Information Leakage Attacks against Smart Card Implementations of the Elliptic Curve Digital Signature Algorithm

Tanja Römer and Jean-Pierre Seifert

Infineon Technologies Corporation
Security & ChipCard ICs
Technical Innovations, D-81609 Munich, Germany
{Tanja.Roemer,Jean-Pierre.Seifer}@infineon.com

Abstract. In this article we will be concerned with a polynomial-time attack against the ECDSA, which computes the secret key of the ECDSA if a few bits of the ephemeral-key from several ECDSA-signatures are known. The number of needed bits per signature is 12, if one has access to an ideal lattice basis reduction algorithm computing the n^{th} successive minimum of a lattice with rank n. The aforesaid bits of the ephemeral-key can be obtained from insecure ECDSA implementations by so called side-channel-attacks like Timing, Simple-Power-Analysis, Differential-Power-Analysis, Electromagnetic or Differential-Fault attacks. Our attack combines a recent idea of Howgrave-Graham and Smart with an old lattice attack against linear congruential pseudo-random number generators due to Frieze, Hastad, Kannan, Lagarias und Shamir. In contrast to Howgrave-Graham and Smart, our approach enables the exact determination of the number of needed (side-channel) bits and uses an easier lattice problem making the attack very practical.

Keywords: Cryptanalysis, ECDSA, Lattice, Lattice basis reduction, LLL, side-channel-attacks, successive minimum.

1 Introduction

The ECDSA *(Elliptic Curve Digital Signature Algorithm)*, see for, e.g., [JM], is a digital signature algorithm whose security is based on the discrete logarithm problem for elliptic curves (abbreviated as ECDLP for Elliptic Curve Discrete Logarithm Problem) and is derived naturally from the DSA which in turn is based on the El-Gamal signature algorithm. For a thorough introduction into the DSA and the El-Gamal signature we refer the reader to [MvOV].

Under slight modifications and assuming the random oracle assumption Bellare et alii [BPVY] have shown that the security of the ECDSA can be reduced to the ECDLP. Excluding insecure elliptic curves the ECDLP needs in general exponential time to be solved, see for, e.g., [BSS]. Thus, practically the ECDSA cannot be broken by solving the ECDLP.

I. Attali and T. Jensen (Eds.): E-smart 2001, LNCS 2140, pp. 211–219, 2001.

However, it is well known that knowledge of the ephemeral-key k of the ECDSA breaks the system. Moreover, choosing the ephemeral-key k uniformly at random is as well very important, which is due to Bellare et alii [BGM].

This article describes a novel attack against the ECDSA, which is a combination of classical cryptanalysis and a side-channel attack. Instead of attacking directly the secret key d we use lattice methods to attack the randomly chosen k_i from several card signatures. For this purpose the attack assumes that we can learn through a side-channel some bits of the the aforesaid randomly chosen ephemeral-keys k_i corresponding to the card signatures. Our attack is based on an idea of [HGS] and using methods from the geometry of numbers according to [FHK$^+$] we can improve the attack of [HGS] substantially while also extending their attack to the elliptic curve variant of the DSA. For a recent survey on lattice methods in cryptography we refer to [NS].

Gaining knowledge of some secret bits of a smart card is in insecure implementations possible by exploiting methods relying on side-channel attacks such like Timing, Simple-Power-Analysis, Differential-Power-Analysis, Electromagnetic or Differential-Fault attacks. For a thorough description of these attacks we refer to [HJMS] and [CKN].

2 Definitions

We now give a brief introduction into basic terms of the lattice theory and elliptic curves and refer the reader for detailed introductions to [Kan,Lov,BSS,Kob99,Men].

