On the Security of Lenstra's Variant of DSA without Long Inversions

Arjen K. Lenstra[1] and Igor E. Shparlinski[2]

[1] Citibank, N.A., Technical University Eindhoven,
1 North Gate Road, Mendham, NJ 07945-3104, U.S.A.
arjen.lenstra@citicorp.com
[2] Department of Computing, Macquarie University,
Sydney, NSW 2109, Australia
igor@comp.mq.edu.au

Abstract. We use bounds of exponential sums to show that for a wide class of parameters the modification of the DSA signature scheme proposed by A. K. Lenstra at Asiacrypt'96 is as secure as the original scheme.

1 Introduction

Let p and $q \geq 3$ be prime numbers with $q|p-1$. As usual $\mathbb{F}_p$ and $\mathbb{F}_q$ denote fields of p and q elements which we assume to be represented by the elements $\{0, \dots, p-1\}$ and $\{0, \dots, q-1\}$, respectively.

For a rational number z and $m \geq 1$ we denote by $\lfloor z \rfloor_m$ the unique integer a, $0 \leq a \leq m-1$ such that $a \equiv z \pmod m$ (provided that the denominator of z is relatively prime to m).

The *Digital Signature Algorithm*, or DSA, can be described in the following way. Let $\mathcal{M}$ be the set of messages to be signed and let $h : \mathcal{M} \longrightarrow \mathbb{F}_q$ be an arbitrary hash-function. Let $g \in \mathbb{F}_p$ be a fixed element of multiplicative order q, that is, $g^q = 1$, which is *publicly* known (as well as p and q). Finally, fix a certain element $\alpha \in \mathbb{F}_q^*$ which is the *secret* key known only to the signer. For a *message* $\mu \in \mathcal{M}$ we select a random element $k \in \mathbb{F}_q^*$ called a *nonce* and we define the function

$$r(k) = \left\lfloor \left\lfloor g^k \right\rfloor_p \right\rfloor_q \qquad \text{and} \qquad s(k, \mu) = \left\lfloor k^{-1} \left(h(\mu) + \alpha r(k) \right) \right\rfloor_q. \tag{1}$$

The pair $(r(k), s(k, \mu))$ is the *DSA signature* of the message μ with nonce k.

Modular inversion of the nonce k in (1) is a time consuming operation. To improve the performance several inversion-free modifications of the basic scheme have been proposed, see [13] as well as Sections 11.5.2 and 11.5.4 in [8] and Section 20.4 of [14]. On the other hand, these schemes, although quite close to the original DSA scheme, may not be compatible with it, see the discussion in [6]. Thus to overcome the incompatibility problem (and a large signature size for some of the aforementioned modifications) a very different algorithm has been proposed in [6]. This algorithm follows the basic DSA scheme except that

K. Kim (Ed.): PKC 2001, LNCS 1992, pp. 64–72, 2001.

the nonce k is generated in a special way which allows to generate k and $\lfloor k^{-1} \rfloor_q$ simultaneously at reasonably low computational cost.
The algorithm from [6] works as follows, in a special partial case. Given a prime q and two more integer parameters $T \geq 2$ and $m \geq 1$:

- Select independently and uniformly at random $2m$ integers $t_1, \ldots, t_{2m} \in [2, T]$;
- For $i = 1, \ldots, 2m$, compute $u_i = \lfloor q^{-1} \rfloor_{t_i}$ and $w_i = (qu_i - 1)/t_i$;
- For $i = 1, \ldots, 2m$, using the identity $t_i^{-1} \equiv w_i \pmod q$, compute $v_i = \lfloor t_i^{-1} \rfloor_q$;
- Compute and output

$$\kappa = \lfloor t_1 \ldots t_m v_{m+1} \ldots v_{2m} \rfloor_q \qquad \text{and} \qquad \lambda = \lfloor v_1 \ldots v_m t_{m+1} \ldots t_{2m} \rfloor_q.$$

It is easy to see that $\lambda = \lfloor \kappa^{-1} \rfloor_q$. The efficiency of the algorithm is based on the observation that for each arithmetic operation it performs one of the operands is of size T. Furthermore, once $\lfloor q \rfloor_{t_i}$ has been computed, the inversion required for the computation of u_i involves only numbers of size $\leq T$. Thus if the bit length of T is essentially smaller than the bit length of q and m is reasonably small this algorithm is faster than the standard inversion modulo q using the Extended Euclid Algorithm. The efficiency of this algorithm (and its slightly more general form described in [6]) has been numerically verified, see [6] and Section 4.

