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

PRÉSENTATION DÉTAILLÉE DU PROTOCOLE ZK-NR : RL ET POSITIONNEMENT DANS L'INVESTIGATION NUMÉRIQUE MODERNE

Rédigé par :

FANTA YADON Félicité (chef)	22P069
GHOUMO DONFACK Olivia Shelsie	22P023
MAKEU TENKU Stely Belva	24P826

Supervisé par :

M. Thierry MINKA

Table des matières

Introduction

À l'ère du numérique, la cryptographie s'est imposée comme un pilier fondamental de la sécurité des communications. Nous maîtrisons aujourd'hui les mécanismes de chiffrement – qu'ils soient symétriques ou asymétriques – qui permettent de protéger la confidentialité de nos échanges. Grâce au chiffrement asymétrique utilisant des paires de clés publiques et privées, nous pouvons sécuriser nos données contre l'interception et prévenir les attaques de type man-in-the-middle.

Toutefois, la simple confidentialité ne suffit plus. Dans un monde où les transactions numériques ont acquis une importance juridique et économique considérable, trois questions cruciales demeurent : Comment garantir l'authenticité d'un message ? Comment empêcher son expéditeur de nier l'avoir envoyé ? Et surtout, comment donner à ces preuves numériques une valeur légale opposable devant un tribunal ?

Prenons deux scénarios révélateurs :

— Dans le premier, Alice envoie un message à Bob pour lui proposer un rendez-vous. Malgré le chiffrement, un attaquant pourrait intercepter ce message et en envoyer un autre, totalement différent et potentiellement menaçant, en se faisant passer pour Alice. Bob recevrait alors un message qu'il croirait authentique, sans aucun moyen de vérifier sa provenance réelle.

— Dans le second scénario, Alice envoie un message compromettant à Bob, qui décide de porter plainte. Alice nie catégoriquement être l'auteure de ce message. Sans mécanisme d'authentification robuste, comment Bob pourrait-il prouver devant un juge que ce message provient effectivement d'Alice ? Et inversement, comment Alice pourrait-elle se protéger contre une fausse accusation ?

C'est précisément à cette intersection entre cryptographie et droit que se situe notre exposé : l'opposabilité légale de la cryptographie. Nous explorerons comment les technologies **cryptographiques** notamment les **signatures numériques** et les **infrastructures à clés publiques** peuvent non seulement résoudre ces problèmes techniques d'authentification et de non-répudiation, mais aussi acquérir une valeur probatoire reconnue par les systèmes juridiques.

I Concepts Clés

I.1 La non-répudiation numérique

La non-répudiation est le fait de s'assurer qu'un contrat, notamment un contrat signé via internet, ne peut être remis en cause par l'une des parties.

Dans le domaine de la sécurité des systèmes d'information, la non-répudiation signifie la possibilité de vérifier que l'envoyeur et le destinataire sont bien les parties qui disent avoir respectivement envoyé ou reçu le message. Autrement dit, la non-répudiation de l'origine prouve que les données ont été envoyées, et la non-répudiation de l'arrivée prouve qu'elles ont été reçues.

I.1.1 Les enjeux de la non-répudiation numérique :

La non-répudiation numérique a diverses enjeux, certains étant :

— **Sécurité des Transactions Électroniques** : La non-répudiation est essentielle pour sécuriser les transactions en ligne (e-commerce, banque, contrats électroniques). Elle permet de prouver l'origine et l'intégrité des données échangées, limitant ainsi les risques de fraude ou de litige.

— **Valeur Juridique des Preuves Numériques** : En cas de conflit, la non-répudiation fournit des preuves irréfutables devant les tribunaux. Par exemple, une signature électronique qualifiée a la même valeur qu'une signature manuscrite.

— **Confiance dans les Systèmes Numériques** : Elle renforce la confiance des utilisateurs et des entreprises dans les systèmes numériques, en garantissant que les engagements pris ne peuvent être reniés. Cela est crucial pour l'adoption massive des services en ligne.

