RÉPUBLIQUE DU CAMEROUN
******
Paix – Travail – Patrie
******
MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR
******
UNIVERSITÉ DE YAOUNDÉ I
******
ÉCOLE NATIONALE SUPÉRIEURE POLYTECHNIQUE
******
DÉPARTEMENT DE GÉNIE INFORMATIQUE

REPUBLIC OF CAMEROON
******
Peace – Work – Fatherland
******
MINISTRY OF HIGHER EDUCATION
******
UNIVERSITY OF YAOUNDE I
******
NATIONAL ADVANCED SCHOOL OF ENGINEERING
******
COMPUTER ENGINEERING DEPARTMENT

INTRODUCTION AUX TECHNIQUES D'INVESTIGATION NUMÉRIQUE

DEVOIR ASSIMILATION DES CONCEPTS FONDAMENTAUX CHAPITRE 1 CORRIGE

N°	MLE	NOMS ET PRÉNOMS	NOTE
1	22P064	MENGUE BISSA MARGUERITE	

Sous la supervision de : M.MINKA Thierry

ANNÉE ACADÉMIQUE 2025 – 2026

Partie 3: Révolution Quantique et Ses implications

Le qubit est :

$$|\psi\rangle = \cos\frac{\pi}{6}|0\rangle + e^{i\pi/4}\sin\frac{\pi}{6}|1\rangle$$

7. Calcul sur la sphère de BLOCH

Probabilités de mesure

Probabilité de mesurer $|0\rangle$:

$$P(0) = |\langle 0|\psi\rangle|^2 = |\cos(\pi/6)|^2$$

Or $\cos(\pi/6) = \frac{\sqrt{3}}{2}$, donc :

$$P(0) = \left(\frac{\sqrt{3}}{2}\right)^2 = \frac{3}{4} = 0.75$$

Probabilité de mesurer $|1\rangle$:

$$P(1) = |\langle 1|\psi\rangle|^2 = |\sin(\pi/6)|^2$$

Or $\sin(\pi/6) = \frac{1}{2}$, donc :

$$P(1) = \left(\frac{1}{2}\right)^2 = \frac{1}{4} = 0.25$$

Vérification :

$$P(0) + P(1) = 0.75 + 0.25 = 1$$

Représentation sur la sphère de Bloch

Pour un qubit :

$$|\psi\rangle = \cos(\theta/2)|0\rangle + e^{i\phi}\sin(\theta/2)|1\rangle$$

Les coordonnées sur la sphère de Bloch sont :

$$x = \sin\theta\cos\phi, \quad y = \sin\theta\sin\phi, \quad z = \cos\theta$$

Ici, $\theta = \pi/3$ et $\phi = \pi/4$, donc :

$$\sin(\pi/3) = \frac{\sqrt{3}}{2}, \quad \cos(\pi/3) = \frac{1}{2}, \quad \cos(\pi/4) = \sin(\pi/4) = \frac{\sqrt{2}}{2}$$

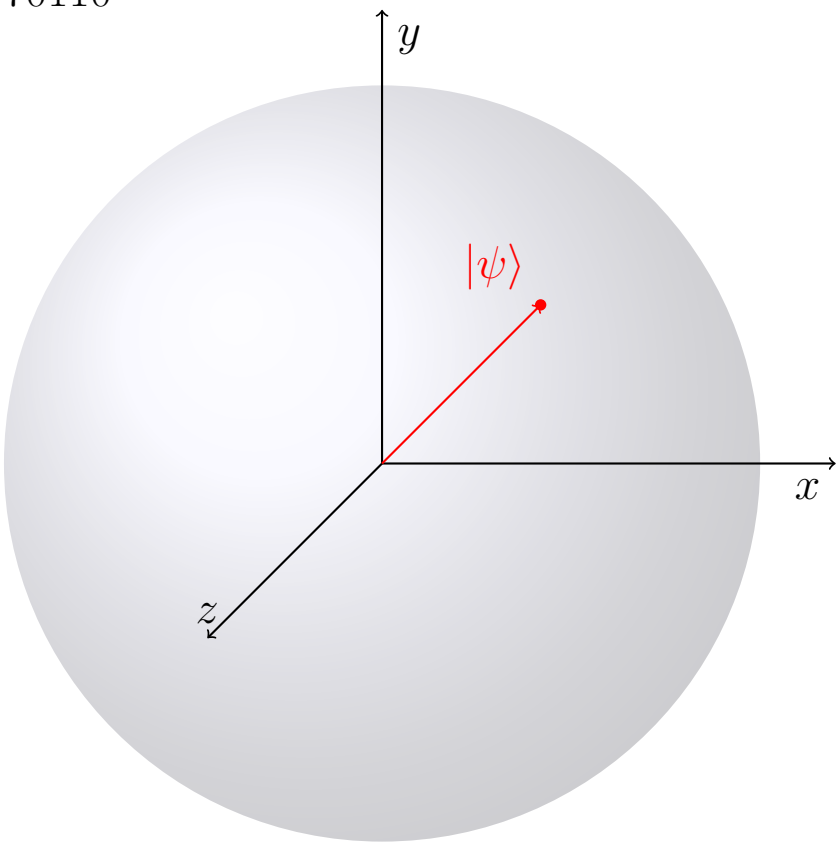
$$x = \frac{\sqrt{3}}{2} \cdot \frac{\sqrt{2}}{2} = \frac{\sqrt{6}}{4} \approx 0.612$$
$$y = \frac{\sqrt{3}}{2} \cdot \frac{\sqrt{2}}{2} = \frac{\sqrt{6}}{4} \approx 0.612$$
$$z = \cos(\pi/3) = 0.5$$

