The Decisional Diffie-Hellman Problem and the Uniform Boundedness Theorem*

Qi Cheng† and Shigenori Uchiyama‡

April 22, 2003

Abstract

In this paper, we propose an algorithm to solve the Decisional Diffie-Hellman problem over finite fields, whose time complexity depends on the effective bound in the Uniform Boundedness Theorem (UBT). We show that curves which are defined over a number field of small degree but have a large torsion group over the number field have considerable cryptographic significance. If those curves exist and the heights of torsions are small, they can serve as a bridge for prime shifting, which results an efficient nonuniform algorithm to solve DDH on finite fields and a nonuniform algorithm to solve elliptic curve discrete logarithm problem faster than the known algorithms. In the other words, if the Decisional Diffie-Hellman problem over finite fields turns out to be nonuniformly hard, then the effective bound in UBT should be very small.

1 Introduction

Since the proposal of the concept of public-key cryptography, certain kinds of computational problems such as the integer factoring, the discrete logarithm problem, the Diffie-Hellman problem [3] and the RSA problem [15] have been much researched for the last two decades. So far, these computational problems are widely believed to be intractable. One of the most important topics in cryptography is to propose a practical and provably-secure cryptographic scheme under such reasonable computational assumptions. Here, we usually say a cryptographic scheme is provably secure if it is proven to be as secure as such an intractable computational problem. Moreover, in order to prove the security of a cryptographic scheme, we sometimes use other kinds of computational problems what we call decisional problems such as the Decisional Diffie-Hellman problem, or the DDH problem for short. This kind of decision problem was firstly introduced in [6] to prove the semantical security of a public-key encryption scheme from a cryptographic point of view. Since then, such a decisional problem has been typically employed to prove the semantical security of public-key encryption schemes such as the ElGamal and Cramer-Shoup encryption schemes [4, 17, 2]. More precisely, the Cramer-Shoup encryption scheme is secure against adaptive chosen ciphertext attack under the DDH and the universal one-way hash assumptions. The

*Part of the research was done while the first author was a student in the University of Southern California and the second author was visiting there. The first author was partially support by NSF grant CCR-9820778.

†School of Computer Science, University of Oklahoma, Norman, OK 73019, USA

‡NTT Laboratories, 1-1 Hikarinooka, Yokosuka-shi, 239-0847 Japan

DDH problem is especially useful and has a lot of applications, so it has been very attractive to cryptographers. For a survey of the DDH problem, see [13, 1].

1.1 Preliminary

Now, we briefly review the definitions of the DDH and related problems. In the following, G denotes a multiplicative finite cyclic group generated by an element g from G, and let l be the order of G. From a cryptographic point of view, we may assume that l is prime.

- **The Discrete Logarithm problem**: Given two elements x and y, to find an integer m so that $y = x^m$.
- **The Diffie-Hellman problem**: Given two elements g^x and g^y, to find g^{xy}.
- **The Decisional Diffie-Hellman problem**: Given two distributions $(g^x,\ g^y,\ g^{xy})$ and (g^x, g^y, g^z), where x, y, z are randomly chosen from $\mathbf{Z}/l\mathbf{Z}$, to distinguish between these two distributions. In other words, given three elements g^x, g^y and g^z, where x, y, z are chosen at random from $\mathbf{Z}/l\mathbf{Z}$, to decide whether $xy \equiv z \pmod{l}$ or not.

It is easy to see that the Diffie-Hellman problem can be efficiently reduced to the Discrete Logarithm problem and the DDH problem can be efficiently reduced to the Diffie-Hellman problem. So far, the best known algorithm for these problems over a general group, is a generic algorithm such as the Baby-Step Giant-Step (BSGS) and Pohlig-Hellman. Their run time are given by $O(\sqrt{l})$, where l is the order of the base group G. Besides, Shoup [16] showed that the lower bound on computation of the DDH problem is the same as that of the Discrete Logarithm problem under the generic model, i.e., the lower bound is given by $c\sqrt{l}$, where c is some constant, for the DDH problem as well as the Discrete Logarithm problem. More precisely, Shoup showed that an algorithm such as the BSGS is the best possible generic algorithm for the DDH, Diffie-Hellman and Discrete Logarithm problems.

