Proceedings STACS 2003,
(Berlin, Germany, Febbruary/March 2003)
Eds. H. Alt, M. Habib, Springer-Verlag, LNCS 2607, pages 145–156

Lattice Reduction by Random Sampling and Birthday Methods.

Claus Peter Schnorr

Fachbereiche Mathematik/Biologie-Informatik,
Universität Frankfurt, PSF 111932, D-60054 Frankfurt am Main, Germany.
schnorr@cs.uni-frankfurt.de http://www.mi.informatik.uni-frankfurt.de/

Abstract. We present a novel practical algorithm that given a lattice basis $b_1, ..., b_n$ finds in $O(n^2(\frac{k}{6})^{k/4})$ average time a shorter vector than b_1 provided that b_1 is $(\frac{k}{6})^{n/(2k)}$ times longer than the length of the shortest, nonzero lattice vector. We assume that the given basis $b_1, ..., b_n$ has an orthogonal basis that is typical for worst case lattice bases. The new reduction method samples short lattice vectors in high dimensional sublattices, it advances in sporadic big jumps. It decreases the approximation factor achievable in a given time by known methods to less than its fourth-th root. We further speed up the new method by the simple and the general birthday method.

1 Introduction and Summary

History. The set of all linear combinations with integer coefficients of a set of linearly independent vectors $b_1, ..., b_n \in \mathbf{R}^d$ is a *lattice* of *dimension* n. The problem of finding a shortest, nonzero lattice vector is a landmark problem in complexity theory. This problem is polynomial time for fixed dimension n due to [LLL82] and is NP-hard for varying n [E81, A98, M98]. No efficient algorithm is known to find very short vectors in high dimensional lattices. Improving the known methods has a direct impact on the cryptographic security of many schemes, see [NS00] for a surview.

Approximating the shortest lattice vector to within an *approximation factor* (*apfa* for short) c means to find a nonzero lattice vector with at most c-times the minimal possible length. We consider integer lattices of dimension n in $\mathbf{Z}^n$ with a given lattice basis consisting of integer vectors of Euclidean length $2^{O(n)}$. The LLL-algorithm of Lenstra, Lenstra, Lovász [LLL82] achieves for arbitrary $\varepsilon > 0$ an *apfa* $(\frac{4}{3} + \varepsilon)^{n/2}$ in $O(n^5)$ steps using integers of bit length $O(n^2)$. This algorithm repeatedly constructs short bases in two-dimensional lattices, the two-dimensional problem was already solved by Gauss. The recent segment LLL-reduction of Koy-Schnorr [KS01a,KS02] achieves the same apfa $(\frac{4}{3} + \varepsilon)^{n/2}$ within $O(n^3 \log n)$ steps.

Finding very short lattice vectors requires additional search beyond LLL-type reduction. The algorithm of Kannan [K83] finds the shortest lattice vector in time $n^{O(n)}$ by a diligent exhaustive search, see [H85] for an $n^{\frac{n}{2}+o(n)}$ time

algorithm. The recent probabilistic sieve algorithm of [AKS01] runs in $2^{O(n)}$ average time and space, but is impractical as the exponent $O(n)$ is about $30\,n$. Schnorr [S87] has generalized the LLL-algorithm in various ways that repeatedly construct short bases of k-dimensional lattices of dimension $k \geq 2$. While $2k$-reduction [S87] runs in $O(n^3k^{k+o(k)}+n^4)$ time, the stronger BKZ-reduction [S87, SE91] is quite efficient for $k \leq 20$ but lacks a proven time bound. LLL-reduction is the case $k = 1$ of $2k$-reduction.

Our novel method randomly samples short lattice vectors in high dimensional sublattices, and inserts by a global transform short vectors into the lattice basis. It remarkably differs from previous LLL-type reductions that locally transform the lattice basis by reducing small blocks of consecutive basis vectors. The new method applies to lattice bases for which the associated orthogonal basis satisfies two conditions, RA and GSA, defined in Section 2. These conditions are natural for worst case lattice bases and also play in AJTAI's recent worst case analysis [A02] of Schnorr's $2k$-reduction. Our new method is practical and space efficient and outperforms all previous algorithms.

Sampling reduction inserts a short vector found by random sampling into the basis, BKZ–reduces the new basis and iterates the procedure with the resulting basis. We observed sporadic big jumps of progress during BKZ–reduction, jumps that are difficult to analyze. We study the progress of the new method in attacks on the GGH-cryptosysytem [GGH97] where we build on our previous experience. We report in detail, we believe that our findings extend beyond GGH to general applications. We expect that the new algorithms lower the security of lattice based cryptosystems.

	time	space/n	*apfa*
1. sampl. reduction	$n^3(\frac{k}{6})^{k/4}$	1	$(\frac{k}{6})^{n/2k}$
2. simple birthday	$n^3(\frac{4}{3})^{k/3}(\frac{k}{6})^{k/8}$	$(\frac{4}{3})^{k/3}(\frac{k}{6})^{k/8}$	$(\frac{k}{6})^{n/2k}$
3. primal–dual (Koy)	$n^3k^{k/2+o(k)}$	1	$(\frac{k}{6})^{n/k}$
4. $2k$-reduction [S87]	$n^3k^{k+o(k)}$	1	$(\frac{k}{3})^{n/k}$

Table 1. Theoretic performance of new and previous methods

The shown time bounds must be completed by a constant factor and an additive term $O(n^4)$ covering LLL-type reduction. The integer $k, 2 \leq k \leq n/2$, can be freely chosen. The entry c under space/n means that $c+O(n)$ lattice vectors, consisting of $c \cdot n + O(n^2)$ integers, must be stored. The original LLL-algorithm uses integers of bit length $O(n^2)$ required to compute the orthogonal basis in exact integer arithmetic. However, by computing the orthogonal basis in approximate rational arithmetic (floating point arithmetic in practice) LLL-type reduction can be done in $O(n^5)$ arithmetic steps using integers of bit length $O(n)$. The proven analysis of Schnorr [S88] induces diligent steps for error correction, but simple methods of scaling are sufficient in practice [KS01b].

Sampling Reduction repeats the algorithm SHORT of Section 2 $O(n)$-times, see Section 3. SHORT runs in $O(n^2(\frac{k}{6})^{k/4})$ time and decreases with probability $\frac{1}{2}$ an *apfa* greater than $(\frac{k}{6})^{n/2k}$ by a factor $\sqrt{0.99}$. The *apfa* $(\frac{k}{6})^{n/2k}$ is about the

4-th root of the proven *apfa* achievable in the same time by Koy's primal–dual method, the best known fully proven algorithm.

