Approximate ℓ-th roots modulo n

Brigitte VALLÉE,
GREYC, Université de Caen, F-14032 Caen Cedex, France

January 23, 2002

Abstract

The security of ESIGN is based on the difficulty of computing approximate ℓ-th roots modulo a composite number n of the form $n = p^2 q$ with distinct primes p, q of the same size. We first recall the general framework of this approximation problem, and we describe the ESIGN scheme. The security of this scheme is based on the difficulty of finding elements of some set that we call $B_c^{[\ell]}$. Then, we ask important questions in four main directions:

(1) What can be said about the distribution of $B_c^{[\ell]}$ inside $Z(n)$?
(2) Can we describe in a geometrical and efficient way the elements of this set?
(3) Can we apply lattice methods to find elements of this set (always in a efficient way)?
(4) Can we use the signatures of this scheme to find some information about the set $B_c^{[\ell]}$?

Approximating ℓ-th roots mod n : three notions of approximation. The problem of finding exact ℓ-th roots mod n, (namely, when y_0 is given, finding x_0 such that $x_0^\ell = y_0 \bmod n$) is surely difficult when the modulus n is composite, with unknown factorisation. In this case, one usually considers "easier" problems where some approximations can be made on variables x, y.

Let $Z(n)$ denote the ring of integers mod n. Given a pair $(x_0, y_0) \in Z(n)^2$, one searches for some another pair (x, y) that is close to (x_0, y_0) and satisfies $x^\ell = y \bmod n$. There are three different approximation problems, according as approximations are allowed on variable x, on variable y, or on both variables x, y. In all the cases, the allowed approximations on variable x (resp. on variable y) are of the form n^a (resp. n^b).

(I) [x-approximation]. Find x near x_0 such that $x^\ell = y_0 \bmod n$

(II) [y-approximation]. Find x such that $x^\ell \bmod n$ is near y_0

(III) [(x,y)–approximation]. Find x near x_0 and y near y_0 such that $x^\ell = y \bmod n$

The main result on Problem (III) is due to Vallée, Girault, Toffin [4], [12]:
Let (a, b) satisfy

$$a\frac{\ell(\ell-1)}{2} + b = 1 - \epsilon \quad \textit{with} \quad b \geq \ell a.$$

The pairs (x, y) that satisfy $|x - x_0| \leq n^a, |y - y_0| \leq n^b$, and $x^\ell = y \bmod n$ can be found in polynomial time.

The best solution to Problem (I) is due to Coppersmith [2]. Previous solutions to Problem (I) were given by Hastad [5] and Vallée, Girault, Toffin [4], [12] around 1986–1988. These authors proved

that Problem (I) can be solved in polynomial time provided that

$$a \leq \frac{2}{\ell(\ell+1)} - \epsilon.$$

Later, in 1996, Coppersmith improved this bound since he showed that Problem (I) can be solved in polynomial time in $(\ell, 1/\epsilon, \log n)$ provided that

$$a \leq \frac{1}{\ell} - \epsilon.$$

Problem (II) was less studied, and, so far, the solutions are obtained in fact by reducing Problem (II) to Problem (III). However, Problem (II) is the basis to the ESIGN scheme that is now described.

The ESIGN scheme: a particular case of Problem (II) when $n = p^2q$ and $b = 2/3$. The ESIGN scheme deals with Problem (II) in the particular case when the modulus n is composite, of the form $n = p^2q$ with p, q distinct primes. The approximation fraction is $b = 2/3$, and more precisely, the scheme uses an approximation interval of length pq.
Let $Z_p(n)$ be formed with elements of $Z(n)$ coprime with p. Each element x of $Z_p(n)$ can be written as $x = r + tpq$ with $0 \leq r < pq$, $\gcd(r, p) = 1$ and $0 \leq t < p$. The ESIGN scheme described in [7] or [8] deals with the set $B_c^{[\ell]}$,

$$B_c^{[\ell]} = \{x \in Z(n) \quad \text{for which } x^\ell \bmod n \quad \text{satisfies} \quad c \leq x^\ell \bmod n < c + pq\}.$$