$\mathbb{R}^m$ denotes the m-dimensional real Euclidean vector space and e_i the i^{th} unit vector in $\mathbb{R}^m$, $\langle\cdot,\cdot\rangle$ the canonical scalar product in $\mathbb{R}^m$ and $\|v\| := \sum_{i=1}^m v_i^2$ for $v \in \mathbb{R}^m$ the Euclidean norm. A *lattice* L is a discrete additive subgroup of the $\mathbb{R}^m$ with $L := \{y \in \mathbb{R}^m \mid y = a_1 b_1 + \cdots + a_k b_k,\ a_i \in \mathbb{Z}\}$, $b_1, \ldots, b_k \in \mathbb{R}^m$ linear independently over $\mathbb{R}^m$ and $k \leq m$. $[b_1, \ldots, b_k]$ is called a *basis* of the lattice L. The i^{the} *successive minimum* $\lambda_i(L)$ of a lattice L is the smallest positive real number r, such that there exists i linear independent vectors $v_1, \ldots, v_i \in L$ of maximum length r, i.e., $\lambda_i(L) = \min_{\text{l.u. } v_1,\ldots,v_i \in L} \max_{j \in \{1,\ldots,i\}} \|v_j\|$.

An elliptic curve (in affine coordinates) over a finite field $\mathbb{K}$ is a set $E(\mathbb{K})$ of points (X, Y) satisfying an equation of the form

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6, \quad a_i \in K,$$

together with a point at infinity $\mathcal{O}$. The set $E(K)$ is an abelean group wrt. addition $+$, where $\mathcal{O}$ is the neutral element, see for, e.g., [BSS]. The order of a point $P \in E(K)$ is the smallest natural number n with $nP = \mathcal{O}$. The ECDLP is given by the following problem. For two given points P and Q on an elliptic curve find the smallest natural number d satisfying $Q = dP$. For a general elliptic curve the ECDLP is only known to be solvable in exponential time.

3 The ECDSA

We now give a brief introduction into the ECDSA, for a thorough description we refer to [JM]. Moreover, for simplicity we assume in the following that we are using a prime field $\mathbb{K} = \mathbb{F}_p$, i.e., p is a prime greater than 2. However, our attacks works also fine over fields of the form $\mathbb{F}_{2^m}$.

We consider the situation where Alice wants to send a signed message m to Bob. Firstly, Alice chooses her public key $(E(K), P, n, Q)$ and as well a private key $d \in [1 : n-1]$. Here, $E(\mathbb{K})$ is an elliptic curve over $\mathbb{K}$ and P a point of prime order n on the curve $\mathbb{K}$ with $Q = dP$ and $n \mid |E(K)|$.

To sign the message $m \in \mathcal{M}$ from an appropriate message space $\mathcal{M}$, Alice now chooses uniformly at random a number $k \in [1 : n-1]$, the so called *ephemeral*-key. Hereafter, Alice computes $kP =: (x_1, y_1)$, $r := x_1 \bmod n$ and as well $s := k^{-1}(h(m) + dr) \bmod n$, where $h : \mathcal{M} \to \mathbb{K}$ denotes an arbitrary cryptographic hash-function. Alice now sends Bob the message m and the corresponding signature (r, s).

In order to verify the signature (r, s) of the message m, Bob computes with the public key $(E(K), P, n, Q)$ of Alice as a first step $w := s^{-1} \bmod n$. Then, Bob computes $u_1 := h(m)w \bmod n$, $u_2 := rw \bmod n$, $u_1P + u_2Q =: (x_0, y_0)$ and $v := x_0 \bmod n$. Finally, to check the authenticity of the signature (r, s), Bob checks that $v = r$ holds.

As already said above, the security of the ECDSA is based on the ECDLP and indeed under slight modifications and assuming the random oracle assumption ([BPVY]) its security is reducible to ECDLP. Thus, excluding insecure elliptic curves the ECDSA cannot be broken by solving the ECDLP in theory.

In the next section, however, we will sketch a new practical lattice attack on the ECDSA which tries to reconstruct the secret key d from short ephemeral-key fragments, i.e., by using only some bits of several keys k generated by several card signatures.

4 The Attack

We consider the scenario, where Alice's public key is given by $(E(K), n, P, Q)$ and her secret key by d. Moreover, we assume that we have signed l messages m_i, $i = 1, \ldots, l$, and obtained their corresponding card signatures (r_i, s_i), $i = 1, \ldots, l$. Now, we want to compute the ephemeral keys k_i, $i = 1, \ldots, l$, chosen uniformly at random by Alice for every single signature (r_i, s_i), $i = 1, \ldots, l$. After having computed the ephemeral keys k_i, $i = 1, \ldots, l$, we directly can compute Alice secret key d.