Section 4 combines random sampling with general birthday methods of [W02]. Birthday sampling stores many statistically independent short lattice vectors $\bar{b}_i$ and searches in the spirit of WAGNER's 2^t-list algorithm a vector $b = \sum_{i=1}^{2^t} \bar{b}_i$ that is shorter than b_1. Simple birthday sampling for $t = 1$ further decreases the *apfa* achievable in a given time to its square root, but its practicability hinges on the required space.

Method 4 produces $2k$-reduced bases [S87, Theorem 3.1], and proceeds via shortest lattice vectors in dimension $2k$ while KOY's primal–dual method 3 repeatedly constructs shortest lattice vectors in dimension k [K00]. The *apfa*'s of Methods 3 and 4 assume the realistic bound $\gamma_k \le k/6$ for $k \ge 24$ for the HERMITE constant γ_k; γ_k is the maximum of $\lambda_1(L)^2(\det(L)^{-2/k}$ for lattices L of dimension k and the length $\lambda_1(L)$ of the shortest, nonzero vector in L.

Notation. An ordered set of linearly independent vectors $b_1, ..., b_n \in \mathbf{Z}^d$ is a *basis* of the integer *lattice* $L = \sum_{i=1}^n b_i\mathbf{Z} \subset \mathbf{Z}^d$, consisting of all linear integer combinations of $b_1, ..., b_n$. We write $L = L(b_1, ..., b_n)$. Let $\widehat{b}_i$ denote the component of b_i that is orthogonal to $b_1, ..., b_{i-1}$ with respect to the *Euclidean inner product* $\langle x, y\rangle = x^\top y$. The *orthogonal vectors* $\widehat{b}_1, ..., \widehat{b}_n \in \mathbf{R}^d$ and the *Gram-Schmidt coefficients* $\mu_{j,i}$, $1 \le i, j \le n$, associated with the basis $b_1, ..., b_n$ satisfy for $j = 1, ..., n$ $\quad b_j = \sum_{i=1}^j \mu_{j,i}\widehat{b}_i, \quad \mu_{j,j} = 1, \quad \mu_{j,i} = 0$ for $i > j$,

$$\mu_{j,i} = \langle b_j, \widehat{b}_i\rangle / \langle \widehat{b}_i, \widehat{b}_i\rangle, \qquad \langle \widehat{b}_j, \widehat{b}_i\rangle = 0 \text{ for } j \ne i.$$

We let $\pi_i : \mathbf{R}^n \to \mathrm{span}(b_1, ..., b_{i-1})^\perp$ denote the *orthogonal projection*, $\pi_i(b_k) = \sum_{j=i}^n \mu_{k,j}\widehat{b}_j$, $\pi_i(b_i) = \widehat{b}_i$. Let $\|b\| = \langle b, b\rangle^{\frac{1}{2}}$ denote the *Euclidean length* of a vector $b \in \mathbf{R}^d$. Let λ_1 denote the length of the shortest nonzero lattice vector of a given lattice. The *determinant* of lattice $L = L(b_1, ..., b_n)$ is $\det L = \prod_{i=1}^n \|\widehat{b}_i\|$. For simplicity, let all given lattice bases be bounded so that $\max_i \|b_i\| = 2^{O(n)}$. Our time bounds count arithmetic steps using integers of bit length $O(n)$.

2 Random Sampling of Short Vectors

Let L be a lattice with given basis $b_1, \ldots, b_n$. As a lattice vector $b = \sum_{j=1}^n \mu_j\widehat{b}_j$ has length $\|b\|^2 = \sum_{j=1}^n \mu_j^2\|\widehat{b}_j\|^2$ the search for short lattice vectors naturally comprises two steps:

1. Decreasing μ_i to $|\mu_i| \le \frac{1}{2}$ for $i = 1, ..., n$: given $b \in L$ with arbitrary μ_i the vector $b' = b - \mu\, b_i$ has $\mu_i' = \mu_i - \mu$ and thus $|\mu_i'| \le \frac{1}{2}$ holds if $|\mu - \mu_i| \le \frac{1}{2}$.

2. Shortening $\widehat{b}_j$, i.e., replacing b_j by a nonzero vector $b \in L(b_j, ..., b_n)$ that minimizes $\|\pi_j(b)\|^2 = \sum_{i=j}^n \mu_i^2\|\widehat{b}_i\|^2$ over a suitable subset $S_j \subset L(b_j, ..., b_n)$.

The various reduction algorithms differ by the choice of S_j. The LLL-algorithm uses $S_j = L(b_j, b_{j+1})$, BKZ-reduction [S87, SE91] uses $S_j = L(b_j, ..., b_{j+k-1})$, $2k$-reduction [S87] uses a subset $S_j \subset L(b_j, ..., b_{j+2k-1})$ and HKZ-reduction minimizes over the entire lattice $L(b_j, ..., b_n)$. LLL-type reduction [LLL82, S87, SE91]

repeatedly replaces a block $b_j, ..., b_{j+k-1}$ for various j by an equivalent block starting with a vector $b \in L(b_j, ..., b_{j+k-1})$ of shorter length $\|\pi_j(b)\| \neq 0$. The vector b is produced by exhaustive enumeration.

The novel *sampling reduction* repeatedly produces via random sampling a nonzero vector $b \in L(b_j, \ldots, b_n)$ with $\|\pi_j(b)\| < \|\widehat{b}_j\|$, and continues with a new basis $b_1, ..., b_{j-1}, b, b_j, ..., b_{n-1}$. Such b cannot be efficiently produced by exhaustive search, the dimension of $L(b_j, \ldots, b_n)$ is to high. Surprisingly, random sampling in high dimension $n-j+1$ outperforms exhaustive search in low dimension k. Here we introduce random sampling for $j = 1$, the algorithm ESHORT of Section 3 uses a straightforward extension to $j \geq 1$. Random sampling for $j = 1$ searches short vectors $b = \sum_{i=1}^{n} \mu_i \widehat{b}_i \in L$ with small coefficients $\mu_1, \ldots, \mu_k$. This makes $\|b\|^2 = \sum_{i=1}^{n} \mu_i^2 \|\widehat{b}_i\|^2$ small. Importantly, the initial vectors $\widehat{b}_1, ..., \widehat{b}_k$ are in practice longer than the $\widehat{b}_i$ for $i > k$, so small coefficients $\mu_1, ..., \mu_k$ have a bigger impact than small μ_i for $i > k$. We analyse this idea assuming that the lengths $\|\widehat{b}_1\|^2, ..., \|\widehat{b}_n\|^2$ are close to a geometric series.

