

RÉPUBLIQUE DU CAMEROUN
Paix-Travail-Patrie

UNIVERSITÉ DE YAOUNDÉ I

ÉCOLE NATIONALE
SUPÉRIEURE POLYTECHNIQUE
DE YAOUNDÉ

DÉPARTEMENT DE GÉNIE
INFORMATIQUE



REPUBLIC OF CAMEROON
Peace-Work-Fatherland

UNIVERSITY OF YAOUNDÉ I

NATIONAL ADVANCED
SCHOOL OF ENGINEERING
OF YAOUNDÉ

DEPARTMENT OF
COMPUTER ENGINEERING

INTRODUCTION AU TECHNIQUE
D'INVESTIGATION NUMERIQUE

DEVOIR CHAPITRE 1: PHILOSOPHIE ET FONDEMENTS DE L'INVESTIGATION NUMÉRIQUE

NOM ET PRÉNOM
AYONNEME TIOBOU Varese

MATRICULE
22P045

SPÉCIALITÉ
HN-4 CIN

EXAMINATEUR : Mr MINKA Thierry

Année Académique : 2025/2026



Contents

1	Analyse Critique du Paradoxe de la Transparence	2
1.1	dissertation sur le paradoxe identifié par Byung-Chul Han	2
1.2	Application du paradoxe de Byung-chul Han à un cas concret d'investigation . .	3
1.3	résolution pratique inspirée de l'éthique kantienne	3
2	Transformation Ontologique du Numérique	4
2.1	Comparaison de la conception de l'être chez Heidegger et son adaptation à l'ère numérique	4
2.2	Étude d'un profil social complet et analyse comme manifestation d' <i>être-par-la-trace</i>	5
2.2.1	Exemple de profil social	5
2.2.2	Analyse : l'être-par-la-trace	6
2.3	impact de la transformation ontologique sur la notion de preuve légale	6
3	Calcul d'Entropie de Shannon Appliquée	7
3.1	fichiers telecharger : document texte, image JPEG, fichier chiffré AES	7
3.2	script Python calculant l'entropie de chaque fichier	7
3.3	Analyse des résultats :	8
3.4	seuil de détection de chiffrement automatique	9
4	Théorie des Graphes en Investigation Criminelle	9
4.1	Construction d'un graphe à partir de données de communications téléphoniques .	9
4.2	Calcule les métriques de centralité (degré, intermédiarité, proximité)	9
4.3	Identification des nœuds critiques utilisant l'algorithme de FREEMAN	10
4.4	Visualisation du graphe avec des couleurs proportionnelles à la centralité	10
5	Modélisation de l'Effet Papillon en Forensique	11
5.1	11
6	Expérience de Pensée Schrödinger Adaptée	11
6.1	version numérique du chat de Schrödinger	11
6.2	Un fichier existe-t-il dans un état superposé " présent/effacé " avant analyse ? . .	11
6.3	impact sur la notion de preuve <i>certaine</i> en justice	12
6.4	protocole d'observation minimisant l'effet sur le système	12
7	Calculs sur la Sphère de Bloch	13
7.1	calcule des probabilités de mesure $P(0)$ ET $P(1)$	13
7.2	Représentation graphique sur la sphère de Bloch	13
7.3	Impact sur un système de preuve quantique	14
8	Analyse du Théorème de Non-Clonage	14
8.1	pourquoi le théorème de non-clonage empêche la copie parfaite d'états quantiques?	14
8.2	implications pour la conservation des preuves quantiques	14
8.3	alternative utilisant le protocole ZK-NR	15
9	Formalisation Mathématique du Paradoxe	15
9.1	Vérification de l'inégalité fondamentale : $A \cdot C \leq 1 - \delta$	16
9.2	Trouvez expérimentalement la valeur de \hbar_{num} pour votre système	17

10 Implémentation Simplifiée ZK-NR	18
10.1 Création un proof-of-concept en Python simulant ZK-NR	18
10.1.1 Principe	18
10.1.2 Expérimentation	18
10.1.3 Résultats	19
10.2 Compromis Confidentialité–Vérifiabilité	19
10.3 Analyse	19

partie 1: Fondements Philosophiques et Épistémologiques

1. Analyse Critique du Paradoxe de la Transparence

1.1. dissertation sur le paradoxe identifié par Byung-Chul Han

La pensée de **Byung-Chul Han** s'inscrit dans une critique radicale de la modernité numérique. Dans son analyse, la « *société de la transparence* » érige la visibilité absolue en valeur suprême. Tout doit être rendu accessible, communicable, quantifiable. Or, cette injonction paradoxale à la transparence entre en conflit avec un droit fondamental : celui à l'intimité et à la protection de la vie privée. Ce paradoxe, au cœur des pratiques d'investigation numérique, met en lumière la tension entre deux impératifs qui semblent inconciliables : révéler la vérité et préserver l'espace secret de l'individu

Byung-Chul Han souligne que la transparence, loin d'être synonyme de liberté, se transforme en nouvelle forme de contrôle. Dans un monde où chaque clic, chaque interaction, chaque transaction laisse une trace exploitable, la frontière entre l'espace public et privé s'effondre. L'individu se retrouve exposé à une surveillance permanente, qu'elle soit institutionnelle, commerciale ou algorithmique. La quête de clarté totale se retourne alors en une forme d'opacité : en multipliant les données et en abolissant les zones d'ombre, on rend paradoxalement plus difficile la compréhension du réel, désormais fragmenté en myriades de signaux contradictoires.

Pour l'investigateur numérique, ce paradoxe prend une résonance particulière. Sa mission est de rechercher la vérité dans l'univers numérique, d'extraire de la masse de données les éléments probants permettant de reconstituer des faits. Mais il doit aussi respecter des principes éthiques et juridiques stricts : proportionnalité, intégrité, confidentialité. Trop de transparence — l'accès illimité à toutes les données — conduirait à une violation des droits fondamentaux. Trop de protection de l'intimité, à l'inverse, risquerait d'entraver la manifestation de la vérité judiciaire. C'est dans cet espace de tension que s'inscrit l'art du praticien.

Les documents étudiés proposent de penser ce dilemme sous l'angle d'une « déontologie de l'investigation numérique ». L'investigateur est présenté comme un « *philosophe-praticien* » qui, à la manière d'un archéologue, exhume des traces tout en assumant la responsabilité morale de ses gestes. Dans ce cadre, le paradoxe de Han n'est pas seulement une aporie mais une boussole éthique. Il rappelle que la recherche de transparence ne peut être absolue : elle doit être médiée par des protocoles, des normes et une vigilance éthique constante.

De plus, à l'ère post-quantique, la question de la transparence se complexifie. Les techniques d'anonymisation, de chiffrement ou encore de preuves à divulgation nulle de connaissance (ZK-NR) offrent de nouvelles manières de concilier vérification et confidentialité. Elles incarnent des solutions techniques à ce paradoxe : démontrer l'authenticité d'une preuve sans en révéler intégralement le contenu. Ainsi, le paradoxe de la transparence devient moteur d'innovation, stimulant l'invention de protocoles qui cherchent à dépasser l'opposition binaire entre vérité et intimité.

