J. Cryptology (2004) OF1–OF20
DOI: 10.1007/s00145-004-0313-x

Journal of
CRYPTOLOGY

Evidence that XTR Is More Secure than Supersingular Elliptic Curve Cryptosystems

Eric R. Verheul
PricewaterhouseCoopers, GRMS Crypto Group,
P.O. Box 85096, 3508 AB Utrecht, The Netherlands
eric.verheul@[nl.pwcglobal.com, ecstr.com]

Communicated by Arjen K. Lenstra

Received 27 January 2003 and revised 26 September 2003
Online publication 30 July 2004

Abstract. We show that finding an efficiently computable injective homomorphism from the XTR subgroup into the group of points over GF(p^2) of a particular type of supersingular elliptic curve is at least as hard as solving the Diffie–Hellman problem in the XTR subgroup. This provides strong evidence for a negative answer to the question posed by Vanstone and Menezes at the Crypto 2000 Rump Session on the possibility of efficiently inverting the MOV embedding into the XTR subgroup. As a side result we show that the Decision Diffie–Hellman problem in the group of points on this type of supersingular elliptic curves is efficiently computable, which provides an example of a group where the Decision Diffie–Hellman problem is simple, while the Diffie-Hellman and discrete logarithm problems are presumably not. So-called distortion maps on groups of points on elliptic curves that play an important role in our cryptanalysis also lead to cryptographic applications of independent interest. These applications are an improvement of Joux's one round protocol for tripartite Diffie–Hellman key exchange and a non-refutable digital signature scheme that supports escrowable encryption. We also discuss the applicability of our methods to general elliptic curves defined over finite fields which includes a classification of elliptic curve groups where distortion maps exist.

Key words. XTR, Decision Diffie–Hellman problem, Supersingular elliptic curves, Inverting MOV embedding, Tripartite Diffie–Hellman key exchange, Escrow.

1. Introduction

XTR is an efficient and compact method to work with order $p^2 - p + 1$ subgroups of the multiplicative group GF(p^6)* of the finite field GF(p^6). It was introduced in [11], followed by several practical improvements in [12] and [13].

Throughout this paper we let $p, l > 3$ denote prime numbers fixed in their context, unless explicitly stated differently. In the context of XTR we further demand that $p \equiv 2 \bmod 3$ and that l divides $p^2 - p + 1$. Let g be a generator of the order l subgroup μ_l of GF(p^6)*. In [11] it is shown that elements of μ_l, the *XTR subgroup*, can be

conveniently represented by their so-called trace over GF(p^2), and it is shown in [11] how this representation can be efficiently computed. Any familiar cryptosystem based on the XTR subgroup (like Diffie–Hellman, ElGamal, DSA) can be easily transformed using this representation, yielding both efficient and compact cryptosystems. Moreover, it is shown in [11] that the security of these transformed systems is equivalent to the ones started with, that is, the security of the discrete logarithm problem in the multiplicative group of the finite field GF(p^6)*. We refer to the group of order $p^2 - p + 1$ of GF(p^6)* as the *XTR supergroup*. It is widely believed that the Diffie–Hellman and discrete logarithm problems in these XTR groups are hard.

At the Crypto 2000 Rump Session [17] the following comparison was presented, suggesting that XTR is nothing other than an elliptic curve cryptosystem in disguise. As is well known, the number of points over GF(p^2) (including the point at infinity) on an elliptic curve defined over GF(p^2) takes the form $p^2 - t + 1$ for some integer called the Frobenius trace number $t \in [-2p, 2p]$. There exist elliptic curves over GF(p^2) of such order equal to $p^2 - p + 1$. These curves are actually characterized in [15] as **C**lass **T**hree supersingular elliptic curves over GF(p^2) with **P**ositive parameter t, namely $t = p$ (as opposed to $t = -p$). This is why we call these curves simply the *CTP curves* for short. Moreover, there exist efficiently computable (i.e., in polynomial time and space in length of input) injective homomorphisms of such curves onto the XTR supergroup. The Menezes–Okamoto–Vanstone (MOV) embedding [16], provides an example of such a homomorphism.

It seems like a plausible hypothesis (see [17]) that the inverses of such homomorphisms might be efficiently computable too. Under this hypothesis the XTR (sub)group is just an instance of an elliptic curve (sub)group and so an attack affecting the security of elliptic curve cryptosystems would affect the security of the XTR cryptosystem. In other words, under this hypothesis the security of XTR cryptosystems is not better than that of elliptic curve cryptosystems.

In this paper, a final version of [21], we show that the hypothesis mentioned above is unlikely to be correct, as we show that under this hypothesis, we can solve several problems that are widely believed to be hard. The Diffie–Hellman problem in the XTR subgroup is an example of such a problem. As a side result we show that the Decision Diffie–Hellman problem in many supersingular elliptic curves is efficiently computable. The results presented in this paper are specifically geared towards XTR, to counter the suggestion that XTR is nothing other than an elliptic curve cryptosystem in disguise. We did not yet succeed in fully generalizing them to other classes of (supersingular) elliptic curves, although we expect they can be (see Section 4). The results in this paper should therefore be interpreted in a broader context. Namely, they provide evidence that the multiplicative group of a finite field provides essentially more, and in any case not less, security than the group of points of a supersingular elliptic curve of comparable size.

The CTP curves take the form $y^2 = x^3 + a$ where $a \in$ GF(p^2) is a square but not a cube in GF(p^2), see [10]. We denote the CTP curves by C_a. Actually, in the category of elliptic curves over GF(p^2) there are only two classes of such curves under efficiently computable isomorphisms. See Lemma 1. The set of points over GF(p^2) (including the point at infinity) on C_a is denoted by C_{a,p^2} and the subgroup thereof of order l is denoted by $C_{a,p^2}[l]$. It is important to consider the elliptic curve $y^2 = x^3 + a$ over the extension field GF(p^6) as well, respectively subgroups of order l therein. These

are denoted respectively by C_{a,p^6} and $C_{a,p^6}[l]$. For further reference, we formulate the hypothesis mentioned above as follows:

X2C There exists an efficiently computable element $s \in \mathrm{GF}(p^2)$ and an efficiently computable injective group homomorphism from the XTR subgroup into $C_{s,p^2}[l]$.

We make some remarks on the hypothesis **X2C**. First, as formulated **X2C** refers to specific prime numbers p, l satisfying certain conditions. So it is more correct to use the notation **X2C**(p, l) instead of simply **X2C**. As we have stated above the prime numbers p, l are considered fixed in its specific context, so we use the somewhat sloppy notation **X2C**. Second, an injective group homomorphism h from the XTR subgroup into $C_{s,p^2}[l]$ is called *efficiently computable* if images under h of arbitrary elements in the XTR subgroup can be efficiently computed. Note that as both the XTR subgroup and its image under h are cyclic groups, any homomorphism can be given by mapping a generator from the domain to a generator in the image. A homomorphism defined this way is efficiently computable if the discrete logarithm problem in the XTR subgroup is efficiently computable. This example also illustrates that "arbitrary" cannot be replaced by "random" in the above definition. Finally, a problem similar to **X2C** is posed by Koblitz on p.328 of [9]. Note that **X2C** seems weaker than only assuming that (a restriction of) an MOV embedding is efficiently invertible. It turns out that that both statements are equivalent. See Theorem 4.

Outline of the paper

In Section 2 we explore the structure of CTP curves. We introduce a so-called distortion map on CTP curves which is of crucial importance for our results, and we prove a more convenient formulation of the **X2C** hypothesis. In Section 3 we present and prove our main results and in Section 4 we discuss some possible extensions of our results also leading to some interesting questions for further research. In Section 5 we discuss some practical applications of distortion maps, including a more computational and communicational efficient variant of the one round protocol for tripartite Diffie–Hellman key exchange described in [6] and a non-refutable digital signature scheme that supports escrowable encryption. Finally, we summarize our results in Section 6.

2. Group Isomorphisms between CTP Curves

We recall that any isomorphism between two elliptic curves defined over a field K induces a group isomorphism (isogeny) between the points on the elliptic curves over the algebraic closure $\bar{K}$ of K but not vice versa. See [15] and [19]. This distinction is important in the following lemma. We also recall that any non-zero isogeny is surjective, see Section 4 in Chapter III of [19], and that an isogeny of an elliptic curve to itself is called an endomorphism.

