Frobenius expansion and the Diffie Hellman problem

V. R. Sule
vrs@ee.iitb.ac.in
Department of Electrical Engineering
Indian Institute of Technology Bombay
Powai, Mumbai 400076, India

May 11, 2006

Abstract

This paper proposes investigation of special sessions of the Diffie Hellman (DH) key exchange scheme on elliptic curves for which the shared key can be computed by a polynomial time algorithm. Such sessions are called *singular*. Existence of singular sessions are demonstrated using the Frobenius expansion and polynomial representation of public keys which lead to an expression for the shared key. When the Weil pairing can be computed on the elliptic curve along with a modified pairing defined by a distortion map efficiently, a sufficient condition is obtained for sessions to be singular which can be verified in polynomial time. Hence this condition identifies sessions whose singular nature can be determined in polynomial time. A single round three party key exchange scheme is proposed using singular sessions in which efficient computation of the shared key of a pair of users by the third party is a necessary requirement. This scheme is thus a positive application of singular sessions and offers a possible alternative to the need for using super singular curves on which pairings can be computed efficiently.

*K*eywords Diffie Hellman scheme, Frobenius expansion, Tri-party key exchange.

1 Introduction

Security of the Diffie Hellman (DH) key exchange scheme over any group rests primarily on the computational difficulty of solving two problems, the discrete logarithm (DL) problem (DLP) and the DH Problem (DHP). The DL computation on cyclic subgroups of elliptic curves is as yet not known to have have yielded to sub-exponential time solutions except in case of super-singular curves. On the other hand provable security can be achieved for the scheme only if the number of all those special key exchange sessions in which the DHP can fall to a polynomial time solution are negligibly small. In this paper we identify such special class of sessions in terms of the parameters of the scheme. While these are insecure for key exchange between two parties, we motivate their positive application, that for single round three party key exchange in which computation of the shared keys of pairs of parties by a third party is a necessary requirement.

A DH session of the DH scheme is defined by the private keys (integers) a, b and corresponding public keys $Q = aP$, $R = bP$ of two parties say A and B where P is a publicly known point on an elliptic curve. Then the shared (or exchanged) key $S = aR = bQ$ and is thus bilinear in the public keys Q, R. It is unknown whether this bilinear function can be constructed, however it would be worthwhile to identify suitable representations of this function and sessions for which computation of S from the public data (P, Q, R) is feasible. A cryptanalyst would naturally construct such representations by means of algorithms and determine the special sessions for which computation of S is possible in polynomial time. We shall call the private key a of A to be *singular* relative to R if a polynomial time algorithm T is available such that $S = T(Q, R)$. The session itself shall be called singular if either a or b is singular relative to R, Q respectively. Further, we shall still call the session singular if a polynomial time algorithm T is available such that Decisional DHP (DDHP) with data $(P, Q, R, T(Q, R))$ can be answered in the affirmative in polynomial time. In practical situations a polynomial time algorithm T may be constructible from the public data to compute $\tilde{S} = T(Q, R)$. Then the sessions are singular whenever $\tilde{S} = S$. However whether or not $\tilde{S} = S$ should be decidable by invoking extra session information which an oracle may provide.

In a practical implementation of the DH scheme the security is thus compromised in singular sessions if there exists such an oracle. Hence accidental occurrence of such sessions during random selection of private keys must be estimated for a given set of parameters of the scheme and such sessions avoided if they are likely to occur frequently. However, singular sessions should have utility in the three party single round key exchange protocol (or in group key exchange schemes). In this protocol it is necessary that each party be able to efficiently compute the solution of the DHP arising from key selection of the other two parties i.e. the DH sessions for any two parties should be intentionally singular. In this way singular DH sessions also have positive applications. A purpose of this paper is to identify singular DH sessions on elliptic curves and to propose their application for the three party key exchange scheme. A central observation of this paper is that such sessions arise from a generalization of the Frobenius expansion of points in $< P >$ on certain elliptic curves.

1.1 Relationships with previous work

The Diffie Hellman key exchange scheme [1] can justifiably be called the flagship of the public key cryptography. Its formulation over elliptic curves and recent progress in understanding and computation of pairings on elliptic curves [3] has especially proved to be very valuable in public key cryptography. Initially the MOV reduction using the Weil pairing on elliptic curves was proposed to reduce the discrete logarithm problem from elliptic curves to that over extension of fields containing a given cyclic group of a point. However it was soon realized that as long as the point has sufficiently high order and has co-ordinates in a field of sufficiently high order, even for a small extension of this field which can encompass the values of the pairing, the DL computation is infeasible and one can utilize pairings for positive applications. This lead to cryptography using pairings. For instance in the three-party key exchange scheme of [6] the DH scheme is modified to what is known as *bilinear* DH scheme, in which the shared key of a pair of parties is a value of a bilinear function of the pair of public keys in a finite field. Applications of pairings however necessitate one to utilize points on super-singular elliptic curves over large extensions of the base field or more generally over curves where the values of pairing involve a small degree field extension thereby giving away the advantage of elliptic curve DL problem. On the other hand it would be worthwhile to explore whether such three or multi-party key exchange schemes can be constructed on general elliptic curves without the use of a bilinear DH scheme or pairings. A necessary requirement of such a scheme for three parties is that each party be able to compute efficiently the two party DHP of every pair of other parties. Thus the DH sessions of each pair of parties must be singular and yet the shared key of the three parties be protected by computation of the DL. In this paper we take the first steps at constructing such a scheme.

Consider an elliptic curve E defined by a polynomial equation with co-efficients over the field $\mathbb{F}_q$ called the *base field*, and let P be a point on $E(\mathbb{F}_{q^m})$ of order n. A DH *session* is defined by the triple $(P, Q, R) = (P, kP, lP)$ called the *public data* of the session for the *private keys* k, l in $\mathbb{Z}_n$. The point $S = klP$ is the *shared key* of the session. Problem of computing S is known as the (computational) DHP. The DL Problem (DLP) of computing k (or l) given the public data, has so far resisted solutions as fast as solving the DLP in groups $\mathbb{F}^*_{q^m}$ (called DLP over finite fields $\mathbb{F}_{q^m}$) which involve sub-exponential time complexity for the index calculus algorithm. Over super-singular curves however, the MOV reduction transforms the DLP in polynomial time to that over a small degree extension of $\mathbb{F}_{q^m}$. Hence for sufficiently large m the DL computation in such a field is still intractable. The DH scheme is then secure if the DH assumption that, the solution of the DHP is as much infeasible as the DL computation, holds. While no formal proof of the DH assumption is known in general, it is often believed to be true for the group under consideration. Several formulations for characterizing the practical validity of this assumption are well known [11, 7, 4, 8]. However in a group being used for the DH scheme, there can be exceptional cases of DH sessions which do not have strong security from the viewpoint of the DH assumption. These are the singular sessions referred above. Singular DH sessions are thus defined by triples (P, k, l) or public data (P, Q, R) for which there is a polynomial time algorithm which can compute S. Recently non-trivial singular cases of the DHP are reported in [9, 10] over finite fields. Note that the singular cases of the DH schemes on elliptic curves which are based on the bilinear DH problem are characterized by the singular cases of the DHP over finite fields. Hence the singular cases discovered in [9, 10] are relevant to pairing based schemes on elliptic curves. This paper extends these singular cases of the DHP to elliptic curves and shows their existence in special cases. A complete and good characterization of these cases is desirable and if achieved, would provide a step in the direction of achieving provable security of the DH scheme.

