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, pobox.com]

Abstract. We show that finding an efficiently computable injective homomorphism from the XTR subgroup into the group of points over $\mathrm{GF}(p^2)$ 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 S. Vanstone and A. 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 problem are presumably not. The cryptanalytical tools we use 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.

1 Introduction

XTR is an efficient and compact method to work with order p^2-p+1 subgroups of the multiplicative group $\mathrm{GF}(p^6)^*$ of the finite field $\mathrm{GF}(p^6)$. It was introduced in [10], followed by several practical improvements in [11] and [12].

Throughout this paper we let $p, q > 3$ denote prime numbers. In the context of XTR we further demand that $p \equiv 2 \bmod 3$ and that q divides p^2-p+1. Let g be a generator of the order q subgroup μ_q of $\mathrm{GF}(p^6)^*$. In [10] it is shown that elements of μ_q, the *XTR subgroup*, can conveniently be represented by their so-called trace over $\mathrm{GF}(p^2)$, and it is shown in [10] how this representation can efficiently be 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 [10] 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 $\mathrm{GF}(p^6)^*$. We refer to the group of order p^2-p+1 of $\mathrm{GF}(p^6)^*$ as the *XTR supergroup*. It is widely believed that the Diffie-Hellman and discrete logarithm problem in these XTR groups is hard.

At the Crypto 2000 Rump Session, [16], the following comparison was presented, suggesting that XTR is nothing else than an elliptic curve cryptosystem in disguise. As is well known, the number of points over $\mathrm{GF}(p^2)$ (including the point at infinity) on an elliptic curve defined over $\mathrm{GF}(p^2)$ takes the form p^2-t+1 for some integer called the Frobenius trace number $t \in [-2p, 2p]$. There exist elliptic curves over $\mathrm{GF}(p^2)$ of such order equal to $p^2 - p + 1$. These curves are actually characterized in [14] as **C**lass **T**hree supersingular elliptic curves over $\mathrm{GF}(p^2)$ 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) imbedding [15], provides an example of such a homomorphism.

It seems like a plausible hypothesis (cf. [16]) 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. Or in other words, under this hypothesis the security of XTR cryptosystems is not better than that of elliptic curve cryptosystems.

In this paper 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 else than an elliptic curve cryptosystem in disguise. We did not attempt to fully generalize them to other classes of (supersingular) elliptic curves, although we expect they can be (cf. 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 $a \in \mathrm{GF}(p^2)$ is a square but not a cube in $\mathrm{GF}(p^2)$, cf. [8]. We denote the CTP curves by C_a. Actually, in the category of elliptic curves over $\mathrm{GF}(p^2)$ only two such curves exist; all others are isomorphic under an efficiently computable isomorphism. Compare Lemma 2.1. The set of points over $\mathrm{GF}(p^2)$ (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 $\mathrm{GF}(p^6)$ as well, respectively subgroups of order l therein. These are denoted by respectively 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 $C_{s,p^2}[q]$.

A similar problem is posed by N. Koblitz in [9, p.328]. Note that **X2C** is more general than only assuming that (a restriction of) an MOV embedding is efficiently invertible. It actually follows from our results (Theorem 3.5) that under the **X2C** hypothesis, (restrictions of) MOV embeddings are efficiently invertible.

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 briefly discuss some possible extensions of our results. 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 [5] 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 between the points on the elliptic curves over K, but not vice versa. See [14], [18]. This distinction is important in the following lemma.

Lemma 2.1 *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 $S : C_{a,p^2} \to C_{a^p,p^2} : (x, y) \to (x^p, y^p)$ is an efficiently computable group isomorphism.*
2. *The equation $u^6 = b/a$ has its solutions in* $\mathrm{GF}(p^6)$ *and for any such solution u, the map $R_u : C_a \to C_b : (x, y) \to (u^2x, u^3y)$ is an isomorphism in the category of elliptic curves over* $\mathrm{GF}(p^6)$ *and induces in particular an efficiently computable group isomorphism $C_{a,p^6} \to C_{b,p^6}$.*
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 w in* $\mathrm{GF}(p^2)$ *and the composite map $R_w \circ S$ is an efficiently computable group isomorphism from 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 [14, Theorem 2.2]. 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 part. □

