An analysis of the vector decomposition problem[⋆]

Steven D. Galbraith[1] and Eric R. Verheul[2]

[1] Mathematics Department,
Royal Holloway, University of London,
Egham, Surrey, TW20 0EX,
United Kingdom.
steven.galbraith@rhul.ac.uk

[2] PricewaterhouseCoopers Advisory, Radboud University Nijmegen,
P.O. Box 22735, 1100 DE, Amsterdam, The Netherlands.
eric.verheul@[nl.pwc.com, cs.ru.nl]

Abstract. The vector decomposition problem (VDP) has been proposed as a computational problem on which to base the security of public key cryptosystems. We give a generalisation and simplification of the results of Yoshida on the VDP. We then show that, for the supersingular elliptic curves which can be used in practice, the VDP is equivalent to the computational Diffie-Hellman problem (CDH) in a cyclic group. For the broader class of pairing-friendly elliptic curves we relate VDP to various co-CDH problems and also to a generalised discrete logarithm problem 2-DL which in turn is often related to discrete logarithm problems in cyclic groups.

Keywords: Vector decomposition problem, elliptic curves, Diffie-Hellman problem, generalised discrete logarithm problem.

1 Introduction

The vector decomposition problem (VDP) is a computational problem in non-cyclic groups G (see Section 2 for the definition of this problem). It was introduced by Yoshida [22, 23] as an alternative to the discrete logarithm or Diffie-Hellman problems for the design of cryptographic systems. Yoshida proved that if certain conditions hold then the VDP is at least as hard as the computational Diffie-Hellman problem (CDH) in a certain cyclic subgroup G_1 of G. Since the CDH in G_1 may be hard, it follows that VDP may be hard, and so it is a potentially useful problem on which to base public key cryptography. Indeed, cryptosystems based on the VDP have been proposed in [22, 23, 10].

As with any new computational problem in cryptography, it is important to understand the hardness of VDP if one is to use it in practice. Apart from the result of Yoshida, there is no discussion in the literature of the difficulty of the VDP. Hence, it is an open problem to determine the precise security level of the VDP and thus to evaluate the security/performance of cryptosystems based on it. That is the primary motivation of this paper.

We prove that the VDP in G is equivalent with certain co-CDH problems in G if a mild condition holds. A corollary is that CDH $\leq$ VDP for a much larger class of groups than considered by Yoshida. We then prove that VDP $\leq$ CDH for groups satisfying a condition similar to that considered by Yoshida (namely, existence of what we call a "distortion eigenvector base"). We show that all the supersingular elliptic curves which can be used in practice satisfy this condition. It follows that CDH and VDP are equivalent in practice for supersingular curves. We also prove this equivalence for the non-supersingular genus 2 curves proposed by Duursma and Kiyavasch [9]. Our results therefore completely resolve the issue of the difficulty of the VDP in the groups considered by [22, 23, 9, 10].

Duursma and Park [10] proposed a signature scheme based on VDP. Our results imply that their signature scheme has no security advantages over systems based on CDH or DLP. One can therefore compare the performance of the scheme in [10] with, say, Schnorr signatures and deduce that their scheme has no advantages in practice.

[⋆] This is the full version of a paper which is to appear in R. Cramer (ed), PKC 2008, Springer LNCS (2008)

To summarise the paper: the main definitions and results are in Section 2. Section 3 proves that distortion eigenvector bases exist for the supersingular elliptic curves which can be used in practice. Section 4 explains how our conditions relate to the definitions given by Yoshida. In Section 5 we review possible constructions of non-cyclic groups for cryptography. Finally, Section 6 gives some methods to reduce the VDP to various generalised discrete logarithm problems.

2 The vector decomposition problem and relations with CDH

Let $r > 3$ be a prime. The vector decomposition problem is usually expressed in terms of a 2-dimensional vector space over $\mathbb{F}_r$. However, it has currently only been instantiated on subgroups of exponent r of the divisor class group of a curve over a finite field. Hence, in this paper we use a group-theoretic formulation.

Throughout the paper G will be an abelian group of exponent r and order r^2 (i.e., G is isomorphic to $(\mathbb{Z}/r\mathbb{Z}) \times (\mathbb{Z}/r\mathbb{Z})$). We assume implicitly that G can be represented compactly and that the group operation can be computed in polynomial time. For examples of such groups see Section 5. We write such groups additively and use capital letters P, Q, R for elements of G. We use the notation $\langle P_1, \dots, P_n \rangle$ for the subgroup of G generated by $\{P_1, \dots, P_n\}$. We call a pair (P_1, P_2) a *base* for G if it generates G, i.e. each element in $Q \in G$ can be uniquely written as a linear combination in P_1 and P_2.

If A and B are computational problems then we denote Turing reduction of A to B by A $\leq$ B. This means that there is a polynomial time algorithm for solving problem A given access to an oracle to solve problem B. We call such a reduction tight if the probability of success of algorithm A is at least the probability of success of oracle B.

Definition 1. *The* ***vector decomposition problem (VDP)****: given a base (P_1, P_2) for G and an element $Q \in G$, compute an element $R \in G$ such that $R \in \langle P_1 \rangle$ and $Q - R \in \langle P_2 \rangle$.*

For a fixed base (P_1, P_2) we define VDP$_{(P_1,P_2)}$ as: given $Q \in G$ find R as above.

Clearly, such an element R is unique and if we write $Q = aP_1 + bP_2$ for unique $a, b \in \mathbb{Z}/r\mathbb{Z}$ then $R = aP_1$. We stress that an algorithm to solve the vector decomposition problem should take as input a triple (P_1, P_2, Q) and output a point R such that $R \in \langle P_1 \rangle$ and $Q - R \in \langle P_2 \rangle$. The **VDP conjecture** is that there exist families of groups for which the VDP is hard in the sense that there is no polynomial time algorithm which succeeds in solving the VDP on groups in the family with non-negligible probability over all possible input triples.

Yoshida proved that CDH $\leq$ VDP under certain conditions (see below). This suggests that VDP can be a hard problem. Our main goal in this paper is to give results in the other direction. As pointed out by an anonymous referee, an easy example of such a result can be obtained in the direct product of a cyclic group.

Definition 2. *Let G_1 be a cyclic group of order r. The* ***computational Diffie-Hellman problem*** *CDH(G_1) is: given $P, aP, bP \in G_1$, compute abP.*

Lemma 1. *Let G_1 be a cyclic group of prime order r and let $G = G_1 \times G_1$. If one can solve the VDP in G then one can solve CDH in G_1.*

Proof. Let P, aP, bP be the input CDH problem. Let $P_1 = (P, aP)$, $P_2 = (0, P)$ and $Q = (bP, rP)$ for a random integer r. Note that $Q = bP_1 + (r - ab)P_2$ so solving the VDP instance (P_1, P_2, Q) gives $R = bP_1 = (bP, abP)$ and extracting the second component solves CDH. □

The literature on the VDP seems to contain only three examples of suitable groups. Precisely, Yoshida [23] suggests the supersingular elliptic curve $y^2 = x^3 + 1$ (see Example 1 below) and Duursma-Kiyavash [9] suggest two non-supersingular genus 2 curves. However, it is obvious that one could use any pairing-friendly elliptic curve for applications based on the VDP.

We remark that VDP does not seem to trivially be random self-reducible. In other words, if we have an algorithm $\mathcal{A}$ which solves VDP for some non-negligible proportion of instances then it seems not to be trivial to convert $\mathcal{A}$ into an algorithm which solves VDP with overwhelming probability over all instances. However, we show in Corollary 2 that one can obtain random self-reducibility for the VDP.

The following definition is the key concept which underlies most of the results in the paper.

Definition 3. *Let G be a group of exponent r and order r^2. Let $F : G \to G$ be a group isomorphism computable in polynomial time. A pair of elements $S, T \in G$ is an* ***eigenvector base*** *with respect to F if $G = \langle S, T \rangle$ and if $F(S) = \lambda_1 S$ and $F(T) = \lambda_2 T$ for some distinct, non-zero $\lambda_1, \lambda_2 \in \mathbb{Z}/r\mathbb{Z}$.*

In practice F will usually be the Frobenius map (more details are given later). Hence we often abbreviate 'eigenvector base with respect to F' by 'eigenvector base'.

Example 1. A standard example of such a group is as follows: Let $p \equiv 3 \pmod 4$ be prime and let $E : y^2 = x^3 + x$ over $\mathbb{F}_p$. Then E is a supersingular elliptic curve and $\#E(\mathbb{F}_p) = p + 1$. Let $r > 3$ be a prime such that $r \mid (p + 1)$. Then we can let $G = E[r] \subseteq E(\mathbb{F}_{p^2})$ be the group of all points on E of order r. Let S be a generator for $E(\mathbb{F}_p)[r]$. Denote by F the p-power Frobenius map $F(x, y) = (x^p, y^p)$. Note that $F(S) = S$ so $\lambda_1 = 1$. Consider the isomorphism ϕ defined by $\phi(x, y) = (x, iy)$ where $i \in \mathbb{F}_{p^2}$ satisfies $i^2 = -1$. Setting $T = \phi(S)$ we have $G = \langle S, T \rangle$ and $F(T) = -T$. Hence (S, T) is an eigenvector base with respect to F. (Indeed, this is also a distortion eigenvector base, which will be defined later.)

