# Corrigés des exercices

## Exercice 1 - Question 1 (MCQ)

Sur quel phénomène physique repose principalement le protocole E91 ?

Réponse : L'intrication quantique

Explication : Le protocole E91 (Ekert 1991) utilise des paires de particules intriquées pour établir une clé sécurisée.

## Exercice 1 - Question 2 (MCQ)

Qui a proposé le protocole E91 ?

Réponse : Artur Ekert

Explication : Comme mentionné dans le cours, Artur Ekert a proposé ce protocole en 1991.

## Exercice 1 - Question 3 (MCQ)

Quelle est la valeur maximale de l'inégalité de Bell (S) en physique classique ?

Réponse : 2

Explication : Selon les inégalités de Bell, la limite classique pour la valeur S est 2.

## Exercice 1 - Question 4 (MCQ)

Quelle valeur de S prouve la présence d'intrication en mécanique quantique ?

Réponse : $S = 2\sqrt{2}$

Explication : En mécanique quantique, la violation de l'inégalité de Bell est représentée par la valeur $2\sqrt{2}$.

## Exercice 1 - Question 5 (MCQ)

Dans l'état $|\Psi\rangle = 1/\sqrt{2}\ (|00\rangle + |11\rangle)$, que se passe-t-il si Alice mesure 0 ?

Réponse : Bob mesure forcément 0

Explication : L'état intriqué assure une corrélation parfaite : si Alice obtient 0, Bob obtiendra également 0.

## Exercice 2 - Question 1 (MCQ)

Que signifie l'acronyme CV-QKD ?

Réponse : Continuous Variable Quantum Key Distribution

Explication : CV-QKD signifie Cryptographie quantique à variables continues.

## Exercice 2 - Question 2 (MCQ)

Quelles variables de la lumière sont utilisées dans la CV-QKD ?

Réponse : L'amplitude et la phase
Explication : Alice encode l'information en modulant continûment l'amplitude et la phase (quadratures X et P).

### Exercice 2 - Question 3 (MCQ)

Quelle technique de détection est utilisée par Bob en CV-QKD ?
Réponse : Détection homodyne
Explication : Bob utilise des techniques d'optique classique comme la détection homodyne pour mesurer les quadratures.

### Exercice 2 - Question 4 (MCQ)

Quelle distribution statistique est suivie par les quadratures en CV-QKD ?
Réponse : Loi Gaussienne
Explication : Alice module les quadratures selon une loi gaussienne.

### Exercice 2 - Question 5 (MCQ)

Quel est l'impact d'un espion sur le signal en CV-QKD ?
Réponse : Il introduit un bruit excédentaire
Explication : Toute tentative d'interception augmente la variance du bruit mesuré par Bob.

### Exercice 3 - Question 1 (MCQ)

Dans le circuit Qiskit fourni, quelle porte crée la superposition ?
Réponse : Porte Hadamard (H)
Explication : La commande 'qc.h(0)' applique une porte Hadamard pour créer une superposition sur le premier qubit.

### Exercice 3 - Question 2 (MCQ)

Quelle porte est utilisée pour intriquer les deux qubits ?
Réponse : Porte CNOT (cx)
Explication : La porte CNOT ('qc.cx(0, 1)') lie l'état du second qubit à celui du premier, créant l'intrication.

### Exercice 3 - Question 3 (MCQ)

Quels sont les résultats attendus d'une simulation d'intrication parfaite ?
Réponse : Majoritairement '00' et '11'
Explication : Pour l'état |00> + |11>, les mesures doivent être corrélées, donnant 00 ou 11.

### Exercice 3 - Question 4 (MCQ)

Que signifie le résultat {'00': 537, '11': 487} ?

Réponse : Les qubits sont fortement corrélés

Explication : L'absence de '01' ou '10' montre que les états des deux qubits sont liés.

### Exercice 3 - Question 5 (MCQ)

Quel objet Qiskit est utilisé pour exécuter le circuit dans le code ?

Réponse : StatevectorSampler

Explication : Le code utilise 'sampler = StatevectorSampler()' pour l'exécution.

### Exercice 4 - Question 1 (MCQ)

Pourquoi la cryptographie classique est-elle menacée ?

Réponse : À cause de l'émergence des ordinateurs quantiques

Explication : Les ordinateurs quantiques peuvent résoudre rapidement les problèmes mathématiques sur lesquels repose la crypto classique.

