The Insecurity of the Digital Signature Algorithm with Partially Known Nonces

Phong Q. Nguyen*
Département d'Informatique, École Normale Supérieure,
45, rue d'Ulm, 75230 Paris Cedex 05, France
Email: pnguyen@ens.fr
URL: http://www.di.ens.fr/~pnguyen

and

Igor E. Shparlinski†
Department of Computing, Macquarie University
Sydney, NSW 2109, Australia
Email: igor@comp.mq.edu.au
URL: http://www.comp.mq.edu.au/~igor/

Abstract. We present a polynomial-time algorithm that provably recovers the signer's secret DSA key when a few consecutive bits of the random nonces k (used at each signature generation) are known for a number of DSA signatures at most linear in $\log q$ (q denoting as usual the small prime of DSA), under a reasonable assumption on the hash function used in DSA. For most significant or least significant bits, the number of required bits is about $\log^{1/2} q$, but can be decreased to $\log \log q$ with a running time $q^{O(1/\log \log q)}$ subexponential in $\log q$, and even further to 2 in polynomial time if one assumes access to ideal lattice basis reduction, namely an oracle for the lattice closest vector problem for the infinity norm. For arbitrary consecutive bits, the attack requires twice as many bits. All previously known results were only heuristic, including those of Howgrave-Graham and Smart who recently introduced that topic. Our attack is based on a connection with the *hidden number problem* (HNP) introduced at Crypto '96 by Boneh and Venkatesan in order to study the bit-security of the Diffie–Hellman key exchange. The HNP consists, given a prime number q, of recovering a number $\alpha \in \mathbb{F}_q$ such that for many known random $t \in \mathbb{F}_q$ a certain approximation of of $t\alpha$ is known. To handle the DSA case, we extend Boneh and Venkatesan's results on the HNP to the case where t has not necessarily perfectly uniform distribution, and establish uniformity statements on the DSA signatures, using exponential sum techniques. The efficiency of our attack has been validated experimentally, and illustrates once again the fact that one should be very cautious with the pseudo-random generation of the nonce within DSA.

Keywords: Cryptanalysis, DSA, lattices, LLL, closest vector problem, distribution, discrepancy, exponential sums.

* Work supported in part by the RNRT "Turbo-signatures" project of the French Ministry of Research.
† Supported in part by ARC.

To appear in the *Journal of Cryptology*.

1. Introduction

1.1. The Digital Signature Algorithm (DSA)

Recall the *Digital Signature Algorithm* (see [26, 43]), or DSA, used in the American federal digital signature standard [29].

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 $\{0, \ldots, p-1\}$ and $\{0, \ldots, q-1\}$ 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). We also use $\log z$ to denote the binary logarithm of $z > 0$.

Let $\mathcal{M}$ be the set of messages to be signed and let $h : \mathcal{M} \to \mathbb{F}_q$ be an arbitrary hash-function. The signer's secret key is an element $\alpha \in \mathbb{F}_q^*$.

Let $g \in \mathbb{F}_p$ be a fixed element of multiplicative order q, that is $g^q = 1$ and $q \neq 1$ which is *publicly* known. To sign a message $\mu \in \mathcal{M}$, one chooses a random integer $k \in \mathbb{F}_q^*$ usually called the *nonce*, and which must be kept secret. One then defines the following two elements of $\mathbb{F}_q$:

$$\begin{aligned} r(k) &= \left\lfloor \left\lfloor g^k \right\rfloor_p \right\rfloor_q \\ s(k,\mu) &= \left\lfloor k^{-1} \left(h(\mu) + \alpha r(k) \right) \right\rfloor_q . \end{aligned}$$

The pair $(r(k), s(k,\mu))$ is the *DSA signature* of the message μ with a nonce k. In general, q has bit-length 160 and p has bit-length between 512 and 1024.

1.2. Former results

The security of DSA relies on the hardness of the discrete logarithm problem in prime fields and it subgroups. Under slight modifications and the random oracle model [4], the security of DSA (with respect to adaptive chosen-message attacks) can be proved relative to the hardness of discrete logarithm (see [9]). The well-known random oracle model assumes that the hash function behaves as a random oracle, that is, its values are independent and uniformly distributed.

However, serious precautions must be taken when using DSA. It was noticed by Vaudenay [45] that the primes p and q need to be validated,

for one could forge signature collisions otherwise. Special care must be taken with the nonce k. It is well-known that if k is disclosed, then the secret key α can easily be recovered. It was shown by Bellare *et al.* [3] that one can still recover α if the nonce k is produced by Knuth's linear congruential generator with known parameters, or variants. That attack is provable under the random oracle model, and relies on Babai's approximation algorithm [2] for the *closest vector problem* (CVP) in a lattice, which is based on the celebrated LLL algorithm [24]. The attack does not work if the parameters of the generator are unknown.

Recently, Howgrave-Graham and Smart [18] introduced a different scenario. Suppose that for a reasonable number of signatures, a small fraction of the corresponding nonce k is revealed. For instance, suppose that the ℓ least significant bits of k are known. Howgrave-Graham and Smart proposed in [18] several heuristic attacks to recover the secret key in such setting and variants (known bits in the middle, or split in several blocks) when ℓ is not too small. Like [3], the attacks are based on LLL-based Babai's CVP approximation algorithm [2]. However, the attacks of [3] and [18] are quite different. Howgrave-Graham and Smart followed an applied approach. The attack used several heuristic assumptions which did not allow precise statements on its theoretical behaviour It was assumed that the DSA signatures followed a perfectly uniform distribution, that some lattice enjoyed some natural however heuristic property, and that Babai's algorithm [2] behaves much better than theoretically guaranteed. Consequently, it was hard to guess what were the limitations of the attack such as how small could ℓ be in practice, and what could be proved.

1.3. Our results

In this paper, we present the first provable polynomial-time attack against DSA when the nonces are partially known, under two reasonable assumptions: the size of q should not be too small compared to p, and the probability of collisions for the hash function h should not be too large compared to $1/q$. More precisely, under these conditions, we show that if for a certain (polynomially bounded) number of random messages $\mu \in \mathcal{M}$ and random nonces $k \in [1, q-1]$ about $\log^{1/2} q$ least significant bits of k are known, then in polynomial time one can recover the signer's secret key α. The same result holds for the most significant bits when one uses an appropriate definition of the most significant bits tailored to modular residues. With the usual definition of most significant bits, one needs one more bit than in the case of least significant bits, as q might be only marginally larger than a power of two

(certainly this distinction is important only for our numerical results). The result is slightly worse for arbitrary windows of consecutive bits: in such a case, one requires twice as many bits (contrary to what the analysis of [18] suggested). For least significant bits (or appropriate most significant bits), the number of bits can be decreased to 2 if one further assumes access to ideal lattice reduction (namely, an oracle for the closest vector problem for the infinity norm). Such an assumption is realistic in low dimension despite NP-hardness results on lattice problems, due to the well-known experimental fact that state-of-the-art lattice basis reduction algorithms behave much better than theoretically guaranteed. Alternatively, the number of bits can be decreased to $\log\log q$ but with a running time $q^{O(1/\log\log q)}$ subexponential in $\log q$, using the closest vector approximation algorithm of [1, Corollary 16]. This subexponential running time is interesting, as the bit-length of q is usually chosen to be 160, in order to avoid square-root attacks.

Our attack has been validated experimentally. Using a standard workstation, we could most of the time recover in a few minutes the signer's DSA 160-bit secret key when only $\ell = 3$ least significant bits of the nonces were known for about 100 signatures. Interestingly, this improves the experimental results of [18], where the best experiment corresponded to $\ell = 8$, and where it was suggested that $\ell = 4$ was impossible.

It should be pointed out that the study of the security of DSA in such settings might have practical implications. Indeed, Bleichenbacher [5] recently noticed that in AT&T's CryptoLib version 1.2 (a widely distributed cryptographic library), the implementation of DSA suffers from the following flaw: the random nonce k is always odd, thus leaking its least significant bit. Apparently, this is because the same routine is used in the implementation of the El Gamal signature scheme, for which k must be coprime with $p-1$, and thus necessarily odd. Our results do not show that CryptoLib's DSA implementation can be broken, but they do not rule out such a possibility either, even with the same attack. In fact, they indicate a potential weakness in this implementation.

This has been confirmed by a very recent important result of Bleichenbacher [6], who has presented a heuristic attack on DSA with time complexity 2^{64} (and requiring memory 2^{40} and 2^{22} signatures), when the pseudo-random number generator suggested by the NIST to produce the nonces is used (see [29]). The NIST generator suffered from the following flaw: the outputs are biased in the sense that small values modulo q are more likely to occur than high values modulo q. This is because the output is some 160-bit pseudo-random number

reduced modulo the 160-bit prime q. Bleichenbacher's heuristic attack also applies to the case when some of the bits of the nonces are known. The attack is based on clever meet-in-the-middle techniques, and not lattices. Currently, the best experimental result with this attack is that one can recover the secret key given a leakage of $\log 3 \approx 1.58$ bits for 2^{22} signatures, in about 3 days on a 450 MHz Ultrasparc using 500Mb of RAM. Thus, our experimental results are superseded by Bleichenbacher's results. Note however that the techniques used are completely different, and that our method remains the only one yielding provable results at the moment.

1.4. Overview of our attack

Our attack follows Nguyen's approach [30] that reduces the DSA problem to a variant of the *hidden number problem* (HNP) introduced in 1996 by Boneh and Venkatesan [7, 8]. The HNP can be stated as follows: recover a number $\alpha \in \mathbb{F}_q$ such that for many known random $t \in \mathbb{F}_q$, an approximation $\mathrm{APP}_{\ell,q}(\alpha t)$ of αt is known. Here, for any rationals n and ℓ, the notation $\mathrm{APP}_{\ell,q}(n)$ denotes any rational r such that:

$$|n - r|_q \leq \frac{q}{2^{\ell+1}},$$

where the symbol $|.|_q$ is defined as $|z|_q = \min_{b\in\mathbb{Z}} |z - bq|$ for any real z.

