over \mathbb{F}_p for large enough prime p . It is well known that the best algorithms for solving the DLP in such fields are of subexponential time complexity in p . However we show that, even if the DLP is hard in \mathbb{F}_{p^m} , there exist special classes of pairs (P, Q) together with choices of private keys a, b, c for which the BDHP can be solved in polynomial time in m without explicitly solving the DLPs. Hence for given pairs of points (P, Q) on a super-singular elliptic curve E , private keys of such class can be considered as weak keys of the BDHP. Investigation of such weak keys is the primary aim of this paper.

2.2 Solving the BDHP using solutions of the DHP

In [2] authors have determined certain weak keys of the two party DH scheme over finite fields. It turns out that the BDHP associated with the tripartite scheme explained above incorporates three DHPs over the field whose shared keys are equal to the shared key of the tripartite scheme. Hence the set of weak keys of the BDHP includes the weak keys of the three DHPs and possibly more. We now discuss these problems. Let the BDHP be given as above and compute $\omega^{ab} = e(AP, BQ)$, $\omega^{bc} = e(BP, CQ)$, $\omega^{ca} = e(CP, AQ)$ all from the public key pairs of the three parties. The shared key is $s = \omega^{abc}$. Consider the three DHPs in which ω^a , ω^b and ω^c are computed from the public keys as shown above.

²Notation: aP equals a times sum of P in E for a in \mathbb{Z}_n and P in E .

Problem 1. Given $\omega, \omega^a, \omega^{bc}$ in \mathbb{F}_{p^m} compute s .

Problem 2. Given $\omega, \omega^b, \omega^{ca}$ in \mathbb{F}_{p^m} compute s .

Problem 3. Given $\omega, \omega^c, \omega^{ab}$ in \mathbb{F}_{p^m} compute s .

It is apparent from these problems that if a class of weak session triples of the standard DHP (between two users) is known then this would give rise to a class of weak keys of the tripartite scheme. One such class is proposed in [2]. For this class of session triples of a DHP over $\mathbb{F}_{p^m}^*$ the shared can be computed in polynomial time in m without solving the DLP. We shall thus develop a class of weak keys for the tripartite scheme above by utilizing this class of weak triples of the DHP.

3 Weak keys of the DHP in the field case

In this section we briefly recall some of the results of [2] giving weak keys of the DHP over finite fields and also introduce notation which is at variance with that of [2] in certain symbols. Consider a finite field $K = \mathbb{F}_{p^m}$ where p is prime denoting the field characteristic. Let ω be an element of K^* of order n . A *session triple* of a DHP over K is the triple (ω, k, l) where k, l in \mathbb{Z}_n are *private keys* of the session. The triple $(\omega, \kappa, \lambda) = (\omega, \omega^k, \omega^l)$ is called the *public data* of the session. The element $s = \omega^{kl}$ in K is called the *shared key*. The DHP is to compute s given the public data. The method initiated in [2] for seeking solutions of the DHP makes use of the structure of algebra of K . For an element ω in \mathbb{F}_{p^m} let $h(\omega, x)$ denote the minimal polynomial of ω in $\mathbb{F}_p[x]$. Denote

$$h_r(x) = \text{lcm}(h(\omega, x), h(\omega^r, x))$$

The following subsets of \mathbb{Z}_n are important for further development.

Definition 2. Let ω in \mathbb{F}_{p^m} be fixed and has order n . Define

1. The Conjugate class

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

($C(n) = \langle p \rangle$ the multiplicative monoid of \mathbb{Z}_n^* generated by p).

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

$$W_1(\omega, l) = \{k \in \mathbb{Z}_n \mid x^k \text{ mod } h(\omega, x) = x^l \text{ mod } h_k(x)\}$$

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

$$W_2(\omega, l) = \{k \in \mathbb{Z}_n \mid x^l \text{ mod } h(\omega, x) = x^k \text{ mod } h_l(x)\}$$

Following results proved in [2] go to show that the above sets are weak keys of the DH scheme since the shared key for the session triple (ω, k, l) can be computed in polynomial time from the public data $(\omega, \kappa, \lambda)$ whenever either k or l belong to the above sets. Denote $W(\omega, r) = W_1(\omega, r) \cup W_2(\omega, r)$.

Theorem 1. The following statements hold

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

$$\begin{aligned}\kappa &= f(\omega) \\ s &= f(\lambda)\end{aligned}\tag{1}$$

iff k belongs to $W_1(\omega, l)$.

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) $\deg g < \deg h(\omega, x)$
 - (b) The following equations hold

$$\begin{aligned}\lambda &= g(\omega) \\ s &= g(\kappa)\end{aligned}\tag{2}$$

iff k belongs to $W_2(\omega, l)$.

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

Theorem 2. The following statements hold

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

$$\begin{aligned}\lambda &= f(\omega) \\ s &= f(\kappa)\end{aligned}\tag{3}$$

iff l belongs to $W_1(\omega, k)$.

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) $\deg g < \deg h(\omega, x)$
 - (b) The following equations hold

$$\begin{aligned}\kappa &= g(\omega) \\ s &= g(\lambda)\end{aligned}\tag{4}$$

iff l belongs to $W_2(\omega, k)$.

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

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

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

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

Remark 1. Theorem 3 and the corollaries following establish existence of the sets $W_1(\omega, \cdot)$ and $W_2(\omega, \cdot)$. Next theorem shall show that these are weak keys of the DHP. The last corollary in particular shows that generators ω of order n for which the field characteristic p is primitive in \mathbb{Z}_n should never be used in DH key exchange.

Theorem 4. Consider a session triple (ω, k, l) (with ω in \mathbb{F}_{p^m} such that $\deg h(\omega, x) = m$) in which either k belongs to $W(\omega, l)$ or l belongs to $W(\omega, k)$. 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 .