### Exercice 4 - Question 2 (MCQ)

Sur quoi repose la sécurité de la cryptographie quantique ?

Réponse : Les lois de la mécanique quantique

Explication : Contrairement à la crypto classique (maths), la crypto quantique repose sur la physique.

### Exercice 4 - Question 3 (MCQ)

Quelle inégalité est utilisée pour démontrer formellement la sécurité d'E91 ?

Réponse : Inégalité de Bell (CHSH)

Explication : L'inégalité CHSH est la forme spécifique de l'inégalité de Bell utilisée dans le protocole E91.

### Exercice 4 - Question 4 (MCQ)

En CV-QKD, comment Alice encode-t-elle l'information ?

Réponse : Sur des états cohérents (quadratures)

Explication : L'information est encodée sur les quadratures X et P du champ électromagnétique.

### Exercice 4 - Question 5 (MCQ)

La CV-QKD est-elle adaptée aux réseaux de fibres optiques actuels ?

Réponse : Oui, elle utilise des techniques d'optique classique

Explication : Sa compatibilité avec les infrastructures existantes est l'un de ses points

forts.

### Exercice 5 - Question 1 (MCQ)

Dans l'équation V_mesuré = V_signal + V_bruit, qu'indique un V_bruit élevé ?
Réponse : Une tentative d'interception (espion)
Explication : Un bruit excédentaire (excess noise) est le signe qu'un tiers a tenté de mesurer le signal.

### Exercice 5 - Question 2 (MCQ)

Quelle est la principale différence entre BB84 et CV-QKD ?
Réponse : BB84 utilise des qubits discrets, CV-QKD des variables continues
Explication : BB84 repose sur des photons uniques (discrets), tandis que CV-QKD module des ondes lumineuses.

### Exercice 5 - Question 3 (MCQ)

Dans le protocole E91, que reçoivent Alice et Bob ?
Réponse : Chacun une particule d'une paire intriquée
Explication : Une source centrale envoie une particule à Alice et l'autre à Bob.

### Exercice 5 - Question 4 (MCQ)

Que signifie la perturbation de l'état quantique par un espion ?
Réponse : L'écoute devient détectable car les corrélations sont détruites
Explication : Mesurer un système quantique change son état, ce qui permet de repérer l'intrusion.

### Exercice 5 - Question 5 (MCQ)

La simulation Qiskit valide-t-elle quelle brique de E91 ?
Réponse : L'intrication quantique
Explication : La simulation montre que les qubits sont liés, prouvant la faisabilité de l'intrication.

### Exercice 6 - Question 1 (MCQ)

Quel type de distribution est utilisé pour les quadratures en CV-QKD ?
Réponse : Gaussienne
Explication : Alice module les quadratures selon une loi gaussienne pour sécuriser le signal.

### Exercice 6 - Question 2 (MCQ)

L'inégalité CHSH est donnée par S = |E(a,b) - E(a,b') + E(a',b) + E(a',b')|. Que représentent a et b ?
Réponse : Des réglages de mesure (angles)
Explication : a et b représentent les orientations des bases de mesure choisies par Alice et Bob.

### Exercice 6 - Question 3 (MCQ)

Pourquoi la simulation affiche-t-elle un histogramme de distribution ?
Réponse : Pour montrer l'effet du bruit sur la quadrature
Explication : L'élargissement de la gaussienne illustre visuellement la présence d'un espion.

### Exercice 6 - Question 4 (MCQ)

Le protocole BB84 est cité dans le texte comme étant :
Réponse : Un protocole antérieur à E91
Explication : Le texte indique qu'après le protocole BB84, d'autres protocoles (comme E91) ont été proposés.

### Exercice 6 - Question 5 (MCQ)

Dans le code Python, que fait la fonction 'np.random.normal' ?
Réponse : Elle génère des nombres selon une loi normale (Gaussienne)
Explication : Elle est utilisée pour simuler le signal gaussien et le bruit quantique.

### Exercice 7 - Question 1 (FILL_IN)

Le protocole E91 repose sur le phénomène d'_____, où deux particules forment un système unique.
Réponse : intrication
Explication : L'intrication est la base du protocole Ekert 1991.