Lemma 1. *Let C_a and C_b be CTP curves* (*in particular, a, b are squares in* $\mathrm{GF}(p^2)$ *but not cubes*), *then the following hold*:

1. *The map* $S\colon C_a \to C_{a^p}\colon (x, y) \to (x^p, y^p)$ *is an injective, efficiently computable isogeny that maps* C_{a,p^2} *to* C_{a^p,p^2}.
2. *The equation* $u^6 = b/a$ *has its solutions in* $\mathrm{GF}(p^6)$ *and for any such solution* u, *the map* $R_u\colon C_a \to C_b\colon (x, y) \to (u^2x, u^3y)$ *is an isomorphism in the category of elliptic curves over* $\mathrm{GF}(p^6)$ *and induces in particular an injective, efficiently computable group isogeny* $C_{a,p^6} \to C_{b,p^6}$.
3. *The map* R_u *is an isomorphism in the category of elliptic curves over* $\mathrm{GF}(p^2)$ *iff* b/a *is a cube in* $\mathrm{GF}(p^2)$.
4. *If* b/a *is not a cube in* $\mathrm{GF}(p^2)$, *then* b/a^p *is a cube in* $\mathrm{GF}(p^2)$. *Also the equation* $w^6 = b/a^p$ *has its solutions in* $\mathrm{GF}(p^2)$ *and for any such solution* w *the composite map* $R_w \circ S$ *is an injective, efficiently computable isogeny that maps* C_{a,p^2} *to* C_{b,p^2}.

Proof. The first part of the lemma is well known and easily verified. That the equation mentioned in the second part of the lemma has a solution in $\mathrm{GF}(p^6)$ follows as b/a is a square in $\mathrm{GF}(p^2)$. The remainder of the second part of the lemma follows for instance from Theorem 2.2 of [15]. The third part also follows from this result combined with the observation that $u^6 = b/a$ has all its solutions u in $\mathrm{GF}(p^2)$ iff b/a is a cube in $\mathrm{GF}(p^2)$. For a proof of the fourth part, let α be a generator of the multiplicative group of $\mathrm{GF}(p^2)$. As $p > 3$ it follows that $p^2 - 1 \equiv 0 \bmod 3$, so the element $x = \alpha^j$ is a cube in $\mathrm{GF}(p^2)^*$ iff j is divisible by three. Now write $a = \alpha^k$ and $b = \alpha^l$. If b/a is not a cube in $\mathrm{GF}(p^2)$, then $k \bmod 3$ and $l \bmod 3$ are different. As $k, l \bmod 3$ are non-zero, it follows from $p \equiv 2 \bmod 3$ that $k \cdot p \bmod 3$ and $l \bmod 3$ are equal. That is, b/a^p is a cube in $\mathrm{GF}(p^2)$. The remainder of the proof of the fourth part of the lemma now follows from the first and third parts. □

From Lemma 1 it follows that the CTP curves split into two equivalence classes under the equivalence relation $C_a \simeq C_b$ iff b/a is a third power in $\mathrm{GF}(p^2)$. From Theorem 3.2 of [15] it follows that there are exactly two isomorphism classes of supersingular elliptic curves over $\mathrm{GF}(p^2)$ of order $p^2 - p + 1$. We conclude that the CTP curves provide a complete representation of such curves.

From the previous result we immediately deduce the following.

Theorem 1. *All CTP groups* C_{a,p^2} *are efficiently computable group isomorphic. Moreover, we can reformulate* **X2C** *as*:

X2C *For each CTP subgroup* $C_{a,p^2}[l]$ *there exists an efficiently computable, injective homomorphism from the XTR subgroup into* $C_{a,p^2}[l]$.

Let C_a be a CTP curve. We recall some facts on elliptic curves which can all be found in [15]. For a divisor l of $p^2 - p + 1$, the *l-torsion group* of C_a is the collection of all points of order dividing l on the curve $y^2 = x^3 + a$ over the algebraic closure of the field $\mathrm{GF}(p^2)$. The torsion group is isomorphic to $\mathbb{Z}/l\mathbb{Z} \times \mathbb{Z}/l\mathbb{Z}$, which is a non-cyclic, abelian group. In addition, as C_a is a so-called Class III supersingular curve, the l-torsion group of C_a is just the collection of all points of order dividing l over $\mathrm{GF}(p^6)$ (including the point at infinity) on the curve $y^2 = x^3 + a$. That is, the l-torsion group of C_a is equal to $C_{a,p^6}[l]$ and is hence a subset of the curve over $\mathrm{GF}(p^6)$.

Before formulating the theorem that is crucial to our results, we need a definition.

Definition 1. Let H be an abelian group, then two elements g_1, g_2 are called independent, provided that $g_1 \notin \langle g_2 \rangle$ and $g_2 \notin \langle g_1 \rangle$.

This definition becomes particularly relevant when the group H is not cyclic itself, which is typically the situation in elliptic curve torsion groups. Before coming to our next result we remark that it is easily verified that the two points in C_{a,p^2} that have a zero first coordinate, augmented with the point at infinity, that is $\{(0, w), (0, -w), \mathcal{O}\}$ with $w^2 = a$, constitutes a subgroup of order 3. We denote this group by G_3.

Theorem 2. *Let C_a be a CTP curve and let $P \neq \mathcal{O}$ be a point on C_{a,p^2}. Then, using the notation from Lemma* 1, *the following hold*:

1. *The equation $u^6 = a/a^p$ has its solutions u in* $\mathrm{GF}(p^6)\backslash\mathrm{GF}(p^2)$ *and for any such solution u, the map D: $C_a \xrightarrow{S} C_{a^p} \xrightarrow{R_u} C_a$ is an injective endomorphism that maps C_{a,p^6} onto itself and which takes the form $(x, y) \to (u^2x^p, u^3y^p)$.*
2. *$\langle P\rangle \cap \langle D(P)\rangle = \mathcal{O}$ if the order of P is not divisible by three and $\langle P\rangle \cap \langle D(P)\rangle = G_3$ otherwise.*
3. *The point P is independent from its image under $D(\cdot)$ iff P has an order different from* 1 *or* 3.

Proof. For a proof of the first part of the theorem, it easily follows (see the proof of Lemma 1) that a/a^p is not a cube in $\mathrm{GF}(p^2)$. Now the proof follows from the last part of Lemma 1. For a proof of the second part of the theorem: the first coordinate of the value (u^2x^p, u^3y^p) under $D(\cdot)$ of a point $Q = (x, y)$ is clearly not an element of $\mathrm{GF}(p^2)$ when x is non-zero. That is, apart from the point at infinity, the only points that can belong to $\langle P\rangle \cap \langle D(P)\rangle$ have a zero first coordinate. As $\langle P\rangle \cap \langle D(P)\rangle$ is a group it is either equal to $\{\mathcal{O}\}$ or G_3. In the latter case it follows that the order of P must be divisible by three. For a proof of the last part, as $D(\cdot)$ is a group automorphism, the orders of P and $D(P)$ coincide. So if these points are dependent it follows from the second part that either P or $D(P)$ is an element of G_3, i.e., of order 1 or 3. □

For convenience we refer to the endomorphism $D(\cdot)$ introduced in Theorem 2 as the *distortion* map. In Fig. 1 a few pages below we have depicted the property of $D(\cdot)$ with $K = \mathrm{GF}(p^2)$ and $K' = \mathrm{GF}(p^6)$. Related to the l-torsion group of C_a, i.e., $C_{a,p^6}[l]$, is the Weil pairing, a function

$$e_l\colon C_{a,p^6}[l] \times C_{a,p^6}[l] \to \mu_l,$$

where μ_l is the subgroup of $\mathrm{GF}(p^6)^*$ of order l. Hence, μ_l is equal to the XTR subgroup. In the setting of supersingular curves, the Weil pairing can be computed efficiently. The Weil pairing satisfies the Identity Rule, i.e., $e_l(P, P) = 1$, and is bilinear. From the latter property it follows that $e_l(a * P, b * Q) = e_l(P, Q)^{ab}$. This formula is particularly useful when $e_l(P, Q)$ is a generator of μ_l, as the map $\langle P\rangle \to \mu_l\colon x \to e_l(x, Q)$ is then a group isomorphism. Actually, this is the MOV embedding mentioned in the Introduction.