1.2 Frobenius expansion

In this paper we specifically investigate the singular DH sessions described above for $m > 1$. In this case the Frobenius map is an automorphism of $E(\mathbb{F}_{q^m})$ (unlike the case where E is defined over $\mathbb{F}_q$ and the generator P is also chosen in $E(\mathbb{F}_q)$) and gives rise to the Frobenius expansion of points of $< P >$. It turns out that if

$$Q = \sum_{i=0}^{\mu} a_i \sigma^i P \quad (1)$$

$$R = \sum_{i=0}^{\mu} b_i \sigma^i P \quad (2)$$

are any Frobenius expansions of the public keys Q, R (which always exist [2]) in terms of the conjugates $\sigma^i P$ of the point P, then the shared key S can be expressed in the form

$$S = \sum_{i=0}^{\mu} a_i \sigma^i R \text{ or} \quad (3)$$

$$S = \sum_{i=0}^{\mu} b_i \sigma^i Q \quad (4)$$

with appropriate summation indices, in terms of the conjugates of the public keys Q, R. The largest index of summation is roughly of the order of $\log n$ where n is the order of P, while the co-efficients a_i, b_i arise from a set of integers not larger in cardinality than q. These expressions show that whenever a polynomial time computation of these co-efficients is possible from the public keys as input data, then it also yields the computation of the shared key efficiently (although does not explicitly yield the DL of Q or R with base P). Hence such sessions are singular.

In this paper we define more general expansions analogous to the Frobenius expansion in terms of polynomial maps and investigate singular sessions determined by such expansions. The singular nature of these sessions is a consequence of certain (weak) commutativity between these maps and the multiplication endomorphisms. However commutativity of multiplication endomorphisms corresponding to the private keys are not known from the public keys but a passive adversary can still compute a generalized Frobenius expansion and a candidate shared key $\tilde{S}$. Hence this computation of $\tilde{S}$ leads to a DDHP. However when additionally the Weil pairing (modified by a distortion map) can be computed efficiently on a subgroup containing P, this DDHP can be resolved efficiently and the above computation along with the pairing determines a condition for singular nature of the session. Hence when such a pairing is computable efficiently, the singular sessions can be identified by this condition and the DHP solved in polynomial time without resorting to the computation of the DL. In this way the condition for singular nature of sessions also identifies exceptional cases of the well known DH assumption. Efficient solubility of the DHP is a feature of singular sessions which could turn out useful for the single round multi party extension of the DH scheme. Due to this reason while singular sessions are undesirable for two party key exchange, they might provide an inexpensive solution for a secure multi party scheme.

1.3 Notations and background

We begin by recalling basic notations and shall consider those in [11, 3] for reference. Consider an elliptic curve E defined over a finite field K. Assume that E is defined by the equation in the Weierstrass form with co-efficients in K,

$$\begin{array}{rcl} Y^2 + Y(a_1X + a_3) & = & X^3 + a_2X^2 + a_4X + a_6 \quad \text{or} \\ Y^2 & = & X^3 + AX + B \end{array} \tag{5}$$

when char K is not $2, 3$ and is nonsingular in both of the above cases as an affine variety. For a finite extension L/K, $E(L)$ denotes the set of all points (x, y), $x, y \in L$ which satisfy the above equation. We assume that $K = \mathbb{F}_q$ is of characteristic p while $L = \mathbb{F}_{q^m}$. A DH scheme is defined on a cyclic subgroup $< P >$ of $E(L)$ where P has order n assumed to be coprime to the characteristic p. The set of all n-torsion points of $E(L)$ is denoted by $E[n]$. Finally it is assumed that arithmetical operations referred as $\mathbb{F}_q$-operations can be accomplished in polynomial time in bit length $\log q$. Hence if a computation is feasible in polynomial number of $\mathbb{F}_q$-operations then it is a polynomial time computation. Frobenius map on $E(\mathbb{F}_{q^m})$ is the map $\sigma : E(\mathbb{F}_{q^m}) \to E(\mathbb{F}_{q^m})$, $\sigma(x, y) = (x^q, y^q)$. In the above situation when the defining equation of E has $\mathbb{F}_q$ co-efficients, σ is also an automorphism of the group $E(\mathbb{F}_{q^m})$ and hence commutes with the multiplication endomorphism $P \to mP$. We shall call the set of all points $\pm\sigma^i P$ the *set of conjugates* of P. Since $P = (x, y)$ has co-ordinates x, y in $\mathbb{F}_{q^m}$ the set of conjugates consists at most of points $\{\pm P, \pm\sigma P, \pm\sigma^2 P, \ldots, \pm\sigma^{m-1}P\}$.

2 Frobenius expansions and expressions for the shared key

Frobenius expansion is a representation of the multiplication endomorphism $P \to rP$ in $E(\mathbb{F}_{q^m})$ by an integer r, as the sum of a divisor defined in terms of conjugates of P. This is a consequence of the following well known result [2]

Lemma 1. Given r in $\mathbb{Z}_n$

$$rP = \sum_{i=0}^{k} r_i \sigma^i P \tag{6}$$

where $r_i \in [-\lceil q/2 \rceil + 1, \ldots, \lfloor q/2 \rfloor]$ and $k \leq 2 \log_q 2r + 3$.

We shall however consider more general expansions and also call them Frobenius expansions. For instance an expansion of rP of the form

$$rP = \sum_{i=0}^{m-1} a_i \sigma^i P \tag{7}$$

where a_i belong to $\mathbb{Z}_n$ shall also be called as Frobenius expansion. Clearly, by incorporating larger number of terms in conjugates of P for expanding the multipliers a_i outside the range of r_i in (6), the above expansion can be brought to the form (6).

Let (P, Q, R) be the public data of a DH session. From above lemma an expansion of the shared key of the session in terms of the conjugates of the public keys Q, R as in (1) and (3) follows.

Proposition 1. There exist integers a_i, b_i in $[-\lceil q/2 \rceil + 1, \ldots, \lfloor q/2 \rfloor]$ for $0 \leq i \leq \mu$ such that the shared key of the session with public data (P, Q, R) is given by (3) where $\mu < 2 \log_q 2n + 3$.

Proof. Consider the Frobenius expansions of Q, R as in (1) wherein the co-efficients a_i, b_i exist in the range specified. Since Q, R belong to the cyclic subgroup $< P >$, the multiplier r in the expansion is at most $(n-1)$ where n is the order of P. This gives the bound μ by above lemma. Given such an expansion for Q and $R = lP$, the shared key S of a session (P, Q, R) is given by

$$\begin{aligned} S = lQ &= l \textstyle\sum_{i=0}^{\mu} a_i \sigma^i P \\ &= \textstyle\sum_{i=0}^{\mu} a_i \sigma^i (lP) \\ &= \textstyle\sum_{i=0}^{\mu} a_i \sigma^i R \end{aligned}$$

where only the commutativity of the endomorphisms σ and l is used. Similarly the second expression in (3) also follows. □

In fact it can be easily seen that we may only have a general Frobenius expansion to get an expression of the shared key.

