Homomorphic Encryption and Lattices, Spring 2011	Instructor: Shai Halevi
Problem Set #4	
May 5, 2011	due May 12

More Learning with Errors

1 The Distribution of the Secret $\vec{s}$

Prove that the decision problem D-LWE$[n, \alpha, q]$ remains just as hard if the secret is chosen from the error distribution (rounded and reduced mod q), $\vec{s} \leftarrow \lceil \Phi_{\alpha q} \rfloor^n \bmod q$, rather than being chosen at random in $\mathbb{Z}_q$. Namely, prove that an efficient distinguisher of D-LWE$[n, \alpha, q]$ in the case where $\vec{s}$ is chosen as above implies also an efficient distinguisher with the same advantage when $\vec{s}$ is chosen uniformly at random.

Hint. Given n samples $(\vec{a_i}, b_i)$, $i = 1, \ldots, n$ consider a matrix $A \in \mathbb{Z}_q^{n \times n}$ with the $\vec{a_i}$'s as columns, and the corresponding vector $\vec{b}$ with the b_i's as entries. Namely $\vec{b} = A\vec{s} + \vec{x}$ where $\vec{x} \leftarrow \lceil \Phi_{\alpha q} \rfloor^n \bmod q$. Assume that A is invertible modulo q. Then for a new sample $(\vec{a}, b)$, consider the transformation

$$f_{A,\vec{b}}(\vec{a}, b) = (-(A^t)^{-1}\vec{a}, \quad b - \langle (A^t)^{-1}\vec{a}, \vec{b} \rangle)$$

(where the arithmetic is modulo q).

2 Another Quadratic-Homomorphic Cryptosystem

The GHV cryptosystem [GHV10] that we saw in class is based on the *dual Regev cryptosystem* of Gentry-Peikert-Vaikuntanathan [GPV08]. The goal here is to construct a different quadratic homomorphic scheme from Regev's original LWE-based scheme [Reg09].

Below we have the usual parameters n, α, q and m, such that $q = \mathsf{poly}(n)$ (q odd), $\alpha = 1/\mathsf{poly}(n) \ll 1/\sqrt{q}$, and $m \geq 3n \log q$. Security of this cryptosystem will be based on the hardness of the decision problem D-LWE$[n, \alpha, q]$.

- The secret key is a short vector $\vec{v} \in \mathbb{Z}_q^{n+1}$ such that the last entry is 1, $v[n+1] = 1$. The first n entries of $\vec{v}$ are chosen at random in $\mathbb{Z}_q^n$, namely $\vec{v} = (\vec{s}|1)$ for a random $\vec{s} \in_R \mathbb{Z}_q^n$.
- The public key is an $(n+1) \times m$ matrix $P = (\frac{A}{\vec{b}})$, where A is a uniformly random matrix $A \in_R \mathbb{Z}_q^{n \times m}$ and $\vec{b} = -\vec{s}A + 2\vec{e} \bmod q$. Here $\vec{s}$ is the "secret part" of the secret key and $\vec{e}$ is chosen from the error distribution $\vec{e} \leftarrow \lceil \Phi_\alpha \rfloor^m \bmod q$. (Note that $\vec{v}P = \vec{s}A + \vec{b} = 2\vec{e} \pmod q$.)
- To encrypt a bit $m \in \{0, 1\}$ with public key $P = (\frac{A}{\vec{b}})$, choose a random 0-1 vector $\vec{r} \in_R \{0, 1\}^m$ and the ciphertext is $\vec{c} = P \times \vec{r} + (0, 0, \ldots, 0, m) \bmod q \in \mathbb{Z}_q^{n+1}$.
- To decrypt a ciphertext $\vec{c}$ using secret key $\vec{v}$, compute $m = (\langle \vec{v}, \vec{c} \rangle \bmod q) \bmod 2$.

A. Prove that for some setting of the parameters α, q, m from above, decryption indeed recovers the correct bit m with high probability.

B. Prove that if the decision problem D-LWE$[n, \alpha, q]$ is hard, then this scheme is CPA-secure. (*Hint.* What would have happened if P was a uniformly random matrix in $\mathbb{Z}_q^{(n+1) \times m}$?)

C. Prove that for some setting of the parameters α, q, m from above, and another parameter ℓ, the sum mod q of upto ℓ ciphertext vectors is decrypted to the sum mod 2 of the corresponding plaintext bits with high probability.

D*. Consider two ciphertexts $\vec{c_i} = P \times \vec{r_i} + (0, 0, \ldots, 0, m_i) \bmod q$, where $\vec{c_i}$ encrypts the bit m_i for $i = 1, 2$. Denote the tensor (outer) product of these two ciphertext vectors (mod q) by $C = \vec{c_1} \otimes \vec{c_2} \bmod q \in \mathbb{Z}_q^{(n+1)\times(n+1)}$. Namely, $C_{i,j} = c_1[i] \cdot c_2[j] \bmod q$.

Describe a decryption procedure that uses the secret key $\vec{v}$ to recover the product of the plaintext bits $m_1 \cdot m_2$ mod 2 from the "product ciphertext" C. (*Hint.* Recall that for four vectors $\vec{a}, \vec{b}, \vec{c}, \vec{d}$ of matching dimensions, it holds that $\vec{a} \times (\vec{b} \otimes \vec{c}) \times \vec{d} = \langle \vec{a}, \vec{b} \rangle \cdot \langle \vec{c}, \vec{d} \rangle$.) How would you set the parameters so that this procedure succeeds with high probability?

E**. Can you extend this cryptosystem to operate on binary matrices as plaintext, using mod-q matrices of the same dimensions as ciphertext? (This will reduce the plaintext-to-ciphertext expansion by a factor of m compared to the scheme above.)

Note: I don't know if this is possible, but it will be interesting if it is.

References

[GHV10] Craig Gentry, Shai Halevi, and Vinod Vaikuntanathan. A Simple BGN-type Cryptosystem from LWE. In *Advances in Cryptology - EUROCRYPT'10*, volume 6110 of *Lecture Notes in Computer Science*, pages 506–522. Springer, 2010. Full version available on-line from `http://eprint.iacr.org/2010/145`.

[GPV08] Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In *STOC'08*, pages 197–206. ACM, 2008.

[Reg09] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. *JACM*, 56(6), 2009.