6.892 Computing on Encrypted Data November 11, 2013

Lecture 7

Lecturer: Vinod Vaikuntanathan *Scribe: Sunoo Park*

Agenda

1. Trapdoors for lattices
2. Use trapdoors to construct identity-based encryption (IBE)

1 Integer Lattices

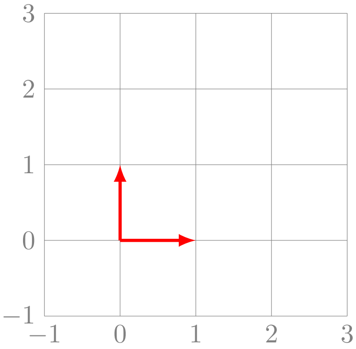
Definition 1. (INTEGER LATTICE)
$\mathcal{L} \subseteq \mathbb{Z}^m$ is an integer lattice (of dimension m) if it is closed under subtraction.

Definition 2. (INTEGER LATTICE (EQUIVALENT DEFINITION))
$\mathcal{L} \subseteq \mathbb{Z}^m$ is a rank-n lattice if there are ℓ independent (over $\mathbb{R}$) vectors in $B = b_1, \ldots, b_n$ such that

$$\mathcal{L}(B) = \sum_i \mathbb{Z} \cdot b_i = \left\{ \sum_i z_i b_i, z_i \in \mathbb{Z} \right\}.$$

1.1 Examples

1. $\mathcal{L} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. (Note that in this example, $b_1 = \binom{1}{0}$ and $b_2 = \binom{0}{1}$ are a *short* basis.)



2. $\mathcal{L} = \{(z_1, z_2) : z_1 + z_2 \text{ is even}\}$.
3. $\mathcal{L} = \begin{pmatrix} 13 & 21 \\ 21 & 34 \end{pmatrix}$. (Note that here we have a *long* basis.)

2 Some Hard Problems

Definition 3. (SHORTEST VECTOR PROBLEM (SVP))
Given a basis B, find the shortest nonzero vector in $\mathcal{L}(B)$. Let the length of this vector be $\lambda_1(\mathcal{L}(B))$.

Known algorithms for SVP have exponential complexity: notably, [AKS01] give an algorithm working in $2^{O(m)}$ time and $2^{O(m)}$ space, and [Kan83] gives one using $n^{O(m)}$ time and $\mathsf{poly}(m)$ space.

Definition 4. (γ-APPROXIMATE SHORTEST VECTOR PROBLEM (SVP$_\gamma$))
For $\gamma \in \mathbb{R}$, given a basis B, find a nonzero $v \in \mathcal{L}(B)$ such that $||v|| \leq \gamma\lambda_1(\mathcal{L}(B))$.

The Lenstra-Lenstra-Lovász algorithm [LLL82] solves $2^{O(n)}$-approximate SVP in $\mathsf{poly}(m)$ time.

Definition 5. (CLOSEST VECTOR PROBLEM (CVP))
Given B and a target vector $t \in \mathbb{Z}^m$, find $v \in \mathcal{L}(B)$ such that $\forall v' \in \mathcal{L}(B), ||v - t|| \leq ||v' - t||$.

Definition 6. (γ-APPROXIMATE CLOSEST VECTOR PROBLEM (CVP$_\gamma$))
Given B and a target vector $t \in \mathbb{Z}^m$, find $v \in \mathcal{L}$ such that $\forall v' \in \mathcal{L}(B), ||v - t|| \leq \gamma||v' - t||$.

The following "rounding" algorithm, due to Babai [Bab86], gives a (coarse) solution to approximate CVP.

Algorithm 1 BABAI'S ROUNDING ALGORITHM

```
Receive inputs $B, t$.
Write $t = B \cdot y$ for coefficients $y \in \mathbb{R}^m$.
Output $v = B \cdot \lceil y \rfloor \in \mathcal{L}(B)$ (i.e. round the coefficients).
```

Lemma 7. *For v outputted by the above algorithm on inputs B, t, it holds that $||v - t|| \leq \frac{1}{2}\sum_i ||b_i||$.*

Remark. It is known that an efficient solution to CVP implies an efficient solution to SVP, but the other direction is open.

Definition 8. (SHORT INTEGER SOLUTIONS PROBLEM (SIS$_\alpha$))
Given $A \in \mathbb{Z}_q^{n\times m}$, find $e \in \mathbb{Z}^m$ satisfying $Ae = 0 \mod q$ and $||e||_2 \leq \alpha$.