We finally mention that two points P, Q in the torsion group $C_{a,p^6}[l]$ are dependent iff $e_l(P, Q) = 1$, see p. 70 of [15].

The following corollary describes the order of a value of the Weil pairing.

Corollary 1. *Let l dividing $p^2 - p + 1$ be a power of a prime number r and let P be a point on C_{a,p^2} of order l. Then, letting $D(\cdot)$ denote the distortion map from Theorem 2, the following hold*:

1. *If $r \neq 3$, then the element $e_l(P, D(P))$ is of order l in* $\mathrm{GF}(p^6)^*$.
2. *If $r = 3$, then the element $e_l(P, D(P))$ is of order at least $l/3$ in* $\mathrm{GF}(p^6)^*$.

Proof. First note that the point $D(P)$ is of order l as $D(\cdot)$ is a group automorphism. For a proof of the first statement, suppose to the contrary that $e_l(P, D(P))^{l/r} = 1$. Then it follows that $e_l(P, l/r \cdot D(P)) = 1$, that is, P and $l/r \cdot D(P)$ are dependent. Hence either, $P \in \langle l/r \cdot D(P)\rangle$ or $l/r \cdot D(P) \in \langle P\rangle$. The first option is ruled out as it implies that the order of P is divisible by l/r. So,

$$l/r \cdot D(P) \in \langle P\rangle \cap \langle D(P)\rangle = \{\mathcal{O}\},$$

where the last equality follows from Theorem 2. That is, $l/r \cdot D(P) = \mathcal{O}$ contradicting that the order of $D(P)$ is equal to l. For a proof of the second statement, we may assume without loss of generality that $l \geq 3^2$. If we assume to the contrary that $e_l(P, D(P))^{l/9} = 1$ and reasoning in a similar way as in the proof of the first part, we conclude that

$$l/9 \cdot D(P) \in \langle P\rangle \cap \langle D(P)\rangle = G_3,$$

where the last equality follows from Theorem 2. This contradicts that the order of $l/9 \cdot D(P)$ is nine. □

3. Hardness of the X2C Hypothesis

Before coming to our main results, we recall some general notions. Let $G = \langle\gamma\rangle$ be any cyclic, multiplicative group of order l, generated by an element γ. The security of the Diffie–Hellman key agreement protocol with respect to γ lies in the *Diffie–Hellman* (DH) problem of computing the values of the function $DH(\gamma^x, \gamma^y) = \gamma^{xy}$. Two other problems are related to the DH problem. The first one is the *Decision Diffie–Hellman* (DDH) problem with respect to γ: given $\alpha, \beta, \delta \in G$ decide whether $\delta = DH(\alpha, \beta)$ or not. The DH problem is at least as difficult as the DDH problem. The second related problem is the *discrete logarithm* (DL) problem in G with respect to γ: given $\alpha = \gamma^x \in G$, with $0 \leq x < l$ then find $x = DL(\alpha)$. The DL problem is at least as difficult as the DH problem. Until recently the following assumption was widely considered true.

Assumption 1. *If the DL problem in G is hard, then so are the DH and DDH problems in G.*

In [6] and [8], examples are provided of groups of points on supersingular elliptic curves where the DL and DH problems are presumably hard, while the DDH problem is

efficiently computable. These results indicate that Assumption 1 is incorrect for groups of points on supersingular elliptic curves and we encounter an example of this kind in Theorem 3. We emphasize however that the results in [6] and [8] are based on the observation that the DDH type of problem in some extensions of supersingular elliptic curves are often efficiently computable using the so-called Weil or Tate pairing (see below).

The results in [6] and [8] do not provide any indication that the DL or DH problems are efficiently computable in the context of supersingular elliptic curves. Moreover, pairings are not known to exist in the context of multiplicative groups of finite fields. Therefore, these results do not provide any indication that Assumption 1 is not true in the context of multiplicative groups of finite fields. We base some of our security discussions on the hypothesis that these assumptions remain valid in that context, see also the remark after Theorem 4. That is, in this paper we use the following assumption that we consider (still) widely accepted.

Assumption 2. *If G is a multiplicative subgroup of a finite field, then the DH and DDH problems in G are hard provided that the DL problem in G is hard.*

We note that with respect to attacks publicly known today, the DL problem in a multiplicative subgroup G of a finite field can be attacked in two ways, see Section 5 of [11]. One can either attack the whole multiplicative group of the minimal finite field surrounding G using the Discrete Logarithm variant of the Number Field Sieve or one can attack the subgroup using Birthday Paradox based methods. This implies that the difficulty of the DL problem in G depends on the size of the minimal surrounding subfield of G and on the size of the maximal prime number dividing the order of G. So both sizes can be easily chosen so that the DL problem in G becomes practically impossible to solve and indeed such choices are required for a secure implementation of XTR.

We use the reasoning in [6] to provide an example indicating that Assumption 1 is not true in the context of CTP supersingular elliptic curves.

Theorem 3. *The DDH problem in any supersingular elliptic curve over* $\mathrm{GF}(p^2)$ *of order* $p^2 - p + 1$ *is efficiently computable.*

Proof. We can restrict ourselves to curves of type C_a. Write $p^2 - p + 1 = t \cdot v$ where t is a power of three and v is relatively prime with three. By virtue of the Pohlig–Hellman algorithm [18], the DDH problem in C_{a,p^2} can be reduced to the DDH problem in the subgroups of order t and v. As one can easily solve the DL problem related to the first subgroup, one can efficiently solve the DDH problem for this subgroup too.

Now, let P be a generator of the subgroup $C_{a,p^2}[v]$ and suppose that points $X = x * P, Y = y * P, Z = z * P$ in $C_{a,p^2}[v]$ are given. To solve the DDH problem in $C_{a,p^2}[v]$, we need to determine whether $z \equiv x * y \bmod v$. By the Identity property of the Weil pairing, its bilinearity and Corollary 1, the Weil pairing $e_v(P, D(P))$ is a vth root of unity of $\mathrm{GF}(p^6)$. So, on the one hand, $e_v(X, D(Y)) = e_v(P, D(P))^{xy}$ and, on the other hand, $e_v(P, D(Z)) = e_v(P, D(P))^z$. That is $z \equiv x * y \bmod v$ iff $e_v(X, D(Y))$ is equal to $e_v(P, D(Z))$, which is an efficiently computable condition. □

There are several cryptographic protocols whose security depends on the difficulty of the DDH problem, like the publicly verifiable voting system in [2] and the Cramer–Shoup [3] public key cryptosystem that is provably secure against adaptive chosen ciphertext attacks. Theorem 3 shows that these protocols should not be based on (CTP) supersingular elliptic curves, even with the "appropriate" key sizes.

The following result shows that the **X2C** hypothesis contradicts Assumption 2 and the remarks following it providing first evidence that this hypothesis is not valid.

Corollary 2. *Under the* **X2C** *hypothesis, the DDH problem in the XTR subgroup is efficiently computable.*

Proof. This follows immediately from Theorem 3. □

Next we show an even stronger consequence of the **X2C** hypothesis, namely that the DH problem in the XTR subgroup is efficiently computable. It is convenient to refer to the DH problem described at the beginning of Section 3 as the *conventional* DH problem and to introduce three variants of this problem. To this end, again let $G = \langle \gamma \rangle$ be any cyclic, multiplicative group of (known) order l, generated by the (known) element γ. Then the *weak DH problem* with respect to γ is the problem of finding any generator κ, such that for all $0 \leq x, y < l$ determining κ^{xy} can be efficiently done on the basis of γ^x and γ^y. That is, κ is only dependent on γ and not on x, y. The *strong DH problem* with respect to γ is the problem of efficiently determining ξ^{xy} on the basis of γ^x and γ^y, for all $0 \leq x, y < l$ and *any* generator ξ of G. Finally, the *DH problem with respect to the group G* is the problem of efficiently determining ξ^{xy} on the basis of α^x and α^y for all $0 \leq x, y < l$ and *any* generators α, ξ of G. Note that this notion is independent of the choice of particular generators of G. For convenience we sometimes call generators of type α *input* generators and those of type ξ *output* generators.

