RSA XI

LLL, Coppersmith/Howgrave-Graham, and stereotyped messages

Tanja Lange

Eindhoven University of Technology

2MMC10 – Cryptology

LLL – Lenstra, Lenstra, and Lovász, 1982

- On input a set of vectors $\{v_1, v_2, \ldots, v_d\}$, entered as row vectors in a matrix M, output matrix with shorter vectors v_j'
so that $v_j' = \sum a_i v_i$ for some $a_i \in \mathbf{Z}$.

LLL – Lenstra, Lenstra, and Lovász, 1982

- On input a set of vectors $\{v_1, v_2, \ldots, v_d\}$, entered as row vectors in a matrix M, output matrix with shorter vectors v_j' so that $v_j' = \sum a_i v_i$ for some $a_i \in \mathbf{Z}$.
- LLL outputs d vectors which are shorter and more orthogonal. Each vector is an integer linear combination of the inputs.
- LLL uses many elements from Gram-Schmidt orthogonalization:
  - for $j = 1$ to d
  - for $i = 1$ to $j - 1$
  - $\mu_{ij} = \frac{\langle v_i^*, v_j \rangle}{\langle v_i^*, v_i^* \rangle}$
  - $v_j^* = v_j - \sum_{i=1}^{j-1} \mu_{ij} v_i^*$
- Note that the μ_{ij} are not integers, so not permitted as coefficients.
- d vectors are LLL reduced for parameter $0.25 < \delta < 1$ if
  - $|\mu_{ij}| \leq 0.5$ for all $1 \leq j < i \leq d$,
  - $(\delta - \mu_{i-1i}^2)||v_{i-1}^*||^2 \leq ||v_i^*||^2$.
- This guarantees $||v_1|| \leq (2/\sqrt{4\delta - 1})^{(d-1)/2} \det(M)^{1/d}$, where $\det(M)$ is the determinant of the matrix.

LLL algorithm (from Cohen, GTM 138, transposed)

Input: $\{v_1, v_2, \ldots, v_d\}$, $0.25 < \delta < 1$
Output: LLL reduced matrix with parameter δ

1. $k \leftarrow 2,\ k_{\max} \leftarrow 1,\ v_1^* \leftarrow v_1,\ V_1 = \langle v_1, v_1 \rangle$
2. if $k \leq k_{\max}$ go to step 3
   else $k_{\max} \leftarrow k$, $v_k^* \leftarrow v_k$, for $j = 1$ to $k - 1$
   - put $\mu_{jk} \leftarrow \langle v_j^*, v_k \rangle / V_j$ and $v_k^* \leftarrow v_k^* - \mu_{jk} v_j^*$

   $V_k = \langle v_k, v_k \rangle$
3. Execute RED$(k, k-1)$. If $(\delta - \mu_{i-1i}^2)V_{k-1} > V_k$ execute SWAP(k) and $k \leftarrow \max\{2, k-1\}$; else for $= k-2$ down to 1 execute RED(k, j) and $k \leftarrow k + 1$.
4. If $k \leq d$ go to step 2; else output basis $\{v_1, v_2, \ldots, v_d\}$.

- RED(k, j): If $|\mu_{jk}| \leq 0.5$ return; else $q \leftarrow \lfloor \mu_{jk} \rceil$, $v_k \leftarrow v_k - qv_j$, $\mu_{jk} \leftarrow \mu_{jk} - q$, for $i = 1$ to $j - 1$ put $\mu_{ik} \leftarrow \mu_{ik} - q\mu_{ij}$ and return.
- SWAP(k): Swap v_k and v_{k-1}. If $k > 2$ for $j = 1$ to $k - 2$ swap μ_{jk} and μ_{jk-1} and update all variables to match (see p.88 in Cohen)

For a nice visualization with animation see pages 61–66 of http://thijs.com/docs/lec1.pdf. (This might need Acroread.)

Theorem by Howgrave-Graham

Let $g(x) = \sum_{i=0}^{d-1} g_i x^i \in \mathbf{Z}[x]$ of $\deg(g) = d - 1$.
Let $b, k \in \mathbf{Z}_{>0}$. If

1. $g(x_0) \equiv 0 \bmod b^k$ with $|x_0| \leq X$,
2. $||g(xX)|| \leq b^k/\sqrt{d}$

then $g(x_0) = 0$ over $\mathbf{Z}$.