Definition 9. (INHOMOGENEOUS SHORT INTEGER SOLUTIONS PROBLEM (ISIS$_\alpha$))
Given $A \in \mathbb{Z}_q^{n\times m}$ and $y \in \mathbb{Z}_q^n$, find $e \in \mathbb{Z}^m$ satisfying $Ae = y \mod q$ and $||e||_2 \leq \alpha$.

Lemma 10. *An efficient solution to ISIS$_\alpha$ implies an efficient solution to SIS$_\alpha$.*

Proof. Given an oracle for ISIS$_\alpha$, the following algorithm gives an efficient solver for SIS$_\alpha$. □

Algorithm 2 SIS SOLVER WITH ORACLE FOR ISIS

```
Choose a short $e' \in \mathbb{Z}^m$.
Let $y = Ae'$.
Query the ISIS oracle for an $e$ such that $Ae = y$.
Output $e - e' \mod q$.
```

3 Two Classes of Average-Case Lattices

3.1 Regev lattices

Definition 11. (REGEV LATTICE)
Fix parameters n, m, q. Given $A \in \mathbb{Z}_q^{n\times m}$, the Regev lattice is $\Lambda(A) = \{A^T s + q\mathbb{Z}^m : s \in \mathbb{Z}^n\}$.

Note that if we consider A to be the generator matrix of a linear code, then $\Lambda(A)$ is the set of all codewords, i.e. all linear combinations of the rows of A. (We need to add $q\mathbb{Z}^m$ to adjust for the fact that codes are defined over finite fields, but the lattice is over $\mathbb{Z}$.)

LWE may be considered a "bounded distance" version of CVP on a Regev lattice, as illustrated below. Properties of Regev lattices:

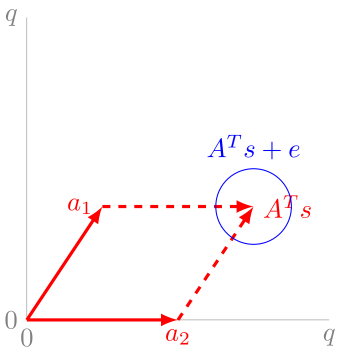


Figure 1: LWE as "bounded distance" CVP on a Regev lattice.

- The number of lattice points in the "primitive cube" is q^n.
- The volume of the *fundamental parallelepiped* is q^{m-n}.
- The length of the shortest vector is $\lambda_1(\mathcal{L}(B)) \le \sqrt{m}(\det(B))^{1/m}$.
- For a $1 - \text{negl}(n)$ fraction of matrices A, it holds that $\lambda_1(\Lambda(A)) \approx q^{\frac{m-n}{m}} = q \cdot q^{-n/m}$. Thus for $m \approx n \log q$, it follows that $\lambda_1(\Lambda(A)) \approx O(q)$.

Definition 12. (Ajtai lattice)
For n, m, q, A as above, the Ajtai lattice is $\Lambda^\perp(A) = \{r \in \mathbb{Z}^m : Ar = 0 \mod q\}$.

Properties of Ajtai lattices:

- For most matrices A, it holds that $\lambda_1(\Lambda^\perp(A)) = O(\sqrt{m})$.

Definition 13. (dual lattices)
$\mathcal{L}$ and $\mathcal{L}'$ are dual lattices *if $\forall x \in \mathcal{L}, y \in \mathcal{L}', \langle x, y\rangle \in \mathbb{Z}$.*

Claim 14. *$\Lambda(A)$ and $\Lambda^\perp(A) \cdot \frac{1}{q}$ are dual lattices.*

Proof. Take any $x \in \Lambda(A)$ and $y \in \Lambda^\perp(A) \cdot \frac{1}{q}$. Then $qy \in \Lambda^\perp(A)$, and by the definitions of the lattices, $x = A^T s$ (for some s) and $A(qy) = 0 \mod q$. It follows that $\langle x, qy\rangle = x^T(qy) = s^T A(qy) = 0 \mod q$. Therefore $\langle x, y\rangle = \langle x, qy\rangle / q \in \mathbb{Z}$. □

4 Constructing IBE

Recall that an identity-based encryption scheme allows encryption of messages for a particular recipient by using the recipient's *identity*, which is publicly known and external to the encryption scheme (e.g. an email address), rather than requiring the use of his *public key* as in traditional encryption schemes. The model for IBE assumes a trusted party to whom users may present their identity, and then receive a secret key using which they may decrypt messages encrypted for that identity. For a formal definition, refer to the notes of the previous lecture.

