Looking back at lattice-based cryptanalysis

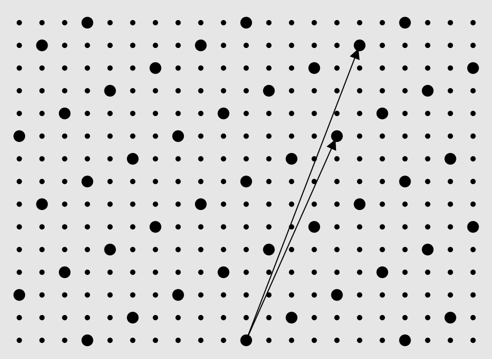
Antoine Joux

Fields Institute, May 2009

Lattices

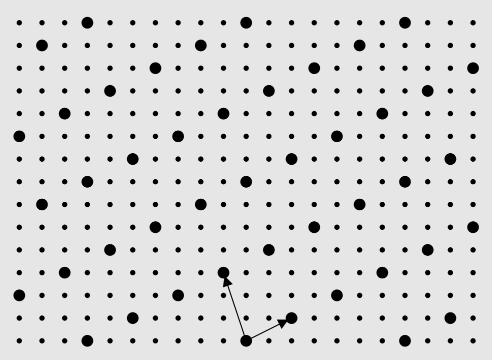
- A lattice is a discrete subgroup of $\mathbb{R}^n$
- Equivalently, set of integral linear combinations:

$$\alpha_1 \vec{b_1} + \cdots + \alpha_n \vec{b}_m \quad \text{with } m \leq n$$



Lattices reduction

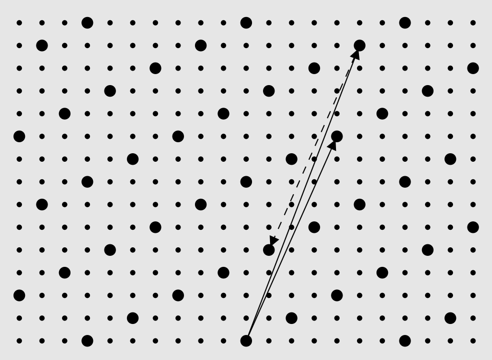
- Lattice reduction looks for a “good” basis
- Easy to view in dimension 2



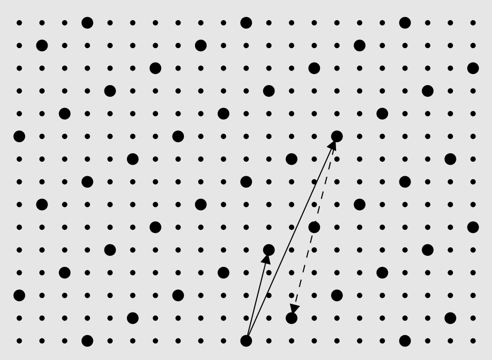
Gauss's reduction algorithm

Require: Initial lattice basis $(\vec{u}, \vec{v})$
if $\|\vec{u}\| < \|\vec{v}\|$ **then**
Exchange $\vec{u}$ and $\vec{v}$
end if
repeat
Minimize $\|\vec{u} - \lambda\vec{v}\|$, i.e., $\lambda \longleftarrow \left\lfloor (\vec{u}|\vec{v})/\|\vec{v}\|^2 \right\rceil$
Let $\vec{u} \longleftarrow \vec{u} - \lambda\vec{v}$
Swap $\vec{u}$ and $\vec{v}$
until $\|u\| \leq \|v\|$
Output $(\vec{u}, \vec{v})$ as reduced basis

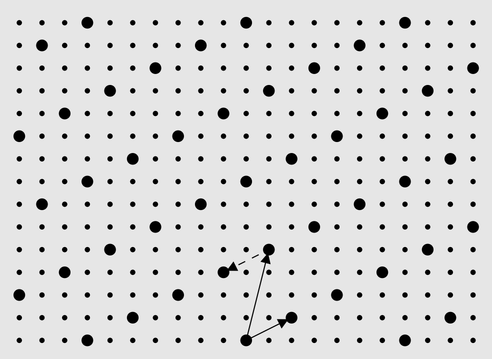
Gauss's reduction algorithm



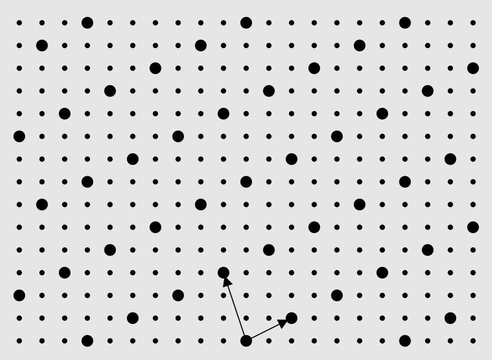
Gauss's reduction algorithm



Gauss's reduction algorithm



Gauss's reduction algorithm



A useful tool: Gram-Schmidt orthogonalization

- Create $(\vec{b_1}^*, \cdots, \vec{b}_m^*)$ such that:
  - $\vec{b}_1^* = \vec{b}_1$,
  - $\vec{b}_i^*$ is the projection of $\vec{b}_i$, orthogonally to previous vectors.
- Defined by the equation:

