Small Solutions of Bivariant Modular Equations and the security of DSA and ECDSA

Dimitrios Poulakis
Department of Mathematics,
Aristotle University of Thessaloniki,
Thessaloniki 54124, Greece,
email:poulakis@math.auth.gr

January 20, 2009

Abstract

In this paper, using the LLL reduction method and an algorithm for the computation of the integral points of a class of conics, we find small solutions of a class of bivariate modular equations of second degree. We use our result for attacking DSA and ECDSA.

Keywords: Public Key Cryptography; Digital Signature Algorithm; Elliptic Curve Digital Signature Algorithm; Algorithm LLL; Discrete Logarithm; Diophantine Equations.

1 Introduction

In August 1991, the U.S. government's National Institute of Standards and Technology (NIST) proposed an algorithm for digital signatures. The algorithm is known as DSA, for Digital Signature Algorithm [11, 10, 9]. It is an efficient variant of the ElGamal digital signature scheme [3] intended for use in electronic mail, electronic funds transfer, electronic data interchange, software distribution, data storage, and other applications which require data integrity assurance and data authentication. In 1998, an elliptic curve analogue called Elliptic Curve Digital Signature Algorithm (ECDSA) was proposed and standarized [4, 8, 9].

Let us recall the outlines of DSA and ECDSA. First, for DSA, the signer chooses a prime p of size between 512 and 1024 bits with increments of 64, q is a prime of size 160 with $q|p-1$ and g is a generator of the unique order q subgroup G of $\mathbb{Z}_p^*$. Further, he chooses $a \in \{1, \ldots, q-1\}$ and computes $A = g^a \bmod p$. The public key of the signer is (p, q, g, A) and his private key a. Furthermore, the signer chooses a publicly known hash function h mapping messages to $\{0, \ldots, q-1\}$. To sign a message m, he chooses a random number $k \in \{1, \ldots, q-1\}$ which is the ephemeral key, computes

$$r = (g^k \bmod p) \bmod q \quad \text{and} \quad s = k^{-1}(h(m) + ar) \bmod q.$$

The signature of m is the pair (r, s). The verification of the signature is performed by checking

$$r = ((g^{s^{-1}h(m) \bmod q} A^{s^{-1}r \bmod q}) \bmod p) \bmod q.$$

The ECDSA uses an elliptic curve E over $\mathbb{Z}_p$ and a point $P \in E(\mathbb{Z}_p)$ with order a prime q of size around 160 bits. The signer selects $a \in \{1, \ldots, q-1\}$ and computes $Q = aP$. Its public key is (p, E, P, q, Q) and his private key a. To sign a message m having hash value $h(m) \in \{0, \ldots, q-1\}$, he selects a random number $k \in \{1, \ldots, q-1\}$ which is the ephemeral key and computes $kP = (x, y)$ (where x and y are regarded as integer between 0 and $p-1$). Next, he computes

$$r = x \bmod q \quad \text{and} \quad s = k^{-1}(h(m) + ar) \bmod q.$$

The signature of m is the pair (r, s). For the verification of the signature one computes

$$u_1 = s^{-1}h(m) \bmod q, \quad u_2 = s^{-1}r \bmod q, \quad u_1P + u_2Q = (x_0, y_0).$$

He accepts the signature if and only if $r = x_0 \bmod q$.

The assumption here is that the only way to forge signature is to recover either the secret key a, or the ephemeral key k (in this case is a simple matter to compute a). Thus, the parameters of the two systems were chosen in such a way that the computation of discrete logarithms is computationally infeasible, and so a or k is well protected.