Definition 3 (Weak Keys of the DHP). A private key k or l of a session (ω, k, l) of a DHP is said to be a *weak key* if the DHP for this session can be solved in polynomial time proportional to the length of the public data $(\omega, \kappa, \lambda)$ of the session. In such cases the session triple itself shall be called as a *weak session triple*.

Remark 2. From the above results it follows that session triples (ω, k, l) with k (respectively l) belonging to $W(\omega, l)$ (respectively $W(\omega, k)$) are weak. The set $C(n)$ is moreover fatally weak since whenever l is in $C(n)$ all k in \mathbb{Z}_n are weak. The weak session triples are exceptions to the well known DH assumption according to which solution of the DLP is the only way to solve the DHP. These aspects are discussed in detail in [2].

All of the above results are valid for the case when ω belongs to \mathbb{F}_{q^m} where q is not prime. However then q must be of the form p^t for some t . In this case statements of above results can still be proved by replacing p with q . In [2] the resulting effect of change in the polynomial ring from $\mathbb{F}_p[x]$ to $\mathbb{F}_q[x]$ is discussed. We shall skip this discussion.

3.1 Algorithm for computing the shared key

The problem of algorithmic computation of the shared key s for a session triple (ω, k, l) is now considered, when one of the numbers k, l falls in the class of weak keys $W_1(\omega, \cdot) \cup W_2(\omega, \cdot)$ discovered from the results of the previous section. Following algorithm returns the shared key s when one of the private keys is weak.

Assume that the degree of minimal polynomial $h(\omega, x)$ of ω over \mathbb{F}_{p^m} is already computed and without loss of generality let this be equal to m . This is a one time computation once the generator ω is fixed and is not required to be repeated for new choices of private keys. In any case this computation involves at most polynomial in m computations. The following algorithm is reproduced from [2].

Algorithm 1. Input public data $(\omega, \kappa, \lambda)$.

1. Compute the polynomials f, g in $\mathbb{F}_p[x]$ (which exist uniquely with degrees at most $m - 1$) satisfying

$$\begin{aligned}\kappa &= f(\omega) \\ \lambda &= g(\omega)\end{aligned}$$

2. Compute $s_1 = f(\lambda), s_2 = g(\kappa)$.
3. Output shared key
 - $s = s_1$ if $k \in W_1(\omega, l)$ or $l \in W_2(\omega, k)$
 - $s = s_2$ if $k \in W_2(\omega, l)$ or $l \in W_1(\omega, k)$

Note that the solutions f, g always exist for arbitrary public data $(\omega, \kappa, \lambda)$ of a DH session [2]. However s_1 or s_2 will return the actual shared key only when k or l belong to the class of weak keys. Further, the solution of polynomials f and g can be obtained by solving linear systems both of size m over \mathbb{F}_p . Theorem 4 concludes the fact that this computation along with computation of the co-efficients of these systems can be carried out in time polynomial in m . Thus the algorithm above involves only polynomial time computation. The problem of verifying whether the private keys k or l chosen last in a session make the session triple weak or not is solved by the algorithm 3 given in section 6.

4 DHP over elliptic curves

The purpose of this section is to develop an extension of the weak keys of the DHP (over $\mathbb{F}_{p^m}^*$) discussed above (and developed in [2]) over elliptic curves. This is an independent development of importance in its own right. As explained above the existence of weak keys of the BDHP and their relevance to tripartite and identity based schemes follows directly from the case of the standard DH scheme over the field case. However the notion of minimal polynomial of the generator and its role in the solution of the DHP can be extended over elliptic curves due to the existence of pairings on elliptic curves. It is for this reason that a this special section is warranted.

Consider the DHP defined over an elliptic curve E over a finite field \mathbb{F}_p for some prime p . Of principal interest in this section 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 $\langle P \rangle$ 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 reference.

Let $e : E[n] \times E[n] \rightarrow \bar{K}$ denote the Weil pairing 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 $\langle P \rangle$ 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

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 $\psi \stackrel{\text{def}}{=} e(S, \tilde{Q}) = \alpha^{kl}$ 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 $\langle P \rangle$ 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 $h_q(x) = \text{lcm}(h(P, x), h(Q, x))$ while $h_r(x) = \text{lcm}(h(P, x), h(R, x))$. Define the analogous modulus conditions relative to the public data (P, Q, R) as follows.

Definition 4 (Modulus conditions). The triple (P, k, l) is said to satisfy the modulus condition C1 if

$$x^k \bmod h(P, x) = x^k \bmod h_r(x) \quad (5)$$

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

$$x^l \bmod h(P, x) = x^l \bmod h_q(x) \quad (6)$$

Also define the analogous conjugate class of session triples as

Definition 5 (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 5. 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 1, 2 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 4 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 4 it follows that this computation does not yield k or l . \square

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 super-singular 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 [1] and [12] on super-singular elliptic curves involve $m \leq 6$ and are important for tripartite and identity based key exchange.

The importance of the above theorem for the pairing 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 super-singular, 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 super-singular 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 pairing based if there is a pairing $\omega : E[n] \times E[n] \rightarrow \mathbb{F}_{p^m}$ 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 super-singular 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 $\langle p \rangle = \mathbb{Z}_n^*$.
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 super-singular 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 super-singular curves of realistic orders shall be necessary for future implementations of these schemes. These developments shall be reported separately.

5 Weak keys of the tripartite scheme

The problem of determining weak keys of the BDHP is now considered using the weak keys $W(\omega, r) \stackrel{\text{def}}{=} W_1(\omega, r) \cup W_2(\omega, r)$ of weak keys of a DHP over $\mathbb{F}_{p^m}^*$. These are expressed in following corollaries of the above theorems and are directly related to the three DHPs associated with the BDHP discussed previously. We shall call private keys of a BDHP as *weak* if the BDHP can be solved in polynomial time in the public data.