However, it has remained an open question whether this new way of generating k and $\lfloor k^{-1} \rfloor_q$ undermines the security of the DSA. In [6, Section 3] some heuristic arguments in support of the security of the new scheme are given. At the rumpsession of Asiacrypt'96, S. Vaudenay [16] presented a partial cryptanalysis of the scheme that only affected the security if the t_i are chosen in some particularly bad way that is explicitly excluded in [6, Section 3].

In this paper we show that using bounds of character sums one can establish rigorous security results for the above scheme (for some values of the parameters T and m). In fact we show that the distribution of the value of κ is exponentially close to the uniform distribution. Therefore any algorithm attacking this modification immediately implies an attack on the original scheme with exponentially close probabilities of success.

More precisely, for $k \in \mathbb{F}_q^*$, let $P_{m,T}(k)$ be the probability that the output κ of the above algorithm equals k. We use some known bounds of exponential sums to prove that for a wide range of parameters T and m the *statistical distance*

$$\Delta(m,T) = \sum_{k \in \mathbb{F}_q^*} \left| P_{m,T}(k) - \frac{1}{q-1} \right| \tag{2}$$

is exponentially small, namely

$$\Delta(m,T) < q^{-\delta}$$

for some constant $\delta > 0$. The range of parameters allowed by this general result do, however, not seem to be of much practical value. We show that under the assumption of the Extended Riemann Hypothesis an essentially stronger result can be obtained that allows parameter choices in a more realistic and practical range.

We stress that the uniformity of distribution of the nonce k is absolutely essential. Indeed, it has been shown in the series of papers [5,10,11] that the knowledge of some bits of k can be used to break the DSA (that is, recovering the private key α) in polynomial time.

2 Preparations

Let $\mathcal{X}$ be the set of multiplicative characters of the multiplicative group $\mathbb{F}_q^*$, see Section 1 of Chapter 5 of [7]. We denote by $\mathcal{X}^*$ the subset of non-trivial characters.

We define

$$\sigma(T) = \max_{\chi \in \mathcal{X}^*} \left| \sum_{t=2}^{T} \chi(t) \right| .$$

Lemma 1. *For any integers $T \ge 2$ and $m \ge 1$ the bound*

$$\Delta(m,T) < q^{1/2} \sigma(T)^{2m-1} T^{-2m+1/2}$$

holds for the statistical distance $\Delta(m,T)$ given by (2).

Proof. Let $N_{m,T}(k)$ be the number of sequences $t_1, \ldots, t_{2m} \in [2,T]$ for which $t_1 \ldots t_m t_{m+1}^{-1} \ldots t_{2m}^{-1} \equiv k \pmod q$. Then $P_{m,T}(k) = N_{m,T}(k) T^{-2m}$.

From the following well-known identity

$$\sum_{\chi \in \mathcal{X}} \chi(z) = \begin{cases} q-1, & \text{if } z = 1, \\ 0, & \text{otherwise,} \end{cases}$$

which holds for any $z \in \mathbb{F}_q^*$ (cf. [7, Theorem 5.4]), we derive

$$N_{m,T}(k) = \frac{1}{q-1} \sum_{t_1,\ldots,t_{2m}=2}^{T} \sum_{\chi \in \mathcal{X}} \chi(t_1 \ldots t_m t_{m+1}^{-1} \ldots t_{2m}^{-1} k^{-1}).$$