Proposition 1. *The VDP$_{(P_1,P_2)}$ with respect to a fixed base (P_1, P_2) is solvable in polynomial time iff (P_1, P_2) is an eigenvector base.*

Proof. For the proof of the "if" part of the result: let $F : G \to G$ be the group isomorphism as in the definition of eigenvector base. Let $\alpha = (\lambda_2 - \lambda_1)^{-1} \pmod r$. For $i = 1, 2$ define the projection map $\psi_i : G \to \langle P_i \rangle$ by

$$\psi_1(R) = \alpha(\lambda_2 R - F(R)) \ \ ; \ \psi_2(R) = \alpha(F(R) - \lambda_1 R).$$

These are efficiently computable group homomorphisms. Note that $\psi_1(P_1) = P_1$ and $\psi_1(P_2) = 0$ and so ψ_1 maps to $\langle P_1 \rangle$. Similarly, ψ_2 maps to $\langle P_2 \rangle$. Since $Q = \psi_1(Q) + \psi_2(Q)$ for all $Q \in G$ and the maps ψ_1, ψ_2 are easily computable, it follows that VDP with respect to (P_1, P_2) is easily solvable.

For the proof of the "only if" part of the result: suppose $\mathcal{A}$ is a polynomial time algorithm to solve VDP$_{(P_1,P_2)}$. Define

$$\psi_1(Q) = \mathcal{A}(Q) \text{ and } \psi_2(Q) = Q - \psi_1(Q).$$

Then ψ_i $(i = 1, 2)$ are group homomorphisms to $\langle P_i \rangle$ which can be computed in polynomial time. Any linear combination $F = \lambda_1\psi_1 + \lambda_2\psi_2$ with distinct, non-zero $\lambda_1, \lambda_2 \in \mathbb{Z}/r\mathbb{Z}$ has the desired properties so that (P_1, P_2) is an eigenvector base. □

The fact that there are easy instances of VDP$_{(P_1,P_2)}$ does not affect the VDP conjecture for such curves. The conjecture is that the VDP should be hard for a randomly chosen input triple from the set G^3. In other words, it is permitted that the VDP be easy for a negligible proportion of triples in G^3.

2.1 Diffie-Hellman problems and relation with VDP

We recall the co-CDH problem as defined by Boneh, Lynn and Shacham [5].

Definition 4. *Let G_1 and G_2 be cyclic groups of order r. The* ***co-Computational Diffie-Hellman problem*** *co-CDH(G_1, G_2) is: Given $P, aP \in G_1$ and $Q \in G_2$, compute aQ.*

Note that having a perfect algorithm to solve co-CDH is equivalent to being able to compute a group homomorphism $\psi : G_1 \to G_2$ such that $\psi(P) = Q$.

Lemma 2. *Let G_1, G_2 be cyclic groups of order r. Then CDH(G_1) $\leq$ (co-CDH(G_1, G_2) and co-CDH(G_2, G_1)).*

Proof. Suppose we have oracles to solve both co-CDH problems which succeed with probability at least ϵ. Let P, aP, bP be given. Choose a random $Q \in G_2$ and a random $x \in (\mathbb{Z}/r\mathbb{Z})^*$ and call the co-CDH(G_1, G_2) oracle on (xP, xaP, Q) to get aQ with probability at least ϵ.

Now, choose random $x_1, x_2 \in (\mathbb{Z}/r\mathbb{Z})^*$ and call the co-CDH(G_2, G_1) oracle on (x_1Q, x_1aQ, x_2bP) to get x_2abP with probability at least ϵ. Exponentiating by x_2^{-1} gives abP as desired. The probability of success is at least ϵ^2. □

In Lemma 4 we give a converse to the above result if additional conditions hold (e.g., for supersingular elliptic curves). Note that if one can solve CDH(G_1) and one has a suitable auxiliary elliptic curve for the Maurer reduction [15, 16] then one can solve the DLP in G_1 and hence solve co-CDH(G_1, G_2). Hence it is natural to conjecture that CDH(G_1) and co-CDH(G_1, G_2) are equivalent. However, it could conceivably be the case that there exist groups such that (co-CDH(G_1, G_2) and co-CDH(G_2, G_1)) is strictly harder than CDH(G_1). It would follow from Theorem 1 below that VDP is a strictly harder problem than CDH(G_1) for these groups.

The following computational problem is similar to the problem DCDH defined by Bao et al [2], who also proved equivalence with CDH. For completeness we give a trivial Lemma which is needed later.

Definition 5. *The **co-Divisional Computational Diffie-Hellman problem** co-DCDH(G_1, G_2) is, given (S, aS, T) for $S \in G_1, T \in G_2$, to compute $a^{-1}T$.*

Lemma 3. *co-DCDH(G_1, G_2) $\leq$ co-CDH(G_1, G_2).*

Proof. Given a co-DCDH instance (S, aS, T) choose uniformly at random $x_1, x_2, x_3 \in (\mathbb{Z}/r\mathbb{Z})^*$ and return $(x_2x_3)^{-1}$co-CDH(x_1aS, x_1x_2S, x_3T). Hence, if we can solve co-CDH with probability at least ϵ then one can solve co-DCDH with probability at least ϵ. □

Yoshida [22, 23] showed that CDH $\leq$ VDP for supersingular elliptic curves having endomorphisms satisfying certain conditions. Theorem 1 below gives a major extension of Yoshida's result, since it has much weaker conditions and can be applied to ordinary curves (we give more discussion of this later). Also note that Yoshida's result requires a perfect oracle to solve VDP (i.e., one which always succeeds) whereas our proof allows an oracle with only some non-negligible probability of success (this is a non-trivial improvement since VDP does not seem to trivially have random self-reducibility).

Theorem 1. *Let G have an eigenvector base (S, T) and define $G_1 = \langle S \rangle$, $G_2 = \langle T \rangle$. Then VDP is equivalent to (co-CDH(G_1, G_2) and co-CDH(G_2, G_1)).*

More precisely, if one can solve VDP with probability at least ϵ then one can solve (co-CDH(G_1, G_2) and co-CDH(G_2, G_1)) with probability at least ϵ. If one can solve (co-CDH(G_1, G_2) and co-CDH(G_2, G_1)) with probability at least ϵ then one can solve VDP with probability at least ϵ^9.

Proof. First we show that co-CDH(G_1, G_2) $\leq$ VDP (the full statement follows by symmetry). We assume that we have a VDP oracle which succeeds with probability ϵ and show that one can solve co-CDH(G_1, G_2) with probability ϵ.

Let S, aS, T be given. Choose uniformly at random $x_1, x_2, y_1, y_2 \in (\mathbb{Z}/r\mathbb{Z})$ such that $x_1x_2 - y_1y_2 \not\equiv 0 \pmod{r}$. Then $(P_1 = x_1S + y_1T, P_2 = y_2S + x_2T)$ is a uniformly random base for G. There exist $\lambda, \mu \in (\mathbb{Z}/r\mathbb{Z})$ such that $aS = \lambda P_1 + \mu P_2$. One has

$$aS = \lambda(x_1S + y_1T) + \mu(y_2S + x_2T) = (\lambda x_1 + \mu y_2)S + (\lambda y_1 + \mu x_2)T$$

and so

$$\begin{pmatrix} x_1 & y_2 \\ y_1 & x_2 \end{pmatrix} \begin{pmatrix} \lambda \\ \mu \end{pmatrix} = \begin{pmatrix} a \\ 0 \end{pmatrix}. \tag{1}$$

Calling a VDP oracle on $(P_1, P_2, aS + u_1P_1 + u_2P_2)$ for uniformly random $u_1, u_2 \in (\mathbb{Z}/r\mathbb{Z})$ and subtracting u_1P_1 from the output gives $\lambda P_1 = \lambda x_1S + \lambda y_1T$ with probability ϵ. Using Proposition 1 one can compute $R = \lambda y_1T$.

Equation (1) implies that $\lambda \equiv (x_1x_2 - y_1y_2)^{-1}x_2a \pmod{r}$. It follows that one can compute aT as

$$aT = (x_1x_2 - y_1y_2)(y_1x_2)^{-1}R.$$

This completes the first part of the proof.

For the second part, we assume oracles to solve co-CDH(G_1, G_2) and co-CDH(G_2, G_1) which work with probability at least ϵ. By Lemma 2 we can also solve ordinary CDH in $\langle S \rangle$ and $\langle T \rangle$ with probability at least ϵ^2. We will show how to solve VDP with probability at least ϵ^9.

Let (P_1, P_2, Q) be the input instance of the VDP. Then

$$Q = aP_1 + bP_2$$

for unknown integers (a, b). Our goal is to compute aP_1.

There exist (unknown) integers $u_{i,j}$ for $1 \leq i, j \leq 2$ such that

$$P_i = u_{1,i}S + u_{2,i}T \tag{2}$$

and integers (v_1, v_2) such that $Q = v_1S + v_2T$. By Proposition 1, we can compute $u_{1,i}S$, $u_{2,i}T$, v_1S and v_2T.