The connection between the DSA problem and the HNP can easily be explained. Assume that we know the ℓ least significant bits of a nonce $k \in \mathbb{F}_q^*$. That is, we are given an integer a such that $0 \leq a \leq 2^\ell - 1$ and $k - a = 2^\ell b$ for some integer $b \geq 0$. Given a message μ signed with the nonce k, the congruence

$$\alpha r(k) \equiv s(k,\mu)k - h(\mu) \pmod{q},$$

can be rewritten for $s(k,\mu) \neq 0$ as:

$$\alpha r(k) 2^{-\ell} s(k,\mu)^{-1} \equiv \left(a - s(k,\mu)^{-1} h(\mu)\right) 2^{-\ell} + b \pmod{q}. \qquad (1)$$

Now define the following two elements

$$\begin{aligned} t(k,\mu) &= \left\lfloor 2^{-\ell} r(k) s(k,\mu)^{-1} \right\rfloor_q, \\ u(k,\mu) &= \left\lfloor 2^{-\ell} \left(a - s(k,\mu)^{-1} h(\mu)\right) \right\rfloor_q \end{aligned}$$

and remark that both $t(k,\mu)$ and $u(k,\mu)$ can easily be computed by the attacker from the publicly known information. Recalling that $0 \leq b \leq q/2^\ell$, we obtain

$$0 \leq \lfloor \alpha t(k,\mu) - u(k,\mu) \rfloor_q < q/2^\ell.$$

And therefore:

$$|\alpha t(k,\mu) - u(k,\mu) - q/2^{\ell+1}|_q \leq q/2^{\ell+1}. \tag{2}$$

Thus, an approximation $\mathrm{APP}_{\ell,q}(\alpha t(k,\mu))$ is known. Collecting several relations of this kind for several pairs (k,μ), the problem of recovering the secret key α is thus a HNP in which the distribution of the multiplier $t(k,\mu)$ is not necessarily perfectly uniform, and which at first sight seems hard to study. This problem of recovering will be called the DSA–HNP in the rest of the paper.

To solve the DSA–HNP, we apply a lattice-based algorithm proposed by Boneh and Venkatesan in [7], which relies on a simple reduction from the HNP to the CVP. This polynomial-time algorithm, which we will call BV, is again based on Babai's CVP approximation algorithm [2]. It provably solves the HNP when $\ell \geq \log^{1/2} q + \log\log q$. That result is often cited as the only positive application known of the LLL algorithm, because it enabled Boneh and Venkatesan to establish in [7] some results on the bit-security of the Diffie–Hellman key exchange and related cryptographic schemes. However, in the latter application, the distribution of the multipliers t is not perfectly uniform, making some of the statements of [7] incorrect. This led Gonzáles Vasco and Shparlinski [16] to extend results on the BV algorithm to the case where t is randomly selected from a subgroup of $\mathbb{F}_q^*$, to obtain rigorous statements on the bit-security of the Diffie–Hellman key exchange and related schemes (see also [17]).

In the DSA–HNP as well, the distribution of the multiplier $t(k,\mu)$ is not necessarily perfectly uniform. Hence, we present another extension of the results of [7] on the BV algorithm using the notion of discrepancy, in the spirit of that of [16, 17]. To achieve the proof of our attack, we show using exponential sum techniques that the DSA signatures follow some kind of uniform distribution.

1.5. Structure of the paper and notation

The paper is organised as follows. In Section 2, we review a few facts on lattices and the HNP and we present three extensions of [7, Theorem 1] where the multipliers can have imperfect uniform distribution. In Section 3, we obtain uniformity results on the distribution of DSA signatures, which might be of independent interest. Finally, in Section 4, we collect the aforementioned results and apply it to DSA.

Throughout the paper the implied constants in symbols 'O' may occasionally, where obvious, depend on the small positive parameter ε

and are absolute otherwise; they all are effective and can be explicitly evaluated.

We use $[\alpha, \beta]$ and $]\alpha, \beta[$ to denote the closed and open intervals, respectively.

As usual, $\Pr(\mathcal{E})$ denotes the probability of an event $\mathcal{E}$.

For a real x, $\lfloor x \rfloor$ denotes the integer part of x, that is the integer n such that $n \leq x < n+1$. $\lceil x \rceil$ is the integer n such that $n \geq x > n-1$.

2. Lattices and the Hidden Number Problem

2.1. Background on lattices

As in [7], our results rely on rounding techniques in lattices. We briefly review a few results and definitions. For general references on lattice theory and its important cryptographic applications, we refer to the recent surveys [32, 33].

Let $\{\mathbf{b}_1, \ldots, \mathbf{b}_s\}$ be a set of linearly independent vectors in $\mathbb{R}^s$. The set of vectors

$$L = \left\{ \sum_{i=1}^{s} n_i \mathbf{b}_i \mid n_i \in \mathbb{Z} \right\},$$

is called an s-dimensional full rank lattice. The set $\{\mathbf{b}_1, \ldots, \mathbf{b}_s\}$ is called a *basis* of L, and L is said to be spanned by $\{\mathbf{b}_1, \ldots, \mathbf{b}_s\}$.

A basic lattice problem is the closest vector problem (CVP): given a basis of a lattice L in $\mathbb{R}^s$ and a target $\mathbf{u} \in \mathbb{R}^s$, find a lattice vector $\mathbf{v} \in L$ which minimises the Euclidean norm $\|\mathbf{u} - \mathbf{v}\|$ among all lattice vectors. The CVP generally refers to the Euclidean norm, but of course, other norms are possible as well: we denote by CVP_∞ the problem corresponding to the infinity norm. Both the CVP and the CVP_∞ are NP-hard (see [32, 33] for references). We call CVP_∞-oracle any algorithm that solves the CVP exactly.

We use the best CVP approximation polynomial-time result known, which follows from the recent shortest vector algorithm of Ajtai *et al.* [1] and Kannan's reduction from approximating the CVP to approximating the shortest vector problem [19]:

LEMMA 1. *For any constant $\gamma > 0$, there exists a randomized polynomial-time algorithm which, given a lattice L and a vector $\mathbf{r} \in \mathbb{Q}^s$, finds a lattice vector $\mathbf{v}$ satisfying with probability exponentially close to*

1 the inequality

$$\|\mathbf{v}-\mathbf{r}\| \leq 2^{\gamma s \log\log s/\log s} \min\{\|\mathbf{z}-\mathbf{r}\|, \quad \mathbf{z} \in L\}.$$

Proof. By taking $k = \lceil c_1 \log n \rceil$ in [1, Corollary 15] where $c_1 > 0$ is a sufficiently large constant, we obtain a randomized polynomial-time algorithm which approximates the shortest vector within $2^{c_2 s \log\log s/\log s}$ for any constant $c_2 > 0$. Besides, Kannan proved in [19, Section 7] that any algorithm approximating the shortest vector problem to within a non-decreasing function $f(s)$ can be used to approximate CVP to within $s^{3/2} f(s)^2$. Since the number of calls of the algorithm remains polynomial, one obtains the desired statement. □

The best deterministic polynomial-time algorithm known for the problem has a slightly larger approximation factor $2^{\eta s \log^2\log s/\log s}$, see for instance [27, Section 2.1], or [32, Section 2.4], or [33, Section 2.4]. This result is a combination of Schnorr's generalisation [38] of the lattice basis reduction algorithm of Lenstra, Lenstra and Lovász [24] with the aforementioned reduction of Kannan [19]. In the literature, one often finds a weaker and older result (due to Babai [2]) where the approximation factor is only $2^{s/2}$.

In Lemma 1, the success probability is exponentially close to 1: in the rest of the paper, we assume that the probability is at least $1-2^{-s^3}$, which we are allowed to because if the probability is at least $1-2^{-cs}$ for some constant $c > 0$, we can obtain the probability $1-2^{-s^3}$ by applying the algorithm a polynomial number of times.

2.2. The Hidden Number Problem

We sketch the Boneh and Venkatesan algorithm (BV) proposed in [7] to solve the HNP. Our presentation is slightly different from that of [7]. Consider an instance of the HNP: let $t_1, \ldots, t_d$ be chosen uniformly and independently at random in $\mathbb{F}_q^*$, and $u_i = \mathrm{APP}_{\ell,q}(\alpha t_i)$. Given $t_1, \ldots, t_d$, $u_1, \ldots, u_d$, ℓ, and q, we wish to find the hidden number α. Recall that by definition, $|u_i - \alpha t_i|_q \leq q/2^{\ell+1}$. The BV algorithm is based on a lattice interpretation of those d inequalities: a vector derived from the u_i's is exceptionally close to a particular lattice vector related to the hidden number α. This is done by considering the $(d+1)$-dimensional

lattice $L(q, \ell, t_1, \ldots, t_d)$ spanned by the rows of the following matrix:

$$\begin{pmatrix} q & 0 & \cdots & 0 & 0 \\ 0 & q & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots \\ 0 & \ldots & 0 & q & 0 \\ t_1 & \ldots & \ldots & t_d & 1/2^{\ell+1} \end{pmatrix}. \tag{3}$$

The inequality $|u_i - \alpha t_i|_q \leq q/2^{\ell+1}$ implies the existence of an integer h_i such that:

$$|u_i - \alpha t_i - q h_i| \leq q/2^{\ell+1}. \tag{4}$$

Notice that the row vector $\mathbf{h} = (\alpha t_1 + q h_1, \ldots, \alpha t_d + q h_d, \alpha/2^{\ell+1})$ belongs to $L(q, \ell, t_1, \ldots, t_d)$, since it can be obtained by multiplying the last row vector by α and then subtracting appropriate multiples of the first d row vectors. Since the last coordinate of this vector discloses the hidden number α, we call $\mathbf{h}$ the *hidden vector*. The hidden vector is very close to the row vector $\mathbf{u} = (u_1, \ldots, u_d, 0)$. Indeed, by (4) and $0 \leq \alpha < q$, we have:

$$\|\mathbf{h} - \mathbf{u}\|_\infty \leq q/2^{\ell+1}.$$

The choice of the $(d+1) \times (d+1)$ entry in the matrix (3) was made to balance the size of the entries of $\mathbf{h} - \mathbf{u}$.