Lemma 2. *In the above context, the weak, conventional and strong DH problem with respect to γ and the DH problem with respect to G are equivalent.*

Proof. We first show the equivalence of the first three problems. Clearly, if one can solve the strong DH problem, one can solve the conventional DH problem. Moreover, if one can solve the conventional DH problem, then by taking $\kappa = \gamma$ one can solve the weak DH problem. To show that these three problems are equivalent, it suffices to show that if one can solve the weak DH problem, one can solve the strong DH problem. To this end, let γ, κ be as described in the definition of the weak DH problem and let ξ be any generator of G. Also, let the function $WDH(\cdot, \cdot)$ be defined by $\kappa^{xy} = WDH(\gamma^x, \gamma^y)$. Then by hypothesis $WDH(\cdot, \cdot)$ is efficiently computable. We only prove the lemma in the case that l is a prime number, which is important to us, and leave the general case to the reader.

We can write $\kappa = \gamma^s$ and $\xi = \gamma^t$ for some $0 \leq s, t < l$, which are unknown. We first claim that we can efficiently compute $\gamma^{(s^n)}$ for any $n \geq 1$. To this end, for any $i \geq 1$ define

$$T(i) = (\gamma^{(s^{i-1})}, \gamma^{(s^i)}).$$

Note that $T(1) = (\gamma, \kappa)$ is efficiently computable. Also note that if $T(i) = (A, B)$ is given, then $T(2i) = (WDH(A, A), WDH(A, B))$ and $T(2i + 1) = (WDH(A, B), WDH(B, B))$. This means that we can compute $T(n)$ in $2 \cdot \log_2(n)$ calls to the function $WDH(\cdot, \cdot)$ using repeated squaring and multiplication (see Algorithm 2.3.7 of [11]). That is, we can efficiently compute $\gamma^{(s^n)}$ for any $n \geq 1$. In particular, we can efficiently compute the element $D = \gamma^{(s^{l-4})}$.

We are now ready to prove that we can solve the strong DH problem with respect to γ. To this end, let $A = \gamma^x$ and $B = \gamma^y$ be given. Then, first,

$$\begin{aligned} E = WDH(D, WDH(A, B)) &= WDH(\gamma^{(s^{l-4})}, WDH(\gamma^x, \gamma^y)) \\ &= WDH(\gamma^{(s^{l-4})}, \kappa^{xy}) \\ &= WDH(\gamma^{(s^{l-4})}, \gamma^{xys}) \\ &= \kappa^{(s^{l-4}xys)} = \kappa^{(xys^{l-3})} \\ &= \gamma^{s(xys^{l-3})} = \gamma^{(xys^{l-2})} \\ &= \gamma^{(xys^{-1})}. \end{aligned}$$

Here we have used that $s^{l-1} \equiv 1 \bmod l$ for any prime number l (i.e., Fermat's little theorem). Now,

$$WDH(E, \xi) = WDH(\gamma^{(xys^{-1})}, \gamma^t) = \kappa^{xys^{-1}t} = \gamma^{s(xyts^{-1})} = \gamma^{xyt} = \xi^{xy}.$$

As we can efficiently compute $E = WDH(D, WDH(A, B))$ and $WDH(E, \xi)$ we can efficiently compute ξ^{xy} on the basis of γ^x and γ^y. That is, we have solved the strong DH problem with respect to γ.

We are left with showing the equivalence between the first three properties mentioned in the lemma and the last one. This comprises of showing that the ability to solve the strong DH problem with respect to γ implies the ability to solve the DH problem with respect to G. To this end, let α, ξ be any generators of G and suppose that α^x, α^y are given for some $0 \leq x, y < l$. Write $\alpha = \gamma^a$ and $\xi = \gamma^t$ for some $0 \leq a, t < l$. First, we can efficiently determine $\gamma^{(a^2)}$ from α, which is a conventional DH problem with respect to γ. Secondly, from the latter result we can efficiently determine $\gamma^{(a^{-2})}$ by using the techniques described above. Finally, from the latter result and ξ, we can efficiently determine $\delta = \gamma^{(a^{-2}t)}$ which is again a conventional DH problem with respect to γ. Now, if we present α^x, α^y to the efficient algorithm solving the strong DH problem with respect to γ and δ it returns $\delta^{(a^2xy)}$ which is equal to $\gamma^{(a^{-2}ta^2xy)} = \gamma^{txy} = \xi^{xy}$. We conclude that we have solved the DH problem with respect to α and ξ. □

Lemma 3. *Let G, Γ be two finite isomorphic, cyclic groups and let $i\colon G \to \Gamma$ and $j\colon \Gamma \to G$ be two efficiently computable, injective homomorphisms. We assume that the order l of G, Γ and a generator for either G or Γ are known. Then the following are equivalent*:

1. *The DH problem is efficiently computable with respect to G.*
2. *The DH problem is efficiently computable with respect to Γ.*

If these hold, then the inverses of $i(\cdot)$ and $j(\cdot)$ are efficiently computable too.

Proof. It easily follows that if one can solve the DH problem in one of G or Γ, then one can solve the weak DH problem in the other one. So the first part of the lemma follows from Lemma 2. For a proof of the second part of the lemma, we show that $i^{-1}(\cdot)$ is efficiently computable by efficiently computing $i^{-1}(\omega)$ for any element ω of Γ. To this end, let g be a generator of G and let $\gamma = i(g)$ and $g_2 = j(\gamma)$. Write $i^{-1}(\omega) = g^x$ and $g_2 = g^b$ for (unknown) $0 \leq b, x < l$. As g is a generator of G it follows that $j(\omega) = j \circ i(i^{-1}(\omega)) = (i^{-1}(\omega))^b = g_2^x$. So by solving the DH problem for $j(\omega)$ and g_2 with respect to g_2 (input generator) and g (output generator) we end up with g^x, i.e., $i^{-1}(\omega)$ as desired. □

The following is one of our main results. It shows that the **X2C** hypothesis contradicts Assumption 2 and the remarks following it providing evidence that this hypothesis is not valid.

Theorem 4. *Under the* **X2C** *hypothesis*, *the following problems are efficiently computable*:

1. *The DH problem in the XTR subgroup of order* l.
2. *The DH problem in the group of points of order* l *on a supersingular elliptic curve over* $\mathrm{GF}(p^2)$ *of order* $p^2 - p + 1$.
3. *Inverting any efficiently computable embedding* (*e.g.*, *based on the MOV embedding*) *from the group of points of order* l *on a supersingular elliptic curve over* $\mathrm{GF}(p^2)$ *of order* $p^2 - p + 1$ *into the XTR subgroup*.

Proof. Suppose that $H(\cdot)$ is an efficiently computable injective homomorphism from the XTR subgroup into some $C_{a,p^2}[l]$. We first prove the first part of the theorem. Consider any generator g of the XTR subgroup. We construct another generator h in the XTR subgroup satisfying the definition of the weak DH problem. To this end, let $h = e_l(H(g), D(H(g)))$ where $e_l(\cdot, \cdot)$ denotes the Weil pairing on the l-torsion group of C_{a,p^2} and $D(\cdot)$ denotes the distortion map from Theorem 2. It also follows from this theorem that the order of h is equal to l.

To break the weak DH problem, with respect to g, h, suppose that $X = g^x, Y = g^y$ are given. Then

$$e_l(H(X), D(H(Y))) = e_l(x * H(g), y * D(H(g))) = e_l(H(g), D(H(g)))^{xy} = h^{xy}.$$

That is, by computing $e_l(H(X), D(H(Y)))$, which can be done efficiently, we have solved the weak DH problem with respect to g, h. The result now follows from Lemma 2. The second and third parts of the theorem follow from the first part and Lemma 3. □

Note that a natural way to break the DDH problem in the XTR group would be by transforming this problem to an isomorphic group of points on a supersingular elliptic curve where the DDH problem is efficiently computable using an efficiently computable embedding. Theorem 4 shows that then the DH problem in the XTR group is also efficiently computable, for which, as said before, no indications exist. The last part of

Theorem 4 states that to prove the validity of the **X2C** hypothesis, one can concentrate on efficiently inverting any MOV embedding into the XTR subgroup.