Write

$$U = \begin{pmatrix} u_{1,1} & u_{1,2} \\ u_{2,1} & u_{2,2} \end{pmatrix}.$$

Since $\{S, T\}$ and $\{P_1, P_2\}$ both generate G, it follows that U is invertible. Clearly,

$$v_1S + v_2T = Q = aP_1 + bP_2 = (au_{1,1} + bu_{1,2})S + (au_{2,1} + bu_{2,2})T \tag{3}$$

and so

$$U \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} v_1 \\ v_2 \end{pmatrix}.$$

Hence,

$$\begin{pmatrix} a \\ b \end{pmatrix} = (u_{1,1}u_{2,2} - u_{1,2}u_{2,1})^{-1} \begin{pmatrix} u_{2,2} & -u_{1,2} \\ -u_{2,1} & u_{1,1} \end{pmatrix} \begin{pmatrix} v_1 \\ v_2 \end{pmatrix}$$

and so

$$aP_1 = (u_{1,1}u_{2,2} - u_{1,2}u_{2,1})^{-1}(u_{2,2}v_1 - u_{1,2}v_2)(u_{1,1}S + u_{2,1}T).$$

Compute $u_{2,2}v_1T, u_{1,1}u_{2,2}S$ and $u_{1,2}u_{2,1}S$ using 3 calls to co-CDH oracles and $u_{1,2}v_2T$ using one call to a CDH oracle for $\langle T \rangle$ (which is achieved using 2 calls to co-CDH oracles). Then solve co-DCDH$(S, (u_{1,1}u_{2,2} - u_{1,2}u_{2,1})S, (u_{2,2}v_1 - u_{1,2}v_2)T)$ using Lemma 3 to get aT.

Given $S, u_{1,1}S, aT$ and $u_{2,1}T$ one can compute aP_1 with one call to a CDH oracle for $\langle T \rangle$ and one call to a co-CDH oracle. It follows that we require 5 co-CDH queries and 2 CDH queries, which means that the algorithm succeeds with probability at least ϵ^9. □

Corollary 1. *Let G be as above and suppose G has an eigenvector base (S, T). Let $G_1 = \langle S \rangle$. Then CDH(G_1) $\leq$ VDP.*

More precisely, if one has an oracle to solve VDP with probability at least ϵ then one can solve CDH(G_1) with probability at least ϵ^2.

Proof. This is immediate from Theorem 1 and Lemma 2. □

Corollary 2. *Suppose G has an eigenvector base. Then the VDP has random self-reducibility.*

Proof. The second part of the proof of Theorem 1 shows how to convert a VDP instance into a number of co-CDH instances. The first part of the proof of Theorem 1 shows how to convert a co-CDH instance into a uniformly random instance of the VDP in G. Hence, a specific VDP instance in G is reduced to a number of uniformly random VDP instances in G. □

2.2 Distortion eigenvector bases and equivalence of VDP and CDH

Definition 6. *An eigenvector base (S, T) is said to be a* ***distortion eigenvector base*** *if there are group homomorphisms $\phi_1 : \langle S \rangle \to \langle T \rangle$ and $\phi_2 : \langle T \rangle \to \langle S \rangle$ computable in polynomial time and if an integer $d \not\equiv 0 \pmod{r}$ is given such that $\phi_2(\phi_1(S)) = dS$.*

In Section 3 we will show that the commonly used pairing-friendly supersingular elliptic curves all have a distortion eigenvector base.

Lemma 4. *Let G be as above and suppose G has a distortion eigenvector base (S, T). Let $G_1 = \langle S \rangle$ and $G_2 = \langle T \rangle$. Then CDH(G_1) is equivalent to co-CDH(G_1, G_2) and co-CDH(G_2, G_1). Moreover, the reductions in both directions are tight.*

Proof. Suppose we have an oracle to solve CDH with probability at least ϵ. Given a co-CDH instance (S, aS, T) we want to compute aT. Note that $\phi_2(T) = cS$ for some (not necessarily explicitly known) integer c and that $\phi_1(cS) = dT$ for known d. Since $\text{CDH}(S, aS, cS) = acS$ it follows that the solution to the co-CDH problem is given by

$$(d^{-1} \pmod r)\phi_1(\text{CDH}(S, aS, \phi_2(T))).$$

Hence, we can solve co-CDH with probability at least ϵ (note that CDH and co-CDH are clearly random self-reducible).

For the converse, suppose S, aS, bS is an instance of CDH(G_1). Then one obtains the co-CDH instance $(S, aS, \phi_1(bS))$ and the solution to the CDH is $(d^{-1} \pmod r)\phi_2(\text{co-CDH}(S, aS, \phi_1(bS)))$. □

This allows a refinement of Corollary 1.

Corollary 3. *Suppose G has a distortion eigenvector base (S, T) and let $G_1 = \langle S \rangle$. Suppose one has an oracle to solve VDP with probability at least ϵ. Then one can solve CDH(G_1) with probability at least ϵ.*

We then obtain one of the main results in the paper, that VDP is equivalent to CDH in many cases. This is a significant sharpening of Yoshida's result, and gives a complete understanding of VDP for supersingular curves.

Corollary 4. *Let (S, T) be a distortion eigenvector base for G. Then VDP is equivalent to CDH($\langle S \rangle$).*

Proof. Let $G_1 = \langle S \rangle$ and $G_2 = \langle T \rangle$. Theorem 1 showed VDP equivalent to co-CDH(G_1, G_2) and co-CDH(G_2, G_1) and so the result follows by Lemma 4. □

Note that when given a CDH oracle then the probability of success in Theorem 1 is ϵ^7 instead of ϵ^9.

2.3 An application of trapdoor VDP

Proposition 1 shows that VDP is easy for certain bases while Theorem 1 indicates that VDP is hard in general. Hence it is natural to ask if there is a way to set up a trapdoor VDP system. We now explain how to do this.

Proposition 2. *Let (S, T) be a distortion eigenvector base for G normalised such that $T = \phi_1(S)$. Let $u_{1,1}, u_{1,2}, u_{2,1}, u_{2,2} \in \mathbb{Z}/r\mathbb{Z}$ be such that $u_{1,1}u_{2,2} - u_{1,2}u_{2,1} \not\equiv 0 \pmod r$. Let $P_1 = u_{1,1}S + u_{2,1}T$ and $P_2 = u_{1,2}S + u_{2,2}T$. Given any $Q \in G$, if one knows the $u_{i,j}$ then one can solve the VDP of Q to the base (P_1, P_2).*

Proof. We have $T = \phi_1(S)$ and replacing ϕ_2 by $(d^{-1} \pmod r)\phi_2$ we have $\phi_2(T) = S$.

Write $Q = aP_1 + bP_2$. We are required to compute aP_1. Since (S, T) is an eigenvector base we can compute v_1S and v_2T such that $Q = v_1S + v_2T$. Using ϕ_1 and ϕ_2 we can compute v_1T and v_2S. By the same arguments as in Theorem 1, writing $w = (u_{1,1}u_{2,2} - u_{1,2}u_{2,1})^{-1} \pmod r$, it follows that

$$\begin{aligned} aP_1 &= w(u_{2,2}v_1 - u_{1,2}v_2)(u_{1,1}S + u_{2,1}T) \\ &= w(u_{2,2}u_{1,1}v_1S + u_{2,2}u_{2,1}v_1T - u_{1,1}u_{1,2}v_2S - u_{1,2}u_{2,1}v_2T) \end{aligned}$$

which is easily computed. □

Note that we do not have a full trapdoor which allows solving any instance (P_1, P_2, Q) of the VDP. Instead, we construct an easy base (P_1, P_2) for the VDP from an existing easy base (S, T).

This idea has several cryptographic applications. For example, one can obtain a public key encryption scheme (having OW-CPA security depending on VDP) with public key $(S, Q = u_{1,2}S + u_{2,2}T)$ and where the private key consists of the $u_{i,j}$. A message $M \in \langle S \rangle$ is encrypted as $C = M + bQ$ for random $1 \le b < r$.

2.4 The decision vector decomposition problem

As suggested by an anonymous referee, one can consider a decision variant of the VDP.

Definition 7. *The **decision vector decomposition problem (DVDP)** is: given (P_1, P_2, Q, R) to test whether $R \in \langle P_1 \rangle$ and $(Q - R) \in \langle P_2 \rangle$.*

Hence the DVDP is just testing subgroup membership, which is a computational problem in cyclic groups rather than in G and which may or may not be easy depending on the groups in question. For example, if $G = E[r]$ for an elliptic curve then one can test subgroup membership using the Weil pairing (namely, $R \in \langle P_1 \rangle$ if and only if $e_r(P_1, R) = 1$). Also, if (S, T) is an eigenvector base with respect to F then testing subgroup membership is easy ($P \in \langle S \rangle$ if and only if $F(P) = \lambda_1 P$ where λ_1 is the eigenvalue of F on S).

The decision version of the co-CDH problem is defined as follows [5].