Proposition 2. Consider a DH session with public data (P, Q, R).

1. If an expansion
$$Q = \sum_{i=0}^{m-1} a_i \sigma^i P$$
is known with a_i in $\mathbb{Z}_n$ then the shared key has an expansion
$$S = \sum_{i=0}^{m-1} a_i \sigma^i R$$

2. If an expansion
$$R = \sum_{i=0}^{m-1} b_i \sigma^i P$$
is known with b_i in $\mathbb{Z}_n$ then the shared key has an expansion
$$S = \sum_{i=0}^{m-1} b_i \sigma^i Q$$

The proof follows as in the above proposition on using commutativity of σ with multiplication endomorphisms. Thus the knowledge of the Frobenius expansion of the public keys leads to the expansion of the shared key in terms of conjugates of the public keys. What is important further for the DH scheme is that, the knowledge of the Frobenius expansion of the public data (say Q) does not automatically yield knowledge of its DL. Hence whenever the Frobenius expansion of the public data can be computed efficiently, the DHP can also be solved efficiently.

2.1 Singular DH sessions

We now formally define sessions in which computation of the shared key in terms of public keys is feasible efficiently and it is also feasible to decide that the session has this property.

Definition 1. Let a, b be private keys of a DH session with public data $(P, Q = aP, R = bP)$. Then a is said to be *singular* relative to R if there is available a polynomial time algorithm T such that $S = T(Q, R)$ is the shared key of the session. We shall call the session itself as a *singular session* if either a is singular relative to R or b is singular relative to Q. We shall also call a session singular if there is available a polynomial time algorithm T such that the DDHP (P, Q, R, S) can be answered in affirmative for $S = T(Q, R)$.

Clearly when a Frobenius expansion (1) can be computed in polynomial time the shared key S itself can be computed in polynomial time. Hence such sessions are singular. Instances of trivially singular sessions are given by the following theorem.

Theorem 1. If there exists $1 \leq i \leq (m-1)$ and $k_i \in \mathbb{Z}_n$ such that

$$\pm\sigma^i P = k_i P \tag{8}$$

then the sessions with public data $(P, \pm(k_i^r \bmod n)P, R)$ or $(P, Q, \pm(k_i^r \bmod n)P)$, $r = 0, 1, 2, \ldots$ are singular.

Proof. Consider the session with public data $(P, Q, R) = (P, \pm(k_i^r \bmod n)P, R)$ for some r. Let $s = ir \bmod m$. Then $Q = \pm\sigma^s P$ is the Frobenius expansion of Q of the type (7). The index s of exponent of σ can be computed in polynomial time by comparing Q with $2m$ conjugates $\pm\sigma^i P$. Then from proposition 2 it follows that the shared key is $S = \pm\sigma^s R$ which can be computed in polynomial time by repeated squaring in $\mathbb{F}_{q^m}$ and action of σ on R. In the case of public data $(P, Q, R) = (P, Q, \pm(k_i^r \bmod n)P)$ it can be similarly shown that the shared key $S = \pm\sigma^s Q$ can be computed in polynomial time. Thus the DDHP (P, Q, R, S) is resolved automatically for these sessions. □

Remark 1. The weak sessions in the above theorem have one of the private keys equal to $\pm(k_i^r \bmod n)$. Hence given that the condition (8) is satisfied for some i, if any one of the users chooses a private key satisfying this relation, then for every choice of private key of the other user the session turns out to be singular. We shall call such private keys as *singular keys of conjugate class.* Further, what is worth noting is the fact that the solutions of the DHPs for above class of DH sessions are obtained without computing the DL of the public data. In fact it is only necessary for an adversary to compute the exponent i of σ and verify whether one of the public keys equals a conjugate. This computation can be done in polynomial time and by itself does not yield the DL of Q or R.

A further fatal consequence of the above theorem for the DH scheme is

Corollary 1. If n is prime, the condition (8) is satisfied for some i and k_i is primitive in $\mathbb{Z}_n^*$ then every DH session is singular.

Proof. Since k_i is primitive in $\mathbb{Z}_n^*$ for every multiplier k, such that $Q = kP$, there exists r such that $k = k_i^r \bmod n$. Thus $Q = \sigma^{ir \bmod m} P$ implying that every Q is a conjugate of P. Hence every session with public data (P, Q, R) is singular by the above theorem. □

Clearly the parameters of the DH scheme such as the co-efficients in the defining equation of the elliptic curve E, the point P and its order which cause conditions of the above corollary to be satisfied lead to an insecure DH scheme. Whether the condition (8) holds can be determined off-line from the parameters of the DH scheme. The trivial case of parameters in which singular sessions exist is when the generator $P \in E(\mathbb{F}_{q^m})$ is chosen for which σP is dependent on P as group element thus (8) is satisfied for $i = 1$. Hence we next consider the problem of establishing conditions under which (8) holds.

2.2 Frobenius expansions when conjugates exist in the cyclic subgroup

The Frobenius automorphism σ acts as an automorphism also of the subgroup $E[n]$ of points of order diving n. Hence all conjugates of points of $E[n]$ are in the same subgroup. However the cyclic subgroup $< P >$ need not be invariant under action of σ. The condition (8) is concerned with those conjugates of P which are in $< P >$. We now show that a Frobenius expansion of any point in $< P >$ can be constructed from the knowledge of solutions of (8). Let $\chi(X) = X^2 - tX + q$ denote the characteristic polynomial of σ and for a polynomial $h(X) \in \mathbb{Z}_n[X]$ let $r(X) = h(X) \bmod \chi(X)$ denote the reminder on division by χ. (Such a reminder always exists since $\chi(X)$ is monic, moreover $\deg r(X) \leq 1$). The next result is a condition for existence of solutions to (8).

Proposition 3. For an index i, $1 \leq i \leq (m-1)$ let $r(X) = m_i X + n_i = X^i \bmod \chi(X)$. Then there exists k_i such that (8) holds for the index i iff $\sigma(m_i P) \in < P >$.

Proof. Clearly, $\pm\sigma^i P = \pm r(\sigma)P$. Hence necessity is obvious. Conversely let there exist $a \in \mathbb{Z}_n$ such that $\sigma(m_i P) = aP$. Then $\sigma^i P = m_i \sigma P + n_i P = aP + n_i P$. Hence (8) is satisfied for $k_i = \pm(a + n_i) \bmod n$. □

Clearly, computing k_i satisfying (8) for any i involves solution of a DLP. However such k_i can be precomputed from the parameters of the DH scheme whenever they exist and will be useful in determining singular keys of the conjugate class when the users select their private keys. One type of Frobenius expansion which exists if the condition (8) is known to satisfy for some i and k_i is as follows. (It would be natural to call this an k_i-adic expansion). Assume that there exist an index j, $1 \leq j \leq (m-1)$ such that (8) holds for this index and let κ be the least positive integer among all such k_j.