4. Extensions

4.1. *Other Extension-Field-Based Public Key Systems*

Two other public key cryptosystems exist that are based on the DL problem in the extension field $GF(p^6)^*$, or actually subfields thereof. The LUC cryptosystem [20], [14] is based on the order $p+1$ subgroup of $GF(p^2)^*$. The variant by Gong and Harn [5] of LUC is based on the p^2+p+1 subgroup of $GF(p^3)^*$, where as in the XTR setting $p \equiv 2 \bmod 3$. For both subgroups one can find supersingular elliptic curves (see [15]) and efficiently computable, isomorphisms from these curves onto these subgroups, based on the Weil pairing. That is, for each of the two cryptosystems one can formulate a hypothesis similar to **X2C**. We remark that there do not exist elliptic curves defined over $GF(p^2)$ with $p^2 + p + 1$ or $p^2 - p + 1$ points over $GF(p^2)$ if $p \equiv 1 \bmod 3$, as the number of isomorphism classes is equal to $1 - (-3/p)$ (see Theorem 3.2 of [15]), which is equal to zero if $p \equiv 1 \bmod 3$ and equal to two if $p \equiv 2 \bmod 3$.

With respect to the Gong and Harn variant of LUC, one could call the related curves *CTN curves*: **C**lass **T**hree supersingular elliptic curves defined over $GF(p^2)$ with **N**egative parameter t, namely $t = -p$ (as opposed to $t = p$). Provided $p \equiv 2 \bmod 3$, it follows that these elliptic curves take the form $y^2 = x^3 + a$ where $a \in GF(p^2)$ is neither a square nor a cube in $GF(p^2)$. This means that the difference with CTP curves lies in the fact that a is a quadratic non-residue. However, it is easily seen that this property is not of significance in the proofs in this paper and all results for CTP curves generalize to CTN elliptic curves. More in particular, the map $(x, y) \rightarrow (u^2 x^p, u^3 y^p)$ where u is a solution of $u^6 = a/a^p$ is an appropriate distortion map on these types of curves. As there exists no point on such curves with first coordinates equal to zero, all points different from the point at infinity on the curve over $GF(p^2)$ are mapped to points outside the curve over $GF(p^2)$. It follows that the existence of any efficiently computable, injective homomorphism from the Gong and Harn group in any supersingular elliptic curve over $GF(p^2)$ of order $p^2 + p + 1$ implies that we can solve the DH problem in the Gong and Harn subgroup of $GF(p^3)^*$ as well as in the related elliptic curve group of points. Moreover, it follows that the DDH problem in these elliptic curve groups is always efficiently computable, irrespective of additional hypotheses.

Our techniques do not completely generalize, at least not in a straightforward fashion, to disprove this hypothesis for the LUC cryptosystem. This is partly due to the fact that we are not aware of a full representation of all isomorphism classes of the corresponding supersingular elliptic curves, i.e., curves over $GF(p)$ of trace zero. However, our techniques do generalize to two particular subclasses of such elliptic curves over $GF(p)$, as one can easily find the appropriate distortion maps. These classes of curves and distortion maps are:

1. $y^2 = x^3 - bx$ with $p \equiv 3 \bmod 4$ and b any non-zero element in $GF(p)$. Here an appropriate distortion map is given by $(x, y) \rightarrow (-x, i \cdot y)$ where $i \in GF(p^2) \backslash GF(p)$ satisfies $i^2 = -1$.

2. $y^2 = x^3 + a$ with $p \equiv 2 \bmod 3$ and a any non-zero element in GF(p). Here an appropriate distortion map is given by $(x, y) \to (x, w \cdot y)$ where $w \in \mathrm{GF}(p^2) \backslash \mathrm{GF}(p)$ satisfies $w^3 = 1$.

It follows that for these groups of points for which a distortion map exists and is effectively computable that the DDH problem is efficiently computable. Joux and Nguyen [8] have constructed examples of supersingular elliptic curves, of the type described above, that have the additional property that the DH problem and the DL problem are equivalently difficult.

4.2. *Possible Generalizations*

In this section we discuss generalizations of our techniques, including the applicability to general elliptic curves, e.g., non-supersingular ones. To this end, let E: $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ be an elliptic curve defined over a finite field $K = \mathrm{GF}(p^n)$ of characteristic p and let P be a point on E over K of prime order l. As usual, we refer to the points on the curve E over a field L (including the point at infinity) by $E(L)$. The endomorphism ring of E over K, denoted by $\mathrm{End}_K(E)$, denotes all endomorphisms of E defined over K. As is customary we let *the* endomorphism ring of E refer to the endomorphism ring of E over the algebraic closure $\bar{K}$ of K and we denote this by simply $\mathrm{End}(E)$.

A *distortion* map (defined over K') with respect to a cyclic subgroup $\langle P \rangle$ of order l is an endomorphism (defined over K') of the curve that maps any non-zero point $Q \in \langle P \rangle$ to a point $D(Q)$ independent from Q (see Fig. 1). As $D(\cdot)$ is a group homomorphism, $D(Q)$ is a non-trivial element of the l-torsion group $E[l]$ of E and it follows that a distortion can only exist if $E[l]$ is non-cyclic. It is well known (see Corollary 6.4 of [19]) that $E[l]$ is non-cyclic if and only if $l \neq p$ in which case $E[l]$ is isomorphic to $\mathbb{Z}/l\mathbb{Z} \times \mathbb{Z}/l\mathbb{Z}$. So throughout this section we can assume $l \neq p$.

Let $K' = \mathrm{GF}(p^{nk})$ be the minimal extension K' of K such that the l-torsion group of E lies in $E(K')$ then $\mathrm{End}_{K'}(E[l])$ denotes the ring of all endomorphisms defined over K' restricted to the torsion group $E[l]$. In a similar fashion we use the notation $\mathrm{End}(E[l])$. Such rings can be seen as subgroups of all l-linear maps on $\mathrm{GF}(l)^2$ and distortion maps correspond with linear maps in such rings that do not have P as an eigenvector. We recall that the number k is the so-called *MOV degree* with respect to the group $\langle P \rangle$. A sufficient condition for the MOV degree being strictly larger than one is that l^2 does not divide $\#(E(K))$. It is shown by Koblitz in [10] that if $l \nmid p^n - 1$, then the MOV degree is the smallest natural number k such that $l \mid p^{nk} - 1$.

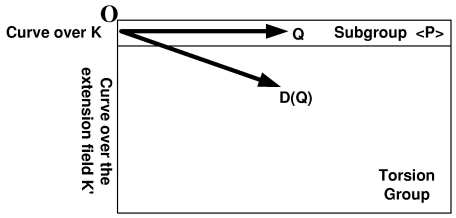

Fig. 1. Distortion maps.

By the MOV degree of E (without reference to a subgroup of $E(K)$) we mean the MOV degree of the group $E(K)$. For supersingular elliptic curves this degree is either 1, 2, 3, 4 or 6. For "ordinary", i.e., non-supersingular elliptic curves the MOV degree is typically large. It is known (see [15]) that for degrees k of size polynomial in $\log_2(\#(K))$ computing the Weil pairing $E_l(\cdot,\cdot)$ can be done in probabilistic polynomial time in $\log_2(\#(K))$ too. Under this condition the existence of a distortion map with respect to P is cryptographically relevant from two perspectives. First, such existence is relevant from a cryptanalytical perspective as it directly follows from the techniques employed in Section 3 that the DDH problem in the group $\langle P\rangle$ is then efficiently computable. Secondly, it is relevant from an applicative perspective as distortion maps can be used as building blocks in applications. See Section 5.

So the following question arises: under what conditions can we expect that distortion maps exist? In answering this question the Frobenius endomorphism with respect to K, $F\colon (x, y) \to (x^{(p^n)}, y^{(p^n)})$ plays an important role. The Frobenius endomorphism acts as a GF(l)-linear mapping on $E[l]$ (considered as a two-dimensional linear space over GF(l)) and its characteristic equation (resp. in GF(l)) is $\lambda^2 - t\lambda + p^n$ (resp. mod l), see Section 7.1 of [15]). Here $t \in \mathbb{Z}$ is the *trace* of the Frobenius endomorphism. The elliptic curve E is supersingular if and only if $t \equiv 0 \bmod p$ [15, Chapter 2]. The trace t is also related to $\#(E(K))$ by Hasse's theorem $\#(E(K)) = p^n - t + 1$, see [15]. The eigenvalues of F with respect to $E[l]$ are one (with corresponding eigenspace $\langle P\rangle$) and $t - 1 \bmod l$. It follows that for $t \not\equiv 2 \bmod l$ the Frobenius endomorphism restricted to $E[l]$ has two different eigenvalues and eigenspaces. Note that the Frobenius endomorphism acts as a distortion map on all cyclic subgroups of $E[l]$ different from its eigenspaces.