The BV algorithm applies Babai's nearest plane algorithm [2] to the lattice $L(q, \ell, t_1, \ldots, t_d)$ and the target vector $\mathbf{u}$, which of course can both be built from available information. This yields a lattice point $\mathbf{v}$ that must satisfy:

$$\|\mathbf{u} - \mathbf{v}\| \leq 2^{(d+1)/4} \|\mathbf{u} - \mathbf{h}\| \leq (d+1)^{1/2} 2^{(d+1)/4} q/2^{\ell+1}.$$

Thus, the lattice vector $\mathbf{h} - \mathbf{v}$ satisfies:

$$\|\mathbf{h} - \mathbf{v}\|_\infty \leq \|\mathbf{h} - \mathbf{u}\|_\infty + \|\mathbf{u} - \mathbf{v}\| \leq \frac{q\left(1 + (d+1)^{1/2} 2^{(d+1)/4}\right)}{2^{\ell+1}}.$$

This means, that if ℓ is not too small, $\mathbf{h} - \mathbf{v}$ is a very short lattice vector. Intuitively, only very particular lattice vectors should have infinity norm less than $q/2^{1+\eta}$. The following lemma (which is actually the core of [7, Theorem 5]) formalises this intuition by characterizing all short vectors in $L(q, \ell, t_1, \ldots, t_d)$:

LEMMA 2. *Let α be a fixed integer in the range $[1, q-1]$ and let $\ell \geq \eta > 0$. Choose integers $t_1, \ldots, t_d$ uniformly and independently at random in the range $[1, q-1]$. Then with probability $P \geq 1 - q/2^{d\eta}$,*

all vectors $\mathbf{w}$ *in* $L(q, \ell, t_1, \ldots, t_d)$ *such that* $\|\mathbf{w}\|_\infty \leq q/2^{1+\eta}$ *are of the form*

$$\mathbf{w} = (0, \ldots, 0, \beta/2^{\ell+1}),$$

where $\beta \equiv 0 \pmod{q}$.

Proof. Let $\mathbf{w} \in L(q, \ell, t_1, \ldots, t_d)$. By definition of the lattice, there exist integers $\beta, z_1, \ldots, z_d$ such that

$$\mathbf{w} = (\beta t_1 - z_1 q, \ldots, \beta t_d - z_d q, \beta/2^{\ell+1}). \tag{5}$$

If $\beta \equiv 0 \pmod{q}$, then each $\beta t_i - z_i q$ is a multiple of q, and therefore, $\|\mathbf{w}\|_\infty \leq q/2^{1+\eta}$ implies that each $\beta t_i - z_i q$ is zero, so that:

$$\mathbf{w} = (0, \ldots, 0, \beta/2^{\ell+1}).$$

Hence, to achieve the proof of the lemma, it suffices to prove that the probability P that there exists an integer $\beta \not\equiv 0 \pmod{q}$ and integers $z_1, \ldots, z_d$ such that $\|\mathbf{w}\|_\infty \leq q/2^{1+\eta}$ (where $\mathbf{w}$ is defined by (5)), is less than $q/2^{d\eta}$.

For any $\beta \not\equiv 0 \pmod{q}$, denote by $E(\beta)$ the event that there exist integers $z_1, \ldots, z_d$ such that $\|\mathbf{w}\|_\infty \leq q/2^{1+\eta}$. Obviously, if $|\beta t_i - z_i q| \leq q/2^{1+\eta}$ then $|\beta t_i|_q \leq q/2^{1+\eta}$ (recall the definition $|n|_q = \min\{\lfloor n \rfloor_q, q - \lfloor n \rfloor_q\}$ in Section 1.4). Hence, the probability of $E(\beta)$ is less than the probability that for all i, $|\beta t_i|_q < q/2^{1+\eta}$. It follows by independence of the t_i's, that $\Pr(E(\beta)) \leq p(\beta, q)^d$, if $p(\beta, q)$ denotes the probability that $|\beta t|_q \leq q/2^{1+\eta}$ for t uniformly chosen in $[1, q-1]$. By definition,

$$p(\beta, q) = 1 - \Pr\left(q/2^{1+\eta} < \lfloor \beta t \rfloor_q < q - q/2^{1+\eta}\right).$$

Since $\beta \not\equiv 0 \pmod{q}$, and t is uniformly chosen in $[1, q-1]$, $\lfloor \beta t \rfloor_q$ is uniformly chosen in $[1, q-1]$, implying that:

$$\begin{aligned} p(\beta, q) &= 1 - \frac{\lfloor q - q/2^{1+\eta} \rfloor - \lceil q/2^{1+\eta} \rceil + 1}{q-1} \\ &\leq 1 - \frac{q - q/2^{\eta} + 1}{q-1} = \frac{q - 2^{1+\eta}}{2^{\eta}(q-1)} \leq \frac{1}{2^{\eta}}. \end{aligned}$$

Hence, the probability of $E(\beta)$ is less than $1/2^{d\eta}$. Finally, notice that $E(\beta)$ occurs only if $E(\lfloor \beta \rfloor_q)$ occurs, so that

$$P \leq \sum_{\beta=1}^{q-1} \Pr(E(\beta)),$$

from which the result follows. □

Now, if $\mathbf{h}-\mathbf{v}$ is sufficiently short to satisfy the condition of Lemma 2, the hidden number α can easily be derived from the last coordinate of $\mathbf{v}$ because of $\mathbf{h}$. A straightforward computation shows that the condition is satisfied for all sufficiently large q, if $\ell = \lceil \log^{1/2} q \rceil + \lceil \log \log q \rceil$ and $d = 2\lceil \log^{1/2} q \rceil$, using Babai's CVP approximation algorithm [2], and not Lemma 1. Thus, with these parameters, the polynomial-time BV algorithm recovers with high probability α, which is formalised by [7, Theorem 1]. Of course the value of ℓ can be slightly decreased if one uses Lemma 1 instead of Babai's algorithm.

2.3. Extending the Hidden Number Problem

As we have seen, the correctness of the BV algorithm relies on Lemma 2. We would like to generalise Lemma 2 to cases where the multiplier t has not necessarily perfectly uniform distribution. A simple look at the proof of Lemma 2 shows that the distribution of t only intervenes in the upper bounding of the probability $p(\beta, q)$ that $|\beta t|_q \leq q/2^{1+\eta}$. We need $p(\beta, q)$ to be less than a constant strictly less than 1. We rewrite $p(\beta, q)$ as:

$$\begin{aligned} p(\beta, q) &= 1 - \Pr\left(q/2^{1+\eta} < \lfloor \beta t \rfloor_q < q - q/2^{1+\eta}\right) \\ &= 1 - \Pr\left(\frac{\lfloor \beta t \rfloor_q}{q} \in \left]\frac{1}{2^{1+\eta}}, 1 - \frac{1}{2^{1+\eta}}\right[\right). \end{aligned}$$

This suggests to use the classical notion of discrepancy [11, 22, 35]. Recall that the *discrepancy* $\mathcal{D}(\Gamma)$ of a sequence $\Gamma = \{\gamma_1, \ldots, \gamma_N\}$ of N elements of the interval $[0, 1]$ is defined as

$$\mathcal{D}(\Gamma) = \sup_{J \subseteq [0,1]} \left| \frac{A(J, N)}{N} - |J| \right|,$$

where the supremum is extended over all subintervals J of $[0, 1]$, $|J|$ is the length of J, and $A(J, N)$ denotes the number of points γ_n in J for $0 \leq n \leq N - 1$. The term $\lfloor \beta t \rfloor_q / q$ in our expression of $p(\beta, q)$ suggests the following definition. We say that a finite sequence $\mathcal{T}$ of integers is Δ-*homogeneously distributed modulo* q if for any integer a coprime with q the discrepancy of the sequence $\{\lfloor at \rfloor_q / q\}_{t \in \mathcal{T}}$ is at most Δ. Indeed, if t is now chosen uniformly at random from a Δ-homogeneously distributed modulo q sequence $\mathcal{T}$, then by definition:

$$\Pr\left(\frac{\lfloor \beta t \rfloor_q}{q} \in \left]\frac{1}{2^{1+\eta}}, 1 - \frac{1}{2^{1+\eta}}\right[\right) \geq \left|\left]\frac{1}{2^{1+\eta}}, 1 - \frac{1}{2^{1+\eta}}\right[\right| - \Delta = 1 - \frac{1}{2^{\eta}} - \Delta.$$

This obviously leads to the following generalization of Lemma 2:

LEMMA 3. *Let α be a fixed integer in the range $[1, q-1]$ and let $\ell \geq \eta > 0$. Choose integers $t_1, \ldots, t_d$ uniformly and independently at random from a Δ-homogeneously distributed modulo q sequence $\mathcal{T}$. Then with probability at least $1-q(1/2^{\eta}+\Delta)^d$, all $\mathbf{w}$ in $L(q, \ell, t_1, \ldots, t_d)$ such that $\|\mathbf{w}\|_\infty \leq q/2^{1+\eta}$ are of the form*

$$\mathbf{w} = (0, \ldots, 0, \beta/2^{\ell+1}),$$

where $\beta \equiv 0 \pmod{q}$.

Using Lemma 3, we easily obtain a generalization of [7, Theorem 1]:

LEMMA 4. *Let $\omega > 0$ be an arbitrary absolute constant. For a prime q, define*

$$\ell = \left\lceil \omega \left(\frac{\log q \log\log\log q}{\log\log q} \right)^{1/2} \right\rceil \qquad \text{and} \qquad d = \lceil 3 \log q/\ell \rceil .$$

Let $\mathcal{T}$ be a $2^{-\ell}$-homogeneously distributed modulo q sequence of integer numbers. There exists a probabilistic polynomial-time algorithm $\mathcal{A}$ such that for any fixed integer α in the interval $[0, q-1]$, given as input a prime q, d integers $t_1, \ldots, t_d$ and d rationals

$$u_i = APP_{\ell,q}(\alpha t_i), \qquad i = 1, \ldots, d,$$

its output satisfies for sufficiently large q

$$\Pr\left[\mathcal{A}\left(q, t_1, \ldots, t_d; u_1, \ldots, u_d\right) = \alpha\right] \geq 1 - q^{-1}$$

where the probability is taken over all $t_1, \ldots, t_d$ chosen uniformly and independently at random from the elements of $\mathcal{T}$ and all coin tosses of the algorithm $\mathcal{A}$.

Proof. We simply follow the sketch of Section 2.2. The algorithm $\mathcal{A}$ applies the algorithm of Lemma 1 with $s = d+1$ and $\gamma = \omega/10$ to the lattice $L(q, \ell, t_1, \ldots, t_d)$ spanned by the rows of the matrix (3), and the target vector $\mathbf{u} = (u_1, \ldots, u_d, 0)$. The algorithm $\mathcal{A}$ outputs $\lfloor \beta \rceil_q$ where $\beta/2^{\ell+1}$ is the last entry of the vector $\mathbf{v}$ yielded by the algorithm of Lemma 1.