Corollary 3. Following statements hold

1. If b, c are private keys of users B, C of the BDHP then all integers a in $W_1(\omega, bc) \cup W_2(\omega, bc)$ are weak keys for user A .
2. If c, a are private keys of users C, A of the BDHP then all integers b in $W_1(\omega, ca) \cup W_2(\omega, ca)$ are weak keys for user B .
3. If a, b are private keys of users A, B of the BDHP then all integers c in $W_1(\omega, ab) \cup W_2(\omega, ab)$ are weak keys for user C .

Proof. Only the first item is proved since the other items are similar. The problem 1 is a DHP with the session triple (ω, a, bc) . Hence from theorem 4 it follows that numbers a in $W_1(\omega, bc) \cup W_2(\omega, bc)$ are weak keys of user A . Hence the BDHP can also be solved from the public data in polynomial time. \square

The problem of deciding whether user A has weak key using public keys of users B , C can be answered quite easily from the definitions of the sets W_1 and W_2 as well as characterization of the conjugate class $C(n)$. We discuss such algorithms in a later section. Next corollary shows that choice of a private key by one user can cause weak keys in combination of the keys of the other two users.

Corollary 4. Following statements hold

1. If a is the private key of user A , then all keys b, c of users B, C respectively such that $bc \in W_1(\omega, a) \cup W_2(\omega, a)$ are weak keys of the tripartite scheme.
2. If b is the private key of user B , then all keys c, a of users C, A respectively such that $ca \in W_1(\omega, b) \cup W_2(\omega, b)$ are weak keys of the tripartite scheme.
3. If c is the private key of user C , then all keys a, b of users A, B respectively such that $ab \in W_1(\omega, c) \cup W_2(\omega, c)$ are weak keys of the tripartite scheme.

Proof. Consider the first item. The triple (ω, a, bc) is a session triple for the problem 1. Hence it follows from theorem 1, 2 that the condition claimed on b, c results in bc as a weak key of this problem. Other items can be proved similarly. \square

Corollary 5. Following statements hold

1. If a belongs to $C(n)$ then $W_1(\omega, a) = \mathbb{Z}_n$ hence all keys b, c are weak.
2. If b belongs to $C(n)$ then $W_1(\omega, b) = \mathbb{Z}_n$ hence all keys c, a are weak.
3. If c belongs to $C(n)$ then $W_1(\omega, c) = \mathbb{Z}_n$ hence all keys a, b are weak.

Proof. Follows from theorem 3 and the formulations of Problem 1, 2 and 3 respectively. \square

We can similarly have the following corollary when private keys of two users in combination belong to the conjugate class.

Corollary 6. Following statements hold

1. If bc belongs to $C(n)$ then $W_1(\omega, bc) = \mathbb{Z}_n$ hence all keys a of the users A are weak.
2. If ca belongs to $C(n)$ then $W_1(\omega, ca) = \mathbb{Z}_n$ hence all keys b of the user B are weak.
3. If ab belongs to $C(n)$ then $W_1(\omega, ab) = \mathbb{Z}_n$ hence all keys c of the user C are weak.

Proof. Follows from the definitions of the three DHPs Problems 1,2,3 and above discussion. \square

Above corollary shows that if product of any two private keys belong to $C(n)$ then the combination is fatally weak since the third party has no choice of a key by which the corresponding session triple is not weak. However there is the larger class of pairs of private keys (say a, b) whose product lies in the union $W_1(\omega, c) \cup W_2(\omega, c)$ which make the session triples (ω, c, ab) weak and subsequently the session³ of the tripartite DH scheme weak. This class is described by the following

³We call (ω, a, b, c) the session of the tripartite DH scheme with private keys of the parties as (a, b, c) and call the session *weak* if the BDHP can be solved in polynomial time in the public data

Corollary 7. Let a tripartite DH scheme have the private keys (a, b, c) . Then the session (ω, a, b, c) is weak if any one of the following conditions hold

1. ab belongs to $W_1(\omega, c) \cup W_2(\omega, c)$
2. bc belongs to $W_1(\omega, a) \cup W_2(\omega, a)$
3. ca belongs to $W_1(\omega, b) \cup W_2(\omega, b)$

The proof is omitted since it follows from the themes of the above corollaries and previous results. In a later section we present algorithms which determine whether a session is weak which take into account all the cases of weakness of keys described in the above corollary.

5.1 Computation of the tripartite shared key

Computation of the shared key s in the tripartite case is now considered when the session is weak. Due to the formulation of the three DHPs associated with the BDHP this can be accomplished by repeated application of Algorithm 1. We assume the super-singular elliptic curve E/\mathbb{F}_p be given as above with a pairing e such that $e(P, Q)$ is in \mathbb{F}_{p^m} but is not an identity.

Algorithm 2. This algorithm computes the shared key s of the BDHP when the session triple (ω, a, bc) of an associated two party DHP is weak.

Input public data $(P, Q), (AP, AQ), (BP, BQ), (CP, CQ)$.

1. Compute $\omega = e(P, Q), \kappa = e(AP, Q), \lambda = e(BP, CQ)$.
2. Compute the polynomials f, g in $\mathbb{F}_p[x]$ (which exist uniquely with degrees at most $m - 1$) satisfying

$$\begin{aligned}\kappa &= f(\omega) \\ \lambda &= g(\omega)\end{aligned}$$

3. Compute $s_1 = f(\lambda), s_2 = g(\kappa)$.
4. Output shared key

- $s = s_1$ if $a \in W_1(\omega, bc)$ or $bc \in W_2(\omega, a)$
- $s = s_2$ if $a \in W_2(\omega, bc)$ or $bc \in W_1(\omega, a)$

The above algorithm must be repeated to take into account possibly weak cases with respect to weak sessions (ω, b, ca) and (ω, c, ab) of the other two DHPs associated with the BDHP. The shared key in the tripartite case is thus obtained in three repetitions of Algorithm 1 when the session is weak. Nevertheless since all steps are computed in time polynomial in m , the solution of the BDHP is obtained in polynomial time whenever any of the keys satisfy above conditions of weakness. Here the time required for computation of the pairing is not considered. However it is well known from [5, 8, 11, 9, 10] that computation of pairings can be carried out in polynomial time for super-singular curves for which m above turns out to be at most 6. Hence such curves are suitable for implementation of pairing based schemes. The security of such schemes therefore relies more on the difficulty

of computation of discrete logarithms in the field \mathbb{F}_{p^m} and the DH assumption that the DHP cannot be solved without computing the logarithms. In this paper we have shown weak cases which are exceptions to be excluded from this assumption. From this viewpoint the need for computation of pairings in the direct solution of the DHP as well as BDHP is not an additional hurdle, it is required even for implementation of the scheme. While the direct solution of BDHP in the weak cases is far less expensive than the solution of the DLP.