Definition 8. *Let G_1 and G_2 be distinct cyclic groups of order r. The **co-decision Diffie-Hellman problem** co-DDH(G_1, G_2) is: Given $S, aS \in G_1$ and $T, T' \in G_2$ to determine whether or not $T' = aT$.*

Note that co-DDH(G_1, G_2) is trivially equivalent to co-DDH(G_2, G_1).

Lemma 5. *If G_1 and G_2 are distinct cyclic subgroups of G then co-DDH$(G_1, G_2) \leq$ DVDP in G.*

Proof. Suppose we have an oracle to solve DVDP and let (S, aS, T, T') be the input co-DDH instance. We assume that $\langle S \rangle \cap \langle T \rangle = \{0\}$ and that $T' \in \langle T \rangle$. Let $b \in (\mathbb{Z}/r\mathbb{Z})$ be such that $T' = bT$.

Choose random $x_{1,1}, x_{1,2}, x_{2,1}, x_{2,2}, z \in (\mathbb{Z}/r\mathbb{Z})^*$ such that $x_{1,1}x_{2,2} - x_{1,1}x_{2,1} \not\equiv 0 \pmod{r}$. Let $P_1 = x_{1,1}S + x_{2,1}T$, $P_2 = x_{1,2}S + x_{2,2}T$, $Q = x_{1,1}aS + x_{2,1}T' + zP_2$ and $R = x_{1,1}aS + x_{2,1}T'$ and call the DVDP oracle on (P_1, P_2, Q, R). If $b \equiv a \pmod{r}$ then $R \in \langle P_1 \rangle$ and the oracle should answer 'true'. If $b \not\equiv a \pmod{r}$ then $R \notin \langle P_1 \rangle$ and the oracle should answer 'false'. □

One can verify that for the case $G = E[r]$, where DVDP is easily solved using the Weil pairing, the proof of Lemma 5 leads to the standard method for solving co-DDH using pairings (note that if G_1 and G_2 are distinct in $E[r]$ then $e_r(S, T) \neq 1$).

Theorem 2. *Let G have an eigenvector base (S, T) and define $G_1 = \langle S \rangle$, $G_2 = \langle T \rangle$. Then DVDP is equivalent to co-DDH(G_1, G_2).*

Proof. Lemma 5 gives co-DDH$(G_1, G_2) \leq$ DVDP. To prove the converse we show how to solve the subgroup membership problem for any subgroup $H = \langle R \rangle \subset G$. If $H = \langle S \rangle$ or $H = \langle T \rangle$ then, as mentioned, we can efficiently solve membership. Hence, we may assume that the projections $\psi_1(R)$ and $\psi_2(R)$ in the proof of Proposition 1 are non-trivial. Let $P \in G$. Then $P \in \langle R \rangle$ if and only if $(\psi_1(R), \psi_1(P), \psi_2(R), \psi_2(P))$ is a valid co-DDH(G_1, G_2) instance. The result follows. □

One might expect a version of the Theorem 2 without the requirement to have an eigenvector base. In fact, the ability to test subgroup membership (and hence solve DVDP) is essentially implicit in the statement of co-DDH: How does one know that $S, aS \in G_1$ and $T, T' \in G_2$? What is the behaviour of a co-DDH oracle if any of these conditions does not hold?

3 Existence of distortion eigenvector bases

We have shown that VDP is equivalent to CDH when G has an distortion eigenvector base. The goal of this section is to show that all the supersingular elliptic curves used in practice have a distortion eigenvector basis. The restriction to "curves used in practice" is because for the case of elliptic curves over $\mathbb{F}_p$ we use an algorithm from [14] whose complexity is exponential in the class number h of the CM field $\mathbb{Q}(\sqrt{t^2 - 4p})$. Although this algorithm has exponential complexity in general, it has polynomial complexity if the class number is bounded by a polynomial in $\log(p)$ (for the purposes of this paper let's insist that $h \leq \log(p)^2$).

Hence the algorithm runs in polynomial time for all curves which can be constructed in polynomial time using the CM method (which is all supersingular curves used in practice).[3] See [14] for more discussion of this issue.

We summarise some standard examples of supersingular elliptic curves and distortion maps ϕ in Table 1. The triple $(\alpha_1, \alpha_2, \alpha_3)$ in the table means that for $S \in E(\mathbb{F}_q)$ and π the q-power Frobenius map we have $\pi(S) = \alpha_1 S$ and $\pi(\phi(S)) = \alpha_2 S + \alpha_3 \phi(S)$ (this is the notation of Yoshida [23]). We can obtain from the table the maps ϕ_1 and ϕ_2 required in Definition 6. Specifically, for the first row of Table 1 one can take $\phi_1 = m + \phi$ where m is defined to be $2^{-1} \pmod{r}$ as in Proposition 3. One then takes $\phi_2 = m + \phi^2$ and it follows (compare the techniques in Theorem 4) that $d \equiv m^2 - m + 1 \pmod{r}$, where d is such that $\phi_2(\phi_1(S)) = dS$. For the last row take $\phi_1 = \phi$ and $\phi_2(x, y) = ((x/\gamma^2)^p, (y/u)^p)$ (so $d = 1$) and for the other three entries one can take $\phi_1 = \phi_2 = \phi$ (so $d = -1$). This shows that all the elliptic curves in Table 1 have a distortion eigenvector base.

E	q	k	$\phi(x,y)$	$(\alpha_1, \alpha_2, \alpha_3)$
$y^2 = x^3 + 1$	p $p \equiv 2 \pmod{3}$	2	$(\zeta_3 x, y)$ where $\zeta_3^2 + \zeta_3 + 1 = 0$	$(1, -1, -1)$
$y^2 = x^3 + x$	p $p \equiv 3 \pmod{4}$	2	$(-x, iy)$ where $i^2 = -1$	$(1, 0, -1)$
$y^2 + y = x^3 + x + b$	2^m $\gcd(m, 2) = 1$	4	$(x + \zeta_3^2, y + \zeta_3 x + t)$ $\zeta_3^2 + \zeta_3 + 1 = 0, t^2 + t = \zeta_3$	$(1, 0, -1)$
$y^2 = x^3 - x + b$	3^m $\gcd(m, 6) = 1$	6	$(\rho - x, iy)$ where $\rho^3 - \rho = b, i^2 = -1$	$(1, 0, -1)$
$y^2 = x^3 + A$ where $A \in \mathbb{F}_{p^2}$ is a square but not a cube	p^2 $p \equiv 2 \pmod{3}$	3	$(\gamma^2 x^p, u y^p)$ where $u^2 = A/A^q$, $u \in \mathbb{F}_{p^2}$ $\gamma^3 = u$, $\gamma \in \mathbb{F}_{p^6}$	$(1, 0, \lambda)$ where $\lambda^2 + \lambda + 1 \equiv 0 \pmod{r}$

Table 1. Suitable elliptic curves for the Yoshida conditions

A corollary of Theorem 3 below is that for every supersingular elliptic curve used in practice there are (P, ϕ, F) satisfying the Yoshida conditions. Recall that Duursma and Kiyavash showed that if E is an elliptic curve over a finite field with a point P and maps ϕ, F which satisfy the Yoshida conditions (see Section 4 below) then E is supersingular. Hence our corollary gives a complete classification of elliptic curves used in practice satisfying the Yoshida conditions.

The restriction to supersingular curves is not surprising: If E is an elliptic curve with a distortion eigenvector base and if F and the group homomorphisms ϕ_1, ϕ_2 are endomorphisms of the elliptic curve, then E must be supersingular (F and ϕ_1 do not commute, so the endomorphism ring is non-commutative).

The case of embedding degree 1 is more subtle. Frobenius acts as the identity, so for an eigenvector base one must take F to be an endomorphism which is not in $\mathbb{Z}[\pi]$ (where π is the q-power Frobenius) but which has (at least) two eigenspaces. Such endomorphisms may or may not exist (see Charles [7]). Distortion eigenvector bases do not exist when $k = 1$ since a further endomorphism is required which does not commute with F or π, and for elliptic curves there can be no such maps.

We begin with three lemmas to deal with the case of embedding degree 3 (i.e., $r \mid \#E(\mathbb{F}_q)$ has $r \mid (q^3 - 1)$). For background in this section see [4, 8, 19]

Lemma 6. *Let E be an elliptic curve over $\mathbb{F}_{q^2}$ with $\#E(\mathbb{F}_{q^2}) = q^2 \pm q + 1$. Then $j(E) = 0$.*

Proof. Let π be the q^2-power Frobenius map, which has degree q^2 and is purely inseparable. Since E is supersingular (q divides the trace of Frobenius) it follows that $[q]$ is also purely inseparable of degree q^2.

[3] One can construct E such that $\mathrm{End}(E)$ is not the maximal order in $\mathbb{Q}(\sqrt{t^2 - 4p})$. However, one can use isogenies to reduce to the case where $\mathrm{End}(E)$ is maximal, so throughout the paper we assume this is the case.