The use of lattices and the so-called LLL reduction method [16] is a well established tool for attacking a variety of cryptosystems. Attacks to DSA and to ECDSA using lattice reduction techniques are given in [1], [7], [12], [13] and [2]. A common feature of these attacks is that take advantage of the form of equality $s = k^{-1}(h(m) + ar) \bmod q$. In [1] it was shown that one can recover the DSA secret key a, if the ephemeral key k is produced by Knuth's linear congruencial generator with known parameters, or variants. In [7], an attack on DSA is described in case where for some number of different signatures a proportion of bits of each of the associated ephemeral keys are revealed. A polynomial-time attack on DSA which recover a is described in [12], in case where the size of q is not too small compared with p, the probability of collisions for the hash function is not too large compared to $1/q$ and for a polynomially bounded number of messages, about $\log_2^{1/2}(q)$ of the least significant bits of the ephemeral keys are known. The previous attack is adapted to the case of ECDSA [13]. Finally, in [2], under the assumption that the second shortest vector of the reduced lattice is suffiiently short, it is determined how large the keys a and k can be in order for them to be computed by considering only one signature.

In this paper, using the algorithm LLL and an algorithm for the computation of the integral points of a class of conics, we find small solutions of a class of bivariate modular equations of second degree. As an application of this result, we give a new attack on DSA and ECDSA which is based on the equality $s = k^{-1}(h(m) + ar) \bmod q$. Assuming that a signature is available and the quantities in at least one of the sets $\{a, k^{-1} \bmod q\}$, $\{k, a^{-1} \bmod q\}$ and $\{a^{-1} \bmod, k^{-1} \bmod q\}$ are smaller that a certain explicit bound, we prove that the secret keys a and k can be revealed. Moreover, if two signatures with

ephemeral keys k_1 and k_2 are available and the quantities in at least one of the sets $\{k_1, k_2^{-1} \bmod q\}$, $\{k_2, k_1^{-1} \bmod q\}$ and $\{k_1^{-1} \bmod, k_2^{-1} \bmod q\}$ are smaller that a certain explicit bound, then k_1, k_2 and so a can be computed. More precisely, we prove the following theorem:

Theorem 1 *Let q be a prime number and $h(x,y) = a+bx+cy+xy$ a polynomial with integer coefficients. Let S be the set of solutions $(x_0, y_0) \in \mathbb{Z}^2$ of the congruence $f(x_0, y_0) \equiv 0 \pmod q$ satisfying $|x_0| < X$ and $|y_0| < Y$ where*

1. $XY < q^{1/2}/2^{7/2}$, *if* $abc \neq 0$,
2. $XY < q^{1/2}/6^{3/4}$, *if* $a = 0$,
3. $XY^2 < q/6^{3/2}$, *if* $b = 0$,
4. $X^2Y < q/6^{3/2}$, *if* $c = 0$.

Then the computation of the elements of S has time complexity $O(q^\epsilon)$, where ϵ is arbitrary small positive real number, provided the prime factorization of integers $da - bc$ and c are known. Moreover, the number of elements of S is also $O(q^\epsilon)$.

Let $x, x' \in \{1, \ldots, q-1\}$ be such that $x = q - x'$. We set $\tilde{x} = x$ if $x \leq x'$ and $\tilde{x} = -x'$, otherwise. Further, if $z = x^{-1} \bmod q$, then we set $\hat{x} = \tilde{z}$. We prove the following corollaries:

Corollary 1 *Let (r, s) be the DSA or ECDSA signature of a message m with ephemeral key k. Suppose that X and Y are positive real numbers such that one of the following conditions is satisfied:*

1. $|\tilde{a}| < X$, $|\hat{k}| < Y$ *and* $XY^2 < q/6^{3/2}$.
2. $|\tilde{k}| < X$, $|\hat{a}| < Y$ *and* $XY^2 < q/6^{3/2}$.
3. $|\hat{k}| < X$, $|\hat{a}| < Y$ *and* $XY < q^{1/2}/6^{3/4}$.

Then the secret exponents a and k can be computed in time $O(q^\epsilon)$, where ϵ is arbitrary small positive number.

Corollary 2 *Let (r_1, s_1) and (r_2, s_2) be the DSA or ECDSA signatures of two messages m_1 and m_2 with ephemeral keys k_1 and k_2, respectively. Suppose that X and Y are positive real numbers such that one of the following conditions is satisfied:*

1. $|\tilde{k_1}| < X$, $|\hat{k_2}| < Y$ *and* $XY^2 < q/6^{3/2}$.
2. $|\tilde{k_2}| < X$, $|\hat{k_1}| < Y$ *and* $XY^2 < q/6^{3/2}$.
3. $|\hat{k_2}| < X$, $|\hat{k_1}| < Y$ *and* $XY < q^{1/2}/6^{3/4}$.