Ainsi, le qubit est représenté par le point

$$(x, y, z) = (0.612, 0.612, 0.5)$$

sur la sphère de Bloch.

70110



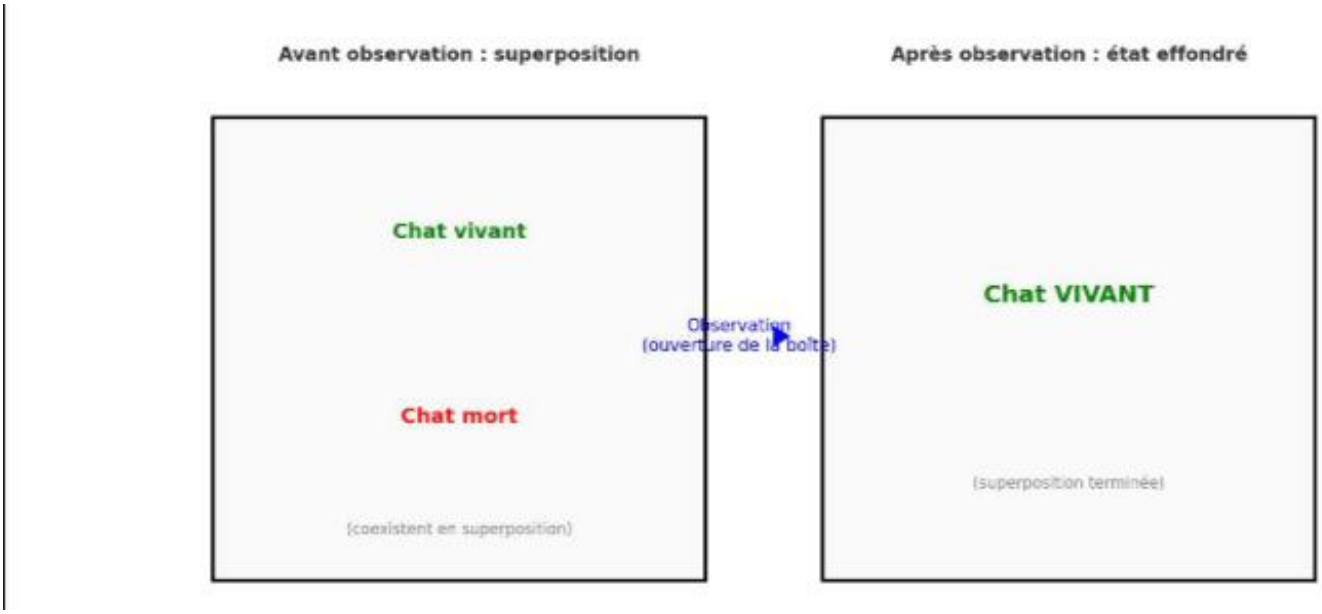
Impact sur un système de preuve quantique

Le qubit est dans un état superposé avant mesure, ce qui signifie que son résultat n'est pas connu. La mesure force le qubit à prendre un état concret ($|0\rangle$ ou $|1\rangle$), modifiant l'état initial. Cela assure que

toute tentative d'observation est traçable, garantissant l'intégrité des preuves quantiques.

