The art of cryptography, summer 2013
Lattices and cryptography

Prof. Dr. Joachim von zur Gathen
Cryptanalysis: It was used to break many cryptosystems. In the 1980’s, the first generation of public-key cryptosystems besides RSA, the *subset sum* system, was obliterated by this attack. For many types of new systems, one has to consider carefully potential attacks using this methodology.

Security reductions: If a system like the Diffie-Hellman key exchange or RSA encryption is secure, it is not clear that partial information like the leading bits of a Diffie-Hellman key or of a prime factor an in RSA modulus are also secure. But lattice technology provides proofs that this is indeed the case.

Cryptography: Since 1996, the method has been used to devise cryptosystems that have (provably under a hardness assumption) a desirable property that no previous system had: breaking an “average instance” is as difficult as breaking a “hardest instance”.
**Definition 1.** Let $a_1, \ldots, a_\ell \in \mathbb{R}^n$ be linearly independent over $\mathbb{R}$. Then

$$L = \sum_{1 \leq i \leq \ell} \mathbb{Z}a_i = \left\{ \sum_{1 \leq i \leq \ell} r_i a_i : r_1, \ldots, r_\ell \in \mathbb{Z} \right\}$$

is the lattice (or $\mathbb{Z}$-module) generated by $a_1, \ldots, a_\ell$. These vectors form a basis of $L$.

**Definition 2.** Let $L$ be a lattice generated by the rows of the matrix $A \in \mathbb{R}^{\ell \times n}$. The norm of $L$ is $|L| = \det(AA^T)^{1/2} \in \mathbb{R}$.  

**Definition 1.** Let $a_1, \ldots, a_\ell \in \mathbb{R}^n$ be linearly independent over $\mathbb{R}$. Then

$$L = \sum_{1 \leq i \leq \ell} \mathbb{Z}a_i = \left\{ \sum_{1 \leq i \leq \ell} r_i a_i : r_1, \ldots, r_\ell \in \mathbb{Z} \right\}$$

is the lattice (or $\mathbb{Z}$-module) generated by $a_1, \ldots, a_\ell$. These vectors form a basis of $L$.

**Definition 2.** Let $L$ be a lattice generated by the rows of the matrix $A \in \mathbb{R}^{\ell \times n}$. The norm of $L$ is $|L| = \det(AA^T)^{1/2} \in \mathbb{R}$. 
Figure: The lattice in $\mathbb{R}^2$ generated by $(12, 2)$ (red) and $(13, 4)$ (blue).
**Example 3.** We let \( \ell = n = 2, \ a_1 = (12, 2), \ a_2 = (13, 4) \) and \( L = \mathbb{Z}a_1 + \mathbb{Z}a_2 \). The figure shows some lattice points of \( L \) near the origin of the plane \( \mathbb{R}^2 \). The norm of \( L \) is

\[
|L| = \left| \det \begin{pmatrix} 12 & 2 \\ 13 & 4 \end{pmatrix} \right| = 22
\]

and equals the area of the gray parallelogram.

We have \( 22 \leq ||a_1|| \cdot ||a_2|| = 74\sqrt{5} \approx 165.47 \). Another basis of \( L \) is \( b_1 = (1, 2) \) and \( b_2 = (11, 0) = 2a_1 - a_2 \), and \( b_1 \) is a “shortest” vector in \( L \). We have \( 22 \leq ||b_1|| \cdot ||b_2|| = 11\sqrt{5} \).
Definition 4. Let $L \subset \mathbb{R}^n$ be an $\ell$-dimensional lattice and $1 \leq i \leq \ell$. The $i$th successive minimum $\lambda_i(L)$ is the smallest real number so that there exist $i$ linearly independent vectors in $L$, all of length at most $\lambda_i(L)$.

Definition 5. Let $b_1, \ldots, b_\ell \in \mathbb{R}^n$ be linearly independent and $(b_1^*, \ldots, b_\ell^*)$ the corresponding Gram-Schmidt orthogonal basis. Then $(b_1, \ldots, b_\ell)$ is reduced if $\|b_i^*\|^2 \leq 2\|b_{i+1}^*\|^2$ for $1 \leq i < \ell$. 
Definition 4. Let $L \subset \mathbb{R}^n$ be an $\ell$-dimensional lattice and $1 \leq i \leq \ell$. The $i$th successive minimum $\lambda_i(L)$ is the smallest real number so that there exist $i$ linearly independent vectors in $L$, all of length at most $\lambda_i(L)$.

Definition 5. Let $b_1, \ldots, b_\ell \in \mathbb{R}^n$ be linearly independent and $(b_1^*, \ldots, b_\ell^*)$ the corresponding Gram-Schmidt orthogonal basis. Then $(b_1, \ldots, b_\ell)$ is reduced if $\|b_i^*\|^2 \leq 2\|b_{i+1}^*\|^2$ for $1 \leq i < \ell$. 
**Theorem 6.** Let $b_1, \ldots, b_\ell \in \mathbb{R}^n$ be a reduced basis of the lattice $L$ and $\lambda_1(L)$ the length of a shortest nonzero vector $x$ in $L$. Then $\|b_1\| \leq 2^{(\ell-1)/2} \cdot \lambda_1(L)$.