Then the secret exponents k_1 and k_2 (and so a) can be computed in time $O(q^\epsilon)$, where ϵ is arbitrary small positive number.

In [15], we presented a version of the DSA which combines the intractability of the integer factorization problem and discrete logarithm problem, and it is at least as secure as DSA. It uses computations in the group $\mathbb{Z}_n^*$, where n is the product of two large primes which is part of the private key, and so the order of the underlying group is hidden. An immediate consequence of this fact is that all the above mentioned attacks (Corollaries 1 and 2 included) do not longer work.

The paper is organized as follows. In Section 2, some results on the LLL reduction method are recalled which are necessary for the proof of Theorem 1. An algorithm for the computation of integer solutions of the Diophantine equation $a+bx+cy+dxy = 0$ is given. The proofs of Theorem 1 and Corollaries 1 and 2 are obtained in Sections 3 and 4, respectively. Finally, Section 5 concludes the paper.

2 Lattices and Polynomials

Let $B = \{\mathbf{b}_1, \ldots, \mathbf{b}_n\} \subset \mathbb{Z}^n$ be a basis of $\mathbb{R}^n$. A *n-dimensional lattice* spanned by B is the set

$$L = \{z_1\mathbf{b}_1 + \cdots + z_n\mathbf{b}_n / \ z_1, \ldots, z_n \in \mathbb{Z}\}.$$

If $\mathbf{b}_i = (b_{i,1}, \ldots, b_{i,n})$ $(i = 1, \ldots, n)$, then the *determinant* $\det L$ of L is the absolute value of the determinant whose (i, j) element is $b_{i,j}$.

The *Euclidean norm* of a vector $\mathbf{v} = (v_1, \ldots, v_n) \in \mathbb{R}^n$ is defined to be the quantity $||\mathbf{v}|| = (v_1^2 + \cdots + v_n^2)^{1/2}$ and for a polynomial $h(x, y) = \sum_{i,j} h_{i,j}x^i y^j$ the quantity $||h|| = (\sum_{i,j} |h_{i,j}|^2)^{1/2}$.

The LLL algorithm [16] acting on a matrix with rows the vectors of a basis of L and produces a basis having a quite short vector. We shall need the following result:

Lemma 1 *(LLL) Let $M = \max\{||\mathbf{b}_1||, \ldots, ||\mathbf{b}_n||\}$. The LLL algorithm finds in time $O(n^6(\log M)^3)$ a vector $\mathbf{b} \in L$ such that*

$$||\mathbf{b}|| \leq 2^{(n-1)/4}(\det L)^{1/n}.$$

Furthermore, we shall use the following well known lemma whose proof is given in [7].

Lemma 2 *(Howgrave-Graham) Suppose $h(x, y) \in \mathbb{Z}[x, y]$ is a polynomial which is the sum of at most ω monomials. Suppose that there are $x_0, y_0 \in \mathbb{Z}$ with $|x_0| < X$, $|y_0| < Y$ and $||h(xX, yY)|| < n/\sqrt{\omega}$. Then $h(x_0, y_0) = 0$ holds over integers.*

3 The Diophantine equation $a + bx + cy + dxy = 0$

Let $f(x, y) = a+bx+cy+dxy$ be a polynomial with coprime integer coefficients. The conic defined by the equation $f(x, y) = 0$ has two valuations at infinity and so, the solutions $(x, y) \in \mathbb{Z}^2$ to the Diophantine equation $f(x, y) = 0$ can be computed by the algorithm of [14, Section 4]. In this section, we give a simple

algorithm for this task specializing the algorithm of [14] to the case of equation $f(x,y)=0$ and we compute its complexity.

SOLVE-CONIC

Input: $f(x,y)=a+bx+cy+dxy\in\mathbb{Z}[x,y]$, with $\gcd(a,b,c,d)=1$ and $bdc\neq 0$.
Output: The solutions $(x,y)\in\mathbb{Z}^2$ to the equation $f(x,y)=0$.