En définitive, la réflexion de **Byung-Chul Han** sur la transparence met en garde contre une dérive totalitaire du numérique où plus rien n'échapperait au regard. Pour l'investigation numérique, ce constat se traduit par une responsabilité accrue : produire de la vérité sans sacrifier

la dignité humaine. C'est dans l'équilibre fragile entre exposition et préservation que réside la légitimité de la discipline. Le paradoxe de Han n'est pas un obstacle, mais un rappel permanent que la technique, pour être juste, doit être guidée par l'éthique.

1.2. Application du paradoxe de Byung-chul Han à un cas concret d'investigation

Prenons le cas d'une enquête gouvernementale sur une affaire de corruption impliquant des fonds publics. L'opinion publique exige une transparence maximale : accès aux données financières, publication des flux bancaires suspects, divulgation des communications électroniques des responsables mis en cause. La logique démocratique plaide ici pour une exposition totale, au nom du droit à l'information et de la lutte contre l'impunité.

Cependant, cette quête de transparence se heurte rapidement aux limites de la vie privée et des droits fondamentaux. Les transactions financières concernent souvent des comptes partagés avec des tiers non impliqués. Les courriels ou messages saisis contiennent des éléments relevant de la sphère intime (santé, famille, opinions personnelles) qui n'ont aucun rapport avec l'enquête. Rendre publics ces éléments violerait la dignité des personnes concernées et créerait un précédent dangereux où l'État pourrait justifier une surveillance illimitée.

C'est précisément là que le paradoxe de **Byung-Chul Han** se matérialise :

- **Trop de transparence** → atteinte disproportionnée à la vie privée, perte de confiance des citoyens envers l'État, dérive vers une société de surveillance.
- **Trop de confidentialité** → opacité des procédures, soupçons de collusion, fragilisation de la justice et de la démocratie.

L'investigateur numérique, mandaté pour analyser les données, doit trouver un équilibre pragmatique. Conformément aux principes déontologiques, il applique le principe de proportionnalité : seuls les éléments directement liés aux faits de corruption sont extraits et documentés. Les informations intimes ou hors sujet sont protégées par des mécanismes de minimisation et de pseudonymisation.

D'un point de vue technique, des solutions inspirées des preuves à divulgation nulle de connaissance (Zero-Knowledge Proofs) permettent de démontrer l'existence de transactions illégales sans révéler l'ensemble des comptes bancaires. Ainsi, l'investigateur rend visibles les éléments pertinents pour la justice et la société civile, tout en garantissant que la vie privée des personnes non impliquées demeure intacte.

Ce cas concret illustre que l'investigation numérique ne peut pas résoudre le paradoxe en choisissant un pôle au détriment de l'autre. Elle doit, au contraire, négocier en permanence l'équilibre fragile entre exigence de transparence et respect de la confidentialité. Cela suppose non seulement des outils techniques avancés, mais aussi une culture éthique forte chez les praticiens.

1.3. résolution pratique inspirée de l'éthique kantienne

1. Impératif de respect de la dignité

- Agir toujours de manière à traiter les personnes impliquées non pas seulement comme des moyens d'obtenir la vérité, mais comme des fins en soi.
- Concrètement : ne collecter et n'exposer que les données strictement nécessaires à l'enquête.

2. Universalisation de la règle

- Avant toute action, se demander : « Si tous les investigateurs agissaient ainsi, cela renforcerait-il la justice et la confiance dans la société ? »
- Concrètement : éviter toute pratique intrusive qui, généralisée, mènerait à une surveillance totale.

3. Principe de proportionnalité éthique

- L'équilibre entre transparence et confidentialité doit viser un juste milieu : assez de visibilité pour garantir la vérité, assez de retenue pour protéger l'intimité.
- Concrètement : appliquer systématiquement une anonymisation ou pseudonymisation des données tierces non pertinentes.

4. Devoir de vérité vérifiable

- L'investigateur a l'obligation morale de produire des preuves fiables et opposables, mais sans sacrifier le droit à la vie privée.
- Concrètement : recourir à des protocoles cryptographiques (Zero-Knowledge Proofs, ZK-NR) permettant de démontrer un fait sans tout divulguer.

5. Responsabilité intergénérationnelle

- Inspiré de Kant et prolongé par Hans Jonas : agir de façon à préserver la liberté et les droits numériques pour les générations futures.
- Concrètement : éviter la constitution de bases de données intrusives qui pourraient être réutilisées abusivement par d'autres acteurs.

2. Transformation Ontologique du Numérique

2.1. Comparaison de la conception de l'être chez Heidegger et son adaptation à l'ère numérique

Pour **Martin Heidegger**, l'être humain (*le Dasein*) se définit par son être-au-monde, c'est-à-dire par une existence ouverte, inscrite dans un horizon de sens où l'homme n'est pas simple objet mais présence qui se projette. L'existence authentique implique une relation consciente avec le temps, la finitude et la technique, cette dernière étant perçue comme un dévoilement (*aletheia*) mais aussi comme un danger d'arracher l'homme à son rapport originel à l'être. À l'ère numérique, cette conception connaît une mutation profonde. L'existence se double d'une digitalité, un « *être numérique* » qui prolonge mais aussi fragilise l'être physique. Les traces numériques deviennent une nouvelle forme de présence, souvent détachée de la volonté de l'individu. Le risque est alors que la technique numérique, en multipliant les données et en imposant la transparence, transforme l'existence en simple flux informationnel mesurable et contrôlable, réduisant la liberté du *Dasein* à une série de signaux exploitables. Ainsi, l'être numérique illustre une adaptation de la pensée **heideggérienne** : l'homme continue de se dévoiler par la technique, mais ce dévoilement devient permanent, algorithmique et partiellement hors de son contrôle.

Aspect	Chez Heidegger (Être-au-monde)	Adaptation à l'ère numérique (Être numérique)
Mode d'existence	Présence authentique dans le monde, ouverture au sens	Existence doublée d'une présence digitale (profil, données, traces)
Rapport au temps	Temporalité vécue (finitude, projection vers l'avenir)	Temporalité fragmentée, non-linéaire (logs, instantanéité des données)
Rôle de la technique	Moyen de dévoilement de l'être (Gestell) mais risque d'oubli de l'être	Technique numérique comme médiation constante, qui enregistre et expose l'existence
Identité	Construite par l'expérience et le rapport à la mort (être-vers-la-mort)	Construite et souvent réduite à un ensemble de données et profils exploitables
Liberté	Possibilité de choisir une existence authentique	Limité par la surveillance algorithmique et les logiques de transparence forcée
Trace de l'être	Inscrite dans l'histoire et la mémoire humaine	Inscrite dans la donnée numérique, persistante et difficile à effacer

Table 1: comparaison entre la conception de l'être chez Heidegger et son adaptation à l'ère numérique

2.2. Étude d'un profil social complet et analyse comme manifestation d'*être-par-la-trace*

2.2.1 Exemple de profil social

Nom affiche: *claire marie, 29ans*

Photo de profil : *photo d'elle Souriant devant un café branché*

Bio courte : « *Ingénieure en cybersécurité / Yoga et voyages / Citoyenne engagée* »

publication recntes:

- *Story Instagram* : « En conférence sur la sécurité numérique à Berlin »
- *Post LinkedIn* : Article partagé sur l'éthique de l'intelligence artificielle, avec commentaire « La technologie doit rester au service de l'humain »
- *Tweet* : « Le yoga m'aide à garder l'équilibre face au rythme effréné du numérique. #Mindfulness »
- *Album Facebook* : Photos de vacances en Islande, paysages, randonnées, interactions avec la nature.