We will make use of a variant of the dual Regev cryptosystem which was discussed in the previous lecture. Our construction follows [GPV08]. Recall that the definition of the cryptosystem is as below.

Definition 15. (dual Regev cryptosystem)

- *Public parameters: $A \in \mathbb{Z}_q^{n\times m}, m = \Omega(n \log q)$.*

- $\mathsf{KeyGen}() = (sk, pk)$, *where secret key* $sk = r \xleftarrow{\$} \{0,1\}^m$ *and public key* $pk = y = Ar \mod q$.
- $\mathsf{Enc}(pk = (A, y), \mu) = ct$, *for ciphertext* $ct = (A^T s + e, y^T s + e' + \mu\lceil q/2 \rfloor)$.
- $\mathsf{Dec}(sk = r, ct = (c_1, c_2)) = c_2 - rc_1 = (ys + e' + \mu\lceil q/2 \rfloor) - r(As + e) = (e' - re) + \mu\lceil q/2 \rfloor \approx \mu\lceil q/2 \rfloor$.

Conceptually, for IBE, it would be useful to generate public key pk_{id} for identity id that has the form $pk_{id} = H(id)$ for some hash function H. In order to achieve this sort of scheme, the trusted authority needs a *trapdoor* that will allow him, given a desired public key pk_{id}, to obtain the correponding secret key sk_{id}. Thus, we would like the trusted authority to generate the public matrix A along with a trapdoor matrix T, using a function $\mathsf{TrapGen}$ with the following properties:

- $\mathsf{TrapGen}(1^n, 1^m, q) = (A, T) \in \mathbb{Z}_q^{n \times m} \times \mathbb{Z}^{m \times m}$, such that
- A is statistically close to uniformly random, and
- T is a short basis of $\Lambda^\perp(A)$, such that $||T||_2 = \mathsf{poly}(m)$, $AT = 0 \mod q$, and T is full-rank over $\mathbb{Z}$.

Idea 1. We would like to begin by coming up with (A, t) such that $At = 0 \mod q$, and $t \in \mathbb{Z}^m$ is short. The following seems a promising start:

$$A = \left(\overbrace{\; A^* \;}^{m^* = m-1} \mid \overbrace{\; b^* = A^* r^* \;}^{W=1} \right), \qquad t = \begin{pmatrix} r^* \\ -1 \end{pmatrix},$$

for $A^* \xleftarrow{\$} \mathbb{Z}_q^{n \times m-1}$ and $r^* \xleftarrow{\$} \{0,1\}^{m-1}$. Then $At = 0 \mod q$, and t is short (since its $\{0,1\}$ entries imply that its norm must be $O(\sqrt{m})$).

In fact, we could increase the value of W in the above construction, and thereby obtain W short vectors t_i each satisfying $At_i = 0 \mod q$ (this would involve using W corresponding vectors $r_i^* \xleftarrow{\$} \{0,1\}^{m-1}$). However, this technique will always yield m^* fewer vectors t_i than we need to construct the matrix T.

Idea 2. Let $q = 2^k$. We define the *canonical lattice* G as follows.

$$G = \overbrace{\begin{pmatrix} 1 & 2 & 4 & \cdots & 2^{k-1} & 0 & & \cdots & & 0 & & & & \cdots & \\ 0 & & \cdots & & 0 & 1 & 2 & 4 & \cdots & 2^{k-1} & & & & \cdots & \\ & & & & & & & & & & \ddots & & & & \\ 0 & & & \cdots & & & & & & 0 & 1 & 2 & 4 & \cdots & 2^{k-1} \end{pmatrix}}^{w = n \log q} \left.\vphantom{\begin{pmatrix} 1 \\ 0 \\ \\ 0 \end{pmatrix}}\right\} n$$

Note that G is full-rank, and can be expressed as the tensor product of $\begin{pmatrix} 1 & 2 & 4 & \cdots & 2^{k-1} \end{pmatrix}$ with the identity matrix.