We now analyze the correctness of $\mathcal{A}$. Letting the lattice vector $\mathbf{h} = (\lfloor \alpha t_1 \rceil_q, \ldots, \lfloor \alpha t_d \rceil_q, \alpha/2^{\ell+1})$, we see from Lemma 1 that the lattice vector $\mathbf{v}$ must satisfy with probability at least $1 - 2^{-d^3}$:

$$\|\mathbf{u}-\mathbf{v}\| \leq 2^{\gamma(d+1)\log\log(d+1)/\log(d+1)} \|\mathbf{u}-\mathbf{h}\| \leq 2^{\omega d \log\log d/9\log d} \|\mathbf{u}-\mathbf{h}\|.$$

Since $\|\mathbf{h}-\mathbf{u}\|_\infty < q/2^{\ell+1}$, we obtain:

$$\|\mathbf{h}-\mathbf{v}\|_\infty \le q2^{-\ell-1+\omega d \log\log d/9\log d}.$$

One easily verifies that

$$\omega d \log\log d/9\log d \le \ell/2$$

for sufficiently large q. Thus, $\mathbf{h}-\mathbf{v}$ satisfies the assumption of Lemma 3 with $\eta = \ell/2+1$ provided that q is large enough. Therefore, $\mathcal{A}$ outputs the hidden number α with probability at least

$$1 - q(2^{-\eta}+2^{-\ell})^d - 2^{-d^3} \ge 1 - q2^{-d(\eta-1)} - 2^{-d^3} \ge 1 - q^{-1}$$

and the result follows. □

Since our results apply lattice reduction, it is interesting to know how our results are affected if ideal lattice reduction is available, due to the well-known experimental fact that lattice basis reduction algorithms behave much better than theoretically guaranteed, despite NP-hardness results for most lattice problems (see [32, 33]). The methodology of Section 2.2 is more adapted to the infinity norm than the Euclidean norm, so the following result is an improved version of Lemma 4, when a CVP_∞-oracle is available:

LEMMA 5. *Let $\eta > 0$ be fixed. For a prime q, define $\ell = 1+\eta$, and*

$$d = \left\lceil \frac{8}{3}\eta^{-1}\log q \right\rceil.$$

Let $\mathcal{T}$ be a $f(q)$-homogeneously distributed modulo q sequence of integer numbers, where $f(q)$ is any function with $f(q)\to 0$ as $q\to\infty$. There exists a deterministic polynomial-time algorithm $\mathcal{A}$ using a CVP_∞-oracle (in dimension $d+1$) such that for any fixed integer α in the interval $[0, q-1]$, given as input a prime q, d integers $t_1,\ldots,t_d$ and d rationals

$$u_i = APP_{\ell,q}(\alpha t_i), \qquad i = 1,\ldots,d,$$

its output satisfies for sufficiently large q

$$\Pr\left[\mathcal{A}(q,t_1,\ldots,t_d;u_1,\ldots,u_d) = \alpha\right] \ge 1 - \frac{1}{q}$$

where the probability is taken over all $t_1,\ldots,t_d$ chosen uniformly and independently at random from the elements of $\mathcal{T}$.

Proof. We follow the proof of Lemma 4, and replace the algorithm of Lemma 1 by a CVP_∞-oracle. This time, we have:

$$\|\mathbf{h}-\mathbf{v}\|_\infty \leq \frac{q}{2^\ell} = \frac{q}{2^{1+\eta}}.$$

Applying Lemma 3, we obtain that the probability of success of the algorithm is at least $1-q(1/2^\eta+f(q))^d$. For sufficiently large q we have $1/2^\eta+f(q)\leq 1/2^{3\eta/4}$, so that:

$$(1/2^\eta+f(q))^d \leq 1/2^{3d\eta/4} \leq 1/2^{2\log q},$$

from which the result follows. □

It is worth noting that in Lemma 5 the assumption on the distribution of $\mathcal{T}$ is quite weak, which explains why in practice, attacks based on variants of the HNP are likely to work (as illustrated in [18, 30]). In fact, only a non-trivial upper bound on the number of fractions $\lfloor at \rfloor_q/q$, $t\in\mathcal{T}$ in a given interval is really needed (rather than the much stronger property of homogeneous distribution modulo q).

We remark that the choice of parameters in DSA and ECDSA is based on the assumption that any attack should take time of order at least $q^{1/2}$. Thus any attack requiring significantly lesser time could still be a threat. Interestingly, one can obtain a combination of Lemma 4 and Lemma 5 which leads to such an attack

LEMMA 6. *For a prime q, define $\ell=\lfloor \log\log q\rfloor$, and*

$$d=\left\lceil 4\frac{\log q}{\log\log q}\right\rceil.$$

Let $\mathcal{T}$ be a $2^{-\ell}$-homogeneously distributed modulo q sequence of integer numbers. There exists a probabilistic algorithm $\mathcal{A}$ which runs in time $q^{O(1/\log\log q)}$ and such that for any fixed integer α in the interval $[0,q-1]$, given as input a prime q, d integers $t_1,\ldots,t_d$ and d rationals

$$u_i = APP_{\ell,q}(\alpha t_i), \qquad i=1,\ldots,d,$$

its output satisfies for sufficiently large q

$$\Pr\left[\mathcal{A}\left(q,t_1,\ldots,t_d;u_1,\ldots,u_d\right)=\alpha\right]\geq 1-\frac{1}{q}$$

where the probability is taken over all $t_1,\ldots,t_d$ chosen uniformly and independently at random from the elements of $\mathcal{T}$.

Proof. We repeat the arguments of the proof of Lemma 4 however we use the closest vector approximation algorithm of [1, Corollary 16] in the corresponding place which runs in time at most $2^{O(d)} = q^{O(1/\log\log q)}$. Following the same calculations as in the proof of Lemma 4, we obtain that the probability of failure does not exceed

$$q\left(d^{1/2}2^{-\ell+O(1)}\right)^d \le q^{-1}$$

for sufficiently large q. □

3. Distribution of Signatures Modulo q

From the previous section, it remains to study the distribution of signatures. In this section, we obtain uniformity results on the distribution of $t(k,\mu)$ modulo q, which might be of independent interest.

3.1. Preliminaries on exponential sums

Let $\mathbf{e}_p(z) = \exp(2\pi iz/p)$ and $\mathbf{e}_q(z) = \exp(2\pi iz/q)$. One of our main tools is the *Weil bound* on exponential sums with rational functions which we present in the following form given by [28, Theorem 2].

LEMMA 7. *For any polynomials $g(X), f(X) \in \mathbb{F}_q[X]$ such that the rational function $F(X) = f(X)/g(X)$ is not constant on $\mathbb{F}_q$, the bound*

$$\left|\sum_{\lambda\in\mathbb{F}_q}{}^*\mathbf{e}_q\left(F(\lambda)\right)\right| \le \left(\max\{\deg g, \deg f\} + u - 2\right) q^{1/2} + \delta$$

holds, where $\sum^*$ means that the summation is taken over all $\lambda \in \mathbb{F}_q$ which are not poles of $F(X)$ and

$$(u,\delta) = \begin{cases} (v,1), & \text{if } \deg f \le \deg g, \\ (v+1,0), & \text{if } \deg f > \deg g, \end{cases}$$

and v is the number of distinct zeros of $g(X)$ in the algebraic closure of $\mathbb{F}_q$.

We also need some estimates from [20] of exponential sums with exponential functions. In fact we present them in the somewhat simplified forms similar to those given in [16].

LEMMA 8. *For any $\varepsilon > 0$ there exists $\delta > 0$ such that for any element $g \in \mathbb{F}_p$ of multiplicative order $T \ge p^{1/3+\varepsilon}$ the bound*

$$\max_{\gcd(c,p)=1} \left| \sum_{x=0}^{T-1} \mathbf{e}_p\left(cg^x\right) \right| \le T^{1-\delta}$$

holds.

Proof. The result follows immediately from the estimate

$$\max_{\gcd(c,p)=1} \left| \sum_{x=0}^{T-1} \mathbf{e}_p\left(cg^x\right) \right| = O\left(B(T,p)\right),$$

where

$$B(T,p) = \begin{cases} p^{1/2}, & \text{if } T \ge p^{2/3}; \\ p^{1/4}T^{3/8}, & \text{if } p^{2/3} > T \ge p^{1/2}; \\ p^{1/8}T^{5/8}, & \text{if } p^{1/2} > T \ge p^{1/3}; \end{cases}$$

which is essentially [20, Theorem 3.4]. □

LEMMA 9. *Let Q be a sufficiently large integer. For any $\varepsilon > 0$ there exists $\delta > 0$ such that for all primes $p \in [Q, 2Q]$, except at most $Q^{5/6+\varepsilon}$ of them, and any element $g_{p,T} \in \mathbb{F}_p$ of multiplicative order $T \ge p^{\varepsilon}$ the bound*

$$\max_{\gcd(c,p)=1} \left| \sum_{x=0}^{T-1} \mathbf{e}_p\left(cg_{p,T}^x\right) \right| \le T^{1-\delta}$$

holds.

Proof. For each integer $T \ge 1$ and for each prime $p \equiv 1 \pmod{T}$ we fix an element $g_{p,T}$ of multiplicative order T. Then [20, Theorem 5.5] claims that for any $U > 1$ and any integer $\nu \ge 2$, for all primes $p \equiv 1 \pmod{T}$ except at most $O(U/\log U)$ of them, the bound

$$\max_{\gcd(c,p)=1} \left| \sum_{x=0}^{T-1} \mathbf{e}_p\left(cg_{p,T}^x\right) \right| = O\left(Tp^{1/2\nu^2}\left(T^{-1/\nu} + U^{-1/\nu^2}\right)\right),$$

holds. We remark that the value of the above exponential sum does not depend on the particular choice of the element $g_{p,T}$.