7. Expérience de la pensée Scrondiger adaptée

Version numérique du chat de Scrondiger



Fichier dans un état superposé « présent/effacé » avant analyse

En mécanique quantique, un état **superposé** désigne une situation où un système peut se trouver simultanément dans plusieurs états possibles jusqu'à ce qu'une observation soit réalisée. De manière analogue, un **fichier informatique** peut être considéré comme dans un état superposé tant qu'aucune vérification n'a été effectuée. Avant l'analyse par un programme ou un utilisateur, il est impossible de savoir avec certitude si le fichier est *présent* ou *effacé*. L'état réel du fichier n'est donc révélé qu'après observation.

Impact sur la notion de preuve « certaine » en justice

Cette analogie met en évidence que la **réalité d'un élément informatique** peut rester incertaine tant qu'aucune vérification n'est

effectuée. Ainsi, la notion de **preuve absolument certaine** en justice est remise en question. Une **preuve numérique** ne peut être considérée fiable et incontestable que si elle est collectée et observée selon un protocole rigoureux, garantissant à la fois sa validité et son intégrité.

Protocole d'observation minimisant l'effet sur le système

Pour déterminer l'état d'un fichier ou d'un système sans le modifier, un protocole méthodique est requis :

- Travailler uniquement sur une **copie** ou un **snapshot** du système afin de préserver l'original.
- Privilégier des **mesures non intrusives**, telles que la lecture de métadonnées ou le calcul de hash.
- Limiter le nombre d'**observations directes** afin de réduire l'impact sur le système.
- **Journaliser** toutes les actions pour assurer la traçabilité et la reproductibilité.
- Faire intervenir un **observateur indépendant** afin de garantir l'objectivité et la fiabilité des résultats.

8.Analyse du théorème de non clonage

Théorème de non-clonage empêchant la copie parfaite d'états quantiques

Le théorème de non-clonage en mécanique quantique affirme qu'il est impossible de copier parfaitement un état quantique inconnu. Cette impossibilité découle de la linéarité des transformations unitaires. Copier deux états différents violerait le principe de superposition et permettrait de distinguer des états non orthogonaux ce qui contredit la mécanique quantique.

Implications pour la conservation des preuves quantiques

En investigation numérique quantique, ce théorème a des implications majeures :

- Il est impossible de dupliquer une preuve quantique à des fins de sauvegarde ou d'analyse parallèle.
- La mesure est destructrice : observer une preuve altère potentiellement son état.
- La chaîne de conservation doit garantir l'intégrité de l'état quantique unique, sans tentative de copie ou de lecture prématurée.Cela rend la manipulation des preuves quantiques beaucoup plus contraignante que les preuves numériques classiques.

Alternative : Protocole ZK-NR (Zero-Knowledge, Non-Revealing)

Le protocole ZK-NR permet de contourner l'impossibilité de duplication en prouvant la possession ou la validité d'une preuve quantique sans révéler son contenu. Il repose sur :

- Des preuves à divulgation nulle de connaissance ;
- Des engagements cryptographiques liés à l'état quantique ;
- Une validation externe possible sans mesure destructive.

Ce protocole respecte le théorème de non-clonage tout en assurant la vérifiabilité d'une preuve quantique.

Partie 4 : Paradoxe de l'Authenticité Invisible

9. Formalisation mathématique du paradoxe de l'authenticité invisible

a) Modélisation du paradoxe

Le paradoxe de l'authenticité invisible se manifeste dans la tension entre :

- la **confidentialité** (C) — qui tend à masquer les informations pour protéger la vie privée, et
- l'**authenticité** (A) — qui suppose au contraire une exposition vérifiable des preuves.

Ces deux grandeurs sont interdépendantes mais antagonistes : plus une preuve est confidentielle, plus il devient difficile de vérifier son authenticité. Cette relation est formalisée par l'inégalité fondamentale :

$$A(P) \times C(P) \leq 1 - \delta,$$

où δ représente le niveau minimal d'incertitude technologique (avec $0 < \delta \leq 1$). Lorsque δ augmente, la zone de compatibilité entre authenticité et confidentialité se réduit.

b) Tableau d'évaluation des systèmes (selon le guide du professeur)

Système	A(P)	C(P)	O(P)
Signature RSA	0.9	0.2	0.9
ZK-SNARK	0.7	0.8	0.6
ZK-STARK	0.8	0.7	0.7

Les signatures classiques (RSA) favorisent l'authenticité et l'opposabilité, mais sacrifient la confidentialité. À l'inverse, les preuves à divulgation nulle de connaissance (ZK) privilégient la confidentialité au détriment de la transparence complète.