The point x belongs to $B_c^{[\ell]}$ if and only if

$$0 \leq (r^\ell + \ell t r^{\ell-1} pq - c) \bmod n < pq.$$

If we let $r^\ell - c = w_0 pq - w_1$ with $0 \leq w_1 < pq$, we remark that we have also $(r^\ell - c) \bmod n = (w_0 \bmod p)pq - w_1$, and we obtain

$$(x^\ell - c) \bmod n = -w_1 + [(\ell t r^{\ell-1} - w_0)]pq \bmod n$$

so that the point x belongs to $B_c^{[\ell]}$ if and only if

$$\ell t r^{\ell-1} - w_0 = 0 \bmod p \quad \text{with} \quad w_0 \bmod p = \lceil \frac{(c - r^\ell) \bmod n}{pq} \rceil.$$

We denote by ϕ the function $\phi : Z_p(pq) \to Z(p)$ which associates to r the number $t \bmod p$. So, the function ϕ is defined by

$$\phi(r) := \lceil \frac{c - r^\ell}{pq} \rceil \frac{1}{\ell r^{\ell-1}} \bmod p = \lceil \frac{(c - r^\ell) \bmod n}{pq} \rceil \frac{1}{\ell r^{\ell-1}} \bmod p. \tag{1}$$

Then, for each value of $r \in Z_p(pq)$, there exists exactly one value of $t \in Z(p)$ [namely $t = \phi(r)$] for which $r + \phi(r)pq$ belongs to $B_c^{[\ell]}(n)$. Finally, the set $B_c^{[\ell]}(n)$ has cardinality $q(p-1)$ and has a precise description given by

$$B_c^{[\ell]}(n) = \{x = r + \phi(r)pq, \quad r \in Z_p(pq)\}$$

Then the ESIGN scheme is based on the following fact: *The set of valid ESIGN signatures coincides with the set $B_c^{[\ell]}(n)$. In another words, all the elements $B_c^{[\ell]}$ provide valid ESIGN signatures for a message c and there are exactly $q(p-1)$ valid ESIGN signatures for such a message c.*

Distribution of the set $B_c^{[\ell]}$. What can be said about the distribution of $B_c^{[\ell]}$? In [7] and [8], the authors state –without any proof– that the distribution of $B_c^{[\ell]}$ is uniform inside $Z(n)$. However, for the author of this report, it is not clear if the statement is true; anyway, the proof of this fact seems to be difficult to obtain.

The study of the distribution of $B_c^{[\ell]}$ inside $Z(n)$ is closely linked to the properties of function $\phi : Z_p(pq) \to Z(p)$ defined by (1). The distribution of $B_c^{[\ell]}$ inside $Z(n)$ is "nearly" uniform if, for each $t \in Z(p)$, the subset $\phi^{-1}(\{t\})$ has about the same cardinality (i.e., a cardinality near to $q(p-1)/p \simeq q$). In this case, each subset of $Z_p(n)$ of the form $[tpq, (t+1)pq[\cap Z_p(n)$ contains a number of elements of $B_c^{[\ell]}$ close to q, and then the distribution of $B_c^{[\ell]}$ is nearly uniform inside $Z_p(n)$.

On the other side, it is proven that, for any exponent $\ell \geq 2$, and any $c \in Z(n)$, there exist exactly $q(p-1)$ elements s coprime with p for which the powers $s^\ell \bmod n$ belong to some interval $[c, c+pq[$. In [6], Mahassni and Shparlinski has proven the more precise result:

Let n be a composite number of the form $n = p^2 q$ with p, q two distinct primes that satisfy $\gcd(p, q-1) = 1$. For any $\delta > 0$ and for any "random" exponent ℓ, the powers $s^\ell \bmod n$ are uniformly distributed in any interval $[c, c+h]$ of length $h \geq n^{1/2+\delta}$.