Here $||g(xX)|| = \sqrt{g_0^2 + g_1^2 X^2 + \cdots + g_{d-1}^2 X^{2(d-1)}}$ is Euclidean norm of the coefficient vector of $g(xX)$.

Proof: Let $v = (1, x_0/X, x_0^2/X^2, \ldots, x_0^{d-1}/X^{d-1})$ and $w = (g_0, g_1 X, g_2 X^2, \ldots, g_{d-1} X^{d-1})$.
Note $v \cdot w = g(x_0)$ and each entry in v is ≤ 1.

Theorem by Howgrave-Graham

Let $g(x) = \sum_{i=0}^{d-1} g_i x^i \in \mathbf{Z}[x]$ of $\deg(g) = d - 1$.
Let $b, k \in \mathbf{Z}_{>0}$. If

1. $g(x_0) \equiv 0 \bmod b^k$ with $|x_0| \leq X$,
2. $||g(xX)|| \leq b^k/\sqrt{d}$

then $g(x_0) = 0$ over $\mathbf{Z}$.

Here $||g(xX)|| = \sqrt{g_0^2 + g_1^2X^2 + \cdots + g_{d-1}^2X^{2(d-1)}}$ is
Euclidean norm of the coefficient vector of $g(xX)$.

Proof: Let $v = (1, x_0/X, x_0^2/X^2, \ldots, x_0^{d-1}/X^{d-1})$ and
$w = (g_0, g_1X, g_2X^2, \ldots, g_{d-1}X^{d-1})$.
Note $v \cdot w = g(x_0)$ and each entry in v is ≤ 1.

By Cauchy-Schwarz inequality $|v \cdot w| < ||v||||w||$.
Strict inequality as they are not linearly dependent.
Here $||v|| \leq \sqrt{1 + 1 + 1 + \cdots + 1} = \sqrt{d}$ and $||w|| = ||g(xX)||$.

Theorem by Howgrave-Graham

Let $g(x) = \sum_{i=0}^{d-1} g_i x^i \in \mathbf{Z}[x]$ of $\deg(g) = d - 1$.
Let $b, k \in \mathbf{Z}_{>0}$. If

1. $g(x_0) \equiv 0 \bmod b^k$ with $|x_0| \le X$,
2. $||g(xX)|| \le b^k/\sqrt{d}$

then $g(x_0) = 0$ over $\mathbf{Z}$.

Here $||g(xX)|| = \sqrt{g_0^2 + g_1^2 X^2 + \cdots + g_{d-1}^2 X^{2(d-1)}}$ is Euclidean norm of the coefficient vector of $g(xX)$.

Proof: Let $v = (1, x_0/X, x_0^2/X^2, \ldots, x_0^{d-1}/X^{d-1})$ and $w = (g_0, g_1X, g_2X^2, \ldots, g_{d-1}X^{d-1})$.
Note $v \cdot w = g(x_0)$ and each entry in v is ≤ 1.

By Cauchy-Schwarz inequality $|v \cdot w| < ||v||||w||$.
Strict inequality as they are not linearly dependent.
Here $||v|| \le \sqrt{1 + 1 + 1 + \cdots + 1} = \sqrt{d}$ and $||w|| = ||g(xX)||$.
Thus $|g(x_0)| = |v \cdot w| < ||v||||w|| \le \sqrt{d} b^k/\sqrt{d} = b^k$.

Theorem by Howgrave-Graham

Let $g(x) = \sum_{i=0}^{d-1} g_i x^i \in \mathbf{Z}[x]$ of $\deg(g) = d - 1$.
Let $b, k \in \mathbf{Z}_{>0}$. If

1. $g(x_0) \equiv 0 \bmod b^k$ with $|x_0| \le X$,
2. $||g(xX)|| \le b^k/\sqrt{d}$

then $g(x_0) = 0$ over $\mathbf{Z}$.

Here $||g(xX)|| = \sqrt{g_0^2 + g_1^2 X^2 + \cdots + g_{d-1}^2 X^{2(d-1)}}$ is Euclidean norm of the coefficient vector of $g(xX)$.