From Lemma 2.1 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 [14, Theorem 3.2] 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 2.2 *All CTP groups C_{a,p^2} are efficiently computable group isomorphic. Moreover, we can reformulate* **X2C** *as:*

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

Let C_a be a CTP curve. We recall some facts on elliptic curves which can all be found in [14]. For a divisor l of $p^2 - p + 1$, the l-th *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 $\mathbf{Z}_l \oplus \mathbf{Z}_l$, which is a non-cyclic, abelian group. In addition, as C_a is a so-called Class III supersingular curve, the l-th 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-th torsion group of C_a is equal to $C_{a,p^6}[l]$ and is hence a subset of $\mathrm{GF}(p^6) \times \mathrm{GF}(p^6)$.

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

Definition 2.3 *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 relevant when the group H is not cyclic itself, which is typically the situation in 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 three. We denote this group by G_3.

Theorem 2.4 *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 2.1, the following hold:*

1. *The equation $u^6 = a/a^p$ has its solutions u in $\mathrm{GF}(p^6) \setminus \mathrm{GF}(p^2)$ and for any such solution u, the map $D : C_{a,p^6} \xrightarrow{S} C_{a^p,p^6} \xrightarrow{R_u} C_{a,p^6}$ is a group automorphism which takes the form $(x, y) \to (u^2 x^p, u^3 y^p)$.*
2. *$\langle P \rangle \cap \langle D(P) \rangle = \mathcal{O}$ if the order of P is not divisible by 3 and $\langle P \rangle \cap \langle D(P) \rangle = G_3$ otherwise.*

3. *The point P is independent from its image under $D(.)$ iff P has an order different from 1 or 3.*

Proof: For a proof of the first part of the theorem, it easily follows (cf. the proof of Lemma 2.1) that a/a^p is not a cube in $\mathrm{GF}(p^2)$. Now the proof follows from the last part of Lemma 2.1. For a proof of the second part of the theorem: the first coordinate of the value (u^2x^p, u^3y^p) under $D(.)$ 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 3. For a proof of the last part, as $D(.)$ 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 map $D(.)$ introduced in Theorem 2.4 as the *distortion* map. In Figure 1 a few pages below we have depicted the property of $D(.)$ with $K = \mathrm{GF}(p^2)$ and $K' = \mathrm{GF}(p^6)$. Related to the l-th torsion group of C_a, i.e., $C_{a,p^6}[l]$, is the Weil pairing, a function

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

where μ_l is the subgroup of $\mathrm{GF}(p^6)^*$ of order l. Hence, μ_q 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 $< P >\to \mu_l : x \to e_l(x, Q)$ 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 [14, p.70].

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

Corollary 2.5 *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 $D(.)$ denote the distortion map from Theorem 2.4, 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 $D(.)$ is a group automorphism. For a proof of the first statement, suppose to the contrary that we have $e_l(P, D(P))^{l/r} = 1$. 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 2.4. 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 2.4. 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 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. It is widely assumed that if the DL problem G is hard, then so are the other two. In [5], Joux notes that Decision Diffie-Hellman type of problems in extensions of supersingular elliptic curves are often efficiently computable. We use Joux's reasoning in the proof of the next result, which in particular provides an example of a supersingular elliptic curve where the Decision Diffie-Hellman problem is efficiently computable, while the discrete logarithm problem is presumably hard.

Theorem 3.1 *The Decision Diffie-Hellman 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 [17], 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 discrete logarithm related to the first subgroup, one can efficiently the Decision Diffie-Hellman 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 Decision Diffie-Hellman problem in $C_{a,p^2}[v]$, we need to determine whether $z = x * y \bmod v$. By the Identity property of the Weil pairing, its bilinearity and Corollary 2.5, the Weil pairing $e_v(P, D(P))$ is a v-th 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 $z = x * y \bmod v$ 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 Decision Diffie-Hellman problem, like the publicly verifiable voting system in [2] and the Cramer-Shoup [3] public key cryptosystem that is provable secure against adaptive chosen ciphertext attacks. Theorem 3.1 shows that these protocols should not be based on (CTP) supersingular elliptic curves, even with the "appropriate" key sizes. We now obtain our first evidence that the **X2C** hypothesis is not valid.