The following result states that distortion maps always exist on groups of points on supersingular elliptic curves.

Theorem 5. *Let E be a supersingular elliptic curve over a finite field $K = \mathrm{GF}(p^n)$ with MOV degree k and let $K' = \mathrm{GF}(p^{nk})$. Let P be a point on E over K of prime order l relatively prime to p, then $\mathrm{End}_{K'}(E[l])$ is isomorphic to the ring $M_2(\mathbb{Z}/l\mathbb{Z})$ of all 2×2 matrices over $\mathbb{Z}/l\mathbb{Z}$. In particular there is an abundance of distortions maps (defined over K') with respect to P.*

Proof. The proof of this result is based on a rather deep structural result on Tate modules on which we provide some background first, see [19]. The lth *Tate module* of the curve E is the inverse limit

$$T_l(E) = \lim_{\leftarrow n} E[l^n],$$

where the inverse limit is taken with respect to the multiplication by l-maps $[l]\colon E[l^{n+1}] \to E[l^n]$. The Tate module is a module over the l-adic integers, $\mathbb{Z}_l$. Any endomorphism $\varphi \in \mathrm{End}_{K'}(E)$ naturally induces an homomorphism $\varphi\colon E[l^n] \to E[l^n]$ for any natural number n and so it induces a homomorphism $\varphi\colon T_l(E) \to T_l(E)$. One denotes all homomorphisms of the l-adic module $T_l(E)$ into itself by $\mathrm{Hom}(T_l(E))$ and we conclude we have a map $T\colon \mathrm{End}_K(E) \to \mathrm{Hom}(T_l(E))$. Now $\mathrm{Hom}(T_l(E))$ is an l-adic module and in fact $\mathrm{Hom}(T_l(E))$ is equal to the ring $M_2(\mathbb{Z}_l)$ of all 2×2 matrices over $\mathbb{Z}_l$ (see Proposition 7.1a of [19]).

One can also consider $\mathrm{End}_K(E)$ as part of an l-adic module by considering the tensor product $\mathrm{End}_K(E) \otimes \mathbb{Z}_l$. Moreover, the map $T(\cdot)$ can be extended in a natural way to a map $T\colon \mathrm{End}_K(E) \otimes \mathbb{Z}_l \to \mathrm{Hom}(T_l(E))$. This map is not only injective (see Theorem 7.4 of [19]) but one can also conveniently describe the image of this map. This consists of the module $\mathrm{Hom}_{K'}(T_l(E))$ of all homomorphisms in $\mathrm{Hom}(T_l(E))$ that commute with the Frobenius endomorphism with respect to K' considered as an element of $\mathrm{Hom}(T_l(E))$. In other words, the map $T\colon \mathrm{End}_K(E) \otimes \mathbb{Z}_l \to \mathrm{Hom}_{K'}(T_l(E))$ is an isomorphism of l-adic rings. This is a theorem of Tate (see Theorem 7.7 of [19]).

In the situation of the lemma the curves are supersingular and so the Frobenius endomorphism with respect to K' is an integer. This is typical for supersingular elliptic curves as the characteristic polynomial of that Frobenius endomorphism has integer solutions in that situation. As every element of $\mathrm{Hom}(T_l(E))$ evidently commutes with an integer it follows that $\mathrm{Hom}_K(T_l(E)) = \mathrm{Hom}(T_l(E)) = M_2(\mathbb{Z}_l)$ and hence $T\colon \mathrm{End}_K(E) \otimes \mathbb{Z}_l \to M_2(\mathbb{Z}_l)$ is an isomorphism. By restricting to the first index only it follows in particular that the map $T\colon \mathrm{End}_K(E) \times \mathbb{Z}/l\mathbb{Z} \to M_2(\mathbb{Z}/l\mathbb{Z})\colon (\varphi, x) \to \varphi \cdot x$ is an isomorphism. It evidently follows that $\mathrm{End}_K(E[l])$ is equal to $M_2(\mathbb{Z}/l\mathbb{Z})$ as desired. □

In the remarks following Theorem 7 we provide an alternative proof for the main result of Theorem 5. The following two results precisely describe when a group of points on a non-supersingular elliptic curve has a distortion.

Theorem 6. *Let E be a non-supersingular elliptic curve over the finite field $K = \mathrm{GF}(p^n)$ and let P be a point on E over K of prime order $l \neq p$. If the MOV degree k related to P is larger than one, then no distortion maps on $\langle P \rangle$ exist.*

Proof. Assume that a distortion map $D(\cdot)$ on $\langle P \rangle$ exists. Then the following equality holds:

$$D(F_K(P)) = F_K(D(P)) = D(P), \tag{1}$$

where $F_K(\cdot)$ denotes the Frobenius endomorphism with respect to K. The first equality follows from the commutativity of $\mathrm{End}(E)$ due to the non-supersingularity of the curve E and the second equality follows as $P \in E(K)$. As the MOV degree k related to P is larger than one it follows that $E[l] \cap E(K) = \langle P \rangle$. This means that $F_K(\cdot)$ maps a point $Q \in E[l] \backslash \langle P \rangle$ to a point different from Q. This holds in particular for $Q = D(P)$ contradicting equality (1). □

Theorem 7. *Let E be a non-supersingular elliptic curve over the finite field $K = \mathrm{GF}(p^n)$ and let P be a point on E over K of prime order $l \neq p$. Let the MOV degree k related to P be equal to one, let t be the trace of the Frobenius endomorphism $F_K(\cdot)$ with respect to K and let the endomorphism θ generate $\mathrm{End}(E)$ over $\mathbb{Z}$ (i.e., $\mathrm{End}(E) = \mathbb{Z}[\theta]$). Then $t \mod l \equiv 2$ and the following hold:*

1. *A distortion on $\langle P \rangle$ exists if and only if P is not an eigenvector of $\theta(\cdot)$.*

2. *The endomorphism $\theta(\cdot)$ is not a scalar and has either one or two one-dimensional eigenspaces. Consequently, all except at most two cyclic subgroups of $E[l]$ have a distortion map.*

Proof. If $t \not\equiv 2 \bmod l$, then the Frobenius endomorphism has an eigenvalue $t - 1 \bmod l$ on $E[l]$ different from one which means that $E[l]$ cannot be contained in $E(K)$, implying that the MOV degree related to P must be larger than one. That a distortion on $\langle P \rangle$ exists if and only if P is not an eigenvector of $\theta(\cdot)$ is straightforward. For a proof of the last part we show that $\#\mathrm{End}(E[l]) = l^2$. As l is relatively prime to p the map $[l]$, i.e., multiplication with l, is separable (see Corollary 5.5 of [19]). It follows from Corollary 4.11 of [19] that any endomorphism that vanishes on $E[l]$ takes the form $\lambda \circ [l]$ where $\lambda(\cdot) \in \mathrm{End}(E)$. Consequently, the restriction map $\mathrm{End}(E) \to \mathrm{End}(E[l])$ has $[l]\mathrm{End}(E)$ as its kernel and so its image $\mathrm{End}(E[l])$ is isomorphic to $\mathrm{End}(E)/[l]\mathrm{End}(E)$. As E is non-supersingular its endomorphism ring is a $\mathbb{Z}$ module of rank 2 (see Theorem 3.1 of [19]) and so $\mathrm{End}(E)/[l]\mathrm{End}(E)$ is of order l^2 as desired. □

We provide some remarks on Theorem 7. If there exists a subfield K_0 of K such that E is defined over K_0 and the Frobenius endomorphism with respect to K_0 has two different eigenspaces on $E[l]$, then these coincide with those of θ.

The idea of the proof of the third part of Theorem 7 can also be used to provide an alternative proof of the result of Theorem 5 that $\mathrm{End}(E[l]) = M_2(\mathbb{Z}_l)$ if the curve E is supersingular. Indeed, in that situation $\mathrm{End}(E)$ is a $\mathbb{Z}$ module of rank 4 (see Theorem 3.1 of [19]), hence $\mathrm{End}(E[l]) = \mathrm{End}(E)/[l]\mathrm{End}(E)$ has l^4 elements and is hence equal to $M_2(\mathbb{Z}/l\mathbb{Z})$. Note that unlike Theorem 5 this proof does not provide information on the degree of the extension K' of K such that $\mathrm{End}_{K'}(E[l])$ contains distortions which are practically relevant.