— **Protection contre la Fraude et l'Usurpation** : La non-répudiation permet de détecter et de prévenir les tentatives d'usurpation d'identité ou de falsification de documents, en associant de manière indissociable une action à son auteur.

— **Conformité Réglementaire** : De nombreux secteurs (banque, santé, administration) sont soumis à des réglementations strictes exigeant la non-répudiation pour la traçabilité et l'auditabilité des actions (ex : RGPD, normes ISO 27001).

I.1.2 Les Outils de la non-répudiation numérique :

— **La Signature Numérique :** La signature numérique repose sur un mécanisme cryptographique asymétrique, où une paire de clés (une privée et une publique) est générée à partir d'algorithmes reconnus comme RSA.

La clé privée, strictement confidentielle et détenue par le signataire, permet de produire une signature unique sur un document, tandis que la clé publique, accessible à tous, sert à vérifier cette signature.

Concrètement, le document est d'abord transformé en une empreinte numérique via une fonction de hachage, puis cette empreinte est chiffrée avec la clé privée pour générer la signature. Le destinataire, en utilisant la clé publique du signataire, peut déchiffrer la signature, recalculer l'empreinte du document reçu, et comparer les deux. Si elles correspondent, l'authenticité du signataire et l'intégrité du document sont confirmées.

— **Le certificat électronique :** Il agit comme une pièce d'identité numérique en associant de manière indissociable une identité (qu'il s'agisse d'une personne, d'un serveur ou d'une organisation) à une clé publique.

Le certificat électronique est émis par une autorité de certification de confiance, ce certificat contient non seulement la clé publique, mais aussi des informations d'identification, une période de validité, et la signature numérique de l'autorité de certification. La confiance dans le certificat repose sur une chaîne de certification, où chaque autorité de certification est elle-même certifiée par une autorité de certification de niveau supérieur, jusqu'à une autorité de certification racine. La validation d'un certificat implique la vérification de sa signature et de son statut de révocation, via des protocoles comme OCSP ou des listes CRL. Sans certificat valide, la clé publique ne peut être considérée comme fiable, ce qui compromettrait l'ensemble du système de signature et d'authentification.

— **L'horodatage numérique :** Ceci apporte une dimension temporelle essentielle à la non-répudiation, en attestant qu'un document ou une transaction existait à une date et une heure précises. Pour ce faire, un serveur d'horodatage (TSA - Timestamp Authority Server) reçoit une empreinte du document, y appose une marque temporelle signée, et renvoie un jeton d'horodatage conforme à la RFC 3161. Ce jeton, qui inclut l'empreinte, la date/heure UTC, et la signature du TSA, peut être vérifié ultérieurement pour prouver que le document n'a pas été modifié depuis son horodatage. Ce mécanisme est particulièrement crucial dans les contextes juridiques ou réglementaires, où la preuve de l'antériorité d'un document peut être déterminante.

— **La fonction de hachage :** Elle joue un rôle central dans la garantie de l'intégrité des données. Elle transforme un document de taille arbitraire en une chaîne de caractères de longueur fixe, appelée empreinte, qui agit comme une signature unique du contenu. Les algorithmes de hachage, tels que SHA-256 ou SHA-3, sont conçus pour être déterministes, irréversibles et résistants aux collisions, ce qui signifie qu'il est pratiquement impossible de retrouver le document original à partir de son empreinte ou de trouver deux documents produisant la même empreinte. Toute modification, même minime, du document original entraîne une empreinte totalement différente, permettant ainsi de détecter instantanément toute altération. Cette propriété est exploitée dans les signatures numériques, les protocoles de sécurité, et les systèmes de preuve d'intégrité, comme les blockchains.