Proposition 4. Let there exist solutions i and k_i to (8) and κ be the least multiplier in these solutions, then there exists a unique expansion of any Q in $< P >$ of the form

$$Q = \sum_{i=0}^{\mu} a_i \sigma^i P$$

where a_i belong to $\mathbb{Z}/\kappa\mathbb{Z}$ and $\mu < m \log_\kappa n$.

Proof. Since $Q = rP$ for some $r < n$ consider the κ-adic expansion of r

$$r = \sum_{l=0}^{\mu} a_l \kappa^l$$

where $l < \log_\kappa n$. Since $\kappa P = \sigma^j P$ for some $1 \leq j \leq (m-1)$ it follows that rP has the expansion claimed where the largest power of σ is bounded by $m \log_\kappa n$. □

3 Analogs of the Frobenius expansion

Frobenius expansion can be generalized using other polynomial maps. Frobenius mapping (being a group endomorphism of E) also commutes with the multiplication endomorphism $r : E \to E$, $P \mapsto rP$. This commutativity plays the main role in causing sessions to be singular whose public keys are conjugates of P. We may extend such commutativity even to maps which may not be endomorphisms yet commute with special multipliers. We moreover need such commutativity to be defined only at a point P to get analogous singular sessions.

Definition 2. Let Φ and Ψ be rational mappings of E into itself. These mappings shall be called *commutative at P* if Φ, Ψ and the compositions $\Phi \circ \Psi$, $\Psi \circ \Phi$ are defined at P and

$$(\Phi \circ \Psi)(P) = (\Psi \circ \Phi)(P)$$

A mapping Φ is said to *commute with r at P* if Φ commutes at P with multiplication endomorphisms $P \mapsto rP$ for r in $\mathbb{Z}_n$.

We can now get an analogue of the expansion of the shared key S in proposition 1 in terms of expansions of the public data as follows.

Proposition 5. Let Φ_i, $i = 1, 2, \ldots, N$ be a family of rational mappings of E defined at P which commute with l at P. Then a DH session with public data (P, Q, R) where $R = lP$ and

$$Q = \sum_{i=1}^{N} a_i \Phi_i(P)$$

has the shared key given by

$$S = \sum_{i=1}^{N} a_i \Phi_i(R)$$

Proof. Immediate from commutation of Φ_i with l at P. □

The Frobenius map powers σ^i are some of the special examples of maps Φ_i. Thus if Q has an expansion of the above form the expression for S is the shared key of any session (P, Q, R) in which Φ_i commute with the DL of R at P. Analogous proposition holds relative to expansion of R as follows.

Proposition 6. Let Ψ_i, $i = 1, 2, \ldots, N$ be a family of rational mappings of E defined at P which commute with k at P. Then a DH session with public data (P, Q, R) where $Q = kP$ and

$$R = \sum_{i=1}^{N} a_i \Psi_i(P)$$

has the shared key given by

$$S = \sum_{i=1}^{N} a_i \Psi_i(Q)$$

We next construct maps in the above propositions from the public data and obtain more general form of singular sessions than those in which the public data consist of conjugates of P. This uses the fundamental property of multipliers, their rational representation.

3.1 Rational representation of multiplication

Elements of $< P >$ have a natural rational representation in terms of co-ordinates x, y of P given by the following well known lemma [11] presented here in slightly restricted form.

Lemma 2. For any $P = (x, y)$ in $E[n]$ of order n and every $k < n$

1. There exists a unique pair of rational functions $r_{1k}(X)$, $r_{2k}(X)$ in $\mathbb{F}_q(X)$ expressed in terms of coprime numerator and denominator, dependent only on k such that
$$kP = (r_{1k}(x), yr_{2k}(x))$$
2. $kP = \infty$ iff $r_{1k}(X)$ is undefined at x (or has a pole at x).
3. If $r_{1k}(X)$ is defined at x then $r_{2k}(X)$ is also defined at x.

In fact a rational representation in the above form holds for all endomorphisms of E and that the second item above means that P is in the kernel of k as an endomorphism iff $r_{1k}(x)$ is undefined. Details may be referred from [11]. From this representation it follows that if (P, Q, R) is the public data of a DH session with parameters (P, k, l) then there exist unique rational functions $r_{ik}(X)$, $r_{il}(X)$ in $\mathbb{F}_q(X)$ such that

$$\begin{array}{rcccl} Q & = & (x_k, y_k) & = & (r_{1k}(x), yr_{2k}(x)) \\ R & = & (x_l, y_l) & = & (r_{1l}(x), yr_{2l}(x)) \end{array} \tag{9}$$

while the shared key can be expressed in either of the following way

$$\begin{array}{rcl} S & = & (x^*, y^*) \\ & = & (r_{1k}(x_l), y_l r_{2k}(x_l)) \\ & = & (r_{1l}(x_k), y_k r_{2l}(x_k)) \end{array} \tag{10}$$

3.2 Polynomial representation

Next we construct a polynomial representation for elements of $< P >$. Let $P = (x, y)$ in $E(\mathbb{F}_{q^m})$ be of order n and let $h(X)$ in $\mathbb{F}_q[X]$ denote the minimal polynomial of x with $d = \deg h(X)$. Clearly $d \leq m$.

Lemma 3. For every $k < n$ there exists a unique pair of polynomials $\phi_k(X)$, $\psi_k(X)$ in $\mathbb{F}_q[X]$ such that

1. $\deg \phi_k(X) < d$, $\deg \psi_k(X) < d$
2. $kP = (\phi_k(x), y\psi_k(x))$

Proof. Consider the rational functions $r_{ik}(X) = p_{ik}(X)/q_{ik}(X)$ of the previous lemma, $i = 1, 2$, where $p_{ik}(X), q_{ik}(X)$ belong to $\mathbb{F}_q[X]$ and are coprime. Since $kP \neq \infty$, $q_{ik}(x) \neq 0$. Hence r_{ik} is defined at all roots of $h(X)$ or that $q_{ik}(X)$ are units in $\mathbb{F}_q[X]/h(X)$. Thus there exist polynomials $f_{ik}(X)$ such that $q_{ik}(X)f_{ik}(X) \bmod h(X) = 1$ which implies $q_{ik}(x)^{-1} = f_{ik}(x)$ for all roots x of $h(X)$. Hence $r_{ik}(x) = p_{ik}(x)f_{ik}(x)$. Let $\phi(X) = p_{1k}(X)f_{1k}(X) \bmod h(X)$ and $\psi(X) = p_{2k}(X)f_k(X) \bmod h(X)$. Then from lemma 2 it follows that $\phi_k(X)$, $\psi_k(X)$ satisfy the conditions claimed while uniqueness follows from uniqueness of $r_{ik}(X)$ in terms of coprime fractions. □

Remark 2. The polynomials representing co-ordinates of points $kP = (x_k, y_k)$ are in $\mathbb{F}_q[X]$ however they are dependent on P which is in $E(\mathbb{F}_{q^m})$. For this reason, unlike the rational functions $r_{ik}(X)$ which depend only on k, the polynomials $\phi_k(X)$, $\psi_k(X)$ are also unique for given k but vary with P. A better notation would have been $\phi_{k,P}(X)$, $\psi_{k,P}(X)$. We shall call representation of kP in the above lemma as *polynomial representations* over $\mathbb{F}_q$ and to be of degree equal to $\max(\deg \phi, \deg \psi)$. Note that only the polynomial representation of degree less than d is unique as shown above. There can be multiple representations of degree $\geq d$.