The Sampling Method. Let $1 \leq u < n$ be constant. Given a lattice basis $b_1, ..., b_n$ we sample lattice vectors $b = \sum_{i=1}^{n} t_i b_i = \sum_{i=1}^{n} \mu_i \widehat{b}_i$ satisfying

$$|\mu_i| \leq \begin{cases} \frac{1}{2} \text{ for } i < n-u \\ 1 \text{ for } n-u \leq i < n \end{cases}, \qquad \mu_n = 1. \tag{1}$$

There are at least 2^u distinct lattice vectors b of this form. The sampling algorithm (SA) below generates a single vector b in time $O(n^2)$. The subsequent algorithm SHORT samples distinct vectors via SA until a vector b is found that is shorter than b_1. The choice of $\mu_n = 1$ implies that $b_1, ..., b_{j-1}, b, b_j, ..., b_{n-1}$ is a lattice basis.

Sampling Algorithm (SA)

INPUT lattice basis $b_1, ..., b_n \in \mathbf{Z}^n$ with coefficients $\mu_{i,j}$.

1. $b := b_n, \quad \mu_j := \mu_{n,j}$ for $j = 1, ..., n-1$
2. FOR $i = n-1, ..., 1$ DO

   Select $\mu \in \mathbf{Z}$ such that $|\mu_i - \mu| \leq \begin{cases} \frac{1}{2} \text{ for } i < n-u \\ 1 \text{ for } i \geq n-u \end{cases}$

   $b := b - \mu\, b_i, \;\; \mu_j := \mu_j - \mu\, \mu_{i,j}$ for $j = 1, ..., i$

OUTPUT b, $\mu_1, ..., \mu_n$ satisfying $b = \sum_{i=1}^{n} \mu_i \widehat{b}_i$ and (1).

The coefficient μ_i is updated $(n-i)$–times. This leads to a nearly uniform distribution of the μ_i, in particular for small i, which is crucial for our method. Note that SA is deterministic, the random sampling is "pseudo-random" in a weak heuristic sense.

Randomness Assumption RA. Let the coefficients μ_i of the vectors $b = \sum_{i=1}^{n} \mu_i \widehat{b}_i$ sampled by SA be uniformly distributed in $[-\frac{1}{2}, \frac{1}{2}]$ for $i < n-u$ and in $[-1, 1]$ for $n-u \leq i < n$, let the μ_i be statistically independent for distinct i, and let the coefficients μ_i, μ_i' of distinct vectors b, b' sampled by SA be statistically independent.

The Geometric Series Asumption (GSA). Let $\|\widehat{b}_i\|^2/\|b_1\|^2 = q^{i-1}$ for $i = 1, ..., n$ be a geometric series with quotient q, $\frac{3}{4} \leq q < 1$.

The GSA *in Practice.* In practice the quotients $\|\widehat{b}_i\|^2/\|b_1\|^2$ approximate the q^{i-1} without achieving equality. Importantly, our conclusions under GSA also hold for approximations where $\sum_{i=1}^{n} \mu_i^2 \, (\, \|\widehat{b}_i\|^2/\|b_1\|^2 - q^{i-1} \,)$ is sufficiently small for random $\mu_i \in_R [-\frac{1}{2}, \frac{1}{2}]$, e.g. smaller than 0.01 for Theorems 1 and 2.

We have tested the GSA for the public GGH-bases according to the cryptosystem of [GGH97]. After either Koy's primal–dual reduction or after BKZ–reduction with block size 20 these bases closely approximate GSA and RA. The GSA–behavior is significantly better after BKZ–reduction than after primal-dual reduction. Lattice bases that are not reduced by an LLL–type reduction usually have bad GSA–behavior.

Under the GSA the values $\log_2(\|b_i\|^2/\|\widehat{b}_i\|^2)$ for $i = 1, ..., n$ are on a straight line. For lattice bases that are BKZ–reduced these values closely approximate a line. Figure 1 shows a GGH–basis generated according to the GGH–cryptosystem [GGH97] after various reductions and a final BKZ–reduction with block size 20.

Fig. 1. The values $\log_2(\|b_1\|^2/\|\widehat{b}_i\|^2)$ for $i = 1, ..., 200$ of a BKZ–basis

Worst case bases satisfy the GSA. We show that lattice reduction is harder the better the given basis approximates a geometric series. Lattice bases satisfying the GSA are worst case bases for lattice reduction. Here, let the goal of lattice reduction be to decrease the proven *apfa*, i.e., to decrease $\max_i \|b_1\|/\|\widehat{b}_i\|$ via a new lattice basis. Note that $apfa \leq \max_i \|b_1\|/\|\widehat{b}_i\|$ holds for all bases while GSA implies $apfa \leq q^{(-n+1)/2}$.

We associate with a basis $b_1, ..., b_n$ the quotients $q_i := (\|\widehat{b}_i\|^2/\|b_1\|^2)^{\frac{1}{i-1}}$ for $i = 2, ..., n$, $q := q_n$. As $apfa \leq q^{(-n+1)/2}$ the goal of the reduction is to increase q. Of course our reduction problem gets easier for smaller n and smaller q.

If GSA does not hold we have that $q_i \neq q$ for some i. Select i as to maximize $|q_i - q|$. We transform the given reduction problem into smaller, easier problems with bases that better approximate the GSA.

If $q_i < q$ we reduce the subbasis $b_1, ..., b_i$ by decreasing $\max_i \|b_1\|/\|\widehat{b}_i\|$ via a new lattice basis. If $q_i > q$ we reduce the basis $\pi_i(b_i), ..., \pi_i(b_n)$. The q-value $\overline{q}_i := (\|\widehat{b}_n\|^2/\|\widehat{b}_i\|^2)^{\frac{1}{n-i}}$ of that basis satisfies $q^{n-1} = q_i^{i-1}\overline{q}_i^{n-i}$, thus either $q_i < q$ or $\overline{q}_i < q$.