We remark that $\chi(\lambda^{-1}) = \overline{\chi(\lambda)}$ for $\lambda \in \mathbb{F}_q^*$ and that $z\bar{z} = |z|^2$, where $\bar{z}$ denotes the conjugate of a complex number z. Therefore, changing the order of summation, separating the term $T^{2m}/(q-1)$ which corresponds to the trivial character, and noting that k^{-1} runs through $\mathbb{F}_q^*$ together with k we obtain

$$\left| N_{m,T}(k) - \frac{T^{2m}}{q-1} \right| = \frac{1}{q-1} \sum_{\chi \in \mathcal{X}^*} \chi(k) \left| \sum_{t=2}^{T} \chi(t) \right|^{2m} .$$

Therefore

$$\begin{aligned}
&\sum_{k\in\mathbb{F}_q^*}\left|N_{m,T}(k)-\frac{T^{2m}}{q-1}\right|^2\\
&\quad=\frac{1}{(q-1)^2}\sum_{k\in\mathbb{F}_q^*}\left(\sum_{\chi\in\mathcal{X}^*}\chi(k)\left|\sum_{t=2}^{T}\chi(t)\right|^{2m}\right)^2\\
&\quad=\frac{1}{(q-1)^2}\sum_{k\in\mathbb{F}_q^*}\sum_{\chi_1,\chi_2\in\mathcal{X}^*}\chi_1(k)\chi_2(k)\left|\sum_{t=2}^{T}\chi_1(t)\right|^{2m}\left|\sum_{t=2}^{T}\chi_2(t)\right|^{2m}\\
&\quad=\frac{1}{(q-1)^2}\sum_{\chi_1,\chi_2\in\mathcal{X}^*}\left|\sum_{t=2}^{T}\chi_1(t)\right|^{2m}\left|\sum_{t=2}^{T}\chi_2(t)\right|^{2m}\sum_{k\in\mathbb{F}_q^*}\chi_1(k)\chi_2(k).
\end{aligned}$$

Using that the product of two characters is a character as well and the identity

$$\sum_{k\in\mathbb{F}_q^*}\chi(k)=\begin{cases}q-1, & \text{if } \chi=\chi_0,\\ 0, & \text{otherwise,}\end{cases}$$

where χ_0 is the trivial character (cf. [7, Theorem 5.4]), we see that the inner sum vanishes unless

$$\chi_2(k)=\chi_1(k)^{-1}=\chi_1(k^{-1})=\overline{\chi_1(k)},\qquad k\in\mathbb{F}_q^*,$$

in which case it is equal to $q-1$. Therefore

$$\begin{aligned}
\sum_{k\in\mathbb{F}_q^*}\left|N_{m,T}(k)-\frac{T^{2m}}{q-1}\right|^2&=\frac{1}{q-1}\sum_{\chi\in\mathcal{X}^*}\left|\sum_{t=2}^{T}\chi(t)\right|^{2m}\left|\sum_{t=2}^{T}\overline{\chi(k)}\right|^{2m}\\
&=\frac{1}{q-1}\sum_{\chi\in\mathcal{X}^*}\left|\sum_{t=2}^{T}\chi(t)\right|^{4m}\le\frac{\sigma(T)^{4m-2}}{q-1}\sum_{\chi\in\mathcal{X}^*}\left|\sum_{t=2}^{T}\chi(t)\right|^{2}.
\end{aligned}$$

We have

$$\frac{1}{q-1}\sum_{\chi\in\mathcal{X}^*}\left|\sum_{t=2}^{T}\chi(t)\right|^2<\frac{1}{q-1}\sum_{\chi\in\mathcal{X}}\left|\sum_{t=2}^{T}\chi(t)\right|^2=T.$$

Hence

$$\begin{aligned}
\sum_{k\in\mathbb{F}_q^*}\left|P_{m,T}(k)-\frac{T^{2m}}{q-1}\right|^2&\le T^{-4m}\sum_{k\in\mathbb{F}_q^*}\left|N_{m,T}(k)-\frac{T^{2m}}{q-1}\right|^2\\
&\le\sigma(T)^{4m-2}T^{-4m+1}.
\end{aligned}$$

From the Cauchy inequality we obtain the desired result.