Geometrical description of $B_c^{[\ell]}$ for $\ell = 2$. When $\ell = 2$, Vallée [10] has precisely studied the distribution of $B = B_0^{[2]}$; she proved that it is not quite uniform, but "quasi-uniform" inside $Z(n)$, for any modulus n, prime or composite. These results show that the distribution of B is essentially independent of the arithmetical properties of modulus n. She first observed in numerical experiments two important facts.

First, the gaps between successive elements of B may have large variations near the rationals $pn/(2q)$, of small denominator q, but their distribution appears to follow a definite pattern inside a *sufficiently small interval* around $pn/(2q)$. There appear sequences of gaps all equal to q, separated by much larger gaps. This pattern seems to vanish when going away from $pn/(2q)$. On the other side, there is a balance between these gaps so that the total number of B's elements inside a *sufficiently large interval* around $pn/(2q)$ is almost the same as if the distribution of B in the whole $Z(n)$ was actually uniform.

It appears that *the length of a convenient interval is inversely proportional to q*: She lets $h = 4n^{2/3}, k = n/h = (1/4)n^{1/3}$. She builds a particular covering of $Z(n)$, the Farey covering of order k, which is made with intervals $I(p,q)$ of center $pn/(2q)$ and radius $n/(2kq) = h/(2q)$, with $|p| \leq q \leq k$ and $(p,q) = 1$.

Inside each interval, she makes a local use of lattices of $\mathbf{Z}^2$. If x_0 is near a rational number $pn/(2q)$ of small denominator, the elements of B near x_0 lead to points of a lattice $L(x_0)$ between two parabolas. More precisely, the lattice $L(x_0)$ is generated by the two vectors $(1, 2x_0)$ and $(0, n)$; if $x = x_0 + u$ is an element of $Z(n)$, one has: $x^2 \bmod n = x_0^2 + 2x_0 u + u^2 + tn$ and, if if one lets $w = 2x_0 u + tn$, one has the equivalence

(i) $x = x_0 + u$ belongs to B,

(ii) there exists w so that the point $m(x) = (u, w)$ belongs to $L(x_0)$ and lies between the two parabolas with respective equations: $w + u^2 + x_0^2 = h$ and $w + u^2 + x_0^2 = -h$.

If now x_0 is the integer nearest to the rational $pn/(2q)$ with a small denominator q, the domain $P(p,q)$, formed with the points $m(x)$ of $L(x_0)$ arising from the points x of $B \cap I(p,q)$, for two integers p and q satisfying $|p| \leq q \leq k$, and $(p,q) = 1$, can be easily described with the basis formed

with the vectors

$$\vec{r} = q(1, 2x_0) - p(0, n), \quad \vec{s} = q'(1, 2x_0) - p'(0, n)$$

that comes from the pair (p', q') relative to the adjacent interval $I(p', q')$ in the Farey covering. Finally, she obtains the following result:

The points of the lattice $L(x_0)$ lie on quasi-horizontal lines which cut on the vertical axis segments of length equal to n/q; moreover, on each line, the points of $L(x_0)$ have horizontal gaps equal to q. From one line to the next, the points of $L(x_0)$ are shifted with an horizontal spacing equal to q' in absolute value.

Vallée uses these results to exhibit two polynomial–time algorithms: the first one draws elements from B in a quasi–uniform way. The second one finds the nearest neighbors (in B) of a point x of $Z(n)$.

A geometrical description of $B_c^{[\ell]}$ for $\ell > 2$? One can try to generalize these geometrical arguments. The points x of $B_c^{[\ell]}$ are exactly the x-coordinates of points (x, y) of $\mathbf{Z}^2$ that are between the two curves $yn = x^\ell - c$ and $yn = x^\ell - c - n^{2/3}$. Elkies describes in [3] an algorithm that finds integer points "near" an algebraic curve.