1. Compute the quantities $A_1=da-bc$, $A_2=c^2$ and $A_3=cd$.
2. Compute the set of divisors D_1 and D_2 of A_1 and c, respectively.
3. Compute the quantities
$$x(u/v)=\frac{A_1v-A_2u}{A_3u},\quad y(u/v)=-\frac{bv+cu}{av},\quad u\in D_1,\ v\in D_2.$$
4. Output the couples $(x(u/v),y(u/v))$ with $u\in D_1$ and $v\in D_2$ such that $x(u/v),y(u/v)\in\mathbb{Z}$ and the couple $(0,-a/c)$ if $c|a$.

Proof of correctness of **SOLVE-CONIC.** We denote by C the affine conic defined by the equation $f(x,y)=0$. First, we shall construct a parametrization of C. Since $c\neq 0$, the point $P_0=(0,-a/c)$ belongs to C. The line $l(t)$ whose equation is $y+a/c=tx$, where $t\in\mathbb{Q}$, intersects C in P_0 and in a unique second point $P(t)=(x(t),y(t))$. Eliminating y between $y+a/c=tx$ and $f(x,y)=0$, we obtain the equation
$$x(dtx-\frac{ad}{c}+ct+b)=0,$$
whence we get
$$x(t)=\frac{A_1-A_2t}{A_3t},\quad y(t)=-\frac{b+ct}{d},$$
where $A_1=ad-bc$, $A_2=c^2$ and $A_3=cd$. Thus, every line $l(t)$ with rational slope t passing through P_0 determines a rational point $P(t)$ on C and a such point determines with P_0 such a line $l(t)$.

Suppose now that $(\alpha,\beta)\in\mathbb{Z}^2$ is a solution to $f(x,y)=0$ with $x\neq 0$. Then there is $t\in\mathbb{Q}$ such that $\alpha=x(t)$ and $\beta=y(t)$. Setting $t=u/v$, where u, v are coprime integers, we obtain the relations:
$$A_3u|A_1v-A_2u\quad\text{and}\quad dv|bv+cu.$$
Since $\gcd(u,v)=1$, we get $u|A_1$ and $v|c$. Thus, if D_1 and D_2 are the set of divisors of A_1 and c, respectively, then the solutions $(x,y)\in\mathbb{Z}^2$ to the equation $f(x,y)=0$ with $x\neq 0$ are among the points $(x(u/v),y(u/v))$ with $u\in D_1$ and $v\in D_2$.

Time complexity of **SOLVE-CONIC.** Put $M=\max\{|a|,|b|,|c|,|d|\}$. Step 1 requires $O((\log M)^2)$ bit operations. If $A_1=p_1^{a_1}\cdots p_k^{a_k}$ is the prime factorization of A_1, then the computation of a divisor $\delta=p_1^{b_1}\cdots p_k^{b_k}$ $(0\leq b_i\leq a_i, i=1,\ldots,k)$ of A_1 requires $O((\log\delta)^2)$ bit operations. By [5, Theorem 315], the number of positive divisors of A_1 is $\tau(A_1)=O(A_1^{\epsilon})$ for arbitrary small $\epsilon>0$. Thus the time complexity of the computation of the set D_1 is $O(A_1^{\epsilon})$. Similarly,

the time complexity of the computation of the set D_2 is $O(c^\epsilon)$. Hence, Step 2 has time complexity $O(M^\epsilon)$, provided the prime factorization of A_1 and c are known. The computation of every couple $(x(u/v), y(u/v))$ has time complexity $O((\log M)^2)$ and so, the time complexity of Step 3 is $O(M^\epsilon)$. Therefore, the time complexity of the algorithm is $O(M^\epsilon)$ for arbitrary small $\epsilon > 0$ (provided the prime factorization of A_1 and c are known).