Corollary 3.2 *Under the* **X2C** *hypothesis, the Decision Diffie-Hellman problem in the XTR subgroup is efficiently computable.*

Proof: This follows immediately from Theorem 3.1. □

Next we show an even stronger consequence of the **X2C** hypothesis, namely that the Diffie-Hellman problem in the XTR subgroup is efficiently computable. It is convenient to first introduce three variants of the Diffie-Hellman 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 basis of γ^x and γ^y. That is, κ is only dependent of γ and not of x, y. The *strong DH problem* with respect to γ is the problem of efficiently determining ξ^{xy} on 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 basis of α^x and α^y for all $0 \leq x, y < l$ and *any* generators ξ, α of G. Note that this notion is independent of the choice of a particular generator γ of G.

Lemma 3.3 *In the setting above, the weak, conventional and strong Diffie-Hellman problem w.r.t.* γ *and the Diffie-Hellman problem w.r.t.* G *are equivalent.*

Proof: We first show equivalence of the first three problems. Clearly, if one can solve the strong Diffie-Hellman problem, one can solve the conventional Diffie-Hellman problem. Moreover, if one can solve the conventional Diffie-Hellman problem then by taking $\kappa = \gamma$ one can solve the weak Diffie-Hellman problem. To show that these three problems are equivalent, it suffices to show that if one can solve the weak Diffie-Hellman problem, one can solve the strong Diffie-Hellman problem. To this end, let γ, κ be as described in the definition of weak Diffie-Hellman problem and let ξ be any generator of G. Also, let the function $WDH(.,.)$ be defined by $\kappa^{xy} = WDH(\gamma^x, \gamma^y)$. Then by hypothesis $WDH(.,.)$ 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 $T(2i)$ is equal to $(WDH(A, A), WDH(A, B))$ and $T(2i + 1)$ is equal to $(WDH(A, B), WDH(B, B))$. This means that we can compute $T(n)$ in $2 \cdot \log_2(n)$ calls to the function $WDH(.,.)$ using repeated squaring and multiplication (cf. [10, Algorithm 2.3.7]). 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 now are ready to prove that we can solve the strong Diffie-Hellman problem with respect to γ. To this end, let $A = \gamma^x$ and $B = \gamma^y$ be given. Then, first of all,

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

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 basis on γ^x and γ^y. That is, we have solved the strong Diffie-Hellman 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. To this end, let ξ, α be 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 of all, we can efficiently determine $\gamma^{(a^2)}$ from α, which is a conventional Diffie-Hellman problem w.r.t. γ. Secondly, from the latter result one 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 Diffie-Hellman problem w.r.t. γ. Now, if we present α^x, α^y to the efficient algorithm solving the strong Diffie-Hellman 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 Diffie-Hellman problem with respect to α and ξ. $\square$

Lemma 3.4 *Let G, Γ be two isomorphic, cyclic groups and let $i : G \to \Gamma$ and $j : \Gamma \to G$ be two efficiently computable, injective homomorphisms. We assume that the order l of G and Γ and some generators are known. Then, the Diffie-Hellman problem with respect to G is efficiently computable iff it is with respect to Γ. Moreover, under this condition, the inverses of $i(.)$ and $j(.)$ are efficiently computable too.*

Proof: It easily follows that if one can solve the Diffie-Hellman problem in one of G or Γ, then one can solve the weak Diffie-Hellman problem in the other one. So the first part of the lemma follows from Lemma 3.3. For a proof of the second part of the lemma, we show that $i^{-1}(.)$ 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 $g_2 = j(\gamma)$. One can easily verify that the algorithm solving the Diffie-Hellman problem with respect to g_2 and g yields $i^{-1}(\omega)$ when presented g_2 and $j(\omega)$. □

Theorem 3.5 *Under the* **X2C** *hypothesis, the following problems are efficiently computable:*

1. *The Diffie-Hellman problem in the XTR subgroup.*
2. *The Diffie-Hellman problem in the group of points of order q 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 q on a supersingular elliptic curves over $\mathrm{GF}(p^2)$ of order $p^2 - p + 1$ into the XTR subgroup.*

Proof: Suppose that $H(.)$ is an efficiently computable injective homomorphism from the XTR subgroup into some $C_{a,p^2}[q]$. 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 $h = e_q(H(g), D(H(g))$ where $e_q(.,.)$ denotes the Weil pairing on the q-th torsion group of C_{a,p^2} and $D(.)$ denotes the distortion map from Theorem 2.4. It also follows from this theorem that the order of h is equal to q.