When it comes to relationships between these problems, Maurer and Wolf [10] showed that the Discrete Logarithm problem can be reduced to the Diffie-Hellman problem, if there exists some auxiliary group defined over $\mathbf{F}_l$ and it has certain nice properties. More precisely, the Maurer and Wolf's idea is given by the following. An auxiliary group can be taken as the rational points on an elliptic curve defined over $\mathbf{F}_l$ whose order is sufficiently smooth. We can easily solve the Discrete Logarithm problem over this elliptic curve by using the Pohlig-Hellman algorithm. Furthermore, since we can reduce the Discrete Logarithm problem over G to that over this elliptic curve by employing the Diffie-Hellman oracle, the Discrete Logarithm problem over G can be reduced to the Diffie-Hellman problem. Namely, in this case, we can say that the Diffie-Hellman problem is as hard as the Discrete Logarithm problem.

On the other hand, very recently, Joux and Nguyen [8] presented very interesting examples such that the DDH problem is easy while the Diffie-Hellman problem is as intractable as the Discrete Logarithm problem over certain groups of the rational points on elliptic curves defined over finite fields. It is obvious that the DDH problem over an elliptic curve defined over a finite field is very easy if we can compute a pairing such as the Weil and Tate pairing. Actually, we assume that $\langle\ ,\ \rangle_l$ is the l-th Tate pairing, where l is prime and also the DDH problem over the group generated by a point P whose order is prime l, then we have $\langle xP, yP\rangle_l = \langle P, P\rangle_l^{xy}$ and

$\langle zP, P\rangle_l = \langle P, P\rangle_l^z$. So, in this case, deciding whether $xy \equiv z \pmod{l}$ or not is very easy unless $\langle P, P\rangle_l = 1$. Anyhow, in such a case, the DDH problem can be solved in polynomial time on the size of the input. Here we note that we are not able to evaluate the Tate pairing for all elliptic curves but special classes of curves such as supersingular and trace 2 elliptic curves. Besides, as mentioned above, according to the result by Maurer and Wolf, if we can generate some auxiliary group for these elliptic curves which satisfy certain good properties, the Diffie-Hellman problem is as hard as the Discrete Logarithm problem. That is, Joux and Nguyen presented supersingular and trace 2 elliptic curves with such good auxiliary groups (see for details in [8]).

This observation raises the following question: Is there an efficient reduction from the DDH problem in a finite field to the DDH problem over some special elliptic curve? This paper will explore the possibility.

1.2 Our results

This paper proposes an attack against the DDH problem in finite fields, whose efficiency relies on the number of torsion points on an elliptic curve over number fields. Suppose that our target finite field is $\mathbf{F}_p$. The prime l is the largest prime factor of $p-1$. Let K be a number field and $[K : \mathbf{Q}] = d$ and $\mathcal{E}$ an elliptic curve defined over K. The celebrated Uniform Boundedness Theorem asserts that the number of K-ratinal torsion points on E is bounded by a constant B_d depending only on d. Current version of UBT shows that the bound B_d depends exponentially on d. If this bound is effective, then for a prime l, there exist a number field K and an elliptic curve $\mathcal{E}/K$ such that $[K : \mathbf{Q}] \leq \log^{O(1)} l$ and $\mathcal{E} : cy^2 = x^3 + ax + b$ has non-trivial K-rational l-torsion points. In addition, assume

1. $\mathcal{E}$ has multiplicative reduction E' at a place above p;
2. All the K-rational l-torsions reduce to non-singular points on E';
3. The y-coordinates of all the torsions have low heights.

