6.5630 Advanced Topics in Cryptography

Problem Set 3

Optional PSET, No Due Date

This problem set has a single problem.

Breaking Functional Encryption. Recall the construction of a predicate encryption scheme supporting the *orthogonality predicate* (alternatively, linear functions with equality test) from the LWE assumption (see Lecture 8 notes, section 3). Such a function is defined by a vector $y \in \mathbb{Z}_q^L$, takes as input $x \in \mathbb{Z}_q^L$ and outputs 1 if

$$\langle y, x \rangle = 0 \bmod q$$

We showed in class that this construction is secure as a weakly hiding predicate encryption. That is, an adversary who gets secret keys corresponding to a number of vectors (linear functions) $y_1, \ldots, y_k$ for a polynomially large k such that

$$\langle x, y_i \rangle \neq 0 \bmod q \text{ for all } i \ ,$$

cannot learn anything about x. Your task is to break this scheme when playing the strong hiding game. That is, when the challenge is (x, x') such that $\langle x, y_i \rangle = \langle x', y_i \rangle \bmod q$ for all i (but some of the inner products could be 0).

Concretely, you task is to design queries y_i such that the outputs $\langle x, y_i \rangle \bmod q$ does not reveal x, yet a ciphertext $\mathsf{Enc}(\mathsf{mpk}, x)$ together with the secret keys $\mathsf{sk}_{y_1}, \ldots, \mathsf{sk}_{y_\ell}$ completely reveals x.