Information Processing Letters 116 (2016) 541–545

Contents lists available at ScienceDirect

Information Processing Letters

www.elsevier.com/locate/ipl

(EC)DSA lattice attacks based on Coppersmith's method

Konstantinos A. Draziotis

Aristotle University of Thessaloniki, Department of Informatics, P.O. Box 114, 54124 Thessaloniki, Greece

ARTICLE INFO

Article history:
Received 23 July 2015
Received in revised form 20 February 2016
Accepted 2 April 2016
Available online 7 April 2016
Communicated by M. Chrobak

Keywords:
Cryptography
Lattices
Digital Signature Algorithm (DSA)
Coppersmith's method

ABSTRACT

We provide an attack to (EC)DSA digital signature built upon Coppersmith's method. We prove that, if a, k are the private and ephemeral key, respectively, of the (EC)DSA scheme and $(k^{-1} \bmod q)^2 a < 0.262 \cdot q^{1.157}$, then we can efficiently find a.

1. Introduction—statement of results

In the present paper we study Digital Signature Algorithm, DSA, and its elliptic curve variant, ECDSA [7]. Both are based on ElGamal signatures [8]. In these schemes Alice, the signer, randomly chooses a private key a from a public finite group G, with $|G| = p$, for some large prime p. Usually G is the finite group of integers modulo p or the group defined by the points of an elliptic curve over a finite field. Then, she publishes an element $g \in G$ and $R = g^a$, for some a randomly chosen from the set $\{1, 2, \ldots, q-1\}$, where q is a prime at least 160-bits, such that $q|p-1$. Also, she considers an ephemeral key k randomly chosen from the set $\{2, 3, \ldots, q-1\}$. Furthermore, Alice chooses an integer, say s, by solving a linear modular equation $f_s(a, k) \equiv 0 \pmod q$, between the secret key a and the ephemeral key k. The purpose of an attacker is to find either a or k, the knowledge of one leads to the discovery of the other. These protocols are based on the difficulty of the Discrete Logarithm Problem (DLP). To attack these digital signatures, someone may try to solve DLP. Another large class of attacks is based on lattices, see [4,11].

For the DLP (but not its elliptic curve variant), the best algorithms have subexponential running time [1,10]. Our attack is based on lattices. We study the modular equation $f_s(a, k) \equiv 0 \pmod q$, which in the case of (EC)DSA has the form,

$$ks - ar \equiv h(m) \pmod q, \tag{1}$$

where $h : G \to \mathbb{Z}_q$ is a hash function which is a public knowledge, $r = (g^k \bmod p) \bmod q$ and s satisfies equation (1). Furthermore, (r, s) is the signature of a message m.

Also, the first attack in (EC)DSA, using Coppersmith's method [5], was given in [3]. The authors managed to prove that, if $ak < q^{0.957}$ (with q 160-bits), then there is an efficient algorithm which provides a. They applied Coppersmith's method to the polynomial given by equation (1). Coppersmith's method has polynomial running time since it uses LLL algorithm.

Before we state our results, we shall define the following notation. Let n be an integer and $\gcd(q, n) = 1$. Then $[n^{-1}]_q$ denote the reminder of an integer in the class $n^{-1} \pmod q$ divided by q. In [13] Coppersmith's method was applied to a quadratic polynomial. Furthermore, assuming that we can factor integers less than 160-bits and if $[k^{-1}]_q^2 a < q/6^{3/2} \approx 0.06 \cdot q$, then the author found a in

E-mail address: drazioti@csd.auth.gr.

http://dx.doi.org/10.1016/j.ipl.2016.04.001
0020-0190/

Table 1
In the second column we calculated $\lfloor \log_2(q^{1.157}Y^{-1.26} \times 0.262)\rfloor - \lfloor \log_2(qY^{-1}6^{-3/2})\rfloor$, with q 160 bits. Thus, we get the advantage (in bits) for X^2, of our method compared with [13].

Bits (Y)	Advantage (in bits)
100	1
93	3
89	4
85	5
77	7
73	8
69	9
66	10

polynomial time (assuming q has 160-bits). In this paper we shall improve this result. If a has less than 101 bits, we show that greater values of $[k^{-1}]_q$ can be used. In our approach we use a lattice of Boneh–Durfee type [6]. Note that our method does not depend on the hypothesis of factoring 160 bits integers, so we allow more than 160-bits for the prime q.