Taking

$$\nu = \left\lfloor \frac{1}{\varepsilon} \right\rfloor + 1, \qquad U = Q^{1/2+\varepsilon/3}, \qquad V = Q^{1/3+\varepsilon/3}$$

after simple computation we obtain that there exists some $\delta > 0$, depending only on ε, such that for any fixed $T \ge Q^{\varepsilon}$ the bound

$$\max_{\gcd(c,p)=1} \left| \sum_{x=0}^{T-1} \mathbf{e}_p\left(cg_{p,T}^{x}\right) \right| \le T^{1-\delta},$$

holds for all except $O(U/\log U)$ primes $p \equiv 1 \pmod{T}$ in the interval $p \in [Q, 2Q]$. As it follows from Lemma 8, a similar bound also holds for $T \ge V$. So the total number of exceptional primes p for which the bound of the lemma does not hold for at least one $T \ge p^{\varepsilon} \ge Q^{\varepsilon}$ is $O(UV) = O\left(Q^{5/6+2\varepsilon/3}\right)$. Thus for sufficiently large Q we obtain the desired result. □

3.2. Distribution of $r(k)$

For any integer $\rho \in [0, q-1]$, we denote by $N(\rho)$ the number of solutions of the equation

$$r(k) = \rho, \qquad k \in [1, q-1].$$

LEMMA 10. *Let Q be a sufficiently large integer. The following statement holds with $\vartheta = 1/3$ for all primes $p \in [Q, 2Q]$, and with $\vartheta = 0$ for all primes $p \in [Q, 2Q]$ except at most $Q^{5/6+\varepsilon}$ of them. For any $\varepsilon > 0$ there exists $\delta > 0$ such that for any element $g \in \mathbb{F}_p$ of multiplicative order $q \ge p^{\vartheta+\varepsilon}$ the bound*

$$N(\rho) = O\left(q^{1-\delta}\right), \qquad \rho \in [0, q-1],$$

holds.

Proof. Let

$$L = \left\lfloor \frac{p-\rho-1}{q} \right\rfloor.$$

We remark that $N(\rho)$ is the number of solutions $k \in [1, q-1]$ of the congruence

$$g^k \equiv qx + \rho \pmod{p}, \qquad k \in [1, q-1],\ x \in [0, L].$$

Using the identity (see Exercise 11.a in [46, Chapter 3])

$$\sum_{c=0}^{p-1} \mathbf{e}_p(cu) = \begin{cases} 0, & \text{if } u \not\equiv 0 \pmod{p}; \\ p, & \text{if } u \equiv 0 \pmod{p}; \end{cases}$$

we obtain

$$\begin{aligned} N(\rho) &= \frac{1}{p}\sum_{k=1}^{q-1}\sum_{x=0}^{L}\sum_{c=0}^{p-1}\mathbf{e}_p\left(c\left(g^k - qx - \rho\right)\right) \\ &= \frac{1}{p}\sum_{c=0}^{p-1}\mathbf{e}_p\left(-c\rho\right)\sum_{k=1}^{q-1}\mathbf{e}_p\left(cg^k\right)\sum_{x=0}^{L}\mathbf{e}_p\left(-cqx\right). \end{aligned}$$

Separating the term

$$\frac{(q-1)(L+1)}{p} \le \frac{(q-1)(p/q+1)}{p} \le 2$$

corresponding to $c = 0$, we derive

$$\begin{aligned} N(\rho) &\le 2 + \frac{1}{p}\sum_{c=1}^{p-1}\left|\sum_{k=1}^{q-1}\mathbf{e}_p\left(cg^k\right)\right|\left|\sum_{x=0}^{L}\mathbf{e}_p\left(-cqx\right)\right| \\ &\le 2 + \frac{1}{p}\sum_{c=1}^{p-1}\left|\sum_{k=1}^{q-1}\mathbf{e}_p\left(cg^k\right)\right|\left|\sum_{x=0}^{L}\mathbf{e}_p\left(cqx\right)\right|. \end{aligned}$$

Combining Lemmas 8 and 9 to estimate the sum over $k \in [1, q-1]$ (certainly the missing term corresponding to $k = 0$ does not change the order of magnitude of this sum) with the estimate

$$\sum_{c=1}^{p-1}\left|\sum_{x=0}^{L}\mathbf{e}_p\left(cqx\right)\right| = \sum_{c=1}^{p-1}\left|\sum_{x=0}^{L}\mathbf{e}_p\left(cx\right)\right| = O(p\log p),$$

see Exercise 11.c in [46, Chapter 3], we obtain the desired result. □

In particular, denote by $\mathcal{S}$ the set of pairs $(k,\mu) \in [1, q-1]\times\mathcal{M}$ with $s(k,\mu) \neq 0$ (that is, the set of pairs (k,μ) for which the congruence (1) holds and thus $t(k,\mu)$ is defined). Then

$$|\mathcal{S}| = q|\mathcal{M}|\left(1 + O\left(q^{-\delta}\right)\right) \tag{6}$$

for all p and q satisfying the conditions of Lemma 10.

3.3. Distribution of $t(k,\mu)$

For a hash function $h : \mathcal{M} \to \mathbb{F}_q$ we also denote by W the number of pairs $(\mu_1,\mu_2) \in \mathcal{M}^2$ with $h(\mu_1) = h(\mu_2)$. Thus, $W/|\mathcal{M}|^2$ is a probability of a *collision* and our results are nontrivial under a reasonable assumption that this probability is of order of magnitude close to $1/q$.

First of all, we need to estimate exponential sums with the multipliers $t(k,\mu)$:

LEMMA 11. *Let Q be a sufficiently large integer. The following statement holds with $\vartheta = 1/3$ for all primes $p \in [Q, 2Q]$, and with $\vartheta = 0$ for all primes $p \in [Q, 2Q]$ except at most $Q^{5/6+\varepsilon}$ of them. For any $\varepsilon > 0$ there exists $\delta > 0$ such that for any element $g \in \mathbb{F}_p$ of multiplicative order $q \ge p^{\vartheta+\varepsilon}$ the bound*

$$\max_{\gcd(c,q)=1} \left| \sum_{(k,\mu)\in\mathcal{S}} \mathbf{e}_q\left(ct(k,\mu)\right) \right| = O\left(W^{1/2} q^{3/2-\delta}\right)$$

holds.

Proof. For each $\mu \in \mathcal{M}$ we denote by $\mathcal{K}_\mu$ the set of $k \in [1, q-1]$ for which $(k,\mu) \in \mathcal{S}$.

We consider a $c_0 \in \mathbb{F}_q^*$ corresponding to the largest exponential sum of interest to us. We denote

$$\sigma = \left| \sum_{(k,\mu)\in\mathcal{S}} \mathbf{e}_q\left(c_0 t(k,\mu)\right) \right| = \max_{\gcd(c,q)=1} \left| \sum_{(k,\mu)\in\mathcal{S}} \mathbf{e}_q\left(ct(k,\mu)\right) \right|.$$

We have

$$\sigma \le \sum_{\mu\in\mathcal{M}} \left| \sum_{k\in\mathcal{K}_\mu} \mathbf{e}_q\left(c_0 t(k,\mu)\right) \right|.$$

For $\lambda \in \mathbb{F}_q$ we denote by $H(\lambda)$ the number of $\mu \in \mathcal{M}$ with $h(\mu) = \lambda$. We also define the integer $a \in [1, q-1]$ by the congruence $a \equiv 2^{-\ell} c_0 \pmod q$. Then

$$\sigma \le \sum_{\lambda\in\mathbb{F}_q} H(\lambda) \left| \sum_{\substack{k=1 \\ \alpha r(k) \not\equiv -\lambda \pmod q}}^{q-1} \mathbf{e}_q\left(a \frac{kr(k)}{\lambda + \alpha r(k)}\right) \right|.$$

Applying the Cauchy inequality we obtain

$$\sigma^2 \le \sum_{\lambda\in\mathbb{F}_q} H(\lambda)^2 \sum_{\lambda\in\mathbb{F}_q} \left| \sum_{\substack{k=1 \\ \alpha r(k) \not\equiv -\lambda \pmod q}}^{q-1} \mathbf{e}_q\left(a \frac{kr(k)}{\lambda + \alpha r(k)}\right) \right|^2. \quad (7)$$

First of all we remark that

$$\sum_{\lambda\in\mathbb{F}_q} H(\lambda)^2 = W. \quad (8)$$

Furthermore,

$$\sum_{\lambda \in \mathbb{F}_q} \left| \sum_{\substack{k=1 \\ \alpha r(k) \not\equiv -\lambda \pmod q}}^{q-1} \mathbf{e}_q\left(a \frac{kr(k)}{\lambda + \alpha r(k)}\right)\right|^2$$

$$= \sum_{\lambda \in \mathbb{F}_q} \sum_{\substack{k=1 \\ \alpha r(k) \not\equiv -\lambda \pmod q}}^{q-1} \times \sum_{\substack{m=1 \\ \alpha r(m) \not\equiv -\lambda \pmod q}}^{q-1} \mathbf{e}_q\left(a\left(\frac{kr(k)}{\lambda + \alpha r(k)} - \frac{mr(m)}{\lambda + \alpha r(m)}\right)\right)$$

$$= \sum_{k,m=1}^{q-1} \sum_{\lambda \in \mathbb{F}_q}{}^* \mathbf{e}_q\left(a\left(\frac{kr(k)}{\lambda + \alpha r(k)} - \frac{mr(m)}{\lambda + \alpha r(m)}\right)\right),$$

where, as in Lemma 7, the symbol $\sum^*$ means that the summation in the inner sum is taken over all $\lambda \in \mathbb{F}_q$ with

$$\lambda \not\equiv -\alpha r(k) \pmod q \qquad \text{and} \qquad \lambda \not\equiv -\alpha r(m) \pmod q.$$

It is easy to see that if $r(k) \neq r(m)$ then the rational function

$$F_{k,m}(X) = \frac{kr(k)}{X + \alpha r(k)} - \frac{mr(m)}{X + \alpha r(m)}$$

is not constant in $\mathbb{F}_q$. If $r(k) = r(m)$ then

$$F_{k,m}(X) = \frac{(k-m)r(k)}{X + \alpha r(k)}.$$

Thus it is constant only if $k = m$ or $r(k) = r(m) = 0$. From Lemma 10 we see that the number of such pairs is $O\left(q^{2-2\delta} + q\right)$ for some $\delta > 0$ for which we estimate the sum over λ trivially as q. For other pairs $(k, m) \in [1, q-1]^2$ we use Lemma 7 getting

$$\sum_{\lambda \in \mathbb{F}_q} \left| \sum_{\substack{k=1 \\ \alpha r(k) \not\equiv -\lambda \pmod q}}^{q-1} \mathbf{e}_q\left(a \frac{kr(k)}{\lambda + \alpha r(k)}\right)\right|^2 = O\left(\left(q^{2-2\delta} + q\right) q + q^{5/2}\right)$$

$$= O\left(q^{3-2\delta}\right)$$

(without loss of generality we may assume that $\delta < 1/4$). Substituting this estimate and the identity (8) in (7), we obtain the desired statement. □