6 Other applications

The above algorithm can be extended to compute the shared key in case of multiparty key exchange schemes such as that proposed in [13] based on multilinear forms. Another application of the weak keys of the DHP proposed in [2] can be made for solution of the DHP associated with the Identity based DH key exchange scheme [12]. This scheme is another example of a pairing based DH scheme. In this section we shall discuss this scheme and also show an application of the above theory to determining weak keys of the DDHP.

6.1 Identity based DH scheme

This scheme can be conceptually described as follows. For more detailed description we refer the reader to [12, 17]. Let E be a super-singular elliptic curve defined over \mathbb{F}_q of characteristic p and let $e : E[n] \times E[n] \rightarrow \mathbb{F}_q^*$ be a pairing on the n torsion points. In this scheme the private keys are integers a, b modulo a prime n and the publicly known data consists of points $P, aP, P_{\text{Bob}} \stackrel{\text{def}}{=} bP$ and Q_{Bob} in $E[n]$. The shared key is computed as $s = e(Q_{\text{Bob}}, P_{\text{Bob}})^a$. Thus we have a pairing based DHP with session triple (ω, a, b) where $\omega = e(Q_{\text{Bob}}, P)$ and the public data $(\omega, \kappa, \lambda)$ with $\kappa = \omega^a = e(Q_{\text{Bob}}, aP)$, $\lambda = \omega^b = e(Q_{\text{Bob}}, P_{\text{Bob}})$. The shared key is $s = \omega^{ab}$. Clearly sets $W_1(\omega, b)$, $W_2(\omega, b)$ defined for this DHP are the weak keys of the identity based DH scheme.

6.2 The decisional DHP

The Decision Diffie Hellman Problem (DDHP) [17] is defined on an elliptic curve E as follows. Let points P, aP, bP, cP be publicly given on E . Given a point Q in E determine whether $Q = abcP$. (Suppose there is given a public data (P, kP, lP) of a DHP on E and given Q it is required to find out whether $Q = abP$. Then such a problem can be solved with the help of a pairing by computing $s = e(P, Q)$. Then $Q = abP$ iff $s = e(aP, bP)$). Hence the DDHP is nontrivial only due to the three public data points instead of two. We now consider the DDHP after computing the pairings. Define $\omega = e(P, P)$, $\kappa = e(mP, P)$, $\lambda = e(kP, lP)$. (Here $e(\cdot, \cdot)$ is the Tate pairing for which $e(P, P)$ is not the identity). Then we are given the public data of a DHP $(\omega, \omega^m, \omega^{kl}) = (\omega, \kappa, \lambda)$ whose shared key is $s = e(abP, P) = \omega^{klm}$. Hence $Q = abP$ iff $s = e(Q, P)$. Hence whenever the computation of pairing can be done in polynomial time and the session triple (ω, m, kl) of the DHP is weak, the DDHP can be solved in polynomial time. Hence the weak keys of the DDHP can be derived from that of the weak keys of the DHP proposed in [2]. Here there are two other choices of session triples for solving the DDHP in weak cases, these are respectively (ω, k, lm) and (ω, l, km) .

Hence weak keys are obtained in terms of weak keys of three different pairing based DHPs as in the case of the BDHP. Since the sets of weak keys are exactly the same as that in BDHP we shall skip the corresponding corollaries.

7 Existence and examples of weak keys of the tripartite scheme

We now provide examples of weak keys of the tripartite DH scheme to get an empirical estimate of their occurrence. First note that in the standard two party DH scheme on groups $\mathbb{F}_{p^m}^*$ the existence of the set of conjugates $C(n)$ being equal to the multiplicative subgroup $\langle p \rangle$ proves existence of weak keys. In [2] several examples are presented which show the occurrence of weak keys in sets $W_1(\omega, l)$ and $W_2(\omega, l)$ outside the set $C(n)$ of conjugate class. If we consider the DH scheme on elliptic curves E/\mathbb{F}_p with a generator P of order n , then the existence of a pairing on $E[n]$ with values in \mathbb{F}_{p^m} shows that the weak keys of the pairing based DH scheme are precisely that of the weak keys of the associated DH scheme in \mathbb{F}_{p^m} . Hence whenever the embedding degree m is small enough the pairing can be computed inexpensively and then the weak keys of the DH scheme in \mathbb{F}_{p^m} are of practical significance. These facts have been analyzed in [2].

