Department of Electrical and Computing Engineering

UNIVERSITY OF CONNECTICUT

CSE 5095-004 (15626) & ECE 6095-006 (15284)
Secure Computation and Storage: Spring 2016

Oral Exam: Theory

There are three problem classes in this oral exam booklet. During your oral exam you will be given this booklet and the instructor will select exactly one problem (at random) out of each class for you to solve in front of the white board. You have **45 minutes** to answer all three questions.

Be neat and legible. If the instructor can't understand your answer, no credit is given! 20% of the grade for each question concerns clear exposition by using the white board and oral explanation.

Write your name in the space below. Write your initials at the bottom of each page.

THIS IS A CLOSED BOOK ORAL EXAM

Do not write in the boxes below

1 (xx/100)	**2 (xx/100)**	**3 (xx/100)**	**Total (xx/300)**

Name:

Student ID:

1. [100 points]: Lattice theory: I will ask you (random choice) one out of the following three questions:

(a) Prove:

(a) Let Δ be a lattice of rank n and let $\{b_i\} \subseteq \Delta$ be n linearly independent lattice vectors. Show that $\{b_i\}$ forms a basis of Δ if and only if $P(b_1, \ldots, b_n) \cap \Delta = \{0\}$.

(b) If U is unimodular, then U^{-1} is also unimodular with only integer matrix entries.

(c) Two bases B_1 and B_2 are equivalent if and only if $B_2 = B_1 U$ for some unimodular matrix.

(d) The determinant of a lattice is well-defined.

(b) Prove the theorem of Blichfeld and Minkowski's convex body theorem:

(a) What do the theorems state?

(b) Prove: If, for all x and y, $\hat{S}_x \cap \hat{S}_y = \emptyset$, then $\sum_{x \in \Delta} vol(\hat{S}_x) \leq vol(P(B))$.

(c) Show $\sum_{x \in \Delta} vol(\hat{S}_x) > vol(P(B))$ and prove Blichfeld.

(d) Conclude Minkowski's convex body theorem.

Initials:

(c) Prove Minkowski's second theorem:

(a) State the theorem.

(b) Define T and explain why T represents an ellipsoid.

(c) Define y and show that $y \notin span(x_1, \ldots, x_k)$ leads to a contradiction.

(d) Conclude $y \in span(\tilde{x}_1, \ldots, \tilde{x}_k)$ and explain why this is a result of Gram-Schmidt orthogonalization.

(e) Prove $y \notin T$.

(f) Show (by applying Minkowski's convex body theorem) a lower bound on $vol(T)$ from which the theorem immediately follows.

Initials:

2. [100 points]: LLL Algorithm & LWE: I will ask you (random choice) one out of the following two questions:

(a) LLL Algorithm:

(a) What is a δ-LLL reduced basis?

(b) Write out the LLL algorithm.

(c) Which property of an LLL reduced basis is taken care of by the swap step and why?

(d) Show that throughout the reduction step the Gram-Schmidt basis does not change. (And as a consequence explain that the output of the algorithm is indeed a basis for $L(B)$.)

(e) Let $i > j$ and consider the jth iteration of the inner loop in the ith iteration of the outer loop: Show that $|\mu_{i,j}| \leq 1/2$. (This proves correctness of the LLL algorithm if it terminates.)

(f) Define the potential D_B and explain why it does not change through the reduction step.

(g) Suppose b_i is swapped with b_{i+1} and prove $D'_{B,i}/D_{B,i} < \sqrt{\delta}$.

(h) Conclude that the number of iterations through the outer loop is polyniomial in the input size.

(i) Just mention what else needs to be shown in order to prove that the LLL algorithm is polynomial in the input size.

(b) LWE problem:

(a) Define $LWE_{n,m,q,\chi}$ in matrix form.

(b) State the decisional LWE assumption. Why are we (in crypto) more interested in the decisional LWE assumption?

(c) Show a reduction from search to decisional LWE: What is the approach (show that if $s_i = g_i$ then a LWE input is generated and if $s_i \neq g_i$ then a random input is generated; why is a random vector c_l needed in the algorithm)?

(d) Prove that if there is an efficient decider for average-case decisonal LWE, then there exists an efficient decider for worst-case decisonal LWE? Why is this and important result if we want to base crypto primitives on decisional LWE?

(e) Describe a public-key encryption scheme based on LWE.

(f) Show correctness.

(g) Show a hybrid arument proving its security (do define statistical distance and you may state without proof the Leftover Hash Lemma).