**Corollary 7.** Given linearly independent vectors $a_1, \ldots, a_\ell \in \mathbb{Z}^n$ whose norm has bit length at most $m$, the basis reduction algorithm computes a reduced basis $b_1, \ldots, b_\ell$ of $L = \sum_{1 \leq i \leq \ell} \mathbb{Z}a_i$. Furthermore, $x = b_1$, is a “short” nonzero vector in $L$ with

$$\|x\| \leq 2^{(\ell-1)/2} \min\{\|y\| : 0 \neq y \in L\}.$$ 

It uses $O(n^6m^2)$ bit operations.
**Theorem 6.** Let \( b_1, \ldots, b_\ell \in \mathbb{R}^n \) be a reduced basis of the lattice \( L \) and \( \lambda_1(L) \) the length of a shortest nonzero vector \( x \) in \( L \). Then \( \|b_1\| \leq 2^{(\ell-1)/2} \cdot \lambda_1(L) \).

**Corollary 7.** Given linearly independent vectors \( a_1, \ldots, a_\ell \in \mathbb{Z}^n \) whose norm has bit length at most \( m \), the basis reduction algorithm computes a reduced basis \( b_1, \ldots, b_\ell \) of \( L = \sum_{1 \leq i \leq \ell} \mathbb{Z}a_i \). Furthermore, \( x = b_1 \), is a “short” nonzero vector in \( L \) with

\[
\|x\| \leq 2^{(\ell-1)/2} \min\{\|y\| : 0 \neq y \in L\}.
\]

It uses \( O(n^6m^2) \) bit operations.
The *subset sum problem* seeks to answer the following.

Given $t_0, t_1, \ldots, t_n \in \mathbb{N}$, are there $x_1, \ldots, x_n \in \{0, 1\}$ with $t_0 = \sum_{1 \leq i \leq n} t_i x_i$?

**Example 8.** The input $(1215, 366, 385, 392, 401, 422, 437)$ means that we ask whether there exist $x_1, \ldots, x_6 \in \{0, 1\}$ such that $366x_1 + 385x_2 + 392x_3 + 401x_4 + 422x_5 + 437x_6 = 1215$. 
Example 9. Alice takes $m = 1009$ and $r = 621$, her secret $s_1, \ldots, s_6$ as follows, and publishes $t_1, \ldots, t_6$.

<table>
<thead>
<tr>
<th>$i$</th>
<th>$s_i$</th>
<th>$t_i$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>233</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>854</td>
</tr>
<tr>
<td>3</td>
<td>7</td>
<td>311</td>
</tr>
<tr>
<td>4</td>
<td>15</td>
<td>234</td>
</tr>
<tr>
<td>5</td>
<td>31</td>
<td>80</td>
</tr>
<tr>
<td>6</td>
<td>60</td>
<td>936</td>
</tr>
</tbody>
</table>

If Bob wants to send the bit string $x = 010110$ to Alice, he encrypts this as $t_0 = t_2 + t_4 + t_5 = 1168$. Alice computes $s_0 = r^{-1}t_0 = 13 \cdot 1168 = 49$ in $\mathbb{Z}_{1009}$, and solves the easy subset sum problem $49 = 3 + 15 + 31$, from which she recovers $x$. 
We start by connecting subset sum problems to short vector problems. For Example 8, we consider the lattice $L \subseteq \mathbb{Z}^7$ generated by the rows of the matrix

\[
\begin{pmatrix}
1215 & 0 & 0 & 0 & 0 & 0 & 0 \\
-366 & 1 & 0 & 0 & 0 & 0 & 0 \\
-385 & 0 & 1 & 0 & 0 & 0 & 0 \\
-392 & 0 & 0 & 1 & 0 & 0 & 0 \\
-401 & 0 & 0 & 0 & 1 & 0 & 0 \\
-422 & 0 & 0 & 0 & 0 & 1 & 0 \\
-437 & 0 & 0 & 0 & 0 & 0 & 1 \\
\end{pmatrix} \in \mathbb{Z}^{7 \times 7}.
\]
Basis reduction then computes the short vector
\[ y = (0, 0, 0, 1, 1, 1, 0) \in L, \] and indeed
\[ 1215 = 366 \cdot 0 + 385 \cdot 0 + 392 \cdot 1 + 401 \cdot 1 + 422 \cdot 1 + 437 \cdot 0. \]
Let \( a_i \) be the \( i \)th row vector, for \( 0 \leq i \leq 6 \), so that
\[ a_6 = (-437, 0, 0, 0, 0, 0, 1) \] as an example, \( x_0 = 1 \), and
\[ x = (0, 0, 1, 1, 1, 0) \in \{0, 1\}^6 \] the solution vector. Then
\[ y = \sum_{0 \leq i \leq 6} x_i a_i. \]
Thus basis reduction solves this particular subset sum problem.
Algorithm 10. Short vectors for subset sums.