From the ECDSA-signature equation

$$s_i := k_i^{-1}(h(m_i) + dr_i) \bmod n, \quad i = 1, \ldots, l,$$

we get

$$s_ik_i - dr_i = h(m_i) \bmod n, \quad i = 1, \ldots, l.$$

Substituting in these l equations with the $l+1$ variables k_i, $i = 1, \dots, l$, and d the variable d by $r_l^{-1} s_l k_l - h(m_l) r_l^{-1} \bmod n$ yields the system

$$s_i k_i - r_i r_l^{-1} s_l k_l = -r_i h(m_l) r_l^{-1} + h(m_i) \bmod n, \quad i = 1, \dots, l-1.$$

Renaming again the variables yields another system of equations

$$b_{ii} k_i + b_{il} k_l = d_i \bmod n, \quad i = 1, \dots, l-1$$

with only $l-1$ equations and l variables $k_1, \dots, k_l$. However, this underdetermined system has naturally no unique solution. Nevertheless, it is known that a unique solution exists and indeed can be computed quickly if some small fraction of the bits of the $k_1, \dots, k_l$ is known, see for, e.g., [FHK$^+$].

Wlog. let $\log n$ the bitlength of the k_i, $i = 1, \dots, l$. If, now, the most significant t bits of the k_i are known, we can write the k_i as

$$k_i = k_i^{(1)} + k_i^{(2)},$$

where the $k_i^{(1)}$ are all known, and $|k_i^{(2)}| \leq n2^{-t}$ holds. Applying this partial knowledge about the k_i's to the aforesaid system of equations and again renaming the coefficients we get the following system of equations:

$$a_{ii} k_i^{(2)} + a_{il} k_l^{(2)} = c_i \bmod n \quad \text{with } |k_i^{(2)}| \leq n2^{-t}. \tag{1}$$

Thus, we have obtained an underdetermined system with the variable constraint $|k_i^{(2)}| \leq n2^{-t}$ where t denotes the number of known most significant bits of the k_i's. To solve this system we use the following theorem.

Theorem 1. *Let*

$$\sum_{j=1}^{l} a_{ij} x_j = c_i \bmod p \tag{2}$$

a system with $a_{ij}, c_i \in \mathbb{Z}$, $i = 1, \dots, s$, p prime and $s \leq l$, and

$$L = \left\{ y \in \mathbb{R}^l \;\middle|\; y = \sum_{i=1}^{s} v_i (a_{i1}, \dots, a_{il})^\top + v_{s+1} p e_1 + \cdots + v_{s+l} p e_l,\ v_i \in \mathbb{Z} \right\}$$

a lattice in $\mathbb{R}^l$ satisfying $\|x\| \leq p \lambda_l^{-1}(L) 2^{-1}$, then there exists at most one solution x for this system. If the a_{ij}, c_i and p are all known for all i, j, then there exists an algorithm which computes for fixed l in polynomial time the solution x or proves that there is no solution.

Proof. The proof of the theorem follows mainly the ideas given in [FHK$^+$]. The idea is to construct from the underdetermined modular system of equations a system of equations with l equations and l variables over $\mathbb{Z}$. Naturally, such a system has at most one solution. We note that the proof will explicitly construct the unique solution, provided that a solution exists.

We start with the recently presented algorithm due to Blömer [Bl], which computes for the given lattice L l linearly independent vectors

$$w_1, \ldots, w_l \in L$$

with $\|w_i\| = \lambda_i(L)$ for $i = 1, \ldots, l$. Its running time is $3^l \cdot l! \cdot s^{O(1)}$, where s denotes the size of the lattice. Thus, for fixed l it is a polynomial-time algorithm. As the vectors $w_1, \ldots, w_l$ are linearly independent lattice vectors we know that there exists some integral $l \times (s + l)$ matrix M satisfying

$$\begin{pmatrix} w_{11} & \cdots & w_{1l} \\ \vdots & & \vdots \\ w_{l1} & \cdots & w_{ll} \end{pmatrix} = M \begin{pmatrix} a_{11} & \cdots & a_{1l} \\ \vdots & & \vdots \\ a_{s1} & \vdots & a_{sl} \\ p & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & p \end{pmatrix}.$$