In either case we solve an easier lattice problem with a smaller q–value and a smaller dimension. Our procedure decreases $|q - q_i|$ providing a basis that better approximates a geometric series. Therefore, lattice bases of the same q–value get harder the better they approximate a geometric series.

Random Sampling Short Vectors. Let $k, u \geq 1$ be constants, $k + u < n$. Consider the event that vectors $b = \sum_{i=1}^{n} \mu_i \widehat{b}_i$ sampled by SA satisfy

$$|\mu_i|^2 \leq \tfrac{1}{4}\, q^{k-i} \qquad \text{for} \quad i = 1, ..., k. \tag{2}$$

Under RA that event has probability $\prod_{i=1}^{k} q^{(k-i)/2} = q^{\binom{k}{2}/2}$. We study the probability that $\|b\|^2 < \|b_1\|^2$ holds under RA and the conditions (1), (2).

Lemma 1. *Random* $\mu_i \in_R [-\frac{1}{2}, \frac{1}{2}]$ *have the mean value* $\mathbf{E}[\mu_i^2] = \frac{1}{12}$.

Lemma 2. *Under* GSA *and* RA *the vectors* b *sampled by* SA *satisfy* $\mathbf{Pr}\big[\, \|b\|^2 \, \|b_1\|^{-2} \leq \frac{1}{12}[k\, q^{k-1} + (q^k + 3\, q^{n-u-1})/(1-q)]\,\big] \geq \frac{1}{2} q^{\binom{k}{2}\frac{1}{2}}$.

Proof. By Lemma 1 we have under (1), (2) the mean value

$$\mathbf{E}[\, \mu_i^2 \,|\, (2)\,] \;=\; \begin{cases} \frac{1}{12}\, q^{k-i} \text{ for } i = 1, \ldots, k \\ 1/12 \quad \text{for } i = k+1, ..., n-u-1 \\ 1/3 \quad \text{for } i = n-u, \ldots, n-1 \end{cases}$$

Under GSA this yields $\mathbf{E}[\, \|b\|^2 \|b_1\|^{-2} \;|\; (2)\,]$

$$\begin{aligned} &= \tfrac{1}{12}\big[\, \textstyle\sum_{i=1}^{k} q^{k-i} \|\widehat{b}_i\|^2 + \sum_{i=k+1}^{n-u-1} \|\widehat{b}_i\|^2 + 4 \sum_{i=n-u}^{n-1} \|\widehat{b}_i\|^2 \big] + \|\widehat{b}_n\|^2 \\ &= \tfrac{1}{12}\big[\, \textstyle\sum_{i=1}^{k} q^{k-i+i-1} + \sum_{i=k+1}^{n-u-1} q^{i-1} + 4\, q^{n-u-1} \sum_{i=1}^{u} q^{i-1} \big] + q^{n-1} \\ &= \tfrac{1}{12}\big[k\, q^{k-1} + [(q^k - q^{n-u-1}) + 4q^{n-u-1}(1-q^u)]/(1-q)\big] + q^{n-1} \\ &= \tfrac{1}{12}\,[k\, q^{k-1} + (q^k + 3\, q^{n-u-1} - 4\, q^{n-1})/(1-q)] + q^{n-1}. \end{aligned}$$

This proves the claim as $4/(q-1) \geq 1$, and (2) holds with probability $q^{\binom{k}{2}/2}$. □

SHORT Algorithm

INPUT lattice basis $b_1, ..., b_n \in \mathbf{Z}^n$ with quotient $q < 1$

Let $u := 1 + \lceil -\binom{k}{2}\frac{1}{2} \log_2 q) \rceil$ be the minimal integer so that $2^u \geq 2\, q^{-\binom{k}{2}\frac{1}{2}}$.

Sample via SA up to 2^u distinct lattice vectors $b = \sum_{i=1}^{n} \mu_i \widehat{b}_i$ satisfying the inequalities (1) until a vector is found such that $\|b\|^2 < 0.99\, \|b_1\|^2$.

OUTPUT lattice vector b satisfying $\|b\|^2 < 0.99\, \|b_1\|^2$.

Theorem 1. *Given a lattice basis $b_1, ..., b_n$ with quotient $q \leq (\frac{6}{k})^{1/k}$,* SHORT *runs in $O(n^2 q^{-k^2/4})$ time and finds under* GSA *and* RA *with probability $\frac{1}{2}$ for sufficiently large k and n a nonzero lattice vector b so that $\|b\|^2 < 0.99\,\|b_1\|^2$.*

Proof. W.l.o.g. let $q^k = \frac{6}{k}$ as the claim holds a fortiori for smaller q. The inequality

$$\tfrac{1}{12}\,[k\,q^{k-1} + (q^k + 3\,q^{n-u-1})/(1-q)] \leq \tfrac{1}{2q} + \tfrac{1}{12}\,\tfrac{q^k+3\,q^{3k}}{1-q} < 0.99.$$

holds for $k = 24$ and $n \geq 3k+u+1$. As $\frac{1}{2q} + \frac{1}{12}\,\frac{q^k+3\,q^{3k}}{1-q}$ decreases for $q = (\frac{6}{k})^{1/k}$ with k the inequality holds for all $k \geq 24$. Hence, the vectors b sampled by SA satisfy $\mathbf{Pr}[\,\|b\|^2\|b_1\|^{-2} < 0.99\,] \geq \frac{1}{2}\,q^{\binom{k}{2}/2}$ by Lemma 2. As SHORT samples $2\,q^{-\binom{k}{2}/2}$ independent vectors b it finds under RA with probability $1 - e^{-1} > \frac{1}{2}$ some b with $\|b\|^2\|b_1\|^{-2} < 0.99$. □

Remark. **1.** SHORT improves under GSA and RA an *apfa* $(\frac{k}{6})^{n/2k}$ in $O(n^2(\frac{k}{6})^{k/4})$ average time by a factor $\sqrt{0.99}$ for $k \geq 24$ and $n \geq 3k + k\ln k$. **2.** We can replace in Theorems 1 and 2 the constant 6 by an arbitrary $\delta < 12$ since $\frac{q^k}{1-q} = \frac{\delta}{\ln(k/\delta)} + O(\delta^3 k^{-2}\ln k)$ holds for $q^k = \frac{\delta}{k}$ and $k \to \infty$, due to [K72, p.107 (14)].

k	q^k	*apfa*	u	time
48	$8/k$	1.017^n	32	$n^2\,2^{32}$
40	$8/k$	1.020^n	24	$n^2\,2^{24}$
30	$7/k$	1.024^n	17	$n^2\,2^{17}$
24	$6/k$	1.029^n	13	$n^2\,2^{13}$

Table 2. SHORT performance according to Theorem 1

A comparison with previous methods illustrates the dramatic progress through random sampling: For $k = 24$ $2k$-reduction [S87] achieves *apfa* 1.09^n, Koy's primal-dual reduction achieves *apfa* 1.06^n in $\gg n^2 2^{13}$ time.