In the case of the BDHP the weak keys are derived from the weak keys of the three associated DHPs discussed above. Hence existence of weak keys of the BDHP follows from the above arguments. In particular it may be noted that in any one of these DHPs say with private keys a and bc the weak keys correspond to the product bc and not the individual keys b, c . Hence there arises a situation in which a random choice of keys b, c even if chosen to avoid the weak class individually, causes the product bc to be weak. This causes a larger number of keys to be weak in the tripartite scheme than the sum of weak keys of the three associated DH problems. The sets of weak keys $W(\omega, l), W(\omega, k)$ of the standard DH scheme proposed in [2] await further characterization. However due to the characterization of the set $C(n)$ of conjugate class it is convenient to determine a lower bound on the number of weak keys of the tripartite scheme. Recall that $C(n)$ is the multiplicative subgroup $\langle p \rangle$ in \mathbb{Z}_n^* since n is prime in the usual DH scheme. The number of conjugate class keys of practical interest in the standard DH scheme is

$$N_2 = |\langle p \rangle|$$

where $m = \deg h(a, x)$. Since the number of possible keys chosen equals $n - m$,⁴ the percentage of weak keys in this scheme is at least as large as

$$w_2 = N_2 \times 100 / (n - m)$$

We also define a related number for tripartite scheme as follows:

Definition 6. Define N_3 to be the number of pairs (b, c) for $m < b, c < n$ such that bc belongs to $C(n)$ among all possible pairs (b, c) with $m < b, c < n$.

Then it is easy to observe

⁴Since $k < \deg h(a, x) = m$ is always weak we can trivially remove these from discussion.

Proposition 1. The percentage of session quadruples (ω, a, b, c) in a tripartite DH scheme for which the keys are weak for one of the three associated DHPs among all possible quadruples with ω of order n is greater than or equal to w_3 where

$$w_3 = N_3 \times 100 / (n - m)^2$$

Proof. Choose a pair of private keys say (b, c) . The session triple (ω, a, bc) for an associated DHP is weak if bc belongs to $C(n)$. There are N_3 such pairs out of the possible pairs $(n - m)^2$ from which the percentage follows. \square

Example 1. Consider the field \mathbb{F}_{p^m} for $p = 2, m = 6$. $\text{ord } a = 62$. $w_2 = 8.06$ while $w_3 = 16.545$.

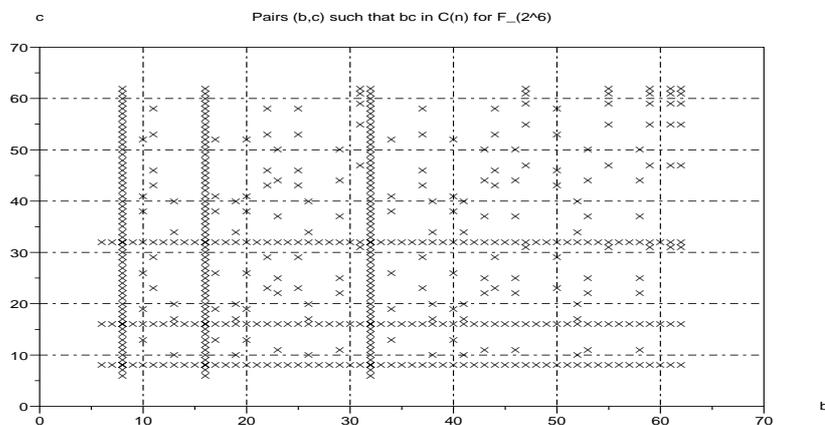


Figure 1: Key pairs (b, c) such that $bc \in C(n)$ for \mathbb{F}_{2^6}

Example 2. Consider the field \mathbb{F}_{p^m} for $p = 3, m = 4$. $\text{ord } a = 80$. $w_2 = 3.75$ while $w_3 = 7.46$.

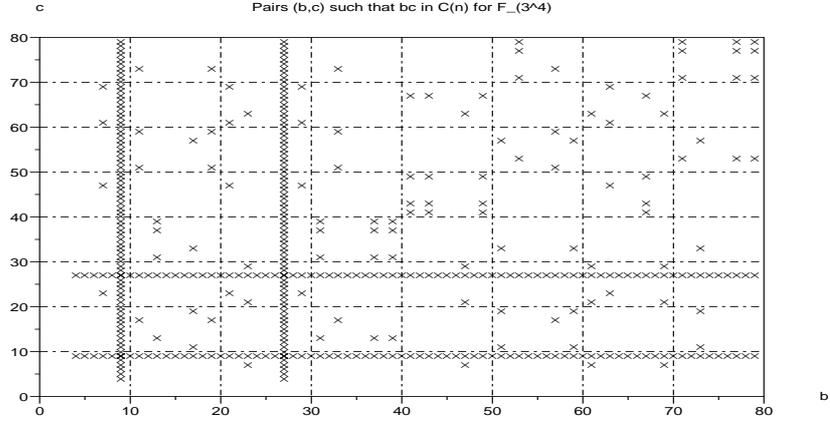


Figure 2: Key pairs (b, c) such that $bc \in C(n)$ for \mathbb{F}_{3^4}

Example 3. Consider the field \mathbb{F}_{p^m} for $p = 2$, $m = 7$. $\text{ord } a = 127$. $w_2 = 4.95$ while $w_3 = 12.47$.

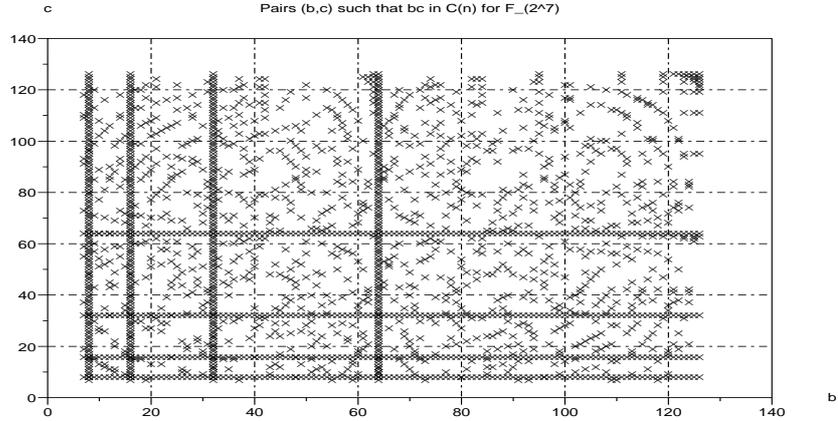


Figure 3: Key pairs (b, c) such that $bc \in C(n)$ for \mathbb{F}_{2^7}

Example 4. Consider the field \mathbb{F}_{p^m} for $p = 5$, $m = 3$. $\text{ord } a = 124$. $w_2 = 1.64$ while $w_3 = 4.57$.