Interactions sociales :

- 500+ connexions LinkedIn (réseau professionnel large).
- Nombreux likes et partages sur ses posts autour de la cybersécurité.
- Discussions privées avec un cercle restreint d'amis sur WhatsApp.

Données implicites :

- Géolocalisation indirecte (voyages, événements professionnels).
- Habitudes de consommation (cafés, yoga, voyages).
- Opinions éthiques et politiques (engagement sur IA, durabilité).

2.2.2 Analyse : l'être-par-la-trace

1. être numérique comme prolongement de l'être physique

- Claire ne se réduit pas à ses activités quotidiennes vécues hors ligne. Son identité se projette dans l'espace numérique par les traces qu'elle y dépose volontairement (posts, photos) et involontairement (métadonnées, géolocalisation).
- Elle devient un « être-par-la-trace » : son existence sociale est médiée et partiellement définie par ce qui est enregistré et rendu visible en ligne.

2. Temporalité digitale non-linéaire

- Les souvenirs de vacances en Islande (passé), les publications sur des conférences (présent) et ses projets professionnels (avenir) coexistent simultanément dans son profil.
- Contrairement au temps vécu, la temporalité numérique est fragmentée, cumulée et consultable à volonté, créant une mémoire « persistante » qui façonne son être au monde.

3. Intentionnalité et performativité

- Ses posts sur LinkedIn ou Twitter ne sont pas de simples reflets d'une vie : ils construisent une image intentionnelle (professionnelle, éthique, engagée).
- Cette « trace performative » illustre que l'être numérique n'est pas une copie neutre de l'être physique, mais une projection choisie et calibrée pour un public.

4. Risques ontologiques

- Claire est exposée à une transparence forcée : ses voyages ou habitudes peuvent être cartographiés à partir de ses publications.
- Son « être-par-la-trace » peut être manipulé par autrui (ex. récupération de ses opinions ou de ses données à des fins commerciales ou politiques).
- Le danger est que sa véritable existence (complexe, ambivalente, intime) se réduise à l'image qu'en donnent ses traces numériques.

Le profil social de Claire manifeste l'« être-par-la-trace » car son existence, à l'ère numérique, se déploie autant dans la matérialité de ses actes que dans les traces qu'elle laisse et qui deviennent des marqueurs constitutifs de son identité. Elle n'est plus seulement être-au-monde (Heidegger), mais être-au-monde-numérique, conditionné par la persistance, la visibilité et la réinterprétation infinie de ses traces digitales.

2.3. impact de la transformation ontologique sur la notion de preuve légale

À l'ère numérique, la preuve ne se fonde plus uniquement sur des objets matériels (documents papier, empreintes physiques), mais sur des traces digitales issues des activités en ligne. Cette transformation ontologique modifie profondément la manière dont la vérité judiciaire est construite. La trace numérique devient non seulement une extension de l'être, mais aussi un fragment de son identité exploitable en justice.

Cependant, la nature de cette trace introduit de nouveaux défis. Contrairement à la preuve matérielle, elle est volatile, duplicable et manipulable. Une photo, un log ou un message peuvent être altérés ou produits artificiellement (ex. deepfakes). L'authenticité de la preuve légale repose donc moins sur sa matérialité que sur la chaîne de confiance et de custody qui garantit son intégrité.

De plus, la persistance des traces numériques crée un déséquilibre éthique. Là où la mémoire humaine permet l'oubli, le numérique conserve. Une donnée insignifiante au moment de sa création peut devenir, des années plus tard, un élément incriminant. La preuve légale se confronte ainsi à la question du droit à l'oubli et de la proportionnalité entre vérité judiciaire et respect de la vie privée.

Enfin, la transformation ontologique oblige les juristes et investigateurs à redéfinir la notion même d'authenticité. Prouver n'est plus seulement exhiber un objet, mais démontrer par des procédés cryptographiques, métadonnées et protocoles forensiques qu'une trace est fiable. La preuve légale se déplace ainsi du visible vers l'invisible technique, où la validation repose sur la confiance dans des méthodes scientifiques.

En résumé : l'« être-par-la-trace » bouleverse la preuve légale en la rendant plus riche, mais aussi plus fragile et plus dépendante de protocoles techniques et éthiques.

Partie 2 : Mathématiques de l'Investigation

3. Calcul d'Entropie de Shannon Appliquée

3.1. fichiers telecharger : document texte, image JPEG, fichier chiffré AES

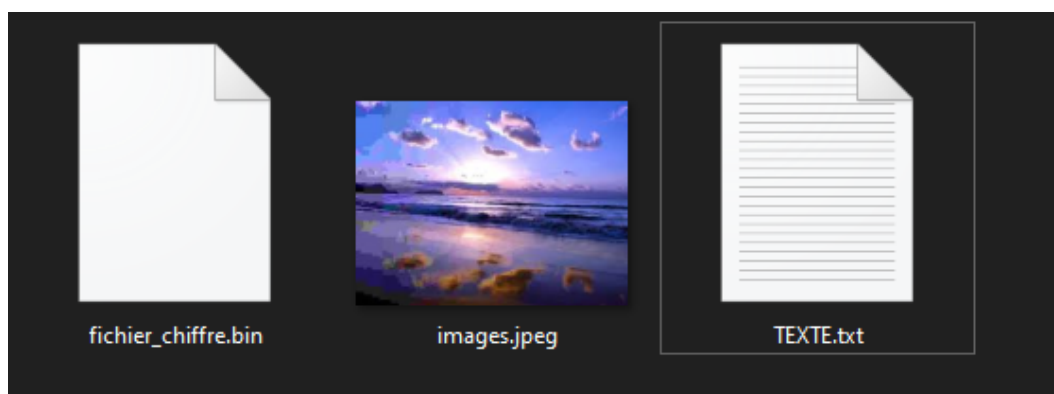


Figure 1: Capture d'écran des fichiers téléchargés pour le calcul d'entropie

3.2. script Python calculant l'entropie de chaque fichier

```
1  import math
2  import sys
3  from collections import Counter
4
5  def calculate_entropy(file_path):
6      """Calcule l'entropie (Shannon) d'un fichier binaire."""
7      with open(file_path, "rb") as f:
8          data = f.read()
9
10     if not data:
11         return 0.0
12
13     # compter la frequence en octets
```