Although G is non-random, we will find that it is still useful to define a "trapdoor" T_G for G such that $GT_G = 0$, as follows.

$$
T_G = \left.\overbrace{\begin{pmatrix}
\multicolumn{6}{c}{\overbrace{\hphantom{2\quad -1\quad 2\quad 0\quad \cdots\quad 0}}^{k}} & & & & & & & \\
2 & 0 & & \cdots & & 0 & 0 & & \cdots & & & 0 & \cdots \\
-1 & 2 & 0 & & \cdots & 0 & & & & & & & \cdots \\
0 & -1 & 2 & 0 & \cdots & 0 & \vdots & & & & & \vdots & \cdots \\
\vdots & & & & & \vdots & & & & & & & \\
0 & & \cdots & & -1 & 2 & 0 & & \cdots & & & 0 & \cdots \\
0 & & \cdots & & & 0 & 2 & 0 & & \cdots & & 0 & \cdots \\
\vdots & & & & & \vdots & -1 & 2 & 0 & & \cdots & 0 & \cdots \\
 & & & & & & \vdots & & & & & \vdots & \cdots \\
0 & & \cdots & & & 0 & 0 & & \cdots & & -1 & 2 & \cdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots
\end{pmatrix}}^{w}\right\} w
$$

Observe that we can efficiently solve ISIS for the matrix G, using the simple algorithm below.

```
Algorithm 3    ISIS SOLVER FOR CANONICAL MATRIX $G$
Let $y_i$ denote the $i^{th}$ entry of $y$, for $i = 1, \cdots, n$.
Output $e = \begin{pmatrix} \text{bit decomposition of } y_1 \\ \vdots \\ \text{bit decomposition of } y_n \end{pmatrix}$.
```

Idea 1 + Idea 2. By combining the preceding two ideas, we can achieve a construction upon which it is possible to build an IBE scheme. Note that what will be achieved below does not exactly satisfy the trapdoor requirements stated above, but what is achieved is sufficient for our purposes.

Exercise. It is possible to achieve the full trapdoor definition using these two ideas – how?

We construct A such that an efficient ISIS solver for G (which, as observed earlier, does exist) implies an efficient ISIS solver for A, as follows. To achieve this, we make use of an auxiliary trapdoor matrix $T_{A\to G} \in \mathbb{Z}^{m\times w}$ which satisfies $AT_{A\to G} = G \in \mathbb{Z}_q^{n\times w}$. Given such a $T_{A\to G}$, the following algorithm exhibits the required reduction.

```
Algorithm 4    ISIS SOLVER FOR $A$ GIVEN $T_{A\to G}$
Solve ISIS for G (using Algorithm 3) to find $r'$ such that $Gr' = y$.
Output $r = T_{A\to G}r'$.
```

Finally, we give a preliminary construction of A and $T_{A\to G}$, below. With the system as given here, there are some minor problems with proving security. In order to prove security, some small adjustments will be made to the scheme in the next lecture.

$$
A = \begin{pmatrix} \overbrace{A^*}^{m^*} & | & \overbrace{A^*R^* + G}^{w} \end{pmatrix}, \qquad T_{A\to G} = \begin{pmatrix} -R^* \\ I \end{pmatrix},
$$

where I denotes the identity matrix, for $A^* \xleftarrow{\$} \mathbb{Z}_q^{n\times m^*}$ and $R^* \xleftarrow{\$} \{0,1\}^{m^*\times w}$. Note that $A^*R^* + G$ is pseudorandom by the Leftover Hash Lemma (covered in an earlier lecture).

References

[AKS01] Miklós Ajtai, Ravi Kumar, and D. Sivakumar. "A sieve algorithm for the shortest lattice vector problem". In: *STOC*. Ed. by Jeffrey Scott Vitter, Paul G. Spirakis, and Mihalis Yannakakis. ACM, 2001, pp. 601–610. ISBN: 1-58113-349-9.

[Bab86] László Babai. "On Lovász' lattice reduction and the nearest lattice point problem". In: *Combinatorica* 6.1 (1986), pp. 1–13.

[GPV08] Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. "Trapdoors for Hard Lattices and New Cryptographic Constructions". In: *Proceedings of the 40th Annual ACM Symposium on Theory of Computing*. STOC '08. Victoria, British Columbia, Canada: ACM, 2008, pp. 197–206. ISBN: 978-1-60558-047-0. DOI: 10.1145/1374376.1374407. URL: http://doi.acm.org/10.1145/1374376.1374407.

[Kan83] Ravi Kannan. "Improved Algorithms for Integer Programming and Related Lattice Problems". In: *STOC*. Ed. by David S. Johnson et al. ACM, 1983, pp. 193–206.

[LLL82] A.K. Lenstra, Jr. Lenstra H.W., and L. Lovsz. "Factoring polynomials with rational coefficients". English. In: *Mathematische Annalen* 261.4 (1982), pp. 515–534. ISSN: 0025-5831. DOI: 10.1007/BF01457454. URL: http://dx.doi.org/10.1007/BF01457454.