II État de l'art et travaux récents

II.1 Présentation synthétique des articles

Exploration de ZK-NR : Vision Globale et Applications

Le protocole **ZK-NR** (Zero-Knowledge Non-Repudiation) est une architecture cryptographique modulaire en couches, axée sur la **non-répudiation préservant la confidentialité** pour la co-production de services numériques publics. Il combine des primitives post-quantiques (STARKs, signatures BLS à seuil, Dilithium) pour créer des preuves sécurisées, vérifiables et surtout **auditables**, sans jamais révéler de contenu sensible. Modélisé dans Tamarin, il s'adresse spécifiquement aux environnements réglementés (finance, e-gouvernement) en offrant des attestations juridiquement admissibles, comblant le fossé entre la sécurité cryptographique et les exigences institutionnelles.**Le Trilemme CRO : Équilibre entre Confidentialité, Fiabilité et Opposabilité**

Le **Trilemme CRO** formalise une incompatibilité fondamentale pour tout système de preuve post-quantique : il est impossible de satisfaire simultanément la **Confidentialité** (Priv), la **Fiabilité** (Rel) et l'**Opposabilité Juridique** (H_{Opp}). Une borne d'impossibilité est établie par la formule : $H_{\text{Opp}} \leq f(\text{Priv}, \text{Rel}) + \eta_q(C) + \text{negl}(\lambda)$. Cette analyse théorique, validée empiriquement ($\Gamma_{\text{CRO}} > 0,8$), sert de fondation théorique aux architectures cherchant à minimiser cette violation, définissant ainsi les contraintes de base pour des protocoles comme ZK-NR. **Q2CSI : Infrastructure de Sécurité Quantique Composable et Contextuelle**

Q2CSI (Quantum-to-Classical Security Infrastructure) est un cadre en couches conçu pour résoudre le Trilemme CRO en décomposant la sécurité en trois strates isolées mais composables : *Fer* (Fiabilité), *Or* (Confidentialité) et *Argile* (Opposabilité). Ce cadre abstrait étend le modèle de Composabilité Universelle (UC) en intégrant des contraintes entropiques, lui permettant d'atteindre une violation du trilemme significativement réduite ($\Gamma_{\text{CRO}} < 0,4$). Basé sur des primitives minimales (IND-CCA2, EUF-CMA), Q2CSI propose la première architecture formelle pour des protocoles post-quantiques juridiquement vérifiables. **Design ZK-NR / Formalizing ZK-NR : Cadre Théorique et Modélisation**

La formalisation du protocole **ZK-NR** s'attache à son design théorique et à sa modélisation. En s'appuyant directement sur les contraintes du trilemme CRO, cette contribution détaille comment des primitives spécifiques (engagements Merkle, STARKs, etc.) sont agencées pour atteindre l'équilibre requis entre **responsabilité** et **confidentialité**. Cette phase inclut une preuve de concept et une modélisation dans l'outil **Tamarin**, fournissant des artefacts pratiques sans encore proposer de preuves formelles de sécurité, lesquelles sont réservées à des travaux futurs.

Le Problème AIIP : Problématiques d'Authenticité et d'Intégrité des Preuves

Le **Problème d'Inversion Itérée Affine (AIIP)** est l'hypothèse cryptographique fondamentale du cadre CASH. Reposant sur la difficulté de résoudre des équations quadratiques multivariées (MQ) et des logarithmes discrets sur des courbes hyperelliptiques de genre élevé (HCDLP), l'AIIP garantit l'**authenticité** et l'**intégrité** des preuves dans les systèmes post-quantiques. Il sert de base de sécurité pour les trois primitives CASH (CEE, AOW, SH), offrant une résilience prouvée contre les adversaires quantiques et assurant la solidité des preuves. **CEE : Cryptographic Evi-**

dence Explainability (Lien vers la Confidentialité)

L'**Expansion Entropique Chaotique (CEE)** est une fonction à sens unique post-quantique, basée sur l'itération de cartes polynomiales. Sa sécurité repose sur l'AIIP. CEE est le composant du cadre CASH dédié à la **Confidentialité** (Privacy), assurant une expansion entropique qui atteint une min-entropie prédictible et une distance statistique minimale par rapport à l'uniforme. Bien que son mécanisme soit plus lent que des solutions classiques comme l'AES, elle assure la résilience quantique nécessaire pour la préservation de l'entropie sémantique des données.

