Homomorphic Encryption and Lattices, Spring 2011	Instructor: Shai Halevi

Problem Set #1

March 3, 2011 — Due March 10

1 Using the Leftover Hash Lemma

The following assertion was used in the proof of security for the encryption scheme of van-Dijk et al. (the "hard core bit" proof).

Let G be a finite additive group, denote the size of G by $|G|$, and let $\ell \geq 3\log|G|$. For any fixed ℓ-vector of group elements, $\vec{x} = \langle x_1, \ldots, x_\ell \rangle$, denote by $\mathcal{S}_{\vec{x}}$ the distribution of random subset-sums of the x_i's. Namely

$$\mathcal{S}_{\vec{x}} \stackrel{\text{def}}{=} \left\{ \sum_{i=1}^{\ell} \sigma_i x_i \ : \ \text{the } \sigma_i\text{'s are uniform and independent in } \{0,1\} \right\}$$

Also denote by $\mathcal{U}_G$ the uniform distribution over G and by $SD(\mathcal{D}_1, \mathcal{D}_2)$ the statistical distance between the two distributions $\mathcal{D}_1, \mathcal{D}_2$.

Prove the following lemma, asserting that for most vectors $\vec{x}$, the distribution $\mathcal{S}_{\vec{x}}$ is close to uniform.

Lemma 1. *For any finite group G (and $\ell \geq 3\log|G|$), it holds for all but at most a $(1/\sqrt{|G|})$-fraction of the vectors $\vec{x} \in G^\ell$, that $\mathcal{S}_{\vec{x}}$ is at most $(1/\sqrt{|G|})$-away from the uniform distribution on G (in statistical distance). Namely,*

$$\Pr_{\vec{x} \in G^\ell}\left[SD(\mathcal{S}_{\vec{x}},\ \mathcal{U}_G) > \frac{1}{\sqrt{|G|}} \right] \leq \frac{1}{\sqrt{|G|}}$$

Hint. Consider the family of hash functions $\mathcal{H} = \{H_{\vec{x}} : \vec{x} \in G^\ell\}$ from $\{0,1\}^\ell$ to G, which are defined by $H_{\vec{x}}(\sigma_1, \ldots, \sigma_\ell) = \sum_i \sigma_i x_i$. Show that this is a 2-universal family of hash functions, and use the leftover-hash-lemma to show that the statistical distance between the distributions $\{(\vec{x}, H_{\vec{x}}(\vec{\sigma}))\}$ and $\{(\vec{x}, y)\}$ is at most $\frac{1}{2}\sqrt{\frac{|G|}{2^\ell}}$ (where $\vec{x} \in G^\ell$, $\vec{\sigma} \in \{0,1\}^\ell$, and $y \in G$ are all chosen uniformly at random). For each $\vec{x} \in G^\ell$, let $\delta_{\vec{x}}$ be the statistical distance between $\mathcal{S}_{\vec{x}}$ and uniform, $\delta_{\vec{x}} = SD(\mathcal{S}_{\vec{x}},\ \mathcal{U}_G)$. Interpret the leftover-lemma proof from above as a bound on the expected size of $\delta_{\vec{x}}$, and use this bound to prove the lemma.

2 Lattices and Bases

A. Discrete Additive Sets. A subset of the Euclidean space $\Lambda \subset \mathbb{R}^n$ is called *discrete* if there exists $\epsilon > 0$ such that the distance between any two points in Λ is at least ϵ. Prove that every discrete additive subset $\Lambda \subset \mathbb{R}^n$ that spans the entire space $\mathbb{R}^n$ is a full-rank lattice with a basis.

Hint. Construct a basis $b_1, \ldots, b_n$ for Λ inductively such that the following property holds for each i: If F_i is the linear span of $b_1, \ldots, b_i$ then every point $u \in \Lambda \cap F_i$ is an integer linear combination of $b_1, \ldots, b_i$. To choose the i'th vector, choose some F_i that extends F_{i-1}, prove that there exist points in $\Lambda \cap F_i$ that have minimum nonzero distance to F_{i-1}, and choose b_i to be one of them.

B. Is this a lattice?

(i) Does the set $\{1, \frac{103}{17}, 23.956\}$ span a lattice in $\mathbb{R}^1$? If so, find a basis for it.

(ii) Show an example of two real numbers that *do not span a lattice in* $\mathbb{R}^1$.

3 q-ary Lattices

A. Let $A \in \mathbb{Z}^{m\times n}$ be a (not necessarily square) integer matrix, and let $q \in \mathbb{Z}$ be an integer larger than one. Prove that the set $S = \{x \in \mathbb{Z}^n : Ax \equiv 0 \pmod{q}\}$ is a full-rank lattice.

B. Find a basis for the lattice $\Lambda = \{x \in \mathbb{Z}^3 : x_1 + 4x_2 - x_3 \equiv 0 \pmod{10}\}$.