Another important characteristic of the polynomial representation say $kP = \Phi_k(P)$ of the multiplier endomorphism k is that the polynomial map $\Phi_k : E \to E$ equals a rational mapping of E defined at P and evaluated at P. Hence the property of commutativity defined above for rational mappings can be extended to polynomial representations also.

Next theorem shows that the polynomial representation is efficiently computable from the public data. Note that a rational representation of multiples kP is well known in terms of the division polynomials. However computation of division polynomials from kP is then equivalent to the DL computation on the elliptic curve.

Theorem 2. Given Q in $< P >$ the unique polynomials ϕ, ψ in $\mathbb{F}_q[X]$ in lemma 3 of degrees less d can be computed in polynomial time.

Proof. Following notations of lemma 3, observe first that the minimal polynomial $h(X)$ of x is computable in polynomial number of $\mathbb{F}_q$ operations. The elements $1, x, x^2 \ldots x^{(d-1)}$ are $\mathbb{F}_q$-linearly independent in $\mathbb{F}_{q^m}$. Hence relative to any basis of $\mathbb{F}_{q^m}$ the conditions $Q = (\phi(x), y\psi(x))$ and ϕ, ψ in $\mathbb{F}_q[X]$ lead to equations,

$$\sigma^i Q = (\phi(x^q), y^q \psi(x^q))$$

for $0 \leq i \leq (d-1)$ which are two systems of d equations in d unknowns. These systems of equations are linear in the unknown co-efficients of each of ϕ, ψ and have unique solutions since $1, x, x^q, \ldots, x^{q^{(d-1)}}$ are $\mathbb{F}_q$-linearly independent. Thus $\mathbb{F}_q$ co-efficients of the polynomials ϕ, ψ can be computed in polynomial number of $\mathbb{F}_q$ operations. □

.

4 Singular Diffie Hellman sessions on elliptic curves

Polynomial time solubility of ϕ, ψ in the above theorem and the analogues of the Frobenius expansions of propositions 6, 5 now lead us to identifying singular sessions when supplemented with the knowledge that the multipliers of P defining the public data commute with these polynomial representations.

Theorem 3. Let (P, Q, R) be a DH session,

1. Let Q have a polynomial representation $Q = \Phi(x, y) = (\phi_1(x), y\phi_2(x))$ and $R = lP$. If Φ commutes with l at P then the session (P, Q, R) is singular and $S = \Phi(R)$ is the shared key of the session.

2. Let R have a polynomial representation $R = \Psi(x, y) = (\psi_1(x), y\psi_2(x))$ and $Q = kP$. If Ψ commutes with k at P then the session (P, Q, R) is singular and $S = \Psi(Q)$ is the shared key of the session.

Proof. Formulas for S are special cases of expansions in propositions 5, 6 which in turn essentially follow from commutativity of Φ, Ψ with l, k respectively. Since co-efficients of Φ and Ψ can be computed in polynomial time and the evaluations $\Phi(R)$, $\Psi(Q)$ can also be carried out in polynomial time, the theorem follows. □

Above theorem shows that the knowledge of commutativity of k, l with Ψ, Φ rather than these parameters themselves is enough for a polynomial time algorithm to compute S. All such sessions which satisfy these commutativity conditions are singular.

Algorithm 1 (Algorithm for computing S for singular sessions)**.** *Input* Public data (P, Q, R).

1. Compute polynomial representations of minimal degree $Q = \Phi(P)$, $R = \Psi(P)$.

2. Compute $S_1 = \Phi(R)$, $S_2 = \Psi(Q)$.

Output Shared key $S = S_1$ if l commutes with Φ at P, $S = S_2$ if k commutes with Ψ at P.

4.1 Identifying singular sessions

Above theorem identifies singular sessions under the knowledge that the maps Φ, Ψ representing the public data at P commute with multipliers k, l at P. In the case of singular sessions identified earlier one of the public data Q or R is a conjugate of P. In this case it is evident that polynomial maps Φ, Ψ being constructed from the powers of the Frobenius map, commute with any multipliers l, k. Hence the DH sessions in which such a commutativity of Φ, Ψ with k, l at P is not known are not necessarily a priori singular. Nevertheless, since Φ, Ψ exist and are computable in polynomial time for a given public data, $\Phi(R)$ and $\Psi(Q)$ can also be computed in polynomial time and are candidates for the shared key even when not confirmed as a shared key. Alternatively, we can say that in the standard DH scheme the lack of knowledge of k, l gives rise to a DDHPs with public data $(P, Q, R, \Phi(R))$ and $(P, Q, R, \Psi(Q))$. Those DH sessions for which these DDHPs can be answered in the affirmative in polynomial time are singular sessions.

(It is worth noting however that the situation is opposite in the case of three party key exchange scheme which utilizes these singular cases of standard DH session. In this scheme a legitimate user has public key of another user (say Q) and is required to choose a private key l such that $(P, Q, R = lP)$ is a singular session since the third party is required to compute the shared key of this session using the public data. Hence it is necessary to construct a condition involving the private key l so that the session (P, Q, lP) is singular).

Consider a DH session (such as an El Gammal encryption session) in which the first user selects a private key and communicates the public key to the second user who wishes to encrypt a message. The second user must then have at her disposal an algebraic formula to check if the private key selected by her makes the session weak. This is given by the following corollary to the above theorem which describes l which make a session singular when k is fixed.

Corollary 2. Let Q be the public key of one of the members of a DH session and let $Q = \Phi(P)$ be a polynomial representation. If l is the private key of the second member with public key $R = lP$ and $R = \Psi(P)$ is a polynomial representation, then the session is singular if any one of the following conditions hold

$$\begin{array}{rcl} lQ & = & \Phi(R) \\ lQ & = & \Psi(Q) \end{array} \tag{11}$$

Proof. Clearly the shared key of the session (P, Q, R) is lQ. First relation is same as $lQ = \Phi(lP)$ which denotes commutation of Φ with l at P. Similarly, since the shared key also equals kR the second relation is equivalent to $kR = \Psi(kP)$. Hence the session is singular due to theorem 3. □

A symmetrically analogous condition for describing k which make a session singular when l is fixed is given by

Corollary 3. Let R be the public key of one of the members of a DH session and let $R = \Psi(P)$ be a polynomial representation. If k is the private key of the second member with public key $Q = kP$ and $Q = \Phi(P)$ is a polynomial representation, then the session is singular if any one of the following conditions hold

$$\begin{array}{rcl} kR & = & \Psi(Q) \\ kR & = & \Phi(R) \end{array} \tag{12}$$

The above corollaries show that given Q the set of all l which commute with the minimal degree polynomial representation $Q = \Phi(P)$ are singualr relative to Q. (Let this set be denoted by $W(Q)$). Symmetrically, given R the set of all k which commute with the minimal degree polynomial representation $R = \Psi(Q)$ are singular relative to R. (Let this be denoted by $W(R)$). Both of these sets are subsets of $\mathbb{Z}_n$ and can be utilized by a user of a DH scheme to determine whether the private key chosen by her makes the session singular. Note that whenever the private keys are singular of conjugate class (see remark after theorem 1) one of the relations in (11) or (12) is automatically satisfied. It is worthwhile noting this as

Corollary 4. Let R be the public key of one member with polynomial representation $R = \Psi(P)$. If the private key l ($R = lP$), is of conjugate class then every k satisfies $kR = \Phi(R)$ for $Q = kP$ and polynomial representation $Q = \Phi(P)$ and l satisfies $lQ = \Phi(R)$.