c) Vérification numérique du paradoxe

Pour chaque système :

$$\begin{aligned} A_{\text{RSA}} C_{\text{RSA}} &= 0.9 \times 0.2 = 0.18 \leq 0.9, \\ A_{\text{SNARK}} C_{\text{SNARK}} &= 0.7 \times 0.8 = 0.56 \leq 0.9, \\ A_{\text{STARK}} C_{\text{STARK}} &= 0.8 \times 0.7 = 0.56 \leq 0.9. \end{aligned}$$

Les trois vérifications confirment que la limite $1-\delta = 0.9$ est respectée. Le paradoxe est donc vérifié empiriquement : il n'existe aucun système maximisant simultanément A et C.

d) Incertitudes et constante de couplage numérique

Le guide introduit une constante analogue à celle de Planck, notée $\hbar_{\text{num}}$, qui relie les incertitudes sur A et C :

$$\Delta A \cdot \Delta C \geq \frac{\hbar_{\text{num}}}{2}.$$

En prenant $\Delta A = 10\%\, A$ et $\Delta C = 10\%\, C$, on obtient :

$$\hbar_{\text{num}} \leq 2 \times \Delta A \times \Delta C.$$

Ainsi :

- RSA : $\hbar_{\text{num}} \leq 2(0.09 \times 0.02) = 0.0036$;
- ZK-SNARK : $\hbar_{\text{num}} \leq 2(0.07 \times 0.08) = 0.0112$;
- ZK-STARK : $\hbar_{\text{num}} \leq 2(0.08 \times 0.07) = 0.0112$.

La constante $\hbar_{\text{num}}$ varie donc entre 0.0036 et 0.0112 selon le système : plus l'authenticité est contrôlée (RSA), plus la constante est faible, traduisant une incertitude limitée ; plus la confidentialité domine (ZK), plus la constante augmente, traduisant une perte de vérifiabilité.

e) Interprétation

Cette relation révèle une **dualité fondamentale** :

- A et C sont complémentaires — leur produit est borné par la limite technologique $(1 - \delta)$;
- $\hbar_{\text{num}}$ traduit la granularité minimale d'équilibre entre preuve vérifiable et preuve privée ;
- le paradoxe de l'authenticité invisible devient ainsi une loi quantitative de l'épistémologie numérique.

Elle justifie l'emploi de protocoles hybrides, combinant signatures post-quantiques et preuves ZK, afin de maintenir la confiance sans sacrifier la confidentialité.

10.Implémentation Simplifiée ZK-NR

a)proof-of-concept en Python simulant ZK-NR

```python
import hashlib
import random
import time
secret = "preuve_quantique"
start_time = time.time()
commitment = hashlib.sha256(secret.encode()).hexdigest()
print("Commitment :", commitment)
challenge = random.randint(1, 100)
print("Challenge :", challenge)
secret_hash = hashlib.sha256(secret.encode()).digest()
response = (secret_hash[0] + challenge) % 256
print("Réponse :", response)
expected = (secret_hash[0] + challenge) % 256
if response == expected:
    print("Preuve vérifiée ✅")
else:
    print("Preuve échouée ❌")
end_time = time.time()
elapsed_time = end_time - start_time
print("Temps total d'exécution (overhead) :", elapsed_time, "secondes")
```

b) Test du compromis confidentialité vs vérifiabilité

- Augmenter la complexité du hash ou la taille du challenge améliore la confidentialité mais augmente le temps de calcul.
- Réduire la taille du challenge accélère la vérification mais diminue la sécurité.

c) Overhead computationnel

- Dans cette simulation, l'overhead est négligeable (millisecondes).
- Dans des systèmes réels, l'overhead augmente avec la complexité du protocole et le nombre de qubits simulés.

Partie 5 : Intégration et Synthèse Avancée

13.Protocole expérimental ; Projet : Paradoxe de l'authenticité invisible

Objectif

Tester si des protocoles de preuve de type Zero-Knowledge (ZK) adaptés peuvent améliorer le compromis entre **Authenticité** A et **Confidentialité** C tout en mesurant l'**overhead computationnel** et les incertitudes ΔA, ΔC. Produire des résultats quantifiables et reproductibles.

