MIT 6.5620/6.875/18.425: Foundations of Cryptography **Due: Dec. 2, 2026**

Problem Set 5

Total Number of Points: 80.
Instructions: Solutions should be typeset in LaTeX and submitted as PDF by 11:59:59 PM ET on the due date. You can collaborate on the psets in small groups (of up to three), but must write your solutions separately, in your own words. This means not copying from a board nor from your collaborator's computer.

We strongly recommend ***not*** using AI tools to solve your problem sets. You are responsible for understanding everything you submit and you must be able to explain and justify every part of your solution. In particular, the oral problem set review (10% of the course grade) will evaluate your understanding of the solutions you submit. In all cases, you must list your collaborators, human or machine.

Problem 1. Zero Knowledge Proof for Knight's Move Sudoku (20 points)

Knight's Move Sudoku is a variant on the popular logic puzzle Sudoku. For a Knight's Move Sudoku puzzle for positive integer n, you are given as input an $n^2 \times n^2$ grid of cells, where the cells are partitioned into n^2 disjoint $n \times n$ subgrids. Some of the cells begin filled with integers from 1 to n^2.

A solution is a way to assign an integer from 1 to n^2 to each cell which hasn't already been filled in a way that:

1. Each row contains each of the integers from 1 to n^2 exactly once.
2. Each column contains each of the integers from 1 to n^2 exactly once.
3. Each of the n^2 different $n \times n$ subgrids contains each of the integers from 1 to n^2 exactly once.
4. For all cells that are a "knight's move" away from each other, the entries are distinct. Two cells $(i_1, j_1) \in [n^2] \times [n^2], (i_2, j_2) \in [n^2] \times [n^2]$ are a "knight's move" away if either (a) $|i_1 - i_2| = 1$ and $|j_1 - j_2| = 2$ or (b) $|i_1 - i_2| = 2$ and $|j_1 - j_2| = 1$.

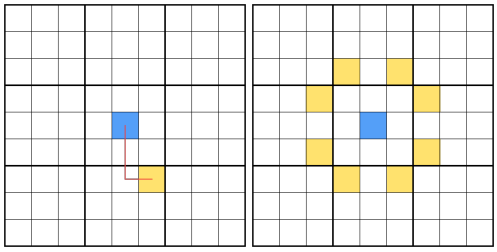


Figure 1: An example demonstrating what a "knight's move" is, for $n = 3$, from here.

Design a zero-knowledge protocol for Knight's Move Sudoku. Your construction should exploit the structure of the puzzle; simply invoking the general theorem that every language in NP has a zero-knowledge proof is not sufficient. Your protocol should be computationally zero knowledge, have perfect completeness, and can have soundness error up to $1 - p(n)$ for a non-negligible p. You must prove that your construction satisfies all of the above properties. You may assume the existence of one-way functions.[1]

[1] **Hint:** One possible approach is for the prover to take a valid solution, apply a uniformly random permutation to the labels $[n^2]$, and commit to the resulting value in each cell. The verifier can then choose a random row, column, or subgrid, ask the prover to open the corresponding commitments, and check that all values in $[n^2]$ appear exactly once. Notice that such a check reveals only a random permutation of $[n^2]$, which is useful for zero knowledge. However, these checks alone are not sufficient for soundness. Think about how to additionally verify consistency with the originally filled cells and the knight's-move constraint, without revealing the solution.

Problem 2. Secret Sharing, Generalized (30 points)

Recall the notion of threshold secret sharing: given n users (numbered 1 through n), define the (t, n)-threshold access structure to be the collection of sets

$$\mathcal{A}_{\text{threshold}} = \{S \subseteq [n] : |S| \geq t\}$$

A secret sharing scheme must satisfy two properties: every set $T \in \mathcal{A}_{\text{threshold}}$ can reconstruct the secret from its shares, while every set $T \notin \mathcal{A}_{\text{threshold}}$ learns no information about the secret.

In this problem, we will generalize secret sharing to other access structures. In general, an access structure $\mathcal{A}$ is a monotone collection of subsets of $[n]$. Here, monotonicity refers to the condition that if $\mathcal{A}$ contains a set T, it also contains all supersets of T. (Do you see why this has to be the case?)