We shall use a lattice such that each row corresponds to a bivariate polynomial, $H(x, y)$, with $H([k^{-1}]_q, a) \in \mathbb{Z}$. Having two short lattice vectors, we get two polynomials having as a common root $([k^{-1}]_q, a)$. Then, we compute the private key a. To implement our attack we use the following heuristic assumption. We assume that $H_1(x, y)$ *and* $H_2(x, y)$ *are algebraically independent polynomials*. So taking the resultant of these two polynomials (with respect either x or y) we get a non-constant polynomial of one variable. The heuristic is supported by many examples (for a discussion see also [6, section 7.3]).

Furthermore, we use the following experimental fact.

FACT 1. *In random lattices with dimension* ≤ 35, *LLL behaves as a SVP-oracle.*

That is will find a shortest vector of the lattice (SVP: Shortest Vector Problem). This was confirmed by many experiments [9]. We prove the following proposition.

Proposition 1.1. *Let* a, k *be the private and an ephemeral key of the (EC)DSA, respectively and* $X, Y \in \mathbb{Z}_{>0}$ *such that* $[k^{-1}]_q < X$, $a < Y$. *Assuming FACT 1 and the heuristic, if* $X^2Y^{1.26} < 0.262 \cdot q^{1.157}$, *then we can efficiently find the private key* a.

For Y less than 101 bits we improve the result of [13]. To see this we constructed Table 1.

Finally, we remark that in the proof of Proposition 1.1 we assumed that the Gaussian heuristic holds in our lattices (see also [2]). Gaussian heuristic predicts the following bound for the first successive minima $\lambda_1(L) \approx (\frac{\sqrt{w}}{2\pi e})^{1/2} \det L^{1/w} = Gauss(L)$, where L is a full rank lattice (i.e. is defined by a rectangular matrix) of volume $\det L$ and with dimension w. We have checked this heuristic experimentally. We ran 1000 random instances of our lattices and we got $|\lambda_1(L) - Gauss(L)| < 10^{-2}$.

We shall now state our theorem.

Theorem 1.2. *Let* a, k *be the private and an ephemeral key of the (EC)DSA, respectively and* m, t *be positive integers. Let also* $X, Y \in \mathbb{Z}_{>0}$ *such that* $[k^{-1}]_q < X$, $a < Y$. *If*

$$X^2 Y^{1+\gamma(t,m)} < (\zeta(w) q^{\alpha(m)+\beta(m)t})^{1/(\alpha(m)+\beta(m)t/2)} \tag{2}$$

where

$$\alpha(m) = \frac{m(m+1)(m+2)}{6},\ \beta(m) = \frac{m(m+1)}{2},$$
$$w = \frac{(m+1)(m+2)}{2} + t(m+1),$$
$$\gamma(t,m) = \frac{\beta(m)t\left(\frac{m+t+1}{m} - \frac{1}{2}\right)}{\alpha(m) + \beta(m)t/2}$$

and

$$\zeta(w) = 2^{-w^2/4} w^{-w/2}, \tag{3}$$

then for sufficiently large m *we can efficiently find two polynomials* $H_1(x, y)$ *and* $H_2(x, y)$ *such that,* $H_1([k^{-1}]_q, a) = H_2([k^{-1}]_q, a) = 0$.

For the proof of this theorem we will construct a suitable lattice and we will then apply Coppersmith's method. In fact in the proposition we shall optimize the previous theorem, to get suitable values for the parameters m, t, such that greater upper bound for $X \cdot Y$ will be reached (compared to [13]). Finally, using FACT 1, the heuristic and plugging $m = 6$ and $t = 1$ in Theorem 1.2, the proposition will follow.

Roadmap. In the second section we present some preliminaries. In section 3 we prove Theorem 1.2 and in the next section we proceed with the proof of Proposition 1.1. Our attack is illustrated by an example in section 5 and in the final section we provide some concluding remarks.

2. Auxiliary results

The main purpose of this section is to present some basic results necessary for the proof of Theorem 1.2. For some details of the computations in Lemmas 2.4 and 2.5 see [6, Chapter 6].