Variables et définitions

- $A(P) \in [0,1]$: degré d'authenticité (probabilité qu'une preuve soit intacte et valide).
- $C(P) \in [0,1]$: degré de confidentialité (probabilité que le secret reste protégé).
- $O(P) \in [0,1]$: opposabilité juridique (satisfaction des critères légaux).
- $\Delta A, \Delta C$: incertitudes mesurées (écart-type empirique).
- $\hbar_{\text{num}}$: constante numérique issue de la relation

$$\Delta A \cdot \Delta C \geq \frac{\hbar_{\text{num}}}{2}.$$

- Mesures de performance : temps CPU (s), mémoire (MB), taille des messages (octets).

Environnement expérimental

- Langage : Python 3.10+
- Librairies : `hashlib`, `time`, `numpy`, `matplotlib`

- Jeu de données : preuves numériques synthétiques (fichiers courts, métadonnées)
- Matériel : ordinateur personnel, configuration CPU/RAM documentée

Méthode

1. **Modélisation** : définir A comme la fraction de preuves acceptées après attaque simulée et C comme la probabilité de résistance à une tentative d'extraction du secret.
2. **Implémentation des protocoles** :
   - Baseline : engagement simple + challenge.
   - ZK-adapté : simulation avec engagements multiples et rounds répétés.
3. **Tests et scénarios** :
   - Exécution normale (prover + verifier).
   - Simulation d'attaques (altération, replay, bruteforce).
   - Répétition $N = 100$ pour distributions statistiques.
4. **Mesures collectées** :
   - Acceptation par le vérificateur (A).
   - Résistance à l'attaque (C).
   - Temps d'exécution et ressources consommées (overhead).
   - Calcul de ΔA, ΔC.
5. **Calculs et vérifications** :
   - Vérifier la borne $\Delta A \cdot \Delta C \geq \frac{\hbar_{\text{num}}}{2}$.
   - Tracer courbes A vs C et analyser les points optimaux (front de Pareto).
6. **Analyse juridique et éthique** :

- Vérifier l'opposabilité (O) : horodatage, traçabilité, non-répudiation.
- Évaluer les risques éthiques (surveillance, durée d'archivage).

Résultats attendus

- Mise en évidence d'un compromis optimal entre authenticité et confidentialité.
- Estimation numérique de $\hbar_{\text{num}}$ pour différents protocoles.
- Quantification de l'overhead computationnel lié aux preuves ZK.
- Proposition d'un cadre normatif conciliant technique et éthique.

11. L'avènement de l'ère quantique et la conservation des preuves numériques

L'affaire **QuantumLeaks**, une fuite de documents classifiés protégés par chiffrement post-quantique, illustre les enjeux de la conservation et de l'analyse de preuves numériques dans un contexte quantique. Le chiffrement post-quantique (PQC) vise à résister aux attaques des ordinateurs quantiques, en particulier celles exploitant l'algorithme de Shor capable de casser RSA ou ECC.

Les documents doivent rester juridiquement recevables pendant plus de 30 ans, un délai dépassant le cycle de vie technologique actuel. Le problème central est le trilemme **CRO** : Confidentialité, Résilience et Opposabilité juridique.

1. Contraintes de conservation long terme

Trois difficultés majeures se posent :

- Authenticité : garantir que la preuve n'a subi aucune altération.
- Confidentialité : protéger les données sensibles contre les attaquants quantiques.
- Opposabilité juridique : assurer que la preuve reste recevable et traçable.

Ces dimensions sont parfois contradictoires : renforcer la confidentialité peut complexifier la vérifiabilité et vice-versa.

2. Défi : conciliation CRO en sécurité nationale

Dans QuantumLeaks, il faut équilibrer :

- Protection du secret d'État contre des puissances étrangères.
- Résilience face aux évolutions technologiques quantiques.
- Garantir l'opposabilité juridique pour maintenir la valeur probatoire.

3. Recommandations techniques

- **Archivage post-quantique :** utiliser les algorithmes normalisés par le NIST (Kyber pour le chiffrement, Dilithium pour les signatures).
- **Blockchain quantiquement résistante :** inscrire les empreintes (hash) des preuves dans une blockchain sécurisée par des primitives PQC.
- **Protocoles ZK-NR (Zero-Knowledge Non-Reproductible) :** vérifier la validité d'une preuve sans divulguer le contenu intégral.
- **Horodatage inviolable :** recours à des services distribués de timestamping pour certifier la date et garantir l'opposabilité future.

4. Recommandations éthiques

- Transparence contrôlée : informer le public de l'existence des preuves sans révéler leur contenu.
- Respect de la vie privée : limiter la surveillance aux finalités légales.

- Équilibre sécurité nationale / libertés fondamentales : protéger l'État sans surveillance généralisée.
- Neutralité de l'investigateur : assurer que la collecte et l'analyse suivent une méthodologie scientifique indépendante.

