Partie cours :

Les éléments d’un système électroniques, par exemple un téléphone sont les suivants :

* Processeur CPU qui fait les calculs
* Mémoire de stockage (Flash, EEPROM, ROM). Certaines mémoires sont réinscriptibles d’autres non (voir cours).
* Mémoire vive (RAM) qui est volatile
* PMU qui gère les tensions d’alimentation
* Baseband qui gère les communications d’un téléphone)
* PCB composé de pistes et de vias assurant les connexions entre les composants.

Les composant actifs, donc utilisant la technologie CMOS, sont constitués de l’élément le plus simple, la jonction PN qui n’est autre qu’une diode. En direct la diode est passante et en inverse elle est bloquée. A partir de cet élément, il est possible de créer un transistor fonctionnant en bloqué ou passant (voir les schémas de fonctionnement des transistors). Le transistor est composé d’une grille servant à piloter le transistor ainsi que de deux “pôles” nommés drain et source. Lorsqu’on parle de transistor NMOS (voir schéma dans le cours) les zones dopées du drain et de la source sont en N et le caisson est en P.

* Si on applique un ‘0’ logique sur la grille, le transistor reste bloqué donc équivalent à un interrupteur ouvert qui bloque le courant.
* Si on applique un ‘1’ logique sur la grille, un champ se crée entre le drain et la source permettant le passage du courant entre les deux. Le transistor est passant donc équivalent à un interrupteur fermé qui laisse circuler le courant.

Pour le transistor PMOS, c’est l’inverse. Les drains et sources sont reliées à du P alors que le caisson est en N. Un ‘0’ logique ferme le transistor alors qu’un ‘1’ logique l’ouvre.

Comme le montre le cours, si un transistor PMOS et un transistor NMOS sont combinés, il est possible de créer une fonction simple d’inversion qui transforme un ‘1’ en entrée en ‘0’ en sortie, et inversement.

Relire également le fonctionnement global des équipements de laboratoire et être capable de décrire leur utilité. Pour rappel, les équipements sont regroupés en quatre catégories :

* Préparation physique : Laser, Chimie, Plasma et Polissage
* Observation : Microscope électronique à balayage (ainsi que le phénomène autour des électrons et leurs noms), Machine à rayons-X
* Interaction avec la matière : FIB, Probes station, Box de lecture
* Attaque par canaux auxiliaires : Electromagnétique, Laser

NB : Aucune question ne sera posée sur les attaques par canaux auxiliaires !

Partie manip :

Revoir la structure interne d’une carte SIM et d’une carte microSD (les différents éléments qui les composent)

Réviser les trois protocoles décrits dans vos rapports (tests de diodes, Réparation de fils de bondings, snif de protocole SD).

Réviser le protocole SD utilisé lors de l’échange entre un PC et une carte microSD (nombre de broches utilisées, nom des signaux, fonction des signaux...).