AOW : Affine One-Wayness (Lien vers la Fiabilité)

L'**Affine One-Wayness (AOW)** est le primitif CASH focalisé sur la **Fiabilité** (Reliability) via la vérification temporelle post-quantique. Basé sur l'AIIP, AOW permet une liaison temporelle robuste intégrée aux preuves STARKs. Il garantit ainsi l'ordonnancement d'événements et la synchronisation distribuée, résistant aux fautes byzantines. AOW répond directement à la propriété de fiabilité du trilemme CRO en assurant l'intégrité et la non-contestabilité du temps de production de la preuve. **SH : Semantic Holder (Lien vers l'Opposabilité)**

Le **Semantic Holder (SH)** est le composant CASH dédié à l'**Opposabilité Juridique** (Opposability). Basé sur l'AIIP, SH garantit des interprétations juridiques vérifiables des preuves. Il permet l'extraction algébrique des traces d'itération polynomiale, assurant un score d'opposabilité élevé ($\Omega \geq 0,60$) grâce à la préservation de l'entropie et à l'**explicabilité institutionnelle**. SH est essentiel pour les applications réglementaires comme les contrats intelligents juridiques et l'audit.

II.2 Synthèse comparative

L'ensemble des travaux présentés forme un écosystème de recherche cohérent, centré sur la construction d'une sécurité cryptographique post-quantique qui respecte les exigences institutionnelles de confiance et de droit.

TABLE 1 – Points Communs et Hypothèses Fondamentales

Caractéristique	Description et Travaux Concernés
Sécurisation des Preuves	Tous les travaux ont pour but de garantir l'intégrité et l'authenticité des preuves cryptographiques (ZK-NR, Q2CSI, CEE, AOW, SH).
Non-Répudiation	Objectif partagé par l'ensemble des protocoles (notamment ZK-NR, AOW, SH) d'assurer que les parties ne peuvent contester leurs actions ou la validité des preuves générées.
Résilience Post-Quantique	Hypothèse de sécurité essentielle pour tous les travaux. Elle est principalement assurée par la dureté de l'**AIIP** (AIIP, CEE, AOW, SH) ou par l'intégration de primitives connues pour leur résistance (Dilithium dans ZK-NR).
Opposabilité Juridique	Intégration d'une dimension institutionnelle (Opposability, H_{Opp} dans CRO) pour que les preuves soient admissibles, auditable et explicables (SH, ZK-NR).
Fondement Théorique	Tous les composants (CEE, AOW, SH) et les cadres (ZK-NR, CASH) sont alignés sur la gestion des contraintes établies par le **Trilemme CRO**.

TABLE 2 – Différences d'Approche et Rôle Spécifique

Travail	Niveau	Contribution Spécifique (Axe CRO)
Trilemme CRO	**Théorique**	**Contrainte** : Définit l'impossibilité de satisfaire simultanément C, R, O. Établit la borne Γ_{CRO}.
Q2CSI	**Architecture**	**Cadre de Solution** : Propose un modèle modulaire (*Fer-Or-Argile*) pour composer des primitives (UC model) et minimiser Γ_{CRO}.
AIIP	**Hypothèse**	**Fondation Cryptographique** : Garantit l'authenticité et l'intégrité des preuves contre les attaques quantiques (base de CASH).
CEE	**Primitive**	**Confidentialité (C)** : Assure la préservation de l'entropie sémantique par expansion chaotique post-quantique.
AOW	**Primitive**	**Fiabilité (R)** : Garantie de la vérification temporelle et de l'ordonnancement dans les systèmes distribués.
SH	**Primitive**	**Opposabilité (O)** : Offre l'explicabilité institutionnelle et l'extraction algébrique nécessaires à l'admissibilité juridique.
ZK-NR	**Protocole**	**Application Pratique** : Intègre les primitives dans une architecture concrète avec preuve de concept (Tamarin) pour des usages réglementés.