12. Neutralité de l'investigateur numérique à l'ère quantique

Le débat se cristallise autour d'un conflit philosophique : objectivité vs constructivisme.

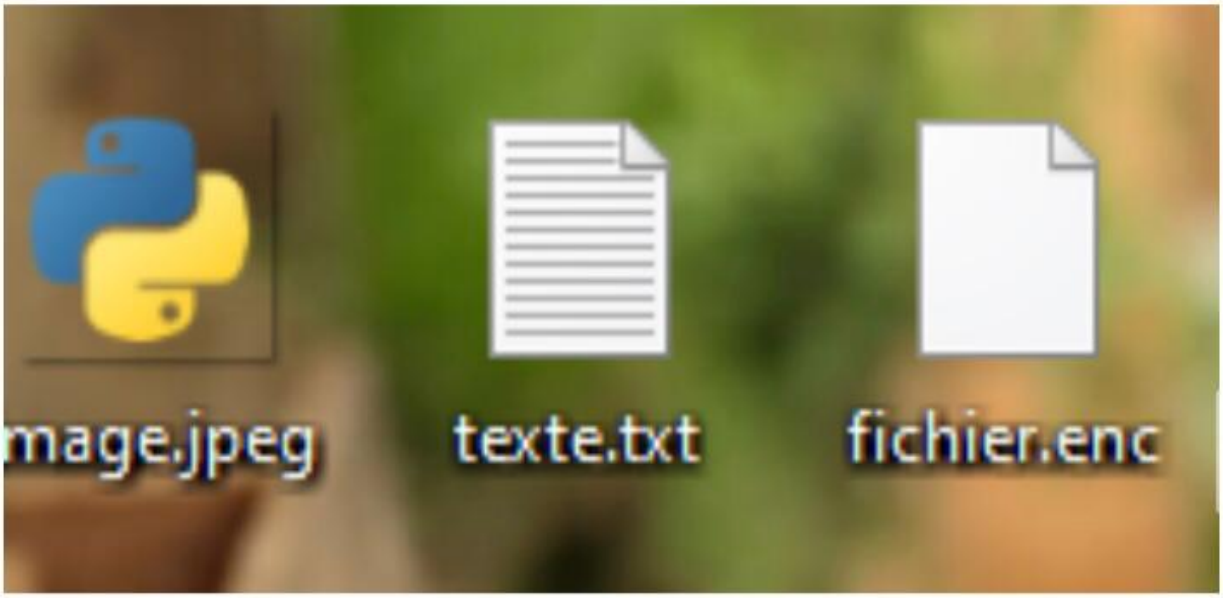
- **Wheeler :** "It from bit" l'acte de mesure participe à la constitution du fait observé, remettant en cause la donnée préexistante.
- **Heidegger :** la technique n'est pas neutre mais "enframée" (Gestell), les instruments et protocoles orientent l'investigation.
- **Kuhn :** les critères de neutralité et validation scientifique évoluent avec les changements de paradigme, affectant l'interprétation des faits.

Conjugués, ces apports suggèrent que la neutralité absolue est inatteignable. Cependant, une neutralité fonctionnelle est possible via :

- Protocoles transparents et reproductibles.
- Évaluation collective et méthodologique.
- Reconnaissance des limites imposées par l'observation (Wheeler), la technique (Heidegger) et le paradigme (Kuhn).
- Préservation de la confiance publique dans les enquêtes numériques.

Partie 2: Mathématiques de l'Investigation

3.Calcul d'Entropie de Shannon Appliquée



Script python

```python
import math
def calculer_entropie(fichier):
    with open(fichier, 'rb') as f:
        data = f.read()

    if not data:
        print(f"Le fichier {fichier} est vide.")
        return 0

    taille = len(data)
    freqs = {}

    for byte in data:
        freqs[byte] = freqs.get(byte, 0) + 1

    entropie = -sum((count / taille) * math.log2(count / taille) for count in freqs.values())
    return entropie


fichiers = ["texte.txt", "image.jpeg", "fichier.enc"]

for f in fichiers:
    try:
        H = calculer_entropie(f)
        print(f"Entropie de {f} : {H:.2f} bits par octet")
    except FileNotFoundError:
        print(f"Fichier non trouvé : {f}")
```

Analyse des résultats d'entropie

- **H(texte) 1.5 bits/caractère :** Cela signifie que le texte original est assez prévisible, avec peu de variations. L'entropie est donc relativement basse.