We can efficiently map the elements in the l-part of the $\mathbf{F}_p^*$ to the points on E'. Suppose that p-adic representation of $\mathcal{E}$ of certain precision is given, we then find the p-adic representations of the corresponding torsions on $\mathcal{E}$ up to the precision, namely, we lift the points on E' to the torsions on $\mathcal{E}$. Lifting to torsions instead of regular points has several potential advantages. 1) the heights of torsions may not explode by multiplication of a big number, while the heights of regular points certainly do. After all, the height will get back to 0 if we multiple the order. 2) it is much easier to calculate the lifted point, because in addition to the curve equation, we have one more equation defining the torsion. There is no problem to compute the p-adic coordinates of the global torsions up to any precision. Since the degree of K is low, we employ **LLL**-algorithm to get the minimum polynomials of the coordinates of the points.

There is a disadvantage with lifting to torsions. We cannot apply the 2-descent method to solve the discrete logarithm problem among global points (torsions). Fortunately since the reduction will preserve the group structure of torsions, we can reduce the curve modulo another prime in hope that the DDH problem over the new curve (defined over a new finite field) becomes easier. There certainly exists a prime r, such that $l|r-1$ and $\mathcal{E}$ has good reduction E'' at a place above r. The coordinates of the corresponding points on E'' will be computed. Note that over finite

fields the y-coordinates will uniquely determine the x-coordinates at a large fraction of the points. The Tate-pairing on the l-part of $E'(\mathbf{F}_r)$ is non-trivial and is efficiently computable. Hence we have the reduction of DDH problem in finite fields to DDH problem over special elliptic curves. This concludes the whole reduction, which can be illustrated by following picture. Our result

$$\begin{array}{ccc} & \mathcal{E}(K) & \\ \nearrow & & \searrow \\ E'(\mathbf{F}_q) & & E''(\mathbf{F}_r) \\ \uparrow & & \\ \mathbf{F}_q^* & & \end{array}$$

illustrates intriguing connections between two seemly unrelated problems:

- The hardness assumption of the Decisional Diffie-Hellman problem.
- The effective bound in UBT.

A statement on one of the problems has implication on the other problem. Another interesting feature of our algorithm is *prime shifting*, namely, we actually reduce the problem over one finite field to the problem over another finite field with different characteristic.

1.3 Non-uniform algorithm

In this paper, when we talk about non-uniform polynomial time algorithm to solve DDH problem, we mean that given a cyclic group G with generator g, there exists an random algorithm $A_{G,g}$, depending on G and g, such that if the input of the circuit is g^x, g^y, g^z, output 1 iff $z \equiv xy \pmod{|G|}$, and the time complexity of the algorithm C_G grows polynomially with $\log|G|$. If we know how to design such an algorithm efficiently given G and g, then we have a uniform polynomial time algorithm to solve DDH problem.

Perhaps the best known non-uniform algorithm in cryptography is the reduction from DH problem to DL problem, proposed by Maurer and Wolf [10]. Given an arbitrary finite field $\mathbf{F}_p$, it is not known how to construct an elliptic curve over $\mathbf{F}_p$ with sufficiently smooth order. Sometimes, even the existence of such a curve is in question.

This paper is organized as follows. First, we introduce the reduction from the multiplicative group of a finite field to the additive group on a singular cubic curve. In the section 3, we formulate the main theorem. In the section 4, we describe an algorithm to lift the points over finite field to torsions over number field, and discuss the idea of shifting prime and prove the main theorem. In the section 5, we apply the idea to elliptic curve discrete logarithm problem.

2 Reduction from finite field to singular cubic curve

We first fix some notations. Suppose we are given a prime p, $g \in \mathbf{F}_p^*$ generate a subgroup S. Assume that $l = |S|$ is a prime. $a, b, c \in S$. Certainly there exist three integers x, y and z such

that $a = g^x, b = g^y, c = g^z$. We want to determine whether $xy \equiv z \bmod l$. This is called the DDH problem over $\mathbf{F}_p$.

There is an analogy problem in elliptic curve cryptography. Given a curve E defined over a finite field $\mathbf{F}_q$. W.l.o.g., assume that the order of $E(\mathbf{F}_q)$ is a prime l. Let G be a generator of $E(\mathbf{F}_q)$. $A, B, C \in E(\mathbf{F}_q)$. There exist three integers x, y and z such that $A = xG$, $B = yG$ and $C = zG$. The DDH problem is to determine whether $xy \equiv z \bmod l$.