Now, we try to adapt Elkies' ideas to the ESIGN framework. We consider the domain

$$\mathcal{A} := \{(x, y),\ 0 \leq x < n,\ 0 \leq x^\ell - c - yn \leq n^{2/3}\}.$$

The two "parallel" curves $yn = x^\ell - c$ and $yn = x^\ell - c - n^{2/3}$ are at distance $n^{-1/3}$, and, since x belong to $Z(n)$, the measure of the total area of the domain $\mathcal{A}$ is about $n^{2/3}$. The idea of Elkies is to partition the total domain in $O(n^a)$ small domains of measure $O(n^b)$ (with $a + b$ near $2/3$) so that, one can hope to find easily some point of Z^2 in each small domain. So, we consider here a partition of $Z(n)$ with $O(n^a)$ intervals I_m of length $O(n^b)$ that gives rise to a partition $\mathcal{A}_m^{[b]}$ of $\mathcal{A}$,

$$\mathcal{A}_m^{[b]} := \{(x, y),\ x \in I_m,\ 0 \leq x^\ell - c - yn \leq n^{2/3}\}.$$

The area of each $\mathcal{A}_m^{[b]}$ is about $0(n^{b-(1/3)})$. Then, we try to approximate each subset $\mathcal{A}_m^{[b]}$ by a paralelepiped $\mathcal{P}_m$ that we obtain by a local linear approximation of the two curves.

Then, we have to find a compromise on the length $O(n^b)$ of each interval I_m:

(i) It must be sufficiently large so that the area of $\mathcal{A}_m^{[b]}$, equal to $0(n^{b-(1/3)})$, is itself sufficiently large, so that we can expect that it contains at least a point of $\mathbf{Z}^2$. We have thus to choose

$$b > \frac{1}{3}.$$

(ii) It must be sufficiently small, so that the parallelepiped $\mathcal{P}_m$ gives a good approximation of the domain $\mathcal{A}_m$. Inside each domain $\mathcal{A}_m^{[b]}$, the maximum distance between the line that gives the best approximation of the curve $yn = x^\ell - c$ and the curve $\mathcal{C}$ itself is of order $O(n^{b(\ell-1)-1})$. However, the two curves $yn = x^\ell - c$ and $yn = x^\ell - c - n^{2/3}$ are at distance $n^{-1/3}$. Then, the condition

$$b(\ell - 1) - 1 < \frac{-1}{3}, \quad \text{i.e.,} \quad b < \frac{2}{3(\ell - 1)}$$

is necessary to insure that the parallepiped $\mathcal{P}_m$ and domain $\mathcal{A}_m$ have a non negligeable intersection. So, this compromise seems to be impossible to obtain, as soon as the exponent ℓ satisfies $\ell > 3$.

The VGT method. The method can be described as follows: Given an integer $\ell \geq 2$ and a pair (x_0, y_0) of two elements of $Z(n)$, VGT consider the equation

$$(x_0 + u)^\ell \ = \ y_0 + v \mod n,$$

and, through a binomial expansion,

$$x_0^\ell + \ C_\ell^1 x_0^{\ell-1} u + ...+ \ \mathbf{C}_\ell^i x_0^{\ell-i} u^i \ + ...+ \ C_\ell^1 x_0 u^{\ell-1} \ + \ u^\ell - v \ = y_0 \mod n.$$

They let $w_i = u^i$ for $1 \leq i \leq \ell - 1$ and $w_\ell = v - u^\ell + (y_0 - x_0^\ell)$, and they consider the lattice $\mathcal{L}$ of the vectors $w = (w_1, w_{2,...}, w_\ell)$ of $\mathbf{Z}^\ell$ such that

$$\sum_{i=0}^{\ell-1} C_\ell^i x_0^{\ell-i} \ w_i \ - w_\ell = 0 \mod n.$$

They have to find, in $\mathcal{L}$, a point w which is –in the sense of an unusual norm– "near" to the point $(0, 0, ..., y_0 - x_0^\ell)$. Lattice $\mathcal{L}$ has the following matrix (ℓ, ℓ)

$$\begin{pmatrix} 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & 0 \\ C_\ell^1 x_0^{\ell-1} & C_\ell^2 x_0^{\ell-2} & C_\ell^3 x_0^{\ell-3} \dots & C_\ell^{\ell-1} x_0 & n & \end{pmatrix}$$