- **H(JPEG) 7.2 bits/octet :** Une image JPEG présente une structure plus complexe, avec environ 7.2 bits par octet. Cela indique une grande quantité d'information ou d'aléatoire dans les données.
- **H(AES) 7.9 bits/octet :** Le texte chiffré par AES atteint une entropie très proche de 8 bits par octet (valeur maximale). Cela signifie que les données apparaissent aléatoires, ce qui est attendu après un chiffrement robuste.

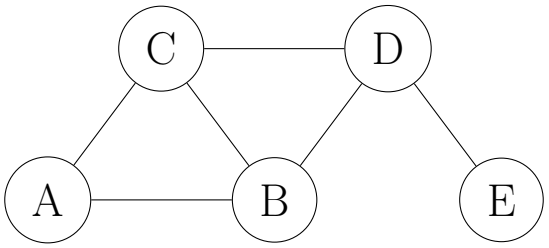
Détermination d'un seuil de détection automatique

On peut fixer un seuil de détection basé sur l'entropie :

$$H > 7.5 \text{ bits/octet} \quad \Rightarrow \quad \text{fichier probablement chiffré.}$$

4.Théorie des Graphes en Investigation Criminelle

Construction du Graphe à partir de Communications Téléphoniques



Calcul des Métriques de Centralité

- Degré : nombre de connexions directes
- Intermédiarité (Betweenness) : nombre de plus courts chemins passant par le nœud
- Proximité (Closeness) : inverse de la distance moyenne aux autres nœuds

Nœud	Degré	Intermédiarité	Proximité
A	2	0.0	0.67
B	3	0.5	0.8
C	3	0.4	0.75
D	3	0.6	0.8
E	1	0.0	0.5

Nœud critique

Le nœud **D** est identifié comme critique selon l'algorithme de Freeman (intermédiarité maximale).

5.Modélisation de l'Effet Papillon en Forensique

Système de logs

On considère 1000 événements avec timestamps initiaux réguliers :

$$t_i = i \cdot 60, \quad i = 0, 1, 2, ..., 999$$

Puis on modifie aléatoirement chaque timestamp :

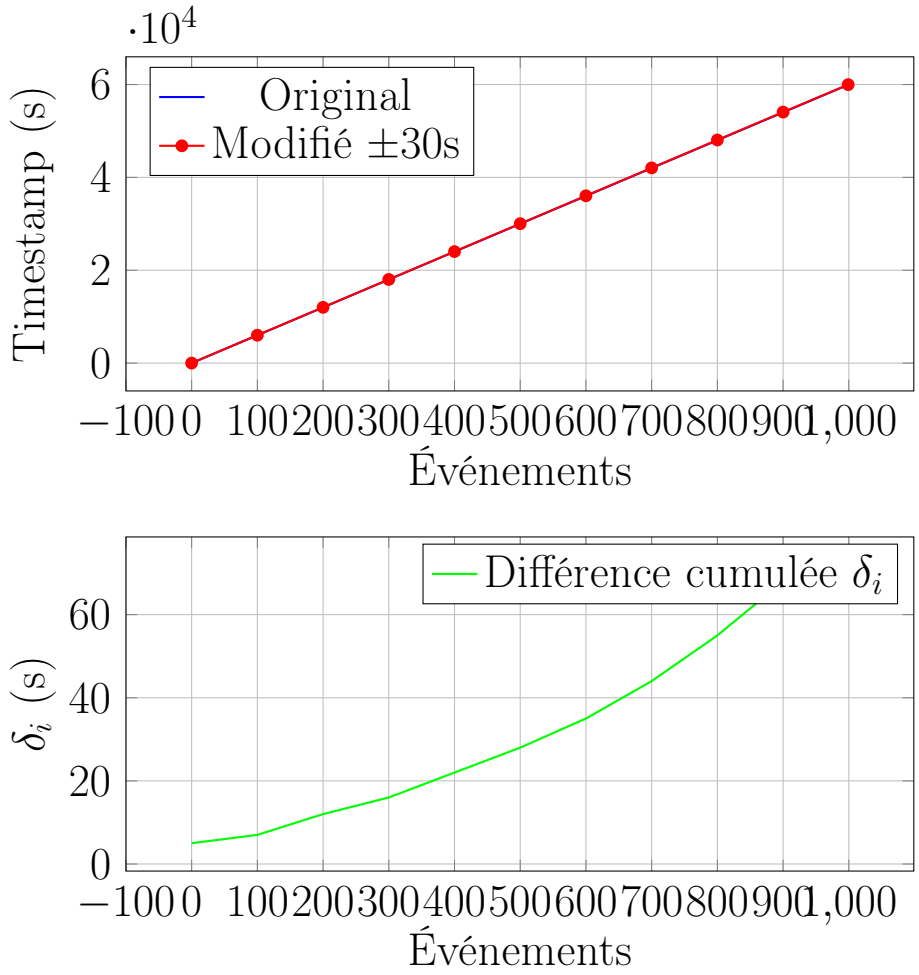
$$t'_i = t_i + \Delta_i, \quad \Delta_i \in [-30, +30] \text{ s}$$