Now, multiplying both sides of the system (2) from left with this matrix M, we get a new modular system

$$\sum_{j=1}^{l} w_{ij} x_j \equiv c'_i \bmod p, \quad i = 1, \ldots, l. \tag{3}$$

Clearly, every solution x of (2) is by construction also a solution of (3). Now, considering an $x \in \mathbb{Z}^l$ satisfying

$$\|x\| \leq \frac{1}{2} p \lambda_l^{-1}(L),$$

we get that

$$\begin{aligned} \left\| \sum_{j=1}^{l} w_{ij} x_j \right\| &\leq \|w_i\| \cdot \|x\| \\ &\leq \lambda_i(L) \cdot \frac{1}{2} p \lambda_l^{-1}(L) \\ &\leq \lambda_l(L) \cdot \frac{p}{2} \lambda_l^{-1}(L) \\ &\leq \frac{p}{2}. \end{aligned}$$

Therefore, choosing the c'_i for $i = 1, \ldots, l$ such that $|c'_i| < p/2$, ensures that an integral solution $x \in \mathbb{Z}^l$ of the system

$$\sum_{j=1}^{l} w_{ij} x_j \equiv c'_i, \quad i = 1, \ldots, l, \tag{4}$$

over $\mathbb{Z}$ will also be an unique solution of the system (3) satisfying $\|x\| \leq \frac{1}{2}p\lambda_l^{-1}(L)$. This is due to the fact that the aforesaid system (4) has at most one solution over $\mathbb{Z}$. Consequently, our starting system (2) has at most one solution satisfying $\|x\| \leq \frac{1}{2}p\lambda_l^{-1}(L)$. □

Now, in order to determine the unknown fraction of the k_i, i.e., $k_i^{(2)}$, we will apply the former theorem to the above equation system (1). However, the applicability of Theorem 1 requires

$$|k_i^{(2)}| \leq n\lambda_l(L)^{-1}2^{-1}l^{-1/2}.$$

With the subconstraint $|k_i^{(2)}| \leq n2^{-t}$ for the unknowns $k_i^{(2)}$ this means that one needs to know

$$t = \log\lambda_l(L) + 1 + \frac{1}{2}\log l$$

bits of every k_i. Therefore, the number t of known bits in advance only depends on $\lambda_l(L)$. Luckily, if the coefficients a_{ij} are chosen uniformly at random, one can show that with high probability

$$\lambda_l(L) < 5\sqrt{l}\varepsilon^{-1/l}n^{1-l-1/l}$$

is satisfied, where $\varepsilon > 0$ is an arbitrarily small positive constant. This will be shown in the following theorem whose proof combines ideas from [FHK$^+$] with latest lattice research due to [Ba].

Theorem 2. *Let n be a prime, $\varepsilon > 0$ and*

$$L := \{y \in \mathbb{R}^l \mid y = \mathbb{Z}a_1 + \ldots + \mathbb{Z}a_{l-1} + \mathbb{Z}ne_1 + \ldots + \mathbb{Z}ne_l\}$$

a lattice in $\mathbb{Z}^l$, where $a_1 := (a_1, 0, \ldots, 0, a_l), \ldots, a_{l-1} := (0, \ldots, 0, a_{l-1}, a_l)$ are randomly chosen in $\mathbb{Z}^l$. Then, with probability $\geq 1 - \varepsilon - O(1/n^{(l-1)/l})$ it holds that

$$\lambda_l(L) \leq \left(\frac{\pi^{l/2}}{\Gamma(\frac{l}{2}+1)}\right)^{1/l} l\,\varepsilon^{-1/l}\,n^{1-(l-1)/l}.$$

Proof. As an abbreviation we define for the basis

$$B := (a_1, \ldots, a_{l-1}, ne_1, \ldots, ne_l)$$

of the lattice L the so called span(B) as

$$\operatorname{span}(B) := \{y \in \mathbb{R}^l \mid y = \mathbb{R}a_1 + \cdots + \mathbb{R}a_{l-1} + \mathbb{R}ne_1 + \cdots + \mathbb{R}ne_l\}.$$