For each component, the prescribed approximation, linked to the choice of the neighbourhoods, is the following one:

$$|w_i| \leq n^{ia} \quad \text{for all} \ \ i : \ 0 \leq i \leq \ell - 1 \ \ \text{and also} \ \ |w_\ell - y_0 + x_0^\ell| \leq 2n^b$$

(For the last condition, they use the hypothesis: $b \geq \ell a$). Generally speaking, these approximations are not equal, and they "expand-contract" the lattice $\mathcal{L}$ into another lattice in which the approximations are made equal, so that the norm sup can be used. The problem now can be solved provided that the product of all the prescribed approximations equals the determinant n of the lattice. This leads to the condition $C(\ell, \epsilon)$:
Let a, b be two real numbers of $[0, 1]$, $\epsilon > 0$ a real number and $\ell \geq 2$ an integer. The pair (a, b) satisfy the conditions $C(\ell, \epsilon)$ if and only if

$$\frac{\ell(\ell-1)}{2} \ a \ + \ \ b \ = \ 1 - \epsilon \ \ \text{and} \ \ b \geq \ell a.$$

Note that the ESIGN scheme deals with $b = 2/3$. So the associate value of a is

$$a_0 = \frac{2}{3\ell(\ell-1)} - \epsilon.$$

The first result of [12] describes the relative spreading of ℓ-th roots and ℓ-th powers.

For $\epsilon > 0$, for $\ell \geq 2$, for a pair (a,b) satisfying $C(\ell)$, there exists an exceptional set $S(\epsilon)$ with $|S(\epsilon)| \leq n^{1-\epsilon}$ such that, for any x_0 not in $S(\epsilon)$, for any y_0, there exists at most one x that satisfies $|x - x_O| \leq n^a$ and $|x^\ell \bmod n - y_0| \leq n^b$.

When applied to the ESIGN framework, this means that the distribution of $B_c^{[\ell]}(n)$ is not too irregular: there is (generally speaking) at most one element of $B_c^{[\ell]}(n)$ in each interval of length n^{a_0}.

The second result of [12] is constructive: *For $\epsilon > 0$, for $\ell \geq 2$, for a pair (a,b) satisfying $C(\ell,\epsilon)$, there exists a polynomial probabilistic algorithm that finds, for each pair $(x_0,y_0) \in Z(n)^2$ with x_0 not in $S(\epsilon)$, the points x (if they exist) that satisfy $|x - x_0| \leq n^a$ and $|x^\ell \bmod n - y_0| \leq n^b$.*

When applied to the ESIGN framework, these results prove that it is possible to decide in polynomial time if an interval of length n^{a_0} contains an element of $B_c^{[\ell]}(n)$. If we suppose that the distribution of $B_c^{[\ell]}(n)$ inside $Z(n)$ is nearly uniform, one has to try n^c intervals of length n^{a_0} with

$$c = \frac{1}{3} - a_0 = \frac{1}{3} - \frac{2}{3\ell(\ell-1)}$$

to find an element of $B_c^{[\ell]}(n)$. Then, except for $\ell = 2$, this method is not efficient since it has a complexity of order $O(n^c)$.

The method of Coppersmith. This method is only useful for solving Problem (I). One has to find small roots u of the polynomial $P(u) = 0 \bmod n$ where $P(u) = (x_0 + u)^\ell - y_0$ and u satisfies $|u| \leq A$. Coppersmith works with the lattice $\mathcal{L}$ generated by polynomials of the family

$$\{(\frac{P(u)}{n})^j \; u^i, 0 \leq i < \ell, 0 \leq j < h\},$$

for some integer h. For each small root u_0, and any polynomial Q of the family, the value $Q(u_0)$ is an integer. The same holds for any polynomial of $\mathcal{L}$, and specially for a short vector V of the lattice $\mathcal{L}$. If this short vector is sufficiently short, one has $|V(u_0)| < 1$ and thus u_0 is a root of polynomial V over $\mathbf{Z}$, so that u_0 is easy to find. The lattice $\mathcal{L}$ has a dimension equal to ℓh. Furthermore, when the polynomials are expressed in the basis $(u/A)^i$, the determinant of the lattice equals