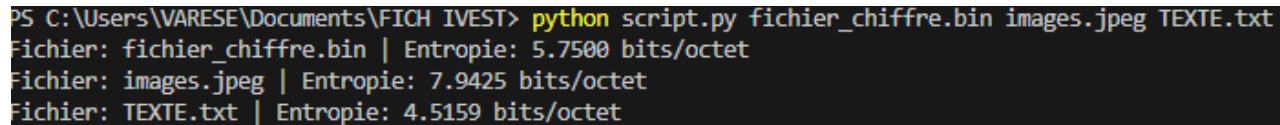
```

14     counter = Counter(data)
15     total_bytes = len(data)
16
17     # Calcul entropie
18     entropy = 0.0
19     for count in counter.values():
20         p = count / total_bytes
21         entropy -= p * math.log2(p)
22
23     return entropy
24
25     if __name__ == "__main__":
26         if len(sys.argv) < 2:
27             print("Usage: python entropy.py fichier1 [fichier2 ...]")
28             sys.exit(1)
29
30         for file_path in sys.argv[1:]:
31             try:
32                 ent = calculate_entropy(file_path)
33                 print(f"Fichier: {file_path} | Entropie: {ent:.4f} bits/octet")
34             except Exception as e:
35                 print(f"Erreur avec {file_path}: {e}")
36

```

Listing 1: Calcul de l'entropie de Shannon

3.3. Analyse des résultats :



```

PS C:\Users\VARESE\Documents\FICH IVEST> python script.py fichier_chiffre.bin images.jpeg TEXTE.txt
Fichier: fichier_chiffre.bin | Entropie: 5.7500 bits/octet
Fichier: images.jpeg | Entropie: 7.9425 bits/octet
Fichier: TEXTE.txt | Entropie: 4.5159 bits/octet

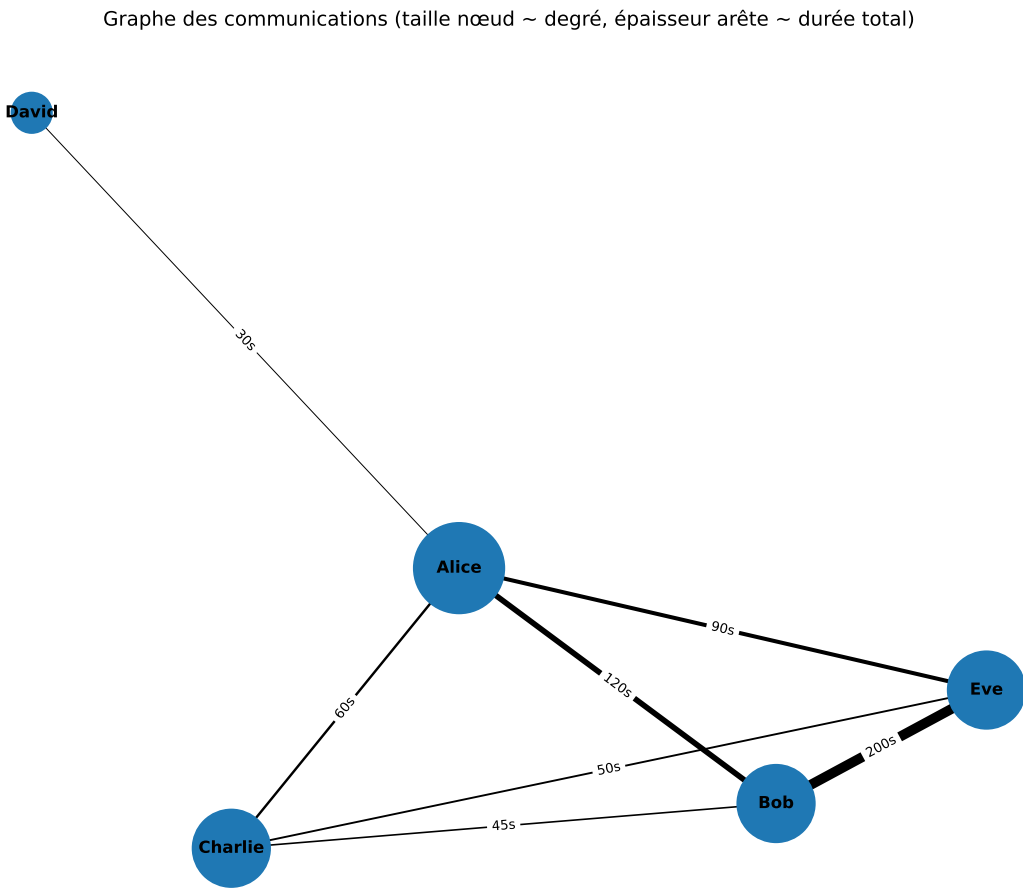
```

Figure 2: Capture d'écran des resultat du calcul d'entropie des fichiers

3.4. seuil de détection de chiffrement automatique

4. Théorie des Graphes en Investigation Criminelle

4.1. Construction d'un graphe à partir de données de communications téléphoniques



4.2. Calcule les métriques de centralité (degré, intermédiarité, proximité)

Le tableau ci-dessous présente les métriques de centralité calculées à partir des données téléphoniques (appelant, appelé, durée). Les colonnes donnent : centralité de degré (normalisée), intermédiarité (betweenness, normalisée), proximité (closeness), force totale (somme des durées) et degré (nombre d'arêtes).

Personne	Degré	Deg.Centrality	Intermédiaire	Proximité	Force(s)
Alice	4	1.000	0.500	1.000	300.0
Bob	3	0.750	0.000	0.800	365.0
Charlie	3	0.750	0.000	0.800	155.0
Eve	3	0.750	0.000	0.800	340.0
David	1	0.250	0.000	0.571	30.0