Practical Experiments. Consider a basis of dimension 160 consisting of integers of bit length 100, generated according to the GGH-cryptosystem [GGH97]. We reduce this basis in polynomial time by segment–LLL reduction [KS01] and primal–dual segment LLL with segment size 36 [K00]. This takes about 50 minutes and yields a basis with *apfa* about 8.25 and quotient $q \approx 0.946$.

Then a single final enumeration of 2^{12} lattice vectors via SA reduced the length of the shortest found lattice vector by 9%. This took just about one minute. The mean value of the μ_i^2 over the 2^{12} enumerated vectors for $i = 1, ..., 144$ (resp., for $i = 145, ..., 159$) was 0.083344 (resp. 0.3637) while the theoretic mean values under RA is $1/12 = 0.08\overline{3}$ (resp. $1/3 = 0.\overline{3}$). The discrepancy of the observed mean values of μ_i^2 from the distribution under RA is smaller for small i because the coefficient μ_i gets updated $(n-i)$-times within SA. The initial quotients q_i of primal–dual reduced basis are sligthly larger than q. This

increases the observed mean value of $\|b\|^2/\|b_1\|^2$ for the b produced by SA a bit against the theoretic mean value under RA, GSA.

The observed 9% length reduction via 2^{12} sampled vectors is close to the value predicted under RA and GSA by our refined analysis. All experiments have been done on a 1700 MHz, 512 MB RAM PC using the software packages of NTL 5.1 and GMP 4.0.1.

Refined Analysis of SHORT. The inequalities (2) are sufficient but not necessary to ensure that $\mathbf{E}[\sum_{i=1}^{k} \mu_i^2 \|\widehat{b}_i\|^2] \leq \frac{1}{12} k q^{k-1}$ holds under RA and GSA. SA achieves the $\frac{1}{12} k q^{k-1}$–upper bound with a better probability than $q^{\binom{k}{2}/2}$. In the refined analysis we liberalize the Inequalities (2) by allowing a few larger coefficients $|\mu_i| > \frac{1}{2} q^{(k-i)/2}$ for $1 \leq i < k$ that are balanced by smaller $|\mu_i| < \frac{1}{2} q^{(k-i)/2}$ so that again $\sum_{i=1}^{k} \mu_i^2 \|\widehat{b}_i\|^2 \leq \frac{1}{12} k\, q^{k-1}$.

3 Sampling Reduction

ESHORT is an extension of SHORT that samples 2^u vectors $b = \sum_{i=1}^{n} \mu_i \widehat{b}_i$ by SA and determines the pair (b, j) for which $\sum_{i=j}^{n} \mu_i^2 \|\widehat{b}_i\|^2 < 0.99\, \|\widehat{b}_j\|^2$ holds for the smallest possible $j \leq 10$. (The heuristic bound $j \leq 10$ covers the case that the basis vectors $b_1, ..., b_{10}$ have bad GSA-behaviour, which happens quite often, so that SA cannot succeed for the very first j.)

Sampling Reduction

This algorithm reduces a given basis $b_1, ..., b_n$ under GSA *and* RA.

1. Search via ESHORT a pair (b, j) so that $\|\pi_j(b)\|^2 < 0.99\, \|\widehat{b}_j\|^2$, $j \leq 10$, and terminate if the search fails. Form the new basis $b_1, \ldots, b_{j-1}, b, b_j, \ldots, b_{n-1}$.

2. BKZ–reduce the new basis $b_1, \ldots, b_{j-1}, b, b_j, \ldots, b_{n-1}$ with block size 20 and go to **1**.

Practical Experiments. With the above method C. Tobias has reconstructed the secret GGH-basis of the GGH-cryptosystem [GGH97] in dimension $n = 160$ and $n = 180$. This has been done by plain lattice reduction without improving the GGH-lattice by algebraic transforms as has been done by Nguyen [N99]. The secret GGH–basis was reconstructed in 40 – 80 minutes for dimension $n = 160$ within 4 iterations, and in about 9 hours for $n = 180$ using 20 iterations. This was not possible by previous lattice reduction algorithms. 2^{12} to 2^{17} vectors have been sampled per iteration. BKZ–reduction was done by the BKZ–algorithm of NTL for block size 20. Usually ESHORT succeeds with $j \leq 10$.

Interestingly, BKZ–reduction of the new basis $b_1, \ldots, b_{j-1}, b, b_j, \ldots, b_{n-1}$ triggers sporadic big jumps of progress. Typically the length of the shortest vector is decreased by a factor 1.2 – 1.5 but occasionally by a factor up to 9. Sometimes the shortest lattice vector was found at an early stage. All experiments have been done on a 1700 MHz, 512 MB RAM PC using the software packages of NTL 5.1 and GMP 4.0.1.

What triggers the big jumps during BKZ*–reduction* ? When ESHORT finds a pair (b, j), so that $\sum_{i=j}^{n} \mu_i^2 \|\widehat{b}_i\|^2 < 0.99\, \|\widehat{b}_j\|^2$, usually $\mu_j, \ldots, \mu_{j+k-1}$ are par-

ticularly small, the subsequent basis $b_1, \ldots, b_{j-1}, b, b_{j+1}, \ldots, b_{n-1}$ has large orthogonal vectors $\widehat{b}_{j+1}, \ldots, \widehat{b}_{j+k-1}$ and badly deviates from the GSA–property in the segment $\widehat{b}_{j+1}, ..., \widehat{b}_{j+k-1}$ following b. The lengths $\|\widehat{b}_{j+i}\|$ oscillate heavily up and down with some large values. Bad GSA–behavior of that type obstructs the SHORT algorithm but triggers big jumps of progress within BKZ–reduction because BKZ–reduction closely approximates the GSA. While BKZ–reduction with block size 20 does not improve a GSA–basis, it greatly improves a basis with bad GSA–behavior.