A group of points on an elliptic curve that has an efficiently computable distortion map and Weil pairing gives rise to applications, see Section 5. Supersingular elliptic curves provide such groups, but according to Theorem 7 non-supersingular elliptic curves can also provide such groups. As an example, consider curves of type E: $Y^2 = X^3 + X$ over $\mathrm{GF}(p)$ such that $p - 1$ is a square and is divisible by a prime $l \equiv 3 \bmod 4$. It follows that -1 is a quadratic residue modulo p (as $p \equiv 1 \bmod 4$) but not modulo l. Moreover, $\#(E(\mathrm{GF}(p))) = p - 1$, i.e., the trace of the Frobenius endomorphism with respect to $\mathrm{GF}(p)$ is equal to two. Let $i \in \mathrm{GF}(p)$ be such that $i^2 = -1$ and let $D(\cdot)$ be the endomorphism $(x, y) \to (-x, i \cdot y)$. It follows that $D \circ D = [-1]$ and so $D(\cdot)$ cannot have eigenvalues on $E[l]$. As in these circumstances the discrete logarithm in any subgroup of order l is reducible to the discrete logarithm in $\mathrm{GF}(l)^*$ it follows that l should be of size ≥ 1024 bits to provide minimal security, this means that p is of size ≥ 2048 bits. As $E[l] \subset E(\mathrm{GF}(p))$, the Weil pairing on points of $E[l]$ is efficiently computable. A drawback of using such elliptic curves is that the number of bits required to represent elements of $\langle P \rangle$ is at least twice as large as required in the situation of supersingular elliptic curves. As an illustration we give an example of such p, l, i which we found using the Magma computational algebra package:

$$
\begin{aligned}
p &= 30^2 * q^2 + 1, \\
l &= 179769313486231590772930519078902473361797697894230657273430081157\backslash \\
&\quad 732675805500963132708477322407536021120113879871393357658789768 8\backslash
\end{aligned}
$$

$$
\begin{aligned}
& 144166224928474306394741243777678934248654852763022196012460941 19\backslash \\
& 453082952085005768838150682342462881473913110540827237163350510 68\backslash \\
& 458629823994724593847971630483535632962422414987 1, \\
i \;=\; & 539307940458694772318791557236707420085393093682691971820290243 47\backslash \\
& 319802741650288939812543196722260806336034163961418007297636930 64\backslash \\
& 432498674785422919184223731333036802745964558289066588037382823 58\backslash \\
& 359248856255017306514452047027388644421739331622481711490051532 05\backslash \\
& 375889471984173781543914891450606898887267244961 30.
\end{aligned}
$$

Observe that the Frobenius endomorphism with respect to GF(p) on this curve is the identity on $E[l]$, i.e., it does not provide a distortion map for any element of $E[l]$. This behavior is not restricted to curves with Frobenius trace 2, but also occurs for $t \bmod l \equiv 2$. To illustrate, the curve E': $Y^2 = X^3 + 5X$ over GF(73) has Frobenius trace $t = -16$ (i.e., $\#E'(\mathrm{GF}(p)) = 90$) and the map $D'(\cdot)$ defined similar to the map $D(\cdot)$ described above does not have eigenvalues on $E[3]$.

Although Theorems 5–7 precisely describe *when* groups of points on elliptic curves have distortion maps, it seems like an interesting question to determine the complexity of effectively calculating them. Recall from Section 3 that if a group of points on an elliptic curve admits an efficiently computable distortion map and Weil pairing, then the DDH problem is efficiently computable. Hence if efficiently computable distortion maps can be efficiently calculated on all groups of points of prime order on supersingular elliptic curves and non-supersingular elliptic curves of Frobenius trace $t \equiv 2 \bmod l$, then the DDH problem is efficiently computable for all such groups, which would be an interesting result from a cryptographic perspective.

5. Applications

Distortion maps on supersingular elliptic curves cannot only be used as cryptanalytical tools, but also as building blocks in actual applications. Since the presentation of the version of this paper [21] in 2001, several such applications have been found, the most impressive of which is probably the identity-based encryption scheme by Boneh and Franklin [1]. We refer to Joux's survey paper [7] for more information. In the applications below we use Weil pairing for ease of exposition, but it is more practical to use the Tate pairing instead.

5.1. *A One Round Protocol for Tripartite Diffie–Hellman Key Exchange*

In [6] Joux proposes schemes for a three participants variation of the Diffie–Hellman protocol. One of his schemes is based on a subgroup of prime order l of a supersingular elliptic curve over a field GF(p^n). Two points P, Q of order l are chosen, such that P is an element of the elliptic curve over GF(p^n) and Q is an element of the l-torsion group that is independent from P. A simple way to establish this, is to choose the element Q of order l so that it is not on the curve itself, but it is on the curve over the extension field GF(p^{nk}) of GF(p^n). Here k is called the MOV degree, which is either 1, 2, 3, 4 or 6. It

follows in particular that the Weil pairing $e_l(P, Q)$ is an lth root of unity in GF(p^{nk}). It is assumed that taking discrete logarithms in the groups $\langle P\rangle$ and $\langle Q\rangle$ is not practically possible.

Now in the tripartite Diffie–Hellman protocol, three parties A, B, C want to establish a shared key, whereby each party only exchanges one message with another party. That is, at most six messages are exchanged. Joux proposes the following protocol. Each ith participant ($i = 1, 2, 3$) generates a random $0 \leq x_i < l$, forms $(A_i, B_i) = (x_i \cdot P, x_i \cdot Q)$ and sends this to the other participants. Now the shared key is the element $e_l(P, Q)^{x_1 \cdot x_2 \cdot x_3}$. To illustrate that each participant can compute the shared key, the first participant can do so by determining

$$e_l(A_2, B_3)^{x_1} = e_l(x_2 \cdot P, x_3 \cdot Q)^{x_1} = e_l(P, Q)^{x_1 \cdot x_2 \cdot x_3}.$$

We now describe the possible application of distortion maps. To this end, let P be a point on an elliptic curve E of order l such that taking discrete logarithms in $\langle P\rangle$ is not practically possible and assume there exists a distortion map $D(\cdot)$ on the curve that maps P to a point $D(P)$ independent from P.

Now if, in our variant of the tripartite Diffie–Hellman protocol, three parties A, B, C want to establish a shared key, then each ith participant ($i = 1, 2, 3$) generates a random $0 \leq x_i < l$, forms the point $x_i \cdot P$ and sends this to the other participants. The shared key is the element $e_l(P, D(P))^{x_1 \cdot x_2 \cdot x_3}$. It is a simple verification to see that each participant can compute this key. Compared with the original tripartite Diffie–Hellman protocol in the curve E, this variant only requires two-thirds of the number of exponentiations and half the number of bits exchanged.

If one can solve the DH problem with respect to P or $e_l(P, Q)$, then one can break this protocol. We are not aware of reverse results.

5.2. *Supporting Non-Repudiation and Escrowable Encryption with Only One Public Key*

To support the non-repudiation of digital signatures fully it is common practice not to escrow the related private keys. To prevent loss of information resulting from loss of private key material, or to comply with legal requirements, end-users will typically be issued two (or even three) certificates: one for non-repudiation services and others for different services.

The use of distortion mappings makes it possible to employ one public key (and hence a certificate) for a non-repudiation service as well as for an encryption service, in such a way that the private signing key is not escrowed, while the encryption service is recoverable. To describe this scheme, once again let P be a point on an elliptic curve E over a finite field GF(p^n) such that taking discrete logarithms in $\langle P\rangle$ is not practically possible. Assume there exists a distortion map $D(\cdot)$ on the curve that maps P to a point $D(P)$ independent from P in the l-torsion group contained in the elliptic curve over the extension field GF(p^{nk}). We assume that the Weil pairing is efficiently computable on $\langle P\rangle \times \langle D(P)\rangle$. Denote the lth root of unity $e_l(P, D(P))$ in GF(p^{nk}) by g.