Remark 1 In case where $f(x, y) = a + cy + dxy$, with $ad \neq 0$, the solutions $(x, y) \in \mathbb{Z}^2$ to $f(x, y) = 0$ satisfy $y|a$ and so, their computation has time complexity $O(M^\epsilon)$ for arbitrary small $\epsilon > 0$ (provided the prime factorization of a is known).

Remark 2 The number of solutions $(x, y) \in \mathbb{Z}^2$ to $f(x, y) = 0$ is $O(M^\epsilon)$.

4 Proof of Theorem 1

(1) Suppose that $abc \neq 0$ and $XY < q^{1/2}/2^{7/2}$. We consider the polynomials $h_0(x, y) = q$, $h_1(x, y) = qx$ and $h_2(x, y) = qy$. The coefficient vectors of $h(xX, yY)$ and $h_i(xX, yY)$ $(i = 0, 1, 2)$ are $\mathbb{R}$-linearly independent and so generate a lattice L of rank 4. Consider the matrix with rows the coefficient vectors of $h(xX, yY)$ and $h_i(xX, yY)$ $(i = 1, 2, 3)$:

$$H = \begin{pmatrix} q & 0 & 0 & 0 \\ 0 & qX & 0 & 0 \\ 0 & 0 & qY & 0 \\ a & bX & cY & XY \end{pmatrix}.$$

We have $\det L = |\det H| = q^3(XY)^2$. By Lemma 1, there is a vector $\mathbf{v} = (c_0, c_1X, c_2Y, c_3XY)$ in L such that

$$||\mathbf{v}|| \leq 2^{3/4} q^{3/4} (XY)^{1/2} < q/2.$$

Put $f(x, y) = c_0 + c_1x + c_2y + c_3xy$. Then $f(xX, yY)$ is an integral linear combination of $h(xX, yY)$ and $h_i(xX, yY)$ $(i = 1, 2, 3)$. It follows that $c_3 \neq 0$ and for every $(x_0, y_0) \in S$, we have $f(x_0, y_0) \equiv 0 \pmod q$. Since $||f(xX, yY)|| < q/2$, Lemma 2 yields $f(x_0, y_0) = 0$, for every $(x_0, y_0) \in S$. The algorithm SOLVE-CONIC computes all the solutions $(x, y) \in \mathbb{Z}^2$ to $f(x, y) = 0$. Thus, the computation of the elements of S has time complexity $O(q^\epsilon)$, where ϵ is arbitrary small.

(2) Suppose that $a = 0$ and $XY < q^{1/2}/6^{3/4}$. Working similarly as in the previous case we consider the lattice Λ having as basis the rows of the matrix

$$I = \begin{pmatrix} qX & 0 & 0 \\ 0 & qY & 0 \\ bX & cY & XY \end{pmatrix}.$$

We have $\det\Lambda = |\det I| = (qXY)^2$. It follows as in the first case that there is a polynomial with integer coefficients $f(x, y) = c_1x + c_2y + c_3xy$ with $c_3 \neq 0$ and

$$||f(xX, yY)|| \leq \sqrt{2}(qXY)^{2/3} < q/\sqrt{3}$$

such that $f(x_0, y_0) \equiv 0 \pmod q$, for every $(x_0, y_0) \in S$, and so, $f(x_0, y_0) = 0$, for every $(x_0, y_0) \in S$. Next, the algorithm SOLVE-CONIC computes all the elements of S in time $O(q^\epsilon)$, where ϵ is arbitrary small.

(3) Suppose that $b = 0$ and $XY^2 < q/6^{3/2}$. We consider the lattice Λ having as basis the rows of the matrix

$$J = \begin{pmatrix} q & 0 & 0 \\ 0 & qY & 0 \\ a & cY & XY \end{pmatrix}.$$

We have $\det\Lambda = |\det J| = q^2XY^2$. It follows that that there is a polynomial with integer coefficients $f(x, y) = c_0 + c_1y + c_2xy$ with $c_2 \neq 0$ and

$$||f(xX, yY)|| \leq \sqrt{2}(q^2XY^2)^{1/3} < q/\sqrt{3}$$

such that $f(x_0, y_0) \equiv 0 \pmod q$, for every $(x_0, y_0) \in S$. Thus, $f(x_0, y_0) = 0$, for every $(x_0, y_0) \in S$. Finally, Remark 1 implies that the elements of S can be computed in time $O(q^\epsilon)$, where ϵ is arbitrary small.