LEMMA 12. *Let Q be a sufficiently large integer. The following statement holds with $\vartheta = 1/3$ for all primes $p \in [Q, 2Q]$, and with $\vartheta = 0$ for all primes $p \in [Q, 2Q]$ except at most $Q^{5/6+\varepsilon}$ of them. For any $\varepsilon > 0$ there exists $\delta > 0$ such that for any element $g \in \mathbb{F}_p$ of multiplicative order $q \ge p^{\vartheta+\varepsilon}$ the sequence $t(k,\mu)$, $(k,\mu) \in \mathcal{S}$, is $2^{-\log^{1/2} q}$-homogeneously distributed modulo q provided that*

$$W \le \frac{|\mathcal{M}|^2}{q^{1-\delta}}.$$

Proof. Let us fix an integer a coprime with q. According to a general discrepancy bound, given by [35, Corollary 3.11] for the discrepancy D of the set

$$\left\{ \frac{\lfloor at(k,\mu) \rfloor_q}{q} \ : \ (k,\mu) \in \mathcal{S} \right\}$$

we have

$$\begin{aligned} D &\le \frac{\log q}{|\mathcal{S}|} \max_{\gcd(c,q)=1} \left| \sum_{(k,\mu)\in\mathcal{S}} \mathbf{e}_q\left(c\lfloor at(k,\mu)\rfloor_q\right) \right| \\ &\le \frac{\log q}{|\mathcal{S}|} \max_{\gcd(c,q)=1} \left| \sum_{(k,\mu)\in\mathcal{S}} \mathbf{e}_q\left(cat(k,\mu)\right) \right| \\ &\le \frac{\log q}{|\mathcal{S}|} \max_{\gcd(c,q)=1} \left| \sum_{(k,\mu)\in\mathcal{S}} \mathbf{e}_q\left(ct(k,\mu)\right) \right|. \end{aligned}$$

Applying Lemma 11 and the bound (6) we obtain

$$D = O\left(W^{1/2} q^{1/2-\delta} |\mathcal{M}|^{-1}\right) = O(q^{-\delta/2}) = o(2^{-\log^{1/2} q})$$

and the desired result follows. □

4. Insecurity of the Digital Signature Algorithm

4.1. Theoretical results

It now suffices to collect the previous results. For an integer ℓ we define the oracle $\mathcal{O}_\ell$ which, for any given DSA signature $(r(k), s(k,\mu))$, $k \in [0, q-1]$, $\mu \in \mathcal{M}$, returns the ℓ least significant bits of k. Combining (2), Lemma 4 and Lemma 12, we obtain:

THEOREM 13. *Let $\omega > 0$ be an arbitrary absolute constant. Let Q be a sufficiently large integer. The following statement holds with $\vartheta = 1/3$ for all primes $p \in [Q, 2Q]$, and with $\vartheta = 0$ for all primes $p \in [Q, 2Q]$ except at most $Q^{5/6+\varepsilon}$ of them. For any $\varepsilon > 0$ there exists $\delta > 0$ such that for any element $g \in \mathbb{F}_p$ of multiplicative order q, where $q \geq p^{\vartheta+\varepsilon}$ is prime, and any hash function h with*

$$W \leq \frac{|\mathcal{M}|^2}{q^{1-\delta}},$$

given an oracle $\mathcal{O}_\ell$ with

$$\ell = \left\lceil \omega \left(\frac{\log q \log\log\log q}{\log\log q} \right)^{1/2} \right\rceil,$$

there exists a probabilistic polynomial-time algorithm to find the signer's DSA secret key α from $O\left((\log q \log\log q / \log\log\log q)^{1/2}\right)$ signatures $(r(k), s(k,\mu))$ with $k \in [0, q-1]$ and $\mu \in \mathcal{M}$ selected independently and uniformly at random. The probability of success is at least $1 - q^{-1}$.

Proof. We choose $k \in [0, q-1]$ and $\mu \in \mathcal{M}$ independently and uniformly at random and ignore pairs $(k, \mu) \notin \mathcal{S}$. It follows from (6) that the expected number of choices in order to get d pairs $(k, \mu) \in \mathcal{S}$ is $d + O\left(dq^{-\delta}\right)$ for some $\delta > 0$ depending only on $\varepsilon > 0$.

Now, combining the inequality (2), Lemma 12 and Lemma 4 we obtain our main result. □

In Section 5.1, we extend this result to other consecutive bits, such as most significant bits or bits in the middle. The result is essentially the same for most significant bits, while one requires twice as many bits for arbitrary consecutive bits.

If a CVP_∞-oracle is available, the number ℓ of required bits can be decreased to 2 due to Lemma 5. The dimension of the lattice used by the oracle is $d + 1$, where the number d of required signatures is $O(\log q)$. More precisely we have:

THEOREM 14. *Let Q be a sufficiently large integer. The following statement holds with $\vartheta = 1/3$ for all primes $p \in [Q, 2Q]$, and with $\vartheta = 0$ for all primes $p \in [Q, 2Q]$ except at most $Q^{5/6+\varepsilon}$ of them. For any $\varepsilon > 0$ there exists $\delta > 0$ such that for any element $g \in \mathbb{F}_p$ of multiplicative order q, where $q \geq p^{\vartheta+\varepsilon}$ is prime, and any hash function h with*

$$W \leq \frac{|\mathcal{M}|^2}{q^{1-\delta}},$$

given an oracle $\mathcal{O}_\ell$ with $\ell = 2$ and a CVP_∞-oracle for the dimension $d+1$ where

$$d = \left\lceil \frac{8}{3} \log q \right\rceil,$$

there exists a probabilistic polynomial-time algorithm to find the signer's DSA secret key α from d signatures $(r(k), s(k,\mu))$ with $k \in [0, q-1]$ and $\mu \in \mathcal{M}$ selected independently and uniformly at random. The probability of success is at least $1 - q^{-1}$.

Accordingly, from Lemma 6 we derive:

THEOREM 15. *Let Q be a sufficiently large integer. The following statement holds with $\vartheta = 1/3$ for all primes $p \in [Q, 2Q]$, and with $\vartheta = 0$ for all primes $p \in [Q, 2Q]$ except at most $Q^{5/6+\varepsilon}$ of them. For any $\varepsilon > 0$ there exists $\delta > 0$ such that for any element $g \in \mathbb{F}_p$ of multiplicative order q, where $q \geq p^{\vartheta+\varepsilon}$ is prime, and any hash function h with*

$$W \leq \frac{|\mathcal{M}|^2}{q^{1-\delta}},$$

given an oracle $\mathcal{O}_\ell$ with

$$\ell = \lceil \log \log q \rceil,$$

there exists a probabilistic algorithm to find the signer's DSA secret key α, in time $q^{O(1/\log\log q)}$, from $O(\log q / \log\log q)$ signatures $(r(k), s(k,\mu))$ with $k \in [0, q-1]$ and $\mu \in \mathcal{M}$ selected independently and uniformly at random. The probability of success is at least $1 - q^{-1}$.

4.2. Experimental results

We report experimental results on the attack obtained with the NTL library [41] (see also [30]). The running time is less than half an hour for a number of signatures d less than a hundred, on a 500 MHz DEC Alpha. We used a 160-bit prime q, and a 512-bit prime p. For each choice of parameters size, we run the attack several times on newly generated parameters (including the prime q and the multipliers of the DSA–HNP). Each trial is referred as a *sample*. Using Babai's nearest plane algorithm [2] and Schnorr's Korkine-Zolotarev reduction [38, 40] with blocksize 20, we could break DSA with ℓ as low as $\ell = 4$ and $d = 70$. More precisely, the method always worked for $\ell = 5$ (a hundred samples). For $\ell = 4$, it worked 90% of the time over 100 samples. For $\ell = 3$, it always failed on about 100 samples, even with $d = 100$.

We made additional experiments with the well-known embedding strategy (see [32, 33]) and Schnorr's improved lattice reduction [38, 40] to solve the CVP. The embedding strategy heuristically reduces the CVP to the lattice shortest vector problem. More precisely, if the CVP-instance is given by the vector $\mathbf{a} = (a_1, \ldots, a_d)$ and a d-dimensional lattice spanned by the row vectors $\mathbf{b}_i = (b_{i,1}, \ldots, b_{i,d})$ with $1 \leq i \leq d$, the embedding strategy builds the lattice L spanned by the rows of the following matrix:

$$\begin{pmatrix} b_{1,1} & \ldots & b_{1,d} & 0 \\ b_{2,1} & \ldots & b_{2,d} & 0 \\ \vdots & & \vdots & \vdots \\ b_{d,1} & \ldots & b_{d,d} & 0 \\ a_1 & \ldots & a_d & 1 \end{pmatrix}.$$

It is hoped that the shortest vector of L (or one of the vectors of the reduced basis) is of the form $(\mathbf{a} - \mathbf{u}, 1)$ where $\mathbf{u}$ is a sufficiently close lattice vector we are looking for. Using that strategy, we were always able to solve the DSA problem with $\ell = 3$ and $d = 100$ (on more than 50 samples). We always failed with $\ell = 2$ and $d = 150$. In our experiments, to balance the coefficients of the lattice, we replaced the coefficient 1 in the lowest right-hand entry by $q/2^{\ell+1}$. When the attack succeeded, the vector $(\mathbf{a} - \mathbf{u}, q/2^{\ell+1})$ (where $\mathbf{u}$ is a lattice point revealing the hidden number) was generally the second vector of the reduced basis.

Our experimental bound is very close to that of Lemma 5. We believe it should be possible to reach $\ell = 2$ in practice using a lattice basis reduction algorithm more suited to the infinity norm (see for instance [37]), especially since the lattice dimension is reasonable. In fact, even $\ell = 1$ might be possible in practice: the proof of Lemma 5 does not rule out such a possibility.

As previously mentioned in the introduction, Bleichenbacher [6] has recently discovered a new attack in this setting, which does not use lattices. This attack is heuristic, but gives better experimental results for currently recommended values of parameters, if one is only interested in minimizing ℓ. More precisely, the best experimental result of [6] shows that one can recover the DSA secret key given a leakage of $\log 3 \approx 1.58$ bits for 2^{22} signatures, in about 3 days on a 450 MHz Ultrasparc using 500Mb of RAM. The number of signatures required is much larger than with the lattice approach with 3 bits (which is close to the information theoretic bound), but it is still reasonably small.

5. Remarks

5.1. Other consecutive bits

A similar argument works if, more generally, we are given consecutive bits at a known position.