According to Kannan [Kan] the lattice dual to the given lattice L is given by

$$L^* := \{z \in \operatorname{span}(B) \mid \forall y \in L : \langle z, y\rangle \in \mathbb{Z}\},$$

which means particularly that

$$\begin{aligned} L^* &= \{z \in \mathbb{R}^l \mid \forall y \in L : \langle z, y\rangle \in \mathbb{Z}\} \\ &= \{z \in \tfrac{1}{n}\mathbb{Z}^l \mid \langle z, a_i\rangle \in \mathbb{Z}, i = 1, \ldots, l-1\}, \end{aligned}$$

and moreover also that

$$nL^* = \{z \in \mathbb{Z}^l \mid \langle z, a_i\rangle \equiv 0 \bmod n, i = 1, \ldots, l-1\}.$$

Thus, we see that for a randomly chosen point $z \in \mathbb{Z}^l$ we have

$$\Pr_{z \in_{\mathcal{U}} \mathbb{Z}^l}[\langle z, a_i\rangle \equiv 0 \bmod n] = \frac{1}{n}$$

for every $i = 1, \ldots, l-1$, which in turn implies that

$$\Pr_{z \in_{\mathcal{U}} \mathbb{Z}^l}[z \in nL^*] = \left(\frac{1}{n}\right)^{l-1}.$$

Let $S_R(o) := \{x \in \mathbb{R}^l \mid \|x\| < R\}$ the usual open sphere with radius R around the origin $o := (0, \ldots, 0)$ and denote by $G_R(o) := |S_R(o) \cap \mathbb{Z}^l|$ the number of $\mathbb{Z}$ lattice points within $S_R(o)$. From the above we are now able to infer that

$$\Pr_{z \in_{\mathcal{U}} \mathbb{Z}^l}[S_R(o) \cap nL^* = \emptyset] = \left(1 - 1/n^{l-1}\right)^{G_R(o))} \geq 1 - G_R(o)/n^{l-1}.$$

Thus, we see that

$$\lambda_1(nL^*) \geq R \quad \Longleftrightarrow \quad \lambda_1(L^*) \geq \frac{R}{n}$$

holds with probabilty $\geq 1 - S_R(o)/n^{l-1}$. Due to Walfisz [Wa] the number $G_R(o)$ is for $R \to \infty$ given by

$$G_R(o) = \frac{\pi^{l/2}}{\Gamma(\frac{l}{2}+1)} R^l + O\left(R^{(l-1)}\right).$$

Choosing now

$$R := \left(\frac{\pi^{l/2}}{\Gamma(\frac{l}{2}+1)}\right)^{-1/l} \varepsilon^{1/l}\ n^{(l-1)/l}$$

yields for $n \to \infty$ that

$$G_R(o) = \varepsilon\ n^{(l-1)} + O\left(n^{(l-1)^2/l}\right),$$

from which we conclude that

$$\lambda_1(L^*) \geq \frac{R}{n} \geq \frac{6}{25}\ \sqrt{l}\ n^{(l-1)/l-1}\ \varepsilon^{1/l}$$

holds with probability $1-\varepsilon+O(n^{-(l-1)/l})$. If we now apply the so called transference bound

$$\lambda_1(L^*) \cdot \lambda_l(L) \leq l$$

due to Banaszcyk [Ba], we finally get our promised result

$$\lambda_l(L) \leq \frac{l}{\lambda_1(L^*)} \leq \frac{25}{6}\sqrt{l}\; n^{1-(l-1)/l}\; \varepsilon^{-1/l}$$

□

If we yet put together all the results we have so far, we get that with

$$t \geq \frac{1}{l}\log_2 n + \log_2 l + \frac{1}{l}\log_2 \varepsilon + 3.06$$

known bits of of the randomly chosen k_i we are able to recover the rest of the k_i. The goal is now simultaneously maximizing the probability $1-\varepsilon+O(n^{-(l-1)/l})$ and minimizing the number t of needed bits in the k_i. We simply set $\varepsilon := 0.01$ and investigate the two functions

$$\begin{aligned} f_1(n,l) &:= \frac{1}{l}\log_2 n + \log_2 l - \frac{1}{l}\log_2(0.01) + 3.06 \\ f_2(n,l) &:= \epsilon + O(n^{-(l-1)/l}) \end{aligned}$$

concerning local minima and maxima. However, for f_2 we need to consult Walfisz [Wa] for the hidden constants in the O resulting from $G_R(o)$. Precise determination of these constants and searching for local minima and maxima results finally in a probability of 0.99 and 12 known bits of the k_i if we assuming that n is a 160-bit prime.