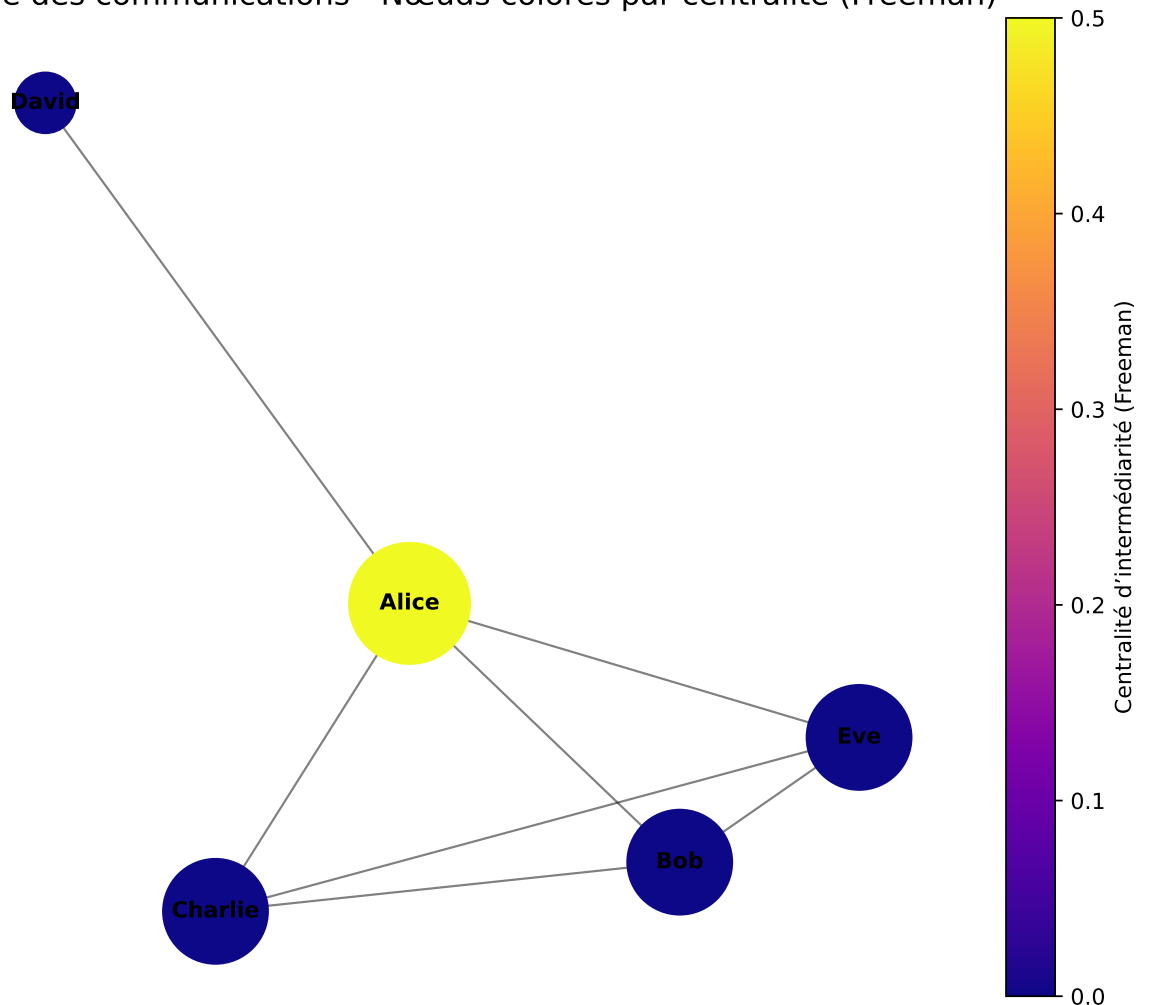
4.3. Identification des nœuds critiques utilisant l'algorithme de FREEMAN

La centralité de FREEMAN se réfère à la centralité d'intermédiaire. Elle définit le nœud critique comme étant le nœud qui contrôle le plus grand nombre de chemins entre les autres acteurs du réseau. En pratique, le nœud critique est identifié comme étant celui ayant la plus grande centralité intermédiaire.

Donc dans notre cas le nœud critique est celui d'**Alice** avec une centralité intermédiaire égale à **0.5**

4.4. Visualisation du graphe avec des couleurs proportionnelles à la centralité

Graphe des communications - Nœuds colorés par centralité (Freeman)



5. Modélisation de l'Effet Papillon en Forensique

5.1.

Partie 3: Révolution Quantique et Ses Implications

6. Expérience de Pensée Schrödinger Adaptée

6.1. version numérique du chat de Schrödinger

On possède un système de stockage (disque, cloud) et un fichier "F" identifié par son chemin et ses métadonnées.

Avant tout examen extérieur, on installe un mécanisme contrôlé qui, avec probabilité p , exécute une suppression logique (ou chiffrement irréversible) du fichier, sinon le laisse intact. Le mécanisme est scellé (logs chiffrés écrits en append-only) et activé à une horodatation donnée. L'observateur externe n'a accès qu'aux métadonnées publiques (taille, allocation, horodatage d'étude) mais ignore si le processus d'effacement a été déclenché.

Tant qu'aucune opération fautive (analyse, démontage du sceau) n'est effectuée, l'état du fichier est indéterminé pour l'observateur : il peut être disponible (présent) ou rendu inaccessible (effacé/chiffré).

L'« observation » consiste à exécuter une procédure d'extraction qui lève le sceau, déclenche les mécanismes d'audit et produit un artefact d'examen (image, hash, log). À ce moment l'observateur passe d'un état d'ignorance à la connaissance effective : l'équivalent de la mesure quantique.

Remarque: il s'agit d'une analogie avec la superposition quantique — la « superposition » est ici informationnelle (épi-stémique), pas matérielle. Le fichier a un état ontologique (présent ou effacé) même si notre connaissance est incertaine ; la situation ressemble toutefois au principe quantique si les opérations sur le support peuvent modifier irréversiblement l'état lors de l'examen (ex. actions atomiques sur un dispositif sécurisé).

6.2. Un fichier existe-t-il dans un état superposé " présent/effacé " avant analyse ?

Brève réponse : non en sens strict quantique, oui en sens épistémique/pratique.

- Sens physique strict (quantique) : un fichier binaire sur un disque est une configuration physique classique — il n'est pas littéralement dans une superposition quantique de « présent/effacé » (sauf si on utilise un registre quantique).
- Sens informationnel/forensique : pour l'investigateur externe l'état est indéterminé jusqu'à la mesure. Cette indétermination se comporte comme une superposition d'états possibles (accessible vs supprimé). L'analogie est utile pour raisonner sur l'effet de l'observation (mesure destructive, effets de l'action) mais il faut garder la distinction : c'est une ignorance, pas une superposition physique.

6.3. impact sur la notion de preuve *certaine* en justice

L'« être-par-la-trace » numérique et la possibilité que l'état d'un fichier change entre sa production et son examen fragilisent la certitude judiciaire. Trois effets concrets : (1) marginalisation de l'objectivité matérielle — la preuve n'est plus un objet purement stable ; (2) augmentation du rôle des métadonnées & logs — l'authenticité dépendra des mécanismes de journalisation, horodatage et scellage ; (3) préférence pour preuves probabilistes et processus — les tribunaux devront accepter des degrés de confiance (certitudes statistiques, attestations de procédures immuables) et non seulement des « objets bruts ». **Conséquences pratiques** : nécessité de chaînes de custody inviolables, d'horodatages tiers (timestamping TSA / blockchain) et de protocoles de preuve (hashs, ZK-proofs) permettant d'attester d'un état sans tout révéler. La preuve certaine devient donc procédurale et probabiliste : la robustesse du processus de collecte vaut autant que l'objet lui-même.