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

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

That is, by computing $e_q(H(X), D(H(Y)))$, which can be done efficiently, we have solved the weak DH problem with respect to g, h. The result now follows from Lemma 3.3. The second and third part of the theorem follow from the first part and Lemma 3.4. □

The last part of Theorem 3.5 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 discrete logarithm problem in the extension field $\mathrm{GF}(p^6)^*$, or actually subfields thereof. The

LUC cryptosystem, [19] and [13], is based on the order $p+1$ subgroup of $\mathrm{GF}(p^2)^*$. The variant by Gong & Harn of LUC is based on the p^2+p+1 subgroup of $\mathrm{GF}(p^3)^*$, where as in the XTR setting $p = 2 \bmod 3$. For both subgroups one can find supersingular elliptic curves (cf. [14]) 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 an hypothesis similar to **X2C**. We remark that there do not exist elliptic curves defined over $\mathrm{GF}(p^2)$ with p^2+p+1 or p^2-p+1 points over $\mathrm{GF}(p^2)$ if $p = 1 \bmod 3$, as the number of isomorphism classes is equal to $1-\left(\frac{-3}{p}\right)$ (cf. [14, Theorem 3.2]), which is equal to zero if $p = 1 \bmod 3$ and equal to two if $p = 2 \bmod 3$.

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 $\mathrm{GF}(p^2)$ 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 $a \in \mathrm{GF}(p^2)$ is neither a square nor a cube in $\mathrm{GF}(p^2)$. This means that the difference with CTP curves lies in the fact that a is a non-quadratic residue. However, it easily follows 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 $(x, y) \to (u^2x^p, u^3y^p)$ 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 $\mathrm{GF}(p^2)$ are mapped to points outside the curve over $\mathrm{GF}(p^2)$. It follows that the existence of any efficiently computable, injective homomorphism from the Gong & Harn group in any supersingular elliptic curve over $\mathrm{GF}(p^2)$ of order p^2+p+1 implies that we can solve the Diffie-Hellman problem in the Gong & Harn subgroup of $\mathrm{GF}(p^3)^*$ as well as in the related elliptic curve group of points. Moreover, it follows that the Decision Diffie-Hellman 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 $\mathrm{GF}(p)$ of trace zero. However, our techniques do generalize to two particular subclasses of such elliptic curves over $\mathrm{GF}(p)$, as one can easily find the appropriate distortion maps. These classes of curves and distortion maps are:

1. $y^2 = x^3 - bx$ with $p = 3 \bmod 4$ and a any non-zero element in $\mathrm{GF}(p)$. Here an appropriate distortion map is given by $(x, y) \to (-x, i \cdot y)$ where $i \in \mathrm{GF}(p^2) \setminus \mathrm{GF}(p)$ satisfies $i^2 = -1$.
2. $y^2 = x^3 + a$ with $p = 2 \bmod 3$ and a any non-zero element in $\mathrm{GF}(p)$. Here an appropriate distortion map is given by $(x, y) \to (x, w \cdot y)$ where $w \in \mathrm{GF}(p^2) \setminus \mathrm{GF}(p)$ satisfies $w^3 = 1$.

It follows in particular that the Decision Diffie-Hellman problem in the group of points over $\mathrm{GF}(p^2)$ on these curves is efficiently computable. Recently, A. Joux and K. Nguyen, [6], have constructed examples of supersingular elliptic curves, of the type described above that have the additional property that the Diffie-Hellman problem and the discrete logarithm problem are equivalently difficult.