III Acteurs et Communauté Scientifique

L'écosystème scientifique et industriel autour des preuves à divulgation nulle de connaissance (Zero-Knowledge), de la cryptographie post-quantique et de l'investigation numérique est porté par plusieurs pôles de recherche et d'innovation.

III.1 Pôle A : Zero-Knowledge et STARKs

Parmi les figures majeures, on retrouve **Eli Ben-Sasson**, co-inventeur des ZK-STARK et cofondateur de la société **StarkWare**, à l'origine de solutions telles que StarkEx et StarkNet. Ses travaux se situent au croisement de la théorie cryptographique et du déploiement industriel à grande échelle. Dans le même domaine, **Alessandro Chiesa**, professeur à UC Berkeley puis à l'EPFL, a participé à la création de la bibliothèque **libsnark** et au protocole **Zerocash**, pionniers dans l'ingénierie des SNARKs. Le chercheur **Jens Groth** est quant à lui connu pour le schéma **Groth16**, une construction de preuves succinctes particulièrement influente dans la communauté (Crypto 2016). Enfin, **Matthew D. Green** (Université Johns Hopkins) s'est distingué par ses contributions aux systèmes **Zerocash/Zcash** et par ses analyses critiques des systèmes cryptographiques appliqués.

III.2 Pôle B : Cryptographie Post-Quantique

La cryptographie post-quantique s'impose comme une priorité face aux menaces posées par l'ordinateur quantique. Des chercheurs tels que **Daniel J. Bernstein (DJB)**, co-auteur des signatures **SPHINCS** et **SPHINCS+**, jouent un rôle clé dans la conception de schémas résistants au quantique. Le **NIST**, à travers son processus de standardisation (PQC), fédère une grande partie de cette recherche en évaluant et sélectionnant les algorithmes de la future génération de signatures et de chiffrement, notamment **CRYSTALS**, **SPHINCS+**, **FALCON** et **HQC**.

III.3 Pôle C : Sécurité Formelle et Composabilité

Ce pôle, davantage théorique, concerne la sécurité formelle et la composabilité. Dans ce domaine, **Ran Canetti** est une figure incontournable grâce à la création du cadre de la **Universal Composability (UC)**, qui permet de formaliser la sécurité des protocoles cryptographiques dans des environnements complexes et modulaires.

III.4 Pôle D : Investigation Numérique et Opposabilité Juridique

Le lien entre cryptographie et investigation numérique se manifeste dans les travaux de **Eoghan Casey**, auteur de l'ouvrage de référence *Digital Evidence and Computer Crime*, qui a largement contribué à définir les standards de la preuve numérique dans les enquêtes judiciaires. Ses travaux illustrent l'importance de relier les garanties cryptographiques aux exigences légales d'opposabilité.

III.5 Pôle E : Projets et Entreprises

Plusieurs entreprises et projets jouent également un rôle moteur. **StarkWare** incarne la traduction industrielle des STARKs, en travaillant sur la scalabilité et la mise en production de ces preuves dans l'écosystème blockchain. **Zooko Wilcox-O'Hearn**, fondateur de **Zcash** et de l'**Electric Coin**

Company, est un acteur clé de la mise en œuvre pratique des protocoles Zero-Knowledge appliqués à la confidentialité des transactions.

III.6 Pôle F : Groupes Académiques et Industriels

Enfin, un sixième pôle regroupe les grandes équipes académiques et industrielles. Des institutions comme le **MIT**, **Berkeley**, le **Technion** ou encore l'**INRIA** participent activement à la recherche sur les SNARKs, les STARKs et leurs applications. Dans le domaine post-quantique, les groupes impliqués dans le développement de **CRYSTALS**, **FALCON**, **HQC** et **SPHINCS+** représentent une force collective d'innovation. Les dépôts collaboratifs tels que **arkworks** ou **libsnark** illustrent la dynamique communautaire qui anime la cryptographie contemporaine.