- We will associate to a subset $T \subseteq [n]$ its characteristic vector $x_T \in \{0,1\}^n$. For example, letting $n = 4$ and $T = \{1, 3\}$, we have $x_T = (1010)$.
- We will associate to an access structure $\mathcal{A}$ a (monotone) Boolean function $f_{\mathcal{A}} : \{0,1\}^n \to \{0,1\}$ where

  $$T \in \mathcal{A} \text{ if and only if } f_{\mathcal{A}}(x_T) = 1 \ .$$

  For example, in the case of the threshold access structure, $f_{\mathcal{A}}$ is simply the threshold function which outputs 1 if and only if the input has at least t ones.

(a) (15 points) Let $n = 3^m$ be the number of parties, and let the hierarchical access structure be defined by the majority-of-majorities function (see Figure 2 for an example with $m = 2$ and $n = 9$). Construct a secret sharing scheme for the hierarchical access structure on $n = 3^m$ users for arbitrary depth m. The shares in your scheme should have bit-length polynomial in n.

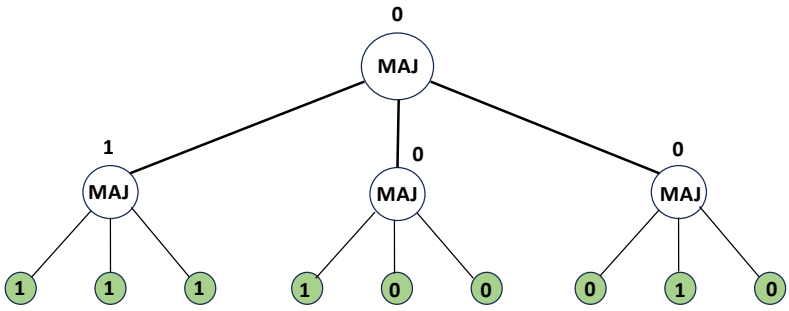


Figure 2: The function f representing a hierarchical access structure on 9 users. A set of users corresponds to a Boolean labeling of the leaves. For example, the labeling of the leaves above corresponds to the set of users $T = \{1, 2, 3, 4, 8\}$. An internal node is labeled 1 if and only if the majority of its children are labeled 1. A given set is in the access structure if and only if the root is labeled 1. (In this case, since the root has label 0, T is not in the access structure.)

(b) (15 points) Let the conjunctive normal form (CNF) access structure be defined by a monotone CNF formula Ψ with n variables and m clauses (monotone in the sense that the formula has no negations). Construct a secret sharing scheme for the CNF access structure. The shares in your scheme should have bit-length polynomial in n and m.

Problem 3. Oblivious Transfer Pro Max (30 points)

In a 1-out-of-2 Oblivious Transfer (OT) protocol, a sender has two message bits $m_0, m_1 \in \{0,1\}$, and a receiver has a choice bit $b \in \{0,1\}$. The sender wants to send m_b to the receiver while satisfying correctness (the receiver obtains m_b), sender's privacy (the receiver gains no knowledge about the message m_{1-b}), and receiver's privacy (the sender gains no knowledge about the choice bit b).

In this problem, we focus on achieving security against *honest-but-curious* senders and receivers.

(a) (10 points) Show how you can use any 1-bit OT scheme to build an ℓ-bit OT scheme for transferring ℓ-bit messages $m_0, m_1 \in \{0,1\}^\ell$. Here $\ell = \ell(\lambda)$ is a (possibly large) polynomial in security parameter λ. Your scheme can only invoke the given 1-bit OT scheme at most λ times. You can assume the existence of a pseudorandom generator.

(b) (20 points) A 1-out-of-n oblivious transfer (OT) scheme is one where the sender has n messages $m_0, \ldots, m_{n-1} \in \{0,1\}^\ell$ and the receiver wants the i^{th} message m_i.

Assume $\ell \geq \lambda$, where λ is the security parameter. You are given a 1-out-of-2 OT scheme with ℓ-bit messages. Show how to construct a 1-out-of-n OT scheme for any integer $n \geq 2$. You can assume the existence of a PRF family. For full credit, your scheme must invoke the 1-out-of-2 OT scheme at most $O(\log n)$ many times.