Initials:

3. [100 points]: Fully Homomorphic Encryption (FHE) and LPN-based PUFs: I will ask you (random choice) one out of the following three questions:

(a) FHE:

(a) What does it mean for a circuit to be C-homomorphic? What is the definition of fully homomorphic?

(b) Present a first simple "non-encryption" scheme (encryption and decryption) where the public key is a random $n \times n$ matrix P with rank $< n$ and where the secret key is a vector s such that $sP = 0 \mod q$. Show how addition and multiplication work and explain why this is not secure.

(c) Tweak the scheme so that $sP \approx 0 \mod q$ (show encryption and decryption). Explain how decryption works and why R should have small entries as a result. Show how addition and multiplication work and why multiplication amplifies the size of the error term too much.

(d) Why is this scheme still not semantically secure (i.e., one can distinguish with non-negligible bias a ciphertext for 0 versus a ciphertext for 1)?

(e) Give the approximate eigenvector encryption scheme (encryption, decryption, and addition). Give intuition why this scheme is semantically secure.

(f) Explain G^{-1}; show how multiplication works; how is the error term bounded?; the distribution of the error term for a ciphertext as a result of evaluating a multiplication or addition is not any more distributed according to the original distribution χ, why is this not a problem?

(g) Explain bootstrapping; why is "circular encryption" introduced as an extra assumption?

Initials:

(b) Reduction worst-case decisional LWE to worst-case BDD:

(a) LWE-Generate(B, x) performs the following steps:

- Sample the discrete Gaussian distribution with parameter r over lattice L^* (assume a polynomial time sampler which is indistinguishable from the actual sampler exists): Let y be the result.
- Compute $y = B^* a$, i.e., $a = B^T y$.
- Compute e as output from a continuous one-dimensional Gaussian as a projection of the spherical n dimenional Gaussian distribution with parameter $\alpha q/(2\sqrt{\pi})$.
- Output $(a \mod q, b = \langle x, y\rangle + [e] \mod q)$ (brackets represent rounding).

Explain the terminology used in this algorithm.

(b) We want to show that LWE-Generate is statistically close to the LWE distribution with secret $s = t \mod q$, where $v = Bt \in L$ is the closest point in L to input x, and with noise parameter $\beta \leq \alpha$ (i.e., the bound on the norm of the error vector is at most βq): First show that $a \mod q$ is close to uniform in the ring of integer vectors of length n modulo q. You will only need to give intuition using pictures.

(c) Next prove that for fixed q, $b = \langle s, a\rangle + [e']$ for some output from a continuous one-dimensional Gaussian as aprojection of the sperical n dimenional Gaussian distribution with parameter $\beta q/(2\sqrt{\pi})$ (where $\beta \leq \alpha$ and is independent the coin flips in LWE-Generate). Start by showing that $b = \langle s, a\rangle + \langle w, y\rangle + e \mod q$ where $w = x - v$.

(d) Now show that $e = \langle w, z'\rangle$ with z' sampled from the sperical n dimensional Gaussian distribution with parameter $\alpha q/(2\sqrt{\pi}|w|)$.

(e) Explain what it means for a Gaussian distribution to be smooth and show how this proves $\langle w, y\rangle + e = \langle w, y + z\rangle$ with $y + z$ indistinguishable from the n dimensional Gaussian distribution with parameter $t = \sqrt{r^2 + (\alpha/(2\sqrt{\pi}|w|))^2}$.

(f) Give intuition why the proof is pretty much completed.

Initials:

(c) LPN-based PUFs:

(a) What is a PUF? Give an example. Why are we interested in stateless PUFs?

(b) What is the LPN problem and how does it relate to LWE?

(c) Draw GenPOK and VerPOK. Explain the basic idea being explored.

(d) Explain inter and intra distributions; define stable bits and derive a lower bound on the probability of a bit being stable as a function of the intra and inter distributions and ϵ_2 (expresses stability); derive a lower bound on m (the number of equations) as a function of ϵ_1 (representing the maximum failure probability), ϵ_2, and m'; how should ϵ_2 and m' be chosen?; show polynomial time recovery with negligible failure probability ϵ_1.

(e) Explain the correlation lemma (VI.2) and give its proof

(f) Give intuition (in global somewhat vague steps) on how breaking the LPN-based PUF reduces to breaking LPN.

(g) Explain why the above is not exactly what we want, and give inutuition on how the paper attempts to solve this.

Initials:

End of Oral Exam

Please double check that you wrote your name on the front of the quiz.

Initials: