Homomorphic Encryption and Lattices, Spring 2011	Instructor: Shai Halevi
Problem Set #5	
June 2, 2011	due June 16

1 Simple Decryption Modulo p

Recall that if we wanted to use the Gentry-Halevi variant as-is with plaintext space $\mathbb{Z}_p$ for some $p > 2$ (co-prime with d), then decryption using the secret key $w \in \mathbb{Z}_d$ would become $[cw]_d \cdot \mu \bmod p$ where $\mu = w^{-1} \pmod p$. Also, in this case it is unlikely that we get $d \equiv 1 \pmod p$. The purpose of this question is to demonstrate how to find another modulus d' and secret key $w' \in \mathbb{Z}_{d'}$ such that $d' \equiv 1 \pmod p$ and decryption can be implemented as $[w' \cdot c]_{d'} \bmod p$.

Notations and facts. If $m, y, z \in \mathbb{Z}$, then $y \stackrel{m}{\equiv} z$ denotes the fact that y, z are congruent modulo m. The same fact is sometimes also denoted $y \equiv z \pmod m$. If z, m are co-primes then $(z^{-1} \bmod m)$ is the unique integer $y \in [0, m)$ such that $yz \equiv 1 \pmod m$. For integers z, m, denote the reduction of z modulo m by $[z]_m$, where this operation maps integers to the interval $[-m/2, m/2)$. The notation "$z \bmod m$" denotes the operation that maps integers to the interval $[0, m)$.

For a rational number q, denote by $\lceil q \rfloor$ the rounding of q to the nearest integer, and by $[q]$ the distance between q and the nearest integer, $[q] = q - \lceil q \rfloor$. These notations are extended to vectors and matrices in the natural way: for example if $\vec{q} = \langle q_0, q_1, \ldots, q_{n-1} \rangle$ is a rational vector then rounding is done coordinate-wise, $\lceil \vec{q} \rfloor = \langle \lceil q_0 \rfloor, \lceil q_1 \rfloor, \ldots, \lceil q_{n-1} \rfloor \rangle$.

The notations $\|\vec{x}\|$, $\|\vec{x}\|_\infty$, $\|\vec{x}\|_1$ denote the Euclidean norm, l_∞ norm, and l_1 norm of the vector $\vec{x}$. For a matrix A, denote by $\|A\|$, $\|A\|_\infty$, $\|A\|_1$ the Euclidean, l_∞, l_1 norms of the largest columns of A, respectively. Here are some facts that may be useful for solving the following questions:

- If $q = y/z$ (with $y, z \in \mathbb{Z}$) then $z \cdot [q] = [y]_z = [zq]_z$.
- If m, y, z are integers such that $y/z \in \mathbb{Z}$ and z is co-prime with m, then $y/z \stackrel{m}{\equiv} y \cdot (z^{-1} \bmod m)$. In words, the integer y/z is congruent modulo m to the integer y times $(z^{-1} \bmod m)$.

Keys, encryption, decryption. Recall that in the Gentry-Halevi variant, an integer polynomial $\vec{v}$ is chosen as $\vec{v} = \vec{s} + (\tau, 0, \ldots, 0)$ where s is a random integer vector with entries bounded by σ (whp), with σ and τ parameters. The rotation basis V of $\vec{v}$ is the "good basis" of the underlying GGH cryptosystem, and its scaled inverse is denoted W (i.e., $WV = dI$, where $d = \mathsf{det}(V)$). Importantly, W is an integer matrix, and it is the rotation basis of the scaled inverse $\vec{w} = d \cdot \vec{v}^{-1}$ (where inverse is taken in the field of rational polynomials modulo $x^n + 1$).

The (implicitly represented) encryption procedure for a plaintext $m \in \mathbb{Z}_p$ consists of choosing a random integer vector $\vec{a}$ with entries bounded whp by ρ (which is another parameter), setting the "error vector" $\vec{e} = p\vec{a} + \vec{m}$ (where $\vec{m} = (m, 0, \ldots, 0)$) and then reducing $\vec{e}$ modulo the "bad basis" of $\Lambda(V)$ in the public key. Hence a ciphertext is a vector $\vec{c} = \vec{v} + \vec{e}$ for some lattice vector $v \in \Lambda(V)$ and the error vector above. Moreover, the structure of the public basis in this variant is such that the vector $\vec{c}$ has a special form $\vec{c} = (c, 0, \ldots, 0)$.