It is believed that in general the DDH problem over an elliptic curve is harder than the DDH problem in a finite field if the groups have the same size. However, in some special case, most notably when the Tate-pairing is non-trivial and is easy to compute, DDH problem over the elliptic curve admits polynomial time algorithm.

It turns out that the isomorphism from the multiplicative group of a finite field to the additive group of a cubic curve is well-known, and is efficiently computable, as shown in the following proposition. However, it is not scientifically interesting in its own regard because the cubic curve is singular, hence the Tate-pairing is trivial.

Proposition 1 *Let K be a finite field and E/K be a curve given by*

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4 + a_6$$

with discriminant $\Delta = 0$. Suppose E has a node S, and let

$$y = \alpha_1 x + \beta_1 \quad \text{and} \quad y = \alpha_2 x + \beta_2$$

be the two distinct tangent lines to E at S. The the map ϕ

$$\begin{array}{rcl} E_{ns} & \rightarrow & \bar{K}^* \\ (x, y) & \rightarrow & \dfrac{y - \alpha_1 x - \beta_1}{y - \alpha_2 x - \beta_2} \end{array}$$

is an isomorphism of abelian groups, which can be computed efficiently. The reverse map can also be computed efficiently.

3 The Main Theorem

We can imagine that there is a elliptic curve over a number field, which has a multiplicative reduction at p or a place above p. The Tate pairing on this global curve is non-trivial. By lifting points from the singular cubic curve to the global curve, we are reducing the DDH problem in finite field to the DDH problem over the global elliptic curve.

The approach sounds appealing. But we are required to lift points over finite field to torsion points over number field. The group order over the finite field is usually very large in cryptography application. One of the obstacles is to describe the global curve, since the curve, as well as the torsions, may be defined over a number field of very high degree. Further more, even if the curve and its torsions are defined over a number field with low degree, the size of the curve is too large to even be stored. In this paper, we make assumption that the maximum possible number of

torsions over a number field grows exponentially with the degree of the number field. We use the p-adic representation of this curve up to the certain precision.

The biggest obstacle is that some of its l-torsions may have huge size too. Note that if E is represented by Weierstrass equation $y^2 = x^3 + ax + b$, $a, b \in \mathbf{Z}_K$, then the l-torsions have very large coordinates. But all the y-coordinates share a lot of common factors. This prompts us to use the representation $cy^2 = x^3 + ax + b$. If c is chosen properly, the height of the y-coordinates of the torsion may be small. Moreover, for a large fraction of the points, the y uniquely determines x, because in those cases, $x^3 + ax + (b - cy^2) = 0$ has only one solution in the field of interest. It is sufficient to require the y-coordinates to be small.

Definition 1 *The height of an integer n, denoted by $ht(n)$, is defined to be $\log(|n| + 1)$. The height of a rational number $\frac{n}{m}$, $n, m \in \mathbf{Z}, (n, m) = 1$, is defined to be $ht(n) + ht(m)$. The height of an integral polynomial $\sum_{i=0}^{n} a_i x^i$ is $\sum_{i=0}^{n} ht(a_i)$ The height of an algebraic integer is the height of its minimum polynomial over $\mathbf{Q}$.*

Theorem 1 *Given a prime p, there exists a random polynomial time algorithm to solve the DDH problem in $\mathbf{F}_p^*$, if for some (absolute) constant c, there exists an elliptic curves $\mathcal{E} : cy^2 = x^3 + ax + b$ over a number field K, satisfy the following conditions.*