$$\vec{b}_i^* = \vec{b}_i - \sum_{j=1}^{i-1} m_{i,j} \vec{b}_j^* \quad \text{where} \quad m_{i,j} = \frac{(\vec{b}_i | \vec{b}_j^*)}{\|\vec{b}_j^*\|^2}$$

- Basis of the same vector space

- Not a lattice basis
- Useful to quantify how “orthogonal” a lattice basis is.

Lenstra-Lenstra-Lovász (1982)

- A polynomial time algorithm
- Arbitrary dimension
- Gauss's algorithm and Gram-Schmidt orthogonalization
- Enforces the following properties on the output basis:

$$\forall\, i < j \quad : \quad \left|(\vec{b}_j|\vec{b}_i^*)\right| \le \frac{\|\vec{b}_i^*\|^2}{2}$$

$$\forall\, i \quad : \quad \delta\|\vec{b}_i^*\|^2 \le \left(\|\vec{b}_{i+1}^*\|^2 + \frac{(\vec{b}_{i+1}|\vec{b}_i^*)^2}{\|b_i^*\|^2}\right)$$

- Implies (note: $1/4 < \delta \le 1$):

$$(\delta - 1/4)\,\|\vec{b}_i^*\|^2 \le \|\vec{b}_{i+1}^*\|^2$$

Key properties of LLL-reduced basis

- First vector is "quite short"

$$\begin{aligned} \lambda_1 &\geq \left(\delta - \frac{1}{4}\right)^{(n-1)/2} \|\vec{b}_1\| \\ \det(L) &\geq \left(\delta - \frac{1}{4}\right)^{n(n-1)/4} \|\vec{b}_1\|^n \end{aligned}$$

- Often used with $\delta = 3/4$:

$$\begin{aligned} \|\vec{b}_1\| &\leq 2^{(n-1)/2}\,\lambda_1 \\ \|\vec{b}_1\| &\leq 2^{(n-1)/4}\,\det(L)^{1/n} \end{aligned}$$

Key properties of LLL-reduced basis

- Last vector is "quite orthogonal" to previous ones

$$\|\vec{b}_n^*\| \geq \left(\delta - \frac{1}{4}\right)^{(n-i)/2} \|\vec{b}_i^*\|$$
$$\|\vec{b}_n^*\|^n \geq \left(\delta - \frac{1}{4}\right)^{n(n-1)/4} \det(L)$$

- In particular, with $\delta = 3/4$:

$$\|\vec{b}_n^*\| \geq \frac{\|\vec{b}_1\|}{2^{(n-1)/2}}$$
$$\|\vec{b}_n^*\| \geq \frac{\det(L)^{1/n}}{2^{(n-1)/4}}$$

Knapsacks

- The subset-sum problem (or knapsack problem) is:
  - Given integers $a_1, \ldots, a_n$ and S
  - Find $\epsilon_1, \ldots, \epsilon_n$ with $0/1$ values such that:

$$S = \sum_{i=1}^{n} \epsilon_i a_i$$

- NP-hard problem
- Some cases are easy (e.g. $a_i = 2^{i-1}$)

Knapsack-based cryptosystems

- Main idea: Hide an easy knapsack in a hard-looking one
- Example: Merkle-Hellman cryptosystem
  - Start from super-increasing knapsack where $a_i > \sum_{j=1}^{i-1} a_j$
  - Choose $q > \sum_{i=1}^{n} a_i$ (prime for simplicity)
  - Choose r a random integer modulo q
  - Form new knapsack with $b_i = r a_{\pi(i)} \pmod{q}$
  - **Encryption:** Compute $S = \sum_{i=1}^{n} \epsilon_i b_i$
  - **Decryption:** Let $S_a = S\, r^{-1} \pmod{q}$ and solve easy knapsack
- Broken by Shamir at Crypto'82