Therefore (see Silverman [19] Corollary II.2.12), $[q] = \phi\pi$ where $\phi \in \mathrm{End}(E)$. Taking degrees implies that $\deg(\phi) = 1$ and, since π and $[q]$ are defined over $\mathbb{F}_{q^2}$, it follows that ϕ is also defined over $\mathbb{F}_{q^2}$ and so $\pi\phi = \phi\pi$.

Substituting $q = \phi\pi$ into the characteristic polynomial of Frobenius gives

$$0 = \pi^2 \pm q\pi + q^2 = (\phi^2 \pm \phi + 1)\pi^2$$

and hence the automorphism ϕ satisfies $\phi^2 \pm \phi + 1 = 0$. It follows that $\pm\phi \in \mathrm{End}(E)$ is an automorphism of order 3. This implies (see [19] Theorem III.10.1) that $j(E) = 0$. □

Lemma 7. *Let $E_A : y^2 = x^3 + A$ be an elliptic curve over $\mathbb{F}_{q^2}$ with $q = p^m$ such that $p > 3$. Then $\#E_A(\mathbb{F}_{q^2}) = q^2 \pm q + 1$ if and only if $p \equiv 2 \pmod 3$ and A is not a cube.*

Proof. It is a standard fact [19] that E is supersingular if and only if $p \equiv 2 \pmod 3$. Let g be a primitive element of $\mathbb{F}_{q^2}$. Then E_A is isomorphic over $\mathbb{F}_{p^2}$ to one of the curves $E_{g^i} : y^2 = x^3 + g^i$ for $0 \le i < 6$. We will determine which of these curves has $q^2 \pm q + 1$ points.

It is easy to check that $E_1 : y^2 = x^3 + 1$ over $\mathbb{F}_q$ has $q + 1 = p^m + 1$ points if m is odd, $(p^d + 1)^2$ points if $m = 2d$ where d is odd, and $(p^d - 1)^2$ points if $m = 2d$ where d is even. Hence the characteristic polynomial of Frobenius over $\mathbb{F}_{q^2}$ is $(T \pm q)^2$ and $\#E_1(\mathbb{F}_{q^2}) = (q \pm 1)^2$. The quadratic twist $E_{g^3} : y^2 = x^3 + g^3$ has $(q \mp 1)^2$ points over $\mathbb{F}_{q^2}$.

We consider $E_g : y^2 = x^3 + g$ over $\mathbb{F}_{q^2}$. Let $\phi : E_g \to E_1$ be the isomorphism $\phi(x, y) = (\alpha x, \beta y)$ where $\alpha \in \mathbb{F}_{q^6}$ and $\beta \in \mathbb{F}_{q^4}$ satisfy $\alpha^3 = g$ and $\beta^2 = g$. Let π be the q^2-power Frobenius on E_g and π' be the q^2-power Frobenius on E_1. Then $\pi' = \mp[q]$ and so $\phi^{-1}\pi'\phi = \mp[q]$. Now $q^2 \equiv 1 \pmod 3$ so

$$\phi^{-1}\pi'\phi(x, y) = \phi^{-1}(\alpha^{q^2} x^{q^2}, \beta^{q^2} y^{q^2}) = \phi^{-1}(\zeta_3 \alpha x^{q^2}, -\beta y^{q^2}) = -\zeta_3\pi(x, y)$$

where $\zeta_3(x, y) = (\zeta_3 x, y)$. It follows that π satisfies $T^2 \pm qT + q^2 = 0$ and so $\#E_g(\mathbb{F}_{q^2}) = q^2 \pm q + 1$.

We now deal with the remaining cases. Since $p \equiv 5 \pmod 6$ it follows that E_{g^5} is isomorphic to the Galois conjugate $y^2 = x^3 + g^p$ of E_g, and so it also has $q^2 \pm q + 1$ points. The quadratic twists $y^2 = x^3 + g^4$ and $y^2 = x^3 + g^2$ therefore also have $q^2 \mp q + 1$ points. □

Lemma 8. *Let E be a supersingular elliptic curve over $\mathbb{F}_q$ (characteristic > 3). Let $r \mid \#E(\mathbb{F}_q)$ with $r > 3$ have security parameter $3/2$ or 3. Then there is a distortion map ϕ on E, with easily computed inverse, such that if $P \in E(\mathbb{F}_q)[r]$ then $\phi(P) \in E(\mathbb{F}_{q^3})[r]$ is a q-power Frobenius eigenvector with eigenvalue q.*

Proof. Let π be the q-power Frobenius. Then security parameter $3/2$ or 3 implies that π satisfies $\pi^2 \pm q\pi + q = 0$. Waterhouse [21] implies $q = p^{2m}$ where $p \equiv 2 \pmod 3$. Hence, by Lemma 6, E is of the form $y^2 = x^3 + A$. Further, by Lemma 7, E is of the form $y^2 = x^3 + A$ where $A \in \mathbb{F}_{q^2}$ is not a cube.

We now define a distortion map on E. Note that A may or may not be a square, but in either case A/A^q is a square. Denote by u a square root of A/A^q, and note that u is not a cube. Let $\gamma \in \mathbb{F}_{q^6}$ satisfy $\gamma^3 = u$ and note that $\gamma^{q^2} = \zeta_3\gamma$ for $\zeta_3 \in \mathbb{F}_{q^2}$ such that $\zeta_3^2 + \zeta_3 + 1 = 0$.

Define

$$\phi(x, y) = (\gamma^2 x^q, u y^q).$$

One can check that if $P \in E(\mathbb{F}_{q^2})$ then $\phi(P) \in E(\mathbb{F}_{q^6})$. Clearly ϕ and ϕ^{-1} are easily computed.

It remains to prove that $\phi(P)$ is a Frobenius eigenvector, which we do in two stages. Let $P \in E(\mathbb{F}_{q^2})[r]$, let $Q \in E(\mathbb{F}_{q^6})[r]$ be a non-trivial point in the q-eigenspace of Frobenius, and let π be the q^2-power Frobenius on E. Then

$$\pi\phi(P) = (\gamma^{2q^2} x_P^{q^3}, u^{q^2} y_P^{q^3}) = ((\gamma^{q^2})^2 x_P^q, u y_P^q).$$

Since $\gamma^{q^2} = \zeta_3\gamma$ we get

$$\pi\phi(P) = \zeta_3^2\phi(P) \qquad (4)$$

where $\zeta_3(x, y) = (\zeta_3 x, y)$ and $\zeta_3^2(x, y) = \zeta_3 \circ \zeta_3(x, y) = (\zeta_3^2 x, y)$. Note that $(\zeta_3^2 + \zeta_3 + 1)(R) = 0$ for all $R \in E(\overline{\mathbb{F}}_q)$. In particular, $(\zeta_3^2 + \zeta_3 + 1)(Q) = 0$.

We now show that $\zeta_3\phi(P)$ is an integer multiple of $\phi(P)$. First note that $r \mid (q^2 \pm q + 1)$ and so $q^4 + q^2 + 1 \equiv 0 \pmod{r}$. Also note that ζ_3 is defined over $\mathbb{F}_{q^2}$ so $\pi\zeta_3 = \zeta_3\pi$. Hence, equation (4) implies

$$(\pi^2 + \pi + 1)(\phi(P)) = (\zeta_3^2 + \zeta_3 + 1)(\phi(P)) = 0.$$

Write $\phi(P) = aP + bQ$ with $0 \leq a, b < r$. Then

$$0 = (\pi^2 + \pi + 1)(\phi(P)) = a(\pi^2 + \pi + 1)(P) + b(\pi^2 + \pi + 1)(Q) = 3aP$$

which implies $a = 0$ as $r > 3$. It follows that $\phi(P) \in \langle Q \rangle$ and $\zeta_3\phi(P) \in \langle Q \rangle$. □

Theorem 3. *Let E be a supersingular elliptic curve over a finite field $\mathbb{F}_q$ suitable for pairing-based cryptography (i.e., with embedding degree $2 \leq k \leq 6$ and such that the class number of the field $\mathbb{Q}(\sqrt{t^2 - 4q})$ is at most $\log(q)^2$). Let $r > 3$ be prime and coprime to q. Suppose that $r \mid \#E(\mathbb{F}_q)$ and that not all points in $E[r]$ are defined over $\mathbb{F}_q$. Let k be the smallest positive integer such that $r \mid (q^k - 1)$. Let π be the q-power Frobenius map. Then $E[r]$ has a distortion eigenvector basis with respect to $F = \pi$.*

Proof. Let π be the q-power Frobenius. Since $r \mid \#E(\mathbb{F}_q)$ and $E[r] \not\subseteq E(\mathbb{F}_q)$ it follows from Balasubramanian and Koblitz [1] that $k > 1$. Hence $q \not\equiv 1 \pmod{r}$. Furthermore, $E[r]$ has a basis $\{P, Q\}$ such that $\pi(P) = P$ (i.e., $P \in E(\mathbb{F}_q)$) and $\pi(Q) = qQ$. It remains to prove the existence of a homomorphism $\phi : \langle P \rangle \to \langle Q \rangle$ for which ϕ and ϕ^{-1} can be computed in polynomial time.

