UNIVERSITÉ DE YAOUNDÉ I
***
ÉCOLE NATIONALE SUPÉRIEURE POLYTECHNIQUE DE YAOUNDÉ
***
DÉPARTEMENT DE GÉNIE INFORMATIQUE
***
HUMANITÉS NUMÉRIQUES

THE UNIVERSITY OF YAOUNDE I
***
NATIONAL ADVANCED SCHOOL OF ENGINEERING OF YAOUNDE
***
DEPARTMENT OF COMPUTER ENGINEERING
***
DIGITAL HUMANITIES

Philosophie et Fondements de l'Investigation Numérique

Exercices des pages 13 à 16

Rédigé par :

FANTA YADON Félicité (chef) 22P069

Supervisé par :

M. Thierry MINKA

I Partie 1 — Fondements Philosophiques et Épistémologiques

I.1 Exercice 1 — Dissertation (Paradoxe de la transparence)

La modernité numérique a propulsé la transparence au rang d'impératif moral et administratif : on exige des institutions, des entreprises et des individus qu'ils « ouvrent » leurs actions. Byung-Chul Han montre que la transparence n'est pas neutre : elle transforme les relations de pouvoir, fragilise l'intimité et installe un régime où l'excès de visibilité finit par aliéner. Dans le contexte d'une investigation numérique, le paradoxe de la transparence consiste en ce que la quête d'une vérité publique et vérifiable entre en tension directe avec le droit à la confidentialité et la préservation de la dignité personnelle.

Sur le plan pratique, la transparence améliore la redevabilité : logs, journaux et traces numériques permettent de reconstituer des événements et d'attribuer des responsabilités. Mais cette même exposition génère des effets pervers : la sur-exposition des citoyens à un contrôle continu, la marchandisation des traces et la réduction des personnes à des profils traçables.

Cas concret : enquête sur la corruption municipale. Une autorité publie des « dumps » d'emails pour prouver une collusion. La diffusion révèle des informations personnelles non nécessaires (santé, opinions privées), ce qui porte atteinte à des tiers non impliqués. La transparence a servi la preuve mais a nui à l'intégrité privée.

Résolution pratique inspirée de Kant :

— ne diffuser que les éléments strictement nécessaires à la preuve (principe de minimisation),

— comité d'éthique pour évaluer les conséquences de la publication,

— techniques d'anonymisation sélective et divulgation contrôlée,

— traçabilité des accès et durée de rétention limitée.

Conclusion : la transparence doit être réencadrée par une éthique de la dignité et des procédures institutionnalisées. L'investigateur devient non seulement un ingénieur de la preuve mais un gardien moral.

I.2 Exercice 2 — Transformation ontologique (Heidegger)

Heidegger voit la technique comme « dévoilement » (aletheia). À l'ère numérique, l'être se traduit par des traces persistantes : un « être-par-la-trace ». L'identité est donc médiatisée par des posts, likes, métadonnées.

Impact sur la preuve légale : les preuves sont distribuées, parfois modifiables. La validation exige donc :

— intégrité cryptographique (hashes, chaînes de custody),

— contextualisation (interprétation experte),

— prudence judiciaire sur la fiabilité.

II Partie 2 — Mathématiques de l'Investigation

II.1 Exercice 3 — Entropie et détection de chiffrement

```python
import math
from collections import Counter
import sys

def entropy_bytes(data: bytes) -> float:
    if not data:
        return 0.0
    counts = Counter(data)
    length = len(data)
    ent = 0.0
    for c in counts.values():
        p = c / length
        ent -= p * math.log2(p)
    return ent

def analyze_file(path):
    with open(path, 'rb') as f:
        data = f.read()
    ent = entropy_bytes(data)
    return ent

if __name__ == "__main__":
    if len(sys.argv) < 2:
        print("Usage: python entropy_check.py <file>")
        sys.exit(1)
    path = sys.argv[1]
    ent = analyze_file(path)
    print(f"Entropy (bits/octet): {ent:.4f}")
    if ent >= 7.7:
        print("Probable chiffrement")
    elif ent >= 6.5:
        print("Compress  ou image")
    else:
        print("Texte naturel ou structur ")
```

II.2 Exercice 4 — Graphes téléphoniques

III Partie 2 — Mathématiques de l'Investigation

III.1 Exercice 4 — Graphes téléphoniques

L'objectif est de modéliser les communications téléphoniques sous forme de graphe orienté pondéré G (V, E, w) afin d'identifier les acteurs critiques d'un réseau.