Sketch of Shamir's attack

- Assume π is identity (or guess $\pi(1)$, $\pi(2)$, $\pi(3)$, $\pi(4)$)
- For simplicity, assume that b_1 and b_2 are coprime
- Let $c_3 = b_3/b_2 \pmod{b_1}$ and $c_4 = b_4/b_2 \pmod{b_1}$
- Form lattice (spanned by rows) :

$$\begin{pmatrix} 1 & c_3 & c_4 \\ 0 & b_1 & 0 \\ 0 & 0 & b_1 \end{pmatrix}$$

- Contains all vectors $(\lambda b_2, \lambda b_3, \lambda b_4)$ modulo b_1
- Remark that $a_1 b_i - a_i b_1 = u_i q$ and u_i small
- Yields short vector (u_2, u_3, u_4)

Sketch of Shamir's attack (continued)

- In particular: $a_1/q = u_i/b_i \pmod{b_1}$
- Let $\mu = u_i/b_i \pmod{b_1}$
- We can now decrypt with (mostly) equivalent key (μ, b_1)

Another approach to break Merkle-Hellman knapsack

- Since a_i is super-increasing, a_n has $2n$ bits
- So does q and all b_is
- Define density of a knapsack:

$$d = \frac{n}{\log_2(\max_i a_i)}$$

- As a general rule:

Low density $\Rightarrow$ Easy to solve

Basic low-density attack

- Consider the lattice generated by columns of:

$$\begin{pmatrix} Ka_1 & Ka_2 & \cdots & Ka_n & Ks \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix}$$

- With K large enough
  - LLL outputs short vector with 0 on the first line
- Short relation $\sum_{i=1}^{n} v_i a_i = s$

Is it the correct $\{0, 1\}$ solution?

Basic low-density attack

- Lagarias-Odlyzko (1985)
- Correct solution when $d < 0.6463$
- Assuming a shortest lattice vector oracle
- Surprisingly:

Works well in practice!

- With LLL bounds, would need $d < O(1)/n$

Improved low-density attacks

- Consider the lattice generated by columns of:

$$\begin{pmatrix} Ka_1 & Ka_2 & \cdots & Ka_n & Ks \\ 1 & 0 & \cdots & 0 & 1/2 \\ 0 & 1 & \cdots & 0 & 1/2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 1/2 \end{pmatrix}$$

- Improved bound $d < 0.9408$

Improved low-density attacks

- Alternative lattice:

$$\begin{pmatrix} Ka_1 & Ka_2 & \cdots & Ka_n & -Ks \\ n+1 & -1 & \cdots & -1 & -1 \\ -1 & n+1 & \cdots & -1 & -1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ -1 & -1 & \cdots & n+1 & -1 \\ -1 & -1 & \cdots & -1 & n+1 \end{pmatrix}$$

- Same bound $d < 0.9408$
- Useful when number of 0s and 1s is unbalanced

A note of caution

- Despite these early success:
  - Lattice-reduction is hard
  - Some cryptosystems even rely on this hardness
- In practice: Lattice-reduction works very well in moderate dimension
- In higher dimension, many problems appear:
  - Exponential gap between $\vec{b_1}$ and first minimum
  - Unstability problems
  - Running time and performance greatly depend on considered lattice

Would be nice to have attacks without oracles.

Knuth's truncated linear congruential generator

- A classical pseudo-random generator defined from sequence:

$$x_{i+1} = a\,x_i + b \pmod{q}$$

  for simplicity, assume that q is prime.
- Write x_i in binary as $y_i \| z_i$
- Output y_i (α-fraction of $k = \log_2 q$)
- Many attacks: most general by Stern (1987)
  - Improved by Contini and Shparlinski

Sketch of attack

- First remark that:

$$x_{i+1} - x_i = a^i\,(x_1 - x_0) \pmod{q}.$$

- If:

$$\sum_{i=0}^{d} \alpha_i (x_{i+1} - x_i) = 0$$

then, assuming $x_2 - x_1 \neq 0 \pmod{q}$, the polynomial

$$P(z) = \sum_{i=0}^{d} \alpha_i z^i$$

has a as a root modulo q.

Sketch of attack

- Given two such polynomials P_1 and P_2:

$$q \mid \mathrm{Res}(P_1, P_2).$$

- With three polynomials, take GCD of resultants.
- It remains to construct such polynomials.