Example 5. In this example we consider a super singular elliptic curve. Let E is given as $y^2 = x^3 + 1$ over a field \mathbb{F}_{101} . A point $P = (21, 24)$ has order 17. Under the Weil pairing it is mapped to a cyclic subgroup of order 17 in the field \mathbb{F}_{101^2} . Hence consider the field \mathbb{F}_{p^m} for $p = 101$, $m = 2$, $w_2 = 5.88$, $w_3 = 30.10$.

Example 6. Consider the field \mathbb{F}_{p^m} with $p = 5$ and $m = 2$. Choosing the minimal polynomial $h(\omega, x) = x^2 + 2$ we get $n = \text{ord } \omega = 24$. Let $a = 6$. We plot all those pairs (b, c)

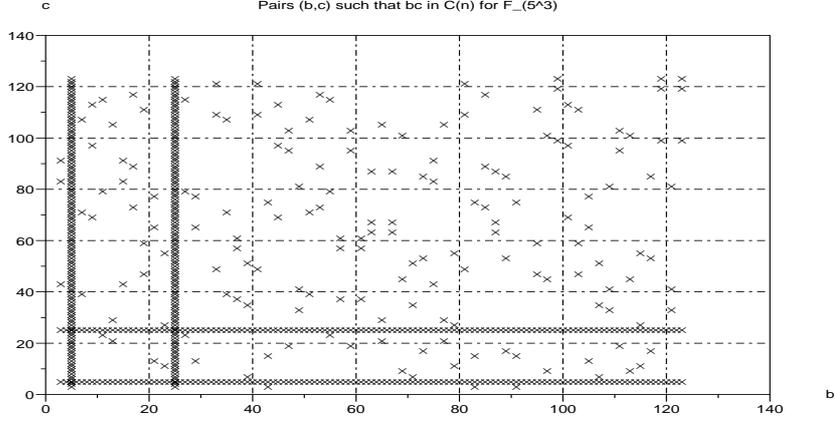


Figure 4: Key pairs (b, c) such that $bc \in C(n)$ for \mathbb{F}_{5^3}

such that the triple (ω, a, bc) satisfies one of the modulus conditions. This plot is shown in figure 6. The number of weak pairs (b, c) is 130 while the total number of possible pairs equals $(n = m)^2 = 529$. Hence the percentage of weak pairs is $130 \times 100/529 = 24.57\%$. However note that for each b there exist weak pairs (a, c) and for each c there exist weak pairs (a, b) . Hence the actual percentage of weak private key triples (a, b, c) for a tripartite session should be higher than the percentage of weak pairs computed above.

Example 7. Now we present an example with practical parameters and show the instances of keys satisfying modulus condition and conjugate class as complete listing of weak keys by exhaustive search is infeasible in reasonable time. Let \mathbb{F}_p be a field with $p = 593917583375891588584754753148372137203682206097$. Let ω be a root of an irreducible polynomial $h(x) = x^2 + x + 2$ over \mathbb{F}_p with order $n = p^2 - 1$. Consider a private keys (b, c) with

$$\begin{aligned} b &= 593917583375891588584754753148372137203682205793 \\ c &= 754523256898294975232475804884023412859850956402 \\ &\quad 03818054246099645349661449424681940813983641137 \end{aligned}$$

It can be seen that $bc \bmod n = p$. This shows that even if b, c are not in conjugate class but their product belongs to $C(n)$. Now we give an instance of private key pairs (b, c) such that their product satisfies modulus condition. Let

$$\begin{aligned} a &= 10002 \\ b &= 2023609450338312739394035451 \\ c &= 44611114391684133095747 \end{aligned}$$

It can be seen that for this choice of private keys, the modulus condition $x^{bc} \bmod h(\omega, x) = x^{bc} \bmod h(\omega^a, x)$ is satisfied. Therefore the shared key ω^{abc} can be computed as $f(\omega^a)$, where $f(x) = x^{bc} \bmod h(\omega, x) = 5708990770823839524233143877797980545530986496x$.

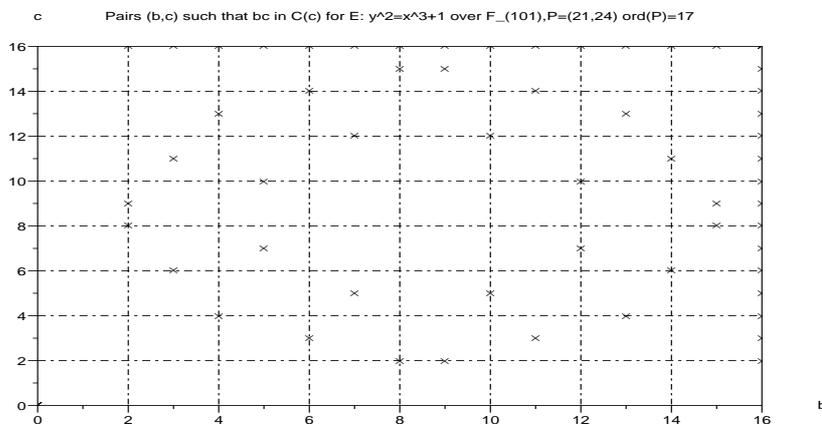


Figure 5: Key pairs (b, c) such that $bc \in C(n)$ for E over \mathbb{F}_{101}

Note that in some of the above examples, the weak key pairs (b, c) are obtained when bc belongs to the conjugate class $C(n)$. Since as shown in [2], there exist nontrivial elements in the set $W(\omega, a)$ not belonging to $C(n)$, the percentage of actual weak pairs (b, c) for which bc belongs to $W(\omega, a)$ should be higher. Hence the percentages w_3 indicated in the examples are lower bounds on the percentage of weak key pairs. Further, this percentage would increase if all the weak keys of all the three possible DHPs are taken into account.