Input: Positive integers $t_0, t_1, \ldots, t_n$.
Output: $(x_1, \ldots, x_n) \in \mathbb{Z}^n$ or “failure”.

1. Let $M = \lceil 2^{n/2} n^{1/2} \rceil + 1$.
2. If $t_0 < \sum_{1 \leq i \leq n} t_i / 2$ then $t_0 \leftarrow \sum_{1 \leq i \leq n} t_i - t_0$.
3. For $0 \leq i \leq n$, let $a_i \in \mathbb{Z}^{n+1}$ be the $i$th row of the matrix
   \[
   \begin{pmatrix}
   t_0 M & 0 & 0 & \cdots & 0 \\
   -t_1 M & 1 & 0 & \cdots & 0 \\
   -t_2 M & 0 & 1 & \cdots & 0 \\
   \vdots & \vdots & \vdots & \ddots & \vdots \\
   -t_n M & 0 & 0 & \cdots & 1
   \end{pmatrix}
   \in \mathbb{Z}^{(n+1) \times (n+1)}.
   \]
4. Let $L \subseteq \mathbb{Z}^{n+1}$ be the lattice generated by $a_0, \ldots, a_n$. Run the basis reduction on this basis to receive a short nonzero vector $y = (y_0, \ldots, y_n) \in L$.
5. If $y_0 = 0$ and there is some $\delta \in \pm 1$ with $\delta y \in \{0, 1\}^{n+1}$, then
   \[
   x \left\{ \begin{array}{ll}
   (1 - \delta y_1, \ldots, 1 - \delta y_n) & \text{if the condition in step 2 is satisfied for the input } t, \\
   (\delta y_1, \ldots, \delta y_n) & \text{otherwise.}
   \end{array} \right.
   \]
   else return “failure”.
6. Return $x$. 5/17
We consider the following set of solvable subset sum problems:

$$E = \{(t_0, \ldots, t_n) \in \mathbb{Z}^{n+1}: \exists x \in \{0, 1\}^n \ t_0 = \sum_{1 \leq i \leq n} t_i x_i > 0$$

and $1 \leq t_i \leq C$ for $1 \leq i \leq n\}.$

**Theorem 11.** Let $\epsilon > 0$, $n \geq 4$, let $C \geq \epsilon^{-1/2} 2^{n(n+\log_2 n+5)/2}$ be an integer, and consider inputs $t = (t_0, t_1, \ldots, t_n) \in E$ to Algorithm 10, where $(t_1, \ldots, t_n)$ is chosen uniformly at random in $T = \{1, \ldots, C\}^n$. Then the algorithm correctly returns a solution $x$ to the subset sum problem $t$ with probability at least $1 - \epsilon.$
Example 12. For \( n = 6 \) and \( \epsilon = 1/10 \), we can take \( C = 36238786559 \). We ran 100 examples with 
\[
(t_1, \ldots, t_6) \leftarrow T = \{1, \ldots, C\}^6 \quad \text{and} \quad x \leftarrow \{0, 1\}^6 \setminus \{(0, \ldots, 0)\},
\]
and the algorithm returned \( x \) in all cases.
The density $\delta(x)$ of a subset sum problem $t = (t_0, \ldots, t_n)$ is

$$\delta(t) = \frac{n}{\max_{1 \leq i \leq n} \{\log_2 t_i\}},$$

assuming that $t_i \geq 2$ for some $i$.

The subset sum cryptosystem encrypts $n$ bits $x_1, \ldots, x_n$ into the single number $t_0 = \sum_{1 \leq i \leq n} t_i x_i$, whose bit length is on average about $\max_{1 \leq i \leq n} \{\log_2 t_i\}$. Thus $\delta(t)$ is roughly the information rate

$$\frac{\text{length of plaintext}}{\text{length of ciphertext}}.$$
When we take $\varepsilon$ to be a constant, we can interpret Theorem 11 as saying that Algorithm 10 solves almost all subset sum problems $t$ with

$$\delta(t) \leq \frac{2}{n}.$$  

In practice, the algorithm performs much better, and seems to solve most subset sum problems with

$$\delta(t) < 0.645.$$
Example 13. The three examples in the text have the following densities.

<table>
<thead>
<tr>
<th></th>
<th>n</th>
<th>max{\log_2 t_i}</th>
<th>\delta(t)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example 8</td>
<td>6</td>
<td>\log_2 437 \approx 8.771</td>
<td>0.684</td>
</tr>
<tr>
<td>Example 9, (t_i)</td>
<td>6</td>
<td>\log_2 60 \approx 5.907</td>
<td>1.016</td>
</tr>
<tr>
<td>Example 9, (s_i)</td>
<td>6</td>
<td>\log_2 936 \approx 9.870</td>
<td>0.608</td>
</tr>
</tbody>
</table>