Proof. Since l is of conjugate class there is an i such that $R = \sigma^i P$. Then $kR = k\sigma^i P = \sigma^i kP = \sigma^i \Phi(P) = \Phi(\sigma^i P) = \Phi(R)$ which follows due to the binomial theorem. Similarly, $lQ = k(lP) = k\sigma^i P = \sigma^i(kP) = \sigma^i Q = \sigma^i(\Phi(P)) = \Phi(\sigma^i P) = \Phi(R)$. □

Similar result holds for k of the conjugate class. These show that the set of pairs (k, l) in which k satisfies one of the relations (11) and l satisfies one of (12) is non empty and contains conjugate class private keys. These relations can have more solutions than that of the conjugate class as demonstrated by the special case of $E(\mathbb{F}_p)$ analyzed below. In this special case there are no conjugates however there exist solutions to relations (11) and (12).

4.2 Modified DH scheme

Consider now a modified form of the standard DH protocol which incorporates rejection of singular sessions of the above type when either k belongs to $W(R)$ or l belongs to $W(Q)$.

Protocol 1 (Diffie Hellman protocol with rejection of singular sessions)**.** Alice and Bob share a key over a public channel. Assume P to be a point on $E(\mathbb{F}_{q^m})$ of order n, while the curve is defined on $\mathbb{F}_q$.

1. Alice and Bob establish priorities for choice of private keys. Let Alice has first priority.
2. Alice chooses a random k, $1 < k < (n-1)$, computes and publishes the public key $Q = kP$.
3. Bob chooses a random l, $1 < l < (n-1)$ and computes $R = lP$ and the polynomial representations of minimal degree $Q = \Phi(P)$ and $R = \Psi(P)$.
4. Bob computes $\Phi(R)$ and $\Psi(Q)$ and checks whether any one of them equal lQ. If neither of $\Phi(R)$, $\Psi(Q)$ equal lQ, Bob publishes R as his public key of the session and ends the protocol.
5. If the above check fails, Bob rejects l and repeats the choice of l till success in the above step.

Above protocol depends on random selection of private keys by the second user and then rejecting those which turn out singular relative to the public key of the first user. A good characterization of singular sessions should lead to a one step selection.

4.3 Occurrence of singular sessions

In practice the keys shared by DH sessions are used as seeds for generation of long encryption keys. A guessed shared key can be verified for its correctness if an oracle service for answering the DDHP is available. In [9, 10] random trials of session generation and the number of times singular sessions occur are reported for the DH scheme over finite fields. These empirical results show that singular sessions can turn out to be significant under certain choices of parameters. A theoretical estimate of their density in the finite fields as well as the elliptic curve case being discussed in this paper is still an unresolved issue which acquires significance in view of the application of the singular sessions for three party key exchange scheme constructed in this paper. The question of existence of singular sessions characterized by (12) and (11) is resolved by the fact that the conjugates of P in $< P >$ satisfy these equations. Moreover for the case of P belonging to $E(\mathbb{F}_p)$ we identify conditions under which there exist singular sessions. Since in this special case the set of conjugates is empty, existence of singular sessions establishes that there exist more singular sessions than those in which the public data contains conjugates of P. Note however that every point in $< P >$ has a polynomial representation hence the shared key of a session itself has a polynomial representation. It appears that there are no singular sessions other than those characterized by the relations (12) and (11). It has however not been possible to prove this result in this paper.

Another argument can be given in support of existence of singular sessions in which the public keys are not conjugates. For instance consider the DH scheme in which P satisfies (8) for powers i, j, $\sigma^i P = k_i P$ and $\sigma^j P = k_j P$. Then $\sigma^i P + \sigma^j P = (k_i + k_j)P = kP$ is an element say Q of $< P >$ which need not be a conjugate of P. However both sessions $(P, k_i P, lP)$ and $(P, k_j P, lP)$ are singular say with shared keys S_i and S_j and the shared key of the session $(P, kP, lP) = (P, Q, R)$ is $S = S_i + S_j$. Now a polynomial time search on i, j such that the equality $\sigma^i P + \sigma^j P = Q$ is verified reveals that $S = \sigma^i R + \sigma^j R$. Thus the session is singular without the private key k being singular of conjugate class.

In the elliptic curve based DH scheme, sessions with conjugate public data as well as possibility of more general sessions becoming singular due to Frobenius expansions being efficiently computable, do not seem to have appeared in the literature to the best of author's knowledge.

4.4 Condition for singular sessions in terms of pairings

It is now apparent that in the elliptic curve case we can resolve the above DDHP arising out of computation of S in theorem 3 in certain cases where the Weil paring can be computed on $E[n]$ efficiently and there is available a distortion map. This is a well known way by which a DDHP with only two parties is resolved by Weil pairing [5, 11]. Let the curve E now be super-singular and $e(.,.)$ denote the Weil pairing on $E[n]$. Assume that there is available a distortion morphism $T : E[n] \to E[n]$ at P which is an isomorphism of the group $E[n]$ such that P and $T(P)$ are independent. We further assume that T can be evaluated on points of $E[n]$ efficiently. Given such a distortion morphism it is well known that $\tilde{e}(P, Q) = e(P, T(Q))$ is a paring on $E[n]$ and $\tilde{e}(P, P)$ is an n^{th} root of unity not equal to one.

Theorem 4. Consider a DH session on a super-singular curve E with public data (P, Q, R) on the subgroup $E[n]$ on which there is available a distortion morphism T such that T can be evaluated on points of $E[n]$ in polynomial time. Let $Q = \Phi(P)$, $R = \Psi(P)$ be polynomial representations of Q, R. Then the session is singular if any one of the following sets of conditions hold.

1. $n\Phi(R) = \infty$, $e(P, \Phi(R)) = 1$ and
$$\tilde{e}(P, \Phi(R)) = \tilde{e}(\Phi(P), R) \tag{13}$$
The point $S = \Phi(R)$ is the shared key.

2. $n\Psi(Q) = \infty$, $e(P, \Psi(Q)) = 1$ and
$$\tilde{e}(P, \Psi(Q)) = \tilde{e}(\Psi(P), Q) \tag{14}$$
The point $S = \Psi(Q)$ is the shared key.