4.2 Possible generalizations

In this section we discuss the applicability our techniques 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 $K = \mathrm{GF}(p^n)$ and let P be a point on E over K of prime order q. As usual, we refer to the points on the curve E over a field L (including the point at infinity) as $E(L)$. Now, a *distortion* map with respect to P is an endomorphism defined over the completion $\overline{K}$ of K that maps P to a point $D(P)$ independent from P (cf. Figure 1). As $D(.)$ is a group homomorphism, it follows that $D(P)$ is an element

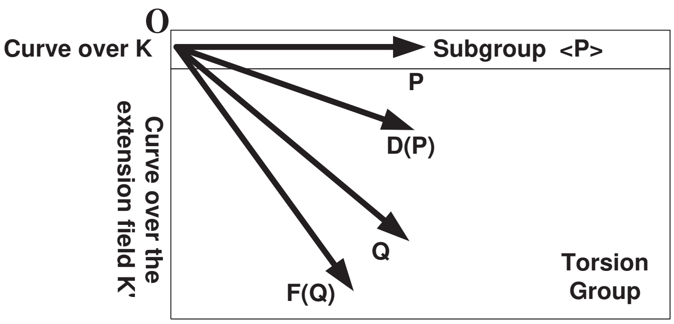

Fig. 1. Distortion maps

of the q-th torsion points $E[q]$ of E. Suppose that the set of q-th torsion points $E[q]$ of E is contained in $E(K')$ for some extension field $K' = \mathrm{GF}(p^{nk})$ of K of degree k, the so-called *MOV degree*. It it known (cf., [14]) that if the degree k is of polynomial size in $\log_2(\#(K))$ then computing the Weil pairing $E_q(.,.)$ can be done in probabilistic polynomial time in $\log_2(\#(K))$ too.

Under this condition it directly follows from the techniques employed in Section 3 that the existence of a distortion map implies that the Decision Diffie-Hellman problem in the group $\langle P \rangle$ is efficiently computable then. Now the following question arises: under what conditions can we expect that distortion maps exist? As pointed out to us by A. Joux, it is a consequence of [18, Ch. III, Th.9.5] that the endomorphism group of a supersingular elliptic curve is so large, that distortion maps always exist in these circumstances, with only a finite number of exceptions. As in this situation the degree k is either 1, 2, 3, 4 or 6, it also follows that the Decision Diffie-Hellman problem is efficiently computable in subgroups on such curves.

With respect to the case of "ordinary", i.e., non supersingular elliptic curves there is one prominent example of a distortion map, namely the Frobenius map with respect to K $F : (x, y) \to (x^{(p^n)}, y^{(p^n)})$. The Frobenius map acts as a GF(q)-linear mapping on $E[q]$ (considered as a two dimensional linear space over GF(q)) and its characteristic equation is $\lambda^2 - t\lambda + p^n$ (cf. [14]). The eigenvalues of F with respect to $E[q]$ are one (with corresponding eigenspace $\langle P \rangle$) and $t - 1 \bmod q$. If $t \neq 2 \bmod q$, then the eigenvectors corresponding with the eigenvalue $t-1 \bmod q$ are not elements of the curve over K. That is, they are outside the original curve and really lie on the extension of the curve over K'. Now if we consider any subgroup $\langle Q \rangle$ of the q-th torsion group different from these eigenspaces, we see that Q and $F(Q)$ are independent. Compare Figure 1 above. So if the MOV degree k is polynomial in $\log_2(\#(K))$ then the Decision Diffie-Hellman problem is efficiently computable in such subgroups. In [1] it is shown that for general elliptic curves over basic fields K it is unlikely that $k < \log_2(\#(K))^2$. We are not aware of general results concerning the case that k is not polynomial in $\log_2(\#(K))$. Moreover, we observe that our techniques do not really require to actually compute values of Weil pairings: only the ability to compare them suffices. For this the efficient calculation of a one bit predicate of a Weil pairing is probably sufficient. It is not a priori clear that it can be excluded that this is possible in polynomial time even if k is not polynomially bounded.

Of course, this does not settle the existence of distortion maps in the original group $\langle P \rangle$. This is very relevant from a practical, cryptographic point of view, as such existence would make the Decision Diffie-Hellman problem in practically used elliptic curve subgroups (possibly) efficiently computable. In discussions with numerous knowledgeable colleagues, it emerged that distortion maps in such elliptic curve subgroups do not exist. The following elegant proof of this was presented to us by Ruud Pellikaan.