1. *The number field $K = \mathbf{Q}[x]/(k(x)) = \mathbf{Q}(\alpha)$ has extension degree $[K : \mathbf{Q}] \leq (\log p)^c$. The polynomial $k(x) \in \mathbf{Z}[x]$ is separable over $\mathbf{F}_p$, its height is bounded by $(\log p)^c$, and it splits completely over $\mathbf{F}_p$. (Hence $K \subseteq \mathbf{Q}_p$.)*
2. *There are l-torsion points $P_1, P_2, ..., P_l = 0 \in \mathcal{E}(K)$, where l is the largest prime divisor of $p - 1$. The curve $\mathcal{E}$ has a multiplicative reduction to E at place v above p, all P_i's reduce to non-singular points. All the factors of $p - 1$ other than l are less than $\log^c p$.*
3. *Let $P_i = (x_i, y_i) \in f$, $1 \leq i \leq l$. Then for all i, the height of y_i are less than $(\log p)^c$.*

We would like to mention several very deep results proved by Mazur [11], Kamienny [9], Merel [12], Parent [14], Hindry and Silverman [7] respectively about the torsions on the elliptic curves.

Proposition 2 *Let $\mathcal{E}$ be an elliptic curve over a number field K. We denote the order of the torsion subgroup of $\mathcal{E}(K)$ by N. Let $d = [K : \mathbf{Q}]$. Suppose that p is a prime divisor of N, and p^n the largest power of p dividing N*

1. *If $d = 1$, the torsion subgroup of $\mathcal{E}(\mathbf{Q})$, is isomorphic to one of the following groups: $\mathbf{Z}/m\mathbf{Z}$ for $m \leq 10$, or $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2m\mathbf{Z}$ for $m \leq 4$.*
2. *If $d = 2$, there is a positive integer B such that $N \leq B$. Moreover, $p \in \{2, 3, 5, 7, 11, 13\}$.*
3. *We have*

$$\begin{aligned} p &\leq (1 + 3^{d/2})^2 \\ p^n &\leq 65(3^d - 1)(2d)^6. \end{aligned}$$

4. *If the curve $\mathcal{E}$ has good reduction everywhere, then the number of K-rational torsion points of $\mathcal{E}$ is bounded by $1\,977\,408 d \log d$.*

4 Torsion-to-torsion Lift and Shifting Primes

In this section, we describe an algorithm to lift the points over finite field (which are certainly torsions) to torsion points over number field. Assume the conditions in the main theorem hold, and we use the same notation as in the above section. First we fix one embedding:

$$K \to \mathbf{Q}_p,$$

by mapping α to one of p-adic roots of $k(x)$. If a p-adic number a is an image of $x \in K$ by this embedding, then the minimum polynomial over $\mathbf{Q}$ of x can be computed in polynomial time on $\log p$ and the size of the minimum polynomial. In the computing, we only need know the first m digits of a, where m is also bounded by polynomial on $\log p$ and the size of the minimum polynomial.

Let

$$\tilde{f}(x, y) = 0$$

be p-adic representation of $\mathcal{E} : cy^2 - x^3 - ax - b = 0$ up to m digits, where m will be set later. Let $F(x, y)$ be $\tilde{f} \bmod p$. $F(x, y) = 0$ is a singular cubic curve with a node. Suppose we want to solve the DDH problem in subgroup S of $\mathbf{F}_p^*$ with order l, where $l|p-1$ is a prime. For any point $Q = (a, b) = \phi^{-1}(x)$ on F (See proposition 1 for the definition of ϕ),

$$lQ = 0 \bmod p.$$

There is a l-torsion point $P = (x, y)$ on f which will reduce to Q. We first calculate the p-adic representation of P.

Let $P = (a + a_1p + a_2p^2 + \cdots, b + b_1p + b_2p^2 + \cdots)$. Using squaring technique, we get a linear equation on a_1 and b_1 from

$$l(a + a_1p, b + b_1p) = 0 \bmod p^2,$$

combined with the curve equation,

$$\tilde{f}(a + a_1p, b + b_1p) = 0 \pmod{p^2},$$

we can solve a_1 and b_1 efficiently. Note that a_1 or b_1 only occur in linear terms. Similarly, from

$$\begin{cases} l(a + a_1p + a_2p^2, b + b_1p + b_2p^2) = 0 \pmod{p^3} \\ \tilde{f}(a + a_1p + a_2p^2, b + b_1p + b_2p^2) = 0 \pmod{p^3} \end{cases}$$

we can get a_2 and b_2. Generalize this idea, we will obtain the p-adic representation up to m digital in time $(m \log p)^{O(1)}$.

