I. INTRODUCTION

Yoshida et al.\cite{1} proposed a new hard problem; that of vector decomposition (VDP). Yoshida proves sufficient conditions for which the VDP on a two-dimensional vector space is at least as hard as the Computational Diffie-Hellman Problem (CDHP) on a one-dimensional subspace. We prove that any elliptic curve for which the sufficient conditions hold is bound to be supersingular. Furthermore we give a family of hyperelliptic curves of genus two that are suitable for the VDP.

Definition 1 The VDP on \( V \) (a two-dimensional vector space over \( F \)) is \(^{\text{"given \( e_1, e_2, v \in V \) such that \( \{e_1, e_2\} \) is an \( F \)-basis for \( V \), find \( u \in V \) such that \( u \in (e_1) \) and \( u \in (e_2) \)^{\text{\prime}}.\) On the other hand, CDHP on \( V \), a one-dimensional vector space, is \(^{\text{"given \( e \in V \) \& \( 0 \) and \( a, b, c \in (e) \), find \( abc \in (e)\)^{\text{\prime}}.}\)

Theorem 1 (Yoshida et al.\cite{1}): The VDP on \( V \) is at least as hard as the CDHP on \( V \) if for any \( e \in V \) there are linear isomorphisms \( \psi, \phi : V \rightarrow V \) which satisfy the following three conditions:

1. For any \( v \in V \), \( \psi(v) \) and \( \phi(v) \) are effectively defined and can be computed in polynomial time.
2. \( \{e, \psi(e), \phi(e)\} \) is an \( F \)-basis for \( V \).
3. There are \( a_1, a_2, a_3 \in F \) with \( \phi(e) = a_1 e + \phi(\psi(e)) = a_2 e + \phi(\psi(e)) \) and \( a_1, a_2, a_3 \neq 0 \). The elements \( a_1, a_2, a_3 \) and their inverses can be calculated in polynomial time.

The conditions stated in the theorem are stronger than what is necessary. Indeed it is enough to have two linear endomorphisms that satisfy the condition stated above. Studying then the endomorphism ring of the curve classifies all the possibilities for the linear endomorphisms \( \psi, \phi : V \rightarrow V \).

II. MAIN RESULTS

Yoshida et al.\cite{1} proposes to choose \( V = E[m] \), the group of \( m \)-torsion points on an elliptic curve, and \( V = E(D) \setminus E[m] \), the subgroup of rational torsion points, where \( m \equiv 2 \pmod{3} \). In other words \( m \) is a prime such that \( 6m = 2 \) and \( E[m] = \{P|mP = 0\} \subset E(D) \). Moreover the map \( \psi \) is chosen to be \( \psi(x, y) = (\zeta x, y) \), where \( \zeta^2 + \zeta + 1 = 0 \) and \( \phi(x, y) = (x^3, y^3) \) is the Frobenius map. But \( E : y^2 = x^3 + 1 \) is supersingular and thus susceptible to the MOV attack. This is not a mere incidence of a bad choice but a general case.

Theorem 2: Any elliptic curve with the two linear endomorphisms \( \psi, \phi : V \rightarrow V \) satisfying the conditions of Theorem 1, where \( V \) is chosen to be \( E[m] \), the group of \( m \)-torsion points, is supersingular.

The difficulty of the vector decomposition problem is based on Theorem 1 above. Thus, the vector decomposition problem is difficult if the Diffie-Hellman problem on a one-dimensional subspace is difficult. If we choose the group \( \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \) as a subgroup of the \( m \)-torsion points in the Jacobian of a higher genus curve then we can avoid the MOV and the Frey-Rück attack \cite{2} and we can satisfy the conditions of Theorem 1 for curves that are not supersingular.

A special case of genus-two curves are those of the form \( y^2 = (x^3 - u^6)(x^3 - v^6) \), where \( u^6 \) and \( v^6 \) are scalars in \( \mathbb{F}_p \). The curves form a one-parameter family in the three-parameter moduli space of genus two curves \cite{3}. The curves in the family have as common properties that the Jacobian of the curve is \( (2,2) \)-isogenous to a product \( E_1 \times E_2 \) of elliptic curves such that \( E_1 \) and \( E_2 \) are \( 3 \)-isogenous. We give the \( j \)-invariants of \( E_1 \) and \( E_2 \).

Lemma 1: The Jacobian of the hyperelliptic curve \( C : y^2 = (x^3 - u^6)(x^3 - v^6) \) is isogenous to a product of elliptic curves \( E_1 \) and \( E_2 \).

\[ E_{1,2} : y^2 = \frac{(a-b)^2 x^3 + (3a-1)^2}{(a-b)^2(a+b)^2} \]

for \( a = u^3, b = \pm v^3 \), respectively.

The isogeny of the elliptic curves \( E_1 \) and \( E_2 \) is defined over an extension of \( \mathbb{F}_p \) that contains the third roots of unity. Over the extension field, both \( E_1 \) and \( E_2 \) have the same number of points.

The setup for the VDP is now as follows. We choose \( C \) starting from an elliptic curve \( E_1 \) that has a large cyclic subgroup \( \mathbb{Z}/m\mathbb{Z} \) of rational points over \( \mathbb{F}_p \), for \( p \equiv 2 \pmod{3} \). Then we choose as two-dimensional vector space \( V \) the \( m \)-torsion \( \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \) in the Jacobian of the hyperelliptic curve \( C : y^2 = (x^3 - u^6)(x^3 - v^6) \) over the extension field \( \mathbb{F}_p \). We choose as one-dimensional subspace \( V \) the subspace \( \mathbb{Z}/m\mathbb{Z} \) of \( V \) that is rational over \( \mathbb{F}_p \). Then the map \( \psi \) is chosen to be \( \psi(x, y) = (\zeta x, y) \) where \( \zeta^2 + \zeta + 1 = 0 \) and \( \phi = (x, y) \) is the Frobenius map.

Theorem 3: Let \( C : y^2 = (x^3 - u^6)(x^3 - v^6) \) be a hyperelliptic curve, and let \( V \) and \( V' \) be vector spaces of dimensions two and one, respectively. For any \( 0 \neq e \in V' \), the two-dimensional vector space \( V \) has a basis \( \{e, \psi(e)\} \) such that \( \phi(e) = e \) and \( \phi(\psi(e)) = -e - \psi(e) \), where \( e = (x, y) \) is a point on the curve over \( \mathbb{F}_p \). Then the VDP on \( V \), with respect to the basis \( \{e, \psi(e)\} \), is at least as hard as the computational Diffie-Hellman problem in \( V' \): \( \text{"given} (e, ae, be) \text{\" compute} ab \).

REFERENCES


\footnote{Supported by Motorola Grant 558910-239016.}