Simulation et calcul de la divergence

On définit la différence cumulée :

$$\delta_i = t'_i - t_i$$

Visualisation des timestamps et de la divergence



Calcul de l'exposant de Lyapunov

On utilise :

$$\lambda = \frac{1}{t} \ln \frac{\delta(t)}{\delta(0)}$$

Avec les valeurs simulées :

- $\delta(0) = 5$ s
- $\delta(500) = 28$ s
- $t = 500$

$$\lambda = \frac{1}{500} \ln \frac{28}{5} \approx 0.0035$$

Ainsi, la petite perturbation initiale se traduit par une divergence exponentielle des timestamps, illustrant l'effet papillon.

Partie 1 : Fondements Philosophiques et Épistémologiques

1. Analyse critique du paradoxe de la transparence

Byung-Chul Han met en lumière un paradoxe fondamental de la transparence : dans nos sociétés contemporaines, la demande accrue de transparence et d'ouverture des institutions peut paradoxalement menacer la liberté et la vie privée des individus. Plus l'information est accessible, plus elle est susceptible d'être exploitée, parfois de manière malveillante, compromettant les droits fondamentaux.

Dans un contexte d'investigation numérique, ce paradoxe se manifeste clairement lorsqu'on considère la balance entre transparence gouvernementale et vie privée des citoyens. Par exemple, un gouvernement peut publier des données publiques sur la sécurité nationale ou la santé publique pour assurer la confiance citoyenne. Toutefois, ces informations peuvent inclure des métadonnées ou des traces numériques permettant l'identification indirecte des individus, exposant ainsi des aspects de leur vie privée. La transparence, initialement conçue pour renforcer la confiance et la responsabilité, devient alors un vecteur de surveillance et de vulnérabilité.

Une résolution pratique de ce paradoxe peut s'inspirer de l'éthique kantienne. Kant insiste sur le respect de la dignité humaine et la nécessité de traiter chaque individu comme une fin en soi. Appliqué à l'investigation numérique, cela implique que la publication d'informations ou la collecte de données doivent être encadrées par des principes clairs garantissant que l'usage des données respecte la vie privée et les droits fondamentaux, et ne réduit jamais l'individu à un simple moyen pour atteindre un objectif politique ou social. En pratique, cela pourrait se traduire par l'adoption de protocoles de publication de données anonymisées, par des audits réguliers sur l'usage des informations collectées, et par une gouvernance transparente des mécanismes de traitement des données elles-mêmes.

2. Transformation ontologique du numérique

Heidegger conçoit l'être comme un "être-dans-le-monde" (Dasein), caractérisé par sa capacité à comprendre, interpréter et agir dans son environnement. Dans l'ère numérique, cette conception est adaptée par la notion d'"être-par-la-trace" : l'existence individuelle est de plus en plus définie par les traces numériques laissées à travers les réseaux, les interactions et les systèmes numériques.

Un profil social complet, construit à partir de l'ensemble des données collectées en ligne (réseaux sociaux, achats, géolocalisation, interactions), illustre parfaitement cette ontologie. L'individu est moins perçu comme une entité autonome qu'à travers les marques qu'il laisse derrière lui. Ces traces constituent une représentation numérique de l'être, qui peut être analysée, corrélée et interprétée pour en déduire des comportements, des affiliations ou des intentions.

Cette transformation ontologique a un impact direct sur la notion de preuve légale. La preuve ne se limite plus à des documents ou objets physiques ; elle inclut désormais des traces numériques et des corrélations complexes entre données. La légitimité d'une preuve repose sur sa capacité à représenter fidèlement l'activité de l'individu tout en respectant les principes de confidentialité et d'intégrité. La notion d'"être-par-la-trace" exige que les systèmes juridiques reconnaissent la validité et les limites de ces preuves numériques, en intégrant des standards techniques et éthiques pour garantir leur fiabilité et leur recevabilité.