Thus, we have proved that with only 12 known bits of every k_i, $i = 1, \ldots, 50$, the ECDSA can be broken in practice. We stress, that these are proven worst-case bounds, whereas in practical experiments we needed much less than 12 bits. Moreover, our attack can be extended to cover even the case when the known bits are somewhere located within the k_i's.

5 Summary

Again, lattice methods have been used to show that a secure proven signature method like the ECDSA can be broken under some circumstances. This implies, that it is very important to protect hard- and software implementations of the ECDSA on smart cards very carefully against side channel attacks in order to avoid any information leakage of secret data to a potential attacker.

References

Ba. W. Banaszczyk, "New Bounds in Some Transference Theorems in the Geometry of Numbers", *Mathematische Annalen* Vol. 296, pp. 625-635, 1993. 216, 218

BGM. M. Bellare, S. Goldwasser, D. Micciancio, "Pseudo-random number generation within cryptogrphic algorithms. The DSS case", *Proc. of CRYPTO '97*, pp. ?-?, LNCS Vol. 1294, Springer Verlag, 1997. 212

BSS. I. Blake, G. Seroussi, N. Smart, *Elliptic Curves in Cryptography*, Cambridge University Press, 1999. 211, 212

Bl. J. Blömer, "Closest Vectors, Successive Minima, and Dual HKZ-Bases of Lattices", *Proc. of 27th ICALP*, pp. ?-?, LNCS Vol. 1835, Springer Verlag, 2000. 215

BPVY. E. Brickell, D. Pointcheval, S. Vaudenay, M. Yung, "Design validations for discrete logarithm based signature schemes", *Proc. of PKC 2000*, pp. 276-292, LNCS Vol. 1751, Springer Verlag, 2000. 211, 213

CKN. J.-S. Coron, P. Kocher, D. Naccache, "Statistics and secret leakage", *Proc. of Financial Cryptography 2000*, Springer LNCS, vol. ?, pp. ?-?, 2000. 212

FHK$^+$. A. Frieze, J. Hastad, R. Kannan, J. Lagarias, A. Shamir, "Reconstructing Truncated Integer Variables Satisfying Linear Congruences", *SIAM J. Comp.* Vol. 17, pp. 262-280, 1988. 212, 214, 216

HJMS. E. Hess, N. Janssen, B. Meyer, T. Schütze, "Information leakage attacks against smart card implementations of cryptographic algorithms and countermeasures", *Proc. of EUROSMART-Security-Conference 2000*, pp. 53-64, 2000. 212

HGS. N. Howgrave-Graham, N. Smart, "Lattice attacks on digital signature schemes", Technical Report HPL-1999-90, HP Labs, 1999. 212

JM. D. Johnson, A. J. Menezes, "The Elliptic Curve Digital Signature Algorithm (ECDSA)", Technical Report CORR 99-34, Dept. of C&O, University of Waterloo, 2000. 211, 213

Kan. R. Kannan, "Algorithmic Geometry of Numbers", *Ann. Rev. Comput. Science* Vol. 2, pp. 231-267, 1987. 212, 216

Kob94. N. Koblitz, *A Course in Number Theory and Cryptography*, Springer Verlag, 1994.

Kob99. N. Koblitz, *Algebraic Aspects of Cryptography*, Springer Verlag, 1999. 212

Lov. L. Lovasz, *An Algorithmic Theory of Graphs, Numbers and Convexity*, SIAM, 1986. 212

Men. A. J. Menezes, *Elliptic Curve Public Key Cryptosystemes*, Kluwer Academic Publishers, 1993. 212

MvOV. A. J. Menezes, P. van Oorschot, S. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1993. 211

NS. P. Nguyen, J. Stern, "Lattice Reduction in Cryptology: An update", *Proc. 4th Algorithmic Number Theory Symposium*, pp. ?-?, LNCS Vol. 1838, Springer Verlag, 2000. 212

Wa. A. Walfisz, *Gitterpunkte in mehrdimensionalen Kugeln*, Polish Scientific Publishers, Warsaw, 1957. 217, 218