### Exercice 7 - Question 2 (FILL_IN)

Pour vérifier la sécurité, Alice et Bob utilisent les inégalités de _____.
Réponse : Bell
Explication : Les inégalités de Bell permettent de distinguer les corrélations classiques des corrélations quantiques.

### Exercice 7 - Question 3 (FILL_IN)

Si la valeur calculée S est supérieure à _____, alors le système est purement quantique.
Réponse : 2

Explication : 2 est la limite locale réaliste (classique) selon le théorème de Bell.

### Exercice 8 - Question 1 (FILL_IN)

Dans un circuit Qiskit, la porte _____ permet de créer une superposition d'états.
Réponse : Hadamard
Explication : La porte H transforme |0> en (|0>+|1>)/√2.

### Exercice 8 - Question 2 (FILL_IN)

La porte _____ est nécessaire pour lier deux qubits entre eux dans un état intriqué.
Réponse : CNOT
Explication : La porte Controlled-NOT crée le lien d'intrication entre le qubit de contrôle et le qubit cible.

### Exercice 8 - Question 3 (FILL_IN)

Le résultat d'une mesure sur deux qubits intriqués dans l'état de Bell donne majoritairement les chaînes de bits '00' et '_____'.
Réponse : 11
Explication : L'état |00> + |11> donne des mesures identiques pour les deux qubits.

### Exercice 9 - Question 1 (FILL_IN)

La CV-QKD utilise des variables _____ de la lumière.
Réponse : continues
Explication : Contrairement aux variables discrètes (qubits), on utilise ici des spectres continus.

### Exercice 9 - Question 2 (FILL_IN)

Alice module les quadratures X et P selon une loi _____.
Réponse : gaussienne
Explication : La modulation gaussienne est le standard pour coder l'information en CV-QKD.

### Exercice 9 - Question 3 (FILL_IN)

Bob mesure ces quadratures grâce à la détection _____.
Réponse : homodyne
Explication : La détection homodyne permet d'extraire l'information de phase et d'amplitude du champ électromagnétique.

### Exercice 10 - Question 1 (FILL_IN)

Toute tentative d'interception par un espion introduit un _____ excédentaire.
Réponse : bruit
Explication : Le bruit quantique est perturbé par l'observation d'un tiers.

### Exercice 10 - Question 2 (FILL_IN)

La sécurité de la CV-QKD est surveillée via la _____ du signal reçu.
Réponse : variance
Explication : Une augmentation de la variance indique une perturbation du canal.

### Exercice 10 - Question 3 (FILL_IN)

Dans l'inégalité CHSH, la valeur théorique maximale est _____.
Réponse : $2\sqrt{2}$
Explication : C'est la borne de Tsirelson pour les systèmes quantiques.

### Exercice 11 - Question 1 (FILL_IN)

La cryptographie _____ repose sur la difficulté mathématique des calculs.
Réponse : classique
Explication : Contrairement à la cryptographie quantique qui repose sur la physique.

### Exercice 11 - Question 2 (FILL_IN)

L'émergence des ordinateurs _____ rend vulnérables les systèmes actuels.
Réponse : quantiques
Explication : Ils possèdent une puissance de calcul capable de briser les codes RSA par exemple.

### Exercice 11 - Question 3 (FILL_IN)

Le protocole E91 a été créé en l'an _____.
Réponse : 1991
Explication : C'est l'année de publication des travaux d'Artur Ekert.

### Exercice 12 - Question 1 (OPEN)

Expliquez pourquoi l'état $|\Psi\rangle = 1/\sqrt{2}\ (|00\rangle + |11\rangle)$ garantit que l'écoute par un espion est détectable.
Réponse : Toute mesure perturbe l'état.
Explication : En mécanique quantique, mesurer un système intriqué sans connaître la base de préparation détruit les corrélations spécifiques. Si un espion (Eve) intercepte la particule, elle force celle-ci dans un état défini, ce qui rompt le lien d'intrication. Alice et Bob, en comparant une partie de leurs résultats, verront que leurs mesures ne sont plus

parfaitement corrélées ou que les inégalités de Bell ne sont plus violées.

## Exercice 13 - Question 1 (OPEN)

Décrivez le rôle de la variance dans la sécurité du protocole CV-QKD.

Réponse : La variance sert d'indicateur d'intrusion.