Thus to estimate the statistical distance we need upper bounds on $\sigma(T)$. The simplest and the most well known bound is given by the *Polya–Vinogradov* inequality

$$\sigma(T) \le q^{1/2} \ln q,$$

see [9, Theorem 2.2], which is non-trivial only for $T \ge q^{1/2+\varepsilon}$. However such values of T are too large to be useful for our application. Instead we use the *Burgess* bound, see [9, Theorem 2.3].

Lemma 2. *For any $\varepsilon > 0$ there exists $\gamma > 0$ such that*

$$\sigma(T) \le Tq^{-\gamma}$$

for $T \ge q^{1/4+\varepsilon}$ and sufficiently large q.

It is known that the *Extended Riemann Hypothesis*, or ERH, implies non-trivial upper bounds for much shorter sums. We therefore use a result that relies on the assumption of the ERH. In particular, we use a bound which follows from one of the results of [3].

Lemma 3. *Let*

$$v = \frac{\ln T}{\ln \ln q} \to \infty.$$

Then, assuming the ERH, the bound

$$\sigma(T) \le Tv^{-v/2+o(v)}$$

holds.

Proof. We recall that an integer $n \ge 1$ is called Y-smooth if all primes dividing it are $\le Y$. Let $\Psi(X,Y)$ denote the total number of Y-smooth numbers $\le X$. The following estimate is a substantially relaxed and simplified version of [4, Corollary 1.3]. Let $X = Y^u$; then for any $u \to \infty$ with $u \le Y^{1/2}$ we have the bound

$$\Psi(X,Y) \ll Xu^{-u+o(u)}. \tag{3}$$

It has been proved in [3, Theorem 2] that

$$\sigma(T) = O\left(\Psi\left(T, \ln^2 q \ln^{20} \ln q\right)\right),$$

provided that $u \to \infty$. One easily verifies that the bound (3) can be applied to the last function with $u = v/2 + o(v)$, producing the desired result.

3 Main Results

Now we are prepared to prove our main results.

Theorem 1. *For any $\varepsilon > 0$ and $A \ge 0$ there exists a constant $m_0(\varepsilon, A) > 0$ such that for any integers $T \ge 2$ and $m \ge 1$ satisfying the inequalities*

$$T \ge q^{1/4+\varepsilon} \qquad \text{and} \qquad m \ge m_0(\varepsilon)$$

the statistical distance $\Delta(m,T)$ given by (2) satisfies the bound $\Delta(m,T) \le q^{-A}$.

Proof. From Lemmas 1 and 2 we obtain the bound

$$\Delta(m,T) < q^{1/2}T^{-1/2}q^{-\gamma(2m-1)} \le q^{1/4-\gamma(2m-1)} \le q^{-A}$$

provided that $m \ge (4A+1)/8\gamma + 1$.

Unfortunately the range of parameters allowed by Theorem 1 does not seem to be of any practical value. However under the ERH an essentially stronger result can be obtained.

Theorem 2. *Assume the ERH. Then for any $A > 0$ and any integers $T \ge 2$ and $m \ge 1$ such that*

$$v = \frac{\ln T}{\ln \ln q} \to \infty \qquad \text{and} \qquad m \ge (2A+1)\frac{\ln q}{v \ln v} + 1$$

for sufficiently large q, the statistical distance $\Delta(m,T)$ given by (2) satisfies the bound $\Delta(m,T) \le q^{-A}$.

Proof. From Lemmas 1 and 3 we obtain the bound

$$\begin{aligned}\Delta(m,T) &< q^{1/2}T^{-1/2}v^{-(v/2+o(v))(2m-1)} \le q^{1/2}v^{-v(2m-1)/3}\\ &\le q^{1/2-(4A+2)/3} \le q^{-A},\end{aligned}$$

provided that q is large enough.