(4) The proof of case $c = 0$ and $X^2Y < q/6^{3/2}$ is similar to (3).

Finally, the maximum of absolute values of the coefficients of $f(x, y)$, in any case, is less than q. Thus, Remark 2 implies that the number of elements of S is $O(q^\epsilon)$.

5 Proof of Corollaries 1 and 2

Proof of Corollary 1. Let m be a message and (r, s) its signature with DSA or ECDSA. Then there is $k \in \{1, \ldots, q-1\}$ such that $r = (g^k \bmod p) \bmod q$ and $s = k^{-1}(h(m) + ar) \bmod q$.

(1) Suppose that there are positive real numbers X and Y such that $|\tilde{a}| < X$, $|\hat{k}| < Y$ and $XY^2 < q/6^{3/2}$. Let S be the set of solutions $(x_0, y_0) \in \mathbb{Z}^2$ of

$$xy + yh(m) - sr^{-1} \equiv 0 \bmod q$$

with $|x_0| < X$ and $|y_0| < Y$. A such solution is the couple $(\tilde{a}, \hat{k})$. By Theorem 1, the elements of S can be computed in time $O(q^\epsilon)$ and its number is $O(q^\epsilon)$. Next, we compute the quantities $g^{x_0} \bmod q$, where $(x_0, y_0) \in S$, until we find $g^{x_0} = A \bmod q$. Then $x_0 = \tilde{a}$. Since $|S| = O(q^\epsilon)$, the time complexity of the computation of $\tilde{a}$ and $\hat{k}$, and hence of a and k, is $O(q^\epsilon)$.

(2) Suppose that there are positive real numbers X and Y such that $|\tilde{k}| < X$, $|\hat{a}| < Y$ and $XY^2 < q/6^{3/2}$. A solution of the congruence

$$xy - h(m)s^{-1}y - rs^{-1} \equiv 0 \bmod q.$$

is $(x, y) = (\tilde{k}, \hat{a})$. Then working as previously, we compute a and k in time $O(q^\epsilon)$.

(3) Suppose that X and Y are positive real numbers such that $|\hat{k}| < X$, $|\hat{a}| < Y$ and $XY < q^{1/2}/6^{3/4}$. The couple $(x, y) = (\hat{k}, \hat{a})$ is a solution of the congruence

$$xy + rh(m)^{-1}y - sh(m)^{-1}x \equiv 0 \bmod q.$$

Working as previously the result follows.

Proof of Corollary 2. Let (r_1, s_1) and (r_2, s_2) be the DSA or ECDSA signatures of two messages m_1 and m_2 with ephemeral keys k_1 and k_2, respectively. Then we have

$$s_1 = k_1^{-1}(h(m_1) + ar_1) \bmod q \quad \text{and} \quad s_2 = k_2^{-1}(h(m_2) + ar_2) \bmod q.$$

Eliminating a from the two equalities we obtain the congruence

$$s_1 r_2 k_1 - r_1 s_2 k_2 + r_1 h(m_2) - h(m_1) r_2 \equiv 0 \pmod{q}.$$

Hence the couples $(\tilde{k_1}, \hat{k_2})$, $(\hat{k_1}, \tilde{k_2})$ and $(\hat{k_1}, \hat{k_2})$ are solutions of the congruences

$$yx + (s_1^{-1} r_1 r_2^{-1} h(m_2) - h(m_1) s_1^{-1}) y - r_1 s_2 s_1^{-1} r_2^{-1} \equiv 0 \pmod{q},$$

$$yx + (s_2^{-1} r_2 r_1^{-1} h(m_1) - h(m_2) s_2^{-1}) y - r_1 s_2 s_1^{-1} r_2^{-1} \equiv 0 \pmod{q},$$

$$yx + r_2 s_1 (r_1 h(m_2) - r_2 h(m_1))^{-1} y - r_1 s_2 (r_1 h(m_2) - r_2 h(m_1))^{-1} x \equiv 0 \pmod{q},$$

respectively. Next, working as in Corollary 1 the result follows.