The big jumps of progress markedly differ from the usual BKZ–reduction of LLL–reduced bases. The latter advances in a slow steady progress. It generates intermediate bases where the lengths $\|\widehat{b}_i\|$ gradually decrease in i with only little fluctuation.

4 General Birthday Sampling

The birthday heuristic is a well known method that given a list of m bit integers, drawn uniformly at random, finds a collision of the given integers in $O(2^{m/2})$ average time. The method can easily be extended to find two random k-bit integers having a small difference, less than 2^{k-m}, $O(2^{m/2})$ time. We extend the birthday method from integers to lattice vectors, we extend random sampling to birthday sampling. Let $\mathbf{Q}$ denote the set of rational numbers, let $m, t \geq 1$ be integers.

Wagner's $(2^t, m)$*-list algorithm* [W02] extends the birthday method to solve the following $(2^t, m)$*-sum problem*. Given 2^t lists $L_1, \ldots, L_{2^t}$ of elements drawn uniformly and independently at random from $\{0,1\}^m$ find $x_1 \in L_1, \ldots, x_{2^t} \in L_{2^t}$ such that $x_1 \oplus x_2 \oplus \cdots \oplus x_{2^t} = 0$. Wagner's algorithm solves the $(2^t, m)$-sum problem in $O(2^t\, 2^{m/(1+t)})$ average time and space by a tree-like birthday method. The $(4, m)$-list algorithm runs in $O(2^{m/3})$ time and space, and coincides with a previous algorithm of Camion, Patarin [CP91]. The *simple* case $t = 1$ is the well known birthday method. Consider the following *small sum problem* (SSP):

$(2^t, m)$-SSP. Given 2^t lists $L_1, \ldots, L_{2^t}$ of rational numbers drawn uniformly and independently at random from $[-\frac{1}{2}, \frac{1}{2}] \cap \mathbf{Q}$ find $x_1 \in L_1, \ldots, x_{2^t} \in L_{2^t}$ such that $|\sum_{i=1}^{2^t} x_i| \leq \frac{1}{2}\, 2^{-m}$.

We extend Wagner's $(2^t, m)$-list algorithm to solve the $(2^t, m)$-SSP. We outline the case $t = 2$ solving the $(4, m)$-SSP in $O(2^{m/3})$ average time. We count for steps additions and comparisons using rational numbers. Let the lists $L_1, \ldots, L_4$ each consist of $\frac{4}{3}\, 2^{m/3}$ random elements drawn uniformly from $[-\frac{1}{2}, \frac{1}{2}] \cap \mathbf{Q}$. Consider the lists

$$L'_1 := \{x_1 + x_2 \mid |x_1 + x_2| \leq \tfrac{1}{2}\, 2^{-m/3}\}, \quad L'_2 := \{x_3 + x_4 \mid |x_3 + x_4| \leq \tfrac{1}{2}\, 2^{-m/3}\}$$
$$L := \{x'_1 + x'_2 \mid |x'_1 + x'_2| \leq \tfrac{1}{2}\, 2^{-m}\},$$

where x_i ranges over L_i and x'_i over L'_i. (We also record the source pair (x_1, x_2) of $x'_i = x_1 + x_2 \in L'_1$.) Applying the subsequent Lemma 3 with $\alpha = 2^{-m/3}$ we have that $\mathbf{Pr}[\, |x_1 + x_2| \leq \frac{1}{2}\, 2^{-m}\,] \geq 2^{-m/3}\, \frac{3}{4}$. The average size of L'_1 (and likewise for L'_2) is : $|L'_1| \geq |L_1| \cdot |L_2| \cdot 2^{-m/3}\, \frac{3}{4} = \frac{4}{3}\, 2^{m/3}$.

Similarly, we have for $x'_i \in L'_i$ and $\alpha = 2^{-2m/3}$ that $\mathbf{Pr}[\,|x'_1 + x'_2| \le \frac{1}{2}\,2^{-m}\,] \ge 2^{-2m/3}\,\frac{3}{4}$, and thus the average size of L is $|L| \ge |L'_1| \cdot |L'_2| \cdot 2^{-2m/3}\,\frac{3}{4} = \frac{4}{3}$.

To construct L'_1 (and likewise L'_2, L) we sort the $x_1 \in L_1$ and the $-x_2 \in -L_2$ according to the numerical values of $x_1, -x_2 \in [-\frac{1}{2}, \frac{1}{2}]$ and we search for close elements $x_1, -x_2$. The sorting and searching is done by bucket sort in $O(2^{m/3})$ average time and space: we partition $[-\frac{1}{2}, \frac{1}{2}]$ into intervals of length $\frac{1}{2}\,2^{-m/3}$, we distribute $x_1, -x_2$ to these intervals and we search for pairs $x_1, -x_2$ that fall into the same interval. This solves the $(4, m)$-SSP in $O(\frac{4}{3}\,2^{m/3})$ average time and space. More generally the $(2^t, m)$-SSP is solved in $O(2^t\,\frac{4}{3}\,2^{\frac{m}{t+1}})$ average time and space.

Lemma 3. *Let $x_i \in_R [-\frac{1}{2}, \frac{1}{2}]$ for $i = 1, 2$ be uniformly distributed and statistically independent. Then $\mathbf{Pr}[\,|x_1 + x_2| \le \alpha/2\,] = \alpha\,(1 - \frac{\alpha}{4})$ holds for $0 \le \alpha \le 2$.*

Proof. For given $|x_1| \le \frac{1-\alpha}{2}$ the interval of all $x_2 \in [-\frac{1}{2}, \frac{1}{2}]$ satisfying $|x_1 + x_2| \le \alpha/2$ has length α. For $|x_1| \ge \frac{1-\alpha}{2}$ the corresponding interval length is $\alpha - y$, where the value $y := |x_1| - \frac{1-\alpha}{2}$ ranges over $[0, \alpha/2]$. Therefore

$$\mathbf{Pr}[\,|x_1 + x_2| \le \alpha/2\,] = \alpha - 2\int_0^{\alpha/2} y\ \mathrm{dy} = \alpha - \tfrac{1}{4}\,\alpha^2. \qquad \square$$