As described in class, the secret key consists of the (implicitly represented) matrices V and W. Below you need to show that one can also use some other matrices. Specifically, consider the following matrices:

- Let $A = (W^{-1} \bmod p)$. Namely $A \in \mathbb{Z}_p$ and $AW \equiv I \pmod{p}$. Then let $B = [d \cdot A]_p$ (i.e., multiply A by the integer $d = \mathsf{det}(V)$ and reduce mod p to the interval $[-p/2, p/2)$).
- Let $S = V^{-1}B$, where V^{-1} is the inverse of V over the reals. S is therefore a rational matrix.
- Let $d' = d \cdot (d^{-1} \bmod p)$ and $U = d'S$, with multiplication over the integers/reals.

The questions below establish that if $c \in \mathbb{Z}_d$ is an encryption of $m \in \mathbb{Z}_p$ and u is the upper-left element in U, then $[uc]_{d'} \equiv m \pmod{p}$.

A. Prove that the matrix W has an inverse mod p (hence the matrices above are well defined). Prove also that the matrix S is invertible over the reals.

B. Prove that the largest entry of S in absolute value is at most pn times larger than in V^{-1}.

C. Prove that $U \equiv I \pmod{p}$.

D. Let $\vec{c}$ be a ciphertext, $\vec{c} = \vec{v} + \vec{e}$, for some lattice vector $\vec{v} \in \Lambda(V)$, and some integer error vector $\vec{e} \in \mathbb{Z}^n$ such that $\|\vec{e}\| < 1/2\|S\|$. Prove that $[\vec{c}S] = \vec{e}S$, and deduce that the two vectors $[\vec{c}S]S^{-1}$ and $\lceil \vec{c}S \rfloor S^{-1}$ are both integer vectors. (Here S^{-1} is the inverse of S over the reals.)

E. Prove that $\lceil \vec{c}S \rfloor \equiv \lceil \vec{c}S \rfloor S^{-1} \pmod{p}$.

F. Deduce that $\vec{e} \equiv \vec{c} - \lceil \vec{c}S \rfloor \pmod{p}$.

G. Prove that $d'[\vec{c}S] = [\vec{c}U]_{d'}$.

H. Deduce that $\vec{e} \equiv [\vec{c}U]_{d'} \pmod{p}$.

I. Conclude that if the ciphertext $\vec{c}$ is of the form $\vec{c} = (c, 0, \ldots, 0)$, and the error vector satisfies $\vec{e} \equiv (m, 0 \ldots, 0) \pmod{p}$, then $[u_0 c]_{d'} \equiv m \pmod{p}$ (where u_0 is the top-left entry in U).

J. Suggest a setting for the parameters σ, τ, ρ (as a function of p, n), so that the cryptosystem with the modified decryption procedure $\mathrm{Dec}_u(c) = ([uc]_{d'} \bmod p)$ still supports homomorphic evaluation of polynomials of degree $2|p|$ with (say) upto $n^{2|p|}$ terms. Make sure that your suggested parameters are not broken by known lattice-reduction algorithms.

2 Elementary Symmetric Polynomials

Let $e_k(x_1, \ldots, x_n)$ be the degree-k elementary symmetric polynomial in n variables over some field K. Prove that for any $v_1, \ldots, v_n \in K$, the value $e_k(v_1, \ldots, v_n)$ equals the coefficient of z^{n-k} in the univariate polynomial $P_{\vec{v}}(z) = \prod_{i=1}^{n}(z + v_i)$.

3 El-Gamal Decryption

Let $p = 2q+1$ be a safe prime and let $g \in \mathbb{Z}_p$ be a generator of $QR(p)$, the group of quadratic residues mod P. Let $e \in \mathbb{Z}_q$ be an El-Gamal secret exponent and $h = g^{-e} \bmod p$ the corresponding public key. Let $e_{n-1} \ldots e_1 e_0$ be the binary representation of e, i.e., $e = \sum_{i=0}^{n} e_i 2^i$. Also, let $m \in QR(p)$ and let (y, z) be an encryption of m with respect to the public key g, h. I.e., $y = g^r \bmod p$ and $z = mh^r \bmod p$ for some $r \in \mathbb{Z}_q$.

Show that El-Gamal decryption can be computed by a degree-n polynomial in the bits of the secre key. Namely, show how to efficiently compute from (y, z) an explicit description of a multilinear polynomial $Q(x_0, \ldots, x_{n-1})$, such that $Q(e_0, \ldots, e_{n-1}) \bmod p = m$.

Hint. Show that the value $y^{e_i 2^i}$ (with e_i a bit) can be expressed as a linear expression in e_i.