Lemma 2.1. *Let* $h(x, y) \in \mathbb{R}[x, y]$ *is a sum of* w *monomials. Let* X, Y *in* $\mathbb{R}_{>0}$ *and integers* x_0, y_0 *such that* $|x_0| < X$, $|y_0| < Y$. *Suppose that*

i. $h(x_0, y_0) \in \mathbb{Z}$, **ii.** $||h(xX, yY)|| = \sqrt{\sum_{i,j}(h_{i,j}X^iY^j)^2} < \frac{1}{\sqrt{w}}$,

then $h(x_0, y_0) = 0$.

Proof. [6, FACT 2.4.1, p.17]. □

Lemma 2.2. *Let* L *be a lattice and* $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_w$ *is an LLL-reduced basis of* L. *Then*

$$||\mathbf{b}_1|| < 2^{(w-1)/4}(\det L)^{1/w},$$
$$||\mathbf{b}_2|| \leq 2^{w/4}\left(\frac{\det L}{||\mathbf{b}_1||}\right)^{1/(w-1)},\ ||\mathbf{b}_2|| < \frac{3}{2}||\mathbf{b}_1||.$$

Proof. For the first two inequalities see [6, FACT 2.2.2, 2.2.3, p.10]. For the third inequality we have $||\mathbf{b}_2|| < ||\mathbf{b}_2^*|| + \frac{1}{2}||\mathbf{b}_1||$. But $||\mathbf{b}_2^*|| < ||\mathbf{b}_1||$ and the result follows. □

Definition 2.3. Let $f(x,y) \in \mathbb{R}[x,y]$. We define the x-shift polynomials of $f(x,y)$, $g_{i,k}(x,y) = x^i f(x,y)^k$ and y-shift polynomials of $f(x,y)$, to be $h_{j,k}(x,y) = y^j f(x,y)^k$.

The integers A, B in the following lemmas are $A = [h(m)r^{-1}]_q$ and $B = [-sr^{-1}]_q$. Of course the results hold in general.

Lemma 2.4. *Let $f(x,y) = \frac{x(y+A)+B}{q}$ and the vectors $\mathbf{b}_{i,k} = (g_{i,k}X^iY^k)_{i,k}$, $k = 0,1,\ldots,m$, $i = 0,1,\ldots,m-k$, for some $m \in \mathbb{Z}_{\geq 0}$ and $g_{i,k}$ the coefficients of the x-shift polynomials of $f(x,y)$. Let the rectangular matrix $M_m = (\mathbf{b}_{i,k})_{i,k}$. Then*

$$\det M_m = q^{-\alpha(m)} X^{2\alpha(m)} Y^{\alpha(m)}, \text{ where}$$
$$\alpha(m) = \frac{m(m+1)(m+2)}{6}.$$

Proof. M_m is the matrix

$$\begin{array}{c} \\ 1 \\ x \\ \underline{f} \\ x^2 \\ xf \\ \underline{f^2} \\ \cdot \\ \cdot \\ f^m \end{array} \begin{array}{c} \begin{array}{ccccccccccc} 1 & x & xy & x^2 & x^2y & x^2y^2 & & & & & x^my^m \end{array} \\ \begin{pmatrix} 1 & & & & & & & & & & \\ & X & & & & & & & & & \\ * & * & q^{-1}XY & & & & & & & & \\ & & & X^2 & & & & & & & \\ * & * & * & * & q^{-1}X^2Y & & & & & & \\ * & * & * & * & * & q^{-2}X^2Y^2 & & & & & \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \\ * & * & * & * & & & & & & & q^{-m}X^mY^m \end{pmatrix} \end{array}$$

The dimension of M_m is $\frac{(m+1)(m+2)}{2}$ since

$$\#\{(i,k) : k = 0,1,..,m,\ j = 0,1,\ldots,m-k\}$$
$$= (m+1) + m + \cdots + 1.$$