Sketch of attack: Stern's construction of polynomials

- First build vectors:

$$Y_i = \begin{pmatrix} y_{i+1} - y_i \\ y_{i+2} - y_{i+1} \\ \vdots \\ y_{i+t} - y_{i+t-1} \end{pmatrix}$$

  we also use notation X_i and Z_i
- Search for a short zero linear combination:

$$\sum_{i=1}^{n} \alpha_i Y_i = 0.$$

- Relations exist with $|\alpha_i| \leq B$ with $B = 2^{t(\alpha k + \log n + 1)/(n-t)}$

Sketch of attack: Stern's construction of polynomials

- Classical use of lattice reduction:

$$\begin{pmatrix} KY_1 & KY_2 & \cdots & KY_n \\ 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$$

- With LLL and $K = \lceil \sqrt{n} 2^{(n-1)/2} B \rceil$, relation satisfies:

$$\sum_{i=1}^{n} \alpha_i^2 \leq K^2$$

Sketch of attack: Stern's construction of polynomials

- Since $\sum_{i=1}^{n} \alpha_i Y_i = 0$, we have:

$$\sum_{i=1}^{n} \alpha_i X_i = \sum_{i=1}^{n} \alpha_i Z_i$$

- Thus, $\sum_{i=1}^{n} \alpha_i X_i$ is small. It is also belongs to the lattice:

$$\begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ a & q & 0 & \cdots & 0 \\ a^2 & 0 & q & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a^{t-1} & 0 & 0 & \cdots & q \end{pmatrix}$$

- No small non-zero vector in this lattice

Sketch of attack: Stern's construction of polynomials

- Thus:

$$\sum_{i=1}^{n} \alpha_i X_i = 0$$

- As a consequence, the polynomial:

$$\sum_{i=1}^{n} \alpha_i \, z^{i-1} = 0$$

admits a as a root modulo q.

Coppersmith's small root algorithms

- Modular version, solve polynomial equation:

$$f(x) = 0 \pmod{N}.$$

Easy when factorization of N is known. Hard in general.

- Bivariate version, find integral roots of:

$$f(x, y) = 0.$$

Diophantine equations. Hard in general.

Variant (for simplified analysis)

- Search rational solutions
- Equivalently, consider homogeneous polynomials
- Modular version, solve polynomial equation:

$$f(x_0, x_1) = 0 \pmod{N}.$$

- Bivariate version, find integral roots of:

$$f(x_0, x_1, y_0, y_1) = 0.$$

Homogeneous separately in x and y.

A simple case (Howgrave-Graham's variation)

- Search small solutions of:

$$f(x_0, x_1) = a\,x_0^2 + b\,x_0\,x_1 + c\,x_1^2 = 0 \pmod{N}.$$

  W.l.o.g, we may assume $c = 1$.
- Fix two parameters, D and t
- Consider homogeneous polynomials of degree D with root (x_0, x_1) modulo N^t
- Obtained by linearly combining:

$$x_0^{D-2i}\,f(x_0, x_1)^i\,N^{\max(0,t-i)} \quad \text{and}$$
$$x_0^{D-2i-1}\,x_1\,f(x_0, x_1)^i\,N^{\max(0,t-i)}$$

A simple case

- Use monomial ordering with $x_1 > x_0$
- Head monomial in

$$x_0^{D-2i-\theta}\, x_1^{\theta}\, f(x_0, x_1)^i\, N^{\max(0,t-i)}$$

is $x_1^{2i+\theta}\, x_0^{D-2i-\theta}$ and has coefficient $N^{\max(0,t-i)}$

Interpret polynomials as lattice points

$$([x_0^D], [x_0^{D-1}x_1], \cdots, [x_0 x_1^{D-1}], [x_1^D])$$

A simple case

- Dimension of the lattice $D+1$
- Determinant of the lattice is $N^{t(t+1)}$
- LLL produces a short vector of norm:

$$\leq \; 2^{D/4}\, N^{t(t+1)/(D+1)}$$

- If $|x_0| \leq B$ and $|x_1| \leq B$ the corresponding polynomial at (x_0, x_1) has value less than:

$$\sqrt{D+1}\, 2^{D/4}\, N^{t(t+1)/(D+1)}\, B^D$$

- With $D = 2t$ and letting $t \to \infty$, assuming $B < N^{1/4-\epsilon}$:

$$\sqrt{D+1}\, 2^{D/4}\, N^{t(t+1)/(D+1)}\, B^D < N^t$$

End of the simple case

- As a consequence, get polynomial F with $F(x_0, x_1) = 0$ over $\mathbb{Z}$
- Dehomogenizing, we find $F_a(x_0/x_1) = 0$
- Solve over $\mathbb{R}$
- Recover x_0 and x_1 from root r using continued fractions

f of degree d $\Rightarrow$ Works up to $N^{1/2d}$ bound on x_0 and x_1

A simple case: bivariate version

- Search rational solutions of $f(x, y) = 0$
- Equivalently, consider homogeneous polynomials
- Simple case, take for homogeneous f:

$$a_0\, x_0 y_0 + a_1\, x_1 y_0 + a_2\, x_0 y_1 + a_3\, x_1 y_1 = 0$$

- Assume that $a_3 > 0$ and is largest coefficient
- Consider lattice containing homogeneous multiples of f of degree D in x and y separately

