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 $\{1, 2, \dots, q-1\}$, 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 $\{2, 3, \dots, q-1\}$. 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/© 2016 Elsevier B.V. All rights reserved.

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*

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

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*

$$||\mathbf{b}_1|| < 2^{(w-1)/4}(\det L)^{1/w},$$

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