Also M_m is lower triangular, so

$$\det M_m = \prod_{k=0}^{m} \prod_{i=0}^{m-k} X^{k+i} Y^k q^{-k}$$

and the result follows. □

Lemma 2.5. *Let $f(x,y) = \frac{x(y+A)+B}{q}$ and $\mathbf{c}_{j,k} = (h_{j,k}X^jY^k)_{i,k}$, $k = 0,1,\ldots,m$, $j = 1,2,\ldots,t$, for some $m,t \in \mathbb{Z}_{\geq 0}$ and $h_{j,k}$ the coefficients of y-shift polynomials of $f(x,y)$. Let $R_{t,m} = (\mathbf{c}_{j,k})_{j,k}$ and $\hat{R}_{t,m}$ be the right block of $R_{t,m}$ of dimension $(m+1)t \times (m+1)t$. Then*

$$\det \hat{R}_{t,m} = q^{-t\beta(m)} X^{t\beta(m)} Y^{t(m+1)(m+t+1)/2}, \text{ where}$$
$$\beta(m) = (m+1)m/2.$$

Proof. We consider the submatrix $\hat{R}_{t,m}$ of dimension $(m+1)t \times (m+1)t$ of the matrix $R_{t,m}$.

$$\hat{R}_{t,m} =$$

$$\begin{array}{c} \\ y \\ yf \\ \cdots \\ \underline{yf^m} \\ \cdot \\ \cdot \\ y^tf^m \end{array} \begin{array}{c} \begin{array}{ccccccccccc} y & xy^2 & x^2y^3 & x^3y^4 & & x^my^{m+1} & & & & & x^my^{m+t} \end{array} \\ \begin{pmatrix} Y & & & & & & & & & & \\ * & q^{-1}XY^2 & & & & & & & & & \\ & & & & & & & & & & \\ * & * & * & * & & q^{-m}X^mY^{m+1} & & & & & \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \\ * & * & * & * & & & & & & & q^{-m}X^mY^{m+t} \end{pmatrix} \end{array}$$

The determinant is $\det \hat{R}_{t,m} = \prod_{k=0}^{m} \prod_{j=1}^{t} q^{-k} X^k Y^{k+j}$. After some calculations, the lemma follows. □

Corollary 2.6. *Let the block matrix $A_{t,m} = \begin{bmatrix} M_m \\ R_{t,m} \end{bmatrix}$, where $M_m, R_{t,m}$ be the matrices defined in the two previous Lemmas 2.4, 2.5. Then*

$$\det A_{t,m} = q^{-(\alpha(m)+\beta(m)t)} X^{2\alpha(m)+\beta(m)t} Y^{\alpha(m)+t(m+1)(m+t+1)/2}.$$

Proof. We get $\det A_{t,m} = \det M_m \det \hat{R}_{t,m}$. The result follows from Lemmas 2.4 and 2.5. □

3. Proof of the theorem

Multiplying both sides of equation (1) by $-(kr)^{-1} \pmod q$, we get

$$k^{-1}(a + h(m)r^{-1}) + (-sr^{-1}) \equiv 0 \pmod q.$$

If we set

$$f(x,y) = \frac{x(y+A)+B}{q}, \tag{4}$$

where $A = [h(m)r^{-1}]_q$ and $B = [-sr^{-1}]_q$, then we get $f([k^{-1}]_q, a) \in \mathbb{Z}$. We consider the lattice L generated by the rows of the matrix $A_{t,m}$ (of Corollary 2.6) with $f(x,y)$ be the polynomial defined by equation (4). We apply LLL algorithm to L and say $\mathbf{b}_1$ is the first LLL-reduced vector. Let $H_1(x,y)$ be the polynomial which corresponds to $\mathbf{b}_1$, that is

$$H_1(x,y) = \mathbf{b}_1 \cdot (1, x/X, xy/XY, \ldots, y/Y, .., x^my^{m+t}/X^mY^{m+t}).$$

Remark that $H_1([k^{-1}]_q, a) \in \mathbb{Z}$. Indeed, first note that

$$g_{i,k}([k^{-1}]_q, a),\ h_{j,k}([k^{-1}]_q, a) \text{ and } f([k^{-1}]_q, a) \in \mathbb{Z}.$$