In particular, if q is about n bits long and T is selected about ℓ bits long with $\ell \ge \ln n^{1+\varepsilon}$, then for m of order $n/\ln \ell$ the algorithm of [6] generates a secure sequence of pairs $\kappa, \lambda = \lfloor \kappa^{-1} \rfloor_q$. Thus the values of T used in this algorithm can be rather small.

4 Practical Considerations

In [6] it was shown that generating k and $\lfloor k^{-1} \rfloor_q$ simultaneously as indicated in Section 1 and with $m = 3$ is about as fast as the regular method of computing $\lfloor k^{-1} \rfloor_q$ given a random k, for the common values $n = 160$ and $\ell = 32$ where n and ℓ are the bit lengths of q and T, respectively. In the analysis of [6] it was assumed

that the regular method makes use of Lehmer's method for the inversion. Thus, in environments where Lehmer's inversion is available there does not seem to be any good reason not to generate k and $\lfloor k^{-1} \rfloor_q$ in the regular way.
Lehmer's method is about twice faster than regular modular inversion (which is based directly on the Extended Euclidean Algorithm) because it replaces most of the extended precision integer divisions by floating point approximations. The disadvantage of Lehmer's method is, however, that it takes substantially more code and memory than regular modular inversion (or than the method from [6]). For computation in more restricted environments (such as a credit card chip) where the space and size needs of Lehmer's method cannot be met, the method of [6] may therefore be an option, because it would be faster than regular modular inversion, even if m is taken as large as 6.

Theorem 2, however, indicates that for $n = 160$ and $\ell = 32$ security can be guaranteed (under the ERH) only for substantially larger choices for m, namely m should be at least about 100. Obviously, such large m severely limit the practical applicability of the method from [6] reviewed in Section 1, assuming that provable security of the choice of k is required: implementation of the method makes sense only if very limited space is available, and division of extended precision integers (as required for regular modular inversion) is not available. It should be kept in mind, however, that the results presented in this paper are just theoretical lower bounds for the security and that in practice much smaller values of m should give satisfactory results, as also indicated in [6]. In fact even our theoretical results can be improved and extended; some further possibilities are indicated in Section 5. We do not present them here because our main motivation has been to indicate a possible way to establish rigorous proofs of security of the approach proposed in [6], rather than deriving all possible results of this kind.

An alternative way of using the idea behind the method from [6] in the vein of the method of [1], as informally and independently proposed by several different people, is as follows. Compute and store $S_1 = \{t_1, \ldots, t_{2r}\}$ and the corresponding $S_2 = \{v_1, \ldots, v_{2r}\}$ for some large value of r and compute the products over the four relevant random subsets of size m of $S_1 \bigcup S_2$ for each pair k, $\lfloor k^{-1} \rfloor_q$ to be generated, where r is substantially larger than m. Given the successful attack (cf. [12]) on the method from [1], however, this approach cannot be recommended.

5 Remarks

The algorithm itself as well as all our main tools, can be extended to composite moduli. The only difference is that Lemma 2 holds in the present form only for square-free moduli, however a slightly weaker result is known in the general case as well (which is nontrivial for $T \geq q^{3/8+\varepsilon}$).

One can also remark that if $T^{2\nu} < q$ for an integer $\nu \geq 1$ then

$$\sum_{\chi \in \mathcal{X}} \left| \sum_{t=2}^{T} \chi(t) \right|^{2\nu} = (q-1)M_\nu(T),$$

where $M_\nu(T)$ is the number of solutions of the equation (rather than a congruence)

$$t_1 \dots t_\nu = t_{\nu+1} \dots t_{2\nu}, \quad t_1, \dots, t_{2\nu} \in [2, T]$$

which can be estimated using various number theoretic tools. In particular, the bound

$$M_\nu(T) \leq T^\nu \left(1 + (\nu - 1)\ln T\right)^{\nu^2 - 1}$$

has been given in [15, Lemma 4].

It is also worth mentioning that, under the ERH, one can improve Theorem 1 (and Theorem 2 for larger values of T). Namely, for any $\varepsilon > 0$, the ERH implies the bound

$$\sigma(T) = O(T^{1/2} q^\varepsilon). \tag{4}$$

In fact, using the so-called "large sieve" method one can probably obtain quite strong unconditional results for "almost all" q rather than for all of them (which still suffices for cryptographic applications).