Theorem 4.1 *Let E be a non-supersingular curve and let $P \in E(K)$ be of order q. If q is relatively prime to p and the q-th torsion group is not contained in $E(K)$ then there can not exist a distortion map $D(.)$ w.r.t. P. Moreover, the second condition is implied by the condition that q^2 does not divide $\#(E(K))$.*

Proof: Suppose, at the contrary, that such a distortion map D exists. Notice that $Q = D(P)$ is not a point on $E(K)$ as this implies that the q-th torsion group is contained in $E(K)$. The crux of the proof is that the endomorphism ring of a non-supersingular elliptic curve is abelian. This follows for instance from the fact that this ring is an order in a quadratic imaginary field (cf. [18, Ch. V, Theorem 3.1]). As before, let F be the K Frobenius map. Now,

$$Q = D(P) = D(F(P)) = F(D(P)) = F(Q),$$

where the second equality follows as $P \in E(K)$. But this means that Q is an element of $E(K)$ and we arrive at a contradiction. The last part of the result easily follows. $\square$

As elliptic curve subgroups used in practical cryptosystems, satisfy the conditions of Theorem 4.1, we conclude that in such circumstances distortion maps do not exist. It seems like an interesting problem to find out if distortion maps can exist in the situation that the q-torsion group is contained in $E(K)$, but that no point of order q is contained in $E(K_0)$ for any genuine subfield K_0 of K.

5 Applications

Distortion maps on (supersingular) elliptic curves can not only be used as cryptanalytical tools, but also as building blocks in actual applications.

5.1 A one round protocol for tripartite Diffie-Hellman key exchange

In [5] A. 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 q of a supersingular elliptic curve over a field $\mathrm{GF}(p^n)$. Two points P, Q of order q are chosen, such that P is an element of the elliptic curve over $\mathrm{GF}(p^n)$ and Q is an element of the q-th torsion group that is independent from P. A simple way to establish this, is to choose the element Q of order q so that it is not on the curve itself, but it is is on the curve over the extension field $\mathrm{GF}(p^{nk})$ of $\mathrm{GF}(p^n)$. Here k is called the MOV degree, which is either $1, 2, 3, 4$ or 6. It follows in particular that the Weil pairing $e_q(P, Q)$ is a q-th root of unity in $\mathrm{GF}(p^{nk})$. 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 6 messages are exchanged. Joux proposes the following protocol. Each i-th participant $(i = 1, 2, 3)$ generates a random $0 \leq x_i < q$, 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 $e_q(P, Q)^{x_1 \cdot x_2 \cdot x_3}$. To illustrate that each participant can compute the shared key, the first participant can do so by determining:

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

We now describe the possible application of distortion maps. To this end, let P be a point on an elliptic curve E of order q such that taking discrete logarithms in $\langle P\rangle$ is not practically possible and assume there exists a distortion map $D(.)$ 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 i-th participant $(i = 1, 2, 3)$ generates a random $0 \leq x_i < q$, forms the point $x_i \cdot P$, and sends this to the other participants. The shared key is the element $e_q(P, D(P))^{x_1 \cdot x_2 \cdot x_3}$. 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 Diffie-Hellman problem with respect to P or $e_q(P, Q)$ then one can break this protocol. We are not aware of reverse results.

5.2 Supporting non-repudiation and escrowable encryption with only public key

To fully support non-repudiation of digital signatures 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 make it possible to employ one public key (and hence 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 $\mathrm{GF}(p^n)$ such that taking discrete logarithms in $\langle P \rangle$ is not practically possible. Assume there exists a distortion map $D(.)$ on the curve that maps P to a point $D(P)$ independent from P in the q-th torsion group contained in the elliptic curve over the extension field $\mathrm{GF}(p^{nk})$. We assume that the Weil pairing is efficiently computable on $\langle P \rangle \times \langle D(P) \rangle$. Denote the q-th root of unity $e_q(P, D(P))$ in $\mathrm{GF}(p^{nk})$ by g.