Since H_1 is a linear combination of x-shift and y-shift polynomials, it follows that $H_1([k^{-1}]_q, a) \in \mathbb{Z}$. Furthermore, $||H_1(xX, yY)|| = ||\mathbf{b}_1||$ and $||H_1(xX, yY)|| < 2^{(w-1)/4} \times \det(L)^{1/w}$. If it turns out that $||H_1(xX, yY)|| \leq 1/\sqrt{w}$, then from Lemma 2.1 we get $H_1([k^{-1}]_q, a) = 0$. So to satisfy

$$||H_1([k^{-1}]_q, a)|| \leq 1/\sqrt{w},$$

we must have

$$2^{(w-1)/4} \det(L)^{1/w} < \frac{1}{\sqrt{w}}.$$

Rearranging the previous inequality yields,

$$\det L \le \frac{1}{2^{w(w-1)/4}\sqrt{w}^{w}} = \zeta_1(w).$$

We need a little smaller bound for $\det L$; we shall need it to build a suitable bound for the second polynomial. We set $\zeta(w) = \frac{1}{2^{w^2/4}\sqrt{w}^{w}}$ (also $\zeta(w) < \zeta_1(w)$). To satisfy $||H_1(xX, yY)|| \le 1/\sqrt{w}$, we must have

$$\det L \le \frac{1}{2^{w^2/4}\sqrt{w}^{w}} = \zeta(w). \tag{5}$$

But from Corollary 2.6 we obtain

$$\det L = q^{-(\alpha(m)+t\beta(m))}(X^2Y)^{\alpha(m)+\frac{\beta(m)t}{2}} Y^{t\beta(m)(\frac{m+t+1}{m}-\frac{1}{2})}, \tag{6}$$

where $\alpha(m) = \frac{m(m+1)(m+2)}{6}$ and $\beta(m) = \frac{(m+1)m}{2}$. So from relations (5) and (6) we get

$$q^{-\alpha(m)+t\beta(m)}(X^2Y)^{\alpha(m)+\frac{\beta(m)t}{2}} Y^{t\beta(m)(\frac{m+t+1}{m}-\frac{1}{2})} < \zeta(w)$$

thus,

$$X^2Y^{1+\gamma(m,t)} < \zeta(w)^{1/(\alpha(m)+t\frac{\beta(m)}{2})} q^{(\alpha(m)+t\beta(m))/(\alpha(m)+t\frac{\beta(m)}{2})}, \tag{7}$$

where

$$\gamma(m,t) = \frac{t\beta(m)\left(\frac{m+t+1}{m}-\frac{1}{2}\right)}{\alpha(m)+\beta(m)t/2}.$$

To find a second polynomial $H_2(x, y)$ such that $H_2([k^{-1}]_q, a) = 0$, we work with the second LLL-reduced vector $\mathbf{b}_2$. Since L is generated from x-shift and y-shift polynomials of $f(x, y)$, it follows that, vector $\mathbf{b}_1$ will be an integer multiple of q^{-m}. Thus $||\mathbf{b}_1|| > q^{-m}$. So from Lemma 2.2 we obtain

$$||H_2(xX, yY)|| \le 2^{w/4}\left(\frac{\det L}{||\mathbf{b}_1||}\right)^{1/(w-1)} \le 2^{w/4}q^{m/(w-1)}(\det L)^{1/(w-1)}.$$

From the previous inequality and (5), we get

$$2^{w/4}q^{m/(w-1)}(\det L)^{1/(w-1)} \le 2^{w/4}q^{m/(w-1)}\zeta(w)^{1/(w-1)} = q^{\frac{m}{w-1}} w^{-\frac{w}{2(w-1)}} 2^{-\frac{w}{4(w-1)}}.$$

To satisfy $H_2([k^{-1}]_q, a) = 0$, we must have $q^{\frac{m}{w-1}} w^{-\frac{w}{2(w-1)}} \times 2^{-\frac{w}{4(w-1)}} < w^{-1/2}$. Hence

$$q^{m/(w-1)} < w^{-\frac{1}{2}+\frac{w}{2(w-1)}} 2^{\frac{w}{4(w-1)}} = w^{\frac{1}{2(w-1)}} 2^{\frac{w}{4(w-1)}}.$$

We conclude therefore that $q^m < w^{1/2}2^{w/4}$. The last inequality holds if m is large enough (since $w = O(m^2+mt)$), which completes the proof.