We extend our method from rational numbers in $[-\frac{1}{2}, \frac{1}{2}]$ to vectors in $\mathbf{Q}^k \cap [-\frac{1}{2}, \frac{1}{2}]^k$. We solve the following *small vector sum problem* $(2^t, m, k)$-VSSP in $O(k\,2^t\,(\frac{4}{3})^k\,2^{\frac{m}{t+1}})$ average time and space (in $O(k\,(\frac{4}{3})^{k/2}\,2^{m/2})$ time for $t = 1$):

$(\mathbf{2^t, m, k})$-VSSP. Let an arbitrary partition $m = m_1 + \cdots + m_k$ be given with real numbers $m_1, \ldots, m_k \ge 0$. Given 2^t lists $L_1, \ldots, L_{2^t}$ of rational vectors drawn uniformly and independently from $[-\frac{1}{2}, \frac{1}{2}]^k \cap \mathbf{Q}^k$ find $\boldsymbol{x}_1 \in L_1, ..., \boldsymbol{x}_{2^t} \in L_{2^t}$, $\boldsymbol{x}_i = (x_{i,1}, \ldots, x_{i,k}) \in \mathbf{Q}^k$, such that $|\sum_{i=1}^{2^t} x_{i,j}| \le \frac{1}{2}\,2^{-m_j}$ for $j = 1, \ldots, k$.

We extend the $(4, m)$-SSP solution to $(4, m, k)$-VSSP. Let each list L_i consist of $(\frac{4}{3})^k\,2^{m/3}$ random vectors of $[-\frac{1}{2}, \frac{1}{2}]^k$ for $i = 1, ..., 4$. Consider the lists

$$\begin{aligned} L'_1 &:= \{x_1 + x_2 \mid |x_{1,j} + x_{2,j}| \le \tfrac{1}{2}\,2^{-m_j/3} \text{ for } j = 1, ..., k\} \\ L'_2 &:= \{x_3 + x_4 \mid |x_{3,j} + x_{4,j}| \le \tfrac{1}{2}\,2^{-m_j/3} \text{ for } j = 1, ..., k\} \\ L &:= \{x'_1 + x'_2 \mid |x'_{1,j} + x'_{2,j}| \le \tfrac{1}{2}\,2^{-m_j} \quad \text{for } j = 1, ..., k\}, \end{aligned}$$

where x_i ranges over L_i and x'_i ranges over L'_i. Then $|L'_2| = |L'_1| \ge |L_1| \cdot |L_2| \cdot 2^{-m/3}\,(\frac{3}{4})^k = (\frac{4}{3})^k\,2^{m/3}$, and $|L| \ge |L'_1| \cdot |L'_2| \cdot 2^{-2m/3}\,(\frac{3}{4})^k = (\frac{4}{3})^k$ holds for the average list sizes. (For $t = 1$ we only need input lists L_i consisting of $(\frac{4}{3})^{k/2}\,2^{m/2}$ vectors to succeed with $|L| \ge 1$.)

General Birthday Sampling (GBS). Given a lattice basis $b_1, ..., b_n$ and 2^t lists $\bar{L}_1, ..., \bar{L}_{2^t}$ of lattice vectors sampled by SA, GBS produces a short vector $b = \sum_{i=1}^{2^t} \bar{b}_i$ with $\bar{b}_i \in \bar{L}_i$ by solving the $(2^t, m, k)$-VSSP for the coefficient vectors $(\bar{\mu}_{1,i}, ..., \bar{\mu}_{k,i}) \in \mathbf{Q}^k \cap [-\frac{1}{2}, \frac{1}{2}]^k$ of $\bar{b}_i = \sum_{\ell=1}^{n} \bar{\mu}_{\ell,i}\,\widehat{b}_\ell \in \bar{L}_i$ for a suitable m.

Theorem 2. *Given $t \geq 1$ and a lattice basis $b_1, ..., b_n$ with quotient $q \leq (\frac{6}{k})^{1/k}$* GBS *finds under* GSA *and* RA*, for sufficiently large k and n, a lattice vector $b \neq 0$, $\|b\|^2 < 0.99\,\|b_1\|^2$ in $O(n^2\,2^t\,(\frac{4}{3})^{2k/3}\,q^{-k^2/4(t+1)})$ average time and space.*

Proof. We replace SA in the proof of Theorem 1 by GBS. Initially GBS forms 2^t lists $\bar{L}_i$, each of of $2^{m/(t+1)}$ lattice vectors $\bar{b}_i \in \bar{L}_i$ sampled by SA for $1 \leq i \leq 2^t$. GBS produces a short lattice vector $b = \sum_i \bar{b}_i$ via a solution of the $(2^t, m, k)$-VSSP for the coefficient vectors $(\bar{\mu}_{1,i}, \ldots, \bar{\mu}_{k,i}) \in \mathbf{Q}^k \cap [-\frac{1}{2}, \frac{1}{2}]^k$ of $\bar{b}_i = \sum_{j=1}^n \bar{\mu}_{j,i}\,\widehat{b}_j \in \bar{L}_i$. Here let $m := m_1 + \cdots + m_k$ for $m_j := \log_2 q^{(-k+j)/2}$, and thus $m = -\binom{k}{2}\frac{1}{2}\log_2 q$. Under GSA and RA the $(2^t, m, k)$-VSSP solution provides a lattice vector $b = \sum_{j=1}^n \mu_j\,\widehat{b}_j$ such that $|\mu_j| \leq \frac{1}{2}\,q^{(k-j)/2}$ for $j = 1, \ldots, k$ and $\mathbf{E}[\mu_j^2] = \frac{2^t}{12}$ (resp., $\frac{2^t}{3}$) holds for $j = k+1, ..., n-u-1$ (resp., for $j \geq n-u$).

Let k be so large that $q^k \leq \frac{6}{k}$. For $q^k = \frac{6}{k}$, $n \geq 3k + u + 1$ we see that

$$\mathbf{E}[\,\textstyle\sum_{j=1}^k \mu_j^2\,\|\widehat{b}_j\|^2/\|b_1\|^2] \leq \frac{1}{12}\sum_{j=1}^k q^{k-j}\,q^{j-1} = \frac{k}{12}\,q^{k-1},$$

$$\mathbf{E}[\,\textstyle\sum_{j=k+1}^n \mu_j^2\,\|\widehat{b}_j\|^2/\|b_1\|^2] \leq \frac{2^t}{12}\,\frac{q^k+3q^{3k}}{1-q},$$

$$\mathbf{E}[\,\|b\|^2/\|b_1\|^2\,] \;\leq\; \frac{1}{2q} + \frac{2^t}{12}\,\frac{q^k+3q^{3k}}{1-q} \;< 0.99$$

holds for sufficiently large k, $k \geq e^{2^t(1+o(1))}$.