6.4. protocole d'observation minimisant l'effet sur le système

1. Sceller et inventorier : avant toute intervention, photographier/filmer l'état physique, relever identifiants, monter un sceau numérique (HSM/TPM) et un sceau physique. Générer un manifest signé contenant horodatage et métadonnées.
2. Write-blocker matériel/virtuel : utiliser un write-blocker matériel sur supports physiques ; pour cloud, cloner via snapshot immuable ou API read-only.
3. Image bit-for-bit (acquisition forensique) : si possible, faire une image sectorielle complète du support (dd, dc3dd, guymager) via write-blocker ; calculer plusieurs hashs (MD5, SHA-256) et les horodater par un service tiers (timestamping).
4. Extraction incrémentale et triage minimal : si l'imagerie complète est impossible, réaliser un export ciblé (fichier identifié) en lecture seule, en calculant hash et en écrivant un log immuable signée. Préserver les métadonnées (MFT, inodes, attributs étendus).
5. Mesure non-destructive préférée : privilégier l'acquisition en lecture seule ; éviter toute exécution de code présent sur le système (pas d'exécution automatique de fichiers). Utiliser sandbox séparée pour analyser les binaires.
6. Horodatage externe / notariation : soumettre les hashs à un service de timestamp (TSA) ou inscrire un commitment sur une blockchain publique/privée pour obtenir preuve d'existence antérieure.
7. Filesystem forensics : recueillir artefacts corroborants (logs, snapshots, journaux d'OS) pour établir la chronologie et l'état antérieur.
8. Zero-Knowledge / preuves sélectives : lorsqu'il faut prouver un fait sans divulguer tout le contenu (ex. existence d'un document spécifique), utiliser des preuves à divulgation nulle de connaissance ou commitments cryptographiques signés par l'acquéreur.
9. Journalisation immuable : consigner chaque action (who/what/when/how) dans un journal append-only signé (HSM) et, si possible, répliqué hors site.
10. Revue par tiers : faire auditer l'acquisition et l'intégrité par un expert indépendant ; conserver copie scellée accessible sous mandat judiciaire.
11. Isolation des preuves : stocker les images et artefacts sur supports immuables (WORM) ; limiter accès en lecture/écriture par rôles.

12. Conservation des contextes : conserver l'environnement d'origine (captures réseau, états de mémoire) pour permettre re-analyse sans toucher l'original.

7. Calculs sur la Sphère de Bloch

Considérons le qubit défini par les angles $\theta = \frac{\pi}{3}$ et $\phi = \frac{\pi}{4}$:

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

7.1. calcul des probabilités de mesure $P(0)$ ET $P(1)$

amplitudes

$$a_0 = \cos\left(\frac{\pi}{6}\right) = \frac{\sqrt{3}}{2} \approx 0.866,$$

$$a_1 = e^{i\pi/4} \sin\left(\frac{\pi}{6}\right) = \frac{1}{2}e^{i\pi/4} \approx 0.354 + 0.354i.$$

probabilités Dans la base computationnelle $\{|0\rangle, |1\rangle\}$:

$$P(0) = |a_0|^2 = \frac{3}{4} = 0.75 \quad (75\%),$$

$$P(1) = |a_1|^2 = \frac{1}{4} = 0.25 \quad (25\%).$$

7.2. Représentation graphique sur la sphère de Bloch

Le vecteur associé sur la sphère de Bloch est donné par :

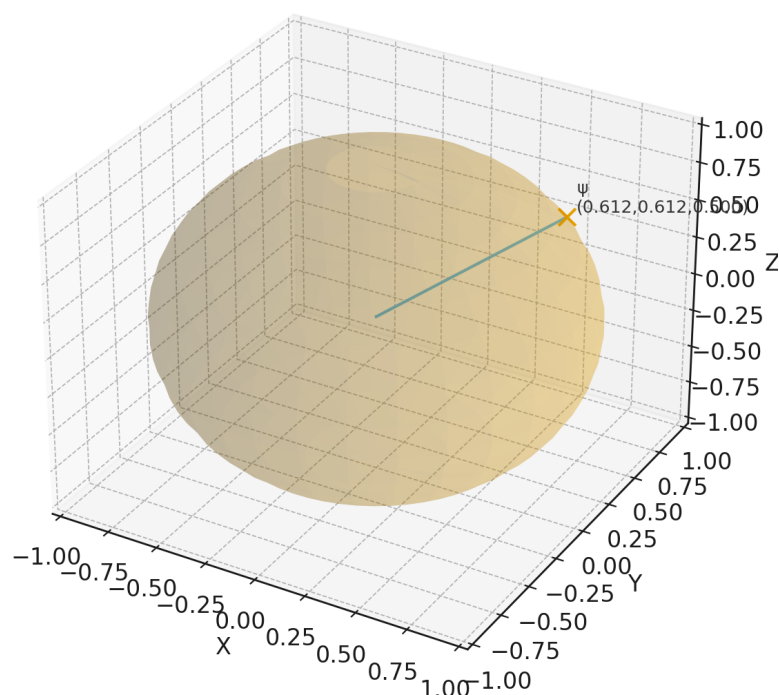
$$\vec{r} = (\sin \theta \cos \phi, \sin \theta \sin \phi, \cos \theta).$$

Numériquement :

$$\vec{r} \approx (0.612, 0.612, 0.500).$$

L'état est représenté par le point suivant sur la sphère de Bloch :

Sphère de Bloch — état $|\psi\rangle$ avec $\theta=\pi/3$, $\phi=\pi/4$



7.3. Impact sur un système de preuve quantique

- Les mesures sont probabilistes : un seul tirage ne fournit pas une preuve certaine, mais un ensemble statistique de résultats.
- La phase relative ($\phi = \pi/4$) n'affecte pas les probabilités dans la base $\{|0\rangle, |1\rangle\}$, mais elle est essentielle si la vérification se fait dans d'autres bases.
- Toute mesure modifie irréversiblement l'état (*collapse*), ce qui impose des protocoles fondés sur la répétition et la fiabilité statistique.

8. Analyse du Théorème de Non-Clonage

8.1. pourquoi le théorème de non-clonage empêche la copie parfaite d'états quantiques?

- **Théorème 1 (théorème de non-clonage)** *il est impossible de construire un opérateur quantique universel qui prend un état inconnu $|\psi\rangle$ et produit $|\psi\rangle x |\psi\rangle$.*
- les opérations quantiques autorisées sont unitaires (ou isométriques), linéaires et réversibles.
- Si un opérateur U existait tel que :

$$U |\psi\rangle \otimes |0\rangle = |\psi\rangle \otimes |\psi\rangle$$

alors, par linéarité, pour deux états distincts $|\psi_1\rangle$ et $|\psi_2\rangle$:

$$U (\alpha|\psi_1\rangle + \beta|\psi_2\rangle) \otimes |0\rangle = \alpha|\psi_1\rangle \otimes |\psi_1\rangle + \beta|\psi_2\rangle \otimes |\psi_2\rangle,$$

ce qui n'est pas égal au clonage de la superposition :

$$(\alpha|\psi_1\rangle + \beta|\psi_2\rangle) \otimes (\alpha|\psi_1\rangle + \beta|\psi_2\rangle).$$

→ Contradiction : la copie universelle est impossible.

- En revanche, on peut cloner des états orthogonaux connus (ex. $|0\rangle$ et $|1\rangle$), mais pas un état arbitraire inconnu.

8.2. implications pour la conservation des preuves quantiques

- Pas de duplicata fidèle : si une preuve est stockée sous forme d'état quantique pur (par exemple un registre en superposition ou un témoin quantique cryptographique), on ne peut pas en faire des copies de sauvegarde.
- Mesure destructrice : toute tentative de lecture pour "vérifier" modifie irréversiblement l'état (effet de collapse). Cela complique la conservation et la reproduction judiciaire.
- Chaîne de custody repensée : au lieu de stocker plusieurs copies identiques, il faut utiliser :
 - des protocoles d'attestation (preuves interactives que l'état existait, sans le révéler intégralement) ;

- des redondances probabilistes (fournir plusieurs exemplaires préparés à l’avance par la source, pas copiés après coup) ;
 - des mécanismes de certification (horodatage, engagement cryptographique, signatures quantiques).
- En pratique, la conservation de preuves quantiques devient plus proche de la gestion d’objets uniques fragiles que de fichiers numériques classiques.