Proof. The two conditions on $\Phi(R)$ viz $n\Phi(R) = \infty$ and $e(P, \Phi(R)) = 1$ imply that $S = \Phi(R)$ is in $< P >$ (as shown in lemma 5.1 of [11]). Now S is the shared key of the session iff
$$e(P, T(S)) = \tilde{e}(Q, R)$$

due to the property of the modified pairing. This is precisely the condition (13) written in terms of the modified pairing. The computation of S involves computation of the polynomial representation $Q = \Phi(P)$ and the evaluation $\Phi(R)$ while verification of $\Phi(R)$ as the shared key S involves computation of the distortions $T(R)$, $T(\Phi(R))$, checking whether n annihilates $\Phi(R)$ and pairings $\tilde{e}(P, \Phi(R))$, $\tilde{e}(Q, R)$ all of which can be computed in polynomial time due to assumptions on T and super singular nature of E. This proves that $S = \Phi(R)$ is the shared key and is computed from the public data in polynomial time whenever the conditions given are satisfied. This proves the first part. The second part can be proved on similar lines by using the symmetry property of the modified pairing $\tilde{e}(,)$ when restricted to the subgroup $< P >$, giving $\tilde{e}(P, Q) = \tilde{e}(Q, P)$ for Q in $< P >$. □

.

A special case of distortion maps viz the trace map is also useful in the above situation. The trace map $\mathrm{Tr} : E(\mathbb{F}_{q^m}) \to E(\mathbb{F}_{q^m})$ is defined as

$$\mathrm{Tr}(P) = \sum_{i=0}^{(m-1)} \sigma^i(P)$$

where the sum on the right hand side in taken in the group E. It is well known that $\mathrm{Tr}(P)$ belongs to $E(\mathbb{F}_q)$ and is an endomorphism of $E(\mathbb{F}_{q^m})$. Further when n is prime and P is not in $E(\mathbb{F}_q)$, $e(P, \mathrm{Tr}(P)) \neq 1$. Thus Tr is a distortion morphism of E.

Corollary 5. Consider a DH session on E with public data (P, Q, R) and let $Q = \Phi(P)$, $R = \Psi(P)$ be polynomial representations over $\mathbb{F}_q$. Then the session is singular if any one of the following conditions hold.

1. $n\Phi(R) = \infty$, $e(P, \Phi(R)) = 1$ and

$$\prod_{i=0}^{(m-1)} e(P, \Phi(\sigma^i R)) = \prod_{i=0}^{(m-1)} e(\Phi(P), \sigma^i R) \tag{15}$$

2. $n\Psi(Q) = \infty$, $e(P, \Psi(Q)) = 1$ and

$$\prod_{i=0}^{(m-1)} e(P, \Psi(\sigma^i Q)) = \prod_{i=0}^{(m-1)} e(\Psi(P), \sigma^i Q) \tag{16}$$

Proof. Proof follows immediately from theorem 4 on using the fact that the modified pairings are symmetric in the sense that $\tilde{e}(R, Q) = \tilde{e}(Q, R)$ when restricted to elements R, Q in $< P >$ and noting that the distortion map is defined by the trace homomorphism. Hence

$$\begin{array}{rcl} \tilde{e}(P, \Phi(R)) & = & e(P, \sum_{i=0}^{m-1} \sigma^i \Phi(R) \\ & = & e(P, \sum_{i=0}^{m-1} \Phi(\sigma^i R)) \\ & = & \prod_{i=0}^{m-1} e(P, \Phi(\sigma^i R)) \end{array}$$

which gives the left hand side of (15). Next

$$\begin{array}{rcl} \tilde{e}(\Phi(P), R) & = & e(\Phi(P), \sum_{i=0}^{m-1} \sigma^i R) \\ & = & \prod_{i=0}^{m-1} e(\Phi(P), \sigma^i R) \end{array}$$

which gives the right hand side of (15). The equation (16) can be similarly established after using symmetry of the pairing. □

4.5 A tri-party key exchange based on singular sessions

We now describe an application of the singular sessions described above for a single round tri-party key exchange protocol. In this case there are three members A, B, C who wish to share a common key. The members first agree on an elliptic curve $E(\mathbb{F}_q)$ and a point P in $E(\mathbb{F}_{q^m})$ of order n. Then they execute the following protocol.

Protocol 2 (Three party single round key exchange protocol)**.** Three users A, B, C exchange a common key.

1. A chooses a private key a randomly in $\mathbb{Z}_n$, computes and publishes the public key $U = aP$ along with the polynomial representation $U = \Phi_a(P)$ of minimal degree.

2. B chooses the private key b in $\mathbb{Z}_n$ randomly and computes $V = bP$ along with the polynomial representation $V = \Phi_b(P)$ of minimal degree.

3. B checks whether one of the relations $bU = \Phi_a(V)$ or $bU = \Phi_b(U)$ holds. If none of these relations are satisfied B rejects b and repeats the choice of b until one of these relations hold. Once one of these relations are satisfied B publishes $U_{ab} = bU$, V and the polynomial representation of minimal degree, $V = \Phi_b(P)$.

4. C chooses private key c in $\mathbb{Z}_n$ randomly and computes $W = cP$ along with the polynomial representation $W = \Phi_c(P)$ of minimal degree.

5. C verifies whether at least one of the relations among $cU = \Phi_a(W)$, $cU = \Phi_c(U)$ as well as at least one among $cV = \Phi_b(W)$, $cV = \Phi_c(V)$ holds. If none of these relations are satisfied, C rejects c and repeats the choice of c until success. Once one of these relations are satisfied, C publishes only $U_{ac} = cU$ and $U_{bc} = cV$.

6. A computes $S_a = aU_{bc}$, B computes $S_b = bU_{ac}$ and C computes $S_c = cU_{ab}$. By design of b, c it follows that $S_a = S_b = S_c = abcP$.

The above protocol achieves a three party key exchange based on the special cases of two party DH sessions in which the DHP can be efficiently solved but does not utilize pairings or need the curve to be super singular. Note that P need not be agreed as a parameter but need only be published as a public key by A if such a choice is acceptable to other users. Security of the above protocol relies on the same fact that the private keys can be computed from the public keys by solution of the DL over the elliptic curve. However the public data (U_{ab}, U_{bc}, U_{ac}) poses a new three party DHP similar to the bilinear DH problem. Note that in the above protocol, the public data consists of points on E, as well as constraints on public keys arising from the polynomial representations.

Problem 1 (Three party DHP)**.** Given the points $(U, V, U_{ab}, U_{bc}, U_{ca})$, the constraints 1) $U_{ab} = \Phi_a(V)$ or $U_{ab} = \Phi_b(U)$, 2) $U_{ab} = bU = aV$, $U_{bc} = cV$, $U_{ac} = cU$ compute $abcP = cU_{ab} = aU_{bc} = bU_{ca}$.

Similarly a decisional version of the above problem can be posed as follows.

Problem 2 (Three party DDHP)**.** Given points $(U, V, U_{ab}, U_{bc}, U_{ca})$ satisfying the constraints as in the above problem and a point S, determine whether $S = abcP$.

Analysis of these problem as well as cryptanalysis of the protocol shall be carried out in greater detail in a future article. Clearly, the analysis of the above three party exchange scheme is not complete unless singular sessions of the three party case can be determined analogous to the two party scheme above and the above protocol is augmented by rejection of singular sessions. This aspect shall be explored elsewhere.