Explication : Dans le protocole CV-QKD, l'information est portée par des distributions gaussiennes. La sécurité repose sur le fait que l'incertitude quantique est minimale dans un canal pur. Si un espion tente de mesurer les quadratures, il injecte inévitablement du bruit (principe d'incertitude), ce qui élargit la distribution statistique et augmente la variance mesurée par Bob. Si V_mesuré > V_signal + V_bruit_naturel, l'intrusion est confirmée.

## Exercice 14 - Question 1 (OPEN)

Comparez brièvement l'approche de la cryptographie classique et celle de la cryptographie quantique.

Réponse : Mathématiques vs Lois de la physique.

Explication : La cryptographie classique repose sur des problèmes mathématiques 'difficiles' (comme la factorisation de grands nombres) qui pourraient être résolus par des algorithmes plus puissants. La cryptographie quantique repose sur les lois immuables de la physique (intrication, non-clonage, incertitude), rendant la sécurité indépendante de la puissance de calcul de l'adversaire.

## Exercice 15 - Question 1 (OPEN)

Quel est l'intérêt d'utiliser l'inégalité de Bell (S > 2) plutôt qu'une simple vérification de bits en E91 ?

Réponse : Prouver l'absence de variables cachées et l'intégrité quantique.

Explication : La violation de l'inégalité de Bell (S > 2) est une preuve irréfutable que les corrélations observées sont de nature quantique et non le résultat d'une stratégie classique pré-établie par un espion. Cela garantit que la source est réellement intriquée et qu'aucune information n'a 'fuité' via un canal classique caché.

## Exercice 16 - Question 1 (REFLECTION)

Si un ordinateur quantique parfait existait aujourd'hui, pourquoi le protocole E91 resterait-il sécurisé alors que RSA ne le serait plus ?

Réponse : Parce que E91 ne dépend pas de la complexité algorithmique.

Explication : RSA repose sur la difficulté de factoriser des nombres, un problème que l'algorithme de Shor sur ordinateur quantique résout facilement. E91 repose sur

l'intrication : les lois de la physique interdisent de copier un état quantique inconnu (théorème de non-clonage) et toute mesure par l'ordinateur quantique de l'espion serait immédiatement visible par la destruction des corrélations de Bell.

## Exercice 17 - Question 1 (REFLECTION)

Pourquoi la CV-QKD est-elle considérée comme plus 'pratique' pour une intégration dans les réseaux de télécommunications actuels par rapport aux protocoles à photons uniques ?

Réponse : Compatibilité avec l'infrastructure standard.

Explication : Les protocoles à photons uniques (comme BB84) nécessitent des détecteurs de photons très sensibles et souvent coûteux ou refroidis. La CV-QKD utilise des composants d'optique cohérente standards (détection homodyne, lasers classiques) déjà utilisés dans les réseaux de fibres optiques à haut débit, facilitant ainsi le déploiement sur les infrastructures existantes.

## Exercice 18 - Question 1 (REFLECTION)

En analysant le circuit Qiskit, pourquoi est-il crucial de ne pas effectuer de mesure avant la porte CNOT si l'on veut obtenir une intrication ?

Réponse : La mesure provoque l'effondrement de la fonction d'onde.

Explication : L'intrication nécessite que les qubits soient dans un état de superposition cohérente. Si on mesure le premier qubit après la porte Hadamard mais avant la CNOT, l'état s'effondre soit en |0>, soit en |1>. Le second qubit ne sera alors plus intriqué mais simplement mis dans un état classique dépendant du résultat précédent. On perd le caractère quantique du système.

## Exercice 19 - Question 1 (CASE_STUDY)

Étude de cas : Une entreprise déploie le protocole E91. Lors d'un test, Alice et Bob calculent une valeur S = 1.95. Doivent-ils valider la clé générée ? Justifiez en analysant les seuils théoriques.

Réponse : Non, la clé doit être rejetée.

Explication : La valeur S = 1.95 est inférieure au seuil classique de 2. Cela signifie que les corrélations observées pourraient être expliquées par de la physique classique ou, plus grave, qu'un espion a intercepté les particules, détruisant l'intrication et ramenant le système vers un comportement classique. Pour garantir une sécurité quantique, S doit être significativement supérieur à 2 (idéalement proche de $2\sqrt{2} \approx 2.82$).