The simplest case is when the consecutive bits are the most significant bits. The definition of most significant bits may depend on the context, as opposed to least significant bits. Here, we study two possible definitions. The usual definition refers to the binary encoding of elements in $\mathbb{F}_q$, where each element is encoded with n bits where $n = 1 + \lfloor \log q \rfloor$ is the bit-length of q. Thus, we define the ℓ most significant bits of an element $x \in \mathbb{F}_q$ as the unique positive integer $\mathrm{MSB}_{\ell,q}(x) \in \{0, \ldots, 2^{\ell-1}\}$ such that:

$$x - 2^{n-\ell}\mathrm{MSB}_{\ell,q}(x) \in \{0, \ldots, 2^{n-\ell} - 1\},$$

For instance, the most significant bit is 1 if $x \geq 2^{n-1}$, and 0 otherwise. However, this definition is not very well-suited to modular residues, since the most significant bit $\mathrm{MSB}_{1,q}(x)$ may in fact leak less than one bit of information: if q is very close to 2^{n-1}, then $\mathrm{MSB}_{1,q}(x)$ is most of the time equal to 0. Hence, Boneh and Venkatesan used in [7] another definition of most significant bits, which we will refer to as most significant modular bits. The ℓ most significant modular bits of an element $x \in \mathbb{F}_q$ are defined as the unique integer $\mathrm{MSMB}_{\ell,q}(x)$ such that

$$0 \leq x - \mathrm{MSMB}_{\ell,q}(x)q/2^{\ell} < q/2^{\ell}.$$

For example, the most significant modular bit is 0 if $x < q/2$, and 1 otherwise.

Now, recall that by definition of the DSA signature:

$$\alpha T(k,\mu) \equiv k - h(\mu)s(k,\mu)^{-1} \pmod{q},$$

where $T(k,\mu) = \lfloor r(k)s(k,\mu)^{-1} \rfloor_q$. It follows that for any integer ℓ:

$$\left|\alpha T(k,\mu) - h(\mu)s(k,\mu)^{-1} - 2^{n-\ell}\mathrm{MSB}_{\ell,q}(k) - 2^{n-\ell-1}\right|_q \leq 2^{n-\ell-1},$$

and

$$\left|\alpha T(k,\mu) - h(\mu)s(k,\mu)^{-1} - \mathrm{MSMB}_{\ell,q}(k)q/2^{\ell} - q/2^{\ell+1}\right|_q \leq q/2^{\ell+1}.$$

In other words, the ℓ most significant bits $\mathrm{MSB}_{\ell,q}(k)$ yield an approximation $\mathrm{APP}_{\ell-1,q}(\alpha T(k,\mu))$, while the ℓ most significant modular bits

$\mathrm{MSMB}_{\ell,q}(k)$ yield an approximation $\mathrm{APP}_{\ell,q}(\alpha T(k,\mu))$. Hence, Theorems 13 and 14 also hold for most significant usual and modular bits, provided that we add one more bit in the case of most significant (usual) bits.

For oracles returning ℓ consecutive bits in the middle, one requires twice as many bits. The idea is to use a trick, which appeared in the work of Frieze *et al.* [15], see (2.13) in that work, on breaking truncated linear congruential generators, and which is based on the following statement for which we provide a proof somewhat simpler to that of [15]. The paper [15] invokes Lenstra's work [25] on integer programming with a fixed number of variables. Our arguments makes use of a simple technique based on continued fractions.

LEMMA 16. *There exists a polynomial-time algorithm which, given A and B in $[1,q]$ finds $\lambda \in \mathbb{Z}_q^*$ such that*

$$|\lambda|_q < B \qquad \textit{and} \qquad |\lambda A|_q \le q/B.$$

Proof. Let P_i and Q_i denote respectively the numerator and denominator of the ith continued fraction convergents to the rational A/q, $i \ge 1$. There exists j such that $Q_j < B \le Q_{j+1}$. Then we have

$$\left| \frac{A}{q} - \frac{P_j}{Q_j} \right| \le \frac{1}{Q_j Q_{j+1}}$$

Therefore $|AQ_j - qP_j| \le q/Q_{j+1}$. Selecting $\lambda = Q_j$, we obtain the desired statement. □

Now, assume that we are given the ℓ consecutive bits of a nonce $k \in \mathbb{F}_q^*$, starting at some known position j. More precisely, we are given an integer a such that $0 \le a \le 2^\ell - 1$ and $k = 2^j a + 2^{\ell+j} b + c$ for some integers $0 \le b \le q/2^{\ell+j}$ and $0 \le c < 2^j$. We apply Lemma 16 with $B = q2^{-j-\ell/2}$ and $A = 2^{j+\ell}$, to obtain $\lambda \in \mathbb{F}_q^*$ such that:

$$|\lambda|_q < q2^{-j-\ell/2} \qquad \text{and} \qquad |\lambda 2^{j+\ell}|_q \le 2^{j+\ell/2}.$$

Multiplying by λ, the equation (1) can be rewritten as:

$$\alpha r(k) \lambda s(k,\mu)^{-1} \equiv \left(2^j a - s(k,\mu)^{-1} h(\mu)\right) \lambda + (c\lambda + 2^{\ell+j} b\lambda) \pmod q.$$

Notice that:

$$\begin{aligned} |c\lambda + 2^{\ell+j} b\lambda|_q &\le c|\lambda|_q + b|2^{\ell+j}\lambda|_q \\ &< 2^j q 2^{-j-\ell/2} + q/2^{\ell+j} 2^{j+\ell/2} = q/2^{\ell/2-1}. \end{aligned}$$

Thus, for arbitrary consecutive bits, one requires roughly twice as many bits. Note that [18] actually suggested that the bounds remained the same with arbitrary consecutive bits. More generally, by using high-dimensional lattice reduction, it is not difficult to show that when ℓ arbitrary bits at known positions are leaked, one requires roughly m as many bits, where m is the number of blocks of consecutive unknown bits.

5.2. Practical implications of our results

First of all we note that the constants in our theoretical results are effective and can be explicitly evaluated. One can also find a precise dependence of δ on ε in the above estimates. In particular, it would be interesting to obtain a non-asymptotic form of our theoretical results for the range of p and q corresponding to the real applications of DSA, that is, when q is a 160-bit prime and p is a 512-bit prime, see [26, 43].

The condition $W \le |\mathcal{M}|^2 q^{-1+\delta}$ does not seem too restrictive, as one could expect $W \sim |\mathcal{M}|^2 q^{-1}$ for any "good" hash function.

It might be worth noting that Lemma 10 implies that $r(k)$ takes exponentially many distinct values. Thus DSA indeed generates exponentially many distinct signatures. Certainly this fact has never been doubted in practice but our results provide its rigorous confirmation. On the other hand, the bound q^{δ} implied by Lemma 10 on the number of distinct values of $r(k)$ falls far below the expected value of order about q. Obtaining such a lower bound is a very challenging question which probably requires some advanced number theoretic tools.

Finally, we observe that if for efficiency reasons, one chooses either a nonce k with fewer bits than q or a sparse nonce k (to speed up the exponentiation at each signature round), then our attack obviously applies, because one then either knows or guesses with high probability sufficiently many bits of the nonce k. We remark that it could be quite tempting to choose such "special" k. Indeed, the size of q is currently determined by the time required by the $q^{1/2}$-attacks on the signer's discrete log key (such as Pollard's rho algorithm, see the survey [44]). However, such attacks fail to recover the value of k from $r(k)$ because the double reduction (modulo p and then modulo q) seems to erase all useful properties of the exponential function. Thus, simple exhaustive search may *a priori* seem the only method to recover k from $r(k)$, and one may believe that taking k in the range $1 \le k \le q^{1/2}$ does not undermine the security of the scheme. Our results show that this choice is fatal for the whole scheme.

To establish the corresponding uniformity of distribution results one can use bounds of exponential sums when k runs over a part of the interval $[1, q-1]$. Namely, for any element $g \in \mathbb{F}_p$ of multiplicative order T the bound

$$\max_{1 \le K \le T} \max_{\gcd(c,p)=1} \left| \sum_{k=1}^{K} \mathbf{e}_p\left(cg^k\right) \right| = O(p^{1/2} \log p)$$

holds, see Lemma 2 of [21] or Theorem 8.2 of [34]. This bound is nontrivial only for $T \ge p^{1/2+\varepsilon}$. Accordingly, our method applies only to larger values of q than in Theorems 13 and 14, namely $q \ge p^{1/2+\varepsilon}$, but the attack itself still can be launched (even without rigorous proof of success). In fact one can obtain an analogue of Lemma 8 for such short sums as well. For sparse exponents one can use the approach of [14] to obtain the necessary bounds of the corresponding exponential sums. We remark that the results of [14] apply only to the case of a primitive root g but the technique can be expanded to g of arbitrary (but sufficiently large) multiplicative order modulo p.

Hence, our results show that it is really essential to the security of DSA that the nonce k be generated by a cryptographically secure pseudo-random number generator. We also remark that a very different heuristic attack on very small values of $k = O(q^{1/2})$ has recently been described in [23]. Even in this case, if the attacker is able to apply a *timing* or *power* attack and select signatures corresponding to small values of k then the whole signature scheme is insecure. Generally, any leakage of information on k could prove dramatic.

5.3. Related signature schemes

One might wonder to which extent our results also apply to other DSA-related signature schemes (see [26, Section 11.5]), such as Schnorr's [39] or El Gamal's [12]. We follow the notations of Section 1.1.

Recall that in Schnorr's signature scheme, the signature of a message μ with a nonce $k \in \mathbb{F}_q^*$ is the pair $(e, s) \in \mathbb{F}_q^2$ defined as (the symbol $\|$ denoting as usual concatenation):

$$\begin{aligned} e(k, \mu) &= h\left(\mu \,\|\, \left\lfloor g^k \right\rfloor_p\right) \\ s(k, \mu) &= \left\lfloor k + \alpha e(k, \mu) \right\rfloor_q \end{aligned}$$

Obviously, the same attack applies with different multipliers. For instance, suppose that the ℓ least significant bits of k are known for several

signatures. Then, as in Section 1.4, it can be seen that recovering the signer's secret key α is a HNP with multiplier

$$t(k,\mu) = \left\lfloor e(k,\mu)2^{-\ell} \right\rfloor_q.$$

Under the random oracle model, $t(k,\mu)$ has (perfect) uniform distribution, making Lemmas 4 and 5 directly applicable. The same holds for any block of consecutive bits. Hence, our results are even simpler with Schnorr's signature scheme.