In our scheme an end-user A chooses his private signing key $0 \leq x < l$ randomly. Its public key (for both the non-repudiation and the encryption service) is the element $y = g^x$ in GF(p^{nk})*. The user's certificate is based on this public key and also references

to (or contains) the system parameters, e.g., the elliptic curve E, the group order l, the point P on it and the element g. To make the encryption service recoverable, the user also forms the point $Y = x \cdot P$ and escrows this at a trusted third party. Now, the end-user could employ any discrete-logarithm-based digital signature scheme, like Schnorr, ElGamal or DSA, thereby using the g, y and the private key x. The encryption service supported is the following variant of the ElGamal [4] encryption scheme:

1. The sender generates a random $0 \leq k < l$ and symmetrically encrypts the information for end-user A using y^k as a session key.
2. The sender forms the point $K = k \cdot P$ on the curve E and sends both the encrypted information and the point K to end-user A.

Now there are essentially two ways for the end-user A to decrypt information encrypted this way. The first way is first to calculate $e_l(K, D(P)) = e_l(k \cdot P, D(P)) = e_l(P, D(P))^k = g^k$ and then secondly calculate $(g^k)^x = y^k$ which enables the end-user to decrypt the symmetrically encrypted information. Note that no secret information is required to determine g^k, so this information could in fact be sent along by the sender, avoiding that the end-user needs to calculate a Weil pairing. The second way to decrypt this information is to calculate $e_l(K, D(Y)) = e_l(k \cdot P, D(x \cdot P)) = e_l(k \cdot P, x \cdot D(P)) = g^{kx} = y^k$ directly on the basis of Y. Note that this operation does not require the private key x but that the escrowed value Y suffices. Hence, if the end-user retrieves a copy of Y from his escrow agent, then he is able to decrypt his messages when he loses his private x. However, the end-user is not able to make new digital signatures as determining the private key x from $Y = x \cdot P$ requires one to solve a discrete logarithm problem in the elliptic curve, which we assumed is not practically possible.

For an indication of security, suppose that an attacker can compute Y on the basis of y, then as y is chosen randomly by the end-user, the attacker has found a computable injective homomorphism from $\langle g \rangle$ to $\langle P \rangle$. It follows from the arguments in Section 3 that the attacker is then also able to solve the DH problem in both these groups. We are not aware of more rigorous security proofs. We finally remark that there exists a more general but less efficient variant of this scheme that does not require a distortion map and whereby one uses two independent points P, Q. We leave the details, which are straightforward, to the reader.

6. Conclusion

We have shown that the existence of any efficiently computable, injective homomorphism from the XTR subgroup in the group of points over $\mathrm{GF}(p^2)$ on a supersingular elliptic curve over $\mathrm{GF}(p^2)$ of order $p^2 - p + 1$ implies that we can solve several problems that are widely believed to be hard. The DH problem in the XTR subgroup is an example of such a problem. We have also shown that the DDH problem in such elliptic curve groups is efficiently computable and that our results can be extended to other supersingular elliptic curve groups. The results in this paper therefore provide evidence that the multiplicative group of a finite field provides essentially more, and in any case not less, security than the group of points of a supersingular elliptic curve of comparable size. In addition to this, we have discussed generalizations to tackle the DDH problem in groups of points on general

elliptic curves over finite fields. Finally, we have shown that the tools we used in our cryptanalysis (distortion maps) can also be used as building blocks in new cryptographic applications. We have illustrated that with two examples: an improvement of Joux's one round protocol for tripartite Diffie–Hellman key exchange and a non-refutable digital signature scheme that supports escrowable encryption. We have also classified elliptic curve groups where distortion maps exist, which apart from (nearly) all supersingular elliptic curve groups also include certain types ($t = 2$) of ordinary elliptic curve groups.

Acknowledgments

I thank Scott Vanstone for posing the **X2C** hypothesis at the Crypto 2000 Rump Session. I am grateful to Antoine Joux, David Kohel, Arjen Lenstra, Ruud Pellikaan, René Schoof and Joe Silverman for the stimulating discussions I had with them. Antoine is specifically thanked for his observation that my initial proof techniques could be elegantly formulated with distortion maps. Arjen is specifically thanked for challenging and helping me to show that the weak Diffie–Hellman problem is equivalent to the conventional one. The results in Section 4.2 on general elliptic curves are for the most part due to Ruud Pellikaan (Theorem 6) and René Schoof (Theorems 5, 7 and the remarks following them). I am grateful to them both for allowing me to include those results in this paper. I finally want to thank the two anonymous referees for pointing out parts of the paper that needed further clarification.

References

[1] D. Boneh, M. Franklin, Identity-based encryption from the Weil pairing, *Proceedings of Crypto* 2001, LNCS 2139, Springer-Verlag, Berlin, 2001, pp. 213–229.

[2] R. Cramer, R. Gennaro, B. Schoenmakers, A secure and optimally efficient multi-authority election scheme, *Advances in Cryptology - EUROCRYPT '97 Proceedings*, Springer-Verlag, Berlin, 1997, pp. 103–118.

[3] R. Cramer, V. Shoup, A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack, *Proceedings of Crypto* 1998, LNCS 1462, Springer-Verlag, Berlin, 1998, pp. 13–25.

[4] T. ElGamal, A public key cryptosystem and a signature scheme based on discrete logarithms, *IEEE Trans. Inform. Theory* 31(4) (1985), 469–472.

[5] G. Gong, L. Harn, Public key cryptosystems based on cubic finite field extensions, *IEEE Trans. Inform. Theory*, (II) 1999.

[6] A. Joux, A one round protocol for tripartite Diffie–Hellman, 4*th International Symposium*, *Proceedings of ANTS*, LNCS 1838, Springer-Verlag, Berlin, 2000, pp. 385–394.

[7] A. Joux, The Weil and Tate pairings as building blocks for public key cryptography, 5*th International Symposium*, *Proceedings of ANTS*, LNCS 2369, Springer-Verlag, Berlin, 2002, pp. 20–32.

[8] A. Joux, K. Nguyen, Seperating Decision Diffie–Hellman from Diffie–Hellman in cryptographic groups, in preparation. Available from eprint.iacr.org.

[9] N. Koblitz, An elliptic curve implementation of the finite field digital signature algorithm, *Proceedings of Crypto* '98, LNCS 1462, Springer-Verlag, Berlin, 1998, pp. 327–337.

[10] N. Koblitz, The 4th Workshop on Elliptic Curve Cryptography (ECC 2000), Essen, October 4–6, 2000.

[11] A.K. Lenstra, E.R. Verheul, The XTR public key system, *Proceedings of Crypto* 2000, LNCS 1880, Springer-Verlag, Berlin, 2000, pp. 1–19; available from www.ecstr.com.

[12] A.K. Lenstra, E.R. Verheul, Key improvements to XTR, *Proceedings of Asiacrypt* 2000, LNCS 1976, Springer-Verlag, Berlin, 2000, pp. 220–223; available from www.ecstr.com.

[13] A.K. Lenstra, E.R. Verheul, Fast irreducibility and subgroup membership testing in XTR, *Proceedings of the* 2001 *Public Key Cryptography Conference*, LNCS 1992, Springer-Verlag, Berlin, 2001, pp. 73–86; available from www.ecstr.com.

[14] R. Lidl, W.B. Müller, Permutation polynomials in RSA-cryptosystems, *Crypto* '83 *Proceedings*, Plemium Press, 1984, pp. 293–301.

[15] A. Menezes, *Elliptic Curve Public Key Cryptosystems*, Kluwer, Boston, MA, 1993.

[16] A. Menezes, T. Okamoto, S.A. Vanstone, Reducing elliptic curve logarithms to a finite field, *IEEE Trans. Inform. Theory*, 39 (1993), 1639–1646.

[17] A. Menezes, S.A. Vanstone, ECSTR (XTR): Elliptic Curve Singular Trace Representation, Rump Session of Crypto 2000.

[18] S.C. Pohlig, M.E. Hellman, An improved algorithm for computing logarithms over GF(p) and its cryptographic significance, *IEEE Trans. Inform. Theory*, 24 (1978), 106–110.

[19] J. Silverman, *The Arithmetic on Elliptic Curves*, Springer-Verlag, New York, 1986.

[20] P. Smith, C. Skinner, A public-key cryptosystem and a digital signature system based on the Lucas function analogue to discrete logarithms, *Asiacrypt* '94 *Proceedings*, Springer-Verlag, Berlin, 1995, pp. 357–364.

[21] E. Verheul, Evidence that XTR is more secure than supersingular elliptic curve cryptosystems, *Proceedings of Eurocrypt* 2001, LNCS 2045, Springer-Verlag, Berlin, 2001, pp. 195–210.