## Exercice 20 - Question 1 (CASE_STUDY)

Étude de cas : En utilisant le simulateur CV-QKD, Bob observe que la variance de son signal reçu est de 1.6 alors que la variance idéale attendue est de 1.1. En sachant que le bruit naturel du canal est estimé à 0.1, déduisez la présence potentielle d'un espion et l'action à entreprendre.
Réponse : Espion détecté, communication à interrompre.
Explication : V_attendu = V_signal + V_bruit_naturel = 1.1 + 0.1 = 1.2. La variance mesurée est de 1.6, ce qui montre un 'excess noise' (bruit excédentaire) de 0.4. Ce surplus de bruit est statistiquement significatif d'une interception. Bob doit considérer le canal comme compromis et ne pas utiliser les données pour générer une clé secrète.

## Exercice 21 - Question 1 (COMPETENCE)

Interprétez les résultats de simulation : {'00': 537, '11': 487}. Calculez le pourcentage de corrélation et expliquez si cela valide l'intrication.
Réponse : Corrélation de 100%, intrication validée.
Explication : Total des mesures = 537 + 487 = 1024. Toutes les mesures sont soit '00' soit '11'. Il n'y a aucun état '01' ou '10'. Le pourcentage de corrélation parfaite est donc de 100%. Cela confirme que les qubits sont dans un état intriqué |00> + |11>, car la mesure de l'un dicte instantanément celle de l'autre.

## Exercice 22 - Question 1 (COMPETENCE)

À partir du code Python fourni pour CV-QKD, expliquez comment le bruit d'Eve est modélisé mathématiquement par rapport au signal d'Alice.
Réponse : Addition d'une variable aléatoire normale à la variance plus élevée.
Explication : Le signal de Bob en présence d'Eve est généré par : 'bob_eve = alice + np.random.normal(0, np.sqrt(V_eve), N)'. Ici, on ajoute au signal original 'alice' un bruit gaussien de variance V_eve (0.5), ce qui est bien supérieur au bruit naturel (0.1). Cela simule l'incertitude introduite par la mesure de l'espion.

## Exercice 23 - Question 1 (COMPETENCE)

Expliquez le rôle de la ligne de code 'qc.h(0)' suivie de 'qc.cx(0, 1)' dans la création d'une paire d'Ekert.
Réponse : Création d'un état de Bell.
Explication : La porte Hadamard (h) met le qubit 0 en superposition (|0>+|1>)/√2. La porte CNOT (cx) utilise le qubit 0 comme contrôle pour basculer le qubit 1. Si le qubit 0 est |0>, le qubit 1 reste |0>. Si le qubit 0 est |1>, le qubit 1 devient |1>. On obtient l'état combiné 1/√2(|00> + |11>), qui est l'état intriqué fondamental du protocole E91.

## Exercice 24 - Question 1 (PROBLEM_SOLVING)

Problème : On vous donne les corrélations suivantes pour un test de Bell : E(a,b)=0.7, E(a,b')=-0.7, E(a',b)=0.7, E(a',b')=0.7. Calculez la valeur de S et déterminez si la sécurité quantique est assurée.

Réponse : S = 2.8, Sécurité assurée.

Explication : Calcul de S : S = |0.7 - (-0.7) + 0.7 + 0.7| = |0.7 + 0.7 + 0.7 + 0.7| = 2.8. Comme 2.8 > 2, l'inégalité de Bell est violée. Cette valeur est très proche du maximum quantique théorique ($2\sqrt{2} \approx 2.82$), ce qui confirme une intrication quasi-parfaite et l'absence d'espion.

## Exercice 25 - Question 1 (PROBLEM_SOLVING)

Problème : Dans une simulation Qiskit, un étudiant oublie la porte Hadamard et n'utilise que 'qc.cx(0, 1)'. Prédisez le résultat des mesures ('counts') si les qubits sont initialisés à |0> et expliquez pourquoi cela échoue pour la cryptographie.

Réponse : Résultat {'00': 1024}. Échec car absence de caractère aléatoire et d'intrication.

Explication : Sans la porte Hadamard, le qubit 0 reste dans l'état |0>. La porte CNOT avec un contrôle à |0> ne modifie pas le qubit cible (1). Les deux qubits restent à |00>. Le résultat sera 100% de '00'. C'est un état déterministe classique : il n'y a ni superposition ni intrication, donc aucune sécurité quantique n'est possible (Eve pourrait copier cet état sans le perturber).