On the other hand, we know that the minimum polynomials of y have coefficients whose sizes are bounded by $(\log p)^c$. Those polynomial, denoted by h, can be computed using **LLL**-algorithm when m is big enough. By factoring h over K, we get the representation of y as elements in K. There certainly exists a prime r, satisfying

1. $l|r-1$ and $l^2 \not| r-1$.
2. There is a place u over r with degree 1 in K.

3. The reduction of $\mathcal{E}$ at place u is non-singular, hence it is an elliptic curve.

Fix an embedding:

$$K \to \mathbf{Q}_r.$$

Let E'' be the reduction of f at place u. All the l-torsion points will reduce to a $\mathbf{F}_r$-rational points on g. They form a subgroup in $E''(\mathbf{F}_r)$. The calculate of Tate-pairing on this subgroup is non-trivial and efficient.

If any of the a, b or c is not mapped to a point where y uniquely determines x, then we use randomness to fix the problem. It is easy to see that the DDH problem at (a, b, c) has the same answer as the problem at $(ag^{a_1}, bg^{a_2}, ca^{a_2}b^{a_1}g^{a_1a_2})$ for any a_1, a_2. The algorithm is summarized in the following:

Non-uniform information: p; The p-adic representation of $\mathcal{E}$ up to to m digits; Prime r; The reduction of f at place u.

Input: $a, b, c \in \mathbf{F}_p$.

1. From p-adic representation of $\mathcal{E}$, compute $E' = \mathcal{E} \bmod p$. We get a singular cubic curve with a node.
2. Compute $A' = \phi^{-1}(a)$, $B' = \phi^{-1}(b)$, $C' = \phi^{-1}(c)$ on E'.
3. Fix $K \to \mathbf{Q}_p$.
4. Lift A', B' and C' to A, B and C on $\mathcal{E}$. We compute the p-adic representations of A, B and C first. Then we use **LLL**-algorithm to compute $A, B, C \in K^2$.
5. Fix $K \to \mathbf{Q}_r$. Let A'', B'' and C'' be the reduction of A, B and C on E''. If for any of the points, the y-coordinate doesn't uniquely determine x, then pick two random numbers a_1 and a_2, let $a \leftarrow ag^{a_1}, b \leftarrow bg^{a_2}, c \leftarrow cb^{a_1}a^{a_2}g^{a_1a_2}$, go to step 2.
6. Solve DDH problem of A'', B'' and C''. Output the answer.

Here we note that, since the prime l satisfies that $l^2 \not| r - 1$, so we can evaluate the l-th Tate-pairing $\langle A'', A'' \rangle_l \neq 1$ (See [8, 5]). That is, we can solve the DDH problem A'', B'' and C''.

The time complexity depends on the degree of the number field where $\mathcal{E}$ is defined and has a large torsion group. It is polynomial if the conditions in the main theorem hold. The algorithm is non-uniform, because for every p, we need the p-adic representation of f, the special prime r and the reduction of f modulo the place u. We don't know how to compute these parameters even they do exist.

5 Application to the elliptic curve discrete logarithm

Let $\mathcal{E}$ be a curve defined over a number field K. $\mathcal{E}_{\text{tor}}(K)$ has order l. For simplicity, we assume that l is a prime. Assume that $\mathcal{E}$ has good reduction $E/\mathbf{F}_q$ at place v. W.l.o.g, we assume that $|E(\mathbf{F}_q)| = l$.