On the other hand, there are infinitely many primes q such that for $T = O(\log q)$ and any $m \geq 1$ the statistical distance $\Delta(m, T)$ is very large. Indeed, it has been shown in [2] that there exists a constant $c > 0$ such that for infinitely many primes q the smallest quadratic non-residue modulo q is at least $c \log q \log\log\log q$ (under the ERH the same result is known with $c \log q \log\log q$). Therefore for such q, $T = \lfloor c \log q \log\log\log q \rfloor$ and any $m \geq 1$ we have $P_{m,T}(k) = 0$ whenever k is one of the $(q-1)/2$ quadratic non-residues modulo q. Therefore, in this case $\Delta(m, T) \geq 1/2$. It should be noted that a large statistical distance does not imply that the corresponding signature scheme is insecure.

A more general modification of the algorithm from [6] (where some of the t_i and v_i are alternated in a random fashion in the expressions for κ and λ) can be studied quite analogously.

Acknowledgement

We thank Hugh Montgomery for indicating a proof of the bound (4).

References

1. V. Boyko, M. Peinado and R. Venkatesan, *Speeding up discrete log and factoring based schemes via precomputations,* Proc. EUROCRYPT'98, Lect. Notes in Comp. Sci., Springer-Verlag, Berlin, **1403** (1998), 221–235.
2. S. W. Graham and C. J. Ringrose, *Lower bounds for least quadratic nonresidues,* Analytic number theory, Progr. Math., 85, Birkhäuser, Boston, MA, 1990, 269–309.

3. A. Granville and K. Soundararajan, *Large character sums,* J. Amer. Math. Soc. (to appear); available from `http://www.ams.org/jams/`.
4. A. Hildebrand and G. Tenenbaum, *Integers without large prime factors,* J. de Théorie des Nombres de Bordeaux, **5** (1993), 411–484.
5. N. A. Howgrave-Graham and N. P. Smart, *Lattice attacks on digital signature schemes*, Designs, Codes and Cryptography (to appear).
6. A. K. Lenstra, *Generating standard DSA signatures without long inversions,* Proc. ASIACRYPT'96, Lect. Notes in Comp. Sci., Springer-Verlag, Berlin, **1163** (1996), 57–64.
7. R. Lidl and H. Niederreiter, *Finite fields,* Cambridge University Press, Cambridge, 1997.
8. A. J. Menezes, P. C. van Oorschot and S. A. Vanstone, *Handbook of Applied Cryptography,* CRC Press, Boca Raton, FL, 1996.
9. W. Narkiewicz, *Classical problems in number theory,* Polish Sci. Publ., Warszawa, 1986.
10. P. Nguyen, *The dark side of the Hidden Number Problem: Lattice attacks on DSA,* Proc. Workshop on Cryptography and Computational Number Theory, Singapore 1999, Birkhäuser, 2000 (to appear).
11. P. Nguyen and I. E. Shparlinski, *The insecurity of the Digital Signature Algorithm with partially known nonces,* Preprint, 2000, 1–26.
12. P. Nguyen and J. Stern, *The hardness of the hidden subset sum problem and its cryptographic implications,* Proc. CRYPTO'99, Lect. Notes in Comp. Sci., Springer-Verlag, Berlin, **1666** (1999), 31–46.
13. K. Nyberg and R. A. Rueppel, *Message recovery for signature schemes based on the discrete logarithm problem,* J. Cryptology, **8** (1995), 27–37.
14. B. Schneier, *Applied cryptography,* John Wiley, NY, 1996.
15. P. J. Stephens, *An average result for Artin's conjecture,* Mathematika, **16** (1969), 178–188.
16. S. Vaudenay, *On the security of Lenstra's DSA variant,* Presented at the Rump Session of ASIACRYPT'96; available from `http://lasecwww.epfl.ch/pub/lasec/doc/lenstra.ps`