IV Rôle du ZK-NR dans l'Investigation Numérique

IV.1 Besoins des enquêteurs

Dans le cadre des enquêtes numériques, les magistrats et les forces de l'ordre se heurtent à plusieurs contraintes majeures :

— **Garantir l'intégrité des preuves collectées** : une preuve numérique est par nature volatile et altérable. Les enquêteurs doivent donc s'assurer que le contenu d'un disque dur, d'un message électronique ou d'un log réseau n'a subi aucune modification entre sa collecte et sa présentation au tribunal.

— **Prouver la non-répudiation des actes** : il ne suffit pas de montrer qu'une donnée existe ; il faut aussi démontrer de façon irréfutable que l'acte est bien attribuable à une personne donnée (ex. : un e-mail signé électroniquement par l'auteur présumé).

— **Préserver la confidentialité des données sensibles** : certaines enquêtes impliquent des données personnelles ou stratégiques. Il est indispensable de protéger ces informations tout en permettant une vérification cryptographique de leur validité.

— **Assurer la traçabilité et la chaîne de possession (chain of custody)** : chaque mouvement d'une preuve (collecte, transfert, stockage, analyse) doit être enregistré de manière fiable et opposable.

V Apports du ZK-NR et CLO

Les innovations récentes, notamment le protocole **ZK-NR (Zero-Knowledge Non-Repudiation)** et le cadre **CLO (Cryptographic Legal Opposability)**, répondent à ces besoins :

V.1 Besoins des enquêteurs

Dans le cadre des enquêtes numériques, les magistrats et les forces de l'ordre se heurtent à plusieurs contraintes majeures :

— **Garantir l'intégrité des preuves collectées** : une preuve numérique est par nature volatile et altérable. Les enquêteurs doivent donc s'assurer que le contenu d'un disque dur, d'un message électronique ou d'un log réseau n'a subi aucune modification entre sa collecte et sa présentation au tribunal.

— **Prouver la non-répudiation des actes** : il ne suffit pas de montrer qu'une donnée existe ; il faut aussi démontrer de façon irréfutable que l'acte est bien attribuable à une personne donnée (exemple : un e-mail signé électroniquement par l'auteur présumé).

— **Préserver la confidentialité des données sensibles** : certaines enquêtes impliquent des données personnelles ou stratégiques. Il est indispensable de protéger ces informations tout en permettant une vérification cryptographique de leur validité.

— **Assurer la traçabilité et la chaîne de possession (chain of custody)** : chaque mouvement d'une preuve (collecte, transfert, stockage, analyse) doit être enregistré de manière fiable et opposable.

V.2 Apports du ZK-NR et CLO

Les innovations récentes, notamment le protocole **ZK-NR (Zero-Knowledge Non-Repudiation)** et le cadre **CLO (Cryptographic Legal Opposability)**, répondent à ces besoins :

— **Création d'attestations invisibles mais vérifiables** : grâce aux preuves à divulgation nulle de connaissance (Zero-Knowledge Proofs), un enquêteur peut prouver l'existence ou la validité d'une information (exemple : une transaction frauduleuse) sans révéler les données sensibles associées.

— **Transformation de la chaîne de possession en un processus certifié cryptographiquement** : chaque transfert ou manipulation de la preuve est scellé par une signature et une preuve cryptographique, garantissant que la chaîne de possession n'a subi aucune altération.

— **Résilience face aux attaques quantiques** : l'usage de primitives post-quantiques (Dilithium, SPHINCS+) permet d'anticiper la menace des ordinateurs quantiques, qui pourraient casser les schémas classiques RSA ou ECC.