III.1.0.1 Méthodologie

1. Construire un graphe orienté pondéré $G(V, E, w)$ à partir des appels.
2. Calculer :
   — le **degré** entrant et sortant,

— l'**intermédiarité** (algorithme de Brandes),

— la **proximité** (closeness centrality).

3. Identifier le nœud critique par intermédiarité maximale.
4. Visualiser avec `networkx` et `matplotlib`.

III.1.0.2 Code Python illustratif

```
import networkx as nx
import matplotlib.pyplot as plt
import random

# Cr ation d'appels synth tiques
nodes = [f'num_{i}' for i in range(1,21)]
calls = [(random.choice(nodes), random.choice(nodes),
          random.expovariate(1/60)) for _ in range(200)]

# Graphe orient  pond r
G = nx.DiGraph()
for src,dst,dur in calls:
    if src != dst:
        if G.has_edge(src,dst):
            G[src][dst]['weight'] += dur
        else:
            G.add_edge(src,dst,weight=dur)

# Calcul des m triques
betw = nx.betweenness_centrality(G, weight='weight', normalized=True)
closeness = nx.closeness_centrality(G, distance='weight')
deg_centrality = nx.degree_centrality(G)

critical = max(betw, key=betw.get)
print("Noeud critique :", critical)

# Visualisation
pos = nx.spring_layout(G)
nx.draw(G, pos, with_labels=True,
        node_size=[5000*betw[n] for n in G],
        node_color=list(betw.values()), cmap=plt.cm.viridis)
plt.show()
```

III.1.0.3 Résultat attendu

Le nœud avec l'intermédiarité maximale est identifié comme **pivot stratégique** du réseau téléphonique.

—

III.2 Exercice 5 — Effet papillon et estimation de Lyapunov

On simule une timeline de 1000 événements corrélés. Une perturbation minime (± 30s) entraîne un désordre croissant. La divergence est modélisée par :

$$\delta(t) \approx \delta(0)\, e^{\lambda t}, \quad \ln \delta(t)\ \ln \delta(0)\ \lambda t$$

où λ est l'exposant de Lyapunov.

III.2.0.1 Code Python de simulation

```
import numpy as np
import matplotlib.pyplot as plt
from scipy import stats

# Timeline originale
N = 1000
times = np.cumsum(np.random.normal(60, 5, N))

# Perturbation
pert = times.copy()
pert[50:] += 5  # +5s apr s l'  vnement  50

# Distance cumulative
delta = np.cumsum(np.abs(times - pert))

# Estimation lambda
t = np.arange(N)
ln_d = np.log(delta[delta>0])
t_s = t[delta>0]
slope, intercept, _, _, _ = stats.linregress(t_s, ln_d)
print("Exposant de Lyapunov estim  :", slope)

# Graphique
plt.plot(t, delta)
plt.yscale('log')
plt.xlabel("  vnement  ")
plt.ylabel("  (t)")
plt.title("Effet papillon - croissance exponentielle")
plt.show()
```

III.2.0.2 Interprétation

— λ 0 : divergence exponentielle (sensibilité extrême).

— $\lambda \approx 0$: système stable.

— λ 0 : convergence (perturbation amortie).

—

IV Partie 3 — Révolution Quantique

IV.1 Exercice 6 — Chat de Schrödinger numérique

IV.1.0.1 Concept Dans l'informatique classique, un fichier est présent ou absent. La métaphore quantique traduit une incertitude pratique (copies multiples, caches). Dans un vrai système quantique, la mesure modifie l'état et rend la preuve intrinsèquement **probabiliste**.

IV.1.0.2 Implications pour la preuve

- Une mesure unique n'est pas suffisante : il faut répéter les mesures.
- Le théorème de non-clonage interdit la duplication parfaite d'une preuve quantique.
- La chaîne de custody doit inclure : **horodatage**, **paramètres de mesure**, **documentation complète**.