Proof: Let $v = (1, x_0/X, x_0^2/X^2, \ldots, x_0^{d-1}/X^{d-1})$ and
$w = (g_0, g_1 X, g_2 X^2, \ldots, g_{d-1} X^{d-1})$.
Note $v \cdot w = g(x_0)$ and each entry in v is ≤ 1.

By Cauchy-Schwarz inequality $|v \cdot w| < ||v|| ||w||$.
Strict inequality as they are not linearly dependent.
Here $||v|| \le \sqrt{1 + 1 + 1 + \cdots + 1} = \sqrt{d}$ and $||w|| = ||g(xX)||$.
Thus $|g(x_0)| = |v \cdot w| < ||v|| ||w|| \le \sqrt{d} b^k/\sqrt{d} = b^k$.
If $g(x_0) \in b^k\mathbf{Z}$ and $|g(x_0)| < b^k$ then $g(x_0) = 0$.
If $z \equiv 0 \bmod b^k$ & $|z| < b^k$ then

Theorem by Howgrave-Graham

Let $g(x) = \sum_{i=0}^{d-1} g_i x^i \in \mathbf{Z}[x]$ of $\deg(g) = d-1$.
Let $b, k \in \mathbf{Z}_{>0}$. If

1. $g(x_0) \equiv 0 \bmod b^k$ with $|x_0| \leq X$,
2. $||g(xX)|| \leq b^k/\sqrt{d}$

then $g(x_0) = 0$ over $\mathbf{Z}$.

Here $||g(xX)|| = \sqrt{g_0^2 + g_1^2 X^2 + \cdots + g_{d-1}^2 X^{2(d-1)}}$ is Euclidean norm of the coefficient vector of $g(xX)$.

Proof: Let $v = (1, x_0/X, x_0^2/X^2, \ldots, x_0^{d-1}/X^{d-1})$ and
$w = (g_0, g_1 X, g_2 X^2, \ldots, g_{d-1} X^{d-1})$.
Note $v \cdot w = g(x_0)$ and each entry in v is ≤ 1.

By Cauchy-Schwarz inequality $|v \cdot w| < ||v||||w||$.
Strict inequality as they are not linearly dependent.
Here $||v|| \leq \sqrt{1+1+1+\cdots+1} = \sqrt{d}$ and $||w|| = ||g(xX)||$.
Thus $|g(x_0)| = |v \cdot w| < ||v||||w|| \leq \sqrt{d}b^k/\sqrt{d} = b^k$.
If $g(x_0) \in b^k\mathbf{Z}$ and $|g(x_0)| < b^k$ then $g(x_0) = 0$.
If $z \equiv 0 \bmod b^k$ & $|z| < b^k$ then $z = 0$; using $z \equiv 0 \bmod b^k \Leftrightarrow z \in b^k\mathbf{Z}$.

What to look for?

We want to find a polynomial $g(x)$ and a root x_0 so that $g(x_0) \in b^k\mathbf{Z}$.

What to look for?

We want to find a polynomial $g(x)$ and a root x_0 so that $g(x_0) \in b^k\mathbf{Z}$.
Here are some polynomials that work:
$g(x) \in b^k\mathbf{Z}$

What to look for?

We want to find a polynomial $g(x)$ and a root x_0 so that $g(x_0) \in b^k\mathbf{Z}$.
Here are some polynomials that work:
$g(x) \in b^k\mathbf{Z} + b^k x\mathbf{Z}$

What to look for?

We want to find a polynomial $g(x)$ and a root x_0 so that $g(x_0) \in b^k\mathbf{Z}$.
Here are some polynomials that work:
$g(x) \in b^k\mathbf{Z} + b^k x\mathbf{Z} + b^k x^2\mathbf{Z}$

What to look for?

We want to find a polynomial $g(x)$ and a root x_0 so that $g(x_0) \in b^k\mathbf{Z}$.
Here are some polynomials that work:
$g(x) \in b^k\mathbf{Z} + b^k x\mathbf{Z} + b^k x^2\mathbf{Z} + b^k x^3\mathbf{Z} \cdots$.

What to look for?

We want to find a polynomial $g(x)$ and a root x_0 so that $g(x_0) \in b^k\mathbf{Z}$.
Here are some polynomials that work:
$g(x) \in b^k\mathbf{Z} + b^k x\mathbf{Z} + b^k x^2\mathbf{Z} + b^k x^3\mathbf{Z} \cdots$.