— **Opposabilité juridique renforcée** : ZK-NR et CLO ajoutent une dimension institutionnelle, permettant de produire des preuves numériques qui respectent à la fois les standards cryptographiques et les exigences juridiques de recevabilité.

V.3 Cas pratiques

Cyberfraude bancaire – Cameroun, 2022

Contexte : Le parquet de Yaoundé a instruit une affaire de fraude où des cybercriminels avaient réussi à pirater les systèmes d'une banque locale via du phishing et des malwares.
Investigation numérique : Analyse des logs de connexion pour identifier les IP utilisées. Exploitation des empreintes numériques laissées dans les transactions. Usage de techniques de corrélation d'adresses blockchain pour retracer les flux d'argent converti en crypto-actifs.

Résultat : Plusieurs suspects ont été arrêtés. Les preuves numériques (hash des disques durs, échanges WhatsApp et courriels piégés) ont été présentées devant le tribunal.
Lien cryptographie : Hashage SHA-256 pour l'intégrité des preuves et conservation en base scellée par signatures électroniques. **Cyberescroquerie BEC (Business Email Compromise) – Yaoundé, 2021**

Contexte : Une société étrangère opérant au Cameroun a porté plainte après avoir été victime d'une escroquerie par e-mails usurpés (faux ordres de virement signés au nom du DG).
Investigation numérique : Extraction des entêtes d'e-mails falsifiés pour tracer les serveurs relais. Corrélation avec les journaux des fournisseurs d'accès internet pour identifier les cybercriminels. Exploitation de l'analyse forensique des ordinateurs saisis (présence de logiciels de spoofing).

Résultat : Les preuves collectées ont démontré l'usurpation et ont permis de récupérer une partie des fonds.

Lien cryptographie : Absence de signature numérique légale (PKI) facilitant la fraude, soulignant la pertinence de solutions comme ZK-NR/CLO.

Affaire "SIMBOX" – Cameroun, 2019

Contexte : Des fraudeurs installaient des SIMBOX pour détourner le trafic téléphonique international et le faire passer pour des appels locaux, causant des pertes colossales aux opérateurs et à l'État.

Investigation numérique :

- Géolocalisation des équipements frauduleux via analyse réseau.
- Saisie et imagerie forensique des serveurs utilisés pour la redirection des appels.
- Vérification cryptographique des journaux de trafic fournis par les opérateurs.

Résultat : Démantèlement d'un réseau international avec des ramifications en Afrique de l'Ouest.

Lien cryptographie : Utilisation de preuves scellées par empreintes numériques pour empêcher toute contestation devant le parquet.

Cas international – Affaire EncroChat (Europe, 2020)

Contexte : EncroChat fournissait des téléphones "chiffrés" à des milliers de criminels. Les autorités ont réussi à infiltrer le système.

Investigation numérique :

- Exploitation des failles dans le chiffrement propriétaire.
- Récupération massive de communications chiffrées (drogue, assassinats commandités, blanchiment).

Résultat : Plus de 6 500 arrestations en Europe.

Lien cryptographie : Montre comment le chiffrement, mal implémenté, peut être retourné contre les criminels.

VI Positionnement dans l'investigation numérique moderne

Dans le paysage actuel de l'investigation numérique, où la dématérialisation des échanges et la complexité des environnements techniques augmentent, l'intégration de mécanismes

cryptographiques avancés n'est plus un luxe mais une nécessité.

— **Par rapport aux méthodes traditionnelles** : les approches classiques reposaient principalement sur le hashing (SHA-256, MD5) et les signatures électroniques simples. Si elles restent utiles, elles montrent leurs limites face aux menaces quantiques ou aux exigences légales internationales.

— **Apport des nouvelles approches** : ZK-NR, CLO et les primitives CASH (CEE, AOW, SH) permettent de franchir un cap en conciliant sécurité technique et recevabilité juridique.