IV.2 Exercice 7 — Calcul sur la sphère de Bloch

État du qubit :

$$|\psi\rangle \ \cos(\tfrac{\pi}{6})|0\rangle \ e^{i\pi/4}\sin(\tfrac{\pi}{6})|1\rangle$$

IV.2.0.1 Calcul des probabilités en base Z

$$P(0) \ \cos^2(\tfrac{\pi}{6}) \ \tfrac{3}{4} \ 0.75, \quad P(1) \ \sin^2(\tfrac{\pi}{6}) \ \tfrac{1}{4} \ 0.25$$

IV.2.0.2 Vecteur de Bloch

$$(x, y, z) \ (\sin\theta\cos\phi, \sin\theta\sin\phi, \cos\theta)$$

avec $\theta \ \pi/3$, $\phi \ \pi/4$:

$$(x, y, z) \approx (0.612, 0.612, 0.5)$$

IV.2.0.3 Probabilités dans d'autres bases

- Base X : $P() \ \frac{1x}{2} \approx 0.806$.
- Base Y : $P(i) \ \frac{1y}{2} \approx 0.806$.

IV.2.0.4 Conclusion L'état est fortement biaisé vers $|0\rangle$ (75%), mais aussi vers $|\rangle$ et $|i\rangle$ (80%). En pratique, plusieurs mesures dans différentes bases sont nécessaires pour reconstruire l'état.

V Partie 4 — Paradoxe de l'Authenticité Invisible

Cette partie aborde une problématique centrale en investigation numérique : comment concilier l'**authenticité** (la capacité de prouver l'origine et la véracité d'une donnée) et la **confidentialité** (la protection des informations sensibles), tout en garantissant l'**opposabilité** juridique (la possibilité que la preuve soit recevable devant un tribunal).

Le paradoxe réside dans le fait que plus une preuve est authentifiée et exposée, moins elle est confidentielle, et inversement : protéger au maximum la confidentialité d'une donnée peut réduire sa valeur probatoire et son opposabilité.

V.1 Exercice 9 — Formalisation Mathématique du Paradoxe

On définit trois grandeurs normalisées sur l'intervalle $[0, 1]$:

— $A(P)$: **Authenticité** de la preuve P (degré de certitude sur son intégrité et sa source),

— $C(P)$: **Confidentialité** de la preuve P (degré de protection des informations sensibles),

— $O(P)$: **Opposabilité** de la preuve P (probabilité de recevabilité juridique).

La relation fondamentale proposée est :

$$A(P) \cdot C(P) \leq 1 - \delta$$

où δ représente un seuil de perte inévitable lié au paradoxe (zone d'incompatibilité).

V.1.0.1 Exemple numérique illustratif

— Preuve 1 : signature numérique classique A 0.95, C 0.20 $\Rightarrow A \cdot C$ 0.19 $\leq 1 - \delta$. Ici, la confidentialité est faible mais l'authenticité est très forte.

— Preuve 2 : protocole Zero-Knowledge (preuve de connaissance sans révélation) A 0.80, C 0.90 $\Rightarrow A \cdot C$ 0.72. Bon compromis entre authenticité et confidentialité, mais opposabilité parfois réduite (juges moins familiers).

— Preuve 3 : donnée chiffrée conservée sans clé publique A 0.40, C 0.95 $\Rightarrow A \cdot C$ 0.38. Forte confidentialité, mais faible authenticité : difficilement recevable.

V.1.0.2 Lien avec l'incertitude quantique L'analogie avec le principe d'incertitude s'exprime par l'inégalité suivante :

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

où ΔA et ΔC sont les incertitudes de mesure de l'authenticité et de la confidentialité, et $\hbar_{num}$ est une constante numérique analogue à la constante de Planck, spécifique au système de preuve numérique utilisé.

Méthode expérimentale pour estimer $\hbar_{num}$:

1. Collecter des jeux de preuves variées (signatures, hash, ZK, blockchain).
2. Mesurer A et C sur chaque preuve selon une grille définie (échelle $[0, 1]$).
3. Estimer leurs écarts-types ΔA et ΔC.
4. Vérifier la borne $\Delta A \cdot \Delta C$ et déduire une valeur empirique de $\hbar_{num}$.