Corollary 1 *Given $E(\mathbf{F}_q)$, there exists a subexpontial algorithm to solve the discrete logarithm on $E(\mathbf{F}_q)$, if there is a constant c such that,*

1. *$K = \mathbf{Q}[x]/k(x) = \mathbf{Q}[\alpha]$, $[K : Q] \leq (\log p)^c$. The polynomial $k(x) \in \mathbf{Z}[x]$ is separable and it splits completely over $\mathbf{F}_p$. The heights of all the coefficients of $k(x)$ are bounded by $(\log p)^c$.*

2. *There are l-torsion points $P_1, P_2, ..., P_l = 0 \in \mathcal{E}(K)$. They form a group.*

3. *$\mathcal{E}$ can be represented by an equation*

$$cy^2 = x^3 + ax + b$$

such that for any $1 \leq i \leq l$, if $P_i = (x_i, y_i)$, the minimum polynomials in $\mathbf{Q}[x]$ for y_1 is $h_i(x) = 0$, then the height of all the coefficients of h_1 are bounded by $(\log p)^c$.

Sketch of the proof: If the conditions in the corollary hold, then there must exist a prime p such that $r|p-1$ and the reduction of $\mathcal{E}$, denoted by $E''/\mathbf{F}_p$, at place u above p is non-singular. Because $\mathcal{E}$ has a torsion group over K, $E''(\mathbf{F}_p)$ has l-part subgroup and the Tate-pairing of elements in the subgroup can be efficiently computed. We can apply FR-algorithm here [5]. Hence the discrete logarithm over the r-part of $E(\mathbf{F}_q)$ has non-uniform subexpontial time solution.

6 Acknowledgments

We thank Dr. Ming-Deh Huang, Dr. Sheldon Kamienny and Dr. Len Adleman for helpful discussions.

References

[1] D. Boneh. The decisional Diffie-Hellman problem. In *Proc. of ANTS-IV*, volume 1423 of *Lecture Notes in Computer Science*, pages 48–63. Springer-Verlag, 1998.

[2] R. Cramer and V. Shoup. A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack. In *Proc. CRYPTO 98*, Lecture Notes in Computer Science, pages 13–25. Springer-Verlag, 1998.

[3] W. Diffie and M.E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6):644–654, 1976.

[4] T. ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory*, 33:469–472, 1985.

[5] G. Frey and H.G. Ruck. A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves. *Mathematics of Computation*, 62(206):865–874, 1994.

[6] S. Goldwasser and S. Micali. Probabilistic encryption. *Journal of Computer and System Sciences*, 28:270–299, 1984.

[7] M. Hindry and J. Silverman. On the number of rational torsion points on an elliptic curve. *C. R. Acad. Sci. Paris Ser. I Math.*, 329(2):97–100, 1999.

[8] A. Joux and K. Nguyen. Separating decisional Diffie-Hellman from Diffie-Hellman in cryptographic groups. Preprint. `http://eprint.org/2001/003`.

[9] S. Kamienny. Torsion points on elliptic curves. *Bull. Amer. Math. Soc. (N.S.)*, 23(2):371–373, 1990.

[10] U. Maurer and S. Wolf. The relationship between breaking the Diffie-Hellman protocol and computing discrete logarithms. *SIAM J. Comput.*, 28(5):1689–1731, 1999.

[11] B. Mazur. *Rational points on modular curves*, volume 601 of *Lecture Notes in Mathematics*. Springer-Verlag, 1976.

[12] L. Merel. Bounds for the torsion of elliptic curves over number fields. *Invent. Math.*, 124(1-3):437–449, 1996.

[13] M. Naor and O. Reingold. Number theoretic constructions of efficient pseudo random functions. In *Proc. 38th IEEE Symp. on Foundations of Comp. Science*, pages 458–467, 1997.

[14] P. Parent. Effective bounds for the torsion of elliptic curves over number fields. *J. Reine Angew. Math*, 506:85–116, 1999.

[15] R. Rivest, A. Shamir, and L.M. Adleman. A method for obtaining digital signatures and public key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.

[16] V. Shoup. Lower bounds for discrete logarithms and related problems. In *Proc. of Eurocrypto*, volume 1233 of *Lecture Notes in Computer Science*, pages 256–266. Springer-Verlag, 1997.

[17] Y. Tsiounis and M. Yung. On the security of elgamal based encryption. In *Proc. of PKC'98*, volume 1431, pages 117–134. Springer-Verlag, 1998.