$$D = n^{-\ell h(h-1)/2} A^{\ell h(\ell h-1)/2},$$

and one can hope to find a short vector of norm $0(1)$ if $D^{1/\ell h} = 0(1)$. This is possible if

$$A \leq c(\ell,h) n^{(h-1)/(\ell h-1)}.$$

The exponent of n, namely $\frac{h-1}{\ell h-1}$ differs from $\frac{1}{\ell}$ by some quantity less than $\frac{1}{\ell h}$. This difference can be made arbitrary small by choosing h larger, at the expense of computational complexity. Then, the bound $A = O(n^{(1/\ell)-\epsilon})$ can be achieved with a running time polynomial in $(\ell, 1/\epsilon, \log n)$. Finally, Coppersmith has proven the following result:

It is possible to find in polynomial time ℓ-th roots of $y_0 \bmod n$ if we know an approximation of them of order $n^{(1/\ell)-\epsilon}$.

The question is : Can this method be extended for solving Problem (III)? One has to find small roots (u, v) of $P(u, v) = 0 \bmod n$ where $P(u, v) = (x_0 + u)^\ell - y_O - v$ and (u, v) satisfies $|u| \leq A, |v| \leq B$. One must work with the lattice $\mathcal{L}$ generated by bivariate polynomials of the family

$$\mathcal{P} := \{(\frac{P(u,v)}{n})^j \ u^i, 0 \leq i < \ell, 0 \leq j < h\},$$

for some integer h. For each small root (u_0, v_0), and any polynomial Q of the family, the value $Q(u_0, v_0)$ is an integer. The same holds for any polynomial of $\mathcal{L}$, and specially for a short vector V of the lattice $\mathcal{L}$. If this short vector is sufficiently short, one has $|V(u_0, v_0)| < 1$ and thus (u_0, v_0) is a root of polynomial V over $\mathbf{Z}^2$.
However, there are now two major drawbacks:

(a) it is no longer true that such a root is easy to find, since a single equation is not enough to solve for u_0 and v_0. We have to find another small vector in the lattice, from which we produce another short polynomial W in the lattice $\mathcal{L}$. If we are fortunate in that V and W are algebraically independent, we can solve the problem using resultants techniques.

(b) The family $\mathcal{Q}$ contains ℓh elements linearly independent, so that lattice $\mathcal{L}$ is of rank ℓh. But the family $\mathcal{Q}$ is now expressed in the basis

$$\mathcal{B} = \{(u/A)^r (v/B)^s, \quad \text{with } 0 \leq s < h, 0 \leq r < \ell h\}.$$

Since $\mathcal{B}$ has cardinality ℓh^2, the matrix that expresses $\mathcal{Q}$ in $\mathcal{B}$ is no longer square. Working with the determinant of a lattice given by a non-square matrix is often a "major piece of work" as Nick Howgrave-Graham says. It seems to be the case here, and it is not clear (at least for the author of this report) how to obtain an expression for the determinant of lattice $\mathcal{L}$. We can perhaps use the same methods as in [1].
The Coppersmith approach is not easy to adapt to the bivariate case.

The approximate common divisor. The general design of the "approximate common divisor" algorithm, due to Nick Howgrave-Graham [1], is the following: Given two inputs a_0 and b_0, and bounds X, Y and M, for which one is assured that d divides $(a_0 + x_0)$ and $(b_0 + y_0)$ for some $d > M$ and x_0, y_0 satisfying $|x_0| \leq X, |y_0| \leq Y$, the algorithm outputs the common divisor d or all of the possible ones if more than one exists.