In characteristic 2, there are only finitely many $\mathbb{F}_q$-isomorphism classes of supersingular elliptic curves and we have $k \leq 4$ (see Menezes [18]). For applications we take $k = 4$, in which case we may assume that E is the elliptic curve

$$E : y^2 + y = x^3 + x + b$$

over $\mathbb{F}_{2^m}$ where $b = 0$ or 1 and m is odd. The field $\mathbb{F}_{2^{4m}}$ has elements s, t such that $s^2 = s + 1$ and $t^2 = t + s$. Following [3] we consider the distortion map $\phi(x, y) = (x + s^2, y + sx + t)$. Note that ϕ and ϕ^{-1} are easily computed. It is immediate that if $P \in E(\mathbb{F}_{2^m})$ then $\pi^2(\phi(P)) = -\phi(P)$. Hence, $(P, \phi(P))$ is a distortion eigenvector base with respect to $F = \pi^2$.

To prove the result for $F = \pi$ suppose $\pi(\phi(P)) = aP + b\phi(P)$ for some $0 \leq a, b < r$. Then $-\phi(P) = \pi(\pi(\phi(P))) = a(b+1)P + b^2\phi(P)$ and so $a(b+1) \equiv 0 \pmod{r}$ and $b^2 \equiv -1 \pmod{r}$. It follows that $a = 0$ and $\phi(P)$ is an eigenvector for Frobenius (with eigenvalue $\pm q \pmod{r}$).

In characteristic 3, there are also only finitely many $\mathbb{F}_q$-isomorphism classes of supersingular elliptic curves and we have $k \leq 6$. For cryptographic applications we take $k = 6$ and so we may assume that

$$E : y^2 = x^3 - x + b$$

over $\mathbb{F}_{3^m}$ where $b = \pm 1$ and $\gcd(m, 6) = 1$. We consider the distortion map $\phi(x, y) = (\rho - x, \sigma y)$ where $\sigma, \rho \in \mathbb{F}_{3^6}$ satisfy $\sigma^2 = -1$ and $\rho^3 = \rho + b$. It is easy to check that if $P \in E(\mathbb{F}_{3^m})$ and if π is the 3^m-power Frobenius then $\pi^3(\phi(P)) = -\phi(P)$ so $(P, \phi(P))$ is a distortion eigenvector base with respect to $F = \pi^3$. The result also follows for $F = \pi$ using the same method as used in the case of characteristic 2: write $\pi(\phi(P)) = aP + b\phi(P)$, then $-\phi(P) = \pi^3(\phi(P)) = a(b^2 + b + 1)P + b^3\phi(P)$ and so $a = 0$ and $b \equiv q \pmod{r}$.

The case $k = 3$ is of interest when $p > 3$ satisfies $p \equiv 2 \pmod{3}$. The result is proved in Lemma 8.

Finally, we consider the case $k = 2$. Galbraith and Rotger [14] have given an algorithm to construct a distortion map ϕ for any supersingular elliptic curve E over $\mathbb{F}_q$ where $q = p^m$ with $k = 2$. The running time of the algorithm is polynomial in the running time of the CM method for constructing such an elliptic curve (and all known constructions of elliptic curves for pairing applications have small class number CM). Proposition 6.1 of [14] constructs the distortion map $\phi = \sqrt{-d}$ in $\mathrm{End}(E)$ where d may be taken to be square-free. Then ϕ is an isogeny of degree d which may be computed using Algorithm 1 of [14]. If E has been constructed in polynomial time then we may assume that d is bounded by a polynomial in $\log(p)$ and so this algorithm is polynomial time and it follows that ϕ may be computed in polynomial time.

Similarly, the dual isogeny $\hat{\phi}$ (see [19]) can be computed in polynomial time using an analogous algorithm. Recall that $\hat{\phi}\phi = [d]$.

Finally, the statement that $\phi(P)$ is a Frobenius eigenvector follows from the proof of Proposition 6.1 of [14]. The q-power Frobenius lifts to the Galois element σ in the proof, and ϕ lifts to an endomorphism Φ satisfying $\Phi^\sigma = -\Phi$. This implies $\pi\phi(P) = -\phi(P) = q\phi(P)$ as required. □

A significant case not covered by the above theorem is the non-supersingular genus 2 curves proposed by Duursma and Kiyavash [9]. They consider the curves $y^2 = x^6 - ax^3 + 1$ and $y^2 = x^6 - ax^3 - 3$ over $\mathbb{F}_p$ (where $p \equiv 2 \pmod 3$). Define the isomorphism $\phi(x, y) = (\zeta_3 x, y)$ where $\zeta_3 \in \mathbb{F}_{p^2}$ is a primitive cube root of 1. Note that $\phi^2 + \phi + 1 = 0$ in $\mathrm{End}(\mathrm{Jac}(C))$. Duursma and Kiyavash show that these curves satisfy the Yoshida conditions (see below). In particular, if $S \in \mathrm{Jac}(C)(\mathbb{F}_p)$ is a divisor class of order r and if F is the p-power Frobenius then $F(S) = S$ and $F(\phi(S)) = -S - \phi(S)$.

Theorem 4. *Let C be one of the Duursma-Kiyavash curves and let notation be as above. Let $m = 2^{-1} \pmod r$ and define $\phi' = m + \phi$. Then $(S, \phi'(S))$ is a distortion eigenvector base.*

Proof. It is easy to check (see Proposition 3 below) that $F\phi'(S) = -\phi'(S)$. Hence $(S, \phi'(S))$ is an eigenvector base. Note also that ϕ' is an efficiently computable group homomorphism.

To show that $(S, \phi'(S))$ is a distortion eigenvector base it remains to prove that there is an efficiently computable homomorphism ϕ'' such that $\phi''\phi = d$ on $\langle S\rangle$. Consider the dual isogeny

$$\widehat{m + \phi} = m + \widehat{\phi}.$$

Since $\widehat{\phi} = \phi^2$ we have

$$(m + \widehat{\phi})(m + \phi) = m^2 + m(\phi + \widehat{\phi}) + \widehat{\phi}\phi = m^2 - m + 1.$$

Hence, define $d = (m^2 - m + 1) \pmod r$ and $\phi'' = m + \phi^2$ so that ϕ'' is efficiently computable and $\phi''\phi' = d$ on $\langle S\rangle$. □

Corollary 4 can therefore be applied to deduce that VDP is equivalent to CDH for the Duursma-Kiyavash curves.

4 Relation with the Yoshida conditions

Yoshida showed that CDH $\leq$ VDP when certain conditions on G are satisfied. We have shown that CDH $\leq$ VDP when the group G has an eigenvector base. In this section we show that Yoshida's result is a subcase of ours, by showing that if G satisfies the Yoshida conditions then it has an eigenvector base. First we recall the conditions introduced by Yoshida in [23].

Definition 9. *We say that G satisfies the **Yoshida conditions for** $S \in G$ if there exist group isomorphisms $\phi, F : G \to G$ such that:*

1. *ϕ and F can be computed in polynomial time;*
2. *$(S, \phi(S))$ is a base for G*
3. *Constants $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{Z}/r\mathbb{Z}$ are given, such that $\alpha_1\alpha_2\alpha_3 \neq 0$ and*

$$F(S) = \alpha_1 S, \qquad F(\phi(S)) = \alpha_2 S + \alpha_3\phi(S).$$

We remark that we have been unable to find any groups satisfying the Yoshida conditions with $\alpha_1 = \alpha_3$. Indeed, all known examples of groups satisfying the Yoshida conditions are when G is a subgroup of a divisor class group of a curve over $\mathbb{F}_q$, P is an element of prime order r defined over the ground field $\mathbb{F}_q$, F is a Frobenius map and ϕ is a non-$\mathbb{F}_q$-rational endomorphism of the curve. It follows that $\alpha_1 = 1$.

Proposition 3. *If G satisfies the Yoshida conditions for S then one can calculate $T \in G$ such that (S, T) is an eigenvector base.*

Proof. Suppose S, F, ϕ satisfy the Yoshida conditions.

First suppose that $\alpha_1 \neq \alpha_3$. Let $m = (\alpha_3 - \alpha_1)^{-1}\alpha_2 \pmod r$ and let $\phi' = m + \phi$. Then

$$\begin{aligned} F(\phi'(S)) &= F(mS + \phi(S)) = \alpha_1 mS + \alpha_2 S + \alpha_3 \phi(S) \\ &= (\alpha_1 m + \alpha_2 - \alpha_3 m)S + \alpha_3 \phi'(S) \\ &= \alpha_3 \phi'(S). \end{aligned}$$

It follows that $(S, \phi'(S))$ is an eigenvector base.