4. The improvement: proof of Proposition 1.1

If the dimension w of the lattice L is ≤ 35, then LLL algorithm will return, in practice, a shortest vector of the lattice. So the constant $\zeta(w)$ of relation (5) (it is a constant if we fix the dimension), can be replaced by another one which is much greater. If $w \le 35$, then we shall replace the bound of the first LLL-reduced vector by $\sqrt{\frac{w}{2\pi e}}\det(L)^{1/w}$.

A shortest lattice vector has length $||L|| \approx \sqrt{\frac{w}{2\pi e}} \times \det(L)^{1/w}$ (the Gaussian heuristic holds in our lattices). To see this, we compute the first minimum $||L||$ of L by estimating the radius of a ball with volume $vol(L) = \det L$. That is $||L|| \approx \sqrt{\frac{w}{2\pi e}}\det(L)^{1/w}$. Assume that $||H_1(xX, yY)|| < \frac{2}{3\sqrt{w}}$. Then from Lemma 2.1 we get $H_1([k^{-1}]_q, a) = 0$. But $||H_1(xX, yY)|| < \sqrt{\frac{w}{2\pi e}}\det(L)^{1/w}$. So, to satisfy $H_1([k^{-1}]_q, a) = 0$ we must have

$$\sqrt{\frac{w}{2\pi e}}\det(L)^{1/w} < \frac{2}{3\sqrt{w}}.$$

Rearranging the previous inequality yields,

$$\det L \le \sqrt{\frac{2\pi e}{w^2}}^{w}\left(\frac{2}{3}\right)^{w} = \sqrt{\frac{8\pi e}{9w^2}}^{w} = \zeta'(w).$$

Hence,

$$X^2Y^{1+\gamma(t,m)} < (\zeta'(w)q^{\alpha(m)+\beta(m)t})^{1/(\alpha(m)+\beta(m)t/2)}. \tag{8}$$

Now, $\zeta'(w) = \sqrt{\frac{8\pi e}{9w^2}}^{w}$, is much greater than $\zeta(w)$. For $t = 1$, $1 \le m \le 6$ the dimension w of L is ≤ 35. Plugging $m = 6, t = 1$ we obtain $X^2Y^{1.26} < 0.262 \cdot q^{1.157}$.

We also need a second polynomial $H_2(x, y)$ such that, $H_2([k^{-1}]_q, a) = 0$. From the third inequality of Lemma 2.2 we get

$$||H_2(xX, yY)|| < \frac{3}{2}||H_1(xX, yY)|| < \frac{3}{2}\cdot\frac{2}{3\sqrt{w}} = \frac{1}{\sqrt{w}}.$$

Again, by Lemma 2.1, we get $H_2([k^{-1}]_q, a) = 0$. Now, assuming our heuristic, we can calculate the resultant (with respect to x) and then we compute their integer roots. One of them will be the private key a.

5. An example

For the computations we used Sagemath [14]. Let

$q = 1420781990420358144729370324145404355374905166249,$

be a 160-bits prime number, the secret key

$a = 24251561979536311495125$ (75-bits)

and the ephemeral key

$k = 913551645485465300451420923974053878879771609110$ (160-bits)

Let (r, s) be the signature of the message m and let $x(A + y) + B \equiv 0 \pmod q$ the signing equation with

$$A = 269366230512225345569353296119811290445931088756,$$
$$B = 542189824416770300914626882856872739739223238744.$$

We set $f(x,y) = \frac{x(y+A)+B}{q}$. Note that $[k^{-1}]_q \cdot a > q/6^{3/2}$. In fact, we have an advantage of 6-bits (since $\text{bits}([k^{-1}]_q^2 \cdot a) = 163$ and $\text{bits}(q/6^{3/2}) = 157$). According to Table 1 we expect to find a. If we try to apply the method of [13] we get a polynomial $H(x,y)$ with $H([k^{-1}]_q, a) \neq 0$, as was expected. We consider the lattice, with parameters $m = 6$, $t = 1$, and $X = 2^{44}, Y = 2^{75}$, which is generated from the coefficients of the polynomials

$$\{1, x, xf, x^2, x^2 f, f^2, \ldots, x^6, x^6 f, \ldots, f^6, y, yf, .., yf^6\}.$$

We apply LLL algorithm to the rows of the resulting matrix of dimension 35×35. The first two vectors after LLL-reduction provide us with the polynomials (after multiplying with q^{-6})

$$H_1(x,y) = -502543239121201023339312059640271269044857887773\, x^6 y^7 + \cdots,$$
$$H_2(x,y) = 289718627031716294189936830682219285510686569846 7x^6 y^7 - \cdots.$$

A straightforward calculation of the resultant $R(y) = res_x(H_1, H_2)$ provide us with a non-constant polynomial of degree 48, such that $R(a) = 0$.