In [1], the following two algorithms are described:
Algorithm 1. Its inputs are two integers a_0, b_0, $a_0 < b_0$ and a real number $\alpha_0 \in [0, 1]$. Let us define $M = b_0^{\alpha_0}$, and $X = b_0^{\beta_0}$, with $\beta_0 < \alpha_0^2$. The algorithm should output all integers $d > M$ such that there exists an x_0 with $|x_0| < X$ and d divides both $a_0 + x_0$ and b_0 or report that no such d exists.
Algorithm 2. Its inputs are two integers a_0, b_0, subject to $a_0 \simeq b_0$ and a real number $\alpha_0 \in [0, 2/3]$. Let us define $M = b_0^{\alpha_0}$, and $X = b_0^{\beta_0}$, with

$$\beta_0 < 1 - \frac{1}{2}\alpha_0 - \sqrt{1 - \alpha_0 - \frac{\alpha_0^2}{2}}.$$

The algorithm should output all integers $d > M$ such that there exist integers x_0, y_0 with $|x_0|, |y_0| < X$ and d divides both $a_0 + x_0$ and $b_0 + y_0$ or report that that is is unlikely that such a such d exists.

The question is: Can this algorithm be useful to recover p or q? Since n is known, it is sufficient to obtain from the public data an interval of length $O(n^{1/12})$ that contains some multiple of p or q, or an interval of length $O(n^{1/3})$ that contains some multiple of pq. Remark that if we are given a signature of $B_c^{[\ell]}$ with a small component r, (i.e., $0 \leq r \leq n^{1/3}$), then this algorithm allows to recover the factorization of $n = p^2 q$. The same situation occurs if one is given two signatures whose r–components are at distance less than $n^{1/3}$ and whose t-components are distinct. However, the probability of such an event is negligible.

Conclusion. The ESIGN scheme was proposed fifteen years ago. Since this date, some attacks were found, only for small exponents ℓ. We have described here various and elaborate tools that can be applied a priori to attack this scheme. However, none of these tools is actually useful: even if these methods are clever, none of them is efficient for $\ell > 4$.

So, we conclude that the ESIGN scheme seems to be secure, even if the exponent ℓ is chosen relatively small $\ell = 8$ for instance.

References

[1] Nick Howgrave–Graham, *Approximate Integer Common Divisors*, Proceedings of the CaLC01 Conference, LNCS (2146), pp 51–66

[2] Don Coppersmith, *Finding Small Solutions to Small Degree Polynomials*, Proceedings of the CaLC01 Conference, LNCS (2146), pp 20-31.

[3] Noam Elkies, *Rational Points near curves and small nonzero $|x^3 - y^2|$ via lattice reduction*, Proceedings of the ANTS IV Conference, LNCS (1838), pp 33-63.

[4] Marc Girault, Philippe Toffin, Brigitte Vallée, *Computation of approximate ℓ-th roots modulo n and applications to cryptography,* Proceedings of Crypto-88, Santa-Barbara, August 1988, LNCS (403) pp 403-418.

[5] J. Hastad, *On using RSA with low exponent in a public key network*, Proceedinngs of CRYPTO'85, LNCS (218), pp 403-408.

[6] Edwin El Mahassni, Igor Shparlinski, *On some uniformity of distribution properties of ESIGN* preprint.

[7] Tatsuaki Okamoto, Akira Shiraishi, *A fast signature based on quadratic inequalities,* Proc. of the ACM Symposium on Security and privacy, ACM Press (1985), pp 123–132.

[8] Tatsuaki Okamoto, *A fast signature Scheme based on Congruential Polynomial Operations,* IEEE Trans. on Inform. Theory, IT-36, pp 47–53, (1990)

[9] Tatsuaki Okamoto, Eiichiro Fujisaki, Hikaru Morita, Efficient Digital Signature Scheme Using Trisection Size Hash, (Submission to P1363a), 1998.

[10] Brigitte Vallée, *Generation of elements with small modular squares and provably fast integer factoring algorithms,* Mathematics of Computation, vol 56, 194, pp 823-849, april 91.

[11] Brigitte Vallée, Marc Girault, Philippe Toffin, *How to break Okamoto's cryptosystem by reducing lattice bases,* Proceedings of Eurocrypt'88, Davos, april 1988, LNCS (330), pp 281-291.

[12] Brigitte Vallée, Marc Girault, Philippe Toffin, *How to guess ℓ-th roots modulo n by reducing lattices bases,* Proceedings of AAECC-88, Rome, July 1988, LNCS (357), pp 427-442.