Note that the absolute values of coefficients of the above modular equations are $< q$, and so in case where the size of q is 160, the factorization of the numbers required by Theorem 1 is not an important problem.

6 Conclusion

In this paper, combining lattice reduction techniques with an algorithm for computing the integral solutions of Diophantine equations of the form $a + bx + cy + dxy = 0$, we give a method for finding small solutions of bivariate modular equations of the form $a + bx + cy + xy \equiv 0 \pmod{q}$. We used this result in order to devellop an attack on DSA and ECDSA. If a signature is available and the two keys (secret and ephemeral) are of a certain size, then they can be computed. The same happens, if two signatures are available and their ephemeral keys have a certain size. These attacks can also be applied on other schemes where the secret and the ephemeral keys are solutions of a modular bivariate linear equation as in DSA or of a modular bivariate equation of second degree, as above. For instance, such schemes are Schnorr' signature, Heyst-Pedersen signature, etc [10, 17].

References

[1] M. Bellare, S. Goldwasser and Micciancio, "Pseudo-random" number generation within cryptographic algorithms: the DSS case. In *Proc. of Crypto '97,* LNCS 1294. IACR, Palo Alto, CA. Springer-Verlag, Berlin 1997.

[2] I. F. Blake and T. Garefalakis, On the security of the digital signature algorithm. *Des. Codes Cryptogr.,* 26, no. 1-3 (2002), 87-96.

[3] T. ElGamal, A public key cryptosystem and a signature scheme based on discrete logarithm, *IEEE Transactions on Information Theory,* 31 (1985), 469-472.

[4] D. Johnson, A. J. Menezes and S. A. Vastone, The elliptic curve digital signature algorithm (ECDSA), *Intern. J. of Information Security,* 1 (2001) 36-63.

[5] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers,* Fifth edition, Oxford University Press 1979.

[6] N. A. Howgrave-Graham, *Finding small roots of univariate equations revisited.* In Cryptography and Coding, vol. 1355 of LNCS, pp. 131-142. Springer Verlag, 1997.

[7] N. A. Howgrave-Graham and N. P. Smart, Lattice Attacks on Digital Signature Schemes, *Des. Codes Cryptogr.* 23 (2001) 283-290.

[8] N. Koblitz, A. J. Menezes and S. A. Vastone, The state of elliptic curve cryptography, *Des. Codes Cryptogr.* 19 (2000), 173-193.

[9] N. Koblitz and A. J. Menezes, A survey of Public-Key Cryptosystems, *SIAM REVIEW,* 46, No. 4 (2004), 599-634.

[10] A. J. Menezes, P. C. van Oorschot and S. A. Vanstone, *Handbook of Applied Cryptography,* CRC Press, Boca Raton, Florida, 1997.

[11] National Institute of Standards and Technology (NIST). *FIPS Publication* 186*: Digital Signature Standard.* May 1994.

[12] P. Nguyen and I. E. Shparlinski, The Insecurity of the Digital Signature Algorithm with Partially Known Nonces, *J. Cryptology,* 15 (2002), 151-176.

[13] P. Nguyen and I. E. Shparlinski, The Insecurity of the Elliptic Curve Digital Signature Algorithm with Partially Known Nonces, *Des. Codes Cryptogr.* 30, (2003), 201-217.

[14] D. Poulakis and E. Voskos, Solving genus zero Diophantine equations with at most two infinite valuations *J. Symbolic Computation* 33 (2002), 479-491.

[15] D. Poulakis, A variant of Digital Signature Algorithm, *Des. Codes Cryptogr.* (to appear).

[16] A. K. Lenstra, H. W. Lenstra Jr., and L. Lovász, Factoring polynomials with rational coefficients, *Math. Ann.*, 261 (1982), 513-534.

[17] D. R. Stinson, *Cryptography, Theory and Practice,* Chapman & Hall/CRC, 2nd ed. 2002.