Remark 5.1. In (EC)DSA if we apply Shank's baby steps-giant steps algorithm (or even Pollard's algorithm), then the discrete logarithm of the public key R, is computed in roughly $q^{1/2}$ steps, where q is the largest prime factor of $p-1$. In our example q has 160-bits. So it is infeasible to apply this attack, even if a (EC)DSA private key (in our example a) is relatively small. Furthermore, in the previous example a has 75-bits, so even a brute force is infeasible.

6. Conclusions

In this paper we improved the result of [13]. We applied Coppersmith's method to a lattice of Boneh–Durfee type [6]. The execution time of our attack is dominated by the running time of the LLL-algorithm in lattices of dimension 35. Our attack is valid when the private key and the inverse of one ephemeral key $[k^{-1}]_q$ satisfy a suitable inequality (k can be large). Equivalently, the attack holds if some bits of the keys are known. Note that, we do not address here how the bits of a and $[k^{-1}]_q$ are to be determined. This may be achieved if we implement fault attacks [12]. Also, the same attack is feasible if we consider the pair $([a^{-1}]_q, k)$ instead of $([k^{-1}]_q, a)$. This can be done, if we multiply both sides of equation (1) by $-(as)^{-1} \pmod q$.

Acknowledgements

The author is indebted to the anonymous referees for their helpful suggestions.

References

[1] L. Adleman, J. DeMarrais, A subexponential algorithm for discrete logarithms over all finite fields, in: Advances in Cryptology, in: LNCS, vol. 773, 1994, pp. 147–158.
[2] A. Becker, N. Gama, A. Joux, Solving shortest and closest vector problems: the decomposition approach, LMS J. Com. Math. 17 (2014) 49–70.
[3] I.F. Blake, T. Garefalakis, On the security of the digital signature algorithm, Des. Codes Cryptogr. 26 (2002) 87–96.
[4] D. Boneh, R. Venkatesan, Hardness of computing the most significant bits of secret keys in Diffie–Hellman and related schemes, in: Advances in Cryptology, CRYPTO'96, in: LNCS, vol. 1109, 1996, pp. 129–142.
[5] Don Coppersmith, Small solutions to polynomial equations, and low exponent RSA vulnerabilities, J. Cryptology 10 (1997) 233–260.
[6] Glenn Durfee, Cryptanalysis of RSA using algebraic and lattice methods, Thesis, Stanford, 2002.
[7] FIPS PUB 186-4, Digital Signature Standard (DSS).
[8] T. ElGamal, A public-key cryptosystem and a signature scheme based on discrete logarithms, IEEE Trans. Inform. Theory 31 (1985) 469–472.
[9] Nicolas Gama, Phong Q. Nguyễn, Predicting lattice reduction, in: Eurocrypt 2008, in: LNCS, vol. 4965, 2008, pp. 31–51.
[10] D. Panario, X. Gourdon, P. Flajolet, An analytic approach to smooth polynomials over finite fields, in: ANTS III, in: LNCS, vol. 1423, 1998, pp. 226–236.
[11] N.A. Howgrave-Graham, N.P. Smart, Lattice attacks on digital signature schemes, Des. Codes Cryptogr. 23 (2001) 283–290.
[12] D. Naccache, Phong Q. Nguyễn, M. Tunstall, C. Whelan, Experimenting with faults, lattices and the DSA, LNCS 3386 (2005) 16–28.
[13] Dimitrios Poulakis, Some lattice attacks on DSA and ECDSA, Appl. Algebra Engrg. Comm. Comput. 22 (5–6) (2011) 347–358.
[14] W.A. Stein, et al., Sage Mathematics Software, The Sage Development Team.