A simple case: bivariate version

- Lattice spanned by polynomials:

$$x_0^i x_1^{D-1-i}\, y_0^j y_1^{D-1-j}\, f$$

- If (X_0, X_1, Y_0, Y_1) is a solution, the vector:

$$\vec{S} = (X_0^D X_1^0 Y_0^D Y_1^0, \cdots, X_0^0 X_1^D Y_0^0 Y_1^D)$$

  is orthogonal to this lattice. Its norm is at most $(D+1)\cdot B^{2D}$
- Construct orthogonal lattice
  - Dimension $(D+1)^2 - D^2 = 2D+1$
  - Determinant: $a_3^{D^2}$

A simple case: bivariate version

- LLL yields short vector of norm:

$$\leq \; 2^{D/2} \, a_3^{D^2/(2D+1)}$$

- When $B < a_3^{1/4-\epsilon}$, expect to find $\vec{S}$

How to make the attack provable ?

Bivariate version: Coppersmith's method

- LLL yields last vector $\vec{b}_{2D+1}$ with

$$\|\vec{b}^*_{2D+1}\| \geq 2^{-D/2}\, a_3^{D^2/(2D+1)}$$

- When $B < a_3^{1/4-\epsilon}$, $\vec{S}$ does not contain $\vec{b}_{2D+1}$
- And $\vec{S}$ orthogonal to $\vec{b}^*_{2D+1}$

$\Rightarrow$ New polynomial with root $(x_0/x_1, y_0/y_1)$

Small root algorithms for integral solutions

- Similar idea, but scaling factors in lattices
- For univariate degree d, modulo N, bound $B < N^{1/d}$
- For bivariate polynomials, first define $M(f)$
  - Degree d in x and y separately:
    $$B_X B_y < M(f)^{2/(3d)}$$
  - Total degree d in x and y:
    $$B_X B_y < M(f)^{1/d}$$

Some cryptographic applications

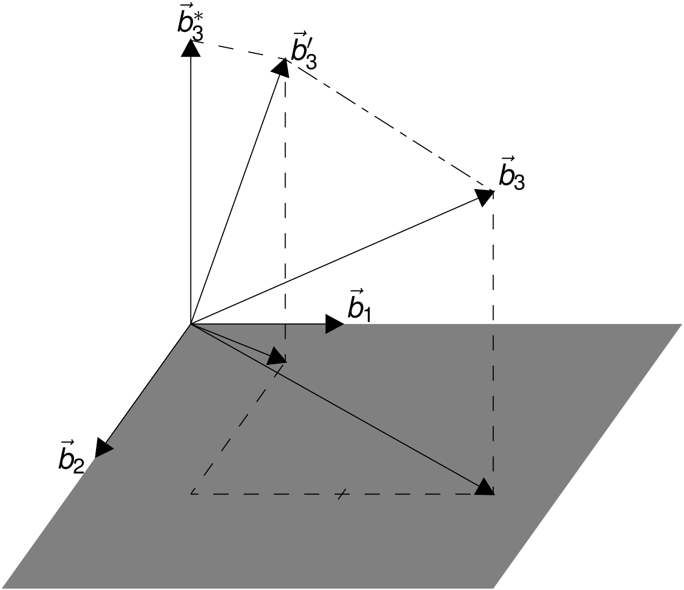
- Factoring with high bits known
- Breaking RSA with small decryption exponent $d < N^{0.292}$
- Approximate GCD (large common factor of A and $B + x$)
- Used by Shoup to prove the security of RSA-OAEP with exponent 3
- Final step of some side channel attacks

See May's survey

Conclusion

Questions ?

Lenstra-Lenstra-Lovász (1982)



Comparing the bounds

- Degree d in x and y separately
- If $M(f)$ comes from highest degree monomial, $M(f) = C\,(B_x B_y)^d$
  - Integral root, bound is: $B_x B_y < C^{2/d}$
  - Rational root, bound is: $B_x B_y < C^{1/d}$
  - I.e., as many bits.
- If $M(f)$ comes from lowest degree monomial, $M(f) = C$
  - Integral root, bound is: $B_x B_y < C^{2/(3d)}$
  - Rational root, bound is: $B_x B_y < C^{1/d}$