In this application our $(2^t, m, k)$-VSSP algorithm runs in $k\,2^t\,(\frac{4}{3})^{2k/3}\,2^{\frac{m}{t+1}}$ time, and even in $2k\,(\frac{4}{3})^{k/3}\,2^{m/2}$ time for $t = 1$. (We use Lemma 3 with the α-values $q^{i/2}$ for $i = 0, ..., k-1$ and the inequality $\prod_{i=0}^{k-1}(1 - q^{i/2}/4) \geq (\frac{3}{4})^{2k/3}$.) Hence, GBS runs in $O(n^2\,2^t\,(\frac{4}{3})^{2k/3}\,2^{\frac{m}{t+1}})$ average time where $m = -\binom{k}{2}\frac{1}{2}\log_2 q$. This yields the claimed time bound. □

Simple GBS for $t = 1$ runs in $O(n^2\,(\frac{4}{3})^{k/3}\,q^{-k^2/8})$ average time. Compared to Theorem 1 it reduces the *apfa* achievable in a given time to its square root, but requires massive space. Iteration of simple GBS via BKZ–reduction achieves in $O(n^3\,(\frac{4}{3})^{k/3}\,q^{-k^2/8})$ average time *apfa* $q^{-n/2}$ for $q \leq (\frac{6}{k})^{1/k}$, $k \geq 60$.

Conclusion. Theorem 1 shows that the new method greatly improves the known algorithms for finding very short lattice vectors. This lowers the security of all lattice based cryptographic schemes. Simple birthday sampling may further decrease that security but its practicability hinges on the required space.

Acknowledgement. I am indepted to C. Tobias for carrying out the practical experiments reported in this paper and for providing Figure 1.

References

[A98] *M. Ajtai*, The shortest vector problem in L_2 is NP-hard for randomised reductions. Proc. 30th STOC, pp. 10–19, 1998.

[A02] *M. Ajtai*, The worst-case behaviour of Schnorr's algorithm approximating the shortest nonzero vector in a lattice. Preprint 2002.

[AKS01] *M. Ajtai, R. Kumar, and D. Sivakumar*, A sieve algorithm for the shortest lattice vector problem. Proc. 33th STOC, 2001.

[CP91] *P. Camion, and J. Patarin*, The knapsack hash function proposed at Crypto'89 can be broken.Proc. Eurocrypt'91, LNCS 457, Springer-Verlag, pp. 39–53, 1991.

[E81] *P. van Emde Boas*, Another NP-complete partition problem and the complexity of computing short vectors in a lattice. Mathematics Department, University of Amsterdam, TR 81-04, 1981.

[GGH97] *O. Goldreich, S. Goldwasser, and S. Halevi*, Public key cryptosystems from lattice reduction problems. Proc. Crypto'97, LNCS 1294, Springer-Verlag, pp. 112–131, 1997.

[H85] *B. Helfrich*, Algorithms to construct Minkowski reduced and Hermite reduced bases. *Theor. Comp. Sc.* **41**, pp. 125–139, 1985.

[K83] *R. Kannan*, Minkowski's convex body theorem and integer programming. *Mathematics of Operations Research* **12** pp. 415–440, 1987, Preliminary version in Proc. 13th STOC, 1983.

[K72] *D. E. Knuth*, The Art of Computer Programming, Vol 1, Fundamental Algorithms. 3rd Edidtion, Addison-Wesley, Reading, 1997.

[KS02] *H. Koy and C.P. Schnorr*, Segment and strong Segment LLL-reduction of lattice bases. Preprint University Frankfurt, 2002, http: //www.mi.informatik.uni-frankfurt.de/research/papers.html

[KS01a] *H. Koy and C.P. Schnorr*, Segment LLL-reduction of lattice bases. Proc. CaLC 2001, LNCS 2146, Springer-Verlag, pp. 67–80, 2001.

[K00] *H. Koy*, Primale/duale Segment-Reduktion von Gitterbasen. Slides of a lecture, Frankfurt, December 2000.

[KS01b] *H. Koy and C.P. Schnorr*, Segment LLL-reduction of lattice bases with floating point orthogonalization. Proc. CaLC 2001, LNCS 2146, Springer-Verlag, pp. 81–96, 2001.

[LLL82] *A. K. Lenstra, H. W. Lenstra, and L. Lovász*, Factoring polynomials with rational coefficients. *Math. Ann.* **261**, pp. 515–534, 1982.

[M98] *D. Micciancio*, The shortest vector in a lattice is NP-hard to approximate to within some constant. Proc. 39th Symp. FOCS, pp. 92–98, 1998, full paper SIAM Journal on Computing, 30 (6), pp. 2008-2035, March 2001.

[N99] *P.Q. Nguyen*, Cryptanalysis of the Goldreich-Goldwasser-Halevi Cryptosystem from Crypto'97. Proc. Crypto'99, LNCS 1666, Springer-Verlag, pp. 288–304, 1999.

[NS00] *P.Q. Nguyen and J. Stern*, Lattice reduction in cryptology: an update. Proc. ANTS-IV, LNCS 1838, Springer-Verlag, pp. 188–112. full version http://www.di.ens.fr/ pnguyen,stern/

[NTL] *V. Shoup*, Number Theory Library. http: //www.shoup.net/ntl

[S87] *C.P. Schnorr*, A hierarchy of polynomial time lattice basis reduction algorithms. *Theor. Comp. Sc.* **53**, pp. 201–224, 1987.

[S88] *C.P. Schnorr*, A more efficient algorithm for lattice reduction. *J. of Algor.* **9**, 47–62, 1988.

[SE91] *C.P. Schnorr and M. Euchner*, Lattice Basis Reduction and Solving Subset Sum Problems. Fundamentals of Comput. Theory, Lecture Notes in Comput. Sci., 591, Springer, New York, 1991, pp. 68–85. The complete paper appeared in Math. Programming Studies, 66A, 2, pp. 181–199, 1994.

[W02] *D. Wagner*, A Generalized Birthday Problem. Proceedings Crypto'02, LNCS 2442, Springer-Verlag, pp. 288–303, 2002. full version http://www.cs.berkeley.edu/ daw/papers/