4.6 The case $E(\mathbb{F}_p)$

We now take a look at the case $m = 1$ for completeness. In this case the Frobenius map is not available as above. However the singular DH sessions can still be defined using the relations (11) defining the set $W(Q)$ and (12) defining the set $W(R)$. Consider the DH session over $E(\mathbb{F}_p)$ with P also over $\mathbb{F}_p$ and the public data $(P, Q = kP, R = lP)$. An obvious polynomial representation for such a data is to choose Φ as the constant polynomial Q and Ψ as the constant polynomial R. Hence singular sessions arise for these polynomial maps when (12) or (11) are satisfied.

Consider the case when Q is specified. The set of all l for which the session is singular is then given by the constraints $lQ = Q$ or $lQ = R$. These equations are respectively $klP - kP = \infty$ or $klP - lP = \infty$. Hence for each k in $\mathbb{Z}_n$ the set of l which can make the session singular (i.e. the set $W(Q)$) is given by

$$W(Q) = \{l \in \mathbb{Z}_n | k(l-1) \bmod n = 0 \text{ or } l(k-1) \bmod n = 0\}$$

If n is prime the only nonzero solutions of l in $W(Q)$ are $l = 1$. It is apparent that the size of $W(Q)$ increases with the number of prime divisors of n and their powers. For instance if $n = p'q'$ with p', q' prime, we have the following relations arising from the Chinese reminder theorem, that l is in $W(Q)$ iff one of $p'|k$, $q'|k$ hold or one of $p'|(l-1)$, $q'|(l-1)$ hold.

This shows that the singular sessions of more general class than the conjugate class exist since solutions to k, l can exist for above equations which arise in this special case $E(\mathbb{F}_p)$ where there are no conjugates of P other than $-P$. It would thus be fruitful to build the multi-party schemes with large prime p and the point order n having several prime factors. However the DL problem is easier when the prime factors of n are small after MOV reduction. Hence a choice of P shall be governed by these considerations. Moreover these special sessions above are defined by the minimal degree polynomial representation. Singular sessions generated using higher degree polynomial representations should provide a larger class of singular sessions and should be useful sessions for the multi-party key exchange. These aspects shall be explored elsewhere.

Appendix

Frobenius expansions defined by endomorphisms

For completeness of discussion consider another analogue of the Frobenius expansion and a subsequent expression of the shared key of a DH session. This expansion can be said to generalize the p-adic expansions well known in finite fields. Let $h : E(\mathbb{F}_{q^m}) \to E(\mathbb{F}_{q^m})$ be an endomorphism of the elliptic curve. Then we call an expansion of an element Q in $< P >$ of the form

$$Q = \sum_{i=0}^{N} a_i h^i(P)$$

where a range for constants a_i and the largest summation index N are specified, as an h-adic expansion of Q. For instance let $q = p^m$, E is defined over $\mathbb{F}_p$ and P belongs to $E(\mathbb{F}_q)$. Also assume that p does not divide the order n of P. If $Q = kP$ and let

$$k = \sum_{i=0}^{N} a_i p^i$$

be the p-adic expansion of k, where a_i belong to $\mathbb{F}_p$ and $N = \lceil \log_p k \rceil$. Then a p-adic expansion of Q in terms of the multiplication endomorphism by p is given by

$$Q = \sum_{i=0}^{N} a_i p^i P$$

As a special case consider the case of binary expansion. Let $k = \beta_0 + \beta_1 2 + \ldots + \beta_t 2^t$ be the binary expansion of k. Then $Q = kP$ has the expansion

$$Q = \sum_{i=0}^{t} \beta_i 2^i P$$

which can be called as binary expansion of Q in terms of P. It follows due to the fact that h is an endomorphism that an analogous expansion formula can be given for the shared key of a DH session.

Proposition 7. Let (P, Q, R) be the public data of a DH session over $E(\mathbb{F}_{p^m})$. If Q, R are expressed in terms of the p-adic Frobenius expansions

$$\begin{aligned} Q &= \sum a_i p^i P && (17) \\ R &= \sum b_i p^i P && (18) \end{aligned}$$

where a_i, b_i belong to $\mathbb{F}_p$, then the shared key has the expansions

$$\begin{aligned} S &= \sum a_i p^i R && (19) \\ S &= \sum b_i p^i Q && (20) \end{aligned}$$

The proof is quite straightforward and only depends on commutativity of multiplication by p with other multipliers. Note however that computation of the co-efficients a_i, b_i is tantamount to computation of the DLs of Q, R. A similar set of formulas can be written for the binary Frobenius expansion.

5 Concluding remarks

This paper builds on the fact that having a Frobenius expansion of public keys in $< P >$ of any DH session in terms of a sum of conjugates of P leads to an expression of the shared key of the session in terms of the co-efficients of this expansion. Following these expansions singular DH sessions are defined for which the computation of the shared key can be carried out in polynomial time. This computation moreover does not yield the discrete logarithms in the elliptic curve group. A more general polynomial representation of public keys is also shown to exist which is used to generalize the Frobenius expansion and analogous definition of singular sessions. On ellliptic curves over which the Weil pairing can be computed efficiently a sufficient condition for sessions to be singular is determined. This condition allows determination of singular nature of sessions in polynomial time. Efficient solution of the DHP is a necessary requirement in multi-party key exchange problems. Hence the singular sessions of the two party DH session can be put to positive use in such schemes. A scheme for three party key exchange based on the singular sessions is constructed in this paper as a first step along this goal. In the use of the DH scheme for two party key exchange, the parameters of the scheme must be selected to cause negligible singular sessions. On the other hand choosing these parameters to cause a large number of singular sessions may be in the interest of a multi party key exchange.

Acknowledgements

Author is thankful to Professor Balwant Singh and Amit Kalele for useful discussions.

References

[1] W. Diffie and M. E. Hellman. New directions in cryptography. IEEE Trans. on Information Theory, IT 22, Nov 1976, pp.644-654.

[2] I. F. Blake, G. Seroussi and N. P. Smart. Elliptic curves in cryptography. Cambridge University Press, 1999.

[3] I. F. Blake, G. Seroussi and N. P. Smart. Advances in elliptic curve cryptography. Cambridge University Press, 2005.

[4] R. Dutta, R. Baruah and P. Sarkar. Pairing based cryptographic protocols, a survey. http://eprint.iacr.org/2004/64.

[5] A. Joux and K. Nguyen. Separating Decision Diffie-Hellman problem from Diffie-Hellman in cryptographic groups. J. Cryptology, 16, pp.239-248, 2003.

[6] A. Joux. A one round protocol for tripartite Diffie Hellman. J. of Cryptology, 17, pp.263-276, 2004.

[7] D. Hankerson, A. J. Menezes and S. C. Vanstone. Guide to elliptic curve cryptography. Springer 2004.

[8] A. J. Menezes, P. C. van Oorschot and S. A. Vanstone. Handbook of Applied Cryptography. CRC Press, 1996.

[9] A. A. Kalele and V. R. Sule. Weak keys of the Diffie Hellman key exchnage I. http://eprint.iacr.org/2005/24.

[10] A. A. Kalele and V. R. Sule. Weak keys of the Diffie Hellman key exchnage II. Pairing based schemes on elliptic curves. http://eprint.iacr.org/2005/30.

[11] L. C. Washington. Elliptic curves, number theory and cryptography. Chapman & Hall/CRC, 2003.