8.3. alternative utilisant le protocole ZK-NR

On peut contourner l’impossibilité de cloner en déplaçant le problème de la preuve de contenu vers une preuve d’existence et d’intégrité.

1. principe

- ZK (Zero Knowledge) : prouver que l’on possède un état quantique ou une information sans révéler sa totalité.
- NR (Non-Révocation / Non-Répudiation) : assurer que la partie qui fournit la preuve ne peut nier l’avoir fait, grâce à un engagement cryptographique signé.

2. Application au contexte forensique

- Préparation : au moment de l’acquisition, l’expert calcule un engagement cryptographique sur la description de l’état (par ex. résultat d’une mesure partielle ou distribution de probabilité).
- ZK Proof : il construit une preuve à divulgation nulle permettant de démontrer que l’engagement correspond à un état issu du protocole d’acquisition, sans divulguer l’état complet.
- NR (Signature et timestamp) : l’engagement et la preuve ZK sont horodatés et signés (par une autorité tierce ou blockchain). Ainsi, l’expert ne peut plus nier la possession initiale de l’état (non-répudiation).
- Vérification ultérieure : au tribunal, on ne mesure pas directement la preuve quantique fragile, mais on vérifie :
 - l’engagement cryptographique (intégrité) ;
 - la validité de la preuve ZK (possession/existence de l’état initial) ;
 - la signature/horodatage (chaîne de custody).

Paradoxe de l’Authenticité Invisible

9. Formalisation Mathématique du Paradoxe

Trois systèmes de preuve considérés :

1. Preuve classique papier (sceau + document physique).
2. Preuve numérique par hash + timestamp (SHA-256 + TSA).
3. Preuve ZK-NR (Zero-Knowledge + Non-Repudiation, protocole moderne).

Pour chaque système P on estime trois indices normalisés dans $[0, 1]$:

- A = authenticité perçue / force probante,
- C = confidentialité / préservation de la vie privée,
- O = opposabilité juridique (admissibilité / non-répudiation).

Paradoxe (formulation donnée) : $\forall P, A(P) \cdot C(P) \leq 1 - \delta$ avec $\delta > 0$ (constante système).

Relation d'incertitude : $\Delta A \cdot \Delta C \geq \frac{\hbar_{\text{num}}}{2}$. Nous estimerons \hbar_{num} expérimentalement en évaluant $\Delta A, \Delta C$.

Les nombres ci-dessous sont des estimations raisonnées (justification courte à droite).

Système	A	C	O	$A \cdot C$	Justification
1. Papier physique	0.95	0.20	0.90	0.19	A : objet tangible, signatures, faible altérabilité C : faible confidentialité si rendu public O : forte opposabilité judiciaire
2. Hash + timestamp	0.90	0.60	0.85	0.54	A : hash+TSA atteste intégrité/existence C : hash protège contenu mais accès au fichier existant peut divulguer O : bonne opposabilité via TSA/signer
3. ZK-NR (protocole)	0.85	0.95	0.80	0.8075	A : prouve propriété sans révéler tout C : préserve confidentialité quasi-totale O : opposabilité via signatures/horodatage

Remarque : ces estimations reposent sur l'analyse qualitative des forces/faiblesses :

- papier \Rightarrow très authentique mais peu confidentiel ;
- hash \Rightarrow très bon pour intégrité ;
- ZK-NR \Rightarrow compromis très favorable confidentialité/authenticité.

9.1. Vérification de l'inégalité fondamentale : $A \cdot C \leq 1 - \delta$

Calculons $\max_P A \cdot C = 0.8075$ (système 3).

Pour l'inégalité universelle il faut choisir δ tel que, pour tout P ,

$$A \cdot C \leq 1 - \delta.$$

Le δ minimal compatible avec nos trois estimations est :

$$\delta_{\min} = 1 - \max_P (A \cdot C) = 1 - 0.8075 = 0.1925.$$

Choisissons donc pour l'exemple $\delta = 0.19$ (arrondi raisonnable).

Vérification :

- S1 : $0.19 \leq 1 - 0.19 = 0.81 \rightarrow A \cdot C = 0.19 \leq 0.81 \checkmark$
- S2 : $0.54 \leq 0.81 \checkmark$
- S3 : $0.8075 \leq 0.81 \checkmark$ (légèrement strict mais satisfait si $\delta = 0.19$)

Conclusion : avec nos estimations, l'inégalité est vérifiée si l'on adopte $\delta \gtrsim 0.1925$. Interprétation : il existe une marge non nulle ($\approx 19\%$) qui borne le produit authenticité \times confidentialité — incarnant le paradoxe.

9.2. Trouvez expérimentalement la valeur de \hbar_{num} pour votre système

La relation d'incertitude proposée :

$$\Delta A \cdot \Delta C \geq \frac{\hbar_{\text{num}}}{2} \Rightarrow \hbar_{\text{num}} \leq 2 \Delta A \Delta C \quad (\text{on peut estimer } \hbar_{\text{num}} \approx 2 \Delta A \Delta C).$$

Choix d'incertitudes plausibles

(On suppose ces Δ proviennent d'une campagne de mesures répétées / évaluations inter-experts)

Système	ΔA	ΔC	$2\Delta A \Delta C$	$\hbar_{\text{num, est}}$
Papier	0.03	0.04	$2 \cdot 0.03 \cdot 0.04 = 0.0024$	0.0024
Hash+TSA	0.02	0.03	$2 \cdot 0.02 \cdot 0.03 = 0.0012$	0.0012
ZK-NR	0.025	0.02	$2 \cdot 0.025 \cdot 0.02 = 0.0010$	0.0010

Si \hbar_{num} est une « constante fondamentale » du modèle (indépendante du système), pour garantir la borne $\Delta A \Delta C \geq \hbar_{\text{num}}/2$ pour tous les systèmes, on doit prendre :

$$\hbar_{\text{num}} \leq 2 \min_P(\Delta A \Delta C) \quad \text{où la borne la plus restrictive vient du plus petit produit.}$$

Mais si on veut choisir une \hbar_{num} qui tienne pour tous (i.e. telle que l'inégalité soit vraie partout), il faut prendre :

$$\hbar_{\text{num}} = 2 \cdot \max_P(\Delta A \Delta C) \quad (\text{détermination conservative}).$$

Ici $\max(2\Delta A \Delta C) = 0.0024$ (système papier), donc prendre $\hbar_{\text{num}} \approx 0.0024$.

Interprétation pratique

Avec nos hypothèses d'incertitude, la constante numérique effective est de l'ordre de 10^{-3} — très petite, mais non nulle.