V.2 Exercice 10 — Implémentation Simplifiée ZK-NR

Pour dépasser le paradoxe, on propose une implémentation simplifiée d'un protocole **Zero-Knowledge Non-Repudiation (ZK-NR)**. L'objectif est de prouver la possession d'une information **sans la révéler**, tout en assurant une non-répudiation (l'auteur ne peut pas nier avoir fourni la preuve).

V.2.0.1 Étapes du protocole simplifié

1. **Commitment (engagement)** : l'investigateur publie un engagement cryptographique E $H(nonce||secret)$.
2. **Challenge** : le vérificateur génère un défi basé sur E et un horodatage.

3. **Response** : l'investigateur calcule une réponse dérivée du secret et du défi, sans dévoiler le secret.
4. **Verification** : le vérificateur confirme la validité de la réponse en fonction du commit et du défi.

V.2.0.2 Code Python simplifié

```python
import os, hashlib, time, hmac

SECRET = b'secret_owner_key'

def commit(secret_data: bytes, nonce: bytes=None):
    if nonce is None:
        nonce = os.urandom(16)
    h = hashlib.sha256(nonce + secret_data).hexdigest()
    return {'commit': h, 'nonce': nonce.hex()}

def prove_knowledge(secret_data: bytes, commit_obj):
    ts = str(int(time.time())).encode()
    challenge = hashlib.sha256(commit_obj['commit'].encode() + ts).digest()
    response = hmac.new(secret_data, challenge, hashlib.sha256).hexdigest()
    return {'timestamp': ts.decode(), 'response': response}

def verify(commit_obj, proof, public_hint: bytes=None):
    challenge = hashlib.sha256(
        commit_obj['commit'].encode() + proof['timestamp'].encode()
    ).digest()
    if public_hint is None:
        return "Cl  de v rification manquante"
    expected = hmac.new(public_hint, challenge, hashlib.sha256).hexdigest()
    return expected == proof['response']
```

V.2.0.3 Analyse du compromis

— **Authenticité** : assurée par l'engagement et la vérification HMAC.

— **Confidentialité** : le secret n'est jamais révélé.

— **Opposabilité** : journaux d'horodatage et signature électronique rendent la preuve recevable.

— **Overhead computationnel** : faible dans cette version (quelques millisecondes par opération).

V.2.0.4 Conclusion de la Partie 4 Le paradoxe Authenticité–Confidentialité peut être modélisé mathématiquement et contourné partiellement par des protocoles ZK-NR. Cependant, un compromis reste inévitable : aucune preuve ne peut atteindre simultanément A 1, C 1 et O 1. L'investigateur doit donc choisir un point d'équilibre en fonction du contexte légal et éthique de l'affaire.

VI Partie 5 — Intégration et Synthèse Avancée

Cette partie propose de mettre en relation les dimensions philosophiques, mathématiques et techniques de l'investigation numérique à travers des cas pratiques, des débats philosophiques et un projet de recherche personnel. Elle illustre la capacité de l'investigateur à **intégrer plusieurs disciplines** afin de répondre à des défis concrets et contemporains.

VI.1 Exercice 11 — Étude de Cas Complexe : Affaire « QuantumLeaks »

VI.1.0.1 Scénario Une fuite massive de documents classifiés survient, mais ceux-ci ont été protégés par un chiffrement post-quantique. L'enjeu principal est de préserver ces preuves pendant au moins 30 ans, dans un contexte où l'informatique quantique progressera inévitablement.

VI.1.0.2 Contraintes

- Assurer une **pérennité cryptographique** des preuves malgré l'évolution des algorithmes.
- Garantir une **chaîne de conservation** fiable et opposable juridiquement.
- Préserver la **confidentialité** des informations sensibles tout en permettant une vérification indépendante.