In El Gamal's signature scheme, there is only one large prime p, and g is a generator of $\mathbb{F}_p^*$. The signature of a message μ with a nonce $k \in [1, p-2]$ coprime with $p-1$ is the pair $(r,s) \in [1,p-1]^2$ defined as:

$$\begin{aligned} r(k) &= \left\lfloor g^k \right\rfloor_p \\ s(k,\mu) &= \left\lfloor k^{-1}(h(\mu) - \alpha r(k)) \right\rfloor_p \end{aligned}$$

This time, we cannot work with the least significant bits, as 2 is not invertible modulo $p-1$. So suppose instead that the ℓ most significant modular bits of k are known for several signatures. Then we obtain a HNP with multiplier:

$$t(k,\mu) = \left\lfloor r(k)s(k,\mu)^{-1} \right\rfloor_p.$$

The resemblance with the DSA case is of course natural. Statements similar to that of Section 3 can be obtained on such multipliers. In fact, for this case, many things can be done in much stronger form. In particular, it has been shown in [42] that in El Gamal's signature scheme the pairs $(r(k), s(k,\mu))$ are uniformly distributed modulo p, rather than just their ratios $t(k,\mu)$. Thus we have no doubt that a similar attack applies to this scheme as well, however we are not able to give a rigorous proof of this statement because the above approach to the HNP fails to work modulo a composite. Probably some further adjustments and modifications should be made to design an algorithm for the HNP modulo a composite, which could be an interesting problem by itself.

The modifications of DSA described in [26, Table 11.5]), see also [36], can be studied by our method as well, see [13]. Also, in [31] we have obtained similar results for the elliptic curve analogue of DSA.

Finally, the results and ideas of this paper have recently been used in [10] to design an attack on another DSA-based cryptosystem. It is shown in [10] that in the above cryptosystem there is a way to extract

all necessary information from the protocol itself, thus no additional "leakage" is assumed. In fact, Lemma 11 allows us to make the attack of [10] rigorously proved and also to extend it to other small subgroups of $\mathbb{F}_p^*$ (not only those with a power of 2 elements as in [10]).

Acknowledgements

We thank Daniel Bleichenbacher, Dan Boneh, Nick Howgrave–Graham and Ramarathnam Venkatesan for helpful discussions. Part of this work was done while the first author was visiting Stanford University, whose hospitality is gratefully acknowledged.

References

1. M. Ajtai, R. Kumar, and D. Sivakumar. A sieve algorithm for the shortest lattice vector problem. In *Proc. 33rd ACM Symp. on Theory of Computation (STOC'2001), Crete*, pages 601–610, 2001.
2. L. Babai. On Lovász lattice reduction and the nearest lattice point problem. *Combinatorica*, 6:1–13, 1986.
3. M. Bellare, S. Goldwasser, and D. Micciancio. "Pseudo-random" number generation within cryptographic algorithms: The DSS case. In *Proc. of Crypto '97*, volume 1294 of *LNCS*. IACR, Springer-Verlag, 1997.
4. M. Bellare and P. Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In *Proc. of the 1st ACM Conference on Computer and Communications Security*, pages 62–73. ACM Press, 1993.
5. D. Bleichenbacher, 1999. Private communication.
6. D. Bleichenbacher. On the generation of DSS one-time keys. Manuscript. The result was presented at the Monteverita workshop in March, 2001., February 2001.
7. D. Boneh and R. Venkatesan. Hardness of computing the most significant bits of secret keys in Diffie-Hellman and related schemes. In *Proc. of Crypto '96*, volume 1109 of *LNCS*. IACR, Springer-Verlag, 1996.
8. D. Boneh and R. Venkatesan. Rounding in lattices and its cryptographic applications. In *Proc. of the 8th Symposium on Discrete Algorithms*, pages 675–681. ACM, 1997.
9. E. Brickell, D. Pointcheval, S. Vaudenay, and M. Yung. Design validations for discrete logarithm based signature schemes. In *Proc. of PKC '2000*, volume 1751 of *LNCS*, pages 276–292. Springer-Verlag, 2000.
10. D. R. L. Brown and A. J. Menezes. A small subgroup attack on a key agreement protocol of Arazi. Technical report, Dept. of Combinatorics and Optimization, Univ. of Waterloo, 2001. CORR 2001–50.
11. M. Drmota and R. Tichy. *Sequences, discrepancies and applications*. Springer-Verlag, Berlin, 1997.
12. T. El Gamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Trans. Inform. Theory*, 31:469–472, 1985.

13. E. El Mahassni, P. Q. Nguyen, and I. E. Shparlinski. The insecurity of Nyberg–Rueppel and other DSA-like signature schemes with partially known nonce. In *Proc. Workshop on Cryptography and Lattices (CALC '01)*, volume 2146 of *LNCS*, pages 97–109. Springer-Verlag, 2001.
14. J. B. Friedlander and I. E. Shparlinski. On the distribution of diffie–hellman triples with sparse exponents. *SIAM J. Discr. Math.*, 14:162–169, 2001.
15. A. M. Frieze, J. Håstad, R. Kannan, J. C. Lagarias, and A. Shamir. Reconstructing truncated integer variables satisfying linear congruences. *SIAM J. Comput.*, 17:262–280, 1988. Special issue on cryptography.
16. M. I. González Vasco and I. E. Shparlinski. On the security of Diffie-Hellman bits. In K.-Y. Lam, I. E. Shparlinski, H. Wang, and C. Xing, editors, *Proc. Workshop on Cryptography and Computational Number Theory (CCNT'99), Singapore*, pages 257–268. Birkhäuser, 2001.
17. M. I. González Vasco and I. E. Shparlinski. Security of the most significant bits of the Shamir message passing scheme. *Math. Comp.*, 71:333–342, 2002.
18. N. A. Howgrave-Graham and N. P. Smart. Lattice attacks on digital signature schemes. *Design, Codes and Cryptography*, 23:283–290, 2001.
19. R. Kannan. Algorithmic geometry of numbers. In *Annual Review of Comp. Sci.*, volume 2, pages 231–267, 1987.
20. S. V. Konyagin and I. E. Shparlinski. *Character sums with exponential functions and their applications*. Cambridge Univ. Press, Cambridge, 1999.
21. N. M. Korobov. On the distribution of digits in periodic fractions. *Math. USSR – Sbornik*, 18:659–676, 1972.
22. R. Kuipers and H. Niederreiter. *Uniform Distribution of Sequences*. Wiley-Interscience, NY, 1974.
23. H. Kuwakado and H. Tanaka. On the security of the ElGamal-type signature scheme with small parameters. *IEICE Transactions on Fundamentals of Electronics, Commun., and Comp. Sci.*, E82-A:93–97, 1999.
24. A. K. Lenstra, H. W. Lenstra, Jr., and L. Lovász. Factoring polynomials with rational coefficients. *Mathematische Ann.*, 261:513–534, 1982.
25. H. W. Lenstra, Jr. Integer programming with a fixed number of variables. *Math. Oper. Res.*, 8(4):538–548, 1983.
26. A. Menezes, P. Van Oorschot, and S. Vanstone. *Handbook of Applied Cryptography*. CRC Press, 1997.
27. D. Micciancio. *On the hardness of the shortest vector problem*. PhD Thesis, MIT, 1998.
28. C. J. Moreno and O. Moreno. Exponential sums and Goppa codes, I. *Proc. Amer. Math. Soc.*, 111:523–531, 1991.
29. National Institute of Standards and Technology (NIST). *FIPS Publication 186: Digital Signature Standard*, May 1994.
30. P. Q. Nguyen. The dark side of the hidden number problem: Lattice attacks on DSA. In K.-Y. Lam, I. E. Shparlinski, H. Wang, and C. Xing, editors, *Proc. Workshop on Cryptography and Computational Number Theory (CCNT'99), Singapore*, pages 321–330. Birkhäuser, 2001.
31. P. Q. Nguyen and I. E. Shparlinski. The insecurity of the elliptic curve Digital Signature Algorithm with partially known nonces. *Design, Codes and Cryptography*, to appear.
32. P. Q. Nguyen and J. Stern. Lattice reduction in cryptology: An update. In *Algorithmic Number Theory – Proc. of ANTS-IV*, volume 1838 of *LNCS*, pages 85–112. Springer-Verlag, 2000.

33. P. Q. Nguyen and J. Stern. The two faces of lattices in cryptology. In *Proc. Workshop on Cryptography and Lattices (CALC '01)*, volume 2146 of *LNCS*, pages 146–180. Springer-Verlag, 2001.
34. H. Niederreiter. Quasi-Monte Carlo Methods and Pseudo-random Numbers. *Bull. Amer. Math. Soc.*, 84:957–1041, 1978.
35. H. Niederreiter. *Random Number Generation and Quasi–Monte Carlo Methods*, volume 63. SIAM, Philadelphia, 1992. CBMS-NSF Regional Conference Series in Applied Mathematics.
36. K. Nyberg and R. A. Rueppel. Message recovery for signature schemes based on the discrete logarithm problem. *J. Cryptology*, 8:27–37, 1995.
37. H. Ritter. Breaking knapsack cryptosystems by max-norm enumeration. In *Proc. of Pragocrypt '96*, pages 480–492. CTU Publishing House, 1996.
38. C. P. Schnorr. A hierarchy of polynomial lattice basis reduction algorithms. *Theoretical Computer Science*, 53:201–224, 1987.
39. C. P. Schnorr. Efficient signature generation by smart cards. *Journal of Cryptology*, 4:161–174, 1991.
40. C. P. Schnorr and M. Euchner. Lattice basis reduction: Improved practical algorithms and solving subset sum problems. *Math. Programming*, 66:181–199, 1994.
41. V. Shoup. Number Theory C++ Library (NTL) version 3.6. Available at `http://www.shoup.net/ntl/`.
42. I. E. Shparlinski. On the uniformity of distribution of the El Gamal signature. *Appl. Algebra in Engin., Commun. and Computing*, to appear.
43. D. R. Stinson. *Cryptography: Theory and Practice*. CRC Press, 1995.
44. E. Teske. Square-root algorithms for the discrete logarithm problem (A survey). In *Proc. of the Conference "Public Key Cryptography and Computational Number Theory", Warszawa, September 11-15, 2000*, pages 283–301, 2001.
45. S. Vaudenay. Hidden collisions on DSS. In *Proc. of Crypto '96*, volume 1109 of *LNCS*, pages 83–88. IACR, Springer-Verlag, 1996.
46. I. M. Vinogradov. *Elements of Number Theory*. Dover Publ., New York, 1954.