In our scheme an end-user A chooses its private signing key $0 \leq x < q$ randomly. Its public key (for both the non-repudiation and the encryption service) is the element $y = g^x$ in $\mathrm{GF}(p^{nk})^*$. 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 q, 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 $0 \leq k < q$ 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 to first calculate $e_q(K, D(P)) = e_q(k \cdot P, D(P)) = e_q(P, D(P))^k = g^k$ 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 directly calculate $e_q(K, D(Y)) = e_q(k \cdot P, D(x \cdot P)) = e_q(k \cdot P, x \cdot D(P)) = g^{kx} = y^k$ on 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 basis of y, then as y is chosen randomly by the end-user, the attacker has found an 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 Diffie-Hellman 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 Diffie-Hellman problem in the XTR subgroup is an example of such a problem. We have also shown that the Decision Diffie-Hellman 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 Decision Diffie-Hellman problem in certain groups of points on non-supersingular 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.

7 Acknowledgments

I want to thank Scott Vanstone for posing the **X2C** hypothesis on the Crypto 2000 Rump Session. I am grateful to Antoine Joux, David Kohel, Arjen Lenstra, Ruud Pellikaan 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. Ruud is specifically thanked for his permission to include Theorem 4.1.

References

1. R. Barasubramanian, N. Koblitz, *The improbability that an elliptic curve has subexponential discrete log problem under the MOV algorithm*, J. of Cryptology, vol 11, 141-145, 1999.
2. R. Cramer, R. Gennaro, B. Schoenmakers, *A Secure and Optimally Efficient Multi-Authority Election Scheme* Advances in Cryptology - EUROCRYPT '97 Proceedings, Springer-Verlag, 1997, 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, 1998, 13-25.
4. T. ElGamal, *A Public Key Cryptosystem and a Signature scheme Based on Discrete Logarithms*, IEEE Transactions on Information Theory 31(4), 1985, 469-472.
5. A. Joux, *A one round protocol for tripartite Diffie-Hellman*, 4th International Symposium, Proceedings of ANTS, LNCS 1838, Springer-Verlag, 2000, 385-394.
6. A. Joux, K. Nguyen, *Seperating Decision Diffie-Hellman from Diffie-Hellman in cryptographic groups*, in preparation. Available from eprint.iacr.org.
7. G. Gong, L. Harn, *Public key cryptosystems based on cubic finite field extensions*, IEEE Trans. on I.T., November 1999.
8. N. Koblitz, The 4th workshop on Elliptic Curve Cryptography (ECC 2000), Essen, October 4-6 2000.
9. N. Koblitz, *An Elliptic Curve Implementation of the Finite Field Digital Signature Algorithm*, Proceedings of Crypto '98, LNCS 1462, Springer-Verlag, 1998, 327-337.
10. A.K. Lenstra, E.R. Verheul, *The XTR public key system*, Proceedings of Crypto 2000, LNCS 1880, Springer-Verlag, 2000, 1-19; available from www.ecstr.com.
11. A.K. Lenstra, E.R. Verheul, *Key improvements to XTR*, Proceedings of Asiacrypt 2000, LNCS 1976, Springer-Verlag, 2000, 220-223; available from www.ecstr.com.
12. 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, 2001, 73-86; available from www.ecstr.com.
13. R. Lidl, W.B. Müller, *Permutation Polynomials in RSA-cryptosystems*, Crypto '83 Proceedings, Plemium Press, 1984, 293-301.
14. A. Menezes, *Elliptic Curve Public Key Cryptosystems*, Kluwer Academic Publishers, Boston 1993.
15. A. Menezes, T. Okamoto, S.A. Vanstone *Reducing elliptic curve logarithms to a finite field*, IEEE Trans. Info. Theory, 39, 1639-1646, 1993.
16. A. Menezes, S.A. Vanstone, *ECSTR (XTR): Elliptic Curve Singular Trace Representation*, Rump Session of Crypto 2000.
17. S.C. Pohlig, M.E. Hellman, *An improved algorithm for computing logarithms over $GF(p)$ and its cryptographic significance*, IEEE Trans. on IT, 24 (1978), 106-110.
18. J. Silverman, *The Arithmetic on Elliptic Curves*, Springer-Verlag, New York, 1986.
19. 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, 1995, 357-364.

This article was processed using the LaTeX macro package with LLNCS style