8 Algorithms

Above examples show that the set of weak keys of the tripartite DH scheme is not negligible enough to be ignored, although we do not have a complete characterization of the density of their occurrence. The problem of choosing private keys which are not weak thus assumes importance in the tripartite DH scheme. In this section we develop algorithms for checking whether the private keys chosen by users of the tripartite DH scheme are weak. The problem of choosing keys which are not weak is not yet resolved. However since checking weakness of keys can be done by a very inexpensive computation and since the weak keys are relatively small in proportion to the set of all keys their selection if done repeatedly shall return strong keys. Hence the algorithms for checking weakness of keys can be utilized for choosing strong keys by repeated selection and checking weakness. The proofs that these algorithms work can be established easily from theorems 1 and 2 which we shall skip for brevity.

8.1 Weak keys of the standard DH scheme

The following algorithm checks for weakness of private keys of the standard DH scheme. The session triple (a, k, l) in this case is assumed to have a generator a whose order n satisfies the condition that p , the field characteristics, is not a primitive element of \mathbb{Z}_n^* and that n is prime.

Algorithm 3. (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} 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

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

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 $X = 1$).

It has been shown in [2] that the above algorithm can be executed in polynomial time (in m).

8.2 Weak keys of the tripartite scheme

The weak keys of the tripartite case proposed above are obtained from weak keys of the three associated standard DH problems as shown. Since the characterization of weak keys of the DH scheme is given above in terms of the sets $W_i(a, l), i = 1, 2$. It is necessary to freeze one of the keys say l to describe weak choice of k and vice versa. Analogously in the tripartite case we develop the algorithms by fixing an arbitrary order of choice of private keys say a, b, c . Note further that since weak keys discussed above arise from weak keys of any one of the three DHPs, none of a, b, c are chosen fatally weak i.e. all of them are chosen randomly to lie outside the set $C(n)$. Next, the choice of private keys is governed by computation of weakness of the last chosen key in following stages

1. Having chosen a outside $C(n)$, to determine if b chosen outside $C(n)$ makes ab belong to $C(n)$.
2. Having chosen a, b so that a, b, ab are outside $C(n)$ to determine if the chosen c makes the session triples weak for any one of the three DHPs.

Algorithm 4. (Given the key a of A , this algorithm checks whether b chosen by user B makes the key ab fatally weak (i.e. belongs to $C(n)$) in which case there is no choice for c to be safe).

Input Public data (AP, AQ) of user A .

1. Choose b randomly in \mathbb{Z}_n outside $C(n)$.
2. Compute the pairing $\omega = e(P, Q)$.

3. Compute the public data (BP, BQ) and pairing $\lambda = e(AP, BQ)$.
4. Compute the minimal polynomials $h(\omega, x)$ and $h(\lambda, x)$ of ω and λ respectively in $\mathbb{F}_p[x]$.
5. Assign boolean variable $Z = 1$ if $h(\omega, x) = h(\lambda, x)$ else $Z = 0$.

Output Z . (ab is fatally weak if $Z = 1$).

Next we consider the problem of determining whether the key c chosen randomly by C makes the session triple weak in any one of the three DHPs given that keys a, b have already been chosen and none of them including their product ab is in $C(n)$ i.e. fatally weak. It is assumed that $\omega = e(P, Q)$ is computed beforehand as well as the degree of the minimal polynomial $h(\omega, x)$ of ω over $\mathbb{F}_p[x]$.

Algorithm 5. (This algorithm checks whether the key c to be chosen by the user C belongs to the class of weak keys of the associated DH problem with public data $(\omega, \omega^c, \omega^{ab})$ from the public keys $(AP, AQ), (BP, BQ)$ of users A, B where $\omega = e(P, Q)$).

Input Public data $(AP, AQ), (BP, BQ)$ of users A, B respectively, $m = \deg h(\omega, x)$.

1. Choose c randomly in \mathbb{Z}_n .
2. Compute the public key (CP, CQ) .
3. Compute pairings $\kappa = e(CP, Q), \lambda = e(AP, BQ)$.
4. Compute polynomials f, g in $\mathbb{F}_p[x]$ of degrees less than m such that $\kappa = f(\omega), \lambda = g(\omega)$.
5. Compute $s = \lambda^c$.
6. Assign boolean $Z = 1$ if $(s - f(\lambda))(s - g(\kappa)) = 0$

Output c, Z . (c is weak if $Z = 1$).

Next algorithm checks for weakness of c with respect to the DHP with public data $(\omega, \omega^a, \omega^{bc})$ where a and b are already chosen.

Algorithm 6. (Algorithm to check if either a belongs to $W_1(\omega, bc) \cup W_2(\omega, bc)$ or that bc belongs to $W_1(\omega, a) \cup W_2(\omega, a)$ where a, b are given and c is chosen randomly by the algorithm).

Input Public data $(AP, AQ), (BP, BQ)$ of A, B respectively and $m = \deg h(\omega, x)$.

1. Choose c randomly in \mathbb{Z}_n .
2. Compute the public data (CP, CQ) .
3. Compute $\kappa = e(AP, Q), \lambda = e(BP, Q)^c, \mu = e(AP, BQ)$ and $s = \mu^c$.
4. Compute f, g in $\mathbb{F}_p[x]$ of degrees less than m such that $\kappa = f(\omega), \lambda = g(\omega)$.
5. Assign boolean $Z = 1$ if $(s - f(\lambda))(s - g(\kappa)) = 0$.

Output c, Z . (c is weak if $Z = 1$).

We now take up the third associated DHP with public data $(\omega, \omega^b, \omega^{ca})$ and present an algorithm to determine whether a chosen key c is weak while having already chosen a and b .