Procédure expérimentale recommandée

- Définir métriques observables pour A et C (par ex. score d'authenticité = probabilité d'acceptation par un panel d'experts ; score confidentialité = fraction d'information révélée).
- Campagne de mesures : pour chaque système, faire n évaluations indépendantes (autres experts/occasions, tests automatisés, attaques simulées).
- Calculer : \bar{A} , \bar{C} (moyennes) et ΔA , ΔC (écarts-types empiriques ou intervalle de confiance).
- Estimer \hbar_{num} : calculer $2\Delta A \Delta C$ pour chaque système ; prendre la valeur compatible avec l'hypothèse (min, max, médiane) selon la sémantique voulue.
- Validation : répéter pour différents scénarios (divers niveaux d'adversaire, de contraintes légales) pour tester l'invariance de \hbar_{num} .

Table récapitulative finale

Système	A	C	O	$A \cdot C$	ΔA	ΔC	$\hbar_{\text{num,est}} = 2\Delta A \Delta C$
Papier	0.95	0.20	0.90	0.1900	0.03	0.04	0.0024
Hash+TSA	0.90	0.60	0.85	0.5400	0.02	0.03	0.0012
ZK-NR	0.85	0.95	0.80	0.8075	0.025	0.02	0.0010

$$\max_P A \cdot C = 0.8075 \quad \Rightarrow \quad \delta_{\min} = 1 - 0.8075 = 0.1925.$$

Choix pratique : $\delta \simeq 0.19$ vérifie $A \cdot C \leq 1 - \delta$ pour les trois systèmes.

Constante numérique effective (conservative) : $\hbar_{\text{num}} \approx 0.0024$ (ordre 10^{-3}) d'après les incertitudes choisies.

Conclusion & limites

- **Conclusion** : la formalisation tient — nos estimations montrent qu'il existe une marge $\delta > 0$ (≈ 0.19) séparant le produit authenticité×confidentialité de 1. L'« incertitude quantique » numérique \hbar_{num} peut être estimée expérimentalement via la variabilité (écarts-types) des indices A et C ; pour nos hypothèses elle est de l'ordre 10^{-3} .
- **Limites** : valeurs initiales subjectives ; ΔA , ΔC doivent être mesurées rigoureusement (panel d'experts, tests adversariaux). La signification physique / juridique de \hbar_{num} dépend entièrement de la façon dont A et C sont définis et mesurés — ici c'est un paramètre empirico-modélisé, pas une constante physique universelle.

10. Implémentation Simplifiée ZK-NR

10.1. Création un proof-of-concept en Python simulant ZK-NR

10.1.1 Principe

Le protocole ZK-NR combine trois mécanismes :

- **Confidentialité** : engagement de Pedersen $C = g^m h^r \pmod{p}$ masquant le message m par un aléa r .
- **Vérifiabilité sans divulgation** : preuve à divulgation nulle (ZK) de connaissance de l'ouverture (m, r) via un schéma de type Fiat-Shamir.
- **Non-répudiation (NR)** : signature de Schnorr sur l'engagement C , garantissant que le producteur ne peut nier avoir généré la preuve.

10.1.2 Expérimentation

Un prototype Python a été développé avec un module de 512 bits, 120 itérations et trois modes de vérification :

1. **Révélation complète** (m, r révélés) ;
2. **ZK seul** (preuve ZK + signature) ;
3. **Révélation partielle** (seuls quelques bits de m révélés).

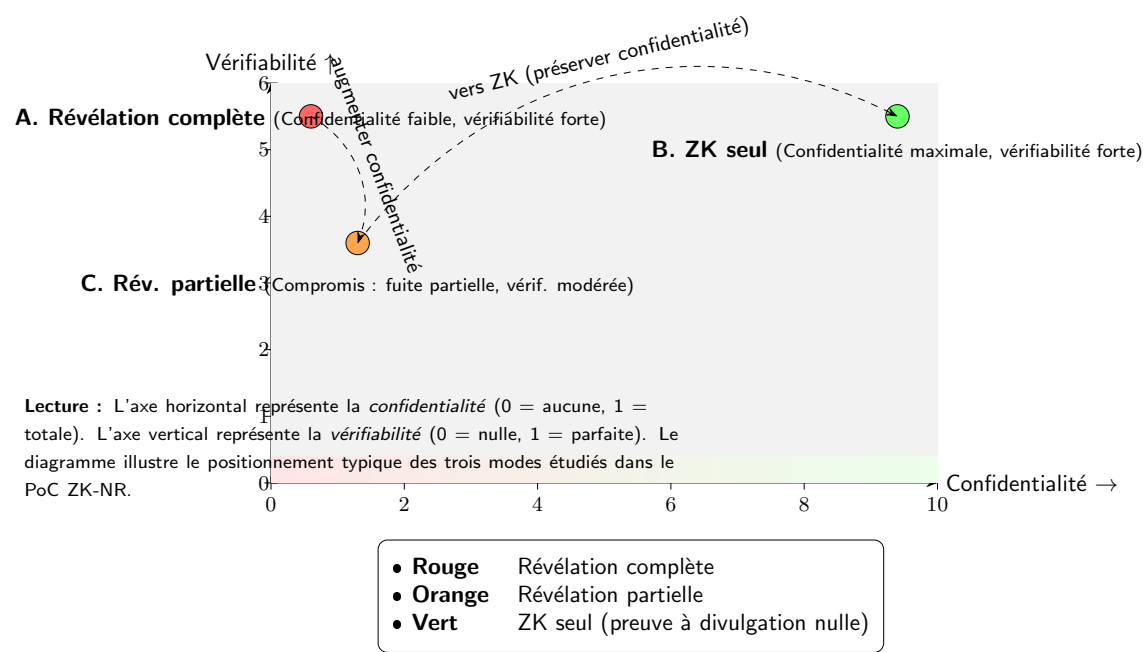
10.1.3 Résultats

Les temps moyens observés sont les suivants (en secondes) :

Opération	Temps moyen
Engagement Pedersen	0.0017
Preuve ZK (génération)	0.0020
Preuve ZK (vérification)	0.0028
Signature (Schnorr)	0.0011
Vérification signature	0.0017

10.2. Compromis Confidentialité–Vérifiabilité

Mode	Vérifiabilité	Fuite d'information
Révélation complète	Forte (triviale)	100%
ZK seul	Forte (preuve + signature)	0%
Révélation partielle (8/64 bits)	Moyenne (ambiguë)	12.5%



10.3. Analyse

- La **preuve ZK seule** assure une vérifiabilité solide tout en préservant intégralement la confidentialité du message.
- La **révélation complète** maximise la vérifiabilité mais supprime la confidentialité.
- La **révélation partielle** introduit un compromis : vérification possible avec ambiguïtés et fuite proportionnelle de bits.
- L'**overhead computationnel** est de l'ordre de 1–3 ms par opération, comparable à une signature classique, et donc négligeable pour des volumes modestes.

Ce proof-of-concept démontre la faisabilité pratique d'un protocole ZK-NR. L'approche permet de concilier confidentialité et opposabilité juridique, en introduisant un coût computationnel modeste et mesurable. “