— **Vers une convergence crypto-légale** : l'investigation numérique moderne n'est pas seulement un défi technique, c'est aussi un enjeu d'opposabilité. L'enquêteur doit produire des preuves exploitables devant des juges, dans des contextes nationaux ou transfrontaliers. Les technologies cryptographiques émergentes assurent cette convergence entre rigueur scientifique et valeur juridique.

Conclusion

L'évolution de la cryptographie, de simple outil de protection des communications à instrument d'opposabilité juridique, transforme profondément le champ de l'investigation numérique.

Désormais, les enquêteurs ne cherchent pas seulement à sécuriser ou à cacher les informations, mais à produire des preuves **authentiques, vérifiables, inaltérables et légalement recevables**. Les protocoles comme ZK-NR, les cadres comme CLO, ainsi que les primitives post-quantiques, ouvrent la voie à une nouvelle génération de pratiques forensiques où la preuve numérique devient incontestable devant un tribunal.

Ainsi, l'investigation numérique moderne ne se limite plus à collecter des données, mais s'inscrit dans une démarche intégrée où la cryptographie devient le **garant de la vérité numérique**.

Références

1. Thierry Emmanuel Minka Minguidoi, Mani Onana Flavien Serge, Djotio Ndié Thomas, *Exploring ZK-NR : A Layered Cryptographic Architecture for Explainable Non-Repudiation*, Cryptology ePrint Archive, Paper 2025/1138. https://eprint.iacr.org/2025/1138
2. Thierry Emmanuel Minka Minguidoi et coauthors, *The CRO Trilemma : Incompatibility Between Confidentiality, Reliability, and Legal Opposability*, Cryptology ePrint Archive, Paper 2025/1348. https://eprint.iacr.org/2025/1348
3. Thierry Emmanuel Minka Minguidoi et coauthors, *Q2CSI 2025 : Quantum-Compliant Cryptographic Systems Investigation*, Cryptology ePrint Archive, Paper 2025/1380. https://eprint.iacr.org/2025/1380
4. Thierry Emmanuel Minka Minguidoi et coauthors, *Design ZK-NR : Layered Post-Quantum Protocol for Legally Explainable Zero-Knowledge Non-Repudiation*, Cryptology ePrint Archive, Paper 2025/1422. https://eprint.iacr.org/2025/1422
5. Thierry Emmanuel Minka Minguidoi et coauthors, *Formalizing ZK-NR : UC-Security Under Contextual Entropy Constraints*, Cryptology ePrint Archive, Paper 2025/1529. https://eprint.iacr.org/2025/1529
6. Thierry Emmanuel Minka Minguidoi et coauthors, *The AIIP Problem : Post-Quantum Hardness via Affine Iterated Inversion*, Cryptology ePrint Archive, Paper 2025/1590. https://eprint.iacr.org/2025/1590
7. Thierry Emmanuel Minka Minguidoi et coauthors, *Chaotic Entropic Expansion (CEE) : Post-Quantum Data Confidentiality Primitive*, Cryptology ePrint Archive, Paper 2025/1615. https://eprint.iacr.org/202
8. Thierry Emmanuel Minka Minguidoi et coauthors, *Affine One-Wayness (AOW) : Post-Quantum Temporal Verification via Polynomial Iteration*, Cryptology ePrint Archive, Paper 2025/1662. https://eprint.iacr.org/2025/1662
9. Thierry Emmanuel Minka Minguidoi et coauthors, *SH : Post-Quantum Secure Hashing and Signature Constructions*, Cryptology ePrint Archive, Paper 2025/1708. https://eprint.iacr.org/2025/1708
10. Cyberfraude bancaire – Cameroun, 2022 : businessincameroon.com
11. Cyberescroquerie BEC – Yaoundé, 2021 : lefinancierdafrique.com
12. Affaire SIMBOX – Cameroun, 2019 : agenceecofin.com
13. Affaire EncroChat – Europe, 2020 : europol.europa.eu