Algorithm 7. (Algorithm to check whether the DHP with public data $(\omega, \omega^b, \omega^{ca})$ has a weak session triple where a, b are given, c is chosen by the algorithm and $\omega = e(P, Q)$).

Input Public data $(AP, AQ), (BP, BQ)$ of A, B respectively and $m = \deg h(\omega, x)$.

1. Choose c randomly in \mathbb{Z}_n .
2. Compute $\kappa = e(BP, Q)$, $\lambda = e(CP, AQ)$, $\mu = e(AP, BQ)$ and $s = \mu^c$
3. Compute f, g in $\mathbb{F}_p[x]$ of degrees less than m such that $\kappa = f(\omega)$ and $\lambda = g(\omega)$.
4. Assign boolean $Z = 1$ if $(s - f(\lambda))(s - g(\kappa)) = 0$ else $Z = 0$.

Output c, Z . (c is weak if $Z = 1$).

All of the above algorithms involve important computational steps such as the computation of pairings, the computation of polynomials f, g and the computation of the minimal polynomial of an element of \mathbb{F}_{p^m} where m is the embedding degree of the group of n -torsion points of the elliptic curve. The later two computations can be easily shown to be possible in polynomial time once the pairing is computed. These facts are discussed in [2].

9 Conclusions

Weak keys of the DH key exchange scheme proposed in [2] lead to weak keys of the tripartite DH key exchange scheme. More generally, these lead to weak keys of the pairing based DH schemes which subsume problems such as the BDHP and the DDHP. For the session triples determined by such weak keys these problems can be solved in polynomial time in the given data without solving the discrete logarithm problems. At present pairing based schemes are utilized only over super-singular elliptic curves where the pairings can be computed in polynomial time however nonsingular elliptic curves with small embedding degrees under a pairing are fast becoming popular for pairing based schemes. Weak keys proposed in this paper should be avoided in such schemes.

The weak keys of both, the BDHP and the DDHP are obtained in terms of weak keys of three different standard DHPs. A blowing up of the number of weak keys in the pairing based problems occurs due to the fact that these associated standard DHPs involve products of two private keys which can turn out to be fatally weak even if the individual keys are chosen carefully not to fall in the fatally weak class. Further, just as in the case of standard DH scheme, the choice of private keys of the tripartite DH scheme must be carried out in an order. This allows private keys to be tested for weakness based on the public data of the choices of private keys made beforehand. This fact shows that a random and independent choice of private keys in the tripartite key exchange protocol is not secure and must be modified to include an order of selection of keys.

In conclusion it can be said that pairing based DH schemes involving three choices of private keys are more insecure than the standard DH schemes involving only two parties. Further the practice of random and independent choice of private keys by users is insecure and should be replaced by choice in an order accompanied by testing of weakness of the choice.

Acknowledgements

Authors are grateful to Professor Balwant Singh for many useful discussions.

References

- [1] A. Joux, “A one round protocol for tripartite Diffie Hellman”, Proc. ANTS 4, Lecture Notes in Comp. Sc., vol. 1838, pp. 385-394, 2000.
- [2] A. A. Kalele and V. R. Sule, “Weak keys of the Diffie Hellman key exchange I”, Cryptology ePrint Archive, 2005/24. <http://eprint.iacr.org/2005/024>.
- [3] W. Diffie and M. Hellman, “New directions in cryptography”, IEEE Trans. on Information Theory, vol. 22, pp. 644-654, 1976.
- [4] R. Lidl, H. Niederreiter, ”Finite Fields”, Ency. of Math. and Its Appln. Cambridge University Press, 1997.
- [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 Yi-Hong Wu, “The discrete logarithm problem in GL_n ”, ARS Combinatoria, vol. 47 pp. 23-32, 1998.
- [7] N. Koblitz , “Introduction to number theory and cryptography” Springer Verlag, 1997.
- [8] G. Frey and H. Ruck, “A remark concerning m - divisibility and the discrete logarithm in the divisor class group of curves”, Mathematics of computation, vol. 62, pp. 865-874, 1994.
- [9] N. Kanayama, T. Kobayashi, T. Saito and S. Uchiyama, “Remarks on elliptic curve discrete logarithm problems”, IEICE Trans. Fundamentals, vol. E83A, no. 1, pp. 17-23, Jan. 2000.
- [10] J. Shikata, Y. Zheng, J. Suzuki and H. Imai, “Optimizing Menezes-Okamoto-Vanstone algorithm for non super-singular curves,” Proc. Asiacrypto’99, Lecture Notes in Comp. Sc., vol. 1716, pp. 86-102, Springer Verlag, 1999.

- [11] T. Saito and S. Uchiyama, “ A remark on MOV algorithm for non super-singular elliptic curves”, IEICE Trans. Fundamentals, vol. E84A, no. 5, pp. 1266-1268, May 2001.
- [12] D. Boneh, M. Franklin, “Identity based encryption from the Weil Pairing. In Advances in Cryptology, Crypto 2001. Lecture Notes in Computer Science No. 2139, pp. 213-229, Springer Verlag, Berlin, 2001.
- [13] D. Boneh, A. Silverberg, ”Application of multilinear forms to cryptology”, Contemporary Math. vol. 324, American Math. Soc. pp. 71-90, 2003.
- [14] J. H. Cheon, D. H. Lee, ”Diffie Hellman problems and bilinear maps”, Cryptology ePrint Archive, no. 117, 2002.
- [15] “Pairing based crypto lounge”,
<http://planeta.terra.com.br/informatica/paulobarreto/pblounge.html>, University of Bristol, UK.
- [16] ”A tutorial on Tate pairing”, <http://www.computing.dcu.ie/~mike/tate.html>.
- [17] L. Washington, Elliptic curves, number theory and cryptography, Chapman & Hall/CRC, 2003.
- [18] 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.