Now we deal with the case $\alpha_1 = \alpha_3$ (which possibly never occurs in practice). Set $\theta = \alpha_2^{-1} \pmod r$, $\gamma = \alpha_2^{-1}\alpha_1 \pmod r$ and define

$$\psi(R) = \theta F(R) - \gamma R$$

for $R \in G$. It follows that

$$\psi(S) = (\theta\alpha_1 - \gamma)S = 0$$

and

$$\psi(\phi(S)) = \theta\alpha_2 S + (\theta\alpha_3 - \gamma)\phi(S) = S.$$

Consequently, if we take $\psi' = \phi \circ \psi$ we get that $\psi'(S) = 0$ and $\psi'(\phi(S)) = \phi(S)$. That is, ψ' is the projection on $\langle \phi(S) \rangle$ w.r.t. the base $(S, \phi(S))$. So $R - \psi'(R)$ is the projection of R on $\langle S \rangle$ w.r.t. the base $(S, \phi(S))$. Consequently if we take $F'(R) = \lambda_2\psi'(R) + \lambda_1(R - \psi'(R))$ for any distinct non-zero $\lambda_1, \lambda_2 \in \mathbb{Z}/r\mathbb{Z}$ it easily follows that $(S, \phi(S))$ is an eigenvector base for F' and ϕ. □

Note that in many cases the above proof yields a distortion eigenvector base. However, we cannot prove this in all cases since the Yoshida conditions contain no requirement that the dual isogeny of ϕ be efficiently computable.

For completeness we show how to transfrom a distortion eigenvector base to satisfy the Yoshida conditions.

Lemma 9. *Let G be a group with homomorphisms ϕ, F and an eigenvector base $(S, \phi(S))$. Let $\phi' = 1 + \phi$. Then G together with ϕ', F satisfies the Yoshida conditions.*

Proof. Clearly the first two Yoshida conditions hold. For the third, one checks that

$$F(\phi'(S)) = F(S + \phi(S)) = \lambda_1 S + \lambda_2\phi(S) = (\lambda_1 - \lambda_2)P + \lambda_2\phi'(P)$$

which completes the proof □

Corollary 5. *Let E be any supersingular elliptic curve used in practice as above. Then one can construct a triple (P, F, ϕ) satisfying the Yoshida conditions.*

5 Non-cyclic groups

The VDP is defined for any group G of exponent r and order r^2. In this section we very briefly recall some non-cyclic groups which might be suitable for cryptography. Recall that the main groups of interest in discrete-logarithm based cryptography are the multiplicative group of a finite field (which is always cyclic) and elliptic curves or divisor class groups of curves (which can be non-cyclic). For background on elliptic curves in cryptography (and pairings) see [4, 8].

1. Direct products $G = G_1 \times G_2$ where G_1, G_2 are cyclic subgroups of finite fields, elliptic curves or divisor class groups.
2. Elliptic curves E over $\mathbb{F}_q$ such that the group of points of order r (called the r-torsion subgroup) is defined over a small degree extension $\mathbb{F}_{q^k}$. Such curves are automatically 'pairing-friendly'. There are two cases:
   (a) Supersingular curves.

   (b) Ordinary curves. There are many methods to generate pairing-friendly ordinary curves (see [11] for a survey).

3. Subgroups of exponent r and order r^2 of the divisor class group of a curve of genus $g \geq 2$ over $\mathbb{F}_{q^k}$. In this case, the full r-torsion is not necessarily defined over $\mathbb{F}_{q^k}$ and so the divisor class group is not necessarily pairing-friendly. Again, there are two cases.
   (a) Supersingular. These curves are necessarily pairing-friendly. There are many examples of supersingular hyperelliptic curves given in the literature (see [13]).
   (b) Non-supersingular. For example the curves with complex multiplication presented by Duursma and Kiyavash [9].
4. The subgroup of order r^2 in $(\mathbb{Z}/n\mathbb{Z})^*$ where $n = pq$ is a product of two primes such that $r \mid (p-1)$ and $r \mid (q-1)$. Care must be taken that r is not too large, or else it is easy to factor n (see McKee and Pinch [17]).
   This case has a very different flavour to the other groups described above, and the methods of the paper do not seem to apply in this case.

Note that not all of the above groups will necessarily have an eigenvector base.

6 Generalised discrete logarithm problems

We have proved that VDP is equivalent to CDH in a cyclic group for all examples proposed in the literature. But one might consider VDP in a more general context where distortion maps ϕ are not available. Hence we give some results relating VDP to generalisations of the discrete logarithm problem. As always, G denotes a group of order r^2 and exponent r where r is prime.

We recall the discrete logarithm problem (DLP$_{G_1}$) for a cyclic group G_1: Given $P, Q \in G_1$, compute an integer a (if it exists) such that $Q = aP$. The discrete logarithm problem has been generalized by many authors in different ways. For example, if G_1 is a cyclic group of prime order and $P_1, P_2 \in G_1$ then Brands [6] defined the **representation problem:** Given $Q \in G_1$ find (a, b) such that $Q = aP_1 + bP_2$. It is easy to show that the the representation problem in the cyclic group G_1 is equivalent to the DLP in G_1.

For groups G of exponent r and order r^2 we define the following generalisation of the discrete logarithm problem.

Definition 10. *The computational problem **2-DL** is: Given $P_1, P_2, Q \in G$ such that $G = \langle P_1, P_2 \rangle$ compute a pair of integers (a, b) such that $Q = aP_1 + bP_2$.*

The following result is natural, but we include it for completeness.

Lemma 10. *The computational problem 2-DL is random self-reducible.*

Proof. Let (P_1, P_2, Q) be a 2-DL instance where $Q = aP_1 + bP_2$. Choose uniformly at random $x_1, x_2, y_1, y_2 \in (\mathbb{Z}/r\mathbb{Z})$ such that $x_1x_2 - y_1y_2 \not\equiv 0 \pmod r$ and define $P_1' = x_1P_1 + y_1P_2$, $P_2' = y_2P_1 + x_2P_2$. Then $G = \langle P_1', P_2' \rangle$ and every pair of generators for G can be obtained from $\{P_1, P_2\}$ via the above process. Let $u_1, u_2 \in \mathbb{Z}/r\mathbb{Z}$ be chosen uniformly at random. Then $(P_1', P_2', Q + u_1P_1' + u_2P_2')$ is a random 2-DL instance.

Given the solution (a'', b'') to this 2-DL instance one can compute $a' = a'' - u_1, b' = b'' - u_2$ so that

$$Q = a'P_1' + b'P_2' = (a'x_1 + b'y_2)P_1 + (a'y_1 + b'x_2)P_2$$

which gives the solution to the original 2-DL problem. □

Lemma 11. *Let G_1 be a cyclic subgroup of G. Then DLP$_{G_1}$ $\leq$ 2-DL.*

Proof. Clearly a DLP instance (P, aP) leads to a 2-DL instance (P, Q, aP) for any random point $Q \notin \langle P \rangle$. Applying Lemma 10, if one has an oracle to solve 2-DL with probability ϵ then one can solve DLP$_{G_1}$ with probability ϵ. □

The following result is clear.

Theorem 5. *Let G be as above. Then VDP $\leq$ 2-DL.*

Proof. Given an input VDP triple (P_1, P_2, Q) we call the 2-DL oracle to get (a, b). Then $R = aP_1$ (which can be computed in polynomial time since the group operation in G may be computed in polynomial time) is the solution to the VDP.

If the 2-DL oracle has success probability ϵ then, by applying Lemma 10, one has solved VDP with probability ϵ. □

The computational problems VDP and 2-DL are both defined for non-cyclic groups. Computational problems in non-cyclic groups have not been studied as closely as those in cyclic groups. The remainder of this section relates the 2-DL problem in non-cyclic groups to discrete logarithm problems in one or more cyclic groups.

Let G_1, G_2 be cyclic groups of order r. We say that two group homomorphisms $\psi_i : G \to G_i$, for $i = 1, 2$, are **independent** if $\ker \psi_1 \cap \ker \psi_2 = \{0\}$. An example of independent group homomorphisms are the projection maps in the proof of Proposition 1.

Theorem 6. *Let G and G_1 be as above and suppose there are two independent group homomorphisms $\psi_1, \psi_2 : G \to G_1$ which can be computed in polynomial time. Then 2-DL is equivalent to DLP$_{G_1}$.*

This result is a special case of the following.

Theorem 7. *Let G be as above and let G_1, G_2 be cyclic groups of order r. Suppose there are two independent group homomorphisms $\psi_i : G \to G_i$ for $i = 1, 2$ which can be computed in polynomial time. Then 2-DL is equivalent to (DLP$_{G_1}$ and DLP$_{G_2}$).*

Proof. It is trivial from Lemma 11 that (DLP$_{G_1}$ and DLP$_{G_2}$) $\leq$ 2-DL. We now prove the opposite (the ideas in the proof are essentially the same as those used in the proof of Theorem 1.)

Let (P_1, P_2, Q) be the input 2-DL and suppose we have oracles O_1, O_2 which solve the DLP in G_1 and G_2 respectively. Fix a generator R_1 for G_1 and a generator R_2 for G_2.

Using O_1 and O_2 we can compute integers $m_{i,j}$ for $1 \leq i, j \leq 2$ such that

$$\psi_i(P_j) = m_{i,j} R_i.$$

Write M for the 2×2 matrix $(m_{i,j})$. Then for $Q = aP_1 + bP_2$ we have

$$\begin{pmatrix} \psi_1(Q) \\ \psi_2(Q) \end{pmatrix} = M \begin{pmatrix} aR_1 \\ bR_2 \end{pmatrix}.$$

The fact that ψ_1 and ψ_2 are independent is equivalent to M being invertible.