We have some polynomial $f(x)$ to start with and know that $f(x_0) \in b^k\mathbf{Z}$ for the x_0 we're looking for.

What to look for?

We want to find a polynomial $g(x)$ and a root x_0 so that $g(x_0) \in b^k\mathbf{Z}$.
Here are some polynomials that work:
$g(x) \in b^k\mathbf{Z} + b^kx\mathbf{Z} + b^kx^2\mathbf{Z} + b^kx^3\mathbf{Z} \cdots$.

We have some polynomial $f(x)$ to start with and know that $f(x_0) \in b^k\mathbf{Z}$ for the x_0 we're looking for.

If $\deg(f) = t$ then we're looking for
$g(x) \in b^k\mathbf{Z} + b^kx\mathbf{Z} + b^kx^2\mathbf{Z} + \cdots + b^kx^{t-1}\mathbf{Z} + f(x)\mathbf{Z}$.
The polynomial f does not need an extra b^k.

What to look for?

We want to find a polynomial $g(x)$ and a root x_0 so that $g(x_0) \in b^k\mathbf{Z}$.
Here are some polynomials that work:
$g(x) \in b^k\mathbf{Z} + b^kx\mathbf{Z} + b^kx^2\mathbf{Z} + b^kx^3\mathbf{Z}\cdots$.

We have some polynomial $f(x)$ to start with and know that $f(x_0) \in b^k\mathbf{Z}$ for the x_0 we're looking for.

If $\deg(f) = t$ then we're looking for
$g(x) \in b^k\mathbf{Z} + b^kx\mathbf{Z} + b^kx^2\mathbf{Z} + \cdots + b^kx^{t-1}\mathbf{Z} + f(x)\mathbf{Z}$.
The polynomial f does not need an extra b^k.

If that's too restrictive we can expand to
$g(x) \in$
$b^k\mathbf{Z} + b^kx\mathbf{Z} + b^kx^2\mathbf{Z} + \cdots + b^kx^{t-1}\mathbf{Z} + f(x)\mathbf{Z} + xf(x)\mathbf{Z} + x^2f(x)\mathbf{Z} + \cdots$.

What to look for and how to find it?

All of these attacks start by finding some polynomial $f(x)$ for which a root modulo b^k is interesting.
Let $\deg(f) = t$ and let $|x_0| \leq X$ for some known X.

To find $g(x) \in$
$b^k\mathbf{Z} + b^k x\mathbf{Z} + b^k x^2\mathbf{Z} + \cdots + b^k x^{t-1}\mathbf{Z} + f(x)\mathbf{Z} + xf(x)\mathbf{Z} + x^2 f(x)\mathbf{Z} + \cdots$
we will use LLL, which builds integer linear combinations of the input rows of a matrix. It returns a vector that is short in the Euclidean norm. (Hence we wanted that in the Howgrave-Graham theorem).

We set up a system of equations in the coefficient vectors, one row per option. $b^k\mathbf{Z}$ turns into coefficient b^k at the x^0 column etc.

For Howgrave-Graham we need to scale the column of x^s by X^s.
So we get

$$\begin{pmatrix} X & a \\ 0 & n \end{pmatrix}$$

$b^k = p$ but we only know n.
But 2×2 likely too small.

What to look for and how to find it?

All of these attacks start by finding some polynomial $f(x)$ for which a root modulo b^k is interesting.
Let $\deg(f) = t$ and let $|x_0| \leq X$ for some known X.

To find $g(x) \in$
$b^k\mathbf{Z} + b^k x\mathbf{Z} + b^k x^2\mathbf{Z} + \cdots + b^k x^{t-1}\mathbf{Z} + f(x)\mathbf{Z} + xf(x)\mathbf{Z} + x^2 f(x)\mathbf{Z} + \cdots$
we will use LLL, which builds integer linear combinations of the input rows of a matrix. It returns a vector that is short in the Euclidean norm. (Hence we wanted that in the Howgrave-Graham theorem).

We set up a system of equations in the coefficient vectors, one row per option. $b^k\mathbf{Z}$ turns into coefficient b^k at the x^0 column etc.