VI.1.0.3 Plan de réponse technique et éthique

1. **Cryptographie hybride** : combiner signatures post-quantiques (Dilithium, Falcon) et schémas classiques éprouvés (RSA, ECDSA) pour garantir la transition.
2. **Horodatage et notarisation** : utiliser des services de timestamping électronique et blockchain permissionnée pour sceller l'existence des preuves.
3. **Redondance et migration** : stocker plusieurs copies distribuées juridiquement et prévoir des mises à jour cryptographiques tous les 5 ans.
4. **Éthique et confidentialité** : instaurer un comité d'éthique supervisant l'accès aux données, appliquer le principe de minimisation et recourir à l'anonymisation.
5. **Plan d'accès contrôlé** : définir des clés d'ouverture partagées (*threshold cryptography*) afin que l'accès soit conditionné à la décision collective.

VI.1.0.4 Conclusion L'affaire « QuantumLeaks »illustre l'importance d'une approche pluridisciplinaire, alliant cryptographie post-quantique, gouvernance éthique et procédures légales solides.

VI.2 Exercice 12 — Débat Philosophique Structuré

VI.2.0.1 Sujet « L'investigateur numérique peut-il rester neutre dans l'ère quantique ? »

VI.2.0.2 Organisation du débat Deux équipes sont formées :

- **Équipe Réaliste (non-neutralité)** : soutient que l'investigateur ne peut jamais être neutre, car tout choix technique ou méthodologique introduit un biais.

— **Équipe Constructiviste (neutralité procédurale)** : affirme que la neutralité parfaite est inatteignable, mais qu'une neutralité relative est possible grâce à des procédures rigoureuses.

VI.2.0.3 Arguments des Réalistes

— Chaque outil technique (hash, graphe, protocole ZK) encode une vision particulière du monde.

— L'investigateur agit toujours sous contraintes institutionnelles, politiques ou économiques.

— L'interprétation des traces numériques est subjective, dépendante du contexte.

VI.2.0.4 Arguments des Constructivistes

— Mise en place de **protocoles standardisés** et d'audits indépendants.

— Utilisation des concepts de Kuhn (paradigmes), Wheeler (participation de l'observateur) et Heidegger (technique comme dévoilement) pour montrer qu'une **neutralité procédurale** est atteignable.

— Importance de la **transparence méthodologique** : documenter chaque étape du processus réduit la subjectivité.

VI.2.0.5 Synthèse du débat

— Neutralité absolue = impossible (biais techniques et contextuels).

— Neutralité procédurale = possible, si l'investigateur adopte un cadre éthique et transparent.

— Conclusion : viser une « neutralité opérationnelle »plutôt qu'une neutralité absolue.

VI.3 Exercice 13 — Projet de Recherche Personnel

VI.3.0.1 Choix du sujet **Titre proposé :** « Mesurer l'impact des protocoles ZK-NR sur l'opposabilité juridique des preuves numériques à l'ère post-quantique ».

VI.3.0.2 Hypothèse de recherche Les protocoles ZK-NR (Zero-Knowledge Non-Repudiation) permettent de concilier confidentialité et authenticité, sans réduire significativement l'opposabilité juridique des preuves.

VI.3.0.3 Méthodologie proposée

1. **Revue de littérature** sur les preuves numériques, le non-clonage quantique, et les preuves à divulgation nulle de connaissance.
2. **Conception d'un prototype** Python simulant ZK-NR (basé sur hash et HMAC).
3. **Simulation de cas d'usage** : fuite de données, audit de logs, contrat numérique.
4. **Évaluation des indicateurs** : authenticité (A), confidentialité (C), opposabilité (O).
5. **Analyse expérimentale** : mesurer l'overhead computationnel, la scalabilité et la robustesse juridique.
6. **Production d'un rapport académique** avec résultats, discussion et recommandations.

VI.3.0.4 Apports attendus

— Définition d'une grille d'évaluation standardisée des preuves numériques.

— Preuve de concept du protocole ZK-NR pour concilier les tensions du paradoxe.

— Contribution à la doctrine juridique émergente sur la recevabilité des preuves quantiques.

VI.3.0.5 Conclusion générale de la Partie 5

Cette partie illustre la capacité de l'investigateur numérique à articuler la technique, la philosophie et le droit. Elle montre que l'avenir de l'investigation repose sur une approche interdisciplinaire capable d'intégrer les défis quantiques et éthiques dans un cadre juridique robuste.