To solve the 2-DL we call O_1 on $\psi_1(Q)$ and O_2 on $\psi_2(Q)$ to find integers (x, y) such that $\psi_1(Q) = xR_1$ and $\psi_2(Q) = yR_2$. Then

$$\begin{pmatrix} x \\ y \end{pmatrix} = M \begin{pmatrix} a \\ b \end{pmatrix}$$

and one can solve for (a, b) thus solving the 2-DL. □

Corollary 6. *If G has an eigenvector base (S, T) then 2-DL is equivalent to (DLP$_{\langle S \rangle}$ and DLP$_{\langle T \rangle}$).*

Corollary 7. *Let G be a group which has a distortion eigenvector base (S, T). Let $G_1 = \langle S \rangle$. Then 2-DL is equivalent to DLP$_{G_1}$.*

Proof. We let ψ_1 be as in the proof of Proposition 1 and let $\psi_2(Q) = \psi_1(\phi(Q))$. One can check that these are independent homomorphisms to $\langle S \rangle$, and so the result follows from Theorem 6. □

Direct products (case 1 of Section 5) are easy to handle.

Corollary 8. *Let G be a direct product of two cyclic groups G_1, G_2 of prime order r. Then 2-DL $\leq$ (DLP$_{G_1}$ and DLP$_{G_2}$).*

Proof. Let $G = G_1 \times G_2$. The homomorphisms $\psi_i : G \to G_i$ are given by $\psi_1(R_1, R_2) = R_i$ for $i = 1, 2$. Theorem 7 then proves the result. □

On ordinary pairing-friendly elliptic curves (i.e., case 2(b) of Section 5) we do not have distortion maps and so it is not possible to have a distortion eigenvector base. We now state the obvious fact that the 2-DL can be reduced to the DLP in a finite field using pairings.

Theorem 8. *Let G be a subgroup of $E(\mathbb{F}_{q^k})$ of exponent r and order r^2. Then $r \mid (q^k - 1)$. Let G_1 be the subgroup of r-th roots of unity in $\mathbb{F}_{q^k}^*$. Then 2-DL $\leq$ DLP$_{G_1}$.*

Proof. The proof uses the Weil pairing, which is a non-degenerate, bilinear map $e_r : E[r] \times E[r] \to \mu_r$ where μ_r is the group of rth roots of unity in $\overline{\mathbb{F}}_q$. The Weil pairing is alternating, which means $e_r(P, P) = 1$ for all points $P \in E[r]$.

First, the statement $r \mid (q^k - 1)$ follows from non-degeneracy of the Weil pairing on $E[r] \subset E(\mathbb{F}_{q^k})$.

Now, let (P_1, P_2, Q) be the 2-DL instance we are required to solve. Since $\{P_1, P_2\}$ generates $E[r]$ and the Weil pairing is non-degenerate and alternating we have $g = e_r(P_1, P_2) \neq 1$. One can appeal to Theorem 6 to give the result, but it is obtained even more directly as follows. Write $Q = aP_1 + bP_2$. To solve the 2-DL one computes the Weil pairing values $e_r(Q, P_2) = g^a$ and $e_r(P_1, Q) = g^b$. By solving the two DLPs in G_1 one obtains (a, b), which is the solution to the 2-DL problem. □

In the ordinary genus 2 case (again, case 3(b) of Section 5) there is another way to potentially attack the 2-DL. One natural approach to constructing a curve C over $\mathbb{F}_q$ whose Jacobian has non-cyclic group order is to choose C such that there are rational maps $\psi_i : C \to E_i$ (for $i = 1, 2$) over $\mathbb{F}_q$ where E_i are elliptic curves over $\mathbb{F}_q$. Then the Jacobian of C is isogenous over $\mathbb{F}_q$ to $E_1 \times E_2$ and if $r \mid \#E_i(\mathbb{F}_q)$ for $i = 1, 2$ then r^2 divides the order of $\mathrm{Jac}(C)(\mathbb{F}_q)$. This approach was used by Duursma and Kiyavash [9]. Since the rational maps ψ_i induce explicit isogenies

$$\psi_i : \mathrm{Jac}(C)(\mathbb{F}_q) \to E_i(\mathbb{F}_q)$$

for $i = 1, 2$ one can apply Theorem 7 to reduce the 2-DL to two DLPs in cyclic groups.

7 Conclusion

We present a thorough analysis of the vector decomposition problem (VDP). We have shown that, for all the supersingular elliptic curves which could be used in practice, VDP is equivalent to CDH in a cyclic group. We have also related VDP to various co-CDH problems and a generalised discrete logarithm problem 2-DL which in turn is often related to discrete logarithm problems in cyclic groups.

Acknowledgements

We thank Iwan Duursma, Seung-Kook Park, Maura Paterson and a number of anonymous referees for helpful comments on a much earlier draft of the paper. Takakazu Satoh is thanked for proof reading. Galbraith also thanks the Fields Institute in Toronto for providing a stimulating research environment during some of this research and EPSRC Research Grant EP/D069904/1 for financial support.

References

1. R. Balasubramanian and N. Koblitz, The improbability that an elliptic curve has subexponential discrete log problem under the Menezes-Okamoto-Vanstone algorithm, *J. Cryptology*, **11**, no. 2 (1998) 141–145.
2. F. Bao, R. H. Deng and H. Zhu, Variations of Diffie-Hellman Problem, in S. Qing et al (eds.) Information and Communications Security ICICS 2003, Springer LNCS 2836 (2003) 301–312.
3. P. S. L. M. Barreto, H. Y. Kim, B. Lynn, and M. Scott. Efficient algorithms for pairing-based cryptosystems, in M. Yung (ed.), CRYPTO 2002, Springer LNCS 2442 (2002) 354–368.
4. I. Blake, G. Seroussi and N. P. Smart (eds.), *Advances in elliptic curve cryptography*, Cambridge University Press, 2005.
5. D. Boneh, B. Lynn and H. Shacham, Short signatures from the Weil pairing, *Journal of Cryptology*, **7** (2004) 297-319.
6. S. Brands, An efficient off-line electronic cash system based on the representation problem, CWI Technical Report CS-R9323 (1993).
7. D. Charles, On the existence of distortion maps on ordinary elliptic curves, arXiv:math/0603724, 2006.
8. H. Cohen and G. Frey (eds.), Handbook of elliptic and hyperelliptic curve cryptography, CRC Press (2006)
9. I. Duursma and N. Kiyavash, The vector decomposition problem for elliptic and hyperelliptic curves, *J. Ramanujan Math. Soc.*, **20**, No. 1 (2005) 59–76.
10. I. M. Duursma and S. K. Park, ElGamal type signature schemes for n-dimensional vector spaces, eprint 2006/311.
11. D. Freeman, M. Scott and E. Teske, A taxonomy of pairing-friendly elliptic curves, preprint 2006.
12. G. Frey, H.-G. Rück. A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves. *Math. Comp.*, **62** (1994) 865–874.
13. S. D. Galbraith, Supersingular curves in cryptography, in C. Boyd (ed.), ASIACRYPT 2001, Springer LNCS 2248 (2001) 495–513.
14. S. D. Galbraith and V. Rotger, Easy decision Diffie-Hellman groups, *LMS J. Comput. Math.* **7** (2004) 201–218.
15. U. Maurer, Towards the equivalence of breaking the Diffie-Hellman protocol and computing discrete logarithms, in Y. Desmedt (ed.), CRYPTO '94, Springer LNCS 839 (1994) 271–281.
16. U. Maurer and S. Wolf, The relationship between breaking the Diffie-Hellman protocol and computing discrete logarithms, *SIAM Journal on Computing*, **28**, No. 5 (1999) 1689–1721.
17. J.F. McKee and R.G.E. Pinch, Further attacks on server-aided RSA cryptosystems, unpublished manuscript (1998).
18. A. J. Menezes, *Elliptic curve public key cryptosystems*, Springer, 1993.
19. J. H. Silverman, *The arithmetic of elliptic curves*, Springer–Verlag, 1986.
20. E. R. Verheul, Evidence that XTR Is More Secure than Supersingular Elliptic Curve Cryptosystems, J. Cryptology, 17,4, (2004), 277-296.
21. W. C. Waterhouse, Abelian varieties over finite fields, Annales Scientifiques de l'École Normale Supérieure, Sér. 4 (1969).
22. M. Yoshida, S. Mitsunari and T. Fujiwara, Vector decomposition problem and the trapdoor inseparable multiplex transmission scheme based the problem, Proceedings of the 2003 Symposium on Cryptography and Information Security (SCIS), (2003) 491–496.
23. M. Yoshida, Inseparable multiplex transmission using the pairing on elliptic curves and its application to watermarking, in *Proc. Fifth Conference on Algebraic Geometry, Number Theory, Coding Theory and Cryptography*, University of Tokyo, 2003.
   Available from:
   `http://www.math.uiuc.edu/~duursma/pub/yoshida_paper.pdf`