For Howgrave-Graham we need to scale the column of x^s by X^s.
So we get

$$\begin{pmatrix} X^2 & aX & 0 \\ 0 & X & a \\ 0 & 0 & n \end{pmatrix}$$

LLL gives $||v_1|| \leq (2/\sqrt{4\delta - 1})^{(d-1)/2} \det(M)^{1/d}$, i.e.,
$||g(xX)|| \leq 2(X^3 n)^{1/3}$ for $\delta = 1/2$.
Then $2(X^3 n)^{1/3} \leq p/\sqrt{3}$ for $X < n^{1/6}/\sqrt{12}$ if $p \approx q$.

Stereotyped message with small e in RSA

```
n = random_prime(2^160)*random_prime(2^160)
m = Integer('myfavoritesubjectiscryptology',36)
c = m^3 % n      # note small primes, reduction happens
```

Stereotyped message with small e in RSA

```
n = random_prime(2^160)*random_prime(2^160)
m = Integer('myfavoritesubjectiscryptology',36)
c = m^3 % n      # note small primes, reduction happens
```

Match this up with
$g(x) \in b^k\mathbf{Z} + b^k x\mathbf{Z} + b^k x^2\mathbf{Z} + \cdots + b^k x^{t-1}\mathbf{Z} + f(x)\mathbf{Z}$.
for $b^k = n, f(x) = (a+x)^3 - c$ with

```
a = Integer('myfavoritesubjectis0000000000',36)
```

Stereotyped message with small e in RSA

```
n = random_prime(2^160)*random_prime(2^160)
m = Integer('myfavoritesubjectiscryptology',36)
c = m^3 % n      # note small primes, reduction happens
```

Match this up with
$g(x) \in b^k\mathbf{Z} + b^k x\mathbf{Z} + b^k x^2\mathbf{Z} + \cdots + b^k x^{t-1}\mathbf{Z} + f(x)\mathbf{Z}$.
for $b^k = n, f(x) = (a+x)^3 - c$ with

```
a = Integer('myfavoritesubjectis0000000000',36)
```

```
X = Integer('zzzzzzzzzz',36)
M = matrix([[X^3, 3*X^2*a, 3*X*a^2, a^3-c],
            [0,n*X^2,0,0],[0,0,n*X,0],[0,0,0,n]])
```

Stereotyped message with small e in RSA

```
n = random_prime(2^160)*random_prime(2^160)
m = Integer('myfavoritesubjectiscryptology',36)
c = m^3 % n      # note small primes, reduction happens
```

Match this up with
$g(x) \in b^k\mathbf{Z} + b^k x\mathbf{Z} + b^k x^2\mathbf{Z} + \cdots + b^k x^{t-1}\mathbf{Z} + f(x)\mathbf{Z}$.
for $b^k = n, f(x) = (a+x)^3 - c$ with

```
a = Integer('myfavoritesubjectis0000000000',36)
```

```
X = Integer('zzzzzzzzzz',36)
M = matrix([[X^3, 3*X^2*a, 3*X*a^2, a^3-c],
            [0,n*X^2,0,0],[0,0,n*X,0],[0,0,0,n]])
```

```
B = M.LLL()
Q = B[0][0]*x^3/X^3+B[0][1]*x^2/X^2+B[0][2]*x/X+B[0][3]
```

Stereotyped message with small e in RSA

```
n = random_prime(2^160)*random_prime(2^160)
m = Integer('myfavoritesubjectiscryptology',36)
c = m^3 % n      # note small primes, reduction happens
```

Match this up with
$g(x) \in b^k\mathbf{Z} + b^k x\mathbf{Z} + b^k x^2\mathbf{Z} + \cdots + b^k x^{t-1}\mathbf{Z} + f(x)\mathbf{Z}$.
for $b^k = n, f(x) = (a + x)^3 - c$ with

```
a = Integer('myfavoritesubjectis0000000000',36)

X = Integer('zzzzzzzzzz',36)
M = matrix([[X^3, 3*X^2*a, 3*X*a^2, a^3-c],
           [0,n*X^2,0,0],[0,0,n*X,0],[0,0,0,n]])

B = M.LLL()
Q = B[0][0]*x^3/X^3+B[0][1]*x^2/X^2+B[0][2]*x/X+B[0][3]

sage: Q.roots(ring=ZZ)[0][0].str(base=36)
'cryptology'
```